報告書

平成 21 年度産業技術研究開発委託費

（産学連携ソフトウェア工学実践事業

（クラウド・コンピューティング時代の Dependability の考え方などに関する米国の動向調査））

平成 22 年 2 月

株式会社アイ・ビー・ティ

目次

第１章　米国における先進的クラウド基盤の利活用状況とその導入にあたっての課題等 ..3
1.1.　クラウド・コンピューティング概念の登場 3
1.2.　NIST によるクラウド・コンピューティングの定義と標準化..... 5
1.2.1.　クラウドにおける NIST の役割とクラウド標準の策定 8
1.2.2.　NIST のクラウド定義 11
1.3.　クラウド・コンピューティングの問題点と課題 22
1.3.1.　クラウド・コンピューティングのリスク要因..... 22
1.3.2.　NIST によるクラウド・コンピューティングの課題と問題点の分析..... 27
1.3.3.　連邦情報セキュリティマネジメント法（FISMA）と NIST..... 31
1.3.4.　データ分散とデータ・プライバシー 40
1.3.5.　サービスレベル契約（SLA） 47
1.3.6.　CSA 等によるクラウド・セキュリティの分析と提言 52
1.4.　オバマ政権におけるクラウド・コンピューティングへの対応..... 65
1.4.1.　2010 年度予算案では、連邦クラウドを重視..... 65
1.4.2.　オバマ政権における連邦 CIO の任命..... 72
1.4.3.　クンドラ連邦 CIO のクラウド・コンピューティング見解 80
1.4.4.　GSA（総合サービス管理局)と連邦クラウド CTO 兼内務省 CTO の任命..... 84
1.4.5.　GSA（総合サービス管理局）による RFQ（見積依頼書） 85
1.5.　連邦政府によるクラウド構築事例..... 92
1.5.1.　GSA（総合サービス管理局）の“Apps.gov”..... 92
1.5.2.　GSA（総合サービス管理局）のクラウド・コンピューティング戦略..... 93
1.5.3.　DOD の Net-Centric 戦略と DISA/ RACE 106
1.5.4.　DISA（国防情報システム局）の RACE 107
1.5.5.　DOD の“ソーシャル・メディア”..... 111
1.5.6.　NASA の Nebula..... 113
1.5.7.　NIEM（National Information Exchange Model） 115
1.6.　【付属資料：現地調査と調査結果】 118
1.6.1.　【付属資料 1：連邦政府関係機関へのインタビュー調査】 118
1.6.2.　【付属資料 2：米国現地インタビューの追跡調査】 141
1.7.　業界団体におけるクラウド・コンピューティングの取組動向..... 161
1.7.1.　OMG によるクラウド標準開発の提案 162
1.7.2.　オープンクラウドマニフェスト 165
1.7.3.　Open Cloud Consortium（OCC） 174
1.8.　主な IT 会社のクラウド・コンピューティングの取組事例..... 176
1.8.1.　マイクロソフト（MS）のクラウド対応 176

1.8.2. 主なクラウド・プラットフォームとクラウド・ベンダーの資料 182
第２章 米国におけるスマートグリッド動向 192
2.1. 最新の米国スマートグリッド政策 192
2.1.1. スマートグリッド法制化までの沿革 192
2.1.2. エネルギー政策法（EPACT）とエネルギー自立&安全保障法（EISA） .. 196
2.1.3. スマートグリッド政策 198
2.1.4. オバマ政権誕生後のスマートグリッド政策の動向 210
2.2. 米国における主な電力グリッドの研究 215
2.2.1 グリッドワイズ・アライアンス 215
2.2.2 電力中央研究所（EPRI） 218
2.2.3 NIST（国立標準技術研究所） 225
第３章 ソフトウェアアシュアランス（SwA）とシステムアシュアランス（SA） 231
3.1. IT を利活用した米国連邦政府の危機管理対策 233
3.1.1 米国の重要インフラ防護対策 233
3.2. ソフトウェアアシュアランスおよびシステムアシュアランス 239
3.2.1 定義 239
3.2.2 国土安全保障省（DHS）の国家サイバー・セキュリティ部門（NCSD） .242
3.2.3 国防省（DOD）の DISA 254
3.2.4 NSA（国家安全保障局）とアシュアードソフトウェアセンター（CAS） .273
3.2.5 その他の動向 275
3.3. 民間によるシステム&ソフトウェアアシュアランスの動向 292
3.3.1 オープングループ（Open Group）の“ProSE”イニシアティブ 294
3.3.2 欧州の ProSE(Promoting Standardization for Embedded Systems) 299
3.3.3 Software Assurance Form for Excellence in Code（SAFECode) 303
【文献及び資料、インタビュー先等】 305

第１章　米国における先進的クラウド基盤の利活用状況とその導入にあたっての課題等

1.1. クラウド・コンピューティング概念の登場

Google のシュミット CEO が 2006 年 8 月 9 日に開催された“検索エンジン戦略会議”の席で“クラウド・コンピューティング”の言葉を使い、電子メールやグループウェア、ERP や CRM などの SaaS (Software as a Service)、仮想化されたアプリケーションサーバやデータベースを提供する PaaS (Platform as a Service)、インターネット経由でハードウェアやインフラを提供する HaaS (Hardware as a Service) または IaaS (Infrastructure as a Service) などインターネットを介して新たなサービスを提供するビジネスモデルが登場した。このビジネスモデルは、IBM や Cisco Systems、Google、Amazon.com、Salesforce.com、マイクロソフトなどにより提供され、自前でコンピュータシステムを所有しないユーザーに対して、コンピュータ資源が“雲の中に隠れている (in The Cloud)”かのように見えない形で IT サービスを提供する。また、IBM や Cisco Systems、HP などの世界的 SI 会社は、インターネット技術を使い IT 機能をユーザーに提供するクラウド・コンピューティングを強化し、サーバーなどの IT 機器を集積したデータセンターの機能を強化し、省エネ・省スペース化や信頼性向上を集中的に進めている。

しかし、クラウド・コンピューティングの定義は各社により異なる。2009 年 5 月 20 日に開催された“2009 MIT Sloan CIO Symposium”のパネルディスカッションの席上、米国 Cisco Systems のサーバ･アクセス／仮想化事業部門担当 CTO であるエド･バグニオン(Ed Bugnion)は、クラウド・コンピューティング技術について、“基本的に、データセンターにおける IT に仮想化技術を導入したもの”と説明し、きわめて大きな発展性を秘めていると語っている。

クラウド・コンピューティングの本質は、「IT の所有から利用へ」である。ユーザーは自前でハードウェアやソフトウェアなどの IT 資産を取得しないでも、対価を払って第 3 者のサービス・プロバイダーを利用する。クラウド・コンピューティングのインフラは、データセンターから提供され、また、異なるレベルの仮想化技術で構築される信頼できるサービスである。ユーザーは、ユーザー数やデータ数の変動を吸収できる仮想化技術を使用したサービス・プロバイダーのデータセンターから提供されるサービスを、インターネットを介して低コストで利用することができる。

クラウド・サービスのメリットは、①割安な IT 関係コスト（アップグレード費やハードウェアなど設備投資コストの軽減、自社用業務アプリケーション開発コストが不要)、②人

的リソースの節約、③柔軟なシステム規模の変更、④ビジネスの成長拡大に応じた極めて高いスケーラビリティの IT 関連機能の拡充などにあると専門家は指摘する。

しかし、クラウド・コンピューティングの利用に際しては、リスクも伴う。ユーザーの利用ニーズに応じて、クラウド・ベースのサービスが適切なのかどうか、また利用可能なサービスのうち適切なものはどれかを十分に分析する必要がある。特定のデータベース集約型アプリケーションを必要とし、厳しい規制を受ける医療などの業種では、クラウド・サービスよりも自社運用型システムを使うほうが賢明との見解も示されている。

クラウド・コンピューティング技術の進展に伴い、コスト効果、人的リソースの節減、柔軟なシステム変更などのユーザメリットは極めて大きくなるが、反面、ベンダーにとっては、ユーザーからの大量のリアルタイム情報を預かって処理することになることから、従来以上に情報システム・ソフトウェアには高い信頼性が求められることになる。

Cisco Systems のジョン・チェンバース（John Chambers）CEO も、インターネット上のサービスとして従量制でコンピューティングを売るという潮流は、“セキュリティ上の悪夢”だと語り、クラウド・コンピューティングの甘美な世界に、クラウドの暗部（Dark Side of Cloud）が潜むことを忠告する。したがって、クラウド基盤に求められる信頼性レベルとその担保のためのソフトウェアエンジニアリングが極めて重要な課題となる。

クラウド・コンピューティングの発展は、コストと人的リソースの節減という利点に加えて、膨大な情報の効果的かつ適切な利活用による企業経営の高度化や生活の質の向上という大きなメリットをもたらすと期待されている。

IDC のシニア バイスプレジデント兼主席アナリスト、Frank Gens によれば、クラウド・コンピューティングの成長率は、2011～2012 年が 25%、2012 年～2013 年が 30%強になると予測され、今後の成長は加速化するだろう。B2B 電子商取引ソリューションのプロバイダーである GXS は、2009 年の e-Commerce 予測の中で、①ERP を B2B クラウドにインテグレーションする難題が解決され、サプライサイドとバイサイドの両ユーザーが同データを使い、サプライチェーンの効率性を高めるようになること、②アマゾン、グーグル、マイクロソフト、セールスフォースのクラウド・プラットフォームが B2B のサービス提供を行うためのパートナーを積極的に探し求めるか、あるいは自社技術を開発するようになること、③銀行が本来の貸付や CD（譲渡性預金証書）の販売などのバンキング業務に力を入れるようになり、現在の業務プロセスや法人顧客や一般顧客向けのサービスを改善するようになり、e-Commerce が活発化することなどを指摘している。

1.2. NISTによるクラウド・コンピューティングの定義と標準化

クラウド・コンピューティングとは何か。どこで、どのよう方法で実装するのか。クラウド・コンピューティングを導入すれば、どのようなチャンスがあるのだろうか。クラウドの問題点と課題は何か。米国では、クラウド・コンピューティングを巡り様々な混乱と議論が生まれている。

クラウド・コンピューティングという専門用語については、①グリッド・コンピューティング、②ユーティリティ・コンピューティング、③オートノミック・コンピューティングの3つと混乱する場合が多い。

①「グリッド・コンピューティング（Grid Computing）：分散型コンピュータおよび並列コンピュータのひとつ形態で、極めて大きなタスクを履行する協調処理で使うネットワーク型の緩やかに連結されるコンピュータで構成されるスーパー＆バーチャルコンピュータ。
②「ユーティリティ・コンピューティング（Utility Computing）：電力などの公益に類似した従量制課金するサービスするコンピューティング・リソースのパッケージ。
③「オートノミック・コンピューティング（Autonomic Computing）：2001年にIBMにより発表された、環境や状況への変化の対応を、人間の自立神経に例えて、自立的に処理するコンピュータシステム。

一般的に、グリッド・コンピューティングは、大規模なタスクを履行して、ITサービスの消費量を計測する超大型のコンピューティング・リソースの集合を繋ぐものとみなされ、クラウド・コンピューティングのITパラダイム変革を引き起こした技術である。また、クラウド・コンピューティングは、1970年代のモデルである“タイムシェアリング”の最新バージョンだと語る者もいる。実際、タイムシェアリングは、コンピューティング能力のコストを大幅に引き下げている。

ガートナーグループでは、クラウド・コンピューティングを、“インターネット技術を使う外部顧客へのサービスとして、極めて大きな拡張性と弾力性のあるIT関連能力を提供するコンピューティング形態（A style of computing whose massively scalable and elastic, IT-related capabilities are provided ‘as a service’ to external customers using Internet technologies.”と定義する。

Forresterグループは、クラウド・コンピューティングを次のように定義している。

- “インターネットをベースにするサービス、ソフトウェアまたはITインフラなどの標準化されたITに基づく能力（Capability）の一形態で、どのコンピュータからでもアクセス可能で、需要に応じて常に利用可能で拡張性があり、ペイパービューまたは広告ベースの料金払いで、Webまたはプログラムによる制御インターフェースを持ち、完全な顧客のセルフサービスを可能にするサービス・プロバイダーにより提供される（A form of standardized IT-based capability - such as internet-based services, software, or IT infrastructure - offered by a service provider that is accessible via Internet protocols from any computer, is always available, and scales automatically to adjust to demand, is either pay-per-use or advertising-based, has Web- or programmatic-based control interfaces, and enables full customer self-service.）。”

Webサービスやクラウド・サービスの専門家の間で定評のあるWikipediaでは、次のように定義されている。

- “Cloud computing is Internet- ("cloud-") based development and use of computer technology ("computing"). In concept, it is a paradigm shift whereby details are abstracted from the users who no longer need knowledge of, expertise in, or control over, the technology infrastructure "in the cloud" that supports them. Cloud computing describes a new supplement, consumption and delivery model for IT services based on the Internet, and it typically involves the provision of dynamically scalable and often virtualized resources as a service over the Internet. The term cloud is used as a metaphor for the Internet, based on the cloud drawing used to depict the Internet in computer network diagrams as an abstraction of the underlying infrastructure it represents. Typical cloud computing providers deliver common business applications online which are accessed from a web browser, while the software and data are stored on servers. These applications are broadly divided into the following categories: Software as a Service (SaaS), Utility Computing, Web Services, Platform as a Service (PaaS), Managed Service Providers (MSP), Service Commerce, and Internet Integration. The name cloud computing was inspired by the cloud symbol that is often used to represent the Internet in flow charts and diagrams.”

InfoWorldのGalen GrumanとEric Knorrによると、クラウド・コンピューティングは、「新規ITインフラ投資、人材の新規雇用、新ソフトウェアのライセンシングを行わなくと

も、能力と容量を拡充する方法のひとつ」であり、インターネットを介してリアルタイムで会員制またはペイパービュー方式で利用できるITサービスである。また、「仮想化とSOA（サービス指向アプローチ）が企業内で浸透してくると、機敏性と拡張性を備えたITインフラ上で動作する緩やかに結合したサービスという考え方が進展し、すべての企業はやがてクラウド内のノード（ネットワーク構成要素）のひとつになろう」。しかし、その道のりは極めて遠いことにも留意する必要がある。

Amazonの副社長兼CTOのWerner Vogelsは、クラウド・コンピューティングを成功させるために実現すべき重要な目的と原則を次の通り列挙している。

- Security（セキュリティ）
- Scalability（拡張性）
- Availability （可用性）
- Performance （パフォーマンス）
- Cost-effective（コスト効果）
- Acquire resources on demand （オンデマンドによるリソースの取得）
- Release resources when no long needed （不必要時にリソースをリリース）
- Pay for what you use （使った分だけを負担する）
- Leverage other's core competencies （他のコアな強みを逆利用する）
- Turn fixed cost into variable cost（固定コストを変動コストに転換する）

米国のNIST（国立標準技術研究所）によると、クラウド・コンピューティングの土台となる基本的な技術は、次の通りである。

- 仮想化（Virtualization）
- グリッド技術（Grid Technology）
- SOA（サービス指向アーキテクチュア）
- 分散型コンピューティング（Distributed Computing）
- ブロードバンドネットワーク
- プラットフォームとしてのブラウザー
- フリー＆オープンソースソフトウェア

その他の必要な技術は次の通りである。

- Autonomic Systems（自立系システム）
- Web 2.0

- Web アプリケーションフレームワーク
- SLA（サービスレベル契約）

クラウドの信頼性とセキュリティの確保を目指す業界団体の「Cloud Security Alliance（CSA）」は、2009 年 12 月 17 日に公表した“Security Guidance for Critical Areas of Focus in Cloud Computing（クラウド・コンピューティングの重点分野のためのセキュリティ指針） V2.1”の中で、クラウド・コンピューティングを、既存のコンピューティングを何か異なるものに変化させようとする数多くの技術とアプローチを指す専門用語であると説明した。そしてクラウド・コンピューティングは、「土台となるインフラ（underlining infrastructure）とサービス提供メカニズムからアプリケーションと情報資源を切り離す」もので、「最適かつ効率的なコンピューティングを通じてコラボレーション、アジリティ（敏捷性）、拡張性および可用性を高め、潜在的なコスト削減をもたらすものである」と解説している。

CSA（クラウド・セキュリティ・アライアンス）によると、クラウド・コンピューティングは、規模の経済性と標準化のメリットをもたらすものの、セキュリティ面では課題が多いと指摘する。しかし、CSA も、クラウドの定義に関しては、NIST（国立標準技術研究所）によるクラウド・コンピューティングの定義を受け入れている。また、NIST によるクラウド・コンピューティングの定義は、多くの連邦政府の CIO や業界団体からも一般的に受容されている。

1.2.1. クラウドにおける NIST の役割とクラウド標準の策定

NIST は、産業界および政府機関の様々な専門家と協議し、将来的な研究のための基礎となるクラウド・コンピューティングの定義を公表し、最新のアップデートを行なっている。

クラウド・コンピューティングにおける NIST の役割は、テクニカルガイダンスを提供し、標準化を促進することにより、政府および産業における実効性の高い技術活用とそのセキュアな利活用を奨励することである。NIST は、政策を策定する立場にはない。

NIST によるクラウド標準のミッションは、すべての関係当事者がクラウド・コンピューティングから最大価値を得ることを可能にするために、クラウド・コンピューティング標準の策定と管理についての指針（ガイダンス）を産業界と政府に提供することである。NIST は、クラウド標準を振興するために、①必要な標準開発ロードマップの提案、②産業界が各業界の標準を策定することを支援するキャタリスト（触媒役）として行動すること、③政府および産業界におけうクラウド標準の導入促進などの意向を表明している。

加えて、NISTは、クラウド・コンピューティングに関する一連の刊行物を発行し、①クラウド・コンピューティングがどのような問題を解決するのか、②クラウド・コンピューティングの技術特性とな何か、③セキュリティを確保しつつクラウド・コンピューティングの長所をどのように活用するのかなどを明らかにする計画である。

NIST（米国国立標準技術研究所）によるクラウド標準策定努力の目標は、次の通りである。

- 代替可能クラウド（Fungible clouds）
  - （相互代替サービス、mutual substitution of services）
  データおよびカストマーアプリケーションのポータビリティ
  - 共通のインターフェース、セマンティック、プログラミング・モデル
  - 連携セキュリティサービス（Federated security service）
  - ベンダーは、効果的な実施の面で競い合う。
- 付加価値サービスを促進する。
  - 先進的技術
  - ベンダーは、イノベーション力で競い合う。

NISTは最小限のクラウド標準を明確にし、①セキュアなクラウドのインテグレーション、アプリケーション・ポータビリティおよびデータ・ポータビリティを実現可能にし、②イノベーションのを阻害するオーバースペックを回避し、③様々なクラウド・モデルには個別に対応する提案を準備している。

クラウド標準開発のロードマップ策定に向けた複数の考え方は次の通りである。

- クラウド標準に関する考え方
  - 通常、SPI（Service Provider Interface）スタックを進めると、サービスのロックインが強まる（クラウド・サービスから離れなくなる）。（IaaS->PaaS->SaaS）
  - IaaSは、既存の企業データセンターからの自然な成り行きの移行ポイント。基本的なサービスは、コンピューティング、ストレージおよびネットワーキング。
  - バーチャルマシーン（VM）は、代替可能クラウドの中核。
  - セキュリティとデータのプライバシー懸念は、クラウド・コンピューティングの採用に際しての最大の障害である。

- 結果
  - 1番目の主要な成果物として、IaaSの全体的な標準ロードマップに焦点を絞り込む。
  - 次の段階で、PaaSとSaaSのロードマップを調査研究する。
  - 可能な限り早急に上記の標準を策定する共同作業を促す。
  - IaaS、PaaSおよびSaaS横断的にセキュリティとデータのプライバシー標準に対する共通のニーズを検証する。
- IaaS標準のロードマップ：必要な標準
  - VM（仮想マシーン）イメージの配布。例、DMTFのOVF（Open Virtualization Format）。
  - VMの準備と制御（provisioning and control）。例、AmazonのEC2 API）
  - Inter-cloud VM exchange
  - 永続性ストレージ（Persistent storage）。例、Azure Storage、S3、EBS、GFS、Atmos。
  - VM SLAs
  - セキュアなVMコンフィギュレーション。例、SCAP。
- PaaSとSaaSの標準ロードマップ
  - 知財権の問題もあり、困難な作業である。
  - NISTの将来的な課題である。
  - PaaSの標準は、①サポート・プログラム言語と②クラウド・サービス用APIを具体化する可能性がある。
  - SaaSの標準は、①SaaS特有の認証と権限付与、②XMLスキーマなどのデータのImport/Exportフォーマット、③各アプリケーションには個別の標準化などを行う可能性がある。
- IaaS、PaaSおよびSaaS横断的にセキュリティとデータのプライバシー標準
  - すでに数多くの標準が存在する。
  - IDおよびアクセス管理（IAM）
  - アイデンティティ・マネージメント（IdM）連携。例、SAML、WS-Fえでらちおｎ、Liberty ID-FF
  - 強固な認証標準。例、HOTP、OCRA、TOTP。
  - データの暗号化、キーマネジメント。例、PKI、PKCS、KEYPROV（C-KIP、DSKPP）、EKMI。
  - E-discovery。例、EDRM

1.2.2. NISTのクラウド定義

ピーター・メル（Peter Mell）をリーダーとする米国 NIST（国立標準技術研究所）のクラウド研究チームは、クラウドのアーキテクチュア、セキュリティ、連邦政府における利活用戦略を調査研究している。ピーター・メルは、NIST 情報技術ラボ・コンピュータセキュリティ部門のシニアコンピュータサイエンストである。ピーター・メル（Peter Mell）とタイム・グランス（Time Grance）を中核とする NIST コンピュータセキュリティ部門のクラウド担当チームは 2009 年 5 月 21 日、産官連携によりクラウド・コンピューティングのワーキング定義を策定し、これを公表した。

NISTは常にクラウド定義の見直しを行なっており、最新版のクラウド定義は、2009年10月7日に公表されたバージョン15である。NISTは、クラウド・コンピューティングの概念を全般的に記述するだかではなく、クラウドの5つの基本特性、3つのクラウド・サービス提供モデル、4つのクラウド利活用モデルを示している。NISTのピーター・メルによると、NISTのクラウド担当チームは、何もかもすべてを網羅して曖昧な定義を行なう民間企業とは異なり、科学者として可能な限り偏見のない形で拡張性を持たせた定義を行なったようである。

クラウド・コンピューティングの定義に際して、ピーター・メルとタイム・グランスは次の2点に留意すべきだと注意を促している。

① クラウド・コンピューティングは、今も進化を続けるパラダイムである。この定義、利用例、対象となる技術、問題点、リスクおよび便益は、公的部門および民間部門による議論を通じて精査される。したがって、クラウドの定義、属性および特性は時の経過に伴い進化・変動するものである。
② クラウド・コンピューティング業界は、数多くのモデル、ベンダーおよび市場ニッチの生の声を代弁するが、NISTは様々なアプローチ手法を網羅する形で以下のような定義を行なっている。

2009年10月7日に公表されたバージョン15におけるクラウド・コンピューティングの定義は次の通りである。

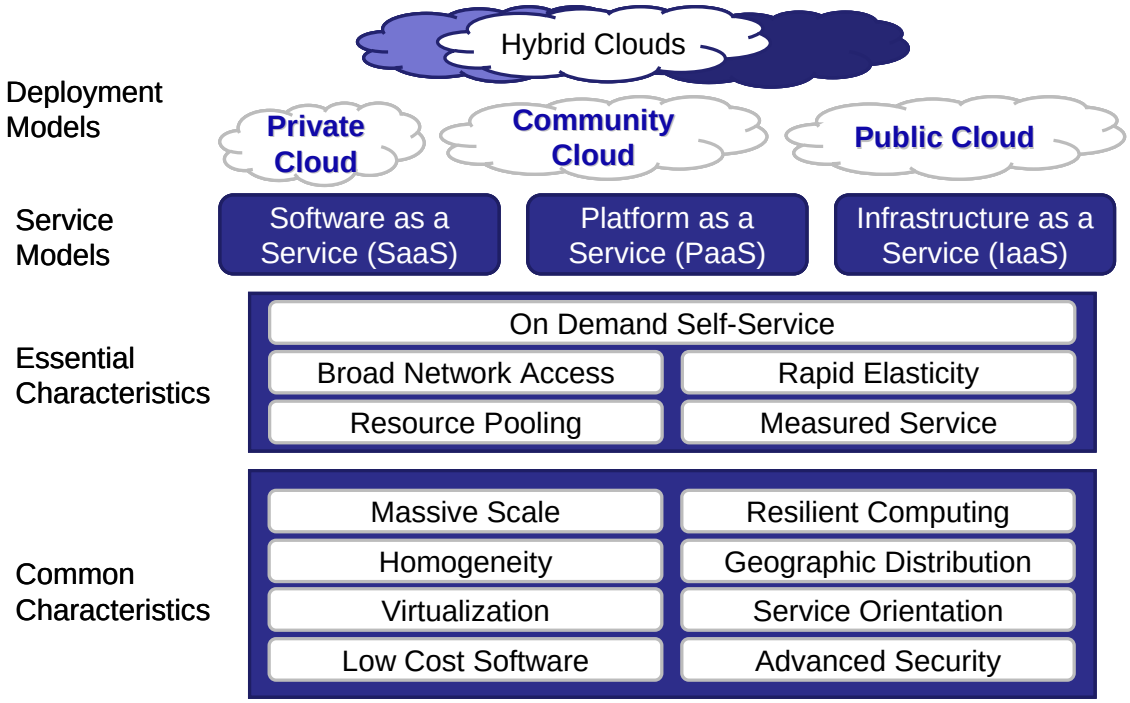
- クラウド・コンピューティングとは、最低限のマネジメント努力またはサービス・プロバイダーの対応（interaction）で、迅速に準備およびリリースすることができる、コンフィギュレーション可能なコンピューティング資源（つまり、ネット

ワーク、サーバー、ストレージ、アプリケーションおよびサービス）の共有プールに対するオンデマンドによる便利なネットワークアクセスを可能とするモデルである。このクラウド・モデルは、可用性（availability）を高めるもので、**5つの基本特性**、**3つのサービス・モデル**と**4つの利活用モデル**から構成される。

原文は次の通り。

- Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of **five essential characteristics**, **three service models**, and **four deployment models**.

図 1　NIST によるクラウドの定義フレームワーク



- 5 つの基本特性（essential characteristics）は、次の通りである。

① オンデマンド・セルフサービス：コンシューマは、人手を介さずに各サービスのプロバイダーと対応して、自動的に必要なサーバ・タイムとネットワーク・ストレージなどのコンピューティング能力を備えることができる。

・ A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service’s provider.

② ブロードネットワーク・アクセス：コンピューティング能力は、ネットワークを介して、携帯電話、ラップトップおよび PDA などの同質的なシン・クライアントまたはシック・クライアントのプラットフォームによる標準的な利用促進メカニズムを通じてアクセスされる。

・ Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

③ リソース・プーリング（ロケーションの独立性）：プロバイダーのコンピューティング資源はプールされ、コンシューマの需要に応じて物理的リソースおよび仮想的リソースをダイナミックに割当・再割当して、マルチテナントモデル

を使う複数のコンシューマにサービスを提供する。コンシューマは、提供されるリソース（コンピューティング資源）の正確なロケーション（保管場所）をコントロールすることも認知することもできないが、国、州またはデータセンターの所在地を特定する可能性はある。このリソースの事例は、ストレージ、処理、メモリ、ネットワーク帯域幅、バーチャルマシーン（VM）である。

- The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

④ 迅速な弾力性（Rapid Elasticity）：場合によっては自動的に、スケール・アウトおよびスケール・インを迅速かつ弾力的に行なえるコンピューティング能力を備えられる。コンシューマにとっては、クラウド・サービスの準備に際して利用可能な能力は無限であるともみられ、ユーザーは必要な時に必要な量を購入することが可能である。

- Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

⑤ 計測済みサービス（Measured Service）：クラウド・システムは、サービスのタイプ（例、ストレージ、処理、帯域幅、アクティブ・ユーザアカウント）に相応する抽象度（level of abstraction）で計測する能力を梃子として使いリソース利用の統制・最適化を自動的に行なう。リソース利用は、利活用されるサービスのプロバイダーとコンシューマの両方にとって透明性のある形でモニタリングし、統制・報告することが可能である。

- Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

しかし、上記のクラウド・サービスは、仮想化技術との関連で利用されることが多いが、必ずしも仮想化技術との関連で利用されるものではないことに留意することが大切である。また、マルチテナントはクラウドの基本的な特性ではないことを認識しておくことが大切である。加えて、マルチテナントモデルは必ずしもクラウドの基本的な特性ではないことに留意すべきである。

また、クラウド・コンピューティングには次のレバレッジ特性がある（これは、2009年6月時点でのバージョンで追記されていた内容であるが、Version 15では割愛されているが、NISTによるPresentationの中に示されている）。

- 大規模（Massive scale）
- 同質性（Homogeneity）
- 仮想化（Virtualization）
- 回復力のあるコンピューティング（Resilient computing）
- 低コストソフトウェア（Low cost software）
- 地理的分散型配布（Geographic distribution）
- サービス指向（Service orientation）
- 先進的セキュリティ技術（Advanced security technologies）

● クラウド・コンピューティングのサービス提供モデルは、サービスとしてのソフトウェア（S）、プラットフォーム（P）およびインフラストラクチュア（I）の3つの頭文字から略称して“SPIモデル”と呼ばれている。この3つのサービス・モデルの定義は次の通りである。

① Cloud Software as a Service（SaaS）：コンシューマに提供されるコンピューティング能力は、クラウド基盤（インフラ）上で稼動するプロバイダーのアプリケーションを利用することである。このアプリケーションは、Webブラウザー（Webベースのe-mail）のようなシン・クライアントのインターフェースを介して様々なクライアント・デバイスからアクセスされる。コンシューマは、ネットワーク、サーバー、OS、ストレージまたは個々のアプリケーションを含む対象となるクラウド基盤を管理または統制することはできない。唯一の例外は、限定的なユーザー固有アプリケーションのコンフィギュレーション設定である。

- The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface

such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

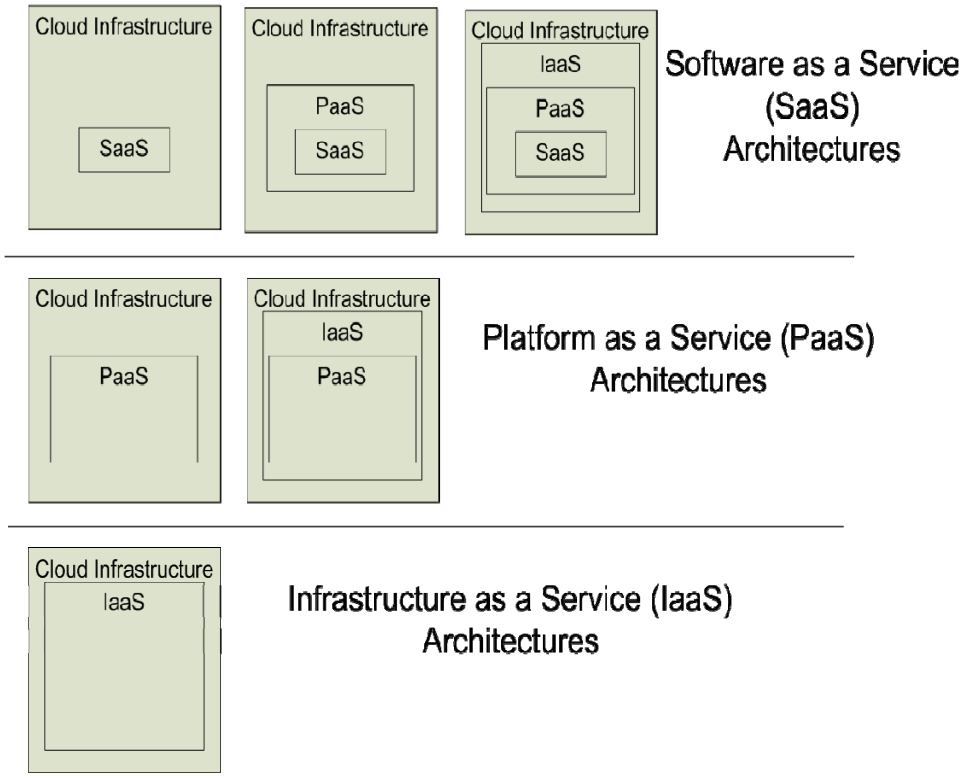
② Cloud Platform as a Service (PaaS) ：コンシューマに提供されるコンピューティング能力は、プロバイダーによりサポートされるプログラム言語とツールを使いコンシューマが開発または取得したアプリケーションをクラウド基盤上で利活用することである。コンシューマは、ネットワーク、サーバー、OS またはストレージを含む対象となるクラウド基盤を管理または統制することはできないが、利活用するアプリケーションをコントロールすることは可能である。

- The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed.

③ Cloud Infrastructure as Service (IaaS) ：コンシューマに提供されるコンピューティング能力は、コンシューマが、OS とアプリケーションを含む専用ソフトウェアを利用・実行することが可能な場所で、処理、ストレージ、ネットワークおよびその他の基本的なコンピューティング資源を備えることである。コンシューマは、土台をなすクラウド基盤 (underlying cloud infrastructure) を管理または統制できないが、OS、ストレージ、利活用するアプリケーションを制御し、更には、特定のネットワーク・コンポーネント（ホストのファイアウォール）を限定的にコントロールするも可能である。

- The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

図 2　サービス・モデルのアーキテクチュア



【NIST の旧バージョン等によるクラウド提供モデルを踏まえた解釈】

① Cloud Software as a Service (SaaS) ：ネットワークを介してプロバイダーのアプリケーションを利用すること。インストール済みのパソコン上でアプリケーションを購入するようなソフトウェア供給モデルが、サービスとしてのソフトウェア（SaaS）である。コンシューマは、ネットワークを介して、プロバイダーが提供するサービスとしてのソフトウェアを“利用する”形のソフトウェア供給モデルである。したがって、コンシューマはアプリケーションを使えるが、アプリケーションを稼動させる OS、ハードウェアまたはネットワーク基盤をコントロールすることができない。コンシューマに提供されるコンピューティング能力は、クラウド基盤（cloud infrastructure）上で稼動し、Web ブラウザー（Web ベースの e-mail）のようなシン・クライアント（thin client）インターフェースを介して様々なクライアント・デバイスからアクセスすることができるプロバイダーのアプリケーションを利用する（use）ことである。コンシューマは対象となるクラウド基盤、ネットワーク、サーバー、OS、ストレージまたは個々のアプリケーションを制御することはできない。

- 米国調査チームの Gates & Co.によると、SaaS 基盤のアプリケーションのアーキテクチュアは、複数のユーザー企業が同時に利用する形のマルチテナント（multi-tenancy）を専ら支援することを目的として設計されている。SaaS は、“pay-as-you-go”方式のライセンスモデルに類似したサービス形態で、SaaS 基盤のアプリケーション管理モデルは ASP モデルに類似している。
- IDC の調査レポート（2009 年 1 月）では、76%の米国法人が 2009 年末までに最低 1 本の SaaS で提供される業務用アプリケーションを利用するとみて、SaaS の伸び率を 2008 年の 40.5%に対して 2009 年には 36%になると観測している。また、IDC は、最低 25%の IT 予算を SaaS ベースのアプリケーションに投資する計画にある米国企業が 2008 年の 23%から 2010 年には約 45%にまで増えると予測している。
- Gartner グループでは、新規ソフトウェア供給の約 30%が 2010 年までに SaaS モデルにより供給されるとみている。2009 年 5 月 7 日のガートナー調査レポートによると、世界の SaaS 市場は 2009 年に 80 億ドルとなる、2008 年の 66 億ドルに比べて約 22%増になると予想。エンタープライズ向けアプリケーションでは、世界の SaaS 売上は 2013 年までに 160 億を突破するだろうとの見方を示している。

② **Cloud Platform as a Service (PaaS)** ：ユーザーが開発したアプリケーションをクラウド内で利活用すること。クラウド・コンピューティングには、Web ベースのカスタム・アプリケーションを構築・稼動するためのプラットフォームが含まれる。コンシューマは、そのアプリケーションを稼動するためのホスティング環境を利用する。プラットフォームはバーチャルマシーン（VM）であるが、アプリケーションフレームワークでもよい。コンシューマに提供されるコンピューティング能力は、プロバイダーによりサポートされるプログラム言語とツール（Java、Python）Net）を使いコンシューマが作成したアプリケーションをクラウド基盤上で利活用することである。コンシューマは、ネットワーク、サーバー、OS またはストレージを含む対象となるクラウド基盤を管理または統制することはできないが、利活用するアプリケーションをコントロールすることは可能である。

- PaaS は、ダウンロードや設定を行なわなくともインターネットを介して OS および関連サービスを提供するものである。PaaS(Platform as a Service)は、コンピューティング資源を私的に所有するコンピュータからインターネットへと動かすことから、“Cloudware”とも呼ばれている。PaaS は、SaaS から派生した概念である。PaaS では、OS の特性を頻繁に変更・更新することが可能である。また、地理的に分散した環境にある開発チームが、同一のソフトウェア開発の共同作業を行なうことも可能になる。複数の機能を履行し、互換性問題に直面するマルチハードウェア環境を利用するのに比べて、

単一のベンダーからインフラ関連サービスを利用するために、初期コストも継続コストも節減することができ、プログラム開発努力を一元化できることにより、トータル経費を最小化することも可能となる。

③ **Cloud Infrastructure as a Service (IaaS)** ：Wikipedia によると、IaaS は、プラットフォーム仮想化環境の中でサービスとしてのコンピュータ・インフラストラクチュアを提供することである。IssS により、ユーザーは、Rent 処理、ストレージ、ネットワーク容量およびその他の基本的なコンピューティング資源を備えることが可能になる。オリジナルの用語は、2006 年 5 月にエコノミストの Nicolas Carr が使った Hardware as Service(HaaS)である。コンシューマは、処理能力、ストレージ、ネットワークコンポーネントまたはミドルウェアのような基本的なコンピューティング・リソースを使う。コンシューマに提供されるコンピューティング能力は、コンシューマが、OS とアプリケーションを含む専用ソフトウェアを利用・実行することが可能な場所で、処理、ストレージ、ネットワークおよびその他の基本的なコンピューティング資源を備えることである。コンシューマは、土台をなすクラウド基盤（underlying cloud infrastructure）を管理または統制できないが、OS、ストレージ、利活用するアプリケーションを制御し、更には、特定のネットワーク・コンポーネント（ホストのファイアウォール）を限定的にコントロールするも可能である。

上記の 3 つのサービス・モデルを“クラウド”とみなすためには、基本的な特性を持つクラウド・インフラストラクチュアの上で利活用しなければならない。

NIST の定義するサービス・モデルでは、様々なクラウドのサービス・プロバイダーとユーザーとの間の関係を調整し、モニタリング、ガバナンス、プロビジョニング（準備）、インテグレーションなどのサービスを提供する仲介業者（Cloud Service Brokers）に関連するサービス・モデルの定義には言及されていない。API（Application Programming Interface）やインターフェースを開発するクラウド・サービスのブローカーが将来的に重要なイノベーションの動力になることを勘案すると、Open Cloud Computing Interface Working Group、Amazon EC2 API、VMware’s DMTF-submitted vCloud API、Sun’s Open Cloud API、Rackspace API、GoGrid’s API など API の取り組むにも留意すべきであると、CSA（クラウド・セキュリティ・アライアンス）はコメントしている。

- 4 つのクラウド利活用モデル（Cloud Deployment Model）は次の通りである。

① プライベート・クラウド：特定の組織のためだけに運転されるクラウド・インフラストラクチュアのことである。これは、組織または第三者によりマネジメントされるもので、当該組織の施設または施設外に存在することもある。→特定の組織が所有またはリースする形の専用目的のクラウド利用。

・ The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

② コミュニティ・クラウド：このクラウド基盤は、複数の組織により共有され、特定のミッション、セキュリティ要件、政策、コンプライアンス留意事項などの利害を共有する特定コミュニティをサポートする。コミュニティ・クラウドは、当該組織または第三者によりマネジメントされ、施設の内外に存在する。→特定のコミュニティ向けの共有クラウド・インフラストラクチュア。

・ The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

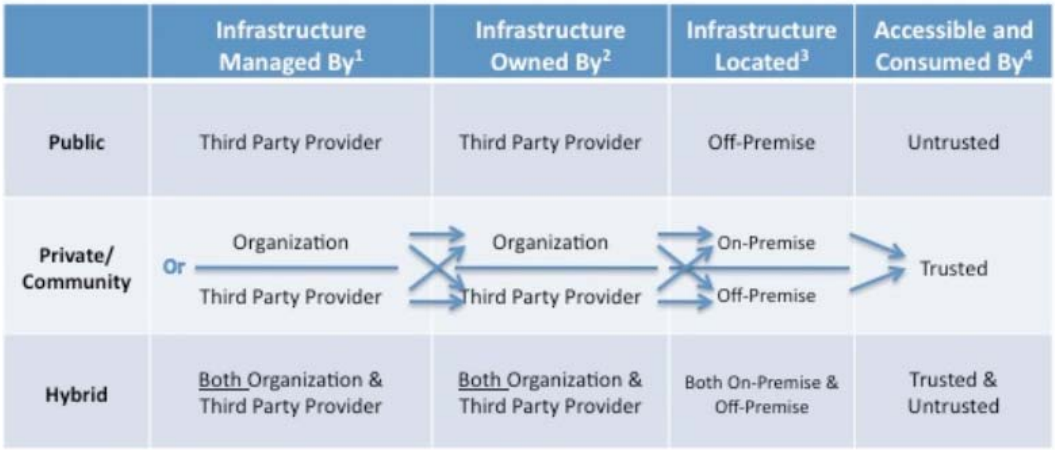
③ パブリック・クラウド：このクラウド基盤は、一般大衆または大規模な業界団体に利用され、クラウド・サービスを販売する組織により所有される。→一般大衆向けに販売されるクラウド・インフラストラクチュア。

・ The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

④ ハイブリッド・クラウド：このクラウド基盤は、プライベート・クラウド、コミュニティ・クラウドまたはパブリック・クラウドの中の２つ以上のクラウドの合成で、ユニークな実体であるが、クラウド間の負荷バランスのためのクラウド拡張（cloud bursting）のような標準化された技術または知財権をもつ技術と結びついている。

・ The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

図 3　クラウド利活用モデル



出所：Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, CSA, December 2009

表 1　NIST（国立標準技術研究所）によるクラウド・コンピューティングの定義

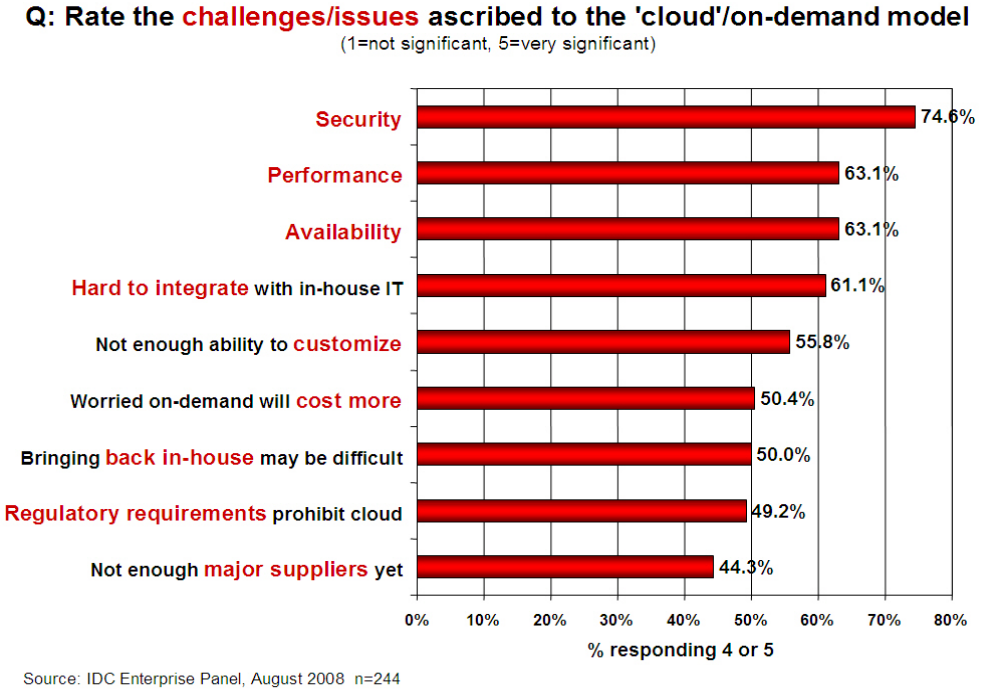
5 つの基本特性	① オンデマンド･セルフサービス (On-demand self-service) ② ブロードネットワーク・アクセス (Broad network access) ③ リソース・プーリング (Resource pooling) ④ 迅速な弾力性 (Rapid Elasticity) ⑤ 計測済みサービス (Measured Service)
3 つのサービス･モデル	① Cloud Software as a Service (SaaS) ② Cloud Platform as a Service(PaaS) ③ Cloud Infrastructure as Service(IaaS)
4 つの利活用モデル	① プライベート・クラウド ② コミュニティ・クラウド ③ パブリック・クラウド ④ ハイブリッド・クラウド

1.3. クラウド・コンピューティングの問題点と課題

1.3.1. クラウド・コンピューティングのリスク要因

2008年8月のIDC Enterprise Panelレポートによると、“クラウド/オンデマンド”で最も重要な課題および問題点は、“セキュリティ（74.6%）”であり、次に、パフォーマンス（63.1%）、可用性（63.1%）、社内ITシステムとのインテグレーションの難しさ、カストマイズ能力が十分ではないこと、On-demandによる先行きのコスト負担増などとなっている。

図 4　IDC Enterprise Panel レポート、2008 年 8 月



ユニシスは2009年9月、クラウド・コンピューティングに影響を及ぼす問題点に関するオンライン調査の結果を発表した。クラウド導入に際しての最大の障害について312人のIT専門家に質問したところ、約51%の専門家がセキュリティとデータ・プライバシーの懸念を挙げている。2番目の障害は、クラウド基盤のアプリケーションの既存システムへのインテグレーション問題である。

アクセンチュアは、クラウド・コンピューティングを導入に際して認識しておく留意点を2009年10月のレポートの中で示している。本レポートによると、他の先進的テクノロジ

ーと同様、クラウド・コンピューティングは、ビジネスや組織のメリットにつながるが、反面、重要な問題点と課題をはらんでいる。アクセンチュア・テクノロジー・ラボでは、技術面と組織面に関連する6つの主要な課題を次の通り指摘する。

① セキュリティ：クラウドの導入を検討する大半の企業にとって、最も重要な目先の懸念は、セキュリティである。具体的には、第3者であるサービス・プロバイダーが管理する環境の中で、どのようにして自社データのセキュリティ保障措置を講じるのかという問題点である。多くのクラウド・サービスのプロバイダーは顧客データのセキュリティを確実に保障することを中核事業としていることから、この分野では大きな進展をみせている。クラウド・プロバイダーの多くは、企業単独のデータセンターに比べると、より精緻なエンド・ツー・エンドのレベルセキュリティとプライバシー保護を提供している。例えば、Amazon（アマゾン）では、顧客データのプライバシー保護を確保するために、利用するストレージの各ブロックを自動的にクリーンナップする知財権のあるディスク仮想化レイヤーで標準のハイパーバイザー（バーチャルマシーンを実現する制御プログラム）の機能強化を図っている。また、シティバンクなどの大手金融機関もクラウド・ソリューションを導入していることから考慮すると、クラウドは当該金融機関の初期検証にも無事に合格したと言える。しかし、データ・コントロールや認証などのオープンな問題点については未解決な部分も残されている。今後のクラウド・コンピューティングの普及速度は主に、これらの問題解決と、クラウド・サービスのプロバイダーが第3者機関からセキュリティのビジネスプラクティスに関する公的認証を取得できるかどうかに左右されることになろう。

② データのロケーション（保管場所）、データ・コンプライアンスおよびインテグレーション：2番目に重要な問題点は、データのロケーション（保管場所）、コンプライアンスおよびインテグレーションを巡るデータ関連である。現行のクラウド・ソリューションでは、データをクラウド内に蓄積する必要がある。つまり、ひとつのユーザー企業が同時に1～2社のクラウド・プロバイダーを利用せざるをえないのが現状である。クラウド市場は極度に細分化された状態にあり、特定の垂直市場に特化したアプリケーション・プロバイダーの数も約700社前後となっている。プロバイダーの整理統合が不可避となろうが、大半のユーザー企業は結局、複数のクラウドを利用せざるをえない可能性が高い。この結果、多くのユーザー企業は、クラウド横断的に分散するデータと、自社のデータセンターにファイアウォールで防護されたデータを同時に取り扱う必要性に直面するだろう。更に困難なことは、クラウド・オペレータは、銀行や医療などの顧客データを特定の司法管轄圏内で蓄積管理することを求める政府規制を遵守しなければならない。このデータの細分化により、ユーザー企業は、極めて大きなインテグレーション問題にも直面することになる。加えて、総合的なエンタープライ

ズアーキテクチュアを開発することも重要な課題となる。

③ サービスレベル保証（SLG）：3番目に重要なは、サービスレベル保証（Service Level Guarantee）である。大半のエンタープライズ・アプリケーションには、特定水準のサービスが求められる。従来型のオン・サイトでの設定では、IT部署がアプリケーションの動作する物理的環境とソフトウェア環境を管理するために、このような要求を容易に満たすことができる。しかし、クラウドになると事態は異なる。この動作環境を管理するアプリケーション・クラウド・プロバイダーは、データがインターネットを介して転送されることから、レスポンス・タイムを保証することはできない。インフラストラクチュア・クラウドの場合には、他の組織からソフトウェア・コードをサポートすることになるために、この課題はより難しくなる。大手プロバイダーは着実に改善努力を払っているが、サービスレベル保証（SLG）の課題が解決されない限り、重要なエンタープライズ・アプリケーションをクラウドへと移行させるのは困難であろう。

④ レガシーシステム：4番目の課題は、レガシーシステムに関連している。レガシー・アプリケーションはクラウドに適合しない。大手ユーザー企業の中核事業にはレガシーシステムがクリティカルであることが多いが、現在のクラウド・インフラストラクチュアはこれをサポートするサービスレベルに欠けている。加えて、多くのレガシー・アプリケーションは基礎となるハードウェアと密接に結びついているために、コストのかかるシステムの再設計を行なわない限り、クラウドの特徴である仮想化と並列化のメリットを受けることができない。レガシー・アプリケーションが組織内にあることだけでも、大手企業の重要なIT機能の目先のクラウド移行の阻害要因となろう。

⑤ 購入プロセス：5番目の課題は、クラウド・サービスの実際の購入プロセスに関するものである。一般的に、Pay-as-you-go方式によるITサービスの利用は、資本を支出しなくとも、営業経費として処理できるので、調達の観点からすれば、極めて魅力的である。しかし、実際には、他のビジネス上の経費処理のようにクレジットカードで決済し、それを経理部門で清算するような柔軟性のあり経理処理を行なうユーザー企業は少ない。クラウド・コンピューティングの利用が進化・発展するに伴い解消される問題ではあるが、クラウドの調達方法やクラウド環境の中ではどのような企業契約を締結するのかという課題が今後の難点になろう。

⑥ ライセンシング：6番目の課題は、ライセンシングに関連したものである。ユーザー数やCPUの数、メトリクスを示す従来のソフトウェアのライセンシングモデルは、クラウド・コンピューティングには簡単に転用できない。エンタープライズ・ソフトウェア

のライセンス計算は極めて難しく、弾力性とスケールアップのための仮想化技術を特徴とするクラウド・コンピューティングでは、エンタープライズ・ライセンスのポータビリティ問題を解決し、時間単位のソフトウェアの利用を計るような別の計算方法が必要となる。

ガートナーは、クラウド・コンピューティングのセキュリティ・リスク評価（Assessing the Security Risks of Cloud Computing）と題した2008年6月付けレポートの中で、クラウド・コンピューティングにはセキュリティ・リスクがあるために、ユーザー企業はクラウド・サービスを利用する前に次の7つのセキュリティ問題に留意する必要があると指摘する。

① 権限を付与されたユーザー・アクセス（Privileged user access）：アウトソーシングされるサービスは、企業のIT部門が社内プログラムに対して行使する“物理的、論理的および人的管理”を迂回することになるために、社外で処理される機密性のあるデータ（Sensitive Data）は、その固有レベルのリスクを包含するものである。社内データをマネジメントする人々に関する可能な限りの情報を入手しなければならない。ユーザー企業の経営陣は、クラウド・サービスのプロバイダーには、権限を付与された管理者の採用と監視に関する特定の情報提供と、彼らのアクセスに対する統制を依頼すべきである。

② 規制コンプライアンス（Regulatory Compliance）：サービス・プロバイダーにより保管されていても、カストマー（ユーザー）が自社データのセキュリティと完全性（integrity）に対する最終責任を負うことになる。従来型のサービス・プロバイダーは外部監査とセキュリティ認証を受ける。しかし、この外部審査を拒否するクラウド・コンピューティングのプロバイダーには、最も瑣末な機能の利用しか依頼できないことに留意すべきである。

③ データのロケーション（保管場所）：クラウドを利用すると、恐らく、どこに自社のデータが保管されているのかが分からなくなる。事実、どの国に自分のデータが保管されているのかも分からない。サービス・プロバイダーに対して、特定の司法管轄権の及ぶ範囲でデータを保管・処理しているのかどうか、また、顧客のために顧客の拠点のある現地のプライバシー要件を遵守する契約上のコミットメントを行なえるかどうかを確認する必要がある。

④ データの隔離（Data Separation）：クラウド内のデータは通常、他の顧客から預かるデータと伴に共有環境で保管される。暗号化（Encryption）は効果的な手法であるが、

必ずしも万全ではない。どのような方法で、保存データ（data at rest）を隔離しているかを把握しておくべきだと、ガートナーは助言する。クラウド・プロバイダーは、暗号化スキームを設計し、これを経験の豊富な専門家による検証を受けているとの確証を提出すべきである。暗号化による事故はデータを全く使えなくなることで、正規の暗号化でも可用性（Availability）を損なうこともある。

⑤ 復旧（Recovery）：データがどこに保管されているのかが分からなくとも、クラウド・プロバイダーは、災害発生時には、貴社のデータとサービスがどうなるのかをユーザーに伝える義務がある。データとアプリケーション・インフラストラクチュアのレプリカを複数のサイトに用意していないプロバイダーのクラウド・サービスは、完全な障害に晒される危険性がある。

⑥ 調査協力（Investigative Support）：不適切な行為や違法行為を捜査することは、クラウド・コンピューティングでは不可能である。マルチ顧客のログイン記録やデータを共同保管し、常に変化するホストやデータセンターに分散管理しているために、クラウド・サービスは特に、調査（捜査）することが難しい。特定の調査に協力するという契約上のコミットメントを得られない限り、調査と復旧を望む要求は実現されない可能性が高い。

⑦ 長期的な実行可能性（Long-term viability）：倒産に陥るとか、大手に吸収合併・買収されることのないクラウド・サービスのプロバイダーを選別することが理想的である。そうした事態になったとしても、貴社のデータが確実に入手可能なようにしておく必要がある。プロバイダーの選択では、貴社のデータをどのようにして返却してもらえるのか、代替アプリケーションに移植可能なフォーマットを利用できるのかどうかを確認する必要がある。

1.3.2. NISTによるクラウド・コンピューティングの課題と問題点の分析

NIST（米国国立標準技術研究所）のピーター・メル（Peter Mell）とタイム・グランス（Time Grance）によると、クラウド・セキュリティの主要な問題点は、“信頼性（trust）”、“マルチテナント（multi-tenancy）”、“暗号化（encryption）”、“コンプライアンス（compliance）”である。クラウドは、巨大な複雑系システムあるが、数千もの時間と共通の機能ユニット複製する単純な原始形態（simple primitives）に縮小可能なものである。したがって、クラウド・セキュリティは、“手に負えない問題（tractable problem）”であるが、これは優位性でもあり、チャレンジでもある。クラウド・コンピューティングには、長所もあれば、欠点もある。

以下は、NISTによるクラウド・セキュリティの長短分析の要点を整理したものである。

- 一般的なクラウド・セキュリティの優位性は次の通り。
  - パブリック・データを外部のクラウドに移行することで、内部の機微データ（機密性のあるデータ：Sensitive Data）のリスク・エクスポージャが縮小する。
  - クラウドの同質性は、セキュリティ監査/検証を簡素化する。
  - クラウドにより、自動化セキュリティ管理が可能となる。
  - 冗長性/災害復旧（Redundancy/Disaster Recovery）が高まる

- 一般的なクラウド・セキュリティの課題
  - ベンダーのセキュリティモデルを信頼すること。
  - カストマー（ユーザー）は、監査で発見された事柄に対応する能力がない。
  - 調査（捜査）協力の確認。
  - 間接的なアドミニストレーター（管理者）の説明責任。
  - 知財権の実行（Proprietary implementation）を検証できない。
  - 物理的コントロールのロス（損失）

- セキュリティに関連するクラウド・コンポーネント
  - クラウド・プロビジョニング（準備）サービス

    優位性

    ・迅速なサービスの再構築

    ・可用性を可能にする：多数のデータセンター・マルチインスタンスを準備

    ・先進的Honeynet能力

課題

・サービス準備を解決することのインパクト

- クラウド・データストレージサービス

優位性

・データの断片化と分散（Data fragmentation and dispersal）

・自動レプリケーション（AR）

・データゾーンのプロビジョニング（準備）（国別）

・蓄積および転送データの暗号化（Encryption at rest and in transit）

・自動データ保持（Automated data retention）

課題

・アイソレーション管理/データマルチテナント

・ストレージコントローラ：単一障害点/解決？（Single point of failure/compromise?）

・外国政府へのデータの露出

- クラウドプロセシング基盤

優位性

・マスターのセキュリティを保護し、セキュアなイメージをプッシュアウトする能力（Ability to secure masters and push out secure images）

課題

・アプリケーション・マルチテナント

・ハイパーバイザーへの依存（Reliance on hypervisors）

・プロセスアイソレーション/アプリケーションサンドボックス（Application sandboxes）

- クラウド・サポートサービス

優位性

・オンデマンド・セキュリティコントロール（認証、ロギング、ファイアウォール）

課題

・カストマーアプリケーションとのインテグレーション時の追加リスク

・別個のアプリケーションとして承認および運用認可（certification and accreditation）を必要とする。

・コードの更新

- クラウド・ネットワーク＆周辺セキュリティ（Perimeter Security）

優位性

・分散型サービス保護の拒絶（Distributed denial of service protection）

・バーチャルLAN（VLAN）能力

・境界セキュリティ（IDS、ファイアウォール、認証）

課題

・Application Mobilityの仮想化ゾーニング（Virtual zoning）

- 弾性要素（Elastic Elements）：ストレージ、プロセシング、バーチャルネットワーク

- クラウド・セキュリティの優位性（第一部）
  - データの断片化と分散（Data Fragmentation and Dispersal）
  - セキュリティ専門家グループ（Dedicated Security Team）
  - セキュリティ基盤投資を増強（Greater Investment in Security Infrastructure）
  - フォールトトレランスと信頼性（Fault Tolerance and Reliability）
  - レジリエンシー（回復力）の強化（Greater Resiliency）
  - ネットワーク攻撃に対するハイパーバイザー（VMの制御プログラム）防護（Hypervisor Protection Against Network Attacks）
  - 承認&運用認可努力の軽減（Possible Reduction of C&A Activities -Access to Pre-Accredited Clouds）

- クラウド・セキュリティの優位性（第二部）
  - コンプライアンス（法令遵守）分析の簡素化（Simplification of Compliance Analysis）
  - 第3者のクラウド・ベンダーによるデータ保管（Data Held by Unbiased Party-cloud vendor assertion）
  - 低コストによる災害回復とデータストレージソリューション（Low-Cost Disaster Recovery and Data Storage Solutions）
  - オンデマンド・セキュリティコントロール（On-Demand Security Controls）
  - リアルタイム改竄検出システム（Real-Time Detection of System Tampering）
  - 迅速なサービス再構築（Rapid Re-Constitution of Services）
  - 先進的ハニーネット能力（Advanced Honeynet Capabilities）

- クラウド・セキュリティの課題（チャレンジ）

（第一部）

  - データ分散と国際プライバシー法（Data dispersal and international privacy laws）

・EU データ保護指令と米国商務省セーフハーバープログラム（EU Data Protection Directive and U.S. Safe Harbor program）
・データの外国政府へのエクスポージャ（露出）とデータ召喚命令（Exposure of data to foreign government and data subpoenas）
・データ保持の諸問題（Data retention issues）

- データ隔離管理の必要性（Need for isolation management）
- マルチテナント（Multi-tenancy）
- ロギングの課題（Logging challenges）
- データ所有権の諸問題（Data ownership issues）
- サービス保証の質（Quality of service guarantees）

（第二部）

- セキュアなハイパーバイザー（VM の制御プログラム）への依存（Dependence on secure hypervisors）
- ハッカーにとって魅力的/攻撃価値が高い（Attraction to hackers-high value target）
- クラウド内のバーチャル OS のセキュリティ（Security of virtual OSs in the cloud）
- 大規模停電が発生する可能性（Possibility for massive outages）
- クラウド・コンピューティングの暗号化ニーズ（Encryption needs for cloud computing）

・クラウド・リソース制御インターフェースへのアクセスの暗号化（Encrypting access to the cloud resource control interface）
・OS インスタンスへの管理者アクセスの暗号化（Encrypting administrative access to OS instances）
・アプリケーションへのアクセスの暗号化（Encrypting access to applications）
・蓄積アプリケーションデータの暗号化（Encrypting application data at rest）

- パブリック・クラウド対内部クラウド・セキュリティ（Public cloud vs. internal cloud security）
- パブリック SaaS 版セキュリティコントロールの欠如（Lack of public SaaS version control）

NIST のピーター・メル（Peter Mell）とタイム・グランス（Time Grance）は、2009 年 10 月 7 日に公表したプレゼンテーション資料の“Effectively and Securely Using the Cloud Computing Paradigm”の中で、“クラウド・コンピューティングのその他の問題点と課題”を次のように提起している。

- 個人 ID 情報（PII）と機微なデータをクラウドに移行することに伴う諸問題（Issues with moving PII and sensitive data to the cloud）
  - プライバシー影響評価（Privacy impact assessments）

- サービスレベル契約（SLA）を使いクラウド・セキュリティを取得すること（Using SLAs to obtain cloud security）
  - クラウド SLA の要求事項の提案（Suggested requirements for cloud SLAs）
  - クラウド鑑識（フォレンジック）に伴う諸問題（Issues with cloud forensics）

- クラウド実行時における緊急対応計画と災害復旧（Contingency planning and disaster recovery for cloud implementations）

- コンプライアンス（法令遵守）対応（Handling compliance）
  - FISMA（2002 年連邦情報セキュリティマネジメント法）
  - HIPAA（2003 年健康保険携帯責任法）
  - SOX（2002 年サーベンス・オクスリー法）
  - PCI（決済カード業界）のコンプライアンスガイド
  - SAS 70 Audits（米国公認会計士協会が定めた監査基準書第 70 号：外部に業委託する際に委託先の内部統制を検証することを義務づける。受託業務にかかわる内部統制について独立した監査人が企業の管理体制の方針や手続きの整備状況およびその有効性に関して検証し、その結果について企業に対して報告するための基準）

上記の問題点と課題の多くは、Cloud Security Alliance（CSA）等のクラウド関連の非営利機関等が“Security Guidance for Critical Areas of Focus in Cloud Computing”のバージョン 1.0 および 2.0 において精力的な研究調査の労作を発表している。クラウド・セキュリティの主な問題点と課題については、次の「CSA 等によるクラウド・セキュリティの分析と提言」の中で記載する。

1.3.3. 連邦情報セキュリティマネジメント法（FISMA）と NIST

クラウド・コンピューティングのセキュリティ問題解決にむけた連邦政府の努力を分析する際には、2002 年の連邦情報セキュリティマネジメント法（FISMA）と NIST（国立標準技術研究所）による連邦政府の情報セキュリティ強化に向けた一連の取組内容を追跡調査する必要がある。特に、オバマ政権下の連邦政府は、セキュリティ・リスクに晒される脆

弱性を持つとみなされる連邦政府クラウド・コンピューティングの導入と普及を本格的に始動させたことから、2002 年の FISMA コンプライアンスを遵守する義務と責任を持つ連邦各省庁は FISMA コンプライアンスの手引書である NIST の FIPS（Federal Information Processing Standards）と Special Publication 800 シリーズに準拠した情報セキュリティ強化の対応をクラウド・プロバイダーに要請することになるためである。

FISMA は連邦情報処理標準を定めた FIPS の遵守を連邦各省庁に義務づけており、行政管理局（OMB）が連邦各省庁に対して Special Publication 800 シリーズ等の NIST 特別刊行物を遵守することを要請する責任を担っている。各省庁の履行能力が乏しいと判断された場合には、行政管理局（OMB）は要望予算を廃止する権限を持つ。また、連邦各省庁の CTO、CIO または CFO は連邦議会で OMB による評価の理由を説明しなければいかないのである。

米国では、電子政府（E-Government）法が 2002 年 12 月 17 日に成立し、2003 年 4 月 17 日から施行されている。この連邦法制定の主たる目的は、①行政管理予算局（OMB）内に連邦 CIO を設置すること、②インターネットを介した IT を利活用して政府の情報とサービスへの一般市民のアクセスを高めるための施策措置を導入することの 2 つの手法を通じて、電子政府サービスおよびプロセスのマネジメントと振興を改善することとにあった。しかし、実際には、オバマ政権が登場し、連邦政府の情報およびサービスのポータルサイトである“USA.gov”が設置されるまでは、具体的な公的ドメイン辞書の策定に向けた動きは講じられなかったといえる。

ところが、オバマ政権下で、連邦政府が積極的にクラウド・コンピューティングを導入するようになり、米国 NIST（国立標準技術研究所）がクラウドの定義を行い、クラウドの標準化に取り組み、クラウド・セキュリティのリスク分析を行なうようになって、NIST が取り組んだ連邦情報セキュリティマネジメント法（FISMA）準拠の認証（Certification）と認定（Accreditation）が極めて重要な意味を持つようになったのである。他方、クラウド・プロバイダーにとっては費用支出と作業の両面で極めて大きな負担ともなっている。

2002 年の電子政府（E-Government）法は、安全保障面と経済面の米国の利益にとって情報セキュリティの持つ重要性を認識し、電子政府法の TitleⅢとして、連邦情報セキュリティマネジメント法（FISMA-Federal Information Security Management Act）を規定。同法は、連邦政府の各機関に対して、他の政府機関、請負業者等により提供または管理されるものも含めて、連邦省庁の業務執行と資産をサポートする情報および情報システム用の情報セキュリティを確保するための省庁横断的なプログラムを開発、文書化および施行することを義務づけている。同法は、連邦省庁の IT 外部委託先にまで適用されることになったのである。

連邦情報セキュリティマネジメント法（FISMA）の制定により、情報システムのセキュリティを強化するための特定の責任が連邦各省庁、NIST（国立標準技術研究所）および行政管理局（OMB）に付与された。

FISMAによると、“情報セキュリティ”の意味は、情報セキュリティの属性である整合性（Integrity）、機密性（Confidentiality）および可用性（Availability）を確保するために、権限を付与されないアクセス、利用、開示、混乱、改ざんまたは破壊から情報と情報システムを防護することである。2004年2月に公表されたFIPS（Federal Information Processing Standards）PUB 199では、連邦政府の情報および情報システムのセキュリティを次の通り、整合性（Integrity）、機密性（Confidentiality）および可用性（Availability）の3つに分類している。

- **Integrity（整合性、完全性）**：″guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity（不当な情報の改ざんまたは破壊を防護することで、情報の否認不可性と真正性の確保を含む）
- **Confidentiality（秘密保持、機密性）**：″preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information（アクセスと情報開示に権限を付与された制限を保持することで、個人のプライバシーと知財権情報の保護を含む）″
- **Availability（可用性）**：″ensuring timely and reliable access to and use of information（情報とその利用に対するタイムリーかつ信頼性のあるアクセスを確保すること）″

“情報（Information）”については、プライバシー、医療、知財権（Proprietary）、金融、調査、セキュリティマネジメントなどの情報、請負業者の機微な情報のようなタイプ別の分類が行われ、特定法、行政命令、指令、政策または規制などで定義される。

連邦情報セキュリティマネジメント法（FISMA）では、連邦各省庁のトップは、FISMAで明記された情報セキュリティ標準、情報セキュリティの標準とガイドライン、情報セキュリティマネジメント等のコンプライアンスを遵守して、連邦政府の情報システムのセキュリティ防護に責任を持つもとのとされている。具体的には、連邦各省庁は、当該責任のある範囲の情報および情報システム（外部委託等を含む）の情報セキュリティ強化に関する年1回の自己監査実施を義務づけけられ、大統領直属の行政管理予算局（OMB）にこの監査結果を報告する必要がある。行政管理予算局（OMB）は、各省庁からの自己監査結果を分析・

評価し、連邦議会に対してサマリ報告を行なう。加えて、各省庁は、現在の IT の弱みとリスクを識別し、その問題解決を図るために、リスクベースでコスト効果の高いアプローチ手法を使い連邦政府のセキュアな情報と情報システムを確保し、将来の脆弱性と脅威に対する防護を図ることになっている。このことは、連邦政府に IT 製品およびサービスを提供するプロバイダーやベンダーにも適用される。しかも、連邦各省庁はこの責務の履行を格付けされることになり、コンプライアンスの遵守違反には厳しい罰則が課されることになった。行政管理予算局（OMB）は、詳細に規定した評価方法により、各省庁の自己監査結果を評価・点数化し、各省庁のステータスのランキング（A～F）を行なう。連邦議会は、各省庁のコンプライアンス遵守スコアカードを公表し、パフォーマンスの低い省庁の CIO に対しては、その理由を連邦議会で説明することを要請する。

連邦情報セキュリティマネジメント法（FISMA）のコンプライアンス遵守の規準となる情報システムセキュリティの標準と指針を策定したのは、米国 NIST（国立標準技術研究所）である。連邦情報セキュリティマネジメント法(FISMA)の規定（§ 11331. Responsibilities for Federal information systems standards）により、NIST の役割は、国家安全保障システム（national security systems）を除く、全省庁のオペレーションと資産の情報セキュリティを確保するための標準、ガイドライン、関連する方法と手法の責任を担うことになった。具体的には次の通りである。

- 標準（FIPS-Federal Information Processing Standards）：リスク水準の範囲に応じて適切な情報セキュリティの水準を提供する目的に基づいて連邦政府の情報と情報システムを分類するために各省庁が利用する連邦情報処理標準。
- ガイドライン（指針：Special Publication シリーズ）：各カテゴリーに含まれる情報および情報システムのタイプを推奨する指針。
- 情報および情報システムのための最低限の情報セキュリティ要件（マネジメント、オペレーションおよび技術的なセキュリティコントロール）。

しかも、FISMA コンプライアンスに準拠する NIST のセキュリティ標準とガイドラインは、“Mandatory Requirement（強制的規制）”となる。各省庁のトップの責任は、IT セキュリティのリスクを受容できる水準までコスト効果の高い削減を行なうことにあった。NIST は連邦各省庁と連携して情報および情報システムを防護し、各省庁における強固な情報セキュリティ計画の土台となる標準とガイドラインを公表することである。NIST の中でこの責務を担ったのは、情報技術研究所（Information Technology Lab）のコンピュータセキュリティ部門である。

米国 NIST（国立標準技術研究所）は、情報システムと情報サービスのセキュリティを促

進・計測して有効化するための標準、メトリクス、テストおよび有効化プログラムの開発に乗り出した。FISMA に規定された情報セキュリティ計画には、リスクの定期的な評価、リスク評価に基づく方針と手順、ネットワーク、ファシリティおよび情報システムなどの適切な情報セキュリティ確保のための事後計画、セキュリティ意識啓蒙教育、情報セキュリティ方針、手順、プラクティスおよびセキュリティコントロールなどの有効性の定期的（一年以内）な検証と評価、セキュリティインシデントの検知、報告・対応の手順策定、情報システムの継続的オペレーションを確保するための計画と手順の策定などが含まれる。

NIST（国立標準技術研究所）は、連邦情報セキュリティマネジメント法（FISMA）の規定に準拠して、連邦政府の情報セキュリティを強化する目的で、FISAM 実施プロジェクト（FISMA Implementation Project）に乗り出したのである。

FISMA 実施プロジェクトは次の 3 段階で遂行されている。

① フェーズⅠ(2003～2008年):標準とガイドラインの開発(Standards and Guidelines Development)

- ✧ 法規を効果的に施行するために必要なセキュリティの標準と指針（ガイダンス）を開発し、連邦各省庁による強固な情報セキュリティ計画の策定とリスク軽減を支援する。具体的な成果としては、FIPS(Federal Information Processing Standards) Publication 199および200、NIST Special Publication 800シリーズを作成・出版する。

- **FIPS Publication 199**, Standards for Security Categorization of Federal Information and Information Systems（連邦情報・情報システムのセキュリティ分類化の標準）；
- **FIPS Publication 200**, Minimum Security Requirements for Federal Information and Information Systems（連邦情報・情報システムの最低限のセキュリティ要求事項）；
- **NIST Special Publication 800-37、**Guide for the Security Certification and Accreditation of Federal Information Systems（連邦情報システムのセキュリティ認証および認定ガイド）。
- **NIST Special Publication 800-37 Revision 1**,（initial public DRAFT) Guide for Security Authorization of Federal Information Systems: A Security Lifecycle Approach (Completion October 2009)、（連邦情報システムのセキュリティ認定のガイド:セキュリティ・ライフサイクル・アプローチ（2009年10月完成）

- **NIST Special Publication 800-39**, (second public draft) NIST Risk Management Framework (Completion December 2009)
- **NIST Special Publication 800-53 Revision 2**, Recommended Security Controls for Federal Information Systems (Completed)
- **NIST Special Publication 800-53 Revision 3**, Recommended Security Controls for Federal Information Systems (Completed)
- **NIST Special Publication 800-53A**, Guide for Assessing the Security Controls in Federal Information Systems (Completed)
- **NIST Special Publication 800-59**, Guide for Identifying an Information System as a National Security System (Completed)
- **NIST Special Publication 800-60, Revision 1**, Guide for Mapping Types of Information and Information Systems to Security Categories (Completed)

② フェーズⅡ（2007～2010年）：セキュリティ評価機関の資格認定プログラム (Organizational Credentialing Program)

- ✧ 連邦各省庁向けにセキュリティ評価サービスを提供する公的部門および民間部門の法人組織の資格認定プログラムを開発。
- ✧ このセキュリティ評価サービスは、セキュリティコントロールの実施で使われるITの製品およびサービスの評価を含む連邦情報システムのマネジメント、業務執行および技術のセキュリティコントロールの総合評価を意味する。
- ✧ このプログラムをサポートする具体的なイニシアティブは、次の通り。

- **Training Initiative**: This initiative will include development of training courses, NIST publication Quick Start Guides (QSG's), and Frequently Asked Questions (FAQ's) to establish a common understanding of the NIST standards and guidelines supporting the NIST Risk Management Framework.
- **Product and Services Assurance Assessment Initiative**: This initiative will include defining criteria and guidelines for evaluating products and services used in the implementation of SP 800-53-based security controls.
- **Support Tools Initiative**: This initiative will include identifying or developing common protocols, programs, reference materials, checklists, and technical guides supporting implementation and assessment of SP 800-53-based security controls in information systems.
- **Harmonization Initiative**: This initiative will include identifying common relationships and the mappings of FISMA standards, guidelines and requirements with: (i) ISO 270000 series information security management

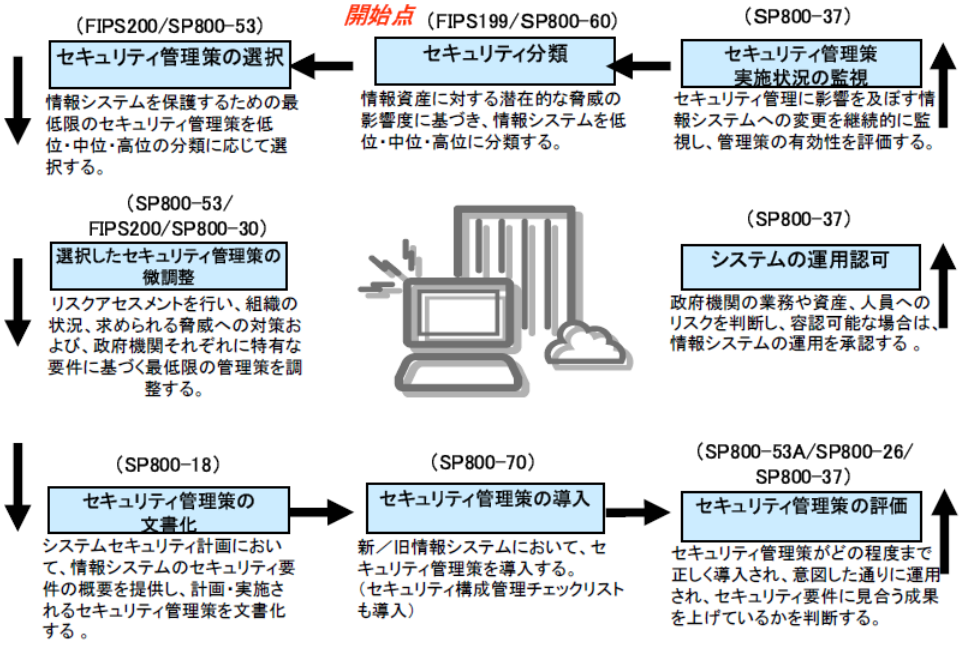
standards; and (2) ISO 9000 and 17000 series quality management, and laboratory testing and accreditation standards. This harmonization is important for minimizing duplication of effort for organizations that must demonstrate compliance to both FISMA and ISO requirements.

③ フェーズⅢ(2008～2009年):セキュリティ・ツール有効性検証プログラム(Security Tool Validation Program)

✧ FISMA実施プロジェクトのフェーズⅢは、単独の段階として削除されたが、今後はフェーズⅡに組み込まれ、既存のIT製品のテスト、評価および有効性検証プログラムを利用する。

FISMA実施プロジェクトのフェーズⅠ（標準とガイドライン）で開発されたFIPS（Federal Information Processing Standards）シリーズとSpecial Publication 800シリーズは、連邦各省庁と連邦政府にIT製品・サービスを提供するベンダーおよびプロバイダーにとって、強制的規制である。各省庁と連邦政府と契約するITベンダーは、最初にFIPS 200（最低限のセキュリティ要求事項）に準拠することが義務づけられ、次に、FIPS 199（組織や組織の資産に対する脅威の影響度を算定し、影響度により各情報システムを低・中・高に分類するための基準）に基づいて該当する連邦情報システムのセキュリティ分類を決定する必要がある。その後、2007年11月に公表された“NIST Special Publication 800-53 Revision 2”の連邦情報システムの推奨セキュリティコントロール指針に準拠して基本的なセキュリティコントロール策を適用することになる。

図 5　FISMA コンプライアンスのリスクマネジメントフレームワーク（RMF）



出所：情報処理推進機構（IPA）「NIST SP 800シリーズに見るBCPとContingency Planning」2006年2月

特に、連邦クラウドの急速な普及・拡大で再び注目されるようになったのは、連邦情報システムのセキュリティ認証・認定（Security Certification and Accreditation）のガイドラインである“NIST Special Publication 800-37”、2009年11月に発表されたばかりの連邦情報システムにリスクマネジメントフレームワークを適用する“NIST Special Publication 800-37 Revision 1（Initial public Draft）”である。換言すれば、連邦政府にIT製品とITサービス（クラウド・サービスも含む）を提供するベンダー・プロバイダーは、FISMAコンプライアンスのセキュリティ認証・認定（Security Certification and Accreditation）を取得することが強制的な義務となる。この認証と認定を取得するプロセスで必要な文書は、“C&Aパッケージ”と略称されている。

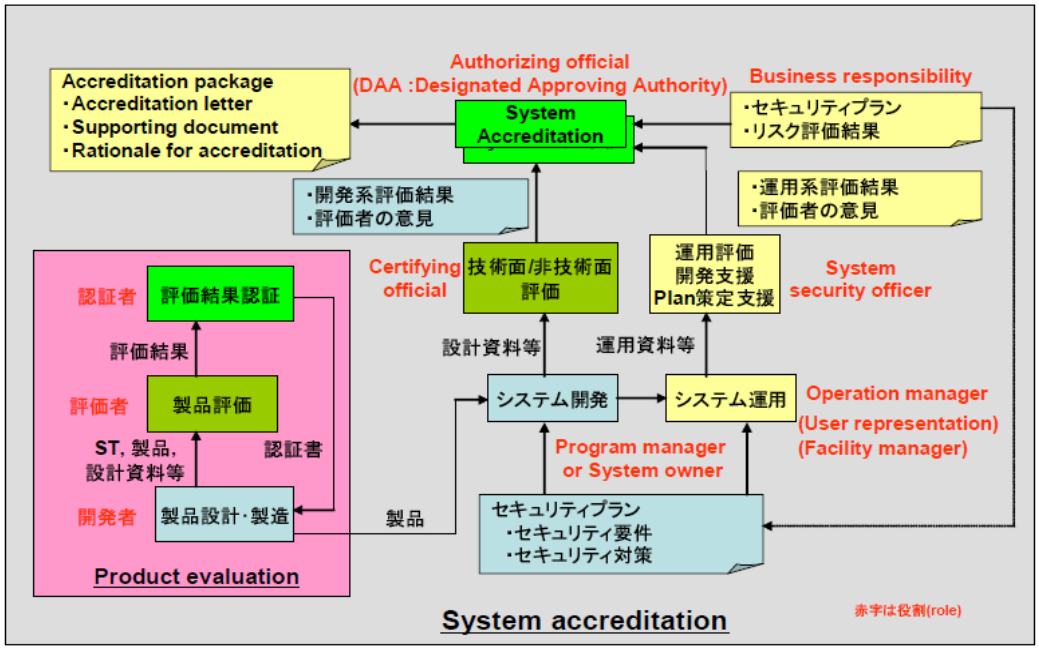
セキュリティ認定（Security Accreditation）とは、情報システムの運用権限を付与し、合意されたセキュリティコントロール策の実施に基づく省庁のオペレーション、資産または個人に伴うリスクを受容することを連邦省庁の上席幹部が公式に決定することである。セキュリティ認証（Security Certification ）とは、情報システムの詳細なセキュリティ検証プロセスのことで、この間に、セキュリティ認定（Security Accreditation）に必要な情報と関連書類（証拠）を作成する。セキュリティ認証（Security Certification ）は、セキュリティ認定を行うために、マネジメント、オペレーションおよび技術的な側面から、

情報システムにおけるセキュリティコントロール策を総合的に評価することである。

セキュリティ認証（Security Certification ）のプロセスは、次の4つの段階から成り立っている。

- Initiation Phase（初期段階）
- Security Certification Phase（セキュリティ認証段階）
- Security Accreditation Phase（セキュリティ認定段階）
- Continuous Monitoring Phase（継続的モニタリング段階）

図 6　システム評価と製品評価



例えば、Googleは2009年9月、2010年に開始予定でGoogle Appsなどの政府（連邦、州および地方）向けクラウド版（NISTの定義するコミュニティ・クラウドに類似）の開発を発表した。このために、Googleは、連邦政府の情報システムのセキュリティ要件を義務づけるFISMAコンプライアンスを遵守するために、データ保管場所を米国領土内にする規制などのNISTの定めるセキュリティ認証・認定（C&A）を2009年内に取得のための膨大な申請作業に取り掛かりっている。SearchCompliance.comの2009年12月18日の記事では、連邦調達庁であるGSA（一般サービス庁）向けに提供する“Google Apps”のシステムセキュリティ計画（1000ページを超える分量）を完成させたようである。Google Appsのセキュリティ担当取締役のEran Fegenbaumによると、インサイダーリスクを最小化するのはクラウド・プロバイダーの責任であるが、FISMAコンプライアンスを遵守するには多大な費用と労力を要すると語る。グーグルでは、役割ベースのセキュリティ、ログ・アクセス、所有者へのデー

タ侵害の通知等を社内で実践している。マイクロソフトも、GSA（一般サービス庁）に提供する“Microsoft Business Productivity Online Suite ”の運用許可を得るためにFISMAコンプライアンスのセキュリティ認定を申請し、2010年からの運用開始を目指している。

1.3.4. データ分散とデータ・プライバシー

NIST のピーター・メル（Peter Mell）とタイム・グランス（Time Grance）による 2009 年 10 月 7 日のプレゼンテーション資料によると。データに関しては、次の 2 つが重要な課題である。

① データ分散と国際プライバシー法（Data dispersal and international privacy laws）
   - EUデータ保護指令と米国商務省セーフハーバープログラム（EU Data Protection Directive and U.S. Safe Harbor program）
   - データの外国政府へのエクスポージャ（露出）とデータ召喚命令（Exposure of data to foreign government and data subpoenas）

② データ保持の諸問題（Data retention issues）

2009年10月6日に開催された“Virtualization, Cloud Computing and Green IT Summit”のパネルでは、連邦CIOカウンシルが設立したFederal Cloud Computing Advisory Council（CCAC）の会長兼エネルギー省のCIOであるPeter Tseronisは、連邦政府によるクラウド導入に際しての主な問題点は、①セキュリティ問題、②データ・プライバシー、③取得プロセス、④標準、⑤サービスレベル契約（SLA）だと発言している。CCACの主なタスクは、クラウド・コンピューティングを巡る疑問や懸念に関するフィードバックを各省庁のCIOから得ることであり、現在、この問題の解決に取り組みつつある。

2009年9月15日、連邦政府機関がクラウド・サービスを購入するためのアプリケーションの“ストアフロント（店頭）”とも呼ばれるWebサイトの“Apps.gov”を立ち上げたと発表。連邦CIOのビベック・クンドラ（Vivek Kundra）によると，Apps.govは，ビジネス・アプリケーション、プロダクティビティ・アプリケーション、クラウドITサービス、ソーシャル・メディア・アプリケーションの4つのカテゴリーに分類され、連邦政府機関の職員が生産性や共同作業の向上，効率化を図るためのクラウド・サービスのアプリケーションをオンラインで簡単に閲覧して購入するためのワンストップ調達サイトである。

この発表の数時間後、Googleは、eメール、ワードプロセッサー、コラボレーション、Webサイト構築などの商用版Google.Appsを連邦政府および公的部門のニーズに対応した形に

して2010年中に連邦政府、州政府および地方政府にクラウド・サービスを提供すると発表している。

ビベック・クンドラ（Vivek Kundra）連邦CIOは、政府クラウド・コンピューティング導入イニシアティブ前進に向けたGoogleのような産業界による積極的な参加を歓迎すると表明している。しかし、連邦政府機関向けにIT製品とサービスを提供するベンダーは、2002年のFISMA（連邦情報セキュリティマネジメント法）コンプライアンスとNIST（国立標準技術研究所）の策定したセキュリティ標準および関連するセキュリティ認証・認定（C&A）を取得しなければならない。この点については、後に掲載する【FISMAとNIST】の中で詳述する。Googleの製品マネジメント担当役員のMatthew Glotzbachは、FISMAコンプライアンスを遵守する手続きを進めるとしながらも、“連邦政府はセキュリティやデータ・プライバシーの問題に関する各省庁の要求事項を標準化する必要性がある”と付言する。“Sensitive Data（機微なデータ）”の分類に関しては、米国法務省（Department of Justice）の策定した基準を連邦政府、州政府および地方政府が準拠している。同様に、セキュリティ、データ・プライバシー等の問題も政府機関の統一的な基準策定が必要になる。

米国の専門家の多くは、PortabilityとInteroperability、ベンダーロックイン、信頼性と可用性、データ・ロケーション（保管場所）などのリスク懸念を指摘する。もう1つの重要な問題は、合衆国憲法修正第4条（Fourth Amendment）が禁じる“不合理な捜査および押収（unreasonable search and seizure)”である。この修正第4条では、身体、住居、書類および所有物に対する不合理な「捜索・押収」を受けない権利を保障していることは、警察官やその他の官憲の捜査活動によるプライバシーの侵害から、個人を保護することを意図してと解釈される。この捜査・押収は、公的機関の公務員によるものに適用されるが、私人によるもの捜査・押収の可否を論じていない。また、クラウド内に格納されるデータには、この修正第4条によるプライバシー保護は適用されない。米国の過去の判例は、私人または組織がそのデータを第3者の手に渡した場合、このデータに持つ権利を失うとしている。ここでも、技術イノベーションの進歩と法解釈の遅れのギャップ問題がみられる。

クラウド・プロバイダーとの契約の中で明記しない限り、プライベート・データを保管するクラウド・サービスを利用する連邦政府は1974年のプライバシー法に違反することになる。問題は、プライバシー法だけではなく、連邦記録管理および処分等の数多くの法規則も関連する。加えて、ビジネス情報および政府情報の秘密保持（Confidentiality）も問題もある。

ワシントンDCに本拠を構える非営利団体の公益研究センターであるEPIC（Electronic Privacy Information Center）は2009年3月17日、連邦取引委員会(FTC-Federal Trade

Commission)に対して、Googleの消費者向けクラウド・コンピューティングサービスの不公平かつ欺瞞のビジネス慣行を訴えたのである。この申し立てによると、最近のGoogle Docsのセキュリティ侵害にみられるように、Googleのユーザー情報の保管には、消費者からオンラインで収集した情報のプライバシーとセキュリティに数多くの懸念を提起している。EPICはグーグルに送付される情報の安全性とセキュリティを調査するように連邦取引委員会(FTC)に訴えている。

連邦取引委員会（FTC）は2009年12月、連邦通信委員会（FCC）に対してFCCの進める“全米ブロードバンド計画（National Broadband Plan)”へのコメントを求められ、クラウド・コンピューティングの技術とID管理をよく調査するよう要請書簡を送付した。連邦取引委員会（FTC）はEPICの訴えもあって、クラウドのプライバシーとセキュリティの調査を進めつつある。クラウド・コンピューティングはコスト節減の潜在的メリットは極めて大きいものの、クラウド内にデータをストレージ（貯蔵）することはコンシューマにとってプライバシーとセキュリティの懸念をもたらすと、FTCの消費者保護局のDavid Vladeckが語っているという。連邦通信委員会（FCC）の申し立てによると、例えば、増大しつつある消費者データを収集し、集約的に保管することは、このデータが容易に他の者と共有されることになり、消費者の当初の理解や意図とは異なる法人格によって大量のデータが利用されるリスクを生み出す。連邦取引委員会（FTC）は、市民のプライバシー保護やログイン時の認証等のID管理システムの調査にも乗り出している。

連邦取引委員会（FTC）は2010年1月28日、カリフォルニア大学バークレー校で、クラウド・コンピューティングやソーシャル・ネットワーキングが消費者のプライバシーに与える影響について公開討論会を開催する。

OECD(経済協力開発機構)の理事会は1980年9月23日、プライバシー・ガイドラインと略称される“プライバシー保護と個人データの国際流通についてのガイドライン(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” を発表し、加盟国内で適用する8つの基本原則を示した。これを踏まえて、EU（欧州連合）は、①個人データ処理と表現の自由、②第三国への個人データの移転の原則を盛り込んだ“EU個人情報保護指令（通称、EUデータ保護指令：95/46/EC)”を1995年10月に採択し、加盟国に対して3年以内に個人情報保護に関する法律の制定、または改正を求め、1998年10月25日発効した。この“第三国に対する個人データの移転（第25条)”は、「当該第三国が適切なレベルの保護を提供している場合に限られることを規定するものと」し、「第三国によって提供される保護レベルの適切性は、一連のデータの移転作業を取り巻く全ての環境に照らして査定されるものとする。特にデータの性質、提案された処理作業の目的及び期間、データの移転元の国及び最終目的国、当該第三国で効力を有する一般的な及び分野別の法律、当該第三

国で遵守されている職業上の規則、及び防衛上の措置が考慮に入れられるものとする」と規定された。加えて、欧州議会は、通称“e-プライバシー指令”と呼ばれる“プライバシー保護に関する欧州議会・理事会指令2002/58/EC”を採択した。

OCEDは2007年6月12日、“Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy（プライバシー保護法の施行における国境を越えるクロスボーダー協力に関するOECD理事会提言）を発表。「国境を越えた情報の流れの増大に伴い、組織及び個人の双方が、コストの低下、効率化及び顧客の利便性の向上といった恩恵」を得ているが、「個人情報の流通は、プライバシーに関する懸念を増大させ、また各人の個人情報を保護することに関して新たな課題を提起している。個人情報が国境を越えて移転する際には、個人情報のその不法な使用及び開示から各個人を保護するために、プライバシー権利を行使する各個人の能力という更なるリスクにさらされることがあり得る。同時に、プライバシー法の執行責任を有する当局は、国境外の組織の活動に関して、苦情処理又は調査を行うことができないことに気付くかも知れない。また、国境を越えて共同で活動するための当局の取り組みは、不十分な防止権限または救済権限、法制度の不整合及びリソースの制約といった実際的な障害によって妨げられる可能性がある」して、OECD加盟国と当該国のプライバシー保護執行機関に対して、次のクロスボーダー協力を求めている。

① プライバシー法執行のための国内の枠組みを改善すること。
② 国境を越えたプライバシー法執行協力を容易にするために有効な国際的な仕組みを開発すること。
③ プライバシー保護法の執行において、適切な保護措置に従い、通知、苦情付託、調査支援及び情報共有を通して行うことを含む相互支援を提供すること。
④ プライバシー保護法の執行協力の促進を目的とした議論及び活動に、関連する利害関係者を参加させること。

更には、EUの情報社会メディア担当のビビアン・レディング（Viviane Reding）コミッショナー（政策委員）は2009年4月、デジタル時代には欧州市民のプライバシーが優先されること（Priority）でなければならないとし、“個人の情報は事前の同意を得てはじめて利用できる”という欧州のプライバシー規則の原則を明言している。RFIDについては、“消費者に対してではなくて、消費者により利用されてはじめてその経済的な潜在性を実現できる”と語り、欧州の市民は、何に利用されるのかを正確に情報開示されないまま、RFIDチップを持ち歩くべきではないとし、いつでもチップを取り外せるようにしないといけないと警告を発している。因みに、レディング（Viviane Reding）は近いうちに、司法、基本的人権および公民権担当のコミッショナーに転任する予定である。

EUデータ保護指令（95/46/EC）の第25条に規定された商用目的でEUから米国に移転される個人データがEUの適切なプライバシー保護基準を満たしていないと米国には移転できないとする禁止措置を巡り、米国の商務省は欧州委員会と長い期間の交渉を行い、“セーフハーバー協定（Safe Harbor Agreement）”を締結した。米国側は2000年7月21日にセーフハーバー原則および関連文書を正式登録している。これは、米国商務省が作成するセーフハーバー原則を産業界が遵守していれば、EU 指令25 条違反にならないという内容の協定である。この原則の主な内容は、①通知（Notice）、②選択（Choice）、③第3者への移転（Transfers to Third Parties）、④アクセス、⑤セキュリティ、⑥データの整合性（Integrity）、⑦執行（Enforcement）である。クラウド・セキュリティの観点からみると、このEUデータ保護指令は、データの外国政府へのエクスポージャ（露出）とデータ召喚命令（Exposure of data to foreign government and data subpoenas）の問題を提起するが、未だに、この問題の解決の糸口はみえていないようである。

しかしながら、プリバシー保護に関する欧州と米国との見解の相違もあって、2005年以降、米国商務省、欧州委員会およびEUのプライバシー保護監視団体のEU Article 29 Working Party on Data Protection（第29条データ保護ワーキングパーティ）は毎年、このセーフハーバー・フレームワークの進展をレビューし、国別、地域別、世界規模別にコンプライアンス（法令遵守）、データ保護およびプライバシーの最新の展開状況についての検証を行ってきている。

2009年11月16日からワシントンDCで開催された2009年の国境を越えるデータ・フロー、データ保護およびプライバシーに関する会議は、“Across the Divide: Successfully Navigating Safe Harbor”と題され、商務省、欧州委員会およびArticle 29 Working Party on Data Protection（第29条データ保護ワーキングパーティ）による主催であった。このパネルの主要議題は、①電子的に保存される情報(ESI-Electrically Stored Information)とも呼ばれる電子フォーマットの情報を取り扱う連邦民事訴訟規則で義務づけられる電子ディスカバリ（情報開示）を意味するElectronic Discovery（eDisvovery）、プライバシー・コンプライアンス、情報セキュリティ、クロスボーダーのデータ共有、グローバル・プライバシー標準、クラウド・コンピューティングにおけるSNSプロバイダーの戦略的情報管理および行動ターゲティング広告（behavioral advertising）などであった。特に、関心が集まったのは、“Cross-Border Discovery Obligations and Data Privacy（国境を越えるディスカバリとデータ・プライバシー）”である。プライバシー問題の専門家であるインディアナ大学のFred Cateがモダレータとなり、グローバルなE-ディスカバリおよびデータ・プライバシー問題のコンサル会社であるDaley & FeyのJames Daley、Eli Lillyのチーフプライバシーオフィサーの Stan Crosley、商務省のLara Ballard、ドイツのデータ保

護庁のKirsten Blockがパネラーとして参加。James Daleyは、プライバシーおよびディスカバリの異なる見解を持つ国の文化的衝突に言及した。商務省のLara Ballardは、データ・プライバシーとクロスボーダー・ディスカバリの間の緊張における重要な根本的役割を果たす米国と欧州の法務省の考え方の違いなどを披露。Eli LillyのStan Crosleyは、この緊張がもたらす多国籍企業への影響、クロスボーダー・ディスカバリの不当な負担、費用支出およびリスクなどの実務上の障害を説明した。データ保護庁のKirsten Blockは、EU Article 29 Working Party on Data Protection（第29条データ保護ワーキングパーティ）によるクロスボーダー・ディスカバリに関するワーキング・ドキュメントについて説明した。

ワシントンDCに本拠を構える非営利公益研究消費者教育団体のWashington Privacy Forumは、クラウド・コンピューティングの主要な問題点を検討し、個人情報のプライバシーと企業情報および政府情報の秘密保持（Confidentiality）のインプリケーションについての興味深いレポートを2009年2月23日に発表している。

米国で、個人情報の収集、維持、利用および開示の公正な情報慣行の基準を定めた法律は、1974年のプライバシー法（Privacy Act）である。しかし、上記のレポートでは、特に連邦各省庁とクラウド・プロバイダーとの間で契約上の取り決めを行なっていない限り、情報をクラウド・プロバイダーと共有することになるクラウド・コンピューティングを連邦省庁が導入すれば、それは1974年のプライバシー法に違反する可能性があると主張している。また、クラウド・プロバイダーが連邦省庁に代ってこのサービスを一般公衆（Public）に提供すれば、連邦法規則で義務づけられる多種多様なセキュリティ・コンプライアンスの遵守を余儀なくされる。連邦記録マネジメントおよび処分にも関連法規が適用される可能性がある。

本レポートは、“クラウド・コンピューティングが持つ個人情報のプライバシーと企業情報および政府情報の秘密保持（Confidentiality）の重要なインプリケーション”の他にも次のようなファクト・ファイディングを示している。

- ユーザーのプライバシーと秘密保持リスクは、クラウド・プロバイダーの策定するサービス条件とプライバシー方針により大きく異なる。
- クラウド・ユーザーの幾つかの情報タイプとカテゴリーにとって、プライバシーおよび秘密保持の権利、義務およびステータスは、ユーザーがクラウド・プロバイダーに情報を開示するときに変化する可能性もある。
- 情報開示と遠隔ストレージ（Remote Storage）は、個人または企業の情報の法的資格または当該情報の保護にとってマイナスの帰結をもたらす可能性がある。

- クラウド内の情報の保管場所（Location）は、情報のプライバシー保護と秘密保持おうよび情報を処理または保存する者のプライバシー義務に重大な影響を与える可能性がある。
- クラウド内の情報は、同時に1つ以上の保管場所に保存され、異なる法的帰結をもたらす可能性がある。
- 法律は、クラウド・プロバイダーに犯罪活動と関連事項の証拠のユーザー記録の検証を義務づける可能性がある。
- 法的な不透明さのために、ユーザーのプライバシーおよび秘密保持保護に加えて、クラウド内の情報ステータスの査定も難しくなる可能性がある。
- クラウド・プロバイダーによる方針と慣行の改善を含むクラウド・コンピューティングのプライバシーおよび秘密保持のリスク対応は、法律とユーザーのより厳しい監視に応じて変化する。

以下は、Washington Privacy Forum による 2009 年 2 月のレポートに記載されたその他の特記事項である。

民間企業がクラウド・プロバイダーと情報を共有する場合、特定の記録または企業に適用される複数のプライバシー法が米国に存在する。1999年に導入された金融機関規制法の中核である“Gramm-Leach-Bliley Act（グラム・リーチ・ブライリー法)”では、金融機関が顧客の個人情報を関係のない第3者に開示することを禁じている。サービス・プロバイダーへの情報開示は一般的に制限されない。しかし、サービス・プロバイダーにより情報が開示され、権利が取得される際の契約条件は、情報開示または後続の利用の合法性にとっては差異を生み出す可能性がある。

同様の結論は、“ビデオ・プライバシー保護法（Video Privacy Protection Act)”で保護されるレンタルビデオ記録と“ケーブル通信政策法（Cable Communications Policy Act)”で保護されるケーブル TV 加入者記録に適用される。当該特別法はクラウド・プロバイダーの利用を直接的に妨害するものではない。

しかし、クラウド・プロバイダーの利用を制限する他の法律もある。1996 年にクリントン大統領の署名により成立した医療情報の電子化推進とそれに伴うセキュリティおよびプライバシーを定めた“HIPAA（健康保険ポータビリティ説明責任法)”に基づいて発布される連邦健康プライバシー規則（Federal Health Privacy Rules）に準拠する健康記録の情報開示には手続き要件が適用される。HIPAA に規定されるプライバシー規則は、付保される法人格（Covered Entity）により個人的に識別される健康情報の利用および開示を規制する総合的スキームを決めている。付保法人格が保護された健康情報をサービス・プロバイ

ダーに移転する前に、当該法人格とサービス・プロバイダーは“Business Associate Agreement（業務請負付随契約)”を締結しなければならない。ビジネス・アソシエィトがHIPAAルールを直接的に遵守していなくとも、ビジネス・アソシエィトと付保された法人格との間の契約は、基本的にはビジネス・アソシエィトに対して付保される法人格に適用されるのと同一の基準を遵守することを義務づけることになる。

HIPAAを準拠する病院は、クラウド・プロバイダーとビジネス・アソシエィト契約を締結しない限り、患者記録をクラウド・プロバイダーにより提供される保管施設に保存する決定を行うことができない可能性がある。特定のケースでは、HIPAAの要求事項はクラウド・プロバイダーのサービス条件を直接の衝突を起こす可能性もある。サービス・プロバイダーは、HIPAA基準と利益相反を起こすような形で健康記録を利用または開示することはできない。以上から、HIPAA対象の法人格は、クラウド・プロバイダーの保管施設に患者記録を保存することを容認するサービス条件でクラウド・プロバイダーに患者記録を保存すると、HIPAAに違反する可能性がある。

この他にも、Tax Preparation Law（課税準備法)、Violence Against Women Law(婦人暴力法)、Legally Privileged Information（法的特権付与情報)、Professional Service Obligations（専門的秘書義務）などでも、様々なプライバシー保護の適用がある。

【個人および企業にとっての第3者データ保存の帰結】に関しては、ユーザーがクラウド・プロバイダーに情報を開示することを阻止する法律または義務はないが、その場合でも、情報開示がなにがしかの帰結をもたらす可能性がある。クラウド・プロバイダーを含む第3者に保存される情報は、情報を策定した者の所有にある情報に比べると、プライバシー保護が少ないか、あるいは脆弱である。政府関係機関は、情報作成者から入手するよりも容易に第3者から情報を取得する可能性がある。第3者から容易に情報を取得できる政府機関の拡大能力は個人と民間企業の両方にマイナスの影響を与えることもある。

1.3.5. サービスレベル契約（SLA)

「Cloud Computing Use Case白書」のサービスレベル契約（SLA）についての定義によると、サービスレベル契約（SLA）とは、「コンシューマの要求事項とプロバイダーのコミットメント（履行約束）を規定するプロバイダー・コンシューマ間の契約」である。一般的には、サービスレベル契約（SLA）には、アップタイム（起動時間)、プライバシー、セキュリティおよびバックアップ手順などの規定が盛り込まれている。

NISTのコメントによると、サービスレベル契約(SLA)の策定では、次の点が重要になる。

- 提供するサービスレベルに関する顧客（カストマー）とサービス・プロバイダーとの間の契約。
- パフォーマンスメトリクス：アップタイム（起動時間）、スループット（単位当たりの処理量、応答時間（Response Time）等。
- 問題管理の詳細
- セキュリティ能力の文書化
- 不履行に関する罰則規定

【サービスレベル契約（SLA）】

米国のベンダーが標準化された報告プロセスをシステム化していないことが、標準的なサービスレベル契約（SLA）の策定を難しくしている。実際、連邦政府の一般調達を担う総合サービス局（GSA）は、各省庁と連携してこの課題解決に取り組みつつあるが、各省庁がそれぞれの政府機関の法律顧問によるサービスレベル契約（SLA）の検証を行なうべきだと進言しているのが現実である。

総合サービス局（GSA）のコメントによると、GSA は、各政府機関がサービス契約および実施条件に取り組む場合の支援を行なう構えはある。しかし、各省庁が製品と契約を検討する際には、総合サービス局（GSA）と各省庁の連絡担当は、情報を共有し、複数の政府機関が同一製品を使用する場合に限り、各省庁と一緒になって契約策定に取り組むとの姿勢である。

有償のアプリケーションはすべて、FAR（連邦購入取締制度）に準拠したサービスレベル契約（SLA）を策定しなければならない。インターネットを介した無償の“ソーシャル・メディア・アプリケーション”では、FAR（連邦購入取締制度）を遵守する必要はない。この状況に対応するため、総合サービス局(GSA)の市民サービス室(Office of Citizen Services)は、連邦政府の要求事項を満たすソーシャル・メディアのプロバイダーと共同でサービス条件の改正に向けた作業を行なっている。この作業が完了すると、TOS（Terms of Service）ガイドラインが“Apps.gov”から入手可能となる。

本調査プロジェクトの米国チームがカーネギーメロン大学のソフトウェアエンジニアリングインスティチュート（SEI）にインタビュー調査を実施したところ、サービスレベル契約（SLA）の仕様書に関する標準は存在しないとの回答であった。Web サービス業界で参考までに最も利用される仕様書は、“Web サービスレベル契約（WSLA)”の言語とフレームワークおよび“Web サービス契約仕様（WS-契約)”である。Web サービスレベル契約（WSLA）

は、IBMにより作成された仕様書とリファレンス・インプリメントである。

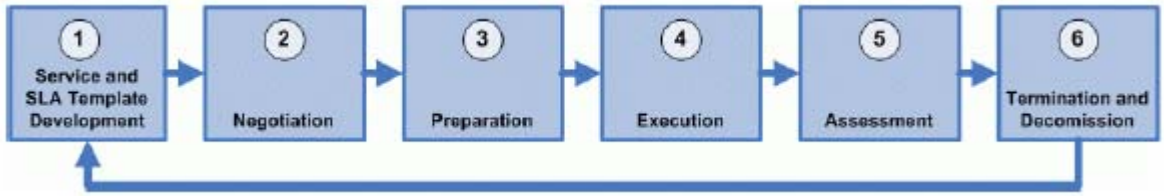
オープングリッドフォーラム（OGF:Open Grid Forum）による Web サービス契約仕様（WS-契約）とは、

- サービス・プロバイダー・消費者間またはサービス・プロバイダー・ユーザ企業間の契約を決めるWebサービス・プロトコルのことで、拡張XML言語を使い、契約の性質と契約当事者を見極めることが可能な契約テンプレートを特定するものである。このWeb サービス契約仕様（WS-契約）は、①契約を特定するスキーマ、②契約テンプレートを特定するスキーマ、③契約の作成、契約期間の終了および契約状況のモニタリングなどサービスレベル契約（SLA）のライフサイクル管理の3つで構成されている。

サービスレベル契約（SLA）の一部であるサービスの質の仕様書を作成する開発も行なわれている。この中で最も進んだものが、IBM、BEA、Microsoft、SAP、Sonic や VeriSign が開発に貢献し、Web World Wide コンソーシアム（W3C)が 2007 年 9 月に推奨した仕様書である。WS-Policy は、Web サービスで XML を使ってポリシー（セキュリティポリシー、QoS ポリシーなど）を外部に公開するための仕様であり、利用者にとってはポリシー要求条件を指定する手段を提供する仕様である。

TMフォーラムの「SAL Handbook Solution Suite V2.0」は、サービスレベル契約（SLA）ライフサイクルの事例を次のように説明している。

図 7　SLA ディプロイメントのフェーズ



① サービスと SLA テンプレートの開発（Service and SLA Template Development）：このフェーズでは、ユーザーが必要なサービス、およびサービスの実施環境に投入できる適切なサービスの特性とパラメーターを特定し、標準の SLA テンプレートを普及させる。

② 折衝（Negotiation）：。ここでは、サービス・パラメーターを定義して値を指定する折衝、サービス利用者のコスト、SLA に違反した場合のサービス・プロバイダーのコスト、およびサービス利用者への報告の定義と周期の定義が行われる。

③ 準備（Preparation）：サービス利用者がサービスを使用できる状態になる。このフェーズで、SLA パラメーターに適合するようにサービスを実施するために、リソースの再構成が必要になる場合がある。

④ 実施（Execution）：サービスはこのフェーズで実際に運用される。この中には、サービスの実施とモニター、リアルタイム・レポート、サービス品質の検証、およびリアルタイムの SLA 違反処理がある。

⑤ 評価（Assessment）：このフェーズは次の 2 つからなる。

- SLA とサービス品質（QoS）の評価は個々の利用者に提供される。各 SLA について、QoS、顧客満足度、改善の余地、要件の変更は周期的に見直される。
- サービスの全般的評価。この評価は内部のビジネス・レビューと結びつけることができる。このレビューの対象になる要素は、すべての利用者に提供される QoS、サービスの目標と運用の再編、サービス・サポート上の問題の特定、および各サービスレベルの必要性の特定である。

⑥ 契約終了（Termination）：契約の満了や違反などの理由によるサービスの終了、またサービスの打ち切りが扱われる。

【SLA パラメーターと測定基準】

SLA パラメーターは、複数の測定基準をまとめて指定される。これらの測定基準によって、SLA パラメーターを満足しているかどうか検証するために収集が必要な指標が決定される。ソフトウェア・エンジニアリング・インスティチュートの「Service Level Agreements in Service-Oriented Architecture 環境（サービス指向アーキテクチャ環境におけるサービ

スレベル契約)」ガイドブックから引用された次のガイドラインでは、SLA の管理が容易になるよう SLA パラメーターを定義することを提案している。SLA が両者で定義、折衝される場合、これらのガイドラインはプロバイダーと利用者の双方に適用される。パラメーターの要件は次のとおり。

- **適正なこと**:関係者の活動が、相互の利益になるようにモチベートする必要がある。例えば、SLA パラメーターが、該当するサービスの数によって支払い額を指定するようになっていれば、利潤の最大化を目指す場合、デザイン品質が低下することになる。
- **実現可能なこと**：両者のコントロールの及ばない事項を基準に含めてはならない。例えば、本質的に予測不可能なインターネット通信では、インターネット間で実行される分散トランザクションの総遅延時間を基準に含めることは意味がない。
- **強制力を持つこと**：この品質はサービスの利用者には特に重要である。SLA は、SLA パラメーターのモニター方法を記述し証拠を含むものとし、さらに利用者による強制力を持つ必要がある。包括的な SLA ソリューションは、サービスの利用者とサービス・プロバイダー側の両方の計測機器と計測を把握している必要がある。例えば、サービスの利用者は、SLA 違反が起きたときにサービス・プロバイダーから通知されることは見込めないからである。
- **測定可能なこと**：サービス基準は定量化されていること、また繰り返し測定できることが必要だ。測定は、その収集があまりに困難であるとか、コストがかかってはならない。例えば、測定の収集に必要なコンピュータリソースが大きすぎれば、実行する価値がなくなる可能性がある。
- **目的のあること**:何通りもの解釈が可能な SLA パラメーターは改訂する必要がある。例えば、トランザクションが遅れた場合、サービス・プロバイダーはサービスの利用者に通知するとするものの、通知の時期に関することには触れない SLA パラメーターがあるとする。このようなパラメーターは、遅延を許容できる時間について、異なる見解を招く可能性がある。

【SLA における折衝と柔軟性】

SLA ライフサイクルの第 2 段階で、折衝は SLA の大きな検討項目とされている。折衝プロセスを円滑に進めるため、次の事項が必須である。

- 利害関係者を広く巻き込み、製品のインプリメントからマーケティングおよび財務まで、すべてのビジネス属性に適切に対応するもとのとする。

- サービスの品質要求は時間の経過とともに変化するものであり、SLA を変更することは受け入れられるべきである。
- 必要なら、サービスレベルを複数設定することを許容し、同じサービスでも利用者が異なれば、異なる保証品質で提供できるようにする。
- SLA のフォーマットは分解できるようにし、サービスの利用品質への関連度に応じて、複数の SLA をまとめて作成できるようにする。例えば、個人を特定できる情報の非開示に関心があり、プライバシーが維持されれば大きなスループットには関心がない、というサービスの利用者もある。分割できることの利点には、SLA のモニターを担当するサードパーティに、SLA 全体を開示する必要なく、構成パラメーターなどを含む SLA の一部を渡すことができることもある。

1.3.6. CSA 等によるクラウド・セキュリティの分析と提言

Cloud Security Alliance (CSA) は、クラウド・コンピューティング内のセキュリティアシュアランスを提供するためのベストプラクティスの利用を促進し、クラウド・コンピューティングの利用に関する教育研修を行なう目的で 2009 年 3 月 31 日に設置された非営利団体(NPO)である。2009 年 4 月 20～24 日にサンフランシスコで開催された“RSA Conference 2009”で公式のデビューを飾っている。

2008 年に米国の情報セキュリティ業界で、クラウド・コンピューティングの問題点と収益機会に注目が集まり、同年 11 月 20 日にラスベガスで開催されたセキュリティ専門家の会議である“ISSA CISCO フォーラム”の席上で、CSA 設立構想が誕生した。設立発起人の Nils Puhlmann および Jim Reavis をはじめとする情報セキュリティの専門家、eBay の副社長兼チーフ Information Security Officer の Dave Cullinane、ING の IT 戦略・アーキテクチュア担当副社長の Alan Boehme、Good Harbor Consulting のパートナーである Paul Kurtz などの IT 業界の首脳達が中心となって CSA を 2009 年 3 月 31 日に創設した。

役員会
• Dave Cullinane, Vice President and Chief Information Security Officer, eBay • Alan Boehme, Senior Vice President of IT Strategy and Architecture, ING • Paul Kurtz, Partner, Good Harbor Consulting • Jerry Archer, EVP and Chief Security Officer, Sallie Mae • Nils Puhlmann, co-founder • Jim Reavis, co-founder
執行部

- Jim Reavis, Executive Director
- Nils Puhlmann, Chief Information Security Officer
- Christofer Hoff, Technical Director
- Zenobia Godschalk, Public Relations Director
- Ben Field, Webmaster

創業メンバー

- Phil Agcaoili, Dell
- Jerry Archer, Intuit
- Todd Barbee, New Dominion Bank
- Jeff Bardin, Treadstone 71
- Girish Bhat, SAVVIS
- Alan Boehme, ING
- Larry Brock, DuPont
- Glenn Brunette, Sun
- Jake Brunetto, Intuit
- Jon Callas, PGP
- Sean Catlett, Barclays
- Shawn Chaput, Privity
- Jay Chaudhry, Zscaler
- Anton Chuvakin, Qualys
- Philippe Courtot, Qualys
- Dave Cullinane, eBay
- Joshua Davis, Qualcomm
- Dr Ken Fauth
- Robert Fly, Salesforce.com
- Jeff Forristal, Zscaler
- Pam Fusco, UAT
- Francoise Gilbert, IT Law Group
- Edward Haletky, AstroArch
- Consulting
- Jim Hietala, The Open Group
- Christofer Hoff, Rational
- Survivability
- Dennis Hurst, HP
- Michael Johnson, Security GRC2
- Shail Khiyara, Cloud Consulting
- Subra Kumaraswamy, Sun
- Paul Kurtz, Good Harbor Consulting
- Mark Leary, Northrop Grumman
- Liam Lynch, eBay
- Tim Mather, RSA Security
- Scott Matsumoto, Cigital
- Dave Morrow, Secure Business Operations
- Izak Mutlu, Salesforce.com
- Brian O'Higgins, Third Brigade
- Jean Pawluk, Visa
- Josh Pennell, IOActive
- Nils Puhlmann, Qualys
- Jim Reavis, Cloud Security Alliance
- George Reese, enStratus
- Jeff Reich, FUDless
- Jeffrey Ritter, Waters Edge Consulting
- Ben Rothke, BT
- Stephen Sengam, Fox/Newscorp
- Ward Spangenberg, IOActive
- Jeff Spivey, RiskIQ
- Michael Sutton, Zscaler
- Lynne Terwoerds, Barclays
- Dave Tyson, eBay
- John Viega, McAfee
- Dov Yoran, MetroSITE Group
- Josh Zachry, Rackspace

Cloud Security Alliance（CSA）の主な目的は次の通りである。

- クラウド・コンピューティングのユーザーとプロバイダー間で、セキュリティ要求事項とアシュアランス証明書（attestation of assurance）に関する共通水準の理解を促進すること。
- クラウド・コンピューティング・セキュリティのベストプラクティスに関する独立系の調査研究を推進すること。
- クラウド・コンピューティングとクラウド・セキュリティソリューションの適切な利用に関する啓蒙キャンペーンと教育プログラムを推進すること。
- クラウド・セキュリティアシュアランスの問題点と手引きのコンセンサスリストを策定すること。

CSA は 2009 年 4 月 22 日、“Security Guidance for Critical Areas of Focus in Cloud Computing（クラウド・コンピューティングの重点分野に関するセキュリティ・ガイダンス）”を、2009 年 4 月 21 日からサンフランシスコで開催された“RSA Conference 2009”で発表している。この白書は、クラウド・コンピューティングのユーザー企業とサービス・プロバイダーに対して 15 の戦略分野（ドメイン）の主要な問題点と助言をまとめたものである。

本白書は、第 1 章のクラウド・アーキテクチュア（Cloud Architecture）、第 2 章のクラウド内のガバナンス（Governing in the Cloud）、第 3 章のクラウド内のオペレーション（Operating in the Cloud）の 3 つの章から構成され、15 のドメイン別にクラウド・セキュリティの問題提起と指針（Guidance）が示されている。

CSA（クラウドセキュリティアライアンス）は 2009 年 12 月 17 日、“Security Guidance for Critical Areas of Focus in Cloud Computing V2.1”を発表し、上記の白書を改定している。バージョン 1.0 がクラウド・セキュリティの問題提起に重点が置かれているのに対して、バージョン 2.0 は、セキュリティ問題解決のための提言（Recommendation）を中心とする内容となっている。

既述した通り、Cloud Security Alliance（CSA）は、NIST によるクラウド・コンピューティングの定義と共通の概念を使用し、共通の言葉による議論を進めている。加えて、Open Cloud Computing Interface Working Group、Amazon EC2 API, Sun の Open Cloud API、Storage Network Industry Association（SNIA)などの団体との協調関係を強めているのが特徴的である。

CSA は 2009 年 5 月 27 日、IBM、 HP、Symantec、ボーイング、 BP、モトローラ、Eli Lilly、KLM などが加盟する国際的な IT セキュリティ団体で、クラウドの導入に伴うリスクとチャンスを評価するための基本的なツールである“Cloud Cube Model”を発表した Jericho Forum と提携。両団体は、クラウド・セキュリティのベスト・プラクティス確立に向けた協働作業を行い、クラウド・コンピューティングの収益機会とセキュアなクラウドのオペレーションに関する啓蒙を図る。また、CSA は 2009 年 12 月 1 日、43 カ国 160 社のメンバー企業が加盟するシステム管理標準団体の Distributed Management Task Force (DMTF)と提携し、クラウド内のセキュリティマネジメントの協働作業を行うと発表している。

以下は、CSA により 2009 年 12 月 17 日に発表された“Security Guidance for Critical Areas of Focus in Cloud Computing V2.1”の 13 のクラウド戦略分野（ドメイン）である。

第1章	クラウド・アーキテクチュア(Cloud Architecture)
	Domain 1: Cloud Computing Architectural Framework
第2章	クラウド内のガバナンス (Governing in the Cloud)
	Domain 2: Governance and Enterprise Risk Management
	Domain 3: Legal and Electronic Discovery
	Domain 4: Compliance and Audit
	Domain 5: Information Lifecycle Management
	Domain 6: Portability and Interoperability
第3章	クラウド内のオペレーション
	Domain 7: Traditional Security, Business Continuity and Disaster Recovery
	Domain 8: Data Center Operations
	Domain 9: Incident Response, Notification and Remediation
	Domain 10: Application Security
	Domain 11: Encryption and Key Management
	Domain 12: Identity and Access Management
	Domain 13: Virtualization

2009 年 4 月のバージョン 1.0 では、クラウド・コンピューティングを導入する組織向けにクラウド・セキュリティのリスク要因分析とリスク縮小に向けた今後の指針を示す目的で、特に、セキュリティの実務担当 (Security Practitioner) 向けにクラウド・プロバイダーとの積極的かつセキュアな関係を構築する際の先行対応 (Proactive) のためのロードマップを示すことを意図している。しかし、多くの指針は、クラウド・プロバイダーにとっても、クラウド・サービス提供のためのサービスの質とセキュリティを改善するための指針にもなる。

ドメイン１の“クラウド･コンピューティングのアーキテクチュア･フレームワーク(Cloud Computing Architectural Framework)”において、CSAは、バージョン１の中で、クラウド・コンピューティングの定義を試み、5つの根本的な特性、3つのクラウド・サービス提供モデル、4つのクラウド・サービスの利活用と消費形態を分類したが、バージョン2.0では、NISTの最新バージョン15の定義に同調する決定を行っている。理由は、NISTの定義が広く認知されるようになったことにある。CSAはバージョン１の中で、SaaS、IaaS、PaaSの3つのサービス提供モデルにおける拡張性（オープン性）とセキュリティ責任の二律背反（トレードオフ）に留意することが大切だと指摘する。

バージョン2.0のリスクに関する編集注記では、クラウドへの移行に伴うリスク認識に関して、クラウドを利活用する際の資産の識別と評価から始めるべきだと提言する。クラウドの利活用の対象となる資産は、①データ、②アプリケーション/機能/プロセスの２つに分類される。

クラウド導入企業にとって最初のリスク対策は、どの資産（データおよび/またはアプリケーション/機能/プロセス）を、いつ、どのようにしてクラウド内で活用するかを決定すること（Deciding What, When, and How to move to the Cloud）だと指摘する。

次に大切なことは、この資産（データまたは機能）が組織にとってどれくらい重要なものかを決めることである。資産の重要性を決定すれば、次は、どのクラウド利活用モデル（パブリック、プライベート、コミュニティおよびハイブリッドの４つ）を活用するかを決めることである。以上のステップを踏むことで、ユーザー企業は、機微な情報やオペレーション機能に伴う潜在的なリスク・エクスポージャの大枠の概念を把握することができ、本白書の提言に従って、クラウド・コンピューティングにおけるセキュリティ管理を評価することが可能になると指摘している。

バージョン2.0におけるDomain １の“Cloud Computing Architectural Framework（クラウド･コンピューティングのアーキテクチュア･フレームワーク）の中では、CSAは再び、“クラウド・コンピューティング（クラウド）とは何か”を問いかけている。「クラウド・コンピューティングとは、コンピューティングを何か異なるものにする数多くの既存の技術とアプローチの開発を記述する進化しつつある専門用語である」と説明。本白書の執筆人によると、クラウドは、「土台となるインフラストラクチュアとクラウド供給メカニズムからアプリケーションおよび情報の資源を切り離す」ものである。クラウドは、「最適かつ効率的なコンピューティングを通じてコラボレーション、アジリティ（敏捷性）、拡張性および可用性を高め、潜在的なコスト削減をもたらす」。しかし、アーキテクチュア

の観点からみると、既存の IT モデルとクラウドの類似性と相違性に関する混乱は多大であり、また、学者、アーキテクト、エンジニア、開発者、経営幹部およびコンシューマの間で出される数々のクラウド定義も混乱を助長させている。

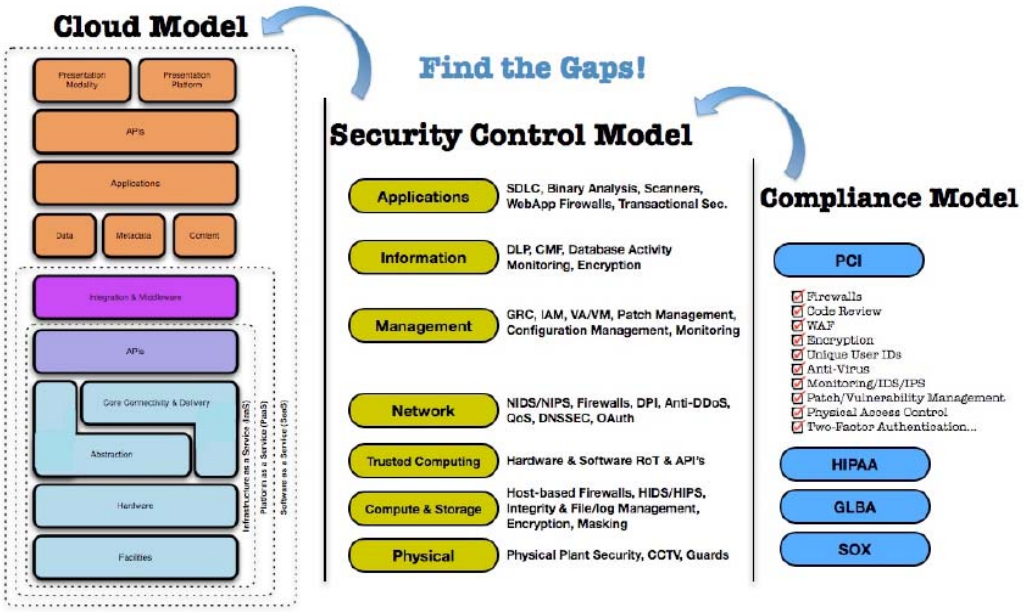
バージョン 1.0 とは異なり、バージョン 2.1 では、一般的な認知度が高まってきたことを理由に、CSA も基本的に NIST（米国国立標準技術研究所）によるクラウド・コンピューティングの定義（5 つの**基本特性**、3 つの**サービス・モデル**と 4 つの**利活用モデル**）に同調している。

しかし特に、CSA は、NIST によるクラウドの基本特性には盛り込まれていないマルチテナント（Multi-tenancy）をクラウドの重要な要素であると指摘し、この懸念を常に視野に置くことが大切だと提言する。クラウド・サービスのモデルにおけるマルチテナントの特性は、施策主導型の実施、セグメンテーション、隔離（Isolation）、ガバナンス、サービスレベルおよび異なるユーザー顧客向けのチャージバック/請求モデルの必要性を示唆している。

CSA（クラウド・セキュリティ・アライアンス）によると、クラウド・コンピューティングは、規模の経済性と標準化のメリットをもたらすものの、セキュリティ面で課題があると指摘する。

クラウド・アーキテクチュアがどのような方法でセキュリティ・アーキテクチュアにインパクトを与えるかを理解するための重要なカギは、共通の正確な語彙であり、クラウドのサービスとアーキテクチュアを分析する際の体系構築を抱き合わせ、セキュリティとオペレーション管理を補うモデル、リスク査定フレームワークおよびマネジメントフレームワーク、コンプライアンス（法令遵守）標準にマッピングすることである。クラウドの利活用に際しては、アーキテクチュア、技術、プロセスおよび所要人的資本がどう変化するのか、あるいは元のままであるのかを理解することが重要である。

図 8　クラウド・モデルのセキュリティ管理モデルおよび
コンプライアンスモデルへのマッピング



出所：Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, CSA, December 2009

特に、IaaS、PaaS および SaaS の 3 つのサービス・モデル間の関係と相互依存性を理解することがクラウドのセキュリティ・リスクを把握する上で極めて重要である。

クラウド・コンピューティングのセキュリティとは何か？クラウド・コンピューティングにおけるセキュリティ管理は、他の IT 環境におけるセキュリティ管理と大きく異なるものはないと、本白書は指摘する。しかし、クラウド・サービスの活用モデル、オペレーション・モデル、利用する技術等の性格からみると、クラウド・コンピューティングは従来型の IT ソリューションとは異なるセキュリティ・リスクを示現する可能性がある。オペレーション上の責任が 2 社以上のサードパーティの双肩にかかるとなると、クラウドは説明責任を維持できたとしてもセキュリティ管理を失ってしまう。アマゾンの AWS EC2 インフラでは、セキュリティに対するベンダーの責任は、ハイパーバイザーに限定され、物理的セキュリティ、環境セキュリティおよび仮想化セキュリティなどのセキュリティ管理の問題解決に取り組むだけである。ユーザーは、OS、アプリケーションおよびデータなどの IT システムに関連するセキュリティ管理に対する責任を負うことになる。反対に、Salesforce.com は、すべてのスタックを提供するために、プロバイダーは物理的および環

境面のセキュリティ管理の責任を担うだけなく、インフラ、アプリケーションおよびデータのセキュリティ管理の問題解決も図るのである。

“Security Guidance for Critical Areas of Focus in Cloud Computing V2.1”の第2章の“クラウド内のガバナンス（Governing in the Cloud）”と第3章の“クラウド内のオペレーション”のドメインとCSAの主な指針は次の通りである。日本語の注記は、バージョン1.0の主要な指針の概要である。右側の英文の日本語注記は、バージョン2.0の提言の概要である。

Governance Domain（ガバナンス・ドメイン）

Domain　主な指針	Guidance dealing with ...
Governance and Enterprise Risk Management ・クラウドにより節減されたコストはセキュリティ強化に充当。 ・プロバイダーは第3者機関のリスク評価を実施し、その内容をユーザーにも開示。 ・プロバイダーの財務力を把握。 ・ミッションクリティカルな業務機能の利用ではクラウド・プロバイダーに対する広範なデュー・デリジェンスを実施。	The ability of an organization to govern and measure enterprise risk introduced by Cloud Computing. Items such as legal precedence for agreement breaches, ability of user organizations to adequately assess risk of a cloud provider, responsibility to protect sensitive data when both user and provider may be at fault, and how international boundaries may affect these issues, are some of the items discussed. （提言） ・ユーザーとプロバイダーの両方が強固な情報セキュリティガバナンスを開発すること。 ・デュー・デリジェンスの一環として、ユーザー側の組織で、特定のセキュリティ管理と情報セキュリティガバナンスを検証すること。 ※エンタープライズリスクマネジメント、情報リスクマネジメントおよびサーボパーティマネジメントに関する提言も示す。
Legal and Electronic Discovery ・プロバイダーが遵守する法律とユーザーを統制する法律との間に利益相反があることに留意。 ・法的な情報規制に対するプロバイダーの対応を把握し置くこと。 ・プロバイダーによるデータの副次的利用を認識し、必要に応じてはこれを	Potential legal issues when using Cloud Computing. Issues touched on in this section include protection requirements for information and computer systems, security breach disclosure laws, regulatory requirements, privacy requirements, international laws, etc. （提言） ・ユーザーとプロバイダーの両方がrediscoveryに関連

禁じる契約書類を整備。 ・国境を越えたデータ移転の可能性を見極め、必要に応じてはこれを禁じる契約書類を整備。 ・プロバイダーとユーザーとの契約書面に、セキュリティ問題の解決を図るサービスレベル契約（SLA）条項を盛り込むこと。	する相互の役割と責任を認識すること。 ・プロバイダーは、データを真正かつ信頼性のある形で保存することを求める顧客要請に確実に情報セキュリティシステムを対応させる。 ・プロバイダーがデータのクロスボーダー移転を制限する現地の法律を遵守することを確認すること。
Compliance and Audit ・コンプライアンス要件を認識するためにデータとシステムを分類。 ・データの保管場所を認識しておくこと。特に、データのコピーが行われるのか。データ管理方法等。 ・プライバシーインパクト評価などの外部リスク評価を履行。 ・SAS 70のType Ⅱ（独立監査人の内部統制評価）やISO 27001認証等。	Maintaining and proving compliance when using Cloud Computing. Issues dealing with evaluating how Cloud Computing affects compliance with internal security policies, as well as various compliance requirements (regulatory, legislative, and otherwise) are discussed here. This domain includes some direction on proving compliance during an audit. （提言） ・法律担当と契約担当のチームを関与させること。 ・ユーザーはプロバイダーを監査する権利を持つこと。 ・コンプライアンス規制の範囲を分析すること。 ・データ・セキュリティに対する規制面のインパクトを分析すること。 ・契約上のデータ保護責任と関連契約を理解すること。 ・プロバイダーのインフラ関連規制へのインパクトを分析すること。
Information Lifecycle Management ・自社データのプライバシー規制等を認識。 ・データ保全とデータ破壊に対するプロバイダーの方針とプロセスを認識。 ・定期的なバックアップと修復テストの実施。	Managing data that is placed in the cloud. Items surrounding the identification and control of data in the cloud, as well as compensating controls which can be used to deal with the loss of physical control when moving data to the cloud, are discussed here. Other items, such as who is responsible for data confidentiality, integrity, and availability are mentioned.
Portability and Interoperability ・ドメイン１の十分な理解。 ・SaaS では、定期的なデータ抽出とバックアップを実施。	The ability to move data/services from one provider to another, or bring it entirely back in-house. Issues surrounding interoperability between providers are also discussed.

・IaaS では、VM イメージから抽出してランタイム環境でアプリケーションを利用。 ・PaaS では、注意を要するアプリケーション開発技術が必要。PaaS プロバイダー市場が急速に発展しつつあり、開発環境も多様。ポータビリティと相互接続性に留意。	（提言） ・すべてのクラウド・ソリューション、IaaS、PaaS、SaaS の各クラウド・ソリューション別に提言を示す。

Operational Domains（オペレーション・ドメイン）

Traditional Security, Business Continuity and Disaster Recovery ・クラウド上にデータが集中するため、プロバイダーのインサイダー脅威が問題となる。 ・プロバイダーは想定される最も厳しい顧客要件をセキュリティのベースラインとして適用すべき。 ・プロバイダーは、業務の分離を徹底し、業務履行に必要な最低限の顧客情報の認識に制限。 ・顧客は、地震やハリケーンなどの災害や停電等の問題対応につき、プロバイダーの復旧計画や事業継続計画を検証。	How Cloud Computing affects the operational processes and procedures currently use to implement security, business continuity, and disaster recovery. The focus is to discuss and examine possible risks of Cloud Computing, in hopes of increasing dialogue and debate on the overwhelming demand for better enterprise risk management models. Further, the section touches on helping people to identify where Cloud Computing may assist in diminishing certain security risks, or entails increases in other areas. ・顧客の RTO（復旧時間目標）を十分に理解し、契約書面に明記すること。 ・ユーザーは、プロバイダイーの役員会で承認した BCP 方針を承認すること。
Data Center Operations ・プロバイダーがクラウド・コンピューティングの 5 つの基本特性を実施しているかどうかを見極め、技術アーキテクチュアとインフラがどう SLA を満たす能力にインパクトを与えるかを認識。 ・プロバイダーは、システム、ネットワーク、管理、サービス準備などの隔離作業を行っていることを実証する必要がある。	How to evaluate a provider’s data center architecture and operations. This is primarily focused on helping users identify common data center characteristics that could be detrimental to on-going services, as well as characteristics that are fundamental to long-term stability. （提言） ・プロバイダーが認証取得を維持しているかどうかにかかわらず、顧客または第3者の監査を行うとのコミットメントまたは許可を取得すること。 ・ユーザーは、プロバイダーのパッチ管理に関する方針

・IaaS と PaaS では、プロバイダーのパッチ管理方針と手順を認識し、ユーザーの開発するアプリケーションにどのようなインパクトを与えるかを理解。 ・ドメイン 8 のように、プロバイダーの復旧計画や事業継続計画を検証。	と手順を理解し、その環境への影響度合いをチェックすること。 ・クラウド環境では、サービスの改善に結びつく方針、手順、プロセスまたはツールの継続的改善が極めて重要である。
Incident Response, Notification and Remediation ・データ漏洩規制でプライベートとして分類されるデータは常に暗号化を行い、インシデント発生のリスク軽減を図る。 ・SOC (Security Operation Center) は、マルチテナントを対象とするクラウド・プロバイダーにとっては不適切なインシデント対応関連の単一のガバナンスを想定していることが多。マルチテナント環境におけるインシデント分析に対応可能であること。 ・プロバイダーは、アプリケーション・レベルのロギングを行い、アプリケーション毎に所有者情報を取得。	Proper and adequate incident detection, response, notification, and remediation. This attempts to address items that should be in place at both provider and user levels to enable proper incident handling and forensics. This domain will help you understand the complexities the cloud brings to your current incident handling program.
Application Security ・IaaS、PaaS、SaaS では、ソフトウェア開発ライフサイクルの信頼境界が多種多様であるため、アプリケーションの開発、テストおよび利用では、信頼境界の説明責任を求めること。 ・IaaS では、高信頼性の VM イメージが成功要因である。 ・DMZ 内のホストと同等のセキュリティ強化を VM マシーンに適用すること。 ・共通のデータセンター内または同じハードウェア・プラットフォーム上で	Securing application software that is running on or being developed in the cloud. This includes items such as whether it's appropriate to migrate or design an application to run in the cloud, and if so, what type of cloud platform is most appropriate (SaaS, PaaS, or IaaS). Some specific security issues related to the cloud are also discussed. （提言） ・ソフトウェア開発ライフサイクル (SDLC) セキュリティが重要。①脅威・信頼モデルのアップデート、②クラウド環境におけるアプリケーション評価ツールのアップデート、③アプリケーション・セキュリティのアーキテクチュア変更のためのSDLCのプロセスと質のチェ九

あっても、ホスト間通信をセキュアにすること。 ・アプリケーションの秘密カギ管理・防護を徹底すること。	ポイントなどのクラウド基盤開発の3つの差別化分野を高次元で解決する。
Encryption and Key Management ・クラウド内に暗号化しないデータを保管することは、データの“流出”とみなされる。 ・バックエンドを管理しないアプリケーション・プロバイダーは、バックエンドでデータ保管を行う際に、確実にデータの暗号化を行うこと。 ・暗号化により、データ保管とデータ利用を分離すること。 ・暗号化規定を契約書に盛り込む際には、使用する暗号が業界標準や政府標準に適合していることを確認。	Identifying proper encryption usage and scalable key management. This section is not prescriptive, but is more informational is discussing *why* they are needed and identifying issues that arise in use, both for protecting access to resources as well as for protecting data.
Identity and Access Management ・クラウドでID管理を行う重要な成功要因は、強固な連携IDアーキテクチャを整備すること。 ・SAML、WS-Federation、Liberty ID-FF等のフェデレーション標準の利用を主張すること。 ・プロバイダーが、ユーザーの社内方針よりも強度なユーザー認証やパスワードポリシーを支持していることを確認。	Managing identities and leveraging directory services to provide access control. The focus is on issues encountered when extending an organization’s identity into the cloud. This section provides insight into assessing an organization’s readiness to conduct cloud-based Identity and Access Management (IAM).
Virtualization ・仮想化OSは、第3者のセキュリティ技術で強化し、階層化されたセキュリティ管理を行い、プラットフォーム依存度を少なくすること。 ・VMプラットフォームから新マシーン・インスタンスを求めることは、セ	The use of virtualization technology in Cloud Computing. The domain addresses items such as risks associated with multi-tenancy, VM isolation, VM co-residence, hypervisor vulnerabilities, etc. This domain focuses on the security issues surrounding system/hardware virtualization, rather than a more general survey of all forms of virtualization.

キュアではない仮想イメージを創出するリスクを招くので、デフォルト・コンフィギュレーションによるセキュリティ強化が必要。 ・仮想化は、隔離環境、アプリケーションの不安定性を最小限化して修復を簡素化するメモリ領域の改善等のセキュリティ面の利点がある。 ・ハイパーバイザーAPI に組み込まれた VM 特有のセキュリティを活用する。 ・管理実務担当の仮想化 OS のアクセスと管理が極めて重要。	提言 ・クラウド・プロバイダーがどのタイプの仮想化を利用しているかを見極めること。 ・侵入検知、アンチウィルス、脆弱性スキャン等、ビルトイン型ハイパーバイザー隔離以外の VM 内にどのようなセキュリティ管理が整備されているのかを理解する。 ・プロバイダーの提供する WM イメージまたはテンプレートの経歴および完全性の有効性を確認すること。 ・VM のマルチテナント状況に留意すること。

1.4. オバマ政権におけるクラウド・コンピューティングへの対応

1.4.1. 2010 年度予算案では、連邦クラウドを重視

オバマ大統領は大統領選挙キャンペーンで、温暖化対策と化石燃料依存の縮小を狙う“米国のための新エネルギー（New Energy for America)”と呼ばれる長期計画を示し、クリーンエネルギーの開発に 1,500 億ドルを投資し、500 万人の雇用を創出することを公約した。この新エネルギー計画を実現する第一歩となったのが 2009 年 2 月 17 日に成立した「2009 年米国再生・再投資法（American Recovery and Reinvestment Act of 2009)」である。オバマ新政権は、2008 年 9 月のリーマンショックに端を発する経済危機を克服するめの緊急避難的な景気刺激策として総額 7,872 億ドル（対 GDP 比 5.7%）の財政出動を決めたのである。

廃棄物による環境汚染がなく CO2 排出量削減につながるクリーンエネルギーの利用促進と再生可能エネルギーの事業化などに巨額の投資を充当していることから、2009 年米国再生・再投資法（ARRA）は“グリーン・ニューディール”とも呼ばれている。

2009 年米国再生・再投資法に基づく 7,872 億ドルの内訳は、①2,880 億ドル（38%）の減税措置（個人の税額控除総額は 2,370 億ドルで、法人税減税額は 510 億ドル等)、②3,552 億ドル（45%）の経済対策、③1,440 億ドルの州・地方への支援金である。総額の約 45%に相当する 3,552 億ドルの経済対策支出の内訳は、エネルギー費が 430 億ドル、インフラ整備・科学技術費が 1,110 億ドル、弱者保護費が 810 億ドル、医療費が 590 億ドル等となっている。

減税装置を含むと 613 億ドルにのぼるエネルギー投資では、①スマートグリッドへの 110 億ドルの資金供与、②再生可能エネルギーおよび送電技術の融資保証に 60 億ドル、③電力グリッドおよびスマートグリッドの近代化を実施する電気エネルギー信頼性オフィスに 45 億ドル、④電気自動車（EV）技術に 4 億ドルなどの内容となっている。IT 投資に関するカテゴリー分類はされていないが、スマートグリッド、ヘルス IT（約 190 億ドル）、ブロードバンド・無線インターネット（72 億ドル）の 3 つが柱となっている。

2009 年 2 月 26 日、オバマ政権になって初めての 2010 年度予算案（概要）は予算編成権のある連邦議会に提案された。「新しい責任の時代：アメリカの約束を刷新（A New Era of Responsibility: Renewing America's Promise）」と題されたこの予算案（Blue Print）では、歳出規模は前年比 9.8%減の約 3 兆 5,520 億ドルとなった。景気刺激策、金融機関へ

の支援策、イラク・アフガニスタンでの戦費拡大などを背景に、2009 年度の財政赤字は 1 兆 7,520 億ドルと、前年度（4,590 億ドル）の 3.8 倍に拡大し、対 GDP 比では 12.3%まで上昇する。2010 年度の財政赤字は 1 兆 1,710 億ドルに減少する見通しである。

環境エネルギー政策では、①クリーンエネルギーへの投資促進、②石油依存の終結、③気候変動問題への取り組み強化、④新規雇用の創出（アウトソーシングできないもの）の 4 つが重点施策となった。オバマ政権は、温室効果ガスを 2020 年までに対 2005 年比で 14%削減、2050 年までに対 2005 年比で約 83%削減すると宣言し、同目標達成へ向けて「排出量取引制度（Cap-and-trade system）」を導入することを決めた。

オバマ政権の 2010 年度予算案（最終の詳細）は 2009 年 5 月 7 日に公表された。2010 年度（2009 年 10 月～2010 年 9 月）予算では、大統領府行政管理予算局（OMB-Office of Management and Budget）は、前年度に比べて大幅な歳出増を計画し、将来的には極めて大きなコスト節減を図ることになる。2010 年度の連邦 IT 支出総額は前年度の 707 億ドルから 7%増の 758 億ドルとなる。主たる IT 予算は、国土安全保障省（Homeland Security）のサイバー・セキュリティ、保健福祉省（HHS）の医療 IT、連邦クラウドおよびグリーンテクノロジーである。オバマ政権は 2010 年度予算案における IT 投資では、特にクラウド・コンピューティングを重視し、連邦 IT におけるイノベーション、効率性および実効性を高める重要なカギとなるツールだと位置づけている。

Input や Market Research Media などのマーケティングリサーチ会社では、連邦政府 IT 支出（2014 年までの 5 年間）は、①クラウド・コンピューティング、②グリーンテクノロジー、③SOA（サービス指向アーキテクチュア）、④医療 IT、⑤サイバー・セキュリティなどの分野で拡大するとの見解を示している。この予測の根拠は、行政管理予算局（OMB）が公表した 2010 年度予算案である。連邦政府による IT 投資は、今後 5 年間に年平均 3.5%の伸び率となり、2014 年には約 900 億ドルに達すると見込まれている。

Input 社のレポートの要約では、主要な IT 投資の今後の動向は次のように記述されている。

① クラウド・コンピューティング：向こう 5 年間で約 30%の成長（市場規模は約 10 億ドル）が期待できるクラウド・コンピューティングを利活用して連邦 IT 基盤の改造に取り組む。連邦政府の効率性と実効性を高める重要なツールとして連邦クラウドを省庁間の最重点課題として取り上げている。NIST（米国国立標準技術研究所）はクラウド・コンピューティングを定義し、連邦クラウドのセキュリティ標準を策定して、連邦レベルでのクラウド構想の実現に拍車をかける。空軍、陸海軍でも SOA（サービ

ス指向アーキテクチュア）を実装し、連邦政府のクラウド・コンピューティング導入を支える。

② サイバー・セキュリティ：連邦政府は情報システムのセキュリティ支出を2009年度の82億ドルから年平均8.3%増額して2014年までに122億ドルとする。連邦IT予算の約10%が、システムとデータのセキュリティ保護の確保や国防省（DOD）のサイバーコマンドやその他のサーバーセキュリティ構想などの新イニシアティブに充当される。ニューヨーク証券取引所やホワイトハウスなどへの最近のサイバー攻撃を踏まえたサイバー・セキュリティ対策の強化が図られることになる。

③ グリーンテクノロジー：2007年のエネルギー自立・安全保障法（EISA- Energy Independence and Security Act of 2007）やその他の緊急経済パッケージに盛り込まれた環境対策を踏まえて、連邦政府はグリーンIT製品・サービスの採用に拍車をかける。よりスマートなエネルギー管理システムには、スマートグリッドによる電力ガス産業の近代化も含まれる。再生可能エネルギー源（RES）とスマートグリッド技術への投資を通じて米国のカーボンフットプリント（CO2が占めるスペース）とエネルギーコストを低減する。オバマ政権は、グリーンテクノロジーの利活用により役割モデルとしてこのこれを主導することになる。

④ 医療IT：医療改革は、電子ヘルス記録、保健情報・決定支援システム、保険請求処理などの重要な医療IT分野の成長に拍車をかかることになる。ヘルスケアIT投資は、現行システムの近代化で始まり、完全なインフラ改造で終わる。オバマ政権の医療IT投資は約190億ドルとなり、この初期投資により医療IT分野の伸びは大きくなろう。

しかしながら、2010年度予算の中では、連邦CIO職が行政管理予算局（OMB）に設けられ、①ニューテクノロジーの導入による政府イノベーションの向上、②効率性と実効性の高いITマネジメントによる重複投資の回避によるIT投資の削減の2つの大きな課題に取り組むことになる。2010年度予算におけるIT政策の中核が、連邦クラウド計画の導入である。

2010年度予算案の「分析上の展望（Analytical Perspectives）」の中の“Crosscutting Programs”において、オバマ政権は“技術力を梃子にして”政府内イノベーションを促進し、政府改革を行なうと宣言している。この技術パワー（Power of Technology）の重心が連邦クラウドの利活用である。つまり、オバマ政権は、①イノベーティブなWeb 2.0技術を採用し、②最新のITシステムの導入で政府サービスの実効性を改善・刷新し、③セキュアな連邦政府の情報システムと国家IT基盤を脅威から防護する動きを強めるのである。

オバマ大統領のオープン政府の重要課題の中核は、①透明性、②説明責任、③公的参加の3つである。この原則に基づくオバマ政権のIT政策では、ニューテクノロジーによる政府イノベーションの促進により、納税者のお金を節約し、情報セキュリティを確保し、個

人のプライバシーを保護する努力を払っている。

この原則を以って、オバマ政権による連邦政府の情報政策では、技術力（Power of Technology）をテコにして連邦政府を変革する方法として次の4点を重視している。

① ノベーティブなWeb 2.0技術の採用で、より透明性のある参加型・協働型政府の実現に向けた大統領誓約を履行すること。
② 最新のITシステムの採用により連邦政府サービスの実効性を近代化･改善すること。
③ 自然の脅威および悪意のある脅威に対する連邦情報システムおよび国家情報インフラの安全保障を確保すること。
④ 各省庁横断的な広範な利用に向けたIT投資と、重複した管理の乏しいプロジェクトを無くし、IT調達を合理化することで納税者のお金を節約すること。

オバマ政権では、大統領府の行政管理予算局（OMB）に連邦 CIO（e ガバメント行政官）を任命し、2010年度予算のITマネジメントのよい大きな責任を当てることになった。

オバマ政権の“ガバメント2.0”の主な情報政策の内容は次の通りである。

- 透明性：オバマ政権は、連邦政府の保有するデータをより利用しやすい形で一般大衆に利用可能にする努力を払う。この課題を促進するために、“USASpending.gov”の新たな方向付けを決め、“Data.gov”を立ち上げる。
- 2009年6月30日、連邦CIOのビベック・クンドラ（Vivek Kundra）は、連邦政府の歳出情報公開サイトの“USASpending.gov”に，IT 投資状況を米国民に情報開示するためのサイトである“IT Dashboard”（ベータ版）を新設したと発表。国防総省や司法省など、27 の政府機関が行政管理予算局（OMB）に報告するデータが公開されている。7000以上のIT投資情報が含まれている。
- “Data.gov”：連邦CIOは、政府データにアクセスするためのオンライン・レポジトリーであるData.govを設け、環境、エネルギー、保健医療、政府運営などの情報をダウンロードできるようにする。
- “政府におけるWeb 2.0”：連邦各省庁は、Web 2.0ツールのような社会的でビジュアルな技術を利活用するなどの市民が関与する新たなアプローチ方法を開発するための創造的な行動をとる。既存の政府ウェブサイトは、コミュニティ主導の特徴と機能を以って再活性化する必要がある。
- その他：「参加と協働」、「Recovery.gov」の設置など。

2010年度予算では、IT政策として次の課題が強調されている。

- 政府 IT 人材の補充：エンタープライズアーキテクチュア、ソリューションズアーキテクチュア、IT セキュリティ、IT プロジェクトマネジメントなどの政府の IT 人材の採用を促進する。2008 年 6 月 30 日現在で 17,652 人、2009 年 5 月現在で 17,785 人の上記の補充人材を拡充する。
- 政府システムをセキュリティで保護（セキュアにする）こと：2002 年の連邦情報セキュリティマネジメントは導入後 7 年目に入ったが、各省庁のセキュリティが十分に確保されていないことは明らかである。連邦政府の調達を担う GSA（総合サービス局)は依然として各省庁のセキュリティの弱みを発見している。米国民はこの脅威を無視することはできない。これに対応し、大統領は、米国の通信および情報インフラ問題を解決する計画、プログラムおよび活動に関する 60 日レビューを開始した。行政管理予算局（OMB）は、IG（監査総監)、CIO、上席プライバシー官（Senior Agency Officials for Privacy)、GAO（会計検査院：Government Accountability Office）および連邦議会と協働で電報政府の IT セキュリティおよびプライバシープログラムを強化する。
- Homeland Security Presidential Directive 12（HSPD-12）：2004 年 8 月 27 日に施行された国土安全保障大統領指令第 12 号（HSPD-12）は、「連邦政府の従業員と下請業者のための共通 ID 標準政策（Policy for a Common Identification Standard for Federal Employees and Contractors)」で、連邦施設及び情報システムのセキュリティ改善を目指す 9 月 11 日委員会の提言に対応する。HSPD-12 に準拠して、各省庁は、従業員および下請業者の ID を検証する標準化の背景を含む連邦認証発行のための特定の技術標準とビジネスプロセスに従うことを義務づけられる。
- 国家情報インフラをセキュリティで保護（セキュアにする）こと：政府のセキュリティ懸念は連邦システムだけでない。連邦政府は国を防護・防御し、市民の幸福を確保する責任を負う。しかし、米国における約 85%のクリティカル情報インフラは、連邦政府以外の利害関係者による所有である。したがって、産業と政府は、国民の情報インフラのセキュリティと信頼性に対する責任を分かち合うべきである。GAO（会計検査院)は米国重要情報インフラの防護の実施に関する懸念を表明している。連邦政府は公民パートナーシップの現在の構造を検証し、何が動いており、何故かを決めなければならない。大統領命令により 60 日間のサイバーレビューの一環として、成功した公民パートナーシップの特性を評価中である。
- プライバシーを防護すること：連邦各省庁のタスクは、(データや情報などの）侵害通知計画（breach notification plans）を実行し、不要な社会保障番号の収集と利用を無くし、不要な ID 情報の所持を少なくし、行動規則の概要を定め、不遵守（non-compliance）に対応する結果と是正措置を明示する政策を策定することである。各省庁は、プライバシー保護のすべての側面の進展を実証することを期待され

ている。連邦政府は、連邦システムおよび情報セクター全体の情報セキュリティの改善を続けることを義務づけられている。

オバマ政権は2010年度予算案における“IMPROVING INNOVATION, EFFICIENCY AND EFFECTIVENESS IN FEDERAL IT（連邦ITにおけるイノベーション、効率性および実効性を改善する)”と題された項目の中で、クラウド・コンピューティングプラットフォームを利活用し、各省庁共通のサービスとソリューションを最適化することを求めている。

連邦政府は、厳しい経済環境の中で最新技術を使ったイノベーションの促進に直面する実業界と同様、ニューテクノロジーを利活用した政府イノベーションの促進を要請。今後は、技術基盤投資を根本的に再検証し、「インフラ近代化プログラム（Infrastructure Modernization Program)」を導入し、新たな課題と責任に取り組むとしている。

オバマ政権は2010年度予算の中で、民間部門よりも早く、連邦政府によるサービスとしてのクラウド基盤（IaaS）を利活用して省庁間および選挙区の両方の効率性と透明性を高める数多くの実証プロジェクトを実施するとし、“連邦クラウド（Federal Cloud)”の導入に乗り出している。

2010年度予算案における連邦クラウドの導入に関する記述を要約すると、次の通りである。

- クラウド・コンピューティングとは、最低限のマネジメント努力またはサービス・プロバイダー相互作用を以って、迅速に提供およびリリースすることができる、コンフィギュレーション可能なコンピューティング・リソース（つまり、ネットワーク、サーバー、ストレージ、アプリケーションおよびサービス）の共有プールへの便利なオンデマンド・ネットワークアクセスを可能とするモデルである、と NISTと同様の定義を行なう。
- クラウド・コンピューティングのクラウド要素は、インターネット向けに使われるメタファ(比喩)から派生するもので、コンピュータネットワークダイアグラム(図)で描かれることが多い。概念的には、これは、拡張可能（scalable）でリアルタイムのインターネットベースのITサービスおよびリソースのモデルを指し、ユーザーがインフラの維持コストを負担することなくユーザーのコンピューティングニーズを満たすものである。
- クラウド・コンピューティングプラットフォームを実装すると、連邦省庁の専用データセンターと比べて異なるリスクを背負うことになる。新技術のサービス供給モデルの実装に伴うリスクには、政策の変更、ダイナミック・アプリケーションの実

装、ダイナミック環境をセキュアにすることなどが含まれる。このリスク軽減計画は、プロアクティブ（先を見越して対処する）プログラム管理オフィス（proactive program management office）を設置して、産業界のベストプラクティスとプログラム管理の政策を実行することにかかっている。

- 加えて、連邦政府は、ダイナミック（動的）なアプリケーション利用と情報共有をセキュアな形で実装することを認める新たなセキュリティ措置を積極的に整備する必要がある。これらの目的を実現するために、パイロット・プログラムを導入して、政府横断的なスケールモデルを提供する。
- クラウド・コンピューティング環境の実装をサポートするパイロット・プログラムは次の通りである。
  - エンドユーザー通信&コンピューティング（End-user communications and computing）：プロビジョニング（ユーザニーズに応じたサービスの提供）とデバイスにとらわれないエンドユーザーアプリケーションの運用を確保する：テレワーカーおよびモバイルワーカーの問題解決。
  - 仮想化されたデータセンターをセキュア（セキュリティで保護）すること。G2G、G2C（コントラクタ）、C2C のサービス提供モデル。
  - ポータル、協働およびメッセージング：データ公表のセキュリティを保護すること、市民その他の利害関係者の関与および労働生産性。
  - コンテント、情報および記録管理：市民および労働者生産性へのサービスの提供。
  - ワークフローとケースマネジメント：市民および労働者生産性へのサービスの提供。
  - データ分析、仮想化および報告：透明性とマネジメント。
  - エンタープライズ SaaS：具体例、金融マネジメント。
- クラウド・コンピューティングは、連邦データ施設の環境を最適化し、広範な消費者にサービスを提供するプラットフォームを創出する上で有益となる。
- “Work-at-a distance イニシアティブ”を新規導入し、最新技術を使って連邦政府の職員の遠隔労働を可能とし、旅費やエネルギー消費を節減する。このプログラムは、行政管理予算局（OMB）の連邦 CIO（e ガバメント行政官）の監督下で CIO 協議会が実施する。予算は、サービス・プロバイダーとしての GSA（総合サービス局）が担当。
- 連邦政府は、データセンターを仮想化し、データセンターと運用を統合化して、最終的にはクラウド・コンピューティングのビジネスモデルを採用して政府の IT インフラを改造する予定である。連邦各省庁と共同で実施する当初のパイロットプロジェクトは、適切なセキュリティおよびプライバシー保護を含む能力を実証するためのテストベッドになる。

- クラウド・コンピューティングの導入が最重要課題であり、この初期投資はやがて回収することになる。各省庁が自前の専用データセンターのホスティングシステムのコストを節減できるようになることから、この節減額はやがて初期 IT 投資額の数倍となろう。

クラウド・コンピューティングの導入実験を中核とする 2010 年度の連邦 IT 支出総額は前年度の 707 億ドルから 7%増の 758 億ドルとなる。しかしながら、行政管理予算局（OMB）の狙いは、連邦 IT におけるイノベーション、効率性および実効性を高めることである。連邦クラウド計画で以って連邦 IT 投資戦略を改革し、省庁レベルにおける重複した IT 投資を削減することである。しかし、2010 年度以降は、多くの省庁が自前のデータセンターのホスティングシステムのコスト節減を行ない、数倍の規模の費用削減を実施すべきだとしている。

1.4.2. オバマ政権における連邦 CIO の任命

ブッシュ政権と異なり、オバマ政権は初めて大統領府行政管理予算局（OMB）の中に連邦 CIO 兼 eGovernment/IT 担当行政官を任命し、効率性と実効性の高い IT マネジメントによる政府イノベーションを促進する。2009 年 3 月 5 日に米国で公式に初めて連邦 CIO に指名されたのは、インドに生まれ米国に移住したビベック・クンドラ（Vivek Kundra）である。非公式には、カレン・エバンズ（Karen S. Evans）が従来、行政管理予算局（OMB）の“e ガバメント&IT 局”行政官として事実上の CIO であった。

ビベック・クンドラ（Vivek Kundra）のプロフィール

- ビベック・クンドラ（Vivek Kundra）は 1974 年 10 月にインドのニューデリーで生まれる。タンザニアを経て、11 歳で両親とともに米国に移住。メリーランド大学（心理学専攻）を卒業し、同大学大学院の修士課程（IT 専攻）を経て、非常勤教授で無線プロトコルから AI にいたる理論と応用を教える。
- アーリントンカウンティのインフラ技術局長を経て、バージニア州の商業技術補佐官に就任。その後、ワシントン DC のコロンビア特別区の CTO として、“Apps for Democracy”イニシアティブを立ち上げ、公的にアクセス可能な Web サービスを使ったオープンソースとクラウドソーシング（Crowd Sourcing）アプリケーションの開発で有名になった。
- InfoWorld 誌から、全米トップ 25 人の CTO のひとりに選ばれている。2009 年 3 月 5 日、オバマ大統領により連邦 CIO に指名される。連邦 CIO の役割は、連邦 IT 投資の政策と戦略的計画を指揮し、連邦技術支出を監督することである。オバマ大統領

によると、クンドラ連邦 CIO は、「可能な限り最もセキュアで、オープンかつ効果的な方法で連邦政府を運営する重要な役割を果たす」人物である。

2009 年 3 月 5 日付けホワイトハウス報道によると、ビベック・クンドラ（Vivek Kundra）連邦 CIO の役割は、連邦 IT 投資の政策・戦略計画を管理し、連邦技術支出の監督責任を担うことである。連邦 CIO は、システム相互運用性および情報共有を確保する EA を策定・監査し、確実に全連邦政府横断的な情報セキュリティとプライバシーを保護することである。連邦 CIO は、連邦 CTO と密接に連携してオバマ大統領の技術政策の課題を押し進めることになる。

他にも、Chief Performance Officer（CPO）に経営コンサルタントのジェフリー・ザインツ（Jeffrey Zients)、連邦 CTO にバージニア州テクノロジー長官のアニーシュ・チョプラ（Aneesh Chopra）が指名されている。バージニア州テクノロジー長官として Web 2.0 サービスの広汎な導入を手掛けたこと、行政 IT に関して斬新なアイデアを持っているチョプラ連邦 CTO に対する期待も高く、グーグルのシュミット CEO はわざわざメッセージを寄せ、ティム・オライリーも「最良の選択」と賞賛している。

クンドラ連邦 CIO の最重点課題は、2010 年度予算において自己中心的（silo'ed）な IT 基盤の構築をやめて IT 予算を削減することである。このためには、①連邦 IT 調達を改善（IT 効率の向上に対するリウォードの提供、各省庁の IT 支出削減のインセンティブ、クラウド・コンピューティングの利用拡大)、②相互運用性、ポータビリティおよび標準の必要性（政府 PAAS？)、③共通クラウド・プラットフォーム上の国防省（DOD)・各省庁間の戦略的調整、④GSA をクラウド・コンピューティングの重心にすること、⑤透明性によるイノベーションの促進などを重視しているようである。

連邦 CIO 兼 e-Government/IT 行政官に指名された直後のビベック・クンドラ（Vivek Kundra）への電話インタビューによると、同氏は連邦 CIO として、連邦政府における IT 技術の使われ方を検討し、政府運営のコストを引き下げ、同時に公的部門の国民との相互作用の方法を根本的に変えるイノベーティブな道筋を探ると語っている。主なインタビュー内容のポイントは次の通りである。

- 所信表明
  - 政府が“我々人民（We the People)”を考えるものであること、市民に関与してもらい公的部門のどこにカネが使われているかを明らかにする官僚の説明責任を維持しつつ、我々がオープンで、透明性のある、(国民）参加型で、協働型の政府を運営する能力があることを明らかにする。

- 同時に、厳しい経済環境の中で、経済危機とエネルギーおよび医療問題に直面していることに留意すること。技術のパワーを梃子にしてこの国が正しい方向に向かいつつあることを確かなものにすること。
- 以上を踏まえて、連邦政府が年間710億ドルものIT支出を行い、最大の技術の買い手となっていることを検討することになる。
- 私は、各省庁のCIOと密接に連携し、各省庁が確実にオープンガバメントの課題を推し進めていること、公的部門の技術を根本的に変革できる方法を検討し、公的部門が民間部門に遅れをとっていることがないようにする。
- 加えて、ニューテクノロジーが、選挙民へのサービスの提供方法を変えるものであり、連邦政府が効率的に運営されていることを明らかにする必要がある。

● 連邦CIOとしての役割
- 私は、連邦CIOとe-Government/IT行政の2つの任務を果たす。我々は、電子政府（e-Government）だけではなく、各省庁のバックエンドシステムを重視し、情報技術（IT）に関する全体的な観点からの検討を行いたい。
- 各省庁のCTOはいずれ大統領により任命されよう。連邦CIOの役割は、次の3つである。①710億ドル（2009年度）の予算を検討し、より効果的な支出を行っているかの観点から連邦政府のオペレーションを検証すること、②国民（the public）が情報にアクセスしていること、国民が政府にアクセスしていることを確保する透明性のあるオープンな政府を重視し、情報経済における連邦政府と国民との相互作用の方法を再考すること、③民間部門らNGOで生まれつつあるイノベーションを梃子として利用する観点から、これを連邦政府に適用し、新技術を導入するスピードを変えること。

● “Data.gov”の設置
- 我々のやりたいことのひとつは、“Data.gov”を立ち上げることである。クンドラ連邦CIOは、コロンビア特別区でも“D.C. Data Catalog”と呼ばれる同様のWebsiteを立ち上げ、建築許可書から道路上で交通事故死する野生動物のピックアップにいたるフィード（Feed）をリアルタイムで公表している。
  “www.data.gov”は、分散化データであり、国民がこのデータにアクセスできるようにする。公的部門の最も難しい問題をいかにして解決するかにつき、市民であれ、NGOであれ、国民の支援を得る。
- NIH（国立衛生研究所）が世界の研究機関と連携してヒトゲノムプロジェクトデータをオンラインで公表した。この結果、500以上の新薬が開発され、食品医薬品局（FDA）に対する新薬審査申請につながっている。

- 国防省（DOD）が開発したGNSS（衛星測位システム）のデータ公表によりGPS革命が起こり、iPhoneやカーナビなどのGPSデバイスの発展につながっている。
- 同じ方法と精神により、連邦政府が持つ多大なデータを公表する。しかし、国家安全保障上の理由などにより民間開放に制限があるものもある。連邦情報公開法（FOIA）などのデフォルト仮説推論で行政情報をパブリックドメインに置く場合の問題を検討し、次になにをプライベートにする必要があるかを検討する。

● デジタルエコノミー
- 政府が直面する挑戦のひとつは、オンラインまたはサイバースペースで情報を公開すれば、バックエンドの問題がより重要となる。特に、デジタル経済に対応できる政府の情報システムのバックエンドである。
- ひとつの例だが、学生用SNSのFacebookでは、自主運営と市民参加が可能となった。140万人以上もの人々が色々な問題や政策を議論できるし、ある動きも起こせる。
- もうひとつのモデルは、連邦政府と市民との二方向のやりとりである。こうした新たな現実に対処可能なためには、政府のバックエンドを大改造しないといけない。率直にいえば、このような大改造に向けた投資は過去に行われていない。
- 21世紀の労働力（Workforce）についても再考しなければならない。
- データフィード（必要な領域）のような情報を可能にする方法も検討する必要がある。コンテクストリッチモデルの中でアプリケーションを作ることができる方法だ。過去に政府がやったことといえば、ホームページ（Website）を作成し、これが一省だというだけであった。こうしたWebsiteのトラフィック量とFacebookと比べてみてもらいたい。いかにして情報を正しい脈絡（コンテキスト）の中で公開していくかを検討する必要がある。
- 例えば、4月15日をみて、ある日に連邦政府が特定の行動を停止したとすれば、この情報が正しいコンテキストの中に置かれているかを確かめないといけない。4月15日前後の税金について気がかりなるとか、この日に関連する他の問題が気になる場合である。政府はコンテクストリッチな情報フローに向かい行動していく必要がある。

● オープンソース
- たとえば、フリーソフトウェアのMediaWikiのようなオープンソースを技術だと考えるとしよう。ワシントンDCのコロンビア特別区でやったことは、ウィキペディア（Wikipedia）ソリューションを使って、ひとりひとりのスタッフがコラボレーションを行い、情報にアクセスしたのである。国土安全保障省（DHS）や連邦航空局（FAA）のような特殊任務のミッションクリティカルな専用ソフトウ

ェアを使う場合もある。ここでは、オープンソースを使うことはできない。ソフトウェアについては、バランス調整のとれたプラグマティックなアプローチ方法で望む必要がある。

- 社会保障データセンター
  - 単純な例は、社会保障局（Social Security Administration）である。全く新しいデータセンターを設置するために予算申請している。我々が確認したいことは、社会保障局が、過去に獲得したものよりも幅広い角度で投資を検討しているのかどうかである。相互運用性のない分断されたインフラの拡散を行うことが多いものである。こうした投資では、連邦政府全体のポートフォリオを検討してみる必要性がある。全く新たなデータセンターを設置する投資を行う際には､大きな連邦 IT のビジョンに照らしてどういうものかを考えないといけない。社会保障局だけにとどまらず、他の省庁の機能にもどのようなレバレッジ効果があるかを考慮する必要がある。

2009 年 4 月 30 日（木)、ビベック・クンドラ（Vivek Kundra）は正式に連邦 CIO 兼 e-Government/IT 行政官に就任した。オバマ政権で新設された連邦 CIO に就任したビベック・クンドラ（Vivek Kundra）は行政管理予算局（OMB）の“e-Government/IT 担当行政官”も兼務することになり、連邦政府の技術投資と技術支出を監査する。

連邦 CIO の役割は、システムの相互運用性（interoperability）と情報共有（information sharing）を確保する EA（enterprise architecture）を策定・監督し、連邦政府横断的な情報セキュリティとプライバシーを確保することになる。同日の電話会議で、クンドラ連邦 CIO は、オープンガバメントを含む IT 政策課題を推し進め、確実に公的部門における技術革命を起こし、公的部門が民間部門よりも遅れているとの意見がでることのないようにすると語っている。

オバマ大統領によると、アメリカン・イノベーションの精神と技術のパワーを使い、連邦政府の運営コストを引き下げ、政府運営のパフォーマンスを改善することをクンドラ連邦 CIO に指示したという。連邦 CIO は、可能な限り最もセキュアで、オープンかつ効率的な方法で連邦政府を運営する上で重要なカギとなる役割を果たす。

2009 年 6 月 17 日の InformationWeek 誌におけるビベック・クンドラ（Vivek Kundra）連邦 CIO との主な質疑応答（要旨のみ）は次の通りである。

- InformationWeek 誌の質問

- 2010 年度予算案では、クラウド・コンピューティングのプロジェクトが言及されていたが、その内容をもう少し言及して欲しい。
- クンドラ連邦 CIO の大きな課題のひとつは、連邦省庁が垂直的に使ってきた IT 予算を、ビジネスプロセスを根本的に変革させるという観点で水平的な実装を行なうときに技術は最も効果的であること。
- クラウド・コンピューティング投資の一部は、政府横断的に水平的に利活用できるプラットフォームに充てられる。2010 年度予算のクラウド・コンピューティング投資は、コストを低減し、連邦横断的なイノベーションを促進し、ワーカーがどこにいても使える技術を利用可能にすることである。以上が、2010 年度予算の狙いか。

- クンドラ連邦 CIO の答え：
  - RFI（情報提供要求書）やクラウド・コンピューティングサミットの内容の如何にかかわらず、GSA（総合サービス局)が公表してきたことを検討すれば、アイデアが詰まってきていることが分かる。10 月に近づけば、2010 年度予算で要求された 3.3 億ドルの具体的なクラウド･コンピューティングのプロジェクト計画と資金使途が決まる。

- InformationWeek 誌の質問：どういうプロジェクトで、何をしようとしているのか

- クンドラ連邦 CIO の答え：
  - 私どもはこれを拡張しつつある問題（scaling problem）に転化しようとし、さらに、省庁横断的な最小公分母（lowest common denominator）を検討している。ブログやビデオ、軽量のワークフロープラットフォームまたは公的参加プラットフォームのような極めてシンプルなツールである。
  - 重要なカギは、簡単な方法で連邦政府に利用可能なものにすることで、セキュリティ要求事項をアーキテクチュアに焼き付けるような前もってセキュリティを取り扱うことである。
  - 目標は、私的な生活の中で e-mail のアドレスを設定するとか、写真共有プラットフォームやオンライン写真保管を利用するときに、クレジットカードを示し、リアルタイムでサービスの提供を受けられるように簡単なものにすることだ。なぜ、こんなことを全省庁で行なえないのか。2002 年の連邦情報セキュリティマネジメント法（FISMA- Federal Information Security Management Act of 2002）で証明されたインフラやプラットフォームを持っていることを何故、前もって確かめることができないのか。なぜ、調達プロセスを遵守しており、リアルタイムでこれ

らのプラットフォームを提供できることを確かめることを巡るサービス提供問題をなぜ解決できないのか。

- 我々は、“これがスケジュールだ”という考え方から、“リアルタイムで提供できるプラットフォームはこれだ”という考え方にシフトしつつある。私どもが取り組んでいるのはこういうことだ。スケジュールを持ち、スケジュール表を抱える行政法人としてのGSA（総合サービス局)という考え方から移行しつつあるが、連邦政府横断的な情報技術（IT）となると重心がみつからない。このために、(2010年度予算で)重心を創出したのである。

- InformationWeek誌の質問：だから、貴方は重心にすることを支援するためにGSA（総合サービス局)と密に働いているのか。

- クンドラ連邦CIOの答え：
  - 我々は、GSA（総合サービス局)を重心（Center of Gravity）にするために極めて密接にGSAと働いている。

- InformationWeek誌の質問：どういう意味か。GSAとしなければならないことは、ITを取り扱うための新たな方法を開発することではないのか。

- クンドラ連邦CIOの答え：
  - それもひとつである。情報セキュリティに関する政策問題を検討すれば分かる。連邦情報セキュリティマネジメント法（FISMA）が好例である。今日、各省庁は、同一の技術を使うときでも自前の証明と認証を行う必要がある。証明を取得してその権利を得ることができる中心となる場所があれば、どれくらいのカネを節約できるかを想像してもらいたい。
  - 2番目は、各省庁の店頭を実際につくりつつあることで、消費者が行える簡単な方法で、(店頭）にサービスを準備しておく（Provision Services）ことだ。
  - 3番目は、対象となる技術を具体的に展開してく（rolling out）プラットフォームである。これらのプラットフォームを確実に拡張可能かつ弾力性のあるもの（scalable and elastic）にしておくことだ。そうすれば、各省庁が技術投資を望む場合にも、10%程度のキャパシティを使うような場所に何かを準備するためだけの契約に金を使うよりも、すばやく実行し、拡張することが可能となる。

- InformationWeek誌の質問：省内に構築するクラウドのような技術についてはどうか。例えば、国防情報システム庁（DISA- Defense Information Systems Agency）は、自

前のプライベート・クラウドを構築しつつある。連邦政府内に集中型プラットフォーム（centralized platform）をおく必要性があるのか。

- クンドラ連邦 CIO の答え：
  - このアプローチは、様々な省庁には異なる要求事項があることを認めるものだ。連邦航空局（FAA）が全米の航空管制のような目標にフォーカスすれば、それは省庁特有のものだ。これに対して、最小公分母（lowest common denominator）である協働プラットフォーム（platform for collaboration）を検討しつつあるとすれば、それは別問題だ。すべての異なる省庁に共通するものはなにか。内部的に、我々は共通プラットフォームを開発して立ち上げようとしている。GSA（総合サービス局)が、こうしたサービスを提供するセンターになる。だから、共通プラットフォームを構築して、それを他のデータセンターに複製品を作ってはいけない。同時に、私どもは確実にオープンアーキテクチュアを重視する必要がある。オープンアーキテクチュアは、情報共有、省庁間協働にとって極めて重要なものである。

- InformationWeek 誌の質問：GSA（総合サービス局)はなんらかの方法で共有サービス機関に変貌する必要があるのか。そうなると、GSA はこの計画に基づくデータセンターの管理運営を行うことになるのか。

- クンドラ連邦 CIO の答え：それは一部だ。私は新政権と伴に働くことを楽しみにしており、GSA が何をする必要性があるのかをみてみたい。

- InformationWeek 誌の質問：政府内の IT 調達は、まるで政府が空母を買い付けるように行う必要があるとの非難に同意するか。IT ではそうすべきではないのか。

- クンドラ連邦 CIO の答え：プロセスをながめ、調達に 18 ヶ月～2 年かかるとすれば、ひとつの革命、つまりひとつのサイクルを逸したことになる。調達プロセスだけを抽出できれば。セキュリティ、アーキテクチュア、サービス準備（Provisioning）など、技術イニシアティブを展開するよりも、むしろ提供されつつあるサービスを梃子として利用することを重視すべきである。これが、連邦政府を動かして向かわせたいところである。これには時間はかかる。それが公的政策となり、調達などになると、大きな変化を起こすことなろう。

- InformationWeek 誌の質問：どれくらいの期間がかかるのか。上記のプロセスを正しい軌道にのせるには 3～4 年かかるとみているのか。抵抗にあうと思うか。

- クンドラ連邦 CIO の答え：
  - 就任して最初の月に、以上の変容努力を主導する人たちを探した。ワーキンググループという点では、クラウド・コンピューティングに大半の人たちがいた。CIO 達は、技術供給の準備以外のことをやろうとしない。彼らの見解は、この技術準備に留意すれば、迅速なサービスを消費者に提供できるという考え方である。
  - 私どもが直面する課題は、セキュリティ、プライバシー、発注契約（Contracting）などを巡るチャレンジである。更に前進すれば、他の多くの課題に直面することになる。我々は調達コミュニティ、プライバシーコミュニティ、セキュリティコミュニティと極めて密接な連携をとりつつある。時間はかかる。しかし、今後数ヶ月内に一連のサービスを立ち上げ（Rolling out）、そこから拡張路線を歩むことになる。
  - （いつスタートするのか）間もなくだ。プラットフォームとしての政府（government as a platform）を念頭におきつつある。

1.4.3. クンドラ連邦 CIO のクラウド・コンピューティング見解

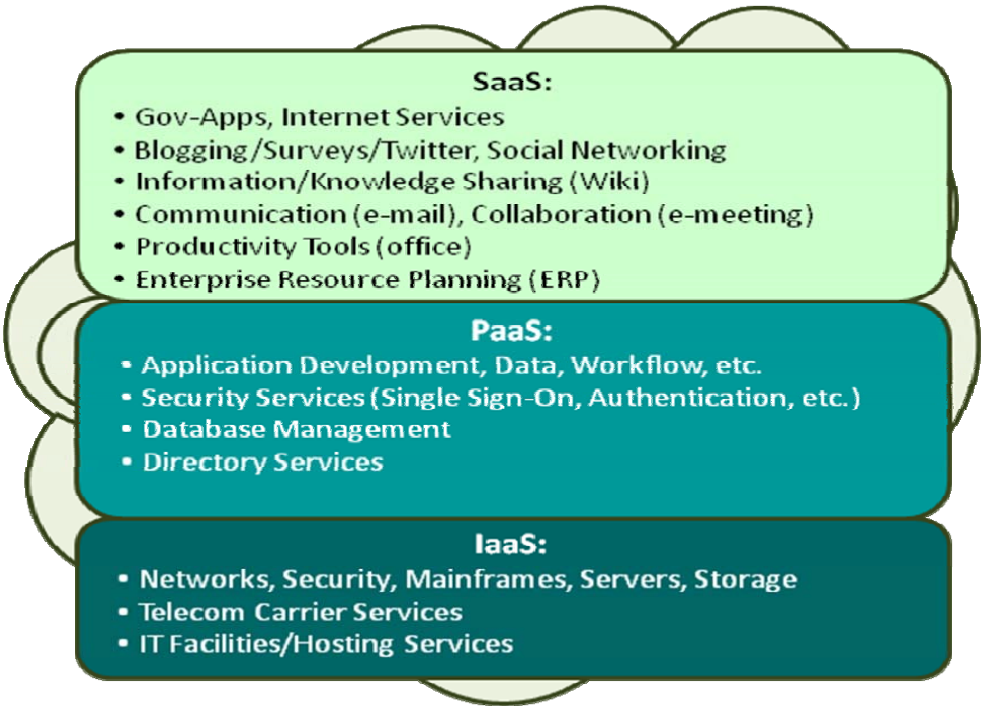
2009 年 7 月 15 日にワシントン DC の国立防衛大学（NDU）で開催された「クラウドコンピューティングシンポジュウム」において、ビベック・クンドラ（Vivek Kundra）連邦 CIO は、中核技術としてクラウド・コンピューティングを連邦政府に導入し、連邦政府の一般調達を担う総合サービス局（GSA）内に連邦省庁向けのワンストップ・ショップである“クラウド・コンピューティング Storefront”を立ち上げると言明した。連邦 CIO と彼のチームは GSA（連邦調達局）を“IT の重心”とし、Amazon.com のような商用オンライン購買サービスを真似て、GSA 内に“連邦クラウド・ストアフロント”を設置する計画である。各省庁は第 3 者プロバイダーにより提供されるワンストップ型のクラウド共通サービスを取得することになる。

連邦各省庁は、製品やサービスが IT 調達規制やサイバー・セキュリティ規則に遵守しているかどうかを気にすることなく、遠隔ストレージやホスト型アプリケーションのような技術サービスの選択が可能になる。GSA は、このサービスが 2002 年の FISMA（連邦情報セキュリティ管理法）を遵守していることを確実に保障し、必要なセキュリティ認証・証明を具備する。

クンドラ連邦 CIO の講演内容は次の通りである。

- “クラウド（雲)”を創出するのは、SaaS（Software as a Service)、PaaS（Platform as a Service)、IaaS（Infrastructure as a Service）の 3 つのサービス提供モデルである。
  - **Software as a Service (SaaS)**：サービス・プロバイダーがオンデマンドとして利用する目的の顧客へアプリケーションをライセンスするためのソフトウェア利用モデル；Software deployment model whereby a provider licenses an application to customers for use as a service on demand
  - **Platform as a service (PaaS)**：サービスとしてのコンピューティング・プラットフォーム＆ソリューションスタック（フル機能ソリューションを提供するための一群の製品またはサービス）；Delivery of computing platform & solution stack as a service
  - **Infrastructure as a Service (IaaS)**：サービスとしてコンピュータインフラ（典型的にはプラットフォーム仮想化環境）の提供；Delivery of computer infrastructure (typically a platform virtualization environment) as a service

図 9　クンドラ連邦 CIO によるプレゼンテーションシート

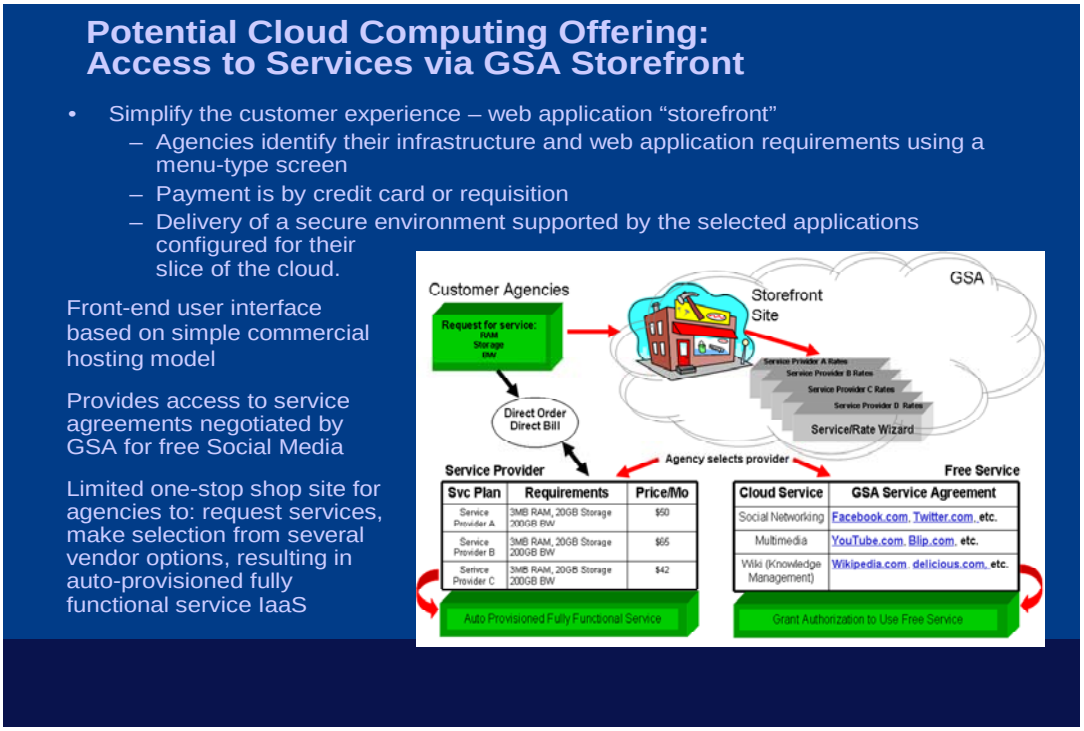


クンドラ連邦 CIO は、Web アプリケーションの Storefront を創出し、連邦政府が標準のセキュアなクラウド・コンピューティングのアプリケーションを簡単に取得できる計画を推進すると語っている。これで、連邦政府は複雑さを取り除くことができ、FISMA（連邦情

報セキュリティマネジメント法）の遵守と証明に煩わされる心配がなくなるという。連邦政府の各省庁は簡単なストアフロントでリアルタイムのクラウド・サービスを準備することができるようになる。

- 総合サービス局（GSA）の店頭（Storefront）を通じてサービスにアクセス
  - Webs アプリケーションの“storefront”で Amazon.com のような顧客体験を簡素化する。
  - 各省庁は、Menu タイプスクリーンを使ってインフラと Web アプリケーション要求事項を識別・認証する。
  - 決済は、クレジットカード決済または徴用（Requisition）
  - シンプルな商用ホスティングモデルに基づくフロントエンド・ユーザーインターフェース
  - 無料 Social Media 向けに GSA との交渉によるサービス契約へのアクセスを提供。

図 10　Storefront を通じてクラウド・サービスを利用



連邦政府の一般調達を担う総合サービス局（GSA）は、サービスとしてのインフラ（IaaS）向けの RFI（情報要求書）を 2009 年 6 月に公表した。連邦政府は既にクラウド・コンピューティングに関する複数のパイロットプロジェクト計画を策定したようである。クンドラ

連邦 CIO と彼のチームは「クラウド・コンピューティングソリューション向けデジタル Storefront」の立ち上げに取り組んでいるのである。

クンドラ連邦 CIO によると、連邦政府をクラウド・コンピューティングモデルに移行することは、連邦政府と民間セクターの大の技術ギャップを解消する上でも極めて重要である。旧来の連邦 IT 調達プロセスでは、新たなシステムを開発・利用するのに約 2 年の期間を費やしている。クラウド・サービスを使う各省庁は、ダウンタイム（システムの停止時間）をかけずともベンダーに委託してシステムの更新を行なうことができる。

以上のようなシンプルなコンシューマ（プライベート＆コミュニティ）クラウド技術でも連邦政府の共通サービスを取得する能力を大幅に簡素化することができる。しかし、機微な連邦政府の公的データについては同様のアプローチ手法が効果的ではないと、クンドラ連邦 CIO は認識しているという。連邦 CIO は 11 の会員グループとどのデータがコンシューマ・クラウド・アプリケーションにとって適切なものであり、どのデータが政府所有のインフラ上に蓄積すべきかを明らかにしようとしているようである。各省庁のデータセンターに莫大な投資を行うのではなく、IT の重心（center of gravity）を構築し、各省庁横断的なリソース共有を行うかを検討しつつある。

ビベック・クンドラ（Vivek Kundra）連邦 CIO は、クラウド・コンピューティングとコンシューマ技術を公的部門に導入し、連邦政府をよりスマートかつ効率的にすると語っている。クンドラ連邦 CIO によると、クラウド・コンピューティングの導入拡大で、データ共有（data sharing）の改善と連邦政府、州政府および地方政府間のコラボレーション促進が進展することになる。

クンドラ連邦 CIO は、クラウド・コンピューティングを、「政府間 IT 関係をリメイクする莫大な収益機会」であるとも語る。「長期にわたり私達は極めて垂直的にものごとを考えつづけ、ものごとを確実に分断化してきた」と過去の IT 政策の盲点を指摘するクンドラ連邦 CIO は、今こそ、水平思考と垂直思考の両面でコラボレーションを推進するソリューションを以って政府間 IT 関係をリードするようである。

現在の議論は、連邦 CIO と行政管理予算局（OMB）が、機微な連邦データに対応するために、これまで以上に集権的な政府インフラの最新バージョンである政府運営のクラウドインフラを構築する意向があるのかどうかに専門家も関心の目を向けつつある。

NASA（国立航空宇宙局）は、“Nebula（ネブラ）”と呼ばれるクラウド・コンピューティングモデルを開発し、数々のプロジェクトをサポートしつつある。Nebula（ネブラ）は、

サービスとしてのインフラ、プラットフォームおよびソフトウェアを組み合わせたものであり、NASA はこれをサポートする IT アーキテクチュアを構築している。コンポーネントには、カリフォルニア大学サンタバーバラ校で開発されたオープンソースのクラウド基盤ソフトウェアで、Amazon のクラウド・サービスの“Amazon Elastic Compute Cloud (EC2)”と互換性のあるインターフェースを備える“Eucalyptus”や、Sun が買収した“Luster ファイルシステム”、Python で実装される Web アプリケーションフレームワークの“Django（ジャンゴ)”、オープンソースの全文検索システムの“Solr”、検索エンジン、統合開発環境などが含まれている。Nebula（ネブラ）は、アマゾン Web サービスと号完成があり、Nebula バーチャルサーバーはアマゾンの“Elastic Compute Cloud”上で稼動する。2009 年 6 月に発表されたホワイトペーパ（ドラフト）の中で、NASA のクリス・ケンプ（Chris Kemp）CIO は、セールフォースドットコム（Salesforce.com）の Force.com やグーグル App エンジンサービスと概念的に比較できる、ユーザー作成ブログ・Wikis と他の開発用 API のテンプレートを含む Web アプリケーションフレームワークを提案している。

NASA は Nebula（ネブラ）を使い諸外国のパートナーや研究機関と共同で NASA のイメージや統計を共有しようとしている。また、クンドラ連邦 CIO も、Nebula（ネブラ）を複数の省庁に役立つ中核プラットフォームにする選択肢を検討しているという。このシステムは、高機能コンピューティング、ストレージおよびネットワーク接続を提供する。

1.4.4. GSA（総合サービス管理局)と連邦クラウド CTO 兼内務省 CTO の任命

行政管理予算局（OMB）の一般暢達を担う GSA（総合サービス管理局)は 2009 年 4 月、エンタープライズアーキテクト（EA）やクラウド・コンピューティングサービスの専門家であるパトリック・ステイングレー（Patrick Stingley）を連邦クラウド CTO 兼内務省 CTO に任命し、連邦政府におけるクラウド・サービス導入の計画を策定中である。しかし、わずか 1 ヵ月半足らずで、パトリック・ステイングレーは土地管理局（Bureau of Land Management）の CTO に復職してしまった。GSA（総合サービス局)は連邦クラウド CTO の役職の設置は少し時期尚早であったと、GSA の CIO であるキャシー・コールマン（Casey Coleman）はコメントしている。

クラウド・コンピューティングは、連邦 CIO のビベック・クンドラ（Vivek Kundra）の主要イニシアティブであり、その重要性は大統領の 2010 年度補正予算に対する附則の中で記述されている。クンドラはワシントン DC の CTO としての前職でも、グーグルのアプリケーションパッケージである Google Apps（グーグルアップス）を市民に紹介し、クラウド・コンピューティングが連邦 IT 予算を削減するひとつの方法になりうると語ったこともある。

また、ステイングレーも引き続きクラウド・コンピューティングを注視し、「連邦クラウド・コンピューティング基盤（Infrastructure）の開発」という講演を行っている。

連邦クラウド CTO の役割を設けるのは時期尚早だったとしても、連邦政府の調達を担う GSA（総合サービス局)はオバマ政権のクラウド・コンピューティング構想を推進する中核的な役割を担い、連邦政府 IT の重心（center of gravity）の一角を占めるべきだ、とコールマン女史は語っている。GSA は現在、Terremark 社のサービスプロダクトとしての Enterprise Cloud 基盤（利用したキャパシティ毎の課金）を使い連邦政府情報 Web サイトの“USA.gov”を運営している。旧ホスティング契約の更新では、競争入札で、Terremark 社と多年度契約を行い 80～90%の費用(約 1.35 億ドル)を節減している。オバマ政権では、GSA がシェアードサービスの役割を担うことも可能である。しかし、この可能性が現実化するかどうかについては、コールマン女史は口を割らないようである。

1.4.5. GSA（総合サービス管理局）による RFQ（見積依頼書）

2009 年 5 月の IaaS に関する RFI（情報依頼書）と同年 6 月の SaaS に関する RFQ（見積依頼書）に続き、米国連邦政府の一般調達を担う GSA（総合サービス管理局）は 2009 年 7 月 31 日、IT 調達スケジュールとして知られる“連邦供給計画（FSS-Federal Supply Schedule）Schedule 70”に基づいて、GSA が長期的な業務委託契約を結ぶ IT ベンダーに対して IaaS（サービスとしてのインフラ）の 3 つの分野に関する RFQ（見積依頼書）を発表し、ベンダーに次のいずれかおよび/または全部の入札参加を要請した。このワークスコープは、GSA のクラウド・ストアフロントを構成する、①クラウド・ストレージサービス、②バーチャルマシーン（VM)、③クラウド Web ホスティングの 3 つの IaaS サービスである。入札は 8 月 12 日に予定されている。

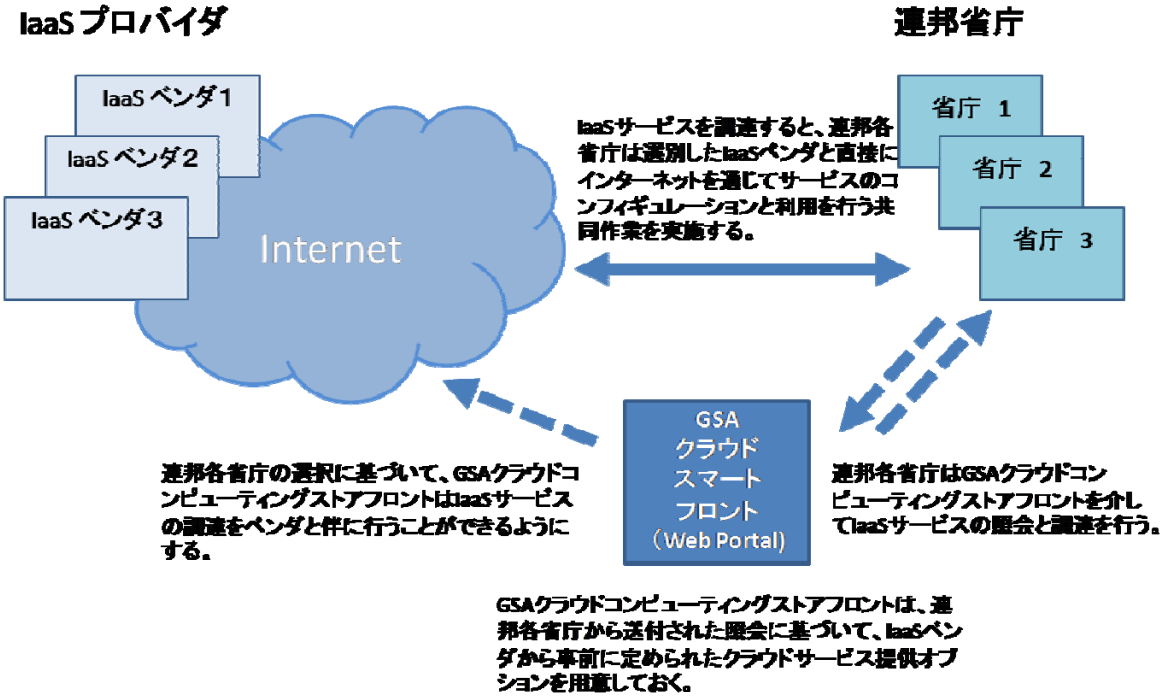
本 RFQ(見積依頼書)におけるクラウド･コンピューティングに関する記載内容を概観し、その後の行政管理局（OMB）および GSA（総合サービス局）の考え方を整理してみると、以下の通りである。

- クラウド・コンピューティングは、オバマ大統領による情報技術（IT）を刷新するための主要イニシアティブである。クラウド・コンピューティングは、サーバー、データベースおよびアプリケーションの仮想化に基づく商用的に利用可能な技術を活用して IT インフラのコストを削減することができる。

- GSA（General Services Administration）は、クラウド・コンピューティングサービスなどの市場イノベーションを利活用することで省庁横断的な共通サービスとソリューションを最適化して効率性を高めるパイロットプロジェクトを実施する。
- 上記の目的で、GSA は、2009 年 6 月 1 日の NIST（米国国立標準技術研究所）のクラウド・コンピューティングに関するワーキング定義（仮定義または作業定義の意味）を採択した。つまり、クラウド・コンピューティングとは、「コンフィギュレーション可能なコンピューティング・リソース（つまり、ネットワーク、サーバー、ストレージ、アプリケーションおよびサービス）の共有プールへの利用可能かつ便利なオンデマンド・ネットワークアクセスを可能とするモデルである」。
- 連邦クラウドコンピューティングフレームワークとは、クラウド・コンピューティングを可能にするために必要となる重要な能力であり、連邦政府向けクラウド・コンピューティングサービスのための重要なカギとなる機能コンポーネントである。それは、アーキテクチュアでもなければ、オペレーティングモデルでもない。このフレームワークは次の 3 つで構成される。
  - クラウド・サービス提供力：クラウド・サービスを提供するために必要とされるコア能力
  - クラウド・サービス：クラウドにより提供されるサービス
  - クラウド・ユーザーツール：ユーザーがクラウド・サービスを調達、管理および利用することができるツールまたは能力

- GSA（総合サービス管理局）は、GSA の Web サイトに “クラウド・コンピューティング・ストアフロント（Storefront)” のサイトを設置し、連邦政府の各省庁によるクラウド・サービスの取得を促進する。連邦政府の購買担当は、クレジットカードまたはその他の決済手段を通じて、GSA が管理維持する “Cloud Computing Storefront” と呼ばれる Web ポータルを通じて必要なクラウド・ストレージサービス、バーチャルマシーン(VM)およびクラウドWebホスティングの3つのIaaSサービス提供物(service offerings）を購入する。これを図式化すると、次のようになる。

図 11　GSA クラウド・コンピューティング・ストアフロントの
クラウド・サービス調達関係図



GSA（総合サービス管理局）による IaaS サービスに関する RFQ（見積要求書）入札に参加する IaaS ベンダーについては、クラウド・コンピューティングに関する一般要求事項、テクニカル要求事項などが示されている。クラウド・コンピューティングの 5 つの基本特性であるオンデマンド・セルフサービス、ユビキタスネットワークアクセス、ロケーション自在のリソース・プーリング（Location Independent Resource Pooling）、速やかな弾力性（Rapid Elasticity：迅速な再生力）、評価済みサービス（Measured Service）の定義も NIST のワーキング定義と同一である。

- IaaS の請負業者（Contractor）は、①サービスレベル契約（SLA）、②ヘルプデスクおよびテクニカルサポート、③リソース（ドキュメンテーション、寄稿・解説記事など）を記載する URL を提供し、サービス準備の能力を示す必要がある。特に、サービスレベル契約（SLA）の中で、次の内容を明らかにしなければならない。
  - 99.95%の高いサービスアベイラビリティ（可用性）：1 ヶ月あたりの総稼動時間（Uptime Hours）÷合計時間（稼働時間＋停止時間）
  - 1 時間以上の緊急停止（Unscheduled downtime）になる重要な停電の発生。
  - ほぼリアルタイムでのサービスの準備と事前準備の時間

- また、IaaS ベンダーは、オンデマンド・セルフサービス発注、サービスの準備（Provisioning)、ユビキタスネットワークアクセス、簡易かつ迅速なサービスの拡充と圧縮、コンシューマ向け利用のモニター、管理および報告を行う能力を具備する必要がある。
- 情報技術（IT）システムセキュリティの要求事項については、大統領府行政管理予算局（OMB）の通達（Circular）A-130 の“連邦情報資源の管理（Management of Federal Information Resources)”は連邦省庁に対してセキュリティ計画を義務づけている。連邦政府と請負業者（Contractor）は、NIST の Special Publication（SP）800-47 の“情報技術（IT）システムの相互接続に関するセキュリティガイド（Security Guide for Interconnecting Information Technology Systems)”と付則 A（セキュリティ要求事項）および付則 B（人事セキュリティ）に規定される相互接続契約（ISA）と MOU を誠実に締結する必要がある。連邦政府は、インパクトの低いシステム向けの NIST の SP 800-53 である“連邦情報システムのための推奨セキュリティコントロール（Recommended Security Control for Federal Information Systems)”に規定される内容に機能面で匹敵する商用セキュリティ慣行を受け入れる意向である。

CPU や記録装置などのリソースを仮想化したアーキテクチュアまたはソフトウェアであるバーチャルマシーン（VM）では、入札に参加する IT ベンダーは、時間当たり利用の最低限の価格で Windows および Linux 向けの CPU および OS を提供しなければならない。クラウド Web ホスティングでは、CPU および OS と、データベース、Web サーバー、e メールサービス、アプリケーションプラットフォームなどの関連ソフトウェアを提供することを求めている。加えて、サイバー・セキュリティに関しては、業務を請け追うコントラクタは、インフラをサポートし、消費者向けにバーチャルマシーン（VM）と IT リソースを提示するハードウェア、ネットワークおよびソフトウェアを準備し、セキュリティを保護し、モニタリングとメンテナンスを行う責任を有する。ホスティング環境の維持に使われるセキュリティでは、時間を短縮するために、“自己査定と自己文書（self-assess and self-document)”もコントラクタの責務となる。しかし、ゲスト OS やゲスト OS 上で動く追加ソフトウェアのセキュリティについては、消費者庁が責任を持つ。

クラウド・ストレージサービス、バーチャルマシーン（VM）およびクラウド Web ホスティングの 3 つの“IaaS サービス”に関する GSA の RFQ（見積要求書）では、公的部門で利活用するクラウド・コンピューティングの特定要件と 3 つの特定ニーズを具体的に記載している。

① クラウド・ストレージサービスの要求事項

サービス内容の記述	サービスのオプション	サービス属性	サービスユニット*
・このサービスは、拡張可能で、冗長性のあるダイナミック Web 基盤ストレージを提供する。 ・ユーザーに対しては、インターネットを介して遠隔操作でデータとファイルストレージを調達・利用する能力を提供する。 ・このサービスは、要求につきインターネットを介してダイナミックにオンデマンドでファイルとオブジェクトデータ能力を提供する。	**ファイルのストレージ**： インターネットを介してクラウド基盤内でコンピュータファイルを貯蔵、アクセスおよび修正できる能力。 **データオブジェクトのストレージ**： インターネットを介してクラウド基盤内でデータオブジェクトを貯蔵、アクセスおよび修正できる能力 **ストレージコマンド/リクエスト**： ストレージサービス（PUT、COPY、POST、LIST、GET、DELETE、HEAD など）におけるファイル/オブジェクトに関するコマンドを実行すること。	**ストレージスペース** オンライン、オンデマンドのバーチャルなファイル/オブジェクトストレージ（シングルサイズの上限は 5GB）	月間使用ストレージの容量（GB）
		データ転送帯域幅	月間の使用データ転送（In, Out）帯域幅（GB）

*サービス属性の購入可能な単位

② バーチャルマシーン（VM）の要求事項

サービス内容の記述	サービスオプション	サービス属性	サービスユニット
・このサービスは、拡張可能で、冗長性のあるダイナミックなコンピューティング能力またはバーチャルマシーン（VM）を提供する。 ・このサービスは、政府ユーザーに対して、インターネットを介して、コンピューティングサービ	**CPU（中央処理装置）**：CPU オプションの供給は次の通り。 ・最低でも 1.1Ghz の CPU 処理速度に匹敵するものを提供する。CPU 処理速度の追加オプションは、本要求書では必要としないが、	**RAM**：最低 1 ギガビットの RAM をサポートする VM インスタンスまたはコンピューティング用の RAM（Random Access Memory）	時間当たりの利用 月間の使用データ転送（In, Out）帯域幅（GB）

スまたはバーチャルマシーン（VM）インスタンス（クラスに属するオブジェクト）を調達・準備できるようにする。 ・このサービスは、ユーザーに対して、インターネットを介して、アプリケーションとデータをコンピューティングまたは VN インスタンスにロード（Load）できるようにする。 ・インターネットを介して Web ブラウザーにより、OS のコンフィギュレーションとマネジメントを可能にする。	提供してもよい。 ・CPU は、32 ビットおよび 64 ビットのオペレーションをサポートすること。 **オペレーティング・システム（OS）：** 最低でも、Windows と LINUX の OS をサポートすること。OS の追加オプションは、本要求書では必要としないが、提供またはサポートしてもよい。	**ディスクスペース**：最低 40GB をサポートするバーチャルマシーン（VM）用ディスクスペース。 **データ転送帯域幅**：インターネットを通じて、最低 400GB のデータ転送（In/Out）をサポートするプロバイダーのインフラのデータ転送に対応する帯域幅。	月間のデータ転送（In, Out）帯域幅（GB）

③クラウド Web ホスティングの要求事項

サービス内容の記述	サービスのオプション	サービス属性	サービスユニット
・クラウド WEB ホスティングは、拡張可能で、冗長性のあるダイナミック Web ホスティングサービスを可能にするクラウドにおける Web アプリケーションのホスティングサービスを提供する。 ・クラウド WEB ホスティングは、政府ユーザーに対して、インターネットを介して、クラウド WEB ホスティングを調達・準備できるようにする。 ・インターネットを介して Web ブラウザーにより、クラウド WEB ホスティングのコンフィギュレーションを可能にする。	**CPU（中央処理装置）**：CPU オプションの供給は次の通り。 ・最低でも 1.1Ghz の CPU 処理速度に匹敵するものを提供する。CPU 処理速度の追加オプションは、本要求書では必要としないが、提供してもよい。 ・CPU は、32 ビットおよび 64 ビットのオペレーションをサポートすること。 **オペレーティング・システム(OS)：** 最低でも、Windows と LINUX の OS をサポートすること。OS の追加オプションは、本要求書では必要としないが、提供またはサポートしてもよい。 **要求される Website ソフトウェア：** ・データベース（DB）インスタンス（MSSQL、MySQL、Oracle、	**ディスクスペース**：最低10GBのディスクスペース。	月当たりの GB のディスクスペース
		データ転送帯域幅：プロバイダーのインフラのデータ転送(In、Out)に使う帯域幅は、インターネットを通じて転送される最低 300GB のデータをサポートする	月当たりの GB の帯域幅（In、Out）

	MS アクセスまたは DB2） ・Web サーバソフトウェア（Apache、IIS） ・DNS（ドメインネームシステム） ・DNS Sec（DNS セキュリティ拡張） ・受託業者はその他の追加ソフトウェアを運用可能。	こと。 受託業者は、コンテント供給ネットワーク（CDN）能力をサポートする。	

1.5. 連邦政府によるクラウド構築事例

1.5.1. GSA（総合サービス管理局）の“Apps.gov”

2009年9月15日、連邦政府機関がクラウド・サービスを購入するためのAmazonやeBayなどと同様に、政府職員がクラウド・コンピューティングのソリューションを購入することができるオンラインの“ストアフロント（店頭）”とも呼ばれるWebサイトの“Apps.gov”を立ち上げたと発表。“Apps.gov”は、連邦省庁の職員がクラウド・コンピューティングサービスを購入することができるワンストップショッピングサイトである。

連邦CIOのビベック・クンドラ（Vivek Kundra）によると，“Apps.gov”は，ビジネス・アプリケーション、プロダクティビティ・アプリケーション、クラウドITサービス、ソーシャル・メディア・アプリケーションの4つのカテゴリーに分類され、連邦政府機関の職員が生産性や共同作業の向上、効率化を図るためのクラウド・サービスのアプリケーションをオンラインで簡単に閲覧して購入するためのワンストップ調達サイトである。

この発表の数時間後、Googleは、eメール、ワードプロセッサー、コラボレーション、Webサイト構築などの商用版Google.Appsを連邦政府および公的部門のニーズに対応した形にして2010年中に連邦政府、州政府および地方政府にクラウド・サービスを提供すると発表。ビベック・クンドラ（Vivek Kundra）連邦CIOも、政府クラウド・コンピューティング導入イニシアティブ前進に向けたGoogleのような産業界による積極的な参加を歓迎すると表明した。

オバマ政権は発足当時から、「透明性」、「参加」および「協調」の3つを政権運営、特に情報政策の柱に設定。この政策実現のために、約50に及ぶ連邦政府機関のうち、24省庁のCIOをメンバーとする連邦CIO会議（Federal CIO Council）をOMB（行政管理予算局）の下に設置し、全体の指揮官としてビベック・クンドラ（Vivek Kundra）を連邦CIOに任命した。24省庁以外も、多くの機関がリエゾンメンバとなっていることから、実質的にはすべての主要省庁をマネジメントする役割である。

クンドラ連邦CIOは、「連邦政府内クラウド」の最初のパイロット・システムとして、連邦政府の一般調達を担うGSA（一般サービス管理局）の調達業務の一部として政府クラウドを立ち上げ、それ求心力に横展開することを企図している。GSAはすでに政府クラウドの運用を開始し、連邦CIO会議（FCIOC）の下、「情報公開」を目的とする“Data.gov”や“IT Dashboard”を設置して、政府クラウド・サービスの展開に乗り出している。

表 2　政府クラウドに着手した政府機関

General Services Administration (GSA): **Apps.gov**
Federal Chief Information Officers Council (FCIOC): **Data.gov & IT Dashboard**
Defense Information Systems Agency (DISA): **Rapid Access Computing Environment (RACE)**
US Department of Energy (DOE): **Magellan**
Department of the Interior: **National Business Center (NBC) Cloud Computing**
NASA: Nebula

出所： http://federalcloudcomputing.wik.is/

1.5.2. GSA（総合サービス管理局）のクラウド・コンピューティング戦略

「クラウド・コンピューティング」による最初のプロジェクトとして連邦 CIO が進めているのが GSA（総合サービス管理局）の調達システムである。GSA は、「仮想化と統合」を目的として連邦 CCI(FCCI: Federal Cloud Computing Initiative)を立ち上げた。

FCCI(連邦クラウドコンピューティングイニシアティブ)には、イニシアティブには Cloud Computing Executive Steering Committee（ESC）と Cloud Computing Advisory Council（AC）があり、ESC が戦略を立案し、AC が計画を設計する。描き出された戦略目標は ITI の“統合（Consolidation）”と“仮想化（Virtualization）”である。

米国では、現在、e-Government の近代化として、Web サービスベースの環境整備を進めているが、これらをより迅速に展開し、更にはコスト削減を可能とする手段がクラウド化である。AC の計画では、クラウドを利用した ITI のビジョンを確立し、さらに 23 の省庁を対象に重複作業排除のための共通ソリューションの選定やコラボレーションを推進する。連邦クラウドコンピューティングイニシアティブ（FCCI）の議長は、連邦 GSA（総合サービス管理局）の CIO であるキャシー・コールマン（Casey Coleman）が就任し，DOE（エネルギー省）の CIO 補佐官である Carl Staton が副議長を務め、Advisory Board には、Federal Enterprise Architects（B. Niemann 等)が任命されている。

【GSA（総合サービス管理局）によるクラウド・コンピューティングの目標】

GSA のクラウド「Apps.gov」の全体のスケジュールは、次のようになっている。

- フェーズ1（Aug- Oct 2009）：Light-weight collaboration & productivity tools and basic infrastructure / platform：クラウド・タイプ：Commercially Available Public Clouds
- フェーズ2（Nov 2009 - Feb 2010）：Rich productivity tools, enhanced platform capabilities：クラウド・タイプ：Public and Outsourced Private Clouds
- フェーズ3（Mar - Jun 2010）：Enterprise Applications in the cloud and integration services：クラウド・タイプ：Private and Hybrid Clouds

【ITILOB】

GSA（総合サービス管理局）の調達システムは、既に、2009年9月にサービスを開始している。FCCI（連邦クラウドコンピューティングイニシアティブ）は、2008年9月に大統領令として発せられた“ITILOB：Information Technology Infrastructure Optimization Line of Business”に沿って、行政サービスの「Webサービス化」の展開を図る。

ITILOBの目標は、「信頼でき安全にサービスを提供できることで各機関の使命を遂行するために、最適化され、コスト効果的で、政府横断的な情報技術基盤を達成することである。FCCI（連邦クラウドコンピューティングイニシアティブ）は、NISTの「クラウド・コンピューティングの定義」と整合させながら、インフラストラクチャからSaaSベンダーまでを含む産業フレームワークに等しい枠組みを示している。このような枠組から、ニュービジネスの機会なども見えてくると共に、ベンダー間の棲み分けなどの議論が活発化するものと思われる。また、このようなフレームワークにより、セキュリティなどの扱いに関する差別化も可能となり、その実施が容易となる。

【クラウドStorefrontの公表】

2009年9月、オバマ政権は、GSA（総合サービス管理局）の最初のクラウド・コンピューティングをクラウド・ストアフロントである“Apps.gov”としてサービスを開始したと公表している。このオンラインストアは、連邦政府機関によるクラウド・コンピューティングサービスを効率的かつ効果的に調達できるものである。既述した通り、“Apps.gov”は、Apps.gov”は、連邦政府の職員がクラウド・コンピューティングのソリューションを購入することができるワンストップショッピングサイトである。

米国連邦政府の一般調達を担うGSA（総合サービス管理局）は2009年7月31日、IT調達スケジュールとして知られる“連邦供給計画（FSS-Federal Supply Schedule）Schedule 70”に基づいて、GSAが長期的な業務委託契約を結ぶITベンダーに対してIaaS（サービス

としてのインフラ）の 3 つの分野に関する RFQ（見積依頼書）を発表し、ベンダーに次のいずれかおよび/または全部の入札参加を要請した。このワークスコープは、GSA のクラウド・ストアフロントを構成する、①クラウド・ストレージサービス、②バーチャルマシーン（VM）、③クラウド Web ホスティングの 3 つの IaaS サービスである。この RFQ（見積依頼書）には、行政管理局（OMB）および GSA（総合サービス管理局）のクラウド・コンピューティングについての考え方が表現されている。

ビベック・クンドラ（Vivek Kundra）連邦 CIO は、「米国納税者に価値をもたらす」と表明し、また、「Apps.gov は組織を超えて政府の IT 資源を利用することを安価で容易にすることで、イノベーションを引き起こす」としている。因みに、クンドラ連邦 CIO は、2009 年 9 月 15 日付の「ホワイトハウスの Blog」で、自から“Apps.gov”の立ち上げをアナウンスしている。

クンドラは自身の Blog の中で、「連邦政府は IT に年間 750 億ドル（6.7 兆円）を支出しており、IT は連邦政府のあらゆる任務の遂行を支援する不可欠な要素である。最も革新的な最新技術にアクセスすることが重要であるにも拘わらず、連邦政府は IT に関して次のような課題を抱えている」としている。

- 新しい IT サービスや製品を上手く導入できない。
- 調達プロセスが複雑で時間がかかる。
- セキュリティ確保の手続きが複雑・高価・冗長で、しかも省庁間で重複している。
- 既存のポリシーが新技術の利用に対して不必要な制限になっている。

「Apps.gov」を通じて連邦政府におけるクラウド・コンピューティング利用を促進することで、これらの課題が解決に向かうことを期待している。「Apps.gov」から入手できる最初のクラウド・サービスはシンプルなものであり、このプログラムの潜在能力が完全に発揮されるまでには、まだ時間を要するというのが、クンドラの見解である。

この新しい“Apps.gov”サービスは、クラウド・コンピューティングサービスを購入するためのワンストップ・サービスで、IT 基盤の持続可能性と費用対効果の改善を通じて、クラウド・コンピューティングを、調達だけでなく、政策、安全、教育訓練、調整、アーキテクチャおよび標準化に拡大する政府方針のひとつであるとしている。

また、クラウドによるストアフロントの集中は、各政府機関の使命遂行を迅速かつ容易なものとしながら、クラウド・コンピューティングにより、政府機関ごとの、コンプライ

アンスやセキュリティ・プロセスの重複を排除し、複数の調達手続きに拡大することができるとしている。

“Apps.gov”は、IT サービスと基盤を、複数の顧客によって「共有可能」とし、物理的に異なる資源（ストレージ、プロセッシング、ネットワーク、仮想マシーンなど）を、顧客要望に沿って、動的に顧客に割り付け、貸出すものである。そのカテゴリーは、機能(CRM、データ管理、コミュニケーションなど）によって分類される。顧客としての政府機関は、プロダクトを識別し比較することが容易となり、購入が決定されると、GSA のオンラインショッピン・発注サイト「GSA Advantage」または、「eBay」を通じて購買できる。

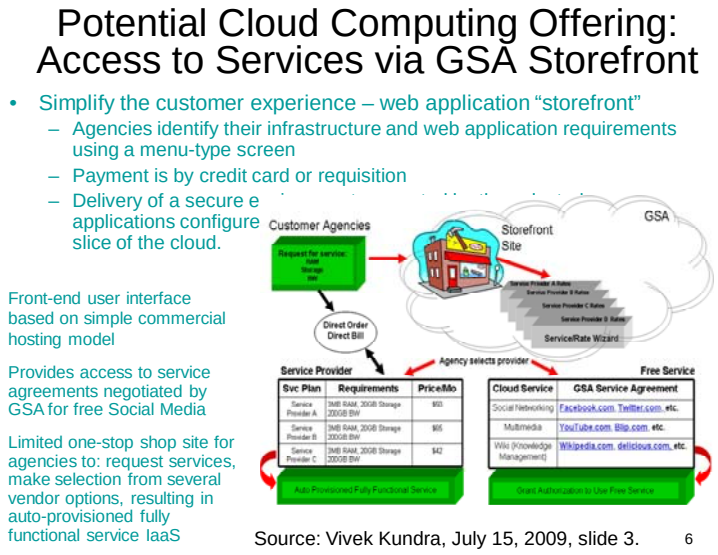
「従来の IT 調達環境では、市民に公開するまでの USA.gov の更新に 6 カ月を要していたが、クラウド環境では 1 日で可能となった。また、USA.gov の費用を年間 1.7M$(15 億円）節約できる」(GSA , Office of Citizen Services and Communications）としている。

“Apps.gov”は、政府機関において、フリーのソーシャル・メディア、Wiki や Blog など Web2.0 ツールを利用できるものである。連邦政府機関の FCCI と Apps.gov のソーシャル・メディア・ツール群は、各政府機関が市民や職員と容易に協業できるツールへアクセスできることを通じて、政府機関におけるイノベーションを促進するものとなるとしている。今日では、政府機関が、自分自身を SaaS ベンダーとして登録でき、将来は、IaaS（Infrastructure as a Service）のショーケースともなることも想定される。

【“Apps.gov” の Storefront の概要】

GSA の“Apps.gov”Storefront は、2009 年 9 月 15 日にサービスを開始した。その概念は、下図のクンドラ連邦 CIO のプレゼンテーションスライド（2009 年 7 月）に示されている。

図 12　“Apps.gov”Storefront 概念



このフェーズ 1 で提供されるサービスは、①Business Apps、②Productivity Apps、③Cloud IT Services、④Social Media Apps の 4 つの分野である。

- 「Business Apps」では、実証済みの商用アプリケーションサービスが価格と共に一覧できる。CRM の Salesforce も登録されている。
- 「Productivity Apps」では、テキスト編集、ワークフロー、プロジェクト管理、文書管理などオフィスで利用されるツール群を提供している。
- 「Cloud IT Services」は、外部パブリック利用にあたるものである。
- 「Social Media Apps」には、オープンソースの Blog ツール WordPress やドキュメント共有の Scribd、さらに Facebook や MySpace、 Flickr などもある。これらのアプリケーションの一部が SaaS サービスである。

これらの商用ツール（多くは無料）の掲載は、民間ベンダーの開発意欲を刺激し、「イノベーション」を引き起こすものとなると思われる。フェーズ 2（2009/11-2010/2）では、パブリック・クラウドだけでなく、プライベート・　クラウドの外部委託や SaaS アプリケーションなどの拡充を行う。

フェーズ 3（2010/3-6）からは一部、プライベート・クラウドの導入が始まり、連邦政府のクラウドはハイブリッドとなり、本格的なミッション・クリティカルなクラウド化が予定されている。

表 3　「Apps.gov」で利用できるツールおよびサービスの一覧

Matrix of Web 2.0 Technology and Government

Technology	Simple Definition	Examples	Opportunity/Potential in Government
Blogs	Journal or diary with social collaboration (comments)	33 federal agencies have public blogs, USA.gov government blog library, Webcontent.gov advice, GovGab.gov	Govt info to new audiences. Puts human face on govt using informal tone. Opens public conversations. Surface issues & solve them.
Wikis	Collaborative authoring & editing	GSA Collab Environment, Core.gov, MAX, NASA, US Courts, Intellipedia, PTO, Diplopedia, Peace Corps, Utah Politicopia	Workgroup or public collaboration for project management, knowledge sharing, public input. Contributions to 3rd party sites e.g. Wikipedia
Video Sharing (and Multimedia)	Videos, images, & audio libraries (YouTube, AOL Video, Yahoo Video, tubemogul, heyspread…)	USA.gov Multimedia library, NOAA & NASA YouTube, Coast Guard, CA &VA YouTube Channels, Americorps contest, Tobacco Free Florida contest	Public outreach, education, training, other communication for "connected" and on-line audiences. How To videos & audios to improve service and achieve mission.
Photo-Sharing	Photo libraries	USA.gov fed/state photo libraries, LoC & USGS galleries w Flickr API, EPA contest	Cost savings potential. New audiences. Awareness.
Podcasting	Multimedia content syndicated out for use on iPod TM, Mp3 players & computers	White House, NASA, USA.gov federal podcast library, Webcontent.gov, Peacecorps, Census daily podcasts	More ways to get message out. Build trust with conversational voice. Use for updates, live govt deliberations, emergencies, how-to messages
Virtual Worlds	Simulations of environments & people (Webkinz, Club Penguin, Neopets, Stardoll, Whyville, Second Life, Active Worlds, Kaneva, Proto Sphere, Entropia Universe, uWorld)	NASA, NOAA, CDC in SL & Whyville, VA, Natl Guard, Energy, DoD, National Defense Univ Federal Consortium for Virtual Worlds, Real Life Govt in 2nd Life Google group	Public outreach & other communication for kids and niche Internet audiences. Virtual Town Halls, Education, Training. Ability to bring people together worldwide for meetings, lectures, etc.
Social Networking Sites	Connecting people globally	EPA Facebook group, NASA Colab, USAgov Facebook page, MySpace, Linkedin	Intranet use to cross internal stovepipes. Cross government coordination. Public communities. Viral impact. Knowledge mgmt. Recruitment. Event announcements.
Syndicated Web Feeds	Automated notifications of frequently updated content (think RSS)	USA.gov Federal RSS Library, NOAA Watch	Do more with RSS, XML/Web feeds. Expand reach. Pull content together across government. Authoritative source. Reduce duplication.
Mashups	Combine content from multiple sources for an integrated experience	USA Search, USGS, NASA, EPA, Virtual Earth, Google Earth, Google maps	Lots of potential. Improved govt reach, service, usefulness, and functionality. Integrate external data. Get licenses, stay vendor neutral. Make content available to others who create mashups
Widgets, Gadgets, Pipes	Small applications & code in Web pages or for desktop use	FBI widgets, Veterans Affairs, Census Population Clock & NASA Planet Discoveries Desktop widgets	Increase awareness, use, and usefulness of gov sites, information, and service. Bring content to the user's home page (iGoogle, netvibes, etc)
Social Bookmark & News (Sharing, Tagging) Sites	Ways of sharing content with others	USA.gov, NASA, Govt blogs, Digg, Delicious Technorati, AddThis	Increase the popularity and use of gov pages, information, and services. Viral marketing.
Micro-blogging. Presence Networks.	Form of blogging which allows brief (Instant Message size) text updates.	Twitter, Jaiku, Cromple, Pownce, NASA Edge, USA.gov, GovGab, Univ of Mich	Seek input. Broadcast msgs: emergencies, news, announcemts. Real time reportg. Recruitg.

July 18, 2008　Bev Godwin, USA.gov and Web Best Practices, GSA Office of Citizen Services

【GSA による政府調達方針】

クンドラ連邦 CIO が、最初の政府クラウド・パイロットとして GSA（総合サービス管理局）の調達業務を選んだことは、2009 年 4 月、ホワイトハウスが示した「政府調達契約（Government Contracting）」に関する各省庁向け Memorandum に示された現状を踏まえたものといえる。この「政府調達契約」に関する覚書によると、連邦政府の調達費用は、2008 年には対 2001 年比で 2 倍を超える約 5,000 億ドルに達しており、完全かつオープンな競争のないコスト補償契約が同期間に倍増している現状に鑑みて、オバマ政権は、よりよい調達慣行を通じて年間 400 億ドルのコスト節減を目指して、次の連邦政府の調達方針を掲げている。

① 単独供給契約（Sole-sourcing contracts）を排除すると同時に定額契約を推奨し、コスト補償契約（Cost-reimbursement contracts）は定額契約が不適切な環境でのみ利用する。

② 納税者から預かった資金を賢く利用するために契約プロセスを一貫して管理・監督できる十分な能力を備える。
③ 本質的に政府が遂行すべき業務は省庁自身によって遂行され、アウトソースされないことを保証する。

これを受けて、オバマ大統領は、OMB（行政管理予算局）に対して、これらの方針を遵守するための政府全体規模のガイダンスを作成するよう指示した。OMB は 2009 年 7 月、各省庁のトップに向けた 3 つの覚書を発行している。

第 1 の覚書は、官民の人員管理に関するものである。この覚書では、行政サービスの提供に必要となる連邦政府職員と民間業者それぞれの適切な役目を認識し、最適な官民人員管理を実現するために、OMB が提供する官民人員計画・管理の枠組みを適用すること、官民人員管理に関するパイロット・プログラムを実施すること、そして“インソーシング”する場合は OMB と DOD が設定した基準に沿ったガイドラインを作成するよう省庁に要求している。

第 2 の覚書は、既存の契約や調達慣行を見直し、2011 年度末までに基準契約支出額の 7%を節約するための計画を立てることと、2010 年度におけるハイリスク契約（コスト償還契約など）への資金を 10%以上削減することを省庁トップに要求するものとなっている。

第 3 の覚書は、契約業者の過去の業績に関する情報をより多く入手・共有するために、契約業者の作業に関する評価を“実績情報検索システム（PPIRS:Past Performance Information Retrieval System)”に保存することを各省庁に求めている。これによって各省庁は、類似の作業を同じ業者に発注することを考慮する際に、そのデータベースを参照して業者の能力を判断できるようになる。

なお、GSA のサイトでは、政府調達における全ライフサイクルをサポートする「統合調達環境（Integrate Acquisition Environment ）が提供され、書式からツールまでの詳細が示されている。

【“USA.gov”】

GSA（総合サービス管理局）は、政府機関を代表して、一般市民向けの政府機関の情報提供、あるいは市民と対話する Web サイトとして“USA.gov”を運営している。連邦政府の公式な Website である“USA.gov”は、米国民が容易に政府情報を入手することを目的として構築されたもので、米国型電子政府のキャタリスト（触媒役）機能を果たすものである。

“USA.gov”の担当部署は、GSA 内のサービス対話室（Office of Citizen Services and Communications）である。国防省（DOD）の補助金を受けて研究開発（R&D）プロジェクトを担った起業家の Eric Brewer が開発した強力な検索エンジンを連邦政府に寄贈したことが契機となって、連邦政府は“USA.gov”を構築することができた。この検索エンジンをベースに、クリントン政権は 2000 年 9 月 22 日、“FirstGov.gov”のサイトを立ち上げ、2007 年 1 月に“USA.gov”へと名称変更している。

【“USASpnding.gov”と“IT Dashboard”】

従来、ブッシュ政権まで、米国連邦政府の IT 基盤や情報の「共有」や「公開」については、各省庁間の壁が厚く、ホワイトハウスが度々、提示してきた FEA（フェデラル・エンタープライズ・アーキテクチャ）や DRM（連邦政府データ管理参照モデル）、あるいは「情報公開法（FOIA）,1966」も容易に成果を示さなかった。

政府委託事業ではデータは連邦調達規則にしたがい、残らず一旦政府に納品され政府情報となる。政府内部で作られたもしくは納品された政府情報は「情報公開法(FIOA)」により速やかに無制限に市民に提供される。しかも、「OMB-circular A-130」によって、特に「付価値生産物」を作成可能な原材料としての配布を強く奨励している。

情報企業や大学はユニークなアイデアと少ないコストでこの「生データ」に対して様々な発見努力や付加価値競争（個人プロジェクト）を行い、結果として豊富な知財が生み出されエンドユーザーは多様な商品、情報、サービスから好みのものを適正な価格で手にいれることができる。「国家プロジェクト」由来の知財は全く認められない一方公共データを用いた「個人プロジェクト」では政府研究助成金（NFS や NIH からの grant）を利用していても、バイドール法によって知財が保護されるために一層発見開発は活気を帯び科学の進歩とともに産業化が保障されている。すなわち、国家プロジェクトは Public Good（公共財）として「生データ」を提供し、市民が平等に付加価値競争や発見競争を行う、 オバマ政権は、「オープンな政府（Open Government）」を政権運営方針として「透明性」を強調している。そのための「行政情報の公開」に極めて積極的であり、その「行政情報」の活用を通じた官民共同による「イノベーション」を期している。クンドラ連邦 CIO は、就任演説時に、「Recovery.gov」の Web ページを示しながら、「真の透明性とは」、「もし、データが民主化されたとき、データがパブリックドメインにおかれたとき、イノベーションの爆発をみるだろう」と発言している。

「Recovery.gov」は、ARRA による政府資金の使途を明らかにするものである。これと同様に、米国政府の資金を受けるもの全てについて、その情報を公開すべきであるとして、FCIOC が政府情報の公開を目的として立ち上げた「クラウド」が次の 2 つである。

① IT Dashboard-USASpending.Gov
② Data.gov

これらの「クラウド」を省庁間の横断的情報共有のための共通プラットフォームとして位置づけ、2010 年度には 33 百万ドル（約 30 億円）を予算計上し、議会承認をうけている。

【IT Dashboard-USASpending.Gov】

ホワイトハウスの連邦 CIO 会議（FCIOC）のもとで立ち上げた行政情報公開サイトの“USASpending.gov”は、「連邦政府資金の説明責任と透明性に関する法律-2006（Transparency Act)」が、米国政府から 25,000 ドル以上の補助金を受けた者に、それぞれの補助金（裁定額）ごとに、「単独で、サーチ可能な Web サイト」によって、次の事項を明らかにすることを求めていることに由来する。

- 支援の名称と支援の対象
- 支援の金額
- 資金提供機関と取引タイプ
- 支援を受けた実体の所在・場所
- 支援ごとに付与されるユニークな識別子

“USAspending.gov”は、OMB をウオッチするため 2007 年 9 月に立ち上がった Web サイトの“「fedspend.org”を 2009 年 10 月から引き継いだサイトである。そのデータの多くは、連邦調達データシステム（FPDS）の契約に関するデータと、連邦補助金データシステム（Federal Assistance Award Data System）の補助金に関するデータを源泉としている。

“IT Dashboard”は、“USASpending.gov”の一部であって、予算執行状況をカラーでビジブルなグラフで表示でき、長期的な傾向を分析するためのツールも用意されている。これにより、補助金を受けているプロジェクトの状況を可視化できるだけでなく、このような膨大なパブリック・データを利用できることが、経済分析、社会動向分析、政策効果測定、など高いインテリジェンスをもつ情報処理技術開発の喚起を促すことが期待される。すでに、「IT Dashboard」では、プロジェクト評価を次のような観点で行うことができる。

- 政府機関によって設定されたフィルターを用いるもの
- 全般的な評価（色別に表示）
- コストによる評価
- スケジュールによる評価
- CIO による評価

さらに、RSS フィードを用いて、同じ情報を他人と共有し、自分の Web サイトにリンクする「共有機能」も用意されている。また、そのフィードもカストマイズできる。Facebook、Twitter などのソーシャル・メディアとの融合は、新しい生活者のコミュニティ形成を通じて、さらに情報技術のイノベーションを生み出すものと期待される。

【“Data.gov”】

同じく、オバマ政権の「政権透明性」を確保するための「情報公開」サイトとして、2009 年 5 月から、連邦 CIO 会議（FCIOC)の下で、“Data.gov”がサービスを開始している。GSA（総合サービス管理局）がサイト運営に当たっている。

前述の通り、“USASpending.gov”は、政府補助金の使途をプロジェクトの状況を可視化できるものであり、“Rcovery.gov”は ARRA（米国国家再生再投資法）による支出を追跡するために提供されたサイトである。

これに対して、“Data.gov”は広く、補助金や政府支出以外に、連邦政府が作成したパブリック・データを公開・共有・活用することを通じたイノベーションの誘発を目的とするものでる。

「パブリック・データ」に関する“Data.gov”の方針は次の通りである。

- “Data.gov”によってアクセス可能なデータセットは、パブリック情報に限定され、法令または権威者によって指定された国家安全保障情報、また法令、慣習、法例によって保護されるデータに限定する。データや情報を提供する政府の省や局は、公共からの情報開示要求について絶えず配慮しなければならない。」（同サイトより）。

多様な「データ・カタログ」を、ユーザーの活用とその経験フィードバック、ユーザー要望にしたがって成長させる構想である。現在のところ、そのデータ検索キーは「カテゴ

リー名」によるものと、「政府機関名」によるものであるが、利用できるデータは限られているようだ。地理情報などは利用イメージが得やすい情報であるが、もともと「公開」を義務づけていない政府情報を公開させるには無理があるという声もある。

しかし、クンドラ連邦 CIO は 2009 年 5 月、「2009 年末までに、行政データセット 500、地理データセット 1,000、を目標とする」と指示した。2009 年末の登録データは、この目標をほぼ実現している。

【概念構想】

“Data.gov”は、2009 年 12 月に Data.gov の普及促進と将来構想示したガイドラインである“Data.gov Concept of Operations”の草案を連邦 CIO 会議（FCIO）名で示している。このガイドラインは、2009 年 5 月の発足時に、120 日後（2010 年 1 月）を目標に作成されていたものである。EPA の Brand Niemann はその推進者のひとりである。その構想は、DOD の DISA/RACE および Forge.mil の構想や GSA の Storefront などと大きな違いはない。その特徴的な部分を以下に紹介する。

【ガイドラインからみる Data.gov の将来像】

① Data.gov の原則

- アクセス（利用）に着目（Focus on Access）：Data.gov は、政府データを、可能な限り信頼できる情報源とするために設計された。その目標は、イノベーティブなアプリケーション（可視化、マッシュアップなど）と第 3 者による分析などを通じて、「透明性」「協調」「参画」を強化しながら、「政府機関の民主化」を促進することにある。
- オープンプラットフォーム（Open Platform）：Data.gov は、行政機関とサードパーティがサービスを共有できるように API（application programming interfaces）モジュール化アプローチを採用する。そのアーキテクチャ、API およびサービスは、行政機関と公共的なインプットによって進化する。
- 生データ（Disaggregation of Data）：政府機関からの報告としてのデータは、可視化やツールのために集約されてはならない（生データ）。
- ユーザフィードバックによる成長と進化（Grow and Improve through User Feedback）：高い価値をもつデータセットを明らかにするためにユーザーからフィードバックを利用しなければならない。そのフィードバックは、データセットの優先度づけやデータとアプリケーションの配布と便宜性を改善するために利用されるべきである。

- プログラムの責任：政府機関のデータ管理者（data stewards）とプログラム管理者は、情報の品質、提供するデータの内容、およびプライバシーと情報セキュリティに責任をもつ。また、機関はデータと情報の効率的な管理、共有ポリシー、連邦政府のポリシーとの整合性確保にも責任を持つ。
- 迅速な統合（Rapid Integration）：政府機関は最新のデータを Data.gov に、十分な文書化と共に統合しなくてはならない。
- ベストプラクティスの促進（Embrace, Scale and Drive Best Practices：Data.gov は、わが国の州、ローカル、および地域を横断的する、データと情報管理、政府機関相互の情報配布と共有のベストプラクティスの実施、強化、普及を図る。

② 運営体制：“Data.gov”は、そのホスティングを GSA が担当しているようであるが、その内容（データ）の収集や管理に関する役割を次のようにしている。（2010 年度以降、NASA の Nebula がそのホスティングを行うようである（2009 年 12 月）。

- 各政府機関の役割：各政府機関は、当該機関の CIO によって任命されたデータ管理者（data stewards）とコンタクト（POC：Pont of Contact)によってデータを生成する。POC は Data.Gov の PMO（Program Management Office ）と緊密な連絡を取る。POC に関しては、各機関の CIO の役割と共に、詳細な役割が述べられているが、ここでは省略する。
- シニア・アドバイザリー・グループ（Senior Advisory Group）：次のような機関による助言グループである。
  - 連邦 CIO 会議（FCIOC）
  - The Interagency Council on Statistical Policy (ICSP),
  - The Federal Geographic Data Committee (FGDC),
  - The Commerce, Energy, NASA, and Defense Information Managers Group (CENDI),
  - The Interagency Working Group on Digital Data (IWGDD),
  - The Networking and Information Technology Research and Development (NITRD) Program,
- 専門分野エキスパート・テクニカル・ワーキング・グループ（SME）：分野別の専門家のグループ。
- Federal Communities of Interest/Information Portals Science.gov や Fedstats.gov など有用な情報をもつ省庁間連コミュニティ
- 州、群、地域の機関

③ 他の省庁 Web サイトとの連携：“Data.gov“は、次のような政府 Web サイトを源泉と

しながら連携する：USA.gov, Federal IT Dashboard, USASearch.gov, FBO.gov, USAspending.gov, Geospatial One Stop, FedStats, および Grants.gov。これらのサイトのデータ構造は、全て Data.gov に登録される。さらに、Data.gov は NASCIO（National Association of State CIOs）など、他の機関と連携して、この「概念とオペレーション」を共有するように作業を行う。また、Data.gov の PMO たちは、この概念が広く国際的にも通用することを願っている。

【セマンティック Web との連携】

2005 年 12 月 16 日に発行された OMB の覚書（M-06-02）には、「特定なグループのデータの交換、配布には公式な情報モデルを必要とする」としている。また、OMB の覚書 M-06-02 は、「公式情報モデルは、システム間の情報交換を可能とする」と述べている。よい例として、OMB の「Office of Information and Regulatory Affair's」がある。また、公的統計のための標準として、Metropolitan Statistical Areas (MSA)や North American Industry Classification System (NAICS)を挙げることができる。

各政府機関は、このようなカテゴリーに関するデータ規格により、クロス・ドメイン（業界横断）分析を可能となる。例えば、ある開発者が、「従業員別の収益ランク」をいくつかのサイトからマッシュアップし可視化したいとき、ある機関が業界の収益を入力し、別な機関がその業界の従業員について入力した結果を、互いに NAICS のような分類に従って登録すれば、そのような分析が可能となる。

そのようなデータに関する「意味的調和」と業界横断のユニーク識別カテゴリーにより、異なる複数のデータ源は、適切に統合され、新しい観点からの分析を可能とする。
政府は、既に、政府データの発見や理解のために、いくつかの「業界横断データ・モデル」をもっている。例えば、NIEM (National Information Exchange Model) と Universal Core (UCore) は、複数の政府機関の情報共有を進めるデータ・モデルである。

NIEM は、National Association of State Chief Information Officers によってサポートされており、RDF の原則に従っており、OWL (Web Ontology Language) による表現も可能としている。

US 軍部は、UCore- UCore-Semantic Layer (SL)で、設問(who, what, when, and where). を OWL で表現できる。これらは、強力なタグとモデリング機構により政府データの発見と共有を進める初期の事例にすぎない。今日の「産業ベストプラクティス」は、一般大衆が直接アクセスできる「セマンティック Web」を可能とするセマンティック技術を発展させた

ものとなっている。OMB の覚書にしたがって、Data.gov は、データセットにマンティック相互運用を可能とする「形式的情報モデル」を適用することになる。

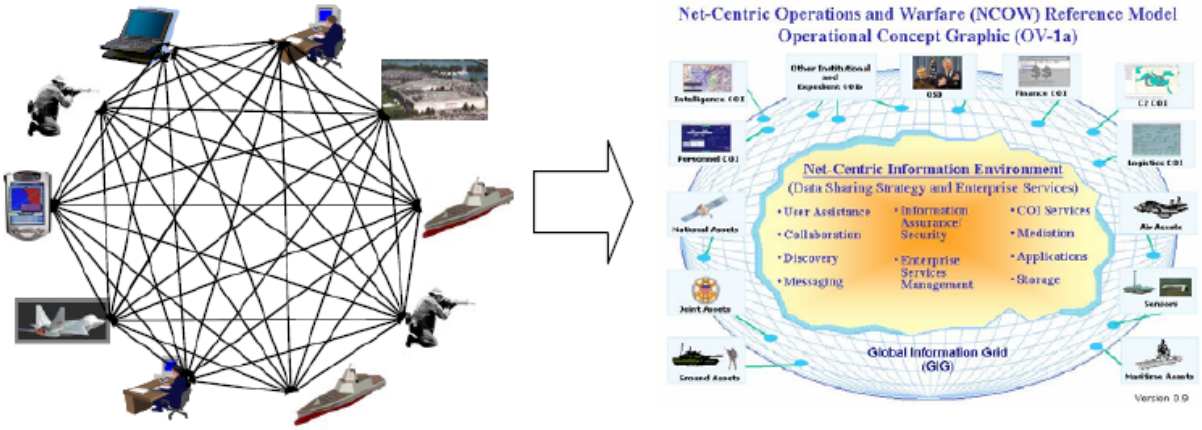
1.5.3. DOD の Net-Centric 戦略と DISA/ RACE

DOD（国防省）の DISA（国防情報システム局）は、2003 年 8 月、当時のラムズフェルド国防長官による「システム中心の工業時代（System-centric Industrial Age）からネット中心の情報時代（Net-centric Information Age）への移行」という宣言を受け、「ネットセントリック戦略」の策定・実行を推し進めてきている。

「ネットセントリック戦略」は、1990 年代から C4ISR(Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance)、または C4I（Command, Control, Communications, Computers, Intelligence）として進められてきた構想を発展させたもので、軍・官・民の多様なステークホルダー間の連携のためのネットワーク基盤（GIG：Global Information Grid）を基に、「ネットセントリック環境」を構築してきた。その環境により、800 万人のユーザーに対して、1,700 におよぶアプリケーションをサービス提供している。

このネットセントリック環境（GIG）は、すでに「クラウド」のインフラストラクチャとも呼べるものとなっている（下図参照）。

図 13　ネットセントリック環境の概念



http://jitc.fhu.disa.mil/iop_conf/2007/downloads/jt_staff_nr_kpp_unclas.pdf より

1.5.4. DISA（国防情報システム局）の RACE

DISA（国防情報システム局）の RACE（Rapid Access Computing Environment）は、70 万人におよぶ DOD（国防省）の職員および SIAC、MITER など関連企業の職員などを対象に、400 万人に及ぶユーザー対して、高度なセキュリティを維持する安全な環境の中で、24 時間稼働する「セルフサービスのソフトウェア開発環境」としての「プライベート・クラウド」である。現在のところ、「政府発行のクレジットカード」か「軍発行の ID カード（Military Interdepartmental Purchase Request（MIPR））」の所有者に限定されている。

DISA（国防情報システム局）がクラウド導入を宣言した背景には、LAMP（Linux, ApacheHTTPServier, MySQL, PHP, Python, Perl）と呼ばれる、オープンソースのソフトウェアの存在があった。つまり、自前の技術に縛られず、市場の最新技術を取込むことが狙いと言える。DISA はもともと、2 年ほど前から「On Demand Computing Service」を立ち上げ、コンピューティングとストレージ容量を利用した分だけ課金するモデルを導入していた。このサービス提供では、DISA の「Defense Enterprise Computing Center」を通じてやり取りする必要があり、最終的に必要なプラットフォームを得るまでに何十日もかかる場合もあった。それを数時間以内に提供（Provisioning）できるサイトして RACE（Rapid Access Computing Environment）としたものである。

RACE 構築の公表は 2008 年 10 月、DISA（国防情報システム局）の CTO によってなされている。DISA（国防情報システム局）は、連邦政府機関の中で最も早い時期に「クラウド宣言」を行ったことになり、サービスも 2009 年 4 月に開始されている。つまり、クンドラ連邦 CIO のクラウド宣言よりもかなり早い時期に議論と準備を進めてきていたことになる[1]。

DISA の The Technical Program Director for DISA's Computing Services Directorate である Harry Sienkiewicz 氏の、2009 年 9 月のプレゼンテーションスライドと講演のビデオが Podcast で参照できる[2]。DISA は、RACE を PaaS または IaaS と位置付け、Forge.mil を SaaS として提供するとしている。

DISA（国防情報システム局）は 2009 年 4 月、軍関係の開発者が「特殊エリア」を設ける

---

[1] 今回の調査では、DISA に属する個人(Jerry Smith 氏）の好意に基づくサポートは受けたが、公式には、「DISA にはクラウド・コンピューティングの専門家はいない」という理由で訪問できなかった。国防上、極めて高い機密性を求められる DOD には、DISA が「クラウド」を構築することへの反対も多かったと聞いている（J. Smith、および B. Niemann（EPA）談）。

[2] 本調査メンバーの一人が、2009 年 4 月に「ネットセントリック戦略」を調査するために DISA を訪問した時は快く受け入れてくれた。しかし、その訪問時、「クラウドへの取り組み」について質問した時、それまで和やかだったミーティングの場が、一瞬、その場が氷いたようになり「慎重に検討中である」という回答があっただけであったことが思い出される。

ことなしに、ソフトウェアのテストと配布展開を、自らの手で容易に実現できる開発環境を、DISA/RACE（Rapid Access Computing Environment）として発表した。「クラウド･コンピューティング」環境のように振舞う、独自のデータセンター構築へ向けて動き出した。

DISA（国防情報システム局）は、新しいコンピューティング･パワーを提供する際に、これまでの制約であった官僚主義を排除し、最終的には軍関係のディベロッパーがソフトウェアのテストとディプロイを自ら行うための、開発とテストのためのツールについて発表。「インターネット上には信じられないほどの拡張された機能があるが、セキュリティと安定性の要件のために、我々は使うことができない。しかし。Amazon と Google が示している可能性を、あるがままに享受したい。そして DOD テクノロジーの素早い革新を実現するために、我々の資産を次のレベルに移行させたい」と、Forge.mil プロジェクトのディレクターである Rob Vietmeyer はインタビューで答えている。

DOD（国防省）における重要な IT 機関としての DISA（国防情報システム局）は、最終的には軍事のためのプライベート･クラウドになっていく“RACE（Rapid Access Computing Environment)”を構築するために、1 年以上の時間を費やしてきた。あらゆる種類の実運用ソフトウェアをホストするために、軍において RACE が使われることを想定している。

しかし、DISA が DOD において、その有用性を高めるため採用したい方式のひとつは、“Forge.mil”から提供される、「SoftwareForge」と呼ばれるソフトウェア開発のためのコラボレーション･ツールとリポジトリを介してとなる。現時点では達成されていないが、Forge.mil は最終的に Forge.mil サイトから、さらには、Eclipse のように開発環境からさえ、RACE 上の新しいソフトウェアとサービスの、自身による迅速なテストとディプロイメントを実現するだろう。それを可能にするための、ひとつの支援テクノロジーになると思われるのが、「CollabNet 」から提供され、Lab Management と呼ばれる、アプリケーション･ライフサイクル管理ソフトウェアの最新バージョンである。

- 「Forge.mil」は、DOD（国防省）の技術開発コミュニティをサポートするサービスの集合である。最近では、オープンソースと DOD コミュニティ・ソース・ソフトウェアによる共同開発を可能としている。ソフトウェアの全ライフサイクルをサポートし、ステークホルダーと開発者、テスト者、認証者、オペレータおよびユーザーの共同作業を支援するものとなる。Forge.mil は、「ネットセントリック作戦」や「戦闘行為」を支援するためにソフトウェアやシステムの開発を迅速に実施できるように、DISA 主導でデザインされたものである。

「Forge.mil」は、「オープンソース･ソフトウェア･リポジトリ」として、一般に人気が

ある「SourceForge」から刺激を受けている。その目標は、ソフトウェアとサービスの、開発、テスト、実装、ディプロイメントを、DoDが容易かつ迅速に進めることである。運用を開始した「SoftwareForge」は、機密とは切り離された領域において、「CollabNet」から提供されるコラボレーション開発ツールに基づき開発を促進する。それは、ソフトウェア・リポジトリとコラボレーションのためのサイトであり、バージョン・コントロールや、問題追跡、Wiki、ディスカッション・フォーラム、ドキュメント・リポジトリなどを取り込んでいる。

「SoftwareForge」は、オープンソースあるいは「DoD コミュニティ・ソース」を必要とし、ロケーションにかかわらず軍の出先を横断するかたちで、コラボレーションとコードの再利用を奨励するための、モジュール式のソフトウェア開発を促進する。したがって、それらの開発テクニックと分散インフラストラクチャを組み合わせることにより、きわめて容易なソフトウェアの分散開発を実現できる。このサイトは、登録された1,300人のDoDディベロッパーに素早く採用され、3 ヶ月のベータ・テスト期間において 60 種類の開発項目に取り組んでいる。そこには、無人探索機のための、システム・ユーティリティや埋め込みシステムなどが含まれる。

次には、「ProjectForge」 と呼ばれる、機密性の高い専用のコードに対応するものが控えている。そして、自動化とリポジトリを介した、「TestForge」 と 「CertificationForge」と呼ばれる領域があり、Forge.mil 上で開発されたソフトウェアのテストと証明により、DoD 仕様が求めるレベルに一致させていく。このテスト環境が仕上がった後に、DISA はエージェンシーおよびベンダーと進めている、パートナーシップを推進していく。そして、実運用ソフトウェアのための、完全にセルフ・サービス化されたディプロイメント環境へと、2010年の夏までに進みたいと望んでいる。 さらに Forge.mil は、Air Force、Navy、Armyと進めている「プライベート・クラウド」に、新しい展開を見いだすかもしれない。

“RACE (Rapid Access Computing Environment)”は、Amazon方式のソフトウェア開発とディプロイメントを採用しないだろう。すでに、RightNow の CRM ソフトウェアのインスタンスが稼動しているが、仮想デスクトップを提供していく可能性に、DISA は注目している。RACEのプログラム・ディレクターであるHarry Sienkiewiczは、ひとつの手段として、DISAが存在するように、彼のチームをDODにおけるホスティング会社やサービス・プロバイダーのようなものと見なしている。「我々は Rackspace や 1&1 に、とても似た機能を持っている。そして、ユーザーが必要とする方式で、いつでも、どこでも、彼らの環境を供給していく。我々は舞台裏にいて、ISP やホスターのような存在でありたいと思う」とインタビューに答えている。

DISA（国防情報システム局）は既に承認済みの Windows Server と Red Hat Enterprise Linux application を、Exchange Server や Apache Web Server のように、セルフ･サービスで供給することを許可している。いま直ぐに、アプリケーションがオンラインされることは無いだろうが、Common Access Card（軍の身元確認と認証形式）を持ち、政府発行のクレジットカードを持っているなら、コンピューティング･リソースを購入し、オンラインで決済できる。 「このタイプの環境と、サーバーと、セキュリティと言うだけで、このポータルに入ることができる」と Sienkiewicz は言う。

しかし、RACE のレンタル･スペースに対する支払い方式は、Amazon Web Services ほど、きめ細かくない。そして、このプライベート･クラウドはマルチ･テナント化されていないが、さらにテクノロジーが改善されるなら、その方向へ向けて DISA が動く可能性もある。

RACE ディベロッパーは、トラフィックと、ストレージと、CPU の利用に対して別々に支払う代わりに、1GB メモリと 50 GB ストレージを取り込んだ仮想マシーンに対して、500 ドルを月ごとに支払う。 それに加えて、イメージごとのストレージが、5 月～6 月までに利用可能になるだろう。そして DISA は、オンラインで Amazon などが行っているように、さらにコストを考慮した方式に注目している。

直ちにプロビジョニング（利用可能にすること）することは、不可能である。いくつかのケースにおいて、RACE は 24 時間以内で、コンピューティング･リソースの供給を実現している。しかし、まったく新規のソフトウェアの場合には、一般的なリクエストに対して 14 日～30 日を要する。 結局のところ、システムが自動的にアプリケーションを証明するようになるにつれて、そのタイムラグは大幅に短縮された。「認証と承認は、テントを立てるための、最も長いポールのようなものである」と Sienkiewicz は言う。正にいま、DISA は「安全性と適合性を備えたシステム･イメージ」をユーザーに提供し、パッチ･リポジトリへのアクセスを彼らに与えているが、それと同時に、ユーザー自身がセキュリティを管理するように要求している。

DISA（国防情報システム局）における構築の次のフェーズの一部として、一連の標準プラクティスに対してセキュリティを立証し、普及率についてテストをするための、何らかのサービスを提供されるだろう。そのためのシステムは、安定性のために構築される。つまり、RACE のデータセンター環境は、ブレードとラックのレベルにおいて、バックアップ、多重冷却、セキュリティ設備、マルチ･ネットワーク･パス、マルチ･ロードバランス DMZ、多重電源などを取り込むことになる。

“RACE (Rapid Access Computing Environment)”は、数多くのベンダーからの支援によ

り成り立っている。そして、その中でも Hewlett-Packard (ProLiant ブレード、HP Service Manager、HP Operations Orchestration) と VMware が主力となっている。 そのほかにも、IBM、Sun、Moab (リソース・ワークフローとスケジューリング)、Vion (ストレージ・サービス) などが含まれる。 とりわけ、Sienkiewicz は VMware のアイデアが V-Cloud イニシアティブの一部として、提起されることに興味を持っているが、DISA が V-Cloud の顧客になることについては、何も発言できないとしている。

DISA のプログラムは、「クラウド・コンピューティング」のリーダーたちの興味を引き付けた。VMware の CEO である Paul Maritz は、今月の始めに DISA のオフィスで、RACE について発言した。そして、Amazon CTO である Werner Vogels と、 Salesforce.com の CEO である Marc Benioff は、今週に開催された DISA のパートナー・カンファレンスでキーノートを担当した。現状で提供されているのは開発・試験用の環境のみだが、セキュリティなどの課題に慎重に対応しつつ、最終的には実利用環境に拡大することも計画されている。

ただし、DISA の CIO である John Garing 氏は、「現在のところ RACE は DISA 内にある独自のクラウド、すなわち「プライベート・クラウド」として構築されており、Google や Amazon などのパブリック・クラウドプロバイダからリソースを調達することは、すぐには起こりそうにない。つまり、セキュリティ確保のためには、データがどこで処理されているか分からない「パブリック・クラウド」を受け入れる段階には至っていない」と述べている。

1.5.5. DOD の“ソーシャル・メディア”

安全保障上、最高の機密性をもつべき DOD において、DISA の「クラウド化」は誰しも「慎重になるべき」と考えたものと言える。一方で、250 万人の軍人を抱える DOD としては、人間としての兵士の「人生の質 (QOL)」を考えざるを得ず、Facebook や Twitter など「ソーシャル・ネットワーキング」をどのように取り込むべきか議論が続いているようである。その議論の経過は、以下のようなものである。

2009 年 9 月末時点で、DOD の「ソーシャル・ネットワーキング」の「便益・リスク」に関する議論は今月中 (2009 年 10 月) に終わるだろうとしている。あるスポークスマンは、Facebook や Twitter などの「ソーシャル・ネットワーキング・ツール」利用の損得による「バランス・アプローチ」がとられるであろうとしている。それらのツールの利用を制限つきで許す方針は、何らかの成果をもたらすであろうとしている。「バランス・アプローチ」は禁止しても有効でない点で、賢いとしている。

Amit Yoran（chief executive officer of NetWitness and the former director of the U.S. Computer Emergency Readiness Team and National Cybersecurity Division of the Homeland Security Department.）は、DOD 内部で「完全に禁止することは不毛なこと」としている。また、「ソーシャル・メディア側も賢くなって、どんな制約も乗り越える道を探るに決まっている」としている。

Grant McLaughlin（principal at Booz Allen Hamilton）は、DOD ほか政府機関の次のステップは、「新しい技術をどのように利用すべきか」を識別することとしている。「我々は、それが玩具である内から、それに正しく移行することが重要だ、そしてそれをうまく利用することだ」としている。また、「既に、それらの技術の可能性を信じる人がクリチカル・マスを超えたときに来ている。各政府機関はその使命遂行上、その可能性をどのように生かすか、決心しなければならない」。

DOD は省内の「ソーシャル・ネットワーキング方針」について最終のミーティングが 2009 年 12 月に行われるとしている。DOD（国防省）CIO の Dave Wennergren は、「責任ある利用および倫理規定への参画として、DOD ソーシャル・メディア方針の設置を固めつつある」としている。先月、「ソーシャル・ネットワーキング利用」のリスクと便益を比較するとしていたが、これまでのところ、公式な全省ガイドライとすることに否定的である。「インターネットは始まった、しかし、われわれは否定的であり、ポリシーの作成に注意深いバランス・アプローチが必要」と Wennergren は言った。「この問題は、ソーシャル・ネットワーキングよりもインターネットそのものの問題ととらえるべき」としている。

「これは、兵士や開発者の生活感（quality of life）の問題だ」とし、「これらのツールは人々が体験している以上のものだ」としている。ソーシャル・ネットワーキングは政府機関間および非政府機関の間で「マス・コラボレーション」能力として広まっており、情報共有や連邦政府のオペレーションの近代化にも寄与している。ソーシャル・メディア戦略は「データの民主化」の一部であるとして、デジタル時代のモダンな政府オペレーションのために、次の 6 点を加えた。

- 情け容赦なくセキュリティを維持した情報共有
- 技術進歩を補足すること
- 既存のモデルを情報共有に変えること
- 「将来は起こっている」を認識すること、技術を徹底利用すること
- 一人の企業家として振る舞うこと
- 全てを積極的にかつ透明に

1.5.6. NASA の Nebula

NASA（米国航空宇宙局）は、2009 年 5 月、“NASA Nebula”とよばれるパイロット・クラウドを立ち上げた。連邦政府機関によるクラウドとしては、最も早い立ち上げとなっている。NASA・Nebula は、カリフォルニアのマウンテン・ビューにある“エームズ研究センター（Ames Research Center)”で開発中のクラウド・コンピューティングのパイロット版である。NIST の分類に従えば、「プライベート・クラウド」と言えるが、公共の用途に供すという点では「パブリック・クラウド」ともいえる。また、特に高度なセキュリティを目指さないクラウドといえる。

Nebula は、もともと、インターネット接続のためのノードサーバだったものを拡張して構築されていることもあって、研究所の敷地内に置かれた「貨物用コンテナー」に構築されたクラウド・コンピューティング・サーバーである。これまでサーバーの所在そのものを秘匿とする慣行からすると奇異な印象もうける。しかし、後述のように、「コンテナー型データセンター」は一つのソリューションとなっている。NASA の公式 Web によると、Nebula は、オープンソースのコンポーネントをシームレスに統合でき、セルフサービスで高容量の計算サービス、記憶領域、およびネットワーク接続を、ビジュアルで、スケーラブルで、高いコスト・エネルギー効率で可能とするものであるとしている。

また、そのデータ蓄積は、天体観測データや外部アマチュア天文家からよる天体画像などを共有することを目指しており、「センシティブ・データ」を含まないとしていることから、冷熱効果を評価して、敢えて貨物コンテナーにしているといえる。さらに特徴的なことは、主として、NASA 職員による「On Demand」な計算サービスと外部開発基盤（Amazon EC2 など）利用のためのハブとしての役割に徹している点で、DISA RACE や Apps.gov などとは一線を画したクラウドといえる。なお、連邦 CIO 会議（FCIOC）および OMB（行政管理予算局）は、Nebula を、“USSpending.gov”、“Apps.gov”、“Data.gov”など連邦政府クラウド群をホスティングするクラウド基盤とすることを考えているようである。

Nebula は、目下のところ、公共インプットと NASA のミッション支援の協業のために、教育と公共利用に供されている。Nebula は、ハイスピードなデータ接続と一貫性のあるツール群と商用クラウドへの API とにより、NASA と外部の科学者との連携を強化している。

Nebula は、カリフォルニア、シリコンバレーのエームズ研究センターに置かれた「貨物コンテナー」内にある。以前は、インターネットのノードの一つで、「Mae West」と呼ばれた Ames Internet Exchange（AIX）であり、現在でも、Tier1 の ISP（Internet Service Provider）であり、「E root」と呼ばれるネームサーバでもある。同時に、そのネットワー

クノードにより、CENIC (Corporation for Education Network Initiative California) や Internet2 への 10 ギガ接続を可能としている。運用上必要となる「SLA (Service Level Agreement)」については、2009 年末でも「目下、法務部門と調整中」となっている。

公式 Web サイトでは、NASA　Nebula について FQA 方式で、次のように述べている。

- Nebulaプロジェクトとは？

  Nebulaは、研究者に、ハイスピードで効率的なクラウド・コンピューティング基盤を「使った分だけ払う」オンライン環境として提供するものである。
- なぜ、NASAはクラウド・コンピューティングを開発するのか？

  NASAは、民間セクターで利用されているコストセービングなクラウド・コンピューティングの便宜の恩恵に預かりたいと願っているからである。Nebulaは、パワフルでハイスケーラブルであり、FISMAへの完全な準拠な基盤を研究者に提供したい、また、データセットを効率的で簡単で安全に共有する方法を求めているからである。
- どのように、NASAのクラウド・コンピューティング能力を使えばよいのか？

  NASAは、Nebulaをその使命のため、教育や公共利用のために使い、公共との協業を強化する。オバマ政権のオープンで透明な政府を目指し、公共によるデータ共有のための容易で安全は方法を求めている。NASAは、他の政府機関と同じく、連邦安全ポリシーを遵守し、外部パートナーや公共と連携する環境を提供する。

  Nebulaのアーキテクチャは、研究者のデータが、どの商用クラウドの上でも動くように、商用クラウド・サービスへのオープンデータAPIの利点を生すように設計されている。Nebula基盤は、インターネットの複雑な機密保持をアクセスすることなく、パートナーに安全なデータアクセスの方法をNASAに提供する。
- なぜ、NASAは商用クラウドを使わないのか？

  Nebulaの開発前、 NASAは調査を実施したが、そのニーズに合致するクラウドを見つけることは出来なかった。つまり、 FISMAと準拠してなかったか、NASAが望む帯域要求を満たすスケーラビリティを持っていなかった。ＮＡＳＡは、商用クラウドが提供するよりも、はるかに大きなネットワークスピードを要求するようなデータセットを使うからである。
- NEBULAは、連邦政府が現在使っているデータ共有/蓄積の形式と同じか？

  そうだ。NEBULAとクラウド・コンピューティングは、すべのデータとコンピュータを一つのプラットフォームに集約し、それぞれ独立に監視されるべきシステムの数を減らすことにより、サイバー攻撃からの「表面」の脆弱性を減少させる。このことは、ネットワーク上のコンピュータのすべてを更新することも容易とする。

- Nebulaは、センシティブな情報を蓄積しているか？

  否。Ｎｅｂｕｌａに蓄積されるデータは、全てパブリック・アベラブルなものであり、今後も機密情報を蓄積することはない。Nebulaは、一般人がデータセットにアクセスできるようにすることで、NASAがより公共的になるために作られている。

- AMAZONのような商用プロバイダーとの関係はいかがか？

  Nebulaのアーキテクチャは、Amazon EC2のような商用クラウドサービス・プロバイダーと相互運用できるように設計されている。それはNASAの研究者に、商用クラウドの上で、彼らのデータやコードが実行できる能力を提供する。

- サーバーを持つことは大量のエネルギーを消費するといわれているが。NASAはNebulaをより確実なものにするためにどのようなことをするつもりか？

  クラウド・コンピューティングはこれまでのネットワークセンタまたはサーバーセンターの3/5の効率的である。その他に、不要の時はコンピュータをネットワークから切り離すことで、従来のデータセンターの50％のエネルギー消費と言われている。

- もし、Nebulaがオープンソースを主張するならば、なぜ、オープン標準化団体とならないのか？

  Nebulaは、現在、オープン標準化ボディに参加し、必要なペーパーワークをしている。Nebulaチームは、NASAの法務部門と作業しており、どの貢献者のコードも「貢献者ライセンス合意」によって支持されように、また、Nebulaがフリー・リブレ・オープンソフトウェア（FLOSS）となることを確認中である。

1.5.7. NIEM (National Information Exchange Model)

「クラウド」そのものではないが、省庁間「組織横断・情報共有」ために、DHS（国家安全保障省）のNIEM（National Information Exchange Model）が情報交換基盤として寄与しており、連邦クラウド・コンピューティングを推進する手段となっている。NIEMにより、財務活動報告の週単位提出、資金供与通知、受領報告提出の透明性が向上したと言っている。「Rcovery.gov」のための情報交換にも寄与している（DHS：Donna Roy、Anthony Hoang）。

災害時や緊急時に適切な対応方針や方策を判断するには、各機関における素早い情報共有や情報交換が必要となる。しかし、各機関の独自の情報システムや専門用語等のため、必要な情報を他機関から得るには数々の調整や書類のやり取りが必要であった。こうした作業の非効率性ひいては経費の無駄を省くために、機関間の情報に関する“橋”の構築が必要となった。

DOJ（司法省）が、法令管理などで基礎となるプログラムを開発し、その部署がDHS に統合され、上記のような問題を解決し、情報交換の標準を定義するものとして、2005 年に米国司法省と国土安全保障省の協同により The National Information Exchange Model(NIEM)として設計された。NIEM は政府の各機関の情報システムや設備の橋渡しを行い、情報の共有を図ることを目的に考案された。2007 年にはNIEM の第 2 版が公開された。NIEM は今や、ニューヨーク、フロリダ、ミネソタ、テキサス等の州政府や各連邦政府機関で利用されている。また、海外でも入管手続きをなどで、100 ケ国以上で利用されている。日本の入管手続きでも利用されている。

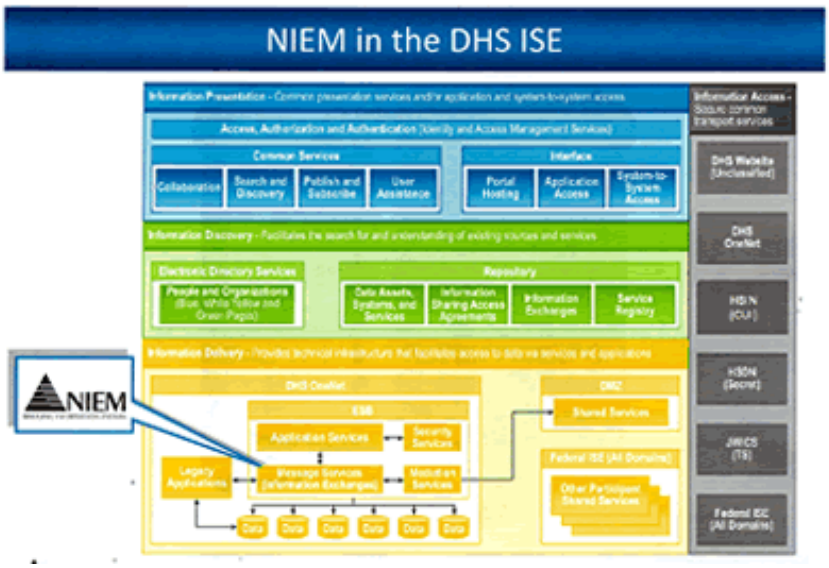
DHS では、機密性の高い情報を各機関（Recovery.Gov など）や部門で効率的共有できる仕組みとして、“DHS ISE(Information Sharing Environment)”と呼ばれる基盤を構築した。中核となる情報交換のための XML スキーマセットが NIEM（National Information Exchange Model）である。

NIEM によるデータ交換標準はグローバルな法務情報の共有化を皮切りに実装に成功し、GJXDM(Global Justice XML Data Model を拡張することによって、安全保障、緊急時、および災害対応機関や国土安全保障関連に関わる官庁や企業間横断的な情報共有を促進した。情報共有の基盤としてNIEM は以下のような役割を果たしている。

- 各関係者の専門領域間で緊急事態時に共有が必要な情報項目を決める。
- 共通語彙およびオンラインの情報共有をサポートするための情報交換用のパッケージ文書のオンライン・レポジトリーを開発するための標準
- データ検索や普及支援、ドキュメントの交換・共有・再利用のための技術的なツールの提供
- 企業向けの情報交換・共有のための技術支援や訓練や実装のためのサポートサービスの提供

NIEM は、すでに 6,000 を超えるスキーマセット（モデルと呼んでいる）を抱えている。その目的は部門間の情報交換にあり、EA における ESB（エンタープライズ・サービス・バス）である「DHS OneNet」の主要技術となっている。

図 14　NIEM 概要



「Recovery.gov」における組織横断の情報交換で、XML をカストマイズする場合と、NIEM 利用の場合を比較したコスト比較が示されている。100 事例で情報交換用のコンテナ（IEPD）を再利用することで、72%のコスト削減になったとしている。

1.6. 【付属資料：現地調査と調査結果】

1.6.1. 【付属資料 1：連邦政府関係機関へのインタビュー調査】

訪問者：東京国際大学 堀内一教授、㈱アイ・ビー・ティ 延原誠市
訪問日時：2009 年 11 月 23 日～26 日
訪問先：

① NCOIC：NCOIC 会長 Terry Morgan、立会；Kevin Jackson, Jerry Smith, Dr.Brand Niemann
② NIST：Dr. Peter Mell、立会；Jerry Smith
③ DHS：Donna Roy,Anthony Hoang,Jeffery Biala、Adam J. Merce、立会；Jerry Smith
④ EPA：Dr.Brand Niemann、立会；Kevin Jackson、Jerry Smith

【調査結果の概要】

オバマ大統領の「オープン政府」の重要課題の中核は、①透明性、②説明責任、③公的参加の 3 つである。この原則を以って、オバマ政権による連邦政府の情報政策では、技術力（Power of Technology）をテコにして連邦政府を変革する方法として次の 4 点を重視している。

- イノベーティブな Web 2.0 技術の採用で、より透明性のある参加型・協働型政府の実現に向けた大統領誓約を履行すること。
- 最新の IT システムの採用により連邦政府サービスの実効性を近代化・改善すること。
- 自然の脅威および悪意のある脅威に対する連邦情報システムおよび国家情報インフラの安全保障を確保すること。
- 各省庁横断的な広範な利用に向けた IT 投資と、重複した管理の乏しいプロジェクトを無くし、IT 調達を合理化することで納税者の税金を節約すること。

- 2002 年米国電子政府法（e-Government Act of 2002）に基づき、米国では、約 50 に及ぶ連邦政府機関のうち、24 省庁の CIO をメンバーとする連邦 CIO 会議（Federal CIO Council）を設置。事務局は、ホワイトハウスの OMB（行政管理予算局）内に Office of E-Government and Information Technology（E-Gov & IT）が設置されている。連邦 CIO 会議（Federal CIO Council）の議長は、OMB（行政管理予算局）に置かれる連邦 CIO と決められている。

- オバマ政権は、連邦 CIO（e ガバメント行政官）として、コロンビア特別区の Mayor である Andrian Fenty の下で CTO として Web サービスを使いオープンソースとクラウドソースのアプリケーションを活用して実績をあげた Vivek Kundra（インド系、若干 35 歳）を任命し、2010 年度予算の IT マネジメントで大きな責任を課した。クンドラは 2009 年 3 月に FCIO に就任した。連邦政府の「クラウド化」は V.クンドラの就任から始まった。

【参考：クンドラ紹介】

http://en.wikipedia.org/wiki/Vivek_Kundra

http://gcn.com/Blogs/Tech-Blog/2009/03/Kundra.aspx

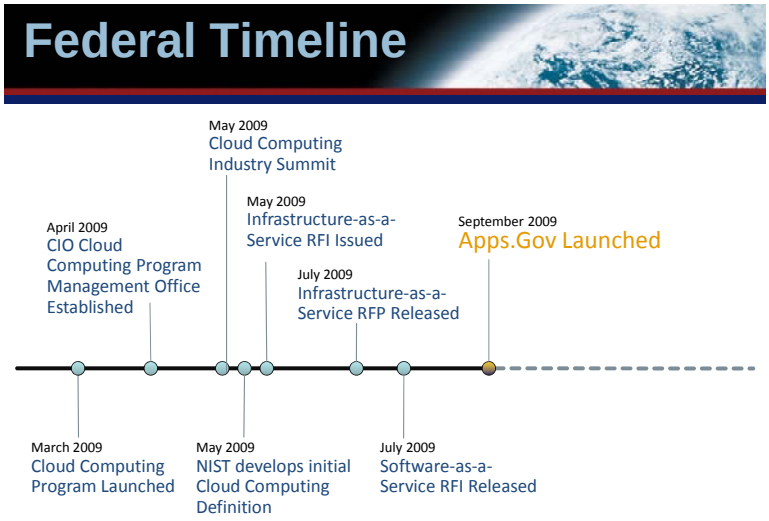
- ホワイトハウスの OMB（行政管理予算局)に属する連邦 CIO は、年間 710 億ドル（約 7 兆円）にも及ぶ政府の IT 予算を管掌し、連邦政府の情報システムをデザインする要職である。オバマ政権の公約にあった CIO と CTO の 2 つのポストの 1 つで、従来、省庁が独自に構築・管理してきた情報リソースを横断的・機動的に利用できるようにすること、セキュリティとプライバシーを確保しつつ政府情報の公開を促進すること、システム全体としての費用対効果を大幅に高めること、などを目標としている。
- 連邦 CIO 会議（Federal CIO Council）は 24 省庁以外も、多くの機関がリエゾンメンバとなっていることから、実質的にはすべての主要省庁を把握しているといえる。連邦政府機関の CIO で「クラウド化に反対する者はいない。約 50 ある連邦政府機関の CIO の「100%」が同意していると」とのこと。
- Vivek Kundra は、コロンビア特別区の CTO として、2007 年に Google APPS を政府 IT に導入し、350 万ドルの費用を削減したことで知られる。“Apps for Democracy”イニシアティブを立ち上げ、公的にアクセス可能な Web サービスを使ったオープンソースとクラウドソーシング（Cloud Sourcing）アプリケーションの開発で有名になった。
- 留意すべきは、クンドラ CTO は、公的データの中で機微なデータ（Sensitive Data）の分類を唱え、これを Google Apps には入れないことに最大の注意を払い、e メールで送受信できるデータだけを Google Apps に入れる方針を掲げて、Google Apps を 38,000 人のワシントン DC の職員に使わせた手腕から、2009 年 3 月に連邦 CIO に任命されている。
- クンドラ連邦 CIO の最重点課題は、2010 年度予算において自己中心的（silo'ed）な IT 基盤の構築をやめて IT 予算を削減することである。その重点課題は；
  - 連邦 IT 調達を改善（IT 効率の向上に対するリウォードの提供、各省庁の IT 支出削減のインセンティブ、クラウド・コンピューティングの利用拡大)、
  - 相互運用性、ポータビリティおよび標準の必要性（政府 PAAS？)、

- 共通クラウド・プラットフォーム上の国防省（DOD）・各省庁間の戦略的調整、
- GSA をクラウド・コンピューティングの重心にすること、

- 「政府透明性」によるイノベーションの促進。OMB（行政管理予算局）の下には、連邦 CIO を中心とする CIO Council だけでなく、プロジェクト評価を担当する CPO（Chief Performance Officer）も組み込まれている。事実、2010 年度、連邦政府予算については、ARRA（国家再生・再投資法）による予算にもかかわらず、各機関とも小規模の増加か、削減となっている。
- 連邦 CIO の Vivek Kundra（ビベック・クンドラ）が導入したのは“Apps.gov”、“Data.gov”、“Federal IT Dashboard”の 3 つである。Apps.gov が中核である。“Federal IT Dashboard”は、主要な政府機関の IT 投資をビジュアル（可視化）にみることができるもの。
- ビベック・クンドラ連邦 CIO は、連邦政府の保有するデータをより利用しやすい形で一般大衆に利用可能にするために、“Data.gov”を立ち上げる。連邦政府の歳出情報公開サイトの“USASpending.gov”に，IT 投資状況を米国民に情報開示するためのサイトである“IT Dashboard”（ベータ版）を新設。最近では、連邦調達を担う GSA(General Service Administration)により、連邦政府機関向けのクラウド・サービス調達サイトである
- “Apps.gov（https://apps.gov/cloud/advantage/main/start_page.do）”を 2009 年 9 月に開設した。“Data.gov”は近々、“Apps.gov”に移行される。
- 「クラウド化」おいて、最も懸念されるセキュリティについては、各機関がそれぞれ独自の要求を持っていることから（DHS、DOD、FAA など）、その調整に NIST（国立標準技術局）のセキュリティ技術部門の Dr.　Peter Mell らが当たることなった。「セキュリティは最大の問題ではない」とし、保護すべき情報とすべきでない情報とを峻別するために、「クラウドのタイプ分け」を重点とする「クラウド定義」を NIST が素案を作った。その「提供タイプ（deployment model）」は次の通りである。
  - プライベート・クラウド：特定組織で基盤として運用される。（特定なセキュリティ要求に対応できる。）
  - パブリック・クラウド：一般市民または大きな業界グループにおけるクラウド基盤であり、クラウド・サービスを売るために一つの組織によって所有される。
  - コミュニティ・クラウド：特定な関心（使命、セキュリティ要求、政策、準拠性などについて）を共有するために複数の組織によって共有されるクラウド基盤である。「組織」またはサードパーティによって管理される。特定な前提を持つものあれば、持たぬものもある。
  - ハイブリッド・クラウド:2 つ以上のクラウド（プライベート、またはパブリック・クラウド）からなるクラウド基盤でありながらも、ユニークな存在であり、デー

タとアプリケーションのポータビリティを可能とする標準的または商業的技術の結合である（例えば、クラウド間の負荷調整ために、データやアプリケーションを移動させるなど)。

- NIST による「クラウド・コンピューティングの定義」は、パブリックコメントとレビューを繰り返し、既に、第 15 版まで改定している。「クラウド化」おいて、最も懸念されるセキュリティについては、各機関がそれぞれ独自の要求を持っていることから（DHS、DOD、FAA など)、その調整に NIST のセキュリティ技術部門の Dr.　Peter Mell らが当たることになったもの。
- 2009 年 3 月の連邦 CIO クンドラの就任から､その最初のパイロットクラウド(Apps.gov)の多仕上げまでの「連邦政府クライド化」の主要なイベントは、次のようなものである。



- 「プライベート・クラウド」の事例は、DISA（国防省情報システム局）の RACE（Rapid Access Computing Environment)、NASA の星雲を意味する Nebula（シリコンバレーの NASA Ames Research Center で開発されているプライベート・クラウド: IaaS/PaaS/SaaS の 3 つのサービスを提供、NFC（公務員給与支払い)。
- 「パブリック・クラウド」の最初の事例が、クンドラが最も力を注いでいる GSA（連邦調達局）の APP.gov である。
- GSA は、政府クラウドを進めるために、FCCI（Federal Cloud Computing Initiative)を編成し、「政府クラウド・コンピューティング・フレームワーク」を示している。ベンダーの棲み分けを示すとともに、今後の産業構造を示し、「サービス・イノベーション」の基礎にもなると言える。
- 「クラウド」全般に関する政府の方針やガイドライン作りは NIST や GSA などが担当し、

その途上にあるが、各省庁がその動きに関心を払いながら、ことを進めている。例えば、DHS などは、既に、19 か所のデータセンターを 2 か所に統合する準備に着手していた。【第 4.2 参照】

- OMB は、連邦政府クラウド（Apps.gov や USAspending.gov, Data.gov）などを、NASA が運営するクラウド（Nebula）に移行する意向である。OMB による「クラウド・コンピューティングを利用しない理由」の報告要求。OMB は、連邦政府機関のクラウド化を推し進めるために、各政府機関に「クラウド・コンピューティングを利用しない理由」を求めている（2009 年 12 月 10 日）。

【セキュリティ】

- クラウド・コンピューティングは「新技術ではなく時代の必然である（Peter Mell)」。セキュリティなどに不安を残すものの、「セキュリティは最大の問題ではない（V. Kundra)」とし、また「それを理由にことを遅らせるべきではない」、連邦政府の CIO たちは、そのように考えているようである。
- そのために、「絶対セキュリティ」でなく「柔軟なセキュリティ対策」を求めて、「クラウドのタイプ」や「データの質」によって取り扱いを変える統一的な概念定義が求められ、NIST による「クラウド・コンピューティングの定義」が始まった。
- クラウドのセキュリティについては、「基盤（インフラ）セントリック・セキュリティ」と「データセントリック・セキュリティ」を分けている。
- これまで、セキュリティ議論や技術開発は、基盤としてのプラットフォームやネットワークに対するもので、DOS 攻撃、BOT やウィルス対策などが主体であった。
- 「クラウド時代」のセキュリティ技術は、クラウドに置かれるデータそのものの防御を主体とする「データセントリック・セキュリティ」である。
- 具体的には、データごとの「データ・センシビティ（データの機微度合いによる重要度区分）による防御を固める」ことを指す。センシビティ（機微性）の低いデータは「パブリック・クラウド」においてもよいが、センシビティの高いデータは、暗号化を徹底しながら「プライベート・クラウド」で管理するといった取扱いが重要となる。
- NIST の Peter Mell らは、セキュリティの専門家であるが、「データ・センシビティ」に関する基準作りは、これからの課題のようである。しかし、訪問先のすべてで「データ・センシビティによるセキュリティ」という言葉を聞いたことから、この方針は、連邦クラウドの方針として徹底されているようである。

【民間クラウド事業者との関係】

- V. Kundra は、2009 年 5 月の「クラウド・サミット」の場で、Google などに対して、

「FISMA」への準拠を求め、その準拠への約を得たことから、連邦政府機関への参入を許したようだ。FISMA への準拠を公言させることで、実質的に Google などの参入を容認したともと言える。事実、すでに DOD など一部の政府機関は Google による「コミュニティ・クラウド」を構築している（DISA /RACE)。

- セキュリティ上の問題がない限り、または政府の方針に整合する限りは、クラウド・サービス・ベンダとして、Google やマイクロソフトなど民間事業者を受け入れ、さらに発展させたいという狙いもあるようである。
- DOD は、2004 年 8 月、Net-Centric 構想を民間に普及させるためのコンソーシアム、NCOIC（Network Centric Operations Industry Consortium ）を発足させている。その構想はクラウドに通じることから、ボーイング、ロッキードマーティン社などメンバー企業が、「クラウドのアクセスパターン」などの技術標準化に取り組み、民間ベースで、NIST とは異なる分野での標準化と普及活動を展開している。基本的に、「政府クラウド」といっても、特別な専用インフラを構築することを意図せず、むしろ民間や一般に広く利用されているインフラと新技術やソリューションを、安全、かつ迅速に、行政業務に導入したいというのが、V.クンドラや連邦 CIO たちの意向である。

【パブリック情報の公開とイノベーション】

- オバマ政権の情報政策方針、「透明性」、「参画」、「協調」に基づき、パブリック情報の活用によるイノベーションを期した情報共有基盤がクラウドとして新たに構築されつつある。これまで,容易に成果を出せなかった連邦政府機関の「情報共有」と「情報公開」については、古くは「情報公開法（FIOA)、1966」や OMB からの通達、所謂、「情報資源管理（OMB circular A-130）と 2004 年の覚書「連邦政府機関のパブリック Web サイトに関する方針(Attachment fulfill the requirement of section 207(f) of the E-Government Act of 2002 (Pub. L. No. 107-347) など、オバマ大統領の「政府透明性」に対する強い姿勢と、連邦 CIO（V. クンドラ）経験、志をもった有識者（B. Niemann など)、各省庁の CIO によって、クラウド（Data.gov, Spending .gov, IT Dashboard）として立ち上がっている。また、「米国再生・再投資」のために確保された連邦政府予算の執行状況を各省ごとに公開するサイト Recovery.gov も機能している。
- ARRA と Recovery.gov：オバマ政権は 2009 年 2 月に、「雇用の創出」、「長期的成長のための投資と経済活動の刺激」、「政府支出の説明責任と透明性の確保」を目的として、「ARRA：American Recovery & Reinvestment Act: 国家再生・再投資法」を施行した。それに基づく予算（2010 年度は約 7000 億ドル）の執行状況を、省庁ごとにその明細の公開を求められている。そのサイトが Recovery.gov であり、OIG（Office of Inspector General ：各省庁の監査人の集まり）によって運営されている。【第 6.2 参照】
- NIEM と Recovery.gov：省庁間「組織横断・情報共有」ために、DHS（国家安全保障省）

の NIEM (National Information Exchange Model) が情報交換基盤として寄与しており、連邦クラウド・コンピューティングを推進する手段となっている。NIEM により、財務活動報告の週単位提出、資金供与通知、受領報告提出の透明性が向上したと言っている。特に、Rcovery.gov のめの情報交換にも寄与している (DHS：Donna Roy、Anthony Hoang)。オバマ政権 2010 年度予算の「クロス・カッティング・プログラム」

- オバマ政権の 2010 年度の予算を、「課題別」、「省庁別」に、2008 年度、2009 年度および 2010 年と、を比較したものを「Cross Cutting Program」と呼で公開している。特に、「国家安全保障確保」の分野、「国家統計データの強化」、「研究開発」などのテーマで比較を示している。一部の省庁では、クラウド・コンピューティングの成果が出ているようである。
- USASpending.gov と IT ダッシュボード：政策評価につながる予算執行状況などをビジブルにするためのクラウド「IT Dashboard」が、Spending.gov としてスタートしている。税金の使途を、政府、州、群単位で、また契約額などを主要企業別に参照できる。
- USA.Gov:米国の一般市民向けに、政府の活動紹介や市民の声を聞くための Web サイト。その情報も州別、群別など地域別に参照できる。
- 「政府の公開情報」がもたらすイノベーションの例：GSA の Apps.gov では、政府機関の「クラウド・コンピューティングサービス」調達を進めるために、民間で広く使われているツールやサービスの一覧を提供している。
- クラウドに限らず、ARRA の支出を明らかにする Recovery.gov のデータを「政策パフォーマンス評価」のために分析できる RIA (Rich Information Application) 製品やソリューション・サービスが民間で開発されつつある。Actuate 社の「BIRT Performance Scorecard 9」、Facebook など「ソーシャル・メディア」の政府利用への浸透なども注目すべきである。
- 一方で、クラウドに限らず、政府機関で、Facebook、Twitter、などの「ソーシャル・メディア」の政府内での利用について、DOD を中心に議論が続いており、その動向も注目される。

【所感】

- 連邦政府の「クラウド化」における連邦 CIO (V. クンドラ) と各省庁 CIO との意思統一は見事と言うほかない。メディアやブログも V. クンドラの発言、一言云々に注目しており、予算執行 (OMB) とリンクした体制は、「クンドラ帝国」ともいえる。
- その大きな目標は、「行政コストの削減」だけでなく、「行政パフォーマンス評価」のための「行政データの公開」、「省庁間横断的情報共有」に置かれている。単に、「データセンター運営費の削減」だけでなく、「行政の質の向上」の視点が貫かれており、そのための「データ集約」が狙いとなっている。さらに、「行政情報の公開」を通じた「イ

ノベーション」にも重点が置かれており、民間で利用されているツールや技術お積極的に取り入れつつある。すでに、GSA の Storefront や Data.gov, URecovery.gov. DISA/RACE、NASA/Nebula などでは、オープンソースのソフトウェアが利用可能であり、それらの公開情報をベースとした高度な情報処理サービスも登場しており、新しい情報活用のイノベーションの姿が見え始めている。

- 全体のパフォーマンス評価やソーシャル・メディアの政府機関への導入に関する明確なガイドラインがないまま、ベンダー論理で進められ、「クラウド間の相互運用性」や「ベンダーロックイン」などに禍根を残す恐れもある。単に「データセンター運用コスト削減」だけでなく、「行政として何を達成したいのか」の議論が必要と感じた次第である。
- 誰もが危惧するセキュリティについて、「最大の問題ではない」というクンドラの方針と「クラウドのタイプ分け定義」が、セキュリティとプラットフォーム技術に拘りがちな風潮を打破して現実的な解を与えたといえる。
- わが国における「クラウド議論」は、プラットフォームなど基盤側の技術的議論に偏るきらいがあり、クラウドを次世代の「イノベーション」につなげる議論が少ない。E-Gov の一形態として、行政が主宰するガバメント・クラウドの「使命に関する議論」が望まれる。
- 一方、今回の調査で、政府機関の要人（Peter Mell、Brand Niemann、Donna Roy など）に、米国国外に目を向けているか否かを確認したが、立ち上げ段階にある「今はその時ではない」と、米国内だけの議論となっていることは、当然であるが、特筆すべきと言える。法的連携についても「可能性はある」だけであった。
- ただし、DHS の NIEM（国家情報交換モデル：XML のスキーマセット）については、その目的と技術の一般性もあり、クラウド相互運用の基盤となりうるものとして、海外への展開に意欲的であった（DHS、Donna Roy）。
- 日本としても、DHS の NIEM チームと連携して、「入管業務」に限定せず、その導入可能性に関する調査を開始すべきと思われる。
- これまで、米国情報産業は、いずれも国防予算や国家主導で（あるいは民間が国家を利用しつつ）発展してきた。今日、連邦政府が後押しする「クラウド・コンピューティング」は、情報産業における米国の次世代「国家産業戦略」と認識すべきかもしれない。
- 日本は「要素技術」のブレークスルーに強いといわれるが「アーキテクチャ」がないとも言える。そのブレークスルーもシーズ先行で偶発的である。それらを後づけで統合するのは困難を伴う。
- アーキテクチャ議論を「大言壮語」として取り合わず、「中身がない」と非難する傾向も強い。多様な関与者が関わる社会システムのような大規模システムでは、個々の要素の標準化では、「すり合わせ」に難航し統合が難しい。「Big Picture」としての構想

をアーキテクチャとして標準化することが求められる。「イノベーション」も、そのようなアーキテクチャを満たすため、あるいはそれを契機に引き起こされる、という印象を受けた。

- また、「クラウド相互運用性」についても、個々のインターフェースを標準化するよりも大きな枠組みとしてのフレームワークやアーキテクチャの標準化が優先する。
- FCIO の V. クンドラはじめ、米国にはアーキテクトが多数いること、その提案するアーキテクチャを、後から「亜流」を作らず、「先行者の提案を尊重し、愚直に実現しようと共同する社会が米国である」と改めて感じた次第である。

【個別政府機関における意見交換のノート】

1. NIST (2009 年 11 月 24 日午前)　Gaithersburg, ML

面談者：Dr. Peter Mell (NIST の情報技術研究所コンピュータセキュリティ部門のシニアコンピュータサイエンスチスト)

- 日本だけではなく、欧州でもクラウドの認識が十分ではない。欧州では、クラウドのメリットに関する理解が深めれば、導入ペースは加速化すると思う。米国では、クラウド・コンピューティングのパラダイム変革が民間企業の間に急ピッチで広がった。資本支出の節減や投資効果は実証済みである。加えて、オープンで健全でもある。

- CIO Council と NIST の取り組み
  - 米国で何か起こったかというと、オバマ大統領がコロンビア特別区の政府でクラウドを実践したビベック・クンドラを連邦 CIO に任命した。連邦政府 IT の全体の構成と機能に対する責任を担うポストである。従って、連邦政府の「クラウド・コンピューティング」浸透は急ピッチで進んだ。
  - NIST の役回りは、Inter-Agency(省庁間)の技術問題の調整と問題解決である。この役割を担うが、私、Peter Mell である。私の下に、セキュリティ、標準、オペレーション、アウトリーチ（評価）の 4 つのワーキンググループがある。トップレベルのマネジメントが各政府機関に受け入れてもらうようにクラウドの取組を行っている。内容は幅広く、意思決定の問題から、一般の COI（関心事コミュニティ）まで幅広い問題を解決している。間にいる中間の職員がやることも多く、最も多くの課題に直面している。トップレベルの関心は、スタッフの数だとか、コストに集まる。

- NIST は、Inter-Agency の技術課題に取り組んでいる。

- 連邦 CIO 室では、毎日のアップデートを実施。Weekly ベースのエクゼクティブ・ステアリング委員会で最新の進捗結果を検証している。Kundra は日報レベルで報告を求めている。エクゼクティブ・ステアリング会議（プログラム管理者）は週 2 回、それ以外は毎週、あとのことは私に任せている。
- 最も悩ましい問題は何かとの質問に対して、データセンターの整理統合だとの返答。クラウドは、ある権威を築いた人々にとっては脅威となる。ソフトウェアとインフラストラクチャとは、分けるべきである。プラットフォームとインフラストラクチャの方がはるかに難しい。次に、重要な課題は、セキュリティである。セキュリティを議論するときには、必ず、①セキュリティ・コンプライアンス（Security Compliance)、②コンピュータセキュリティの 2 つを混在させないようにすべきである。現在、GSA のセキュリティ WG で、セキュリティ・コンプライアンスの要求事項を検討中である。

- GSA の調達基準は変わるのか？
  - GSA の IT 調達では、調達契約（Purchasing Agreement ）の内容は以前と同じである。最重要視しているのは、セキュリティ・コンプライアンス問題の対応である。クラウドは、リソース・プールのシステムを前提にしているので、アウトソーシングは特定のものだけである。クラウドでは、ひとつのシステムに対して、クライアントの数は多数になる。各クライアントには、各セキュリティポリシーがある。また、50 の省庁も独自のセキュリティポリシーを持っている。これをすべて持ち込めば、大変なことになる。そこで、NIST では、政府機関間の調整をおこない、オーソライジングプロセスの検討を進めている。
  - DOD（国防総省）や DHS（国土安全保障省）のソフトウェアアシュアランス（SwA）イニシアティブの議論も踏まえ、同じコンプライアンス（法規遵守規則）システムを作ろうとしている。特に、軍事部門は、これに加味したものをつくろうとしている。しかし、コミュニティとインテリジェンスでは、セキュリティは異なってくるのではないかとの質問に対して、重要なことは Data Sensitivity（データの機密性）をいかに分類するかである。これは、パブリック・クラウドとプライベート・クラウドでのデータの取り扱いの基準にもなる。軍事にかかわるものは、Data Sensitivity（データの機密性）が高くなるので、クラウドも高いセキュリティを必要として、スマートなプライベート・クラウドで対応する。プライベークラウドのサーバー数は 1,000 程度のイメージである。他方、Sensitivity の低いものは、パブリック・クラウドで対応すればよい。
  - 我々が考える重要な基準は、①Data Sensitivity（データの機密性)、② Virtualization（仮想化)、③経済環境の 3 つである。

- クラウド間の相互運用性（Interoperability）について。
  - クラウド間の相互運用性（Interoperability）は確かに必要になる。しかし、小さなAgencyでは大した問題ではない。Interoperabilityの問題は、①災害復旧＝disaster　recovery（災害によるシステム復旧）と②ベンダーロックインを防ぐためだけである。もちろん、Inter-Cloudの相互運用性も課題としてある。しかし、現在、米国は、プライベート・クラウドを立ち上げつつあるという初期段階であるので、詳細な議論にはなっていない。重要な要素は、クラウドのPortability（可搬性）とVirtualization（仮想化）、ベンダーロックインの防御である。
  - クラウド・コンピューティングの概念は、新たなIT資産を作ることではなく、既存のIT資産を統合化･収れん化することである。Web2.0など技術はそろっている。今日の経済環境が、クラウド・コンピューティングを受け入れさせている。

- 経済的インセンティブをどのように考えているのか。
  - 費用便益分析（CBA）については、モデルによって変わる。パブリック・クラウドはイニシアルコストが不要であるので、検討する必要はない。プライベート・モデルでは、先行投資が必要になるので、検討する必要がある。
  - コスト効果については、年間50ドルで、ワープロ,ワークシート、スプレッドシート、PPT、e-Mail、(Google Appsなど）が利用できる環境の意義は大きい。私は、Google Apps を推薦しているわけではないが、Googleなどのセキュリティレベルは上がっている。Googleは、政府向けに1,000ページに及ぶセキュリティ報告書を提出してきた（私は見てない)。
  - 米国政府は、プロバイダーを3つに分けている。小さくてスケーラブルで、それだけでリソースをプールさせるもの。プライベート・クラウドの事例では、DISA（国防省情報システム局）のRACE（Rapid Access Computing Environment)、NASAの星雲を意味するNebula（シリコンバレーのNASA Ames Research Centerで開発されているプライベート・クラウド)、NFC（公務員給与支払い）などがある。

- US パトリオット法（反テロリズム法の H.R.2975 パトリオット法）とプライバシーについて。
  - （2001年の反テロリズム法であるH.R.2975パトリオット法（Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001）は、米国内のサーバー上にあるデータは司法当局および連邦捜査局による調査の対象となることを義務づける。クラウド・サービスの提供事業者が米国内にサーバーを設置している場合、そのサービスの利用状況や保存データが調査の対象になりうると考えられる)。
- Q:パトリオット法がデータ管理の秘匿性に影響を与えるという意見があるが、どうか?

- A: 私はこの問題の専門家ではないが、一部のマスコミなどが騒いでいるだけだと思う。愛国者法の侵害問題は、要するデータ管理の秘匿性の問題である。重要なことは、Data Sensibility（データの機微性）の管理である。

- Q:クラウド・セキュリティのために新たな技術開発はやっているか？
  - A:新たな技術開発は考えていない。当面は、通信基盤として「IPV4」から「IPV6」への転換に努める。
- Q:Data Sensitivity データの機密性）の分類」はやっているか？
  - A:今はやってない。米国政府は、データセンターをすべてCloseして、すべてをPublic Cloudにするとは言っていない。

- 標準化について。
  - Functional Standard（機能の標準）を考えると、インフラであるIaaSは、Durable（恒久性）のあるもので、機能規格（インフラストラクチャ、仮想化、プロビジョニング）については耐久的（durable）で可能である。つまり強制力が強い。しかし、サービスとしてのPlatformは難しい。
  - 国際標準化団体とのHarmonizationも検討中。現在のところ、規制や法律を変える意向はない。標準化については、業界標準が先で、次にNationalレベル、その後に国際標準化の協議という手順だと理解している。今は、これを考えるときではないと考えている。

2. DHS（国家安全保障省）：2009年11月24日午後

面談者：Donna Roy（NIEM Executive Director, Office of DHS CIO）Anthony Hoang（NIEM Program manager,）、Jeffrey Biala（Enterprise Knowledge Management Architect）、OCIO/Enterprise Data Management Office

場所：DHS: 3801 Nebraska Avenue NW、Washington DC 20528

- DHS（Department of Homeland Security）は、同時多発テロのあと、2003年にDOJ（法務省）から独立して設置された。全米で約25万人の職員を抱え、ミッションも多様である。空港の指紋照合から、沿岸警備、メキシコ、カナダの不法移民、ハリケーン、山火事や森林火災などの非常事態対応、原子力保安などの幅広い業務分野にまたがっている。我々の任務は、こうした多様なミッションに対応できる情報システムに取り組むことである。DODとも連携協力しつつ、情報シェアリングモデルであるNIEMの構築を行っている。
- NIEMとは、国家情報交換モデル（National Information Exchange Model）の略語で、法務省と国土安全保障省（DHS）との連携で、緊急事態における重要情報（critical information）をシェアすることが可能する組織ワイドの情報交換の標準とプロセスを

開発・普及・支援することを目指した取組で、各省庁の日常業務を支援する。NIEM は、現在および今後のビジネスプラクティスの一環として組織間の情報シェアリングに特化し、実際のデータ交換スタンダードであるコンテンツの標準化も目指している。

- DHS が進める「NIEM」は、ARRA（国家再生・再投資法）に基づく政府支出を監視するためのサイト Recovery.gov（http://www.recovery.gov/About/Pages/About.aspx）の基盤として、省庁間の情報交換に寄与している。【5.6 参照】
- DHS は、現在、連邦議会と連携して、19 か所にある「データセンター」を統合して 2 つの信頼性のあるデータセンターに集約する作業を進めている。マイグレーションをどうするかが大きな課題である。データセンター統合の狙いは、システム運用コストを下げることにあるが、連邦政府予算約 25B$（2200 億円）のうち、DHS が 6B$（400 億円）を占めている。（因みに DOD/DISA は 70 億ドルである。）
- 「クラウド化」については、全面的に NIST の方針に従う。もちろん、すべてのデータがクラウドに置かれるわけではない。レガシーにも保管することになる。
- 特に、重要な点は、重要情報（Critical Information）のセキュリティ対策である。オープンなデータとパブリックなデータを区別することが大切。連邦政府では、Sensitive Information（機微な情報）という視点から、Data Sensitivity（データの機密性）に基づいて、重要情報の分類を行っている。

※註：Data Sensitivity（データの機密性）とは、組織のミッションや日常業務にとって、IT システムにより加工、蓄積および伝送される情報の重要性と正確を測定する尺度である。データの Sensitivity（機密性または機微性）のレベルに応じて情報を区分することをデータ分類化（Data Classification）と呼ぶ。

ブッシュ大統領により 2003 年に発布された大統領命令（Executive Order）13292 は、
① 米国政府に所有・作成され管理されている情報。
② 機密区分する情報分野に該当する情報、
③ 許可なく公開することによって国家安全を害することが容易に想定できる情報
のすべての要件を満たす国家安全保障情報（National Security Information）の分類（Classifying）、保障措置（Safeguarding）、分類解除（Declassifying）を行うことを定めている。

具体的には、Top Secret（レベル 3）、Secret（レベル 2）、Confidential（レベル 1）の 3 つにデータ分類化のレベルを定めている。他にも、Unclassified というカテゴリーがあるが、これはテクニカル面では“分類化（Classification）”ではなく、許可なくても個人に発信される情報を指している。

- 米国の行政当局は、具体的には次の 4 つのカテゴリーに分類している。

  ① **トップ・シークレット**：国家安全に「非常に重大なダメージ」を及ぼす可能性のある情報。
  ② **シークレット**：国家安全に「重大なダメージ」を及ぼす可能性のある情報。
  ③ **SBU(Sensitive But Unclassified)**：これは、機微なもの（取扱注意）ではあるが機密扱いでないもの。正確に表現すると、Top Secret（レベル 3）、Secret（レベル 2）、Confidential（レベル 1）に分類される情報ではないが、公表には制限が設けられる情報である。この SBU は、行政用語で、“Sensitive Security Information (SSI)”、“Critical Program Information (CPI)”、“For Official Use Only (FOUO)” “Law Enforcement Sensitive (LES)”など 180 種類の区分がある。因みに、Law Enforcement Sensitive (LES)は、法律施行に係る関係省庁・機関の者に限って開示される情報である。
  ④ **Unclassified。非分類（機密扱いしない）**。

- 19 ヵ所を 2 ヶ所のデータセンターに統合するのは、新たに設置される部門（22 部門）を支援することもあるが、コストだけでなく、よりよいデータ・マネジメントを行なうこと、データ交換を円滑に行なうことが主目的である。DHS では、SOA（サービス指向アーキテクチュア）をソフトウェアエンジニアリングの手法で重要視している。これは、まさに、クラウド・コンピューティングに向かう動きで、我々は、クラウド環境におけるシェアードサービスを行なうことを検討しつつある。
- （連邦政府から政府クラウドで進めるとの指示のもとで、データセンター統合化の動きに乗り出したのか？）：米国では、政府主導によるクラウド導入の動きは起こっていない。政府サイドは、Web2.0 のコンセプトを取り入れ始め、ソフトウェアのリリースサイクルの終焉などの問題を検討した。現在のドライバーは、データである。データをいかにシェアするかが今のキャッチフレーズである。

- （セキュリティと Interoperability の問題をどう考えているのか？）：我々の理解では、プライベート・クラウドの中では Interoperability の問題を意識しなければならない。セキュリティでは、先ほども言及した“Data Security”も重要な問題である。誰が特定情報にアクセスする権利があるのかを考える必要がある。クラウドを使うようになれば、データの利用可能性（Availability）が増えてくる。政治家は、透明性を評価尺度にして、クラウドを評価している。産業界の CIO は、クラウドの Visualization（可視化）を評価する。
- DHS のトップ・プライオリティは、DHS の情報システムを信頼性の高い情報システム（Trusted IS）にするために、19 のデータセンターを 2 つに統合化するのである。コ

スト節減だけではなく、データのより良いマネジメントが主たる狙いである。今は、プライベート・クラウドを構築しつつあるので、プライベート・クラウドにおけるセキュリティと Interoperability の問題を語るには時期尚早である。先ほども話した通り、ここでは、データ・セキュリティを重要な課題とみなしている。今は、“情報基盤セキュリティ（Information based security”から“データ中心セキュリティ（Data Centric Security”への移行期である。

- この移行期には、データ・マネジメントが重要な課題である。データの移動を休ませるサーバー上の「Data At Rest（休眠データ）」については、データの暗号化と似た方法で厳重に管理している。休眠が解除されたデータについては、NIEM に従い適切なタグを付与し、情報活用に寄与させながらも取扱を厳重に行う。DHS では、暗号化と DRM（デジタル権利マネジメント）を組み合わせた情報の管理を行なっている。
- NIEM は、すでに 6,000 を超えるスキーマセット（モデルと呼んでいる）を抱えている。その目的は部門間の情報交換にあり、EA における ESB（エンタープライズ・サービス・バス）である「DHS OneNet」の主要技術となっている。
- セキュリティにおける NIEM の利点は、XML による情報交換で、タグにより情報の一部（文書の一部）を「機密」として扱う「柔軟性」をもつことにある。ただし、交換のための XML スキーマとしては極めて一般的なものであることから、今後、「クラウド相互運用性」のために、クラウド間の標準情報交換仕様とすることを意図している。
- 連邦 CIO のクンドラも NIEM に着目し、クラウド間の相互運用性における標準の一つとしての可能性を認めている。

【参照サイト】Federal Computer 誌、2009 年 10 月 2 日
http://fcw.com/articles/2009/10/02/kundra-interoperability-standards.aspx

- また、その技術の一般性から、「連邦情報処理規格（FIPS）」となっている。そのコア部分は、「Who」、「What」、「When」、「Where」の記述になり、同じような構想をもつ DOD の U-Core と競合するところもあるようだ。NIEM のコアは、U-Core と対応可能（Mappable）と言っていた。DOD とは、何かと競合している気配を感じた（同行した DOD の Jerry Smith 氏とは、皮肉の応酬があった）。
- NIEM は、もともと DOJ（法務省）の法令記述などの業務で使い始めたとのこと。その適用は米国の州レベルからその下の群レベルまで広がっているとのこと。また世界で「ハーグ条約」に参加する 100 カ国（英国、フランス、ニージーランド、メキシコ、・・日本？）で利用されているとのこと（日本は、入管業務と思われる）。
- Donna Roy ディレクターは、「是非、次回のミーティングは日本で」とその拡大・普及に意欲を見せた。

【参考】
2009 年度の ARRA 法に基づく DHS の支出関係明細は下記（recovery.gov）で参照できる。
http://www.recovery.gov/Accountability/inspectors/Pages/findings.aspx?agency_code=70
なお、DHS のデータセンター統合のため、2010 年度に 150M$（130 億円）の予算を獲得したとのことである。
【参考サイト】
http://www.informationweek.com/news/government/cloud-saas/showArticle.jhtml?articleID=222002709&cid=RSSfeed_IWK_Government
http://www.fcw.com/Articles/2009/01/21/NIEM.aspx

3. EPA（2009 年 11 月 25 日午前・午後）

面談者：Dr.Brand Niemann、EPA Enterprise Architect,
Mr. Kevin Jackson（ジャーナリスト、クラウドウォッチャー）
場所：EPA 本部、Clear City, DC.

※本面談は、EPA というよりも、識者としての Dr.Brand Niemann と Kevin Jackson と米国政府のクラウドへの取り組みや、技術的な動向を議論することを目的とした。
※Dr. Brand Niemann について：もともと気象学者であり、EPA の観測データ管理などから情報分野で活躍する。2005 年から、CIO Council の下、連邦 EA のための DRM2.0 （データ管理参照モデル 2.0）の開発でリーダーシップを発揮した。その後、DRM3.0 による EPA のアーキテクチャを開発し、2008 年ころから「セマンティック Web」の開発でも発言し、68 歳という年齢ながら、現在も EPA の Enterprise Architect として、活躍している。
【参考サイト】 http://semanticommunity.wik.is/People/Brand_Niemann
Informal Presentation on Cloud Computing
Title: Semantic Cloud Computing with Open Linked Data (RDF) Technical Pattern
http://federalcloudcomputing.wik.is/

【議論の要点】

以下の見解は、EPA（環境保護庁）や連邦 CIO オフィスの公式見解ではなく、個人の意見である。全体的な参照 URL は次の通り。特に、2009 年 11 月 25 日に本出張関連の URL が掲載されている。http://federalcloudcomputing.wik.is/

- 各省庁の CIO から構成される“連邦 CIO 会議（FCIO Council）”の会長は OMB(行政管理局)の行政管理担当局長補佐の Jeffrey Zients。キーパーソンは、ビベック・クンド

ラ（Vivek Kundra）連邦 CIO 兼 E-Gov & IT 担当行政官（所属は OMB)。CTO の Aneesh Chopra(チーフ・アーキテクト)。一般調達サービス庁（GSA）の CIO の Casey Coleman。この下に、エネルギー省（DOE）の CIO 補佐官（Deputy Associate Chief Information Officer）の Peter Tseronis が位置する。その他のメンバーは次の通り。http://www.cio.gov/members/members.cfm

- 本日は、DOE の Peter Tseronis CIO 補佐官が参加できなかったので、彼のプレゼンテーション資料を基に話したい。
- クラウド・コンピューティングに関する NIST の定義は進化しつつある。クラウドは、本質的には、トップ・レイヤーの SaaS、ミドル・レイヤーの PaaS、基礎レイヤーの IaaS の 3 段階のレイヤーから構成される、“拡張性（Scalable)、サービス指向の次世代コンピューティング・プラットフォーム”である。
- クラウド・コンピューティングの長所は、IT インフラへの資本投資が最低限ですみ、消費しただけ支払うというビジネスモデルである。2 番目は、政府がひとつまたは複数のベンダーに縛られる必要がないこと。ハードウェアもソフトウェアもアップグレード費用が少なくてすむ。他のメリットは、フォールトトレランス（障害耐用性)、信頼性（Reliability)、スケーラビリティ（拡張性）である。このために、多重のデータセンターも容認され、省庁間のリソースの可用性（Availability）が増すことになる。この他にも、数多くのメリットがある。
- クラウド・コンピューティング導入戦略では、リスクの緩和が重要。クラウド・コンピューティングのリスクは、他の技術に伴うリスクと同じである。ファイアウォール、暗号化、認証、VLAN やその矢のデバイスを使いリスクマネジメントを行う。加えて、規制当局がクラウド導入のドライバーになる。クラウド・コンピューティング周辺をセキュアにすることも重要。
- 連邦政府のクラウド・コンピューティングのパイロットプロジェクトでは、GSA、DISA、National Business Center が動いている。
- 国防省（DOD）の DIA（国防情報システム局）のクラウド・コンピューティングへのコミットメントは他の省庁よりも強い。DISA では、RACE(Rapid Access Computing Environment)が事例である。RACE は、利用料が無料で、On-demand のシェアードサービスであり、他のクラウド・コンピューティング・プラットフォームと異なり、DISA 内に設置されている。DOD 関係者のみが使用可能なクラウド・システムで DOD 内コンピューティング・リソース共有化を可能にする。このコンセプトは米政府や各州のシステムにも波及する動き。特に災害時の対応に利用することが検討されている
- 内務省（DOI）の National Business Center では、トップの Douglas J. Bourgeois（元特許商標庁の CIO）がバーチャル IT サービスを提供できる IT インフラサービスを提供中である。

- 連邦政府の一般調達を担うGSA(総合サービス管理局)では、“Apps.com”を立ち上げ、連邦政府のIT調達サイトにしている。クンドラ連邦CIOの設計指導の下で、CIOのCasey Colemanが連邦クラウド計画を推進している。主な開発計画は、第1段階（2009年8月～10月）：軽量コラボレーション＆生産性ツールおよび基本インフラ・プラットフォーム（クラウド・タイプ：Commercially Available Public Clouds)、第2段階（2009年11月～2010年2月）：リッチな生産性ツール、プラットフォーム能力の拡充（クラウド・タイプ：Public and Outsourced Private Clouds)、第3段階（2010年3月～6月）：クラウド・インテグレーションサービスにおけるエンタープライズ・アプリケーション（クラウド・タイプ：Private and Hybrid Clouds)。
- オバマ政権になって、連邦CIOは、Apps.govを中核として、“Data.gov”、“USASpending.com”、“USA Recovery.gov”などの新しいサイトを立ち上げた。
- USAspending.gov ：“Federal TI Dashboard”とも呼ばれている。750億ドルのIT歳出の使い方を示したもので、各省庁の予算計画が可視化され、透明性の高い形で表現されて、連邦議会と国民への報告という性格である。ITプロジェクトのレーティングを実施（年1回、四半期毎に検証)。例えば、赤マークは問題あり、グリーンのマークは継続。ITプロジェクトの明細を2週間毎に報告。かつて、クンドラ連邦CIOがワシントンDCの市長に報告していたときと同様のスピードと形式で実行。
- Data.gov：連邦政府の行政当局が作成するデータに一般国民がアクセスできるようにしたもの。①生データ（Raw Data Catalog)、②分析ツール（Tool Catalog)、③地域別データ（Geo Data Catalog）がカタログとして提供される。これを用いてユーザーとなる市民や団体は、自由な加工や分析が出来る。当初の立ち上げ時点では、連邦データベースの利用可能性は当面、限定されている。データはカテゴリー別、機関別に検索できる。今後、国民の意見、要望を反映しながら拡充を図る。
- Recovery.gov：2009年米国復興再投資法（American Recovery and Reinvestment Act of 2009）に基づくIT投資に重点をおく景気対策予算（7,870億ドル）の透明な政府支出を、どのように使われるかまで含めて詳細に表示。

- Quality of Data（データの質）をどのように確保するかが重要。テンプレート/スプレッドシートでモニタリングや検証を行うWebsiteにアップしているが、セキュリティの問題は残っている。Enterprise Architectureも最善を尽くしてはいるが、推測を前提としたものにならざるをえない。

  註：Open Government Directive：2009年12月8日にリリース。連邦各省庁に対して、高付加価値の情報をオープンで、アクセス可能な形で一般国民に提供することを義務づけた政令。
- 現状、クラウド・コンピューティングが何を実現することができるかについては、明確にはなっていない。主な問題点は、①セキュリティ、②データ・プライバシー、③

取得プロセス、⑤標準とサービスレベル契約（SLA）など。GSA と CIO Council（CIO 会議）の中で議論されていることは、クラウド・コンピューティングのフレームワーク開発では、①セキュリティ、②調達（Procurement）の 2 つが重要課題となり、パイロットプロジェクトを推し進めようという形になり、Data.gov の開発に乗り出した。

- 米国では、クラウド・コンピューティングの普及で、①Net-Centric アプローチ、②Data-Centric アプローチ、③Content-Centric アプローチなども話題になっている。③は ID を利用したものである。NCOIC（Network Centric Operations Industry Consortium）は DOD の Net-Centric 戦略をサポートしている。2003 年 8 月にラムズフェルド国防長官による「システム中心の工業時代（System-centric Industrial Age)」から「ネット中心の情報時代（Net-centric Information Age)」への移行に対応の宣言を踏まえて、ネットセントリック戦略で、組織横断的にデータリソースを、①可視化、②アクセス可能、③理解可能（Understandable)、④高信頼性（Trusted)、⑤相互運用性（Interoperable)、⑥対応型（Responsive）にすること。

【その他の留意点】

- クラウドの定義を NIST に委託したのは、クンドラ連邦 CIO である。5 つの特性、供給モデル、利用モデルを中心に定義を進化させている。
- データの情報開示であるが、Secret、Confidential、Public という形で、情報区分を考えている。どの省庁の、どのような力のあるひとがどういう政策を作り出すかで、発信する情報の区分も異なる。オバマ大統領やクンドラ連邦 CIO の考え方は、行政当局にある情報を透明性が高くオープンな形でいかに“Public”にするかである。この Public の意味は、一般国民が知りうる公衆のための情報という意味である。したがって、Public Cloud の意味は、インターネットを介してアプリケーションやストレッジを一般大衆に利用可能とするサービス・モデルである。これは、Private Cloud が、クラウド・コンピューティング技術を使う知財権のあるネットワークまたはデータセンターと区別するために使われた用語である。
- NIST の利活用モデルの定義では、Public Cloud は、「クラウド基盤を一般大衆または大型産業グループに提供し、クラウド・サービスを提供する組織がクラウド基盤を所有する)：単純に表現すれば、パブリック・クラウドは、インターネットを通じて第 3 者のサービス・プロバイダーからクライアントに提供されるクラウド・サービスの利活用モデルである。“パブリック（public）”は、フリーまたは安価に利用できることを意味するが、いつもフリーを意味するものではない」となっている。これに対して、Private Cloud は、「エンタープライズが所有またはリースする：クラウド基盤はひとつの組織だけのために運用される。これは、当該組織またはサードパーティにより管理され、敷地内外に存在する」。米国内でも議論の混乱があったことは事実である。

コミュニティ・クラウドは、特定のセキュリティ要件や共通ミッションなどの利害を共有する組織のグループによりコントロール・利用される。コミュニティのメンバーがクラウドの中のデータとアプリケーションにアクセスできる。

- 連邦政府の各省庁にある連邦データをどのように Web 2.0 技術を使って統合化するかについては、“FEA(Federal Enterprise Architect)Evolution/Innovation Roadmap”に詳述されている（http://federaldata.wik.is/)。

【以下は、IBT 調査グループの「質問状（本報告参考資料に添付)」に対する Brand Niemann の回答である】

Q：「オバマ大統領は、連邦クラウドを推進しているが、連邦 CIO の下、これまでの進捗はいかがか？」
A：BN（Brand Niemann による回答）： 下記の page 2-3 を参照してほしい。
http://networkcentricity.wik.is/@api/deki/files/33/=BrandNiemann10222009.doc
Q:「 NIST プロジェクトの背景は、どのようなものか？」
A:BN: 連邦 CIO 議会(FCIOC)はアーキテクチャと、セキュリティ、調達などに関する最初の定義をもとめた。
Q:「その目的は、連邦政府 IT 関連コストの削減にあったのか？」
A: BN: Yes, see
http://www.whitehouse.gov/omb/budget/fy2010/assets/crosscutting.pdf
Q: 「NIST の定義の公表後、これまでに、どんな反応があったか？」
A: NIST will tell you. 15+ revisions.
Q: 「OMB や FCCI (Federal Cloud Computing Initiative)」とはどのような協力をしているか？
A: Yes, see slide 4 for how the NCOIC/OMG Cloud Computing Team can help the OMB/CIOC)
http://networkcentricity.wik.is/@api/deki/files/46/=BrandNiemann11202009_(1).ppt
NIST は、クラウドについて、次のような概念定義をおこなった。
Private Cloud, Community Cloud, Public Cloud, and Hybrid Cloud
On-demand Service, Ubiquitous Network Access, Rapid Elasticity, and Measured Service,
Service model, Deployment model,
Q：アーキテクチャと技術に関する相違は何か？　明快に定義できたのか？
A：その途上である。
Q：クラウドのタイプについては、どのようにその相違を識別するのか？
A:これも途上にある。タクソノミー、オントロジー、パッターン、など多義的で同じである
Q：政府分野において、クラウドを推進するのに、どのようなポリシーや支援が必要か？

A：先の回答と同じ。クラウド・コンピューティングは、公共部門と民間部門の両者に大きな変化をもたらす。
Q：クラウド・コンピューティングにおける将来のマーケットサイズに対する認識は如何か？
A：Kevin Jackson が回答するだろう。
Q：どんな新しい「ビジネス機会」が期待できるか？。Q：産業構造に、どのような変化を期待できるか？またどんなニュービジネスを期待できるか？
A：これも Kevin Jackson に聞いてほしい。
Q：Google は政府専用のサービスを提供するとしているが、これまでの Google サービスとどのように異なるのか？
A：これも Kevin Jackson に聞いてほしい。
Q：セキュリティ認証として FISMA 以外に、政府の要求はあるのか？
A：2009 年 6 月 15 日、Federal Cloud Symposium で、Google は FISMA の全面準拠を約束した。
Q：GSA は、調達基準と仕組みを描きつつあるが、その背景はなにか？
A： Vendor must be on Schedule 70.
Q：産業界からのリアクションはあったか？
A： 私は知らない。

標準化について；

Q：セキュリティだけでなく、どのような産業標準化が求められるか？
A ：Bob Marcus がこの分野に取り組んでいる。
【参考サイト】 http://federalcloudcomputing.wik.is, December 9th OMG Meeting.
Q：ISO, ISO/IEC JTC1OASIS, OMG, など標準化団体（SDO）とどのように調整していくつもりか？
A：同上
Q：複数のクラウドが立ち上がった時、それらの相互運用性について、現状の標準化で十分と思うか？
A： No.

セキュリティと dependability について：

Q：従来のネットワークシステムとクラウドを比較したとき、セキュリティ技術の相違はなにか？
A：私は専門家ではないが、「政府セキュリティ要求」に対する「行政サービス」における「政府データ」のあり方が問題となるであろう。
Q：米国のパトリオット法に関する懸念が取りざたされているが、政府の認識はいかがか？

A：パトリオット法は、データ管理におけるプライバシーに関するものと思う。
今週（2009年11月最終週）の会議で、この件について次の3つのカテゴリーについて触れた。
(a)「安全」;「安全な情報共有」のために「知る必要性（need to know)」から「共有する必要性（need to share)」に変える必要がある。
(b)「機密」;(Confidential:business operation data, Personal Identifiable Information, Census Data)
(c)「公共」;(V.クンドラは、「非公開の情報については、その正当性を明らかにすべき」としている).
2009年1月21日の「透明性、公開、協調に関する大統領メモ」をフォローアップする新しい方針を待っているところである。

Q：クラウドのセキュリティとディペンダビリティの分析の方法やツールが必要性についてどのように思うか？
A：そうだ。NISTが取り組んでいる。
Q：「Security as a Service」などというものも議論されていると聞いている。そのような概念をどの思うか？
A：ロッキードマーティン社が、この分野で作業している。

法的課題について：
BN：私は、この分野については、全く関与していないし、何もしていない。
ただ、将来、この分野における日米協調の可能性については、「大いにある」としただけである。

4. NCOIC（2009年11月23日午後）
面談者：Terry Morgan（NCOIC会長、Director, Network Centric Strategy, Global Government Solution Group, Cisco System, Inc.)、Kevin Jackson（Director, Business Development, DATALINE)
場所：　Cisco office, Dulles Technology Drive, Herndon, VA 20171.

註：NCOIC（Network Centric Operations Industry Consortium）とは；
2004年8月、航空・防衛・通信・情報関連の大手企業28社が結成した国際的コンソーシアムで、DODのネットワークシステム（Grid Enterprise Service：Grid ESプロジェクト）の相互運用性の推進を目的とする。成果を、まずは軍事産業に展開し、その後、民間産業に寄与していく。
【参考サイト】：http://www.ncoic.org

- 会員企業は、80 社ほどである。会員は、3 階層に分かれており会費も異なる。
  - Tier-1 メンバー (13) : BAE Systems、Boeing、Cisco Systems、Deloitte & Touche、IBM、General Dynamics、Raytheo、Norhtlop Grumman、Thales
  - Tier-2 メンバー (2) : L3 Communication, Harris
  - Tier-3 メンバー (60) : MITER, Microsoft. OMG、Rockwell Collins, ABG, AFEI など。
  - 海外からも、18 カ国（英国、カナダ、ドイツ、イタリア、仏、デンマークなど）
  - NATO 諸国の企業も参加している。

- その活動は DOD/DISA (Defense Information Service Agency) と協調して、製造業に限らず、広く産業の基盤として Net-Centric 戦略を普及することある。その戦略は、まさに「クラウド」と同じでることから、特に、クラウドの利用側面からの技術標準の開発に力を入れている。
- 特に、「Net Centric-Pattern」と呼ばれる UML モデルによるパターン群（約 100 種）は、OMG へ RFP を提出する予定である。
- DOD/DISA が OMG で、既に規格化した UPDM (Unified Profile for DODAF/MODAF) は、SOSE (System of Systems Engineering) を目標としたアーキテクチャと SysML などのプロフィールを統合したものである。既に、金融機関で適用が始まったようである。
- Net Centric-Pattern 群は、UPDM と連携して、クラウドへの関わりを示すアーキテクチャやインターフェースのプロトコルなどとして標準化を目標としている。
- もともと、DOD/DISA は、国際標準化に力を入れており、多くの国際規格開発に関与している。

- NCOIC における「相互運用性フレームワーク (NIF)」と「パンターン化」

【参考サイト】

http://networkcentricity.wik.is/Practical_Guidance_for_Net-Centric_Patterns_Developers

NCOIC Interoperability Framework (NIF™)

http://ncoic.cachefly.net/NIF/presentation/index.html

https://www.ncoic.org/technology/deliverables/nif/

- NCOIC では、「相互運用性フレームワーク (NIF)」を開発中である。NIF は政府機関、および民間企業間の相互運用性確保を目的として開発されているアーキテクチャと標準・情報要素、およびメタモデル (UML) のセットである。その目的は、あまたの規格・標準群を適切に選択し、組み合わせることにある。

- その点で、NIF は、「フレームワークのフレームワーク（Framework Of Framework)」と呼べるもので、特定な目的と相互運用可能な要素をもつサブ・フレームワークを統合することを目標としている。SOA に基づきながら低位の「サービス」群と上位の「ミッション領域（Net-Enabled Logistics, Mobile Emergency Communications Interoperability, etc)」などから構成されている。

1.6.2. 【付属資料 2：米国現地インタビューの追跡調査】

以下は、2009 年 11 月 23～26 日に本調査チームが実施した連邦政府機関に対するインタビュー調査に関する詳細な追跡調査を実施したことから得たファクトファインディングである。この付属資料 2 は、米国の非営利法人の Intellgere が本追跡調査業務を快諾し、「連邦政府のクラウド・コンピューティングのディペンダビリティおよびセキュリティに関する現地調査レポート」として英文で提出されたレポートの抄訳である。調査を快諾してくれたのは、国防省（DoD）CIO オフィスの Jerry Smith 氏である。同氏は、連邦 CIO クラウドコンピューティングカウンシルの国防省代表でもある。

①┌ 調査対象機関

- ✧ National Institute of Standards and Technology (NIST)
- ✧ Environmental Protection Agency (EPA)
- ✧ Department of Homeland Security (DHS)
- ✧ Department of Defense (DoD) - CIO Office of the DoD Executive Agent for IT
- ✧ Standardization
- ✧ Department of Energy (DOE)
- ✧ Federal CIO Council Cloud Computing Project
- ✧ Network Centric Operations Industry Consortium (NCOIC)

②┌ 主たる参加メンバー

National Institute of Standards and Technology (NIST)

- Mr. Peter Mell
- Dr. Evan Wallace
- Dr. EdBarkmeyer

Environmental Protection Agency (EPA)

・Dr. Brand Niemann

Department of Homeland Security (DHS)
・Ms. Donna Ray
・Mr. AnthonyHoang
・Mr. JefferyBiala

Department of Defense (DoD) - CIO Office of the DoD Executive Agent for IT Standardization
・Mr. Jerry Smith

Department of Energy (DOE)
・Mr. Peter Seronis

Federal CIO Council Cloud Computing Project
・Mr. Peter Seronis

Federal CIO Council Cloud Computing Project - Cloud Computing Standards Working Group・Mr. Peter Mell ・Mr. Jerry Smith

Network Centric Operations Industry Consortium (NCOIC)
・Mr. Kevin Jackson
・Mr. Terry Morgan

主な調査内容

- クラウド・コンピューティングの定義
  - ✧ グリッド・コンピューティングとクラウド・コンピューティングの概念と定義
  - ✧ Gartner グループの定義
  - ✧ Forrester グループの定義
  - ✧ Wikipedia などの記述
  - ✧ NIST の定義

- クラウド・コンピューティングについては、信頼性、データ・セキュリティ、セキュリティの法規遵守(コンプライアンス)、プライバシーなどの解決すべき問題点が多い。次の表は、クラウド・コンピューティングを巡る主な問題点と課題を一覧表にしたも

のである。

Data Security	Where is my data and who has access to it?
	How is my IP protected?
	What is the Backup & Recovery plan?
Performance Guarantee	I/O sharing may be problematic
	Network bottlenecks can make your applications slow
Service Availability	Possibility of massive outages
	Ensuring there is no single source of failure
	What is the level of up-time ?
Data Lock-In/Migration	Can applications move from one cloud to another?
	Can applications move back in-house?
Compliance	What are the laws and other regulatory obligations and impacts of my business for using cloud?
	Who is responsible for monitoring and auditing SLAs?
Business Process Mapping	Mapping the organizations business requirements to cloud applications may require large and pervasive process changes
Customization & Integration	Can cloud applications integrate seamlessly with your Legacy and home grown applications?
Infancy Stage	Not enough players yet out there....

- 連邦政府では、セキュリティが最大の懸念である。他にも、コンプライアンス、ベンダーロックイン、ポータビリティなどの懸念もある。特に、機微なデータ（Sensitive Data）は、悪意のある第3者により取得される危険性があるために、特にデータの安全性確保が重要な課題となっている。加えて、蓄積データ（data at rest）と転送中データ（data in transit）の暗号化と保護も大切である。
- 現在のWebサービス技術の標準に頼ることができない相互運用性（Interoperability）については、OMGやDMTFで標準化努力が行われている。大切なことは、デファクト標準と方法論の構築である。

【連邦政府のクラウド導入事例】

- クラウド・サービスは、顧客がバーチャルマシーンのインスタンスをレンタルしてアプリケーションを実行する場合に重視する点と能力、さらに必要なレベルのストレージとコンピュータ処理リソースに拡張できるかという点で大幅に異なるものである。アマゾン(Amazon:アマゾン・エラスティック・コンピュート・クラウド(Amazon Elastic Compute Cloud：EC2)、マイクロソフト（Microsoft：AZURE)、グーグル（Google：http://sites、google、com/site/cloudcomputingwiki//）などの例の詳細は、インターネットから一般に参照できるので、このレポートでは重複して説明しない。

- **国防省の国防情報システム局（DISA）のRACE（ラピッド・アクセス・コンピューティング環境）**：国防省（DoD）は、DISA（国防情報システム局）の提供するクラウド・サービスであるRACEが、グーグル（Google）などの民間クラウド・プロバイダーのサービスに比べて、より安全で信頼性が高いと言明している。
  - ✧ RACE（Rapid Access Computing Environment）は、70万人におよぶDOD（国防省）の職員およびSIAC、MITERなど関連企業の職員などを対象に、400万人に及ぶユーザー対して、高度なセキュリティを維持する安全な環境の中で、24時間稼働するセルフサービスのソフトウェア開発環境として提供されたプライベート・クラウドである。現在のところ、「政府発行のクレジットカード」か「軍発行のIDカード（Military Interdepartmental Purchase Request（MIPR））」の所有者に限定されている。
  - ✧ 国防省（DoD）がどこよりも早くプライベート・クラウドを導入した理由は、ブッシュ政権が、ネット中心（Net-centric）な運用により、よりアジャイル（agile：俊敏）かつ効率的なシステム運用を行うようにDoDに圧力をかけたことである。DISA（国防情報システム局）は2007年1月、共同プロジェクトとして、RACE開発に着手している。
  - ✧ RACEは、Webポータルを介して24時間の利用が可能なセルフサービスであり、数時間以内でプラットフォームのカスタマイズ・調達・受領が可能となる。政府機関のユーザーは、特定の時点でアプリケーションの開発およびテストに必要なコンピューティング・リソースだけを支払えばよい。アプリケーションが実働段階に入ると、このリソースは、DISAのデータセンターでサポートされる「コンピューティングクラウド」に戻される。連邦各省庁のユーザーはオンラインポータルを利用してRACEにアクセスし、アクセス無制限で月500ドルの料金を払うだけである。政府が発行するクレジットカードでも決済が可能でアル。ユーザー数の増加に伴い、経済的なスケールメリットから料金は低減するものと予測される。

  - ✧ RACEの特長と機能は次の通り。

表：RACEの機能と特徴

・ 24時間稼働	・ オンラインのセルフサービス
・ 需要に対応した容量	・ 月極めサービス
・ 資本投資が不要	・ 年間メンテナンス料金なし
・ 365日24時間のサービスデスクサポート	・ 必要に応じた支払いのみ
・ DISAのDECC標準プラットフォーム	・ テストサーバーは毎月/イメージによって課金
・ NIPR接続性	
・ LAMPスタック	・ DoD IA標準で開発

・ MS WindowsまたはRed Hat Linuxオペレーティング環境を選択	・ 1～4 CPU、1～8 GBメモリ、60 GB ストレージ ・ アプリケーション開発用に構成されたSTIGオペレーティング環境

- ✧ RACE は迅速なソリューションを提供することから、国防省（DoD）のユーザーは高度に標準化されたプラットフォームを、すばやく、手ごろな価格で、セキュアな利用を行うことができる。ユーザーは、スムーズな認証によるセルフサービス形式で、事前に設定された IA コントロールを得ることができ、またプロジェクトとプログラムをテスト段階から開発環境へとスムーズに移行することができる。
- ✧ コスト節減と提供時間の短縮以外にも、将来的には、省庁間のコラボレーションやサポートを容易にするアプリケーションの標準化も可能である。RACE は、基本的に全部門に標準アーキテクチャを提供し、1 回限りのソリューションに縛られるこもなく、リソースや実務担当の専門家をおく必要性もなくなる。RACE は、誰もが、「スピードと経済性のメリットが必要なら、この標準ソリューションに従うことが必要だ」と考えざるを得なくなる標準プラットフォームである。
- ✧ RACE は、民間のクラウド・サービスよりも、セキュアで安定したクラウド・コンピューティングのプラットフォームである。例えばグーグル（Google）では、高度な機能を備える Gmail およびグーグル（Google）ニュースなどが幾度もサービス停止の被害を蒙っている。RACE のユーザーには、同一基準のサービスレベル契約（SLA）を適用する結果、常に 99.999%の可用性（Availability）が実現されている。対照的に、グーグルアプリケーション（Google Apps）は 99.9%の可用性であると、Google は述べている。
- ✧ DISA は、従来型のプラットフォーム上で稼動するアプリケーションに適用したのと同一の情報アシュアランス（IA）プロセスを、クラウド・アプリケーションに適用もしている。DISA では、セキュリティ認証プロセスをスムーズに実施する方法を把握し、80 日かかっていたの時間が今では平均 40 日に代わった。情報アシュアランスコントロールを RACE プラットフォームに組み込んだため、この期間を短縮できたと語る。「我々は複数による保有と、部門内で情報アシュアランスへの関心をどのように許可するかに注目した。通常クラウド環境では、アプリケーションをラックに入れて積み上げておくことができる。これに対して我々はアプリケーションの分離を組み込んだ…。部門のポリシーは、アプリケーション、データベースおよび Web サーバーを相互に分離することだ。これらはすべて反映された」。

- ✧ DISA はそのクラウド・ベースのアプリケーションに対して全 SAS の 70 の監査を実施した。DISA には、アプリケーションを RACE プラットフォームから削除する場合、およびバーチャルサーバーとストレージメディアを一掃する必要がある場合に、厳格なデータクリーニングが用意されている。「DISA のクラウドオファリングを使用した市場に対して、他のすべてのコンピューティングサービスと同じだけのセキュリティと信頼性を与えることができる。セキュリティ は最重要項目として保持すべき項目の 1 つである…これは、同時期の他のクラウド・コンピューティングとは大きく異なる。」2008 年の RACE の運用開始以来、指揮および制御システム、護衛制御システム、および衛星プログラムを含む数百の軍事アプリケーションが、RACE 上のユーザーに与えられたバーチャルサーバーで開発されテストされた。

- **NASA ネブラ (NASA NEBULA)**：NASA（米国航空宇宙局）は2009年5月、“NASA Nebula”を立ち上げた。NASAのネブラ（Nebula）は試験的なクラウド・コンピューティングで、ブッシュ政権時代に始まり、オバマ政権下でもカリフォルニアのマウンテン・ビューに拠点を構える“エームズ研究センター（Ames Research Center)”で開発されたクラウド・コンピューティングのパイロット版である。
  - ✧ ネブラ（Nebula）は、インターネット接続のためのノードサーバだったものを拡張して、エームズ研究所内の貨物用コンテナーで構築されたクラウド・コンピューティング用のサーバーである。以前は、インターネットのノードの 1 つで、「Mae West」と呼ばれた Ames Internet Exchange（AIX）であり、現在でも、Tier 1 の ISP（Internet Service Provider）であり、「E root」と呼ばれるネームサーバでもある。同時に、そのネットワークノードにより、CENIC（Corporation for Education Network Initiative California）や Internet2 への 10 ギガ接続を可能としている。
  - ✧ ネブラ（Nebula）は、オープンソース・コンポーネントをシームレスに統合し、セルフサービス形式で、高容量の計算サービス、記憶領域およびネットワーク接続を可能とする。ネブラは、バーチャル化による拡張性の高い方法で、大容量のコンピュータ処理機能、ストレージおよびネットワーク接続性を備えて、低廉なコストと高いエネルギー効率を達成している。
  - ✧ ネブラ（Nebula）は現在、教育と一般向けのサービス提供、コラボレーションおよび一般からの入力、また NASA のミッション支援にも使用されている。ネブラ（Nebula）チームは NASA の法務部門との共同作業で、コントリビューターのコードがコントリビューターのライセンス契約の対象になり、ネブラ（Nebula）はフリーまたはリブラ（libra）オープンソースソフトウェア（FLOSS）になりえることを確認している。

- ✧ NASA の意向は、民間セクターで採用されているクラウド・コンピューティングのメリットとコスト節減を達成することにある。 ネブラ（Nebula）によって、研究者は強力で拡張性が高く、また完全に FISMA に準拠したインフラストラクチャにすばやくアクセスすることができる上、コストは自前で構築した場合より小さい。NASA はネブラ（Nebula）を使用して、任務の支援、教育および一般向けのサービスを提供し、さらにコラボレーションと一般からの入力を促進する。
- ✧ 開かれた透明な政府を構築しようとするオバマ政権の取組努力に応じて、NASA は米国民とデータを共有することができる簡単で効率のよいセキュアな方法を検討。NASA は他の連邦政府関係機関と同様に、連邦のセキュリティポリシーに準拠する必要があり、外部パートナーまたは一般人とのデータ共有のためのコラボレーション環境の形成を課題としたからである。ネブラ（Nebula）のアーキテクチャは、民間クラウドサービス・プロバイダーとの相互運用性に関してオープンデータ API のメリットを活用して、研究者がデータセットとコードを移植して、民間のクラウドで実行できるように設計されている。ホスティングをネブラ（Nebula）プラットフォームで実施すれば、NASA は安全な方法でパートナーがデータをアクセスできるようにし、高度に保護された内部ネットワークへのアクセス許可は回避される。
- ✧ ネブラ（Nebula）は、高速データ接続、完全性のあるツールセットおよび民間クラウド・プロバイダーが使用するオープンデータ API を備えており、外部の科学者や研究者とのコラボレーションを強化している。透明性と一般とのコラボレーションの原則をゼロから構築したネブラ（Nebula）は、またオープンソースプロジェクトでもある。ネブラ（Nebula）は効率性と拡張性の高いコンテナー型のインフラストラクチャで、研究者はストレージとバーチャル化インスタンスに、居ながらにして従量制の手ごろな料金でアクセスできるオンライン環境である。
- ✧ クラウドのホストになるエイムズインターネットエクスチェンジ（Ames Internet Exchange：AIX）は、以前はインターネットの当初のノードの 1 つであるメイウェスト（Mae West）で、今も Tier 1 の主要なピアロケーションであり、さらに「E」ルート名サーバーのフォームである。ネブラ（Nebula）はコンテナー型データセンターを使用して、NASA エームズ研究センター（NASA Ames Research Center）敷地内のサーバーを収容している。
- ✧ このコンテナー型センターは、高密度で温度を低く維持するために必要なエネルギーが少なく、「もっともグリーンな（環境に優しい）形態であることが実証されている。クラウド・コンピューティングの効率は、従来のネットワークまたサーバーセンターの 3 倍から 5 倍になりえる。ネブラ（Nebula）はまた、ネットワーク上のコンピュータを実際にオフにしてエネルギーを節減し、クラウド・コンピ

ューティングの効率を向上させている。ネブラ（Nebula）が従来のデータセンターのエネルギー効率より 50%高いことを示した推測もある。

- ✧ ネブラ（Nebula）およびクラウド・コンピューティングは、すべての情報およびコンピュータを 1 つのプラットフォームに統合し、統合されていない状態なら個別に保守および監視が必要なシステム数が減少するため、サイバー攻撃に対する「表面の」脆弱性を削減できる。これによって、ネットワーク上のすべてのコンピュータを最新の状態に保持することが容易になる。
- ✧ ネブラ（Nebula）に保管されている情報は、一般向けのデータのみで、現在機密上の重要な情報を保管する計画はない。ネブラ（Nebula）は、NASA が Web 上で一般と容易に連携でき、NASA のデータを一般に公開できるようにするために構築された。
- ✧ ネブラ（Nebula）のアーキテクチャは、EC2 など民間のクラウドサービス・プロバイダーと相互運用できるように設計されている。これによって、NASA の研究者はそのデータセットとコードを民間のクラウドで実行するために移植できる。ネブラ（Nebula）プラットフォームでデータをホスティングすることは、そのデータを NASA の外部パートナーにアクセス可能にする安全な方法である。

- **農務省（USDA）の全米ファイナンス・センター（NFC）**：ルイジアナ州ニューオリンズにある農務省（USDA）の全米ファイナンス・センター（NFC:National Finance Center）は、信頼性とコスト効果の高い、従業員指向のシステムとサービスを連邦の各機関に提供し、各機関が任務を遂行して国家に寄与できるようにした。NFCのユーザーベースは、政府の3つの部門のすべてを代表する140の連邦機関から構成されている。NFCは小規模および大規模利用者に同様のサービスを提供する。給与/人事の最小利用者のアカウントはわずか2つで、最大の利用者のアカウントは約14万である。NFCシステムは、各利用者固有のニーズと任務の要件に特に対応できる状態になっている。
  - ✧ NFC は、給与/人事システムを統合し、給与支払いプロセスに関連する必要な支援サービスをすべて備える。NFC は他にも次の 2 つの給与/人事関連システムを連邦政府全体に対して運用している。人事局（OPM）の連邦公務員医療保障（FEHB）および集中登録手形交換所システム（Centralized Enrollment Clearinghouse System：CLER）は、給与担当部門とキャリア FEHB レコードをタイムリーかつ正確に調整し、保険料金直送システム（Direct Premium Remittance System：DPRS）は、FEHB プログラムへの参加を選択してその対象となった非連邦公務員からの健康保険の保険料の請求と集金に使用されている。

- **内務省（DOI）の全米ビジネス・センター（NBC）**：内務省（DOI）の全米ビジネス・センター（NBC：National Business Center）は、連邦各省庁がまがいものを排し、クラ

ウド・コンピューティングがITサービスの提供形態を変える強力な原動力になることを支援している。NBCはクラウド・コンピューティングを連邦政府と関連付けることは、そのメリットを確認するだけでなく、固有のリスクを理解し重視することになると確信している。内務省のクラウドコンピューティング・プロジェクトに関する情報は、ナショナル・ビジネス・センター（National Business Center）のWebサイトで公開されている。

- **エネルギー省(DOE)**：米国エネルギー省（DOE）は、プロジェクト・マゼラン（PROJECT MAGELLAN）という3,200万ドルのクラウド・コンピューティング導入イニシアティブを開始した。これは、科学者が情報を共有し、生物学、物理学および気候変動での科学的データの共有と高度な分析など、多様な分野での発見を促進するための、コスト効果とエネルギー効率の高い方法とされている。マゼラン（MAGELLAN）は、リソースを集中し、規模による効率化を得ようとしている。このプロジェクトによって科学者はさらに大きな科学的課題の解決に向かってレベルアップし、個々のアプリケーション要件に必要とされるシステム・ソフトウェアを見極めることができるようになる。このプロジェクトには、 アルゴンヌ国立研究所（Argonne National Laboratory）とローレンスバークレー国立研究所（Lawrence Berkeley National Laboratory）が加わっている。複数のシステムから組み合わされたセットは、クラウドテストベッドを形成し、科学者がコンピュータ処理に使用するとともに、特定の研究プロジェクトでのクラウド・コンピューティングの効率もテストできる。

- **米国の連邦のポリシーとイニシアティブ**：1996年、IT管理改革法（Clinger-Cohen Act3）によって、連邦政府のトップレベルに最高情報責任者（CIO）委員会が設けられた。現在この法律は、政府行政機関の一部門である行政管理予算局（Office of Management and Budget：OMB）が集中して展開している。OMBには電子政府（e-Gov）とITオフィスがあり、局長はビベック・クンドラ（Vivek Kundra）氏、スタッフは原則としてホワイトハウス出身である。現在連邦のチーフCIOの重点は、次の主要3件のイニシアティブにある。

[3] The Clinger-Cohen Act, formerly the Information Technology Management Reform Act of 1996 (ITMRA), is a 1996 U.S Federal law, designed to improve the way the Federal government acquires, uses and disposes information technology (IT). The Clinger-Cohen Act supplements the information resources management policies by establishing a comprehensive approach for executive agencies to improve the acquisition and management of their information resources, by:
focusing information resource planning to support their strategic missions;
implementing a capital planning and investment control process that links to budget formulation and execution; and
rethinking and restructuring the way they do their work before investing in information systems.
The Clinger-Cohen Act of 1996 directed the development and maintenance of a Federal Enterprise Architecture to maximize the benefits of information technology (IT) within the Government.

- USA Spending：連邦政府の支出を一層可視化し、透明化するプロジェクトおよびWebサイト。予算750億ドルの、ITプロファイルを評定し、ITプロジェクトを投資ポートフォリオのように扱うシステムである。

- recovery.gov：「奨励」基金源に関する情報を収容するプロジェクトとWeb サイト。これには、ITプロジェクトの主要な基金（例：電子健康レコードの基金は5,000万ドル）などがあり、データの品質を検出するテンプレートがある（インタビュー時に米国の国勢調査データは非常に高品質だが、予算の作業 データは、対極的に非常に劣悪な品質のデータであることが示された)。

- data.gov：政府のデータに関するプロジェクトとWebサイト。このプロジェクトの始まりは、2009年1月21日のオバマ大統領からのメモで、そこでは「… 開かれた透明性のある、かつコラボレーションが必要 …」ということが強調されている。インプリメントの公式ガイドでは、120日以内に提供するとされていたが、まだ発行されていない[4]。

  ✧ セマンティックに使用可能になったデータコンセプトは十分練り上げられ、試験は成功裡に実施されたので、data.gov チームは連邦各省庁のデータセット内のセマンティックなマークアップを、機関がインプリメントできるように固有のガイダンスを提供していく。特にdata.govチームは、data.govサイト内のセマンティックに使用可能にされた技法を活用するだけでなく、データセット内のセマンティックに使用可能にされたデータを各機関がインプリメントすることを支援し、データセット内のデータの活用が、data.govによるだけでなく、データの他のエンドユーザーによっても一層活用されるようにする。

  ✧ オバマ政権はブッシュ政権のイニシアティブを継続しているが、それは一層強化されている。行政管理予算局（OMB）および連邦CIOオフィスは、クラウド・ソリューションへの移行の歴史があり、現在OMBは新しい体制によってクラウド・コンピューティングを連邦クラウド・コンピューティング・イニシアティブ（FCCI）として重視している。そこではプロジェクト管理オフィス、各機関にまたがるテクノロジー作業グループ、および管理体制が設けられた

  ✧ OMBは、次の3つの優先順位があることを示した。
    ① クラウド・コンピューティングのフレームワークを開発するとともに、セキュリティと調達という重要な課題を重視する。
    ② 試験プロジェクトを開発する。

[4] Current rumors indicate its publication in December

③ “data.gov”を開発する。

✧ クラウド･コンピューティングの優先順位は、連邦CIOのビベク・クンドラ氏(Vivek Kundra）にとって現在最高である。同氏は、クラウド・コンピューティングへの移行戦略について、5本の「柱」を次のように明らかにした。

① 政府のコストの低減
② 市民との連携
③ イノベーション
④ 透明性
⑤ サイバー・セキュリティ

【連邦クラウド・コンピューティング構想（FCCI)】

● ビベック・クンドラ（Vivek Kundra）連邦CIOは2009年7月15日、ワシントンDCの国立防衛大学（NDU）で開催された「クラウドコンピューティングシンポジュウム」において、連邦クラウド・コンピューティング構想（FCCI）を発表した。

✧ 連邦CIOは、中核技術としてクラウド・コンピューティングを連邦政府に導入し、連邦政府の一般調達を担う総合サービス局（GSA）内に連邦省庁向けのワンストップ・ショップである“クラウド・コンピューティングStorefront”を立ち上げ、GSA（一般サービス管理局）を“ITの重心”とし、Amazon.comのような商用オンライン購買サービスを真似て、GSA内に“連邦クラウド・ストアフロント”を設置する計画を明らかにした。

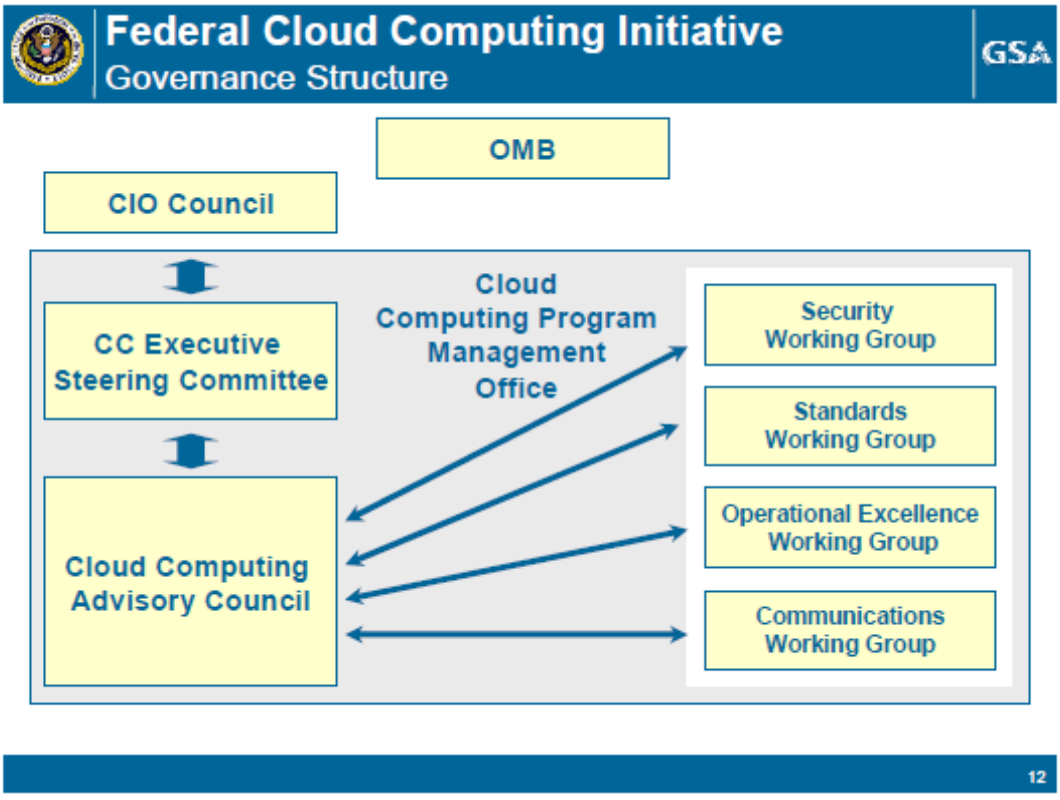
✧ 連邦各省庁は、製品やサービスがIT調達規制やサイバー・セキュリティ規則に遵守しているかどうかを気にすることなく、遠隔ストレージやホスト型アプリケーションのような技術サービスの選択が可能になる。GSAは、このサービスが2002年のFISMA（連邦情報セキュリティ管理法）を遵守していることを確実に保障し、必要なセキュリティ認証・証明を具備する。

✧ クンドラ連邦CIOは、NASAのエームズ研究センター（NASA Ames Research Center）で最近行った講演で、次のように述べている。

・ 「私どもは、政府の運用コストを低減するとともに、政府内のイノベーションを促進するために、“App.gov”を立ち上げた。連邦政府関係機関は、新しいITサービスと製品の展開に多くの難問を抱えている。調達プロセスは複雑に絡み合い時間がかかる。セキュリティ手順は、複雑でコストがかかり、連邦省庁をまたがって時間を要し重複もある。我々のポリシーは新しい動向に遅れを取り、新しいテクノロジーの使用に関して不要な制約を生んでいる。過去の余りにも多くの使用実態で、購入

したIT昨日を十分に活用できない結果が連邦政府全般にわたって起きていた。我々はこれらの障壁への対応と、政府が新しいテクノロジーを活用する手段の改善に専念する。我々はこれらを請け負ったばかりであり、クラウド・コンピューティングの潜在能力をすべて活用するまでに時間はかかるだろう（例えば10年）。“Apps.gov”は、連邦政府関係機関がクラウド・ベースのITサービスを迅速に調べ購入して生産性、コラボレーションおよび効率を向上させるための、オンラインの販売拠点である。“data.gov”と同様、“Apps.gov”は当初、規模の小さいものだが、急速に規模を拡大することを目標にしている。クラウド・サービスを拡大するには、その途上でセキュリティ、プライバシー、情報管理および調達に関連する多くの課題に対応することが必要だろう」。

図　：連邦クラウド・コンピューティング構想（FCCI）の体制



- 連邦クラウド・コンピューティング構想（FCCI）は、コスト効果が高く、クリーンで持続可能な連邦クラウド・コンピューティングのソリューションをすべての連邦政府関係機関に導入させることを目的として、次の具体的な目標を掲げている。
  - ✧　セキュリティ、標準およびガバナンスに対する連邦ポリシーの策定。

- ✧ 連邦各省庁を支援するクラウド・コンピューティングのソリューション提供。
- ✧ 戦略的ロードマップ、ベストプラクティスおよび調達ガイダンスの提供。

- ビベック・クンドラ（Vivek Kundra）連邦CIOは、政府におけるApps.govの導入は、米国の納税者に価値をもたらし、は組織を超えて政府のIT資源を利用することを安価で容易にすることで、イノベーションを引き起こすとも語っている。因みに、クンドラ連邦CIOは、2009年9月15日付の「ホワイトハウスのBlog」で、自から“Apps.gov”の立ち上げをアナウンスしている。
  - ✧ この新しい“Apps.gov”サービスは、クラウド・コンピューティングサービスを購入するためのワンストップ・サービスで、IT 基盤の持続可能性と費用対効果の改善を通じて、クラウド・コンピューティングを、調達だけでなく、政策、安全、教育訓練、調整、アーキテクチャおよび標準化に拡大する政府方針のひとつである。
  - ✧ “Apps.gov”は、IT サービスと基盤を、複数の顧客によって「共有可能」とし、物理的に異なる資源（ストレージ、プロセッシング、ネットワーク、仮想マシーンなど）を、顧客要望に沿って、動的に顧客に割り付け、貸出すものである。そのカテゴリーは、機能（CRM、データ管理、コミュニケーションなど）によって分類される。顧客としての政府機関は、プロダクトを識別し比較することが容易となり、購入が決定されると、GSA のオンラインショッピン・発注サイト「GSA Advantage」または、「eBay」を通じて購買できる。

- クラウド・コンピューティングに関する現状の連邦ポリシーは次の通りである。
  - ✧ 2005 年半ばに確立されたテクノロジーとベンダーが不可視のサービスベース環境への移行を継続する。
  - ✧ クリーンな（ストーブの煙突を開発する必要のない）テクノロジーソリューションの連邦政府への急速な展開を可能にする。
  - ✧ 既存の機能と新しい機能に対応できる拡張性を備える。
  - ✧ バーチャル化によるコスト節減を強化する。
  - ✧ インフラストラクチャ、ビル、電力および要員のコストを潜在的に削減する。
  - ✧ 透明で開かれた参加型政府を構築する連邦政府の能力を強化する。

- FY2010連邦予算によれば、2010会計年度の政府基金は、クラウド・コンピューティングへの移行について、次の目標を設定している。
  - ✧ 連邦テクノロジー環境には、テクノロジーインフラ投資の基本的な再調査が必要である。

- ✧ インフラ近代化プログラムには、新しい課題と責任を設定する必要がある。クラウド・コンピューティングを新たに強調したエンタープライズ全般にわたる共通のサービスとソリューションを明らかにするために、連邦各省庁横断的なアーキテクチャを利用するためのパイロットプロジェクトを実施する。
- ✧ 連邦政府は、そのITインフラを、データセンターのバーチャル化、データセンターと運用の統合、クラウド・コンピューティングのビジネスモデルを全面的に導入する。

- オバマ政権の連邦クラウド・コンピューティング構想（FCCI）を担うのは、GSA（一般サービス管理局）のプロジェクトマネジメント室（Project Management Office）である。連邦クラウド・コンピューティングの指針と展開を支援するため、元の「ビジネスPMO」は、クラウド・コンピューティングPMOの「ITI LoBイニシアティブ構築」として、次の重点課題を設定している。
  - ✧ テクノロジーとベンダーに依存しないサービス環境への移行を継続する。
  - ✧ ストーブ煙突を開発する必要のない連邦政府向けのクリーンな技術ソリューションの展開を加速化する。
  - ✧ 既存の機能と新しい機能に対応できる拡張性を備える。
  - ✧ バーチャル化によって節減を拡大する。
  - ✧ インフラストラクチャ、ビル、電力、および要員のコストを潜在的に削減する。
  - ✧ 透明で開かれた参加型政府を構築する政府の力を強化する。

- 連邦クラウド・コンピューティング構想（FCCI）のミッションとビジョンは、セキュアで、使い勝手の良いクラウド・サービスを可能とすることで、政府全体で調整したコスト効果の高い、クリーンで持続可能な連邦クラウド・コンピューティング努力を実施することにある。主なミッションは次の通りである。
  - ✧ 迅速かつ簡素な調達・認証プロセス。
  - ✧ コンピューティング・リソースを弾力的な従量制で提供。
  - ✧ 移植性が高く、再使用可能で相互運用性のあるビジネス指向のソリューションを提供。

- 連邦クラウド・コンピューティング構想（FCCI）のゴールは、連邦各省庁のミッション履行を支援し、高い信頼性およびセキュリティを確保した安全なサービスを提供する一方、最適化されたコスト効果の高いITインフラ（ITI）を実現することである。PMOは政府全般わたるITインフラ（ITI）最適化ビジョンを次のように決めている。
  - ✧ 23の連邦省庁のコラボレーションによる管理フレームワークを構築する。
  - ✧ 次の重要な情報を収集・分析する。

○ 最適化戦略
○ 共通ソリューション
○ パフォーマンス測定
○ 政府全般で使用するITインフラストラクチャーツール

✧ 連邦 ITI データのベンチマークを実行する。

- 連邦クラウド・コンピューティング構想（FCCI）は、ITILoBの取り組みの中で収集した情報を使い、クラウド・コンピューティングのテクノロジープラットフォームを使用した「共通ソリューション」を次の原則で展開する。
  ✧ サービス指向アプローチを遵守すること。
  ✧ 連邦省庁のニーズに基づくこと。
  ✧ コラボレーションによる管理フレームワークを保持すること。

- ビベック・クンドラ（Vivek Kundra）連邦CIOは、「オープン政府指針（Open Government Directive)」のを2009年12月8日に発表した。本原稿執筆段階では、ドラフト案に基づいて概要を記載していることから、本項では、本文に基づいて加筆訂正を行っている。以下のURLを参照されたい。2009年12月18日付けのオープンガバメント指針（Open Government Directive）は、伝統的な閉ざされた政府から透明の高い、オープンな政府へ移行するための連邦政府指針に関するメモである。
  ✧ このオープンガバメント指針は、2009 年 1 月 21 日にオバマ大統領が OMB（行政管理予算局）に指示した透明かつオープンな政府に関するメモに基づくオープン政府指針の策定命令に基づいて策定されたものである。
  ✧ オープン政府指針の 3 つの原則とは、透明性(Transparency)、参加(Partipation)、協働（Collaboration）である。

- このオープン政府指針メモは、連邦各省庁に対して、よりオープンな政府を創造する目標に向けて次のステップを講じるように要請している。主なステップ内容は次の通りである。

  ① オンライン政府情報の公開：連邦各省庁は、連邦記録法（FRA）およびその他の法規則に準拠してオープンフォーマットでタイムリーなオンライン政府情報へのアクセスを拡充すること。具体的には、次の他に多数の要望を盛り込んでいる。
  ✧ 連邦各省庁は 45 日以内に、ヘルスケア、教育、エネルギー関連を含む価値の高い」データセットを最低でも 3 つを特定し、“Data.gov”を通じて、オープンフォーマットでオンライン公開・登録すること。

✧ 連邦各省庁は60日以内に、オープン政府のWebページを“http://www.[agency].gov/open”ttp://www.[agency].gov/open”内に立ち上げること。

② 政府情報の質の向上：一般国民に利用可能な政府情報の質を改善するために、各省庁の幹部はOMB（行政管理予算局）の情報の質[5]に関する指針を順守すること。

③ オープン政府カルチャーの創出と制度化

④ オープン政府の政策フレームワークの策定

- オープン政府指針メモでは、連邦各省庁に対してオープンフォーマットによるオープン政府計画の策定と公開を付属書として要請している。この計画策定では、①各省庁の政策、法律、技術を担当する幹部と②一般国民とオープン政府専門家の意見を反映し、具体的な行動を盛り込むことを求めらている。

- 連邦クラウド・コンピューティング構想（FCCI）の進捗状況の概要は次の通りである。
  - ✧ 連邦省庁の各CIOと幹部から構成される連邦クラウド・コンピューティング執行委員会（FCCESC:Executive Steering Committee）を設置すること。
  - ✧ クラウド・コンピューティングPMOをGSA（一般サービス管理局）CIOオフィス傘下に設置すること。
  - ✧ 次の4つの主要分野のワーキンググループ（WG）を設置すること。
    - セキュリティWG：管理、集中管理（CC）サービスの政府全般のセキュリティ認証、問題とソリューション、最善の手法、セキュリティ標準、RFQ(見積要求仕様書)の検証。
    - 標準WG：共通サービス、クラウド・コンピューティングのアーキテクチャ、ポート、標準、RFQ(見積要求仕様書)の検証。
    - 運用WG：調達手段の確定、クラウドのストアフロント、パイロット活動、ビジネスケースのテンプレート、パフォーマンス・メトリックス、省庁ガイド、政府全般のサービス、共通インターフェース
    - 通信WG：アウトリーチ、通信計画、セントラル・ポータル、オンライン・コンテンツ、研修用コンテンツ
  - ✧ 連邦クラウド・コンピューティング執行委員会（FCCESC）は、IaaSおよびSaaSの大手サービス・プロバイダーの経営幹部と話し合いを行い、民間業界による連邦政府のニーズと要求事項の受け入れ準備と実現性を検討すること。

[5] The Federal Government has defined quality and objectivity in, “Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies” (67 FR 8452). Quality is “…the encompassing term, of which ‘utility,’ ‘objectivity,’ and ‘integrity’ are the constituents.” “‘Objectivity’ focuses on whether the disseminated information is being presented in an accurate, clear, complete, and unbiased manner, and as a matter of substance, is accurate, reliable, and unbiased.”

- 連邦クラウド・コンピューティング執行委員会（FCCESC）は、連邦クラウド・コンピューティング構想（FCCI）向けに不可欠な管理・監視体制を整備すること。主な重点課題は次の通り。

  - ✧ ガバナンスの策定と管理。
  - ✧ クラウド技術革新の促進。
  - ✧ 調達を主導。
  - ✧ 集中管理（CC）の導入と実施。
  - ✧ 持続可能かつコスト効果の高いコンピューティングの確立。
  - ✧ サービス・プロバイダーとしての運用。
  - ✧ アウトリーチ活動の実施

以上の連邦クラウド・コンピューティング導入加速の流れの中で、今回の経済産業省の委託調査を受けたチームによるインタビュー調査では、次のポイントが確認された。

- 災害復旧とベンダーロックインの回避は、連邦政府向けアプリケーションの代替クラウド・モデルを評価する上で重要な2つの要因である。本インタビュー調査では、連邦クラウド担当の政府代表は、セキュリティ、コンプライアンス（法令順守)、ベンダーロックイン、ポータビリティ（移植性）の4つが連邦政府によるクラウド・コンピューティングの導入に際しての重要な課題であるとの強調を繰り返している。

- 加えて、本インタビュー調査では、連邦政府のクラウド担当代表は、相互運用性（Interoperability）の標準化ニーズも高いと指摘している。クラウド・コンピューティングの標準化に関する議論では、セキュリティの標準規格のニーズが高いことも明らかになった。一方、クラウド・コンピューティングのプロビジョニング（ニーズ対応の備え）とプラットフォームを標準化することは極めて難しいが、機能標準の基盤構築は実行しやすいとの意見が多勢を占めた。ソフトウェア・サービスの標準については、最も実現が難しいという見解であった。NIST（国立標準研究所）の連邦クラウドWGは、クラウド・コンピューティングについての標準ロードマップの構築作業に取り組んでいる最中である。

- セキュリティとデータ・センシティビティ（機微性または機密性）についての議論では、TS-SCI（Top Secret Sensitive Compartmented Information)、SEC（Secret)、SBU（Secret But Unclassified）およびUNCLASS（Unclassified）の4段階の政府情報の分類カテゴリーを認識することが重要であると同意した。ただし、この他にも、機微性

（Sensitivity）に関しては、多くのカテゴリーや分類法が米国に存在することも議論された。データの重要性は、固有のセキュリティ要件とソリューション判別の重要な要因である。データ・センシティビティ（機微性または機密性）は、特定のセキュリティ要件とソリューションを決める際に極めて重要である。米国政府のデータ・センシティビティの検討では、音楽などのDRM（デジタル権利マネジメント）と類似の議論が重なることも示唆された。暗号化とDRMとは、適切な管理を行うべきもので、正確なデータの部分にだけマークを付ける適切な柔軟性を確保する必要がある。データのタグ付けは、蓄積データ（data at rest）と転送中のデータ（data in transit）に必要となるが、データ移動にはメタデータの移動が必要となり、この標準化ニーズは極めて重要である。

- 本インタビュー調査に対応した連邦政府の関係者は、「政府のセキュリティ要件」に合致する「政府データ」が「政府のサーバー」上に置くべきだと結論している。データ管理のプライバシーに関しても懸念が表明された。このアプロー方法は、次の3つに分類される。① “知る必要がある（need to know)”から、“セキュアな情報共有（secure information sharing)”を“共有する必要がある（need to share)”へと転換するセキュア（確実に保証される）な軍隊、諜報機関および法執行当局、②機密を要するオペレーション・データや、個人のID情報、 国勢調査データ)、③一般公開情報（「連邦各省庁は、一般公開情報に該当しない政府データの根拠を示す必要がある」と、クンドラ連邦CIOは述べているた)。

- 国土安全保障省（DHS）では、2年前のブッシュ政権の時代に、連邦各省庁のデータセンターを統合化する作業に着手している。19ヵ所のデータセンターを1つのデータセンターに統合化する動きは進展しつつある。

【要約】

- クラウド・コンピューティングとは何か。その実装の方法と場所はどこか。また、クラウド・コンピューティングに伴うビジネスチャンス、問題点と課題など、クラウド・コンピューティングを巡って、米国でも混乱と議論が生じている。

- 何をクラウド・コンピューティングとみなし、何をグリッド・コンピューティングとみるかについても多少の混乱がある。一般的に、グリッド・コンピューティングは、大規模なタスクを履行して、ITサービスの消費量を計測する超大型のコンピューティング・リソースの集合を繋ぐものとみなされ、クラウド・コンピューティングのITパラダイム変革を引き起こした技術である。

- 既存のクライアント/サーバー技術のソリューションでは、現代の大企業や巨大な組織で必要とされる複雑で堅牢な情報システムを求めるニーズを効果的に満たすことはできない。WebベースでITサービスを提供するパラダイムとモデルであるクラウド・コンピューティングへと移行しつつある最新の動向を観察すると、クラウド・コンピューティングの基底にある技術（Web、Webサービス、シン・クライアント、グリッド、セマンティックWeb、オープンソースソフトウェアなど）の収れん化したものがクラウド・コンピューティングだともいえる。クラウド・コンピューティングの推進力は、上記の最新技術の導入動向とグローバルな経済環境の低迷にある。

- クラウド・コンピューティング自体はテクノロジーではない。クラウド・コンピューティングとは、実務面では、仮想化を可能にする様々な技術要素と、コンピュータリソースを組み合わせて、ダイナミックな個別ニーズへの対応が可能なセキュアなバーチャル力にできる関連技術から生じたオンラインビジネスサービスであるとみなすが最善である。現状では、クラウド・コンピューティングはデータセンターの統合化の中で最も利用されているようである。

- 多くの専門家は、クラウド技術を、まだ未成熟な技術とみなしている。また、大半の企業や組織は、クラウドの持つ問題点と課題の解決を望みつつも、対象を絞り込んだ小規模なプロジェクトやアプリケーションを試験的に行い、注意深く検証しつつあるのが現状である。

【結論】

- クラウド・コンピューティングは、混乱と議論をもたらす未成熟な段階にあるが、早いテンポで成長と拡大を続けている。近年、クラウド・コンピューティングは実現が可能となった。最近になって、Web、Webサービス、シン・クライアント、グリッド、セマンティックWeb、オープンソースソフトウェアなどの技術の収れん化により実現可能となったのが、クラウド・コンピューティングである。

- クラウド・コンピューティングはかつてない機会をユーザーにもたらしている。ユーザーは、ハードウェアやソフトウェア、サービスに投資しなくとも、使った分の料金だけをクラウド・プロバイダーに支払うだけで済むためである。電気や水道などの慮金と同じ方式か、定期購読の新聞や雑誌のように加入ベースの購読料にように料金支払いを行うために、先行投資が発生しない。クラウド・プロバイダーによっては、電気料金の方式ではなくて、月額定額制でサービス料金を請求するモデルもある。

- クラウド・コンピューティングは、地球規模での持続可能性を支え、環境面の責務に貢献するグリーン技術ともみなされている。

- オバマ政権は、クラウド・コンピューティングへの移行に対するブッシュ政権のイニシアティブを引き継ぎ、重要課題として取り組んでいる。OMB（行政管理予算局）と連邦政府CIOオフィスは、クラウド・ソリューションへの移行実績を示し、重要な課題である連邦政府クラウド・コンピューティング構想（FCCI）に取り組んでいる。

- 本インタビュー調査にける経済産業省の委託を受けた調査チームによるリサーチ手法は、論理的で、念入りに考え抜かれた包括的かつ完璧な調査方法であった。細部を詰めたうえで、事前に調査計画を立て、連邦政府の適切な代表メンバーとのインタビュー調整を行ったために、米国側も快く対応したことから、本調査チームは、連邦政府連邦政府クラウド・コンピューティングのディペンダビリティ（高信頼性）＆セキュリティを巡る一連の問題点と課題に関する詳細な議論を成功裏に実施できた。本レポートは、今後の継続的な意見交換と対話を重要視して、関係者の努力の成果として生まれたものである。

1.7. 業界団体におけるクラウド・コンピューティングの取組動向

表：主なクラウド業界団体の一覧表

団体名称 （発足日）	設立の目的と 活動内容	参加企業
OMG （1989 年）	オブジェクト指向の概念と技術を利用して、異なった機種でも統一されたコンピュータの操作環境を実現する目的で発足された非営利の国際的コンソーシアム。	Accenture, BAE Systems, Boeing, CA, Fujitsu, GSA, HP , Hitachi, Microsoft, SAP など多数。
Open Cloud Manifesto （2009 年 3 月）	クラウド・コンピューティングの相互運用性の確保。	IBM, Cisco, Red Hat, SAP,VMWare, ノースカロライナ州立大学など 300 社以上。
Open Cloud Consortium （2009 年）	クラウドの標準インターフェースの確立。	IBM、OMG、Sun Microsystems、VMware、Cisco、EMC、SAP、AMD、Elastra、Akamai、AT&T、Siemens、Novell、トレンドマイクロ、など 38 の会社・団体。
Open Cloud Standards Incubator （2009 年 7 月）	インターフェースの互換性	Cisco、HP、IBM、Microsoft。VMWare など 13 社。
Cloud Security Alliance （2009 年月）	セキュリティ	eBay,ING,DuPOnt,HP,Sun,Dell,Intuit ,Salesforce.com など
Jerico Forum （2008 年 12 月）	セキュリティ	ユーザーとベンダーの双方で組織。IBM、Symantec、Boeing、AstraZeneca、Qualys、British Petroleum(BP)、Eli Lilly、KLM、Gap、Gemini、Motorola、Hewlett Packard など 500 以上の企業が参加
Cloud Work Group （2009 年 8 月）	The Open Group により設立された委員会。エンドユーザーとプロバ	

	イダー双方の共通理解を深めるのが目的	

1.7.1. OMG によるクラウド標準開発の提案

2009 年 7 月 13 日にバージニア州アーリントンで開催された「クラウド標準サミット（Cloud Standards Summit)」の円卓会議で、オブジェクトマネジメントグループ（OMG）は、Distributed Management Task Force (DMTF)、Open Grid Forum (OGF)、Storage Networking Industry Association (SNIA)、Open Cloud Consortium (OGC) および Cloud Security Alliance（CSA）の IT 技術標準開発団体と共同歩調で、クラウド・コンピューティングおよびストレージの標準化活動を連携していくと発表した。

クラウド標準サミットの目標は、政府 IT 担当高官との対話を開始し、政府クラウド・コンピューティング路上の障害を取り除く標準化活動の調整を行い、連邦クラウド・コンピューティング利活用を遅らせる主要な論点に関するフィードバック情報を提供することであった。主な問題点は、セキュリティ、ガバナンス、サービスレベル契約（SLA)、クラウド横断的なポータビリティ/相互運用性、コンプライアンス（法令遵守)、レガシーシステムインテグレーション、API、仮想化リソース管理などである。

OMG をはじめとする IT 技術標準開発団体（SDO）は、誰でも参加できるワーキンググループ（WG）を設置し、確実に重要な標準ニーズに対応してもらうために、政府や企業の IT リーダーの参加を誘致する。このワーキンググループ（WG）は、Networked Resources Management（SCRM）ワーキンググループにおける既存の標準開発団体コラボレーションから発展したものである。この WG への参加団体は既に各団体が書き込める wiki ページを創設し、SDO（標準開発団体）の各代表は wiki の更新を担当する。

以下は、クラウド・コンピューティング標準に向けて共創するワーキンググループの意義を語る SDO（標準開発団体）の各代表のコメントである。

- 「OMG は、クラウド・コンピューティングを含む複雑なビジネス課題に対応するモデリングに基づくソリューションの提供をコミットメントしている。クラウド・コンピューティングは主に経営判断における運用経費対資本コスト（operating expense vs. capital expense）の問題であるが、これは標準を通じたビジネスプロセスの最適化にフォーカスしたビジネスエコロジー（Business Ecology）という OMG のビジョンに適合するものである」と、オブジェクト指向や UML の活動範

囲をクラウド・コンピューティングの標準化活動の連携にまで拡充するOMGのリチャード・ソーリー（Richard Mark Soley）会長兼CEOは語る。

- ✧ 「Cloud-standards.orgは、クラウド・コンピューティングの世界で不可欠な協調メカニズムを提供するものだ。OGFはこの場を活用してエンドユーザー、開発者、ベンダーなどのすべてのクラウド利害関係者のために拍車をかけたい」と、Open Grid Forumのクレイグ・リー（Claig A. Lee）会長は述べている。
- ✧ 「DMTFは多くのSDOs（標準開発団体）との提携プログラムを通じた協力関係を構築し、この連携により、仮想アプライアンスの標準規格であるOVF（(Open Virtual Machine Format)」(Open Virtual Machine Format)」）のようなDMTF標準を策定した」と、DMTFのウィリアム・バンパス（Winston Bumpus)会長は語る。「最近設立したDMTF Open Cloud Standards Incubatorでも、DMTF標準とSDOsや業界団体の標準との間で、活動の重複を発見して標準間ギャップを見つける協調作業はますます重要となっている」。
- ✧ 「ストレージと情報技術（IT）の進展を主な役割とするSNIA（Storage Networking Industry Association）では現在、複数のSDOs（標準開発団体）および業界団体から協力・支援を得てクラウドストレージタクソノミー（分類)、クラウド参照モデルとCloud Data Management Interface（CDMI）仕様の定義を行いつつある」と、SNIA副理事長でSNIA Cloud Storage委員長を務めるヴィンセント・フランチェスキーニ（Vincent Franceschini）は語る。「私どものクラウド・コンピューティング標準化連携こそが、既存のストレージやコンピューティング標準を補完するとともに、新しいクラウド・ストレージの業界標準が新製品やサービスとしてリリースされ普及していくための成否の鍵を握る」。
- ✧ 「今回のコラボレーションにより、大型データクラウドおよびクラウド間通信の標準を開発しつつあるOCCの努力を梃子として利用して他分野での標準化努力とのシナジー効果を期待している」と、Open Cloud Consortium（OCC）のロバート・グロスマン（Robert Grossman)会長は語る。
- ✧ 「クラウド･コンピューティングサービスの信頼性(Trust)を高めていくことが、クラウド発展の重要なカギを握る」と語るCloud Security Alliance（CSA） の共同創立者ジム・リーヴィス（Jim Reavis)は、「CSAが、クラウド・コンピューティングのセキュリティを保護し、信頼される業界のベースラインを創出するベストプラクティスの普及を奨励する努力を払う」。

OMGのアンドリュー・ワトソン（Andrew Watson）副会長（技術担当）によると、「クラウド・コンピューティングを歓迎する期待は大きいが、その用語についての情報や合意がなされていない。・・・中略・・・OMGがIT技術標準開発団体と連携するのは、専門用語集を作成し、ユーザー企業や政府、プロバイダーの間で一貫性のあるものにするである」。この

ワーキンググループは、サービス、相互運用性およびセキュリティの利活用とコンフィギュレーションに的を絞り込んだ仕様書作成でも連携する。日常のやりとりは、wiki ページと e メールで行い、会議は四半期毎に行うようである。OMG の技術的貢献としては、特にサービスレベル契約（SLA）などのクラウド利用もモデリングになる公算が高いと、ワトソンは語る。

- 主な円卓会議の講演内容

1. Morning Session 9:30 - 12:00
▪ Introduction and goals of the Summit ▪ NIST's perspective on Cloud Computing Standards ▪ Report on May 6 Federal CIO Cloud Working Group Meeting including key concerns. Discussion of the Unified Cloud Interface (UCI) project ▪ Comment by Richard Soley: MDA versus Semantic Ontology? ▪ Feedback from Federal CIO on Cloud Computing issues ▪ Vivek Kundra: My number one goal is to stop building silo'ed IT infrastructures in order to save money in the 2010 budget. ▪ Description of new initiative. ▪ General Discussion
2. Afternoon Session 1:00 - 6:00
▪ DMTF Standards: A Foundation for Managing Cloud Computing Environments ▪ SNIA Cloud Storage Reference Model and Standards ▪ Open Cloud Consortium: Update on Recent Activities including Benchmarks and Interoperability ▪ Open Cloud Computing Interface (OCCI) for portability and interoperability across Clouds ▪ Best Practices for Security in Cloud Computing ▪ Cloud Computing Standards: Status, Needs and Prospects ▪ Telecom initiative on Cloud Computing ▪ OMG Cloud Computing Standards: Building a Multi-View Specification ▪ Prepare report for NDU Cloud Computing Symposium on July 15 Richard Soley
Cloud Standards Groups Summit Participants:（4 月 29 日時点での参加予定組織）
▪ Open Grid Forum's Open Cloud Computing Initiative ▪ Cloud Security Alliance ▪ Open Cloud Consortium ▪ Storage Networking Industry Association ▪ Object Management Group

- Cloud Computing Interoperability Forum
- Organization for the Advancement of Structured Information Standards (OASIS)
- Network Centric Operations Industry Consoritum (preliminary)
- Distributed Management Task Force's Open Cloud Standards Incubator (preliminary)

●主たる講演者一覧

- Dr. Robert Childs, Senior Director, IRM College
- Vivek Kundra, Federal Chief Information Officer
- Dave Girouard, President, Enterprise, Google
- David Wennergren, Deputy Assistant Secretary of Defense for Information Management, Integration, and Technology & Deputy Chief Information Officer
- David Cearley, Vice President & Gartner Fellow, Gartner
- Erich Clementi, Vice President, Strategy & General Manager, Enterprise Initiatives, IBM
- Russ Daniels, Vice President & Chief Technology Officer, HP
- Richard Soley, Chairman and CEO, Object Management Group
- John Garing , Director, Strategic Planning & Information, DISA
- Matt Quinn, Senior Vice President-Engineering & Chief Strategy Officer, TIBCO Software Inc.
- Kevin L. Jackson, Vice President of Dataline, LLC and Editor of eMagazine "Government Cloud Computing"
- Randy Garrett, Director of Technology Integrated Intelligence Program, NSA
- Alfred Rivera, Director, Computing Services, DISA
- Hal Stern, Sun Microsystems VP Global Systems Engineering
- Srinivas Polisetty , CSC, Director - Strategic Initiatives
- David Hunter, VMware, CTO, Public Sector
- Sushil Kumar, Oracle , VP Product Strategy & Business Development
- Pat Arnold, Microsoft, Federal CTO
- Curt Aubley, Lockheed-Martin, CTO Operations & Next Generation Solutions
- John Shea, Enterprise Services Integration, OSD

1.7.2. オープンクラウドマニフェスト

2009 年 3 月 30 日、クラウド・コンピューティングの相互運用性の確保を目指すベンダー各社は、クラウドの定義と課題、6 つの原則を示した「オープンクラウドマニフェスト (Open

Cloud Manifesto)」というオープン・クラウドの宣言文に署名し、専用サイトを立ち上げて本文を公表した。

参加したのは、IBM、OMG、Sun Microsystems、VMware、Cisco、EMC、SAP、AMD、Elastra、Akamai、AT&T、Siemens、Novell、トレンドマイクロ、Rackspace、RightScale、GoGrid など 38 の会社・団体である。EC2（Elastic Compute Cloud）を展開する Amazon や Google、Azure クラウド・プラットフォームを立ち上げたマイクロソフトは参加していない。

クラウド・コンピューティングを巡る騒動と混乱が熱を浴びている最中に、この宣言文が発表されたのである。クラウド・コンピューティングとは何か。何をもってクラウド・コンピューティングとみなすのか。その実装方法はどうするのか。データの保管場所はどう確保するのか。クラウドによるビジネスチャンスはどのようなもので、問題点とリスク要因は何かなどを巡り、今も米国では混乱と議論が続いている。

このオープンクラウドマニフェスト（Open Cloud Manifesto）では、クラウド・コンピューティングの基本的な概念と定義は、グリッド・コンピューティング、ユーティリティ・コンピューティング、SOA、Web 2.0 などの多数の技術の集積であるが、正確な定義を巡っては議論が続いていると断言する。しかし、より重要なことは、クラウド・コンピューティングの主な特性は、次の 4 つのコア価値の提案（Value Proposition）だと宣言する。

⑤ オンデマンド拡張性（Scalability On Demand)。
⑥ データセンターの合理化（Streamlining Data Centers)。
⑦ ビジネスプロセスの改善（Improving Business Processes)。
⑧ 起動コストの最小化（Minimizing Startup Costs)。

クラウドの利活用はユーザー法人に莫大な収益機会とバリューをもたらすが、セキュリティ、インテグレーションなどの通常の IT 要求事項も適用しなければならない。加えて、クラウドは、同じハードウェア上に複数のユーザー企業の情報を保管するマルチテナント特性があるために、クラウド・コンピューティング導入に際しては、解決すべき次の 5 つの課題と障害もある。

① セキュリティ：大半のユーザー法人は、自前のデータとアプリケーションを自己コントロールしないシステム上に保管（ストレージ）することに安心できないものである。作業負荷（Workload）を共有インフラにマイグレーションすると、不正アクセス（Unauthorized Access）とリスク・エクスポージャの危険性が増すことになる。認証、ID 管理、コンプライアンス（法令遵守）およびアクセス技術の重要性が

高まることになろう。クラウド・プロバイダーは、透明性の高いオペレーションを行う必要性がある。

② データおよびアプリケーションの相互運用性（Interoperability）：データとアプリケーションの両方が標準インターフェースとシステム連携していることが重要である。組織のファイアウォール内にあるパブリック・クラウド、プライベート・クラウド、旧来型の IT 環境の如何にかかわらず、組織は、相互に運用するデータとアプリケーションで可能になるニューソリューションを生み出したいと願うものである。クラウド・プロバイダーは相互運用性の標準をサポートしなればならず、それによって、法人組織はクラウド・プロバイダーの能力を自らのソリューションへと結実させることができる。

③ データおよびアプリケーションのポータビリティ（Portability）：標準がなければ、内部システムに逆戻りするか、あるいは他のクラウド・プロバイダーの乗り換えることも、知財権を持つインターフェースの制約に阻まれてしまう。組織がひとたびクラウド・プロバイダーのサービス提供を使うシステムを構築または利用すると、自前の内部システムに逆戻りするのは難しく、コストも割高になる。

④ ガバナンスと管理（Governance and Management）：IT 担当部局が旧来型のデータセンターでクラウド・ソリューションを導入すると、新たな課題が生まれる。共有クラウド基盤のライフサイクルマネジメント、ライセンシングおよびチャージバックは、クラウド・プロバイダーが共同で解決すべきガバナンスおよび管理問題のひとつである。

⑤ 計測と監視（Metering and Monitoring）：経営首脳は自社の IT ソリューションでは複数のクラウド・プロバイダーを利用したく、ソリューション全般のシステムパフォーマンスをモニタリングする必要があろう。クラウド・プロバイダーは、クラウドでのアプリケーションとサービスのパフォーマンスをモニタリングするフォーマットを提供し、既存のモニタリングシステムとの互換性を保つ必要がある。クラウド・コンピューティングを効果的に使うものには明らかに収益機会が大きいが、それには、リスクと障害が伴う。クラウド・プロバイダーが確実にクラウドをオープンにすることを保証する場合に限り、クラウド・コンピューティングの価値を十分に味わうことができるということが、私どもの見解である。

顧客は、自らが利用するクラウド・サービスが他の IT と同様にオープンであることを期待する。オープン・クラウドが現実のものになれば、経営首脳の受ける恩恵は大きい。したがって、オープン・クラウドの目的は、次の通りである。

① 様々なプロバイダーやアーキテクチュアを使うことができる選択（Choice）

② 異なるクラウド・プロバイダー間の相互運用性を確保できる柔軟性（Flexibility）

③ ハードウェアとソフトウェアの拡張性を可能にするクラウド・コンピューティングの価値提案を組織変更があっても対応できるスピードと敏捷性（Speed and Agility）
④ 専門分野の限られるIT専門家でも少ない新技術で人材確保が可能となるオープン・クラウドのスキル

- オープン・クラウドの原則：クラウドの各Capabilityのための標準を定義し、単一の同質的なクラウド環境を創出ことは我々の意向ではない。クラウドがオープンなもので、選択、柔軟性と敏捷性を提示することを確保するために、複数の重要な原則を遵守したいとして、次の6つの基本原則を提議している。

① クラウド・プロバイダーは協力して、オープンなコラボレーションと適切な標準の利用により、クラウド導入上の課題（セキュリティ、インテグレーション、ポータビリティ、相互運用性、ガバナンス/管理、計測と監視）に取り組まなければならない。
② クラウド・プロバイダーは、市場における立場を利用して顧客を自社の特定プラットフォームに縛りつけことや、顧客によるプロバイダーの選択を制限することを行ってはならない。
③ クラウド・プロバイダーは、現存する標準が適切な限り、現行標準を利用・採択する必要がある。IT業界は現行標準と標準団体に極めて大きな投資を行ってきたことから、この複製や改変は不要である。
④ 新たな標準（または、現存する標準の調整）が必要になれば、過多な標準を策定しないように適切かつ現実的に対応しなければならない。標準は確実にイノベーションを促進し、イノベーションを阻害するものではないことを保証しなければならない。
⑤ オープン・クラウドを巡るいかなるコミュニティの取組努力も、クラウド・プロバイダーの技術ニーズではなくて、顧客ニーズ主導で行うべきであり、実際の顧客ニーズに対する試験・検証を行わなければならない。
⑥ クラウド・コンピューティングの標準開発団体、支持団体およびコミュニティは協働関係を維持し、利害の相反や衝突をしないように留意すべきである。

ところが、上記のオープンクラウドマニフェスト（The Open Cloud Manifesto）の策定プロセスに対して、マイクロソフトのスティーブン・マーティン（Steven Martin）は、クラウド・コンピューティングにおける相互運用性の原則とガイドラインを定めようとする考え方には賛同するが、今回のマニフェストはオープン性に欠けており、閉ざされたプロセスで秘密裏に作成されたものだと批判し、Wikiのようなオープンなメカニズムを介して公開の議論とコメントを求めるべきであるとコメントしている。

また、Amazon.com の広報担当者によれば、このマニフェスト文を耳にしたのはつい最近のことであるとし、他の標準や慣行と同様の考え方で、オープンクラウドマニフェスト（The Open Cloud Manifesto）を検証するとコメントしている。

Salesforce.com は、クラウド相互運用性の目的を支持し、マニフェストに署名した企業と連携するとともに、Google、Amazon および Facebook のパートナー会社との協力も継続することを期待する表明している。クラウド・プラットフォームは、レガシーなクライアント／サーバシステムに比べ、よりオープンであり、オープンであるべきだと確信するとコメントしている。

また、当初はマニフェストに署名した Cloud Computing Interoperability Forum（CCIF）も、3 月 29 日付ブログ投稿でこの取り組みから手を引いたことを明らかにしている。

「我々はマニフェストの内容や、真にオープンなクラウドを目指すという精神には深く賛同していたため、今回の決断を下さねばならなかったのは非常に残念である。しかし彼らは、オープン性やプロセスの公平性をあからさまに押しつけてきた。これでは CCIF としても、同マニフェストを誠心誠意支持することはできない」との見解を CCIF のブログに投稿している。Google は、「当社は同マニフェストには関与していないが、（中略）あらゆるベンダー、あらゆるデータとの相互運用性について、オープン性を保っていくつもりだ」と述べている。しかし、直接的に利害関係を持たない専門家は、このマニフェストを好意的にとらえている。Redmonk のアナリストであるステファン・オグレイディ（Stephen O'Grady）の意見によると、マニフェストそのものは「野心的でありつつも、正しい方向を向いた現実的なもの」と評価し、「現状を放置して数年後、特定のベンダーに取り込まれ、金を搾り取られるか、今この段階で問題に立ち向かうかのどちらかだ」と述べているようである。オグレイディによれば、従来の社内 IT システムと比べて、クラウド・コンピューティング分野では互換性やベンダーロックインがより切実な問題となる。

このマニフェストのクラウド・コンピューティング Use Case グループは 2009 年 7 月 31 日に同年 7 月 13 日の Draft2 に続き、「A Whitepaper produced by the Could Computing Use Case Discussion Group」を発表した。同年 10 月 30 日には、「Cloud Computing Use かせ White Paper Version 2.0」を公表している。

Use Case グループによる「白書」寄稿者の中には、連邦クラウド CTO 兼内務省 CTO に任命され、時期尚早との理由で土地管理局の CTO に復職したパトリック・ステイングレー

(Patrick Stingley)、トロントの Enomaly Inc の創業者兼 CTO の Reuven Cohen、日本からは ASPIC(ASP･SaaS インダストリ･コンソーシアム)の佐々木豊主幹研究員も加わっている。

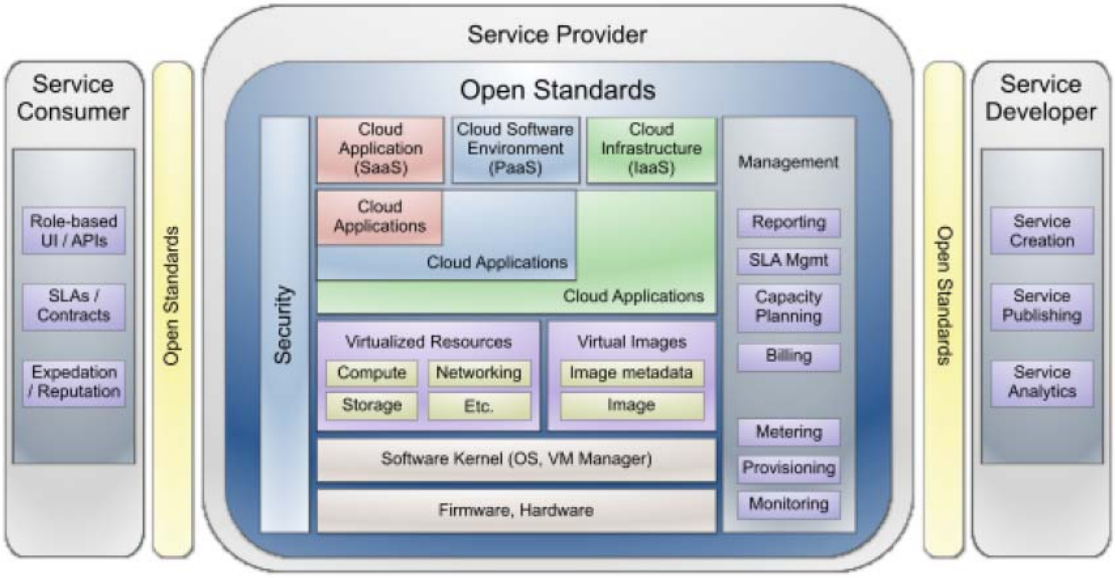
寄稿者一覧
Dustin Amrhein, Joe Armstrong, Ezhil Arasan B, Richard Bruklis, Reuven Cohen, Rodrigo Flores, Gaston Fourcade, Thomas Freund, William Jay Huie, Sam Johnston, Ravi Kulkarni, Anil Kunjunny, Gary Mazzaferro, Andres Monroy-Hernandez, Dirk Nicol, Lisa Noon, Santosh Padhy, Balu Ramachandran, Jason Reed, German Retana, Dave Russell, Krishna Sankar, Patrick Stingley, Robert Syputa, Doug Tidwell, Kris Walker, Kurt Williams, John M Willis, Yutaka Sasaki, and Fred Zappert

「クラウド・コンピューティングのユースケース白書」の中で、Use Case 執筆グループはオープンクラウドマニフェスト（The Open Cloud Manifesto）の 6 原則を繰り返して強調し、広範なコンシューマのニーズに基づき、クラウド・コンピューティングの経済的メリットとパフォーマンスを証明し、クラウドのコンシューマとベンダーに共通するユースケース（Use Case）予測シナリオを明らかにしようとしている。この白書の狙いは、「相互運用性（Interoperability）を確保し、インテグレーションとポータビリティを緩やかにするクラウド環境における標準化すべき能力と要求事項（capabilities and requirements）を強調する」ことである。

「ベンダーのロックイン（Lock-in）を最小化し、顧客の選択肢を増やしつつ、オープン環境としてのクラウド・コンピューティングの発展を確保する」ために、このユースケース白書は、①相互運用性と標準に関する議論に向けて顧客の経験に基づく実務的なコンテキスト（文脈）を提供し、②現存する標準を利用することを明確にして、③オープン・クラウドコンピューティングの重要性に対する業界の関心を重視するなどの目的を示している。

このユースケース白書では、ドラフト 2 を若干修正し、NIST（米国国立標準技術研究所）のクラウド・コンピューティング、3 つのサービス供給モデル（SaaS、PaaS、IaaS)、利活用モデル、基本的特性の定義を繰り返して掲載し、相互運用性（Interoperability)、インテグレーション、ポータビリティ、サービスレベル契約 (SLA) などの用語を定義している。

図 15 ユースケースで示されたクラウド・コンピューティングのタクソノミー（分類）

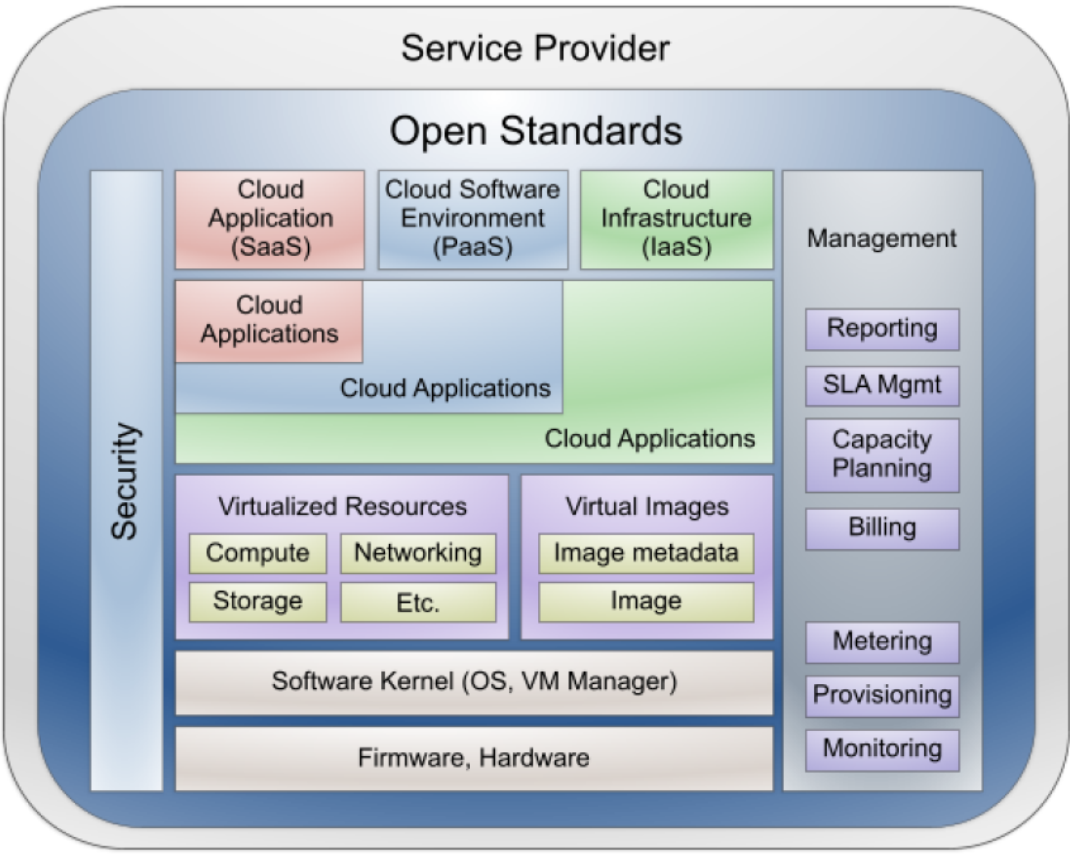


出所：Cloud Computing Use Case Group

上記の図では、サービスコンシューマは、クラウドを介して提供されるサービスを利用し、サービス・プロバイダーはクラウド基盤（cloud infrastructure）を管理し、サービス開発業者はサービスそのものを創出する形となっている。

- サービスコンシューマは、サービスとしてのソフトウェア、プラットフォーム、インフラの如何を問わず、実際にサービスを利用するエンドユーザーまたはエンタープライズである。
- サービス・プロバイダーは、SaaS、PaaS、IaaS のサービスをサービスコンシューマに提供する。実際のタスクは、どのタイプのサービスを提供するかにより異なる。
- サービスデベロッパーは、クラウド・サービスの創出、発表およびモニタリングを行う。
- サービス・プロバイダー：サービス・プロバイダーは、SaaS、PaaS、IaaS のサービスをサービスコンシューマに提供する。実際のタスクは、どのタイプのサービスを提供するかにより異なる。
- サービスとしてのソフトウェア（SaaS）については、プロバイダーはソフトウェアをインストールし、管理・維持を行なう。プロバイダーは必ずしも物理的基盤を所有するとは限らない。

図 16　サービス・プロバイダー

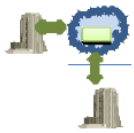
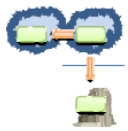
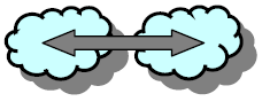


出所：Cloud Computing Use Case Group

- サービスとしてのプラットフォーム（PaaS）では、プロバイダーはプラットフォーム用クラウド基盤を管理する。インフラがバーチャルマシーンを実行する環境であるケースもある。換言すれば、それは、特定タイプのアプリケーションのフレームワークである。
- サービスとしてのインフラ（IaaS）については、プロバイダーは、ストレージ、データベース、メッセージキュー（Message queue）またはその他のミドルウェアを維持する。

エンタープライズ・クラウドの利用シナリオでは、次の典型的なクラウドの Use Case が事例として示されるが、クラウド環境内で実現すべき排他的なリストを意味するものではない。

図 17　エンタープライズ・クラウド利用シナリオ

End User to Cloud	Applications running on the cloud and accessed by end users	
Enterprise to Cloud to End User	Applications running in the public cloud and accessed by employees and customers	
Enterprise to Cloud	Cloud applications integrated with internal IT capabilities	
Enterprise to Cloud to Enterprise	Cloud applications running in the public cloud and interoperating with partner applications (supply chain)	
Private Clouds	A cloud hosted by an organization inside that organization's firewall.	
Changing Cloud Vendors	An organization using cloud services decides to switch cloud providers or work with additional providers.	
Hybrid Cloud	Multiple clouds work together, coordinated by a cloud broker that federates data, applications, user identity, security and other details.	

出所：Cloud Computing Use Case Group

- End User to Cloud：この用例シナリオでは、エンドユーザーがクラウドの中のデータまたはアプリケーションにアクセスする。アプリケーションはクラウド上で実行される（例: Gmail や Facebook）。クラウド・サービスは、エンドユーザーを認証しなければならない。サービスレベル契約（SLA）は、エンタープライズ向けよりも簡単なものになる。
- Enterprise to Cloud to End User：アプリケーションはパブリック・クラウドの中で稼動し、社員およびカストマーがアクセスする。この用例シナリオでは、エンタープライズはクラウドを使いデータおよびサービスをエンドユーザーに提供する。エンドユーザーがエンタープライズとやりとりする際には、エンタープライズはクラウドにアクセスしてデータを取得および/または操作する。クラウド・サービスは、エン

ドユーザーを認証しなければならない。エンドユーザーの必要とする ID に加えて、Federated Identity を必要とする。精緻なセキュリティ要件を満たす必要がある。エンドユーザーに求められるサービスレベル契約（SLA）に加えて、標準的な方法のパフォーマンスのベンチマークを必要とする。

- Enterprise to Cloud：エンタープライズが社内プロセスのためにクラウド・サービスを利用するユースケース。初期段階では、最も一般的な用例。滅多に利用しないデータのバックアップや保管などの必要なリソースの補完。
- Enterprise to Cloud to Enterprise：2 つの企業が同一のクラウドを利用する用例。クラウドにリソースをホスティングすることで、企業のアプリケーションは相互運用性を保つ。アプリケーションはパブリック・クラウドで稼動し、パートナー会社との相互運用性を確保。明らかな用例は、サプライチェーン。
- Private Cloud:エンタープライズのファイアウォールで保護された社内にクラウドを構築する点で他の Use Case と異なる。大手企業に有用で、給与計算等のピーク時にワークロードが急増する処理に柔軟に対応。
- Changing Cloud Vendors：クラウド・ベンダーを他のベンダーに乗り換えるケースや別のベンダーと共同作業するケース。
- Hybrid Cloud：最初のタイトルは“Cloud to Cloud”であり、この方が意味は通じやすいかもしれない。パブリック・クラウドとプライベート・クラウドとの連携利用。複数のクラウドを同時に利用。

1.7.3. Open Cloud Consortium（OCC）

オープンクラウドコンソーシャム（OCC）は、運営母体の異なるクラウド・サービスをシームレスに結びつけるクラウド標準インターフェースの確立を目的とした非営利団体である。米国イリノイ大学シカゴ校などが中心となって組織された同団体は、地理的に離れた場所にあるデータセンターをまたぐ、ストレージおよびコンピューティング・リソースのパフォーマンス向上と同時に、運営母体の異なるクラウド・サービスをシームレスに結び付ける仕組みの整備を目標としている。具体的には、Amazon.com のクラウド・サービスを利用している組織が、ほかのサービスに乗り換える場合、その組織が標準仕様を採用していれば、サービスとのインターフェースを変更する必要はない。このためには、クラウド・コンピューティングをサポートするさまざまなソフトウェアの互換性を確保するインターフェースが不可欠だと、Open Cloud Consortium は考えている。

オープンクラウドコンソーシャム（OCC）のワーキンググループは次の通り。

- Working Group on Standards and Interoperability for Clouds that Provide On-demand Computing Capacity focuses on developing standards for interoperating clouds that provide on-demand computing capacity.
- Working Group on Wide Area Clouds and the Impact of Network Protocols on Clouds focuses on developing technology for wide area clouds, including creation of methodologies and benchmarks to be used for evaluating wide area clouds.
- Working Group on Information Sharing, Security, and Clouds focuses on standards and standards-based architectures for sharing information between clouds.
- Open Cloud Test-bed Working Group manages and operates the Open Cloud Test-bed.

オープンクラウドコンソーシャム（OCC）の議長で、イリノイ大学アドバンスド・コンピューティング研究所（LAC）／国立データ・マイニング・センター（NCDM）のディレクターを務めるロバート・グロスマン（Robert Grossman）は、「誤解してほしくないのだが、Open Cloud Consortiumはクラウド・コンピューティングの宣伝団体ではない。Open Cloud Consortiumは、いまだ明確には理解されていないと思われるクラウド・サービス間の互換性問題や、クラウドを広域展開する手段などを考えていく組織」であると述べている。

1.8. 主な IT 会社のクラウド・コンピューティングの取組事例

1.8.1. マイクロソフト（MS）のクラウド対応

マイクロソフト（MS）は 2008 年 10 月、クラウド・コンピューティングに乗り出す戦略を公表した。“Windows Azure”と呼ばれる大規模データセンター向けのクラウド OS を発表し、インターネットを介してアクセスできるデータセンターを通じてクラウドの中でアプレケーションを稼動させる。同時に、マイクロソフトは、クラウド・コンピューティングのサポートを行うデータセンターをイリノイ州シカゴに設立する計画を明らかにした。シカゴ以外にも、テキサス、ワシントン、アイルランドのダブリンにデータセンターを設置する。

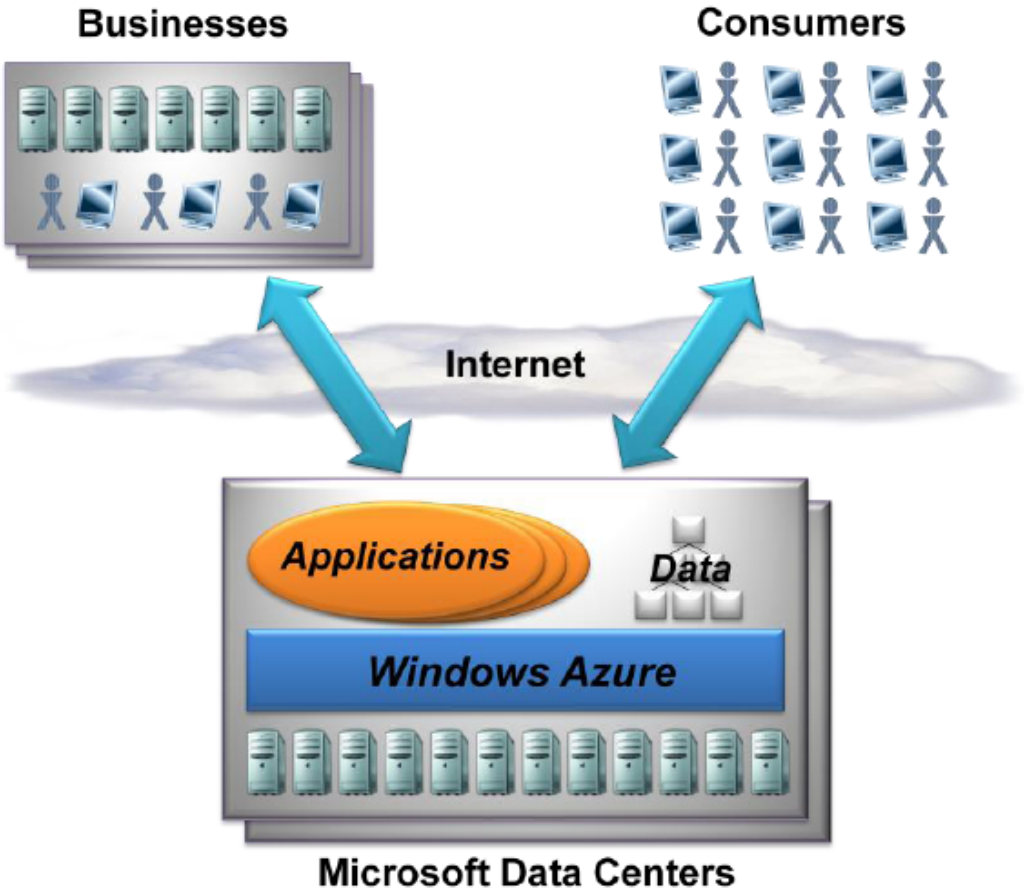
2009 年 11 月 17 日、マイクロソフト（MS）は、ロサンゼルス開催された開発者向け“2009 PDC(Professional Developer Conference)”において、クラウド・サービスの“Windows Azure Platform”のリリースを発表した。商用サービスは 2010 年 1 月 1 日に開始され、同年 2 月 1 日から課金が開始される。

Windows Azure プラットフォームのターゲットは ISV（独立系ソフトウェアベンダー）の開発者である。クラウドコンピューティングプラットフォームに期待する能力、可用性および拡張性のニーズを満たすために、マイクロソフトは、大地震や大災害に備えて地理的に分散させたデータセンターで Windows Azure のホスティングを行う。しかし、Google と異なり、マイクロソフトはデスクトップ OS を放棄することなく、引き続き重要コンポーネントに位置づけている。マイクロソフト（MS）では、Windows デスクトップ、携帯デバイスと TV の 3 つのスクリーンと 1 つのクラウド（Azure）を中核に、異なるプラットフォームを横断的かつシームレスに利用できるアプリケーションの創出で開発者を支援することを当面の目標としている。

2009 年 12 月、マイクロソフト（MS）は、Server & Tools Business（STB）内に“Server & Cloud”部門と呼ばれる新しい部隊を設置し、Windows Azure と Windows Server & Solutions の両グループを統合すると発表した。Windows Azure の開発チームは、Bob Muglia をトップ（President）と Server & Tools Business（STB)内の Server & Cloud 部門に移行する。

マイクロソフト（MS）の Windows Azure の狙いは、クラウドで稼動する On-premises（内部）アプリケーション、データのストレージなどのプラットフォームを供給して ISV（独立系ソフトウェアベンダー）の開発をサポートすることである。

図：Windows Azure アプリケーションは MS のデータセンターで稼動し、インターネットと通じてアクセス可能



出所：David Chappel& Associates、Introducing Windows Azure, December 2009

上図で分かる通り、Windows Azure は、マイクロソフトのデータセンターの中のマシーン上で稼動する。従来のデスクトップでは、ユーザーがインストールして自分で稼動するソフトウェアを提供するのではなくて、Windows Azure はクラウド・サービスを提供する。ユーザーは、Windows Azure のサービスを利用して、マイクロソフトが所有・運転するデータセンターにあるインターネットでアクセスするマシーン上でアプリケーションを稼動し、データを保管する。Windows Azure は、コンピューティング能力とストレージを提供するクラウド・サービスで、Microsoft の所有しているデータセンターに設置され、顧客はインターネット経由でこのサービスにアクセスする。

Windows Azure アプリケーションの主な特徴は、次の通りである。

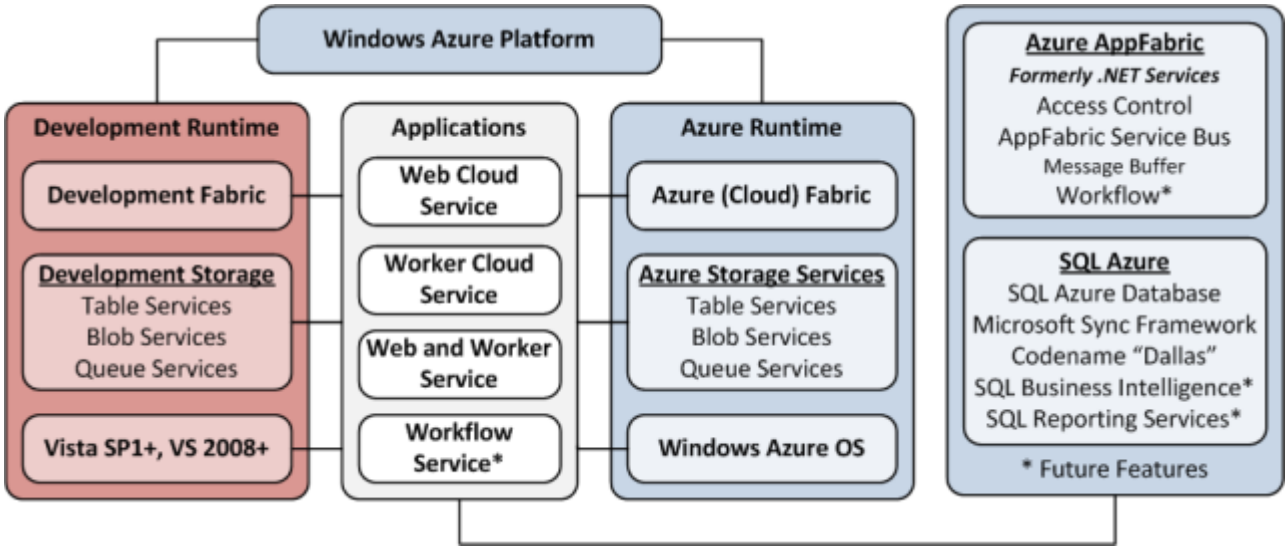
ISV（独立系ソフトウェアベンダー）は、Software as a Service（SaaS）と呼ばれるビジネスユーザーを対象とするアプリケーションを開発することができる。ISV は、Windows Azure を基盤として使い業務用 SaaS アプリケーションを開発する

- Azure のリリースで、Microsoft は、オンラインストレージやコンピューティングサービスを提供し、Amazon、Salesforce.com、Rackspace などのクラウド・プロバイダーと競合することになる。
- ISV は、消費者を対象とする SaaS アプリケーションを開発することも可能である。Windows Azure は、拡張性の高いソフトウェア開発を企図しているので、大規模消費市場をターゲットにする会社が、新アプリケーションのプラットフォームとして利用する可能性もある。
- 企業が Windows Azure を利用して社内の従業員が利用するアプリケーションを構築・稼動する可能性もある。Widows Azure の提供する信頼性と管理可能性は魅力的である。

Windows Azure プラットフォームは、クラウドのアプリケーションとサービスを創出する開発者向けの柔軟性のある環境を提供する。主な製品構成は次の通りである。

- Windows Azure：オンラインサービスで、アプリケーションをホスティングするクラウド OS である。
- Microsoft SQL Azure：クラウド用データベースソリューション
- Windows Azure プラットフォーム AppFabric：クラウド・サービスと On-premises アプリケーションを簡単に接続でき、クラウドで Windows アプリケーションを稼動させ、データ保管を行うためのプラットフォームである。

図：Windows Azure プラットフォームの構成図



NASA、Domino's Pizza、Coca Cola など 20 以上の企業が既に“Windows Azure Platform”を利用している。

マイクロソフト（MS）の最初の業務用 SaaS は、Dynamics CRM Online, Exchange Online, Office Communications Online と SharePoint Online であった。各サービス・ツールは、マルチテナント版で、中小企業を対象とするもので、シングルテナント向けでは、5,000＋ライセンスを必要としていた。消費者向けでは、マイクロソフトは、Windows Live、Office Live と Xbox Live を投入。Autodesk、Blockbuster、Energizer、Ingersoll-Rand などの多数のユーザー企業が利用している。コカコーラも、2009 年末までに、オンライン版 Exchange /SharePoint を 3 万 Seats 加盟する計画である。

MS のクラウドインフラストラクチュアサービス部門の Doug Hauger によると、マイクロソフトは、「On-premises 用に開発するソフトウェアを取り出して、クラウドの中に投げ入れるのではなくて、クラウド用ソフトウェアを開発しつつある」。マイクロソフトの Windows Azure では、ユーザーは、大型サーバー基盤を利用する必要もなく、クラウドか On-premises（内部）で利用するだけである。サービス対象となるデータベース、セキュリティ、認証、バックアップ、インテグレーションなどはすべてマイクロソフトで処理されるので、開発者にはこうしたタスクの負荷はかからないという。

マイクロソフト（MS）CEO の Steve Ballmer によると、より多くのプロダクトの投入を計画しているという。Azure、Windows アップグレードなど、一般消費者および企業向けに多

数の刺激的なプロダクトを市販し、「メインフレームからPC、クライアントコンピューティング、インターネットへのコンピューティングパラダイムの根本的な移行であるクラウド・コンピューティングに精力的に取り組む」と語っている。

【MSの情報セキュリティとクラウドの信頼性】

マイクロソフト（MS）は2009年5月、“Securing Microsoft’s Cloud Infrastructure”と題した24ページのペーパーを発表している。対象は、MSのクラウド・インフラストラクチュア用セキュリティマネジメントをになうGlobal Foundation Services部門のオンラインサービスセキュリティ＆コンプライアンス（OSS）チームである。

マイクロソフト（MS）は過去15年にわたり、クラウド・コンピューティング導入に伴う以下のオンラインサービスセキュリティの課題解決に取り組んできたという。

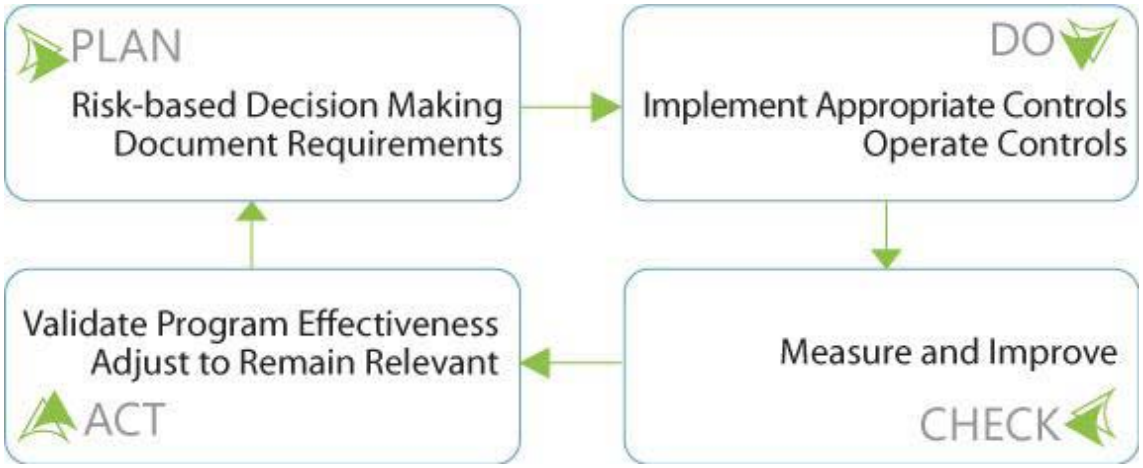
- 新成長分野のクラウドビジネスモデルは、クラウド利用における公的部門と民間部門の組織や企業の間の相互依存を高めつつある。マイクロソフトは、両部門と協力して、ユーザーからの信頼感のあるインフラを提供し、セキュリティセントリックなリスクマネジメントプロセス導入を促進する。
- 実効性の高い情報セキュリティプログラムを通じて、マイクロソフトは、ソフトウェア＋サービス戦略を実行してクラウド・サービス導入の加速化し、ダイナミックなホスティング環境を創出する。
- マイクロソフトは、政策当局、ユーザー法人パートナー、一般諸費者、IT業界パートナー、調査機関など機微なデータでの不正なアクセスの脅威対策を講じる。
- 複雑なコンプライアンス規制の問題解決に努め、既存のサービスに加えて新サービスのグローバル展開を促進する。

マイクロソフトが提供する信頼性のあるクラウドの重点分野は、次の3つである。

- セキュリティと運用上の脅威を監査。優先付けるリスクに基づく情報セキュリティプログラムを利活用する。
- リスクを緩和する詳細なセキュリティコントロールのセットを維持・更新する。
- 適切なコントロールを企図し、効果的な運用をアク保するコンプライアンスの枠組みを運用する。

マイクロソフトの Global Foundation Services 部門のオンラインサービスセキュリティ＆コンプライアンス（OSS）チームが、オンラインセキュリティリスクの管理のための方針と計画を含むクラウド・インフラストラクチュア・セキュリティ・プログラムの責任を担っている。

このクラウド基盤セキュリティ計画は、ISO/IEC 27001（2005 framework of “Plan, Do, Check, Act）を準拠したものである。主な内容は次の通りである。



- Plan
  - ✧ Risk-based decision making：重要な活動とリソース配分の優先付けにより、リスクベースの意思決定を行う。
  - ✧ Document requirements：明確で一貫性のある正確な方法で、文書化したコントロールフレームワークにより第 3 者認証と認定を取得するための文書要求事項を策定する。
- Do
  - ✧ Implement appropriate controls：セキュリティ行動計画に基づく適切なセキュリティコントロールを実施する。
  - ✧ Operate controls：インフラ脅威のマネジメントやデータセンターの物理的保証などのグローバル犯罪法規制などで使う多数のセキュリティコントロールを直接に実行・運用する。
- Check
  - ✧ Measure and improve：継続的にコントロール活動を評価する。
- Act
  - ✧ Validate program effectiveness：社内チームと外部監査人とで定期的に情報セキュリティ計画を検証する。

✧ Adjust to remain relevant：情報セキュリティプログラムと、法規制、ユーザー業界などの要求事項と標準に対するコントロールフレームワークを評価し、改善分野などを特定する。

1.8.2. 主なクラウド・プラットフォームとクラウド・ベンダーの資料

以下は、主要なクラウド・プラットフォームを比較した表である。

	概要	強み	弱み
Salesforce Force.com	Visualforce (custom user interface creation) と Apex Code(ビジネス・ロジックとデータを操作する Java 言語のような)のような新しいツールのついた AppExchange とホストを開発したプラットフォーム	・CRM アプリケーションをコアにした顧客ベースであること ・マルチテナント型 ・相対的な成熟度	・独自の言語（Apex Code) ・Web スケールインフラクチュアでないスケーラブル
Google App Engine	Web アプリケーションのための開発と帆スティング環境がコンパクトに統合されている；動的なランタイム、 永続ストレージ、 ユーザー認証、 E-mail、サービスモニタリング、ログ解析など。	・既存 ・完成度の高い Web-Scale インフラクチュア；グーグルサービス・アプリケーション・プログラミング・インターフェースの設定 ・低価額（無料体験）	・Request-driven ・ページ指向のモデル ・Google インフラストらクチュアへの直接アクセスがない ・サービスレベルアグリーメントがない
Amazon Infrastructure Cloud	インフラサービスのアラカルト -Elastic Compute Cloud(EC2) -Simple Storage	・Ready-to-go ・Amazon.com によるインフラクチュアのシェア ・使用したサービス	・IDE サポートなし ・サービスの限界 ・エンタープライズ市場へ新規であること

	Service(s3) -simple Queue Service(SQS) -SimpleDB	に応じた料金体制 ・Web サービスインターフェイスの標準化 ・言語に依存しない	
IBM Blue Cloud	プライベート・クラウド構築のためのハードウェアとソフトウェア； -リナックスベースのサービス -グリッドコンピューターエンジン -Xen -PowerＶM、-Hadoop - Tivoli Bland Center	・バックオフィス、開発環境が最強 ・オープンソース・コンポーネント ・カスタマイズ可能	・ベンダー固有のハードウェア ・複雑さ ・コスト高
Microsoft Windows Azure	・ソフトウェア+サービス　ハイブリッドモデル ・オンラインサービスによるアセンブル機能（記憶、アイデンティティ、データサービス） ・デスクトップクライアントとクラウドのための同じアプリケーションプログラムインターフェイス	・投資規模のスケールと大規模な開発者コミュニティにおけるビジョンの完全性 ・開発ツールと技術、マイクロソフトをベースとしたアップリケーションとの統合が容易である	・開発時間 ・ビジネスモデルのオプションによる複雑さ
VMware vCloud	仮想データセンターオペレーションシステム構築とクラウド環境下で仮想マシーンを実行するための具象的な状態のトラ	・On-premise 仮想インフラクチュアと外部 Mwere-enabled in-the -cloud　データセンター間におけるサポートの移植	・サービスプロバイだーのラインナップによるイニシアティブ （いつできるのかが明らかでない）

	ンスファーのセットベースのアプリケーションプログラミング・インターフェイスと料金やサービスレベルの合意をトラッキングするような設定（vService）		

以下は米国の主なクラウド・ベンダーの一覧表である。

Vendor	Description
3Leaf Systems	Describes itself as a provider of “next-generation server solutions to enable cloud computing.” Specifically, 3Leaf offers to help companies “achieve a terabyte of DRAM at dramatically low cost” based on low-cost commodity servers by providing virtualization of CPU and memory for an entire server farm.
3PAR	Recently announced is “Cloud Agile” program, a new partnership initiative “to promote the adoption of cloud computing and cloud-based services offered by leading providers with infrastructures powered by 3PAR Utility Storage.”
3Tera	Offering what it calls “Cloud Computing Without Compromise”, 3Tera enables the provision and deployment of “scalable clustered applications in minutes from anywhere in the world.” The company currently has partners and is running in datacenters in seven countries (U.S., Japan, Singapore, Argentina, U.K., Netherlands, and Serbia) on four continents, with additional resources in South America and Australia.
10Gen	10Gen offers “innovative platform technology” around the Mongo database, an open source document-oriented database “that makes data storage for Web (and other) applications fast and easy.”
Adaptivity	Adaptivity provides integrated solutions that automate IT delivery optimization across enterprise computing environments. The team behind the company built the largest private cloud while at Wachovia, and are today building clouds with Unisys. Adaptivity sees the cloud computing opportunity from a much broader perspective. “IaaS- type resources managed externally from the enterprise do provide value; however, the larger opportunity is enabling enterprises to change how they deliver and consume IT resources”.
Agathon Group	A dedicated grid environment that allows charitable and non-profit campaigns to scale on demand.
Akamai	Akamai claims to have been optimizing the cloud for over 10 years, building a global computing platform “that helps make cloud computing

	a reality." Services for cloud optimization are a vital part of the company's total offering.
Appirio	Offers services and products to accelerate the adoption of on-demand solutions, and recently secured US$5.6 million of financing in a Series B round led by Sequoia Capital.
Appistry	Appistry offers a grid-based application platform that makes it easy to scale-out CPU- and data-intensive applications across a virtualized grid of commodity servers. Unlike traditional grid products based on legacy scheduler technology, the company's "fabric" architecture has no single point of failure and "is well suited for extreme transaction processing (XTP), software-as-a-service (SaaS), cloud computing, and other data- and CPU-intensive applications.
Apprenda	Apprenda is the company behind SaaSGrid, an operating system for building and deploying Software-as-a-Service applications and a platform for conducting Software-as-a-Service business.
Appzero	Pioneer of virtual application appliances (VAA) that decouple an application from the operating system and its underlying infrastructure. "The resultant virtual application appliance contains an application with its dependencies but with zero operating system component." The aim of VAAs is to enable enterprises to provision server-based applications to any machine in the data center in a matter of seconds or move an application from the data center to the cloud (D2C).
Aptana	Aptana recently beta-released Aptana Cloud, which it says "is architected to complement cloud infrastructure providers like Amazon, Google, Joyent, and others.
Arjuna	Arjune describes itself as an "on-ramp the cloud that allows the IT department of begin to experiment with cloud computing in a gradual, incremental way without any need for disruption to existing service.
AT&T	AT&T broke into the cloud business in August 2008 with the global launch of what it calls AT&T Synaptic Hosting, described as "a next-generation utility computing service with managed networking, security, and storage for businesses."
Bluewolf	A leading provider of on-demand software deployment services, Bluewolf offers remote database management and recently announced its Arcade cloud storage offering that allows users to economically store a virtually unlimited number of files of all sizes through the Salesforce.com interface.
Boomi	Creater of AtomSphere, which the company calls "the industry's first integration platform-as-a-service. It is a pure SaaS integration platform that does not require software or appliances.
Booz Allen Hamilton	Management consultancies are also part of the cloud eco-system due to their wide range of offerings. Booz Allen has positioned itself in the forefront of the federal government's cloud computing initiative. According to the company's website, "Booz Allen is prepared to support all elements of government defense and civilian missions and migration efforts to "the cloud." Booz Allen is also developing new economic

	analyses, addressing all cost categories for a variety of potential cloud uses to help agencies make the case for migrating to the cloud.
Computer Associates	Bought the key assets, software assets, and engineering team of Cassatt in June 2009
Callidus Software	This provider of Sales Performance Management solutions has launched Callidus On-Demand SPM, "a scalable, secure, subscriber-based model that does not require additional IT resources."
Cisco	By virtue of its recent acquisitions - WebEx and PostPath - Cisco is participating in cloud computing. "We are believers in the cloud-based delivery model for certain types of services, in particular inter-company collaboration services.
Cloud9 Analytics	Offers what it calls "the industry's first truly on-demand analytics platform."
CloudBerry Lab	Established in 2008 by a group of experienced IT professionals with the mission "to help organizations in adopting cloud computing technologies by closing the gap between cloud vendors' propositions and consumer needs through development of innovative low-cost solutions." Their flagship product is CloudBerry Explorer for Amazon S3.
Cloudera	Cloudera helps its customers install, configure, and run Hadoop for large-scale data processing and analysis.
Cloudscale	Cloudscale's technology "automatically provides the parallelism and scalability required to handle anything from one-off personal analytics agents up to the most demanding live analytics applications required by business, science, and government.:
Cloudswitch	A fast-growing cloud computing company backed by Matrix Partners, Altas Venture, and Commonwealth Capital Ventures, Cloudswitch is developing what it describes as "an innovative software appliance that delivers the power of cloud computing seamlessly and securely so enterprises can dramatically reduce costs and improve responsiveness to the business."
Cloudworks	Cloudworks allows small and mid-market companies to outsource all of their computers, software, and data. Completely Web-based, it works like Salesforce.com or Hotmail.
CohesiveFT	Provides "elastic server on-demand", aimed at "enabling customers to build and manage applications for virtualized infrastructure and cloud computing." The company's elastic server platform allows users to assemble and deploy servers to cloud computing platforms "in minutes".
Cordys	The Process Factory by Cordys is a simple, reliable, and secure solution to create MashApps business processes from the cloud by mixing and matching standard business applications like Google Apps and commercially available services.
Cumulux	Cumulux is a cloud solution provider offering products and services that "help enterprises harness the benefits of the cloud." The company's flagship product - Hybrid Axis - "helps enterprises extend their current investments to the cloud by integrating traditional and cloud-based applications."

Desktoptwo	This cloud desktop offering from Sun Global Partner, Sapotek, describes itself as "your home in the cloud" and claims to have users in 120 countries.
Elastra	Elastra offers to "design, deploy, and manage database and application infrastructure in the cloud in minutes." The company's aim is to help a business "unlock the value of cloud computing by using virtualized hardware environments with cloud-provisioned database and infrastructure software that is easily configurable and does not require scripting, responds elastically to changing load, and is delivered in the cloud with meter-based pricing.
EMC	When creating a cloud computing division within the company in February 2008, the CEO declared that 85% of data will be managed in what he called "big, safe information repositories in the Internet 'sky'"
Engine Yard	Engine Yard offers rails-focused 24/7 operations support on top of great infrastructure to companies in search of a smooth path from 100 users to 100,000 users. In July 2008, the company closed US$15 million of Series B financing led by New Enterprise Associates, and participation from Amazon.com
ENKI	The company's aim is "to allow you to focus on delivering your application to your customers while we handle the operations side: providing computing as a reliable service."
Enomalism	Founded in November 2005 by Enomaly, Inc., Enomalism is an elastic computing platform that focuses on "solving the cost and complexity for enterprises that run large technical server infrastructures." It simplifies IT management and increases efficiencies in system resources.
EVapt	eVapt claims to enable "usage-based monetization (instant SaaS metering) for SaaS and cloud computing vendors
FlexiScale	FlexiScale is a flexible, scalable, automated hosting platform (cloud computing on-demand)
GigaSpaces	Founded in 2000, GigaSpace allows users to "predictably scale on-line systems under any peak demand, guarantee real-time performance under any data processing load and seamlessly leverage the economies of scale offered by virtual computing environments such as clouds and grids"
GoGrid/ServPath	Launched in 2006 by ServePath, GoGrid claims to "deliver true control in the cloud by combining many of the familiar features of dedicated server or managed hosting with the flexibility and scalability of cloud server hosting." GoGrid customers can grow production servers in real-time to meet demand without affecting their uptime.
GOS	Founded in 2007, Good OS is an operating system software company based in Silicon Valley, California, and Taipei, Taiwan. The company's mission is to "enable cloud computing through software."
Grid Dynamics	A technology consultancy company that helps customers "architect, design, and deliver business systems that handle peak loads, scale on demand, and always stay up, using the latest advances in grid and cloud computing."
Heroku	In May 2008, the company raised US$3 million in funding for its online

	deployment system for Ruby on Rails applications.
Hyperic	Founded in 2004, Hyperic provides complete, easy-to-use monitoring and management software for all types of Web applications, including hosting it in the cloud via its CloudStatus dashboard, currently in beta.
Intel	Intel believes in Open Cloud Standards and one commentator believes there is a strong correlation between how fast cloud computing can proliferate and how well Intel plays its role to lead the open cloud solutions at IaaS and PaaS layers.
Interoute	Europe's largest and most advanced fiber optic network, the Interoute platform operates as as Europe's largest privately owned cloud.
Joyent	The Joyent platform, which "enables teams to effectively communicate and collaborate with emaii, calendaring, contacts, file sharing, and other shared applications" serves billions of Web pages every month ahd helped LinkedIn scale to 1 billion page views per month. Self-described as an "on-demand computing" provider, the company has developed, built, and scaled some of the earliest Ruby on Rails applications, and developed a world-class infrastructure, methodology around how to deploy and scale Rails applications.
JumpBox	JumpBox describes itself as a suppler of "instant infrastructure", specifically it is a ready-to-deploy virtual computer that contains a pre-configured instance of an application.
Kaavo	Kaavo provides a platform for managing distributed applications in the clouds. The core product, Infrastructure and Middleware On Demand (IMOD) "makes it easier for individuals and businesses to implement on-demand infrastructure and middleware and run secure and scalable web services and applications.
Keynote Systems	Long a player in the SaaS space, in 2009 Keynote Systems opened its cloud infrastructure and offered any Web team free access to KITE (Keynote Internet Testing Environment), its product for testing and analyzing the performance of web applications across the Internet cloud. With KITE, companies have free access to Keynote's cloud infrastructure and a tool to test and monitor their applications from cities all over the world.
Layered Technologies	Offers virtualization and cloud computing systems
LongJump	The Platform-as-a-Service (PaaS) solution that LongJump offers is described by the company as an "on-demand platform for creating and delivering business applications to manage data, streamline collaborative processes, and provide actionable analysis." The company claims that the LongJump platform has "extensive features around security access, data analysis and visualization, and process automation, all on the Web."
Meeza	Qatar-based Meeza is currently the main cloud service provider in the Middle East/North Africa region.
Mezeo Software	Based in Houston, Texas, this privately funded software solution provider has created what it calls "the industry's first deployable, white label cloud storage platform, enabling service providers to

	quickly and efficiently enter the cloud storage market." Called: Mezeo Cloud Storage Platform.
Nirvanix	A provider of an enterprise cloud computing offering that allows companies with more than 5TBs of data a highly scalable storage and delivery platform. Nirvanix has raised more than US$18 million in funding from world-class investors, including Intel Capital.
Novell	The recently announced Novell Cloud Security Service "enables cloud service providers and Software-as-a-Service vendors to ensure their offerings meet the strict security and compliance standards required by global businesses."
OpenNebula	OpenNebula is a widely used open-source tool for the efficient, dynamic, and scalable management of virtual machines within datacenters (private clouds) involving a large amount of virtual and physical servers.
OpSource	OpSource delivers a complete Web operations solution for Software-as-a-Service and Web companies. Its OpSource Cloud is currently in private beta, aimed at providing every user with a "virtual private cloud" within the public cloud.
Oracle	Oracle believes that private clouds for the exclusive use of one enterprise can mitigate concerns about security, quality of service, integration, compliance, lock-in and long-term costs of public clouds by giving the enterprise greater control.
Parallels	Founded in 1999, Parallels optimizes computing by providing virtualization and automation software to businesses and service providers across all major hardware, operating systems, and virtualization platforms. Parallels works closely with a network of ISVs and service providers to enable them to build their cloud computing and software-as-a-service offerings, meeting the needs of end-user organizations of all sizes. Parallels' technology is also used by large enterprises creating their own in-house clouds.
ParaScale	ParaScale's software "enables the enterprise or service provider to build enormous storage pools on commodity hardware at an affordable cost."
Penguin Computing	Penguin has launced an HPC cloud called Penguin on Demand (POD). Penguin is targeting researchers, scientists, and engineers who need surge capacity for time-critical analyses.
Platform Computing	Founded in 1992, Platform is a pioneer and global leader in HPC and believes there is an intersection between grid computing and cloud computing in that both cloud computing and grid propose an architecture that masks the complexity of managing thousands of commodity services from their users.
Quantivo	Quantivo claims to be "revolutionizing the business intelligence world by combining cloud computing with an innovative and patented "affinity analytics" technology. The company recently won the Silicon Valley/San Jose Business Journal's "Emerging Technology Award" in the cloud computing category.
Rackspace	Rackspace is a market-leading specialist in hosting and cloud computing services. The company delivers computing-as-a-service, "integrating

	the industry's best technologies into a flexible service offering, making computing more reliable and affordable."
RedHat	RedHat believes that is consistent dedication to open source and open standards will further the success of a strong cloud ecosystem. A company spokesman said, "by bringing together thousands of RedHat-certified applications, RedHad Enterprise Linux, Jboss Enterprise Middleware and RedHat Enterprise Virtualization, we aim to deliver the next generation of computing architectures.
Rhomoble	Rhomobile provides RhoHub, "the world's first Development-as-a-Service for mobile." RhoHub provides a cloud-based service for both smartphone applications development and hosting of mobile applications.
RightScale	RightScale offers a fully automated cloud management platform that enables organizations to "easily deploy and manage business-critical applications across multiple clouds with complete control and portability." The RightScale Cloud Management Platform is delivered as a software-as-a-service and is available in a range of editions, from a free developer edition to enterprise editions.
RPath	Founded in 2005, rPath helps organizations "realize the promise and avoid the perils" of cloud computing, "rPath's Cloud Computing Adoption Model provides a pragmatic, actionable, step-by-step framework for achieving measurable benefits, while laying a foundation for the strategic benefits of a cloud infrastructure over time."
Savvis	Provider of Savvis Cloud Compute, a "right-sized computing environment" launched in February 2009.
SIMtone	SIMtone has developed and commercialized a "Universal Cloud Computing Platform" that allows network operators and businesses "to host, manage, and quickly provision any cloud-hosted services, and deliver them to zero-touch terminals that can be standalone, low-cost hardware appliances, or software terminals usable via browsers or on PCs, thin clients, and mobile devices."
Skytap	Skytap's goal is "to make serving up virtual machines over the Internet as ubiquitous as delivering HTML to a browser." Skytap Virtual Lab is a hosted, on-demand service for virtual lab automation and management.
SLA@SOI	SLA@SOI's vision is "to create a business-ready service-oriented infrastructure that will empower the service economy in a flexible and dependable way."
SmugMug	Founded in 2004, SmugMug calls itself "the ultimate in photosharing" since it offers unlimited storage and stores backup copies of each photo in multiple datacenters. With more than 315,000 paying customers and 288,000,000 photos in storage, SmugMug is a QED of cloud computing.
SOASTA	SOASTA announced in 2007 a cloud-based testing solution "build on the cloud to enable application testing in a cloud"
Terremark	Offering Enterprise Cloud services that "let you control a resources pool of processing, storage, and networking, and allow you to deploy server capacity on demand".

Unisys	The Unisys cloud computing strategy enables clients to choose the type of datacenter computing services that best meet their business objectives, from self-managed, automated IT infrastructures, to Unisys-managed cloud services. Using Unisys services and technologies, organizations can create a private cloud within their datacenters, a public cloud through secure Unisys-managed cloud solutions, or a hybrid cloud solution combining the best of both private and Unisys-managed cloud services.
Univa UD	Univa UD is an innovator in software solutions for cloud enablement. The company's software suite includes infrastructure management and service governance for cloud and HPC environments and spans all three cloud scenarios: public, private, and hybrid.
Vertica	Vertica Analytic Database for the cloud is an "on-demand version fo Vertica's fast, grid-enabled columnar database hosted on Amazon's EC2
WorkXpress	A PaaS pioneer, WorkXpress released v. 2.0 of its flagship customizable software platform in April 2009.
Zetta	A provider of what it calls "best-in-class NAS storage in the cloud"
Zimory	A spin-off of Deutsche Telekom Laboratories, Zimrooy "enables dynamic, on-demand movement of applications automatically between servers in one or many locations, as well as creating the world's first marketplace for computing capacity. Based in Berlin, Germany, the company develops a dynamic infrastructure solution for datacenters to create a modern Adaptive Cloud Infrastructure.
Zuora	The company describes its Z-Commerce Platform as "the first commerce platform for cloud developers."

第２章　米国におけるスマートグリッド動向

2.1.　最新の米国スマートグリッド政策

2.1.1.　スマートグリッド法制化までの沿革

2003 年 2 月 6 日、ブッシュ前大統領は、経済的および国家的な安全保障のために、米国の“電気供給システムを近代化する”必要性を強調した。この大統領の言明と“National Transmission Grid Study（国家送電グリッド研究)”で示された 51 の提言を踏まえて、エネルギー省（DOE）と傘下に新設されたスマートグリッドを担う“送電&配電局（Office of Electric Transmission and Distribution)”は 2003 年 7 月、“21 世紀最高のエンジニアリング成果”であるとみなされることを期待して、北米のための未来電気システムのビジョンを描いた“Grid 2030 - A National Vision for Electricity’s Second 100 Years”を発表した。

●2003 年 4 月 2～3 日の“Grid 2030 会議”

目　的：発電、送電、配電、貯蔵および末端利用の電気供給バリューチェーンを転換し、未来電気システムの国家ビジョン（National vision of the future electric system）を明らかにすること。
重　点：中央発電プラントと消費者との間にある電力基盤である“Grid”問題とそのシステム計画と市場オペレーションを統制する規制上の枠組みが中心課題となる。
参加者：電力業界、機器装置メーカー、IT プロバイダー、連邦および州政府関係省庁、利益集団、大学、国研の代表等 65 人。
ファクトファインディング
➢　20 世紀最高のエンジニアリングの成果を実現した米国の電力システムは老朽化しつつあり、非効率的で、混雑し、情報経済の未来のエネルギー需要を満たす容量がないために、運転改善と今後数十年の抜本的な設備投資が必要。
➢　（エンロン事件、大停電、設備増設計画の解約、送電系統や配電系統の新設投資が過去最低水準を記録したことなどを背景に）未来の需要を満たす電力業界の系統能力を巡る前代未聞のリスクと不安が高まっている。
➢　連邦レベルおよび州レベルの両面で、電力市場の規制上の枠組みも期待される成果をだせないストレス状態にある。
➢　米国の電力供給システムを近代化・拡充し、電力系統の混雑を緩和し、電力供給システムの計画策定と運用上の問題を解決することに役立つ幾つもの期待できる技術が生まれている。具体的には、先進的伝導体、先進的電気貯蔵システム、分散型スマート制御装置、AC-DC コンバータなどの電力エレクトロニクスデバイ

ス、On-site 発電や需要マネジメントなどの分散型エネルギー資源など。

- 通信などを普及させた IT 革命も電力業界の改革に寄与する。マイクロプロセッサーの拡散により、電力系統の信頼性と電力の質を向上させるニーズが高まる。
- 電力負荷が大きくなる都市部や都市近郊では、伝統的な架空送電線（conventional overhead transmission lines）の新設が難しくなっている。①既存の送電資産経由でより多くの電力を受容できる電子ソリューションの利活用と②土地利用問題を配慮する低インパクトのグリッドソリューションの開発で、上記の問題を解決できる。

結　論

- 重要な電力システムの“技術準備度（technology readiness）を加速化する必要がある。
- 特に、高温超電導ケーブおよびトランスフォーマー、低コスト電気貯蔵デバイス、分散型インテリジェンス＆“スマートパワー”システムのための標準化されたアーキテクチュアおよび技術、原子力、クリーンコール、熱電併給などの再生可能および分散型エネルギーデバイス。
- 政治的な行き詰まり状況（political log jam）を解消し、昨今の規制上の枠組みが原因のリスクと不安を少なくするブレークスルーが不可欠。
- 具体的には、競争市場のルールを決める省庁間の管轄問題を解消すること、ユニバーサルサービスと公的目的プログラムのメカニズムを確保すること、長期投資を促進する安定的なビジネス環境を支援すること。
- 電気機器の取替投資には今後数十年で数十億ドルの投資が必要となる。新型機器の経済寿命は 40 年以上である。したがって、今後の投資では、クリーン、効率的、信頼性のある、セキュアで、手頃な価格の次世代の電気技術を利用する必要がある。
- 次のステップとして、“全米電気供給技術ロードマップ（National Electric Delivery Technologies Roadmap)”を共同開発する。

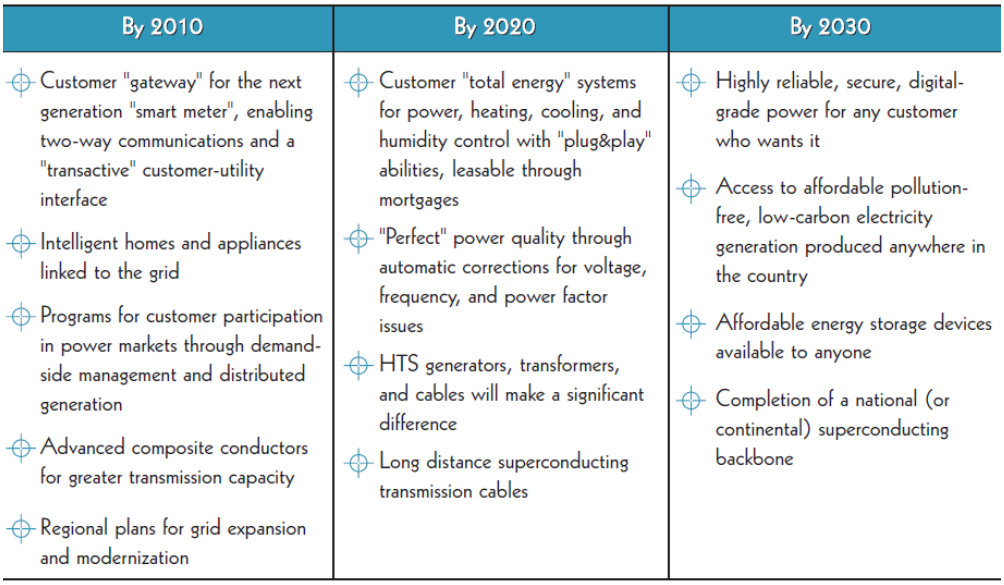
“Grid 2030”ビジョン文書は、上記の通り、2003 年 4 月 2～3 日にワシントン DC で開催された“全米電気システム（Grid）ビジョン会議”に参加した 65 人の電力業界、機器装置メーカー、IT プロバイダー、連邦および州政府関係省庁、利益集団、大学、国研の代表の意見や優先課題を反映したものである。2003 年 4 月の Grid 2030 ビジョン会議は、ブッシュ政権のエネルギー政策、国家送電グリッド研究（National Transmission Grid Study）およびエネルギー省（DOE）長官の電力諮問会議報告書（Report of the Secretary of Energy’s Electricity Advisory Board）で示された数多くの提言に対応。この会議成果を取り纏

めた“Grid 2030”文書は、米国の電気供給システムを現代化して拡充するためのビジョンとロードマップを示し、総合的アプローチの概要を記述している。

未来の電力系統（Grid）のビジョン
「Grid 2030 は、すべての消費者とノードを監視および制御する完全自動化された電力供給ネットワークであり、発電所と電気機器の間およびその間のすべてのポイント間の電気と情報の双方向の流れ（two-way flow）を確保する。この分散型インテリジェンスは、ブロードバンド通信および自動化制御システムと抱き合わせて、ヒト、建物、工場、発電施設および電気ネットワーク間のリアルタイムな市場取引とシームレスなインターフェースを可能にするものである」。 Grid 2030 is a fully automated power delivery network that monitors and controls every customer and node, ensuring a two-way flow of electricity and information between the power plant and the appliance, and all points in between. Its distributed intelligence, coupled with broadband communications and automated control systems, enables real-time market transactions and seamless interfaces among people, buildings, industrial plants, generation facilities, and the electric network.

“Grid 2030”文書では、この未来の電力系統（後に“スマートグリッド”と呼ばれる）のビジョンを実現するためには､次の 3 段階方式による総合アプローチ手法を示している。第 1 段階（2010 年まで）では、先進的技術の R&D（研究開発）と実証および規制上の枠組みの刷新を行い、第 2 段階（2020 年まで）で、電力資産の資本回転率と最新システムへの更新を実施し、第 3 段階（2030 年まで）で、Grid 2030 を地方・地域展開して全米市場と国際市場に拡充する。

図 18　Grid 2030 のロードマップ

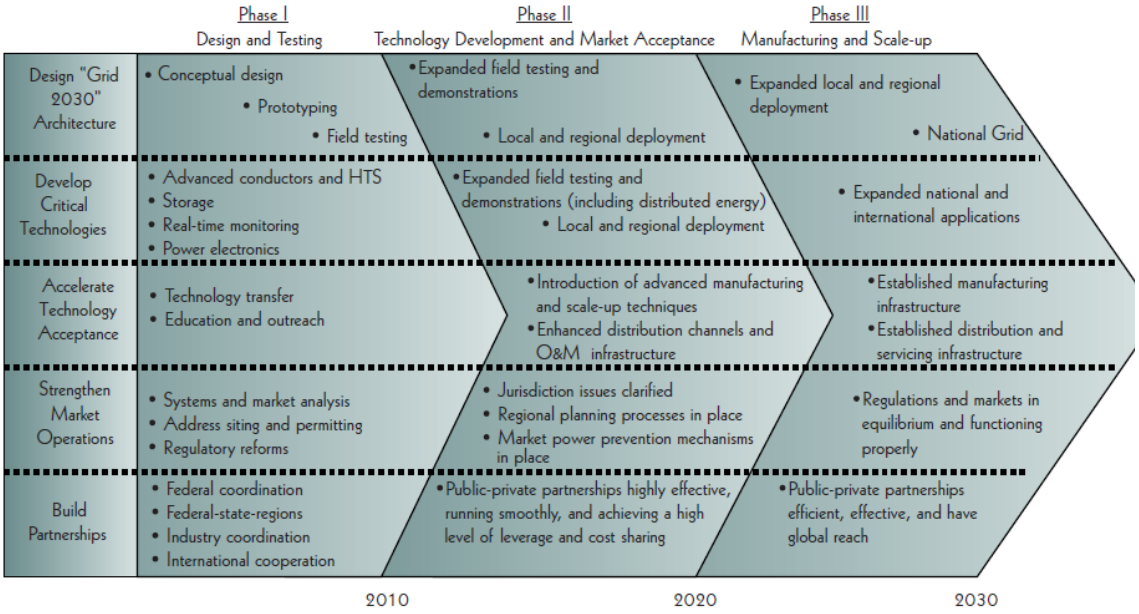


By 2010	By 2020	By 2030
Customer "gateway" for the next generation "smart meter", enabling two-way communications and a "transactive" customer-utility interface	Customer "total energy" systems for power, heating, cooling, and humidity control with "plug&play" abilities, leasable through mortgages	Highly reliable, secure, digital-grade power for any customer who wants it
Intelligent homes and appliances linked to the grid	"Perfect" power quality through automatic corrections for voltage, frequency, and power factor issues	Access to affordable pollution-free, low-carbon electricity generation produced anywhere in the country
Programs for customer participation in power markets through demand-side management and distributed generation	HTS generators, transformers, and cables will make a significant difference	Affordable energy storage devices available to anyone
Advanced composite conductors for greater transmission capacity	Long distance superconducting transmission cables	Completion of a national (or continental) superconducting backbone
Regional plans for grid expansion and modernization		

エネルギー省（DOE)、スマートグリッドの所轄として新設された“送電&配電局（Office of Electric Transmission and Distribution)”は 2003 年 7 月 8～9 日に約 200 人の専門家によるワークショップを開催し、その成果を踏まえて、2004 年 1 月に北米のグリッドを大改造するための手引書である“National Electric Delivery Technologies Roadmap”を発表した。この電力供給技術ロードマップ報告書は、米国グリッドを現代化するために、①“Grid 2030”ビジョンのアーキテクチュアの概念設計、②高温超電導（HTS)、電気貯蔵デバイス、分散型インテリジェンス、センサー、スマートシステム、低コストで耐久性の高い信頼性のある電力電子デバイスなどの重要技術の開発、③先進的技術の受容を加速化、④電力市場の強化、⑤官民パートナーシップの構築などのアクションアジェンダを示している。

下記の図は、米国の電力供給システムを現代化する“Grid 2030”ビジョンに対応した全米技術ロードマップの概要を示したものである。

図 19　“Grid 2030”ビジョン全米技術ロードマップ概要



2.1.2.　エネルギー政策法（EPACT）とエネルギー自立&安全保障法（EISA）

2005 年 7 月に成立した“2005 年エネルギー政策法（EPACT-Energy Policy Act)”は、需要反応（DR）およびスマートメーターリング（Section1252）の中で、①DOE（エネルギー省）に対して、需要に応じて利用時間別に電気料金の価格設定を求める需要応答（Demand Response）の潜在的可能性を全国レベルで評価することと（“National Demand Response Potential Assessment”および“National Action Plan for Demand Response”の策定と履行)、②連邦規制委員会（FERC）に対して、年次需要反応（DR）評価と需要反応を可能とする先進的（スマート）メータリングの電力業界における浸透率を調査することを指令した。これにより、米国は、時間別価格設定と需要反応（DR）システム導入を促進することになったのである。

2005 年エネルギー政策法（EPACT）の成立により、連邦議会は、政策と実業の両面から需要反応（DR）を米国の電気システムの中に組み込む意向を表明し、先進的な次世代電力網（Grid）を開発するための重要なカギとなる需要反応とそれを可能にする技術を認識して実装するための複数の政策措置を講じることになったのである。州レベルのアプローチとその活動にはバラツキがみられる。2008 年末現在、2005 年エネルギー政策法（EPACT）の Section1252（需要反応およびスマートメーターリング）の連邦指令に準拠する州も一部にあるが、多くの州は独自のイニシアティブを展開している。

エネルギー省(DOE)傘下の国研である“National Energy Technology Laboratory (NETL)”は、2007年4月に“A Vision for Modern Grid (現代グリッドのビジョン)”を発表し、21世紀の先進的なグリッドの目標として、①信頼性、②セキュア（確実なセキュリティの保証)、③経済性、④環境にやさしい、⑤安全性をあげている。また、Modern Grid のビジョンとして、①自己発熱 (Self-heating)、②消費者の動機付けとグリッドへの参加、③物理的攻撃およびサイバー攻撃への抵抗力、④21世紀のユーザーの要求に対応できる電力の質、⑤あらゆる種類の発電および電気貯蔵を受容することが可能、⑥マーケットEnabler、⑦資産の最適化と効率的な運転を例示している。

米国のスマートグリッド政策は、元々、“クリーンエネルギー法案”と呼ばれた“2007年エネルギー自立＆安全保障法 (EISA-Energy Independence and Security Act of 2007)”において初めて法律として制度化された。

ブッシュ大統領は2007年12月19日、自動車燃料の経済効率を高め、代替燃料の比率を高めることで、米国の石油依存度を低減させる“エネルギー自立＆安全保障法”に署名した。この法律は、2007年1月の一般教書演説 (State of the Union Address) で示された“Twenty in Ten (10年間でガソリン消費量を20%削減)”イニシアティブに対応したもので、エネルギーの自立と安全保障を促進し、製品、建築物および車の効率性を高め、温室効果ガスの研究開発を促進し、連邦政府のエネルギー性能を高めることを目的にしたものである。

2007年エネルギー自立＆安全保障法の主な規定は次の通りである。

- 自動車の燃費改善によるエネルギー安全保障 (Title 1)
  - 2005年エネルギー政策を土台として、1975年のCAFÉ(Corporate Average Fuel Economy：企業平均自動車燃費節減)規制の強化。自動車メーカーは、2020年までに1ガロン当たり35マイル(14.8km/l)の燃費基準の達成を義務づけられる。
  - 先進的バッテリー開発のための融資保証プログラム、プラグインハイブリッド車開発の補助金、各種電気自動車開発のインセンティブ供与。
  - バイオ燃料の生産拡大を義務づける代替燃料基準 (RFS-Renewable Fuel Standard) の強化 (Title 2)。

- 電気器具および照明デバイスの基準改定によるエネルギー節減 (Title 3)
  - GSA (一般サービス局：調達局) 内に高性能グリーンビルディング部局(OHPGB)を設置。
  - “エネルギー政策及び省エネ法(EPCA)”を改正し、家電品へのエネルギー効率ラ

ベルの貼付、地域冷暖房の効率、住宅のボイラー効率の、電子モーターの効率、家庭用電気製品の効率などを実現する。

- 建築物および産業のエネルギー節減（Title 4）
  - エネルギー効率の高い“グリーンビル”などの高性能商業ビル開発の促進。
  - 連邦政府機関や公共機関の建物の新設および改築では、2010 年までに対 2003 年水準で 55%の化石燃料の削減。新設の連邦政府の建物では 2030 年までにカーボン中立を義務づける。
  - 産業部門のエネルギー効率化の促進。
  - “グリーンスクール”と呼ばれる健康的な高性能学校の建設促進。

- エネルギー省（DOE）を中心とする研究開発（R&D）の加速化（Title 6）
  - 太陽光エネルギー。
  - 地熱エネルギー（Geothermal Energy）。
  - 海洋・水力再生可能エネルギー（Marine and Hydrokinetic Renewable Energy）。
  - エネルギー備蓄システム。
  - その他。

- エネルギー政策のマネジメント改善（Title 8）

- 国際エネルギープログラム（Title 9）
  - 商務省を通じて、クリーン＆効率エネルギー技術を諸外国に輸出。USAID（国際開発庁）がこれを支援する。
  - 温室効果ガス（GHQ）排出量を削減する長期的目標を実現するための国際クリーンエネルギー財団の創設。

- エネルギー輸送およびインフラ（Title 11）
  - DOT（運輸省）に気候変動環境局（OCCE）を設置。

- 小規模事業者エネルギープログラム（Title 12）

- スマートグリッド（Title 13）

2.1.3. スマートグリッド政策

2007 年エネルギー自立＆安全保障法（Energy Independence and Security Act of 2007）

は、Title 13（スマートグリッド）の中で、米国の法律の中で初めて電力システムの近代化の必要性を認識し、“スマートグリッド（Smart Grid)”導入に向けた諸規定を設け、スマートグリッドの広範な設置に伴う規制面と技術面の障壁除去に向けた取り組みを示している。

2007 年エネルギー自立&安全保障法に規定されたスマートグリッド（Title 13）の“電気グリッドの現代化政策（Section 1301：Statement of Policy on Modernization of Electricity Grid)”では、米国のスマートグリッド政策を、将来的な需要の伸びを満たすことができる“信頼性のある、セキュアな電力インフラを維持するために米国の送電システムおよび配電システムの現代化を支援する”ものと規定している。

2007 年エネルギー自立&安全保障法（EISA）におけるスマートグリッド政策

スマートグリッド（Title 13）のセクション 1301： “電気グリッドの現代化に関する政策の表明（Statement of Policy on Modernization of Electricity Grid)”
米国のスマートグリッド政策は、将来的な需要の伸びを満たすことができる信頼性のある、セキュアな電力インフラを維持するために米国の送電システムおよび配電システムの現代化を支援することである。

上記の通り、2007 年エネルギー自立&安全保障法（EISA）は、スマートグリッド法の最初の規定である“Section 1301”の中で、確実な信頼性とセキュリティを保障する基幹インフラである電力グリッドの現代化を支援する政策を実施することを表明している。

米国は、先行きのエネルギー需要の大幅増加に対応するためには、発電プラントの新設と送電線の増設により、既存の送電系統および配電系統（T&D）のインフラを増強するのではなくて、先進的な情報基盤技術を利用してパワーグリッドの効率性、信頼性およびセキュリティを改善することを目指したのである。

National Electrical Manufacturers Association（NEMA:米国電気機器製造協会)や CRS（米国議会調査サービス局）によると、スマートグリッド政策の目的は、情報基盤技術を利用して、電力グリッドの効率性、信頼性および柔軟性を向上し、電力基盤増設の料金を引き下げることである。

2007 年エネルギー自立&安全保障法（EISA）のスマートグリッド政策の背景には、先進的インテリジェント IT を利用して既存のグリッド基盤を“現代化”して、可能な限り効

率的で、信頼性の高いセキュアなインテリジェント電力グリッド（つまり、“スマータグリッド）にして、電力の生産、供給および消費のバリューチェーン全体のビジネスプラクティスを改革することを目指しているとも解釈できる。

こうした考えや見解は、2007 年 12 月 18 日の NEMA（米国電気機器製造協会）の“電気サプライチェーンの知的レベル及びパフォーマンス分類の標準化[6]”レポートや CRS（米国議会調査サービス局）の連邦議会向け CRS レポート（第 110 回連邦議会包括的エネルギー法、H.R. 6）に詳しく表現されている。

2007 年エネルギー自立&安全保障法（EISA）に影響を与えたとみられる NEMA（米国電気機器製造協会）の上記のレポートは、ABB, Cooper Power Systems, Eaton, Emerson, GE, Nexans, Rockwell Automation, Siemens などの寄稿によるものである。本レポートでは、米国の電力業界は、発電、送電・配電ネットワーク等の電力供給、末端ユーザー（住居、商業ビル、工場、政府施設および軍事施設等）の 3 つの部分から構成される電気サプライチェーンのインテリジェンスの水準を向上させる努力を払うべきだと指摘する。しかし、インテリジェントな電気サプライチェーン要素の正確な意味とこのインテリジェンス（＝Smartness）を測定する方法が不透明である。

本レポートでは、電気サプライチェーンのシステムパフォーマンスを記述する主たる属性として次の要因を挙げている。

- 効率性（Efficiency）：電気サプライチェーンはどう効率的か？
  高性能システムはエネルギー効率が良く、エネルギーの転換と供給のプロセスにおけるエネルギーロス（損失）を最小化する。大幅なエネルギー節減は、発電資源の最適利用、最適な送電・配電ネットワークの設計と運転、効率的な需要サイド管理を通じて実現できる。
- 可用性と信頼性（Availability/Reliability）：デバイス、サブシステム、システムの信頼性（reliability）と高信頼性（dependability）はあるのか。アウトプットの質はどうか。
  電力グリッドを現代化し、システムの冗長性（system redundancy）を向上させれば、信頼性は改善される。しかし、デバイスとシステムの信頼性は個別に拮抗関係で作業すべきものではなくて、全体のシステムパフォーマンスに妥協をもたらさない方法で調整すべき課題である。また、システムの冗長性は割高になり、ハードウェアとソフトウェア分析の冗長性とのトレードオフの関係を考慮する必要がある。信頼性の別の側面は、アウトプットの質の問題に関係する。低品質の電

[6] Standardizing the Classification of Intelligence Levels and Performance of Electricity Supply Chains

気は電気サプライチェーン内でデバイスとシステムに悪い影響をもたらす。

- 制御可能性と相互運用性（Controllability and Interoperability）：デバイス、サブシステムおよびシステムは制御可能で、他との相互運用性はあるのか？
  現代の電力システムの重要な側面のひとつは、大きな可観測性（observability）を提供することである。戦略的に新作動システム（actuation systems）を実装するか、休止要素（dormant elements）を可能にすることで、その資産の制御可能性は大きくなる。制御可能性と相互運用性の程度が大きくなればなるほど、全体のシステムパフォーマンスは向上する。
- 持続可能性（Sustainability）：持続可能エネルギーの開発により未来のエネルギー需要を満たす。エネルギー効率の高い動力装置、ベストプラクティス管理、再生可能エネルギー源の利用拡大なども重要。
- セキュリティ：安定性、物理的セキュリティ、サーバーセキュリティに分類できる。高性能なシステムとデバイスの装備では、セキュリティの脅威問題を解決し、そのインパクトを軽減するセキュリティ措置を講じる必要がある。

本レポートが指摘するインテリジェンス（＝Smartness）の要因は次の通りである。

- 通信：状況意識を改善し、業界標準通信プロトコルをサポートする企業間のデータおよび制御パラメーターの相互作用と交換。
- コンピューテイションとアルゴリズム：機能アルゴリズムの複雑性と実効性。
- センシング技術と反応：センシングデータから完全にどのような情報を抽出することができるのか。
- アクション：どのようなアクションを実行できるのか。
- 適合性（Adaptability）：変化する環境における適合する柔軟性の度合い。

今の送電・配電系統を現代化するとの意味は、既存の電力グリッドを、次第に増大する将来の電力需要を満たす信頼性のあるパワーシステムに設備更新することで、極めて効率性の高い運転を行なえるグリッドにすることである。

NEMA（米国電気機器製造協会）によれば、今の送電システムをスマートグリッドに設備更新する主な狙いは、グリッドの電力供給容量を最大化して管理することである。大きく進歩したセンサー、通信、コンピューティングおよび情報技術（IT）を利活用することで、電気サプライチェーンを、よりインテリジェントで柔軟性のあるものにすることが可能となる。そうすれば、スマートグリッドは、“より信頼性が高く、より効率的で、障害および攻撃に対する回復力も強くなる（more reliable, more efficient, and more resilient to failures and even deliberate attacks）としている。

以上の背景から、エネルギー自立&安全保障法（EISA）は2007年12月19日にブッシュ大統領の署名により成立したのである。

2007年12月19日のエネルギー自立&安全保障法（EISA）は、スマートグリッドの諮問委員会とタクスフォースの設置（Section 1303）を義務づけて、スマートグリッド技術の研究開発と実証（Section 1304）を促進し、スマートグリッド投資のための連邦マッチングファンドの創設（Section 1306）を定めている。

また、Section 1305（スマートグリッドの相互運用性フレームワーク）に基づき、NIST（国立標準技術研究所）は、エネルギー省（DOE）と連邦エネルギー規制委員会（FERC）と協働して、スマートグリッドのデバイスおよびシステムの相互運用性を実現する情報マネジメントのためのプロトコルおよびモデル標準を含むフレームワーク開発に関する基本的な調整責任を担うと定められた。

以下は、2007年エネルギー自立&安全保障法（EISA）の主な規定の概要を可能な限り詳しく記載したものである。

2007年エネルギー自立&安全保障法におけるスマートグリッドの主な内容
① 電気グリッド（Electricity Grid）現代化政策の表明（Section 1301）：米国の（スマートグリッド）政策は、将来の需要の伸びを満たすことができる信頼性のあるセキュアなインフラを維持するために送電系統と配電系統を現代化することを支援することである。 ② スマートグリッドシステム報告（Section 1302）：エネルギー省（DOE）、電気供給&エネルギー信頼性局（OEDER-Office of Electricity Delivery and Energy Reliability）、新設するスマートグリッドタスクフォースは、スマートグリッドの利活用状況と規制面及び行政面の障害に関するスマートグリッドシステム報告書を連邦議会に提出すること（本法成立の1年後、その後は2年毎）。 ③ スマートグリッド諮問委員会とスマートグリッドタスクフォースの設置（Section 1303）。 ④ スマートグリッド研究開発および実証（Section 1304） ➢ 電力グリッド（Power Grid）デジタルIT（2008～2012年） ➢ スマートグリッド地域実証イニシアティブ（2008～2012年） ⑤ スマートグリッド相互運用性フレームワーク（Section 1305） ➢ NIST（国立標準技術研究所）は、スマートグリッドのデバイスおよびシステムの相互運用性を実現する情報マネジメントのためのプロトコルおよびモデル標準を

含むフレームワーク開発を調整する基本的な責任を担う。

⑥ スマートグリッド投資コストを賄う連邦マッチングファンドプログラムの設置(Section 1306)

⑦ 各州のスマートグリッド投資の検討（Section 1307）

⑧ 熱電伝併給施設（Combined Heat and Power Facilities）の開発に関する民間所有電線法（Private Wire Laws）の調査研究（Section 1308）

⑨ DOE（エネルギー省）によるスマートグリッドシステムのセキュリティ属性の調査研究（Section 1309）

2007 年エネルギー自立＆安全保障法（EISA）の送電系統および配電系統の現代化政策（Section 1301）において、スマートグリッドの特性は次のように定められている。

スマートグリッドの特性（Section 1301）

①┌ 電気グリッド（Electric Grid）の信頼性、セキュリティおよび効率性（reliability, security and efficiency）を改善するために、デジタル情報および制御技術(digital information and controls technology)の利用を増進すること。

②┌ グリッドの運転と資源のダイナミックな最適化と完全なサイバー・セキュリティ対応。

③┌ 再生可能資源を含む分散型資源＆発電の利活用と統合化。

④┌ 需要対応（DR-Demand Response）、需要サイド資源およびエネルギー効率資源の開発と組み込み。

⑤┌ メーター、グリッドのオペレーションと状態に関する通信および供給自動化のための“スマート”技術の利活用（スマート技術とは、家電機器およびコンシューマ・デバイスの物理的運転を最適化するリアルタイム、自動化および双方向の技術）。

⑥┌ “スマート”家電機器およびコンシューマ・デバイスのインテグレーション。

⑦┌ 先進的電気貯蔵技術およびピーク時電力抑制（Peak-shaving）技術のインテグレーション。プラグイン電気自動車・ハイブリッド車、蓄熱式空調（thermal-storage air conditioning）を含む。

⑧┌ 消費者へのタイムリーな情報と制御オプションの提供。

⑨┌ インフラを含む電力グリッドに繋げられる家電装置・機器の通信と相互運用性（communication and interoperability）の標準開発。

⑩┌ スマートグリッドの技術、プラクティスおよびサービスの導入に際してのづ合理かつ不要な障壁を明らかにし、削減すること。

しかし、このスマートグリッド定義を示す特性は極めて幅広い内容で、電力グリッドの多くの側面を網羅するものである。したがって、Congressional Research Service（CRS, 米国議会調査サービス局）などは、高度スマートメーターシステム（AMI-Advanced Metering

Infrastructure）により可能となる潜在的な顧客サービスに重点を置く次のような要約を示している。

高度スマートメーターシステム(AMI)とは、電気メーター、ガスメーター、水道メーターなどのデータ管理・表示・制御機器、マネジメント・システム、各機器間の通信などからなる新たな通信ネットワークおよびDBシステムである。AMIは、スマートメーターやその他のエネルギー管理デバイスとの2方向通信を含むもので、電力事業者とも双方向でデータの交換を通じて、消費者による需要対応（DR）を可能とするものである。

連邦議会向けCRSレポート：第110回連邦議会包括的エネルギー法（H.R. 6）の要約[7]
スマートグリッド（Smart Grid）とは、 家庭内のサーモスタット、電気製品およびその他のデバイスおよび電力会社への2方向で消費者のメーターからの情報の流れを許容する配電システムを指す用語である。 The term Smart Grid refers to a distribution system that allows for flow of information from a customer’s meter in two directions: both inside the house to thermostats and appliances and other devices, and back to the utility.
・電力需要が高まり、コストが高くなる期間に電気器具のスイッチを切り、常に変化する電気料金に関するリアルタイム情報を消費者に提供する。 ・スマートグリッド導入の目的は、電力グリッド（power grid）の効率性、信頼性および柔軟性を改善し、電気料金を節減することにある。 ・規制面と技術面の障壁で、これがスマートグリッド技術の導入を制限している。 ・現状、スマートグリッド技術の標準がなく、これがスマートグリッドの相互運用性を制限し、特定技術を実装したい企業の選択肢を制約している。

以上の通り、2つの食い違うスマートグリッドの定義は、米国内でもやや混乱を生じているが、大半の定義内容は今後の相互運用性と標準の開発ニーズに左右されると解釈されている。

2008年6月19～20日、政府関係省庁、電力業界、機器業界、大学および国研などの代表140人が参加してDOE（エネルギー省）主催の“スマートグリッド実装ワークショップ”が開催された[8]。このワークショップでは、2007年エネルギー自立&安全保障法（EISA）の送電系統および配電系統の現代化政策（Section 1301）において定められた10の“スマートグリッド特性”に関する議論が交わされ、GridWise Alliance, Electric Power Research Institute, Edison Electric Institute, Galvin Initiativeおよび Modern Grid Strategy

[7] Summary in the Smart Grid Provisions in H.R. 6, 110th Congress
[8] Metric for Measuring Progress Toward Implementation of the Smart Grid, Results of the Breakout Session Discussions at the Smart Grid Implementation Worksop

の間で一般的な合意を得て、次の 7 つに関するコンセンサスが得られた。

2008 年 6 月のスマートグリッド実装ワークショップの“スマートグリッド特性”に関するコンセンサス
特に、正当に計画、設計、実装・運用されるスマートグリッドは ① 消費者による積極的な参加を可能にする。 ② すべての発電オプションと電気貯蔵オプションを受容する。 ③ 新たな製品、サービスおよび市場を可能にする。 ④ デジタル経済における多様なニーズを応える電力の質を提供する。 ⑤ 資産効率を最適化し、効率的な運転を行なう。 ⑥ 自己発熱（self-heating）方式でシステム異常を予知し、これに応戦する。 ⑦ 物理的攻撃とサイバー攻撃および自然災害に対して回復力のある運転をする。

スマートグリッドの実装に伴う計測では、メトリックスとベースラインの確定、開発を追跡調査するデータの収集などが必要となる。上記の 7 つのスマートグリッド特性のメトリックスの事例は次の通りである。

- グリッドオペレータから情報を受けることが可能な消費者の割合（%）とこの情報に基づいて電気消費を決めるか、あるいは委任するオプションを持つ消費者の割合（%）。
- 電力システムのニーズに応じて制御可能な分散発電および貯蔵デバイスの割合（%）。
- end-to-end の相互運用性を証明する販売用スマートグリッド製品の数。
- イベントやシステム異常などの電力の質に関するデータを収集するための消費者一人当たりの計測ポイントの数。
- 電力供給システムに繋がれ、他に送電可能な資源（dispatchable resource）としてシステムオペレータに利用可能な分散型発電容量（MW）。
- モニターし、制御可能で、自動化されるグリッド資産（送電および配電機器など）の割合（%）。

因みに、2009 年 2 月 22 日にエネルギー省(DOE)の“電気供給&エネルギー信頼性局(Office of Electricity Delivery and Energy Reliability)”により発表された“The Smart Grid: An Introduction”では、2007 年 4 月の“A Vision for Modern Grid（現代グリッドのビジョン)”の中で示された今のグリッドとスマートグリッドの比較を次のように示している。

表 4　今のグリッドとスマートグリッドとの比較

スマートグリッドの特性	今のグリッド	スマートグリッド
積極的な消費者の参加を可能	消費者には情報を提供しない	消費者への情報提供と消費者

にする。	し、消費者が電力システムにも参加していない。	の積極的な関与：需要対応（DR）と分散型エネルギー資源。
全ての発電および電気貯蔵オプションを受容する。	中央型発電プラントにより占有：分散型エネルギー資源の相互連結には数多くの障害がある。	“プラグ&プレー”の便利さを持つ数多くの分散型エネルギー資源が再生可能を重視。
新たな製品、サービスおよび市場を可能にする。	限定的な卸電力市場：十分に統合化されていないことが、消費者の機会を制限。	熟成し、十分に統合化された卸市場：消費者のための新電気市場の成長。
デジタル経済に電力の質を提供。	停電を重視：電力の質の問題への対応が遅い。	電力の質が最重要課題で、質と価格のオプションも多様：早期問題解決。
資産効率の最適化と効率的な運転。	資産管理を伴う運転データのインテグレーションが不十分：縦割り型ビジネスプロセス（business process silos）。	グリッドパラメーターの大型データの取得：予防を重視し、消費者へのインパクトを軽減。
システム異常（自己発熱）を予見・対応。	更なる打撃を防止するための対応：資産を守ることを重視。	問題を自動的に検知して対応する：予防を重視し、消費者へのインパクトを軽減。
攻撃および自然災害に対して回復力のある運転。	悪意のあるテロ行為および自然災害に対して脆弱。	迅速な回復力を持ち、攻撃や自然災害に対する弾力性（Resilient）がある。

DOE（エネルギー省)のスマートグリッド実装ワークショップの議論
スマートグリッドの価値分野 ● 信頼性 ● セキュア ● 経済性 ● 効率性 ● 環境にやさしい ● 安全性

DOE（エネルギー省）の電気諮問委員会（EAC-Electricity Advisory Committee）は 2008 年 12 月、スマートグリッドの現状報告書を発表し、スマートグリッドの実装を促進するための 7 つの提言を示している。本報告書は、米国の“電力供給システム（エネルギーグリ

ッド）を、高経済成長、環境スチュワードシップ、エネルギー安全保障および消費者の選択を可能にする、よりインテリジェントで、障害回復力のある（resilient)、信頼性のある、自己平衡（self-balancing）で、しかも双方向性のネットワークに転換するという目標”に向けた電気諮問委員会（EAC）レポートである。

同レポートでは、①地球温暖化、②エネルギーコストの増大、③資本、原材料および人件費の上昇、④老朽化するインフラと労働力、⑤国家セキュリティ懸念の持続、⑥環境意識の高まり、⑦社会的プレッシャー、⑧エネルギー効率の要請、⑨エネルギー需要の増大、⑩消費者の期待の高まり、⑪早い技術イノベーションの課題を解決するのがスマートグリッドであると断言。様々な定義があることを認めつつ、同レポートでは、“スマートグリッド”を、“エネルギーバリューチェーンを最適化する広範なソリューション（a broad range of solutions that optimize the energy value chain)”であると定義している。

以下は、同レポートの概要を示し、2008 年 12 月現在の米国のスマートグリッドの実態を解析したものである。

電力会社のスマートグリッド導入の現状
➢ 大半の公益事業会社は、スマートグリッド計画の第 1 段階を決めるプロセスにある。複数の公益事業会社は既にスマートグリッドの主要要素を大規模利活用するための認可と補助金を規制当局から受領している ➢ 大半の会社は、コスト効果が高いとの実例があり、補助金も至急されることから、スマートメーターシステムから着手している。 ➢ 規模と程度にはばらつきがあるが、数多くの実証実験では、既にスマートグリッドの技術テストと消費者の受容検証を実施しつつある。 ➢ 他にも、停電、作業管理システム、変動所自動化（substation automation）、遠隔機器モニタリングなどの付加価値で、自動化メータリングシステムのための通信システムのメリットを活用しつつある。 ➢ 先行事例は、①Austin Energy、②Southern California Edison、③ONCOR AND CENTERPOINT である。 ① Austin Energy：オースチン・エナジー（Austin Energy）社のスマートグリッドイニシアティブは、SOA（サービス指向アーキテクチュア）を使うビジネスプロセスの再定義を行なう努力の中から生まれ、エンタープライズアーキテクチュア（EA）プログラムとして開始されたものである。オースチン・エナジーは、様々な需要対応（DR）、分散型発電および再生可能エネルギープログラムを通じて消費者の選択を可能にしている。以上のプログラムを実施した結果、同社は、運転コストを削減し、消費者に余剰コストを負担させることなく新技術投資が可能となっている。2008 年 8 月現在、13,000 のスマート

メーターと 70,000 のスマートサーモスタットの技術利用を進めている。2009 年 1～2 月までに、10,000 の新 T&D（送電・配電）グリッドセンサー、270,000 のスマートメーターおよび 70,000 のスマートサーモスタットの増設を計画している。現時点で、オースチン・エナジー（Austin Energy）社の顧客基盤の 100%はスマートグリッド技術によるサービス提供となろう。

② Southern California Edison（SEC）：2007 年エネルギー自立&安全保障法（EISA）の成立に先立つ 2006 年 7 月、カリフォルニア州は公益事業会社の PG&E が約 20 億ドルを投じて高度スマートメーターシステム(AMI)を設置する事業認可を行っている。カリフォルニアでは、スマートグリッド拡大の前提条件がコスト効果の高い AMI である。同州では、2010 年までにスマートグリッド利活用計画の要件を決める主要な法規則導入する予定である。この法案が通過すれば、カリフォルニアが州全域でスマートグリッドを導入する米国初の州になろう。2008 年 9 月、規制委員会であるカリフォルニア公益事業委員会（CPUC）は、料金負担者からの 16.3 億ドルのファンディングを使う SEC のスマートメータリングプログラムを認可した。エネルギー使用の効率化による需要対応（DR）と再生可能で分散された発電システムの実現を目的に、一般家庭や小規模事業者にスマートメーターに対する助成金拠出を行っている。サザンカリフォルニアエジソン（SEC）社は 2009～2012 年の期間、居住者および小規模事業者向けに 530 万のスマートメーターを新設する。Avanti として知られる電気回路(electricity circuit)を設計・活用して 14,000 件の顧客に電力を供給している。SCE は直近 5 年間に 50 億ドル、今後 5 年間に 90 億ドルを投じて、インフラを拡充し、拡大するサービス分野への対応と老朽化するコンポーネントを取り替え、複数のグリッドを空港、港湾、プラグイン車などの電子運転技術（electro-drive technology）に繋ぐ計画である。

③ ONCOR と CENTERPOINT:テキサス公益事業委員会(PUCT)は 2008 年 8 月、オンカー(ONCOR)社の先進的メータリングシステム（AMS）計画を承認した。この計画では、2012 年までに 300 万以上の先進的メーターをサービスエリアに設置する。居住者向けの月額のサーチャージは 2.21 ドルで、その他のコンシューマは約 2.41 ドル～5.18 ドルとなる。オンカーは、高速で無効電力を制御できる世界最大の静止形無効電力補償装置（SVC-Static Var Compensator)を設置する計画である。テキサス公益事業委員会（PUCT）は、センターポイントエナジー（CenterPoint Energy）が 127,000 の先進的メーターをヒューストン地区に設置することを承認した。

DOE（エネルギー省）の電気諮問委員会（EAC）は、スマートグリッドの重要性を検討し、コスト効果の高いスマートグリッド技術を開発することが最も米国民の利益に適うと認識。スマートグリッドは、エネルギー安全保障、気候変動、電力グリッドの信頼性および経済

成長における米国の目標を実現するメカニズムであるが、同時に、スマートグリッドのタイムリーな開発には、重大な課題もあるとして、次の7つの提言を行なっている。

EAC（電気諮問委員会）による7つの提言
① 全米にスマートグリッドを実現するためのロードマップを2009年12月までに開発。このロードマップに含めるべき要件は次の通り。 ・ スマートグリッドの基本的なコンポーネントの記述。 ・ 当該コンポーネント開発の優先順位付け。 ・ 追加投資を特に必要とするスマートグリッドのサブセクターの識別。 ・ 全米の公益事業会社およびその他の利害関係者により必要とされるスマートグリッド投資のタイムテーブル。 ・ シームレスに相互作用できる必要性のある電力グリッドにおける領域の識別。
② スマートグリッドのロードマップに基づいて、次のステップを明らかにするために、研究開発プロジェクトを開発、管理、実施および伝達し、2007年エネルギー自立&安全保障法（EISA）のスマートグリッド研究開発および実証（Section 1304）で認定されたスマートグリッド地域実証イニシアティブと連邦マッチングファンド（スマートグリッド投資マッシング助成金プログラム）を指令。
③ 連邦議会がスマートグリッド地域実証イニシアティブとスマートグリッド投資マッシング助成金プログラムに必要なファンドを配分することを要請する。また、連邦議会がNIST（国立標準技術研究所）に対して情報マネジメントのためのプロトコルおよびモデル標準を含むフレームワークを開発する調整機能を担うための助成金を供与することを要請する。
④ スマートグリッドのロードマップ実行を促すスマートグリッドプログラム局(Smart Grid Program Office)をDOE（エネルギー省）内に新設する。実施項目は次の通り。 ・ Webベースのセルサービス・ツールを使いグローバルスマートグリッド情報のクリアリングハウスとして機能すること。 ・ ベストプラクティス、技術支援、インフラ計画などの情報提供。 ・ 公益事業者規制当局、公益事業者、コンシューマやその他の利害関係者に教育材料を開発し、利用できるようにすること。 ・ 適切な各種組織におけるスマートグリッド活動の調整役を担うこと。 ・ NIST（国立標準技術研究所）が2007年エネルギー自立&安全保障法（EISA）で定められた評価の課題を完了すれば、公益事業者に比較スコアを公表することを要請し標準ベースの作業を促進すること。
⑤ DOE（エネルギー省）は、エネルギーのコストとこのコストをいかにすればよりよく管理できるかについての消費者教育に重点を置いた教育キャンペーンを実施すること。
⑥ 連邦議会、産業界、各州の規制当局およびその他の利害関係者と共同で、スマートグ

リッド対応の電気器具およびその他のデバイスの市場を駆動するインセンティブを創出すること。

⑦ 電気諮問委員会（EAC）をオバマ政権の“グリッド現代化委員会”として機能させ、全米レベルでのスマートグリッド導入を促進すること。

2.1.4. オバマ政権誕生後のスマートグリッド政策の動向

バラク・オバマ大統領は就任1ヵ月後の2009年2月17日、“2009年米国再生・再投資法（ARRA-American Recovery and Reinvestment Act)”に署名。オバマ新政権は、2008年9月のリーマンショックに端を発する経済危機を克服するめの緊急避難的な景気刺激策として総額7,872億ドル（対GDP比5.7%）の財政出動を決めたのである。この緊急対策の中のエネルギー予算は、390億ドルである。減税装置を含むと630億ドルにのぼるエネルギー投資は、①スマートグリッドへの110億ドルの資金供与（2010年末までに執行）、②再生可能エネルギーおよび送電技術の融資保証に60億ドル、③電力グリッドの現代化を実施する電気供給&エネルギー信頼性局（EDER）に45億ドル、④電気自動車（EV）技術に4億ドルなどの内容となっている。110億ドルのスマートグリッド緊急景気対策予算は、スマートグリッド技術、送電系統の拡張と設備更新、送電インフラの現代化と改善等に充当される。米国電気グリッドを現代化し、スマートで、エネルギー効率の高い、信頼性のある電気供給基盤への投資には、①エネルギー貯蔵、②サイバー・セキュリティと研究投資、③スマートグリッド技術の開発と実証、④エネルギー基盤のセキュリティと信頼性の向上、⑤エネルギー供給異常からの回復促進などである。

連邦助成金の配分を担うのはエネルギー省（DOE）である。連邦エネルギー規制委員会（FERC）は、送電グリッドの相互運用性と信頼性の標準を策定する責任を担うことになる。DOEの電気供給&エネルギー信頼性局（EDER-OFFICE OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY）は、2009年米国再生・再投資法（ARRA）に基づき、米国の電力グリッドを現代化するための110億ドルの助成金配分を担う。

予算の重点的配分分野
● 需要対応（DR）機器。 ● エネルギー基盤のセキュリティと信頼性。 ● エネルギー貯蔵の研究開発と実証、利活用。 ● エネルギー供給の混乱からの回復。 ● 2007 年エネルギー自立安全保障法（EISA）のスマートグリッド規程で認可されたスマートグリッド技術の研究開発および実証などのプログラムの実施。 ● スマートグリッド相互運用性フレームワークの実施。 ● スマートグリッド投資コストを賄う連邦マッチングファンド。

電気供給&エネルギー信頼性局（EDER または OE）の担当予算の多くは、専門家人材の雇用を加速化する予算で、1 億ドルがワーカー研修に充当される。その他の主な内容は、スマートグリッド相互運用性フレームワーク（1,000 万ドル）、未来の需要と送電要求のリソース評価と分析（8,000 万ドル）などとなっている。

2009 年 2 月 26 日、オバマ政権になって初めての 2010 年度予算案（概要）は予算編成権のある連邦議会に提案された。「新しい責任の時代：アメリカの約束を刷新（A New Era of Responsibility: Renewing America's Promise）」と題されたこの予算案（Blue Print）では、歳出規模は前年比 9.8%減の約 3 兆 5,520 億ドルとなった。景気刺激策、金融機関への支援策、イラク・アフガニスタンでの戦費拡大などを背景に、2009 年度の財政赤字は 1 兆 7,520 億ドルと、前年度（4,590 億ドル）の 3.8 倍に拡大し、対 GDP 比では 12.3%まで上昇する。2010 年度の財政赤字は 1 兆 1,710 億ドルに減少する見通しで、2013 年度までに半分まで減少させる計画である。

環境エネルギー政策では、①クリーンエネルギーへの投資促進、②石油依存の終結、③気候変動問題への取り組み強化、④新規雇用の創出（アウトソーシングできないもの）の 4 つが重点施策となった。オバマ政権は、温室効果ガスを 2020 年までに対 2005 年比で 14%削減、2050 年までに対 2005 年比で約 83%削減すると宣言し、同目標達成へ向けて「排出量取引制度（Cap-and-trade system）」を導入することを決めた。

エネルギー省(DOE)の予算要求額は 263 億ドルで前年度に比べて僅かに減少しているが、2008 年度の 241 億ドルを上回っている。主たる使途は、スマートグリッド、再生可能エネルギー、CCS（carbon capture and storage、炭素回収貯留）技術などである。これとは別に、DOE は景気刺激策として 387 億ドルを受領。うち 110 億ドルを、スマートグリッド技術、送電系統の拡張と設備更新、送電インフラの現代化と改善等に投じつつある。Yucca

Mountain に計画されていた核廃棄物貯蔵施設の建設は中断され、別の計画が求まられている。この他には、クリーンコール、CSS 技術などの投資、クリーンエネルギーへのローン保証などが決まっている。

2009 年米国再生・再投資法（ARRA）による総合景気対策の一環として、エネルギー省の電気供給&エネルギー信頼性局（EDER）は、39 億ドルのスマートグリッド関連プロジェクトの公募を公益事業者およびベンダーに呼びかけた。大半は、折半によるマッチングファンドの形をとっている。2009 年 6 月に公式発表された主な Call 内容は、①エネルギー貯蔵、②スマートグリッド/グリッドの信頼性、③送電および配電に分類されている。詳細は次の“Recovery.com”の“スマートグリッド投資グラント計画”を参照されたい。
http://www.energy.gov/recovery/infrastructurefunding.htm#SMARTGRID

オバマ政権の 2010 年度予算案（最終の詳細）は 2009 年 5 月 7 日に公表された。2010 年度（2009 年 10 月～2010 年 9 月）予算では、大統領府行政管理予算局（OMB-Office of Management and Budget）は、前年度に比べて大幅な歳出増を計画し、将来的には極めて大きなコスト節減を図ることになる。2010 年度の連邦 IT 支出総額は前年度の 707 億ドルから 7%増の 758 億ドルとなる。主たる IT 予算は、国土安全保障省（Homeland Security）のサイバー・セキュリティ、保健福祉省（HHS）の医療 IT、連邦クラウドおよびグリーンテクノロジーである。オバマ政権は 2010 年度予算案における IT 投資では、特にクラウド・コンピューティングを重視し、連邦 IT におけるイノベーション、効率性および実効性を高める重要なカギとなるツールだと位置づけている。

エネルギー省（DOE）の 2010 年度予算要求額は、前年度（338 億ドル）比 21.9%減の 264 億ドルである。2009 年度には、米国再生・再投資法（ARRA）の景気対策予算の 387 億ドルが追加されている。

2010 年度要求額が前年度に比べて約 73 億 5,400 万ドル下回っているのは、2009 年度予算に自動車産業救済を目的とする先進技術自動車製造ローン計画予算（75.1 億ドル）が含まれていたためである。ブッシュ前大統領の 2009 年度予算要求額との比較ではオバマ大統領の 2010 年度予算は 13 億 7,900 万ドル（5.5%）の増額となる。2010 年度予算要求は、輸入石油依存の軽減、米国の科学リーダーシップの回復、グリーンエネルギー経済への投資による雇用回復に対する大統領コミットメントを反映している。主な予算支出は、① 送電インフラの改善および再生可能エネルギー資源利用の拡大、②スマートグリッド開発の支援、③科学研究およびイノベーションによる米国リーダーシップ回復の促進、④プラグインハイブリッド車、原子力およびクリーンコール技術などである。エネルギー効率化および再生可能エネルギーの予算費目は、①燃料電池技術（6820 万ドル）、②ソーラーエネル

ギー（3.2億ドル)、③風力（7500万ドル)、④自動車技術（約3.3億ドル）などとなっている。

エネルギー省（DOE）の電気供給&エネルギー信頼性局（EDER）が担う2010年度予算は前年度に比べて7,100万ドル増の2億800万ドルである。要求予算増額の主因は、①エネルギー貯蔵、②スマートグリッド技術、③サイバー・セキュリティなどの研究開発投資である。

電気供給&エネルギー信頼性局（EDER）の主たる予算の内訳
① **研究開発（R&D）** ・ **クリーンエネルギーの送電と信頼性（4,200万ドル）**：グリッドの信頼性、効率性およびセキュリティを改善する先進的な送電主導技術（北米広域モニタリングシステム、第二世代超電導ケーブルのエネルギーロスを緩和する等） ・ **スマートグリッド研究開発（6,700万ドル）**：運転上のインテリジェンスと接続性を向上するために、全米の電気供給ネットワークを現代化する先進的技術を導入・統合することで効率的かつ完全に統合化されたスマートグリッドシステムの開発を促進。2010年度は、再生可能システム向けスマートグリッド機能の開発、プラグインハイブリッド車および末端利用アプリケーションなどの先進的制御方法の研究、産業および政策当局向けのスマートグリッドシステムのシュミレーションツールの開発、スマート素材基盤のセンサーおよびデバイスに特化した新グリッド素材、デバイスおよびシステムハブの構築。 ・ **エネルギー貯蔵（1,500万ドル）**：エネルギー貯蔵技術の開発促進等（2010年度） ・ **エネルギー供給システム向けサイバー・セキュリティ（5,000万ドル）**：2010年度の活動は、電力系統監視システムのSCADA/EMS System（Supervisory Control and Data Acquisition/Energy Management System)のテストベッド評価、レガシーシステムの移行戦略として信頼性のあるシステムを構築するためのモデル開発、サイバー・セキュリティに対応可能なセキュアシステムを開発するためのスマートグリッド技術の研究。 ② **許認可、分析等（640万ドル）**：クリーンエネルギーのアクセスに必要な電力基盤の開発を促進するための政策、市場メカニズム、州法などの技術および財政支援等。 ③ **電力供給基盤セキュリティおよびエネルギー信頼性（620万ドル）**：全米のクリティカルなエネルギー基盤を脅威と災害から防護するセキュリティの改善活動。停電および復旧の可視化およびモデル化の促進などの電力供給基盤の信頼性の向上、州・地方政府の緊急対応活動の支援、重要な資産および相互依存を識別するための堅牢（Robust）なシステム分析。 ④ **プログラム指示（2,140万ドル）**

2010 年度予算案では、研究開発プログラムの再編が行われ、2009 年度予算の高温超電導 R&D、再生可能・分散型エネルギーシステム統合、送電信頼性関連活動が“クリーンエネルギーの送電と信頼性”に統合化され、サイバー・セキュリティ活動が“エネルギー供給給システム向けサイバー・セキュリティ”となった。新設されたのは、“スマートグリッド研究開発”である。

2.2.　米国における主な電力グリッドの研究

2.2.1　グリッドワイズ・アライアンス

米国では、官民パートナーシップの非営利団体である“GridWise Alliance（グリッドワイズ・アライアンス）”が、エネルギー省（DOE）と提携して、イノベーティブな新技術を利活用して米国電力網（national electricity grid）を抜本的に変革する構想の実現に取り組んでいる。

グリッドワイズ・アライアンス（GridWise Alliance）が創設された背景は、エネルギー省（DOE）の PNNL（パシフィックノースウェスト国立研究所）の技術者リーダー達が 2000 年の春に、いかにして 2010 年までにエネルギーシステムを進化させるかを検討したことに始まる。送電系統の実績がある電力網（electric power grid）の専門家達が、分散型発電や負荷管理などの統合型分散リソースの潜在的影響を理解する努力を払った。また、これに平行して、エネルギー科学者達が商業ビルのエネルギーシステムのエネルギー廃棄物を見極める自動診断システムの収益機会が極めて大きいことを発見したのである。カリフォルニアの電力危機が契機となって、既存のエネルギー市場が新技術導入を妨げているかが明らかになった。以上のような考え方が重なり合って、電力システムを大転換させる新エネルギー技術の潜在的な可能性を実現するためには、情報技術（IT）がキャタリスト（触媒）機能を果たすイネブラー（Enabler）になるとの構想につながったのである。

エネルギー省（DOE）傘下の PNNL（パシフィックノースウェスト国立研究所）は、自己資金で“エネルギーシステム転換イニシアティブ（ESTI）”に着手し、この科学技術基盤の研究を行い、関連する技術と政策の特性を見極めることになった。こうした努力から蓄積された知識に基づく先進的電力システムのビジョンを表示する言葉として、“GridWise（グリッドワイズ）”が選ばれたのである。

未来の電力網を描くグリッドワイズ（GridWise）ビジョンでは、IT による電力系統の革命という考え方が前提となっている。基本的には、“鉄よりも、ビットの方が割安”であるからだ。IT を使い分散型のネットワーク基盤電力システムを構築すると、価格安定化にとって重要なカギである消費者のエネルギー市場参加を促すことができる。公益事業会社から、サードパーティや消費者にいたる市場参加者も、企業や規制の枠組みを超えた横断的なソリューションを開発し、利活用することで付加価値を生み出すことになる。エネルギーシステムの大転換は、国家安全保障を高める喫緊のニーズに対応するものである。

2001 年 9 月 11 日のテロ攻撃、2003 年 8 月の米国北東部の大停電、ハリケーン・イザベ

ルによる停電などを契機に、米国エネルギー基盤の脆弱性に対する関心が強まり、GridWise（グリッドワイズ）ビジョンが 2005 年度に大統領のイニシアティブによりエネルギー省（DOE）の新政策として提案されたのである。この結果、エネルギー省（DOE）と連携した形で産業界も巻き込み、GridWise（グリッドワイズ）ビジョンを実現する官民パートナーシップの非営利法人として、グリッドワイズ・アライアンス（GridWise Alliance）が 2004 年に創設されたのである。また、相互運用性のある、対人交流通信（interoperable, transactive communications）の全体的枠組みを定義するために、グリッドワイズ・アーキテクチュア会議も設置されたのである。

グリッドワイズ・アライアンス（GridWise Alliance）は 2004 年 3 月 25 日に、エネルギー省（DOE）の配電エネルギー信頼性局（Office of Electricity Delivery & Energy Reliability）との間で、米国電力グリッド転換ビジョンを実現する共同事業のための MOU（覚書）を締結している。この目標は次の通りである。

- IT を利活用して､他のビジネス面を革命したようにエネルギーシステムを革命すること。
- 企業および規制の垣根を超える横断的な技術ソリューションを開発し、利活用することですべてのエネルギー市場参加者に価値を創造すること。
- 柔軟性と適応性のある情報量の豊富な電力グリッドを通じてセキュリティと信頼性を向上すること。
- 消費者が電力グリッド運転への参加による恩恵を授かるようにすること。

グリッドワイズ・アライアンス（GridWise Alliance）のアクションプランは次の通り。

- チャレンジ１：グリッド転換によるメリットを実現するイノベーティブナ技術の開発と利用。産業横断的にさまざまな技術課題を推進し、新技術ニッチを開拓し、新製品・サービスのイノベーションを促す広範な技術戦略を策定する。①業界の専門家グループによる産業横断的な共同作業の対話の枠組みを決め、メンバーと産業グループとの交流を促進して、技術ギャップを見極め、技術ギャップを埋める、②合理的な実用できるグリッドワイズの構成や範囲の実証課題を策定する、
- チャレンジ２：イノベーションを支える産業インフラへの再投資。イノベーティブナ技術を利活用するための成功する事業戦略と規制戦略を策定し、新たな製品とサービスの研究開発を維持するために不可欠な官民両面の投資を促す。①オープン・フォーラムを通じた規制上の問題点や障害を明らかにし、問題解決を図る、②先進的ソリューションを使い、既存の電力網基盤に替わる新たなビジネスモデルを構築する、③エンドユーザーからバルク電力市場に至るエネルギー産業バリューチェーンの官民連

携やパートナーシップを促し、独創的で、イノベーティブなソリューションを図る地方、地域および国レベルの意見交換の場を設定。

- チャレンジ3：グリッド大転換を促すビジョンと価値を構築し、情報公開を促進。

グリッドワイズ・アライアンス（GridWise Alliance）

米国エネルギー省（DOE）と連携する官民コンソーシアムの非営利法人で、ITを利活用して既存の電力網を大転換し、インフラ、プロセス、デバイス、情報、市場を統合化し、コスト効率と実効性の高い発電と配電、電力消費を行い、より堅牢で、セキュアな信頼性のあるエネルギーシステムを構築することを目的とする。連邦政府、州政府および産業界の官民コンソーシアムとして、エネルギー省（DOE）との2004年3月のMOUで定められた目標とアクションプランに基づき、グリッドワイド（GridWise）ビジョンに関する業界や規制の枠組みを超えた意見交換、問題解決を図る議論を行うフォーラムを開催。

① エネルギー省（DOE）傘下のPNNL（パシフィックノースウェスト国立研究所）とバッテル（Battelle）研究所等の関連研究機関は、創業メンバーとして、エネルギー省(DOE)を代表して、グリッドワイズ・アライアンス(GridWise Alliance)の活動を支援する。

② 2002年の先進的通信制御プログラムと2004年の分散相互接続プログラムを踏まえて2005年向けに新たに“DOE(エネルギー省)グリッドワイズ計画”を策定。CERTS（電力信頼性技術ソリューション）、EPRI（電力研究所）のインテリグリッド（InteliGrid）、ワシントン州立大学GRIDSTATなどの研究事業を展開。

会長：Guido Bartels：
IBMのGlobal Energy & Utilities industryのジェネラルマネージャ。

グイルド・バーテルズ（Guido Bartels ）はオランダ人で、米国で居住。IBMでエネルギー業界との戦略的ビジネス連携の責任者。米国エネルギー省（DOE）の電力諮問委員会（EAC）委員兼スマートグリッド委員会の委員長として、2005年エネルギー法、2007年エネルギー独立・安全保障法の策定を支援。

プレジデント：Katherine Hamilton：
プライベートインベストメント会社、Good Energies, Incを経てグリッドワイズ・アライアンス（GridWise Alliance）の副会長に就任。

キャサリン・ハミルトン（Katherine Hamilton）は、エネルギー省（DOE）の NREL（米国代替可能エネルギー研究所）で勤務し、連邦エネルギー監査および節水計画を含む 1992 年エネルギー政策法に盛り込まれた複数のプログラムを策定。ハミルトングループの創業者兼 CEO。米国バイオエネルギー協会（American Bioenergy Association）の共同ディレクターを歴任。

副会長：Terry Mohn：Sempra Energy の技術ストラテジスト。2 社のインターネット会社を創業し、国際放送局の CTO を経て、Sempra Energy に入社。

メンバー：
ABB、アクセンチュア、アルカテル・ルーセント、AEP、アレバ T&D、AT&T、Austin Energy、シスコ、Duke Energy、EDF、ESRI、フロリダ州立大学、HP、IBM、インテル、Itron、KEMA、Landis+gyr、ロッキードマーティン、PNNL（パシフィックノースウェスト国立研究所）、シャープ、SAP、シーメンス、ワシントン州立大学、その他。

グリッドワイズ・アライアンス（GridWise Alliance）担当 PNNL（パシフィックノースウェスト国立研究所）の主要メンバー

マネジメントチーム
Jeff Dagle：電気エンジニア。先進的電力系統分析およびシミュレーションソフトウェアの専門家。 インフラ情報アシュアランス（IA）技術、システムおよびアプローチ手法に関する技術支援を提供。
Carl Imhoff ：エネルギーオペレーションおよびプロダクトチームのエンジニア。
Rob Pratt：PNNL のエネルギーシステム大転換イニシアティブのリーダー。

2.2.2 電力中央研究所（EPRI）

電力中央研究所（EPRI-Electric Power Research Institute）は、米国の 90%以上の発電会社および送配電会社の会員企業と世界 40 カ国の 450 のメンバーによる資金拠出で設立された独立系 NPO の研究機関である。EPRI のオフィスは、シリコンバレーのパロアルト、ニューヨークのシャーロット、テネシーのノックスビル、マサチューセッツのレノックスにある。電力中央研究所（EPRI）は、一般公衆の利益になる発電、電力の供給と利用に関連する研究開発を実施し、学術界と産業界の科学者、技術者および専門家を集め、電力の信頼性、効率性、保健、安全性および環境などの問題解決を支援している。EPRI（電力中

央研究所）はまた、長期的なR&D計画を牽引する技術、政策および経済分析を行い、エマージングテクノロジーの研究も支援している。

電力中央研究所（EPRI）の協働研究（Collaborative Research）チームは、学術界および産業界の異業種間の科学者、技術者および専門家チームで構成され、1ドルの研究投資につき、10ドルの価値をもつ研究開発、技術の実証を実現することを求められている。2007年には、米国電力業界のR&D投資の約72%は電力中央研究所（EPRI）で行なわれている。電力分野の主な研究セグメントは、発電、環境、電力供給&エネルギー利用、原子力である。年間1600以上の研究開発プロジェクトが実施され、3億ドル以上の研究開発投資が行われ、400人以上の異業種の科学者、技術者および専門家がR&Dプロジェクトに関与している。

2008年3月5日、米国エネルギー省（DOE）とEPRI（電力中央研究所）は、エネルギー効率の改善促進を目指すエネルギー技術の研究開発および利活用に関する協力体制を強化する覚書（MOU）を締結した。この狙いは、ピーク時のエネルギー利用を抑制する努力の中でエネルギー効率を改善し、電力の需要反応（DR-demand response）計画の広範な採用を促進することにより米国民の増大する電力需要を満たすことである。

エネルギー効率代替可能エネルギー局次官補（Assistant Secretary for Energy Efficiency and Renewable Energy）のアレクサンダー・カースナー（Alexander Karsner）と電力供給エネルギー信頼性局次官補のケビン・コールバー（Kevin Kolevar）の両氏がエネルギー省（DOE）を代表してMOUに署名している。また、研究開発担当の上席副理事長のマイケル・ハワード（Dr. Michael Howard）と、電力供給利活用担当の副理事長であるアーシャ・マンスール（Arsha Mansoor）の両氏がEPRI（電力中央研究所）を代表してMOUに署名している。

両機関は、定期的な会合、公表データの交換、ワークショップの開催などを通じたコラボレーションを進めていく。この協働ワークの目的と活動は次の通りである。

① ビル、産業プロセスおよび末端利用における需要反応とエネルギー効率、エネルギー消費デバイスと装置に関連する研究の協力と支援。
② 米国内のエネルギー効率、健康および生産性を高めるために、ビルと電力システムの機能性を向上させる電力システムの相互運用性とビル関連ソフトウェアおよびデジタルデバイスを奨励する作業を電力業界、通商団体および関連業種で実施する。

③ ダイナミックなエネルギー管理システムとスマートグリッド型アプリケーションの一部となるデジタルデバイスの機能性と相互運用性を実証する試験を協働して実施する。
④ 電力会社がエネルギー効率と需要応答の計画と技術から CO2 排出量の削減などを行なうことができるガイドラインと方法を開発する。
⑤ 電力会社のエネルギー効率計画の管理者により維持されるデータベースを比較分析と比較検証し、エネルギー効率技術の性能一覧表を作成する。

電力中央研究所（EPRI-Electric Power Research Institute）

米国の 90%以上の発電会社および送配電会社の会員企業と世界 40 カ国の 450 のメンバーを抱える独立系 NPO の電力研究機関である。米国エネルギー省（DOE）と密接に連携している。主なオフィスは、シリコンバレーのパロアルト、ニューヨークのシャーロット、テネシーのノックスビル、マサチューセッツのレノックスにある。

① 電力中央研究所（EPRI）の協働研究（Collaborative Research）チームは、学術界および産業界の異業種 400 人以上の科学者、技術者および専門家で構成され、1 ドルの研究投資につき、10 ドルの価値をもつ研究開発、技術の実証を実現。
② 米国電力業界の 2007 年度の R&D 投資の約 72%は電力中央研究所（EPRI）で実施。主な研究セグメントは、発電、環境、電力供給&エネルギー利用、原子力。
③ 年間 1600 以上の研究開発プロジェクトが実施され、3 億ドル以上の研究開発投資を実施する。

主な幹部

会長:Richard H. Silverman:アリゾナ州フェニックスの水道・電力会社、Salt River Project（SRP）の General Manager 兼 CEO
副会長：James L. Turner：Duke Energy Corporation のグループ CEO
理事長兼 CEO:Steven R. Specker:30 年の GE での勤務（発電、送電および配電）後、Specker Consulting, LLC の社長、2004 年 9 月に、EPRI の理事長兼 CEO に就任。
上席副理事長（渉外）：Henry A. ″Hank″ Courtright
上席副理事長（総務、秘書）：Norma Formanek,
上席副理事長（研究開発）；Dr. Michael Howard
副理事長（技術アドバイザリサービス）：Rob Chapman
副理事長（原子力、チーフ核オフィサー）：Chris Larsen
副理事長（電力供給・利用）：Arshad Mansoor
副理事長（マーケティング&IT）：Dennis Murphy

副理事長（イノベーション）；Rosa Yang

【インテリグリッド・コンソーシャム(InteliGrid Consortium)】

米国の電力供給システムは主に 1950 年代に開発された技術に基づいており、設置してから 40 年以上も経過している。北米電力信頼性協議会（NERC）の信頼性評価レポートによると、需要は 2002～2011 年の期間に 20%の伸び率となるが、わずか 3.5%の送電系統の設備投資しか計画されていない。一方、一日あたりの卸電力取引量は 1998 年以降、約 400%の増加となっている。この結果、米国では、送電線の混雑が深刻な程度に拡大し、卸電力フローのボトルネックの主因となっており、また、電力供給システムのストレス水準も増大している。以上の背景から頻繁に生じる大きな停電などの事件を背景に、米国の電力業界は電力供給システムに ICT（情報通信技術）を利活用する研究技術開発に乗り出したのである。

EPRI（電力中央研究所）に吸収合併された E2i（Electricity Innovation Institute；電力イノベーション研究所）は 2001 年、50 万ドルの助成金を得て、デジタル社会のニーズを満たすために、ICT を使った未来のインテリジェント電力供給システムを構築するための産官学コンソーシアムを開始した。GE が幹事会社となり、SISCO、ルーセント、UCI（Utility Consulting International）などの国内外のエネルギー会社、連邦政府および州政府の関係機関、テクノロジー会社が結集して官民パートナーシップで開始されたこのプロジェクトは、デジタル社会を支える電気インフラコンソーシャム（CEIDS-Consortium for. Electric Infrastructure to Support a Digital Society）と呼ばれが、後に、インテリグリッド・コンソーシャム（InteliGrid Consortium）と改称された。

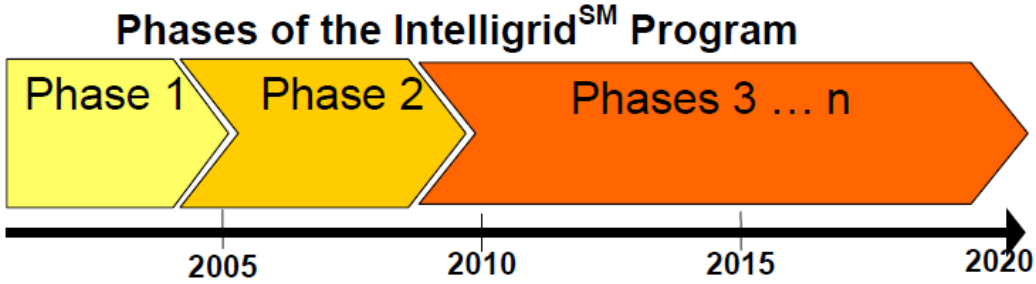
米国のインテリグリッド・コンソーシャム（InteliGrid Consortium)は、より堅牢で、需要応答型の電力供給網（power delivery grid）である未来のインテリジェント電力供給システムを構築するための産官学共同 R&D 組織である。電力会社、製造業者、研究者、政府高官が官民パートナーシップにより、未来のインテリジェントな、自己加熱電力システム（Self-heating power system）を実現するためのエマージング技術を統合化する共同研究であるともいえよう。

2003 年 4 月、エネルギー省（DOE）は、多年度予算計画である CEIDS（デジタル社会を支える電気基盤コンソーシアム）への参加を表明。米国は、官民連携で、デジタル化が強まる社会の需要に対応する 21 世紀の電力供給基盤を確保するために必要な複雑問題の解決に乗り出したのである。エネルギー省長官の Spencer Abraham の上席政策顧問であった Jimmy Glotfelty が、エネルギー省（DOE）側の CEIDS 担当責任者となった。CEIDS は、ルーセン

ト・テクノロジーなどとの共同研究で、GE Global Research をヘッドとする送電・配電システムのオープンアーキテクチュアの初期設計を実施するプロジェクトを決めた。18 ヶ月の期間でで数百万ドルを費やす送電配電系統オープンアーキテクチュアの開発プロジェクトは、未来のスマートグリッドを支えるのに必要な通信インテリジェント機器設計のための全体的な技術上の枠組みを定義するものであった。

インテリグリッド（InteliGrid）プロジェクトは次の 3 段階による。

図 20　インテグリッドプロジェクトのフェーズ



インテリグリッド（IntelliGrid）計画のフェーズⅠである“CEIDS（デジタル社会を支える電気基盤コンソーシアム）”は未来の電力供給システムのビジョンを策定するために、2003 年 7 月に“CEIDS マスタープラン”を開発し、2004 年 8 月に、機能要求である“Integrated Energy and Communication Systems Architecture Vol. Ⅱ, Functional Requirements（IECSA）”を策定した。2001～2004 年の多年度予算による CEIDS（デジタル社会を支える電気基盤コンソーシアム）の初期プロジェクトは、この IECSA の開発で第一段階を完了した。

プロジェクト参加メンバーは次の通り。

- 電力会社：Aliant Energy、Bonneville Power Administration、Consolidated Edison Company、Exelon、Kansas City Power & Light、Long Island Power Authority, New York Power Authority、Salt River Project 他。2008 年 9 月、IBM も参加。
- 国際電力会社：EDF（フランス電力公社）、Polish Power Grid Company
- 官庁：米国エネルギー省（DOE）、California Energy Commission
- 製造業者：Cisco Systems、ABB、UTC Power

2004年8月のIECSA（総合エネルギー通信システムアーキテクチュアVol.Ⅱ：機能要求事項）は後に、インテリグリッド・アーキテクチュア（IntelliGrid Architecture）と呼ばれるようになった。インテリグリッド・アーキテクチュアは、未来の全体グリッドの包括的なレファレンス・アーキテクチュアに基づくオープンシステムである。この機能要求のガイドラインに依拠すれば、インテリジェント機器とデータ通信ネットワークを電力業界の分散型コンピューティングシステムの中にインテグレーションすることが可能になる。

2004年8月に発表されたインテリグリッド・アーキテクチュア（IntelliGrid Architecture）は、通信と電力を“スマートグリッド”へと繋ぎ、デジタル化を強める社会により求められる機能性と柔軟性を提供する最初の包括的な技術フレームワークである。ここでは、①未来の電力供給システムを支える通信基盤の機能要求、②通信システムの設計時に電力会社が使う方法論とツール、③通信システムの設計とインストール時に電力会社が使う標準と技術の提案などが定義されたのである。

欧州委員会が他国のエネルギー研究をまとめたレポートによると、米国の初期段階（2000～2004年）の“インテリグリッド・コンソーシャム（IntelliGrid Consortium）”の概要は次の通りである。

インテリグリッド・コンソーシャム（IntelliGrid Consortium）
① 2000～2004年のインテリグリッド（旧CEIDS）産学研究プロジェクトに約1,260万ユーロの助成金が付与される。既存の電力系統の設備更新と近代化による電力システムの改善を促進した点で注目に値する。 ② インテリグリッド（IntelliGrid）プロジェクトは、既存の電力系統における複数の機能ギャップ問題の解決を図ることでインテリジェント電力基盤の構築を目指す 重要な取組課題 ➢ 通信基盤/オープンアーキテクチュアのインターフェースを構築する。 ➢ 電力基盤をモデル化・分析するための高速かつ正確な計算手法を開発する。 ➢ 電力基盤のSQRA（Security、Quality、Reliability、Availability：セキュリティ、質、信頼性および可用性）の要求事項の特性を示す。 ➢ 電力供給システムの自動化、ライアルタイム・モニタリングおよび制御をサポートするコスト効果の高いテクノロジーを開発・実装する。 ➢ 分散型エネルギー源（DER）がエネルギー市場で一定の役割を担うことを可能にする。 ➢ 供給、負荷および市場データための効果的な予測ツールを開発する。

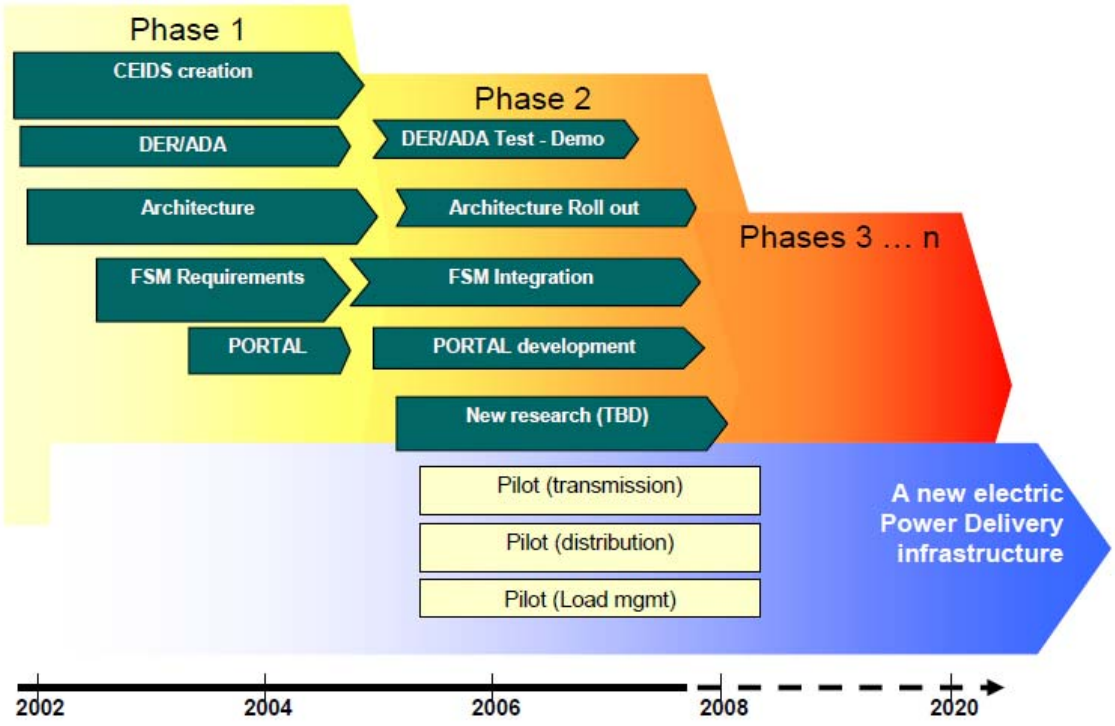
- 消費者と企業が、環境にやさしいエネルギー利用を制御し、最適化および指令することに役立つコスト効果の高い高付加価値な製品とサービスを創出する。

③ インテリグリッド（IntelliGrid）プロジェクトの主な成果は、高速シミュレーションとモデリングツールの機能要件とアプリケーション、双方向の消費者ポータルの設計などである。

同プロジェクトの狙いは、長期的な利用によりユーティリティ当たり数百万ドルの節減である。先進的な電力供給システムの金銭的利益は、業界全体で約 6,720 億ユーロ/年と見積もられている。電力系統全体のソリューションは信頼性を高めると期待され、業界全体で約 269 億ユーロの金銭的利益があると見込まれる。オープンアーキテクチュア使用の実装で、設備投資所要額は軽減され、業界全体でユーティリティ当たり数千万ドルの節減になる。

インテリグリッド（IntelliGrid）計画のフェーズⅠでは、電力業界向けの未来の電力供給システムのビジョンを策定し、重要な Enabling テクノロジーを研究開発する 4 つのプロジェクトに取り組み、2004 年 8 月に、未来の電力グリッドのオープンアーキテクチャの機能要求であるインテリグリッド・アーキテクチュア（IntelliGrid Architecture）を公表した。2005 年から開始されたフェーズⅡでは、フェーズⅠの R&D 努力を引き継ぎ、電力供給システム内の新たな機能性を創出する技術の実装を行っている。フェーズⅡのプロジェクト概要は次の通りである。

図 21　インテグリッドプロジェクト　フェーズⅡ概要



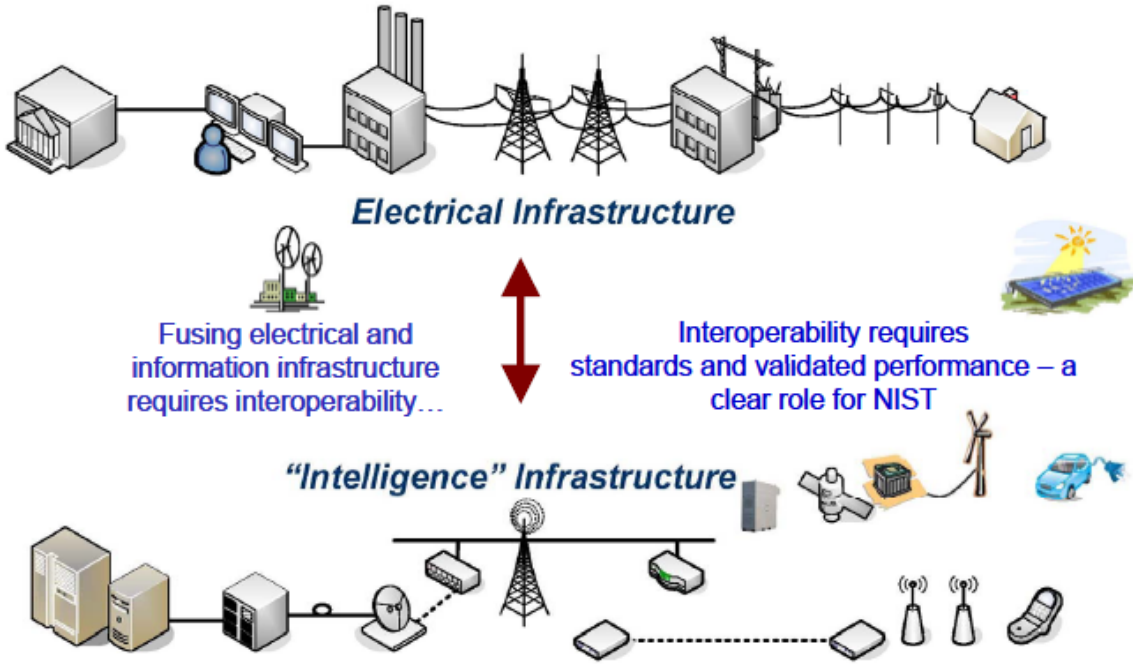
2.2.3　NIST（国立標準技術研究所）

NIST（国立標準技術研究所）は、米国商務省（DOC）傘下にある非規制連邦エージェンシーの計測標準研究機関である。NIST の任務は、先進的な計測科学、標準および技術の促進により米国のイノベーションと産業競争力を強化することである。2009 年の予算額は 16 億ドルで、科学者、エンジニア、技術専門職およびアドミスタッフの数は 2900 人にのぼる。NIST の主なプログラムは、①NIST ラボ（米国の技術基盤を前進させる研究を実施）、②ボルリッジ国家品質計画（Baldrige National Quality Program）、③Hollings Manufacturing Extension Partnership（HMEP）、④産学共同研究を促進するテクノロジーイノベーションプログラム（TIP）の 4 つである。

NIST（国立標準技術研究所）はエネルギー省（DOE）と連邦エネルギー規制委員会（FERC）とも協働ワークを実施し、公益事業会社、機器メーカー、電力系統事業関係者とも計測技術や国際標準化活動の支援を行っている。2007 年のエネルギー自給及び安全保障法（EISA-Energy Independence and Security Act）に基づき、NIST はスマートグリッドのデバイス

およびシステムの相互運用性を実現する情報マネジメントのためのプロトコルおよびモデル標準を含むフレームワーク開発の調整責任を担っている。特に、オバマ政権のエネルギー自給と温室効果ガス排出の削減を柱とする経済対策である 2009 年の“米国回復再投資法（ARRA）”では、エネルギー省（DOE）から 1,000 万ドルの予算を獲得し、エネルギー自給及び安全保障法（EISA）で指定された責務を遂行することになっている。加えて、NIST は米国回復再投資法（ARRA）ファンディングから 500 万ドルの助成金を取得し、米国電力系統向けの相互互換性のある全米規模のスマートグリッドの包括的フレームワークの共同開発を支援する。

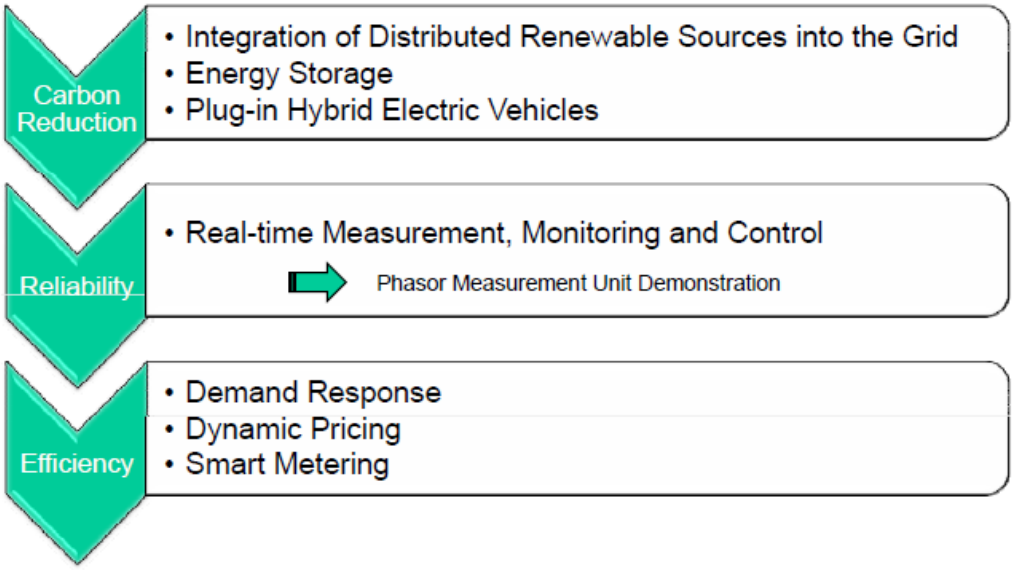
図 22　スマートグリッドが繋ぐ電力基盤とインテリジェンス基盤の関係図



電力系統のデバイスとコンポーネントを相互接続する相互運用性（Interoperability）の確保は、電力グリッドの数多くの相互接続された要素間のインテグレーションと双方向通信を可能にするスマートグリッドの性能にとっては極めて重要である。実効性の高い相互運用性は、インターフェース、プロトコルおよびその他のコンセンサス標準の統合フレームワークの上に構築される。例えば、スマートグリッドの“スマート装置”とメーターは消費者がどのくらいの電力を使い、いくらの料金になるかを消費者に示し、消費者が電気の消費と電気代をコントロールすることができるようになる。また、このコンセンサス標準は、太陽光発電、風力発電や代替可能エネルギー源など様々なエネルギー供給源のミックス管理を図ることを可能にし、気候変動への応戦にもなる。NIST のタスクは、次世代通信ネットワークの標準開発に酷似している。テレコムネットワークのように、スマート

グリッドは業界が完全所有し、運転するものである。したがって、スマートグリッドの相互運用性とサイバー・セキュリティの標準は、必要に応じては政府主導により、業界のコンセンサスを反映し、業界の積極的な参加を促す必要性がある。以上の考え方を背景に、NIST（国立標準技術研究所）は、先進的ネットワーク技術とサイバー・セキュリティ対策の知見とノウハウを活かし、スマートグリッド相互運用性標準プロジェクトに着手したのである。

図 23　NIST スマートグリッド相互運用性標準プロジェクト



スマートグリッドに相互運用性を導入する NIST の初期段階努力は次の通りである。

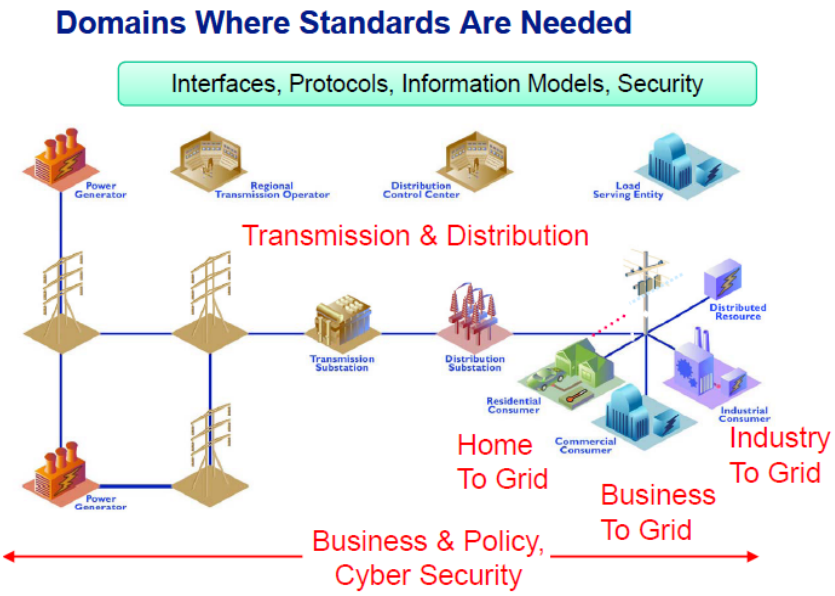
NIST の 3 ヵ年の実績
2007 年 12 月 ● 2007 年のエネルギー自給及び安全保障法（EISA- Energy Independence and Security Act）に基づき、NIST はスマートグリッドのデバイスおよびシステムの相互運用性を実現する情報マネジメントのためのプロトコルおよびモデル標準を含むスマートグリッド標準化調整責任を指定される。 2008 年 ● エネルギー省、連邦エネルギー規制委員会（FERC）とも協働ワークを実施し、公益事業会社、機器メーカー、電力系統事業関係者とも計測技術や国際標準化活動の支援を行う。 ● 100 社以上の参加企業を得て、ドメインエキスパートワーキンググループ（DEMW）を組織化。

- 公的傘下を促進する Twiki Collaboration ウェブサイトを開始。
- 相互運用性知識基盤を開始。
- 2008 年 11 月、Grid Interop 会議で 3 日間のワークショップを開催。

2009 年

- スマートグリッドがオバマ新政権の重要課題となる。
- エネルギー省の ARRA（米国回復再投資法）は、NIST への 1000 万ドルを含む 45 億ドルのスマートグリッド資金供与を決める。
- スマートグリッドの標準策定が喫緊の課題となる。
- 3 段階計画を発表。

図 24　NIST が考える標準を必要なとするドメイン分野の図



- エネルギー省（DOE）傘下に設置された電力のサプライヤーとユーザーの団体である GWAC（GridWise Architectural Council）と連携して、ドメインエキスパートワーキンググループ（DEMW）を設けて、次のテーマに特化した取組を行ってきている。

  - Transmission and Distribution（送電および配電）
  - Building to Grid
  - Industry to Grid
  - Home to Grid

➢ Business and Policy.

- サイバーセキュリティコーディネーションタスクグループを設置し、他のクロスドメインタスクグループと一緒に重複する課題の解決に取り組んでいる。
- GWAC（GridWise アーキテクチュア会議）と協働して、NIST は利害関係者向けにフレームワーク開発計画の広報活動を行い、スマートグリッドのドメイン分野における重要な事業目的と障害などの優先課題を決めている。また、標準ロードマップの策定に必要なステップとして、NIST は現状のスマートグリッド相互運用性と利害関係者の活動計画を評価している。
- 電力業界とは、ビジネス利用事例集を策定し、標準開発のガイド作りを支援している。
- 相互運用性知識基盤（Interoperability Knowledge Base）の開発に乗り出し、度相互理解を促し、スマートグリッドの標準、タクソノミー（カテゴリー分類）、インターフェースおよび専門用語などのコンセンサス形成を図っている。

オバマ政権の最重要課題であるスマートグリッドの開発を加速化するために、NIST（国立標準技術研究所）は、米国回復再投資法（ARRA）からの 500 万ドルの助成金を使い、スマートグリッドの実装を早める動きを取り出している。NIST は、国家スマートグリッド相互運用性調整局（National Coordinator for Smart Grid Interoperability Office）を新設し、2009 年 4 月から 3 段階計画でスマートグリッドの相互運用性標準の開発と広範な利用を促進する動きを開始したところである。この 3 段階計画は次の通りである。

表 5　NIST の 3 段階加速化計画

フェーズⅠ：ロードマップ&スマートグリッドリリースⅠ
♦ 2009 年 4 月 1 日、電力中央研究所（EPRI）とスマートグリッド標準ニーズを評価し、標準ロードマップの中間報告案を策定する技術支援契約を締結。 ♦ 2009 年 5 月 19～20 日、ロードマップ・サミットを開催。 ♦ 2009 年 6 月 18 日、NIST の委託により EPRI が作成したスマートグリッド標準に関する中間報告書（300 ページ）を発表し、パブリックコメントを求める。 ♦ 2009 年 7 月、標準サミットを開催。 ♦ 2009 年 8 月、相互運用性標準ワークショップを開催 ♦ 2009 年 9 月、アーキテクチュア、標準化優先課題、リリースⅠ標準の選別、将来の開発に向けた標準開発機構に対する責務の割当、タイムテーブルに関するコンセンサスを繁栄する報告著を公表。 ※NIST は、2009 年の初秋までに、最初のスマートグリッド・アーキテクチュア、サーバ

ーセキュリティを含む相互運用性標準の優先課題、実装をサポートする最初の標準を既述することをキタイし、残りの標準ニーズを満たす計画である。

フェーズⅡ：中長期的な進展に向けた官民パートナーシップ

- 2009 年 5 月、RFP の発表。
- 2009 年末を期日として、スマートグリッド相互運用性標準のパネルを立ち上げる。
  - ロードマップを進展させる。
  - 継続的な調整。
  - 確実に実装する。

※NICT は中長期的な進展に向けて官民連携による相互運用性パネルを立ち上げ、2009 年中に最初のスマートグリッド標準を選定する一方、ギャップを解決し、標準の意見統一を行い、最新技術を取り込む更なる標準の開発を実施する。

フェーズⅢ：試験及び認証のフレームワーク

- 2009 年末までに計画を策定。
- 2010 年に実装開始
  相互運用性とセキュリティの両方の課題に取り組む。

※NIST は、業界、政府およびその他の利害関係者と協議を重ね、スマートグリッドのデバイス、システムおよびプロセスに標準を実装する方法の試験および認証のための枠組みを開発し、実際のオペレーション諸条件下での相互運用性とセキュリティを確保する最優先課題に取り組む。

米国では、エネルギー、輸送、電気通信などの国家の重要インフラをはじめ、ビジネスもサービスもソフトウェアへの依存度を強めており、ソフトウェアは国家の重要インフラのオペレーションにとって不可欠となっている。こうした重要インフラと主要リソースを支えるソフトウェアの脆弱性は大きなリスク要因でもある。ソフトウェアの規模と複雑性、資格のないサプライヤーの生産したソフトウェアの利用、ソフトウェアシステムの相互依存性などにより、このリスクは重層化してきている。公表されているセキュリティインシデントの約 90%がソフトウェアの設計またはコードの欠陥に対する私的利用に起因すると報告されており、ソフトウェアの整合性を確保することが脅威や脆弱性から重要インフラを防護し、サイバー攻撃にさらされる全般的なリスクを軽減する上で重要なカギになる。

情報システムの信頼性（reliability)、完全性（integrity）およびセキュリティを確保するためには、Enabling Software(作動可能な状態の有資格のソフトウェア)のセキュリティを、設計段階からビルトインする規定を盛り込むことが重要である。2003 年に国防省（DOD)によって開始されたソフトウェアアシュアランス（SwA：Software Assurance）イニシアティブは、国土安全保障省（DHS)の国家サイバー・セキュリティ部門（NCSD）に受け継がれ、「国家サイバースペース安全確保戦略（National Strategy to Secure Cyberspace)」のアクション/勧告 2－14 に基づくソフトウェアの完全性、セキュリティおよび信頼性のための高レベルのスタンダードを設定することになった。

ソフトウェアの完全性、セキュリティおよび信頼性を高める国家サイバー・セキュリティ部門（NCSD）の戦略的イニシアチブプロジェクトは、「Build Security In Software Assurance Initiative (BSI)」と呼ばれている。この戦略を実行するために、国土安全保障省(DHS)の国家サイバー・セキュリティ部門(NCSD)はソフトウェアアシュアランス(SwA)プログラムを打ち出している。

一方、米国には、情報アシュアランス（IA：Information Assurance）という概念もある。国家安全保障システム委員会（CNSS）によると、これは、「可用性（Availability）、完全性（Integrity)、認証（Authentication)、機密性（Confidentiality）,否認防止（non-dupidiation）を確実に保証することにより、情報及び情報システムを保護および防護する」ことと定義されている。国家セキュリティシステム委員会（CNNC）は、セキュリティの信頼感（コンフィデンス）に加えて、ソフトウェアの予測可能性（Predictability）も重視している。

この情報アシュアランス（IA）の概念は、1970年代に機密性、完全性および可用性の属

性を持つ情報セキュリティの概念を基に発展したものである。つまり、情報アシュアランス（IA）は、“安全性を確保した情報セキュリティ（Secured Information Security)”であり、これに対比して、ソフトウェアアシュアランス（SwA）は、“確実な保証を得た（アシュアード）ソフトウェアのセキュリティ（Assured Security of Software)”を意味する概念として使われてきている。

直近では、大型システムや“システムズの中のシステム（SOS-systems of systems）”を構築、取得または管理する立場にある人たちの間では、知財権のあるソフトウェアやレガシーシステムやオープンソースソフトウェアから構成されるシステムの複雑性を再認識し、現代の複雑系システムの脅威はシステムのライフサイクル全般を通じて存在すると認識されている。この結果、米国でも、アシュアランスの概念はシステム全体についても導入されつつある。

国防省（DOD）は、米国国防産業協会（NDIA）および他省庁と連携して、システムズアシュアランス（Systems Assurance）の問題解決にも取り組んできている。国防副次官（買収・技術担当：DSUD/A&T）は 2006 年、システムズ＆ソフトウェアエンジニアリング局長の下に“ソフトウェア＆システムズアシュアランス担当副局長”を任命し、システムズアシュアランスのニーズ検証、DOD の事業運営戦略、アシュアードシステムズ（確実な保証を得たシステムズ）の政策・手引きのフレームワークなどの作業を進めた。

国防省（DOD）の定義によると、システムアシュアランス（System Assurance）とは、「システム機能が意図した通りに機能し、ライフサイクル期間中に任意のタイミングでシステムの一部として意図的または意図的ではない形で設計または挿入された攻略できる脆弱性（exploitable vulnerabilities）を回避する正当化されたコンフィデンス（justified confidence）」である。

また、国防省（DOD）の委託を受けて、カーネギーメロン大学の SEI(ソフトウェアエンジニアリングインスティチュート)は 2007 年 10 月から、システムズの中のシステム（SOS）問題に関する実証の現状を検討し、今後の問題点を明らかにしようとした。2008 年の成果発表では、昨今のシステムを通常の SOS 環境の中で使っても、あまり多くのシステム障害は発生しないとされた。しかし、DOD の命令制御システムの規模と複雑性が増大すると、DOD のテスト評価（T&E）プロセスには大きな負担になる。以上のことから、SEI(ソフトウェアエンジニアリングインスティチュート)は、DOD のシステムアシュアランス（SA）の定義と重点課題を検証し直し、複数の提言を行っている。戦場情報システム、SOA(サービス指向アーキテクチュア)を使うシステムや巨大な複雑系システムでは、技術的な問題の困難度が増してきており、正当化されたコンフィデンスを獲得するのは難しいという。

ところが、米国では、「IT の所有から利用へ」の潮流を促すクラウド・コンピューティングの概念とビジネスモデルが発展。オバマ政権は、クラウド・コンピューティングを連邦政府に導入する動きを加速化してきている。

一方、直近の 1〜2 年の間に、連邦議会の多数の議員の IT システムがハッカー攻撃に晒されていることや、一般国民も情報システムの脆弱性とディペンダビリティ（高信頼性）の確保を強く意識するようになってきている。また、クラウドの暗い部分でもある、データセンターに対する第 3 者によるハッカー攻撃や、その他の攻略されやすい脆弱性リスクの回避や、ディペンダビリティの確保に向けた課題も重要視されるようになったのである。

2009 年 5 月 29 日のプレス発表で、オバマ大統領は、ホワイトハウス官邸でサイバースペースにおける米国民のセキュリティを確実に保証する国家戦略に責任を持つサイバー・セキュリティ調整官を設置して、その任務を明確にすることを明らかにした。具体的な人物名は公表されなかったが、このサイバー・セキュリティ調整官（cybersecurity coordinator）は、連邦政府のサーバーセキュリティ政策全般を指揮・統合する役割を担い、大統領自身が任命する。これは、連邦政府がサイバー・セキュリティを最も高い注意と焦点を絞り込む動きを取ることを意味する。2009 年 12 月、マイクロソフトの eBay のチーフセキュリティオフィサーを務めた Howard A. Schmidt がホワイトハウスのサイバー・セキュリティ調整官に任命された。ハワード・シュミットの任務は、サイバー攻撃から ICT 基盤を含む米国の重要インフラを防護するトップダウン型の監督を行うことである。

シュミットは 2010 年 1 月、連邦 CIO のビベック・クンドラ（V Kundra）および連邦 CTO の Aneesh Chopra（チョプラ）と会議を行い、クラウドの賛同者であることを公表し、セキュリティ対策で協業することを確認している。データ保護が重要なカギで、セキュリティとプライバシー（自由人権）の 2 つを同時に取り組むことも公表している。

3.1. IT を利活用した米国連邦政府の危機管理対策

3.1.1 米国の重要インフラ防護対策

1993 年の同時多発テロ時の貿易センタービルへの攻撃、1995 年の Alfred P Murrah 連邦ビル（オクラハマ市）の爆破などの人為的な惨事、ハリケーンカトリーナなどの自然災害、1995 年のロシア人ハッカーグループによるシティコープの電子資金振替システム（EFT）への侵入事件などを背景に、クリントン大統領は 1996 年 7 月に、大統領行政命令第 13010 号（Executive Order 13010）を発布し、大統領重要インフラ防護委員会（PCCIP）を設置し、

今後の重要インフラ防護（CIP）戦略の立案を指示した。PCCIP の任務は、主にサイバー脅威にフォーカスした米国のクリティカルインフラにとっての脆弱性と脅威の範囲と性格を大統領に報告し、重要インフラ防護（CIP）の総合政策と実行計画を提言し、法律および政策問題を決め、この提言に必要な制度・規制の変更を進言することであった。1996 年 7 月の PCCIP(大統領重要インフラ防護委員会)の設置が米国の重要インフラ防護（CIP）政策の出発点である。

1997 年 10 月の「重要基盤：米国のインフラ防護（Critical Foundations: Protecting America's Infrastructures)」、1998 年 5 月のクリントン大統領決定指令第 63 号（PDD 63）における国家インフラ防護計画（NIPP)、2000 年 1 月の「National Plan for Information Systems Protection（国家情報システム防護計画)」、2002 年 7 月の「国家国土安全保障戦略（National Strategy for Homeland Security)」などの政策措置を踏まえて、重要インフラ防護対策を強化した。

2003 年 1 月に国土安全保障省（DHS）が創設されると、連邦政府は、2003 年 2 月の国家サイバースペース安全性確保戦略（National Strategy to Secure Cyberspace)、2003 年 12 月の国土安全保障大統領指令第 7 号、2006 年 6 月の国家インフラ防護計画（NIPP)、2007 年 5 月のセクター別プラン（SSP）と IT セクター別プランにいたる国家重要インフラ防護を中心とする情報システム・ソフトウェアのセキュリティ、脅威・脆弱性に関する政令・政施策などを相次いで打ち出しきている。

2001年9月11日の同時多発テロ事件を契機に、2002年7月に公表された国土安全保障国家戦略を行動に移す目的で2003年1月に設立された米国国土安全保障省（DHS：Department of Homeland Security）は、22の省庁を再編統合して設置された、国防総省（DOD）に次ぐ巨大な省である。

2002 年 7 月の国土安全保障国家戦略（The National Strategy for Homeland Security）によると、“Homeland Security（国土安全保障)”とは、米国内におけるテロリスト攻撃を防護し、アメリカのテロリズムに対する脆弱性を縮小し、発生する攻撃による損害の最小化と回復を図る米国の一致団結した努力である。

米国の重要インフラ防護（CIP：Critical Infrastructure Protection）とは、米国の脆弱に相互接続されたインフラストラクチュアのセキュリティ（安全保障）を保証する国家プログラムである。米国以外では、重要インフラ防護（CIP）は、国家重要インフラの安全を保証し、防護する公式宣言または特定プログラムを意味している。

2007 年 10 月 9 日に発表された最新の国土安全保障国家戦略（National Strategy for Homeland Security）は、連邦戦略（Federal strategy）ではなくて、ナショナル戦略（national strategy）で、2002 年 7 月の国土安全保障国家戦略を改定したものである。2007 年 10 月の改訂版は、米国が直面する脅威に関する理解の深化を反映し、実世界の大惨事から得た教訓を盛り込み、国土安全保障基盤を強化することで長期的な成功を確保する方法を規定し、今後数年間の国土をセキュアにするためのアプローチ手法を明文化したものである。

国土安全保障国家戦略の目的は、セキュアな国土安全保障を確保する米国の努力を導き、組織化および統合化することである。具体的な戦略プログラムは、(1) テロリスト攻撃の防護と破壊、(2) 米国民、米国の重要インフラおよび主要リソース（CIKR）の防護、(3) 発生する緊急事態への対応と回復、(4) 長期的成功を確保するための基盤強化の継続の 4 つである。この 4 つのうちの最初の 3 つのゴールは米国の努力を組織化することを支援するもので、最後のゴールは、国土安全保障の原則、システム、体制および機関の創出および編成を含むものである。

1997 年 10 月の「重要基盤：米国のインフラ防護（Critical Foundations: Protecting America's Infrastructures）」以降、米国は数々の重要インフラ防護（CIP）に関連する政策アクションを打ち出し、実行してきている。

国家インフラ防護計画（NIPP）の狙いは、テロリストによる破壊、無能力化または私的利用の影響を防護、検出、無効または緩和するために、米国の重要インフラ・主要リソース（CIKR）の防護を向上することで、より安全で、セキュアな堅牢性のある米国を構築し、攻撃、自然災害またはその他の緊急事態の発生時に、国家の構え、タイムリーな対応および急速な復興を強化することにある。

米国の重要インフラ（Critical Infrastructure）とは、その無効化または破壊が国家の安全保障（security）、経済活動の保安、公的保健または安全、またはこれらの組み合わせに深刻な影響を与えることになる米国にとって極めて重要な物理的または仮想的な資産、システムおよびネットワークのことである。主要リソースとは、経済および政府の最低限のオペレーションにとって必要不可欠な公的または私的に所有支配される資源のことである。

2003年12月17日の国土安全保障大統領指令第7号（HSPD-7）は、米国の重要インフラ・主要リソース（CIKR）を明らかにし、優先順位をつけて、テロ攻撃から防護する国家政策を定め、17の重要インフラ・主要リソース（CIKR）を明らかにした。加えて、大統領指令第7号（HSPD-7）はセクター別管轄機関（SSA-Federal Sector-Specific Agency）を指定して、

この17のセクターの防護を、NIPPフレームワークの応用を詳述したセクター別計画（SSO-Sector-Specific Plan）に沿って担わせている。

国土安全保障省（DHS）が明らかにした重要インフラ・主要リソース（CIKR）と所轄官庁は次の通りである。

表 6　重要インフラ・主要リソースと所轄官庁

重要インフラ・主要リソース（CIKR） セクター別計画（Sector-Specific Plan）	セクター別管轄官庁（SSA）
農業および食料品：	農業省 保健人的サービス省連邦食品医薬品局（FDA）
銀行・金融	財務省
化学： 基礎化学品、スペシャリティ化学品、ライフサイエンス、コンシューマ製品	国土安全保障省（DHS）
商業施設	国土安全保障省（DHS）
通信	国土安全保障省（DHS）
ダム	国土安全保障省（DHS）
国防産業基盤	国防省（DOD）
緊急サービス	国土安全保障省（DHS）
エネルギー： 電力、石油、天然ガス	エネルギー省（DOE）
政府施設	国土安全保障省（DHS）
情報技術（IT）	国土安全保障省（DHS）
国家記念碑・建造物	内務省
原子炉、核物質・廃棄物	国土安全保障省（DHS）
郵便・配送サービス	国土安全保障省（DHS）
公衆衛生・保健医療	保健人的サービス省（DHHS）
輸送システム	国土安全保障省（DHS）
水	環境保護庁（EPA）

出所：Homeland Securityのセクター別計画（SSO-Sector-Specific Plan）

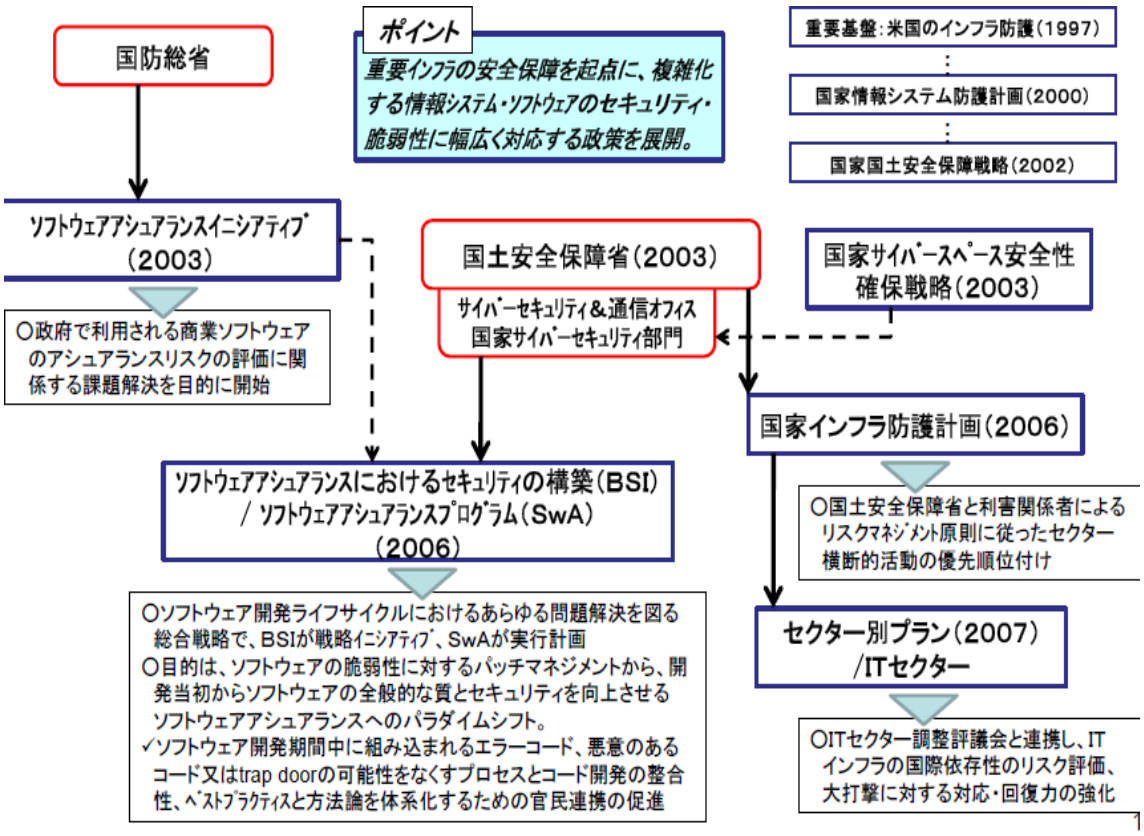
2006年6月の国家インフラ防護計画（NIPP）は、上記17セクターの重要インフラ・主要リソース（CIKR）防護に関するプログラムおよび活動を統合化するための全体の枠組みを提供するものである。2007年5月21日、国土安全保障省（DHS）は17セクターのセクター別プラン（SSP-Sector Specific Plan）を公表した。国土安全保障省（DHS）によるサイバー・

セキュリティの基準および13の責務については、“Critical Infrastructure Protection: Sector Specific Plan’s Coverage of Key Cyber Security Elements Varies”と題された下院国土安全保障委員会向け証言の中に示されている。

情報技術（IT）セクターに関して、国土安全保障省（DHS）は2006年中に、商務省（DOC）、国防省（DOD）、法務省、国務省および財務省の代表から構成されるIT政府調整評議会（Information Technology Government Coordinating Council-GCC）、国家情報長官官房（Office of the Director of National Intelligence)、大統領府行政管理予算局（Office of Management and Budget National)、全米州政府CIO会議（Association of State Chief Information Officers)などのメンバーと密接な共同作業を行い、ITセクター調整評議会（IT Sector Coordinating Council-SCC）と連携してITセクター別プラン（SSP-Sector Specific Plan）を開発した。クリティカルなITセクター別プランでは、①ITセクターの目標および重要機能の定義、②リスクマネジメント（ITセクターのリスク環境、リスクプロファイル、リスクマネジメント手法、脅威・脆弱性などの評価）、③防護計画の策定と実行、④情報共有、⑤重要インフラ・主要リソース（CI/KR）の研究開発、⑥ITセクターの責任などが記述されている[9]。

[9] Information technology: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan May 2007 Homeland Security

図 25　米国の政策体系と IT に係る信頼性とセキュリティ政策の位置づけ



3.2. ソフトウェアアシュアランスおよびシステムアシュアランス

3.2.1 定義

2004 年 12 月に設置された DOD（国防省）の“ソフトウェアアシュアランスタイガーチーム”は、ソフトウェアアシュアランス（SwA）を、「意図した通りにソフトウェアが機能し、ソフトウェアの一部に意図的または意図しない形で設計または挿入された脆弱性から免れているというコンフィデンス（信頼感）の水準」であると定義している。

国防省（DOD）のソフトウェアアシュアランス（SwA）イニシアティブのルーツは、国防科学委員会（Defense Science Board）による 1999 年 12 月のグローバリゼーション&セキュリティ報告書で示された勧告である。この勧告は、国防省副長官（ASD）レベルにおけるソフトウェアアシュアランス（SwA）プログラムの設置を求めるもので、国防省が外国製造業者の商用ソフトウェアに依存していることによる潜在的な脅威に対応するためのセキュリティと知的対抗策を改善すべきだとの内容である。

この基本にある考え方は、ソフトウェアの脆弱性（Vulnerabilities）は、知財（IP)、消費者の信頼および事業活動を大きく損なう可能性があり、報告されるセキュリティインシデントの 90%は、“意図的または偶発的”な形でソフトウェアの設計またはコードに挿入された欠陥によるものである。国家重要インフラを脅威と脆弱性から防護し、サイバー攻撃に対する全般的なリスクを縮小するためには、ソフトウェアの完全性（Integrity）を確保することが重要なカギになる。以上の考え方は、物理的攻撃およびサイバー攻撃に直面した米国の国防省（DOD）と国土安全保障省（DHS）のソフトウェア・情報システムの完全性と安全性を含む高信頼性（Dependability）を担保する米国政府の情報通信技術（ICT）政策の根底に流れている。

1998年5月のクリントン大統領決定指令（Presidential Decision Directive）第63号（PDD 63）に基づき、米国政府は、2003年までに物理およびサイバーの両面の“意図的な攻撃”から米国の重要インフラを防護する能力の強化を打ち出し、情報および通信、バンキングおよびファイナンスなどの防護すべき重要インフラと所轄官庁を明らかにする国家戦略を打ち出し、重要インフラ防護（CIP）の課題と官民連携による実施に取り組んできている。米国の重要インフラ（Critical Infrastructure）とは、その無効化または破壊が国家の安全保障（security）、経済活動の保安、公的保健または安全、またはこれらの組み合わせに深刻な影響を与えることになる米国にとって極めて重要な物理的または仮想的な資産、システムおよびネットワークのことである。主要リソース（Key Resources）とは、経済および政府の最低限のオペレーションにとって必要不可欠な公的または私的に所有支配され

る資源のことである。

エネルギー、輸送、電気通信などの国家の重要インフラをはじめ、ビジネスもサービスもソフトウェアへの依存度を強めており、ソフトウェアは国家の重要インフラのオペレーションにとって不可欠となっている。こうした重要インフラと主要リソースを支えるソフトウェアの脆弱性は大きなリスク要因でもある。ソフトウェアの規模と複雑性、資格のないサプライヤーの生産したソフトウェアの利用、ソフトウェアシステムの相互依存性などにより、このリスクは重層化してきている。公表されているセキュリティインシデントの約 90%がソフトウェアの設計またはコードの欠陥に対する私的利用に起因すると報告されており、ソフトウェアの完全性を確保することが脅威や脆弱性から重要インフラを防護し、サイバー攻撃にさらされる全般的なリスクを軽減する上で重要なカギになる。情報システムの信頼性 (reliability)、完全性 (integrity) およびセキュリティを確保するためには、Enabling Software(作動可能な状態の有資格のソフトウェア)のセキュリティを設計段階からビルトイン (組み込む) する規定を盛り込むことが重要である。

国土安全保障省 (DHS) は、2003 年 2 月の国家サイバースペース安全性確保戦略 (National Strategy to Secure Cyberspace) を中核とする計画展開を実施している。米国のサーバースペースをセキュア (確実に脆弱性や危険から防護するという意味) にする戦略計画を実行するために、国土安全保障省 (DHS) の国家サイバー・セキュリティ部門 (NCSD) は、「国家サイバースペース安全性確保戦略」のアクション/勧告 2－14 に基づいて、「Build Security In Software Assurance Initiative (BSI)」を導入し、ソフトウェアアシュアランス (SwA) プログラムを展開することになった。

この BSI 戦略に基づき、DHS は、ソフトウェアの完全性、セキュリティおよび信頼性を高める努力を払っている。国土安全保障省 (DHS) によると、ソフトウェアアシュアランス (SwA) は、脆弱性や脅威に対して確実にソフトウェアのセキュリティを保証することを意味する。

ソフトウェアアシュアランス (SwA) は、「確実に保証されたソフトウェア」の属性を以下の 3 つとして、この課題解決に取り組むことを重要視している。

- Trustworthiness (信用性、信頼する価値があること) : 悪意のあるまたは意図的ではない挿入によるものの如何にかかわらず、私的利用 (＝搾取) 目的の脆弱性 (exploitable vulnerabilities) がないこと。
- 予測可能な実行 (Predictable Execution) : 実行する際に、意図した通りにソフトウェアが機能するとの正当なコンフィデンス (信頼感) を提供するもの。
- Conformance(適合性) : 要求、標準/手順に適合するソフトウェアのプロセスと製品を確保する計画的かつ体系的な複合専門領域 (multi-disciplinary) の諸活動

セット。

国土安全保障省（DHS）は、ソフトウェア開発期間中に導入されるエラーコード、悪意のあるコードまたは trap doors（秘密の落し戸）の可能性を無くすプロセスと手順を含むソフトウェア・コード開発の整合性、セキュリティおよび信頼性を向上するベストプラクティスと方法論を体系化する全米規模の官民連携努力を促進している。

国立標準技術研究所（NIST）は、ソフトウェアアシュアランス（SwA）を、「ソフトウェアのプロセスおよびプロダクトが、要件事項、標準および手順に確実に適合していることを保証するための計画的かつ系統的な活動（the planned and systematic set of activities that ensures that software processes and products conform to requirements, standard, and procedures to help achieve)」であると定義している。

- 信頼性(Trustworthiness)： 悪意によるか、あるいは意図しないにもかかわらず、悪用可能な脆弱性が存在しないこと（No exploitable vulnerabilities exist, either of malicious or unintentional origin)。
- 予想可能な実行（Predictable Execution)： ソフトウェアが、実行時に意図したとおりに機能することの正当と認められるコンフィデンス（Justifiable confidence that software, when executed, functions as intended.）

2007 年 7 月 31 日の“Software Security Assurance”によると、最近まで、ソフトウェアアシュアランス（Software Assurance）という専門用語は、ソフトウェア品質アシュアランスの略語としての品質（quality）と、安全性を含むリライアビリティ（信頼性）の 2 つの関連する属性を意味してきた。情報アシュアランスと表現される「安全性を保証された」情報セキュリティとの対比で、ソフトウェアアシュアランスが「確実に保証されたソフトウェアのセキュリティ（assured security of software)」の意味で使われだしたのはここ 5 年くらいのことである。

国家セキュリティシステム委員会（CNNS）は、セキュリティにおけるコンフィデンス（信頼感）に加えて、ソフトウェアの予測可能性（predictability）を重視して、「意図的にソフトウェアにデザインインされるか、設計後のライフサイクル期間に偶発的に挿入されたかの如何にかかわらず、ソフトウェアの脆弱性がないことと、ソフトウェアが意図された形で機能することのコンフィデンス（信頼感）の水準である」と定義している。

NASA（航空宇宙局)による定義は、「ソフトウェアのプロセスおよび製品が要求、標準および手順に適合することを確保する計画的かつ体系的な諸活動のセット（Planned and

systematic set of activities that ensures that software processes and products conform to requirements, standards, and procedures)」である。計画的かつ系統的な諸活動のセット（planned and systematic set of activities）には、要求仕様、テスト（testing)、妥当性検証（validation)、報告（reporting）が含まれる。ソフトウェア開発ライフサイクル期間中のこれらの機能のアプリケーションがソフトウェアアシュアランスと呼ばれている[10]。NASA の定義には、ソフトウェアアシュアランスはソフトウェア自体だけのために実現すべきではなく、開発、運用および維持するためのプロセスを目的として実現する必要性があるとしている。

DOD（国防省）は、システムアシュアランスを、「システムが意図したとおりに機能し、ライフサイクル期間におけるどの時点でも、システムの一部として、意図的または偶発的に、悪用可能な脆弱性に晒されないという信頼性の尺度（the measure of confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the lifecycle)」であると定義している。

DOD（国防省）によれば、システムアシュアランスは、「ソフトウェアが意図したとおりに機能し、意図的または偶発的に設計または挿入された脆弱性から免れているというコンフィデンス(信頼感)の水準(the level of confidence that software functions as intended and is free from vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software)」に関連したものである。

また、国防省（DOD）の委託を受けて、カーネギーメロン大学の SEI(ソフトウェアエンジニアリングインスティチュート)は 2007 年 10 月から、システムズの中のシステム（SOS）問題に関する実証の現状を検討し、今後の問題点を明らかにしようとした。2008 年の成果発表では、昨今のシステムを通常の SOS 環境の中で使っても、あまり多くのシステム障害は発生しないとされた。しかし、DOD の命令制御システムの規模と複雑性が増大すると、DOD のテスト評価（T&E）プロセスには大きな負担になる。以上のことから、SEI(ソフトウェアエンジニアリングインスティチュート)は、DOD のシステムアシュアランスの定義と重点課題を検証しなおし、複数の提言を行っている。戦場情報システム、SOA(サービス指向アーキテクチュア)を使うシステムや巨大な複雑系システムでは、技術的な問題の困難度が増してきており、正当化されたコンフィデンスを獲得するのは難しいという。

3.2.2 国土安全保障省（DHS）の国家サイバー・セキュリティ部門（NCSD）

[10] 1992 年 11 月の定義。

2001年9月11日のテロ攻撃の応戦するために、2002年11月に成立した国土安全保障法（Homeland Security Act）に基づいて、国土安全保障省（DHS-Department of Homeland Security）が2003年1月に創設された。

ホームランドセキュリティ（DHS）の中核政策は、2003年2月に発表された「国家サイバースペース安全性確保戦略（National Strategy to Secure Cyberspace）」である。これは、米国の情報システムおよびネットワークのセキュリティを確保するために、サイバースペースを防護するための努力を組織化し、問題解決の優先順位をつけるための第1次フレームワークである。

国家サイバースペース安全性確保戦略（National Strategy to Secure Cyberspace）は、次の3つの戦略目標を掲げている。

① 米国重要インフラに対するサイバー攻撃の防護。
② サイバー攻撃に対する脆弱性の縮小。
③ サイバー攻撃が発生した際の損害と復旧時間の最小限化

国土安全保障省（DHS）の国家サイバー・セキュリティ部門（NCSD）のミッションは、2003年12月17日の国土安全保障大統領指令第7号（HSPD-7）を根拠として、官民連携および国際協力によるサイバースペースおよび米国のサイバー資産を確保することにある。

この戦略目標を実現するために、国土安全保障省（DHS）は、国家サイバー・セキュリティ部門（NCSD）を設置し、米国のサイバーインフラストラクチュア安全確保にとって重大な防護措置のひとつとして、「Build Security In Software Assurance Initiative (BSI)」と呼ばれるサイバー・セキュリティ戦略を策定したのである。

ソフトウェアアシュアランスへのセキュリティの組み込みを意味するBSI戦略は、2003年2月の「国家サイバースペース安全性確保戦略（National Strategy to Secure Cyberspace）」にアクション/勧告2－14基づいて、米国のサーバースペースをセキュア（確実に脆弱性や危険から防護するという意味）にするために導入されたサイバー・セキュリティ対策である。

国土安全保障省（DHS）の国家サイバー・セキュリティ部門（NCSD）は、サイバーリスクマネジメントプログラムを通じて、リスクを評価し、米国のサイバーインフラストラクチュア安全確保にとって重大な防護措置を講じている。主なプログラム内容は次の通りである。

- Cyber Exercises:サイバーストーム（Cyber Storm）は全米サイバー・セキュリティ実習シリーズで、2年に1回(2006年2月、2008年3月)の割合で開催されている。連邦政府、州政府、海外政府、民間セクターを横断的に対象として開催されるHomeland Securityのサイバー攻撃応戦のための実習である。
- National Outreach Awareness Month：国家サイバー・セキュリティ部門（NCSD）は毎年10月に実施する国家サイバー・セキュリティ意識（National Cyber Security Awareness）を高めるための月である。
- Software Assurance Program（**ソフトウェアアシュアランスプログラム**）：国家サイバー・セキュリティ部門（NCSD）のBSI戦略的イニシアティブの実行プログラムで、ソフトウェア脆弱性の縮小、搾取の最小化、信頼の置けるソフトウェア製品常の開発・利用を改善する方法などの課題解決を図る。

サイバーインフラを防護するために、ホームランドセキュリティの国家サイバー・セキュリティ部門（NCSD）は次の戦略的目標を明らかにしている。

- 実効性の高い国家サイバースペース対応システムを構築・維持すること。
- 重要インフラの防護のためのサイバーリスクマネジメントプログラムを実施すること。

ソフトウェアアシュアランス（SwA）プログラムは、上記サイバーリスクマネジメントプログラムのひとつである。ソフトウェアの完全性、セキュリティおよび信頼性を高める国家サイバー・セキュリティ部門（NCSD）の戦略が、「Build Security In Software Assurance Initiative（BSI)」であり、この実行計画が「ソフトウェアアシュアランス（SwA）プログラム」であると言い換えることもできる。

BSI戦略では、セキュリティ問題をソフトウェアエンジニアリングの課題とみなし、全ソフトウェア開発ライフサイクルにわたり系統的にこの課題解決に取り組む必要性があるとの考え方を基本原則としている。BSIには、安全で回復可能なソフトウェア開発をサポートする最適な手法、ツール、ガイドライン、ルール、原則などが含まれている。

BSI戦略イニシアティブは、行政管理予算局（OMB）と総合サービス管理局（GSA）との間でも、“Federal Network Security（連邦ネットワークセキュリティ)” プログラムを開始。主な特徴は次の通りである。

- “Trusted Internet Connection”イニシアティブでは、政府システムから外部へのアクセス・ポイントの削除、これらのアクセス・ポイントでの機能の標準化を

目標とする。

- OMB（行政管理予算局）と GSA（総合サービス管理局）との共同作業を進め、企業全体で使用する契約を標準化する。
- OMB（行政管理予算局）との作業では、サイバー・セキュリティ行程を進捗させる一般的な FISMA ガイドラインも対象とする。

国家サイバー・セキュリティ部門（NCSD）の BSI（Build Security In Software Assurance Initiative）では、カーネギーメロン大学のソフトウェアエンジニアリング研究所（SEI）と連携してプロセスおよびテクノロジーの重点分野を定めている。SEI のチームメンバーとその他の貢献者がソフトウェアアシュアランスとソフトウェアセキュリティに関する情報収集と開発を担い、セキュアな情報システム開発を支援している。Build Security In（BSI）の Website の執筆メンバーは、カーネギーメロン大学ソフトウェアエンジニアリング研究所（SEI）の教授や研究者、Cigital, Inc、フォード、Ernst & Young などのセキュリティ専門家、世界的に著名なセキュリティの専門家、Kenneth R. van Wyk など、多彩な顔ぶれである。

国家サイバー・セキュリティ部門（NCSD）の戦略的イニシアティブである“Build Security In プロジェクト”チームは、IT セキュリティ必須知識体系（EBK- IT Security Essential Body of Knowledge）をまとめている。IT セキュリティ EBK は、進化する IT セキュリティの課題解決を図るために新しい手法として IT セキュリティスキルを概念化したものである。IT セキュリティ監査人（security practitioners）が特定の役割と責務を履行するのに必要な必須の知識とスキルを表現する基準を提供し、米国が最も資質の高い適切な教育を受けた IT セキュリティワーカーを抱えていることを立証する。IT セキュリティ EBK は、IT セキュリティの役割に対する能力（competencies）と機能面の見通しを加えたアンブレラ・ドキュメントである。これは、国土安全保障省（DHS）によるスタンダード、指令または政策ではなく、主要な IT セキュリティ用語と概念を明らかにし、セキュリティ上の役割を識別し、主な 4 つの機能面の見方を定義し、IT セキュリティの役割、権能および機能マトリックスを策定している。

BSI は、ソフトウェアのアーキテクト、ディベロッパーおよびセキュリティ監査人（security practitioners）がソフトウェア開発の各段階でセキュリティをソフトウェアに組み入れる際に使うプラクティス、ツール、ガイドライン、ルール、原則、その他のリソースを提供する協働努力である。BSI のコンテントは、ソフトウェアセキュリティが基本的にはソフトウェアエンジニアリングの問題であり、ソフトウェア開発のライフサイクル期間を通じて体系的な方法で解決しなければならないとの原則に準拠している。

DHS 国家サイバー・セキュリティ部門（NCSD）の BSI プログラムがスポンサーとなっている「Software Assurance Landscape」の初期ドラフトによると、NIST(米国標準技術研究所)、DoD（国防省）、国家安全保障局（NSA)、OMG、ISO/IEC/IEEE、学術界、業界は、DoD/DHS ソフトウェアアシュアランス作業グループと補完関係を維持しながら共同作業を行っている。

NIST のソフトウェアアシュアランスの基準とツール評価（SAMATE）のように、DHS から一部の助成を受けているものもある。NIST SAMATE 作業は、公式分類学の開発に重点を置き、ソフトウェアアシュアランスおよびシステムアシュアランスの課題に適用できる各種のツールを記述している。DoD（国防省）は、DoD/DHS ソフトウェアアシュアランス作業グループとフォーラムでの作業に加えて、次の作業を行った。

- セキュリティー・ソフトウェア・ベース・システムに関する課題を研究するタイガーチームを編成。
- 本件に関する国防科学評議委員会を設立した DoD に対しアシュアードソフトウェアセンターを設置。

BSI の最新プログラムは次の通りである。

Portal for System Assurance：公的部門と民間コミュニティは、この Web サイト・ポータルから最新の研究および開発情報を入手している。情報は非常に詳細ですべてのプロジェクトが、結果を受け入れる前に厳密なガイドラインに従う必要がある。

Assurance Cases（アシュアランス事例）：ソフトウェアアシュアランス（SwA）の事例と標準もこのポータルに掲載されている。ソフトウェアとシステムのセキュリティを保証することはできない。この評価は継続的に実施され、ゼロリスクを期待するものではないが、状況に応じてリスク管理を行う必要がある。この状況を考慮して、Build Security In イニシティィブは、 アシュアランス事例をセキュリティの評価に使用することを推奨している。 これらは訴訟事例と類似し、 構造化された論拠のセットが構築され、株主もレビューする可能性のあるアシュアランスに関するクレームを作成する。

Resiliency Maturity Model（高完成度モデル）：SEI Cert は、Resiliency Maturity Model（RMM）を機能および高完成度モデル・フレームワークでの運用に重点を置いて作成したものである。課題は弾力性の管理である。この前提には、 特に継続的な新しい COTS、新たなヴィールスによって継続して変化する脅威の状況、および新しいアップグレードなど技術の崩壊による、要件および複雑性、相互運用能力への期待が高まっていることがある。RMM 1.0 が最近リリースされた。これは、プロセス改善モデルを含み、セキュリ

ティの収束、ビジネス・コミュニティおよびIT 運用を重視して、運用リスクを管理し 運用の弾力性を確立するものである。

刊行物のBSIMM：Adobe、EMC、QUALCOMM、Google、Wells Fargo、Microsoft、 Depository Trust & Clearing Corporation などの専門家がBSI プロジェクトに参加して策定したものである。BSIMM は、個人や組織のセキュリティ計画を支援する。

BSI の今後の方向性は、SDLC（ソフトウェア開発ライフサイクル）におけるセキュリティ・プロセスの更なる開発と促進である。主な計画は次の通りである。

1. 計画策定と開始

全般	セキュリティ
プロジェクトの概要	
達成すべき必須機能およびビジネスの目標および目的の詳細な概括	高レベルのセキュリティ目標および目的 (機密性、完全性、使用可能性) ビジネスの目標および目的がベース
プロジェクトチームのメンバー選定と役割分担	セキュリティチーム・メンバーの割り当て
プロジェクトチームの研修	セキュリティチームの研修
候補システムの記述作成	ビジネスへの影響度に従ったシステム分類 （高、中、低）の割り当て

2. 分析と要件の作成

全般	セキュリティ
利用者/株主の要件収集	初期のリスク 評価の実施、およびベースライン・セキュリティー・コントロールの選択と文書化 定義したビジネス要件をサポートする他のセキュリティ要件の定義
開発するアプリケーション・システム機能の導出と定義	開発するセキュリティ機能の定義
システム・ドキュメントの保守	セキュリティ構成要素がプロジェクト・ドキュメントに含まれていることの確認

3. 設計

全般	セキュリティ

詳細なシステム要件の定義	リスク評価の調整/更新 必要ならセキュリティコントロールの更新
システム・アーキテクチャ（情報 モデル、データベース設計、開発用プラットフォームなど)の定義	セキュリティ・アーキテクチャの定義
詳細なシステム・ドキュメントの作成	セキュリティ要件がドキュメントに含まれていることの確認
プロジェクト・ドキュメントの更新	セキュリティ ・ドキュメントの支援
システム認証作成パッケージの更新	セキュリティ関連物作成の支援

4. インプリメント

全般	セキュリティ
ソフトウェア・コードの開発	セキュリティコードが含まれていることの確認
プロトタイプの開発（該当する場合）	
ユニットおよび統合テストの実施	セキュリティコントロール テストの実施/支援
システム認証計画の作成	該当する場合、支援
システム認証パッケージの取り込み	該当する場合、支援
運用システムのインストール	
システムのシステム認証プロセスへの提出	セキュリティ・リスク分析の実行 セキュリティ上の問題に対してセキュリティ・リソースとして待機
システム認証の獲得	認証プロセスで組織の定義した役割(エキスパート・リソース)を実行
システムをビジネスの運用に展開	

5. 保守

全般	セキュリティ
継続的監視機能の確立	セキュリティ構成要素に対する継続的監視機能の確立
構成管理および変更コントロール機能(要件の改訂、プラットフォーム変更、ポリシー変更を反映した訂正など)の実施	セキュリティコントロール要件および必要な更新/改訂を重点とする構成管理および変更コントロールの検討への参画
必要に応じたシステム機能の更新/改版	必要に応じたセキュリティコントロールの更新/改版
必要に応じたシステム再認証の実行	認証で組織の定義した役割(エキスパートリソース)を実行

6. 廃棄

全般	セキュリティ
廃棄戦略/計画の作成	以下を必要とする廃棄計画の評価 ・ メディアの消去 ・ 情報の保存 ・ 処理記録の保持 廃棄要件の担当機関への提示 1
システムの廃止	
ハードウェア/ソフトウェアの処分	

国防省（DOD）は 2003 年、Joe Jarzombek をヘッドとして米国におけるソフトウェアアシュアランス（SwA：Software Assurance）構想を導入し、国土安全保障省（DHS）も 2004 年にこのイニシアティブに参画することになった。2003 年 7 月、国防省（DOD）の ASD/NII(ネットワーク・インフォメーションインテグレーション担当国防省副長官)は、政府環境における利用増に伴う商業用に取得したソフトウェアのアシュアランスリスクを評価することに関連する課題解決を目的として、ソフトウェアアシュアランス（SwA）イニシアティブを導入したのである。2004 年 12 月、ASD/NII は OUTSD/AT&L(Office of the Under Secretary of Defense/Acquisition Technology and Logistics)と連携して DOD の傘下にソフトウェアアシュアランスタイガーチームを設置し、連邦政府のリスク感応性を減少させる戦略策定を目指したのである。

タイガーチームのアプローチはシステムレベルにおけるソフトウェアセキュリティの問題解決を図ることであった。この背景には、ソフトウェアセキュリティの多くの脅威はソフトウェアレベルだけではコスト効果的な解決が不可能との考え方があったためである。したがって、タイガーチームは国防省(DoD)の関連団体である国防産業協会(NDIA-National Defense Industrial Association）と連携し、セキュリティシステムのエンジニアリングプラクティスをソフトウェア製品開発へと統合化し、ソフトウェアアシュアランスの IT 履行に与えるインパクトを重視する産業界主導の動きを牽引している。ASD/NII および OUTSD/AT&L が監督・仲介の役割を果たし、ソフトウェアアシュアランスタイガーチームは数々のフォーラムを開催し、産業界と連携して“脆弱性フリーのソフトウェア（vulnerability-free software)”を構築する競争力のある市場を創造する努力を払い、産官学連携により、ソフトウェアアシュアランスリスクの評価・査定に関連する諸問題の共通要素の解決に乗り出した。タイガーチームに貢献したのは、AIA(航空宇宙工業会)、GEIA(政府電子情報技術協会)、OMG(オブジェクトマネジメントグループ)である。2005 年 3 月、Joe Jarzombek は DHS 国家サイバー・セキュリティ部門（NCSD）ソフトウェアアシュアランス（SwA）担当ディレクターとなり、省庁間横断的なソフトウェアアシュアランス努力の調整役となっている。

国家サイバー・セキュリティ部門（NCSD）は、全米レベルの官民連携努力により、ソフトウェア開発期間中に導入されるエラーコード、悪意のあるコードまたは trap doors（秘密の落し戸）の可能性を無くすプロセスと手順を含むソフトウェア・コード開発の整合性、セキュリティおよび信頼性を向上するベストプラクティスと方法論を体系化しようとしたのである。これが、ソフトウェアアシュアランス（SwA）プログラム策定の努力であった。

“Build Security In （BSI）”の実行計画であるソフトウェアアシュアランス（SwA）プログラムは、ソフトウェア開発ライフサイクル（SDLC）におけるヒト、プロセス、技術、取得などの問題解決を図る枠組みであり、総合戦略でもある。国土安全保障省サイバー・セキュリティ＆通信オフィス（CS&C）の傘下にある国家サイバー・セキュリティ部門（NCSD）は、サイバー攻撃のリスク緩和の一環として、ソフトウェアアシュアランス（SwA）プログラムを通じて、よりセキュアで、信頼性のあるソフトウェアの開発利用を促進し、重要インフラおよび企業の情報システムを支えている。

ソフトウェアアシュアランス（SwA）プログラムは、ソフトウェアエンジニアリングの実務ガイダンスおよびツール開発の最先端を切り拓くもので、セキュアなソフトウェアエンジニアリング研究開発を促進する。このプログラムは、ソフトウェア脆弱性の削減と私的利用の最小化を図り、信頼の置けるソフトウェア製品（trustworthy software products）の開発・利用を改善する方法などの課題解決に取り組んでいる。加えて、企業および重要インフラに不可欠なミッション要求を支えるよりセキュアで、信頼できるソフトウェアの実装を可能とするものである。

国土安全保障省（DHS）によれば、ソフトウェアアシュアランスの重点課題は、次の３つの属性課題の解決である。

- Trustworthiness（信用性、信頼する価値があること）：悪意のあるまたは意図的ではない挿入によるものの如何にかかわらず、私的利用（＝搾取）目的の脆弱性（exploitable vulnerabilities）がないこと。
- Predictable Execution（予測可能な実行）：実行する際に、意図した通りにソフトウェアが機能するとの正当なコンフィデンス（信頼感）を提供するもの。
- Conformance(適合性)：要求、標準/手順に適合するソフトウェアのプロセスと製品を確保する計画的かつ体系的な複合専門領域（multi-disciplinary）の諸活動セット。

ホームランドセキュリティ（DHS）の国家サイバー・セキュリティ部門（NCSD）は、2008

年１月に､包括的国家サイバーセキュリティイニシアティブ(CNCI：Comprehensive National Cyber Security Initiative）を策定し、政府、業界および学会および国際的なコミュニティの協力関係を樹立し、 国家の情報技術（IT）および通信インフラストラクチャのセキュリティ、弾力性および信頼性を向上させようとしている。DHS の包括的国家サイバーセキュリティイニシアティブ（CNCI）は、次の３つを重点分野としている。

- 現在の脆弱性を減少し侵入を防ぐ第一線の防御を確立する。
- インテリジェントかつ強化されたサプライ・チェーン・セキュリティーを使用してすべての脅威を防御する。
- 研究、開発および教育を強化するとともに進化する技術を調査して将来の環境を形成する。

ソフトウェアアシュアランス（SwA）プログラムの主な狙いは、パッチマネジメントからソフトウェアアシュアランスへのセキュリティパラダイム・シフトを起こすことにある。この変化により、脆弱性が発見された後で情報システムにパッチ処理するのではなくて、開発当初からフトウェア開発者はソフトウェアの全般的な質とセキュリティを向上させることができるようになる。ソフトウェア開発のライフサイクル期間を通じてシステマティックな方法でセキュリティ問題を解決する必要があることを認識した上で、ソフトウェアアシュアランス（SwA）プログラムは、官民連携で、様々な刊行物の出版、セミナーや会議を通じて、公的セクターと民間セクターの両部門のすべてのソフトウェア開発者に対して、ソフトウェアのクォリティとセキュリティ、リライアビリティとディペンダビリティの改善努力とスタンダードの提起を奨励している。

国土安全保障省（DHS）のソフトウェアアシュアランス（SwA）プログラムは、隔月ベースで開催される次の７つの作業部会を支援している。

- ビジネスケース（マーケティングと公共福祉）：この作業グループは、保証されているソフトウェアの認識、理解、および需要の推進に力を入れている。この作業グループは整合したメッセージを作成するが、その形式は、情報アシュアランスのニーズが急務であることを理解するレベルに応じて複数になる。
- 技術、ツールおよび製品評価：この作業グループは、ソフトウェアアシュアランスの技術面に重点を置く。製品の評価およびこの目的達成に必要なツールを確認している。この作業グループは、DHS がスポンサーの NIST SAMATE プログラム、MITRE Common Weakness Enumeration (CWE)のアクティビティ、および NSA CAS の作業を記録し、関与している。
- 調達：この作業グループは、安全なソフトウェアの調達を確実に行うための要件

に重点を置く。ソフトウェア・サプライ・チェーン管理を、リスク管理および安全なソフトウェアとの契約によって強化することに注目している。この作業グループの最初の製品は、ドラフト・ガイダンス・ドキュメントで、ソフトウェア製品とサービスの調達ドキュメント（プロポーザル要求、作業ステートメントなど）でのソフトウェアアシュアランス関連用語のドラフト、要請文書への応答のセキュリティ評価基準の確立、およびこれらの基準を要請文書への応答の評価に使用する方法を支援する。「Acquisition Management Guide for Software Assurance（ソフトウェアアシュアランスの調達管理ガイド)」は、学界、業界、および政府からの寄付によって共同開発され、調達に関わるすべての関係者を対象にしている。

- プロセスと手法：この作業グループは、ソフトウェア開発プロセスの改善によって、安全なソフトウェアの生成が導かれる事を重視する。特にガイダンスを特定、また場合によってガイダンス、標準、手法の例、構成ガイダンスを作成し、安全なソフトウェア開発アクティビティの促進を助ける適合性確認を実施する。この作業グループの主要なアクティビティは、「Security in the Software Life Cycle」ドキュメントの作成と ISO/IEC、Institute of Electrical and Electronics Engineers (IEEE)、および OMG ソフトウェアアシュアランス関連標準イニシティィブを記録し関与することにある。
- 要員、教育および研修：この作業グループは、ドラフトの Common Body of Knowledge (CBK) を、学術的なインストラクターが大学、地方大学などの学術機関に安全なソフトウェア・エンジニアリング・カリキュラムを開発できるようにするベースとして作成する。また、対応して「Essential Body of Knowledge (EBK)」もドラフトし、要員研修プログラムとクラスの開発ベースとして提供する。
- 測定：政府、業界および学会からの代表者による作業グループである。グループは、ソフトウェアによって提供されるアシュアランスのレベルを、定量および定量的方式と技法によって評価する方法を検討する。ドキュメント「Practical Guidance for Software Assurance and Information Security Management（ソフトウェアアシュアランスと情報セキュリティ管理の実際的なガイドライン)」が公開された。このドキュメントは、ソフトウェアアシュアランス技法をソフトウェア開発プロセスに組み込み、それらのプロセスから作成されたソフトウェアの信頼性向上レベルからみた効果について定量化して評価する手法を定義する。
- 悪意あるソフトウェア：悪意あるソフトウェア（malware）の属性の列挙に力を入れ、各種の malware の特性を分類し、属性ベースの特性を適正に定義する動きと結合する。この作業は、Common Malware Enumeration (CME)の作業を補完するものとされる。

国土安全保障省（DHS）のソフトウェアアシュアランス（SwA）プログラムでは、数多くの問題点が明らかにされている。この問題点は、セキュリティを確保していないソフトウェアが連邦 IT 環境に入り込むことに関連したもので、ハードウェアおよびソフトウェアの脆弱性の解消を必要とするものである。連邦政府は、こうした脆弱性を特定する努力を払い、プロジェクトの初期段階から IT ベンダーと連携してセキュリティを情報システムに組み込むことに注力している。Federal Network Security グループと呼ばれる団体が連邦省庁と連携してソフトウェアアシュアランスのギャップを埋めている。

現在、国土安全保障省（DHS）のソフトウェアアシュアランス（SwA）プログラムは、実務的なガイダンスおよびツールを開発し、安全なソフトウェアエンジニアリングの研究開発を推し進めている。具体的には、基本的なプログラミング・エラーを回避する新しい手法から、システム・ソフトウェアの一部に妥協がある場合に安全性を維持する企業システムにいたる広範な内容を調査検証している。

国土安全保障省（DHS）の国家サイバー・セキュリティ部門（NCSD）は、NIST（国立標準研究所）により 2004 年秋から開始された SAMATE（Software Assurance Metrics and Tool Evaluation）プロジェクトを支援し、ソフトウェアアシュアランス（SwA）ツールの識別、強化、開発を促進している。NIST の SAMATE プロジェクトは、ソフトウェアアシュアランスの改善、 ソフトウェアのツールを評価できる方式の開発、ツールおよび技法の効率の測定、ツールおよびメソッドのギャップの特定などを重点的に対応している。SAMATE プロジェクトの範囲は広く、オペレーティング・システムからファイアウォール、SCADA から Web アプリケーション、ソースコードのセキュリティ分析から「作成時に訂正」方式まで及んでいる。

今後のソフトウェアアシュアランス（SwA）プログラムの方針は、現在のプロジェクトを継続することである。加えて、次の点にも留意している。

- 脆弱性の識別をハードウェア、ソフトウェアおよび人に拡大する。
- 相互運用可能なサイバー・エコシステムを、関連する ポリシーを使用して作成する。これは拡張 SCAP になるだろう。
- 市場および他のエコシステムを推進し、セキュリティ、特にソフトウェアアシュアランス の知識および基準の構築に関する選択を効率化する。

国土安全保障省（DHS）は将来的には、次のワーキンググループの活動を支援する計画である。

- クラウド・コンピューティングのサービスレベル契約（SLA)、SOA および SaaS 。具体的には、この関連の契約が法規制にどのような影響を与えるのかを調査する。
- 共通脆弱性タイプ一覧(CWE) のスコアリングシステム。1999 年頃から米国政府の支援を受けた非営利団体の MITRE が中心となり仕様策定が行われ、2006 年 3 月に最初の原案が公開された CWE（Common Weakness Enumeration）の資料はこれまでに公表されているが、今後は、最初にどの作業を行うかの課題に取り組む。
- 共通報告フォーマット。 この優先順位は高い。
- Malware Attribution Enumeration Categorization。 MITRE は Web サイトを立ち上げ、年末までに この問題を記載する。
- オンライン教育および研修。 この教育モデルによって脅威を仕事として扱う担当者が教えることができる。

DHS は、さらにレッド・チームおよびブルー・チームを形成して静的および動的分析を行うことを計画している。FNS は政府機関が SCAP、CWE、CAPEC、ISO、NIST 標準および他のツールをインプリメントすることを助け、脆弱性を客観的に評価する。

3.2.3 国防省（DOD）の DISA

国防省（DOD）は 2008 年、陸軍、海軍、空軍に次ぐ 4 番目のドメインとして“サイバースペース”を位置づけると発表した。最近のエストニアとグルジアでの戦争を教訓に、DOD は 未来の戦争では、サイバースペースが前線になるとの確信にいたったからである。今後、国防省（DoD）にとっては、このサイバースペースの安全保障が重要な課題となる。

DOD（国防省）の DISA（国防情報システム局）は、2003 年 8 月、当時のラムズフェルド国防長官による「システム中心の工業時代（System-centric Industrial Age）からネット中心の情報時代（Net-centric Information Age）への移行」という宣言を受け、「ネットセントリック戦略」を進めてきている。

国防省（DoD）の新造語である“ネットセントリック（net-centricity)”は、軍・官・民の多様なステークホルダー間の連携のためのネットワーク基盤(GIG:Global Information Grid）を基にした DOD の情報システム戦略を特徴づける用語である。このネットセントリック戦略は 1990 年代に、C4ISR(Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance)または C4I （Command, Control, Communications, Computers, Intelligence）として進められてきた構想を発展させたもので、軍・官・民の多様なステークホルダー間の連携のためのネットワーク基盤（GIG：Global Information Grid）を基に、「ネットセントリック環境」を構築してきた。その環境により、

800 万人のユーザーに対して、1,700 におよぶアプリケーションをサービス提供している。

国防省（DoD）の今後の課題は、グローバル分散する国防省管轄の情報システムをセキュアにすることである。この DOD の計画は、「GID（グローバル情報グリッド)」と呼ばれている。このタスクの担い手は、国防情報システム局（DISA: Defense Information Systems Agency である。

DISA（国防情報システム局）の主な役割は次の通り。

- スピード：IT 機能およびサービス提供のスピード向上
- 最先端に向けた活力： 企業サービスを最先端に拡張
- 優れた運用：運用効果と効率の向上
- 情報の共有と防御：情報を強固に保護しながら共有
- 価値の最適化：DISA 機能とサービス価値の顧客への周知徹底

DISA（国防情報システム局）が担う GIG（Global Information Grid）構想のビジュンは、情報マネジメント、通信およびアシュアランスにおける基本的な変化を提言することである。GIG と呼ばれるグローバル分散型情報システムは、地球規模で連結されたエンド・ツー・エンドの情報機能セットで、軍隊、政策策定部隊、サポート部隊の要請に応じて、情報を収集、プロセス、保管、普及および管理するものである。換言すれば、ユーザーがグリッド内のどの位置からでもオンデマンドで情報を利用、共有、収集、処理、保管、発信、管理できる環境の必要性に対処するために発展したものである。

GIG の目的は、ネットワーク中心の環境で情報の優位性を実現することである。その手段として、スタンドアロンのマシーンでは対処できない問題を解決する際に、各種システムとメッセージングをベースとした Web サービスが同時に相互運用できるようにしている。GIG ユーザーは、複数の自動情報システム・アプリケーションから時間が経過した情報を取得し、その情報に依存するのではなく、情報を送信および取得してリアルタイムで決定を下すことができる。GIG はグローバルなコンテキストで運用されるネット中心のシステムで、情報のプロセス、保管、管理および伝送を行って、米国の DOD 関連の安全保障と関連インテリジェンス・コミュニティ機関および部門を支援する。GIG の機能は、基地、駐屯地、キャンプ、施設、モバイル・プラットフォームおよび開発サイトで使用することができる。

GIG 構想のビジョンを実現するためには、新たな技術、オープン標準ベース機能の拡張によって可能になる情報共有技術を適用する必要がある。GIG 機能の優位性は、商用技術お

よび標準を、使用可能度、完全性、機密性、アクセス・コントロール、および拒絶性のない、DoD 独自のミッション・クリティカルなニーズに合致するために必要な機能によって補完して活用することによって実現される。ただし、現在使用できる製品は、ネット中心の GIG ビジョンをサポートするために必要な情報アシュアランス機能をすべて満たすものではない。

DISA（国防情報システム局）は、その担当分野に広範な技術を含む。例えば、無線およびモバイル機能、音声メールおよび電子メール、機密および非機密双方のネットワークなどである。これらの技術を、妥協することなく、グローバル・ベースおよび分散ベースでさらに拡大して使用することを意図している。

- 認証（真の利用者および情報であることの確認）
- 機密性（情報の非許可利用者への開示を回避）
- 完全性（データの非許可利用者による変更の不能化）
- 使用可能度（必要なとき利用可能な情報、システムとセキュリティコントロール）
- 非拒絶（送信者はトランザクションの送信を拒絶できない、受信者はその受信を拒絶できない）

【DOD の問題点】

システムが 安全な要素から構築されていれば、システムの境界レイヤーが重要になる。最大のニーズは、中核的で重要なソフトウェアが確実なものになることであり、信頼性の高い要素を作成できる場のあることである。Gus Guissanie によれば、すべてのコンピュータを見守ることは不可能であることから、重要なポイントは、クリティカルな部分に焦点を絞り込み、何かが危うくなっても、運用可能にし、どこかに危険があれば、この修復を行うことである。

DOD の主な問題点は、次の通りである。

- サイバー・セキュリティ はリーダーシップの問題である。
- グローバル化。
- 相互運用性。
- 安全な要素を集めて安全なシステムを構築することが必要。
- GIG の複雑性と依存性の増大。
- 高度化する外敵。
- 民営化とシステム のシステム（個別システムが集合したシステム）のミッション

分析（SOS）。

- 困難な課題に対して支援できる有能な人材の募集。
- 定義されたシステム内部の重要性分析 – 信頼性の高い要素と、高くない要素または素性の判らない要素の混在から信頼性の高いシステムを構築。
- サイバー攻撃への対応方法を要員に訓練する必要性。
- 兵器の新しい構成要素でのコードの増加。
- ソフトウェアアシュアランスのプロセスおよび測定可能要素への組み込みが必要。
- これは単にエンジニアリングの問題でなく、運用と組織の重点である。

【DISA の問題点】

DISA（国防情報システム局）の問題点は、Miriam Moss、DISA Corporate Communications から「The Challenges of Information Assurance」レポートに列挙されている。

ネットワークセキュリティ： DISA は、機密性の高い SIPRNet（Secret Internet Protocol Router Network）へのアクセス・コントロールの強化についてイニシティィブを持っている。特に、ハードウェア・デバイスおよびソフトウェア、さらに人に対する Network Admission Control（NAC）というプログラムによる認証機能の向上が重視されている。このプログラムは、ハードウェア・デバイスを認証する公開鍵インフラストラクチャ（PKI）プロセスへのアップグレードを伴う。 DISA は NSA ともチームを結成し、非機密ネットワークで使用される共通アクセス・カードと類似性の高いトークンを使用する人のサイバー識別プロセスを強化している。

コンフィギュレーション標準： DISA は、NIST が主導する Security Content Automation Protocol（SCAP）を支援し、コンフィギュレーション標準を定義している。DISA は、NSA および NIST とともに国防機関向けの SCAP ガイドラインを刊行する予定である。SCAP はオープン標準のセットで、ネットワークのすべてのデバイスの監視、積極的管理、および安全な状況のレポートが可能になる。 DISA のチーフ情報アシュアランス・エグゼクティブの Richard Hale によれば、「非機密ネットワーク上にインターネット・プロトコル・アドレスを持つデバイスは約 700 万台ある。これらを正しく構成し、その構成を正しく保持して測定することは、DoD のミッションと機動性が膨大に拡大していることを考慮すれば、非常に重い課題だ。われわれの機動性は世界中の他のどの組織とも比較にならないぐらい大きい」。

無線センサーグリッド： 従業員が企業の非機密ネットワークに自宅から接続すると、重要なデータが露出する。現在の解決策ではスキャンしてパッチで修正する。Computer

Network Defense Enterprise Solutions Steering Group は、DISA は、イニシティィブがさらに全体論による解決策を見つけ出すべきかどうかについて評価することを助けている。

容易な使用と管理： 進入の検出、進入に対する防御、脆弱性のスキャン、および脆弱性の修正に関する現在のプロセスおよびツールは、軍事サービス部門のシステム管理者およびセキュリティのプロフェッショナルが使用するには、非常に難しい。DISA は、業界がこのニーズについて話し合える各種の公共および民間組織に参画し、インプリメントと運用を容易にする機能を開発するように仕向けている。

DoD は Globalization グローバリゼーションタスクフォースを結成し、米軍が使用する情報システムのグローバリゼーションによって生まれる国家のセキュリティ・リスクを軽減しようとしている。これは、特に従来のリスク管理、サプライチェーンのリスク 管理、情報システムアシュアランスとソフトウェアアシュアランスの両方に重点が置かれている。主な問題点は、次の通りである。

- 重要なシステムおよびコンポーネントの最小化。 規模の経済性に基づけば、セキュリティとコスト間にはトレードオフの関係がある。 総システム・コストは、COTS（即利用可能）をソースとする重要性のないコンポーネントの数を最大化し、コストのかかるセキュリティ測定を必要とする重要なコンポーネントを減らすことによって管理できる。
- アシュアランスケースの定義と測定
- ハードウェア・セキュリティとソフトウェアセキュリティのバランス
- システム・インテグレーションと商用の即使用可能（COTS）ソフトウェアベンダーのバランスに関するガイダンス

現在のプログラム内容は次の通りである。

- トランザクションのリスク管理：GTF は、CFIUS および FCC など既存のリスク 管理 プログラムのインプリメントとサポートを続けている。
- サプライチェーン リスク管理（SCRM）：CFIUS に残されたギャップを埋めるため SCRM の下に、プログラムが追加分類された。特にこれは概念から開発、展開から使用停止に至るソフトウェア製品の全ライフサイクルに対応するものではない。また、戦略的な パートナーシップ、アウトソーシング契約、域外契約またはサービスレベル契約（SLA)にも対応しない。SCRM プログラムは、ソフトウェア開発ライフサイクル（SDLC)全体の調達ツールのセット、技法およびインテリジェンス・

リソースを提供するものである。

- ソフトウェアアシュアランスおよび信頼されているICメーカーの両方のシステムアシュアランス

国防省（DOD）は、全米国防産業協会（NDIA: National Defense Industries Association）の執筆した「システムアシュアランス・ガイドラインのためのエンジニアリング（Engineering for System Assurance guidelines）, Version 1.0」を出版した。この刊行物は、 AT&L および NII が“NDIA システムアシュアランス委員会”の下で作成したもので、合理的なセキュリティおよびアシュアランス・エンジニアリング手法を提供し、重要性を要素化して、アシュアランス事例の作成と測定を行っている。

NSA（国家安全保障局）との共同プログラムである“Trusted Foundry（信頼できる供給元)”は、システム障害が許されない情報システムに組み込まれるハードウェアのセキュリティを重要視している。このTrusted Foundryプログラムは、DoDの特別なセキュリティ基準を遵守させるのではなくて、マイクロ・エレクトロニック部品ベンダーを信頼できる納入業者として認証するスキームである。この狙いは、潜在的な偽造、改ざん、妨害行為、サボタージュ、不正の解消にある。

テストおよび評価によるソフトウェアアシュアランス（SwA）プログラムには、NSA（国家安全保障局）の Center for Assured Software（CAS）と Common Weakness Enumeration（CWE）Formalized Demonstration の２つがある。 CAS（アシュアードソフトウェアセンター）プログラムは静的評価ツールおよびバイナリー・ツールを評価している。CWE は歴史的に非公式の定義を使用してきた。DoDは、NSAやNIST、OMG（Object Management Group）と協力して、知識発見メタモデル（KDM: Knowledge Discovery Meta Model)、共通ビジネス言語セマンティックス、DHS/NIST テスト・ケース・ジェネレーターおよびCOTS 分析 ツールを使用してCWE（共通脆弱性タイプ一覧）を公式化しようとしている。

- **CAS 戦略**：NSA（国家安全保障局）CAS（アシュアードソフトウェアセンター） の全ライフサイクルソフトウェアアシュアランス評価メソドロジーを完成・施行を目指す CAS 戦略は、公共ソフトウェアアシュアランス標準アクティビティに参画し、メソドロジーのサポートに使用できる商用およびオープンソース・ツールおよび技法の技術的な方向性に影響を与える。CASは、NSAの内部ソフトウェアアシュアランス標準を定義し、それらの標準への準拠を確実にする。この中には、「Guidance for Addressing Malicious Code Risk（悪意あるコードのリスクに対応するガイダンス)」などがある。
- **CAMP**:コード査定手法の策定を目指すCAMP(Code Assessment Methodology Project)

は、 米国政府のソフトウェアアシュアランス強化、および非国際的および国際的に挿入された悪意あるコードからの防御に関するニーズに対して、信頼されていないコードを分析するソフトウェア評価メソドロジーに関する基盤を据えて応える。 プロジェクトは、悪意あるコードおよび悪意をもって挿入されたソフトウェアの脆弱性のリスクに重点を置く。

- **AT/SPI**：空軍の研究ラボ AFRL（Air Force Rome Laboratories Sensors Directorate）では、改ざん防止とソフトウェア保護を目的とする AT/SPI（Anti-Tamper/Software Protection Initiative（AT/SPI）イニシアティブが設置された。この構想の狙いは、国家安全保障システム内のソフトウェアコンポーネントとアプリケーションに対する敵対者によるリバース・エンジニアリングや危険性を撃退することである。AT/SPI は、ソフトウェア要件を決定し、保護技法の開発をガイドする。AT/SPI の主要な対象は、重要な国家安全保障ソフトウェア・サービスの許可のない配布、改ざん、サービス拒絶にある。SPI の目的は次のとおりである。
  - 保護措置を、既存の DoD ソフトウェアコンポーネント、アプリケーションおよびシステムに導入。
  - 現行保護措置の有効性を検証。
  - 新しいソフトウェア保護技術の研究
  - SPI ソフトウェア保護の方針に基づくソフトウェア 開発コミュニティの教育。
  - ハイエンド・ソフトウェアへの脅威の認識強化とその保護の必要性。
  - ソフトウェア保方法における官民協力。
  - 現在のソフトウェア保護ポリシーおよび新しいポリシー開発の研究

現在までのところ、AT/SPI 構想における作業努力の結果、ソフトウェアのフルライフサイクル保護、サーバー攻撃シミュレーションツール、特定の脅威環境に提供される保護のレベルを正確に測定するツール開発を確保する安全な開発環境などの技術面での進展があった。

AT/SPI 計画では、検証されたツールのセットで、安全な環境でのコード開発をサポートとし、そのコードのソフトウェアを配布・利用する前に保護するようにサポートする SPC も策定されている。

DoD は、ソフトウェア業界のテスト・サイクル後のセキュリティ評価サイクルのモデル化を探求している。Naval Postgraduate School の研究者は、GIG Lite という研究イニシティブで、この実現性を研究している。GIG Lite は Joint Interoperability Test Command の補助を受け、サービスおよびアプリケーションを Global Information Grid (GIG)で使用するための認証および認証に関わる時間の短縮方法を求めている。

【今後の方向性】

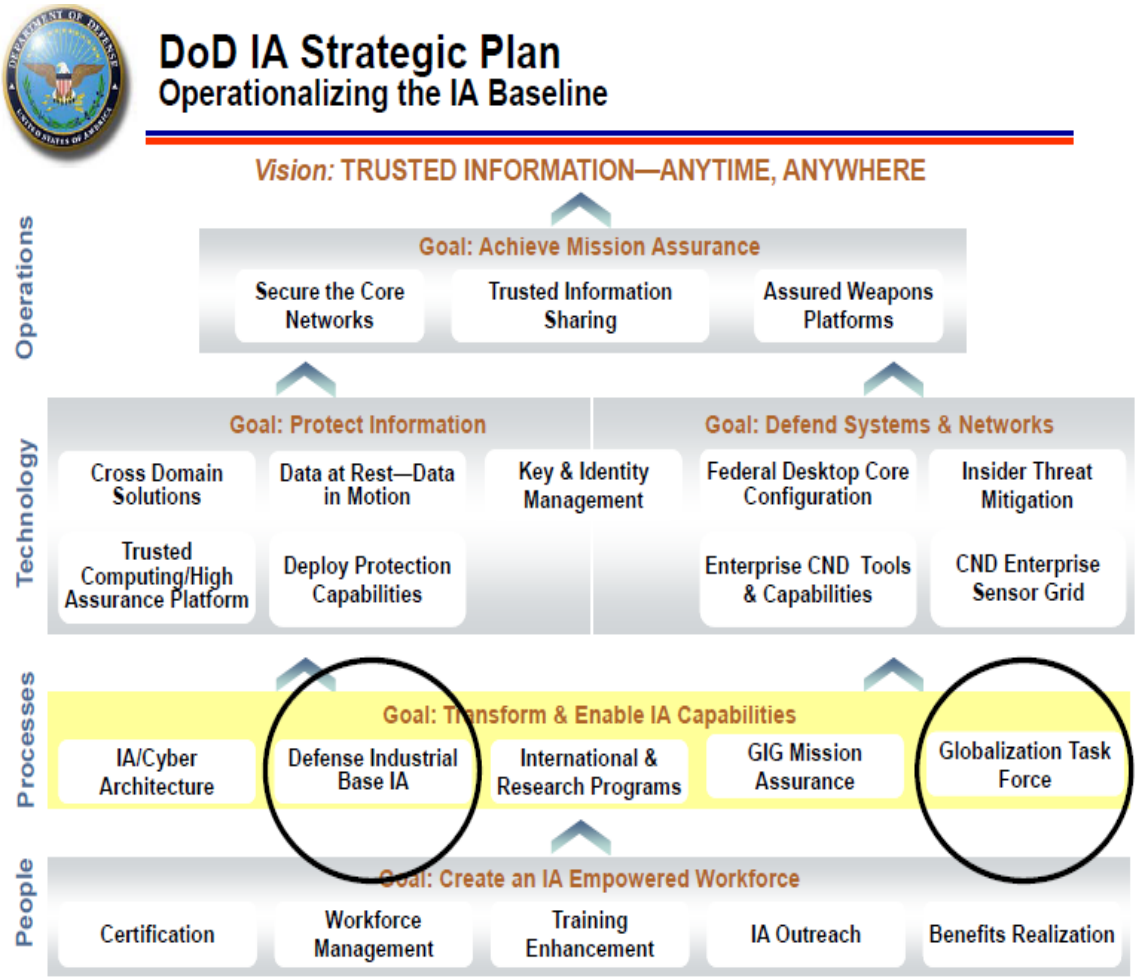
サイバースペースでの処理の自由度は、機敏性と応答性、連携するものとの信頼性の高い情報共有、脅威への対抗性、および運用の弾力性によるものである。

- DoD イニシティィブ 5200.39 上に、調達、システム・アシュアランス・エンジニアリング、研究および開発、ソフトウェアおよびハードウェアのアシュアランスに関するパイロット・プログラムによって、DoD の SCRM をインプリメンテーションする。
- DoD サプライチェーン・リスク評価機能を確立する。
- DoD と業界との連携協力を拡大する。

【事例：米太平洋軍司令部（PACOM)】

国防省（DoD）が陸軍、海軍、空軍に次ぐ 4 番目のドメインとして“サイバースペース”を位置づけるために、戦闘司令部（COCOM)は情報アシュアランス（IA）とサイバー要素のインテグレーションに乗り出し、先陣を走るのは米太平洋軍司令部（PACOM）である。PACOM の第 1 Tier 演習の Terminal Fury（終末段階の怒り） は、国防省（DoD）におけるサイバー要素のインテグレーションの演習である。 Terminal Fury やその他の PACOM 演習は、個々の機能、複数の機能、および司令部のパフォーマンスをテストし評価する。演習の重点は、計画、ポリシー、個人およびネットワークの運用手順、方向性およびコントロール、またコンピューター・ネットワークの防御（CND）応答および復元の演習にある。成功する訓練イベントには、決定とアクティビティを推進するシナリオが、詳細にまた統合され、さらにそれが投入され更新されることを伴う。 その目的は、運用上重大な局面のストレスに満ちた環境で、迅速で効果的な応答を必要とする複雑な問題に対して、訓練を受けた担当者が、その能力を顕示することにある。

図 26　国防省（DOD）の情報アシュアランス戦略計画



Source:　Mitch Komafoff, Globalization Task Force, OASD、DoD, CIO

Sample Lifecycle Management Strategy

Life Cycle Phases	Design	Manufacturing	Integration	Distribution	Operations	Services/ Maintenance	Retirement
Sample Protective Measures	• Identify critical components early •Use isolation and separation	• Employ service level agreements related to quality and security •Trusted suppliers	• Limit online SW installations •Thoroughly vet updates	• Use secure distribution channels	• Implement and enforce traditional information assurance policies	• Confirm the integrity of network mapping	•Secure destruction of media and computers
← To meet tomorrow's threat we must develop protection measures across product lifecycle *and* reinforce these measures through USG acquisition processes and effective implementation of agency security practices →							

Source:　Mitch Komafoff, Globalization Task Force, OASD(NII) DoD, CIO

【国家安全保障システム委員会（CNSS)】

国防省（DOD）の国家安全保障システム委員会（CNSS）は、情報時代の重要インフラ防護対策である 2001 年 10 月の大統領行政命令第 13231 号（Executive Order 13231）に基づいて、DOD が議長を務める国家安全保障通信情報システムセキュリティ委員会（NSTISS）を再編して設置された。CNSS は、通信および情報システム保護する連邦政府の国家の安全保障コミュニティを代表する 21 人のメンバーから構成され、米国の国家安全保障をサポートしている。

国防省(DoD)が主導する CNSS は､すべての政府機関を拘束する情報アシュアランス(IA)、セキュリティ、調達、標準、プロポーザルおよびアーキテクチャに関連する施策を策定して、これを公表している。主な国家安全保障システム委員会（CNSS）のセキュリティ関連システムは次の活動に関与している。

- インテリジェンス活動
- 国家の安全保障に関連する暗号活動
- 軍部の指令・統制
- 武器または兵器システムの一部である機器
- 軍隊またはインテリジェンス・ミッションの履行の中でクリティカルなもの（日常の事務管理やアプリケーションを除く）

CNSS は、国家の安全保障プログラムのセキュリティに関して、ポリシー問題を検討するフォーラムの開催、国家ポリシーの策定、方針、運用手順、ガイダンスの普及を行っている。国家安全保障システムは、機密レベル分類システムに基づく情報を含む米国政府、政府調達請負業者またはエージェントに適用される情報システムである。

CNCC の全身である国家安全保障通信情報システムセキュリティ委員会(NSTISS:National Security Telecommunications and Information Systems Security Committee）は 2000 年 1 月、国家情報アシュアランス調達方針第 11 号(National Information Assurance Acquisition Policy No. 11(NSTISSP No.11)を発行し、情報アシュアランス（IA）と IA 対応 IT 製品の調達に関する連邦政府の方針を規定している。

国家安全保障システム委員会（CNSS）は、情報アシュアランス（IA）を次のように定義している。

- Measures that protect and defend information and information systems by

ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
訳：可用性（Availability)、完全性（Integrity)、認証（Authentication)、機密性（Confidentiality)、否認防止（non-dupidiation）を確実に保証することにより、情報及び情報システムを保護および防護する措置

一方、CNSS の定義するソフトウェアアシュアランス（SwA）は、“Level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner（ソフトウェアが、そのライフサイクル期間中のいかなる時点でも、意図的に設計されたか、あるいは偶発的に挿入された脆弱性から免れていること、ならびに、ソフトウェアが意図した方法で機能していることのコンフィデンス（信頼感）の水準）である。加えて、国家セキュリティシステム委員会（CNNC）は、セキュリティの信頼感（コンフィデンス）に加えて、ソフトウェアの予測可能性（Predictability）も重視している。

次の表は、2008 年の重点課題と実績を一覧表にまとめたものである。

2008 年度の重点課題	成果
確認された情報の共有	
CNSS と Information Sharing Environment (PM-ISE)の プログラムマネージャ間のパートナーシップを強化し、PM-ISE アーキテクチャ、共通標準イニシティブ、情報の共有に関する国家戦略のインプリメントを支援する	CNSS は、複数分野にわたる担当情報の共有を刷新し Assured Information Sharing Working Group (AISWG) を再度活性化し、PM-ISE とのパートナーシップを強化して、アーキテクチャ、共通標準、情報の共有に関する国家戦略のインプリメントを支援した。AISWG は CNSS Policy #24「The National Information Sharing Policy for National Security Systems」を作成した。
重要で価値の高いモバイル・コンピューティング ・デバイスおよびリムーバブル・メディア上の非機密データを除くすべての重要なデータを保護し、国家の安全保障全般で保存データの高度な割引調達方法を促進する。	150 万ライセンスが、Data at Rest（保存データ）Tiger Team Blanket Purchase Agreements (BPA) によって連邦、州、および地方政府に売られ、コントロールされた非機密情報 (CUI) をモバイル・デバイスおよびリムーバブル・デバイス上で確実に保護することに貢献した。 CNSS は Wireless Tiger Team を設立し、NCSS ポリシー #17 の「National Information Assurance Policy on Wireless Capabilities」を更新し、リスク管理のガイドラインを運用環境で使用するように、また評価の共通プロセス、および進化

	する無線技術を取り入れた。
DoD/インテリジェンス・コミュニティ分野の単一のインプリメント・プロセスを支援して、連邦政府全般の情報共有を促進する。	Unified Cross Domain Management Office は、政府機関が全分野にわたってNSSをサポートするソリューションを取得するための、合理化されたプロセスを策定した。 国家安全保障コミュニティでの Blackberry およびインターネット・プロトコル経由の音声通信（VoIP）電話の使用が増加した。

2008 の優先順位	成果
リスク管理	
NSSの共通リスク 評価メソドロジーを公式ポリシーを使用して運用可能にし、連邦政府全般での採用を促進する	CNSS developed CNSS ポリシー #22 の「Risk Management Policy for National Security Systems,」を作成した。これによって、単一の統一されたリスク 管理フレームワークおよびシステム認証の受け入れを促進する。
連邦政府の共通で統一された証明および認定プロセスをインプリメントし、セキュリティコントロール、影響度、統一証明プロセスに関するCNSS ポリシーおよび指示を刊行する。	CNSS、DoD、Office of the Director of National Intelligence、NIST はポリシーと指示を作成し、NSS の証明および認証の共通手法に関する基盤を提供した。
連邦政府全般にわたるサプライチェーン・リスク管理インプリメントを支援する。このため、連邦調達プロセスおよびガイダンスを使用して調達ポリシー、プロセス、ガイダンスを作成し、NSS ポリシーおよび手法への整合性を確認する。	連邦調達プロセスに、複数のガイドおよびパイロット・プログラムを使用して、情報アシュアランスおよびセキュリティに関与する事項を組み込みための手法を提示し、サプライチェーン・リスク管理に対応した。 CNSS はポリシーを作成し、サプライチェーン・リスク 管理の一環として、ソフトウェア 調達のセキュリティ要件に対応している。
アシュアランスの識別	
公開鍵インフラストラクチャ（PKI）の相互運用性および情報共有要件のベースラインを機密および非機密ネットワークの両方に対して作成し、連邦政府全般に普及させる。	CNSS ポリシー #25 の「National Information Assurance Policy for Public Key Infrastructure in National Security Systems」を、Sensitive Compartmented Information（SCI）環境用に IC によってインプリメントされた階層 PKI の後に、SECRET 環境用の PKI をパターン化してインプリメントするために最終的なものにした。 CNSS PKI 作業グループは指示を作成し、SECRET および下位システム用の PKI 証明書の 運用を管轄する。 DoD は新しいポリシーを採用し、連邦ブリッジ証明許可によってサードパーティ PKI を受け入れた。
NSS 識別アシュアランス・ロードマップおよ	連邦機関および政府機関の担当者間の情報共有

びアーキテクチャを複数要因認証のインプリメント、国家寿命基準作業および連邦商用即使用可能ソリューションの促進用に発行する。	を増進し、信用認定管理提供に関わるコストを軽減するため、DoD は複数の DoD Web サイトおよび情報システムへの電子認証を、連邦機関および政府機関利用者に、Homeland Security Presidential Directive 12 に準拠するカードによって拡大した。

2008 年の優先順位	成果
ミッションを保証するネットワークの弾力性	
連邦ネットワーク上の CUI の保護レベル向上と最適手法と技法交換のサポート	Defense Industrial Base (DIB) サイバー・セキュリティおよび IA プログラムによって、DoD、CNSS、DIB セクターは DIB 非機密 ネットワーク上の CUI を保護するため協力体制をとっている。 新たに 2 つの DoD 機関が設立され、脅威の情報、IA 最適手法、サイバー・アラートを DIB セクターのパートナーと共有している。
ネットワークの弾力性に関して CNSS 作業グループを設立し、National Security Community のグローバル情報インフラストラクチャへの依存性に対応するため、 ネットワークの多様性と弾力性に対して不足している点および潜在的に必要な改善点を特定する。	DoD タスク・フォースは、ネットワークの弾力性に関する主要な機能およびリソースのギャップを特定し、NSS の重要な情報インフラストラクチャの保護を強化する、実際的なモデル作成、演習、ネットワークの弾力性、運用計画策定の継続性、およびシミュレーションを促進した。DoD は、サイバー攻撃と動的攻撃 に対して運用を継続するための能力をインプリメント定期的に演習する、ポリシー、計画、およびプログラムを改善するアクションとマイルストーンの計画を策定した。 CNSS は Network Resilience Tiger チームを設立し、DoD タスク・フォースによる検出と結果を、National Security Community 全般に拡大し、NSS およびサポートするインフラストラクチャ向けに弾力的ポリシーと標準を策定した。

2008 年の優先順位	成果
優れた情報アシュアランス作業要員の育成と維持	
国際的な学界援助作業の強化	National Security Agency は、英国の大学および政府職員に米国 CAE について IA 教育プログラムで概説し、CAE プログラムおよびプロセスに関するレポートを作成して、英国、オーストラリア、ニュージーランド、カナダのパートナーに配布した。
IA 教育での国際的な Centers of Academic Excellence (CAE) による革新化推進	NSA および国土安全保障省は CAE の年次学長会議の共同スポンサーになり、アメリカの重要な情報インフラストラクチャの安全保護における高度な教育の役割を検討するフォーラムを開催し

	ている。ここでは、国家レベルの IA 作業および機会での CAE の更新、および政府との CAE 協力体制を強化して、エキスパートとリソースの増員している。 Comprehensive National Cybersecurity Initiative (CNCI) の一環として、CAE は研究案件に対する「利害共同体」を作成し、研究の躍進と IA カリキュラムの改善について、NSA、DHS、CNSS、CAE、および業界との協力を強めている。
民間セクターの研修および証明ベンダーと CNSS の関係強化	SANS Institute および International Information Systems Security Certification Consortium などの業界パートナーと協力およびチーム体制が拡大された。CAE は have joined forces with 業界と協力要員を持ち、CAE カリキュラムが業界のニーズに合致するようにしている。

出典: CNSS Report: Progress Against 2008 Priorities.

【IATAC (Information Assurance Analytical Center】

一般国民への情報開示をタイムリーかつ正確に積極展開する米国のネットワーク型情報システムは、ユーザーと敵対者の両方から簡単にアクセス可能で、しかも大規模かつ複雑なシステムとアプリケーションで構成されていることから、情報戦争に対する脆弱性は極めて危険なものになりやすい。しかし、この巨大な情報インフラのクリティカルパスと主要な脆弱性を見極めることは莫大な作業を必要とする。こうした背景要因を受けて、IATAC（情報アシュアランス技術解析センター）は、国防省（DoD）傘下の国防技術情報センター(DTIC)の管轄下に設置された。ITAC は、Booz・Allen & Hamilton Inc、IIT Research Institute および Kaman Sciences Corporation により運営されている。

IATAC の主なミッションは、国防省（DoD）に対して、情報アシュアランス（IA）に関連するデータと情報を提供することである。主な重点分野は、システムの脆弱性、研究・開発、情報戦争（IW)攻撃に対する効果的な防御をサポートする解析である。IATAC は、「State-of-the-Art Report on Software Security Assurance（SOAR)」レポートを公表し、現在のソフトウェアアシュアランス構想を明確にして説明している。 ソフトウェアセキュリティアシュアランスに関する最新レポートを意味する SOAR レポートは、ソフトウェアが作動しなければならない環境の現状、ソフトウェアセキュリティアシュアランスの促進に伴う最新の活動状況や組織機関などを示している。本レポートは、正当なコンフィデンス（信頼感）を以ってセキュアであると言えるソフトウェアを特定、取得、生産、評価、利用する目的で政府、産業界、学術界で使われているテクニックや技術についても記載し、

専門分野としてのソフトウェアセキュリティの注目すべき動向に関する知見も提供している。

SOAR（Software Security Assurance State-of-the-Art Report）レポートの主な留意点は次の通りである。

- “ソフトウェアセキュリティ（Software Security)”と“セキュアソフトウェア(Secure Software)”に関する最近の多数の記事や書物、その他の関連資料からは、“セキュリティソフトウェア（Security Software)”と“セキュアソフトウェア（Secure Software)”の区別については、少なくとも理論上、幅広く認識されつつあるようである。
- ソフトウェアセキュリティ（Software security）およびセキュアソフトウェア（secure software）はソフトウェアアシュアランスの文脈の中で議論されることが多い。ソフトウェアアシュアランスは、ソフトウェアセキュリティよりも幅広概念で、ソフトウェアセキュリティの属性に加えて、ソフトウェアの安全性と信頼性の属性を含んでいる。ソフトウェアアシュアランスの主な目標は、ソフトウェアが脆弱性から脱しているとの正当な信頼感を提供することである。
- アウトソーシングとオフショア開発のリスク：特に政府や、産業界でも外国のソフトウェア開発者およびサプライヤーによりさらされる潜在的なセキュリティの脅威に対する懸念を強めているが、それは外国の影響を受けた開発者が悪意のあるコードを輸出用ソフトウェアに埋め込んでいるという可能性の観点だけで論じられることが多い。しかし、米国に本拠を構える開発会社やSI会社の内部の悪いアクターであるインサイダーの脅威に対する注意が欠けている。たとえ、インサイダー脅威の問題が持ち上がっても、米国企業で働く外国人ワーカーに目が向いてしまう。
- SDLC（システム開発ライフサイクル）における悪意のあるコード：オフショア開発ソフトウェアに対する懸念と関連するもので、ネットワークを介したウィルスやワーム、スパイウェアなどのオペレーション上の手段だけではなくて、配送販売前のソフトウェアにおけるトロイの木馬や悪質なボット（malicious bots)、論理・時間爆弾（logic and time bombs）の埋め込みによるユーザー環境への悪意のあるコードの侵入可能性も、インサイダー脅威としての米国に本拠を構える開発者の可能性と考えられている。実際にどんなコードが悪質なのかの定義は未だ解決されていない。
- 脆弱性の報告：最も積極的に取り組まれている研究および実用分野のひとつは、ソフトウェアにおける脆弱性のレポーティングである。過去 5 年以上にわたり、脆弱性の報告データを標準化、集中化する動きがあった。その結果、MITRE CorporationのCVE(Common Vulnerabilities and Exposures)やNIST(全米標準技

術研究所)のNVD(National Vulnerability Database)が生まれている。収集した大量の脆弱性データを特定層に対して分析しやすくすることで、CWE（Common Weakness Enumeration)やVEDEF(Vulnerability Exploit Description and Exchange Formats)などの分類、分類学（タクソノミー、Taxonomy）およびメタデータなども誕生している。

【国土安全保障省（DHS)、国防省（DOD）などの連携】

DoD（国防省）のソフトウェアアシュアランスイニシアティブは、ネットワーク情報（Defense for Networks and Information Integration)担当国防次官によって、2003年7月に設置されたソフトウェアアシュアランス問題解決に取り組むためのプログラムである。

既述した通り、国防省（DOD）のASD/NII(ネットワーク・インフォメーションインテグレーション)は2004年12月、同省の防衛調達技術ロジスティクス局（OUTSD/AT&L：Office of the Under Secretary of Defense/Acquisition Technology and Logistics)と連携してDODの傘下にソフトウェアアシュアランスタイガーチームを設置し、連邦政府のリスク感応性を減少させる戦略策定を目指している。

2005年5月2日に承認されたTiger Team戦略は、官民連携によるワーキンググループを編成して問題解決に乗り出したのである。2006 年になると、ソフトウェアアシュアランスWG の産業範囲はシステムアシュアランスにまで拡大し、システムアシュアランスワーキンググループ（SAWG）と名称変更されている。SAWGのメンバーは、国防省AT&L（調達技術ロジスティクス局）を代表として、NSA（国家安全保障局)、NII（国立情報学研究所)、国家偵察局（NRO: National Reconnaissance Office）などで構成されている。主な活動内容は、システムアシュアランス（SA）の方針およびガイダンスなどの策定である。

タイガーチームのアプローチはシステムレベルにおけるソフトウェアセキュリティの問題解決を図ることであった。この背景には、ソフトウェアセキュリティの多くの脅威はソフトウェアレベルだけではコスト効果的な解決が不可能との考え方があったためである。したがって、タイガーチームは国防省(DoD)の関連団体である国防産業協会(NDIA-National Defense Industrial Association）と連携し、セキュリティシステムのエンジニアリングプラクティスをソフトウェア製品開発へと統合化し、ソフトウェアアシュアランスのIT履行に与えるインパクトを重視する産業界主導の動きを牽引している。ASD/NII およびOUTSD/AT&L が監督・仲介の役割を果たし、ソフトウェアアシュアランスタイガーチームは数々のフォーラムを開催し、産業界と連携して“脆弱性フリーのソフトウェア（vulnerability-free software)”を構築する競争力のある市場を創造する努力を払い、

産官学連携により、ソフトウェアアシュアランスリスクの評価・査定に関連する諸問題の共通要素の解決に乗り出したのである。タイガーチームに貢献したのは、AIA(航空宇宙工業会)、GEIA(政府電子情報技術協会)、OMG(オブジェクトマネジメントグループ)である。2005 年 3 月、Joe Jarzombek は DHS 国家サイバー・セキュリティ部門（NCSD）ソフトウェアアシュアランス（SwA）担当ディレクターとなり、省庁間横断的なソフトウェアアシュアランス努力の調整役となっている。

国防省(DoD)と連携してシステムアシュアランスに取り組む NDIA(国防産業協会)では、システムアシュアランスを次のように定義している。

- Justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle.
  訳：システム機能が意図した通りに機能し、ライフサイクル期間中に任意のタイミングでシステムの一部として意図的または意図的ではない形で設計または挿入された攻略できる脆弱性を回避する正当化されたコンフィデンス。

国防産業協会（NDIA）は、ソフトウェアアシュアランスの問題に関して長期的解決策の可能性の範囲を調査するため、ソフトウェアアシュアランスのワークショップとサミットを開催した後、NDIA システムアシュアランス委員会を設立した。NDIA のシステムアシュアランス委員会では、国防省（DoD）の指令、統制、通信および武器関連システムなどの情報システムが外部侵入に対して脆弱でないようにシステムのコンフィデンスを高める努力を払っている。

同委員会の主なタスクは、“Acquisition Handbook for System Assurance（システムアシュアランスのための調達ハンドブック)”の作成である。これは、DoD（国防省）と DHS（国土安全保障省）のソフトウェアアシュアランス活動と協力した取り組みである。

国防省（DoD）の情報システムが脆弱性を回避できる確実な保証を意味する“System Assurance(SA)”の概念は、ソフトウェアアシュアランス（SwA）の活動努力の中から進化したものである。DoD は、システムアシュアランス計画を推進する努力として、多重セキュリティの方針と実施を統合化するフレームワークである PPP（プログラム保護計画）を開発し、セキュリティ要件に対応する統合政策フレームワークを示している。PPP（プログラム保護計画）は、リスク基盤のセキュリティ対策で、システムアシュアランスとソフトウェア開発プロセスを合理化し、冗長性をなくし、保護措置を講じている。

2007 年 10 月に開催された第 10 回国防産業協会（NDIA）システム会議における NDIA のシステムアシュアランス委員会の Paul Croll 副議長によると、今日のシステムの中のシステム（System of Systems）とも呼ばれる現代の大規模システムは、知財権を持つソフトウェアやオープンソースソフトウェア、レガシーシステム、ハードウェア、ファームウェアなどの極めて複雑なサプライチェーンのインテグレーションが不可欠である。加えて、大規模システムの開発では、世界中のエンジニアを使う複数のサプライヤーを使うことになる。大型システムには、機能性の優れた多くのソフトウェアを含むが、信頼性とセキュリティの高いディペンダビリティを確保する技術力は不十分である。したがって、ライフサイクル期間にわたる情報システムのアシュアランス問題を解決する努力が不可欠となる。

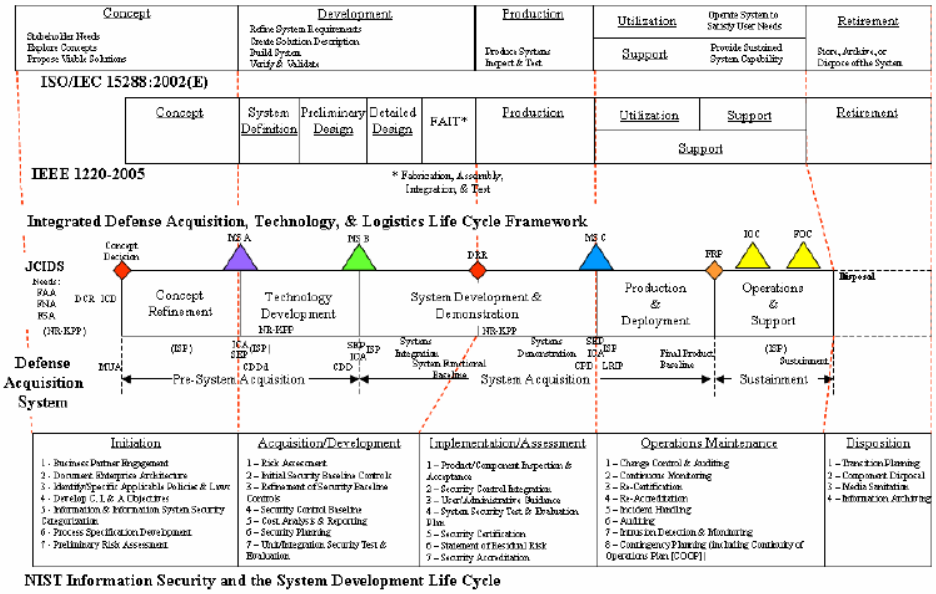
ソフトウェアリスクとタイムリーな方法でリスクを診断・緩和する有効な能力を基本的に欠いていることが、ソフトウェアアシュアランスの基本的な問題である。以上から、国防省（DoD）と NDIA のシステムアシュアランス委員会は、官民連携により政府調達のライフサイクルとサプライチェーンに及ぶシステムアシュアランス（SA）問題を解決するための新たなアプローチ法と既存のアプローチ、標準、ツールの改善に取り組んでいるのである。

国防省は 2008 年 10 月、国防産業協会（NDIA：National Defense Industries Association）の執筆した「システムアシュアランス（SA）ガイドラインのためのエンジニアリング（Engineering for System Assurance guidelines）Version 1.0」を出版している。この刊行物は、 AT&L および NII が“NDIA システムアシュアランス委員会”の下で作成したもので、合理的なセキュリティおよびアシュアランス・エンジニアリング手法を提供し、重要性を要素化して、アシュアランス事例の作成と測定を行っている。

このガイドラインの主な目的は、プログラムマネージャとシステムエンジニアを対象として、情報システムのライフサイクルにアシュアランス（確実な保証）を組み込む支援を行うことである。これは、システムエンジニアリング活動、プロセス、ツールなどのシステムアシュアランス問題解決するための要件を検討し、早期にアシュアランスの問題点を解決するための生きた文書である。

国防産業協会（NDIA）の刊行したシステムアシュアランスの手引書には、“Systems Assurance – Delivering Mission Success in the Face of Developing Threats（システムズアライアンス：発展する脅威に直面したミッションの成功)”がある。この手引書は、アシュアランスの懸念があるシステム開発の責任を持つソフトウェアエンジニア向けの情報システムとソフトウェアの知識を補完する目的で作成されたものである。

図 27　標準の統合（Alignment of Standards in the Guidebook）



NIST Information Security and the System Development Life Cycle

国防省（DOD）および国土安全保障省（DHS） は、各省内の個々の担当分野で使われているソフトウェアの運用上の安全性の確保に向けて様々な対応を図っている。DoD/DHS の共同ソフトウェアアシュアランス WG とフォーラムは、隔月ベースで開催され、ソフトウェアの安全性を様々な角度から検討している。ワシントン DC で開催されているワーキンググループでは、ソフトウェアアシュアランスのビジネスケース、調達、プロセスと技法、計測、ツールと技術、専門家研修などを行い、3 回に 1 回の割合で、ソフトウェア・アシュアランス・フォーラムを開催している。

このワーキンググループの代表的な成果は、①国土安全保障省（DHS）の BSI ウェブサイト、②DHS の Software Assurance Common Body of Knowledge（ソフトウェアアシュアランス一般知識体系）、③DHS の Security in the Software Lifecycle（ソフトウェアライフサイクルにおけるセキュリティ）などである。

DOD（国防省）の国防情報庁（DIA: Defense Intelligence Agency）と空軍（Air Force）は 2007 年 6 月、ソフトウェアアシュアランスイニシアチブを開始した。ソフトウェアセキュリティアシュアランスへの関心が急速に強まってきていることの証である。

DOD（国防省）と DHS（国土安全保障省）にまたがるソフトウェアアシュアランスの共同プロジェクトは過去に類がないほど密接な省庁間の連絡と調整を行い、省庁間にまたがる重複努力の無駄が省かれ、限られたリソースの最適化が図られている。しかしながら、NASA、FAA（連邦航空局）、エネルギー省（DOE）などのソフトウェアアシュアランスプログラムと

の密接な連携が図られていないのが問題である。また、友好国とのソフトウェアアシュアランスプログラムの連携および調整も不十分なようであり、テロ戦争における貧弱な多国間協力の問題を提起している。国際協力のないままソフトウェア開発者の法規制やライセンス供与が進展すれば、ソフトウェア産業のグローバル特性を考慮すると、世界的に大きな影響が生じることになろう。

DOD(国防省)および DHS(国土安全保障省)の一体型のソフトウェアアシュアランスの取り組みは、DOD(国防省)や DHS(国土安全保障省)という単一の省を超えた利用を目的としたセキュアなソフトウェア開発ツールの開発から、DOD や DHS の枠組みを超えた国際標準の定義にいたる幅広い活動を展開している。任務の特性から、DOD(国防省)のソフトウェアアシュアランス計画は、DHS のそれに比べてやや狭く、DOD は自省のニーズと問題にフォーカスし、DHS はサイバー情報インフラを含む全米の重要インフラ防護をミッションとし、広範な活動を展開している。

3.2.4 NSA（国家安全保障局）とアシュアードソフトウェアセンター（CAS）

国防省の一部である米国を代表するインテリジェンス機関である国家安全保障局（NSA：National Security Agency）は、電子機器を使った情報収集活動とその分析、集積、報告を担当する米国の中核的諜報機関である。国家安全保障局(NSA)の情報アシュアランス(IA)のミッションは、大統領国家安全保障行政命令 42 号（National Security Directive 42）に準拠して、国家安全保障情報と情報システムを防護することに特化している。

この行政命令は、連邦政府内の IT および通信セキュリティの基本目標と実施戦略の概要を定め、米国の国家安全保障に関連する通信・情報技術は、信頼性があり、効果的かつ効率的で、健全な技術基盤を持つことを義務づけている。この目的を実現するために設置された NSC/PCC（国家安全保障通信情報システム政策調整委員会）は、国家安全保障の通信のセキュリティを管理・運営・監視し、セキュリティ提言も行っている。

NSA の情報アシュアランスミッションの重点課題は次の通りである。

- Comprehensive vulnerability and threat analysis
- Guidance on information assurance security solutions
- Tiered security assessments
- Tailored solutions for specialized needs
- Network security products and solutions to enable assured information sharing across security domains or between communities of interest

- A 24/7 watch and analysis activity providing threat warnings, attack alerts, and bulletins
- Training and security awareness support
- The Key Management Infrastructure that provisions end cryptographic units
- Security engineering services that leverage government and commercial solutions
- A need for automation tools
- Greater foundational research and community collaboration
- Improved standards and guidelines that will reduce the cost of the software lifecycle and operations and assure missions.
- Ensure software has no exploitable flaws

現在のNSAの情報アシュアランスミッションの重点課題は､アーキテクチュアの水準で、いかにして異なるレベルのアシュアランスを、ミッションを履行するためのソフトウェアにインテグレーションするかである。

国家安全保障局（NSA）は、NISTの標準を活用。また、ホームランドセキュリティ（DHS）とも協力して、専門家教育のための大学プログラムも利用している。

NSA(国家安全保障局)は2005年11月、ソフトウェアアシュアランス問題に対応する部門として、NSAアシュアードソフトウェアセンター（CAS：Center for Assured Software）を設置した。

CAS（アシュアードソフトウェアセンター）は、NSA（国家安全保障局)およびDoD（国防省）におけるソフトウェアアシュアランス（SwA）問題解決の中核拠点となっている。CASは、DOD ソフトウェアアシュアランスタイガーチーム、DHS(国土安全保障省)のスポンサーによるソフトウェアアシュアランスワーキンググループと密接な連携を行い、国防省（DOD）のクリティカルな情報システムのソフトウェア脆弱性を最小化すると同時に、産官学連携によりソフトウェアアシュアランス業界におけるソフトウェアアシュアランスの優先順位を決め、研究促進と調整を行っている。

加えて、CAS（アシュアードソフトウェアセンター）は、重要なDODのシステムおよびネットワークで利活用する COTS(Commercial-off-the-shelf、店頭販売汎用ソフトウェア)や政府開発のソフトウェアを含むソフトウェアのライフサイクル期間中のソフトウェアの信頼性（trustworthiness）を総合的に評価する方法論とツールの開発に取り組んでいる。

国家安全保障局（NSA）の CAS（アシュアードソフトウェアセンター）は、NIST のソフトウェアアシュアランス基準とツール評価（SAMATE）プログラムの作業もコーディネーションする。CAS は、ソフトウェア・アシュアランス・コミュニティ全体でのソフトウェア・アシュアランス・アクティビティの研究、コーディネーションおよび優先順位決定に関する米国政府、学界および業界全般の共同作業をリードしている。CAS は、またメソドロジーの確立と、ソフトウェアのライフサイクル全般にわたるソフトウェアの信頼性の包括的ツールを推進しようとしている。CAS はその評価活動の結果、DoD、インテリジェンス・コミュニティ、他の連邦政府機関、さらに業界標準の機関（ISO/IEC、OMG など）に、勧告を提示しようとしている。その内容は、恒久的にアシュアランスのレベルを改善および拡張するポリシーと標準の変更､および商用ソフトウェアおよび政府開発ソフトウェアに関与するアシュアランスの測定能力に関するものである。CAS は、また公正な確かさ（アスアランス）の測定可能レベルを示す、以下のテスト可能なソフトウェアの特性も特定している。

- ソフトウェアがその目的とする機能を安全、適切、また予測可能な方法で実行すること。
- ソフトウェアが許可されない機能を実行しないこと。
- ソフトウェアが、意図的または偶然の欠陥にかかわらず、露呈されるインプリメントでの欠陥を含まないこと。

こうした動き以外にも、ソフトウェアアシュアランスの強化、信頼できないコードを分析するソフトウェア評価方法の開発基盤を整備することで、意図的または故意の挿入による悪意のあるコードの防護に取り組む CAMP(Code Assessment Methodology project)、DOD（国防省）の AT/API(Anti-Tamper and Software Protection Initiative)および傘下のソフトウェア防護センター（SPI）国防省（DoD)のソフトウェアに対する外国の影響力を分析する DSB タスク・フォースなど､数多くのプロジェクトやイニシアティブが誕生している。

3.2.5 その他の動向

【NASA の RSSR】

数千のコンピュータシステムとアプリケーションがネットワークで繋がっている NASA（航空宇宙局）では、ソフトウェアセキュリティが重要な懸念である。特に、ミッションクリティカルな情報システムのデータの紛失や破壊、情報の盗用、可用性のないことなどにかかるコストも膨大である。このために、NASA の IV&V (Goddard Independent Verification and Validation)は、RSSR (Reducing Software Security Risk) と呼ばれる研究プロジェクトを実施し、高品質のソフトウェアおよびシステムを開発するために、既

存の手法と新しい手法にセキュリティを統合する方法の開発しつつある。RSSR はソフトウェアのセキュリティとシステム開発に関連する次の問題を課題としている。

- ソフトウェア&システムエンジニアリングでのセキュリティの欠落
- 以前に指定されたコスト高のセキュリティ特性
- 「侵入とパッチ」の繰り返し
- セキュリティアシュアランスの主軸となっている断片化手法

このセキュリティ評価のツールと手法は次の 5 つで構成されている。

① A Vulnerability Matrix：脆弱性マトリックス。
② Additional Security Assessment Tools (SATs)：追加セキュリティ評価ツール。
③ A Property Based Testing (PBT) Instrument：プロパティベースのテストツール。
④ A Model Based Verification (MBV) Instrument incorporating a Flexible
⑤ A Software Security Checklist (SSC)：ソフトウェアセキュリティチェックリスト。

【NIST（国立標準技術研究所)】

オバマ政権下の連邦政府は積極的にクラウド・コンピューティングを導入するようになり、米国 NIST（国立標準技術研究所）がクラウドの定義を行い、クラウドの標準化に取り組み、クラウド・セキュリティのリスク分析を行なうようになって、NIST が取り組んだ連邦情報セキュリティマネジメント法（FISMA）準拠の認証（Citification）と認定（Accreditation）が極めて重要な意味を持つようになっている。

NIST（国立標準技術研究所）は、連邦情報セキュリティマネジメント法（FISMA）のコンプライアンス遵守の規準となる情報システムセキュリティの標準と指針を策定。連邦情報セキュリティマネジメント法（FISMA）の§11331 規定により、NIST は、国家安全保障システム（national security systems）を除く、全省庁のオペレーションと資産の情報セキュリティを確保するための標準、ガイドライン、関連する方法と手法の責任を担っている。

NIST の連邦情報セキュリティマネジメント法（FISMA）標準実施プロジェクトは、第 1 章でも詳述した通り、FIPS や SP 800 シリーズなどの政府調達基準に関する重要なセキュリティ標準とガイドラインを作成している。

FISMA コンプライアンスに準拠する NIST のセキュリティ標準とガイドラインは、“Mandatory Requirement（強制的規制）”となる。各省庁のトップの責任は、IT セキュリティのリスクを受容できる水準までコスト効果の高い削減を行なうことにあった。NIST は連邦各省庁と連携して情報および情報システムを防護し、各省庁における強固な情報セキュリティ計画の土台となる標準とガイドラインを公表している。NIST の情報技術研究所（ITL）のコンピュータセキュリティ部門がこの責務を担っている。米国 NIST（国立標準技術研究所）は、情報システムと情報サービスのセキュリティを促進・計測して有効化するための標準、メトリクス、テストおよび有効化プログラムの開発に乗り出し、連邦情報セキュリティマネジメント法（FISMA）の規定に準拠して、連邦政府の情報セキュリティを強化する目的で、FISAM 実施プロジェクト（FISMA Implementation Project）を実施している。

NIST の NVD（National Vulnerability Database)は、標準ベースの脆弱性マネジメントデータのレポジタリである。NVD（全米脆弱性データベース)は、国土安全保障省（DHS）の国家サイバー・セキュリティ部門（NCSD）の助成金を受けて、NIST のセキュリティ部門が“SCAP(セキュリティコンテンツ自動化プロトコル)”を使って開発した脆弱性 DB 製品である。このデータを使うと、脆弱性マネジメント、セキュリティ計測、連邦情報セキュリティ管理法(FISMA)などの遵守が可能になる。NVD（全米脆弱性データベース)は、セキュリティチェックリスト、セキュリティ関連ソフトウェアの欠陥、コンフィギュレーション間違い、製品名、インパクトメトリクスなどを含んでいる。また、NVD（全米脆弱性データベース)は、セキュリティの技術オペレーションの自動化および標準化を可能にする多省庁間イニシアティブの ISAP(情報化セキュリティプログラム)をサポートしている。2008 年 9 月、NVD は“Version 2.2.”にアップグレードされている。NVD は OVAL-ID を基準として含み、CVE-ID および OVAL-ID から検索することができる。IPA の脆弱性対策情報データベース「JVN iPedia」も、NVD 情報を活用している。

NIST（国立標準技術研究所）の SAMATE（Software Assurance Metrics and Tool Evaluation）は、国土安全保障省（DHS）の国家サイバー・セキュリティ部門（NCSD）および NIST をスポンサーとして、2004 年に開始されたプロジェクトである。

SAMATE（ソフトウェアアシュアランスメトリックス＆ツール評価）プロジェクトの主な内容は、既知の弱点によって攻撃されているテスト・アプリケーションの開発および公開で、そのタイプの弱点の検出に特定のツールまたは技法がどのような効果を発揮するか把握する必要性に対して、実際に利用できるテスト素材になる。SAMATE Test Reference Datasets（TRD）は CWE の弱点のタイプによって編成され、複雑性のレベルも各タイプの弱点にふさわしく多様である。したがって、複雑な弱点の例の検出に効果の高い、または低いツールを特定できる。

SAMATE プロジェクトは、ホームランドセキュリティ（DHS）のソフトウェアアシュアランスツールと R&D 要件を識別するプログラムである。NIST は、①ソフトウェア評価ツール、②ツールの実効性の計測、③ツールと手法のギャップの特定などの方法を開発し、ソフトウェアアシュアランスの改善努力を払っている。

NIST（国立標準研究所）の SAMATE ツール評価 WG、NSA（国家安全保障局）のアシュアランス WG、OMG のソフトウェアアシュアランス SIG は、緊密な共同努力を払い、CWE（共通脆弱性タイプ一覧）を開発する努力を払っている。CWE 策定努力では、ソフトウェアの脆弱性を招くソフトウェア、デザイン、およびアーキテクチャの弱点の共通辞書の作成を目的とし、民間、学界、および政府から有識者を集め、抽出可能な既知のタイプのシステムの教育、研修、評価、および証明の基盤として使用できるリファレンス・ソースを開発する。CWE　は、運用上使用されているソフトウェアの弱点が検出された特定のケースをカタログ化する CVE（Common Vulnerabilities and Exposures）イニシアティブと緊密に連携し、これらの問題に対してソフトウェアおよびオペレーティング・システムの運用バージョンが終わるまでに、ソフトウェアを検査するツールおよび評価方法の基盤の作成を支援している。

NIST の IT 製品用 Security Configuration Checklists プログラムは、設定とオプション選択のチェックリストで、連邦政府で使うコンピュータ機器と情報システムに関連するセキュリティ・リスクを最小化するものである。スポンサーは、DHS の国家サイバー・セキュリティ部門（NCSD）である。「このチェックリストを、周到に作成されたガイダンス、高品質のセキュリティ技能、ベンダー製品の知識、運用上の経験、さらにツールと組み合わせることによって、組織の脆弱性の露出を大幅に低減できる」。

Extensible Configuration Checklist Description Format（XCCDF)は、国家安全保障局（NSA）および NIST（国立標準技術研究所）が作成した、セキュリティチェックリスト、ベンチマークなどのコンフィギュレーションガイダンスの表現に関する統一基盤で、セキュリティ手法が改善されたアプリケーションを普及するものである。XCCDF のデフォルト構成チェック技術は OVAL。

【システム/ソフトウェアアシュアランスをサポートする標準】

主な標準化活動としては、“ISO/IEC 15026:2006（System and Software Integrity Levels、システムおよびソフトウェア完全性水準）”、“IEEE Standard 1074-2006（Developing a Software Project Life Cycle Process、ソフトウェア製品ライフサイクルプロセス）”、

ISO/IEC JTC1 の SC22（プログラミング言語）で取り組む“ISO/IEC Project 22.24772（Guidance for Avoiding Vulnerabilities through Language Selection and Use)”、同じく ISO/IEC JTC1 の SC22 WG 14 がフォーカスするプログラミング言語のための安全性およびセキュリティの定義、IEEE Standards P2600（Hardcopy System and Device Security）のセクション 9.2.2（Methodologies and Processes for the Development of Secure HCDs）などがある。

システムアシュアランスセキュリティについては、次の標準が一般に受容・適用されている。

- **ISO/IEC 21827 - System Security Engineering Capability Maturity Model (SSE CMM)：**
  - 米カーネギーメロン大学ソフトウェア工学研究所が公表したソフトウェア開発プロセスの改善モデルとアセスメント手法である CMM（Capability Maturity Model）の一部として、ソフトウェア&システムエンジニアリング CMM も策定されている。また、システムセキュリティエンジニアリング（SSE）CMM も完成に近い。SSE-CMM は、Systems Security Engineering- Capability Maturity Model の略語であり、システムエンジニアリング CMM（SE-CMM）の出発点として開発されたものでる。より一般的なソフトウェアエンジニアリングの成果をソフトウェア開発プロセスに活かすためのモデルであるソフトウェア CMM と、ソフトウェア CMM を運用面 等の別の観点から捉えなおした SE-CMM モデルの成果を引き継いでいる。SSE-CMM は、開発者が経験を積むごとに複数の段階を踏んで成熟度を高めていくという考え方を踏まえて、CMM のアプローチ手法をセキュリティエンジニアリングに適用しようとする技術である。
  - SSE-CMM は、1999 年に設立された国際的な非営利組織である ISSEA(International Systems Security Engineering Association）によってメンテナンスされている。また、SSE-CMM は、2002 年 10 月に国際標準化され、ISO/IEC 21827: 2002-10-01 (E) Information technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM®) として出版されている。
  - この標準は、確実に良いセキュリティエンジニアリングを確保する必要のある政府機関や会社組織のセキュリティエンジニアリングプロセスの基本的な特性を記述したものである。モデルは、下記を含むセキュリティエンジニアリング手法の標準である。
    - 開発、運用、保守、システム寿命の決定（decommissioning）を含む全ライフサイクル。
    - 組織全体。管理、組織的なエンジニアリング・アクティビティ。

- 他の分野との並行相互作用。他の分野には、システム、ソフトウェア、ハードウェア、人間的要因、テスト・エンジニアリング、システム管理、運用、保守が含まれる。
- 他の組織との相互作用。他の組織には、アクィジション、システム管理、証明、認定、評価が含まれる。

➢ SSE-CMM の対象となるプロセスは、規格のモデルの上ではプロセスエリア（PA：Process Areas）と呼ばれる。このプロセスエリアは、①PA01-11 セキュリティ独自のプロセスエリア（狭義のセキュリティプロセスエリア）と②PA12-22 プロジェクト・組織に関するプロセスエリアの 2 種類に分類される。セキュリティ独自のプロセスエリアは、「リスク」、「エンジニアリング」および「保証」の 3 つのプロセスカテゴリから成り、「PA04 脅威の評価」、「PA05 脆弱性の評価」、「PA02 被害の評価」、「PA03 リスク評価」の 4 つで構成される。

- **ISO/IEC 15443-A FrameWork for IT Security Assistance (FRITSA)：**
  - ➢ ISO/IEC JTC1/SC27 で策定された ISO/IEC TR 15443-framework for IT security assurance(FRITSA)のテクニカルレポート（TR）は 2004 年 7 月に発行された。
  - ➢ 3 つのパートから成るこの TR は、IT セキュリティ専門家の手引書で、適切なアシュアランス方法を選択して、セキュリティのサービス、製品、環境要因（配布物など）の指定、選択または利用を行うものである。この目的は、 配布物が記述された IT セキュリティアシュアランスの要求事項を確実に満たすために必要なアシュアランスのタイプと量を理解することである。

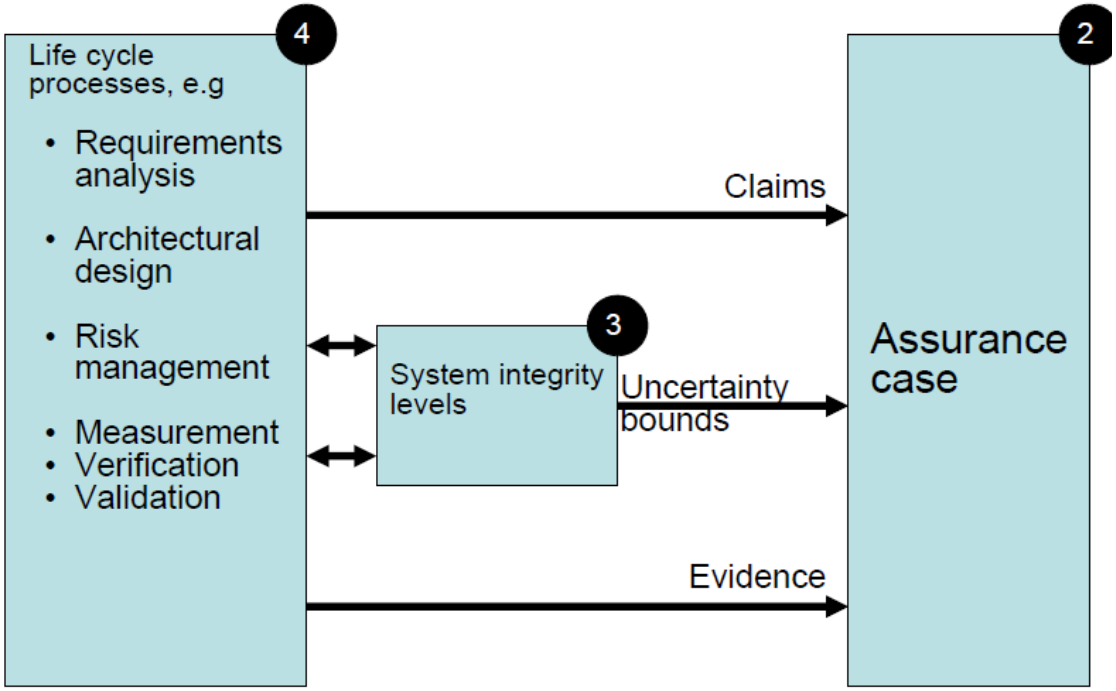
- **ISO/IEC DTR 19791-Security Assessment of Operational Systems:**
  - ➢ この運用システムのセキュリティ評価の標準は、運用システムの情報技術とセキュリティ評価のためのセキュリティ技術を記述している。

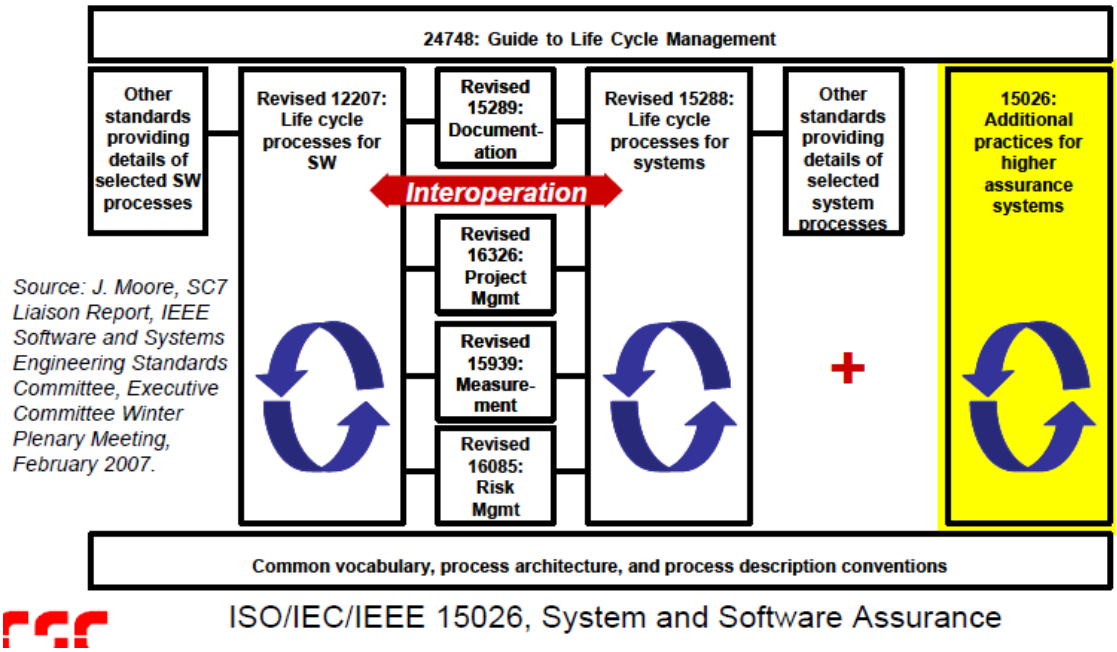
- **ISO 15026-Systems and Software Assurance:**
  - ➢ 規格番号の 15288 、12207 SE と ソフトウェア標準の相違を示し、ソフトウェア開発ライフサイクルの アシュアランスプロセスを定義する。次の通り、4 部構成の規格を作成中である。この標準規格は、防衛産業やその他の業界がよりアシュアードなシステムを構築する際の基礎になるものである。

    - 15026-1: Concepts and vocabulary (initially a TR2 and then revised to be an IS)
    - 15026-2: Assurance case (including planning for the assurance case itself)

- 15026-3: System integrity levels (a revision of the 1998 standard)
- 15026-4: Assurance in the life cycle (including project planning for assurance considerations)

上の4部の関係図





ISO/IEC/IEEE 15026, System and Software Assurance

[その他の主なプログラム]

Anti-Spyware Coalition (ASC)：ASC は、スパイウェアなど潜在的な望ましくない技術に関する定義と、最適手法についての合意を構築することに特化されている。ASC はアンチスパイウェアの企業、学界、および消費者グループから構成され、スパイウェアなど潜在的な望ましくない技術をコントロールする問題に関して、広範な見解をまとめようとしている。

Application Security Industry Consortium (AppSIC)：AppSIC は、セキュリティと技術のエキスパートが集まった小さなコミュニティで、国際的な業種全般のアプリケーションセキュリティガイドラインと測定を確立、定義し、アプリケーション・セキュリティ問題とビジネスニーズ間のギャップを埋めること、安全なソフトウェア開発プロセスの基準を作成すること、アプリケーション・セキュリティ評価基準を作成すること、アプリケーション・セキュリティの投資効果を増すことを探求している。

Center for Internet Security (CIS) Benchmarks：CIS Benchmark は、セキュリティコンフィギュレーションに最適な業界標準として、FISMA を準拠する米国政府機関、情報セキュリティ関連の ISO 規格を遵守するセキュリティ監査人、SOX 法、GLB (Graham-Leach-Bliley) 法、HIPPA (Health Insurance Portability and Accountability Act) などの規制に対応する人々により広く受容されている。CIS Benchmarks は、産官学の連携で開発したもので、セキュリティコンフィギュレーションの業界標準として認知されている。

Center for High Assurance Computing Systems (CHACS)：海軍研究所 (NRL) の IT 部門管轄下の CHACS (高アシュアランスコンピューティングシステム) は、セキュリティ、安全性、使用可能度およびコンピューティング結果のタイムリーな配布などの重点分野の研究を実施している。CHACS の主要なアクティビティでは、重要なシステム特性の正確性と維持を支援する公式な方式に重点が置かれている。CHACS の 6 つの主要な研究タスクのうち 3 つのタスクは、次のソフトウェアのセキュリティアシュアランスを重視している。

CERIAS/Perdue University's Cassandra：Purdue 大学の CERIAS (Center for Education and Research in Information Assurance and Security) が配布する無償の Cassandra は NIST の National Vulnerability Database (旧 ICAT) と Secunia の脆弱性データベースを検索できる。Cassandra は製品、ベンダー、およびキーワードのリストをこれらの「ソース」から「プロファイル」に保存し、更新があればサブスクライバーに電子メールで伝えられ

る。利用者は、ネットワーク、通常のインストール、重要なホスト、また他の関心のある分野について、必要なだけプロファイルを作成できる。

Common Announcement Interchange Format (CAIF)：CAIF は XML ベースのフォーマットで、ドイツ、シュツットガルト大学の RUS-CERT（コンピュータ緊急応答チーム）によって開発された XML ベースのフォーマットで、セキュリティ脆弱性の注意喚起（security announcement）の保存・交換を行うことができる。セキュリティに関連する問題の主要な局面を記述するように作成され、基本的であるが、包括的なセットの要素を提供する。セットになった要素は、一時的、外来的、また新しい要求をドキュメント単位で反映するように、簡単に拡張できる。

Common Configuration Enumeration (CCE)：『設定上のセキュリティ問題』に一意の番号（設定項目識別子）を付与する CCE は、セキュリティのコンフィギュレーションとエクスポージャに特化した脆弱性識別子を規定する CVE（Common Vulnerabilities and Exposures）の一部である。CCE はシステム構成に固有の ID を指定し、複数の情報ソースおよびツールにわたる構成データの相関関係を迅速かつ正確に把握できるようにしている。

Common Malware Enumeration (CME)：CME は、新しいウィルスの脅威を １つ認識にまとめて共通化し、マルウェア発生時の一般の混乱を軽減するものである。CME は、ヴィールスや他のフォームのマルウェアに使用されているベンダー名に置き換わろうとするものではなく、マルウェアの索引機能の共有と中立化を容易に適用できるようにしようとするものである。

Common Vulnerabilities and Exposures (CVE)：**CVE®**は、共通の脆弱性およびエクスポージャ（Common Vulnerabilities and Exposures）の略称で、一般的に知られている情報セキュリティの脆弱性およびエクスポージャの辞書である。CVEの共通識別子(identifier)を使えば、セキュリティ製品間のデータ交換が可能となり、ツールとサービスの保証範囲（coverage）を評価するための基本的なインデックスを提供する。ひとつの脆弱性やエクスポージャにひとつの名前をつけ、各脆弱性または各エクスポージャに標準化された記述を行いもので、データベースよりも、むしろ辞書である。国土安全保障省（DHS）のNCSD（国家サイバーセキュリティ部門）がスポンサーになっている。

Common Weaknesses Enumeration (CWE)： MITRE Corporation が 1999 年に CVE リストを作成し、ソフトウェアの弱点の分類化に乗り出し、共通したソフトウェアの弱点を定義するために、脆弱性、攻撃、フォールトおよびその他の概念を分類し、類別化する。しかし、コードセキュリティ査定業界内で提供される機能性を分類するにはこのグループ化は極め

て雑なものであった。国土安全保障省国家サイバー・セキュリティ部門（NCSD）がスポンサーとなったNISTのSAMATE(Software Assurance Metrics and Tool Evaluation)プロジェクトへの関与を契機に、MITREは本格的なプロジェクトを開始した。CWE（共通脆弱性タイプ一覧）は、ソフトウェア開発者、セキュリティ監査人（security practitioners）をターゲットにして、①アーキテクチュア、設計またはコードにおけるソフトウェアセキュリティの弱点を記述するための共通言語、②こうした弱点を狙うソフトウェアセキュリティツールのための標準スティック、③弱点の識別、緩和および抑制のための共通基準スタンダードとして役立つソフトウェアの弱みタイプのリストである。

Common Vulnerability Scoring System (CVSS)：共通脆弱性評価システムのCVSSは、情報システムの脆弱性に対するオープンで包括的、汎用的な評価手法の確立と普及を目指すNIAC（National Infrastructure Advisory Council）のプロジェクトで2004年10月に原案を作成。現在、Forum of Incident Response and Security Teams（FIRST)によって維持されている。FIRSTのCVSS-SIG(Special Interest Group)で適用推進や仕様改善が行われており、2005年6月にCVSS v1が、2007年6月にCVSS v2が公開されCVSSは、ベンダーに依存しない業界のオープン標準で、脆弱性の重大度を伝え、対応の緊急性と優先順位の判断を支援するように作成された。複数の非互換スコア付けシステムの問題を解決し、誰にも使用でき、容易に理解できる。日本のIPAもCVSS-SIGに参画し、脆弱性対策情報データベースJVN iPediaや、脆弱性関連情報の調査結果のウェブサイトでCVSS v2基本値を公表している。

DISA Security Technical Implementation Guides (STIGS)：DoDの国防情報システム局（DISA）財務会計課のセキュリティ技術実装ガイドであるSTIGSは、国防省(DoD)のDefense Information Systems機関（DISA）のセキュリティ技術インプリメント・ガイド（STIGS）は、DoDの情報アシュアランスと情報アシュアランスを有効にするネットワークの接続性を保証するセキュリティ設定ポリシーを定めている。

Distributed Management Task Force (DMTF)：DMTFは、1992年に設立されたPCや周辺機器、インターネット環境の相互運用性と管理規格を策定し、その促進を図る業界団体で、現在では大手情報機器メーカーを中心に100社以上で構成されている。日本の企業では日立製作所が、役員メンバーである。DMTF標準は、プラットフォームに依存しない技術的に中立な方法で、計測、コントロールおよび通信に共通管理基盤を提供する。

DMTFの Common Information Model (CIM)： CIMとは、IT環境における管理対象を典型的なオブジェクトとその関係で表現する方法を定義したオープン標準である。これにより、そうした管理対象をメーカーに関わらず一貫して管理することを意図している。これは、

ネットワーク/企業環境での管理全般を記述するインプリメントに中立なスキーマの共通データ・モデルである。

DMTF の Web-based Enterprise Management (WBEM)： WBEM は、企業のコンピューティング環境を統合するために開発された管理およびインターネットの標準技術のセットである。

DMTF の Web Services for Management (WS-Management)：WS-Management 仕様は、管理アプリケーションと管理対象のリソース間の相互運用性を、Web サービスの仕様と使用方法の要件の中核的なセットを識別することによって促進し、すべてのシステム管理の中心になる運用の共通セットを提示するものである。

DMTF の Systems Management Architecture for Server Hardware (SMASH)：SMASH イニシティブは、アーキテクチャのセマンティック、業界標準プロトコルおよびプロファイルを提供する仕様をまとめたもので、データセンターの管理を統合するものである。

DMFT の Open Cloud Standards Incubator：DMFT は 2009 年 4 月、“**Open Cloud Standards Incubator**”を創設。Cisco、Citrix、HP、IBM、Microsoft、VMware などベンダー13 社がメンバー。クラウド・リソース管理仕様の策定に当たり、オープンなクラウド・リソース管理技術を通じてプラットフォーム間の相互運用性を高めることで、企業内のプライベート・クラウドとほかのプライベート／パブリック／ハイブリッド・クラウド間のオペレーションを容易にすることが狙いだ。Open Cloud Standards Incubator は、相互運用可能なクラウド管理技術を実現する仕様を策定するために最適な体制であるといわれている。

Microsoft の Dynamic Systems Initiative (DSI)：DSI は、自己管理型の動的システムを提供するために Microsoft およびそのパートナーが進める取り組みである。目的は、IT チームが知識を習得および活用してより管理しやすいシステムを設計したり、継続的な作業を自動化したりすることを助け、最終的には、コストを削減すると同時に、組織にとってより重要な問題に積極的に集中できるようにすること。

Microsoft の System Definition Model (SDM)：SDM は、Microsoft とその協力会社による、アプリケーション開発ツール、オペレーティング システム、アプリケーション、ハードウェア、管理ツールを包含した統合イノベーションを可能にする統一スレッドである。企業によって統合された革新技術を、アプリケーション開発ツール、オペレーティング・システム、アプリケーション、ハードウェア、および管理ツールにわたって有効にする統合スレッド。SDM は、分散システムの定義作成に使用するモデル。SDM は、分散システムの定義を作成するのに使用するモデルである。SDM を使用すると、企業はシステム全体の生の

青写真を作成できます。この青写真はさまざまなソフトウェア ツールで作成および操作でき、システム要素を定義して、開発、展開、運用にかかわるデータを取り込むことで、IT ライフ サイクル全体と関連付けることができる。

National Cyber Security Partnership (旧 Cyber Security Industry Alliance) ：National Cyber Security Partnership (NCSP) は、ホームランドセキュリティ (DHS) の National Strategy to Secure Cyberspace(NSSC)と IT 業界の共同主催による National Cyber Security Summit 会議に端を発して発足。学術経験者、CEO、連邦政府機関および業界の専門家にゆおる自発的な協力を得て、Business Software Alliance (BSA)、Information Technology Association of America (ITAA)、TechNet および商工会議所によるサイバー・セキュリティの強化を推進する団体である。国家セキュリティ強化に向けた様々な政策提言をまとめている。共有戦略とプログラムを開発し、アメリカの重要な情報インフラのセキュリティ強化に努めている。次のタスク・フォースがある。Awareness for Home Users および Small Businesses、Cyber Security Early Warning、Corporate Governance、Security Across the Software Development Life Cycle、および Technical Standards および Common Criteria。

Open Vulnerability and Assessment Language (OVAL)：コンピュータのセキュリティ設定状態を検査するための仕様の OVAL は、国際的な情報セキュリティの業界標準で、一般に公開されている。米国政府が推進している情報セキュリティにかかわる技術面での自動化と標準化を実現する技術仕様 SCAP(Security Content Automation Protocol)の一部である。DHS の国家サイバー・セキュリティ部門 (NCSD) がスポンサーとなり、非営利団体の MITRE がが中心となり仕様策定を進める。2002 年 10 月に開催された SANS Network Security 2002 において、脆弱性対策のための確認作業を機械的に実現するための仕様として発表。2007 年からは、米国政府のデスクトップ基準である FDCC(Federal Desktop Core Configuration)での適用などを通して仕様改善が行われている。

SANS Top Twenty：“SANS Top 20 ”は、セキュリティ研究機関の SANS Institute が連邦警察局 (FBI) と共同で、最も重要なインターネットセキュリティ上の脆弱性を公表する合意リストで、サイバー・セキュリティの専門家が防御システムを調整して、攻撃側がコンピュータを乗っ取り、重要で価値のある情報を盗み出す最も重要な新しい脆弱性を明らかにしている。

CERT Vulnerability Notes、Technical Alerts & Security Bulletins：米国CERT は、様々な脆弱性に関する情報を刊行している。深刻な脆弱性に関しては、“US-CERT Technical Cyber Security Alert”で公表し、その他の脆弱性の情報は、“US-CERT Vulnerability Notes”で公表されている。米国CERTは、“Technical Cyber Security Alerts”も刊行し、現在の

セキュリティ問題、脆弱性、不具合に関する情報をタイムリーに提供する。また、“Cyber Security Bulletins”は新しい脆弱性とパッチができたときにそのパッチ情報を毎週要約して提供する。

【ソフトウェアアシュアランスの学習】

NASA（航空宇宙局）は、長年にわたりソフトウェア依存度を高めながら、NASA が開発・利用するシステムの機能性を提供している。ソフトウェア品質アシュアランス（SQA）は、システム開発プロジェクトの重要な成功要因であるが、その役割と責任は誤解されていることが多い。ソフトウェア品質アシュアランス（SQA）は、安全性、信頼性、IV&V（重要なソフトウェアの第3者評価）およびメトリックスなどのソフトウェア開発プロセス（SDP）のすべての段階を対象としている。ただし、多くの場合、プロジェクトの参加者が関連性を理解し、適切な品質アシュアランスを低廉なコストで適用することは難しい。

以下のソフトウェアアシュアランスの 12 の教訓は、2003 年に出版された“Managing Software Engineering Knowledge”からの抜粋したものである。この教訓は、NASA のゴダード宇宙飛行センター（GSFC:Goddard Space Flight Center）の品質アシュアランス担当局長の Dr. Linda H. Rosenberg による 10 年にわたるソフトウェア品質アシュアランス研究に基づいて書かれたものである。

① プロジェクトマネージャとソフトウェア開発者は、ソフトウェア品質アシュアランス（SQA）が何かと、担当するプロジェクト がそのアプリケーションからどのような恩恵を受けるかを理解する必要がある。

- ✧ ソフトウェアの品質は「Handbook of Software Quality Assurance」の中で複数の方法により定義されている。ただし、ソフトウェアの品質はソフトウェア製品利用への適合性であると結論付けている。この定義では、ソフトウェアの品質評価がソフトウェア品質の仕様およびアプリケーションに関連することが示唆されている。

② ソフトウェア品質アシュアランス（SQA）の実行は、プロジェクトに適切なバランス調整を図る活動である。

- ✧ NASA（航空宇宙局）では、過去のソフトウェア開発で十分な予算を確保できたプロジェクトはなく、特にソフトウェア品質アシュアランス（SQA）活動の実施では予算不足であった。相関関係があるために、すべての品質を満たすことは

不可能である。ソフトウェア品質アシュアランスのエンジニアは、個々のプロジェクトの狙いが異なるために、特定プロジェクトの中で何をトレードオフにするべきかを経験に基づいて決定する必要がある。これは各プロジェクトの目的が異なるからである。品質アシュアランス基準間のこれらの関連性は、使用性と効率と対照的な関連性と定義でき、また保守性と再使用性間に直接関連すると定義できる。

③ ソフトウェア品質アシュアランスは、プロセスと製品の両方を評価する必要がある。

✧ ソフトウェア品質アシュアランス(SQA)は、要求事項ドキュメント、デザイン、コード・リスト、テスト計画などのプロダクトを重視することが多い。に重点をおきがちである。しかしながら、ソフトウェア品質アシュアランスが重要視するのは、ソフトウェア開発ライフサイクルを通した継続的なモニタリングを行うことで、提供するプロダクトの品質を確保することである。このためには、プロセスとプロダクトの両方をモニタリングする必要がある。プロセスアシュアランスでは、ソフトウェア品質アシュアランスが承認された計画、手順、標準、分析に関する客観的なフィードバックを管理者に提供する。 プロダクトアシュアランス活動では、要求事項、デザイン、コード、テスト計画などのライフサイクルの各段階におけるプロダクト品質の変化する水準を重視する。この目的は、ライフサイクル期間を通じてできる限り早く欠陥を識別し、これをなくすことで、テストとメンテナンスにかかるコストを軽減することにある。

④ ソフトウェアアシュアランス（SwA）計画を策定しなければあならない。

✧ ソフトウェア品質アシュアランス計画では、プロジェクトの目標、実行の対象、開発作業を測定する標準、関連するすべての手順、ソフトウェア開発プロジェクト内のアシュアランスの組織的な構造を指定する必要がある。

⑤ ソフトウェア品質アシュアランスは、ソフトウェア開発ライフサイクル全般に行き渡ることが必要。

✧ ソフトウェア開発は、構想段階から始まり、メンテナンスにいたるライフサイクル全般に及ぶ。ソフトウェア品質アシュアランス（SQA）活動と資金調達も、概念定義から始まって開発ライフサイクル全般を対象にする必要がある。段階毎に、実行すべき活動がある。プロジェクトチームとソフトウェア品質アシュアランス（SQA）チームは共同して、各段階で適切なアクティビティが何かを、

リスクおよびリソースに基づいて判別する必要がある。品質アシュアランス計画では、どの活動を実行したのか、その決定の根拠と何か、なにとトレードオフしたのかを明らかにする必要がある。

⑥ 要求事項こそソフトウェア開発プロジェクト成功のカギ。

- ソフトウェア品質アシュアランスはライフサイクル全般を通じて実施されるものの、ソフトウェア開発プロジェクトの成功のカギは、要求事項に払う注意により決まることが多い。ライフサイクルの初期段階で潜在的なリスクを早期に識別できればできるほど、当該リスクを招く諸条件とマネジメントすることや、リスクの消去も容易になる。問題の発見がテスト段階まで伸びてしまうと、このときの修正コストは、要求事項を決める段階で早期検出して修正する場合に比べて約 14 倍の割高となる。要件仕様の品質が乏しいものであれば、プロジェクトは開始前からリスクを抱えることになる。

⑦ ソフトウェア品質アシュアランスのテストは同一でない。

- プロジェクトマネージャは、ソフトウェア品質アシュアランスを得たものと想定すること多い。この理由は、すでにテストを実施したか、あるいは、テストまで品質アシュアランスの確保が必要ないと信じていることにある。このような誤った前提は、経験、理解、また知識の欠如から生まれるものである。 品質アシュアランスの観点による、テストの目的は次の通りである。
- 問題を文書化し、修正を加えて、プロセス改善に利用することを確認すること。
- 妥当性を検討するために問題レポートを査定することを確認すること。
- レポートされた問題とこれに関連した訂正が、顧客が承認した解決策に基づいて実施されていることを確認すること。
- 問題となっている状況の開発者担当者および利用者にフィードバックを提供すること。
- ソフトウェアの品質と信頼性を計測・予見できるデータを提供すること。

⑧ メトリックスの必要性。

- ソフトウェアメトリックスは、ソフトウェア開発ライフサイクルの初期段階で無視され、必ずしてもソフトウェア品質アシュアランスと積極的に関連づけられていないことが多いが、このことは避けなければならない。ソフトウェア品質アシュアランスの実務担当者にとって、計測は重要な活動である。メトリッ

クスは、ライフサイクルの段階毎の製品とプロセスの品質の評価において計り知れない価値を持つことは実証されている。

⑨ 安全性および信頼性はソフトウェア品質アシュアランスの重要な観点。

✧ 安全性は、チーム単位の努力で、各メンバーの責任である。例えば、NASA で使うソフトウェアは、NASA の情報システムの命となる重要な部分であり、ミッションの安全性に影響を与えることもある。プロジェクトマネージャ、システムエンジニア、ソフトウェア指示者およびエンジニア、ソフトウェアアシュアランスまたは品質アシュアランスやシステム安全性の実務担当者のすべての者が安全なシステム開発の一翼を担う。信頼性と安全性は、プロジェクトの最後にテストするものでなく、ソフトウェア開発時に組み込むべきものである。

⑩ 第 3 者評価（IV&V）は、ソフトウェア品質アシュアランスの重要なツールである。

✧ NASA は、ソフトウェア開発ライフサイクル全般を通じてソフトウェア 製品の修正と品質を評価するために、システムエンジニアの厳格な方法論として第 3 者検証・妥当性検査（IV&V）を義務づけている。ソフトウェア品質アシュアランス（SQA）なしでは、IV&V の費用は割高なものとなり、費用対効果も低くなる。ソフトウェア品質アシュアランスは、プロジェクト全般をカバーするもので、ソフトウェアを含むすべての製品とプロセスを監視する機能である。IV&V は、最も高リスクと判別されたプロセスおよび製品のみを対象として、詳細な評価を行う。IV&V はすべてのプロジェクトに使用するものでなく、ミッションの信頼性およびミッション成功の確率を高めるツールである。

⑪ ハードウェアとソフトウェアの両方のアシュアランスが必要。

✧ ハードウェアの品質保証（アシュアランス）の影響は、ソフトウェア品質アシュアランス（SQA）実務担当者にも影響を及ぼすことは確かである。ハードウェア集約型システムと典型的なハードウェアに関連する懸念が強い場合には、尚更である。ハードウェア、時間および運用条件を巡る議論でも、この 2 つの問題が中心的なテーマとなる。しかしながら、ソフトウェアは異なる制約を受ける。NASA は、これらの相違点と、ハードウェアの品質保証およびソフトウェア品質アシュアランスの相違点を認識する最適なアプローチ法をとってきている。NASA のゴダード宇宙飛行センター（GSFC ）などでは、ハードウェア品質保証

とソフトウェア品質アシュアランスが、ひとつの部署の中で対応して共同作業を行っている。プロジェクトを成功させるためには、両方を必要とする。

⑫ リスク 管理はオプションでない。

✧ すべてのソフトウェア開発プロジェクトで、リスクは日常的な現実であり、継続的なリスクマネジメントを日常業務にする必要がある。このルーチンワークは、忘れてもいけないし、強要するものではなくて、満足して継続するものである。日常作業にシームレスに溶け込むことが必要である。惨事、開発手戻りや行き過ぎを回避するために役立つことから、ソフトウェアリスクマネジメントは極めて重要である。ソフトウェアリスクマネジメントの目的は、成功の障害になり、開発手戻りの主因になる前に、リスクを特定して、これを除去することである。優秀なプロジェクトマネージャは、優秀なリスクマネージャでもある。

以上の 12 の教訓は、すべてのソフトウェアアシュアランス（SwA）活動にも当てはまるが、個々の開発事情に応じて個別対応する必要がある。

3.3. 民間によるシステム＆ソフトウェアアシュアランスの動向

既述した通り、民間セクターでも、システムアシュアランス（SA）とソフトウェアアシュアランス（SwA）に関する様々な取り組みが展開されている。

MITRE Corporation は、1999 年に CWE（共通脆弱性タイプ一覧）を作成し、ソフトウェアの弱点の分類化に乗り出すしている。MITRE は、国土安全保障省（DHS）の国家サイバー・セキュリティ部門(NCSD)がスポンサーとなったNISTのSAMATE(Software Assurance Metrics and Tool Evaluation)プロジェクトへの関与を契機に本格的なプロジェクトを開始。そのCWE（共通脆弱性タイプ一覧）は、共通したソフトウェアの弱点を定義するために、脆弱性、攻撃、フォールトおよびその他の概念を分類し、類別化する。CWE は、ソフトウェア開発者、セキュリティ監査人（security practitioners）を対象とした、①アーキテクチュア、設計またはコードにおけるソフトウェアセキュリティの弱点を記述するための共通言語、②こうした弱点を狙うソフトウェアセキュリティツールのための標準スティック、③弱点の識別、緩和および抑制のための共通基準スタンダードとして役立つソフトウェアの弱みタイプのリストなどを作成している。

Forum of Incident Response and Security Teams (FIRST)によって維持されている共通脆弱性評価システムの **Common Vulnerability Scoring System (CVSS)**は、情報システムの脆弱性に対するオープンで包括的、汎用的な評価手法の確立と普及を目指し、NIAC（National Infrastructure Advisory Council）のプロジェクトである。FIRST のCVSS-SIG(Special Interest Group)で適用推進や仕様改善が行われており、2005 年 6 月にCVSS v1 が、2007 年 6 月に CVSS v2 が公開され CVSS は「ベンダーに依存しない業界のオープン標準で、脆弱性の重大度を伝え、対応の緊急性と優先順位の判断を支援するように作成された。複数の非互換スコア付けシステムの問題を解決し、誰にも使用でき、容易に理解できる」。日本の IPA も CVSS-SIG に参画し、脆弱性対策情報データベース JVN iPedia や、脆弱性関連情報の調査結果のウェブサイトで CVSS v2 基本値を公表している。

OMG のソフトウェアアシュアランス SIG(特殊利害グループ) は、外部組織と連携して、ソフトウェアの信頼性向上のための共通フレームワークを作成することをミッションとしている。SIG は、“Software Assurance Whitepaper”に基づき、ソフトウェア品質保証における立証（ファクト）のメタモデルを定義しようとしている。成果物の設計、実装の記録から派生する立証物を扱い、品質問題に対する OMG のアプローチとしては最初のもので、品質保証の基準ではなく、品質を立証するためのファクトを異なる環境、ツール、組織の間で共有するための相互運用性標準である。また、OMG のソフトウェアアシュアランス SIG

は、ツールによって最終的に OMG ソフトウェアアシュアランスの技術的手法で特定できることが必要なソフトウェア問題の 1 つのタイプとして CWE（共通脆弱性タイプ一覧）を使用している。この手法の一環には、ビジネス語彙およびビジネス・ルール言語のセマンティックを使用して、各種の CWE のモデル化の可能性を明らかにすることがある。

National Cyber Security Partnership (NCSP) は、ホームランドセキュリティ（DHS）の National Strategy to Secure Cyberspace（NSSC）と IT 業界の共同主催による National Cyber Security Summit 会議に端を発して発足。学術経験者、CEO、連邦政府機関および業界の専門家にゆおる自発的な協力を得て、Business Software Alliance (BSA)、Information Technology Association of America（ITAA)、TechNet および商工会議所によるサイバー・セキュリティの強化を推進する団体である。国家セキュリティ強化に向けた様々な政策提言をまとめている。共有戦略とプログラムを開発し、アメリカの重要な情報インフラのセキュリティ強化に努めている。

Distributed Management Task Force (DMTF)は、1992 年に設立された PC や周辺機器、インターネット環境の相互運用性と管理規格を策定し、その促進を図る業界団体である。日本の企業では日立製作所が、役員メンバーである。DMTF 標準は、プラットフォームに依存しない技術的に中立な方法で、計測、コントロールおよび通信に共通管理基盤を提供する。DMFT は 2009 年 4 月、Cisco、Citrix、HP、IBM、Microsoft、VMware などベンダー13 社がメンバーとして、“Open Cloud Standards Incubator”を創設。クラウド・リソース管理仕様の策定に当たり、オープンなクラウド・リソース管理技術を通じてプラットフォーム間の相互運用性を高めることで、企業内のプライベート・クラウドとほかのプライベート／パブリック／ハイブリッド・クラウド間のオペレーションを容易にすること目指している。

Systems and Software Consortium (SSCI)の旧名は Software Productivity Consortium で、生産性、収益性および競争力を向上させるためのソフトウェア開発手法、ツール、技術などを提供することを目的として 1986 年に非営利団体として設立された。主な加盟メンバーは、航空宇宙、防衛、IT、通信、金融、政府機関、大学などの主要な機関・会社である。BEA Systems、Computer Science Corporation (CSC)、EDS (Electronic Data Systems)、General Dynamics、Lockheed Martin、Raytheon、Unisys などが参加している。

SSCI のミッションは、加盟メンバーのシステム、ソフトウェアおよび運用プログラムのビジネスパフォーマンスの改善を加速化することである。コンソーシアムとして SSCI は、ビジネス性能を改善するシステム＆ソフトウェアプロセスの開発への産官共同投資を促し、このプロセス利用で学ぶ教訓を共有している。SSCI の提供するサービスは次の通りである。

- Architecture guidance for systems and software engineering
- Agile development approaches
- Requirements Engineering
- Measurement for systems and software
- Model-based development and testing
- Verification and validation
- Program and project management

SSCI のアジャイル開発方法には、Scrum、FCC および XP が含まれている。同コンソーシアムはアジャイルプログラミングの分野に関連して、Managing Agile Software Development と呼ばれる１日半のトレーニングコースを設ける他、以下のようなワークショップを会員向けに提供している。

- Agile Customer Focus Review Workshop
- Agile Kickoff Workshop
- Agile Mid-cycle Review Workshop
- Agile Retrospective Workshop

この他にも、OWASP(Open Web Application Security Project)、WASC(Web Application Security Group)、ICASI(Industry Consortium for Advancement of Security on the Internet)、AppSIC(Application Security Industry Consortium)、SSF(Secure Software Forum)、PA-DSS(Payment Application Data Security Standard) 、AMTSO(Anti-Malware Testing Standards Organization)などがある。

3.3.1 オープングループ（Open Group）の“ProSE”イニシアティブ

米国のオープングループ（Open Group）は、UNIX 関連の API（application programming interface）仕様の標準化を進めるために 1984 年に設立された“X/Open”と、UNIX の標準化を目指して，IBM，HP，デジタルイクイップメント（現 HP）などが 88 年 5 月に設立した“OSF（Open Software Foundation）”が 1996 年に合併して設立されたベンダー中立的かつ技術中立的な企業コンソーシアムによる業界団体である。ボストン（米国）、サンフランシスコ（米国）、レディング（英国）、東京（日本）の 4 ヶ所に拠点を擁し、ヒューレット・パッカード（HP），シスコシステムズ（Cisco Systems）、インテル(Intel)、富士通，日立製作所，IBM，サン・マイクロシステムズ、WindRiver、国防省（DoD）、NASA（航空宇宙局）などのメンバー企業／団体数は 300 以上に達している。

The Open Group は、「境界なき情報フロー（Boundaryless Information Flow）」というビジョンを掲げている。このビジョンは、セキュアで、信頼性の高いタイムリーな方法で、企業内および企業間のオープン規格と世界的な相互運用性を通じた境界のない情報の流れを実現することを目指している。Open Group は、研究機関や標準化団体に加え、業界パートナー（IT ユーザー、システムおよびソリューション・サプライヤー、ツール・ベンダー）と以下の面で連携している。

- 現在の要求事項や新たな要求事項を把握、理解して諸問題を解決し、方針を策定し、ベストプラクティスを共有すること。
- 相互運用性を促進し、コンセンサスを形成し、仕様書およびオープンソース技術を進化させて統合化すること。
- 会員メンバーのオペレーション効率を高める包括的なサービスパッケージを提供すること。
- 業界最高の認証サービスを提供すること。

特に、オープングループの著名なサービスは、認証プログラムで、Common Operating Environment（COE）プラットフォーム 、LDAP、POSIX、Schools Interoperability Framework（SIF）、UNIX、Wireless Application Protocol（WAP）の認証を行っている。The Open GroupはUNIXの登録商標の権利保有者でもある。

また、オープングループには、アーキテクチュアフォーラム、Grid Enterprise Service Forum、プラットフォームフォーラム、セキュリティフォーラム、Real Time and Embedded System Forumなどを開催している。

オープングループは、アーキテクチャ・フォーラム（IT ユーザー、ベンダー企業を含む）により開発された業界標準のアーキテクチャ・フレームワークである TOGAF（Open Group Architecture Framework)を推進している。TOGAF は、組織内で使う情報システム・アーキテクチャの開発を希望する組織が使用できる業界標準のアーキテクチャ・フレームワークである。Open Group から認証を受けると、オープン規格への適合性が保証された製品およびサービスを提供するユーザーは、市場拡大が可能となる。オープングループ（Open Group）はエンタープライズ･アーキテクチャに関しては､TOGAF 8 認証プログラムを導入している。これは、業界全体における TOGAF 8 の一貫した応用および利用を保証するもので、ユーザーに向けて TOGAF 8 の価値を保護するものである。認証プログラムの存在は、組織（民間部門、公共部門）にとって、独自の手法に固執するのを避け、エンタープライズ・アーキテクチャ向けのオープンな手法を基盤にする強力な動機となる。認証により、ツールやサービスの調達などにあたり、広く認められた分野としてエンタープライズ・アーキテクチ

ャを導入できる。

【MILSとDependability through Assuredness】

The Open Groupのリアルタイム&組み込みシステムフォーラム（RETS）は、60社を超えるメンバー数で、国防省（DoD）のIT研究部隊、NATOやDISAの参加を得て、組み込みシステムにおける相互運用性の確保など目指し、既存のアーキテクチュアアプローチの利用に基づくリアルタイムの組み込みシステム標準を定義、調整、統合および優先順序化している。このフォーラムでは、当該標準に準拠する製品の適合性を確実に保証するためのテストスイートや認証プログラムも定義している。対象業界は、航空宇宙、防衛、通信、製造、自動車、医療・科学研究などである。

主な組織体制

- **Forum Chairs**
  - Chair - Glen Logan
  - Vice Chair – Edwin Lee, Raytheon
- **Working Groups/Chairs**
  - **Open Architecture for RTES – Glen Logan/Edwin Lee**
    - Modular Open Systems Architecture –Glen Logan
    - Architecting to the Edge ™ – Edwin Lee
  - **IEEE POSIX RT Standards, Profiles, & Certification - Joe Gwinn, Raytheon**
    - IEEE POSIX 1003.13 – Joe Gwinn
    - IEEE POSIX 1003.26 – Joe Gwinn
  - **RT (Security & Safety) - Critical Systems - Michael McEvilley, MITRE/ Rance DeLong, LynuxWorks/ Edwin Lee, Raytheon**
    - MILS Demos – Ben Calloni, Lockheed Martin
    - Lexicon – Michael McEvilley
    - Standardization – Carolyn Boettcher
    - Protection Profiles – Rob Hoffman
    - MILS Integration – Rance DeLong
    - Compositional Certification – John Rushby, SRI
    - Cyber-Physical Systems – Rance DeLong
    - Commercial approach to Evaluation, Certification and Accreditation – Rance DeLong
  - **Safety Critical RT Java/JSR 302 – Doug Locke, LLC**
    - Specification
  - **Secure Mobile Architecture - Steve Venema, Boeing**
    - SCADA
    - Medical Devices
    - Intelligent Transportation Systems

リアルタイム&組み込みシステムフォーラム（RETS）担当ディレクターのJoseph I Bergmannによると、RETSのビジョンは、広く支持されるオープンなリアルタイム標準とEnabling技術を使い、テストと認証が可能なコスト効果の高いシステムを提供することである。そのミッションは、フォーラムを提供し、知識を共有し、オープン構想と統合化して承認された製品とプロセスを認証することで、リアルタイム組み込みシステムの市場導入のための時間とコストを改善することである。

Open Group は、セキュリティ関連の議題を重要視している。オープングループのリアル

タイム組み込みシステムフォーラム（RETS）では、この分野に関して、2つのプロジェクトを推進している。

１つ目は、MILS（Multiple Independent Levels of Security)で、これは、意図的または偶発的な脅威やエラーを高レベルの防護で保証し、セキュアかつ安全な運用を可能にする高保証と堅牢性の高いセキュリティ・アーキテクチュアを開発するプロジェクトである。

2008年11月に、Open Groupコンソーシアムは、サンディエゴで開催されたMILCOMコンベンションにおいてMILS(Multiple Independent Levels of Security)技術の実証を行う計画を発表。このサンディエゴ会議で発表されたMILSの実証デモンストレーションは、国防省（DoD、ボーイング、ロッキードマーティン、Raytheonおよびロックウェル・コリンズなどのOpen Groupメンバーによる長年にわたる共同研究の成果である。店頭（Off-the-shelf）製品を使い情報アシュアランスを得ることが可能となるMILSアーキテクチュアを使うことで、高アシュアランスなシステム開発、認証、認定、購入、利活用および運用がより効率的になり、手頃に利用可能となり、リスクも低くなり、伝統的な連邦政府のシステムに代替可能だとという。この会議では、MILSアーキテクチュアにより、特に、軍部や諜報活動で使われる機微な通信ネットワークの防護で実証されたと発表されている。

MILS認証により、組み込みシステムは、さまざまなセキュリティレベルが要求されるデータを処理できるようになる。MILSアーキテクチャ基盤は、Open Group、空軍研究所(AFRL)、アメリカ全国規格協会（NSA）、アイダホ大学、ロッキードマーティン、ボーイング、ロックウェル・コリンズ（Rockwell Collins）、マイター（MITRE Corporation）、オブジェクティブインターフェース システムズ社（Objective Interface Systems）、グリーンヒルズ・ソフトウェア（Green Hills Software）、リナックスワークス（LynuxWorks）、ウインドリバー（Wind River）により開発された。MILS認証は、データ、情報、ユーザーの垂直分離および水平分離を保証する証拠を提示する形式的方法を通じて取得できる。フォーラムは、UNIX/POSIX環境向けの標準MILS APIを作成する予定である。

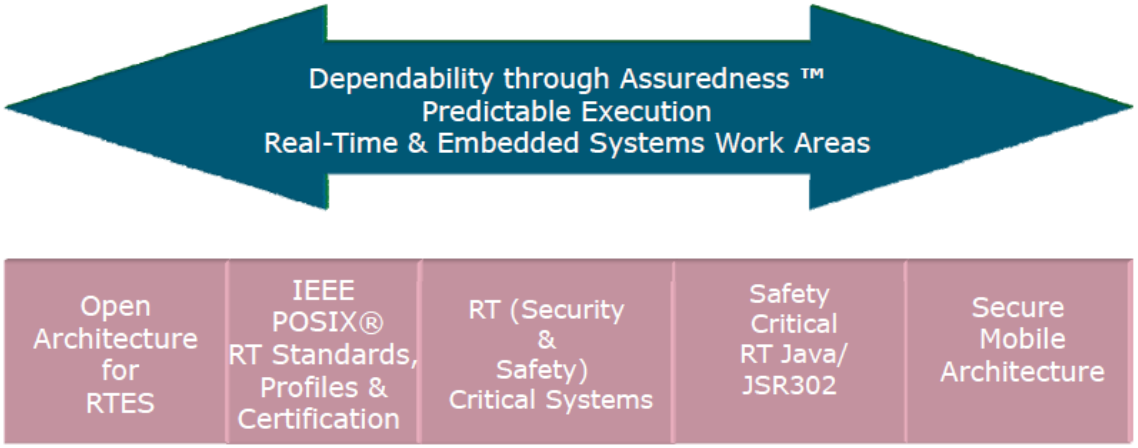
2つ目は、“Dependability through Assuredness（確実な保証を通じたディペンダビリティ）”と呼ばれるイニシアティブである。これは、ディペンダビリティの属性であるセキュリティ、フォールトトレランスなどを確実に提供する組み込みシステムの構築方法を幅広く検討するものである。

オープングループ（Open Group）の“Dependability through Assurednessイニシアティブ”では、フォーマルメソッドとオープンスタンダードに基づく認証可能な相互運用性の

あるツールを使って、高保証と堅牢性を実現する手法の開発を促進し、さらに、ドメイン横断的にコンポーネントおよびシステムをテスト、認証および認定することを目的とした分散リアルタイム・テスト・ベッド・アーキテクチャをサポートする。オープングループ（Open Group）はこのワーキンググループにおいて、次のように、堅牢な認証プロセスを開発する。この狙いは、認証ソフトウェア開発者やツール、確実性／堅牢性に優れたアプリケーションの能力開発を促進することである。

- ドメイン横断的にコンポーネントおよびシステムをテスト、認証、認定するための分散リアルタイム・アーキテクチャを定義する。
- ミッションクリティカル／セーフティクリティカル・システム（恐らくはドメイン固有）の現在のベスト・プラクティスを利用し、フォーマルメソッドおよびオープンスタンダード基づく認証可能な相互運用性のあるツールを使う。

リアルタイム&組み込みシステムフォーラム（RETS）の対象範囲



“Dependability through Assuredness”のワーキンググループは、以下の団体と協力関係にある。

- 国際標準化機構（ISO）
- 米国電気電子学会（IEEE、Institute of Electrical and Electronics Engineers ）
- 米国立標準技術研究所（NIST、National Institute for Standards and Technology ）
- オブジェクトマネージメントグループ（OMG 、Object Management Group ）
- ソサエティ・オブ・オートモーティブ・エンジニアズ（SAE、Society of Automotive Engineers）
- システムエンジニアリング国際評議会（INCOSE、International Council on Systems Engineering）
- 米国航空宇宙学会（AIAA、American Institute of Aeronautics and Astronautics ）

- ソフトウェア工学研究所（SEI、Software Engineering Institute ）

3.3.2 欧州の ProSE(Promoting Standardization for Embedded Systems)

欧州では、“ProSE（Promoting Standardization for Embedded Systems)”と呼ばれる組み込みシステムの標準化を促進する新たなイニシアティブが 2008 年に設置されている。この構想は、欧州の組み込みシステムの R&D 成果を標準化する試みである。

欧州の懸念は、グローバルな技術課題の解決と競争力強化にいかに対応するかである。主な視点は、多額の予算を投じている研究開発（R&D）成果を欧州および地球規模での標準にするために、欧州諸国で共同して組み込みシステムの R&D 成果の標準化に乗り出したのである。

欧州委員会（EC）の情報社会・メディア総局（Directorate General Information Society and Media）の組み込みシステム部門と業界は、組み込みシステムの標準化を重要視し、この市場創出を戦略的課題に設定。欧州連合（EU）の執行機関である欧州委員会（EC）は 2006 年 11 月、欧州テクノロジープラットフォーム（ETP）の組み込みインテリジェンス＆システムの標準化ワーキンググループである ARTEMIS を EU の第 7 次研究開発フレームワークプログラム（FP 7）における官民連携の共同技術イニシアティブ（JTI）方式で推進することを決め、2008 年 5 月に始動した。2007 年に開始する FP 7 では、2013 年までの R&D 予算として ICT に 90 億ユーロが投入された。

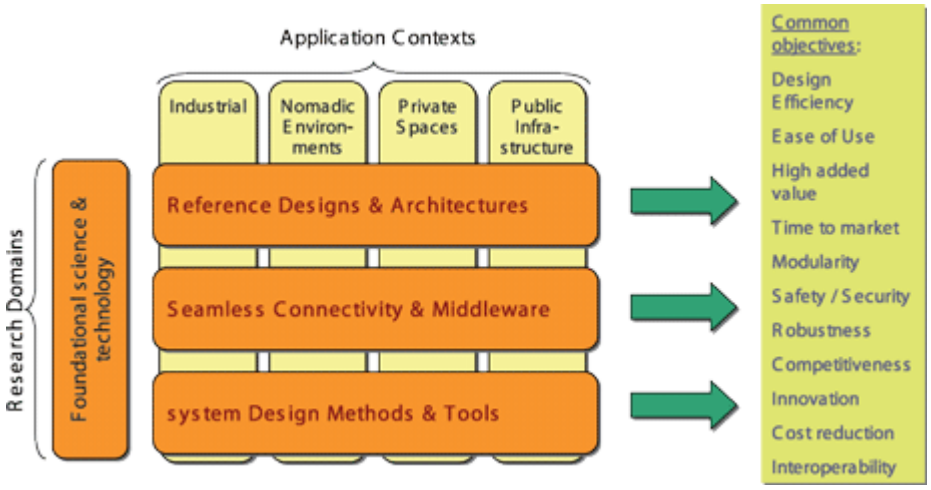
欧州テクノロジープラットフォーム(ETP)として設置された ARTEMIS(Advanced Research & Technology for Embedded Intelligence in Systems）は、フィリップス、ノキア、タレス、ダイムラー・クライスラー、ST マイクロエレクトロニクスのような欧州の主要企業 17 社が参加し、EU に加盟する 14 ヵ国も参加している。ARTEMIS イニシアティブの予算は、2007～2013 年までの 7 年間で約 30 億ユーロで、50%以上を参加企業が負担し、残りを加盟国政府と欧州委員会が負担する欧州の戦略的に重要な課題分野である。

下図の通り、ARTEMIS は第 7 次フレームワークプログラムの中で、情報システムとソフトウェアに焦点を絞るクリティカルな組み込みシステム関連のディペンダビリティ問題を重点的な研究課題とした。

しかし、ARTEMIS の抱える不安は、組み込みシステムを供給する業界と研究機関の分断化状態である。セクター間の障壁をなくし、業界の垂直統合構造を水平化することで、セクター間横断的なツールと技術を共有することが、重要な課題となったのである。この組み

込みシステム標準化の戦略的研究課題を取り上げたのが ProSE イニシアティブである。

図 28　ARTEMIS の戦略的研究課題（SRA）：研究ドメインとアプリケーション



ProSE イニシアティブのコーディネータは、フランスの Thales SA グループの Laila Gide 氏である。テクニカル・プロジェクト・マネージャーは、ARCS(Austrian Research Centers)の Erwin Schoitsch 氏である。その他の参加メンバーは、ドイツの FhG-IGD と Fraunhofer-IGD、スペインの ESI（European SW Institute)、オーストリアの研究センターである ARC と AVL List、ベルギーの ST Microelectronics、フランス原子力庁（CEA）、スペインの Acciona Infraestructuras、スウェーデンの Ericsson AB などである。

ProSE イニシアティブの主な狙いは、組み込みシステムの目的合理的かつ効率的な標準化に向けた提言を行うことで、業界全体の相乗効果を促進し、標準規格の開発および進化を加速させ、急速に進化する市場のニーズに応えることである。

ProSE プロジェクトは次の通り、4 段階で推進されている。

- 第1段階：最初のタスクは、組み込みスマートシステムのミドルウェアとアプリケーション分野の姿を明らかにして、現行および将来手のR&D成果の中で、新標準化分野となる50程度の規格を見極めることである。
- 第2段階：現存および今後の研究開発（R&D）成果の中から、ProSE参加メンバーは、標準化候補として容認される優れた候補を識別し、評価基準に照らして標準化候補リストに掲載する。
- 第3段階：利害当事者と300人程度の専門家を招聘して、オープンワークショップを

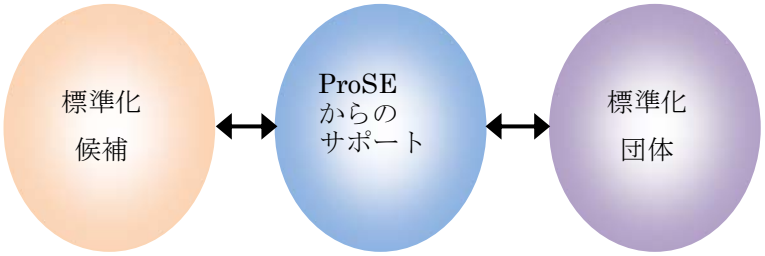
開催。

- 第4段階：標準化団体に接触し、5つ前後の標準化活動を開始する。

以上のアプローチ方法を実現するために、ProSE プロジェクトでは、標準化の現状を分析するためのフレームワークのほか、組み込みシステムの標準化の優先順位を判別する手法を開発している。

ProSE は、適切な標準化候補を特定する方法論に則り、現状調査とギャップ分析を実施する。応用分野や関連団体が細分化されている上に、標準化候補を体系的かつ選択的に規格化して組み込みシステム分野の目標をサポートできる状態にないため、望まれる規格の策定と進化は、一層加速する技術開発に追いついていない。

図 29　ProSE の役割



ProSE の主な課題は、このギャップを以下により埋めることである。

- 様々な組み込みシステムのドメインにおける既存の標準規格の知識を体系化して普及すること。
- 系統的かつ選別的な方法で標準化に適した規格候補を識別して優先順位をつけるための一連の基準を提供すること。
- 最終的な受容を目指して規格を成熟化させる実際的な方法を提案し、分野横断的な互換性と高度な再利用性を実現または促進すること。

ProSE イニシアティブは、組み込みソフトウェアや組み込みシステムの再利用性、信頼性、検証、認証をはじめとする分野横断的な固有の課題に取り組むことにより、業界全体で相乗効果を促進しようとするものである。ProSE はまた、現行の標準規格の採用を巡る問題解決にも取り組み、現在のところ適切に対処されていない分野の新スタンダードを主導・促進しつつある。

加えて、ProSE は、産業セクター横断的な相乗効果を見極めて、標準化団体に対して ProSE

ビジョンをプロモーションするため、自動車、航空機、鉄道、エネルギー、電気通信、消費財、医療などの特定市場における現行の標準規格を調査している。ProSE は、研究機関のほか、業界団体、欧州標準化団体、国際標準化団体の連携確立を図っている。本プロジェクトでは、規格候補の評価基準に加え、規格候補の普及を図り最終的に規格として成立させることを目的とした作業モデルおよび手順も開発する。長期に渡り影響力を維持するため、ProSE チームは、分野横断的なソリューションを探る上での課題に対処し、組み込みシステム分野で再利用性を向上させるのに効果的である限り、予定されているプロジェクト自体が終了しても存続する自律型プロセス（作業手法や作業方法を含む）の構築を目指している。これには、利害関係者や一般ユーザーと対話を図り普及に努めるだけでなく、意識を醸成することも求められる。

ProSE イニシアティブは、欧州の国内標準化団体および国際標準化団体と連携して、標準化に関するさまざまなニーズを分類し（ワークショップなどを通じて）、各種研究分野およびプロジェクトに共通の課題を洗い出している。この成果として、ProSE イニシアティブは組み込みシステムの標準化における課題に関するオープン・フォーラムを立ち上げる予定である。プロジェクトチームは、CENELEC、CEN、AUTOSAR をはじめとする欧州標準化団体のほか、IEC、ISO、ITU (International Telecommunication Union)などの国際標準化団体と密接に連携している。こうした団体が共同して、標準化に関するさまざまなニーズについてワークショップで議論し、各種研究分野およびプロジェクトに共通の課題を洗い出している。

前述のとおり、ProSE プロジェクトの目的は、組み込みシステムの標準化をサポートすることであり、組み込みシステムが抱えるセクター横断的な課題と信頼性に重点的に取り組むことである。ProSE は、急速に成長を続ける組み込みシステム分野で標準規格の採用を拡大するための具体的なソリューションを提供し、標準化プロセスに利害関係者を幅広く巻き込むことにより、2006 年 3 月に欧州委員会が定義した ICT の行動計画にも寄与している。

ProSE プロジェクトでは、欧州や国内における今後の作業計画の基礎となる戦略的な標準化アジェンダも提示している。主な狙いは、ARTEMIS および ARTEMISIA と協力して、優先順位を決定する方法論を確立し、標準化団体との連携を構築して標準規格の策定を推進することにより、標準化を適切にサポートすることである。ProSE の主な目的は、ARTEMISIA が採用する標準規格に関して ARTEMIS ワーキンググループをサポートすることにより、標準規格の戦略アジェンダの策定、整備、監督に ARTEMISIA と共に取り組むことである。

3.3.3 Software Assurance Form for Excellence in Code (SAFECode)

Software Assurance Form for Excellence in Code (SAFECode) は 2007 年 10 月に設立された非営利団体(NPO)である。SAFECode は、よりセキュアで信頼性の高いソフトウェア、ハードウェアおよびサービスを開発・提供することを主なミッションとしている。重点課題は、実効性の高いソフトウェアアシュアランス (SwA) 方法を進展させることで情報・通信技術製品およびサービスの信頼性を向上することである。SAFECode はグローバルな業界主導の活動で、ソフトハードウェアおよびサービスの安全性と信頼性を向上させる最適化開発手法を見極めて、この推進に取り組んでいる。会員企業は、EMC Corporation、Juniper Networks、マイクロソフト、Symantec、ノキア、SAP AG などである。Vista のウィルス対策のセキュリティ情報を Symantec に提供を拒んだマイクロソフトと Symantec は 2007 年 10 月、顧客の利益に応えるために SAFECode プロジェクトでは協力することを決めた。

SAFECode の代表 (Executive Director) は、Cyber Security Industry Alliance の創業メンバーのひとりで、クリントン政権とブッシュ政権でホワイトハウスの National Security Council と Homeland Security Council のメンバーであった Paul Kurtz である。

SAFECode の具体的な取組内容は次の通りである。

- ベンダーが使うセキュアな開発方法と完全性 (integrity) コントロールへの理解を向上させること。
- 信頼性の高いエコシステムを促進するために、ベンダー・ユーザー間で実績のあるソフトウェアアシュアランスのベストプラクティスを作成・普及すること。
- ベンダーがソフトウェアアシュアランスのベストプラクティスを利用して、企業リスクのマネジメント力を強化する支援を行うこと。
- 情報および通信技術のサイバー・エコシステムをサポートするのに必要な大学カリキュラム変更を推進すること。
- ソフトウェアアシュアランス分野での重要な研究開発プロジェクト活動を支援すること。

主な公開文書は、次の通りである。

- Framework for Software Supply Chain Integrity: Defining Risks and Responsibilities for Securing Software in the Global Supply Chain
  - ✧ 2009 年 7 月 21 日発表。

- ✧ 最初の業界主導のフレームワークで、グローバルなソフトウェア・サプライ・チェーンを確実に保証するためのリスクと責任を定義。初めてソフトウェアの完全性（Integrity）の主要な要素とソフトウェア・サプライ・チェーンを明確に定義することで、ソフトウェアエンジニアの視点からソフトウェア完全性のベストプラクティスを特定、比較、評価することを支援し、脅威を識別し、リスクを評価し、関連するリスクを緩和するためのベストプラクティスを共有して、グローバルサプライチェーンを通じて生産するソフトウェアの完全性を保護するためのプロセスガイドラインを開発。

- Fundamental Practices for Secure Software Development： A Guide to the Most Effective Secure Development Practices in Use Today
  - ✧ 2008 年 10 月 8 日発表
  - ✧ SAFECode メンバー企業による個別のソフトウェアアシュアランス努力に基づき、ベンダー毎に異なる開発環境を横断的に適用できるソフトウェアセキュリティ改善のためのセキュアな開発プラクティスをコアセットとして示す。

- Software Assurance: An Overview of Current Industry Best Practices
  2008 年 2 月発表。
  政府機関や実業界で使う情報インフラの重要な要素となっている COTS（店頭販売用ソフトウェア）などの商業利用の増加、サイバー攻撃などによる複雑かつダイナミックなリスク環境に伴う商用ソフトウェアの完全性、セキュリティおよび信頼性に対する不安の増加を解決するために、ソフトウェアアシュアランス努力のアプローチ法と、ソフトウェア開発の商用アプリケーションの管理と完全性の強化方法を示す。

【文献及び資料、インタビュー先等】

・“10 Essentials of IBM’s Cloud Computing Strategy.” John Foley. June 2009.
・2009 Cloud Consensus Report, Merlin Initiative.
・2010 Strategic Plan. Office of Electricity Delivery & Energy Reliability, September 2009.
・“A Hitchhikers Guide to the Inter-Cloud.” Krishna Sankar, Cisco.
・Accelerating Smart Grid Investments.” World Economic Forum in partnership with Accenture. 2009
・“Accenture Takes its Smart Grid Story on the Road.” Ginger L. Juhl, Accenture.
・“AMD Taps into Sun Utility Grid.” ChannelWeb. September 2006
・“AMR to Smart Grid: Today’s Technology is the Cornerstone for Tomorrow’s Grid.” Utility Automation & Engineering T&D. R. Bryan Seal. July 2009
・“Assuring a Trusted and Resilient Information and Communications Infrastructure.” NDIA Cyber Policy Review, 2009.
・“A Vision for the Modern Grid.” National Energy Technology Laboratory, U.S. Department of Energy Office of Electricity Delivery and Energy Reliability. March 2007
・“Baltimore Gas and Electric Company Unveils Plans for One of the Most Advanced Smart Grid Initiatives in the Nation.” Smart Grid press release. July 13, 2009.
・“Being Explicit about Security Weaknesses.” Robert A Martin, MITRE; Sean Barnum, Cigital; Steve Christey, MITRE.
・“A Belated Spring Makeover for VMware: TechAlpha Research Brief.” George Gilbert and Jurgen Urbanski, TechAlpha
・“Building the Smart Grid.” The Economist June 4, 2009
・“Can the U.S. Government Help Cloud Computing Reach a Tipping Point?” Om Malik. Gigaom. July 23, 2009.
・“Can a New Grid Collaborative Create National Alignment?”. Steve Pullins. SmartGrid News. April 2007
・“The Challenges of Information Assurance.” Miriam Moss, DISA Corporate Communications.
・“Cisco Clarifies its Cloud Computing Strategy: Cisco Won’t Take on Amazon in Cloud.” Stephen Lawson, IDG News Service, June 2009
・“Citigroup signs 30,000-seat deal with Salesforce.com.” Computerworld UK. November 2007
・“Coke’s Largest Bottler Taps Microsoft for SaaS” InformationWeek. July 2008
・“Cloud Computing a ‘Security Nightmare’, Says Cisco CEO.” Robert McMillan. PCWorld magazine. April 22, 2009.
・Cloud Computing: Implementation, Management, and Security. John W. Rittenhouse; James F. Ransome. CRC Press publisher. Copyright 2010

- “Cloud Computing Gains Momentum but Security and Privacy Issues Persist,” GovTech.com.
- “Cloud Computing Security Standards: Evolving from the Classic Data Center Baseline” Booz Allen Hamilton whitepaper
- “Cloud Computing and Virtualization,” David Ayoub, GRD&T Chief Technology Officer, SAIC. October 2009.
- Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration. Jericho Forum. April 2009.
- “Corporate IT. The Long Nimbus.” The Economist. October 2008
- “Diamond High Assurance Security Program: Trusted Computing Exemplar.: Naval Postgraduate School Monterey, California, Department of Computer Science. Irvine, Levin, Dinolt.
- “DOE Labs to Build Science Clouds.” HPC Wire. October 13, 2009.
- “Early Experiments in Cloud Computing.” InfoWorld. April 2008
- “The Energy Web.” Steve Silberman. Wired Magazine. July 2001
- “Federal Information Security Management Act (FISMA) Implementation Project” announcement. NIST website.
- “Federal CIO Vivek Kundra Sees Potential of Cloud Computing.” Mary Hayes Weier. InformationWeek. April 24, 2009.
- “Federal Budget Lays Out Government Cloud Computing Plans.” J. Nicholas Hoover. InformationWeek. May 12, 2009.
- “First-ever Smart Grid Tax Breaks Hitch Ride on Bailout Bill.” Dow Jones International News. Siobhan Hughes. October 9, 2008
- “Global Installed Base for Smart Electricity Meters to Reach 76 Million in 2009.” Press release on ABI Research website. March 2009
- “Google and the Wisdom of Clouds.” Business Week. Stephen Baker. December 13, 2007
- “Google to Deliver Government Cloud to Feds in 2010.” Robert McMillan. ComputerWorld magazine. September 15, 2009
- “Google to Launch Government Cloud.” GovTech.com. September 15, 2009.
- “Google PowerMeter to Track Home Energy Data.” Green Economy Initiative, February 2009.
- “Grid 2030: A National Vision for Electricity’s Second 100 Years.” U.S. Department of Energy; Office of Electric Transmission and Distribution. July 2003
- “GSA Outlines U.S. Government’s Cloud Computing Requirements.” J. Nicholas Hoover. InformationWeek. August 3, 2009

- ‘Guide to Cloud Computing.” InformationWeek. Richard Martin, J. Nicholas Hoover. June 21, 2008
- “How Government’s Driving Cloud Computing Ahead.” John Foley. Network Computing, July 6, 2009.
- “How SOA Could Change the Way You Buy Electricity.” Joanne Cummings. Network World. October 2007
- “IBM Computing on Demand Evolves Toward Cloud Computing Service.” HPC Wire. August 19, 2009
- “Information Assurance Integration into U.S. Pacific Command Exercises.” William Romano and Leigh Bender. IA Newsletter Vol 12 No 4 Fall 2009.
- “Interior developing cloud infrastructure services.” Joab Jackson. Government Computer News, Oct 06, 2009
- “Is Cloud Computing More than Just Smoke?” Martin LaMonica, TrendMicro
- “Jericho Forum and Cloud Security Alliance Join Forces to Address Cloud Computing Security.” Press Release, May 2009
- “Joint Forces Command to test new network encryption.” Amber Corrin. Government Computer News, Sep 01, 2009.
- “Let IT rise: Special Report on Corporate IT.” The Economist. October 23, 2008
- “Lost in the Cloud.” New York Times. Jonathan Zittrain. July 20, 2009
- “New Federal CIO Vivek Kundra wants a Web 2.0 government.” Patrick Thibodeau. ComputerWorld. March 5, 2009.
- “ Major Standards Organizations Collaborate to Further Adoption of Cloud Standards.” Press release: Object Management Group. July 13, 2009
- Managing Software Engineering Knowledge. Aurum, Jeffery, Wholin, and Handzic. Springer publishing.
- “Management Report for Consideration of Smart Grid Investments.” PURPA. February 2, 2009.
- “Meritalk Announces 2009 Cloud Consensus Report: Bringing the Cloud Down to Earth” July 29, 2009
- “Michigan Plans New Data Center and Government Cloud,” Annie Shum. mitcio.com September 3, 2009
- “Move to Cloud Security Accelerates.” Tony Larks, TrendMicro
- National Defense Industrial Association, “Cyberspace Policy Review 2009: Assuring a Trusted and Resilient Information and Communications Infrastructure.” September 2009

・National Institute of Standards and Technology, “Testimony of Patrick D. Gallagher, Deputy Director, NIST before the Committee on Energy and Natural Resources, United States Senate.” March 3, 2009
・“National Electricity Delivery Technologies Roadmap: Transforming the Grid to Revolutionize Electric Power in North America.” U.S. Department of Energy, Office of Electric Transmission and Distribution. January 2004.
・“A National Smart Grid Remains a Vision.” New York Times. October 22, 2009.
・“Navy Experiments With Secure Cloud Computing,” Kevin Jackson blog. August 20, 2009.
・The NETL Modern Grid Initiative: A Vision for the Modern Grid. Conducted by the National Energy Technology Laboratory for the U.S. Department of Energy Office of Electricity Delivery and Energy Reliability. March 2007
・“New Appliances, in Sync with Meters, Shift to Energy-Saver Modes when Told.” Wall Street Journal. September 28, 2009
・“New Federal CIO Vivek Kundra wants a Web 2.0 government.” Patrick Thibodeau. ComputerWorld. March 5, 2009.
・“NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0,” Sept. 2009
・“NSF Awards Millions to 14 Universities for Cloud Computing Research,” HPC Wired, April 23, 2009.
・“NVIDIA RealityServer Propels 3D Cloud Computing Using GPUs.” HPC Wire. October 20, 2009
・“NY Consortium Undertakes Statewide Smart Grid Project.” Smart Grid News. Aug 27, 2009.
・“Obama Administration Launches GSA Cloud Storefront Apps.gov,” GSA press release, September 15, 2009.
・“Obama Outlines Cybersecurity Plans, Cites Grave Threat to Cyberspace. Jaikumar Vijayan. ComputerWorld. May 29, 2009.
・“Obama Putting $3.4 billion Toward Smart Power Grid.” Associated Press. October 27, 2009
・“Overcoming Obstacles to Smart Grid Future.” SolveClimate. Laura Shin. May 2009.
・“Pacific Northwest National Laboratory aims to empower utility customers.” IBM. September 17 2009.
・“Peco, PSE&G debut 'smart-meter' plans.” Philadelphia Inquirer. Aug. 7, 2009
・Perfect Power: How the Microgrid Revolution will Unleash Cleaner, Greener, and More Abundant Energy. Robert Galvin and Kurt Yeager. McGraw Hill publisher.

- Report to NIST on the Smart Grid Interoperability Standards Roadmap. June 17, 2009
- “Report of the Illinois Smart Grid Initiative.” April 2009.
- “The Role of Defense Science and Technology in Software for the Warfighter.” CHIPS - The Department of the Navy Information Technology Magazine. Jan-Mar 2005
- “Securing Microsoft’s Cloud Infrastructure.” Azure Services Platform Center. May 2009
- “The Security Vulnerabilities of Smart Grid.” Jude Clemente, Energy Security Analyst with the Homeland Security Department at San Diego State University. June 18, 2009
- Security Guidance for Critical Areas of Focus in Cloud Computing. Prepared by the Cloud Security Alliance. April 2009
- “The Security Vulnerabilities of Smart Grid.” Jude Clemente, Energy Security Analyst with the Homeland Security Department at San Diego State University. June 18, 2009
- “Service Level Agreements in Service-Oriented Architecture Environments.” Software Engineering Institute, Carnegie Mellon University. September 2008
- “SGMM: First Annual Report on Smart Grid Implementation.” Software Engineering Institute Carnegie Mellon University.
- “Smart Grid: The Road Ahead.” Larry Sollecito. GE Digital Energy
- “Smart Grid and The Cloud: Why are They Linked?” by Mark Thiele, VMWare. June 2009
- “Smart Grid Security.” Government Security News. June 15, 2009.
- “Smart Grid Security Requirements Released,” Government Technology. March 16, 2009.
- “The SmartGrid: An Introduction.” U.S. Department of Energy. Litos Strategic Communications.
- “Smart Meter, Dumb Idea?” Wall Street Journal. April 27, 2009.
- “A Smart Recloser for Smart Grid.” Nick Carlson; Hauker Asgeirsson, DTE Energy. Transmission & Distribution World. June 2008
- “Software Assurance Landscape.” U.S. Department of Homeland Security, January 2009. Preliminary draft.
- “The software needs of the Smart Grid,” MBT Magazine. October 22, 2009
- “Software Security Assurance.” State-of-the-Art (SOAR) Report. Information Assurance Technology Analysis Center and Data and Analysis Center for Software. July 2007
- “Software as a Service Threatens Partner Revenue and Profit Streams, New Partners Emerging, IDC Research Shows.”

- “SoS Navigator 2.0: A Context-based Approach to System-of-System Challenges.” SEI SoS Navigator Team. June 2008
- “Stimulus Funds Speed Transformation Toward Smart Grid.” Wall Street Journal. September 28, 2009
- The Strategic Plan 2009-2014. Federal Energy Regulatory Commission
- “Suggested Practices for Avian Protection on Power Lines: The State of the Art in 2006” Edison Electric Institute.
- “Sun Expands Network.com On-Demand Application Offerings.” February 2008.
- “Systems Security Engineering: A Critical Discipline of Systems Engineering.” Kristen Baldwin. July 2009.
- “System-of-Systems Navigator: An Approach for Managing System-of-Systems Interoperability.” U.S. Department of Defense; Software Engineering Institute, Carnegie Mellon University. April 2006
- “Unisys and Cloud Computing: Exclusive Interview with Rich Marcello.” Cloud Computing Journal. July 2009
- The U.S. Smart Grid Revolution: KEMA’s Perspectives for Job Creation. January 13, 2009.
- “U.S. Stimulus Critical for Smart Grid Industry.” Forbes magazine. David Lawsky. February 17, 2009
- U.S. Department of Energy, Smart Grid System Report. July 2009
- What the Enterprise Needs to Know about Cloud Computing. Accenture Technology Labs. 2009
- “What the Smart Grid Means to America’s Future.” DOE. DE-AC26-04NT41817, Subtask 500.01.02
- “Where the Cloud Meets the Ground.” The Economist. October 23, 2008
- “White House Mulls Making NASA a Center for Federal Cloud Computing.” NextGov.com Aliya Sternstein July 24, 2009
- “Why cloud computing is still a red herring.” Michael DaConta. Government Computer News. September 2009.
- “Wiser Wires.” The Economist October 8, 2009
- “Workday: The Next Software Power?” Business Week. August 2008
- “Xcel launches Boulder as first ’smart grid’ city.” Denver Business Journal. September 8, 2009.
- Presentations at the November 2009 Software Assurance Forum
- Philip Reitinger, DHS, Deputy Undersecretary of the Department’s National Protection and Programs Directorate
- Mitch Komaroff, Director, Globalization Task Force, OASD/NII

- Julie Deger, VAO/NSA
- Donna Dodson, Deputy Chief Cybersecurity Advisor NIST
- Paul Lewis, UK National Archives
- Dan Wolf, President, Cyber Pack Ventures
- Patrick Arnold, CTO, Trustworthy Computing, Microsoft
- Lou Kratz, Vice President, Focused Logistics, Lockheed Martin
- Ron Ritchey, Principal, Booz Allen Hamilton
- Warren Axelrod, Executive Advisor, Financial Services Technology Consortium
- John Weinschenk, CEO, Cenzic
- Lynn Penn, Director, Program Process Management, Lockheed Martin
- Jeffrey Ritter, Attorney, Waters Edge, LLC
- David White, Sr. Member Technical Staff, CERT Software Engineering Institute, Carnegie Mellon University
- Janne Uusilehto, Head of Nokia Product Security, Nokia and Vice Chair of SAFECode
- Mike Kass, Computer Scientist, NIST
- John Gilligan, President, Gilligan Group and Advisor to President Barack Obama
- Bruce Weimer, Software Engineering Center Software Assurance Division, U.S. Army
- Djenana Campara, Chief Executive Officer, KDM
- Todd Landry, Sr Product Manager, Klocwork
- Sean Barnum, Director of Knowledge. Management, Cigital
- Dr. Vehbi Tasar, Manager of Professional Programs, ISC2
- Alan Paller, Director of Research, SANS Institute
- Robert Seacord, Senior Vulnerability Analyst, SEI/CERT
- David Stender, Associate CIO Cyber Security, CISO, IRS
- Jim Molini, Security Professional, Microsoft
- Ian Brown, Senior Associate, Booz Allen Hamilton
- Bert Miuccio, Vice President, CIS
- Cheryl Jones, Software Engineer, US Army ARDEC
- Thomas Rhodes, Computer Specialist, NIST
- Shari Pfleeger, Sr. Scientist, Rand
- Dan Reddy, Consulting Product Manager in the Product Security Office, EMC
- Matt Coose, NPPD Federal Network Security (FNS) Director, Department of Homeland Security
- Bob Dix, Vice President of Government Affairs & Critical Infrastructure Protection, Juniper Networks
- Hart Rossman, Vice President and Chief Technology Officer for Cyber Programs, SAIC
- Michael Brown, CISO, FAA

・Kenneth Hong Fong, CTO, Office of the Under Secretary of Defense for. Acquisition, Technology and Logistics (OUSD(AT&L)
・Marirose Ziebarth, Associate, Cyber Security Education/Training, Booz Allen Hamilton
・Linda Wilbanks, Chief Information Officer for the National Nuclear Security Administration
・Guy Copeland, President of IT Information Sharing, CSC
・Lawrence Hale, Chief Technology Officer & Director of the Office of Infrastructure Optimization for Integrated Technology Services, GSA
・James Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies
・Matt Moynahan, CEO, Veracode
・Dave Waltermire, NIST, SCAP
・James Q. Chen, Professor and Program Director of Information Technology, UMUC
・John Streufert, Deputy Chief Information Office for Security, Department of State
・Andras Szakal, Distinguished Engineer and the Chief Software IT Architect for the Federal Software Group, IBM

主な民間部門のインタビュー先

・Department of Homeland Security Joe Jarzombek, Director of Software Assurance, National Cyber Security Division
・CERT Software Engineering Institute, Carnegie Mellon University Carol Woody, Senior Member of Technical Staff
・MITRE Bob Martin, Principal Software Systems Engineer
・Booz Allen Hamilton Michele Moss, Associate
・Idaho State University Dr. Corey Schou, Professor of Information Systems
・OASD/NII Don Davidson, ICT-SCRM Specialist for the Globalization Task Force
・Booz Allen Hamilton Stan Wisseman, CISSP, CISM, Sr. Associate
・EMC Spencer Brown
・Citigroup Chii-Ren Tsai, Sr. Vice President, IT Risk & Program Management
・LDRA Jeff Price, Senior Regional Sales Manager
・Intel Jeffrey Cohen, Director of Validation, Manageability & Platform Software Division
・CERT Software Engineering Institute, Carnegie Mellon University Lisa Young, Senior Member Technical Staff

・Artisan Software Tools Matthew Hause, Chief Consulting Engineer
・Microsoft Vince Menzione, General Manager, Partner Organization & Strategy
・Microsoft Susie Adams, Federal CTO
・Salesforce.com Mark Regan, Technical Sales Engineer
・Long Island Power Authority Dr. Predrag Vujovic, Director of Technology & Development Planning
・Extreme Networks Vish Nandlall, CTO
・SAFECode Paul Kurtz, Executive Director
・Demand Response and Smart Grid Coalition Dan Delurey, Executive Director
・Exelon Corporation Jeffrey Barnett, Manager, Corporate Development
・CompuSearch Software Systems Carole Dicker, Director, Information Assurance
・Accenture Paul Daugherty, Chief Technology Architect
・Sun Microsystems Hal Stern, Vice President, Global Systems Engineering