米国の電力セクターにおけるサイバーセキュリティについて

米国の電力セクターでは、現在様々な課題が検討されているが、その中でも電力網（グリッド）の近代化は、連邦政府、州政府、電力業界が最も注目しているテーマの一つである。最近では、9 月 27 日に（米国）エネルギー省が初めて「4 年ごとの技術検討報告書（QTR）」を発行し、米国における電力網の近代化を同省のエネルギー技術計画の 2 つの最優先事項のうちの 1 つとして挙げている（もう1つは先進自動車技術）。

電力網の近代化には、各種スマートグリッド技術、エネルギー貯蔵技術、その他多数の技術を含む、多様な課題がある。一般的な分野では、近代化プロセスの主要な側面として、米国のグリッド内のサイバーセキュリティの確保に関する問題に政府と業界の両方からの関心がますます高まっている。米国の電力網（およびエネルギーセクター全般）のサイバーセキュリティに対する政府の取り組みは進展し続けており、連邦および州レベルで様々な機関やプログラムへと発展している。最近の取り組みとしては、次のものが挙げられる。

- 2011 年 9 月 15 日、エネルギー省（DOE）は、「エネルギー供給システムにおけるサイバーセキュリティ確保のための 2011 年ロードマップ」を発表した。このロードマップは、DOE の「エネルギーセクターにおける制御システムのセキュリティ確保のための 2006 年ロードマップ」の改訂版である。2011 年版では、業界、ベンダー、学界、政府関係者が安全なエネルギー供給システムを開発していくための、今後 10 年間にわたる戦略的枠組みの概要が示されている。

- また、2011 年 9 月、DOE は、国立標準技術研究所（NIST）、北米電力信頼度協議会（NERC）と連携して「電力業界におけるサイバーセキュリティリスク管理ガイドライン」の草稿を発表し、意見公募を行っている。同ガイドラインは、米国の電気事業者が全組織レベルでサイバーセキュリティリスクを管理するための方法を提供する。DOE は 2011 年 10 月 28 日まで同ガイドラインに対する一般からの意見を受け付けている。

- さらに 9 月 15 日には、米国連邦エネルギー規制委員会（FERC）が、電力網における「重要インフラ保護（CIP）の信頼性基準」に関する規則制定案の告示を行った。これは、北米電力信頼度協議会（NERC）が開発し、FERC へ提出したものである。

米国政府のサイバーセキュリティに関するさらなる取り組みの詳細を以下に説明する。この分野は成長市場であり、米国内の外国企業を含む多様なベンダーにおいて投資対象となっている。

1. エネルギーセクターのサイバーセキュリティに関する米国政府のアプローチの背景

電力セクターを対象とした米国政府のサイバーセキュリティ政策は、重要インフラ保護（CIP）の一般的な問題に対処する連邦法、規制、政策、および大統領令などに基づいて、過去 10～15 年の間に発展してきた。この分野の主要政府機関は国土安全保障省になる。

1） 大統領令第 63 号（PDD-63）

- 1998 年 5 月 22 日発行の大統領令第 63 号（PDD-63）が、重要インフラ保護とサイバーセキュリティに関する連邦政府のアプローチの基盤となっている。概して、PDD-63 には保護が必要な重要インフラが記載されており、具体的には次の項目が挙げられている。

情報とコミュニケーション、銀行・金融、水道、運輸（航空、高速道路、公共交通、パイプライン、鉄道、水上輸送など）、緊急時法執行サービス；緊急消防隊と政府の継続性；公共医療サービス、電気・石油・ガスの生産と貯蔵。

- PDD-63 はまた、各重要インフラを主導する機関を特定している。エネルギーセクターの主導機関は、エネルギー省になる。主導機関は民間セクターとの協力活動に関する責任を負う。公共・民間セクターは、協力してインフラの脆弱性を評価し、脆弱性を除去するシステムを提案する計画を策定する義務がある。

- サイバーセキュリティに関しては、同大統領令により、連邦政府と重要インフラの民間所有者が重要インフラとサイバー攻撃に関する情報を共有・分析することを目的とした情報共有分析センターが設立された。現在、同センターの任務の大半は、米国コンピューター緊急事態対応チーム（US-CERT）が担っている。

2） 2002 年国土安全保障法

9・11 同時多発テロ事件を機に、2002 年 11 月 22 日に「2002 年国土安全保障法」が制定された。同法により、国土安全保障省（DHS）が設立され、サイバーセキュリティを含め、重要インフラの保護に関する責務全般が DHS に課されている。

- 2003 年 2 月、ホワイトハウスは「サイバーセキュリティ国家戦略」を発表した。これには、次のものを含む DHS の責務が記載されている。

①重要インフラおよび主要リソース（CIKR）の保護を目的とした全国計画の開発、②情報システムが攻撃を受けた際の危機管理の実施、③情報システム障害時の公共・民間セクターへの技術サポート提供、④州・地方政府および民間セクターへの警告情報の提供、⑤国土の安全確保のための技術研究への資金提供。

3） 国土安全保障に関する大統領令第 7 号（HSPD-7）

- 2003 年 12 月 17 日、ブッシュ前大統領は「国土安全保障に関する大統領令第 7 号（HSPD-7）」を発行した。HSPD-7 により、PDD-63 は廃止された。HSPD-7 に準じ、DHS は、重要インフラおよび主要リソース（CIKR）の特定、優先順位付け、保護を目的とした活動を統合する義務を負う。HSPD-7 は、エネルギー省をはじめ、分野専門ごとに連邦政府機関の役割を定めている（エネルギーセクターには石油、ガス、電力の精製、生産、貯蔵が含まれる）。

- HSPD-7 に準じ、DHS は 2006 年に「国家インフラ保護計画（NIPP）」を発行した。これは 2009 年に改訂され、次の 18 項目が 2009 年 NIPP の対象となる重要インフラに指定されている。

農業・食糧、軍事産業基盤、エネルギー、医療・公衆衛生、国家的記念建造物・象徴物、銀行・金融、水道、化学薬品、商業施設、重要製造業、ダム、救急サービス、原子炉・核物質・核廃棄物、情報技術、コミュニケーション、郵便・運送、交通システム、政府施設。

NIPP は、連邦政府の各部門や州・地方政府、および民間セクターが CIKR を特定し保護するための枠組みを提供する。

- 各セクターについて、民間セクターとの調整協議会（電力では NERC）、セクター別管轄機関（電力ではエネルギー省）、および政府調整協議会が設立されている。

4） エネルギーセクター計画（SSP）

2007 年 5 月、エネルギー政府調整協議会（DHS および DOE 主導）は電気・石油・天然ガスセクターの調整協議会（電力の NERC を含む）と連携し、国家インフラ保護計画への提言として、エネルギーセクター計画（SSP）を策定した。SSP の改訂版が 2010 年に発表された。

5） 2009 年サイバースペース政策見直し

オバマ大統領は就任後、60 日間でサイバー政策を総合的に見直し、「米国のサイバーセキュリティに関する政策と構造を審査する」よう指示した。レビュー結果は、2009 年 5 月 29 日に発表された。全体として、オバマ政権は、前政権の政策および組織をそのまま保持している。「2009 年サイバースペース政策見直し」の結果により、ホワイトハウス高官として、連邦政府全体のサイバーセキュリティ政策および企画を担当するサイバーセキュリティ調整官を設置することが決定された。

2. 電力セクターのサイバーセキュリティに関する連邦政府機関の役割

米国の電力セクターのサイバーセキュリティへの取り組みに関する主要政府機関には、北米電力信頼度協議会（NERC）、国立標準技術研究所（NIST）、米国連邦エネルギー規制委員会（FERC）、エネルギー省（DOE）がある。

1) 北米電力信頼度協議会(NERC)

NERC:「2005 年エネルギー政策法(EPAct 2005)」により、米国初の電力信頼性機関(ERO)が認可された。ERO の概念は、米国通信システムのユーザー、所有者、プロバイダーすべてに対し、電力の信頼性に関する義務的な規制を執行する独立した自主規制機関として機能するというもの。産業主導型の任意団体として 1960 年代より活動してきた NERC は、米国連邦エネルギー規制委員会(FERC)の認可を受け、2007 年 1 月より ERO として活動している。

NERC は、重要インフラ保護(CIP)政策を支持し、基幹電力系統の物理的およびサイバー上のセキュリティ向上に向けての取り組みを調整する。これらの取り組みには、規格開発、コンプライアンスの実施、リスクアセスメントおよびリスクに対する準備、警告の発信による業界への重要情報の普及、主要課題に対する認識の向上などが含まれる。

- 前述のとおり NERC は、米国政府の重要インフラ保護計画において、電力セクター「業界」を代表する存在である。NERC の重要インフラ保護委員会(CIPC)の執行委員会は、大統領および NERC の CEO と共に電力セクター調整協議会として機能し、電力セクターの重要インフラとセキュリティに関する問題について、エネルギー省(DOE)および国土安全保障省(DHS)と連携する。

- NERC は様々な業界向けのセキュリティガイドラインを開発し、制御システムのセキュリティ、ファイアウォール、侵入検知、アクセス制御などの問題に対処している。2008 年、NERC の開発した重要インフラ規格が FERC より承認された。これらの規格により、基幹電力系統の運用およびサポートに必要な電子情報交換の安全性を確保し、重要サイバー資産への物理的および電子的な不正アクセスを阻止するための要件が確立された。

これらの規格は、基幹電力系統の特定のユーザー、所有者、プロバイダーに対し、制御システムへの物理的・電子的アクセスの保護、重要サイバー資産の保護、セキュリティ関連業務に従事する人員の訓練、セキュリティ事故の報告、サイバー事故発生時の復旧対策を実施するためのセキュリティ方針、計画、運用手順を確立するよう義務付けている。

しかし、前述のとおり、この分野における NERC の活動は NIST や DOE、FERC などの政府機関と合同で行われるため、今後も進化していくと考えられる。例えば、2010 年 11 月に NERC は、電力サブセクター調整協議会(ESCC)の「重要インフラ戦略ロードマップ」を承認した。このロードマップは、非常に深刻なサイバーリスクを含め、顧客への電力供給に深刻な混乱をもたらすリスクを特定するための枠組みを提供するとともに、信頼性と復元力を強化するために必要な活動を推進している。(詳細については、以降のセクション 4.を参照。)

2) 国立標準技術研究所(NIST)

NIST:「2007 年エネルギー自給・安全保障法(EISA)」により、国立標準技術研究所(NIST)は、ス

マートグリッドシステムおよびネットワークの相互運用性などの確保を目的とした枠組み開発を調整するよう指示された。

- その活動の一環として NIST は、これらのシステムやネットワークの安全性を確保するためのサイバーセキュリティ規格の策定を行っている。2009 年 3 月、NIST は、各団体（公共事業、機器製造業者、規制機関など）向け開発ガイドラインの作成などを目的とした、スマートグリッドのサイバーセキュリティに関する作業部会を設立した。

- 2010 年 1 月 19 日、NIST は「フレームワークおよびロードマップ」を発行し、重要な規格のリスト、サイバーセキュリティの一次戦略、および米国スマートグリッドの開発をサポートするその他の枠組みに関する情報を公表した。
- 2010 年 9 月 2 日、NIST は、「スマートグリッドのサイバーセキュリティに関するガイドライン（NISTIR 7628）」の第 1 版を発行した。

NIST の活動は現在も進行中であり、電力研究所、グリッドワイズ・アーキテクチャ協議会、全米電気機器製造業者協会、米国電気電子学会（IEEE）、NERC などを含む様々な利害関係者と連携して行われている。（詳細については、以降のセクション 3.を参照。）

3) 米国連邦エネルギー規制委員会（FERC）

FERC：電力システムの主要規制機関である米国連邦エネルギー規制委員会（FERC）は、グリッドの安全性を確保するために必要と考えられる規格（NERC や NIST の活動の一環として認定されるもの）を採択する。

4) エネルギー省（DOE）配電・電力信頼性局（OE）

DOE：DOE の配電・電力信頼性局（OE）は、電力網の近代化およびインフラの安全性と信頼性の向上を目指す連邦政府の取り組みで DOE を主導する部門である。NIST、NERC、FERC は主に規格・規制の開発に重点を置いているが、DOE の OE は、サイバーセキュリティに関する各種技術の研究開発とテストに重点を置いている。例えば、OE はサイバーセキュリティを支援する次の活動を行っている。

- 安全で復元力のある電力インフラを構築するための先進技術の研究開発への資金提供
- サイバーセキュリティの向上を目指したリスク管理のベストプラクティスおよび戦略の促進
- DOE のテストプログラムへの支援（DOE のナショナル SCADA テストベッド〈NSTB〉計画など）
- 電力セクターにおけるサイバーセキュリティ要員の強化・増員

詳細については、セクション 5.を参照。

3. NIST による規格開発

前述のとおり、NIST の主な役割は、スマートグリッドの相互運用性規格とサイバーセキュリティ規格の開発の調整である。NIST の活動は現在も進行中であり、電力研究所、グリッドワイズ・アーキテクチャ協議会、全米電気機器製造業者協会、米国電気電子学会(IEEE)、NERC などを含む様々な利害関係者と連携して行われている。

- 2010 年 10 月 13 日、NIST は FERC に対し、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「基本」となる 5 規格の策定が終了し、連邦および州のエネルギー規制機関による検討を受ける準備ができたと報告した。この規格は、国際電気標準会議(IEC)が作成したもので、効率的で信頼性の高いグリッドの運用およびサイバーセキュリティにとって重要な情報モデルおよびプロトコルに重点を置いている。この規格とその機能は次のとおりである。

* IEC 61970 および IEC 61968:主に送電(IEC 61970)および配電(IEC 61968)ドメインにおける、デバイスとネットワーク間でのデータ交換に必要な共通情報モデル(CIM)の提供。
* IEC 61850:変電所の自動化および通信、ならびに共通データフォーマットによる相互運用性の促進。
* IEC 60870～6:制御センター間の情報交換の促進。
* IEC 62351:上記の IEC 規格により定義された通信プロトコルに関するサイバーセキュリティの検討。

1) FERC の懸念

ただし FERC は、2010 年 10 月に NIST が提示した「基本」の 5 規格に関する規則制定を現時点では見送ることにした。

- NIST が規格を特定した後、FERC は、全米公益事業規制委員協会(NARUC)などの利害関係者と合同で会議を招集し(2010 年 11 月と 2011 年 1 月)、今後の取り組みについて討議を行った。これらの会議により、この問題に対する業界のコンセンサスに関する疑問が浮上した。FERC はまた、より多くの意見を求めるため、2011 年 2 月に「意見募集に関する補足通知書」を発表した。基本的に FERC は、現時点では規則制定作業を進めるには「コンセンサスが不十分である」という決断に達した。

- FERC は決断の根拠として、サイバーセキュリティの欠陥や「早計に個々の規格を採用することにより意図しない結果が生じる」可能性などの懸念を挙げている。

- それと同時に FERC は、NIST に対する決断を否定的に捉えられないようにするため、FERC が

NIST の標準規格への取り組みを強く支持する姿勢は変わらないと強調している。当初、米国では NIST のスマートグリッド標準規格への取り組みに対し、非常に遅すぎる、綿密さに欠けるなど批判の声が多かった。それにも関わらず FERC は、NIST における継続的なスマートグリッドへの取り組み強化、特にスマートグリッド相互運用性パネル（SGIP）の強化について高く評価している。FERC はまた、スマートグリッドの利害関係者（公共事業、機器製造業者、政府規制機関など）に対し、NIST の作業に「積極的に協力」するよう促している。

2） NIST による 6 つの標準規格

－2011 年 7 月 26 日、NIST は、スマートグリッド関連技術の新しい標準規格カタログに最初の 6 規格をエントリーしたと発表した。これら 6 規格はすべて SGIP の理事会により承認済みで、SGIP メンバーの 90%以上が承認している。これらの 6 規格は、NIST の 19 の優先行動計画（PAP）のうち、SGIP がスマートグリッドが適正に機能するうえで早期対応が最も必要だと考える 5 つの問題に対応している。これらの規格は以下に対応している。

＊ デバイスの情報交換に使用されるインターネットプロトコル標準
＊ 利用者が特定の時点でのエネルギー使用料を把握できるようにするための、エネルギー使用量情報の基準
＊ 電気自動車の電源接続を確保するために必要な充電スタンドの基準
＊ 電力負荷の大きいプラグイン自動車がグリッドに過度の負担をかけないようにするための、プラグイン自動車とグリッド間のコミュニケーションのユースケース
＊ 家庭用電力量計をスマートメーターにアップグレードするための要件
＊ グリッドの通信に必要なワイヤレス通信機器で、携帯電話などの一般的なデータ通信機器に比べて信号の遅延や中断に対する許容度の低いワイヤレス通信機器の標準規格審査に関するガイドライン

NIST は 2011 年夏に発表した 6 つの新しいスマートグリッド標準規格において、以下の内容を公式声明で強調しているが、その根拠の 1 つには、2010 年 10 月に提示した標準規格の開発があると考えられる。

①6 つの標準規格はすべて SGIP の理事会の承認を得ており、SGIP メンバーの 90%以上からも承認を得ている（コンセンサスを強調）
②SGIP は 675 の公共・民間団体と、1,800 名近くの個人メンバーを有し、さらに統合的な「コンセンサスベースのグループ」になりつつある（プロセスの広範性を強調）

また、NIST は 2011 年 9 月 13 日、欧州連合（EU）のスマートグリッド調整グループ（SG-CG）と共同でスマートグリッド標準規格の開発を開始したと発表した。

- SG-CG は、 欧州標準化機構(CEN)、欧州電気標準化機構(CENELEC)、欧州電気通信標準化機構(ETSI)の 3 つの民間セクターの標準化機構を代表している。

- サイバーセキュリティ要件や技術情報を含む、定期的な情報交換の推進を目的としている。

4. FERC と NERC による重要電力セクターインフラの定義に関する最近の開発

1) 重要インフラ保護(CIP)信頼性基準

前述のとおり、FERC は 9 月 15 日、米国の基幹電力系統で重要なサイバー資産を特定する新手法を含む、8 つの重要インフラ保護(CIP)信頼性基準について再検討を行うよう提案した。

- FERC は、提案した CIP 標準規格「バージョン 4」について、米国電力業界と NERC がサイバーセキュリティ事故に耐えうるグリッドを確保するための統合的なアプローチを開発する上での暫定的なステップだと述べている。

- 新規格は、既存のリスクベースの評価方法に取って代わるもので、重要資産を均一で「明確な」17 の基準により特定する。また、重要資産を特定する際の自由裁量の余地を制限することで、プロセスの一貫性と明確性を向上させる。

FERC の規則案決定の通知(NOPR)では、2008 年 1 月に元の CIP 標準規格を承認した FERC の命令 706 で指示された変更事項について、NERC はすべてに対応できていないと指摘している。

- NOPR では、NERC は 2012 年第 3 四半期末までに命令 706 に準拠する規格を提出するよう求めている。

- 提案規則へのコメント(RM11-11)の期限は、官報発行後 60 日以内である。

2) FERC と NERC の意見相違

前述のとおり、信頼性に関する規則の施行可能な範囲と領域に関して NERC と FERC の間にはある程度の意見の相違がある。2005 年エネルギー政策法(EPACT)に基づき、NERC は、信頼性規格を制定する義務がある。しかし、これらの規格は FERC の承認を得なければならない。

- 過去数年にわたり FERC は、より積極的に信頼性規格を施行するよう NERC に圧力をかけてきた。FERC はまた、NERC は、信頼性規格の適用対象となる「重要インフラ」と見なされる電力系統機器を決定する際に、許容範囲が広すぎるのではないかと示唆している。

- サイバーセキュリティ分野については、どの機器を重要インフラと考えるかについて FERC と NERC の見解が異なっている。

例えば、FERC の新しい提案によると、1,500 メガワットを超える発電能力を有する単一施設にはサイバーセキュリティ規定が厳格に適用される。さらにこの提案では、500 キロボルト(kV)以上のすべての送電施設および 300kV 以上の特定の送電施設、すなわち他施設と無数の相互接続を行う送電施設は、サイバーセキュリティを目的とした重要インフラであると定義している。

5. 電力・エネルギーセクターのサイバーセキュリティに関する DOE の取り組み

1) サイバーセキュリティ確保のための 2011 年ロードマップ

2011 年 9 月 15 日、エネルギー省(DOE)は、「エネルギー供給システムにおけるサイバーセキュリティ確保のための 2011 年ロードマップ」を発表した。同ロードマップは、DOE の「エネルギーセクターにおける制御システムのセキュリティ確保のための 2006 年ロードマップ」を改訂したものである。2011 年版では、業界、ベンダー、学界、政府関係者が安全なエネルギー供給システムを開発していくための、今後 10 年間にわたる戦略的枠組みの概要が示されている。

同報告書は、DOE のエネルギーセクターにおける制御システムに関する作業部会(ESCSWG)が作成した。作業部会は、以下の企業・団体の代表により構成される。

- アリエスカ・パイプライン
- BP
- エネルギー省、配電・電力信頼性局
- 米国国土安全保障省、国家保護およびプログラム局
- 米国国土安全保障省、科学技術局
- エジソン電気協会
- エル・パソ社
- テキサス電気信頼性評議会
- エルゴン・リファイニング社
- 米国連邦エネルギー規制委員会
- オンタリオ卸売電力市場
- 北米電力信頼度協議会
- プログレス・エナジー社

概して、これは非常に「トップレベル」の報告書であり、次の項目に関する戦略計画の概要が述べられている。

- エネルギーセクターにおける「セキュリティ文化」の構築

- 業界内でのリスクの評価および監視
- リスク削減に向けての新しい保護方法の開発と実施
- 事故の処理
- セキュリティの持続的改善

このロードマップは、ESCSWG と電力サブセクター調整協議会（ESCC）、石油・天然ガスセクターの調整協議会、エネルギーの政府調整協議会（DOE および DHS）との協力により、DHS の重要インフラセキュリティ諮問委員会（CIPAC）の枠組みの下に作成された（1.に記載）。

2) DOE による具体的な取り組み

より具体的な取り組みについては、DOE の配電・電力信頼性局（OE）が DOE を主導し、米国エネルギーセクターにおけるサイバーセキュリティ強化を目指している。DOE の OE は様々な活動を行っているが、サイバーセキュリティ分野では主に各種技術の研究開発、テスト、およびサイバーセキュリティに関する技術評価、ベストプラクティス、ガイドラインの作成に重点を置いている。例えば、次の活動が挙げられる。

①- DOE は、2009 年 11 月、DHS および 5 大学（コーネル大学、ダートマス大学、カリフォルニア大学デーヴィス校、イリノイ大学アーバナ・シャンペーン校、ワシントン州立大学）と共同出資した 1,880 万ドルを TCIPG（電力網のための信頼できるサイバーインフラ）プログラムに投じると発表した。このプログラムは、主に米国国立科学財団により資金提供を受けていた以前の研究を活用し、発展させることを目的としている。

②- DOE の OE はまた、米国再生・再投資法（ARRA）に準じ、各 DOE 賞の 45 億ドルを監督しており、米国全土にわたって 100 以上のスマートグリッドへの投資および実証プロジェクトを支援している。プロジェクトの受賞者は、サイバーリスク評価、軽減策、デバイスやベンダー選定時のサイバーセキュリティ基準、プロジェクトが準拠する関連標準規格やベストプラクティスを含む、サイバーセキュリティ計画の開発と実施に尽力している。

③- DOE の OE はナショナル SCADA テストベッド（NSTB）計画も監督している。この計画は、SCADA（監視制御とデータ収集）や制御システムの脆弱性に関する問題の特定および解決、新規および既存の設備のテスト、安全な設計や技術進歩の発展において、エネルギーセクター（電気、石油、天然ガス）を支援する国家的リソースとしての機能を果たしてきた。NSTB は複数の研究所のパートナーシップから成り、アルゴンヌ、アイダホ、オークリッジ、パシフィック・ノースウエスト、サンディアの各国立研究所の専門知識やリソースを活用している。

NSTB では様々な活動を行っており、これまでに制御システムおよびコンポーネントにおける 37 のサイバー脆弱性アセスメントを完了している（アイダホ国立研究所（INL）が実施）。現在までに、

14のベンダーコンポーネントと15のベンダーシステムの実験的評価、資産所有者のシステム上での 8 のオンサイトアセスメントを実施している。

④- レムノス相互運用セキュリティプロジェクトでは、DOE が費用の一部を負担し、異なるベンダー間で運用される 2 つの制御システムネットワーク間で安全な通信チャネルを作成するための相互運用可能な構成プロファイルの開発と実証が行われた。ガレット・コム、インダストリアル・ディフェンダー、N-ディメンション、フエニックス・コンタクト、ラグド・コム、シュヴァイツァー・エンジニアリング・ラボラトリーズ、シーメンスなどのベンダーがテストを実施し、レムノスプロファイルを使用した相互運用性の公開実証実験を行った。このプロファイルは、サンディア国立研究所の「相互運用可能な設計のためのオープン PCS アーキテクチャ（OPSAID）」プロジェクトに基づいて構築されており、UCA 国際ユーザーグループ（UCAIug）配下のオープンスマートグリッド（OpenSG）セキュリティ作業部会タスクフォースの基盤として承認されている。

⑤- INL はこれまでに2,300名以上のオペレーターおよびその他の利害関係者のトレーニングを実施しており、NERC 認定の 2 コースを含む、DOE および DHS の提供する初級、中級、上級レベルのセキュリティ関連コースを実施している。これらのコースにより、脆弱性や攻撃メカニズム、運用上の問題に関する認識を向上させている。 これまでに電気、石油、天然ガスのサブセクターのエネルギー供給会社を代表して 224 名以上が、1 週間にわたるクラスルーム形式のコースや、上級トレーニングでの終日チーム演習に参加した。これらのコースは、参加者が各自の施設に持ち帰って利用できるようなセキュリティ技術を提供するよう設計されている。

⑥- スマートグリッドの高度セキュリティ促進プロジェクト（ASAP-SG）は、北米電力会社と DOE による公共民間共同プロジェクトで、これにより先進的メータリング・インフラ（AMI）用と第三者のデータアクセス用の 2 つのセキュリティプロファイルがリリースされた。AMI プロファイルは、AMI ソリューションの開発と実装を行う組織にガイダンスとセキュリティ管理を提供する。AMI プロファイルは 2009 年 12 月に UCAIug 内の AMI セキュリティ（AMI-SEC）タスクフォースによって採択・承認され、AMI-SEC は 2010 年 6 月にバージョン 2.0 を発表した。ASAP-SG の AMI プロファイルによって AMI-SEC の作業は促進され、わずか 1 年以内にドキュメントの作成開始から承認、バージョン 2.0 のリリースまで達成することができた。AMI プロファイルは、国立標準技術研究所（NIST）のサイバーセキュリティ作業部会が NIST 内部機関報告書（NISTIR）7628「スマートグリッドのサイバーセキュリティに関するガイドライン」（前述）を作成する際の参考資料として使用された。

⑦- 2010 年、DOE は、EnergySec、電力研究所（EPRI）と共に 1,650 万ドルを投資し、電力セクターのサイバーセキュリティに関する 2 つの機構、NESCO と NESCOR を設立すると発表した。

⑧- NESCO（米国電力セクター・サイバーセキュリティー機構）は EnergySec の主導により、サイバ

一関連の脅威についてデータ分析と科学調査を行い、電力システムの信頼性向上に努める。また、グリッド信頼性の問題を特定し、対応準備を行うためのフレームワーク作成支援、国内外の電力セクター関係者との情報、ベストプラクティス、リソース、ソリューションの共有、電力セクターの主要サプライヤーおよびベンダーへのサポートや交流の促進も行っている。

⑨- NESCOR（米国電力セクター・サイバーセキュリティー機構リソース）は EPRI の主導により、サイバーセキュリティ要件、結果、標準規格の分析を評価するとともに、研究所でのセキュリティ技術実験およびパイロットプロジェクトにおいて NESCO を支援する。

⑩- 2011 年 2 月、DOE は、NIST および NERC との協力により、サイバーセキュリティのリスク管理プロセスガイドラインを開発し、電力セクターの組織がサイバーセキュリティリスクを予防管理できるような一貫したプロセスを提供する、公共民間セクター共同研究を開始した。このリスク管理プロセス（RMP）は NIST 特別刊行物 800-39『情報セキュリティリスクの管理：機関、目標、情報システムの概観』を基盤としている。ただし、このガイドラインは、特に電力セクターに適用され、適切な場合はその他の標準規格やガイドライン、ベストプラクティスを活用するために開発されたものである。RMP はガイドラインであり、規制基準とは何の関わりもない点に注意すべきである。9 月 15 日、DOE、NERC、NIST は「電力業界におけるサイバーセキュリティリスク管理ガイドライン」の草稿を発表し、10 月 28 日まで意見公募を行っている。FEC、DHS、米国電力会社もこの草案に取り組んでいる。

DOE の OE もまた、多数のサイバーセキュリティ関連技術プログラムを実施中である。

作成：ITTA
翻訳・編集：ジェトロ北米課