

インターテックリサーチ株式会社 情報セキュリティポリシー

Rev.1 平成 21 年 6 月 1 日

第 1 章 総則

(目的)

第 1 条 この情報セキュリティポリシーは、インターテックリサーチ株式会社の情報資産及びこれに係る情報システムを様々な脅威から保護するために必要な対策を明らかにし、その適正な運用を図ることによって、健全な運用を確保し、円滑なビジネス遂行を図ることを目的とする。

(定義)

第 2 条 この規定において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

(1) 情報資産

ネットワーク及び情報システムの開発と運用に関する全てのデータ並びにネットワーク及び情報システムで取り扱う全てのデータ及び機器をいう。

(2) 情報システム

ハードウェア、ソフトウェア、ネットワーク及び記録媒体で構成されるものであって、これら全体で業務処理を行う仕組み又は通信を行う仕組みをいう。

(3) 情報セキュリティ

情報の機密性、完全性及び可用性を維持することをいう。

(4) 機密性

情報について、当該情報を利用する権限を有するものだけが当該情報を利用することを確実にすることをいう。

(5) 完全性

情報、処理の方法及び通信が正確及び完全である状態を安全防護することをいう。

(6) 可用性

情報について、これを利用する権限を有する者が必要なときにこれを利用することができることを確実にすることをいう。

(8) ドキュメント

調査報告書や、その基礎資料等の文書及び電磁的記録をいう。

(位置づけと義務)

第 3 条 情報セキュリティポリシーの位置付けと従業者の義務

当社役員及び従業員は、この情報セキュリティポリシーを遵守し、情報セキュリティの確保に努めなければならない。

2 外部委託業者は、情報セキュリティの重要性について共通の認識を持つとともに、利用にあたっては情報セキュリティポリシーを遵守する義務を負うものとする。

(情報資産への脅威)

第 4 条 情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮し、情報セキュリティポリシーを策定するうえで特に認識すべき脅威は、次の各号に掲げるとおりである。

- (1) 部外者による故意の不正アクセスまたは不正操作、データやプログラムの持出・盗聴・改ざん・消去、機器及び媒体の盗難等
- (2) 従業員及び外部委託業者による意図しない操作及び不注意な操作、故意の不正アクセスまたは不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び媒体の盗難及びパソコン等の不正接続によるデータ漏洩等
- (3) 地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止
(情報セキュリティ対策基準の制定)

第 5 条 前条の脅威から情報資産を防護するため、情報の機密性、完全性及び可用性を踏まえ、その重要性に従って分類し、その分類に基づき、次章に定めるところにより情報セキュリティ対策基準を定めるものとする。

第 2 章 情報セキュリティ対策基準

(情報セキュリティ対策基準の制定)

第 6 条 情報セキュリティ対策を具体的に講ずるにあたって遵守すべき行為及び判断等の統一的な基準として必要な情報セキュリティ対策基準は、情報セキュリティ管理責任者が別に定めるものとする。

2 前項の情報セキュリティ対策基準は、次の各号の項目について定めるものとする。

- (1) 目的
- (2) 組織・体制
学校間総合ネットが保有する情報資産についての情報セキュリティ対策を推進・管理するための体制
- (3) 情報の分類と管理
情報資産の内容に応じた分類と、その重要度に応じた情報セキュリティ対策
- (4) 物理的セキュリティ対策
情報システムの設置場所について、不正な立入り、損傷及び妨害から保護するための適切な設備の設置、入退室管理及び執務室にあるパソコン等の盗難防止等の物理的な対策
- (5) 人的セキュリティ対策
情報セキュリティに関する権限や責任を定め、全ての職員等に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるために必要な対策
- (6) 技術的セキュリティ対策
情報システムの運用管理手順やネットワーク管理、記録媒体等の保護及び他の組織とデータ交換を行う際の情報資産を保護するための技術的な対策
- (7) 有害情報対策

インターテックリサーチ株式会社 情報セキュリティポリシー

Rev.1 平成 21 年 6 月 1 日

児童生徒を有害情報から保護するための有害情報除去対策

(8) 運用におけるセキュリティ対策

情報セキュリティポリシーの遵守状況の確認等の運用面の対策及び緊急事態が発生した際の危機管理対策

(9) 法令遵守

関連する法令等への遵守義務

(10) 情報セキュリティポリシーに関する違反に対する対応

情報セキュリティポリシーに違反した場合の対応

(11) 評価及び見直し

- 情報セキュリティポリシーが遵守されていることを検証するための点検の実施
- 情報セキュリティの点検結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価の実施並びに情報セキュリティを取り巻く状況の変化に対応するための情報セキュリティポリシーの見直し

3 情報セキュリティ対策基準は、情報セキュリティを確保するため非公開とする。

以上