学校間総合ネット情報セキュリティポリシー

情報セキュリティ基本方針

第１章　総則

第１条　目的

学校間総合ネットの情報資産及び情報システムを、様々な脅威から守ること及び学校間総合ネットに起因した被害を対外的に与えないことは、健全な学校間総合ネットの運営を行い、円滑な教育活動を推進するために不可欠なものである。

この学校間総合ネット情報セキュリティポリシー「情報セキュリティ基本方針」（以下「基本方針」という。）は、学校間総合ネット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、学校間総合ネットの健全な運用を確保し、円滑な教育活動の維持向上を図ることを目的とする。

第２条　用語の定義

基本方針の用語の意義は、それぞれ次に定めるところによる。

（１）情報資産

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情報システムで取り扱う全てのデータ、またそれらを取り扱うネットワーク及び機器をいう。

（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）情報セキュリティポリシー

情報資産に対する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものをいい、この基本方針及び第６条第１項の規定に定める情報セキュリティ対策基準からなるものをいう。

（５）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。

（６）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。

（７）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

情報システムに関する次に掲げる文書及び電磁的記録をいう。

ア　システム設計書　情報処理の手順並びに機器及びプログラムの構成概要を記録したもの
イ　プログラム仕様書　情報処理の手順を記録したもの
ウ　プログラムリスト　情報処理の手順をプログラム言語を用いて記述したもの
エ　操作説明書　機器の操作方法の説明を記録したもの

第３条　情報セキュリティポリシーの位置付けと職員等の義務

学校間総合ネットに接続する教育機関（以下、「接続機関」という。）における情報セキュリティ対策は、全てこの基本方針に定める情報セキュリティポリシーを遵守する必要があるものとする。

２　学校間総合ネットが所有する情報資産を利用する全ての接続機関の職員及び外部委託業者は、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。

第４条　情報資産への脅威

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又は不正操作、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、重要情報の詐取等

（２）職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又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、メンテナンス及び管理の不備、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、機器故障等によるサービス及び業務の停止

第５条　情報セキュリティ対策基準の制定

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

第６条　情報セキュリティ対策基準の制定

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､教育研修課長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

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

ア　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

イ　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。

第３章　雑則

第７条　委任

この基本方針に定めるもののほか、基本方針の施行に関し必要な事項は教育研修課長が別に定める。

附　則

この基本方針は、平成１６年４月１日から施行する。

附　則

この基本方針は、平成１８年４月１日から施行する。

附　則

この基本方針は、平成２１年６月１日から施行する。

附　則

この基本方針は、平成２３年４月１日から施行する。