平成 29 年 2 月 9 日
第 3 回教育委員会資料
教 育 部 学 務 課

立川市立学校情報セキュリティポリシーの概要

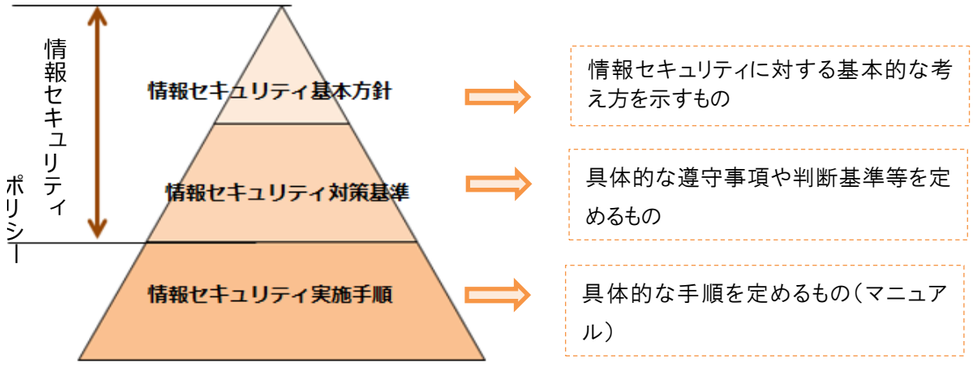
情報セキュリティを確保するための方針、体制、対策等を包括的に定めている情報セキュリティポリシー（以下、「ポリシー」という。）について、再構築を行い、学校独自のポリシーを新たに策定いたします。ポリシーの主な内容は、以下のとおりです。

【 情報セキュリティとは・・・情報資産の機密性・完全性・可用性を保つこと 】

機密性：許可された者だけが、情報にアクセスできること。　完全性：情報が正確で完全であること。　可用性：必要なときに情報資産にアクセスできること。

0. 情報セキュリティポリシーとは

情報セキュリティ対策に関する規程は下図の体系で構成され、「情報セキュリティ基本方針」と「情報セキュリティ対策基準」をあわせて「情報セキュリティポリシー」と称します。



1. 対象

①対象者

立川市立学校に所属する全教職員

※市が保有する情報資産（ノートパソコン等）を利用する教職員は、市の情報セキュリティポリシーも遵守すること

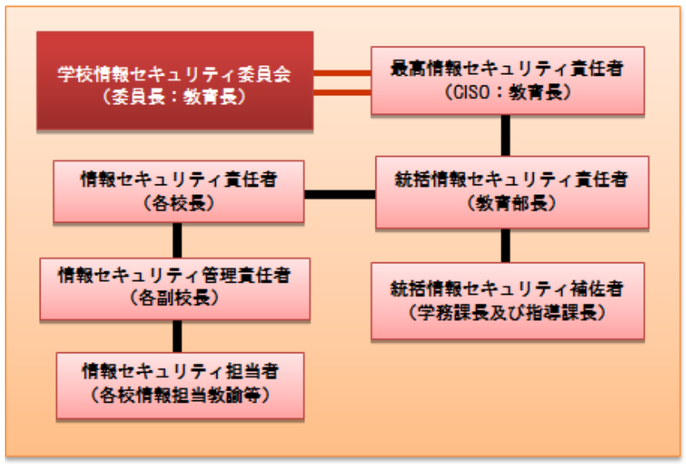
※委託等により学校が保有する情報資産を利用する者も、ポリシーを遵守すること（ボランティア等含む）

②対象とする情報資産

情報資産の種類		情報資産の例
情報システム等	ネットワーク	通信回線、ルータ等の通信機器
	情報システム	サーバ、パソコン、タブレット端末、ソフトウェア等
	これらに関する設備	コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル
	電磁的記録媒体	サーバ装置、端末、USBメモリ、外付けハードディスクドライブ、DVD-R等の外部電磁的記録媒体
紙文書		紙文書全般

2. 組織体制

情報セキュリティ対策を組織として効果的に実施するための組織体制を規定しています。



POINT

①最高情報セキュリティ責任者（CISO）をトップとして体系的に責任者等を配置します。

②各校の校長を情報セキュリティ責任者とし、学校の情報セキュリティ対策に関する統括的な権限及び責任を有します。

③情報セキュリティの統一的な維持管理、重要事項に関する調査等を行う組織として学校情報セキュリティ委員会を設置します。

3. 情報資産の分類

情報資産は重要性に応じて次のとおり分類しています。

分類	分類	区分・事例	措置
Ⅰ	情報セキュリティの侵害があった場合に、児童・生徒及び保護者等に損害が生じるおそれ又は学校運営に重大な影響を及ぼすおそれのある情報	①　個人情報等 ②　法令・条例により守秘義務が課せられている情報 ③　法人等に関する情報であって、漏えいすることにより当該団体の利益を侵害するおそれのあるもの ④　滅失又は毀損した場合に、その復元が困難となり、学校運営に重大な影響を及ぼすおそれのある情報 ⑤　漏えい等が児童・生徒及び保護者等の生命、プライバシー又は財産等に影響を及ぼすおそれのある情報	最小限者のみが取り扱うこととし、権限を有しない者の利用・接触等が絶対にないよう、特段の取扱制限を行う。
Ⅱ	情報セキュリティの侵害があった場合に、学校運営等に影響を及ぼすおそれのある情報	≪事例≫ ・出勤簿 ・内部会議の資料 ・定期考査答案用紙　等	関係者以外の利用・接触等がないよう、取扱制限を行う。
Ⅲ	上記以外の情報		

4. 物理的セキュリティ対策

サーバ、通信回線及びパソコン等の管理について、物理的な対策を講じます。

POINT

サーバの管理	✓ 火災、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定しなければならない。 ✓ ネットワークの基幹機器及び重要な情報システムを設置している区域（保管庫）は、鍵や監視機能等によって未許可の立入りを防止しなければならない。
端末・電磁的記録媒体等の管理	✓ パソコンのワイヤーによる固定、モバイル端末の使用時以外の施錠管理等、物理的措置を講じなければならない。 ✓ 電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。
認証機能	✓ 情報システムにログインするための認証機能（ID・パスワード等）を設定しなければならない。

5. 人的セキュリティ対策

教職員が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じます。

POINT

●教職員の遵守事項

教職員の遵守事項

目的外使用の禁止　支給以外の端末等の利用禁止　ID・パスワードの取扱い　など

●研修・訓練

情報セキュリティ研修と時勢に応じて必要とされる随時研修・セルフチェック・訓練の実施を規定する。

✦平成 29 年度の予定✦

市のシステム利用者：①情報推進課で企画する、セキュリティ研修の受講。
②情報推進課で企画する、e-ラーニングの実施。
③その他、情報推進課で実施するアンケート等の実施。

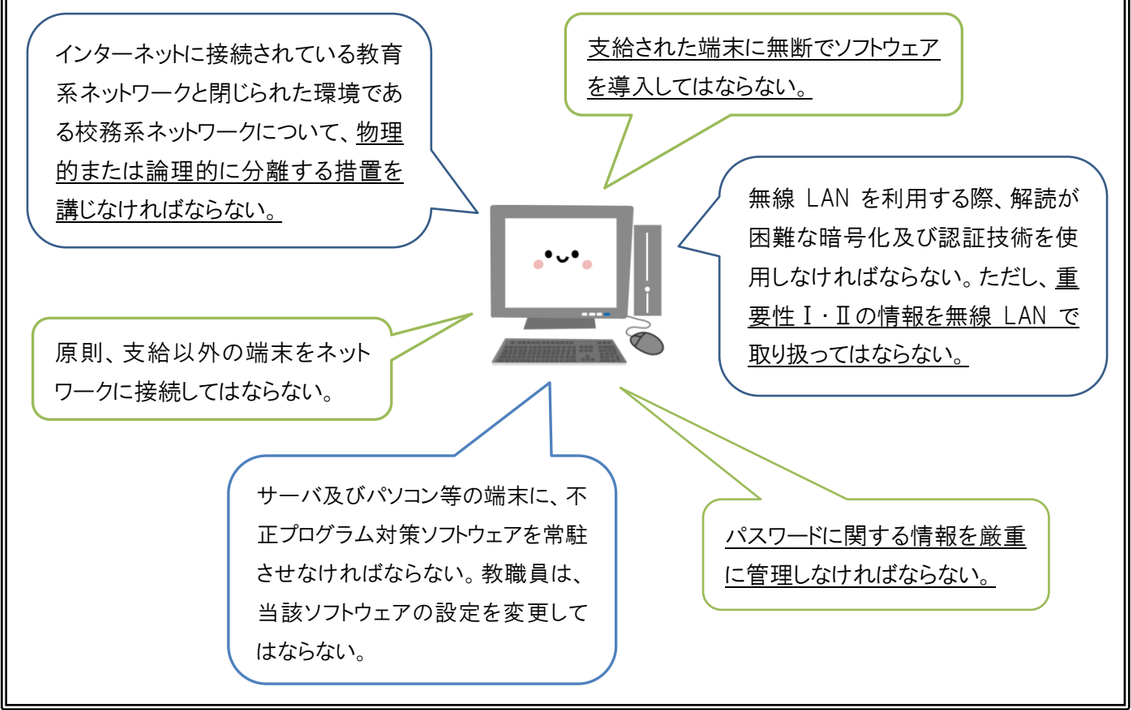
その他教職員　：情報セキュリティセルフチェックの実施。

※平成 30 年度はセキュリティ研修（セキュリティ責任者及び担当者向け）を実施する予定。

6. 技術的セキュリティ対策

コンピュータ等の管理、アクセス制御、不正プログラム対策等の技術的な対策を講じます。

POINT



7. 運用　8. 外部サービスの利用　9. 評価見直し

セキュリティポリシーの運用面の対策、外部サービス利用時の規定、ポリシーの評価・見直しについて定めます。

抜粋

✓ 情報セキュリティ責任者（校長）及び情報セキュリティ管理責任者（副校長）は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに統括情報セキュリティ責任者（教育部長）に報告しなければならない。

✓ 教職員は、情報セキュリティポリシーに違反している事実又は兆候を把握した場合、直ちに統括情報セキュリティ責任者（教育部長）及び情報セキュリティ責任者（校長）に報告を行わなければならない。

✓ ポリシーに違反した教職員及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象となることがある。

✓ 約款への同意及び簡易なアカウント登録により利用可能なサービス（電子メール、ファイルストレージサービス等）を使用してはならない。

✓ 教職員は、原則としてソーシャルメディアサービスを利用してはならない。

✓ 重要性Ⅰ・Ⅱの情報をソーシャルメディアサービスで発信してはならない（個人のアカウントでの情報発信を含む。）。

✓ CISO（教育長）は、学校情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査を実施しなければならない。

✓ 情報セキュリティ責任者（校長）は、所管する学校の情報セキュリティ対策の実施状況について、定期的又は必要に応じて自己点検を実施しなければならない。