ISMS-S-P-001

# 神戸市情報セキュリティ対策基準（学校編）

制定日：平成 23 年 3 月 30 日
改正日：令和 4 年 1 月 12 日
施行日：令和 4 年 1 月 12 日

神戸市

改訂履歴

| 施行年月日 | 版番号 | 改訂理由・内容 |
|---|---|---|
| 平成 23 年 4 月 1 日 | 第 1.0 版 | 初版発行（平成 23 年 3 月 30 日決裁） |
| 平成 24 年 4 月 1 日 | 第 1.1 版 | 情報資産の重要性分類の区分変更（平成 24 年 3 月 28 日決裁） |
| 平成 25 年 4 月 1 日 | 第 1.2 版 | 職制改正等にともなう一部改正（平成 25 年 3 月 25 日決裁） |
| 平成 26 年 4 月 1 日 | 第 1.3 版 | 職制改正等にともなう一部改正（平成 26 年 3 月 24 日決裁） |
| 平成 26 年 10 月 1 日 | 第 1.4 版 | 情報セキュリティ管理体制の見直し（平成 26 年 10 月 1 日決裁） |
| 平成 27 年 4 月 1 日 | 第 1.5 版 | 番号制度導入等にともなう一部改正（平成 27 年 3 月 18 日決裁） |
| 平成 28 年 4 月 1 日 | 第 1.6 版 | 総務省ガイドライン改正等にともなう一部改正（平成 28 年 3 月 10 日決裁） |
| 平成 29 年 4 月 1 日 | 第 1.7 版 | 職制改正等にともなう一部改正（平成 29 年 3 月 14 日決裁） |
| 平成 31 年 3 月 1 日 | 第 2.0 版 | 資産管理システム再構築にともなう運用変更（平成 31 年 2 月 26 日決裁） |
| 令和 2 年 7 月 1 日 | 第 3.0 版 | 文部科学省ガイドライン改正にともなう一部改正（令和 2 年 7 月 1 日決裁） |
| 令和 3 年 3 月 31 日 | 第 3.1 版 | BYOD 端末の運用開始等にともなう一部改正（令和 3 年 3 月 31 日決裁） |
| 令和 4 年 1 月 12 日 | 第 4.0 版 | 総務省ガイドラインおよび文部科学省ガイドライン改正にともなう一部改正（令和 4 年 1 月 12 日決裁） |
| 年　月　日 | | |

-目次-

# 1. 目的

神戸市情報セキュリティ対策基準（学校編）とは、神戸市情報セキュリティ基本方針に基づき情報セキュリティ対策等を実施するために適用範囲における共通の基準として具体的な遵守事項及び判断基準を定めたものである。

# 2. 適用範囲及び用語説明

## 2.1 適用範囲

神戸市立学校設置条例(昭和39年３月条例第87号)第１条により設置する市立学校（以下「学校園」という。）のうち、同条例第３条に規定する別表１から別表６に掲げる幼稚園、小学校、中学校、義務教育学校、高等学校及び特別支援学校とする。

## 2.2 用語説明

ア　校務系情報

児童生徒の成績、出欠席及びその理由、健康診断結果、指導要録、教員の個人情報など、学校が保有する情報資産のうち、それら情報を学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報

イ　校務外部接続系情報

校務系情報のうち、保護者メールや学校ホームページ等インターネット接続を前提とした校務で利用される情報

ウ　学習系情報

児童生徒のワークシート、作品など、学校が保有する情報資産のうち、それら情報を学校における教育活動において活用することを想定しており、かつ当該情報に教員及び児童生徒がアクセスすることが想定されている情報

エ　校務系システム

校務系ネットワーク、校務系サーバ及び校務用端末から構成される校務系情報を取扱うシステム

オ　校務外部接続系システム

校務外部接続系ネットワーク、保護者メール用メールサーバ、ホームページ運用サーバ（CMS)及び校務外部接続用端末等から構成される校務外部接続系情報を取扱うシステム

カ　学習系システム

学習系ネットワーク、学習系サーバ、学習者用端末及び指導者用端末から構成される学習系情報を取扱うシステム

# 3. 情報セキュリティ管理体制

## 3.1 体制

適切に情報セキュリティ対策を推進・管理するための体制として、次の者を置く。

### 3.1.1 情報セキュリティ最高責任者（CISO：Chief Information Security Officer、以下「CISO」という。）

神戸市情報化推進体制の整備に関する要綱に定める情報化統括責任者をCISOとする。

### 3.1.2 学校園情報セキュリティ統括責任者

教育委員会事務局長を学校園情報セキュリティ統括責任者とする。

### 3.1.3 学校園情報セキュリティ責任者

教育委員会事務局学校支援部長を学校園情報セキュリティ責任者とする。

### 3.1.4 学校園情報セキュリティ管理者

教育委員会事務局学校支援部担当課長(情報監理担当)を学校園情報セキュリティ管理者とする。

### 3.1.5 学校園情報管理者

情報資産を取扱う学校園の長を、所管する学校園の学校園情報管理者とする。

### 3.1.6 学校園業務システム管理者

各業務システムを所管する課の長又は学校園長を当該業務システムに関する学校園業務システム管理者とする。

### 3.1.7 学校園情報取扱者

教職員（地方公務員法(昭和25年法律第261号)第3条に規定する地方公務員（教育公務員特例法昭和24年1月12日法律第1号)第2条に定める教育公務員を含む）をいう。）及び委託業務等従事者を学校園情報取扱者とする。

### 3.1.8 学校園情報セキュリティ監査統括責任者

教育委員会事務局学校支援部長を学校園情報セキュリティ監査統括責任者とする。

### 3.1.9 学校園情報セキュリティ委員会

学校園情報セキュリティ委員会の構成員は、学校園情報セキュリティ責任者、学校園情報セキュリティ管理者のほか必要に応じて情報セキュリティに精通した外部の有識者等を構成員とし、セキュリティ侵害等の重大事案が発生した場合又は発生のおそれがある場合に、必要に応じて開催する。

## 3.2 権限と責任

神戸市情報セキュリティ基本方針及び前項で定めた情報セキュリティ管理体制における権限と責任については次のとおりとする。

### 3.2.1 CISO

ア　CISOは、本市における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

イ　CISOは、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有する専門家をアドバイザーとして置くものとする。

ウ　CISOは、・サイバー攻撃もしくはそのおそれのあるもの・情報漏えいもしくはそのおそれあるもの・システム上の欠陥及び誤動作のいずれか又は複数に該当する事案（以下「情報セキュリティインシデント」という。）に対処するための体制(CSIRT：Computer Security Incident Response Team、以下「CSIRT」という。)を整備し、役割を明確化する。

### 3.2.2　学校園情報セキュリティ統括責任者

ア　学校園情報セキュリティ統括責任者はCISOを補佐しなければならない。

イ　学校園情報セキュリティ統括責任者は、学校園にかかる全てのネットワーク、情報システム等の情報資産における開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

ウ　学校園情報セキュリティ統括責任者は、学校園にかかる全ての情報資産における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する。

エ　学校園情報セキュリティ統括責任者は、学校園情報セキュリティ責任者、学校園情報セキュリティ管理者、学校園情報管理者、学校園業務システム管理者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

オ　学校園情報セキュリティ統括責任者は、学校園にかかる情報資産に対する情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合に、CISOの指示に従い、CISOが不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

カ　学校園情報セキュリティ統括責任者は、緊急時等の円滑な情報提供を図るため、CISO、学校園情報セキュリティ統括責任者、学校園情報セキュリティ責任者、学校園情報セキュリティ管理者、学校園情報管理者、学校園業務システム管理者を網羅する連絡体制を整備しなければならない。

キ　学校園情報セキュリティ統括責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて CISOにその内容を報告しなければならない。

### 3.2.3　学校園情報セキュリティ責任者

ア　学校園情報セキュリティ責任者は学校園情報セキュリティ統括責任者を補佐しなければならない。

イ　学校園情報セキュリティ責任者は、学校園情報セキュリティ管理者、学校園情報管理者、学校園業務システム管理者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

ウ　学校園情報セキュリティ責任者は、学校園にかかる情報資産に対する情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合に、学校園情報セキュ

リティ統括責任者の指示に従い、学校園情報セキュリティ統括責任者が不在の場合には自らの判断に基づき、学校園情報セキュリティ管理者、学校園情報管理者、学校園業務システム管理者に円滑な情報提供を行わねばならない。

エ　学校園情報セキュリティ責任者は、学校園にかかる共通的なネットワーク、情報システム、情報等の情報資産における開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

オ　学校園情報セキュリティ責任者は、学校園にかかる共通的なネットワーク、情報システム、情報等の情報資産における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する。

カ　学校園情報セキュリティ責任者は、学校園にかかる共通的なネットワーク、情報システム、情報等の情報資産に関する情報セキュリティ実施手順の維持・管理を行う統括的な権限及び責任を有する。

### 3.2.4　学校園情報セキュリティ管理者

ア　学校園情報セキュリティ管理者は学校園情報セキュリティ統括責任者及び学校園情報セキュリティ責任者を補佐し、その実務を担当する。

イ　学校園情報セキュリティ管理者は、学校園業務システム管理者及び学校園情報管理者を監督し、学校園における緊急時等の連絡体制の整備並びに教職員に対する助言及び指示を行う。

ウ　学校園情報セキュリティ管理者は、学校園にかかる共通的なネットワーク、情報システム、情報等の情報資産における開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

エ　学校園情報セキュリティ管理者は、学校園にかかる共通的なネットワーク、情報システム、情報等の情報資産の情報セキュリティ対策に関する権限及び責任を有する。

オ　学校園情報セキュリティ管理者は、学校園にかかる共通的なネットワーク、情報システム、情報等の情報資産に係る情報セキュリティ実施手順を策定し、その維持・管理を行う。

カ　学校園情報セキュリティ管理者は、学校園にかかる共通的なネットワーク、情報システム、情報等の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、学校園情報セキュリティ責任者、学校園情報セキュリティ統括責任者、CISOへ速やかに報告を行い、指示を仰がなければならない。

キ　学校園情報セキュリティ管理者は、学校園にかかる共通的なネットワーク、情報システム、情報等の情報資産のうち、パーソナルコンピュータ等についての物理的セキュリティに関する管理を学校園情報管理者に行わせることができる。

### 3.2.5　学校園情報管理者

ア　学校園情報管理者は、所管する学校園における情報等の情報資産の情報セキュリティ対策に関する権限及び責任を有する。

イ　学校園情報管理者は、学校園情報セキュリティ管理者の指示に従い学校園にかかる共通的なネットワーク、情報システム、情報等の情報資産のうち所管する学校園のパーソナルコンピュータ等についての物理的セキュリティに関する管理を行う。

ウ　学校園情報管理者は、所管する学校園における情報等の情報資産に対する情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合には、学校園情報セキュリティ管理者、学校園業務システム管理者、学校園情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。

### 3.2.6　学校園業務システム管理者

ア　学校園業務システム管理者は、当該業務システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

イ　学校園業務システム管理者は、当該業務システムの情報セキュリティ対策に関する権限及び責任を有する。

ウ　学校園業務システム管理者は、当該業務システムに係る情報セキュリティ実施手順を策定し、その維持・管理を行う。

エ　学校園業務システム管理者は、当該業務システムにおいて情報資産に対する情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合には、学校園情報セキュリティ管理者、学校園情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。

オ　学校園業務システム管理者は、当該業務システムにおける開発、設定の変更、運用等についての作業を学校園業務システム管理者が指名する者に行わせることができる。

### 3.2.7　学校園情報取扱者

学校園情報取扱者は、学校園における情報資産の作成・入手・利用等を行う。

### 3.2.8　学校園情報セキュリティ監査統括責任者

学校園情報セキュリティ監査統括責任者は、情報セキュリティ監査の計画、実施、報告等を行う権限及び責任を有する。

### 3.2.9　学校園情報セキュリティ委員会

学校園情報セキュリティ委員会において、学校園における情報セキュリティに関する重要な事項を審議し、その内容をCISOに報告する。

### 3.2.10　兼務の禁止

ア　情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

イ　情報セキュリティ監査の実施において、監査を受ける者とその監査を実施す

る者は、同じ者が兼務してはならない。

### 3.3 CSIRT の設置・役割

#### 3.3.1 CSIRTの設置

ア　CISOは、情報セキュリティの統一的な窓口機能を有するCSIRTを設置しなければならない。

イ　CISOは情報セキュリティの統一的な窓口が情報セキュリティインシデントについて部局等より報告を受けた場合は、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。

#### 3.3.2 CSIRTの役割

ア　CISO による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供しなければならない。

イ　情報セキュリティインシデントを認知した場合には、CISO、総務省、都道府県等へ報告しなければならない。

ウ　情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティの統一的な窓口機能を有する部署、外部の事業者等との情報共有を行わなければならない。

#### 3.3.3 CSIRTの連絡体制

CSIRTの統一窓口は、学校園情報セキュリティ管理者とする。学校園情報セキュリティ管理者は、情報セキュリティインシデントが発生したときは、その内容に応じて、学校園業務システム管理者等と適宜連絡し、神戸市等の関係機関との情報共有を行う。

## 4. 情報資産の分類と管理

### 4.1 情報資産の分類と管理方法

対象となる情報資産は、各々の情報資産の機密性、完全性及び可用性を踏まえ、次の重要分類に従って分類する。

### 4.1.1 機密性

| 分類 | 分類基準 | 該当する情報資産のイメージ |
|---|---|---|
| 3 | 学校で取扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産<br>（データだけではなくそれらが含まれる電磁的記録媒体、パーソナルコンピュータ、システム等も同様） | 特定の教職員のみが知り得る状態を確保する必要のある情報で秘密文書に相当するもの<br>（例）<br>・指導要録原本<br>・教職員の人事情報<br>・入学者選抜問題<br>・教育情報システム仕様書 |
| 2B | 秘密文書に相当する機密性は要しないが、直ちに一般に公開することを前提としていない情報資産 | 教職員のみが知り得る状態を確保する必要がある情報資産（教職員のうち特定の教職員のみが知り得る状態を確保する必要があるものを含む）<br>（例）<br>・成績関係（通知表・考査結果等）<br>・児童生徒の個人情報（生活歴、心身の状態、財産状況、住所、電話番号、生年月日等）<br>・教職員の個人情報<br>・学習記録のうち児童生徒を特定でき、得点や評価のあるもの |
| 2A | 直ちに一般公開することを前提としていないが、児童生徒がアクセスすることを想定している情報資産 | 教職員及び児童生徒同士のみが知り得る状態を確保する必要がある情報資産（教職員及び児童生徒のうち特定の教職員及び児童生徒のみが知り得る状態を確保する必要があるものを含む）<br>（例）<br>・児童生徒、保護者、教職員の氏名（氏名以外の個人情報を含まない場合に限る）<br>・授業用教材、生徒用配布プリント<br>・学習記録のうち児童生徒を特定できないもの<br>・学習記録のうち得点や評価のないもの |
| 1 | 機密性2A、機密性2B又は機密性３以外の情報資産 | 公表されている情報資産または公表することを前提として作成された情報資産（教職員及び児童生徒以外の者が知り得ても支障がないと認められるものを含む）<br>（例）<br>・学校行事のしおり<br>・各種届ひな形 |

### 4.1.2 完全性

| 分類 | 分類基準 | 該当する情報資産のイメージ |
|---|---|---|
| 2B | 学校で取扱う情報資産のうち、改ざん、誤びゅう又は破損により学校関係者の権利が侵害される又は可能性があるデータ又は学校事務及び教育活動の的確な遂行に支障（軽微なものを除く）を及ぼすおそれがある情報資産 | 情報が正確・完全な状態である必要があり、破壊、改ざん、破損または第三者による削除等の事故があった場合、業務の遂行に支障がある情報<br>（例）機密性2B参照 |
| 2A | 学校で取扱う情報資産のうち、改ざん、誤びゅう又は破損により学校関係者の権利が侵害される又は学校の事務及び教育活動の的確な遂行に軽微な支障を及ぼすおそれがある情報資産 | 情報が正確・完全な状態である必要があり、破壊、改ざん、破損または第三者による削除等の事故があった場合、業務の遂行に軽微な支障がある情報<br>（例）機密性2A参照 |
| 1 | 完全性2A又は完全性2B以外の情報資産 | 事故があった場合でも業務の遂行に支障がない情報<br>（例）機密性1参照 |

### 4.1.3 可用性

| 分類 | 分類基準 | 該当する情報資産のイメージ |
|---|---|---|
| 2B | 学校で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、学校関係者の権利が侵害される又は学校事務及び教育活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産 | 必要な時にいつでも利用できる必要があり、情報システムの障害等による滅失、紛失や、情報システムの停止等があった場合、業務の安定的な遂行に支障がある情報<br>（例）機密性2B参照 |
| 2A | 学校で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、学校関係者の権利が侵害される又は学校事務及び教育活動の安定的な遂行に軽微な支障を及ぼすおそれがある情報資産 | 必要な時にいつでも利用できる必要があり、情報システムの障害等による滅失、紛失や、情報システムの停止等があった場合、業務の安定的な遂行に軽微な支障がある情報<br>（例）機密性2A参照 |
| 1 | 可用性2A又は可用性2Bの情報資産以外の情報資産 | 滅失、紛失や情報システムの停止等があっても業務の遂行に支障がない情報<br>（例）機密性1参照 |

#### 4.1.4　重要性分類に応じた対応

ア　情報資産の機密性、完全性、可用性のいずれかの重要性分類2A以上に分類される情報資産は、この対策基準の対象とする。

イ　重要性分類がいずれも１の情報資産も、必要なものはできる限りこの対策基準に準じた対応を講じるものとする。

### 4.2　情報資産の管理

#### 4.2.1　管理責任

ア　情報資産は、学校園情報セキュリティ管理者、学校園業務システム管理者及び学校園情報管理者（以下「学校園情報資産管理責任者」という）がそれぞれ所管する情報資産についての管理責任を有する。

イ　学校園情報セキュリティ管理者は、当該情報資産の利用範囲を定め、リスクを分析し、リスクに応じた対策を講じなければならない。また、リスク分析及び受容可能なリスクの水準等は、情報セキュリティに関する状況の変化等を踏まえ、定期的に見直しを行うものとする。

ウ　学校園情報取扱者は、情報資産の作成・入手・利用等に際しては、十分にその責任を自覚したうえで行わなければならない。

エ　情報が複製又は伝送された場合には、当該複製等も原本と同様に管理しなければならない。

#### 4.2.2　情報資産の分類の表示

情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

#### 4.2.3　情報の作成

ア　学校園情報取扱者は、業務上必要のない情報を作成してはならない。

イ　学校園情報取扱者は、情報の作成時に重要性分類に基づき、当該情報の分類を定めなければならない。

ウ　学校園情報取扱者は、作成した情報の分類が不明な場合、学校園情報資産管理責任者に判断を求めなければならない。

エ　学校園情報取扱者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

#### 4.2.4　情報資産の入手

ア　学校園情報取扱者は、他の学校園情報取扱者が作成した情報資産を入手したときは、入手元の情報資産の分類に基づいた取扱いをしなければならない。

イ　学校園情報取扱者は、学校園情報取扱者以外の者が作成した情報資産を入手

したときは、重要性分類に基づき、当該情報の分類を定めなければならない。

ウ　学校園情報取扱者は、入手した情報資産の分類が不明な場合、学校園情報資産管理責任者に判断を求めなければならない。

### 4.2.5　情報資産の利用

ア　学校園情報取扱者は、情報資産を業務上の目的以外に利用してはならない。

イ　情報資産の利用においては、情報資産の分類に応じ、利用者並びにアクセス権限を定めなければならない。

ウ　機密性2B以上の情報は、学校園情報資産管理責任者の許可を得た場合、複製・電子メール等による送信を行うことができる。また、権限のある者だけがアクセスできる環境で、保存・利用をしなければならない。複数の権限ある者で情報を共有するときや、所属する学校園の外に情報を電子メール等により送信するときは、暗号化及びパスワード等により、情報漏えい対策を施さなければならない。ただし、電子メール等による送信に必要な宛名や連絡先等については、この限りではない。

エ　情報資産を利用する者は、電磁的記録媒体又は紙媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該媒体を取扱わなければならない。

### 4.2.6　情報資産の保管

ア　学校園情報資産管理責任者は、情報資産の重要性分類に従って、情報資産の保管を適切に行わなければならない。

イ　学校園情報資産管理責任者は、情報資産を記録した電磁的記録媒体を保管する場合は、書込禁止の措置を講じなければならない。

ウ　学校園情報資産管理責任者は、持ち運び可能な電磁的記録媒体を耐火、耐熱、耐水及び耐湿対策を講じたうえ施錠可能な場所への保管等適切な管理を行わなければならない。

エ　学校園情報資産管理責任者は、情報システムのバックアップで取得した情報を記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域への保管を考慮しなければならない。なお、クラウドサービスを利用する場合はサービスの機能として自然災害対策がなされていることを確認すること。

### 4.2.7　情報資産の運搬

ア　機密性2B以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化及びパスワード等の設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

イ　機密性2B以上の情報資産を運搬する者は、学校園情報資産管理責任者に許可を得なければならない。

#### 4.2.8　情報資産の提供・公表

ア　機密性2A以上の情報資産を外部に提供する者は、必要に応じ暗号化及びパスワード等の設定を行わなければならない。

イ　機密性2B以上の情報資産を外部に提供する者は、学校園情報管理者に事前に許可を得たうえで、日時・担当者及び提供概要を記録しなければならない。

ウ　学校園情報資産管理責任者は、住民に公開する情報資産について、完全性を確保しなければならない。

#### 4.2.9　情報資産の廃棄

ア　情報資産の廃棄を行う者は、情報を記録している電磁的記録媒体が不要になった場合、当該媒体の初期化等を行ったうえで物理的に破壊する等、復元不可能な状態にして廃棄しなければならない。紙媒体が不要となった場合は、焼却、裁断、溶解等により廃棄しなければならない。

イ　情報資産の廃棄を行う学校園情報取扱者は、行った処理について日時、担当者及び処理内容を記録しなければならない。

ウ　情報資産の廃棄を行う学校園情報取扱者は、学校園情報資産管理責任者の許可を得なければならない。

#### 4.2.10　文書の管理

ア　情報セキュリティ対策基準を実施していくうえで必要とされる文書は、神戸市教育委員会公文書管理規程及び情報セキュリティに係る文書管理基準（学校編）等の定めに従い管理しなければならない。

イ　情報セキュリティに係る文書（以下「文書」という）を作成又は更新する場合は、あらかじめ定められた者による承認を受けなければならない。

ウ　文書は、定期的に見直しを行い、必要に応じて更新しなければならない。

エ　文書を廃棄する場合は、廃棄文書が誤って使用されないようにしなければならない。ただし、廃棄文書を保持する必要がある場合には、廃棄文書と分かるように適切な識別を施さなければならない。

#### 4.2.11　記録の管理

情報セキュリティ対策基準（学校編）の効果的運用の証拠を示すために、記録を作成し、適切な管理をしなければならない。

## 5.　物理的セキュリティ

### 5.1　サーバ等の管理

#### 5.1.1　機器の取付け

学校園情報セキュリティ管理者及び学校園業務システム管理者は、ネットワーク機器及び情報システム機器の取付けを行う場合、火災、水害、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な固

定を行う等必要な措置を講じなければならない。

### 5.1.2 サーバの冗長化

学校園情報セキュリティ管理者及び業務システム管理者は、可用性2B以上の情報資産について二重化等を行い、同一データを保持する等の対策を講じなければならない。

### 5.1.3 機器の電源

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者は、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

イ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、落雷等による過電流に対してサーバ等の機器を保護するための措置を講じなければならない。

### 5.1.4 通信ケーブル等の配線

ア　配線の変更、追加については、学校園情報セキュリティ管理者及び学校園業務システム管理者等限られた者の権限とする。

イ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

ウ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

エ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

オ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、自ら又は情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

### 5.1.5 機器等の定期保守及び修理

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者は、可用性３のサーバ等の機器は、定期保守を実施しなければならない。

イ　学校園情報資産管理責任者は、記憶装置を内蔵する機器を外部の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。内容を消去できない場合、外部の業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結する他、秘密保持体制の確認等を行わなければならない。

#### 5.1.6　敷地外への機器の設置

学校園情報セキュリティ管理者及び学校園業務システム管理者は、学校園の敷地外にサーバ等の機器を設置する場合、学校園情報セキュリティ統括責任者の許可を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

#### 5.1.7　機器の廃棄等

学校園情報資産管理責任者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、すべてのデータを消去のうえ、復元不可能な状態にする措置を施さなければならない。復元不可能な状態にする作業を外部に委託する場合は、委託事業者との間で守秘義務契約を締結するだけでなく、データ消去証明書等の提出を求めなければならない。

### 5.2　管理区域（情報システム室等）の管理

#### 5.2.1　管理区域の構造等

ア　管理区域とは、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、当該機器等の管理及び運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

イ　管理区域を新設する場合は、立ち入りを許可されていない不特定多数の者が出入りできる場所に設置してはならない。

ウ　施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

エ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

オ　管理区域に配置する消火薬剤や消防用設備等が、機器及び電磁的記録媒体等に影響を与えないようにしなければならない。

#### 5.2.2　入退室の管理等

ア　管理区域への入退室は、許可された者のみに制限し、IDカード等による認証及び入退室管理簿の記載による入退室管理を行わなければならない。ただし、教職員が日常業務を行う職員室等に管理区域を設けている場合は、当該室内への立ち入りの規定に従うものとする。

イ　教職員等及び外部委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

ウ　外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された教職員等が付き添うものとし、外見上教職員等と区別できる措置を講じなければならない。

エ　管理区域について、当該情報システムに関連しない、または個人所有である端末、モバイル端末（執務区域外に持ち出しての使用が可能な端末）、通信回線装置、電磁的記録媒体等持ち込ませないようにしなければならない。ただし、教職員が日常業務を行う職員室等に管理区域を設けている場合は、当該室内への立ち入りの規定に従うものとする。

オ　学校園情報資産管理責任者は、重要性分類2B以上のデータを取扱う執務区域については、許可された者以外の立入を制限するなどの適正な入退室管理を行わなければならない。ただし、教職員が日常業務を行う職員室等に管理区域を設けている場合は、当該室内への立ち入りの規定に従うものとする。

#### 5.2.3　機器等の搬入出

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者は、機器等を搬入する場合、あらかじめ当該機器等の既存情報システムに与える影響について、教職員に確認を行わせなければならない。

イ　機器等の搬入出には教職員が同行する等の必要な措置を施さなければならない。

### 5.3　ネットワークの管理

#### 5.3.1　通信回線及び通信回線装置の管理

学校園情報セキュリティ管理者及び学校園業務システム管理者は、学校園の通信回線及び通信回線装置を施設管理部門と連携し、適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

#### 5.3.2　外部ネットワークへの接続

学校園情報セキュリティ管理者及び学校園業務システム管理者は、通信回線による外部ネットワークへの接続は必要最低限のものに限定し、できる限り接続ポイントを減らさなければならない。

#### 5.3.3　機密を要する情報システムで使用する回線

学校園情報セキュリティ管理者及び学校園業務システム管理者は、所管する情報システムにおいて機密性2Aの情報資産を取扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討のうえ、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

#### 5.3.4　ネットワークで使用する回線

ア　ネットワークに使用する回線は送信途上においてデータの破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策が実施されたものでなければならない。

イ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、ネットワークで使用する回線を選択するにあたって、必要な可用性を考慮しなければならない。

## 5.4 教職員等の利用する端末や電磁的記録媒体等の管理

### 5.4.1 端末等の盗難防止策

学校園情報資産管理責任者は、学校園の執務区域等の端末等について、盗難防止のための措置を講じなければならない。また、学校園情報資産管理責任者は電磁的記録媒体の使用時以外の施錠管理等の措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

### 5.4.2 ログイン認証

学校園情報セキュリティ管理者及び学校園業務システム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。また、必要に応じて電源起動時のパスワード（BIOS パスワード、ハードディスクパスワード等）を併用しなければならない。

### 5.4.3 認証の併用

学校園情報セキュリティ管理者及び学校園業務システム管理者は、取扱う情報の重要性分類に応じて、パスワード以外に必要に応じてIDカード等を導入し、二要素認証を行うものとする。

### 5.4.4 暗号化機能の利用

学校園情報セキュリティ管理者及び学校園業務システム管理者は、端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末等にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。また、電磁的記録媒体についても、取扱う情報の重要度に応じてデータ暗号化機能を備える媒体を使用しなければならない。

### 5.4.5 所属する学校園の外への端末持ち出し時の対策

ア　所属する学校園の外で端末を利用する場合は、生体認証等によるロックをせずに、端末内部に機密性2A以上の情報を保存してはならない。また、通信については、暗号化されたものを使用しなければならない。

イ　物理的な覗き見防止の措置を講じなければならない。

## 5.5 学習用端末の管理

ア　学校園情報セキュリティ管理者は、盗難防止のため、教室等で利用するパソコンの保管庫による管理等の物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

イ　学校園業務システム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

ウ　授業等学習活動において、児童生徒が個人所有するパソコン等を利用する場合、学校園情報管理者は、盗難防止措置や破損防止措置などを含む適切な管理方法につ

いて児童生徒に説明・指導するとともに、児童生徒が利用する端末を把握しなければならない。

# 6. 人的セキュリティ

## 6.1 教職員の遵守事項

### 6.1.1 情報セキュリティポリシー等の遵守

教職員は、情報セキュリティポリシー及びこれに基づく文書に定められている事項を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点がある場合には、学校園情報管理者等権限のある者に相談し、指示を仰がなければならない。

### 6.1.2 業務以外の目的での使用禁止

教職員は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールの使用及びインターネットへのアクセス等を行ってはならない。

### 6.1.3 指示に基づいた情報資産の利用等

教職員は、学校園情報管理者等権限のある者の指示等に従い、情報資産を利用するとともに、開発、設定の変更、運用、更新等の作業を行う。

### 6.1.4 情報資産の持ち出し及び送信禁止

教職員は、学校園情報管理者等権限のある者の許可を得た場合に限り、記録を作成したうえで、所属する学校園の外へ情報資産を持ち出し又は送信することができる。

### 6.1.5 所属する学校園の外における情報処理作業の制限

ア　学校園情報セキュリティ統括責任者は、機密性2B以上、可用性2B、完全性2Bの情報資産を所属する学校園の外で処理する場合における安全管理措置を定めなければならない。

イ　教職員は、所属する学校園の外で情報処理作業を行う場合には、学校園情報管理者等権限のある者の許可を得なければならない。

ウ　教職員は、所属する学校園の外で端末を使用して情報処理作業を行う場合には、大量または機微な個人情報を取扱ってはならない。ただし、在宅勤務等で行われる校務系システム上での作業はこの限りではない。また、公共の場又は公共の乗り物においては個人情報を取扱ってはならない。

エ　教職員は紛失・盗難を防止するため、移動の際は細心の注意をもって端末を携行しなければならない。

オ　教職員は覗き見を防止するため、学校園の外において教職員等以外の目に触れないように取扱わなければならない。

カ　教職員は不正使用を防止するため、端末を使用しないときは、他者に端末が使用されないように必要な対策を取らなければならない。

キ　教職員は端末でデータを保存する場合、指定されたファイルサーバの領域にデータを保存することとし、原則として端末内にデータを保存してはならない。

ク　教職員は、所属する学校園の外で情報処理作業を行う際、学校管理外のパーソナルコンピュータによる情報処理を行ってはならない。ただし、学校園情報セキュリティ統括責任者が別途定める情報処理作業については、学校園情報管理者等権限のある者の事前の許可を得た場合に限り、所属する学校園と同等のセキュリティが確保できる学校管理外のパーソナルコンピュータで行うことができる。

### 6.1.6　支給以外の端末、モバイル端末及び電磁的記録媒体等の業務利用

ア　教職員は、支給以外の端末、モバイル端末及び電磁的記録媒体等（データ保存機能のないマウスやキーボード等のPC周辺機器を除く）を原則として業務に利用してはならない。ただし多要素認証に利用する場合においては、学校園情報管理者の許可を得て、支給以外のモバイル端末を利用することができる。

イ　教職員は、支給以外の端末、モバイル端末及び電磁的記録媒体等では、機密性2B以上の情報を扱ってはならない。

### 6.1.7　持ち出しの記録

学校園情報管理者は、端末等の持ち出しについて、記録を作成し、保管しなければならない。

### 6.1.8　端末のセキュリティ設定変更の禁止

教職員は、端末のソフトウェアに関するセキュリティ機能の設定を学校園情報セキュリティ管理者及び学校園業務システム管理者の許可なく変更してはならない。

### 6.1.9　机上の端末等の管理

教職員は、端末や電磁的記録媒体、データが印刷された文書等について、第三者に使用されること、又は学校園情報管理者等管理権限のある者の許可なく情報を閲覧されることがないように、離席時の端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

### 6.1.10　異動、退職時等の遵守事項

教職員は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

### 6.1.11　対象教職員等

情報資産を取扱う全ての教職員等（人材派遣職員等も含む）に対し、学校園情報管理者等権限のある者は従事させる業務の範囲を指定する。また、全ての教職員等（人材派遣職員等も含む）は6.1.1～6.1.10に定める事項を守らなければならない。

### 6.1.12　情報セキュリティポリシー等の掲示

情報管理者は、教職員等が常に情報セキュリティポリシー及びこれに基づく文書

を参照できるよう配慮しなければならない。

## 6.2 研修・訓練

### 6.2.1 情報セキュリティに関する研修・訓練

CISOは、定期的に学校園情報取扱者に対する情報セキュリティに関する研修・訓練を実施させなければならない。

### 6.2.2 研修計画の策定及び実施

ア　学校園情報セキュリティ統括責任者は、学校園情報取扱者に対する情報セキュリティに関する研修計画を定期的に策定し、CISOに報告しなければならない。

イ　学校園情報セキュリティ統括責任者は、学校園情報取扱者を対象とする情報セキュリティに関する研修を毎年度最低１回実施しなければならない。

ウ　学校園情報セキュリティ統括責任者は、新規採用の教職員を対象とする情報セキュリティに関する研修を実施しなければならない。

エ　研修は、学校園情報セキュリティ統括責任者、学校園情報セキュリティ責任者、学校園情報セキュリティ管理者、学校園情報管理者、学校園業務システム管理者及び学校園情報取扱者に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

オ　学校園情報管理者は、所属の研修の実施状況を記録し、学校園情報セキュリティ責任者及び学校園情報セキュリティ統括責任者に対して、報告しなければならない。

カ　学校園情報セキュリティ統括責任者は、研修の実施状況を分析、評価し、毎年度１回、CISOに情報セキュリティ対策に関する研修の実施状況について報告しなければならない。

### 6.2.3 緊急時対応訓練

CISOは、緊急時対応を想定した訓練を定期的に実施させなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。なお、CISOは、緊急時対応訓練の実施結果を受けて、緊急時の体制や対応手順の改善を行わなければならない。

### 6.2.4 研修・訓練への参加

すべての学校園情報取扱者は、情報セキュリティに関する意識を深め情報セキュリティ上の問題が生じないようにするため、定められた研修・訓練に参加しなければならない。

## 6.3 情報セキュリティインシデントの報告

### 6.3.1 情報セキュリティインシデントの報告

ア　学校園情報取扱者は、情報セキュリティインシデントを発見した場合、若しくは保護者等外部から報告を受けた場合、速やかに学校園情報管理者に報告し

なければならない。

イ　報告を受けた学校園情報管理者は、速やかに学校園情報セキュリティ管理者に報告しなければならない。また、当該情報セキュリティインシデントが共通的なネットワークに関連する場合は、学校園業務システム管理者等に対しても報告しなければならない。

ウ　学校園情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、神戸市等の関係機関に必要な連絡を行うとともに、学校園情報セキュリティ責任者、学校園情報セキュリティ統括責任者及びCISOに報告しなければならない。また情報セキュリティインシデントの重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。

### 6.3.2　情報セキュリティインシデントの報告内容

学校園情報管理者等から情報セキュリティ管理者への報告は、以下の内容を含むものとする。

ア　件名

イ　判明した日時

ウ　発生した日時

エ　通報者

オ　事件事故等の内容

カ　漏えいした情報

キ　想定される原因

ク　事件事故等への対応

ケ　復旧方針

### 6.3.2　情報セキュリティインシデントの原因の究明・記録、再発防止等

ア CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行う。

イ CSIRT は、情報セキュリティインシデントであると評価した場合、CISO に速やかに報告する。

ウ CSIRT は、情報セキュリティインシデントに関係する情報管理者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行う。

エ CSIRT は、これらの情報セキュリティインシデント原因を究明し、記録を保存する。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、CISO に報告する。

オ　CISOは、CSIRTから、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示する。

## 6.4　アクセスのための認証情報及びパスワードの管理

### 6.4.1　ID カード等の管理

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者はIDカード等の適正な管理を行わなければならない。

イ　学校園情報取扱者は、次の事項を遵守しなければならない。

(1) IDカード等は、学校園情報取扱者間で共有しない。ただし、限定された利用者による共有使用を目的としたIDカード等については除く。

(2) 業務上必要のないときは、IDカード等をカードリーダ又は端末のスロット等から抜いておかなければならない。

(3) IDカード等を紛失した場合には、学校園情報セキュリティ管理者及び学校園業務システム管理者に速やかに通報し、指示を仰がなければならない。

ウ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、通報があり次第速やかに当該IDカード等を使用したアクセス等を停止しなければならない。

エ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、IDカード等を切り替える場合、切り替え前のIDカード等を回収し、データの消去又は破砕する等復元不可能な処理を実施しなければならない。

### 6.4.2　IDの管理

ア　学校園情報取扱者は、他人に自己が利用しているIDを利用させてはならない。

イ　共用IDを利用する場合は、共用IDの利用者以外に利用させてはならない。

### 6.4.3　パスワードの取扱い

ア　学校園情報取扱者は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

(1) パスワードは、他者に知られないように管理しなければならない。

(2) パスワードは秘密にし、パスワードの照会等には一切応じてはならない。

(3) パスワードは十分な長さ（原則として８文字以上）とし、文字列は想像しにくいもの（英字（大文字・小文字区別有）、数字、記号を組み合わせたものなど）としなければならない。

(4) 原則として、パスワードを記載したメモを作成しない。やむを得ずメモを作成する場合は、特定の場所に施錠して保管する等により、他人が容易に見ることができない措置をとる。

(5) パスワードが流出したおそれがある場合には、学校園情報セキュリティ管理者及び学校園業務システム管理者等権限のある者に速やかに報告し、パスワードを速やかに変更しなければならい。

(6) ID・パスワードのみでログインする情報システムを扱う場合は、同一のパスワードをシステム間で用いてはならない。

(7) 仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。

(8) パーソナルコンピュータ等のパスワードの記憶機能を利用してはならない。
(9) 学校園情報取扱者間でパスワードを共有してはならない（ただし、共有IDに対するパスワードは除く）。

イ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、パスワードの照会等には一切応じてはならない。

# 7. 技術的セキュリティ

## 7.1 コンピュータ及びネットワークの管理

### 7.1.1 情報の保存

情報の保存については、学校園情報セキュリティ管理者等管理権限のある者の定める方法により保存を行わなければならない。

### 7.1.2 ファイルサーバの設定等

学校園情報セキュリティ管理者が情報を共有するためのファイルサーバを設置する場合には、次の事項を守らなければならない。

ア 教職員が使用できるファイルサーバの容量を定め、教職員に周知しなければならない。

イ　ファイルサーバを学校園単位で構成する場合には、教職員が他の学校園のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

ウ　特定の教職員のみが取扱う権限を持つ情報については、同一の学校園であっても、権限のない者が閲覧及び使用できないよう設定しなければならない。

### 7.1.3 バックアップの実施

学校園情報セキュリティ管理者及び学校園業務システム管理者は、所管するシステムにおいて、必要なものはサーバの二重化対策実施の有無に関わらず、定期的に情報資産のバックアップのための対応を行うものとする。

### 7.1.4 他団体との情報システムに関する情報等の交換

学校園情報セキュリティ管理者及び学校園業務システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、学校園情報セキュリティ統括責任者の許可を得なければならない。

### 7.1.5 システム管理記録及び作業の確認

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

イ　学校園情報セキュリティ管理者及び学校園業務システム管理者、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理しなければならない。

ウ　学校園情報セキュリティ管理者及び学校園業務システム管理者又は教職員等及び契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、2名以上で作業し、互いにその作業を確認しなければならない。

### 7.1.6　情報システム仕様書等の管理

学校園情報セキュリティ管理者及び学校園業務システム管理者は、所管するシステムのネットワーク構成図、情報システム仕様書等に関し、記録媒体の形態に関わらず、業務上必要とする者以外の者が閲覧したり、紛失したりすることがないよう、適切な保管をしなければならない。

### 7.1.7　ログの取得等

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者は、所管するシステムにおいて、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

イ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対応等について定め、適正にログを管理しなければならない。

ウ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

エ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、システムから自動出力したログ等について、必要に応じ、外部記録媒体にバックアップしなければならない。

### 7.1.8　障害記録

学校園情報セキュリティ管理者及び学校園業務システム管理者は、所管するシステムにおいて、学校園情報取扱者からのシステム障害の報告、システム障害に対する処理結果又は問題等を障害記録として体系的に記録し、適切に保存しなければならない。

### 7.1.9　ネットワークの接続制御、経路制御

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者は、アクセス可能なネットワーク又はネットワーク上のサービス毎にアクセスできる者を定めなければならない。また、ネットワークサービスを利用する権限を有しない者が当該サービスを利用できるようにしてはならない。

イ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等に搭載されている通信ソフトウェア等を設定しなければならない。

ウ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

### 7.1.10　外部の者が利用するシステムの分離等

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者は、インターネット等により外部の者（学校園情報取扱者以外の者）が利用できるシステムにおいては、必要に応じ他のネットワーク及び情報システムと物理的に分離する等、情報セキュリティ対策について特に強固に対策を講じなければならない。

イ　外部の者が利用できるシステムにおいて、機密性2B以上の情報を照会又は更新するために外部の者がインターネット経由でシステムにアクセスしようとする場合は、必要に応じ、多段階認証又は多要素認証等のセキュリティ措置を講ずることとする。ただし、定型的な回答又は届出を送信するためにアクセスしようとする場合はこの限りではない。

### 7.1.11　外部ネットワークとの接続制限等

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者は、外部ネットワークとの接続にあたり当該外部ネットワークのネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、学校園にかかる情報資産に影響が生じないことを確認しなければならない。なお、学校園業務システム管理者は、学校園情報セキュリティ管理者の許可に基づき接続しなければならない。

イ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、接続に際して情報セキュリティの確保できるネットワーク構成を採らなければならない。学校園情報セキュリティ管理者及び学校園業務システム管理者は、当該外部ネットワークの瑕疵により学校園にかかるデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対応するため、必要に応じて当該外部ネットワークの管理責任者による損害賠償責任を契約上担保するよう努めなければならない。

ウ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、ウェブサーバ等をインターネットに公開する場合、学校園のネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

エ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、学校園にかかる情報資産に脅威が生じるおそれがある場合には、当該外部ネットワークとの接続を物理的に遮断しなければならない。

### 7.1.12　機微情報に対するインターネットリスク、児童生徒による機微情報へのアクセスリスクへの対応

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者は、校務系システム及び学習系システム間の通信経路の論理的又は物理的な分離をするとともに、ウェブ閲覧やインターネットメールなどのインターネットリスクの高いシステムと機微情報（特に校務系）を論理的又は物理的に分離をする、もしくはこれらに類する安全管理措置を講じなければならない。特にクラウドについても、通信経路の論理的又は物理的な分離によるセキュリティの品質に準じた安全管理措置を講じること。

イ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、校務系システムとその他のシステム（校務外部接続系システム、学習系システム）との間で通信する場合には、ウイルス感染のない無害化通信など、適切な措置を図らなければならない。

### 7.1.13　Web サイトでの情報公開時の注意事項

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者は、Webサイトにより情報を公開・提供する場合に、所管するサイトに係るシステムにおいて情報の漏えい・改ざん・消去、踏み台、DoS攻撃等を防止しなければならない。また、なりすまし防止などの観点から、可能な限り「ed.jp」ドメインを利用したり、ドメイン変更時に旧ドメインを一定期間保有したりするなど、ドメインを適正に設定し、管理しなければならない。

イ　メールシステムを含め各業務システムにおいても、他のシステムに対する攻撃の踏み台とならないようにコンピュータウイルス対策等適正な管理をしなければならない。

ウ　新たにWebサイトを公開する場合、全てのページでTLS通信を利用すること。なお、現状未対応の公開Webサイトは、全てのページでTLS通信を利用するために必要な作業を実施しなければならない。

### 7.1.14　複合機のセキュリティ管理

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者は、複合機を調達する場合、当該複合機が備える機能及び設置環境並びに取扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

イ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

ウ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消する又は再利用できないようにする対策を講じなければならない。

### 7.1.15　IoT機器を含む特定用途機器のセキュリティ管理

学校園情報セキュリティ管理者及び学校園業務システム管理者は、所管する特定

用途機器について、取扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

### 7.1.16 無線 LAN 等の利用

ア　学校園情報取扱者は、学校園にかかるネットワーク（以下「内部ネットワーク」という）において、無線LANを利用した接続又は端末等の無線機能を利用した端末間通信を行ってはならない。

イ　専ら教育目的または校務処理での利用で、合理的な理由があり、学校園情報セキュリティ統括責任者が情報セキュリティを確保するために、解読が困難な暗号化及び認証技術の使用等別途定める要件を満たす場合、学校園情報セキュリティ管理者の許可を得て、無線LANを利用した接続等を行うことができる。

### 7.1.17 電子メールのセキュリティ管理

ア　学校園情報取扱者が電子メールの利用を希望する場合、学校園情報管理者が、学校園情報セキュリティ管理者に対し、メールアドレスの取得を申請するものとする。

イ　学校園情報セキュリティ管理者は、電子メールの送受信容量の上限を定め、上限を超える電子メールの送受信を不可能にしなければならない。

ウ　学校園情報セキュリティ管理者は、電子メールに添付されるファイルについて、セキュリティ上問題があると思われるファイルについては、送受信を制限できるようにしなければならない。

エ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

オ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、システム開発や運用、保守等のため庁舎内に常駐している外部委託事業者の作業員による電子メールアドレス利用について、外部委託事業者との間で利用方法を取り決めなければならない。

### 7.1.18 電子メールの利用制限

ア　メールアドレスを保有する学校園情報取扱者は、自動転送機能を用いて、電子メールを転送してはならない。

イ　メールアドレスを保有する学校園情報取扱者は、業務上必要のない送信先に電子メールを送信してはならない。

ウ　メールアドレスを保有する学校園情報取扱者は、複数の宛先に電子メールを送信する場合、必要がある場合を除き他の送信先の電子メールアドレスがわからないようにしなければならない。

エ　メールアドレスを保有する学校園情報取扱者は、重要な電子メールを誤送信した場合、学校園情報セキュリティ管理者に報告しなければならない。

オ　教職員等は、インターネット上で利用できる電子メールやファイルストレージ等において、私的な個人アカウント等を用いて使用してはならない。

**7.1.19　電子署名・暗号化**

ア　学校園情報取扱者は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、学校園情報セキュリティ統括責任者が定めた電子署名、暗号化及びパスワード設定等セキュリティを考慮して、送信しなければならない。

イ　学校園情報取扱者は、暗号化を行う場合に学校園情報セキュリティ統括責任者が定める以外の方法を用いてはならない。また、学校園情報セキュリティ統括責任者が定めた方法で暗号のための鍵を管理しなければならない。

ウ　学校園情報セキュリティ統括責任者は、電子署名や電子証明書を使用して暗号化をする場合には、電子署名の正当性を検証するための情報又は手段を、正当な署名検証者へ提供できるようにしなければならない。

**7.1.20　無許可ソフトウェアの導入等の禁止**

ア　学校園情報取扱者は、各自に供与された端末に対して、学校園情報セキュリティ管理者が定めるもの以外のソフトウェアの導入を行ってはならない。ただし、業務を円滑に遂行するために必要なソフトウェアについては、学校園情報セキュリティ管理者の許可を得た場合に限り、利用することができる。

イ　学校園情報取扱者は、不正にコピーしたソフトウェア及び個人所有のソフトウェアを導入又は使用してはならない。

**7.1.21　機器構成の変更の禁止**

学校園情報取扱者は、ネットワーク及び各自に供与された端末等に対して、端末及びその他機器の接続、増設又は改造を行ってはならない。軽微な機器の増設の場合は、学校園情報セキュリティ管理者等権限のある者の許可を必要とする。

**7.1.22　無許可でのネットワーク接続の禁止**

学校園情報取扱者は、学校園情報セキュリティ管理者等権限のある者の許可なく端末等をネットワークに接続してはならない。

**7.1.23　利用可能なネットワークプロトコル**

学校園情報取扱者が利用できるネットワークプロトコルは、業務上必要最低限のものとする。

**7.1.24　業務以外の目的でのWebサイト閲覧の禁止**

ア　教職員等は、業務以外の目的でWebサイトを閲覧してはならない。

イ　学校園情報セキュリティ管理者等権限のある者は、学校園情報取扱者のWeb利用について、明らかに業務に関係のないWebサイトを閲覧していることを発見し

た場合は、学校園情報管理者に通知し適正な措置を求めなければならない。

## 7.2 アクセス制御

学校園情報セキュリティ管理者及び業務システム管理者は、所管するネットワーク又はシステムにおいて、次の事項を実施しなければならない

### 7.2.1 アクセス制御

学校園情報セキュリティ管理者及び業務システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない教職員がアクセスできないように、システム上制限しなければならない。

### 7.2.2 利用者 ID の取扱い

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者は、所管するネットワーク又は情報システムに権限がない学校園情報取扱者がアクセスすることが不可能となるように、利用者の識別及び認証等適切な対応を行わなければならない。

イ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、利用者の登録、変更、抹消等の情報管理、教職員の異動、出向及び退職に伴う利用者IDの取扱い等については、定められた方法に従って行わなければならない。必要な利用者登録・変更・抹消は、学校園情報セキュリティ管理者及び学校園業務システム管理者に対する申請により行う。ただし、学校園ごとに配布されたID等については除く。

ウ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、利用されていないIDが放置されないよう、人事管理部門と連携し、点検しなければならない。

エ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、IDに割り当てているアクセス権の正当性を確保するために、定められた方法に従って点検しなければならない。

### 7.2.3 特権 ID の管理等

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者は、管理者権限等の特権IDを利用する者を必要最小限にし、当該IDのパスワードの漏えい等が発生しないよう、当該ID及びパスワードを厳重に管理しなければならない。

イ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、特権ID及びパスワードの変更について、原則として外部委託事業者に行わせてはならない。

ウ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、特権を付与されたID及びパスワードについて、学校園情報取扱者の端末等のパスワードと同等あるいはそれ以上のセキュリティ強化を実施しなければならない。

エ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、特権によ

るネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

オ　学校園情報セキュリティ管理者及び業務システム管理者は、特権IDを初期設定以外のものに変更しなければならない。

### 7.2.4　ネットワークにおけるアクセス制御

学校園情報セキュリティ管理者及び学校園業務システム管理者は、アクセス可能なネットワーク又はネットワーク上のサービス毎にアクセスできる者を定めなければならない。また、ネットワークサービスを利用する権限を有しない学校園情報取扱者が当該サービスを利用できるようにしてはならない。

### 7.2.5　外部からのアクセス

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者は、外部からのアクセスを許可する場合、合理的理由を有する必要最低限のものに限定しなければならない。

イ　学校園情報セキュリティ管理者及び業務システム管理者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

ウ　学校園情報セキュリティ管理者及び業務システム管理者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

エ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、所属する学校園の外で利用可能な端末のセキュリティ確保について必要な措置を講じなければならない。

オ　学校園情報セキュリティ管理者及び業務システム管理者は、学校園以外のネットワークから学校園のネットワークへのアクセスに公衆通信回線（公衆無線LAN）等の利用を認める場合、論理的専用回線の利用に限定する等のセキュリティ措置を講じなければならない。

### 7.2.6　内部ネットワーク間の接続

学校園情報セキュリティ管理者及び学校園業務システム管理者は、他の内部ネットワークとの接続については、あらかじめ接続先の内部ネットワークの管理者と協議し、以下の内容を確認したうえで、接続しなければならない。

ア　接続によりそれぞれの情報資産に影響が生じないこと

イ　接続した場合のそれぞれの情報システムの責任範囲

ウ　障害発生時の対応体制

### 7.2.7　自動識別の設定

学校園情報セキュリティ管理者及び学校園業務システム管理者は、内部ネットワークで使用される機器について、機器固有情報等によって端末とネットワークとの

接続の可否が自動的に識別されるよう必要に応じてシステムを設定するものとする。

### 7.2.8　ログイン試行回数の制限等

学校園情報セキュリティ管理者及び学校園業務システム管理者は、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ学校園情報取扱者がログインしたことを確認することができるようにシステムを設定しなければならない。

### 7.2.9　認証情報の管理

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者は、学校園情報取扱者の認証情報を厳重に管理しなければならない。また、学校園情報取扱者のパスワードを発行する場合において、仮のパスワードを発行する場合、ログイン後直ちに仮のパスワードを変更させなければならない。認証情報ファイルを不正利用から保護するため、オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

イ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、教職員等のパスワードを発行する場合において、仮のパスワードを発行する場合、ログイン後直ちに仮のパスワードを変更させなければならない。

ウ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、仮のパスワードも含めパスワードを発行する場合、パスワードの長さ（原則として８文字以上）は十分な長さとし、文字列は他者が想像しにくいもの（英字（大文字・小文字区別有）、数字、記号を組み合わせたものなど）とする。

エ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、原則として特権IDのパスワードは定期的（原則として８文字以上）又は一定のアクセス回数経過後に変更し、古いパスワードを再利用しないものとする。

オ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、認証情報の不正利用を防止するための措置を講じなければならない。

### 7.2.10　インターネット上のサービスの利用

学校園情報管理者は、インターネット上で公開されている通信・ネットワークサービスを利用するにあたり、そのサービスで必要とされるネットワークプロトコル、ポート番号及び通信回線容量をサービス提供者に確認したうえで、学校園情報セキュリティ統括責任者の許可に基づき利用しなければならない。

### 7.2.11　児童生徒が個人所有するパソコン等の接続制限等

学校園情報セキュリティ管理者及び学校園業務システム管理者は、児童生徒が個人所有するパソコンや保護者所有であるモバイル端末等がアクセスする本市情報資産の範囲を、合理的理由を有する必要最低限のものに限定しなければならない。

## 7.3　システム開発、導入、保守等

### 7.3.1　情報システムの調達

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者は、情報システム開発、導入、保守等の調達にあたって、一般に公開する調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

イ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、調達した情報システムの情報セキュリティ対策を適切に推進・管理するための基礎資料として、情報システム台帳を作成し、学校園情報セキュリティ管理者に報告しなければならない。情報システムの更新・廃止等により情報システム台帳の記載内容に変更があった場合も同様とする。

ウ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、機器及びソフトウェアの調達にあたって、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

### 7.3.2　情報システムの開発

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者は、ネットワーク及び情報システムの開発、導入、更新及び運用保守にあたって、次の事項を定める。

(1) 責任者及び監督者
(2) 従事者及び作業範囲
(3) 開発するシステムと運用中のシステムとの分離
(4) 開発・保守に関する設計仕様等の成果物の提出
(5) セキュリティ上問題となり得るおそれのあるハードウェア及びソフトウェアの使用禁止
(6) アクセス制限
(7) 機器の搬入出の際の許可及び確認
(8) 記録の提出義務
(9) 仕様書・マニュアル等の定められた場所への保管
(10) 情報システムに係るソースコードの適切な方法での保管
(11) 開発・保守を行った者の利用者ID、パスワード等の当該開発・保守終了後に不要となった時点での速やかな抹消
(12) 情報システムセキュリティ実施手順書等の整備

イ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、ネットワーク及び情報システムの開発、導入、更新及び運用保守にあたって、不正にコピーしたソフトウェア及び個人所有のソフトウェアを導入又は使用等、問題のある行為が発生しないようにしなければならない。

ウ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、ネットワ

ーク及び情報システムの開発、導入、更新及び運用保守にあたって、コンピュータウイルス等対策ソフトウェアを導入する等、ウイルス感染やサイバー攻撃による情報漏えい等が発生しないようにしなければならない。

### 7.3.3 情報システムの導入

ア　リスクの把握

学校園情報セキュリティ管理者及び学校園業務システム管理者は、導入するシステムやサービスのリスクの把握に努めなければならない。

イ　開発環境と運用環境の分離及び移行手順の明確化

(1) 学校園情報セキュリティ管理者及び学校園業務システム管理者は、システム開発・保守計画の策定時に情報システムの移行手順を明確にしなければならない。

(2) 学校園情報セキュリティ管理者及び学校園業務システム管理者は、システム開発保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

(3) 学校園情報セキュリティ管理者及び学校園業務システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

(4) 学校園情報セキュリティ管理者及び学校園業務システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

(5) 学校園情報セキュリティ管理者及び学校園業務システム管理者は、導入するシステムやサービスのリスクを把握し、適切にコントロールされていることを確認した上で導入しなければならない。

ウ　テスト

(1) 学校園情報セキュリティ管理者及び学校園業務システム管理者は、新たに情報システムを導入する際には、既に稼働している情報システムに接続する前に、十分な試験を行わなければならない。

(2) 学校園情報セキュリティ管理者及び学校園業務システム管理者は、擬似環境による動作確認後を行わなければならない。また、作業については、作業経過を確認しながら実施するとともに、作業内容を記録しなければならない。

(3) 学校園情報セキュリティ管理者及び学校園業務システム管理者は、原則として個人情報及び機密性の高い生データを試験データに使用してはならない。ただし、合理的な理由がある場合で、学校園情報セキュリティ統括責任者が許可した場合は、この限りではない。

(4) 情報システム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなけ

ればならない。

(5) 学校園情報セキュリティ管理者及び学校園業務システム管理者は、試験に使用したデータ及びその結果を一定期間厳重に管理しなければならない。

### 7.3.4 システム開発・保守に関する資料等の整備・保管

ア 学校園情報セキュリティ管理者及び業務システム管理者は、システム開発・保守に関連する資料及びシステム関連文書を適正に整備･保管しなければならない。

イ 学校園情報セキュリティ管理者及び学校園業務システム管理者は、担当するシステムにおいて行ったシステム変更等の作業やテスト結果については､教職員等による十分な検証が行われその結果が上長により承認された作業記録を作成しなければならない。作成した作業記録は、窃取、改ざん等をされないように適切に管理を行わなければならない。

ウ 学校園情報セキュリティ管理者及び学校園業務システム管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

### 7.3.5 情報システムにおける入出力データの正確性の確保

ア 学校園情報セキュリティ管理者及び学校園業務システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を必要に応じて組み込むように情報システムを設計しなければならない。

イ 学校園情報セキュリティ管理者及び学校園業務システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

ウ 学校園情報セキュリティ管理者及び学校園業務システム管理者は、情報システムから出力されるデータは、保存された情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

### 7.3.6情報システムの変更管理

学校園情報セキュリティ管理者及び業務システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

### 7.3.7 ソフトウェアの保守及び更新

学校園情報セキュリティ管理者及び学校園業務システム管理者は、ソフトウェア等を更新、又は修正プログラムを導入する場合、不具合及び他のシステムとの相性の確認を行い、計画的に更新し又は導入しなければならない。

また、情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムについては、学校園情報セキュリティ管理者及び学校園業務システム管理者は、速やかに対応を行わなければならない。

### 7.3.8 システム更新又は統合時の検証等

学校園情報セキュリティ管理者及び学校園業務システム管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

#### 7.3.9 委託業務等従事者の身分確認

学校園情報セキュリティ管理者及び学校園業務システム管理者は、作業前に委託業務等従事者に対して身分証明書の提示を求め、契約で定められた資格を有するものが作業に従事しているか確認をすることができるようにしておかなければならない。

### 7.4 不正プログラム対策

#### 7.4.1 学校園情報セキュリティ管理者の措置事項

学校園情報セキュリティ管理者は、次の事項を措置しなければならない。

ア　コンピュータウイルス等の情報について学校園情報取扱者に対する注意喚起を行う。

イ　常時コンピュータウイルス等に関する情報収集に努める。

ウ　コンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものに保たせるよう指導等を行う。

#### 7.4.2 学校園情報資産管理責任者の措置事項

学校園情報資産管理責任者は、必要に応じて、次の事項を措置しなければならない。

ア　所管するサーバ及び端末に、コンピュータウイルス等対策ソフトウェアを常駐させなければならない。ただし、再起動により環境復元するソフトウェアが導入されている場合はこの限りではない。

イ　情報システムにおいて電磁的記録媒体を使用する場合、学校園が管理しているものを学校園情報取扱者に使用させるとともに、当該媒体の使用にあたり、ウイルスチェックを行わせなければならない。

ウ　コンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものに保たなければならない。インターネットに接続していないシステムにおいても、定期的に当該ソフトウェア及び定義ファイルの更新を実施しなければならない。

エ　業務で利用するソフトウェアには、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを原則として利用してはならない。

オ　コンピュータウイルス対策ソフトウェア等の設定変更権限については、一括管理し、学校園情報管理者が許可した教職員を除く教職員等に当該権限を付与してはならない。

#### 7.4.3 学校園情報取扱者の遵守事項

学校園情報取扱者は、次の事項を遵守しなければならない。

ア　端末において、コンピュータウイルス等対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更しない。

イ　外部ネットワーク及び電磁的記録媒体からデータ又はソフトウェアを取り入れる際には、必ずコンピュータウイルス等対策ソフトウェアによるチェックを行う。

ウ　外部ネットワーク及び電磁的記録媒体へデータ又はソフトウェアを送信・書き込みする際には、必ずコンピュータウイルス等対策ソフトウェアによるチェックを行う。

エ　差出人が不明であるなど、不審な電子メールを受信した場合は速やかに削除する。

オ　端末に対して、コンピュータウイルス等対策ソフトウェアによる完全スキャンを定期的に行い、スキャンの実行を途中で止めない。

カ　学校園情報セキュリティ管理者が提供するコンピュータウイルス等の情報を常に確認する。

キ　添付ファイルのあるメールを送受信する場合は、コンピュータウイルス等対策ソフトウェアでチェックを行う。

ク　コンピュータウイルス等に感染したおそれがある場合は、LANケーブルの即時取り外し又は端末の通信機能の停止等、他への感染を防止する措置を講じるとともに、速やかに学校園情報管理者等権限のある者に報告する。

ケ　端末には、業務に必要なソフトウェアのみをインストールするとともに、端末に導入されているソフトウェアについて、学校園情報セキュリティ管理者等から最新版へのアップデートの指示等があったときは、速やかにその指示に従う。

### 7.4.4　専門家の支援体制

学校園情報セキュリティ統括責任者は、実施しているコンピュータウイルス等対策では不十分な事態が発生した場合に備え、コンピュータウイルス等対策ソフトのサポート契約を締結する等、外部の専門家の支援を受けられるようにしておかなければならない。

## 7.5　不正アクセス対策

### 7.5.1　使用されていないポートの閉鎖等

学校園情報セキュリティ管理者及び学校園業務システム管理者は、所管するシステムにおいて、不正なアクセスによる影響を防止するため、以下の措置を講じなければならない。

ア　使用されていないポートを閉鎖する。

イ　サーバ上の不要なサービスについて、機能を削除又は停止しなければならない。

ウ　不正アクセスによるデータの書換えを検出する等、Webサイトの改ざんを防止しなければならない。

エ　ソフトウェアにセキュリティホールが発見された場合は、速やかに修正プログラムを適用しなければならない。

オ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

### 7.5.2　攻撃への対処

学校園情報セキュリティ管理者及び学校園業務システム管理者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合には、システムの停止を含む必要な措置を講じなければならない。また、警察・関係機関との連絡を密にして情報の収集に努めなければならない。

### 7.5.3　記録の保存

CISO及び学校園情報セキュリティ統括責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察・関係機関との緊密な連携に努めなければならない。

### 7.5.4　内部からの攻撃

学校園情報セキュリティ管理者及び学校園業務システム管理者は、学校園情報取扱者が使用している端末からの学校園のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

### 7.5.5　学校園情報取扱者による不正アクセス

学校園情報セキュリティ管理者及び学校園業務システム管理者は、学校園情報取扱者による不正アクセスを発見した場合、当該学校園情報取扱者が所属する学校園の学校園情報管理者に通知し、適切な措置を求めなければならない。

### 7.5.6　サービス不能攻撃

学校園情報セキュリティ管理者及び学校園業務システム管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

### 7.5.7　標的型攻撃

学校園情報セキュリティ管理者及び学校園業務システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、研修・啓発や自動再生無効化等の人的対策・入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

### 7.6 セキュリティ情報の収集

#### 7.6.1 セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

学校園情報セキュリティ管理者は、セキュリティホール等のセキュリティに関する情報を収集し、必要に応じ関係者間で情報を共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

#### 7.6.2 不正プログラム等のセキュリティ情報の収集・周知

学校園情報セキュリティ管理者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、学校園情報取扱者に周知しなければならない。

#### 7.6.3 情報セキュリティに関する情報の収集及び共有

学校園情報セキュリティ管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

## 8. 運用面のセキュリティ

### 8.1 情報システムの監視

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者は、セキュリティに関する事象を検知するため、情報システムの監視を行わなければならない。

イ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、重要なアクセスログ等を取得するサーバの正確な時刻設定又はサーバ間の時刻同期ができる措置を施さなければならない。

ウ　学校園情報セキュリティ管理者及び学校園業務システム管理者は、外部ネットワークと接続するシステムを稼働中、常時監視しなければならない。

### 8.2 情報セキュリティポリシーの遵守状況の確認

#### 8.2.1 遵守状況の確認及び対処

ア　学校園情報資産管理責任者は、情報セキュリティポリシー及びこれに基づく文書の遵守状況について常に確認を行い、問題を認めた場合には速やかに学校園情報セキュリティ管理者に報告しなければならない。

イ　学校園情報セキュリティ管理者は、発生した問題について、適切かつ速やかに対処しなければならない。

ウ　学校園情報資産管理責任者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシー及びこれに基づく文書の遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

#### 8.2.2 端末及び電磁的記録媒体等の利用状況調査

学校園情報資産管理責任者は、犯罪捜査への協力、不正アクセス、不正プログラム、情報漏えい等の調査のために、教職員等が使用している端末及び電磁的記録媒体等のログ、電子メールの送受信記録・内容等の利用状況を調査することができる。

#### 8.2.3 教職員等の報告義務

ア　学校園情報取扱者は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに学校園情報セキュリティ管理者及び学校園情報管理者に報告を行わなければならない。

イ　当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると学校園情報セキュリティ統括責任者が判断した場合において、学校園情報取扱者は、緊急時対応手順書に従って適正に対処しなければならない。

#### 8.2.4 セキュリティポリシー等の閲覧

学校園情報資産管理責任者は、教職員が常に情報セキュリティポリシー及びこれに基づく文書を参照できるよう配慮しなければならない。

### 8.3 管理者権限の代行

学校園情報資産管理責任者の権限を代行する者は、それぞれが指名する。

### 8.4 侵害時の対応

#### 8.4.1 情報セキュリティインシデント発生時の対応手順書の策定

学校園情報セキュリティ管理者及び学校園業務システム管理者は、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において、連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、情報セキュリティインシデント発生時の対応手順書を定めておき、セキュリティ侵害時には当該手順書に従って適正に対処しなければならない。

#### 8.4.2 緊急時対応計画に盛り込むべき内容

情報セキュリティインシデント発生時の対応手順書には、以下の内容を定めなければならない。

ア　緊急時連絡網

イ　意思決定の所在

ウ　発生した事象に係る報告すべき事項

エ　発生した事象への対応措置

オ　再発防止措置の策定

#### 8.4.3 緊急連絡網に盛り込むべき内容

緊急時の連絡先（所属、役職、電話番号、電子メールアドレス等）及び連絡順序がわかるように記載する。内部や委託先だけでなく、警察・関係機関も記載されていることが望ましい。

#### 8.4.4 業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、学校園情報セキュリティ責任者は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

#### 8.4.5 情報セキュリティインシデント発生時の対応手順書の見直し

学校園情報セキュリティ管理者及び学校園業務システム管理者は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて情報セキュリティインシデント発生時の対応手順書の規定を見直さなければならない。

### 8.5 例外措置

#### 8.5.1 例外措置の許可

学校園情報資産管理責任者は、情報セキュリティポリシーを遵守することが困難な状況で、学校業務の適正な遂行を継続するため、遵守事項とは異なる方法を採用する又は遵守事項を実施しないことについて合理的な理由がある場合には、CISOの許可を得て、例外措置を講じることができる。なお、学校園情報セキュリティ統括責任者が、軽微な例外措置と判断したものについては、学校園情報セキュリティ統括責任者が許可することにより、例外措置を講じることができる。

#### 8.5.2 緊急時の例外措置

学校園情報資産管理責任者は、前項に該当する場合であって、学校業務の遂行に緊急を要し、前項に定める許可を得る時間的な猶予のないときは、例外措置を実施し、実施後速やかにCISO及び学校園情報セキュリティ統括責任者に報告しなければならない。

#### 8.5.3 例外措置の申請書等の管理

CISOは、例外措置の申請書、報告書及び審査結果を適切に保管させなければならない。

### 8.6 法令の遵守

教職員は、職務の遂行において使用する情報資産を保護するために、以下の法令のほか関係法令等を遵守しこれに従わなければならない。

ア　教育公務員特例法（昭和24年法律第１号）
イ　地方公務員法（昭和25年法律第261号）
ウ　不正アクセス行為の禁止等に関する法律（平成11年法律第128号）
エ　著作権法（昭和45年法律第48号）
オ　個人情報の保護に関する法律（平成15年法律第57号）
カ　行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号）
キ　行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）
ク　サイバーセキュリティ基本法（平成26年法律第104号）
ケ　神戸市個人情報保護条例（平成９年10月条例第40号）

コ　神戸市教育委員会電子計算機処理に係るデータ保護管理規程（平成21年４月教委訓令甲第１号）

サ　神戸市教育委員会公文書管理規程（昭和43年３月教委訓令甲第３号）

### 8.7　懲戒処分

#### 8.7.1　懲戒処分

情報セキュリティポリシー及びこれに基づく文書に違反した教職員及びその監督責任者は、その重大性、発生した事象の状況等に応じて、地方公務員法による懲戒処分の対象となる。

#### 8.7.2　再発防止の指導等

学校園情報取扱者に情報セキュリティポリシー及びこれに基づく文書に違反する行為がみられた場合には、学校園情報資産管理責任者は、速やかに次の措置を講じなければならない。

ア　再発防止の指導その他適切な措置

当該学校園情報取扱者に対して違反する行為の事実を通知し、再発防止の指導その他適切な措置を行う。

イ　使用権の停止・剥奪

指導等によっても改善されない場合、当該学校園情報取扱者の情報資産の使用権を停止あるいは剥奪する。

ウ　報告

違反する行為が生じた場合、違反する行為の内容、指導内容その他措置の状況について学校園情報セキュリティ管理者に報告する。

## 9.　外部サービスの利用

### 9.1　外部委託

#### 9.1.1　外部委託事業者の選定基準

特定個人情報を扱う業務又はネットワーク及び情報システムの開発･保守並びにデータ処理その他情報処理に係る業務を外部委託する場合は、委託先の選定にあたり、委託内容に応じた情報セキュリティ対策の実施が確保されることを確認しなければならない。

#### 9.1.2　契約書の記載事項

ア　特定個人情報を扱う業務又はネットワーク及び情報システムの開発・保守並びにデータ処理その他情報処理に係る業務を外部委託する場合は、当該委託先事業者との間で、下記事項を明記した契約を締結しなければならない。

(1) データその他業務上知り得た情報（以下「データ等」という）の秘密の保持に関する事項

(2) 第三者への委託（以下、「再委託」という。）の禁止又は制限に関する事項

(3) データ等の目的以外の目的のための使用及び第三者への提供の禁止に関する事項
(4) データ等の複写及び複製の禁止に関する事項
(5) データ等の取扱いに関する事故の発生時における報告義務に関する事項
(6) データ等の取扱いに関する検査の実施に関する事項
(7) 契約に違反した場合における契約の解除及び損害賠償に関する事項
(8) 委託業務終了時の情報資産の返還、廃棄等に関する事項
(9) 情報セキュリティポリシー及びこれに基づく文書の遵守に関する事項
(10)事故時等の公表に関する事項
(11)委託先の責任者、委託内容、従事者、作業場所の特定に関する事項
(12)委託先の責任者及び従事者に対する研修の実施に関する事項
(13)情報セキュリティ確保への取り組みの実施状況に係る報告義務に関する事項

イ　前項に加えて、次に掲げる事項を必要に応じて契約書等に明記するよう努めるものとする。
(1) 提供されるサービスレベルの保証に関する事項
(2) 委託業務の定期報告及び緊急時報告義務に関する事項
(3) 外部施設等への情報資産の搬送時における紛失、盗難、不正コピー等の防止に関する事項

### 9.1.3　確認・措置等

学校園情報セキュリティ管理者及び学校園業務システム管理者は、当該委託先事業者の情報セキュリティ確保への取組みの実施状況等について、定期的若しくは随時、調査を行い、安全を確保しなければならない。学校園情報セキュリティ責任者から内容の報告を求められた場合には、報告を行わなければならない。

### 9.1.4　再委託等

再委託（再々委託を含む）を受ける事業者がある場合、9.1.2及び9.1.3に定める事項は再委託（再々委託を含む）を受ける事業者にも適用する。ただし、再委託先として電気・ガス・空調等のビル等建築物の管理サービス、運送サービス、印刷・出版及び教育・研修等に関する業務を再委託する場合は除くものとする。

## 9.2　約款による外部サービスの利用

ア　利用規約等に同意して利用する外部サービス（民間事業者等が規定した約款に基づきインターネット上で提供される情報処理サービス。ただし、9.4に規定された内容を踏まえて選定されたクラウドサービスを除く。）では、原則として機密性2B以上の情報を扱ってはならない。ただし、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたもので学校園情報セキュリティ統括責任者が認めたものはこの限りではない。

イ　利用規約等に同意して利用する外部サービスにて機密性2B以上の情報を取扱う場合には学校園情報セキュリティ管理者の許可を得なければならない。

### 9.3　ソーシャルメディアサービスの利用

ア　本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を行うこと。

イ　パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（IC カード等）等を適切に管理するなどの方法で、不正アクセス対策を行うこと。

ウ　機密性 2A 以上の情報はソーシャルメディアサービスで発信してはならない。

エ　利用するソーシャルメディアサービスごとの責任者を定めなければならない。

オ　アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。

### 9.4　クラウドサービスの利用

ア　学校園業務システム管理者は、クラウドサービス（民間事業者が提供するものに限らず、本市が自ら提供するもの等を含む。以下同じ。）を利用するにあたり、取扱う情報資産の分類及び分類に応じた取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断しなければならない。

イ　学校園業務システム管理者は、クラウドサービスで取扱われる情報に対して国内法以外の法令が適用されるリスクを評価して事業者を選定し、必要に応じて実施場所及び契約に定める準拠法・裁判管轄を指定しなければならない。

ウ　学校園業務システム管理者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、事業者を選定する際の要件としなければならない。

エ　学校園業務システム管理者は、クラウドサービスの特性を考慮した上で、多段階認証又は多要素認証の導入や操作ログの保存等、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、セキュリティ要件を定めなければならない。

オ　学校園業務システム管理者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービス提供事業者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

カ　学校園業務システム管理者は、上記アからオに定める事項を踏まえ、学校園情報セキュリティ管理者にクラウドサービス利用の可否を問わなければならない。

## 10. 学習用パソコンにおける情報セキュリティ

児童生徒に支給する学習用パソコンにおける情報セキュリティ対策について規定す

る。なお児童生徒が個人所有する端末及びこれに準じる端末は対象としない。

また学習用パソコンの情報セキュリティ対策のうち、設定、運用等に関する権限及び責任は学校園情報セキュリティ管理者が有し、所管する学校園における情報モラル教育等に関する権限及び責任は学校園情報管理者が有する。

## 10.1 学習用パソコンの情報セキュリティ対策

### 10.1.1 不適切なウェブページの閲覧防止

学校園情報セキュリティ管理者は、児童生徒が学習用パソコンを利用する際に不適切なウェブページの閲覧を防止する対策を講じなければならない。

また学校園情報管理者は学習用パソコンで閲覧可能な不適切なウェブページを知り得た場合には、学校園情報セキュリティ管理者に情報提供しなければならない。

### 10.1.2 マルウェア感染対策

学校園情報セキュリティ管理者は、学校園内外での学習用パソコンの利用におけるマルウェア感染対策を講じなければならない。

### 10.1.3 不適切な利用の防止

学校園情報セキュリティ管理者は、学習用パソコンの情報セキュリティ状態の監視に加えて、不適切なアプリケーションやコンテンツの利用を制限し、安全・安心な利用環境を維持しなければならない。また学校園情報管理者は、児童生徒に対して学習用パソコンの不適切な利用等に関する情報モラル教育を定期的に行わなければならない。

### 10.1.4 セキュリティ設定の一元管理

学校園情報セキュリティ管理者は、児童生徒への学習用パソコン配布後においても、学習用パソコンのセキュリティ設定やOSアップデート、ウェブブラウザのアップデート、学習用パソコンの利用履歴確認などについて、離れた場所からでも一元管理できるようにしなければならない。

### 10.1.5 端末の盗難・紛失時の情報漏洩対策

学校園情報セキュリティ管理者は、児童生徒が学習用パソコンを紛失しても、遠隔操作でロックをかける、あるいはデータ消去することで第三者による不正操作や情報漏洩を防ぐ等の安全管理措置を講じなければならない。

### 10.1.6 運用・連絡体制の整備

学校園情報セキュリティ管理者は、学校園内外での学習用パソコンの運用ルールを制定し、紛失、盗難等のインシデント発生時における対応方法を各学校園に周知しなければならない。

## 10.2 児童生徒用ID及びパスワードの管理

学校園情報セキュリティ管理者は児童生徒用ID及びパスワードの管理に関し、次の事項を遵守しなければならない。

ア　ID及びパスワードは教育委員会事務局にて一元管理する。

イ　校種間の進学を除き、進級時に ID の変更が不要となるよう定める。
ウ　転出や卒業、退学時には、ID の利用停止後、ID 及び関連するデータの削除を行う。

# 11. 評価・改善・見直し

## 11.1　監査

### 11.1.1　実施方法

CISO は、学校園情報セキュリティ監査統括責任者に命じ、情報セキュリティ対策状況について、定期的及び必要に応じて監査を行わせなければならない。

### 11.1.2　監査を行う者の要件

ア　学校園情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査学校園から独立した者に対して、監査の実施を依頼しなければならない。

但し、学校園情報セキュリティ管理者が認める場合、過去に被監査学校園に所属していた者でも監査を実施することができる。

イ　監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

### 11.1.3　監査実施計画の立案及び実施への協力

ア　学校園情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を策定し、CISOに報告しなければならない。

イ　被監査学校園は、監査の実施に協力しなければならない。

### 11.1.4　外部委託先事業者に対する監査

学校園情報セキュリティ監査統括責任者は、委託先事業者に対して、委託先事業者からの再委託（再々委託含む）の事業者も含めて、情報セキュリティポリシーの遵守について監査を定期的及び必要に応じて行わなければならない。

### 11.1.5　監査の報告

学校園情報セキュリティ監査統括責任者は、監査結果を取りまとめ、CISOに報告する。

### 11.1.6　保管

学校園情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を紛失等が発生しないように適切に保管しなければならない。

### 11.1.7　監査結果への対処

CISOは、監査結果を踏まえ、指摘事項に関係する学校園情報管理者等に対し、当該事項への対処を指示しなければならない。また、指摘事項に関係しない学校園情報管理者等に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。なお、学校園で横断的な改善が必要な事項については、学校園情報セキュリティ責任者に対し、当該事項への対

処を指示しなければならない。

#### 11.1.8　情報セキュリティポリシー及び関係規程等の見直し等への活用

CISOは、情報セキュリティポリシー等情報セキュリティ対策の見直し時に監査結果を活用しなければならない。

### 11.2　自己点検

#### 11.2.1　実施方法

ア　学校園情報セキュリティ管理者及び学校園業務システム管理者は、所管するネットワーク及び情報システムの情報セキュリティ対策状況について、定期的及び必要に応じて自己点検を実施しなければならない。

イ　学校園情報管理者は、所管する学校園の情報セキュリティポリシーに沿った情報セキュリティ対策状況について、定期的及び必要に応じて自己点検を行わなければならない。

ウ　学校園情報セキュリティ管理者がセキュリティ事故の増加などによりセキュリティ事故事例をとりあげた事例研修の実施が効果的であると判断した場合、セキュリティ事故事例の事例研修を自己点検の実施と兼ねることができる。

#### 11.2.2　報告

ア　学校園情報資産管理責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、学校園情報セキュリティ責任者に報告しなければならない。

イ　学校園情報セキュリティ責任者は、報告を受けた点検結果及び改善策を学校園情報セキュリティ統括責任者に報告し、CISOに報告しなければならない。

#### 11.2.3　自己点検結果の活用

ア　学校園情報取扱者は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

イ　CISOは、情報セキュリティポリシー等情報セキュリティ対策の見直し時に点検結果を活用しなければならない。

#### 11.2.4　改善

**ア　是正措置**

学校園情報資産管理責任者は、業務上発見された問題、保護者等からの指摘による問題、監査及び自己点検において指摘された問題等に対する再発防止のため、その原因を除去するための措置を施さなければならない。

**イ　予防措置**

学校園情報資産管理責任者は、業務上予見される問題、他の組織で発生したものと同種の情報セキュリティ事件・事故等を未然に防止するため、その原因を除去するための措置を施さなければならない。

### 11.3　情報セキュリティポリシー及び関係規程等の見直し

CISOは、監査及び自己点検の結果、改善の状況、残留リスク、情報セキュリティに関

する状況の変化等を踏まえ、必要があると認めた場合、情報セキュリティポリシー等情報セキュリティ関連文書の見直しを行う。

### 11.4　情報セキュリティ個別基準の策定

学校園情報セキュリティ統括責任者は、情報セキュリティポリシーを補完するために必要な学校園共通の事項に関して、具体的な内容を定めた情報セキュリティ個別基準を策定する。

### 11.5　情報セキュリティ実施手順の策定

学校園情報セキュリティ統括責任者は、情報セキュリティポリシーに基づき、所管するシステム等に対する情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定させなければならない。