第1章　総則

1.目的

本方針は、八丈町教育委員会（以下「教育委員会」という。）および八丈町立小中学校（以下「学校」という。）が取り扱う教育情報及び校務情報（以下「教育情報等」という。）の機密性・完全性・可用性を確保し、もって教育活動の適正かつ円滑な実施並びに児童生徒及び教職員等の権利利益の保護を図ることを目的とする。

2.適用範囲

⑴行政機関等

本対策基準が適用される行政機関等は、教育委員会及び学校とする。

⑵情報資産の範囲

本方針は、電子的情報、紙媒体、クラウドサービス、ネットワーク、端末・周辺機器、ログ等、教育委員会及び学校が管理し、又は利用する一切の情報資産に適用する。

3.基本方針

1　教育情報等の取扱いに当たっては、ゼロトラストセキュリティの考え方に基づき、最小権限及び多要素認証の徹底、アクセス主体（ID）・端末の健全性・利用状況等のコンテキストに応じた認可を行う。

2　クラウドサービスの利用を原則とし、第三者認証、約款及びデータ所在の確認、監査ログの取得・保存、可用性の確保等、必要なセキュリティ要件を満たすものを採用する。

3　情報資産はその重要度に応じて分類し、共有範囲、外部提供、持出し、保存年限及び記録・監査の要件を明確化する。

4　教育情報等の保護と教育の質の向上の両立を図るため、生成AI等の新技術の活用を推進しつつ、入力情報の適正管理、生成物の検証及び記録の整備を行う。

5　本方針の実効性を担保するため、自己点検・内部監査、研修・周知、演習を計画的に実施し、継続的改善を図る。

4.用語の定義

⑴校務系情報

学校が保有する情報資産のうち、それらの情報を学校・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

⑵学習系情報

学校が保有する情報資産のうち、それらの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

⑶校務用端末

校務系情報にアクセス可能な端末

⑷学習者用端末

学習系情報にアクセス可能な端末で、児童生徒が利用する端末

⑸指導者用端末

学習系情報にアクセス可能な端末で、教員のみが利用する端末

5.組織体制

⑴最高情報セキュリティ責任者（CISO:Chief Information Security Officer、以下「CISO」という。）

①副町長を、CISOとする。CISOは、本市における全ての教育ネットワーク、教育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。

②CISO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した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。

⑵統括教育情報セキュリティ責任者

①教育長を、CISO直属の統括教育情報セキュリティ責任者とする。統括教育情報セキュリティ責任者はCISOを補佐しなければならない。

②統括教育情報セキュリティ責任者は、本町の全ての教育ネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③統括教育情報セキュリティ責任者は、本町の全ての教育ネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

④統括教育情報セキュリティ責任者は、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者及び教育情報システム担当者に対して、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。

⑤統括教育情報セキュリティ責任者は、本町の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セキュリティ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。

⑥統括教育情報セキュリティ責任者は、本町の共通的な教育ネットワーク、教育情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

⑦統括教育情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、統括教育情報セキュリティ責任者、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者、教育情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

⑧統括教育情報セキュリティ責任者は、緊急時にはCISOに早急に報告を行うとともに、回復のための対策を講じなければならない。

⑶教育情報セキュリティ責任者

①教育課長を教育情報セキュリティ責任者とする。

②教育情報セキュリティ責任者は、本町の教育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。

③教育情報セキュリティ責任者は、本町において所有している教育情報システムにおける開発、設定の変更、運用、見直し等を行う際の情報セキュリティに関する統括的な権限及び責任を有する。

④教育情報セキュリティ責任者は、本町において所有している教育情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約及び教職員等（臨時的任用教職員、非常勤講師を含めた教職員全員をいう。以下同じ。）に対する教育、訓練、助言及び指示を行う。

⑷教育情報セキュリティ管理者

①校長を、教育情報セキュリティ管理者とする。

②教育情報セキュリティ管理者は当該学校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。

③教育情報セキュリティ管理者は、当該学校において、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セキュリティ侵害のおそれがある場合には、教育情報セキュリティ責任者、統括教育情報セキュリティ責任者及びCISOへ速やかに報告を行い、指示を仰がなければならない。

⑸教育情報システム管理者

①教育課庶務係長を、教育情報システムに関する教育情報システム管理者とする。

②教育情報システム管理者は、所管する教育情報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。

③教育情報システム管理者は、所管する教育情報システムにおける情報セキュリティに関する権限及び責任を有する。

④教育情報システム管理者は、所管する教育情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

⑹教育情報システム担当者

①教育課庶務係職員を、教育情報システムに関する教育情報システム担当者とする。

②教育情報システム担当者は、教育情報システム管理者の指示等に従い、教育情報システムの開発、設定の変更、運用、更新等の作業を行う。

⑺情報セキュリティ委員会

①本町の情報セキュリティ対策を統一的に行うため、CISO、CIO、統括教育情報セキュリティ責任者、教育情報セキュリティ責任者、教育情報セキュリティ管理者及びCISOが別途選任した者から構成される情報セキュリティ委員会を設置し、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。

②情報セキュリティ委員会は、毎年度、本町における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。

⑻兼務の禁止

①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。

②監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

⑼情報セキュリティに関する統一的な窓口の設置

①CISOは、情報セキュリティインシデントの統一的な窓口の機能を有する組織を整備し、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には、その状況を確認し、自らへの報告が行われる体制を整備する。

②統括教育情報セキュリティ責任者は、当該情報セキュリティインシデントに対して、その重大性・緊急性に鑑みて教育委員会 CSIRT（以下「CSIRT」という。）を設置することができる。

③CSIRTの責任者は統括教育情報セキュリティ責任者とし、統括教育情報セキュリティ責任者は、緊急時対応計画に基づき CSIRT 内の業務統括及び外部との連携等を行う職員等を定めなければならない。

④統括教育情報セキュリティ責任者は、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の意見を聴くことができる。

⑤CSIRTは、情報セキュリティインシデントを認知した場合には、CISO に報告するとともに、必要に応じて市長部局の情報セキュリティ担当部署と連携しなければならない。

⑥CSIRTは、その情報セキュリティインシデントの重要性・規模等を勘案し、国や東京都等の関係機関へ報告しなければならない。

⑦CSIRTは、情報セキュリティインシデントを認知した場合には、その重要度や影響範囲を勘案し、報道機関への通知・公表対応を行わなければならない。

⑧CSIRTは、日頃から情報セキュリティに関して、町長部局の情報セキュリティ担当部署の他、関係機関や外部の事業者等との情報共有を行わなければならない。

⑽教職員等

①臨時的任用教職員、非常勤講師を含めた教職員全員を、教職員等と称する。

②教職員等は学校が所管する情報資産を取り扱う立場にあり、教育情報セキュリティ管理者の指導の下、情報セキュリティを遵守しなければならない。

⑾教育委員会事務局職員

①教育ネットワークを利用して、学校が所管する情報にアクセスできる教育委員会事務局職員を指す。

②教育委員会事務局職員は学校の情報資産にアクセスできる立場にあり、教育情報セキュリティ責任者の指導の下、情報セキュリティを遵守しなければならない。

第2章　情報資産の分類と管理方法

1.情報資産の分類

本町における情報資産は、機密性、完全性及び可用性の3つの観点から影響度を評価し、次のとおり4段階の重要性分類を行い、必要に応じて取扱制限を行うものとする。

重要性分類
Ⅰ セキュリティ侵害が教職員等、児童生徒及び保護者の生命、財産、プライバシー 等へ重大な影響を及ぼす。 Ⅱ セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす。(Ⅰを除く。) Ⅲ セキュリティ侵害が学校事務及び教育活動の実施に影響を及ぼす。(Ⅱ以上を除く。) Ⅳ セキュリティ侵害が学校事務及び教育活動の実施に影響をほとんど及ぼさない。(Ⅲ以上を除く。)

機密性による情報資産の分類

分類	分類基準	該当する情報資産のイメージ
機密性3	学校で取り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	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
機密性2B	学校で取り扱う情報資産のうち、秘密文書に相当する機密性は要し ないが、直ちに一般に公表するこ 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。)
機密性2A	学校で取り扱う情報資産のうち、直ちに一般に公表することを前提 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。)
機密性1	機密性2A、機密性2B又は機密 性3の情報資産以外の情報資産	公表されている情報資産又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。)

完全性による情報資産の分類

分類	分類基準	該当する情報資産のイメージ
完全性2B	学校で取り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、破損又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
完全性2A	学校で取り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、破損又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
完全性1	完全性2A又は完全性2Bの情報 資産	事故があった場合でも業務の遂行に

	以外の情報資産	支障がない情報

可用性による情報資産の分類

分類	分類基準	該当する情報資産のイメージ
可用性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
可用性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
可用性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

2.情報資産の管理

①管理責任

ア　統括教育情報セキュリティ責任者は、教育情報システムとその運用管理を定めた教育情報セキュリティ対策基準を作成しなければならない。

イ　統括教育情報セキュリティ責任者は、教育情報セキュリティ対策基準に基づき、必要に応じて学校現場での情報セキュリティ運用管理に関する実施手順ひな形を作成しなければならない。

ウ　統括教育情報セキュリティ責任者は、学校で標準的に所管する情報資産につい て、分類を定義した標準情報資産台帳（以下「標準台帳」という。）を作成し、適 宜更新しなければならない。

エ　教育情報セキュリティ管理者は、実施手順ひな形に基づき、必要に応じて自校 の実施手順を作成しなければならない。

オ　教育情報セキュリティ管理者は、標準台帳に基づき、自校で所管する情報資産 を確認し、不足内容を補完した自校向け情報資産台帳を整備しなければならない。

カ　教育情報システム管理者及び教育情報セキュリティ管理者は、その所管する情 報資産について管理責任を有する。

キ　教育情報セキュリティ管理者は、教職員等の情報資産の取扱いに際し、自校向け情報資産台帳及び実施手順に基づいた運用管理を指導しなければならない。

ク　教職員等は、自校向け情報資産台帳及び実施手順に基づき、適切に情報資産を 取り扱わなければならない。

②情報資産の分類の表示
教職員等は、情報資産について、ファイルの属性や分類ラベルを利用して、情報資産の分類を明示し、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。

③情報の作成
ア　教職員等は、業務上、必要のない情報を作成してはならない。
イ　情報を作成する教職員等は、情報の作成時に第2章1の⑴の分類に基づき、当該情報の分類を定め、分類に準拠した取扱いを行わなければならない。
ウ　情報を作成する教職員等は、作成途上の情報についても、取扱いを許可されて いない者の閲覧や紛失・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情報資産の入手
ア　教職員等が作成した情報資産を入手した教職員等は、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　教職員等以外の者が作成した情報資産を入手した教職員等は、第2章1の⑴の分類に基づき、当該情報の分類を定め分類に準拠した取扱いを行わなければならない。
ウ　情報資産を入手した教職員等は、その情報資産の分類が不明な場合、教育情報 セキュリティ管理者に判断を仰がなければならない。

⑤情報資産の利用
ア　情報資産を利用する教職員等は、業務以外の目的で情報資産を利用してはならない。
イ　情報資産を利用する教職員等は、情報資産の分類に応じ、適切な取扱いをしな ければならない。
ウ　情報資産を利用する教職員等は、電磁的記録媒体又は保存されている領域（フ ォルダやサーバ）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、当該電磁的記録媒体又は保存されている領域を取り扱わなければならない。
エ　情報資産を利用する教職員等は、必要以上の複製及び配布をしてはならない。

⑥情報資産の保管
ア　教育情報セキュリティ管理者又は教育情報システム管理者の措置事項
（ア）教育情報セキュリティ管理者は、情報資産台帳に従って、情報資産の保管先を定め、教職員等に周知しなければならない。

（イ）教育情報システム管理者及び教育情報セキュリティ管理者は、情報資産を記録した USB メモリ等の外部電磁的記録媒体を保管する場合は、外部電磁的記録媒体への書込み禁止の措置を講じなければならない。

（ウ）教育情報システム管理者及び教育情報セキュリティ管理者は、教育情報シ ステムのバックアップで取得したデータを記録する電磁的記録媒体を保管する 場合は、自然災害を被る可能性が低い場所に保管しなければならない。なお、クラウドサービスを利用するときは、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。

（エ）教育情報システム管理者及び教育情報セキュリティ管理者は、重要性分類 Ⅲ以下の情報を記録した電磁的記録媒体を保管する場合には、耐火、耐震、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

イ　教職員等の遵守事項
（ア）教職員等は、教育情報セキュリティ管理者が指定した保管先にのみ情報資産を保管しなければならない。
（イ）教職員等は、児童生徒が生成する学習系情報の保管先について児童生徒に 指示し、それ以外の場所に保管しないよう指導しなければならない。

⑦情報資産の外部持出し
ア　分類に応じた情報資産の外部持出し制限
（ア）教職員等は、重要性分類Ⅱ以上の情報資産を外部持出しする場合は、制限されたアクセス措置設定（アクセス制限や暗号化）を行い、教育情報セキュリティ管理者の個別許可を得なければならない。なお、外部持出しツールに限定され たアクセスの措置設定（アクセス制限や暗号化）機能を有する場合には、有効にしなければならない。

（イ）重要性分類Ⅲの情報資産については、教職員等の外部持出しについて、教育情報セキュリティ管理者の判断で包括的許可を可とする。なお、外部持出しツールに限定されたアクセスの措置設定（アクセス制限や暗号化）機能を有する場合には、有効にしなければならない。

イ　電子メール、外部ストレージサービスによる情報の送信
情報資産が組織内部から組織外部（家庭や地域、事業者等）に電子メール等により外部送信される場合は、情報資産分類に応じ以下を実施しなければならない。

（ア）電子メールにより重要性分類Ⅲ以上の情報を外部に送信する者は、電子メールへ直接添付してはならない。外部ストレージサービスを利用し、限定されたアクセスの措置設定（アクセス制限や暗号化）を行わなければならない。

（イ）利用する電子メール、外部ストレージサービスは教育委員会又は学校から提供される公式サービスのみを利用し、私的に契約したサービスを利用してはならない。

ウ　外部電磁的記録媒体を用いた情報の外部持出し
USBメモリ等の物理的な媒体による情報の外部持ち出しは、紛失・盗難リスクを伴うことから、例外なく認めない。

エ　FAXによる情報の送信
FAXによる情報の送信は、限定されたアクセスの措置（アクセス制限や暗号化）が不可能であること、誤送信のリスクがあることに鑑み、送信相手がFAX 受信を指定してきた場合にのみ利用することが望ましい。

オ　情報資産の運搬
(ア) 車両等により重要性分類Ⅲ以上の情報資産を運搬する場合は、必要に応じ暗号化又はパスワードの設定を行う等の安全管理措置を講じ、宛名・ 差出名を明記して、厳重に封印しなければならない。

(イ) 重要性分類Ⅲ以上の情報資産を運搬する教職員等は、教育情報セキュリ ティ管理者に許可を得なければならない。

カ　情報資産の公表
(ア) 教育情報セキュリティ管理者は、公開する情報が正しい内容であることを事前に確認し、誤公開を防がなければならない。

(イ) 教育情報セキュリティ管理者は、住民に公開する情報資産について、改ざんや消去されないように定期的に確認しなければならない。

キ　情報資産の廃棄
(ア) 情報資産を廃棄する教育委員会事務局職員又は教職員等は、重要性分類Ⅲ以上の情報が記載された紙媒体の書類を廃棄する場合には、内容が復元できないように細断、熔解またはこれに準ずる方法にて廃棄しなけれ ばならない。

(イ) 情報を記録している電磁的記録媒体を利用しなくなった場合、情報を復元できないように処置した上で廃棄しなければならない。

(ウ) 情報資産の廃棄・リース返却を行う教育委員会事務局職員は教育情報シ ステム管理者の、教職員等は教育情報セキュリティ管理者の許可をそれぞれ得て、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。

(エ) 業者に廃棄委託する場合、廃棄する情報資産を業者が引き取る際、教育委員会事務局職員又は教職員等が立ち会わなければならない。

第3章　物理的セキュリティ

1.通信回線及び通信回線装置の管理

①統括教育情報セキュリティ責任者は、施設内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。

②統括教育情報セキュリティ責任者は、外部へのネットワーク接続ポイント及び該当ポイントに接続される端末を正確に把握し、適切な管理を行わなければなら ない。

③統括教育情報セキュリティ責任者は、重要性分類Ⅲ以上の情報資産を取り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上、適切な回線を選択しなければならない。また、インターネットを通信経路とする回線の場合、通信の暗号化を行わなければならない。

④統括教育情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、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を実施しなければならない。

⑤統括教育情報セキュリティ責任者は、重要性分類Ⅱ以上の情報資産を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。

⑥統括教育情報セキュリティ責任者は、学校運営上必要なネットワーク帯域を確保するとともに、遅延等に対する適切な対策を講じなければならない。クラウドサービ ス提供事業者側のサービス要件基準を満たす配慮を含めてネットワーク構成を設計する。また、運用開始前には十分検証し、利用状況に応じて定期的に改修計画を行うこと。

2.教職員等の利用する端末や電磁的記録媒体等の管理

①教育情報システム管理者は、不正アクセス防止のため、ログイン時のID及びパスワードによる認証、加えて多要素認証の実施等、使用する目的に応じた適切な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。

②教育情報システム管理者は、校務系システム、教育情報システムへアクセスする端末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。

③教育情報システム管理者は、取り扱う情報の重要度に応じてパスワード以外に生体認証や物理認証等の多要素認証を設定しなければならない。 特に、パブリッククラウド上で重要な情報（重要性分類Ⅱ以上）を取り扱う際には、多要素認証を含む強固なアクセス制御による対策を講じなければならない。 ただし、児童生徒またはその保護者が重要性分類Ⅱ以上の情報資産にアクセスする場合は、児童生徒本人またはその保護者が、当該児童生徒に関するもののみ にアクセスすることを想定していることから、多要素認証を設定することが望 ましいものの、パスワードの秘匿管理の徹底、複数回誤ったパスワードを入力した際のロック機能の有効化、パスワードの複雑性の確保等により本人確認を厳格に行う前提で、ID及びパスワードでの認証を許容する。

④教育情報システム管理者は、パソコンやモバイル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。端末に暗号化機能を持つセキュリ 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。同様に、電磁的記録媒体についても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教育情報システム管理者は、特に強固なアクセス制御による対策を講じたシステム構成の場合、重要性分類Ⅲ以上の情報資産を取り扱う端末に対し、当該データ 暗号化等の措置により、不正アクセスや教員の不注意等による情報流出への対策を講じなければならない。

⑥教育情報システム管理者は、端末の学校外での業務利用の際は、上記対策に加え、遠隔消去機能を利用する等の措置を講じなければならない。

⑦教育情報システム管理者は、パソコンやモバイル端末におけるマルウェア感染の脅威に対し、ウイルス対策ソフトの導入等の対策を講じなければならない。なお、OSによっては標準的にウイルス対策ソフトを備えている製品、OSとしてウイ ルス感染のリスクが低い仕組みとなっている製品などもあるため、実際に運用する端末において適切な対策を講じること。強固なアクセス制御による対策を講じたシステム構成の場合、重要性分類Ⅱ以上の情報資産を取り扱う端末に対し、当該端末の状況および通信内容を監視し、異常、あるいは不審な挙動を検知する仕組み（ふるまい検知）等の活用を検討し、適切な対策を講じること。

⑧教育情報システム管理者は、インターネットへ接続をする場合、教職員等のパソコン、モバイル端末に対して不適切なウェブページの閲覧を防止するWebフィルタリング等の対策を講じなければならない。

3.学習者用端末のセキュリティ対策

①児童生徒が端末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。

②学校内外での端末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。

③端末の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、常に安全で児童生徒が安心して利用できる状態を維持しなければならない。

④児童生徒への端末配布後においても、端末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、学習用ツールのインストール、端末の利用履歴も含めた状態確認などの作業を、離れた場所からでも一元管理できることが望ましい。

⑤児童生徒が端末を紛失しても、遠隔操作でロックをかける、あるいはワイプ（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。

第4章　人的セキュリティ

1. 教育情報セキュリティ管理者の措置事項

⑴情報資産の管理

①教育情報セキュリティ管理者は、教職員等による情報資産の外部持ち出しについて、記録管理しなければならない。

②情報資産の廃棄管理
ア　教育情報セキュリティ管理者は、廃棄処理を外部に委託する場合は、学校の外に委託業者が持ち出す行為に教職員等が立ち合うように指示し、誤廃棄を予防しなければならない。

イ　教育情報セキュリティ管理者は、廃棄した情報資産を記録管理しなければならない。

⑵教職員等の情報セキュリティ意識醸成

①教育情報セキュリティ管理者は、教職員等に対して、日頃から情報セキュリティに関する話題を積極的に提供し、情報セキュリティ研修を受講させるなど、積極的にセキュリティ認識の向上を図らなければならない。

②教育情報セキュリティ管理者は、校内でセキュリティ事故につながりかねないヒヤリ・ハット事案を抑止するために、教職員等が事案を発見した際に、ただちに対処し、すみやかに報告が上

がるよう、教職員等に対する情報セキュリティ意識の醸成と風通しのよい関係性維持に努めなければならない。

③教育情報セキュリティ管理者は、教職員等が常に教育情報セキュリティポリシー及び実施手順を閲覧・確認できるように配慮しなければならない。

⑶端末等の持ち出し及び持ち込みの記録

教育情報セキュリティ管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

⑷教職員等への情報セキュリティポリシー等の遵守指導

①教育情報セキュリティ管理者は、新規採用教職員等及び他自治体から新規赴任した教職員等、及び非常勤及び臨時の教職員に対し、教育情報セキュリティポリシー等遵守すべき内容を理解・浸透するように指導を行わなければならない。

②教育情報セキュリティ管理者は、教職員等に対して、必要に応じて情報セキュリティポリシーの遵守の同意書への署名を求める。

⑸新規ソフトウェア及びコンテンツの導入・利用判断

教育情報セキュリティ管理者は、教職員等から、導入したソフトウェア・コンテン ツの制限解除や、業務上新たなソフトウェア・コンテンツの導入について、事前に相談があった場合は、教育情報システム管理者に上申して、判断を仰がなければならな い。

⑹インターネット接続及び電子メール利用の制限

①教育情報セキュリティ管理者は、教職員等に業務端末による作業を行わせる場合において、業務以外でのインターネット接続及び電子メールの利用をしないよう教職員等に指導しなければならない。なおWebフィルタリングの設定について、教職員等から相談があった場合は、教育情報システム管理者に上申して、判断を仰がなければならない。

②教育情報セキュリティ管理者は、パソコンやモバイル端末の機能は、教職員等の業務内容に応じて、不必要な機能については制限することが適切である。

⑺校内及び執務室での管理

教育情報セキュリティ管理者は、教職員等と協力して下記を管理しなければならな い。
①来校者の氏名及び入退時刻を記録しなければならない。

②来校者には名札などを着用させ、第三者であることが識別できるようにしなけ ればならない。

③地域住民、保護者などに校内施設を開放する場合、執務室等開放していない施設へは入場できないよう制限を設けなければならない。

⑻自己点検の実施

教育情報セキュリティ管理者は、年1回、学校の自己点検を行わなければならない。

2.教職員等の遵守事項

教職員等は、教育情報セキュリティ管理者の指導の下、以下の規定を遵守しなければな らない。

⑴教育情報セキュリティポリシー等の遵守

教職員等は、教育情報セキュリティポリシー及び実施手順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等がある場合は、速やかに教育情報セキュリティ管理者に相談し、指示を仰がなければならない。

⑵執務上での管理

①執務室にて教職員等が不在となる場合には、執務室を施錠しなければならない。

②来校者等を執務室に入れる場合には、教育情報セキュリティ管理者または学校教育情報セキュリティ・システム担当の許可を求めなければならない。

③教職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報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教育情報セキュリティ管理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。

⑶支給端末の取扱い

①教職員等は、業務目的以外で支給端末を利用してはならない。

②教職員等は、外部のソフトウェアを無断で支給端末にインストールしてはならない。業務上必要な場合には、事前に教育情報セキュリティ管理者の許可を得る こと。

③教職員等は、支給端末の利用において、下記のカスタマイズを無断でしてはならない。
ア　セキュリティ機能に関する設定変更

イ　メモリ増設等の改造

④教職員等は、モバイル端末を利用する場合は、盗難・紛失リスクに備えての安全管理をすること。

⑤端末から離れる時は、端末をロックするなど、他者が閲覧できないようにしなければならない

⑥業務終了後と外出時には、スリープもしくは電源をオフにしなければならない。

⑷支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

①業務上やむを得ない場合を除いて、支給以外の端末及び電磁的記録媒体等を原則業務に利用してはならない。

②端末及び電磁的記録媒体等を用いる場合には、教育情報セキュリティ管理者の許可を得た上で、必要な安全管理措置を講じなければならない。

⑸モバイル端末や電磁的記録媒体等の持ち出し及び教育委員会・学校が構築・管理 している環境（本ガイドラインが適用されているクラウドサービスや学校外での利用が認められている情報端末等を含む環境）の外部における情報処理作業の制限

①学校のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、教育情報セキュリティ管理者の許可を得なければならない。

②外部で情報処理業務を行う場合には、教育情報セキュリティ管理者の許可を得なければならない。

⑹IDの取扱い

教職員等は、自己の管理するIDに関し、次の事項を遵守しなければならない。

①自己が利用しているIDは、他人に利用させてはならない。

②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

③教職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、統括教育情報セキュリティ責任者又は教育情報システム管理者に通知しなければな らない。

⑺パスワードの取扱い

教職員等は、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パスワードを秘密にし、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とし、文字列は想像しにくいものにしなければならない。

④パスワードが流出したおそれがある場合には、教育情報セキュリティ管理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ない。

⑤複数の教育情報システムを扱う教職員等は、同一のパスワードを複数のシステム間で用いてはならない。（シングルサインオンを除く）

⑥仮のパスワード（初期パスワードを含む）は、最初のログイン時点で変更しなければならない。

⑦複数の教職員が使用する可能性のある端末にパスワードを記憶させては ならない。

⑧教職員等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）

⑻電子メールの利用制限

①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。

②複数人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分からないようにしなければならない。

③重要な電子メールを誤送信した場合、速やかに教育情報セキュリティ管理者に報告しなければならない。

④ウェブで利用できるフリーメールサービス等を統括教育情報セキュリティ責任者の許可無しに使用してはならない。

⑤ 電子メールにより重要性分類Ⅲ以上の情報を外部に送信する者は、電子メールへ直接添付してはならない。外部ストレージサービスを利用し、限定されたアクセスの措置設定（アクセス制限や暗号化）を行わなければならない。

⑥送信時には誤送信を予防するため、送信先のメールアドレス、添付ファイルの内容を確認しなければならない。

⑦差出人、添付ファイル又は本文中のリンク先等が不審なメールを受信した場合には、添付ファイルの閲覧やリンク先（URL）にアクセスせずに、教育情報セキュリティ管理者に指示を仰がなければならない。

⑼クラウドサービス、ソーシャルメディアサービス利用制限

①強固なアクセス制御による対策を講じたシステム構成でない場合、重要性分類Ⅱ以上の情報資産を、インターネットを通信経路としたパブリッククラウドサービスで取り扱ってはならない。

②私的に契約したクラウドサービスや個人アカウントを業務利用してはならない。

③ソーシャルメディアサービスを利用して、業務上知り得た情報を公開してはならない。

⑽不正プログラム対策

教職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

①パソコンやモバイル端末において、不正プログラム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てはならない。OS及びコンピュータウイルス対策ソフトウェアが常に最新の状態に保てるようにしなければならない。自動更新される設定の場合は、自動更新設定を変えてはならない。

②外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

③差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削 除しなければならない。

④端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

⑤添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。

⑥統括教育情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。

⑦コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、すみやかに教育情報セキュリティ管理者に報告し、指示を仰がなければならない。また、以下の対応を行わなければならない。

ア　直ちに利用を中止し、通信を行わない設定への変更を行わなければならな い。

イ　指示があるまでは、端末の電源は切らずに保持しなければならない。

⑾電子署名・暗号化

①教職員等は、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、CISOが定めた電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならな い。

② 教職員等は、暗号化を行う場合にCISOが定める以外の方法を用いてはならない。また、CISO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。

③ CISOは、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

⑿無許可ソフトウェアの導入等の禁止

① 教職員等は、端末に無断でソフトウェアを導入してはならない。

② 教職員等は、業務上の必要がある場合は、統括教育情報セキュリティ責任者及び教育情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、教育情報セキュリティ管理者又は教育情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

③ 教職員等は、不正にコピーしたソフトウェアを利用してはならない。

⒀機器構成の変更の制限

① 教職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。

② 教職員等は、業務上、端末に対し機器の改造及び増設・交換を行う必要がある場合には、統括教育情報セキュリティ責任者及び教育情報システム管理者の許可を得なければならない。

⑭児童生徒への指導事項

教職員等は、児童生徒に学習者用端末等を利用させるに当たり、以下の事項について指導を行わなければならない。

① 学習者用端末及び学習系クラウドサービスは学習目的で利用すること。

② ID及びパスワードは他の人に知られないようにすること。

③ ウイルス対策ソフトウェアは常に最新の状態に保つこと。

④ 利用する端末のセキュリティ機能の設定を、許可なく変更してはならないこと。

⑤ 端末で生成した情報の保存先を学習系クラウドに指定できる機能がある場合には、この機能を利用して原則学習系クラウドに保管し、学習者用端末にローカル保存は必要最小限とすること。

⑥ 無断で外部ソフトウェアをインストールしないようにすること。

⑦ 学校から許可されたコミュニケーションツールのみを利用すること。

⑧ 学習用端末が動かない、勝手に操作されている、いつもと異なる画面や警告が表示されるなどの症状がでた場合、すぐに担任教員に報告すること。

⑨ 学習用端末は大事に取り扱い、盗難・紛失・破損等に注意すること。

⑩ 私物端末など許可されていない端末を学校に持ち込んで、学校のネットワーク につながないこと。

⑪ 重要性分類Ⅱ以上の情報資産を端末にダウンロードした場合には、目的を達成し次第すみやかに消去を行う等の対策を講じること。また、該当資産を閲覧する際には、離席時に端末ロックし、周囲に他の児童生徒がいる状態では閲覧しない等の対策を講じる こと。

⑮異動・退職時等の遵守事項

教職員等は、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（紙情報、データの格納された端末、外部記録媒体等）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。

3.教育委員会事務局職員の遵守事項

教育委員会事務局職員は、教育情報セキュリティ責任者の指導の下、以下の規定を遵守 しなければならない。

⑴教育情報セキュリティポリシー等の遵守

⑵業務以外の目的での使用の禁止

⑶校務用端末による外部における情報処理作業の禁止

⑷重要性分類Ⅱ以上の情報資産について校務用端末以外のパソコン、モバイル端末及び電磁的記録媒体等によるアクセスの禁止

⑸知りえた情報の秘匿

⑹業務を離れる場合の遵守事項

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すべて返却する。また、その後も業務上知り得た情報を漏らさない。

4.研修・訓練

⑴情報セキュリティに関する研修・訓練

CISOは、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

⑵研修計画の策定及び実施

① CISOは、教職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、情報セキュリティ委員会の承認を得なければならない。

② 研修計画において、教職員等は、毎年度最低1回は情報セキュリティ研修を受講できるようにしなければならない。

③ 新規採用の教職員等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。

④ 研修は、統括教育情報セキュリティ責任者、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者、教育情報システム担当者及びその他教職員等に対して、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。

⑤ CISOは、毎年度1回、情報セキュリティ委員会に対して、教職員等の情報セキュリティ研修の実施状況について報告しなければならない。

⑶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しなければならない。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。

⑷研修・訓練への参加

全ての教職員等は、定められた研修・訓練に参加しなければならない。

5.情報セキュリティインシデントの連絡体制の整備

⑴学校内からの情報セキュリティインシデントの報告

① 教職員等は、情報セキュリティインシデントを認知した場合、速やかに教育情報セキュリティ管理者に報告しなければならない。

② 報告を受けた教育情報セキュリティ管理者は、速やかに統括教育情報セキュリティ責任者、教育情報システム管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

③ 教育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、必要に応じてCISO及び教育情報セキュリティ責任者に報告しなければならない。

⑵学校内からの情報セキュリティ違反行為の報告

① 教職員等は、教育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、直ちに統括教育情報セキュリティ責任者及び教育情報セキュリティ管理者に報告を行わなければならない。

② 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統括教育情報セキュリティ責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

⑶住民等外部からの情報セキュリティインシデントの報告

① 教職員等は、管理対象のネットワーク及び教育情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、教育情報セキュリティ管理者に報告しなければならない。

② 報告を受けた教育情報セキュリティ管理者は、速やかに統括教育情報セキュリティ責任者及び教育情報システム管理者に報告しなければならない。

③ 教育情報セキュリティ管理者は、当該情報セキュリティインシデントについて、必要に応じてCISO及び教育情報セキュリティ責任者に報告しなければならない。

⑷情報セキュリティインシデント原因の究明・記録、再発防止等

① 統括教育情報セキュリティ責任者は、情報セキュリティインシデントについて、教育情報セキュリティ管理者、教育情報システム管理者及び情報セキュリティに関する統一的な窓口と連携し、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原因究明の結果から、再発防止策を検討し、CISOに報告しなければならない。

② CISOは、統括教育情報セキュリティ責任者から、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しなければならない。

⑸支給端末の運用・連絡体制の整備

学校内外での支給端末の運用ルールを制定し、インシデント時の連絡先対応方法を各学校にて整理し、実施手順に反映しなければならない。

第5章　技術的セキュリティ

1.コンピュータ及びネットワークの設定管理

⑴ログの取得等

① 統括教育情報セキュリティ責任者及び教育情報システム管理者は、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。

② 統括教育情報セキュリティ責任者及び教育情報システム管理者は、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処等について定め、適切にログを管理しなければならない。

③ 統括教育情報セキュリティ責任者及び教育情報システム管理者は、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。

⑷ネットワークの接続制御、経路制御等

① 統括教育情報セキュリティ責任者は、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、所管するネットワークの内部におけるファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

② 統括教育情報セキュリティ責任者は、不正アクセスを防止するため、所管する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

⑸外部の者が利用できるシステムの分離等

教育情報システム管理者は、保護者等の外部の者が利用できるシステム等がある場合、重要性が高い情報、特に重要性分類Ⅱ（セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす情報資産）以上の情報資産を扱うシステムにおけるアクセス権管理の徹底を行うこと。

⑹複合機のセキュリティ管理

① 統括教育情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を策定しなければならない。

② 統括教育情報セキュリティ責任者は、複合機が備える機能について適切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。

③ 統括教育情報セキュリティ責任者は、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。

⑺無線LAN及びネットワークの盗聴対策

① 統括教育情報セキュリティ責任者は、無線LANの利用を認める場合、解読が困難な通信の暗号化及び認証技術の使用を義務付けなければならない。

② 統括教育情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、通信の暗号化等の措置を講じなければならない。

⑻電子メールのセキュリティ管理

① 統括教育情報セキュリティ責任者は、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。

② 統括教育情報セキュリティ責任者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。

③ 統括教育情報セキュリティ責任者は、教職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように添付ファイルの監視等によりシステム上措置しなければならない。

2.アクセス制御

⑴アクセス制御等

統括教育情報セキュリティ責任者又は教育情報システム管理者は、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等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。特に強固なアクセス制御による対策 を講じたシステム構成の場合、重要性分類Ⅱ以上の情報資産へのアクセスについて は、多要素認証等のアクセスの真正性に関する要素技術を取り入れることで、当該シ ステムへの認証強度の向上とアクセス権管理を徹底すること。

⑵外部からのアクセス等の制限

① 統括教育情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最限の者に限定しなければならない。

② 統括教育情報セキュリティ責任者は、民間事業者等の外部組織からのシステムアクセスを認める場合、アクセスする利用者の本人確認、システムアクセスの対象となる児童生徒の本人（保護者）同意を得る等の措置を講じなければならない。

③ 統括教育情報セキュリティ責任者は、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通信の暗号化等の措置を講じなければならない。

④ 統括教育情報セキュリティ責任者及び教育情報システム管理者は、外部からのアクセスに利用する端末を教職員等に貸与する場合、端末管理ソフト（MDM）の導入等を通じて、セキュリティ確保のために必要な措置を講じなければならない。

⑶ログイン時の表示等

教育情報システム管理者は、ログイン時におけるメッセージ、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教職員等がログインしたことを確認することができるようシステムを設定しなければならない。

⑷特権による接続時間の制限

教育情報システム管理者は、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。

3.システム開発、導入、保守等

⑴情報システムの調達

① 統括教育情報セキュリティ責任者及び教育情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、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。

② 統括教育情報セキュリティ責任者及び教育情報システム管理者は、機器及びソフトウェアの調達に当たっては、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。

⑵情報システムの開発

①教育情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための規則を確立しなければならない。

②システム開発における責任者、作業者のIDの管理

ア　教育情報システム管理者は、システム開発の責任者及び作業者が使用するIDを管理し、開発完了後、開発用IDを削除しなければならない。

イ　教育情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならない。

③システム開発に用いるハードウェア及びソフトウェアの管理

ア　教育情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

イ　教育情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

⑶情報システムの導入

① 開発環境と運用環境の分離及び移行手順の明確化

ア　教育情報システム管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。

イ　教育情報システム管理者は、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。

ウ　教育情報システム管理者は、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。

エ　教育情報システム管理者は、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。

② テスト

ア　教育情報システム管理者は、新たに情報システムを導入する場合、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。

イ　教育情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。
ウ　教育情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

エ　教育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。

オ　教育情報システム管理者は、運用環境への移行に先立ち、システムの脆弱性テストを行い、その結果を確認しなければならない。

⑷システム開発・保守に関連する資料等の整備・保管

① 教育情報システム管理者は、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切に整備・保管しなければならない。

② 教育情報システム管理者は、テスト結果を一定期間保管しなければならない。

③ 教育情報システム管理者は、情報システムに係るソースコードならびに使用したオープンソースのバージョン（リポジトリ）を適切な方法で保管しなければならない。

⑸情報システムにおける入出力データの正確性の確保

① 教育情報システム管理者は、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。

② 教育情報システム管理者は、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。

③ 教育情報システム管理者は、情報システムから出力されるデータについて、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。

⑹情報システムの変更管理

教育情報システム管理者は、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。

⑺開発・保守用のソフトウェアの更新等

教育情報システム管理者は、開発・保守用のソフトウェア等を更新又はパッチの適 用をする場合、他の情報システムとの整合性を確認しなければならない。

⑻システム更新又は統合時の検証等

教育情報システム管理者は、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。

4.不正プログラム対策

⑴統括教育情報セキュリティ責任者の措置事項

統括教育情報セキュリティ責任者は、不正プログラム対策として、次の事項を措置しなければならない。

① 外部ネットワークから受信したファイルは、インターネットのゲートウェイなどにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。
② 外部ネットワークに送信するファイルは、インターネットのゲートウェイなどにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

③ コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ教職員等に対して注意喚起しなければならない。

④ 所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

⑤ 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

⑥ 不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

⑦ 業務で利用するソフトウェアは、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利用してはならない。

⑵教育情報システム管理者の措置事項

教育情報システム管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

① 教育情報システム管理者は、その所掌するサーバ及びパソコン等の端末を守るため、コンピュータウイルス等の不正プログラムへの対策を講じなければならない。

② 不正プログラム対策は、常に最新の状態に保たなければならない。

5.不正アクセス対策

⑴統括教育情報セキュリティ責任者の措置事項

統括教育情報セキュリティ責任者は、不正アクセス対策として、以下の事項を措置しなければならない。

① 使用されていないポート及びSSID（無線LANネットワーク名）を閉鎖しなければならない。
② 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。
③ 不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括教育情報セキュリティ責任者及び教育情報システム管理者へ通 報するよう、設定しなければならない。
④ 重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。

⑤ 統括教育情報セキュリティ責任者は、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切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。

⑵ 標的型攻撃

統括教育情報セキュリティ責任者及び教育情報システム管理者は、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、教育や自動再生無効化等の人的対策や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。

6.セキュリティ情報の収集

⑴セキュリティホールに関する情報の収集及び共有並びにソフトウェアの更新等

統括教育情報セキュリティ責任者及び教育情報システム管理者は、セキュリティホ ール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、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。

⑵不正プログラム等のセキュリティ情報の収集及び周知

統括教育情報セキュリティ責任者は、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、教職員等に周知しなければならない。

⑶情報セキュリティに関する情報の収集及び共有

統括教育情報セキュリティ責任者及び教育情報システム管理者は、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。

第6章 運用

1.情報システムの監視

⑴情報システムの監視

①統括教育情報セキュリティ責任者及び教育情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。特に重要性分類Ⅱ以上の情報資産へのアクセスについては、侵入検知システム（IDS）や侵入防御システム（IPS）などの端末・通信の監視・制御等によるセキュリティ対策を講じなければならな い。

②統括教育情報セキュリティ責任者及び教育情報システム管理者は、教職員等及び外部委託事業者が使用しているパソコン等の端末からの所管するネットワーク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。

2.ドキュメントの管理

⑴システム管理記録及び作業の確認

① 教育情報システム管理者は、所管する教育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。

② 統括教育情報セキュリティ責任者及び教育情報システム管理者は、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切に管理しなければならない。

③ 統括教育情報セキュリティ責任者、教育情報システム管理者又は教育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。

⑵情報システム仕様書等の管理

統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク構成図、情報システム仕様書等について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適切に管理しなければならない。

⑶障害記録の管理

統括教育情報セキュリティ責任者及び教育情報システム管理者は、教職員等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、障害記録として記録し、適切に保存しなければならない。

⑷記録の保存

CISO及び統括教育情報セキュリティ責任者は、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、警察及び関係機関との緊密な連携に努めなければならない。

3.教職員等の ID 及びパスワードの管理

⑴利用者 ID の取扱い

① 統括教育情報セキュリティ責任者及び教育情報システム管理者は、利用者の登録、変更、抹消等の情報管理、教職員等の異動、出向、退職者に伴う利用者 IDの取扱い等の方法を定めなければならない。

② 統括教育情報セキュリティ責任者及び教育情報システム管理者は、利用されていない ID が放置されないよう、点検しなければならな い。

⑵パスワードに関する情報の管理

① 統括教育情報セキュリティ責任者又は教育情報システム管理者は、教職員等のパスワードに関する情報を厳重に管理しなければならない。パスワード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。

② 統括教育情報セキュリティ責任者又は教育情報システム管理者は、教職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、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。

4. 児童生徒におけるID及びパスワード等の管理

⑴ID登録・変更・削除

①IDについてはシンプル・ユニーク（唯一無二）・パーマネント/パーシスタント（永続的な識別）な構成要素になっていることや、児童生徒の発達段階に応じた複雑性を上げたパスワードポリシーによりセキュリティ強度を上げていくなど 適切な措置を講じなければならない。ID登録やパスワードポリシーにおいては情報セキュリティ対策として重要な要素であるため学校毎に管理するのではなく、同一の教育委員会等の組織にて一元管理することが望ましい。

②IDについては原則として進級/進学にも変更不要とすることが望ましい。IDを変えることなくIDの属性情報（進級時の組・出席番号、進学先学校名など）の更新を行っておくことで、MDMによる各種ポリシーや使用アプリケーションの変更を効率的に行うことが可能となる。さらに統合型校務支援システム等における児童生徒の氏名と連動したID管理を行うことで、校務側で管理している属性情報と一体となったIDを含んだマスター管理の一元化が望ましい。

③ユニークなIDは個人を識別できる可能性があるため、個人情報保護の観点から、サービス提供期間を超えて個人を特定する情報を保持しないようにする必要がある。転出や卒業/退学時に学習用ツールのサービス利用期間が終了する場合は、あらかじめ児童生徒本人によるデータ移行をサービス利用期間内に実施し、IDの利用停止後、最終的にはID及び関連するデータの完全削除を行うこと。

⑵学習用ツールへのシングルサインオン

学習履歴を活用したり、個人の成果物を保存するアプリケーションが増えてくると、サービス利用時に都度ID及びパスワード等の認証情報を入力したり、サービス毎のアカウント情報管理が非常に煩雑になるため、一度の認証により一定時間は各種サ ービスにアクセスが行えるシングルサインオンの導入を行うことが望ましい。

5.特権を付与されたIDの管理等

⑴特権を付与されたIDの管理等

①統括教育情報セキュリティ責任者及び教育情報システム管理者は、管理者権限等の特権を付与された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。

②統括教育情報セキュリティ責任者及び教育情報システム管理者の特権を代行する者は、統括教育情報セキュリティ責任者及び教育情報システム管理者が指名し、CISOが認めた者でなければならない。

③CISOは、代行者を認めた場合、速やかに統括教育情報セキュリティ責任者、教育情報セキュリティ責任者、教育情報セキュリティ管理者及び教育情報システム管理者に通知しなければならない。

④統括教育情報セキュリティ責任者及び教育情報システム管理者は、特権を付与されたID及びパスワードの変更について、外部委託事業者に行わせてはならない。

⑤統括教育情報セキュリティ責任者及び教育情報システム管理者は、特権を付与されたID及びパスワードについて、その利用期間に合わせて特権IDを作成・削除する、もしくは、入力回数制限を設ける等のセキュリティ機能を強化しなければならない。

⑥統括教育情報セキュリティ責任者及び教育情報システム管理者は、特権を付与されたIDを初期設定以外のものに変更しなければならない。

⑦統括教育情報セキュリティ責任者及び教育情報システム管理者は、特権を付与されたIDのログ監視を行わなければならない。

6.教育情報セキュリティポリシーの遵守状況の確認・管理

⑴遵守状況の確認・管理

① 教育情報セキュリティ責任者及び教育情報セキュリティ管理者は、教育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CISO及び統括教育情報セキュリティ責任者に報告しなければならない。

② CISO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。

③ 統括教育情報セキュリティ責任者及び教育情報システム管理者は、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切かつ速やかに対処しなければならない。

⑵端末の利用状況調査

CISO及びCISOが指名した者は、不正アクセス、不正プログラム等の調査のために 教職員等が使用している端末のログ、電子メールの送受信記録等の利用状況を調査することができる。

⑶業務以外の目的でのウェブ閲覧の禁止

統括教育情報セキュリティ責任者は、教職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、教育情報セキュリティ管理者に通知し適切な措置を求めなければならない。

⑷教職員等による不正アクセスの管理

統括教育情報セキュリティ責任者及び教育情報システム管理者は、教職員等による不正アクセスを発見した場合は、当該教職員等が所属する学校等の教育情報セキュリ ティ管理者に通知し、適切な処置を求めなければならない。

7.専門家の支援体制等

⑴専門家の支援体制

統括教育情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、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。

⑵他団体との情報システムに関する情報等の交換

教育情報システム管理者は、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、統括教育情報セキュリティ責任者及び教育情報セキュリティ責任者の許可を得なければならない。

8.侵害時の対応等

⑴緊急時対応計画の策定

CISO又は情報セキュリティ委員会は、情報セキュリティインシデント、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、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適切に対処しなければならない。

⑵緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

① 関係者の連絡先

② 発生した事案に係る報告すべき事項

③ 発生した事案への対応措置

④ 再発防止措置の策定

⑶業務継続計画との整合性確保

自然災害、大規模又は広範囲に及ぶ疾病等に備えて別途業務継続計画を策定し、情報セキュリティ委員会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。

⑷緊急時対応計画の見直し

CISO又は情報セキュリティ委員会は、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、必要に応じて緊急時対応計画の規定を見直さなければならない。

9.例外措置

⑴例外措置の許可

教育情報セキュリティ管理者及び教育情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、学校事務及び教育活動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し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、例外措置を取ることができる。

⑵緊急時の例外措置

教育情報セキュリティ管理者及び教育情報システム管理者は、学校事務及び教育活動の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかにCISOに報告しなければならない。

⑶例外措置の申請書の管理

CISOは、例外措置の申請書及び審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

10.法令等遵守

⑴法令等遵守

教職員等は、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、次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。

① 地方公務員法（昭和25年12月13日法律第261号）

② 教育公務員特例法（昭和24年１月12日法律第１号）

③ 著作権法（昭和45年法律第48号）

④ 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）

⑤ 個人情報の保護に関する法律（平成15年５月30日法律第57号）

⑥ 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）

⑦ サイバーセキュリティ基本法（平成26年法律第104号）

11.懲戒処分等

⑴懲戒処分

教育情報セキュリティポリシーに違反した教職員等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、地方公務員法をはじめとするによる懲戒処分の対象とする。

⑵違反時の対応

教職員等の教育情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

① 統括教育情報セキュリティ責任者が違反を確認した場合は、統括教育情報セキュリティ責任者は当該教職員等が所属する学校の教育情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

② 教育情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括教育情報セキュリティ責任者及び当該教職員等が所属する学校の教育情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

③ 教育情報セキュリティ管理者の指導によっても改善されない場合、統括教育情報セキュリティ責任者は、当該教職員等の教育ネットワーク又は教育情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、統括教育情報セキュリティ責任者は、教職員等の権利を停止あるいは剥奪した旨をCISO及び当該教職員等が所属する学校の教育情報セキュリティ管理者に通知しなければならない。

第7章　外部委託

1.外部委託

⑴外部委託事業者の選定基準

① 教育情報システム管理者は、外部委託事業者の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

②教育情報システム管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者を選定しなければならない。

⑵契約項目

情報システムの運用、保守等を外部委託する場合には、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

・教育情報セキュリティポリシー及び教育情報セキュリティ実施手順の遵守
・外部委託事業者の責任者、委託内容、作業者、作業場所の特定
・提供されるサービスレベルの保証
・外部委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法
・外部委託事業者の従業員に対する教育の実施
・提供された情報の目的外利用及び受託者以外の者への提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・町による監査、検査
・町による情報セキュリティインシデント発生時の公表
・教育情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

⑶確認・措置等

教育情報システム管理者は、外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、（2）の契約に基づき措置しなければならない。また、その内容を統括教育情報セキュリティ責任者に報告するとともに、その重要度に応じてCISOに報告しなければならない。

⑷外部委託事業者に対する説明

教育情報システム管理者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

第8章　SaaS型パブリッククラウドサービスの利用

1.SaaS型パブリッククラウドサービスの利用における情報セキュリティ対策

⑴利用者認証

①クラウド利用者は、クラウド事業者における当該クラウドサービスを提供する情報システムの運用もしくは開発に従事する者又は管理者権限を有する者について、適切な利用者確認がなされていることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

②クラウド利用者は、当該クラウドサービスのログインに関わる認証機能の提供をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

③クラウド利用者側管理者権限を有する者のIDの管理について、「第6章 5 特権を付与されたIDの管理等」を遵守しなければならない。

⑵アクセス制御

①クラウド利用者は、当該クラウドサービスに対して、アクセスする権限のない者がアクセスできないように、システム上制限する機能の提供をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

②クラウド利用者は、クラウド事業者の提供するアクセス制御機能を用いて、情報資産毎に、許可されたクラウドを利用する教職員等及び児童生徒のみがアクセスできる環境を設定しなければならない。

⑶クラウドに保管するデータの暗号化

①クラウド利用者は、当該クラウドサービスへのデータの保管に際し、情報漏えい等に備えて、暗号化等の保護措置を講じられていることを、クラウド事業者にサービス提供定款や契約書面上で確認または合意しなければならない。

⑷マルチテナント環境におけるテナント間の安全な管理

①クラウド利用者は、複数のクラウド利用者がクラウドリソースを共用する環境において、特定のクラウド利用者に対して発生したセキュリティ侵害が、他のクラウド利用者に影響を与えないように対策が講じられていることを、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

⑸クラウドサービスを提供する情報システムに対する外部からの悪意のある脅威の侵入を想定した技術的セキュリティ対策

①クラウド利用者は、当該クラウドサービスを提供する情報システムを監視し、セキュリティ侵害を検知することを、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

②クラウド利用者は、当該クラウドサービスを提供する情報システムのインターネット接続境界において、クラウド利用者以外による不正な通信・侵入を防ぐ措置を講じるとともに、外部脅威の侵入を検知し、防御する対策を講ずることを、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

⑹情報の通信経路のセキュリティ確保

①クラウド利用者は、教育情報システムのインターネット境界から当該クラウドサービスを提供する情報システムまでの情報の通信経路において、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準・手順等の整備、通信の暗号化等）をクラウド事業者に求め、合意のうえ、利用しなければならない。

②クラウド利用者は、クラウド事業者が保守運用等を遠隔で行う場合の、保守運用拠点と管理区域間での通信回線及び通信回線装置の管理について、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準・手順等の整備、通信の暗号化等）をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

⑺クラウドサービスを提供する情報システムの物理的セキュリティ対策

①クラウド利用者は、クラウド事業者が提供する情報システムの物理的セキュリティについて、入退室管理、監視・録画、盗難・持ち出し防止、火災等の災害対策、電源冗長化、そして資源廃棄処理が適切に講じられていることを、第三者認証（ISO/IEC 27001、SOC 2等）や監査報告書を用いて確認し、契約書面で確認または合意しなければならない。

②クラウド利用者は、クラウド事業者側の管理区域（サーバ等設置場所）及び保守運用拠点の管理について、①と同等の管理基準が適用されることを確認し、契約書面上で合意しなければならない。

③クラウド利用者は、クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）に当たり、セキュリティを確保した対応となっているかをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。なお、当該確認に当たっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用できる。

⑻クラウドサービスを提供する情報システムの運用管理

①クラウド利用者は、クラウド事業者に対して、サービスの一時停止等クラウド利用者に影響があり得る運用手順の有無、有る場合にはクラウド利用者への影響範囲（時間、サービス内容）、連絡方法等について情報提供を求め、クラウド利用者が業務運営に支障がないことを確認し、合意しなければならない。また、クラウド事業者の設定不備等によるインシデント発生時にも同様の確認をしなければならない。

②クラウド利用者は、クラウドサービス事業者と連携し、情報セキュリティインシデント発生時の速やかな報告及び対応策の実行について、サービス契約書に明記された手順を遵守しなければならない。インシデントの内容や進行状況に関して、定期的に事業者と情報共有し、必要に応じて外部監査機関と協力しなければならない。

③クラウド利用者は、サービスの可用性（サービス稼働率・故障時復旧）のために、クラウド事業者が提供する冗長化構成（RTO/RPO）、切替方式（同一DC／ゾーン間／地域間）を明確にし、SLA（サービスレベルアグリーメント）として契約書面に反映させなければならない。

④クラウド利用者は、当該クラウドサービスにおけるデータ保護のため、バックアップ対象・方式（完全／増分等）、頻度・世代数、保存期間、暗号化、保管場所（リージョン）、復旧手順（演習・検証を含む）を明確化をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

⑤クラウド利用者は、監査・責任追跡性の確保のため、取得・保持すべきログ（認証・アクセス・管理操作・共有設定・監査イベント等）の種類、改ざん耐性、保存期間、時刻同期、抽出・エクスポート手段及び提供SLOを定め、定期取得・保管をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

⑼クラウドサービスを提供する情報システムのマルウェア感染対策

①クラウド利用者は、クラウドサービスを提供する情報システムを構成するサーバ及び運用管理端末等について、マルウェア感染対策を講じることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

②クラウド利用者は、内部システムに侵入した攻撃を検知して対処するために、通信をチェックする等の対策を講じることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

⑽クラウド利用者側のセキュリティ確保

①クラウド利用者は、当該クラウドサービスにおけるセキュリティ対策として、外部からの脅威に対する防御措置を強化し、侵入検知システム（IDS）や侵入防御システム（IPS）を導入することをクラウド事業者に求め、サービス提供定款や契約書面で確認または合意しなければならない。加えて、マルウェア対策として、クラウドサービスが提供するサーバや運用端末に対してウイルス対策ソフトウェアの導入や定期的なスキャンを実施し、侵入を未然に防ぐための対応策を講じなければならない。また、ゼロデイ攻撃など新たな脅威に対応するため、クラウド事業者は、脅威インテリジェンスを活用し、リアルタイムでセキュリティインシデントを監視する体制を構築し、その情報をクラウド利用者に提供することを求める。

②クラウド利用者は、標的型攻撃による外部からの脅威の侵入を防止するために、クラウドを利用する教職員等及び児童生徒への教育や入口対策を講じなければならない。

⑾クラウド事業者従業員の人的セキュリティ対策

①クラウド利用者は、クラウドサービスに関わるクラウド事業者従業員に対して、クラウド事業者の情報セキュリティポリシー及び保守運用管理規程等を遵守することをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

②クラウド利用者は、クラウドサービスに関わるクラウド事業者従業員に対して、業務に用いるID及びパスワードその他の個人認証に必要な情報及び媒体について、部外者及び業務に関わらない従業員に漏えいすることがないように、適切に管理することをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

③クラウド利用者は、クラウドサービスに関わらない従業員等がクラウド利用者のデータを知り得る状態にならないよう、業務に関わるクラウド事業者従業員に対して秘匿を義務づけることをクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

④クラウド利用者は、クラウド利用者のデータ及びデータを格納した端末機器又は電磁的記録媒体の外部持ち出しについて、クラウド利用者の許可なく外部持ち出しできないこと及び外部持ち出しにおける安全管理手順をクラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

⑤クラウド利用者は、クラウドサービスを提供する情報システムを構成するサーバ及び運用管理端末等に、マルウェアを侵入させないよう、クラウド事業者に求め、サービス提供定款や契約書面上で確認または合意しなければならない。

⑿サービス終了時等のデータの廃棄及び利用者アカウント抹消

①クラウド利用者は、サービス利用終了時等において、クラウド利用者のデータ及び利用者アカウント情報が不用意に残置されないよう、適切に破棄するための流れについてサービス提供定款や契約書面上で確認または合意しておかなければならない。

②クラウド利用者は、サービス利用終了時等におけるデータの扱いについて、スムーズに回収、次期システムへの移行等を行えるよう、その措置の流れについてサービス提供定款や契約書面上で確認または合意しておかなければならない。

③クラウド利用者は、クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

④クラウド利用者は、サービス利用終了時におけるデータの廃棄及び移行について、クラウド事業者に対し、データの破棄証明書及び移行スケジュールを提供するよう求め、契約書面で確認しなければならない。

⑬クラウドサービス要件基準を満たす配慮を含めたネットワーク設計

①クラウド利用者は、利用するクラウドサービスの要件基準を確認し、要件基準を満たすネットワークを設計しなければならない。

2.SaaS型パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項

⑴守秘義務、目的外利用及び第三者への提供の禁止

①クラウド利用者は、クラウド事業者と契約時に守秘義務、目的外利用及び第三者への提供の禁止条項を締結しなければならない。クラウドサービス事業者がコンテンツにアクセスできるかどうかを確認し、サービスに係る情報及び受託した情報に関する守秘義務、目的外利用及び第三者への提供の禁止条項について、サービス提供に係る契約に含めなければならない。契約には、当該条項に違反したクラウドサービス事業者に対する損害賠償規定を含めること。

⑵準拠する法令、情報セキュリティポリシー等の確認

①クラウド利用者は、クラウド事業者がどのような規範に基づいてサービス提供するか開示を求め、クラウド利用者の準拠する法令、情報セキュリティポリシーを確認し、それらとの整合を確認しなければならない。（クラウド事業者の準拠する認証制度、個人情報保護指針、プライバシーポリシー、情報セキュリティに関する基本方針及び対策基準、保守運用管理規程等）

⑶クラウド事業者の管理体制

①クラウド利用者は、クラウド事業者に対して、情報セキュリティポリシー等の遵守を担保する管理体制が整備されているか、クラウド事業者の組織体制を確認し、合意しなければならない。確認すべき項目例を下記に示す。

ア　サービスの提供についての管理責任を有する責任者の設置

イ　情報システムについての管理責任を負い、これについて十分な技術的能力及び経験を有する責任者（システム管理者）の設置

ウ　サービスの提供に係る情報システムの運用に関する事務を統括する責任者の設置

⑷クラウド事業者従業員への教育

①クラウド利用者は、クラウド事業者に、従業員に対して個人情報保護等の関係法令、守秘義務等、業務遂行に必要な知識、意識向上のための適切な教育及び訓練を実施し、充分な知識とセキュリティ意識を醸成することを求めなければならない。

②クラウド利用者は、クラウド事業者に、従業員への上記育成計画、教育実績等の情報を提示させ、自らデータを管理する場合と同様の教育・訓練を実施しているかを確認しなければならない。

⑸情報セキュリティに関する役割の範囲、責任分界点

①クラウド利用者は、クラウド事業者の情報セキュリティに関する役割の範囲と責任分界点について開示するよう求めなければならない。

②クラウド利用者は、クラウド事業者の情報セキュリティに関する役割の範囲と責任分界点がクラウド利用者側で講ずる情報セキュリティ対策の役割の範囲と整合することを確認し、合意しなければならない。

⑹監査

①クラウド利用者は、クラウドサービスの監査状況、範囲・条件、内容等についてクラウド事業者に開示するよう求めなければならない。

②クラウド利用者は、クラウド事業者によるクラウドサービスに関する監査レポート等を根拠にして、自らの関係法令、情報セキュリティポリシーと照らし合わせ、安全性が確保されているかについて確認しなければならない。

⑺情報インシデント管理及び対応フローの合意

①クラウド利用者は、情報セキュリティインシデント管理に関する責任範囲と及びインシデント対応フローを、サービス仕様の一部として定めることについて、クラウド事業者に対して求めなければならない。

②クラウド利用者は情報セキュリティインシデント管理に関する責任範囲と及びインシデント対応フローを検証し、インシデントに備えた組織体制を整備しなければならない。

⑻クラウドサービスの提供水準及び品質保証

①クラウド利用者は、クラウドサービスの提供水準（サービス内容、提供範囲等）と品質保証（サービス稼働率、故障等の復旧時間等）を確認するとともに、それらの水準・品質が、業務遂行に求められる要求水準を満たすことを確認し、合意しなければならない。

⑼クラウド事業者の再委託先等との合意事項

①クラウド利用者は、クラウド事業者と合意したサービス履行内容及び情報セキュリティ対策について、クラウド事業者自らが実施する内容と、再委託先等に委託する内容も含めて提示することをクラウド事業者に求めなければならない。また、サプライチェーンリスク対策が適切に講じられていることをクラウド事業者に求めなければならない。

②クラウド利用者は、①の提示内容が、クラウド事業者と合意したサービス履行内容及び情報セキュリティ対策と整合していることを確認しなければならない。

③クラウド利用者は、再委託先等が関与する場合、そのセキュリティ要件及び契約内容を事前に確認し、再委託先にも同等の情報セキュリティ対策が適用されることを、クラウド事業者に求め、合意書面で確認しなければならない。

⑽その他留意事項

①クラウド利用者は、クラウド事業者がサービスを安定して提供可能な企業・団体であるかについて考慮しなければならない。

②クラウド利用者は、クラウド事業者間でのデータ形成の互換性が必ずしも保証されている訳ではないことから、事業者を変更する際のデータ移行の方法などについて、クラウド事業者にサービス提供定款や契約書面上で確認または合意しなければならない。

③クラウド利用者は、クラウド事業者に対して、クラウドサービスにおいて扱う情報資産や情報システム等について、日本の法令が適用されること及び係争等における管轄裁判所が日本国内であることを確認すること。また、国内法以外の法令及び規制が適用される場合にはそのリスクを評価した上でクラウド事業者を選定しなければならない。

④クラウド利用者は、クラウド事業者において個人情報の適切な管理が行われているか確認するとともに、確認した項目については、調達時においてサービスの過剰な排除にならないよう留意した上で、契約要件等として定めなければならない。

3.SaaS型パブリッククラウドサービス利用における教職員等の留意点

⑴ID及びパスワード等の秘匿

①教職員等は、ID及びパスワードについて秘匿管理を行わなければならない。

②教職員等は、多要素認証に必要な要素（知識、生体、物理）についても適切に管理を行わなければならない。もし該当要素が流出等したと考えられる場合には、速やかに教育情報セキュリティ管理者に報告しなければならない。

⑵モバイル端末持ち歩きリスク

教職員等は、クラウドサービスにアクセスする際に活用するモバイル端末について、紛失・盗難を避けるよう、適切に管理しなければならない。

⑶重要性分類に基づく情報管理

パブリッククラウド上で重要な情報（重要性分類Ⅱ以上）を取り扱う際には、多要素認証を含む強固なアクセス制御による対策を講じなければならない。ただし、児童生徒またはその保護者が重要性分類Ⅱ以上の情報資産にアクセスする場合は、児童生徒本人またはその保護者が、当該児童生徒に関するもののみにアクセスすることを想定していることから、多要素認証を設定することが望ましいものの、パスワードの秘匿管理の徹底、複数回誤ったパスワードを入力した際の

ロック機能の有効化、パスワードの複雑性の確保等により本人確認を厳格に行う前提で、ID及びパスワードでの認証を許容する。

⑷学校外からのパブリッククラウド利用

①教職員等は、学校外からクラウドサービスを利用する際、情報資産の取扱いをクラウドサービス上のみで行うことを原則とする。

②クラウドサービスから端末にファイルをダウンロードする際は、情報資産の外部持ち出しに基づく安全管理措置として、端末の安全性を事前に確認するとともに、作業が終わり次第当該端末から情報資産をすみやかに消去しなければならない。

⑸SaaS型パブリッククラウドサービスの学習用途、校務用途混在リスクへの対応

①教職員等は、強固なアクセス制御による対策を講じたシステム構成にてクラウドサービスを利用している場合には、クラウドサービスを学習用途と校務用途で適切に使い分けるよう、共有先やダウンロード方法等の運用ルールについてあらかじめ確認し、適切に運用しなければならない。

②教職員等は、ネットワーク分離による対策を講じたシステム構成の場合にてクラウドサービスを利用している場合には、クラウドサービスを学習用途と校務用途で使い分けるよう、適切に運用しなければならない。

4.約款による外部サービスの利用

⑴約款による外部サービスの利用に係る規定の整備

①教育情報システム管理者は、以下を含む約款による外部サービスの利用に関す る規定を整備しなければならない。また、当該サービスの利用において、機密性の高い情報の取扱いには十分に留意するように規定しなければならない。

ア　約款によるサービスを利用してよい範囲

イ　業務により利用する約款による外部サービス

ウ　利用手続及び運用手順

②教育情報システム管理者は、約款による外部サービスの利用に当たっては、約款において以下の点が規定されていることを確認しなければならない。

ア　利用者が登録した情報が、利用者の同意なく無断使用（目的外利用、第三者への提供等）されないこと

イ　サービス事業者が業務上知り得た情報の守秘義務が守られること

⑵約款による外部サービスの利用における対策の実施

教職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリ スクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切 な措置を講じた上で利用しなければならない。

5.ソーシャルメディアサービスの利用

⑴ソーシャルメディアサービスの利用

教育情報システム管理者は、教育委員会又は学校が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

① 本町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。

② 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

③重要性分類Ⅲ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。

④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。

第9章　評価・見直し

1.監査

⑴実施方法

CISOは、必要に応じて情報セキュリティ監査統括責任者を指名し、教育ネットワーク及び教育情報システム等の情報資産における情報セキュリティ対策状況について、監査を行わせなければならない。

⑵監査を行う者の要件

① 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、被監査部門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。

② 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。

⑶監査実施計画の立案及び実施への協力

①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、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。

②被監査部門は、監査の実施に協力しなければならない。

⑷外部委託事業者に対する監査

外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業者から下請けとして受託している事業者も含めて、教育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に又は必要に応じて行わなければならない。

⑸報告

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、情報セキュリティ委員会に報告する。

⑹保管

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。

⑺監査結果への対応

CISOは、監査結果を踏まえ、指摘事項を所管する教育情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない教育情報セキュリティ管理者に対しても、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。

⑻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

情報セキュリティ委員会は、監査結果を情報セキュリティポリシー及び関係規定等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

2.自己点検

⑴実施方法

①統括教育情報セキュリティ責任者及び教育情報システム管理者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

②教育情報セキュリティ責任者は、教育情報セキュリティ管理者と連携して、所管する部局における教育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、毎年度及び必要に応じて自己点検を行わなければならない。

⑵報告

統括教育情報セキュリティ責任者、教育情報システム管理者及び教育情報セキュリティ責任者は、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、情報セキュリティ委員会に報告しなければならない。

⑶自己点検結果の活用

① 教職員等は、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。

② 情報セキュリティ委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

3.教育情報セキュリティポリシー及び関係規程等の見直し

⑴教育情報セキュリティポリシー及び関係規程等の見直し

情報セキュリティ委員会は、情報セキュリティ監査及び自己点検の結果並びに法令改正やセキュリティ脅威の変化、組織体制の変更、重大インシデント等の発生時に、必要に応じて評価を行い、必要があると認めた場合、改善を行うものとする。