島根県教育情報セキュリティポリシー

令和８年４月

島根県教育委員会

目次

教育情報セキュリティポリシーの構成・・・・・・・・・・・・・・・・・・・・・・・・・－ 1 －
第１章　教育情報セキュリティ基本方針・・・・・・・・・・・・・・・・・・・・・・・－ 2 －
第２章　教育情報セキュリティ対策基準・・・・・・・・・・・・・・・・・・・・・・・－ 3 －
１　対象機関等・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・－ 3 －
２　教育情報セキュリティの管理体制・・・・・・・・・・・・・・・・・・・・・・・・－ 3 －
２．１．管理体制 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・－ 3 －
２．２．管理体制（県立学校のみ関係するもの）・・・・・・・・・・・・・・・・・・－ 7 －
２．３．兼務の禁止・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・－ 7 －
３　情報資産の分類と管理方法・・・・・・・・・・・・・・・・・・・・・・・・・・－ 8 －
３．１．情報資産の分類・・・・・・・・・・・・・・・・・・・・・・・・・・・・・－ 8 －
３．２．情報資産の管理・・・・・・・・・・・・・・・・・・・・・・・・・・・・・－ 11 －
４　物理的セキュリティ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・－ 14 －
４．１．サーバ等の管理・・・・・・・・・・・・・・・・・・・・・・・・・・・・・－ 14 －
４．２．通信回線及び通信回線装置の管理・・・・・・・・・・・・・・・・・・・・・－ 15 －
４．３．教職員等の利用する端末や電磁的記録媒体等の管理・・・・・・・・・・・・－ 16 －
４．４．学習者用端末のセキュリティ対策・・・・・・・・・・・・・・・・・・・・－ 17 －
４．５．パソコン教室等における学習者用端末や電磁的記録媒体の管理・・・・・・－ 18 －
５　人的セキュリティ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・－ 19 －
５．１．教育情報セキュリティ管理者の措置事項・・・・・・・・・・・・・・・・・－ 19 －
５．２．教職員等の遵守事項・・・・・・・・・・・・・・・・・・・・・・・・・・・－ 20 －
５．３．教育委員会事務局職員の遵守事項・・・・・・・・・・・・・・・・・・・・－ 26 －
５．４．研修・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・－ 26 －
５．５．情報セキュリティインシデントの連絡体制の整備・・・・・・・・・・・・・－ 27 －
６　技術的セキュリティ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・－ 29 －
６．１．コンピュータ及びネットワークの設定管理・・・・・・・・・・・・・・・・－ 29 －
６．２．アクセス制御・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・－ 31 －
６．３．システム開発、導入、保守等・・・・・・・・・・・・・・・・・・・・・・－ 32 －
６．４．不正プログラム対策・・・・・・・・・・・・・・・・・・・・・・・・・・－ 34 －
６．５．不正アクセス対策・・・・・・・・・・・・・・・・・・・・・・・・・・・－ 35 －
６．６．セキュリティ情報の収集・・・・・・・・・・・・・・・・・・・・・・・・－ 36 －
７　運用・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・－ 37 －
７．１．情報システムの監視・・・・・・・・・・・・・・・・・・・・・・・・・・－ 37 －
７．２．ドキュメントの管理・・・・・・・・・・・・・・・・・・・・・・・・・・－ 37 －
７．３．教職員等のＩＤ及びパスワードの管理・・・・・・・・・・・・・・・・・－ 38 －
７．４．児童生徒におけるＩＤ及びパスワード等の管理・・・・・・・・・・・・・－ 38 －
７．５．特権を付与されたＩＤの管理等・・・・・・・・・・・・・・・・・・・・－ 39 －
７．６．教育情報セキュリティポリシーの遵守状況の確認・管理・・・・・・－ 40 －

７．７．侵害時の対応等・・・・・・・・・・・・・・・・・・・・・・・・- 41 -
７．８．例外措置・・・・・・・・・・・・・・・・・・・・・・・・・・・- 41 -
７．９．法令等遵守・・・・・・・・・・・・・・・・・・・・・・・・・・- 42 -
７．10．懲戒処分等・・・・・・・・・・・・・・・・・・・・・・・・・・- 42 -
８　外部委託・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・- 44 -
９　SaaS 型パブリッククラウドサービスの利用・・・・・・・・・・・・・・・- 45 -
９．１．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・・- 45 -
９．２．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 ・・- 48 -
９．３．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・・- 51 -
９．４．約款による外部サービスの利用・・・・・・・・・・・・・・・・・・- 52 -
９．５．ソーシャルメディアサービスの利用・・・・・・・・・・・・・・・・- 52 -
10　評価・見直し・・・・・・・・・・・・・・・・・・・・・・・・・・・・- 54 -
10．１．監査・・・・・・・・・・・・・・・・・・・・・・・・・・・・・- 54 -
10．２．自己点検・・・・・・・・・・・・・・・・・・・・・・・・・・・- 55 -
10．３．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・・・・・・- 55 -
附則・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・- 55 -
【別表】教育情報セキュリティ委員名簿・・・・・・・・・・・・・・・・・・- 56 -
【参考】島根県教育委員会ＣＳＩＲＴ体制図・・・・・・・・・・・・・・・・- 57 -
【参考】情報インシデント発生時の通報先・・・・・・・・・・・・・・・・・- 58 -
【参考】セキュリティ担当者等の報告先・・・・・・・・・・・・・・・・・・- 58 -
【参考】島根県情報セキュリティポリシー（第１章　情報セキュリティ基本方針）・・- 59 -

教育情報セキュリティポリシーの構成

島根県教育情報セキュリティポリシーは、島根県教育委員会（以下「県教委」という）が管理する情報資産を適切に保護するため、県教委が行う情報セキュリティ対策について、総合的、体系的に取りまとめたものである。

情報セキュリティポリシーは、全ての県教委職員（常勤職員、会計年度任用職員、非常勤職員及び臨時的任用職員）（以下、「教職員等」という）並びに業務委託事業者に浸透、定着させるものであり、安定的な規範であることが要請される。

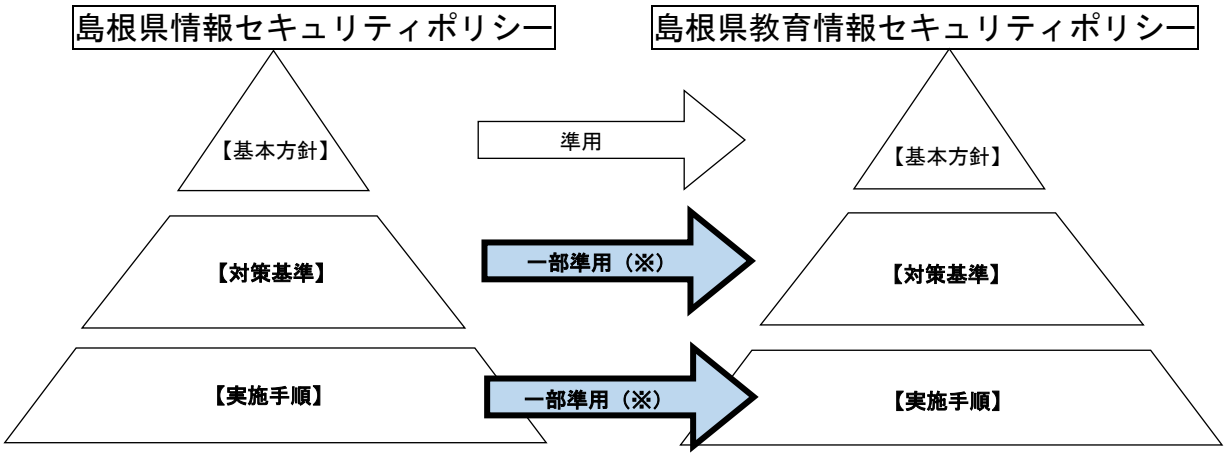
しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（セキュリティ基準）で構成する。

【情報セキュリティ基本方針】・・・情報セキュリティ対策の基本的な方針
【情報セキュリティ対策基準】・・・基本方針を実行に移すための全ての情報資産に共通の情報セキュリティ対策の基準

また、情報セキュリティポリシーに基づき、具体的な情報セキュリティ対策を実施するため【情報セキュリティ実施手順】を策定することとする。

なお、島根県教育情報セキュリティポリシーは、既に島根県において策定されている島根県情報セキュリティポリシーと共通する部分が多いため、以下の図に示すとおり、島根県情報セキュリティポリシーを準用する。



（※）【情報セキュリティ対策基準】及び【情報セキュリティ実施手順】については、対象資産の一部（県立学校以外において教職員用端末以外で取り扱う対象資産）は、島根県の【対策基準】及び【実施手順】を準用する。

第１章　教育情報セキュリティ基本方針

島根県の情報セキュリティ基本方針を準用する。

第２章　教育情報セキュリティ対策基準

１　対象機関等

⑴　対象機関

島根県教育委員会

⑵　対象者

① 島根県教育委員会教育長
② 島根県教育委員会委員
③ 対象機関における業務に携わる教職員等（臨時的任用職員、非常勤職員等を含む）

⑶　対象資産

島根県教育委員会が保有する情報資産

ただし、知事所管情報資産（標準パソコンで取り扱う情報等）は、島根県情報セキュリティポリシーが適用されるため、本対象資産には含まれない。

⑷　留意事項

「県立学校以外において教職員用端末以外で取り扱う対象資産」は教育庁総務課が総括し、「県立学校以外において教職員用端末で取り扱う対象資産」及び「県立学校において取り扱うすべての対象資産」については、教育連携推進課教育ＤＸ推進室（以下、教育ＤＸ推進室という）が総括するものとする。

２　教育情報セキュリティの管理体制

２．１．管理体制

教育情報セキュリティポリシーに定める情報セキュリティ対策は、以下の管理体制により、体系的に実施する。

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

① 県教委の情報セキュリティを統括する最高責任者として、ＣＩＳＯを置く。
② ＣＩＳＯは、副教育長をもって充てる。
③ ＣＩＳＯは、教育情報セキュリティ委員会を招集し、主宰する。
④ ＣＩＳＯは、情報セキュリティの実施状況及び教育情報セキュリティ委員会の活動状況等について、必要に応じて教育長に報告する。
⑤ ＣＩＳＯは、情報セキュリティに係るリスク管理上の初動対応を迅速かつ機動的に進める場合など必要と認める時は、統括教育情報セキュリティ責任者にその任を代行させることができる。

⑵　統括教育情報セキュリティ責任者

①　ＣＩＳＯを補佐する者として、統括教育情報セキュリティ責任者を置く。

②　統括教育情報セキュリティ責任者は、教育監及び教育次長をもって充てる。

③　統括教育情報セキュリティ責任者は、ＣＩＳＯが不在の場合及び前項⑤に基づきＣＩＳＯの代行を命じられた場合に、その任にあたる。

④　統括教育情報セキュリティ責任者は、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。

⑶　教育情報セキュリティ責任者

①　統括教育情報セキュリティ責任者を補佐する者として、教育情報セキュリティ責任者を置く。

②　教育情報セキュリティ責任者は、教育庁総務課長及び教育ＤＸ推進室長をもって充てる。

③　教育情報セキュリティ責任者は、教育情報システムの開発、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、緊急時等における連絡体制の整備、教育情報セキュリティポリシーに関する意見の集約及び教職員等に対する研修等を行う。

⑷　教育情報セキュリティ委員会

①　情報セキュリティ対策を推進し、適正な運用及び管理を総合的に審議するため、教育情報セキュリティ委員会を置く。

②　教育情報セキュリティ委員は、別表に掲げる職にある者をもって充てる。

③　教育情報セキュリティ委員会は、教育情報セキュリティポリシーについて必要に応じて検討・見直しを行う。

④　教育情報セキュリティ委員会は、情報セキュリティに関する統一的な窓口の機能を有し、情報の安全性を侵害する重大な事故が発生した場合は、その対応策を検討する。

⑸　島根県教育委員会ＣＳＩＲＴ（シーサート）

①　情報セキュリティに係るリスク管理上の初動対応を迅速かつ機動的に進めるため、ＣＩＳＯ及び統括教育情報セキュリティ責任者の指揮のもと、島根県教育委員会ＣＳＩＲＴを置く。島根県教育委員会ＣＳＩＲＴは、必要に応じて、島根県ＣＳＩＲＴと協議しながら対応するものとする。

②　島根県教育委員会ＣＳＩＲＴの構成員は、統括教育情報セキュリティ責任者が教育情報セキュリティ委員、教育庁総務課職員、教育ＤＸ推進室職員及び委託事業者等の中から指名する。

なお、ＣＳＩＲＴの責任者を置き、ＣＳＩＲＴ内の業務統括、外部との連携等

を行う職員などを定めることとし、体制図のとおりとする。

③　島根県教育委員会ＣＳＩＲＴは、初動対応を迅速かつ機動的に遂行するために必要となる権限をＣＩＳＯ及び統括教育情報セキュリティ責任者から付与されるものとし、情報セキュリティインシデントが発生した場合は、事故対応の状況を確認し、必要に応じてシステム管理者及び関係する所属を始め全ての実施機関に対し、指示・指導・助言を行うことができる。

④　島根県教育委員会ＣＳＩＲＴは、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、その内容を対象機関へ提供する。

⑤　島根県教育委員会ＣＳＩＲＴ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、島根県ＣＳＩＲＴへ報告するとともに、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行う。

⑥　全ての対象機関は、島根県教育委員会ＣＳＩＲＴの指示・指導・助言を受けた時は、速やかに対処しなければならない。

⑦　島根県教育委員会ＣＳＩＲＴは、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等の情報セキュリティに関する統一的な窓口の機能を有する部署、委託事業者等との情報共有を行う。

⑹　教育情報セキュリティ委員会事務局

教育情報セキュリティ委員会の運営に関する事務は、教育庁総務課が所掌する。

⑺　システム管理者

①　各情報システムにおいて、この基準に基づき情報セキュリティ対策を実施し、安定的な運用を図るため、システム管理者を置く。

②　システム管理者は、各情報システムの運用管理を行う所属の長をもって充てる。

③　システム管理者は、所管する情報システムにおける開発、設定の変更、運用、更新等を行う権限及び責任を有する。

④　システム管理者は、所管する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。

⑤　新たな情報システムを開発する場合は、開発を担当する所属の長をシステム管理者とする。

⑥　システム管理者は、情報セキュリティ対策を実施し、安定的な運用を図るため必要と認める時は、その任を代行させる者を指定することができる。

⑻　ネットワーク管理者

システム管理者のうち、もっぱらネットワークの適正な運用管理を行うため、ネットワーク管理者を置く。

⑼　運用（開発）担当者

①　システム管理者を補助し、情報システムの適切な利用を推進するため、各情報

システムに運用（開発）担当者を置く。

② 運用（開発）担当者は、システム管理者が指定する者をもって充てる。

③ システム管理者は、毎年度、運用（開発）担当者の職指名を教育庁総務課長または教育ＤＸ推進室長に報告するものとする。年度途中において運用（開発）担当者を変更した場合も同様とする。

⑽ 所属長（県立学校は、２．２⑴教育情報セキュリティ管理者とする）

① 所属で保有する情報資産（システム管理者が管理するものを除く）を管理し、教育情報セキュリティ委員会及びシステム管理者が定める実施手順書に基づき、情報セキュリティ対策の適切な運用を図る。

② 所属内で情報セキュリティに関する研修及び啓発を定期的に行う。

⑾ セキュリティ担当者（県立学校は、２．２⑵教育情報セキュリティ担当者とする）

① 所属長を補助し、情報資産の適切な利用を推進するため、所属にセキュリティ担当者を置く。

② セキュリティ担当者は、総括担当の課長補佐又は所属長が指定する者（地方機関にあっては、所属長が適当と認める課長等）をもって充てる。

③ 所属長は、毎年度、セキュリティ担当者の職氏名を教育庁総務課長または教育ＤＸ推進室長に報告するものとする。年度途中においてセキュリティ担当者を変更した場合も同様とする。

④ セキュリティ担当者は、情報セキュリティ対策に関する次の各号に掲げる業務を行う。

(ｱ) コンピュータウイルス対策の徹底

(ｲ) ＩＤ、パスワード及び情報システムの設定情報の適切な運用の徹底

⑤ セキュリティ担当者は、必要に応じて所属の職員に前項に掲げる業務の遂行を補助させることができる。

⑿ 教職員等（県立学校は、２．２⑶ 教職員等とする）

所属長及びシステム管理者の指示に従い、情報資産を適切に取り扱う。

２．２．管理体制（県立学校のみ関係するもの）

⑴　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。

④　教育情報セキュリティ管理者は、２．１．⑽所属長の各項に掲げる業務を行う。

⑵　教育情報セキュリティ担当者

①　教頭及び事務長を、教育情報セキュリティ担当者とする。

②　教育情報セキュリティ担当者は、教育情報セキュリティ管理者を補佐する。

③　教育情報セキュリティ担当者は、教育情報セキュリティ管理者が不在の場合は、その任に当たる。

④　教育情報セキュリティ担当者は、２．１．⑾セキュリティ担当者の④及び⑤に掲げる業務を行う。

⑶　教職員等

教育情報セキュリティ管理者の指示に従い、情報資産を適切に取り扱う。

２．３．兼務の禁止

⑴　情報セキュリティ対策の実施において、止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。

⑵　情報セキュリティ監査の実施において、止むを得ない場合を除き、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　情報資産の分類と管理方法」以下については、「県立学校以外において教職員用端末以外で取り扱う対象資産」は、島根県情報セキュリティ対策基準を準用する。

３　情報資産の分類と管理方法

３．１．情報資産の分類

⑴　情報資産の分類

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又は児童生徒の生命、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）

情報資産の分類		情報資産の例示		
		各情報資産にアクセスする主体		
重要性分類	定義	教職員等・教育委員会	教職員等・教育委員会・児童生徒・保護者	不特定多数
Ⅰ	セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼす。	業務に係る特定の教職員等・教育委員会のみがアクセスすることが想定される情報 ○情報システムの設計に関する情報・教育情報システム設計書・設定書 ○学校運営に関する情報・入学者選抜問題・指導要録原本・教職員の人事記録 ○健康に関する情報（医師等による指導・診療・調剤の事実等要配慮個人情報を含むもの） ○指導に関する情報（犯罪の経歴、犯罪により害を被った事実、少年法に関する事項等要配慮個人情報を含むもの） ○その他要配慮個人情報を含む情報等	業務に係る特定の教職員等・教育委員会に加えて、児童生徒またはその保護者がアクセスする場合、児童生徒本人の情報のみにアクセスすることが想定される、要配慮個人情報等を含む情報 ○健康に関する情報（医師等による指導・診療・調剤の事実等要配慮個人情報を含むもの）・健康診断票 ○その他要配慮個人情報を含む情報等	
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）	業務に係る教職員等・教育委員会のみがアクセスすることが想定される情報 ○情報システムの運用に関する情報・システムログイン ID 管理台帳・端末ログイン ID 管理台帳 ○学校運営に関する情報（Ⅰを除くもの）・教職員および児童生徒の、生活歴、電話番号、メールアドレス、住所、生年月日、性別等の基本情報を含むもの ○健康に関する情報（医師等による指導・診療・調剤の事実等要配慮個人情報を含まないもの）・養護教諭・スクールカウンセラー等による記録 ○指導に関する情報（Ⅰを除くもの）・個別指導計画・生徒指導に関する記録・家庭訪問や個別面談に関する記録 ○成績に関する情報・進級・卒業認定資料 ○進路に関する情報・進路希望調査・入学者選抜に関	業務に係る教職員等・教育委員会に加えて、児童生徒またはその保護者がアクセスする場合、児童生徒本人の情報のみにアクセスすることが想定される、要配慮個人情報等を含まない情報 ○成績に関する情報・通知表・定期考査・テスト等の採点結果 ○健康に関する情報（医師等による指導・診療・調剤の事実等要配慮個人情報を含まないもの）等	

		する表簿（願書等）・調査書・推薦書・卒業生進路先情報 ○学籍に関する情報・転退学・転入学・就学・休学等に関する情報・教科用図書の給付に関する情報 ○児童生徒の氏名・所属等に関する情報・児童生徒名簿、児童生徒住所録・保護者緊急連絡網・職員緊急連絡網、職員住所録等		
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）	教職員等全員・教育委員会がアクセスすることが想定される情報 ○学校運営に関する情報（職員室等で日常的に運用するもので、Ⅱ以上を除くもの）・職員会議資料 ○児童生徒の氏名・所属等に関する情報（教室等で日常的に運用するもので、Ⅱ以上を除くもの）・出席簿等	教職員等全員・教育委員会に加えて、児童生徒及び保護者がアクセスすることが想定される情報 ○児童生徒の氏名・所属等に関する情報・座席表・児童生徒委員会名簿 ○学校運営に関する情報・卒業アルバム・児童生徒の個人写真・集合写真、学校行事等の児童生徒の写真 ○学習活動の中で生成される情報・児童生徒の学習記録（確認テスト、ワークシート、レポート、作品、日常的な簡易な健康観察等）・学習活動の記録（動画・写真等） ○学習指導に関する情報・授業用教材、児童生徒用配布プリント等	
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）	教職員等全員・教育委員会がアクセスすることが想定される、Ⅲ以上を除く情報	教職員等全員・教育委員会に加えて、児童生徒及び保護者がアクセスすることが想定される、Ⅲ以上を除く情報	不特定多数に公開することが想定される情報 ○学校運営に関する情報（広報等のため活用するもの）・学校要覧・学校紹介パンフレット・学校ホームページ掲載情報 ○学習活動で生成される情報（保護者の同意等を得て広報等のため活用するもの） 等

３．２．情報資産の管理

⑴　管理責任

①　ＣＩＳＯまたは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策定する。

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対策基準に基づき、学校での情報セキュリティ運用管理に関する実施手順を作成する。

③　教育情報セキュリティ管理者は、自校の情報資産について管理責任を有する。

④　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、実施手順に基づいた運用管理を指導する。

⑤　教職員等は、実施手順に基づき、適切に情報資産を取り扱う。

⑵　情報資産の分類の表示

教職員等は、情報資産について、その分類を表示し、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。

⑶　情報の作成

①　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。

②　情報を作成する教職員等は、情報の作成時に３．１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。

③　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。

⑷　情報資産の入手

①　本県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。

②　本県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、３．１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。

③　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。

⑸　情報資産の利用

①　情報資産を利用する教職員等は、業務以外の目的に情報資産を利用してはならない。

②　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。

③　情報資産を利用する教職員等は、電磁的記録媒体また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または保存されている領域を取り扱わなければならない。

④　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。

⑹　情報資産の保管

①　教育情報セキュリティ管理者又は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　教育情報セキュリティ管理者又はシステム管理者は、情報資産を記録した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禁止の措置を講じなければならない。

ウ　教育情報セキュリティ管理者又はシステム管理者は、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地域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。

エ　教育情報セキュリティ管理者又はシステム管理者は、重要性分類Ⅲ以上の情報を記録した電磁的記録媒体を保管する場合、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。

②　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。

⑺　情報資産の外部持ち出し

①　分類に応じた情報資産の外部持ち出し制限

ア　教職員等は、重要性分類Ⅱ以上の情報資産を外部持ち出しする場合は、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。また、持ち出し持ち帰りの記録をつけなければならない。

イ　重要性分類Ⅲの情報資産については、教職員等の外部持ち出しについて、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。

②　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（組織が利用するサーバやクラウドサービス等）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、外部ストレージサービスにより重要性分類Ⅲ以上の情報を外部送信する者は、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。

③　外部電磁的記録媒体を用いた情報の外部持ち出し

ＵＳＢメモリ等の物理的な媒体による情報の外部持ち出しでは、紛失・盗難リスクを伴うことから以下を遵守しなければならない。

ア　管理された外部電磁的記録媒体以外の使用禁止

県及び教育委員会から支給された公的な媒体のみを利用すること。

イ　外部電磁的記録媒体の暗号化の徹底

暗号化機能つきの媒体を利用し、暗号化機能を活かすこと。

④　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。

⑤　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。

⑥　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。

⑻　情報資産の廃棄

①　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。

②　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。

③　情報資産の廃棄・リース返却を行う教職員等は、教育情報セキュリティ管理者の許可を得て、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。

④　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、教職員等が立ち会わなければならない。

４．物理的セキュリティ

４．１．サーバ等の管理

⑴　機器の取付け

システム管理者は、サーバ等の機器の取付けを行う場合、地震、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に固定する等、必要な措置を講じなければならない。

⑵　サーバの冗長化

①　システム管理者は、重要性分類Ⅱ以上の情報資産を格納しているサーバを冗長化し、同一データを保持しなければならない。また、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。

②　システム管理者は、重要性分類Ⅲの情報資産を格納しているサーバのハードディスクを冗長化しなければならない。

⑶　機器の電源

①　システム管理者は、教育情報セキュリティ責任者及び施設管理部門と連携し、重要性分類Ⅱ以上の情報資産を格納している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、当該機器が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。

②　システム管理者は、教育情報セキュリティ責任者及び施設管理部門と連携し、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。

⑷　通信ケーブル等の配線

①　教育情報セキュリティ責任者及びシステム管理者は、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。

②　教育情報セキュリティ責任者及びシステム管理者は、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。

③　教育情報セキュリティ責任者及びシステム管理者は、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。

④　教育情報セキュリティ責任者及びシステム管理者は、自ら又はネットワークを管理する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又は追加できないように必要な措置を施さなければならない。

⑸　機器の定期保守及び修理

①　システム管理者は、重要性分類Ⅲ以上のサーバ等の機器の定期保守を実施しなければならない。

②　システム管理者は、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。内容を消去できない場合、システム管理者は、外部の事業者に故障を修理させるに当たり、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とともに秘密保持体制の確認等を行わなければならない。

⑹　施設外又は学校外への機器の設置

教育情報セキュリティ責任者及びシステム管理者は、施設外又は学校外にサーバ等の機器を設置する場合、ＣＩＳＯの承認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。

⑺　機器の廃棄等

システム管理者は、機器を廃棄又はリース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

４．２．通信回線及び通信回線装置の管理

⑴　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。

⑵　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。

⑶　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教育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。

⑷　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。

⑸　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教育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。

⑹　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。

４．３．教職員等の利用する端末や電磁的記録媒体等の管理

⑴　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。

⑵　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。

⑶　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。

⑷　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、不正アクセスや教職員等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。

⑸　教育情報セキュリティ責任者は、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。

⑹　教育情報セキュリティ責任者は、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。

４．４．学習者用端末のセキュリティ対策

⑴　不適切なウェブページの閲覧防止

教育情報セキュリティ責任者及びシステム管理者は、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。

⑵　マルウェア感染対策

教育情報セキュリティ管理者は、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。

⑶　端末を不正利用させないための防止策

教育情報セキュリティ管理者は、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。

⑷　セキュリティ設定の一元管理

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。

⑸　端末の盗難・紛失時の情報漏洩対策

教育情報セキュリティ責任者及びシステム管理者は、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。

４．５．パソコン教室等における学習者用端末や電磁的記録媒体の管理

⑴　教育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。

⑵　教育情報セキュリティ管理者は、パソコン及び電磁的記録媒体について、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。

⑶　教育情報セキュリティ管理者は、教育情報システムへのアクセスにおけるログインパスワードの入力等による認証を設定しなければならない。

５．人的セキュリティ

５．１．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 情報資産の持ち出しの記録管理

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ポリシー等の閲覧容易性確保

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 教職員等への教育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本県に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、必要に応じて教育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、教育情報セキュリティ責任者に上申して、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、教育情報セキュリティ責任者に上申して、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

① 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 教育情報セキュリティ管理者は、自己点検の結果を教育情報セキュリティ委員会に報告しなければならない。

５．２．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 執務室の施錠管理

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 来校者等への対応

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教育情報セキュリティ担当者の許可を求めなければならない。

③ 机上の書類・端末等の管理

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、離席時のパソコン、モバイル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。

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 業務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、電源を落とさなければならない。

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 教職員等は、休暇連絡等別に定める軽易な事務を除いて、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を原則業務に利用してはならない。ただし、業務上必要な場合は、教育情報セキュリティ責任者の定める手順に従い、教育情報セキュリティ管理者の許可を得て利用することができる。

② 教職員等は、①に従って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を用いる場合には、必要な安全管理措置を講じなければならない。

⑸　支給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（本対策基準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　教職員等は、支給端末、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　教職員等は、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。

⑹　ＩＤ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、教育情報セキュリティ責任者又は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　サーバ、ネットワーク機器及びパソコン等の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）

⑨　共有ＩＤに対するパスワードは定期的に又はアクセス回数に基づいて変更しなければならない。

⑻　外部電磁的記録媒体の取扱い

①　利用する外部電磁的記録媒体は県、教育委員会又は学校から支給された媒体を使用しなければならない。その他の媒体の使用は禁止する。

② 外部電磁的記録媒体は、職員室の書庫等の鍵のかかる場所に施錠保管しなければならない。

⑼ 電子メールの利用制限

① 教職員等は、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。
② 教職員等は、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。
③ 教職員等は、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。
④ 教職員等は、重要な電子メールを誤送信した場合、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。
⑤ 教職員等は、ウェブで利用できるフリーメールサービス等を使用してはならない。
⑥ 情報ファイルを添付する場合には、パスワード設定等の対策を講じなければならない。その際、パスワードを同一メールに記載しないこと。
⑦ 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。
⑧ 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。

⑽ 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。

⑾ 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　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　パソコン等の端末の場合　有線ＬＡＮにつながる業務端末（教職員用端末等）の場合は、ＬＡＮケーブルの即時取り外しを行わなければならない。
イ　モバイル端末の場合　無線ＬＡＮにつながる業務端末（教職員用端末及び学習者用端末）の場合は、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。
ウ　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。

⑿　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。

⒀　無許可ソフトウェアの導入等の禁止

①　教職員等は、パソコンやモバイル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、教育情報セキュリティ責任者及び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。

⒁　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、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、教育情報セキュリティ責任者及びシステム管理者の許可を得なければならない。

⑮ 無許可での教育情報ネットワーク接続の禁止

教職員等は、教育情報セキュリティ責任者の許可なくパソコンやモバイル端末を教育情報ネットワークに接続してはならない。

⑯ 業務以外の目的でのウェブ閲覧の禁止

教職員等は、業務以外の目的でウェブを閲覧してはならない。

⑰ 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 学習用途の利用限定
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 利用者認証情報の秘匿管理
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の管理
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 端末のソフトウェアに関するセキュリティ機能の設定変更禁止
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 学習系情報は学習系クラウドに保管
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禁止
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 コミュニケーションツールの利用制限
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 ウイルス感染が疑われる場合の報告
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 端末の安全な取扱い
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の利用禁止
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（児童生徒本人の情報に限る）の管理該当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。

⑱　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。

５．３．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　教職員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教職員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　知り得た情報の秘匿
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。

５．４．研修

⑴　情報セキュリティに関する研修

ＣＩＳＯは、定期的に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。

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、教育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、システム管理者、セキュリティ担当者、教育情報セキュリティ管理者、教育情報セ

キュリティ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、教育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　研修への参加

全ての教職員等は、定められた研修に参加しなければならない。

５．５．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、速やかに教育情報セキュリティ責任者、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及び総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。

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、速やかに教育情報セキュリティ責任者及び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及び総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。

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責任者、教育情報セキュリティ管理者、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。

６．技術的セキュリティ

６．１．コンピュータ及びネットワークの設定管理

⑴　文書サーバ及び端末の設定等

①　システム管理者は、教職員等が使用できる文書サーバの容量を設定し、教職員等に周知しなければならない。

②　システム管理者は、文書サーバを学校等の単位で構成し、教職員等が他の学校等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。

③　システム管理者は、住民の個人情報、人事記録等、特定の教職員等しか取扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一学校等であっても、担当職員以外の教職員等が閲覧及び使用できないようにしなければならない。

④　システム管理者は、インターネット接続を前提とする校務外部接続系サーバ及び学習系サーバに保管する情報（学習系サーバにおいては、個人情報などを含む重要性が高い情報を保管する場合に限る）については、標的型攻撃等によるデータの外部流出の可能性を考慮し、データ暗号化等による安全管理措置を講じなければならない。

⑵　ログの取得等

①　教育情報セキュリティ責任者及びシステム管理者は、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　教育情報セキュリティ責任者及びシステム管理者は、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　教育情報セキュリティ責任者及びシステム管理者は、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。

⑶　ネットワークの接続制御、経路制御等

①　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　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。

⑷　外部の者が利用できるシステムの分離等

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、特に情報資産重要性分類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）以上を扱うシステムとの論理的又は物理的な分離、もしくは各システムにおけるアクセス権管理の徹底を行うこと。

⑸ 外部ネットワークとの接続制限等

① システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、ＣＩＳＯ及び統括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。

② システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内及び学校の全てのネットワーク、情報システム等の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。

③ システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、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処するため、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しなければならない。

④ 教育情報セキュリティ責任者及びシステム管理者は、ウェブサーバ等をインターネットに公開する場合、教育情報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。

⑤ 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、情報資産に脅威が生じることが想定される場合には、教育情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

⑹ 重要性が高い情報に対するインターネットを介した外部からのリスク、児童生徒による重要性が高い情報へのアクセスリスクへの対応

① システム管理者は、強固なアクセス制御による対策を講じたシステム構成の場合は、各システムにおけるアクセス権管理の徹底をしなければならない。 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を介した外部からのリスクの高いシステムと重要性が高い情報（特に校務系）を論理的又は物理的に分離をしなければならない。

② 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、各システムにおけるアクセス権管理の徹底を行う等の適切な措置を図らなければならない。また、ネットワ

ーク分離による対策を講じたシステム構成で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。

⑺ 複合機のセキュリティ管理

① 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 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 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。

⑻ 特定用途機器のセキュリティ管理

教育情報セキュリティ責任者は、特定用途機器について、取り扱う情報、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実施しなければならない。

⑼ 無線 LAN 及びネットワークの盗聴対策

① 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 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。

６．２．アクセス制御

⑴ アクセス制御等

教育情報セキュリティ責任者及びシステム管理者は、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 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小限の者に限定しなければならない。
② 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 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 教育情報セキュリティ責任者は、外部から教育ネットワークに接続することを許可する場合は、利用者のＩＤ及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（ＩＣカード等）による認証に加えて通信内容の暗号化等、情報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 端末とネットワークの接続可否の自動識別（端末認証）の設定

教育情報セキュリティ責任者及びシステム管理者は、ネットワークで使用される機器について、機器固有情報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システムを設定しなければならない。

⑷ ログイン時の表示等

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。

⑸ 特権による接続時間の制限

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。

６．３．システム開発、導入、保守等

⑴ 情報システムの調達

① 教育情報セキュリティ責任者及びシステム管理者は、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 教育情報セキュリティ責任者及びシステム管理者は、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 システム開発における責任者及び作業者の特定

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 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 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 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 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 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 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 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 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 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 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 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 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 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　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　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　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　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　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　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

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

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

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。

６．４．不正プログラム対策

⑴　教育情報セキュリティ責任者の措置事項

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 システム管理者の措置事項

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 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。
③ インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、県及び県教育委員会が管理している電磁的記録媒体以外を教職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

６．５．不正アクセス対策

⑴ 教育情報セキュリティ責任者の措置事項

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、教育情報セキュリティ責任者及び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　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　攻撃の予告

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ることが明確になった場合、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、関係機関と連絡を密にして情報の収集に努めなければならない。

⑶　サービス不能攻撃

教育情報セキュリティ責任者及びシステム管理者は、外部からアクセスできる教育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、教育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。

⑷　標的型攻撃

教育情報セキュリティ責任者及びシステム管理者は、教育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。

６．６．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

教育情報セキュリティ責任者及びシステム管理者は、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

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

教育情報セキュリティ責任者及びシステム管理者は、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。

７．運用

７．１．情報システムの監視

⑴　教育情報セキュリティ責任者及びシステム管理者は、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、侵入検知システム（ＩＤＳ）や侵入防御システム（ＩＰＳ）などの端末・サーバ・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。

⑵　教育情報セキュリティ責任者及びシステム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置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及びシステム管理者は、重要性分類Ⅱ以上の情報資産を格納するシステムを常時監視しなければならない。

⑷　教育情報セキュリティ責任者及びシステム管理者は、重要性分類Ⅲの情報資産を格納するシステムを常時監視しなければならない。

⑸　内部からの攻撃監視

教育情報セキュリティ責任者及びシステム管理者は、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。

７．２．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　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　教育情報セキュリティ責任者及びシステム管理者は、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　教育情報セキュリティ責任者、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

教育情報セキュリティ責任者及びシステム管理者は、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、紛失したりすることがないよう、適切に管理しなければならない。

⑶ 障害記録の管理

教育情報セキュリティ責任者及びシステム管理者は、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。

７．３．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 教育情報セキュリティ責任者及びシステム管理者は、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 教育情報セキュリティ責任者及びシステム管理者は、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。

⑵ パスワードに関する情報の管理

① 教育情報セキュリティ責任者又はシステム管理者は、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 教育情報セキュリティ責任者又はシステム管理者は、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。

７．４．児童生徒におけるＩＤ及びパスワード等の管理

⑴ ＩＤ登録・変更・削除

① 入学/転入時のＩＤ登録処理

ＩＤ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。

② 進級/進学時のＩＤ関連情報の更新

ＩＤ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 転出/卒業/退学時のＩＤ削除処理

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 多要素認証等によるなりすまし対策

本人確認を厳格に行う必要がある場合においては児童生徒のＩＤ及びパスワードに加えて多要素認証を設定することが望ましい。

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。

⑶ 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。

７．５．特権を付与されたＩＤの管理等

⑴ 教育情報セキュリティ責任者及びシステム管理者は、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。

⑵　教育情報セキュリティ責任者及びシステム管理者の特権を代行する者は、教育情報セキュリティ責任者及び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。

⑶　ＣＩＳＯ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システム管理者に通知しなければならない。

⑷　教育情報セキュリティ責任者及びシステム管理者は、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。

⑸　教育情報セキュリティ責任者及びシステム管理者は、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。

⑹　教育情報セキュリティ責任者及びシステム管理者は、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。

７．６．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　遵守状況の確認及び対処

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　教育情報セキュリティ責任者及びシステム管理者は、ネットワーク及びサーバ等のシステム設定等における教育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　パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

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パソコン、モバイル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

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

教育情報セキュリティ責任者及びシステム管理者は、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。

７．７．侵害時の対応等

⑴ 緊急時対応計画の策定

ＣＩＳＯ又は教育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、教育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、教育情報セキュリティ委員会は当該計画と教育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又は教育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。

７．８．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。

７．９．法令等遵守

⑴ 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）

７.10. 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 教育情報セキュリティ責任者が違反を確認した場合は、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 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、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、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。

８．外部委託

⑴　外部委託事業者の選定基準

①　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　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
- 県による監査、検査
- 教育委員会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

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、⑵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

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、教育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。

９．SaaS 型パブリッククラウドサービスの利用

９．１．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、「７．５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、当該クラウドサービスのサーバ等の管理条件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、クラウド事業者側の管理区域（サーバ等を設置）及び保守運用拠点の管理対策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い。

② クラウド利用者は、当該クラウドサービスにおけるサーバの冗長化対策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、当該クラウドサービスにおけるデータバックアップ及び復旧手順についての対策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、当該クラウドサービスにおける情報セキュリティの確保や監査に必要なログの取得についての対策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、クラウドサービスにアクセスするクラウドを利用する教職員等及び児童生徒側端末について、保管するデータの外部流出、改ざん等から保護するために必要な措置を講じなければならない。

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。

⒀　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。

９．２．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。

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。

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。

９．３．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

⑴　ＩＤ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。

⑸　SaaS 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。

９．４．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 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 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。

９．５．ソーシャルメディアサービスの利用

⑴ 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 教育委員会又は学校のアカウントによる情報発信が、実際の教育委員会又は学校からのものであることを明らかにするために、教育委員会又は学校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

⑵　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。

⑶　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。

10. 評価・見直し

10.１．監査

⑴ 実施方法

ＣＩＳＯは、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、毎年度及び必要に応じ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、教育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、教育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

教育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。

10.２．自己点検

⑴ 実施方法

① 教育情報セキュリティ責任者及びシステム管理者は、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、教育情報セキュリティ責任者及びシステム管理者は、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、教育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 教育情報セキュリティ委員会は、この点検結果を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、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。

10.３．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情報セキュリティに関する状況の変化等をふまえ、教育情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。

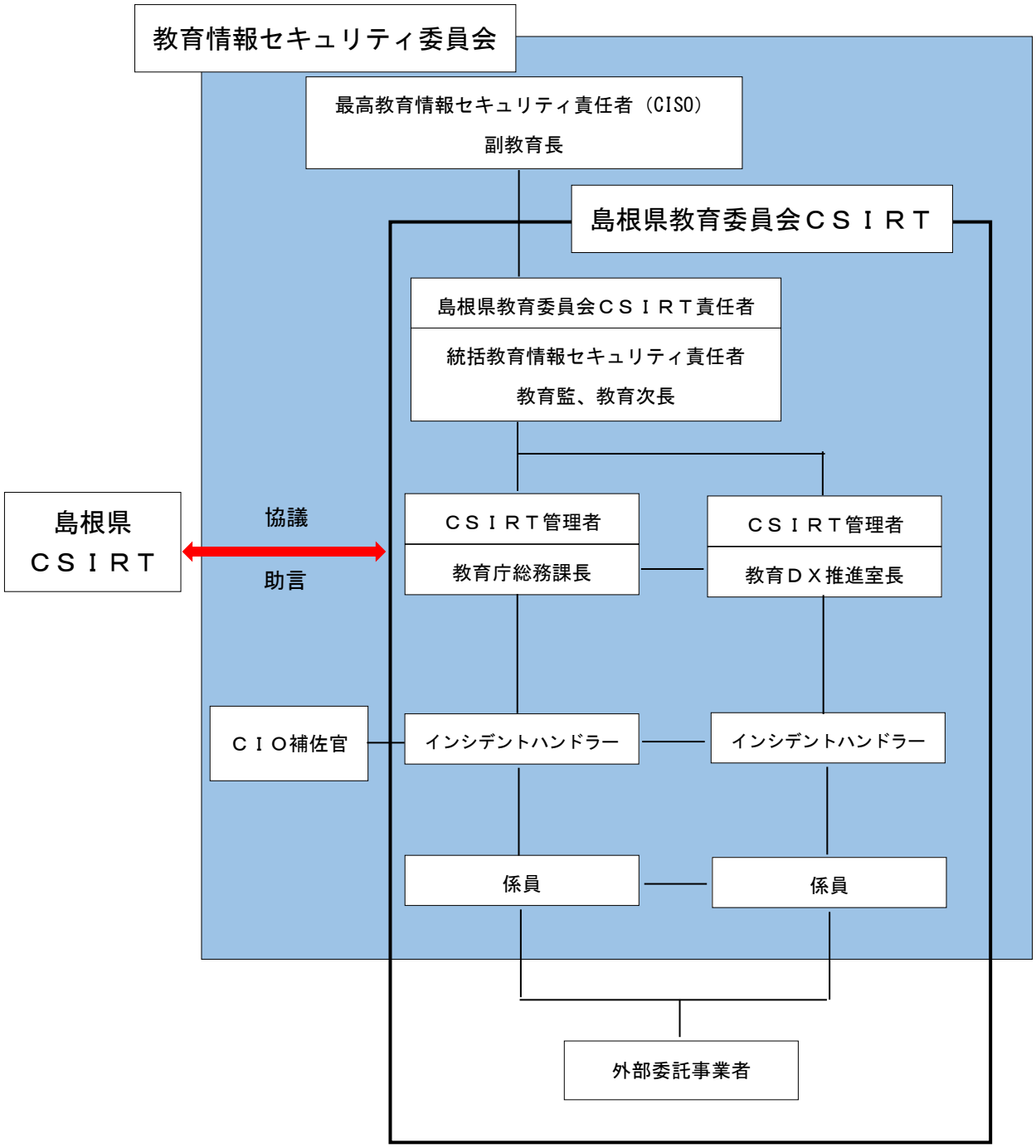
附則

１　この教育情報セキュリティポリシーは、令和８年４月１日から施行する。

【別表】教育情報セキュリティ委員名簿

委員長	最高教育情報セキュリティ責任者（ＣＩＳＯ）
副委員長	統括教育情報セキュリティ責任者
委員	教育庁総務課長
	教育施設課長
	学校企画課長
	学校教育課長
	教育連携推進課長
	教育ＤＸ推進室長
	特別支援教育課長
	保健体育課長
	社会教育課長
	人権同和教育課長
	文化財課長
	福利課長
	教育センター所長
事務局	教育庁総務課

【参考】島根県教育委員会ＣＳＩＲＴ体制図



【参考】情報インシデント発生時の通報先

発生機関	発生源	通報先
本庁 教育事務所 埋蔵文化財調査センター 教育機関	標準ＰＣ、公用ＵＳＢ（※）	情報システム推進課
	教職員用端末	教育ＤＸ推進室
	標準ＰＣ、教職員用端末以外の端末	教育庁総務課
	その他（ＵＳＢ、ＦＡＸ、紙等）	
県立学校	標準ＰＣ、公用ＵＳＢ（※）	情報システム推進課
	教職員用端末	教育ＤＸ推進室
	標準ＰＣ、教職員用端末以外の端末	
	その他（ＵＳＢ、ＦＡＸ、紙等）	

（※）公用ＵＳＢとは、情報システム推進課から貸し出されたものをいう。

【参考】セキュリティ担当者等の報告先

報告元	報告先
本庁 教育事務所 埋蔵文化財調査センター 教育機関	教育庁総務課
県立学校	教育ＤＸ推進室

【参考】島根県情報セキュリティポリシー（第１章　情報セキュリティ基本方針）

１　目　的

この基本方針は、県が保有する情報資産の機密性、完全性及び可用性を維持するため、県が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

２　定　義

⑴ 情報資産

情報及び情報システムをいう。

⑵ 情報

職務の遂行に伴って取り扱う全ての情報（紙及び電磁的記録媒体に記録されたもの、会話等を含む）をいう。

⑶ ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

⑷ 情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

⑸ 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

⑹ 情報セキュリティポリシー

情報セキュリティ基本方針及び情報セキュリティ対策基準をいう。

⑺ 機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

⑻ 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

⑼ 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

⑽ マイナンバー利用事務系

「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」に規定された個人番号利用事務に関わる情報システムをいう。

⑾ 行政系

職員等が一般行政事務に使用することを目的とし、総合行政ネットワーク（以下、「ＬGWAN」という。）に接続された情報システムをいう（マイナンバー利用事務系を除く。）。

⑿ インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システムをいう。

⒀ 通信経路の分割

行政系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

⒁ 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着がない等、安全が確保された通信をいう。

⒂ 情報セキュリティインシデント

単独もしくは一連の望まないあるいは予期しない情報セキュリティに関する事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。具体的にはサイバー攻撃、意図的な要因による情報漏えい、破壊、改ざん、機器故障等の非意図的な要因による情報漏えい、破壊、改ざん等をいう。

3　対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

⑴　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

⑵　情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

⑶　地震、落雷、火災等の災害によるサービス及び業務の停止等

⑷　大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

⑸　電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

4　対象機関

情報セキュリティポリシーの対象となる機関（以下「実施機関」という。）は、知事部局、企業局、病院局、議会事務局、各行政委員会及び警察本部（警察署を含む。）とする。なお、知事部局及び企業局以外の機関については、知事が管理運用する情報資産を利用する場合に限る。ただし、知事部局及び企業局以外の機関が知事が管理運用する以外の情報資産を利用する場合に、この情報セキュリティポリシーを準用することは妨げない。

5　職員等の義務

職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければな

らない。

6　情報セキュリティ対策

上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

⑴ 組織体制

県の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

⑵ 情報資産の分類と管理

県の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

⑶ 情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

① マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、重要情報の流出を防ぐ。

② 行政系においては、行政系の情報システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③ インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、県及び市町村のインターネットとの通信を集約した上で、しまねセキュリティクラウドの導入等を実施する。

⑷ 物理的セキュリティ

サーバ、情報システム室、通信回線及び職員等のパソコンやモバイル端末の管理について、物理的な対策を講じる。

⑸ 人的セキュリティ

情報セキュリティに関し、職員等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る。

⑹ 技術的セキュリティ

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、不正アクセス対策等の技術的対策を講じる。

⑺ 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

⑻ 業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者（再委託事業者等も含む）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確認し、必要に応じて契約に基づき措置を講じる。

外部サービス（クラウドサービス）を利用する場合には、利用にかかる規程を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、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る。

7　情報セキュリティ監査及び自己点検の実施

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及び自己点検を実施する。

8　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

9　情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

10　情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、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するものとする。

なお、情報セキュリティ実施手順は、公にすることにより県の行政運営に重大な支障を及ぼすおそれがあることから非公開とする