令和８年４月改訂版

能登町
教育情報セキュリティポリシーに関するガイドライン

１．基本方針

【教育情報セキュリティポリシー等の遵守】

教育情報セキュリティを確保するために、定められている事項等を遵守しなければならない。また、教育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。

【ネットワーク運用に係る組織の設置】

学校の情報セキュリティ管理については、以下の組織・体制とする。

（１）最高情報セキュリティ責任者（CISO）

副町長または総務課長を、地方公共団体における全ての教育ネットワーク、情報システム等の情報資産の管理や情報セキュリティに関する権限及び責任を有する最高情報セキュリティ責任者（CISO）とする。

（２）最高情報統括責任者（CIO）

副町長または総務課長を、情報通信技術の活用による住民の利便性の向上及び行政運営改善等に関するものを統括する最高情報統括責任者（CIO）とする。

（３）統括教育情報セキュリティ責任者

教育長を、CISO を補佐する役割であり、地方公共団体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、見直し等の権限及び責任を有するほか、情報セキュリティ対策に関する権限及び責任を、また、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統括教育情報セキュリティ責任者とする。緊急時等の円滑な情報共有のために関係者の緊急連絡網を整備し、情報セキュリティインシデント発生時等には中心となって被害の拡大防止、事態の回復のための対策実施、再発防止策の検討を行う。

（４）教育情報セキュリティ責任者

教育委員会事務局長を、教育情報セキュリティ対策に関する権限及び責任を有し、地方公共団体が所有している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教育情報セキュリティ責任者とする。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に対する教育、訓練、助言及び指示を行う。

（５）教育情報システム管理者

教育委員会事務局長を、個々の教育情報システムの開発、設定の変更、運用、見直し等を行う権限及び責任を有するほか、所管する教育情報システムに対する情報セキュリティに関する権限及び責任を有する教育情報システム管理者とする。個々の教育情報システムに関する情報セキュリティ実施手順の維持・管理を行う。

（６）教育情報システム担当者

教育委員会事務局職員を、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、見直し等の作業を行う教育情報システム担当者とする。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する。

（７）教育情報セキュリティ管理者

各学校長を、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教育情報セキュリティ管理者とする。学校で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、指示を仰ぐ。なお、教職員等は、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する。

（８）情報セキュリティ委員会

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。毎年度、情報セキュリティ対策の改善計画を策定してその実施状況を確認する役割を合わせて担うことが望ましい。

（９）情報セキュリティに関する統一的な窓口

情報セキュリティインシデントのとりまとめ、CISO・CIO への報告、報道機関等への通知・公表、関係機関との情報共有などの、情報セキュリティインシデントに関するコミュニケーションの核となる体制であり、その窓口を教育委員会事務局が担う。

２．対策基準

【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軽微な影響を及ぼす。（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）

【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
（１）教育情報セキュリティポリシー等の遵守
（２）業務以外の目的での使用の禁止
（３）校務用端末による外部における情報処理作業の禁止
（４）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
（５）知りえた情報の秘匿
（６）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

【教職員等の遵守事項及び実施事項】
　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。
（１）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。

（２）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学校教育情報セキュリティ・システム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。

（３）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。

（４）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、業務上やむを得ない場合を除いて、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。
②教職員等は、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、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。

（５）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教職員等は、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。

（６）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、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。

（７）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。

（８）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教育委員会又は学校から支給された公式の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。

（９）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。
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ぎなければならない。

（１０）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。

（１１）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）パソコン等の端末の場合 有線 LAN につながる業務端末（校務用端末等）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（指導者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。

（１２）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。
③CISO 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。

（１３）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、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。

（１４）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、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。

（１５）無許可でのネットワーク接続の禁止
　教職員等は、統括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）外部からのアクセス等の制限
①教職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、教育情報セキュリティ管理者を介して、統括教育情報セキュリティ責任者及び当該情報システムを管理する教育情報システム管理者の許可を得なければならない。
②教職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を施設内のネットワークに接続する前に、アンチウイルス等を通じて、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

（１８）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（SNS,チャット等）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

（１９）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。

※なお、このガイドラインは能登町情報セキュリティポリシーに準じる。