平内町教育情報セキュリティ対策基準

制定日：令和６年 10 月 31 日

平内町教育委員会

-目次-

1. 目的

平内町教育情報セキュリティ対策基準とは、平内町情報セキュリティ基本方針に基づき、学校にかかる情報資産への情報セキュリティ対策等を実施するために、平内町の小中学校における共通の基準として遵守事項及び判断基準を定めたものである。

2. 適用範囲及び用語説明

2.1 適用範囲

平内町小中学校設置条例(昭和 39 年７月６日条例第 20 号)により設置する小中学校

2.2 用語説明

（１）校務系情報

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

（２）校務外部接続系情報

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

（３）学習系情報

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

（４）校務系システム

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

（５）校務外部接続系システム

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

（６）学習系システム

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

3. 組織体制

3.1 体制

（１） 教育情報セキュリティ統括責任者

平内町教育委員会は、設置する学校における教育情報セキュリティ全般を管理し、その教育情報セキュリティ統括責任者を平内町教育委員会教育長（以下「教育長」という）とする。

（2）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

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を平内町教育委員会学校教育課長（以下「課長」という。）が兼ねる。

（3）教育情報セキュリティ管理者

設置された学校においては当該の校長を教育情報セキュリティ管理者とする。

（4）学校情報取扱者

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

3.2　権限と責任

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

（1）教育情報セキュリティ統括責任者（教育長）

・教育情報セキュリティ統括責任者は、町内のすべての学校における教育情報システムの運用及び情報セキュリティ対策に関する権限と責任を有する。

・教育情報セキュリティ統括責任者は、情報セキュリティインシデント発生時には、その状況を確認し、被害の拡大防止、事態の回復、再発防止策の検討を行う体制を整備しなければならない。

（2） 教育情報セキュリティ責任者（課長）

・ 教育情報セキュリティ責任者は、学校にかかる共通的なネットワーク、情報システム、情報等の情報資産に関する情報セキュリティ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責任者は、学校にかかる情報資産に対する情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合に、統括責任者の指示に従い、必要な措置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（課長）

・教育情報システム管理者は教育情報資産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は、情報資産に対する情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合に、教育情報セキュリティ統括責任者の指示に従い、必要な措置を実施する。

（4）教育情報セキュリティ管理者（校長）

教育情報セキュリティ管理者は、所管する学校における情報資産の情報セキュリティ対策に関する権限及び責任を有する。

教育情報セキュリティ管理者は、教育情報システム管理者の指示に従い学校にかかる共通的なネットワーク、情報システム、情報等の情報資産のうち所管する学校のパーソナルコンピュータ等についての管理を行う。

教育情報セキュリティ管理者は、所管する学校における情報等の情報資産に対する情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合には、教育情報セキュリティ統括責

任者、教育情報セキュリティ責任者、教育情報システム管理者へ速やかに報告を行い、指示を仰がなければならない。

（５）学校情報取扱者（教職員）

学校情報取扱者は、セキュリティポリシーを遵守し、学校における情報資産の作成・入手・利用等を行う。

4. 情報資産の分類と管理

4.1 情報資産の分類と管理方法

対象となる情報資産は、各々の情報資産の機密性、完全性及び可用性を踏まえ、次の重要性分類に従って分類する。なお情報資産の機密性、完全性及び可用性の各要素を分類基準に照らし合わせて、最も高い分類をその情報資産の重要性とする。

（１）情報資産の分類

ア 機密性

分類	分類基準
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
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
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
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

イ 完全性

分類	分類基準
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
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
１	完全性 2A 又は完全性 2B の情報資産以外の情報資産

ウ 可用性

分類	分類基準
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
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
1	可用性 2A 又は可用性 2B の情報資産以外の情報資産

（2）重要性分類

重要性	重要性の定義
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と想定される情報資産
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と想定される情報資産
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情報資産
Ⅳ	影響をほとんど及ぼさない情報資産（上記Ⅰ、Ⅱ、Ⅲ以外のもの）。

（3）情報資産の例

重要性分類	情報資産の例		
Ⅰ	・指導要録原本 ・教職員の人事情報 ・入学者選抜問題 ・教育情報システム仕様書		
Ⅱ	○学籍関係 ・卒業証書授与台帳 ・転入退学受付（整理）簿 ・就学児童・生徒異動報告書 ・休学・退学願等受付（整理）簿 ・教科用図書給付児童・生徒名簿 ・要・準要保護児童・生徒認定台帳 ・その他校内就学援助関係書類 ○成績関係 ・通知表 ・評定一覧表 ・進級・卒業認定資料 ・定期考査・テスト等の答案用紙	○進路関係 ・調査書 ・推薦書 ・公立高校入学者選抜に係る成績一覧表 ・入学者選抜に関する表簿（願書等） ・私立高校入試に係る事前相談資料 ・卒業生進路先一覧等 ・進路希望調査 ・進路判定会議資料 ・進路指導記録簿 ○児童・生徒に関する個人情報 （生活歴、心身の状況、財産状況等の	○教職員に割り当てた機密性の高い情報 ・情報システムログイン ID/PW 管理台帳 ・情報端末ログイン ID/PW 管理台帳 ○児童生徒の学習系情報 ・学習システムログイン ID/PW 管理台帳 ・学習用端末 ID/PW 管理台帳 ○名簿等 ・児童生徒名簿 ・保護者緊急連絡網

	・定期考査素点表 ・成績に関する個票等 〇指導関係 ・事故報告書・記録簿 ・生徒指導・特別指導等記録簿 ・児童・生徒等の写真 ・指導記録・指導カード ・教育相談・面接の記録・カード等 ・個別の教育支援計画 （学校生活支援シート） ・個別指導計画 ・家庭訪問記録・個別面談記録 ・教務手帳 ・週ごとの指導計画 （個人情報が含まれるもの）	情報、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） 〇学校教職員に関する個人情報 （病歴、心身の状況、収入等の情報、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） 〇健康関係 ・健康診断票 ・歯の検査表 ・心臓管理等医療情報 ・学校生活管理指導票 ・児童・生徒等健康調査票 ・児童・生徒の健康保険等被保険者証の写 ・健康診断に関する表簿 ・就学時健康診断票	・児童生徒の住所録 ・PTA 会員名簿 ・職員緊急連絡網・職員住所録 ・委員会名簿 ・PTA 役員連絡網 〇各種帳票ファイル ・指導要録作成システム等、データの入っていない帳票 〇その他 ・給食関係書類
Ⅲ	〇児童生徒の氏名 ・出席簿 ・名列表 ・座席表 ・児童生徒委員会名簿	〇学校運営関係 ・卒業アルバム ・学校行事等の児童・生徒の写真 ・授業用教材 ・教材研究資料 ・生徒用配布プリント	〇児童生徒の学習系情報 ・児童生徒の学習記録 （確認テスト、ワークシート、レポート、作品等） ・学習活動の記録（動画・写真等）
Ⅳ	〇学校運営関係 ・学校要覧 ・学校紹介パンフレット ・使用教科書一覧 ・教育課程編成表 ・学校設定科目の届け出 ・学校徴収金会計簿 （学年費、教育振興費等）	・学校行事実施計画 （避難訓練・体育祭実施計画等） ・保護者等への配布文書文例 ・各種届様式・校務分掌表 ・ＰＴＡ資料 ・学校・学年・学級だより ・学校ホームページ掲載情報 ・学校行事のしおり	〇学校活動の記録 ※以下は保護者の承諾がある場合に限る ・学校行事等の児童・生徒の写真 ・学習活動の記録（動画・写真・作品等）

※ 本表は例示であり、個別の事情により本表とは異なる分類となる場合がある。

「4.1(1) 分類基準」に従い、判断すること。

（4）重要性分類に応じた対応

・ 情報資産の重要性分類Ⅰ～Ⅲに分類される情報資産は、この対策基準の対象とする。

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

4.2 情報資産の管理

（1）管理責任

・ 情報資産は、教育情報セキュリティ管理者がそれぞれ所管する情報資産についての管理責任を有する。

・ 教育情報セキュリティ管理者は、情報が複製又は伝送された場合には、当該複製等も原本と同様に管理しなければならない。

・ 学校情報取扱者は、情報資産について、ファイル、電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

（2）情報の作成

・ 学校情報取扱者は、業務上必要のない情報を作成してはならない。

・ 学校情報取扱者は、情報の作成時に重要性分類に基づき、当該情報の分類と取扱制限を定めなければならない。

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

（3）情報資産の入手

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

・ 学校情報取扱者は、学校外の者が作成した情報資産を入手したときは、重要性分類に基づき、当該情報の分類と取扱制限を定めなければならない。

（4）情報資産の利用

・ 学校情報取扱者は、情報資産を業務以外の目的に利用してはならない。

・ 情報資産の利用においては、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。

（5）情報資産の保管

・ 教育情報システム管理者又は教育情報セキュリティ管理者は、情報資産の重要性分類に従って、情報資産を適切に保管しなければならない。

・ 教育情報システム管理者又は教育情報セキュリティ管理者は、情報資産をデジタルデータとして保管する場合は、教育委員会が指定するサーバまたはクラウドサービスを利用し保管しなければならない。

（6）情報資産の運搬《原則禁止》

・ 重要性Ⅰ・Ⅱの情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化又

はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

・ 重要性Ⅰ・Ⅱの情報資産を運搬する者は、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。

（7）情報資産の提供・公表

・ 重要性Ⅲ以上の情報資産を外部に提供する者は、必要に応じアクセス制限や暗号化、パスワード設定等を行わなければならない。

・ 重要性Ⅰ・Ⅱの情報資産を外部に提供する者は、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。

・ 教育情報システム管理者又は教育情報セキュリティ管理者は、保護者等に公開する情報資産について、完全性を確保しなければならない。

（8）情報資産の廃棄等

・ 情報資産の廃棄を行う者は、情報を復元不可能な状態にしなければならない。また、行った処理について日時及び処理内容等を記録しなければならない。

・ 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を終了する場合は、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。

5. 人的セキュリティ

5.1 教職員の遵守事項

（1）情報セキュリティポリシー等の遵守

教職員は、情報セキュリティポリシー及びこれに基づく文書に定められている事項を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点がある場合には、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）業務以外の目的での使用禁止

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

（3）ID 及びのパスワードの管理・取扱

・ 学校情報取扱者は、自己が利用している ID を他人に利用させてはならない。

・ 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。

・ 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。

・ パスワードは秘密にし、パスワードの照会等には一切応じてはならない。

・ 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い。

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

・ パーソナルコンピュータ等の端末に原則としてパスワードを記憶させてはならない。
・ 学校情報取扱者間でパスワードを共有してはならない。

（3）指示に基づいた情報資産の利用等

教職員は、教育情報セキュリティ管理者の指示に従って情報資産を利用するとともに、設定の変更、運用、更新等の作業を行う。

（4）情報資産の持ち出し及び送信禁止

教職員は、教育情報セキュリティ管理者の許可を得た場合に限り、記録を作成したうえで、所属する学校の外へ情報資産を持ち出し又は送信することができる。

（5）所属する学校の外への端末持ち出し時の対策

・ 所属する学校の外で端末を利用する場合は、端末内部に重要性Ⅰ～Ⅲの情報を保存してはならない。また、通信については、暗号化されたものを使用しなければならない。
・ 教職員は紛失・盗難を防止するため、移動の際は細心の注意をもって端末等を携行しなければならない。
・ 教職員は不正使用を防止するため、端末を使用しないときは、他者に端末が使用されないように必要な対策を取らなければならない。

（6）所属する学校の外における情報処理作業の制限

・ 重要性Ⅰ・Ⅱの情報資産を所属する学校の外で処理する場合は、教育情報セキュリティ管理者の許可を得た上で、ネットワークに接続されていない端末を用いなければならない。また、その際端末内部に重要性Ⅰ～Ⅲの情報を保存してはならない。
・ 教職員は、所属する学校の外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。
・ 教職員は、所属する学校の外で情報処理作業を行う際、学校管理外の端末による情報処理を行ってはならない。ただし、教育情報セキュリティ管理者の許可を得た場合に限り、所属する学校と同等のセキュリティが確保できる学校管理外の端末で行うことができる。
・ 教職員は、所属する学校の外で情報処理作業を行う場合には、大量または機微な個人情報を取扱ってはならない。また、公共の場においては個人情報を取扱ってはならない。
・ 教職員は覗き見を防止するため、学校の外において教職員等以外の目に触れないように取扱わなければならない。

（6）持ち出しの記録

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

（7）電磁的記録媒体等の管理

・ 教育情報セキュリティ管理者は、情報システムにおいて電磁的記録媒体を使用する場合、学校が管理しているものを学校情報取扱者に使用させなければならない。
・ 教職員は学校指定以外の電磁記録媒体を校内ネットワークに接続したり、業務に利用したりしてはならない。
・ 教育情報セキュリティ管理者は、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。

（8）端末のセキュリティ設定変更の禁止

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

（9）机上の端末等の管理

教職員は、端末や電磁的記録媒体、データが印刷された文書等について、第三者に使用されること、又は管理権限のある者の許可なく情報を閲覧されることがないように、離席時の端末のロックや文書等が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。

（10）異動、退職時等の遵守事項

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

（11）対象教職員等

情報資産を取扱う全ての教職員等（人材派遣職員等も含む）は教育情報セキュリティポリシーに定める事項を遵守しなければならない。

（12）セキュリティポリシー等の閲覧

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

5.2 情報セキュリティインシデント発生時の対応について

（1）情報セキュリティインシデントの報告

・ 学校情報取扱者は、情報セキュリティインシデントを発見した場合、若しくは保護者等外部から報告を受けた場合、速やかに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。

・ 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に報告しなければならない。

・ 教育情報セキュリティ責任者は、報告のあった情報セキュリティインシデントについて、関係機関に必要な連絡を行うとともに、教育情報セキュリティ統括責任者及び平内町総務課長に報告しなければならない。

（2）緊急時対応計画の整備

教育情報セキュリティ統括責任者は、情報資産に対するセキュリティ侵害が発生した場合において、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正に対処しなければならない。

（3）緊急時対応計画の内容

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 緊急時連絡網

② 発生した事象に係る報告事項

③ 発生した事象への対応措置
④ 再発防止措置の策定

（4）情報セキュリティインシデントの報告内容

教育情報セキュリティ管理者等から教育情報セキュリティ責任者への報告は、以下の内容を含むものとする。

① 件名
② 判明した日時
③ 発生した日時
④ 通報者
⑤ 事件事故等の内容
⑥ 漏えいした情報
⑦ 想定される原因
⑧ 事件事故等への対応
⑨ 復旧方針

（5）原因の記録・究明、再発防止等

教育情報セキュリティ統括責任者は、情報資産に対するセキュリティ侵害が発生した場合において、その原因を究明し、記録を保存しなければならない。また、再発防止策を実施するために必要な措置を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管理

（1）ファイルサーバの設定等

教育情報システム管理者が情報を共有するためのファイルサーバを設置する場合には、次の事項を守らなければならない。

① ファイルサーバを学校単位で構成する場合には、特段の理由がない限り、教職員が他の学校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。
② 特定の教職員のみが取扱う権限を持つ情報については、同一の学校であっても、権限のない者が閲覧及び使用できないよう設定しなければならない。

（2）無許可ソフトウェアの導入等の禁止

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

（3）業務以外の目的での Web サイト閲覧の禁止

教職員等は、業務以外の目的で Web サイトを閲覧してはならない。教育情報セキュリティ管理者は、学校情報取扱者の Web 利用について、明らかに業務に関係のない Web サイトを閲覧していることを発見した場合は、学校情報管理者に通知し適正な措置を求めなければならない。

（4）通信回線及び通信回線装置の管理

教育情報システム管理者又は教育情報セキュリティ管理者は、学校の通信回線及び通信回線装置を適切に管理しなければならない。また、ネットワークに使用する回線は十分なセキュリティ対策が実施されたものでなければならない。

（5）外部ネットワークとの接続制限等

教育情報システム管理者は、外部ネットワークとの接続に際して情報セキュリティの確保できるネットワーク構成を採らなければならない。

6.2 不正プログラム等への対策

（1）学校情報取扱者の遵守事項

学校情報取扱者は、次の事項を遵守しなければならない。

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

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

・ コンピュータウイルス等に感染したおそれがある場合は、校務系端末の場合は電源ケーブルの即時取り外し、学習系端末の場合はバッテリーの即時取り外し等、他への感染を防止する措置を講じるとともに、速やかに教育情報セキュリティ管理者に報告する。

・ メールやSMSに添付されているURLを安易にクリックせず、あらかじめ登録しているURLからアクセスするなど、詐欺サイト等へのアクセスに注意する。

（2）攻撃への対処

教育情報システム管理者又は教育情報セキュリティ管理者は、サーバ等に攻撃を受けた場合は、システムの停止を含む必要な措置を講じなければならない。

（3）学校情報取扱者による不正アクセス

教育情報システム管理者は、学校情報取扱者による不正アクセスを発見した場合、当該学校情報取扱者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。

7. 運用面のセキュリティ

（1）情報システムの監視

教育情報システム管理者又は教育情報セキュリティ管理者は、セキュリティに関する事象を検知するため、情報システムの監視を行わなければならない。

（2）教職員等の報告義務

・ 学校情報取扱者は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに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。

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

（2）再発防止の指導等

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

ア 再発防止の指導その他適切な措置

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

イ 使用権の停止・剥奪

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

ウ 報告

違反する行為が生じた場合、違反する行為の内容、指導内容その他措置の状況について教育情報セキュリティ統括責任者に報告する。

8. 業務委託等と外部サービスの利用

8.1 業務委託等

（1）委託事業者等の選定基準

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

（2）契約書の記載事項

重要な情報資産を扱う業務又はネットワーク及び情報システムの開発・保守並びにデータ処理その他情報処理に係る業務委託においては、当該委託先事業者等との間で、下記事項を明記した契約を締結しなければならない。

① データその他業務上知り得た情報の守秘義務
② 第三者への委託等の禁止又は制限
③ データその他業務上知り得た情報の目的外利用及び第三者への提供の禁止
④ データその他業務上知り得た情報の複写及び複製の禁止
⑤ 契約に違反した場合における契約の解除及び損害賠償
⑥ 委託業務等終了時の情報資産の返還、廃棄等
⑦ 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
⑧提供されるサービスレベルの保証

8.2 外部サービスの利用

・ 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及び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については、「教育情報セキュリティポリシーに関するガイドライン（文部科学省）」記載の詳細に従う。

・ クラウドサービスでは、教育情報システム管理者は次の事項に留意しなければならない。
⑴ クラウドサービスを利用するにあたり、取扱う情報資産の分類及び分類に応じた取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断しなければならない。
⑵ クラウドサービスの特性を考慮した上で、セキュリティが適切に確保されていることを確認しなければならない。

9. 学習用端末における情報セキュリティ

児童生徒に支給する学習用端末における情報セキュリティ対策について規定する。また学習用端末の情報セキュリティ対策のうち、設定、運用等に関する権限及び責任は教育情報セキュリティ管理者が有し、所管する学校における情報モラル教育等に関する権限及び責任は学校情報管理者が有する。

9.1 学習用端末の情報セキュリティ対策

（1）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管理者は、児童生徒が学習用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。また学校情報管理者は学習用端末で閲覧可能な不適切なウェブページを知り得た場合には、教育情報セキュリティ管理者に情報提供しなければならない。

（2）不適切な利用の防止

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

9.2 児童生徒用 ID の管理

転入学や卒業、転出時等における ID 及び関連するデータについて、教育情報システム管理者又は教育情報セキュリティ管理者は、適切に処理をしなければならない。

10. 点検・報告・改善

10.1 点検

（1）実施方法

・ 教育情報セキュリティ責任者は、所管するネットワーク及び情報システムの情報セキュリティ対策状況について、定期的及び必要に応じて点検を実施しなければならない。
・ 教育情報セキュリティ管理者は、所管する学校の情報セキュリティポリシーに沿った情報セキュリティ対策状況について、定期的及び必要に応じて点検を実施しなければならない。

（2）報告

教育情報セキュリティ管理者は、点検を行った際は結果と改善策を取りまとめ、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。 なお、学校情報取扱者は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。

（3）改善

教育情報セキュリティ責任者は、業務上発見された問題、保護者等からの指摘による問題、点検において指摘された問題等に対し必要な改善を施さなければならない。なお、ネットワーク等の技術的な問題に対応する場合は、平内町総務課と連携し対応する。

11. 情報セキュリティに関する法令の遵守

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

⑴ 教育公務員特例法（昭和 24 年法律第１号）
⑵ 地方公務員法（昭和 25 年法律第 261 号）
⑶ 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）
⑷ 著作権法（昭和 45 年法律第 48 号）
⑸ 個人情報の保護に関する法律（平成 15 年法律第 57 号）
⑹ 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）
⑺ サイバーセキュリティ基本法（平成 26 年法律第 104 号）
⑻ 平内町個人情報の保護に関する条例（令和５年３月 17 日条例第１号）
⑼ 平内町個人情報の保護に関する規則（令和５年４月 27 日規則第 17 号）
⑽平内町文書取扱規則（昭和 30 年３月 31 日規則第３号）