鵜川小学校
情報セキュリティポリシーに関するガイドライン

令和８年６月

目次　　ページ

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

【教職員等の遵守事項】

(1) 情報セキュリティポリシー等の掲示

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を閲覧できるように掲示しなければならない。

(2) 業務以外の目的での使用の禁止

教職員等は、業務以外の目的で情報資産の外部への持ち出し、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

(3) 配備以外のパソコンやモバイル端末等の業務利用

自宅や学校外等での業務作業においては配備された端末を使用することは原則禁止とする。やむを得ず外部で業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。

(注) 教職員等は、配備以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、無許可で重要情報等を持ち出す行為を禁止する。情報セキュリティ管理者の許可を得た上で、外

部で情報処理作業を行う際には下記①・②を元に安全管理措置を遵守しなければならない。

①配備以外の端末のセキュリティに関する教育を受けた者のみ使用を許可する

②業務利用する必要がなくなった場合は、配備以外のパソコンやモバイル端末等から業務に関係する情報を削除する。

(4) 持ち出し及び持ち込みの記録

学校内のパソコン、モバイル端末及び電磁的記録媒体、情報資産及びソフトウェアの持ち出しや業務利用を許可された支給以外のパソコン、モバイル端末及び電磁的記録媒体の持ち込みについては現状把握や資産管理のため記録簿を作成し、保管しなければならない。

（注１）記録簿には、持ち出しの項目として、所属名、名前、日時、持出物、個数、用途、持出の場所、返却日、管理者の確認印等を設ける。

（注２）持ち込みの項目としては、所属名、名前、日時、持込物、個数、用途、持込の場所、持ち帰り日、管理者の確認印等を設ける。

(5) パソコンやモバイル端末におけるセキュリティ設定変更の禁止

教職員等は、パソコンや、モバイル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情報セキュリティ管理者の許可なく変更してはならない。

(6) 机上の端末等の管理

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。

(7) 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を返却し、コピーや持ち出しを原則禁止とする。その後も、業務上知り得た情報を漏らしてはならない。ただし、情報セキュリティ管理者の許可を得た情報資産のコピーは例外とする。

また、転入において他市等で使用していた情報資産のコピーや持ち込みを原則禁止とする。ただし、情報セキュリティ管理者の許可を得た情報資産のコピーは例外とする。

【情報資産について】

学校で扱う情報資産は，大きく校務系情報、学習系情報、公開系情報に分けられ「重要性分類」によってその守り方が異なるため、各分類毎にシステムを分けて管理を行わなければならない。

３． 実施手順

【教職員等の具体的な実施事項について】

(1) 自己管理事項(アカウント、ID、パスワード、電子メール等)の遵守

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。

教職員等が使用しているアカウント、ID、パスワード、電子メール等は、教育情報セキュリティ管理されているものであることを念頭に置いて使用しなければならない。また、支給されたパソコンにおいては、ネットワーク管理者から支給されたアカウント以外の使用する事を禁止とする。

〔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。

・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。
・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。
・パスワードが流出したおそれがある場合には、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。
・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）
・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。
・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。
・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）
・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。

(2) 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、「BCC」（ブラック・カーボン・コピー）で送信する。
④教職員等は、重要な電子メールを誤送信した場合、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ネットワーク管理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。
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。

(3)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。

(4)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。

(5)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。

(6) 無許可ソフトウェアの導入等の禁止

①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。

②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。

③教職員等は、業務上の必要がある場合は、情報セキュリティ管理者が申請書を提出し、ネットワーク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、情報セキュリティ管理者は、ソフトウェアのライセンスを管理しなければならない。

④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。

⑤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。

(7) 機器構成の変更の制限

①教職員等は、支給された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、情報システム管理者は申請書を提出し、ネットワーク管理者の許可を得なければならない。

(8) 無許可でのネットワーク接続の禁止

教職員等は、ネットワーク管理者及び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。

(9) 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。

(注) 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、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。

・セキュリティに問題が発生した時又は発生する恐れがある場合、ネットワーク管理者は端末のログ履歴等を収集・解析することができる。

(10) 外部からのアクセス等の制限

・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。

・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。

４．学習者への指導

児童は、教職員等でないことから、教育情報セキュリティポリシーを遵守する義務を負うものではないが、情報モラル教育の観点、学校の学習系システムを利用することから、教職員等は、児童に対し、学習者用端末等を活用させるにあたり、以下の事項について指導することが重要である。以下に例を示す。

〔児童への指導事項〕

・学習用端末や学習系クラウドサービスは、学習目的で使用すること。
・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。
・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。
・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。
・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場合は、原則学習系クラウドに保存し、端末のローカル保存は必要最低限とすること。
・無断で外部ソフトウェアをインストールしないこと。
・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。
・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が出るといった症状がでた場合、すぐに担任教員に報告すること。
・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。
・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。
・許可のないゲームソフト等は使用しないこと。