佐々町立学校教育における
情報セキュリティポリシー

佐々町教育委員会

令和２年１１月

目次

1. 対象範囲及び用語説明

【趣旨】

情報セキュリティポリシーを適用する行政機関等の範囲、情報資産の範囲及び用語を明確にする。

（1）行政機関等の範囲

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（小学校、中学校を言う。以下同じ。）とする。

（2）情報資産の範囲

本対策基準が対象とする情報資産は、次のとおりとする。

①教育ネットワーク、教育情報システム、これらに関する設備、電磁的記録媒体

②教育ネットワーク及び教育情報システムで取り扱う情報（これらを印刷した文書を含む。）

③ 教育情報システムの仕様書及びネットワーク図等のシステム関連文書

（3）用語説明

本対策基準における用語は、以下の通りとする。

用　語	定　　義
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
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
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
校務用端末	校務系情報にアクセス可能な端末
校務外部接続用端末	校務外部接続系情報にアクセス可能な端末
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

指導者用端末	学習系情報にアクセス可能な端末で、教員のみが利用可能な端末
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り扱うシステム
校務外部接続系システム	校務外部接続系ネットワーク、メールサーバ、ホームページ運用サーバ（CMS)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り扱うシステム
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り扱うシステム
教育情報システム	校務系システム、校務外部接続系システム及び学習系システムを合わせた総称
校務系サーバ	校務系情報を取り扱うサーバ
校務外部接続系サーバ	校務外部接続系情報を取り扱うサーバ
学習系サーバ	学習系情報を取り扱うサーバ

2. 組織体制

【趣旨】

組織として、情報セキュリティ対策を確実に実施するに当たっては、情報セキュリティ対策に取り組む十分な組織体制を整備し、一元的に情報セキュリティ対策を実施する必要がある。このことから、情報セキュリティ対策のための組織体制、権限及び責任を規定する。

（1）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、本町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、必要に応じて、情報セキュリティ委員会を開催することができる。

（2）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。

（3）教育情報セキュリティ責任者

①教育委員会事務局の教育次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関する意見の集約及び教職員等（教職員、非常勤教職員及び臨時教職員をいう。以下同じ。）に対する教育、訓練、助言及び指示を行う。

（4）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。

（5）教育情報システム管理者

①教育委員会事務局の教育次長を、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。

（6）教育情報システム担当者

①教育委員会の職員を、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。

（7）情報セキュリティ委員会

①「佐々町情報セキュリティ対策基準」に基づき、本町に情報セキュリティ委員会が設置される。

②情報セキュリティ委員会は、本町の情報セキュリティ対策を統一的に行うため、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。

（8）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。

3. 情報資産の分類と管理方法

【趣旨】

情報資産を保護するに当たっては、まず情報資産を分類し、分類に応じた管理体制を定める必要がある。情報資産の管理体制が不十分な場合、情報の漏えい、紛失等の被害が生じるおそれがある。そこで、機密性、完全性及び可用性に基づく情報資産の分類と分類に応じた取扱いを定めた上で、情報資産の管理責任を明確にし、情報資産のライフサイクルに応じて取るべき管理方法を規定する。

4. 物理的セキュリティ

4.1. サーバ等の管理

【趣旨】

本項においては、特にサーバ及び管理区域に関する部分の取扱いについては、主にオンプレミスの場合を想定している。クラウドサービスを利用する場合には、「9 クラウドサービスの利用」を軸に確認・検討すること。

サーバ等のハードウェアは、情報システムの安定的な運用のために適切に管理する必要があり、管理が不十分な場合、情報システム全体に悪影響が及んだり、業務の継続性に支障が生じるおそれがある。このことから、サーバ等の設置や保守・管理、配線や電源等の物理的セキュリティ対策を規定する。

4.2. 管理区域（情報システム室等)の管理

【趣旨】

情報システム室等は、重要な情報資産が大量に保管又は設置されており、特に厳格に管理する必要がある。情報システム室等が適切に管理されていない場合には、盗難損傷等により重大な被害が発生するおそれがあり、このことから、情報システム室等の備えるべき要件や入退室管理、機器等の搬入出に関する対策を規定する。ただし、対策によっては建物の改修を必要とするなど多額の費用を要するものもある。対策の実施に当たっては、費用対効果を考慮して行う必要がある。

4.3. 通信回線及び装置の管理

【趣旨】

ネットワーク利用における通信回線及び通信回線装置が適切に管理されていない場合はネットワークそれ自体のみならず、ネットワークに接続している情報システム等に対しても損傷や不正アクセス等がおよぶおそれがある。このことから、外部ネットワーク接続等の通信回線及び通信回線装置の管理にセキュリティ対策を規定する。

4.4. 教職員等の利用する端末や電磁的記録媒体等の管理

【趣旨】

教職員等が利用するパソコン、モバイル端末及び電磁的記録媒体等が適切に管理されていない場合は、不正利用、紛失、盗難、情報漏えい等の被害を及ぼすおそれがある。この

ことから、これらの被害を防止するために、教職員等の利用するパソコン、モバイル端末及び電磁的記録媒体等の盗難及び情報漏えい防止策、持ち出し・持ち込み等に関する対策を規定する。

5. 人的セキュリティ

5.1. 教職員の遵守事項

【趣旨】

教職員等が情報資産を不正に利用したり、適正な取扱いを怠った場合、コンピュータウイルス等の感染、情報漏えい等の被害が発生し得る。このことから、情報セキュリティポリシーの遵守や情報資産の業務以外の目的での使用の禁止等、教職員等が情報資産を取り扱う際に遵守すべき事項を明確に規定する。教職員だけでなく、非常勤職員及び臨時職員、外部委託事業者についても、遵守事項を定めなければならない。

情報漏えい事案の多くが、教職員等の過失による規定違反から生じており、職場の実態等を踏まえつつ、教職員等の遵守事項を適正に定めるとともに、規程の実効性を高める環境を整備することが重要である。

5.2. 研修・訓練

【趣旨】

情報セキュリティを適切に確保するためには、情報セキュリティ対策の必要性と内容を全ての教職員等が十分に理解していることが必要不可欠である。また、情報セキュリティインシデントの多くは、教職員等の規定違反に起因している場合がある。さらに、情報セキュリティの向上は、利便性の向上とは、必ずしも相容れない場合がある。教職員等が業務を優先することが、情報セキュリティ対策の軽視につながることもある。

また、情報セキュリティに関する脅威や技術の変化は早いことから、教職員等に対しては、常に最新の状況を周知することが重要である。

さらに、実際に情報セキュリティインシデントが発生した場合に的確に対応できるようにするため、緊急時に対応した訓練を実施しておくことが必要である。

これらのことから、教職員等に情報セキュリティに関する研修・訓練を行うことを規定する。

5.3. 情報セキュリティインシデントの報告

【趣旨】

情報セキュリティインシデントやその発生の予防が重要なことは言うまでもないが、実

際に情報セキュリティインシデントを認知した場合に、責任者に報告を速やかに行うことにより、被害の拡大を防ぎ、早期に回復を図れるようにしておくことも必要である。このことから、情報セキュリティインシデントを認知した場合の報告義務について規定する。

なお、報告に対する対応については、「7.3. 侵害時の対応等」による。

5.4. ID 及びパスワード等の管理

【趣旨】

情報システムを利用する際の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）の管理が適切に行われない場合は、情報システム等を不正に利用されるおそれがある。このことから、ID及びパスワード等の管理に関する遵守事項を規定する。

認証情報等は、人的な原因により漏えいしやすい情報である。教育情報システム管理者からの認証情報等の発行から教職員等での管理に至るまで、人的な原因で情報の漏えいするリスクを最小限にとどめる必要がある。

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

【趣旨】

ネットワークや情報システム等の管理が不十分な場合、不正利用による情報システム等へのサイバー攻撃、情報漏えい、損傷、改ざん、重要情報の詐取、内部不正等の被害が生じるおそれがある。このことから、情報システム等の不正利用を防止し、また不正利用に対する証拠の保全をするために、ログの管理やシステム管理記録の作成、バックアップ、無許可ソフトウェアの導入禁止、機器構成の変更禁止等の技術的なセキュリティ対策を規定する。

なお、多くの情報システムにおいては、クラウドサービスを適切に利用することで、オンプレミスよりも効率的に情報セキュリティレベルを向上させることが可能となる。

離する等の措置を講じなければならない。

6.2. アクセス制御

【趣旨】

情報システム等をアクセス権限のない者に利用できる状態にしておくと、情報漏えいや情報資産の不正利用等の被害が発生し得る。そこで、アクセス制御を業務内容、権限ごと

に明確に規定しておく必要がある。また、不用意なアクセス権限付与による不正アクセスを防ぐために、アクセス権限の管理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に集約することが重要である。

このことから、利用者登録や特権管理等を用いた情報システムへのアクセス制御、ログイン手順、接続時間の制限等不正なアクセスを防止する手段について規定する。

6.3. システム開発、導入、保守等

【趣旨】

システム開発、導入、保守等において、技術的なセキュリティ対策が十分に行われない場合は、プログラム上の欠陥（バグ）によるシステム障害等により業務に重大な支障が生じるおそれがある。このことから、システム開発、導入、保守のそれぞれの段階における対策を「9. クラウドサービスの利用」の記載も参照しつつ、規定する。なお、本規定にはシステムの更新又は統合時の十分な検証等も含まれる。

6.4. 不正プログラム対策

【趣旨】

情報システムにコンピュータウイルス等の不正プログラム対策が十分に行われていない場合は、システムの損傷、情報漏えい等の情報セキュリティインシデントが発生するおそれがある。不正プログラム対策としては、不正プログラム対策ソフトウェアを導入するとともに、パターンファイルの更新、ソフトウェアのパッチの適用等を確実に実施することが基本であり、被害の拡大を防止することになる。

これらを踏まえ、不正プログラムの感染、侵入を予防し、さらには感染時の対応として取るべき手段を規定する。

6.5. 不正アクセス対策

【趣旨】

情報システムに不正アクセス対策が十分に行われていない場合は、システムへの攻撃、情報漏えい、損傷、改ざん等の被害を及ぼすおそれがある。このことから、不正アクセスの防止又は被害を最小限にするため、不正アクセス対策として取るべき措置、攻撃を受けた際の対処及び関係機関との連携等について規定する。

6.6. セキュリティ情報の収集

【趣旨】

ソフトウェアにセキュリティホールが存在する場合、システムへの侵入、改ざん、損傷、漏えい等の被害を及ぼすおそれがある。また、情報セキュリティを取り巻く社会環境や技術環境等は刻々と変化しており、新たな脅威により情報セキュリティインシデントを引き起こすおそれがある。これらのことから、セキュリティホールをはじめとするセキュリティ情報の収集、共有及び対策の実施について規定する。

7. 運用

7.1. 情報システムの監視

【趣旨】

情報システムにおいて、不正プログラム又は不正アクセス等による情報システムへの攻撃又は侵入、部内職員の不正な利用、自らのシステムが他の情報システムに対する攻撃に悪用されること等を防ぐためには、ネットワーク監視等により情報システムの稼働状況について常時監視を行うことが必要である。したがって、情報システムの監視に係る対策について規定する。

7.2. 教育情報セキュリティポリシーの遵守状況の確認

【趣旨】

教育情報セキュリティポリシーの遵守を確保するため、教育情報セキュリティポリシーの遵守状況等を確認する体制を整備するとともに、問題があった場合の対応について規定する。

7.3. 侵害時の対応等

【趣旨】

情報セキュリティインシデント、システム上の欠陥及び誤動作並びに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事案が発生した場合に、迅速かつ適切に被害の拡大防止、迅速な復旧等の対応を行うため、緊急時対応計画の策定について規定する。

7.4. 例外措置

【趣旨】

情報セキュリティポリシーの規定をそのまま適用した場合に、学校事務及び教育活動の適正な遂行を著しく妨げるなどの理由により、これに代わる方法によることやポリシーに定められた事項を実施しないことを認めざるを得ない場合がある。このことから、あらかじめ例外措置について規定する。

7.5. 法令等遵守

【趣旨】

教職員等は、全ての法令を遵守することは当然であるが、教職員等が業務を行う際の参考として、情報セキュリティに関する主要な法令を明示し、法令の遵守を確実にする。

7.6. 懲戒処分等

【趣旨】

教育情報セキュリティポリシーの遵守事項に対して、教職員等が違反した場合の事項を定めておくことは、教育情報セキュリティポリシー違反の未然防止に、一定の効果が期待される。このことから、教育情報セキュリティポリシー違反に対する懲戒処分の規定及び懲戒に係る手続きについて規定する。

8.外部委託

【趣旨】

情報システムの外部委託を行う際は、外部委託事業者からの情報漏えい等の事案を防止するために、情報セキュリティを確保できる外部委託事業者を選定し、契約で遵守事項を定めるとともに、定期的に対策の実施状況を確認する必要がある。

このことから、外部委託を行う際に、情報セキュリティ確保上必要な事項について規定する。

なお、個別の地方公共団体が単独で外部委託する場合だけでなく、共同アウトソーシングの形態等により地方公共団体が共同で外部委託する場合にも対策を行う必要があることに留意する。なお、クラウドサービスを利用する場合は、「9. クラウドサービスの利用」を参照すること。

9. クラウドサービスの利用

9.1 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

【趣旨】

校務系システム、学習系システムにおいてクラウドサービスを利用する場合、クラウドの利用者である教育委員会等（以下、クラウド利用者と言う）は、クラウド事業者（以下、クラウド事業者と言う）が、自らの情報資産を預けるに値する安心安全で信頼できるパートナーであることを慎重に確認しなければならない。

※本項における「クラウド利用者」とは、クラウドサービスの選定・契約の主体となり得る者（主に教育委員会）を想定している。教職員や児童生徒は、別途、「エンドユーザ」として整理する。

クラウドサービスにおいて情報セキュリティを確保するためには、クラウド事業者が協働して情報セキュリティ対策を構築することが必要となる。

そこで、クラウド利用者は、クラウドサービスを提供する全てのクラウド事業者が役割分担して総合的な情報セキュリティ対策を講じているかを確認する必要がある。

9.2．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

【趣旨】

クラウド利用者は、教育情報システムにパブリッククラウドサービスを利用する場合においては、クラウド事業者及び提供サービスに対する信頼性や内在するリスクを評価し、総合的に情報セキュリティを確保ができるクラウド事業者が提供するサービスを選定する必要がある。この観点からクラウド事業者のサービス提供ポリシーや体制等について確認・検証すべき事項について規定する。

クラウド利用者は、クラウドサービス及びクラウド事業者が保有するセキュリティリスクを踏まえ、自ら実施するセキュリティ対策と総合して関係法令、教育情報セキュリティポリシーが遵守できるかを評価する必要がある。

9.3．約款による外部サービスの利用

【趣旨】

本項でいう約款による外部サービスとは、インターネット上に約款を掲示し、同意した利用者に対して情報処理機能を提供するサービスであり、SaaS型パブリッククラウドサービスの一種であるが、9.2及び9.3で想定する個別契約締結型サービスとは別種であり、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除くものである。

原則、約款に提示された提供条件だけで利用を判断することになるため、リスクを十分踏まえて、利用に際して適切なセキュリティ対策を講じる必要がある。

9.4．ソーシャルメディアサービスの利用

【趣旨】

住民への情報提供など、ソーシャルメディアサービスを利用する場合は、約款による外部サービスを利用することが多くなるが、なりすましやサービス停止のおそれがあるため、ソーシャルメディアサービスによる情報発信時の対策を講じる必要がある。

10. 事業者に対して確認すべきプライバシー保護に関する事項

【趣旨】

外部委託やクラウドサービスの利用に当たっては、事業者における個人情報の適切な管理が行われていることが必須であることから、個人情報の収集・利用範囲や管理期間、データの統制と所有の在り方等について、事業者に確認を行う必要がある。

これらの項目については、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ることも有効である。

11. 評価・見直し

11.1. 監査

【趣旨】

情報セキュリティポリシーの実施状況について、客観的に専門的見地から評価を行う監査が実施されない場合は、情報セキュリティ対策が徹底されない状態や情報セキュリティポリシーが業務に沿わない状態が続くおそれがある。このことから、監査の実施及びその方法について規定する。

監査を行う者は、十分な専門的知識を有するものでなければならない。また、適正な監査の実施の観点から、監査の対象となる情報資産に直接関係しない者であることが望ましい。また、地方公共団体内の情報セキュリティ対策の監査・報告について中立性を保証され、監査に必要な情報へのアクセス等の権限が明確に与えられる必要がある。監査作業に伴う情報の漏えいのリスクを最小限とするため、監査人等が取り扱う監査に係る情報について、漏えい、紛失等が発生しないように保管する必要がある。

11.2. 自己点検

【趣旨】

情報セキュリティポリシーの履行状況等を自ら点検、評価することは、情報セキュリティポリシーの遵守事項を改めて認識できる有効な手段である。自己点検は、情報システム等を運用する者又は利用する者自らが実施するので、監査のような客観性は担保されないが、監査と同様に、点検結果を踏まえ各部門で改善を図ったり、組織全体のセキュリティ対策の改善を図る上での重要な情報になる情報セキュリティ対策の評価を行い、対策の見直しに資するものである。また、教職員等の情報セキュリティに関する意識の向上や知識の習得にも有効である。

このことから、自己点検を定期的に実施する規定を設け、その活用方法とあわせて規定する。

11.3. 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

【趣旨】

情報セキュリティ対策は、情報セキュリティに関する脅威や技術等の変化に応じて、必要な対策が変化するものであり、教育情報セキュリティポリシー及び関係規程等は、定期的に見直すことが求められる。また監査や自己点検の結果等から、同ポリシー及び関係規程等の見直しの必要性が確認される場合もある。

このことから、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について規定する。