坂戸市教育情報セキュリティポリシー

令和８年４月

坂戸市教育委員会

目　次

【公開文書】

教育情報セキュリティ基本方針（宣言書）

坂戸市教育委員会の教育情報システムが取り扱う情報には、児童生徒の個人情報のみならず、学校運営上重要な情報が多数含まれています。これらの情報に改ざん、破壊、漏えいなどの事故が生じた場合、児童生徒や学校運営に対して深刻な問題を引き起こすこととなります。

教育情報システムや教育ネットワークで取り扱う情報資産をさまざまな脅威から保護し、機密性、完全性及び可用性を維持する、いわゆる情報セキュリティ対策の推進は、市民の財産やプライバシーを守ることはもとより、坂戸市教育委員会に対する市民からの信頼の維持や向上に寄与するなど、教育行政を安定的に運営していくために極めて重要な取組です。

そのため、坂戸市教育委員会では、情報資産を故意や偶然という区別に関係なく、改ざん、破壊、漏えいなどの事故から保護することを目的に「教育情報セキュリティポリシー」を策定し、安全対策に努めています。坂戸市教育委員会が保有する情報資産を利用する者には、「教育情報セキュリティポリシー」に基づく行動の遵守を徹底し、強固な情報セキュリティ体制の維持・向上を図ってまいります。

令和８年４月１日

坂戸市教育委員会

教育長　太 田　正 久

序　坂戸市教育情報セキュリティポリシーの構成

坂戸市教育情報セキュリティポリシー（以下、「本ポリシー」という。）とは、坂戸市教育委員会（以下、「教育委員会」という。）及び坂戸市立小・中学校（以下、「学校」という。）が保有する教育の情報資産に関する情報セキュリティ対策について取りまとめたものである。

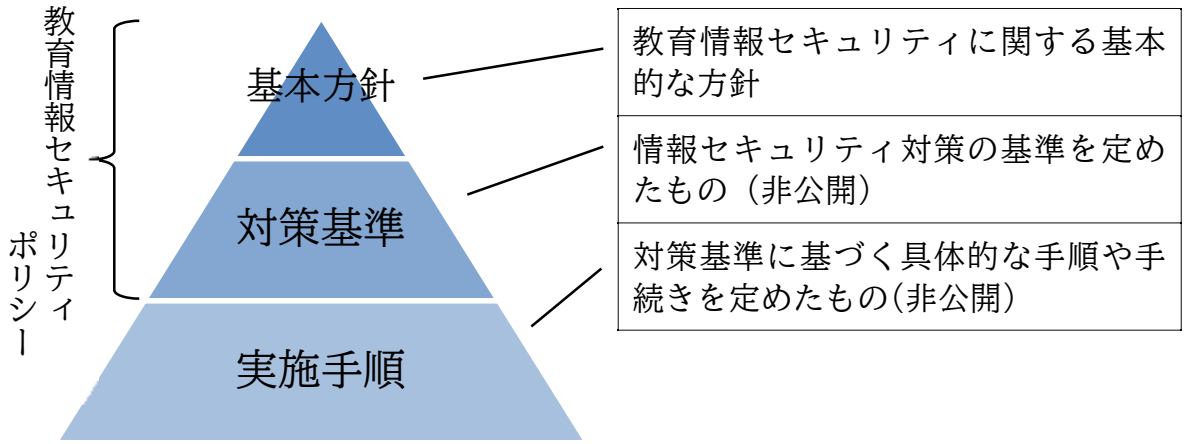
本ポリシーは、教育委員会及び学校が保有する情報資産を取り扱うすべての教職員に浸透、普及、定着させるものであり、安定的な規範であることが求められる。一方で、教育情報セキュリティを取り巻く急速な状況の変化に対し柔軟に対応することも必要である。

このようなことから、本ポリシーは、一定の普遍性を備えた部分としての「教育情報セキュリティ基本方針（以下、「基本方針」という。）」と、情報資産を取り巻く状況の変化に対応する部分として「教育情報セキュリティ対策基準（以下、「対策基準」という。）」の２階層から成るものとして策定する。また、本ポリシーに基づき、具体的な情報セキュリティ対策の実施手順として「坂戸市教育情報セキュリティポリシー実施手順（以下、「実施手順」という。）」を策定する。

なお、本来は、坂戸市（以下、「市」という。）が作成する情報セキュリティポリシーが市全体を包括するポリシーでなければならないが、学校においては、児童生徒が学習活動において日常的に教育情報システムにアクセスするなど、市とは異なる特徴を有していることから、それらを前提とした情報セキュリティ対策が求められるところである。

これらを踏まえ、本ポリシーにおける基本方針は、市の基本方針の内容を踏襲することとし、対策基準及び実施手順については、教育委員会及び学校の実態を踏まえた内容としている。

【図】坂戸市教育情報セキュリティポリシーの構成



第１章　教育情報セキュリティ基本方針

１　目的

学校教育で取り扱う情報には、児童生徒の個人情報のみならず、保護者、教職員、その他地域住民に関する情報等の重要な情報が多く含まれ、漏えいした場合に極めて深刻な問題を引き起こすおそれがある。

したがって、本市の教育ネットワーク及び教育情報システムにおいて、個人情報を始めとする各種情報資産をさまざまな脅威から守り、安全性を確保することは、学校教育の安定的かつ継続的な実施を実現するために教育委員会に課せられた責務である。

そのため、本基本方針は、教育委員会及び学校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に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。

また、すべての教職員は、保有する情報資産に対する脅威への対応が重大かつ喫緊の課題であることを認識し、情報セキュリティ対策の積極的な推進に取り組むこととする。

２　定義

（１）教育ネットワーク

本市の学校教育において情報資産を扱う通信回線やルータ等の通信機器で接続し、情報を伝達するための仕組みのことをいう。

（２）教育情報システム

本市の学校教育において使用されるパソコン、ソフトウェア及び電磁的記録媒体等で構成され情報処理を行う仕組みのことをいう。

（３）情報セキュリティ

情報資産を脅威（自然災害、機器障害、悪意のある行為等の損失を発生させる直接の要因をいう。）から保護し、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。

（４）機密性

情報に接続することを認められた者だけが、情報に接続できる状態を確保することをいう。

（５）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。

（６）可用性

情報に接続することが認められた者が、必要なときに中断されることなく、情報に接続できる状態を確保することをいう。

3　対象とする脅威

（1）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

（2）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、外部委託管理の不備、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

（3）地震、水害、落雷、火災等の災害によるサービス及び業務の停止等

（4）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

（5）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　適用範囲

（1）行政機関等の範囲

本基本方針が適用される機関は、教育委員会及び学校とする。

（2）情報資産の範囲

①　教育ネットワーク、教育情報システム及び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（印刷した文書を含む）
③　教育情報システムの仕様書及び教育ネットワーク図等のシステム関連文書

5　教職員の遵守義務

教職員は、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を遵守しなければならない。

6　情報セキュリティ対策

（1）組織体制

教育委員会及び学校の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

（2）情報資産の分類と管理

教育委員会及び学校が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。

（３）物理的セキュリティ

教育情報システムを設置する施設への不正な立入り、情報資産の損傷・妨害等から保護するために物理的な対策を講じる。

（４）人的セキュリティ

情報セキュリティに関し、教職員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。

（５）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。

（６）運用

教育ネットワークの監視、本ポリシーの遵守状況の確認等、教育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の対策を講じる。

（７）安定性の確保

教育ネットワークや教育情報システムは、可能な限り冗長化を図るなどにより安定した運用となる環境を構築するとともに、障害発生時にも短時間で復旧可能な対策を講じる。

（８）業務委託とクラウドサービスの利用

市の業務を受託する事業者（当該事業者から派遣されている者を含む。）に当該業務を行わせる場合には、教育委員会が定める情報セキュリティ要件等の遵守させるべき事項を、委託事業者の選定要件として提示する。さらに、教育委員会が定める情報セキュリティ要件を契約に明記し、事業者において要件を満たすセキュリティ対策が確保されていることを確認、又は、別途、書面による提出を求める等の措置を講じる。

なお、クラウドサービスの利用にあたっては、利用に関する手順や利用できる情報の範囲を定める等の対策を講じる。

７　監査及び自己点検の実施

本ポリシーの遵守状況を検証するため、必要に応じて監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。

８　教育情報セキュリティポリシーの見直し

教育情報セキュリティ監査及び自己点検の結果、本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に新たに対策が必要となった場合には、適宜本ポリシーを見直す。

9　教育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対策基準を策定する。

なお、対策基準は、公にすることにより本市教育行政に重大な支障を及ぼすおそれがあることから、教育委員会及び学校以外に対しては非公開とする。

10　教育情報セキュリティ実施手順の策定

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実施手順を策定するものとする。

なお、実施手順は、公にすることにより本市教育行政に重大な支障を及ぼすおそれがあることから、教育委員会及び学校以外に対しては非公開とする。

【参考】資料編

1　策定・改訂記録

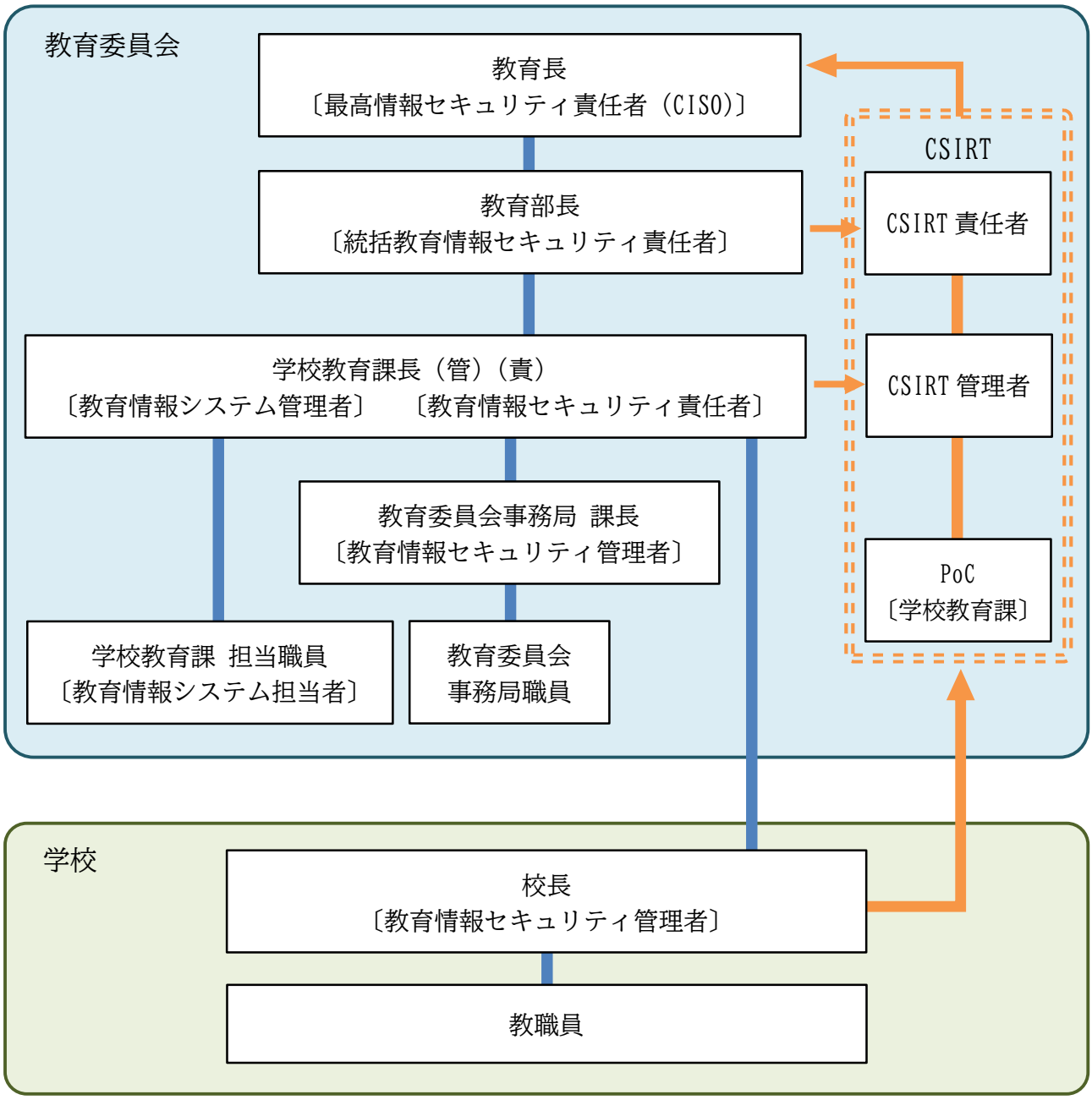
（１）教育情報セキュリティ基本方針

決裁日	施行日	備考
令和４年１１月　１日	令和４年１１月　１日	策定
令和８年　３月１７日	令和８年　４月　１日	改訂（教育長決裁）

（２）教育情報セキュリティ対策基準

決裁日	施行日	備考
令和４年１１月　１日	令和４年１１月　１日	策定
令和８年　３月１７日	令和８年　４月　１日	改訂（教育長決裁）

2　組織体制図


教育委員会
教育長
〔最高情報セキュリティ責任者（CISO)〕
教育部長
〔統括教育情報セキュリティ責任者〕
学校教育課長（管）（責）
〔教育情報システム管理者〕　〔教育情報セキュリティ責任者〕
教育委員会事務局 課長
〔教育情報セキュリティ管理者〕
学校教育課 担当職員
〔教育情報システム担当者〕
教育委員会
事務局職員
CSIRT
CSIRT 責任者
CSIRT 管理者
PoC
〔学校教育課〕
学校
校長
〔教育情報セキュリティ管理者〕
教職員

3　重要性分類に基づく情報資産の例示

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・教育委員会	教職員・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・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 ・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	**業務に係る特定の教職員・教育委員会に加えて、児童生徒又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	
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・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	**業務に係る教職員・教育委員会に加えて、児童生徒又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）	

		・転退学・転入学・就学等に関する情報 ・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		
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	**教職員全員・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	
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）

4　一般用語の解説

用語	定義・解説
CSIRT（シーサート）	機関等において発生した情報セキュリティインシデントに対処するため、当該機関等に設置された体制をいう。Computer Security Incident Response Team の略。
クラウドサービス	事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、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いう。 クラウドサービスの例としては、SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）等がある。なお、統一基準におけるクラウドサービスは、機関等外の一般の者が一般向けに情報システムの一部又は全部の機能を提供するクラウドサービスであって、当該サービスにおいて機関等の情報が取り扱われる場合に限るものとする。
SaaS（サース/サーズ）	利用者に、特定の業務系のアプリケーション、コミュニケーション等の機能、運用管理系の機能、開発系の機能、セキュリティ系の機能等がサービスとして提供されるもの。Software as a Service の略。
アクセス制御	情報又は情報システムへのアクセスを許可する主体を制限することをいう。
アプリケーション	OS 上で動作し、サービスの提供、文書作成又は電子メールの送受信等の特定の目的のために動作するソフトウェアをいう。
サービス不能攻撃	悪意ある第三者等が、ソフトウェアの脆弱性を悪用しサーバ装置又は通信回線装置のソフトウェアを動作不能にさせることや、サーバ装置、通信回線装置又は通信回線の容量を上回る大量のアクセスを行い通常の利用者のサービス利用を妨害する攻撃をいう。
ソーシャルメディア	インターネット上において、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等の、利用者が情報を発信し、形成していくものをいう。
ソフトウェア	サーバ装置、端末、通信回線装置等を動作させる手順及び命令を、当該サーバ装置等が理解できる形式で記述したものをいう。OS や OS 上で動作するアプリケーションを含む広義の意味である。
パブリッククラウド	クラウドサービスの提供方式のひとつ。CPU、ストレージ、メモリ等のコンピュータリソースの利用率を最適化するために、一般ユーザーや複数の利用者でリソースを共用して実装されるクラウドコンピューティング方式。
モバイル端末	端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

暗号化	第三者が復元することができないよう、定められた演算を施しデータを変換することをいう。
記憶媒体	情報が記録され、又は記載される有体物をいう。 記録媒体において、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物を「書面」といい、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるものを「電磁的記録」といい、電磁的記録に係る記録媒体を「電磁的記録媒体」という。 また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USB メモリ、外付けハードディスクドライブ、DVD-R 等の外部電磁的記録媒体がある。
情報セキュリティインシデント	望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営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。
通信回線	複数の情報システム又は機器等（機関等が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、機関等の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、機関等が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。
通信回線装置	通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。また、物理的なハードウェアを有する通信回線装置を「物理的な通信回線装置」という。
不正プログラム	コンピュータウイルス、ワーム（他のプログラムに寄生せず単体で自己増殖するプログラム）、スパイウェア（プログラムの使用者の意図に反して様々な情報を収集するプログラム）等の、情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称をいう。
複合機	プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器をいう。
無線 LAN	IEEE80211a、80211b、80211g、80211n、80211ac、80211ad 等の規格により、無線通信で情報を送受信する通信回線をいう。