大阪市教育委員会情報セキュリティ対策基準

1　目的

この大阪市教育委員会情報セキュリティ対策基準（以下「対策基準」という。）は、大阪市教育委員会情報セキュリティ管理規程（平成25年達３号。以下「規程」という。）第９条に基づき、教育委員会（以下「委員会」という。）における情報資産の取扱いについて遵守すべき事項及び情報セキュリティ対策の実施に関する統一的な基準を定めることにより、委員会が保有する情報資産をさまざまな脅威から守り、機密性、完全性、可用性（注）を維持することによって、本市の教育行政サービスを安全に提供し、もって教育市政の円滑な運営及び教育市政に対する信頼を確保することを目的とする。

（注）：国際標準化機構(ISO)が定めるもの(ISO7498-2：1989)

- 機密性(confidentiality)：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。
- 完全性(integrity)：情報及び処理の方法の正確さ及び完全である状態を安全防護すること。
- 可用性(availability)：許可された利用者が必要なときに情報アクセスできることを確実にすること。

2　用語

この対策基準において使用する用語は、規程において使用する用語の例によるほか、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

（１）　職員　教育委員会事務局及び委員会が所管する学校その他の教育機関に所属する職員をいう。

（２）　端末機　職員又は学習者が活用するパソコンやモバイル端末機等の機器をいう。

（３）　セキュリティインシデント　情報セキュリティに関する問題として捉えられる事象（障害、事件、事故、欠陥、攻撃、侵害等）をいう。

（４）　学校園情報通信ネットワーク　大阪市教育委員会学校園情報通信ネットワーク管理要綱（以下「ネットワーク管理要綱」という。）の規定に基づく、学校園において共通の基盤となる情報通信ネットワークをいう。

（５）　標的型攻撃　明確な意思と目的を持った人間が特定のターゲットや情報に対して特定の目的のために行うサイバー攻撃の一種をいう。

（６）　ＩＤＣ サーバ機器等を安全に設置するため、高度な電源・空調設備を備え、セキュリティ・災害耐性が整備された施設をいう。(Internet Data Center)

３　適用範囲

この対策基準の適用範囲は、規程第１条に規定する情報資産とする。

４　対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（１）　不正アクセス、ウイルス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、落雷、火災等の災害等

（４）　電力供給の途絶、通信の途絶等のインフラの障害からの波及等

５　情報セキュリティ対策

脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（１）　情報資産の分類と管理

本市の保有する情報資産を機密性、完全性及び可用性を踏まえ重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

（２）　物理的セキュリティ

サーバ等、情報システム室等、通信回線等及び職員の端末機等の管理について、物理的な対策を講じる。

（３）　人的セキュリティ

情報セキュリティに関し、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。

（４）　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。

（５）　運用

情報システムの監視、情報セキュリティポリシー（以下「ポリシー」という。）の遵守状況の確認、外部委託を行う際のセキュリティ確保等、ポリシーの運用面の対策を講じるものとする。

６　組織・体制及び役割・責任

（１）　情報セキュリティに係る管理体制・役割

規程第４条から第６条に基づき、情報セキュリティ対策が円滑に推進されるた

めの体制・役割を定める。

① 教育最高情報セキュリティ責任者等

ア 教育最高情報セキュリティ責任者は、委員会における情報セキュリティを総括し、教育情報セキュリティ管理者に対し、情報セキュリティ対策の統一的な実施に必要な指導、助言又は調整を行う。

イ 教育最高情報セキュリティ責任者は、委員会における情報セキュリティ対策の連絡体制の構築並びにポリシーの遵守に関する意見の集約及び職員に対する教育、指導及び指示を行う。

ウ 教育統括情報セキュリティ責任者及び教育情報セキュリティ責任者は、前項に規定する教育最高情報セキュリティ責任者の業務を補佐する。

② 教育ＩＣＴ管理者

教育ＩＣＴ管理者は、委員会における各情報システムの開発及び運用状況、データの管理状況、学校園情報通信ネットワークの利用状況等を把握し、委員会において情報セキュリティ対策が適切かつ確実に実施されるよう必要な指導、助言又は調整を行う。

③ 教育情報セキュリティ管理者

ア 教育情報セキュリティ管理者は、自らが管理する情報システムの開発及び運用状況、データの管理状況、学校園情報通信ネットワークの利用状況等を把握するとともに、当該システムへのアクセスが可能な利用者並びにそのデータ及びプログラムを利用できる範囲等（以下「アクセス権限」という。）を設定し、適切に管理を行い、学校園及び課等（以下、「学校等」という。）における情報セキュリティ対策が実施されるよう指導を行う。

イ 教育情報セキュリティ管理者は、自らが管理する情報資産の情報セキュリティ対策が適切かつ確実に実施されるよう必要な措置を行う。

ウ 教育情報セキュリティ管理者は、職員に対するポリシーの遵守に関する指導、助言又は研修その他情報セキュリティの確保のために必要な措置を行う。

④ 学校等情報セキュリティ責任者等

ア 学校等情報セキュリティ責任者は、学校等においてアクセス権限を管理し利用者が規程第 10 条に規定する実施手順に基づき安全性に十分考慮し適切な利用を行うよう、システムの利用管理及び端末機等の運用管理を担う。

イ 情報セキュリティ担当者は前項に規定する、学校等情報セキュリティ責任者の業務を補佐する。

（２） システムに係る管理体制・役割

① 教育情報セキュリティ管理者

ア 教育情報セキュリティ管理者は、システムの開発、運用、保守の実施並びに管理を担う。

イ　教育情報セキュリティ管理者は、システムの運用を開始しようとするときは、運用管理の体制並びに業務の運用形態・計画及び当該システムに係るハードウェア・ソフトウェアの運用管理の方法等を定めなければならない。

ウ　教育情報セキュリティ管理者は、システムの運用において、入力資料の作成、電子計算機処理、帳票の出力等に至る業務全体の実施状況を把握・管理するとともに、システムの保守を適切に実施しなければならない。

エ　教育情報セキュリティ管理者及び教育情報通信ネットワーク管理責任者は、当該システムのハードウェア及びソフトウェアの運用管理を担う。

オ　教育情報セキュリティ管理者は、システムの運用計画並びに情報セキュリティ実施手順（以下「実施手順」という。）等に基づき、システムが正常に稼働するよう、安全性に十分配慮し適切な運用管理を行わなければならない。

②　学校等情報セキュリティ責任者

ア　学校等情報セキュリティ責任者は円滑に業務処理が実施されるよう、システムの利用管理を担う。

イ　学校等情報セキュリティ責任者は、アクセス権限並びに実施手順等に基づき、安全性に十分配慮し適切な利用が行われるよう、端末機の運用管理を行わなければならない。

（３）　ネットワークに係る管理体制・役割

委員会の各システムの基盤となる学校園情報通信ネットワークの整備及び運用について、安全性及び信頼性を確保するための体制を定める。

①　教育ＩＣＴ管理者

教育ＩＣＴ管理者は、教育情報セキュリティ管理者と連携を図り、委員会における障害に関する連絡調整など、委員会におけるネットワークの適切な運用管理を行う。

②　教育情報通信ネットワーク管理責任者

ア　教育情報通信ネットワーク管理責任者は、学校園情報通信ネットワークの稼働状況及び障害管理、ネットワーク上へのアクセス権限の設定など、ネットワークの運用管理を担い、教育ＩＣＴ基盤担当課長をもって充てる。

イ　教育情報通信ネットワーク管理責任者は、ネットワークについて、規程に基づき、情報セキュリティ実施手順を作成しなければならない。

③　学校等情報通信ネットワーク運用責任者

ア　学校等情報通信ネットワーク運用責任者は学校等のネットワークについて配線及び機器の維持管理、稼働状況及び障害の管理など、学校等のネットワークの管理を担い、規程第６条に規定する学校等情報セキュリティ責任者をもって充てる。

（４）　兼務の禁止

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諾者又は許可者は、同じ者が兼務してはならない。

7　情報セキュリティに係る連絡調整体制

（1）　連絡体制

情報セキュリティの適切な管理及びデータの適正な管理を推進し、システム、データ、ネットワーク等情報資産の情報セキュリティ対策に万全を期すため、教育最高情報セキュリティ責任者は、委員会における情報セキュリティ対策の連絡体制を設置し、以下の関係者その他必要と認める者を随時招集し、ポリシーの遵守に関する事務及びデータ保護に関する事務の連絡調整を行うとともに情報セキュリティ対策の周知徹底を図る。

①　教育統括情報セキュリティ責任者
②　教育情報セキュリティ責任者
③　教育ＩＣＴ管理者
④　教育情報セキュリティ管理者
⑤　学校等情報セキュリティ責任者

（2）　サイバー攻撃等侵害時における緊急連絡体制

教育最高情報セキュリティ責任者は、サイバー攻撃等による緊急の事態により情報資産に重大な被害が生じた場合又は生じるおそれがある場合、緊急連絡体制を設置し、以下の関係者その他必要と認める者と連携を図り、情報セキュリティ対策が適切に実施されるよう監督、指導を行わなければならない。

①　教育統括情報セキュリティ責任者
②　教育情報セキュリティ責任者
③　教育ＩＣＴ管理者
④　教育情報セキュリティ管理者
⑤　学校等情報セキュリティ責任者

8　情報資産等の管理

教育最高情報セキュリティ責任者は、以下の情報セキュリティ対策を行わなければならない。

（1）　情報資産の管理責任

①　管理責任

情報資産は、当該情報資産を所管する学校等が適切に管理する責任を有する。

②　利用者の責任

情報資産を業務上利用する職員は、適切に利用する責任を有する。

③　重要性の効力

データが複製又は伝送された場合には、当該複製等も分類に基づき管理しなければならない。

（２）　データの管理と情報資産の管理

①　データの管理

ア　データの分類

対象となるシステムのデータは、各々のデータの機密性、完全性、可用性を踏まえ、以下の重要性分類に従って分類し、重要性分類に従ったアクセス権限を適切に設定しなければならない。

Ⅰ　セキュリティ侵害が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データ

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データ

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データ

Ⅳ　影響をほとんど及ぼさないデータ

イ　データの作成

（ア）　業務上必要のないデータを作成してはならない。

（イ）　作成したデータは、重要性分類を定めなければならない。

（ウ）　作成途上のデータであっても漏えい、滅失、き損、改ざん等を防止しなければならない。また、作成途上で不要になった場合は、当該データを消去しなければならない。

ウ　データの入手

（ア）　他の学校等が作成したデータを入手した場合、入手元の重要性分類に基づいた取扱いをしなければならない。

（イ）　外部のものが作成したデータを入手した場合、８（２）①「ア　データの分類」に基づいて当該データの重要性分類を定めなければならない。

（ウ）　データを入手した者は、その重要性分類が不明な場合、学校等情報セキュリティ責任者に判断を仰がなければならない。

エ　他の業務に係るデータの利用

他の業務の目的で収集されたデータを利用しようとする学校等の長は、第３号様式によるデータ利用依頼書により当該データを所管する教育情報セキュリティ管理者に申し出なければならない。

オ　外部へのデータの提供

本市以外のものにデータを提供するときは、必要に応じデータの提供を受けるものと協定又は契約を締結し、次に掲げる事項を定めなければならない。

・ データ名及び提供するデータ項目

・ 利用目的
・ 利用条件
・ データの管理に関する事項
・ データの秘密保持に関する事項
・ データの無断使用及び第三者への提供の禁止に関する事項
・ データの複写及び複製の禁止に関する事項
・ 電子計算機処理終了後の措置に関する事項
・ 事故発生時の報告に関する事項
・ その他教育最高情報セキュリティ責任者が必要と認める事項

② 情報資産の管理

ア 情報資産の管理及び取扱い

（ア） 情報資産の管理については、大阪市個人情報保護条例（平成７年大阪市条例第 11 号。以下「個人情報保護条例」という。）、その他の関連する法令及び規程に基づき、データの漏えい、滅失、き損、改ざん、消去、盗難等の防止を図るため必要な措置を講じなければならない。

（イ） 所管する情報資産を他の所属に利用させようとするときは、セキュリティ対策上支障がないか確認しなければならない。また、情報資産を利用させようとする他の所属と情報セキュリティに係る連絡調整体制を構築し、ポリシー及び実施手順に準じた情報資産の取扱いを指導及び遵守させなければならない。

（ウ） ファイル、データを格納する記録媒体、ドキュメント等の情報資産は、当該情報資産に記録されたデータの重要性分類に従い、適切に取り扱わなければならない。

（エ）市民等に公開するデータについて、完全性を確保しなければならない。

イ 情報資産の利用

（ア） 業務以外の目的に情報資産を利用してはならない。

（イ） 情報資産について、定められた場所以外で利用してはならない。ただし、業務遂行上、外部への持ち出しが不可欠である場合については、学校等情報セキュリティ責任者の許可を得て持ち出すことができる。

（ウ） 重要性分類Ⅲ以上のデータを外部へ持ち出すときは、必要に応じて暗号化又はパスワード設定を行わなければならない。

（エ） 外部ネットワークを利用し、本市以外のものと電子メール等により送受信を行うときは、「電気通信回線を利用した公文書の取扱いに関する要領」（平成 16 年 5 月 28 日施行）に基づき適切に取り扱わなければならない。また、重要性分類Ⅲ以上のデータを学校外（庁外及び学校園外をいう。以下同じ。）へ電子メール等により送信するときは、必要に応じて暗号化又はパスワード

設定を行わなければならない。

（オ） 重要性分類Ⅲ以上のデータをメールにより取り扱う必要がある場合については、学校等情報セキュリティ責任者の承認を得るとともに、連絡相手のメールアドレス及びメール受取の確認を行う等、厳格に取り扱わなければならない。なお、学校内（庁内及び学校園内をいう。以下同じ。）においてメールを利用する場合においても、上記の取扱いに準じ、適切に運用を行わなければならない。

（カ） データを学校外で処理する場合は実施手順において情報資産の安全管理措置を定めなければならない。

ウ 記録媒体等の管理

（ア） 学校等情報セキュリティ責任者は、ファイルが格納された記録媒体等の授受について台帳整備し、次の事項を記録しなければならない。また、ファイルを搬送するときは、データの漏えい、滅失、き損、改ざん等を防止するため、専用トランクを使用する等適切な措置を講じなければならない。

- ファイルの名称
- 搬入者及び受領者の氏名並びにその所属等の名称
- 媒体の種別
- 媒体の識別番号
- 授受年月日
- その他教育情報セキュリティ管理者が必要と認める事項

（イ） 学校等情報セキュリティ責任者は、ファイルが格納された記録媒体等の保管について台帳整備し、データの重要性が容易に識別できるよう次の事項を記録するとともに、これらを所定の場所において適切に管理しなければならない。また、ファイルのバックアップを定期的に取得し、所定の場所において適切に管理しなければならない。

- ファイルの名称
- 学校園又は業務主管課等の名称
- 媒体の種別
- 媒体の識別番号
- 作成年月日
- 保管期限
- 消去年月日
- 格納場所
- その他教育情報セキュリティ管理者が必要と認める事項

（ウ） 学校等情報セキュリティ責任者は、ファイルが格納された記録媒体を長期保管する場合は、必要に応じて書込禁止の措置を講じなければならない。

（エ） 学校等情報セキュリティ責任者は、保護データ（重要性分類Ⅰから Ⅲに該当するデータをいう）を保管する場合は、データを記録しているファイルが格納された記録媒体等について、耐火保管庫に保管し、又は予備を作成して別の施設に保管しなければならない。

（オ） 学校等情報セキュリティ責任者は、磁気ディスクその他記録媒体に不要なデータが放置されないよう、不要となったデータを速やかに消去するなど、適正に運用しなければならない。

（カ）車両等により重要性分類Ⅲ以上の情報資産を運搬する者は、学校等情報セキュリティ責任者に許可を得たうえで、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等の設定を行う等、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。

（キ） 学校等情報セキュリティ責任者は、情報資産を廃棄するときは、データ消去その他の適切な措置を講じなければならない。特に、保護データについては、初期化等、情報を復元できないよう確実に消去を行うとともに、行った処理について、日時、担当者、処理内容等その他必要な事項を記録しなければならない。

（ク） ファイルが格納された記録媒体等の廃棄を行う者は、情報セキュリティ責任者（学校等情報セキュリティ責任者）の許可を得なればならない。ただし、システムに関するものである場合は、システム管理者（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。

エ 特定個人情報の取扱い

特定個人情報を取り扱う場合は、インターネットから切り離された環境で取り扱わなければならない。ただし、特に必要な場合は、学校園情報通信ネットワーク上に構築された業務システム内で取り扱うものとし、利用者認証によるアクセス制限や特定個人情報を格納するサーバ等のセグメント分割、ファイルやデータの暗号化など漏えい防止のための措置を講じなければならない。

9 物理的セキュリティ

（1） システムにおける措置

① サーバ等（IDC に設置する場合を含む）

ア 装置の取付け等

（ア） サーバ等を取付ける場合は、地震、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置するとともに、当該場所については、職員が不在時の盗難防止のため、施錠等による措置を講じなければならない。

（イ） 保護データを取り扱い、かつ、システムの停止によって、委員会の業務運

営はもとより教育行政サービスに大きな影響を及ぼす可能性があるシステム（以下「重要システム」という。）のサーバ等については、原則として当該機器等の管理及び運用を行うための部屋（以下「情報システム室」という。）に設置しなければならない。

（ウ）　サーバ等の取付けに当たっては、震災時の転倒又は盗難の防止のため、適切に固定する等必要な措置を講じなければならない。

イ　サーバ等の冗長化

重要システムのサーバ等の機器については、原則として冗長化を図り、メインサーバに障害が発生した場合には速やかにセカンダリサーバで対応を行えるようにするなど、システム運用が停止しない措置を講じなければならない。

ウ　電源設備

業務要件やシステムの特性に応じて、サーバ等の機器の電源については、停電時に当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付け、また、落雷等による異常電流から保護するための措置を講じなければならない。

エ　通信ケーブル等の配線

（ア）　配線通信ケーブルについては、傍受、通信ケーブル及び電源ケーブルについては損傷を受けることがないように可能な限り必要な措置を講じなければならない。また、主要な箇所の配線については、損傷等についての定期的な点検を行わなければならない。

（イ）　教育情報通信ネットワーク管理責任者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

（ウ）教育情報通信ネットワーク管理責任者は、自ら又はシステム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更又は追加できないように必要な措置を施さなければならない。

オ　サーバ等の機種更新

サーバ等の機種更新を行おうとする時、特に並行稼働時においては、サーバ等の設置場所における電源設備、空調設備等の能力、容量並びに現時点での設備の残存能力、容量を把握し、適切な対応を講じなければならない。

カ　敷地外への機器の設置

教育情報セキュリティ管理者は、委員会が保有するサーバ等の機器を庁舎の敷地外に設置する場合、定期的に当該機器へのセキュリティ対策状況について点検を行わなければならない。

キ　機器の廃棄等

教育情報セキュリティ管理者は、機器を廃棄又はリースの返却等をする場合、

機器内部の記憶装置から、全ての情報を消去の上、復元困難な状態にする措置を講じなければならない。

② 端末機等（職員用）

ア 執務室等における措置

端末機等が設置される執務室等については、職員が不在時の盗難防止のため、執務室等の施錠等による措置を講じなければならない。

イ 情報システム室における措置

情報システム室に設置される端末機等については、震災時の転倒又は盗難の防止のため、適切に固定する等必要な措置を講じなければならない。

ウ モバイル端末等のセキュリティ

・教育情報セキュリティ管理者は、不正アクセス防止のため、ログイン時の ID パスワードによる認証、加えて多要素認証の実施等、使用する目的に応じた適切な措置を講じなければならない。電磁的記録媒体については、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。

・教育情報セキュリティ管理者は、校務系サーバ、パソコン等教育情報システムへアクセスする端末へのログインパスワードの入力を必要とするように設定しなければならない。

・教育情報セキュリティ管理者は、取り扱う情報の重要度に応じてパスワード以外に生体認証や物理認証等の多要素認証を設定しなければならない。

③ 端末機等（学習者用）

GIGA スクール構想において整備した１人１台端末におけるセキュリティについては、後段で別途定めることとする。

ア 教育情報セキュリティ管理者は、盗難防止のため教室等で利用するパソコンの保管庫による管理等の物理的措置を講じなければならない。電磁的記録媒体については、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。

イ 教育情報セキュリティ管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

ウ 児童生徒が悪意のあるサイト等へのアクセスができないよう適切な措置を講じなければならない。

（２） ネットワークにおける措置

① ネットワーク構築上の措置

学校園情報通信ネットワークについては、別途定めるネットワーク管理要綱に基づき整備しなければならない。

ア　このポリシーは、業務運営のために用いる学校園情報通信ネットワークを対象とする。

イ　ネットワークについて、業務等を取り扱うシステムが利用するネットワーク及び委員会全体として情報の共有、活用を行うためのネットワーク（以下「校務系ネットワーク」という。）と学校教育において利用するネットワーク（以下「学習系ネットワーク」という。）と切り分けて構築しなければならない。

ウ　業務系ネットワークの外部へのネットワーク接続については、公益上特に必要である場合を除き行わないこととし、かつ、接続する場合であっても、必要最小限の範囲に限る。業務系ネットワーク及び教育系ネットワークの外部へのネットワーク接続については、接続ポイントを一元化し、情報セキュリティ対策を集約的に実施できるようにする。

エ　事業の目的により無線通信とする場合は、次の事項を遵守すること

・　解読が困難な暗号化及び認証技術を使用し、アクセスポイントへの不正な接続を防ぐこと

②　ネットワーク機器等

ア　ネットワークの基幹機器（管理用及び認証用サーバ、交換機等）については、情報システム室又は通信機械室に設置しなければならない。また、ネットワークの運用上重要な機能を有するサーバ等の機器については、障害発生時にネットワークの運用が停止しないように冗長化を図る等必要な措置を講じなければならない。

イ　主要なネットワーク機器（ハブ、ルータ等）及び配線については、管理者以外の者が容易に操作できないような場所に格納する等必要な措置を講じなければならない。

ウ　ネットワーク機器等の構成管理を適切に行わなければならない。

エ　主要なネットワーク機器については、落雷等による異常電流及び停電等の電気的障害に対し必要な措置を講じなければならない。

③　通信回線及び通信回線装置の管理

ア　教育統括情報セキュリティ責任者は、拠点間を結ぶ通信回線（ＷＡＮ）については、専用回線又は高いセキュリティ機能を有する回線により構成し、外部からの情報の盗聴及び情報の漏えい等を防止するなど、適切に管理しなければならない。

イ　教育統括情報セキュリティ責任者は、外部へのネットワーク接続ポイント及び該当ポイントに接続される端末を正確に把握し、適切な管理を行わなければならない。

ウ　主要な拠点間を結ぶ通信回線においては、バックアップ用の回線を敷設する等、障害の発生に備えなければならない。また、必要に応じ、通信経路上での暗号化を

行わなければならい。

（３）　情報システム室における措置

①　管理責任

重要システムのサーバ等の機器又はネットワークの基幹機器を設置する情報システム室の管理責任については、教育情報セキュリティ管理者が担う。

②　管理区域（情報システム室）

ア　管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋や電磁的記録媒体の保管庫をいう。

イ　情報システム室については、無窓の構造とする等、外部からの侵入が容易にできない管理区域としなければならない。

ウ　管理区域から外部に通じるドアについては必要最小限とし、施錠、警報装置、監視装置等により許可されていない者の立入りを防止しなければならない。

エ　情報システム室については、外部にその表示を行わない等、できるだけ所在を明らかにしないようにしなければならない。

③　入退室管理

ア　情報システム室に入室しようとする者は、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。ただし、当該情報システム管理者の属する課等の職員（以下「所属職員」という。）については、この限りでない。

イ　教育情報セキュリティ管理者は、許可を受けた者が情報システム室へ入室するときは、次の事項等を記録し、入室証及び名札を着用させ、必要に応じその提示を求めなければならない。

・入室年月日
・入退室時分
・所属または団体名及び氏名
・入室目的
・その他教育情報セキュリティ管理者が必要と認める事項

ウ　教育情報セキュリティ管理者は、入室を許可した者に対して、必要に応じて立入区域を制限し、所属職員の立会い等の措置を講じなければならない。

エ　教育情報セキュリティ管理者は、当該情報システム室に関係しない端末機、通信回線装置、記録媒体等を持ち込ませないようにしなければならない。

オ　教育情報セキュリティ管理者は、記録媒体等の情報資産の外部への持ち出しについて厳重な管理を行わなければならない。

④　機器等の搬入出

ア　情報システム室に機器等を搬入出する場合は、あらかじめ当該機器等の既存システムに対する安全性について、教育情報セキュリティ管理者による確認を行わなければならない。

イ　機器等の搬入出には、教育情報セキュリティ管理者の立会い等必要な措置を講じなければならない。

⑤　火災・震災等災害に対する措置

ア　情報システム室は、防火区画を設ける等の防火及び防煙に対する措置を講じなければならない。

イ　情報システム室の消火設備は、サーバ等の機器や記録媒体に影響を与えるものであってはならない。また、火気の取扱いについて厳重な管理を行わなければならない。

ウ　情報システム室を設置する建物及び情報システム室は、地震等に対する耐震措置を講じなければならない。また、情報システム室内の機器類は転倒防止措置を講ずるとともに、緊急時に職員及び委託事業者が円滑に避難できるように配置しなければならない。

エ　情報システム室には、浸水及び漏水防止等の措置を講じなければならない。

オ　空気調和設備は、急激な温湿度変化等に対処するため、その容量に配慮しなければならない。

⑥　電気的障害に対する措置

ア　情報システム室は、無停電電源装置の設置等、落雷等による異常電流に対する措置を講じなければならない。

イ　停電によるシステム等の停止が業務運営等に重大な影響を及ぼす可能性がある場合、必要に応じ、自家発電装置の設置等の措置を講じなければならない。

10　人的セキュリティ

（1）　職員における情報セキュリティの徹底

①　ポリシー等の遵守

全ての職員は、ポリシー及び実施手順に定められている事項を遵守しなければならない。

②　教育、研修

ア　ポリシーの周知等

（ア）　教育最高情報セキュリティ責任者は、委員会における情報セキュリティの連絡体制を利用し、教育情報セキュリティ管理者や学校等情報セキュリティ責任者その他必要と認める者に対し、ポリシー及び実施手順の周知徹底を行わなければならない。また、委員会が実施する研修等により、所属職員に対しポリシー及び実施手順の遵守について啓発しなければならない。

（イ）　教育情報セキュリティ管理者及び学校等情報セキュリティ責任者は、所属職員がポリシー及び実施手順について理解し、情報セュリティ上の問題が生じないよう、教育、指導を行わなければならない。

（ウ）　職員は、定められた研修・訓練に参加しなければならない。

イ　システムに係る情報セキュリティの徹底

教育情報セキュリティ管理者及び学校等情報セキュリティ責任者は、研修の実施等により、システムの運用に関わる職員を対象に、システム及び当該システムにより処理されるデータに係る情報セキュリティの実施手順並びに実施に必要な知識及び技術等について教育、指導を行わなければならない。

ウ　ネットワークに係る情報セキュリティの徹底

教育情報セキュリティ管理者は、必要と認める者に対し、ネットワークにおける情報セキュリティの実施手順並びに実施に必要な知識及び技術等について周知徹底を行わなければならない。

③　職員における情報管理

ア　情報の適切な処理及び業務目的以外の使用禁止

（ア）　職員は、設定されているアクセス権限に基づき、業務上必要な情報の処理を適切に処理しなければならない。

（イ）　職員は、業務目的以外での情報資産の外部への持ち出し、システムへのアクセス、インターネットのアクセス、メールの使用等ネットワークの利用を行ってはならない。

（ウ）　職員は、ウェブで利用できるフリーメール、ネットワークストレージサービスを使用してはならない。ただし、教育情報セキュリティ管理者が業務上、必要と判断した場合を除く。

（エ）　職員は、教育情報通信ネットワーク管理責任者の許可なく端末機を学校園情報通信ネットワークに接続してはならない。

（オ）　職員は、庁外で情報処理業務を行う場合には、学校等情報セキュリティ責任者の許可を得なければならない。

（カ）　外部ネットワークを利用し、本市以外のものとメールにより事務連絡等を行うときは、「電気通信回線を利用した公文書の発送及び収受に係る取扱要領」（平成 16 年 5 月 28 日施行）に基づき適切に取り扱わなければならない。また、保護データをメールにより取り扱う必要がある場合について、利用者は学校等情報セキュリティ責任者の承認を得るとともに、連絡相手のメールアドレス及びメール受取の確認を行う等、厳格に取り扱わなければならない。なお、学校内においてメールを利用する場合においても、上記の取扱いに準じ、適切に運用を行わなければならない。

イ　情報の漏えい等の防止及びアクセス権限情報の管理

（ア）　職員は、教育情報セキュリティ管理者又は学校等情報セキュリティ責任者の許可なくして、端末機又は記録媒体等を執務室以外に持ち出してはなら

ない。ただし、テレサポート機能の利用による業務実施時は、テレサポート機能用パソコン利用管理簿に記入のうえ、承認得た場合のみ、端末機または記録媒体等の持ち出しを許可する。

（イ）　職員は、貸与以外のパソコン、モバイル端末及び記録媒体等を原則業務に利用してはならない。ただし、業務上必要な場合は、学校等情報セキュリティ責任者の許可を得て利用することができる。

（ウ）　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秘匿しなければならない。

（エ）　学校等情報セキュリティ責任者は、端末機及び記録媒体の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

（オ）　職員は、端末機のソフトウェアに関する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。

（カ）　職員は、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。

・自己が利用しているＩＤは、他人に利用させてはならない。
・共用ＩＤを利用する場合は、学校等情報セキュリティ責任者が、利用者を管理すること。

（キ）　職員は、アクセス権限に係る情報を適切に管理し、自己の保有するパスワードに関しては、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ないこと。
・パスワードは十分な長さ（最低 8 文字以上とする。）とし、文字列は想像しにくいものとすること。
・パスワードは定期的に変更すること。
・仮のパスワードは、最初のログイン時点で変更すること。
・必要でない限りシステム間及び職員間でのパスワードの共有は行わないこと。
・端末機等のパスワードの記憶機能を利用してはならない。
・パスワードが流出した可能性がある場合は、速やかに学校等情報セキュリティ責任者に報告し、パスワードを変更しなければならない
・取り扱う情報の重要度に応じてパスワード以外に生体認証や物理認証等の多要素認証を設定しなければならない。

（ク）　職員は、使用する機器や記録媒体について、権限を有しない者の使用や閲覧を防止するため、端末から離れる場合にはログオフにする等適切な措置を講じなければならない。

（ケ）非常勤及び臨時の職員への対応

・学校等情報セキュリティ責任者は、非常勤及び臨時の職員に対し、採用時に教育情報セキュリティポリシー等のうち、非常勤及び臨時の職員が守るべき内容を理解させ、また実施及び遵守させなければならない。

・学校等情報セキュリティ責任者は、非常勤及び臨時の職員に端末機による作業を行わせる場合において、インターネットへの接続及びメールの使用等が不要の場合、これを利用できないようにしなければならない。

ウ　無許可ソフトウェアの導入等の禁止

（ア）　職員は、端末機へのソフトウェアのインストール及びアンインストール、若しくは機器の改造、設定変更、増設、交換を行う場合は、教育情報セキュリティ管理者又は学校等情報セキュリティ責任者の許可を得なければならない。

（イ）　職員は、著作権法や使用許諾契約等に違反するソフトウェアの使用又は複製等を行ってはならない。

エ　クラウドサービスの利用

（ア）　教育情報セキュリティ責任者は、クラウドサービス（事業者が提供するものに限らず、本市が自ら提供するもの等を含む。以下同じ。）を利用するに当たり、取り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。

（イ）　教育情報セキュリティ責任者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定しなければならない。

（ウ）　教育情報セキュリティ責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件としなければならない。

（エ）　教育情報セキュリティ責任者は、クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定めなければならない。

（オ）　教育情報セキュリティ責任者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービス提供事業者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

オ　セキュリティインシデントに対する報告

（ア）　職員は、システムの利用に際してセキュリティインシデントを発見した場

合又は市民等外部から通報を受けた場合は、速やかに学校等情報セキュリティ責任者に報告しなければならない。

（イ）　職員は、ネットワークの利用に際してセキュリティインシデントを発見した場合は、速やかに学校等情報セキュリティ責任者に報告しなければならない。

（ウ）　職員は、教育情報セキュリティ管理者又は学校等情報セキュリティ責任者の指示に従い、セキュリティインシデントに対し適切に対処しなければならない。

（エ）　職員は、情報セキュリティに対する事故、システム上の欠陥及び誤動作を発見した場合又は市民等外部から通報を受けた場合、学校等情報セキュリティ責任者に報告しなければならない。

（２）　外部委託（指定管理者に本市の電子計算機処理業務を実施させる場合を含む。以下同じ。）における管理

①　委託処理に当たっての基本原則

ア　システム及びネットワークの開発又は運用、保守を所管するシステムの管理者は、これらの業務の全部又は一部を事業者（指定管理者を含む。以下同じ。）に委託しようとする場合又は事業者の再委託を許可する場合、主体性が損なわれないよう委員会の責務等次の点に留意するとともに、事業者において情報セキュリティ対策が徹底されるよう必要な措置を講じなければならない。なお、再委託を受けた事業者も同様とする。

（ア）　調整・管理機能、スケジュール等業務全体の遂行を左右する重要な要件や機能を委員会のコントロール下におくこと。

（イ）　システム及びネットワークに係る業務を委託しようとするときは、システム等のブラックボックス化を防止するために、定期的に検討会議等を設置するなど適切な措置を講じること。

イ　システムに係る業務の委託については、事業者において厳重な情報セキュリティ対策が実施されるように管理、指導を行わなければならない。

ウ　システム及びネットワークの開発、運用等において複数の委託事業者が関わる場合は、その分担範囲・責任範囲を明確にするとともに、それらの連携を確保しなければならない。

エ　クラウドサービスを利用する場合は、データの重要性分類に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

②　委託処理における措置

ア　次の事項を委託契約書若しくは協定書に明記し、事業者にその内容を遵守させなければならない。

・　ポリシー及び実施手順の遵守

・　事業者の責任者、委託内容、作業者、作業場所の特定
・　提供されるサービスレベルの保証
・　事業者にアクセスを許可する情報の種類と範囲、アクセス方法
・　事業者の従業員に対する教育の実施
・　提供された情報の目的外利用及び受託者以外の者への提供の禁止
・　業務上知り得た情報の守秘義務
・　再委託に関する制限事項の遵守
・　委託業務終了時の情報資産の返還、廃棄等
・　委託業務の定期報告及び緊急時報告義務
・　本市による監査、検査
・　本市によるセキュリティインシデント発生時の公表
・　ポリシーが遵守されなかった場合の規定(損害賠償等)

イ　委託業務の処理に当たっては、委託先となる事業者について委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

ウ　事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ契約に基づき措置しなければならない。また、その内容を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。

エ　重要な情報を処理する場合等必要に応じ、職員が処理に立ち会うこと。

オ　委託業務に関わる事業者の職員に対し身分証明書等の携帯、着用を義務付ける等、契約で定められた資格を有する者が作業に従事していることを確認すること。

カ　作業を行う者のユーザＩＤ、パスワード等について、作業終了後、不要となった時点で速やかに抹消すること。

11　技術的セキュリティ

（1）　アクセス制御

①　アクセス権限の明確化

ア　教育情報セキュリティ管理者は、所管するシステムの機密保護を図るため、当該システムへアクセスが可能な利用者及びその利用範囲等アクセス権限を明確にし、権限のない利用者がアクセスできないように、システム上制限しなければならない。

イ　教育情報通信ネットワーク管理責任者は、ネットワークの機密保護を図るため、当該ネットワークへアクセスが可能な利用者及びその利用範囲等アクセス権限を定めなければならない。

②　アクセス権限の管理

ア　システム及びネットワークへのアクセス権限については、ユーザＩＤ及びパスワードにより管理を行わなければならない。取り扱う情報の重要度に応じてパス

ワード以外に生体認証等を併用した多要素認証を適用しなければならない。

イ　教育情報セキュリティ管理者及び教育情報通信ネットワーク管理責任者は、システムへのアクセス権限の把握、管理を適切に行わなければならない。また、ログインにおいて、正しくない操作が繰り返しなされた場合、ロックをかける等アクセスの制御を行わなければならない。

ウ　教育情報セキュリティ管理者及び教育情報通信ネットワーク管理責任者は、ユーザＩＤ及びパスワードについて、次の事項を定めなければならない。

・ユーザＩＤ及びパスワードの付与及び削除手続き
・ユーザＩＤの保管方法
・パスワードの守秘義務
・パスワードの変更時の管理方法
・その他教育情報セキュリティ管理者及び教育情報通信ネットワーク管理責任者が必要と認める事項

エ　教育情報セキュリティ管理者及び教育情報通信ネットワーク管理責任者は、利用されていないＩＤが放置されないよう、点検しなければならない。

オ　教育情報セキュリティ管理者は、管理者権限等の特権を付与されたＩＤを利用する者を必要最小限にし、当該ＩＤのパスワードの漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理しなければならない。

カ　教育情報セキュリティ管理者又は教育情報通信ネットワーク管理責任者の特権を代行する者は、教育情報セキュリティ管理者又は教育情報通信ネットワーク管理責任者が指名し、学校等情報セキュリティ責任者が認めた者でなければならない。

キ　教育情報セキュリティ管理者及び教育情報通信ネットワーク管理責任者は、特権を付与されたパスワードを初期設定以外のものに変更しなければならない。また、その変更を外部委託事業者に行わせてはならない。

ク　教育情報セキュリティ管理者及び教育情報通信ネットワーク管理責任者は、特権を付与されたＩＤ及びパスワードについて、その利用期間に合わせて特権ＩＤを作成・削除する、もしくは、入力回数制限を設ける等のセキュリティ機能を強化しなければならない。

③　職員による学校外からのアクセス等の制限

ア　職員が学校外から学校園情報通信ネットワーク又は内部のシステムにアクセスする場合は、教育情報通信ネットワーク管理責任者及び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。

イ　教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、学校園情報通信ネットワーク、又は内部のシステムに対する学校外からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければなら

ない。

ウ　教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、学校外からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

エ　教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、学校外からのアクセスに利用する端末機を職員に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

オ　職員等は、持ち込んだ又は外部から持ち帰った端末を施設内のネットワークに接続する前に、コンピュータウイルスに感染していないことを確認しなければならない。

④　ネットワーク接続管理

ア　教育情報通信ネットワーク管理責任者は、ネットワークに接続するサーバ及び端末機等機器を特定する識別記号を設定・配付し、ネットワークへの接続を適切に管理しなければならない。

イ　教育情報通信ネットワーク管理責任者は、サーバ及び端末機等機器をネットワークに接続するポートの管理及び不正接続の監視等を行わなければならない。

⑤　ネットワーク稼働環境の管理

ア　教育情報通信ネットワーク管理責任者は、ネットワーク設定情報について不正に変更されないよう、アクセス管理を行うとともに、障害時等に備え、設定情報のバックアップを確保しなければならない。また、ネットワーク構成等に関する情報は、関係者以外に開示してはならない。

イ　教育情報通信ネットワーク管理責任者は、ネットワーク上の通信利用状況並びにネットワーク設計の稼働実績及び資源の利用状況を把握するとともに、障害箇所の検知機能を備え、ネットワークの性能改善に向け必要な措置を講じる等、ネットワークを適正な稼働状況に保たなければならない。

ウ　教育情報通信ネットワーク管理責任者は、ネットワーク利用に大きな支障を生じさせかねない大容量のファイルの通信を制限する等、ネットワークの円滑な利用を図っていかなければならない。

エ　教育情報通信ネットワーク管理責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

（2）　不正アクセス対策

①　各種ログの取得等

ア　教育情報セキュリティ管理者及び教育情報通信ネットワーク管理責任者は、ログイン試行回数の制限、アクセスタイムアウトの設定およびログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ職員等がログインしたことを確認

することができるようシステムを設定しなければならない。

イ　教育情報セキュリティ管理者及び教育情報通信ネットワーク管理責任者は、各種ログ及び情報セキュリティの確保に必要な次の事項を記録し、一定の期間保存するとともに、窃取、改ざん、消去されないように必要な措置を講じなければならない。

- 利用年月日
- 利用開始時分及び終了時分
- 利用者
- 業務名
- その他教育情報セキュリティ管理者及び教育情報通信ネットワーク管理責任者が必要と認める事項

ウ　教育情報セキュリティ管理者及び教育情報通信ネットワーク管理責任者は、ネットワークへのアクセス記録等を取得し、アクセス状況について定期的に解析、点検しなければならない。必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析をしなければならない。また、当該アクセス記録等は一定の期間保存するとともに、窃取、改ざん、消去されないように必要な措置を講じなければならない。

エ　教育情報通信ネットワーク管理責任者は、ネットワークの利用に当たり、業務目的以外のインターネットへのアクセス等不適切な利用が行われないように制限をかけることができる。また、教育情報通信ネットワーク管理責任者は、職員が業務目的以外の不適切な利用を行おうとしていることが判明した場合、当該職員が属する学校等情報セキュリティ責任者に通知し、適切な措置を講じなければならない。

②　外部ネットワークとの接続に係る措置

ア　ネットワーク及びシステムを外部ネットワークと接続するとき、教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、接続を行う外部ネットワークの構成、セキュリティレベル並びに委員会内部のネットワーク及びシステムにおけるリスク等を詳細に検討し、必要な情報セキュリティ対策が講じられることを明確に確認したうえで、接続を行わなければならない。また、外部ネットワークへの接続について、教育最高情報セキュリティ責任者の承認を受け、適切に実施及び管理を行わなければならない。

イ　教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、接続した外部ネットワークにセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、教育統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

ウ　外部からのアクセスの許可は、必要最小限にしなければならない。また、外部

からネットワーク、システムにアクセスする場合は、外部アクセスサーバに対してのみ接続を許可する等、内部への不正なアクセスを防御する構成としなければならない。

エ　外部からの不正なアクセスを防御するため、ファイアウォール、侵入検知装置の設置、ポートの管理、アクセス状況の監視等、不要なサービスの停止等、必要な措置を講じなければならない。

オ　外部ネットワークを利用し、委員会以外のものと通信（メールの利用又はホームページによる情報提供等を行う場合を除く。）を行うときは、原則として重要性分類Ⅲ以上のデータは取り扱ってはならない。業務上、重要なデータの取扱いが特に必要な場合については、情報の漏えい、改ざん等を防止するため、あらかじめ個人情報保護条例その他の関連する法令等に基づき必要な対処を行うとともに、通信先との相互の認証、データの暗号化、セキュリティの高い通信回線の利用等必要な措置を講じなければならない。また、その際、使用する暗号鍵については厳重に管理しなければならない。

カ　ホームページを利用した情報提供等においても、原則として個人情報は取り扱ってはならない。ただし、学校教育上個人情報を取り扱う必要があるときは、あらかじめ個人情報保護条例に基づき必要な対処を行い適正に運用しなければならない。なお、学校内向けのホームページについても、上記の取扱いに準じ、適切に運用を行わなければならない。

キ　重要性が高い情報に対するインターネットを介した外部からのリスク、児童生徒による重要性が高い情報へのアクセスリスクの対応は次のとおりとする。

・教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、校務系システム及び学習系システム間の通信経路の論理的又は物理的な分離をするとともに、ウェブ閲覧やインターネットメールなどのインターネットを介した外部からのリスクの高いシステムと重要性が高い情報を論理的又は物理的に分離をする、もしくは、各システムにおけるアクセス権管理の徹底を行う措置を講じなければならない。

・教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、校務系システムとその他のシステムとの間で通信する場合には、各システムにおけるアクセス権管理の徹底を行う、ウイルス感染のない無害化通信など、適切な措置を図らなければならない。

③　不正アクセス等発見時の対応

ア　教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、不正アクセスによるネットワーク及びシステムへの攻撃を発見したときは、影響範囲及び侵入経路等の調査並びに攻撃の記録を保存し、必要な対策を速やかに講じなければならない。また、必要に応じて警察及び関係機関との緊密な連携に努めな

ければならない

イ　教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、不正アクセスによる攻撃を受け、ネットワーク及びシステム等情報資産に影響が生じたときは、適切な措置を講じなければならない。

ウ　教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、攻撃の予告等により攻撃を受けることが明確になった場合、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。また、関係機関と連絡を密にして情報の収集に努めなければならない。

エ　教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、職員による不正アクセスを発見した場合は、当該職員が属する学校等情報セキュリティ責任者に通知し、適切な処置を求めなければならない。

オ　教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

（3）　コンピュータウイルス対策

①　ウイルス対策の実施

ア　教育情報通信ネットワーク管理責任者は、外部のネットワークから受信したファイルについてウイルスチェックを行うなど、ネットワークへの感染を防止しなければならない。

イ　教育情報通信ネットワーク管理責任者は、外部のネットワークへ送信するファイルについてウイルスチェックを行うなど、外部へのウイルスの拡散を防止しなければならない。

ウ　教育情報通信ネットワーク管理責任者は、ウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

エ　教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、ウイルスの感染、侵入が生じる可能性が著しく低い場合を除き、ウイルスチェック用のソフトウェアを導入しなければならない。

オ　教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、サーバ及び端末機に、ウイルスチェック用のソフトウェアを常駐させなければならない。

カ　教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、端末機に対して、ウイルスチェック用の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。

キ　教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、システムがインターネットに接続している場合、ウイルスチェック用のソフトウェア及びパターンファイルを常に最新の状態に保つよう努めなければならない。

ク　教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、システムがインターネットに接続していない場合、定期的にウイルスチェック用のソフトウェア及びパターンファイルの更新を実施しなければならない。また、記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、貸与以外の記録媒体を職員に利用させてはならない。ただし、業務上必要な場合は、学校等情報セキュリティ責任者の許可を得て利用することができる。

ケ　業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。

②　ウイルス対策の周知・徹底

職員は、次の事項を遵守しなければならない。

・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、必ずウイルスチェックを行うこと

・添付ファイルのあるメールを送受信するときは、添付ファイルにウイルスが感染していないかどうか確認を行うこと

・差出人が不明又は不自然に添付されたファイルは開かず速やかに削除すること

・教育情報セキュリティ管理者から提供されるウイルス情報に留意し対応すること

・教育情報セキュリティ管理者又は学校等情報セキュリティ責任者が許可した記録媒体以外は使用しないこと

・端末機において、ウイルスチェック用の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こと

③　ウイルス感染時の対応

ア　教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、ウイルスチェックの結果、ウイルスの感染を発見したときは、影響範囲及び感染経路等を調査し、ウイルスの駆除等必要な対策速やかに講じなければならない。

イ　教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、ウイルスによりネットワーク及びシステム等情報資産に影響が生じたときは、侵害時の対応に基づき必要な措置を講じなければならない。

ウ　職員は、ウイルスに感染した場合又は感染が疑われる場合は、以下の対応を行わなければならない。

・パソコン等の LAN ケーブルの即時取り外しを行うこと

・モバイル端末等の利用を直ちに中止し、通信を行わない設定への変更又はシャ

ットダウンを行うこと

（４）　システムの開発、導入、保守における措置

①　システムの調達

ア　教育情報セキュリティ管理者は、システムの開発、導入、保守等の調達に当たって、調達仕様書が情報セキュリティの確保の上で問題のないようにしなければならない。

イ　教育情報セキュリティ管理者は、機器及びソフトウェアを調達する場合は、製品が情報セキュリティ上問題にならないかどうか、確認しなければならない。

②　システムの開発

ア　教育情報セキュリティ管理者は、学校園情報通信ネットワークを利用し、システムの開発を行うときは、教育最高情報セキュリティ責任者に協議しなければならない。

イ　教育情報セキュリティ管理者は、システムの開発に当たって、リスク分析を行うとともに、事故、障害等による被害の発生を防止する､若しくは最小限に抑えるため、次の事項に留意し、必要な対策を講じなければならない。

・システムの運転状況を監視する機能を備えるとともにシステムの障害箇所の検知機能を備えること

・障害箇所を特定するため、ロギング情報（処理及び操作の記録情報）が取得できること

・必要に応じて故障箇所を閉塞し縮退運転ができるようにすること

・必要に応じてサーバ、ディスク装置等主要機器の代替機器を備え、障害時に代替機器への切替が容易に行えること

・本番の運用環境と開発、保守環境とは別に分けること

・本番のシステムデータ及びプログラムとテスト用のデータ及びプログラムは別に管理すること

・データ及びシステムのバックアップが容易に行えるようにすること

・データ入力時のエラーチェックを行えるようにすること

・システム開発の責任者及び作業者が使用するＩＤを管理し、開発完了後、開発用ＩＤを削除すること

・システム開発の責任者及び作業者のアクセス権限を設定すること

ウ　教育情報セキュリティ管理者は、システムの維持管理に必要な各種ドキュメントを整備し、保管場所を定め厳重に保管しなければならない。

また、ネットワーク構成図、情報システム仕様書等について、記録媒体等に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適切に管理しなければならない。

エ　教育情報セキュリティ管理者は、所管するシステムの運用において実施した作業について、作業記録を作成しなければならない。また、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないよう適切に管理しなければならない。

オ　教育情報セキュリティ管理者及び契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、２名以上で作業し、互いにその作業を確認しなければならない

カ　教育情報セキュリティ管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

③　システムの導入

ア　教育情報セキュリティ管理者は、システムを導入する前に十分なテストを行い、不具合の発見及び解消に努めなければならない。

イ　教育情報セキュリティ管理者は、既存のネットワークを利用したシステムを導入しようとするときは、当該ネットワークの教育情報セキュリティ管理者に協議し、ネットワークへの接続テストを行うとともに、アクセス権限を明確にし、アクセスの管理等に関する事項を定めなければならない。

④　システムの保守

ア　教育情報セキュリティ管理者は、システムの保守を行うときは、不具合の確認を行い、既存のシステムの運用に影響が出ないようにしなければならない。

イ　教育情報セキュリティ管理者は、システムの追加、変更、廃棄等をしたときは、その際の履歴を記録するとともに、ドキュメントの変更整備を行わなければならない。

⑤　機器の保守等

ア　機器の保守点検を定期的に実施するとともに、その記録を適切に保存しなければならない。

イ　記録媒体の含まれる機器について、外部の業者に修理させる場合は、当該機器に記録されている内容が消去された状態で行わなければならない。ただし、情報を消去することが難しい場合は、修理を委託する事業者に対し秘密を守ることを契約に定めなければならない。

ウ　記録媒体の含まれる機器を廃棄、リース返却等をする場合は、当該機器に記録されている全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

（５）電子メールのセキュリティ対策

①　電子メールのセキュリティ管理

ア　教育統括情報セキュリティ責任者は、権限のない利用者により、外部から外部

への電子メール転送が行われることを不可能とするよう、電子メールのサーバの設定を行わなければならない。

イ　教育統括情報セキュリティ責任者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。

ウ　教育統括情報セキュリティ責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

エ　教育統括情報セキュリティ責任者は、職員が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を教職等に周知しなければならない。

②　電子メールの利用制限

ア　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。

イ　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。

ウ　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。

エ　職員等は、重要な電子メールを誤送信した場合、学校等情報セキュリティ責任者に報告しなければならない。

（6）　セキュリティ情報の収集

①　セキュリティホールに関する情報の収集及び修正

教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、情報セキュリティに関する最新の情報を収集し、必要に応じ関係者間で共有しなければならない。また、緊急度に応じてネットワーク、システムの端末機及びサーバ等のソフトウェアに最新のプログラム修正を行うことにより、セキュリティホールを防ぐ等、必要な措置を講じなければならない。

②　セキュリティ侵害の対策

教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、情報セキュリティに関する最新の情報を収集し、必要に応じて関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

③　ウイルス対策の周知・徹底

教育情報通信ネットワーク管理責任者及び教育情報セキュリティ管理者は、常時ウイルスに関する情報収集に努めるとともに、必要に応じてウイルス対策について職員に対する啓発を行わなければならない。

12　運用

（1） システム等の適正運用

① 実施手順の作成

ア 教育情報セキュリティ管理者は、ポリシーに基づき、当該システムにおける情報セキュリティ対策の実施に関し必要となる事項を定めた実施手順を作成し、教育最高情報セキュリティ責任者の承認を得なければならない。

イ 教育情報通信ネットワーク管理責任者は、ポリシーに基づき、当該ネットワークにおける情報セキュリティ対策の実施に関し必要となる事項を定めた実施手順を作成し、教育最高情報セキュリティ責任者の承認を得なければならない。

② 運用管理手法、運用計画の明確化

ア 教育情報セキュリティ管理者は、システムの運用を開始する前に、運用管理の手法及び体制等について明らかにしなければならない。

イ 教育情報セキュリティ管理者は、システムの運用に当たり、運用計画を策定し、年間・月間・週間等における運用スケジュール、システムの運用時間、運用形態等運用管理に必要な事項を明確にしなければならない。

ウ 教育情報通信ネットワーク管理責任者は、ネットワークの運用に当たり、運用管理の手法及び体制、運用計画を明らかにしなければならない。

③ 機器操作の適正化

ア システムにおける措置

（ア） システムのサーバ等の機器については教育情報セキュリティ管理者、また端末機については学校等情報セキュリティ責任者が、それぞれ指示若しくは承認した者が操作を行わなければならない。

（イ） 教育情報セキュリティ管理者は、操作マニュアル等を作成し、研修を実施する等機器操作の適正化に努めなければならない。また、システムの追加、変更、廃棄等をしたときは、その履歴を記録するとともに常に変更を反映し、操作マニュアル等を最新の状態にしなければならない。

（ウ） 教育情報セキュリティ管理者は、システムのオペレーション作業の実施に当たり、次の事項について管理方法を明確に定め、適切に運用管理を行わなければならない。

- スケジュール管理
- 出力及び廃棄帳票の管理
- 磁気テープ等の記録媒体の管理
- オペレータの電子計算機室への入退室管理
- オペレータの作業内容の把握、管理
- 電子計算機機器及びネットワーク機器の障害時の対応
- その他必要な事項

イ ネットワークにおける措置

（ア）　ネットワーク機器の操作については、教育情報通信ネットワーク管理責任者が指示若しくは承認した者が行わなければならない。

（イ）　教育情報通信ネットワーク管理責任者は、操作マニュアル等を作成する、又は利用方法の周知を行う等ネットワークの利用の適正化に努めなければならない。また、ネットワークの追加、変更、廃棄等をしたときは、その履歴を記録するとともに常に変更を反映し、操作マニュアル等を最新の状態にしなければならない。

（ウ）　教育情報通信ネットワーク管理責任者は、ネットワークのオペレーション作業の実施について適切に管理しなければならない。

④　データ等のバックアップ運用

ア　教育情報セキュリティ管理者は、万一の事故、障害等の発生に備え、データ・プログラムのバックアップを適切に行わなければならない。

イ　データ・プログラムのバックアップに当たっては、次の事項に留意しなければならない。

（ア）　教育情報セキュリティ管理者は、バックアップコピーを取得するデータ、取得の方法及びサイクルを定め、それに基づいてデータのバックアップを適切に実施しなければならない。

（イ）　教育情報セキュリティ管理者は、プログラムの変更の都度、プログラムのバックアップコピーを取得しなければならない。

（ウ）　教育情報セキュリティ管理者は、データのバックアップ取得後、次のデータのバックアップ取得までの間、必要に応じて、データベースの更新記録情報を取得しなければならない。

（２）　システム等の監視及び予防措置

①　システム等の監視

ア　重要システムの運用に当たっては、情報セキュリティに関する事案を検知するため、教育情報セキュリティ管理者は、常にシステムの稼働監視を行わなければならない。特に、外部と接続するシステムについては、ファイアウォール等を用い、不正なアクセスによる攻撃を受けていないかどうか監視、分析を行わなければならない。

イ　ネットワークに係る情報セキュリティに関する事案を検知するため、教育情報通信ネットワーク管理責任者は、ネットワークの稼働監視を行わなければならない。特に、外部と接続するネットワークについては、ファイアウォール、侵入監視装置等を用い、不正なアクセスによる攻撃を受けていないかどうか監視、分析を行わなければならない。

ウ　監視により得られた結果については、消去や改ざんされないために必要な措置

を講じ、定期的に安全な場所に保管しなければならない。

エ　重要なログ等を取得するサーバについては、正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

②　予防措置

ア　教育情報セキュリティ管理者は、システム及びネットワークに障害又は侵害が発生し、システムが利用できない場合に備え、業務への影響を最小限に抑えるため、代替処理方法を定めなければならない。

イ　システムに被害が生じるおそれがある事案を発見した場合、教育情報セキュリティ管理者は予防措置を講じなければならない。また、教育情報セキュリティ管理者は、直ちに教育ＩＣＴ管理者に報告しなければならない。

ウ　教育ＩＣＴ管理者は、直ちに、当該事案を教育最高情報セキュリティ責任者に報告しなければならない。

エ　ネットワークに被害が生じるおそれがある事案を発見した場合、教育情報通信ネットワーク管理責任者は、予防措置を講じなければならない。また、教育情報通信ネットワーク管理責任者は、直ちに、当該事案を教育ＩＣＴ管理者に報告しなければならない。

オ　教育ＩＣＴ管理者は、直ちに、当該事案を教育最高情報セキュリティ責任者に報告しなければならない。

（３）　システム等の障害時、侵害時の対応

①　障害時の対応

ア　システムにおける措置

（ア）　責任体制

教育情報セキュリティ管理者及び学校等情報セキュリティ責任者は、システムの障害時における連絡及び対処の責任者となり、関係者との連携によりシステムを速やかに回復しなければならない。

（イ）　障害時における対応方法の周知

教育情報セキュリティ管理者及び学校等情報セキュリティ責任者は、システムの運用を開始する前に、障害時における対応マニュアルを関係者に周知しなければならない。

（ウ）　障害時の連絡及び対処

a　システムの利用者が障害を発見したときは、直ちに学校等情報セキュリティ責任者に報告し、学校等情報セキュリティ責任者は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。

b　教育情報セキュリティ管理者は、障害を発見し、又は障害の連絡を受けたときは、直ちに、障害状況及び影響範囲を調査するとともに、必要に応じて障害状況等を学校等情報セキュリティ責任者に連絡しなければならない。

c　教育情報セキュリティ管理者及び学校等情報セキュリティ責任者は、システムの回復に向け適切な措置を講じなければならない。

d　教育情報セキュリティ管理者及び学校等情報セキュリティ責任者は、障害・故障の発生に関係した部門から原因及び処理の報告を求めるとともに、当該障害・故障の原因及び処理結果について障害記録簿を作成・記録しなければならない。

e　教育情報セキュリティ管理者は、障害の被害が重大な場合又はシステムの運用に著しい支障（以下「重大障害」という。）が発生している場合は、直ちに、教育ＩＣＴ管理者に第 1－1 号様式により報告を行わなければならない。

f　報告を受けた教育ＩＣＴ管理者は、直ちに、教育最高情報セキュリティ責任者に報告を行わなければならない。

（エ）　再発防止措置

教育情報セキュリティ管理者及び学校等情報セキュリティ責任者は、障害原因等を分析し、再発防止に向け必要な改善措置を講じなければならない。

（オ）　事後検証

教育最高情報セキュリティ責任者は、報告のあった障害事案について、再発防止に向け必要な改善措置が講じられているか教育ＩＣＴ管理者に報告を求めることができる。

イ　ネットワークにおける措置

（ア）　責任体制

教育情報通信ネットワーク管理責任者は、障害時における連絡及び対処の責任者となり、関係者との連携によりネットワークを速やかに回復しなければならない。

（イ）　障害時における対応方法の周知

教育情報通信ネットワーク管理責任者は、障害時における対応方法について、関係者に周知しなければならない。

（ウ）　障害時の連絡及び対処

a　ネットワークの利用者が障害を発見したときは、直ちに、学校等情報セキュリティ責任者に報告し、学校等情報セキュリティ責任者は教育情報通信ネットワーク管理責任者に連絡しなければならない。

b　教育情報通信ネットワーク管理責任者は、障害を発見し、又は障害の連絡を受けたときは、直ちに、障害状況及び影響範囲を調査するとともに、学校等情報セキュリティ責任者に当該障害状況等を連絡しなければならない。

c　教育情報通信ネットワーク管理責任者は、障害に関係する学校等情報セキュリティ責任者と連携し、障害の回復に向け適切な措置を講じなければな

らない。

d　教育情報通信ネットワーク管理責任者は、障害発生に関係した部門から障害の原因及び処理の報告を求めるとともに、ネットワーク上の障害、故障の原因及び処理結果について障害記録簿を作成、記録しなければならない。

e　教育情報通信ネットワーク管理責任者は、ネットワークに重大障害が発生している場合は、直ちに、教育ＩＣＴ管理者に第1－1号様式により報告を行わなければならない。

f　報告を受けた教育ＩＣＴ管理者は、直ちに教育最高情報セキュリティ責任者に報告を行わなければならない。

（エ）　再発防止措置

教育情報セキュリティ管理者及び学校等情報セキュリティ責任者は、障害原因等を分析し、再発防止に向け必要な改善措置を講じなければならない。

（オ）　事後検証

教育最高情報セキュリティ責任者は、報告のあった障害事案について、再発防止に向け必要な改善措置が講じられているか教育ＩＣＴ管理者及び教育情報通信ネットワーク管理責任者に報告を求めることができる。

②　侵害時の対応

ア　システムにおける措置

（ア）　責任体制

教育情報セキュリティ管理者及び学校等情報セキュリティ責任者は、所管する情報資産において、不正行為等による情報の漏えい、滅失、改ざん等の侵害事案が発生した場合、連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速に実施するとともに、再発防止の措置を講じなければならない。また、教育最高情報セキュリティ責任者は、侵害時の対応が円滑に実施されるよう、監督、指導を行わなければならない。

（イ）　侵害時の対応方法の周知

教育情報セキュリティ管理者は、所管する情報資産に対し作成される実施手順において、侵害時の対応方法を明記させるとともに、関係する管理者、職員に対し当該対応方法について周知を行わなければならない。

（ウ）　侵害時の連絡

a　システムの利用者が侵害事案の発生を発見したときは、直ちに、学校等情報セキュリティ責任者に報告し、学校等情報セキュリティ責任者は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。また、教育情報セキュリティ管理者が侵害事案の発生を発見したときは、教育情報セキュリティ管理者は学校等情報セキュリティ責任者に報告しなければならない。

b　教育情報セキュリティ管理者は、侵害事案の発生を発見し、又は侵害の報

告を受けたときは、直ちに、教育ＩＣＴ管理者に第1－1号様式又は第1－2号様式により報告を行わなければならない。

c　報告を受けた教育ＩＣＴ管理者は、直ちに、教育最高情報セキュリティ責任者に報告しなければならない。

d　教育ＩＣＴ管理者及び教育情報セキュリティ管理者は、侵害事案が法令等に違反するものと見込まれる場合、教育最高情報セキュリティ責任者と協議し、警察等関係機関に通報しなければならない。

e　教育最高情報セキュリティ責任者は、侵害事案がサイバー攻撃等による緊急時の場合においては、緊急連絡体制を設置し、情報セキュリティ対策が適切に実施されるよう、監督、指導を行わなければならない。

f　侵害を発見した者又は侵害の報告を受けた者は、当該侵害事案を報告すべき者が不在の場合その他の場合において、急を要するときは、上記の規定にかかわらず、直ちに、当該侵害事案を報告すべき者の上位の者に報告しなければならない。

(エ)　事案への対処

a　教育情報セキュリティ管理者及び学校等情報セキュリティ責任者は、侵害事案が発生したときは、次の事項について調査を実施しなければならない。

・　事案の内容
・　事案が発生した原因
・　確認した被害・影響範囲

b　教育情報セキュリティ管理者は、次の事案が発生し情報資産保護のためにシステムの停止がやむを得ない場合は、学校等情報セキュリティ責任者に協議の上、システムを停止しなければならない。ただし、情報資産を保護するため急を要する場合には、教育情報セキュリティ管理者は当該協議をしないでシステムを停止することができる。

・　システムの運用に著しい支障をきたす攻撃が継続しているとき
・　コンピュータウイルス等不正プログラムが情報に深刻な被害を及ぼしているとき
・　その他の情報資産に係る重大な被害が想定されるとき

c　教育情報セキュリティ管理者及び学校等情報セキュリティ責任者は、事案に係るシステムのアクセス記録及び現状を保存するとともに、事案に対処した経過を記録しなければならない。

d　事案に係る証拠保全の実施を完了するとともに、再発防止の暫定措置を講じた後、システムの復旧を行う。

e　教育ＩＣＴ管理者は、上記の対処に当たり、教育情報セキュリティ管理者から随時報告を求め、作業の実施を管理しなければならない。

（オ）　再発防止措置

教育情報セキュリティ管理者及び学校等情報セキュリティ責任者は、当該事案に係る原因及びリスク等を分析し、再発防止に向け必要な改善措置を講じなければならない。また、教育ＩＣＴ管理者は、改善措置の実施について確認を行うとともに、再発防止に向け、関係する管理責任者、職員に対し対応方法について周知を行わなければならない。

（カ）　事後検証

教育最高情報セキュリティ責任者は、報告のあった侵害事案について、再発防止に向け必要な改善措置が講じられているか教育ＩＣＴ管理者に報告を求めることができる。

イ　ネットワークにおける措置

（ア）　責任体制

教育情報通信ネットワーク管理責任者は、ネットワークにおいて、不正行為等による情報の漏えい、滅失、改ざん等の侵害事案が発生した場合、連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速に実施するとともに、再発防止の措置を講じなければならない。

また、教育最高情報セキュリティ責任者は、侵害時の対応が円滑に実施されるよう、監督、指導を行わなければならない。

（イ）　侵害時の対応方法の周知

教育情報通信ネットワーク管理責任者は、ネットワークに係る実施手順において、侵害時の対応方法を明記するとともに、関係する管理責任者、職員に対し当該対応方法について周知を行わなければならない。

（ウ）　侵害時の連絡

a　ネットワークの利用者が侵害事案の発生を発見したときは、直ちに、学校等情報セキュリティ責任者に報告し、学校等情報セキュリティ責任者は教育情報通信ネットワーク管理責任者に報告しなければならない。

b　教育情報通信ネットワーク管理責任者は、侵害事案の発生を発見し、又は侵害の報告を受けたときは、直ちに、教育ＩＣＴ管理者に第1－1号様式又は第1－2号様式により連絡を行わなければならない。

c　報告を受けた教育ＩＣＴ管理者は、直ちに、教育最高情報セキュリティ責任者に報告を行わなければならない。

d　教育ＩＣＴ管理者及び教育情報セキュリティ管理者は、侵害事案が法令等に違反するものと見込まれる場合、教育最高情報セキュリティ責任者と協議し、警察等関係機関に通報しなければならない。

e　教育最高情報セキュリティ責任者は、侵害事案がサイバー攻撃等による緊急時の場合においては、緊急連絡体制を設置し、情報セキュリティ対策が適切に

実施されるよう、監督、指導を行わなければならない。

f　侵害を発見した者又は侵害の報告を受けた者は、当該侵害事案を報告すべき者が不在の場合その他の場合において、急を要するときは、上記の規定にかかわらず、直ちに、当該侵害事案を報告すべき者の上位の者に報告しなければならない。

(エ)　事案への対処

a　教育情報通信ネットワーク管理責任者は、侵害事案が発生したときは、次の事項について調査を実施しなければならない。

- 事案の内容
- 事案が発生した原因
- 確認した被害・影響範囲

b　教育情報通信ネットワーク管理責任者は、次の事案が発生し情報資産保護のためにやむを得ない場合は、ネットワークの停止を含む必要な措置を講じなければならない。

- ネットワークの運用に著しい支障をきたす攻撃が継続しているとき
- コンピュータウイルス等不正プログラムがネットワーク経由で拡がっているとき
- 委員会のメールサーバ等が原因となって他者に被害を与えるおそれがあるとき
- その他の情報に係る重大な被害が想定されるとき

c　教育情報セキュリティ管理者は、事案に係るシステムのアクセス記録及び現状を保存するとともに、事案に対処した経過を記録しなければならない。

d　事案に係る証拠保全の実施を完了するとともに、再発防止の暫定措置を講じた後、ネットワークの復旧を行う。

e　ネットワークに係る対処に当たり、教育最高情報セキュリティ責任者は、教育ＩＣＴ管理者から随時報告を求め、作業の実施を管理しなければならない。

(オ)　再発防止措置

教育情報通信ネットワーク管理責任者は、当該事案に係る原因及びリスク等を分析し、再発防止に向け必要な改善措置を講じなければならない。教育情報通信ネットワーク管理責任者は、ネットワークの改善措置の実施について確認を行うとともに、再発防止に向け、関係する管理責任者、職員に対し対応方法について周知を行わなければならない。

(カ)　事後検証

教育最高情報セキュリティ責任者は、報告のあった侵害事案について、再発防止に向け必要な改善措置が講じられているか教育ＩＣＴ管理者及び教育情報通信ネットワーク管理責任者に報告を求めることができる。

（４）　例外措置

①　例外措置の許可

教育情報セキュリティ管理者及び学校等情報セキュリティ責任者は、ポリシー等を遵守することが困難な状況で、事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合には、教育最高情報セキュリティ責任者に第２号様式により許可を受けて、例外措置を取ることができる。

②　緊急時の例外措置

教育情報セキュリティ管理者及び学校等情報セキュリティ責任者は、事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後直ちに教育最高情報セキュリティ責任者に第２号様式により報告しなければならない。

13　ポリシー等の遵守状況の確認

（１）　ポリシー等の遵守状況の確認

①　学校等情報セキュリティ責任者は、学校等において、ポリシー及び所管する情報資産に係る実施手順が遵守されているかどうか、また、侵害等の問題が発生していないかについて確認し、問題が発生した場合には、直ちに、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。

②　教育情報セキュリティ管理者は、委員会において、ポリシー及び所管する情報資産に係る実施手順が遵守されているかどうか、また、侵害等の問題が発生していないかについて確認し、問題が発生した場合には、直ちに、教育最高情報セキュリティ責任者に報告しなければならない。

③　教育最高情報セキュリティ責任者は、ポリシー等の遵守状況及び問題発生の状況について確認を行うため、教育情報セキュリティ管理者に報告を求めることができる。

④　実施手順の作成方法等については、教育最高情報セキュリティ責任者が定める。教育最高情報セキュリティ責任者は、所管する情報資産について実施手順の作成又は見直しが行われた場合、当該教育情報セキュリティ管理者から報告を受けなければならない。また、教育情報セキュリティ管理者は、実施手順を見直し、変更（役職名や連絡先の変更等の軽微なものを除く。）が行われた場合、教育最高情報セキュリティ責任者に報告を行わなければならない。

（２）　ポリシー違反に関する対応

①　システムの利用者が違反を確認したときは、教育情報セキュリティ管理者に報告すること。

②　報告を受けた教育情報セキュリティ管理者は、適切な措置を行うこと。

③　教育情報セキュリティ管理者の指導によっても改善されない場合は、教育最高情報セキュリティ責任者は、当該職員のネットワーク又はシステムを使用する権利を停止あるいは剥奪することができる。その後速やかに、教育最高情報セキュリティ責任者は、職員の権利を停止あるいは剥奪した旨を教育情報セキュリティ管理者に通知すること。

14　１人１台端末におけるセキュリティ

（１）学習者用端末のセキュリティ対策

①　授業に支障のないネットワーク構成の選択

クラウドサービス提供事業者側のサービス要件基準を満たしたネットワーク構成を設計する。また、運用開始時には十分検証し、利用状況に応じて定期的に改修計画を行うこと。

②　不適切なウェブページの閲覧防止

児童生徒が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。

③　マルウェア感染対策

学校内外での端末の利用におけるマルウェア感染対策を講じなければならない。

④　端末を不正利用させないための防止策

端末の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、常に安全で児童生徒が安心して利用できる状態を維持しなければならない。

⑤　セキュリティ設定の一元管理

児童生徒への端末配布後においても、端末のセキュリティ設定や OS アップデート、ウェブブラウザのアップデート、学習用ツールのインストール、端末の利用履歴も含めた状態確認などの作業を、離れた場所からでも一元管理できることが望ましい。

⑥　端末の盗難・紛失時の情報漏洩対策

児童生徒が端末を紛失しても、遠隔操作でロックをかける、あるいはデータ消去することで第三者による不正操作や情報漏洩を防ぐ等の安全管理措置を講じなければならない。

⑦　運用・連絡体制の整備

学校内外での端末の運用ルールを制定し、インシデント時の連絡先対応方法を各学校にて整理しなければならない。

（２）児童生徒における ID 及びパスワード等の管理

①　入学・転入時の ID 登録処理

ID についてはシンプル・ユニーク（唯一無二）・パーマネント/パーシスタント（永

続的な識別）な構成要素になっていることなど適切な措置を講じなければならない。ID 登録やパスワードポリシーにおいては情報セキュリティ対策として重要な要素であるため学校毎に管理するのではなく、同一ドメインの委員会で一元管理することが望ましい。

② 進級・進学時の ID 関連情報の更新

ID については原則として進級・進学にも変更不要とすることが望ましい。そのため ID を変えることなく ID の属性情報（進級時の組・出席番号、進学先学校名など）の更新を行っておくことで、MDM による各種ポリシーや使用アプリケーションの変更を効率的に行うことが可能となる。さらに統合型校務支援システム等における児童生徒の氏名と連動した ID 管理を行うことで、校務側で管理している属性情報と一体となった ID を含んだマスター管理の一元化が望ましい。

③ 転出・卒業・退学時の ID 削除処理

ユニークな ID は個人を識別できる可能性があるため、個人情報保護の観点から、サービス提供期間を超えて個人を特定する情報を保持しないようにする必要がある。転出や卒業、退学時に学習用ツールのサービス利用期間が終了する場合は、あらかじめ児童生徒本人によるデータ移行をサービス利用期間内に実施し、ID の利用停止後、最終的には ID 及び関連するデータの完全削除を行うこと。

ただし、本人同意や個人情報保護条例に従った適切な管理の下、一部のデータを活用することは可能である。

④ 多要素認証によるなりすまし防止

成績評価につながるなど、本人確認を厳格に行う必要がある場合においては児童生徒の ID・パスワードに加えて多要素認証を設定することが望ましい。

⑤ 学習用ツールのシングルサインオン

学習履歴を活用したり、個人の成果物を保存するアプリケーションが増えてくると、サービス利用時に都度 ID・パスワード等の認証情報を入力したり、サービス毎のアカウント情報管理が非常に煩雑になるため、一度の認証により一定時間は各種サービスにアクセスが行えるシングルサインオンの導入を行うことが望ましい。

15 点検・評価及び見直し

（1） 点検・評価

① 教育情報セキュリティ管理者は、所管するシステム及びネットワークに係る実施手順に基づき必要な情報セキュリティ対策が実際に実施されているかどうか、ま

た、実施手順に記載された情報セキュリティ対策に不足がないかどうかについて、定期的に点検を行わなければならない。外部委託事業者に委託している場合も、ポリシーの遵守について定期的に点検を行わなければならない。

② 教育情報セキュリティ管理者は、点検結果に基づき、必要な改善を行わなければならない。また、点検結果において、ポリシーの記載に疑義が生じたときは、直ちに、教育最高情報セキュリティ責任者に報告しなければならない。

③ 職員は、点検結果に基づき、自己の権限の範囲内で改善を図らなければならない。

④ 教育最高情報セキュリティ責任者は、教育情報セキュリティ管理者に対し、情報セキュリティ対策の検査、点検実施の要請、点検結果の報告を求めることができる。

⑤ 教育最高情報セキュリティ責任者は、実施手順に基づき必要な情報セキュリティ対策が実際に実施されているかどうか、また、実施手順に記載された情報セキュリティ対策に不足がないかどうかについて、定期的に点検を行うとともに、点検結果に基づき、必要な改善を行わなければならない。

（２） セキュリティ対策の見直し、変更

① 教育最高情報セキュリティ責任者は、情報セキュリティをめぐる情勢の変化及び情報セキュリティ検査の結果を踏まえ、適宜対策基準の実効性を評価し、必要があるときは見直し、変更を行わなければならない。

② 教育最高情報セキュリティ責任者は、対策基準の変更を行ったときは、速やかに教育情報セキュリティ管理者その他関係者に周知を行わなければならない。

③ 教育情報セキュリティ管理者は、所管するシステム及びネットワークについて、ポリシーの変更並びに情報セキュリティをめぐる情勢の変化等に伴い、適宜情報セキュリティ対策の見直しを行ない、必要があると認めるときは、当該システム及びネットワークの実施手順の変更を行わなければならない。

④ 教育最高情報セキュリティ責任者は、ネットワークについて、ポリシーの変更に伴う情報セキュリティ対策の見直しを行わなければならない。

15 対策基準等の取扱い

対策基準及び実施手順のうち、公にすることにより委員会の運営に重大な支障を及ぼすおそれのある情報については、非公開とする。

附 則

この対策基準は、平成 25 年４月１日より施行

（経過措置）

改正対策基準の施行時点において情報システムが機能的に要件を満たしていない場合はこの限りではない。ただし、当該情報システムは、システム更改時等に準拠しなければなら

ない。

附　則

　この対策基準は、平成 29 年４月１日より施行する。

附　則

　この対策基準は、令和元年７月１日より施行する。

附　則

　この改正対策基準は、令和４年６月１日より施行する。

（経過措置）

　改正対策基準の施行時点において情報システムが機能的に要件を満たしていない場合はこの限りではない。ただし、当該情報システムは、システム更改時等に準拠しなければならない。