京都市教育委員会
情報セキュリティ対策基準

令和８年６月改正

目次

1　目的 1

2　適用範囲等 1

(1)　用語 1
(2)　適用範囲 1
(3)　情報資産の範囲 1

3　組織体制 2

(1)　最高情報セキュリティ責任者 2
(2)　情報セキュリティ統括者 2
(3)　情報セキュリティ管理責任者 2
(4)　情報システム管理者 2
(5)　情報セキュリティ管理者 3
(6)　情報セキュリティ対策支援員 3
(7)　緊急時即応体制 3
(8)　申請者、承認者等の区別 3

4　情報セキュリティ運用手順 3

(1)　情報セキュリティ共通運用手順の策定 3
(2)　情報セキュリティ運用手順の策定 4

5　情報資産の分類と管理方法 4

(1)　情報資産の分類 4
(2)　情報資産の管理 4

6　物理的セキュリティ対策 7

(1)　サーバ等の管理 7
(2)　情報システム室等の管理 8
(3)　通信経路の分離 9
(4)　通信回線及び通信回線装置の管理 10
(5)　職員のパソコン、モバイル端末、記録媒体等の管理 10
(6)　小型大容量記録媒体の使用等の制限 10

7　人的セキュリティ対策 12
(1)　職員の遵守事項 12
(2)　研修・訓練 14
(3)　ＩＤ、パスワード等の管理 14
(4)　情報セキュリティ対策基準等の遵守状況の確認 16
(5)　違反時の対応等 16
(6)　情報セキュリティインシデントの報告 17
(7)　侵害時の対応等 17
(8)　職員以外の者による情報システムの利用 18
(9)　例外措置 18
8　技術的セキュリティ対策 19
(1)　情報システムの管理 19
(2)　アクセス制御 23
(3)　情報システムの開発、導入、保守等 25
(4)　不正プログラム対策 27
(5)　不正アクセス対策 29
(6)　情報システムの監視 30
(7)　セキュリティ情報の収集 30
9　業務委託と外部サービスの利用 30
(1)　業務委託 30
(2)　外部サービス（クラウドサービス※・約款による外部サービス※を含む。）の利用 32
(3)　外部サービス利用の特則 33
(4)　ソーシャルメディア※サービスの利用 37
(5)　Web 会議サービスの利用 37
10　評価・見直し 37
(1)　監査 37
(2)　自主点検 38
(3)　情報セキュリティ対策基準の見直し 38

1　目的

京都市教育委員会情報セキュリティ対策基準は、京都市教育委員会高度情報化推進のための情報システムの適正な利用等に関する規程（以下「規程」という。）第１４条の規定に基づき策定するもので、教育委員会事務局等の情報資産における情報セキュリティを確保するための遵守事項及び判断基準を定めることにより、適切な情報セキュリティ水準を維持することを目的とする。

2　適用範囲等

⑴　用語

本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。

⑵　適用範囲

本対策基準が適用される範囲は、規程第２条第６号に規定する課等とする。

なお、本対策基準における職員には、非常勤嘱託員、会計年度任用職員、臨時的任用職員並びに情報システム管理者の許可を受けて教育委員会事務局等の情報システムを利用する市長部局等の職員（非常勤嘱託員、会計年度任用職員及び臨時的任用職員を含む。）及び委託事業者を含む。

⑶　情報資産の範囲

本対策基準が対象とする情報資産は、規程第２条第４号に規定する情報資産とする。

情報資産の種類		情報資産の例
情報システム	電子計算機	・サーバ、パソコン、モバイル端末等
	ソフトウェア	・オペレーティングシステム、アプリケーションソフトウェア等
	記録媒体	・サーバ、パソコン等の内蔵記録媒体 ・外付型ハードディスク又は外付型ＳＳＤ、ＤＶＤ、磁気テープ等の外部記録媒体 ・小型大容量記録媒体※1等
	ネットワーク	・通信回線、ルータ等の通信回線装置等
電子情報		・情報システムで利用される電磁的情報
入出力帳票		・情報システムに入力するための届出票、情報システムの出力帳票等
情報システムに係る設計書、仕様書その他情報システムの企画、調達、開発、運用、管理及び評価を行うために必要な資料		・システム設計書、プログラム仕様書、ネットワーク構成図、オペレーションマニュアル、端末管理マニュアル等

※1　「小型大容量記録媒体」とは、次に掲げる記録媒体をいう。

⑴　ＵＳＢメモリ、ＳＤメモリカード、メモリースティック、コンパクトフラッシュ等のフラッシュメモリ

⑵　マイクロドライブなどの小型ハードディスク又は小型ＳＳＤ

⑶　その他情報セキュリティ統括者が指定した記録媒体

3　組織体制

適切に情報セキュリティ対策を推進・管理するための体制、役割について以下のとおり定める。

⑴　最高情報セキュリティ責任者

最高情報セキュリティ責任者（以下「ＣＩＳＯ」※2という。）は、教育委員会事務局等における全て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。

⑵　情報セキュリティ統括者

ア　情報セキュリティ統括者は、ＣＩＳＯを補佐しなければならない。

イ　情報セキュリティ統括者は、教育委員会事務局等の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

ウ　情報セキュリティ統括者は、教育委員会事務局等の全てのネットワークにおける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。

エ　情報セキュリティ統括者は、情報セキュリティ管理責任者、情報システム管理者、情報セキュリティ管理者に対して、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。

オ　情報セキュリティ統括者は、教育委員会事務局等の情報資産に対する漏えい、改ざん、滅失、毀損その他の事故（以下「セキュリティ侵害」という。）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。

カ　情報セキュリティ統括者は、緊急時等の円滑な情報共有を図るため、ＣＩＳＯ、情報セキュリティ統括者、情報セキュリティ管理責任者、情報システム管理者、情報セキュリティ管理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。

キ　情報セキュリティ統括者は、緊急時にはＣＩＳＯに早急に報告を行うとともに、復旧のための対策を講じなければならない。

⑶　情報セキュリティ管理責任者

情報セキュリティ管理責任者は、情報セキュリティ統括者を補佐し、その実務を担当する。

⑷　情報システム管理者

ア　情報システム管理者は、所管する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。

イ　情報システム管理者は、所管する情報システム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。

ウ　情報システム管理者は、所管する情報システムに係る情報セキュリティ運用手順を策定し、その維持及び管理を行う。

エ　情報システム管理者は、所管する情報システムにおいて、情報資産に対するセキュリティ侵害が

※2　「ＣＩＳＯ」とは、「Chief Information Security Officer」の略称である。

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、情報セキュリティ管理責任者へ直ちに報告を行い、指示を仰がなければならない。

⑸ 情報セキュリティ管理者

ア　情報セキュリティ管理者は、所管する課等内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。

イ　情報セキュリティ管理者は、所管する課等内における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、情報セキュリティ管理責任者へ直ちに報告を行い、指示を仰がなければならない。

⑹ 情報セキュリティ対策支援員

情報セキュリティ対策支援員は、所属する課等において、次に掲げる事項を取り扱う。

ア　情報セキュリティ管理者の補佐

イ　情報システムの導入及び運用に係る諸制度の職員への周知及び運用

ウ　情報化及び情報セキュリティ対策に関する教育委員会事務局総務部総務課及び学校事務支援室との連絡調整

⑺ 緊急時即応体制

ア　緊急時即応体制（以下「ＣＳＩＲＴ※3」という。）は、情報セキュリティインシデント※4について報告を受けた場合には、その状況を確認し、必要がある場合は、直ちにＣＩＳＯに報告しなければならない。

イ　ＣＳＩＲＴは、情報セキュリティインシデントを認知した場合には、その重要度、影響範囲等を勘案し、関係機関への通知・公表対応を行わなければならない。

ウ　ＣＳＩＲＴは、情報セキュリティに関して、関係部局及び事業者等との情報共有を行う。

⑻ 申請者、承認者等の区別

ア　承認又は許可の申請を行う者とその承認又は許可を行う者とは、やむを得ない場合を除き、異なる者でなければならない。

イ　監査を受ける者とその監査を行う者とは、やむを得ない場合を除き、異なる者でなければならない。

4　情報セキュリティ運用手順

⑴ 情報セキュリティ共通運用手順の策定

情報セキュリティ統括者は、本対策基準を遵守し、情報セキュリティを確保するため、全ての情報

※3　「ＣＳＩＲＴ」とは、「Computer Security Incident Response Team」の略称である。

※4　「情報セキュリティインシデント」とは、本市の教育行政、学校事務又は教育活動の遂行に影響を与えたり、情報セキュリティを脅かしたりする事件又は事故をいう。

システムにおいて共通的な手順、手続等を明記した「京都市教育委員会情報セキュリティ共通運用手順」（以下「共通運用手順」という。）を策定するものとする。

⑵　情報セキュリティ運用手順の策定

情報システム管理者は、所管する情報システムにおいて、本対策基準を遵守し、情報セキュリティを確保するため、共通運用手順により示される手順、手続等以外に、情報システムを安全に運用するために個別に必要となる具体的な手順、手続等を明記した情報セキュリティ運用手順を策定しなければならない。

5　情報資産の分類と管理方法

⑴　情報資産の分類

電子情報及び入出力帳票（以下「電子情報等」という。）は、重要性が高位のものから順に、次のとおり重要性Ⅰ、重要性Ⅱ、重要性Ⅲ及び重要性Ⅳに分類し、適切に管理するものとする。また、電子計算機等の情報資産は、取り扱う電子情報等の重要性に基づき分類するものとし、重要性が異なる複数の電子情報等を取り扱う場合は、最高位の重要性の分類に基づくものとする。

なお、本市の主な情報資産とその分類の一覧表を別表のとおり例示するので、分類に当たって必要に応じ参照すること。ただし、同種の情報資産でも取り扱う状況に応じて重要性が異なる可能性があることに留意すること。

ア　重要性Ⅰ

セキュリティ侵害が市民、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情報

イ　重要性Ⅱ

セキュリティ侵害が教育行政、学校事務又は教育活動の実施に重大な影響を及ぼす情報。ただし、重要性Ⅰに該当する情報を除く。

ウ　重要性Ⅲ

セキュリティ侵害が教育行政、学校事務又は教育活動の実施に軽微な影響を及ぼす情報。ただし、重要性Ⅱ以上に該当する情報を除く。

エ　重要性Ⅳ

セキュリティ侵害が教育行政、学校事務又は教育活動の実施に影響をほとんど及ぼさない情報。ただし、重要性Ⅲ以上に該当する情報を除く。

⑵　情報資産の管理

ア　管理責任

(ｱ) 情報セキュリティ管理者及び情報システム管理者は、所管する情報資産を重要性の分類に基づき、管理しなければならない。情報資産が複製又は伝送された場合も同様とする。

(ｲ) 情報セキュリティ管理者は、所管する課等における情報資産のうち、電子計算機、記録媒体等の物理的な情報資産について、その保管場所、数量、重要性の分類等を情報資産管理簿により管理しなければならない。ただし、重要性Ⅳの電子情報のみを保存した情報資産については、情報

資産管理簿による管理を不要とする。

(ｳ) 情報システム管理者は、課等における情報資産を適切に管理することが可能な場合は、情報セキュリティ管理者に代わり、情報資産管理簿による管理を行うことができる。

イ　電子情報等の作成

(ｱ) 情報セキュリティ管理者及び情報システム管理者は、電子情報等の作成時に、重要性の分類に基づき、当該電子情報等の重要性を定めなければならない。

(ｲ) 職員は、業務上必要のない電子情報等を作成してはならない。

(ｳ) 職員は、作成中の電子情報等についても、紛失、流出等を防止しなければならない。また、作成中に不要になった場合は、当該電子情報等を適切に消去しなければならない。

ウ　情報資産の入手

(ｱ) 情報セキュリティ管理者及び情報システム管理者は、他の課等において作成された情報資産を入手した場合は、入手元の重要性の分類に基づき、当該情報資産の重要性を定めなければならない。

(ｲ) 情報セキュリティ管理者及び情報システム管理者は、職員以外の者が作成した情報資産を入手した場合は、重要性の分類に基づき、当該情報資産の重要性を定めなければならない。

エ　情報資産の利用

(ｱ) 職員は、業務以外の目的に情報資産を利用してはならない。

(ｲ) 職員は、重要性の分類に基づき、情報資産を適切に取り扱わなければならない。

(ｳ) 情報セキュリティ管理者及び情報システム管理者は、他の業務目的で収集された電子情報等を利用する場合は、あらかじめ、当該電子情報等を管理する情報セキュリティ管理者又は情報システム管理者の承認を得なければならない。ただし、重要性Ⅳの電子情報等を利用する場合は承認を不要とする。

オ　情報資産の保管

(ｱ) 情報セキュリティ管理者及び情報システム管理者は、重要性の分類に基づき、情報資産を適切に保管しなければならない。

(ｲ) 情報セキュリティ管理者及び情報システム管理者は、電子情報を記録した記録媒体を保管する場合は、記録された電子情報の滅失、毀損その他の事故が生じないよう適切な措置を講じなければならない。

(ｳ) 情報セキュリティ管理者及び情報システム管理者は、耐火、耐熱、耐水及び耐湿対策を講じたうえ施錠可能な場所に保管するなど、記録媒体を適切に管理しなければならない。

(ｴ) 情報システム管理者は、情報システムのバックアップにより作成した記録媒体を保管する場合は、情報システムと同時に被災しないよう遠隔地に保管するなど、業務継続のための措置を検討しなければならない。

カ　電子情報の送信

(ｱ) 職員は、業務上必要な場合を除き、電子情報を、電子メール等を利用して本市職員以外の者又は本市が所管していない電子計算機に送信してはならない。

(ｲ) 職員は、重要性Ⅰの電子情報を、電子メール等を利用して本市職員以外の者又は本市が所管していない電子計算機に送信してはならない。ただし、次に掲げる事由（以下「情報資産管理にお

ける許可事由」という。）に該当し、情報セキュリティ管理者が許可したときを除く。

a　国の行政機関等から資料等の提供を求められている場合

b　庁外※5において、交渉、協議、相談、催促、会議等に用いる場合

c　秘密保持に係る定めを取り交わしている相手方に対し、提示又は提供する場合

d　その他、情報セキュリティ統括者が承認した場合

(ｳ) 職員は、前項ただし書の許可を得て、重要性Ⅰの電子情報を送信する場合は、パスワード、暗号化等による情報保護対策（以下「情報保護対策」という。）を行わなければならない。ただし、送信経路又は送信先における情報システム上の制約により情報保護対策ができない場合等、特段の事情がある場合を除く。

キ　情報資産の提供

(ｱ) 職員は、業務上必要な場合を除き、情報資産を本市職員以外の者に提供してはならない。

(ｲ) 職員は、重要性Ⅰの情報資産を本市職員以外の者に提供してはならない。ただし、情報資産管理における許可事由に該当し、情報セキュリティ管理者が許可したときを除く。

(ｳ) 職員は、前項ただし書の許可を得て、重要性Ⅰの情報資産を提供する場合は、情報保護対策を行わなければならない。

ク　情報資産の運搬

(ｱ) 職員は、情報資産を運搬する場合は、必要に応じ鍵付きのケース等に格納し、情報保護対策を行う等、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。

(ｲ) 職員が郵送、文書交換、自動車等の交通手段により輸送するときは、郵送中又は輸送中の情報の漏えい、破損等を防止するため、電子情報等を物理的に保護するための適切な措置を講じなければならない。

ケ　情報資産の廃棄

(ｱ) 職員は、記録媒体が不要になった場合（リース期間満了等により処分する場合を含む。）は、情報セキュリティ管理者の承認を得たうえで廃棄し、廃棄処理を行った日時、担当者及び処理内容を記録しなければならない。

(ｲ) 職員は、記録媒体を廃棄するときは、裁断、溶解等による物理的又は電磁的破壊、専用のソフトウェア等を用いたデータ消去、ブロック消去、暗号化消去等の方法により、当該記録媒体に記録されている電子情報を復元できないよう処置したうえで廃棄しなければならない。特に、個人番号利用事務系（個人番号利用事務又は戸籍事務に関わる情報システムをいう。以下同じ。）の電子情報が保存された記録媒体を廃棄する場合は、原則として、物理的に破壊する方法により行わなければならない。

(ｳ) 職員は、記録媒体の廃棄処理を委託等により事業者に行わせる場合は、廃棄処理を行った日時、担当者及び処理内容を記録した証明書等を事業者に提出させなければならない。また、電子情報が復元できないように処置されるまで立会いを行うなど、盗難、紛失等による情報漏えいがないように、確実な履行を担保しなければならない。特に、個人番号利用事務系の電子情報が保

※5　「庁外」とは、本市が所管する施設以外をいう。

存された記録媒体の廃棄処理を委託等により事業者に行わせる場合は、前項に示した廃棄方法のうち、いずれかの方法により、庁内において情報の復元が困難な状態までデータの消去を行ったうえで事業者に引き渡しを行い、物理的破壊の証明書等（原則として、提出期限を定めたうえで、破壊の証拠写真の添付を求めること）により、適切な措置が講じられているか確認しなければならない。

(ｴ) 職員は、重要性Ⅰの情報が記録された入出力帳票を廃棄するときは、秘密文書回収、焼却、裁断、溶解等により廃棄しなければならない。

コ　私物機器による情報資産の取扱いの制限

(ｱ) 職員は、個人が所有するパソコン、モバイル端末、記録媒体等（以下「私物機器」という。）を使用して、本市の情報資産の作成、編集、保存、送受信その他の取扱いをしてはならない。ただし、業務上必要な場合であって、次の事由に該当するときを除く。

a　電子メール等により職員等への事務連絡を行うとき。

b　緊急時において証拠保全等を目的とした情報の記録を行うとき。

c　教育委員会事務局等のネットワークへ接続を行わない場合で情報セキュリティ管理者の許可を得たとき。

d　情報システムを利用するための認証手段として情報システム管理者が認めるとき。

e　その他情報セキュリティ統括者が認めるとき。

(ｲ) 職員は、前項ただし書の規定により私物機器を使用して本市の情報資産を取り扱う場合には、次の事項を遵守しなければならない。

a　私物機器で重要性Ⅱ以上の電子情報等（事務連絡に必要となる職員等の連絡先を除く。）を取り扱ってはならない。ただし、情報セキュリティ統括者が許可した場合又は情報セキュリティ管理者が業務の遂行に当たり緊急かつやむを得ないと認める場合を除く。

b　私物機器に対し、パスワード等による端末のロック、不正プログラム対策、ハードウェア及びソフトウェアに係る脆弱性への対応を行うとともに、情報セキュリティ管理者の指導に従い、情報セキュリティの確保に努めなければならない。

c　私物機器に保存した電子情報を、第三者に使用又は閲覧されないよう適切に管理するとともに、業務の遂行に当たり必要なくなったときは、直ちに削除しなければならない。

(ｳ) 情報セキュリティ管理者は、職員が私物機器を使用して情報資産を取り扱う場合には、取り扱う電子情報等の重要性に応じて本市が所管する情報システムに準じた情報セキュリティが確保されるよう、職員を指導しなければならない。

6　物理的セキュリティ対策

(1)　サーバ等の管理

ア　機器の設置

情報システム管理者は、サーバ等の機器を設置する場合は、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施錠可能な区画内に設置し、容易に取り外せないよう適切に固定する等、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

情報システム管理者は、サーバ等の機器が停止することで、本市の教育行政、学校事務又は教育活動の安定的な遂行に支障を及ぼすおそれがある場合は、サーバ等の機器を冗長化しなければならない。

ウ　機器の電源

(ｱ) 情報システム管理者は、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間、十分な電力を供給できるよう予備電源を備え付けなければならない。

(ｲ) 情報システム管理者は、落雷等による過電流に対して、サーバ等の機器を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) 情報システム管理者は、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等、必要な措置を講じなければならない。

(ｲ) 情報システム管理者は、通信ケーブル及び電源ケーブルについて、損傷等の報告があった場合、速やかに対応しなければならない。

(ｳ) 情報システム管理者は、ネットワークの接続口（ハブのポート等）を他人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。

(ｴ) 情報システム管理者は、操作を認められた職員又は委託事業者以外が配線を変更、追加できないよう必要な措置を講じなければならない。

オ　機器の保守及び修理

(ｱ) 情報システム管理者は、サーバ等の機器について、取り扱う電子情報等の重要性、サーバ等の機器が故障した場合の業務への影響等を勘案し、適切に保守を実施しなければならない。

(ｲ) 情報システム管理者は、記録媒体が内蔵された機器を委託事業者に修理させる場合は、あらかじめ記録された電子情報を消去したうえで行わせなければならない。電子情報を消去できない場合は、委託事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認などを行わなければならない。

カ　庁外への機器の設置

(ｱ) 情報システム管理者は、庁外にサーバ等の機器を設置する場合は、情報セキュリティ統括者の承認を得なければならない。

(ｲ) 情報セキュリティ統括者は、当該施設が本対策基準に定める内容と同等の情報セキュリティが確保されていることを確認したうえで、承認を与えることができる。

(ｳ) 情報システム管理者は、承認を得た施設について、必要な情報セキュリティが継続して確保されていることを定期的に確認しなければならない。

キ　機器の処分

情報システム管理者は、廃棄、返却等機器を処分する場合は、機器に内蔵された記録媒体から全ての電子情報を消去のうえ、復元できないよう必要な措置を講じなければならない。

(2) 情報システム室等の管理

情報システム管理者は、重要性Ⅰの電子情報が記録された記録媒体及び入出力帳票の保管場所並

びにそれを取り扱うサーバ、パソコン等の設置場所について、適切に入退室管理を行わなければならない。

特に、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、当該機器等の管理及び運用を行うための区画（以下「情報システム室」という。）については、次の事項に従い適切に管理しなければならない。

ア　情報システム室の構造等

(ｱ) 情報システム管理者は、外部から容易に侵入できない場所に情報システム室を配置しなければならない。

(ｲ) 情報システム管理者は、情報システム室から外部に通ずる出入口は必要最小限とし、鍵、監視機能、警報装置等によって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。

(ｳ) 情報システム管理者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

(ｴ) 情報システム管理者は、情報システム室に配置する消火薬剤、消防用設備等が、機器、記録媒体等に影響を与えないようにしなければならない。

イ　情報システム室の入退室管理等

(ｱ) 情報システム管理者は、情報システム室への入退室を許可された者のみに制限し、ＩＤカード、生体認証等による認証又は入退室管理簿の記載による入退室管理を行わなければならない。

(ｲ) 職員及び委託事業者は、情報システム室に入室する場合、入室証又は名札を着用するとともに、身分証明書等を携帯し、求めに応じて提示しなければならない。

(ｳ) 情報システム室に入室する者は、当該情報システムに関連しないパソコン、モバイル端末、通信回線装置、記録媒体その他電子情報等を外部へ持ち出すことができる機器を持ち込んではならない。ただし、情報システム管理者が許可したときを除く。

ウ　機器等の搬入出

情報システム管理者は、情報システム室の機器等を搬入出する場合は、職員を立ち会わせなければならない。

⑶　通信経路の分離

ア　個人番号利用事務系は、ＬＧＷＡＮ接続系（総合行政ネットワーク（以下「ＬＧＷＡＮ」という。）に接続された情報システムをいう。以下同じ。）及びインターネット接続系（インターネットに接続された情報システムをいう。以下同じ。）と通信経路を分離したうえで、他の情報システムと通信できないようにしなければならない。ただし、情報セキュリティ統括者の許可を得た場合は、十分に安全性が確保された外部接続先に限り、ＬＧＷＡＮを経由して、インターネット接続系にある国等の公的機関が構築したシステム等と個人番号利用事務系との双方向通信でのデータ移送をすることができる。この場合、通信経路及びアプリケーションプロトコルの制限並びに個人番号利用事務系のサーバ・端末のウイルス対策ソフトの導入及び最新の定義ファイルの常時更新並びにＯＳの修正プログラムの常時更新をしなければならない。

イ　ＬＧＷＡＮ接続系とインターネット接続系は、通信経路を分離したうえで、相互の通信は必要最小限に限定するとともに、インターネット接続系からＬＧＷＡＮ接続系に電子情報を伝送すると

きは、ウイルス等を自動的に削除する無害化処理を実施しなければならない。

⑷ 通信回線及び通信回線装置の管理

ア　情報セキュリティ統括者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

イ　情報セキュリティ統括者は、国等のネットワークに接続する場合は、ＬＧＷＡＮに集約するように努めなければならない。

ウ　情報システム管理者は、所管するネットワークに係る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、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

エ　情報システム管理者は、ネットワークで使用する回線について、伝送中に電子情報の破壊、盗聴、改ざん、消去等が生じないよう通信経路の暗号化等、必要な措置を講じなければならない。また、必要に応じ、送受信される電子情報の暗号化を行わなければならない。

オ　情報システム管理者は、情報システムに通信回線を接続する場合は、取り扱う電子情報の重要性、送受信される電子情報の容量等を勘案し、専用回線等、適切な回線を選択しなければならない。

カ　情報システム管理者は、情報システムに接続する通信回線について、当該通信回線が停止した場合の業務への影響等を勘案し、通信回線及び通信回線装置を冗長構成にする等、情報システムを安定的に運用するための措置を講じなければならない。

⑸ 職員のパソコン、モバイル端末、記録媒体等の管理

ア　情報セキュリティ管理者及び情報システム管理者は、パソコン、モバイル端末、記録媒体等の盗難に伴う電子情報の漏えいを防止するため、取り扱う電子情報の重要性に応じた情報セキュリティ対策を講じなければならない。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　情報セキュリティ管理者及び情報システム管理者は、職員にパソコン、モバイル端末等を利用させる場合は、ログインパスワード※6等の認証情報の入力を必要とするよう設定しなければならない。

ウ　情報システム管理者は、取り扱う電子情報等の重要性に応じて、多要素認証（記憶、所有物、生体情報等の要素を複数併用する認証方法をいう。以下同じ。）を導入しなければならない。特に、個人番号利用事務系においては、必ず多要素認証を導入しなければならない。

⑹ 小型大容量記録媒体の使用等の制限

ア　使用等の制限

職員は、業務を遂行するに当たり、小型大容量記録媒体並びに小型大容量記録媒体の使用に必要なカードリーダー及びカードアダプタ（以下「小型大容量記録媒体等」という。）を使用又は購入

※6　「ログインパスワード」とは、オペレーティングシステム、ソフトウェア等にログインする際に使用するパスワードをいう。

してはならない。ただし、撮影又は録音した電子情報を記録するため、あらかじめ撮影機器又は録音機器に付属しているものを除く。

イ　使用等の許可

(ｱ) 情報セキュリティ管理者は、前項の規定にかかわらず、次のいずれかに該当する場合に限り、情報セキュリティ統括者の許可を得て、小型大容量記録媒体等を職員に使用させ、又は購入することができる。

a　撮影機器又は録音機器で撮影又は録音した電子情報を記録するための小型大容量記録媒体があらかじめこれらの機器に付属していないとき。

b　撮影機器又は録音機器で撮影又は録音した電子情報を記録するための小型大容量記録媒体の記録容量が不足しているとき。

c　撮影機器又は録音機器で撮影又は録音した電子情報を記録するための小型大容量記録媒体が毀損したとき。

d　使用する機器が備える構造などの制約により、小型大容量記録媒体等しか使用できないとき。

e　前４項のほか、情報セキュリティ統括者が特段の事情があると認めるとき。

(ｲ) 情報セキュリティ統括者は、小型大容量記録媒体の使用又は購入を許可する場合は、使用する機器１台に対して、必要最小限度の記録容量を持つもの１個に限定しなければならない。ただし、情報セキュリティ統括者が特段の事情があると認めるときを除く。

ウ　使用及び管理

職員は、前項の許可を得て小型大容量記録媒体等を使用する場合は、次の事項を遵守しなければならない。

(ｱ) 小型大容量記録媒体の紛失及び他の用途への転用を防ぐため、その記録媒体を使用する機器から取り外してはならない。

(ｲ) 情報の漏えい、滅失、毀損その他の事故を防ぐため、業務を完了した後、直ちに小型大容量記録媒体に記録した電子情報をその保存が認められた電子計算機又はその他の記録媒体に記録し、当該記録媒体からは電子情報を消去しなければならない。

(ｳ) 小型大容量記録媒体に記録した電子情報をその保存が認められた電子計算機又はその他の記録媒体に保存する場合において、報告機器が備える構造などの制約により、その機器から取り外す方法しか手段がないときは、取り外して使用することができる。ただし、使用を終えた後、直ちに取り外した小型大容量記録媒体を報告機器に格納しなければならない。

エ　引継ぎ

(ｱ) 情報セキュリティ管理者は、小型大容量記録媒体等が不要になった場合は、情報セキュリティ統括者に引き継がなければならない。

(ｲ) 情報セキュリティ統括者は、引き継いだ小型大容量記録媒体等を適正に管理し、必要に応じて他の所属に引き継ぐなど、有効活用を図るものとする。

7　人的セキュリティ対策

⑴　職員の遵守事項

ア　法令遵守

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

(ｱ) 地方公務員法（昭和２５年法律第２６１号）

(ｲ) 教育公務員特例法（昭和２４年法律第１号）

(ｳ) 著作権法（昭和４５年法律第４８号）

(ｴ) 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）

(ｵ) 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）

(ｶ) サイバーセキュリティ基本法（平成２６年法律第１０４号）

(ｷ) 個人情報の保護に関する法律（平成１５年法律第５７号）

(ｸ) 京都市個人情報保護条例（令和４年条例第２６号）

(ｹ) 京都市情報公開条例（平成３年条例第１２号）

(ｺ) 京都市教育委員会事務局公文書取扱規程（平成３年教育委員会教育長訓令甲第２号）

(ｻ) 京都市立学校幼稚園文書取扱規程（昭和３０年教育委教育長訓令甲第６号）

(ｼ) 京都市教育委員会高度情報化推進のための情報システムの適正な利用等に関する規程（平成２３年教育委員会教育長訓令甲第２号）

イ　情報セキュリティ対策基準等の遵守

(ｱ) 情報セキュリティ管理者は、職員に対し、本対策基準、共通運用手順及び所管業務で使用する情報システムに係る情報セキュリティ運用手順（以下「対策基準等」という。）について、職員が守るべき内容を理解させ、また遵守させなければならない。

(ｲ) 情報セキュリティ管理者は、職員が常に対策基準等を参照できるようにしなければならない。

(ｳ) 職員は、対策基準等の内容を理解し、遵守しなければならない。

ウ　業務以外の目的での使用の禁止

職員は、業務以外の目的で情報資産の庁外への持出し、情報システムへのアクセス、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。

エ　庁外への電子情報等の持出しの制限

(ｱ) 職員は、電子情報等を庁外に持ち出す場合は、情報セキュリティ管理者の許可を得るとともに、情報セキュリティ管理者の指示に従い、セキュリティ侵害が生じないよう適切に管理しなければならない。ただし、職員が業務において本庁、教育機関及び学校等の本市が所管する施設間を移動する場合及び文書交換を利用して輸送する場合は、庁外への持出しには当たらない。

(ｲ) 職員は、重要性Ⅰの電子情報等を庁外に持ち出してはならない。ただし、情報資産管理における許可事由に該当し、情報セキュリティ管理者が許可したときを除く。

(ｳ) 情報セキュリティ管理者は、職員以外の者が電子情報等を庁外に持ち出す場合は、セキュリティ侵害が生じないよう、これを適切に監督又は指導しなければならない。

オ　庁外へのパソコン、モバイル端末等の持出し許可及び制限

(ｱ) 情報システム管理者は、職員によるパソコン、モバイル端末等の庁外への持出しが業務上必要な場合は、あらかじめセキュリティ侵害が生じないよう使用方法及び手続に関する手順を定めなければならない。ただし、職員が業務において本庁、教育機関及び学校等の本市が所管する施設間を移動する場合は庁外への持出しには当たらない。

(ｲ) 情報セキュリティ管理者は、職員以外の者がパソコン、モバイル端末等を庁外に持ち出す場合は、別に定める規定によらなければならない。ただし、職員以外の者が職員の監督下にある場合は庁外への持出しには当たらない。

(ｳ) 情報セキュリティ管理者は、課等で管理するパソコン、モバイル端末等の持出しの状況を把握しなければならない。

(ｴ) 職員は、パソコン、モバイル端末等を庁外に持ち出す場合は、情報セキュリティ管理者の許可を得るとともに、情報システム管理者が(ｱ)で定めた手順を遵守しなければならない。

(ｵ) 職員は、庁外に持ち出したパソコン、モバイル端末等を教育委員会事務局等のネットワークに接続する場合は、あらかじめ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。

(ｶ) 情報セキュリティ管理者は、職員以外の者が庁外に持ち出したパソコン、モバイル端末等を教育委員会事務局等のネットワークに接続する場合は、あらかじめ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。

カ　私物機器の接続の制限

(ｱ) 職員は、私物機器を教育委員会事務局等の情報システムに接続してはならない。ただし、インターネット等の外部ネットワークから接続が可能な情報システムへの接続であって、情報セキュリティ統括者が許可した場合を除く。

(ｲ) 情報システム管理者は、(ｱ)ただし書以外の場合で私物機器を教育委員会事務局等の情報システムに接続する必要がある場合は、8(1)キ(ｱ)に規定する情報セキュリティ統括者の承認をあらかじめ得なければならない。

キ　パソコン、モバイル端末等のセキュリティ機能の設定変更の禁止

職員は、パソコン、モバイル端末等について、ソフトウェアに関するセキュリティ機能の設定を変更してはならない。ただし、情報システム管理者が許可したときを除く。

ク　電子情報等の管理

職員は、パソコン、モバイル端末、記録媒体及び入出力帳票について、第三者に使用又は閲覧されないよう、次のとおり適切に管理しなければならない。

(ｱ) 離席するときは、パソコンをユーザーロックしなければならない。

(ｲ) 離席するときは、モバイル端末並びに重要性Ⅰの電子情報が記録された記録媒体及び入出力帳票を机上に放置してはならない。

(ｳ) モバイル端末並びに重要性Ⅰの電子情報が記録された記録媒体及び入出力帳票を使用しないときは、施錠可能な場所に保管しなければならない。

(ｴ) 職員以外の者が周囲にいる状況で、重要性Ⅱ以上の電子情報をパソコン若しくはモバイル端末又は大型掲示装置等の映像出力機器に表示してはならない。

ケ　退職時等の取扱い

職員は、異動、出向、退職その他の理由により、情報資産を利用する必要がなくなった場合は、速やかに当該情報資産を返却しなければならない。

コ　非常勤嘱託員、会計年度任用職員、臨時的任用職員等への対応

情報セキュリティ管理者は、次の職員に情報システムを利用させる場合は、対策基準等及び関係法令を理解させるとともに、これらを遵守する旨の誓約書を提出させなければならない。

(ｱ) 非常勤嘱託員

(ｲ) 会計年度任用職員

(ｳ) 臨時的任用職員

(ｴ) 情報システム管理者の許可を受けて、情報システムを利用する市長部局等の職員（非常勤嘱託員、会計年度任用職員及び臨時的任用職員を含む。）

(ｵ) 委託事業者

サ　委託事業者に対する説明

情報システム管理者は、情報システムの開発、保守等を委託事業者に発注する場合は、委託契約書又は仕様書に本対策基準の遵守に関する事項を明記するとともに、再委託事業者も含めて、委託事業者が守るべき内容について説明しなければならない。

⑵　研修・訓練

ア　情報セキュリティに関する研修

(ｱ) 情報セキュリティ統括者は、職員に対する情報セキュリティに関する研修計画を定期的に策定しなければならない。

(ｲ) 情報セキュリティ統括者は、研修計画に基づき、情報セキュリティに関する研修・訓練を実施しなければならない。

(ｳ) 情報セキュリティ統括者は、毎年度１回、ＣＩＳＯに対して、職員の情報セキュリティ研修の実施状況について報告しなければならない。

イ　緊急時対応訓練

(ｱ) 情報セキュリティ統括者は、緊急時を想定した訓練を定期的に実施しなければならない。

(ｲ) 情報セキュリティ統括者は、訓練を効果的に実施できるよう、想定する情報システムの規模等を勘案し、訓練の内容を定めなければならない。

ウ　研修・訓練への参加

情報セキュリティ管理者及び情報システム管理者を含む全ての職員は、研修・訓練への参加を求められた場合は、情報セキュリティに関する意識を深め、情報セキュリティ上の問題が生じないようにするため、研修・訓練に参加しなければならない。

⑶　ＩＤ、パスワード等の管理

ア　ＩＤの取扱い

(ｱ) 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。

a　自己が利用しているＩＤを他人に利用させてはならない。ただし、課等ごとに発行され、あらかじめ共用が認められたＩＤ（以下「共用ＩＤ」という。）を除く。

b　自己のＩＤ及び共用ＩＤは、他人又は利用者以外に知らせてはならない。

c　ＩＤを不正利用された場合は、直ちに情報セキュリティ管理者及び情報システム管理者に報告するとともに、情報システム管理者の指示に従わなければならない。

(ｲ) 情報システム管理者は、所管する情報システムで利用するＩＤに関し、次の事項を遵守しなければならない。

a　原則として利用者ごとにＩＤを発行しなければならない。ただし、利用範囲を明確に定めたうえで、利用者ごとの操作履歴、閲覧履歴その他情報セキュリティの確保に必要な記録の取得等を行う場合は、共用ＩＤを発行することができる。

b　ＩＤの不正利用の通報を受けた場合は、当該ＩＤの利用を直ちに停止しなければならない。

イ　ＩＤカード等[※7]の取扱い

(ｱ) 職員は、自己の管理するＩＤカード等に関し、次の事項を遵守しなければならない。

a　ＩＤカード等を、職員間で共用してはならない。ただし、課等ごとに発行され、あらかじめ共用が認められたＩＤカード等（以下「共用ＩＤカード等」という。）を除く。

b　ＩＤカード等を使用しない場合は、ＩＤカード等をカードリーダー、パソコン等の端末のスロット等から取り外すとともに、施錠可能な場所に保管する等、紛失、盗難等を防止するための必要な措置を講じなければならない。

c　ＩＤカード等を紛失した場合は、直ちに情報セキュリティ管理者及び情報システム管理者に報告するとともに、情報システム管理者の指示に従わなければならない。

(ｲ) 情報セキュリティ管理者は、共用ＩＤカード等の発行を受けた場合は、情報システム管理者の指示するところにより、共用ＩＤカード等を管理し、及び使用の記録を行わなければならない。

(ｳ) 情報システム管理者は、所管する情報システムで使用するＩＤカード等に関し、次の事項を遵守しなければならない。

a　原則として利用者ごとにＩＤカード等を配付しなければならない。ただし、共用ＩＤを発行している場合は、必要に応じて共用ＩＤカード等を発行することができる。この場合は、共用ＩＤカード等の管理及び使用の記録に係る手順を定め、情報セキュリティ管理者に指示しなければならない。

b　ＩＤカード等の紛失等の通報を受けた場合は、当該ＩＤカード等の使用を直ちに停止しなければならない。

ウ　生体認証情報の取扱い

(ｱ) 職員は、自己の生体認証情報により他人に情報システムを利用させてはならない。

(ｲ) 情報システム管理者は、生体認証情報が不正に利用された場合は、当該生体認証情報による情報システムの利用を直ちに停止しなければならない。

エ　パスワードの取扱い

(ｱ) 職員は、自己の管理するパスワードを次のとおり適切に管理しなければならない。

a　パスワードは、他人に知られないよう管理し、パスワードの照会等には一切応じてはならな

※7 「ＩＤカード等」とは、ＩＤカード、ＵＳＢトークン等、情報システム管理者から配付された認証を行うための物理的な認証装置の総称。

い。

b　パスワードは十分な文字数とし、文字列は他人が容易に想像できないものにしなければならない。

c　パスワードが流出したおそれがある場合は、直ちに情報セキュリティ管理者に報告し、パスワードを変更しなければならない。

d　複数の情報システムを扱う職員は、同一のログインパスワードを情報システム間で用いてはならない。ただし、シングルサインオン※8等によりあらかじめ認証情報を一元的に管理することが認められている場合を除く。

e　仮のログインパスワード（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。

f　サーバ、ネットワーク機器及びパソコン等の端末にログインパスワードを記憶させてはならない。

g　パスワードを記載したメモを作成してはならない。やむを得ずメモを作成する場合は、他人に分からない場所に保管しなければならない。

h　職員間でパスワードを共用してはならない。ただし、共用ＩＤ等を利用する場合を除く。

⑷　情報セキュリティ対策基準等の遵守状況の確認

ア　遵守状況の確認及び対処

(ｱ) 情報セキュリティ管理者は、所管する課等内における本対策基準の遵守状況について常に確認を行い、問題を認めた場合は、直ちに情報セキュリティ管理責任者に報告しなければならない。

(ｲ) 情報システム管理者は、所管するネットワーク又はサーバ等の情報システムにおける本対策基準の遵守状況について、定期的に確認を行い、問題を認めた場合は、適切かつ速やかに対処しなければならない。

イ　パソコン、モバイル端末等の利用状況調査

情報セキュリティ統括者は、職員が利用するパソコン、モバイル端末等について、不正アクセス、不正プログラム等の調査又は適切な利用の確保のため、操作履歴及び閲覧履歴等のログ並びに電子メールにより送受信された電子情報を含む送受信記録等を調査することができる。

ウ　職員の報告義務

職員は、本対策基準に違反する行為を発見した場合は、直ちに情報セキュリティ管理者及び情報セキュリティ管理責任者に報告しなければならない。

⑸　違反時の対応等

ア　違反時の対応

職員が本対策基準に違反した場合は、速やかに次の措置を講じなければならない。

※8　「シングルサインオン」とは、一度の利用者認証で複数の情報システムを利用できるようにする仕組みをいう。

(ｱ) 情報セキュリティ管理責任者が違反を確認した場合は、当該職員が所属する課等の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。

(ｲ) 情報システム管理者が違反を確認した場合は、直ちに情報セキュリティ管理責任者及び当該職員が所属する課等の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。

(ｳ) 情報セキュリティ管理者が違反を確認した場合は、直ちに当該職員に対して指導を行い、是正するとともに、情報セキュリティ管理責任者に報告しなければならない。

(ｴ) 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、情報セキュリティ管理責任者は、当該職員のネットワーク又は情報システムを利用する権利の一部若しくは全部を停止又は剥奪することができる。その場合速やかに、情報セキュリティ管理責任者は、職員の権利の一部若しくは全部を停止又は剥奪した旨を情報セキュリティ統括者及び当該職員が所属する課等の情報セキュリティ管理者に通知しなければならない。

イ　懲戒処分

本対策基準に違反した職員は、その重大性、発生した事案の状況等に応じて、「京都市教育委員会職員の懲戒処分に関する指針」又は「京都市立学校幼稚園教職員の処分等に関する指針」に基づき、処分の対象とする。

⑹ 情報セキュリティインシデントの報告

ア　情報セキュリティインシデントの報告

(ｱ) 職員は、情報セキュリティインシデントを認知した場合は、直ちに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、情報セキュリティ管理者が不在のときは、直ちに情報セキュリティ管理責任者に報告するものとする。

(ｲ) 情報セキュリティ管理者は、職員から報告を受けた場合は、直ちに当該情報セキュリティインシデントに関連する情報システム管理者及び情報セキュリティ管理責任者に報告しなければならない。

(ｳ) 情報セキュリティ管理責任者は、報告のあった情報セキュリティインシデントについて、ＣＳＩＲＴとして対処し、必要に応じて、ＣＩＳＯに報告しなければならない。

イ　情報セキュリティインシデントの原因の究明・記録、再発防止等

(ｱ) ＣＳＩＲＴは、情報セキュリティインシデントを引き起こした課等の情報セキュリティ管理者及び情報システム管理者と連携し、情報セキュリティインシデントの原因を究明するとともに、行った対応について記録を保存しなければならない。また、情報セキュリティインシデントの原因究明結果から、再発防止策を検討し、ＣＩＳＯに報告しなければならない。

(ｲ) ＣＩＳＯは、ＣＳＩＲＴから情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

⑺ 侵害時の対応等

ア　緊急時対応計画の策定

情報セキュリティ統括者は、情報セキュリティインシデント、本対策基準の違反等により情報資

産に対するセキュリティ侵害が発生し、又は発生するおそれがある場合において、連絡、証拠保全、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、あらかじめ緊急時対応計画を定めるとともに、セキュリティ侵害時には当該計画に従って適切に対処しなければならない。

イ　緊急時対応計画に盛り込むべき内容

緊急時対応計画には、次の内容を定めなければならない。

(ｱ) 緊急時の対応方法

(ｲ) 緊急時の報告及び公表方法

(ｳ) 平常時の危機管理方法

(ｴ) その他情報セキュリティ統括者が必要と認める事項

ウ　緊急時対応計画の見直し

情報セキュリティ統括者は、情報セキュリティを取り巻く状況の変化、組織体制の変動等に応じ、緊急時対応計画を見直さなければならない。

エ　緊急時の対応手順等の作成

情報システム管理者は、緊急時に備えて対応手順並びに委託事業者を含む連絡体制及び緊急連絡網を作成したうえで、常に最新の状態に保つとともに、これを常備しなければならない。

⑻　職員以外の者による情報システムの利用

ア　職員以外の者が遵守すべき事項

情報システム管理者は、職員以外の者が情報システムを利用する際に遵守すべき事項を情報セキュリティ運用手順に定めなければならない。

イ　職員以外の者への指導

情報セキュリティ管理者は、アで定めた事項について、必要に応じて職員以外の者に指導しなければならない。

⑼　例外措置

ア　例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、本対策基準を遵守することが困難な状況において、教育行政、学校事務又は教育活動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は、情報セキュリティ統括者の許可を得て、例外措置を取ることができる。

イ　緊急時の例外措置

情報セキュリティ管理者及び情報システム管理者は、教育行政、学校事務又は教育活動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避けられないときは、実施後速やかに情報セキュリティ統括者に報告しなければならない。

ウ　例外措置の把握

情報セキュリティ統括者は、例外措置の実施状況を適切に把握するとともに、定期的にその必要性について確認しなければならない。

8　技術的セキュリティ対策

(1)　情報システムの管理

ア　情報システム仕様書等の整備

(ｱ) 情報システム管理者は、所管する情報システムを適切に管理するため、次に掲げる仕様書等を整備しなければならない。

a　情報システムを構成する機器等を管理する文書

b　情報システムの利用者及び利用者権限を管理する文書

c　ネットワーク仕様書、ネットワーク構成図等

(ｲ) 情報システム管理者は、仕様書等について、常に情報システムとの整合性を維持しなければならない。

(ｳ) 情報システム管理者は、仕様書等について、業務上それらを必要とする職員以外の者が閲覧できないよう適切に保管しなければならない。

イ　情報システム変更等の記録及び作業の確認

(ｱ) 職員は、情報システム変更等の作業を行う場合は、あらかじめ情報システム管理者の承認を得るとともに、実施した作業内容について記録を作成し、情報システム管理者に提出しなければならない。

(ｲ) 情報システム管理者は、システム変更等の作業記録について、漏えい、改ざん等のないよう適切に管理しなければならない。

ウ　ログの取得等

(ｱ) 情報システム管理者は、操作履歴、閲覧履歴等の各種ログ及び情報セキュリティの確保に必要な記録を取得するとともに、取得したログの保存期間を適切に定め、保存しなければならない。

(ｲ) 情報システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。

(ｳ) 情報システム管理者は、悪意ある第三者等からの不正アクセスの有無について、取得したログを定期的に又は必要に応じ点検及び分析をしなければならない。ただし、特定個人情報を取り扱うシステムは、取得したログを定期的にかつ必要に応じ点検及び分析をしなければならない。

(ｴ) 情報システム管理者は、ログの改ざん、窃盗又は消去を防止するために、必要な措置を講じなければならない。

エ　障害記録

情報システム管理者は、職員からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

オ　バックアップの実施

情報システム管理者は、所管する情報システムにおいて、サーバの冗長化対策の有無にかかわらず、取り扱う電子情報の重要性、情報システムが停止した場合の業務への影響等を勘案し、定期的に電子情報等のバックアップを実施しなければならない。

カ　ファイルサーバ等による電子情報の共有

情報システム管理者は、職員間で電子情報を共有するためファイルサーバ等を設置する場合は、

次の事項を措置しなければならない。

(ｱ) ファイルサーバ等を課等の単位で構成するなど、職員が業務上必要のないフォルダ及び電子情報等を閲覧又は使用できないように設定しなければならない。ただし、業務を遂行するために必要であると認める場合は、複数の課等の職員がフォルダ及び電子情報を閲覧又は使用できるように設定することができる。

(ｲ) ファイルサーバ等の構成単位ごとに利用可能な容量を制限しなければならない。

(ｳ) 職員に対し、取り扱う情報の重要性に応じて、電子情報に対して情報保護対策を適切に行うよう義務付けなければならない。

キ　ネットワーク構築

(ｱ) 情報システム管理者は、サーバ、パソコン、モバイル端末等の機器によりネットワークを構築し、又は構成を変更する場合（有線回線の無線化等を含む。）は、あらかじめ情報セキュリティ統括者の承認を得なければならない。

なお、個人番号利用事務系の情報システムの保守等のために外部と接続する場合は、情報システム管理者は、接続を開始する前に外部の専門家による監査を実施のうえ、情報セキュリティ統括者の承認を得なければならない。また、接続後は定期的にかつ必要に応じ監査を実施し、継続して情報セキュリティ対策等が遵守されていることを確認のうえ、情報セキュリティ統括者に報告しなければならない。

(ｲ) 情報システム管理者は、職員以外の者が利用するネットワーク及び情報システムについて、他のネットワーク及び情報システムに影響を及ぼさないよう、これらと物理的又は論理的に分離する等の情報セキュリティ対策を必要に応じて施さなければならない。

ク　ネットワークの接続制御、経路制御等

情報システム管理者は、不正アクセスを防止するため、ファイアウォール、ルータ等のハードウェア及びソフトウェア等を適切に設定するとともに、ネットワークに適切なアクセス制御を講じなければならない。

ケ　外部ネットワークを介して利用できる情報システムの分離等

情報システム管理者は、インターネット等の外部ネットワークを介して利用できる情報システムについて、必要に応じ他の情報システムと分離する等、情報セキュリティ対策について特に強固な対策を講じなければならない。

コ　外部ネットワークとの接続制限等

(ｱ) 情報システム管理者は、サーバ、パソコン、モバイル端末等の機器を外部ネットワークと接続する場合は、原則として教育イントラネット※9を経由させなければならない。

(ｲ) 情報システム管理者は、教育イントラネットを経由せず外部ネットワークと接続する場合は、特段の事情があり、当該外部ネットワークのネットワーク構成、機器構成、情報セキュリティ対策等を調査し、教育委員会事務局等のネットワーク、情報システム等の情報資産に影響が生じないことを確認し、継続的に情報セキュリティを確保するための措置を講じたうえで、情報セキュ

※9 「教育イントラネット」とは、教育委員会事務局が本庁、教育機関及び学校を接続するネットワーク。

リティ統括者の許可を得て接続しなければならない。

(ｳ) 情報システム管理者は、接続した外部ネットワークの瑕疵による電子情報の漏えい、破壊又は改ざん、システムダウン等により業務への影響が生じた場合を想定し、必要に応じて当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

(ｴ) 情報システム管理者は、サーバ等をインターネット上に公開する場合、教育委員会事務局等のネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置したうえで接続しなければならない。

(ｵ) 情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、セキュリティ侵害のおそれがある場合は、直ちに当該外部ネットワークを遮断しなければならない。

サ　業務外（無許可）ネットワークへの接続禁止

情報セキュリティ管理者及び情報システム管理者は、有線・無線を問わず、パソコン、モバイル端末等をネットワークに接続する場合は、次に掲げる事項を遵守しなければならない。

(ｱ) パソコン、モバイル端末等をインターネット等の外部ネットワークに接続する場合は、情報セキュリティ統括者の許可を得なければならない。

(ｲ) パソコン、モバイル端末等を教育委員会事務局等のネットワークに接続する場合は、該当のネットワークを管理する情報システム管理者の許可を得なければならない。

(ｳ) 接続許可を得たネットワークと異なるネットワークに、パソコン、モバイル端末等を接続してはならない。

(ｴ) パソコン、モバイル端末等について、OS のポリシー設定等により異なるネットワークに接続できないよう技術的に制限しなければならない。

シ　無線ＬＡＮのセキュリティ管理

情報システム管理者は、無線ＬＡＮを利用する場合は、当該無線ＬＡＮにおいて取り扱う電子情報の重要性、接続するネットワーク等を勘案し、無線ＬＡＮについて解読が困難な暗号化、認証技術等の適切な措置を講じなければならない。

ス　複合機※10のセキュリティ管理

(ｱ) 情報セキュリティ管理者及び情報システム管理者は、複合機を利用する場合は、複合機が備える機能、設置環境及び取り扱う電子情報の重要性等に応じた対策を実施しなければならない。

(ｲ) 情報セキュリティ管理者及び情報システム管理者は、複合機の運用を終了する場合、複合機に保存された全ての電子情報を抹消し、又は再利用できないようにしなければならない。

セ　特定用途機器※11のセキュリティ管理

情報セキュリティ管理者及び情報システム管理者は、特定用途機器を利用する場合は、取り扱う

※10　「複合機」とは、プリンタ、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。

※11　「特定用途機器」とは、テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されているもの又は記録媒体を内蔵しているもの。

電子情報、利用方法、通信回線への接続形態等により、必要な情報セキュリティを確保するため、当該機器の特性に応じた対策を実施しなければならない。

ソ　電子メールのセキュリティ管理

(ｱ) 情報システム管理者は、権限のない利用者による外部から外部への電子メール転送（電子メールの中継処理）を防止するため、電子メールサーバを適切に設定しなければならない。

(ｲ) 情報システム管理者は、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、電子メールサーバの運用を停止しなければならない。

(ｳ) 情報システム管理者は、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防止しなければならない。

(ｴ) 情報システム管理者は、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なければならない。

(ｵ) 情報システム管理者は、システム開発、運用、保守等のために庁内又は情報セキュリティ統括者の承認を受けた施設に常駐する委託事業者による電子メールアドレスの利用について、事前に委託事業者との間で利用方法を取り決めなければならない。

(ｶ) 情報システム管理者は、職員等が電子メール等により情報資産を無断で外部に持ち出すことがないよう、添付ファイルの監視等システム上の措置を講じなければならない。

タ　電子メールの利用に関する遵守事項

(ｱ) 職員は、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。ただし、情報セキュリティ統括者が許可したときを除く。

(ｲ) 職員は、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) 職員は、電子メールを送受信するに当たり、情報システム管理者から付与された電子メールアドレスを使用しなければならない。

(ｴ) 職員は、電子メールを送受信するに当たり、情報システム管理者が指定するパソコン、モバイル端末等を使用しなければならない。

(ｵ) 職員は、電子メールを送受信するに当たり、情報システム管理者が指定するソフトウェアを使用しなければならない。また、当該ソフトウェアを情報システム管理者が定める設定で使用しなければならない。

(ｶ) 職員は、複数人に電子メールを送信する場合は、必要があるときを除き、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。

(ｷ) 職員は、電子メールを誤送信した場合、直ちに情報セキュリティ管理者に報告しなければならない。

(ｸ) 職員は、メーリングリストに参加する場合は、情報セキュリティ管理者の許可を得なければならない。

チ　無許可ソフトウェアの導入等の禁止

(ｱ) 職員は、不正にコピーしたソフトウェア及び個人が所有するソフトウェアを利用してはならない。

(ｲ) 職員は、パソコン、モバイル端末等にソフトウェアを導入する場合は、情報システム管理者の許可を得なければならない。

(ｳ) 情報システム管理者又は情報セキュリティ管理者は、パソコン、モバイル端末等に導入したソフトウェアのライセンスを適切に管理しなければならない。

ツ　機器構成の変更の制限

職員は、パソコン、モバイル端末等の情報システムを構成する機器の改造、交換及び増設を行ってはならない。ただし、情報システム管理者が許可したときを除く。

テ　ウェブページの閲覧に関する遵守事項

(ｱ) 職員は、業務以外の目的でウェブページを閲覧してはならない。

(ｲ) 職員は、ウェブページを閲覧するに当たり、情報システム管理者が指定するソフトウェアを使用しなければならない。

(ｳ) 情報セキュリティ管理責任者は、職員が明らかに業務に関係のないウェブページ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。

ト　個人番号利用事務系における出力の制限

情報システム管理者は、個人番号利用事務系においては、原則として、電子情報を端末から外部記録媒体に出力できないよう、システム上の制限を講じなければならない。外部記録媒体に電子情報を出力しなければならない場合、以下の対策をすべて実施しなければならない。

(ｱ) 端末に接続し情報を出力する外部記録媒体は、情報システム管理者が許可したものでなければならない。

(ｲ) 出力した情報に対して情報保護対策を実施しなければならない。

(ｳ) 出力した情報の利用記録を取得しなければならない。

(ｴ) 情報の受渡しに関して、情報セキュリティ管理者の承認を受け、承認の記録を保存しなければならない。

(2) アクセス制御

ア　アクセス制御

(ｱ) 利用者の識別及び認証

情報システム管理者は、所管するネットワーク、サーバ等の情報システムについて、利用者の識別、認証等、権限のない職員がアクセスできないよう適切な措置を講じなければならない。特に、個人番号利用事務系においては、多要素認証を用いなければならない。

(ｲ) 利用者の権限制御

情報システム管理者は、情報システムの利用を許可した職員について、担当する業務及び必要性を勘案し、取扱可能な電子情報及び利用可能な機能の範囲等を必要最小限に設定する等、適切にアクセス権限を設定しなければならない。

(ｳ) 利用者ＩＤの取扱い

a　情報システム管理者は、情報システムの利用を許可した職員以外に、利用者ＩＤ及びパスワードを付与してはならない。

b　情報システム管理者は、職員が、異動、出向、退職その他の理由により情報システムを利用する必要がなくなった場合は、速やかに当該利用者の利用者ＩＤ及びパスワードを無効にし

なければならない。

c　情報システム管理者は、利用者ＩＤの不正使用の報告を受けた場合は、直ちに当該利用者ＩＤによる情報システムの利用を停止しなければならない。

d　情報システム管理者は、利用されない利用者ＩＤが放置されないよう、適切に管理しなければならない。

e　職員は、情報システムを利用する必要がなくなった場合は、利用者ＩＤによる情報システムの利用を停止するよう、情報システム管理者に報告しなければならない。

(ｴ) 特権を付与されたＩＤの取扱い

a　情報システム管理者は、管理者権限等の特権を付与されたＩＤ（以下「特権ＩＤ」という。）を利用する者を必要最小限にしなければならない。

b　情報システム管理者は、特権ＩＤ及び当該ＩＤのパスワードについて、初期設定されたものから変更しなければならない。

c　情報システム管理者は、特権ＩＤについて、当該ＩＤのパスワードの漏えい等を防止するため、他のＩＤよりも文字数が多く他人が容易に想像できないパスワードを設定するとともに定期的な変更を行う等、特に厳重に管理しなければならない。

d　情報システム管理者は、特権ＩＤによる情報システムへの接続時間を必要最小限にしなければならない。

イ　外部からのアクセス等の制限

(ｱ) 情報セキュリティ統括者は、外部から教育委員会事務局等の情報システムへのアクセスを許可する場合は、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。

(ｲ) 前項の規定により、情報セキュリティ統括者が外部からのアクセスを認める場合、当該情報システムの情報システム管理者は、第三者のなりすましを防止し、アクセスする者が確実に許可された者であることを確認するため適切な措置を講じなければならない。

(ｳ) (ｱ)の規定により、情報セキュリティ統括者が外部からのアクセスを認める場合、当該情報システムの情報システム管理者は、通信中の盗聴を防止するため、送受信される電子情報の暗号化、通信経路の暗号化等の措置を講じなければならない。

ウ　不正ログインの防止

情報システム管理者は、正当なアクセス権限を持つ職員以外の者が情報システムを利用できないよう、ログイン試行回数の制限、アクセスタイムアウトの設定等の適切な措置を講じなければならない。

エ　認証情報の管理

(ｱ) 情報システム管理者は、職員の認証情報を厳重に管理しなければならない。

(ｲ) 情報システム管理者は、認証情報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。

(ｳ) 情報システム管理者は、職員に対してパスワードを発行するときは、不正利用を防止するため以下の措置を講じなければならない。

a　情報システム管理者は、パスワードについて、文字数、使用する文字種及び管理方法を定め、職員に周知しなければならない。

b　情報システム管理者は、仮のパスワードも含めパスワードを発行する場合は、十分な文字数とし、文字列は他人が想像しにくいものにしなければならない。

c　情報システム管理者は、職員に対し、仮のパスワードを発行するときは、ログイン後直ちに仮のパスワードを変更させなければならない。

d　情報システム管理者は、パスワードを不正利用されないよう、パスワードをハッシュ化の技術を用いて保管する等、適切に管理しなければならない。

⑶　情報システムの開発、導入、保守等

ア　情報システムの調達

(ｱ) 情報システム管理者は、情報システムの開発、導入、更新及び保守（リモートを含む。）の調達に当たっては、調達仕様書に必要とするセキュリティ要件を明記しなければならない。

(ｲ) 情報システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上必要な機能を有することを確認しなければならない。

イ　情報システムの開発等

情報システム管理者は、情報システムの開発、導入、更新及び保守に当たっては、次に掲げる事項を定めなければならない。

(ｱ) 責任者及び監督者

(ｲ) 作業者及び作業範囲

(ｳ) 開発、保守等を行う情報システムと運用中の情報システムとの分離

(ｴ) 開発、保守等を行う情報システムのソースコードの提出義務

(ｵ) 開発、保守等に関する作業記録の提出義務

(ｶ) 開発、保守等における情報セキュリティ上問題となるおそれがあるソフトウェアの使用の禁止に関する事項

(ｷ) 開発、保守等に伴う事故及び不正行為に係る脅威の分析

(ｸ) 開発、保守等における情報システムへのアクセスの制限

(ｹ) 機器の搬入出の規制

(ｺ) 仕様書、マニュアル等の定められた場所への保管

(ｻ) 開発、保守等を行う者のＩＤ、パスワード等の管理及び作業終了後の当該ＩＤ、パスワード等の抹消

ウ　情報システムの導入

(ｱ) 情報システム管理者は、情報システムの導入又は更新を行う場合は、あらかじめ京都市個人情報保護条例に基づく手続等、必要な手続を踏まなければならない。

(ｲ) 情報システム管理者は、情報システムの導入又は更新を行う場合は、あらかじめ当該情報システムが停止した場合の業務への影響等を勘案し、障害等に備えた冗長化等の対策が講じられていることを確認しなければならない。

(ｳ) 情報システム管理者は、開発又は保守等に関する計画の策定時に、情報システムの移行手順を明確にしなければならない。

(ｴ) 情報システム管理者は、情報システムを移行する場合は、運用中の情報システムに記録されて

いる電子情報を確実に保存し、移行に伴う情報システムの停止等の影響を最小限に抑えなければならない。

(ｵ) 情報システム管理者は、あらかじめ擬似環境において十分な動作確認を行ったうえ、情報システムの移行を行わなければならない。

エ　情報システムの導入等のテスト

(ｱ) 情報システム管理者は、情報システムの導入又は更新を行う場合は、既に稼働している情報システムに障害等の影響を与えないよう事前に十分なテストを行わなければならない。

(ｲ) 情報システム管理者は、重要性Ⅰに分類される電子情報等を、テストデータとして使用してはならない。ただし、合理的な理由があり、情報セキュリティ統括者が適切な情報セキュリティが確保されていると認める場合を除く。

(ｳ) 情報システム管理者は、テストに使用した電子情報等及びその結果を一定期間厳重に保管しなければならない。

オ　ソフトウェアの保守及び更新等

(ｱ) 情報システム管理者は、ソフトウェアを更新し、又は修正プログラムを導入する場合は、ソフトウェア又は修正プログラムに不具合がないこと及び他の情報システムに障害等の影響を与えないことを確認しなければならない。

(ｲ) 情報システム管理者は、セキュリティ侵害のおそれがあるソフトウェアの欠陥に対しては、修正プログラムを適用する等により、速やかに対応しなければならない。また、当該ソフトウェアの利用を予定している期間中にパッチ、バージョンアップ等の開発元のサポートが終了する予定がないことを確認しなければならない。

カ　開発、保守等に関する資料等の整備及び保管

(ｱ) 情報システム管理者は、情報システムの開発、保守等に関する資料及び当該情報システムの仕様書等の文書（以下「システム関連文書」という。）を適切に整備しなければならない。

(ｲ) 情報システム管理者は、システム関連文書の内容に変更が生じた場合は、直ちに当該変更の内容をシステム関連文書へ反映し、常に最新の状態を維持するとともに、当該変更履歴を記録しなければならない。

(ｳ) 情報システム管理者は、情報システムのソースコードを適切に保管しなければならない。

(ｴ) 情報システム管理者は、業務上必要とする職員以外の者が、情報システム関連文書を許可な閲覧できないよう適切に保管しなければならない。

キ　情報システムにおける入出力情報の正確性の確保

(ｱ) 情報システム管理者は、情報システムに入力される電子情報等について、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を備えるよう情報システムを設計しなければならない。

(ｲ) 情報システム管理者は、情報システムから出力される電子情報等について、情報の処理が正しく反映され、出力されるよう情報システムを設計しなければならない。

(ｳ) 情報システム管理者は、インターネットに公開するウェブサイトを構築する場合は、原則として、行政機関若しくは教育機関のみが登録することができる「属性型 JP ドメイン（lg. jp ドメイン、ed. jp ドメイン等）」又は本市が保有する「地域型 JP ドメイン」を使用しなければならな

い。

(ｴ) 情報システム管理者は、ドメインを運用停止する場合は、第三者に不正に取得されないよう、運用停止後も可能な限りドメインを保持しなければならない。

(ｵ) 情報システム管理者は、インターネットに公開するウェブサイトを構築する場合は、転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じるとともに、既知の脆弱性に対して適切な対策を講じなければならない。

ク　情報システムの変更管理

情報システム管理者は、情報システムを変更した場合、仕様書等の変更履歴を記録し、適切に管理しなければならない。

⑷　不正プログラム対策

ア　情報セキュリティ管理責任者の措置事項

情報セキュリティ管理責任者は、不正プログラム対策に関し、次の事項を措置しなければならない。

(ｱ) コンピュータウイルス等の不正プログラムに関する情報を収集し、必要に応じ職員に対して注意喚起を行わなければならない。

(ｲ) 不正プログラム対策ソフトウェア及び当該ソフトウェアの定義ファイルを常に最新の状態に保たせるよう指導しなければならない。

イ　教育イントラネットを管理する情報システム管理者の措置事項

教育イントラネットを管理する情報システム管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

(ｱ) 外部ネットワークから受信した電子情報は、インターネットのゲートウェイ※12においてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムの侵入を防止しなければならない。

(ｲ) 外部ネットワークに送信する電子情報は、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

ウ　情報システム管理者の措置事項

情報システム管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

(ｱ) 所管するサーバ、パソコン等の機器に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。ただし、不正プログラム対策ソフトウェアをインストールできない電子計算機については、オペレーティングシステムのバージョンを最新の状態に保たなければならない。

(ｲ) 不正プログラム対策ソフトウェアは、常に最新の状態に保たなければならない。

(ｳ) 不正プログラム対策ソフトウェアの定義ファイルは、常に最新の状態に保たなければならな

※12　「ゲートウェイ」とは、インターネットと教育イントラネットの境界に設置される機器をいう。

い。

(ｴ) インターネット等の外部ネットワーク又は他のネットワークと接続していない情報システムにおいても、不正プログラムの感染、侵入等が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及び定義ファイルを更新しなければならない。

(ｵ) コンピュータウイルス等の不正プログラムに関する情報を得た場合は、必要に応じて情報システムに必要な措置を講じるとともに、職員に対して注意喚起を行わなければならない。

(ｶ) 職員の操作記録、コンピュータウイルス等の不正プログラムの検出記録等について、定期的又は必要に応じ分析し、必要に応じて対策を講じなければならない。

(ｷ) 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等の脅威に備えて、あらかじめ対応手順を策定し、データのバックアップをオフラインで取得する等の被害を受けた際の低減策を講じるとともに、職員に周知しなければならない。また、対応手順を定期的に確認しなければならない。

(ｸ) 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等の脅威に備えて、原則として、侵入したコンピュータウイルスが不審な行動をしているかどうか検知できる状態にする対策（エンドポイント対策）を講じなければならない。また、ネットワーク機器、情報システム等を導入した事業者及び保守を行う事業者との契約では、役割分担を明確に定めなければならない。

(ｹ) 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のおそれがある場合は、直ちに情報セキュリティ管理責任者に報告しなければならない。

エ　情報セキュリティ管理者の措置事項

情報セキュリティ管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

(ｱ) 情報システム管理者の指示に従い、コンピュータウイルス等の不正プログラムの脅威に関する対策を実施しなければならない。

(ｲ) 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のおそれがある場合は、直ちに情報システム管理者及び情報セキュリティ管理責任者に報告しなければならない。

オ　職員の遵守事項

職員は、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。

(ｱ) パソコン、モバイル端末等に導入されている不正プログラム対策ソフトウェアの設定を変更してはならない。

(ｲ) 外部から電子情報等又はソフトウェアを入手した場合は、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。ただし、不正プログラム対策ソフトウェアをインストールできない電子計算機については、電子情報等の発信元又は正規のソフトウェアであること等を確認しなければならない。

(ｳ) 差出人が不明又は不自然に添付された電子情報を受信した場合は、開封せずに速やかに情報セキュリティ管理者及び情報セキュリティ管理責任者に報告しなければならない。

(ｴ) パソコン、モバイル端末等に対して、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行わなければならない。ただし、不正プログラム対策ソフトウェアをインストールできない電子計算機については、不審なソフトウェアが動作していないことを定期的に確認しなけ

ればならない。

(ｵ) 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によるチェックを行わなければならない。

(ｶ) インターネット接続系で受信した電子メール又はインターネット経由で入手したファイルをＬＧＷＡＮ接続系に取り込む場合は、無害化しなければならない。

(ｷ) 情報システム管理者が提供するコンピュータウイルス等の不正プログラムに関する情報を、常に確認しなければならない。

(ｸ) 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のおそれがある場合は、直ちにＬＡＮケーブルの取外し又は無線ネットワークからの切断等、他の機器等への感染を防止する措置を講じるとともに、直ちに情報セキュリティ管理者及び情報セキュリティ管理責任者に報告しなければならない。

カ　専門家の支援体制

情報セキュリティ統括者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、不正プログラム対策ソフトウェアの提供事業者とサポート契約を締結する等、外部の専門家の支援を受けられるよう体制を整備しておかなければならない。

⑸ 不正アクセス対策

ア　情報システム管理者の措置事項

情報システム管理者は、不正アクセス対策として、次の事項を措置しなければならない。

(ｱ) 所管する情報システムについて、使用していないポートを閉鎖するとともに、不要なサービスを停止しなければならない。

(ｲ) 不正アクセスによるウェブページの改ざんを防止するため、電子情報の書換えを検出するソフトウェアを導入する等、適切な措置を講じなければならない。

(ｳ) 修正プログラムの提供、バージョンアップの提供等の開発元のサポートがあるハードウェア及びソフトウェアを利用しなければならない。

(ｴ) ハードウェア及びソフトウェアに係る修正プログラムが公開された場合は、必要に応じて動作確認等の検証を行ったうえ、速やかに当該修正プログラムを適用しなければならない。

イ　攻撃の予告等に対する措置

情報システム管理者は、サーバ等に攻撃を受けることが明確になった場合、情報システムの停止を含む必要な措置を講じるとともに、関係機関と連携し、情報収集に努めなければならない。

ウ　記録の保存

情報システム管理者は、不正アクセス行為の禁止等に関する法律違反等、犯罪の可能性がある不正アクセスを受けた場合は、不正アクセスの記録の保存に努めるとともに、警察等関係機関と連携し、対処しなければならない。

エ　サービス不能攻撃

情報システム管理者は、インターネット等の外部ネットワークを介して利用できる情報システムについて、第三者からのサービス不能攻撃により情報システムが停止することを防止するため、必要に応じ、サービス不能攻撃に係る通信の監視及び遮断等、サービス不能攻撃の影響を排除又は

低減するための対策を講じなければならない。

オ　標的型攻撃

情報システム管理者は、標的型攻撃による教育委員会事務局等のネットワークへの侵入を防止するために、教育等の人的対策を講じなければならない。また、教育委員会事務局等のネットワークへの侵入のリスクを低減する対策（入口対策）及び内部に侵入した攻撃を早期に検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する等の対策（内部対策及び出口対策）を講じなければならない。

⑹　情報システムの監視

情報システム管理者は、不正プログラム、不正アクセス等による情報システムへの攻撃及び情報システムの不正利用を早期に検知し、適切に対処するため、次の事項を措置しなければならない。

ア　取り扱う電子情報等の重要性、情報システムが停止した場合の業務への影響等を勘案し、情報セキュリティインシデント、障害等を早期に検知するため、情報システムを監視しなければならない。

イ　重要なログ等を取得するサーバについて、正確な時刻設定及びサーバ間の時刻同期を行い、ログ等の記録について正確性を確保しなければならない。

ウ　インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見及びその対処、ＬＧＷＡＮへの不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

⑺　セキュリティ情報の収集

情報セキュリティ管理責任者は、ハードウェア及びソフトウェアの脆弱性並びに不正プログラム等に関する情報を収集し、必要に応じ、情報セキュリティ管理者及び情報システム管理者と情報を共有しなければならない。

9　業務委託と外部サービスの利用

⑴　業務委託

ア　委託事業者の選定基準

(ｱ) 情報システム管理者は、委託事業者の選定に当たり、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。

(ｲ) 情報システム管理者は、必要に応じ、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、委託事業者を選定しなければならない。

イ　契約項目

情報システム管理者は、所管する重要な情報資産を取り扱う業務又は情報システムに関する業務を委託する場合は、委託事業者に本対策基準を遵守させるため、委託契約書又は仕様書に次の事項を明記しなければならない。

(ｱ) 委託契約書又は仕様書の記載事項

a　本対策基準の遵守に関する事項

b　委託事業者の責任者、委託内容、作業者、作業場所の特定に関する事項

c　委託事業者にアクセスを許可する情報の種類及び範囲、アクセス方法の明確化等、情報のライフサイクル（作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等）全般での管理方法

d　委託事業者の従業員に対する教育の実施に関する事項

e　提供された情報の目的外利用及び委託事業者以外の者への提供の禁止に関する事項

f　提供された情報の複写及び複製の禁止に関する事項

g　業務上知り得た情報の守秘義務に関する事項

h　再委託に関する制限事項の遵守に関する事項

i　委託業務終了時の情報資産の返還、廃棄等に関する事項

j　委託業務の定期報告及び緊急時報告義務に関する事項

k　本市による監査、検査の受入れ義務に関する事項

l　本市による情報セキュリティインシデント発生時の公表に関する事項

m　前各号に掲げる事項に違反した場合における契約の解除等の措置及び損害賠償義務に関する事項

(ｲ) 必要に応じ記載する事項

委託契約書又は仕様書には、必要に応じ、次に掲げる事項を明記するものとする。

a　提供されるサービスレベルの保証に関する事項

b　情報資産の授受及び搬送に関する事項

c　その他委託事業者に実施させる情報セキュリティ対策に関する事項

ウ　再委託の制限

(ｱ) 個人情報を取り扱う情報システムにおける制限

a　情報システム管理者は、個人情報を取り扱う情報システムに関する業務を委託する場合は、原則として委託業務の履行について再委託を承認してはならない。

b　情報システム管理者は、委託事業者から再委託の承認を求められた場合又はあらかじめ委託業務の履行に複数の事業者が関与することが想定される場合は、原則として次のいずれかの方法により契約を締結しなければならない。

(a) 委託業務の履行に関与する全ての事業者と個別に契約を締結

(b) 委託業務の履行に関与する全ての事業者連名による契約を締結

(c) 委託業務の履行に関与する全ての事業者にコンソーシアムを構成させ、当該コンソーシアムの代表会社と契約を締結

(ｲ) 再委託の承認

a　情報システム管理者は、再委託の承認を求められた場合は、再委託の内容、再委託の相手方、再委託の理由等を付した書面により事前に申請を受けなければならない。

b　情報システム管理者は、再委託に関する申請を受けたときは、委託事業者が次の条件を満たす場合に限り、承認を与えることができるものとし、書面により承認又は不承認を通知しなければならない。

(a) 再委託の相手方に委託業務の契約に基づく一切の義務を遵守させること。

(b) 再委託の相手方の全ての行為及びその結果について責任を負うこと。

(c) 再委託の相手方との契約において再委託の相手方を監督するための手続及び方法を具体的に定めること。

(d) 再委託の相手方における履行状況を適切に管理すること。

エ　誓約書等の提出

情報システム管理者は、所管する情報システムに関する業務を委託する場合において、委託事業者に教育委員会事務局等の情報資産を使用させるときは、当該事業者の代表者から要員名簿を提出させるとともに、委託業務担当者本人から、秘密の保持その他電子情報等の適切な取扱いに関する誓約書を提出させなければならない。

オ　委託事業者に対する監査・確認・措置等

情報システム管理者は、委託事業者において必要な情報セキュリティが確保されていることを定期的又は必要に応じ確認し、安全を確保しなければならない。

⑵　外部サービス（クラウドサービス※13・約款による外部サービス※14を含む。）の利用

ア　外部サービスの利用に関する規定整備

情報セキュリティ統括者は、外部サービスの利用に関する規定を整備しなければならない。

イ　外部サービスの選定

(ｱ) 情報システム管理者は、外部サービスを利用して重要性Ⅰの情報を取り扱う場合は、情報セキュリティに係る要件を踏まえて、外部サービスを選定しなければならない。

(ｲ) 情報システム管理者は、外部サービスを利用して重要性Ⅰの情報を取り扱う場合、外部サービスの情報セキュリティ対策に関する情報の提供を事業者等に求め、その内容を確認し、本対策基準を満たしているか評価しなければならない。

ウ　外部サービスの利用承認

情報システム管理者は、外部サービスを利用して重要性Ⅰの情報を取り扱う場合、情報セキュリティ統括者（重要性Ⅰ以外の情報を取り扱う場合は、情報セキュリティ管理責任者）に利用申請をしなければならない。また、外部サービスを利用するに当たり、教育委員会事務局等のネットワークをはじめ他の情報システム管理者が管理する情報システムを活用する場合には、当該情報システム管理者と十分な調整を行わなければならない。

エ　外部サービスの調達・契約

(ｱ) 情報システム管理者は、外部サービスを利用して重要性Ⅰの情報を取り扱う場合、外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めなければならない。

(ｲ) 情報システム管理者は、外部サービスを利用して重要性Ⅰの情報を取り扱う場合、調達仕様を

※13　「クラウドサービス」とは、情報システムを所有するのではなく、インターネット等を通じて、情報システムを利用する形態をいう。

※14　「約款による外部サービス」とは、有料、無料にかかわらず、約款への同意及び簡易なアカウント登録により利用可能なサービスをいう。

満たすことを契約までに確認し、調達仕様の内容を契約に含めなければならない。

オ　外部サービスのセキュリティ対策

情報セキュリティ統括者は、外部サービスの特性、責任分界点に係る考え方等を踏まえ、外部サービスを利用して重要性Ⅰの情報を取り扱う場合の以下のセキュリティ対策を規定しなければならない。

(ｱ)　外部サービスを利用した情報システムの導入・構築時の対策

(ｲ)　外部サービスを利用した情報システムの運用・保守時の対策

(ｳ)　外部サービスを利用した情報システムの更改・廃棄時の対策

カ　外部サービス実施状況の確認・記録

外部サービスを利用して重要性Ⅰの情報を取り扱う場合、外部サービスを利用する情報システム管理者は、前項に定める規定に対し、外部サービスの実施状況を確認・記録しなければならない。

キ　外部サービスで発生したインシデントへの対処

外部サービスを利用する情報システム管理者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備しなければならない。

(3)　外部サービス利用の特則

ガバメントクラウド（デジタル社会形成基本法第２９条に規定する「全ての地方公共団体が官民データ活用推進基本法第２条第４項に規定するクラウド・コンピューティング・サービス関連技術に係るサービスを利用することができるようにするための国による環境の整備」としてデジタル庁が整備するものをいう。以下同じ。）を利用する場合は、次に掲げる事項を遵守しなければならない。

ア　ガバメントクラウド利用における組織体制

情報セキュリティ統括者は、ガバメントクラウドを利用する際には、複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制を構築しなければならない。また、ガバメントクラウド利用における情報セキュリティ対策に取り組むための十分な組織体制を確立しなければならない。

イ　ガバメントクラウド利用における情報資産の管理

情報システム管理者は、ガバメントクラウドの環境に保存される情報資産についても情報資産の分類に基づき管理しなければならない。また、情報資産がライフサイクルごとに適切に取扱われることを確認しなければならない。ガバメントクラウドを更改する際の情報資産の移行及びこれらの情報資産の全ての複製のガバメントクラウドを提供するクラウドサービス事業者（以下、「ガバメントクラウドサービス事業者」という。）からの削除の記述を含むサービス利用の終了に関する内容について、サービス利用前に文書での提示を求め、又は公開されている内容を確認しなければならない。

ウ　ガバメントクラウドにおける情報資産の廃棄

情報システム管理者は、ガバメントクラウドで利用する全ての情報資産について、ガバメントクラウドの利用終了時期を確認し、ガバメントクラウドで取り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。

エ　個人番号利用事務系と接続されるガバメントクラウド上での情報システムの取り扱い

個人番号利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド上の情報システムの領域については、個人番号利用事務系として取り扱い、本市の他の領域とはネットワークを分離しなければならない。

オ　個人番号利用事務系と接続されるガバメントクラウド上での情報資産の取扱い

個人番号利用事務系の情報システムをガバメントクラウドにおいて利用する場合は、その情報資産の機密性を考慮し、暗号による対策を実施する。その場合、暗号は十分な強度を持たなければならない。また、ガバメントクラウドサービス事業者が暗号に関する対策を行う場合又はガバメントクラウドサービス事業者が提供する情報資産を保護するための暗号機能を利用する場合、ガバメントクラウドサービス事業者が提供するそれらの機能や内容について情報を入手し、その機能について理解に努め、必要な措置を行わなければならない。

カ　ＬＧＷＡＮ接続系と接続されるガバメントクラウド上での情報システムの扱い

ＬＧＷＡＮ接続系の情報システムをガバメントクラウド上へ配置する場合は、その領域をＬＧＷＡＮ接続系として扱い、本市の他の領域とはネットワークを分離し、専用回線を用いて接続しなければならない。

キ　ガバメントクラウドサービス事業者が利用する機器の処分

ガバメントクラウドサービス事業者が利用する資源（装置等）を処分する場合は、セキュリティを確保した対応となっているか、ガバメントクラウドサービス事業者の方針及び手順について確認しなければならない。

なお、当該確認にあたっては、ガバメントクラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用できる。

ク　ガバメントクラウド利用における遵守事項

職員は、ガバメントクラウドの利用にあたっても本対策基準を遵守し、ガバメントクラウドの利用に関する自らの役割及び責任を意識しなければならない。

ケ　ガバメントクラウドの情報セキュリティに関する研修・訓練

情報システム管理者は、ガバメントクラウドを利用する職員に対して、情報セキュリティに関する意識向上、教育及び訓練を定期的に実施するとともに、委託先を含む関係者については委託先等で教育、訓練が行われていることを確認しなければならない。

コ　ガバメントクラウド利用における庁内での情報セキュリティインシデントの報告

情報システム管理者は、ガバメントクラウド利用における情報セキュリティインシデントの報告について連絡体制に従って報告しなければならない。

サ　ガバメントクラウド利用における外部からの情報セキュリティインシデントの報告

情報システム管理者は、ガバメントクラウドサービス事業者が検知した情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みの構築を契約等で取り決めなければならない。

シ　ガバメントクラウド利用におけるバックアップの実施

情報システム管理者は、ガバメントクラウドサービス事業者のバックアップ機能を利用する場合、ガバメントクラウドサービス事業者にバックアップ機能の仕様を要求し、その仕様を確認しな

ければならない。また、その機能の仕様が本市の求める要求事項を満たすことを確認しなければならない。ガバメントクラウドサービス事業者からバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行わなければならない。

ス　ガバメントクラウド利用におけるログの取得等

(ｱ) 情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、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実施しなければならない。なお、ガバメントクラウドサービス事業者が収集し、保存する記録（ログ等）に関する保護（改ざんの防止等）の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認しなければならない。

(ｲ) 情報システム管理者は、監査及びデジタルフォレンジック※15に必要となるガバメントクラウドサービス事業者の環境内で生成されるログ等の情報（デジタル証拠）について、ガバメントクラウドサービス事業者から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、ガバメントクラウドサービス事業者に提出を要求するための手続を明確にしなければならない。

セ　ガバメントクラウド利用における不正プログラム対策

情報システム管理者は、仮想マシンを設定する際に不正プログラムへの対策（必要なポート、プロトコル及びサービスだけを有効とすること、マルウェア対策及びログ取得等の実施）を確実に実施しなければならない。SaaS 型を利用する場合は、これらの対応が、外部サービス事業者側でされているのか、サービスを利用する前に確認しなければならない。また、サービスを利用している状況下では、これらのセキュリティ対策が適切にされているのか定期的にガバメントクラウドサービス事業者に報告を求めなければならない。

ソ　ガバメントクラウド利用におけるアクセス制御

(ｱ) 情報システム管理者は、情報セキュリティ統括者が定めた外部サービスの利用に関する規定におけるアクセス制御に関する事項が、ガバメントクラウドにおいて実現できるのか又はガバメントクラウドサービス事業者の提供機能等により実現できるのか、利用前にガバメントクラウドサービス事業者に確認しなければならない。

(ｲ) 情報システム管理者は、ガバメントクラウドを利用する際に、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させ、ガバメントクラウドにアクセスさせなければならない。

(ｳ) 情報システム管理者は、パスワードなどの認証情報の割り当てが ガバメントクラウド側で実施される場合、その管理手順等が、情報セキュリティ統括者が定めた外部サービスの利用に関する規定の内容を満たすことを確認しなければならない。

タ　ガバメントクラウド利用におけるセキュリティ情報の収集

情報システム管理者は、ガバメントクラウドサービス事業者に対して、利用するガバメントクラウドに影響し得る技術的脆弱性の管理内容について情報を求め、本市の業務に対する影響や保有

※15 「デジタルフォレンジック」とは、電子データを調査分析することで事実解明及び証拠保存を行うための技術のこと。

するデータへの影響について特定する。そして、技術的脆弱性に対する脆弱性管理の手順について、ガバメントクラウドサービス事業者に確認しなければならない。

チ　ガバメントクラウド における監視

(ｱ) 情報システム管理者は、利用するガバメントクラウドで取得される重要なログ等の時刻の同期についても適切になされているのか確認しなければならない。

(ｲ) 情報システム管理者は、必要となるリソースの容量・能力が確保できるガバメントクラウドサービス事業者を選定しなければならない。また、利用するガバメントクラウドにおいて必要な監視機能を確認するとともに、監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めなければならない。

(ｳ) 情報セキュリティ統括者及び情報システム管理者は、イベントログ取得に関するポリシーを定め、利用するガバメントクラウドがその内容を満たすことを確認し、ガバメントクラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討しなければならない。

ツ　ガバメントクラウド利用における手順化

情報システム管理者は、ガバメントクラウド利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認しなければならない。

(ｱ) サーバ、ネットワーク、ストレージ等の仮想化されたデバイスのインストール、変更及び削除

(ｲ) ガバメントクラウド利用の終了手順

(ｳ) バックアップ及び復旧

テ　ガバメントクラウド利用における緊急時対応計画の策定

情報セキュリティ統括者は、ガバメントクラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてガバメントクラウドの障害時を想定した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。

ト　ガバメントクラウド利用におけるライセンス管理

情報システム管理者は、ガバメントクラウドに商用ライセンスのあるソフトウェアをインストールする（IaaS 等でアプリケーションを構築する）場合は、そのソフトウェアのライセンス条項への違反を引き起こすことがないよう、利用するソフトウェアにおけるライセンス規定に従わなければならない。

ナ　ガバメントクラウド利用における委託事業者に対する監査

情報システム管理者は、ガバメントクラウドサービス事業者の本対策基準の遵守状況について、定期的に監査を行わなければならない。ガバメントクラウドサービス事業者にその証拠（文書等）の提示を求める場合は、第三者の監査人が発行する証明書や監査報告書等をこの証拠とすることもできる。

(4) ソーシャルメディア※16サービスの利用

ア　職員は、ソーシャルメディアサービスを利用する場合は、職員であることの自覚及び責任を持つとともに、法令及び職員の服務や情報の取扱いに関する規程等を遵守しなければならない。

イ　職員は、重要性Ⅰの電子情報をソーシャルメディアサービスで発信してはならない。

ウ　情報セキュリティ管理者は、ソーシャルメディアサービスを利用する場合は、アカウントによる情報発信が、教育委員会事務局等によるものであることを明らかにするため、アカウントの運用組織、情報発信の目的等を明確にする等の適切な措置を講じたうえで利用しなければならない。

(5) Web 会議サービスの利用

ア　情報セキュリティ統括者は、Web 会議を適切に利用するための利用手順を定めるものとする。

イ　職員は、本市の定める利用手順に従い、Web 会議を利用する場合は、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施しなければならない。

ウ　職員は、Web 会議を主催する場合は、会議に無関係の者が参加できないよう対策を講じなければならない。

10　評価・見直し

(1) 監査

ア　監査の実施

(ｱ) 情報セキュリティ統括者は、教育委員会事務局等の情報資産における本対策基準の遵守状況について確認するため、定期的に又は必要に応じ監査を実施しなければならない。

(ｲ) 情報セキュリティ統括者は、委託事業者に対して、再委託事業者も含めて、委託契約書及び仕様書に定めた内容が遵守されていることを確認するため、定期的に又は必要に応じ監査を実施しなければならない。

(ｳ) 情報セキュリティ統括者は、情報セキュリティ監査を効率的かつ効果的に実施するため、共通的な手順、手続等を明記した「京都市教育委員会情報セキュリティ監査実施要綱」を制定するものとする。

イ　監査人の指名

情報セキュリティ統括者は、監査の実施に当たり、被監査部門から独立した者を監査人に指名しなければならない。

ウ　監査計画の策定及び実施への協力

(ｱ) 情報セキュリティ統括者は、監査の実施に当たり、監査計画を策定しなければならない。

(ｲ) 監査人は、監査計画に基づき、監査を実施しなければならない。

(ｳ) 被監査部門は、監査の実施に協力しなければならない。

エ　監査結果の報告

(ｱ) 監査人は、監査結果及び指摘事項の改善状況等について、監査報告書を取りまとめ、情報セ

※16　「ソーシャルメディア」とは、インターネットを利用して、ユーザーが情報を発信し、又は相互に情報をやり取りするメディアをいう。

キュリティ統括者に報告しなければならない。

(ｲ) 情報セキュリティ統括者は、前項の報告を受けた場合は、ＣＩＳＯに報告しなければならない。

オ　監査結果への対応

情報セキュリティ統括者は、監査結果を踏まえ、指摘事項に関係する情報システム管理者又は情報セキュリティ管理者に対し、当該指摘事項への対処を指示しなければならない。また、指摘事項に関係しない情報システム管理者又は情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該指摘事項に関する課題及び問題点の有無について確認させなければならない。

カ　監査結果の活用

ＣＩＳＯは、監査結果を本対策基準の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

⑵　自主点検

ア　自主点検の実施

(ｱ) 情報セキュリティ統括者は、教育委員会事務局等の情報資産における情報セキュリティを継続的に確保するため、定期的又は必要に応じ自主点検を実施しなければならない。

(ｲ) 情報システム管理者は、所管する情報システムにおける本対策基準の遵守状況について、定期的又は必要に応じ自主点検を実施しなければならない。

(ｳ) 情報セキュリティ管理者は、所管する課等における本対策基準の遵守状況について、定期的又は必要に応じ自主点検を実施しなければならない。

イ　自主点検結果の報告

(ｱ) 情報システム管理者及び情報セキュリティ管理者は、自主点検結果及び自主点検結果に基づく改善状況を取りまとめ、情報セキュリティ統括者に報告しなければならない。

(ｲ) 情報セキュリティ統括者は、前項の報告を受けた場合は、ＣＩＳＯに報告しなければならない。

ウ　自主点検結果の活用

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

(ｲ) ＣＩＳＯは、自主点検結果を本対策基準の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

⑶　情報セキュリティ対策基準の見直し

ＣＩＳＯは、監査及び自主点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、必要があると認めるときは、本対策基準の改善を行うものとする。

別表（情報資産の重要性分類）

情報資産の分類		情報資産の例示（アクセス主体別）		
重要性	定義	職員	職員・児童生徒・保護者	不特定多数
Ⅰ	セキュリティ侵害が市民、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情報	**業務に係る特定の職員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 ・情報システムの設計書、設定書等 ○学校運営に関する情報 ・入学者選抜問題 ・指導要録原本 ・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・調剤の事実等の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の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 等	**業務に係る特定の職員に加えて、児童生徒又はその保護者が当該児童生徒の情報に限定して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・調剤の事実等の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 等	
Ⅱ	セキュリティ侵害が教育行政、学校事務又は教育活動の実施に重大な影響を及ぼす情報。ただし、重要性Ⅰに該当する情報を除く。	**業務に係る特定の職員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） ・職員及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（Ⅰを除く） ・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） ・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 ・転退学、転入学、就学、休学等に関する情報 ・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 等	**業務に係る特定の職員に加えて、児童生徒又はその保護者が当該児童生徒の情報に限定して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（Ⅰを除く） ○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 等	

情報資産の分類		情報資産の例示（アクセス主体別）		
重要性	定義	職員	職員・児童生徒・保護者	不特定多数
Ⅲ	セキュリティ侵害が教育行政、学校事務又は教育活動の実施に軽微な影響を及ぼす情報。ただし、重要性Ⅱ以上に該当する情報を除く。	**職員全員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） ・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） ・出席簿 ・保護者からの欠席連絡 等	**職員全員に加えて、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 ・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（確認プリント、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 ・児童生徒配布プリント 等	
Ⅳ	セキュリティ侵害が教育行政、学校事務又は教育活動の実施に影響をほとんど及ぼさない情報。ただし、重要性Ⅲ以上に該当する情報を除く。	**職員全員がアクセスすることが想定される、Ⅲ以上を除く情報**	**職員全員に加えて、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 ・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） 等