令　和　８　年　第　４　回

教育委員会定例会教育長報告

令和８年４月１７日（金）

１	武蔵村山市情報セキュリティポリシーの改定及び基本方針の公表に係る経過について	資料１
２	令和７年度区域外就学の状況について	資料２
３	令和７年度学校選択制の結果（令和８年度入学）について	資料３
４	令和８年度児童・生徒数及び学級数の状況について	資料４
５	令和８年度小・中学校等の教職員数及び令和８年度教職員の異動状況について	資料５
６	武蔵村山市立学校令和８年度行事予定等一覧について	資料６
７	令和８年度武蔵村山市立学校研究活動等一覧について	資料７
８	～いきいきわくわく狭山丘陵ウォーク～第４９回武蔵村山市歩け歩け大会の開催について	資料８
９	令和８年度 蔵書点検に伴う臨時休館について	資料９
10	その他	

資料１－１

武蔵村山市情報セキュリティ基本方針

１　目的

本基本方針は、本市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、本市が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。

２　定義

⑴　ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

⑵　情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

⑶　情報セキュリティ

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。

⑷　情報セキュリティポリシー

本基本方針及び行政機関等が別に定める情報セキュリティ対策基準（以下「対策基準」という。）をいう。

⑸　機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

⑹　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。

⑺　可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

⑻　マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税又は防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

⑼　LGWAN 接続系

LGWAN に接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。

⑽　インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

⑾　通信経路の分割

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

⑿　無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

３　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。

⑴　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

⑵　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、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

⑶　地震、落雷、火災等の災害によるサービス及び業務の停止等

⑷　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

⑸　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

⑴　行政機関等の範囲

本基本方針が適用される行政機関等は、市長部局及び市の行政委員会等（議会、教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会、市立小学校及び市立中学校をいう。）とする。

⑵　適用を受ける者

本基本方針の適用を受ける者は、前号に掲げる行政機関等に属する地方公務員法（昭和２５年法律第２６１号）第３条第２項に規定する一般職の職員及び同条第３項に規定する特別職の職員並びに教育公務員特例法（昭和２４年法律第１号）第２条第１項に規定する教育公務員のうち、当該行政機関等の情報資産を取り扱う者（以下「職員等」という。）とする。

⑶　情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

ア　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

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

ウ　情報システムの仕様書及びネットワーク図等のシステム関連文書

５　職員等の遵守義務

職員等は、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情報セキュリティポリシー及び情報セキュリティ実施手順（以下「実施手順」という。）を遵守しなければならない。

６　情報セキュリティ対策

上記３の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。

⑴　組織体制

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横断的な体制を確立する。

⑵　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。

⑶　情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

ア　マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

イ　LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

ウ　インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

⑷　物理的セキュリティ

サーバ、電算室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

⑸　人的セキュリティ

情報セキュリティに関し、職員等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。

⑹　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。

⑺　運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、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、「武蔵村山市業務継続計画（ＩＣＴ編）」等により、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な対応を可能とするための危機管理対策を行う。

⑻　業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託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確認し、必要に応じて契約に基づき措置を講じる。

外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

⑼　評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ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。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

７　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

８　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティ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新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

９　対策基準と実施手順の策定

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。

また、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業務担当課において策定するものとする。

なお、対策基準及び実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから原則として非公開とする。

資料１－２

武蔵村山市情報セキュリティ対策基準

１　目的

武蔵村山市情報セキュリティ対策基準（以下「対策基準」という。）は、武蔵村山市情報セキュリティ基本方針を実行に移すための、本市における情報セキュリティを確保するために遵守すべき行為及び判断等、情報セキュリティ対策を行う上で必要となる基本的な要件を規定し、円滑な行政運営を図ることを目的に策定するものとする。

２　適用範囲

⑴　行政機関等の範囲

本対策基準が適用される行政機関等は、市長部局及び市の行政委員会等（議会、教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会、市立小学校及び市立中学校をいう。）とする。

⑵　適用を受ける者

本対策基準の適用を受ける者は、行政機関等に属する地方公務員法（昭和２５年法律第２６１号）第３条第２項に規定する一般職の職員及び同条第３項に規定する特別職の職員並びに教育公務員特例法（昭和２４年法律第１号）第２条第１項に規定する教育公務員であって行政委員会等が別に定める者を除いた者（以下「職員等」という。）とする。

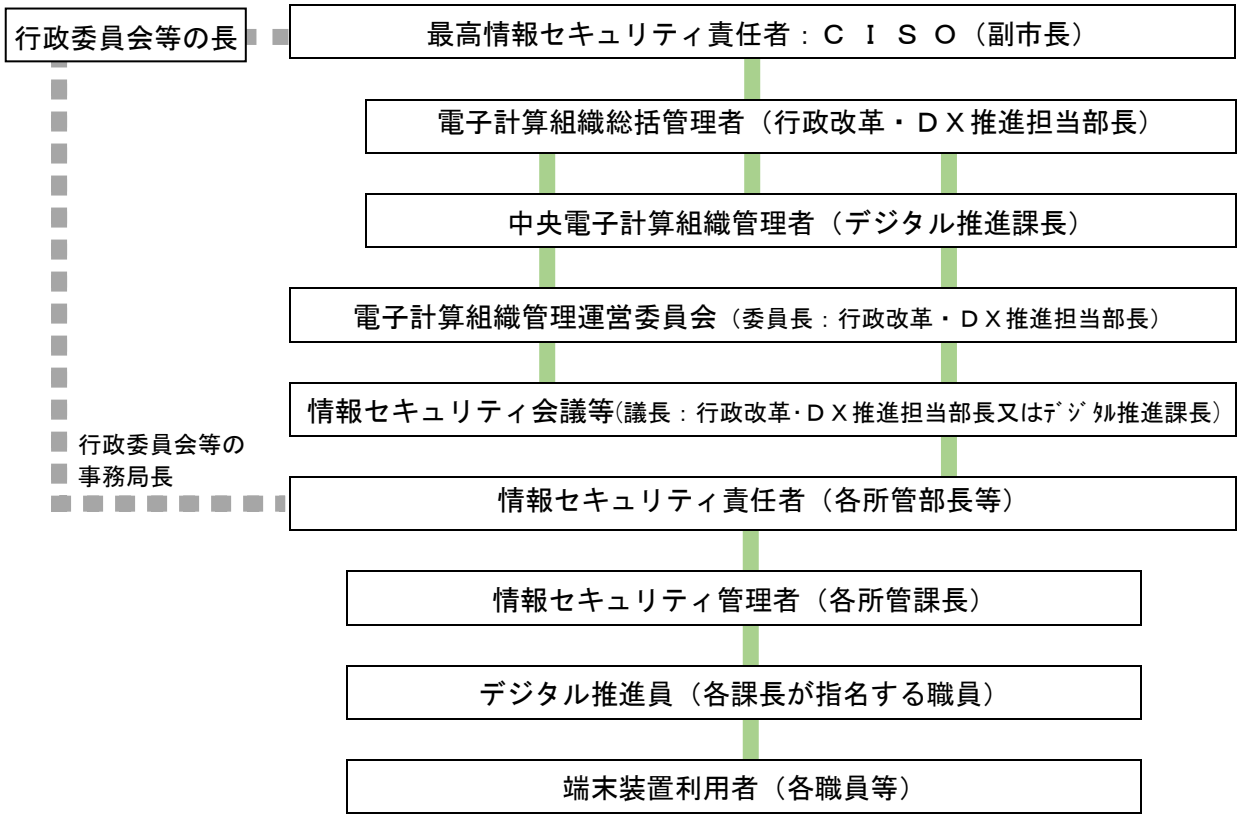
⑶　情報資産の範囲

本対策基準が対象とする情報資産は、基本方針で定める情報資産のうち、行政委員会等が別に定める情報資産を除いたものとする。

３　組織体制

⑴　情報セキュリティ対策の管理体制

本市における情報セキュリティ対策を組織全体で継続的に実施するための管理体制を整備する。



⑵　役割と責務

ア　最高情報セキュリティ責任者（CISO: Chief Information Security Officer、以下「CISO」という。）（副市長）

(ｱ)　副市長を CISO とする。CISO は、本市における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

(ｲ)　CISO は、必要に応じ、業務内容を定めた上で情報セキュリティに関する専門的な知識及び経験を有した専門家を、最高情報セキュリティアドバイザーとして置くことができる。

(ｳ)　CISO は、情報セキュリティインシデントに対処するための体制（CSIRT：Computer Security Incident Response Team）を整備し、役割を明確化する。

(ｴ)　CISO は、CISO を助けて本市における情報セキュリティに関する事務を整理し、CISO の命を受けて本市の情報セキュリティに関する事務を総括する最高情報セキュリティ副責任者（以下「副 CISO」という。）１人を必要に応じて置くことができる。

(ｵ)　CISO は、本対策基準に定められた自らの担務を、副 CISO その他の本対策基準に定める責任者に担わせることができる。

イ　電子計算組織総括管理者（行政改革・ＤＸ推進担当部長）

(ｱ)　行政改革・ＤＸ推進担当部長を電子計算組織総括管理者とする。

(ｲ)　CISO 及び副 CISO を補佐し、CISO 及び副 CISO が不在の場合には自らの判断に基づき、必要な措置を行う。

(ｳ)　本市の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

(ｴ)　本市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総合的な権限及び責任を有する。

(ｵ)　中央電子計算組織管理者、情報セキュリティ責任者、情報セキュリティ管理者及び端末装置利用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。

(ｶ)　本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISO の指示に従い、CISO が不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。

(ｷ)　本市の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

(ｸ)　武蔵村山市業務継続計画（ＩＣＴ編）の策定及び管理を行う。

(ｹ)　緊急時等の円滑な情報共有を図るため、CISO、電子計算組織総括管理者、中央電子計算組織管理者、情報セキュリティ責任者及び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。

(ｺ)　機密性の高い情報資産に対するセキュリティ侵害が発生した又はセキュリティ侵害のおそれがある場合には、CISO に早急に報告を行うとともに、武蔵村山市情報セキュリティ会議（以下「情報セキュリティ会議」という。）を招集する。

(ｻ)　情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて CISO にその内容を報告しなければならない。

ウ　中央電子計算組織管理者（デジタル推進課長）

(ｱ)　企画財政部デジタル推進課長を中央電子計算組織管理者とする。

(ｲ)　電子計算組織総括管理者を補佐し、電子計算組織総括管理者が不在の場合には必要な措置を行う。

(ｳ)　機密性の低い情報資産に対するセキュリティ侵害が発生した又はセキュリティ侵害のおそれがある場合には、電子計算組織総括管理者に早急に報告を行うとともに、武蔵村山市緊急対策会議（以下「緊急対策会議」という。）を招集する。

エ　情報セキュリティ責任者（各所管部長等）

(ｱ)　各所管部長及び行政委員会等の事務局の長を情報セキュリティ責任者とする。

(ｲ)　当該部局等の情報セキュリティ対策に関する総括的な権限及び責任を有する。

(ｳ) 当該部局等に属する情報セキュリティ管理者から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との報告を受けた場合には、電子計算組織総括管理者に速やかに報告する。なお、行政委員会等の情報セキュリティ責任者においては、行政委員会等の長にも速やかに報告する。

(ｴ) 当該部局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う総括的な権限及び責任を有する。

(ｵ) 当該部局等において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約並びに職員等に対する教育、訓練、助言及び指示を行う。

オ 情報セキュリティ管理者（各所管課長）

(ｱ) 各所管課長を情報セキュリティ管理者とする。

(ｲ) 当該所属する課の職員等に対して、情報セキュリティ対策に関する教育、指導及び啓発を行う。

(ｳ) 所掌す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、情報セキュリティ責任者及び中央電子計算組織管理者に速やかに報告する。

(ｴ) 所管する情報システムに関して、中央電子計算組織管理者の指示等に従い、開発、設定の変更、運用、更新等を行う。

カ デジタル推進員（各課長が指名する職員等）

各所属長の指名に基づき任命された職員等をデジタル推進員とし、情報セキュリティ対策の啓発及び普及、DX 施策の推進及び情報通信技術の事務処理への活用並びに端末装置等の操作指導に係る連絡調整を行う。

キ 端末装置利用者（各職員等）

情報資産に携わる職員等は、情報セキュリティポリシーに定める事項を遵守する。

ク 電子計算組織管理運営委員会（委員長：行政改革・ＤＸ推進担当部長）

(ｱ) 武蔵村山市電子計算組織の管理運営に関する規則第３条の規定に基づいて設置する。

(ｲ) 本市の情報セキュリティの維持管理を統一的な視点で行うため、情報セキュリティポリシー等の情報セキュリティ対策に関する重要な事項を審議する。

⑶ 兼務の禁止

ア 情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

イ 情報セキュリティ監査の実施において、やむを得ない場合を除き、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

⑷ 情報セキュリティインシデントへの対応

ア 情報セキュリティ会議等（議長：行政改革・ＤＸ推進担当部長又はデジタル推進課長）

(ｱ) 武蔵村山市情報セキュリティ会議等設置要綱第１条の規定に基づいて設置する。

(ｲ) 本市のネットワーク電子計算組織において障害又は不正行為（以下「緊急事態」という。）が発生し又は発生するおそれがある場合に、迅速かつ的確な対応を実施するため、緊急事態の区分に応じ、情報セキュリティ会議又は緊急対策会議（以下「情報セキュリティ会議等」という。）において対策を決定する。

(ｳ) 次に掲げる事項を所掌する。

a 緊急事態の状況の把握に関すること。

b 緊急事態の復旧作業体制の確立に関すること。

c 関係諸団体への連絡及び技術的支援依頼に関すること。

d 代替措置の決定に関すること。

e 住民対応方法の決定に関すること。

f 前各号に掲げるもののほか、緊急事態の対策に関すること。

イ　情報セキュリティに関する統一的な窓口

(ｱ)　デジタル推進課を、情報セキュリティインシデントの統一的な窓口の機能を有する組織とし、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、CISO 及び電子計算組織総括管理者への報告を行うものとする。

(ｲ)　情報セキュリティ会議等は、情報セキュリティインシデントを認知した場合には、総務省、東京都等へ報告しなければならない。

(ｳ)　情報セキュリティ会議等は、情報セキュリティインシデントを認知した場合には、その重要度や影響範囲などを勘案し、報道機関への通知・公表対応を行わなければならない。

(ｴ)　電子計算組織管理運営委員会は、CISO による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供しなければならない。

(ｵ)　デジタル推進課は、情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、委託事業者等との情報共有を行う。情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、発生した情報セキュリティインシデントを正確に把握・分析し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行う。

４　情報資産の分類と管理

⑴　情報資産の分類

本市における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

【機密性による情報資産の分類】

分類	分類基準	取扱制限
自治体機密性３Ａ	行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」（平成２３年４月１日内閣総理大臣決定）に定める秘密文書に相当する文書	・支給された端末以外での作業の原則禁止（自治体機密性３の情報資産に対して） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
自治体機密性３Ｂ	行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	
自治体機密性３Ｃ	行政事務で取り扱う情報資産のうち、自治体機密性３B 以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	
自治体機密性２	行政事務で取り扱う情報資産のうち、自治体機密性３に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
自治体機密性１	自治体機密性２又は自治体機密性３の情報資産以外の情報資産	―

【完全性による情報資産の分類】

分類	分類基準	取扱制限
自治体 完全性２	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
自治体 完全性１	自治体完全性２の情報資産以外の情報資産	―

【可用性による情報資産の分類】

分類	分類基準	取扱制限
自治体 可用性２	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
自治体 可用性１	自治体可用性２の情報資産以外の情報資産	―

⑵　情報資産の管理

ア　管理責任

(ｱ)　中央電子計算組織管理者及び情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

(ｲ)　中央電子計算組織管理者及び情報セキュリティ管理者は、所管する情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳を整備しなければならない。

(ｳ)　中央電子計算組織管理者及び情報セキュリティ管理者は、情報資産が複製又は伝送された場合には、複製等された情報資産も⑴の分類に基づき管理しなければならない。

イ　情報資産の分類の表示

職員等は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

ウ　情報の作成

(ｱ)　職員等は、業務上必要のない情報を作成してはならない。

(ｲ)　情報を作成する者は、情報の作成時に⑴の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

(ｳ)　情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

エ　情報資産の入手

(ｱ)　職員等が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

(ｲ)　職員等以外の者が作成した情報資産を入手した者は、⑴の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

(ｳ)　情報資産を入手した者は、入手した情報資産の分類が不明な場合、中央電子計算組織管理者に判断を仰がなければならない。

オ　情報資産の利用

(ｱ)　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

(ｲ)　情報資産を利用する者は、情報資産の分類に応じ、適正な取扱いをしなければならない。

(ｳ)　情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

カ　情報資産の保管

(ｱ)　中央電子計算組織管理者及び情報セキュリティ管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

(ｲ)　中央電子計算組織管理者及び情報セキュリティ管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

(ｳ)　中央電子計算組織管理者及び情報セキュリティ管理者は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。

(ｴ)　中央電子計算組織管理者及び情報セキュリティ管理者は、自治体機密性２以上、自治体完全性２又は自治体可用性２の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

キ　情報の送信

電子メール等により自治体機密性２以上の情報を送信する者は、必要に応じ、パスワード等による暗号化を行わなければならない。

ク　情報資産の運搬

(ｱ)　車両等により自治体機密性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、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)　自治体機密性２以上の情報資産を運搬する者は、中央電子計算組織管理者又は情報セキュリティ管理者に許可を得なければならない。

ケ　情報資産の提供・公表

(ｱ)　自治体機密性２以上の情報資産を外部に提供する者は、必要に応じパスワード等による暗号化を行わなければならない。

(ｲ)　自治体機密性２以上の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

(ｳ)　情報セキュリティ管理者は、住民に公開する情報資産について、完全性を確保しなければならない。

コ　情報資産の廃棄等

(ｱ)　情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。

(ｲ)　情報資産の廃棄やリース返却等を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

(ｳ)　情報資産の廃棄やリース返却等を行う者は、情報セキュリティ管理者の許可を得なければならない。

５　情報システム全体の強靭性の向上

⑴　マイナンバー利用事務系

ア　マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定（ＭＡＣアドレス、ＩＰアドレス）及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、

この限りではなく、LGWAN を経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

イ　情報のアクセス及び持ち出しにおける対策

(ｱ)　情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。また、業務ごとに専用端末を設置することが望ましい。

(ｲ)　情報の持ち出し不可設定

原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

⑵　LGWAN 接続系

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

ア　インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送するメールテキスト化方式

イ　インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

ウ　危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

⑶　インターネット接続系

ア　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と対処及び 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。

イ　都道府県及び市区町村のインターネットとの通信を集約する自治体情報セキュリティクラウドに参加するとともに、関係省庁や都道府県等と連携しながら、情報セキュリティ対策を推進しなければならない。

６　物理的セキュリティ

６．１　サーバ等の管理

⑴　機器の取付け

中央電子計算組織管理者は、サーバ等の機器の取付けを行う場合、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し、容易に取り外せないよう適正に固定する等、必要な措置を講じなければならない。

⑵　サーバの冗長化

ア　中央電子計算組織管理者は、重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバを冗長化し、同一データを保持しなければならない。

イ　中央電子計算組織管理者は、サーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。

⑶　機器の電源

ア　中央電子計算組織管理者は、電子計算組織総括管理者及び施設管理部門と連携し、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、当該機器が適正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なければならない。

イ　中央電子計算組織管理者は、電子計算組織総括管理者及び施設管理部門と連携し、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。

⑷　通信ケーブル等の配線

ア　中央電子計算組織管理者は、施設管理部門と連携し、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　中央電子計算組織管理者は、主要な箇所の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、施設管理部門と連携して対応しなければならない。

ウ　中央電子計算組織管理者は、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正に管理しなければならない。

エ　中央電子計算組織管理者は、自ら又はデジタル推進課職員及び契約により操作を認められた委託事業者以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

⑸　機器の定期保守及び修理

ア　中央電子計算組織管理者は、自治体可用性２のサーバ等の機器の定期保守を実施しなければならない。

イ　中央電子計算組織管理者は、電磁的記録媒体を内蔵する機器を事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、中央電子計算組織管理者は、事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

⑹　庁外への機器の設置

中央電子計算組織管理者は、庁外にサーバ等の機器を設置する場合、CISO の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

⑺　機器の廃棄等

中央電子計算組織管理者及び情報セキュリティ管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

６．２　管理区域の管理

⑴　管理区域の構造等

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、当該機器等の管理及び運用を行うための部屋（以下「電算室」という。）や電磁的記録媒体の保管庫をいう。

イ　中央電子計算組織管理者は、管理区域を地階又は１階に設けてはならない。また、外部からの侵入が容易にできないように無窓の外壁にするよう努めなければならない。

ウ　中央電子計算組織管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

エ　中央電子計算組織管理者は、電算室内の機器等に、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。

オ　中央電子計算組織管理者は、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部を全て塞がなければならない。

カ　中央電子計算組織管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器及び電磁的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。

⑵　管理区域の入退室管理等

ア　中央電子計算組織管理者は、管理区域への入退室を許可された者のみに制限し、IC カード、指紋認証等の生体認証や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　職員等及び委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

ウ　中央電子計算組織管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

エ　中央電子計算組織管理者は、自治体機密性２以上の情報資産を扱うシステムを設置してい

る管理区域について、当該情報システムに関連しない、又は個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的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。

⑶　機器等の搬入出

ア　中央電子計算組織管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員等又は委託事業者に確認を行わせなければならない。

イ　中央電子計算組織管理者は、電算室の機器等の搬入出について、職員等を立ち会わせなければならない。

６．３　通信回線及び通信回線装置の管理

⑴　中央電子計算組織管理者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正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正に保管しなければならない。

⑵　中央電子計算組織管理者は、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施しなければならない。

⑶　中央電子計算組織管理者は、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。

⑷　中央電子計算組織管理者は、行政系のネットワークを LGWAN に集約するように努めなければならない。

⑸　中央電子計算組織管理者は、自治体機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

⑹　中央電子計算組織管理者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように、不正な通信の有無を監視する等の十分なセキュリティ対策を実施しなければならない。

⑺　中央電子計算組織管理者は、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順を定めなければならない。また、必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講じなければならない。

⑻　中央電子計算組織管理者は、自治体可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

６．４　職員等の利用する端末や電磁的記録媒体等の管理

⑴　中央電子計算組織管理者及び情報セキュリティ管理者は、盗難防止のため、執務室等で利用するパソコンのワイヤーによる固定、モバイル端末及び電磁的記録媒体の使用時以外の施錠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。

⑵　中央電子計算組織管理者は、情報システムへのログインに際し、パスワード、スマートカード、或いは生体認証等複数の認証情報の入力を必要とするように設定しなければならない。

⑶　中央電子計算組織管理者は、端末の電源起動時のパスワード（BIOS パスワード、ハードディスクパスワード等）を併用するよう努めなければならない。

⑷　中央電子計算組織管理者は、マイナンバー利用事務系では「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証）を行うよう設定しなければならない。

⑸　中央電子計算組織管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についてもデータ暗号化機能を備

える媒体を使用するよう努めなければならない。

⑹　中央電子計算組織管理者は、モバイル端末の庁外での業務利用の際は、上記対策に加え、遠隔消去機能を利用する等の措置を講じるよう努めなければならない。

7　人的セキュリティ

7．1　職員等の遵守事項

⑴　情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに中央電子計算組織管理者に相談し、指示を仰がなければならない。

⑵　業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、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。

⑶　個人情報を含むデータへのパスワード設定

職員等は、個人情報に関する電磁的記録を保存する場合（電磁的記録媒体に保存する場合を含む。）には、パスワードを設定しなければならない。

⑷　モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

ア　CISO は、自治体機密性２以上、自治体可用性２、自治体完全性２の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

イ　職員等は、本市のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

ウ　職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。

⑸　支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

ア　職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、支給以外の端末の業務利用の可否判断を CISO が行った後に、業務上必要な場合は、電子計算組織統括管理者の定める実施手順に従い、中央電子計算組織管理者の許可を得て利用することができる。

イ　職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置に関する規定を遵守しなければならない。

⑹　持ち出し及び持ち込みの記録

情報セキュリティ管理者は、端末等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。

⑺　パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を中央電子計算組織管理者の許可なく変更してはならない。

⑻　机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

⑼　退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

⑽　情報セキュリティポリシー等の掲示

中央電子計算組織管理者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

⑾　委託事業者に対する説明

中央電子計算組織管理者及び情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を事業者に発注する場合、再委託事業者も含めて、情報セキュリティポリシー等のうち委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

７．２　研修・訓練

⑴　情報セキュリティに関する研修・訓練

電子計算組織総括管理者は、定期的に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。

⑵　研修計画の策定及び実施

ア　電子計算組織総括管理者は、全ての職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行わなければならない。

イ　研修計画において、職員等は毎年度情報セキュリティ研修を受講できるように努めなければならない。

ウ　新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

エ　研修は、電子計算組織におけるそれぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

オ　中央電子計算組織管理者は、研修の実施状況を分析、評価し、電子計算組織総括管理者に情報セキュリティ対策に関する研修の実施状況について報告しなければならない。

カ　電子計算組織総括管理者は、電子計算組織管理運営委員会に対して、職員等の情報セキュリティ研修の実施状況について定期的に報告しなければならない。

⑶　緊急時対応訓練

CISO は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

⑷　研修・訓練への参加

全ての職員等は、定められた研修・訓練に参加しなければならない。

７．３　情報セキュリティインシデントの報告

⑴　庁内での情報セキュリティインシデントの報告

ア　職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者に報告しなければならない。

イ　報告を受けた情報セキュリティ管理者は、速やかに情報セキュリティ責任者及び中央電子計算組織管理者に報告しなければならない。

ウ　中央電子計算組織管理者は、報告のあった情報セキュリティインシデントについて、必要に応じて CISO 及び電子計算組織総括管理者に報告しなければならない。

なお、行政委員会等の情報セキュリティ責任者は、当該行政委員会等の長に速やかに報告しなければならない。

エ　情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報保護委員会へ報告しなければならない。

⑵　住民等外部からの情報セキュリティインシデントの報告

ア　職員等は、本市が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、速やかに情報セキュリティ管理者に報告しなければならない。

イ　報告を受けた情報セキュリティ管理者は、速やかに情報セキュリティ責任者及び中央電子計算組織管理者に報告しなければならない。

ウ　中央電子計算組織管理者は、当該情報セキュリティインシデントについて、必要に応じて CISO 及び電子計算組織総括管理者に報告しなければならない。なお、行政委員会等の情報セキュリティ責任者においては、行政委員会等の長にも速やかに報告しなければならない。

エ　CISO は、情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けるための窓口の設置と、当該窓口への連絡手段を公表するよう努めなければならない。

⑶　情報セキュリティ会議・緊急対策会議の招集

電子計算組織総括管理者及び中央電子計算組織管理者は、行政運営に及ぼす影響等に応じて情報セキュリティ会議又は緊急対策会議を招集しなければならない。

⑷　情報セキュリティインシデント原因の究明・記録、再発防止等

ア　情報セキュリティ会議等は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

イ　情報セキュリティ会議等は、情報セキュリティインシデントであると評価した場合、CISO にその詳細を速やかに報告しなければならない。

ウ　情報セキュリティ会議等は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。また、情報セキュリティ会議等は、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報セキュリティ責任者へ確認を指示しなければならない。

エ　情報セキュリティ会議等は、これらの情報セキュリティインシデント原因を究明し、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の結果から、再発防止策を検討し、CISO に報告しなければならない。

オ　CISO は、情報セキュリティ会議等から、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。

７．４　ＩＤ及びパスワード等の管理

⑴　IC カード等の取扱い

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

(ｱ)　認証に用いる IC カード等を、職員等間で共有してはならない。ただし、共有端末装置においてはこの限りではない。

(ｲ)　業務上必要のないときは、IC カード等をカードリーダ又はパソコン等の端末のスロット等から抜いておかなければならない。

(ｳ)　IC カード等を紛失した場合には、速やかに中央電子計算組織管理者に通報し、指示に従わなければならない。

イ　中央電子計算組織管理者は、IC カード等の紛失等の通報があり次第、当該 IC カード等を使用したアクセス等を速やかに停止しなければならない。

ウ　中央電子計算組織管理者は、IC カード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

⑵　ID の取扱い

職員等は、自己の管理する ID に関し、次の事項を遵守しなければならない。

ア　自己が利用している ID は、他人に利用させてはならない。

イ　共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

⑶　パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

ア　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。

イ　パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

ウ　パスワードは十分な長さとし、文字列は想像しにくいもの（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）にしなければならない。

エ　パスワードが流出したおそれがある場合には、中央電子計算組織管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

オ　複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。
カ　仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。
キ　サーバ、ネットワーク機器及びパソコン等の端末に、パスワードを記憶させることで、パスワードの入力なしに認証を可能とする設定は行ってはならない。
ク　職員等間でパスワードを共有してはならない（ただし、共用 ID に対するパスワードは除く）。

8　技術的セキュリティ

8．1　コンピュータ及びネットワークの管理

⑴　ファイルサーバの設定等

ア　中央電子計算組織管理者は、職員等が使用できるファイルサーバの容量を設定し、職員等に周知しなければならない。
イ　中央電子計算組織管理者は、ファイルサーバを課等の単位で構成し、職員等が他課等のフォルダ及びファイルを閲覧及び使用できないように設定しなければならない。
ウ　中央電子計算組織管理者は、住民の個人情報、人事記録等、特定の職員等しか取り扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一課室等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

⑵　バックアップの実施

ア　中央電子計算組織管理者及び情報セキュリティ管理者は、業務システムのデータベースやファイルサーバ等に記録された情報について、サーバの冗長化対策にかかわらず、必要に応じて定期的にバックアップを実施しなければならない。
イ　中央電子計算組織管理者及び情報セキュリティ管理者は、重要な情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得しなければならない。
ウ　中央電子計算組織管理者及び情報セキュリティ管理者は、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しなければならない。

⑶　他団体との情報システムに関する情報等の交換

中央電子計算組織管理者及び情報セキュリティ管理者は、他の団体と情報システムに関する情報（サーバやネットワークの設定等の情報）を交換する場合、その取扱いに関する事項をあらかじめ定め、電子計算組織総括管理者及び情報セキュリティ責任者の許可を得なければならない。

⑷　システム管理記録及び作業の確認

ア　中央電子計算組織管理者及び情報セキュリティ管理者は、所管する情報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。
イ　中央電子計算組織管理者及び情報セキュリティ管理者は、所管するシステムにおいて、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に適正に管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければならない。
ウ　職員等及び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。

⑸　情報システム仕様書等の管理

中央電子計算組織管理者及び情報セキュリティ管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体にかかわらず、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、適正に管理しなければならない。また、構築に際して事業者に委託した場合、当該事業者に守秘義務を課さなければならない。

⑹　ログの取得等

ア　中央電子計算組織管理者は、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し、

一定の期間保存しなければならない。

イ　中央電子計算組織管理者は、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、適正にログを管理しなければならない。

ウ　中央電子計算組織管理者は、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。また、必要に応じて情報セキュリティ担当者にアクセス記録を通知すること。

⑺　障害記録

中央電子計算組織管理者は、職員等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、適正に保存しなければならない。

⑻　ネットワークの接続制御、経路制御等

ア　中央電子計算組織管理者は、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、ファイアウォールや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。

イ　中央電子計算組織管理者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

ウ　中央電子計算組織管理者は、保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保しなければならない。また、情報セキュリティ対策について、定期的な確認により必要に応じて見直さなければならない。

⑼　外部の者が利用できるシステムの分離等

中央電子計算組織管理者は、電子申請の受付システム等、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

⑽　外部ネットワークとの接続制限等

ア　中央電子計算組織管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、CISO 及び電子計算組織総括管理者の許可を得なければならない。

イ　中央電子計算組織管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内の全てのネットワーク、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なければならない。

ウ　中央電子計算組織管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、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　中央電子計算組織管理者は、ウェブサーバ等をインターネットに公開する場合、次のセキュリティ対策を実施しなければならない。

(ｱ)　庁内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上で接続しなければならない。

(ｲ)　脆弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用しなければならない。

(ｳ)　ウェブサーバからの不用意な情報漏えいを防止するための措置を講じなければならない。

(ｴ)　ウェブコンテンツの編集作業を行う主体を限定しなければならない。

(ｵ)　インターネットを介して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よう努めなければならない。

オ　中央電子計算組織管理者及び情報セキュリティ管理者は、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、情報資産に脅威が生じることが想定される場合には、電子計算組織総括管理者の判断に従い、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。この場合、中央電子計算組織管理者は、電子計算組織総括管理者に報告するとと

もに、市長を通じ、武蔵村山市個人情報保護審議会に報告しなければならない。

⑾　複合機のセキュリティ管理

ア　中央電子計算組織管理者及び情報セキュリティ管理者は、複合機を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

イ　中央電子計算組織管理者及び情報セキュリティ管理者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

ウ　中央電子計算組織管理者及び情報セキュリティ管理者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消し、又は再利用できないようにする対策を講じなければならない。

⑿　IoT 機器を含む特定用途機器のセキュリティ管理

中央電子計算組織管理者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

⒀　無線 LAN のセキュリティ対策及びネットワークの盗聴対策

ア　中央電子計算組織管理者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

イ　中央電子計算組織管理者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

⒁　電子メールのセキュリティ管理

ア　中央電子計算組織管理者は、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（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

イ　中央電子計算組織管理者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。

ウ　中央電子計算組織管理者は、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不可能にしなければならない。

エ　中央電子計算組織管理者は、職員等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、上限を超えないよう職員等に周知しなければならない。

オ　中央電子計算組織管理者は、システム開発や運用、保守等のため庁舎内に常駐している委託事業者の作業員による電子メールアドレス利用について、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　中央電子計算組織管理者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように添付ファイルの監視等によりシステム上措置を講じるよう努めなければならない。

⒂　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、中央電子計算組織管理者及び情報セキュリティ管理者に報告しなければならない。

オ　ウェブで利用できる電子メール、ネットワークストレージサービス等を使用する場合は、中央電子計算組織管理者の許可を得なければならない。

⒃　電子署名・暗号化

ア　職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、CISO が定めた電子署名、パスワード等による暗

号化等、セキュリティを考慮して、送信しなければならない。

イ　職員等は、暗号化を行う場合に CISO が定める以外の方法を用いてはならない。また、CISO が定めた方法で暗号のための鍵を管理しなければならない。

ウ　CISO は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

⑰　無許可ソフトウェアの導入等の禁止

ア　職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

イ　職員等は、業務上の必要がある場合は、中央電子計算組織管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者は、ソフトウェアのライセンスを管理しなければならない。

ウ　職員等は、不正にコピーしたソフトウェアを利用してはならない。

エ　中央電子計算組織管理者は許可を行うに当たり、当該ソフトウェアがセキュリティ上安全であるか確認しなければならない。

オ　無許可で標準実装以外のアプリケーションソフトをパソコンにインストールし、又はデスクトップ等の設定を変更した職員等は、端末装置の使用を禁止する。

⑱　機器構成の変更の制限

ア　職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。

イ　職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、中央電子計算組織管理者及び情報セキュリティ管理者の許可を得なければならない。

⑲　業務外ネットワークへの接続の禁止

ア　職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう情報セキュリティ管理者によって定められたネットワークと異なるネットワークに接続してはならない。

イ　中央電子計算組織管理者は、支給した端末について、端末に搭載された OS のポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限することが望ましい。

⑳　業務以外の目的でのウェブ閲覧の禁止

ア　職員等は、業務以外の目的でウェブを閲覧してはならない。

イ　中央電子計算組織管理者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適正な措置を求めなければならない。

㉑　Web 会議サービスの利用時の対策

ア　電子計算組織総括管理者は、Web 会議を適切に利用するための利用手順を定めなければならない。

イ　職員等は、本市の定める利用手順に従い、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すること。

ウ　職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

エ　職員等は、外部から Web 会議に招待される場合は、本市の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。

㉒　ソーシャルメディアサービスの利用

ア　情報セキュリティ管理者は、本市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

(ｱ)　本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし

対策を実施すること。

(ｲ) パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ハードディスク、USB メモリ、紙等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること。

イ　自治体機密性２以上の情報はソーシャルメディアサービスで発信してはならない。

ウ　利用するソーシャルメディアサービスごとの責任者を定めなければならない。

エ　アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。

オ　自治体可用性２の情報の提供にソーシャルメディアサービスを用いる場合は、本市の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。

８．２　アクセス制御

⑴　アクセス制御等

ア　アクセス制御

中央電子計算組織管理者及び情報セキュリティ管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように必要最小限の範囲で適切に設定する等、システム上制限しなければならない。

イ　利用者 ID の取扱い

(ｱ) 中央電子計算組織管理者及び情報セキュリティ管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職に伴う利用者 ID の取扱い等の方法を定めなければならない。

(ｲ) 職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、中央電子計算組織管理者に通知しなければならない。

(ｳ) 中央電子計算組織管理者及び情報セキュリティ管理者は、利用されていない ID が放置されないよう、職員課と連携し、点検しなければならない。

(ｴ) 中央電子計算組織管理者及び情報セキュリティ管理者は、各ＩＤに対して不要なアクセス権限が付与されていないか定期的に確認しなければならない。

ウ　特権を付与された ID の管理等

(ｱ) 中央電子計算組織管理者及び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。

(ｲ) 中央電子計算組織管理者及び情報セキュリティ管理者は、管理者権限の特権を持つ ID 及びパスワードや主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講じなければならない。

(ｳ) 電子計算組織総括管理者及び中央電子計算組織管理者の管理者の特権を代行する者は、電子計算組織総括管理者が指名し、CISO が認めた者でなければならない。

(ｴ) CISO は、代行者を認めた場合、速やかに電子計算組織総括管理者、中央電子計算組織管理者、情報セキュリティ責任者及び情報セキュリティ管理者に通知しなければならない。

(ｵ) 中央電子計算組織管理者及び情報セキュリティ管理者は、特権を付与された ID 及びパスワードの変更について、委託事業者に行わせてはならない。

(ｶ) 中央電子計算組織管理者及び情報セキュリティ管理者は、特権を付与された ID 及びパスワードについて、人事異動の際のパスワードの変更、入力回数制限等のセキュリティ機能を強化しなければならない。

(ｷ) 中央電子計算組織管理者及び情報セキュリティ管理者は、特権を付与された ID を初期設定以外のものに変更しなければならない。

⑵　職員等による外部からのアクセス等の制限

ア　職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、中央電子計算組織管理者及び当該情報システムを管理する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　電子計算組織総括管理者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、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　電子計算組織総括管理者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

エ　電子計算組織総括管理者は、外部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。

オ　電子計算組織総括管理者及び中央電子計算組織管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、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。

カ　職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁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、パッチの適用状況等を確認し、情報セキュリティ管理者の許可を得るか、又は情報セキュリティ管理者によって事前に定義されたポリシーに従って接続しなければならない。

キ　電子計算組織総括管理者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者の ID、パスワード及び生体認証に係る情報等の認証情報並びにこれを記録した媒体（IC カード等）による認証に加えて通信内容の暗号化等、情報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。

⑶　自動識別の設定

中央電子計算組織管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

⑷　ログイン時の表示等

中央電子計算組織管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・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。

⑸　認証情報の管理

ア　中央電子計算組織管理者は、職員等の認証情報を厳重に管理しなければならない。認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

イ　中央電子計算組織管理者及び情報セキュリティ管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回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。

ウ　中央電子計算組織管理者及び情報セキュリティ管理者は、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。

⑹　特権による接続時間の制限

中央電子計算組織管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

８．３　システム開発、導入、保守等

⑴　機器等の調達に係る運用規程の整備

ア　中央電子計算組織管理者は、機器等の選定基準を運用規程として整備しなければならない。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加

えられないような対策を講じなければならない。

イ　中央電子計算組織管理者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備しなければならない。

⑵　機器等及び情報システムの調達

ア　中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムの開発に当たっては、武蔵村山市情報システム調達基本方針を遵守しなければならない。

イ　中央電子計算組織管理者及び情報セキュリティ管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。また、業務システムに誤ったプログラムが組み込まれないよう、不具合等を考慮した技術的なセキュリティ機能を調達仕様書に記載しなければならない。

ウ　中央電子計算組織管理者及び情報セキュリティ管理者は、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問題のないことを確認しなければならない。

⑶　情報システムの開発

ア　システム開発における責任者及び作業者の特定

中央電子計算組織管理者及び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を特定しなければならない。また、システム開発のための規則を確立しなければならない。

イ　システム開発における責任者、作業者の ID の管理

(ｱ)　中央電子計算組織管理者及び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 ID を管理し、開発完了後、開発用 ID を削除しなければならない。

(ｲ)　中央電子計算組織管理者及び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のアクセス権限を設定しなければならない。

ウ　システム開発に用いるハードウェア及びソフトウェアの管理

(ｱ)　中央電子計算組織管理者及び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、それ以外のものを使用させてはならない。

(ｲ)　中央電子計算組織管理者及び情報セキュリティ管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

エ　アプリケーション・コンテンツの開発時の対策

中央電子計算組織管理者及び情報セキュリティ管理者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。

⑷　情報システムの導入

ア　開発環境と運用環境の分離及び移行手順の明確化

(ｱ)　中央電子計算組織管理者及び情報セキュリティ管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。

(ｲ)　中央電子計算組織管理者及び情報セキュリティ管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

(ｳ)　中央電子計算組織管理者及び情報セキュリティ管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

(ｴ)　中央電子計算組織管理者及び情報セキュリティ管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

イ　テスト

(ｱ)　中央電子計算組織管理者及び情報セキュリティ管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分なテストを行わなければな

らない。

(ｲ)　中央電子計算組織管理者及び情報セキュリティ管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

(ｳ)　中央電子計算組織管理者及び情報セキュリティ管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

(ｴ)　中央電子計算組織管理者及び情報セキュリティ管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

(ｵ)　中央電子計算組織管理者及び情報セキュリティ管理者は、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮したテスト計画を策定し、確実に検証が実施されるよう、必要かつ適切に委託事業者の監督を行わなければならない。

ウ　機器等の納入時又は情報システムの受入れ時

(ｱ)　中央電子計算組織管理者及び情報セキュリティ管理者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認しなければならない。

(ｲ)　中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。

⑸　情報システムの基盤を管理又は制御するソフトウェア導入時の対策

ア　中央電子計算組織管理者及び情報セキュリティ管理者は、ソフトウェアを導入する端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置を講じるよう努めなければならない。

イ　中央電子計算組織管理者及び情報セキュリティ管理者は、利用するソフトウェアの特性を踏まえ、以下の全ての実施手順を整備しなければならない。

(ｱ)　情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順

(ｲ)　情報システムの基盤を管理又は制御するソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順

⑹　情報システムの基盤を管理又は制御するソフトウェア運用時の対策

ア　中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムの基盤を管理又は制御するソフトウェアを運用・保守する場合は、以下の全てのセキュリティ対策を実施するよう努めなければならない。

(ｱ)　情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するための対策

(ｲ)　脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策

イ　中央電子計算組織管理者及び情報セキュリティ管理者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行わなければならない。

⑺　システム開発・保守に関連する資料等の整備・保管

ア　中央電子計算組織管理者及び情報セキュリティ管理者は、システム開発・保守に関連する資料及びシステム関連文書を適正に整備・保管しなければならない。

(ｱ)　中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について電子計算組織総括管理者に報告しなければならない。

(ｲ)　中央電子計算組織管理者及び情報セキュリティ管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む情報システム関連文書を整備するよう努めなければならない。

・情報システムを構成するサーバ装置及び端末関連情報

・情報システムを構成する通信回線及び通信回線装置関連情報

(ｳ) 中央電子計算組織管理者及び情報セキュリティ管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む実施手順を整備しなければならない。

・情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順

・情報セキュリティインシデントを認知した際の対処手順

・情報システムが停止した際の復旧手順

イ 中央電子計算組織管理者及び情報セキュリティ管理者は、テスト結果を一定期間保管しなければならない。

ウ 中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

⑻ 情報システムにおける入出力データの正確性の確保

ア 中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムに入力されるデータについて、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組み込むように情報システムを設計しなければならない。

イ 中央電子計算組織管理者及び情報セキュリティ管理者は、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。

(ｱ) 利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直さなければならない。

(ｲ) 運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じなければならない。

(ｳ) ウェブアプリケーション・コンテンツにおいて、故意又は過失により情報が改ざんされる、又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

ウ 中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

⑼ 情報システムの変更管理

中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

⑽ 開発・保守用のソフトウェアの更新等

中央電子計算組織管理者及び情報セキュリティ管理者は、開発・保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

⑾ システム更新又は統合時の検証等

中央電子計算組織管理者及び情報セキュリティ管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

⑿ 情報システムについての対策の見直し

中央電子計算組織管理者及び情報セキュリティ管理者は、対策の推進計画等に基づき情報システムの情報セキュリティ対策を適切に見直さなければならない。また、本市内で横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直さなければならない。なお、措置の結果については、電子計算組織総括管理者に報告しなければならない。

８．４ 不正プログラム対策

⑴ 中央電子計算組織管理者の措置事項

中央電子計算組織管理者は、不正プログラム対策として、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ファイルは、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、不正プログラムのシステムへ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ファイルは、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　コンピュータ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　所掌するサーバ及びパソコン等の端末に、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。

オ　不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

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

キ　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。また、当該製品の利用を予定している期間中に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する予定がないことを確認しなければならない。

⑵　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　所掌するサーバ及びパソコン等の端末に、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システムに常駐させなければならない。

イ　不正プログラム対策ソフトウェアのパターンファイルは、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のソフトウェアは、常に最新の状態に保たなければならない。

エ　インターネットに接続していないシステムにおいて、電磁的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、市が管理している媒体以外を職員等に利用させてはならない。また、不正プログラムの感染、侵入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パターンファイルの更新を実施しなければならない。

オ　不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報セキュリティ管理者が許可した職員を除く職員等に当該権限を付与してはならない。

⑶　職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

ア　パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

イ　外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

ウ　差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

エ　端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

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でチェックを行わなければならない。インターネット接続系で受信したインターネット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。

カ　中央電子計算組織管理者が提供するウイルス情報を、常に確認しなければならない。

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又は感染が疑われる場合は、事

前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末においてLANケーブルの取り外しや、通信を行わない設定への変更などを実施しなければならない。

⑷　専門家の支援体制

中央電子計算組織管理者及び情報セキュリティ管理者は、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、外部の専門家の支援を受けられるようにしておかなければならない。

８．５　不正アクセス対策

⑴　中央電子計算組織管理者の措置事項

中央電子計算組織管理者は、不正アクセス対策として、以下の事項を措置しなければならない。

ア　使用されていないポートを閉鎖しなければならない。

イ　不要なサービスについて、機能を削除又は停止しなければならない。

ウ　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に、データの書換えを検出し、中央電子計算組織管理者及び担当職員等が属する課の情報セキュリティ管理者へ通報するよう、設定しなければならない。

エ　重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。

オ　中央電子計算組織管理者は、電子計算組織管理運営委員会と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

⑵　攻撃への対処

電子計算組織総括管理者及び中央電子計算組織管理者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、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、総務省、東京都等と連絡を密にして情報の収集に努めなければならない。

⑶　記録の保存

電子計算組織総括管理者及び中央電子計算組織管理者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、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。

⑷　内部からの攻撃

電子計算組織総括管理者及び中央電子計算組織管理者は、職員等及び委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

⑸　職員等による不正アクセス

電子計算組織総括管理者及び中央電子計算組織管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課等の情報セキュリティ管理者に通知し、適正な処置を求めなければならない。

⑹　サービス不能攻撃

電子計算組織総括管理者及び中央電子計算組織管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

⑺　標的型攻撃

電子計算組織総括管理者及び中央電子計算組織管理者は、標的型攻撃による内部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、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、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対策（内部対策及び出口対策）を講じなければならない。

８．６　セキュリティ情報の収集

⑴　セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

電子計算組織総括管理者及び中央電子計算組織管理者は、サーバ装置、端末及び通信回線装置等におけるセキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

⑵　不正プログラム等のセキュリティ情報の収集・周知

電子計算組織総括管理者及び中央電子計算組織管理者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。

⑶　情報セキュリティに関する情報の収集及び共有

電子計算組織総括管理者及び中央電子計算組織管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、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。

９　　運用

９．１　情報システムの監視

⑴　情報システムの運用・保守時の対策

ア　中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用しなければならない。

イ　中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。

ウ　中央電子計算組織管理者及び情報セキュリティ管理者は、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をしなければならない。

⑵　情報システムの監視機能

ア　中央電子計算組織管理者は、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装しなければならない。

イ　中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用しなければならない。

ウ　中央電子計算組織管理者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直さなければならない。

エ　中央電子計算組織管理者及び情報セキュリティ管理者は、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講じなければならない。

⑶　情報システムの監視

ア　中央電子計算組織管理者及び情報セキュリティ管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

イ　中央電子計算組織管理者及び情報セキュリティ管理者は、重要なログ等を取得するサーバの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。

ウ　中央電子計算組織管理者及び情報セキュリティ管理者は、外部と常時接続するシステムを常時監視しなければならない。

エ　中央電子計算組織管理者及び情報セキュリティ管理者は、暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入するよう努めなければならない。

９．２　情報セキュリティポリシーの遵守状況の確認

⑴　遵守状況の確認及び対処

ア　情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに CISO 及び電子計算組織総括管理者に報告しなければならない。

イ　CISO は、発生した問題について、適正かつ速やかに対処しなければならない。

ウ　中央電子計算組織管理者及び情報セキュリティ管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

⑵　パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

ア　CISO 及び CISO が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

イ　法令等で定められた個人情報の保護に関する情報の閲覧に関しては、当該法令等で定められた手続に従わなければならない。

ウ　中央電子計算組織管理者及び中央電子計算組織管理者が指名した者は、知り得た情報を他に漏らしてはならない。

⑶　職員等の報告義務

ア　職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに中央電子計算組織管理者及び情報セキュリティ管理者に報告を行わなければならない。

イ　違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると中央電子計算組織管理者が判断した場合は、武蔵村山市業務継続計画（ＩＣＴ編）に従って適正に対処しなければならない。

９．３　侵害時の対応等

⑴　武蔵村山市業務継続計画（ＩＣＴ編）の策定

CISO 又は電子計算組織管理運営委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合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正に実施するために、武蔵村山市業務継続計画（ＩＣＴ編）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。

⑵　武蔵村山市業務継続計画（ＩＣＴ編）に盛り込むべき内容

武蔵村山市業務継続計画（ＩＣＴ編）には、以下の内容を定めなければならない。

ア　関係者の連絡先

イ　発生した事案に係る報告すべき事項

ウ　発生した事案への対応措置

エ　再発防止措置の策定

⑶　武蔵村山市業務継続計画（ＩＣＴ編）との整合性確保

電子計算組織管理運営委員会は、自然災害、大規模・広範囲にわたる疾病等に備えて策定した武蔵村山市業務継続計画（ＩＣＴ編）と情報セキュリティポリシーの整合性を確保しなければならない。

⑷　武蔵村山市業務継続計画（ＩＣＴ編）の見直し

CISO 又は電子計算組織管理運営委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて武蔵村山市業務継続計画（ＩＣＴ編）の規定を見直さなければならない。

９．４　例外措置

⑴　例外措置の許可

電子計算組織総括管理者及び情報セキュリティ責任者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政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する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、CISO の許可を得て、例外措置を取ることができる。

⑵　緊急時の例外措置

電子計算組織総括管理者及び情報セキュリティ責任者は、行政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、事後速やかに CISO に報告しなければならない。

⑶　例外措置の申請書の管理

CISO は、例外措置の申請書及び審査結果を適正に保管し、定期的に申請状況を確認しなければならない。

９．５　法令遵守

職員等は、職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。

⑴　地方公務員法（昭和２５年法律第２６１号）
⑵　著作権法（昭和４５年法律第４８号）
⑶　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）
⑷　個人情報の保護に関する法律（平成１５年法律第５７号）
⑸　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）
⑹　サイバーセキュリティ基本法（平成２６年法律第１０４号）
⑺　武蔵村山市個人情報の保護に関する法律施行条例（令和４年条例第３０号）

９．６　懲戒処分等

⑴　懲戒処分

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

⑵　違反時の対応

職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

ア　電子計算組織総括管理者又は中央電子計算組織管理者が違反を確認した場合は、中央電子計算組織管理者は当該職員等が所属する部等の情報セキュリティ責任者及び情報セキュリティ管理者に通知し、適正な措置を求めなければならない。

イ　職員等が違反を確認した場合は、違反を確認した者は速やかに中央電子計算組織管理者及び当該職員等が所属する課等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。

ウ　情報セキュリティ責任者及び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、電子計算組織総括管理者は、当該職員等のネットワーク又は情報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。電子計算組織総括管理者は、その後速やかに、職員等の権利を停止あるいは剥奪した旨を CISO と当該職員等が所属する部の情報セキュリティ責任者及び情報セキュリティ管理者に通知しなければならない。

10　業務委託と外部サービス（クラウドサービス）の利用

１０．１　業務委託

⑴　業務委託に係る運用規定の整備

電子計算組織総括管理者は、業務委託に係る以下の内容を全て含む運用規定を整備しなければならない。

ア　委託事業者への提供を認める情報及び委託する業務の範囲を判断する基準（以下「委託判断基準」という。）

イ　委託事業者の選定基準

⑵　業務委託実施前の対策

ア　中央電子計算組織管理者及び情報セキュリティ管理者は、業務委託の実施までに、以下を全て含む事項を実施しなければならない。

(ｱ)　委託する業務内容の特定

(ｲ)　委託事業者の選定条件を含む仕様の策定

(ｳ)　仕様に基づく委託事業者の選定

(ｴ)　情報セキュリティ要件を明記した契約の締結（契約項目）

重要な情報資産を取扱う業務を委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ等に係る要件を明記した契約を締結しなければならない。

・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
・個人情報漏えい防止のための技術的安全管理措置に関する取り決め
・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
・提供されるサービスレベルの保証
・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法
・委託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委託事業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
・市による監査・検査
・市による情報セキュリティインシデント発生時の公表
・情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

(ｵ)　委託事業者に重要情報を提供する場合は、秘密保持契約（ＮＤＡ）の締結

イ　中央電子計算組織管理者及び情報セキュリティ管理者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託事業者に求めなければならない。

(ｱ)　仕様に準拠した提案

(ｲ)　契約の締結

(ｳ)　委託事業者において重要情報を取り扱う場合は、秘密保持契約（ＮＤＡ）の締結

⑶　業務委託実施期間中の対策

ア　中央電子計算組織管理者及び情報セキュリティ管理者は、業務委託の実施期間において、以下を全て含む対策を実施しなければならない。

(ｱ)　委託判断基準に従った重要情報の提供

(ｲ)　契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施

(ｳ)　電子計算組織総括管理者へ措置内容の報告（重要度に応じて CISO に報告）

(ｴ)　委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等により受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

イ　中央電子計算組織管理者及び情報セキュリティ管理者は、業務委託の実施期間において、以下を全て含む対策の実施を委託事業者に求めなければならない。
(ｱ)　情報の適正な取扱のための情報セキュリティ対策
(ｲ)　契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告
(ｳ)　委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処

⑷　業務委託終了時の対策
ア　中央電子計算組織管理者及び情報セキュリティ管理者は、業務委託の終了に際して、以下を全て含む対策を実施しなければならない。
(ｱ)　業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収
(ｲ)　委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認
イ　中央電子計算組織管理者及び情報セキュリティ管理者は、業務委託の終了に際して、以下を全て含む対策の実施を委託事業者に求めなければならない。
(ｱ)　業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検
(ｲ)　提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

１０．２　情報システムに関する業務委託

⑴　情報システムに関する業務委託における共通的対策
中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムに関する業務委託の実施までに、情報システムに本市の意図せざる変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様を策定しなければならない。

⑵　情報システムの構築を業務委託する場合の対策
中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託事業者に求めなければならない。
ア　情報システムのセキュリティ要件の適切な実装
イ　情報セキュリティの観点に基づく試験の実施
ウ　情報システムの開発環境及び開発工程における情報セキュリティ対策

⑶　情報システムの運用・保守を業務委託する場合の対策
ア　中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。
イ　中央電子計算組織管理者及び情報セキュリティ管理者は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託事業者に速やかな報告を求めなければならない。

⑷　本市向けに情報システムの一部の機能を提供するサービスを利用する場合の対策
ア　中央電子計算組織管理者及び情報セキュリティ管理者は、外部の一般の者が本市向けに重要情報を取り扱う情報システムの一部の機能を利用するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託事業者の選定条件に業務委託サービスに特有の選定条件を加えなければならない。
イ　中央電子計算組織管理者又は情報セキュリティ管理者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定しなければならない。
ウ　中央電子計算組織管理者又は情報セキュリティ管理者は、委託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。
エ　中央電子計算組織管理者又は情報セキュリティ管理者は、業務委託サービスを利用する場

合には、電子計算組織総括管理者又は情報セキュリティ責任者へ当該サービスの利用申請を行わなければならない。

オ　電子計算組織総括管理者又は情報セキュリティ責任者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定しなければならない。

カ　電子計算組織総括管理者又は情報セキュリティ責任者は、業務委託サービスの利用申請を承認した場合は、承認済業務委託サービスとして記録し、業務委託サービス管理者を指名しなければならない。

１０．３　外部サービス（クラウドサービス）の利用（自治体機密性２以上の情報を取り扱う場合）

⑴　クラウドサービスの選定に係る運用規定の整備

電子計算組織総括管理者は、自治体機密性２以上の情報を取り扱う場合、以下を含む外部サービス（クラウドサービス、以下「クラウドサービス」という。）の選定に関する規定を整備しなくてはならない。

ア　クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下９.３節において「クラウドサービス利用判断基準」という。）

イ　クラウドサービス提供者の選定基準

ウ　クラウドサービスの利用申請の許可権限者と利用手続

エ　クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

⑵　クラウドサービスの利用に係る運用規定の整備

電子計算組織総括管理者は、自治体機密性２以上の情報を取り扱う場合、以下を含むクラウドサービス（自治体機密性２以上の情報を取り扱う場合）の利用に関する規定を整備しなければならない。

ア　電子計算組織総括管理者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を運用規定として整備しなければならない。

イ　電子計算組織総括管理者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用規定として整備しなければならない。

ウ　電子計算組織総括管理者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を全て含むクラウドサービスの利用を終了する際のセキュリティ対策の基本方針を運用規定として整備しなければならない。

(ｱ)　クラウドサービス利用終了時における対策

(ｲ)　クラウドサービスで取り扱った情報の廃棄

(ｳ)　クラウドサービス利用のために作成したアカウントの廃棄

⑶　クラウドサービスの選定

ア　中央電子計算組織管理者は、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス利用判断基準に従って、業務に係る影響度等を検討した上でクラウドサービスの利用を検討しなければならない。

イ　中央電子計算組織管理者は、クラウドサービスで取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス提供者の選定基準に従ってクラウドサービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策をクラウドサービス提供者の選定条件に含めなければならない。

(ｱ)　クラウドサービスの利用を通じて本市が取り扱う情報のクラウドサービス提供者における目的外利用の禁止

(ｲ)　クラウドサービス提供者における情報セキュリティ対策の実施内容及び管理体制

(ｳ)　クラウドサービスの提供に当たり、クラウドサービス提供者若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制

(ｴ)　クラウドサービス提供者の資本関係・役員等の情報、クラウドサービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定
(ｵ)　情報セキュリティインシデントへの対処方法
(ｶ)　情報セキュリティ対策その他の契約の履行状況の確認方法
(ｷ)　情報セキュリティ対策の履行が不十分な場合の対処方法

ウ　中央電子計算組織管理者は、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、クラウドサービス提供者の選定条件に含めなければならない。

エ　中央電子計算組織管理者は、クラウドサービスの利用を通じて本市が取り扱う情報の格付等を勘案し、必要に応じて以下の内容をクラウドサービス提供者の選定条件に含めなければならない。
(ｱ)　情報セキュリティ監査の受入れ
(ｲ)　サービスレベルの保証

オ　中央電子計算組織管理者は、クラウドサービスの利用を通じて本市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価してクラウドサービス提供者を選定し、必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めなければならない。

カ　中央電子計算組織管理者は、クラウドサービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、選定条件で求める内容をクラウドサービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し、本市の承認を受けるよう、クラウドサービス提供者の選定条件に含めなければならない。また、クラウドサービス利用判断基準及びクラウドサービス提供者の選定基準に従って再委託の承認の可否を判断しなければならない。

キ　中央電子計算組織管理者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、クラウドサービスを選定しなければならない。また、クラウドサービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めなければならない。

ク　中央電子計算組織管理者は、クラウドサービスの特性を考慮した上で、クラウドサービスが提供する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、情報セキュリティに関する役割及び責任の範囲を踏まえて、以下を全て含むセキュリティ要件を定めなければならない。
(ｱ)　クラウドサービスに求める情報セキュリティ対策
(ｲ)　クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法
(ｳ)　クラウドサービスに求めるサービスレベル

ケ　電子計算組織総括管理者は、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、クラウドサービス提供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。

⑷　クラウドサービスの利用に係る調達・契約

ア　中央電子計算組織管理者は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウド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　中央電子計算組織管理者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認し、利用承認を得なければならない。また、調達仕様の内容を契約に含めなければならない。

⑸　クラウドサービスの利用承認

ア　中央電子計算組織管理者及び情報セキュリティ管理者は、クラウドサービスを利用する場合には、電子計算組織総括管理者へクラウドサービスの利用申請を行わなければならない。

イ　電子計算組織総括管理者は、職員等によるクラウドサービスの利用申請を審査し、利用の可否を決定しなければならない。

ウ　電子計算組織総括管理者は、クラウドサービスの利用申請を承認した場合は、承認済みクラウドサービスとして記録し、クラウドサービス管理者を指名しなければならない。

⑹　クラウドサービスを利用した情報システムの導入・構築時の対策

ア　電子計算組織総括管理者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、以下を含むクラウドサービスを利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。

(ｱ)　不正なアクセスを防止するためのアクセス制御

(ｲ)　取り扱う情報の機密性保護のための暗号化

(ｳ)　開発時におけるセキュリティ対策

(ｴ)　設計・設定時の誤りの防止

イ　クラウドサービス管理者は、情報システムにおいてクラウドサービスを利用する際には、情報システム台帳及び関連文書に記録又は記載しなければならない。なお、情報システム台帳に記録又は記載した場合は、電子計算組織総括管理者へ報告しなければならない。

ウ　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始までに以下の全ての実施手順を整備しなければならない。

(ｱ)　クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順

(ｲ)　クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順

(ｳ)　利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

エ　クラウドサービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録しなければならない。

⑺　クラウドサービスを利用した情報システムの運用・保守時の対策

ア　電子計算組織総括管理者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスを利用して情報システムを運用する際のセキュリティ対策を規定しなければならない。

(ｱ)　クラウドサービス利用方針の規定

(ｲ)　クラウドサービス利用に必要な教育

(ｳ)　取り扱う資産の管理

(ｴ)　不正アクセスを防止するためのアクセス制御

(ｵ)　取り扱う情報の機密性保護のための暗号化

(ｶ)　クラウドサービス内の通信の制御

(ｷ)　設計・設定時の誤りの防止

(ｸ)　クラウドサービスを利用した情報システムの事業継続

イ　クラウドサービス管理者は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合、情報システム台帳及び関連文書を更新又は修正しなければならない。なお、情報システム台帳を更新又は修正した場合は、電子計算組織総括管理者へ報告しなければならない。

ウ　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。

エ　中央電子計算組織管理者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウド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。

オ　クラウドサービス管理者は、前各項において定める規定に対し、運用・保守時に実施状況

を定期的に確認・記録しなければならない。

⑻　クラウドサービスを利用した情報システムの更改・廃棄時の対策

ア　電子計算組織総括管理者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスの利用を終了する際のセキュリティ対策を規定しなければならない。

(ｱ)　クラウドサービスの利用終了時における対策

(ｲ)　クラウドサービスで取り扱った情報の廃棄

(ｳ)　クラウドサービスの利用のために作成したアカウントの廃棄

イ　クラウドサービス管理者は、前項において定める規定に対し、クラウドサービスの利用終了時に実施状況を確認・記録しなければならない。

１０．４　外部サービス（クラウドサービス）の利用（自治体機密性２以上の情報を取り扱わない場合）

⑴　クラウドサービスの利用に係る規定の整備

電子計算組織総括管理者は、自治体機密性２以上の情報を取り扱わない場合、以下を含むクラウド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。

ア　クラウドサービスを利用可能な業務の範囲

イ　クラウドサービスの利用申請の許可権限者と利用手続

ウ　クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

エ　クラウドサービスの利用の運用手順

⑵　クラウドサービスの利用における対策の実施

ア　職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で、自治体機密性２以上の情報を取り扱わない場合のクラウドサービスの利用を申請しなければならない。また、承認時に指名されたクラウドサービス管理者は、当該クラウドサービスの利用において適切な措置を講じなければならない。

イ　中央電子計算組織管理者は、職員等によるクラウドサービスの利用申請を審査し、利用の可否を決定しなければならない。また、承認したクラウドサービスを記録しなければならない。

11　評価・見直し

１１．１　監査

⑴　実施方法

CISO は、情報セキュリティ監査総括責任者として電子計算組織総括管理者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じて監査を行わせなければならない。

⑵　監査を行う者の要件

ア　情報セキュリティ監査総括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。なお、情報セキュリティ監査総括責任者は、必要に応じ外部の第三者機関に監査の実施を依頼することができるものとする。

イ　監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

⑶　監査実施計画の立案及び実施への協力

ア　情報セキュリティ監査総括責任者は、監査を行うに当たって、監査実施計画を立案し、電子計算組織管理運営委員会の承認を得なければならない。

イ　被監査部門は、監査の実施に協力しなければならない。

⑷　監査の実施スケジュール

おおむね以下のスケジュールにより監査実施計画を定め、監査を実施する。

主な監査業務	実施時期	備考
監査実施計画策定	４月～７月	
監査準備	４月～７月	監査項目等の整理
監査通知の送付	７月～８月	被監査部門との日程調整、 各対象課に通知を行う。
予備調査	７月～８月	アンケート調査等
実査	９月～12月	被監査部門の日程等を考慮して、本期間内において監査を実施する等
監査報告書提出	２月～３月	最高情報セキュリティ責任者及び必要に応じ電子計算組織管理運営委員会に報告

⑸　委託事業者に対する監査

事業者に業務委託を行っている場合、情報セキュリティ監査総括責任者は委託事業者（再委託事業者を含む。）に対して、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

⑹　報告

情報セキュリティ監査総括責任者は、監査結果を取りまとめ、CISO に報告し、又は必要に応じて電子計算組織管理運営委員会に報告する。

⑺　保管

情報セキュリティ監査総括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適正に保管しなければならない。

⑻　監査結果への対応

ア　CISO は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ責任者に対し、当該事項への対処（改善計画の策定等）を指示しなければならない。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

イ　CISO は、指摘事項を所管していない情報セキュリティ責任者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。また、庁内で横断的に改善が必要な事項については、電子計算組織総括管理者に対し、当該事項への対処（改善計画の策定等）を指示しなければならない。なお、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

⑼　情報セキュリティポリシー及び関係規程等の見直し等への活用

電子計算組織管理運営委員会は、監査結果を情報セキュリティポリシー及び関係規程等の見直し、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。

１１．２　自己点検

⑴　実施方法

ア　中央電子計算組織管理者及び情報セキュリティ管理者は、所管するネットワーク及び情報システムの取扱状況について、毎年度及び必要に応じて自己点検を実施しなければならない。

イ　中央電子計算組織管理者は、情報セキュリティ管理者と連携して、所管する部局における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行わなければならない。

⑵　報告

中央電子計算組織管理者及び情報セキュリティ管理者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、電子計算組織管理運営委員会に報告しなければならない。

⑶　自己点検結果の活用

ア　職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

イ　電子計算組織管理運営委員会は、この点検結果を情報セキュリティポリシー及び関係規程

等の見直し、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。

１１．３　情報セキュリティポリシー及び関係規程等の見直し

電子計算組織管理運営委員会は、情報セキュリティ監査及び自己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、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合にリスク評価を行い、必要があると認めた場合、改善を行うものとする。なお、横断的に改善が必要となる情報セキュリティ対策の運用見直しについて、内部の職制及び職務に応じた措置の実施又は指示をし、措置の結果について CISO に報告しなければならない。

資料１－３

武蔵村山市情報セキュリティポリシーの改定について（概要）

１　情報セキュリティポリシーとは

情報セキュリティ対策を組織的に統一して推進するため、総合的及び体系的に取りまとめたもので、その体系は階層構造となっており、「基本方針」と「対策基準」を総称して「情報セキュリティポリシー」という。

情報セキュリティ対策の基本的な考え方を定めるものが「基本方針」、基本方針に基づき共通の情報セキュリティ対策の基準を定めるものが「対策基準」である。

２　令和７年度改定について

⑴　改正地方自治法への対応

令和８年４月１日から、改正地方自治法の施行により地方公共団体の議会及び長その他の執行機関は、サイバーセキュリティを確保するための方針（基本方針）を定め、必要な措置を講じるとともに公表しなければならないとされた。

同改正法では、各執行機関がそれぞれ方針を定める必要があるが、必要となる情報セキュリティ対策が概ね同様であるなど、別個の方針を定めることが非効率となるような場合には共同で策定することが可能とされていることから、本市においては共同で策定する。

なお、共同策定の場合においても、各執行機関等において決裁等により方針を決定する必要がある。

〔対象〕議会、教育委員会、選挙管理委員会、監査委員、農業委員会及び固定資産評価審査委員会

※個別策定済：教育委員会（教育情報システムのみ）、湖南衛生組合（公表は令和８年４月１日以降）

⑵　最新のガイドラインへの対応

本市では、国の「地方公共団体における情報セキュリティポリシーに関するガイドライン」に基づき、平成１６年３月に情報セキュリティポリシーを策定し、現在、令和４年３月版のガイドラインに対応しているが、その後の改定を含む最新の令和７年３月版に対応する必要がある。

なお、本市の情報セキュリティポリシーは、国のガイドラインに準拠しているものの、記載順や文章表現等に違いが多く、毎年度改訂される国のガイドラインに適切に対応するとともに、改定作業を効率化するためには、今回の改正において、国のガイドライン（記載例）における構成や文章表現に原則として統一させる所要の規定の整備を行うこととする。

⑶　公表対象の変更

改正地方自治法においては、「基本方針」のみ公表対象であり、「対策基準」には情報セキュリティを確保するために公表すべきでない情報が含まれる場合があり非公開とする自治体が多いことから、本改定を機に「対策基準」を原則として非公開とする。

⑷ 改定スケジュール

●このまでの審議経過

日　程	件　名	議題等
令和７年１０月　３日	関係課事前協議	事務局改定案提示及び各行政委員会等手続確認
１２月１２日	電子計算組織管理運営委員会	事務局改定案の審議
２５日	各行政委員会等への意見照会	改定案に対する各行政委員会等への意見照会
〔１～２月〕	各行政委員会等における改定案確認及び意見調整	
令和８年　２月２０日	意見照会回答期限	
３月　９日	調整会議	各行政委員会等の意見を踏まえた改定案提示

●今後の予定

令和８年　３月２６日	庁議	情報セキュリティポリシーの改定について
～３月３０日	市長決裁及び各行政委員会等の長の決裁	庁議決定後、各行政委員会等に共有
～３月３１日	広資料及びホームページで公表	

４　改定の概要

⑴ 基本方針

①行政機関の範囲の見直し

基本方針が対象とする行政機関の範囲に、議会を構成する議員や行政委員会の委員を追加する。

②業務委託及び外部サービス（クラウドサービス）の利用に係る規定の追加

委託先に提供した情報の適切な保護について、委託先に求めるべき対策を規定する。

③公表対象の見直し

改定後の基本方針は、改正地方自治法第２４４条の６第１項の方針として位置付け、広資料及びホームページにより公表する。

なお、対策基準については、今回の改定から非公開に変更する。

⑵ 対策基準

対策基準は、基本方針に基づき、共通の情報セキュリティ対策の基準として、「どのような情報を」「どのような脅威から」「どのように守るのか」という情報セキュリティ対策を行う上で、必要となる基本的な要件を規定している。

① 適用範囲の見直し

基本方針の改定と同様、対策基準の適用対象となる行政機関の範囲に、議会を構成する議員や行政委員会の委員を追加する。

② 情報資産の分類の細分化

クラウドサービスの利用が拡大している状況を踏まえ、これまで情報資産の分類を見直し、機密性、完全性及び可用性それぞれ別に規定するとともに、機密性については、自治体が扱う個人情報の量や種類、頻度が、国に比べ大きく重要であることから細分化する。

分類	重要性の分類
Ⅰ	個人情報及び本市の業務上必要とする情報で、最小限の者のみが扱う情報
Ⅱ	情報の公開を予定していない情報
Ⅲ	外部に公開する情報のうち、業務上重要な情報
Ⅳ	上記以外の情報

詳細別紙

機密性による分類	完全性による分類	可用性による分類
自治体機密性３Ａ	自治体完全性２	自治体可用性２
自治体機密性３Ｂ		
自治体機密性３Ｃ		
自治体機密性２		
自治体機密性１	自治体完全性１	自治体可用性１

③ 業務委託と外部サービス（クラウドサービス）の利用に係る規定の追加

委託先に提供した情報が適切に保護されるよう、業務委託契約時、実施期間中、終了後に取るべき対策について、本市で実施すべき対策及び委託先に求めるべき対策をそれぞれ規定。

・委託事業者への提供を認める情報及び業務の範囲を判断する基準、委託事業者の選定基準の整備
・契約に基づく情報セキュリティ対策の履行状況の定期的な報告等の実施
・委託業務において取り扱った情報の返却、廃棄又は抹消の実施

●情報資産の分類の細分化（別紙）

分類	分類基準	取扱制限
機密性３Ａ	「行政文書の管理に関するガイドライン」（平成２３年４月１日内閣総理大臣決定）に定める秘密文書に相当する文書 ・国や中央省庁が指定した極秘文書及び秘文書	・支給された端末以外での作業の原則禁止（自治体機密性３の情報資産に対して） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
機密性３Ｂ	漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報 ・住民情報システム等に保存される住民の個人情報、職員の属性に基づく個人情報	
機密性３Ｃ	機密性３Ｂ以上に相当する機密性は要しないが、基本的に公表することを前提としていない情報 ・システム及びセキュリティ対策に関する情報、文書管理システムに決裁文書として保存されいる個人情報、施設設計情報、入札予定価格等	
機密性２	機密性３に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報 ・公開の承認を得ていない企画・検討段階の情報、調査照会・回答文書、庁内向け通知	
機密性１	機密性２以上に相当する機密性は要しない情報 ・将来公表する予定の文書（計画案等）、公表された情報	―
完全性２	改ざん、誤びゅう又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
完全性１	自治体完全性２の情報資産以外の情報資産	―
可用性２	滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性１	自治体可用性２の情報資産以外の情報資産	―

資料１－４

行政委員会等への意見照会に対する対応状況

（意見照会期間：令和７年１２月２５日（木）から令和８年２月２０日（金）まで）

１　情報セキュリティ基本方針について

意見提出元	No.	意見の内容	意見に対する対応状況
教育委員会	１	■２　定義　(4)情報セキュリティポリシー 「資料１_武蔵村山市情報セキュリティポリシーの構成」において、武蔵村山市情報セキュリティポリシーの定義がされていることから、基本方針と一体でない場合は、基本方針において定義すべきである。 また、本基本方針と教育情報セキュリティ対策基準を合わせて教育情報セキュリティポリシーと解釈できるよう定義付けしていただきたい。	本基本方針と各行政委員会等で策定する「情報セキュリティ対策基準」を総称して情報セキュリティポリシーと定義できるよう「行政機関等が別に定める」を加えた。
	２	■４　適用範囲　(1)行政機関 公立小・中学校は地方公共団体が設置する教育機関であることから、行政機関「等」としていただきたい。また、教育委員会には公立小･中学校は含まれないため､「武蔵村山市立の小学校及び中学校」を行政機関等の内訳に追記していただきたい。	「行政機関」を「行政機関等」とし、行政機関等の内訳に「市立小学校及び市立中学校」を加えた。
	３	■４　適用範囲　(2)適用を受ける者 「地方公務員法第３条第２項に規定する一般職の職員」には、東京都が採用し配置されている都事務支援員(都費会計年度任用職員)は含まれるのか。	都事務支援員は、地方公務員法第３条第２項に規定する一般職に該当することから、原案のとおりとした。
	４	■５　職員等の遵守義務 項番２における定義によると情報セキュリティポリシーは市長部局が作成する基本方針及び対策基準に限定されるため、教育情報セキュリティポリシーも遵守するような表現にしていただきたい。	No.１の対応により、原案のとおりとした。

意見提出元	No.	意見の内容	意見に対する対応状況
教育委員会	5	■６　情報セキュリティ対策　⑶　情報システム全体の強靭性の向上 　ウ　インターネット接続系における「高度な情報セキュリティ対策」について、「都道府県及び市町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。」とあるが、公立小・中学校におけるセキュリティ対策はゼロトラストセキュリティを採用しているため、整合性のとれる表現に変更していただきたい。	「自治体情報セキュリティクラウド」については、国が推奨する高度な情報セキュリティ対策としての例示であり、限定するものではない。 　本市においても導入済みであるが、各システムの状況により、セキュリティクラウドを経由しない場合であっても、同水準の対策を求めるものであり、公立小・中学校における対策を否定するものではないことから、原案のとおりとした。
教育委員会	6	■６　情報セキュリティ対策　⑺　運用 　セキュリティ侵害が発生した場合には「武蔵村山市業務継続計画（ＩＣＴ編）」に基づき対応を行うとあるが、この計画に小・中学校は含まれていないという認識である。ついては、含まれていない組織の対応を網羅するような記載に変更していただきたい。	「武蔵村山市業務継続計画（ＩＣＴ編）」に「等」を加える。
固定資産評価審査委員会	7	■２　定義 　現行の情報セキュリティポリシーで定義されている「情報資産」に係る定義を改定版にも追加した方が、読み手が理解しやすいのではないか。	４　適用範囲　⑶　情報資産の範囲において、詳細に規定していることから、原案のとおりとした。

２　情報セキュリティ対策基準について

意見提出元	No.	意見の内容	意見に対する対応状況
議会事務局	1	■４　情報システム全体の強靭性の向上 　⑶ インターネット接続系　イ「自治体情報セキュリティクラウドに参加」については、重要な情報以外等付記事項又は整理が必要。	「自治体情報セキュリティクラウド」は、国が推奨する高度な情報セキュリティ対策としての例示であり、限定するものではない。 　本市においても導入済みであるが、各システムの状況により、セキュリティクラウドを経由しない場合であっても、同水準の対策を求めるものであることから、原案のとおりとした。 　なお、自治体情報セキュリティクラウド経由の要否については、各システムの取り扱う情報等を踏まえ判断していく。

資料１－５

武蔵村山市情報セキュリティ基本方針　新旧対照表

改定後（新）	現行（旧）	改定理由
武蔵村山市情報セキュリティ基本方針	**第２章**　武蔵村山市情報セキュリティ基本方針	
１　目的 **本基本方針**は、本市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、本市が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。	１　目的 **情報セキュリティ基本方針（以下「基本方針」という。）**は、本市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、本市が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。	・ガイドライン準拠
２　定義 ⑴　ネットワーク コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。 ⑵　情報システム コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。	２　定義 ⑴　ネットワーク コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。 ⑵　情報システム コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。	
⑶　情報セキュリティ 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。	**⑿**　情報セキュリティ 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。	・ガイドライン準拠
⑷　情報セキュリティポリシー **本**基本方針及び**行政機関等が別に定める**情報セキュリティ対策基準**（以下「対策基準」という。）**をいう。	**⒀**　情報セキュリティポリシー **組織における情報資産の情報セキュリティ対策について、総合的及び体系的に取りまとめたものであり、**基本方針及び情報セキュリティ対策基準をいう。	・ガイドライン準拠
⑸　機密性 **情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。**	**⑶**　機密性 **権限のない者への重要な情報の漏えいを防止することをいう。**	・ガイドライン準拠
⑹　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。	**⑷**　完全性 情報**の改ざん、破壊による被害を防止**することをいう。	・ガイドライン準拠

改定後（新）	現行（旧）	改定理由
(7) 可用性 **情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保**することをいう。	(5) 可用性 **権限のある者に対し、必要なときに情報の利用を可能と**することをいう。	・ガイドライン準拠
(8) マイナンバー利用事務系（個人番号利用事務系） 個人番号利用事務（社会保障、地方税又は防災に関する事務）**又は戸籍事務等**に関わる情報システム及びデータをいう。	(6) マイナンバー利用事務系（個人番号利用事務系） 個人番号利用事務（社会保障、地方税又は防災に関する事務等）に関わる情報システム及びデータをいう。	・ガイドライン準拠
(9) LGWAN接続系 LGWANに接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。	(7) **総合行政ネットワーク（**LGWAN**）**接続系 **総合行政ネットワーク（**LGWAN**）**に接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。	・ガイドライン準拠
(10) インターネット接続系 インターネット**メール**、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。	(8) インターネット接続系 インターネット、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。	・ガイドライン準拠
(11) 通信経路の分割 LGWAN接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。	(9) 通信経路の分割 **総合行政ネットワーク（**LGWAN**）**接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。	・ガイドライン準拠
(12) 無害化通信 インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。	(10) 無害化通信 インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。	・ガイドライン準拠
	(11) 情報資産 情報システムで取り扱う情報で、開発と運用に係る全ての情報をいう。	・項番４で規定

改定後（新）	現行（旧）	改定理由
３　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。 **⑴　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** **⑵　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、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** **⑶　地震、落雷、火災等の災害によるサービス及び業務の停止等** **⑷　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** **⑸　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**	**５　情報資産への**脅威 情報資産**への**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。 **⑴　人による脅威（故意）** **不正アクセスやウイルス攻撃等のサイバー攻撃、機器の盗難、不正な操作や持ち出し等の故意による情報資産の漏えい・破壊・改ざん・消去等** **⑵　人による脅威（過失）** **情報資産の管理不備、無許可ソフトウェアの使用等の規定違反、プログラム上の欠陥、操作・設定ミス、委託管理の不備等の過失による情報資産の漏えい・破壊・破壊消去等** **⑶　災害による脅威** **地震、落雷、火災、水害等の災害によるサービス及び業務の停止、情報資産の消失等** **⑷　必要資産の不足、故障等による脅威** **電力及び通信等の途絶、交通機能の麻痺や大規模・広範囲にわたる疾病のまん延による要員の不足、機器の故障等によるサービス及び業務の停止、情報システム運用の機能不全等**	・ガイドライン準拠
４　適用範囲 ⑴　行政機関**等**の範囲 **本**基本方針が適用される行政機関**等**は、市長部局**及び市の行政委員会等（**議会、教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会**、市立小学校及び市立中学校をいう。）**とする。 **⑵　適用を受ける者** **本基本方針の適用を受ける者は、前号に掲げる行政機関**	**３**　適用範囲 ⑴　行政機関の範囲 基本方針が適用される行政機関**の範囲**は、市長部局**、**議会**事務局**、教育委員会**事務局**、選挙管理委員会**事務局**、監査**事務局**、農業委員会**事務局**及び固定資産評価審査委員会**事務局**とする。	・改正地方自治法対応 ・対象の明確化のため

改定後（新）	現行（旧）	改定理由
等に属する地方公務員法（昭和２５年法律第２６１号）第３条第２項に規定する一般職の職員及び同条第３項に規定する特別職の職員並びに教育公務員特例法（昭和２４年法律第１号）第２条第１項に規定する教育公務員のうち、当該行政機関等の情報資産を取り扱う者（以下「職員等」という。）とする。		
⑶　情報資産の範囲 **本**基本方針が対象とする情報資産は、次のとおりとする。 ア　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体 イ　**ネットワーク及び**情報システムで取り扱う情報（これらを印刷した文書を含む。） ウ　情報システムの仕様書及びネットワーク図等のシステム関連文書	⑵　情報資産の範囲 基本方針が対象とする情報資産は、次のとおりである。 ア　**情報システム（コンピュータ、ネットワーク及び電磁的記録媒体）及びこれらに関する設備** イ　**情報システム（コンピュータ、ネットワーク及び電磁的記録媒体）**で取り扱う情報（これらを印刷した文書を含む。） ウ　情報システムの仕様書及びネットワーク図等の情報システム関連文書	・ガイドライン準拠
５　職員等の**遵守義務** 職員等は、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情報セキュリティポリシー及び**情報セキュリティ**実施手順**（以下「実施手順」という。）**を遵守しなければならない。	**４**　職員等**及び委託事業者の責務** 職員等**及び委託事業者**は、情報セキュリティの重要性について共通の認識を持**つとともに**、業務の遂行に当たって**は**情報セキュリティポリシー及び実施手順を遵守しなければならない。	・委託事業者の責務を項番６⑻で別に規定
６　情報セキュリティ対策 **上記３**の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。 ⑴　組織体制 情報資産について、情報セキュリティ対策を推進**する組織横断的な体制を確立する。**	**７**　情報セキュリティ対策 **前記５で示した**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**ものとする**。 ６　情報セキュリティ管理体制 **本市の**情報資産について、情報セキュリティ対策を推進**・管理するため、情報セキュリティ管理体制を確保する。**	・ガイドライン準拠

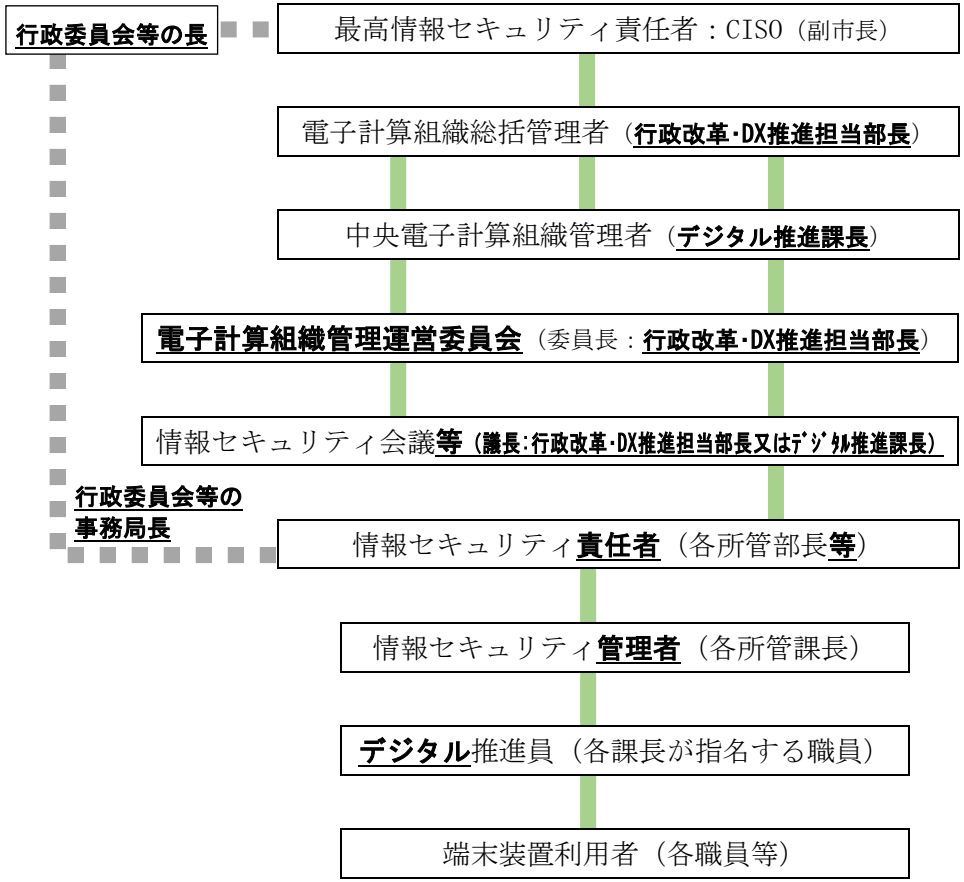
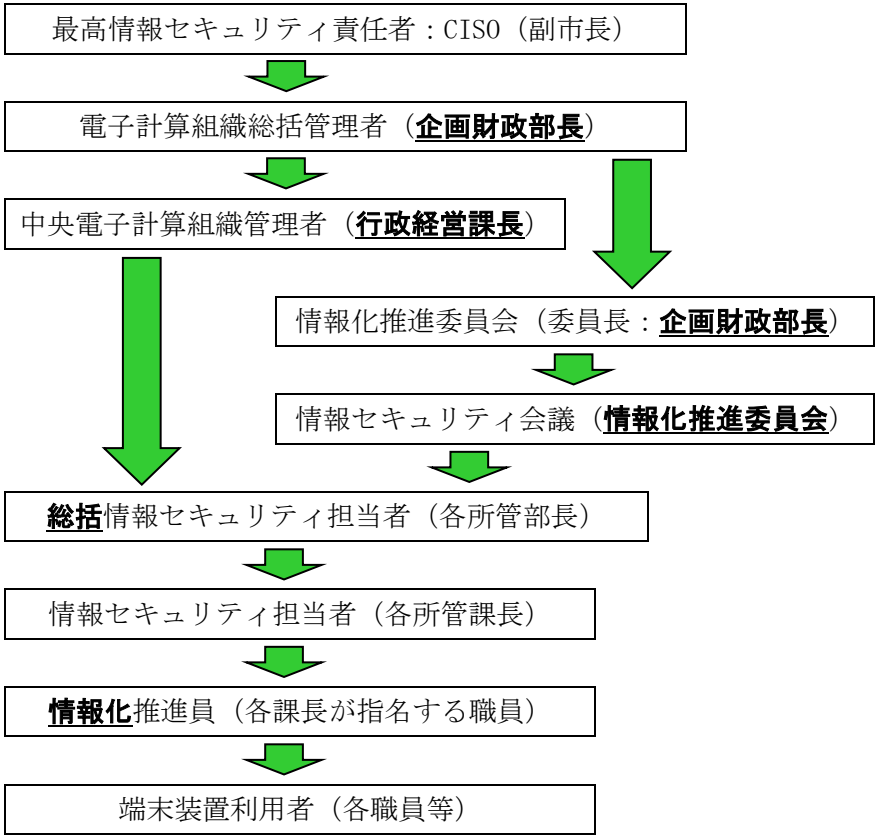
改定後（新）	現行（旧）	改定理由
⑵ 情報資産の分類と管理 **本市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。**		・対策基準での分類を細分化するには、基本方針で定義する必要があるため
⑶ 情報システム全体の強靭性の向上 **情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、**情報システム全体に対し、次の三段階の対策を講じる。	⑴ 情報システム全体の強靭性の向上 情報システム全体に対し、次の三段階の対策を講じる。	・ガイドライン準拠
ア　マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。	ア　マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証*の導入等により、住民情報の流出を防ぐ。	
イ　LGWAN接続系においては、LGWANと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。	イ　**総合行政ネットワーク（**LGWAN**）**接続系においては、**総合行政ネットワーク（**LGWAN**）**と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。	
ウ　インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。	ウ　インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。	
⑷ 物理的セキュリティ **サーバ、電算室、通信回線及び職員等のパソコン**等の管理について、物理的な対策を講じる。	⑵ 物理的セキュリティ **コンピュータ、ネットワーク**等の管理について、物理的な対策を講じる。	・ガイドライン準拠
⑸ 人的セキュリティ 情報セキュリティに関し、職員等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。	⑶ 人的セキュリティ 情報セキュリティに関し、職員等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。	・ガイドライン準拠

改定後（新）	現行（旧）	改定理由
⑹　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。	⑷　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な対策を講じる。	・ガイドライン準拠
⑺　運用 　情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等**、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、**「武蔵村山市業務継続計画（ＩＣＴ編）」**等**により、**情報資産に対するセキュリティ侵害**が発生した**場合等**に迅速な対応を可能とするための危機管理対策を行う。	⑸　運用 　情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際の情報セキュリティの確保等の運用面の対策を講じる。 **１０　緊急時の対応** 　「武蔵村山市業務継続計画（ＩＣＴ編)」により、**緊急事態**が発生した**際**に迅速な対応を可能とするための危機管理対策を行う。	・ガイドライン準拠
⑻　業務委託と外部サービス（クラウドサービス）の利用 **　業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託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確認し、必要に応じて契約に基づき措置を講じる。** **　外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。** **　ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。**		・クラウドサービス利用の増加に対応するため、委託先に提供した情報の適切な保護のため、委託先に求めるべき対策の考え方を追加
⑼　評価・見直し **　情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ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。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。**		・常に変化するセキュリティリスクに対応するため、定期的又は必要に応じて点検等を行い運用改善を図っている考えを明確にするもの

改定後（新）	現行（旧）	改定理由
７　情報セキュリティ監査及び自己点検の実施 　**情報セキュリティポリシーの**遵守**状況**を検証するため、定期**的**又は**必要に応じて情報セキュリティ**監査及び自己点検を実施する。	**１１**　情報セキュリティ監査及び自己点検の実施 　**基本方針、対策基準及び実施手順（以下「基本方針等」という。）が**遵守**されていること**を検証するため、**ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について**定期**に**又は**随時に**監査及び自己点検を実施する。	・ガイドライン準拠
８　情報セキュリティポリシーの見直し 　情報セキュリティ監査及び自己点検の結果**、**情報セキュリティ**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新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。**	**１２**　情報セキュリティポリシー**等**の見直し 　情報セキュリティ監査及び自己点検の結果**又は**情報セキュリティ**に関する状況の変化に対応する必要がある場合には、情報セキュリティポリシー及び実施手順の見直しを行い、必要に応じて改定する。**	・常に変化するセキュリティリスクに対応するため定期的又は必要に応じて点検結果等を踏まえ、見直していく考えを明確にするもの
９　**対策基準と実施手順**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。**また、**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業務担当課において策定するものとする。なお、**対策基準及び**実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから**原則として**非公開とする。	**８**　**情報セキュリティ**対策基準の策定 　**情報セキュリティ対策**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**た「情報セキュリティ対策基準（以下「対策基準」という。）」**を策定する。 **９**　**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**に関する**対策を実施するための具体的な手順を定めた**「情報セキュリティ**実施手順**（以下「実施手順」という。）」**を業務担当課において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の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。	・非公開の対象に対策基準を追加

武蔵村山市情報セキュリティ対策基準　新旧対照表

改定後（新）	現行（旧）
武蔵村山市情報セキュリティ対策基準	**第３章**　武蔵村山市情報セキュリティ対策基準
１　目的 **武蔵村山市情報セキュリティ対策基準（以下「対策基準」という。）は、武蔵村山市情報セキュリティ基本方針を実行に移すための、本市における情報セキュリティを確保するために遵守すべき行為及び判断等、情報セキュリティ対策を行う上で必要となる基本的な要件を規定し、円滑な行政運営を図ることを目的に策定するものとする。**	**１　対策基準の考え方** **対策基準は、情報セキュリティ対策を講じるため、組織全体の対策に関する統一的な方針を定めた基本方針に基づいて、具体的にどのような対策を取るべきかを記述したものである。** **２　目的** **対策基準は、基本方針に定められた情報セキュリティを確保するために遵守すべき行為及び判断等、情報セキュリティ対策を行う上で必要となる基本的な要件を規定し、円滑な行政運営を図ることを目的に策定するものとする。**
２　適用範囲 **⑴　行政機関等の範囲** **本**対策基準が適用される行政機関**等**は、**市長部局及び市の行政委員会等（議会、教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会、市立小学校及び市立中学校をいう。）**とする。 **⑵　適用を受ける者** **本対策基準の適用を受ける者は、行政機関等に属する地方公務員法（昭和２５年法律第２６１号）第３条第２項に規定する一般職の職員及び同条第３項に規定する特別職の職員並びに教育公務員特例法（昭和２４年法律第１号）第２条第１項に規定する教育公務員であって行政委員会等が別に定める者を除いた者（以下「職員等」という。）とする。**	**３**　適用範囲 対策基準が適用される行政機関**の範囲は、市長部局、議会事務局、教育委員会事務局、選挙管理委員会事務局、監査事務局、農業委員会事務局及び固定資産評価審査委員会事務局のうち、中央電子計算組織が設置されている部署及び個別電子計算組織又は小規模電子計算組織が設置されている部署**とする。

改定後（新）	現行（旧）
⑶　情報資産の範囲 **本対策基準が対象とする情報資産は、基本方針で定める情報資産のうち、行政委員会等が別に定める情報資産を除いたものとする。**	
３　組織体制 ⑴　情報セキュリティ対策の管理体制 本市における情報セキュリティ対策を組織全体で継続的に実施するための管理体制を整備する。  	**４**　組織体制 ⑴　情報セキュリティ対策の管理体制 本市における情報セキュリティ対策を組織全体で継続的に実施するための管理体制を整備する。 

改定後（新）	現行（旧）
⑵　役割と責務 ア　最高情報セキュリティ責任者（CISO: Chief Information Security Officer**、以下「CISO」という。**）（副市長） **(ｱ)　副市長をCISOとする。CISOは、**本市における全てのネットワーク、情報システム**等の**情報資産の**管理及び**情報セキュリティ対策**に関する最終決定権限及び責任を有する。** **(ｲ)　CISOは、必要に応じ、業務内容を定めた上で情報セキュリティに関する専門的な知識及び経験を有した専門家を、最高情報セキュリティアドバイザーとして置くことができる。** **(ｳ)　CISOは、情報セキュリティインシデントに対処するための体制（CSIRT：Computer Security Incident Response Team）を整備し、役割を明確化する。** **(ｴ)　CISOは、CISOを助けて本市における情報セキュリティに関する事務を整理し、CISOの命を受けて本市の情報セキュリティに関する事務を総括する最高情報セキュリティ副責任者（以下「副CISO」という。）１人を必要に応じて置くことができる。** **(ｵ)　CISOは、本対策基準に定められた自らの担務を、副CISOその他の本対策基準に定める責任者に担わせることができる。** イ　電子計算組織総括管理者**（行政改革・ＤＸ推進担当部長）** (ｱ)　**行政改革・ＤＸ推進担当部長を**電子計算組織総括管理者とする。 (ｲ)　CISO**及び副**CISOを補佐し、CISO**及び副**CISOが不在の場合には自らの判断に基づき、必要な措置を行う。 **(ｳ)　本市の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。** **(ｴ)**　本市**の**全てのネットワーク**における**情報セキュリティ**対策**に関する総合的な権限**及び責任**を有する。	⑵　役割と責務 ア　最高情報セキュリティ責任者（CISO：Chief Information Security Officer）（副市長） 副市長**をもって最高情報セキュリティ責任者とし、**本市における全てのネットワーク、情報システム**及び**情報資産の情報セキュリティ対策**を総括する。** イ　電子計算組織総括管理者**（企画財政部長）** (ｱ)　**企画財政部長をもって**電子計算組織総括管理者とする。 (ｲ)　**最高情報セキュリティ責任者**を補佐し、**最高情報セキュリティ責任者**が不在の場合には自らの判断に基づき、必要な措置を行う。 **（※ウ(ｲ)デジタル推進課長の役割から変更）** (ｳ)　本市**における**全てのネットワーク**、情報システム及び情報データの**情報セキュリティに関する総合的な権限を有する。

改定後（新）	現行（旧）
(ｵ)　中央電子計算組織管理者、情報セキュリティ責任者、情報セキュリティ管理者及び端末装置利用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。	**（※ウ(ｵ)デジタル推進課長の役割から変更）**
(ｶ)　本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISO の指示に従い、CISO が不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。	
(ｷ)　本市の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。	**(ｵ)　電子データに関する情報セキュリティ実施手順等の維持管理を行う。**
(ｸ)　武蔵村山市業務継続計画（ＩＣＴ編）の策定及び管理を行う。	**（※ウ(ｷ)デジタル推進課長の役割から変更）**
(ｹ)　緊急時等の円滑な情報共有を図るため、CISO、電子計算組織総括管理者、中央電子計算組織管理者、情報セキュリティ責任者及び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。	**（※ウ(ｸ)デジタル推進課長の役割から変更）**
(ｺ)　機密性の高い情報資産に対する**セキュリティ**侵害**が発生した**又は**セキュリティ**侵害のおそれがある場合には、CISO に早急に報告を行うとともに、武蔵村山市情報セキュリティ会議（以下「情報セキュリティ会議」という。）を招集する。	**(ｴ)**　情報資産に対する侵害又は侵害のおそれのある場合には、**最高情報セキュリティ責任者**に早急に報告を行うとともに、情報セキュリティ会議を招集する。
(ｻ)　情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて CISO にその内容を報告しなければならない。	
ウ　中央電子計算組織管理者（**デジタル推進課長**）	ウ　中央電子計算組織管理者（**行政経営課長**）
(ｱ)　企画財政部**デジタル推進課長**を中央電子計算組織管理者とする。	(ｱ)　企画財政部**行政経営課長**をもって中央電子計算組織管理者とする。
(ｲ)　電子計算組織総括管理者を補佐し、電子計算組織総括管理者が不在の場合には必要な措置を行う。	**(ｶ)　本市の情報資産に対する侵害又は侵害のおそれがある場合には、電子計算組織総括管理者の指示に従い、電子計算組織総括管理者が**

改定後（新）	現行（旧）
	不在の場合には自らの判断に基づき必要かつ十分な全ての措置を行う。
（※行政改革・ＤＸ推進担当部長の役割へ変更）	㈠　本市における全てのネットワークに関する開発、設定の変更、運用及び更新等を行う。
（※情報セキュリティ管理者の役割に含む）	㈡　所管する情報システムにおける開発、設定の変更、運用、更新等を行う。
（※㈠の補佐業務に含む）	㈢　他の所管に係る情報システムについて指導・助言を行う。
（※㈠の補佐業務に含む）	㈣　総括情報セキュリティ担当者、情報セキュリティ担当者及び端末装置利用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。
㈤　機密性の低い情報資産に対するセキュリティ侵害が発生した又はセキュリティ侵害のおそれがある場合には、電子計算組織総括管理者に早急に報告を行うとともに、武蔵村山市緊急対策会議（以下「緊急対策会議」という。）を招集する。	
（※行政改革・ＤＸ推進担当部長の役割へ変更）	㈥　本市の全てのネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持、管理を行い、武蔵村山市業務継続計画（ＩＣＴ編）の策定及び管理を行う。
（※行政改革・ＤＸ推進担当部長の役割へ変更）	㈦　緊急時等の円滑な情報共有を図るため、最高情報セキュリティ責任者、電子計算組織総括管理者、中央電子計算組織管理者、総括情報セキュリティ担当者及び情報セキュリティ担当者を網羅する連絡体制を含めた緊急連絡網を整備する。
エ　情報セキュリティ**責任者**（各所管部長等）	**カ**　総括情報セキュリティ**担当者**（各所管部長）
㈠　各所管部長**及び行政委員会等の事務局の長**を**情報セキュリティ責任者**とする。	㈠　各所管部長をもって**総括情報セキュリティ担当者**とする。
㈡　当該部局等の情報セキュリティ対策に関する総括的な権限及び責任を有する。	
㈢　当該部局等に属する情報セキュリティ**管理者**から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	㈡　当該所属する部に属する情報セキュリティ**担当者**から情報資産に対する侵害又は侵害のおそれがあるとの報告を受けた場合には、電子

改定後（新）	現行（旧）
があるとの報告を受けた場合には、電子計算組織総括管理者に速やかに報告する。**なお、行政委員会等の情報セキュリティ責任者においては、行政委員会等の長にも速やかに報告する。** **(ｴ)　当該部局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う総括的な権限及び責任を有する。** **(ｵ)　当該部局等において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約並びに職員等に対する教育、訓練、助言及び指示を行う。** **オ**　情報セキュリティ**管理者**（各所管課長） (ｱ)　各所管課長を情報セキュリティ**管理者**とする。 (ｲ)　当該所属する課の職員等に対して、情報セキュリティ対策に関する教育、指導及び啓発を行う。 (ｳ)　所掌す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、**情報セキュリティ責任者**及び中央電子計算組織管理者に速やかに報告する。 (ｴ)　所管する情報システムに関して、中央電子計算組織管理者の指示等に従い、開発、設定の変更、運用、更新等を行う。 **カ　デジタル推進員**（各課長が指名する**職員等**） 各所属長の指名に基づき任命された**職員等**を**デジタル推進員**とし、情報セキュリティ対策の啓発及び普及、**DX 施策**の推進及び情報通信技術の事務処理への活用並びに端末装置等の操作指導に係る連絡調整を行う。 **キ**　端末装置利用者（各職員等） 情報資産に携わる職員等は、情報セキュリティポリシーに定める事項を遵守する。	計算組織総括管理者に速やかに報告する。 **(ｲ)　情報セキュリティポリシーの部内における意見の集約及び当該所属する部の情報セキュリティ担当者に対する助言を行う。** **キ**　情報セキュリティ**担当者**（各所管課長） (ｱ)　所管課長をもって情報セキュリティ**担当者**とする。 (ｲ)　**総括情報セキュリティ担当者の下で、**当該所属する課の職員に対して、情報セキュリティ対策に関する教育、指導及び啓発を行う。 (ｳ)　所掌する情報資産に対する侵害又は侵害のおそれ**の**ある場合には、中央電子計算組織管理者**、総括情報セキュリティ担当者及び情報化推進委員会**に速やかに報告する。 (ｴ)　所管する情報システムに関して、中央電子計算組織管理者の指示等に従い、開発、設定の変更、運用、更新等を行う。 **ク　情報化推進員**（各課長が指名する**委員**） 各所属長の指名に基づき任命された**職員**を**情報化推進員**とし、情報セキュリティ対策の啓発及び普及、**情報化施策**の推進及び情報通信技術の事務処理への活用並びに端末装置等の操作指導**及び情報化**に係る連絡調整を行う。 **ケ**　端末装置利用者（各職員等） 情報資産に携わる職員等は、情報セキュリティポリシーに定める事項を遵守する。

改定後（新）	現行（旧）
ク　電子計算組織管理運営委員会（委員長：**行政改革・ＤＸ推進担当部長**） (ｱ)　武蔵村山市電子計算組織の管理運営に関する規則第３条の規定に基づいて設置する。 (ｲ)　本市の情報セキュリティの維持管理を統一的な視点で行うため、**情報セキュリティポリシー等の**情報セキュリティ対策に関する重要な事項を審議する。	**エ　情報化推進委員会**（委員長：**企画財政部長**） (ｱ)　武蔵村山市電子計算組織の管理運営に関する規則第３条の規定に基づいて設置する。 (ｲ)　本市の情報セキュリティの維持管理を統一的な視点で行うため、情報セキュリティ対策に関する重要な事項を審議する。
⑶　兼務の禁止 ア　情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。 イ　情報セキュリティ監査の実施において、やむを得ない場合を除き、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。	⑶　兼務の禁止 ア　情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。 イ　情報セキュリティ監査の実施において、やむを得ない場合を除き、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。
⑷　情報セキュリティインシデントへの対応 ア　情報セキュリティ会議**等（議長：行政改革・ＤＸ推進担当部長又はデジタル推進課長）** **(ｱ)　武蔵村山市情報セキュリティ会議等設置要綱第１条の規定に基づいて設置する。** **(ｲ)　本市のネットワーク電子計算組織において障害又は不正行為（以下「緊急事態」という。）が発生し又は発生するおそれがある場合に、迅速かつ的確な対応を実施するため、緊急事態の区分に応じ、情報セキュリティ会議又は緊急対策会議（以下「情報セキュリティ会議等」という。）において対策を決定する。** **(ｳ)　次に掲げる事項を所掌する。** **a　緊急事態の状況の把握に関すること。** **b　緊急事態の復旧作業体制の確立に関すること。** **c　関係諸団体への連絡及び技術的支援依頼に関すること。** **d　代替措置の決定に関すること。**	**⑵ オ　情報セキュリティ会議（情報化推進委員会）** **障害及び不正行為等のうち、市民生活に影響が大きい場合の緊急時に対する対応策を協議する。**

改定後（新）	現行（旧）
e **住民対応方法の決定に関すること。** f **前各号に掲げるもののほか、緊急事態の対策に関すること。** **イ** 情報セキュリティに関する統一的な窓口 (ｱ) **デジタル推進課**を、情報セキュリティインシデントの統一的な窓口の機能を有する組織とし、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、CISO **及び電子計算組織総括管理者**への報告を行うものとする。 (ｲ) **情報セキュリティ会議等**は、情報セキュリティインシデントを認知した場合には、総務省、東京都等へ報告しなければならない。 (ｳ) **情報セキュリティ会議等**は、情報セキュリティインシデントを認知した場合には、その重要度や影響範囲などを勘案し、報道機関への通知・公表対応を行わなければならない。 (ｴ) **電子計算組織管理運営委員会**は、CISO による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供しなければならない 。 (ｵ) **デジタル推進課**は、情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、委託事業者等との情報共有を行う。情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、発生した情報セキュリティインシデントを正確に把握・分析し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行う。 **4** 情報資産の分類と管理 ⑴ 情報資産の分類 本市における情報資産は、機密性、完全性及び可用性**により、次のとおり分類し、必要に応じ取扱制限を行うものとする。**	**(2) コ** 情報セキュリティに関する統一的な窓口 (ｱ) **情報化推進委員会**を、情報セキュリティインシデントの統一的な窓口の機能を有する組織とし、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、**最高情報セキュリティ責任者**への報告を行うものとする。 (ｳ) **情報化推進委員会**は、情報セキュリティインシデントを認知した場合には、総務省、東京都等へ報告しなければならない。 (ｴ) **情報化推進委員会**は、情報セキュリティインシデントを認知した場合には、その重要度や影響範囲などを勘案し、報道機関への通知・公表対応を行わなければならない。 (ｲ) **情報化推進委員会**は、**最高情報セキュリティ責任者**による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供しなければならない。 (ｵ) **情報化推進委員会**は、情報セキュリティに関して、関係機関、他の地方公共団体の情報化推進委員会の機能を有する部署及び委託事業者等との情報共有を行う。情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、発生した情報セキュリティインシデントを正確に把握・分析し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行う。 **5** 情報資産の分類と管理**方法** ⑴ 情報資産の分類 本市における情報資産は、機密性、完全性及び可用性**を踏まえ、次の重要性の分類に従って分類する。**

改定後（新）	現行（旧）

【機密性による情報資産の分類】

分類	分類基準	取扱制限
自治体機密性３Ａ	行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」（平成２３年４月１日内閣総理大臣決定）に定める秘密文書に相当する文書	・支給された端末以外での作業の原則禁止（自治体機密性３の情報資産に対して） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
自治体機密性３Ｂ	行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	
自治体機密性３Ｃ	行政事務で取り扱う情報資産のうち、自治体機密性３B 以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	
自治体機密性２	行政事務で取り扱う情報資産のうち、自治体機密性３に相当する機密性は	

分類	重　要　性　の　分　類
Ⅰ	個人情報及び本市の業務上必要とする情報で、最小限の者のみが扱う情報
Ⅱ	情報の公開を予定していない情報
Ⅲ	外部に公開する情報のうち、業務上重要な情報
Ⅳ	上記以外の情報

改定後（新）			現行（旧）
	要しないが、直ちに一般に公表することを前提としていない情報資産		
自治体機密性１	自治体機密性２又は自治体機密性３の情報資産以外の情報資産	―	

【完全性による情報資産の分類】

分類	分類基準	取扱制限
自治体完全性２	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
自治体完全性１	自治体完全性２の情報資産以外の情報資産	―

【可用性による情報資産の分類】

分類	分類基準	取扱制限
自治体可用性２	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管

改定後（新）		現行（旧）
	遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	
自治体可用性１	**自治体可用性２の情報資産以外の情報資産**	―

⑵　情報資産の管理

ア　管理責任

(ｱ)　**中央電子計算組織管理者及び情報セキュリティ管理者**は、その所管する情報資産について管理責任を有する。

(ｲ)　中央電子計算組織管理者及び情報セキュリティ管理者は、所管する情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳を整備しなければならない。

(ｳ)　**中央電子計算組織管理者及び情報セキュリティ管理者は、**情報資産が複製又は伝送された場合には、複製等された情報資産も⑴の分類に基づき管理しなければならない。

イ　情報資産の分類の表示

職員等は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等**適正**な管理を行わなければならない。

ウ　情報の作成

(ｱ)　職員等は、業務上必要のない情報を作成してはならない。

(ｲ)　情報を作成する者は、情報の作成時に⑴の分類に基づき、当該情報

⑵　情報資産の管理

ア　管理責任

(ｱ)　**各所属長**は、その所管する情報資産について管理責任を有する。

(ｲ)　情報資産が複製又は伝送された場合には、複製等された情報資産も⑴の分類に基づき管理しなければならない。

(ｳ)　取出しが可能な電磁的記録媒体は、適切な管理を行わなければならない。

イ　情報資産の分類の表示

職員等は、情報資産について、**第三者が重要性の識別を容易に認識できないように留意しつつ、**ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等**適切**な管理を行わなければならない。

ウ　情報**資産**の作成

(ｱ)　職員等は、業務上必要のない情報**資産**を作成してはならない。

(ｲ)　情報**資産**を作成する者は、情報**資産**の作成時に⑴の分類に基づき、

改定後（新）	現行（旧）
の分類と**取扱制限**を定めなければならない。	当該情報**資産**の分類と**権限**を定めなければならない。
(ｳ) 情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。	(ｳ) 情報**資産**を作成する者は、作成途上の情報**資産**についても、紛失や流出等を防止しなければならない。また、情報**資産**の作成途上で不要になった場合は、当該情報**資産**を消去しなければならない。
エ 情報資産の入手	エ 情報資産の入手
(ｱ) 職員等が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。	(ｱ) 職員等が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。
(ｲ) 職員等以外の者が作成した情報資産を入手した者は、(1)の分類に基づき、当該情報の分類と取扱制限を定めなければならない。	(ｲ) 職員等以外の者が作成した情報資産を入手した者は、(1)の分類に基づき、当該情報資産の分類と権限を定めなければならない。
(ｳ) 情報資産を入手した者は、入手した情報資産の分類が不明な場合、中央電子計算組織管理者に判断を仰がなければならない。	(ｳ) 情報資産を入手した者は、入手した情報資産の分類が不明な場合、中央電子計算組織管理者に判断を仰がなければならない。
オ 情報資産の利用	オ 情報資産の利用 情報資産を利用する者は、情報資産の利用に関し、次の事項を遵守しなければならない。
(ｱ) 情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。	(ｱ) 業務以外の目的に情報資産を利用しないこと。
(ｲ) 情報資産を利用する者は、情報資産の分類に応じ、**適正**な取扱いをしなければならない。	(ｲ) 情報資産の分類に応じ、**適切**な取扱いをすること。
(ｳ) 情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。	(ｳ) 電磁的記録媒体に情報資産の分類が異なる情報資産が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱うこと。
カ 情報資産の保管	カ 情報資産の保管
(ｱ) 中央電子計算組織管理者及び情報セキュリティ**管理者**は、情報資産の分類に従って、情報資産を**適正**に保管しなければならない。	(ｱ) 中央電子計算組織管理者及び情報セキュリティ**担当者**は、情報資産の分類に従って、情報資産を**適切**に保管しなければならない。
(ｲ) 中央電子計算組織管理者及び情報セキュリティ**管理者**は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。	(ｲ) 中央電子計算組織管理者及び情報セキュリティ**担当者**は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

改定後（新）	現行（旧）
(ｳ)　中央電子計算組織管理者及び情報セキュリティ**管理者**は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。	(ｳ)　中央電子計算組織管理者及び情報セキュリティ**担当者**は、**重要な情報資産（分類Ⅰ）を収めた電磁的記録媒体、**利用頻度が低い電磁的記録媒体又は情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。
(ｴ)　中央電子計算組織管理者及び情報セキュリティ**管理者**は、**自治体機密性２以上、自治体完全性２又は自治体可用性２の情報**を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。	(ｴ)　中央電子計算組織管理者及び情報セキュリティ**担当者**は、**重要な情報資産（分類Ⅱ以上）**を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。
	(ｵ)　職員等は、情報資産の複製を庁外の保管場所へ移動する場合、当該保管場所からバックアップのために情報システムの設置場所に戻す場合及び業務上必要な場合には所定の手続を経た上で外部への持ち出し又は送付をしなければならない。
キ　情報の送信 **電子メール等により自治体機密性２以上の情報**を送信する者は、必要に応じ、パスワード等による暗号化を行わなければならない。	**ク**　情報**資産**の送信・提供・公表 **（※該当部抜粋）** (ｱ)　**重要な情報資産（分類Ⅱ以上）**を送信する者は、必要に応じ、パスワード等による暗号化を行わなければならない。
	(ｲ)から(ｴ)まで　略
ク　情報資産の運搬	**キ**　情報資産の運搬**・送付**
(ｱ)　車両等により**自治体機密性２以上の情報資産**を運搬する者は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、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。	(ｱ)　車両等により**重要な情報資産（分類Ⅱ以上）**を運搬する者は、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。
(ｲ)　**自治体機密性２以上の情報資産**を運搬する者は、中央電子計算組織管理者又は情報セキュリティ**管理者**に許可を得なければならない。	(ｲ)　**重要な情報資産（分類Ⅱ以上）**を運搬する者は、中央電子計算組織管理者又は情報セキュリティ**担当者**に許可を得なければならない。
	(ｳ)　電磁的記録媒体を送る場合は信頼できる者を選定し、複製の禁止及び電磁的記録媒体の物理的保護規定を定め、違反した場合の罰則規定を定めなければならない。また、郵送等の手段を取る場合はでき

改定後（新）	現行（旧）
	る限り安全な手段を講じること。
ケ　情報資産の提供・公表	**ク**　情報資産**の送信**・提供・公表**（※該当部再掲）**
(ｱ)　**自治体機密性２以上の情報資産**を外部に提供する者は、パスワード等による暗号化を行わなければならない。	(ｱ)　**略**
(ｲ)　**自治体機密性２以上の情報資産**を外部に提供する者は、情報セキュリティ**管理者**に許可を得なければならない。	(ｲ)　**重要な情報資産（分類Ⅱ以上）**を外部に提供する者は、パスワード等による暗号化を行わなければならない。
(ｳ)　情報セキュリティ**管理者**は、住民に公開する情報資産について、完全性を確保しなければならない。	(ｳ)　**重要な情報資産（分類Ⅱ以上）**を外部に提供する者は、情報セキュリティ**担当者**に許可を得なければならない。
	(ｴ)　情報セキュリティ**担当者**は、住民に公開する情報資産について、完全性を確保しなければならない。
コ　情報資産の廃棄等	**ケ**　情報資産の廃棄等
(ｱ)　情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。	(ｱ)　情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。
(ｲ)　情報資産の廃棄やリース返却等を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。	(ｲ)　情報資産の廃棄やリース返却等を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。
(ｳ)　情報資産の廃棄やリース返却等を行う者は、情報セキュリティ**管理者**の許可を得なければならない。	(ｳ)　情報資産の廃棄やリース返却等を行う者は、情報セキュリティ**担当者**の許可を得なければならない。
	６　特定個人情報等の取扱い **特定個人情報等の取扱いは、分類Ⅰの情報資産として、「武蔵村山市における特定個人情報等の取扱いに関する管理規程（平成２７年１２月２８日市長決裁）」に基づく安全管理措置を講じなければならない。**
５　情報システム全体の強靭性の向上	**７**　情報システム全体の強靭性の向上
(1)　マイナンバー利用事務系	(1)　マイナンバー利用事務系
ア　マイナンバー利用事務系と他の領域との分離	ア　マイナンバー利用事務系と他の領域との分離
マイナンバー利用事務系と他の領域を通信できないようにしなければ	マイナンバー利用事務系と他の領域を通信できないようにしなければ

改定後（新）	現行（旧）
ならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定（ＭＡＣアドレス、ＩＰアドレス）及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWAN を経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。	ならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定（ＭＡＣアドレス、ＩＰアドレス）及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWAN を経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。
イ　情報のアクセス及び持ち出しにおける対策	イ　情報のアクセス及び持ち出しにおける対策
(ｱ)　情報のアクセス対策 情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。また、業務ごとに専用端末を設置することが望ましい。	(ｱ)　情報のアクセス対策 情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。また、業務ごとに専用端末を設置することが望ましい。
(ｲ)　情報の持ち出し不可設定 原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。	(ｲ)　情報の持ち出し不可設定 原則として、ＵＳＢメモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。
(2)　**LGWAN 接続系**	(2)　**総合行政ネットワーク（LGWAN）接続系**
	ア　総合行政ネットワーク（LGWAN）とインターネット接続系の分割
LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを **LGWAN 接続系**に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。	**総合行政ネットワーク（LGWAN）接続**とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを**総合行政ネットワーク（LGWAN）接続系**に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。
ア　インターネット環境で受信したインターネットメールの本文のみを **LGWAN 接続系**に転送するメールテキスト化方式	(ｱ)　インターネット環境で受信したインターネットメールの本文のみを**総合行政ネットワーク（LGWAN）接続系**に転送するメールテキスト化方式
イ　インターネット接続系の端末から、**LGWAN 接続系**の端末へ画面を転送	(ｲ)　インターネット接続系の端末から、**総合行政ネットワーク（LGWAN）**

改定後（新）	現行（旧）
する方式	**接続系**の端末へ画面を転送する方式
ウ　危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式	(ｳ)　危険因子をファイルから除去し､又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式
⑶　インターネット接続系	⑶　インターネット接続系
ア　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と対処及び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。	ア　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と対処及び**総合行政ネットワーク（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。
イ　都道府県及び市区町村のインターネットとの通信を集約する自治体情報セキュリティクラウドに参加するとともに、関係省庁や都道府県等と連携しながら、情報セキュリティ対策を推進しなければならない。	イ　都道府県及び市区町村のインターネットとの通信を集約する自治体情報セキュリティクラウドに参加するとともに、関係省庁や都道府県等と連携しながら、情報セキュリティ対策を推進しなければならない。
６　物理的セキュリティ	**８**　物理的セキュリティ
６．１　サーバ等の管理	⑴　サーバ等の管理
⑴　機器の取付け	ア　機器の取付け
中央電子計算組織管理者は、サーバ等の機器の取付けを行う場合、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し、容易に取り外せないよう**適正**に固定する等、必要な措置を講じなければならない。	中央電子計算組織管理者は、サーバ等の機器の取付けを行う場合、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。
⑵　サーバの冗長化	イ　サーバの冗長化**等**
ア　中央電子計算組織管理者は、重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバを冗長化**し、同一**データを保持しなければならない。	(ｱ)　中央電子計算組織管理者は、重要情報を格納しているサーバ、セキュリティサーバ､住民サービスに関するサーバ及びその他の基幹サーバを冗長化**又は電磁的記録媒体等にバックアップを取る等**データを保持しなければならない。
イ　中央電子計算組織管理者は、サーバに障害が発生した場合に、速やかに**セカンダリサーバを起動**し、システムの運用停止時間を最小限にしなければならない。	(ｲ)　中央電子計算組織管理者は、サーバに障害が発生した場合に、速やかに**代替サーバを起動又はバックアップデータから起動等**し、システムの運用停止時間を最小限にしなければならない。

改定後（新）	現行（旧）
⑶　機器の電源	ウ　機器の電源
	中央電子計算組織管理者は、電子計算組織総括管理者及び施設管理部門と連携し、機器の電源について、次の事項を措置しなければならない。
ア　中央電子計算組織管理者は、電子計算組織総括管理者及び施設管理部門と連携し、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**適正**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なければならない。	(ｱ)　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に十分な電力を供給する容量の予備電源を備え付けること。
イ　中央電子計算組織管理者は、電子計算組織総括管理者及び施設管理部門と連携し、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。	(ｲ)　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ること。
⑷　通信ケーブル等の配線	エ　通信ケーブル等の配線
	中央電子計算組織管理者は、通信ケーブル等の配線について、次の事項を遵守しなければならない。
ア　中央電子計算組織管理者は、施設管理部門と連携し、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。	(ｱ)　施設管理部門と連携し、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ること。
イ　中央電子計算組織管理者は、主要な箇所の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、施設管理部門と連携して対応しなければならない。	(ｲ)　主要な箇所の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、施設管理部門と連携して対応すること。
ウ　中央電子計算組織管理者は、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**適正**に管理しなければならない。	(ｳ)　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**に管理すること。
エ　中央電子計算組織管理者は、自ら**又はデジタル推進課職員**及び契約により操作を認められた委託事業者以外の者が配線を変更、追加できないように必要な措置を講じなければならない。	(ｴ)　自ら及び契約により操作を認められた委託事業者以外の者**（端末使用許可者を含む。）**が配線を変更、追加できないように必要な措置を施すこと。
⑸　機器の定期保守及び修理	
ア　中央電子計算組織管理者は、自治体可用性２のサーバ等の機器の定	

改定後（新）	現行（旧）
期保守を実施しなければならない。 **イ　中央電子計算組織管理者は、電磁的記録媒体を内蔵する機器を事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、中央電子計算組織管理者は、事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。** ⑹　庁外への機器の設置 中央電子計算組織管理者は、庁外にサーバ等の機器を設置する場合、CISOの承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。 ⑺　機器の廃棄等 中央電子計算組織管理者及び**情報セキュリティ管理者**は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。 ６．２　管理区域の管理 ⑴　管理区域の構造等 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、当該機器等の管理及び運用を行うための部屋（以下「電算室」という。）や電磁的記録媒体の保管庫をいう。 イ　中央電子計算組織管理者は、管理区域を地階又は１階に設けてはならない。**また、外部からの侵入が容易にできないように無窓の外壁にするよう努めなければならない。** ウ　中央電子計算組織管理者は、**施設管理部門と連携して、**管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等に	オ　庁外への機器の設置 中央電子計算組織管理者は、庁外にサーバ等の機器を設置する場合、**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。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。 カ　機器の廃棄等 中央電子計算組織管理者及び**情報セキュリティ担当者**は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報資産を消去の上、復元不可能な状態にする措置を講じなければならない。 ⑵　管理区域の管理 ア　管理区域**（電算室等）**の構造等 (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、当該機器等の管理及び運用を行うための部屋（以下「電算室」という。）や電磁的記録媒体の保管庫をいう。 (ｲ)　中央電子計算組織管理者は、管理区域を地階又は１階に設けてはならない。 (ｳ)　中央電子計算組織管理者は、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立

改定後（新）	現行（旧）
よって許可されていない立入りを防止しなければならない。	入りを防止しなければならない。
エ　中央電子計算組織管理者は、電算室内の機器等に、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)　中央電子計算組織管理者は、電算室内の機器等に、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。**なお、電算室の機器類の配置は、緊急時に職員等が円滑に避難できるように配慮しなければならない。**
オ　中央電子計算組織管理者は、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部を全て塞がなければならない。	(ｵ)　中央電子計算組織管理者は、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部を全て塞がなければならない。
カ　中央電子計算組織管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器及び電磁的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。	(ｶ)　中央電子計算組織管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的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。
⑵　管理区域の入退室管理等	イ　管理区域の入退室管理等
ア　中央電子計算組織管理者は、管理区域への入退室を許可された者のみに制限し、IC カード、指紋認証等の生体認証や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。	(ｱ)　中央電子計算組織管理者は、管理区域への入退室を許可された者のみに制限し、IC カード、指紋認証等の生体認証や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　職員等及び委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。	(ｲ)　職員等及び委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。
ウ　中央電子計算組織管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。	
エ　中央電子計算組織管理者は、自治体機密性２以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しない、又は個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的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。	
⑶　機器等の搬入出	ウ　機器等の搬入出
	中央電子計算組織管理者は、機器等の搬入出について、次の事項を遵

改定後（新）	現行（旧）
	守しなければならない。
ア　中央電子計算組織管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員**等**又は委託事業者に確認を行わせなければならない。	(ｱ)　搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は委託事業者に確認を行うこと。
イ　中央電子計算組織管理者は、電算室の機器等の搬入出について、職員**等**を立ち会わせなければならない。	(ｲ)　電算室の機器等の搬入出について、職員を立ち会わせること。
６．３　通信回線及び通信回線装置の管理	(3)　通信回線及び通信回線装置の管理 中央電子計算組織管理者は、通信回線等の管理について、次の事項を遵守しなければならない。
(1)　中央電子計算組織管理者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、**適正**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**適正**に保管しなければならない。	ア　庁内の通信回線及び通信回線装置を、施設管理部門と連携し、**適切**に管理すること。また、通信回線及び通信回線装置に関連する文書を**適切**に保管すること。
(2)　中央電子計算組織管理者は、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施しなければならない。	
(3)　中央電子計算組織管理者は、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　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すこと。
(4)　中央電子計算組織管理者は、行政系のネットワークをLGWANに集約するように努めなければならない。	ウ　行政間のネットワークを**総合行政ネットワーク（LGWAN）**に集約するように努めること。
(5)　中央電子計算組織管理者は、**自治体機密性２以上の情報資産**を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、**適正**な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。	エ　**重要な情報資産（分類Ⅱ以上）**を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、**適切**な回線を選択すること。また、必要に応じ、送受信される情報**資産**の暗号化を行うこと。
(6)　中央電子計算組織管理者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように、**不正**	オ　ネットワークに使用する回線について、伝送途上に情報**資産**が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施

改定後（新）	現行（旧）
な通信の有無を監視する等の十分なセキュリティ対策を実施しなければならない。	すること。
⑺　中央電子計算組織管理者は、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順を定めなければならない。また、必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講じなければならない。	
⑻　中央電子計算組織管理者は、**自治体可用性２の情報**を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。	カ　**重要な情報資産（分類Ⅱ以上）**を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。
６．４　職員等の利用する端末**や電磁的記録媒体**等の管理	⑷　職員等のパソコン等の管理
⑴　**中央電子計算組織管理者及び情報セキュリティ管理者**は、盗難防止のため、執務室等で利用するパソコンのワイヤーによる固定、モバイル端末及び電磁的記録媒体の使用時以外の施錠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。	ア　**職員等**は、ノート型等の持ち運びが可能なパソコンを使用時間外は施錠のできる場所に保管又はワイヤーによる固定をしなければならない。また、デスクトップ型等の据置のパソコンは盗難防止のための物理的措置を講じなければならない。モバイル端末及び電磁的記録媒体についても、使用時以外の施錠管理等の物理的措置を講じなければならず、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。
⑵　中央電子計算組織管理者は、情報システムへの**ログインに際し、パスワード、スマートカード、或いは生体認証等複数の認証情報**の入力を必要とするように設定しなければならない。	イ　中央電子計算組織管理者は、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　中央電子計算組織管理者は、ログインパスワード以外に指紋認証等の多要素認証を併用しなければならない。
⑶　中央電子計算組織管理者は、端末の電源起動時のパスワード（BIOS パスワード、ハードディスクパスワード等）を併用するよう努めなければならない。	
⑷　中央電子計算組織管理者は、マイナンバー利用事務系では「知識」、「所	

改定後（新）	現行（旧）
持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証）を行うよう設定しなければならない。 **⑸　中央電子計算組織管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用するよう努めなければならない。** **⑹　中央電子計算組織管理者は、モバイル端末の庁外での業務利用の際は、上記対策に加え、遠隔消去機能を利用する等の措置を講じるよう努めなければならない。**	
7　人的セキュリティ 7．1　職員等の遵守事項 ⑴　情報セキュリティポリシー等の遵守 職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに中央電子計算組織管理者に相談し、指示を仰がなければならない。 ⑵　業務以外の目的での使用の禁止 職員等は、業務以外の目的で情報資産の外部への持ち出し、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。 ※7　7．1　⑳に記載	9　人的セキュリティ ⑴　職員等の遵守事項 ア　情報セキュリティポリシー等の遵守 職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに中央電子計算組織管理者に相談し、指示を仰がなければならない。 イ　業務以外の目的での使用の禁止 職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用、インターネットへのアクセス**及び電子商取引**を行ってはならない。 ウ　業務以外の目的でのウェブ閲覧の禁止 中央電子計算組織管理者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ担当者に通知し**適切**な措置を求めなければならない。

改定後（新）	現行（旧）
⑶　個人情報を含むデータへのパスワード設定 職員等は、個人情報に関する電磁的記録を保存する場合（電磁的記録媒体に保存する場合を含む。）には、パスワードを設定しなければならない。	エ　個人情報を含むデータへのパスワード設定 職員等は、個人情報に関する電磁的記録を保存する場合（電磁的記録媒体に保存する場合を含む。）には、パスワードを設定しなければならない。
⑷　モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限	オ　モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限
ア　CISOは、自治体機密性２以上、自治体可用性２、自治体完全性２の情報資産を外部で処理する場合における安全管理措置を定めなければならない。	
イ　職員等は、**本市の**モバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ**管理者**の許可を得なければならない。	職員等は、モバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ**担当者**の許可を得なければならない。
ウ　職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。	
⑸　支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用	カ　支給以外のパソコン、モバイル端末、電磁的記録媒体等の業務利用
ア　職員等は、支給以外のパソコン、モバイル端末**及び**電磁的記録媒体等を原則業務に利用してはならない。ただし、支給以外の端末の業務利用の可否判断をCISOが行った後に、業務上必要な場合は、電子計算組織統括管理者の定める実施手順に従い、中央電子計算組織管理者の許可を得て利用することができる。	職員等は、支給以外のパソコン、モバイル端末、電磁的記録媒体等を原則業務に利用してはならない。ただし、支給以外の端末の業務利用の可否判断を**最高情報セキュリティ責任者**が行った後に、業務上必要な場合は、電子計算組織統括管理者の定める実施手順に従い、中央電子計算組織管理者の許可を得て利用することができる。
イ　職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置に関する規定を遵守しなければならない。	
⑹　持ち出し及び持ち込みの記録 **情報セキュリティ管理者は、端末等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。**	

改定後（新）	現行（旧）
⑺　パソコンやモバイル端末におけるセキュリティ設定変更の禁止 職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を中央電子計算組織管理者の許可なく変更してはならない。	キ　パソコンやモバイル端末におけるセキュリティ設定変更の禁止 職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を中央電子計算組織管理者の許可なく変更してはならない。
⑻　机上の端末等の管理 職員等は、パソコン、モバイル端末、電磁的記録媒体**及び**情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ**管理者**の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、**適正**な措置を講じなければならない。	ク　机上の端末等の管理 職員等は、パソコン、モバイル端末、電磁的記録媒体**、**情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ**担当者**の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等を容易に閲覧されない場所へ保管する等、**適切**な措置を講じなければならない。
⑼　退職時等の遵守事項 職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。	ケ　退職時等の遵守事項 職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を、返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。
⑽　情報セキュリティポリシー等の掲示 **中央電子計算組織管理者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。**	
⑾　委託事業者に対する説明 **中央電子計算組織管理者及び情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を事業者に発注する場合、再委託事業者も含めて、情報セキュリティポリシー等のうち委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。**	
７．２　研修・訓練	⑵　研修・訓練
⑴　情報セキュリティに関する研修・訓練 電子計算組織総括管理者は、定期的に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。	ア　情報セキュリティに関する研修・訓練 電子計算組織総括管理者は、定期的に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。

改定後（新）	現行（旧）
⑵　研修**計画の策定及び**実施	イ　研修の実施
ア　電子計算組織総括管理者は、全ての職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行わなければならない。	
イ　研修計画において、職員等は毎年度情報セキュリティ研修を受講できるように努めなければならない。	
ウ　新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。	新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。
エ　研修は、電子計算組織におけるそれぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。	
オ　中央電子計算組織管理者は、研修の実施状況を分析、評価し、電子計算組織総括管理者に情報セキュリティ対策に関する研修の実施状況について報告しなければならない。	
カ　電子計算組織総括管理者は、電子計算組織管理運営委員会に対して、職員等の情報セキュリティ研修の実施状況について定期的に報告しなければならない。	
⑶　緊急時対応訓練	ウ　緊急時対応訓練
CISOは、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。	**電子計算組織総括管理者**は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。
⑷　研修・訓練への参加	エ　研修・訓練への参加
全ての職員等は、定められた研修・訓練に参加しなければならない。	職員等は、定められた研修・訓練に参加しなければならない。
7．3　情報セキュリティインシデントの報告	⑶　情報セキュリティインシデントの報告
⑴　庁内での情報セキュリティインシデントの報告	ア　庁内からの情報セキュリティインシデントの報告
ア　職員等は、情報セキュリティインシデントを認知した場合、速やか	(ｱ)　職員等は、情報セキュリティインシデントを認知した場合、速やか

改定後（新）	現行（旧）
に**情報セキュリティ管理者**に報告しなければならない。 イ　報告を受けた**情報セキュリティ管理者**は、速やかに**情報セキュリティ責任者及び中央電子計算組織管理者**に報告しなければならない。 **ウ　中央電子計算組織管理者は、報告のあった情報セキュリティインシデントについて、必要に応じて CISO 及び電子計算組織総括管理者に報告しなければならない。** **なお、行政委員会等の情報セキュリティ責任者は、当該行政委員会等の長に速やかに報告しなければならない。** **エ　情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報保護委員会へ報告しなければならない。** **⑵　住民等外部からの情報セキュリティインシデントの報告** **ア　職員等は、本市が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、速やかに情報セキュリティ管理者に報告しなければならない。** **イ　報告を受けた情報セキュリティ管理者は、速やかに情報セキュリティ責任者及び中央電子計算組織管理者に報告しなければならない。** **ウ　中央電子計算組織管理者は、当該情報セキュリティインシデントについて、必要に応じて CISO 及び電子計算組織総括管理者に報告しなければならない。** **なお、行政委員会等の情報セキュリティ責任者においては、行政委員会等の長にも速やかに報告しなければならない。** **エ　CISO は、情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けるための窓口の設置と、当該窓口への連絡手段を公表するよう努めなければならない。**	に**情報セキュリティ担当者**に報告しなければならない。 (ｲ)　報告を受けた**情報セキュリティ担当者**は、速やかに**中央電子計算組織管理者、総括情報セキュリティ担当者及び情報化推進委員会**に報告しなければならない。

改定後（新）	現行（旧）
⑶　情報セキュリティ会議・緊急対策会議の招集 電子計算組織総括管理者**及び中央電子計算組織管理者は、行政運営に及ぼす影響等に応じて情報セキュリティ会議又は緊急対策会議を招集しなければならない。**	イ　情報セキュリティ会議・緊急対策会議の招集 電子計算組織総括管理者**は、報告内容を検討し、市民生活に影響を及ぼすおそれがあると認めるときは情報セキュリティ会議を招集しなければならない。また、市民生活に影響がなく、他のシステムに影響を及ぼすと認められるときは、中央電子計算組織管理者に緊急対策会議の招集を命ずることとする。**
⑷　情報セキュリティインシデント原因の究明・記録、再発防止等 **ア　情報セキュリティ会議等は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。** **イ　情報セキュリティ会議等は、情報セキュリティインシデントであると評価した場合、CISO にその詳細を速やかに報告しなければならない。** **ウ　情報セキュリティ会議等は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。また、情報セキュリティ会議等は、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システム責任者へ確認を指示しなければならない。**	ウ　情報セキュリティインシデント原因の究明・記録、再発防止等
エ　**情報セキュリティ会議等は、**これらの情報セキュリティインシデント原因を究明し、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の結果から、再発防止策を検討し、CISO に報告しなければならない。	(ｱ)　**中央電子計算組織管理者は、情報セキュリティインシデントを引き起こした部門の総括情報セキュリティ担当者、情報セキュリティ担当者及び情報化推進委員会と連携し、**これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。 (ｲ)　**情報化推進委員会は、**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、**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。

改定後（新）	現行（旧）
オ　CISOは、**情報セキュリティ会議等**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。	(ｳ)　**最高情報セキュリティ責任者**は、**情報化推進委員会**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講じなければならない。
7．4　ID及びパスワード等の管理	⑷　ID及びパスワード等の管理
⑴　ICカード等の取扱い	ア　ICカード等の取扱い
ア　職員等は、自己の管理するICカード等に関し、次の事項を遵守しなければならない。	(ｱ)　職員等は、自己の管理するICカード等に関し、次の事項を遵守しなければならない。
(ｱ)　認証に用いるICカード等を、職員等間で共有してはならない。ただし、共有端末装置においてはこの限りではない。	a　認証に用いるICカード等を、職員等間で共有してはならない。ただし、共有端末装置においてはこの限りではない。
(ｲ)　業務上必要のないときは、IC カード等をカードリーダ又はパソコン等の端末のスロット等から抜いておかなければならない。	b　業務上必要のないときは、IC カード等をカードリーダ又はパソコン等の端末のスロット等から抜いておかなければならない。
(ｳ)　IC カード等を紛失した場合には、速やかに中央電子計算組織管理者に通報し、指示に従わなければならない。	c　IC カード等を紛失した場合には、速やかに中央電子計算組織管理者に通報し、指示に従わなければならない。
イ　中央電子計算組織管理者は、IC カード等の紛失等の通報があり次第、当該 IC カード等を使用したアクセス等を速やかに停止しなければならない。	(ｲ)　中央電子計算組織管理者は、IC カード等の紛失等の通報があり次第、当該ICカード等を使用したアクセス等を速やかに停止しなければならない。
ウ　中央電子計算組織管理者は、ICカード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。	(ｳ)　中央電子計算組織管理者は、IC カード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。
⑵　IDの取扱い	イ　IDの取扱い
職員等は、自己の管理するIDに関し、次の事項を遵守しなければならない。	職員等は、自己の管理するIDに関し、次の事項を遵守しなければならない。
ア　自己が利用しているIDは、他人に利用させてはならない。	(ｱ)　自己が利用しているIDは、他人に利用させてはならない。
イ　共用IDを利用する場合は、共用IDの利用者以外に利用させてはならない。	(ｲ)　共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

改定後（新）	現行（旧）
⑶　パスワードの取扱い 職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。	ウ　パスワードの取扱い 職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。
ア　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。	(ｱ)　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。
イ　パスワードを秘密にし、パスワードの照会等には一切応じてはならない。	(ｲ)　パスワードを秘密にし、パスワードの照会等には一切応じてはならない。
ウ　パスワードは十分な長さとし、文字列は想像しにくいもの**（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）**にしなければならない。	(ｳ)　パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。
エ　パスワードが流出したおそれがある場合には、中央電子計算組織管理者に速やかに報告し、パスワードを速やかに変更しなければならない。	(ｴ)　パスワードが流出したおそれがある場合には、中央電子計算組織管理者に速やかに報告し、パスワードを速やかに変更しなければならない。
オ　複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。	
カ　仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。	
キ　**サーバ、ネットワーク機器及び**パソコン等の端末に、パスワードを記憶させ**ることで、パスワードの入力なしに認証を可能とする設定は行ってはならない。**	(ｵ)　パソコン等の端末にパスワードを記憶させてはならない。
ク　職員等間でパスワードを共有してはならない**（ただし、共用 ID に対するパスワードは除く）**。	(ｶ)　職員等間でパスワードを共有してはならない。**ただし、共有端末装置においてはこの限りではない。**
8　技術的セキュリティ	１０　技術的セキュリティ
8．1　コンピュータ及びネットワークの管理	⑴　コンピュータ及びネットワークの管理
⑴　ファイルサーバの設定等	ア　ファイルサーバの設定等 中央電子計算組織管理者は、ファイルサーバの設定等について、次の事項を措置しなければならない。

改定後（新）	現行（旧）
ア　中央電子計算組織管理者は、職員等が使用できるファイルサーバの容量を設定し、職員等に周知しなければならない。 イ　中央電子計算組織管理者は、ファイルサーバを課等の単位で構成し、職員等が他課等のフォルダ及びファイルを閲覧及び使用できないように設定しなければならない。 **ウ　中央電子計算組織管理者は、住民の個人情報、人事記録等、特定の職員等しか取り扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一課室等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。**	(ｱ)　職員等が使用できるファイルサーバの容量を設定し、職員等に周知すること。 (ｲ)　ファイルサーバを課等の単位で構成し、職員等が他課等のフォルダ及びファイルを閲覧及び使用できないように、設定すること。
⑵　バックアップの実施 ア　中央電子計算組織管理者**及び情報セキュリティ管理者**は、**業務システムのデータベースや**ファイルサーバ等に記録された情報について、サーバの冗長化対策にかかわらず、必要に応じて定期的にバックアップを実施しなければならない。 **イ　中央電子計算組織管理者及び情報セキュリティ管理者は、重要な情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得しなければならない。** **ウ　中央電子計算組織管理者及び情報セキュリティ管理者は、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しなければならない。**	イ　バックアップの実施 中央電子計算組織管理者は、ファイルサーバ等に記録された情報資産について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。
⑶　他団体との情報システムに関する情報等の交換 **中央電子計算組織管理者及び**情報セキュリティ**管理者**は、他の団体と情報システムに関する情報（サーバやネットワークの設定等の情報）を交換する場合、その取扱いに関する事項をあらかじめ定め、**電子計算組織総括管理者及び情報セキュリティ責任者**の許可を得なければならない。	ウ　他団体との情報システムに関する情報等の交換 情報セキュリティ**担当者**は、他の団体と情報システムに関する情報（サーバやネットワークの設定等の情報）を交換する場合、その取扱いに関する事項をあらかじめ定め、**総括情報セキュリティ担当者及び中央電子計算組織管理者**の許可を得なければならない。

改定後（新）	現行（旧）
⑷　システム管理記録及び作業の確認	エ　システム管理記録及び作業の確認
	中央電子計算組織管理者及び情報セキュリティ担当者は、システム管理記録及び作業の確認について、次の事項を遵守しなければならない。
ア　中央電子計算組織管理者及び情報セキュリティ管理者は、所管する情報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。	(ｱ)　所管する情報システムの運用において実施した作業について、作業記録を作成すること。
イ　中央電子計算組織管理者及び情報セキュリティ管理者は、所管するシステムにおいて、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に**適正**に管理し、**運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければならない。**	(ｲ)　所管するシステムにおいて、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に**適切**に管理すること。
ウ　職員等及び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。	
⑸　情報システム仕様書等の管理	オ　情報システム仕様書等の管理
中央電子計算組織管理者**及び情報セキュリティ管理者**は、ネットワーク構成図、情報システム仕様書について、記録媒体にかかわらず、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、**適正**に管理しなければならない。また、構築に際して事業者に委託した場合、当該事業者に守秘義務を課さなければならない。	中央電子計算組織管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、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。また、構築に際して事業者に委託した場合、当該事業者に守秘義務を課さなければならない。
⑹　ログの取得等	カ　ログの取得等
	中央電子計算組織管理者は、ログの取得等について、次の事項を遵守しなければならない。
ア　中央電子計算組織管理者は、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し、一定の期間保存しなければならない。	(ｱ)　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し、一定の期間保存すること。
イ　中央電子計算組織管理者は、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、	

改定後（新）	現行（旧）
適正にログを管理しなければならない。	
ウ　中央電子計算組織管理者は、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。また、必要に応じて情報セキュリティ担当者にアクセス記録を通知すること。	(ｲ)　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すること。また、必要に応じて情報セキュリティ担当者にアクセス記録を通知すること。
⑺　障害記録 中央電子計算組織管理者は、職員等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、**適正**に保存しなければならない。	キ　障害記録 中央電子計算組織管理者は、職員等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。
⑻　ネットワークの接続制御、経路制御等	ク　ネットワークの接続制御、経路制御等 中央電子計算組織管理者は、ネットワークの制御等について、次の事項を遵守しなければならない。
ア　中央電子計算組織管理者は、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、ファイアウォールや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。	(ｱ)　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、ファイアウォール等の通信ソフトウェア等を設定すること。
イ　中央電子計算組織管理者は、不正アクセスを防止するため、ネットワークに**適正**なアクセス制御を施さなければならない。	(ｲ)　不正アクセスを防止するため、ネットワークに**適切**なアクセス制御を行うこと。
ウ　中央電子計算組織管理者は、保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保しなければならない。また、情報セキュリティ対策について、定期的な確認により必要に応じて見直さなければならない。	
⑼　外部の者が利用できるシステムの分離等 中央電子計算組織管理者は、電子申請の受付システム等、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。	ケ　外部の者が利用できるシステムの分離等 中央電子計算組織管理者は、電子申請の**汎用**受付システム等、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

改定後（新）	現行（旧）
⑽　外部ネットワークとの接続制限等 ア　中央電子計算組織管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、CISO及び電子計算組織総括管理者の許可を得なければならない。 イ　中央電子計算組織管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内の全てのネットワーク、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なければならない。 ウ　中央電子計算組織管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、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　中央電子計算組織管理者は、ウェブサーバ等をインターネットに公開する場合、次のセキュリティ対策を実施しなければならない。 (ｱ)　庁内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上で接続しなければならない。 **(ｲ)　脆弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用しなければならない。** **(ｳ)　ウェブサーバからの不用意な情報漏えいを防止するための措置を講じなければならない。** **(ｴ)　ウェブコンテンツの編集作業を行う主体を限定しなければならない。** **(ｵ)　インターネットを介して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よう努めなければならない。**	コ　外部ネットワークとの接続制限等 (ｱ)　中央電子計算組織管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、**最高情報セキュリティ責任者**及び電子計算組織総括管理者の許可を得なければならない。 (ｲ)　中央電子計算組織管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内の全てのネットワーク、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なければならない。 (ｳ)　中央電子計算組織管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、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)　中央電子計算組織管理者は、ウェブサーバ等をインターネットに公開する場合、庁内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上で接続しなければならない。

改定後（新）	現行（旧）
オ　**中央電子計算組織管理者及び情報セキュリティ管理者**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、情報資産に脅威が生じることが想定される場合には、**電子計算組織総括管理者**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。この場合、中央電子計算組織管理者は、電子計算組織総括管理者に報告するとともに、市長を通じ、武蔵村山市個人情報保護審議会に報告しなければならない。	(ｵ)　**情報セキュリティ担当者**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、情報資産に脅威が生じることが想定される場合には、**中央電子計算組織管理者**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。この場合、中央電子計算組織管理者は、電子計算組織総括管理者に報告するとともに、市長を通じ､武蔵村山市個人情報保護審議会に報告しなければならない。
⑾　複合機のセキュリティ管理	サ　複合機等のセキュリティ管理
ア　中央電子計算組織管理者及び情報セキュリティ管理者は、複合機を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。	
イ　中央電子計算組織管理者**及び情報セキュリティ管理者**は、複合機が備える機能について**適正**な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。	(ｱ)　中央電子計算組織管理者は、複合機が備える機能について**適切**な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。
ウ　中央電子計算組織管理者**及び情報セキュリティ管理者**は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消し、又は再利用できないようにする対策を講じなければならない。	(ｲ)　中央電子計算組織管理者は、複写機の運用を終了する場合、複写機の持つ電磁的記録媒体の全ての情報を抹消し、又は再利用できないようにする対策を講じなければならない。
⑿　IoT 機器を含む特定用途機器のセキュリティ管理 **中央電子計算組織管理者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。**	
⒀　無線 LAN **のセキュリティ対策**及びネットワークの盗聴対策	シ　無線 LAN 及びネットワークの盗聴対策 中央電子計算組織管理者は、無線 LAN 及びネットワークの盗聴対策について、次の事項を遵守しなければならない。

改定後（新）	現行（旧）
ア　中央電子計算組織管理者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。	(ｱ)　無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けること。
イ　中央電子計算組織管理者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。	(ｲ)　機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じること。
⑭　電子メールのセキュリティ管理	ス　電子メールのセキュリティ管理 中央電子計算組織管理者は、電子メールのセキュリティ管理について、次の事項を措置しなければならない。
ア　中央電子計算組織管理者は、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（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。	(ｱ)　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（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行うこと。
イ　中央電子計算組織管理者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。	(ｲ)　スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止すること。
ウ　中央電子計算組織管理者は、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不可能にしなければならない。	(ｳ)　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すること。
エ　中央電子計算組織管理者は、職員等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、上限を超えないよう職員等に周知しなければならない。	(ｴ)　職員等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、上限を超えないよう職員等に周知すること。
オ　中央電子計算組織管理者は、システム開発や運用、保守等のため庁舎内に常駐している委託事業者の作業員による電子メールアドレス利用について、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。	(ｵ)　システム開発や運用、保守等のため庁舎内に常駐している委託事業者の作業員による電子メールアドレス利用について、委託事業者との間で利用方法を取り決めること。
カ　中央電子計算組織管理者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように添付ファイルの監視等によりシステム上措置を講じるよう努めなければならない。	

改定後（新）	現行（旧）
⑮　電子メールの利用制限	セ　電子メールの利用制限
	職員等は、電子メールの利用について、次の事項を厳守しなければならない。
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。	(ｱ)　自動転送機能を用いて、電子メールを転送しないこと。
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。	(ｲ)　業務上必要のない送信先に電子メールを送信しないこと。
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。	(ｳ)　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すること。
エ　職員等は、重要な電子メールを誤送信した場合、中央電子計算組織管理者及び情報セキュリティ管理者に報告しなければならない。	(ｴ)　重要な電子メールを誤送信した場合、中央電子計算組織管理者及び情報セキュリティ担当者に報告すること。
オ　ウェブで利用できる電子メール、ネットワークストレージサービス等を使用する場合は、中央電子計算組織管理者の許可を得なければならない。	(ｵ)　ウェブで利用できる電子メール、ネットワークストレージサービス等を使用する場合は、中央電子計算組織管理者の許可を得ること。
⑯　電子署名・暗号化	ソ　電子署名・暗号化
ア　職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、**CISOが定めた**電子署名、パスワード等による暗号化等、セキュリティを考慮して、送信しなければならない。	職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、電子署名、パスワード等による暗号化等、セキュリティを考慮して、送信しなければならない。
イ　職員等は、暗号化を行う場合にCISOが定める以外の方法を用いてはならない。また、CISOが定めた方法で暗号のための鍵を管理しなければならない。	
ウ　CISOは、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。	
⑰　無許可ソフトウェアの導入等の禁止	タ　無許可ソフトウェアの導入等の禁止
ア　職員等は、パソコンやモバイル端末に無断でソフトウェアを導入し	

改定後（新）	現行（旧）
<u>てはならない。</u> イ　職員等は、業務上の必要がある場合は、中央電子計算組織管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ**<u>管理者</u>**は、ソフトウェアのライセンスを管理しなければならない。 ウ　職員等は、不正にコピーしたソフトウェアを利用してはならない。 エ　中央電子計算組織管理者は許可を行うに当たり、当該ソフトウェアがセキュリティ上安全であるか確認しなければならない。 オ　無許可で標準実装以外のアプリケーションソフトをパソコンにインストールし、又はデスクトップ等の設定を変更した職員等は、端末装置の使用を禁止する。	(ｱ)　職員等は、業務上の必要がある場合は、中央電子計算組織管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ**<u>担当者</u>**は、ソフトウェアのライセンスを管理しなければならない。 (ｲ)　職員等は、不正にコピーしたソフトウェアを利用してはならない。 (ｳ)　中央電子計算組織管理者は許可を行うに当たり、当該ソフトウェアがセキュリティ上安全であるか確認しなければならない。 (ｴ)　無許可で標準実装以外のアプリケーションソフトをパソコンにインストールし、又はデスクトップ等の設定を変更した職員等は、端末装置の使用を禁止する。
⑱　機器構成の変更の制限 ア　職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。 イ　職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、中央電子計算組織管理者及び情報セキュリティ**<u>管理者</u>**の許可を得なければならない。	チ　機器構成の変更の制限 職員等は、機器構成の変更の制限について、次の事項を厳守しなければならない。 (ｱ)　パソコンやモバイル端末に対し機器の改造及び増設・交換を行わないこと。 (ｲ)　業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、中央電子計算組織管理者及び情報セキュリティ**<u>担当者</u>**の許可を得ること。
⑲　業務外ネットワークへの接続の禁止 ア　職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう情報セキュリティ**<u>管理者</u>**によって定められたネットワークと異なるネットワークに接続してはならない。 イ　中央電子計算組織管理者は、支給した端末について、端末に搭載された OS のポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限することが望ましい。	ツ　業務外ネットワークへの接続の禁止 (ｱ)　職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう情報セキュリティ**<u>担当者</u>**によって定められたネットワークと異なるネットワークに接続してはならない。 (ｲ)　中央電子計算組織管理者は、支給した端末について、端末に搭載された OS のポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限することが望ましい。

改定後（新）	現行（旧）
⑳　業務以外の目的でのウェブ閲覧の禁止	ウ　業務以外の目的でのウェブ閲覧の禁止**（※９(1)ウ再掲）**
ア　職員等は、業務以外の目的でウェブを閲覧してはならない。	
イ　中央電子計算組織管理者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し**適正**な措置を求めなければならない。	中央電子計算組織管理者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ担当者に通知し**適切**な措置を求めなければならない。
㉑　Web 会議サービスの利用時の対策	テ　Web 会議サービスの利用時の対策
ア　電子計算組織総括管理者は、Web 会議を適切に利用するための利用手順を定めなければならない。	(ｱ)　電子計算組織統括管理者は、Web 会議を適切に利用するための利用手順を定めなければならない。
イ　職員等は、本市の定める利用手順に従い、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すること。	(ｲ)　職員等は、本市の定める利用手順に従い、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すること。
ウ　職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。	(ｳ)　職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。
エ　職員等は、外部から Web 会議に招待される場合は、本市の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。	(ｴ)　職員等は、外部から Web 会議に招待される場合は、本市の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。
㉒　ソーシャルメディアサービスの利用	(5)　ソーシャルメディアサービスの利用**（※１２(5)再掲）**
ア　**情報セキュリティ管理者**は、本市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。	ア　**中央電子計算組織管理者**は、本市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めた運用手順を定めなければならない。
(ｱ)　本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。	(ｱ)　本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を行うこと。
(ｲ)　パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（**ハードディスク、USB メモリ、紙等**）等を**適正**に管理す	(ｲ)　パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（**IC カード等**）等を**適切**に管理するなどの方法で、不正アクセス

改定後（新）	現行（旧）
るなどの方法で、不正アクセス対策を実施すること。	対策を行うこと。
イ　**自治体機密性２以上の情報**はソーシャルメディアサービスで発信してはならない。	イ　**重要な情報資産（分類Ⅱ以上）**はソーシャルメディアサービスで発信してはならない。
ウ　利用するソーシャルメディアサービスごとの責任者を定めなければならない。	ウ　利用するソーシャルメディアサービスごとの責任者を定めなければならない。
エ　アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。	エ　アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。
オ　自治体可用性２の情報の提供にソーシャルメディアサービスを用いる場合は、本市の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。	
８．２　アクセス制御	
⑴　アクセス制御**等**	⑵　アクセス制御
ア　アクセス制御	ア　アクセス制御
中央電子計算組織管理者及び情報セキュリティ**管理者**は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように**必要最小限の範囲で適切に設定する等、**システム上制限しなければならない。	中央電子計算組織管理者及び情報セキュリティ**担当者**は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、**ID、パスワードの設定等の措置を講じ、**システム上制限しなければならない。
イ　利用者 ID の取扱い	イ　利用者 ID の取扱い
㋐　中央電子計算組織管理者及び情報セキュリティ**管理者**は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職に伴う利用者 ID **の取扱い等の方法を定めなければならない。**	㋐　中央電子計算組織管理者及び情報セキュリティ**担当者**は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職に伴う利用者 ID **を適切に取り扱わなければならない。**
㋑　**職員等**は、業務上必要がなくなった場合は、利用者登録を抹消するよう、中央電子計算組織管理者に通知しなければならない。	㋑　**情報セキュリティ担当者**は、業務上必要がなくなった場合は、利用者登録を抹消するよう、中央電子計算組織管理者に通知しなければならない。
㋒　中央電子計算組織管理者及び情報セキュリティ**管理者**は、利用されていない ID が放置されないよう、職員課と連携し、点検しな	㋒　中央電子計算組織管理者及び情報セキュリティ**担当者**は、利用されていない ID が放置されないよう、職員課と連携し、点検しなければな

改定後（新）	現行（旧）
ければならない。 **(エ) 中央電子計算組織管理者及び情報セキュリティ管理者は、各 ID に対して不要なアクセス権限が付与されていないか定期的に確認しなければならない。** ウ　特権を付与された ID の管理等 (ア) 中央電子計算組織管理者及び情報セキュリティ**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。 **(イ) 中央電子計算組織管理者及び情報セキュリティ管理者は、管理者権限の特権を持つ ID 及びパスワードや主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講じなければならない。** (ウ) **電子計算組織総括管理者及び**中央電子計算組織管理者の管理者の特権を代行する者は、**電子計算組織総括管理者**が指名し、CISO が認めた者でなければならない。 **(エ) CISO は、代行者を認めた場合、速やかに電子計算組織総括管理者、中央電子計算組織管理者、情報セキュリティ責任者及び情報セキュリティ管理者に通知しなければならない。** **(オ) 中央電子計算組織管理者及び情報セキュリティ管理者は、特権を付与された ID 及びパスワードの変更について、委託事業者に行わせてはならない。** **(カ) 中央電子計算組織管理者及び情報セキュリティ管理者は、特権を付与された ID 及びパスワードについて、人事異動の際のパスワードの変更、入力回数制限等のセキュリティ機能を強化しなければならない。**	らない。 ウ　特権を付与された ID の管理等 (ア) 中央電子計算組織管理者及び情報セキュリティ**担当者**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。 (イ) 中央電子計算組織管理者の管理者の特権を代行する者は、**中央電子計算組織管理者**が指名し、**最高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。

改定後（新）	現行（旧）
(ｷ)　中央電子計算組織管理者**及び情報セキュリティ管理者**は、特権を付与された ID を初期設定以外のものに変更しなければならない。	(ｳ)　中央電子計算組織管理者は、特権を付与された ID を初期設定以外のものに変更しなければならない。
⑵　職員等による外部からのアクセス等の制限	エ　職員等による外部からのアクセス等の制限
ア　職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、中央電子計算組織管理者及び**当該情報システムを管理する情報セキュリティ管理者**の許可を得なければならない。	(ｱ)　職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、**電子計算組織統括管理者及び**中央電子計算組織管理者の許可を得なければならない。
イ　電子計算組織総括管理者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、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。	(ｲ)　電子計算組織統括管理者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、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　電子計算組織総括管理者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。	(ｳ)　電子計算組織統括管理者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。
エ　電子計算組織総括管理者は、外部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)　電子計算組織統括管理者は、外部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。
オ　電子計算組織総括管理者及び中央電子計算組織管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、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)　電子計算組織統括管理者及び中央電子計算組織管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、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。
カ　職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁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、パッチの適用状況等を確認し、情報セキュリティ管理者の許可を得るか、又は情報セキュリティ管理者によって事前に定義されたポリシーに従って接続しなければならない。	(ｶ)　職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁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、パッチの適用状況等を確認し、情報セキュリティ担当者の許可を得るか、又は情報セキュリティ担当者によって事前に定義されたポリシーに従って接続しなければならない。
キ　電子計算組織総括管理者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者の ID、パスワード及び生体認証に係る情報等の認証情報並びに	(ｷ)　電子計算組織統括管理者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合には、利用者の ID、パスワード及び生体認証に係る情報等の認証情報並

改定後（新）	現行（旧）
これを記録した媒体（IC カード等）による認証に加えて通信内容の暗号化等、情報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。 ⑶　自動識別の設定 中央電子計算組織管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。 ⑷　ログイン時の表示等 中央電子計算組織管理者は、ログイン時におけるメッセージ、**ログイン試行回数の制限、**アクセスタイムアウトの設定及びログイン・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。 ⑸　**認証**情報の管理 ア　中央電子計算組織管理者は、職員等の**認証**情報を厳重に管理しなければならない。**認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。** **イ　中央電子計算組織管理者及び情報セキュリティ管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回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。** **ウ　中央電子計算組織管理者及び情報セキュリティ管理者は、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。** **⑹　特権による接続時間の制限** **中央電子計算組織管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。**	びにこれらを記録した媒体（IC カード等）による認証に加えて通信内容の暗号化等、情報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　自動識別の設定 中央電子計算組織管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。 カ　ログイン時の表示等 中央電子計算組織管理者は、ログイン時におけるメッセージ、アクセスタイムアウトの設定及びログイン・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。 キ　**パスワードに関する**情報の管理 中央電子計算組織管理者は、職員等の**パスワードに関する**情報を厳重に管理しなければならない。

改定後（新）	現行（旧）
８．３　システム開発、導入、保守等	⑶　システム開発、導入、保守等
⑴　機器等の調達に係る運用規程の整備 **ア　中央電子計算組織管理者は、機器等の選定基準を運用規程として整備しなければならない。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられないような対策を講じなければならない。** **イ　中央電子計算組織管理者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備しなければならない。**	
⑵　機器等及び情報システムの調達	ア　情報システムの調達 中央電子計算組織管理者及び情報セキュリティ**担当者**は、情報システムの調達について、次の事項を措置しなければならない。
ア　中央電子計算組織管理者及び情報セキュリティ**管理者**は、情報システムの開発に当たっては、武蔵村山市情報システム調達基本方針を遵守しなければならない。	(ｱ)　情報システムの開発に当たっては、武蔵村山市情報システム調達基本方針を遵守しなければならない。
イ　中央電子計算組織管理者及び情報セキュリティ**管理者**は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。**また、業務システムに誤ったプログラムが組み込まれないよう、不具合等を考慮した技術的なセキュリティ機能を調達仕様書に記載しなければならない。**	(ｲ)　情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記すること。
ウ　中央電子計算組織管理者及び情報セキュリティ**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問題のないことを確認しなければならない。	(ｳ)　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問題のないことを確認すること。
⑶　情報システムの開発	イ　情報システムの開発
ア　システム開発における責任者及び作業者の特定 中央電子計算組織管理者及び情報セキュリティ**管理者**は、システム開発の責任者及び作業者を特定しなければならない。また、システム	(ｱ)　システム開発における責任者及び作業者の特定 中央電子計算組織管理者及び情報セキュリティ**担当者**は、システム開発の責任者及び作業者を特定しなければならない。また、システム開

改定後（新）	現行（旧）
開発のための規則を確立しなければならない。	発のための規則を確立しなければならない。**開発を外部に委託する場合、中央電子計算組織管理者及び情報セキュリティ担当者は、業者のシステム開発責任者及び作業者を特定しなければならない。**
イ　システム開発における責任者、作業者の ID の管理	(ｲ)　システム開発における責任者、作業者の ID の管理 中央電子計算組織管理者及び情報セキュリティ**担当者**は、システム開発における責任者等の管理について、次の事項を遵守しなければならない。
(ｱ)　中央電子計算組織管理者及び情報セキュリティ**管理者**は、システム開発の責任者及び作業者が使用する ID を管理し、開発完了後、開発用 ID を削除しなければならない。	a　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。
(ｲ)　中央電子計算組織管理者及び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のアクセス権限を設定しなければならない。	b　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　システム開発に用いるハードウェア及びソフトウェアの管理	(ｳ)　システム開発に用いるハードウェア及びソフトウェアの管理 中央電子計算組織管理者及び情報セキュリティ**担当者**は、システム開発の機器等の管理について、次の事項を遵守しなければならない。
(ｱ)　中央電子計算組織管理者及び情報セキュリティ**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、**それ以外のものを使用させてはならない。**	a　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すること。
(ｲ)　中央電子計算組織管理者及び情報セキュリティ**管理者**は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。	b　利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除すること。
エ　アプリケーション・コンテンツの開発時の対策 中央電子計算組織管理者及び情報セキュリティ**管理者**は、**ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。**	**(ｴ)　システム開発におけるリスクの分析** 中央電子計算組織管理者及び情報セキュリティ**担当者**は、**システム開発の事故・不正行為にかかるリスクを分析しなければならない。**

改定後（新）	現行（旧）
	(ｵ) システム開発における機器の搬出入 **機器の搬出入の際、中央電子計算組織管理者及び情報セキュリティ担当者は、許可及び確認しなければならない。**
⑷ 情報システムの導入	ウ 情報システムの導入
ア 開発環境と運用環境の分離及び移行手順の明確化	(ｱ) 開発環境と運用環境の分離及び移行手順の明確化 中央電子計算組織管理者及び情報セキュリティ**担当者**は、開発環境等について、次の事項を遵守しなければならない。
(ｱ) 中央電子計算組織管理者及び情報セキュリティ**管理者**は、システム開発､保守及びテスト環境とシステム運用環境を分離しなければならない。	a システム開発、保守及びテスト環境とシステム運用環境を分離すること。
(ｲ) 中央電子計算組織管理者及び情報セキュリティ**管理者**は、システム開発･保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。	b システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にすること。
(ｳ) 中央電子計算組織管理者及び情報セキュリティ**管理者**は、移行の際、情報システムに記録されている情報資産の保存を確実に行い､移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。	c 移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮すること。
(ｴ) 中央電子計算組織管理者及び情報セキュリティ**管理者**は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。	d 導入するシステムやサービスの可用性が確保されていることを確認した上で導入すること。
イ テスト	(ｲ) テスト 中央電子計算組織管理者及び情報セキュリティ**担当者**は、テストを実施する際、次の事項を遵守しなければならない。
(ｱ) 中央電子計算組織管理者及び情報セキュリティ**管理者**は、新たに情報システムを導入する場合､既に稼働している情報システムに接続する前に十分なテストを行わなければならない。	a 新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分なテストを行うこと。

改定後（新）	現行（旧）
(ｲ)　中央電子計算組織管理者及び情報セキュリティ**管理者**は、運用テストを行う場合､あらかじめ擬似環境による操作確認を行わなければならない。	b　運用テストを行う場合、あらかじめ擬似環境による操作確認を行うこと。
(ｳ)　中央電子計算組織管理者及び情報セキュリティ**管理者**は、個人情報及び機密性の高い生データを､テストデータに使用してはならない。	c　個人情報及び機密性の高い生データを、テストデータに使用しないこと。
(ｴ)　中央電子計算組織管理者及び情報セキュリティ**管理者**は、開発したシステムについて受け入れテストを行う場合､開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。	d　開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行うこと。
(ｵ)　中央電子計算組織管理者及び情報セキュリティ管理者は、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮したテスト計画を策定し､確実に検証が実施されるよう､必要かつ適切に委託事業者の監督を行わなければならない。	
ウ　機器等の納入時又は情報システムの受入れ時	
(ｱ)　中央電子計算組織管理者及び情報セキュリティ管理者は、機器等の納入時又は情報システムの受入れ時の確認･検査において､調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認しなければならない。	
(ｲ)　中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。	
⑸　情報システムの基盤を管理又は制御するソフトウェア導入時の対策	
ア　中央電子計算組織管理者及び情報セキュリティ管理者は、ソフトウェアを導入する端末、サーバ装置、通信回線装置等及びソフトウェア	

改定後（新）	現行（旧）
自体を保護するための措置を講じるよう努めなければならない。 **イ　中央電子計算組織管理者及び情報セキュリティ管理者は、利用するソフトウェアの特性を踏まえ、以下の全ての実施手順を整備しなければならない。** **(ｱ)　情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順** **(ｲ)　情報システムの基盤を管理又は制御するソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順** **(6)　情報システムの基盤を管理又は制御するソフトウェア運用時の対策** **ア　中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムの基盤を管理又は制御するソフトウェアを運用・保守する場合は、以下の全てのセキュリティ対策を実施するよう努めなければならない。** **(ｱ)　情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するための対策** **(ｲ)　脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策** **イ　中央電子計算組織管理者及び情報セキュリティ管理者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行わなければならない。**	
(7)　システム開発・保守に関連する資料等の整備・保管 ア　中央電子計算組織管理者及び情報セキュリティ**管理者**は、システム開発・保守に関連する資料及びシステム関連文書を**適正**に整備・保管しなければならない。	エ　システム開発・保守に関連する資料等の整備・保管 中央電子計算組織管理者及び情報セキュリティ**担当者**は、システム開発時等に作成された資料等の整備・保管について、次の事項を遵守しなければならない。 (ｱ)　システム開発・保守に関連する資料及びシステム関連文書を**適切**に整備・保管すること。

改定後（新）	現行（旧）
(ｱ)　中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について電子計算組織総括管理者に報告しなければならない。 **(ｲ)　中央電子計算組織管理者及び情報セキュリティ管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む情報システム関連文書を整備するよう努めなければならない。** **・情報システムを構成するサーバ装置及び端末関連情報** **・情報システムを構成する通信回線及び通信回線装置関連情報** **(ｳ)　中央電子計算組織管理者及び情報セキュリティ管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む実施手順を整備しなければならない。** **・情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順** **・情報セキュリティインシデントを認知した際の対処手順** **・情報システムが停止した際の復旧手順**	
イ　中央電子計算組織管理者及び情報セキュリティ**管理者**は、テスト結果を一定期間保管しなければならない。	(ｲ)　テスト結果を一定期間保管すること。
ウ　中央電子計算組織管理者及び情報セキュリティ**管理者**は、情報システムに係るソースコードを**適正**な方法で保管しなければならない。	(ｳ)　情報システムに係るソースコードを**適切**な方法で保管すること。
⑻　情報システムにおける入出力データの正確性の確保	オ　情報システムにおける入出力データの正確性の確保
ア　中央電子計算組織管理者及び情報セキュリティ**管理者**は、情報システムに入力されるデータについて、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組み込むように情報システム	中央電子計算組織管理者及び情報セキュリティ**担当者**は、情報システムにおける入出力データについて、次の事項を遵守しなければならない。 (ｱ)　情報システムに入力されるデータについて、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組み込むように情報システムを設計すること。

改定後（新）	現行（旧）
を設計しなければならない。 **イ　中央電子計算組織管理者及び情報セキュリティ管理者は、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。** **(ｱ)　利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直さなければならない。** **(ｲ)　運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じなければならない。** (ｳ)　ウェブアプリケーション・コンテンツにおいて、故意又は過失により情報が改ざんされる、又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。	(ｲ)　故意又は過失により情報が改ざんされる、又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計すること。
ウ　中央電子計算組織管理者及び情報セキュリティ**管理者**は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。	(ｳ)　情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計すること。
⑼　情報システムの変更管理 中央電子計算組織管理者及び情報セキュリティ**管理者**は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。	カ　情報システムの変更管理 中央電子計算組織管理者及び情報セキュリティ**担当者**は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。
⑽　開発・保守用のソフトウェアの更新等 中央電子計算組織管理者及び情報セキュリティ**管理者**は、開発・保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。	キ　開発・保守用のソフトウェアの更新等 中央電子計算組織管理者及び情報セキュリティ**担当者**は、開発・保守用のソフトウェア等の更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。
⑾　システム更新又は統合時の検証等 中央電子計算組織管理者及び情報セキュリティ**管理者**は、システム更	ク　システム更新又は統合時の検証等 中央電子計算組織管理者及び情報セキュリティ**担当者**は、システム

改定後（新）	現行（旧）
新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。 **⑿　情報システムについての対策の見直し** **中央電子計算組織管理者及び情報セキュリティ管理者は、対策の推進計画等に基づき情報システムの情報セキュリティ対策を適切に見直さなければならない。また、本市内で横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示に基づき、情報セキュリティ対策を適切に見直さなければならない。なお、措置の結果については、電子計算組織総括管理者に報告しなければならない。**	更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。
８．４　不正プログラム対策 ⑴　中央電子計算組織管理者の措置事項 中央電子計算組織管理者は、不正プログラム対策として、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ファイルは、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、不正プログラムのシステムへ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ファイルは、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　コンピュータ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　所掌するサーバ及びパソコン等の端末に、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。 オ　不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。	⑷　不正プログラム対策 ア　中央電子計算組織管理者の措置事項 中央電子計算組織管理者は、不正プログラム対策として、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ファイルは、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、不正プログラムのシステムへ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ファイルは、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)　コンピュータ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)　所掌するサーバ及びパソコン等の端末に、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。 (ｵ)　不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

改定後（新）	現行（旧）
カ　不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。	(カ)　不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。
キ　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。また、当該製品の利用を予定している期間中に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する予定がないことを確認しなければならない。	(キ)　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。また、当該製品の利用を予定している期間中に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する予定がないことを確認しなければならない。
⑵　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。	イ　情報セキュリティ担当者の措置事項 情報セキュリティ担当者は、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　所掌するサーバ及びパソコン等の端末に、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システムに常駐させなければならない。	(ア)　所掌するサーバ及びパソコン等の端末に、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システムに常駐させること。
イ　不正プログラム対策ソフトウェアのパターンファイルは、常に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のパターンファイルは、常に最新の状態に保つこと。
ウ　不正プログラム対策のソフトウェアは、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のソフトウェアは、常に最新の状態に保つこと。
エ　インターネットに接続していないシステムにおいて、電磁的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、市が管理している媒体以外を職員等に利用させてはならない。また、不正プログラムの感染、侵入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パターンファイルの更新を実施しなければならない。	(エ)　インターネットに接続していないシステムにおいて、電磁的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、市が管理している媒体以外を職員等に利用させないこと。また、不正プログラムの感染、侵入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パターンファイルの更新を実施すること。
オ　不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報セキュリティ管理者が許可した職員を除く職員等に当該権限を付与してはならない。	(オ)　不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報セキュリティ担当者が許可した職員を除く職員等に当該権限を付与してはならない。

改定後（新）	現行（旧）
⑶　職員等の遵守事項 職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。	ウ　職員等の遵守事項 職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。
ア　パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。	(ｱ)　パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更しないこと。
イ　外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。	(ｲ)　外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行うこと。
ウ　差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。	(ｳ)　差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除すること。
エ　端末に対して、不正プログラム対策ソフトウェアによる**フルチェック**を定期的に実施しなければならない。	(ｴ)　端末に対して、不正プログラム対策ソフトウェアによる**チェック**を定期的に実施すること。
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でチェックを行わなければならない。インターネット接続系で受信したインターネット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。	(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でチェックを行うこと。また、インターネットメール又はインターネット経由で入手したファイルを**総合行政ネットワーク（LGWAN）接続系**に取り込む場合は無害化を行うこと。
カ　中央電子計算組織管理者が提供するウイルス情報を、常に確認しなければならない。	(ｶ)　中央電子計算組織管理者が提供するウイルス情報を、常に確認すること。
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又は感染が疑われる場合は、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末においてLANケーブルの取り外しや、通信を行わない設定への変更などを実施しなければならない。	(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又は感染が疑われる場合は、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末においてLANケーブルの取り外しや通信を行わない設定への変更などを実施しなければならない。
	(ｸ)　不正プログラム対策ソフトウェアによるチェックの実行を途中で

改定後（新）	現行（旧）
	中断しないこと。
⑷　専門家の支援体制 中央電子計算組織管理者及び情報セキュリティ管理者は、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、外部の専門家の支援を受けられるようにしておかなければならない。	エ　専門家の支援体制 中央電子計算組織管理者及び情報セキュリティ担当者は、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、外部の専門家の支援を受けられるようにしておかなければならない。
８．５　不正アクセス対策	⑸　不正アクセス対策
⑴　中央電子計算組織管理者の措置事項 中央電子計算組織管理者は、不正アクセス対策として、以下の事項を措置しなければならない。	ア　中央電子計算組織管理者の措置事項 中央電子計算組織管理者は、不正アクセス対策として、以下の事項を措置しなければならない。
ア　使用されていないポートを閉鎖しなければならない。	(ｱ)　使用されていないポートを閉鎖しなければならない。
イ　不要なサービスについて､機能を削除又は停止しなければならない。	(ｲ)　不要なサービスについて､機能を削除又は停止しなければならない。
ウ　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に、データの書換えを検出し、**中央電子計算組織管理者及び**担当職員等が属する課の情報セキュリティ**管理者**へ通報するよう、設定しなければならない。	(ｳ)　不正アクセスによるウェブページの改ざんを確実に防止するために、担当職員等によるものであるか否かに関わりなくデータの書換えを検出した場合は、**電子計算組織総括管理者**及び担当職員等が属する課の情報セキュリティ**担当者**へ通報するよう、設定しなければならない。
エ　重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。	(ｴ)　重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。
オ　中央電子計算組織管理者は、**電子計算組織管理運営委員会**と連携し、監視、通知、外部連絡窓口及び**適正**な対応などを実施できる体制並びに連絡網を構築しなければならない。	(ｵ)　中央電子計算組織管理者は、**情報化推進委員会**と連携し、監視、通知、外部連絡窓口及び**適切**な対応などを実施できる体制並びに連絡網を構築しなければならない。
⑵　攻撃への対処 **電子計算組織総括管理者及び**中央電子計算組織管理者は、サーバ等に攻撃を**受けた場合又は攻撃を受けるリスクがある場合は**、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、**総務省、東京都等**と連絡を密にして情報の収集に努めなければならない。	イ　攻撃への対処 中央電子計算組織管理者は、サーバ等に攻撃を**受けることが明確になった場合**、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。

改定後（新）	現行（旧）
⑶　記録の保存 **電子計算組織総括管理者及び**中央電子計算組織管理者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、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。 ⑷　内部からの攻撃 **電子計算組織総括管理者及び**中央電子計算組織管理者は、職員等及び委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。 ⑸　職員等による不正アクセス 電子計算組織総括管理者及び中央電子計算組織管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課等の情報セキュリティ**管理者**に通知し、**適正**な処置を求めなければならない。 ⑹　サービス不能攻撃 **電子計算組織総括管理者及び**中央電子計算組織管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。 ⑺　標的型攻撃 **電子計算組織総括管理者及び**中央電子計算組織管理者は、標的型攻撃による内部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、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、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対策(内部対策及び出口対策）を講じなければならない。	ウ　記録の保存 中央電子計算組織管理者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、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。 エ　内部からの攻撃 中央電子計算組織管理者は、職員等及び委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。 オ　職員等による不正アクセス 電子計算組織総括管理者及び中央電子計算組織管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課等の情報セキュリティ**担当者**に通知し、**適切**な処置を求めなければならない。 カ　サービス不能攻撃 中央電子計算組織管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。 キ　標的型攻撃 中央電子計算組織管理者は、標的型攻撃による内部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、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、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対策（内部対策及び出口対策）を講じなければならない。

改定後（新）	現行（旧）
７．６　セキュリティ情報の収集 ⑴　セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等 **電子計算組織総括管理者及び**中央電子計算組織管理者は、**サーバ装置、端末及び通信回線装置等における**セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。 ⑵　不正プログラム等のセキュリティ情報の収集・周知 **電子計算組織総括管理者及び**中央電子計算組織管理者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。 ⑶　情報セキュリティに関する情報の収集及び共有 電子計算組織総括管理者及び中央電子計算組織管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、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。	⑹　セキュリティ情報の収集 ア　セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等 中央電子計算組織管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。 イ　不正プログラム等のセキュリティ情報の収集・周知 中央電子計算組織管理者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。 ウ　情報セキュリティに関する情報の収集及び共有 電子計算組織総括管理者及び中央電子計算組織管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、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。
９　運用 ９．１　情報システムの監視 **⑴　情報システムの運用・保守時の対策** **ア　中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用しなければならない。** **イ　中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視**	１１　運用

改定後（新）	現行（旧）
等の状況により見直しを適時検討し、必要な措置を講じなければならない。 **ウ　中央電子計算組織管理者及び情報セキュリティ管理者は、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をしなければならない。** **⑵　情報システムの監視機能** **ア　中央電子計算組織管理者は、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装しなければならない。** **イ　中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用しなければならない。** **ウ　中央電子計算組織管理者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直さなければならない。** **エ　中央電子計算組織管理者及び情報セキュリティ管理者は、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講じなければならない。**	
⑶　情報システムの監視 ア　中央電子計算組織管理者及び情報セキュリティ**管理者**は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。 イ　中央電子計算組織管理者及び情報セキュリティ**管理者**は、重要なログ等を取得するサーバの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。	⑴　情報システムの監視 中央電子計算組織管理者及び情報セキュリティ**担当者**は、情報システムの監視について、次の事項を措置しなければならない。 ア　セキュリティに関する事案を検知するため、情報システムを常時監視すること。 エ　内部のシステムについて、アクセスコントロール等を行い、異常な運用等の監視を行うこと。 イ　重要なログ等を取得するサーバの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ること。

改定後（新）	現行（旧）
ウ　中央電子計算組織管理者及び情報セキュリティ**管理者**は、外部と常時接続するシステムを常時監視しなければならない。	ウ　外部と常時接続するシステムを常時監視すること。
エ　中央電子計算組織管理者及び情報セキュリティ管理者は、暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入するよう努めなければならない。	
９．２　情報セキュリティポリシーの遵守状況の確認	⑵　情報セキュリティポリシーの遵守状況の確認
⑴　遵守状況の確認及び対処	ア　遵守状況の確認及び対処
ア　情報セキュリティ責任者及び情報セキュリティ**管理者**は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに CISO 及び電子計算組織総括管理者に報告しなければならない。	(ｱ)　総括情報セキュリティ担当者及び情報セキュリティ**担当者**は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに**最高情報セキュリティ責任者**及び電子計算組織総括管理者に報告しなければならない。
イ　CISO は、発生した問題について、**適正**かつ速やかに対処しなければならない。	(ｲ)　**最高情報セキュリティ責任者**は、速やかに発生した問題に**適切**に対処するため、**電子計算組織総括管理者に対策を講じるよう指示をしなければならない。**
ウ　中央電子計算組織管理者及び情報セキュリティ**管理者**は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には**適正**かつ速やかに対処しなければならない。	(ｳ)　中央電子計算組織管理者及び情報セキュリティ**担当者**は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には**適切**かつ速やかに対処しなければならない。
⑵　パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査	イ　パソコン、モバイル端末、電磁的記録媒体等の利用状況調査
ア　CISO **及び** CISO が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。	(ｱ)　**中央電子計算組織管理者及び中央電子計算組織管理者**が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン、モバイル端末、電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。
イ　法令等で定められた個人情報の保護に関する情報の閲覧に関しては、当該法令等で定められた手続に従わなければならない。	(ｲ)　法令等で定められた個人情報の保護に関する情報の閲覧に関しては、当該法令等で定められた手続に従わなければならない。

改定後（新）	現行（旧）
ウ　中央電子計算組織管理者及び中央電子計算組織管理者が指名した者は、知り得た情報を他に漏らしてはならない。	(ｳ)　中央電子計算組織管理者及び中央電子計算組織管理者が指名した者は、知り得た情報を他に漏らしてはならない。
⑶　職員等の報告義務	ウ　職員等の報告義務
ア　職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに中央電子計算組織管理者及び情報セキュリティ管理者に報告を行わなければならない。	(ｱ)　職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに中央電子計算組織管理者及び情報セキュリティ担当者に報告を行わなければならない。
イ　違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると中央電子計算組織管理者が判断した場合は、武蔵村山市業務継続計画（ＩＣＴ編）に従って**適正**に対処しなければならない。	(ｲ)　違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると中央電子計算組織管理者が判断した場合は、武蔵村山市業務継続計画（ＩＣＴ編）に従って**適切**に対処しなければならない。
９．３　侵害時の対応等	⑶　侵害時の対応等
⑴　武蔵村山市業務継続計画（ＩＣＴ編）の策定	ア　武蔵村山市業務継続計画（ＩＣＴ編）の策定
CISO**又は電子計算組織管理運営委員会**は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合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**適正**に実施するために、武蔵村山市業務継続計画（ＩＣＴ編）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。	**最高情報セキュリティ責任者又は情報化推進委員会**は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合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、武蔵村山市業務継続計画（ＩＣＴ編）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**適切**に対処しなければならない。
⑵　武蔵村山市業務継続計画（ＩＣＴ編）に盛り込むべき内容	イ　武蔵村山市業務継続計画（ＩＣＴ編）に盛り込むべき内容
武蔵村山市業務継続計画（ＩＣＴ編）には、以下の内容を定めなければならない。	武蔵村山市業務継続計画（ＩＣＴ編）には、以下の内容を定めなければならない。
ア　関係者の連絡先	(ｱ)　関係者の連絡先
イ　発生した事案に係る報告すべき事項	(ｲ)　発生した事案に係る報告すべき事項
ウ　発生した事案への対応措置	(ｳ)　発生した事案への対応措置
エ　再発防止措置の策定	(ｴ)　再発防止措置の策定

改定後（新）	現行（旧）
⑶　武蔵村山市業務継続計画（ＩＣＴ編）**との整合性確保** **電子計算組織管理運営委員会**は、自然災害、大規模・広範囲にわたる疾病等に備えて策定した武蔵村山市業務継続計画（ＩＣＴ編）と情報セキュリティポリシーの整合性を確保しなければならない。 ⑷　武蔵村山市業務継続計画（ＩＣＴ編）**の見直し** CISO **又は電子計算組織管理運営委員会**は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて武蔵村山市業務継続計画（ＩＣＴ編）の規定を見直さなければならない。	ウ　武蔵村山市業務継続計画（ＩＣＴ編）の**見直し** **最高情報セキュリティ責任者又は情報化推進委員会**は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて武蔵村山市業務継続計画（ＩＣＴ編）の規定を見直し、情報セキュリティポリシーと武蔵村山市業務継続計画（ＩＣＴ編）の整合性を確保しなければならない。
９．４　例外措置 ⑴　例外措置の許可 電子計算組織総括管理者及び情報セキュリティ**責任者**は、情報セキュリティ関係規定を遵守することが困難な状況で、行政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する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、CISO の許可を得て、例外措置を取ることができる。 ⑵　緊急時の例外措置 電子計算組織総括管理者及び情報セキュリティ**責任者**は、行政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、事後速やかに CISO に報告しなければならない。 ⑶　例外措置の申請書の管理 CISO は、例外措置の申請書及び審査結果を**適正**に保管し、定期的に申請状況を確認しなければならない。	⑷　例外措置 ア　例外措置の許可 中央電子計算組織管理者及び情報セキュリティ**担当者**は、情報セキュリティ関係規定を遵守することが困難な状況で、行政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、**最高情報セキュリティ責任者**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 中央電子計算組織管理者及び情報セキュリティ**担当者**は、行政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、事後速やかに**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。 ウ　例外措置の申請書の管理 **最高情報セキュリティ責任者**は、例外措置の申請書及び審査結果を**適切**に保管し、定期的に申請状況を確認しなければならない。
９．５　法令遵守 職員等は、職務の遂行において使用する情報資産を保護するために、	⑸　法令遵守 職員等**及び委託事業者**は、職務の遂行において使用する情報資産を保護

改定後（新）	現行（旧）
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。 ⑴　地方公務員法**（昭和２５年法律第２６１号）** ⑵　著作権法**（昭和４５年法律第４８号）** ⑶　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）** ⑷　個人情報の保護に関する法律**（平成１５年法律第５７号）** ⑸　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）** ⑹　サイバーセキュリティ基本法**（平成２６年法律第１０４号）** ⑺　武蔵村山市個人情報の保護に関する法律施行条例**（令和４年条例第３０号）**	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**（職員等のみ）** イ　著作権法 ウ　不正アクセス行為の禁止等に関する法律 エ　個人情報の保護に関する法律 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 カ　サイバーセキュリティ基本法 キ　武蔵村山市個人情報保護条例
９．６　懲戒処分等 ⑴　懲戒処分 情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。 ⑵　違反時の対応 職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。 ア　電子計算組織総括管理者又は中央電子計算組織管理者が違反を確認した場合は、中央電子計算組織管理者は当該職員等が所属する**部等**の**情報セキュリティ責任者及び**情報セキュリティ**管理者**に通知し、**適正**な措置を求めなければならない。 イ　職員等が違反を確認した場合は、違反を確認した者は速やかに**中央電子計算組織管理者**及び当該職員等が所属する課等の情報セキュリティ**管理者**に通知し、**適正**な措置を求めなければならない。	⑹　懲戒処分等 ア　懲戒処分 情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。 イ　違反時の対応 職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。 (ｱ)　電子計算組織総括管理者又は中央電子計算組織管理者が違反を確認した場合は、中央電子計算組織管理者は当該職員等が所属する**課等**の情報セキュリティ**担当者**に通知し、**適切**な措置を求めなければならない。 (ｲ)　職員等が違反を確認した場合は、違反を確認した者は速やかに**電子計算組織総括管理者**及び当該職員等が所属する課等の情報セキュリティ**担当者**に通知し、**適切**な措置を求めなければならない。

改定後（新）	現行（旧）
ウ　情報セキュリティ**責任者及び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、**電子計算組織総括管理者**は、当該職員等のネットワーク又は情報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。**電子計算組織総括管理者**は、その後速やかに、職員等の権利を停止あるいは剥奪した旨を CISO と当該職員等が所属する部の**情報セキュリティ責任者及び情報セキュリティ管理者**に通知しなければならない。	(ｳ)　情報セキュリティ**担当者**の指導によっても改善されない場合、**中央電子計算組織管理者**は、当該職員等のネットワーク又は情報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、**中央電子計算組織管理者**は、職員等の権利を停止あるいは剥奪した旨を**最高情報セキュリティ責任者、電子計算組織総括管理者及び**当該職員等が所属する部の**総括情報セキュリティ担当者**に通知しなければならない。
１０　**業務委託と**外部サービス**（クラウドサービス）**の利用	１２　外部サービスの利用
１０．１　業務委託	
⑴　業務委託に係る運用規定の整備 **電子計算組織総括管理者は、業務委託に係る以下の内容を全て含む運用規定を整備しなければならない。** **ア　委託事業者への提供を認める情報及び委託する業務の範囲を判断する基準（以下「委託判断基準」という。）** **イ　委託事業者の選定基準**	**⑴　委託事業者の選定基準** **中央電子計算組織管理者及び情報セキュリティ担当者は、委託事業者の選定について、次の事項を遵守しなければならない。** **ア　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すること。** **イ　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、委託事業者を選定すること。**
⑵　業務委託実施前の対策 **ア　中央電子計算組織管理者及び情報セキュリティ管理者は、業務委託の実施までに、以下を全て含む事項を実施しなければならない。** **(ｱ)　委託する業務内容の特定**	

改定後（新）	現行（旧）
(ｲ)　委託事業者の選定条件を含む仕様の策定	
(ｳ)　仕様に基づく委託事業者の選定	
(ｴ)　情報セキュリティ要件を明記した契約の締結（契約項目） **重要な情報資産を取扱う業務を**委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ等に係る要件を明記した契約を締結しなければならない。	**⑵　契約項目** **情報システムの運用、保守等を業務**委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。
・情報セキュリティポリシー**及び情報セキュリティ実施手順の遵守**	ア　情報セキュリティポリシーの遵守
・個人情報漏えい防止のための技術的安全管理措置に関する取り決め	
・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定	イ　委託事業者の責任者、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	ウ　提供されるサービスレベルの保証
・委託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**の明確化など、情報のライフサイクル全般での管理方法**	エ　委託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
・委託事業者の従業員に対する**教育**の実施	オ　委託事業者の従業員に対する**研修**の実施
・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	カ　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
・業務上知り得た情報の守秘義務	キ　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	ク　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	ケ　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	コ　委託業務の定期報告及び緊急時報告義務
・市による監査・検査	サ　市による監査、検査
・市による情報セキュリティインシデント発生時の公表	シ　市による情報セキュリティインシデント発生時の公表
・情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）	ス　情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）
(ｵ)　委託事業者に重要情報を提供する場合は、秘密保持契約（ＮＤＡ）の締結	

改定後（新）	現行（旧）
イ　中央電子計算組織管理者及び情報セキュリティ管理者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託事業者に求めなければならない。 (ｱ)　仕様に準拠した提案 (ｲ)　契約の締結 (ｳ)　委託事業者において重要情報を取り扱う場合は、秘密保持契約（ＮＤＡ）の締結 ⑶　業務委託実施期間中の対策 ア　中央電子計算組織管理者及び情報セキュリティ管理者は、業務委託の実施期間において、以下を全て含む対策を実施しなければならない。 (ｱ)　委託判断基準に従った重要情報の提供 (ｲ)　契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施 (ｳ)　電子計算組織総括管理者へ措置内容の報告（重要度に応じてCISOに報告） (ｴ)　委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等により受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求 イ　中央電子計算組織管理者及び情報セキュリティ管理者は、業務委託の実施期間において、以下を全て含む対策の実施を委託事業者に求めなければならない。 (ｱ)　情報の適正な取扱のための情報セキュリティ対策 (ｲ)　契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告 (ｳ)　委託した業務において、情報セキュリティインシデントの発生	

改定後（新）	現行（旧）
又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処 ⑷　業務委託終了時の対策 ア　中央電子計算組織管理者及び情報セキュリティ管理者は、業務委託の終了に際して、以下を全て含む対策を実施しなければならない。 (ｱ)　業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収 (ｲ)　委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認 イ　中央電子計算組織管理者及び情報セキュリティ管理者は、業務委託の終了に際して、以下を全て含む対策の実施を委託事業者に求めなければならない。 (ｱ)　業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検 (ｲ)　提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消 １０．２　情報システムに関する業務委託 ⑴　情報システムに関する業務委託における共通的対策 中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムに関する業務委託の実施までに、情報システムに本市の意図せざる変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様を策定しなければならない。 ⑵　情報システムの構築を業務委託する場合の対策 中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託事業者に求めなければならない。	

改定後（新）	現行（旧）
ア　情報システムのセキュリティ要件の適切な実装 イ　情報セキュリティの観点に基づく試験の実施 ウ　情報システムの開発環境及び開発工程における情報セキュリティ対策 ⑶　情報システムの運用・保守を業務委託する場合の対策 ア　中央電子計算組織管理者及び情報セキュリティ管理者は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。 イ　中央電子計算組織管理者及び情報セキュリティ管理者は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託事業者に速やかな報告を求めなければならない。 ⑷　本市向けに情報システムの一部の機能を提供するサービスを利用する場合の対策 ア　中央電子計算組織管理者及び情報セキュリティ管理者は、外部の一般の者が本市向けに重要情報を取り扱う情報システムの一部の機能を利用するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託事業者の選定条件に業務委託サービスに特有の選定条件を加えなければならない。 イ　中央電子計算組織管理者又は情報セキュリティ管理者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定しなければならない。 ウ　中央電子計算組織管理者又は情報セキュリティ管理者は、委託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。 エ　中央電子計算組織管理者又は情報セキュリティ管理者は、業務委託	

改定後（新）	現行（旧）
サービスを利用する場合には、電子計算組織総括管理者又は情報セキュリティ責任者へ当該サービスの利用申請を行わなければならない。 **オ　電子計算組織総括管理者又は情報セキュリティ責任者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定しなければならない。** **カ　電子計算組織総括管理者又は情報セキュリティ責任者は、業務委託サービスの利用申請を承認した場合は、承認済業務委託サービスとして記録し、業務委託サービス管理者を指名しなければならない。**	
１０．３　外部サービス**（クラウドサービス）**の利用（**自治体機密性２以上の情報**を取り扱う場合） **⑴　クラウドサービスの選定に係る運用規定の整備** **電子計算組織総括管理者は、自治体機密性２以上の情報を取り扱う場合、以下を含む外部サービス（クラウドサービス、以下「クラウドサービス」という。）の選定に関する規定を整備しなくてはならない。** ア　**クラウド**サービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下**９．３節において「クラウドサービス利用判断基準」**という。） イ　**クラウド**サービス提供者の選定基準 ウ　**クラウド**サービスの利用申請の許可権限者と利用手続 エ　**クラウド**サービス管理者の指名とクラウドサービスの利用状況の管理 **⑵　クラウドサービスの利用に係る運用規定の整備** **電子計算組織総括管理者は、自治体機密性２以上の情報を取り扱う場合、以下を含むクラウドサービス（自治体機密性２以上の情報を取り扱う場合）の利用に関する規定を整備しなければならない。** **ア　電子計算組織総括管理者は、クラウドサービスの特性や責任分界点**	⑶　外部サービスの利用（**重要な情報資産（分類Ⅱ以上）**を取り扱う場合） ア　**外部**サービスの**利用**に係る規定の整備 **中央電子計算組織管理者及び情報セキュリティ担当者**は、以下を含む**外部**サービス（**重要な情報資産（分類Ⅱ以上）**を取り扱う場合）の利用に関する規定を整備しなければならない。 (ｱ)　**外部**サービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下**の節において「外部サービス利用判断基準」**という。） (ｲ)　**外部**サービス提供者の選定基準 (ｳ)　**外部**サービスの利用申請の許可権限者と利用手続 (ｴ)　**外部**サービス管理者の指名と外部サービスの利用状況の管理

改定後（新）	現行（旧）
に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を運用規定として整備しなければならない。 **イ　電子計算組織総括管理者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用規定として整備しなければならない。** **ウ　電子計算組織総括管理者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を全て含むクラウドサービスの利用を終了する際のセキュリティ対策の基本方針を運用規定として整備しなければならない。** **(ｱ)　クラウドサービス利用終了時における対策** **(ｲ)　クラウドサービスで取り扱った情報の廃棄** **(ｳ)　クラウドサービス利用のために作成したアカウントの廃棄**	
⑶　**クラウド**サービスの選定 ア　中央電子計算組織管理者は、取り扱う情報の格付及び取扱制限を踏まえ、**クラウド**サービス利用判断基準に従って、業務に係る影響度等を検討した上で**クラウド**サービスの利用を検討しなければならない。 イ　中央電子計算組織管理者は、**クラウド**サービスで取り扱う情報の格付及び取扱制限を踏まえ、**クラウド**サービス提供者の選定基準に従って**クラウド**サービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策を**クラウド**サービス提供者の選定条件に含めなければならない。 (ｱ)　**クラウド**サービスの利用を通じて本市が取り扱う情報の**クラウド**サービス提供者における目的外利用の禁止 (ｲ)　**クラウド**サービス提供者における情報セキュリティ対策の実施内容及び管理体制	イ　**外部**サービスの選定 (ｱ)　中央電子計算組織管理者は、取り扱う情報の格付及び取扱制限を踏まえ、**外部**サービス利用判断基準に従って**外部**サービスの利用を検討すること。 (ｲ)　中央電子計算組織管理者は、**外部**サービスで取り扱う情報の格付及び取扱制限を踏まえ、**外部**サービス提供者の選定基準に従って外部サービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策を**外部**サービス提供者の選定条件に含めること。 a　**外部**サービスの利用を通じて本市が取り扱う情報の外部サービス提供者における目的外利用の禁止 b　**外部**サービス提供者における情報セキュリティ対策の実施内容及び管理体制

改定後（新）	現行（旧）
(ｳ)　**クラウド**サービスの提供に当たり、**クラウド**サービス提供者若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制	c　**外部**サービスの提供に当たり、**外部**サービス提供者若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制
(ｴ)　**クラウド**サービス提供者の資本関係・役員等の情報、**クラウド**サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定	d　**外部**サービス提供者の資本関係・役員等の情報、**外部**サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定
(ｵ)　情報セキュリティインシデントへの対処方法	e　情報セキュリティインシデントへの対処方法
(ｶ)　情報セキュリティ対策その他の契約の履行状況の確認方法	f　情報セキュリティ対策その他の契約の履行状況の確認方法
(ｷ)　情報セキュリティ対策の履行が不十分な場合の対処方法	g　情報セキュリティ対策の履行が不十分な場合の対処方法
ウ　中央電子計算組織管理者は、**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、**クラウド**サービス提供者の選定条件に含めなければならない。	(ｳ)　中央電子計算組織管理者は、**外部**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、**外部**サービス提供者の選定条件に含めること。
エ　中央電子計算組織管理者は、**クラウド**サービスの利用を通じて本市が取り扱う情報の格付等を勘案し、必要に応じて以下の内容を**クラウド**サービス提供者の選定条件に含めなければならない。	(ｴ)　中央電子計算組織管理者は、**外部**サービスの利用を通じて本市が取り扱う情報の格付等を勘案し、必要に応じて以下の内容を**外部**サービス提供者の選定条件に含めること。
(ｱ)　情報セキュリティ監査の受入れ	a　情報セキュリティ監査の受入れ
(ｲ)　サービスレベルの保証	b　サービスレベルの保証
オ　中央電子計算組織管理者は、**クラウド**サービスの利用を通じて本市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して**クラウド**サービス提供者を選定し、必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めなければならない。	(ｵ)　中央電子計算組織管理者は、**外部**サービスの利用を通じて本市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して**外部**サービス提供者を選定し、必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めること。
カ　中央電子計算組織管理者は、**クラウド**サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、選定条件で求める内容を**クラウド**サービス提供者に担保させるとともに、再委託先の情報	(ｶ)　中央電子計算組織管理者は、**外部**サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、**外部サービス提供者の**選定条件で求める内容を**外部**サービス提供者に担保させるととも

改定後（新）	現行（旧）
セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し、本市の承認を受けるよう、**クラウド**サービス提供者の選定条件に含めなければならない。また、**クラウド**サービス利用判断基準及び**クラウド**サービス提供者の選定基準に従って再委託の承認の可否を判断しなければならない。	に、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し、本市の承認を受けるよう、**外部**サービス提供者の選定条件に含めること。また、**外部**サービス利用判断基準及び**外部**サービス提供者の選定基準に従って再委託の承認の可否を判断すること。
キ　中央電子計算組織管理者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、**クラウド**サービスを選定しなければならない。また、**クラウド**サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めなければならない。	(ｷ)　中央電子計算組織管理者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、**外部**サービスを選定すること。また、**外部**サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めること。
ク　中央電子計算組織管理者は、**クラウド**サービスの特性を考慮した上で、**クラウド**サービスが提供する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、情報セキュリティに関する役割及び責任の範囲を踏まえて、**以下を全て含む**セキュリティ要件を定めなければならない。 **(ｱ)　クラウドサービスに求める情報セキュリティ対策** **(ｲ)　クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法** **(ｳ)　クラウドサービスに求めるサービスレベル**	(ｸ)　中央電子計算組織管理者は、**外部**サービスの特性を考慮した上で、**外部**サービスが提供する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、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めること。
ケ　電子計算組織総括管理者は、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**サービス提供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。	(ｹ)　電子計算組織統括管理者は、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、**外部**サービス提供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すること。
⑷　**クラウド**サービスの利用に係る調達・契約	ウ　**外部**サービスの利用に係る調達・契約
ア　中央電子計算組織管理者は、**クラウド**サービスを調達する場合は、**クラウド**サービス提供者の選定基準及び選定条件並びに**クラウド**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	(ｱ)　中央電子計算組織管理者は、**外部**サービスを調達する場合は、**外部**サービス提供者の選定基準及び選定条件並びに**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ること。

改定後（新）	現行（旧）
ならない。 イ　中央電子計算組織管理者は、**クラウド**サービスを調達する場合は、**クラウド**サービス提供者及び**クラウド**サービスが調達仕様を満たすことを契約までに確認し、**利用承認を得なければならない。また、**調達仕様の内容を契約に含めなければならない。	(ｲ)　中央電子計算組織管理者は、**外部**サービスを調達する場合は、**外部**サービス提供者及び**外部**サービスが調達仕様を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ること。
⑸　**クラウド**サービスの利用承認 ア　中央電子計算組織管理者**及び情報セキュリティ管理者**は、**クラウド**サービスを利用する場合には、**電子計算組織総括管理者**へ**クラウド**サービスの利用申請を行わなければならない。	エ　**外部**サービスの利用承認 (ｱ)　中央電子計算組織管理者は、**外部**サービスを利用する場合には、**利用申請の許可権限者**へ**外部**サービスの利用申請を行うこと。
イ　**電子計算組織総括管理者**は、職員等による**クラウド**サービスの利用申請を審査し、利用の可否を決定しなければならない。	(ｲ)　**利用申請の許可権限者**は、職員等による**外部**サービスの利用申請を審査し、利用の可否を決定すること。
ウ　**電子計算組織総括管理者**は、**クラウド**サービスの利用申請を承認した場合は、承認済み**クラウド**サービスとして記録し、**クラウド**サービス管理者を指名しなければならない。	(ｳ)　**利用申請の許可権限者**は、**外部**サービスの利用申請を承認した場合は、承認済み**外部**サービスとして記録し、**外部**サービス管理者を指名すること。
⑹　**クラウド**サービスを利用した情報システムの導入・構築時の対策 ア　電子計算組織総括管理者は、**クラウド**サービスの特性や責任分界点に係る考え方等を踏まえ、以下を含む**クラウド**サービスを利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。 (ｱ)　不正なアクセスを防止するためのアクセス制御 (ｲ)　取り扱う情報の機密性保護のための暗号化 (ｳ)　開発時におけるセキュリティ対策 (ｴ)　設計・設定時の誤りの防止	オ　**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 (ｱ)　電子計算組織統括管理者は、**外部**サービスの特性や責任分界点に係る考え方等を踏まえ、以下を含む**外部**サービスを利用して情報システムを構築する際のセキュリティ対策を規定すること。 a　不正なアクセスを防止するためのアクセス制御 b　取り扱う情報の機密性保護のための暗号化 c　開発時におけるセキュリティ対策 d　設計・設定時の誤りの防止
イ　クラウドサービス管理者は、情報システムにおいてクラウドサービスを利用する際には、情報システム台帳及び関連文書に記録又は記載しなければならない。なお、情報システム台帳に記録又は記載した場合は、電子計算組織総括管理者へ報告しなければならない。	

改定後（新）	現行（旧）
ウ　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始までに以下の全ての実施手順を整備しなければならない。 **(ｱ)　クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順** **(ｲ)　クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順** **(ｳ)　利用するクラウドサービスが停止又は利用できなくなった際の復旧手順** エ　**クラウド**サービス管理者は、**前項**において定める規定に対し、構築時に実施状況を確認・記録しなければならない。 (7)　**クラウド**サービスを利用した情報システムの運用・保守時の対策 ア　電子計算組織総括管理者は、**クラウド**サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む**クラウド**サービスを利用して情報システムを運用する際のセキュリティ対策を規定しなければならない。 (ｱ)　**クラウド**サービス利用方針の規定 (ｲ)　**クラウド**サービス利用に必要な教育 (ｳ)　取り扱う資産の管理 (ｴ)　不正アクセスを防止するためのアクセス制御 (ｵ)　取り扱う情報の機密性保護のための暗号化 (ｶ)　**クラウド**サービス内の通信の制御 (ｷ)　設計・設定時の誤りの防止 (ｸ)　**クラウド**サービスを利用した情報システムの事業継続 **イ　クラウドサービス管理者は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合、情報システム台帳及び関連文書を更新又は修**	(ｲ)　**外部**サービス管理者は、**(7)**において定める規定に対し、構築時に実施状況を確認・記録すること。 カ　**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 (ｱ)　電子計算組織統括管理者は、**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、以下を含む**外部**サービスを利用して情報システムを運用する際のセキュリティ対策を規定すること。 a　**外部**サービス利用方針の規定 b　**外部**サービス利用に必要な教育 c　取り扱う資産の管理 d　不正アクセスを防止するためのアクセス制御 e　取り扱う情報の機密性保護のための暗号化 f　**外部**サービス内の通信の制御 g　設計・設定時の誤りの防止 h　**外部**サービスを利用した情報システムの事業継続

改定後（新）	現行（旧）
正しなければならない。なお、情報システム台帳を更新又は修正した場合は、電子計算組織総括管理者へ報告しなければならない。 **ウ　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。** エ　中央電子計算組織管理者は、**クラウド**サービスの特性や責任分界点に係る考え方を踏まえ、**クラウド**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。 オ　**クラウド**サービス管理者は、**前各項**において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録しなければならない。 ⑻　**クラウド**サービスを利用した情報システムの更改・廃棄時の対策 ア　電子計算組織総括管理者は、**クラウド**サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む**クラウド**サービスの利用を終了する際のセキュリティ対策を規定しなければならない。 (ｱ)　**クラウド**サービスの利用終了時における対策 (ｲ)　**クラウド**サービスで取り扱った情報の廃棄 (ｳ)　**クラウド**サービスの利用のために作成したアカウントの廃棄 イ　**クラウド**サービス管理者は、**前項**において定める規定に対し、**クラウド**サービスの利用終了時に実施状況を確認・記録しなければならない。	(ｲ)　中央電子計算組織管理者は、**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すること。 (ｳ)　**外部**サービス管理者は、**(ｱ)及び(ｲ)**において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録すること。 キ　**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 (ｱ)　電子計算組織統括管理者は、**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、以下を含む**外部**サービスの利用を終了する際のセキュリティ対策を規定すること。 a　**外部**サービスの利用終了時における対策 b　**外部**サービスで取り扱った情報の廃棄 c　**外部**サービスの利用のために作成したアカウントの廃棄 (ｲ)　**外部**サービス管理者は、**(ｱ)**において定める規定に対し、**外部**サービスの利用終了時に実施状況を確認・記録すること。
１０．４　外部サービス**（クラウドサービス）**の利用（**自治体機密性２以上の情報**を取り扱わない場合） ⑴　**クラウド**サービスの利用に係る規定の整備 電子計算組織総括管理者は、**自治体機密性２以上の情報**を取り扱わない場合、以下を含む**クラウド**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。	⑷　外部サービスの利用（**重要な情報資産（分類Ⅱ以上）**を取り扱わない場合） ア　**外部**サービスの利用に係る規定の整備 電子計算組織統括管理者は、以下を含む**外部**サービス（**重要な情報資産（分類Ⅱ以上）**を取り扱わない場合）の利用に関する規定を整備すること。

改定後（新）	現行（旧）
ア　**クラウド**サービスを利用可能な業務の範囲	(ｱ)　**外部**サービスを利用可能な業務の範囲
イ　**クラウド**サービスの利用申請の許可権限者と利用手続	(ｲ)　**外部**サービスの利用申請の許可権限者と利用手続
ウ　**クラウド**サービス管理者の指名と**クラウド**サービスの利用状況の管理	(ｳ)　**外部**サービス管理者の指名と**外部**サービスの利用状況の管理
エ　**クラウド**サービスの利用の運用手順	(ｴ)　**外部**サービスの利用の運用手順
⑵　**クラウド**サービスの利用における対策の実施	イ　**外部**サービスの利用における対策の実施
ア　職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で、**自治体機密性２以上の情報**を取り扱わない場合の**クラウド**サービスの利用を申請しなければならない。また、承認時に指名された**クラウド**サービス管理者は、当該**クラウド**サービスの利用において適切な措置を講じなければならない。	(ｱ)　職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で**重要な情報資産（分類Ⅱ以上）**を取り扱わない場合の**外部**サービスの利用を申請すること。また、承認時に指名された**外部**サービス管理者は、当該**外部**サービスの利用において適切な措置を講ずること。
イ　中央電子計算組織管理者は、職員等による**クラウド**サービスの利用申請を審査し、利用の可否を決定しなければならない。また、承認した**クラウド**サービスを記録しなければならない。	(ｲ)　情報セキュリティ責任者は、職員等による**外部**サービスの利用申請を審査し、利用の可否を決定すること。また、承認した**外部**サービスを記録すること。
※７　７．１(22)に記載	**⑸　ソーシャルメディアサービスの利用**
	ア　中央電子計算組織管理者は、本市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めた運用手順を定めなければならない。
	(ｱ)　本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を行うこと。
	(ｲ)　パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（IC カード等）等を適切に管理するなどの方法で、不正アクセス対策を行うこと。

改定後（新）	現行（旧）
	イ　重要な情報資産（分類Ⅱ以上）はソーシャルメディアサービスで発信してはならない。 **ウ　利用するソーシャルメディアサービスごとの責任者を定めなければならない。** **エ　アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。**
１１　評価・見直し １１．１　監査	１３　評価・見直し ⑴　監査 **ア　定義** **監査は、対象となる被監査部門とは別の組織体系に所属する者が、独立の立場から対象組織の管理策の実装と運用状況を評価し、情報セキュリティを所管する部署に評価結果と改善について意見具申するものである。一方、点検は、情報セキュリティ担当者が自分の組織の管理策の実装と運用状況を評価し、所管するネットワーク及び情報セキュリティの取扱状況を見直すとともに、情報セキュリティを所管する部署に結果を報告することで、取扱状況を確認するための方法である。** **イ　実施方針** **監査の実施に当たっては、情報システムの内容（特定個人情報を含む。）について監査するものとする。** **監査は、保護すべき情報資産を脅威から守るために、情報セキュリティ管理体制のもとで、情報システムの管理、媒体等機器の管理、ユーザーの管理、個人情報の取扱い等の事項について実施できているかという視点で実施する。** **また、社会保障・税番号制度（マイナンバー制度）が開始されたことから、特定個人情報の適正な管理及び運用が行われているかという**

改定後（新）	現行（旧）
	点も併せて監査を行う。
⑴　実施方法 CISOは、情報セキュリティ監査総括責任者として電子計算組織総括管理者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、**毎年度及び必要に応じて**監査を行わせなければならない。	ウ　実施方法 **最高情報セキュリティ責任者**は、情報セキュリティ監査総括責任者として電子計算組織総括管理者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、**定期に又は随時に**監査を行わせなければならない。
⑵　監査を行う者**の要件** ア　情報セキュリティ監査総括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。なお、情報セキュリティ監査総括責任者は、必要に応じ外部の第三者機関に監査の実施を依頼することができるものとする。	エ　監査を行う者 情報セキュリティ監査総括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。なお、情報セキュリティ監査総括責任者は、必要に応じ外部の第三者機関に監査の実施を依頼することができるものとする。
イ　監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。	
⑶　監査実施計画の**立案**及び実施への協力 ア　情報セキュリティ監査総括責任者は、監査を行うに当たって、監査実施計画を**立案**し、**電子計算組織管理運営委員会**の承認を得なければならない。 イ　被監査部門は、監査の実施に協力しなければならない。	カ　監査実施計画の**策定**及び実施への協力 (ｱ)　情報セキュリティ監査総括責任者**から監査の実施を依頼された者は、**監査を行うに当たって、監査実施計画を**策定**し、**必要に応じて情報化推進委員会**の承認を得なければならない。 (ｲ)　被監査部門は、監査の実施に協力しなければならない。
⑷　監査の実施スケジュール おおむね以下のスケジュールにより監査実施計画を定め、監査を実施する。	オ　監査の実施スケジュール おおむね以下のスケジュールにより監査実施計画を定め、監査を実施する。

主な監査業務	実施時期	備考
監査実施計画策定	４月～７月	
監査準備	４月～７月	監査項目等の整理
監査通知の送付	７月～８月	被監査部門との日程調整、各対象課に通知を行う。
予備調査	７月～８月	アンケート調査等

主な監査業務	実施時期	備考
監査実施計画策定	４月～７月	
監査準備	４月～７月	監査項目等の整理
監査通知の送付	７月～８月	被監査部門との日程調整、各対象課に通知を行う。
予備調査	７月～８月	アンケート調査等

改定後（新）	現行（旧）
<table><tr><td>実査</td><td>９月～12月</td><td>被監査部門の日程等を考慮して、本期間内において監査を実施する等</td></tr><tr><td>監査報告書提出</td><td>２月～３月</td><td>最高情報セキュリティ責任者及び必要に応じ**電子計算組織管理運営委員会**に報告</td></tr></table>	<table><tr><td>実査</td><td>９月～12月</td><td>被監査部門の日程等を考慮して、本期間内において監査を実施する等</td></tr><tr><td>監査報告書提出</td><td>２月～３月</td><td>最高情報セキュリティ責任者及び必要に応じ**情報化推進委員会**に報告</td></tr></table>
⑸　委託事業者に対する監査 事業者に業務委託を行っている場合、情報セキュリティ監査総括責任者は委託事業者（再委託事業者を含む。）に対して、情報セキュリティポリシーの遵守について監査を**定期的に又は**必要に応じて行わなければならない。	キ　委託事業者に対する監査 事業者に業務委託を行っている場合、情報セキュリティ監査総括責任者は委託事業者（再委託事業者を含む。）に対して、情報セキュリティポリシーの遵守について監査を必要に応じて行わなければならない。
⑹　報告 情報セキュリティ監査総括責任者は、監査結果を取りまとめ、CISOに報告し、又は必要に応じて**電子計算組織管理運営委員会**に報告する。	ク　報告**等** **⑺　監査を行った者は、被監査部門の情報セキュリティ担当者に監査の実施を通して収集した監査証拠を返却する。** **⑴　監査を行った者は、情報セキュリティ監査総括責任者及び被監査部門の情報セキュリティ担当者に監査結果を報告する。** (ｳ)　情報セキュリティ監査総括責任者は、監査結果を取りまとめ、**最高情報セキュリティ責任者**に報告し、又は必要に応じて**情報化推進委員会**に報告する。
⑺　保管 情報セキュリティ監査総括責任者は、**監査の実施を通して収集した監査証拠、**監査報告書の作成のための監査調書を、紛失等が発生しないように**適正**に保管しなければならない。	ケ　保管 **⑺　被監査部門の情報セキュリティ担当者は、監査の実施のために提出した監査証拠を紛失等しないように適切に保管しなければならない。** (ｲ)　情報セキュリティ監査総括責任者は、監査報告書の作成のための監査調書を紛失等しないように**適切**に保管しなければならない。

改定後（新）	現行（旧）
⑻　監査結果への対応 ア　CISOは、監査結果を踏まえ、指摘事項を所管する情報セキュリティ**責任者**に対し、当該事項への対処**（改善計画の策定等）**を指示しなければならない。**また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。** **イ　CISOは、**指摘事項を所管していない情報セキュリティ**責任者**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、当該課題及び問題点の有無を確認させなければならない。また、庁内で横断的に改善が必要な事項については、**電子計算組織総括管理者**に対し、当該事項への対処**（改善計画の策定等）**を指示しなければならない。**なお、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。**	コ　監査結果への対応 **情報セキュリティ監査総括責任者**は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ**担当者**に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ**担当者**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、当該課題及び問題点の有無を確認させなければならない。なお、庁内で横断的に改善が必要な事項については、**中央電子計算組織管理者**に対し、当該事項の対処を指示しなければならない。
⑼　情報セキュリティポリシー及び関係規程等の見直し等への活用 **電子計算組織管理運営委員会**は、監査結果を情報セキュリティポリシー及び関係規程等の見直し、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。	サ　情報セキュリティポリシー及び関係規程等の見直し等への活用 **情報化推進委員会**は、監査結果を情報セキュリティポリシー及び関係規程等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。
１１．２　**自己**点検 ⑴　実施方法 ア　中央電子計算組織管理者及び情報セキュリティ**管理者**は、所管するネットワーク及び情報システムの取扱状況について、**毎年度及び必要に応じて自己**点検を実施しなければならない。 イ　中央電子計算組織管理者は、情報セキュリティ**管理者**と連携して、所管する部局における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、**毎年度及び必要に応じて自己**点検を行わなければならない。	⑵　点検 ア　実施方法 (ｱ)　中央電子計算組織管理者及び情報セキュリティ**担当者**は、所管するネットワーク及び情報システムの取扱状況について、**定期に又は随時に**点検を実施しなければならない。 (ｲ)　中央電子計算組織管理者は、情報セキュリティ**担当者**と連携して、所管する部局における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、**定期に又は随時に**点検を行わなければならない。

改定後（新）	現行（旧）
⑵　報告 中央電子計算組織管理者及び情報セキュリティ**管理者**は、**自己**点検結果と**自己**点検結果に基づく改善策を取りまとめ、**電子計算組織管理運営委員会**に報告しなければならない。	イ　報告**等** 中央電子計算組織管理者及び情報セキュリティ**担当者**は、点検結果と点検結果に基づく改善策を取りまとめ、**必要があると認めるときは、情報セキュリティ監査総括責任者、総括情報セキュリティ担当者及び情報化推進委員会**に報告しなければならない。
⑶　**自己**点検結果の活用 ア　**職員等**は、**自己**点検の結果に基づき、**自己の権限の範囲内で**改善を図らなければならない。 イ　**電子計算組織管理運営委員会**は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、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。	ウ　点検結果の活用 (ｱ)　**中央電子計算組織管理者及び情報セキュリティ担当者**は、点検の結果に基づき改善を図らなければならない。 (ｲ)　**情報化推進委員会**は、この点検結果を情報セキュリティポリシー及び関係規程等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。 **(ｳ)　中央電子計算組織管理者及び情報セキュリティ担当者は、必要に応じ情報資産に対する脅威及び情報の重要性の分類によって、情報セキュリティに対するリスクを評価しなければならない。** **(ｴ)　情報資産のリスク評価により、保有する情報資産に対して、現状の情報セキュリティ対策と比較を行い、情報セキュリティ対策が十分であるかどうかを点検しなければならない。** **(ｵ)　情報セキュリティ対策が不足している場合は、適切な情報セキュリティ対策を実施しなければならない。その場合は、情報の機密性、完全性及び可用性を考慮しなければならない。**
１１．３　情報セキュリティポリシー及び関係規程等の見直し **電子計算組織管理運営委員会**は、情報セキュリティ監査及び**自己**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、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に**リスク**評価を行い、必要があると認めた場合、改善を行うものとする。**なお、横断的に改善が必要となる情報セキュリティ対策の運用見直し**	⑶　情報セキュリティポリシー及び関係規程等の見直し **情報化推進委員会**は、情報セキュリティ監査及び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、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。

改定後（新）	現行（旧）
<u>について、内部の職制及び職務に応じた措置の実施又は指示をし、措置の結果について CISO に報告しなければならない。</u>	

資料２

令和７年度　区域外就学の状況について

令和８年３月３１日現在

○住所が他市区町村にあって本市の学校へ通学している児童及び生徒

（単位：人）

区分／項目	１　学　期 4/1～8/31			２　学　期 9/1～12/31			３　学　期 1/1～3/31			合　　計		
	小学校	中学校	計	小学校	中学校	計	小学校	中学校	計	小学校	中学校	計
転入先付け	2		2				2		2	4		4
学期途中最終学年	1		1							1		1
両親共働き												
その他	2		2	5	1	6	18	7	25	25	8	33
計	5	0	5	5	1	6	20	7	27	30	8	38

○住所が本市にあって他市区町村の公立学校へ通学している児童及び生徒

（単位：人）

区分／項目	１　学　期 4/1～8/31			２　学　期 9/1～12/31			３　学　期 1/1～3/31			合　　計		
	小学校	中学校	計	小学校	中学校	計	小学校	中学校	計	小学校	中学校	計
転出先付け	1		1				3		3	4		4
学期途中最終学年	7	5	12	10	1	11	8	3	11	25	9	34
両親共働き												
その他	1	2	3	2	1	3	1	4	5	4	7	11
計	9	7	16	12	2	14	12	7	19	33	16	49

※　学期別の集計は区域外就学承諾日で計上
　　ただし、３学期分については、３月中に申請があった者を含む

※　その他の主なもの…教育的配慮、家庭の事情等

資料３

令和７年度　学校選択制の結果(令和８年度入学) について

令和８年３月３１日現在

○転入・転出状況

（単位：人）

選択校／指定校	第一中学校	村山学園第二中学校	第三中学校	大南学園第四中学校	第五中学校	転出計
第一中学校		0	5	6	1	12
村山学園第二中学校	0		4	1	0	5
第三中学校	1	0		2	0	3
大南学園第四中学校	2	0	6		0	8
第五中学校	16	0	0	0		16
転入計	19	0	15	9	1	44

○主な理由

（単位：人）

理由／選択校	友人関係	クラブ活動	通学距離	伝統や校風	その他	計
第一中学校	8	6	0	4	1	19
村山学園第二中学校	0	0	0	0	0	0
第三中学校	3	5	4	1	2	15
大南学園第四中学校	2	3	2	0	2	9
第五中学校	1	0	0	0	0	1
計	14	14	6	5	5	44

その他の主な理由

兄弟関係

令和8年度児童・生徒数及び学級数の状況について

令和8年4月7日現在

1 小学校

学級編制基準　小1～中1:35人、中2・中3:40人

区分	学級数 通常の学級 1年	2年	3年	4年	5年	6年	小計	特別支援学級	合計	在籍者数 通常の学級 1年	2年	3年	4年	5年	6年	小計	特別支援学級(固定)	合計	備考(特別支援学級種別等)
第一小学校	2	2	2	2	2	2	12	7	19	5	4	9	4	2	3	27	46	347	知的障害(固定) 4学級
										0	2	4	5	2	6	19			自閉症・情緒障害(固定) 3学級
										48	54	49	52	43	55	301			
第二小学校	2	2	2	2	2	2	12		12	51	62	41	59	65	62	340		340	
第三小学校	2	2	2	2	2	3	13		13	61	62	61	49	59	73	365		365	
村山学園第四小学校	2	2	2	2	2	2	12		12	51	63	60	68	65	64	371		371	日本語(通級) 2学級
大南学園第七小学校	3	3	3	3	4	4	20		20	102	97	104	96	114	104	617		617	特別支援教室拠点校
第八小学校	3	3	3	4	3	4	20		20	90	91	103	109	105	106	604		604	特別支援教室拠点校
第九小学校	2	2	2	2	2	2	12		12	41	44	48	46	45	39	263		263	難聴(通級) 1学級 言語障害(通級) 3学級 特別支援教室拠点校
第十小学校	2	2	2	2	2	2	12	3	15	3	4	0	1	2	3	13	20	373	知的障害(固定) 2学級
										1	2	0	3	0	1	7			自閉症・情緒障害(固定) 1学級
										53	56	62	54	63	65	353			
雷塚小学校	1	1	1	2	1	1	7	7	14	7	10	6	6	3	8	40	53	215	知的障害(固定) 5学級
										3	1	0	2	3	4	13			自閉症・情緒障害(固定) 2学級
										20	30	23	36	30	23	162			
小学校計	19	19	19	21	20	22	120	17	137	15	18	15	11	7	14	80	119	3,495	知的障害(固定)
										4	5	4	10	5	11	39			自閉症・情緒障害(固定)
										517	559	551	569	589	591	3,376			

在籍者数の3段書き上2段は特別支援学級(固定級)の児童数であり外数

2 中学校

区分	学級数 通常の学級 1年	2年	3年	小計	特別支援学級	合計	在籍者数 通常の学級 1年	2年	3年	小計	特別支援学級(固定)	合計	備考(特別支援学級種別等)
第一中学校	6	4	5	15	5	20	12	11	12	35	35	551	知的障害(固定) 5学級
							188	155	173	516			
村山学園第二中学校	2	2	2	6	8	14	14	6	5	25	55	208	知的障害(固定) 4学級
							6	7	17	30			自閉症・情緒障害(固定) 4学級
							44	53	56	153			
第三中学校	4	4	4	12		12	5	3	7	15		281	チャレンジクラス 3学級
							71	97	98	266			特別支援教室拠点校
大南学園第四中学校	3	3	3	9		9	103	89	88	280		280	
第五中学校	5	5	5	15		15	171	163	178	512		512	特別支援教室拠点校
中学校計	20	18	19	57	13	70	26	17	17	60	90	1,832	知的障害(固定)
							6	7	17	30			自閉症・情緒障害(固定)
							582	560	600	1,742			

在籍者数の2段書き上段及び3段書き上2段は特別支援学級(固定級)の生徒数であり外数

ただし、第三中学校在籍者数の上段はチャレンジクラスの生徒数であり外数

第三中学校チャレンジクラス3学級(各学年1学級)は「通常の学級」内に含む

第三中学校チャレンジクラスの生徒は通常学級に含む

令和8年度児童・生徒数総数

	通常学級	特別支援学級	合 計
小学校	3,376	119	3,495
中学校	1,742	90	1,832
合 計	5,118	209	5,327

3 日本語学級通級児童数(村山学園第四小学校)

学年	1年	2年	3年	4年	5年	6年	合 計
児童数	2	7	8	4	6	0	27

4 難聴通級指導学級通級児童数(第九小学校)

学年	1年	2年	3年	4年	5年	6年	合 計
児童数	0	0	1	1	1	1	4

5 言語障害通級指導学級通級児童数(第九小学校)

学年	1年	2年	3年	4年	5年	6年	合 計
児童数	7	6	5	11	12	4	45

6 特別支援教室利用児童数(拠点校:◎)

設置校	拠点校	1年	2年	3年	4年	5年	6年	合 計
第一小学校	九小	3	3	1	6	1	4	18
第二小学校	八小	1	2	3	4	1	2	13
第三小学校	九小	4	3	5	3	3	4	22
村山学園第四小学校	七小	0	8	3	9	3	5	28
大南学園第七小学校	◎	3	3	8	5	6	4	29
第八小学校	◎	3	0	3	5	2	8	21
第九小学校	◎	0	2	2	4	5	0	13
第十小学校	八小	0	2	5	2	4	3	16
雷塚小学校	七小	2	1	2	2	0	1	8
利用者数計		16	24	32	40	25	31	168

7 特別支援教室利用生徒数(拠点校:◎)

設置校	拠点校	1年	2年	3年	合計
第一中学校	三中	2	6	7	15
村山学園第二中学校	五中	1	3	4	8
第三中学校	◎	0	3	6	9
大南学園第四中学校	五中	1	4	6	11
第五中学校	◎	4	6	6	16
利用者数計		8	22	29	59

表3～表7は表1、2の児童・生徒数の内数

資料５

令和8年度小・中学校等の教職員数

令和8年4月1日現在

単位:人

小学校

学校名	学級数	校長	副校長	主幹教諭	指導教諭	主任教諭	教諭	主幹教諭（養護）	主任養護教諭	養護教諭	主任栄養教諭	栄養教諭	事務職員	計	暫定（定年前）再任用（短）	非常勤教員
第一小学校	12 (7)	1	1	2		4	19			1				28		
第二小学校	12	1	1	2		6	8			1				19		
第三小学校	13	1	1	3		8	7			1				21		
村山学園小学部	12 (2)		2	2		4	13			1				22		
大南学園第七小学校	19 (1)	1	1	2		12	17		1			1		35		1
第八小学校	20 (1)	1	1	2	1	11	16			1				33		
第九小学校	12 (5)	1	1	3		5	18			1				29	1	
第十小学校	12 (3)	1	1	2		10	10			1			4	29		
雷塚小学校	7 (7)	1	1	1		6	12			1				22		
小計	119 (26)	8	10	19	1	66	120	0	1	8	0	1	4	238	1	1

中学校

学校名	学級数	校長	副校長	主幹教諭	指導教諭	主任教諭	教諭	主幹教諭（養護）	主任養護教諭	養護教諭	主任栄養教諭	栄養教諭	事務職員	計	暫定（定年前）再任用（短）	非常勤教員
第一中学校	15 (5)	1	1	3		9	22			1				37		
村山学園中学部	6 (8)	1	1	1		7	17		1				4	32		1
第三中学校	9 (4)	1	1	2		7	15			1				27		2
大南学園第四中学校	9	1	1	3		5	7		1					18	1	
第五中学校	15 (1)	1	1	2		6	19		1					30		
小計	54 (18)	5	5	11	0	34	80	0	3	2	0	0	4	144	1	3

	学級数	校長	副校長	主幹教諭	指導教諭	主任教諭	教諭	主幹教諭（養護）	主任養護教諭	養護教諭	主任栄養教諭	栄養教諭	事務職員	計	暫定（定年前）再任用（短）	非常勤教員
小・中学校計	173 (44)	13	15	30	1	100	200	0	4	10	0	1	8	382	2	4

		主幹教諭	栄養士
学校給食課	防災食育ｾﾝﾀｰ		2
指導主事		3	

※ （ ）内は特別支援学級、特別支援教室、日本語学級及びチャレンジクラス

令和8年度教職員の異動状況

令和8年4月1日現在

単位：人

学校名		校長		副校長		教諭（主幹教諭・主任教諭含む）		養護（主幹・主任養護教諭含む）		栄養教諭		事務職員		教諭・栄養・養護・事務職員計	
		転入	転出	転入	転出	転入	転出	転入	転出	転入	転出	転入	転出	転入	転出
小学校	第一小学校					7 (3)	7 (2)							7 (3)	7 (2)
	第二小学校					6 (2)	5							6 (2)	5
	第三小学校			転任	転任	3 (1)	1							3 (1)	1
	村山学園小学部			転任 転任	転任 転任	5 (4)	4 (1)							5 (4)	4 (1)
	大南学園第七小学校					4 (2)	2							4 (2)	2
	第八小学校			転任	転任	4 (2)	5 (1)							4 (2)	5 (1)
	第九小学校	昇任	退職			6 (4)	5							6 (4)	5
	第十小学校					4 (1)	3					1	1	5 (1)	4
	雷塚小学校					6 (2)	6							6 (2)	6
	小計	1	1	4	4	45 (21)	38 (4)	0	0	0	0	1	1	46 (21)	39 (4)
中学校	第一中学校		特命			12 (6)	8 (2)							12 (6)	8 (2)
	村山学園中学部	転任	転任			7 (3)	4					2	2	9 (3)	6
	第三中学校	転任	転任			4 (2)	2							4 (2)	2
	大南学園第四中学校					2 (1)	2 (2)							2 (1)	2 (2)
	第五中学校					5 (2)	5 (1)							5 (2)	5 (1)
	小計	2	3	0	0	30 (14)	21 (5)	0	0	0	0	2	2	32 (14)	23 (5)
合計		3	4	4	4	75 (35)	59 (9)	0	0	0	0	3	3	78 (35)	62 (9)

※転入の(　)内は新規採用教員の内数

※転出の(　)内は退職者の内数

栄養士	転入	転出
防災食育センター	1	1

指導主事	転入	転出
	1	0

令和８年度　武蔵村山市立学校　行事予定等一覧表

【教育目標】（平成23年12月改定）

学校教育においては、家庭における教育の成果を基盤としながら、児童・生徒が、豊かな心をもち、確かな学力や健やかな体力を身に付けることができるようにするために、

○自らまなび、主体的に判断し、創造力豊かに、よりよく問題を解決しようとする子供

○思いやりと協力を重んじ、規範意識及び公共の精神に基づき、進んで社会の形成に参画しようとする子供

○生命を尊び、自然を大切にし、環境の保全に寄与しようとする子供

○伝統と文化を尊重し、我が国と郷土を愛するとともに、国際社会の平和と発展に貢献しようとする子供の育成を重視する。

令和8年度　特色ある学校づくり推進校　研究発表会

雷塚小学校：令和9年1月29日（金）

主題「対話と通して協働的に学び続ける児童の育成」

小中一貫校村山学園：令和9年2月5日（金）

主題「自ら考え、判断し、表現できる児童・生徒の育成

～デジタルを活用した基礎的・基本的な学力の向上～」

教育相談室

【住所】学園4−5−1　市民総合センター3階【電話】0120−910−548/590−1470

【相談受付時間】土・日・祝日を除く　午前9時～午後5時

ゆうゆう教室（適応指導教室）

【住所】学園4−5−1　市民総合センター3階【電話】590−1253

	第一小学校 校長　押本　純樹 【住所】 本町1−1−11 【電話】 561−1751	第二小学校 校長　細田　真司 【住所】 三ツ木2−12−2 【電話】 560−1752	第三小学校 校長　佐々木　琢 【住所】 中藤1−36−1 【電話】 561−1753	第八小学校 校長　井口　洋 【住所】 三ツ藤2−50−1 【電話】 560−7151	第九小学校 校長　加藤　寛之 【住所】 学園1−85−1 【電話】 564−1359	第十小学校 校長　今井　一馬 【住所】 残堀5−100−1 【電話】 560−1710	雷塚小学校 校長　赤坂　弘樹 【住所】 学園4−6−1 【電話】 561−1775	小中一貫校村山学園 統括校長　飯星　健司 【住所】緑が丘1460 【電話】561−1762		小中一貫校大南学園 第七小学校 校長　川口　周作 【住所】 大南2−78−1 【電話】 564−1286	第四中学校 校長　福泉　宏介 【住所】 大南2−79−1 【電話】 564−4341	第一中学校 校長　森元　隆之 【住所】 本町2−76−1 【電話】 560−1761	第三中学校 校長　井内　潔 【住所】 神明4−117−1 【電話】 564−3001	第五中学校 校長　大野　博史 【住所】 残堀5−55 【電話】 560−3155
始業式	◆1学期始業式：4月7日（火）　◆2学期始業式：9月1日（月）〔第九小：8月31日（月）、第十小：8月28日（金）、第七小：8月31日（月）、第四中：8月31日（月）、第三中：8月31日（月）、第五中：8月27日（木）〕　◆3学期始業式：1月8日（金）													
終業式・修了式	◆1学期終業式：7月17日（金）　◆2学期終業式：12月25日（金）　◆修了式：3月25日（木）													
入学式 卒業証書授与式	◆入学式：4月7日（火）　◆卒業証書授与式：3月24日（水）							◆入学式：4月8日（水） ◆卒業証書授与式（小）：3月24日（水） ◆卒業証書授与式（中）：3月19日（金）		◆入学式： 4月7日（火） ◆卒業証書授与式： 3月24日（金）	◆入学式： 4月8日（水） ◆卒業証書授与式： 3月19日（金）	◆入学式：4月8日（水）　◆卒業証書授与式：3月19日（金）		
道徳地区公開講座	6月6日（土）	5月9日（土）	9月26日（土）	9月26日（土）	6月13日（土）	9月18日（金）	12月12日（土）	10月7日（水）		10月3日（土）	10月10日（土）	9月4日（金）	1月16日（土）	1月16日（土）
離任式	3月25日（木）	4月24日（金）	5月1日（金）	4月24日（金）	5月1日（金）	3月25日（木）	3月25日（木）	3月25日（木）		3月23日（火）	3月25日（木）	3月25日（木）	3月25日（木）	3月25日（木）
連合音楽会	11月17日（火）〔全小学校5年生対象〕													
合唱コンクール								10月24日（土）			10月23日（金）	3月5日（金）	10月21日（水）	10月22日（木）
音楽鑑賞教室	11月4日（水）〔全小学校6年生対象〕													
芸術・ 演劇鑑賞教室	日時未定	日時未定	12月11日（金）	10月実施予定	日時未定	11月27日（金）	12月実施予定	隔年実施 （今年度は実施予定なし）		日時未定				
小中一貫教育の日	◆一中校区 10月14日（水）	◆五中校区 10月7日（水）	◆三中校区 3月2日（火）	◆五中校区 10月7日（水）	◆一中校区 10月14日（水）	◆五中校区 10月7日（水）	◆三中校区 3月2日（火）	10月15日（木）		10月14日（水）		◆一中校区 10月14日（水）	◆三中校区 3月2日（火）	◆五中校区 10月7日（水）
文化的行事等	◆学習発表会 11月20日（金） 11月21日（土）	◆展覧会 11月27日（金） 11月28日（土）	◆学習発表会 2月19日（金） 2月20日（土）	◆展覧会 11月26日（木） ～11月28日（土）	◆展覧会 11月27日（金） 11月28日（土）	◆学習発表会 2月18日（木） ～2月20日（土）	◆音楽会 11月20日（金） 11月21日（土）	◆展覧会 11月27日（金） 11月28日（土）		◆展覧会 12月18日（金） 12月19日（土）				
運動会	10月10日（土）	10月10日（土）	10月17日（土）	10月10日（土）	10月10日（土）	6月6日（土）	10月17日（土）	5月30日（土）		10月31日（土）	5月30日（土）			
セーフティ教室	10月16日（金） 10月19日（月）	9月17日（金）	9月24日（金）	6月6日（土）	10月6日（火） ～10月8日（木）	10月6日（火） ～10月8日（木）	10月7日（水） ～10月9日（金）	6月10日（水）		10月2日（金） 10月3日（土）	6月12日（金）	6月11日（木）	6月12日（金） スケアードストレイト：11月5日（木）	6月12日（金）
交通安全教室等	5月9日（土）	4月28日（火） 自転車安全教室：2月25日（木）	5月8日（金）中高 5月14日（木）低	4月10日（金）	5月8日（金）	4月28日（火） （1・4年）	4月13日（月）	自転車安全教室：4月16日（木） 交通安全指導：5月8日（金）		6月8日（月）4年 6月23日（火）3年				
移動教室（小6） 修学旅行（中3）	7月5日（日） ～7月7日（火）	6月24日（水） ～6月26日（金）	6月17日（水） ～6月19日（金）	6月30日（火） ～7月2日（木）	6月1日（月） ～6月3日（水）	10月21日（水） ～10月23日（金）	6月11日（木） ～6月13日（土）	7月7日（火） ～7月9日（木）	9月25日（金） ～9月27日（日）	6月25日（木） ～6月27日（土）	9月24日（木） ～9月26日（土）	10月11日（日） ～10月13日（火）	10月1日（木） ～10月3日（土）	10月1日（木） ～10月3日（土）
特別支援学級 宿泊行事	さくら・杉の子 9月11日（金） 9月12日（土）						なのはな・ひまわり 10月29日（木） 10月30日（金）	S組 10月8日（木） 10月9日（金）				I組 9月16日（水） 9月17日（木）		
もちつき大会	実施予定なし	12月12日（土）	1月16日（土）	1月16日（土）	1月16日（土）	1月23日（土）	実施予定なし	1月15日（金）		実施予定なし				
都民の日		休日	休日			休日	休日			休日		休日		
その他行事	◆サマーコンサート 7月15日（水） ♦スマイルコンサート 12月19日（土） ♦プラバン定期演奏会 2月27日（土）	◆栄村学校訪問 7月7日（火） ～7月9日（木） ◆高尾林間学校 7月27日（月） 7月28日（火） ◆二小秋まつり 9月12日（土） ♦ももの木コンサート 2月28日（日）	◆丘の上キャンプ 9月11日（金） 9月12日（土） ◆村山大島紬体験 10月5日（月）	♦きょうだい学級遠足 5月8日（金） ◆徳育科授業地区公開講座 9月26日（土）	◆全校遠足 10月28日（水） ◆九小祭 1月16日（土）	◆十小夏まつり 6月27日（土） ◆職場体験 7月21日（火） ～7月24日（金）	♦ふれあいフェスティバル 6月24日（水） ◆総合防災訓練 2月13日（土）	◆名栗移動教室 10月28日（水） ～10月30日（金）	◆職場体験 7月8日（水） ～7月10日（金） ◆スキー教室 1月27日（水） ～1月29日（金）	◆社会科見学 5月28日（木）6年 6月12日（金）4年 11月12日（木）2年 11月19日（木）1年 11月26日（木）5年 1月28日（木）3年	◆職場体験 9月7日（月） ～9月9日（水） ◆スキー教室 1月24日（日） ～1月26日（火）	◆職場体験 7月1日（水） ～7月3日（金） ♦ティキティキフェスティバル 12月12日（土） ♦スマイルコンサート 12月19日（土） ◆スキー教室 2月7日（日） ～2月9日（火）	◆職場体験 6月24日（水） ～6月26日（金） ◆食育講演会 11月21日（土） ◆スキー教室 2月4日（木） ～2月6日（土）	♦五中フェスティバル 7月4日（土） ◆職場体験 9月1日（火） ～9月3日（木） ◆スキー教室 2月11日（木） ～2月13日（土）
学校公開週間	10月5日（月） ～10月8日（火）	9月16日（水） ～9月18日（金）	9月24日（木） ～9月26日（土）	10月14日（水） ～10月16日（金）	9月18日（金） 9月19日（土）	10月6日（火） ～10月8日（木）	10月7日（水） ～10月9日（金）	6月10日（水）～6月12日（金） 10月5日（月）～10月7日（水）		10月2日（金） 10月3日（土）	6月8日（月） ～6月12日（金）	6月8日（月） ～6月12日（金）	6月8日（月） ～6月13日（土）	6月8日（月） ～6月12日（金）

令和8年4月1日現在

令和8年度 武蔵村山市立学校 研究活動等一覧

校区	校区目標	学校名	まちづくり学習目標	研究指定・事業名				発表会・報告会
施設一体型 小中一貫校	9年間の義務教育における系統的・継続的な学びを通して、「社会を構成し運営するとともに、自立した一人の人間としてカ強く生きていくための総合的な力」である「人間力」（知的能力、対人関係力、自己制御力）を身に付けた児童・生徒を育成する。	小中一貫校村山学園 H22年度 校庭芝生化 H23年度 コミュニティスクール	地域と連携した探究学習で、市の発展や課題を考え、地域を大切にする心と主体的・協働的に挑戦する力を養う。	平成23年度～	学校と家庭の連携推進校	都	16	特色ある学校づくり推進校発表会 令和9年2月5日 （金）
				平成23年度～	小中一貫教育研究指定校	市	16	
				平成30年度～	地域防災連携「村学レンジャー」	市	9	
				平成30年度～	太陽光パネルを活用した環境教育推進校	市	9	
				令和7・8年度	特色ある学校づくり推進校	市	2	
				令和8年度	「デジタルを活用したこれからの学び」実践協力校	都	1	
施設隣接型 小中一貫校	「自主創造」 自主・自立 共生・貢献 健康・大志	小中一貫校大南学園 第七小学校 H23年度 校庭芝生化 H25年度 コミュニティスクール	武蔵村山市の良さを見付け、自分たちでできることを考え実践していく力を身に付ける。	平成24年度～	教育課題研究校「食育・学校園活用」	市	15	
				平成27年度～	小中一貫教育研究指定校	市	12	
				令和3年度～	学校と家庭の連携推進校	都	4	
				令和6・7年度	体育健康教育推進校	都	3	
				令和6年度～	小学校教科担任制等推進事業	都	3	
		小中一貫校大南学園 第四中学校	・自分たちの住んでいる武蔵村山市の伝統や文化を知り、故郷についての理解や郷土愛を深める。 ・よりよい地域づくりのために課題を見出し主体的に考え、行動しようとする実践意欲と態度を育てる。	平成23年度～	学校と家庭の連携推進校	都	16	
				平成27年度～	小中一貫教育研究指定校	市	12	
				平成27年度～	部活動ハンドボール競技奨励校	市	12	
				平成30年度～	太陽光パネルを活用した環境教育推進校	市	9	
施設分離型 小中一貫教育 【一中校区】	共に生きることに喜びを感じ、自ら学びに向かい、心身ともに健やかで、粘り強く取り組む児童・生徒を育成する。 ①自ら学びに向かう児童・生徒 ③心身ともに元気な児童・生徒 ②心豊かにやさしい児童・生徒 ④あきらめず頑張る児童・生徒	第一小学校 H23年度 校庭芝生化 H25年度 コミュニティスクール	主体的に地域とかかわり、地域に根差した探究的な学習を深めることにより、地域を大切にする思いをはぐくみ、よりよい社会の実現に向け、自分たちに何ができるか考え、行動する態度を育てる。	令和元年度～	小中一貫教育推進校（一中校区）	市	8	
				令和2年度～	学校と家庭の連携推進校	都	7	
				令和7年度～	ゼロカーボンシティチャレンジ校	市	2	
				令和8・9年度	特色ある学校づくり推進校	市	1	
		第九小学校 H24年度 校庭芝生化 H26年度 コミュニティスクール	・地域への興味・関心を高める。 ・身の回りの課題に対して自分なりにできることを考える。 ・地域に愛着をもち、地域の一員としての意識を高める。	平成28年度～	学校と家庭の連携推進校	都	11	
				令和元年度～	小中一貫教育推進校（一中校区）	市	8	
				令和7年度～	ゼロカーボンシティチャレンジ校	市	2	
		第一中学校 H23年度 校庭芝生化 H25年度 コミュニティスクール	地域との関わりの中で生徒が地域を大切にする思いを育む。	平成25年度～	学校と家庭の連携推進校	都	14	
				平成27年度～	海外派遣教師によるALL ENGLISH講座事業	市	12	
				平成30年度～	太陽光パネルを活用した環境教育推進校	市	9	
				令和元年度～	小中一貫教育推進校（一中校区）	市	8	
				令和7年度～	ゼロカーボンシティチャレンジ校	市	2	
				令和8・9年度	特色ある学校づくり推進校	市	1	
施設分離型 小中一貫教育 【三中校区】	家庭・地域・学校が一体となり、子供たちの道徳的実践力の育成及び学力向上を目指す。	第三小学校 H23年度 校庭芝生化 H26年度 コミュニティスクール	・武蔵村山市の魅力を知り、市・地域への愛着を深め、将来の担い手としての自覚を育む。 ・武蔵村山市のために自分たちができることを考え、実行・実現させるために行動することができる。	平成24年度～	学校と家庭の連携推進校	都	15	
				平成30年度～	小中一貫教育推進校（三中校区）	市	9	
				令和7・8年度	「デジタルを活用したこれからの学び」実践協力校	都	2	
		雷塚小学校 H24年度 校庭芝生化 H25年度 コミュニティスクール	・身近な地域に興味・関心をもち、まちへの愛着を育てる。 ・地域の発展や課題について考え、まちをよりよくしようとする思いを育む。	平成25年度～	太陽光パネルを活用した環境教育推進校	市	14	特色ある学校づくり推進校発表会 令和9年1月29日 （金）
				平成28年度～	学校と家庭の連携推進校	都	11	
				平成30年度～	小中一貫教育推進校（三中校区）	市	9	
				令和7・8年度	特色ある学校づくり推進校	市	2	
		第三中学校 H23年度 校庭芝生化 H25年度 コミュニティスクール	環境教育（ゼロカーボン学習）に取り組み、生徒が環境保全の意識を高め、よりよい地域づくりに参画する意欲・行動力の育成を推進する。また、平和学習をとおして今後の平和な社会を築く一員としての自覚・態度を養う。	平成28年度～	学校と家庭の連携推進校	都	11	
				平成30年度～	小中一貫教育推進校（三中校区）	市	9	
				平成30年度～	太陽光パネルを活用した環境教育推進校	市	9	
				令和6年度	チャレンジクラス（不登校対応校内分教室）設置校	都	3	
				令和6年度	校内別室指導支援員配置校	都	3	
				令和8年度	教育課程実践検証協力校	国	1	
施設分離型 小中一貫教育 【五中校区】	確かな学力と豊かな心を育み、自信と誇りをもって21世紀を逞しく生き抜く子供の育成	第二小学校 H24年度 校庭芝生化 H26年度 コミュニティスクール	本校学区域や武蔵村山市の産業や伝統文化等について、探究的な学習を通して地域に対する理解を深めるとともに、愛着と誇り、将来への希望をもつことができる。	平成25年度～	完全午前5時間制推進校	市	14	
				令和元年度～	小中一貫教育推進校（五中校区）	市	8	
				令和2年度～	学校と家庭の連携推進校	都	7	
				令和8・9年度	教育課題柔軟化サキドリ研究校	国	1	
		第八小学校 H24年度 校庭芝生化 H24年度 コミュニティスクール	・自ら生活する地域について知り、視野を広げ、地域の一員として生きていこうとする態度を身に付ける。 ・地域の人々と関わり合って生活をしていることに気付き、よりよい人との関わりについて考え行動できる。	平成26年度～	「徳育科」推進モデル校	市	13	
				平成28年度～	学校と家庭の連携推進校	都	11	
				平成30年度～	教育課程特例校（徳育科）	国	9	
				令和元年度～	小中一貫教育推進校（五中校区）	市	8	
				平成21年度～	完全午前5時間制推進校	市	18	
				令和7年度～	小学校教科担任制等推進事業	都	2	
		第十小学校 H24年度 校庭芝生化 H26年度 コミュニティスクール	地域資源・人材等を活用した教育活動を通して、新たな学びの実現を目指す。	平成22年度～	日本の伝統・文化教育推進事業	市	17	
				令和元年度～	小中一貫教育推進校（五中校区）	市	8	
				令和3年度～	学校と家庭の連携推進校	都	6	
				令和4年度～	完全午前5時間制推進校	市	5	
		第五中学校 H23年度 校庭芝生化 H26年度 コミュニティスクール	まちづくり学習を通して、自分が住む地域に対する歴史、風土、産業などを知り、郷土愛を深めるとともに、現在の課題を模索し、解決する方法を考えることで、未来のまちづくりを担おうとする態度を養う。	平成27年度～	地域防災連携五中レスキュー隊	市	12	
				平成27年度～	部活動ハンドボール競技奨励校	市	12	
				平成30年度～	太陽光パネルを活用した環境教育推進校	市	9	
				令和元年度～	小中一貫教育推進校（五中校区）	市	8	
				令和2年度～	学校と家庭の連携推進校	都	7	
				令和6年度	不登校対応巡回教員配置校	都	3	

資料８

令和８年度～いきいきわくわく狭山丘陵ウォーク～
第４９回武蔵村山市歩け歩け大会について

１　主　　催　　武蔵村山市教育委員会

２　主　　管　　武蔵村山市スポーツ推進委員協議会

３　協　　力　　一般社団法人武蔵村山市体育協会
武蔵村山市中藤地区スポーツ協力員連絡会
武蔵村山市西部地区スポーツ協力員連絡会
武蔵村山市北部地区スポーツ協力員連絡会
武蔵村山市南部地区スポーツ協力員連絡会

４　期　　日　　令和８年５月１７日（日）雨天中止
受　　付　　午前９時００分から９時３０分まで
スタート　　受付後順次スタート
※開催の有無は午前７時３０分に決定（市ＳＮＳで周知）

５　集合場所　　野山北公園運動場

６　コ　ー　ス　　約６．５ｋｍコース
※別紙 第４９回武蔵村山市歩け歩け大会コース一覧のとおり

７　制限時間　　３時間以内（午後０時３０分までに）ゴールすること。

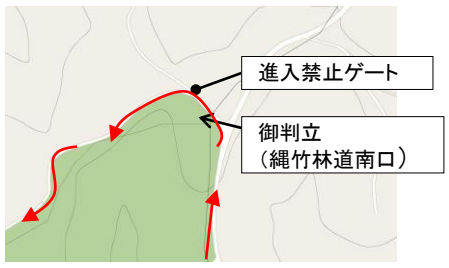
８　参加資格　　市内在住・在勤・在学者で完歩する体力のある方。
ただし、小学校３年生以下の参加は、保護者同伴とする。

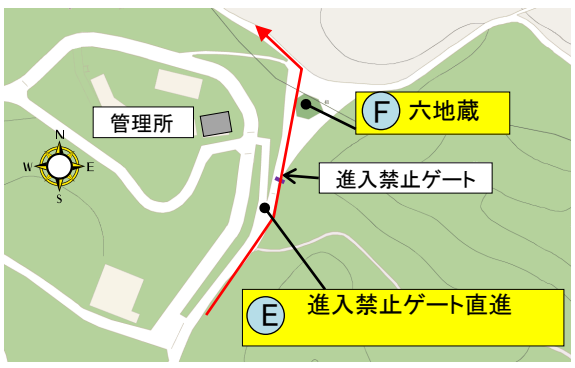
９　申 込 み　　大会当日、現地での受付とする。
申込書は、４月３０日（木）から、スポーツ振興課、総合体育館、市政情報コーナー、緑が丘出張所、市民総合センター緑が丘ふれあいセンターに配置するほか、当日会場にも用意する。

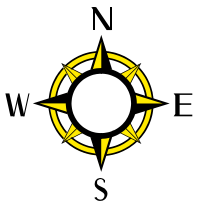
10　参 加 費　　無料

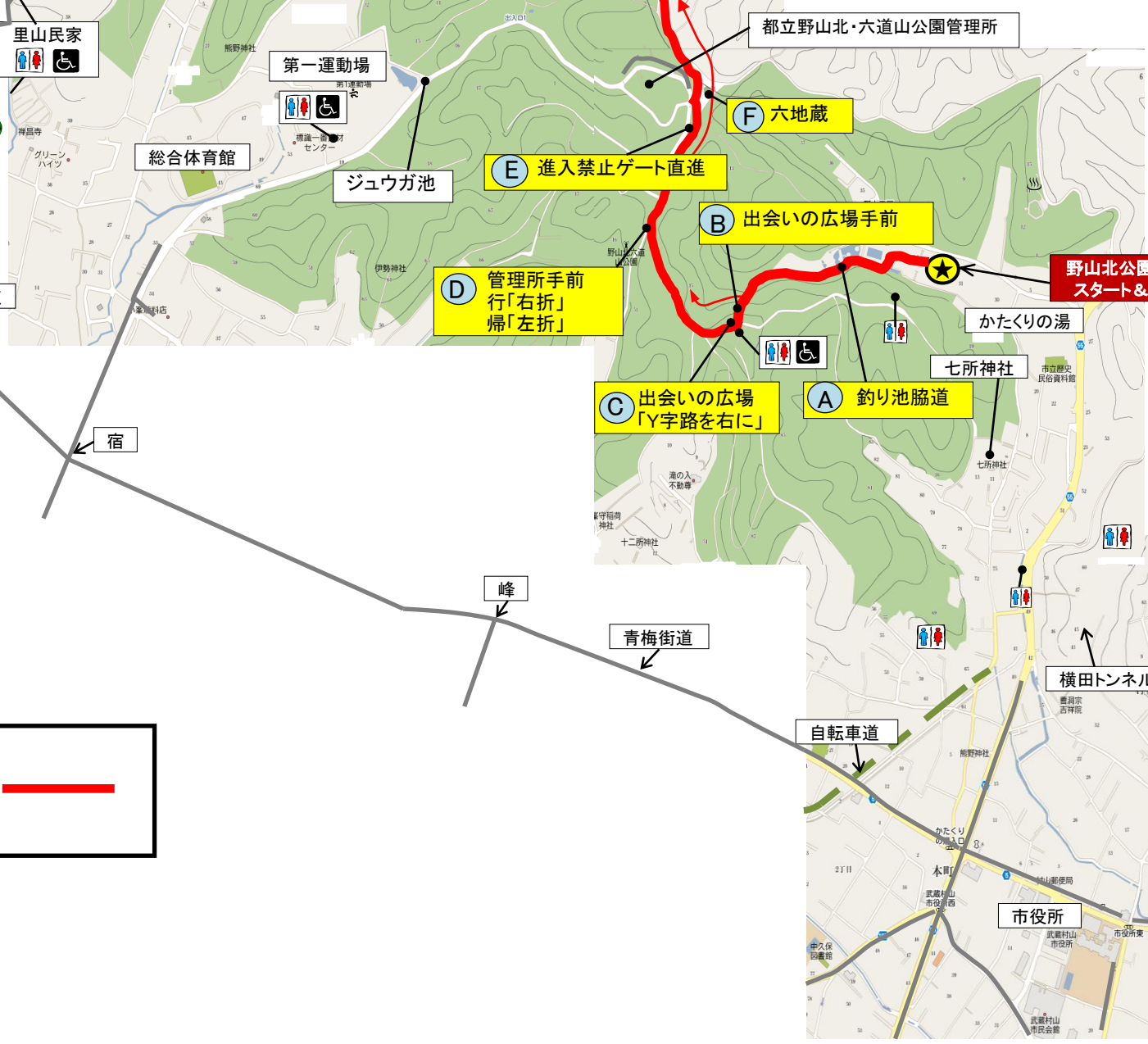
別紙

第49回武蔵村山市歩け歩け大会コース　令和8年5月17日(日)開催









資料９

令和８年度 蔵書点検に伴う臨時休館について

1　目的

所蔵している資料を点検確認し、所在不明資料の除籍処理を行うなど適正な資料管理を行う。

2　休館日（日付順）

図書館名	休　館　日
中藤地区図書館	令和８年５月１２日（火）から１５日（金）まで
残堀・伊奈平地区図書館	令和８年５月１９日（火）から２２日（金）まで
大南地区図書館	令和８年５月２６日（火）から２９日（金）まで
三ツ木地区図書館	令和８年６月２日（火）から５日（金）まで
雷塚図書館	令和８年６月９日（火）から１２日（金）まで
中久保図書館	令和８年６月１６日（火）から１９日（金）まで