武蔵村山市情報セキュリティポリシー

令和４年８月（改定）

武　蔵　村　山　市

目　次

第１章　武蔵村山市情報セキュリティポリシーの構成 1

第２章　武蔵村山市情報セキュリティ基本方針 2

１　目的 2

２　定義 2

⑴　ネットワーク 2

⑵　情報システム 2

⑶　機密性 2

⑷　完全性 2

⑸　可用性 2

⑹　マイナンバー利用事務系（個人番号利用事務系） 2

⑺　総合行政ネットワーク（LGWAN）接続系 2

⑻　インターネット接続系 2

⑼　通信経路の分割 2

⑽　無害化通信 3

⑾　情報資産 3

⑿　情報セキュリティ 3

⒀　情報セキュリティポリシー 3

３　適用範囲 3

⑴　行政機関の範囲 3

⑵　情報資産の範囲 3

４　職員等及び委託事業者の責務 3

５　情報資産への脅威 3

⑴　人による脅威（故意）……3
⑵　人による脅威（過失）……4
⑶　災害による脅威……4
⑷　必要資産の不足、故障等による脅威……4
6　情報セキュリティ管理体制……4
7　情報セキュリティ対策……4
⑴　情報システム全体の強靭性の向上……4
⑵　物理的セキュリティ……4
⑶　人的セキュリティ……5
⑷　技術的セキュリティ……5
⑸　運用……5
8　情報セキュリティ対策基準の策定……5
9　情報セキュリティ実施手順の策定……5
１０　緊急時の対応……5
１１　情報セキュリティ監査及び自己点検の実施……5
１２　情報セキュリティポリシー等の見直し……6
第３章　武蔵村山市情報セキュリティ対策基準……7
1　対策基準の考え方……7
2　目的……8
3　適用範囲……8
4　組織体制……9
⑴　情報セキュリティ対策の管理体制……9
⑵　役割と責務……10

⑶　兼務の禁止 12
5　情報資産の分類と管理方法 12
⑴　情報資産の分類 12
⑵　情報資産の管理 12
6　特定個人情報等の取扱い 15
7　情報システム全体の強靭性の向上 15
⑴　マイナンバー利用事務系 15
⑵　総合行政ネットワーク（LGWAN）接続系 15
⑶　インターネット接続系 16
8　物理的セキュリティ 16
⑴　サーバ等の管理 16
⑵　管理区域の管理 17
⑶　通信回線及び通信回線装置の管理 18
⑷　職員等のパソコン等の管理 19
9　人的セキュリティ 19
⑴　職員等の遵守事項 19
⑵　研修・訓練 20
⑶　情報セキュリティインシデントの報告 21
⑷　ID 及びパスワード等の管理 21
１０　技術的セキュリティ 22
⑴　コンピュータ及びネットワークの管理 22
⑵　アクセス制御 27
⑶　システム開発、導入、保守等 28

⑷　不正プログラム対策 31
⑸　不正アクセス対策 33
⑹　セキュリティ情報の収集 34
１１　運用 35
⑴　情報システムの監視 35
⑵　情報セキュリティポリシーの遵守状況の確認 35
⑶　侵害時の対応等 36
⑷　例外措置 36
⑸　法令遵守 37
⑹　懲戒処分等 37
１２　外部サービスの利用 38
⑴　委託事業者の選定基準 38
⑵　契約項目 38
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） 38
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） 42
⑸　ソーシャルメディアサービスの利用 42
１３　評価・見直し 43
⑴　監査 43
⑵　点検 45
⑶　情報セキュリティポリシー及び関係規程等の見直し 46
用語集 47

第１章　武蔵村山市情報セキュリティポリシーの構成

本市が所掌する情報資産に関する情報セキュリティ対策については、武蔵村山市個人情報保護条例第９条に個人情報の適正管理が規定され、これを受けて武蔵村山市電子計算組織の管理運営に関する規則では、データの管理規定が設けられている。

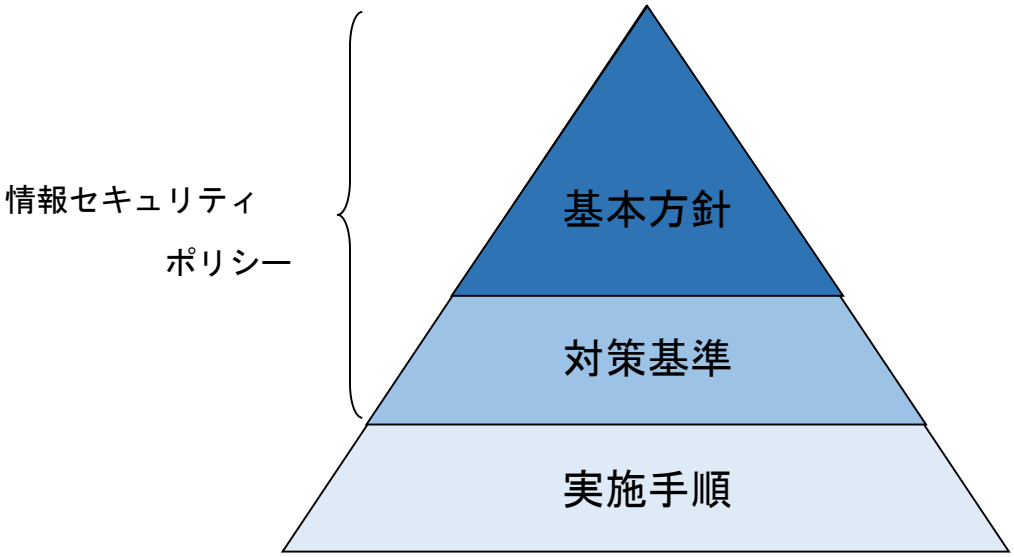
武蔵村山市情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）は、これらの規定をより具体化し、本市が所掌する情報資産に関する業務に携わる全職員、非常勤及び臨時職員（以下「職員等」という。）並びに委託事業者に浸透、普及、定着させるものであり、安定的な規範である。

しかしながら一方では、情報技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーは、一定の普遍性を備えた部分である情報セキュリティ基本方針と情報資産を取り巻く状況の変化に依存する部分である情報セキュリティ対策基準に分けて策定することとする。

なお、情報セキュリティ実施手順は、情報セキュリティ対策基準を踏まえ、具体的なシステムや手順、手続に展開して個別の実施事項について、業務担当課において策定するものであることから、情報セキュリティポリシーには含まれない。

情報セキュリティポリシーの構成



第２章　武蔵村山市情報セキュリティ基本方針

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。

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　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。

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。

⑸　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。

⑹　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。

⑺　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。）。

⑻　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。

⑼　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。

⑽　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。

⑾　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。

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。

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。

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。

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

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。

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

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。

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。

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。

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　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。

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。

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。

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。

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。

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。

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。

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。

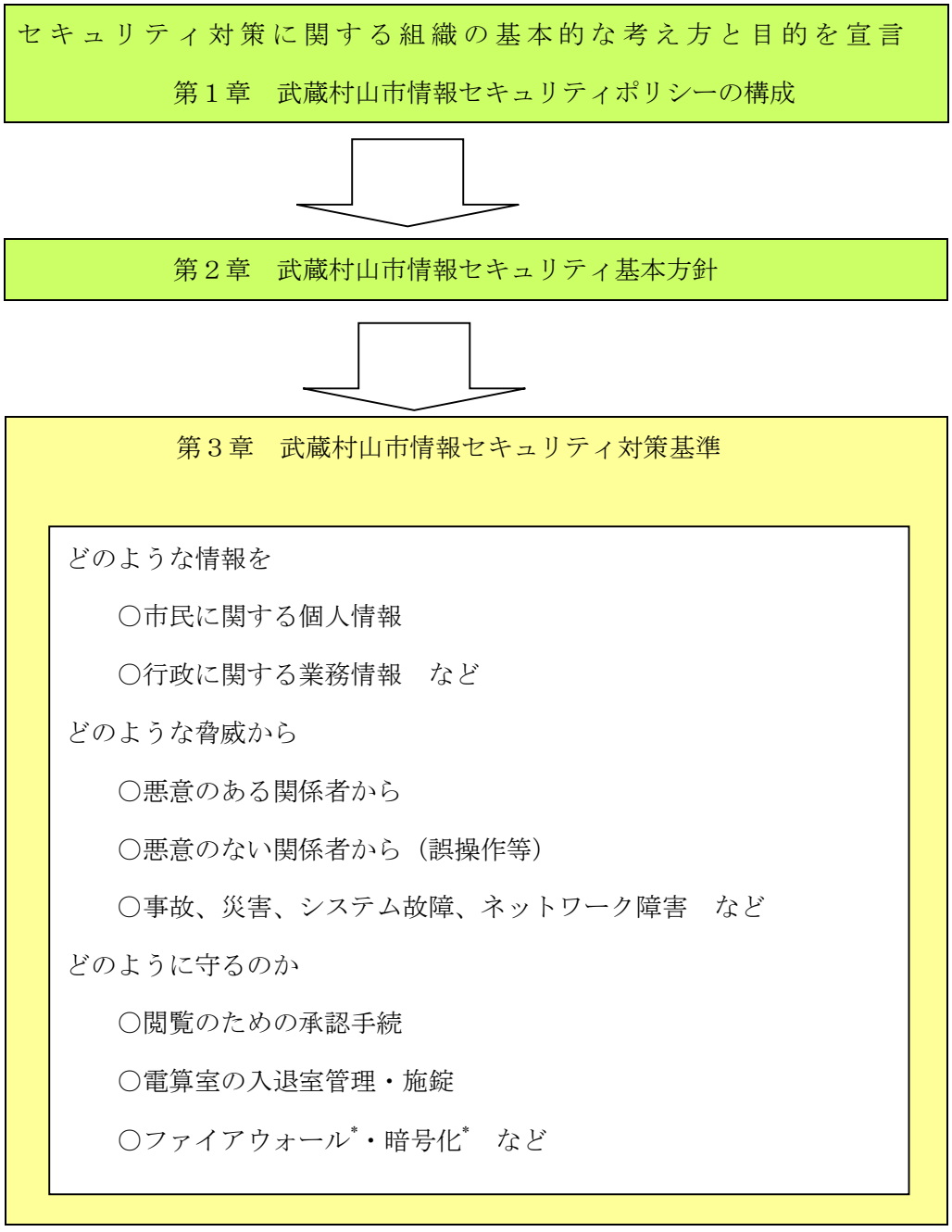
１２　情報セキュリティポリシー等の見直し

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。

第３章　武蔵村山市情報セキュリティ対策基準

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。

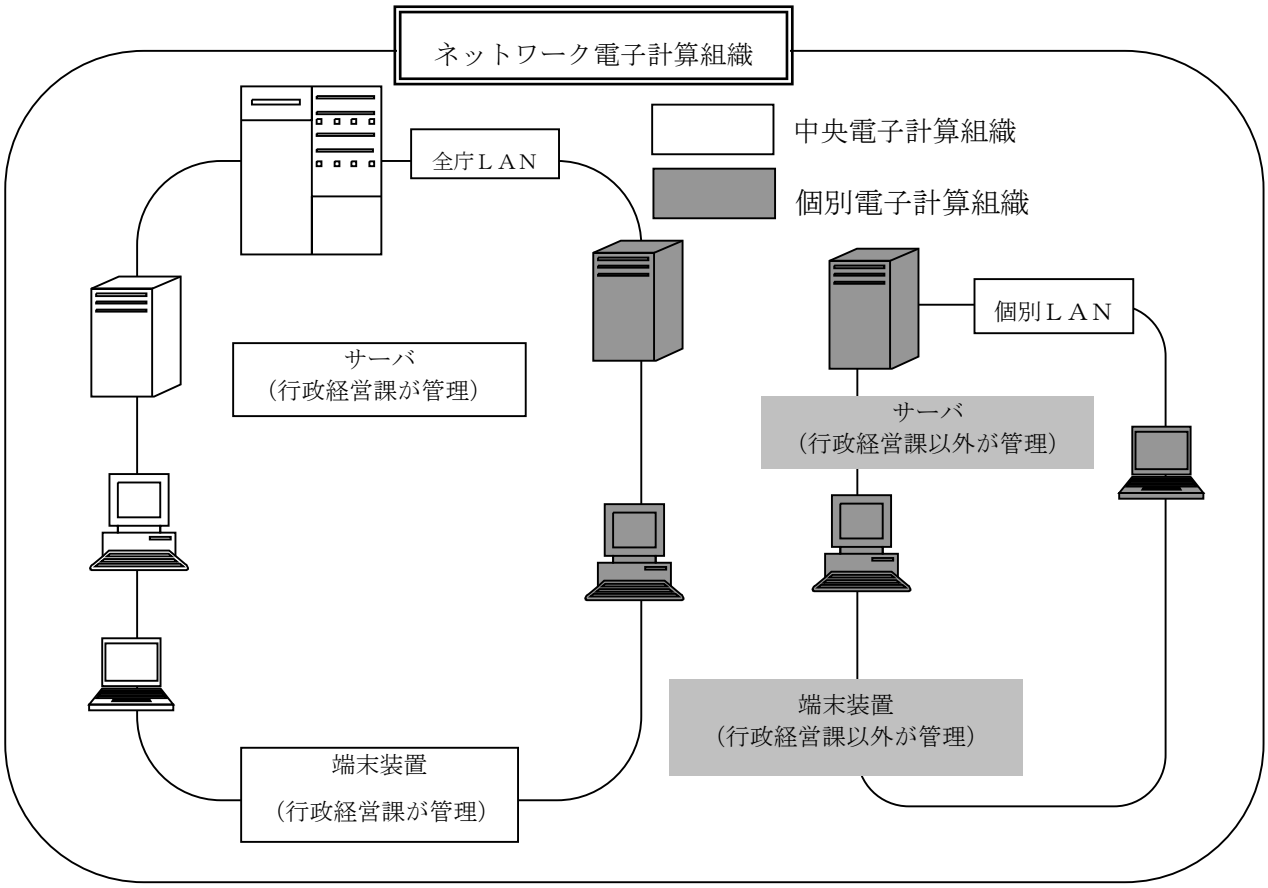


2　目的

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。

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。

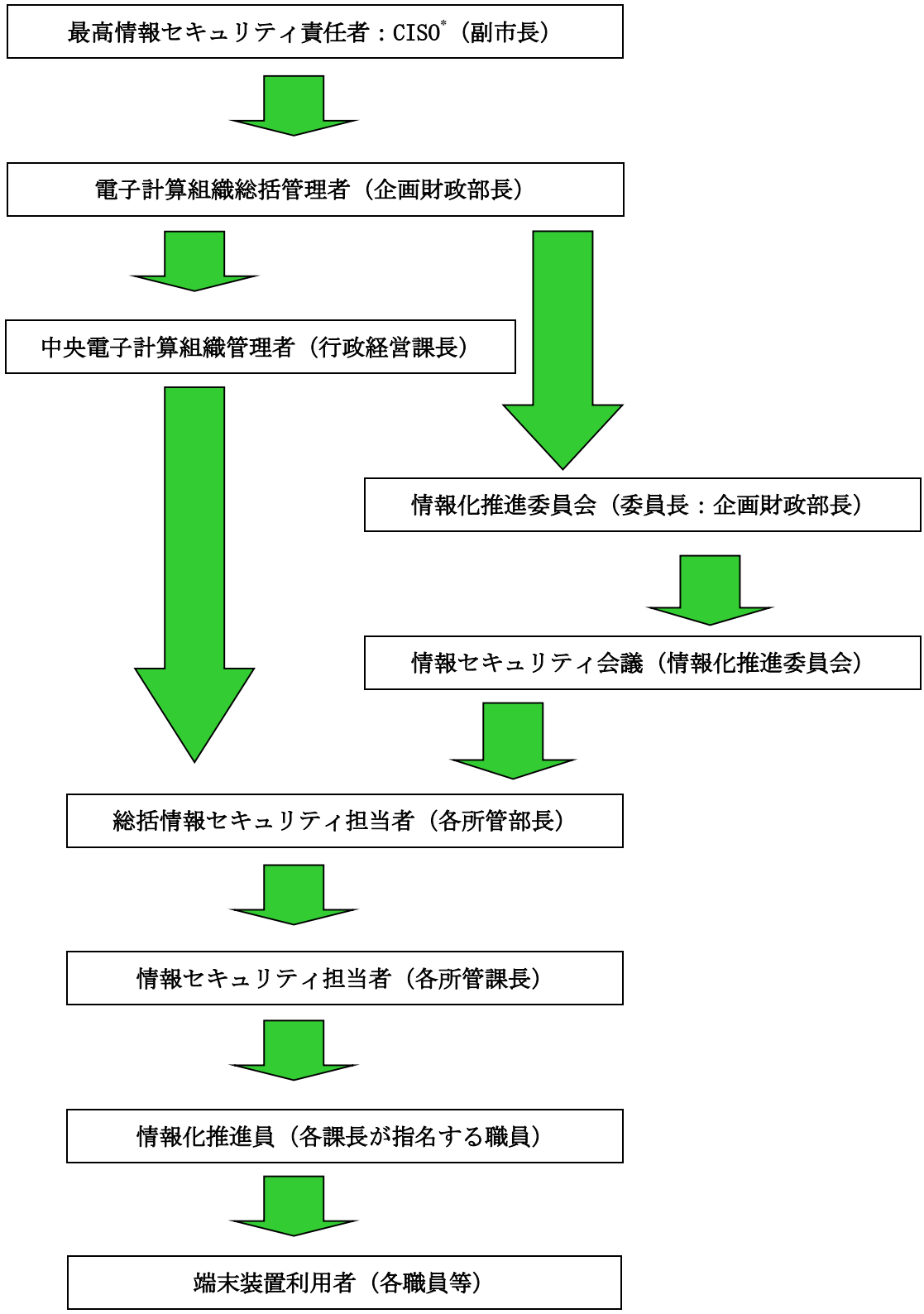


＊ ネットワークに接続されていない端末装置（パソコン）については、小規模電子計算組織となる。

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。



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)　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。

(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。

(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。

ウ　中央電子計算組織管理者（行政経営課長）

(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)　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。

(ｳ)　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。

(ｴ)　他の所管に係る情報システムについて指導・助言を行う。

(ｵ)　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。

(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。

(ｷ)　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。

(ｸ)　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。

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。

カ　総括情報セキュリティ担当者（各所管部長）

(ｱ)　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。

(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。

(ｳ)　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、電子計算組織総括管理者に速やかに報告する。

キ　情報セキュリティ担当者（各所管課長）

(ｱ)　各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。

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。

(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。

(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。

(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。

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。

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。

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

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(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

(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。

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)　業務以外の目的に情報資産を利用しないこと。

(ｲ)　情報資産の分類に応じ、適切な取扱いをすること。

(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

(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。

(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　情報資産の運搬・送付

(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)　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る限り安全な手段を講じること。

ク　情報資産の送信・提供・公表

(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)　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)　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。

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。

(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。

7 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 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

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、総合行政ネットワーク（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。

8　物理的セキュリティ

⑴　サーバ等の管理

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切に固定する等、必要な措置を講じなければならない。

イ　サーバの冗長化*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。

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)　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)　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。

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)　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)　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)　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)　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。

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。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。

(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。

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。

(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　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、次の事項を遵守しなければならない。

(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)　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。

⑶　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。

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。

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。

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。

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。

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すること。

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。

⑷　職員等のパソコン等の管理

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。

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。

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。

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。

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

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。

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

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。

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。

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。

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。

⑵　研修・訓練

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。

イ　研修の実施

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。

ウ　緊急時対応訓練

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。

エ　研修・訓練への参加

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。

⑶　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。

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。

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

(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。

(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。

⑷　ID及びパスワード等の管理

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。

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。

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。

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。

(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。

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。

(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。

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。

(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)　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。

(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。

１０　技術的セキュリティ

⑴　コンピュータ及びネットワークの管理

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。

(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。

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。

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。

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)　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)　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。

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。

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)　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)　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。

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。

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)　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)　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。

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。

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。

(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。

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。

(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。

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。

(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) 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。

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) 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) 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) 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) 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) 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。

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) 自動転送機能を用いて、電子メールを転送しないこと。

(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) 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) 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ること。

ソ 電子署名・暗号化

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。

タ　無許可ソフトウェアの導入等の禁止

(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、情報セキュリティ担当者は、ソフトウェアのライセンスを管理しなければならない。

(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。

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担当者の許可を得ること。

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担当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。

テ　Web会議サービス*の利用時の対策

(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。

(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。

⑵　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

(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)　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。

(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。

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、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。

⑶　システム開発、導入、保守等

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)　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)　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) 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。

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

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。

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。

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

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。

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。

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) 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。

(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。

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

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。

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。

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。

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。

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

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。

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。

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。

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。

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。

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。

(ｲ)　テスト結果を一定期間保管すること。

(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。

オ　情報システムにおける入出力データの正確性の確保

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。

(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)　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。

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。

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。

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。

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。

(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。

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。

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。

(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中断しないこと。

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。

⑸　不正アクセス対策

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。

(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。

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。

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。

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。

１１　運用

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。

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。

ウ　外部と常時接続する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。

⑵　情報セキュリティポリシーの遵守状況の確認

ア　遵守状況の確認及び対処

(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)　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。

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)　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。

(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　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）に従って適切に対処しなければならない。

⑶　侵害時の対応等

ア　武蔵村山市業務継続計画（ＩＣＴ編）の策定

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。

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。

(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

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。

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。

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

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。

(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。

１２　外部サービス*の利用

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　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。

ア　情報セキュリティポリシーの遵守

イ　委託事業者の責任者、委託内容、作業者、作業場所の特定

ウ　提供されるサービスレベルの保証

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

オ　委託事業者の従業員に対する研修の実施

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

キ　業務上知り得た情報の守秘義務

ク　再委託に関する制限事項の遵守

ケ　委託業務終了時の情報資産の返還、廃棄等

コ　委託業務の定期報告及び緊急時報告義務

サ　市による監査、検査

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

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）

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

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

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

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

e　情報セキュリティインシデントへの対処方法

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

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、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、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。

a　情報セキュリティ監査の受入れ

b　サービスレベルの保証

(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、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、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、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。

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、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。

(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。

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)　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)　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。

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)　外部サービス管理者は、(ｱ)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

(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。

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。

(ｱ)　外部サービスを利用可能な業務の範囲

(ｲ)　外部サービスの利用申請の許可権限者と利用手続

(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)　外部サービスの利用の運用手順

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)　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。

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。

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。

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点も併せて監査を行う。

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。

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。

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
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 必要に応じ情報化推進委員会に報 告

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。

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。

ク　報告等

(ｱ)　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。

(ｲ)　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。

ケ　保管

(ｱ)　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。

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。

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。

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。

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。

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。

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。

用語集

アカウント

コンピュータやソフトウェア、ネットワーク等を使用するための権利や資格のこと。また、それらのシステムにログインするために必要な ID とパスワードの組み合わせをアカウントと呼ぶこともある。

暗号化

情報を他人に知られないようにするため、データを見てもその内容が分からないように、定められた処理手順でデータを変えること。暗号化されたデータは、復号という処理によって元のデータに戻すことができる。

Web（ウェブ）会議サービス

専用のアプリケーションや Web ブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行える外部サービスをいう。なお、特定用途機器同士で通信を行うもの（テレビ会議システム等）は含まれない。

外部サービス

事業者等の庁外の組織が情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において自組織の情報が取り扱われる場合に限る。

外部サービス管理者

外部サービスの利用における利用申請の許可権限者から利用承認時に指名された当該外部サービスに係る管理を行う者をいう。

外部サービス提供者

外部サービスを提供する事業者をいう。外部サービスを利用して自組織に向けて独自のサービスを提供する事業者は含まれない。

ゲートウェイ

情報システムにおける通信において、異なるネットワーク間での通信を中継する役割を持つ機器や

仕組みのこと。

サービス不能攻撃

インターネット上で提供されるサービスについて、不正に大量の電子データを送り付ける等して対象サービスに過剰な負荷を与えて停止させたり、サービスの正常な稼働を妨害したりする攻撃のこと。

CISO

Chief Information Security Officer の略で最高情報セキュリティ責任者のこと。地方公共団体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や情報セキュリティに関する権限及び責任を有する。

冗長化

情報システムの運用において、システム障害や機器、ネットワーク回線等の故障等が発生しても、情報システムを停止させずに稼働し続けられるように、予備の装置等をあらかじめ配置し運用しておくこと。

情報セキュリティインシデント

情報セキュリティに関する障害・事故及びシステム上の欠陥のこと。

スパムメール

利用者が送信を要求していないにも関わらず、勝手に送り付けてくる商品広告等の電子メールのこと。

セキュリティホール

ソフトウェア等において、情報セキュリティ上の欠陥となる不具合のこと。脆弱性とも呼ばれる。

総合行政ネットワーク（LGWAN）

地方公共団体の組織内ネットワーク（庁内LAN）を相互に接続し、高度なセキュリティを維持した行政専用ネットワークのこと。

ソーシャルメディアサービス

インターネット上で展開される情報メディアの在り方で、組織や個人による情報発信や個人間のコミュニケーション、人の結び付きを利用した情報流通などといった社会的な要素を含んだメディアのこと。利用者の発信した情報や利用者間のつながりによってコンテンツを作り出す要素を持ったWebサイトやネットサービスなどを総称する用語で、電子掲示板(BBS)やブログ、動画共有サイト、動画配信サービス、ショッピングサイトの購入者評価欄等を含む。

ソースコード

情報システムにおける各種プログラムの動作の全てが記述されたテキストファイルのこと。ソースコードは人間が読み書きできる言語で記述されており、これをコンピュータが理解できる言語に変換することでプログラムが完成する。

多要素認証

以下のうち、二つ以上の認証方式を組み合わせてセキュリティを高める方式のこと。

・ID/パスワード等対象者の知識を利用したもの

・ICカード等対象者の持ち物を利用したもの

・指紋認証等対象者の身体の特徴を利用したもの

通信ソフトウェア

フィルタリングやルーティングの設定を行うために利用されるソフトウェアのこと。

ネットワークストレージサービス

インターネット上で電子データをアップロードすることができるサービスのこと。一般的にはアップロードした本人しか電子データを利用できないが、利用するサービスによっては、特定の個人や不特定多数に向けて電子データを公開することができるものがある。ビジネスにおいては、電子メールの添付ファイルで送信できない大容量の電子データの受け渡し等において本サービスが多く活用されている。

パッチ

完成したプログラムに対して、脆弱性等をなくすために後から配布される修正プログラムのこと。

メーカーのホームページ等で提供されている。

標的型攻撃

特定の組織を狙って、機密情報や知的財産、アカウント情報等を窃取しようとする攻撃のこと。この攻撃では、標的の組織がよくやり取りをする形式のメールを送り付け、そこに付いている添付ファイルやリンクをクリックさせ、そこからコンピュータウイルス感染サイト等に誘導する等の手口がよく使われている。

ファイアウォール

外部のネットワークと内部のネットワークを結ぶ箇所に導入するシステムで、外部からの不正な侵入を防ぐことができる。

フィルタリング

有害情報サイト等からの保護等を行うこと。その他に、コンピュータウイルスや不正アクセスからの保護を主な目的とするファイアウォールもフィルタリングの一種である。

複合機

プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器のこと。

モバイル端末

業務上の必要に応じて移動させて使用することを目的とした端末のこと。端末の形態は問わない。

ルーティング

情報システム間でやり取りされる電子データの通信経路（電子データの届け先）を設定すること。

改定履歴

・平成１６年３月　策　　定
・平成３０年３月　全部改定
・令和２年４月　　一部改定
・令和３年４月　　一部改定
・令和４年８月　　一部改定

武蔵村山市情報セキュリティポリシー
発行年月／令和４年８月
発　　行／武蔵村山市
編　　集／武蔵村山市企画財政部行政経営課
〒208-8501
武蔵村山市本町一丁目１番地の１
TEL　042（565）1111（代表）