

サイバーセキュリティを確保する ための方針

令和8年4月1日策定

〈 目 次 〉

第1章 情報セキュリティ基本方針	1
1 目的	1
2 定義	1
3 対象とする脅威	2
4 適用範囲	2
5 職員等の遵守事項	3
6 情報セキュリティ対策	3
7 情報セキュリティ監査及び自己点検の実施	4
8 情報セキュリティポリシーの見直し	4
9 情報セキュリティ対策基準の策定	5
10 情報セキュリティ実施手順の策定	5

第1章 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は、市及び一部事務組合の議会、長（地方公営企業の管理者を含む。）並びに委員会及び委員（以下、「執行機関等」という。）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、執行機関等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

(1) 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及びその構成機器（ハードウェア及びソフトウェアを含む。）をいう。

(2) 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。

(3) 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。

(4) 情報セキュリティポリシー

情報セキュリティ基本方針及び情報セキュリティ対策基準をいう。

(5) 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。

(6) 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。

(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。

(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）、戸籍事務等に関わる情報システム及びデータをいう。

(9) LGWAN接続系

LGWAN（総合行政ネットワークをいう。以下同じ。）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。）。

(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。

(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。

(12) 無害化通信

インターネットメール本文のテキスト化、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な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、次の脅威を想定し、情報セキュリティ対策を実施する。

- (1) 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃、部外者の侵入等の意図的な要因による情報資産の漏えい、破壊、改ざん、消去、重要情報の詐取、内部不正等
- (2) 情報資産の無断持出し、無許可ソフトウェアの使用等の規定違反、設計及び開発の不備、プログラム上の欠陥、操作及び設定のミス、メンテナンス不備、内部及び外部の監査機能の不備、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の要因による情報資産の漏えい、破壊、消去等
- (3) 地震、落雷、火災等の災害によるサービス及び業務の停止等
- (4) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
- (5) 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

4 適用範囲

(1) 行政機関の範囲

本基本方針が適用される行政機関は、市長部局、行政委員会、議会事務局、監査委員事務局及び地方公営企業並びに執行機関等とする。

(2) 情報資産の範囲

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、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、非常勤職員、会計年度任用職員等（以下「職員等」という。）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を遵守しなければならない。

6 情報セキュリティ対策

(1) 組織体制

執行機関等の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

(2) 情報資産の分類と管理

執行機関等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。

(3) 情報システム全体の強靱性の向上

情報セキュリティの強化を目的とし、業務の効率性及び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することができないようにした上で、端末からの情報持出不可設定、端末への二つ以上を併用する認証（以下「多要素認証」という。）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し、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し、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する自治体情報セキュリティクラウドの導入等を実施する。

(4) 物理的セキュリティ

サーバ、電算機室（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をいう。以下同じ）、通信回線、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。

(5) 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。

(6) 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。

(7) 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、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

(8) 業務委託及びクラウドサービスの利用

ア 業務委託を行う場合には、執行機関等が業務を委託する事業者（以下「委託事業者」という。）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。

イ 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。

ウ 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。

(9) 評価及び見直し

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、リスクを検討した上で、情報セキュリティポリシーを見直す。

9 情報セキュリティ対策基準の策定

第1章第6項、第7項及び前項に規定する対策等を実施するため、具体的な遵守事項、判断基準等を定める情報セキュリティ対策基準を策定するものとする。

10 情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、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情報セキュリティ実施手順を策定するものとし、情報セキュリティ実施手順は、公にすることにより執行機関等の運営に重大な支障を来すおそれがあることから非公開とする。