加須市情報セキュリティ基本方針

（平成２８年１２月２８日市長決裁）
（改定　平成３１年　４月　１日一部改定）
（改定　令和　２年　４月　１日一部改定）
（改定　令和　３年　４月　１日一部改定）
（改定　令和　５年　４月　１日一部改定）
（改定　令和　７年　４月　１日一部改定）

（目的）

第１条　この基本方針は、本市が保有するネットワーク、情報システム及びこれらに関する設備並びに情報資産（以下「対象資産」という。）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。

（定義）

第２条　この基本方針における用語の定義は、当該各号に定めるところによる。

（１）　コンピュータ

パーソナルコンピュータ、サーバ、ストレージ等の機器をいう。

（２）　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）をいう。

（３）　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。

（４）　情報資産

情報システムで取扱う情報で、開発及び運用に係るものを含むすべての情報をいう。

（５）　情報セキュリティ

対象資産の機密性、完全性及び可用性を維持することをいう。

（６）　情報セキュリティポリシー

この基本方針及び情報セキュリティ対策基準をいう。

（７）　機密性

対象資産にアクセスすることを認められた者のみが、情報にアクセスできる状態を確保することをいう。

（８）　完全性

対象資産が破壊、改ざん、消去又は不正なデータのない状態を維持し、データの正当性、正確性、一貫性等を確保することをいう。

（９）　可用性

対象資産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。

（１０）　マイナンバー利用事務系

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。

（１１）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）。

（１２）インターネット接続系

インターネットメール等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。

（１３）通信経路の分割

LGWAN 接続系とインターネット接続系と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。

（１４）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の有無を確認し安全が確保された通信をいう。

（対象とする脅威）

第３条　対象資産に対する脅威として、次の各号の脅威を想定し、情報セキュリティ対策を実施する。

（１）　人による脅威（故意）

不正アクセス又はウイルス攻撃等のサイバー攻撃、機器の盗難、対象資産の不正な操作及び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

（２）　人による脅威（過失）

対象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又は操作ミス若しくは設定ミス、システムのメンテナンス不備、委託管理の不備等の過失による情報資産の漏えい、破壊、消去等

（３）　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

（４）　必要資源の不足、故障等による脅威

災害の影響又はその他の原因による電力、通信、水道の途絶、交通機能の麻痺、大規模又は広範囲にわたる疾病の蔓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、システム運用の機能不全等

（適用範囲）

第４条　この基本方針の適用範囲は、本市が保有するすべての対象資産に関する業務に携わる全ての特別職及び一般職の職員（非常勤職員を含む。以下「職員等」という。）並びに委託事業者とする。

（遵守義務）

第５条　前条に規定する者は、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。

（情報セキュリティ対策）

第６条　第３条の脅威から対象資産を保護するために、次の各号の情報セキュリティ対策を講じるものとする。

（１）　組織体制

本市が保有する情報資産について、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）　情報資産の分類及び管理

本市が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、当該分類に基づく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ものとする。

ア　マイナンバー利用事務系は、次の LGWAN 接続系及びインターネット接続系に掲げる領域との通信をできないようにし、端末からの情報持ち出し不可設定、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ようにしなければならない。

イ　LGWAN 接続系は、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、無害化通信を実施しなければならない。

ウ　インターネット接続系は、不正通信の監視機能の強化その他の高度な情報セキュリティ対策を実施する。この場合において、埼玉県及び埼玉県内の市町村のインターネット接続口を集約し、自治体情報セキュリティクラウドの導入を実施するものとする。

（４）　物理的セキュリティ

対象資産の設置方法又は保管施設の管理についての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な対策を講じる。

（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情報セキュリティの確保等に係る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、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）　業務委託と外部サービス(クラウドサービス)の利用

ア　業務委託を行う場合には、委託事業者を選定し、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、情報セキュリティ要件を明記した契約を締結するものとする。

イ　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ものとする。

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・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。

（情報セキュリティに関する監査及び自己点検の実施）

第７条　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に関する監査及び自己点検を実施する。

（情報セキュリティポリシーの見直し及び改定）

第８条　情報セキュリティに関する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の見直しを行い、必要に応じて改定する。

（情報セキュリティ対策基準の策定）

第９条　第６条、第７条及び前条に規定する対策等を実施するため、具体的な遵守事項及び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。

（情報セキュリティ実施手順等の策定）

第１０条　情報セキュリティ対策基準に基づき、情報セキュリティに関する対策を実施するため、必要に応じて、具体的な手順を定める情報セキュリティ実施手順等を策定する。