基本方針

第２章　情報セキュリティ基本方針

2.1 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と共に情報システムの安全かつ適正な運用を確保するため、サイバーセキュリティの確保を重要な施策と位置づけ、必要な措置を講じることを目的とする。

2.2 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、その構成機器(ハードウェア及びソフトウェア)をいう。

(2)　情報システム

コンピュータ、ネットワーク及び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

本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、地方税若しく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。

(9)　情報系

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。）。

(10)　インターネット接続系

インターネットに接続された情報システム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

情報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や端末への画面転送等により、コンピュータウィ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。

(13)　Web 会議系

LGWAN を経由せずに直接インターネットに接続し、Web 会議等を行う通信をいう。

2.3 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。

(1) 外部からの不正アクセス、マルウェア感染、情報漏えい等の脅威に対し、技術的・組織的対策を講じる。

(2) セキュリティパッチの適用、ウイルス対策ソフトの導入、ファイアウォールの設定等を継続的に実施する。

(3) サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報資産の漏洩・破壊・改ざん・消去、重要情報の搾取、内部不正等

(4) 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洩・破壊・消去等

(5) 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

(6) 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

(7) 電力供給の途絶、通信の途絶、水道供給の途絶等の提供サービスの障害からの波及等

2.4 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、選挙管理委員会、公平委員会、監査委員、固定資産評価審査委員会、議会、農業委員会、教育委員会、消防本部及び地方公営企業とする。特に教育委員会事務局、小中学校、教育関連施設（社会教育施設・図書館等）、並びにこれらに関連する外部委託事業者を含む。教育現場においては、『みやま市教育委員会教育情報セキュリティポリシー』及び文部科学省『教育情報セキュリティポリシーガイドライン』を参照し、児童生徒の個人情報及び教育データの保護を徹底する。

(2)　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。

① ネットワーク、情報システム並びにこれらに関する設備、電磁的記録媒体

② 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。）

③ 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

(3)　職員等の範囲

本基本方針が適用される職員及び職員に準ずる者（以下「職員等」という。）は次のとおりとする。

①（１）に示す行政機関に所属する職員、再任用職員、会計年度任用職員及び特別職等

②①に準じ、（２）に示す情報資産を取り扱う者（教職員、議員、各行政委員会等の委員、地方公営企業の職員及び委託事業者等）

2.5 職員等の遵守義務

上記(3)で示す範囲の者（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。

2.6 情報セキュリティ対策

上記2.3.の対象とする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。

(1)　組織体制

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

(2) サイバー攻撃等のインシデント発生時には、速やかに対応できる体制を整備し、関係機関との連携を図る。

(3) インシデント対応マニュアルを整備し、定期的な見直しを行う。

(4)　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。

(5) 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。

① 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。

② 情報系においては、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。

③ 情報系及び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、福岡県とみやま市のインターネットとの接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

(6)　物理的セキュリティ

サーバ等、サーバ室、通信回線等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、サイバーセキュリティに関する教育・訓練を定期的に実施し、意識の向上を図る。

(7)　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。

(8)　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。

(9)　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、外部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、情報資産への侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応マニュアルを策定する。

(10)　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、利用にかか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。~~情報システムの運用・保守等を外部に委託する場合は、委託先に対しても同等のセキュリティ対策を求め、契約に明記する。

(11)　評価・見直し

サイバーセキュリティに関する脅威や技術の変化に対応するため、情報セキュリティ方針を定期的に見直し、必要な改定を行う。

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、情報セキュリティポリシーの見直しを行う。

2.7 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。

2.8 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、情報セキュリティポリシーを見直す。

2.9 情報セキュリティ対策基準の策定

上記2.6.，2.7.及び2.8.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情報セキュリティ対策基準を策定する。

2.10 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する。

なお、情報セキュリティ実施手順は、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。