第１章　情報セキュリティ基本方針

１　目的

この基本方針は、羽生市（以下「市」という。）の職員等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、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、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

この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

情報が破壊され、改ざんされ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）　ＬGWAN

地方公共団体の組織内ネットワークを相互に接続した行政専用のセキュリティネットワーク（総合行政ネットワーク（Local Government Wide Area Network）の略称）

（９）　ＬGWAN-ＡＳＰ

ＬGWANを介して、利用者である地方公共団体に各種行政事務を行うためのシステムやサービスを提供することをいう。許可された者のみが利用できる閉域接続とファイルの無害化処理等により強固なセキュリティを有している。

（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を含む。）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、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。

（１３） 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なく、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、次に掲げる脅威を想定し、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、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

（２） 人による脅威（過失）

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、設計又は開発の不備、プログラム上の欠陥、操作又は設定のミス、メンテナンス不備、内部又は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

（３） 災害による脅威

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） 新型インフルエンザ等の疾病による脅威

大規模かつ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） 電力不足、故障等による脅威

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） 執行機関等の範囲

この基本方針が適用される執行機関等の範囲は、市長の執行部局、教育委員会等の行

政委員会又は委員、議会（議員及び議会事務局）、消防本部及び地方公営企業とする。なお、基本方針の策定及び見直しは、各執行機関間で市長部局と同一の情報システムやネットワークを使用しており、共通するセキュリティ対策が多くあることから、行政委員会又は委員においては地方自治法（昭和２２年法律６７号）第１８０条の７の規定により長の補助機関である職員に委任して、議会及び地方公営企業においては共同で行うものとする。

（２） 情報資産の範囲

この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

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

５ 職員等の遵守義務

執行機関等の職員（臨時的任用職員及び会計年度任用職員を含む。）、行政委員会の委員及び市議会の議員（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

脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講じる。

（１） 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全庁的な組織体制を確立する。

（２） 情報資産の分類と管理

情報資産を機密性、完全性及び可用性に応じて分類し、管理する。

（３） 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、業務の効率性及び利便性の観点から、情報システムの全体に対し、次に掲げる区分に応じた対策を講じる。

① マイナンバー利用事務系　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を導入する。

② ＬGWAN接続系　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とともに、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 インターネット接続系　都道府県及び市区町村のインターネット回線が集約された「自治体情報セキュリティクラウド」を導入し、不正通信の監視機能の強化

した環境を構築する。

（４） 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。

（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。

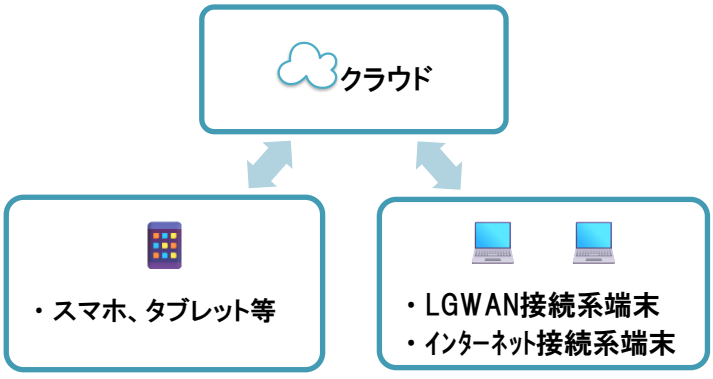
（８） 業務委託と外部サービス（クラウドサービス）の利用

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（図１参照））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。

Ｘ、Ｉｎｓｔａｇｒａｍ、ＬＩＮＥ、Ｆａｃｅｂｏｏｋ等のソーシャルメディアサービスを運用する場合は、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。

図１：クラウドサービスの例示



インターネット上の仮想ストレージに自身のデータを保存し、閲覧することができるサービス

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、利用する情報システムに係る脅威の発生の可能性、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

６～８の前３項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。（図２参照）

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、情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより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。

図２：体系図