【A】

羽村市
情報セキュリティ基本方針

制定	2004 年 6 月	最終改定	2021 年 9 月

【A】

<table>
<tr><td rowspan="2">羽村市</td><td rowspan="2">情報セキュリティ基本方針</td><td>文書－SEC101</td></tr>
<tr><td>第３版</td></tr>
</table>

<table>
<tr><td>制定</td><td>2004 年 6 月</td><td>最終
改定</td><td>2021 年 9 月</td></tr>
</table>

【A】

目　　次

１　目的 ･･ １
２　定義 ･･ １
３　対象とする脅威･･ ２
４　適用範囲･･･ ２
５　情報資産の範囲･･ ２
６　職員及び受託者の責務･･･ ３
７　情報セキュリティ対策･･･ ３
８　情報セキュリティ対策基準の策定･･････････････････････････････････････ ４
９　情報セキュリティ実施手順の策定･･････････････････････････････････････ ４

羽村市情報セキュリティ基本方針

１　目的

羽村市情報セキュリティ基本方針（以下「基本方針」という。）は、市が保有する情報資産を様々な脅威から組織的、体系的かつ継続的に保護するための統一的な方針並びに情報資産の安全管理対策を実践するにあたっての基本的な考え方及び方策を定めることを目的とする。

２　定義

この基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(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)　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。

(5)　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。

(6)　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。

(7)　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。

(8)　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。）。

(9)　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。

(10) 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。

(11) 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。

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)　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)　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、外部委託管理の不備、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)　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

この基本方針は、市が保有する情報資産、情報資産を取り扱う全職員及び市の事務事業の委託を受けた者（以下「受託者」という。）に適用する。

５　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

６　職員及び受託者の責務

職員及び受託者は、情報セキュリティ対策の重要性について共通の認識をもつとともに、業務の遂行において、基本方針を遵守しなければならない。

７　情報セキュリティ対策

上記３の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

情報セキュリティ対策を推進及び管理するための組織体制を整備する。

(2)　情報資産の分類と管理

情報資産を価値等により分類し、当該分類に基づき情報資産の適切な管理を実施する。

(3)　情報システムの強靭化対策

情報セキュリティの強化を目的とし、業務の効率化・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 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 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を実施する。

(4)　物理的セキュリティ対策

情報システムの設置場所、保管場所、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)　人的セキュリティ対策

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対策

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)　外部委託管理

市の事務事業を委託した場合における情報セキュリティを確保するため、外部委託管理を実施する。

(8)　監査、自己点検及びセキュリティポリシーの見直し

セキュリティポリシーの遵守状況を検証するため、情報セキュリティに係る監査及び自己点検を実施する。また、セキュリティポリシーの実効性を維持するためにセキュリティポリシーの見直しを実施する。

８　情報セキュリティ対策基準の策定

上記７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。

なお、情報セキュリティ対策基準は、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。

９　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。