青梅市情報セキュリティ基本方針

1　目的

青梅市情報セキュリティ基本方針（以下「基本方針」という）は、青梅市（以下「市」という。）が保有および管理する情報資産の機密性、完全性および可用性を確保するため、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。

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、その他構成機器（ハードウェアおよびソフトウェア）をいう。

(2) 情報システム

コンピュータ、ネットワークおよ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) マイナンバー利用事務系

個人番号利用事務、戸籍事務等に関わる情報システムおよびデータをいう。

(4) ＬＧＷＡＮ接続系

人事給与、財務会計および文書管理等ＬＧＷＡＮに接続された情報システムおよびその情報システムで取り扱うデータをいう。

(5) 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およびその情報システムで取り扱うデータをいう。

(6) 通信経路の分離

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。

(7) 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。

(8) 庁内ＬＡＮ

市の行政事務を執り行うための情報システムをいう。具体的には、マイナンバー利用事務系、ＬＧＷＡＮ接続系およびインターネット接続系の総体を指す。

(9) 庁内ＬＡＮユーザ

庁内ＬＡＮのアカウントを付与された者のことをいう。

(10) 職員

市の正規職員および会計年度任用職員等のことをいう。

(11) 情報資産

市が保有・管理するデータ（市と委託契約等の関係にある者が委託契約等の業務上管理するものを含む）のことをいう。

(12) 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。

(13) 完全性

情報が破壊、改ざんまたは消去されていない状態を確保することをいう。

(14) 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。

(15) 情報セキュリティ

情報資産の機密性、完全性および可用性を維持することをいう。

(16) 情報セキュリティポリシー

基本方針および情報セキュリティ対策基準をいう。

(17) 外部サービス

市が物理的に管理する情報システム以外のもので、外部主

体により提供される情報システム上のサービス（ソフトウェア、プラットフォームおよびインフラ等）をいう。具体的には、クラウドサービス、ホスティングサービスおよびソーシャルメディアサービス等をいう。

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、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および業務の停止等

(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

適用範囲は、次のとおりとする。ただし、他の情報セキュリティポリシー等に定めがあるものについては適用範囲外とする。

(1) 庁内ＬＡＮおよび庁内ＬＡＮに接続する各種機器（電磁的記録媒体を含む。）

(2) 職員

(3) 市と委託契約等の関係にある者（以下「委託事業者」という。）

(4) 情報資産

5　遵守義務

職員および委託事業者は、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およ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

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

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) 情報資産の分類と管理

市の保有する情報資産を機密性、完全性および可用性に応じて分類し、当該分類にもと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・利便性の観点を踏まえ、庁内ＬＡＮ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。

イ　ＬＧＷＡＮ接続系においては、ＬＧＷＡＮと接続する業務システムと、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。

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する。高度な情報セキュリティ対策として、都道府県および市区町村

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

端末、サーバ、情報システム室および通信回線等の管理について、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、十分な教育およ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

庁内ＬＡＮ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の利用

業務委託を行う場合には、委託事業者と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もとづき措置を講じる。

外部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。

7　情報セキュリティ監査および自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的または必要に応じて情報セキュリティ監査およ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および自己点検の結果、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およ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。

9　情報セキュリティ対策基準の策定

上記６、７および８に規定する対策等を実施するために、具体的な遵守事項およ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、市の行政運営に重大な影響を及ぼすおそれがあることから外部に周知すべき事項を除いて原則非公開とする。

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もとづき、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、市の行政運営に重大な影響を及ぼすおそれがあることから非公開とする。