厚木市情報セキュリティポリシー 概要

第１章　情報セキュリティ基本方針

１　目的

本市が取り扱う情報には、市民の個人情報のみならず行政運営上重要な情報等が数多く含まれ、外部への漏えい等が発生した場合には、極めて重大な結果を招くおそれがある。

したがって、情報資産を漏えいや改ざん、コンピュータウイルスによるシステム障害、災害や事故等の様々な脅威から防御することは、市民の財産及びプライバシー等の保護及び事務の安定的な運用のためには必要不可欠なことである。

こうしたことから、本市が所管する情報資産に関する情報セキュリティ対策を総合的、体系的かつ具体的に整備することを目的に、厚木市情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）を定めることとする。

なお、情報セキュリティポリシーは、本市が所管する情報資産に関する業務に携わる本市の職員、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会、地方公営企業、指定管理者及び委託事業者に浸透させ、普及させ、及び定着させるものであり、安定的な規範であることが要請される。一方、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを、一定の普遍性を備えた部分（情報セキュリティ基本方針）と情報資産を取り巻く状況の変化に依存する部分（情報セキュリティ対策基準）に分けて策定するものとする。

このうち、情報セキュリティ基本方針は、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

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、処理を行う仕組みをいう。

(3) 情報資産

ネットワーク及び情報システムで取り扱う情報並びに紙等の有体物に出力し、又は記録された情報をいう。

(4) 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。

(5) 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。

(6) 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。

(7) 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。

(8) 可用性

情報にアクセスすることを認められた者だけが、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。

(9) 職員

職員、再任用職員、任期付職員、会計年度任用職員、非常勤特別職職員及び労働派遣契約等により本市に従事する者をいう。ただし、教育委員会がその服務について監督権を有する者を除く。

(10) 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。

(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、次の事項を想定し、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

(1) 対象者

本市の職員、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会、地方公営企業、指定管理者及び委託事業者（以下「職員等」という。）

(2) 対象範囲

本市が所管する全ての情報資産

5　職員等の遵守義務

職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たり情報セキュリティポリシー及び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

３で示した脅威から情報資産を保護するために、次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及び適切に管理するための体制を確立する。

(2) 情報資産の分類と管理

本市の情報資産をその内容の重要度に応じて分類し、その重要度に応じた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。

ア　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の導入等により、住民情報の流出を防ぐ。

イ　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。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

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。また、インターネット接続口は、原則として神奈川情報セキュリティクラウドに集約する。

(4) 物理的セキュリティ

サーバ、管理区域、通信回線及び職員等の端末の管理について、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する権限や責任を定め、職員等に情報セキュリティポリシーの内容を周知徹底するための十分な教育及び啓発を行う等の人的対策を講じる。

(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、情報セキュリティ上の緊急事態が発生した際に迅速かつ適正に対応するための危機管理対策を講じる。

(8) 業務委託と外部サービスの利用

ア　業務委託を行う場合

委託事業者を選定し、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た上で、必要に応じて契約に基づき措置を講じる。

イ　外部サービスを利用する場合

クラウドサービスなどの外部サービス及び外部サービス提供者を選定し、利用するための基準は別に定める。

ウ　ソーシャルメディアサービスを利用する場合

本市が管理するアカウントによるソーシャルメディアサービスの利用について、利用に係る基準等は別に定める。

(9) 評価及び見直し

情報セキュリティポリシーを適正に運用するため、定期的又は必要に応じて検証し、運用改善を行い、情報セキュリティの向上を図る。

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となった場合には、情報セキュリティポリシーの見直しを実施する。

９　情報セキュリティ対策基準の策定

６の対策を講じるに当たり、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の一部は、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。

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。

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。