綾瀬市情報セキュリティ基本方針

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（ハードウエア及びソフトウエア）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

情報セキュリティ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) 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。）。

(10) 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。

(11) 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。

(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) 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、無許可ソフトウエ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提供サービスの障害からの波及等

4　対象範囲

(1) 対象とする機関

対象とする機関は、内部部局、行政委員会、議会事務局、消防本部及び地方公営企業とする。

(2) 対象とする情報資産

対象とする情報資産は、次のとおりとする。

ア　ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

ィ　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。）

ウ　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

職員（特別職を含む。）、非常勤職員及び臨時的任用職員（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つとともに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

職員等は、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実施する。

(1) 組織体制

本市の情報資産について、適切に情報セキュリティ対策を推進、管理するための組織体制を確立する。

(2) 情報資産の分類と管理

本市の保有する情報資産は、その内容に応じて分類し、当該分類に基づき管理を行う。

(3) 情報システム全体の強靭性の向上

ア　マイナンバー利用事務系については、他の領域からの通信を遮断し、端末からの情報の持ち出し不可設定や端末への多要素認証の導入等の対策を講じる。

イ　ＬＧＷＡＮ接続系においては、ＬＧＷＡＮ接続系とインターネット接続系の通信経路は分割し、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、県及び市町村のインターネットとの通信を集約する自治体情報セキュリティクラウドの導入等、不正通信の監視機能の強化等の高度なセキュリティ対策を実施する。

(4) 物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷及び妨害等から保護するための物理的な対策を行う。

(5) 人的セキュリティ対策

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教育及び訓練を行う。

(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を実施する。

(7) 運用におけるセキュリティ対策

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の対策を実施する。また、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、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

外部サービス（クラウドサービス）を利用する場合には、利用に係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　情報セキュリティに関する監査及び自己点検の実施

情報セキュリティ対策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、運用改善を行い、情報セキュリティの向上を図る。

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により、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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、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

上記６、７及び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。

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。

１１情報セキュリティポリシーに関する違反への対応

情報セキュリティポリシーに違反した職員等及びその監督責任者は､その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分等の対象とする。

１２情報セキュリティポリシーの公開

情報セキュリティ基本方針は公開とするが、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本市の行政運営、情報セキュリティの維持に支障を及ぼすおそれがあることから非公開とする。

附　則

1　この基本方針は、平成２３年７月１日から施行する。

2　綾瀬市情報セキュリティポリシー（平成１６年３月１日施行）は、廃止する。

附　則

１　この基本方針は、令和８年３月１９日から施行する。