日立市情報セキュリティ基本方針

デジタル推進課

令和元年１２月策定

（令和８年３月改定）

＜目　次＞

１　目的

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

本方針及び別に定める情報セキュリティ対策基準（以下「対策基準」という。）において掲げる用語の意義は次のとおりとする。

(1)　ネットワーク

多数のコンピュータや情報機器が、相互にデータのやり取りを行うことができる通信環境のことをいう。

(2)　情報システム

コンピュータやネットワークで構成され、業務を遂行するために構築された情報処理の仕組みをいう。

(3)　情報資産

情報システムを構成する機器及び情報システムで取り扱う全ての情報をいう。

（外部記憶媒体及び情報システムから印刷した文書を含む。）

(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)　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保持することをいう。

(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保持することをいう。

(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せることなく、情報にアクセスできる状態を保持することをいう。

(8)　基幹系（マイナンバー利用事務系）

個人番号を取り扱う事務又は戸籍事務等の個人情報を取り扱う情報システム及びそのネットワークをいう。

(9)　情報系（ＬＧＷＡＮ接続系）

職員が事務に利用するイントラ、人事給与、財務会計等の情報システム及びそのネットワークをいう。

(10)　インターネット系

インターネットに接続された情報システム及びそのネットワークをいう。（インターネット仮想接続は除く。）

(11) 脅威

情報セキュリティを阻害する要因をいう。

(12) 情報セキュリティインシデント

脅威により発生した情報セキュリティに対する侵害や、情報システム又はネットワークの故障等、情報資産が損なわれた状態又は損なわれる可能性が高い状態をいう。

(13) 情報セキュリティポリシー

本方針及び情報セキュリティ対策基準をいう。

3　情報セキュリティ対策基準の策定

本方針で規定する情報セキュリティ対策を実施するため、具体的な遵守事項及び基準等を定める情報セキュリティ対策基準を策定する。

4　情報セキュリティ対策実施手順の策定

情報資産に対するセキュリティ侵害が発生した場合に迅速かつ適切に対応するため、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対策実施手順を策定する。

なお、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。

5　対象とする脅威

情報資産に対する脅威として以下を想定し、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物理的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、詐取、内部不正

(2)　情報セキュリティポリシー違反

(3)　設計・開発の不備、プログラム上の欠陥、操作・設定ミス、管理の不備、外部委託先の契約違反、機器の故障

(4)　地震、落雷、火災等の災害によるサービス及び業務の停止

(5)　電力供給の途絶、通信の途絶等のインフラ障害によるサービス及び業務の停止

6　適用範囲

本方針は、市長部局、教育委員会、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、企業局、消防本部、議会及び議会事務局が保有する情報資産を取り扱う全ての職員に適用する。

７　職員の遵守義務

職員は、情報セキュリティの重要性について共通の認識を持ち、常に情報セキュリティポリシーを遵守しなければならない。

８　情報セキュリティ対策の概要

上記３で示した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ずる。

(1)　組織体制の確立

本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)　情報セキュリティインシデント対応

情報セキュリティインシデントが発生した際に組織的に対応する体制を確立する。

(3)　物理的セキュリティ対策

職員のパソコン、通信回線、サーバ室等の管理について、物理的なセキュリティ対策を講ずる。

(4)　人的セキュリティ対策

情報セキュリティに関し、職員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ずる。

(5)　技術的セキュリティ対策

情報システムの管理、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ずる。

(6)　運用における情報セキュリティ対策

情報システム及びログの監視、情報セキュリティポリシーの遵守状況の確認、例外措置、違反時の対応等、運用面の対策を講ずるものとする。

(7)　外部サービスの利用

情報システムの構築を外部委託する場合は、情報セキュリティ要件を明記した契約を締結し、外部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なければならない。

(8)　評価・見直し

本方針の遵守状況を検証するため、定期的に自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。また、必要に応じて情報セキュリティポリシー及び実施手順の見直しを行う。