上尾市情報セキュリティ基本方針

（平成２１年２月２７日
市　　長　　決　　裁）

情報セキュリティ基本方針（平成１５年８月４日市長決裁）の全部を改正する。

目次

上尾市が取り扱う情報資産には、市民の個人情報を始めとして行政運営上重要な情報など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情報が多数含まれている。したがって、情報資産、情報資産を取り扱うネットワーク及び情報システムを人的脅威や災害、事故等から防御することは、市民の財産、プライバシー等を守るためにも、また、安全かつ安定的な行政サービスを確保するためにも必要不可欠であり、このことが上尾市に対する市民からの信頼向上に寄与するものである。また、情報通信技術の進歩と情報ネットワークの発達による市行政システムの電子化への期待に応えていくためにも、全てのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。このため、上尾市の情報資産の機密性、完全性及び可用性を維持するための対策を整備するために、情報セキュリティポリシーを定めることとし、情報セキュリティの確保に最大限取り組むこととする。

第１章　総則

（目的）

第１条　この上尾市情報セキュリティ基本方針（以下「方針」という。）は、上尾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、上尾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。

（定義）

第２条　方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(1)　情報　文書、図面、写真、図書、それらが表示された画面及び記録媒体に記録したデータ並びに業務遂行上必要な事実、概念及び指示をいう。

(2)　情報資産　情報システム並びに情報システムの開発及び運用に係るすべての情報をいう。

(3)　情報システム　ハードウェア、ソフトウェア、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。

(4)　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をいう。

(5)　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により、情報資産を脅威から保護し、危険のない、不安のない、安全な状態に維持することをいう。

(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、認められた範囲内の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)　情報セキュリティポリシー　方針及び情報セキュリティ対策基準で構成され、情報資産の情報セキュリティ対策について総合的、体系的かつ具体的に明記されたものをいう。

(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その情報システムで取り扱うデータをいう。

(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　電子メール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。

(13)　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。

(14)　無害化通信　電子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。

（情報セキュリティポリシーの体系図）

第３条　情報セキュリティポリシーの体系図は、別図のとおりとする。

第２章　この方針が対象とする範囲

（対象とする脅威）

第４条　情報資産に対する脅威は、次の各号に掲げる要因の区分に応じ、当該各号に定めるものする。

(1)　意図的な要因　サイバー攻撃（不正アクセス、ウィルス攻撃、サービス不能攻撃等をいう。）及び部外者の侵入等による情報資産の漏えい、破壊、改ざん又は消去、重要情報の詐取、内部不正等

(2)　非意図的な要因　情報資産の無断持ち出し、紛失又は置き忘れ、無許可のソフトウェアの使用等の規定違反、設計又は開発の不備、プログラム上の欠陥、メンテナンスの不備、内部又は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、操作又は設定のミス、機器の故障等による情報資産の漏えい、破壊、改ざん、消去等

(3)　災害による要因　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)　疾病による要因　大規模かつ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)　インフラによる要因　電力若しくは水道の供給又は通信の途絶等のインフラの障害からの波及等

（機関の範囲）

第５条　方針が適用される機関は、次に掲げるものとする。

(1)　市長

(2)　教育委員会（教育委員会の所管に属する機関（上尾市立学校設置条例（昭和３９年３月３０日上尾市条例第１１号）に規定する小学校及び中学校に限る。）を除く。）

(3)　選挙管理委員会

(4)　公平委員会

(5)　監査委員

(6)　農業委員会

(7)　固定資産評価審査委員会

(8)　水道事業の管理者の権限を行う市長

(9)　消防長

(10)　議会

（情報資産の範囲）

第６条　方針が対象とする情報資産は、次に掲げるものとする。

(1)　ネットワーク、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、ネットワーク図等のシステム関連文書

第３章　情報セキュリティ対策

（職員の遵守義務）

第７条　第５条各号に掲げる行政機関に所属する一般職の職員、特別職の職員（議員及び消防団員を除く。）、会計年度任用職員、臨時的任用職員及び再任用職員（次条においてこれらを単に「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ち、情報資産の利用に当たっては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。

（情報セキュリティ対策）

第８条　第４条各号に掲げる脅威から情報資産を保護するため、次の各号に掲げる情報セキュリティ対策の種類の区分に応じ、当該各号に定める対策を講ずるものとする。

(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)　情報資産の分類及び管理の対策　本市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

(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、端末から電磁的記録媒体を利用しない方法での情報の持ち出しや端末への多要素認証の導入等により、情報の流出を防ぐ。

イ　ＬＧＷＡＮ接続系においては、ＬＧＷＡＮ接続系の情報システムと、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、両環境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、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

(4)　物理的セキュリティの対策　サーバ、情報システム室、通信回線、パソコン等について、物理的な対策を講じる。

(5)　人的セキュリティの対策　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の対策　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)　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、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（クラウドサービス）の利用　業務委託を行う場合には、委託事業者を選定し、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基づき措置を講じる。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。また、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。

(9)　評価・見直し　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し、運用改善を行い、情報セキュリティの向上を図る。また、情報セキュリティポリシーの見直しが必要な場合は、適宜見直しを行う。

（情報セキュリティ対策基準の策定）

第９条　市長は、前条各号に掲げる対策を実現するため、情報セキュリティ対策を行うために必要となる基本的な要件を定めた情報セキュリティの対策となる基準を策定する。

（情報セキュリティ実施手順の策定）

第１０条　情報セキュリティ対策を確実に実施するため、情報セキュリティ対策基準に基づき、情報セキュリティ実施手順を策定する。

２　前項の情報セキュリティ実施手順は、公開することにより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。

第４章　情報セキュリティ監査等

（監査及び自己点検）

第１１条　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行う。

（情報セキュリティポリシーの見直し）

第１２条　前条の規定により情報セキュリティ監査及び自己点検を行った結果、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ものとする。

附　則

この方針は、決裁の日から施行する。

附　則（平成２３年２月８日市長決裁）

この方針は、決裁の日から施行する。

附　則（平成２７年１０月５日市長決裁）

この方針は、決裁の日から施行する。

附　則（令和３年７月１日市長決裁）

この方針は、決裁の日から施行する。

附　則（令和４年１１月２８日市長決裁）

この方針は、決裁の日から施行する。

附　則（令和８年３月１６日市長決裁）

この方針は、決裁の日から施行する。

別図（第３条関係）

情報セキュリティポリシー体系図