

小企情発第22号
小議発第211号
小選発第108号
小監発第58号
小農発第73号
小固審発第20号
小教学庶発第179号
小土公発第81号
令和8年3月31日

小金井市情報セキュリティ基本方針

目次

1 目的	… 1
2 定義	… 2
3 対象とする脅威	… 2
4 適用範囲	… 3
5 職員等の遵守義務	… 3
6 情報セキュリティ対策	… 3
7 自己点検及び情報セキュリティに関する監査の実施	… 4
8 情報セキュリティポリシーの見直し	… 4
9 情報セキュリティ対策基準の策定	… 4
10 情報セキュリティ実施手順の策定	… 5

1 目的

小金井市の各情報システムが取り扱う情報には、住民の個人情報のみならず行政運営上重要な情報等、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、情報資産や情報資産を取り扱うネットワーク及び情報システムを様々な脅威から防御することは、住民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが小金井市に対する住民からの信頼の維持向上に寄与するものである。

今後、各種手続のオンライン利用の本格化や情報システムの高度化等、電子自治体の推進を図るに当たり、住民生活等に重大な支障が生じないよう、全てのネットワーク及び情報システムが高度で確実な安全性を有することが不可欠な前提条件である。

本基本方針は、小金井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、小金井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とともに、総務省が策定した「地方公共団体におけるサイバーセキュリティを確保するための方針の策定又は変更に関する指針（案）」を踏まえて、小金井市のサイバーセキュリティを確保するための方針として定めるものである。

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及びその構成機器（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、情報処理を行う仕組みをいう。
- (3) 電子情報
電子化されたプログラム及びデータ（資料及び帳票を含み、職員個人が資料整理等のために作成した個人利用ファイルを除く。）をいう。
- (4) 電子情報資産
電子情報並びに電子情報を作成し、管理し、及び保護する上で必要とされる情報システムをいう。
- (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、地方税も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。
- (13) 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。
- (14) 情報セキュリティポリシー
本基本方針、小金井市電子情報資産の安全管理対策に関する規程（平成16年規程第1号）及び情報セキュリティ対策基準（平成16年4月策定）をいう。
- (15) 職員等
地方公務員法（昭和25年法律第261号）における一般職とする。ただし、小金井市の情報システムを使用する場合には、特別職も本基本方針の対象となる。

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) 職員等による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程違反、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) 行政機関の適用範囲

本基本方針が適用される行政機関は、小金井市情報公開条例（平成14年条例第31号）第2条第1号に規定する実施機関とする。ただし、小金井市教育情報セキュリティ基本方針（令和2年10月全面改訂）の適用範囲を除く。

(2) 情報資産の適用範囲

本基本方針が対象とする情報資産は、次のとおりとする。

- ① ネットワーク及び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

職員等は、情報資産に対する脅威への対応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及び10に定める情報セキュリティ実施手順等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) 情報資産の分類と管理

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実施する。

(3) 情報システム全体の強じん性の向上

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3段階の対策を講じる。

- ① 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。
- ② LGWAN接続系においては、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、両環境間で通信する場合には、無害化通信を実施する。

- ③ 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、都道府県及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等を実施する。
- (4) 物理的セキュリティ対策
サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、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) 運用面での対策
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、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) 業務委託及びクラウドサービスの利用に係る対策
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。
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 自己点検及び情報セキュリティに関する監査の実施

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、リスクを検討した上で、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から8までに示す対策等を実施するため、必要に応じて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ものとする。

なお、当該対策基準は、小金井市における情報セキュリティ対策の基準を定めるものであり、公にすることにより、小金井市行政の運営に重大な支障を及ぼすおそれがあることから、当該対策基準については、非公開とする。

10 情報セキュリティ実施手順の策定

上記9に定める情報セキュリティ対策基準を踏まえ、必要に応じて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、当該実施手順は、関連する情報システム等の情報セキュリティ対策を具体的かつ詳細に定めるものであり、公にすることにより、関連する業務の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。

付 則

本基本方針は、令和8年4月1日から施行する。