飯能市情報セキュリティポリシー

（情報セキュリティ基本方針）

令和８年３月

目　次

第１章　総則

１　策定の経緯

地方公共団体においては、情報セキュリティ対策を徹底するためには、対策を組織的に統一して推進することが必要となり、そのためには組織として意思統一し、明文化された文書を定める必要がある。

行政手続等における情報通信の技術の利用に関する法律（平成１４年法律第１５１号）第９条第１項では、「地方公共団体は、地方公共団体に係る申請、届出その他の手続における情報通信の技術の利用の促進を図るため、この法律の趣旨にのっとり、当該手続に係る情報システムの整備及び条例又は規則に基づく手続について必要な措置を講ずること」に努めなければならないと規定しており、条例等に基づく手続については、同法第８条第２項（安全性及び信頼性の確保）の趣旨にのっとり、地方公共団体は情報セキュリティポリシーの策定や見直しを行うことが求められている。

また、番号制度等の最新の制度に係るセキュリティ対策、例えば、情報提供ネットワークシステム等の技術的基準、「特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）」（令和２年５月２５日改正個人情報保護委員会）が示す安全管理措置等についても遵守しなければならない。

さらに、サイバーセキュリティ基本法第５条では、地方公共団体においてサイバーセキュリティに関する自主的な施策の策定と実施が責務規定として法定化され、これにより、情報セキュリティポリシーの未策定団体には策定が必須となり、策定済み団体においても、適時適切な見直しとそれを遵守することが重要となっている。

総務省では、地方公共団体における情報セキュリティポリシーの策定を推進するため、平成１３年３月３０日に「地方公共団体における情報セキュリティポリシーに関するガイドライン」を策定し、必要に応じ改定を行ってきた。

この度、令和２年５月２２日には、「クラウド・バイ・デフォルト原則」、行政手続のオンライン化、働き方改革、サイバー攻撃の増加といった新たな時代の要請や「三層の対策」の課題を踏まえた「自治体情報セキュリティ対策の見直しについて」が取りまとめられた。同取りまとめ及び平成３０年７月の政府機関の情報セキュリティ対策のための統一基準の改定等を踏まえて、令和２年１２月２８日にガイドラインが改訂された。

令和３年度には、「デジタル庁設置法」、「デジタル社会形成基本法」、「地方公共団体情報システムの標準化に関する法律」等のデジタル改革関連法が成立・施行され、国及び地方のデジタル・トランスフォーメーション（ＤＸ）が推し進められることとなった。これらの地方公共団体におけるデジタル化の動向や令和３年７月の政府機関のサイバーセキュリティ対策のための統一基準の改定を踏まえて、令和４年３月２５日にガイドラインが改訂された。

標準化法により、地方公共団体において、標準化基準（標準化法第６条第１項及び第７条第１項に規定する標準化のために必要な基準をいう。以下同じ。）に適合する基幹業務システム（以下「標準準拠システム」という。）の利用が義務付けられ、標準準拠システムについてガバメントクラウド（デジタル社会形成基本法第２９条に規定する「全ての地方公共団体が官民データ活用推進基本法第２条第４項に規定するクラウド・コンピューティング・サービス関連技術に係るサービスを利用することができるようにするための国による環境の整備」としてデジタル庁が整備するものをいう。以下同じ。）を利用することが努力義務とされた。

また、令和４年１０月に、標準化法第５条第１項に基づき、地方公共団体情報システムの標準化の推進を図るための基本的な方針として、「地方公共団体情報システム標準化基本方針」が閣議決定された。当該方針のサイバーセキュリティに係る事項において「地方公共団体が利用する標準準拠システム等の整備及び運用に当たっては、総務省が作成する地方公共団体における情報セキュリティポリシーに関するガイドラインを参考にしながら、セキュリティ対策を行うものとする。」とされたところである。なお、地方公共団体においては、クラウドサービス上での標準準拠システム等の整備及び運用を開始するまでに、第４編「地方公共団体におけるクラウド利用等に関する特則」に示された対策基準（例文及び解説）の内容を参考にセキュリティポリシーの見直しを行う必要があり、令和５年３月２８日に一部改定を行った。

令和５年度には、Web 会議等の目的で、LGWAN 接続系の業務端末からインターネット経由で、特定のクラウドサービスを安全に利用するための対策（アクセス制御等）、令和５年７月の政府機関のサイバーセキュリティ対策のための統一基準の改定を踏まえた業務委託先管理の強化、機密性分類基準の見直し、サイバーレジリエンスの強化等について、令和６年１０月２日に一部改定を行った。

令和６年５月には、「国・地方のネットワークの将来像及び実現シナリオに関する検討会」報告書において、国・地方のネットワークの将来像の例として、「国・

地方の職員が、セキュリティを確保しつつ、一人一台の端末で効率的に業務ができ、テレワーク等の柔軟な働き方が可能であること」が示され、令和６年地方分権改革に関する提案において、マイナンバー利用事務系への無線 LAN 接続等を可能とする具体的な対策の明示が求められた。

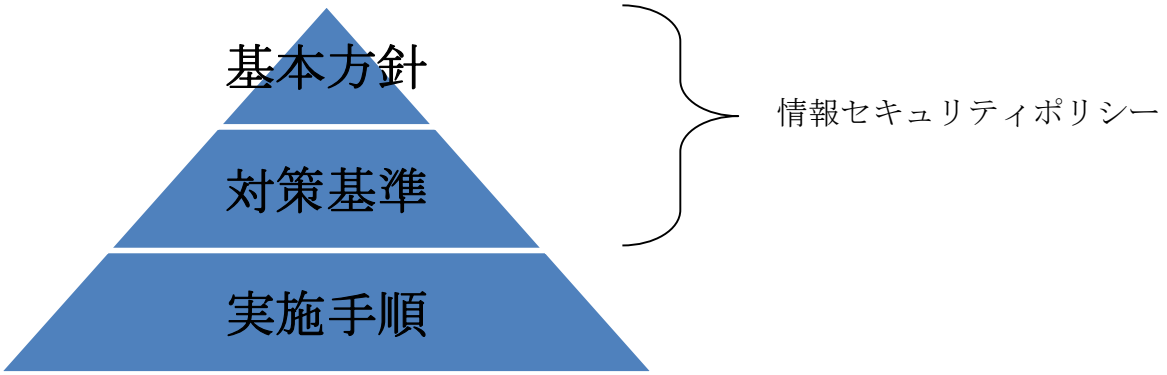
これらを受け、本市の飯能市情報セキュリティポリシーを改訂する。

２　情報セキュリティポリシーの構成

情報セキュリティポリシーの体系は、図１に示すとおりとする。

本市の情報セキュリティ対策における基本的な考え方を定めるものを「基本方針」とし、この基本方針に基づき、全ての情報システムに共通の情報セキュリティ対策の基準を定めたものを「対策基準」とする。この「基本方針」と「対策基準」を総称して「情報セキュリティポリシー」という。また、「対策基準」を、具体的なシステムや手順、手続に展開して個別の実施事項を定めるものを「実施手順」という。

図 1



第２章　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）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

本基本方針及び情報セキュリティ対策基準をいう。

（５）行政情報

行政情報とはポリシーで定める行政機関の職員が職務上作成し、又は取得した文書、図画及び電磁的記録(電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。)であって、当該行政機関の職員が組織的に用いるものとして、当該実施機関が保有しているものをいう。

（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）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。

(10) 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。）。

(11) 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(議場等で議会に関わる資料を閲覧するための議会ネットワークも含む。)。

(12) 学校ネットワーク

教育委員会、各学校で使用する校務支援システム用ネットワーク、GIGAスクール用ネットワークをいう。文部科学省から教育情報セキュリティポリシーに関するガイドラインが別途示されている。

(13) 医療系ネットワーク

市医療機関等（南高麗診療所など）において使用する患者情報を含む医療情報を扱うネットワークをいう。厚生労働省から医療情報システムの安全管理に関するガイドラインが別途示されている。

(14) 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。

(15) 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）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）行政機関の範囲

本基本方針が適用される行政機関は、市長部局、教育委員会（幼稚園、小学校及び中学校を含む。）、議会事務局（議会を含む。）、選挙管理委員会、監査委員事務局、公平委員会、農業員会事務局、固定資産評価審査委員会及び地方公営企業（以下「行政機関」という。）とする。

ただし、学校ネットワーク、医療系ネットワークなど所管省庁のガイドラインがあるものについては対象外とする。

（２）情報資産の範囲

本基本方針が対象とする情報資産は、行政情報のうち次のとおりとする。

ただし、行政情報を取り扱わない職員が個人的に保有する情報システム及びそこで取り扱う情報等については対象外とする。

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（会計年度任用職員、特別職、非常勤特別職を含む。）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

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

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。

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。

②LGWAN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、両システム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

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

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

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、利用にかか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。

（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。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

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ものとする。

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。