伊那市情報セキュリティ基本方針

令和８年４月１日

伊那市情報セキュリティ委員会・伊那市議会・伊那市教育委員会

・伊那市選挙管理委員会・伊那市公平委員会・伊那市監査委員

・伊那市農業委員会・伊那市固定資産評価審査委員会

（目的）

第１条　この方針は、市が管理する市民の個人情報をはじめとした情報資産の機密性、完全性及び可用性を維持するため、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により、市民に信頼される行政運営を推進することを目的とする。なお、当該基本方針は、地方自治法（昭和 22 年法律第 67 号）第 244 条の６第１項に規定するサイバーセキュリティを確保するための方針として位置付けるものとする。

（定義）

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

(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

コンピュータ等で構成され、情報処理を行う仕組みをいう。

(3) システム関連文書

情報システムの仕様書及びネットワーク図等をいう。

(4) 情報

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。）並びにシステム関連文書をいう。

(5) 情報資産

情報並びにネットワーク、情報システム、これらに関する設備及び電磁的記録媒体をいう。

(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) 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。

(10) 職員

地方公務員法（昭和 25 年法律第 261 号）に規定された特別職及び一般職に属する地方公務員のうち、市に勤務する者をいう。

(11) 関係機関の職員等

行政委員会事務局、議会事務局及び各施設等に勤務し、又は市が管理する情報資産を利用する者をいう。

(12) 職員等

職員及び関係機関の職員等（それぞれ再任用職員、任期付職員、会計年度任用職員及び特別職等を含む。）をいう。

(13) 外部委託事業者

業務委託先等（地方自治法（昭和22年法律第67号）第244条の２第３項に規定する指定管理者を含む。）、契約等に基づき市の管理する情報資産の取扱いを含む業務等に従事する者（再委託等により当該業務等に従事する者を含む。）をいう。

(14) 部外者

職員等及び外部委託事業者以外の者で、市の管理する情報資産に接することが認められていないものをいう。

(15) 不正アクセス

不正アクセス行為の禁止等に関する法律（平成11年法律第128号）第３条第２項に規定する不正アクセス行為その他の不正な手段により行うアクセス（権限外のアクセスを含む。）をいう。

(16) 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。

(17) 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。）。

(18) 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。

(19) 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。

(20) 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。

（情報セキュリティポリシー）

第３条　情報セキュリティポリシーは、この方針及び第12条に定める情報セキュリティ対策基準により構成され、情報セキュリティ対策の頂点に位置するものとする。

（情報セキュリティポリシーの適用範囲）

第４条　情報セキュリティポリシーの適用範囲は、次の各号に定めるところによる。

(1) 情報資産の範囲

市が管理するすべての情報資産とする。ただし、小中学校においては、事務室の情報資産とする。

(2) 対象者の範囲

前号に定める情報資産に接するすべての職員等及び外部委託事業者とする。

（職員等の遵守義務）

第５条　職員等は、情報セキュリティの重要性について共通の認識を持ち、関係法令、情報セキュリティポリシー及び第 13 条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。

２　職員等は、外部委託事業者において必要な情報セキュリティ対策が確保されることを、確実にしなければならない。

（情報セキュリティ管理体制）

第６条　情報資産について、適切な情報セキュリティ対策を推進するために、全庁的な体制を確立するものとする。

（情報資産の分類）

第７条　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ものとする。

（情報資産への脅威）

第８条　情報資産に対する脅威として、次のものを想定する。

(1) 次に掲げる意図的な要因による情報資産の漏えい、破壊、改ざん及び消去、重要情報の詐取、内部不正等

ア　サイバー攻撃をはじめとする部外者の情報システムへの侵入

イ　不正アクセス

ウ　ウイルス攻撃及びサービス不能攻撃

(2) 次に掲げる非意図的な要因による情報資産の漏えい、破壊、消去等

ア　情報資産の無断持ち出し

イ　無許可ソフトウェアの使用等の規定違反

ウ　情報システムの設計及び開発の不備

エ　プログラム上の欠陥

オ　誤操作及び誤設定

カ　メンテナンスの不備

キ　内部及び外部監査機能の不備
ク　外部委託管理の不備
ケ　マネジメントの欠陥
コ　機器の故障

(3)　次に掲げる要因によるサービス及び業務の停止等
ア　地震、落雷、火災等の災害
イ　電力供給、通信及び水道供給の途絶
ウ　要員不足に伴うシステム運用の機能不全
エ　事故
オ　機器の故障
カ　大規模で広範囲な疾病の流行等

（情報セキュリティ対策）

第９条　情報資産を前条の脅威から保護するために、次の情報セキュリティ対策を講じるものとする。

(1) 組織及び情報資産の分類と管理

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とともに、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。

(2) 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、業務の効率性及び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。

イ　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、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。

(3) 物理的セキュリティ対策

情報資産の管理について、物理的な対策を講じる。

(4) 人的セキュリティ対策

情報セキュリティに関し、職員等及び外部委託事業者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。

(5) 技術的セキュリティ対策

情報資産の管理、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な対策を講じる。

(6) 運用面のセキュリティ対策

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、業務委託を行う際のセキュリティ確保等、運用面の対策を講じる。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。

(7) 業務委託と外部サービス（クラウドサービス）の利用対策

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。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のアカウントごとに責任者を定める。

(8) 評価及び見直し

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。

（情報セキュリティ監査及び自己点検の実施）

第 10 条　情報セキュリティポリシーが遵守されていることを検証するため、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。

（情報セキュリティポリシーの見直し）

第 11 条　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となった場合には、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。

（情報セキュリティ対策基準の策定）

第 12 条　第 9 条、第 10 条及び前条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ものとする。

２　情報セキュリティ対策基準は、各組織の情報システムの状況等を踏まえて必要に応じて組織ごとに個別に策定する。ただし、各組織の特性に応じて組織間合同で策定することを妨げない。

３　情報セキュリティ対策基準は、公にすることにより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。

（情報セキュリティ実施手順の策定）

第 13 条　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。

２　情報セキュリティ実施手順は、公にすることにより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。