甲州市情報セキュリティポリシー

平成 18 年　8 月　3 日 策定

平成 20 年全部改訂

平成 25 年一部改定

平成 28 年　3 月一部改定

令和元年 9 月一部改定

令和 8 年 3 月一部改定

甲州市情報セキュリティ委員会

第1章　情報セキュリティ基本方針

1 目的

甲州市の各情報システムが取扱う情報には、市民の個人情報、行政運営上重要な情報など、外部への漏洩、消失、破壊、改竄、情報システムの停止等が発生した場合、極めて重大な結果を招くものが含まれている。

これらの情報及び情報を取り扱うシステムを様々な脅威から防御することは、事務の安定的な運営を図り、市民の財産、プライバシー等を守るため不可欠である。

また、情報技術の進歩にともない、より高度で広範囲な行政の情報化が進められている。

甲州市がこれに対応していくためには、全ての情報システムの運用に対して十分な安全性を維持していくことが求められる。

この要求に答えるため、甲州市職員等が情報資産を安全に取り扱うための規範である甲州市情報セキュリティポリシーを定める。

甲州市情報セキュリティポリシーは、これを職員等に浸透、普及、定着を図ることにより、取り扱われる情報資産の安全性を高め、市民からの信頼の維持向上に寄与するためのものである。

2 定義

(1) ネットワーク

甲州市における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（ハードウエア及びソフトウエア）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、情報の各種処理を行う仕組みをいう。

(3) 情報資産

ネットワーク及び情報システムの開発と運用に係る全ての情報並びにネットワーク及び情報システムで取り扱う全ての情報（印刷した文書も含む。）をいう。

(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) 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。

(6) 機密性

情報にアクセスを認可された者だけが、アクセスできる状態を確実にすることをいう。

(7) 完全性

情報が、故意、過失、災害などで改ざんされたり、破壊されたりしない状態を確実にすることをいう。

(8) 可用性

認可された利用者が、必要なときに中断されることなく、情報及び関連する資産にアクセスできる状態を確実にすることをいう。

(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。

(12) 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。

(13) 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、コンピュータウィ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

情報資産への脅威は、情報を取り扱う環境に広く存在し、その形態も多様であるうえ、新たな種類の脅威が発生する場合もあるので、脅威の存在やその影響を常に監視するように努める。

本情報セキュリティポリシー策定時に特に考慮した、注意すべき脅威は以下のとおりである。

(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･盗聴･改ざん･消去、重要情報の詐

取、内部不正等

⑵ 情報資産の無断持出、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

⑶ 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

⑷ 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

⑸ 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

⑴ 行政機関の範囲

本セキュリティポリシーが適用される行政機関は、市長部局、教育委員会、行政委員会、議会、議会事務局及び地方公営企業とする。

⑵ 情報資産の範囲

本セキュリティポリシー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

情報セキュリティポリシーは、甲州市が所掌する情報資産に関する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取りまとめたものであり、情報セキュリティ対策の頂点に位置する。

甲州市長をはじめ、甲州市が所掌する情報資産に関する業務に携わる全ての職員等及び外部委託事業者は、情報セキュリティの重要性について共通の認識をもつとともに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じる。

⑴ 組織体制

甲州市の情報資産について、情報管理対策を推進・管理するための全庁的な体制を確立する。

⑵ 情報資産の分類と管理

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。

⑶ 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て、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。

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を導入する。

⑷ 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。

⑸ 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。

⑹ 技術的セキュリティ対策

コンピュータの管理、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。

⑺ 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。また、情報資産への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、緊急時対応体制を策定する。

⑻ 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、利用に係る文書等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方針等を定め、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。

⑼ 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が遵守されていることを検証するために、必要に応じて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見直し

情報セキュリティ監査及び自己点検の結果により、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を取り巻く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

甲州市の様々な情報資産について、上記6，7及び8に規定する対策等を実施するために、具体的な順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。

なお、情報セキュリティ対策基準は、公にすることにより甲州市の行政運営に支障を及ぼす恐れのある情報資産であることから非公開とする。

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。

なお、情報セキュリティ実施手順は、公にすることにより甲州市の行政運営に重大な支障を及ぼす恐れのある情報資産であることから非公開とする。