

平川市情報セキュリティポリシー

平成18年11月28日 策定

平成26年11月19日 一部改正

平成29年 9月 8日 一部改正

令和 3年 7月29日 一部改正

令和 4年 4月 1日 一部改正

令和 5年 1月23日 一部改正

平川市情報セキュリティ委員会

序 文

本市は、ICTを重要な社会の基盤として捉え、これを利用した情報化を推進することにより、電子自治体の構築を目指している。

情報化を推進し、電子自治体を構築するにあたっては、保有する情報を不正なアクセス、情報の漏えい・改ざん等の脅威から防御し、高度な健全性を有した情報システムを構築していかなければならない。

このような状況を踏まえ、本市は、保有する情報及び情報システムに関するセキュリティ対策を総合的、体系的かつ具体的に規定した平川市情報セキュリティポリシーを策定することとした。

平川市情報セキュリティポリシーについては、本市の全ての職員等及び委託事業者がその内容を十分理解した上で、各業務において率先して遵守すべきものであるため、安定的な規範であることが要請される一方、情報の処理技術や通信技術等の進展に伴う急速な状況の変化に柔軟に対応できることも必要とされる。

このようなことから、平川市情報セキュリティポリシーは、規範性を有する「情報セキュリティ基本方針」、情報及び情報システムを取り巻く状況変化に応じ、随時適切な見直しを行う「情報セキュリティ対策基準」により構成し、またそれらに基づいて情報システムごとに職員等が従うべき具体的な手順を「情報セキュリティ実施手順」に定めるものとする。

情報セキュリティポリシーの構成

文書名		内容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一かつ基本的な方針。
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準。
情報セキュリティ実施手順		ネットワーク及び情報システムごとに定める情報セキュリティ対策基準に基づいた具体的な実施手順。

第1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

情報セキュリティポリシーにおける用語の意義は、次の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、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、ソフトウェア、ネットワーク及び記録媒体で構成され、情報の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) 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。

(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。

(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。

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な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、内部部局、行政委員会、議会事務局、診療所とする。

(2) 情報資産の範囲

本基本方針が対象とする情報資産は、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、会計年度任用職員等（以下、「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、業務の遂行にあ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靱性の向上

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。

- 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

サーバ等、情報システム室等、通信回線等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。

ソーシャルメディアを含む外部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。

(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、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。

第2章 情報セキュリティ対策基準

1 趣旨

情報セキュリティ対策基準（以下「対策基準」という。）は、「情報セキュリティ基本方針」を実現するため、本市の職員等が個々に行う対策を具体化し、遵守すべき情報セキュリティの基準に関し、必要な事項を定めるものとする。

2 対象範囲

対策基準が適用される行政機関及び情報資産の対象範囲をこの項で定める。

- (1) 行政機関の範囲
- (2) 情報資産の範囲

3 組織体制

対策基準のうち、情報セキュリティの推進及び向上、また、非常時の連絡体制にかかる組織体制と、各組織の役割をこの項で定める。

- (1) 最高情報セキュリティ責任者
- (2) 統括情報セキュリティ責任者
- (3) 情報セキュリティ責任者
- (4) 情報セキュリティ管理者
- (5) 情報システム管理者
- (6) 情報システム担当者
- (7) 情報セキュリティ委員会
- (8) 兼務の禁止
- (9) CSIRT の設置・役割

4 情報資産の分類と管理方法

対策基準のうち、行政情報や記録媒体などの情報資産の分類と取扱いをこの項で定める。

- (1) 情報資産の分類
- (2) 情報資産の管理

5 情報システム全体の強靱性の向上

対策基準のうち、マイナンバー利用事務系、LGWAN 接続系、インターネット接続系の三層分離に関する取扱いについて必要な事項をこの項で定める。

- (1) マイナンバー利用事務系
- (2) LGWAN 接続系
- (3) インターネット接続系

6 物理的セキュリティ

対策基準のうち、情報セキュリティ確保のための設備、環境及び機器の取扱いについて必要な事項をこの項で定める。

6-1 サーバ等の管理

- (1) 機器の取付け
- (2) サーバの冗長化
- (3) 機器の電源
- (4) 通信ケーブル等の配線
- (5) 機器の定期保守及び修理
- (6) 庁外への機器の設置
- (7) 機器の廃棄等

6-2 管理区域（サーバー室等）の管理

- (1) 管理区域の構造等
- (2) 管理区域の入退室管理等
- (3) 機器等の搬入出

6-3 通信回線及び通信回線装置の管理

6-4 職員等の利用する端末や電磁的記録媒体等の管理

7 人的セキュリティ

対策基準において、職員が服務上遵守すべき事項をこの項で定める。

7-1 職員等の遵守事項

- (1) 職員等の遵守事項
- (2) 会計年度任用職員等への対応
- (3) 情報セキュリティポリシー等の掲示
- (4) 委託事業者に対する説明

7-2 研修・訓練

- (1) 情報セキュリティに関する研修・訓練
- (2) 研修の計画及び実施
- (3) 緊急時対応訓練
- (4) 研修・訓練への参加

7-3 情報セキュリティインシデントの報告

- (1) 庁内での情報セキュリティインシデントの報告
- (2) 住民等外部からの情報セキュリティインシデントの報告
- (3) 情報セキュリティインシデント原因の究明・記録、再発防止等

7-4 ID及びパスワード等の管理

- (1) ICカード等の取扱い
- (2) IDの取扱い
- (3) パスワードの取扱い

8 技術的セキュリティ

対策基準においてセキュリティを高めるために機器に施す措置、システムの開発、通信制御等について必要な事項をこの項で定める。

8-1 コンピュータ及びネットワークの管理

- (1) ファイルサーバの設定等
- (2) バックアップの実施
- (3) 他団体との情報システムに関する情報等の交換
- (4) システム管理記録及び作業の確認
- (5) 情報システム仕様書等の管理
- (6) ログの取得等
- (7) 障害記録
- (8) ネットワークの接続制御、経路制御等
- (9) 外部の者が利用できるシステムの分離等
- (10) 外部ネットワークとの接続制限等
- (11) 複合機のセキュリティ管理
- (12) IoT 機器を含む特定用途機器のセキュリティ管理
- (13) 無線 LAN 及びネットワークの盗聴対策
- (14) 電子メールのセキュリティ管理
- (15) 電子メールの利用制限
- (16) 電子署名・暗号化
- (17) 無許可ソフトウェアの導入等の禁止
- (18) 機器構成の変更の制限
- (19) 業務外ネットワークへの接続の禁止
- (20) 業務以外の目的でのウェブ閲覧の禁止
- (21) Web 会議サービスの利用時の対策
- (22) ソーシャルメディアサービスの利用

8-2 アクセス制御

- (1) アクセス制御
- (2) 職員等による外部からのアクセス等の制限
- (3) 自動識別の設定
- (4) ログイン時の表示等
- (5) 認証情報の管理
- (6) 特権による接続時間の制限

8-3 システム開発、導入、保守等

- (1) 情報システムの調達
- (2) 情報システムの開発
- (3) 情報システムの導入
- (4) システム開発・保守に関連する資料等の整備・保管
- (5) 情報システムにおける入出力データの正確性の確保

- (6) 情報システムの変更管理
- (7) 開発・保守用のソフトウェアの更新等
- (8) システム更新又は統合時の検証等

8-4 不正プログラム対策

- (1) 統括情報セキュリティ責任者の措置事項
- (2) 情報システム管理者の措置事項
- (3) 職員等の遵守事項
- (4) 専門家の支援体制

8-5 不正アクセス対策

- (1) 統括情報セキュリティ責任者の措置事項
- (2) 攻撃への対処
- (3) 記録の保存
- (4) 内部からの攻撃
- (5) 職員等による不正アクセス
- (6) サービス不能攻撃
- (7) 標的型攻撃

8-6 セキュリティ情報の収集

- (1) セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等
- (2) 不正プログラム等のセキュリティ情報の収集・周知
- (3) 情報セキュリティに関する情報の収集及び共有

9 運用

対策基準を運用するにあたり、通常業務時、セキュリティ侵害や緊急時の対応、外部委託時の対応において、必要な事項をこの項で定める。

9-1 情報システムの監視

9-2 情報セキュリティポリシーの遵守状況の確認

- (1) 遵守状況の確認及び対処
- (2) パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査
- (3) 職員等の報告義務

9-3 侵害時の対応等

- (1) 緊急時対応計画の策定
- (2) 緊急時対応計画に盛り込むべき内容
- (3) 業務継続計画との整合性確保
- (4) 緊急時対応計画の見直し

9-4 例外措置

- (1) 例外措置の許可
- (2) 緊急時の例外措置
- (3) 例外措置の申請書の管理

9-5 法令遵守

9-6 懲戒処分等

- (1) 懲戒処分
- (2) 違反時の対応

10 業務委託と外部サービスの利用

対策基準を運用するにあたり、業務委託と外部サービスの利用について、必要な事項をこの項で定める。

10-1 業務委託

- (1) 委託事業者の選定基準
- (2) 契約項目
- (3) 確認・措置等
- (4) 再委託等

10-2 外部サービスの利用

11 評価・見直し

対策基準の評価、見直しにかかる事項をこの項で定める。

11-1 監査

- (1) 実施方法
- (2) 監査を行う者の要件
- (3) 監査実施計画の立案及び実施への協力
- (4) 委託事業者に対する監査
- (5) 報告
- (6) 保管
- (7) 監査結果への対応
- (8) 情報セキュリティポリシー及び関係規程等の見直し等への活用

11-2 自己点検

- (1) 実施方法
- (2) 報告
- (3) 自己点検結果の活用

11-3 情報セキュリティポリシー及び関係規程等の見直し