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

平川市情報セキュリティ委員会

序 文

平川市は、ＩＴ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、平川市の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、平川市は、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、平川市の全職員がその内容を十分理解した上で、各職場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が従うべき具体的手順を「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的かつ基本的な方針。
	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 趣旨

情報セキュリティ基本方針は、平川市（以下「本市」という。）の情報資産の機密性、完全性及び可用性を維持するために必要な、情報セキュリティポリシーの対象、適用範囲等情報セキュリティ対策に関する基本的な事項を定めるものとする。

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（ハードウエ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）情報資産

情報システムで取扱うすべての情報をいう。なお、情報資産は紙等の有体物に出力された情報も含むものとする。

（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）脅威

自然災害、悪意のある行為等情報資産に被害を与える要因をいう。

(10) 職員等

本市に在職する正職員、非常勤職員及び臨時職員をいう。

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 部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃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、プログラム上の欠陥、操作ミス、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 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、情報システム及びこれらに関する設備、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行う。

（3）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。

（4）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。

（5）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。

（6）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、外部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、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

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。

11 情報セキュリティポリシーの公開

情報セキュリティポリシーには、公開することにより本市の行政運営に重大な支障を及ぼす恐れがある内容が含まれることから、情報セキュリティ基本方針及び情報セキュリティ対策基準の概要についてのみ公開するものとし、情報セキュリティ対策基準の全文及び情報セキュリティ実施手順については公開しないものとする。

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）電子計算機管理運営委員会
（９）兼務の禁止
(10) 情報セキュリティに関する統一的な窓口の設置

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 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。

５－１ サーバ等の管理

（１）機器の取付け
（２）サーバの二重化
（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）敷地外への機器の設置
（７）機器の廃棄等

５－２ 管理区域（電算室等）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

５－３ 通信回線及び通信回線装置の管理

５－４ 職員等のパソコン等の管理

６ 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。

６－１ 職員等の遵守事項
（１）職員等の遵守事項
（２）非常勤及び臨時職員への対応
（３）情報セキュリティポリシー等の掲示
（４）外部委託事業者に対する説明

６－２ 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

６－３ 事故、欠陥等の報告
（１）庁内からの事故等の報告
（２）住民等外部からの事故等の報告
（３）事故等の分析・記録等

６－４ ＩＣカード及びＩＤ・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

７ 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装置、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。

7－1 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）アクセス記録の取得等
（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) 無線LAN の盗聴対策
(12) 電子メールのセキュリティ管理
(13) 電子メールの利用制限
(14) 電子署名・暗号化
(15) 無許可ソフトウェアの導入等の禁止
(16) 機器構成の変更の制限
(17) 無許可でのネットワーク接続の禁止
(18) 業務以外の目的でのウェブ閲覧の禁止

7－2 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）パスワードに関する情報の管理
（6）特権による接続時間の制限

7－3 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

7－4 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

７－５ 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）攻撃の予告
（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

７－６ 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

８　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。

８－１ 情報システムの監視

８－２ 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）端末及び記録媒体等の利用状況調査
（３）職員等の報告義務

８－３ 侵害時の対応

（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）緊急時対応計画の見直し

８－４ 外部委託

（１）外部委託先の選定基準
（２）契約項目
（３）確認・措置等

８－５ 例外措置

（１）例外措置の許可
（２）緊急時の例外措置

８－６ 法令遵守

８－７ 懲戒処分等

（１）懲戒処分

（２）違反時の対応

９　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。

９－１ 監査

（１）実施方法

（２）監査実施計画の立案及び実施への協力

（３）報告

（４）保管

（５）監査結果への対応

（６）情報セキュリティポリシーの見直し等への活用

９－２ 自己点検

（１）実施方法

（２）報告

（３）自己点検結果の活用