〈　目　　次　〉

序　札幌市情報セキュリティポリシーの構成

札幌市情報セキュリティポリシー（以下「ポリシー」という。）は、札幌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る。

ポリシーは、札幌市が所掌する情報資産に携わる職員、委託事業者等にも浸透、普及、定着されるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、ポリシーは一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と情報資産を取巻く状況の変化に依存する部分「情報セキュリティ対策基準」の２層に分けて構成する。（下表参照）

札幌市情報セキュリティポリシーの構成

文　書　名		内　容
札幌市 情報セキュリティポリシー	情報セキュリティ基本方針	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すべ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

第１章　情報セキュリティ基本方針

１　目的

本市は、市民生活を豊かにするまちづくりのために情報化を推進しているところである。しかし、情報活用の一方で、各情報システムが取り扱う情報には、市民の個人情報のみならず行政運営上重要な情報など、外部への漏えい等が発生した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、取り扱う情報を様々な脅威から防御することは、市民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが本市に対する市民からの信頼の維持向上に寄与するものである。

また、近年いわゆるＩＴ革命の進展により、電子商取引の発展や電子自治体の構築が現実のものとなっている。本市が電子自治体を構築するためには、すべてのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

本市は、市民が安心・信頼して行政サービスを利用することができるようにするとともに、本市における継続的かつ安定的な行政事務の執行を確保するために、情報資産の機密性、完全性及び可用性(注)を維持するための対策（情報セキュリティ対策）を整備するものである。

(注)：国際標準化機構（ＩＳＯ）が定めるもの(IS07498-2：1989)

機密性(confidentiality)：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

完全性（integrity）　：情報及び処理の方法の正確さ及び完全である状態を安全防御すること。

可用性(availability)　：許可された利用者が必要な時に情報にアクセスできることを確実にすること。

２　定義

⑴　情報セキュリティ

情報資産の機密の保持、正確性及び完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

⑵　ネットワーク

電子計算機等を相互に接続するための通信回線及びその構成機器（ハードウェア及びソフトウェア）をいう。

⑶　情報システム

電子計算機、ネットワーク、電磁的記憶媒体等により、情報処理を行う仕組みをいう。

⑷　情報資産

情報システムで取り扱うすべての電磁的データをいう。

⑸　住民基本台帳ネットワークシステム

電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準（平成 14 年総務省告示第 334 号）第１の１に規定する住民基本台帳ネットワークシステムをいう。

⑹　マイナンバー利用事務系

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をいう。

⑺　校務系情報

児童生徒の成績、出欠席、健康診断結果及び指導要録、教員の個人情報等、学校が所有する情報資産のうち、学校・学級の管理運営、学習指導、生徒指導及び生活指導等に活用することを想定しており、かつ、児童生徒がアクセスすることが想定されていないものをいう。

⑻　教育系情報

児童生徒のワークシート及び作品等、学校が所有する情報資産のうち、それら情報を学校における教育活動において活用することを想定しており、かつ当該情報に教員及び児童生徒がアクセスすることが想定されている情報をいう。

⑼　学校情報システム

校務系情報又は教育系情報を取り扱う情報システムをいう。

3　対象範囲

ポリシーは、本市のすべての執行機関（市長、教育委員会、選挙管理委員会、人事委員会、監査委員、農業委員会、固定資産評価審査委員会、公営企業管理者及び消防長）及び議会事務局を対象とする。ただし、学校情報システム及び当該システムで取り扱う情報資産については、対象から除く。

4　ポリシーの位置付け

ポリシーは、本市の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、情報セキュリティ管理の最上位の位置付けとする。

5　職員の責務

本市の情報資産に接するすべての職員（特別職、会計年度任用職員、非常勤職員及び臨時職員を含む。以下同じ。）は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たってポリシーを遵守する義務を負うものとする。

また、情報資産を取り扱う委託事業者等に対しても、契約を通じて、又は別途取り決めを行うことにより、ポリシーを遵守させるための措置を講じなければならない。

6　情報セキュリティ管理体制

本市の情報資産について、情報セキュリティ対策を推進し、管理するための組織・体制を確立し、その役割、責任等を定める。

情報セキュリティインシデント対応及び外部との情報共有を役割とした統一的な体制「ＣＳＩＲＴ（シーサート）」を構築する。

7　情報資産の分類

情報資産をその内容に応じて分類し、その重要性に応じた情報セキュリティ対策を行うものとする。

8　情報セキュリティに対する脅威

情報セキュリティに対する脅威とは、情報セキュリティを脅かす好ましからぬ事態及び事故をいう。特に認識すべき脅威は、次のとおりである。

⑴　意図的（計画的）な人為的脅威

故意の不正アクセス又は不正操作による機器又は情報資産の破壊、盗難、改ざん、消去、無断持ち出し、ソフトウェアのライセンス違反、ＡＰＴ攻撃等。

⑵　偶発的な人為的脅威

誤操作等によって起きる情報資産の破壊、漏えい、消去等及び搬送中の事故等による情報資産の盗難、漏えい、紛失等。

また、開発・設計・設定・メンテナンスの不備によるシステム障害や、委託先管理・マネジメントの欠如による情報資産の盗難、漏えい、紛失等。

⑶　環境的脅威

地震、落雷、火災、水害、停電、パンデミック（業務執行体制の維持が困難となるような大規模な感染症の流行）等の災害又は事故による情報資産の破壊、消失、サービス又は業務の停止等。

9　情報セキュリティ対策

情報セキュリティに対する脅威から本市の情報資産を保護するために次の対策を講ずる。

⑴　人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、十分な教育及び啓発により、すべての職員、委託事業者等にポリシーの内容を周知徹底するなど、守るべき行動基準及び判断基準を定める。

⑵　物理的セキュリティ対策

不正侵入又は盗難から情報資産を保護するために、管理区域の設置等情報資産への物理的なアクセスを制御するための対策を講ずる。

⑶　技術面及び運用面におけるセキュリティ対策

情報資産を外部又は内部からの不正アクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策及び委託等による情報システム開発・運用保守の基準、ポリシー遵守状況の確認等の運用面の対策を講ずる。

⑷　情報システム全体の強靭性の向上

本市における住民基本台帳ネットワークシステム及び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ための措置を講ずる。

⑸　管理区域以外への情報システム等の設置に係る規定の整備

外部委託によって管理区域外にシステム等の設置、情報資産の保存を行う場合、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、契約に基づきセキュリティ確保のための措置を講じる。約款による外部サービスやソーシャルメディアサービスを利用する場合には、利用に係る規定を整備しセキュリティ対策を講じる。

⑹　危機管理対策

緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

10　情報セキュリティ実施手順の策定

対策基準を遵守して情報セキュリティ対策を実施するために、情報資産に対する脅威及び情報資産の重要性に対応する対策基準の基本的な要件に基づき、各部局の長等が所管する情報資産の情報セキュリティ実施手順（以下「実施手順」という。）を策定する。

11　情報セキュリティ監査の実施

ポリシーが遵守されていることを検証するため、定期的に監査を実施する。

12　評価及び見直しの実施

情報セキュリティ監査の結果等により、ポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、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、ポリシーの見直しを実施する。

13　情報セキュリティに関する違反への対応

ポリシー及び実施手順に違反した職員については、その重大性、発生した事案の状況等に応じて懲戒処分の対象となることがある。

14　公開方針

ポリシー及び実施手順は、公表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のある事項を含んでいることから、基本方針を公開とし、対策基準及び実施手順は非公開とする。また、情報セキュリティ監査の概要については、公開とする。