ISMS-P-001

神戸市情報セキュリティ基本方針

制定日：平成 15 年 1 月 27 日
改正日：令和 2 年 3 月 16 日
施行日：令和 2 年 4 月 1 日

神戸市

改訂履歴

施行年月日	版番号	改訂理由・内容
平成 15 年 1 月 27 日	第 1.0 版	初版発行（平成 15 年 1 月 27 日決裁）
平成 17 年 6 月 1 日	第 2.0 版	第２章　対策基準の追加（平成 17 年 5 月 31 日決裁）
平成 20 年 4 月 1 日	第 3.0 版	全部改正（平成 20 年 2 月 13 日決裁）
平成 23 年 4 月 1 日	第 4.0 版	全部改正（平成 23 年 3 月 30 日決裁）
平成 26 年 4 月 1 日	第 4.1 版	一部改正（平成 26 年 3 月 24 日決裁）
平成 31 年 4 月 1 日	第 5.0 版	自治体強靭性向上事業にかかる対策基準の追加等（平成 31 年 3 月 25 日決裁）
令和元年 9 月 1 日	第 5.1 版	一部改正（令和元年 8 月 16 日決裁）
令和 2 年 4 月 1 日	第 5.2 版	一部改正（令和 2 年 3 月 16 日決裁）
年　月　日		
年　月　日		
年　月　日		
年　月　日		
年　月　日		

目次

１．目的

本市の情報システムが取り扱う情報には、市民の個人情報や行政運営上重要な情報が多数含まれており、情報資産を人的脅威や災害、事故等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、継続的かつ安全・安定的な行政サービスの実施を確保するためにも必要不可欠である。

このため、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ことを目的として神戸市情報セキュリティ基本方針（以下「情報セキュリティ基本方針」という）を定める。神戸市の情報資産に関する情報セキュリティ対策の基本的な考え方と方針を規定するものである。

２．定義

（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

コンピュータ及びネットワークで構成され、情報処理を行う仕組みをいう。

（３）データ

電子計算機処理に係る入出力帳票、磁気テープ、磁気ディスク、光ディスクその他の記録媒体に記録されている情報又は通信回線により送信される情報をいう。

（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

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）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、個人番号利用事務と経常的にデータ連携を行っている事務に関わる情報システム及びデータをいう。

（１０）LGWAN 接続系

人事給与、財務会計及び文書管理等 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。

（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．情報セキュリティポリシーの位置付け及び構成

情報セキュリティポリシーは、本市が保有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かつ体系的に取りまとめた情報セキュリティ対策の基本となるものであり、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から構成される。

情報セキュリティ対策基準は、情報セキュリティ基本方針に基づき、情報セキュリティ対策等を実施するために最低限必要な水準として、職員、再任用職員、任期付職員、教員、臨時的任用職員、会計年度任用職員、特別職非常勤職員、労働者派遣契約等により本市業務に従事する者（以下「職員等」という。）が遵守すべき事項及び判断基準をまとめたものである。本市では、組織等の状況に合わせた情報セキュリティ対策基準を策定する。

４．対象とする脅威

情報セキュリティ対策を講じるうえでは、情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。特に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、外部委託管理の不備、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

（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

5．適用範囲

（1）組織の範囲

神戸市事務分掌条例(平成 15 年 10 月条例第 19 号)第 1 条に規定する局及び室、区役所、会計室、消防局、水道局、交通局、教育委員会、選挙管理委員会事務局、人事委員会事務局、監査事務局、農業委員会事務局、市会事務局とする。

（2）情報資産の範囲

情報セキュリティ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、電子記録媒体

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

6．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つとともに、業務の遂行にあたっては情報セキュリティポリシーを遵守しなければならない。

7．情報セキュリティ対策

上記４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）情報セキュリティ管理体制

本市の情報資産について、適切に情報セキュリティ対策を推進・管理するため、神戸市情報化推進体制の整備に関する要綱に定める情報化統括責任者（情報化の推進を所管する実施組織を担任する副市長）を情報セキュリティ最高責任者とし、その下に全庁的な組織体制を確立する。必要な体制、役割、権限等については情報セキュリティ対策基準にて定める。

（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講じる。

（3）情報システム全体の強靭性の向上

情報システム全体に対し、情報資産の分類に応じた情報セキュリティ対策を講じるとともに、次の対策も併せて講じる。

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。

②LGWAN 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、無害化通信を行う。

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。

（4）物理的セキュリティ

コンピュータ設置場所への入退室、サーバ等の管理、通信回線及び端末等への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、十分な研修・訓練及び啓発を実施するなど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、コンピュータウイルス等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、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切に対応するため、情報セキュリティ事件・事故等緊急時対応基準を策定する。

（8）外部サービスの利用

外部委託する場合には、外部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、外部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。

8．情報セキュリティ監査及び自己点検の実施

情報セキュリティ対策の実施状況を評価するため、定期的及び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。

9．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。

１０．情報セキュリティ対策基準の策定

上記７、８及び９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。

１１．情報セキュリティ個別基準の策定

情報セキュリティ対策基準を補完するために必要な内容に関して、具体的な内容を定める情報セキュリティ個別基準を策定するものとする。なお、情報セキュリティ個別基準は、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。

１２．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及び情報セキュリティ個別基準に基づき、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。