高砂市情報セキュリティポリシー

文書番号			
制定日	平成 16 年３月 17 日	最新改定日	令和５年６月２１日
作成者	情報セキュリティ事務局		

制定／改定の履歴

版数	制定日／改定日	改定内容・理由
1	2004／05／24	統括情報責任者の職務代理
2	2005／04／01	機構改革に伴う改定
3	2006／04／01	指定管理者制度の導入に伴う改定
4	2007／04／01	地方自治法の改正に伴う改定
5	2010／12／01	メールボックス容量の上限
6	2013／04／01	事務分掌規則改正に伴う改定
7	2015／11／17	番号制度改正等に伴う改定
8	2016／04／01	機構改革等に伴う改定
9	2021／04／01	機構改革等に伴う改定
10	2023／03／07	セキュリティ対策強化のための改定
11	2023／06／21	セキュリティポリシーガイドライン改定に伴う改定

〈目次〉

はじめに　高砂市情報セキュリティポリシーの構成

高砂市情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）とは、高砂市（以下「本市」という。）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を総称する。

情報セキュリティポリシーは、本市が所掌する情報資産に関する業務に携わる正規職員、任期付職員、再任用職員及び会計年度任用職員（以下「職員等」という。）並びに委託事業者、外部サービス提供者及び指定管理者（以下「委託事業者等」という。）に浸透させ、普及させ、かつ定着させるものであり、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、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（対策基準）に分けて策定することとした。具体的には、情報セキュリティポリシーを、

①情報セキュリティ基本方針

②情報セキュリティ対策基準

の２階層に分け、それぞれを策定することとする。

また、情報セキュリティポリシーに基づき、情報システムごとの具体的な情報セキュリティ対策の実施手順として情報セキュリティ実施手順を策定することとする（下表参照）。

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
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

本市の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、これらの情報資産、情報を取り扱うネットワーク及び情報システム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、近年のいわゆる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。

そのため、本市の情報資産の機密性、完全性及び可用性[1]を維持するための対策（以下「情報セキュリティ対策」という。）を整備するために情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については本市の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

２　定義

(1)　ネットワーク

本市における部、室、各地方公営企業、消防本部、議会事務局、教育委員会及び各行政委員会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）及び記録媒体を含む。）により、通信処理を行う仕組みをいう。

(2)　情報システム

電子計算機（ソフトウェアを含む。）及び記録媒体で構成され、業務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並びにネットワーク及び情報システムで取り扱うすべてのデータをいう。

(4)　情報セキュリティ

情報資産の機密の保持及び正確性、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。

(5)　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。

(6)　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。）。

(7)　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。

(8)　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、安全に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。

---

[1]機密性：情報にアクセスすることを認められた者が、情報にアクセスできる状態を確保することをいう。
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。
可用性：情報にアクセスすることを認められた者だけが、必要な時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)　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と職員等及び委託事業者等の義務

情報セキュリティポリシーは、本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ものである。

したがって、市長をはじめとして本市が所掌する情報資産に関する業務に携わる職員等及び委託事業者等は、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当たって情報セキュリティポリシーを遵守する義務を負うものとする。

４　情報セキュリティ管理体制

本市の情報資産について、管理職員が率先して情報セキュリティ対策を推進・管理するための体制を確立するものとする。

５　情報資産の分類

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

６　情報資産への脅威

情報セキュリティポリシーを策定する上で、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と、特に認識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、改ざん、消去、重要情報の詐取、内部不正等

(2)　職員等及び委託事業者等による機器又は情報資産の持ち出し、誤操作、アクセスのための認証情報又はパスワードの不適切管理、故意の不正アクセス又は不正行為による破壊・盗聴・改ざん・消去等、搬送中の事故等による機器又は情報資産の盗難、規定外の端末[2]又は記録媒体の接続によるデータ漏えい等

(3)　地震、落雷、火災等の災害、事故、故障等によるサービス及び業務の停止等

(4)　電力供給、通信、水道供給の途絶等のインフラの障害からの波及等

７　情報セキュリティ対策

上記６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ずるものとする。

(1)　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、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。

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

[2]端末：パソコン、モバイル端末等

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。

(2)　物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

(3)　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、全ての職員等及び委託事業者等が情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が行われるように必要な対策を講ずる。

(4)　技術及び運用におけるセキュリティ対策

情報資産をからの不正な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システム開発等の委託、ネットワークの監視、情報セキュリティポリシー遵守状況の確認等の運用面における対策を講ずる。

また、緊急事態が発生した際に迅速に対応できるよう緊急時対応計画を策定する。

８　情報セキュリティ対策基準の策定

本市の様々な情報資産について、上記７の情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

９　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を遵守して情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ対策基準及び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　情報セキュリティ監査の実施

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、情報セキュリティ監査を実施する。

11　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、情報セキュリティ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に、適宜情報セキュリティポリシーの見直しを実施する。