「明石市情報セキュリティ基本方針」

明石市情報管理課

２０２３年（令和５年）４月

目　次

１．総則

１．１ 目的

明石市情報セキュリティ基本方針（以下「基本方針」という。）は、明石市の情報セキュリティに対する基本的な指針を示したものであり、実施機関が管理する情報資産を適正に保護することを目的とする。

１．２ 用語の定義

この基本方針において、次の各号に掲げる用語の意義は、それぞれ当該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

業務の遂行に伴ってコンピュータ及び電磁的記録媒体[1]に記録されたデータをいう。

(3) 情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(4) 情報資産

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) 脅威

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、重要情報の搾取、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

(6) 情報セキュリティ

脅威から市が管理する情報資産を保護し、情報資産の「機密性」、「完全性」及び「可用性」を確保することをいう。

・「機密性」：権限のない者への重要な情報の漏洩を防止すること

[1]**電磁的記録媒体**：サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体及びＵＳＢメモリ、外付けハードディスクドライブ、ＤＶＤ－Ｒ、磁気テープ等の外部電磁的記録媒体のことをいう。

・「完全性」：情報の改ざん、破壊による被害を防止すること

・「可用性」：権限のある者に対し、いつでも情報の利用を可能とすること

(7) 情報セキュリティ対策

情報セキュリティを維持するための管理策をいう。

(8) 実施機関

市長、教育委員会、選挙管理委員会、監査委員、公平委員会、農業委員会、固定資産評価審査委員会、公営企業管理者、消防長及び議会をいう。

(9) 職員

実施機関の職員（非常勤職員、臨時及び嘱託職員を含む）の総称をいう。

(10) 外部要員

職員以外で、職務において実施機関の情報資産を取り扱う者の総称をいう。

(11) 情報セキュリティポリシー

本基本方針及び明石市情報セキュリティ対策基準をいう。

(12) 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。

(13) ＬＧＷＡＮ接続系

人事給与、財務会計及び文書管理等ＬＧＷＡＮ[2]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。

(14) インターネット接続系

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。

１．３ 適用範囲

この基本方針の適用範囲は、次に定めるところによる。

(1) 適用対象者

職員及び外部要員とする。

(2) 適用資産

実施機関が管理する全ての情報資産とする。

１．４ 職員の義務

職員は、次に掲げる義務を負うものとする。

(1) この基本方針を遵守し、情報セキュリティ対策を有効に機能させなければならない。

(2) 職務上知り得た秘密を漏らしてはならない。その職を退いた後も同様とする。

---

[2] LGWAN：Local Government Wide Area Network 地方公共団体の組織内のネットワークを相互に接続する広域行政のネットワーク。地方公共団体システム機構（J-LIS）により運営されている。

１．５ 外部要員の参加

外部要員は、情報資産の利用範囲に応じて、職員の義務と同様の義務が生じ得るものとし、実施機関が実施する情報セキュリティ対策に積極的に関与するものとする。

１．６ 外部要員の管理

外部要員を使用する職員は、契約等に基づき、職員の義務と同様の内容を外部要員に対しても義務づけ管理するものとする。

２．情報区分

実施機関が管理する情報資産は、その重要度に応じて区分し、その区分に応じた情報セキュリティ対策を講ずるものとする。そのため、必要な情報区分の定義及び区分に応じた情報セキュリティ対策の要件を、別に定める情報セキュリティ対策基準に規定するものとする。

３．情報セキュリティ体系

３．１ 情報セキュリティ対策

実施機関が管理する情報資産を脅威から保護するために、次に掲げる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

情報システム全体に対し、次の三段階の対策を講じる。

① 個人番号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環境を分離し、必要な通信だけを許可できるようにする。なお、両システム間で通信する場合には、無害化通信[3]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している兵庫県情報セキュリティクラウド[4]を利用する。

(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

職員に対して情報セキュリティの重要性を認識させ、情報セキュリティの啓発に有効と考えられる教育活動等の必要な対策を講ずる。

(4) 技術的セキュリティ対策

3 無害化通信：仮想デスクトップ化による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。

4 兵庫県情報セキュリティクラウド：高度な情報セキュリティ対策として、兵庫県と県下全市町のインターネット接続口を集約し、異常通信の監視・分析・対策等を行う

情報システムの誤操作、不正アクセス[5]等から情報資産を保護するために、情報資産へのアクセス制御等の技術的な対策を講ずる。

(5) 情報システム開発セキュリティ対策

情報システムの誤作動、不正利用、情報漏洩等から情報資産を保護するために、開発環境、品質保持に必要な対策を講ずる。

(6) 情報システム運用セキュリティ対策

情報システムの誤作動、不正利用、情報漏洩等から情報資産を保護するために、情報システムの運用、保守、監視等に必要な対策を講ずる。

(7) ネットワークセキュリティ対策

ネットワーク障害、不正アクセス等から情報資産を保護するために、ネットワークの可用性確保、ネットワーク監視等の必要な対策を講ずる。

(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。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用規定を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

３．２ 情報セキュリティ対策基準

実施機関は、この基本方針に従い、情報セキュリティ対策を講ずるにあたって、遵守すべき行為や判断等の統一基準となる情報セキュリティ対策基準（以下「対策基準」という。）を定め、想定される脅威に対応するための対策要件を規定するものとする。

３．３ 情報セキュリティ実施手順

実施機関は、この基本方針及び対策基準に従い、情報セキュリティ対策に関する具体的な手法、手順を明記した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上に重大な支障を及ぼす恐れがあることから非公開とする。

４．情報セキュリティ管理体制

この基本方針及び対策基準に規定された情報セキュリティ対策の推進・管理にあたり、以下の組織・体制を置くものとする。

(1) 情報セキュリティ対策本部

(2) 情報セキュリティ最高責任者

(3) 情報セキュリティ統括責任者

---

[5]**アクセス**：コンピュータやネットワークを利用して情報の閲覧、取り出し、登録などを行うこと。

(4) 情報セキュリティ対策委員会
(5) 情報セキュリティ責任者
(6) 情報セキュリティ管理者
(7) 情報セキュリティ担当者
(8) 情報セキュリティに関する統一的な窓口

５．情報セキュリティに関する監査

実施機関は、この基本方針及び対策基準が遵守されていることを検証するため、定期的に、又は必要に応じて随時に情報セキュリティ監査及び自己点検を実施するものとする。

６．改訂

この基本方針は必要に応じて、内容の妥当性について審議し見直しをするものとする。

７．法令等の遵守

全ての適用対象者は、職務遂行において、この基本方針、対策基準に定める規定及び次の法令の他、情報セキュリティに関連する法令等に従わなければならない。

(1) 地方公務員法(昭和二十五年十二月十三日法律第二百六十一号)
(2) 著作権法（昭和四十五年法律第四十八号）
(3) 不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）
(4) 個人情報の保護に関する法律（平成十五年五月三十日法律第五十七号）
(5) 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成二十五年法律第二十七号）
(6) サイバーセキュリティ基本法（平成二十八年法律第三十一号）
(7) 明石市情報公開条例（平成十四年三月二十七日条例第五号）
(8) 明石市個人情報保護法施行条例（令和四年十二月二十三日条例第二十三号）

附　則（平成１６年３月３日制定）

（施行期日）

この基本方針は、平成１６年４月１日より施行する。

附　則（平成２０年２月２５日制定）

（施行期日）

この基本方針は、平成２０年３月１日より施行する。

附　則（平成２９年３月２７日制定）

（施行期日）

この基本方針は、平成２９年４月１日より施行する。

附　則（平成３１年３月１３日制定）

（施行期日）

この基本方針は、平成３１年４月１日より施行する。

附　則（令和５年３月１３日制定）

（施行期日）

この基本方針は、令和５年４月１日より施行する。