第１章　情報セキュリティ基本方針

１．目的

市民の財産、プライバシー等の保護及び市政の安定的な運営を図ることを目的として岸和田市情報セキュリティ基本方針（以下「本基本方針」という。）を制定する。

２．位置づけ

本基本方針は、本市の保有する情報資産についての情報セキュリティ対策を、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を実施するうえでの基本的な事項を定めたものである。

３．定義

本基本方針及び情報セキュリティ対策基準にて使用する用語の定義は、以下のとおりとする。

①ネットワーク

コンピュータ等を通信回線で接続することにより、一体として情報の処理を行う情報通信網、その構成機器をいう。

②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。

③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。

④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、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。

⑤ＬＧＷＡＮ接続系

総合行政ネットワーク（Local Government Wide Area Network）（以下「ＬＧＷＡＮ」という。）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。

⑥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。

⑦管理系（サーバ系）

財務会計、文書管理システムやセキュリティ関連システム、ファイルサーバ等の管理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を分離したうえで、安全が確保された通信だけ許可できるようにすることをいう。

⑨情報セキュリティインシデント

望まない単独若しくは一連の情報セキュリティ事象、予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

４．対象範囲

（１）組織の範囲

①市の内部の組織（実施機関）

市長（市民病院における医療部門を除く。）、議会、教育委員会（学校園を除く。）、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会、上水道事業及び下水道事業の管理者の権限を行う市長、消防長

②市の外部の組織

市の保有する情報資産を取扱う外部委託事業者等（当該受託業務に限る。）

（２）人の範囲

上記（１）①に掲げる実施機関の指揮監督権に服する全ての職員（一般職もしくは特別職、常勤もしくは非常勤の地方公務員をいう。ただし市議会議員は除く。）及び②の組織の従業者であって本市の情報資産の取扱いに従事している者（以下「職員等」という。）

（３）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、情報システムで取り扱う情報

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

④ 情報資産の範囲には、各種申請書等の紙情報を原則含まないが、情報システムから紙等の有体物に出力された情報や、業務上の理由により情報資産の所管部署から持ち出される入力帳票については、対象範囲内とする。

５．対象範囲外への対応

本基本方針の対象範囲外とした紙情報についても、本基本方針の趣旨を尊重しつつ、これまでと同様、当該文書の取扱いを定めた関連法令等に基づいて、引続き適正な取扱いに努めるものとする。

また、市民病院における医療部門、学校園については、本基本方針の理念を尊重した情報セキュリティ対策を講じるものとする。

６．情報セキュリティポリシー及び関連法令等の遵守

（１）職員の責務

① 職員は、情報セキュリティの重要性を認識し、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する義務を負う。また、情報資産の利用や保管等を行う際は、個人情報の保護に関する法律（平成 15 年法律第 57 号）等関連する法令等を遵守しなければならない。

② 情報セキュリティポリシーに違反した職員は、生じた結果の重大性及び違反の悪質性等の状況に応じて、地方公務員法等に基づき懲戒処分等の対象になることがある。

（２）外部委託事業者等への対応

外部委託事業者等に対しても、情報セキュリティの重要性を認知させ、契約書等において情報セキュリティポリシーの遵守事項及び違反した場合の責任について明確にするものとする。

７．情報資産に対する脅威

（１）情報資産に対する主な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。

・不正アクセス、コンピュータウイルス等不正プログラム攻撃、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洩、破壊、盗聴、改ざん、消去、情報の搾取、無断持ち出し、内部不正等

・無許可ソフトウェアの使用、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、機器故障等の非意図的要因による情報資産の漏洩、破壊、消去等

・搬送中の事故等による情報資産の盗難、紛失等

・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

・事故、機器故障等によるサービス及び業務の停止

・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

（２）職員等は、上記（１）の脅威に対し認識を深めるとともに、これら以外の脅威についても注意を払わなければならない。

８．運用体制

情報セキュリティ対策の推進、情報セキュリティへの侵害（以下「セキュリティ侵害」という。）に対する迅速な対応を図るための全庁的な運用体制を確立するものとする。

なお、セキュリティ侵害とは、「７.情報資産に対する脅威」に記述するような脅威が発生した状態をいう。

９．情報資産の分類

情報資産を内容に応じて分類し、その重要度に即した対策を講じるものとする。

10. 対策

「７.情報資産に対する脅威」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じるものとする。

（１）物理的対策

情報システムを設置する施設への不正な立ち入りや、自然災害により起こる破壊、盗難等から情報資産を保護するために行う入退室管理等の物理的な対策

（２）人的対策

情報資産を取扱う職員等の情報セキュリティに関する権限や責任、運用体制の明確化、情報セキュリティポリシーの内容を周知徹底するために行う教育、訓練等の人的な対策

（３）技術的対策

情報資産を不正なアクセス等から適正に保護するための情報資産へのアクセス制限、コンピュータウイルス等不正プログラムからの脅威への対策等の技術的な対策

（４）情報システム全体の強靭化

情報システム全体に対し、以下の対策を講じる。

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。

② ＬGWＡＮ接続系においては、ＬGWＡＮと接続する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。

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、大阪府と市区町村のインターネット接続口を集約した大阪版自治体情報セキュリティクラウドの導入等を実施する。

④ 管理系においては、マイナンバー利用事務系、ＬGWＡＮ接続系、インターネット接続系との通信経路を分割する。

（５）外部サービスの利用

① 外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

② 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手順を定め、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。

11. 情報セキュリティ対策基準の策定

「10.対策」で示した対策を講じるにあたって、職員等が遵守すべき事項や判断の基準等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実施する上で必要となる一定の基準を示した、情報セキュリティ対策基準を策定するものとする。

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を確実に実施していくためには、個々の情報資産に関する具体的な対策の方法や手順を定めておく必要がある。そのため、情報セキュリティ対策基準に基づく実施マニュアルとして、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、具体的な対策の手順やノウハウについて記述するものであり、公開することにより行政運営に重大な支障を及ぼすおそれがあるため、非公開とする。

13. セキュリティ対策の点検と情報セキュリティポリシーの見直し

日々の情報セキュリティに対する脅威に対応するため、情報セキュリティポリシーに定める事項及び実施手順の遵守状況を確認するため、定期的又は必要に応じて情報セキュリティ監査を実施する。

また、情報セキュリティポリシーの内容についても必要に応じて見直し、本市におけるセキュリティレベルの向上を図るものとする。