宜野湾市情報セキュリティ基本方針

制定：平成18年1月1日
改訂：令和2年8月14日
市長決裁
（行政情報化推進本部会議決定）

目次

第１章　総則

（制定の趣旨）

第１条　本市において取り扱う情報には、市民の個人情報や行政運営上重要な情報等、外部への漏えい等が発生した場合に極めて重大な影響を及ぼす情報が多数含まれており、これらの情報資産を適切に保護し、責任を持って管理するためには、情報セキュリティマネジメント（情報資産を適切に保護するための組織としての継続的かつ計画的な取り組み）が必要不可欠である。

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「宜野湾市情報セキュリティ基本方針」を定める。これは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。

（目的）

第２条　宜野湾市情報セキュリティ基本方針（以下「基本方針」という。）は、本市の職員及び外部委託事業者が、情報セキュリティの確保に関する包括的な対策を講じることにより、本市の情報資産を適切に保護することを目的とする。

（定義）

第３条　基本方針及び、これに基づき定められた規定等において、次の各号に掲げる用語の意義は、当該各号の定めるところによる。

（１）　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。
（２）　機密性　許可された者だけが情報資産を利用できることを保証することをいう。
（３）　完全性　情報資産が正確及び完全であることを常に維持することをいう。
（４）　可用性　許可された者が、確実に情報資産を利用できることをいう。
（５）　情報　職員が職務上作成し、又は取得した事項を電磁的に記録したもの及び、これらを出力したものをいう。
（６）　個人情報　宜野湾市個人情報保護条例（平成13年宜野湾市条例第17号）第２条第１項第１号に規定する個人情報をいう。
（７）　情報システム　与えられた一連の処理手順に従い事務処理を行う仕組み及び、宜野湾市個人情報保護条例第２条第１項第10号に規定する電子計算組織をいう。
（８）　情報資産　情報及び情報システムの総称をいう（教育機関で専ら教育用に使用する情報資産は含まない）。
（９）　情報セキュリティポリシー　本市の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、基本方針と対策基準から成る。
（10）　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）に関わる情報システム及びデータをいう。
（11）　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。
（12）　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の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。
（13）　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。
（14）　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。
（15）　実施機関　宜野湾市個人情報保護条例第２条第１項第３号に規定する実施機関をいう。

（16） 職員　実施機関の職員（一般職、特別職、非常勤、臨時職員、会計年度任用職員等）の総称をいう。
（17） 外部委託事業者　本市の情報資産に関連する開発、導入及び保守等のための委託を受けたすべての事業者等をいう。
（18） 情報セキュリティに関する事案　不正アクセス、コンピュータウイルスの感染等、情報セキュリティに関する事故、事件をいう。

（適用範囲）
第４条　基本方針の適用範囲は、実施機関におけるすべての情報資産及び職員、並びに外部委託事業者に対して適用する。
２　基本方針の適用にあたっては、本市の教育機関における教育及び研究活動、議会における政治活動を制限することがないよう、十分な配慮をしなければならない。
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

（対象とする脅威）
第５条　情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。
（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

（情報セキュリティポリシーの構成）
第６条　本市の情報セキュリティポリシー（以下「ポリシー」という。）は、本市における情報セキュリティに関する基本的な考え方を述べた「基本方針」と、基本方針に基づき、情報セキュリティを確保するために遵守すべき行為等の基準を示した「対策基準」からなるものとする。また、ポリシーに基づき、情報セキュリティ対策の具体的な手順等を定めた、宜野湾市情報セキュリティ実施手順（以下「実施手順」という。）を、必要に応じて個別の情報システム又は業務毎等に想定しておく。

第２章　基本的な考え方

（職員及び外部委託事業者の責務）
第７条　全ての職員及び外部委託事業者は、ポリシーを理解し、遵守することで、情報資産を適切に保護しなければならない。

（組織及び体制）
第８条　実施機関における情報セキュリティ対策は、責任や役割を明確にした組織及び体制のもとに行うものとし、対策基準にて定める。

（情報の分類と管理）
第９条　実施機関は、取扱う情報について、重要な情報を重点管理するため、重要度に応じた情報分類の定義を行い、情報の管理責任及び管理方法を明確にする。

（情報システム全体の強靭性の向上）
第10条　情報システム全体に対し、次の三段階の対策を講じるものとする。
（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、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（人的セキュリティ）

第 11 条　実施機関は、職員及び外部委託事業者について、情報セキュリティに関する役割や責任を明確化し、ポリシーの内容を周知徹底するため、教育等の必要な対策を講ずるものとする。

（物理的セキュリティ）

第 12 条　実施機関は、情報資産を設置及び保管する場所について、許可を得ない者の不正な立入による、情報資産への損傷及び妨害から情報資産を適切に保護するため、入退室管理等の物理的な対策を講ずるものとする。

（技術的対策及び運用管理）

第 13 条　実施機関は、情報資産を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必要な対策を講ずるものとする。

（コンピュータウイルス対策）

第 14 条　実施機関は、コンピュータウイルス等の悪意のあるプログラムから情報資産を適切に保護するため、また、自らが加害者にならないために必要な対策を講ずるものとする。

（記録媒体の取扱い及び管理）

第 15 条　実施機関は、記録媒体について、紛失等による脅威の発生を防止するため、これらを適切に管理するための対策を講ずるものとする。

（情報システムの開発、導入及び保守）

第 16 条　実施機関において情報システムの開発、導入及び保守を行う者は、情報資産を適切に保護するために必要な対策を講ずるものとする。

（外部サービスの利用）

第 17 条　実施機関は、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。

２　実施機関は、約款による外部サービスを利用する場合には、情報セキュリティ要件を確保するため、利用にかかる規定を整備し対策を講じる。

３　実施機関は、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アカウントごとの責任者を定める。

（情報セキュリティに関する事案への対応）

第 18 条　実施機関は、情報セキュリティに関する事案が発生した場合の対応をあらかじめ定めるとともに、情報セキュリティに関する事案が発生した際には、定められた対応を迅速かつ円滑に実施し、その影響を最小限にするとともに、再発防止のために必要な対策を講ずるものとする。

（遵守）

第 19 条　職員は、ポリシーに定められた条項のほか、情報資産の利用において、関連法令、条例等を遵守するものとする。

（評価及び見直し）

第 20 条　実施機関は、情報セキュリティの実施状況を評価するため、定期的に情報セキュリティの監査を行う。また、今後発生する新たな脅威等に備え、必要に応じポリシーの見直しを行う。

第３章　雑則

（公開範囲）

第 21 条　ポリシーは、情報資産を利用、運用、管理、保守するすべての職員及び外部委託事業者に公

開するものとする。

（出資法人等の扱い）

第 22 条　市が出資している法人のうち、宜野湾市個人情報保護条例第 31 条第１項に定める出資法人は、ポリシーの趣旨にのっとり、必要な措置を講じなければならない。

２　実施機関は、出資法人等に対し、ポリシーの規定による本市の施策に準じた措置を講じるよう要請するものとする。

（その他）

第 23 条　基本方針に定めるもののほか情報セキュリティに関し必要な事項については別に定める。

附　則

この基本方針は、平成１８年１月１日より施行する。

附　則

この基本方針は、平成２６年４月１日より施行する。

附　則

この基本方針は、令和２年８月１４日より施行する。