宗像市情報セキュリティポリシー

基本方針

令和８年４月

宗像市

改訂履歴

施行年月	版番号	改訂理由・内容
平成 16 年 3 月	1.0 版	策定
平成 16 年 7 月	1.1 版	一部改訂（別表修正等）
平成 19 年 9 月	1.2 版	一部改訂（機構改革等に伴う文言修正）
平成 20 年 4 月	1.3 版	一部改訂（機構改革に伴う文言修正）
平成 23 年 2 月	1.4 版	一部改訂（所掌事務変更等に伴う文言修正）
平成 24 年 4 月	1.5 版	一部改訂（機構改革に伴う文言修正）
平成 27 年 9 月	1.6 版	一部改訂（番号法施行に伴う修正）
平成 28 年 4 月	2.0 版	全部改訂
平成 29 年 4 月	2.1 版	一部改定（情報セキュリティ強靭化に伴う文言修正）
令和 4 年 8 月	3.0 版	全部改訂
令和 8 年 4 月	4.0 版	一部改訂（地方自治法改正に伴う修正）

目　　次

1. 目的

本基本方針は、宗像市が保有する情報資産の機密性、完全性及び可用性を確保し、行政サービスの安定的な提供と市民の信頼を維持するため、本市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。また、新たに発生する脅威に対応するため、継続的な見直し及び改善を行う。

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、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、電磁的記録媒体及びクラウドサービス等で構成され、情報処理及び管理を行う仕組みをいう。

（3）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確保し、これを維持することをいう。

（4）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。

（5）機密性

情報にアクセスすることを認められた者のみが、情報にアクセスできる状態を確保することをいう。

（6）完全性

情報が破壊、改ざん又は消去されることなく正確に維持される状態を確保することをいう。

（7）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、情報にアクセス及び利用できる状態を確保することをいう。

（8）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当該事務で取り扱うデータをいう。

（9）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。）。

（１０）インターネット接続系

インターネットに接続して利用する情報システム及びそのデータをいう。

（１１）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。

（１２）無害化通信

不正プログラムの混入を防ぐために内容を安全な形式に変換し、安全を確保した通信をいう。

（１３）サイバー脅威

サイバー空間において、情報資産に対する攻撃や侵害を意図する行動や現象をいう。

（１４）クラウドサービスの利用ポリシー

外部サービスを利用する際のセキュリティ要件と運用手順を規定する文書をいう。

3. 対象とする脅威

情報資産に対する脅威として、以下に示す脅威を想定し、情報セキュリティ対策を実施する。

また、これらへの対策を講ずるとともに、技術の進展等により新たに生じうる脅威にも適切に対応する。

（１） 不正アクセス・外部攻撃

標的型攻撃、ランサムウェア、マルウェア・ウイルス感染、脆弱性を利用した攻撃、クラウドサービスへの不正ログイン、API・外部連携を悪用した侵入など

（２） 内部不正・内部脅威

職員・委託職員による不正アクセス、情報の不正持ち出し・漏えい、なりすまし・権限乱用、閲覧権限の不適切管理による漏えいなど

（３） 誤操作・設備不備

職員の誤送信、誤登録・誤削除、システムやクラウドサービスの設定誤り、初期設定のまま運用されることによる危険など

（４） 情報機器・媒体の紛失・盗難

ノートパソコン、タブレット、USB メモリ等の記録媒体、持出端末の盗難・置き忘れなど

（５） システム障害・機器故障

ハードウェアの故障、ソフトウェアの不具合、障害発生時に復旧できない事態、通信障害（回線・VPN・クラウド接続など）など

（６） 外部サービス・クラウドの障害

SaaS 障害、ガバメントクラウド障害、外部 API 停止、サービス提供者側の事故による影響

（７） 電子データの破壊・改ざん・消去

外部攻撃や内部不正によるデータ破壊、システム更新時のデータ損失、バックアップ不備によるデータ喪失など

（８） 自然災害・火災・停電等による影響

地震、風水害、津波、火災、落雷、停電、電源障害、庁舎の被災によるシステム停止など

（９） 供給業者・委託先に起因する脅威

委託事業者の不正、再委託先での事故、ソフトウェア・システムの脆弱な保守、サプライチェーン攻撃など

（１０）社会情勢・外的要因に関連する脅威

サイバー犯罪の高度化、国際情勢の緊張による攻撃増加、SNS 等での虚偽情報による混乱

（１１）IoT デバイスに関する脅威

接続されたデバイスの脆弱性を突いた攻撃及び不正アクセスなど

（１２）フィッシング攻撃

職員を狙った詐欺的なコミュニケーション手法など

4. 適用範囲

（１）行政機関の範囲

本基本方針が適用される行政機関は、市長部局、議会事務局、監査委員事務局、会計管理者（会計課)、農業委員会事務局、各種行政委員会とする。

（２）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 ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

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

④ 上記の情報資産の範囲には市のホームページで公開される情報や、外部クラウドで運用されるシステムも含むものとする。

5. 職員等の遵守義務

職員、非常勤職員及び臨時職員等（以下「職員等」という。）は、情報セキュリティの重要性を認識し、業務の遂行に当たっては情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

6. 情報セキュリティ対策

上記３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）組織体制

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（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実施する。

（３）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等により、住民情報の漏えいを防ぐ。

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、不正通信対策を強化するとともに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を活用する。

（４）物理的セキュリティ

サーバ、情報システム室、通信設備及び情報機器について、不正な立ち入りや盗難等を防止するため、必要な物理的対策を講じる。

（５）人的セキュリティ

職員等が遵守すべき事項を明確にし、継続的な教育及び啓発を行う等の人的な対策を講じる。定期的なセキュリティ意識向上研修を必須化し、研修資料は最新の脅威に基づくものとする。

（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、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）運用管理セキュリティ

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、業務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。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正に対応するため、緊急時対応計画を策定する。

（８）業務委託と外部サービスの利用

業務委託を行う場合には、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、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。

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。

ソーシャルメディアサービスを利用する場合には、運用手順を定め、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。

（９）評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、監査及び自己点検を実施し、必要に応じて運用改善を行い、情報セキュリティの向上を図る。また、環境の変化応じて情報セキュリティポリシーを適宜改定する。

7. 情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、その結果を踏まえて必要な改善を行う。

8. 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。

9. 情報セキュリティ対策基準の策定

上記６、７及び８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。

10. 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に基づき、対策実施の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。