石垣市サイバーセキュリティ基本方針【首長部局版】

令和８年３月

石垣市

〈 改 定 履 歴 〉

版数	作成年月日	作成改訂理由
第1版	令和8年3月2日	新規制定

目　次

1. 目的

石垣市（以下「市」という。）は、行政運営上、個人情報などの重要な情報を多数取り扱っているだけでなく、公共インフラ事業を担うことにより、市民生活及び社会経済活動に必要不可欠なサービスを提供している。よって、これらを支える情報システムに加え、これらで取り扱う重要な情報などの情報資産を様々な脅威から守り、安全性を確保することは、行政及び公共インフラ事業の安定的・継続的な運営を実現するために、市に課せられた責務である。

そのため、石垣市サイバーセキュリティ基本方針（以下「本方針」という。）は、市が実施するサイバーセキュリティ対策に関する基本的な事項を定め、サイバー攻撃等の様々な脅威から、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する。

また、全ての職員等は、市が保有する情報資産に対する脅威への対応が重大かつ喫緊の課題であることを改めて認識し、市におけるサイバーセキュリティ対策の推進に積極的に取り組むこととする。

2. 定義

(1) 情報

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。）、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をいう。

(2) 情報システム

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

(3) 情報資産

情報及び情報システムをいう。

(4) 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及びその構成機器（ハードウェア及びソフトウェア）をいう。

(5) サイバーセキュリティ

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。

(6) サイバーセキュリティ基本方針

本方針をいう。

(7) 情報セキュリティポリシー

情報セキュリティ基本方針及び情報セキュリティ対策基準をいう。

(8) 職員等

4. (2)の適用機関に属する特別職及び一般職の全ての職員並びに委託事業者及び指定管理者をいう。

(9) 機密性

情報にアクセスすることを許可された者だけが、情報にアクセスできる状態を確保することをいう。

(10) 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。

(11) 可用性

情報にアクセスすることを許可された者が、必要なときに、中断されることなく、情報にアクセスできる状態を確保することをいう。

(12) マイナンバー利用事務系

マイナンバー利用事務（社会保障、地方税及び防災に関する事務）又は戸籍事務等に関わる情報システム及びその情報システムで取り扱うデータをいう。

(13) ＬＧＷＡＮ接続系

総合行政ネットワーク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。

3. 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、サイバー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・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、操作ミス、設定ミス、保守の不備、内部・外部監査機能の不備、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、通信の途絶等のインフラ障害からの波及等

4. 適用範囲

(1) 情報資産の範囲

本方針が対象とする情報資産は、市が保有する情報資産（教育ネットワークシステムは除く。）とする。

(2) 適用機関の範囲

本方針が適用される機関は、石垣市行政組織条例（平成18年石垣市条例第24号）第1条第2項に定める部を対象とする。

5. 職員等の遵守義務

職員等は、サイバーセキュリティの重要性について共通の認識を持ち、業務の遂行に当たり、本方針等を遵守しなければならない。

6. サイバーセキュリティ対策

情報資産を脅威から保護するために、以下のサイバーセキュリティ対策を講ずる。

(1) 組織体制

市の情報資産について、サイバー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

市の保有する情報資産をその重要性に応じて分類し、適切なサイバーセキュリティ対策を行う。

(3) 情報システム全体の強靭性の向上

サイバー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、マイナンバー利用事務（個人番号利用事務）系の情報システム、ＬＧＷＡＮ接続系の情報システム及びインターネット接続（内部）系の情報システムという三層の情報システムからなる強じん性向上対策を講じる。

(4) 物理的セキュリティ対策

情報システムの設置場所への不正な立入りの防止等、情報資産を保護するために物理的な対策を講じる。

(5) 人的セキュリティ対策

情報セキュリティに関する権限及び責任並びに遵守事項を定め、職員等に本方針の内容を周知徹底し、十分な教育及び啓発を行うために必要な対策を講じる。

(6) 技術的セキュリティ対策

情報資産を不正アクセス等から保護するために、情報資産へのアクセス制御やネットワーク管理等の技術的な対策を講じる。

(7) 運用面における情報セキュリティ対策

情報システムの監視、本方針の遵守状況の確認、(8)の業務委託と外部サービス（クラウドサービス）を利用する際のセキュリティの確保等、本方針の運用面での対策を講じる。

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の緊急時対応計画を策定する。

(8) 業務委託と外部サービス（クラウドサービス）の利用における対策

業務委託を行う場合には、委託事業者を選定し、サイバー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（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。

特にソーシャルメディアサービスの利用については、情報発信の責任者を明確にし、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た運用手順を定める。

7. サイバーセキュリティに関する監査及び自己点検の実施

本方針の遵守状況を評価・検証するため、定期的又は必要に応じてサイバーセキュリティに関する監査及び自己点検を実施し、運用改善を行い、サイバーセキュリティの向上を図る。

8. 本方針の見直し

サイバーセキュリティに関する監査及び自己点検の結果、本方針の見直しが必要となった場合又は、サイバー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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討した上で、本方針の見直しを実施する。

9. サイバーセキュリティ対策基準の策定

サイバーセキュリティ対策を実施するために、必要に応じて、具体的な遵守事項、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。

なお、当該対策基準は、公にすることにより、市行政の運営に重大な支障を及ぼすおそれがあることから、当該対策基準については、4. (1)に定める行政機関の適用範囲以外に対しては非公開とする。