○石垣市情報セキュリティ基本方針

令和4年4月1日

市長決裁

(趣旨)

第1条　この基本方針は、本市が保有するネットワーク、情報システム及びこれらに関する設備並びに情報資産（以下「対象資産」という。）について、本市が実施する情報セキュリティに関する基本的な事項を定めることにより、行政の適正かつ円滑な運営を図り、もって市政に対する市民の信頼を確保することを目的とする。

(定義)

第2条　この基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1)　コンピュータ

パーソナルコンピュータ、サーバ、ストレージ等の機器をいう。

(2)　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。

(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

情報システムで取り扱う情報で、開発及び運用に係るものを含むすべての情報をいう。

(5)　情報セキュリティ

対象資産の機密性、完全性及び可用性を維持することをいう。

(6)　情報セキュリティポリシー

この基本方針及び情報セキュリティ対策基準をいう。

(7)　機密性

対象資産にアクセスすることを認められた者だけが、対象資産にアクセスできる状態を確保することをいう。

(8)　完全性

対象資産が破壊、改ざん、消去又は不正なデータがない状態を維持し、データの正当性、正確性、一貫性等を確保することをいう。

(9)　可用性

対象資産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、対象資産にアクセスできる状態を確保することをいう。

(10)　特定個人情報

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第2条に規定する、個人番号をその内容に含む個人情報をいう。

(11)　個人番号利用事務系

個人番号利用事務系（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。

(12)　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（個人番号利用事務系を除く。）。

(13)　インターネット接続系

インターネットメール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。

(14)　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。

(15)　無害化通信

端末への画面転送やファイルの無害化処理等により、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。

(対象とする脅威)

第3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)　人による脅威（故意）

不正アクセスやウイルス攻撃等のサイバー攻撃、機器の盗難、対象資産の不正な操作や持ち出し等の故意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)　人による脅威（過失）

対象資産の管理不備、無許可ソフトウェアの使用等の規定違反、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

ト管理の不備、マネジメントの欠陥、機器故障等の過失による情報資産の漏えい・破壊・消去等

(3)　災害による脅威

地震、落雷、火災、水害等の災害によるサービス及び業務の停止、情報資産の消失等

(4)　必要資源の不足、故障等による脅威

災害の影響又はその他の原因による電力、通信、水道の途絶、交通機能の麻痺や大規模・広範囲にわたる疾病の蔓延による要員の不足、機器の故障等によるサービスや業務の停止、システム運用の機能不全等

(適用範囲)

第4条　この基本方針の適用範囲は、本市が保有する対象資産、対象資産に関する事務に携わる全ての職員、非常勤職員、臨時職員、労働者派遣事業により本市の事務に携わる者（以下「職員等」という。） 及び委託事業者とする。

(遵守義務)

第5条　前条に規定する者は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって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。

(職員等の遵守)

第6条　情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

(情報セキュリティ対策)

第7条　第3条の脅威から対象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)　組織体制

情報セキュリティ対策を推進する全庁的な組織体制の確立

(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、当該分類に基づく情報セキュリティ対策

(3)　情報システム全体の強靭性の向上

ア　個人番号利用事務系は、他の領域との通信不可、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

イ　ＬＧＷＡＮ接続系は、インターネット接続系との通信経路の分割、両システム間の無害化通信

ウ　インターネット接続系は、不正通信の監視機能の強化、県及び市のインターネットへの通信の集約、自治体情報セキュリティクラウドの導入等

(3)　物理的セキュリティ

対象資産の設置方法又は保管施設の管理についての物理的な対策

(4)　人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策

(5)　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

(6)　運用

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、外部委託を行う際の情報セキュリティの確保等、情報セキュリティポリシーの運用面の対策、対象資産への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の策定

(7)　外部サービスの利用

情報セキュリティ要件を明記した契約の締結､約款による外部サービスを利用する場合には、利用にかかる規定の整備等、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の確認

(8)　ソーシャルメディアの利用

ソーシャルメディアサービスの運用手順、発信できる情報の規定、利用するソーシャルメディアサービスごとの責任者の選定

(9)　評価・見直し

定期的な情報セキュリティ監査及び自己点検等による情報セキュリティポリシーの遵守状況の検証、定期的な情報セキュリティポリシーの見直しの実施

(情報セキュリティに関する監査及び自己点検の実施)

第8条　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に関する監査及び自己点検を実施する。

(情報セキュリティポリシーの見直し及び改定)

第９条　情報セキュリティに関する監査及び自己点検の結果又は情報セキュリティに関する状況の変化に対応するため、定期的に情報セキュリティポリシーの見直しを行い、必要に応じて改定する。

(情報セキュリティ対策基準の策定)

第10条　第5条から第8条まで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。

(情報セキュリティ実施手順の策定)

第11条　情報セキュリティ対策基準に基づき、情報セキュリティに関する対策を実施する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について石垣市情報公開条例に定める非公開情報に該当するものは非公開とする。