石垣市議会サイバーセキュリティ基本方針

令和８年３月 19 日
議　長　決　裁

（目的）

第１条　この基本方針は、石垣市議会（以下「議会」という。）が保有し、又は管理する情報資産について、サイバーセキュリティを確保するための基本的な考え方、管理体制及び実施の方向性を定めることにより、議会活動の継続性を確保し、もって市民の信頼の確保に資することを目的とする。

（適用範囲）

第２条　この基本方針は、議員及び議会が保有し、又は管理する情報資産に適用する。

２　議会事務局職員については、石垣市情報セキュリティ基本方針を適用する。

（定義）

第３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)　情報資産は、次に掲げるものをいう。

ア　議会が保有し、又は管理する情報及びデータ

イ　議会活動に使用する情報システム及びネットワーク

ウ　議員が議会活動のために利用する電子機器及びクラウドサービス

(2)　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確保するための管理的、技術的及び人的措置をいう。

(3)　インシデント

情報資産の機密性、完全性又は可用性が損なわれ、又はそのおそれがある事象をいう。

（基本理念）

第４条　議会におけるサイバーセキュリティの確保は、次に掲げる原則に基づき実施する。

(1)　多層防御の原則

(2)　最小権限の原則

(3)　リスク管理に基づく対策の実施

(4)　継続的改善（PDCA）の推進

(5)　市の情報セキュリティ対策との整合確保

(6)　情報資産の重要度に応じた適切な管理

(7)　議会活動の継続性の確保

（管理体制）

第５条　議長は、議会におけるサイバーセキュリティ確保の最高責任者とする。

２　議長は、必要に応じてサイバーセキュリティ責任者を指名し、管理体制を整備する。

３　議長は、議会が保有し、又は管理する情報資産を把握し、リスク評価を実施し、その結果に基づき必要な対策を講ずる。

４　重大なインシデントが発生した場合は、市長部局その他関係機関と連携する。

（議員の責務）

第６条　議員は、議会活動に関連して情報資産を取り扱うに当たり、次に掲げる事項を遵守する。

(1)　不正アクセス、情報漏えいその他の事故の防止に努めること。

(2)　議会が定める技術的基準及び利用規程に従うこと。

(3)　セキュリティ事故又はその疑いを認知した場合は、速やかに報告すること。

（情報資産の管理）

第７条　議会は、情報資産を重要度及び内容に応じて分類し、その区分に応じた管理措置を講ずる。

２　重要な情報資産については、特に厳格な管理を行う。

（技術的及び物理的対策の基本方針）

第８条　議会は、次に掲げる対策を基本として実施する。

(1)　外部からの不正侵入防止対策

(2)　マルウェア対策

(3)　アクセス制御及び認証の強化

(4)　ログの取得及び適切な保管

(5)　通信及び保存情報の暗号化

(6)　クラウドサービス利用時の安全確保

(7)　端末の紛失・盗難防止その他の物理的対策

(8)　必要なバックアップの実施

２　前項に掲げる対策の具体的な基準及び管理方法は、別に定める。

（教育及び訓練）

第９条　議会は、議員に対し、情報セキュリティに関する教育及び訓練を定期的に実施する。

２　議員は、前項の教育及び訓練に積極的に参加するよう努める。

（インシデント対応）
第10条　サイバーセキュリティに関するインシデントが発生した場合は、被害拡大の防止を最優先とする。
２　原因分析を行い、再発防止策を講ずる。
３　必要に応じて、市長部局その他関係機関と情報共有を行う。
（点検、監査及び見直し）
第11条　議会は、本基本方針及び関連規程の実施状況について、定期的に点検を行う。
２　必要に応じて外部専門的知見を活用する。
３　国の指針改定、重大なインシデントの発生その他必要があると認める場合は、本基本方針を見直す。
（事業継続の確保）
第12条　議会は、サイバーセキュリティ事案が発生した場合においても議会機能を維持できるよう、復旧体制及びバックアップ体制を整備する。
（委任）
第13条　この基本方針の実施に関し必要な事項は、議長が別に定める。

附　則

この方針は、令和８年４月１日から施行する。