那覇市議会情報セキュリティポリシー

序　那覇市議会情報セキュリティポリシーの構成

那覇市議会情報セキュリティポリシー(以下「議会情報セキュリティポリシー」という。)とは、本市議会が保有する情報資産に関する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ある。議会情報セキュリティポリシーは、本市議会が保有する情報資産を取り扱う議員並びに本市議会事務局の職員及び会計年度任用職員(以下「事務局職員等」という。)に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、議会情報セキュリティポリシーを一定の普遍性を備えた部分(基本方針)と情報資産を取り巻く状況の変化に依存する部分(対策基準)に分けて策定することとする。

具体的には、議会情報セキュリティポリシーを、

①議会情報セキュリティ基本方針

②議会情報セキュリティ対策基準

の２階層に分け、それぞれを策定することとする。また、議会情報セキュリティポリシーに基づき、情報システム毎の具体的な議会情報セキュリティ対策の実施手順として議会情報セキュリティ実施手順を策定することとする(下表参照)。なお、議会情報セキュリティポリシー(議会情報セキュリティ対策基準)及び議会情報セキュリティ実施手順は、公開することにより本市の議会運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

議会情報セキュリティポリシーの構成

文 書 名		内 容
議会情報セキュリティポリシー	議会情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	議会情報セキュ	議会情報セキュリティ基本方針を実行

	リティ対策基準	に移すための全ての情報システムに共通の情報セキュリティ対策の基準
議会情報セキュリティ実施手順		情報システム毎に定める議会情報セキュリティ対策基準に基づいた具体的な実施手順

議会情報セキュリティ基本方針

1　目的

本市議会の各情報システムが取り扱う情報には、市民の個人情報のみならず議会運営上重要な情報など、部外に漏えい等した場合には重大な結果を招く情報が含まれている。

したがって、これらの情報及び情報を取り扱う情報システムを様々な脅威から防御することは、市民の財産、プライバシー等を守るためにも、また、議会の安定的な運営のためにも必要不可欠である。

そのため、本市議会の情報資産の機密性、完全性及び可用性を維持するための対策（情報セキュリティ対策）を整備するために議会情報セキュリティポリシーを定めることとし、このうち、議会情報セキュリティ基本方針については本市議会の情報セキュリティ対策の基本的な方針として、また、地方自治法（昭和22年法律第67号）第244条の６第１項に規定するサイバーセキュリティを確保するための方針として、議会情報セキュリティポリシーの対象、位置付け等を定めるものとする。

なお、議員が、議員活動（会派・議員個人による調査研究等）の中で取得した情報資産は、議会情報セキュリティ基本方針の対象外とする。

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（ハードウェア及びソフトウェア）をいう。

(2)　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。

(3)　情報資産

ネットワーク及び情報システムの開発と運用に係る全てのデータ並びにネットワーク及び情報システムで取り扱う全ての情報をいう。

なお、情報資産には、紙等の有体物に出力された情報も含むものとする。

(4)　情報セキュリティ

情報資産の機密の保持及び正確性､完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

(5)　機密性(confidentiality)

情報にアクセスすることが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。

(6)　完全性(integrity)

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。

(7)　可用性(availability)

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、情報にアクセスできる状態を確保することをいう。

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、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、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

4　適用範囲

(1)　組織の範囲

本基本方針が適用される機関は那覇市議会とする。那覇市議会には次の機関を含む。

①　那覇市議会委員会条例（昭和 47 年 5 月 15 日条例第 83 号）第２条、第４条、第６条及び第７条に規定する委員会

②　那覇市議会会議規則（昭和47年5月11日議会規則第3号）第166条に規定する協議等の場

③　その他議会が公務のために設置する組織

④　那覇市議会事務局設置条例(昭和47年那覇市条例第84号)第1条に規定する那覇市議会事務局

(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。

なお、執行部と同一の設備等を事務局職員等が利用する場合は、本基本方針における情報資産の範囲に含めず、執行部の基本方針の規程を適用する。

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（以下「設備等」という。）

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

5　議員及び事務局職員等及び外部委託事業者の義務

議長をはじめとして本市議会が保有する情報資産に関する業務に携わる議員及び事務局職員等並びに外部委託事業者は、情報セキュリティの重要性について共通の認識をもつとともに業務の遂行に当たって議会情報セキュリティポリシー及び議会情報セキュリティ実施手順を遵守する義務を負うものとする。

6　情報セキュリティ対策

上記３で示した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ものとする。

(1)　組織体制

本市議会の情報資産について、議員及び事務局職員等が率先して情報セキュ

リティ対策を推進･管理するための組織体制を確立するものとする。

(2)　情報資産の分類と管理

本市議会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)　物理的セキュリティ対策

サーバ等、情報システム室等、通信回線等及び事務局職員等のパソコン等の管理について、物理的な対策を講じる。

(4)　人的セキュリティ対策

情報セキュリティに関する権限や責任を定め､議員及び事務局職員等並びに外部委託事業者に議会情報セキュリティポリシーの内容を周知徹底する等､十分な教育及び啓発が行われるよう必要な対策を講じる。

(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を講じる。

(6)　運用

情報システムの監視、議会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、議会情報セキュリティポリシーの運用面の対策を講じるものとする。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。

(7)　業務委託と外部サービス（クラウドサービス）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（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。

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サービスごとの責任者を定める。

(8)　評価・見直し

議会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、運用改善を行い情報セキュリティの向上を図る。議会情報セキュリティポリシーの見直しが必要な場合は、適宜議会情報セキュリティポリシーの見直しを行う。

7　議会情報セキュリティ対策基準の策定

本市の様々な情報資産について、上記６の情報セキュリティ対策を実施するため、具体的な遵守すべき事項及び判断等の基準を定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した議会情報セキュリティ対策基準を策定するものとする。なお、議会情報セキュリティ対策基準は、公開することにより本市の議会運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

8　議会情報セキュリティ実施手順の策定

議会情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対応する議会情報セキュリティ対策基準に基づき、議会情報セキュリティ実施手順を策定するものとする。

なお、議会情報セキュリティ実施手順は、公開することにより本市の議会運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

9　情報セキュリティ監査及び自己点検の実施

議会情報セキュリティポリシーが遵守されていることを検証するため、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する。

10　議会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、議会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、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、リスクを検討したうえで、議会情報セキュリティポリシーを見直す。

付　則

この要綱は、令和８年４月１日から施行する。