鳴門市議会情報セキュリティポリシー

鳴門市議会情報セキュリティポリシーは、鳴門市議会（以下「議会」という。）が所掌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を総称する。

情報セキュリティを取り巻く状況は、技術の進歩等により急速に変化していることから、これらの変化に柔軟に対応するため、鳴門市議会情報セキュリティポリシーは、一定の普遍性を備えた部分である鳴門市議会情報セキュリティ基本方針と、情報資産を取り巻く状況の変化に依存する部分である鳴門市議会情報セキュリティ対策基準に区分して策定するものとする。

また、鳴門市議会情報セキュリティポリシーのための方針に基づき、ネットワーク及び情報システム毎の具体的な情報セキュリティ対策の実施手順として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）。

文　書　名		内　容
鳴門市議会情報セキュリティポリシー	鳴門市議会情報セキュリティ基本方針	鳴門市議会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。
	鳴門市議会情報セキュリティ対策基準	鳴門市議会情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の鳴門市議会情報セキュリティ対策の基準。
情報セキュリティ実施手順		ネットワーク及び情報システム毎に定める鳴門市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。

鳴門市議会情報セキュリティ基本方針

１　目的

鳴門市議会情報セキュリティ基本方針（以下「本基本方針」という。）は、議会が保有又は管理する情報資産の機密性、完全性及び可用性を維持するため、議会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。

２　用語の定義

本基本方針において使用する用語の定義は、次に掲げるところによる。

（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。

（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。

（4）　鳴門市議会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ていない状態を確保することをいう。

（7）　可用性

情報にアクセスを認められた者が、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

議会の情報資産に対する脅威として、次に掲げる事項を想定し、必要な情報セキュリティ対策を講ずるものとする。

（1）　不正アクセス、ウイルス感染、サービス妨害攻撃等のサイバー攻撃又は部外者の侵入等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停滞又は機能不全

（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）　本基本方針が適用される機関

議会

（2）　情報資産の範囲

本基本方針が対象とする議会が議会活動のため保有する情報資産は、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そ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、ネットワーク図等の関連文書

5　議員の遵守義務

議員は、情報セキュリティの重要性を認識し、鳴門市議会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　職員等の遵守義務

事務局職員及び会計年度任用職員（以下「職員等」という。）は、鳴門市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に従わなければならない。

7　組織体制

議会の情報セキュリティ対策を推進するため議会の組織体制を確立する。

８　情報資産の分類と管理

情報資産は、その機密性、完全性及び可用性の重要度に応じて分類し、分類に応じた管理を行う。

９　物理的セキュリティ

端末及び記録媒体等について、盗難防止措置等の物理的対策を講じる。

１０　人的セキュリティ

議員に対し、情報セキュリティに関する教育及び啓発を行う等の人的な対策を講じる。

１１　技術的セキュリティ

アクセス制御、不正プログラム対策、不正アクセス防止、暗号化通信の確保等の技術的対策を講じる。

１２　運用及び緊急時対応

情報システムの監視、ログ管理、セキュリティポリシーの遵守状況確認等の運用管理を実施するとともに、情報資産に対するセキュリティ侵害が発生した場合には、速やかに市の関連部局と連携し対応する。

１３　業務委託の利用

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、必要に応じて契約に基づき措置を講じる。

１４　外部サービス（クラウドサービス）の利用

外部サービス（クラウドサービス）を利用する場合には、利用にかかる規定を整備し対策を講じる。

１５　情報セキュリティ監査及び自己点検

情報セキュリティポリシーの遵守状況を確認するため、定期的に監査及び自己点検を実施する。

１６　評価・見直し

情報セキュリティ監査及び自己点検の結果又は社会情勢・技術環境の変化により、必要があると認められるときは、本基本方針を見直すものとする。

１７　鳴門市議会情報セキュリティポリシー見直し

情報セキュリティ監査及び自己点検の結果、鳴門市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となった場合には、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、鳴門市議会情報セキュリティポリシーを見直す。

１８　鳴門市議会情報セキュリティ対策基準の策定

本基本方針に基づき、具体的な遵守事項及び判断基準を定めた鳴門市議会情報セキュリティ対策基準を策定する。

１９　情報セキュリティ実施手順の策定

鳴門市議会情報セキュリティ対策基準に基づき、具体的な運用手順を定めた情報セキュリティ実施手順を別に定める。

なお、情報セキュリティ実施手順は、公にすることにより議会の運営に重大な支障を及ぼすおそれがあるため、非公開とする。

鳴門市議会情報セキュリティ対策基準

1　目的

鳴門市議会情報セキュリティ対策基準(以下「本対策基準」という。）は、鳴門市議会情報セキュリティ基本方針を実行に移すため、議員における情報資産に関する情報セキュリティ対策の基準を定めたものである。

2　対象者

本対策基準の対象者は議員とする。

3　用語の定義

（1）　情報資産

文書、電子データ、システム、記録媒体等のうち、議会が議会活動のため保有又は管理するものをいう。

（2）　インシデント

情報資産に対する漏えい、紛失、破壊、不正利用、改ざんなどのセキュリティ上の問題が発生、またはそのおそれがある事象のことをいう。

4　組織体制

（1）　統括情報セキュリティ責任者

① 議会に統括情報セキュリティ責任者（以下「統括責任者」という。）を置き、議会事務局長をもってこれに充てる。

② 統括責任者は、議会が保有するネットワーク及び情報システムの開発、設定の変更、運用、見直し等及び情報セキュリティ対策に関する権限及び責任を有し、情報セキュリティの推進及び事故対応の総括を行う。

（2）　情報セキュリティ担当者

議会に情報セキュリティ担当者を置き、統括責任者の指示等に従い、情報システムの開発並びに設定、運用、更新等の日常的な作業及び利用者への周知啓発を行う。

（3）　クラウドサービス利用における組織体制

クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立しなければならない。

5　情報資産の分類

議会における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に

応じ取扱制限を行うものとする。

ア　機密性による情報資産の分類

分類	分類基準	取扱制限
自治体 機密性 ３Ａ	議会活動で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」（平成 23 年４月１日内閣総理大臣決定）に定める秘密文書に相当する文書	・支給された 端末以外での作業の原則禁止（ 自治体 機密性３の情報資産に対して） ・必要以上の複製及び配布禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼できるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
自治体 機密性 ３Ｂ	議会活動で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	
自治体 機密性 ３Ｃ	議会活動で取り扱う情報資産のうち、自治体機密性３Ｂ以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	
自治体 機密性２	議会活動で取り扱う情報資産のうち、自治体機密性３に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
自治体 機密性１	自治体機密性２又は 自治体 機密性３の情報資産以外の情報資産	―

イ　完全性による情報資産の分類

分類	分類基準	取扱制限

自治体 完全性２	議会活動で取り扱う情報資産のうち、改ざん、誤謬又は破損により、住民 の権利が侵害される又は議会活動の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
自治体 完全性１	自治体完全性２の情報資産以外の情報資産	―

ウ　可用性による情報資産の分類

分類	分類基準	取扱制限
自治体 可用性２	議会活動で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は議会活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
自治体 可用性１	自治体可用性２の情報資産以外の情報資産	―

6　保管・廃棄

各分類２以上の情報資産については、適切に保管し不要となった場合は、復元不可能な方法で廃棄する。

7　端末の管理及び運用等

公用の会議用タブレット型端末の管理及び運用については、別に定める情報セキュリティ実施手順による。なお、公用のタブレット型端末でインターネットに接続する場合は、市が管理する専用 Wi-Fi を利用しなければならない。

8　会議システムの管理及び運用

会議システムの管理及び運用は、別に定める情報セキュリティ実施手順による。

9　啓発

統括責任者は、適宜、情報セキュリティに関する研修を実施する。

１０　監査・自己点検

定期的に監査・自己点検を実施し、改善が必要な事項を報告・是正する。

１１　インシデントへの対応

情報セキュリティインシデントが発生した場合は、直ちに統括責任者に報告し、市の関連部局と連携し、被害拡大防止措置等を講じる。

令和８年２月２６日　策定