竹田市議会
情報セキュリティ基本方針

策定日：令和８年３月１７日

竹田市議会

情報セキュリティ基本方針　目次

情報セキュリティ基本方針

１　目的

竹田市議会情報セキュリティ基本方針（以下「基本方針」という。）は、竹田市議会（以下「議会」という）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。

なお、竹田市議会議員（以下「議員」という）個人が、議員活動の中で取得した情報資産は、基本方針の対象外のとする。

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

コンピュータおよびネットワークおよ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）　情報セキュリティポリシー

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ものだけが、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

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

情報にアクセスすることを認められたものが、必要な時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。

（８）　無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、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。

３　対象とする脅威

竹田市議会事務局職員（以下「事務局職員」という。）は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、ウィルス攻撃、サービス不能攻撃など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、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および業務の停止等

①　大規模・広範囲にわたる疾病による要因不足に伴うシステム運用の機能不全等

②　電力供給の途絶、通信の途絶、水道供給の途絶などのインフラの障害からの波及等

４　適用範囲

（１）　対象者

基本方針の対象は、議会が保有する情報資産を取り扱う議員及び事務局職員とする。

（２）　情報資産の範囲

基本方針における議会が保有する情報資産の対象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こ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及びネットワーク図等のシステム関連文書

５　遵守義務

議員及び事務局職員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基本方針及び「竹田市議会タブレッ

ト型情報端末機使用基準」等の議会で策定した情報セキュリティに関する個別の基準（以下「個別基準」という。）を実施しなければならない。

６　情報セキュリティ対策

上記３の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。

（１）　組織体制

議会が保有する情報資産について、情報セキュリティ対策を推進する議会組織体制を確立する。

（２）　情報資産の分類と管理

議会が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

サーバ、電算室、通信回線及びパソコン、タブレット端末等の管理について、物理的な対策を講じる。

（４）　人的セキュリティ

情報セキュリティに関し、議員及び事務局職員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を講じる。

①　情報資産の持ち出し

・議会が保有する情報資産は、市が貸与する端末以外へ転送しない。ただし、統括情報セキュリティ責任者が許可した場合はこの限りではない。

②　ソフトウェアの仕様

・市から貸与された端末で、無許可のソフトウェアや外部サービスを利用しない。

③　内部不正の対策

・市から貸与された端末は、議会関係者以外が閲覧できない環境で利用する。

④　機器廃棄

・コンピュータ等の機器を廃棄等する場合は、機器内部の記憶装置の初期化処理だけでなく、必ず記録領域の消磁（磁気消去）や記憶装置の物理的破壊等によるデータ復元が不可能な措置を行うこと。また、

機器の廃棄等を委託する場合は、破砕証明等を委託事業者と取り交わすこと。

・リース返却する場合は、上記の措置が講じられたことを証明するデータ消去に係る確認書をリース元事業者と取り交わすこと。

（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。

①　不正アクセス

・不正アクセスを防ぐため、端末利用時はユーザー認証を行う。

・不正に操作された恐れがある場合はアクセスログ・操作ログ等の調査及び分析を行う。

②　ウィルス対策

・コンピュータには、ウィルス対策ソフトを導入する。

・ウィルス対策ソフトの実行ファイルやパターンファイルは、最新のバージョンに更新する。

（７）　業務継続計画（ＢＣＰ）

①　風水害、地震、火山噴火、事故災害等による業務の停止等の対策

・竹田市議会業務継続計画（議会ＢＣＰ）に従い対応する。

・システムが停止した場合、竹田市議会災害対策会議と竹田市災害対策本部と連携し復旧対応を行う。

②　大規模感染症等による要員不足に伴うシステム運用の機能不全等の対策

・竹田市業務継続計画（ＢＣＰ）（以下「市ＢＣＰ」という。）に従い対応する。

③　電力、通信、水道供給の途絶等のインフラ障害に係る対策

・市ＢＣＰに従い対応する。

（８）　運用

情報システムの監視、基本方針や個別基準の遵守状況の確認、業務委託を行う際のセキュリティ確保など、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は市の策定する緊急時対応計画を準用し、迅速かつ適正に対応する。

（９）　業務委託と外部サービス（クラウドサービス）の利用

①　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。

② 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。

③ 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ごとの責任者を定める。

（１０）評価・見直し

基本方針や個別基準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。基本方針や個別基準の見直しが必要な場合は、適宜見直しを行う。

7　情報セキュリティ監査及び自己点検の実施

事務局職員は、基本方針や個別基準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する。

8　基本方針等の見直し

事務局職員は情報セキュリティ監査及び自己点検の結果、基本方針や個別基準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、基本方針や個別基準の見直しを行う。

9　情報セキュリティ対策基準の策定

議会は上記６、７及び８に規定する対策等を実施するために、必要に応じて具体的な遵守事項及び判断基準等を情報セキュリティ対策基準として策定する。

１０情報セキュリティ実施手順の策定

議会は、竹田市情報セキュリティ対策基準に基づき、情報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手順を定めた情報セ

キュリティ実施手順を策定する。

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