豊前市議会
情報セキュリティポリシー

豊前市議会

令和８年３月９日制定

目　次

第１章　情報セキュリティ基本方針
１　目的 …… １
２　定義 …… １～２
（１）　ネットワーク
（２）　情報システム
（３）　情報セキュリティ
（４）　情報セキュリティポリシー
（５）　機密性
（６）　完全性
（７）　可用性
（８）　マイナンバー利用事務系（個人番号利用事務系）
（９）　ＬＧＷＡＮ接続系
(10)　インターネット接続系
(11)　通信経路の分割
(12)　無害化通信
３　適用範囲 …… ２
（１）　機関の範囲
（２）　情報資産の範囲
４　対象とする脅威 …… ２～３
５　議員の遵守義務 …… ３
６　情報セキュリティ対策 …… ３～４
（１）　組織体制
（２）　情報資産の分類と管理
（３）　物理的セキュリティ
（４）　人的セキュリティ
（５）　技術的セキュリティ
（６）　運用
（７）　外部サービス（クラウドサービス）の利用
（８）　評価・見直し
７　情報セキュリティ監査及び自己点検の実施 …… ４
８　情報セキュリティポリシーの見直し …… ４
９　情報セキュリティ対策基準の策定 …… ４
10　情報セキュリティ実施手順の策定 …… ４～５

第２章　情報セキュリティ対策基準
１　組織体制 …… ６～７
（１）　最高情報セキュリティ責任者
（２）　統括情報セキュリティ責任者
（３）　情報セキュリティ責任者
（４）　情報セキュリティ管理者
（５）　情報システム管理者
（６）　情報システム担当者
（７）　情報セキュリティに関する重要な事項
（８）　兼務の禁止
（９）　ＣＳＩＲＴの設置・役割
２　情報資産の分類と管理 …… ８～11
（１）　情報資産の分類
（２）　情報資産の管理
３　物理的セキュリティ …… 11
４　人的セキュリティ …… 12～14
４．１　議員の遵守事項 …… 12
（１）　議員の遵守事項
（２）　情報セキュリティポリシー等の掲示
４．２　研修・訓練 …… 13
（１）　情報セキュリティに関する研修・訓練
（２）　研修計画の策定及び実施
（３）　緊急時対応訓練
（４）　研修・訓練への参加
４．３情報セキュリティインシデントの報告 …… 13～14
（１）　庁内での情報セキュリティインシデントの報告
（２）　住民等外部からの情報セキュリティインシデントの報告
（３）　情報セキュリティインシデント原因の究明・記録、再発防止等
４．４　パスワードの管理 …… 14
（１）　ＩＤの取扱い
（２）　パスワードの取扱い
５　技術的セキュリティ …… 15～18
５．１　コンピュータ及びネットワークの管理 …… 15～17
（１）　ログの提供
（２）　電子メールの利用制限
（３）　暗号化

（４）　無許可ソフトウェアの導入等の禁止
（５）　機器構成の変更の制限
（６）　他のネットワークへの接続の禁止
（７）　議会活動以外の目的でのウェブ閲覧の禁止
（８）　Ｗｅｂ会議サービスの利用時の対策
（９）　ソーシャルメディアサービスの利用
５．２　アクセス制御 …… 17
（１）　利用者ＩＤの取扱い
（２）　議員による外部からのアクセス等の制限
５．３　不正プログラム対策 …… 17～18
５．４　議員による不正アクセス対策 …… 18
５．５　情報セキュリティに関する情報の共有 …… 18
６　運用 …… 18～20
６．１　情報セキュリティポリシーの遵守状況の確認 …… 18～19
（１）　遵守状況の確認及び対処
（２）　貸与されているパソコン等の利用状況調査
（３）　議員の報告義務
６．２　法令遵守 …… 19
６．３　違反時の対応 …… 19～20
７　外部サービス（クラウドサービス）の利用 …… 20～22
７．１　外部サービス（自治体機密性２以上の情報を取り扱う場合）20～21
（１）　クラウドサービスの選定に係る運用規程の整備
（２）　クラウドサービスの利用に係る運用規程の整備
（３）　クラウドサービスの選定
（４）　クラウドサービスの利用に係る調達・契約
（５）　クラウドサービスの利用承認
（６）　クラウドサービスを利用した情報システムの導入・構築時の対策
（７）　クラウドサービスを利用した情報システムの運用・保守時の対策
（８）　クラウドサービスを利用した情報システムの更改・廃棄時の対策
７．２　外部サービス（自治体機密性２以上の情報を取り扱わない場合）21～22
（１）　クラウドサービスの利用に係る規定の整備
（２）　クラウドサービスの利用における対策の実施
８　評価・見直し …… 22～24
８．１　監査 …… 22～23
（１）　実施方法

（２）　監査実施計画の立案及び実施への協力
（３）　報告
（４）　監査結果への対応
（５）　情報セキュリティポリシー及び関係規程等の見直し等への活用
８．２　自己点検 …… 23
（１）　実施方法
（２）　報告
（３）　自己点検結果の活用
８．３　情報セキュリティポリシー及び関係規定等の見直し …… 24

第１章　情報セキュリティ基本方針

１　目的

本基本方針は、豊前市議会が保有する情報資産に係る機密性、完全性及び可用性を維持するため、豊前市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　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

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。

（８）　マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（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。

（９）　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（マイナンバー利用事務系を除く。）。

(10)　インターネット接続系

インターネットメール、ホームページ管理システム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。

(11)　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。

(12)　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　適用範囲

本基本方針が対象とする情報資産は、次のとおりとする。

（１）　機関の範囲

本基本方針が適用される機関は、豊前市議会とする。

（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。ただし、豊前市議会議員（以下「議員」という。）が議会活動により入手ができるものに限る。

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

④ 議員が資料請求で入手した情報

４　対象とする脅威

上記３に示しているが、本基本方針が対象とする情報資産の範囲は、議員が議会活動により入手できるものに限定されており、また、豊前市議会は、ネットワーク及び情報システムの構築並びにネットワーク及び情報システムを用いたサービスの提供を実施しておらず、ネットワーク及び情報システム並びにこれらに関連する設備等の導入・維持管理等も行っていない。よって、主に議員が、豊前市（以下「本市」という。）で管理するネットワーク及び情報システム並びにこれらに関連する設備等を利用することについて、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、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、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

※　豊前市議会におけるネットワーク及び情報システム並びにこれらに関連する設備の導入・保守契約等に関する事務は、これまでと同様に、議会事務局で行う。なお、議会事務局は、本市が定める情報セキュリティポリシーの適用範囲に含まれているため、同ポリシーに従いそれらの事務を行うことになる。

５　議員の遵守義務

議員は、情報セキュリティの重要性について共通の認識を持ち、議会活動に当たって、本市より議員に貸与されているパソコン及び電磁的記録媒体（以下「貸与されているパソコン等」という。）を使用する場合は、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　情報セキュリティ対策

上記４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

豊前市議会の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。なお、本市が定める情報セキュリティ対策基準（以下「本市情報セキュリティ対策基準」という。）の組織体制を基本とし、豊前市議会を本市情報セキュリティ対策基準における内部部局と同じ位置付けとする。

（２）　情報資産の分類と管理

豊前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

貸与されている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

情報セキュリティに関し、議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。

（５）　技術的セキュリティ

貸与されているパソコン等の管理、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

情報セキュリティポリシーの遵守状況の確認、貸与されているパソコン等を使用する際のセキュリティ確保等、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。

（７）　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

情報セキュリティポリシーの遵守状況を検証するため、本市情報セキュリティ監査統括責任者が定期的又は必要に応じて実施する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。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

７　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、本市情報セキュリティ監査統括責任者が定期的又は必要に応じて実施する情報セキュリティ監査の受入れ及び自己点検を実施する。

８　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、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、保有する情報の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

９　情報セキュリティ対策基準の策定

豊前市議会における上記６、７及び８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。

10　情報セキュリティ実施手順の策定

情報セキュリティ対策基準を策定した場合は、当該対策基準に基づき、情

報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を、必要に応じて策定するものとする。なお、情報セキュリティ実施手順は、公にすることにより豊前市議会の情報セキュリティ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。

第２章　情報セキュリティ対策基準

本対策基準は、情報セキュリティ基本方針を実行に移すための、豊前市議会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。

１　組織体制

本市情報セキュリティ対策基準で定める組織体制を基本とし、豊前市議会を同組織体制の内部部局と同じ位置付けとする。

（１）　最高情報セキュリティ責任者（ＣＩＳＯ:Ｃｈｉｅｆ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｓｅｃｕｒｉｔｙ　Ｏｆｆｉｃｅｒ）

本市情報セキュリティ対策基準でＣＩＳＯと定める者（以下「ＣＩＳＯ」という。）とし、役割、権限等についても本市情報セキュリティ対策基準で定めるものと同様とする。

（２）　統括情報セキュリティ責任者

本市情報セキュリティ対策基準で統括情報セキュリティ責任者と定める者（以下「本市統括情報セキュリティ責任者」という。）とし、役割、権限等についても本市情報セキュリティ対策基準で定めるものと同様とする。

（３）　情報セキュリティ責任者

①　議会事務局長を情報セキュリティ責任者とする。

②　情報セキュリティ責任者は、豊前市議会の情報セキュリティ対策に関する統括的な権限及び責任を有する。

③　情報セキュリティ責任者は、豊前市議会において所有している情報システムにおける設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

④　情報セキュリティ責任者は、豊前市議会において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約を行う。また、情報セキュリティ責任者は、議員に対する教育、訓練、助言及び指示を行う。

なお、議会事務局長は、本市情報セキュリティ対策基準においても本市の情報セキュリティ責任者となるが、本市内部の情報セキュリティの知識を持っている議員がいないため、本市情報セキュリティ対策基準と同一レベルの基準を確保する目的で、議会事務局長を本対策基準においても情報セキュリティ責任者とする。

（４）　情報セキュリティ管理者

①　議長を情報セキュリティ管理者とする。

②　情報セキュリティ管理者は、豊前市議会の情報セキュリティ対策に関する権限及び責任を有する。

③　情報セキュリティ管理者は、豊前市議会において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、情報セキュリティ責任者、本市統括情報セキュリティ責任者及びＣＩＳＯへ速やかに報告を行い、 指示を仰がなければならない。

（５）　情報システム管理者

本市情報セキュリティ対策基準で情報システム管理者と定める者（以下「本市情報システム管理者」という。）とし、役割、権限等についても本市情報セキュリティ対策基準で定めるものと同様とする。

（６）　情報システム担当者

本市情報セキュリティ対策基準で情報システム担当者と定める者とし、役割、権限等についても本市情報セキュリティ対策基準で定めるものと同様とする。

（７）　情報セキュリティに関する重要な事項

豊前市議会の情報セキュリティ対策を統一的に実施するため、議会運営委員会において、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。

（８）　兼務の禁止

①　情報セキュリティ対策の実施において、止むを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

②　情報セキュリティ監査の実施において、止むを得ない場合を除き、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

（９）　ＣＳＩＲＴの設置・役割

本市情報セキュリティ対策基準で設置されたＣＳＩＲＴを本対策基準のＣＳＩＲＴとし、役割、権限等についても本市情報セキュリティ対策基準で定めるものと同様とする。

２　情報資産の分類と管理

（１）　情報資産の分類

本市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。

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	行政事務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	・貸与されているパソコン等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付禁止 ・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 ・信頼の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	行政事務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	行政事務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	行政事務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	

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	行政事務で取り扱う情報資産のうち、改ざん、誤り又は破損により、住民の権利が侵害される又は行政事務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	・原則取扱い禁止
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	

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	行政事務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行政事務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	・原則取扱い禁止
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	

（２）　情報資産の管理

①　管理責任

（ア）　情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

（イ）　情報セキュリティ管理者は、情報資産が複製又は伝送された場合には、複製等された情報資産も（１）の分類に基づき管理しなければならない。

②　情報資産の分類の表示

議員は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

③　情報の作成

（ア）　議員は、議会活動に必要のない情報を貸与されているパソコン等で作成してはならない。

（イ）　貸与されているパソコン等で情報を作成する議員は、情報の作成時に（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

（ウ）　貸与されているパソコン等で情報を作成する議員は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、貸与されているパソコン等の当該情報を消去しなければならない。

④　情報資産の入手

（ア）　本市職員が作成した情報資産を入手した議員は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

（イ）　本市職員以外の者が作成した情報資産を入手した議員は、（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

（ウ）　情報資産を入手した議員は、入手した情報資産の分類が不明な場合、情報セキュリティ責任者に判断を仰がなければならない。

⑤　情報資産の利用

（ア）　情報資産を利用する議員は、議会活動以外の目的に情報資産を利用してはならない。

（イ）　情報資産を利用する議員は、情報資産の分類に応じ、適正な取扱いをしなければならない。

（ウ）　情報資産を利用する議員は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

⑥　情報資産の保管

（ア）　議員は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

（イ）　議員は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

（ウ）　議員は、利用頻度が低い電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。

（エ）　議員は、自治体機密性２以上の情報を記録した電磁的記録媒体を保管する場合、施錠可能な場所に保管しなければならない。

⑦　情報の送信

電子メール等により自治体機密性２以上の情報を貸与されているパソコン等から送信する議員は、必要に応じ、パスワード等による暗号化を行わなければならない。

⑧　情報資産の運搬

（ア）　車両等により自治体機密性２以上の情報資産を運搬する議員は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

（イ）　自治体機密性２以上の情報資産を運搬する議員は、情報セキュリティ責任者に許可を得なければならない。

⑨　情報資産の提供・公表

（ア）　議員は、自治体機密性２以上の情報資産を外部に提供してはならない。

（イ）　議員は、住民に公開する情報資産について、完全性を確保しなければならない。ただし、この完全性については、この情報資産を入手した状態を確保するものとする。

⑩　情報資産の廃棄等

（ア）　情報資産の廃棄を行う議員は、貸与されているパソコン等及びその他情報を記録している電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。

（イ）　情報資産の廃棄を行う議員は、行った処理について、日時及び処理内容を記録しなければならない。

（ウ）　情報資産の廃棄を行う議員は、情報セキュリティ責任者の許可を得なければならない。

３　物理的セキュリティ

情報セキュリティ責任者は、盗難防止のため、貸与されているパソコン等の使用時以外の施錠管理等の物理的措置を講じなければならない。議員は、情報が保存される必要がなくなった時点で速やかに貸与されているパソコン等に記録した情報を消去しなければならない。

４　人的セキュリティ

４．１　議員の遵守事項

（１）　議員の遵守事項

①　情報セキュリティポリシー等の遵守

議員は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ責任者に相談し、指示を仰がなければならない。

②　議会活動以外の目的での使用の禁止

議員は、議会活動以外の目的で情報資産の外部への持ち出し、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

③　貸与されているパソコン等の持ち出し

議員は、貸与されているパソコン等及び情報資産を外部に持ち出す場合には、情報セキュリティ責任者の許可を得なければならない。

④　持ち出しの記録

情報セキュリティ責任者は、貸与されているパソコン等の持ち出しについて、記録を作成し、保管しなければならない。

⑤　貸与されているパソコン等におけるセキュリティ設定変更の禁止

議員は、貸与されているパソコン等のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ責任者の許可なく変更してはならない。

⑥　貸与されているパソコン等の管理

議員は、貸与されているパソコン等及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ責任者の許可なく情報を閲覧されることがないように、離席時のパソコン等のロックや電磁的記録媒体、文書等を容易に閲覧されない場所へ保管するなど、適正な措置を講じなければならない。

⑦　辞職等の遵守事項

議員は、辞職等により議員でなくなった場合には、議会活動で入手した自治体機密性２以上の情報資産を返却しなければならない。また、その後も議会活動で知り得た自治体機密性２以上の情報資産を漏らしてはならない。

（２）　情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、議員が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

４．２　研修・訓練

（１）　情報セキュリティに関する研修・訓練

情報セキュリティ責任者は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

（２）　研修計画の策定及び実施

① 情報セキュリティ責任者は、ＣＩＳＯが策定した情報セキュリティに関する研修計画に基づき、研修計画を策定する。

② 情報セキュリティ管理者は、新たに議員になった者を対象とする情報セキュリティに関する研修を実施しなければならない。

③ 研修は、情報セキュリティ管理者及び議員に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

④ 情報セキュリティ責任者は、豊前市議会の実施状況を記録し、本市統括情報セキュリティ責任者に対して、報告しなければならない。

（３）　緊急時対応訓練

情報セキュリティ責任者は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

（４）　研修・訓練への参加

議員は、定められた研修・訓練に参加しなければならない。

４．３　情報セキュリティインシデントの報告

（１）　庁内での情報セキュリティインシデントの報告

① 議員は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ責任者に報告しなければならない。

② 報告を受けた情報セキュリティ責任者は、速やかに本市統括情報セキュリティ責任者及び本市情報セキュリティ対策基準で定める情報セキュリティに関する統一的な窓口（以下「情報セキュリティに関する統一的な窓口」という。）に報告しなければならない。

③ 情報セキュリティ責任者は、報告のあった情報セキュリティインシデントについて、ＣＩＳＯに報告しなければならない。

（２）　住民等外部からの情報セキュリティインシデントの報告

① 議員は、本市が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告

を受けた場合、情報セキュリティ責任者に報告しなければならない。

② 報告を受けた情報セキュリティ責任者は、速やかに本市統括情報セキュリティ責任者、本市情報システム管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

③ 情報セキュリティ責任者は、当該情報セキュリティインシデントについて、必要に応じてＣＩＳＯに報告しなければならない。

（３） 情報セキュリティインシデント原因の究明・記録、再発防止等

ＣＩＳＯが、情報セキュリティインシデントについて再発防止策を実施するために必要な措置を指示した場合、情報セキュリティ責任者及び情報セキュリティ管理者は、その指示内容を豊前市議会で実施しなければならない。

４．４ パスワードの管理

（１） ＩＤの取扱い

議員は、自己の管理するＩＤに関し、次の事項を遵守しなければならない。

① 自己が利用しているＩＤは、他人に利用させてはならない。

② 共用ＩＤを利用する場合は、共用ＩＤの利用者以外に利用させてはならない。

（２） パスワードの取扱い

議員は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

① パスワードは、他者に知られないように管理しなければならない。

② パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

③ 共用のものを除き、パスワードは十分な長さとし、文字列は想像しにくいもの（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）にしなければならない。

④ パスワードが流出したおそれがある場合には、情報セキュリティ責任者に速やかに報告し、パスワードを速やかに変更しなければならない。

⑥ 仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。

⑦ 貸与されているパソコン等に、パスワードを記憶させることで、パスワードの入力なしに認証を可能とする設定は行ってはならない。

⑧ 職員等間でパスワードを共有してはならない（ただし、共用ＩＤに対するパスワードは除く）。

５　技術的セキュリティ

５．１　コンピュータ及びネットワークの管理

（１）　ログの提供

議員は、本市統括情報セキュリティ責任者及び本市情報システム管理者から、貸与されているパソコン等のログの提供を求められた場合は、これに応じなければなければならない。

（２）　電子メールの利用制限

① 議員は、貸与されているパソコン等から自動転送機能を用いて、電子メールを転送してはならない。

② 議員は、貸与されているパソコン等から議会活動に必要のない送信先に電子メールを送信してはならない。

③ 議員は、貸与されているパソコン等から複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

④ 議員は、貸与されているパソコン等から自治体機密情報２以上の情報電子メールを誤送信した場合、情報セキュリティ責任者に報告しなければならない。

（３）　暗号化

① 議員は、情報資産の分類により定めた取扱制限に従い、貸与されているパソコン等から外部に送るデータの機密性又は完全性を確保することが必要な場合には、ＣＩＳＯが定めた電子署名、パスワード等による暗号化等、セキュリティを考慮して、送信しなければならない。

② 議員は、貸与されているパソコン等から外部に送るデータの暗号化を行う場合に、ＣＩＳＯが定める以外の方法を用いてはならない。また、ＣＩＳＯが定めた方法で暗号のための鍵を管理しなければならない。

（４）　無許可ソフトウェアの導入等の禁止

① 議員は、貸与されているパソコン等に無断でソフトウェアを導入してはならない。

② 議員は、議会活動で必要がある場合は、本市統括情報セキュリティ責任者及び本市情報システム管理者の許可を得て、貸与されているパソコン等にソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ責任者及び本市情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

③ 議員は、不正にコピーしたソフトウェアを利用してはならない。

（５）　機器構成の変更の制限

①　議員は、貸与されているパソコン等に対し機器の改造及び増設・交換を行ってはならない。

②　議員は、議会活動上、貸与されているパソコン等に対し機器の改造及び増設・交換を行う必要がある場合には、本市統括情報セキュリティ責任者及び本市情報システム管理者の許可を得なければならない。

（６）　他のネットワークへの接続の禁止

議員は、貸与されているパソコン等を、有線・無線を問わず、そのパソコン等を接続して利用するよう本市情報システム管理者によって定められたネットワークと異なるネットワークに接続してはならない。

（７）　議会活動以外の目的でのウェブ閲覧の禁止

①　議員は、議会活動以外の目的で貸与されているパソコン等を使用してウェブを閲覧してはならない。

②　議員のウェブ利用について、本市統括情報セキュリティ責任者から明らかに議会活動に関係のないサイトを閲覧していることを発見され、適正な措置を求めた通知を受けた場合は、情報セキュリティ管理者は、議会活動に関係のないサイトを閲覧していた議員に対し、情報セキュリティポリシーを遵守するよう適切な処置措置を実施しなければならない。

（８）　Ｗｅｂ会議サービスの利用時の対策

①　議員は、本市の定める利用手順に従い、Ｗｅｂ会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施しなければならない。

③　議員は、Ｗｅｂ会議を主催する場合、会議に無関係の者が参加できないよう対策を講じなければならない。

④　議員は、外部からＷｅｂ会議に招待される場合は、本市統括情報セキュリティ責任者が定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。

（９）　ソーシャルメディアサービスの利用

①　議員は、豊前市議会が管理するアカウントでソーシャルメディアサービスを利用する場合、本市が定めたソーシャルメディアサービス運用手順に従わなければならない。

②　自治体機密性２以上の情報はソーシャルメディアサービスで発信してはならない。

③　情報セキュリティ管理者は、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なければならない。

④　アカウント乗っ取りを確認した場合には、情報セキュリティ責任者又は情報セキュリティ管理者は、本市統括情報セキュリティ責任者及び情

報セキュリティに関する統一的な窓口に報告するとともに、被害を最小限にするための措置を講じなければならない。

⑤　自治体可用性２の情報の提供にソーシャルメディアサービスを用いる場合は、本市のホームページに当該情報を掲載して参照可能としなければならない。

５．２　アクセス制御

（１）　利用者ＩＤの取扱い

①　議員は、議会活動上必要がなくなった場合は、利用者登録を抹消するよう、情報セキュリティ管理者に届け出なければならない。

②　議員から届け出を受けた情報セキュリティ管理者は、情報セキュリティ責任者に報告し、報告を受けた情報セキュリティ責任者は、本市統括情報セキュリティ責任者及び本市情報システム管理者に通知しなければならない。

（２）　議員による外部からのアクセス等の制限

①　議員が外部から内部のネットワーク又は情報システムにアクセスする場合は、情報セキュリティ責任者を通じて本市統括情報セキュリティ責任者及び当該本市情報システムを管理する本市情報システム管理者の許可を得なければならない。

②　議員は、自身が持ち込んだパソコン、モバイル端末又は電磁的記録媒体を庁内のネットワーク及び情報システムに接続に接続してはならない。

③　議員は、許可を得て外部に持ち出し、持ち帰った貸与されているパソコン等を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、情報セキュリティ責任者の許可を得るか、若しくは情報セキュリティ責任者によって事前に指示された手順に従って接続しなければしてはならない。

５．３　不正プログラム対策

議員は、不正プログラム対策に関し、次の事項を遵守しなければならない。

①　貸与されているパソコン等において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

②　貸与されているパソコン等に外部からデータを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければな

らない。

③　貸与されているパソコン等で差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

④　貸与されているパソコン等に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

⑤　貸与されているパソコン等で添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。

⑥　貸与されているパソコン等にコンピュータウイルス等の不正プログラムが感染した場合又は感染が疑われる場合は、事前に本市情報セキュリティ対策基準で決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末においてＬＡＮケーブルの取り外しや、通信を行わない設定への変更などを実施しなければならない。

５．４　議員による不正アクセス対策

本市統括情報セキュリティ責任者及び本市情報システム管理者から議員による不正アクセスを発見したとの通知を受けた場合は、情報セキュリティ管理者は、当該議員に適正に処置するよう指示しなければならない。

５．５　情報セキュリティに関する情報の共有

統括情報セキュリティ責任者及び情報システム管理者が収集した情報セキュリティに関する情報の提供を受けた場合は、必要に応じ、情報セキュリティ責任者、情報セキュリティ管理者及び議員間で共有しなければならない。

６　運用

６．１　情報セキュリティポリシーの遵守状況の確認

（１）　遵守状況の確認及び対処

情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかにＣＩＳＯ及び本市統括情報セキュリティ責任者に報告しなければならない。

（２）　貸与されているパソコン等の利用状況調査

ＣＩＳＯ及びＣＩＳＯが指名した者は、不正アクセス、不正プログラム等の調査のために、貸与されているパソコン等のログ、電子メールの送受信記録等の利用状況を調査することができる。

（３）　議員の報告義務

①　議員は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに情報セキュリティ責任者及び情報セキュリティ管理者に報告を行わなければならない。

②　報告を受けた情報セキュリティ責任者及び情報セキュリティ管理者は、直ちに本市統括情報セキュリティ責任者に報告しなければならない。

③　当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括情報セキュリティ責任者が判断した場合において、議員は、本市情報セキュリティ対策基準で定める緊急時対応計画に従って適正に対処しなければならない。

６．２　法令遵守

議員は、議会活動の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

①　地方自治法（昭和２２年法律第６７号）

②　著作権法（昭和４５年法律第４８号）

③　不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）

④　個人情報の保護に関する法律（平成１５年法律第５７号）

⑤　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（平成２５年法律第２７号）

⑥　サイバーセキュリティ基本法（平成２６年法律第１０４号）

⑦　豊前市議会個人情報の保護に関する条例（令和５年条例第１３号）

６．３　違反時の対応

議員の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

①　本市統括情報セキュリティ責任者が違反を確認した場合は、本市統括情報セキュリティ責任者は、情報セキュリティ責任者に通知し、通知を受けた情報セキュリティ責任者は、情報セキュリティポリシーを遵守するよう適切な処置措置を実施しなければならない

②　本市情報システム管理者等が違反を確認した場合は、違反を確認した

者は速やかに本市統括情報セキュリティ責任者及び情報セキュリティ責任者に通知し、適正な措置を求めなければならない。

③　情報セキュリティ責任者及び情報セキュリティ管理者の指導によっても改善されない場合、本市統括情報セキュリティ責任者は、当該議員のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、本市統括情報セキュリティ責任者は、当該議員のネットワーク又は情報システムを使用する権利を停止あるいは剥奪した旨をＣＩＳＯ及び情報セキュリティ責任者に通知しなければならない。

７　外部サービス（クラウドサービス）の利用

７．１　外部サービス（自治体機密性２以上の情報を取り扱う場合）

（１）　クラウドサービスの選定に係る運用規程の整備

豊前市議会が自治体機密性２以上の情報を取り扱う場合は、本市統括情報セキュリティ責任者が定めるクラウドサービス（本市情報セキュリティ基準方針で規定する「クラウドサービス」をいう。以下同じ。）の選定に関する規程を準用する。

（２）　クラウドサービスの利用に係る運用規程の整備

豊前市議会が自治体機密性２以上の情報を取り扱う場合は、本市統括情報セキュリティ責任者が定めるクラウドサービス（自治体機密性２以上の情報を取り扱う場合）の利用に関する規程を準用する。

（３）　クラウドサービスの選定

豊前市議会がクラウドサービスを選定する場合、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービスの選定に係る利用規程に従い、議会活動に係る影響度等を検討した上で、議会事務局に行わせなければならない。

※議会事務局は、本市情報セキュリティ基本方針の適用範囲に含まれており、本市情報セキュリティ対策基準に従いクラウドサービスの選定を行う。

（４）　クラウドサービスの利用に係る調達・契約

豊前市議会がクラウドサービスを調達する場合、議会事務局に調達・契約を行わせなければならない。

※議会事務局は、本市情報セキュリティ基本方針の適用範囲に含まれており、本市情報セキュリティ対策基準に従いクラウドサービスの利用に係る調達・契約事務を行う。

（５）　クラウドサービスの利用承認

情報セキュリティ責任者は、クラウドサービスを利用する場合には、本市情報セキュリティ対策基準で定める利用申請の許可権限者へクラウドサービスの利用申請を行わなければならない。

（６）　クラウドサービスを利用した情報システムの導入・構築時の対策

①　豊前市議会がクラウドサービスを利用して情報システムを構築する際は、本市情報セキュリティ対策基準のクラウドサービスを利用した情報システムの導入・構築時の対策に関する規定を準用する。

②　クラウドサービスの利用承認時に許可権限者から指名されたクラウドサービス管理者（以下「クラウドサービス管理者」という。）は、情報システムにおいてクラウドサービスを利用する際には、情報システム台帳及び関連文書に記録又は記載しなければならない。なお、情報システム台帳に記録又は記載した場合は、本市統括情報セキュリティ責任者へ報告しなければならない。

③　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備しなければならない。

（ア）　クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順

（イ）　クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順

（ウ）　利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

④　クラウドサービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録しなければならない。

（７）　クラウドサービスを利用した情報システムの運用・保守時の対策

豊前市議会がクラウドサービスを利用して情報システムを運用する際は、本市情報セキュリティ対策基準のクラウドサービスを利用した情報システムの運用・保守時の対策に関する規定を準用する。

（８）　クラウドサービスを利用した情報システムの更改・廃棄時の対策

豊前市議会がクラウドサービスを利用した情報システムの更改・廃棄する際は、本市情報セキュリティ対策基準のクラウドサービスを利用した情報システムの更改・廃棄時の対策に関する規定を準用する。

７．２　外部サービス（自治体機密性２以上の情報を取り扱わない場合）

（１）　クラウドサービスの利用に係る規定の整備

豊前市議会が自治体機密性２以上の情報を取り扱わないクラウドサービスを利用する場合は、本市統括情報セキュリティ責任者が定めるクラウドサービスの利用に関する規定を準用する。

（２）　クラウドサービスの利用における対策の実施

① 豊前市議会が自治体機密性２以上の情報を取り扱わないクラウドサービスを利用する場合、情報セキュリティ管理者は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で自治体機密性２以上の情報を取り扱わない場合のクラウドサービスの利用を申請しなければならない。また、承認時に指名されたクラウドサービス管理者（本市情報セキュリティ対策基準におけるクラウドサービスの利用申請の許可権限者が指名する「クラウドサービス管理者」をいう。）は、当該クラウドサービスの利用において適切な措置を講じなければならない。

② 情報セキュリティ責任者は、情報セキュリティ管理者によるクラウドサービスの利用申請を審査し、議会活動上必要と判断した場合は、本市情報セキュリティ対策基準におけるクラウドサービスの利用申請の許可権限者にクラウドサービスの利用申請をしなければならない。また、承認したクラウドサービスを記録しなければならない。

８　評価・見直し

８．１　監査

（１）　実施方法

豊前市議会は、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、ＣＩＳＯが指名した情報セキュリティ監査統括責任者（以下「情報セキュリティ監査統括責任者」という。）が実施する監査を、毎年度及び必要に応じて受けなければならない。

（２）　監査実施計画の立案及び実施への協力

① 監査実施計画は、情報セキュリティ監査統括責任者が監査を行うに当たって立案し、本市情報セキュリティ対策基準で定める情報セキュリティ委員会（以下「情報セキュリティ委員会」という。）の承認を得たものでなければならない。

② 豊前市議会は、監査の実施に協力しなければならない。

（３）　報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、情報セ

キュリティ委員会及び情報セキュリティ責任者に報告する。報告を受けた情報セキュリティ責任者は、情報セキュリティ管理者及び議会運営委員会に監査結果を報告する。

（４）　監査結果への対応

① ＣＩＳＯは、監査結果を踏まえ、情報セキュリティ責任者に対し、指摘事項への対処（改善計画の策定等）を指示しなければならない。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

② ＣＩＳＯは、本市の行政機関の指摘事項を情報セキュリティ責任者に対して、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。また、豊前市議会及び本市の行政機関で横断的に改善が必要な事項については、本市統括情報セキュリティ責任者に対し、当該事項への対処（改善計画の策定等）を指示しなければならない。なお、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

（５）　情報セキュリティポリシー及び関係規程等の見直し等への活用

情報セキュリティ管理者及び議会運営委員会は、監査結果を情報セキュリティポリシー及び関係規定等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

８．２　自己点検

（１）　実施方法

情報セキュリティ責任者は、情報セキュリティ管理者と連携して、豊前市議会における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行わなければならない。

（２）　報告

本市統括情報セキュリティ責任者、本市情報システム管理者及び情報セキュリティ責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告しなければならない。

（３）　自己点検結果の活用

情報セキュリティ責任者、情報セキュリティ管理者及び議会運営委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

８．３　情報セキュリティポリシー及び関係規定等の見直し

情報セキュリティ管理者及び議会運営委員会は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合にリスク評価を行い、必要があると認めた場合、改善を行うものとする。なお、横断的に改善が必要となる情報セキュリティ対策の運用見直しについて、情報セキュリティ委員会に職制及び職務に応じた措置の実施又は指示を依頼しなければならない。