# 白岡市議会情報セキュリティ基本方針

令和８年３月１８日　策定

第１．０版

白岡市議会

# 改定履歴

| 版番号 | **改定年月日** | **改定理由・内容** |
|---|---|---|
| 第１．０版 | 令和８年３月１８日 | 初版発行（令和８年３月１８日決裁） |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# 白岡市議会情報セキュリティ基本方針

## 第１章　目的

白岡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、白岡市議会（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の基本事項を定め、議会活動の信頼性を維持し、市民の権利利益を保護することを目的とする。

## 第２章　定義

本基本方針において使用する用語の意義は、次に掲げるところによる。

１　「情報資産」とは、議会が保有し、又は管理する情報及びこれを取り扱うための設備、システムその他一切の資源をいう。

２　「ネットワーク」とは、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。

３　「情報システム」とは、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。

４　「情報セキュリティ」とは、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。

５　「機密性」とは、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」とは、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」とは、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　「情報セキュリティインシデント」とは、情報資産の漏えい、滅失、毀損、不正利用その他情報セキュリティ上の支障が生ずるおそれのある事象をいう。

９　その他必要な用語は、白岡市情報セキュリティ基本方針に定めるところによる。

## 第３章　対象とする脅威

議会は、情報資産に対し、次に掲げる脅威を想定し、情報セキュリティ対策を実施する。

１　サイバー攻撃（不正アクセス、マルウェア感染等）

２　人的要因（誤操作、紛失、盗難、事務処理上の過誤等）

３　物理的・環境的要因（災害、停電、インフラ障害等）

４　その他情報資産の安全性を損なうおそれのある事象

## 第４章　適用範囲

本基本方針の適用範囲は、次の各号に掲げるものとする。

１　対象範囲

本基本方針は、議員並びに議会事務局職員（臨時・非常勤職員を含む。）及びその他議会の情報資産を取り扱う者（以下「議会事務局職員等」という。）に適用する。

2　情報資産の範囲

本基本方針が対象とする情報資産は、議会が管理・利用するネットワーク、情報システム並びにこれらに関する設備、電磁的記録媒体、情報（印刷物を含む）及び関連文書とする。

なお、議員個人が議員活動の中で取得した情報資産は、本基本方針の対象外とする。

また、基幹系及び情報系ネットワークや共同利用クラウド、認証基盤等、執行機関と共同利用する情報資産の安全確保に関しては、白岡市情報セキュリティ基本方針に定める事項を準用する。

## 第５章　遵守義務

議員及び議会事務局職員等は、情報セキュリティの重要性について共通の認識を持ち、次に掲げる事項を遵守しなければならない。

**１　議員の遵守事項**

議員は、次の事項を遵守する。ただし、基幹系及び情報系ネットワークや共同利用クラウド、認証基盤等、執行機関と共同利用する情報資産の安全確保に関しては、白岡市情報セキュリティ基本方針に定める事項を準用する。

（１）議会が貸与する機器・アカウントの適正利用

（２）認証情報の厳格な管理

（３）インシデント発生時の速やかな報告

**２　議会事務局職員等の遵守事項**

議会事務局職員等は、市長部局が管理する情報システムを利用して業務を行う場合においては、白岡市情報セキュリティ基本方針、同対策基準、同実施手順及び関連規程を遵守する。

## 第６章　情報セキュリティ対策

**１　組織体制**

（１）　議会の最高情報セキュリティ責任者（議会ＣＩＳＯ：Chief Information Security Officer、以下「議会ＣＩＳＯ」という。）は、議長とする。

（２）　議会事務局長は、議会の情報セキュリティに関する実務責任者として、必要な措置を講ずるものとする。

（３）　議会事務局長は、必要に応じて情報セキュリティ担当者を指名し、情報資産の管理及び情報セキュリティ対策の実施を行わせることができる。

（４）　議会は、執行機関の情報セキュリティ担当部門と連携し、必要な情報共有及び協力を行うものとする。

**２　情報資産の分類と管理**

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・人的・技術的セキュリティ対策**

議会は、情報資産を保護するため、次に掲げる安全管理措置を講じる。

（１）　議会資料のうち非公開情報を含むものについては、施錠保管その他必要な物理的管理を行うものとする。

（２）　議員及び議会事務局職員等に対する情報セキュリティ意識の向上に関する措置に加え、本基本方針及び関連規定を遵守する。

（３）　議員及び議会事務局職員に貸与する端末等について、アクセス制御、暗号化等の技術的対策を講じるものとする。

（４）　その他必要な情報セキュリティ対策を行う。

**４　インシデント対応**

議員及び議会事務局職員等は、情報セキュリティインシデントが発生した場合、速やかに議会ＣＩＳＯに報告する。議会ＣＩＳＯは、必要に応じて執行機関と連携し、被害拡大防止、復旧及び再発防止策を講じる。

**５　教育・研修**

議会ＣＩＳＯは、議員及び議会事務局職員等が情報セキュリティに関する適切な知識と意識を保持できるよう、必要に応じて研修及び啓発に努める。

## 第７章　情報セキュリティ監査及び自己点検の実施

１　議会事務局長は、議会における情報セキュリティの遵守状況を確認するため、必要に応じて自己点検を実施するものとする。

２　議会は、必要に応じて執行機関の監査部門等との連携を含め、情報セキュリティに関する監査を受けるものとする。

## 第８章　基本方針の見直し

本基本方針は、自己点検及び情報セキュリティ監査の結果又は法令の改正、技術の進展、社会情勢の変化等に応じて、適宜見直しを行う。

## 第９章　対策基準・実施手順の策定

議会は、情報資産の安全を確保するため、必要に応じて情報セキュリティに関する対策基準及び実施手順の整備に努める。

なお、情報セキュリティに関する対策基準及び実施手順は、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。