大網白里市議会

情報セキュリティ基本方針

令和８年３月　策定

大網白里市議会情報セキュリティ基本方針

（目的）

第１条　大網白里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、大網白里市議会（以下「市議会」という。）に係る情報資産について、市議会が講ずべき情報セキュリティ対策の基本的な事項を定めることにより、当該情報資産を保護することを目的とする。

（定義）

第２条　この基本方針における用語の意義は､次の各号に定めるところによる。

(1) 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。

(2) 情報資産　情報システムを用いて作成された情報（情報システムから出力された文書を含む。）をいう。

(3) 情報システム　電子計算機（以下「コンピュータ」という。）、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) 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であって、当該構成機器であるハードウェア及びソフトウェアをいう。

(5) 電磁的記録媒体　コンピュータでデータを記録するための媒体をいう。

(6) 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可能な状態を確保することをいう。

(7) 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。

(8) 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。

(9) 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（第５条から第７条までに規定する対策等の実施のために具体的な遵守事項及び判断基準を定めたものをいう。以下「対策基準」という。）を総称したものをいう。

(10) 議員等　大網白里市議会議員及び大網白里市議会事務局の職員をいう。

（対象とする脅威）

第３条　本基本方針において想定する情報資産に対する脅威は、次の各号に掲げる事項とし、市議会は当該脅威に対する情報セキュリティ対策を実施するものとする。

(1) 不正アクセス、ウイルス攻撃、サービス不能攻撃その他のサイバー攻撃並びに部外者の侵入等による意図的な情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取及び内部不正

(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及び機器故障による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、火災その他の災害によるサービス及び業務の停止等

(4) 大規模又は広範囲にわたる疾病による職員の不足に伴う機能不全等

(5) 電力供給の途絶、通信の途絶、水道供給の途絶その他のインフラ障害からの波及等

（適用範囲）

第４条　基本方針の適用範囲は、次の各号に掲げる区分に応じ当該各号に定めるとおりとする。

(1) 組織的範囲　市議会

(2) 人的範囲　議員等及び議員等から業務を受託した者

(3) 情報資産の範囲は、次に掲げるとおりとする。

ア　情報システム並びに当該システムに附属する設備及び電磁的記録媒体

イ　情報システムで取り扱う情報（情報システムから出力された文書を含む。）

ウ　情報システムの仕様書及びネットワーク図等の文書

（議員等の遵守義務）

第５条　議員等は、情報セキュリティの重要性を認識し、各業務の遂行に当たっては、法令、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（情報セキュリティ対策の具体的手順を定めたものをいう。以下「実施手順」と

いう。）を遵守しなければならない。

（情報セキュリティ対策）

第６条　第３条に規定する脅威から情報資産を保護するための対策は、次の各号に掲げる区分に応じ当該各号に定めるとおりとする。

(1) 組織体制　情報セキュリティ対策を推進する組織体制を確立する。

(2) 情報資産の分類と管理　保有する情報資産を機密性、完全性及び可用性に応じ分類・管理する。

(3) 物理的セキュリティ　議員等のコンピュータ（公用又は私用を問わず情報資産を扱うものに限る。）について、情報資産の盗難等を防止する物理的対策を講じる。

(4) 人的セキュリティ　議員等が遵守すべき事項について十分な教育及び啓発等を講じる。

(5) 技術的セキュリティ　コンピュータの管理、アクセス制御、不正プログラム対策、不正アクセス対策等、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、業務委託を行う際のセキュリティ確保その他情報セキュリティポリシー運用に係る対策を講じるとともに、情報セキュリティインシデント（情報資産を脅かすセキュリティ上好ましくない事象又は事態のことをいう。）に迅速かつ適正に対応するための危機管理対策を講じる。

(7) 業務委託　業務委託する場合は、委託事業者と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いた措置を講じる。

(8) 外部サービスの利用　ソーシャルメディアサービス等の外部サービスの利用にあっては、運用手順及び責任者を定める。

（情報セキュリティ監査又は自己点検の実施）

第７条　市議会は、情報セキュリティポリシーの遵守状況を検証するため、適時、情報セキュリティ監査又は自己点検を実施する。

（情報セキュリティポリシーの見直し）

第８条　市議会は、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な場合又は情報セキュリティに関する新たな

対策が必要な場合は、情報セキュリティポリシーを見直すものとする。

（情報セキュリティ対策基準の策定）

第９条　市議会は、基本方針とは別に対策基準を策定するものとする。

２　市議会は、前項の対策基準に基づき実施手順を策定するものとする。

３　対策基準及び実施手順は、非公開とする。

（補則）

第１０条　この基本方針に定めるもののほか、市議会における情報セキュリティ対策に必要な事項は、議長が定める。

附　則

本基本方針は、令和８年４月１日から施行する。