君津市選挙管理委員会情報セキュリティ基本方針

（趣旨）

1　この基本方針は、君津市選挙管理委員会（以下「委員会」という。）が管理する情報資産（以下「情報資産」という。）をセキュリティの侵害等の脅威から保護するため、委員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ものとする。

（定義）

2　この基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(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これを構成する情報機器（ハードウェア及びソフトウェアをいう。以下同じ。）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) 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。

(5) 完全性　情報が破壊、改ざん又は消去をされていない状態を確保することをいう。

(6) 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。

(7) 基幹業務系　個人番号（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）第２条第５項に規定する個人番号をいう。）を利用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。

(8) 庁内情報系　ＬＧＷＡＮ（地方公共団体を相互に接続する行政専用のネットワークをいう。）に接続された情報システム及び当該情報システムで取り扱うデータ（これらのうち前号に該当するものを除く。）をいう。

(9)　インターネット接続系　インターネットメールシステム、ホームページ管理システムその他のインターネットに接続された情報システム及び当該情報システムで取り扱うデータをいう。

(10)　間接アクセス系　庁内情報系及びインターネット接続系の各ネットワークにおいて仮想化した情報の表示及び操作をするための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　庁内情報系、インターネット接続系及び間接アクセス系の各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、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通信その他の安全が確保された通信をいう。

（適用範囲）

3　この基本方針の適用範囲は、委員会の職員及び情報資産とする。

（情報資産の範囲）

4　情報資産の範囲は、次に掲げるとおりとする。

(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（入出力帳票その他の用紙に記録されたもの及び情報システムで保有する情報と同種の情報であって、紙媒体で保有するものを含む。）

(3)　情報システムの仕様書、ネットワーク図その他のシステム関連情報

（職員の遵守義務）

5　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、業務の遂行に当たらなければならない。

（情報資産に対する脅威）

6　情報資産に対する脅威は、次に掲げるとおりとする。

(1)　不正なアクセス、ウイルス攻撃、サービス不能攻撃（ネットワークに接続されたコンピュータに過剰な負荷をかけてサービスの提供をできないようにする攻撃をいう。）等のサイバー攻撃、部外者の侵入その他の意図的な要

因による情報資産の漏えい、改ざん及び消去、重要情報の詐取、内部不正等

(2) 情報資産の無断持出し、委員会が許可していないソフトウェアの使用等の規定違反、情報システムの設計又は開発の不備、プログラム上の欠陥、操作及び設定のミス、メンテナンスの不備、監査機能の不備、情報システムの委託管理の不備、マネジメントの欠陥、機器の故障その他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) 大規模又は広範囲にわたる疾病による要員不足に伴う情報システムの運用に係る機能不全等

(5) 電力供給、通信及び水道供給の途絶その他の社会基盤の障害からの波及等

（情報セキュリティ対策）

7　委員会は、6に規定する脅威から情報資産を保護するため、次の各号に掲げる事項ごとに当該各号に定める情報セキュリティ対策を講ずるものとする。

(1) 組織体制　情報資産について、情報セキュリティ対策を推進するための組織体制を確立すること。

(2) 情報資産の分類及び管理　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講ずること。

(3) 情報システム全体の強靭性の向上　情報セキュリティの強化を目的とし、業務の効率性及び利便性の観点を踏まえ、情報システム全体に対し、次に掲げる区分に応じ、それぞれに定める対策を講じること。

ア　基幹業務系　原則として、他の領域との通信ができないようにした上で、端末からの情報の持ち出しができない設定、端末への多要素認証（複数の異なる種類の認証を組み合わせて行う認証をいう。）の導入等により、住民情報の流出を防ぐこと。

イ　庁内情報系　庁内情報系、インターネット接続系及び間接アクセス系の各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とともに、各環境のシステム間で通信する場合には、無害化通信を実施すること。

ウ　インターネット接続系　高度な情報セキュリティ対策として、不正通信の監視機能の強化、千葉県自治体情報セキュリティクラウド（千葉県及び

千葉県内の市町村のインターネットとの通信を集約した上で、不正通信の監視機能の強化等を行うシステムをいう。）の導入等を実施すること。

エ　間接アクセス系　庁内情報系、インターネット接続系及び間接アクセス系の各環境間の通信環境を分離し、各環境のシステム間で通信する場合は、無害化通信を実施すること。

(4) 物理的セキュリティ　サーバ、サーバ室及び通信回線並びにパソコン等の管理について、物理的な対策を講ずること。

(5) 人的セキュリティ　情報セキュリティに関し、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ずること。

(6) 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な対策を講ずること。

(7) 業務委託及び外部サービスの利用　次に掲げる区分に応じ、それぞれに定める対策を講ずること。

ア　業務委託を行う場合　適切な委託事業者を選定し、情報セキュリティに係る要件を明記した契約を締結するとともに、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ずること。

イ　外部サービスを利用する場合　利用に係る規定を整備し、情報の機密性に応じたセキュリティレベルを確保するための対策を講じること。

ウ　ソーシャルメディアサービスを利用する場合　イに掲げる対策のほか、利用に係る運用手順、当該サービスにおいて発信できる情報及び当該サービスごとの責任者を定めること。

（情報セキュリティの点検の実施）

8　委員会は、定期的に、又は必要に応じて、情報セキュリティの自己点検を実施するものとする。

（情報セキュリティ対策の見直し）

9　委員会は、情報セキュリティの点検の結果又は情報セキュリティに関する状況の変化により、新たに対策が必要になったときは、情報セキュリティ対策を見直すものとする。

（補則）

１０　この基本方針に定めるもののほか必要な事項は、別に定める。

附　則

この方針は、令和８年４月１日から施行する。