# 南房総市議会情報セキュリティ規程

（趣旨）

第１条　この告示は、本市議会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、本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。

（定義）

第２条　この告示において、次の各号に掲げる用語の意義は、それぞれ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その構成機器（ハードウエア及びソフトウエア）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　この告示及び別に定める情報セキュリティ対策基準（以下「対策基準」という。）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)　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。）。

(9)　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。

(10)　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。

(11)　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。

（対象とする脅威）

第３条　情報資産に対する脅威として、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) 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) 情報資産の無断持ち出し、無許可ソフトウエアの使用等の規定違反、設計及び開発の不備、プログラム上の欠陥、操作及び設定ミス、メンテナンス不備、内部及び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、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及び業務の停止等

(4) 大規模及び広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

(5) 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

（適用範囲）

第４条　この告示が適用される実施機関は、議会及び議会事務局とする。

２　この告示が対象とする情報資産は、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（これらを印刷した文書を含む。）

(3) 情報システムの仕様書、ネットワーク図等のシステム関連文書

（議員等の遵守義務）

第５条　議員、職員、非常勤職員及び臨時的任用職員（以下「議員等」という。）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情報セキュリティポリシー（以下「ポリシー」という。）及び情報セキュリティ実施手順（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に、次に掲げる情報セキュリティ対策を講じる。

(1) 本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。

(2) 本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) 情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の対策を講じる。

ア　ＬGWAN接続系においては、ＬGWANと接続する業務用システムと、インターネット接続系の情報システムとの通信経路の分割をする。なお、両システム間で通信する場合には、無害化通信を実施する。

イ　インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県と市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

(4) サーバ、サーバ室、通信回線、議員等のパソコン等の管理について、物理的な対策を講じる。

(5) 情報セキュリティに関し、議員等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。

(6) 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。

(7) 情報システムの監視、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等、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に迅速かつ適切に対応するため、緊急時対応計画を策定する。

(8) 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。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。

（情報セキュリティ監査及び自己点検の実施）

第７条　ポリシー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。

（ポリシーの見直し）

第８条　情報セキュリティ監査及び自己点検の結果、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、リスクを検討した上で、ポリシーを見直す。

（対策基準の策定）

第９条　前３条に規定する対策等を実施するために、具体的な遵守事項、判断基準等を定める対策基準を策定する。

（実施手順の策定）

第１０条　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実施手順を策定するものとする。

２　実施手順は、公にすることにより本市議会の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。

（委任）

第１１条　この告示に定めるもののほか、必要な事項は、議長が別に定める。

附　則

この告示は、令和８年４月１日から施行する。