袖ケ浦市情報セキュリティポリシー

（令和５年４月改正版：公開用）

改正履歴

改正日	改正理由
平成 15 年 11 月 1 日	策定
平成 19 年 4 月 17 日	全部改正
平成 25 年 3 月 1 日	一部改正
平成 27 年 12 月 21 日	一部改正
平成 29 年 4 月 1 日	一部改正
平成 31 年４月１日	全部改正
令和２年４月１日	一部改正
令和３年４月１日	一部改正
令和５年４月１日	一部改正

第１章　総則

１　情報セキュリティポリシー

情報セキュリティポリシーとは、袖ケ浦市の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書をいう。

情報セキュリティポリシーは、袖ケ浦市が所管する情報及び情報を格納する機器並びに記録媒体（以下「情報資産」という。）に関する業務に携わる全職員（常勤特別職を含む。）、会計年度任用職員、臨時的任用職員、行政委員会の長及び市長が必要と認めた者並びに外部委託事業者に浸透、普及、定着させるものであり、安定的な規範であることが要請される。また、技術の進歩や新たな脅威等に対応するべく、情報セキュリティポリシーの評価及び見直しを行い、情報セキュリティ対策の実効性を確保する必要もある。

２　袖ケ浦市における情報セキュリティの考え方

袖ケ浦市では、法令等に基づき、住民の個人情報や企業の経営情報等の重要情報を多数保有するとともに、他に代替することができない行政サービスを実施している。

また、業務の多くが電子情報システムやネットワークに依存していることから、住民生活や地域の社会経済活動を保護するため、情報セキュリティ対策を講じて、その保有する情報を守り、業務を継続することが必要となっている。

今後、電子情報システムの高度化等、電子自治体が進展することにより、電子情報システムの停止等が発生した場合、広範囲の業務が継続できなくなり、住民生活や地域の経済社会活動に重大な支障が生じる可能性も高まる。また、ＬＧＷＡＮ等のネットワークにより相互に接続しており、発生したＩＴ障害がネットワークを介して他の団体に連鎖的に拡大する可能性も否定できない。

これらの事情から、情報セキュリティの実効性を高めるとともに、対策レベルを強化していくことが必要となっている。また、情報セキュリティの確保に絶対安全ということはないことから、情報セキュリティに関する事故の未然防止のみならず、事故が発生した場合の拡大防止、迅速な復旧及び再発防止の対策を講じていくことが必要である。

３　情報セキュリティポリシーの構成

情報セキュリティポリシーの体系は、階層構造となっており、情報セキュリティ対策における基本的な考え方を定めるものが「基本方針」である。この基本方針に基づき、すべての電子情報システムに共通の情報セキュリティ対策の基準を定めるのが「対策基準」である。この「基本方針」と「対策基準」を総称して「情報セキュリティポリシー」という。この「対策基準」を、具体的なシステムや手続に展開して個別の実施事項を定めるものが「実施手順」である。

第２章　情報セキュリティ基本方針

１　目的

本基本方針は、袖ケ浦市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

電子情報システムのコンピュータ間を接続するための通信網及び構成機器（ハードウェア及びソフトウェア）をいう。

（２）電子情報システム

コンピュータのハードウェア及びソフトウェア、ネットワーク及び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

本情報セキュリティ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

情報資産にアクセスすることを認められた者だけが、情報資産にアクセスできる状態を確保することをいう。

（６）完全性

情報資産が破壊、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

情報資産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、情報資産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）ネットワーク

個人番号を取り扱う事務又は戸籍事務等に関わる電子情報システム及びその電子情報システムで取り扱う情報を送受信するネットワークをいう。

（９）ＬGWAN接続系ネットワーク

ＬGWANに接続された電子情報システム及びその電子情報システムで取り扱う情報を送受信するネットワークをいう（マイナンバー利用事務系ネットワークを除く。）。

（１０）インターネット接続系ネットワーク

インターネットメール等に関わる千葉県自治体情報セキュリティクラウドを介してインターネットに接続された電子情報システム及びその電子情報システムで取り扱う情報の送受信を行うネットワークをいう。

（１１）全庁ＬＡＮシステム

マイナンバー利用事務系ネットワーク、ＬＧＷＡＮ接続系ネットワーク、インターネット接続系ネットワーク全体の総称をいう。

（１２）通信経路の分割

マイナンバー利用事務系ネットワーク、ＬＧＷＡＮ接続系ネットワーク、インターネット接続系ネットワークの通信を分離した上で、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。

（１３）無害化通信

インターネットメール本文のテキスト化やコンピュータ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　対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

ア　部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃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

イ　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、操作及び設定ミス、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、機器故障等の非意図的要因による情報資産の漏えい、破壊及び消去等

ウ　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

エ　電力供給の途絶、通信の途絶等の提供サービスの障害からの波及等

オ　大規模又は広範囲にわたる疾病の蔓延による要員不足に伴うシステム運用の機能不全等

４　適用範囲

（１）行政機関の範囲

情報セキュリティポリシーが適用される行政機関は袖ケ浦市行政組織条例（平成３年条例第３号)第１条に定める部、並びに会計室、行政委員会事務局、議会事務局及び消防組織（以下「部等」という。）とする。

（２）情報資産の範囲

情報セキュリティポリシーが対象とする情報資産は、次のとおりとする。

ア　ネットワーク（学校間ネットワークは除く。以下同じ）、電子情報システム、及びこれらに関する設備、記録媒体

イ　ネットワーク及び電子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。）

ウ　電子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（以下「システム関連文書」という。）

５　職員等の遵守義務

全職員（常勤特別職を含む。）、会計年度任用職員、臨時的任用職員、行政委員会の長及び市長が必要と認めた者（以下「職員等」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及び情報セキュリティ共通実施手順（以下「情報セキュリティポリシー等」という。）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３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

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（２）情報資産の分類と管理

本市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、情報セキュリティ対策を実施する。

（３）電子情報システム全体の強靭性の向上

電子情報システム全体に対し、次の三段階の対策を講じる。

ア　マイナンバー利用事務系ネットワークにおいては、原則として、他の領域との通信をできないようにした上で、コンピュータからの情報持ち出し不可設定やコンピュータ及びモバイル端末（以下、「コンピュータ等」という。）への多要素認証の導入等により、住民情報の流出を防ぐ。

イ　ＬＧＷＡＮ接続系ネットワークにおいては、ＬＧＷＡＮと接続する電子情報システムと、インターネット接続系ネットワークの電子情報システムとの通信経路を分割する。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。

ウ　インターネット接続系ネットワークにおいては、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行う。高度な情報セキュリティ対策として、千葉県自治体情報セキュリティクラウドへ参加する。

（４）物理的セキュリティ

サーバー、ネットワーク、電子情報システム、コンピュータ等、及びこれらに関する設備、記録媒体並びに管理区域等の管理について、物理的な対策を講じる。

（５）人的セキュリティ

情報セキュリティに関し、職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）技術的セキュリティ

サーバー、ネットワーク、電子情報システム及び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）運用

電子情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う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。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）外部委託と外部サービスの利用

外部委託する場合には、外部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、外部委託事業者において必要な情報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。約款による外部サービスを利用する場合には、利用にかか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。

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、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。

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、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

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本市の行政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。

11　情報部門における業務継続計画（ＩＣＴ－ＢＣＰ）の策定

地震、落雷、火災等の災害等によるサービス及び業務の停止等に対応するために、具体的な実施手順及び判断基準等を定めるＩＣＴ－ＢＣＰを策定する。

第３章　情報セキュリティ対策基準

※情報セキュリティ対策のため非公開