西原町情報セキュリティポリシー

令和７年２月１日

西原町情報セキュリティ管理委員会

目　次

改訂履歴

・平成 16 年　1 月　8 日　策定
・平成 16 年　4 月　1 日　改定　（組織改編対応）
・平成 29 年　2 月　1 日　改定　（全部改正）委員会承認：平成 29 年　1 月 31 日
・令和　7 年　2 月　1 日　改定　（一部改正）委員会承認：令和　7 年　1 月 30 日

序章

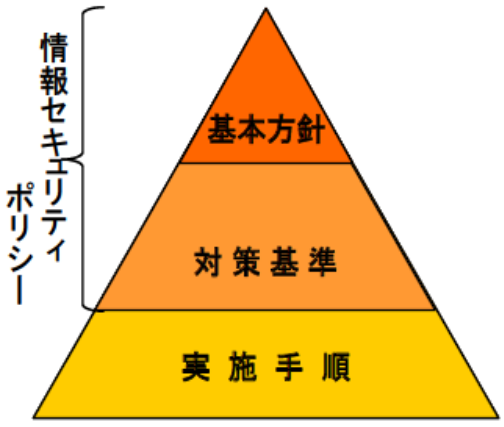
1.情報セキュリティポリシー

情報セキュリティポリシーとは、組織内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。地方公共団体における情報セキュリティは、各地方公共団体が保有する情報資産を守るにあたって自ら責任を持って確保すべきものであり、情報セキュリティポリシーも各地方公共団体が組織の実態に応じて自主的に策定するものである。地方公共団体においては、情報セキュリティ対策を徹底するには、対策を組織的に統一して推進することが必要であり、そのためには組織として意思統一し、明文化された文書として、情報セキュリティポリシーを定める。また、定めるだけではなく情報セキュリティポリシーの定期的な評価・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とともに、対策レベルを高めていくことが重要である。

なお、「サイバーセキュリティ基本法」第5条では、地方公共団体においてサイバーセキュリティに関する自主的な施策の策定と実施が責務規定として法定化された。これにより、情報セキュリティポリシーの未策定団体においては策定が必須となり、策定済み団体においても、適時適正な見直しとそれを遵守することが重要となっている。

また、番号制度等の最新の制度に係るセキュリティ対策、例えば、情報提供ネットワークシステム等の技術的基準、「特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）」（令和 3 年 8 月改正 個人情報保護委員会）が示す安全管理措置等についても遵守しなければならない。情報セキュリティポリシーの体系は、図表1に示す階層構造となっている。本町の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、全ての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順、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。

このように、情報セキュリティポリシーは、情報セキュリティ対策の頂点に位置するものであることから、町長をはじめ、全ての職員等及び委託事業者は、業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負う。



図表1　情報セキュリティポリシーに関する体系図

第１章　情報セキュリティ基本方針

１.目的

本町が取り扱う情報には住民の個人情報をはじめ行政運営上の機密情報など、部外に漏えい等した場合には極めて重大な結果を招く情報が多数含まれており、これらの情報を様々な脅威から守ることは、住民の財産・プライバシー等の保護を行うためにも、行政事務の安定的な運営のためにも必要不可欠である。また、マイナンバーを含む特定個人情報の保護は、漏えいした際には、本町住民の被害に止まらず、本町を含むすべての自治体、社会システムそのものの信頼に関わることから非常に重要な課題である。

そのため、町の情報資産の機密性、完全性及び可用性を維持するための対策（情報セキュリティ対策）を整備するために西原町情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については町の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

２.定義

（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、その構成機器（ハードウェア及びソフトウェア）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

本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）マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）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。

（９）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。）。

（１０）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。

（１１）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。

（１２）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。

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。

（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・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、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・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

４.適用範囲

（１）行政機関の範囲

本基本方針が適用される行政機関は、町長部局、各行政委員会、議会事務局及び地方公営企業とする。

（２）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

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及びネットワーク図等のシステム関連文書

5.職員等の遵守義務

職員、会計年度任用職員等（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実施手順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

本町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

本町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・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

①マイナンバー利用事務系においては、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､端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

②LGWAN 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。

③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、都道府県及び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）物理的セキュリティ

サーバ、情報システム室、通信回線及び職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）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

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

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、業務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正に対応する

ため、緊急時対応計画を策定する。

（8）業務委託と外部サービス（クラウドサービス）の利用

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。

（9）評価・見直し

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し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

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、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、リスクを検討したうえで、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町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。