横芝光町
情報セキュリティ基本方針

平成 19 年 4 月　策　定

令和　8 年 3 月　改　訂

目　　次

はじめに

近年、情報通信技術の進展は著しく、行政を取り巻く環境も大きく変化しています。サイバー攻撃の高度化や巧妙化により、行政機関に対する脅威は増大しており、情報資産の安全を確保することは、住民の信頼を守る上で極めて重要な課題となっています。

また、改正地方自治法においては、地方公共団体におけるサイバーセキュリティ対策の強化、職員に対する情報セキュリティ教育の実施、不正プログラムへの対応などが明確に求められるようになりました。これにより、組織的かつ計画的な取り組みを推進する必要性が、これまで以上に高まっています。

さらに、近年は多くの業務システムがクラウド環境で提供されるようになり、国におけるシステム標準化やガバメントクラウドの活用も進展しています。こうした利用環境の変化に対応することも重要です。

「横芝光町情報セキュリティ基本方針」（以下「本基本方針」という。）は、これらの状況を踏まえ、横芝光町（以下「本町」という。）における情報セキュリティに関する基本方針と行動の指針を定めるものです。職員一人一人が本基本方針を理解し、確実に実践することで、住民に信頼される安全・安心な行政サービスを継続して提供してまいります。

ここに、本町は、住民の大切な情報を守り抜くとともに、変化する時代に対応したセキュリティ体制を確立し、安心と信頼に基づく行政運営を実現することを、改めて強く宣言します。

第 1 編　目的

本町が取り扱う情報資産には、住民の個人情報のみならず行政運営上重要な情報など、毀損、滅失あるいは外部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いる。このため、本町の行政サービスの対象となる個人・企業・団体の安心で安全な生活・活動を確保・維持するために、その規模に応じた最適な情報セキュリティ対策が必須となる。

本町が保有する情報資産の機密性、完全性及び可用性(注)の維持を図るため、物理的脅威、技術的脅威及び人的脅威等、あらゆる脅威に対する予防・抑止・発見・回復のための方策について、組織的かつ計画的に取り組まなければならない。また、情報セキュリティ対策を確実なものとするため、本町の行政に関わる関係者全てが情報セキュリティ対策の重要性を理解し、本基本方針を遵守しなければならない。これは、行政を安全かつ安定的に継続させることを確実にするためにも必要不可欠である。

本基本方針は、情報セキュリティを実践するに当たり、基本的な考え方及び方針を定め、本町における情報資産の管理を徹底することを目的とする。

（注）「第２編　定義」参照

第 2 編　定義

以下の用語の定義は、情報セキュリティ管理・運用で使用する全ての文書に適用される。

（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、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子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ない等、安全が確保された通信をいう。

（13）職員等

職員、再任用職員、非常勤職員及び会計年度任用職員等の任用形態、職位及び勤務地を問わず、本町の全職員をいう。

（14）電磁的記録媒体、電子記録媒体

磁気ディスク、磁気テープ、光ディスクその他これらに類する、電子情報を保管する記録媒体のこと。（例：ハードディスク、CD、DVD、USB メモリ、テープ等）

（15）情報セキュリティ事件・事故

情報システムの障害、機密漏えい、被災等、人的誤りを含む情報セキュリティ上の事件・事故の全てのこと。

第 3 編　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

第 4 編　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、町長内部部局、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子的記録媒体

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

第 5 編　職員等の遵守義務

職員等は、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。

第 6 編　情報セキュリティ対策

第３編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３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。

（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。

第 ７ 編　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。

第 ８ 編　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、リスクを検討した上で、情報セキュリティポリシーを見直す。

第 ９ 編　情報セキュリティ対策基準の策定

第６編、第７編及び第８編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。なお、情報セキュリティ対策基準は、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

第 10 編　情報セキュリティ実施手順の策定

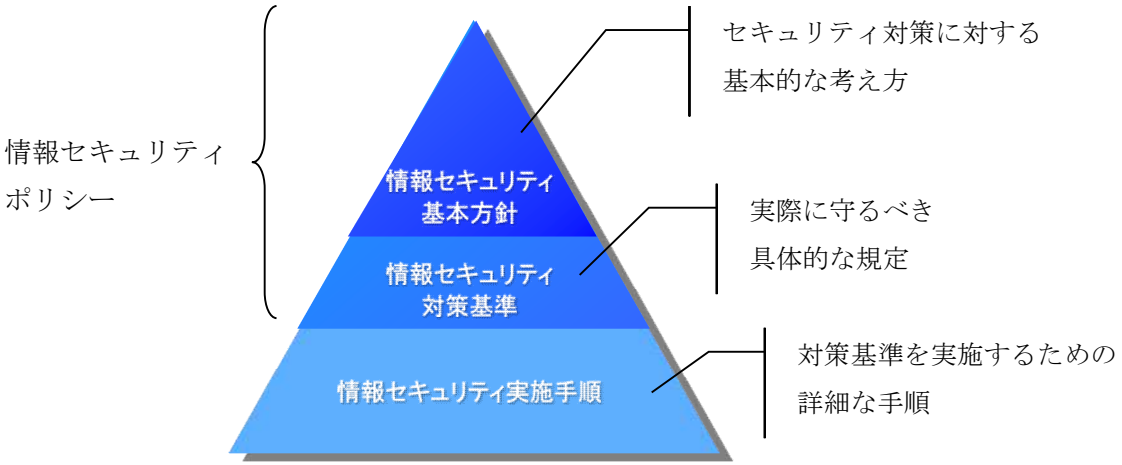
情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

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。

第 11 編　情報セキュリティポリシーの位置付け

本基本方針と情報セキュリティ対策基準から構成される情報セキュリティポリシーは、本町が管理する情報資産に関する情報セキュリティ対策の原理、原則を定めるものであり、情報セキュリティ対策の頂点に位置するものである。



第 12 編　関連法令の遵守

職員等は、情報セキュリティポリシーのみならず、関連する法律・条例等についてもこれを遵守しなければならない。

第 13 編　情報セキュリティに関する違反への対応

情報セキュリティ基本方針・情報セキュリティ対策基準及び情報セキュリティ実施手順、その他の関連法令に違反した場合は、地方公務員法に基づき、当該違反により生じた結果の重大性及び当該違反の悪質性等の状況に応じて、懲戒処分等の対象とする場合がある。

附則

（施行期日）この基本方針は、平成 19 年 4 月より施行する。

（施行期日）この基本方針は、平成 29 年 4 月より施行する。

（施行期日）この基本方針は、令和 6 年 1 月より施行する。

（施行期日）この基本方針は、令和 8 年 3 月より施行する。