七戸町
情報セキュリティポリシー

令和８年３月

七戸町

（七戸町・教育委員会・選挙管理委員会・農業委員会・固定資産評価審査委員会・監査委員・議会）

改訂履歴

施行日	改訂理由
平成 30 年 3 月 30 日	初版発行
令和 8 年 3 月 10 日	総務省「地方公共団体における情報セキュリティポ リシーに関するガイドライン」の改定に伴う改定 （令和 7 年 3 月 3 日決裁、3 月 17 日通知）

第１章 総則

１ 情報セキュリティポリシーの構成

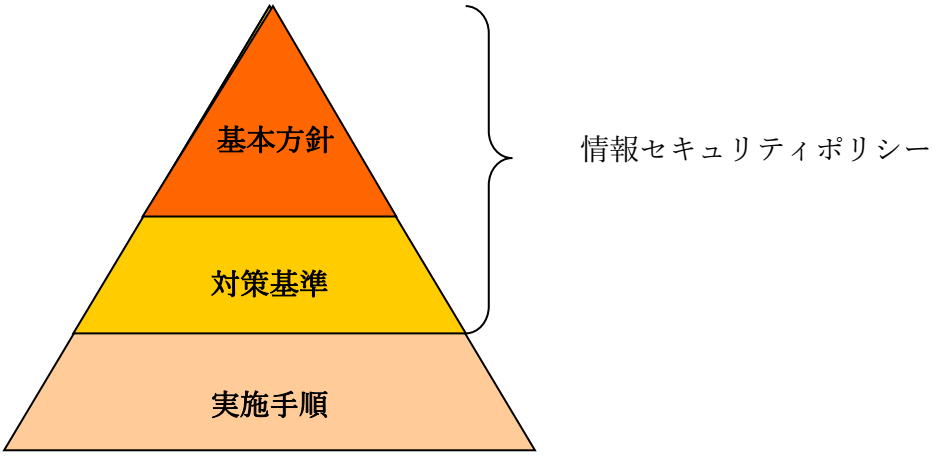
情報セキュリティポリシーとは、七戸町が有する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものを総称する。情報セキュリティポリシーは、七戸町が所掌する情報資産に関する業務に携わる職員、臨時職員、非常勤職員(以下、「職員等」という。)及び外部委託事業者に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分(基本方針)と情報資産を取り巻く状況の変化に依存する部分(対策基準)に分けて策定することとした。

具体的には、情報セキュリティポリシーの体系を、情報セキュリティ対策における基本的な考え方を定めた「基本方針」と、基本方針に基づきすべ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た「対策基準」の２階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、情報システム毎の具体的な情報セキュリティ対策の実施手順として実施手順を策定することとする。

情報セキュリティポリシーは、情報セキュリティ対策の上位に位置するものであることから、町長をはじめ、すべての職員等及び外部委託事業者は、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。

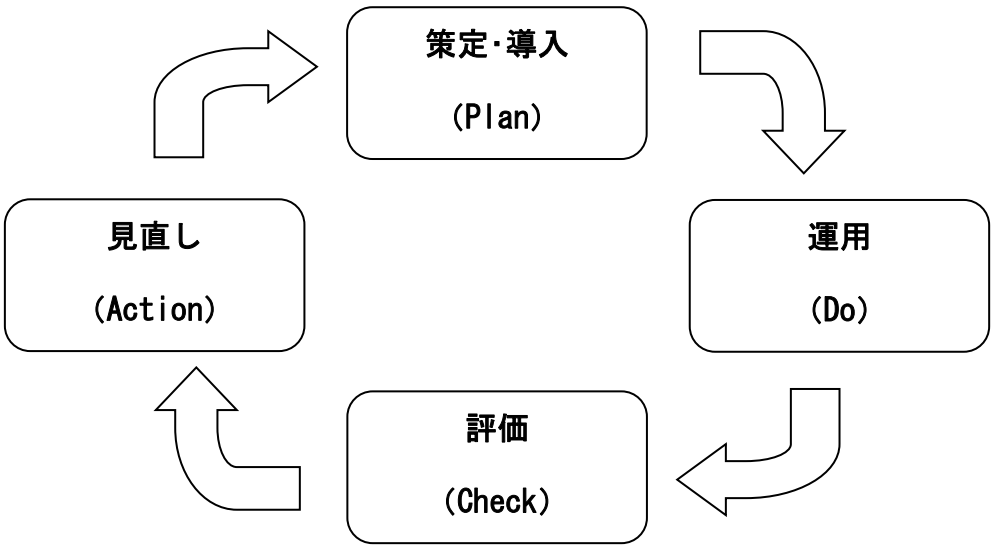
なお、本ガイドラインの対象とする範囲は「情報セキュリティポリシー」を構成する「基本方針」及び「対策基準」であり、「実施手順」は含まれない。



図表１情報セキュリティポリシーに関する体系図

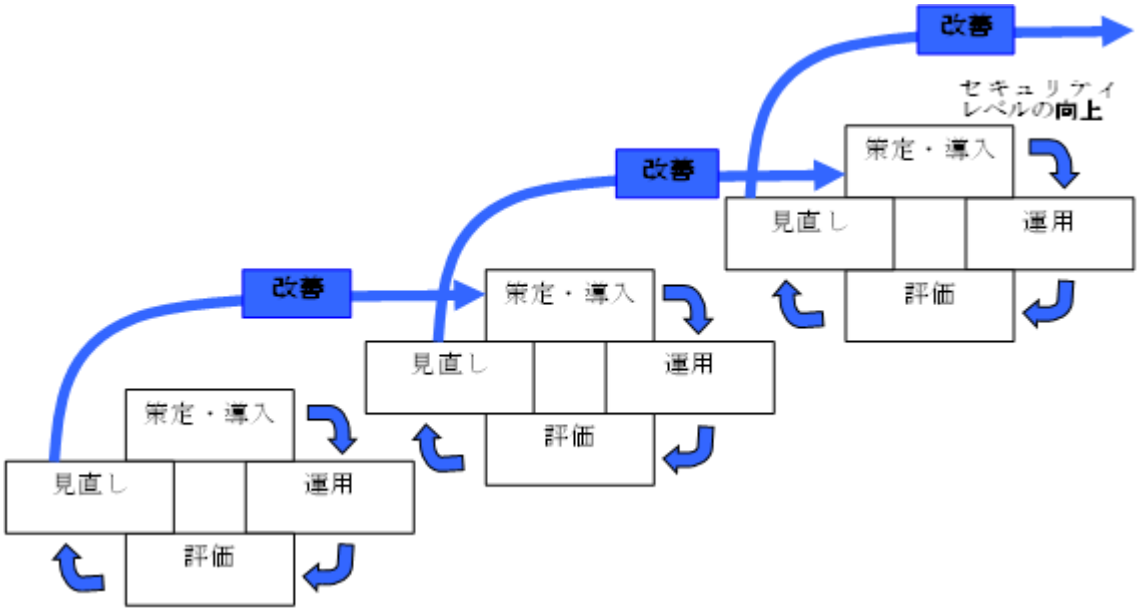
情報セキュリティ対策の実施サイクル

情報セキュリティ対策の実施プロセスは、図表２のとおり、策定･導入(Plan)、運用(Do)、評価(Check)、見直し(Action)のサイクルを回し情報セキュリティの確保をする。



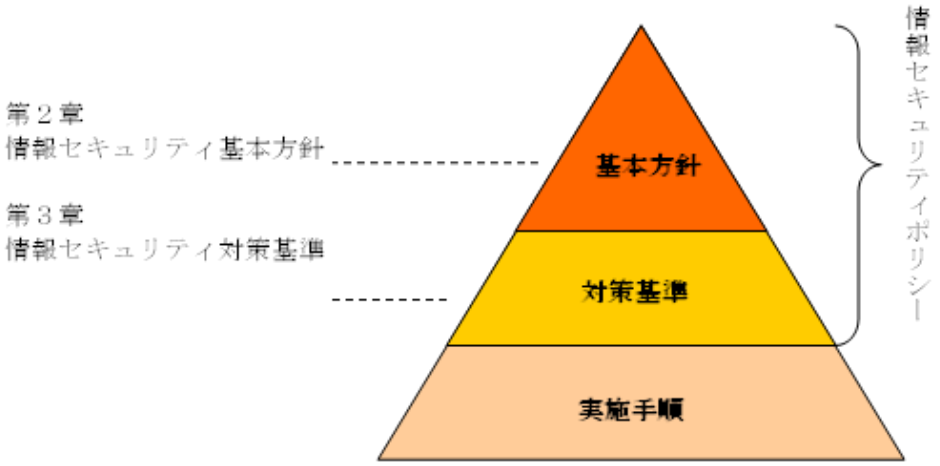
図表２情報セキュリティ対策のＰＤＣＡサイクル

情報セキュリティを取り巻く脅威や対策は常に変化しており、以上のＰＤＣＡサイクルは、一度限りではなく、図表３のとおり、これを定期的に繰り返すことで、環境の変化に対応しつつ、情報セキュリティ対策の水準の向上を図らなければならない。



図表３ＰＤＣＡサイクルの繰り返しによるセキュリティ対策の水準の向上

次章より、情報セキュリティポリシーの具体的な内容を記述するが、図表４のとおり、第２章が「情報セキュリティ基本方針」に関するガイドライン、第３章が「情報セキュリティ対策基準」に関するガイドラインとなっている。



図表４セキュリティポリシーの対応関係

第２章 情報セキュリティ基本方針

１ 目的

本基本方針は、七戸町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、七戸町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

⑴ 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。

⑵ 情報システム

コンピュータ、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。

これら一部又は全体で業務処理を行う仕組み（構成、仕様に関する資料等を含む）をいう。

⑶ 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。

⑷ 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。

⑸ 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。

⑹ 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。

⑺ 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。

⑻ 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。

⑼ 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。）。

⑽ 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。

⑾ 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。

⑿ 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。

⒀ 行政情報

七戸町の業務上、作成又は収得した情報で、情報システムに電磁的に記録されるもの及び入出力帳票をいう。

⒁ 記録媒体

行政情報の記録・管理に使用される磁気ディスク、磁気テープ、光ディスク、フラッシュメモリ等をいう。

⒂ 情報資産

行政情報及び情報システムをいう。

⒃ パソコン

情報システムのうち、職員等に貸与されるコンピュータをいう。

⑰ 端末

ネットワーク及び情報システムに接続されるすべてのコンピュータ（パソコン、サーバー等を含む）をいう。

⑱ 職員等

職員、臨時職員、非常勤職員等の任用形態、職位を問わず、七戸町の全職員をいう。

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。

⑴ 不正アクセス、ウイルス攻撃、サービス不可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

⑵ 情報資産の無断持ち出し、無許可ソフトウェアの仕様等の規定違反、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、外部委託管理の不備、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

⑶ 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

⑷ 大規模・広範囲にわたる疾病による要因不足に伴うシステム運用の機能不全等電力供給、通信、水道供給の途絶等のインフラ障害からの波及等

4 適用範囲

⑴ 行政機関の範囲

本基本方針が適用される行政機関は、すべての執行機関（町長部局、教育委員会、選挙管理委員会、農業委員会、固定資産評価審査委員会、監査委員及び公営企業管理者）及び町議会とする。

⑵ 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、情報システム及びこれらに関する設備、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。

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。

⑴ 組織体制

七戸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。

⑵ 情報資産の分類と管理

七戸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行う。

⑶ 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。

⑷ 物理的セキュリティ

サーバー等、情報システム室等、通信回線等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。

⑸ 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。

⑹ 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。

⑺ 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、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、情報資産への侵害が発生した場合等に迅速かつ適切に対応するための手順を策定する。

⑻ 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。

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に規定する対策を実施するために、具体的な遵守事項及び判断基準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七戸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。