門川町情報セキュリティポリシー

平成２３年１２月　２日　門川町 IT 推進会議　策定

平成３０年　６月２９日　〃　改訂

令和　３年　６月２４日　〃　改訂

令和　５年　４月　１日　〃　改訂

令和　８年　３月１９日　〃　改訂

＜ 目　　次 ＞

序　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、本町が所掌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、本町が所掌する情報資産に関する業務に携わる常勤職員及び非常勤職員(以下、「職員等」という。)及び委託事業者に浸透、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を、

① 情報セキュリティ基本方針
② 情報セキュリティ対策基準

の２階層に分け、それぞれを策定することとする。

情報セキュリティポリシーの構成

文　書　名		内　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針。
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準。

第１章　情報セキュリティ基本方針

１．目的

今日､インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活･経済･社会のあらゆる面で拡大している。一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。

本町は、町民の個人情報や行政運営上重要な情報を多数取り扱っている。また、電子自治体の構築が進み、多くの業務が情報システムやネットワークに依存している。したがって、これらの情報資産を様々な脅威から防御することは、町民の権利・利益を守るためにも、また、行政の安定的で継続的な運営のためにも必要不可欠である。また、本町には、地域全体の情報セキュリティ基盤を強化していく役割も期待されている。

本基本方針は、これらの状況を鑑み、本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、本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

（１）ネットワーク

本町における内部部局、各行政委員会、地方公営企業及び教育機関を相互に接続するための通信網、その構成機器(ハードウエア及びソフトウェア)及び記録媒体で構成され、処理を行う仕組みをいう。

（２）情報システム

業務系の電子計算機(業務系におけるネットワーク、ハードウェア及びソフトウェア)及び記録媒体で構成され、処理を行う仕組みをいう。

（３）情報資産

ネットワーク及び情報システムの開発と運用に係る全ての情報並びにネットワーク及び情報システムで取り扱う全ての情報をいう。

なお、情報資産には紙等の有体物に出力された情報も含むものとする。

（４）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。

（５）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。

（６）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。

（7）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。

（8）可用性

情報にアクセスすることを認められた者だけが、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。

（9）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。

(10) LGWAN接続系

人事給与、財務会計及び文書管理等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。

(11) 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。

(12) 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。

(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．情報セキュリティポリシーの位置付けと職員等及び委託事業者の義務

情報セキュリティポリシーは､本町が所掌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。

したがって､町長をはじめとして本町が所掌する情報資産に関する業務に携わる全ての職員等及び委託事業者は、情報セキュリティの重要性について共通の認識をもつとともに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ものとする。

4．適用範囲

（1）行政機関の範囲

この情報セキュリティポリシーが適用される行政機関の範囲は､町長部局､議会､教育委員会、選挙管理委員会、公平委員会、監査委員会、農業委員会、固定資産評価審査委員会及び公営企業とする。但し、町内各学校については、門川町立小・中学校情報セキュリティポリシーにおいて

定める。

（2）情報資産の範囲

この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である。

ア　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

イ　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。）

ウ　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．情報資産への脅威

情報セキュリティポリシーを策定するうえで、情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

（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による機器又は情報資産の破壊・盗難、故意の不正アクセス又は不正操作による機器又は情報資産の破壊・盗聴・改ざん・消去等

（2）職員等又は委託事業者による機器又は情報資産の無断持出、無許可ソフトウェアの使用等の規律違反、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、火災等の災害並びに事故、故障等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障害からの波及等

6．情報セキュリティ対策

上記5で示した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ずるものとする。

（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・管理するための体制を確立するものとする。

（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、その重要度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。

ア　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。

イ　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、県及び市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対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

（5）人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、全ての職員等及び委託事業者に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるように必要な対策を講ずる。

（6）技術及び運用におけるセキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、不正プログラム対策、不正アクセス対策、ネットワーク管理等の技術面の対策、また、システム開発等の委託を行う際のネットワークの監視、情報セキュリティポリシーの遵守状況の確認等の運用面の対策を講ずる。

また、情報資産に対するセキュリティ侵害が発生した際に迅速な対応を可能とするため緊急時対応計画を策定する。

（7）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、委託事業者を選定後、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するとともに、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、運用手順を定め、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。

（8）評価及び見直し

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が遵守されていることを検証するため、定期的、または、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．評価及び見直しの実施

情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを実施する。

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。