○下川町情報セキュリティ基本方針

令和7年3月28日

訓令第12号

下川町情報セキュリティ基本方針(平成15年下川町訓令第27号)の全部を改正する。

(目的)

第1条　下川町の各種情報システムが取り扱う情報には､町民の個人情報のみならず行政運営上重要な情報など、改ざん又は部外に漏洩等が生じた場合の重大性を鑑みこれらの情報及び情報を取り扱う情報システムをさまざまな脅威から防御し、町の情報資産の機密性、安全性及び可用性を維持するための基本的対策を定め、町民の財産、プライバシー等を守り安定的な行政運営に資することを目的とする。

(定義)

第2条

(1)　ネットワーク

情報処理を行う際に利用する通信網並びに町長部局、各行政委員会、消防、各教育機関(事務室及び職員室のみ)、地方公営企業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)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

情報処理機(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データ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データをいう。

(4)　機密性

情報にアクセスすることが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。

(5)　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。

(6)　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。

(7)　情報セキュリティ対策

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。

(8)　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。

(9)　マイナンバー利用事務(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)又は戸籍事務等を関わる情報システム及びデータをいう。

(10)　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。)

(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、コンピューター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。

（対象とする脅威）

第3条　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セキュリティポリシー違反、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、機械故障等の非意図的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・小範囲にわたる疫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

（適用範囲）

第4条　本基本方針が適用される行政機関は、町長部局、行政委員会、議会事務局、消防本部及び地方公営企業とする。

2　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

（職員等の遵守義務）

第5条　情報セキュリティポリシーは、下川町の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下川町の情報資産に関する業務に携さわる全ての職員等及び部外委託者は、情報セキュリティポリシーの重要性について共通の認識を持つとともに業務の遂行に当って情報セキュリティポリシーを遵守する責務を負うものとする。

(情報セキュリティ対策)

第6条　第3条の脅威から情報資産を保護するために、以下のセキュリティ対策を講じる。

(1)　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)　本町の保有する情報資産の機密性、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､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)　サーバ、電算室、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)　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)　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。

(運用)

第7条　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。

(業務委託と外部サービス(クラウドサービス)の利用)

第8条　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(以下「SNS」という。)を利用する場合には、SNSの運用手順を定め、SNSで発信できる情報を規定し、利用するSNSサービスごとの責任者を定める。

(情報セキュリティ監査及び自己点検の実施)

第9条　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。

(情報セキュリティポリシーの見直し)

第10条　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。

(情報セキュリティ対策基準の策定)

第11条　第6条、第7条及び第8条に対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。

（情報セキュリティ対策手順の策定）

第12条　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書を策定するものとする。

なお、情報セキュリティ実施手順書は、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。

附　則

この訓令は、令和7年4月1日から施行する。