○八頭町行政情報セキュリティポリシー（基本方針）要綱

（令和２年３月 23 日訓令第 12 号）

改正　令和８年３月 30 日訓令第６号

（目的）

第１条　この訓令は、本町が保有し又は管理する情報資産について、サイバー攻撃、災害、障害、内部不正等の脅威から保護し、並びに機密性、完全性及び可用性を維持するために必要な情報セキュリティ対策の基本的な事項を定め、もって情報システムの安定的な運用及びデジタル化の推進を図り、本町における住民サービスの向上及び行政運営の継続性確保に資することを目的とする。

（基本原則）

第２条　本町の情報セキュリティ対策は、次に掲げる基本原則に基づき実施する。

⑴ リスクベース

情報資産の重要度及びリスク評価に基づき、合理的に優先順位を付して対策を講じる。

⑵ 最小権限・職務分離

権限を必要最小限とし、誤操作及び不正の影響を局所化する。

⑶ 侵害を前提

侵害の未然防止に加え、検知、封じ込め、復旧及び再発防止を含めた対策を講じる。

⑷ 外部サービスの条件付き活用

外部サービスは、利用目的・責任分界・安全管理措置が明確であり、必要な統制を確保できる場合に限り活用する。

⑸ 継続的改善

監査及び自己点検の結果並びに脅威動向等を踏まえ、継続的に見直す。

⑹ 透明性

本指針は公表し、町としての方向性を明確にする。

（定義）

第３条　本要綱において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

⑴　ネットワークとは、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　情報システムとは、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。

⑶　情報資産とは、次に掲げるものをいう。

ア　ネットワーク、情報システム及びこれらに関する設備並びに電磁的記録媒体

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、設定情報、ネットワークの構成図等の関連文書

⑷　セキュリティポリシーとは、この訓令及び八頭町行政情報セキュリティポリシー（対策基準）要綱（令和２年訓令第 13 号）をいう。

⑸　機密性とは、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　完全性とは、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　可用性とは、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）とは、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接続系とは、人事給与、財務会計等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。
⑽　インターネット接続系とは、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　通信経路の分割とは、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　無害化通信とは、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　クラウドサービスとは、ネットワークを介して提供される情報処理及び情報保管等のサービスをいう。
⒁　外部サービスとは、町以外の者が提供する情報処理、保管、通信等の役務（クラウドサービス、オンライン会議、生成ＡＩ、ソーシャルメディア等を含む。）をいう。

（対象とする脅威）

第４条　情報資産に対する脅威として、次の脅威を想定し、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、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員不足に伴うシステム運用の機能不全等
⑸　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
⑹　委託先、再委託先、供給網に起因する事故、障害又は侵害

（適用範囲）

第５条　この訓令が適用される町の機関は、町長、町議会、教育委員会、選挙管理委員会、公平委員会、監査委員及び農業委員会とする。

（職員等の遵守義務）

第６条　職員、会計年度任用職員（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を遵守しなければならない。

（（情報セキュリティポリシーの構成））

第７条　情報セキュリティポリシーは、情報セキュリティ対策の基本的な方針を定めた基本方針（本要綱。以下、「基本方針」という。）及び当該方針を実行に移すための全ての情報

資産に共通する遵守事項及び判断基準を定めた対策基準（以下、「対策基準」という。）により構成する。

2　基本方針は公開することとし、対策基準は公開することにより町の情報セキュリティ確保に支障を生じ得る事項を含み得るため、非公開とする。

(情報セキュリティ対策)

第８条　第４条の脅威から情報資産を保護するために、次の情報セキュリティ対策を講じる。

⑴　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統一的に実施するため、全庁的な組織体制として、情報セキュリティ委員会を設置するとともに、情報セキュリティインシデントに緊急即応するための体制を整備する。

⑵　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。

⑶　情報システム全体の強靭性の向上

情報システム全体の強靭性向上のため、次に掲げる対策を講じる。

ア　マイナンバー利用事務系

原則として他の領域と通信できない構成とし、端末からの情報持ち出し制限、多要素認証等により、住民情報の流失を防止する。

イ　LGWAN接続系

LGWANに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の分割を行い、両システム間で通信する場合には、無害化通信等により安全性を確保する。

ウ　インターネット接続系

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とともに、自治体情報セキュリティクラウド等を活用し、監視、検知及び対処を強化する。

エ　動的アクセス制御の導入

ゼロトラストの考え方を踏まえ、動的なアクセス制御（利用者、端末、接続条件及びリスク状況に応じてアクセス権限を判断し、変更する仕組みをいう。）の導入を段階的に検討し、必要な対策を講じる。

⑷　物理的セキュリティ

端末、サーバ及び電磁的記録媒体、電算室、通信回線の管理については、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、啓発並びに訓練を行う等の人的な対策を講じる。

⑹　技術的セキュリティ

端末及びサーバの管理、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、情報資産に対するセキュリティ侵害等が発生した場合又は発生のおそれがある場合等に迅速かつ適正に対応するため、対応の具体的手順や平時における対応力向上のための措置を定めた緊急時対応計画を策定する。

⑻　外部サービスの利用

外部サービスを利用する場合には、利便性と安全性を両立させる観点から、次に掲げる原則に基づき契約を締結して行う。

ア　取扱情報の明確化

利用目的、取扱情報の機密性の分類、責任分界及び運用責任を明確にする。

イ　事前審査・台帳管理

機密性の高い情報を外部サービスで取り扱う場合は、利用開始前に審査し、外部サービス台帳に登録し、定期的に見直す。

ウ　客観的根拠に基づく選定

機密性の高い情報を取り扱うクラウドサービスは、原則として、公的又は第三者による評価・監査等により一定水準が確認できるものを優先して選定する。

エ　LGWAN 経由サービスの活用

LGWAN-ASP 等、閉域網を前提とする外部サービスについては、町の取扱情報及び運用要件に照らし、必要な統制が確保できるものを選定する。

オ　約款型サービスの統制

約款により提供され条件交渉が困難な外部サービスについては、サービス内容、データの保存・再利用・第三者提供・学習利用等の条件及び退出時措置を確認し、町の要件に合致する場合に限り利用する。

カ　ソーシャルメディアサービスの利用

ソーシャルメディアサービスを利用する場合には、当該サービスの運用ガイドラインを定め、当該サービスで発信できる情報を規定するとともに、利用に当たっては、責任者を定める。

キ　生成ＡＩ等の利用

生成ＡＩ等を利用する場合は、入力情報の取扱い（保存・学習利用等）及び出力物の正確性、権利、個人情報混入等のリスクを踏まえ、職員による確認を前提とした利用ルールを定め、これに基づき利用する。

⑼　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、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、情報セキュリティポリシーの見直しを行う。

（α’モデルを採用時の措置）

第９条　クラウドサービスの安全な活用のため、α’モデル（事前のリスク査定の結果を踏まえ、三層分離を基本とするネットワーク構成の安全性を維持しつつ、LGWAN 接続系の業務端末からインターネット経由で、特定のクラウドサービスを安全に利用するための対策（アクセス制御等）を組み込んだ構成という。）を採用する場合は、対象クラウドの限定、強固な認証、端末及び接続条件に基づくアクセス制御、ログ取得・保全等の必要な対策を講じる。

（情報セキュリティ監査及び自己点検の実施）

第10条　情報セキュリティポリシーの遵守状況及び対策の実効性を検証するため、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11条　情報セキュリティ監査及び自己点検の結果、脅威動向、制度改正、技術動向及び外部サービスの利用状況等を踏まえ、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は、情報セキュリティポリティーを見直す。

（情報セキュリティ対策基準）

第12条　第8条、第10条及び第11条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別要綱の八頭町行政情報セキュリティポリシー（対策基準）要綱で定める。

附　則