八重瀬町情報セキュリティ基本方針

１　目的

本基本方針は、八重瀬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、八重瀬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。

⑶情報資産

情報、情報を取り扱うための機器（情報を処理するコンピュータ、及びそれを利用するために必要なデータ通信装置、記憶媒体等を含む)、サービス（電力、通信サービス等を含む)、ソフトウェア、及びそれらを取り扱う人材をいう。

⑷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確保し、維持することをいう。

⑸情報セキュリティポリシー

組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書のことであり、「基本方針」と「対策基準」の総称のこと。

⑹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。

⑺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。

⑻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。

⑼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。

⑽LGWAN 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。（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)組織

八重瀬町の行政機関のことをいう。

(14)職員等

当該組織に勤務又は従事する全ての職員のことをいう。町長、副町長及びこれに準ずるもの、職員、嘱託職員、派遣職員、会計年度職員並びに委託職員のことをいう。

(15)第三者

当該組織には属さないが、業務上の関係のあるもののことをいう。

(16)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　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)台風、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

4　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、町長部局、教育委員会、農業委員会、選挙管理委員会、固定資産評価審査委員会、監査委員会及び議会事務局とする。

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り扱う情報（これらを印刷した文書を含む。）

③電力、通信サービス等のサービス

④ネットワーク、情報システム及びこれらに関するソフトウェア

⑤情報を取り扱う人材

⑥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　情報資産に対する基本的な考え方

情報資産に対する権限は、業務上必要なもののみに必要な権限のみを与えるものとする。また、必要な情報を適時に利用できるようにするための適切な体制を構築するものとする。

7　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

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。

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、最高情報統括責任者によって適切に管理された上で、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、都道府県と市区町村のインターネット接続口を集約した上で、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。

(5) 人的セキュリティ

情報セキュリティに関する権限や責任を定め、職員等に情報セキュリティポリシーの内容を周知徹底する等、職務に応じた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、ネットワーク管理等の技術的対策を講じる。

(7) 運用

職員等が機密性、完全性、可用性を守るため、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

業務委託する場合には、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。

8　情報資産の取り扱い

当該組織及び町民等が当該組織に預託した情報資産は、法令、契約および当該組織の定める情報セキュリティに関連する規定に従い、適切に取り扱われなければならな

い。

9　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い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) 部外者による意図的又は非意図的な要因による不正アクセスまたは不正操作によるデータやプログラムの持出・盗聴・改ざん・消去、機器及び媒体の盗難等

(2) 職員等及び外部委託者を含めた第三者による意図しない操作、故意の不正アクセスまたは不正操作によるデータやプログラムの持出・盗聴・改ざん・消去並びに機器及び媒体の規定外の端末接続によるデータ漏洩等

(3) 地震、落雷及び火災等の災害、事故並びに故障等によるサービス停止及び業務の停止

１０　教育

当該組織の全ての職員等は、定期的又は必要に応じて、職務に応じて必要な情報セキュリティ教育を受けなければならない。

１１　情報セキュリティ対策基準の策定

八重瀬町の様々な情報資産について、情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる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。

１２　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。

１３　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。

１４　情報セキュリティ事故の対応

(1) 情報セキュリティに関連する事故が発生した場合は、発見者は、情報セキュリティ対策基準に示された手順に従わなければならない。

(2) 職員等は、緊急事態が発生した際に危機管理対策に示された手順に従い、迅速に対応

しなければならない。

(3) 情報セキュリティに関連する事故原因は分析され、必要に応じて再発防止策を講じなければならない。

１５　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、リスクを検討したうえで、情報セキュリティポリシーを見直す。

１６　例外管理

技術的要件、費用等の問題等で情報セキュリティに関連する規定に定められた事項の達成が困難と認められる場合は、CISO 例外措置を講じることができる。