○国見町情報セキュリティ対策要綱

（令和３年４月１日訓令第８号）

改正 令和５年４月１日訓令第17号

国見町情報セキュリティ対策要綱（以下「本要綱」という。）は、国見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、国見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及び情報セキュリティ方針を実行に移すための国見町における情報資産に関する情報セキュリティ対策の基準を定めたものである。

第１編　情報セキュリティ基本方針

第１章　基本方針

（定義）

第１条　本要綱において、次に掲げる用語の定義は、それぞれ当該各号に定めるところによる。

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

情報セキュリティ基本方針、情報セキュリティ対策基準及び情報セキュリティ実施手順をいう。

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

マイナンバー利用事務系を除く、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。

(10)　インターネット接続系

インターネットメール及びホームページ管理システムで取り扱うデータをいう。

(11)　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。

(12)　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ないなど、安全が確保された通信をいう。

(対象とする脅威)

第2条　情報資産に対する脅威として、次に掲げる脅威を想定し、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、重要情報の詐取及び内部不正等

(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、外部委託管理の不備、マネジメントの欠陥及び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、落雷及び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、通信の途絶及び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3条　本要綱が対象とする適用範囲は、それぞれ当該各号に定めるところによる。

(1)　行政機関の適用範囲

ア　町長部局

イ　教育委員会

ウ　選挙管理委員会事務局

エ　監査委員事務局

オ　農業委員会事務局

カ　固定資産評価委員会事務局

キ　公営企業

ク　議会事務局

ケ　上記に掲げるもののほか、国見町が保有する情報資産を扱う組織に所属する者

⑵　情報資産の適用範囲（町小中学校における教育分野に係るものを除く。以下同様とする。）

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並びにこれらを印刷した文書

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

（職員等の遵守義務）

第４条　職員、非常勤職員、再任用職員、任期付職員及び会計年度任用職員等（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は、情報セキュリティポリシーを遵守しなければならない。

（情報セキュリティ対策）

第５条　第２条に定める脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講じる。

⑴　組織体制

国見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

国見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

情報セキュリティの強化を目的として、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て、次に掲げる３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こととし、その際の両システム間での通信については、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ため、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

ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための施設（以下「サーバ室」という。）、情報システムのある区域、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。

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など、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、アクセス制御及び不正プログラム対策など、技術的対策を講じる。

⑺　運用におけるセキュリティ対策

ア　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及び外部委託を行う際のセキュリティ確保など、情報セキュリティポリシーの運用面の対策を講じる。

イ　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。

⑻　外部サービスの利用

ア　外部委託する場合は、外部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するとともに、外部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た上で、必要に応じて契約に基づき措置を講じる。

イ　約款による外部サービスを利用する場合は、利用に係る規定を整備し、対策を講じる。

ウ　ソーシャルメディアサービスを利用する場合は、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。

⑼　評価及び見直し

ア　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。

イ　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。

（情報セキュリティ監査及び自己点検の実施）

第６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７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は、情報セキュリティポリシーを見直すものとする。

（情報セキュリティ対策基準の策定）

第８条　前３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定める対策基準を策定する。

（情報セキュリティ実施手順の策定）

第９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を策定するものとする。ただし、情報セキュリティ実施手順は、公にすることにより国見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。