北栄町情報システム管理要綱

平成20年２月15日

訓令第５号

（目的）

第１条　この要綱は、町が所管する情報資産の機密性、完全性及び可用性を確保するため、様々な脅威に対する抑止、予防、検知及び回復について、組織的かつ計画的に取り組むための統一的な方針であり、情報セキュリティを実践するに当たっての基本的な考え方及び方策を定めることを目的とする。

（用語の定義）

第２条　この要綱において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（１）　情報システム　端末やサーバ、ネットワークで構成された情報処理又は通信に用いる仕組みをいう。

（２）　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る情報システム及びデータをいう。

（３）　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。

（４）　インターネット接続系　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。

（５）　情報資産　情報システム及び情報システムにより処理又は通信される電子データをいう。

（６）　電子データ　電磁的方法(電子的方法、磁気的方法その他の人の知覚によっては認識することができない方法をいう。)により処理又は保管できる情報をいう。

（７）　ネットワーク　端末を相互に接続するための通信回線網及びその構成機器をいう。

（８） 記録媒体　ハードディスク、USBメモリ、フロッピーディスク、光学式ディスク(MO、CD、DVD等)、磁気テープ等電子データを記録する媒体をいう。

（９） サーバ　情報システムにおいて、端末からの要求に応じてサービスを提供するコンピュータのことをいう。

(10) 端末　コンピュータ、その周辺機器、プリンター等をいう。

(11) 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。

(12) 情報セキュリティポリシー　この要綱及び情報セキュリティ対策基準をいう。

(13) 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。

(14) 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。

(15) 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。

(16) 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。

(17) 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。

（対象となる脅威）

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） 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

（適用範囲）

第４条　この要綱が適用される行政機関は、内部部局、行政委員会、議会事務局及び地方公営企業とする。

２　この要綱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り扱う情報(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　職員、会計年度任用職員及び臨時的任用職員等(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。

（管理体制）

第６条　町は、情報資産の統一的な情報セキュリティを確保するため、全庁的な組織体制を整備する。

（情報の分類及び管理）

第７条　町は、情報資産について、情報の機密性、完全性及び可用性を踏まえ、適切な管理を行うものとする。

（情報セキュリティ対策）

第８条　町は、情報資産を故意(盗難、盗聴、不正アクセス、改ざん、破壊等)、過失(入力ミス、操作ミス等)、災害(火災、地震等)又は故障等の脅威から守るため、次の対策を講じる。

（１）　情報システム全体の強靭化の向上　情報セキュリティの強化を目的とし、業務の効率性・利便性を踏まえ、情報システム全体に対し、次の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。

（２）　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、情報資産への損害及び利用の妨害等から保護するための物理的な対策

（３）　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及び遵守すべき事項を明確に定め、職員等に対する周知及び徹底を図るとともに、十分な教育・啓発が行われるよう必要な対策

（４）　技術的セキュリティ対策　情報資産を不正アクセス等から保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術的な対策

（５） 運用等における対策　情報システムの監視、情報セキュリティ対策の遵守状況の確認等運用面の対策

（６） 緊急時におけるセキュリティ対策　緊急事態が発生した場合に、迅速かつ適切な対応が可能となるような危機管理対策の整備等による対策

（対策基準の策定）

第９条　町は、この要綱に基づき、情報セキュリティ対策を実施するに当たっての遵守すべき事項や、判断等の統一的な基準（以下「対策基準」という。）を定めるものとする。なお、対策基準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。

（実施手順の策定）

第10条　町は、この要綱及び対策基準に基づき、情報セキュリティ対策を具体的に実施するための手順（以下「実施手順」という。）を定めるものとする。なお、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。

（情報セキュリティ監査及び自己点検）

第11条　町は、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ものとする。

（評価及び見直し）

第12条　町は、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、情報セキュリティポリシーの見直しを実施するものとする。

附　則

この要綱は、平成20年３月１日から施行する。

附　則（平成27年３月31日訓令第20号）

この要綱は、平成27年４月１日から施行する。

附　則（令和２年12月４日訓令第26号）

この要綱は、令和２年12月４日から施行する。

附　則（令和８年３月６日訓令第８号）

この要綱は、令和８年３月６日から施行する。