利根町情報セキュリティポリシー

平成１７年　４月　１日　施行
平成３０年　６月２０日　全部改正
令和　２年　４月　１日　一部改正
令和　３年　４月　１日　一部改正
令和　５年　９月　１日　一部改正

目次

情報セキュリティ基本方針 3
１　目的 3
２　用語の定義 3
３　対象とする脅威 4
４　適用範囲 4
５　遵守義務 5
６　情報セキュリティ対策 5
７　自己点検の実施 6
８　情報セキュリティポリシーの見直し 6
９　情報セキュリティ対策基準の策定 6
１０　情報セキュリティ実施手順の策定 6

情報セキュリティ基本方針

１　目的

本基本方針は,本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,本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　用語の定義

この基本方針において，次の各号に掲げる用語の意義は，それぞれ当該各号に定めるところによる。

（１）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。

（２）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。

（３）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することをいう。

ア　機密性　情報にアクセスする権限のある者だけが，情報にアクセスできる状態を確保すること。

イ　完全性　情報が改ざん，破壊又は消去されていない状態を確保すること。

ウ　可用性　権限のある者が,いつでも必要な情報が利用できる状態を確保すること。

（４）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。

（５）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。

（６）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。）。

（７）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。

（８）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。

（９）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）故意による人的な脅威

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）過失による人的な脅威

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）情報システムの脅威

情報システムの故障，誤作動等

（4）自然の脅威

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

（5）その他の脅威

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及び電力供給の途絶，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

この基本方針の適用範囲は，次に定めるところによる。

（1）対象者の範囲

本基本方針が適用される行政機関は，町長，教育委員会（小中学校を除く。），農業委員会，選挙管理委員会，監査委員，固定資産評価審査委員会，議会とし，本町が保有する情報資産と情報資産に接する全ての職員，非常勤特別職の職員，会計年度任用職員，労働者派遣事業等により本町の事務に携わる者（以下「職員等」という。）及び委託事業者を対象とする。

（2）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。

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（これらを印刷した文書を含む。）

ウ　情報システムの仕様書及びネットワーク構成図等のシステム関連文書

5　遵守義務

前記４の対象者は，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　情報セキュリティ対策

町が管理する情報資産を脅威から保護するために，以下の情報セキュリティ対策を講ずるものとする。

（１）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。

（２）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。

（３）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ずる。

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，茨城県及び県内市町村のインターネットとの通信を集約した上で，いばらき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

情報システムを設置する施設への不正な立入り，情報資産への損傷，妨害等から保護するために物理的な対策を講ずる。

（５）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，情報セキュリティの啓発に有効と考えられる教育活動等，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，不正アクセス対策等の技術的な対策を講ずる。

（7）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，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ずるものとする。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の利用

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いた措置を講ずる。

約款による外部サービスを利用する場合には，利用にかかる規定を整備し対策を講ずる。

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。

（9）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，定期的又は必要に応じて自己点検を実施し，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，適宜情報セキュリティポリシーの見直しを行う。

7　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自己点検を実施する。

8　情報セキュリティポリシーの見直し

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を見直す。

9　情報セキュリティ対策基準の策定

本町における情報セキュリティ対策の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。なお，情報セキュリティ対策基準は，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。

１０　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。