標茶町訓令第23号

標茶町情報セキュリティ基本方針を次のように定める。

令和８年３月31日

標茶町長　佐藤　吉彦

標茶町情報セキュリティ基本方針

（目的）

第１条　この訓令は、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。

（定義）

第２条　この訓令において、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）　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及びその構成機器（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維持することをいう。

（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）　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。

（６）　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。

（７）　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。

（８）　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、地方税若又は防災に関する事務）又は戸籍事務等に係る情報システム及びその情報システムで取扱う情報をいう。

（９）　LGWAN接続系　人事給与、財務会計、文書管理等の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扱う情報をいう。

(10)　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扱う情報をいう。

(11)　通信経路の分離　LGWAN接続系及びインターネット接続系の通信を相互に分離した上で、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又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。

（対象とする脅威）

第３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、サービス不能攻撃その他のサイバー攻撃又は部外者の侵入その他の意図的な要因による情報資産の漏えい、破壊、改ざん又は消去、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、設計又は開発の不備、プログラム上の欠陥、操作又は設定のミス、メンテナンス不備、内部監査又は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、機器故障その他の非意図的要因による情報資産の漏えい、破壊又は消去等

（３）　地震、落雷、火災その他の災害によるサービス及び業務の停止等

（４）　大規模又は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、水道供給の途絶その他のインフラの障害からの波及等

（適用範囲）

第４条　この訓令が適用される対象機関及び対象とする情報資産の範囲は、以下のとおりとする。

（１）　この訓令が適用される対象機関は、町長部局、行政委員会、議会、教育委員会及びその所管に属する教育機関並びに地方公営企業とし、一部事務組合その他の関係団体については、必要に応じて情報セキュリティ対策の連携を図るものとする。

（２）　この訓令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、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　前条第１号に規定する機関に属する特別職及び一般職の職員（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。

（情報セキュリティ対策）

第６条　第３条で想定す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。

（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）　情報資産の分類及び管理　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、業務の効率性及び利便性の観点を踏まえ、情報システム全体に対し、次に掲げる対策を講じる。

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、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 と接続する情報システム及びインターネット接続系

の情報システムの通信を分離し、両者間で通信を行う場合には、無害化通信を行うものとする。

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に、都道府県が主体となり整備する自治体情報セキュリティクラウドを活用する。

（４）　物理的セキュリティ　サーバ、情報システム室、通信回線、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等の人的な対策を講じる。

（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対策を講じる。

（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、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し、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）　業務委託又は外部サービス（クラウドサービス）の利用　業務委託又は外部サービスを利用する場合は、次に掲げる対策を講じる。

ア　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き措置を講じる。

イ　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。

ウ　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。

（情報セキュリティ監査及び自己点検の実施）

第７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し、運用改善及び情報セキュリティの向上を図ると共に、必要に応じて、適宜情報セキュリティポリシーの見直しを行う。

（情報セキュリティポリシーの見直し）

第８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、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。

（情報セキュリティ対策基準の策定）

第９条　第６条から前条まで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

準等を定める情報セキュリティ対策基準を策定する。ただし、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情報セキュリティ確保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。

（情報セキュリティ実施手順の策定）

第 10 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本町の情報セキュリティ確保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。

附　則

この訓令は、令和８年４月１日から施行する。