美郷町情報資産管理規則

平成27年12月22日
規則第26号

（目的）

第１条　この規則は、美郷町（以下「町」という。）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に町が実施する情報セキュリティ対策を適切に管理、運用する基本的な事項を定め、もって町民の財産及びプライバシー等の保護の万全を期するとともに町の事務事業の安定的な運営を確保することを目的とする。

（定義）

第２条　この規則において、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）　情報資産　職員、非常勤職員、臨時的任用職員及び会計年度任用職員（以下「職員等」という。）が職務上使用することを目的として町が調達し、又は、開発した情報システム、庁内ネットワーク、外部電磁的記録媒体等に記録された情報及び紙媒体の情報であって、職員等が職務上取り扱う情報をいう。

（２）　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。

（３）　庁内ネットワーク　町長部局、行政委員会、議会及び地方公営企業の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。

（４）　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。また、ネットワーク接続をしない機器で情報処理を行う仕組みも同様とする。

（５）　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。

（６）　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。
（７）　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。
（８）　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。
（９）　情報セキュリティインシデント　情報資産に対して脅威となる事象の発生又は発生するおそれがあることをいう。
（１０）　情報セキュリティ対策基準　この規則に基づき情報セキュリティに関する対策（以下「情報セキュリティ対策」という。）を行うにあたり、統一的に遵守すべき行為、判断等の基準であって、別に定めるものをいう。
（１１）　情報セキュリティポリシー　この規則及び情報セキュリティ対策基準をいう。
（１２）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。
（１３）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。）。
（１４）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。
（１５）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。
（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、コンピュータウィ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。

（職員等の遵守義務）

第３条　職員等は、情報セキュリティの重要性について十分な認識を持つとともに、情報資産に関する業務を行うにあたり、情報セキュリティポリシーを遵守する義務を負うものとする。

（適用範囲）

第４条　この規則の適用範囲は、次に掲げるとおりとする。

（１）　行政機関の範囲　町長部局、行政委員会、議会及び地方公営企業。ただし、適用する範囲は行政ネットワークに限るものとする。

（２）　情報資産の範囲

ア　ネットワーク、情報システム及びこれらに関する設備、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及び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

（対象とする脅威）

第５条　情報資産に対する脅威として、次の各号に掲げる脅威を想定するものとする。

（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、外部委託管理の不備、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

（情報セキュリティ対策）

第６条　前条に規定する脅威から情報資産を保護するため、次に掲げる情報セキュリティ対策を講じる。

（１）　組織体制　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　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、当該分類に基づき管理を行う。

（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。

（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、情報セキュリティ対策基準の遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティ対策基準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切に対応するため、サイバー攻撃等及び機器故障・通信障害による情報セキュリティインシデント対応マニュアルを策定する。
（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。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。
（９）　評価・見直し　情報セキュリティ対策基準の遵守状況を検証するため、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。情報セキュリティ対策基準の見直しが必要な場合は、適宜情報セキュリティ対策基準の見直しを行う。
(情報セキュリティ対策基準の策定)

第７条　前条に規定する対策等を実施するための具体的な手順及び個別の実施事項を情報セキュリティ対策基準として定める。なお、当該対策基準は、公にすることにより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の実施）

第８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９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、情報セキュリティポリシーを見直すものとする。

附　則

この規則は、公布の日から施行する。

附　則（平成30年３月28日規則第８号）

この規則は、公布の日から施行する。

附　則（令和２年２月21日規則第９号）

この規則は、令和２年４月１日から施行する。

附　則（令和８年３月１６日規則第７号）

この規則は、令和８年４月１日から施行する。