○おいらせ町情報セキュリティ基本方針

令和６年３月２２日

訓令第６号

おいらせ町情報セキュリティポリシー規程(平成18年訓令第8号)の全部を改正する。

前文

おいらせ町長、おいらせ町議会、おいらせ町選挙管理委員会、おいらせ町監査委員、おいらせ町農業委員会、おいらせ町固定資産評価審査委員会は、おいらせ町情報セキュリティ基本方針を共同で定める。

また、当該基本方針については、地方自治法（昭和２２年法律第６７号）第２４４条の６第１項に規定するサイバーセキュリティを確保するための方針として位置付けるものとする。

(目的)

第１条　この訓令は、当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、当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、次の各号に定めるところによる。

（１）　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。

（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）　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。

（４） 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。

（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、必要な時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。

(職員等の遵守義務)

第３条　情報資産に関するすべての職員(地方公務員法(昭和 25 年法律第 261 号)第 22 条の２に規定する会計年度任用職員を含む。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。

(適用範囲)

第４条　この基本方針が適用される実施機関は、町長部局、教育委員会、議会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会とする。ただし、機関で扱う情報資産のうち、各機関により個別に定められた方針の対象となる情報資産は、この基本方針の対象外とする。

２　この基本方針が対象とする情報資産は、次の各号に掲げるとおりとする。

（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

(情報資産への脅威)

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

(情報セキュリティ対策)

第６条　前条で示した脅威から情報資産を保護するために、次の各号に掲げる情報セキュリティ対策を講ずるものとする。

（１） 組織体制　当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　当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） 物理的セキュリティ　サーバ、情報システム室、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。

（４） 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。

（５） 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。

（６） 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。

（７） 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。

（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する。

（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及び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ものとする。

（情報セキュリティ対策基準の策定）

第９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情報セキュリティ対策基準を定めるものとする。また、当該情報セキュリティ対策基準と異なる対応を必要とする機関は、当該対応に係る情報セキュリティ対策基準を別に策定することができる。

なお、対策基準は、公にすることにより当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(以下「実施手順」という。)を策定するものとする。なお、実施手順は、公にすることにより当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。

附　則

この訓令は、公表の日から施行する。

附　則

この訓令は、公表の日から施行する。