萩・長門清掃一部事務組合

情報セキュリティポリシー

令和８年（2026 年）３月１１日

目次

第１章　情報セキュリティ基本方針

１．　目的

本基本方針は、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、本組合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、本組合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．　定義

（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）情報資産

自治体の業務に係る紙の資料や電磁的記録媒体、サーバ等に保管されている情報全てのことを言う。

（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）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。

（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だけが、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）ＬGWAN（総合行政ネットワーク）接続系

ＬGWAN－ＡＳＰサービスを利用するための専用端末及びその専用端末で取り扱うデータをいう。

（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り扱うデータをいう。

（１１）職員

組合の情報資産を取り扱う、任用形態、職種及び勤務地を問わない組合の全職員をいう。

（１２）外部委託事業者

業務委託先社員（システム開発業務を委託する外部業者等）等、契約に基づいて市の機関で作業する者の総称をいう。

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）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

４． 適用範囲

（１）行政機関の範囲

本基本方針が適用される行政機関は、組合事務局、行政委員会及び議会事務局とする。

（２）情報資産の範囲

本基本方針が対象とする情報資産は、本組合の保有する全ての情報資産とする。

５． 職員の遵守義務

職員は、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

上記３の脅威から情報資産を保護するために、以下のセキュリティ対策を講じる。

（１）組織体制

本組合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

本組合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

（ア）ＬＧＷＡＮ（総合行政ネットワーク）接続系においては、ＬＧＷＡＮ－ＡＳＰサービス利用時の情報セキュリティ対策を実施する。

（イ）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。

（４）物理的セキュリティ

サーバ、通信回線及び職員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、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。

（８）業務委託とクラウドサービスの利用

業務委託する場合には、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。

クラウドサービスを利用する場合には、取扱う情報の機密性に留意する。

（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．　情報セキュリティ対策基準の策定

上記６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。

８． 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。

９． 情報セキュリティポリシーの公開

情報セキュリティ実施手順は、公開することにより行政運営に重大な支障を及ぼす恐れがあることから非公開とする。

第２章　情報セキュリティ対策基準

情報セキュリティ基本方針を適切に実施し、本組合が有する情報資産を守るための具体的な情報セキュリティ対策基準を定める。

１．　組織体制

（１）最高情報セキュリティ責任者（ＣＩＳＯ：Chief Information Security Officer、以下「ＣＩＳＯ」という。）

- 事務局長をＣＩＳＯとする。ＣＩＳＯは、本組合における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。
- ＣＩＳＯは、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。
- ＣＩＳＯは、情報セキュリティインシデントに対応するための計画（情報セキュリティ緊急時対応計画）を定めるものとする。

（２）情報セキュリティ責任者(次長)

- 事務局次長を情報セキュリティ責任者(次長)とする。
- 情報セキュリティ責任者(次長)は、本組合の情報セキュリティ対策に関する統括的な権限及び責任を有する。
- 情報セキュリティ責任者(次長)は、本組合において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。
- 情報セキュリティ責任者(次長)は、本組合において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約並びに本組合の情報資産を取り扱う、任用形態、職種及び勤務地を問わない本組合の全職員（以下「職員」という。）に対する教育、訓練、助言及び指示を行う。

（３）情報セキュリティ管理者(係長)

- 事務局総務管理係長を情報セキュリティ管理者(係長)とする。
- 情報セキュリティ管理者(係長)は、本組合の情報セキュリティ対策に関する権限及び責任を有する。
- 情報セキュリティ管理者(係長)は、本組合において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、情報セキュリティ責任者(次長)、統括情報セキュリティ責任者(次長)及びＣＩＳＯへ速やかに報告を行い、指示を仰がなければならない。

（４）情報システム担当者

- 情報セキュリティ管理者(係長)は、情報システム担当者を指名する。

・ 情報システム担当者は、情報セキュリティ管理者(係長)を補佐し、所管するシステムにおける情報セキュリティに関する事務を行う。

2． 情報資産の分類と管理

(1)情報資産の分類

本組合における情報資産は次のとおり分類し、職員は必要に応じ取扱い制限を行うものとする。

情報資産の分類

重要性	分類基準
重要性Ⅰ	個人情報及び業務上必要とする最小限の者のみが扱うデータ
重要性Ⅱ	公開することを予定していないデータ及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼすデータ その他情報セキュリティ管理者(係長)、又は情報セキュリティ責任者(次長)が必要と認めた情報資産
重要性Ⅲ	重要性Ⅰ又は重要性Ⅱの情報資産以外の情報資産

(2)情報資産の管理

情報資産は、その取扱う行政情報の重要性によって分類し、その重要性に応じて管理するものとする。

① 管理責任

(ア)情報セキュリティ責任者(次長)は、その所管する情報資産について管理責任を有する。

(イ)情報セキュリティ責任者(次長)は、情報資産が複製又は伝送された場合、複製等された情報資産も分類に基づき管理しなければならない。

② 情報資産の分類表示

(ア)職員は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

③ 情報の作成

(ア)職員は、業務上必要のない情報を作成してはならない。

(イ)情報を作成する職員は、情報の作成時に２．(１)「情報資産の分類」の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

(ウ)情報を作成する職員は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

④ 情報資産の入手

(ア)庁外の者が作成した情報資産を入手した者は、２．(１)「情報資産の分類」の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

(イ)情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ管理者(係長)に判断を仰がなければならない。

⑤ 情報資産の利用

(ア)情報資産を利用する職員は、業務以外の目的に情報資産を利用してはならない。

(イ)情報資産を利用する職員は、情報資産の分類に応じ、適正な取扱いをしなければならない。

(ウ)情報資産を利用する職員は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

⑥ 情報資産の保管

(ア)職員は、情報資産の分類に従って、情報資産を適正に保管しなければならない。なお、重要度の高いものについては、自然災害を被る可能性が低い場所にバックアップを保管するように努めるものとする。

(イ)職員は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

(ウ)職員は、重要性Ⅰ及び重要性Ⅱの情報を記録した電磁的記録媒体を保管する場合、安全で施錠可能な場所に保管しなければならない。

⑦ 情報の送信

(ア)電子メール等により重要性Ⅰ及び重要性Ⅱの情報を送信する職員は、必要に応じ、暗号化又はパスワード設定を行わなければならない。

⑧ 情報資産の運搬

(ア)車両等により重要性Ⅰ及び重要性Ⅱの情報資産を運搬する職員は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

(イ)重要性Ⅰ及び重要性Ⅱの情報資産を運搬する職員は、情報セキュリティ責任者(次長)に許可を得なければならない。

⑨ 情報資産の提供・公表

(ア)重要性Ⅰ及び重要性Ⅱの情報資産を外部に提供する職員は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

(イ)重要性Ⅰ及び重要性Ⅱの情報資産を外部に提供する職員は、情報セキュリティ責任者(次長)に許可を得なければならない。

(ウ)情報セキュリティ責任者(次長)は、住民に公開する情報資産について、完全性を確保しなければならない。

⑩ 情報資産の廃棄等

(ア)情報資産の破棄やリース返却等を行う者は、記録されている情報の機密性に応じ、情報を復元できないように処置した上で廃棄しなければならない。また、当

該措置を外部の者に依頼する場合は、確実に実施されたことを確認しなければならない。

(イ)情報資産の破棄やリース返却等を行う者は、行った処理について日時、担当者及び処理内容を記録しなければならない。

(ウ)情報資産の廃棄やリース返却等を行う者は、情報セキュリティ責任者(次長)の許可を得なければならない。

3． 情報システム全体の強靭性の向上

① ＬGWAN（総合行政ネットワーク）接続系

ＬGWAN（総合行政ネットワーク）接続系においては、専用の端末を新設し、ＬGWAN－ＡＳＰサービス利用方法手順に示されるセキュリティ対策を実施しなければならない。

② インターネット接続系

インターネット接続系においては、通信パケットの監視、 振る舞い 検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及び情報セキュリティ対策を講じなければならない。

4． 物理的セキュリティ

(1)サーバ等の管理

① 機器の取付

(ア)情報セキュリティ責任者(次長)は、サーバ等の機器の取付けを行う場合、火災、水害、ほこり、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう必要な措置を講じなければならない。

(イ)サーバ等の情報機器は、専用ラックに設置し施錠により管理するものとする。

② サーバの冗長化

(ア)情報セキュリティ責任者(次長)は、重要情報を格納しているサーバを冗長化（RAID 構成）し、同一データを保持するよう努めるものとする。

③ 機器の電源

(ア)情報セキュリティ責任者(次長)は、サーバ等機器電源について、停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に十分な電力を供給する容量の無停電電源装置を備え付けなければならない。

(イ)情報セキュリティ責任者(次長)は、工場運営会社と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

④ 通信ケーブル等の配線

(ア)情報システム担当者は、工場運営会社と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

(イ)情報システム担当者は、主要な箇所の通信ケーブル及び電源ケーブルについて、工場運営会社から損傷等の報告があった場合、連携して対応しなければならない。

(ウ)情報システム担当者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正に管理しなければならない。

(エ)情報セキュリティ責任者(次長)は、情報システム担当者及び契約により操作を認められた委託事業者以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

⑤ 機器の定期保守及び修理

(ア)情報セキュリティ管理者(係長)及び情報システム担当者は、定期的な保守が必要なサーバ等の機器の定期保守を実施しなければならない。

(イ)情報セキュリティ管理者(係長)及び情報システム担当者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報セキュリティ管理者(係長)は、外部の事業者に故障を修理させるに当たり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

⑥ 機器の廃棄等

(ア)情報セキュリティ管理者(係長)及び情報システム担当者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

(２)通信回線及び通信回線装置の管理

① 情報セキュリティ責任者(次長)及び情報セキュリティ管理者(係長)は、庁内の通信回線及び通信回線装置を、工場運営会社と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

② 情報セキュリティ責任者(次長)及び情報セキュリティ管理者(係長)は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

③ 情報セキュリティ責任者(次長)及び情報セキュリティ管理者(係長)は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

(３)職員の利用する端末や電磁的記録媒体等の管理

① 情報セキュリティ責任者(次長)は、盗難防止のため、利用端末のワイヤーによる固定や執務室の施錠等により管理しなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

② 情報セキュリティ責任者(次長)、情報セキュリティ管理者(係長)及び情報システム担当者は、情報システムへのログインに際し、パスワード、スマートカード、或いは生体認証等複数の認証情報の入力を必要とするように設定しなければならない。

５． 人的セキュリティ

（１）職員の遵守事項

① 情報セキュリティポリシー等の遵守

職員は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者(係長)に相談し、指示を仰がなければならない。

② 業務以外の目的での使用の禁止

職員は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

③ モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

(ア)職員は、本組合の情報資産を外部に持ち出す場合には、情報セキュリティ責任者(次長)の許可を得なければならない。

(イ)職員は、許可を得て情報資産を持ち出す場合、盗難、破損、紛失等に注意しなければならない。

④ 支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

(ア)職員は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、支給以外の端末の利用が業務上必要とＣＩＳＯが判断した場合は、利用することができる。

(イ)職員は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、以下の対策を講じなければならない。

・コンピュータウイルス対策
・ソフトウェアライセンス管理
・パスワード管理
・その他情報セキュリティ管理者(係長)が指示する対策

⑤ 持ち出し及び持ち込みの記録

情報セキュリティ責任者(次長)は、端末等および電磁的記録媒体の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

⑥ パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者(係長)の許可なく変更してはならない。

⑦ 机上の端末等の管理

職員は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ責任者(次長)の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

⑧ 退職時等の遵守事項

職員は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

(２)研修・訓練

職員は、構成市で開催される情報セキュリティ研修を受講するものとする。また、情報セキュリティ責任者(次長)は、職員の情報セキュリティ研修の受講状況を確認しなければならない。

(３)情報セキュリティインシデントの報告

① 職員は、情報セキュリティインシデントを発見又は外部から連絡を受けた場合には、速やかに情報セキュリティ管理者(係長)に報告し、指示を仰がなければならない。

② 情報セキュリティ管理者(係長)は、情報セキュリティインシデントの報告を受けた場合、軽微な事案を除き、情報セキュリティ責任者(次長)に報告し、指示を仰がなければならない。なお、情報セキュリティ責任者(次長)は、情報セキュリティインシデントの報告を受けた場合、必要に応じて、組合管理者、ＣＩＳＯに報告しなければならない。

③ 情報セキュリティ責任者(次長)は、個人情報・特定個人情報の漏えい等重大なセキュリティインシデントが発生した場合は、警察などの関係機関と連絡をとり、指示を受けなければならない。

④ 情報セキュリティ責任者(次長)、情報セキュリティ管理者(係長)及び情報システム担当者はは、情報セキュリティインシデントの原因調査及び分析を行い、再発防止策を講じなければならない。

(４)ＩＤ及びパスワードの管理

① ID の取扱い

職員は、自己の管理する ID に関し、次の事項を遵守しなければならない。

(ア)自己が利用している ID は、他人に利用させてはならない。

(イ)共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

② パスワードの取扱い

職員は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

(ア)パスワードは、他者に知られないように管理しなければならない。

(イ)パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

(ウ)パスワードは十分な長さとし、文字列は想像しにくいもの（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）にしなければならない。

(エ)パスワードが流出したおそれがある場合には、情報セキュリティ責任者(次長)に速やかに報告し、パスワードを速やかに変更しなければならない。

(オ)仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。

(カ)パソコン等の端末にパスワードを記憶させることで、パスワードの入力なしに認証を可能とする設定は行ってはならない。

6． 技術的セキュリティ

(1)コンピュータ及びネットワークの管理

① 文書サーバの設定等

(ア)情報セキュリティ管理者(係長)は、文書サーバを係等の単位で構成し、職員が他係のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

(イ)情報セキュリティ管理者(係長)は、個人情報、人事記録等、特定の職員しか取扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一係等であっても、担当職員以外の職員が閲覧及び使用できないようにしなければならない。

② バックアップの実施

情報セキュリティ責任者(次長)、情報セキュリティ管理者(係長)及び情報システム担当者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じてバックアップを実施しなければならない。

③ 情報システム仕様書等の管理

情報セキュリティ責任者(次長)、情報セキュリティ管理者(係長)及び情報システム担当者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧など、紛失等がないよう、適正に管理しなければならない。

④ ログの取得等

(ア)情報システム担当者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

(イ)情報セキュリティ責任者(次長)、情報セキュリティ管理者(係長)及び情報システム担当者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

⑤ 障害記録

情情報セキュリティ管理者(係長)及び情報システム担当者は、職員からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適正に保存しなければならない。

⑥ ネットワークの接続制御、経路制御等

(ア)情報セキュリティ責任者(次長)、情報セキュリティ管理者(係長)及び情報システム担当者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

(イ)情報セキュリティ責任者(次長)、情報セキュリティ管理者(係長)及び情報システム担当者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

⑦　無線ＬＡＮ及びネットワークの盗聴対策

(ア)情報セキュリティ責任者(次長)は、無線ＬＡＮの利用を認める場合、脆弱性が明らかである認証方式は利用してはならない。

(イ)情報セキュリティ責任者(次長)、情報セキュリティ管理者(係長)及び情報システム担当者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

⑧　電子メールの利用制限

(ア)職員は、自動転送機能を用いて、電子メールを転送してはならない。

(イ)職員は、業務上必要のない送信先に電子メールを送信してはならない。

(ウ)職員は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

(エ)職員は、重要な電子メールを誤送信した場合、速やかに電子メール送信先へ削除を促す旨の連絡を行い、情報セキュリティ責任者(次長)に報告しなければならない。

(オ)職員は、メールの添付ファイルや本文、差出人などが不審と感じるメールを受信した場合は、当該メールの添付ファイルやＵＲＬなどは開いてはならない。

(カ)職員は、情報セキュリティ責任者(次長)が業務上必要と許可しているサービスを除き、ウェブで利用できる電子メール、ネットワークストレージサービス等を使用してはならない。

⑨ 暗号化・パスワード設定

職員は、２．(１)「情報資産の分類」の重要性Ⅰ及び重要性Ⅱに当たる情報は原則として電子メールを利用して庁外に送信してはならない。業務上やむを得ず外部に送るデータの機密性又は完全性を確保することが必要な場合には、暗号化又はパスワード設定等、セキュリティを考慮し、情報セキュリティ責任者(次長)の許可を得た上で、送信しなければならない。

⑩ 無許可ソフトウェアの導入等の禁止

(ア)職員は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

(イ)職員は、業務上必要がある場合は、情報セキュリティ責任者(次長)及び情報セキュリティ管理者(係長)の許可を得てソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者(係長)は、ソフトウェアのライセンスを管理しなければならない。

(ウ)職員等は、不正にコピーしたソフトウェアを利用してはならない。

(エ)情報セキュリティ管理者(係長)は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

⑪ 機器構成の変更の制限

(ア)職員は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。

(イ)職員は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、情報セキュリティ責任者(次長)及び情報セキュリティ管理者(係長)の許可を得なければならない。

⑫ 無許可でのネットワーク接続の禁止

職員は、情報セキュリティ責任者(次長)の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

⑬ 業務以外の目的でのウェブ閲覧の禁止

職員は、業務以外の目的でウェブを閲覧してはならない。

情報セキュリティ責任者(次長)は、必要に応じて、職員のウェブ閲覧の内容を確認することができる。

情報セキュリティ責任者(次長)は、職員のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、適正な措置をしなければならない。

(２)アクセス制御

① アクセス制御

情報セキュリティ管理者(係長)及び情報システム担当者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員がアクセスできないように、必要最小限の範囲で適切に設定する等、システム上制限しなければならない。

② 利用者 ID の取扱い

情報セキュリティ責任者(次長)、情報セキュリティ管理者(係長)及び情報システム担当者は、利用者の登録、変更、抹消等の情報管理、職員の異動、退職者に伴う利用者ＩＤの取扱い等を適切に管理しなければならない。

③ 認証情報の管理

(ア)情報セキュリティ責任者(次長)、情報セキュリティ管理者(係長)及び情報システム担当者は、職員の認証情報を厳重に管理しなければならない。

(イ)情報セキュリティ責任者(次長)、情報セキュリティ管理者(係長)及び情報システム担当者は、認証情報の不正利用を防止するための措置を講じなければならない。

(３)システム開発、導入、保守等

① 機器等及び情報システムの調達

(ア)情報セキュリティ責任者(次長)は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。また、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載しなければならない。

(イ)機情報セキュリティ責任者(次長)は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

② 情報システムの導入

(ア)情報セキュリティ管理者(係長)及び情報システム担当者は、開発環境、検証環境と本番環境を分離しなければならない。

(イ)情報セキュリティ管理者(係長)及び情報システム担当者は、開発環境・検証環境から本番環境への移行について、手順を明確にしなければならない。

(ウ)情報セキュリティ管理者(係長)及び情報システム担当者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

(エ)情報セキュリティ管理者(係長)及び情報システム担当者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

③ 情報システム開発等の外部委託

情報セキュリティ責任者(次長)は、情報システム等の開発、導入、保守業務等を事業者に委託しようとする場合又は事業者の再委託を許可する場合は、事業者において情報セキュリティ対策が確実に実施されるようにしなければならない。

④ システム開発・保守に関連する資料等の整備・保管

情報セキュリティ管理者(係長)及び情報システム担当者は、システム開発・保守に関連する資料及びシステム関連文書を適正に整備・保管しなければならない。

⑤ 情報システムの変更管理

情報セキュリティ管理者(係長)及び情報システム担当者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

⑥ 情報システムについての対策の見直し

情報セキュリティ管理者(係長)は、自己点検等の結果等に合わせ、情報セキュリティ対策を適切に見直さなければならない。また、改善が必要となる情報セキュリティ対策が確認された場合は、情報セキュリティ対策を適切に見直さなければならない。

(4)不正プログラム対策

① 情報セキュリティ管理者(係長)及び情報システム担当者の措置事項

(ア)コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員に対して注意喚起しなければならない。

(イ)サーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

(ウ)不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

(エ)不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

(オ)業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。

② 職員の順守事項

(ア)パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

(イ)外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

(ウ)メールの添付ファイルや本文、差出人などが不審と感じるメールを受信した場合は、情報セキュリティ管理者(係長)及び情報セキュリティ委員会事務局に報告しなければならない。その際、当該メールの添付ファイルやＵＲＬなどは開いてはならない。

(エ)端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

(オ)添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。

(カ)提供のあるウイルス情報を、常に確認しなければならない。

(キ)コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、直ちにネットワークから切断し、自ら駆除せずに電源を入れたまま報告をし、指示を仰がなければならない。また、完全に駆除が終了するまでネットワークへの再接続と、該当する端末での業務を行ってはならない。

(５)不正アクセス対策

① 攻撃への対処

ＣＩＳＯ、情報セキュリティ責任者（次長）は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。また、構成市等と連絡を密にして情報の収集に努めなければならない。

② 記録の保存

ＣＩＳＯ、情報セキュリティ責任者（次長）は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

③ 内部からの攻撃

情報セキュリティ管理者（係長）及び情報情報システム担当者は、職員が使用しているパソコン等の端末から庁内のサーバや外部サイト等に対する攻撃を監視しなければならない。

④ 職員による不正アクセス

情報セキュリティ管理者（係長）及び情報情報システム担当者は、職員による不正アクセスを発見した場合は、情報セキュリティ責任者（次長）に報告し、適正な処置を求めなければならない。

⑤ 標的型攻撃

情報セキュリティ責任者（次長）、情報セキュリティ管理者（係長）及び情報情報システム担当者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、必要に応じて教育等の人的対策を講じなければならない。

(6)セキュリティ情報の収集

情報セキュリティ責任者（次長）及び情報セキュリティ管理者（係長）は、情報セキュリティに関する情報を収集し、必要に応じ関係者間で共有し、職員に周知しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

7． 運用

(1)情報システムの監視

① 情報セキュリティ責任者（次長）及び情報セキュリティ管理者（係長）は、セキュリティに関する事案を検知するため、情報システムを監視しなければならない。

② 情報セキュリティ責任者（次長）及び情報セキュリティ管理者（係長）は、重要なログ等を取得するサーバの正確な時刻設定ができる措置を講じなければならない。情報セキュリティポリシーの遵守状況の確認

(2)情報セュリティポリシーの遵守状況の確認

① 遵守状況の確認及び対処

(ア)情報セキュリティ責任者（次長）は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかにＣＩＳＯに報告しなければならない。

(イ)ＣＩＳＯは、発生した問題について、適正かつ速やかに対処しなければならない。

(ウ)情報セキュリティ責任者（次長）及び情報セキュリティ管理者（係長）は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

② パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

ＣＩＳＯ及びＣＩＳＯが指名した者は、不正アクセス、不正プログラム等の調査のために、職員が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

③ 職員の報告義務

(ア)職員は、情報セキュリティポリシーに対する違反行為を発見した場合、ただちに情報セキュリティ責任者（次長）に報告を行わなければならない。

(イ)当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると情報セキュリティ責任者（次長）が判断した場合において、職員は、実施手順等により適正に対処しなければならない。

(3)侵害時の対応等

① 緊急時対応計画の策定

ＣＩＳＯは、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、情報セキュリティ緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

② 緊急時対応計画に盛り込むべき内容

情報セキュリティ緊急時対応計画には、以下の内容を定めなければならない。

(ア)発生した事案に係る報告すべき事項

(イ)発生した事案への対応措置

(ウ)再発防止措置の策定

③ 業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定するとともに、業務継続計画の策定時及び変更時等において、当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

④ 緊急時対応計画の見直し

ＣＩＳＯは、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて情報セキュリティ緊急対応実施手順の規定を見直さなければならない。

(4)法令等の遵守

職員は、職務の遂行において使用する情報資産を保護するために、次の法令等のほか関係法令を遵守し、これに従わなければならない。

① 地方公務員法（昭和 25 年法律第 261 号）

② 著作権法（昭和 45 年法律第 48 号）

③ 不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）

④ 個人情報の保護に関する法律（平成 15 年法律第 57 号）

⑤ 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）

⑥ サイバーセキュリティ基本法（平成 26 年法律第 104 号）

⑦ 萩・長門清掃一部事務組合個人情報の保護に関する法律施行条例（令和５年３月１日条例第１号）

(5)懲戒処分等

① 懲戒処分

情報セキュリティポリシーに違反した職員及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

② 違反時の対応

職員の情報セキュリティポリシーに違反する行動を確認した者は、速やかにＣＩＳＯに通知し、適正な措置を求めなければならない。

ＣＩＳＯの指導によっても改善されない場合、情報セキュリティ管理者（係長）及び情報システム担当者は、当該職員のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、職員の権利を停止あるいは剥奪した旨を組合管理者に通知しなければならない。

8． 業務委託とクラウドサービスの利用

（1）業務委託

① 委託事業者の選定基準

(ア)情報セキュリティ責任者（次長）は、外部委託事業者の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

(イ)情報セキュリティ責任者（次長）は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者を選定しなければならない。

② 契約項目

情報セキュリティ管理者（係長）及び情報システム担当者は、情報システムの運用、保守等を外部委託する場合には、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

(ア)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の遵守
(イ)外部委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
(ウ)提供されるサービスレベルの保証
(エ)外部委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法
(オ)外部委託事業者の従業員に対する教育の実施
(カ)提供された情報の目的外利用及び受託者以外の者への提供の禁止
(キ)業務上知り得た情報の守秘義務
(ク)再委託に関する制限事項の遵守
(ケ)委託業務終了時の情報資産の返還、廃棄等
(コ)委託業務の定期報告及び緊急時報告義務
(サ)市による監査、検査
(シ)市による情報セキュリティインシデント発生時の公表
(ス)情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

③ 確認・措置等

情報セキュリティ管理者（係長）は、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定期的に確認し、必要に応じ、②の契約に基づき措置を実施

しなければならない。また、その内容を情報セキュリティ責任者（次長）に報告しなければならない。

④ 業務委託終了時の対策

（2）クラウドサービス

① 職員は、クラウドサービスを利用する場合は、情報セキュリティ責任者（次長）の許可を得なければならない。

② 情報セキュリティ責任者（次長）は、当該サービス提供事業者の信頼性が十分であることを総合的・客観的に評価し判断した上で、許可をしなければならない。

9． 点検・見直し

（1）点検

① 情報セキュリティ責任者（次長）、情報報セキュリティ管理者（係長）及び情報システム担当者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

② 情報セキュリティ責任者（次長）は、情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行わなければならない。

③ 情報セキュリティ責任者（次長）は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、職員に通知しなければならない。

④ 職員は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

（2）見直し

① 情報セキュリティ責任者（次長）は、点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。

② 情報セキュリティ責任者（次長）、情報セキュリティポリシーの改訂に応じて実施手順を見直すものとする。

附 則

この情報セキュリティポリシーは、令和８年４月１日から施行する。