

下関市行政情報セキュリティポリシー

下 関 市

令和6年4月1日

目 次

情報セキュリティ基本方針

第1. 目的	1
第2. 定義	1
(1) ネットワーク	1
(2) 情報システム	1
(3) 情報セキュリティ	1
(4) 情報セキュリティポリシー	1
(5) 機密性	1
(6) 完全性	1
(7) 可用性	1
(8) マイナンバー利用事務系（個人番号利用事務系）	1
(9) LGWAN 接続系	1
(10) インターネット接続系	1
(11) 通信経路の分離	1
(12) 無害化通信	1
(13) 記録媒体	2
(14) 外部サービス	2
第3. 対象とする脅威	2
第4. 適用範囲	2
(1) 対象範囲	2
(2) 情報資産の範囲	2
第5. 職員等の遵守義務	3
第6. 情報セキュリティ対策	3
(1) 組織体制	3
(2) 情報資産の分類と管理	3
(3) 情報システム全体の強靱性の向上	3
(4) 物理的セキュリティ	3
(5) 人的セキュリティ	3
(6) 技術的セキュリティ	3
(7) 運用	3
(8) 業務委託と外部サービスの利用	4
(9) 評価・見直し	4
第7. 情報セキュリティ監査及び自己点検の実施	4
第8. 情報セキュリティポリシーの見直し	4
第9. 情報セキュリティ対策基準の策定	4
第10. 情報セキュリティ実施手順の策定	4

情報セキュリティ対策基準

第1．組織体制	5
(1) 最高情報セキュリティ責任者	5
(2) 統括情報セキュリティ責任者	5
(3) 統括情報セキュリティ責任者補佐官	5
(4) 情報セキュリティ責任者	6
(5) 情報セキュリティ管理者	6
(6) 情報システム管理者	6
(7) 情報システム担当者	6
(8) 兼務の禁止	6
(9) CSIRT の設置・役割	7
(10) クラウドサービス利用における組織体制	7
第2．情報資産の分類と管理	7
(1) 情報資産の分類	7
(2) 情報資産の管理	8
(3) 個人情報の管理	10
(4) 特定個人情報の管理	11
第3．情報システム全体の強靱性の向上	11
1 マイナンバー利用事務系	11
(1) マイナンバー利用事務系と他の領域との分離	11
(2) 情報のアクセス及び持ち出しにおける対策	11
(3) マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの扱い	11
(4) マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱い	11
2 LGWAN 接続系	12
(1) LGWAN 接続系とインターネット接続系の分割	12
(2) LGWAN 接続系と接続されるクラウドサービス上での情報システムの扱い	12
3 インターネット接続系	12
第4．物理的セキュリティ	12
1 サーバ等の管理	12
(1) 機器の取付け	12
(2) サーバの冗長化	12
(3) 機器の電源	13
(4) 通信ケーブル等の配線	13
(5) 機器の定期保守及び修理	13

(6) 外部への機器の設置	13
(7) 機器の廃棄等	13
2 管理区域の管理	15
(1) 管理区域の構造等	15
(2) 管理区域の入退室管理等	15
(3) 機器等の搬入出	16
3 通信回線及び通信回線装置の管理	16
4 職員等の利用する端末や電磁的記録媒体等の管理	16
第5. 人的セキュリティ	17
1 職員等の遵守事項	17
(1) 職員等の遵守事項	17
(2) 会計年度任用職員及び特別職非常勤職員への対応	18
(3) 情報セキュリティポリシー等の掲示	18
(4) 委託事業者に対する説明	18
2 研修及び訓練	18
(1) 情報セキュリティに関する研修及び訓練	18
(2) 研修計画の策定及び実施	19
(3) 緊急時対応訓練	19
(4) 研修及び訓練への参加	19
3 情報セキュリティインシデントの報告	19
(1) 職員等内部での情報セキュリティインシデントの報告	19
(2) 住民等外部からの情報セキュリティインシデントの報告	20
(3) 情報セキュリティインシデント原因の究明、記録、再発防止等	20
4 ID 及びパスワード等の管理	20
(1) IC カード等の取扱い	20
(2) ID の取扱い	21
(3) パスワードの取扱い	21
第6. 技術的セキュリティ	21
1 情報システム等の管理	21
(1) ファイルサーバの設定等	21
(2) バックアップの実施	21
(3) 他団体との情報システムに関する情報等の交換	22
(4) システム管理記録及び作業の確認	22
(5) 情報システム仕様書等の管理	22
(6) ログの取得等	22
(7) 障害記録	23
(8) ネットワークの接続制御、経路制御等	23
(9) 外部の者が利用できるシステムの分離等	23

(10)	外部ネットワークとの接続制限等	23
(11)	複合機のセキュリティ管理	23
(12)	IoT 機器を含む特定用途機器のセキュリティ管理	24
(13)	無線 LAN 及びネットワークの盗聴対策	24
(14)	電子メールのセキュリティ管理	24
(15)	電子メールの利用制限	24
(16)	電子署名等	24
(17)	無許可ソフトウェアの導入等の禁止	25
(18)	機器構成の変更の制限	25
(19)	業務外でのネットワークへの接続の禁止	25
(20)	業務以外の目的でのウェブ閲覧の禁止	25
(21)	Web 会議サービスの利用時の対策	25
2	アクセス制御等	25
(1)	アクセス制御等	25
(2)	職員等による外部からのアクセス等の制限	26
(3)	ログイン時の表示等	27
(4)	認証情報の管理	27
(5)	特権による接続時間の制限	27
3	システム開発、導入、保守等	27
(1)	情報システムの調達	27
(2)	情報システムの開発	27
(3)	情報システムの導入	28
(4)	システム開発・保守に関連する資料等の整備・保管	28
(5)	情報システムにおける入出力データの正確性の確保	28
(6)	情報システムの変更管理	29
(7)	開発・保守用のソフトウェアの更新等	29
(8)	システム更新・統合時の検証等	29
4	不正プログラム対策	29
(1)	統括情報セキュリティ責任者補佐官等の措置事項	29
(2)	職員等の遵守事項	30
(3)	専門家の支援体制	30
5	不正アクセス対策	30
(1)	統括情報セキュリティ責任者補佐官等の措置事項	30
(2)	攻撃への対処	31
(3)	記録の保存	31
(4)	内部からの攻撃	31
(5)	職員等による不正アクセス	31
(6)	サービス不能攻撃	32

(7) 標的型攻撃	32
6 セキュリティ情報の収集	32
(1) セキュリティホールに関する情報の収集及び共有並びにソフトウェアの更新等	32
(2) 不正プログラム等のセキュリティ情報の収集及び周知	32
(3) 情報セキュリティに関する情報の収集及び共有	32
第7. 運用	32
1 情報システムの監視	32
2 情報セキュリティポリシーの遵守状況の確認	33
(1) 遵守状況の確認及び対処	33
(2) 端末、電磁的記録媒体等の利用状況調査	33
(3) 職員等の報告義務	33
3 侵害時の対応等	34
(1) 緊急時対応計画の策定	34
(2) 緊急時対応計画に盛り込むべき内容	34
(3) ICT 部門における業務継続計画との整合性確保	34
(4) 緊急時対応計画の見直し	34
4 例外措置	34
(1) 例外措置の許可	34
(2) 緊急時の例外措置	34
(3) 例外措置の申請書の管理	34
5 法令遵守	34
6 懲戒処分等	35
(1) 懲戒処分	35
(2) 違反時の対応	35
第8. 業務委託と外部サービスの利用	35
1 業務委託	35
(1) 委託事業者の選定基準	35
(2) 契約項目	35
(3) 確認・措置等	36
2 外部サービスの利用（機密性2以上の情報を取り扱う場合）	36
(1) 外部サービスの利用に係る規定の整備	36
(2) 外部サービスの選定	36
(3) 外部サービスの利用承認	38
(4) 外部サービスの利用に係る調達・契約	38
(5) 外部サービスを利用した情報システムの導入・構築時の対策	38
(6) 外部サービスを利用した情報システムの運用・保守時の対策	38
(7) 外部サービスを利用した情報システムの更改・廃棄時の対策	39

3	外部サービスの利用（機密性2以上の情報を取り扱わない場合）・・・	39
	（1）外部サービスの利用に係る規定の整備	39
	（2）外部サービスの利用における対策の実施	39
4	ソーシャルメディアサービスの利用	40
第9.	評価等	40
1	監査	40
	（1）実施方法	40
	（2）監査を行う者の要件	40
	（3）監査実施計画の策定及び実施への協力	40
	（4）委託事業者に対する監査	40
	（5）報告	41
	（6）保管	41
	（7）監査結果への対応	41
	（8）情報セキュリティポリシー及び関係規程等の見直し等への活用・	41
2	自己点検	41
	（1）実施方法	41
	（2）報告	41
	（3）自己点検結果の活用	41
3	情報セキュリティポリシー及び関係規程等の見直し	42

情報セキュリティ基本方針

第1．目的

本基本方針は、本市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、本市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。

第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（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の定義による）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。

(9) 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。）。

(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) 通信経路の分離

ある領域と他の領域との通信をできない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。

(13) 記録媒体

「記録媒体」とは、情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物と、電子的方式、磁気的方式その他の知覚によっては認識することができない方式で作られる記録であって、情報処理の用に供されるものに係る記録媒体（以下「電磁的記録媒体」という。）がある。

(14) 外部サービス

一般の業者等の庁外の組織が情報システムの一部又は全部の機能を提供するクラウドサービス、ホスティングサービス、ハウジングサービス、ソーシャルメディアサービス等をいう。

第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及び部外者の侵入等の意図的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

第4. 適用範囲

(1) 対象範囲

本基本方針の適用範囲は、下関市事務分掌条例（平成17年条例第11号）第1条に掲げる部局及び下関市役所総合支所設置条例（平成17年条例第13号）第1条に掲げる総合支所並びに出納室、教育委員会の事務部局（小中学校については、統括情報セキュリティ責任者補佐官が管理するシステムの利用に係る部分に限る。）、選挙管理委員会事務局、監査委員事務局、公平委員会事務局、農業委員会事務局、議会事務局、消防局、上下水道局及びポートレース企業局とする。

(2) 情報資産の範囲

本基本方針が対象とする情報資産は、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機器及び設備並びに電磁的記録媒体
- 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図等のシステム関連文書

エ その他、第２（１３）に定める記録媒体及びそれに記録されている情報

第５．職員等の遵守義務

職員、会計年度任用職員及び特別職非常勤職員（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。

第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、以下の情報セキュリティ対策を講じる。

（１）組織体制

本市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

本市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靱性の向上

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、必要に応じて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、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。

（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、契約に基づき措置を講じる。

外部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。

また、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。

第7. 情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、毎年度及び必要に応じて、情報セキュリティ監査及び自己点検を実施する。

第8. 情報セキュリティポリシーの見直し

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。

第9. 情報セキュリティ対策基準の策定

上記6、7及び8に規定する対策等を実施するために、具体的な遵守事項、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。

第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市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。

情報セキュリティ対策基準

本対策基準は、情報セキュリティ基本方針を実行に移すための、本市における情報資産に関する情報セキュリティ対策の基準を定めたものである。

第1．組織体制

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

ア 副市長をCISOとする。CISOは、本市におけるすべてのネットワーク、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。

イ CISO は、情報セキュリティインシデントに対処するための体制（CSIRT：Computer Security Incident Response Team、以下「CSIRT」という。）を整備し、役割を明確化する。

ウ CISO は、本市の情報セキュリティ対策を統一的に実施するため、情報セキュリティポリシー等の情報セキュリティに関する重要な事項を決定する。

エ CISO は、必要に応じて、本市における情報セキュリティ対策の改善計画を策定し、その実施状況を確認することができる。

(2) 統括情報セキュリティ責任者

ア 総合政策部長をCISO直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者はCISOを補佐しなければならない。

イ 統括情報セキュリティ責任者は、本市の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、CISOの指示に従い、CISOが不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。

ウ 統括情報セキュリティ責任者は、緊急時にはCISOに早急に報告を行うとともに、回復のための対策を講じなければならない。

(3) 統括情報セキュリティ責任者補佐官

ア 情報政策課長を統括情報セキュリティ責任者補佐官とする。

イ 統括情報セキュリティ責任者補佐官は、本市のすべてのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

ウ 統括情報セキュリティ責任者補佐官は、本市のすべてのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

エ 統括情報セキュリティ責任者補佐官は、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

オ 統括情報セキュリティ責任者補佐官は、本市の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

カ 統括情報セキュリティ責任者補佐官は、緊急時等の円滑な情報共有を図るため、CISO、統括情報セキュリティ責任者、統括情報セキュリティ責任者補佐官、情報セキュリティ責

任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

- キ 統括情報セキュリティ責任者補佐官は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて CISO 及び統括情報セキュリティ責任者にその内容を報告しなければならない。

(4) 情報セキュリティ責任者

- ア 部局等の長（出納室にあつては会計管理者）を情報セキュリティ責任者とする。
- イ 情報セキュリティ責任者は、所管する部局等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。
- ウ 情報セキュリティ責任者は、所管する部局等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。
- エ 情報セキュリティ責任者は、所管する部局等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職員等に対する教育、訓練、助言及び指示を行う。

(5) 情報セキュリティ管理者

- ア 各課所の長（出納室にあつては出納室長）を情報セキュリティ管理者とする。
- イ 情報セキュリティ管理者は、所管する課所等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。
- ウ 情報セキュリティ管理者は、所管する課所等において、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、情報セキュリティインシデントの報告方法に沿って速やかに報告を行い、指示を仰がなければならない。

(6) 情報システム管理者

- ア 各情報システムの担当課所の長（出納室にあつては出納室長）を当該情報システムの情報システム管理者とする。
- イ 情報システム管理者は、所管する情報システムにおける開発、設定の変更、運用、更新等を行う権限及び責任を有する。
- ウ 情報システム管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。
- エ 情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

(7) 情報システム担当者

情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者を情報システム担当者とする。

(8) 兼務の禁止

- ア 情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。
- イ 情報セキュリティ監査の実施において、やむを得ない場合を除き、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

(9) CSIRT の設置・役割

- ア CISO は、CSIRT を整備し、その役割を明確化しなければならない。
- イ CISO は、CSIRT に所属する職員等を選任し、その中から CSIRT 責任者を置かなければならない。また、CSIRT 内の業務統括及び外部との連携等を行う職員等を定めなければならない。
- ウ CISO は、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。
- エ CISO による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供しなければならない。
- オ 情報セキュリティインシデントを認知した場合には、CISO、総務省、都道府県等へ報告しなければならない。
- カ 情報セキュリティインシデントを認知した場合には、その重要度及び影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。
- キ 情報セキュリティに関して、関係機関及び他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、委託事業者等との情報共有を行わなければならない。

(10) クラウドサービス利用における組織体制

情報セキュリティ責任者は、クラウドサービスを利用する際には、複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制を構築しなければならない。また、クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立しなければならない。

第2. 情報資産の分類と管理

(1) 情報資産の分類

本市における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じて、取扱制限を行うものとする。

機密性による情報資産の分類

分類	分類基準	取扱制限
機密性3	行政事務で取り扱う情報資産のうち、秘密保全を要する文書（以下「秘密文書」という。）に相当する機密性を要する情報資産	・機密性3の情報資産に対する支給以外のパソコン及びモバイル端末（以下「端末」という。）での作業の原則禁止 ・必要以上の複製及び配付の禁止

機密性 2	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	<ul style="list-style-type: none"> ・保管場所の制限及び保管場所への必要以上の端末、電磁的記録媒体等の持込みの禁止 ・情報の送信、情報資産の運搬又は提供時における暗号化、パスワードの設定又は鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う場合の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
機密性 1	機密性 2 以上の情報資産以外の情報資産	

完全性による情報資産の分類

分類	分類基準	取扱制限
完全性 2	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	<ul style="list-style-type: none"> ・バックアップ及び電子署名の付与 ・外部で情報処理を行う場合の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
完全性 1	完全性 2 の情報資産以外の情報資産	

可用性による情報資産の分類

分類	分類基準	取扱制限
可用性 2	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	<ul style="list-style-type: none"> ・バックアップ及び指定する時間以内の復旧 ・外部で情報処理を行う場合の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
可用性 1	可用性 2 の情報資産以外の情報資産	

(2) 情報資産の管理

ア 管理責任

- (ア) 情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。
- (イ) 情報セキュリティ管理者は、情報資産が複製又は伝送された場合には、複製等された情報資産も（１）の分類に基づき管理しなければならない。
- (ウ) 情報システム管理者は、クラウドサービスの環境に保存される情報資産についても（１）の分類に基づき管理しなければならない。また、情報資産におけるライフサイクル（作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等）の取扱いを定め、クラウドサービスを更改する際の情報資産の移行及びこれらの情報資産の全ての複製のクラウドサービス事業者からの削除の記述を含むサービス利用の終了に関する内容について、サービス利用前に文書での提示を求め、又は公開されている内容を確認しなければならない。

イ 情報資産の分類の表示

職員等は、情報資産について、必要に応じて、ファイル（ファイル名、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、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。

ウ 情報の作成

- (ア) 職員等は、業務上必要のない情報を作成してはならない。
- (イ) 情報を作成する者は、情報の作成時に（１）の分類に基づき、当該情報の分類及び取扱制限を定めなければならない。
- (ウ) 情報を作成する者は、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。

エ 情報資産の入手

- (ア) 職員等が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。
- (イ) 職員等以外の者が作成した情報資産を入手した者は、（１）の分類に基づき、当該情報の分類及び取扱制限を定めなければならない。
- (ウ) 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は、情報セキュリティ管理者に判断を仰がなければならない。

オ 情報資産の利用

- (ア) 情報資産を利用する者は、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者は、情報資産の分類に応じて、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者は、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。

カ 情報資産の保管

- (ア) 情報セキュリティ管理者又は情報システム管理者は、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。

(イ) 情報セキュリティ管理者又は情報システム管理者は、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) 情報セキュリティ管理者又は情報システム管理者は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い場所に保管するよう努めなければならない。

(エ) 情報セキュリティ管理者又は情報システム管理者は、機密性 2 以上、完全性 2 又は可用性 2 の情報を記録した電磁的記録媒体を保管する場合、施錠可能な場所に保管し、耐火、耐熱、耐水及び耐湿についても考慮しなければならない。

キ 情報の送信

電子メール等により機密性 2 以上の情報を送信する者は、必要に応じて、パスワード等による暗号化を行わなければならない。

ク 情報資産の運搬

(ア) 車両等により機密性 2 以上の情報資産を運搬する者は、必要に応じて、鍵付きのケース等に格納し、パスワード等による暗号化を行う等、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) 機密性 2 以上の情報資産を運搬する者は、情報セキュリティ管理者の許可を得なければならない。

ケ 情報資産の提供等

(ア) 機密性 2 以上の情報資産を外部に提供する者は、必要に応じて、パスワード等による暗号化を行わなければならない。

(イ) 機密性 2 以上の情報資産を外部に提供する者は、情報セキュリティ管理者の許可を得なければならない。

(ウ) 情報セキュリティ管理者は、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。

コ 情報資産の廃棄等

(ア) 情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体が不要になった場合、記録されている情報の機密性に応じ、電磁的記録媒体の情報を復元できないように処置しなければならない。

(イ) 情報資産の廃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、情報セキュリティ管理者の許可を得なければならない。

(エ) 情報システム管理者は、クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時には、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

(3) 個人情報の管理

統括情報セキュリティ責任者補佐官、情報セキュリティ管理者及び情報システム管理者は、

個人情報について、その機密性等に応じ、別に定める下関市個人情報取扱要綱に基づき管理を行わなければならない。

(4) 特定個人情報の管理

統括情報セキュリティ責任者補佐官、情報セキュリティ管理者及び情報システム管理者は、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）第2条に規定する特定個人情報について、機密性3、完全性2及び可用性2を有する情報資産に位置付け、別に定める下関市特定個人情報取扱要綱に基づき管理を行わなければならない。

第3. 情報システム全体の強靱性の向上

1 マイナンバー利用事務系

(1) マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(MACアドレス、IP アドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。

ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWANを経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

(2) 情報のアクセス及び持ち出しにおける対策

(ア) 情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。また、業務毎に専用端末を設置することが望ましい。

(イ) 情報の持ち出し不可設定

原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

(3) マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの扱い

マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるクラウド上の情報システムの領域については、マイナンバー利用事務系として扱い、本市の他の領域とはネットワークを分離しなければならない。

(4) マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱い

マイナンバー利用事務系の情報システムをクラウドにおいて利用する場合は、その情報資産の機密性を考慮し、暗号による対策を実施するものとする。その場合、暗号は十分な強度を持たなければならない。

また、クラウドサービス事業者が暗号に関する対策を行う場合又はクラウドサービス事業者が提供する情報資産を保護するための暗号機能を利用する場合、クラウドサービス事

業者が提供するそれらの機能や内容について情報を入手し、その機能について理解に努め、必要な措置を行わなければならない。

2 LGWAN 接続系

(1) LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は両環境間の通信経路を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信等を図らなければならない。

(ア) インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送するメールテキスト化方式

(イ) インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

(ウ) 危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

(2) LGWAN 接続系と接続されるクラウドサービス上での情報システムの扱い

LGWAN 接続系の情報システムをクラウドサービス上へ配置する場合は、その領域を LGWAN 接続系として扱い、マイナンバー利用事務系とネットワークを分離し、専用回線を用いて接続しなければならない。

3 インターネット接続系

(1) インターネット接続系においては、通信パケットの監視、ふるま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 LGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を必要に応じて講じなければならない。

(2) 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する自治体情報セキュリティクラウドへの参加等、関係省庁や都道府県等と連携しながら、情報セキュリティ対策を推進しなければならない。

第4. 物理的セキュリティ

1 サーバ等の管理

(1) 機器の取付け

情報システム管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、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適正に固定する等、必要な措置を講じなければならない。

(2) サーバの冗長化

ア 情報システム管理者は、必要に応じて、重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバその他基幹サーバを冗長化し、同一データを保持しなければならない。

イ 情報システム管理者は、サーバの冗長化を行っている場合、メインサーバに障害が発

生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。

(3) 機器の電源

ア 情報システム管理者は、必要に応じて統括情報セキュリティ責任者補佐官及び施設管理部門と連携し、サーバ等の機器の電源について、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予備電源を備え付けなければならない。

イ 情報システム管理者は、必要に応じて統括情報セキュリティ責任者補佐官及び施設管理部門と連携し、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 情報システム管理者は、統括情報セキュリティ責任者補佐官及び施設管理部門と連携し、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 統括情報セキュリティ責任者補佐官及び情報システム管理者（以下「統括情報セキュリティ責任者補佐官等」という。）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、施設管理部門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 情報システム管理者は、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 情報システム管理者は、自ら又は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及び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 情報システム管理者は、可用性2の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 情報システム管理者は、電磁的記録媒体を内蔵する機器を事業者修理に依頼する場合、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、情報システム管理者は、事業者修理に依頼するにあたり、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) 外部への機器の設置

情報システム管理者は、外部にサーバ等の機器等を設置する場合、CISO、統括情報セキュリティ責任者及び統括情報セキュリティ責任者補佐官の承認を得なければならない。また、必要に応じて、当該機器等への情報セキュリティ対策状況について確認しなければならない。

(7) 機器の廃棄等

ア 情報システム管理者は、機器を廃棄、リース返却等をする場合、次の表に沿った措置を講じなければならない。

情報の機密性に応じた機器の廃棄等の方法

分類	機器の廃棄等の方法	確実な履行を担保する方法
----	-----------	--------------

<p>(1) マイナンバー利用事務系の領域において住民情報を保存する電磁的記録媒体</p>	<p>当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすることが必要である。</p> <p>なお、対象となる機器について、リース契約により調達する場合においても、リース契約終了後、当該機器の電磁的記録媒体については、物理的に破壊を行う。この場合、予め仕様に明記のうえ、機器の廃棄方法を契約において明記することが望ましい。</p>	<p>職員が左記措置の完了まで立ち会いによる確認を行う方法又は、庁舎内において後述(3)で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の完了証明書により確認する方法のいずれかとする。当該完了証明書については、破壊の証拠写真が添付されるとともに、その提出期限が定められていることが望ましい。</p>
<p>(2) 機密性2以上に該当する情報を保存する電磁的記録媒体 (上記(1)に該当するものを除く。)</p>	<p>一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消(下記例①～⑤のうちいずれかの方法)を行うことが必要である。</p> <p>【例】</p> <p>① 物理的な方法による破壊</p> <p>② 磁気的な方法による破壊</p> <p>③ OS等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去</p> <p>④ ブロック消去</p> <p>⑤ 暗号化消去</p>	<p>庁舎内において後述(3)で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認する方法など適切な方法により確認を行う。</p>
<p>(3) 機密性1に該当する情報を保存する電磁的記録媒体</p>	<p>一般的に入手可能な復元ツールの利用によっても復元が困難な状態に消去することが必要である。</p> <p>具体的には、(2)に記述した方法①～⑤のほか、OS等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアにより上書き</p>	<p>庁舎内において消去を実施し、職員が作業完了を確認する方法など適切な方法により確認を行う。</p>

	<p>消去する方法がある。</p> <p>OS 及び記憶装置の初期化(フォーマット等)による方法は、HDD の記憶演算子にはデータの記憶が残った状態となるため、適当ではない。</p>	
--	---	--

※上記(1)は、オンプレミスの場合を想定したもの(ハウジングを含む)

イ 情報システム管理者は、クラウドサービス事業者が利用する資源(装置等)の処分(廃棄)について、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手順について確認しなければならない。

なお、当該確認にあたっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用してもよい。

2 管理区域の管理

(1) 管理区域の構造等

ア 管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うため等の部屋(以下「情報システム室等」という。)並びに電磁的記録媒体の保管庫をいう。

イ 情報システム管理者は、管理区域を地階又は1階以外に設けるように努めなければならない。また、外部からの侵入が容易にできないようにしなければならない。

ウ 情報システム管理者は、施設管理部門と連携し、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

エ 情報システム管理者は、情報システム室内の機器等に、転倒、落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

オ 情報システム管理者は、施設管理部門と連携し、管理区域を囲む外壁等の開口部からの侵入が容易にできないようにしなければならない。

カ 情報システム管理者は、管理区域に配置する消火薬剤、消防用設備等が、機器及び記録媒体に影響を与えないようにしなければならない。

(2) 管理区域の入退室管理等

ア 情報システム管理者は、管理区域への入退室を許可された者のみに制限し、ICカード、指紋認証等の生体認証又は入退室管理簿の記載による入退室管理を行わなければならない。

イ 職員等及び委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

ウ 情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて、立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うもの

とし、外見上職員等と区別できる措置を講じなければならない。

エ 情報システム管理者は、機密性 2 以上の情報資産を取り扱う管理区域について、当該情報システムに関連しない、または個人所有である端末、通信回線装置、電磁的記録媒体等を許可なく持ち込ませないようにしなければならない。

(3) 機器等の搬入出

ア 情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員等又は委託事業者を確認を行わせなければならない。

イ 情報システム管理者は、管理区域への機器等の搬入出について、職員を立ち会わせなければならない。

3 通信回線及び通信回線装置の管理

ア 統括情報セキュリティ責任者補佐官等は、施設管理部門と連携し、内部の通信回線及び通信回線装置並びにこれらに関する文書を適正に管理・保管しなければならない。

イ 統括情報セキュリティ責任者補佐官等は、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。

ウ 統括情報セキュリティ責任者補佐官等は、内部情報系のネットワークを総合行政ネットワーク（LGWAN）に集約するように努めなければならない。

エ 統括情報セキュリティ責任者補佐官等は、機密性 2 以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じて、送受信される情報の暗号化を行わなければならない。

オ 統括情報セキュリティ責任者補佐官等は、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。

カ 統括情報セキュリティ責任者補佐官等は、可用性 2 の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じて、回線を冗長構成にする等の措置を講じなければならない。

4 職員等の利用する端末や電磁的記録媒体等の管理

ア 情報セキュリティ管理者は、盗難防止のため、執務室等で利用するパソコンのワイヤーによる固定、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を講じなければならない。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。

イ 情報システム管理者は、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、あるいは生体認証等、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。

ウ 情報システム管理者は、端末の電源起動時のパスワード（BIOS パスワード、ハードディスクパスワード等）を併用するよう努めなければならない。

エ 情報システム管理者は、マイナンバー利用事務系では「知識」、「所持」、「存在」を利用

する認証手段のうち二つ以上を併用する認証（多要素認証）を行うよう設定しなければならない。

オ 情報システム管理者は、端末におけるデータの暗号化等の機能を必要に応じて有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についてもデータ暗号化の機能を備えた機器を使用するよう努めなければならない。

カ 情報システム管理者は、モバイル端末を外部で業務利用する場合は、必要に応じて上記対策に加え、遠隔消去機能を利用する等の措置を講じなければならない。

第5．人的セキュリティ

1 職員等の遵守事項

(1) 職員等の遵守事項

ア 情報セキュリティポリシー等の遵守

職員等は、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又は遵守することが困難な点がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

イ 業務以外の目的での使用の禁止

職員等は、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。

ウ 端末、電磁的記録媒体等の持出し及び外部における情報処理作業の制限

(ア) 情報セキュリティ責任者は、自らが所管するシステムについて、機密性2以上、完全性2又は可用性2の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

(イ) 職員等は、情報資産を外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

(ウ) 職員等は、外部で情報処理作業を行う場合には、情報セキュリティ管理者の許可を得なければならない。

(エ) 職員等は、機密性2以上、完全性2又は可用性2の情報資産を外部で情報処理作業を行う場合には、安全管理措置に関する規定を遵守しなければならない。

エ 支給以外の端末、電磁的記録媒体等の業務利用

職員等は、支給以外の端末、電磁的記録媒体等を原則として業務に利用してはならない。ただし、業務上必要な場合は、情報セキュリティ管理者及び情報システム管理者の許可を得て利用することができる。

オ 持出し及び持込みの記録

情報セキュリティ管理者は、端末等の持出し及び持込みについて、記録を作成し、保管しなければならない。

カ 端末におけるセキュリティ設定変更の禁止

職員等は、端末のセキュリティ機能の設定を情報システム管理者の許可なく変更して

はならない。

キ 机上の端末等の管理

職員等は、端末、電磁的記録媒体、情報が印刷された文書等について、第三者に使用され、又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時の端末のロック、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。

ク 退職時等の遵守事項

職員等は、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。

ケ クラウドサービス利用時等の遵守事項

職員等は、クラウドサービスの利用にあたり、情報セキュリティポリシーを遵守し、クラウドサービスの利用に関する自らの役割及び責任を意識しなければならない。

(2) 会計年度任用職員及び特別職非常勤職員（以下「会計年度任用職員等」という。）への対応

ア 情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、会計年度任用職員等に対し、採用時に情報セキュリティポリシー等のうち、会計年度任用職員等が守るべき内容を理解させ、実施及び遵守させなければならない。

イ 情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は、会計年度任用職員等の採用の際、必要に応じて、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

ウ インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、会計年度任用職員等に端末による作業を行わせる場合において、インターネットへの接続、電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

(3) 情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるようにしなければならない。

(4) 委託事業者に対する説明

情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を事業者委託する場合、再委託事業者も含めて、情報セキュリティポリシー等のうち委託事業者が守るべき内容を遵守させなければならない。

2 研修及び訓練

(1) 情報セキュリティに関する研修及び訓練

ア CISO は、クラウドサービスを含むシステムを利用する職員等に対して、情報セキュリティに関する意識向上を図るとともに研修及び訓練を定期的実施しなければならない。

イ 情報システム管理者は、委託先を含む関係者については委託先等でどのような教育及び訓練が行われているかを確認し、記録を残さなければならない。

(2) 研修計画の策定及び実施

ア CIS0 は、すべての職員等に対する情報セキュリティに関する研修計画の策定及びその実施体制の構築を定期的に行わなければならない。

イ CIS0 は、研修計画において、職員等が毎年度最低 1 回は情報セキュリティ研修を受講できるように努めなければならない。

ウ CIS0 は、研修計画において、新規採用の職員等を対象とする情報セキュリティに関する研修を計画しなければならない。

エ 研修は、統括情報セキュリティ責任者、統括情報セキュリティ責任者補佐官、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者その他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

オ 情報セキュリティ管理者は、所管する課室等の教育の実施状況を記録し、統括情報セキュリティ責任者及び情報セキュリティ責任者に対して、報告しなければならない。

カ 統括情報セキュリティ責任者は、教育の実施状況を分析、評価し、CIS0 に情報セキュリティ対策に関する教育の実施状況について報告しなければならない。

キ CIS0 は、職員等の情報セキュリティ研修の実施状況について報告が行われるように、実施体制を構築しなければならない。

(3) 緊急時対応訓練

CIS0 は、緊急時対応を想定した訓練を必要に応じて、実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、効果的に実施できるようにしなければならない。

(4) 研修及び訓練への参加

職員等は、定められた研修及び訓練に参加するよう努めなければならない。

3 情報セキュリティインシデントの報告

(1) 職員等内部での情報セキュリティインシデントの報告

ア 職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口で報告しなければならない。

イ 情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、速やかに統括情報セキュリティ責任者補佐官、情報セキュリティ責任者及び関係する情報システム管理者に報告しなければならない。

ウ 統括情報セキュリティ責任者補佐官は、報告のあった情報セキュリティインシデントについて、CIS0 及び統括情報セキュリティ責任者に報告しなければならない。

エ 情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、複数の課所に関係がある場合には、関係する課所の情報セキュリティ管理者に報告しなければならない。

オ 情報セキュリティ管理者は、クラウドサービス利用における情報セキュリティインシデントの報告について連絡体制の対象者に報告しなければならない。

(2) 住民等外部からの情報セキュリティインシデントの報告

ア 職員等は、本市が管理する情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、情報セキュリティ管理者に報告しなければならない。

イ 情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、速やかに統括情報セキュリティ責任者補佐官及び関係する情報システム管理者に報告しなければならない。

ウ 統括情報セキュリティ責任者補佐官は、報告のあった情報セキュリティインシデントについて、必要に応じて CISO 及び統括情報セキュリティ責任者に報告しなければならない。

エ 情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、必要に応じて情報セキュリティ責任者に報告しなければならない。

オ 情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、複数の課所に関係がある場合には、関係する課所の情報セキュリティ管理者に報告しなければならない。

カ 情報システム管理者は、クラウドサービス事業者が検知した情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みの構築を契約等で取り決めるか、約款等により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原因の究明、記録、再発防止等

ア CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

イ CSIRT は、情報セキュリティインシデントであると評価した場合、CISO に速やかに報告しなければならない。

ウ CSIRT は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。

エ CSIRT は、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明結果から、再発防止策を検討し、CISO に報告しなければならない。

オ CISO は、CSIRT から、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

4 ID 及びパスワード等の管理

(1) IC カード等の取扱い

ア 職員等は、自己の管理する IC カード等に関し、次の事項を遵守しなければならない。
(ア) 認証に用いる IC カード等を職員等間で共有してはならない。ただし、共用の IC カードについては、この限りでない。

(イ) 業務上必要のないときは、IC カード等をカードリーダー、端末のスロット等から抜いておかなければならない。

(ウ) IC カード等を紛失した場合には、速やかに情報セキュリティ管理者に報告し、指示に従わなければならない。

イ 情報セキュリティ管理者は、IC カード等の紛失等の報告があった場合、当該 IC カード等を使用したアクセス等を速やかに停止する措置を講じなければならない。

ウ 情報システム管理者は、IC カード等を切り替える場合、切替え前のカードを回収し、復元できないように処置しなければならない。

(2) ID の取扱い

職員等は、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 の利用者以外の者に利用させてはならない。

(3) パスワードの取扱い

職員等は、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、他人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、速やかに情報セキュリティ管理者に報告し、パスワードを変更しなければならない。

オ 複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。ただし、シングルサインオンを利用している場合は、この限りでない。

カ 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。

キ サーバ、ネットワーク機器及び端末にパスワードを記憶させてはならない。

ク 職員等間でパスワードを共有してはならない。ただし、共用 ID のパスワードについては、この限りでない。

第 6. 技術的セキュリティ

1 情報システム等の管理

(1) ファイルサーバの設定等

ア 情報システム管理者は、職員等が使用できるファイルサーバの容量を設定し、職員等に周知しなければならない。

イ 情報システム管理者は、ファイルサーバを構成する際に、職員等が権限のない課所等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。

ウ 情報システム管理者は、住民の個人情報、人事記録等、特定の職員等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、同一課所等であっても、担当職員以外の職員等の閲覧及び使用を防止するようにしなければならない。

(2) バックアップの実施

情報システム管理者は、業務システムのデータベースやファイルサーバ等に記録された情報について、クラウドサービス等システムの提供形態及びサーバの冗長化対策に関わらず、定期的にバックアップを実施しなければならない。

(3) 他団体との情報システムに関する情報等の交換

情報システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、統括情報セキュリティ責任者、統括情報セキュリティ責任者補佐官及び情報セキュリティ責任者の許可を得なければならない。

(4) システム管理記録及び作業の確認

ア 情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

イ 情報システム管理者は、所管する情報システムにおいて、設定変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理しなければならない。

ウ 情報システム管理者又は情報システム担当者若しくは契約により操作を認められた委託事業者がシステム変更等の作業を行う場合は、2名以上で作業し、互いにその作業を確認しなければならない。ただし、システム障害の危険性を伴わない作業については、この限りでない。

(5) 情報システム仕様書等の管理

情報システム管理者は、ネットワーク構成図及び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の閲覧、紛失等がないよう、適正に管理しなければならない。

(6) ログの取得等

ア 情報システム管理者は、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 情報システム管理者は、ログとして取得する項目、保存期間、取扱方法、ログが取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。

ウ 情報システム管理者は、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、取得したログの点検及び分析を実施しなければならない。なお、クラウドサービス事業者が収集し、保存する記録（ログ等）に関する保護（改ざんの防止等）の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認しなければならない。

エ 情報システム管理者は、監査及びデジタルフォレンジックに必要となるクラウドサービス事業者の環境内で生成されるログ等の情報（デジタル証拠）について、クラウドサービス事業者から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、クラウドサービス事業者に提出を要求するための手続を明確にしなければならない。

ない。

(7) 障害記録

情報システム管理者は、職員等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。

(8) ネットワークの接続制御、経路制御等

ア 情報システム管理者は、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 情報システム管理者は、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。

(9) 外部の者が利用できるシステムの分離等

情報システム管理者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じて、他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

(10) 外部ネットワークとの接続制限等

ア 情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、統括情報セキュリティ責任者補佐官の許可を得なければならない。

イ 情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、内部のすべてのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

ウ 情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊又は改ざん、システムダウン等による業務への影響が生じた場合に対処するため、必要に応じて、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

エ 情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、内部ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

オ 情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者補佐官の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

(11) 複合機のセキュリティ管理

ア 複合機を管理する課所は、統括情報セキュリティ責任者補佐官と連携し、複合機を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

イ 複合機を管理する課所は、統括情報セキュリティ責任者補佐官と連携し、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

ウ 複合機を管理する課所は、統括情報セキュリティ責任者補佐官と連携し、複合機の運

用を終了する場合、複合機の電磁的記録媒体に記録されたすべての情報を抹消する又は再利用できないようにする対策を講じなければならない。

(1 2) IoT 機器を含む特定用途機器のセキュリティ管理

統括情報セキュリティ責任者補佐官等は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

(1 3) 無線 LAN 及びネットワークの盗聴対策

ア 情報システム管理者は、無線 LAN を利用する場合、解読が困難な暗号化及び認証技術を使用しなければならない。

イ 情報システム管理者は、無線 LAN を利用する場合、利用する無線 LAN が内部のすべてのネットワーク、情報システム等の情報資産に影響が生じないことを確認し、統括情報セキュリティ責任者補佐官の許可を受けなければならない。

ウ 情報システム管理者は、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るよう努めなければならない。

エ マイナンバー利用事務系においては無線 LAN を利用してはならない。

(1 4) 電子メールのセキュリティ管理

ア 情報システム管理者は、権限のない利用者により、外部から外部への電子メールの転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

イ 情報システム管理者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。

ウ 情報システム管理者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

エ 情報システム管理者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

オ 情報システム管理者は、システム開発、運用、保守等のため庁舎内に常駐している委託事業者の作業員による電子メールアドレス利用について、委託事業者との間で利用方法を取り決めなければならない。

(1 5) 電子メールの利用制限

ア 職員等は、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。ただし、情報システム管理者が特に必要と認めるときは、この限りでない。

イ 職員等は、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 職員等は、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 職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。

(1 6) 電子署名等

ア 職員等は、情報資産の分類により定めた取扱制限に従い、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、CISO が定めた電子署名、パスワード等による暗号化等を使用し、セキュリティを考慮して、送信しなければならない。

イ 職員等は、暗号化を行う場合に CISO が定める以外の方法を用いてはならない。また、CISO が定めた方法で暗号のための鍵を管理しなければならない。

ウ CISO は、電子署名の正当性を検証するための情報又は手段を署名検証者へ安全に提供しなければならない。

(17) 無許可ソフトウェアの導入等の禁止

ア 職員等は、端末に無断でソフトウェアを導入してはならない。

イ 職員等は、業務上の必要がある場合は、情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する場合は、情報セキュリティ管理者又は情報システム管理者は、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。

(18) 機器構成の変更の制限

ア 職員等は、端末に対し機器の改造、増設及び交換を行ってはならない。

イ 職員等は、業務上、端末に対し機器の改造、増設及び交換を行う必要がある場合には、情報システム管理者の許可を得なければならない。

(19) 業務外でのネットワークへの接続の禁止

ア 職員等は、支給された端末を有線・無線を問わず、その端末を接続して利用するよう情報システム管理者によって定められたネットワークと異なるネットワークに接続してはならない。

イ 情報システム管理者は、支給した端末について、必要に応じて、端末に搭載された OS のポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限しなければならない。

(20) 業務以外の目的でのウェブ閲覧の禁止

ア 職員等は、業務以外の目的でウェブを閲覧してはならない。

イ 統括情報セキュリティ責任者補佐官等は、職員等のウェブ利用について、明らかに業務以外の目的でサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適正な措置を求めなければならない。

(21) Web 会議サービスの利用時の対策

ア 情報システム管理者は、Web 会議を適切に利用するための利用手順を定めなければならない。

イ 職員等は、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施しなければならない。

ウ 職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講じなければならない。

2 アクセス制御等

(1) アクセス制御等

ア アクセス制御

情報システム管理者は、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等がアクセスできないように、システム上制限しなければならない。

イ 利用者 ID の取扱い

(ア) 情報システム管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向及び退職に伴う利用者 ID の取扱い等の方法を定めなければならない。

(イ) 情報セキュリティ管理者は、業務上必要がなくなった場合は、利用者登録を抹消するよう、情報システム管理者に通知しなければならない。

(ウ) 情報システム管理者は、利用されていない ID が放置されないよう、人事管理部門と連携し、点検しなければならない。

ウ 特権を付与された ID の管理等

(ア) 情報システム管理者は、管理者権限等の特権を付与された ID を利用する者を必要最小限にし、当該 ID 及びパスワードの漏えい等が発生しないよう、当該 ID 及びパスワードを厳重に管理しなければならない。

(イ) 情報システム管理者の特権を代行する者は、情報システム管理者が指名した者でなければならない。

(ウ) 情報システム管理者は、特権を付与された ID 及びパスワードの変更について、委託事業者に行わせてはならない。

(エ) 情報システム管理者は、特権を付与された ID 及びパスワードについて、職員等の端末等のパスワードよりも厳重に管理しなければならない。

(オ) 情報システム管理者は、特権を付与された ID を初期設定以外のものに変更しなければならない。

(2) 職員等による外部からのアクセス等の制限

ア 職員等又は委託事業者が外部から内部のネットワーク又は情報システムにアクセスする場合は、統括情報セキュリティ責任者補佐官及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

イ 統括情報セキュリティ責任者補佐官等は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

ウ 統括情報セキュリティ責任者補佐官等は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

エ 統括情報セキュリティ責任者補佐官等は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

オ 統括情報セキュリティ責任者補佐官等は、外部からのアクセスに利用する端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

カ 職員等は、持ち込んだ又は外部から持ち帰った端末を内部のネットワークに接続する前に、コンピュータウイルス等の不正プログラム（以下「不正プログラム」という。）に感染していないこと、パッチの適用状況等を確認し、情報セキュリティ管理者の許可を

得てから接続しなければならない。

キ 統括情報セキュリティ責任者補佐官等は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者の ID、パスワード及び生体認証に係る情報等の認証情報並びにこれを記録した媒体（IC カード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

（３）ログイン時の表示等

情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定、ログイン・ログアウト時刻の表示等の機能がある場合、その機能を有効に活用し、正当なアクセス権を持つ職員等がログインしたことを確認することができるようシステムを設定しなければならない。

（４）認証情報の管理

ア 情報システム管理者は、職員等の認証情報を厳重に管理しなければならない。認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

イ 情報システム管理者は、職員等に対してパスワードを発行する場合は、原則、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させなければならない。

ウ 統括情報セキュリティ責任者又は情報システム管理者は、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。

（５）特権による接続時間の制限

情報システム管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

３ システム開発、導入、保守等

（１）情報システムの調達

ア 情報システム管理者は、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。

イ 情報システム管理者は、情報システム開発、導入等における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、統括情報セキュリティ責任者補佐官と連携して、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。

ウ 情報システム管理者は、情報システム開発、導入等における機器及びソフトウェアの調達に当たっては、内部のすべてのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

（２）情報システムの開発

ア システム開発における責任者及び作業者の特定

情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための規則を確立しなければならない。

イ システム開発における責任者、作業者のIDの管理

(ア) 情報システム管理者は、システム開発の責任者及び作業者が使用するIDを管理し、開発完了後、当該IDを削除しなければならない。ただし、そのまま運用保守に用いる場合はこの限りではない。

(イ) 情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならない。

ウ システム開発に用いるハードウェア及びソフトウェアの管理

(ア) 情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

(イ) 情報システム管理者は、システムに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。

(3) 情報システムの導入

ア 開発環境と運用環境の分離及び移行手順の明確化

(ア) 情報システム管理者は、必要に応じて、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。

(イ) 情報システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

(ウ) 情報システム管理者は、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之、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) 情報システム管理者は、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。

イ テスト

(ア) 情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

(イ) 情報システム管理者は、運用テストを行う場合、あらかじめテスト環境による操作確認を行わなければならない。

(ウ) 情報システム管理者は、個人情報及び機密性の高い生データをテストデータに使用してはならない。

(エ) 情報システム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織及び導入する組織が、それぞれ独立したテストを行わなければならない。

(4) システム開発・保守に関連する資料等の整備・保管

ア 情報システム管理者は、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。

イ 情報システム管理者は、テスト結果を一定期間保管しなければならない。

ウ 情報システム管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

(5) 情報システムにおける入出力データの正確性の確保

ア 情報システム管理者は、情報システムに入力されるデータについて、範囲及び妥当性のチェック機能並びに不正な文字列等の入力除去する機能を組み込むように情報システムを設計しなければならない。

イ 情報システム管理者は、故意又は過失により情報が改ざんされ、又は漏えいするおそれがある場合に、これを検出する機能を組み込むように情報システムを設計しなければならない。

ウ 情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

(6) 情報システムの変更管理

情報システム管理者は、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。

(7) 開発・保守用のソフトウェアの更新等

情報システム管理者は、開発・保守用のソフトウェア等を更新し、又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

(8) システム更新・統合時の検証等

情報システム管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

4 不正プログラム対策

(1) 統括情報セキュリティ責任者補佐官等の措置事項

統括情報セキュリティ責任者補佐官等は、不正プログラム対策として、次の事項を措置しなければならない。

ア 外部ネットワークに接続しているシステムにおいて、外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいて不正プログラムのチェックを行う等、不正プログラムのシステムへの侵入を防止しなければならない。

イ 外部ネットワークに接続しているシステムにおいて、外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいて不正プログラムのチェックを行う等、不正プログラムの外部への拡散を防止しなければならない。

ウ 不正プログラムの情報を収集し、必要に応じて職員等に対して注意喚起しなければならない。

エ 所掌するサーバ、端末に、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。

オ 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。

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

キ 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。

ク サーバ等のシステム環境を構築する際は、不正プログラムへの対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施）を確実に実施しなければならない。SaaS 型を利用する場合は、これらの対応が、クラウドサービス事業者側でされているのか、サービスを利用する前に確認しなければならない。また、サービスを利用している状況下では、これらのセキュリティ対策が適切にされているのか定期的に確認しなければならない。

ケ インターネットに接続していないシステムにおいて、電磁的記録媒体を使用する場合、不正プログラムの感染を防止するために、市が管理している電磁的記録媒体以外を職員等に利用させてはならない。また、不正プログラムの感染又は侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

コ 不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、職員等に当該権限を付与してはならない。

（２）職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

ア 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 差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

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 インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルを LGWAN 接続系に取り込む場合は、無害化又は不正プログラム対策ソフトウェアでのチェックを行わなければならない。

カ 統括情報セキュリティ責任者補佐官が提供するウイルス情報を、常に確認しなければならない。

キ 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、端末のネットワークからの切断又は通信を行わない設定への変更を行わなければならない。

（３）専門家の支援体制

統括情報セキュリティ責任者補佐官は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

5 不正アクセス対策

(1) 統括情報セキュリティ責任者補佐官等の措置事項

統括情報セキュリティ責任者補佐官等は、不正アクセス対策として、必要に応じて以下の事項を措置しなければならない。

ア 使用されていないポートを閉鎖しなければならない。

イ 不要なサービスについて、機能を削除又は停止しなければならない。

ウ 不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括情報セキュリティ責任者補佐官又は情報システム管理者へ通報するようにしなければならない。

エ 重要なシステムの設定を行ったファイル等について、必要に応じて、当該ファイルの改ざんの有無を検査しなければならない。

オ 統括情報セキュリティ責任者補佐官は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡、適正な対応等を実施できる体制及び連絡網を構築しなければならない。

カ 情報セキュリティポリシーにおけるアクセス制御に関する事項が、クラウドサービスにおいて実現できるのか、又はクラウドサービス事業者の提供機能等により実現できるのか、利用前にクラウドサービス事業者を確認しなければならない。

キ クラウドサービスを利用する際に、委託事業者等に管理権限を与え、機密性3に分類される情報を取り扱う場合は、多要素認証を用いて認証させ、クラウドサービスにアクセスさせなければならない。

ク パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が、人的セキュリティのID及びパスワード等の管理並びに技術的セキュリティの認証情報の管理を満たすことを確認しなければならない。

(2) 攻撃への対処

CISO、統括情報セキュリティ責任者及び統括情報セキュリティ責任者補佐官は、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、総務省、都道府県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。

(3) 記録の保存

CISO、統括情報セキュリティ責任者及び統括情報セキュリティ責任者補佐官は、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。

(4) 内部からの攻撃

統括情報セキュリティ責任者補佐官等は、職員等及び委託事業者が使用している端末からの内部のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

(5) 職員等による不正アクセス

統括情報セキュリティ責任者補佐官等は、職員等による不正アクセスを発見した場合は、

当該職員等が所属する課所等の情報セキュリティ管理者に通知し、適正な処置を求めなければならない。

(6) サービス不能攻撃

統括情報セキュリティ責任者補佐官等は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

(7) 標的型攻撃

統括情報セキュリティ責任者補佐官等は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

6 セキュリティ情報の収集

(1) セキュリティホールに関する情報の収集及び共有並びにソフトウェアの更新等

ア 統括情報セキュリティ責任者補佐官等は、セキュリティホールに関する情報を収集し、必要に応じて、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

イ 統括情報セキュリティ責任者補佐官等は、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、本市の業務に対する影響や保有するデータへの影響について特定し、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者を確認しなければならない。

(2) 不正プログラム等のセキュリティ情報の収集及び周知

統括情報セキュリティ責任者補佐官は、不正プログラム等のセキュリティ情報を収集し、必要に応じて、対応方法について、職員等に周知しなければならない。

(3) 情報セキュリティに関する情報の収集及び共有

統括情報セキュリティ責任者補佐官等は、情報セキュリティに関する情報を収集し、必要に応じて、関係者間で共有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。

第7. 運用

1 情報システムの監視

ア 情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

イ 情報システム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。また、利用するクラウドサービスで使用する時刻の同期についても適切になされているのか確認しなければならない。

- ウ 情報システム管理者は、外部と常時接続するシステムを常時監視しなければならない。
- エ 情報システム管理者は、必要となるリソースの容量・能力が確保できるクラウドサービス事業者を選定しなければならない。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めなければならない。
- オ 情報システム管理者は、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討しなければならない。
- カ 情報システム管理者は、クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作の手順に関して確認しなければならない。
 - (ア) サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除
 - (イ) クラウドサービス利用の終了手順
 - (ウ) バックアップ及び復旧

2 情報セキ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及び情報セキュリティ管理者は、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、速やかに統括情報セキュリティ責任者補佐官に報告しなければならない。
- イ 統括情報セキュリティ責任者補佐官は、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 統括情報セキュリティ責任者補佐官は、発生した問題について、必要に応じて、CISO及び統括情報セキュリティ責任者に報告しなければならない。
- エ 統括情報セキュリティ責任者補佐官等は、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) 端末、電磁的記録媒体等の利用状況調査

統括情報セキュリティ責任者補佐官等は、不正アクセス、不正プログラム等の調査のために、職員等が使用している端末、電磁的記録媒体等のログ、電子メールの送受信記録及び内容等の利用状況を調査することができる。

(3) 職員等の報告義務

- ア 職員等は、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、直ちに統括情報セキュリティ責任者補佐官及び情報セキュリティ管理者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 CISO が判断した場合において、職員等は、緊急時対応計画に従って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

ア 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、緊急時対応計画を策定しなければならない。

イ CSIRT は、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。

ウ 情報システム管理者は、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担をあらかじめ明確に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

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 関係者の連絡先

イ 発生した事案に係る報告すべき事項

ウ 発生した事案への対応措置

エ 再発防止措置の策定

(3) ICT 部門における業務継続計画との整合性確保

CISO は、自然災害、大規模・広範囲にわたる疾病等に備えて ICT 部門における業務継続計画を策定し、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、緊急時対応計画の規定を見直さなければならない。

4 例外措置

(1) 例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用する又は遵守事項の実施しないことについて合理的な理由がある場合には、CISO 及び統括情報セキュリティ責任者補佐官の許可を得て、例外措置を講じることができる。

(2) 緊急時の例外措置

情報セキュリティ管理者及び情報システム管理者は、行政事務の遂行に緊急を要する場合で、例外措置を実施することが避けられないときは、事後速やかに CISO に報告しなければならない。

(3) 例外措置の申請書の管理

統括情報セキュリティ責任者補佐官は、例外措置の申請書及び審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

5 法令遵守

職員等は、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、次の法令のほか関係法令を遵守し、これに従わなければならない。

- ア 地方公務員法（昭和 25 年法律第 261 号）
- イ 著作権法（昭和 45 年法律第 48 号）
- ウ 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）
- エ 個人情報の保護に関する法律（平成 15 年法律第 57 号）
- オ 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）
- カ サイバーセキュリティ基本法（平成 26 年法律第 104 号）
- キ 下関市個人情報保護法施行条例（令和 4 年条例第 35 号）

6 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等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なる場合がある。

（2）違反時の対応

職員等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場合には、速やかに次の措置を講じなければならない。

- ア 統括情報セキュリティ責任者補佐官が違反を確認した場合は、統括情報セキュリティ責任者補佐官は当該職員等が所属する課所等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。
- イ 情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ責任者補佐官及び当該職員等が所属する課所等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。
- ウ 情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリティ責任者補佐官は、当該職員等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又は剥奪することができる。その後速やかに、統括情報セキュリティ責任者補佐官は、職員等の権利を停止又は剥奪した旨を CIS0 及び当該職員等が所属する課所等の情報セキュリティ管理者に通知しなければならない。

第 8. 業務委託と外部サービスの利用

1 業務委託

（1）委託事業者の選定基準

- ア 情報セキュリティ管理者は、委託事業者の選定にあたり、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 情報セキュリティ管理者は、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、委託事業者を選定しなければならない。

(2) 契約項目

重要な情報資産を取扱う業務を委託する場合には、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 委託事業者の責任者、委託内容、作業者の所属及び作業場所の特定
- ウ 提供されるサービスレベルの保証
- エ 委託事業者にアクセスを許可する情報の種類、範囲及びアクセス方法の明確化等、情報のライフサイクル全般での管理方法
- オ 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委託事業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 市による監査及び検査
- 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 損害賠償等の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

(3) 確認・措置等

情報セキュリティ管理者は、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、必要に応じて、契約に基づき措置を実施しなければならない。また、措置した内容を統括情報セキュリティ責任者補佐官に報告するとともに、その重要度に応じて統括情報セキュリティ責任者及びCISOに報告しなければならない。

2 外部サービスの利用（機密性2以上の情報を取り扱う場合）

(1) 外部サービスの利用に係る規程の整備

統括情報セキュリティ責任者は、以下を含む外部サービス（機密性2以上の情報を取り扱う場合）の利用に関する規定を整備しなければならない。

- ア 外部サービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下、「外部サービス利用判断基準」という。）
- イ 外部サービス提供者の選定基準
- ウ 外部サービスの利用申請の許可権限者と利用手続
- エ 外部サービスの利用状況の管理
- オ クラウドサービスの利用状況の管理

(2) 外部サービスの選定

- ア 情報システム管理者は、取り扱う情報の分類及び分類に応じた取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討しなければならない。
- イ 情報システム管理者は、外部サービスで取り扱う情報の分類及び分類に応じた取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定しなけ

ればならない。また、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めなければならない。

(ア) 外部サービスの利用を通じて本市が取り扱う情報の外部サービス提供者における目的外利用の禁止

(イ) 外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制

(ウ) 外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制

(エ) 外部サービス提供者の資本関係・役員等の情報、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供（国籍については、個々人に紐付かない形で該当する国名を提出すること。）並びに調達仕様書による施設の場所やリージョンの指定

(オ) 情報セキュリティインシデントへの対処方法

(カ) 情報セキュリティ対策その他の契約の履行状況の確認方法

(キ) 情報セキュリティ対策の履行が不十分な場合の対処方法

ウ 情報システム管理者は、前記イに関する情報の提供を求め、その内容を確認し、利用する外部サービス（クラウドサービス）が、情報セキュリティポリシーを満たしているか否かを評価しなければならない。

エ 情報システム管理者は、外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含めなければならない。

オ 情報システム管理者は、クラウドサービス事業者と情報セキュリティに関する役割及び責任の分担について確認しなければならない。

カ 情報システム管理者は、外部サービスの利用を通じて本市が取り扱う情報の分類等を勘案し、必要に応じて、以下の内容を外部サービス提供者の選定条件に含めなければならない。

また、クラウドサービスの利用前に合意した事項があれば、その内容についてサービス合意書（SLA）に定め、クラウドサービス事業者のサービス利用規約等が変更できない場合は、機密性・完全性・可用性・安全性・個人情報等の扱いに関するクラウドサービス事業者の定める条件に鑑み、その規約内容が本市によって受容可能か判断しなければならない。

(ア) 情報セキュリティ監査の受入れ

(イ) サービスレベルの保証

キ 情報システム管理者は、外部サービスの利用を通じて本市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて、本市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めなければならない。

ク 情報システム管理者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるととも

に、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し、本市の承認を受けるよう、外部サービス提供者の選定条件に含めなければならない。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断しなければならない。

ケ 情報システム管理者は、外部サービスの特性を考慮した上で、必要に応じて、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めなければならない。

コ 情報システム管理者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス提供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なければならない。

(3) 外部サービスの利用承認

ア 情報システム管理者は、外部サービスの契約前に、利用申請の許可権限者へ外部サービスの利用申請を行わなければならない。

イ 利用申請の許可権限者は、情報セキュリティ管理者による外部サービスの利用申請を審査し、利用の可否を決定し、通知する。

ウ 利用申請の許可権限者は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録する。

(4) 外部サービスの利用に係る調達・契約

ア 情報システム管理者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めなければならない。

イ 情報システム管理者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めなければならない。

(5) 外部サービスを利用した情報システムの導入・構築時の対策

ア 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、以下を含む外部サービスを利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。

(ア) 不正なアクセスを防止するためのアクセス制御

(イ) 取り扱う情報の機密性保護のための暗号化

(ウ) 開発時におけるセキュリティ対策

(エ) 設計・設定時の誤りの防止

(オ) クラウドサービスにおけるユーティリティプログラムに対するセキュリティ対策

イ 情報システム管理者は、前記アにおいて定める規定に対し、構築時に実施状況を確認しなければならない。

(6) 外部サービスを利用した情報システムの運用・保守時の対策

ア 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスを利用して情報システムを運用する際のセキュリティ対策を規定しなければならない。

- (ア) 外部サービス利用方針の規定
- (イ) 外部サービス利用に必要な教育
- (ウ) 取り扱う資産の管理
- (エ) 不正アクセスを防止するためのアクセス制御
- (オ) 取り扱う情報の機密性保護のための暗号化
- (カ) 外部サービス内の通信の制御
- (キ) 設計・設定時の誤りの防止
- (ク) 外部サービスを利用した情報システムの事業継続
- (ケ) 設計・設定変更時の情報や変更履歴の管理

イ 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備しなければならない。

ウ 情報システム管理者は、前記アにおいて定める規定に対し、運用・保守時に実施状況を定期的に確認しなければならない。

(7) 外部サービスを利用した情報システムの更改・廃棄時の対策

ア 統括情報セキュリティ責任者は、利用する外部サービスの特性や責任分界点に係る考え方を踏まえ、あらかじめ以下を含む外部サービスの利用を終了する際のセキュリティ対策を規定しなければならない。

- (ア) 外部サービスの利用終了時における対策
- (イ) 外部サービスで取り扱った情報の廃棄
- (ウ) 外部サービスの利用のために作成したアカウントの廃棄

イ 情報システム管理者は、前記アにおいて定める規定に対し、外部サービスの利用終了時に実施状況を確認しなければならない。

3 外部サービスの利用（機密性2以上の情報を取り扱わない場合）

(1) 外部サービスの利用に係る規定の整備

統括情報セキュリティ責任者は、以下を含む外部サービス（機密性2以上の情報を取り扱わない場合）の利用に関する規定を整備しなければならない。

- ア 外部サービスを利用可能な業務の範囲
- イ 外部サービスの利用申請の許可権限者と利用手続
- ウ 外部サービスの利用状況の管理
- エ 外部サービスの利用の運用手順

(2) 外部サービスの利用における対策の実施

ア 情報システム管理者は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で機密性2以上の情報を取り扱わない

場合の外部サービスの利用を申請し、当該外部サービスの利用において適正な措置を講じた上で利用しなければならない。

イ 利用申請の許可権限者は、情報システム管理者による外部サービスの利用申請を審査し、利用の可否を決定し、承認した外部サービスを記録しなければならない。

4 ソーシャルメディアサービスの利用

(1) 情報セキュリティ管理者は、本市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

ア 本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理ウェブサイト当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

イ パスワードや認証のためのコード等の認証情報及びこれを記録した媒体(ICカード等)等を適正に管理するなどの方法で、不正アクセス対策を実施すること。

(2) 職員等は、機密性2以上の情報をソーシャルメディアサービスで発信してはならない。

(3) 情報セキュリティ管理者は、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なければならない。

(4) アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。

第9. 評価等

1 監査

(1) 実施方法

CISOは、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における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、監査を行わせなければならない。

(2) 監査を行う者の要件

ア 情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に、監査を実施させなければならない。

イ 監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

(3) 監査実施計画の策定及び実施への協力

ア 情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を策定し、CISOの承認を得なければならない。

イ 被監査部門は、監査の実施に協力しなければならない。

(4) 委託事業者に対する監査

ア 事業者業務委託を行っている場合、情報セキュリティ監査統括責任者は委託事業者

(再委託事業者を含む。)に対して、情報セキュリティポリシーの遵守について監査を定期的に、又は必要に応じて、行わなければならない。

イ 情報システム管理者は、クラウドサービスを利用している場合は、クラウドサービス事業者が自ら定める情報セキュリティポリシーの遵守について、必要に応じて、監査を行わなければならない。クラウドサービス事業者はその証拠(文書等)の提示を求める場合は、第三者の監査人が発行する証明書や監査報告書等をこの証拠とすることができ

(5) 報告

情報セキュリティ監査統括責任者は、監査結果を CIS0 に報告しなければならない。

(6) 保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠及び監査報告書の作成のための監査調書を、紛失等が発生しないように適正に保管しなければならない。

(7) 監査結果への対応

CIS0 は、監査結果を踏まえ、被監査部門に対し、指摘事項への対処を指示しなければならない。また、指摘事項を被監査部門以外に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。なお、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。

(8) 情報セキュリティポリシー及び関係規程等の見直し等への活用

CIS0 は、監査結果を情報セキュリティポリシー、関係規定等及びその他情報セキュリティ対策の見直しに活用しなければならない。

2 自己点検

(1) 実施方法

ア 情報システム管理者は、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。

イ 情報セキュリティ責任者は、情報セキュリティ管理者と連携し、所管する部局における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。

(2) 報告

統括情報セキュリティ責任者補佐官、情報システム管理者及び情報セキュリティ責任者は、自己点検結果及び自己点検結果に基づく改善策を取りまとめ、CIS0 に報告しなければならない。

(3) 自己点検結果の活用

ア 職員等は、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。

イ CIS0 は、点検結果を情報セキュリティポリシー、関係規程その他情報セキュリティ対

策の見直しに活用しなければならない。

3 情報セキュリティポリシー及び関係規程等の見直し

CISO は、情報セキュリティ監査及び自己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、関係規程等について定期的に、又は重大な変化が発生した場合に見直しを行い、必要があると認めた場合、改定を行うものとする。

附 則

(施行期日)

- 1 このセキュリティポリシーは、令和3年6月1日から施行する。

(経過措置)

- 2 このセキュリティポリシーの施行の日の前に改正前の下関行政情報セキュリティポリシーによりなされた、手続その他の行為は、このセキュリティポリシーによってなされたものとみなす。

附 則

このセキュリティポリシーは、令和5年2月1日から施行する。

附 則

このセキュリティポリシーは、令和5年4月1日から施行する。

附 則

(施行期日)

- 1 このセキュリティポリシーは、令和6年4月1日から施行する。

(経過措置)

- 2 このセキュリティポリシーの施行の日の前に改正前の下関行政情報セキュリティポリシーによりなされた、手続その他の行為は、このセキュリティポリシーによってなされたものとみなす。