

「生成AIサービス提供業務」に関する質疑応答集

1 ■実施要領 4 参加事業者の資格要件等

【質問】

2025年7月1日に社名変更を予定しているため事業者登録の変更を予定しているが、新社名での事業者登録が完了するまでは旧社名の書類での提出で問題ないでしょうか。

また、社名変更手続きに伴い法務局での法人登記簿謄本が閉鎖されるため、コピーでの提出でも良いでしょうか。

【回答】

本プロポーザルには旧社名で提出いただいて問題ありません。

また、法人登記簿謄本のコピーでも問題ありません。

2 ■提案書作成要領 5 提案者が（中略）～記載すること

【質問】

弊社は●●グループ内の地域営業会社の為、本業務は弊社を営業窓口グループ会社である●●を再委託先として実施する予定です。問題ございませんでしょうか。

【回答】

本業務は、生成AIサービスの「提供」という位置付けです。よって、再委託の手続きは不要ですが、サービス提供の体制を確認できる資料を提案書に盛り込んでください。

なお、秘密保持契約はサービス提供体制全体に適用されます。

3 ■実施要領 10プレゼンテーション・審査

【質問】

Cisco Webexはブラウザでの参加は可能でしょうか。
参加人数等に制約はございますでしょうか。
協業先の関係者も同席させていただくことは可能でしょうか。

【回答】

ブラウザでの参加も可能です。
参加人数は5名まで、Webexのミーティングルームに入室される際は5アカウントまでにしてください。
サービス提供体制に含まれる方は同席可能です。

4 ■仕様書 2業務内容

【質問】

提供する生成AIサービスは、既存SaaS型（例：ChatGPT、Microsoft Copilot等）の利用を想定していますか？それとも、オンプレ/独自環境での構築を想定されていますでしょうか。

【回答】

提供していただくサービス形式は、SaaS型（LGWAN-ASPサービス）を想定しております。

5 ■仕様書 2業務内容

【質問】

ヘルプデスク対応において「直接対応」とありますが、具体的に想定されるチャンネル（電話・メール・チャット等）に制限はありますか。
プロンプト評価・改善相談の対応範囲として、生成内容の品質確認やガバナンス対策（情報漏洩の回避など）も含まれると解釈してよいでしょうか。

【回答】

メール対応は必須要件になります。
メール対応に加えて、電話対応も可能な場合は評価します。
メール対応の代わりとして、チャットでの対応も可とします。ただし、チャット環境は受注事業者で提供してください。
またヘルプデスクの役割として、サービスの障害対応と、生成内容の精度向上やユーザの想定どおりの回答を生成させるために必要なサポートを想定しています。ガバナンス対策を提案に含んでいただいても構いません。

6 ■仕様書 2 業務内容

【質問】

提供を求めるプロンプトテンプレートの件数や、対象業務カテゴリ（例：文書作成、条例起案、FAQ作成など）に関する指定はありますか。

【回答】

指定はありませんが、次の内容が望ましいと考えます。

件数：20件以上

カテゴリ：会議録の要約や説明原稿の作成、RAGを使用する際に最適なプロンプト。また、税業務や福祉業務といった、各業務にそのまま使用可能なプロンプトの提供は評価します。

7 ■仕様書 3 職員研修

【質問】

RAG研修において、対象職員の技術レベルや想定される実装範囲（PoCレベルか実業務適用までか）を教えてください。

プロンプト研修は、特定業務部門（例：税務・福祉など）を想定した内容が求められますか？それとも汎用的なAIリテラシー研修でよいのでしょうか。

【回答】

実業務適用までサポート可能な事業者を評価します。

汎用的なAIリテラシー研修は必須とし、そこからレベルアップした内容であったり、各業務に合わせた内容を提供していただける場合は評価します。

8 ■仕様書 3 職員研修

【質問】

研修の実施回数について、ご希望はございますでしょうか。

【回答】

研修の実施回数について、指定はありません。

回数や形式、内容を総合的に評価します。

9 ■仕様書 4 その他

【質問】

情報資産の「廃棄」の対象には、生成AIサービス上に残るユーザ履歴・ログ等も含まれると解釈してよろしいでしょうか。

【回答】

御認識のとおりです。

10 ■仕様書 4 その他

【質問】

貴自治体の「セキュリティポリシー」や「契約規則」等、提案・見積に影響する制約条件は事前に閲覧可能でしょうか。

【回答】

本市のセキュリティポリシーは、この質疑応答集に添付しますので御確認ください。

契約規則は下記 URLから閲覧可能です。

西脇市例規集 西脇市契約規則

https://en3-jg.d1-law.com/nishiwaki/d1w_reiki/H417902100048/H417902100048.html

11 ■サービス・機能要件一覧 No.3

【質問】

ユーザ数 600・同時利用30の設定については、初期導入時点でのアカウント発行数ですか？それともライセンス最大枠の条件を指すものでしょうか。

【回答】

初期導入時点で最低限必要な数として「ユーザ登録数 600以上、同時利用ユーザ数30以上」を定めております。

12 ■サービス・機能要件一覧 No.4

【質問】

「Webサービス」と明記されていますが、シングルサインオン（SSO）連携やID基盤（例：Azure AD）との連携要件はありますか。

【回答】

連携要件はありません。

13 ■サービス・機能要件一覧 No.8

【質問】

要件として「GPT-4 Omni等と同等以上の性能」とありますが、これは精度ベンチマーク等の比較資料提出を求めるものでしょうか？それともベンダーの仕様上の記載・説明で足りますか。

【回答】

サービスに、GPT-4 Omni、Gemini 2.0 Flash、Claude 3.5 Sonnetを含まず、独自開発モデルでの提供となる場合は、評価のために必要なベンチマーク結果を提出してください。

なお、ベンチマークの種類は問いませんが、日本語での文章生成能力を評価するベンチマーク結果を提出してください。

14 ■サービス・機能要件一覧 No.9

【質問】

文字数のカウント方式（例：プロンプト+応答を含む等）は具体的にありますか。

【回答】

入力文（プロンプト）と生成文を双方を含みます。

一般的な生成AIサービスでは、トークン数という形で表現されていますが、日本語と英語でカウント数が異なる場合があるという認識です。

そのため、「日本語で、一月当たり500万文字使用可能」なサービスを提供してください。

15 ■サービス・機能要件一覧 No.11

【質問】

LGWAN-ASPサービスリストに掲載されていること。との記載がありますが、LGWAN経由で生成AIを利用する前提で認識合っていますでしょうか。

【回答】

御認識のとおりです。

16 ■サービス・機能要件一覧 No.11

【質問】

「LGWAN-ASPサービスリストに掲載されていること」とありますが、本件提案時点で掲載予定または申請中の場合は対象外となりますでしょうか。

また、掲載済と判断するために、登録番号やサービス名称などの証明資料の提出が必要ですか。

【回答】

登録番号（ASPコード）を提示してください。LGWAN-ASPポータルサイトに掲載されていることが確認出来れば、証明資料の提出は不要です。

リストの更新タイミングによって、LGWAN-ASPポータルサイト上で確認できない場合は、別途証明資料を提出してください。

なお、サービス利用開始日である令和7年9月1日までにLGWAN-ASPサービスとして登録されることが決定していない場合、No.11の要件は満たさないとします。

17 ■サービス・機能要件一覧 No.14

【質問】

ログ出力において「送信内容」や「出力文」まで記録する必要がありますが、これらの保存期間・形式（例：CSV, API連携等）についての指定はありますか。

【回答】

形式は問いませんが、一般的なテキストエディタで閲覧できる形式が望ましいと考えます。

API連携も認めますが、情報担当職員に対しログ閲覧が可能な状態までサポートしてください。

保存期間は、1ヵ月前までの情報が確認できることを必須とします。

18 ■サービス・機能要件一覧 No.15、17

【質問】

アップロードされたファイルやログのバックアップ・保持ポリシーについて、市側で指定や制限がある場合は明示いただけますでしょうか。

【回答】

「サービス・機能要件一覧」記載の内容以外の指定はありません。

19 ■サービス・機能要件一覧 No.16

【質問】

RAG対象ファイルについて、PDF内の画像化された文字等はOCR処理が必要になりますが、この処理は要件に含まれますでしょうか。

【回答】

画像化されたPDFのOCR処理は必須要件ではありません。
対応可能であれば評価します。

20 ■サービス・機能要件一覧 No.18

■評価基準

RAG機能関連

【質問】

サービス・機能要件一覧ではRAGの必須要件で「ファイルの総アップロード容量は10GB以上であること。」となっていますが、評価基準では「西脇市のユーザ全体でアップロードできるファイル容量が20GB以上あるか」になっています。必須は10GB以上で20GB以上だと評価点が高くなるという理解でよろしかったでしょうか？

【回答】

10GBは必須となる機能要件です。
20GB以上を提案していただいた際に、その容量に対して評価します。

21 ■サービス・機能要件一覧 No.18

【質問】

RAG対応について、「アップロードデータ10GB以上」との要件がありますが、これは全体共有ストレージでしょうか？それともユーザ個別の容量制限に関するものですか。

【回答】

市全体で10GB以上のストレージ容量が必須要件になります。

以上

西脇市情報セキュリティポリシー

令和4年10月

西脇市

情報セキュリティ基本方針

近年、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。

本市は、市民の個人情報や行政運営上重要な情報など多数取り扱っている。また、電子自治体の構築が進み、多くの業務が情報システムやネットワークに依存している。したがって、これらの情報資産を様々な脅威から防御することは、市民の権利、利益を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠である。

これらの状況を鑑み、本市における情報資産に対する安全対策を推進し、市民からの信頼を確保するため、以下に積極的に取り組むことを宣言する。

- (1) 情報セキュリティ対策に取り組むための全庁的な体制を確立する。
- (2) 情報セキュリティ対策の基準として情報セキュリティ対策基準を策定し、その実行のための手順等を盛り込んだ実施手順を策定する。
- (3) 本市の保有する情報資産を適切に管理する。
- (4) 情報セキュリティ対策の重要性を認識させ、当該対策を適切に実施するために、職員等に対して必要な教育を実施する。
- (5) 情報セキュリティインシデントが発生した場合又はその予兆があった場合に速やかに対応するため、緊急時対応計画を定める。
- (6) 情報セキュリティ対策の実施状況の監査及び自己点検等を通して、定期的に対策の見直しを実施する。
- (7) 全ての職員等は、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基本方針、情報セキュリティ対策基準及び情報セキュリティ実施手順を遵守する。

令和4年10月

最高情報セキュリティ責任者

西脇市情報セキュリティ対策基準

－目次－

1	目的	1
2	定義	1
3	対象とする脅威	2
4	適用範囲	2
	(1) 行政機関の範囲	2
	(2) 情報資産の範囲	2
5	職員等の遵守義務	3
6	組織体制	3
	(1) 最高情報セキュリティ責任者	3
	(2) 統括情報セキュリティ責任者	3
	(3) 情報セキュリティ責任者	4
	(4) 情報セキュリティ管理者	4
	(5) 情報管理者	4
	(6) 情報システム担当者	5
	(7) 情報化推進委員会	5
	(8) 兼務の禁止	5
	(9) 情報セキュリティに関する統一的な窓口の設置	5
7	情報資産の分類と管理	5
	(1) 情報資産の分類	5
	(2) 情報資産の管理	7
8	情報システム全体の強靱性の向上	9
	(1) マイナンバー利用事務系	9
	(2) LGWAN接続系	9
	(3) インターネット接続系	10
9	物理的セキュリティ	10
	(1) サーバ等の管理	10
	(2) 管理区域（情報システム室等）の管理	11
	(3) 通信回線及び通信回線装置の管理	12
	(4) 職員等のパソコン等の管理	13
10	人的セキュリティ	13
	(1) 職員等の遵守事項	13
	(2) 研修及び訓練	15
	(3) 情報セキュリティインシデントの報告	16
	(4) ID及びパスワード等の管理	17
11	技術的セキュリティ	18
	(1) コンピュータ及びネットワークの管理	18

(2)	アクセス制御.....	23
(3)	システム開発、導入、保守等.....	26
(4)	不正プログラム対策.....	28
(5)	不正アクセス対策.....	30
(6)	セキュリティ情報の収集.....	31
12	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.....	32
(3)	侵害時の対応等.....	33
(4)	例外措置.....	33
(5)	法令遵守.....	33
(6)	懲戒処分等.....	34
13	業務委託と外部サービスの用.....	34
(1)	業務委託.....	34
(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).....	35
(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
14	情報セキュリティ監査及び自己点検の実施.....	39
(1)	監査.....	39
(2)	自己点検.....	40
15	情報セキュリティポリシー及び関係規程等の見直し.....	41

西脇市情報セキュリティ対策基準

1 目的

本市の情報システムが取り扱う情報には、市民の個人情報や行政運営上重要な情報が多数含まれており、情報資産を人的脅威や災害、事故等様々な脅威から防御することは、市民の財産、プライバシー等を守るためにも、また、継続的かつ安全・安定的な行政サービスの実施を確保するためにも必要不可欠である。

このため、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ことを目的とした情報セキュリティ対策を実施するために、適用範囲における共通の基準として具体的な遵守事項及び判断基準を定める。

2 定義

(1) 情報システム

コンピュータや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。

(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) 機密性

情報資産にアクセスすることを認められた者だけが、情報資産にアクセスできる状態を確保することをいう。

(5) 完全性

情報資産が破壊、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。

(6) 可用性

情報資産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。

(7) 情報セキュリティポリシー

情報セキュリティ基本方針及び情報セキュリティ対策基準をいう。

(8) 情報セキュリティインシデント

情報セキュリティを脅かす事件や事故、情報システム上の欠陥をいう。

(9) 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。

(10) LGWAN接続系

人事給与、財務会計及び文書管理等 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。

(11) 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。

(12) 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。

(13) 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。

3 対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、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・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

本対策基準が適用される行政機関は、内部部局、行政委員会、議会事務局及び地方公営企業とする。

(2) 情報資産の範囲

本対策基準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、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（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

5 職員等の遵守義務

職員及び会計年度任用職員（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を遵守しなければならない。

6 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。）

ア 副市長をCISOとする。

イ CISOは、本市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。

(2) 統括情報セキュリティ責任者

ア 情報管理担当部長をCISO直属の統括情報セキュリティ責任者とする。

イ 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。

ウ 統括情報セキュリティ責任者は、本市の全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。

エ 統括情報セキュリティ責任者は、本市の全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。

オ 統括情報セキュリティ責任者は、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。

カ 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。

- キ 統括情報セキュリティ責任者は、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。
- ク 統括情報セキュリティ責任者は、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、情報セキュリティ責任者、情報セキュリティ管理者、情報管理者、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。
- ケ 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。
- コ 統括情報セキュリティ責任者は、情報セキュリティ関係規定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にその内容を報告しなければならない。
- (3) 情報セキュリティ責任者
- ア 内部部局の長、行政委員会事務局の長、議会事務局の長及び地方公営企業の局長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、当該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、その所管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、その所管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。
- (4) 情報セキュリティ管理者
- ア 内部部局の課室長、内部部局の出張所等出先機関の長、行政委員会事務局の長、議会事務局の主幹及び地方公営企業の課室長を、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、その所管する課室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、その所掌する課室等において、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、情報セキュリティ責任者、統括情報セキュリティ責任者及びCISOへ速やかに報告を行い、指示を仰がなければならない。
- (5) 情報管理者
- ア 各情報システムの担当課室長等を当該情報システムに関する情報管理者とする。

- イ 情報管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。
- ウ 情報管理者は、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。

(6) 情報システム担当者

情報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。

(7) 情報化推進委員会

本市の情報セキュリティ対策を統一的に実施するため、情報化推進委員会において、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。

(8) 兼務の禁止

ア 情報セキュリティ対策の実施において、止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 監査を受ける者とその監査を実施する者は、止むを得ない場合を除き、同じ者が兼務してはならない。

(9) 情報セキュリティに関する統一的な窓口の設置

ア 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所管部局等から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すること。

イ 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すること。

ウ 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、兵庫県等へ報告すること。

エ 情報セキュリティインシデントを認知した場合には、その重要度や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。

オ 情報セキュリティに関して、関係機関や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うこと。

7 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、必要に応じ取扱制限を行うものとする。

ア 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、秘密文書に相当する機密性を要する情報資産	<ul style="list-style-type: none"> ○個人所有の端末での作業の原則禁止（機密性3のみ） ○必要以上の複製及び配付禁止 ○保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持込み禁止
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ない情報資産	<ul style="list-style-type: none"> ○情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ○復元不可能処理を施して廃棄 ○信頼のできるネットワーク回線の選択 ○庁外で情報処理を行う際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又は機密性3の情報資産以外の情報資産	

イ 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、市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、電子署名付与 ○庁外で情報処理を行う際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	

ウ 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、市民の権利が侵害され、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	○バックアップ、指定する時間以内の復旧 ○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	

(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上記7-(1)の分類に基づき管理しなければならない。

イ 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、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。

ウ 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) 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に判断を仰がなければならない。

エ 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、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。

オ 情報資産の保管

- (ア) 情報セキュリティ管理者又は情報管理者は、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地域に保管しなければならない。
- (エ) 情報セキュリティ管理者又は情報管理者は、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、耐火、耐熱、耐水及び耐湿を講じた施設可能な場所に保管しなければならない。

カ 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、必要に応じパスワード等による暗号化を行わなければならない。

キ 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に許可を得なければならない。

ク 情報資産の提供及び公表

- (ア) 機密性2以上の情報資産を外部に提供する者は、必要に応じパスワード等による暗号化の設定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に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、市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。

ケ 情報資産の廃棄

- (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について、その情報の機密性に応じ、情報の初期化等、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。

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。

8 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

ア 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送信を可能とする。

イ 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。

(2) LGWAN接続系

ア 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環境を分離した上で、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

(3) インターネット接続系

ア 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講じなければならない。

イ 兵庫県及び本市のインターネットとの接続を集約する自治体情報セキュリティクラウドに参加するとともに、関係省庁や兵庫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。

9 物理的セキュリティ

(1) サーバ等の管理

ア 機器の取付け

情報管理者は、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。

イ サーバの冗長化

(ア) 情報管理者は、重要情報を格納しているサーバ、セキュリティサーバ、市民サービスに関するサーバ及びその他の基幹サーバを冗長化し、同一データを保持するように努めなければならない。

(イ) 情報管理者は、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するなどして、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。

ウ 機器の電源

(ア) 情報管理者は、統括情報セキュリティ責任者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又は UPSを備え付けなければならない。

(イ) 情報管理者は、統括情報セキュリティ責任者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。

エ 通信ケーブル等の配線

(ア) 統括情報セキュリティ責任者及び情報管理者は、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及び情報管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、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) 統括情報セキュリティ責任者及び情報管理者は、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) 統括情報セキュリティ責任者及び情報管理者は、自ら又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。

オ 機器の定期保守及び修理

- (ア) 情報管理者は、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) 情報管理者は、電磁的記録媒体を内蔵する機器を事業者に故障を修理させる場合、機器内部の記憶装置から全ての情報を消去の上で行わせなければならない。内容を消去できない場合、情報管理者は、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などを行わなければならない。

カ 庁外への機器の設置

統括情報セキュリティ責任者及び情報管理者は、庁外にサーバ等の機器を設置する場合、CIS0の承認を得なければならない。また、定期的に当該機器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。

キ 機器の廃棄等

情報管理者は、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) 管理区域（情報システム室等）の管理

ア 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の部屋や電磁的記録媒体の保管庫をいう。
- (イ) 統括情報セキュリティ責任者及び情報管理者は、管理区域を地階又は1階に設けてはならない。また、外部からの侵入が容易にできないような措置を講じなければならない。

- (ウ) 統括情報セキュリティ責任者及び情報管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能及び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) 統括情報セキュリティ責任者及び情報管理者は、管理区域内の機器等に、転倒及び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) 統括情報セキュリティ責任者及び情報管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

イ 管理区域の入退室管理等

- (ア) 情報管理者は、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や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、必要に応じて立入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) 情報管理者は、機密性2以上の情報資産を取り扱うシステムを設置している管理区域について、当該情報システムに関連しない、または個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を許可なく持ち込ませてはならない。

ウ 機器等の搬入出

- (ア) 情報管理者は、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、あらかじめ職員又は委託業者に確認を行わせなければならない。
- (イ) 情報管理者は、管理区域内の機器等の搬入出について、職員を立ち合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は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、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。
- イ 統括情報セキュリティ責任者は、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は、行政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、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、伝送途上に情報の破壊、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は、可用性 2 の情報資産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、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) 職員等のパソコン等の管理
- ア 情報管理者は、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 情報管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。
 - ウ 情報管理者は、取り扱う情報資産の重要度に応じてパスワード以外に指紋認証等の二要素認証を併用しなければならない。

10 人的セキュリティ

(1) 職員等の遵守事項

ア 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情報セキュリティ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) 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
 - a CIS0は、機密性2以上、可用性2、完全性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。
 - b 職員等は、本市のモバイル端末、電磁的記録媒体、情報資産及びソフトウェア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。
 - c 職員等は、外部で情報処理業務を行う場合には、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) 個人所有のパソコン、モバイル端末及び電磁的記録媒体等の業務利用
 - a 職員等は、個人所有のパソコン、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、業務上必要な場合は、情報セキュリティ管理者の許可を得て利用することができる。
 - b 職員等は、個人所有のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、情報セキュリティ管理者の許可を得た上で、外部で情報処理業務を行う際に安全管理措置に関する規定を遵守しなければならない。
 - (オ) 持ち出し及び持込みの記録

情報セキュリティ管理者は、パソコン、モバイル端末及び電磁的記録媒体等の持ち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) 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

職員等は、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、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、文書等が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。

イ 会計年度任用職員への対応

(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、会計年度任用職員が守るべき内容を理解させ、また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、会計年度任用職員の採用の際に、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、会計年度任用職員にパソコンやモバイル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及び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。

ウ 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情報セキュリティ実施手順を閲覧できるように掲示しなければならない。

エ 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・保守等を委託事業者が発注する場合、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の遵守及びその機密事項を説明しなければならない。

(2) 研修及び訓練

ア 情報セキュリティに関する研修及び訓練

CIS0は、定期的に情報セキュリティに関する研修及び訓練を実施しなければならない。

イ 研修計画の策定及び実施

(ア) CIS0は、全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とその実施体制の構築を定期的に行い、情報化推進委員会の承認を得なければならない。

(イ) 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実施しなければならない。

(ウ) CIS0は、毎年度1回、情報化推進委員会に対して、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しなければならない。

ウ 緊急時対応訓練

CIS0は、緊急時対応を想定した訓練を定期的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、また、効果的に実施できるようにしなければならない。

エ 研修及び訓練への参加

全ての職員等は、定められた研修及び訓練に参加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

ア 庁内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に報告しなければならない。

(イ) 報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報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。

(ウ) 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、CIS0及び情報セキュリティ責任者に報告しなければならない。

イ 市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、本市が管理するネットワーク及び情報システム等の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、市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) 報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報管理者に報告しなければならない。

(ウ) 情報セキュリティ管理者は、必要に応じて当該情報セキュリティインシデントについて、CIS0及び情報セキュリティ責任者に報告しなければならない。

ウ 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) 統括情報セキュリティ責任者は、情報セキュリティインシデントを引き起こした部門の情報セキュリティ管理者、情報管理者、情報セキュリティに関する統一的な窓口と連携し、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、CIS0に報告しなければならない。

(イ) CIS0は、統括情報セキュリティ責任者から、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

ア 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。
 - a 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。
 - b 業務上必要のないときは、ICカード等をカードリーダー若しくはパソコン等の端末のスロット等から抜いておかななければならない。
 - c ICカード等を紛失した場合には、速やかに統括情報セキュリティ責任者及び情報管理者に通報し、指示に従わなければならない。
- (イ) 統括情報セキュリティ責任者及び情報管理者は、ICカード等の紛失等の通報があり次第、当該ICカード等を使用したアクセス等を速やかに停止しなければならない。
- (ウ) 統括情報セキュリティ責任者及び情報管理者は、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、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

イ 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の利用者以外に利用させてはならない。

ウ 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、情報セキュリティ管理者に速やかに報告し、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取り扱う職員等は、できるだけ同一のパスワードをシステム間で用いないように努めなければならない。
- (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パソコン等の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（ただし共有IDに対するパスワードは除く）。

11 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

ア 文書サーバの設定等

- (ア) 情報管理者は、職員等が使用できる文書サーバ（Nドライブ）の容量を設定し、職員等に周知しなければならない。
- (イ) 情報管理者は、文書サーバを課室等の単位で構成し、職員等が他課室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) 情報管理者は、個人情報や人事記録等、特定の職員等しか取り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、同一課室等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

イ バックアップの実施

統括情報セキュリティ責任者及び情報管理者は、文書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、必要に応じて定期的にバックアップを実施しなければならない。

ウ 他団体との情報システムに関する情報等の交換

情報管理者は、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。

エ システム管理記録及び作業の確認

- (ア) 情報管理者は、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) 統括情報セキュリティ責任者及び情報管理者は、所管するシステムにおいて、システム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) 情報システム担当者及び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、統括情報セキュリティ責任者及び情報管理者に、作業日程及び作業内容等について届出なければならない。また、作業は2人以上で実施し、互いにその作業を確認しなければならない。

オ 情報システム仕様書等の管理

統括情報セキュリティ責任者及び情報管理者は、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。

カ ログの取得等

(ア) 統括情報セキュリティ責任者及び情報管理者は、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) 統括情報セキュリティ責任者及び情報管理者は、ログとして取得する項目、保存期間、取扱方法及び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) 統括情報セキュリティ責任者及び情報管理者は、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。

キ 障害記録

統括情報セキュリティ責任者及び情報管理者は、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。

ク ネットワークの接続制御、経路制御等

(ア) 統括情報セキュリティ責任者は、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) 統括情報セキュリティ責任者は、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。

ケ 外部の者が利用できるシステムの分離等

情報管理者は、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。

コ 外部ネットワークとの接続制限等

- (ア) 情報管理者は、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、CISO及び統括情報セキュリティ責任者の許可を得なければならない。
- (イ) 情報管理者は、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、庁内の全てのネットワーク、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、改ざん又は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、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) 統括情報セキュリティ責任者及び情報管理者は、ウェブサーバ等をインターネットに公開する場合、庁内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。

サ 複合機のセキュリティ管理

- (ア) 統括情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能、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) 統括情報セキュリティ責任者は、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) 統括情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を消去し、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。

シ 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。

ス 無線 LAN及びネットワークの盗聴対策

- (ア) 統括情報セキュリティ責任者は、無線 LANの利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。
- (イ) 統括情報セキュリティ責任者は、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。

セ 電子メールのセキュリティ管理

- (ア) 統括情報セキュリティ責任者は、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) 統括情報セキュリティ責任者は、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) 統括情報セキュリティ責任者は、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) 統括情報セキュリティ責任者は、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) 統括情報セキュリティ責任者は、システム開発や運用、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。

ソ 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。
- (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。

タ 電子署名、暗号化

- (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、CIS0が定めた電子署名、パスワード等による暗

号化等、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。

チ 無許可ソフトウェアの導入等の禁止

(ア) 職員等は、パソコン、タブレット及び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) 職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者及び情報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、導入する際は、情報セキュリティ管理者又は情報管理者は、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。

ツ 機器構成変更の制限及びネットワーク接続の制限

(ア) 職員等は、パソコン、タブレット及び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) 職員等は、業務上、パソコン、タブレット及び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、統括情報セキュリティ責任者及び情報管理者の許可を得なければならない。

(ウ) 職員等は、統括情報セキュリティ責任者の許可なくパソコン、タブレット及びモバイル端末をネットワークに接続してはならない。

テ 業務外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) 情報管理者は、支給した端末について、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することが望ましい。

ト 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は、職員等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、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。

- ナ Web会議サービスの利用時の対策
- (ア) 統括情報セキュリティ責任者は、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、本市の定める利用手順に従い、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すること。
 - (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ずること。
 - (エ) 職員等は、外部からWeb会議に招待される場合は、本市の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。
- ニ ソーシャルメディアサービスの利用
- (ア) 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。
 - a 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Webサイトに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。
 - b 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(ハードディスク、USBメモリ、紙等)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。
 - (イ) 機密性2以上の情報はソーシャルメディアサービスで発信してはならない。
 - (ウ) 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。
 - (エ) 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。
- (2) アクセス制御
- ア アクセス制御
- (ア) アクセス制御等
統括情報セキュリティ責任者又は情報管理者は、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

- a 統括情報セキュリティ責任者及び情報管理者は、利用者の登録、変更、消去等の情報管理、職員等の異動、出向、退職に伴う利用者のIDの取扱い等の方法を定めなければならない。
 - b 職員等は、業務上必要がなくなった場合は、利用者登録を消去するよう、統括情報セキュリティ責任者又は情報管理者に通知しなければならない。
 - c 統括情報セキュリティ責任者及び情報管理者は、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
- a 統括情報セキュリティ責任者及び情報管理者は、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の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。
 - b 統括情報セキュリティ責任者及び情報管理者の特権を代行する者は、統括情報セキュリティ責任者及び情報管理者が指名し、CISOが認めた者でなければならない。
 - c CISOは、代行者を認めた場合、速やかに統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者及び情報管理者に通知しなければならない。
 - d 統括情報セキュリティ責任者及び情報管理者は、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。
 - e 統括情報セキュリティ責任者及び情報管理者は、特権を付与されたID及びパスワードについて、職員等のパソコン、タブレット及びモバイル端末のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。
 - f 統括情報セキュリティ責任者及び情報管理者は、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。
- イ 職員等による外部からのアクセス等の制限
- (ア) 職員等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及び当該情報システムを管理する情報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及び情報管理者は、外部からのアクセスに利用するモバイル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、持ち込み、又は外部から持ち帰ったモバイル端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。
- (キ) 統括情報セキュリティ責任者は、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、止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及び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。

ウ ログイン時の表示等

情報管理者は、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及びログイン・ログアウト時刻の表示等により、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。

エ 認証情報の管理

- (ア) 統括情報セキュリティ責任者又は情報管理者は、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) 統括情報セキュリティ責任者又は情報管理者は、職員等に対してパスワードを発行する場合は、できるだけ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

させるよう努めなければならない。

- (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。

オ 特権による接続時間の制限

情報管理者は、特権ユーザ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

ア 情報システムの調達

- (ア) 統括情報セキュリティ責任者及び情報管理者は、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) 統括情報セキュリティ責任者及び情報管理者は、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。

イ 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及び作業者のIDの管理

a 情報管理者は、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、開発用のIDを削除しなければならない。

b 情報管理者は、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

a 情報管理者は、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。

b 情報管理者は、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。

ウ 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

a 情報管理者は、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。

- b 情報管理者は、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。
 - c 情報管理者は、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し、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。
 - d 情報管理者は、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
- a 情報管理者は、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。
 - b 情報管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。
 - c 情報管理者は、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。
 - d 情報管理者は、開発したシステムについて受入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。
- エ システム開発・保守に関連する資料等の整備・保管
- (ア) 情報管理者は、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。
- オ 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、妥当性のチェック機能及び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) 情報管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック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

システムを設計しなければならない。

カ 情報システムの変更管理

情報管理者は、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。

キ 開発・保守用のソフトウェアの更新等

情報管理者は、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。

ク システム更新又は統合時の検証等

情報管理者は、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

ア 統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、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コンピュータウイルス等の不正プログラムのチェックを行い、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コンピュータウイルス等の不正プログラムのチェックを行い、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) 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。

(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。

(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。

イ 情報管理者の措置事項

情報管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

- (ア) 情報管理者は、その所掌する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システムに常駐させなければならない。
- (イ) 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。
- (ウ) 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。
- (エ) 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う場合、コンピュータウイルス等の感染を防止するために、本市が管理している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、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。
- (オ) 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、情報管理者が許可した職員を除く職員等に当該権限を付与してはならない。

ウ 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) 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) 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) 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。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しなければならない。
- (カ) 統括情報セキュリティ責任者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) 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、次の対応を行わなければならない。
 - a パソコン等の端末の場合
LANケーブルの即時取り外しを行わなければならない。
 - b モバイル端末の場合
直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。
 - エ 専門家の支援体制
統括情報セキュリティ責任者は、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
- ア 統括情報セキュリティ責任者の措置事項
統括情報セキュリティ責任者は、不正アクセス対策として、次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及び情報管理者へ通報するよう、設定しなければならない。
 - (エ) 統括情報セキュリティ責任者は、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、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。
 - イ 攻撃への対処
CIS0及び統括情報セキュリティ責任者は、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、兵庫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。
 - ウ 記録の保存
CIS0及び統括情報セキュリティ責任者は、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。
 - エ 内部からの攻撃
統括情報セキュリティ責任者及び情報管理者は、職員等及び委託事業者が使用しているパソコン等の端末からの庁内のサー

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。

オ 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及び情報管理者は、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室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。

カ サービス不能攻撃

統括情報セキュリティ責任者及び情報管理者は、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。

キ 標的型攻撃

統括情報セキュリティ責任者及び情報管理者は、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

ア セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

統括情報セキュリティ責任者及び情報管理者は、セキュリティホールに関する情報を収集し、必要に応じ、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 不正プログラム等のセキュリティ情報の収集・周知

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

ウ 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及び情報管理者は、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。

12 運用

(1) 情報システムの監視

ア 統括情報セキュリティ責任者及び情報管理者は、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 統括情報セキュリティ責任者及び情報管理者は、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。

ウ 統括情報セキュリティ責任者及び情報管理者は、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。

(2) 情報セキュリティポリシーの遵守状況の確認

ア 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。

(イ) CISO及び統括情報セキュリティ責任者は、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及び情報管理者は、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。

イ 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、職員等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。

ウ 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ると統括情報セキュリティ責任者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

ア 緊急時対応計画の策定

CISO又は情報化推進委員会は、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。

イ 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、次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

ウ 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し、情報化推進委員会は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。

エ 緊急時対応計画の見直し

CISO又は情報化推進委員会は、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内容を見直さなければならない。

(4) 例外措置

ア 例外措置の許可

情報セキュリティ管理者及び情報管理者は、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し又は遵守事項を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の許可を得て、例外措置を講じることができる。

イ 緊急時の例外措置

情報セキュリティ管理者及び情報管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかにCISOに報告しなければならない。

ウ 例外措置の申請書の管理

CISOは、例外措置の申請書及び審査結果を適正に保管し、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 西脇市個人情報保護条例（平成17年西脇市条例第22号）

(6) 懲戒処分等

ア 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する。

イ 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が違反を確認した場合、統括情報セキュリティ責任者は当該職員等が所属する課室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) 情報管理者が違反を確認した場合は、速やかに統括情報セキュリティ責任者及び当該職員等が所属する課室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、あるい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は、職員等の権利を停止、あるいは剥奪した旨をCISO及び当該職員等が所属する課室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。

13 業務委託と外部サービスの利用

(1) 業務委託

ア 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。

イ 契約項目

職員等が情報システムの構築、運用、保守等を業務委託する場合には、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、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と範囲、アクセス方法
 - (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) 本市による監査、検査
 - (シ) 本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）

ウ 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十分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、上記イの契約に基づき措置を実施しなければならない。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じて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）

ア 外部サービスの利用に係る規定の整備

情報セキュリティ管理者は、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すること。

(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) 外部サービス管理者の指名と外部サービスの利用状況の管理

イ 外部サービスの選定

(ア) 情報セキュリティ責任者は、取り扱う情報の格付け及び取扱制限を踏まえ、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すること。

(イ) 情報セキュリティ責任者は、外部サービスで取り扱う情報の格付け及び取扱制限を踏まえ、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すること。

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ること。

a 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

b 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

c 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

d 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

e 情報セキュリティインシデントへの対処方法

f 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

g 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) 情報セキュリティ責任者は、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ること。

(エ) 情報セキュリティ責任者は、外部サービスの利用を通じて本市が取り扱う情報の格付け等を勘案し、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ること。

a 情報セキュリティ監査の受入れ

b サービスレベルの保証

- (ア) 情報セキュリティ責任者は、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ること。
 - (カ) 情報セキュリティ責任者は、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ること。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すること。
 - (キ) 情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、外部サービスを選定すること。また、外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めること。
 - (ク) 情報セキュリティ責任者は、外部サービスの特性を考慮した上で、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ること。
 - (ケ) 統括情報セキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の設定・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すること。
- ウ 外部サービスの利用に係る調達・契約
- (ア) 情報セキュリティ責任者は、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ること。
 - (イ) 情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者は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ること。

- エ 外部サービスの利用承認
- (ア) 情報セキュリティ責任者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行うこと。
 - (イ) 利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。
 - (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し、外部サービス管理者を指名すること。
- オ 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すること。
 - a 不正なアクセスを防止するためのアクセス制御
 - b 取り扱う情報の機密性保護のためのアクセス制御
 - c 開発時におけるセキュリティ対策
 - d 設計・設定時の誤りの防止
 - (イ) 外部サービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録すること。
- カ 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すること。
 - a 外部サービス利用方針の規定
 - b 外部サービス利用に必要な教育
 - c 取り扱う資産の管理
 - d 不正アクセスを防止するためのアクセス制限
 - e 取り扱う情報の機密性保護のための暗号化
 - f 外部サービス内の通信の制御
 - g 設計・設定時の誤りの防止
 - h 外部サービスを利用した情報システムの事業継続
 - (イ) 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すること。
 - (ウ) 外部サービス管理者は、全各項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・記録すること。
- キ 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、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の利用を終了する際のセキュリティ対策を規定すること。
 - a 外部サービスの利用終了時における対策
 - b 外部サービスで取り扱った情報の廃棄
 - c 外部サービスの利用のために作成したアカウントの破棄
- (イ) 外部サービス管理者は、前項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・記録すること。
- (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)
 - ア 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すること。
 - (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) 外部サービス管理者の指名と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
 - イ 外部サービスの利用における対策の実施
 - (ア) 職員等は、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すること。また、承認時に指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講ずること。
 - (イ) 情報セキュリティ責任者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。また、承認した外部サービスを記録すること。

14 情報セキュリティ監査及び自己点検の実施

(1) 監査

ア 実施方法

CIS0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。

イ 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対して、監査の実施を依

頼しなければならない。

- (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。

ウ 監査実施計画の立案及び実施への協力

- (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、監査実施計画を立案し、情報化推進委員会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。

エ 委託事業者に対する監査

事業者は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。

オ 報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、情報化推進委員会に報告する。

カ 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、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。

キ 監査結果への対応

CISOは、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、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。

ク 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

情報化推進委員会は、監査結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

(2) 自己点検

ア 実施方法

- (ア) 統括情報セキュリティ責任者及び情報管理者は、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、情報管理者と連携して、所管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。

イ 報告

統括情報セキュリティ責任者、情報管理者及び情報セキュリティ責任者は、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、情報化推進委員会に報告しなければならない。

ウ 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) 情報化推進委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

15 情報セキュリティポリシー及び関係規程等の見直し

情報化推進委員会は、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。