兵庫県後期高齢者医療広域連合
情報セキュリティ対策基準

（令和 6 年3 月31 日 改正版）

制定日：平成 19 年6 月25 日
改正日：令和　6 年3 月31 日
施行日：令和　6 年5 月　1 日

兵庫県後期高齢者医療広域連合

目次

1. 目的

兵庫県後期高齢者医療広域連合情報セキュリティ対策基準（以下「対策基準」という。）とは、兵庫県後期高齢者医療広域連合（以下「広域連合」という。）が定める兵庫県後期高齢者医療広域連合情報セキュリティ基本方針に基づき情報セキュリティ対策等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たものである。

2. 適用範囲

本対策基準が適用される範囲は兵庫県後期高齢者医療広域連合事務分掌規則（平成19年２月１日規則第１号。）第２条に規定する内部組織及び当広域連合が提供するシステムの利用をする者とする。

3. 組織体制

3.1 体制

適切に情報セキュリティ対策を推進・管理するため、次の者を置く。

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

事務局長をCISO とする。

3.1.2 情報セキュリティ統括責任者

事務局次長を情報セキュリティ統括責任者とする。

3.1.3 情報セキュリティ管理者

インターネット接続系に属するシステム関連において総務課長を、それ以外のネットワークに属するシステム関連において情報システム課長を情報セキュリティ管理者とする。なお、インターネット接続系に属するシステム関連において、情報システム課長は技術的支援及び助言を行うものとする。

3.1.4 情報管理者

情報資産を取り扱う課（課に準ずる組織を含む。以下同じ。）の長を、所管する課の情報管理者とする。

3.1.5 業務システム管理者

各業務システムを所管する課の長を当該業務システムに関する業務システム管理者とする。

3.1.6 情報セキュリティ監査統括責任者

事務局次長を情報セキュリティ監査統括責任者とする。

3.1.7 利用責任者

広域連合の提供する情報システムを利用するシステム利用団体において、それぞれ選任する者を所管における利用責任者とする。

3.2　権限と責任

3.2.1　CISO

ア　CISO は、広域連合における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

イ　CISO は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有する専門家をアドバイザーとして置くものとする。

ウ　CISO は、サイバー攻撃もしくはそのおそれのあるもの、情報漏えいもしくはそのおそれのあるもの、システム上の欠陥及び誤動作のいずれか又は複数に該当する事案（以下「情報セキュリティインシデント」という。）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。

3.2.2　情報セキュリティ統括責任者

ア　情報セキュリティ統括責任者は CISO を補佐する。

イ　情報セキュリティ統括責任者は、全てのネットワーク、情報システム等の情報資産における開発、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。

ウ　情報セキュリティ統括責任者は、全ての情報資産における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。

エ　情報セキュリティ統括責任者は、情報セキュリティ管理者、情報管理者、業務システム管理者に対して、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　情報セキュリティ統括責任者は、情報資産に対する情報セキュリティ侵害が発生した場合又は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。

カ　情報セキュリティ統括責任者は、緊急時等の円滑な情報提供を図るため、CISO、情報セキュリティ統括責任者、情報セキュリティ管理者、情報管理者、業務システム管理者を網羅する連絡体制を整備しなければならない。

キ　情報セキュリティ統括責任者は、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 にその内容を報告しなければならない。

ク　情報セキュリティ統括責任者は、共通的なネットワーク、情報システム等の情報資産に関する情報セキュリティ実施手順の維持・管理を行う統括的な権限及び責任を有する。

ケ　情報セキュリティ統括責任者は、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、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。

コ　情報セキュリティ統括責任者は、情報管理者を監督し、広域連合における緊急時等の連絡体制の整備並びに職員に対する助言及び指示を行う。

サ　情報セキュリティ統括責任者は、広域連合内の業務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。

シ　情報セキュリティ統括責任者は、当該業務システム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。

ス　情報セキュリティ統括責任者は、当該業務システムに関する情報セキュリティ実施手順の維持・管理を行う統括的な権限及び責任を有する。

セ　情報セキュリティ統括責任者は、当該業務システムについて、緊急時等の連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約及び職員に対する助言及び指示を行う。

3.2.3　情報セキュリティ管理者

ア　情報セキュリティ管理者は情報セキュリティ統括責任者を補佐し、その実務を担当する。

イ　情報セキュリティ管理者は、共通的なネットワーク、情報システム、情報等の情報資産における開発、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　情報セキュリティ管理者は、共通的なネットワーク、情報システム、情報等の情報資産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。

エ　情報セキュリティ管理者は、共通的なネットワーク、情報システム、情報等の情報資産に係る情報セキュリティ実施手順を策定し、その維持・管理を行う。

オ　情報セキュリティ管理者は、共通的なネットワーク、情報システム、情報等の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、情報セキュリティ統括責任者、情報セキュリティ管理者へ速やかに報告を行い、指示を仰がなければならない。

カ　情報セキュリティ管理者は、共通的なネットワーク、情報システム、情報等の情報資産のうちパーソナルコンピュータ等についての物理的セキュリティに関する管理を情報管理者に行わせることができる。

3.2.4　情報管理者

ア　情報管理者は、所管課内における情報等の情報資産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。

イ　情報管理者は、情報セキュリティ管理者の指示に従い適用範囲における共通的なネットワーク、情報システム、情報等の情報資産のうち所管組織内のパーソナルコンピュータ等についての物理的セキュリティに関する管理を行う。

ウ　情報管理者は、所管課内における情報等の情報資産に対する情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合には、情報セキュリティ統括責任者及び情報セキュリティ管理者へ速やかに報告を行い、指示を仰がなければならない。

3.2.5　業務システム管理者

ア　業務システム管理者は、当該業務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。

イ　業務システム管理者は、当該業務システム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　業務システム管理者は、当該業務システムに係る情報セキュリティ実施手順を策定し、その維持・管理を行う。

エ　業務システム管理者は、当該業務システムにおける開発、設定の変更、運用等についての作業を業務システム管理者が指名する者に行わせることができる。

3.2.6　情報セキュリティ監査統括責任者

情報セキュリティ監査統括責任者は、情報セキュリティ監査の計画、実施、報告等を行う権限及び責任を有する。

3.2.7　利用責任者

ア　利用責任者は、システム利用団体においてこの情報セキュリティポリシー及び業務システム管理者が定める実施手順が遵守されるよう必要な措置を講じなければならない。

イ　利用責任者は、システム利用団体において、情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には、情報セキュリティ管理者（不在の場合は情報セキュリティ統括責任者）へ速やかに報告を行い、指示を仰がなければならない。

ウ　利用責任者は、当該業務システムに係る情報セキュリティ実施手順を策定し、その維持・管理を行う。

3.2.8　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　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。

3.2.9　代行

CISO が欠けたとき又は事故があるときは、事務局次長がその事務を代行する。

3.3　CSIRT の設置・役割

3.3.1　CSIRT の設置

ア CISO は、情報セキュリティの統一的な窓口機能を有する CSIRT を設置し、CSIRT に所属する職員を選任しなければならない。情報セキュリティ管理者を CSIRT 責任者とする。また、CSIRT 内の業務統括及び外部との連携等を行う職員を定めなければならない。

イ　CISO は、情報セキュリティの統一的な窓口が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。

3.3.2　CSIRT の役割

ア　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。

イ　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。

ウ　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の統一的な窓口機能を有する部署、委託事業者等との情報共有を行わなければならない。

4.　情報資産の分類と管理

4.1　情報資産の分類と管理方法

対象となる情報資産は、各々の情報資産の機密性、完全性及び可用性を踏まえ、次の重要性分類に従って

分類する。

4.1.1　機密性

分類	分類基準
3	行政事務で取り扱う情報資産のうち、特に機密性を要するもの （例えば下記のデータが考えられる。なお、次のデータだけではなくそれらが含まれる電磁的記録媒体、パーソナルコンピュータ、システム等も同様） ・特定個人情報に関するデータ ・保有個人情報に関するデータ（出版、報道等により公知の情報を除く。） ・法令の規定により秘密を守る義務を課されているデータ ・部外に知られることが適当でない法人その他団体に関するデータ ・部外に漏れた場合に行政の信頼を著しく害する可能性があるデータ ・公開することでセキュリティ侵害が生じる可能性があるデータ
2	機密性 3 には当てはまらないが、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
1	機密性 2 又は機密性 3 以外の情報資産 ・情報公開請求により開示可能な情報（保有個人情報に関するデータのうち出版、報道等により公知の情報を含む。）

4.1.2　完全性

分類	分類基準
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
1	完全性 2 以外の情報資産

4.1.3　可用性

分類	分類基準
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
1	可用性 2 以外の情報資産

4.1.4　重要性分類に応じた対応

ア　情報資産の機密性、完全性、可用性のいずれかの重要性分類が 2 以上に分類される情報資産は、この対策基準の対象とする。

イ　重要性分類がいずれも 1 の情報資産も、必要なものはできる限りこの対策基準に準じた対応を講じるものとする。

4.2　情報資産の管理

ア　管理責任

(1) 情報資産は、情報管理者がそれぞれ所管する情報資産についての管理責任を有する。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管理し、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）の取扱いを定めなければならない。また、情報管理者は、当該情報資産の利用範囲を定め、リスクを分析し、リスクに応じた対策を講じなければならない。

(2) 情報管理者は、クラウドサービスを更改する際の情報資産の移行及び、これら情報資産の全複製がクラウドサービスから削除されることの記述を含む、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。

(3) 職員及び委託業務従事者等は、情報資産の作成・入手・利用等に際しては、十分にその責任を自覚したうえで行わなければならない。

(4) 情報管理者は、情報が複製又は伝送された場合には、当該複製等も原本と同様に管理しなければならない。

イ　情報資産の分類の表示

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

ウ　情報の作成

(1) 職員は、業務上必要のない情報を作成してはならない。

(2) 情報を作成する者は、情報の作成時に重要性分類に基づき、当該情報の分類と取扱制限を定めなければならない。

(3) 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

(1) 広域連合内の者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。

(2) 広域連合外の者が作成した情報資産を入手した者は、重要性分類に基づき、当該情報の分類と取扱制限を定めなければならない。

(3) 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

(1) 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。

(2) 情報資産の利用においては、情報資産の分類に応じ、利用者並びにアクセス権限を定めなければならない。

(3) 機密性 2 以上の情報は、情報管理者の許可を得た場合、複製・電子メール等による送信を行うことができる。また、権限のある者だけがアクセスできる環境で、保存・利用をしなければならない。複数の権限ある者で情報を共有するときや、所属外に情報を電子メール等により送信するときは、パスワード等による暗号化による情報漏えい対策を施さなければならない。ただし、電子メール等による送信に必要な宛名や連絡先等については、この限りではない。

(4) 情報資産を利用する者は、電磁的記録媒体又は紙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、当該媒体を取り扱わなければならない。

カ　情報資産の保管

(1) 情報管理者は、情報資産の重要性分類に従って、情報資産を適正に保管しなければならない。

(2) 情報管理者は、情報資産を記録した電磁的記録媒体を保管する場合は、書込禁止の措置を講じなければならない。

(3) 情報管理者は、持ち運び可能な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錠可能な場所に保管しなければならない。

(4) 情報セキュリティ管理者及び業務システム管理者は、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情報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への保管を考慮しなければならない。

キ　情報資産の運搬

(1) 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、機密情報を運搬する専用のサービスを利用する等、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。インターネットを利用した外部サービス等で委託事業者等へ重要な情報資産を運搬する場合は、アクセス制御等のシステム設定が適切にされているか、重要な情報資産を暗号化して保存しているか、外部委託事業者等と接続する通信が暗号化されているか等を確認しなければならない。

(2) 機密性 2 以上の情報資産を運搬する者は、情報管理者に許可を得なければならない。

(3) 機密性 2 以上の情報資産を運搬する者は、委託事業者等に重要な情報資産が運搬された後の情報の管理を徹底しなければならない。

ク　情報資産の提供・公表

(1) 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を行わなければならない。

(2) 機密性 2 以上の情報資産を外部に提供する者は、情報管理者に事前に許可を得たうえで、日時・担当者及び提供概要を記録しなければならない。

(3) また、外部に提供する場合は、次に掲げる事項を明記した覚書を広域連合長と提供先の代表者との間で取り交わすものとする。なお、広域連合を構成する市町が、後期高齢者医療制度運用のための本来目的で広域連合事務局にデータ作成を依頼する場合は、広域連合内部利用として取り扱い、別途定める手続きをとるものとする。

①データの内容に関する事項

②データの利用する業務の根拠法令に関する事項

③データの利用目的に関する事項

④データの提供方法に関する事項

⑤データの秘密の保持に関する事項

⑥データの目的外の利用及び第三者への提供の禁止に関する事項

⑦データの複写及び複製の禁止に関する事項

⑧データの取扱いに関する事故の発生時における報告義務に関する事項

⑨データの返還又は廃棄が必要な場合にあっては、データの返還又は廃棄に関する事項

⑩データの利用又は管理の状況の実地による調査等が必要な場合にあっては、当該調査の実施に関する事項

(4) 情報管理者は、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。

ケ　情報資産の廃棄等

(1) 情報資産の廃棄や機器の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、当該媒体の初期化等を行ったうえで物理的に破壊する等、復元不可能な状態にしなければならない。紙媒体が不要となった場合は、焼却、裁断、溶解等により廃棄しなければならない。

(2) 情報資産の廃棄や機器の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。

(3) 情報資産の廃棄や機器のリース返却等を行う者は、情報管理者の許可を得なければならない。

(4) 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期を確認し、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。

4.3　文書の管理

ア　情報セキュリティ対策基準を実施していくうえで必要とされる文書は、公文書管理規程及び情報セキュリティに係る文書管理基準等の定めに従い管理しなければならない。

イ　情報セキュリティに係る文書（以下「文書」という。）を作成又は更新する場合は、あらかじめ定められた者による承認を受けなければならない。

ウ　文書は、定期的に見直しを行い、必要に応じて更新しなければならない。

エ　文書を廃棄する場合は、廃棄文書が誤って使用されないようにしなければならない。ただし、廃棄文書を保持する必要がある場合には、廃棄文書と分かるように適切な識別を施さなければならない。

4.4　記録の管理

情報セキュリティ対策基準の効果的運用の証拠を示すために、記録を作成し、適切な管理をしなければならない。

5.　情報システム全体の強靭性の向上

5.1　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として情報セキュリティ統括責任者が認めるものについては、この限りではなく、インターネットに接続されていない専用ネットワークを経由して、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。

イ　情報のアクセス及び持ち出しにおける対策

(1) 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。

(2) 原則として、USB メモリ等の電磁的記録媒体やモバイル端末等による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。

ウ　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、当広域連合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。

エ　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。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。

5.2　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 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行わなければならない。

イ　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。

5.3　その他の情報システム

マイナンバー利用事務系、インターネット接続系のいずれにも該当しない情報システムについては、重要性分類に応じた情報セキュリティ対策を講じなければならない。

6.　物理的セキュリティ

6.1　サーバ等の管理

6.1.1　機器の取付け

情報セキュリティ管理者及び業務システム管理者は、ネットワーク機器及び情報システム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な固定を行う等必要な措置を講じなければならない。

6.1.2　サーバの冗長化

情報セキュリティ管理者及び業務システム管理者は、可用性 2以上の情報資産について二重化等を行い、同一データを保持する等の対策を講じなければならない。

6.1.3　機器の電源

ア　情報セキュリティ管理者及び業務システム管理者は、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　情報セキュリティ管理者及び業務システム管理者は、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。

6.1.4　　通信ケーブル等の配線

ア　配線の変更、追加については、情報セキュリティ管理者及び業務システム管理者等限られた者の権限とする。

イ　情報セキュリティ管理者及び業務システム管理者は、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施さなければならない。

ウ　情報セキュリティ管理者及び業務システム管理者は、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。

エ　情報セキュリティ管理者及び業務システム管理者は、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。

オ　情報セキュリティ管理者及び業務システム管理者は、自ら又は職員及び契約により操作を認められた委託事業者等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。

6.1.5　　機器の定期保守及び修理

ア　情報セキュリティ管理者及び業務システム管理者は、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　情報セキュリティ管理者、業務システム管理者及び情報管理者は、記憶装置を内蔵する機器を事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、事業者に故障を修理させるにあたり、委託事業者等との間で、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。

6.1.6　　敷地外への機器の設置

情報セキュリティ管理者及び業務システム管理者は、庁舎の敷地外にサーバ等の機器を設置する場合、情報セキュリティ統括責任者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。

6.1.7　　機器の廃棄等

ア　情報セキュリティ管理者、業務システム管理者及び情報管理者は、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。

イ　情報セキュリティ管理者、業務システム管理者及び情報管理者は、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）をする場合、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。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すること。

6.2　管理区域（情報システム室等）の管理

6.2.1　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の部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

イ　管理区域を新設する場合は、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にしなければならない。

ウ　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、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　情報セキュリティ管理者及び業務システム管理者は、情報システム室内の機器等に、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　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等に影響を与えないようにしなければならない。

6.2.2　入退室の管理等

ア　管理区域への入退室は、許可された者のみに制限し、ID カード等による認証及び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　職員及び委託事業者等は、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　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が付き添うものとし、外見上職員と区別できる措置を講じなければならない。

エ　管理区域について、当該情報システムに関連しない、又は個人所有である端末、モバイル端末、通信回線装置、電磁的記録媒体等持ち込ませないようにしなければならない。

オ　情報管理者は、重要性分類 2 以上のデータを取扱う執務区域については、許可された者以外の立入を制限するなどの適正な入退室管理を行わなければならない。

6.2.3　機器等の搬出入

ア　情報セキュリティ管理者及び業務システム管理者は、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、あらかじめ職員又は委託事業者等に確認を行わせなければならない。

イ　機器等の搬出入には、職員が同行する等の必要な措置を講じなければならない。

6.3　ネットワークの管理

6.3.1　通信回線及び通信回線装置の管理

情報セキュリティ管理者及び業務システム管理者は、事務局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。

6.3.2　外部ネットワークへの接続

情報セキュリティ管理者及び業務システム管理者は、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。

6.3.3　インターネットに接続されていない専用ネットワークへの集約

情報セキュリティ統括責任者は、国・県・市町等のネットワークに接続する場合は、インターネットに接続されていない専用ネットワークに集約するように努めなければならない。

6.3.4　機密を要する情報システムで使用する回線

情報セキュリティ管理者及び業務システム管理者は、所管する情報システムにおいて機密性 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うえ、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や送信する情報を必要最小限にする等、情報保護のために適正な措置を講じなければならない。

6.3.5　ネットワークで使用する回線

ア　情報セキュリティ管理者及び業務システム管理者は、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。

イ　情報セキュリティ管理者及び業務システム管理者は、ネットワークで使用する回線を選択するにあたって、必要な可用性を考慮しなければならない。

6.3.6　執務区域外からのマイナンバー利用事務系への接続制限

情報セキュリティ管理者および業務システム管理者は、執務区域外で業務を行うモバイル端末からマイナンバー利用事務系にアクセスできるようにしてはならない。

6.4　端末や電磁的記録媒体等の管理

6.4.1　端末等の盗難防止策

情報管理者は、執務区域等の端末等について盗難防止のための措置を講じなければならない。また、情報管理者は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。

6.4.2　ログイン認証

ア　情報セキュリティ管理者及び業務システム管理者は、情報システムへのログインに際し、パスワード、IC カード、或いは生体認証等複数の認証情報の入力を必要とするよう努めなければならない。また、必要に応じて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）を併用するものとする。

イ　情報セキュリティ管理者及び業務システム管理者は、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）を行うよう努めなければならない。

6.4.3　暗号化機能の利用

情報セキュリティ管理者及び業務システム管理者は、端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末等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。また、電磁的記録媒体についても、取り扱う情報の重要度に応じてデータ暗号化機能を備える媒体を使用しなければならない。

6.4.4　モバイル端末のセキュリティ

ア　モバイル端末とは、端末のうち執務区域外に持ち出して使用が可能な端末をいい、端末の形態は問わない。

イ　紛失・盗難に遭った際の対応として、遠隔消去（リモートワイプ）や自己消去機能などを活用できるときは、それらの機能を活用し、モバイル端末内のデータを消去しなければならない。

ウ　モバイル端末には覗き見防止の措置を講じ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及び業務システム管理者は、モバイル端末を執務区域外で業務利用する場合は、上記対策に加え、端末の紛失・盗難対策として、普段からパスワードによる端末ロックを設定しておかなければならない。また、執務区域外で機密性 2以上の情報を処理・保管する場合は、管理システム（MDM）を導入しなければならない。

6.4.5　業務外ネットワークへの接続の禁止

情報セキュリティ管理者及び業務システム管理者は機密性 2以上の情報を取り扱う支給端末（事務処理用PC 等）を情報セキュリティ統括責任者等権限のある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。

7.　人的セキュリティ

7.1　職員の遵守事項

7.1.1　職員の遵守事項

ア　情報セキュリティポリシー等の遵守

職員は、情報セキュリティポリシー及びこれに基づく文書に定められている事項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、速やかに情報管理者等権限のある者に相談し、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等を行ってはならない。

ウ　指示に基づいた情報資産の利用等

職員は、情報管理者等権限のある者の指示等に従い、情報資産を利用するとともに、開発、設定の変更、運用、更新等の作業を行う。

エ　情報資産の持ち出し禁止

職員は情報管理者の許可を得た場合に限り、記録を作成したうえで、執務区域外へ情報資産を持ち出すことができる。

オ　執務区域外における情報処理作業の制限

(1) 職員は、執務区域外で情報処理作業を行う場合には、情報管理者の許可を得なければならない。

(2) 職員は、執務区域外で端末を使用して情報処理作業を行う場合には、大量または機微な保

有個人情報を取り扱ってはならない。また、公共の場又は公共の乗り物内においては保有個人情報を取り扱ってはならない。

(3) 職員は紛失・盗難を防止するため、移動の際は細心の注意をもってモバイル端末を携行しなければならない。

(4) 職員は覗き見を防止するため、執務区域外において職員以外の目に触れないように取り扱わなければならない。

(5) 職員は不正使用を防止するため、モバイル端末を使用しないときは、他者に端末が使用されないように必要な対策を取らなければならない。

(6) 職員はモバイル端末でデータを保存する場合、指定されたファイルサーバの領域にデータを保存することとし、原則として端末内にデータを保存してはならない。

(7) 職員は、使用しているモバイル端末について、定期的に情報管理者の確認を受けなければならない。

(8) 職員は、執務区域外でモバイル端末を使用する場合、原則としてモバイル端末をプリンタに接続して、機密性 2 以上の情報資産の出力等を行ってはならない。

カ　支給以外の端末及び電磁的記録媒体等の業務利用

職員は、支給以外の端末及び電磁的記録媒体等（データ保存機能のないマウスやキーボード等の PC 周辺機器を除く）を原則として業務に利用してはならない。ただし、支給以外の端末の業務利用については、情報セキュリティ統括責任者が利用手順を定め、職員は利用手順に従い情報管理者の許可を得て利用することができる。

キ　持ち出しの記録

情報管理者は、端末等の持ち出しについて、記録を作成し、保管しなければならない。

ク　端末やモバイル端末におけるセキュリティ設定変更の禁止

職員は、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又は業務システム管理者の許可なく変更してはならない。

ケ　机上の端末等の管理

職員は、端末や電磁的記録媒体、情報が印刷された文書等について、第三者に使用されること、又は情報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や電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

コ　退職時等の遵守事項

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

サ　クラウドサービス利用時等の遵守事項

職員は、クラウドサービスの利用にあたっても情報セキュリティポリシー等を遵守し、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。

シ　生成AI 利用時等の遵守事項

職員は、生成AI（人工的な方法により学習、推論、判断等の知的機能を備え、かつ、質問その他の電子計算機に対する指令に応じて当該知的機能の活用により得られたテキスト、画像、音声または他のメディア等の結果を自動的に出力するよう作成されたプログラム及び当該プログラムと連携して動作するプログラム）の利用にあたっては、総務省のAI利活用ガイドライン及び情報セキュリティポリシー等を遵守し、生成AI 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。特に以下の点を意識すること。

(1) 生成AI の利用にあたっては本文書の「8.1.26 生成AI システムの構築・利用」に従い、当該生

成AI の構築・利用について必要な指定又は許可を受けていることを確認すること。

(2) 生成AI は業務執行にあたり補助的な役割を果たすものであり、職員が適切に利用範囲を判断すること。

(3) 生成AI の出力には、事実と異なる内容が含まれる可能性があるため、利用に際しては必ず事実確認を行うこと。

(4) 生成AI の出力には、第三者の著作物が含まれる可能性があるため、利用に際しては著作権を侵害しないよう留意すること。

7.1.2 臨時的任用職員への対応

非常勤職員、臨時職員及び契約等により当該業務に従事する者が情報資産を取り扱う必要が生じた場合は、情報管理者等管理権限のある者は従事させる事務の範囲を指定する。また、臨時的任用職員及び会計年度任用職員並びに特別職非常勤職員は 7.1.1 に定める事項を守らなければならない。

7.1.3 情報セキュリティポリシー等の掲示

情報管理者は、職員が常に情報セキュリティポリシー及びこれに基づく文書を参照できるよう配慮しなければならない。

7.2 研修・訓練

7.2.1 情報セキュリティに関する研修・訓練

ア CISO は、定期的に情報セキュリティに関する研修・訓練を実施させなければならない。イ CISO は、定期的にクラウドサービスを利用する職員の情報セキュリティに関する意識向上、教育及び訓練を実施させるとともに、外部委託事業者等を含む関係者については外部委託事業者等で教育、訓練が行われていることを確認させなければならない。

7.2.2 研修計画の策定及び実施

ア 情報セキュリティ統括責任者は、職員に対する情報セキュリティに関する研修計画を定期的に策定し、CISO に報告しなければならない。

イ 職員を対象とする情報セキュリティに関する研修を毎年度最低１回実施しなければならない。

ウ 職員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。

エ 研修は、情報セキュリティ統括責任者、情報セキュリティ管理者、情報管理者及び職員に対して、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 情報管理者は、所属の研修の実施状況を記録し、情報セキュリティ統括責任者に対して、報告しなければならない。

カ 情報セキュリティ統括責任者は、研修の実施状況を分析、評価し、CISO に情報セキュリティ対策に関する研修の実施状況について報告しなければならない。

7.2.3 緊急時対応訓練

CISO は、緊急時対応を想定した訓練を定期的に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。なお、CISO は、緊急時対応訓練の実施結果を受けて、緊急時の体制や対応手順の改善を行わなければならない。

7.2.4　研修・訓練への参加

すべての職員は、情報セキュリティに関する意識を深め情報セキュリティ上の問題が生じないようにするため、定められた研修・訓練に参加しなければならない。

7.3　情報セキュリティインシデントの報告

7.3.1　情報セキュリティインシデントの報告

ア　職員は、情報セキュリティインシデントを発見した場合、若しくは住民等外部から報告を受けた場合、速やかに情報管理者に報告しなければならない。

イ　報告を受けた情報管理者は、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。また、当該情報セキュリティインシデントが共通的なネットワークに関連する場合は、業務システム管理者に対しても報告しなければならない。あわせて当該情報セキュリティインシデントの重要性又は緊急性によっては、情報管理者から直接CISO に報告しなければならない。

ウ　情報管理者は、報告のあった情報セキュリティインシデントについて、国、県等の業務上の関係機関に必要な連絡を行うとともに、情報セキュリティ統括責任者に報告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。

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、情報セキュリティ統括責任者及びCISO、並びに総務省、都道府県等へ報告すること。

オ　情報セキュリティ統括責任者は、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を構築させなければならない。

7.3.2　情報セキュリティインシデントの報告内容

ア　情報管理者等から情報セキュリティ管理者への報告は、以下の内容を含むものとする。
(1) 件名
(2) 判明した日時
(3) 発生した日時
(4) 通報者
(5) 事件事故等の内容
(6) 漏えいした情報
(7) 想定される原因
(8) 事件事故等への対応
(9) 復旧方針

イ　業務システム管理者は、クラウドサービス事業者からの報告については、情報セキュリティインシデント発生時の報告手順を定め、クラウドサービス事業者の状況を適正かつ速やかに確認できるよう、インシデント発生時の報告に必要な要件を契約やSLA に定めるか、クラウドサービスの利用前に利用規約等を確認すること。

7.3.3　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管理者に対し、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の結果から、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。

7.4　アクセスのための認証情報及びパスワードの管理

7.4.1　ID カード等の管理

ア　情報セキュリティ管理者及び業務システム管理者は ID カード等の適正な管理を行わなければならない。

イ　職員は、次の事項を遵守しなければならない。

(1) ID カード等は、職員で共有しない。ただし、所属等ごとに配布された ID カード等については除く。

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

(3) ID カード等を紛失した場合には、速やかに情報管理者に報告し、指示に従わなければならない。

ウ　情報セキュリティ管理者及び業務システム管理者は、ID カード等の紛失等の報告があり次第、当該 ID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。

エ　情報セキュリティ管理者及び業務システム管理者は、ID カード等を切り替える場合、切替え前の ID 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。

7.4.2　ID の取扱い

職員は、自己の管理する ID に関し、次の事項を遵守しなければならない。

ア　自己が利用している ID は、他人に利用させてはならない。

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

7.4.3　パスワードの取扱い

職員は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

ア　パスワードは、他者に知られないように管理しなければならない。

イ　パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

ウ　パスワードは十分な長さ（原則として 8 文字以上）とし、文字列は想像しにくいもの（英字（大文字・小文字区別有）、数字、記号を組み合わせたものなど）としなければならない。ただし、端末や IC カード内に保存されている情報との照合を行うためのPIN についてはこの限りではない。

エ　パスワードを記載したメモを作成する場合は、特定の場所に施錠して保存する等により、他人

が容易に見ることができない措置をとる。

オ　パスワードが流出したおそれがある場合には、情報管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

カ　複数の情報システムを扱う職員は、同一のパスワードをシステム間で用いてはならない。

キ　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。

ク　サーバ、ネットワーク機器及び端末等に原則としてパスワードを記憶させてはならない。

ケ　職員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）。

8.　技術的セキュリティ

8.1　　コンピュータ及びネットワークの管理

8.1.1　　情報の保存

情報の保存については、情報セキュリティ管理者及び業務システム管理者等管理権限のある者の定める方法により保存を行わなければならない。

8.1.2　　ファイルサーバの設定等

情報セキュリティ管理者が情報を共有するためのファイルサーバを設置する場合には、次の事項を守らなければならない。

(1) 職員が使用できるファイルサーバの容量を設定し、職員に基本的事項を周知しなければならない。

(2) ファイルサーバを所属等の単位で構成し、職員が他所属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。

(3) 特定の職員のみが取扱う権限を持つ情報については、同一所属であっても、権限のない職員が閲覧及び使用できないよう設定しなければならない。

8.1.3　　バックアップの実施

ア　情報セキュリティ管理者及び業務システム管理者は、所管するシステムにおいて、必要なものはサーバの二重化対策実施の有無に関わらず、定期的に情報資産のバックアップのための対応を実施しなければならない。

イ　情報セキュリティ管理者及び業務システム管理者は、クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者にバックアップ機能の仕様を要求し、その仕様を確認しなければならない。また、その機能の仕様が当広域連合の求める要求事項を満たすことを確認しなければならない。クラウドサービス事業者からバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップのための対応を実施しなければならない。

8.1.4　　他団体との情報システムに関する情報等の交換

情報セキュリティ管理者及び業務システム管理者は、他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、情報セキュリティ統括責任者の許可を得て、当該内容を明記した合意文書を取り交わさなければならない。

8.1.5　　システム管理記録及び作業の確認

ア　情報セキュリティ管理者及び業務システム管理者は、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　情報セキュリティ管理者及び業務システム管理者は、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　情報セキュリティ管理者及び業務システム管理者又は職員及び契約により操作を認められた委託事業者等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。

8.1.6　　情報システム仕様書等の管理

情報セキュリティ管理者及び業務システム管理者は、所管するシステムのネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失したりすること等がないよう、適正に管理しなければならない。

8.1.7　　ログの取得等

ア　情報セキュリティ管理者及び業務システム管理者は、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　情報セキュリティ管理者及び業務システム管理者は、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　情報セキュリティ管理者及び業務システム管理者は、取得したログを定期的に点検又は分析する機能を設ける等、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。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　情報セキュリティ管理者及び業務システム管理者は、システムから自動出力したログ等について、必要に応じ、外部記録媒体にバックアップしなければならない。

オ　情報セキュリティ管理者及び業務システム管理者は、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。

8.1.8　　障害記録

情報セキュリティ管理者及び業務システム管理者は、所管するシステムにおいて、職員からのシステム障害の報告、システム障害に対する処理結果又は問題等を障害記録として体系的に記録し、適正に保存しなければならない。

8.1.9　　ネットワークの接続制御、経路制御等

ア　情報セキュリティ管理者及び業務システム管理者は、アクセス可能なネットワーク又はネット

ワーク上のサービス毎にアクセスできる者を定めなければならない。また、ネットワークサービスを利用する権限を有しない者が当該サービスを利用できるようにしてはならない。

イ　情報セキュリティ管理者及び業務システム管理者は、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。

ウ　情報セキュリティ管理者及び業務システム管理者は、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。

8.1.10　外部の者が利用できるシステムの分離等

ア　情報セキュリティ管理者及び業務システム管理者は、電子申請の汎用受付システム等、外部の者（職員及び委託業務従事者等以外の者）が利用できるシステムにおいては、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、情報セキュリティ対策について特に強固に対策を講じなければならない。

イ　外部の者が利用できるシステムにおいて、機密性　2以上の情報を照会又は更新するために外部の者がインターネット経由でシステムにアクセスしようとする場合は、不正アクセスを防止するため認証情報を設定しなければならない。

ウ　外部の者が利用できるシステムにおいて、兵庫県後期高齢者医療広域連合個人情報保護法施行条例第２条及び兵庫県後期高齢者医療広域連合議会の個人情報の保護に関する条例第２条に規定する要配慮個人情報または財産的価値のある情報を照会又は更新するために外部の者がインターネット経由でシステムにアクセスしようとする場合は、多段階認証又は多要素認証を利用できるようにしなければならない。

8.1.11　外部ネットワークとの接続制限等

ア　情報セキュリティ管理者及び業務システム管理者は、外部ネットワークとの接続にあたり、当該外部ネットワークのネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、適用範囲における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。

イ　情報セキュリティ管理者及び業務システム管理者は、接続に際して情報セキュリティの確保できるネットワーク構成を採らなければならない。情報セキュリティ管理者及び業務システム管理者は、当該外部ネットワークの瑕疵により当広域連合のデータの漏えい、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応するため、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するよう努めなければならない。

ウ　情報セキュリティ管理者及び業務システム管理者は、ウェブサーバ等をインターネットに公開する場 合、事務局内の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。

エ　情報セキュリティ管理者及び業務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、適用範囲における情報資産に脅威が生じることが想定される場合には、速やかに当該外部ネットワークとの接続を物理的に遮断しなければならない。

8.1.12　Web サイトでの情報公開時の注意事項

ア　情報セキュリティ管理者及び業務システム管理者は、Web サイトにより情報を公開・提供する

場合に、所管するサイトに係るシステムにおいて情報の漏えい・改ざん・消去、踏み台、DoS 攻撃等を防止しなければならない。また、なりすまし防止などの観点から、ドメイン変更時に旧ドメインを一定期間保有したりするなど、ドメインを適正に設定し、管理しなければならない。

イ　メールシステムを含め各業務システムにおいても、他のシステムに対する攻撃の踏み台とならないようにコンピュータウイルス対策等適正な管理をしなければならない。

ウ　新たに Web サイトを公開する場合、全てのページでTLS 通信を利用すること。なお、現状未対応の公開Web サイトは、全てのページでTLS 通信を利用するために必要な作業を実施しなければならない。

8.1.13　複合機のセキュリティ管理

ア　情報セキュリティ管理者及び業務システム管理者は、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　情報セキュリティ管理者及び業務システム管理者は、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　情報セキュリティ管理者及び業務システム管理者は、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。

8.1.14　IoT 機器を含む特定用途機器のセキュリティ管理

情報セキュリティ管理者及び業務システム管理者は、所管する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。

8.1.15　無線LAN 等の利用

ア　職員及び委託業務従事者等は、適用範囲内のネットワーク（以下「内部ネットワーク」という。）において、無線 LAN を利用した接続又は端末等の無線機能を利用した端末間通信を行ってはならない。

イ　合理的な理由があり、情報セキュリティ統括責任者が情報セキュリティを確保するために別途定める要件を満たす場合、情報セキュリティ管理者の許可を得て、無線 LAN を利用した接続等を行うことができる。ただし、マイナンバー利用事務系は無線LAN を利用することはできない。

8.1.16　電子メールのセキュリティ管理

ア　電子メールの利用を希望する場合は、その所属長が利用者を特定し、メールアドレスの取得を申請するものとする。

イ　情報セキュリティ管理者及び業務システム管理者は、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。

ウ　情報セキュリティ管理者及び業務システム管理者は、電子メールに添付されるファイルについて、セキュリティ上問題があると思われるファイルについては、送受信を制限できるようにしなければならない。

エ　情報セキュリティ管理者及び業務システム管理者は、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。

オ　　情報セキュリティ管理者及び業務システム管理者は、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等の作業員による電子メールアドレス利用について、委託事業者等との間で利用方法を取り決めなければならない。

8.1.17　電子メールの利用制限

ア　メールアドレス保有者は、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　メールアドレス保有者は、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　メールアドレス保有者は、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　メールアドレス保有者は、重要な電子メールを誤送信した場合、情報管理者に報告しなければならない。

8.1.18　電子署名・暗号化

ア　職員及び委託業務従事者等は、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、情報セキュリティ統括責任者が定めた電子署名、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　職員及び委託業務従事者等は、暗号化を行う場合に情報セキュリティ統括責任者が定める以外の方法を用いてはならない。また、情報セキュリティ統括責任者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　情報セキュリティ統括責任者は、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。

8.1.19　無許可ソフトウェアの導入等の禁止

ア　職員及び委託業務従事者等は、端末やモバイル端末に情報セキュリティ管理者に無断でソフトウェアを導入してはならない。

イ　職員及び委託業務従事者等は、業務を円滑に遂行するために必要なソフトウェアがある場合、情報セキュリティ管理者が定める手続きを行い、必要な許可を得て導入することができる。

ウ　職員及び委託業務従事者等は、不正にコピーしたソフトウェア及び個人所有のソフトウェアを導入又は使用してはならない。

8.1.20　機器構成の変更の制限

職員及び委託業務従事者等は、ネットワーク及び各自に供与された端末等に対して、端末及びその他機器の接続、増設又は改造を行ってはならない。軽微な機器の増設の場合は、情報セキュリティ管理者及び業務システム管理者等権限のある者の許可を必要とする。

8.1.21　業務外ネットワークへの接続の禁止

ア　職員及び委託業務従事者等は、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

用するよう情報セキュリティ管理者及び業務システム管理者等権限のある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　情報セキュリティ管理者及び業務システム管理者等権限のある者は、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よう努めなければならない。

8.1.22　利用可能なネットワークプロトコル

職員及び委託業務従事者等が利用できるネットワークプロトコルは、業務上必要最低限のものとする。

8.1.23　業務以外の目的でのWeb サイト閲覧の禁止

ア　職員は、業務以外の目的でWeb サイトを閲覧してはならない。

イ　情報セキュリティ管理者及び業務システム管理者等権限のある者は、職員のウェブ利用について、明らかに業務に関係のない Web サイトを閲覧していることを発見した場合は、情報管理者に通知し適正な措置を求めなければならない。

8.1.24　Web 会議サービスの利用時の対策

ア　職員は、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すること。イ　職員は、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。

8.1.25　ソーシャルメディアサービスの利用

ア　情報管理者は、当広域連合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、次の情報セキュリティ対策を行わなければならない。

(1) 当広域連合のアカウントによる情報発信が、実際の当広域連合のものであることを明らかにするために、 当広域連合の自己管理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。

(2) 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。

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

オ　可用性 2の情報の提供にソーシャルメディアサービスを用いる場合は、当広域連合のWeb サイト に当該情報を掲載して参照可能とすること。

8.1.26　生成AI システムの構築・利用

ア 情報管理者、業務システム管理者、情報セキュリティ管理者（以下、情報管理者等という。）は、生成AI を利用したシステム（以下「生成AI システム」という。）を構築・利用する場合、次の対策を行わなければならない。

(1) 生成AI システムへの入力情報が当広域連合の許可なく生成AI の学習に利用されないことを確認すること。

(2) 生成AI システムへの入力情報が当広域連合の許可なく同システムを提供する事業者による監査等により閲覧されないことを確認すること。

イ 情報管理者等は、AI チャットボット（人工的な方法により学習、推論、判断等の知的機能を備え、かつ、質問その他の電子計算機に対する指令に応じて当該知的機能の活用により得られた結果を自動的に回答するよう作成されたプログラムのうち生成AI に属するものをいう。）及びそれに類するものを除く生成AI において当広域連合の情報資産を取り扱う場合は、情報セキュリティ管理者の審査を受け、許可を得なければならない。

8.2 アクセス制御

8.2.1 アクセス制御等

ア アクセス制御

情報セキュリティ管理者及び業務システム管理者は、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

(1) 情報セキュリティ管理者及び業務システム管理者は、所管するネットワーク又はシステムに権限がない職員がアクセスすることが不可能となるように、利用者の識別及び認証等適正な対応を行わなければならない。

(2) 情報セキュリティ管理者及び業務システム管理者は、利用者の登録、変更、抹消等の情報管理、職員の異動、出向、退職に伴う利用者ID の取扱い等については、定められた方法に従って行わなければならない。必要な利用者登録・変更・抹消は、情報セキュリティ管理者及び業務システム管理者に対する申請により行う。ただし、所属等ごとに配布されたID 等については除く。

(3) 情報セキュリティ管理者及び業務システム管理者は、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。

(4) 情報セキュリティ管理者及び業務システム管理者は、ID に割り当てているアクセス権の正当性を確保するために、定められた方法に従って点検しなければならない。

ウ 特権 ID の管理等

(1) 情報セキュリティ管理者及び業務システム管理者は、管理者権限等の特権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。

(2) 情報セキュリティ管理者及び業務システム管理者は、特権ID 及びパスワードの変更について、原則として委託事業者等に行わせてはならない。

(3) 情報セキュリティ管理者及び業務システム管理者は、特権ID 及びパスワードについて、職員の端末等のパスワードと同等あるいはそれ以上のセキュリティ強化を実施しなければならない。

(4) 情報セキュリティ管理者及び業務システム管理者は、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。

(5) 情報セキュリティ管理者及び業務システム管理者は、特権ID を初期設定以外のものに変更しなければならない。

8.2.2 外部からのアクセス

ア 情報セキュリティ管理者及び業務システム管理者は、外部からのアクセスを許可する場合、合理的理由を有する必要最低限のものに限定しなければならない。

イ　情報セキュリティ管理者及び業務システム管理者は、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。

ウ　情報セキュリティ管理者及び業務システム管理者は、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。

エ　情報セキュリティ管理者及び業務システム管理者は、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。

オ　情報セキュリティ管理者及び業務システム管理者は、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禁止しなければならない。

8.2.3　内部ネットワーク間の接続

情報セキュリティ管理者及び業務システム管理者は、他の内部ネットワークとの接続については、あらかじめ接続先の内部ネットワークの管理者と協議し、以下の内容を確認したうえで、接続しなければならない。

ア　接続によりそれぞれの情報資産に影響が生じないこと

イ　接続した場合のそれぞれの情報システムの責任範囲

ウ　障害発生時の対応体制

8.2.4　自動識別の設定

情報セキュリティ管理者及び業務システム管理者は、内部ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるよう必要に応じてシステムを設定するものとする。

8.2.5　ログイン試行回数の制限等

情報セキュリティ管理者及び業務システム管理者は、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がログインしたことを確認することができるようにシステムを設定しなければならない。

8.2.6　認証情報の管理

ア　情報セキュリティ管理者及び業務システム管理者は、職員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　情報セキュリティ管理者及び業務システム管理者は、職員のパスワードを発行する場合において、仮のパスワードを発行する場合、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　情報セキュリティ管理者及び業務システム管理者は、仮のパスワードも含めパスワードを発行する場合、パスワードは十分な長さ（原則として8文字以上）とし、文字列は想像しにくいもの（英字（大文字・小文字区別有）、数字、記号を組み合わせたものなど）としなければならない。

エ　情報セキュリティ管理者及び業務システム管理者は、特権 ID のパスワードは定期的（概ね6か月以内）又はアクセス回数に基づいて変更し、古いパスワードを再利用しないものとする。

オ　情報セキュリティ管理者及び業務システム管理者は、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。

8.3 システム開発、導入、保守等

8.3.1 情報システムの調達

ア 情報セキュリティ管理者及び業務システム管理者は、情報システム開発、導入、保守等の調達に当たっては、一般に公開する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 情報セキュリティ管理者及び業務システム管理者は、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。

ウ 情報セキュリティ管理者は、適正に情報セキュリティ対策を推進・管理するための基礎資料として、情報システム台帳を作成し、整理する。情報セキュリティ管理者及び業務システム管理者は、情報システムを新たに調達したり、既にある情報システムを廃止したりしたときは、情報セキュリティ管理者からの求めに応じて、その旨を報告しなければならない。

エ 機密性 2以上の情報資産を扱う情報システムを開発または導入する場合は、情報セキュリティ管理者の審査を受け、許可を得なければならない。ただし、AI チャットボット及びそれに類するものを除く生成AI システムを開発または導入する場合は、取り扱う情報資産の機密性のいかんに関わらず、情報セキュリティ管理者の審査を受け、許可を得なければならない。

8.3.2 情報システムの開発

ア 情報セキュリティ管理者及び業務システム管理者は、ネットワーク及び情報システムの開発、導入、更新及び運用保守にあたっては、次の事項を定める。

(1) 責任者及び監督者
(2) 従事者及び作業範囲
(3) 開発するシステムと運用中のシステムとの分離
(4) 開発・保守に関する設計仕様等の成果物の提出
(5) セキュリティ上問題となり得るおそれのあるハードウェア及びソフトウェアの使用禁止
(6) アクセス制限
(7) 機器の搬入出の際の許可及び確認
(8) 記録の提出義務
(9) 仕様書・マニュアル等の定められた場所への保管
(10) 情報システムに係るソースコードの適正な方法での保管
(11) 開発・保守を行った者の利用者 ID、パスワード等の当該開発・保守終了後に不要となった時点での速やかな抹消
(12) 情報システムセキュリティ実施手順書等の整備

イ 情報セキュリティ管理者及び業務システム管理者は、ネットワーク及び情報システムの開発、導入、更新及び運用保守にあたって、不正にコピーしたソフトウェア及び個人所有のソフトウェアの導入又は使用等、問題のある行為が発生しないようにしなければならない。

ウ 情報セキュリティ管理者及び業務システム管理者は、ネットワーク及び情報システムの開発、導入、更新及び運用保守にあたって、コンピュータウイルス等対策ソフトウェアを導入する等、ウイルス感染やサイバー攻撃による情報漏えい等が発生しないようにしなければならない。

8.3.3　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

(1) 情報セキュリティ管理者及び業務システム管理者は、システム開発・保守計画の策定時に情報システムの移行手順を明確にしなければならない。

(2) 情報セキュリティ管理者及び業務システム管理者は、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。

(3) 情報セキュリティ管理者及び業務システム管理者は、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い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

(4) 情報セキュリティ管理者及び業務システム管理者は、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。

(5) 情報セキュリティ管理者及び業務システム管理者は、導入するシステムやサービスのリスクを把握し、適切にコントロール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

(1) 情報セキュリティ管理者及び業務システム管理者は、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。

(2) 情報セキュリティ管理者及び業務システム管理者は、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。また、作業については、作業経過を確認しながら実施するとともに、作業内容を記録しなければならない。

(3) 情報セキュリティ管理者及び業務システム管理者は、原則として保有個人情報及び機密性の高い生データを試験データに使用してはならない。ただし、合理的な理由がある場合で、情報セキュリティ統括責任者が許可した場合は、この限りではない。

(4) 業務システム管理者は、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。

(5) 情報セキュリティ管理者及び業務システム管理者は、試験に使用したデータ及びその結果を一定期間厳重に管理しなければならない。

8.3.4　システム開発・保守に関連する資料等の整備・保管

ア　情報セキュリティ管理者及び業務システム管理者は、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　情報セキュリティ管理者及び業務システム管理者は、担当するシステムにおいて行ったシステム変更等の作業やテスト結果については、職員による十分な検証が行われその結果が上長により承認された作業記録を作成しなければならない。作成した作業記録は、窃取、改ざん等をされないように適正に管理を行わなければならない。

ウ　情報セキュリティ管理者及び業務システム管理者は、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。

8.3.5　情報システムにおける入出力データの正確性の確保

ア　情報セキュリティ管理者及び業務システム管理者は、情報システムに入力されるデータについ

て、範囲、妥当性のチェック機能及び不正な文字列等の入力を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　情報セキュリティ管理者及び業務システム管理者は、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　情報セキュリティ管理者及び業務システム管理者は、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。

8.3.6　情報システムの変更管理

情報セキュリティ管理者及び業務システム管理者は、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。

8.3.7　ソフトウェアの保守及び更新

情報セキュリティ管理者及び業務システム管理者は、ソフトウェア等を更新、又は修正プログラムを導入する場合、不具合及び他のシステムとの相性の確認を行い、計画的に更新し又は導入しなければならない。

また、情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムについては、情報セキュリティ管理者及び業務システム管理者は、速やかに対応を行わなければない。

8.3.8　システム更新又は統合時の検証等

情報セキュリティ管理者及び業務システム管理者は、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。

8.3.9　委託業務等従事者等の身分確認

情報セキュリティ管理者及び業務システム管理者は、作業前に委託業務等従事者等に対して身分証明書の提示を求め、契約で定められた資格を有するものが作業に従事しているか確認をすることができるようにしておかなければならない。

8.4　不正プログラム対策

8.4.1　情報セキュリティ管理者等の措置事項

情報セキュリティ管理者、業務システム管理者及び情報管理者は、必要に応じて、次の事項を措置しなければならない。

ア　所管するサーバ及び端末に、原則としてコンピュータウイルス等対策ソフトウェアを常駐させなければならない。

イ　情報システムにおいて電磁的記録媒体を使用する場合、当広域連合が管理しているものを職員情報取扱者に使用させるとともに、当該媒体の使用にあたり、ウイルスチェックを行わせなければならない。

ウ　コンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものに保たなければならない。インターネットに接続していないシステムにおいても、定期的に当該ソフトウェア及び定義ファイルの更新を実施しなければならない。

エ　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原則として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。

オ　コンピュータウイルス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に当該権限を付与してはならない。

カ　ランサムウェアへの事前対策として、不正プログラム対策が適切に講じられているかを確認しなければならない。

キ　仮想マシンを設定する際に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クラウドサービス事業者に報告を求めなければならない。

8.4.2　職員及び委託業務事業者等の遵守事項

職員及び委託業務従事者等は、次の事項を遵守しなければならない。

ア　端末において、コンピュータウイルス等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ない。

イ　外部ネットワーク及び電磁的記録媒体からデータ又はソフトウェアを取り入れる際には、必ずコンピュータウイルス等対策ソフトウェアによるチェックを行う。

ウ　外部ネットワーク及び電磁的記録媒体へデータ又はソフトウェアを送信・書き込みする際には、必ずコンピュータウイルス等対策ソフトウェアによるチェックを行う。

エ　差出人が不明であるなど、不審な電子メールを受信した場合は速やかに削除する。

オ　端末に対して、コンピュータウイルス等対策ソフトウェアによる完全スキャンを定期的に行い、スキャンの実行を途中で止めない。

カ　情報セキュリティ管理者が提供するコンピュータウイルス等の情報を常に確認する。

キ　添付ファイルのあるメールを送受信する場合は、コンピュータウイルス等対策ソフトウェアでチェックを行う。

ク　コンピュータウイルス等に感染したおそれがある場合は、速やかに情報管理者に報告するとともに、その指示に従い、LAN ケーブルの取り外しや端末の通信機能の停止等、他への感染を防止する措置を講じる。

ケ　端末には、業務に必要なソフトウェアのみをインストールするとともに、端末に導入されているソフトウェアについて、情報セキュリティ管理者及び業務システム管理者等から最新版へのアップデートの指示等があったときは、速やかにその指示に従う。

コ　メールやSMS に添付されている URL は安易にクリックせず、ウェブサイトにアクセスする際は、あらかじめ登録しているURL からアクセスする。

サ　Web サービスにログインする場合に、多要素認証等の設定が可能な場合、有効化する。

8.4.3　専門家の支援体制

情報セキュリティ統括責任者は、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、コンピュータウイルス等対策ソフトのサポート契約を締結する等、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。

8.5　不正アクセス対策

8.5.1　使用されていないポートの閉鎖等

情報セキュリティ管理者及び業務システム管理者は、所管するシステムにおいて、不正なアクセスによる影響を防止するため、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データの書換えを検出する等、Web サイトの改ざんを防止しなければならない。

エ　ソフトウェアにセキュリティホールが発見された場合は、速やかに修正プログラムを適用しなければならない。

オ　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。

カ　情報セキュリティポリシー等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に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る場合、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、情報セキュリティポリシー等を満たすことを確認しなければならない。クラウドサービスのシステムやアプリケーション設定を変更するユーティリティプログラムは、原則として使用を禁止する。利用が必須なものは情報セキュリティ管理者又は業務システム管理者の承認を取得し、利用を管理した上で使用すること。

8.5.2　攻撃への対処

情報セキュリティ管理者及び業務システム管理者は、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、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。

8.5.3　記録の保存

CISO 及び情報セキュリティ統括責任者は、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。

8.5.4　内部からの攻撃

情報セキュリティ管理者及び業務システム管理者は、職員及び委託事業者等が使用している端末からの事務局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。

8.5.5　職員による不正アクセス

情報セキュリティ管理者及び業務システム管理者は、職員による不正アクセスを発見した場合は、当該職員が所属する課の情報管理者に通知し、適正な処置を求めなければならない。

8.5.6　サービス不能攻撃

情報セキュリティ管理者及び業務システム管理者は、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。

8.5.7　標的型攻撃

情報セキュリティ管理者及び業務システム管理者は、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。

8.6　セキュリティ情報の収集

8.6.1　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

ア　情報セキュリティ管理者は、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　情報セキュリティ管理者又は業務システム管理者は、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、当広域連合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すること。その上で、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に確認しなければならない。

8.6.2　不正プログラム等のセキュリティ情報の収集・周知

情報セキュリティ管理者は、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、職員に周知しなければならない。

8.6.3　情報セキュリティに関する情報の収集及び共有

情報セキュリティ管理者は、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。

9.　運用

9.1　情報システムの監視

ア　情報セキュリティ管理者及び業務システム管理者は、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　情報セキュリティ管理者及び業務システム管理者は、重要なログ等を取得するサーバの正確な時刻設定又は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　情報セキュリティ管理者及び業務システム管理者は、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　情報セキュリティ管理者及び業務システム管理者は、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　情報セキュリティ管理者及び業務システム管理者は、利用するクラウドサービスが、本文書の「8.1.7 ログの取得等」に定めた基準を満たすことを確認し、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　情報セキュリティ管理者及び業務システム管理者は、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に関して、手順化し、確認しなければならない。

(1) 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
(2) クラウドサービス利用の終了手順
(3) バックアップ及び復旧

9.2　情報セキュリティポリシーの遵守状況の確認

9.2.1　遵守状況の確認及び対処

ア　情報管理者は、情報セキュリティポリシー及びこれに基づく文書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、発生した問題について、適正かつ速やかに対処しなければならない。

ウ　情報セキュリティ管理者及び業務システム管理者は、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及びこれに基づく文書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。

9.2.2　端末、モバイル端末及び電磁的記録媒体等の利用状況調査

情報セキュリティ管理者及び業務システム管理者は、不正アクセス、不正プログラム等の調査のために、職員が使用している端末、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。

9.2.3　職員の報告義務

ア　職員は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに情報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情報セキュリティ統括責任者が判断した場合において、職員は、緊急時対応手順書に従って適正に対処しなければならない。

9.3　管理者権限の代行

情報セキュリティ管理者、業務システム管理者及び情報管理者の権限を代行する者は、それぞれが指名する。

9.4　侵害時の対応等

9.4.1　情報セキュリティインシデント発生時の対応手順書の策定

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

イ　情報セキュリティ統括責任者は、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明確にし、これらを踏まえてクラウドサービスの障害時を想定した、情報セキュリティインシデント発生時の対応手順書を定めておき、セキュリティ侵害時には当該手順書に従って適正に対処しなければならない。

9.4.2　情報セキュリティインシデント発生時の対応手順書に盛り込むべき内容

情報セキュリティインシデント発生時の対応手順書には、以下の内容を定めなければならない　。

ア　緊急時連絡網

イ　意思決定の所在

ウ　発生した事案に係る報告すべき事項

エ　発生した事案への対応措置

オ　再発防止措置の策定

9.4.3　緊急連絡網に盛り込むべき内容

緊急時の連絡先（所属、役職、電話番号、電子メールアドレス等）及び連絡順序がわかるように記載する。当広域連合内部や外部委託事業者等だけでなく、警察・関係機関も記載されていることが望ましい。

9.4.4　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、情報セキュリティ統括責任者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。

9.4.5　情報セキュリティインシデント発生時の対応手順書の見直し

情報セキュリティ統括責任者は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて情報セキュリティインシデント発生時の対応手順書の規定を見直さなければならない。

9.5　例外措置

9.5.1　例外措置の許可

情報セキュリティ管理者、業務システム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する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。なお、情報セキュリティ統括責任者が、軽微な例外措置と判断したものについては、当該責任者の許可により、例外措置を講じることができる。

9.5.2　緊急時の例外措置

情報セキュリティ管理者、業務システム管理者及び情報管理者は、前項に該当する場合であって、行政事務の遂行に緊急を要し、前項に定める許可を得る時間的な猶予のないときは、例外措置を実施し、実施後速やかに CISO に報告しなければならない。

9.5.3　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させなければならない。

9.6　法令遵守

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

(1) 地方公務員法（昭和 25 年法律第 261 号）
(2) 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）
(3) 著作権法（昭和 45 年法律第 48 号）
(4) 個人情報の保護に関する法律（平成 15 年法律第 57 号）
(5) 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）
(6) サイバーセキュリティ基本法（平成 26 年法律第 104 号）
(7) 兵庫県後期高齢者医療広域連合個人情報保護法施行条例
(8) 兵庫県後期高齢者医療広域連合議会の個人情報の保護に関する条例
(9) 兵庫県後期高齢者医療広域連合個人情報保護法施行条例施行規則
(10) 兵庫県後期高齢者医療広域連合文書規程（平成１９年３月２９日　訓令第２号）
(11) 各システム利用団体が定める個人情報保護制度に関する条例等

イ　情報セキュリティ管理者及び業務システム管理者は、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS 等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従わなければならない。

9.7　懲戒処分

9.7.1　懲戒処分

情報セキュリティポリシー及びこれに基づく文書に違反した職員及びその監督責任者は、その重大性、発生した事象の状況等に応じて、地方公務員法による懲戒処分の対象となる。

9.7.2　再発防止の指導等

職員及び委託業務従事者等に情報セキュリティポリシー及びこれに基づく文書に違反する行為がみられた場合には、情報管理者は、速やかに次の措置を講じなければならない。

ア　再発防止の指導その他適切な措置

該当者に対して違反する行為の事実を通知し、再発防止の指導その他適切な措置を行う。

イ　使用権の停止・剥奪

指導等によっても改善されない場合、当該職員の情報資産の使用権を停止あるいは剥奪する。

ウ　報告

違反する行為が生じた場合、違反する行為の内容、指導内容その他措置の状況について情報セキュリティ管理者に報告する。

10. 業務委託等と外部サービスの利用

10.1　業務委託等

10.1.1　委託事業者等の選定基準

特定個人情報を扱う業務又はネットワーク及び情報システムの開発・保守並びにデータ処理その他情報処理に係る業務の委託等においては、外部委託事業者等の選定にあたり、委託等の内容に応じた情報セキュリティ対策の実施が確保されることを確認しなければならない。

10.1.2　契約書の記載事項

ア　重要な情報資産を扱う業務又はネットワーク及び情報システムの開発・保守並びにデータ処理その他情報処理に係る業務委託においては、当該外部委託事業者事業者等との間で、下記事項を明記した契約を締結しなければならない。

(1) データその他業務上知り得た情報（以下「データ等」という。）の秘密の保持に関する事項
(2) 第三者への委託等（以下、「再委託等」という。）の禁止又は制限に関する事項
(3) データ等の目的以外の目的のための使用及び第三者への提供の禁止に関する事項
(4) データ等の複写及び複製の禁止に関する事項
(5) データ等の取り扱いに関する事故の発生時における報告義務に関する事項
(6) データ等の取り扱いに関する市による検査の実施に関する事項
(7) 契約に違反した場合における契約の解除及び損害賠償に関する事項
(8) 委託業務等終了時の情報資産の返還、廃棄等に関する事項
(9) 情報セキュリティポリシー及びこれに基づく文書の遵守に関する事項
(10) 事故時等の公表に関する事項
(11) 外部委託事業者等の責任者、委託等の内容、従事者の所属、作業場所の特定に関する事項
(12) 外部委託事業者等の責任者及び従事者に対する研修の実施に関する事項
(13) 情報セキュリティ確保への取り組みの実施状況に係る報告義務に関する事項
(14) 情報のライフサイクル全般での管理義務に関する事項

イ　前項に加えて、次に掲げる事項を必要に応じて契約書等に明記するよう努めるものとする。

(1)　提供されるサービスレベルの保証に関する事項
(2)　委託業務等の定期報告及び緊急時報告義務に関する事項
(3)　外部施設等への情報資産の搬送時における紛失、盗難、不正コピー等の防止に関する事項

10.1.3　確認・措置等

情報セキュリティ管理者及び業務システム管理者は、契約締結後においても、当該外部委託事業者事業者等の情報セキュリティ確保への取組みの実施状況等について、定期的若しくは随時、調査を行い、安全を確保しなければならない。情報セキュリティ統括責任者から内容の報告を求められた場合には、報告を行わなければならない。

10.1.4　再委託等

再委託（再々委託を含む。以下同様）を受ける事業者がある場合、10.1.2、10.1.3 に定める事項は再委託を受ける事業者にも適用する。

10.2　外部サービスの利用

事業者等の当広域連合の外部の組織が、情報システムの一部又は全部の機能を、その組織が定めた利用規約等に基づいて提供するサービスにおいて、当広域連合の情報資産を取り扱う場合は、CISO が別途整備する外部サービス利用基準に基づいて行うこととする。

11. 評価・見直し

11.1　監査

11.1.1　実施方法

CISO は、情報セキュリティ監査統括責任者に命じ、情報セキュリティ対策状況について、定期的及び必要に応じて監査を行わせなければならない。

11.1.2　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。

11.1.3　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、監査実施計画を策定し、CISO に報告しなければならない。

イ　被監査部門は、監査の実施に協力しなければならない。

11.1.4　委託事業者等に対する監査

ア　情報セキュリティ監査統括責任者は、外部委託事業者事業者等に対して、外部委託事業者事業者等からの再委託等（再々委託等を含む）の事業者も含めて、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及び必要に応じて行わなければならない。

イ　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、定期的に監査を行わなければならない。クラウドサービス事業者にその証拠（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もできる。

11.1.5　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、CISO に報告しなければならない。

11.1.6　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、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。

11.1.7　監査結果への対応

CISO は、監査結果を踏まえ、指摘事項に関係する情報管理者等に対し、当該事項への対処を指示しなければならない。また、指摘事項に関係しない情報管理者等に対しても、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、事務局内で横断的に改善が必要な事項については、情報セキュリティ統括責任者に対し、当該事項への対処を指示しなければならない。

11.1.8　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

CISO は、情報セキュリティポリシー等情報セキュリティ対策の見直し時に監査結果を活用しなければならない。

11.2　自己点検

11.2.1　実施方法

ア　情報セキュリティ管理者及び業務システム管理者は、所管するネットワーク及び情報システムの情報セキュリティ対策状況について、定期的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　情報管理者は、所管する所属の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、定期的及び必要に応じて自己点検を行わなければならない。

11.2.2　報告

ア　情報セキュリティ管理者、業務システム管理者及び情報管理者は、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、情報セキュリティ統括責任者に報告しなければならない。

イ　情報セキュリティ統括責任者は、報告を受けた点検結果及び改善策を CISO に報告しなければならない。

11.2.3　自己点検結果の活用

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

イ　CISO 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。

11.2.4　改善

ア　是正措置

情報セキュリティ管理者、業務システム管理者及び情報管理者は、業務上発見された問題、住民からの指摘による問題、監査及び自己点検において指摘された問題等に対する再発防止のため、その原因を除去するための措置を施さなければならない。

イ 予防措置

情報セキュリティ管理者、業務システム管理者及び情報管理者は、業務上予見される問題、他の組織で発生したものと同種の情報セキュリティに関する事件・事故等の発生を未然に防止するため、その原因を除去するための措置を施さなければならない。

11.3　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、監査及び自己点検の結果、改善の状況、残留リスク、情報セキュリティに関する状況の変化等を踏まえ、必要があると認めた場合、情報セキュリティポリシー等情報セキュリティ関連文書の見直しを行う。

11.4　情報セキュリティ個別基準の策定

CISO は、情報セキュリティポリシーを補完するために必要な全市共通の事項に関して、具体的な内容を定めた情報セキュリティ個別基準を策定する。

11.5　情報セキュリティ実施手順の策定

情報セキュリティ統括責任者は、情報セキュリティポリシーに基づき、所管するシステム等（専用 PC や Web サイトのうち保有個人情報を取扱うものも含む）に対する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させなければならない。