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

第１章　対象範囲

（適用の範囲）

第１条　本対策基準が適用される範囲は、職員、利用者及び外部委託事業者とする。

（情報資産の範囲）

第２条　本対策基準が対象とする情報資産は、次のとおりとする。

(1)　広域連合が管理する全てのネットワーク及び情報システム及びこれらに関する設備、電磁的記録媒体並びに情報システムへ入力する紙媒体の情報（以下「紙媒体情報」という。）

(2)　前項に関するネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

(3)　前二項に関する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

図１　情報資産の範囲

別紙参照

第２章　組織体制

（最高情報統括責任者）

第３条　広域連合長を、最高情報統括責任者（CIO；Chief Information Officer）とする。最高情報統括責任者は、広域連合が管理す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　最高情報統括責任者は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家をアドバイザーとして置くものとする。

（統括情報セキュリティ責任者）

第４条　広域連合事務局長を、最高情報統括責任者直属の統括情報セキュリティ責任者（CISO;Chief Information Security Officer）とする。統括情報セキュリティ責任者は最高情報統括責任者を補佐しなければならない。

２　統括情報セキュリティ責任者は、広域連合が管理する全てのネットワーク及び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。

３　統括情報セキュリティ責任者は、広域連合が管理する全てのネットワーク及び情報システム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。

４　統括情報セキュリティ責任者は、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。

５　統括情報セキュリティ責任者は、広域連合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、最高情報統括責任者の指示に従い、最高情報統括責任者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行う権限及び責任を有する。

６　統括情報セキュリティ責任者は、広域連合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。

７　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、最高情報統括責任者、統括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及び利用責任者を網羅する連絡体制を整備しなければならない。

８　統括情報セキュリティ責任者は、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、利用者及び外部委託事業者に対する教育、訓練、助言及び指示を行う。

（情報セキュリティ管理者）
第５条　広域連合の課長を、情報セキュリティ管理者とする。
２　情報セキュリティ管理者はその所管する課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。
３　情報セキュリティ管理者は、その所掌する課において、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、統括情報セキュリティ責任者及び最高情報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。

（情報システム管理者）
第６条　情報システム課長を、当該情報システムに関する情報システム管理者とする。
２　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、見直し等を行う権限及び責任を有する。
３　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。
４　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作成・維持・管理を行う。

（情報システム担当者）
第７条　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。

（情報セキュリティ委員会）
第８条　広域連合の情報セキュリティ対策を統一的に行うため、情報セキュリティ委員会において、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。
２　委員会の委員長は最高情報統括責任者をもって充てる。
３　委員会の委員は統括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をもって充てる。

（システム利用団体）
第９条　広域連合の情報システムは、システム利用団体との共同による開発・利用を基本とする。また、システム利用団体は、情報システムの運用にあたり情報セキュリティの維持向上に努めるものとする。

（利用責任者）
第１０条　システム利用団体に情報システムの利用責任者（以下、「利用責任者」という。）を置く。
２　利用責任者は、システム利用団体において選任する。
３　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情報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。
４　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及び情報システム管理者（不在の場合は統括情報セキュリティ責任者）へ速やかに報告を行い、指示を仰がなければならない。

（利用者）
第１１条　利用者は、この情報セキュリティポリシー及び実施手順を遵守し、情報システムを適正に利用しなければならない。

（兼務の禁止）
第１２条　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。

２　監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

図２　情報セキュリティ推進体制
別紙参照

図３　情報セキュリティ連絡体制
別紙参照

第３章　情報資産の分類と管理について

（情報資産の分類）
第１３条　広域連合における情報資産は、機密性、完全性及び可用性を踏まえ、次のとおり分類する。また、必要に応じ取扱制限を行うものとする。

分類	分類基準
Ⅰ	・業務上必要とする最小限の者のみが扱う情報で、情報が脅威にさらされた場合に組織運営に被害を受ける情報又はプライバシー等へ重大な影響を及ぼす情報 ・公開することを予定していない情報で、情報が脅威にさらされた場合に実害を受ける危険性が高い情報
Ⅱ	・公開することを予定していない情報で、情報が脅威にさらされた場合に実害を受ける危険性は低いが保護すべきと判断される情報
Ⅲ	・外部に公開する情報 ・上記以外の情報

（管理責任）
第１４条　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。
２　利用責任者は、その所管する情報資産について管理責任を有する。
３　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前条の分類に基づき管理しなければならない。

（情報の作成及び入手）
第１５条　職員、利用者及び外部委託事業者は、業務上必要のない情報を作成、入手してはならない。
２　職員及び利用者は、情報を第１３条の分類に基づき、適切に管理しなければならない。

（情報資産の利用）
第１６条　職員、利用者及び外部委託事業者は、業務以外の目的に情報資産を利用してはならない。
２　職員、利用者及び外部委託事業者は、情報資産の分類に応じ、適切な取扱いをしなければならない。

（情報資産の保管）
第１７条　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、情報資産を適切に保管しなければならない。

（情報の送信）
第１８条　分類Ⅰの情報は、電子メール等により送信を行ってはならない。
２　業務上やむを得ず送信をする場合は、情報セキュリティ管理者に許可を得たうえで、必要に応じて暗号化又はパスワード設定を行わなければならない。

（情報資産の運搬）
第１９条　車両等により分類Ｉの情報資産を運搬する場合は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。
２　分類Ｉの情報資産を運搬する場合は、情報セキュリティ管理者に許可を得なければならない。

（情報資産の提供・公表）
第２０条　分類Ｉの情報資産を外部に提供する場合は、必要に応じ暗号化又はパスワードの設定を行わなければならない。
２　分類Ｉの情報資産を外部に提供する場合は、情報セキュリティ管理者に許可を得なければならない。
３　情報セキュリティ管理者は、外部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。

（情報資産の廃棄）
第２１条　分類Ｉの情報資産を記録している記録媒体が不要になった場合、記録媒体の初期化等、情報を復元できないように処置した上で廃棄しなければならない。
２　情報資産の廃棄を行う場合は、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　情報資産の廃棄を行う場合は、情報セキュリティ管理者の許可を得なければならない。

第４章　物理的セキュリティ

第１節　サーバ等の管理

（機器の取付け）
第２２条　情報システム管理者及び利用責任者は、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切に固定する等、必要な措置を講じなければならない。

（サーバの二重化）
第２３条　情報システム管理者は、重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバを二重化し、ミラーリング等により同一データを保持しなければならない。
２　情報システム管理者は、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。

（機器の電源）
第２４条　情報システム管理者は、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、当該機器が適切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。
２　情報システム管理者は、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。

（通信ケーブル等の配線）
第２５条　統括情報セキュリティ責任者、情報システム管理者及び利用責任者は、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。

２　統括情報セキュリティ責任者、情報システム管理者及び利用責任者は、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。
３　統括情報セキュリティ責任者、情報システム管理者及び利用責任者は、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切に管理しなければならない。
４　統括情報セキュリティ責任者、情報システム管理者及び利用責任者は、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外部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施さなければならない。

（機器の保守及び修理）
第２６条　情報システム管理者は、迅速な保守体制を確保しなければならない。
２　情報システム管理者は、記憶媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報システム管理者は、外部の事業者に故障を修理させるにあたり、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他、秘密保持体制の確認などを行わなければならない。

（広域連合事務局以外への機器の設置）
第２７条　統括情報セキュリティ責任者及び情報システム管理者は、広域連合事務局以外にサーバ等の機器を設置する場合、最高情報統括責任者の承認を得なければならない。
２　業務委託によって前項を実施する場合、第２２条から第２６条及び第２８条から第３０条に準ずる内容を満たしていることを確認するとともに、サーバ等設置場所の管理者との間でその遵守について明記した契約を締結しなければならない。
３　統括情報セキュリティ責任者及び情報システム管理者は、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。

（機器の廃棄等）
第２８条　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、機器内部の記憶装置から、すべ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。

第2節　管理区域の管理

（管理区域の構造等）
第２９条　管理区域とは、広域連合事務局内において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、当該機器等の管理並びに運用を行うための部屋及び電磁的記録媒体並びに紙媒体情報の保管庫となる部屋をいう。
２　統括情報セキュリティ責任者及び情報システム管理者は、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。
３　統括情報セキュリティ責任者及び情報システム管理者は、管理区域内の機器等に、転倒及び落下防止等の耐震対策、防火措置等を講じなければならない。

（管理区域の入退室管理等）
第３０条　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等による入退室管理を行わなければならない。
２　職員及び外部委託事業者は、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。
３　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。
４　情報システム管理者は、分類Ｉの情報資産を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コンピュータ、通信回線装置、外部記録媒体等を持ち込ませないようにしなければならない。

（機器等の搬入出）

第３１条　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、あらかじめ職員又は外部委託事業者に確認を行わせなければならない。

２　情報システム管理者は、管理区域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。

第3節　通信回線及び通信回線装置の管理

（通信回線及び通信回線装置の管理）

第３２条　統括情報セキュリティ責任者は、広域連合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、適切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切に保管しなければならない。

２　統括情報セキュリティ責任者は、広域連合事務局外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

３　統括情報セキュリティ責任者は、分類Ｉ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、適切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。

４　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。また、無線LANの使用は認めてはならない。

第4節　パソコン等の管理

（パソコン等の管理）

第３３条　情報システム管理者は、執務室等のパソコン等の端末について、盗難防止のための物理的措置を講じなければならない。

２　情報システム管理者は、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。

第５章　人的セキュリティ

第1節　遵守事項

（情報セキュリティポリシー等の遵守）

第３４条　職員、利用者及び外部委託事業者は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

（業務以外の目的での使用の禁止）

第３５条　職員、利用者及び外部委託事業者は、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。

（パソコン等の端末の持ち出し及び外部における情報処理作業の制限）

第３６条　最高情報統括責任者は、分類Ｉ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。

２　職員及び外部委託事業者は、広域連合が管理するパソコン等の端末、記録媒体、情報資産及びソフトウエ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。
３　職員及び外部委託事業者は、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。
４　システム利用団体は、広域連合が管理する機器等の撤去、移設等（軽微なものを除く）を行おうとする場合には、事前に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。

（パソコン等の端末等の持込）
第３７条　職員及び外部委託事業者は、私物のパソコン及び記録媒体を広域連合事務局内に持ち込んではならない。

（パソコン等の端末におけるセキュリティ設定変更の禁止）
第３８条　職員及び外部委託事業者は、パソコン等の端末のソフトウエアに関する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。

（机上の端末等の管理）
第３９条　職員及び外部委託事業者は、パソコン等の端末や記録媒体、情報が印刷された文書等及び紙媒体情報について、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、離席時の端末のロックや記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない（クリアデスク・クリアスクリーン）。

（退職時等の遵守事項）
第４０条　職員、利用者及び外部委託事業者は、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。

（非常勤、臨時職員及び契約等により当該業務に従事する者への対応）
第４１条　広域連合の非常勤、臨時職員及び契約等により当該業務に従事する者に対しては、次に掲げる事項を実施しなければならない。
(1)　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、非常勤、臨時職員及び契約等により当該業務に従事する者の採用時等の際、必要に応じ、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。
(2)　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、非常勤、臨時職員及び契約等により当該業務に従事する者にパソコン等の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。

（情報セキュリティポリシー等の掲示）
第４２条　情報セキュリティ管理者は、職員、利用者及び外部委託事業者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掲示するとともに、周知しなければならない。

第２節　研修・訓練

（情報セキュリティに関する研修・訓練）
第４３条　最高情報統括責任者は、定期的に情報セキュリティに関する研修（個人情報、個人番号及び特定個人情報（以下「特定個人情報等」という。）の保護に関する研修を含む。以下同じ。）・訓練を実施しなければならない。

（研修計画の立案及び実施）

第４４条　最高情報統括責任者は、職員及び利用者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立案し、情報セキュリティ委員会の承認を得なければならない。
２　研修計画において、職員及び利用者は毎年度最低１回は情報セキュリティ研修を受講できるようにしなければならない。
３　研修は、統括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、その他職員及び利用者に対して、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。
４　最高情報統括責任者は、毎年度１回、情報セキュリティ委員会に対して、職員及び利用者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。

（研修・訓練への参加）
第４５条　職員及び利用者は、定められた研修・訓練に参加しなければならない。

第3節　事故、欠陥等の報告

（内部からの事故等の報告）
第４６条　職員、利用者及び外部委託事業者は、情報セキュリティに関する事故、システム上の欠陥及び誤動作を発見した場合、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。
２　報告を受けた情報セキュリティ管理者は、当該事故等が情報システムに関連する場合、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。
３　情報セキュリティ管理者は、報告のあった事故等について、必要に応じて最高情報統括責任者に報告しなければならない。

（住民等外部からの事故等の報告）
第４７条　職員、利用者及び外部委託事業者は、広域連合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事故、欠陥について、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。
２　報告を受けた情報セキュリティ管理者は、当該事故等が情報システムに関連する場合、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。また、当該事故等がネットワークに関連する場合は、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。
３　情報セキュリティ管理者は、当該事故等について、必要に応じて最高情報統括責任者に報告しなければならない。

（事故等の分析・記録等）
第４８条　統括情報セキュリティ責任者は、事故等を引き起こした部門の情報セキュリティ管理者及び情報システム管理者と連携し、これらの事故等を分析し、記録を保存しなければならない。

第4節　ＩＤ及びパスワード等の管理

（ＩＤの取扱い）
第４９条　職員、利用者及び外部委託事業者は、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。
⑴　自己が利用しているＩＤは、他人に利用させてはならない。
⑵　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。

（パスワードの取扱い）
第５０条　職員、利用者及び外部委託事業者は、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。
⑴　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。

(2)　パスワードを記載したメモを作成してはならない。
(3)　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。
(4)　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、パスワードを速やかに変更しなければならない。
(5)　パスワードは定期的に、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てはならない。
(6)　複数の情報システムを扱う職員、利用者及び外部委託事業者は、同一のパスワードをシステム間で用いてはならない。
(7)　仮のパスワードは、最初のログイン時点で変更しなければならない。
(8)　パソコン等の端末のパスワードの記憶機能を利用してはならない。
(9)　職員、利用者及び外部委託事業者間でパスワードを共有してはならない。

第６章　技術的セキュリティ

第1節　コンピュータ及びネットワークの管理

（文書サーバの設定等）
第５１条　情報システム管理者は、職員及び外部委託事業者が使用できる文書サーバの容量を設定し、職員及び外部委託事業者に周知しなければならない。
２　情報システム管理者は、文書サーバを課の単位で構成し、職員及び外部委託事業者が他課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　情報システム管理者は、特定個人情報等及び人事記録等、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、同一課であっても、担当以外の職員及び外部委託事業者が閲覧及び使用できないようにしなければならない。

（バックアップの実施）
第５２条　統括情報セキュリティ責任者及び情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの二重化対策に関わらず、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。

（システム管理記録及び作業の確認）
第５３条　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。
２　統括情報セキュリティ責任者及び情報システム管理者は、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、窃取、改ざん等をされないように適切に管理しなければならない。
３　統括情報セキュリティ責任者、情報システム管理者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外部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。

（情報システム仕様書等の管理）
第５４条　統括情報セキュリティ責任者及び情報システム管理者は、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が閲覧したり、紛失等がないよう、適切に管理しなければならない。

（アクセス記録の取得等）
第５５条　統括情報セキュリティ責任者及び情報システム管理者は、各種アクセス記録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。
２　重要システム等の管理を外部委託する場合は、各種アクセス記録及び情報セキュリティの確保

に必要な記録を取得させなければならず、その旨を契約に明記しなければならない。
3　統括情報セキュリティ責任者及び情報システム管理者は、アクセス記録等が窃取、改ざん、誤消去等されないように必要な措置を講じなければならない。
4　統括情報セキュリティ責任者及び情報システム管理者は、システムから自動出力したアクセス記録等について、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。

（障害記録）
第５６条　統括情報セキュリティ責任者及び情報システム管理者は、職員、利用者及び外部委託事業者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、適切に保存しなければならない。

（ネットワークの接続制御、経路制御等）
第５７条　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エア等を設定しなければならない。
2　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、ネットワークに適切なアクセス制御を施さなければならない。

（ネットワークの領域分割）
第５８条　情報システム管理者は、特に重要なネットワーク及び情報システムについては、他のネットワーク及び情報システムと領域を分割しなければならない。

（外部ネットワークとの接続制限等）
第５９条　情報システム管理者は、所管するネットワークを広域連合の管理外のネットワーク（以下、「外部ネットワーク」という。）と接続しようとする場合には、最高情報統括責任者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。
2　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、所管する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。
3　統括情報セキュリティ責任者及び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、所管する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うえで接続しなければならない。
4　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。

（ネットワークの盗聴対策）
第６０条　統括情報セキュリティ責任者は、機密性の高い情報を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。

（電子メールのセキュリティ管理）
第６１条　統括情報セキュリティ責任者は、職員以外の外部の者により、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。
2　統括情報セキュリティ責任者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。
3　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。
4　統括情報セキュリティ責任者は、職員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に周知しなければならない。

（電子メールの利用制限）
第６２条　職員及び外部委託事業者は、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。
２　職員及び外部委託事業者は、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。
３　職員及び外部委託事業者は、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。
４　職員及び外部委託事業者は、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。
５　職員及び外部委託事業者は、ウェブで利用できるフリーメール、ネットワークストレージサービス等を使用してはならない。

（暗号化）
第６３条　職員は、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、最高情報統括責任者が定めた暗号化又はパスワード設定の方法を使用して、送信しなければならない。

（無許可ソフトウエアの導入等の禁止）
第６４条　職員、外部委託事業者は、サーバ、パソコン等に無断でソフトウエアを導入してはならない。
２　利用者においては、広域連合が管理する機器等に無断でソフトウエアを導入してはならない。
３　職員、利用者及び外部委託事業者は、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システム管理者の許可を得て、ソフトウエアを導入することができる。
４　職員、利用者及び外部委託事業者は、不正にコピーしたソフトウエアを利用してはならない。

（機器構成の変更の制限）
第６５条　職員、利用者及び外部委託事業者は、サーバ、パソコン等に対し機器の改造及び増設・交換を行ってはならない。
２　職員、利用者及び外部委託事業者は、業務上、サーバ、パソコン等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システム管理者の許可を得なければならない。

（無許可でのネットワーク接続の禁止）
第６６条　職員、利用者及び外部委託事業者は、統括情報セキュリティ責任者の許可なくサーバ、パソコン等をネットワークに接続してはならない。

（業務以外の目的でのウェブ閲覧の禁止）
第６７条　職員及び外部委託事業者は、業務以外の目的でウェブを閲覧してはならない。
２　統括情報セキュリティ責任者は、職員及び外部委託事業者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切な措置を求めなければならない。

第2節　アクセス制御

（アクセス制御）
第６８条　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、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、利用者及び外部委託事業者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。

（利用者ＩＤの取扱い）
第６９条　統括情報セキュリティ責任者及び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、利用者及び外部委託事業者の異動、出向、退職者等に伴う利用者ＩＤの取扱い等の方法を定めなければならない。

２　職員、利用者及び外部委託事業者は、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、統括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。

３　統括情報セキュリティ責任者及び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、点検しなければならない。

（特権を付与されたＩＤの管理等）

第７０条　統括情報セキュリティ責任者及び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　統括情報セキュリティ責任者及び情報システム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システム管理者が指名し、最高情報統括責任者が認めた者でなければならない。

３　最高情報統括責任者は、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、情報セキュリティ管理者及び情報システム管理者に通知しなければならない。

４　統括情報セキュリティ責任者及び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、外部委託事業者に行わせてはならない。

５　統括情報セキュリティ責任者及び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、利用者及び外部委託事業者の端末等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。

（外部からのアクセス等の制限）

第７１条　職員、外部委託事業者が広域連合事務局内部のみで使用するネットワーク又は情報システムに外部から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システム管理者の許可を得なければならない。

２　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。

３　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。

４　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。

５　統括情報セキュリティ責任者及び情報システム管理者は、外部からのアクセスに利用するパソコン等の端末を職員、利用者及び外部委託事業者に貸与する場合、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。

６　職員、利用者及び外部委託事業者は、持ち込んだ又は外部から持ち帰ったパソコン等の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。

（パスワードに関する情報の管理）

第７２条　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、職員、利用者及び外部委託事業者のパスワードに関する情報を厳重に管理しなければならない。パスワード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パスワード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。

２　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、職員、利用者及び外部委託事業者に対してパスワードを発行する場合は、仮のパスワードを発行し、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。

（特権による接続時間の制限）

第７３条　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。

第3節　システム開発、導入、保守等

（情報システムの調達）

第７４条　統括情報セキュリティ責任者及び情報システム管理者は、情報システム開発、導入、保守等の調達にあたっては、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。

２　統括情報セキュリティ責任者及び情報システム管理者は、機器及びソフトウエアの調達にあたっては、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。

（情報システムの開発）

第７５条　情報システムの開発にあたっては、次に掲げる事項を遵守しなければならない。

(1)　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。

(2)　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、開発用ＩＤを削除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らない。

(3)　システム開発に用いるハードウエア及びソフトウエアの管理

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エア及びソフトウエアを特定しなければならない。

イ　情報システム管理者は、利用を認めたソフトウエア以外のソフトウエアが導入されている場合、当該ソフトウエアをシステムから削除しなければならない。

（情報システムの導入）

第７６条　情報システムの導入にあたっては、次に掲げる事項を遵守しなければならない。

(1)　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、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。

イ　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。

(2)　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、あらかじめ擬似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、特定個人情報等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。

（システム開発・保守に関連する資料等の保管）

第７７条　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文書を適切な方法で保管しなければならない。

２　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。

３　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切な方法で保管しなければならない。

（情報システムにおける入出力データの正確性の確保）

第７８条　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、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。

２　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。

３　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。

（情報システムの変更管理）

第７９条　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。

（開発・保守用のソフトウエアの更新等）

第８０条　情報システム管理者は、開発・保守用のソフトウエア等を更新、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。

第4節　不正プログラム対策

（統括情報セキュリティ責任者の措置事項）

第８１条　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。

(1)　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。

(2)　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。

(3)　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、利用者及び外部委託事業者に対して注意喚起しなければならない。

(4)　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エアを常駐させなければならない。

(5)　不正プログラム対策ソフトウエ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。

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

（情報システム管理者の措置事項）

第８２条　情報システム管理者は、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。

(1)　情報システム管理者は、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エアをシステムに常駐させなければならない。

(2)　不正プログラム対策ソフトウエ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。

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

(4)　インターネットに接続していないシステムにおいて、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、広域連合が管理している媒体以外を職員、利用者及び外部委託事業者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エアを導入し、定期的に当該ソフトウエ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。

（遵守事項）

第８３条　職員、利用者及び外部委託事業者は、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。

(1)　パソコン等の端末において、不正プログラム対策ソフトウエアが導入されている場合は、当該ソフトウエアの設定を変更してはならない。

(2)　外部からデータ又はソフトウエ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エアによるチェックを行わなければならない。

(3)　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。

(4)　端末に対して、不正プログラム対策ソフトウエ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。

(5)　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エアでチェックを行わなければならない。

(6)　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。

(7)　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は、LAN ケーブルの即時取り外し又は機器の電源遮断を行わなければならない。

第５節　不正アクセス対策

（統括情報セキュリティ責任者の措置事項）

第８４条　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、以下の事項を措置しなければならない。

(1)　使用されていないポートを閉鎖しなければならない。

(2)　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システム管理者へ通報するよう、設定しなければならない。

（攻撃の予告）

第８５条　最高情報統括責任者、統括情報セキュリティ責任者及び利用責任者は、サーバ等に攻撃を受けることが明確になった場合、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、関係機関と連絡を密にして情報の収集に努めなければならない。

（記録の保存）

第８６条　最高情報統括責任者、統括情報セキュリティ責任者及び利用責任者は、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。

（内部からの攻撃）

第８７条　統括情報セキュリティ責任者、情報システム管理者及び利用責任者は、職員、利用者及び外部委託事業者が使用しているパソコン等の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。

（職員、利用者及び外部委託事業者による不正アクセス）

第８８条　統括情報セキュリティ責任者、情報システム管理者及び利用責任者は、職員、利用者及び外部委託事業者による不正アクセスを発見した場合は、当該職員、利用者及び外部委託事業者が所属する課の情報セキュリティ管理者又は利用責任者に通知し、適切な処置を求めなければならない。

（サービス不能攻撃）

第８９条　統括情報セキュリティ責任者、情報システム管理者及び利用責任者は、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。

（標的型攻撃）

第９０条　統括情報セキュリティ責任者、情報システム管理者及び利用責任者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

第6節　セキュリティ情報の収集

（セキュリティホールに関する情報の収集・共有及びソフトウエアの更新等）

第９１条　統括情報セキュリティ責任者及び情報システム管理者は、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、ソフトウエア更新等の対策を実施しなければならない。

（不正プログラム等のセキュリティ情報の収集・周知）

第９２条　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、利用者及び外部委託事業者に周知しなければならない。

第7章　運用

第1節　情報システムの監視

（情報システムの監視）

第９３条　統括情報セキュリティ責任者及び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。

２　統括情報セキュリティ責任者及び情報システム管理者は、重要なアクセス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。

３　統括情報セキュリティ責任者及び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。

第2節　情報セキュリティポリシーの遵守状況の確認

（遵守状況の確認及び対処）

第９４条　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、速やかに最高情報統括責任者に報告しなければならない。

２　最高情報統括責任者は、発生した問題について、適切かつ速やかに対処しなければならない。

３　統括情報セキュリティ責任者及び情報システム管理者は、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切かつ速やかに対処しなければならない。

（端末及び記録媒体等の利用状況調査）

第９５条　最高情報統括責任者及び最高情報統括責任者が指名した者は、不正アクセス、不正プログラム等の調査のために、職員、利用者及び外部委託事業者が使用しているパソコン等の端末、記録媒体のアクセス記録、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。

（職員、利用者及び外部委託事業者の報告義務）

第９６条　職員、利用者及び外部委託事業者は、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。
２　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統括情報セキュリティ責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

第3節　侵害時の対応

（緊急時対応について）
第９７条　情報セキュリティ委員会は、情報セキュリティに関する事故、情報セキュリティポリシーの違反等により情報資産への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切に実施しなければならない。
２　緊急時の対応のためには、以下の内容を定めなければならない。
(1)　関係者の連絡先
(2)　発生した事案に係る報告すべき事項
(3)　発生した事案への対応措置
(4)　再発防止措置の策定

第4節　システム利用団体との情報の授受等

（システム利用団体との情報システムに関する必要な情報の授受等）
第９８条　情報システム管理者は、システム利用団体と情報システムに関する必要な情報を授受等する際に、その取扱いに関する事項を定め、最高情報統括責任者の許可を得て、システム利用団体と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。

第5節　外部委託

（外部委託先の選定基準）
第９９条　情報セキュリティ管理者は、外部委託先の選定にあたり、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。
２　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等を参考にして、事業者を選定しなければならない。

（契約項目）
第１００条　特定個人情報等を取扱う事務の全部又は一部を外部委託する場合若しくは情報システムの運用等を外部委託する場合には、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。
(1)　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
(2)　委託先の責任者、委託内容、作業者、作業場所の特定
(3)　提供されるサービスレベルの保証
(4)　従業員に対する教育の実施
(5)　提供された情報の目的外利用及び受託者以外の者への提供の禁止
(6)　提供された情報の複製等の禁止
(7)　業務上知り得た情報の守秘義務
(8)　情報の保護について委託事業者の代表者及び従業員からの誓約書提出義務
(9)　再委託に関する制限事項の遵守
(10)　委託業務終了時の情報資産の返還、廃棄等
(11)　委託業務の定期報告及び緊急時報告義務
(12)　広域連合による監査、検査
(13)　広域連合による事故時等の公表

(14)　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）

（確認・措置等）

第１０１条　情報セキュリティ管理者は、外部委託事業者（再委託先を含む。）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、前条の契約に基づき措置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最高情報統括責任者に報告しなければならない。

第6節　例外措置

（例外措置の許可）

第１０２条　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、最高情報統括責任者の許可を得て、例外措置を取ることができる。

（緊急時の例外措置）

第１０３条　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、事後速やかに最高情報統括責任者に報告しなければならない。

（例外措置の申請書の管理）

第１０４条　最高情報統括責任者は、例外措置の申請書及び審査結果を適切に保管しなければならない。

第7節　法令遵守

（法令遵守）

第１０５条　職員、利用者及び外部委託事業者は、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（昭和二十五年十二月十三日法律第二百六十一号）
(2)　著作権法（昭和四十五年法律第四十八号）
(3)　不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）
(4)　個人情報の保護に関する法律（平成十五年五月三十日法律第五十七号）
(5)　兵庫県後期高齢者医療広域連合個人情報保護条例（平成十九年条例第十九号）
(6)　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（平成二十五年法律第二十七号）
(7)　各システム利用団体が施行する個人情報保護条例等

第8節　違反時の対応

（懲戒処分）

第１０６条　情報セキュリティポリシーに違反した職員及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法及び関係法令（広域連合の条例及び規則を含む。）等による懲戒処分の対象とする。

（違反時の対応）

第１０７条　職員、利用者及び外部委託事業者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。

(1)　統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該

職員、利用者及び外部委託事業者が所属する課の情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

(2)　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及び当該職員、利用者及び外部委託事業者が所属する課の情報セキュリティ管理者又は利用責任者に通知し、適切な措置を求めなければならない。

(3)　情報セキュリティ管理者又は利用責任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、利用者及び外部委託事業者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、利用者及び外部委託事業者の権利を停止あるいは剥奪した旨を最高情報統括責任者及び当該職員、利用者及び外部委託事業者が所属する課の情報セキュリティ管理者又は利用責任者に通知しなければならない。

第８章　評価・見直し

第1節　監査

（実施方法）

第１０８条　情報セキュリティ委員会は、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、定期的に又は必要に応じて監査を行わせなければならない。

（監査を行う者の要件）

第１０９条　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。

２　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。

（監査実施計画の立案及び実施への協力）

第１１０条　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、情報セキュリティ委員会の承認を得なければならない。

２　被監査部門は、監査の実施に協力しなければならない。

（外部委託事業者に対する監査）

第１１１条　外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業者から下請けとして受託している事業者も含めて、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に又は必要に応じて行わなければならない。

（報告）

第１１２条　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、情報セキュリティ委員会に報告する。

（保管）

第１１３条　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切に保管しなければならない。

（監査結果への対応）

第１１４条　最高情報統括責任者は、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。

（情報セキュリティポリシーの見直し等への活用）
第１１５条　情報セキュリティ委員会は、監査結果を情報セキュリティポリシーの見直し、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。

第2節　自己点検

（実施方法）
第１１６条　統括情報セキュリティ責任者及び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、定期的に又は必要に応じ自己点検を実施しなければならない。
２　統括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て、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、毎年度又は必要に応じ自己点検を行わなければならない。

（報告）
第１１７条　統括情報セキュリティ責任者、情報システム管理者は、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、情報セキュリティ委員会に報告しなければならない。

（自己点検結果の活用）
第１１８条　職員、利用者及び外部委託事業者は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。
２　情報セキュリティ委員会は、この点検結果を情報セキュリティポリシーの見直し、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。

第3節　情報セキュリティポリシーの見直し

（情報セキュリティポリシーの見直し）
第１１９条　情報セキュリティ委員会は、情報セキュリティポリシーについて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ふまえ、必要があると認めた場合、その見直しを行うものとする。

附　則
この対策基準は、平成19年6月25日から施行する。
附　則
この対策基準は、平成23年4月1日から施行する。
附　則
この対策基準は、平成25年7月3日から施行する。
附　則
この対策基準は、平成27年9月1日から施行する。
附　則
この対策基準は、平成27年12月28日から施行する。
附　則
この対策基準は、平成28年4月1日から施行する。

図１　兵庫県後期高齢者医療広域連合　情報資産の範囲

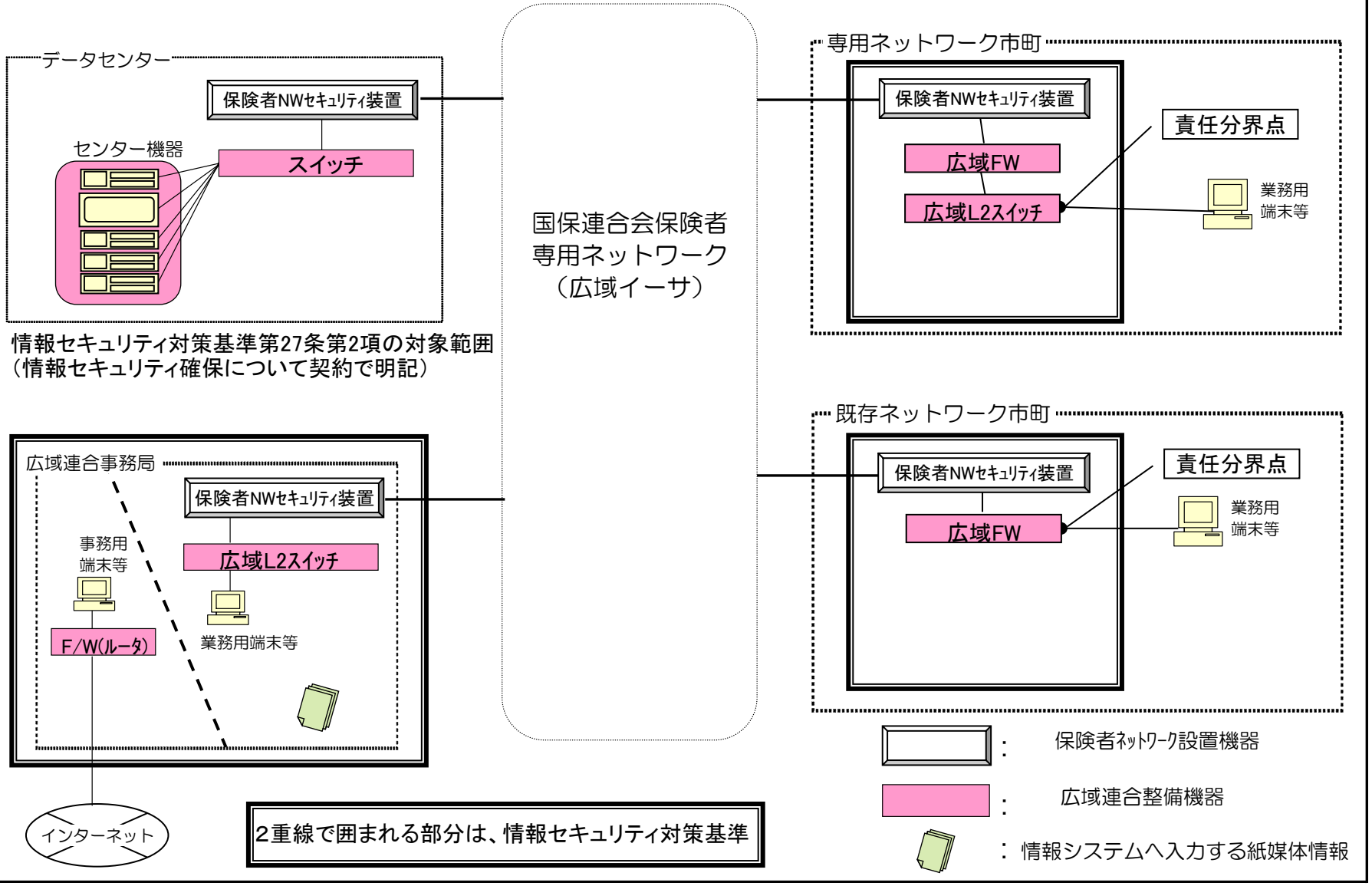


図　2

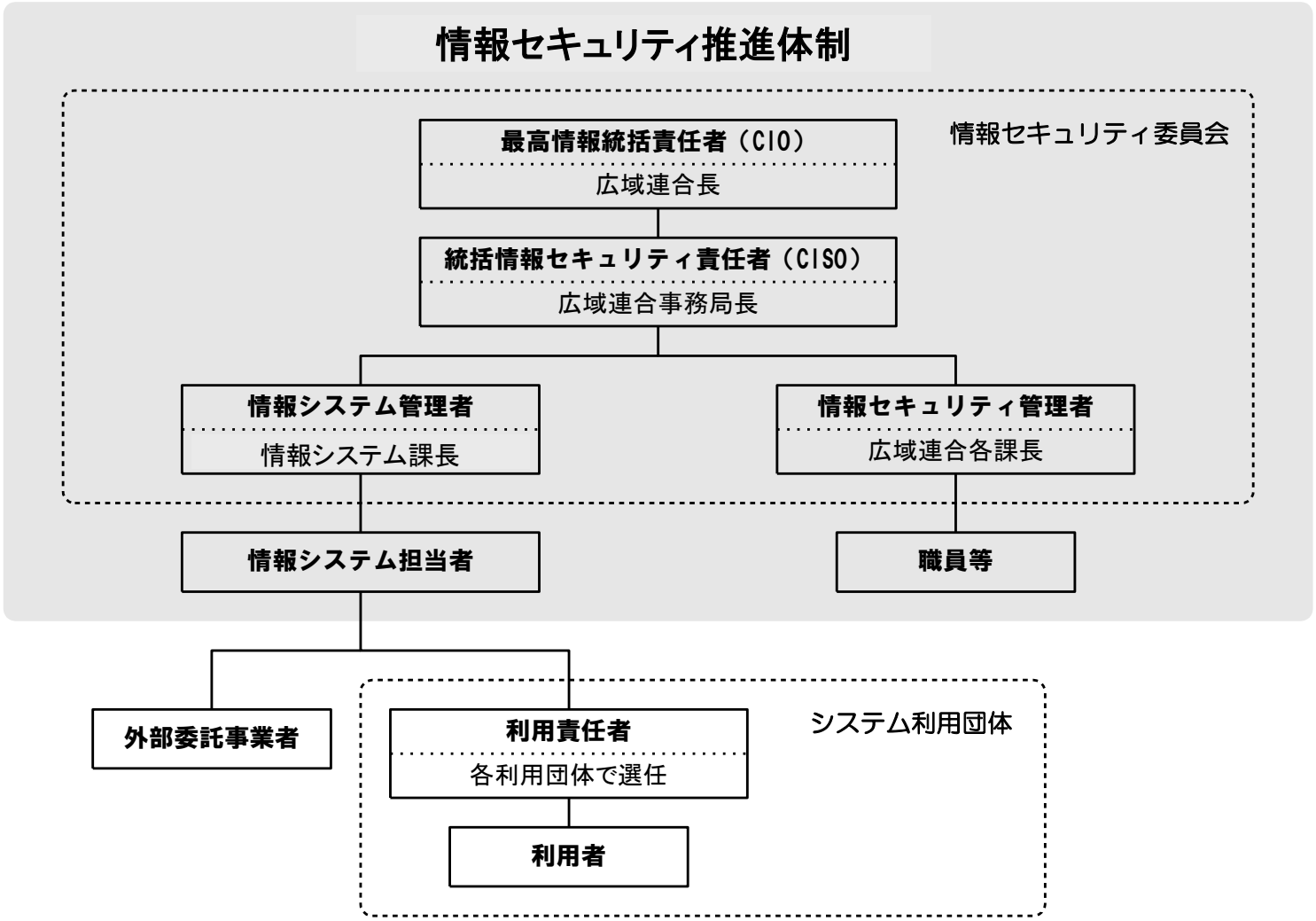
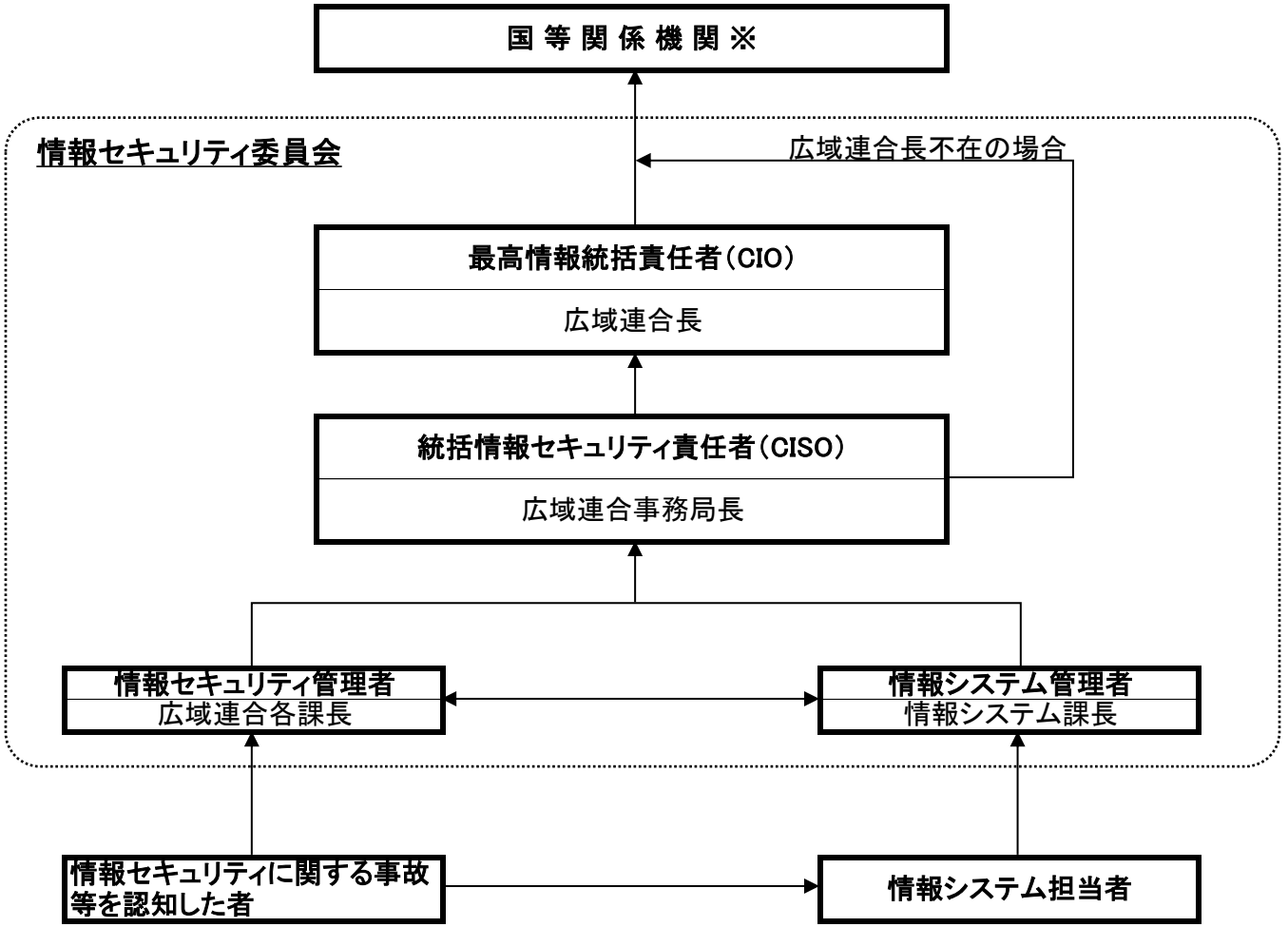

情報セキュリティ推進体制
情報セキュリティ委員会
最高情報統括責任者（CIO）
広域連合長
統括情報セキュリティ責任者（CISO）
広域連合事務局長
情報システム管理者
情報システム課長
情報セキュリティ管理者
広域連合各課長
情報システム担当者
職員等
外部委託事業者
利用責任者
各利用団体で選任
システム利用団体
利用者

図 3

情報セキュリティ連絡体制



※ 厚生労働省その他国の関係機関や警察等