茨城県後期高齢者医療広域連合
情報セキュリティポリシー

茨城県後期高齢者医療広域連合

目　　次

(2) 情報セキュリティポリシーの見直し

第１章　情報セキュリティ基本方針

１　目的

茨城県後期高齢者医療広域連合（以下「広域連合」という。）の情報システムが取り扱う情報には、被保険者等の個人情報及び業務運営上の重要な情報が多数含まれている。広域連合が保有する情報資産を、人的脅威、災害及び事故等の様々な脅威から防御することにより、被保険者等の個人情報及びプライバシー等を保護することになる。また、広域連合が、継続的に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。

この情報セキュリティ基本方針は、上記のことを踏まえ、広域連合が保有する情報資産の機密性、完全性及び可用性を維持するため、広域連合が実施する情報セキュリティ対策について総合的、体系的な基本方針を定めることを目的として制定するものである。

２　情報セキュリティポリシーの構成

広域連合の情報セキュリティ対策については、下図に示す階層構造から成り立つものである。それぞれの概要については以下のとおりであり、このうち「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」の２つを、「情報セキュリティポリシー」と総称するものである。

(1) 情報セキュリティ基本方針

広域連合の情報セキュリティ対策における基本的な考え方を定めるものである。

(2) 情報セキュリティ対策基準

情報セキュリティ基本方針に基づき、すべての情報システムに共通の情報セキュリティ対策の基準を定めるものである。

(3) 情報セキュリティ実施手順

情報セキュリティ対策を確実に実施していくため、情報セキュリティ対策基準に基づき、情報システム又は業務における具体的な対策の手順及び手続を定めるものである。

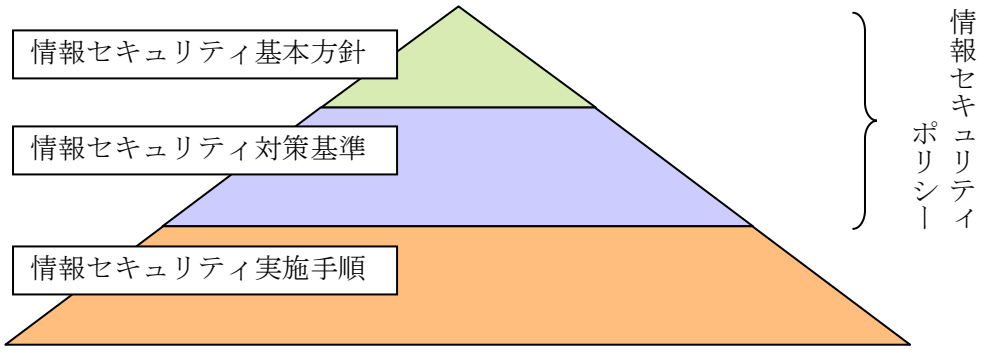

図　情報セキュリティポリシーに関する体系図

3　定義

(1) コンピュータ

ハードウェア及びソフトウェアで構成する電子計算機、周辺機器及び記録媒体等で構成する集合体をいう。

(2) 記録媒体

コンピュータで使用される磁気ディスク、磁気テープ、光ディスク、フラッシュメモリその他これらに類する記録媒体をいう。

(3) ネットワーク

コンピュータ等を相互に接続するための通信網及びその構成機器（ソフトウェアを含む。）をいう。

(4) 情報システム

コンピュータ、ネットワーク及び記録媒体で構成された情報処理を行う仕組みをいう。

(5) 行政情報

広域連合の行政事務の執行に係わる情報で、かつ、情報システムで取り扱うものをいう。

(6) 情報資産

情報システム及び行政情報をいう。

(7) 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。

ア　機密性（confidentiality）

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

イ　完全性（integrity）

情報が、破壊、改ざん又は消去されていない状態を確保することをいう。

ウ　可用性（availability）

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

(8) 職員等

広域連合に常勤する職員、嘱託職員及び臨時職員をいう。

4　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) 部外者の侵入、不正アクセス、ウィルス攻撃又はサービス不能攻撃等の意図的な要因による情報資産の漏えい、破壊、改ざん及び消去等

(2) 情報資産の無断持ち出し若しくは無許可ソフトウェアの使用等の規定違反又はプログラム上の欠陥、操作ミス若しくは故障等の非意図的要因による情報資産の漏えい、破壊及び消去等

(3) 地震、落雷及び火災等の災害による業務の停止等

5　職員等の遵守義務

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ポリシー、情報セキュリティ実施手順及び情報セキュリティに関する法令等を遵守しなければならない。

6　情報セキュリティ対策

情報資産に対する脅威から情報資産を保護するために、次の情報セキュリティ対策を講じるものとする。

(1) 組織体制

広域連合の情報資産を保護するために、情報セキュリティ対策を推進するとともに、情報資産を適切に管理するための組織体制を確立する。

(2) 情報資産の分類及びその管理

広域連合の保有する情報資産を、その重要度に応じて分類し、当該分類ごとに定める情報セキュリティ対策を行う。

(3) 物理的セキュリティ

情報資産の保管場所への不正な立入り、情報システムの損傷及び第三者からの妨害等を防止するために物理的対策を講じる。

(4) 人的セキュリティ

情報資産に接する職員等の情報セキュリティに関する権限や責任を定めるとともに、すべての職員等に情報セキュリティポリシーの内容を周知するための十分な教育及び啓発を行う等の必要な対策を講じる。

(5) 技術的セキュリティ

情報資産の管理、アクセス制御、不正プログラム対策及び不正アクセス対策等の技術的対策を講じる。

(6) 運用

情報資産を、外部からの不正なアクセス等から適切に保護するために、情報システムの監視、情報セキュリティポリシーの遵守状況の確認及び外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。

7　自己点検の実施

情報セキュリティポリシーに沿った情報セキュリティの対策状況を検証するために、定期的に又は必要に応じて自己点検を実施しなければならない。

8　情報セキュリティポリシーの見直し

自己点検の結果及び情報セキュリティに関する新たな対策が必要となった場合は、情報セキュリティポリシーの見直しを行うものとする。

9　情報セキュリティ対策基準の策定

情報セキュリティ対策の実施における具体的な遵守事項及び判断基準等を定めるため、情報セキュリティ対策基準を策定する。

10　情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策の実施における具体的な手順を定めるため、情報セキュリティ実施手順を策定する。

なお、情報セキュリティ実施手順は、公開することにより広域連合の運営に重大かつ深刻な支障を及ぼすおそれがあるため、非公開とする。

第２章　情報セキュリティ対策基準

情報セキュリティ対策基準とは、広域連合の保有する情報資産を保護するために、情報セキュリティ基本方針に沿って、その具体的なセキュリティ対策を講じるための指針となるものである。

第１節　総則

1　組織体制

情報セキュリティの管理は、次の体制で行う。

(1) 情報統括責任者

広域連合における情報セキュリティを統括する責任者として、情報統括責任者（以下「統括責任者」という。）を置き、事務局長をもって充てる。

(2) 副情報統括責任者

統括責任者を補佐するため、副情報統括責任者（以下「副統括責任者」という。）を置き、事務局次長をもって充てる。

(3) 情報セキュリティ管理者

情報セキュリティ対策の実務を統括する情報セキュリティ管理者（以下「セキュリティ管理者」という。）を置き、電算担当課の長をもって充てる。

(4) 情報システム管理者

各課等における情報セキュリティの適正な運営及び管理を行うために、情報システム管理者（以下「システム管理者」という。）を置き、各課等の長をもって充てる。

(5) 情報システム担当者

各課等における情報セキュリティの調整を図るために、情報システム担当者（以下「システム担当者」という。）を置き、当該システム担当者は、セキュリティ管理者が指定する。

(6) 情報セキュリティ委員会

ア　広域連合の情報セキュリティについて協議するため、情報セキュリティ委員会（以下「委員会」という。）を置く。

イ　委員会は、委員長、副委員長及び委員をもって構成する。

ウ　委員長は、統括責任者をもって充てる。

エ　副委員長は、副統括責任者をもって充てる。

オ　委員は、セキュリティ管理者及びシステム管理者をもって充てる。

カ　委員会の庶務は、電算担当課において処理する。

キ　上記のほか、委員会の運営に必要な事項は、委員長が委員会に諮って定める。

2　情報資産の分類及び管理の方法

(1) 情報資産の管理責任

ア　管理責任

情報資産の管理責任は、システム管理者が有する。

イ　利用者の責任

情報資産の利用責任は、当該利用者が有する。

ウ　重要性の効力

データが複製又は伝送された場合は、当該複製データ又は伝送されたデータも原本と同様に管理しなければならない。

(2) 情報資産の分類及び管理の方法

ア　情報資産の分類

(ｱ) 情報資産におけるデータは、次の重要性分類に従って分類するものとする。

区　分	重　　要　　性　　分　　類
分類Ⅰ	(1) 個人情報が含まれているデータ (2) 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 (3) 部外に知られることが適当でない法人その他の団体に関するデータ (4) 部外に漏れた場合に行政の信頼を著しく害するおそれのあるデータ (5) 滅失又は損傷した場合にその復元が著しく困難であるため、行政の円滑な運営が妨げられるおそれのあるデータ (6) 公開することによりセキュリティの侵害が生じるおそれのあるデータ
分類Ⅱ	上記以外のデータ

(ｲ) 情報資産の重要性分類Ⅰに分類される情報資産は、この対策基準の対象とする。また、重要性分類Ⅱに分類される情報資産についても、できる限り情報セキュリティ対策基準に準じた対応を講じるものとする。

イ　情報資産の管理の方法

(ｱ) 情報資産の管理

①　情報資産のうち重要性分類Ⅰに分類されるものは、情報資産の取り扱いにおいて、情報資産の利用者並びにアクセス権限を定めなければならない。

②　情報資産のうち重要性分類Ⅰに分類されるものは、システム管理者の許可を得た場合に限り、データの複写、複製、送付又は送信を行うことができる。

(ｲ) 記録媒体の管理

①　持ち運びが可能な記録媒体は、セキュリティ管理者が、施錠が可能な保管庫等によ

り適切な管理を行わなければならない。

② 記録媒体の搬送にあたっては、損傷等から物理的に保護する対策を講じなければならない。

(ｳ) 情報資産の廃棄

必要がなくなった情報資産は、データ等の消去を行ったうえで、復元をすることが不可能な状態にして廃棄しなければならない。

第２節　物理的セキュリティ

1　サーバ等の設置基準

(1) 入退室の管理

セキュリティ管理者は、重要性分類Ｉのデータが記録されている記録媒体の保管場所及びそれを取り扱う情報システムの設置場所への入退室について、適正な管理を行わなければならない。

(2) 機器の取付け等

ア　サーバ等の機器の設置及びネットワーク回線の敷設を行う場合は、火災、水害、埃、振動、温度及び湿度等の影響を可能な限り排除した場所に設置するなど適切な措置を講じなければならない。

イ　情報システムの停止により、業務の遂行に重大な影響を及ぼすおそれがあるものは、情報システムの二重化等、当該情報システムの運用に支障が生じないように適切な措置を講じるよう努めなければならない。

ウ　セキュリティ管理者など権限のある者以外の者が、容易に情報システムを操作できないように、利用者のＩＤ、パスワードの設定等の措置を講じなければならない。

(3)　電源

ア　サーバ等の機器の電源については、突発的な停電に対応するため、当該機器を適切に停止するまでの間に十分な電力を供給できる容量の予備電源を設置しなければならない。

イ　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装置を設置しなければならない。

(4) 配線

配線の変更又は追加を行う場合は、セキュリティ管理者にあらかじめ協議のうえその承認を受けなければならない。

(5) 機器等の搬入又は移動

ア　サーバ等の機器を搬入又は移動する場合は、あらかじめ当該機器による他の情報システ

ムに対する安全性について、セキュリティ管理者の確認を受けなければならない。

イ　サーバ等の機器の搬入又は移動をする場合は、職員等が同行するなどの必要な措置を講じなければならない。

2　ネットワーク

(1) 通信回線による外部へのネットワークの接続は、必要最小限のものに限定し、可能な限り接続ポイントを減らさなければならない。

(2) ネットワークに使用する回線は、伝送途上においてデータの破壊、盗聴、改ざん又は消去等が生じないように十分なセキュリティ対策が講じられたものでなければならない。

3　端末機等の盗難の防止

事務室に職員等が不在となる場合は、事務室の施錠等を確実に行い、盗難防止のための措置を講じなければならない。

第3節　人的セキュリティ

1　職員等の責務

(1) 情報セキュリティ対策の遵守義務

職員等は、情報システムの操作等を行う場合においては、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に定められている事項を遵守しなければならない。

(2) 職員等は、職務に従事する場合において使用する情報資産について、情報セキュリティポリシー及び情報セキュリティ実施手順に定めるもののほか、関係法令等を遵守して取り扱わなければならないものとする。

(3) 職員等は、情報資産を業務上の目的以外に使用してはならない。

(4) 職員等は、システム管理者の指示に従い、情報資産を利用するとともに、情報システムの開発、設定の変更、情報システムの運用及びデータの更新等の作業を行わなければならない。

(5) その他

ア　職員等は、業務で使用する端末機及び記録媒体を、第三者に使用されること、又はデータを閲覧されることがないように、適切な管理をしなければならない。

イ　職員等は、端末機及び記録媒体等を、事務室外に持ち出してはならない。ただし、やむを得ない事情がある場合に限り、システム管理者の許可を得て、端末機及び記録媒体等を、事務室外に持ち出すことができるものとする。

ウ　職員等は、情報システム等の操作により知り得た情報を、他に漏らしてはならない。人

事異動又は退職等によりその職を離れた場合も同様とする。

エ　職員等は、自己の保有するパスワードについて、他に漏らすこと又は他のものが容易に知り得るような記録を作成するなどの行為を慎み、パスワードの秘密保持に努めなければならない。

オ　職員等は、情報システムの認証に用いるために貸与されたＩＤカードを、適切に管理しなければならない。

カ　職員等は、情報セキュリティ実施手順について、不明な事項、遵守することが困難な事項がある場合には、システム管理者の指示を受けなければならない。ただし、システム管理者が、判断し難い場合においては、セキュリティ管理者と協議のうえ、その対応を決定しなければならないものとする。

(6) 嘱託職員及び臨時職員を、情報システムの操作又は情報資産を取り扱う事務に従事させるときは、システム管理者がセキュリティ管理者と協議して、当該職員が従事する事務の範囲を定めなければならないものとする。また、システム管理者は、当該職員が事務に従事する前に、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に関し、十分な説明を行わなければならないものとする。

2　教育

(1) 統括責任者は、職員等に対して、定期的に又は必要に応じて情報セキュリティに関する研修及び啓発を行わなければならない。

(2) 職員等は、統括責任者が定めた研修に参加し、情報セキュリティに関する意識を深め、情報資産の保護に努めなければならない。

3　外部委託に関する管理

(1) 情報システムの開発及び運用管理等を第三者に委託するときは、システム管理者は、当該業務を受託する第三者との間で、情報セキュリティ要件を明記した契約等を締結し、当該第三者が遵守すべき情報セキュリティに関する事項を説明しなければならない。

(2) システム管理者は、情報システムの開発及び運用管理等を第三者に委託するときは、あらかじめセキュリティ管理者と協議し、当該業務を受託する第三者との間で締結する情報セキュリティ要件を定めなければならないものとする。

第４節　技術的セキュリティ

1　情報資産の管理

(1) セキュリティ管理者は、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（以下「アクセス記録等」という。）を取得し、当該アクセス記録等の盗難、改ざん及び消去等を防止する措置を講じたうえで、一定期間保存しなければならない。また、セキュリティ管理者は、取得したアクセス記録等を分析し、不正アクセス等の有無を確認しなければならない。

(2) セキュリティ管理者は、必要があると認めるときは、担当職員に命じて情報システムへのアクセス状況の監視を行うものとする。

(3) セキュリティ管理者は、ネットワーク構成図及び情報システム仕様書等を、適切に保管しなければならない。

(4) システム管理者は、情報資産のき損等の事故に備え、定期的に情報資産のバックアップを行うものとする。

(5) セキュリティ管理者は、アクセスする権限を有しない職員等が、情報システムへアクセスすることが不可能となるように、必要な措置を講じなければならない。

(6) インターネット等を介して職員等以外の者が利用できる情報システム（以下「ホームページ等という。」においては、当該情報システムと他のネットワークおよび情報システムを物理的に分けるものとする。物理的に分けることが困難である場合においては、その他必要な情報セキュリティ対策を講じなければならない。

(7) Ｗｅｂサイトにより広域連合の情報を公開又は提供する場合には、当該サイトに係る情報システムにおいて、データ等の盗聴、改ざん若しくは消去、又は踏み台若しくはＤｏＳ攻撃等を防止する措置を講じなければならない。また、電子メールシステムを含め各情報システムにおいても、他の情報システムに対する踏み台又はＤｏＳ攻撃等を防止する措置を講じるとともに、コンピュータウィルス対策等、適切な管理及び運用を行わなければならない。

＊　踏み台

ネットワーク及び情報システムを管理するものが感知しないうちに、情報システムを乗っ取り、不正アクセス及び迷惑メール配信の中継地点等に利用すること。

＊　ＤｏＳ攻撃

大量のデータ又は不正パケットを情報システムに送り、当該情報システムによるサービスを提供することを不可能とすること、又は情報システムそのものをダウンさせること。

(8) 通信回線によりデータ等を伝送する場合は、専用通信回線の使用又は伝送するデータ等の最小限化を図るなど、適切な措置を講じなければならない。

2　職員等が情報資産を使用するときの遵守事項

(1) 業務目的以外の使用の禁止

職員等の情報資産の使用は、当該職員等が業務を遂行するうえで必要な場合に限るものと

する。職員等は、業務目的以外での情報システムへのアクセス、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。

(2) 情報資産の持ち出し又はインターネット等による情報資産の送受信の禁止

職員等は、情報資産を取り扱う場合、次の行為を行ってはならない。

ア　広域連合の事務室外へ持ち出すこと。ただし、情報資産のバックアップ等、合理的な理由があり、かつ、システム管理者の事前の許可を得た場合に限り、事務室外への持ち出しができるものとする。

イ　インターネット等による送受信を行うこと。ただし、Ｗｅｂサイトにより情報を公開又は提供しているものを除く。

ウ　職員等が個人で所有する記録媒体等を持ち込むこと。

(3) 無許可ソフトウェアのインストール等の禁止

職員等は、各自に貸与された端末機等に、セキュリティ管理者が定めていないソフトウェアのインストールを行ってはならない。特に、ネットワーク上の情報資産の盗聴ができる監視ソフトウェア、ネットワークの状態を探索できるセキュリティ関連のソフトウェア及びハッキングソフトウェアをインストールし、又は使用してはならない。ただし、業務を円滑に遂行するために必要なソフトウェアについては、合理的な理由があり、かつ、セキュリティ管理者の事前の許可を得た場合に限り、利用することができるものとする。

(4) 機器構成の変更の禁止

職員等は、各自に貸与された端末機等及びネットワークに、セキュリティ管理者が定めていない機器を増設し、又は端末機の改造を行ってはならない。特に、モデム、ルータ等の機器を増設して、インターネット等の他の環境へのネットワーク接続を行うこと、及び広域連合の事務室外からのアクセスを可能とする仕組みを構築してはならない。ただし、業務を円滑に遂行するために合理的な理由があり、かつ、セキュリティ管理者の事前の許可を得た場合に限り、端末機及びネットワークへの機器の増設又は変更を行うことができるものとする。

(5) 情報システムにおける入出力データ等の安全性の確保

ア　情報システムに入力されるデータ等は、当該データ等を入力する前に、データ等の正確性及び安全性が確保されていることを確認するための適切なチェック等を行わなければならない。

イ　情報システムから出力されるデータ等は、当該情報システムに保存されたデータ等の処理が正しく反映され、出力されることを確保しなければならない。

(6) その他の事項

職員等が使用する端末機に係るネットワークプロトコルの設定は、必要最低限の範囲のものとする。

3　アクセス制御

(1) 利用者登録

セキュリティ管理者は、職員等の採用、人事異動、退職又は派遣期間の開始もしくは終了に伴って、利用者の登録、変更または抹消を直ちに行わなければならない。特に、職員等の退職又は派遣期間の終了に伴う当該職員等の利用者ＩＤ等について、当該利用者ＩＤ等に係る記録を作成し、適切に管理を行わなければならない。

また、各課等の長は、職員等の採用、人事異動、退職又は派遣期間の開始若しくは終了があったときは、セキュリティ管理者に対して、利用者の登録、変更又は抹消の申請を速やかに行わなければならないものとする。

(2) インターネット以外のネットワークにおけるアクセス制限

セキュリティ管理者は、インターネット及び電子メールシステムを含め各情報システムにアクセスできる職員等の範囲を定めなければならない。また、当該情報システムにアクセスする権限を有しない職員等がアクセスすることが不可能となるように、各情報システム上において制限を行わなければならないものとする。

(3) 強制的な経路制御

セキュリティ管理者は、不正アクセスを防止するため、適切なネットワーク経路を制御する適切な措置を講じなければならない。

(4) 外部からのアクセス

ア　情報システム（ホームページ等及び電子メールシステムを除く。）への外部からのアクセスは、必要最小限にしなければならない。

イ　職員等が、情報システムおよび内部のネットワークへアクセスを行う場合において、当該職員等が正当な利用者としての真正性が確保できるものでなければならない。

(5) 内部ネットワーク間の接続

広域連合の内部ネットワーク間の接続については、情報資産に影響が生じないことを確認し、それぞれの情報システムの責任範囲を明確にしたうえで、接続しなければならない。ただし、内部ネットワーク間の接続をしようとするときは、あらかじめセキュリティ管理者と協議しなければならない。

(6) 外部ネットワークとの接続

ア　セキュリティ管理者は、広域連合が管理するネットワーク以外のネットワーク（以下「外部ネットワーク」という。）との接続を行う場合においては、当該外部ネットワークのネットワーク構成、機器構成、セキュリティレベル等を詳細に検討し、広域連合の情報資産に影響が生じないことを確認したうえで、統括責任者の許可を受けなければならない。

イ　外部ネットワークとの接続を行う場合は、情報セキュリティの確保できるネットワーク

構成をとらなければならない。この場合において、セキュリティ管理者は、当該外部ネットワークのかしにより、広域連合のデータ等の漏えい、破壊若しくは改ざんし、又は当該情報システムのダウン等による業務への影響が生じないような対策を講じておかなければならない。

ウ　セキュリティ管理者は、接続した外部ネットワークの情報セキュリティに問題があると認められ、広域連合の情報資産の安全性の確保に脅威が生じることが想定される場合には、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。

(7) パスワードの管理方法

ア　セキュリティ管理者は、職員等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。

イ　パスワードの長さは十分な長さとし、文字列は想像しにくいものとする。

ウ　パスワードは定期的に、若しくはアクセス回数に基づいて変更し、使用されたパスワードの再利用は行わないものとする。

4　システムの開発、導入又は保守等

(1) 情報システムの開発又は導入

ア　セキュリティ管理者は、情報システムを開発又は導入する場合において、当該情報システムの調達仕様書が、十分な情報セキュリティが確保されていることを確認しなければならない。

イ　セキュリティ管理者は、新たな機器又はソフトウェアを導入する場合において、当該機器又はソフトウェアが、十分な情報セキュリティが確保されることを確認しなければならない。

(2) 情報システムの移行時の試験等

ア　セキュリティ管理者は、新たな情報システムを導入又は既存の情報システムを更新する場合には、当該情報システムを導入又は更新する前に、既に稼動している情報システムとの連携について、十分な試験を行わなければならない。

イ　セキュリティ管理者は、既に稼動している情報システムとの連携に係る試験に使用したデータ等及びその結果を、厳重に保管しなければならない。

(3) ソフトウェアの保守及び更新

ア　セキュリティ管理者及びシステム管理者は、情報セキュリティに影響を及ぼすおそれがあると認められるソフトウェアについては、適切な保守を行わなければならない。当該ソフトウェアの保守を行った結果、情報システムに不具合があると認められるときは、直ちに当該ソフトウェアの利用停止又は他のソフトウェアと交換をする等の必要な措置をとら

なければならない

イ　セキュリティ管理者は、重要な情報システムのソフトウェアの更新等については、計画的に実施しなければならない。

ウ　セキュリティ管理者は、情報システムに修正プログラムをインストールする必要がある場合は、あらかじめ当該修正プログラムの不具合及び他の情報システムへの影響を検証してからでなければ、当該作業を行ってはならない。

(4) 業務委託事業者従業員の身分確認

セキュリティ管理者は、上記アからウをまでの作業を第三者に業務委託して行う場合において、当該作業に従事する前に、当該業務委託事業者の従業員に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であることを確認しなければならない。

(5) 管理記録

セキュリティ管理者は、情報システムに対して行った変更等の作業については、記録を作成し、適切に管理を行わなければならない。

5　機器の修理

(1) 記録媒体の含まれる機器を、第三者に業務委託して修理させ、又は廃棄する場合は、当該機器の記録媒体に記録されたデータ等を消去した状態を確認してからでなければ行ってはならない。

(2) 記録媒体の含まれる機器を、第三者に業務委託して修理させる場合において、データ等を消去することが困難であると認めるときは、当該修理を受託する事業者との間で、業務上の守秘に関する契約を締結しなければならない。

6　コンピュータウィルス対策

(1) 外部ネットワーク及び記録媒体からデータ等又はソフトウェアを取り入れるときは、あらかじめウィルスチェックを行ってからでなければ、当該作業を行ってはならない。

(2) 外部ネットワーク及び記録媒体へデータ等又はソフトウェアを送信若しくは転送するときは、ウィルスが拡散することを未然に防止する措置を行ってからでなければ、当該作業を行ってはならない。

(3) システム担当者は、次の事項を実施しなければならない。

ア　常時、ウィルスに関する情報収集に努めること。

イ　ウィルス情報について、職員等に対する注意喚起を行うこと。

ウ　ウィルスチェック用の定義ファイルを、常に最新のものに保つこと。

エ　サーバ及び端末機等において、ウィルスチェックを行うこと。

(4) 職員等は、次の事項を遵守しなければならない。

ア　差出人が不明又は不自然に添付されたファイルは、速やかに削除すること。

イ　添付ファイルのある電子メールを送受信する場合は、ウィルスチェックを行うこと。

ウ　記録媒体を使用する場合は、セキュリティ管理者が管理するものを使用するとともに、当該記録媒体の使用にあたり、あらかじめウィルスチェックを行うこと。

(5) システム担当者は、職員等から報告のあった情報、システムの障害に対する処理又は問題等を、障害記録として体系的に記録し、常に活用できるように保存しなければならない。

7　不正アクセス対策

(1) セキュリティ管理者は、不正なアクセスによる影響を防止するための必要な措置を講じなければならない。

(2) セキュリティ管理者は、Ｄｏｓ攻撃等を受けることが明確な場合には、情報システムの停止又は他のネットワークとの切断などの必要な措置を講じなければならない。

(3) Ｄｏｓ攻撃等を受け、当該攻撃が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）に抵触する可能性がある場合には、記録の保存に努めるとともに、警察等の関係機関との緊密な連携に努めなければならない。

(4) セキュリティ管理者は、職員等による不正アクセスがあったときは、当該職員等が所属する各課等の長に通知し、適切な措置を求めなければならない。

8　情報セキュリティ情報の収集

システム管理者は、情報セキュリティに関する情報を収集し、職員等及び情報システムの運用管理の業務を受託した事業者へ通知するとともに、セキュリティ対策上の措置を講じる必要が生じたときは、所要の対応を行わなければならない。

第５節　運用面のセキュリティ

1　情報システムの監視

セキュリティ管理者は、情報セキュリティに関する事案を検知するため、情報システムの監視を行わなければならない。

2　情報セキュリティ対策基準等の遵守状況の確認

セキュリティ管理者は、情報セキュリティ対策基準の遵守状況及び情報システム運用における問題の発生の有無について、常に確認を行わなければならない。なお、問題が発生した場合

には、セキュリティ管理者を経由して、速やかに統括責任者に報告するとともに必要な措置をとらなければならない。

3　運用管理における留意点

(1) システム管理者は、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参照できるように配慮しなければならない。

(2) 管理者権限

ア　共通する基幹ネットワークの管理は、セキュリティ管理者が行うものとする。

イ　セキュリティ管理者及びシステム管理者の権限を代行する者は、あらかじめ統括管理者が指名するものとする。

4　情報セキュリティ侵害の対応、対処、調査及び再発防止

(1) 情報セキュリティ侵害への対応

情報セキュリティ侵害に関する事案を認めた職員等は、速やかにセキュリティ管理者に報告しなければならない。また、セキュリティ管理者は、情報資産に重大な被害が想定される場合には、統括責任者に報告し、その指示を受けなければならない。

(2) 情報セキュリティ侵害への対処

ア　セキュリティ管理者は、次の事案が発生し、情報資産の防護のためにネットワークの切断がやむを得ないと認める場合には、ネットワークを切断することができる。

(ｱ) 異常なアクセスが継続しているとき、又は不正なアクセスがあることが判明したとき。

(ｲ) 情報システムの運用に影響を及ぼすおそれがあると認められるＤｏｓ攻撃等を感知したとき。

(ｳ) コンピュータウィルス等の不正プログラムが、ネットワーク経由で拡散するおそれがあると認められるとき。

(ｴ) 情報資産に、被害を生じることが想定されるとき。

イ　セキュリティ管理者は、次の事案が発生し、情報資産の防護のために情報システムの停止がやむを得ないと認める場合には、情報システムを停止することができる。

(ｱ) コンピュータウィルス等の不正プログラムが、情報資産に深刻な被害を及ぼしているとき、又はそのおそれがあると認められるとき。

(ｲ) 災害等により電源を供給することが危険なとき、又は困難なとき。

(ｳ) その他の障害等により情報資産に被害を生じることが想定されるとき。

ウ　セキュリティ管理者は、情報資産の被害の拡大を直ちに回避するため、個々の端末機等をネットワークから切断させる必要があると認める場合には、当該端末機等をネットワー

クから切断させることができる。

エ　セキュリティ管理者は、情報セキュリティ侵害が発生したときは、関係機関と連携し、又は協力し、早急な復旧に努めるとともに、次の措置を講じなければならない。

(ｱ) 情報セキュリティ侵害の事案に係る情報システムへのアクセス記録の保存

(ｲ) 情報セキュリティ侵害の事案に対処した経過の記録

(ｳ) 情報セキュリティ侵害の事案に係る証拠保全の実施及び再発防止の暫定措置の検討

(ｴ) 再発防止の暫定措置の実施および暫定措置を講じた後の早急な復旧

(ｵ) 復旧後、必要と認められる期間の再発の監視

(3) 情報セキュリティ侵害の調査

セキュリティ管理者は、情報セキュリティ侵害の事案の詳細な調査を行い、その調査に関する記録を作成するとともに、次の項目について、速やかに統括責任者に報告を行うものとする。

ア　情報セキュリティ侵害の事案の内容

イ　情報セキュリティ侵害の事案が発生した原因

ウ　確認した被害及び影響の範囲

(4) 情報セキュリティの再発防止の措置

ア　セキュリティ管理者は、当該情報セキュリティ侵害の事案に係るリスク分析を実施し、情報セキュリティ対策基準の改善等の措置が必要な場合は、統括責任者に報告するものとする。

イ　セキュリティ管理者は、情報セキュリティ対策の改善等に係る再発防止策を策定し、統括責任者へ報告しなければならない。統括責任者は、これらの再発防止策が有効であると認められる場合は、これを承認し、情報セキュリティ侵害の事案の概要及び当該再発防止策を職員等に周知しなければならない。

ウ　セキュリティ管理者は、当該情報セキュリティ侵害の事案に係る安全の確保について確認を行った後でなければ、情報システムのネットワークへの接続等を行ってはならない。

第６節　情報セキュリティポリシーの運用

1　情報セキュリティ実施手順の策定

(1) 策定の手続

システム管理者は、関係法令、広域連合の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に基づき、当該システム管理者が管理する情報システムごとに情報セキュリティ実施手順を定めなければならない。ただし、情報セキュリティ実施手順を定めるときは、セキュリ

ティ管理者を経由して、統括責任者と協議しなければならないものとする。

(2) 確保すべき水準

システム管理者は、情報セキュリティ実施手順を定めるにあたり、当該情報システムで取り扱う情報資産の重要性を踏まえ、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の求める水準を確保できるものとしなければならない。

2　情報セキュリティに関する違反に対する対応

システム管理者は、職員等に情報セキュリティ対策基準等に違反する行為が見られた場合には、直ちに次の措置を講じなければならない。

(1) システム管理者は、当該職員等に対して情報セキュリティに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わなければならない。

(2) 当該職員等が指導によっても情報セキュリティに違反する行為が改善されない場合は、システム管理者は、当該職員等の当該情報システム及び情報資産の使用の停止又は禁止をすることができる。

(3) 職員等に情報セキュリティに違反する行為が生じた場合、システム管理者は、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、セキュリティ管理者を経由して統括責任者に速やかに報告しなければならない。

3　評価及び見直し

(1) 自己点検

ア　セキュリティ管理者は、情報セキュリティについて、定期的に又は必要と認めるときは、自己点検を行わなければならない。

イ　情報システムの開発及び運用管理等を第三者に業務委託している場合は、当該委託業務を受託した第三者から再委託を受けた事業者も含めて、セキュリティ管理者は、情報セキュリティについて点検及び調査を行わなければならない。

ウ　セキュリティ管理者は、情報セキュリティについての自己点検の結果を、自己点検を行うたびごとに統括責任者に報告するものとする。

(2) 情報セキュリティポリシーの見直し

統括責任者は、自己点検の結果及び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の見直しを行うものとする。