徳島中央広域連合情報セキュリティポリシー

R6.6.21

第１編　情報セキュリティ基本方針

１　目的

この情報セキュリティポリシーは、徳島中央広域連合（以下、「本広域連合」という。）が保有する情報資産の機密性、完全性及び可用性を維持するため、本広域連合が実施する情報セキュリティ対策に関する基本的な方針を定めることにより、情報システムを活用した行政事務の効率化を図ることを目的とする。

２　用語の定義

（１）ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器(ハードウェア及びソフトウェア)をいう。

（２）情報システム

コンピュータ、電磁的記録媒体及びこれらを接続するネットワークで構成され、情報処理を行う仕組みをいう。

（３）情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（４）情報セキュリティポリシー

情報セキュリティに関する基本的な考え方を規定した「基本方針」と情報セキュリティを確保するために遵守すべき行為等の基準を示した「対策基準」をいう。

本広域連合における情報セキュリティポリシーは、この「第１編　情報セキュリティ基本方針」及びこの基本方針に基づき定められた「第２編　情報セキュリティ対策基準」をもって構成する。

（５）機密性

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

（６）完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（７）可用性

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

（８）ＣＩＳＯ（シーアイエスオー）

最高情報セキュリティ責任者(Chief Information Security Officer)の略称をいう。情報セキュリティ体制を強化するため、情報セキュリティを統括する機関として設置される。

（９）ＣＳＩＲＴ（シーサート）

情報セキュリティインシデント対応チーム(Computer Security Incident Response Team)の略称をいう。情報システムに対するサイバー攻撃等による情報セキュリティ上の事故(インシデント)が発生した際に、状況の把握・分析、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能とするための機能を有する体制を指す。

(10) インターネット接続系

電子メール、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、事務処理システム及びその情報システムで取り扱うデータをいう。

(11) 通信経路の分割

各システム及びインターネット接続系の各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。

(12) 実施機関

実施機関とは、連合長、消防長、議会、選挙管理委員会及び監査委員をいう。

3　適用範囲

（1）対象の範囲

本基本方針が適用される対象範囲は、本広域連合の情報資産に関する業務に携わる全ての職員等及び外部委託者等とする。

（2）情報資産の範囲

本基本方針が対象とする情報資産の範囲は次のとおりとする。

① 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

② 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 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

4　対象とする脅威

情報資産に対する脅威として、次に示す脅威を想定し、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・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（3）地震、落雷、火災等の災害によるサービス及び業務の停止等

（4）大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（5）電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

5　職員等の遵守義務

本広域連合の業務に携わる全ての職員等及び外部委託事業者は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティポリシー実施手順を遵守しなければならない。

6　情報セキュリティ対策

上記４の脅威から情報資産を保護するために、以下の情報セキュリティ対策を実施する。

（１）組織体制

本広域連合の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（２）情報資産の分類と管理

本広域連合の保有する情報資産を重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

（３）情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、必要な対策を実施する。

（４）物理的セキュリティ

サーバー、通信回線及び職員等のパソコン等の管理について、物理的な対策を実施する。

（５）人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を実施する。

（６）技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を実施する。

（７）運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、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実施する。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、障害等対応手順を策定する。

（８）外部サービスの利用

外部委託する場合には、外部委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、外部委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。約款による外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運

用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

（9）評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

7　情報セキュリティ監査及び自己点検の実施

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

8　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

9　対策基準及び実施手順の策定

（1）6、7及び8に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

（2）対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた実施手順を策定する。なお、情報セキュリティ実施手順は、公にすることにより本広域連合の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

第2編　情報セキュリティ対策基準

第1章　総則及び組織・体制

1　目的

この情報セキュリティ対策基準（以下、「対策基準」という。）は、情報セキュリティ基本方針（以下、「基本方針」という。）に基づき、本広域連合における情報資産に関する情報セキュリティ対策の基準等を定めることを目的とする。

2　組織体制

情報セキュリティの管理については、以下の体制とする。

（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。）

① ＣＩＳＯは、事務局長とする。ＣＩＳＯ（事務局長）は、本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。

② ＣＩＳＯ（事務局長）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最高情報セキュリティアドバイザーとして置き、

その業務内容を定めることができる。

③ ＣＩＳＯ（事務局長）は、情報セキュリティインシデントに対処するための体制(ＣＳＩＲＴ：Computer Security Incident Response Team、以下「ＣＳＩＲＴ」という。)を整備し、役割を明確化する。

④ ＣＩＳＯ（事務局長）は、情報セキュリティポリシーに定められた自らの担務を、情報セキュリティポリシーに定める責任者に担わせることができる。

（２）副最高情報セキュリティ責任者

ＣＩＳＯ（事務局長）を補助し、本広域連合における情報セキュリティに関する事務を整理し、ＣＩＳＯの命を受けて本広域連合の情報セキュリティに関する事務を統括する副最高情報セキュリティ責任者（以下、「副ＣＩＳＯ」という。）１人を必要に応じて置く。

（３）情報セキュリティ責任者

① 情報セキュリティ責任者は、事務局次長・消防次長とする。

② ＣＩＳＯ（事務局長）及び副ＣＩＳＯ（消防長）を補佐する。

③ 事務局次長が空席の場合は事務局総務課長を充てる。

④ 所管する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。

⑤ 所管する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。

⑥ 所管する情報セキュリティ管理者、情報システム管理者、ネットワーク管理者及び情報システム担当者（事務局総務課担当者）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。

⑦ 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（事務局長）の指示に従い、ＣＩＳＯ（事務局長）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。

⑧ 所管する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。

⑨ 緊急時等の円滑な情報共有を図るため、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。

⑩ 緊急時にはＣＩＳＯ（事務局長）に早急に報告を行うとともに回復のための対策を実施しなければならない。

（４）情報セキュリティ管理者

① 情報セキュリティ管理者は、事務局総務課長、消防本部総務課長、消防課長、通信指令室長及び各消防署長（以下、「所属長」という。）とする。

② 所管組織の情報セキュリティ対策に関する権限と責任を有するものとする。

③ 所管組織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（事務局次長・消防次長）へ速やかに報告を行い、指示を仰がなければならない。

（5）情報システム管理者

① 情報システム管理者は、事務局総務課長及び消防本部総務課長とする。

② 所管組織の情報システムの運用、管理に関する権限と責任を有するものとする。

③ 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ものとする。

④ 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ものとする。

⑤ 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）ネットワーク管理者

① ネットワーク管理者は、事務局総務課長とする。

② 情報セキュリティ責任者（事務局次長・消防次長）を補佐し、本広域連合の共通的なネットワーク、情報システム関係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。

③ 情報セキュリティ責任者（事務局次長・消防次長）が、その所管する部局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う場合、ネットワーク運営管理の見地から助言、協力しなければならない。

④ 次に掲げる事項を行わなければならない。

（ア）ネットワーク及び情報システムの適正かつ効率的な運用を図るため、ネットワーク接続の正常な維持管理に関すること。

（イ）サーバー室、通信機械室等の管理の適正化に関すること。

（ウ）端末機等の適正な管理及び効率的な運用に関すること。

（エ）ネットワーク及び情報システムに係わる情報セキュリティ実施手順の作成、維持及び管理に関すること。

（7）情報システム担当者

① 情報システム担当者は、情報システム管理者（事務局総務課長・消防本部総務課長）が所管するシステムの担当者とする。

② 情報システム管理者（事務局総務課長・消防本部総務課長）の指示に従い、情報システムの設定変更、運用、更新等の作業を行う。

（8）情報セキュリティ委員会

① 本広域連合における情報セキュリティに関する最高意思決定は、徳島中央広域連合セキュリティ委員会（以下、「委員会」という。）が行う。

② 委員会は次の事項を審議する。

（ア）情報セキュリティポリシー及び基本方針の運用及び見直しに関する事項

（イ）情報セキュリティに関する事案の調査に関する事項
（ウ）情報セキュリティ監査の実施手順等に関する事項
（エ）その他情報セキュリティに係る重要事項に関する事項

③ 委員会は、
・最高情報セキュリティ責任者（事務局長）
・副最高情報セキュリティ責任者（消防長）
・情報セキュリティ責任者（事務局次長・消防次長）
・情報システム管理者（事務局総務課長・消防本部総務課長）
・ネットワーク管理者（事務局総務課長）
をもって構成する。

④ 委員会の長は、最高情報セキュリティ責任者とする。

⑤ 委員会の事務は、事務局総務課が行う。

⑥ 委員会は必要に応じて、情報セキュリティ対策の監査作業を行う「情報セキュリティ監査チーム」等の「専門チーム」を編成することができる。

3　兼務の禁止

（1）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。

4　情報セキュリティに関する統一的な窓口の設置

（1）ＣＩＳＯ（事務局長）は、情報セキュリティインシデントの統一的な窓口（以下「ＣＳＩＲＴ(シーサート)」という。）の機能を有する組織を整備し、情報セキュリティインシデントについて課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する。

（2）ＣＩＳＯ（事務局長）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、その内容を関係課室署等に提供する。

（3）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。

（4）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、外部の事業者等との情報共有を行う。

第２章　情報資産の管理

第１節　情報資産の分類

1　情報資産の分類

本広域連合における情報資産は、重要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。

① 個人情報及びセキュリティ侵害が住民の生命、財産等へ重大な影響を及ぼす情報（以下、「重要性Ⅰ」という。）

② 公開することを予定していない情報及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報(以下「重要性Ⅱ」という。）

③ 外部に公開する情報のうち、セキュリティ侵害が行政事務の執行等に軽微な影響を及ぼす情報(以下、「重要性Ⅲ」という。）

④ 上記以外の情報(以下、「重要性Ⅳ」という。）

第２節　情報資産の管理

1　情報の作成

（１）職員等は、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、情報の作成時に情報資産の分類に基づき、必要に応じて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。

2　情報資産の入手

（１）本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）本広域連合外の者が作成した情報資産を入手した者は、情報資産の分類に基づき、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、情報セキュリティ管理者に判断を仰がなければならない。

3　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）情報資産を利用する者は、情報資産の分類に応じて適正な取扱いをしなければならない。

（３）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。

4　管理責任

（１）情報セキュリティ管理者（所属長）は、その所管する情報資産について管理責任を有する。

（２）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情報資産の分類に基づき管理しなければならない。

5　情報資産の分類の表示

（１）職員等は、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。

6　情報資産の保管

（1）情報セキュリティ管理者（所属長）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。

（2）情報セキュリティ管理者（所属長）は、情報資産を記録した電磁的記録媒体を長期間保管する場合は、書込禁止の措置を実施しなければならない。

（3）情報セキュリティ管理者（所属長）は、重要性Ⅱ以上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錠可能な場所等に保管しなければならない。

7　情報の送信

電子メール等により重要性分類Ⅱ以上の情報を送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。

8　情報資産の運搬

（1）車両等により重要性分類Ⅱ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、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）重要性分類Ⅱ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（所属長）の許可を得なければならない。

9　情報資産の提供・公表

（1）重要性Ⅱ以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスードの設定を行わなければならない。

（2）重要性Ⅱ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（所属長）に許可を得なければならない。情報セキュリティ管理者（所属長）は、許可をする前に情報セキュリティ責任者（事務局次長・消防次長）の承認を得なければならない。

（3）情報セキュリティ管理者（所属長）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。

１０　情報資産の廃棄

（1）重要性Ⅱ以上の情報資産を廃棄する者は、情報を記録している電磁的記録媒体が不要になった場合、電磁的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）情報資産の廃棄を行う者は、情報セキュリティ管理者（所属長）の許可を得なけ

ればならない。

１１　情報システム全体の強靭性の向上

（１）クラウドサービスを利用する際にマネージドサービスやＯＳの修正プログラム等の適用、ソフトウェアのアクティベーション等で、限定的にインターネットと接続が必要となる場合は、リスクアセスメントを実施し、リスクの明確化と定期的な監査を行わなければならない。

（２）インターネット接続系

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等の情報セキュリティ対策を実施しなければならない。

第３章　物理的セキュリティ対策

第１節　サーバー等の管理

１　機器の取付け

ネットワーク管理者（事務局総務課長）は、サーバー等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じなければならない。

２　機器の電源

（１）ネットワーク管理者（事務局総務課長）は、施設管理部門と連携し、サーバー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。

（２）ネットワーク管理者（事務局総務課長）は、施設管理部門と連携し、落雷等による過電流に対して、サーバー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。

３　通信ケーブル等の配線

（１）ネットワーク管理者（事務局総務課長）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）ネットワーク管理者（事務局総務課長）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）ネットワーク管理者（事務局総務課長）及び施設管理部門は、ネットワーク接続口（ハブのポート等）を適切に管理しなければならない。

（４）ネットワーク管理者（事務局総務課長）は、自ら又は情報システム担当者（事務

局総務課長及び消防本部総務課長が所管するシステムの担当者）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又は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。

4　機器の定期保守及び修理

（1）ネットワーク管理者（事務局総務課長）は、重要性Ⅱ以上のサーバー等の機器の定期保守を実施しなければならない。

（2）情報セキュリティ管理者（所属長）は、電磁的記録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なければならない。

なお、内容を消去できない場合、情報システム管理者（事務局総務課長・消防本部総務課長）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ほか、秘密保持体制の確認等を行わなければならない。

5　本広域連合外への機器の設置

ネットワーク管理者（事務局総務課長）は、本広域連合外にサーバー等の機器を設置する場合、ＣＩＳＯ（事務局長）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　機器の廃棄等

情報セキュリティ管理者（所属長）は、機器を廃棄・リース終了返却等をする場合、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実施しなければならない。

第２節　管理区域の管理

1　管理区域の構造等

（1）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区域や電磁的記憶媒体の保管庫をいう。

（2）情報セキュリティ責任者（事務局次長・消防次長）は、管理区域の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等の対策を実施しなければならない。

（3）情報セキュリティ責任者（事務局次長・消防次長）は、管理区域に配置する消火薬剤や消防用設備等が、機器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。

2　機器等の搬入出

（1）情報セキュリティ責任者（事務局次長・消防次長）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した業者に確認を行わせなければならない。

（2）情報セキュリティ責任者（事務局次長・消防次長）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

1　通信回線の管理

（1）情報セキュリティ責任者（事務局次長・消防次長）は、本広域連合の通信回線及び通信回線装置を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する文書を適切に保管しなければならない。

（2）情報セキュリティ責任者（事務局次長・消防次長）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。

（3）情報セキュリティ責任者（事務局次長・消防次長）は、重要性分類Ⅱ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。

（4）情報セキュリティ責任者（事務局次長・消防次長）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。

（5）情報セキュリティ責任者（事務局次長・消防次長）は、重要性分類Ⅱ以上の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、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。

第４節　職員等の利用する電磁的記録媒体等の管理

1　電磁的記録媒体等の管理

（1）情報システム管理者（事務局総務課長・消防本部総務課長）は、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、情報セキュリティ責任者（事務局次長・消防次長）へ報告しなければならない。

（2）情報セキュリティ責任者（事務局次長・消防次長）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４章　人的セキュリティ対策

第１節　職員等の遵守事項

1　情報セキュリティポリシー等の遵守

（1）職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。

（2）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がある場合は、速やかに情報セキュリティ管理者（所属長）に相談し、指示を仰がなければならない。

2　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。

3　外部における情報処理作業

（1）ＣＩＳＯ（事務局長）は、重要性分類Ⅱ以上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）職員等は、本広域連合のパソコン、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（所属長）の許可を得なければならない。

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

4　支給以外のパソコン等の業務利用

（1）職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を業務に利用してはならない。ただし、やむを得ず業務上必要な場合は、情報セキュリティ管理者（所属長）の許可を得て利用することができる。

（2）職員等は、情報セキュリティ管理者（所属長）の許可を得て、支給以外のパソコン及び電磁的記媒体等を用いる場合は、外部で情報処理を行う際に安全管理措置を遵守しなければならない。

5　持ち出し及び持ち込みの記録

情報セキュリティ管理者（所属長）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。

6　セキュリティ設定変更の禁止

職員等は、パソコン、モバイル端末及び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責任者（事務局次長・消防次長）の許可なく変更してはならない。

7　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個人情報等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（所属長）の許可なく情報が閲覧されることがないように、長時間離席時にはパソコンをスリープモードにして、再起動時にパスワード入力が必要な状態にすることや電子的記録媒体、個人情報等が記録された文書等が容易に閲覧されないよう扉及び鍵つきの書類棚への保管を行う等、適切な措置を講じなければならない。

8　異動、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。

9　インターネットの利用制限

職員等は、インターネットを利用する場合、次に掲げる行為をしてはならない。

① 公序良俗に反する行為
② 事実に反する情報を提供する行為
③ 個人的な行為及び営利を目的とした行為
④ 他人を詐称する行為
⑤ 他人の財産又はプライバシーを侵害する行為
⑥ 他人の著作権、その他の権利を侵害する行為
⑦ 他人を誹謗・中傷する行為
⑧ ネットワークの正常な運用に支障を及ぼす行為
⑨ システムの不正利用又はそれを助ける行為
⑩ 権限なくプログラムやデータ等の改変又は破壊をする行為
⑪ 政治活動又は宗教活動を目的とする行為
⑫ インターネットの円滑な運用を妨げる行為
⑬ インターネット上の各種有料サイトを利用する行為
⑭ 法令等に違反する行為又は違反のおそれがある行為
⑮ その他社会慣行に反する行為

１０　会計年度任用職員への対応

（１）情報セキュリティ管理者（所属長）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。

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

（３）情報セキュリティ管理者（所属長）は、会計年度任用職員にパソコン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。

１１　情報セキュリティポリシー等の閲覧

情報セキュリティ責任者（事務局次長・消防次長）は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

１２　外部委託事業者に対する説明

情報セキュリティ管理者（所属長）は、ネットワーク及び情報システムの導入・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外部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。

第２節　研修・訓練

１　情報セキュリティに関する研修・訓練

ＣＩＳＯ（事務局長）は、定期的に情報セキュリティに関する研修・訓練を実施し

なければならない。

2　研修計画の策定及び実施

（1）ＣＩＳＯ（事務局長）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必要に応じて行い、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）研修は、情報セキュリティ責任者（事務局次長・消防次長）、情報セキュリティ管理者（所属長）、情報システム担当者及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

3　緊急時避難訓練

（1）ＣＩＳＯ（事務局長）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。

（2）訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制・範囲等を定め、効果的に実施できるようにしなければならない。

4　研修・訓練への参加

全ての職員等は、定められた研修・訓練に参加しなければならない。

第３節　情報セキュリティインシデントの報告

1　本広域連合内からの報告

（1）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（所属長）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（所属長）は、速やかに統括情報セキュリティ責任者（事務局次長・消防次長）に報告しなければならない。

（3）情報セキュリティ管理者（事務局次長・消防次長）は、報告のあった情報セキュリティインシデントについて、必要に応じてＣＩＳＯ（事務局長）に報告しなければならない。

2　住民等外部からの報告

（1）職員等は、本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情報セキュリティインシデントについて、住民等外部から報告を受けた場合、情報セキュリティ管理者（所属長）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（所属長）は、速やかに情報セキュリティ責任者（事務局次長・消防次長）に報告しなければならない。

（3）情報セキュリティ責任者（事務局次長・消防次長）は、当該情報セキュリティインシデントについて、必要に応じてＣＩＳＯ（事務局長）に報告しなければならない。

3　原因の究明・記録、再発防止等

（1）情報セキュリティ責任者（事務局次長・消防次長）は、情報セキュリティインシデントを引き起こした部署の情報セキュリティ管理者（各課等の長）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。

（2）情報セキュリティ責任者（事務局次長・消防次長）は、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（事務局長）に報告しなければならない。

（3）ＣＩＳＯ（事務局長）は、情報セキュリティ責任者（事務局次長・消防次長）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。

第４節　ＩＤ及びパスワード等の管理

1　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。

① 自己が利用しているＩＤは、他人に利用させてはならない。

② 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。

2　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。

① 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。

② 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。

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（所属長）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等は、同一のパスワードをシステム間で用いてはならない。

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 パソコン等の端末にパスワードを記憶させてはならない。

⑨ 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）。

第５章　技術的セキュリティ対策

第１節　コンピュータ及びネットワークの管理

1　文書サーバーの設定等

（1）ネットワーク管理者（事務局総務課長）は、職員等が使用できる文書サーバーの容量を設定し、必要に応じて職員等に周知しなければならない。

（2）ネットワーク管理者（事務局総務課長）は、必要に応じて文書サーバーを課室署等の単位で構成しなければならない。

2　バックアップの実施

ネットワーク管理者（事務局総務課長）は、ファイルサーバー等に記録された情報について、サーバー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。

3　システム管理記録及び作業の確認

（1）情報システム管理者（事務局総務課長・消防本部総務課長）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）情報システム管理者（事務局総務課長・消防本部総務課長）は、所管するシステムにおいて、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。

（3）情報システム管理者（事務局総務課長・消防本部総務課長）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名以上で作業をし、互いにその作業を確認しなければならない。

4　情報システム仕様書等の管理

情報システム管理者（事務局総務課長・消防本部総務課長）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、適正に管理しなければならない。

5　ログの取得等

（1）情報システム管理者（事務局総務課長・消防本部総務課長）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。

（2）情報システム管理者（事務局総務課長・消防本部総務課長）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。

（3）情報システム管理者（事務局総務課長・消防本部総務課長）は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作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。

6　障害記録

情報システム管理者（事務局総務課長・消防本部総務課長）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。

7　ネットワークの接続制御、経路制御等

（1）ネットワーク管理者（事務局総務課長）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。

（2）ネットワーク管理者（事務局総務課長）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　外部ネットワークとの接続制限等

（1）情報システム管理者（事務局総務課長・消防本部総務課長）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、情報セキュリティ責任者（事務局次長・消防次長）の許可を得なければならない。

（2）情報システム管理者（事務局総務課長・消防本部総務課長）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、本広域連合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。

（3）情報システム管理者（事務局総務課長・消防本部総務課長）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。

（4）ネットワーク管理者（事務局総務課長）は、ウェブサーバー等をインターネットに公開する場合、本広域連合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。

（5）情報システム管理者（事務局総務課長・消防本部総務課長）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、情報セキュリティ責任者（事務局次長・消防次長）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。

9　複合機のセキュリティ管理

（1）情報セキュリティ責任者（事務局次長・消防次長）は、複合機が備える機能について適切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実施しなければならない。

（2）情報セキュリティ責任者（事務局次長・消防次長）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。

１０　電子メールのセキュリティ管理

（1）ネットワーク管理者（事務局総務課長）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（電子メールの中断処理）が行われることを不可能とするよう、電子メールサーバーの設定を行わなければならない。

（2）ネットワーク管理者（事務局総務課長）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、メールサーバーの運用を停止しなければならない。

（3）ネットワーク管理者（事務局総務課長）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）ネットワーク管理者（事務局総務課長）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。

１１　電子メールの利用制限

（１）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。

（２）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。

（３）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。

（４）職員等は、電子メールを誤送信した場合、情報セキュリティ管理者（各課等の長）に報告しなければならない。

（５）職員等は、業務においてウェブで利用できる電子メール、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。

（６）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、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

１２　無許可ソフトウェアの導入等の禁止

（１）職員等は、パソコン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。

（２）職員等は、業務上の必要がある場合は、情報セキュリティ責任者（事務局次長・消防次長）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（所属長）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。

（３）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。

１３　機器構成の変更の制限

職員等は、パソコンに対し機器の改造及び増設・交換を行ってはならない。ただし、やむを得ず業務上、パソコン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、情報セキュリティ責任者（事務局次長・消防次長）の許可を得なければならない。

１４　無許可でのネットワーク接続の禁止

職員等は、情報セキュリティ責任者（事務局次長・消防次長）の許可なくパソコンをネットワークに接続してはならない。

１５　業務以外の目的でのウェブ閲覧の禁止

（１）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。

（２）情報セキュリティ責任者（事務局次長・消防次長）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（所属長）に通知し適正な措置を求めなければならない。

第２節　アクセス等制御等

1　アクセス制御

情報システム管理者（事務局総務課長・消防本部総務課長）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。

2　利用者ＩＤの取扱い

（1）情報セキュリティ責任者（事務局次長・消防次長）は、利用者の登録、変更、抹消等の情報管理、職員等の異動、退職者に伴う利用者ＩＤの取扱い等の方法を定めなければならない。

（2）職員等は、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ネットワーク管理者（事務局総務課長）に通知しなければならない。

（3）情報システム管理者（事務局総務課長・消防本部総務課長）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。

3　特権を付与されたID の管理等

（1）情報セキュリティ責任者（事務局次長・消防次長）及び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）情報セキュリティ責任者（事務局次長・消防次長）の特権を代行する者は、情報セキュリティ責任者（事務局次長・消防次長）が指名し、ＣＩＳＯ（事務局長）が認めた者でなければならない。

（3）ＣＩＳＯ（事務局長）は、代行者を認めた場合、速やかに情報セキュリティ責任者（事務局次長・消防次長）に通知しなければならない。

（4）情報セキュリティ責任者（事務局次長・消防次長）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）情報セキュリティ責任者（事務局次長・消防次長）は、特権を付与されたＩＤ及びパスワードについて、定期変更及び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。

（6）情報セキュリティ責任者（事務局次長・消防次長）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。

3　パスワードに関する情報の管理

情報セキュリティ責任者（事務局次長・消防次長）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。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。

4　職員等による外部からのアクセス等の制限

（1）職員等が外部から内部ネットワーク又は情報システムにアクセスする場合は、情報セキュリティ責任者（事務局次長・消防次長）及び当該情報システムを管理する

情報セキュリティ管理者（各課等の長）の許可を得なければならない。

（２）情報セキュリティ責任者（事務局次長・消防次長）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が必要な場合、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）情報セキュリティ責任者（事務局次長・消防次長）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）情報セキュリティ責任者（事務局次長・消防次長）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施さなければならない。

（５）情報セキュリティ責任者（事務局次長・消防次長）及び情報セキュリティ管理者（所属長）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。

（６）職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を本広域連合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。

（７）職員等は、公衆通信回線(公衆無線 LAN 等)の外部通信回線を本広域連合内のネットワークに接続してはならない。

5　特権による接続時間の制限

特権を付与されたＩＤを利用する者は、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　システム導入、機器・ソフトウェア調達、保守等

1　情報システム、機器・ソフトウェア等の調達

（１）情報システム管理者（事務局総務課長・消防本部総務課長）は、システム導入、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。

（２）情報システム管理者（事務局総務課長・消防本部総務課長）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。

（３）情報システム管理者（事務局総務課長・消防本部総務課長）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。

（４）情報システム管理者（事務局総務課長・消防本部総務課長）は、システムの旧環境から新環境への移行の際、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。

（５）情報システム管理者（事務局総務課長・消防本部総務課長）は、導入するシステ

ム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。

2　システム導入のテスト

（1）情報システム管理者（事務局総務課長・消防本部総務課長）は、新たにシステムを導入する場合、既に稼働している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）情報システム管理者（事務局総務課長・消防本部総務課長）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実施しなければならない。

（3）情報システム管理者（事務局総務課長・消防本部総務課長）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。

3　システム導入・保守に関連する資料等の整備・保管

（1）情報システム管理者（事務局総務課長・消防本部総務課長）は、システム導入・保守に関連する資料及びシステム関連文書を適切に整備・保管しなければならない。

（2）情報システム管理者（事務局総務課長・消防本部総務課長）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（事務局総務課長・消防本部総務課長）は、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。

4　情報システムにおける入出力データの正確性の確保

（1）情報システム管理者（事務局総務課長・消防本部総務課長）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（事務局総務課長・消防本部総務課長）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（事務局総務課長・消防本部総務課長）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。

5　情報システムの変更管理

情報システム管理者（事務局総務課長・消防本部総務課長）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。

6　開発・保守用のソフトウェアの更新等

情報システム管理者（事務局総務課長・消防本部総務課長）は、開発・保守用のソフトウェ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。

7　システム更新又は統合時の検証等

情報システム管理者（事務局総務課長・消防本部総務課長）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。

第４節　不正プログラム対策

1　情報セキュリティ責任者（事務局次長・消防次長）の措置事項

情報セキュリティ責任者（事務局次長・消防次長）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する。

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する。

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、必要に応じ職員等に対して注意喚起する。

④ 所掌するサーバー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る。

⑤ 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つ。

⑥ 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ない。

2　情報システム管理者（事務局総務課長・消防本部総務課長）の措置事項

情報システム管理者（事務局総務課長・消防本部総務課長）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 その所掌するサーバー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ること。

② 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つこと。

③ 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、本広域連合が管理している媒体以外を職員等に利用させないこと。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すること。

3　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。

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こと。

② 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うこと。

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、速やかに削除すること。

④ 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すること。

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ェアでチェックを行うこと。

⑥ 情報セキュリティ責任者（事務局次長・消防次長）が提供するウイルス情報を、常に確認すること。

⑦ パソコン等が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、端末のＬＡＮケーブルの即時取り外しを行うこと。

4　専門家の支援体制

情報セキュリティ責任者（事務局次長・消防次長）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、必要に応じて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。

第５節　不正アクセス対策

1　情報セキュリティ責任者（事務局次長・消防次長）の措置事項

情報セキュリティ責任者（事務局次長・消防次長）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すること。

② 不要なサービスについて、機能を削除又は停止すること。

③ 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、情報セキュリティ責任者（事務局次長・消防次長）へ通報するよう設定すること。

④ 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すること。

2　攻撃への対処

情報セキュリティ責任者（事務局次長・消防次長）は、サーバー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、システムの停止を含む必要な措置を実施しなければならない。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。

3　記録の保存

情報セキュリティ責任者（事務局次長・消防次長）は、サーバー等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

4　内部からの攻撃

情報セキュリティ責任者（事務局次長・消防次長）及び情報セキュリティ管理者（所属長）は、職員等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本広域連合のサーバー等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

5　職員等による不正アクセス

情報セキュリティ管理者（所属長）は、職員等による不正アクセスを発見した場合は、情報セキュリティ責任者（事務局次長・消防次長）に通知し、適正な処置を求めなければならない。

6　サービス不能攻撃

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

7　標的型攻撃

情報セキュリティ責任者（事務局次長・消防次長）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実施しなければならない。

第６節　セキュリティ情報の収集

1　セキュリティホールに関する情報

情報セキュリティ責任者（事務局次長・消防次長）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。

2　不正プログラム等に関する情報

情報セキュリティ責任者（事務局次長・消防次長）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。

3　情報セキュリティに関する情報

情報セキュリティ責任者（事務局次長・消防次長）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実施しなければならない。

第６章　運用

第１節　　情報システムの監視

1　情報システムの監視

（1）情報セキュリティ責任者（事務局次長・消防次長）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）情報セキュリティ責任者（事務局次長・消防次長）は、重要なログ等を取得するサーバーの正確な時刻設定及びサーバー間の時刻同期ができる環境設定を構築しなければならない。

（3）情報セキュリティ責任者（事務局次長・消防次長）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

1　遵守状況の確認及び対処

（1）情報セキュリティ管理者（各課等の長）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（事務局長）及び情報セキュリティ責任者（事務局次長・消防次長）に報告しなければならない。

（2）ＣＩＳＯ（事務局長）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。

（3）情報セキュリティ責任者（事務局次長・消防次長）は、ネットワーク及びサーバー等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

2　パソコン等の利用状況調査

ＣＩＳＯ（事務局長）及びＣＩＳＯ（事務局長）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。

3　職員等の報告義務

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、直ちに情報セキュリティ責任者（事務局次長・消防次長）及び情報セキュリティ管理者（所属長）に報告を行わなければならない。

第３節　侵害時の対応等

1　緊急時の対応

ＣＩＳＯ（事務局長）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しなければならない。

第４節　例外措置

1　例外措置の許可

情報セキュリティ管理者（所属長）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、業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（事務局長）の許可を得て、例外措置をとることができる。

2　緊急時の例外措置

情報セキュリティ管理者（所属長）は、業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（事務局長）に報告しなければならない。

3　例外措置の申請書の管理

ＣＩＳＯ（事務局長）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。

第５節　法令遵守

1　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。

① 地方公務員法(昭和 25 年法律第 261 号)
② 著作権法(昭和 45 年法律第 48 号)
③ 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)
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 徳島中央広域連合個人情報保護法施行条例(令和 5 年条例第 1 号)

第６節　懲戒処分等

1　懲戒処分

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法(昭和 25 年法律第 261 号)による懲戒処分の対象とする。

2　違反時の対応

職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

① 情報セキュリティ責任者（事務局次長・消防次長）が違反を確認した場合は、当該職員等が所属する情報セキュリティ管理者（所属長）に通知し、適正な措置を求める。
② 情報セキュリティ管理者（所属長）の指導によっても改善されない場合、情報セキュリティ責任者（事務局次長・消防次長）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、

情報セキュリティ責任者（事務局次長・消防次長）は、速やかに職員等の権利を停止あるいは剥奪した旨をＣＩＳＯ（事務局長）及び当該職員等が所属する情報セキュリティ管理者（所属長）に通知する。

第７章　外部サービスの利用

第１節　外部委託

1　外部委託事業者の選定基準

（１）情報セキュリティ管理者（所属長）は、外部委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

（２）情報システム管理者（事務局総務課長・消防本部総務課長）は、クラウドサービスを利用する場合は情報の機密性に応じた情報セキュリティレベルが確保されているサービスを利用しなければならない。

2　契約項目

情報システムの運用、保守等を外部委託する場合には、外部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 委託事業者の責任者、委託内容、作業者及び作業場所の特定
③ 提供されるサービスレベルの保証
④ 外部委託事業者にアクセスを許可する情報の種類と範囲及びアクセス方法
⑤ 外部委託事業者の従業員に対する教育の実施
⑥ 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
⑦ 業務上知り得た情報の守秘義務
⑧ 再委託に関する制限事項の遵守
⑨ 委託業務終了時の情報資産の返還・廃棄等
⑩ 委託業務の定期報告及び緊急時報告義務
⑪ 本広域連合による監査及び検査
⑫ 本広域連合による情報セキュリティインシデント発生時の公表
⑬ 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)

3　確認・措置等

情報セキュリティ管理者（各課等の長）は、外部委託事業者において必要なセキュリティ対策が確保されていることを確認し、委託にあたっては必要に応じて「２契約項目」に基づき措置を実施しなければならない。また、その内容を情報セキュリティ責任者（事務局次長・消防次長）に報告をするとともに、その重要度に応じてＣＩＳＯ（事務局長）に報告しなければならない。

第２節　約款による外部サービスの利用

1　約款による外部サービスの利用に係る規定の整備

情報セキュリティ責任者（事務局次長・消防次長）は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、重要性分類Ⅱ以上の情報が取り扱われないように規定しなければならない。

① 約款によるサービスを利用してよい範囲

② 業務により利用する約款による外部サービス

③ 利用手続及び運用手順

2　約款による外部サービスの利用における対策の実施

職員等は、利用するサービスの約款、その他インターネット上で提供されているフリーメールやファイルストレージサービス等の約款による外部サービス等の約款による外部サービスは、情報セキュリティ責任者（事務局次長・消防次長）が使用を認めたものを除き、業務に使用してはならない。

第３節　ソーシャルメディアサービスの利用

1　ソーシャルメディアサービスの利用

情報セキュリティ責任者（事務局次長・消防次長）は、本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、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。

① 本広域連合のアカウントによる情報発信が、実際の本広域連合のものであることを明らかにするために、本広域連合の自己管理ウェブ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等を適正に管理するなどの方法で、不正アクセス対策を行うこと。

2　重要性分類Ⅱ以上の情報発信について

重要性分類Ⅱ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。

3　ソーシャルメディアサービスの責任者について

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。

第８章　評価・見直し

第１節　監査

1　監査の実施方法

ＣＩＳＯ（事務局長）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、必要に応じて監査を行わせなければならない。

2　監査を行う者の要件

（１）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。

３　監査実施計画の立案及び実施への協力

（１）情報セキュリティ監査統括責任者は、監査を行うにあたって、監査実施計画を立案し、ＣＩＳＯ（事務局長）の承認を得なければならない。

（２）被監査課室署は、監査の実施に協力しなければならない。

４　外部委託事業者に対する監査

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。

５　監査報告

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及び委員会に報告する。

６　保管

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

７　監査結果への対応

ＣＩＳＯ（事務局長）及び委員会は、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（所属長）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（所属長）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。

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（事務局長）及び委員会は、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。

第２節　自己点検

１　自己点検の実施方法

（１）ネットワーク管理者（事務局総務課長）及び情報システム管理者（事務局総務課長・消防本部総務課長）は、所管するネットワーク及び情報システムについて、必要に応じて自己点検を実施しなければならない。

（２）情報セキュリティ責任者（事務局次長・消防次長）は、情報セキュリティ管理者（所属長）と連携し、所管組織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、必要に応じて自己点検を行わなければならない。

2　自己点検報告

情報セキュリティ責任者（事務局次長・消防次長）及び、情報セキュリティ管理者（所属長）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、委員会に報告しなければならない。

3　自己点検結果の活用

（1）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。

（2）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。

第3節　情報セキュリティポリシー及び関係規程等の見直し

1　情報セキュリティポリシー及び関係規程等の見直し

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ときは、改善を行うものとする。