大分県後期高齢者医療広域連合
情報セキュリティポリシー

平成１９年９月１日制定

(平成２８年１月１日改定)

＜目　次＞

第１章　大分県後期高齢者医療広域連合情報セキュリティポリシーの目的及び構成

１　目的

大分県後期高齢者医療広域連合(以下「広域連合」という。)が取り扱う情報には、個人情報や事業運営上重要な情報など、外部に漏えい等した場合に極めて重大な結果を招く情報が多数含まれている。

したがって、これらの情報及び情報を取り扱う情報システムを様々な脅威から防御する必要がある。そのため、広域連合の情報資産の機密性、完全性及び可用性を維持するための対策（以下「情報セキュリティ対策」という。)を整備するために、大分県後期高齢者医療広域連合情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）を定めることとする。

２　構成

情報セキュリティポリシーは、広域連合が保有する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものである。

情報セキュリティポリシーは、広域連合が保有する情報資産を取り扱うすべての職員に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかし一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化に対し柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーは、一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に対応する部分としての「情報セキュリティ対策基準」から構成する。

情報セキュリティポリシーの構成

文　書　名		内　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための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

第２章　情報セキュリティ基本方針

１　趣旨

この情報セキュリティ基本方針は、広域連合の情報セキュリティ対策の基本的な方針を定めるものとする。

２　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、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

（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

本基本方針及び情報セキュリティ対策基準をいう。

（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。

３　対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（１）不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（２）情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・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

４　適用範囲

（１）実施機関の範囲

本基本方針が適用される実施機関は、広域連合長、選挙管理委員会、監査委員及び議会とする。

（２）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

ア　ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

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

ウ　情報システムの仕様書及びネットワーク図等のシステム関連文書

５　職員等の遵守義務

職員、非常勤職員及び臨時職員（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

６　情報セキュリティ対策

上記３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講じる。

（１）組織体制

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組織体制を確立する。

（２）情報資産の分類と管理

広域連合の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

（３）物理的セキュリティ

サーバ等、情報システム室等、通信回線等及び職員等のパソコン等の管理について、物理的な対策を講じる。

（４）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講じる。

（５）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講じる。

（６）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講じるものとする。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切に対応するため、緊急時対応計画を策定する。

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　情報セキュリティ対策基準の策定

上記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。

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するものとする。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。

11　市町村等の対応

広域連合を構成する市町村等において、後期高齢者医療の事務を行う場合、各自で定めている情報セキュリティポリシーに基づき、適切に対応するものとする。

第３章　情報セキュリティ対策基準

１　趣旨

情報セキュリティ基本方針において規定する情報セキュリティ対策を実行に移すため、広域連合の情報セキュリティ対策の基準を定めるものとする。

２　対象範囲

（１）実施機関の範囲

本対策基準が適用される実施機関は、広域連合長、選挙管理委員会、監査委員及び議会とする。

（２）情報資産の範囲

本対策基準が対象とする情報資産は、次のとおりとする。

ア　ネットワーク、情報システム、これらに関する設備、電磁的記録媒体

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

ウ　情報システムの仕様書及びネットワーク図等のシステム関連文書

３　組織体制

（１）　最高データ取扱責任者

ア　広域連合事務局長を、最高データ取扱責任者とする。最高データ取扱責任者は、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　最高データ取扱責任者は、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ものとする。

（２）　データ保護管理者

ア　広域連合事務局次長を、最高データ取扱責任者直属のデータ保護管理者とする。データ保護管理者は最高データ取扱責任者を補佐しなければならない。

イ　データ保護管理者は、広域連合の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

ウ　データ保護管理者は、広域連合の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

エ　データ保護管理者は、データ取扱責任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。

オ　データ保護管理者は、広域連合の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、最高データ取扱責任者の指示に従い、最高データ取扱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。

カ　データ保護管理者は、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。

キ　データ保護管理者は、緊急時等の円滑な情報共有を図るため、最高データ取扱責任者、データ保護管理者、データ取扱責任者、情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

ク　データ保護管理者は、緊急時には最高データ取扱責任者に早急に報告を行うとともに、回復のための対策を講じなければならない。

ケ　データ保護管理者は、自己の権限及び責任において処理する事務について、と認めた場合には、最高データ取扱責任者に報告し、指示を仰がなければならない。

（３）データ取扱責任者

ア　各課室等の長をデータ取扱責任者とする。

イ　データ取扱責任者は、各課室等の情報セキュリティ対策に関する統括的な権限及び責任を有する。

ウ　データ取扱責任者は、保有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

エ　データ取扱責任者は、保有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約及び職員等（職員、非常勤職員及び臨時職員をいう。以下同じ。）に対する教育、訓練、助言及び指示を行う。

オ　データ取扱責任者は、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、データ保護管理者及び最高データ取扱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。

カ　データ取扱責任者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

（４）端末装置管理責任者

ア　端末装置を設置する各課室等の長を端末装置管理責任者とする。

イ　端末装置管理責任者は、端末装置の厳正な管理及び端末装置の利用によって処理されるデータの的確な管理が行われるように措置を講じなければならない。

（５）情報システム担当者

データ取扱責任者の指示等に従い、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。

（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。

イ　情報セキュリティ委員会は、毎年度、広域連合における情報セキュリティ対策計画を策定し、その実施状況を確認しなければならない。

（7）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、やむを得ない場合を除き、同じ者が兼務してはならない。

（8）　情報セキュリティに関する統一的な窓口の設置

ア　最高データ取扱責任者は、情報セキュリティインシデントの統一的な窓口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。

イ　最高データ取扱責任者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、その内容を関係職員等に提供する。

ウ　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。

エ　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。

4　情報資産の分類と管理方法

（1）情報資産の分類

広域連合における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

機密性による情報資産の分類

分類	分類基準	取扱制限
機密性３	広域連合の業務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	・支給以外の端末での作業の原則禁止（機密性３の情報資産に対して） ・必要以上の複製及び配付禁止

機密性２	広域連合の業務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
機密性１	機密性２又は機密性３の情報資産以外の情報資産	

完全性による情報資産の分類

分類	分類基準	取扱制限
完全性２	広域連合の業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広域連合の業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	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
完全性１	完全性２情報資産以外の情報資産	

可用性による情報資産の分類

分類	分類基準	取扱制限
可用性２	広域連合の業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広域連合の業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性１	可用性２の情報資産以外の情報資産	

（２）情報資産の管理

ア　管理責任

（ア）　データ取扱責任者は、その所管する情報資産について管理責任を有する。

（イ）　情報資産が複製又は伝送された場合には、複製等された情報資産も（１）の分類に基づき管理しなければならない。

イ　情報資産の分類の表示

職員等は、情報資産について、情報を記録した電磁的記憶媒体等に分類を表示し、適切な管理を行わなければならない。

ウ　情報の作成

（ア）　職員等は、業務上必要のない情報を作成してはならない。

（イ）　情報を作成する者は、情報の作成時に（１）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。

（ウ）　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

（ア）　事務局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。

（イ）　事務局外の者が作成した情報資産を入手した者は、（１）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。

（ウ）　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、データ取扱責任者に判断を仰がなければならない。

オ　情報資産の利用

（ア）　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

（イ）　情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。

（ウ）　情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

カ　情報資産の保管

（ア）　データ取扱責任者は、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。

（イ）　データ取扱責任者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

（ウ）　データ取扱責任者は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。

（エ） データ取扱責任者は、機密性２以上、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

キ　情報の送信

電子メール等により機密性２以上の情報を送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。

ク　情報資産の運搬

（ア） 車両等により機密性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、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。

（イ） 機密性２以上の情報資産を運搬する者は、データ取扱責任者に許可を得なければならない。

ケ　情報資産の提供・公表

（ア） 機密性２以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

（イ） 機密性２以上の情報資産を外部に提供する者は、データ取扱責任者に許可を得なければならない。

（ウ） データ取扱責任者は、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。

コ　情報資産の廃棄

（ア） 機密性２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。

（イ） 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。

（ウ） 情報資産の廃棄を行う者は、データ取扱責任者の許可を得なければならない。

５　物理的セキュリティ

（１）サーバ等の管理

ア　機器の取付け

端末装置管理責任者は、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。

イ　サーバの冗長化

データ取扱責任者は、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冗長化し、同一データを保持しなければならない。

ウ　機器の電源

（ア）　端末装置管理責任者は、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。

（イ）　端末装置管理責任者は、施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

エ　通信ケーブル等の配線

（ア）　端末装置管理責任者は、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。

（イ）　端末装置管理責任者は、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。

（ウ）　端末装置管理責任者は、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。

（エ）　端末装置管理責任者は、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。

オ　機器の定期保守及び修理

（ア）　端末装置管理責任者は、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）　端末装置管理責任者は、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せなければならない。内容を消去できない場合、端末装置管理責任者は、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ほか、秘密保持体制の確認などを行わなければならない。

カ　外部への機器の設置

端末装置管理責任者は、外部にサーバ等の機器を設置する場合、データ保護管理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。

キ　機器の廃棄等

データ取扱責任者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

（２）管理区域の管理

ア　管理区域の構造等

（ア）　管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋（以下「事務室等」という。）

や電磁的記録媒体の保管庫をいう。

（イ） 施設管理部門の長は事務室等の出入りについて、制御機能、鍵、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。

（ウ） 端末装置管理責任者は、情報機器等に、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。

（エ） 端末装置管理責任者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

イ 管理区域の入退室管理等

（ア） 端末装置管理責任者は、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、入退室管理簿等により入退室管理を行わなければならない。

（イ） 職員等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。

（ウ） 端末装置管理責任者は、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を立ち合わせなければなければならない。

ウ 機器等の搬入出

（ア） 端末装置管理責任者は、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した業者に確認を行わせなければならない。

（イ） 端末装置管理責任者は、事務室等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。

（３）通信回線及び通信回線装置の管理

ア 端末装置管理責任者は、広域連合内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連する文書を適切に保管しなければならない。

イ 端末装置管理責任者は、 外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

ウ 端末装置管理責任者は、機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適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。

エ 端末装置管理責任者は、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。

オ 端末装置管理責任者は、可用性２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。

（４）職員等のパソコン等の管理

ア　端末装置管理責任者は、盗難防止のため、施錠管理等の物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

イ　端末装置管理責任者は、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。

6　人的セキュリティ

（1）職員等の遵守事項

ア　職員等の遵守事項

(ア)　情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び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、速やかにデータ取扱責任者に相談し、指示を仰がなければならない。

(イ)　業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

(ウ)　モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

a　最高データ取扱責任者は、機密性２以上、可用性２、完全性２の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

b　職員等は、広域連合のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、データ取扱責任者の許可を得なければならない。

c　職員等は、外部で情報処理業務を行う場合には、データ取扱責任者の許可を得なければならない。

d　職員等は、外部で情報処理作業を行う際、私物パソコンを用いる場合には、データ保護管理者の許可を得た上で、安全管理措置を遵守しなければならない。また、機密性３の情報資産については、私物パソコンによる情報処理を行ってはならない。

(エ)　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の業務利用

a　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原則業務に利用してはならない。ただし、業務上必要な場合は、データ取扱責任者の許可を得て利用することができる。

b　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用いる場合には、データ取扱責任者の許可を得た上で、外部で情報処理作業を

行う際に安全管理措置を遵守しなければならない。

（オ） 持ち出し及び持ち込みの記録

データ取扱責任者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

（カ） パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定をデータ取扱責任者の許可なく変更してはならない。

（キ） 机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又はデータ取扱責任者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等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） 退職時等の遵守事項

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

イ 非常勤及び臨時職員への対応

（ア） 情報セキュリティポリシー等の遵守

データ保護管理者は、非常勤及び臨時職員に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び臨時職員が守るべき内容を理解させ、また実施及び遵守させなければならない。

（イ） 情報セキュリティポリシー等の遵守に対する同意

データ保護管理者は、非常勤及び臨時職員の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

（ウ） インターネット接続及び電子メール使用等の制限

データ保護管理者は、非常勤及び臨時職員にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

ウ 情報セキュリティポリシー等の掲示

データ保護管理者は、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。

エ 外部委託事業者に対する説明

データ取扱責任者は、ネットワーク及び情報システムの開発・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。

（２）研修・訓練

ア　情報セキュリティに関する研修・訓練

最高データ取扱責任者は、定期的に情報セキュリティに関する研修・訓練を実施し、職員等に対し情報セキュリティポリシーについて、教育しなければならない。

イ　最高データ取扱責任者は。緊急時対応を想定した訓練等を年１回以上実施しなければならない。

ウ　職員等は、定期的に研修・訓練を受けることにより、情報セキュリティポリシーを理解し、情報セキュリティ上の問題が生じないようにしなければならない。

（３）情報セキュリティインシデントの報告

ア　職員等からの情報セキュリティインシデントの報告

（ア）　職員等は、情報セキュリティインシデントを認知した場合、速やかにデータ取扱責任者に報告しなければならない。

（イ）　報告を受けたデータ取扱責任者は、速やかに情報セキュリティに関する統一的な窓口に報告しなければならない。

（ウ）　データ取扱責任者は、報告のあった情報セキュリティインシデントについて、必要に応じて最高データ取扱責任者及びデータ保護管理者に報告しなければならない。

イ　住民等外部からの情報セキュリティインシデントの報告

（ア）　職員等は、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、データ取扱責任者に報告しなければならない。

（イ）　報告を受けたデータ取扱責任者は、速やかにデータ保護管理者に報告しなければならない。

（ウ）　データ保護管理者は、当該情報セキュリティインシデントについて、必要に応じて最高データ取扱責任者に報告しなければならない。

ウ　情報セキュリティインシデント原因の究明・記録、再発防止等

（ア）　データ保護管理者は、情報セキュリティインシデントを引き起こした部門のデータ取扱責任者及び情報セキュリティに関する統一的な窓口と連携し、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明結果から、再発防止策を検討し、最高データ取扱責任者に報告しなければならない。

（イ）　最高データ取扱責任者は、データ保護管理者から、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

（４）ＩＤ及びパスワード等の管理

ア　ＩＣカード等の取扱い

（ア） 職員等は、自己の管理するＩＣカード等に関し、次の事項を遵守しなければならない。

a 認証に用いるＩＣカード等を、職員等間で共有してはならない。

b 業務上必要のないときは、ＩＣカード等をカードリーダ若しくはパソコン等の端末のスロット等から抜いておかなければならない。

c ＩＣカード等を紛失した場合には、速やかにデータ保護管理者及び端末装置管理責任者に通報し、指示に従わなければならない。

（イ） データ保護管理者及びデータ取扱責任者は、ＩＣカード等の紛失等の通報があり次第、当該ＩＣカード等を使用したアクセス等を速やかに停止しなければならない。

（ウ） データ保護管理者及び端末装置管理責任者は、ＩＣカード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

イ ＩＤの取扱い

職員等は、自己の管理するＩＤに関し、次の事項を遵守しなければならない。

（ア） 自己が利用しているＩＤは、他人に利用させてはならない。

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

ウ パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

（ア） パスワードは、他者に知られないように管理しなければならない。

（イ） パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

（ウ） パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

（エ） パスワードが流出したおそれがある場合には、データ取扱責任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。

（オ） 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。

（カ） 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。

（キ） 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。

（ク） 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。

（ケ） 職員等間でパスワードを共有してはならない。

7 技術的セキュリティ

（1）コンピュータ及びネットワークの管理

ア 文書サーバの設定等

（ア） 文書サーバを所管する端末装置管理責任者は、職員等が使用できる文書サー

バの容量を設定し、職員等に周知しなければならない。

（イ） 文書サーバを所管する端末装置管理責任者は、住民の個人情報、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、同一課室等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

イ　バックアップの実施

文書サーバを所管する端末装置管理責任者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

ウ　他団体との情報システムに関する情報等の交換

端末装置管理責任者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、データ保護管理者の許可を得なければならない。

エ　システム管理記録及び作業の確認

（ア） データ取扱責任者は、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） データ取扱責任者は、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切に管理しなければならない。

（ウ） データ取扱責任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。

オ　情報システム仕様書等の管理

データ取扱責任者は、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。

カ　ログの取得等

（ア） データ取扱責任者は、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） データ取扱責任者は、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、適切にログを管理しなければならない。

（ウ） データ取扱責任者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、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。

キ　障害記録

データ取扱責任者は、職員等からのシステム障害の報告、システム障害に対する処

理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

ク　ネットワークの接続制御、経路制御等

（ア）　データ取扱責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

（イ）　データ取扱責任者は、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。

ケ　外部の者が利用できるシステムの分離等

データ取扱責任者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

コ　外部ネットワークとの接続制限等

（ア）　端末装置管理責任者は、所管するネットワークを外部ネットワークと接続しようとする場合には、最高データ取扱責任者及びデータ保護管理者の許可を得なければならない。

（イ）　端末装置管理責任者は、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、事務局内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

（ウ）　端末装置管理責任者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

（エ）　端末装置管理責任者は、ウェブサーバ等をインターネットに公開する場合、事務局内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

（オ）　端末装置管理責任者は、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、データ保護管理者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

サ　複合機のセキュリティ管理

（ア）　データ保護管理者は、複合機を調達する場合、当該複合機が備える機能、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、適切なセキュリティ要件を策定しなければならない。

（イ）　データ保護管理者は、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講じなければならない。

（ウ） データ保護管理者は、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。

シ　特定用途機器のセキュリティ管理

（ア） データ保護管理者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を実施しなければならない。

ス　無線ＬＡＮ及びネットワークの盗聴対策

（ア） データ保護管理者は、無線ＬＡＮの利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

（イ） データ保護管理者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

セ　電子メールのセキュリティ管理

（ア） データ保護管理者は、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。

（イ） データ保護管理者は、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。

（ウ） データ保護管理者は、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。

（エ） データ保護管理者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

（オ） データ保護管理者は、システム開発や運用、保守等のため事務局舎内に常駐している外部委託事業者の作業員による電子メールアドレス利用について、外部委託事業者との間で利用方法を取り決めなければならない。

（カ） データ保護管理者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように添付ファイルの監視等によりシステム上措置しなければならない。

ソ　電子メールの利用制限

（ア） 職員等は、自動転送機能を用いて、電子メールを転送してはならない。

（イ） 職員等は、業務上必要のない送信先に電子メールを送信してはならない。

（ウ） 職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

（エ） 職員等は、重要な電子メールを誤送信した場合、データ取扱責任者に報告しなければならない。

（オ） 職員等は、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。

タ　電子署名・暗号化

（ア）　職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、データ保護管理者が定めた電子署名、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。

（イ）　職員等は、暗号化を行う場合にデータ保護管理者が定める以外の方法を用いてはならない。また、データ保護管理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）　データ保護管理者は、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。

チ　無許可ソフトウェアの導入等の禁止

（ア）　職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

（イ）　職員等は、業務上の必要がある場合は、データ保護管理者及びデータ取扱責任者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、データ取扱責任者は、ソフトウェアのライセンスを管理しなければならない。

（ウ）　職員等は、不正にコピーしたソフトウェアを利用してはならない。

ツ　機器構成の変更の制限

（ア）　職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。

（イ）　職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、データ保護管理者の許可を得なければならない。

テ　無許可でのネットワーク接続の禁止

職員等は、データ保護管理者の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

ト　業務以外の目的でのウェブ閲覧の禁止

（ア）　職員等は、業務以外の目的でウェブを閲覧してはならない。

（イ）　端末装置管理責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、データ保護管理者に通知し適切な措置を求めなければならない。

（２）アクセス制御

ア　アクセス制御

（ア）　アクセス制御等

データ保護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無い職員等がアクセスできないように、システム制限しなけれ

ばならない。

（イ） 利用者ＩＤの取扱い

a　データ保護管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、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。

b　職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、データ保護管理者に通知しなければならない。

c　データ保護管理者は、利用されていないＩＤが放置されないよう、人事管理部門と連携し、点検しなければならない。

（ウ） 特権を付与されたＩＤの管理等

a　データ保護管理者は、管理者権限等の特権を付与されたＩＤを利用する者を必要最小限にし、当該ＩＤのパスワードの漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理しなければならない。

b　データ保護管理者 の特権を代行する者は、データ保護管理者が指名し、最高データ取扱責任者が認めた者でなければならない。

c　最高データ取扱責任者は、代行者を認めた場合、速やかにデータ保護管理者に通知しなければならない。

d　データ保護管理者は、特権を付与されたＩＤ及びパスワードについて、職員等の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。

e　データ保護管理者は、特権を付与されたＩＤを初期設定以外のものに変更しなければならない。

イ　職員等による外部からのアクセス等の制限

（ア） 職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、データ保護管理者の許可を得なければならない。

（イ） データ保護管理者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

（ウ） データ保護管理者は、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。

（エ） データ保護管理者は、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。

（オ） データ保護管理者及びデータ取扱責任者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

（カ） 職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を事務局内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、

パッチの適用状況等を確認しなければならない。

（キ） データ保護管理者は、公衆通信回線（公衆無線ＬＡＮ等）の事務局外通信回線を事務局内ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者のＩＤ及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（ＩＣカード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

ウ　パスワードに関する情報の管理

データ保護管理者又はデータ取扱責任者は、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。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。

エ　特権による接続時間の制限

データ取扱責任者は、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。

（３）システム開発、導入、保守等

ア　情報システムの調達

（ア） データ保護管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

（イ） データ保護管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

イ　情報システムの開発

（ア） システム開発における責任者及び作業者の特定

データ保護管理者は、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。

（イ） システム開発における責任者、作業者のＩＤの管理

ａ　データ保護管理者は、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。

ｂ　データ保護管理者は、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。

（ウ） システム開発に用いるハードウェア及びソフトウェアの管理

ａ　データ保護管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

ｂ　データ保護管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならな

い。

ウ　情報システムの導入

（ア）　開発環境と運用環境の分離及び移行手順の明確化

a　データ取扱責任者は、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。

b　データ保護管理者又はデータ取扱責任者は、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。

c　データ取扱責任者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

（イ）　テスト

a　データ保護管理者又はデータ取扱責任者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

b　データ保護管理者又はデータ取扱責任者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

c　データ保護管理者又はデータ取扱責任者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

d　データ保護管理者又はデータ取扱責任者は、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。

エ　システム開発・保守に関連する資料等の整備・保管

（ア）　データ保護管理者又はデータ取扱責任者は、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切に整備・保管しなければならない。

（イ）　データ保護管理者又はデータ取扱責任者は、テスト結果を一定期間保管しなければならない。

（ウ）　データ保護管理者又はデータ取扱責任者は、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。

オ　情報システムにおける入出力データの正確性の確保

（ア）　データ保護管理者又はデータ取扱責任者は、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）　データ保護管理者又はデータ取扱責任者は、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）　データ保護管理者又はデータ取扱責任者は、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。

カ　情報システムの変更管理

データ保護管理者又はデータ取扱責任者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

キ　開発・保守用のソフトウェアの更新等

データ保護管理者又はデータ取扱責任者は、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。

ク　システム更新又は統合時の検証等

データ保護管理者又はデータ取扱責任者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

（4）不正プログラム対策

ア　データ保護管理者の措置事項

データ保護管理者は、不正プログラム対策として、次の事項を措置しなければならない。

（ア）　外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

（イ）　外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

（ウ）　コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

（エ）　サーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

（オ）　不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

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

（キ）　パッチやバージョンアップなどについての開発元のサポートが終了したソフトウェアを利用してはならない。

イ　データ取扱責任者の措置事項

データ取扱責任者は、不正プログラム対策に関し、次の事項を措置しなければならない。

（ア）　データ取扱責任者は、その所掌するサーバ及びパソコン等の端末に、コンピ

ュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させなければならない。

（イ） 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、広域連合が管理している媒体以外を職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

ウ　職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

（ア） パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

（イ） 外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

（ウ） 差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

（エ） 端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

（オ） 添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。

（カ） データ保護管理者が提供するウイルス情報を、常に確認しなければならない。

（キ） コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、以下の対応を行わなければならない。

ａ　パソコン等の端末の場合

ＬＡＮケーブルの即時取り外しを行わなければならない。

ｂ　モバイル端末の場合

直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。

エ　専門家の支援体制

データ保護管理者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

（５）不正アクセス対策

ア　データ保護管理者の措置事項

データ保護管理者は、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。

（ア） 使用されていないポートを閉鎖しなければならない。

（イ） 不要なサービスについて、機能を削除又は停止しなければならない。

（ウ） 不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、データ保護管理者 及びデータ取扱責任者へ通報するよう、設定しなければならない。

（エ） 重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。

（オ） データ保護管理者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築しなければならない。

イ 攻撃の予告

データ保護管理者は、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。

ウ 記録の保存

データ保護管理者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

エ 内部からの攻撃

データ保護管理者は、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。

オ 職員等による不正アクセス

データ保護管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課室等のデータ取扱責任者に通知し、適切な処置を求めなければならない。

カ サービス不能攻撃

データ保護管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

キ 標的型攻撃

データ保護管理者は、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。

（6） セキュリティ情報の収集

ア セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

データ保護管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、

ソフトウェア更新等の対策を実施しなければならない。

イ　不正プログラム等のセキュリティ情報の収集・周知

データ保護管理者は、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、職員等に周知しなければならない。

ウ　情報セキュリティに関する情報の収集及び共有

データ保護管理者は、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。

8　運用

（1）情報システムの監視

（ア）　データ保護管理者は、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）　データ保護管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

（ウ）　データ保護管理者は、外部と常時接続するシステムを常時監視しなければならない。

（2）情報セキュリティポリシーの遵守状況の確認

ア　遵守状況の確認及び対処

（ア）　データ取扱責任者は、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、速やかにデータ保護管理者に報告しなければならない。

（イ）　データ保護管理者は、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。

（ウ）　データ保護管理者は、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。

イ　パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

最高データ取扱責任者及び最高データ取扱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、職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

ウ　職員等の報告義務

（ア）　職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちにデータ保護管理者に報告を行わなければならない。

（イ）　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データ保護管理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。

（３）侵害時の対応等

ア　緊急時対応計画の策定

最高データ取扱責任者又は情報セキュリティ委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適切に対処しなければならない。

イ　緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

（ア）　関係者の連絡先

（イ）　発生した事案に係る報告すべき事項

（ウ）　発生した事案への対応措置

（エ）　再発防止措置の策定

ウ　業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、情報セキュリティ委員会は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

エ　緊急時対応計画の見直し

最高データ取扱責任者又は情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

（４）例外措置

ア　例外措置の許可

データ取扱責任者は、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、広域連合の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、データ保護管理者の許可を得て、例外措置を取ることができる。

イ　緊急時の例外措置

データ取扱責任者は、広域連合の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、事後速やかにデータ保護管理者に報告しなければならない。

ウ　例外措置の申請書の管理

データ保護管理者は、例外措置の申請書及び審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

（５）法令遵守

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

（ア） 地方公務員法(昭和 25 年法律第 261 号)

（イ） 著作権法（昭和 45 年法律第 48 号)

（ウ） 不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号)

（エ） 個人情報の保護に関する法律（平成 15 年日法律第 57 号)

（オ） 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号)

（カ） 大分県後期高齢者医療広域連合個人情報保護条例（平成 19 年条例第 27 号)

（キ） 大分県後期高齢者医療広域連合情報公開条例(平成 19 年条例第 26 号)

（ク） 大分県後期高齢者医療広域連合電子計算機処理の管理運営に関する規程（平成 19 年訓令第 10 号)

（６）懲戒処分等

ア 懲戒処分

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

イ 違反時の対応

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

（ア） データ保護管理者が違反を確認した場合は、データ保護管理者は当該職員等が所属する課室等のデータ取扱責任者に通知し、適切な措置を求めなければならない。

（イ） データ取扱責任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データ保護管理者及び当該職員等が所属する課室等のデータ取扱責任者に通知し、適切な措置を求めなければならない。

（ウ） データ取扱責任者の指導によっても改善されない場合、データ保護管理者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、データ保護管理者は、職員等の権利を停止あるいは剥奪した旨を最高データ取扱責任者及び当該職員等が所属する課室等のデータ取扱責任者に通知しなければならない。

９ 外部サービスの利用

（１）外部委託

ア 外部委託事業者の選定基準

（ア） データ取扱責任者は、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。

（イ） データ取扱責任者は、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。

イ　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。

・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
・外部委託事業者の責任者、委託内容、作業者、作業場所の特定
・提供されるサービスレベルの保証
・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、アクセス方法
・外部委託事業者の従業員に対する教育の実施
・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
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・広域連合による監査、検査
・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
・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

ウ　確認・措置等

データ取扱責任者は、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定期的に確認し、必要に応じ、イの契約に基づき措置しなければならない。また、その内容をデータ保護管理者 に報告するとともに、その重要度に応じて最高データ取扱責任者に報告しなければならない。

（２）ソーシャルメディアサービスの利用

（ア）　データ取扱責任者は、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。

a　広域連合のアカウントによる情報発信が、実際の広域連合のものであることを明らかにするために、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行うこと。

b　パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ＩＣカード等）等を適切に管理するなどの方法で、不正アクセス対策を行うこと

（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。

10　評価・見直し

（1）監査

ア　実施方法

最高データ取扱責任者は、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じて監査を行わせなければならない。

イ　監査を行う者の要件

（ア）　情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

（イ）　監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

ウ　監査実施計画の立案及び実施への協力

（ア）　情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。

（イ）　被監査部門は、監査の実施に協力しなければならない。

エ　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必要に応じて行わなければならない。

オ　報告

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

カ　保管

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

キ　監査結果への対応

最高データ取扱責任者は、監査結果を踏まえ、指摘事項を所管するデータ取扱責任者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していないデータ取扱責任者に対しても、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。

ク　情報セキュリティポリシー及び関係規程等の見直し等への活用

情報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及び関係規定等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

（2）自己点検

ア　実施方法

（ア）　データ保護管理者及び端末装置管理責任者は、所管するネットワーク及び情

報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

（イ） データ保護管理者及び端末装置管理責任者は、各課室等における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行わなければならない。

イ 報告

データ保護管理者及び端末装置管理責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告しなければならない。

ウ 自己点検結果の活用

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

（イ） 情報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。

（3）情報セキュリティポリシー及び関係規程等の見直し

情報セキュリティ委員会は、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ふまえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。

〈参考文献〉

・総務省策定「地方公共団体における情報セキュリティポリシーに関するガイドライン（平成２７年３月版）」

・総務省策定「情報セキュリティ対策基準　例文」