○後志広域連合情報セキュリティに関する規程

（平成28年10月７日
訓令第３号）

第１章　基本方針

（目的）

第１条　後志広域連合（以下「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、広域連合が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

（定義）

第２条　次の各号に掲げる用語の意義は、当該各号に定めるところによる。

⑴　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。

⑵　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。

⑶　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。

⑷　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。

⑸　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。

⑹　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。

（対象とする脅威）

第３条　情報セキュリティ対策を講じるべき情報資産に対する脅威は、次の各号に掲げるものとする。

⑴　不正アクセス、コンピュータウイルス攻撃、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、消去、重要情報の詐取及び内部不正等

⑵　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、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、機器故障等の非意図的要因による情報資産の漏えい、破壊及び消去等

⑶　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

（適用範囲）

第４条　この規程（以下「セキュリティ規程」という。）が適用される機関は、広域連合の全ての執行機関（広域連合長、議会事務局、選挙管理委員会、監査委員）とする。

２　セキュリティ規程が対象とする情報資産は、広域連合が管理及び保有する次の各号に掲げるものとする。ただし、本広域連合を構成する町村において取り扱われるものを除

く。

⑴　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

⑵　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。）

⑶　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

（職員等の遵守義務）

第５条　職員、非常勤職員及び臨時職員（以下「職員」という。）は、情報セキュリティの重要性について共通認識を持ち、業務の遂行に当たってセキュリティ規程を遵守するものとする。

（情報セキュリティ対策）

第６条　第３条各号に掲げる脅威から情報資産を保護するために、次の各号に掲げる対策を行うものとする。

⑴　物理的セキュリティ　部外者の侵入による不正な立入り又は情報資産への損傷・妨害等から保護するために物理的な対策を講じる。

⑵　人的セキュリティ　情報セキュリティに関する権限や責任を定め、職員及び外部委託事業者にセキュリティ規程の内容を周知徹底する等の研修及び啓発の対策を講じる。

⑶　技術及び運用におけるセキュリティ　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、情報資産のアクセスの制御、ネットワーク管理等の技術的な対策、システム開発等の外部委託及びセキュリティ規程の遵守状況確認等の運用面の対策を講じる。

（セキュリティ規程の見直し）

第７条　情報セキュリティに関する状況の変化等を踏まえ、必要に応じ適宜セキュリティ規程の見直しを行う。

第２章　情報セキュリティ対策基準

第１節　組織及び体制

（組織及び体制）

第８条　情報セキュリティ対策を適切に管理・推進するため、情報セキュリティ管理体制に次の者を置く。

⑴　最高情報セキュリティ責任者

⑵　統括情報セキュリティ責任者

⑶　情報システム管理者

⑷　情報システム担当者

（最高情報セキュリティ責任者）

第９条　最高情報セキュリティ責任者に、副広域連合長を充てる。

２　最高情報セキュリティ責任者は、広域連合における全てのネットワーク及び情報システム等の情報資産の管理、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ものとする。

（統括情報セキュリティ責任者）

第１０条　統括情報セキュリティ責任者に、事務局長を充てる。

２　統括情報セキュリティ責任者は、次の各号に掲げる責任及び権限を有するものとする。

⑴　最高情報セキュリティ責任者を補佐する。

⑵　広域連合全てのネットワークにおける開発、設定の変更、運用及び見直し等を行う。

⑶　広域連合全てのネットワークにおける情報セキュリティ対策を行う。

⑷　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。

⑸　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、最高情報セキュリティ責任者の指示に従い、最高情報セキュリティ責任者が不在の場合は自らの判断に基づき、必要かつ十分な措置を行う。

⑹　緊急時等の円滑な情報共有を図るため、最高情報セキュリティ責任者、統括情報セキュリティ責任者、情報システム管理者及び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する。

⑺　緊急時に、最高情報セキュリティ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る。

⑻　職員等が使用する端末及びＵＳＢメモリ等の電子記録媒体の総合的な管理及び配置を行う。

（情報システム管理者）

第１１条　情報システム管理者に、各担当課室長を充てる。

２　情報システム管理者は、次の各号に掲げる責任及び権限を有するものとする。

⑴　所管する情報システムにおける開発、設定の変更、運用及び見直し等を行う。

⑵　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対策を行う。

（情報システム担当者）

第１２条　情報システム担当者に、各担当係長を充てる。

２　情報システム担当者は、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、運用及び更新等の作業を行う。

（情報セキュリティ委員会）

第１３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を置く。

２　情報セキュリティ委員会は、情報セキュリティに関する重要な事項を審議し決定する。

３　情報セキュリティ委員会は、第８条第１号から第３号に規定する者をもって構成する。

（情報セキュリティに関する統一的な窓口の設置）

第１４条　最高情報セキュリティ責任者は、情報セキュリティインシデントに関する統一的な窓口の機能を有する組織を設置し、総務課がその役割を担う。

２　前項の組織の役割は、情報セキュリティインシデントに対処し、被害拡大防止、復旧、再発防止、国、道、関係町村等の関係機関及びシステム保守委託事業者等の連絡・情報共有等の対応を迅速かつ的確に実施するものとする。

第２節　物理的セキュリティ

（サーバ等の管理）

第１５条　情報システム管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度及び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に適切に固定する等、必要な措置を講じなければならない。

２　情報システム管理者は、サーバ等の機器に障害が発生し、システムの運用が停止しないようシステムの運用停止時間を最小限にするため、サーバ等の機器を冗長化し、同一データを保持しなければならない。

３　サーバ等の機器の電源は、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。

４　通信ケーブル等の配線は、次の各号に掲げる措置を講じなければならない。

⑴　損傷等を防止するため、配線収納管を使用する等必要な措置を施すこと。

⑵　第８条各号に掲げる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すこと。

５　情報システム管理者は、システムの安定的な運用のため、サーバ等の機器の定期保守を実施しなければならない。

６　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、庁外にサーバ等の機器を設置する場合、最高情報セキュリティ責任者の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認をしなければならない。

７　情報システム管理者は、サーバ等の機器を廃棄又はリースの返却等をする場合、当該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。

（通信回線等の管理）

第１６条　統括情報セキュリティ責任者は、庁内の通信回線、通信回線装置及びそれに関連する文書を適切に管理しなければならない。

２　外部へのネットワーク接続は、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。

３　行政系のネットワークは、取り扱う情報の重要度及び性質に応じてネットワークを分割し、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　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、改ざん及び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。

（パソコン等の端末の管理）

第１７条　情報システム管理者は、盗難防止のための物理的措置を講じるよう努めるものとする。また、執務室等に職員がいない場合は、部外者の侵入を防ぐよう執務室等の施錠等を行うものとする。

２　情報システム管理者は、パソコン等の端末（以下「端末」という。）の電源起動時及び情報システム起動時に、ＩＤ及び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。

３　情報システム管理者は、前条第３項により分割したネットワークで取り扱う情報の重

要度及び性質に応じて、ＩＤ及びパスワード以外にＩＣカード等による二要素認証を併用してネットワークにログインするよう設定しなければならない。

４　情報システム管理者は、端末におけるデータ暗号化機能を有効に利用しなければならない。また、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用しなければならない。

第３節　人的セキュリティ

（職員の遵守事項）

第１８条　職員は、セキュリティ規程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、速やかに統括情報セキュリティ責任者に相談し、指示を仰がなければならない。

２　職員は、業務以外の目的で情報資産の外部の持ち出し、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　端末及び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は、次のとおり制限するものとする。

⑴　職員は、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、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。

⑵　職員は、外部で情報処理業務を行う場合は、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。

４　広域連合の支給以外の端末及び電磁的記録媒体等の業務利用は、次のとおり制限するものとする。

⑴　職員は、広域連合の支給以外の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、統括情報セキュリティ責任者の許可を得て利用することができる。

⑵　職員は、広域連合の支給以外の端末及び電磁的記録媒体等を利用する場合は、統括情報セキュリティ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。

５　統括情報セキュリティ責任者は、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。

６　職員は、端末のソフトウェアに関するセキュリティ機能の設定を統括情報セキュリティ責任者の許可なく変更してはならない。

７　職員は、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統括情報セキュリティ責任者の許可なく情報を閲覧されることがないように、離席時の端末のロックや電磁的記録媒体及び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。

８　職員は、異動又は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。

（非常勤及び臨時職員への対応）

第１９条　情報セキュリティ管理者は、非常勤職員及び臨時職員に対し、採用時に情報セ

キュリティに関して、非常勤職員及び臨時職員が守るべき内容を理解させ、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は、非常勤職員及び臨時職員に端末等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。

（セキュリティ規程等の提示）

第２０条　統括情報セキュリティ責任者は、職員が常にセキュリティ規程を閲覧できるように提示しなければならない。

（外部委託事業者に対する説明）

第２１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、セキュリティ規程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。

（研修・啓発）

第２２条　最高情報セキュリティ責任者は、職員に対する情報セキュリティに関する研修会の実施又は関連資料の配布等により、情報セキュリティに関する啓発をしなければならない。

（情報セキュリティインシデントの報告）

第２３条　職員は、情報セキュリティインシデントを発見した場合、速やかに統括情報セキュリティ責任者、情報システム管理者、情報システム担当者及び情報セキュリティインシデントに関する統一的な窓口に報告しなければならない。

２　前項により報告を受けた統括情報セキュリティ管理者は、必要に応じ最高情報セキュリティ責任者に報告しなければならない。

３　統括情報セキュリティ責任者は、情報セキュリティインシデントの原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、最高情報セキュリティ責任者に報告しなければならない。

４　最高情報セキュリティ責任者は、統括情報セキュリティ責任者から前項の報告を受けたときは、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。

５　最高情報セキュリティ責任者は、情報セキュリティインシデントの重要度や影響範囲等を勘案し必要と認めるときは、報道機関への通知・公表対応を行う。

（ＩＤ、パスワード及びＩＣカードの管理）

第２４条　職員は、自己の管理するＩＤに関し、次の事項を遵守しなければならない。

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　共同ＩＤを利用する場合は、共同ＩＤの利用者以外に利用させてはならない。

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

⑴　パスワードは、他人に知られないように管理しなければならない。

⑵　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。

⑶　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。
⑷　パスワードが流出したおそれがある場合には、統括情報セキュリティ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。
⑸　パスワードは定期的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。
⑹　複数の情報システムを扱う職員は、同一のパスワードをシステム間で用いてはならない。
⑺　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。
⑻　端末にパスワードを記憶させてはならない。
⑼　職員間でパスワードを共有してはならない。

３　職員は、自己の管理するＩＣカードに関し、次の事項を遵守しなければならない。
⑴　認証に用いるＩＣカードを、職員間で共有してはならない。
⑵　業務上必要がないときは、ＩＣカードをカードリーダ若しくは端末のスロット等から抜いておかなければならない。
⑶　ＩＣカードを紛失した場合は、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、指示に従わなければならない。

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、ＩＣカードの紛失の報告があり次第、当該ＩＣカード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。

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、ＩＣカードを切り替える場合、切り替え前のＩＣ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うで廃棄しなければならない。

第４節　技術的セキュリティ

（ファイルサーバの設定等）

第２５条　統括情報セキュリティ責任者は、ファイルサーバを課単位で構成し、職員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。

２　特定の職員しか取り扱えない住民の個人情報並びに人事記録等のデータは、同一課であっても別途ディレクトリを作成するなど、担当係以外の職員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２６条　緊急時に備え、ファイルサーバに記録された情報は、定期的にバックアップを実施しなければならない。

（他団体との情報システムに関する情報等の交換）

第２７条　他の団体との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、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。

（情報システム仕様書等の管理）

第２８条　情報システムに関する仕様書及びネットワーク構成図等は、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・紛失等することがないよう、適切に管理しな

ければならない。

（ログの取得等）

第２９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、端末及び情報システム等に関する各種ログ及び情報セキュリティの確保に必要な記録を一定期間保存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、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か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。

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、取得したログを必要に応じて悪意ある第三者からの不正侵入、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。

（障害記録）

第３０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及び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。

（不正アクセスの防止）

第３１条　統括情報セキュリティ責任者は、ネットワークの接続で、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設定しなければならない。

（外部ネットワークとの接続制限）

第３２条　情報システム管理者は、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は、最高情報セキュリティ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、庁内のネットワーク及び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　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、ウェブサイトにより情報を公開・提供する場合、庁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うえで接続しなければならない。

５　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。

（複合機のセキュリティ管理）

第３３条　統括情報セキュリティ責任者は、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、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。

２　統括情報セキュリティ責任者は、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。

（特定用途機器のセキュリティ管理）

第３４条　統括情報セキュリティ責任者は、特定用途機器（テレビ会議システム、ＩＰ電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている又は電磁的記録媒体を内蔵しているものをいう。）について、取り扱う情報、利用方法及び通信回線への接続形態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。

（無線ＬＡＮ及びネットワークの盗聴対策）

第３５条　統括情報セキュリティ責任者は、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。

２　統括情報セキュリティ責任者は、情報の盗聴等を防ぐため、機密性の高い情報を取扱うネットワークに暗号化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３６条　統括情報セキュリティ責任者は、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、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　統統括情報セキュリティ責任者は、職員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ないよう、必要な措置を講じなければならない。

（電子メールの利用制限）

第３７条　職員は、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　職員は、重要な電子メールを誤送信した場合、情報システム管理者に報告しなければならない。

５　職員は、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。

（電子署名・暗号化）

第３８条　職員は、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、最高情報セキュリティ責任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。

２　職員は、暗号化を行う場合に、最高情報セキュリティ責任者が定める方法以外の方法を用いてはならない。また、最高情報セキュリティ責任者が定めた方法で暗号のための鍵を管理しなければならない。

（無許可ソフトウェアの導入等の禁止）

第３９条　職員は、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、ソフトウェアを導入することができる。なお、導入する際は、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、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。

（機器構成の変更の制限）

第４０条　職員は、端末に対し機器の改造、増設及び交換を行ってはならない。

２　職員は、業務上端末に対し機器の改造、増設又は交換を行う必要がある場合は、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４１条　職員は、統括情報セキュリティ責任者の許可なく端末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４２条　職員は、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、情報システム管理者に通知し適切な措置を求めなければならない。

（アクセス制御）

第４３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がアクセスできないように制限しなければならない。

（利用者ＩＤの取扱い）

第４４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、職員等の異動、出向、退職等に伴う利用者ＩＤは、適切に取り扱わなければならない。

（特権を付与されたＩＤの管理等）

第４５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、最高情報セキュリティ責任者が認めた者でなければならない。

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、特権を付与されたＩＤ及びパスワードの変更を外部委託事業者に行わせてはならない。

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を初期設定以外のものに変更しなければならない。

（職員等による外部からのアクセス等の制限）

第４６条　職員が、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、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。

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は、公衆通信回線（公衆無線ＬＡＮ等）の庁外通信回線を庁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。

（自動識別の設定）

第４７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、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるよう設定しなければならない。

（ログイン時の表示等）

第４８条　情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定又はログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ職員がログインしたことを確認することができるよう設定しなければならない。

（パスワードに関する情報の管理）

第４９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。

（情報システムの調達）

第５０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、情報システムの開発、導入及び保守等にあっては、セキュリティ機能が確保されるよう必要な措置を講じるものとする。

２　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と、システム運用環境を分離しなければならない。

３　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、既に稼動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。また、試験に使用するデータは、個人情報及び機密性の高いデータをテストデータに使用してはならない。

４　情報システム管理者は、システム開発、導入、保守等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。

（不正プログラム対策）

第５１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、次の各号に定める事項ついて措置しなければならない。

⑴　外部ネットワークから受信したファイルは、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。

⑵　外部ネットワークに送信するファイルは、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。

⑶　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、必要に応じ職員に対して注意喚起しなければならない。

⑷　所掌するサーバ及び端末に、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。

⑸　不正プログラム対策ソフトウェアは、常に最新の状態に保たなければならない。

⑹　業務で利用するソフトウェアは、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。

２　情報システム管理者は、不正プログラム対策に関し、次の各号に定める事項について措置しなければならない。

⑴　情報システム管理者は、その所掌するサーバ及び端末に、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。

⑵　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に利用させてはならない。

３　職員は、不正プログラム対策に関し、次の各号に定める事項を遵守しなければならない。

⑴　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。

⑵　外部からデータ又はソフトウェアを取り入れる場合は、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。

⑶　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。

⑷　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。

⑸　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。

⑹　新しいコンピュータウイルス情報を、常に確認しなければならない。

⑺　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、ＬＡＮケーブルの即時取外しを行わなければならない。

（不正アクセス対策）

第５２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、次の各号に掲げる事項を措置するものとする。

⑴　使用されていないポートを閉鎖しなければならない。

⑵　不正アクセスによるウェブページのデータの書換えを検出する等、ウェブページの改ざんを防止しなければならない。

⑶　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。

２　統括情報セキュリティ責任者は、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るとともに、関係機関と連携し情報の収集に努めなければならない。

３　統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス行為の禁止等に関する法律（平成11年法律第128号）に違反する等の犯罪の可能性がある場合は、攻撃の記録を保存するとともに、警察及び関係機関との連携に努めなければならない。

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、職員及び外部委託事業者が使用している端末から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。

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、職員等による不正アクセスを発見した場合は、適切な処置を行うものとする。

６　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、職員の教育や自動再生無効化等の人的対策及び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。

（セキュリティ情報の収集）

第５３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、必要に応じ職員間で共有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、必要に応じセキュリティ侵害を未然に防止するための対策を講じなければならない。

第５節　運用面のセキュリティ

（情報システムの監視）

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、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。

（セキュリティ規程の遵守状況の確認）

第５５条　統括情報セキュリティ責任者は、セキュリティ規程の遵守状況について確認を行い、問題を認めた場合は、最高情報セキュリティ責任者に報告しなければならない。

２　最高情報セキュリティ責任者は、前項により報告を受けたときは、適切に対処しなければならない。

３　最高情報セキュリティ責任者及び最高情報セキュリティ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、職員が使用している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。

４　職員は、セキュリティ規程に違反する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に報告を行わなければならない。

５　統括情報セキュリティ責任者は、前項による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判断したときは、適切に対処しなければならない。

（侵害時の対応等）

第５６条　統括情報セキュリティ責任者は、情報セキュリティインシデント又はセキュリティ規程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、復旧及び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、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。

２　統括情報セキュリティ責任者は、前項による措置を実施したときは、次の各号に掲げる事項を最高情報セキュリティ責任者及び情報セキュリティ委員会に報告するものとする。

⑴　発生した事案に係る報告すべき事項

⑵　発生した事案への対応措置

⑶　再発防止措置の策定

３　最高情報セキュリティ責任者及び情報セキュリティ委員会は、自然災害又は大規模かつ広範囲にわたる疾病等に備えて業務継続計画を策定する場合、セキュリティ規程との整合性を確保しなければならない。

（例外措置）

第５７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は、最高情報セキュリティ責任者の許可を得て、例外措置を取ることができる。

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、行政事務の遂行に緊急を要する等の場合であって、前項の許可を取る時間的余裕がないときは、事後速やかに最高情報セキュリティ責任者に報告しなければならない。

３　最高情報セキュリティ責任者は、例外措置の関係書類を適切に保管しなければならない。

（懲戒処分等）

第５８条　セキュリティ規程に違反した職員及びその監督責任者は、その重大性及び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。

２　職員のセキュリティ規程違反の行動を確認した場合は、速やかに次の各号に掲げる措置を講じなければならない。

⑴　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が所属する情報システム管理者に適切な措置を求めなければならない。

⑵　情報システム管理者が違反を確認した場合は、速やかに統括情報セキュリティ責任者に報告し適切な措置を求めなければならない。

⑶　統括情報セキュリティ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とともに、最高情報セキュリティ責任者及び当該職員が所属する情報システム管理者に報告しなければならない。

第６節　外部委託

（外部委託事業者の選定基準）

第５９条　最高情報セキュリティ責任者は、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。

２　最高情報セキュリティ責任者は、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。

（外部委託の契約項目）

第６０条　情報システムの運用及び保守等を外部委託する場合は、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で締結するものとする。

⑴　情報セキュリティに関連するセキュリティ規程等の遵守

⑵　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

⑶　提供されるサービスレベルの保障

⑷　外部委託事業者にアクセスを許可する情報の種類、範囲、アクセス方法

⑸　外部委託事業者の従業員に対する教育の実施

⑹　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

⑺　業務上知り得た情報の守秘義務

⑻　再委託に関する制限事項の遵守

⑼　委託業務終了時の情報資産の返還、廃棄等

⑽　委託業務の定期報告及び緊急時報告

⑾　広域連合による検査

⑿　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

⒀　情報セキュリティに関連するセキュリティ規程等が遵守されなかった場合に外部委託事業者が行う損害賠償等の規定

（確認・措置等）

第６１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、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若しくは随時確認を行い、

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。

第７節　評価・見直し

（点検）

第６２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、情報システム及び情報セキュリティ対策状況について、必要に応じて点検を実施するものとする。

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、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するものとする。

（点検結果等の活用）

第６３条　情報セキュリティ委員会は、前条の点検結果及び改善策をセキュリティ規程及び情報セキュリティ対策の見直し時に活用するものとする。

附　則

この訓令は、公布の日から施行する。