# 北海道情報セキュリティ対策基準

# 北海道情報セキュリティ対策基準

平成14年12月27日　総合企画部長決定

平成27年12月25日　全面改正

平成31年４月１日　一部改正

令和３年４月１日　一部改正

令和４年３月24日　一部改正

## 第１編　総則

### 第１章　通則

（趣旨）

第１条　この基準は、北海道情報セキュリティ基本方針（平成14年12月27日知事決定）第10条に基づき、道が保有、使用又は管理する情報システムの情報セキュリティ対策に関し必要な基準を定める。

（定義）

第２条　この基準において、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。

(1) 職員等

北海道情報セキュリティ基本方針第4条第2項に規定する職員並びに職員以外の者で第５条によりこの基準の適用に同意した者をいう。

(2) 侵害等

北海道情報セキュリティ基本方針第3条に規定する脅威、電子データの漏洩、不正プログラムの感染、不正アクセス、システムの障害及びその他次に掲げるものを含む情報セキュリティにおける機密性、完全性又は可用性のいずれか若しくは複数の性質を損ね又は損ねるおそれのあるあらゆる事象（以下、「情報セキュリティインシデント」と総称する。）をいう。

(3) サーバー

情報システムの構成機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持している機能を提供するもの（搭載されるソフトウェア及び直接接続され一体として扱われる周辺機器を含む。）をいう。

(4) 端末機等

ネットワークへの接続の有無にかかわらず、職員等が電子データの処理を行うために直接操作するコンピュータ（搭載されるソフトウェア及び直接接続され一体として扱われる周辺機器を含む。）のうち、次に定めるものをいう。

①Windowsパソコン

オペレーティングシステム(以下「OS」という。)に、Microsoft社製Windowsを搭載したコンピュータをいう。

②その他パソコン

OSに、UNIX又はLinuxをベースとしたソフトウェア(MacOS、GoogleChrome等)を搭載し、職員等がキーボードにより操作を行うことを主目的としたコンピュータをいう。

③携帯端末

OSに、iOS、AndroidOS及び携帯電話機能に適応したソフトウェアを搭載したスマートフォン、タブレット及びフューチャーフォンなどのコンピュータをいう。

④特定用途機器

情報の収集や分析を行うことを主目的としたセンサーや観測機器などのIoT機器をいう。

⑤その他端末

上記以外のコンピュータをいう。

(5) テレワーク端末

前号①のうち、執務室外での利用を行うことが可能な端末として、別に統括情報セキュリティ責任者が指定するものをいう。

(6) 公用スマートフォン

第４号③のうち、前号と併せて執務室外での利用を行うことが可能な端末として、別に指定するものをいう。

(7) モバイル端末

端末機等のうち、業務上の必要に応じ、執務室外に移動させて使用するもの（但し、テレワーク端末及び公用スマートフォンを除く。）をいう。

(8) 公衆通信端末

端末機等のうち、３Ｇ、ＬＴＥ及び５Ｇ等の公衆回線との通信機能を内蔵するもの（但し、公用スマートフォンを除く。）をいう。

(9) 外部記録媒体

電子データを記録するための媒体のうち、コンピュータに内蔵（但し、簡易な方法で取り外せないものに限る。）された記録媒体以外をいう。

(10)外部記録媒体点検責任者

外部記録媒体の一斉点検を行う各部等の次長、総合振興局及び振興局の副局長並びに労働委員会の総務審査課長をいう。

(11)外部の機器等

電子データ及びその記録媒体並びに当該電子データを処理若しくは伝送するための設備及び機器で、道の使用、所有又は管理に属さないものをいう。

(12)冗長化

情報システムの一部に何らかの障害が発生した場合に備え、障害発生後においても情報システム全体の機能を維持し続けられるように予備装置を平常時からバックアップとして配置し運用することをいう。

(13)不正プログラム

ウイルス、ワーム、マクロウイルス、トロイの木馬、スクリプトウイルス、スパイウェアなど、その名称及び挙動の種類を問わず、不正又は有害な動作を行う意図で作成されたソフトウェアや悪質なコードを総称していう。

(14)不正アクセス

正当なアクセス権限を有しない者による不正なコンピュータの利用又はそのような不正利用を試みる行為をいう。

(15)ログ

情報システム又は端末機等における、ハードウェアの状況、OSの動作状況、サービスの稼働状況、サービスへのアクセス状況、ユーザ認証の成功並びに失敗状況、エラーや警告の発出状況等、システムの管理作業等のために必要な電子データの記録をいう。

(16) 外部サービス

ネットワークを経由してサービス提供者が管理するサーバーを用いて利用者が情報の作成、保存又は送信等を行うサービスをいう。

(17)外部委託等

外部の事業者に行わせる情報システムの開発業務、運用業務、提供業務、保守業務、賃貸借業務、情報資産の保守業務並びに処分業務等及びその他の役務の提供を主とするサービスをいう。

(18)約款による外部サービス

ネットワークを経由してサービス提供者が管理するサーバーを用いて利用者が情報の作成、保あ存又は送信等を行うサービスのうち、広く公衆に提供されるものであり、当該サービスの開始に当たり約款への同意が必要なものをいう。

(18)ソーシャルメディアサービス

約款による外部サービスのうち、ネットワークを用いて利用者相互が情報を交換する機能を提供するサービスをいう。

(20)特定個人情報

個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。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）第７条第１項及び第２項、第８条並びに第48条並びに附則第３条第１項から第３項まで及び第５項を除く。）をその内容に含む個人情報をいう。

(21)道庁行政情報ネットワーク

LGWAN、インターネット、本庁及び出先機関を各種回線で結び、道の各種情報システムと相互に接続する基幹的な情報ネットワークをいう。

(22)相互接続システム

道庁行政情報ネットワークに接続している情報システムをいう。

(23)個別システム

道庁行政情報ネットワークと接続していない情報システムをいう。

(24)北海道自治体情報セキュリティクラウド

道及び道内市町村等のインターネット接続口を集約し、高度な情報セキュリティ対策を施して構築したシステムをいう。

(25)マイナンバー利用事務系

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及び電子データをいう。

(26)LGWAN 接続系

LGWANに接続された情報システム及びその情報システムで取り扱う電子データをいう（マイナンバー利用事務系を除く。）。

(27)インターネット接続系

インターネットに接続された情報システム及びその情報システムで取り扱う電子データをいう。

(28)通信経路の分割

LGWAN接続系とインターネット接続系の両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。

(29)特定通信

マイナンバー利用事務系、LGWAN接続系及びインターネット接続系の間において、通信元及び通信先を限定し、特定の通信だけを許可することをいう。

(30)無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

（適用範囲）

第３条　この基準は、職員等に適用する。

（職員等の一般的責務）

第４条　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、業務の遂行に当たりこの基準、この基準に基づく情報セキュリティ対策実施手順及びその他の関連規程等を遵守しなければならない。

２　職員等は、善良なる管理者の注意をもって情報資産を取り扱わなければならない。

３　職員等は、情報セキュリティに関する情報の収集に努めなければならない。

４　職員等は、研修の受講等により、情報セキュリティに関する知識を習得しなければならない。

５　職員等は、情報資産に関する情報を外部の者に漏らしてはならない。

６　職員等は、人的または技術的手段を用い、この基準に基づく情報セキュリティ対策が、意図的にその効力を失わせようとする行為をおこなってはならない。

７　前６項に定めるもののほか、職員等は、情報資産に対する情報セキュリティ上の危険性からの回避に努めなければならない。

（外部委託等の特例）

第５条　職員は、情報資産の使用、保管、処分、開発、保守又は修繕等の業務等を外部の者に行わせる場合は、当該外部の者にこの基準が適用されること、業務上知り得た情報の守秘義務及びその他の情報セキュリティ対策上必要な事項について説明し、契約の締結時までに統括情報セキュリティ責任者が別に定める方法により、当該外部の者の同意を得なければならない。

２　前項について、契約を締結しない場合においては、その外部の者が情報資産の使用等を開始する前までに、統括情報セキュリティ責任者が別に定める方法により、当該外部の者の同意を得なけれ

ばならない。

第５条の２　前条により同意した者は、統括情報セキュリティ責任者の指示に基づき、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者、その他本対策基準で定める者を置かなければならない。

## 第２章　組織体制

### 第１款　執行体制

（最高情報セキュリティ責任者）

第６条　情報セキュリティ対策を全庁的かつ総合的に実施するため、最高情報セキュリティ責任者（CISO: Chief Information Security Officer、以下「CISO」という。）を置く。

２　CISOは、情報セキュリティ対策を所管する部を担当する副知事とする。

３　CISOは、道における全ての情報セキュリティ対策に関する総括的な権限及び責任を有する。

４　CISO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ものとする。

５　CISO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。

６　CISOは、CISOを補佐し情報セキュリティ対策を全庁的かつ総合的に実施するため、最高情報セキュリティ副責任者（以下「副CISO」という。）を置く。

７　副CISOは、総合政策部次世代社会戦略監とする。

８　副CISOは、CISOの命を受けた情報セキュリティ対策の実施に関する権限及び責任を有する。

９　CISOは、本基準に定められた自らの担務を、副CISOその他の本基準に定める責任者に担わせることができる。

（統括情報セキュリティ責任者）

第７条　全庁の情報セキュリティ対策を担当する局長をCISO直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は、CISO及び副CISOを補佐しなければならない。

２　統括情報セキュリティ責任者は、道におけ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。

３　統括情報セキュリティ責任者は、道における全てのネットワークにおける情報セキュリティ対策の実施に関する権限及び責任を有する。

（統括情報セキュリティ責任者の権限）

第８条　統括情報セキュリティ責任者は、この基準の施行及び運用等に必要な細則、指針、情報セキュリティ対策ガイドライン及びその他の規程を制定する権限を有する。

２　統括情報セキュリティ責任者は、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者に対して、情報セキュリティ対策に関する指示、指導及び助言を行う権限を有する。

３　統括情報セキュリティ責任者は、道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、CISOの指示に従い、CISO及び副CISO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実施する権限及び責任を有する。

４　統括情報セキュリティ責任者は、道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。

（情報セキュリティ責任者）

第９条　情報セキュリティ対策を各部局等において適正かつ確実に行うため情報セキュリティ責任者を置く。

２　情報セキュリティ責任者は、部長、出納局長、総合振興局長、振興局長及び労働委員会事務局長とする。

３　情報セキュリティ責任者は、その所管する部局等における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。

４　情報セキュリティ責任者は、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、見直し等を行う統括的な権限及び責任を有する。

５　情報セキュリティ責任者は、その所管する部局に所属する職員に対して、情報セキュリティ対策に関する教育、訓練、指導及び助言を行わなければならない。

６　第５条に同意した者にあっては、その同意毎に情報セキュリティ責任者に相当する者を置き、統括情報セキュリティ責任者に報告しなければならない。

（情報セキュリティ管理者）

第10条　情報セキュリティ対策を各課等において適正かつ確実に実施するために、情報セキュリティ管理者を置く。

２　情報セキュリティ管理者は、次の各号に定める者とする。

(1) 本庁及び労働委員会の課長（課に相当する組織の長を含む。）

(2) 出先機関のうち課（課に相当する組織を含む。）を置くものにあっては当該出先機関の課長

(3) 出先機関のうち課を置かないものにあっては当該出先機関の長

３　情報セキュリティ管理者は、その所管する課等における情報セキュリティ対策の実施に関する権限及び責任を有する。

４　情報セキュリティ管理者は、その所管する課等における情報セキュリティ対策の実施並びに状況の把握及び職員に対する教育、訓練、指導並びに助言を行わなければならない。

５　情報セキュリティ管理者は、自らが新たに就任した場合及び情報システム管理者並びに第14条で定める補助者に変更が生じたときは、速やかに全庁の情報セキュリティ対策を所管する課長に対し報告しなければならない。

６　情報セキュリティ管理者は、その所掌する課室等において、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、統括情報セキュリティ責任者及びCISOへ速やかに報告を行い、指示を仰がなければならない。

（情報セキュリティ副管理者）

第10条の２　情報セキュリティ管理者は、情報セキュリティ対策を各課等において適正かつ確実に実施するため、その所管する課等における管理職員から情報セキュリティ副管理者を１名指定することができる。

２　情報セキュリティ管理者は、人事異動や事故等によるやむを得ない場合を除き、在任中一度指定した情報セキュリティ副管理者を変更することは出来ない。

3　情報セキュリティ副管理者は、情報セキュリティ管理者が不在の際、情報セキュリティ管理者の任を代わりに担うものとする。

4　情報セキュリティ副管理者は、前項の規定により情報セキュリティ管理者の職務を担ったときは、情報セキュリティ管理者の復帰後、直ちに報告しなければならない。

（情報システム管理者）

第11条　各情報システムにおける情報セキュリティ対策を適正かつ確実に実施するため、情報システム管理者を置く。

2　情報システム管理者は、次の各号に該当する者でかつ情報システムの開発又は運用を所管する者とする。

(1) 本庁及び労働委員会の課長（課に相当する組織の長を含む。）

(2) 出先機関のうち課（課に相当する組織を含む。）を置くものにあっては当該出先機関の課長

(3) 出先機関のうち課を置かないものにあっては当該出先機関の長

3　情報システム管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

4　情報システム管理者は、その所管する情報システムにおける情報セキュリティ対策を実施する権限及び責任を有する。

5　情報システム管理者は、その所管する情報システムにおける情報セキュリティ対策の実施並びに状況の把握及び当該情報システムの開発又は運用を担当する職員の情報セキュリティ対策に関する知識習得の支援を行わなければならない。

（補助者の設置）

第12条　情報セキュリティ管理者及び情報システム管理者は、その所管する情報セキュリティ対策を実施するため、指定した職員に補助させることができる。

2　前項の補助者の名称は各々、情報セキュリティ担当者及び情報システム担当者とする。

（情報セキュリティ委員会）

第13条　情報セキュリティ対策を全庁的かつ統一的に実施するため、情報セキュリティ委員会を設置する。

2　情報セキュリティ委員会の構成員は、CISO、副CISO、統括情報セキュリティ責任者及び情報セキュリティ責任者とする。

3　情報セキュリティ委員会は、CISOが招集する。

4　情報セキュリティ委員会は、次の各号に掲げる案件を所掌する。

(1) 情報セキュリティ対策に関する年間計画の承認

(2) 前号の計画の実施結果報告の承認

(3) この基準の改廃に関する承認（組織機構の改正に伴う所属名若しくは職名の変更、その他軽微な変更を除く。）

(4) その他情報セキュリティ対策に関する重要事項の承認

5　CISOは、委員会を招集する暇がないと認めるときは、持ち回りにより決議を行うことができる。

6　情報セキュリティ委員会の事務局は、総合政策部次世代社会戦略局情報政策課に置く。

（兼務禁止の原則）

第14条　職員は、情報セキュリティ対策に関する手続において、承認若しくは許可の申請者とその承認者若しくは許可者又は監査を受ける者とその監査を実施する者を兼務してはならない。

２　職員は、情報セキュリティ監査の実施において、監査を受ける者とその監査を実施する者を兼務してはならない。

３　前項の規定にかかわらず、代替的措置のないやむを得ない事情により、承認若しくは許可の申請者とその承認者若しくは許可者、監査を受ける者とその監査を実施する者を兼ねる必要がある場合は、これらを兼ねることができる。

（CSIRTの設置・役割）

第15条　CISOは、CSIRTを整備し、その役割を明確化しなければならない。

２　前項の組織は、CISOに直属するものとする。

３　前２項に定めるもののほか、CSIRTの運営等に関する事項については、統括情報セキュリティ責任者が別途定める。

第２款　監査体制

（情報セキュリティ監査責任者）

第16条　CISOは、情報セキュリティ対策を所管する部の次長を情報セキュリティ監査責任者とし、監査を統括させなければならない。

（情報セキュリティ監査責任者の任務）

第17条　情報セキュリティ監査責任者は、情報セキュリティ対策の実施状況及び第４条に規定する責務の履行状況について監査を行う権限を有する。

（情報セキュリティ監査担当者）

第18条　情報セキュリティ監査責任者は、全庁の情報セキュリティ対策を所管する課の職員を情報セキュリティ監査担当者として、監査を実施させることができる。

第３章　情報資産

（情報資産の管理責任）

第19条　情報セキュリティ管理者は、その所管する課等に配置された情報資産及びその所管する課等の職員が利用する情報資産について管理責任を負う。

２　情報システム管理者は、所管する情報システムに係る情報資産について管理責任を負う。

３　職員等は、前２項の管理責任の履行に協力しなければならない。

（情報セキュリティ対策の実施義務）

第20条　情報セキュリティ管理者及び情報システム管理者は、統括情報セキュリティ責任者と連携して、情報資産に対する脅威となり得る事項の把握に努めるとともに、適正な情報セキュリティ対策を実施しなければならない。

（情報の作成）

第21条　職員等は、業務上の必要なく電子データを作成し又は複製してはならない。

２　職員等は、作成途上の文書（電子文書を含む。以下同じ。）や資料的文書も含め、作成、複製又は保管している電子データについて紛失や流出等のないよう適正に取り扱わなければならない。

（情報資産の利用）

第22条　職員等は、業務目的以外に情報資産を使用してはならない。

（情報資産の保管）

第23条　職員等は、個人情報を含む電子データ等、取り扱う電子データの性質に応じて、当該電子データに対してパスワード設定又は暗号化等の処理を行わなければならない。

２　職員等は、テレワーク端末及び公用スマートフォンに内蔵されている記録媒体について、暗号化の処理を行いパスワードを設定しなければならない。

３　職員等は、長期的に保管する電子データ及び最終的に確定した電子データについては、上書不能な記録媒体に保管するか又は記録媒体に対し書込禁止の処理を行わなければならない。

４　情報セキュリティ管理者又は情報システム管理者は、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電子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、バックアップ元の情報システムと同時に自然災害を被る可能性が低い地域に保管するよう努めなければならない。

（電子データの送信）

第24条　職員は、電子メール等により電子データを送信する場合は、取り扱う電子データの重要度に応じ、パスワード設定等の情報漏洩防止対策を講じなければならない。

（情報資産の廃棄）

第25条　記録媒体を含む情報資産を処分するときは、職員は、外部の者によって記録媒体の電子データを復元され情報が流出することを防止するため、電子データの完全消去を行うための専用ソフトウェアの使用、記録媒体の物理的な破壊又は専用装置による電気的若しくは磁気的な塗りつぶしによる消去等を行い、記録媒体の電子データの復元が完全に不可能な状態に処置しなければならない。

２　情報資産の廃棄を行う者は、情報セキュリティ管理者又は情報システム管理者の承認を得なければならない。

３　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。

## 第４章　情報システム全体の強靭性の向上

（マイナンバー利用事務系）

第26条　統括情報セキュリティ責任者は、マイナンバー利用事務系と他の領域を通信できないようにしなければならない。ただし、マイナンバー利用事務系が外部との通信をする必要がある場合は、通信経路の限定(MAC アドレス、IPアドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、インターネット等からLGWAN-ASP を経由してマイナンバー利用事務系に電子データの取り込みを可能とする。

２　マイナンバー利用事務系は、情報システムが正規の利用者であることを判断する認証手段のうち、二つ以上を併用する多要素認証を利用しなければならない。

３　マイナンバー利用事務系は、原則として、外部記録媒体による端末機等からの情報持ち出しがで

きないように設定しなければならない。

（LGWAN接続系）

第27条　LGWAN接続系とインターネット接続系の両環境間の通信環境を分離した上で、必要な通信のみ許可できるようにしなければならない。なお、メールや電子データをLGWAN 接続系に取り込む場合は、次の各号による手法を用い、統括情報セキュリティ責任者が指定する方法により、無害化通信を図らなければならない。

(1) インターネット環境で受信したインターネットメールの本文のみをLGWAN接続系に転送するメールテキスト化方式

(2) インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

(3) 危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

２　LGWAN接続系を利用可能な情報システムは、道庁行政情報ネットワーク及び相互接続システムとする。

（インターネット接続系）

第28条　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及び他のネットワークへの不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

２　インターネットとの通信は、道及び市区町村のインターネットとの通信を集約する自治体情報セキュリティクラウドを経由するよう努めるとともに、関係省庁や都府県等と連携しながら、情報セキュリティ対策を推進しなければならない。

３　業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末と入札情報や職員の情報等重要な情報資産を配置する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施するよう努めなければならない。

（インターネット直接接続端末）

第28条の２　情報システム管理者及び情報セキュリティ管理者は、前条のネットワークを経由せず、端末機等を直接インターネットに接続してはならない。

２　前項の規定にかかわらず、業務の遂行上やむを得ない理由によりインターネットに端末機等を直接接続する必要がある場合、情報セキュリティ管理者は、接続を行う前に次の各号に掲げる事項を含めた端末機の利用に関する規程の案を作成し、統括情報セキュリティ管理者の承認を得なければならない。また、端末機等において、個人情報等の重要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) 当該端末機等を利用してよい業務の範囲

(2) 当該端末機等で取り扱うことができる情報の範囲

(3) 当該端末機等利用手続及び運用手順

３　統括情報セキュリティ責任者は、情報セキュリティの観点から、業務の遂行上やむを得ないと認められる場合に限り、前項の承認を行うことができる。

４　前３項の規定は、公衆通信端末の購入に準用する。

５　情報セキュリティ管理者は、前２項に基づき承認を受けた端末機等の利用状況について、統括情報セキュリティ責任者が別に定める内容に基づき、毎年報告しなければならない。

## 第２編　情報セキュリティ対策

### 第１章　物理的セキュリティ対策

#### 第１款　サーバー等の管理

（機器の取付）

第29条　情報システム管理者は、サーバー等の重要な情報処理機器の取付けに当たっては、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の必要な措置を講じなければならない。

（冗長化の原則）

第30条　情報システム管理者は、重要な情報を保存しているサーバー、セキュリティサーバー、住民サービスに関するサーバー及びその他の重要なサーバーを冗長化し、同一電子データを保持しなければならない。

２　情報システム管理者は、メインサーバーに障害が発生した場合に、速やかにセカンダリサーバーを起動し、システムの運用停止時間を最小限にしなければならない。

３　やむを得ない事情により前項のサーバーの冗長化ができない場合は、情報システム管理者は、電子データの喪失を防止するために必要な措置を講じなければならない。

（機器の電源）

第31条　情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、サーバ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るよう努めなければならない。

２　情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、落雷等による過電流に対して、サーバー等の機器を保護するための措置を講じるよう努めなければならない。

（通信ケーブル等の配線）

第32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、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るよう努めなければならない。

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、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

３　統括情報セキュリティ責任者及び情報システム管理者は、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正に管理しなければならない。

４　統括情報セキュリティ責任者、情報システム管理者は、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講じなければならない。

（機器の定期保守）

第33条　情報システム管理者は、サーバー等の重要な機器について、定期的に保守点検を実施しなけ

ればならない。

2　前項の保守点検を委託等により外部の者に行わせるときは、情報システム管理者は、第5条の規定に従わなければならない。

（機器の修理）

第34条　情報システム管理者は、電子データを内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報システム管理者は、外部の事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

（庁外への機器の設置）

第35条　庁外にサーバー等の機器を設置する際は、この基準が求める物理的セキュリティの要件を満たす等適正な情報セキュリティ対策が実施されている場所に設置しなければならない。

2　情報システム管理者は、 庁外にサーバー等の機器を設置する場合は、事前に前項の情報セキュリティ対策状況を確認しなければならない。

3　情報システム管理者は、庁外にサーバー等の機器を設置したときは、統括情報セキュリティ責任者に報告しなければならない。

（機器の廃棄等）

第36条　情報システム管理者は、機器を廃棄又はリース物件の返却等をするときは、当該機器に対して第25条の処置を施さなければならない。

第２款　管理区域

（管理区域）

第37条　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部屋や電磁的記録媒体の保管庫をいう。

2　統括情報セキュリティ責任者及び情報システム管理者は、管理区域を地階又は１階に設けないよう努めなければならない。また、外部からの侵入が容易にできないように無窓の外壁とするよう努めなければならない。

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、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止するよう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、管理区域内の機器等に、転倒並びに落下防止等の耐震対策、防火措置及び防水措置等の必要な措置を講じなければならない。

5　統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部を全て塞ぐよう努めなければならない。

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、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努めなければならない。

7　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、管理区域に対し、外部の者が管理区域であることを判断できる表示を行ってはならない。

（管理区域の施錠及び監視）

第38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、管理区域を常時施錠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又は情報システム管理者は、個人番号利用事務系の機器等を設置する特に重要な管理区域については、監視カメラを設置して監視を行わなければならない。

（入退室管理）

第39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、管理区域への入退室を許可された者のみに制限し、入退室管理簿の記録及びICカード等による入退室管理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又は情報システム管理者は、事業者等が管理区域に入室する必要がある場合は、身分証明書等の本人確認ができる書証を常時携帯させ、必要の都度、その提示を求め確認しなければならない。

（部外者の入室禁止）

第40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、管理区域内に部外者を入室させてはならない。

２　前項の規定にかかわらず、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、部外者を管理区域内に入室させる特別の必要性がある場合には、必要に応じて立ち入り区域を制限するとともに、管理区域への入退室を許可された職員を常時付き添わせなければならない。

３　前項の場合において、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、管理区域への入室を認めた部外者に対し、外見上職員と区別できる措置を講じなければならない。

（目的外機器の持込禁止）

第41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、管理区域内に設置された情報システムに関連しない、又は職員個人所有のコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等電子データの持込又は持出が可能な物品を持ち込ませてはならない。

（機器等の搬入出）

第42条　情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は委託した業者に確認を行わせなければならない。

２　情報システム管理者は、管理区域内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。

（管理区域の代替措置）

第43条　情報システム管理者は、やむを得ない事情により管理区域の確保が不可能な場合は、サーバー等の主要な機器を扉付きのラックに装着し常時施錠管理しなければならない。

２　前項の場合においては、情報システム管理者は、ラックを強固に固定し、転倒又は機器の落下等を未然に防止しなければならない。

（通信回線及び通信回線装置の管理）

第44条　統括情報セキュリティ責任者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理するよう努めなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管するよう努めなければならない。

２　統括情報セキュリティ責任者は、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。

3　統括情報セキュリティ責任者は、個人情報等重要な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　統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上で情報の破壊、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　統括情報セキュリティ責任者は、個人情報等重要な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３款　外部記録媒体の管理

（外部記録媒体の管理責任）

第45条　情報セキュリティ管理者は、外部記録媒体の紛失、盗難の防止及び保管している電子データの漏洩防止のために必要な措置を講じなければならない。

2　情報セキュリティ管理者は、外部記録媒体に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。

3　情報セキュリティ管理者は、外部記録媒体を新たに調達する場合は、パスワード設定機能又は電子データ暗号化機能を備えた媒体の調達に努めなければならない。

4　情報セキュリティ管理者は、パスワード設定機能又は電子データ暗号化機能を備えていない外部記録媒体に対し、運用上やむを得ない場合を除き、ＯＳの標準機能を用いた電子データ暗号化機能を適用しなければならない。

5　職員は、パスワード設定機能又は電子データ暗号化機能を備えた外部記録媒体の使用に当たっては、当該機能を有効に活用しなければならない。

（外部記録媒体の管理方法）

第46条　情報セキュリティ管理者は、所管する外部記録媒体の数量、配置箇所等の使用状況を常に把握し、管理簿により管理しなければならない。

2　情報セキュリティ管理者は、執務室等に職員がいない時は、電子データを記録した外部記録媒体を施錠管理又は固定するなど、紛失・盗難が発生しないよう適切に管理しなければならない。

3　情報セキュリティ管理者は、電子データを記録した外部記録媒体を外部の者に貸与する場合は、貸与の都度、複製の禁止及び媒体管理等に関する取り決め事項を定め、当該外部の者の文書による同意を得るとともに、同意の内容を適正に保管しなければならない。

（外部記録媒体の持出及び持込）

第47条　職員等は、外部記録媒体を執務室外に持ち出し又は所管外の外部記録媒体を執務室内に持ち込んではならない。

2　前項の規定にかかわらず、職員は、業務上外部記録媒体の持ち出し又は持ち込みが必要な場合は、その理由及び内容を当該外部記録媒体を管理する情報セキュリティ管理者に申告し、許可を得なければならない。

3　前項の持ち出し又は持ち込みが庁舎外に及ぶ場合は、職員は、情報セキュリティ管理者の文書による許可を得なければならない。また、情報セキュリティ管理者は、許可の内容を適正に保管しな

ければならない。

４　前３項の規定は、次の各号に掲げる場合においては、これを適用しない。

(1) 国若しくは他の地方公共団体との間又は内部で行われる調査若しくは照会の依頼又は回答等に際して電子データを外部記録媒体に複製して提出する場合。

(2) 道の施策等に関する広報等の目的をもって外部記録媒体を不特定多数の者に配布する場合。

（一斉点検の実施）

第48条　外部記録媒体点検責任者は、統括情報セキュリティ責任者の定めるところにより、所管する外部記録媒体の管理状況について一斉点検を行わなければならない。

２　外部記録媒体点検責任者は、一斉点検の結果を統括情報セキュリティ責任者及び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、一斉点検の結果を取りまとめの上、CISOに報告しなければならない。

（随時点検の実施）

第49条　外部記録媒体点検責任者は、自ら必要と認めるときは、随時に所管する外部記録媒体の管理状況について点検を行うことができる。

２　統括情報セキュリティ責任者は、必要に応じ外部記録媒体点検責任者に対して随時点検の実施を求めることができる。

３　前２項の点検の方法等は、統括情報セキュリティ責任者が別途定める。

（端末の管理）

第50条　第45条、第46条、第48条及び前条の規定は、モバイル端末について準用する。

２　前５条の規定は、携帯端末及びその他端末について準用する。

## 第２章　人的セキュリティ対策

### 第１款　職員等の遵守事項

（対策基準等の遵守）

第51条　職員等は、本対策基準及び各情報システムにおける実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

（業務以外の目的での使用の禁止）

第52条　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。

（端末機等の持出等の取扱い）

第53条　職員等は、端末機等（但し、テレワーク端末及び公用スマートフォンを除く。）及び外部記録媒体並びにその他の情報資産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が別に定める規定に基づき、情報セキュリティ管理者の許可を得なければならない。

２　職員等は、統括情報セキュリティ責任者が別に定める規定に基づき、テレワーク端末及び公用スマートフォンを執務室外に持ち出すことができる。

（支給以外機器等の使用禁止）

第54条　職員等は、支給された端末機等以外の外部の機器等を業務に利用してはならない。

２　前項の規定にかかわらず、やむを得ず外部の機器等を業務で使用する場合には、職員等は、外部の機器等で情報処理作業を行う際の安全管理措置に関する規定を遵守するとともに、情報システム管理者の許可を得なければならない。

３　前２項の規定は、情報資産に対する侵害等の発生に際し、当該侵害等の分析及び復旧等の作業を受託した事業者が、当該分析及び復旧等のために必要な専用機器等を使用する場合には、これを適用しない。

（持ち出し及び持ち込みの記録）

第55条　情報セキュリティ管理者は、端末等の持ち出し及び持ち込みについて、統括情報セキュリティ責任者が別に定める規定に基づき、記録を作成し、保管しなければならない。

（端末機等の現状変更の禁止）

第56条　職員等は、情報システム管理者の許可を得ずに端末機等の改造、増設若しくは交換、ネットワークとの切り離し若しくは接続等、現状を変更する行為を行ってはならない。

（情報資産の管理）

第57条　職員等は、自己が利用する情報資産が第三者に使用され、情報セキュリティ管理者の許可なく情報を閲覧され若しくは盗難され又は紛失することがないよう、容易に閲覧されない場所への保管等、適正な取扱いを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、テレワーク端末及び公用スマートフォンにおける電子データの暗号化等の機能を有効に利用しなければならない。また、端末にセキュリティチップが搭載されている場合、その機能を有効に活用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、テレワーク端末及び公用スマートフォンの業務利用を認める際は、前号の対策に加え、遠隔消去機能を利用する等の措置を講じなければならない。

（退職時等の遵守事項）

第58条　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。

（情報セキュリティ管理者の指導義務）

第59条　情報セキュリティ管理者は、所属の職員等に対して、情報セキュリティ基本方針、この基準、この基準に基づく情報セキュリティ対策実施手順及びその他の関連規程等の遵守を指導しなければならない。

(非常勤及び会計年度任用職員への対応)

第60条　情報セキュリティ管理者は、所属の非常勤及び会計年度任用職員に対し、採用時に情報セキュリティに関して守るべき内容を理解させ、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、非常勤及び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を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。

（電子メールの利用制限）

第61条　職員等は、情報システム管理者から与えられた電子メールアドレス以外の電子メールアドレスを業務目的で使用してはならない。

２　前項の規定にかかわらず、やむをえない事情により業務目的で他の電子メールアドレスを利用する場合、職員等は、あらかじめ利用する電子メールアドレスについて情報セキュリティ管理者の許可を受けなければならない。

３　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。

４　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。

５　職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。

６　本条の規定は、外部委託等を受託した事業者には、これを適用しない。

（無許可プログラムの導入禁止）

第62条　職員等は、情報セキュリティ管理者又は情報システム管理者の許可を得ていないプログラムを端末機等に導入してはならない。

（無許可でのネットワーク接続の禁止）

第63条　職員等は、統括情報セキュリティ責任者の許可を得ることなく端末機等をネットワークに接続させてはならない。

（インターネットサイト閲覧の制限）

第64条　職員等は、業務目的以外でインターネットサイトを閲覧してはならない。

２　職員は、他の職員等が業務目的以外でインターネットサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に報告しなければならない。

３　前項の報告を受けた情報セキュリティ管理者は、適正な措置を講ずるとともに、必要に応じ統括情報セキュリティ責任者に協議しなければならない。

（設定変更の禁止）

第65条　職員等は、情報システムの情報セキュリティに関する設定を情報システム管理者の許可なく変更してはならない。

（この基準等の掲示）

第66条　統括情報セキュリティ責任者は、職員等が常に情報セキュリティ基本方針及びこの基準を閲覧できるようにしなければならない。

第２款　研修及び訓練

（情報セキュリティに関する研修）

第67条　統括情報セキュリティ責任者は、職員等を対象として定期的に情報セキュリティ対策に関する研修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、前項に定める研修が各職員等の業務経験、役割及び情報セキュリティに関する理解度等に応じた内容となるよう努めなければならない。

３　前２項に定めるもののほか、情報セキュリティ管理者及び情報システム管理者は、所管する職員等に対し、情報セキュリティ対策に関する研修を実施することができる。

４　職員等は、定められた研修に参加しなければならない。

（研修計画の策定）

第68条　統括情報セキュリティ責任者は、幹部を含め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を策定しなければならない。

２　研修計画において、職員等は毎年度最低１回は情報セキュリティ研修を受講できるようにしなければならない。

３　新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

４　研修は、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者及び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するよう努めなければならない。

（研修実施状況の報告）

第69条　情報セキュリティ管理者及び情報システム管理者は、第67条第３項に基づき研修を実施した場合は、実施後速やかに、当該研修の実施状況を統括情報セキュリティ責任者に報告しなければならない。

（緊急時対応訓練）

第70条　統括情報セキュリティ責任者は、定期的に緊急時の対応を想定した訓練を実施しなければならない。

２　前項に定めるもののほか、情報セキュリティ管理者及び情報システム管理者は、各々が所属の職員を対象とした訓練を実施することができる。

３　前２項の場合において、統括情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者は、訓練の計画策定に当たり、ネットワーク並びに情報システムの規模等を考慮して訓練実施の体制及び範囲等を定め、訓練の効果的な実施を図らなければならない。

４　全ての職員は、定められた訓練に参加しなければならない。

第３款　情報セキュリティインシデントの報告

（庁内での情報セキュリティインシデントの報告）

第71条　職員等は、情報システムの異常や情報セキュリティインシデントを認知した場合、速やかに情報情報セキュリティ管理者に報告しなければならない。

２　情報セキュリティ管理者は、前項の報告を受けたときは、情報システム管理者と協議の上、その状況について、速やかに統括情報セキュリティ責任者に報告しなければならない。

（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）

第72条　職員等は、道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に報告しなければならない。

２　情報セキュリティ管理者は、前項の報告を受けたときは、情報システム管理者と協議の上、その状況について、速やかに統括情報セキュリティ責任者に報告しなければならない。

（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）

第73条　CSIRTは、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

２　CSIRT は、情報セキュリティインシデントであると評価した場合、CISO に速やかに報告しなければならない。

３　CSIRT は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。

４　CSIRT は、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の結果から、再発防止策を検討し、CISO に報告しなければならない。

５　CISO は、CSIRT 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款　ID及びパスワード等の管理

(ICカード等の取扱い)

第74条　職員等は、自己が使用するICカード等に関し、次の事項を遵守しなければならない。

(1) 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。

(2) 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又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。

(3) IC カード等を紛失した場合には、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。

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、ICカード等の紛失等の報告があり次第、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。

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、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

(IDの取扱い)

第75条　職員等は、自己が使用するIDに関し、次の事項を遵守しなければならない。

(1) 自己が使用しているIDを他人に使用させてはならない。

(2) 端末機や机上等、職員等以外の第三者が閲覧出来る場所にIDを表示してはならない。

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

(パスワードの管理)

第76条　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) 自己が使用しているパスワードを他人に使用させてはならない。

(2) パスワードを他者に知られないように管理するとともに、端末機や机上等、第三者が閲覧可能な場所に表示してはならない。

(3) 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。

(4) 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。

(5) パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パ

スワードを速やかに変更しなければならない。

(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（初期パスワード含む）は、最初のログイン時点で変更しなければならない。

(8) サーバー、ネットワーク機器及びパソコン等の端末機に、パスワードの入力を省略することを目的として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３章　技術的セキュリティ対策

### 第１款　コンピュータ及びネットワークの管理

（技術の活用）

第77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、情報システムのより高度な安全性及び信頼性を確保するため、常に最新の情報技術に関する情報の収集及び知識の習得及びその評価に努めなければならない。

（バックアップの実施）

第78条　情報システム管理者は、サーバー等に記録された電子データについて、定期的なバックアップを実施しなければならない。

（情報交換の制限）

第79条　職員は、他の団体と情報システムに関する情報を交換する場合は、開示する情報の内容を明確に示した上で、情報セキュリティ管理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　前項の場合において、開示する情報の内容が道全体にわたる場合は、職員は、情報システム管理者及び情報セキュリティ管理者を経由の上、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。

（システム管理記録及び作業の確認）

第80条　情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

２　情報システム管理者は、所管するシステムにおいて、システム改修等の変更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、情報システム担当者又は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改修等の変更作業を行う場合は、2名以上で作業し、互いにその作業を確認するよう努めなければならない。

（仕様書等の管理）

第81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、帳票、情報システムの仕様書及びその他の情報システムに関連する文書について、業務上必要とする者以外の者が閲覧することのないよう適正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は、前項に定める文書を当該情報システムが存続する限り保持しなければならない。

（ログの取得）

第82条　統括情報セキュリティ責任者及び情報システム管理者は、各種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、適正に管理及び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、テレワーク端末及び公用スマートフォンに対し、位置情報や操作履歴など詳細なログの取得が可能なモバイルデバイスマネジメントシステムを導入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、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。

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、取得したログを必要に応じ点検し、不正侵入、不正操作並びにその他の攻撃行為の有無及び方法等について分析しなければならない。

（障害記録）

第83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。

（ネットワークの接続制御、経路制御等）

第84条　情報システム管理者は、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。

2　情報システム管理者は、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。

（外部の者が利用できるシステムの分離等）

第85条　情報システム管理者は、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。

（外部ネットワークとの接続制限等）

第86条　ネットワークを管理する情報システム管理者は、所管するネットワークを所管外のネットワーク（以下、「外部のネットワーク」という。）と接続する場合には、当該外部ネットワークの構成及びセキュリティの状況を調査し、情報資産に影響が生じないことを確認した上で、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は、接続した外部ネットワークの瑕疵により電子データの漏えい、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　情報システム管理者は、ウェブサーバー等をインターネットに公開する場合、内部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は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに

当該外部ネットワークを物理的に遮断しなければならない。

（複合機のセキュリティ管理）

第87条　統括情報セキュリティ責任者は、プリンター、スキャナ、コピー及びＦＡＸ機能のうち複数の機能がついた機器（以下、「複合機」という。）を調達する場合、当該複合機が備える機能及び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、適正なセキュリティ要件を策定しなければならない。

２　統括情報セキュリティ責任者は、複合機が備える機能について適正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。

３　情報セキュリティ管理者は、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。

（特定用途機器のセキュリティ管理）

第88条　統括情報セキュリティ責任者は、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講じなければならない。

（無線LAN 及びネットワークの盗聴対策）

第89条　情報システム管理者は、所管するシステムで無線LANを利用する場合、解読が困難な暗号化及び認証技術を使用しなければならない。

２　情報セキュリティ管理者は、前項により無線 LAN を利用する場合については、あらかじめ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。

３　統括情報セキュリティ責任者は及び情報システム管理者は、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。

（電子メールのセキュリティ管理）

第90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、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、電子メールサーバー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及び情報システム管理者は、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、メールサーバー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及び情報システム管理者は、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。

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。

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、システム開発や運用、保守等のため庁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。

（電子メールアドレスの漏洩対策）

第91条　情報システム管理者は、職員等が複数人に電子メールを送信した場合、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を分からなくするシステム上の措置を講じるよう努めなければならない。

（電子署名・暗号化）

第92条　職員等は、外部に送る電子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、情報セキュリティ統括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　職員等は、暗号化を行う場合に統括情報セキュリティ責任者が定める以外の方法を用いてはならない。また、情報セキュリティ統括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。

３　情報セキュリティ統括責任者は、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。

（許可ソフトウェアの導入）

第93条　職員等は、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が別に定める規定に基づき、端末機等にソフトウェアを導入することができる。

２　前項に基づき端末機等にソフトウェアを導入する際は、情報セキュリティ管理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。

（機器構成の変更）

第94条　職員等は、業務上、端末機等に対し改造及び増設・交換を行う必要がある場合には、情報システム管理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、端末機等の構成を把握するシステム上の措置を講じるよう努めなければならない。

（無許可でのネットワーク接続の禁止）

第95条　職員等は、統括情報セキュリティ責任者の許可なく端末機等を外部の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96条　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　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、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適正な措置を求めなければならない。

第２款　アクセス制御

（アクセス制御）

第97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。

（アクセス制御の設定）

第98条　情報システム管理者は、情報システムへのログインに際し、パスワード、IC カード又は生体認証等認証情報の入力を必要とするように設定しなければならない。また、取り扱う電子データの重要性に応じ、複数の認証情報の入力を必要とするように設定するよう努めなければならない。

（利用者IDの取扱い）

第99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、統括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。

３　統括情報セキュリティ責任者及び情報システム管理者は、利用されていないIDが放置されないよう、人事管理部門と連携し、点検しなければならない。

（特権を付与されたIDの管理等）

第100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は、代行者を認めた場合、速やかに統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者に通知しなければならない。

４　統括情報セキュリティ責任者及び情報システム管理者は、特権を付与されたID及びパスワードについて、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。

５　統括情報セキュリティ責任者及び情報システム管理者は、特権を付与されたIDを初期設定以外のものに変更しなければならない。

（外部からのアクセスの制限）

第101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、内部の情報システム又はネットワーク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。

（職員等による外部からのアクセス等の制限）

第102条　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、統括情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

２　情報システム管理者は、職員等に対し外部から内部のネットワーク又は情報システムへのアクセスを許可する場合には、あらかじめ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。

３　情報システム管理者は、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。

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、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。

５　統括情報セキュリティ責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

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、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。

７　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庁内のネットワークに接続する前に、不正プログラムに感染していないこと、パッチの適用状況等を確認し、情報セキュリティ管理者の許可を得てから接続しなければならない。

８　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。ただし、やむを得ず接続を許可する場合は、利用者のID、パスワード及び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。

（自動識別の設定）

第103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システムを設定するよう努めなければならない。

（ログイン時の表示等）

第104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及びログイン・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等がログインしたことを確認することができるようシステムを設定するよう努めなければならない。

（認証情報の管理）

第105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、職員等の認証情報を厳重に管理しなければならない。認証情報ファイルを不正利用から保護するため、OS等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

２　統括情報セキュリティ責任者又は情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させなければならない。

３　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、認証情報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。

（特権による接続時間の制限）

第106条　情報システム管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

第３款　情報システムの開発、導入及び保守等

（情報システムの調達）

第107条　情報セキュリティ管理者及び情報システム管理者は、情報システムを新たに調達又は更新しようとするときは、

次の各号に掲げる事項について事前に検討し、これらに適合する情報システムを選定するよう努めなければならない。

(1) 行政サービスの質的な向上

(2) 業務の簡素化、効率化、経費の節減

(3) 情報セキュリティの確保

2　情報セキュリティ管理者及び情報システム管理者は、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。

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、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

4　情報システム管理者は、設計、製造、テスト及び導入後の運用の各段階において、情報セキュリティ機能の品質を適正に管理しなければならない。

（システム開発における責任者及び作業者の特定）

第108条　情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための規則を確立しなければならない。

（システム開発における責任者、作業者のIDの管理）

第109条　情報システム管理者は、システム開発の責任者及び作業者が使用するIDを管理し、開発完了後、開発用IDを削除しなければならない。

2　情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

（情報システムの導入）

第110条　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するよう努めなければならない。

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。

3　情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

4　情報システム管理者は、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。

（情報システムのテスト）

第111条　情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

2　情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行うよう努めなければならない。

3　情報システム管理者は、個人情報及び機密性の高い電子データを、テストデータに使用してはならない。

（資料等の整備及び保管）

第112条　情報システム管理者は、情報システムの開発並びに保守に関する資料及びシステム関連文書を整備の上、当該システムが存続する間、適正に保管しなければならない。

2　情報システム管理者は、テスト結果を一定期間保管しなければならない。

３　情報システム管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

（情報システムにおける入出力データの正確性の確保）

第113条　情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

２　情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計するよう努めなければならない。

３　情報システム管理者は、情報システムから出力される電子データについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

（情報システムの変更管理）

第114条　情報システム管理者は、情報システムを変更した場合は、仕様書等の変更履歴を作成しなければならない。

（開発・保守用のソフトウェアの更新等）

第115条　情報システム管理者は、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。

（更新時等の検証）

第116条　情報システム管理者は、情報システムの更新並びに統合時における管理体制の構築、移行基準の明確化及び更新並びに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款　不正プログラム対策

（不正プログラムの侵入防止）

第117条　情報システム管理者は、外部のネットワークを経由した電子データの受信又はダウンロード等を行う場合は、当該電子データが内部のネットワークに至る以前に不正プログラムの検査を行い、不正プログラムの内部のネットワークへの侵入防止に努めなければならない

（不正プログラムの拡散防止）

第118条　情報システム管理者は、外部のネットワークを経由して電子データを送信する場合は、当該電子データが外部のネットワークに至る以前に不正プログラムの検査を行い、不正プログラムの外部ネットワークへの拡散防止に努めなければならない

（不正プログラムの注意喚起）

第119条　統括情報セキュリティ責任者は、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。

２　統括情報セキュリティ責任者が提供するコンピュータウイルス等の不正プログラム情報を、常に確認しなければならない。

（不正プログラム対策ソフトウェア）

第120条　情報システム管理者は、所管するサーバー及び端末機等に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。

２　情報システム管理者は、職員が不正プログラム対策ソフトウェア及びそのパターンファイルを常に最新の状態に保つことができるよう環境を整備しなければならない。

３　職員等は、不正プログラム対策ソフトウェア及びそのパターンファイルを常に最新の状態に保たなければならない。

（サポート期限切れソフトウェアの利用禁止）

第121条　統括情報セキュリティ責任者は、業務上やむを得ない場合を除き、システム管理者に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させてはならない。

（ネットワークに接続していないシステムの不正プログラム対策）

第122条　情報システム管理者は、ネットワーク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、情報セキュリティ管理者が管理している外部記録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。

（不正プログラム対策ソフトウェアの管理）

第123条　不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、職員等に当該権限を付与してはならない。

２　職員等は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。

（電子データの授受）

第124条　職員等は、外部から電子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の検査を行わなければならない。

２　職員等は、差出人が不明又は不自然に添付された電子メール等を受信した場合は、速やかに削除しなければならない。

３　職員等は、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。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルをLGWAN 接続系に取り込む場合は無害化しなければならない

（不正プログラムへの対処）

第125条　職員等は、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、即座にLANケーブルの取り外しや通信を行わない設定への変更を行わなければならない。

（全ディスク検査の実施）

第126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、必要に応じ、端末機等に対する不正プログラム対策ソフトウェアによる全ディスクの検査を職員等に指示することができる。

（専門家への意見聴取）

第127条　統括情報セキュリティ責任者は、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体制の整備に努めなければならない。

### 第５款　不正アクセス対策

（不正アクセス対策）

第128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に対して、不正アクセスを防止するため、次の各号の措置を講じなければならない。

①使用されていない物理ポートを閉鎖しなければならない。また、閉鎖が困難な場合においては、認証技術等を用いネットワークへの不正アクセスを防止する措置を講じなければならない。

②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。

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、電子データの書換えを検出し、統括情報セキュリティ責任者及び情報システム管理者へ通報するよう、設定するよう努めなければならない。

④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するよう努めなければならない。

⑤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統一的な窓口と連携し、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しなければならない。

（攻撃への対処）

第129条　CISO及び統括情報セキュリティ責任者は、サーバー等情報システムに対する攻撃を受けた場合又は攻撃を受けるリスクがある場合は、直ちに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、総務省及び関係機関と連絡を密にして情報の収集に努めなければならない。

（記録の保存）

第130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、サーバー等に情報システムに対する攻撃を受けた場合は、第75条第１項及びその他の記録を保存するとともに、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

（内部からの攻撃）

第131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庁内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。

（職員等による不正アクセス）

第132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、職員等による不正アクセスを発見した場合は、当該職員等を所管する情報セキュリティ管理者に通知し、適正な処置を求めなければならない。

（サービス不能攻撃）

第133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、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

（標的型攻撃）

第134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。

（攻撃の種類に応じた対応）

第135条　前２条のほか、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、攻撃による被害を最小限にするため、攻撃の種類に応じた適正な対応策を検討し、これを実行しなければならない。

第６款　セキュリティ情報の収集

（セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等）

第136条　統括情報セキュリティ責任者及び情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

（不正プログラム等のセキュリティ情報の収集・周知）

第137条　統括情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。

（情報セキュリティに関する情報の収集及び共有）

第138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。

第３編　運用

第１章　運用体制

（運用の一般原則）

第139条　情報システム管理者は、所管する情報システムの運用並びに管理体制の明確化、所属の職員に対する指導並びに研修及びその他の必要な措置を講ずる等、当該情報システムの円滑かつ効率的な運用並びに管理に努めなければならない。

２　前項の各種措置の実施に当たっては、情報システム管理者は、情報セキュリティ管理者の承認を得なければならない。

（情報システムの監視）

第140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。

４　暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入するよう努めなければならない。

（情報セキュリティポリシーの遵守状況の確認及び対処）

第141条　情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに統括情報セキュリティ責任者に報告しなければならない。

２　統括情報セキュリティ責任者は、発生した問題について、適正かつ速やかに対処し、CISO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及び情報システム管理者は、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。

（利用状況の調査）

第142条　統括情報セキュリティ責任者は、職員による基本的責務の違反、情報セキュリティインシデント、端末機等の紛失及び盗難等の調査のために、取得したログ、職員等が使用している端末機等及び外部記録媒体等を調査することができる。

２　統括情報セキュリティ責任者は、前項の調査に当たり、当該情報システム、端末機等及び外部記録媒体等の現状変更の禁止及びその他の必要な措置を当該職員等に命ずることができる。

３　前2項の場合において、当該職員等は、プライバシー権その他の権利の主張をもって調査の全部又は一部を拒否することができない。

４　統括情報セキュリティ責任者は、当該職員の基本的責務の違反、情報セキュリティインシデント及び第183条に該当する場合の調査目的以外で利用状況の調査を行った場合は、遅滞なく調査結果を当該職員等に通知しなければならない。

（職員等の報告義務）

第143条　職員等は、使用している情報システムのこの基準への遵守状況について齟齬を発見した場合は、速やかに情報セキュリティ管理者及び情報システム管理者に報告しなければならない。

２　情報セキュリティ管理者及び情報システム管理者は、前項の齟齬の状況を確認の上、必要と認めるときは、速やかに統括情報セキュリティ責任者に報告しなければならない。

３　統括情報セキュリティ責任者は、前項の齟齬に対し適正かつ速やかに対処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、所管する情報システムのこの基準への遵守状況について必要に応じ確認を行い、齟齬を発見した場合は、適正かつ速やかに対処しなければならない。

（権利及び法益の保護）

第144条　職員等は、情報システムの運用及び管理に当たり、個人情報及び著作権等の権利並びに法益の保護に万全を期さなければならない。

２　前項の規定に違反する行為を未然に防止するため、情報セキュリティ管理者は、所属の職員等に対し必要な指導及び助言をしなければならない。

３　マイナンバー利用事務系に接続する情報システムの情報システム管理者は、個人情報保護委員会の定める安全管理措置を施さなければならない。

４　前項の安全管理措置は、第157条に基づく実施手順において定めることとし、その具体的事項につ

いては、第８条第１項に基づく情報セキュリティ対策ガイドラインにおいて定める。

## 第２章　侵害等発生時の対応

### 第１款　緊急時対応計画の策定

（緊急時対応計画の策定）

第145条　CISO 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正に実施するために、情報システム管理者に、緊急時対応計画を定めさせなければならない。

２　情報システム管理者は、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正に対処しなければならない。

３　情報システム管理者は、緊急時対応計画を定めたときは、速やかに当該計画を統括情報セキュリティ責任者に報告しなければならない。

４　統括情報セキュリティ責任者は、必要に応じて前項の緊急時対応計画を修正し若しくは情報セキュリティ管理者及び情報システム管理者に対して当該計画の修正を求めることができる。

５　緊急時対応計画は、これを非公開とする。

（緊急時対応計画の内容）

第146条　情報システム管理者は、緊急時対応計画において次の各号に掲げる事項を定めなければならない。

(1) 連絡体制及び責任者

(2) 報告すべき事項

(3) 証拠の記録及び保管に関する事項

(4) 対応措置

(5) 再発防止措置

(6) 関係機関への報告

２　前項の規定は、情報システム管理者が当該計画において前項各号に掲げる以外の事項を定めることを妨げない。

（業務継続計画との整合性確保）

第147条　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。

（緊急時対応計画の改正）

第148条　情報システム管理者は、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、必要の都度、速やかに緊急時対応計画を改正しなければならない。

２　前項の改正に当たっては、第145条第３項ないし第４項の規定を準用する。

### 第２款　情報資産への侵害等発生時の対応

（侵害等発生時の対応）

第149条　情報セキュリティ管理者及び情報システム管理者は、情報セキュリティインシデント、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は、統括情報セキュリティ責任者と協議の上、緊急時対応計画に従って適正に対処し、統括情報セキュリティ責任者に報告しなければならない。

２　前項の場合において、統括情報セキュリティ責任者は、必要に応じ侵害等への対応措置について情報セキュリティ管理者又は情報システム管理者に指導又は助言を行うとともに、当該侵害等の再発防止のための措置を講じなければならない。

（関係機関との連携）

第150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、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）及びその他の法律に違反するおそれがある侵害等が発生した場合は、第82条第1項及びその他の侵害等に関する記録を保全するとともに、警察及び関係機関と連携し、迅速な対応を行わなければならない。

（ネットワークの遮断）

第151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、情報資産への侵害等が発生し又はそのおそれがある場合において必要と認めるときは、自らの判断でネットワークの全部又は一部を遮断することができる。

２　前項の場合において、ネットワークの遮断の対象となった所属の情報セキュリティ管理者は、所管する職員等に対し、即座に端末機等の使用を停止させなければならない。ただし、統括情報セキュリティ責任者又は情報システム管理者が別の指示を発した場合はこの限りではない。

３　情報システム管理者は、第１項の規定によりネットワークを遮断したときは、当該遮断の原因となった事項並びにその状況、遮断の範囲並びに対象人数及びその他の必要事項を速やかに情報セキュリティ管理者及び統括情報セキュリティ責任者に報告しなければならない。

４　統括情報セキュリティ責任者は、自らネットワークの遮断を行った場合及び前項の報告を受けた場合は、速やかにCISOに報告しなければならない

（外部からの侵害等の報告）

第152条　前３条の規定は、職員等が外部の者から情報資産への侵害等又はそのおそれについての連絡を受けた場合にこれを準用する。

（重大な侵害等の取扱い）

第153条　統括情報セキュリティ責任者は、ネットワークの遮断、個人情報その他秘匿性の高い情報の漏えい、集団的な不正プログラムへの感染又はその他の情報資産への重大な侵害等が発生した場合は、当該侵害等が発生した所属の情報セキュリティ管理者及び情報システム管理者と連携して、当該侵害等の記録を保存しかつ原因を究明の上、再発防止策を検討し、CISOに報告しなければならない。

２　CISO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。

第３款　例外措置

（例外措置の許可）

第154条　情報セキュリティ管理者及び情報システム管理者は、この基準、この基準に基づく情報セキュリティ対策実施手順及びその他の関連規程等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、これらの規定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、統括情報セキュリティ責任者の許可を得て、例外措置を講じることができる。

２　統括情報セキュリティ責任者は、前項による許可を行うときは、あらかじめCISOに認可を得なければならない。

（緊急時の例外措置）

第155条　統括情報セキュリティ責任者は、行政事務の遂行に緊急を要し例外措置が不可避であると認めるときは、自らの判断により当該例外措置を許可又は実施し、事後速やかにCISOに報告しなければならない。

（例外措置の記録管理）

第156条　統括情報セキュリティ責任者は、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３章　情報セキュリティ対策実施手順

（情報セキュリティ対策実施手順の策定）

第157条　情報システム管理者は、この基準を遵守し情報セキュリティ対策を円滑に実施するため、所管する情報システムにおける情報セキュリティ対策の具体的な実施事項等を明記した情報セキュリティ対策実施手順を策定し、情報セキュリティ管理者の承認を得なければならない。

２　情報セキュリティ管理者は、情報セキュリティ対策実施手順を承認したときは、速やかに当該手順を統括情報セキュリティ責任者に報告しなければならない。

３　統括情報セキュリティ責任者は、必要に応じて前項の情報セキュリティ対策実施手順を修正し若しくは情報セキュリティ管理者及び情報システム管理者に対して当該手順の修正を求めることができる。

（情報セキュリティ対策実施手順の非公開）

第158条　情報セキュリティ対策実施手順は、これを非公開とする。

（情報セキュリティ対策実施手順の内容）

第159条　情報システム管理者が情報セキュリティ対策実施手順において定めるべき具体的な実施事項等については、第８条第1項に基づき、統括情報セキュリティ責任者が別途定める情報セキュリティ対策ガイドラインに例示する。

２　統括情報セキュリティ責任者は、情報システム管理者による情報セキュリティ対策実施手順の策定に当たり、適正な指導及び助言を行わなければならない。

（情報セキュリティ対策実施手順の改正）

第160条　第148条の規定は、情報セキュリティ対策実施手順の改正について、これを準用する。

## 第４章　外部サービスの利用

### 第１款　外部サービスの利用

（外部サービスの利用）

第161条　情報セキュリティ管理者及び情報システム管理者は、この章の規定に基づき外部委託等並びに統括情報セキュリティ責任者が別に定める約款による外部サービス及びソーシャルメディアサービスを利用することができる。

（外部サービス利用の許可）

第162条　情報セキュリティ管理者及び情報システム管理者は、前条で別に定めるもの以外の約款による外部サービス、ソーシャルメディアサービス及びこの章において規定されていない外部サービスを業務の遂行上利用する必要がある場合は、あらかじめ統括情報セキュリティ責任者の文書による許可を得なければならない。

（サービス提供拠点の制限）

第163条　情報セキュリティ管理者及び情報システム管理者は、外部サービスを処理するサーバーその他の電子データを保存する機器が海外に設置されている場合やサービス拠点を海外に置く外部サービス等については、統括情報セキュリティ責任者が別に定める外部サービスを除き、日本の国内法の適用に支障が生じるため、当該外部サービスを利用してはならない。

２　情報セキュリティ管理者及び情報システム管理者は、前項の規定にかかわらず、日本の国内法の適用に支障が生じるおそれがない等、当該外部サービスの利用を肯定するに足る特段の事由があり、業務の遂行上当該サービスを利用する必要がある場合は、あらかじめ統括情報セキュリティ責任者の文書による許可を得なければならない。

（許可の要件）

第164条　情報セキュリティ管理者及び情報システム管理者は、前2条に係る利用の許可を得ようとするときは、当該サービスの名称、仕様、サービス提供者、セキュリティ対策の状況及びその他の必要事項を記載した文書により統括情報セキュリティ責任者に協議しなければならない。

２　統括情報セキュリティ責任者は、前項の協議を受けた場合、次の各号の全てに該当する場合でなければ、その利用を許可してはならない

(1) 当該外部サービスの利用が業務の遂行上必要であり、他の手法と比較した際に合理性のあること。

(2) 当該外部サービスで取り扱う情報が、情報資産の性質に応じ適切であること。

(3) 日本の国内法の適用に支障が生じるおそれがない又は国内法以外の法令が適用されるリスクを評価し、必要に応じ委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定できること。

(4) 当該外部サービスの利用部分を含む情報の流通経路全般にわたる情報セキュリティが適切に確保されていること。

(5) 当該外部サービスで取り扱う情報に個人情報などの重要情報や非公開情報が含まれる場合、情報セキュリティマネジメントシステムの国際規格の認証や政府情報システムのためのセキュリティ評価制度の登録状況等により、情報資産の情報セキュリティを脅かすおそれがないことが確認できること。

(6) 既存の情報システムの運用に影響を及ぼさないこと

(7) 当該外部サービスを利用することが公務の遂行手段として社会通念上是認できること

(8) 当該外部サービスの利用を否定すべきその他の事由がないこと

第２款　外部委託等

（外部委託等事業者の選定）

第165条　情報セキュリティ管理者及び情報システム管理者は、外部委託事業者（クラウドサービス提

供事業者を含む。）の選定に当たり、外部委託等の内容に応じた十分な情報セキュリティ対策が確保されることを確認しなければならない。

2　情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者を選定しなければならない。

3　情報セキュリティ管理者及び情報システム管理者は、必要に応じて次の各号に例示する基準をもって外部委託等事業者を選定するものとする。

(1) 外部委託等先に提供する情報の外部委託等先における目的外利用の危険性

(2) 外部委託等における情報セキュリティ対策の実施内容及び管理体制

(3) 外部委託等事業の実施に当たり、外部委託等先企業又はその従業員、再外部委託等先、若しくはその他の者による意図せざる変更が加えられないための管理体制

(4) 外部委託等先の資本関係並びに役員等の情報、外部委託等事業の実施場所、外部委託等事業従事者の所属並びに専門性及び実績に関する情報

(5) 情報資産に対する侵害等への対応能力

(6) 情報セキュリティ対策その他の契約の履行状況の確認方法の適否

(7) 情報セキュリティ対策の履行が不十分な場合の対処方法の適否

(8) 情報セキュリティ監査受入れの可否

(9) 外部委託の中断や終了時における、円滑な業務の移行の　可否

（外部委託等の契約項目）

第166条　情報セキュリティ管理者及び情報システム管理者は、情報システムの運用、保守等を外部委託等する場合には、外部委託等事業者との間で次の各号に掲げる事項を明記した契約書により契約を締結しなければならない。

(1) この基準及び情報セキュリティ対策実施手順及びその他の関連規程等の遵守

(2) 外部委託等事業者の責任者、委託内容、作業者の所属、作業場所の特定

(3) 提供されるサービス水準の保証

(4) 外部委託等事業者にアクセスを許可する情報の種類並びに範囲及びアクセス方法

(5) 外部委託等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事業実施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) 再外部委託等に関する制限事項の遵守

(9) 外部委託等業務終了時の情報資産の返還、廃棄等

(10)外部委託等業務の定期報告及び緊急時報告義務

(11)道による監査及び検査

(12)情報資産への侵害等発生時の公表

(13)この基準及び情報セキュリティ対策実施手順その他の関連規程等が遵守されなかった場合の規定

（確認及び措置等）

第167条　情報セキュリティ管理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に確認し、必要に応じ、前条の契約に基づき措置を実施しなければならない。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じてCISOに報告しなければならない。

第３款　約款による外部サービス

（約款による外部サービスの利用）

第168条　情報セキュリティ管理者及び情報システム管理者は、統括情報セキュリティ責任者が別に定める約款による外部サービス及びソーシャルメディアサービスを利用することができる。

（情報セキュリティ管理者の承認）

第169条　情報システム管理者は、前条に基づき約款による外部サービスを利用しようとする場合は、次の各号に掲げる事項を含む約款による外部サービスの利用に関する規程の案を作成し、情報セキュリティ管理者の承認を得なければならない。また、当該サービスの利用において、個人情報等の重要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) 当該サービスを利用してよい業務の範囲

(2) 当該サービスで取り扱うことができる情報の範囲

(3) 利用手続及び運用手順

２　情報セキュリティ管理者は、前項の規定に従い約款による外部サービスに関する規程を承認したときは、速やかに当該規程を統括情報セキュリティ責任者に報告しなければならない。

３　統括情報セキュリティ責任者は、必要に応じて前項の規程を修正し若しくは情報セキュリティ管理者及び情報システム管理者に対して当該規程の修正を求めることができる。

（約款による外部サービスの利用における対策の実施）

第170条　職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用について、適正な措置を講じた上で利用しなければならない。

第４款　ソーシャルメディアサービス

（運用手順の制定）

第171条　情報セキュリティ管理者及び情報システム管理者は、ソーシャルメディアサービスを利用する場合は、情報セキュリティ対策に関する次の各号に例示する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) 道として用いているアカウントからの情報発信が真正なものであることを明らかにするため、道のウェブサイトに当該情報を掲載して相互に参照可能にし、かつ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、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（ICカード等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること

(3) その他、道として用いているアカウントの正常な利用を侵害する行為を防止するための措置に関すること

（発信する情報の制限等）

第172条　職員は、次の各号に掲げる情報をソーシャルメディアサービスを用いて発信してはならない。

(1) 個人情報等の重要情報

(2) 非公開の情報

(3) 政治的中立性を損なう情報

(4) 公序良俗に反する情報

(5) 特定の個人の不利益となるおそれのある情報

(6) 特定の企業又は事業者の便宜となる情報

(7) 社会通念上道が発信することがふさわしくない情報

(8) 統括情報セキュリティ責任者が発信を禁止する情報

(9) その他道に対する信頼を失墜させるおそれがある情報

（運用責任者の設置）

第173条　情報セキュリティ管理者及び情報システム管理者は、利用するソーシャルメディアサービスごとに運用責任者を定めなければならない。

２　運用責任者は、外部の者による前条に該当する書き込みがあった場合は、直ちにこれを消去しなければならない。

３　運用責任者は、アカウント乗っ取りを確認した場合には、情報セキュリティ管理者及び情報システム管理者に直ちに報告するとともに、被害を最小限にするための措置を講じなければならない。

４　前項については、第149条を準用する。

（情報セキュリティ対策の確認）

第174条　情報セキュリティ管理者及び情報システム管理者は、第162条及び第163条第２項に定める統括情報セキュリティ責任者の許可を申請する場合は、利用するサービスの約款、その他当該サービスの仕様等により、この基準及び情報セキュリティ対策実施手順等の要件を満たす情報セキュリティ対策が実施されていることを確認するなど、適正な措置を講じなければならない。

（外部サービスの許可申請）

第175条　情報セキュリティ管理者及び情報システム管理者は、第162条及び第163条第２項の許可を申請する場合は、次の各号に掲げるすべての文書を添付しなければならない。

(1) 第164条第2項各号の事項を記載した文書

(2) 第167条又は第169条に基づき作成した規程の案

(3) 前条の確認及び措置を記載した文書

(4) その他、統括情報セキュリティ責任者が許可を行うのに必要と指示する文書

## 第５章　研修及び訓練

### 第１款　情報セキュリティに関する研修

（研修の実施）

第176条　統括情報セキュリティ責任者は、職員を対象として定期的に情報セキュリティ対策に関する研修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、前項に定める研修が各職員の業務経験、役割及び情報セキュリ

ティに関する理解度等に応じた内容となるよう努めなければならない。

３　前２項に定めるもののほか、情報セキュリティ管理者又は情報システム管理者は、所管する職員に対し、情報セキュリティ対策に関する研修を実施することができる。

４　全ての職員は、定められた研修に参加しなければならない。

（研修計画の策定）

第177条　統括情報セキュリティ責任者は、幹部を含め全ての職員に対する情報セキュリティに関する研修計画を策定しなければならない。

（研修実施状況の報告）

第178条　情報セキュリティ管理者又は情報システム管理者は、第176条第３項に基づき研修を実施した場合は、実施後速やかに、当該研修の実施状況を統括情報セキュリティ責任者に報告しなければならない。

第２款　緊急時対応訓練

（緊急時対応訓練）

第179条　統括情報セキュリティ責任者は、定期的に緊急時の対応を想定した訓練を実施しなければならない。

２　前項に定めるもののほか、情報セキュリティ管理者及び情報システム管理者は、各々が所属の職員を対象とした訓練を実施することができる。

３　前２項の場合において、統括情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者は、訓練の計画策定に当たり、ネットワーク並びに情報システムの規模等を考慮して訓練実施の体制及び範囲等を定め、訓練の効果的な実施を図らなければならない。

４　全ての職員は、定められた訓練に参加しなければならない。

第180条　前条第４項の規定にかかわらず、統括情報セキュリティ責任者は、一部の職員を直接の訓練対象者とすることができる。

２　統括情報セキュリティ責任者は、訓練の想定、効果及びその他の訓練の性質上、事前通告をせずに訓練を実施することが妥当と認める場合は、事前の通告を行わずに訓練を実施することができる。

（訓練実施状況の報告）

第181条　統括情報セキュリティ責任者は、第179条第１項の規定による訓練の実施状況について、CIS0に報告しなければならない。

２　情報セキュリティ管理者及び情報システム管理者は、第179条第２項の規定による訓練の実施状況について、統括情報セキュリティ責任者に報告しなければならない。

第６章　法令遵守及び処分等

（法令遵守）

第182条　職員等は、情報資産を使用する業務の遂行に当たっては、次の各号に掲げる法令例規及びその他の関係する法令例規を遵守しなければならない。

(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年法第128号）

(4) 個人情報の保護に関する法律（平成15年5月30日法律第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28年法律第31号）

(7) 北海道個人情報保護条例（平成6年3月31日条例第2号）

(8) 北海道文書管理規程（平成10年3月31日訓令7号）

（懲戒処分等）

第183条　前条の法令例規、北海道情報セキュリティ基本方針、この基準及びその他の関連規程等に違反した職員及びその監督責任者は、当該違反の重大性及び発生した事案の状況等に応じ、地方公務員法第29条による懲戒処分等の対象とする。

（違反時の対応）

第184条　統括情報セキュリティ責任者は、職員等による北海道情報セキュリティ基本方針及びこの基準に違反する行動を発見した場合は、当該違反職員等の所属を所管する情報セキュリティ管理者に連絡し、適正な措置を指示しなければならない。

２　情報システム管理者は、前項の違反を発見した場合は、速やかに統括情報セキュリティ責任者及び当該違反職員等の所属を所管する情報セキュリティ管理者に報告し、適正な措置を求めなければならない。

３　職員は、第1項の違反を発見した場合は、自己の所属を所管する情報セキュリティ管理者を通じて速やかに統括情報セキュリティ責任者及び当該違反職員等の所属を所管する情報セキュリティ管理者に報告し、適正な措置を求めなければならない。

（利用権の停止又は剥奪）

第185条　前条の場合において、情報セキュリティ管理者の指導によっても違反が改善されない場合は、統括情報セキュリティ責任者は、当該違反職員等の情報システム及びネットワークを使用する権利を停止又は剥奪することができる。

２　統括情報セキュリティ責任者は、前項の権利の停止ないしは剥奪を行った場合は、CISO及び当該違反職員等の所属を所管する情報セキュリティ管理者に対し速やかに当該停止又は剥奪について通知しなければならない。

## 第４編　評価及び改正

### 第１章　監査

（実施方法）

第186条　CISO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。

（監査を行う者の要件）

第187条　情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

２　前項の場合において、監査及び情報セキュリティに関する専門知識を有する者でなければならな

い。

（監査実施計画）

第188条　情報セキュリティ監査責任者は、各所属における情報セキュリティ対策の実施状況及び第４条に規定する責務の履行状況について、監査実施計画を策定の上、監査を行うことができる。

２　監査の対象とされた所属の職員は、監査の実施に協力しなければならない。

（外部委託事業者に対する監査）

第189条　情報セキュリティ監査責任者は、再外部委託等事業者を含む外部委託等事業者に対し、外部委託等契約書に定める義務の履行状況について監査を行うことができる。

（監査報告）

第190条　情報セキュリティ監査責任者は、監査結果を取りまとめ、CISOに報告しなければならない。

（監査保管）

第191条　情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書や監査資料を、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。

（監査結果への対応）

第192条　CISOは、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。なお、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。

（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）

第193条　CISO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。

第２章　自己点検

（実施方法）

第194条　統括情報セキュリティ責任者は、毎年度、職員の自己点検を実施しなければならない。

２　前項の自己点検の実施方法については、統括情報セキュリティ責任者が別途定める。

３　情報システム管理者は、自ら必要と認めるときは、随時に所管する情報システムを利用する職員に対して自己点検を行わせることができる。

（自己点検結果の報告）

第195条　統括情報セキュリティ責任者は、前条第１項の自己点検の結果を取りまとめなければならない。

２　情報システム管理者は、前条第３項の自己点検の結果を取りまとめ、統括情報セキュリティ責任者に報告しなければならない。

（職員による改善）

第196条　職員は、自己点検の結果に基づき、改善すべきと思われる事項がある場合は、自己の権限の範囲内で改善を図らなければならない。

第３章　評価

（監査、自己点検及び訓練結果の利用）

第197条　統括情報セキュリティ責任者は、監査結果、自己点検結果及び訓練結果を評価し、この基準及びその他の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に反映させなければならない。

## 第４章　見直し及び改正

（対策の見直し）

第198条　統括情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者は、前条の評価及び情報セキュリティに関する状況の変化等を踏まえ、情報資産の情報セキュリティ対策の見直しを図らなければならない。

２　職員は、情報セキュリティ対策の見直しをすべき事項を認知したときは、速やかに統括情報セキュリティ責任者、情報セキュリティ管理者又は情報システム管理者に報告しなければならない。

（基準の改正）

第199条　統括情報セキュリティ責任者は、この基準について、第197条の評価、前条の見直し内容及び情報セキュリティに関する社会環境並びに技術環境の変化を踏まえ、随時に改正を行うなど、より効果的な情報セキュリティ対策の実施に努めなければならない。

附　則

この基準は、平成14年12月27日から施行する。

附　則

この基準は、平成16年4月1日から施行する。

附　則

この基準は、平成18年4月1日から施行する。

附　則

この基準は、平成21年4月1日から施行する。

附　則

この基準は、平成22年4月1日から施行する。

附　則

この基準は、平成22年4月1日から施行する。

附　則

この基準は、平成24年4月1日から施行する。

附　則

この基準は、平成27年12月28日から施行する。

附　則

この基準は、平成31年４月１日から施行する。

附　則

この基準は、令和３年４月１日から施行する。

附　則

この基準は、令和４年４月１日から施行する。

（経過措置）

２　第５条第２項の規定による情報資産の使用等に係る外部の者の同意について、従前より行政情報ネットワークを利用していることから、北海道公営企業条例（昭和39年４月１日条例第８号）第５条に定める北海道企業局、北海道病院事業条例（昭和42年12月25日条例第45号）第６条に定める北海道道立病院局、北海道議会事務局組織規程（昭和52年２月１日議会訓令第１号）第１条に定める北海道議会事務局、地方自治法（昭和22年法律第67号）第181条及び第200条により北海道に設置される選挙管理委員会及び監査委員事務局、北海道人事委員会事務局の組織等に関する規則（昭和33年４月16日人事委員会規則２―５）第1条に定める北海道人事委員会事務局、土地収用法（昭和26年法律第219号）第51条により設置される北海道収用委員会、北海道教育庁組織規則（昭和46年10月９日教育委員会規則第16号）第２条に定める北海道教育庁、北海道連合海区漁業調整委員会設置規則（昭和26年１月７日規則第２号）第1条に定める北海道連合海区漁業調整委員会、漁業法第171条に定める北海道内水面漁場管理委員会、漁業法（昭和24年法律第267号）第136条第1項の規定により設置された、石狩後志、檜山、渡島、胆振、日高、釧路十勝、根室、網走、宗谷及び留萌海区に係る同第137条に定める海区漁業調整委員会及び地方公務員等共済組合法第3条に基づき設立された地方職員共済組合については、本対策基準の施行後も行政情報ネットワークに利用に際し同意があったものとして取り扱うことを妨げない。