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31年４月１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５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3条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

電子データの漏洩、不正プログラムへの感染、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をいう。

①　不正アクセス、ウィルス攻撃、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洩、破壊、改ざん、消去及び重要情報の窃取並びに内部不正等

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、開発上の不備、プログラム上の欠陥、操作上の過誤、設定上の過誤、保守上の不備、監査機能の不備、外部委託管理の不備、システム管理上の不備及び機器の故障等の非意図的要因による情報資産の漏洩、破壊並びに消去等

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　大規模又は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　通信サービス、電力供給及び水道供給の途絶等、公共社会資本における障害からの波及等

(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サービスを提供するもの（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ー（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。

(5)　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をいう。

(6)　外部記録媒体

電子データを記録するための媒体のうち、コンピューターに内蔵された内部記録媒体を除いたものをいう。

(7)　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。

(8)　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。

(9)　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。

(10)　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。

(11)　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。

(12)　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。

(13)　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。

(14)　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、保存又は送信等を行うサービスで、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。

(15)　ソーシャルメディアサービス

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。

(16)　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。

(17)　道庁行政情報ネットワーク

本庁及び出先機関を結び、電子メール、共有ドライブ及び財務会計トータルシステム等の各種情報システムに利用される基幹的な情報ネットワークをいう。

(18)　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。

(19)　マイナンバー利用事務系

個人番号利用事務（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第２条第10項に規定する事務をいう。）に関わる情報システム及び電子データをいう。

(20)　LGWAN 接続系

LGWANに接続された道庁行政情報ネットワークを利用する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。

(21)　インターネット接続系

北海道自治体情報セキュリティクラウドを介してインターネットを利用する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。

(22)　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。

(23)　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、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及び知識の習得に努めなければならない。

４　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。

５　前４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当該外部の者の書面による同意を得なければならない。

（兼務禁止の原則）

第６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　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。

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７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を置く。

２　最高情報セキュリティ責任者は、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　最高情報セキュリティ責任者は、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。

（統括情報セキュリティ責任者）

第８条　情報セキュリティ対策に関する業務を統括的に実施するため、統括情報セキュリティ責任者を置く。

２　統括情報セキュリティ責任者は、全庁の情報セキュリティ対策を担当する局長とする。

３　統括情報セキュリティ責任者は、最高情報セキュリティ責任者を補佐しなければならない。

４　統括情報セキュリティ責任者は、道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助言・指導権限）

第９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。

（情報セキュリティ対策に関する統括組織の設置）

第10条　最高情報セキュリティ責任者は、情報セキュリティ対策に関する統括的機能を有

する組織を設置しなければならない。
２　前項の組織は、最高情報セキュリティ責任者に直属するものとする。
３　前２項に定めるもののほか、情報セキュリティ対策に関する統括的機能を有する組織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。
（情報セキュリティ責任者）
第11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を実施する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。
（情報セキュリティ管理者）
第12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。
（情報システム管理者）
第13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、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。

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14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15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、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、最高情報セキュリティ責任者が招集する。

（所掌案件）

第16条　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

（持ち回り決議）

第17条　最高情報セキュリティ責任者は、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。

（事務局の設置）

第18条　情報セキュリティ委員会の事務局は、総合政策部情報統計局情報政策課に置く。

第２款　監査体制

（情報セキュリティ監査責任者）

第19条　最高情報セキュリティ責任者は、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20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21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。

２　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について管理責

任を負う。
３　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。
４　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23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。
（電子データの管理義務）
第24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、作成途上の文書や資料的文書も含め、保管している電子データについて漏えいのないよう適正に取り扱わなければならない。
３　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。
４　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。
（外部の機器等の使用禁止）
第25条　職員等は、外部の機器等を庁内の情報システムで使用してはならない。
２　職員は、外部の機器等を庁内の情報システムで外部の者に使用させてはならない。
３　前項の規定にかかわらず、やむを得ず外部の機器等を庁内の情報システムで使用する場合には、職員等は、情報システム管理者の許可を得なければならない。
４　前３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。
（情報資産の持出禁止）
第26条　職員等は、情報資産を執務室外に持ち出してはならない。
２　前項の規定にかかわらず、業務の都合により情報資産を執務室外に持ち出す場合には、職員等は、情報セキュリティ管理者の許可を得なければならない。
３　前２項の規定は、電子メールによる文書施行を行う場合以外の電子メールによる添付ファイルの送付に準用する。
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)　業務上必要な電子データを電子メールの添付ファイルとして庁内の者に送信する場合。
(2)　業務上必要な電子データを電子メールの添付ファイルとして国、他の地方公共団体その他の関係者に送信する場合。
（情報資産の処分）
第27条　職員は、情報資産を処分するときは、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。
２　前項の場合において、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。

第４章　情報システムの強靭性の向上

（マイナンバー利用事務系）

第28条　マイナンバー利用事務系とLGWAN接続系及びインターネット接続系を通信できないようにしなければならない。ただし、外部との通信をする必要がある場合は、通信経路の限定等を行うとともに、外部接続先もインターネット等と接続してはならない。

２　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　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29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。

２　インターネットメールや電子データをインターネット接続系からLGWAN接続系に取り込む場合は、無害化通信を図らなければならない。

（インターネット接続系）

第30条　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LGWAN接続系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。

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31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32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及びその他の重要なサーバーを冗長化しなければならない。

２　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。

（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。

（庁外への機器の設置）

第34条　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ときは、統括情報セキュリティ責任者の承認を得なければならない。

２　前項の設置場所は、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なければならない。

３　第１項により庁外にサーバー等の機器を設置する場合は、情報システム管理者は、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。

４　第１項により庁外にサーバー等の機器を設置した場合は、情報システム管理者は、定期的に当該機器に対する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。

（機器の廃棄等）

第35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27条第2項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36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、サーバー等の重要な機器を集中的に設置した場所を管理区域と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、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。

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、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37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、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。

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、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機器若しくは外部記録媒体等、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。

（部外者の入室禁止）

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。

（管理区域の代替措置）

第40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。

第３款　外部記録媒体の管理

（外部記録媒体の管理責任）

第41条　情報セキュリティ管理者は、外部記録媒体の紛失並びに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、外部記録媒体を新たに調達する場合は、パスワード設定機能又はデータ暗号化機能等の情報セキュリティ機能を備えた媒体の調達に努めなければならない。

３　職員は、パスワード設定機能又はデータ暗号化機能等の情報セキュリティ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42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、当該外部の者の書面による同意を得なければならない。

（外部記録媒体の持出及び持込）

第43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書面による許可を得なければならない。

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44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、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。

（随時点検の実施）

第45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。

（モバイル端末の管理）

第46条　第41条、第42条、第44条及び前条の規定は、モバイル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

（情報システムの利用）

第47条　職員等は、情報システム利用のために発行された認証情報及びカード等の認証媒体について、漏えい又は紛失のないよう努めなければならない。

２　職員等は、情報システムの利用に際し、当該情報システムへのログイン時間が必要最小限になるように努めるとともに、離席時には、原則としてログアウトしなければならない。

（端末機等の持出等の取扱い）

第48条　職員は、端末機等及び外部記録媒体並びにその他の情報資産の持出及び持込については、第25条及び第26条の規定に従い、適正にこれを取り扱わなければならない。

（電子データの送信）

第49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、必要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。

（電子メールの利用制限）

第50条　職員は、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庁内で使用してはならない。

２　職員は、複数人に電子メールを送信する場合は、特に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。

（無許可プログラムの導入禁止）

第51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。

（端末機等の現状変更の禁止）

第52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。

（無許可でのネットワーク接続の禁止）

第53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54条　職員等は、業務上の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、他の職員等が業務上の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55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。

（机上の情報資産の管理）

第56条　職員等は、机上の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。

（この基準等の掲示）

第57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。

（情報セキュリティ管理者の指導義務）

第58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。

２　情報セキュリティ管理者は、所属の非常勤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守るべき内容を理解させ、遵守させなければならない。

第２款　ID及びパスワード等の管理

（IDの取扱い）

第59条　職員は、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　職員は、共同IDを使用する場合は、当該共同IDの使用者以外に使用させてはならない。

（パスワードの管理）

第60条　職員は、パスワードを他人に知られないように管理し、他人からの照会等に応じてはならない。

２　前項の場合において、職員は、容易に推定されない文字列を用いてパスワードを作成しなければならない。

第３款　セキュリティ情報の周知

（情報収集）
第61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、ソフトウェアの脆弱性に関する情報、不正プログラムに関する情報及びその他の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。
（ソフトウェアの更新）
第62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、ソフトウェアの脆弱性に関する情報を収集したときは、必要に応じ修正プログラム等を配付する等、適正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、前項の修正プログラム等が配付された場合は、所属の職員が確実に適用するよう指示し、必要な指導及び助言をしなければならない。
（不正プログラムの情報）
第63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、不正プログラムに関する情報を収集したときは、その緊急性、分布状況、不正プログラム対策ソフトウェアの対応状況及びその他の情報に基づき、必要に応じて職員に対して警告を発する等、適正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、前項の警告が発せられた場合は、所属の職員全員に当該警告が伝達されているかを確認し、必要な指導及び助言をしなければならない。
（情報の共有）
第64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、情報セキュリティに関する情報が必要な職員間で迅速に共有できる体制を整備しなければならない。
２　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、情報セキュリティに関する社会環境及び技術環境の変化による情報セキュリティ上の新たな危険性を認識したときは、情報資産に対する侵害等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章　技術的セキュリティ対策

第１款　情報システム及びネットワークの管理

（技術の活用）
第65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66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67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。

（仕様書等の管理）

第68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69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、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。

第２款　アクセス制御

（アクセス制御の設定）

第70条　情報システム管理者は、所管する情報システムにおいて取り扱う電子データの性質に応じた認証手段を当該情報システムに装備しなければならない。

２　情報システム管理者は、利用者の登録、変更及び抹消を適正に行わなければならない。

（外部の者が利用できるシステムの分離等）

第71条　情報システム管理者は、外部の者が利用できる情報システムについて、必要に応じ他の情報システム及びネットワークと分離する等の措置を講じなければならない。

（ネットワークのアクセス制御）

第72条　ネットワークを管理する情報システム管理者は、不正アクセスを防止するため、部課等単位にアクセス可能なネットワーク及びサービスを定める等、適正な経路制御を行わなければならない。

（外部ネットワークとの接続制限等）

第73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外部のネットワーク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。

（ネットワークの情報窃取防止対策）

第74条　ネットワークを管理する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は、情報窃取を防止するための適正な措置を講じなければならない。

２　職員等は、第26条第2項の許可を得て外部に持ち出した端末機等を公衆無線LAN等、道が管理又は契約していないネットワークに接続させてはならない。

（アクセス制御）

第75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、所管する情報システム又はネットワークについて、正当な権限を有しない者によるアクセスを防止するための

システム上の制限を設けなければならない。

（外部からのアクセスの制限）

第76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。

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77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

（情報システムの開発及び運用）

第78条　情報システム管理者は、情報システムの開発、導入、保守等の調達に当たっては、必要とする技術的なセキュリティ機能を調達仕様書に明記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、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、必要とする情報セキュリティ機能を満たしている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、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。

（資料等の整備及び保管）

第79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、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。

（更新時等の検証）

第80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81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82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。

（不正プログラム対策ソフトウェア）
第83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。
第84条　前条の規定は、ネットワークへの接続の有無にかかわらず全てのサーバー及び端末機等について、これを適用する。
（電子データの授受）
第85条　職員等は、外部記録媒体により外部と電子データを授受する場合には、不正プログラムの検査を行わなければならない。
（全ディスク検査の実施）
第86条　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87条　統括情報セキュリティ責任者は、不正プログラム対策に関して、必要に応じて外部の専門家の意見を聴取できる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88条　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の適正な措置を講じなければならない。
（攻撃への対処）
第89条　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は、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、速やかに必要な措置の検討、実施及び情報の収集を行わなければならない。
（記録の保存）
第90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、情報システムに攻撃を受けた場合は、第69条第１項及びその他の記録を保存しなければならない。
（職員等による不正アクセス）
第91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。
（攻撃の種類に応じた対応）
第92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、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３編　運用
第１章　運用体制

（運用の一般原則）

第93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。

（権利及び法益の保護）

第94条　職員等は、情報システムの運用並びに管理に当たり、個人情報及び著作権等の権利若しくは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111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９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。

（遵守状況）

第95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。

（情報システム等の状況把握）

第96条　統括情報セキュリティ責任者は、外部の団体等が提供する情報システム等の情報セキュリティ状況の診断サービス等を有効に活用し、情報システム及びネットワークの状況を常に把握するとともに、必要に応じ適正な修正等を行わなければならない。

（利用状況の調査）

第97条　統括情報セキュリティ責任者は、不正アクセス又は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端末機等の利用状況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、当該端末機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。

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98条　情報システム管理者は、情報資産への侵害等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、伝達、証拠の保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に実行し、再発防止等の措置を講ずるために、情報セキュリティ管理者の承認を得て、緊急時対応計画を定めなければならない。

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。

３　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。

４　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99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。

（緊急時対応計画の改正）

第100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、情報セキュリティ管理者の承認を得て、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98条第１項ないし第３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

（職員等の報告義務）

第101条　職員等は、情報システムの異常を発見した場合は、速やかに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。

（侵害等発生時の対応）

第102条　情報セキュリティ管理者及び情報システム管理者は、前条の状況が情報資産への侵害等と認められるときは、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ないし情報システム管理者に指導若しく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、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69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。

（不正プログラムへの感染が疑われる場合の対応）

第104条　職員等は、端末機等への不正プログラムの感染が疑われる場合は、直ちに当該端末機等をネットワークから取り外す等、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105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においては、職員等は、端末機等の使用を即座に停止しなければならない。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、速やかに最高情報セキュリティ管理者に報告しなければならない。

（外部からの侵害等の報告）

第106条　前５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107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、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、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108条　統括情報セキュリティ責任者は、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、最高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。

（緊急時の例外措置）

第109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実施し、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。

（例外措置の記録管理）

第110条　統括情報セキュリティ責任者は、例外措置の記録を適正に保管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111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112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113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9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114条　第100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115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、外部委託等及び統括情報セキュリティ責任者が別に定める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116条　情報セキュリティ管理者及び情報システム管理者は、約款による外部サービス、前条で別に定めるもの以外の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書面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117条　統括情報セキュリティ責任者は、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等、日本の国内法の適用に支障が生じるおそれがある場合は、原則として当該外部サービスの利用を許可してはならない。

２　前項の規定にかかわらず、サービス拠点を海外に置く外部サービスについて、日本の国内法の適用に支障が生じるおそれがない等、当該サービスの利用を肯定するに足る特段の事由がある場合は、統括情報セキュリティ責任者は、当該サービスの利用を許可することができる。

（定めのない外部サービス等）

第118条　情報セキュリティ管理者及び情報システム管理者は、この章において規定されていない外部サービス又は第115条で別に定めるもの以外のソーシャルメディアサービスを利用する場合は、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書面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。

（許可の要件）

第119条　第116条、第117条第２項及び前条の場合において、統括情報セキュリティ責任者は、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不可欠でありかつ代替的手段がないこと

(2)　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

(3)　既存の情報システムの運用に影響を及ぼさないこと

(4)　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

(5)　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120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

（外部委託等契約の条項）

第121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122条　情報セキュリティ管理者及び情報システム管理者は、外部委託等において事業者が必要な情報セキュリティ対策を確保していることを確認しなければならない。

２　前項の確認の結果、不適当と認める事項がある場合は、情報セキュリティ管理者及び情報システム管理者は、必要に応じ前条の契約に基づき対処しなければならない。

第３款　約款による外部サービス

（情報セキュリティ管理者の承認）

第123条　情報システム管理者は、第116条に基づき統括情報セキュリティ責任者による許可を得て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。
(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。

（情報セキュリティ対策の確認）

第124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116条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。

（約款による外部サービスの許可申請）

第125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116条の許可を申請する場合は、次の各号に掲げるすべての書面を整備し、申請書に添付しなければならない。

(1)　第119条第1項各号の事項を記載した書面

(2)　第123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書面

第４款　ソーシャルメディアサービス

（運用手順の制定）

第126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)　パスワード並びに認証のためのコード等の認証情報及びこれを記録した媒体等を適正に管理しアカウントの乗っ取りに対する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

（運用責任者の設置）

第127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。

（ソーシャルメディアサービスの利用）

第128条　情報セキュリティ管理者及び情報システム管理者は、利用するサービスの利用規程等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の実施並びに第119条第1項各号の事項を確認するなど、適正な措置を講じなければならない。

（発信する情報の制限等）

第129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)　政治的中立性を損なう情報

(2)　公序良俗に反する情報
(3)　特定の個人の不利益となるおそれのある情報
(4)　特定の企業又は事業者の便宜となる情報
(5)　社会通念上道が発信することがふさわしくない情報
(6)　その他道に対する信頼を失墜させるおそれがある情報

２　運用責任者は、外部の者による前項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。

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130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131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132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130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133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134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135条　統括情報セキュリティ責任者は、第133条第１項の規定による訓練の実施状況について、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　情報セキュリティ管理者及び情報システム管理者は、第133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136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年法律第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137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138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139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、最高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

（監査実施計画）

第140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　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。

（監査への協力義務）

第141条　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。

（監査報告）

第142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、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。

第２章　自己点検

（自己点検の実施）

第143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。

第144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145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146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147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148条　統括情報セキュリティ責任者は、この基準について、第146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。