北海道情報セキュリティ対策ガイドライン

令和元年５月30日　総合政策部情報統計局長決定

【趣旨】

このガイドラインは、各情報システムにおける情報システム管理者が情報セキュリティ対策実施手順を作成するにあたり参考とすべき内容を定めるものである。

なお、本ガイドラインに示す例文は、あくまでも情報セキュリティ対策実施手順において定めるべき標準的な内容の一例を示すものであるから、適宜、各システムの状況により規定の要否及び規定の内容を検討し、規定の取捨選択、修文又は追加を行い、各情報システムの仕様ないしは運用実態に合わせた実施手順の作成に努められたい。

【特定個人情報に係る留意事項】

本ガイドラインにおいて、「特定個人情報の適正な取扱いに関するガイドライン」（行政機関等・地方公共団体等編）（平成26年12月18日（平成30年９月28日一部改正）・個人情報保護委員会）２－Ｃ－ａ（組織体制の整備）に定める各責任者等の名称は、北海道情報セキュリティ対策基準及び本ガイドラインにおける名称に合わせ、下表のとおり読み替えるものとする。

特定個人情報の適正な取扱いに関するｶﾞｲﾄﾞﾗｲﾝにおける名称	北海道情報セキュリティ対策基準及び本ガイドラインにおける名称
総括責任者	最高情報セキュリティ責任者
保護責任者	情報システム利用課長
監査責任者	情報セキュリティ監査責任者
事務取扱担当者	情報システム利用者

また、本ガイドラインの例文中、ゴシック体表記となっているものについては、「特定個人情報の適正な取扱いに関するガイドライン」に定められた内容を例文化したものであり、情報セキュリティ対策上、特に重要なものであることから、特定個人情報を取り扱う情報システムの情報セキュリティ対策実施手順においては、同旨の内容を必ず定めることとする。

【例文】

Ⅰ　総則

1　通則

(1) 目的

この手順は、北海道情報セキュリティ対策基準（以下「基準」という。）第111条乃至第114条の規定に基づき、○○情報システム（以下「本システム」という。）の運用に必要な情報セキュリティ対策の実施手順について定めるものとする。

(2) 定義

・　北海道情報セキュリティ基本方針（以下「方針」という。）・基準に定める用語以外で実施手順で使用する用語について定義をする。

(3) 適用範囲

・　対象者

本手順の対象者は、本システムを開発・運用及び利用する職員を対象とする。

・　対象とする情報資産

本手順の対象とする情報資産は、本システム及び本システムで取り扱う方針第２条第１項第４号に定める情報資産とする。

(4)　委託等事業者に関する定め

本システムについて委託等により外部の事業者に当該システムの開発、運用、改修及び保守等を行わせる場合は、事前に方針及び基準を当該事業者に手交し、契約書に記載されるセキュリティポリシー及び関連規程等の遵守義務、情報の目的外利用の禁止、守秘義務、再委託に関する制限及びその他の重要事項について説明するものとする。

(5)　実施手順の非公開

本手順は、これを非公開とする。

2　実施体制

(1) 情報システム管理者

・　情報システム管理者の指定

本システムの情報システム管理者は○○部○○課長（参事）をいう。

・　情報システム管理者の役割

情報システム管理者は、本システムの開発、運用、改修及び保守等における管理について決定する権限を有しかつ責任を負う。

・　特定個人情報を扱う情報システム管理者の決定事項

特定個人情報を扱う情報システム管理者は、次の各号に掲げる事項を決定し、関係者に通知するものとする。 ①　情報システム利用者及びその役割の明確化 ②　情報システム利用者が取扱う特定個人情報等の範囲の明確化 ③　特定個人情報等を複数の部署で取扱う場合の各部署の任務分担及び責任の明確化

(2) 情報システム担当者

・　情報システム担当者の指定

本システムの情報システム担当者は、情報システム管理者が指定した職員とする。

・　情報システム担当者の役割

情報システム担当者は、情報システム管理者を補佐するとともに、情報システム管理者の指示を受け、本システムの開発、運用、改修及び保守等を担当する職責を負う。

(3) 情報システム利用課長

・　情報システム利用課長の指定

情報システム利用課長は、本システムを利用する（※所属名等によりシステムの利用範囲を指定）における、基準で定められた情報セキュリティ管理者とする。

・　情報システム利用課長の役割

情報システム利用課長は、セキュリティポリシー、この実施手順、その他の関連規程等及び情報システム管理者の指示に従い、本システムの適切な利用及び情報セキュリティの保持について、所管する情報システム利用者に指導、監督及び助言を行う職責を負う。

(4) 情報システム利用者

・　情報システム利用者の指定

情報システム利用者は、本システムを利用する一般職員、非常勤職員の取扱いに基づき任用した非常勤職員及び臨時職員取扱要綱に基づき任用した臨時職員とする。

・　情報システム利用者の役割

情報システム利用者は、セキュリティポリシー、この実施手順、その他の関連規程等、情報システム管理者の指示及び情報システム利用課長の指導に従い、本システムを適切に利用し、かつ情報セキュリティの保持に努める職責を負う。

(5) 委託等事業者

・　委託等事業者の指定

本システムにおける運用（※開発、改修、保守等）業務の委託等事業者は、○○とする。

・　委託等事業者の役割

上記委託等事業者の業務内容については、○○業務処理要領において別に定めるところによる。

※　委託等事業者が複数にわたる場合等については、適宜別表で定めるなど、各システムの実情に合った規定内容とする。

※　上記(1)～(5)以外にも、各システムごとの必要に応じて、情報セキュリティ管理者、統括情報セキュリティ責任者等についての定めを置くことができる。

3　情報資産

(1) 情報資産の管理責任者

・　情報システム管理者の管理責任

情報システム管理者は、次の各号に定める情報資産について管理責任を負う。 ①　本システムにおけるネットワーク関係機器（※ネットワーク接続されていない場合は単に「関係機器」） ②　本システムの業務内容に係る情報を記録したサーバー等 ③　上記①及び②に係る本システム、これらの機器に記録されたシステムの仕様及び各種設定など、システムの開発並びに運用管理に関する情報及び②の機器に記録された情報システムの業務内容に係る情報 ④　外部記録媒体に記録された上記③のバックアップファイル ⑤　上記①～④の他、電子データを入力するための帳票及び情報システムの仕様書等、本システムに関連する文書

・　情報システム担当者の実施事項

情報システム担当者は、情報システム管理者の指示に従い、上記①～⑤の情報資産の管理に関する作業を実施するものとする。

・　情報システム利用課長の管理責任

情報システム利用課長は、次の各号に定める情報資産について管理責任を負う。 ①　本システムで利用する端末機等、プリンタ及びこれに附属する機器 ②　上記①に係る情報システム並びに端末機等及びこれに附属する機器に記録された情報 ③　外部記録媒体に記録された上記②のバックアップファイル ④　上記①の端末機等で直接、外部記録媒体に作成したファイル

・　情報システム利用者の管理責任

情報システム利用者は、次の各号に定める情報資産について管理責任を負う。 ①　利用する端末機等やプリンタ等の機器 ②　利用する端末機等の記録媒体に記録される情報 ③　利用する外部記録媒体及び外部記録媒体に記録される情報

(2) 情報セキュリティ対策の実施

・ 脅威情報の把握方法

情報システム管理者及び情報システム担当者は、統括情報セキュリティ責任者から提供される脅威情報のほか、次の各号に定める方法により脅威情報の早期把握に努めるものとする ① ○○○○ ② ○○○○ *※ 具体的方法を列挙する* *（例）「JPCERTが発行するアラートメール及びウィークリーレポート」など*

・ 実施事項に関する定め

情報システム管理者は、脅威情報を把握した場合、速やかにその対策方法を検討し、(1)に定める管理責任に従い当該対策方法を実行するものとする。

・ 情報資産の非公開

情報資産については、非公開とする。

(3) 電子データの管理義務

・ 基準§24(3)の「データの性質」に関する定め

基準第24条第3項により本システムにおいて暗号化（※パスワード設定）する電子データは、次の各号に定める電子データとする。 ① 個人情報を含む電子データ ② 入札の設計積算に関する電子データ *※ 各システムで扱う電子データの内容に合わせて規定する*

・ 特定個人情報に係るパスワード等に関する定め

特定個人情報を取扱う情報システムにおける暗号化又はパスワードによる電子データの保護に当たっては、不正に入手した者が容易に復元できないように、暗号鍵及びパスワードの運用管理、パスワードに用いる文字の種類や桁数等の要素を考慮するものとする。

(4) 特定個人情報の持出及び持込

・ 特定個人情報の持出及び持込に係る措置に関する定め

情報システム利用者は、本手順の規定に基づき、特定個人情報等が記録された外部記録媒体又は書類等を持ち出し又は持ち込む必要が生じた場合、個人番号が判明しない措置の実施、追跡可能な移送手段の利用等を行うほか、外部記録媒体又は書類等の移動等において、紛失や盗難等により容易に個人番号が判明しないよう、次の措置を講ずる。 ① 外部記録媒体を用いて持ち出すデータの暗号化、パスワードによる保護、施錠できる搬送容器の使用等。但し、行政機関等に法定調書等をデータで提出するに当たっては、当該行政機関等が指定する提出方法に従うものとする。 ② 特定個人情報等が記載された書類等の封緘、目隠しシールの貼付等。

(5) 情報資産の処分

・ 基準§27(2)の具体的実施内容

本システムにおいて基準第27条第2項に定める処理を行う場合は、○○（※ソフトウェア名、仕様等により指定する）以上の消去能力を有するソフトウェアによるものとする。

情報システム利用者は、特定個人情報等が記録された機器等及び外部記録媒体について、保存年限を経過した場合、基準第27条第2項の方法により処理するものとする。

・ **特定個人情報の削除等に関する定め**

情報システム利用者は、特定個人情報等が記録された書類等について、保存年限を経過した場合、焼却又は溶解等の復元不可能な手段により廃棄するものとする。

情報システム利用者は、個人番号若しくは特定個人情報ファイルを削除した場合、又は外部記録媒体等を廃棄した場合には、削除又は廃棄した記録を保存するものとする。

情報システム利用者は、上記の作業を委託する場合、委託先が確実に削除又は廃棄したことについて、証明書等により確認するものとする。

Ⅱ 情報セキュリティ対策

1 物理的セキュリティ対策

(1) サーバー等の管理

・ サーバーの冗長化に関する定め

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、速やかにセカンダリサーバーに処理を移行し、システムの運用停止時間を最小限にするものとする。

・ 機器の電源に関する定め

情報システム管理者は、情報システム利用課長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できる容量の予備電源を備え付けるものとする。

情報システム管理者は、情報システム利用課長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に、○○○○（※具体的方法を記載）等必要な措置を講じるものとする。

・　通信ケーブル及び回線等の保護等に関する定め

情報システム管理者及び情報システム利用課長は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じるものとする。

情報システム管理者及び情報システム利用課長は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応するものとする。

情報システム管理者及び情報システム利用課長は、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するものとする。

情報システム管理者及び情報システム利用課長は、自ら及び情報システム担当者並びに契約により操作を認められた委託等事業者以外の者が配線を変更、追加できないように、○○○○（※具体的方法を記載）等必要な措置を講じるものとする。

(2) 管理区域

・　管理区域の管理に関する定め

管理区域及び個別に設置する機器の配置場所は、非公開とする。

※　各システムにおいて管理区域の管理に関して基準に定める以外の方法を行う場合は、その方法及び取扱方法についての規定を置く。

・　管理区域の設備に関する定め

管理区域には、火災等に備えるため、火災検知装置及び消火設備を配備するものとする。

機器及びサーバー等は固定し、転倒防止策を施すものとする。

・　**特定個人情報の物理的セキュリティ対策に関する定め**

情報システム管理者は、本システムにおいて特定個人情報等を取り扱うサーバー等主要な機器等を設置する管理区域を明確にし、必要な物理的安全管理措置を講ずる。

情報システム利用課長は、特定個人情報等を取り扱う事務を実施する区域（以下「取扱区域」という。）について、情報システム利用者等以外の者が特定個人情報等を容易に閲覧等できない措置を講ずる。

・　入退室管理に関する定め

情報システム管理者は、次の各号のいずれかに該当し、事前に登録された者の入室を許可することができる。 ①　情報システムの開発及び機器や情報の管理を行う情報システム担当者 ②　情報システムの開発及び機器や情報の管理を行う委託等事業者 ③　情報システム機器の保守点検作業に従事する委託等事業者 ④　管理区域の電気設備及び空調設備等の保守点検作業に従事する委託等事業者 ⑤　その他情報システム管理者が必要と認める者

管理区域の鍵及び入室カードの管理は情報システム管理者が行い、入退室の許可を得た者に限り、鍵又は入室カードを貸与するものとする。

管理区域に入退室する者は、情報システム管理者の指示に従うとともに、次の各号に掲げる事項を遵守しなければならない。 ①　業務処理に必要ない機器や外部記録媒体は持ち込まないこと。 ②　許可なく撮影機材を室内に持ち込み、又は撮影をしないこと。 ③　室内において喫煙又は飲食をしないこと。 ④　情報システム管理者は、委託等事業者が管理区域に入室する場合、情報システム担当者を立ち会わせなければならない。

・　管理区域内への機器の搬入出に関する定め

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、あらかじめ情報システム担当者又は委託等事業者に確認を行わせるものとする。

情報システム管理者は、情報システム室の機器等の搬入出について、情報システム担当者を立ち会わせるものとする。

・　特定個人情報における管理区域の設備

基準第37条に定めるものの他、情報システム管理者は、特定個人情報を取り扱う情報システムを設置する管理区域について、外部からの不正な侵入に備え、警報装置等を設置する。

・　個別に配備されているサーバー等に関する定め

※　基準第40条により管理区域を設けずにサーバー等を設置する場合の規定

情報システム管理者は、本システムの運用に当たって、配備されているサーバー等の機器等について、次の各号に掲げる安全対策を講じるものとする。 ①　サーバー等は、機器及び設置場所等の態様により、ラック等に入れて保管・施錠、若しくはICカードやパスワード等によるアクセス制限を行う。 ②　機器及びサーバー等は、固定するなど、転倒防止策を施す。 ③　委託等事業者が本システムの開発又は運用管理、若しくは機器等の保守点検等を行う場合は、予め庁舎管理者に通知する。

機器の配置場所等は、非公開とする。

・　通信回線及び通信回線装置の管理に関する定め

情報システム管理者は、通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理するものとする。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ものとする。

情報システム管理者は、外部へのネットワーク接続を必要最低限に限定するものとする。

情報システム管理者は、本システムに通信回線を接続する場合、必要な情報セキュリティ水準を検討の上、適正な回線を選択し、送受信される情報の暗号化を行うものとする。

情報システム管理者は、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、○○○○（※具体的方法を記載）等必要な措置を講じるものとする。

情報システム管理者は、本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、回線を冗長構成にする等の措置を講じるものとする。

(3) 外部記録媒体の取扱い

※　*当該システムに特有の外部記録媒体がある場合はその取扱いに関する定めを置く（暗号化の採否、管理方法、管理者等）*

・　**特定個人情報の施錠管理等に関する定め**

情報システム管理者は、管理区域及び取扱区域における特定個人情報等を取り扱う機器、外部記録媒体及び書類等の盗難又は紛失等を防止するために、施錠できるキャビネット、書庫又は必要に応じて耐火金庫等へ保管するなどの物理的な安全管理措置を実施する。

(4) モバイル端末の取扱い

・　モバイル端末の利用に関する定め

情報システム管理者は、庁外での業務利用時における紛失等に備えて、モバイル端末に遠隔消去機能等の措置を講じるものとする。

2　人的セキュリティ対策

(1) 利用者の遵守事項

・　基準第47条第2項の例外措置

情報システム利用者は、本システムの利用中に離席し、その時間が短時間の場合、次の各号のいずれかの措置によることができる。 ①　スクリーンセーバにパスワードを設定することによるロック ②　端末機等のオペレーティングシステムにおけるロック機能の活用

(2) ID及びパスワードの取扱い

・　ID及びパスワードの発行方法等に関する定め

情報システム管理者は、情報システム利用課長からの申請に基づき、情報システム利用者のログインID等の利用者情報の登録、変更及び抹消を行うものとする。

利用者情報の登録内容については、情報システム管理者がこれを定めるものとする。

・　**個人番号利用事務に係る認証方法に関する定め**

情報システム管理者は、本システムにおいて個人番号利用事務を行う場合、情報システム利用者が正当なアクセス権を有する者であることについて、パスワード、磁気カード、ＩＣカード及び生体情報等の各種認証方法から二つ以上の要素により識別した結果に基づき認証する。

・　パスワードの管理に関する定め

情報システム利用者は、システムに接続する場合、ログイン時に必要となるパスワードを次の各号により厳重に管理するものとする。 ①　複数のシステム間で同一のパスワードを用いてはならない。 ②　パスワードには名前、誕生日、連続番号など推測されやすい文字列などは使用しないこと。 ③　パスワードのメモを作成しないなど、他人に漏れないようにすること。 ④　パスワードの共有は行わないこと。 ⑤　仮のパスワード（初期パスワードを含む）は、最初のログイン時点で変更しなければならない。 ⑥　サーバー、ネットワーク機器及び端末機等にパスワードを記憶させてはならない。

・　認証情報の管理

情報システム管理者及び情報システム利用課長は、情報システム利用者等の認証情報を厳重に管理するとともに、認証情報ファイルを不正利用から保護するため、オペレーティングシステム等による認証情報設定の情報セキュリティ強化機能を活用するものとする。

情報システム管理者及び情報システム利用課長は、情報システム利用者等に対してパスワードを発行する場合、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させるものとする。

情報システム管理者及び情報システム利用課長は、認証情報の不正利用を防止するために、○○○○（※具体的方法を記載）等必要な措置を講じるものとする。

・　利用者IDの取扱いに関する定め

情報システム管理者は、情報システム利用者の登録、変更、抹消等の情報管理、情報システム利用者等の異動、出向、退職に伴う利用者IDの取扱い等の方法を定めるものとする。

情報システム利用者は、業務上必要がなくなった場合、利用者登録を抹消するよう、情報システム管理者に通知しなければならない。

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、点検するものとする。

・　特権を付与されたIDの管理等に関する定め

情報システム管理者は、管理者権限等の特別な権限を付与された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するものとする。

情報システム管理者及び情報システム利用課長は、特別な権限を付与されたID及びパスワードについて、情報システム利用者等の端末等のパスワードよりも定期変更、入力回数制限等の情報セキュリティ機能を強化するものとする。

情報システム管理者は、特別な権限を付与されたID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するものとする。

・　ICカード等の取扱いに関する定め

情報システム利用者等は、自己の管理するICカード等に関し、次の事項を遵守しなければならない。

①　認証に用いるIC カード等を、情報システム利用者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又は端末機等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、速やかに情報セキュリティ責任者及び情報システム管理者に通報し、指示に従わなければならない。

情報システム管理者及び情報システム利用課長は、ICカード等の紛失等の通報があり次第、当該ICカード等を使用したアクセス等を速やかに停止するものとする。

情報システム管理者及び情報システム利用課長は、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するものとする。

・　ソフトウエアの安全性の確保に関する定め

情報システム管理者は、本システムに接続されている端末機等のオペレーティングシステムやソフトウェア等のサポートが終了し、情報セキュリティ対策上、問題を生じる恐れがある場合、情報システムとの接続ができなくなる旨、十分な猶予期間を設けた上で、事前に情報システム利用課長に周知し、情報システム利用課長は、端末機等やオペレーティングシステムの更新を円滑に行うものとする。

情報システム管理者は、本システムに接続する端末機等について、情報システム管理者が定める要件を満たしていない場合、当該端末機等の接続を停止するものとする。

(3)　特定個人情報の取扱いに関する定め

・　**特定個人情報の取扱いに関する定め**

情報システム管理者及び情報システム利用課長は、特定個人情報等が適正に取り扱われるよう、情報システム利用者に対して必要かつ適切な監督を行う。

3　技術的セキュリティ対策

(1) コンピューター及びネットワークの管理

・　各サーバーの設定等に関する定め

※　*サーバーの種類に応じた設定内容について定める。下記は文書サーバーにおける規定の例。*

情報システム管理者は、文書サーバーの設定にあたり次の各号に掲げる事項に従うものとする。

①　情報システム管理者は、情報システム利用者等に対し、使用できる文書サーバーの容量を設定し、周知しなければならない。

②　情報システム管理者は、文書サーバーを課室等の単位で構成し、情報システム利用者等が他課室等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。

③　情報システム管理者は、住民の個人情報、人事記録等、特定の情報システム利用者等しか取扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一課室等であっても、担当以外の情報システム利用者等が閲覧及び使用できないようにしなければならない。

・　特定個人情報の利用状況等の記録に関する定め

情報システム管理者は、次の各号に例示する特定個人情報等の利用状況等を記録し、その記録を一定の期間保存し、定期及び必要に応じ随時に分析等するための体制を整備するとともに、記録については、改ざん、窃取又は不正な削除の防止のために必要な措置を講じ、分析等を行う。

①　特定個人情報ファイルの利用・出力状況の記録
②　書類・媒体等の持出及び持込の記録
③　特定個人情報ファイルの削除・廃棄記録
④　削除・廃棄を委託した場合、これを証明する記録等
⑤　特定個人情報ファイルを情報システムで取り扱う場合、事務取扱担当者の情報システムの利用状況（ログイン実績、アクセスログ等）の記録

情報システム管理者は、次の各号に例示する、特定個人情報ファイルの取扱状況を確認するための適切な手段を整備する。なお、取扱状況を確認するための記録等には、特定個人情報等は記載してはならない。

①　特定個人情報ファイルの名称
②　行政機関等の名称及び特定個人情報ファイルが利用に供される事務をつかさどる組織の名称
③　特定個人情報ファイルの利用目的
④　特定個人情報ファイルに記録される項目及び本人として特定個人情報ファイルに記録される個人の範囲
⑤　特定個人情報ファイルに記録される特定個人情報等の収集方法

・　システム管理記録及び作業の確認に関する定め

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、作業記録を作成するものとする。

情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合、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するものとする。

情報システム管理者若しく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委託等事業者がシステム変更等の作業を行う場合、2名以上で作業し、互いにその作業を確認するものとする。

・　ネットワークの接続制御及び経路制御に関する定め

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するものとする。

・　外部ネットワーク等との接続制限等に関する定め

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するものとする。

情報システム管理者及び情報システム利用課長は、ウェブサーバー等をインターネットに公開する場合、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上で接続するものとする。

・　複合機の情報セキュリティ管理に関する定め

情報システム管理者は、複合機を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正な情報セキュリティ要件を策定するものとする。

情報システム管理者は、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るものとする。

情報システム管理者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じるものとする。

・　特定用途機器の情報セキュリティ管理に関する定め

情報システム管理者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合、当該機器の特性に応じた○○○○（※具体的方法を記載）等の必要な対策を講じるものとする。

・　電子メールの情報セキュリティ管理に関する定め

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うものとする。

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、メールサーバーの運用停止を含め、適切な措置を講じるものとする。

情報システム管理者は、上限を超える電子メールの送受信を不可能にするため、電子メールの送受信容量の上限を設定するものとする

情報システム管理者は、情報システム利用者等に対し、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周知するものとする

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委託等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、委託等事業者との間で利用方法を取り決めるものとする。

情報システム管理者は、情報システム利用者が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるよう、添付ファイルの監視等によるシステム上の措置を講じるものとする。

・　電子署名・暗号化に関する定め

情報システム利用者等は、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、情報システム管理者が定めた電子署名、暗号化又はパスワード設定等、情報セキュリティを考慮して、送信しなければならない。

情報システム利用者等は、暗号化を行う場合、情報システム管理者が定める以外の方法を用いてはならない。また、情報システム管理者が定めた方法で暗号のための鍵を管理しなければならない。

(2) アクセス制御

・　アクセス権限の設定に関する定め

情報システム管理者は、情報システム利用者に対し、その利用目的に沿ったアクセス権限を設定するものとする。

・　外部からのアクセス制限に関する定め

情報システム管理者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行うために○○○○（※具体的方法を記載）等の機能を確保するものとする。

情報システム管理者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じるものとする。

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情報システム利用者等に貸与する場合、情報セキュリティ確保のために○○○○（※具体的方法を記載）等の必要な措置を講じるものとする。

・　特定個人情報に係るアクセス制御に関する定め

情報システム管理者は、本システムを使用して個人番号利用事務等を行う場合、情報システム利用者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、次の各号に例示するアクセス制御を行うものとする。

①　特定個人情報ファイルを取り扱うことのできる端末機等を限定する。

②　各システムにおいて、アクセスすることのできる特定個人情報ファイルを限定する。

③　ユーザーＩＤに付与するアクセス権により、特定個人情報ファイルを取り扱う情報システムを使用できる者を情報システム利用者に限定する。

④　特定個人情報ファイルへのアクセス権を付与すべき者を最小化する。

⑤　アクセス権を有する者に付与する権限を最小化する。

⑥　情報システムの管理者権限を有するユーザーであっても、情報システムの管理上特定個人情報ファイルの内容を知らなくてもよいのであれば、特定個人情報ファイルへ直接アクセスできないようにアクセス制御をする。

⑦　特定個人情報ファイルを取り扱う情報システムに導入したアクセス制御機能の脆弱性等を検証する。

情報システム管理者は、特定個人情報を取り扱う情報システムについて、基準第73条第２項に定める措置を行わなければならない。また、インターネットから独立する等の高い情報セキュリティ対策を備えたシステム構築や運用体制を整備するものとする。

・　他の情報システムとの接続に関する定め

情報システム管理者は、他の情報システムと接続する場合、その方法を確認し、管理運用する情報資産に、影響が生じないことを確認するものとする。

情報システム管理者は、他の情報システムが不正プログラムに感染するなどの情報セキュリティ上の問題が発生したことにより、管理運用する情報資産に被害が生じた、又は生じる恐れがある場合、速やかに他の情報システムとの接続を物理的に遮断し、被害や影響の有無を確認するものとする。

・　自動識別の設定に関する定め

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ものとする。

・　ログイン時の表示等に関する定め

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情報システム利用者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ものとする。

(3) システムの開発、導入及び保守等

・　調達仕様書の作成に関する定め

情報システム管理者は、情報システムの調達を委託する場合、次の各号に掲げる事項に留意して調達仕様書の作成を行うものとする。

① 情報システムに必要な機器等について、ＩＰアドレス等の設定情報を記載しないこと。

② 機器の設置場所、設置環境などの外的要件や情報セキュリティ要件などを勘案し、必要となる機器、部材等を調達する旨、記載すること。

③ 重要なサーバー等については、二重化する旨、記載すること。

④ 情報システムで調達するソフトウェアについては、最新のバージョンとすることとし、最新のサービスパック及び修正プログラムを適用するよう記載すること。

⑤ 情報システムで調達するハードウェア、ソフトウェアに関する設定内容ついては、別に指示する旨、記載すること。

⑥ 情報システムで調達するハードウェア、ソフトウェアに関する情報セキュリティ上の問題については、瑕疵担保適用期間中は、委託等事業者の責任において対処する旨、記載すること。

・　委託する場合の留意事項に関する定め

情報システム管理者は、システムの開発、運用保守等を外部に委託する場合、次の事項に留意して契約を締結するものとする。

① 基準及び本手順の遵守、また、遵守されなかった場合の損害賠償規定を明記すること。

② 外部へ搬送した外部記録媒体の盗難防止や不正な複製等の防止について明記すること。

③ 委託業務の終了時には、委託業務期間中に使用した情報や記録媒体の消去、廃棄等を行うことを明記すること。

④ 委託等事業者が再委託をする場合、上記の事項に準ずる条項を含む契約を締結することを明記すること。

・　システム開発における責任者及び作業者の特定に関する定め

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するとともに、システム開発のための規則を確立するものとする。

・　システム開発における責任者、作業者のＩＤの管理に関する定め

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を削除するものとする。

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するものとする。

・　システム開発に用いるﾊｰﾄﾞｳｪｱ及びｿﾌﾄｳｪｱの管理に関する定め

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ハードウェア及びソフトウェアを特定するものとする。

情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除するものとする。

・　開発環境と運用環境の分離及び移行に関する定め

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ものとする。

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するものとする。

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するものとする。

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するものとする。

・　テストに関する定め

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うものとする。

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ものとする。

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

情報システム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行うものとする。

・　システム開発・保守に関連する資料等の整備び保管に関する定め

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するものとする。

・　情報システムにおける入出力データの正確性確保に関する定め

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するものとする。

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、これを防止する機能とともに、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ものとする。

情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計するものとする。

・　開発・保守用のソフトウェアの更新等に関する定め

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するものとする。

(4) 不正プログラム対策

・　情報システム利用者への情報提供に関する定め

情報システム管理者は、統括情報セキュリティ責任者、関係機関等から提供される情報及びインターネットから収集した情報に基づき、不正プログラムに関して注意を喚起する必要がある場合、情報システム利用課長及び情報システム利用者へ周知するものとする。

・　不正プログラム対策ソフトに関する定め

情報システム管理者は、不正プログラム対策ソフトのインストール状況を定期的に監視し、インストールされていない端末機等やサーバーは情報システムから切り離し、その旨を情報システム利用課長に通知するものとする。

情報システム管理者は、情報システム利用者による電子メールの送受信について、不正プログラムのチェックを行うものとする。

・　感染源等の調査に関する定め

情報システム管理者は、不正プログラムへの感染が発生した場合、感染した不正プログラムの種類及び名称、感染経路等の情報について調査するものとする。

・　情報システム利用者の対策事項に関する定め

情報システム利用者は、次の各号に掲げる現象を発見した場合、速やかに情報システム管理者及び情報システム利用課長に報告しなければならない。

①　不正プログラム対策ソフトが動作していない場合

②　不正プログラム対策ソフト又はパターンファイルが最新のものに更新されない場合

情報システム利用者は、情報システム管理者が提供する不正プログラム対策情報を必ず閲覧し、適切に不正プログラム対策を行うものとする。

情報システム利用者は、次のようなメールを受信した場合、削除しなければならない。

① 差出人に心当たりのないメール

② タイトルが意味不明なメール

③ メール本文の内容と一致しない添付ファイル名が存在するメール

情報システム利用者は、他の業務で使用していた端末機等を、本システムに接続する場合、接続前に必ず不正プログラムのチェックを行い、不正プログラムの感染していないことを確認の上、情報システム管理者の承認を得て接続するものとする。

(5) 不正アクセス対策

・ 外部との接続制限に関する定め

情報システム管理者は、情報システムにおいて、インターネットや他のネットワークと接続する場合、使用しないポート（情報の受送信口）については、ファイアーウォール、中継機器等の設定により閉じるものとする。

情報システム管理者は、サーバー及び端末機等における不必要なサービスの削除を行うなど、不正アクセスを防止するための措置を講じるものとする。

情報システム管理者は、不正アクセスによるホームページの改ざんを防止するため、データの書換えを検出し、通報されるよう、設定するものとする。

情報システム管理者は、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ものとする。

・ 情報政策課との連携に関する定め

情報システム管理者は、不正アクセス行為を受けた場合、情報政策課と連携を図り、適正な対策を講じるものとする。

・ 情報システムの停止等に関する定め

情報システム管理者は、統括情報セキュリティ責任者からの情報により不正アクセスを受ける恐れがあると認められる場合、本システムの設定変更や停止等の措置をとるものとする。

・　特定個人情報に係る不正アクセス等の防止に関する定め

情報システム管理者は、次の各号に定める外部等からの不正アクセス又は不正プログラムから保護する仕組み等を導入し、適切に運用するとともに、個人番号利用事務の実施に当たり接続する情報提供ネットワークシステム等の接続規程等が示す安全管理措置を遵守するものとする。 ①　本システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する。 ②　定期に及び必要に応じ随時にログ等の分析を定期的に行い、不正アクセス等を検知する。 ③　情報システムの不正な構成変更（許可されていない電子媒体、機器の接続等、ソフトウェアのインストール等）を防止するために必要な措置を講ずること。

Ⅲ　運用

1　運用体制

・　情報システムの監視に関する定め

情報システム管理者は、情報システムを安全に稼動させるため、ネットワークや情報システムの監視を行い、異常が確認され、情報システムに影響を及ぼす恐れがある場合、ネットワークの切断や情報システムの停止などの措置を講じるとともに、原因を究明し、再発防止策を講じるものとする。

・　トラフィック監視

情報システム管理者は、設置されているネットワーク機器のトラフィック情報を定期的に監視し記録を保持するものとする。

・　ファイアウォール監視

情報システム管理者は、外部（インターネット）、外部公開用サーバー及び端末機等からの過剰なアクセスについて監視し記録を保持するものとする。

・　不正プログラムの監視

情報システム管理者は、不正プログラム対策ソフトにより、ウイルスの検知及び感染の情報を取得するとともに、パターンファイルの更新状況について監視し記録を保持するものとする。

・　ネットワークの侵入監視

情報システム管理者は、ネットワーク侵入監視装置のイベント情報を監視し記録を保持するとともに、必要があれば、情報システムの脆弱性について調査するものとする。

・　時刻同期に関する定め

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るものとする。

2　侵害時の対応

・　侵害等への対処に関する定め

情報システム利用課長は、侵害等の事案の発生により、他の情報システムに影響を及ぼす恐れがある場合、情報システム管理者の指示により、速やかに調査を行い、報告しなければならない。

情報システム利用課長は、調査の結果、他の情報システムに影響を及ぼす恐れがある場合、関係者に連絡するなど適切に対処するものとする。

情報システム利用課長は、侵害等の再発の恐れがある場合、防止策を講じ、情報システム管理者に報告するものとする。

情報システム管理者は、情報システム利用者等から侵害等の報告を受けた場合、情報システム利用者に対し必要な措置を講じるよう指示するものとする。

情報システム管理者は、侵害等が全庁的あるいは他機関等に影響を及ぼす恐れがある場合、ネットワークの遮断や情報システムの停止などの措置を講じるものとする。

情報システム管理者は、侵害等について次の各号に掲げる事項の原因を調査・分析し、復旧にあたるものとする。 ①　各種のイベントの状況 ②　システムの負荷状況 ③　ネットワークの負荷状況 ④　ファイルの改ざん ⑤　存在すべきファイルの抹消や不明なファイルの存在 ⑥　ファイル利用量の急激な増減 ⑦　本来稼動しているはずのサービスの停止 ⑧　不明なプロセスの実行 ⑨　本来利用できないはずのシステム利用者のシステムアクセス

情報システム管理者は、侵害等の再発の恐れがある場合、再発防止策を講じるものとする。

情報システム管理者は、次のような事態が生じた場合、または生じるおそれがある場合、基準第105条及び第106条の規定に従い、本システムの全部又は一部の遮断等の措置を行うことができる。

① 地震、落雷、火災等の災害及び事故、故障等によるネットワークシステムの障害

② 部外者等による不正アクセス又は不正操作による情報資産の持出し、改ざん、消去などの不測の事態

③ 情報システム利用者及び委託等事業者による意図しない操作、未許可の端末接続による情報流出等の不測の事態

④ その他の侵害等によりシステムの切断等が必要と認められる場合

・ 特定個人情報の情報漏えい等に関する定め

情報システム管理者は、特定個人情報等をインターネット等により外部に送信する場合、次の各号により通信経路における情報漏えい等の防止措置を実施する。

① 通信経路の暗号化等

② データの暗号化又はパスワードによる保護等

情報システム管理者は、特定個人情報に係る情報漏えい等の事案の発生又は兆候を把握した場合、次の各号に掲げる事項につき緊急時対応計画に従い適切かつ迅速に対応するものとする。

① 情報漏えい等の事案が発覚した際の報告・連絡等

② 事実関係の調査及び原因の究明

③ 影響を受ける可能性のある本人への連絡

④ 委員会及び主務大臣等への報告

⑤ 再発防止策の検討及び決定

⑥ 事実関係及び再発防止策等の公表

情報システム管理者は、情報漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表するものとする。

3 研修・訓練

・ 研修・訓練の実施に関する定め

情報システム管理者は、基準第98条に基づき策定した緊急時対応計画について、情報システム利用課長及び情報システム利用者を対象に研修を実施するものとする。

情報システム管理者は、基準第130条に定めるものの他、情報システム利用者に対する情報セキュリティ対策に係る知識及び技術の習得に関する研修の実施、指導及び支援を行うことができる。

・　特定個人情報に係る研修に関する定め

情報システム管理者及び情報システム利用課長は、情報システム利用者に対し、特定個人情報等の適正な取扱いについて理解を深め、特定個人情報等の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行うものとする。

情報システム管理者は、情報システム利用者に対し、特定個人情報等の適切な管理のために、情報システムの管理、運用及び情報セキュリティ対策に関して必要な教育研修を行うものとする。

情報システム管理者は、情報システム利用課長に対し、課室等における特定個人情報等の適切な管理のために必要な研修を行うものとする。

情報システム利用課長は、特定個人情報等の適切な管理のために、情報システム利用者に対して教育研修への参加の機会を付与するとともに、研修未受講者に再受講の機会を付与する等の必要な措置を講ずるものとする。

・　緊急時対応訓練に関する定め

情報システム管理者は、基準第133条に定めるものの他、必要に応じて本システムにおける緊急時対応訓練を実施することができる。

・　特定個人情報に係る訓練等に関する定め

情報システム管理者は、特定個人情報への不正アクセス、不正プログラム感染の事案に加え、標的型攻撃等の被害を受けた場合の対応について、関係者において定期的に確認又は訓練等を実施するものとする。

4　法令遵守及び処分等

・　特定個人情報に係る違反等への対処

情報システム管理者及び情報システム利用課長は、法令又は内部規程等に違反した職員に対し、法令又は内部規程等に基づき厳正に対処するものとする。

Ⅳ　評価及び改正

1　自己点検に関する定め

情報システム管理者は、基準第143条に定める自己点検に併せて、本システムの情報セキュリティ対策において必要な点検項目を追加して、情報システム利用者に点検させることができる。

情報システム利用課長は、情報セキュリティ対策に係る職場研修の実施及び自己点検の指導を行うものとする。

2　監査及び評価に関する定め

情報システム管理者は、セキュリティポリシー及び本手順の遵守状況について、必要の都度、実地調査を行う権限を有する。

・　**特定個人情報に係る監査等に関する定め**

情報システム管理者は、特定個人情報の管理の状況について、定期に又は随時に監査（外部監査及び他所属等による点検を含む。）を行い、その結果等を踏まえ、必要があると認める場合、本手順等の見直し等の措置を講ずるものとする。

情報システム管理者は、本システムの運用状況、実地調査の結果、研修・訓練の結果及び自己点検の結果を評価し、この手順の見直し、その他情報セキュリティ対策の見直しに反映させるものとする。

3　運用見直し及び改正

情報システム管理者は、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運用の見直しを図るものとする。

情報システム利用者は、情報セキュリティ対策の運用の見直しをすべき事項を認知した場合、速やかに情報システム管理者に報告するものとする。

情報システム管理者は、この手順と異なる取扱いをする必要が生じた場合、あらかじめ委託等事業者等と協議の上、その取扱いを決定するものとする。

情報システム管理者は、この手順について随時評価を行い、必要な改正を行うものとする。

ガイドラインの沿革

平成17年12月27日　策定

平成18年4月1日　改正

平成19年7月1日　改正

平成21年4月1日　改正

平成22年4月1日　改正

平成24年4月1日　改正

平成27年12月25日　改正

令和元年5月30日　改正

緊急時対応計画の作成例について

令和元年５月３０日
総合政策部情報統計局情報政策課

北海情報セキュリティ対策基準（以下「基準」という。）第98条により、情報システム管理者は所管する情報システムの緊急時対応計画を作成し、情報セキュリティ管理者の承認を得なければならない（基準第98条第１項）。
また、当該計画を承認した情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者に当該計画を報告しなければならない（基準第98条第２項）。

緊急時対応計画において定めるべき事項については、基準第99条においてに列挙してあるが、各情報システム管理者の便宜を考慮し、より具体的な資料として、緊急時対応計画の作成例を示すこととした。

この作成例では、ほとんどの情報システムに該当すると思われる事項を記載するにとどめてあるので、各情報システム管理者におかれては、この作成例を参考にしつつも、各情報システムの構成、特性や職場の組織実態などに合わせて適宜追加の定めを設けるなど、より実態に即した緊急時対応計画の作成に努められたい。

〇〇〇〇システム

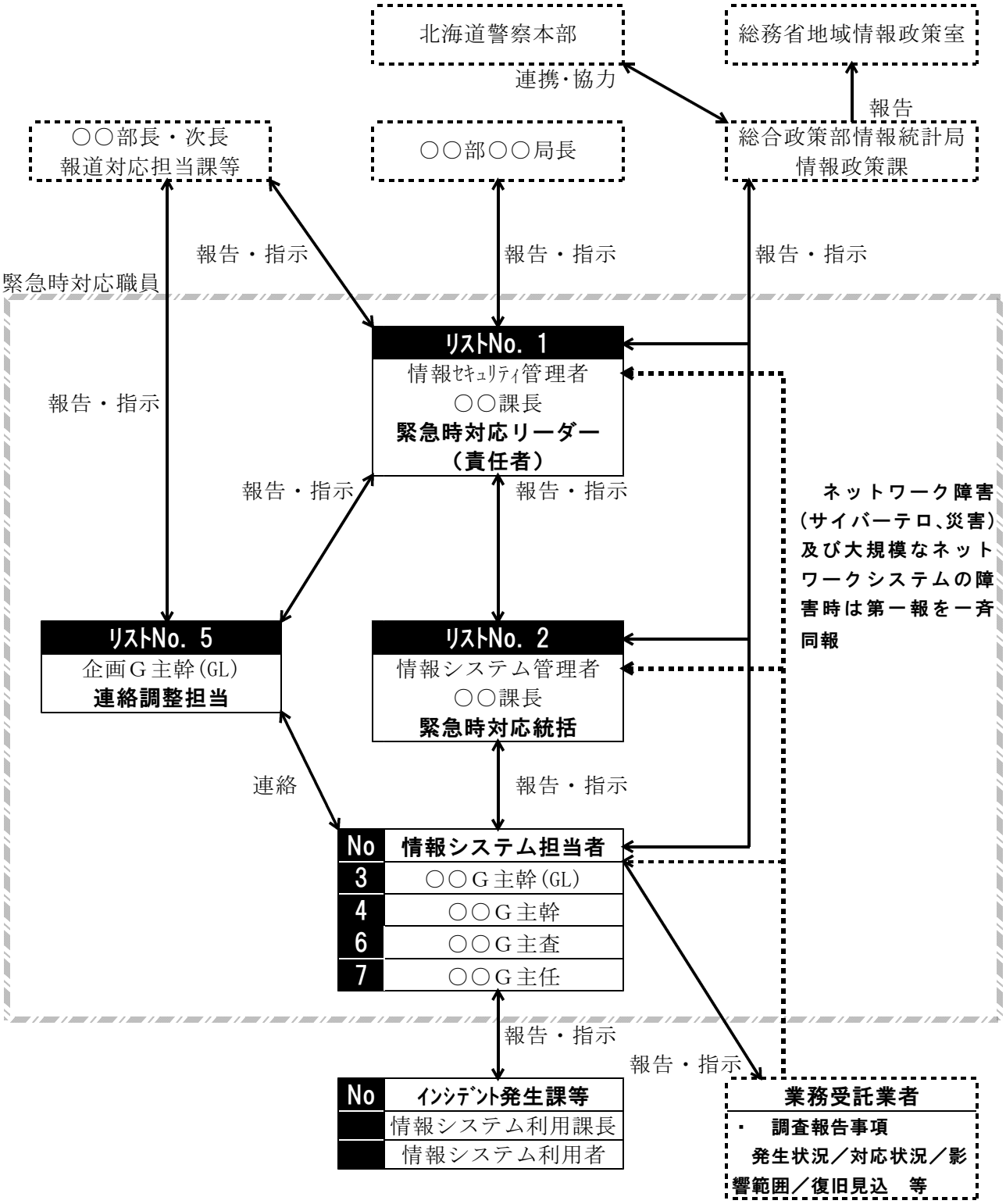
緊急時対応計画

（ 作 成 例 ）

令和〇〇年〇〇月

〇〇部〇〇局〇〇課

1　連絡体制及び責任者


北海道警察本部
総務省地域情報政策室
連携･協力
報告
○○部長・次長
報道対応担当課等
○○部○○局長
総合政策部情報統計局
情報政策課
報告・指示
報告・指示
報告・指示
緊急時対応職員
報告・指示
ﾘｽﾄNo. 1
情報ｾｷｭﾘﾃｨ管理者
○○課長
緊急時対応リーダー
（責任者）
報告・指示
報告・指示
ネットワーク障害（サイバーテロ、災害）及び大規模なネットワークシステムの障害時は第一報を一斉同報
ﾘｽﾄNo. 5
企画Ｇ主幹(GL)
連絡調整担当
ﾘｽﾄNo. 2
情報システム管理者
○○課長
緊急時対応統括
連絡
報告・指示
No
情報システム担当者
3
○○Ｇ主幹(GL)
4
○○Ｇ主幹
6
○○Ｇ主査
7
○○Ｇ主任
報告・指示
報告・指示
No
ｲﾝｼﾃﾞﾝﾄ発生課等
情報システム利用課長
情報システム利用者
業務受託業者
・　調査報告事項
発生状況／対応状況／影響範囲／復旧見込　等

２　報告すべき事項

・　侵害等の緊急事態が発生した際には、まずは電話により下表に示す事項を連絡をする。
・　下表の事項のすべてが判明していない場合は、報告時点で判明している内容を報告する。
・　電話による報告後、速やかに「北海道情報セキュリティ対策基準における様式に関する細則」別記第７号様式の記載要領にしたがい報告書を作成し、関係報告先に伝達する。

１　障害及び事故の区分	・ コンピュータウイルス感染　・ パソコンや外部記録媒体の紛失等 ・ 情報システムへの不正アクセス　・ その他（　　）
２　発見した日時	令和　　年　　月　　日　　時　　分頃
３　情報システム名	
４　障害及び事故の内容	
５　原因	
６　現在行っている対応	
７　その他特記事項	

３　証拠の記録及び保管に関する事項

情報システム管理者は、下表に示すサーバー等のログを記録し、これを１年間保管するものとする。

サーバー等の名称	コンピューター名等	収集・記録するログの名称

4　対応措置

情報セキュリティ管理者及び情報システム管理者は、侵害等の緊急事態の報告を受けた時は、概ね次の手順に従い対応を措置する。

(1) 報告された内容の事実確認
報告された内容が誤認に基づくものでないかを調査・確認する。

(2) 想定される被害の範囲の決定
事案の性質に応じ、被害の範囲内にある端末機等のLANケーブル取り外し、電源の切断、一定のセグメントのネットワーク遮断、システム全体のネットワーク遮断等、必要な措置を行う。

(3) 被害の程度等の把握
各種ログの記録等をもとに情報流出の有無・程度、またサーバー側に被害が及んでいる場合はその状況を把握する。併せて、(2)で決定した範囲以外で何らかの侵害等が発生していないかについて追跡調査を行う。

(4) 復旧
(3)の結果に基づき、復旧計画を策定し実施する。
この際、(2)でネットワークの遮断を行った場合は、○○システムを構成するすべての情報資産が完全に復旧していることを確認の上、ネットワークの再接続を行うこととする。ただし、被害を受けた端末機等が少数に特定されている場合などにおいては、当該端末機等の復旧を待たずに、当該端末機等をネットワークから取り外した上でネットワークの再接続を行うことができるものとする。

5　再発防止措置

情報セキュリティ管理者及び情報システム管理者は、システムの復旧後速やかに再発防止のための措置を検討するものとする。
検討にあたっては、概ね次の事項を調査・分析するものとする。

(1) 規程類の遵守状況
法令例規、北海道情報セキュリティ基本方針、北海道情報セキュリティ対策基準、○○システム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に抵触している事項はないかについて調査を行い、抵触がある場合はその原因及び解決方法を検討する。

(2) 人的セキュリティ
検討対象となっている侵害等の発生において人的要因が関与していないかを調査・分析し、人的要素の関与が認められる場合は、その原因及び解決方法を検討する。

(3) 物理的セキュリティ
検討対象となっている侵害等の発生において物理的要因が関与していないかを調査・分析し、物理的要素の関与が認められる場合は、その原因及び解決方法を検討する。

(4) 技術的セキュリティ
検討対象となっている侵害等の発生において技術的要因が関与していないかを調査・分析し、技術的要素の関与が認められる場合は、その原因及び解決方法を検討する。
併せて、当該侵害等の防止に関連する最新の技術動向について調査し、有効な新たな技術がある場合には、その導入についても検討する。

６　関係機関への報告

本システムにおいて侵害等の緊急事態が発生した場合に連絡又は報告を必要とする機関等は、下記に示す様式により、情報システム管理者が別途定める。

機関等の名称	担当部署	担当者名	電話番号	電子メールアドレス