○北海道警察における情報セキュリティに関する対策基準について

令和５年３月22日
道本情第8100号

／警察本部各部、所属の長／警察学校長／各方面本部長／各警察署長／宛て

北海道警察における情報セキュリティについては、北海道警察情報セキュリティに関する訓令（平成16年警察本部訓令第７号）第８条に基づき、関係規程により実施してきたところであるが、今般、政府のサイバーセキュリティ戦略本部が定める国の行政機関等におけるサイバーセキュリティに関する対策の基準との準拠性を明らかにすること等を目的として、別添のとおり「警察における情報セキュリティに関する対策基準」を定め、令和５年４月１日から実施することとしたので、事務処理上遺漏のないようにされたい。

なお、本通達の実施に伴い、以下の通達は、同日付けで廃止する。

・「北海道警察における情報セキュリティに係る管理体制について」（令４．３．25道本情第6725号）
・「警察情報システム及び管理対象情報の取扱いについて」（令４．３．25道本情第6727号）
・「警察情報システムの情報セキュリティ要件について」（令４．３．25道本情第6730号）
・「情報セキュリティインシデント対処要領について」（令４．３．25道本情第6732号）
・「警察情報セキュリティポリシーの遵守事項に関する例外措置の適用申請手続について」（平30．１．24道本情第3741号）

別添

北海道警察における情報セキュリティに関する対策基準

第１　総則

１　目的

この文書は、北海道警察情報セキュリティに関する訓令（平成16年警察本部訓令第７号。以下「訓令」という。）第８条に基づき、警察における情報セキュリティを確保するために必要な対策を定めるものとする。

２　管理対象情報の分類・取扱制限

⑴　管理対象情報の分類

管理対象情報の分類は次のとおりとする。

ア　機密性

㋐　機密性３（高）情報

管理対象情報のうち、特定秘密（北海道警察における特定秘密の保護に関する規程（平成26年警察本部訓令第20号）第１条に定めるものをいう。）又は秘密文書（北海道警察文書管理規程（平成27年警察本部訓令第６号）第３条第５号に定めるものをいう。）としての取扱いを要する情報を含むもの

㋑　機密性２（中）情報

管理対象情報のうち、北海道情報公開条例（平成10年北海道条例第28号。以下「情報公開条例」という。）第10条第２項各号に掲げる非開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、機密性３（高）情報以外のもの

㈢　機密性１（低）情報
管理対象情報のうち、情報公開条例第10条第２項各号に掲げる非開示情報に該当すると判断される蓋然性の高い情報を含まないもの

イ　完全性

㈠　完全性２（高）情報
管理対象情報（書面に記載された情報を除く。）のうち、改ざん又は滅失した場合に業務の的確な遂行に支障を及ぼすおそれがあるもの

㈡　完全性１（低）情報
管理対象情報（書面に記載された情報を除く。）のうち、完全性２（高）に分類される以外のもの

ウ　可用性

㈠　可用性２（高）情報
管理対象情報（書面に記載された情報を除く。）のうち、その情報が使用できないときに業務の安定的な遂行に支障を及ぼすおそれがあるもの

㈡　可用性１（低）情報
管理対象情報（書面に記載された情報を除く。）のうち、可用性２（高）に分類される以外のもの

⑵　管理対象情報の取扱制限

管理対象情報の分類に応じて、複製禁止、持ち出し禁止、配布禁止、読後廃棄、閲覧の制限等の管理対象情報の適正な取扱いを職員に確実に行わせるための制限をいう。主な取扱制限の例を次に示す。

ア　複製の禁止
当該情報について、複製を禁止する必要がある場合に「複製禁止」等の指定をする。

イ　持ち出しの禁止
当該情報について、定められた場所からの持ち出しを禁止する必要がある場合に「持ち出し禁止」等の指定をする。

ウ　配布の禁止
当該情報について、定められた者以外への配布を禁止する必要がある場合に「配布禁止」等の指定をする。

エ　読後廃棄
当該情報について、読後に廃棄する必要がある場合に「読後廃棄」等の指定をする。

オ　閲覧の制限
当該情報について、閲覧可能な範囲を制限する必要がある場合に「○○限り」等の指定をする。

３　用語の定義

警察情報セキュリティポリシーにおいて、次に掲げる用語の意義は、それぞれ当該各号に定めるほか、訓令における用語の例による。

⑴　警察情報セキュリティポリシー　訓令及び訓令に基づいて定められた情報セキュリティに関する事項をいう。

⑵　所属　北海道警察本部（以下「警察本部」という。）の課（課に相当するものを含む。）、北海道警察学校の部及び課、方面本部の課（課に相当するものを含む。）、警察署並びにサイバーセキュリティ対策本部をいう。

⑶　職員　警察情報システム及び管理対象情報を取り扱う北海道警察（以下「道警察」という。）の職員をいう。
⑷　要機密情報　機密性３（高）又は２（中）に分類される管理対象情報をいう。
⑸　要保全情報　完全性２（高）に分類される管理対象情報をいう。
⑹　要安定情報　可用性２（高）に分類される管理対象情報をいう。
⑺　要保護情報　要機密情報、要保全情報又は要安定情報に一つでも該当する管理対象情報をいう。
⑻　外部記録媒体　ＵＳＢメモリ、外付けハードディスクドライブ、ＤＶＤ－Ｒ等の電子計算機に接続し情報を入出力する電磁的記録媒体をいう。
⑼　ネットワーク機器　情報システムを構成するルータ、ハブ等の機器又はこれらから出力されるデータを利用することによりネットワークを管理する機能を有する機器をいう。
⑽　外部回線　警察の管理が及ばない電子計算機が論理的に接続され、当該電子計算機の通信に利用されるインターネットその他の電気通信回線をいう。
⑾　ネットワーク端末　ネットワークを介して他の電子計算機と接続された端末であって、インターネットに接続されていないものをいう。
⑿　インターネット端末　インターネットに接続された端末をいう。
⒀　スタンドアロン端末　他の電子計算機と接続されていない端末をいう。
⒁　移動通信事業者　電気通信役務としての移動通信サービスを提供する電気通信事業を営む者であって、当該移動通信サービスに係る無線局を自ら開設（開設された無線局に係る免許人等の地位の承継を含む。）又は運用している者をいう。
⒂　携帯電話機　フィーチャーフォン、スマートフォン等の移動通信事業者の回線を利用し音声通話及び情報の処理を行うための端末をいう。
⒃　モバイル端末　一の警察の庁舎内から移動して運用するものとして整備した端末（携帯電話機を除く。）をいう。
⒄　サーバ等　情報を体系的に記録し、検索し、又は編集する機能を有するサーバ及びメインフレームをいう。
⒅　情報セキュリティインシデント　情報セキュリティの維持を困難とする事案をいう。
⒆　ＣＳＩＲＴ（Computer Security Incident Response Team）情報セキュリティインシデントに迅速かつ組織的に対処するための体制をいう。
⒇　基盤となる情報システム　他の機関と共通的に使用する情報システム（一つの機関でハードウェアからアプリケーションまで管理・運用している情報システムを除く。）をいう。
㉑　暗号化消去　情報を電磁的記録媒体に暗号化して記録したもので、情報の抹消が必要になった際に情報の復号に用いる鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法をいう。
㉒　情報の抹消　全ての情報を利用不能かつ復元が困難な状態にすること（電磁的記録媒体を物理的に破壊すること及び「電子政府における調達のために参照すべき暗号のリスト（ＣＲＹＰＴＲＥＣ暗号リスト）」（平成25年３月１日総務省・経済産業省）によって安全性が確認された暗号アルゴリズムを用いた暗号化消去を含む。）をいう。

⑵3　外部委託　業務委託及び外部サービスをいう。
⑵4　業務委託　警察の業務のうち、管理対象情報を取り扱う業務の一部又は全部について、「委任」、「準委任」、「請負」等の契約形態を問わず、契約をもって外部の者に実施させることをいう。業務委託の例としては、警察情報システムの開発及び構築業務、警察情報システムの運用業務、リース契約等が挙げられる。
⑵5　外部サービス　部外の者が一般向けに情報システムの一部又は全部の機能を提供するサービスのうち、当該機能において管理対象情報が取り扱われるものをいう。外部サービスの例としては、クラウドサービス、ウェブ会議サービス、ソーシャルメディアサービス、データセンター、通信回線等の賃貸借等が挙げられる。
⑵6　クラウドサービス　外部サービスのうち、事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに係る十分な条件設定の余地があるものをいう。
⑵7　ウェブ会議サービス　専用のアプリケーションやウェブブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行える外部サービスをいう。
　なお、特定用途機器相互で通信を行うもの及び警察情報システムのサーバ等により提供されるものを含まない。
⑵8　ソーシャルメディアサービス　インターネット上において、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等の、利用者が情報を発信し、形成していくものをいう。
⑵9　外部サービス管理者　外部サービスの利用における利用申請の際、許可権限者から利用承認時に指名された当該外部サービスに係る管理を行う者をいう。
⑶0　外部サービス提供者　外部サービスを提供する事業者をいう（外部サービスを利用して警察に向けて独自のサービスを提供する事業者を除く。）。
⑶1　外部サービス利用者　外部サービスを利用する職員又は業務委託した委託先において外部サービスを利用する場合の委託先の従業員をいう。
⑶2　識別　情報システムにアクセスする主体を、当該情報システムにおいて特定することをいう。
⑶3　主体　情報システムにアクセスする者又は他の情報システムにアクセスする端末及びサーバ等をいう。
⑶4　識別コード　識別コード、ホスト名等の、主体を識別するために、情報システムが認識するコード（符号）をいう。
⑶5　共用識別コード　複数の主体が共用するために付与された識別コードをいう。
⑶6　主体認証　識別コードを提示した主体が、その識別コードを付与された正当な主体であるか否かを検証することをいう。
⑶7　主体認証情報　パスワード等の、主体認証をするために、主体が情報システムに提示する情報をいう。
⑶8　主体認証情報格納装置　ＩＣカード等の、主体認証情報を格納した装置であり、正当な主体に所有又は保持させる装置をいう。

⑶９　ＲＰＡ（Robotic Process Automation）　マウス操作やキーボード入力等の作業について、人間に代わって一定のルールに基づき自動的に処理を行う事務の自動化技術をいう。
⑷０　耐タンパ性　暗号処理や署名処理を行うソフトウェアやハードウェアに対する外部からの解読攻撃に対する耐性をいう。
⑷１　自己復号型暗号　特定のソフトウェアをインストールすることなく情報を復号することのできる暗号をいう。
⑷２　電子署名　電子署名及び認証業務に関する法律（平成12年法律第102号）第２条第１項に規定する電子署名をいう。
⑷３　アプリケーション・コンテンツ　情報の提供、行政手続、意見募集等の行政サービスのために利用者に提供するアプリケーションプログラム、ウェブコンテンツ等の総称をいう。
⑷４　ドメイン名　国、組織、サービス等の単位で割り当てられたネットワーク上の名前であり、英数字及び一部の記号を用いて表したものをいう。
⑷５　複合機　プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器をいう。
⑷６　特定用途機器　テレビ会議システム、ＩＰ電話システム、ネットワークカメラシステム、監視カメラ等の特定の用途に使用される情報システム特有の構成要素となる機器であって、電気通信回線に接続されている、又は電磁的記録媒体が内蔵されているものをいう。
⑷７　ドメインネームシステム（ＤＮＳ）　クライアント等からの問合せを受けて、ドメイン名やホスト名とＩＰアドレスとの対応関係について回答を行う情報システムをいう。
⑷８　ＤＮＳサーバ　コンテンツサーバ、キャッシュサーバ等、名前解決のサービスを提供するソフトウェア及びそのソフトウェアを動作させるサーバをいう。
⑷９　名前解決　ドメイン名やホスト名とＩＰアドレスを変換することをいう。
⑸０　データベース　サーバのうち、特にデータの管理に特化し、専用の装置とデータベースファイルを合わせたもので、要保護情報を保管するものをいう。
⑸１　テレワーク　情報通信技術（ＩＣＴ：Information and Communication Technology）を活用した、場所や時間を有効に活用できる柔軟な働き方のうち、自宅で業務を行う在宅勤務及び主たる勤務官署以外に設けられた執務環境で業務を行うサテライトオフィス勤務のことをいう。
⑸２　モバイル勤務　情報通信技術を活用した、場所や時間を有効に活用できる柔軟な働き方のうち、モバイル端末等を活用して移動中や出先で業務を行うことをいう。

第２　情報セキュリティ対策の基本的枠組み

１　体制の整備

⑴　区域情報セキュリティ管理者等の設置

ア　区域情報セキュリティ管理者の設置

⑦　情報セキュリティ管理者は、各庁舎の敷地を複数の区域に分割し、当該区域をクラス０から３に分類する。

⑴　クラス０の区域を除く各区域に区域情報セキュリティ管理者を置

き、情報セキュリティ管理者が指名する者をもって充てる。

イ　運用管理者の設置

㈠　所属に運用管理者を置き、それぞれ当該所属の長をもって充てる。

㈡　運用管理者は、所属における警察情報システムの運用に関し、情報セキュリティの維持及び管理対象情報の適正な取扱いを確保するために必要な事務を処理するものとする。

ウ　管理責任者の設置

㈠　所属に管理責任者を置き、警察本部、方面本部、警察学校及びサイバーセキュリティ対策本部にあっては次席（次席に相当する者を含む。）、警察署にあっては副署長をもって充てる。

㈡　管理責任者は、運用管理者を補佐するものとする。

エ　システムセキュリティ責任者の設置

㈠　警察情報システムの整備を担当する所属にシステムセキュリティ責任者を置き、それぞれ当該所属の長をもって充てる。

㈡　システムセキュリティ責任者は、整備する警察情報システムが必要な情報セキュリティ要件を備え、当該警察情報システムの情報セキュリティを維持するための事務を処理するものとする。

オ　システムセキュリティ維持管理者の設置

㈠　警察情報システムを構成する電子計算機及びネットワーク機器の適切な維持管理のため、システムセキュリティ責任者が必要と認めた範囲の管理者権限を保有する所属に、システムセキュリティ維持管理者を置き、それぞれ当該所属の長をもって充てる。

㈡　システムセキュリティ維持管理者は、システムセキュリティ責任者の指示等を受け、担当する警察情報システムの維持管理のための事務を処理するものとする。

⑵　情報セキュリティインシデントに備えた体制の整備

ア　セキュリティインシデントに迅速かつ的確に対処するため、道警察に北海道警察ＣＳＩＲＴを置く。

イ　北海道警察ＣＳＩＲＴの長は、警察本部情報管理課長をもって充てる。

また、北海道警察ＣＳＩＲＴの長を補佐させるため副長を置き、警察本部情報管理課次席をもって充てる。

ウ　北海道警察ＣＳＩＲＴの運営に係る事項については、北海道警察ＣＳＩＲＴの長の検討結果を基に、情報セキュリティ管理者が関係所属の長と協議して定める。

⑶　兼務を禁止する役割

ア　職員は、情報セキュリティ対策の運用において、以下の役割を兼務しないこと。

㈠　承認又は許可（以下「承認等」という。）の申請者と当該承認等を行う者（以下「承認権限者等」という。）

㈡　監査を受ける者とその監査を実施する者

イ　職員は、承認等を申請する場合において、自らが承認権限者等であるときその他承認権限者等が承認等の可否の判断をすることが不適切と認められるときは、当該承認権限者等の上司又は適切な者に承認等を申請し、承認等を得ること。

⑷　その他

区域情報セキュリティ管理者、運用管理者、システムセキュリティ責任者及びシステムセキュリティ維持管理者は、それぞれの事務のうち分庁舎において処理されるものについて、情報セキュリティ管理者の許可を受けた場合には、当該分庁舎の警視の階級にある警察官又はこれに相当する一般職員を指名した上で分掌させることができる。

２　運用

⑴　情報セキュリティ関係規程の運用

ア　情報セキュリティ対策の運用

㋐　情報セキュリティ管理者は、警察情報セキュリティポリシーに係る課題、問題点及び重大な違反の報告を受けた場合には、速やかに警察庁情報セキュリティ管理者（警察庁長官官房技術企画課長をいう。以下同じ。）に報告すること。

㋑　情報セキュリティ管理者は、警察情報セキュリティポリシーの解釈に関する疑義を裁定すること。

イ　違反への対処

㋐　職員は、警察情報セキュリティポリシー又は第５の１の⑵のアの事項に基づき制定する運用要領等に違反する行為を認知したときは、システムセキュリティ維持管理者を通じて、速やかにシステムセキュリティ責任者に報告すること。

㋑　システムセキュリティ責任者は、警察情報セキュリティポリシー又は運用要領等への重大な違反を認知した場合には、違反者及び必要な者に情報セキュリティの維持に必要な措置を講じさせるとともに、情報セキュリティ管理者に報告すること。

⑵　例外措置

ア　例外措置手続

㋐　職員は、警察情報セキュリティポリシーにおいて定められた情報セキュリティの維持に関する事項を遵守することが困難であり、かつ合理的理由がある場合は、㋑、イ、ウの事項及び情報セキュリティ管理者が別に定める手続により、当該事項の適用の除外（以下「例外措置」という。）を受けることができる。

なお、例外措置の適用に当たっては、当該事項の趣旨を踏まえ、できる限り代替措置を講ずるよう努めること。

㋑　職員からの例外措置の適用申請について審査し、許可する者（以下「許可者」という。）は、情報セキュリティ管理者とする。ただし、例外措置の適用申請を行う職員（以下「申請者」という。）が情報セキュリティ管理者である場合及び申請が警察情報セキュリティ監査に関するものである場合は、警察本部長を許可者とする。

イ　例外措置の運用

㋐　申請者は、情報セキュリティ管理者が別に定める様式により、許可者に対して事前に申請を行うこと。ただし、緊急を要する場合は、システムセキュリティ維持管理者又は運用管理者の許可を受けることで例外措置の適用を受けたものとみなす。この場合において、許可者に対する申請は、例外措置の適用後、速やかに行うこと。

なお、例外措置の適用期間は、申請の対象となる警察情報システム

の整備目的等を踏まえ許可者が特に認めた場合を除き、最長１年間とする。

㈠　許可者は、申請内容を審査し、情報セキュリティ上の影響と対処方法を検討し、その検討結果を記録すること。

㈡　許可者は、㈠の事項の検討を基に許可の可否を決定し、情報セキュリティ管理者が別に定める様式により審査の結果を申請者に通知すること。

㈢　許可者は、㈠の事項に定める申請及び㈡の事項に定める通知に係る文書を適正に管理すること。

ウ　その他

㈠　職員は、大規模災害、重大テロ等の緊急事態であって、この文書に定める規定を遵守することが困難なときは、運用管理者等の指示により、これらの規定によらずに管理対象情報を処理することができる。

㈡　情報セキュリティ管理者は、災害時等において、警察情報システムの復旧、通信手段の確保等のためにやむを得ないときは、警察情報セキュリティポリシーの規定にかかわらず、所要の措置を講ずること。

㈢　システムセキュリティ責任者は、特定の警察情報システムについて、この文書に定めた情報セキュリティ要件を適用することが困難であると判断したときは、情報セキュリティ管理者と協議の上、当該警察情報システムの情報セキュリティ要件について、別段の定めを置くことができる。

⑶　教養

ア　情報セキュリティ管理者は、職員に警察情報セキュリティポリシーを正しく理解させ、確実に遵守させるため、職員に対し、職務に応じた教養を実施すること。

イ　職員は、教養実施計画に従って、適切な時期に教養を受講すること。

ウ　運用管理者は、職員に対して警察情報セキュリティポリシーに係る教養を適切に受講させること。また、運用管理者は、ＣＳＩＲＴに属する職員に役割に応じた教養を適切に受講させること。

エ　運用管理者は、職員に対する教養の実施状況について、情報セキュリティ管理者に報告すること。

オ　システムセキュリティ維持管理者は、システム管理担当者及びネットワーク管理担当者に対して、規範意識等の醸成に資する教養を定期的に実施すること。

⑷　情報セキュリティインシデントへの対処

ア　情報セキュリティインシデントに備えた事前準備

㈠　情報セキュリティインシデントの可能性がある事案のうち、北海道警察ＣＳＩＲＴへの報告を要するもの（以下「要報告インシデント」という。）は、次に掲げるものとする。

ａ　情報流出事案

管理対象情報の流出事案

ｂ　重大障害事案

警察情報管理システム（警察情報管理システム運営規程（令和３年警察本部訓令第14号）第２条に定めるものをいう。以下同じ。）において発生した障害であって、30分以上にわたって警察業務に重

大な影響を及ぼす事案

c　不正プログラム感染事案、不正アクセス事案及びサイバー攻撃事案

⒜　警察情報システムにおける不正プログラム感染事案

⒝　警察情報システムに対する不正アクセス事案

⒞　警察情報システムに対するサイバー攻撃事案（⒜及び⒝の事項に掲げるものを除く。）

d　警察情報システムの不正使用事案

あらかじめ定められた目的以外の目的で当該警察情報システムを不正に使用した事案

e　個人所有の機器の不正使用事案

⒜　管理対象情報を、個人所有の機器において不正に処理した事案

⒝　個人所有の機器を警察情報システムに不正に接続した事案

f　外部委託先等における情報流出事案

⒜　警察情報システムに係る外部委託先における事案

⒝　警察情報システムに係る外部委託について、契約に至らずとも契約を前提としてやり取りを行った事業者における事案

⒞　都道府県警察の情報システムに係る外部委託先における事案

⒟　その他の外部委託について、重大なインシデントに当たる可能性のある事案

⒠　その他の外部委託について、重大なインシデントに当たると認められない事案

g　その他社会的反響が大きいと予想される事案（ａからｆまでの事項に掲げるものを除く。）警察情報システム及び管理対象情報並びに道警察が設置又は運用する情報システム（警察情報システムに該当するものを除く。）に係る情報セキュリティを損なう事案であって、ａからｆまでの事項に掲げるものを除き、報道されるなど社会的反響が大きいと予想されるもの。

⑷　情報セキュリティ管理者は、情報セキュリティインシデントに備え、業務の遂行のため特に重要と認めた警察情報システムについて、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。

⑸　情報セキュリティ管理者は、情報セキュリティインシデントへの対処の訓練の必要性を検討し、業務の遂行のため特に重要と認めた警察情報システムについて、その訓練の内容及び体制を整備すること。

⑹　情報セキュリティ管理者は、情報セキュリティインシデントについて部外の者から報告を受けるための窓口を整備し、その窓口への連絡手段を部外の者に明示すること。

⑺　情報セキュリティ管理者は、対処手順が適切に機能することを訓練等により確認すること。

⑻　北海道警察ＣＳＩＲＴの長は、情報セキュリティインシデントの種類、規模及び影響を総合的に検討し、必要に応じて、北海道警察ＣＳＩＲＴ、情報セキュリティインシデントが発生した所属、その他関連所属の役割分担を調整すること。

イ　情報セキュリティインシデントへの対処

⑴　職員は、要報告インシデントを認知したときは、北海道警察ＣＳＩ

ＲＴ、関係する警察情報システムの維持管理を担当する所属及び当該所属の運用管理者に速やかに報告し、指示に従うこと。

㈠　㈠の事項の報告を受けた北海道警察ＣＳＩＲＴは、警察庁ＣＳＩＲＴに速やかに報告すること。

㈡　北海道警察ＣＳＩＲＴの長は、報告された情報セキュリティインシデントの可能性がある事案について、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うこと。

㈢　北海道警察ＣＳＩＲＴの長は、情報セキュリティインシデントの発生及び対処状況について、遅滞なく情報セキュリティ管理者に報告すること。

㈣　北海道警察ＣＳＩＲＴの長は、関係するシステムセキュリティ責任者及び情報セキュリティインシデントが発生した所属の長に対し、被害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必要な指示又は助言を行うこと。

㈤　システムセキュリティ責任者は、情報セキュリティインシデントの可能性を認知した場合は、関係するシステムセキュリティ責任者、システムセキュリティ維持管理者及び運用管理者と緊密に連携し、あらかじめ定められた対処手順及び北海道警察ＣＳＩＲＴの長からの指示又は助言に従って、適切に対処すること。

㈥　㈤の事項の情報セキュリティインシデントの可能性を認知した際に、「政府共通プラットフォーム」等の基盤となる情報システムに関するものであり、当該基盤となる情報システムの情報セキュリティ対策に係る運用管理規定等が定められている場合は、その規定に従い、適切に対処すること。

㈦　北海道警察ＣＳＩＲＴは、要報告インシデントが警察における情報セキュリティの確保に重大な支障を及ぼし、又は及ぼすおそれがあるときは、関係する警察本部の所属及び北海道警察サイバーセキュリティ対策本部に、社会的な反響が大きいと予想されるときは、併せて警察本部広報課にその概要を連絡すること。さらに、第２の２の⑷のアの㈠のｃの㈢の事項に定める事案に該当するおそれがあるときは、北海道警察情報通信部情報技術解析課にその概要を連絡すること。

㈧　北海道警察ＣＳＩＲＴの長は、関係するシステムセキュリティ責任者及び情報セキュリティインシデントが発生した所属の長に対し、被害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必要な指示又は助言を行うこと。

㈨　北海道警察ＣＳＩＲＴは、情報セキュリティインシデントへの対処の内容について、必要な事項を記録すること。

㈩　北海道警察ＣＳＩＲＴによる情報セキュリティインシデントへの対処状況を検証するため、北海道警察ＣＳＩＲＴの長は、必要に応じて情報セキュリティ委員会に活動状況を報告すること。

ウ　情報セキュリティインシデントの再発防止・教訓の共有

㈠　システムセキュリティ責任者は、北海道警察ＣＳＩＲＴの長から応急措置の実施及び復旧に係る指示又は助言を受けた場合は、当該指示又は助言を踏まえ、情報セキュリティインシデントの原因を調査するとともに、再発防止策を検討し、情報セキュリティ管理者に報告する

こと。

㈠　報告を受けた情報セキュリティ管理者は、その内容を確認し、必要に応じて再発防止策を実施するために必要な措置を指示すること。

㈡　北海道警察ＣＳＩＲＴの長は、情報セキュリティインシデントへの対処により得られた教訓について、システムセキュリティ責任者等に対して共有を図ること。さらに、情報セキュリティインシデントではないと評価した場合であっても、注意喚起等が必要と考えられるものについては、関係する者に情報共有を図ること。

３　情報セキュリティ対策の自己点検

⑴　自己点検の実施

ア　情報セキュリティ管理者は、職員に対し、情報セキュリティ対策に関する自己点検の実施を指示すること。

イ　職員は、情報セキュリティ管理者から指示された自己点検票及び自己点検の手順を用いて自己点検を実施すること。

⑵　自己点検結果の評価・改善

情報セキュリティ管理者は、道警察に共通の課題の有無を確認するなどの観点から自己点検結果を分析し評価すること。

４　情報セキュリティ関係規程の見直し

情報セキュリティ管理者は、情報セキュリティの運用及び自己点検・監査等の結果等を踏まえて警察情報セキュリティポリシーの規定について見直しを行う必要性の有無を適宜検討し、必要があると認めた場合にはその見直しを行うこと。

第３　管理対象情報の取扱い

管理対象情報の取扱いについては、文書管理に関する規程、個人情報保護に関する規程等の別に定める規程による適正な管理を行うほか、本項目に定めるところにより行うものとする。

１　管理対象情報の取扱い

⑴　管理対象情報の目的外での利用等の禁止

職員は、自らが担当している業務の遂行のために必要な範囲に限って、警察情報システム及び管理対象情報を取り扱うこと。

⑵　管理対象情報の分類及び取扱制限の決定・明示等

ア　職員は、管理対象情報を作成又は職員以外の者から入手したときは、当該情報の分類及び当該分類に応じた取扱制限を定めること。

イ　職員は、管理対象情報を機密性１（低）情報に分類する場合には、当該情報が明らかに非開示情報に該当すると判断される蓋然性の高い情報を含まないものである場合を除き、所属の上級の職員の承認を得ること。

ウ　職員は、部内においては、管理対象情報の機密性の分類及び取扱制限が明らかである場合を除き、管理対象情報の機密性の分類及び取扱制限を明示すること。

エ　職員は、職員以外の者に管理対象情報を提供する場合には、情報セキュリティ管理者が別に定めるものを除き、管理対象情報の機密性の分類及び取扱制限を明示すること。

オ　職員は、管理対象情報を作成又は複製する場合際に、参照した管理対象情報又は入手した管理対象情報に分類及び取扱制限の決定が既になされている場合には、元となる管理対象情報の機密性に係る分類及び取扱

制限を継承すること。

カ　職員は、修正、追加、削除その他の理由により、管理対象情報の分類及び取扱制限を見直す必要がある場合には、管理対象情報の分類及び取扱制限の決定者等に確認し、その結果に基づき見直すこと。

⑶　管理対象情報の利用・保存

ア　職員は、次に掲げる事項に留意して、管理対象情報を適切に取り扱うこと。

㋐　管理対象情報を不正に作成又は入手しないこと。

㋑　管理対象情報を不正に利用又は毀損しないこと。

㋒　要保護情報を放置しないこと。

㋓　要機密情報を必要以上に配布しないこと。

㋔　要機密情報を必要以上に複製しないこと。

イ　職員（運用管理者以上の職位の者を除く。）は、警察庁舎外において、機密性３（高）情報を利用する場合は、⑸のイの㋑の事項に定める手続により運用管理者の許可を得ること。

ウ　職員は、情報セキュリティ管理者が別に定める場合を除き、警察庁舎外に設置されている機器に要機密情報を保存しないこと。

エ　職員は、保存する管理対象情報にアクセス制限を設定するなど、管理対象情報の分類及び取扱制限に従って管理対象情報を適切に管理すること。

オ　職員は、外部記録媒体を用いて管理対象情報を取り扱う場合には、第８の１の⑵のウの規定に従うこと。

カ　職員は、外部との電子メールの送受信等、要機密情報の取扱いが認められるものとして整備された警察情報システムを除き、外部回線に接続する警察情報システムにおいて、要機密情報を取り扱わないこと。

キ　職員は、警察が維持管理を行っていない機器に、機密性３（高）情報を保存しないこと。

⑷　管理対象情報の提供・公表

ア　職員は、管理対象情報を公表する場合には、当該情報が機密性１（低）情報に分類されることを確認すること。

イ　職員は、要機密情報について、閲覧可能な範囲外の者への提供を行う場合には、⑸のイの事項に定める手続により提供すること。また、提供先において、当該情報に付された分類及び取扱制限に応じて適切に取り扱われるよう、取扱上の留意事項を確実に伝達するなどの措置を講ずること。

ウ　職員は、管理対象情報を職員以外の者に電磁的記録で提供する場合には、ファイルの属性情報等からの情報漏えいを防止すること。

⑸　管理対象情報の運搬・送信

ア　職員は、要保護情報が記録又は記載された記録媒体の警察庁舎外への運搬を第三者へ依頼する場合には、情報セキュリティを損なうことのないよう留意して運搬方法を決定し、管理対象情報の分類及び取扱い制限に応じて、適切な措置を講ずること。

イ　職員（運用管理者以上の職位の者を除く。）は、要機密情報について、警察庁舎外への持ち出しを行う場合には、⑵のカの事項に基づき当該情報の分類及び取扱制限の見直しを行った上で、次の事項を遵守すること。

㈠　機密性２（中）情報を警察庁舎外に持ち出す場合には、所属の上級の職員に報告すること。

㈡　機密性３（高）情報を警察庁舎外に持ち出す場合には、運用管理者の許可を得ること。

ウ　職員は、機密性２（中）情報を外部回線を用いた電子メールにより送信する場合には、情報セキュリティを損なうことのないよう留意して送信の手段を決定し、管理対象情報の分類及び取扱制限に応じて、適切な措置を講ずること。

エ　職員は、機密性３（高）情報を外部回線を用いた電子メールを送信しないこと。

⑹　管理対象情報の消去

ア　職員は、電磁的記録媒体に保存された管理対象情報が職務上不要となった場合には、速やかに当該管理対象情報を消去すること。

イ　職員は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に管理対象情報が残存した状態とならないよう、全ての管理対象情報を復元できないように抹消すること。

なお、端末やサーバ等をリース契約で調達する場合の、契約終了に伴う返却時の情報の抹消方法及び履行状況の確認手段については、必要な対策を講ずること。

ウ　職員は、要機密情報が記載された書面を廃棄する場合には、復元が困難な状態にすること。

⑺　管理対象情報のバックアップ

ア　職員は、要保全情報又は要安定情報を持ち出すときは、運用管理者の許可を得るとともに、必要に応じてバックアップを取得すること。

イ　職員は、取得した管理対象情報のバックアップについて、分類及び取扱制限に従って適切に管理すること。

２　管理対象情報を取り扱う区域の管理

⑴　区域における対策の基準

各区域の特性に応じた対策の基準は、情報セキュリティ管理者が別に定める。

⑵　区域ごとの対策の決定

ア　情報セキュリティ管理者は、⑴の事項に定める対策の基準を踏まえ、施設及び執務環境に係る対策を行う単位ごとの区域を定めること。

イ　区域情報セキュリティ管理者は、⑴の事項に定める対策の基準を踏まえ、当該区域における情報セキュリティの確保のための管理対策を講ずること。

⑶　区域における対策の実施

ア　区域情報セキュリティ管理者は、管理する区域に対して定めた対策を実施すること。また、職員が講ずべき対策については、職員が認識できる措置を講ずること。

イ　区域情報セキュリティ管理者は、自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策を講ずること。

ウ　職員は、利用する区域について区域情報セキュリティ管理者が定めた対策に従って利用すること。また、職員以外の者を立ち入らせるときには、当該職員以外の者にも当該区域で定められた対策に従って利用させ

ること

第４　外部委託

１　業務委託

⑴　業務委託に係る契約

ア　システムセキュリティ責任者は、次に掲げる事項を例として、情報セキュリティ対策の実施を委託先の選定条件とし、仕様書等に盛り込むこと。

㈠　委託先に提供する管理対象情報の委託先における目的外利用の禁止

㈡　委託先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

㈢　委託事業の実施に当たり、委託先事業者若しくはその従業員、再委託先、又はその他の者による意図しない変更が加えられないための管理体制

㈣　委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供

㈤　情報セキュリティインシデントへの対処方法

㈥　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

㈦　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

イ　システムセキュリティ責任者は、委託する業務において取り扱う管理対象情報の分類等を勘案し、必要に応じて次に掲げる事項を仕様書等に盛り込むこと。

㈠　情報セキュリティ監査の受入れ

㈡　サービスレベルの保証

ウ　システムセキュリティ責任者は、外部委託によって情報セキュリティが損なわれることのないよう、十分に検討の上、委託先には事業継続性を有すると認められる事業者を選定すること。

エ　システムセキュリティ責任者は、委託先がその役務内容を一部再委託する場合には、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、⑴のアからウまでの事項に定める措置の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を委託先に報告させるなどにより、適切に対策が実施されているかどうか確認するために必要な情報をシステムセキュリティ責任者に提供し、システムセキュリティ責任者の承認を受けるよう、仕様書等に盛り込むこと。

オ　システムセキュリティ責任者は、委託先によるアクセスを認める情報及び情報システムの範囲を適切に判断すること。

カ　システムセキュリティ責任者は、あらかじめ当該委託に係る作業を監督する職員の任務を定めるとともに、情報セキュリティの観点から委託の相手方に遵守させるべき事項を仕様書等に盛り込むこと。

⑵　業務委託における対策の実施

ア　システムセキュリティ責任者は、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認すること。

イ　システムセキュリティ責任者は、委託した業務において、情報セキュリティインシデント、管理対象情報の目的外利用等を認知した場合又はその旨の報告を職員より受けた場合は、委託業務を一時中断するなどの

必要な措置を講じた上で、委託先に契約に基づく対処を講じさせること。

ウ　システムセキュリティ責任者は、委託した業務の終了時に、委託先において取り扱われた管理対象情報が確実に返却又は抹消されたことを確認すること。

⑶　業務委託における情報の取扱い

ア　職員は、委託先に要保護情報を提供する場合は、提供する管理対象情報を必要最小限とし、あらかじめ定められた安全な受渡し方法により提供すること。

イ　職員は、提供した要保護情報が委託先において不要になった場合は、これを確実に返却又は抹消させること。

ウ　職員は、委託した業務において、情報セキュリティインシデント、情報の目的外利用等を認知した場合は、速やかにシステムセキュリティ責任者又は運用管理者に報告すること。

２　外部サービスの利用

⑴　要機密情報を取り扱う場合

ア　外部サービスの選定（クラウドサービスの場合）

⑺　システムセキュリティ責任者又は運用管理者は、クラウドサービスを利用する際、次に掲げる規定に従ってクラウドサービスを選定すること。

ａ　取り扱う管理対象情報の分類及び取扱制限を踏まえ、情報セキュリティ管理者が別に定める利用判断基準に従ってクラウドサービスの利用を検討し、利用する際は必要な手続をとること。ただし、検討に当たっては、リスク及びその低減措置を考慮すること。

ｂ　クラウドサービスで取り扱う管理対象情報の分類及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。また、業務に特有のリスクが存在する場合には、必要な情報セキュリティ対策を外部サービス提供者の選定条件に含めること。

ｃ　取り扱う管理対象情報の分類及び取扱制限並びにクラウドサービスとの情報セキュリティに関する役割及び責任の範囲を踏まえて情報セキュリティ要件を定め、クラウドサービスを選定すること。

⑴　システムセキュリティ責任者又は運用管理者は、情報を取り扱う場所及び契約に定める準拠法・裁判管轄を国内に指定すること。

なお、準拠法・裁判管轄を指定しても情報の開示が懸念される場合は、警察が管理する暗号鍵で情報を暗号化するなどの措置を検討すること。

⑼　職員は、最高情報セキュリティ管理者（警察庁長官官房長をいう。）が認めた場合を除き、クラウドサービスで機密性３（高）情報を取り扱わないこと。

⑽　１の⑴のウの事項は、クラウドサービスの選定に準用し、本規定中「システムセキュリティ責任者」とあるのは「システムセキュリティ責任者又は運用管理者」と読み替える。

⑾　システムセキュリティ責任者又は運用管理者は、外部サービス提供者がその役務内容を一部再委託する場合には、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外

部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報をシステムセキュリティ責任者に提供し、システムセキュリティ責任者の承認を受けるよう、外部サービス提供者の選定条件に含めること。また、外部サービスの利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断すること。

イ　外部サービスの選定（クラウドサービス以外の場合）

㈠　システムセキュリティ責任者又は運用管理者は、取り扱う管理対象情報の分類及び取扱制限を踏まえ、利用判断基準に従って外部サービス（クラウドサービスを除く。以下「その他の外部サービス」という。）の利用を検討し、利用する際は、必要な手続をとること。

㈡　システムセキュリティ責任者又は運用管理者は、その他の外部サービスで取り扱う管理対象情報の分類及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。

㈢　システムセキュリティ責任者又は運用管理者は、その他の外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含めること。

㈣　１の⑴のウ並びに２の⑴のアの㈡及び㈣の事項は、その他の外部サービスの選定に準用し、これらの規定中「システムセキュリティ責任者は」とあるのは「システムセキュリティ責任者又は運用管理者は」と読み替える。

㈤　システムセキュリティ責任者又は運用管理者は、取り扱う管理対象情報の分類及び取扱制限に応じて情報セキュリティ要件を定め、その他の外部サービスを選定すること。また、その他の外部サービスの情報セキュリティ要件として情報セキュリティに係る国際規格等と同等以上の水準を求めること。

㈥　システムセキュリティ責任者又は運用管理者は、その他の外部サービスの特性を考慮した上で、その他の外部サービスが提供する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るよう、情報の流通経路全般を見渡した形で情報セキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、情報セキュリティ要件を定めること。

㈦　システムセキュリティ責任者又は運用管理者は、その他の外部サービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し、利用の可否を判断すること。

ウ　外部サービスの利用に係る調達・契約

㈠　システムセキュリティ責任者又は運用管理者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めた情報セキュリティ要件を仕様書に含めること。

㈡　システムセキュリティ責任者又は運用管理者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが仕様書を満たすことを契約までに確認し、仕様書の内容を契約に含めること。

㈢　１の⑵及び⑶の事項は、外部サービスの利用に係る調達・契約に準用し、これらの規定中「システムセキュリティ責任者は」とあるのは「システムセキュリティ責任者又は運用管理者は」と読み替える。

エ　外部サービスの利用承認

㈠　システムセキュリティ責任者又は運用管理者は、外部サービスを利用する場合には、利用申請の許可権限者に外部サービスの利用申請を行うこと。

㈡　利用申請の許可権限者は、職員による外部サービスの利用申請を審査し、利用の可否を決定すること。

㈢　許可権限者は、当該申請に係る利用を承認した場合、利用承認した外部サービスについて記録し、申請者を外部サービス管理者として指名すること。

㈣　外部サービスの利用申請の許可権限者は、情報セキュリティ管理者とする。ただし、警察情報管理システムにおいてクラウドサービスを利用する場合は、情報セキュリティ管理者を経由して警察庁情報セキュリティ管理者の許可を得ること。

オ　外部サービスを利用した警察情報システムの導入・構築時の対策

㈠　システムセキュリティ責任者又は運用管理者は、外部サービスを利用して警察情報システムを構築する場合は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、次に掲げる事項を遵守すること。

ａ　不正なアクセスを防止するためのアクセス制御

ｂ　取り扱う情報の機密性保護のための暗号化

ｃ　開発時における情報セキュリティ対策

ｄ　設計・設定時の誤りの防止

㈡　システムセキュリティ責任者又は運用管理者は、㈠に掲げる事項について、構築時に実施状況を確認・記録すること。

㈢　１の⑴のオ及びカの事項は、外部サービスを利用した警察情報システムの導入・構築時の対策に準用する。

カ　外部サービスを利用した警察情報システムの運用・保守時の対策

㈠　外部サービス管理者は、外部サービスを利用した情報システムの運用・保守に際し、必要な対策を講ずること。

㈡　外部サービス管理者は、外部サービスで情報セキュリティインシデントを認知した場合は、第２の２の⑷のイの㈠、㈡、㈣及び㈥の事項に基づき、適切に対処すること。

㈢　外部サービス管理者は、㈠及び㈡の事項について、運用・保守時にその実施状況を定期的に確認・記録すること。

キ　外部サービスを利用した警察情報システムの更改・廃棄時の対策

㈠　外部サービス管理者は、外部サービスを利用した情報システムの更改・廃棄に際し、必要な対策を講ずること。

㈡　外部サービス管理者は、㈠の事項について、外部サービスの利用終了時に実施状況を確認・記録すること。

⑵　要機密情報を取り扱わない場合

ア　職員は、利用するサービスの約款、その他の提供条件等から、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、利用する際は必要な手続をとること。また、承認時に指名された外部サービス管理者は、

当該外部サービスの利用において適切な措置を講ずること。ただし、イの事項に定める場合及び検索サービスその他の外部サービスによりインターネット上に掲出された情報を閲覧する場合（アカウントの取得を必要としない場合に限る。）はこの限りでない。

イ　検索サービスその他の外部サービスによりインターネット上に掲出された情報を閲覧する場合（アカウントの取得を必要とする場合に限る。）には、取り扱う管理対象情報をアカウントの登録に必要な情報に限定した上で、運用管理者の許可を得ること。

ウ　ア及びイの事項における情報の閲覧の場合であっても、検索する情報が当該外部サービスの提供側において収集、分析され、関心事項が把握される可能性があることに留意すること。

エ　外部サービス上において要機密情報を取り扱わない場合に適用される規定について、次のとおり定める。

㈠　クラウドサービスを利用する場合

１及び２の⑴のエの規定を適用する。

㈡　その他の外部サービスを利用する場合

１の⑴のオ、カ及び２の⑴のエの規定を適用する。

第５　警察情報システムのライフサイクル

１　警察情報システムに係る文書等の整備

⑴　情報システム台帳の整備

ア　情報セキュリティ管理者は、道警察が整備した全ての情報システムに対して、情報システム台帳を整備すること。

イ　システムセキュリティ責任者は、所管する警察情報システムに係る情報システム台帳を、毎年４月及び警察情報システムを整備・変更する都度作成するとともに、その写しを情報セキュリティ管理者に提出しなければならない。

⑵　情報システム関連文書の整備

ア　システムセキュリティ責任者は、所管する警察情報システムごとに、当該警察情報システムを利用する業務を主管する所属の長と連携の上、情報セキュリティ管理者と協議し、当該警察情報システムの運用要領等を制定すること。

イ　アの運用要領等には、職員が当該警察情報システムを取り扱う際に遵守すべき事項として、次に掲げる事項を含むこと。

㈠　当該警察情報システムにおいて取り扱うことのできる管理対象情報の機密性、完全性及び可用性の分類の範囲

㈡　当該警察情報システムにおいて利用を認めるソフトウェア及び利用を禁止するソフトウェア

㈢　当該警察情報システムにおいて職員が独自の判断で行うことのできる改造（新たな機器の接続、ソフトウェア追加等）の範囲

㈣　当該警察情報システムにおける構成要素ごとの情報セキュリティ水準の維持に関する手順

㈤　情報セキュリティインシデントを認知した際の対処手順

ウ　職員は、アの事項に定める運用要領等について、警察情報セキュリティポリシーに定める管理体制と同等以上の水準であることについて情報セキュリティ管理者の確認を受けた場合には、当該運用要領等に従う

ものとする。

2　警察情報システムのライフサイクルの各段階における対策

⑴　警察情報システムの企画・要件定義

ア　実施体制の確保

㋐　システムセキュリティ責任者は、所管する警察情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保に努めること。

㋑　システムセキュリティ責任者は、基盤となる情報システムを利用して警察情報システムを構築する場合は、基盤となる情報システムに係る運用管理規程等で求められる事務を処理すること。

イ　警察情報システムのセキュリティ要件の策定

㋐　システムセキュリティ責任者は、警察情報セキュリティポリシーに定めるもののほか、所管する警察情報システムの設置環境、取り扱う管理対象情報の分類、管理対象情報を取り扱う者等に応じて、必要な対策を講ずること。

㋑　システムセキュリティ責任者は、インターネット回線と接続する警察情報システムを構築する場合は、接続するインターネット回線を定めた上で、標的型攻撃を始めとするインターネットからの様々なサイバー攻撃による情報の漏えい、改ざん等のリスクを低減するための多重防御のためのセキュリティ要件を策定すること。

㋒　システムセキュリティ責任者は、「IT製品の調達におけるセキュリティ要件リスト」（平成30年２月28日経済産業省）を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するための情報セキュリティ要件を策定すること。

㋓　システムセキュリティ責任者は、基盤となる情報システムを利用して警察情報システムを構築する場合は、基盤となる情報システム全体の情報セキュリティ水準を低下させることのないように、基盤となる情報システムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリティ要件を適切に策定すること。

ウ　警察情報システムの構築を業務委託する場合の対策

システムセキュリティ責任者は、警察情報システムの構築を業務委託する場合は、委託先に実施させる事項として、次に掲げる事項のほか、２の⑴のイの㋐、⑵のイの㋑、⑷のア、第６の２の⑴のアの事項等を、仕様書に記載するなどして、適切に実施させること。

㋐　警察情報システムのセキュリティ要件の適切な実装

㋑　警察情報セキュリティの観点に基づく試験の実施

㋒　警察情報システムの開発環境及び開発工程における情報セキュリティ対策

エ　警察情報システムの運用・保守を業務委託する場合の対策

㋐　システムセキュリティ責任者は、警察情報システムの運用又は保守を業務委託する場合は、警察情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、仕様書に記載するなどして、適切に実施させること。

㋑　システムセキュリティ責任者は、警察情報システムの運用又は保守

を業務委託する場合には、当該警察情報システムに対して委託先が実施する情報セキュリティ対策による当該警察情報システムの変更内容について、速やかに報告させること。

オ　その他

(ｱ)　システムセキュリティ責任者は、警察情報システムについてプログラム開発を行うときは、情報セキュリティを維持できるよう必要な対策を講ずること。

(ｲ)　システムセキュリティ責任者は、整備する警察情報システムの情報セキュリティ要件について、あらかじめ情報セキュリティ管理者の確認を受けること。

⑵　警察情報システムの調達・構築

ア　機器等の選定時の対策

(ｱ)　システムセキュリティ責任者は、機器等の選定時において、(ｲ)から(ｵ)までの事項を確認し、その結果を機器等の選定における判断の一要素として活用すること。

(ｲ)　システムセキュリティ責任者は、機器の調達については、(ｳ)、(ｴ)、２の⑴のイの(ｳ)及び２の⑵のウの(ｱ)の事項に定めるもののほか、情報セキュリティを維持できるよう必要な対策を講ずること。

(ｳ)　システムセキュリティ責任者は、機器の選定に当たっては、当該機器及び当該機器の製造者に係る情報の入手に努めること。

(ｴ)　システムセキュリティ責任者は、機器の選定に当たっては、(ｳ)の事項において入手した情報等を基に、情報セキュリティの確保に必要な機能及び信頼性を有するものを選定すること。

(ｵ)　システムセキュリティ責任者は、委託先の選定に当たっては、「IT調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」（平成30年12月10日関係省庁申合せ）に係る所要の措置を講ずること。

イ　警察情報システムの構築時の対策

(ｱ)　システムセキュリティ責任者は、警察情報システムの構築において、情報セキュリティの観点から必要な措置を講ずること。

(ｲ)　システムセキュリティ責任者は、警察情報システムの運用開始の手順及び環境を定めるに当たっては、情報セキュリティを損なうことのないよう留意するとともに、必要に応じて試験を実施すること。

ウ　納品検査時の対策

(ｱ)　システムセキュリティ責任者は、警察情報システムを構築する機器の調達に当たっては、必要に応じて、機器の納入時、検査等を実施すること。

(ｲ)　システムセキュリティ責任者は、警察情報システムの開発事業者から運用業者又は保守業者に引き継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認すること。

⑶　警察情報システムの運用・保守

ア　システムセキュリティ責任者は、所管する警察情報システムの運用及び保守において、当該警察情報システムに実装されたセキュリティ機能を適切に運用すること。

イ　システムセキュリティ責任者は、基盤となる情報システムを利用して

構築された警察情報システムを運用する場合は、基盤となる情報システムを整備し運用管理する組織との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切に警察情報システムを運用すること。

ウ　システムセキュリティ責任者は、必要に応じて、所管する警察情報システムにおける不正な通信等を監視するとともに、不正な通信等を認知した場合は、速やかに必要な対応を行うこと。

エ　システムセキュリティ維持管理者は、情報システムの構成や情報の処理手順を変更するなどの維持管理作業に必要なドキュメント及び記録簿を整備し、その内容を常に最新のものとしておくこと。

オ　システムセキュリティ維持管理者は、不正プログラム感染や不正アクセス等の外的要因によるリスク及び職員等の不適切な利用や過失等の内的要因によるリスクを考慮して、担当する警察情報システムの維持管理を行うこと。

⑷　警察情報システムの更改・廃棄

システムセキュリティ責任者は、警察情報システムの更改又は廃棄を行う場合には、当該警察情報システムに保存されている管理対象情報について、当該情報の分類及び取扱制限を考慮した上で、次に掲げる措置を適切に講ずること。

ア　警察情報システム移行時の管理対象情報の移行作業における情報セキュリティ対策

イ　警察情報システム廃棄時の不要な管理対象情報の抹消

⑸　警察情報システムについての対策の見直し

ア　システムセキュリティ責任者は、所管する警察情報システムの情報セキュリティ対策について脆弱性検査等により見直しを行う必要性の有無を適宜検討し、必要があると認めた場合にはその見直しを行い、必要な措置を講ずること。

イ　システムセキュリティ責任者は、この文書が施行された時点で整備済みの警察情報システムであって、この文書に定める事項を満たしていないものに限り、当該事項について、適用を猶予することができる。このとき、システムセキュリティ責任者は、可能な限り早期に要件を満たすことができるよう努めるとともに、情報セキュリティを確保するための代替手段を講ずること。

3　警察情報システムの業務継続計画の整備・整合的運用の確保

⑴　情報セキュリティ管理者は、非常時優先業務を支える警察情報システムの業務継続計画を整備するに当たり、非常時における情報セキュリティに係る対策事項を検討すること。

⑵　システムセキュリティ責任者は、所管する警察情報システムについて、非常時においても継続して運用できるよう十分検討し、必要に応じて業務継続計画を策定すること。また、当該業務継続計画は、可能な限り警察情報セキュリティポリシーとの整合を図ること。

⑶　情報セキュリティ管理者は、警察情報システムの業務継続計画の教養訓練や維持改善を行う際等に、非常時における情報セキュリティに係る対策事項が運用可能であるかを確認すること。

第６　警察情報システムの情報セキュリティ要件

システムセキュリティ責任者は、整備する警察情報システムについて、必要に応じてシステムセキュリティ維持管理者等に指示するなどして、次に定める技術的要件を満たすこと。

１　警察情報システムのセキュリティ機能

⑴　主体認証機能

ア　主体認証機能の導入

㋐　システムセキュリティ責任者は、ログイン時に主体認証を行う機能を設けること。

㋑　システムセキュリティ責任者は、国民・事業者と警察との間で申請、届出等のオンライン手続を提供する警察情報システムを整備する場合は、オンライン手続におけるリスクを評価した上で、主体認証に係る要件を策定すること。

㋒　システムセキュリティ責任者は、主体認証を行う警察情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずること。

イ　識別コード及び主体認証情報の管理

㋐　システムセキュリティ責任者は、警察情報システムにアクセスする全ての主体に対して、識別コード及び主体認証情報を適切に付与し、管理するための措置を講ずること。

㋑　システムセキュリティ維持管理者は、主体が警察情報システムを利用する必要がなくなった場合は、当該主体の識別コード及び主体認証情報の不正な利用を防止するための措置を速やかに講ずること。

⑵　アクセス制御機能

ア　システムセキュリティ責任者は、警察情報システムの特性、当該警察情報システムが取り扱う管理対象情報の分類及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設けること。

イ　システムセキュリティ維持管理者は、維持管理する警察情報システム及び管理対象情報へのアクセスを許可する主体が確実に制限されるように、アクセス制御機能を適切に運用すること。

⑶　権限の管理

ア　システムセキュリティ責任者は、主体から警察情報システム及び管理対象情報に対するアクセスの権限を適切に管理すること。

イ　システムセキュリティ維持管理者は、主体に対して管理者権限を付与する場合、主体の識別コード及び主体認証情報が、第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講ずること。

ウ　システムセキュリティ維持管理者は、管理者権限を適正に運用すること。

エ　システムセキュリティ維持管理者は、その管理する警察情報システムごとにシステム管理担当者を指名し、業務の責務に即した真に必要な範囲において、必要最小限の管理者権限を付与すること。

オ　エの指名に当たっては、システム管理担当者としての適格性について、あらかじめ情報セキュリティ管理者と協議して行うこと。ただし、警察

庁情報セキュリティ管理者が認める警察情報システムにあっては、この限りでない。

カ　システム管理担当者は、担当する警察情報システムに係るシステム管理に関する業務を行うものとする。

キ　システムセキュリティ維持管理者は、その管理するネットワークごとにネットワーク管理担当者を指名し、業務の責務に即した必要な範囲において、管理者権限を付与すること。

ク　ネットワーク管理担当者は、担当するネットワーク機器に係るネットワーク管理に関する業務を行うものとする。

⑷　証跡の取得・管理

ア　システムセキュリティ責任者は、警察情報システムにおいて、警察情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために、証跡を取得し、保管する機能を設けること。

イ　システムセキュリティ責任者は、情報システムにおいて、その特性に応じて証跡を取得する目的を設定した上で、証跡を取得する対象の機器等、証跡として取得する情報項目、証跡の保存期間等について、適切に証跡を管理すること。

ウ　システムセキュリティ責任者は、警察情報システムにおいて、取得した証跡を定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施すること。

⑸　暗号・電子署名

ア　暗号化機能・電子署名機能の導入

システムセキュリティ責任者は、警察情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、次に掲げる措置を講ずること。

㈠　管理対象情報を取り扱う警察情報システムについては、暗号化機能を設けること。ただし、次に掲げるものについては、この限りでない。

ａ　内蔵された電磁的記録媒体に要機密情報を保存しない電子計算機

ｂ　サーバ等であって、技術的に又は運用上暗号化が困難であるもの

ｃ　支給された携帯電話機（以下「公用携帯電話機」という。）であって、技術的に暗号化が困難であるもの

㈡　要保全情報を取り扱う警察情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。

㈢　暗号化又は電子署名の付与に当たって用いる暗号アルゴリズムについては、警察庁情報セキュリティ管理者の許可を受けた場合を除き、「電子政府における調達のために参照すべき暗号のリスト（ＣＲＹＰＴＲＥＣ暗号リスト）」（平成25年３月１日総務省・経済産業省。以下「暗号リスト」という。）に掲げたものを使用すること。

㈣　警察情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、暗号リストに記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること。

㈤　暗号化及び電子署名に使用する暗号（せい）アルゴリズムが危殆（たい）化した場合又はそれを利用したプロトコルに脆弱性が確認された場合を想定した

緊急対応手順を定めること。

㈎　暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定めること。

㈏　電子署名の目的に合致し、かつ適用可能な公的な公開鍵基盤が存在する場合はそれを使用するなど、目的に応じた適切な公開鍵基盤を使用すること。

イ　暗号化・電子署名に係る管理

システムセキュリティ責任者は、暗号及び電子署名を適切な状況で利用するため、次に掲げる措置を講ずること。

㈎　電子署名の付与を行う警察情報システムにおいて、電子署名の正当性を検証するための情報又は手段を、署名検証者に安全な方法で提供すること。

㈏　暗号化を行う警察情報システム又は電子署名の付与若しくは検証を行う警察情報システムにおいて、暗号化又は電子署名のために選択された暗号アルゴリズムの危殆化及びプロトコルの脆弱性に関する情報を定期的に入手すること。

2　情報セキュリティの脅威への対策

⑴　ソフトウェアに関する脆弱性対策

システムセキュリティ責任者は、ソフトウェアに関する脆弱性対策として次に掲げる措置を講ずること。

ア　警察情報システムの設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を講ずること。

イ　公開された脆弱性情報がない段階においても、サーバ等、端末及びネットワーク機器上で講じ得る対策がある場合は、必要な対策を講ずること。

ウ　サーバ等、端末及びネットワーク機器上で利用するソフトウェアにおける脆弱性対策の状況を確認する時間間隔を可能な限り短くすること。

エ　脆弱性情報が所管する警察情報システムにもたらすリスクを分析した上で、脆弱性対策計画を策定し、必要な措置を講ずること。

⑵　不正プログラム対策

システムセキュリティ責任者は、不正プログラム対策として次に揚げる措置を講ずること。

ア　電子計算機には、当該電子計算機上で動作するウイルス対策ソフトウェアが存在しない場合を除き、ウイルス対策ソフトウェアを導入すること。

イ　想定される不正プログラムの感染経路の全てにおいて、ウイルス対策ソフトウェア等により対策を講ずること。この場合において、必要に応じて、既知及び未知の不正プログラムの検知及びその実行の防止の機能を設けること。

ウ　不正プログラム対策の実施を徹底するため、ウイルス対策ソフトウェア等の導入状況、定義ファイルの更新状況等を把握し、必要な対処を行うこと。

⑶　サービス不能攻撃対策

システムセキュリティ責任者は、サービス不能攻撃対策として次に掲げる措置を講ずること。

ア　要安定情報を取り扱う外部回線に接続された警察情報システムについては、サービス提供に必要なサーバ等、端末及びネットワーク機器が装備している機能又は事業者等が提供する手段を用いてサービス不能攻撃への対策を講ずること。

イ　外部回線に接続する警察情報システムにおいて、要安定情報を取り扱う場合は、サービス不能攻撃を受けた場合の影響を最小とするため、ウの事項及び情報セキュリティ管理者が別に定める措置を講ずること。

ウ　サーバ等、端末、ネットワーク機器又は電気通信回線から監視対象を特定し、監視すること。

⑷　標的型攻撃対策

システムセキュリティ責任者は、標的型攻撃対策として次に掲げる措置を講ずること。

ア　標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずること。

イ　外部回線に接続された警察情報システムにおいて、内部ネットワークに侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講ずること。

⑸　外部記録媒体の利用に係る対策

システムセキュリティ責任者は、情報セキュリティ管理者が別に定めるところにより、外部記録媒体の利用を制限する機能を設けること。

3　アプリケーション・コンテンツの作成・提供

⑴　アプリケーション・コンテンツの作成時の対策

ア　システムセキュリティ責任者は、アプリケーション・コンテンツの提供時に道警察外の情報セキュリティ水準の低下を招かぬよう、アプリケーション・コンテンツの仕様書等に次に掲げる事項を盛り込むこと。

㈠　提供するアプリケーション・コンテンツが不正プログラムを含まないこと。

㈡　提供するアプリケーション・コンテンツが脆弱(ぜい)性を含まないこと。

㈢　実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。

㈣　電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。

㈤　提供するアプリケーション・コンテンツの利用時に、脆弱(ぜい)性が存在するバージョンのＯＳやソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、ＯＳやソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。

㈥　サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなど、サービス利用に当たって必須ではない機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。

イ　システムセキュリティ責任者は、アプリケーション・コンテンツの開発・作成を業務委託する場合には、アに掲げる内容を仕様書等に盛り込

むこと。

⑵　アプリケーション・コンテンツ提供時の対策

ア　行政機関のドメイン名の使用

システムセキュリティ責任者は、職員以外の者に電子メールを送信することを目的とした情報システム及びウェブサイト（業務委託する場合を含む。）については、外部サービスを利用する場合、公用携帯電話機を使用する場合又は特別な事情がある場合を除き、行政機関であることが保証されるドメイン名（「lg.jp」等）を使用すること。

イ　不正なウェブサイトへの誘導防止

システムセキュリティ責任者は、利用者が検索サイト等を経由して道警察のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講ずること。

ウ　アプリケーション・コンテンツの告知

⑺　職員は、アプリケーション・コンテンツを告知する場合は、告知する対象となるアプリケーション・コンテンツに利用者が確実に誘導されるよう、必要な措置を講ずること。

⑴　職員は、警察以外の者が提供するアプリケーション・コンテンツを告知する場合は、告知するURL等の有効性を保つこと。

第７　警察情報システムの構成要素

１　端末・サーバ等

⑴　端末

ア　端末の導入時の対策

⑺　システムセキュリティ責任者は、要保護情報を取り扱う端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

⑴　システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。

イ　端末の運用時の対策

⑺　システムセキュリティ責任者は、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。

⑴　システムセキュリティ責任者は、端末の情報セキュリティ対策について脆弱性検査等により見直しを行う必要性の有無を適宜検討し、必要があると認めた場合にはその見直しを行い、必要な措置を講ずること。

⑼　システムセキュリティ維持管理者は、各種ソフトウェアのうち利用しない機能を無効化すること。

⑽　システムセキュリティ維持管理者は、定期的に端末の脆弱性情報に係る対策及び端末に導入したソフトウェアのバージョンアップ等の状況を記録し、これを確認、分析すること。

ウ　端末の運用終了時の対策

システムセキュリティ責任者は、警察情報システムの更改又は廃棄を

行う場合には、当該警察情報システムの端末が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた管理対象情報が漏えいすることを防止するため、当該管理対象情報について、当該情報の分類及び取扱制限を考慮した上で、第５の２の(4)の事項に掲げる措置を適切に講ずること。

エ　モバイル端末及び公用携帯電話機の導入及び利用時の対策

(ｱ)　システムセキュリティ責任者は、モバイル端末について、盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための対策を講ずること。

(ｲ)　システムセキュリティ責任者は、公用携帯電話機について、盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための対策を講ずること。

(ｳ)　システムセキュリティ責任者は、モバイル端末及び公用携帯電話機の導入及び利用時の対策について、第８に定める対策を講ずることのできるよう情報セキュリティ要件を検討すること。

オ　個人所有の機器の導入及び利用時の対策

職員は、第８の１の(2)のエの事項に基づき個人所有の機器を利用する場合は、個人所有の機器の導入及び利用時の対策について、盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するため、必要な対策を講ずること。

(2)　サーバ等

ア　サーバ等の導入時の対策

(ｱ)　(1)のアの事項は、サーバ等の導入時の対策に準用する。

(ｲ)　システムセキュリティ責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、要安定情報を取り扱う警察情報システムについては、サービス提供に必要なサーバ等を２系統で構成する冗長化等により可用性を確保すること。

(ｳ)　システムセキュリティ責任者は、遠隔地からサーバ等に対して行われる保守又は診断の際に送受信される情報が漏えいすることを防止するための対策を講ずること。

イ　サーバ等の運用時の対策

(ｱ)　(1)のイの事項は、サーバ等の運用時の対策に準用する。

(ｲ)　システムセキュリティ責任者は、情報セキュリティインシデントの発生を監視する必要があると認めた場合には、監視のために必要な機能を設けること。

ウ　サーバ等の運用終了時の対策

(1)のウの事項は、サーバ等の運用終了時の対策に準用する。

(3)　複合機・特定用途機器

ア　複合機

(ｱ)　システムセキュリティ責任者は、複合機が備える機能、設置環境及び取り扱う管理対象情報の分類に応じ、適切な情報セキュリティ要件を満たすこと。

(ｲ)　システムセキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより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ずること。

㈢　システムセキュリティ責任者は、複合機の運用を終了する際には、複合機の電磁的記録媒体の全ての管理対象情報を抹消すること。ただし、情報セキュリティ管理者が別に定める場合にあっては、この限りでない。

イ　IoT機器を含む特定用途機器

システムセキュリティ責任者は、特定用途機器について、取り扱う管理対象情報、利用方法、電気通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じた対策を講ずること。

2　電子メール・ウェブ等

⑴　電子メール

システムセキュリティ責任者は、インターネットに接続された警察情報システムへの電子メールの導入時に次に掲げる対策を講ずること。

ア　電子メールサーバが電子メールの不正な中継を行わないように設定すること。

イ　電子メールの送受信時に主体認証を行う機能を設けること。ただし、シングルサインオン機能を利用することを妨げない。

ウ　電子メールのなりすましの防止策を講ずること。

エ　第８の１の⑶のキの事項に定める対策を講ずることのできるよう情報セキュリティ要件を検討すること。

⑵　ウェブ

システムセキュリティ責任者及びシステムセキュリティ維持管理者は、インターネットに接続された警察情報システムへのウェブサーバ等の導入時等に次に掲げる対策を講ずること。

ア　ウェブサーバの導入・運用時の対策

㈠　ウェブサーバが備える機能のうち、不要な機能を停止又は制限すること。

㈡　ウェブコンテンツの編集作業を担当する主体を限定すること。

㈢　公開してはならない又は無意味なウェブコンテンツが公開されないように管理すること。

㈣　ウェブコンテンツの編集作業に用いる端末を限定し、識別コード及び主体認証情報を適切に管理すること。

㈤　インターネットを介して転送される管理対象情報の盗聴及び改ざんを防止するため、当該管理対象情報に対する暗号化及び電子証明書による認証を行うこと。

㈥　ウェブサーバに保存する管理対象情報を特定し、サービスの提供に必要のない管理対象情報がウェブサーバに保存されないことを確認すること。

イ　ウェブアプリケーションの開発時・運用時の対策

ウェブアプリケーションの運用時において、既知の種類の脆弱性を排除するための対策に漏れが無いか定期的に確認し、対策に漏れがある状態が確認された場合は必要な措置を講ずること。

⑶　ドメインネームシステム（ＤＮＳ）

システムセキュリティ責任者及びシステムセキュリティ維持管理者は、インターネットに接続された警察情報システムへのドメインネームシステム（ＤＮＳ）の導入時等に次に掲げる対策を講ずること。

ア　ＤＮＳの導入時の対策

㈠　要安定情報を取り扱う情報システムの名前解決を提供するコンテンツサーバにおいて､名前解決を停止させないための措置を講ずること。

㈡　キャッシュサーバにおいて、名前解決の要求への適切な応答するための措置を講ずること。

㈢　コンテンツサーバにおいて、機関等のみで使用する名前の解決を提供する場合、当該コンテンツサーバで管理する情報が外部に漏えいしないための措置を講ずること。

イ　ＤＮＳの運用時の対策

㈠　系統間で同期をとるなどして情報の整合性を確保すること。

㈡　コンテンツサーバにおいて管理するドメインに関する情報が正確であることを定期的に確認すること。

㈢　キャッシュサーバにおいて、名前解決の要求への適切な応答を維持するための措置を講ずること。

⑷　データベース

システムセキュリティ責任者及びシステムセキュリティ維持管理者は、データベースの導入・運用時に次に掲げる対策を講ずること。

ア　データベースに対する内部不正を防止するため、管理者権限を持つ識別コードの適正な権限管理を行うこと。

イ　データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずること。

ウ　データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずること。

エ　データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するための対策を講ずること。

オ　データの窃取、電磁的記録媒体の盗難等による管理対象情報の漏えいを防止する必要がある場合は、適切に暗号化すること。

３　電気通信回線

⑴　電気通信回線

ア　電気通信回線の導入時の対策

㈠　システムセキュリティ責任者は、要機密情報を送受信する電気通信回線の選定に当たっては、機密性のみならず、完全性及び可用性の確保の観点から、次に掲げる順序で検討を行うこと。

ａ　拠点間の回線

専用回線（有線回線に限る。）、広域イーサネット（有線回線であって事業者閉域網のものに限る。）、ＩＰ－ＶＰＮ（有線回線であって事業者閉域網のものに限る。）、携帯電話回線（事業者閉域網のものに限る。）の順

ｂ　庁舎内回線

有線回線、無線回線の順

㈡　システムセキュリティ責任者は、必要に応じて、電気通信回線に接続される電子計算機をグループ化し、それぞれ電気通信回線上で論理的に分離すること。また、グループ化された電子計算機間での通信要件を検討し、当該通信要件に従ってネットワーク機器を利用しアクセス制御及び経路制御を行うこと。

⑺　システムセキュリティ責任者は、要機密情報を取り扱う警察情報システムを電気通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずること。

⑻　システムセキュリティ責任者は、ネットワーク機器を警察が管理する区域に設置すること。ただし、警察が管理する区域への設置が困難な場合は、施錠可能なラック等に設置するなどの措置を講ずること。

⑼　システムセキュリティ責任者は、要機密情報を電子メール等で送受信するインターネット回線について、次のａからｃまでの順序で導入を検討した上で、当該回線について各項目で示す事項を満たしていることについて情報セキュリティ管理者の確認を受けること。

ａ　一つの情報システムが単独で利用するインターネット回線（有線回線又は携帯電話回線）であること。

ｂ　他の情報システムとインターネット回線を共有する場合は、論理的に他の情報システムと分離していること。

ｃ　他の情報システムとインターネット回線を共有し、論理的に他の情報システムと分離できない場合は、次に掲げる対策を講ずること。

⒜　情報システム内の他の機器への不正な接続を制限する。

⒝　アクセス可能なウェブサイトを必要最小限に制限する。

⑽　システムセキュリティ責任者は、外部回線に接続された警察情報システムについて、メールサーバ、ファイアウォール、IDS/IPS等に係るアクセス等の履歴を管理するとともに、当該履歴の重要なイベントを検知後、直ちにネットワーク管理担当者等監視を担当している者に自動的に伝達されるようにすること。

⑾　システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、ネットワーク機器で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。

⑿　システムセキュリティ責任者は、ネットワーク機器が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順を整備すること。ただし、ソフトウェアを変更することが困難なネットワーク機器の場合は、この限りでない。

⒀　システムセキュリティ責任者は、遠隔地からネットワーク機器に対して行われる保守又は診断の際に送受信される情報が漏えいすることを防止するための対策を講ずること。

イ　電気通信回線の運用時の対策

⑺　システムセキュリティ責任者は、ネットワークの監視を行うこと。また、監視により得られた結果は、消去や改ざんが行われないように管理すること。

⑻　１の⑴のイの⑷及び⑸の事項は、電気通信回線の運用時の対策に準用し、これらの規定中「端末」とあるのは「電気通信回線及びネットワーク機器」と読み替える。

⑼　システムセキュリティ責任者は、所管する警察情報システムの情報セキュリティの確保が困難な事由が発生した場合には、当該警察情報システムが他の情報システムと共有している電気通信回線について、

共有先の情報システムを保護するため、必要に応じて、当該電気通信回線とは別に独立した閉鎖的な電気通信回線（論理的に他の情報システムと分離している場合を含む。）に構成を変更すること。

ウ　電気通信回線の運用終了時の対策

１の⑴のウの事項は、電気通信回線の運用終了時の対策に準用する。

エ　無線ＬＡＮ環境導入時の対策

システムセキュリティ責任者は、要機密情報を送受信するため、無線ＬＡＮ技術を利用して電気通信回線を構築する場合は、電気通信回線の導入時共通の対策に加えて、通信内容の秘匿性を確保するための通信路の暗号化を行うこと。

⑵　ＩＰｖ６通信回線

ア　ＩＰｖ６通信を行う警察情報システムに係る対策

㋐　システムセキュリティ責任者は、ＩＰｖ６技術を利用する通信を行う警察情報システムを構築する場合は、製品として調達する機器等について、IPv6 Ready LogoProgramに基づくPhase-2準拠製品を、可能な場合には選択すること。

㋑　システムセキュリティ責任者は、ＩＰｖ６通信の特性等を踏まえ、ＩＰｖ６通信を想定して構築する警察情報システムにおいては、次の事項を含む脅威又は脆弱性に対する検討を行い、必要な措置を講ずること。

ａ　グローバルＩＰアドレスによる直接の到達性における脅威

ｂ　ＩＰｖ６通信環境の設定不備等に起因する不正アクセスの脅威

ｃ　ＩＰｖ４通信とＩＰｖ６通信を情報システムにおいて共存させる際のＩＰｖ６通信の制御の不備に起因する脆弱性の発生

ｄ　ソフトウェアにおけるＩＰｖ６アドレスの取扱いの不備に起因する脆弱性の発生

イ　意図しないＩＰｖ６通信の抑止・監視

システムセキュリティ責任者は、サーバ等、端末及びネットワーク機器を、ＩＰｖ６通信を想定していない通信回線に接続する場合には、自動トンネリング機能で想定外のＩＰｖ６通信パケットが到達する脅威等、当該通信回線から受ける不正なＩＰｖ６通信による情報セキュリティ上の脅威を防止するため、ＩＰｖ６通信を抑止するなどの措置を講ずること。

第８　警察情報システムの利用

１　警察情報システムの利用

⑴　警察情報システム利用者の規定の遵守を支援するための対策

ア　システムセキュリティ責任者は、職員による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ警察情報システムを構築すること。

イ　職員は、簿冊により管理することとされている事項その他の警察情報セキュリティポリシーに定める手続について、システム構築等の技術的措置による電子化を検討し、事務負担の軽減に努めること。

ウ　イの定めに基づき電子化する手続は、警察情報セキュリティポリシーに定める手続と同等以上の管理水準であることについて情報セキュティ管理者の確認を受けることにより、警察情報セキュリティポリシーによ

らないことができる。

⑵　警察情報システム等の利用時の基本的対策

ア　警察情報システム

㈠　職員は、定められた目的以外の目的で警察情報システムを不正に使用しないこと。

㈡　職員は、外部回線に接続することを前提として整備された場合を除き、警察情報システムを外部回線に接続しないこと。

㈢　職員は、警察情報システムで利用される電気通信回線に、システムセキュリティ責任者の許可を受けていない警察情報システムを接続しないこと。

㈣　職員は、第５の１の⑵のイの㈢の事項に該当する場合を除き、システムセキュリティ責任者の許可なく、警察情報システムを構成する機器の改造（新たな機器の接続、ソフトウェア追加等）をしないこと。

㈤　職員は、警察情報システムにおいて管理対象情報を取り扱う場合には、システムセキュリティ責任者が定めた当該警察情報システムにおいて取り扱うことのできる機密性、完全性及び可用性の範囲を超えた管理対象情報を取り扱わないこと。

㈥　職員は、情報セキュリティ管理者が別に定める場合を除き、機器を警察庁舎外に不正に持ち出さないこと。

㈦　職員は、情報セキュリティ管理者が別に定める場合を除き、警察が管理する区域以外において外部回線に接続したことのある端末を、内部ネットワークに直接接続しないこと。

㈧　職員は、警察情報システムの利用時には、利用環境に配意し、関係のない者に管理対象情報を視認されないよう留意すること。特に主体認証情報を入力する際には、権限のない者に視認されていないことを確認すること。

㈨　職員は、他の者からアクセスさせる必要がない管理対象情報については、アクセスできないよう設定すること。

㈩　職員は、電子計算機又はネットワーク機器の取扱いに当たっては、設置環境を踏まえ、障害等により可用性を損なわないよう配慮すること。

㈪　職員は、この文書に定めるもののほか、取り扱う警察情報システムについて運用要領等の別に定められた文書や指示事項があるときは、それを遵守すること。

イ　公用携帯電話機

㈠　職員は、公用携帯電話機内の要機密情報を必要最小限にした上で、公用携帯電話機の警察庁舎外への持ち出しを行うことができる。ただし、共用する公用携帯電話機（音声通話機能のみを使用するものを除く。）については、情報セキュリティ管理者が別に定める手続により許可を得ること。

㈡　職員は、公用携帯電話機について、送受信メール履歴、電話帳等の情報のうち、要機密情報に当たるものを閲覧する場合には、主体認証情報入力等の主体認証を求められるよう設定すること。

㈢　職員は、公用携帯電話機について、情報セキュリティ管理者が別に定める方法により、適正に管理すること。

㈡　職員は、要機密情報を取り扱った公用携帯電話機を廃棄する場合には、情報の抹消を実施すること。

ウ　外部記録媒体

㈠　職員は、外部記録媒体について、情報セキュリティ管理者が別に定める方法により、適正に管理すること。

㈡　職員は､外部記録媒体を警察庁舎外に持ち出す必要がある場合には、外部記録媒体内の要機密情報を必要最小限にするとともに、情報セキュリティ管理者が別に定める手続により許可を得ること。

㈢　所属に一人又は複数人の管理補助者を置き、運用管理者が情報セキュリティ管理者が別に定める様式により指名する者をもって充てる。

㈣　管理補助者は、警部以上の階級にある警察官又はこれに相当する一般職員とする。

㈤　管理補助者は、電子計算機及び貸与された携帯電話機（公費で整備されたものに限る。）の管理並びに外部記録媒体及び外部記録媒体を利用した管理対象情報の入出力の管理に係る事務を処理するものとする。

エ　個人所有の機器

職員は、情報セキュリティ管理者が別に定める場合を除き、個人所有の機器において管理対象情報を処理しないこと。

⑶　電子メール・ウェブの利用時の対策

ア　職員は、管理対象情報を含む電子メールを送受信する場合には、警察が管理・運用（業務委託による場合を含む。）する電子メール機能又は公用携帯電話機の電子メール機能を利用すること。

イ　職員は、外部の者と電子メールにより情報を送受信する場合は、当該電子メールのドメイン名に行政機関であることが保証されるドメイン名を使用すること。ただし、第４の２の事項に規定する外部サービスを利用する場合、公用携帯電話機を使用する場合又は特別な事情がある場合を除く。

ウ　職員は、不審な電子メールを受信したときは、開封せずにシステム管理担当者に連絡すること。

エ　職員は、ウェブクライアントの設定を見直す必要がある場合は、情報セキュリティに影響を及ぼすおそれのある設定変更を行わないこと。

オ　職員は、外部回線から電子計算機にソフトウェアをダウンロードする場合には､電子署名により当該ソフトウェアの配布元を確認すること(電子署名が付与されていないものを除く。)。

カ　職員は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、次に掲げる事項を確認すること。

㈠　送信内容が暗号化されること。

㈡　当該ウェブサイトが送信先として想定している組織のものであること。

キ　職員は、機密性２（中）情報を電子メールにより外部に送信する場合には、当該情報に主体認証情報を設定し又は暗号化すること。

ク　職員は、多数の者に電子メールを一斉送信するときは、受信者同士でメールアドレス情報を共有する必要がある場合を除き、Ｂｃｃ（Blind

carbon copy）等の機能を用いて、受信者のメールアドレスが漏えいすることのないようにすること。

ケ　職員は、要機密情報を電子メールにより外部に送信したときは、やむを得ない場合を除き、送信後直ちに端末に内蔵された電磁的記録媒体から当該情報を消去すること。

コ　職員は、要機密情報を電子メールにより外部から受信したときは、当該情報を外部回線に接続された端末に内蔵された電磁的記録媒体に保存しないこと。やむを得ず一時的に保存したときは、外部記録媒体を用いて外部回線と接続されていない端末に取り込むなどして、可能な限り速やかに消去すること。

⑷　識別コード・主体認証情報の取扱い

ア　職員は、自己の識別コード以外の識別コードを不正に用いて、警察情報システムを使用しないこと。

イ　職員は、自己の主体認証情報を権限のない者に知られないよう管理を徹底すること。

⑸　暗号・電子署名の利用時の対策

ア　職員は、復号又は電子署名の付与に用いる鍵をインターネットに接続された電子計算機に保存しないこと。

イ　職員は、必要に応じて、鍵のバックアップを取得し、オリジナルの鍵と同等の安全管理を実施すること。

⑹　不正プログラム感染防止

ア　職員は、不正プログラム感染防止に関する措置に努めること。

イ　職員は、外部から受領した外部記録媒体又は外部の電子計算機に接続して利用した外部記録媒体を電子計算機に接続するときは、情報セキュリティ管理者が別に定める安全な方法によって外部記録媒体に不正プログラムが記録されていないことを確認すること。

⑺　ウェブ会議サービスの利用時の対策

ア　職員は、職務上ウェブ会議サービスを利用しようとする場合には、第４の２の⑴のアの⑺のａ、イの⑺又は⑵のアの事項に定める手続をとり、ウェブ会議の参加者や取り扱う管理対象情報に応じた情報セキュリティ対策を実施すること。

イ　職員は、ウェブ会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

２　ソーシャルメディアサービスによる情報発信

職員は、ソーシャルメディアサービスによる情報発信時に次に掲げる対策を講ずること。

⑴　職務上ソーシャルメディアサービスを利用し、情報発信をしようとする場合には、第４の２の⑵のアの事項に定める手続をとること。また、当該サービスの利用において、要機密情報を取り扱わないこと。

⑵　要安定情報の国民への提供にソーシャルメディアサービスを用いる場合は、道警察のウェブサイトに当該情報を掲載して参照可能とすること。

３　テレワーク及びモバイル勤務

⑴　実施環境における対策

ア　システムセキュリティ責任者は、テレワーク及びモバイル勤務の実施により外部回線を経由して警察情報システムへリモートアクセスする形

態となる警察情報システムを構築する場合は、通信経路及びリモートアクセス特有の攻撃に対する情報セキュリティを確保すること。

イ　システムセキュリティ責任者は、リモートアクセスに対し多要素主体認証を行うこと。

ウ　システムセキュリティ責任者は、リモートアクセスする端末を許可された端末に限定する措置を講ずること。

エ　システムセキュリティ責任者は、リモートアクセスする個人所有の端末を最新の脆弱性対策や不正プログラム対策が施されている端末に限定すること。

⑵　実施時における対策

ア　職員は、テレワーク及びモバイル勤務の実施前並びに実施後にチェックすべき項目について確認すること。

イ　職員は、画面ののぞき見や盗聴を防止できるようテレワーク又はモバイル勤務の実施場所を選定すること。また、自宅以外でテレワーク又はモバイル勤務を実施する場合には、離席時の盗難に注意すること。

ウ　職員は、テレワーク及びモバイル勤務時に、警察情報システムへの接続に利用する回線については、情報セキュリティ管理者が別に定める回線を使用すること。

第９　その他

この文書の実施に必要な細部事項については、情報セキュリティ管理者が別に定める。