原議保存期間	5年（令和14年3月31日まで）
有効期間	一種（令和14年3月31日まで）

庁内各局部課長
各附属機関の長
各地方機関の長　殿
各都道府県警察の長

警察庁 丙技企発第83号、丙生企発第45号
丙刑企発第15号、丙組一発第12号
丙交企発第21号、丙備企発第39号
丙外事発第27号、丙備一発第14号
丙サ企発第23号

令和８年４月27日
警察庁長官官房長
警察庁生活安全局長
警察庁刑事局長
警察庁交通局長
警察庁警備局長
警察庁サイバー警察局長

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（通達）

警察における情報セキュリティについては、警察における情報セキュリティに関する訓令（平成15年警察庁訓令第３号）第６条第２項、第８条第３項及び第９条に基づき、「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（通達）（令和５年９月28日付け警察庁丙技企発第61号ほか。以下「旧通達」という。）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政府機関等におけるサイバーセキュリティ対策のための統一基準群の改定等に伴い、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８年５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、旧通達は廃止する。

別添

令和８年４月

警察における情報セキュリティに関する

対策基準

目次

第１　総則

１　目的

この文書は、警察における情報セキュリティに関する訓令（平成15年警察庁訓令第３号。以下「訓令」という。）第６条第２項、第８条第３項及び第９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

(1)　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（警察庁における特定秘密の保護に関する訓令（平成26年警察庁訓令第８号）第１条に定めるものをいう。）、重要経済安保情報（警察庁における重要経済安保情報の保護に関する訓令（令和７年警察庁訓令第８号）第１条に定めるものをいう。）又は秘密文書（警察庁における行政文書の管理に関する訓令（平成23年警察庁訓令第９号）第２条第５号に定めるものをいう。）としての取扱いを要するもの

(ｲ)　機密性２（中）情報

管理対象情報のうち、行政機関の保有する情報の公開に関する法律（平成11年法律第42号。以下「情報公開法」という。）第５条各号における不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

(ｳ)　機密性１（低）情報

管理対象情報のうち、情報公開法第５条各号における不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

(ｱ)　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

(ｲ)　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

(ｱ)　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

(ｲ)　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

(2)　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　警察情報システムの分類等

(1)　警察情報システムの分類及び分類基準

警察情報システムの分類及び分類基準は次のとおりとする。

ア　重要度（高）システム

情報セキュリティインシデント発生時に、警察業務に重大な影響を及ぼす又は他の重要度（高）システムに影響を与える警察情報システム

イ　重要度（中）システム

要保護情報を取り扱う又は情報セキュリティインシデント発生時に他の重要度（中）システムに影響を与える警察情報システム（重要度（高）システムを除く。）

ウ　重要度（低）システム

重要度（高）システム及び重要度（中）システム以外の警察情報システム

(2)　警察情報システムの分類基準に基づいた情報セキュリティ対策

警察情報システムの分類基準に基づいた情報セキュリティ対策について、次のとおり定める。

ア　基本セキュリティ対策

警察情報システムの構成要素及び警察情報システムのセキュリティ要件に係る情報セキュリティ対策のうち、基本的な対策として全ての警察情報システムが実施すべき対策を基本セキュリティ対策とする。

なお、警察情報セキュリティポリシーにおいて、追加セキュリティ対策と示されていない警察情報システムの構成要素等に係る情報セキュリティ対策は全て基本セキュリティ対策に分類される。

イ　追加セキュリティ対策

警察情報システムの構成要素等に係る情報セキュリティ対策のうち、重要度が高いシステムに対して、基本セキュリティ対策に加えて実施することを求めるより高度な情報セキュリティ対策を追加セキュリティ対策とする。

4　用語の定義

警察情報セキュリティポリシーにおいて、次の各号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。

(1)　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。

(2)　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。

(3)　暗号リスト等

暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」及び別途警察庁情報セキュリティ管理者が定めた暗号リスト（ハイブリッド構成を含む。）をいう。

(4)　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。

(5)　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クラウドサービスをいう。

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。

(6)　外部委託

業務委託及びクラウドサービスをいう。

(7)　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。

(8)　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。

(9)　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。

(10) 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。

(11) 業務委託

外部委託のうち、警察の業務の一部又は全部について、契約をもって外部の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。ただし、当該業務において管理対象情報が取り扱われる場合に限る。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。

(12) クラウドサービス

部外の者が一般向けにインターネット等のネットワークを経由して情報システムの一部又は全部の機能を提供する、SaaS（Software as a Service)、PaaS（Platform as a Service)、IaaS（Infrastructure as a Service）等をいう。ただし、当該機能において管理対象情報が取り扱われる場合に限定する。

(13) クラウドサービス管理者

クラウドサービスの利用における利用申請の許可の権限を有する者から利用承認時に指名された当該クラウドサービスに係る管理を行う者をいう。

(14) クラウドサービス提供者

クラウドサービスを提供する事業者（クラウドサービスプロバイダ）をいう。

(15) クラウドサービス利用者

クラウド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クラウドサービスを利用する場合の委託先の従業員をいう。

(16) 警察共通基盤システム

「警察共通基盤システム等運営要領の制定について（通達)」（令和４

年12月１日付け警察庁丙技企発第22号ほか。）第１の２の用語の定義に定めるものをいう。

(17) 警察情報管理システム

「警察共通基盤システム等運営要領の制定について（通達）」（令和４年12月１日付け警察庁丙技企発第22号ほか。）第１の２の用語の定義に定めるものをいう。

(18) 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。

(19) 携帯電話機

フィーチャーフォン、スマートフォン等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。

(20) 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。

(21) 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。

(22) 識別コード

ユーザID、ホスト名等、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。

(23) 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、サーバ等をいう。

(24) 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。

(25) 主体認証情報

パスワード等、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。

(26) 主体認証情報格納装置

ICカード等、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。

(27) 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。

(28) 情報の抹消

電磁的記録媒体に記録された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をいう。情報の抹消には、情報自体を消去することのほか、暗号技術検討会及び関連委員会（CRYPTREC）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や、情報を記録している記録媒体を物理的に破壊すること等も含まれる。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態とはいえず、情報の抹消には該当しない。

(29) 職員

警察情報システム及び管理対象情報を取り扱う警察庁職員及び都道府県警察の職員をいう。

(30) 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。

(31) 政府共通利用型システム

他の政府機関を含め共通的に利用することを目的として、一つの政府機関が管理・運用する情報システムであって、他の政府機関が整備する情報システムに対し、同情報システムと連携して、情報システムのセキュリティ機能を提供する情報システム及び他の政府機関に機器等を提供し、他の政府機関の職員等が利用する情報システムをいう。

なお、政府共通利用型システムを構築・運用する機関を「政府共通利用型システム管理機関」といい、政府共通利用型システムが提供するセキュリティ機能を利用して情報システムを構築・運用する政府機関及び政府共通利用型システムが提供する機器等を利用する政府機関を「政府共通利用型システム利用機関」という。

(32) 戦略本部監査

サイバーセキュリティ基本法第26条第１項第２号に基づきサイバーセ

キュリティ戦略本部が実施する監査をいう。

(33) 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（SNS)、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。

(34) 耐量子計算機暗号

量子コンピュータによる攻撃への耐性、いわゆる耐量子計算機性を持つ一連の暗号をいう。PQC（Post-Quantum Cryptography）と呼ばれる。

(35) 通信回線装置

電気通信回線間又は電気通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。また、物理的なハードウェアを有する通信回線装置を「物理的な通信回線装置」という。

(36) 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。

(37) データ連係装置

セキュリティ要件の異なる分離された情報システム間においてネットワークを物理的又は論理的に切り替える、一方向にデータ移動するなどにより安全なデータ共有を図る装置をいう。

(38) 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。

(39) 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。

(40) 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する機能を備えている、又は電磁的記録媒体が内蔵されているものをいう。

(41) 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。

(42) 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。

(43) 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。

(44) ハイブリッド構成

既存の公開鍵暗号及び耐量子計算機暗号の両方を選択的に利用可能とする構成をいう。

(45) 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。

(46) 無害化

不正プログラム等の危険な要素を取り除く対策を実施することをいう。

(47) 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。

(48) 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。

(49) 要管理対策区域

情報セキュリティを確保するための対策を実施する必要がある区域をいう。

(50) 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。

(51) 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。

(52) 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。

(53) ルートヒント

最初に名前解決を問い合わせるDNSコンテンツサーバの情報をいう。

(54) 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。

(55) CYMAT（Cyber Incident Mobile Assistance Team）

サイバー攻撃等により政府機関等の情報システムに障害が発生した場合又はその発生のおそれがある場合であって、政府として一体となった対応が必要となる情報セキュリティに係る事象に対して機動的な支援を行うため、内閣官房国家サイバー統括室に設置される体制をいう。

(56) 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。

(57) DNSSECトラストアンカー

DNSSEC検証を行う際の、信頼の連鎖の起点情報をいう。

(58) HNDL（Harvest Now, Decrypt Later）攻撃

攻撃者が事前に暗号技術で保護されたデータを収集して保存しておき、量子コンピュータが利用可能となった後に当該データに対して行う攻撃をいう。

(59) IoT（Internet of Things）機器

従来インターネットに接続していなかったが、インターネットに接続する機能を備えるようになった機器をいう。

(60) 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。

第２　情報セキュリティ対策の基本的枠組み

１　導入・計画

(1)　組織・体制の整備

ア　情報セキュリティ管理者等の設置

(ｱ)　情報セキュリティ管理者の設置

a　警察庁及び都道府県警察に、情報セキュリティ管理者を置く。

b　情報セキュリティ管理者は、次に掲げる機関ごとに、それぞれに掲げる者をもって充てる。

(a)　警察庁内部部局

長官官房技術企画課長

(b)　警察大学校

教務部庶務課長

(c)　科学警察研究所

総務部総務課長

(d)　皇宮警察本部

監察課長

(e)　管区警察局（四国警察支局及び府県情報通信部を除く。）

情報通信部情報技術解析課長

(f)　四国警察支局（県情報通信部を除く。）

情報通信部情報技術解析課長

(g)　東京都警察情報通信部

情報技術解析課長

(h)　北海道警察情報通信部（方面情報通信部を除く。）

情報技術解析課長

(i)　府県情報通信部（四国警察支局の県情報通信部を含む。以下同じ。）及び方面情報通信部

部長

(j)　都道府県警察

情報管理に関する事務を所掌する部（部に準ずるものを含む。）の長

c　情報セキュリティ管理者は、それぞれの機関における情報セキュリティに係る事務を統括する。

d　情報セキュリティ管理者は、情報セキュリティに係る事務を統括するに当たっては、その事務に関係する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の意見を聴き、十分検討した上で処理すること。

e　警察庁情報セキュリティ管理者（ｂ(a)に定める者をいう。以下同じ。）は、最高情報セキュリティ管理者及び最高情報セキュリティ副管理者を補佐するため、附属機関及び地方機関の情報セキュリティ管理者が行う事務を総括整理するとともに、各都道府県警察の情報セキュリティ管理者が行う事務を調整する。

f　管区警察局及び四国警察支局の情報セキュリティ管理者は、管轄区域（中国四国管区警察局にあっては四国警察支局の管轄区域を除く。以下同じ。）の各府県情報通信部の情報セキュリティ管理者が行う事務を総括整理するとともに、管轄区域の各府県警察の情報セキュリティ管理者が行う事務を調整する。

g　北海道警察情報通信部の情報セキュリティ管理者は、各方面情報通信部の情報セキュリティ管理者が行う事務を総括整理する。

(ｲ)　区域情報セキュリティ管理者の設置

a　情報セキュリティ管理者は、それぞれの機関の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。

b　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。

(ｳ)　運用管理者の設置

a　警察情報システムを運用する警察庁及び都道府県警察の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。

b　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。

(ｴ)　システムセキュリティ責任者の設置

a　警察情報システムの整備を担当する所属にその企画の着手まで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。

b　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

a　警察情報システムを構成する電子計算機及び通信回線装置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。

b　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。

イ　最高情報セキュリティアドバイザーの設置

(ｱ)　警察庁に最高情報セキュリティアドバイザーを置き、警察庁長官官房技術企画課情報セキュリティ対策室長をもって充てる。

(ｲ)　最高情報セキュリティアドバイザーは、最高情報セキュリティ管理者及び最高情報セキュリティ副管理者に対し、情報セキュリティ対策の推進に係る助言を行う。

ウ　情報セキュリティ対策推進体制の整備

(ｱ)　警察庁長官官房技術企画課に、情報セキュリティ対策推進体制を置く。

(ｲ)　情報セキュリティ対策推進体制の長として、警察庁情報セキュリティ管理者をもって充てる。

(ｳ)　情報セキュリティ対策推進体制の構成員は、警察庁情報セキュリティ管理者が指名する。

エ　情報セキュリティインシデントに備えた体制の整備

(ｱ)　情報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、警察庁に警察庁CSIRTを置く。

(ｲ)　警察庁CSIRTの長は、警察庁長官官房技術企画課情報セキュリティ対策室長をもって充てる。

(ｳ)　警察庁CSIRTの運営に係る事項については、警察庁CSIRTの長の検討結果を基に、警察庁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。

(ｴ) 警察庁CSIRTに属する職員として、専門的な知識又は適性を有すると認められる者を指名する。

(ｵ)　最高情報セキュリティ管理者は、人事課長と調整の上、CYMATに属する職員を指名する。

オ　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、次に掲げる役割を兼務しないこと。

ａ　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。）

ｂ　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。

カ　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（警察庁内部部局にあっては警視正）相当職以上の職員を指名した上で分掌させることができる。

(2)　リスク評価の実施

最高情報セキュリティ管理者は、自己点検の結果、情報セキュリティ監査、戦略本部監査等の結果等を踏まえ、警察における情報セキュリティの維持に係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを評価すること。

(3)　対策推進計画の策定

ア　対策推進計画の策定

(ｱ)　最高情報セキュリティ管理者は、情報セキュリティ委員会（以下「委員会」という。）における審議を経て、情報セキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を定めること。

(ｲ)　最高情報セキュリティ管理者は、「対策推進計画策定マニュアル」（内閣官房国家サイバー統括室）を参照して対策推進計画を定め、少なくとも１年に１回、策定した対策推進計画の総合評価を実施し、その結果等からの対策推進計画の見直しを踏まえて、次年度の「全体方針」及び「個別の取組の方針・重点等」を定めること。

イ　対策推進計画の内容

アの対策推進計画には、警察庁の業務、警察庁が設置する警察情報システム及び管理対象情報に関するリスク評価の結果を踏まえた全体方針並びに次に掲げる取組の方針・重点及びその実施時期を含めること。

(ｱ)　情報セキュリティに関する教養

(ｲ)　情報セキュリティ対策の自己点検

(ｳ)　情報セキュリティ監査

(ｴ)　警察情報システムに関する技術的な対策を推進するための取組

(ｵ)　過年度の情報セキュリティ監査、戦略本部監査等の結果を踏まえた対策への取組

(ｳ)　前各号に掲げるもののほか、情報セキュリティ対策に関する重要な取組

(4)　都道府県警察における措置

ア　都道府県警察が設置する情報システム（警察情報システムに該当するものを除く。）及び当該情報システムで取り扱われる情報の取扱いについては、都道府県警察の長が、この文書の規定に準じて対策を講ずること。

イ　都道府県警察の情報セキュリティ管理者は、都道府県警察に設置されている警察情報システムの情報セキュリティ監査を実施すること。

２　運用

(1)　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)　警察庁情報セキュリティ管理者が別途定めるところにより、採用、退職、人事異動期等における情報セキュリティ対策について、附属機関､地方機関及び各都道府県警察の情報セキュリティ管理者に対して、適切に指示すること。

(ｲ)　情報セキュリティ対策推進体制は、警察庁情報セキュリティ管理者が別途定める事務を処理すること。

(ｳ)　情報セキュリティ管理者（警察庁情報セキュリティ管理者を除く。）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に報告すること。

(ｴ)　警察庁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及び問題点を含む運用状況並びに運用要領等の整備状況を適宜に把握し、必要に応じて最高情報セキュリティ管理者にその内容を報告すること。

(ｵ)　警察庁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(2)アで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、警察庁情報セキュリティ管理者を通じて、最高情報セキュリティ管理者に報告すること。

(2)　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、ウ及び警察庁情報セキュリティ管理者が別途定める手続により、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、警察庁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。）が警察庁情報セキュリティ管理者である場合及び申請が情報セキュリティ監査に関するものである場合は、最高情報セキュリティ副管理者を許可者とする。

イ　例外措置の運用

(ｱ)　申請者は、警察庁情報セキュリティ管理者が別途定める例外措置適用申請書により、許可者に対して、原則として、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。また、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。

(ｲ)　許可者は、申請内容を審査し、その検討結果を記録すること。

(ｳ)　許可者は、(ｲ)の検討を基に許可の可否を決定し、例外措置適用申請書の「許可に関する事項」欄に必要事項を記入し、その写しを送付するなどして、審査の結果を申請者に通知するとともに、許可の内容を台帳として整備すること。また、許可者が警察庁情報セキュリティ

管理者の場合においては、許可者は申請者に通知した内容をまとめて最高情報セキュリティ副管理者に四半期に１度報告すること。

(ｴ)　許可者は、例外措置適用申請書を適正に管理すること。

(ｵ)　警察庁情報セキュリティ管理者は、例外措置の申請状況を踏まえた警察情報セキュリティポリシーの規定の追加又は見直しの検討を行い、必要に応じて最高情報セキュリティ管理者にその内容を報告すること。

ウ　その他

(ｱ)　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。

(ｲ)　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。

(ｳ)　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、警察庁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。

(3)　教養

ア　教養体制の整備・教養実施計画の策定

(ｱ)　警察庁情報セキュリティ管理者は、対策推進計画に基づき教養実施計画を策定し、その実施計画に基づき実施体制を整備すること。

(ｲ)　警察庁情報セキュリティ管理者は、情報セキュリティの状況の変化に応じ、教養すべき事項を修正する必要がある場合には、当該教養実施計画を見直すこと。

イ　教養の実施

(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毎年１回以上実施すること。

なお、採用、人事異動等により新たに職員になった者に対しては、原則として、採用等から３か月以内に実施すること。

(ｲ)　情報セキュリティ管理者（警察庁情報セキュリティ管理者を除く。）は、職員に対する教養の実施状況について、警察庁情報セキュリティ管理者に報告すること。

(ｳ)　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。

(ｴ)　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、CYMAT及び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。

(ｵ)　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。

(ｶ)　警察庁情報セキュリティ管理者は、情報セキュリティ対策に関する教養の実施状況を分析し評価するとともに、評価結果を最高情報セキュリティ管理者に報告すること。

(ｷ)　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。

(4)　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

(ｱ)　警察庁情報セキュリティ管理者は、警察庁CSIRTへの報告を要する情報セキュリティインシデント（以下「要報告インシデント」という。）の可能性を認知した際の報告手順を整備し、報告が必要な具体例を含め、職員等に周知すること。

なお、別途通達するまでの間は、従前のとおり報告等を行うこと。

(ｲ)　警察庁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。

(ｳ)　警察庁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。

(ｴ) 警察庁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。

(ｵ) 警察庁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。

(ｶ) 警察庁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、警察庁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

(ｱ) 職員は、要報告インシデントを認知したときは、情報管理を担当する所属及び関係する警察情報システムの維持管理を担当する所属に速やかに報告し、指示に従うこと。

(ｲ) (ｱ)の報告を受けた情報管理を担当する所属及び警察情報システムの維持管理を担当する所属は、警察庁CSIRTに速やかに報告すること。この場合において、府県警察及び府県情報通信部（四国警察支局の県情報通信部を含む。）の情報管理を担当する課にあっては、併せて当該府県を管轄区域とする管区警察局情報通信部情報技術解析課（四国警察支局が管轄する県警察及び県情報通信部にあっては四国警察支局情報通信部情報技術解析課）にも速やかに報告すること。

(ｳ) 警察庁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。

(ｴ) 警察庁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、遅滞なく最高情報セキュリティ管理者に報告すること。

(ｵ) 警察庁CSIRTの長は、関係する情報セキュリティ管理者、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。また、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて関係する情報セキュリティ管理者等に確認を指示すること。

(ｶ) 情報セキュリティ管理者及び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警察庁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。

なお、認知した情報セキュリティインシデントが政府共通利用型システムに関するものである場合には、当該政府共通利用型システムの情報セキュリティ対策に係る運用管理規程に従い、適切に対処すること。

(ｷ) 警察庁CSIRTの長は、発生した情報セキュリティインシデントについて、当該事案の被害状況や原因等を速やかに内閣官房国家サイバー統括室に連絡すること。

(ｸ) 警察庁CSIRTの長は、警察庁の外部委託先等において発生した情報流出事案が「委託先等で発生した政府機関の要保護情報に係るセキュリティインシデントの情報共有に関する申合せ」（令和２年６月30日関係省庁申合せ）における重大なインシデントに当たると認められた場合は、当該事案の被害状況や原因等を速やかに内閣官房国家サイバー統括室に連絡すること。

(ｹ) 警察庁CSIRTの長は、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、関係する警察庁の所属に、社会的な反響が大きいと予想されるときは､併せて警察庁長官官房総務課広報室にその概要を連絡すること。さらに、大規模サイバー攻撃事態（「大規模サイバー攻撃事態等発生時における対処要領」（令和４年４月１日付け警察庁丙備企発第171号ほか別添）で定義されるものをいう。）に該当するおそれがあると

きは、併せて警備局警備企画課及びサイバー警察局各課にその概要を連絡し、「大規模サイバー攻撃事態等への初動対処について」（平成22年３月19日内閣危機管理監決裁）に基づく報告連絡を依頼すること。

(ｺ)　警察庁CSIRTの長は、要報告インシデントにより発生した保有個人情報・特定個人情報の漏えい等が個人の権利利益を害するおそれが大きいもの（「個人情報の保護に関する法律施行規則」（平成28年個人情報保護委員会規則第３号）及び「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29条の４第１項及び第２項に基づく特定個人情報の漏えい等に関する報告等に関する規則」（平成27年特定個人情報保護委員会規則第５号）で定義されるものをいう。）に該当するおそれがあるときは、警察庁長官官房総務課情報公開・個人情報保護室に連絡し、対応について助言を受けること。

(ｻ)　警察庁CSIRTの長は、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。

(ｼ)　警察庁CSIRTの長は、CYMATの支援を受ける場合には、必要な情報提供を行うこと。

(ｽ)　警察庁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、警察庁CSIRTの長は、定期的に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

(ｱ)　情報セキュリティ管理者は、警察庁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、警察庁情報セキュリティ管理者に報告すること。

(ｲ)　報告を受けた警察庁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。

(ｳ)　警察庁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、警察庁情報セキュリティ管理者、関係する情報セキュリティ管理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。

エ　都道府県警察における対処等

都道府県警察が設置又は運用する情報システム及び当該情報システムで取り扱われる情報に係る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、都道府県警察は、警察庁CSIRTに準ずる体制をCSIRTとして整備するとともに、情報セキュリティインシデント対処要領等を定め、要報告インシデントについては、警察庁CSIRTと連携し適切に対処するよう努めること。

3　点検

(1)　情報セキュリティ対策の自己点検

ア　自己点検計画の策定・手順の準備

(ｱ)　警察庁情報セキュリティ管理者は、対策推進計画に基づき警察庁職員に対する年度自己点検計画を策定すること。

(ｲ)　警察庁情報セキュリティ管理者は、年度自己点検実施計画に基づき、職員ごとの自己点検票及び自己点検の実施手順を整備すること。

(ｳ)　警察庁情報セキュリティ管理者は、情報セキュリティの状況の変化に応じ、点検すべき事項を修正する必要がある場合には、当該年度自己点検計画を見直すこと。

イ　自己点検の実施

(ｱ)　警察庁情報セキュリティ管理者は、当該年度自己点検計画に基づき、警察庁職員に対し、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。

ウ　自己点検結果の評価・改善

(ｱ)　警察庁情報セキュリティ管理者は、警察庁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（附属機関及び地方機関の自己点検結果も含む。）を分析し評価するとともに、評価結果を最高情報セキュリティ管理者に報告すること。

(ｲ)　最高情報セキュリティ管理者は、自己点検結果を全体として評価し、自己点検の結果より明らかになった問題点について、警察庁情報セキュリティ管理者に改善を指示するとともに、改善結果の報告を受けること。

(2)　情報セキュリティ監査

ア　監査の種類

監査の種類は、通常監査及び特別監査とする。

イ　監査実施計画の策定

(ｱ)　情報セキュリティ監査責任者（以下「監査責任者」という。）は、警察庁の内部部局の課（これに準ずるものを含む。）、附属機関及び地方機関並びに都道府県警察に対し、通常監査を実施するため、毎年度、年度情報セキュリティ監査計画の案を作成し、委員会の審議を経た上、最高情報セキュリティ管理者の承認を得て、これを策定すること。

(ｲ)　(ｱ)の年度情報セキュリティ監査計画において、監査の重点項目、監査の対象部署（以下「対象部署」という。）及び監査の時期について定めること。

(ｳ)　監査責任者は、年度情報セキュリティ監査計画に基づき、対象部署ごとに、監査実施計画を策定すること。

(ｴ)　最高情報セキュリティ管理者が特に必要があると認める場合には、監査責任者は、監査実施計画を定め、特別監査を実施すること。

ウ　監査官の指名等

監査責任者は監査官及び監査補佐官の指名等を行うこと。

エ　監査の実施

(ｱ)　監査責任者は、監査実施計画に基づき、通常監査の実施を監査官に指示すること。

(ｲ)　監査官は、通常監査を終了したときは、対象部署ごとに監査調書を作成し、監査責任者に提出すること。

(ｳ)　監査責任者は、監査調書に基づき監査報告書を作成し、最高情報セキュリティ管理者に提出すること。

(ｴ)　監査官は、通常監査を実施するに当たっては、次の事項に留意すること。

ａ　取り扱う情報の保秘を徹底すること。

ｂ　厳正かつ公平を旨とすること。

ｃ　資料及び情報を十分に収集し、正確な事実の把握に努めること。

ｄ　必要な限度を超えて関係者の職務に支障を及ぼさないよう注意すること。

オ　監査結果に応じた対処

(ｱ)　最高情報セキュリティ管理者は、情報セキュリティ監査、戦略本部監査等の結果等を踏まえ、改善を求める事項その他必要と認める事項を委員会の審議を経て決定し、警察庁情報セキュリティ管理者及び対象部署の長に指示すること。

(ｲ)　警察庁情報セキュリティ管理者は、(ｱ)に基づく改善の指示のうち、警察庁及び都道府県警察に共通の改善を必要とする事項について、速やかに必要な措置を講じ、その措置結果を最高情報セキュリティ管理者に報告すること。

(ｳ)　(ｱ)の指示を受けた対象部署の長は、当該指示の内容を踏まえ、速やかに必要な措置を講じ、その措置結果を最高情報セキュリティ管理者に報告すること。

(ｴ)　(ｱ)の指示を受けた警察庁情報セキュリティ管理者及び対象部署の長は、速やかな措置が困難な事項については、その影響を低減させるための補完的な措置を検討した上で改善計画を策定し、措置が完了するまでの間、定期的に措置状況及び改善計画を最高情報セキュリティ管理者に報告すること。

カ　特別監査

ウ、エ(ｲ)から(ｴ)、オ(ｳ)及び(ｴ)の規定は、特別監査について準用する。

4　情報セキュリティ対策の見直し

(1)　情報セキュリティ関係規程の見直し

警察庁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、情報セキュリティ監査、戦略本部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。

(2)　対策推進計画の見直し

最高情報セキュリティ管理者は、情報セキュリティ対策の運用及び自己点検、情報セキュリティ監査、戦略本部監査等の結果等を総合的に評価するとともに、リスク評価に変化が生じた場合には、委員会の審議を経て、対策推進計画について定期的な見直しを行うこと。

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、文書管理規程、個人情報保護に関する規程等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

(1)　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。

(2)　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。

なお、管理対象情報の作成又は複製に当たり既存の管理対象情報を参照等した場合には、原則として、当該既存の管理対象情報の機密性に係る分類及び取扱い制限を継承すること。

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不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、部内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、警察庁情

報セキュリティ管理者が別途定めるものを除き、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、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。

(3)　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き損しないこと。

(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、要保全情報又は要安定情報を利用する場合は、(5)ウ(ｲ)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、警察庁情報セキュリティ管理者が別途定める場合を除き、警察庁舎外に設置されている機器等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(2)ウの規定に従うこと。

カ　職員は、データ連係装置を用いて管理対象情報を取り扱う場合には、第８の１(2)エの規定に従うこと。

キ　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。

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

(4)　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、(5)ウ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。

(5)　管理対象情報の運搬・送信

ア　職員は、要機密情報を運搬・送信する場合には、情報漏えいを防止するため、必要に応じて次の措置を講ずること。

(ｱ)　運搬・送信する要機密情報は、暗号化する。暗号化が困難である場合は、主体認証を設定する。

(ｲ)　主体認証機能や暗号化機能等を備えるセキュアな外部記録媒体を利用する。

(ｳ)　自組織以外の組織から受け取った外部記録媒体は、自組織と当該機関との間で情報を運搬する目的に限って使用することとし、当該外部記録媒体から情報を入出力する場合の安全確保のために必要な措置を講ずる。

イ　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制限に応じて、適切な措置を講ずること。

ウ　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、(2)オ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。

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

(ｲ)　機密性３（高）情報、要保全情報又は要安定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。

エ　職員は、機密性２（中）情報、要保全情報又は要安定情報を外部回線を用いて送信する場合には、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。

オ　職員は、機密性３（高）情報を外部回線を用いて送信しないこと。

(6)　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。

(7)　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について、適切な方法で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保存場所、保存方法、保存期間等を定め適切に管理すること。

ウ　職員は、保存期間を過ぎたバックアップについて、適切な方法で消去、抹消又は廃棄すること。

２　管理対象情報を取り扱う区域の管理

(1)　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、警察庁情報セキュリティ管理者が別途定める。

(2)　区域ごとの対策の決定

ア　情報セキュリティ管理者は、(1)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、(1)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。

(3)　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　区域情報セキュリティ管理者は、職員以外の者が要管理対策区域内に立ち入り盗難若しくは破壊をすること又は警察情報システムを直接操作して情報窃取することなどを防止するために、施設及び環境面から対策を講ずること。

エ　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

(1)　業務委託に係る運用規定

警察庁情報セキュリティ管理者は、業務委託に際し、次の運用規定を定めること。

ア　委託先への提供を認める情報及び委託する業務の範囲を判断する委託判断基準（以下「委託判断基準」という。）

イ　委託先の選定基準

(2)　業務委託の各段階における対策

ア　業務委託実施前の対策

システムセキュリティ責任者又は運用管理者は、業務委託の実施までに、次に掲げる事項を実施すること。

(ｱ)　委託判断基準に基づく委託する業務内容の特定

(ｲ)　委託先の選定条件を含む仕様の策定

(ｳ)　仕様に基づく委託先の選定

(ｴ)　契約の締結

(ｵ)　委託先に要機密情報を提供する場合は、秘密保持契約（NDA）の締結

イ　業務委託実施期間中の対策

システムセキュリティ責任者又は運用管理者は、業務委託の実施期間において、次に掲げる事項を含む対策を実施すること。

(ｱ)　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とともに、委託先に管理対象情報の適正な取扱いを求めること。

(ｲ)　契約に基づき委託先に実施させる情報セキュリティ対策の履行状況を定期的に確認すること。

(ｳ)　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　業務委託終了時の対策

システムセキュリティ責任者又は運用管理者は、業務委託の終了に際し、次に掲げる事項を含む対策を実施すること。

(ｱ)　業務委託の実施期間を通じて情報セキュリティ対策が適切に実施されたことの確認を含む検収を実施すること。

(ｲ)　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。

(3)　警察情報システムに関する業務委託

ア　警察情報システムに関する業務委託における共通的対策

システムセキュリティ責任者は、警察情報システムに関する業務委託

の実施までに、委託先の選定条件に意図しない変更が加えられないための対策に係る選定条件を加え、仕様を策定すること。

イ　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、次に掲げる事項を含む対策を仕様書に記載し、契約に基づき委託先に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)　警察における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

ウ　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、仕様書に記載し、契約に基づき委託先に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、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。

エ　警察向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

(ｱ)　システムセキュリティ責任者又は運用管理者は、一般の者が警察向けに要機密情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、警察情報システムに関する業務委託を実施する場合は、委託先の選定条件に業務委託サービスに特有の選定条件を加えること。

(ｲ)　システムセキュリティ責任者又は運用管理者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定すること。

(ｳ)　システムセキュリティ責任者又は運用管理者は、委託先の信頼性が十分であることを総合的・客観的に評価し判断すること。

(ｴ)　システムセキュリティ責任者又は運用管理者は、業務委託サービスを利用する場合は、情報セキュリティ管理者と調整の上、当該サービ

スの利用申請を行うこと。

(ｵ) 情報セキュリティ管理者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定すること。

(ｶ) 情報セキュリティ管理者は、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名すること。

2 クラウドサービスの利用

(1) クラウドサービスの利用に係る運用規定（要機密情報を取り扱う場合）

警察庁情報セキュリティ管理者は、クラウドサービスの利用に際し、次の運用規定を定めること。

ア クラウドサービス利用判断基準

イ クラウドサービスの選定基準

ウ クラウドサービスの利用申請の利用手続

エ クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

(2) クラウドサービスの選定（要機密情報を取り扱う場合）

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場合は､次に掲げる事項に従ってクラウドサービスを選定すること。

ア 取り扱う管理対象情報の分類及び取扱制限を踏まえ、クラウドサービス利用判断基準に従って業務に係る影響度等を検討した上でクラウドサービスの利用を検討すること。

イ 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並びにクラウドサービス提供者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、次に掲げるセキュリティ要件を定め、クラウドサービス提供者を選定すること。

(ｱ) クラウドサービスに求める情報セキュリティ対策

(ｲ) クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法

(ｳ) クラウドサービスに求めるサービスレベル

ウ クラウドサービスの選定基準に従い、前項で定めたセキュリティ要件を踏まえて、原則としてISMAP（Information system Security Management

and Assessment Program）クラウドサービスリスト又はISMAP-LIU（ISMAP for Low-Impact Use）クラウドサービスリスト（以下「ISMAP等クラウドサービスリスト」という。）からクラウドサービスを選定すること。

(3)　クラウドサービスの利用に係る調達（要機密情報を取り扱う場合）

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場合は、次に掲げる事項に従って、クラウドサービスを調達すること。

ア　クラウドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件を仕様に含めること。

イ　クラウドサービス提供者及びクラウドサービスが仕様を満たすこと並びに情報セキュリティに関する役割及び責任の範囲が明確になっていることを契約までに確認し、利用承認を得ること。また、仕様の内容は、契約に含めること。

(4)　クラウドサービスの利用承認（要機密情報を取り扱う場合）

ア　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場合には、利用申請の承認権限者にクラウドサービスの利用申請を行うこと。

イ　利用申請の承認権限者は、職員によるクラウド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。

ウ　承認権限者は、当該申請に係る利用を承認した場合は、クラウドサービス管理者を指名し、承認したクラウドサービスを記録すること。

エ　クラウドサービスの利用申請の承認権限者は原則、警察庁情報セキュリティ管理者とする。ただし、警察庁情報セキュリティ管理者が別途定める場合はこの限りでない。

(5)　クラウドサービスの利用（要機密情報を取り扱う場合）

ア　クラウドサービスの利用に係る運用規定の整備

(ｱ)　警察庁情報セキュリティ管理者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して警察情報システムを導入・構築する際の情報セキュリティ対策の基本方針を整備すること。

(ｲ)　警察庁情報セキュリティ管理者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して警察情報システムを運用・保守する際の情報セキュリティ対策の基本方針を整備すること。

(ｳ)　警察庁情報セキュリティ管理者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、次の事項を含むクラウドサービスの利用を終了する際の情報セキュリティ対策の基本方針を整備すること。

ａ　クラウドサービスの利用終了時における対策

ｂ　クラウドサービスで取り扱った情報の廃棄

ｃ　クラウドサービスの利用のために作成したアカウントの廃棄

イ　クラウドサービスの利用に係るセキュリティ要件の策定

(ｱ)　クラウドサービス管理者は、クラウドサービスを利用する目的、対象とする業務等の業務要件及びクラウドサービスで取り扱われる管理対象情報の分類等に基づき、アの各項で整備した基本方針に従い、クラウドサービスの利用に係る内容を確認すること。

(ｲ)　クラウドサービス管理者は、クラウドサービスを利用する目的、対象とする業務等の業務要件及びクラウドサービスで取り扱われる管理対象情報の分類等に基づき、アの各項で整備した基本方針に従い、クラウドサービスの利用に係るセキュリティ要件を策定すること。

ウ　クラウド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

(ｱ)　クラウドサービス管理者は、イ(ｲ)において定めるセキュリティ要件に従いクラウドサービス利用における必要な措置を講ずること。また、実施状況を確認・記録すること。

(ｲ)　クラウドサービス管理者は、警察情報システムにおいてクラウドサービスを利用する際には、情報システム台帳及び情報システム関連文書に記録又は記載すること。

(ｳ)　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに次の事項の実施手順を整備すること。

ａ　クラウドサービスで利用するサービスごとの情報セキュリティ水

準の維持に関する手順

b　クラウドサービスを利用した警察情報システムの運用・監視中における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

c　利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

エ　クラウド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

(ｱ)　クラウドサービス管理者は、ア(ｲ)で定めた基本方針を踏まえて、クラウドサービスに係る運用・保守を適切に実施すること。また、実施状況を定期的に確認・記録すること。

(ｲ)　クラウドサービス管理者は、情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合は、情報システム台帳及び情報システム関連文書を更新又は修正すること。

(ｳ)　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずること。

オ　クラウド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

(ｱ)　クラウドサービス管理者は、ア(ｳ)で定めた基本方針を踏まえて、クラウド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。

(ｲ)　クラウドサービス管理者は、(ｱ)に定める事項について、実施状況を確認・記録すること。

(6)　クラウドサービスの選定・利用（要機密情報を取り扱わない場合）

警察庁情報セキュリティ管理者は､次の事項を含むクラウドサービス(要機密情報を取り扱わない場合）の利用に関する運用規定を整備すること。

ア　クラウドサービスを利用可能な業務の範囲

イ　クラウドサービスの利用申請の利用手続

ウ　クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

(7)　クラウドサービスの利用承認（要機密情報を取り扱わない場合）

ア　システムセキュリティ責任者又は運用管理者は、要機密情報を取り扱わないことを前提としたクラウドサービスを利用する場合、利用するク

ラウドサービスの定型約款、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申請の承認権限者に要機密情報を取り扱わない場合のクラウドサービスの利用申請を行うこと。

イ　利用申請の承認権限者は、アにおいてクラウドサービスの利用申請者が確認した結果を踏まえて、クラウド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。

ウ　利用申請の承認権限者は、要機密情報を取り扱わないクラウドサービスの利用申請を承認した場合は、クラウドサービス管理者を指名し、承認したクラウドサービスを記録すること。

エ　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの利用の運用要領等を整備すること。

オ　クラウドサービス管理者は、要機密情報を取り扱わないクラウドサービスを安全に利用するための適切な措置を講ずること。

カ　クラウドサービスの利用申請の承認権限者は、(4)エを準用する。

3　機器等の調達

(1)　機器等の調達に係る機器等の選定基準の整備

警察庁情報セキュリティ管理者は、機器等の選定基準を定めること。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を確認できることを加えること。

(2)　機器等の納入時の確認・検査手続の整備

警察庁情報セキュリティ管理者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。

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

(1)　情報システム台帳の整備

ア　警察庁情報セキュリティ管理者並びに附属機関及び地方機関の情報セキュリティ管理者は、自機関が整備した全ての警察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　各都道府県警察の情報セキュリティ管理者は、自組織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。

ウ　附属機関及び地方機関の情報セキュリティ管理者は、警察情報システムを構築、更改又は変更する際には、情報システム台帳に記録又は記載し、当該内容について警察庁情報セキュリティ管理者に報告すること。

(2)　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　職員は、ア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警察庁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。

ウ　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を実施するために、次の事項を含む文書を整備すること。

(ｱ)　当該警察情報システムを構成するサーバ等及び端末関連情報

(ｲ)　当該警察情報システムを構成する電気通信回線及び通信回線装置関連情報

(ｳ)　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

(ｴ)　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

(ｵ)　当該警察情報システムが停止した際の復旧手順

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

(1)　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（政府共通利用型システムを除く。以下同じ。）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、警察情報システムを構築する目的、対象とする業務等の業務要件及び当該警察情報システムで取り扱われる情報の分類等を勘案し、警察情報システムの分類基準に応じた具体的な対策事項を踏まえて、次の事項を含む警察情報システムのセキュリティ要件を策定すること。

a　警察情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等のセキュリティ機能要件

b　警察情報システム運用時の監視等の運用管理機能要件（監視するデータが暗号化されている場合は、必要に応じて復号すること。）

c　警察情報システムに関連する脆弱性及び不正プログラムについての対策要件

d　警察情報システムの可用性に関する対策要件

e　警察情報システムのネットワーク構成に関する要件

(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」（経済産業省。以下「セキュリティ要件リスト」という。）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。

(ｵ) システムセキュリティ責任者は、構築する警察情報システムが取り扱う情報や警察情報システムを利用して行う業務の内容等を踏まえ高度な情報セキュリティ対策を要する警察情報システムについては、警察情報システムの分類に応じて策定したセキュリティ要件について、最高情報セキュリティアドバイザー等に助言を求め、業務の特性や警察情報システムの特性を踏まえて、上位の情報セキュリティ対策をセキュリティ要件として盛り込む必要が無いかを確認すること。

ウ　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。

(2) 警察情報システムの調達・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、警察情報システムを新規に構築し、又は更改する際には、警察情報システムの分類基準に基づいて警察情報システムの分類を行い、情報システム台帳を作成又は更新すること。

ウ　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発生時の業務影響度や脅威動向等を踏まえて、上位又は下位の警察情報システムの分類の適用が望ましい場合には、システムセキュリティ責任者に修正の指示を行うこと。

エ　警察庁情報セキュリティ管理者は、警察情報システムの分類基準等について、次に掲げる措置を講ずること。

(ｱ) 警察情報システムの分類基準と当該分類基準に応じた情報セキュリ

ティ対策の具体的な対策事項について定期的な確認による見直しを行うこと。

(ｲ)　全ての警察情報システムが分類基準に基づいて適切に分類が行われていることを定期的に確認すること。

オ　システムセキュリティ責任者は、構築した警察情報システムを運用保守段階に移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずること。

カ　システムセキュリティ責任者は、機器等の納入時又は警察情報システムの受入れ時の確認・検査において、仕様書等に定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認すること。

キ　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。

(3)　警察情報システムの運用・保守時の対策

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監視を含む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、不正な行為及び意図しない警察情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直すこと。

エ　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・保守にお

いて、情報システム台帳及び情報システム関連文書の内容に変更が生じた場合、情報システム台帳及び情報システム関連文書を更新又は修正すること。

オ　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新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、速やかに必要な対応を行うこと。

カ　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。

キ　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。

(4)　警察情報システムの更改・廃棄時の対策

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

(5)　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、警察庁情報セキュリティ管理者から示された横断的に改善が必要な事項について、情報セキュリティ対策を適切に見直すこと。また、措置の結果については、警察庁情報セキュリティ管理者に報告すること。

ウ　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、この文書に定められた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

(1)　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、地震、津波、火災、高出力電磁波、感染症、情報セキュリティインシデント等（以下「危機的事象」という。）発生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。

(2)　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、危機的事象発生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。

(3)　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、危機的事象発生時における情報セキュリティに係る対策事項及び実施手順が運用可能であるかを定期的に確認すること。

4　政府共通利用型システム

(1)　政府共通利用型システム管理機関における対策

ア　情報セキュリティ対策に関する運用管理要領等の整備

システムセキュリティ責任者は、政府共通利用型システムを構築する場合は、次に掲げる事項を含む情報セキュリティ対策に関する運用管理規程を整備し、政府共通利用型システム利用機関と十分な合意形成を行うこと。

(ｱ)　政府共通利用型システム管理機関と政府共通利用型システム利用機関との間の責任分界

(ｲ)　平常時及び非常時の協力・連携体制

(ｳ)　非常時の具体的対応策

イ　情報システム台帳及び情報システム関連文書の整備

(ｱ)　警察庁情報セキュリティ管理者は、第５の１(1)で整備する情報システム台帳について、政府共通利用型システム利用機関に関係するセキュリティ要件に係る事項を含めて整備すること。

(ｲ)　システムセキュリティ責任者は、第５の１(2)ウで整備する政府共通利用型システムに関する文書について、政府共通利用型システム利用機関に関係する情報を含めて整備すること。

なお、政府共通利用型システム利用機関に提供した機器等に係る情報については、政府共通利用型システム利用機関の求めに応じ、必要な範囲で提供すること。

(2)　政府共通利用型システム利用機関における対策

ア　政府共通利用型システム利用機関における体制の整備

(ｱ)　システムセキュリティ責任者は、政府共通利用型システムが提供するセキュリティ機能を利用して警察情報システムを構築する場合は、政府共通利用型システム管理機関が定める運用管理規程に応じた体制の確保を最高情報セキュリティ管理者に求めること。

(ｲ)　警察庁情報セキュリティ管理者は、政府共通利用型システムが提供する機器等の提供を受け、これを自組織の職員が利用する場合は、当該利用に係る情報セキュリティ対策に関する事務を統括する管理者として、政府共通利用型システムごとに政府共通利用型システム利用管理者を指名すること。

(ｳ)　政府共通利用型システム利用管理者は、当該政府共通利用型システムの利用に際し、当該政府共通利用型システム管理機関が定める運用管理規程に応じた体制の確保を最高情報セキュリティ管理者に求めること。

イ　政府共通利用型システム利用機関における情報セキュリティ対策

(ｱ)　システムセキュリティ責任者は、政府共通利用型システムが提供するセキュリティ機能を利用する警察情報システムを構築する場合は、政府共通利用型システム管理機関が定める運用管理規程に基づき、政府共通利用型システム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、適切にセキュリティ要件を策定し、運用すること。

(ｲ) システムセキュリティ責任者は、政府共通利用型システム管理機関が定める運用管理規程に基づき、政府共通利用型システムに関する情報セキュリティインシデントに適切に対処すること。

(3) 政府共通利用型システム利用機関における機器等の管理

ア 政府共通利用型システム利用管理者は、政府共通利用型システム管理機関が提供する機器等を自組織の職員が利用する場合は、当該機器等の利用に関する情報セキュリティ対策に係る運用要領等を整備すること。

イ 政府共通利用型システム利用管理者は、提供を受けた政府共通利用型システムの機器等を把握するために、情報システム台帳に次に掲げる事項を記載すること。

(ｱ) 当該機器等を管理又は利用する職員を特定する情報

(ｲ) 当該機器等の設置場所並びにその区域のクラス及び当該設置場所の区域情報セキュリティ管理者

ウ 政府共通利用型システム利用管理者は、政府共通利用型システム管理機関が情報システム台帳や情報システム関連文書を整備するために必要な情報について､政府共通利用型システム管理機関に提供するとともに、当該情報に変更が生じた場合は速やかに通知すること。

エ 政府共通利用型システム利用管理者は、政府共通利用型システム管理機関が定める運用管理規程等に基づき、政府共通利用型システムに関する情報セキュリティインシデントに適切に対処すること。

第６ 警察情報システムの構成要素

１ 端末・サーバ等

(1) 端末

ア 端末の導入時の対策

(ｱ) 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。

(ｲ)　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を定め、それ以外のソフトウェアは利用させない技術的な措置を講ずること。

(ｳ)　システムセキュリティ責任者は、端末への接続を認める機器等を定め、接続を認めた機器等以外は接続させないこと。

(ｴ)　システムセキュリティ責任者は、警察情報システムのセキュリティ要件として策定した内容に従い、端末に対して適切なセキュリティ対策を実施すること。

(ｵ)　システムセキュリティ責任者は、端末において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対策を実施すること。

(ｶ)　システムセキュリティ責任者は、仮想デスクトップ技術を活用し、物理的な端末を共用する場合は、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、セキュリティ要件を策定し、適切なセキュリティ対策を設けること。

イ　端末の運用時の対策

(ｱ)　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について、追加や継続の適否を定期的に検討し、見直しを行うこと。

(ｲ)　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。

(ｳ)　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ソフトウェア又は機能を削除又は無効化すること。

(ｴ)　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

たとき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(4)の各号に掲げる措置を適切に講ずること。

エ　モバイル端末及び支給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、支給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、モバイル端末及び支給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セキュリティ要件を検討すること。

(2)　サーバ等

ア　サーバ等の導入時の対策

(ｱ)　サーバ等の導入時の対策については、(1)アの各号の対策を準用する。

(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)　サーバ等の運用時の対策については、(1)イの各号の対策を準用する。

(ｲ)　システムセキュリティ責任者は、サーバ等に係る情報セキュリティインシデントの発生を監視するため、当該サーバ等を監視するための

措置を講ずること。

(ｳ)　システムセキュリティ責任者は、要安定情報を取り扱うサーバ等について､危機的事象発生時に適切な対処が行えるよう運用をすること。

ウ　サーバ等の運用終了時の対策

サーバ等の運用終了時の対策については、(1)ウの対策を準用する。

(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。

(ｳ)　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、警察庁情報セキュリティ管理者が別途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

(1)　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　電子メールのサーバ間通信の暗号化の対策を講ずること。

(2)　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・運用時に次に掲げる対策を講ずること。

ア　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。

イ　ウェブサーバからの不用意な情報漏えいを防止するための措置を講ずること。

ウ　ウェブコンテンツの編集作業を行う主体を限定すること。

エ　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。

オ　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。

カ　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。

キ　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。

(3)　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

(ｱ)　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。

(ｲ)　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するための措置を講ずること。

(ｳ)　コンテンツサーバにおいて、自組織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

(ｱ)　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。

(ｲ)　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。

(ｳ)　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。

(4)　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

(1)　電気通信回線

ア　電気通信回線の導入時の対策

(ｱ)　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（外部回線を除く。）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　庁舎内回線

有線回線、無線回線の順

ｂ　その他

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

(ｲ)　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通信回線装置を利用しアクセス制御及び経路制御を行うこと。

(ｳ)　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。

(ｴ)　システムセキュリティ責任者は、通信回線装置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。

(ｵ)　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。

(a)　情報システム内の他の機器等への不正な接続を制限する。

(b)　アクセス可能なウェブサイトを必要最小限に制限する。

(ｶ)　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。

(ｷ)　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、通信回線装置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。

(ｸ)　システムセキュリティ責任者は、通信回線装置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通信回線装置の場合は、この限りでない。

(ｹ)　システムセキュリティ責任者は、遠隔地から通信回線装置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。

(ｺ)　システムセキュリティ責任者は、警察情報システムで利用される内部ネットワークに情報システムが接続された際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずること。

(ｻ)　システムセキュリティ責任者は、要安定情報を取り扱う警察情報システムが接続される電気通信回線について、当該電気通信回線の継続的な運用を可能とするための措置を講ずること。

イ　外部回線の接続時の対策

システムセキュリティ責任者は、内部ネットワークに外部回線を接続する場合には、次の事項を満たしていることについて警察庁情報セキュリティ管理者の確認を受けること。

(ｱ)　内部ネットワークにインターネット回線、公衆通信回線等の外部回線を接続する場合には、内部ネットワーク及び当該内部ネットワークに接続されている警察情報システムの情報セキュリティを確保するための措置を講ずること。

(ｲ)　内部ネットワークと外部回線との間及び内部ネットワーク内の不正な通信の有無を監視するための措置を講ずること。

(ｳ)　保守又は診断のために外部回線から内部ネットワークに接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保すること。

(ｴ)　電気通信事業者の電気通信回線サービスを利用する場合には、当該電気通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、警察情報システムの構築を委託する事業者と契約時に取り決めておくこと。

ウ　電気通信回線の運用時の対策

(ｱ)　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。

(ｲ)　１(1)イ(ｲ)及び(ｴ)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「電気通信回線及び通信回線装置」と読み替える。

(ｳ)　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。

(ｴ)　システムセキュリティ責任者は、経路制御及びアクセス制御を適切に運用し、電気通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の確認及び見直しを適宜行うこと。

(ｵ)　システムセキュリティ責任者は、内部ネットワークと外部回線との間及び内部ネットワーク内の不正な通信の有無を監視するための措置を講じ、定期的に確認すること。

エ　電気通信回線の運用終了時の対策

電気通信回線の運用終了時の対策については、１(1)ウの対策を準用

する。

(2)　通信回線装置

ア　通信回線装置の導入時の対策

システムセキュリティ責任者は、物理的な通信回線装置を設置する場合、第三者による破壊や不正な操作等が行われないようにすること。

イ　通信回線装置の運用終了時の対策

通信回線装置の運用終了時の対策については、１(1)ウの対策を準用する。

(3)　無線LAN

システムセキュリティ責任者は、無線LAN技術を利用して電気通信回線を構築する場合は、電気通信回線の構築時共通の対策に加えて、通信内容の漏えいや改ざんを防止するために通信路の暗号化その他の情報セキュリティ確保のために必要な措置を講ずること。

(4)　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 Logo Program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、端末及び通信回線装置を

IPv６通信を想定していない電気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。

４　警察情報システムの基盤を管理又は制御するソフトウェア

(1)　警察情報システムの基盤を管理又は制御するソフトウェアの導入時の対策

ア　システムセキュリティ責任者は、情報セキュリティの観点から警察情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ等、通信回線装置等及びソフトウェア自体を保護するための措置を講ずること。

イ　システムセキュリティ責任者は、利用するソフトウェアの特性を踏まえ、次に掲げる実施手順を整備すること。

(ｱ)　警察情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順

(ｲ)　警察情報システムの基盤を管理又は制御するソフトウェアで発生した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

(2)　警察情報システムの基盤を管理又は制御するソフトウェアの運用時の対策

システムセキュリティ責任者は、警察情報システムの基盤を管理又は制御するソフトウェアを運用・保守する場合は、次に掲げるセキュリティ対策を実施すること。

ア　警察情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するための対策

イ　脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策

５　アプリケーション・コンテンツ

(1)　アプリケーション・コンテンツ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、アプリケーション・コンテンツの提供時に自組織外の情報セキュリティ水準の低下を招かぬよう、セキュリ

ティ要件を仕様に含めること。

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、セキュリティ要件を仕様に含めること。

(2)　アプリケーション・コンテンツの開発時の対策

システムセキュリティ責任者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずること。

(3)　アプリケーション・コンテンツの運用時の対策

ア　システムセキュリティ責任者は、利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直すこと。

イ　システムセキュリティ責任者は、運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講ずること。

ウ　システムセキュリティ責任者は、ウェブアプリケーションやウェブコンテンツにおいて、アプリケーションやコンテンツの改ざんを検知するための措置を講ずること。

(4)　アプリケーション・コンテンツ提供時の対策

ア　政府ドメイン名の使用

(ｱ)　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、クラウドサービスを利用する場合、支給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（「go.jp」、「lg.jp」等）を使用すること。

(ｲ)　システムセキュリティ責任者は、自組織外に提供するウェブサイト等の作成を業務委託する場合には、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を使用するよう仕様に含めること。

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自組織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

(ｱ)　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。

(ｲ)　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

(1)　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、警察情報システムや管理対象情報へのアクセス主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の識別及び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。

(2)　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。

(3)　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必要最小限の範囲に設定するよう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、担当する通信回線装置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。

(4)　ログの取得・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、ログを取得し、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、警察情報システムにおいて、その特性に応じてログを取得する目的を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法等について定め、適切にログを管理すること。

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、取得したログ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。

(5)　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。

(ｱ)　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　支給携帯電話機であって、技術的に暗号化が困難であるもの

(ｲ)　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。

(ｳ) 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及び鍵長については、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、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」に基づくこと。さらに、要配慮個人情報、捜査情報等の機密性が高い情報を取り扱う警察情報システムは、警察庁情報セキュリティ管理者が定めた暗号リストから耐量子計算機暗号等を選択的に利用可能とすることを検討すること。これら暗号リスト等を用いて、警察情報システムで使用する暗号・電子署名のアルゴリズム及び鍵長並びにそれらを利用した安全なプロトコルを定めること。また、その運用方法について実施手順を定めること。

(ｴ) 警察情報システムの新規構築又は更新に伴い、暗号化機能又は電子署名機能を導入する場合には、やむを得ない場合を除き、暗号リスト等に記載されたアルゴリズム及び鍵長並びにそれらを利用した安全なプロトコルを採用すること。

(ｵ) 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。

(ｱ) 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。

(ｲ) 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(たい)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。

(6)　監視機能

ア　システムセキュリティ責任者は、警察情報システム運用時に必要となる監視に係る運用管理機能要件を策定し、監視機能を実装すること。

イ　システムセキュリティ責任者は、警察情報システムの運用において、警察情報システムに実装された監視機能を適切に運用すること。

ウ　システムセキュリティ責任者は、新たな脅威の出現、運用の状況等を踏まえ、警察情報システムにおける監視の対象や手法を定期的に見直すこと。

2　情報セキュリティの脅威への対策

(1)　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、サーバ等、端末及び通信回線装置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、端末及び通信回線装置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定期的及び適時に確認すること。

なお、状況確認の時間間隔については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。

(2)　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掲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不正プログラム対策ソフトウェアが存在しない場合を除き、不正プログラム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、不正プログラム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、不正プログラム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。

(3)　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、端末及び通信回線装置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、ウ及び警察庁情報セキュリティ管理者が別途定める措置を講ずること。

ウ　サーバ等、端末、通信回線装置又は電気通信回線から監視対象を特定し、監視すること。

(4)　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。

(5)　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、警察庁情報セキュリティ管理者が別途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。

(6)　データ連係装置の利用に係る対策

システムセキュリティ責任者は、情報漏えい防止を図るため、警察庁情

報セキュリティ管理者が別途定めるところにより、データ連係装置の利用を制限する機能を設けること。

3　ゼロトラストアーキテクチャ

(1)　動的なアクセス制御の実装時の対策

ア　動的なアクセス制御における責任者の設置

警察庁情報セキュリティ管理者は、複数の警察情報システム間で動的なアクセス制御を実装する場合は、複数の警察情報システム間で横断的な対策の企画・推進・運用に関する事務の責任者として、システムセキュリティ責任者を選任すること。

イ　動的なアクセス制御の導入方針の検討

システムセキュリティ責任者は､動的なアクセス制御を導入する場合、動的アクセス制御の対象とする警察情報システムのリソースを識別し、動的なアクセス制御の導入方針を定めること。

ウ　動的なアクセス制御の実装時の対策

(ｱ)　システムセキュリティ責任者は、動的なアクセス制御の実装に当たり、リソースの信用情報の変化に応じて動的にアクセス制御を行うためのアクセス制御ポリシー（以下「アクセス制御ポリシー」という。）を作成すること。

(ｲ)　システムセキュリティ責任者は、アクセス制御ポリシーに基づき、動的なアクセス制御を行うこと。

(2)　動的なアクセス制御の運用時の対策

ア　動的なアクセス制御の実装方針の見直し

システムセキュリティ責任者は、動的なアクセス制御の運用に際し、情報セキュリティに係る重大な変化等を踏まえ、アクセス制御ポリシーの見直しを行うこと。

イ　リソースの信用情報に基づく動的なアクセス制御の運用時の対策

システムセキュリティ責任者は、動的なアクセス制御の運用に際し、リソースの信用情報の収集により検出されたリスクへの対処を行うこと。

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

(1)　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警察庁情報セキュリ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。

(2)　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

(ｱ)　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。

(ｲ)　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。

(ｳ)　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。

(ｴ)　職員は、システムセキュリティ責任者が制定した運用要領等に定められた範囲を超えた警察情報システムを構成する機器等の改造（新たな機器等の接続、ソフトウェア追加等）をシステムセキュリティ責任者の許可なく実施しないこと。

(ｵ)　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。

(ｶ)　職員は、警察庁情報セキュリティ管理者が別途定める場合を除き、機器等を警察庁舎外に不正に持ち出さないこと。

(ｷ)　職員は、警察庁情報セキュリティ管理者が別途定める場合を除き、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。

(ｸ)　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。

(ｹ)　職員は、警察情報システムの紛失又は盗難を防止するための措置を講ずること。

(ｺ)　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。

(ｻ)　職員は、電子計算機又は通信回線装置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。

(ｼ)　職員は、業務の性質上、職員以外の者に端末の操作、画面の閲覧又は画面の接写をさせる必要がある場合は、必要な情報以外の情報の表示等を防止するための対策を講ずること。

(ｽ)　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途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　支給携帯電話機

(ｱ)　職員は、共用で利用する支給携帯電話機（音声通話機能のみを使用するものを除く。）を警察庁舎外に持ち出す場合は、部内の上級の職員の許可を得ること。

(ｲ)　職員は、支給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。

(ｳ)　職員は、支給携帯電話機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。

(ｴ)　職員は、支給携帯電話機を適正に管理すること。

ウ　外部記録媒体

(ｱ)　職員は、外部記録媒体を適正に管理すること。

(ｲ)　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、部内の上級の職員の許可を得ること。

　なお、機密性３（高）情報、要保全情報又は要安定情報を持ち出す場合は、運用管理者の許可を得ること。

(ｳ)　外部記録媒体を利用する警察庁及び都道府県警察の所属に一人又は複数人の媒体利用管理者を置き、運用管理者が指名する者をもって充てる。

(ｴ)　媒体利用管理者は、警部（警察庁内部部局にあっては警視）相当職以上の職員とする。ただし、やむを得ない事情があるときはこの限りでない。

(ｵ)　媒体利用管理者は、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行うものとする。

エ　データ連係装置

(ｱ)　職員は、データ連係装置により要機密情報を移動する必要がある場合には、必要最小限にするとともに、部内の上級の職員又はデータ連係装置を運用するシステムセキュリティ責任者の許可を得ること。

　なお、機密性３（高）情報を移動する場合は、運用管理者の許可を得ること。

(ｲ)　データ連係装置を利用する警察庁及び都道府県警察の所属に一人又は複数人のデータ連係装置利用管理者を置き、運用管理者が指名する者をもって充てる。

(ｳ)　データ連係装置利用管理者は、警部（警察庁内部部局にあっては警視）相当職以上の職員とする。ただし、やむを得ない事情があるときはこの限りでない。

(ｴ)　データ連係装置利用管理者は、データ連係装置を利用した管理対象情報の入出力の管理に係る事務を行うものとする。

オ　個人所有の機器等

(ｱ)　職員は、警察庁情報セキュリティ管理者が別途定める場合を除き、個人所有の機器等において管理対象情報を処理しないこと。

(ｲ)　運用管理者は、(ｱ)に基づく個人所有の機器等の利用について適切に管理すること。

(ｳ)　システムセキュリティ責任者は、(ｱ)に基づく個人所有の機器等の利用について情報セキュリティを維持するための環境を構築すること。

(3)　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支給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に規定するクラウドサービスを利用する場合、支給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。

(ｱ)　送信内容が暗号化されること。

(ｲ)　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）情報を外部に送信する場合には、当該情報を

暗号化すること。暗号化が困難である場合は、主体認証を設定すること。また、機密性３（高）情報を送信しないこと。

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削除すること。

(4)　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、自己に付与された識別コードを適切に管理すること。

ウ　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。

(5)　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。

(6)　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、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。

(7)　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(4)ア又は(7)アに定める手続を執り、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。

(8)　クラウドサービスの利用時の対策

ア　職員は、業務の遂行において、利用承認を得ていないクラウドサービスを利用しないこと。

イ　職員は、部外の者と情報の共有を行うことを目的とし、クラウドサービス上に要保護情報を保存する場合は、情報の共有を行う必要のある者のみがクラウドサービス上に保存した要保護情報にアクセスすることが可能となるための措置を講ずること。

ウ　職員は、部外の者と情報の共有を行うことを目的とし、クラウドサービス上に要保護情報を保存する場合は、情報の共有が不要になった時点で､クラウドサービス上に保存した要保護情報を速やかに削除すること。

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。

(1)　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(7)アに定める手続を執ること。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。

(2)　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、自組織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

(1)　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、テレワークの実施により電気通信回線を経由して警察情報システムに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。

(2)　実施時における対策

ア　職員は、テレワークの実施前及び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の実施場所を選定すること。また、自宅以外でテレワーク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、警察庁情報セキュリティ管理者が別途定める回線を使用すること。

4　警察庁舎外におけるモバイル端末利用時の対策

(1)　利用環境における対策

利用環境における対策については、3(1)ア、イ、ウの対策を準用する。

(2)　利用時における対策

職員は､画面の盗み見や盗聴を防止できるよう利用場所を選定すること。また、情報システムの紛失又は盗難を防止するための措置を講ずること。

第9　その他

本通達の実施に必要な細部事項については、警察庁情報セキュリティ管理者が別途定める。