原議保存期間	5年（令和9年3月31日まで）
有効期間	一種（令和9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 丙情管発第45号、丙企画発第58号
丙生企発第104号、丙刑企発第65号
丙組企発第23号、丙交企発第105号
丙備企発第162号、丙外事発第46号
丙備一発第20号

令和３年10月５日
警察庁情報通信局長
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

警察における情報セキュリティに係る管理体制について（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項及び第９条の規定に基づき、「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（通達）」（平成30年９月11日付け警察庁丙情管発第44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、情報セキュリティをめぐる情勢の変化を踏まえ別添のとおり「警察における情報セキュリティに係る管理体制」を改正し、令和３年10月15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

警察における情報セキュリティに係る管理体制

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項及び第９条の規定に基づき、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管理体制を定めるものとする。

２　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。

(1)　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。）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

(2)　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

(3)　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

３　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。

(1)　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。

(2)　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。

(3)　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。

(4)　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。

(5)　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。

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)　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。

(2)　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。

(3)　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。

(4)　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。

(5)　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。

(6)　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。

(7)　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。

(8)　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。

(9)　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。

(10) 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。

(11) 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。

(12) 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。

(13) 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。

(14) 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。

(15) 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。

(16) 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。

(17) 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。

(18) 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。

(19) 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。

(20) 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。

(21) 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。

(22) 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。

(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) 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。

(25) 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。

(26) 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。

(27) 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。

(28) 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。

(29) 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。

(30) 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。

(31) 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。

(32) 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。

(33) 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。

(34) 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。

(35) 外部委託

業務委託及び外部サービスをいう。

(36) 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。

(37) 外部サービス

外部委託のうち、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ものをいう。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る。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等が挙げられる。

(38) 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。

(39) 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。

(40) 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。

(41) 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。

(42) 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。ただし、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は含まれない。

(43) 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。

(44) 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。

(45) 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。

(46) 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。

(47) 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、内閣官房内閣サイバーセキュリティセンターに設置される体制をいう。

(48) 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。

(49) 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。

(50) 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。

(51) 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。

(52) 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　最高情報セキュリティ管理者の遵守事項

１　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。）を定めるものとする。

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ものとする。

(1)　情報セキュリティに関する教養

(2)　情報セキュリティ対策の自己点検

(3)　情報セキュリティ監査

(4)　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

(5)　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

2　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（第３の１(2)アに定める者をいう。以下同じ。）に改善を指示するとともに、改善結果の報告を受けるものとする。

3　最高情報セキュリティ管理者は、監査報告書の内容を踏まえ、改善を求める事項その他必要と認める事項を情報セキュリティ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ものとする。

4　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・監査結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ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ものとする。

5　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ものとする。

第３　情報セキュリティ管理者

１　情報セキュリティ管理者の設置

(1)　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。

(2)　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。

ア　警察庁内部部局

情報通信局情報管理課長

イ　警察大学校

教務部庶務課長

ウ　科学警察研究所

総務部総務課長

エ　皇宮警察本部

監察課長

オ　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

カ　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

キ　東京都警察情報通信部

情報技術解析課長

ク　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

ケ　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

コ　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

2　情報セキュリティ管理者の責務

(1)　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ものとする。

(2)　警察庁情報セキュリティ管理者は、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。

(3)　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。

(4)　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。

3　情報セキュリティ管理者の遵守事項

(1)　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しなければならない。

(2)　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しなければならない。また、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しなければならない。

(3)　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しなければならない。

(4)　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しなければならない。

(5)　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しなければならない。

(6)　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を適時に把握し、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しなければならない。

(7)　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、所要の措置を執るものとする。

(8)　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

を策定するとともに、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さなければならない。

(9)　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とともに、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さなければならない。また、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しなければならない。

(10) 警察庁情報セキュリティ管理者は、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、適切に指示しなければならない。

(11) 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しなければならない。

(12) 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しなければならない。

(13) 警察庁情報セキュリティ管理者は、第２の３の規定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、必要な措置を執った上で、改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ管理者に報告しなければならない。

(14) 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執らせるとともに、最高情報セキュリティ管理者に報告しなければならない。

(15) 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しなければならない。

(16) 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しなければならない。

(17) 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しなければならない。

(18) 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しなければならない。

(19) 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、別紙に掲げる事項を記録又は記載した情報システム台帳を整備しなければならない。

(20) 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別紙に掲げる事項を記録又は記載し、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しなければならない。

(21) 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、別紙に掲げる事項を記録又は記載した情報システム台帳を整備しなければならない。

第４　情報セキュリティ対策推進体制

１　情報セキュリティ対策推進体制の設置

(1)　警察庁情報通信局情報管理課に、情報セキュリティ対策推進体制を置く。

(2)　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。

(3)　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。

２　情報セキュリティ対策推進体制の事務

情報セキュリティ対策推進体制は、次の事務を処理する。

(1)　警察情報セキュリティポリシー及び対策推進計画の策定に係る事務

(2)　警察情報セキュリティポリシーの運用に係る事務

(3)　遵守事項に関する例外措置に係る事務

(4)　情報セキュリティ対策の教養の実施（警察庁内部部局に係るものに限る。）に係る事務

(5)　情報セキュリティ対策の自己点検に係る事務

(6)　(1)から(5)に掲げるもののほか、警察庁情報セキュリティ管理者が必要と認める事務

第５　最高情報セキュリティアドバイザー

１　最高情報セキュリティアドバイザーの設置

警察庁に最高情報セキュリティアドバイザーを置き、警察庁情報通信局情報管理課情報セキュリティ対策官をもって充てる。

２　最高情報セキュリティアドバイザーの責務

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ものとする。

３　最高情報セキュリティアドバイザーの遵守事項

最高情報セキュリティアドバイザーは、次に定める事項について助言を行わなければならない。

(1)　警察情報セキュリティポリシーの整備

(2)　対策推進計画の策定

(3)　教養実施計画の策定

(4)　警察情報システムに係る技術的事項

(5)　警察情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定

(6)　前各号に掲げるもののほか、情報セキュリティ対策に係る事項

第６　区域情報セキュリティ管理者

１　区域情報セキュリティ管理者の設置

(1)　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。

(2)　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。

(3)　区域の分類及び区域情報セキュリティ管理者の指名の方法は次の基準による。

ア　クラス０

各庁舎の敷地内であって、職員以外の者が自由に立ち入ることのできる区域は、一の区域とし、クラス０に分類する。

イ　クラス１

各庁舎における廊下等、職員の共用の区域は、一の区域とし、クラス１に分類するとともに、区域情報セキュリティ管理者に、当該庁舎の庁舎管理に関する事務を処理する者を指名する。

ウ　クラス２

執務室は、所属ごとに一の区域とし、クラス２に分類するとともに、区域情報セキュリティ管理者に、各所属の長を指名する。

エ　クラス３

警察情報システムに係る機械室は、室ごとに一の区域とし、クラス３に分類するとともに、区域情報セキュリティ管理者に、当該機械室を管理する所属の長を指名する。

２　区域情報セキュリティ管理者の責務

区域情報セキュリティ管理者は、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ものとする。

３　区域情報セキュリティ管理者の遵守事項

(1)　区域情報セキュリティ管理者は、関係する他の区域情報セキュリティ管理者、情報セキュリティ管理者等と連携し、次のアからウに定める対策を講じなければならない。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執らなければならない。

ア　クラス１の管理対策

(ｱ)　職員以外の者が不正に立ち入ることがないよう壁、施錠可能な扉、パーティション等で囲むことで、クラス０と明確に区分するなどの対策を講ずること。

(ｲ)　出入口が無人になるなどにより立入りの確認ができない時間帯がある場合には､確認ができない時間帯に施錠するなどの措置を執ること。

(ｳ)　職員以外の者を立ち入らせるときは、その者の氏名、所属、訪問目的及び訪問相手を確認すること。ただし、継続的に立入りを許可された者にあっては、この限りでない。

(ｴ)　職員以外の者を立ち入らせるときは、職員とは種別の異なるカードを身に付けさせるなどして、職員とそれ以外の者を視覚上区別できるようにすること。

イ　クラス２の管理対策

(ｱ)　下位区域との境界を施錠可能な扉等によって仕切ること。

(ｲ)　無人となるときは施錠すること。

(ｳ)　クラス２の区域へ立入りを許可されていない者が容易に立ち入らないように、立ち入る者が許可された者か否かを確認できるような措置を執ること。

(ｴ)　当該区域内に設置された電子計算機の画面の不正な視認や、機器の持込みによる不正な撮影及び録音がされないよう必要に応じ措置を執ること。

(ｵ)　クラス０に分類される区域と接するときは、当該境界においてアに定める対策を講ずること。ただし、合同庁舎等において、他の機関がアと同等以上の対策を講じているときは、この限りでない。

ウ　クラス３の管理対策

(ｱ)　常時施錠するとともに、システムセキュリティ維持管理者からの申請を基に、立ち入ることができる者の名簿を整備すること。名簿に記載された者以外の者が立ち入る必要があるときは、区域情報セキュリティ管理者の許可を得ること。

(ｲ)　クラス３の区域への立入りを許可されていない者が立ち入らないように、立ち入る者が許可された者か否かを確認できるような措置を執ること。

(ｳ)　当該区域に立ち入る者の氏名とその入退室の時刻を記録すること。当該記録は、可能な限り電磁的に記録すること。

(ｴ)　電子計算機の画面、システムドキュメント及び入出力資料をその区域の外から視認することができない構造とすること。

(ｵ)　職員以外の者が立ち入っている間は、職員の立会いや監視カメラ等により監視するなどの措置を執ること。

(ｶ)　区域情報セキュリティ管理者が許可した場合を除き、電子計算機及び外部記録媒体を持ち込まないこと。

(ｷ)　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。

(2)　区域情報セキュリティ管理者は、各区域の周辺環境や当該区域で行う業務の内容、取り扱う情報等を勘案し、(1)に定める対策のみでは安全性が確保できない場合は、当該区域において実施する個別の対策を決定しなければならない。

4　基準による運用が困難な場合の措置

情報セキュリティ管理者が、1(3)の基準による運用を困難と認めたときは、当該基準によらない区域を設けることができる。このとき、情報セキュリティ管理者は、3の規定を参考として、関係する他の情報セキュリティ管理者等と連携の上、可能な限り情報セキュリティの確保のための管理対策を講じなければならない。

第7　システムセキュリティ責任者

1　システムセキュリティ責任者の設置

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。

2　システムセキュリティ責任者の責務

(1)　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。

(2)　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ものとする。

3　システムセキュリティ責任者の遵守事項

(1)　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なければならない。

(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なければならない。

(3)　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、次の仕様書等を整備しなければならない。

ア　サーバ等及び端末の仕様書又は設計書

イ　電気通信回線及びネットワーク機器の仕様書又は設計書

(4)　システムセキュリティ責任者は、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、セキュリティ機能の利用方法等に関わる教養を実施しなければならない。

(5)　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しなければならない。

(6)　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わなければならない。

(7)　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しなければならない。

(8)　システムセキュリティ責任者は、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、署名検証者へ安全な方法で提供しなければならない。

(9)　システムセキュリティ責任者は、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(ぜい)性に関する情報を定期的に入手しなければならない。

(10) 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の主管課の長と連携の上、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しなければならない。

(11) (10)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。

ア　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

イ　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

ウ　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

エ　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

オ　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

(12) 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を構成する機器のソフトウェアの名称、バージョン等に関する情報を自動で収集し、管理する機能を導入しなければならない。

(13) システムセキュリティ責任者は、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わなければならない。

(14) 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、情報セキュリティに係る脆弱性情報（原因、影響範囲、対策方法、脆弱性を悪用する不正プログラムの流通状況を含む。）を適宜入手するとともに、脆弱性情報（広報、報道等が行われているものを除く。）を入手したときは、警察庁情報セキュリティ管理者に連絡しなければならない。

(15) システムセキュリティ責任者は、(14)で入手した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、必要な措置を執らなければならない。

(16) システムセキュリティ責任者は、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、必要な対策を講じなければならない。

(17) 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、災害時等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しなければならない。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らなければならない。

(18) 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を構成するネットワーク機器については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しなければならない。

(19) 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しなければならない。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。

(20) 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、必要な措置を執らなければならない。

(21) 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執らなければならない。

(22) システムセキュリティ責任者は、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しなければならない。

(23) システムセキュリティ責任者は、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執らなければならない。

(24) 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しなけ

ればならない。

(25) 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、必要な対策を講じなければならない。

4　細目的事項の委任

その他システムセキュリティ責任者が遵守すべき警察情報システムの運用保守に必要な事項については､警察庁情報セキュリティ管理者が別途定める。

第８　システムセキュリティ維持管理者

1　システムセキュリティ維持管理者の設置

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。

2　システムセキュリティ維持管理者の責務

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。

3　システムセキュリティ維持管理者の遵守事項

(1)　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わなければならない。

(2)　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しなければならない。

(3)　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執らなければならない。

(4)　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しなければならない。

(5)　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は無効化しなければならない。

(6)　システムセキュリティ維持管理者は、定期的に脆弱性情報に係る対策及び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、分析するとともに、不適切な状態にある電子計算機及びネットワーク機器を把握した場合には、システムセキュリティ責任者に報告し、指示を受けて適切に対処しなければならない。また、対処の結果については速やかにシステムセキュリティ責任者に報告しなければならない。

(7)　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しなければならない。

(8)　システムセキュリティ維持管理者は、警察情報セキュリティポリシー又は運用要領に違反する行為を認知したときは、速やかにシステムセキュリティ責任者に報告しなければならない。

4　細目的事項

その他システムセキュリティ維持管理者が遵守すべき警察情報システムの運用保守に必要な事項については、警察庁情報セキュリティ管理者が別途定める。

第９　運用管理者

１　運用管理者の設置

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。

２　運用管理者の責務

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。

３　運用管理者の遵守事項

(1)　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なければならない。

(2)　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なければならない。

(3)　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しなければならない。

第10　システム管理担当者

1　システム管理担当者の設置

(1)　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しなければならない。

(2)　(1)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わなければならない。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。

2　システム管理担当者の責務

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。

3　システム管理担当者の遵守事項

(1)　システム管理担当者は、権限のない者に識別コードを発行してはならない。

(2)　システム管理担当者は、警察情報システムに係るドキュメントを適正に管理しなければならない。

(3)　システム管理担当者は、管理対象となる電子計算機に関連する脆弱性情報の入手に努めなければならない。脆弱性情報を入手した場合には、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に報告しなければならない。

(4)　システム管理担当者は、クラス３に指定された区域に設置されている警察情報システムを構成する機器、外部記録媒体及びシステムドキュメン

トを、クラス２以下に指定された区域に持ち出すときは、その状況を記録しなければならない。

(5)　システム管理担当者は、警察情報システムの構成の変更等の作業（軽微なものを除く。）を行う場合において、情報セキュリティの観点から、あらかじめその影響を確認するとともに、その作業を監視し、必要な対応を行わなければならない。

(6)　システム管理担当者は、警察情報システムを管理する目的以外の目的で管理者権限を使用してはならない。

第11　ネットワーク管理担当者

１　ネットワーク管理担当者の設置

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、管理者権限を付与しなければならない。

２　ネットワーク管理担当者の責務

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。

３　ネットワーク管理担当者の遵守事項

(1)　ネットワーク管理担当者は、管理対象となるネットワーク機器に関連する脆弱性情報の入手に努めなければならない。脆弱性情報を入手した場合には、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に報告しなければならない。

(2)　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ついて、データ伝送に関する監視及び制御を行わなければならない。

(3)　ネットワーク管理担当者は、ネットワークの構成の変更等の作業（軽微なものを除く。）を行う場合において、情報セキュリティの観点から、あらかじめその影響を確認するとともに、その作業を監視し、必要な対応を行わなければならない。

(4)　ネットワーク管理担当者は、警察情報システムを管理する目的以外の目的で管理者権限を使用してはならない。

第12　媒体利用管理者

1　媒体利用管理者の設置

(1)　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。

(2)　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。

2　媒体利用管理者の責務

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。

第13　その他

1　情報セキュリティインシデント発生時の措置

不正プログラム感染等の情報セキュリティインシデントが発生した際の措置については、最高情報セキュリティ管理者が別途定める。

2　分掌

区域情報セキュリティ管理者、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。

3　兼務を禁止する役割

(1)　職員は、情報セキュリティ対策の運用において、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。）を兼務してはならない。

(2)　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、承認等を得なければならない。

4　管理体制の代替措置

第７の３(10)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。

５　警察情報セキュリティポリシーの見直し

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・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わなければならない。

６　警察情報セキュリティポリシーの解釈

警察情報セキュリティポリシーの解釈に関し疑義があるときは、警察庁情報セキュリティ管理者がこれを裁定する。

別紙

情報システム台帳に記載すべき項目

１　情報システム名

２　システムセキュリティ責任者の役職名

３　システムセキュリティ維持管理者の役職名

４　システム管理担当者の氏名及び連絡先

５　ネットワーク管理担当者の氏名及び連絡先

６　運用開始年月日

７　運用終了予定日

８　情報システム構成図

９　接続する電気通信回線の種別（次に掲げる事項を例として記載する。）

(1)　インターネット回線

(2)　専用線

(3)　広域イーサネット（有線）

(4)　携帯電話網（閉域網）

(5)　その他（具体的に）

10　ネットワーク機器

11　アプリケーション

12　取り扱う管理対象情報の分類及び取扱制限に関する事項

13　当該警察情報システムの設計・開発、運用・保守に関する事項

14　事業者等が提供する情報処理サービスにより情報システムを構築する場合には、次に掲げる事項を含む内容についても台帳として整備すること。

(1)　情報処理サービス名

(2)　契約事業者

(3)　契約期間

(4)　情報処理サービスの概要

(5)　ドメイン名

(6)　取り扱う管理対象情報の分類及び取扱制限に関する事項

15　情報セキュリティインシデント発生時に報告する内容のうち、情報システムに関する事項