○群馬県警察情報セキュリティに係る管理対象情報の分類及び管理体制運用要領の制定について（例規通達）

平成30年３月20日群本例規第７号（情管）

改正

平成31年３月29日群本例規第９号（情管）

群馬県警察情報セキュリティに係る管理対象情報の分類及び管理体制運用要領の制定について（例規通達）

この度、別添のとおり群馬県警察情報セキュリティに係る管理対象情報の分類及び管理体制運用要領を制定し、平成30年４月１日から施行することとしたから、事務処理上遺漏のないようにされたい。

なお、群馬県警察情報セキュリティに係る情報の分類及び管理体制運用要領の制定について（平成26年群本例規第10号）は、廃止する。

別添

群馬県警察情報セキュリティに係る管理対象情報の分類及び管理体制運用要領

第１　総則

１　目的

この要領は、群馬県警察情報セキュリティに関する訓令（平成15年群馬県警察本部訓令甲第12号。以下「訓令」という。）第５条第２項及び第９条の規定に基づき、警察情報セキュリティを確保するために必要な管理対象情報の分類及び管理体制について必要な事項を定めるものとする。

２　用語の定義

この要領における用語の意義は、訓令に定めるもののほか、次に定めるところによる。

（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

警察情報システム等及び管理対象情報を取り扱う警察職員（非常勤嘱託員及び臨時職員を含む。）をいう。

（３）　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。

（４）　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。

（５）　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装置及びメインフレームをいう。

（６）　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。

（７）　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。

（８）　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。

（９）　識別コード

ユーザＩＤ、ホスト名等主体を識別するため情報システムが認識するコード（符号）をいう。

(10)　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。

(11)　主体認証情報

パスワード等主体認証をするため主体が情報システムに提示する情報をいう。

(12)　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。

(13) 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。

(14) 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。

(15) 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。

第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

（１）　機密性３（高）情報

管理対象情報のうち、特定秘密（群馬県警察の特定秘密の保護に関する訓令（平成27年群馬県警察本部訓令甲第６号）第１条第１項に定めるものをいう。）又は秘密文書（群馬県警察の秘密文書管理に関する訓令（平成14年群馬県警察本部訓令甲第７号）第２条第１項に定めるものをいう。）に相当する機密性を要する情報を含むもの

（２）　機密性２（中）情報

管理対象情報のうち、非開示情報（群馬県情報公開条例（平成12年群馬県条例第83号）第14条各号に定めるものをいう。以下同じ。）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

（３）　機密性１（低）情報

管理対象情報のうち、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

２　完全性

（１）　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、改ざんされた場合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

（２）　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

（１）　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

（２）　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

第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、次の例により、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行うものとする。

１　複製の禁止

管理対象情報について、複製を禁止する必要がある場合は、「複製禁止」等の指定をすること。

２　持ち出しの禁止

管理対象情報について、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は、「持ち出し禁止」等の指定をすること。

３　配布の禁止

管理対象情報について、定められた者以外への配布を禁止する必要がある場合は、「配布禁止」等の指定をすること。

４　読後廃棄

管理対象情報について、読後に廃棄する必要がある場合は、「読後廃棄」等の指定をする。た

だし、廃棄日が未定のため、期限を設けること。

５　閲覧の制限

管理対象情報について、閲覧可能な範囲を制限する必要がある場合は、「○○限り」等の指定をすること。

第４　管理体制

１　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総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、及びその実施状況について、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（平成30年９月11日付け警察庁丙情管発第44号ほか）に定める警察庁情報セキュリティ管理者（以下「警察庁情報セキュリティ管理者」という。）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等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、警察情報システム等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）　情報セキュリティ管理者は、災害時等において、警察情報システム等の復旧、通信手段の確保等のためにやむを得ない場合は、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。

（７）　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、警察本部長に報告しなければならない。

（８）　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等について、緊急連絡先、連絡手段及び連絡内容を含む緊急連絡網を整備しなければならない。

（９）　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等について、その訓練の内容及び体制を整備しなければならない。

(10)　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。

(11)　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。

(12)　情報セキュリティ管理者は、群馬県警察が整備した全ての情報システムに対して、別表に掲げる事項を記録し、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。

２　情報セキュリティ責任者

（１）　情報セキュリティ責任者の設置

群馬県警察に情報セキュリティ責任者を置き、警務部情報管理課長をもって充てる。

（２）　情報セキュリティ責任者の責務

情報セキュリティ責任者は、情報セキュリティ管理者に対し、情報セキュリティ対策の推進に係る助言を行うほか、情報セキュリティの確保に必要な事務を処理するものとする。

（３）　情報セキュリティ責任者の遵守事項

情報セキュリティ責任者は、次に定める事項について助言を行わなければならない。

ア　警察情報セキュリティポリシーの整備

イ　警察情報システム等に係る技術的事項
ウ　警察情報システム等の設計・開発を外部委託により行う場合における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
エ　前記アからウまでに掲げるもののほか、情報セキュリティ対策に係る事項

3　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

ア　情報セキュリティ管理者は、庁舎（群馬県警察の庁舎の管理に関する訓令（昭和42年群馬県警察本部訓令甲第２号）第２条に規定する庁舎をいう。以下同じ。）の敷地を複数の区域に分割し、当該区域をクラス０からクラス３に分類する。
イ　各区域（クラス０の区域を除く。）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　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
各庁舎の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
警察情報システム等に係る機械室は、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

ア　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、次に定める対策を講じ、及び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
ａ　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。
ｂ　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。
ｃ　職員以外の者を立ち入らせる場合は、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。
ｄ　職員以外の者を立ち入らせる場合は、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
ａ　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。
ｂ　無人となる場合は、施錠すること。
ｃ　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。
ｄ　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。
ｅ　クラス０に分類される区域と接する場合は、当該境界において前記（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、他の機関が前記（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

ａ　常時施錠し、立ち入ることができる者の名簿を作成すること。この場合において、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。

ｂ　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。

ｃ　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。この場合において、当該記録は、可能な限り電磁的に記録すること。

ｄ　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。

ｅ　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。

ｆ　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。

ｇ　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。

イ　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、前記ア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は、前記（１）のウの基準による運用を困難と認めた場合は、当該基準によらない区域を設けることができる。この場合において、情報セキュリティ管理者は、前記（３）の規定を参考として、関係する他の区域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。

４　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

警察情報システム等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

ア　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等が必要な情報セキュリティ要件を備え、当該情報システム等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。

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等を構築する場合は、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

ア　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等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責任者を経て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。

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等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。

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等について、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

エ　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。

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等の運用及び保守において、当該情報システム等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。

カ　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等における不

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。

キ　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等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。

ク　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等において、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。

ケ　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等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等において、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たい化及びプロトコルのぜい弱性に関する情報を定期的に入手しなければならない。

コ　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等ごとに、当該情報システム等を利用する業務の主管課の長と連携の上、当該情報システム等の運用要領を策定するなどして､職員が当該情報システム等を取り扱う際に遵守すべき事項を職員に周知するとともに、情報セキュリティ管理者に通知しなければならない。この場合において、遵守すべき事項には、次に掲げる事項を含むものとする。

（ア）　当該情報システム等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）　当該情報システム等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）　当該情報システム等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）　当該情報システム等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

サ　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等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。

シ　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。

ス　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等について、公開された情報セキュリティに係るぜい弱性情報（原因、影響範囲、対策方法及びぜい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､ぜい弱性情報を入手した場合は、情報セキュリティ責任者を経て情報セキュリティ管理者に連絡しなければならない。

セ　システムセキュリティ責任者は、前記スで入手したぜい弱性情報が所管する警察情報システム等にもたらすリスクを分析した上で、ぜい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。

ソ　システムセキュリティ責任者は、公開されたぜい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。

タ　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等について、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。この場合において、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。

チ　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等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。

ツ　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。

テ　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等の情報セキュリティ対策についてぜい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。

ト　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、既知の種類のぜい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。

ナ　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。

ニ　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。

ヌ　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等を運用する場合は、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等を運用しなければならない。

ネ　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等の設置環境、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

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等の運用保守に必要な事項については、情報セキュリティ管理者が別に定める。

５　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

警察情報システム等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等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

ア　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。

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等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。

ウ　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等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。

エ　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、利用しない機能については、無効化しなければならない。

オ　システムセキュリティ維持管理者は、定期的にぜい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。この場合において、対処の結果を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。

カ　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場合は、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等の運用保守に必要な事項については、情報セキュリティ管理者が別に定める。

6　運用管理者

（1）　運用管理者の設置

警察情報システム等を運用する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等の運用に関し、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

ア　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。

イ　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。

7　システム管理担当者

（1）　システム管理担当者の設置

システムセキュリティ維持管理者は、その管理する警察情報システム等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）　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等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

ア　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。

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

ウ　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ぜい弱性情報の入手に努めなければならない。この場合において、情報を入手したときは、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。

エ　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等を構成する機器、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場合は、その状況を記録しなければならない。

オ　システム管理担当者は、警察情報システム等の構成の変更等の作業（軽微なものを除く。）を行う場合は、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。

8　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

ア　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ぜい弱性情報の入手に努めなければならない。この場合において、情報を入手したときは、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。

イ　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。

ウ　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。）を行う場合は、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。

９　運用責任者

（１）　運用責任者の設置

警察情報システム等を運用する所属に運用責任者を置き、警察本部の所属にあっては次席（部の附置機関の副隊長及び副校長を含む。）を、警察署にあっては副署長をもって充てる。

（２）　運用責任者の責務

運用責任者は、運用管理者を補佐し、機器及び外部記録媒体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。

10　運用補助者

（１）　運用補助者の設置

ア　外部記録媒体を利用する所属に一人又は複数人の運用補助者を置き、運用管理者が指名する者をもって充てる。

イ　運用補助者は、警部（警部相当職の一般職員を含む。）以上の階級の職員とする。ただし、警部以上の者を指名できないやむを得ない事情がある場合は、警部補（警部補相当職の一般職員を含む。）の階級にある者のうち、運用管理者が指名するものをもって充てることができる。

（２）　運用補助者の責務

運用補助者は、運用責任者を補佐し、機器及び外部記録媒体の適正な取扱いを確保するために必要な事務のほか、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５　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、別に定める。

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は、当該分庁舎の警視（警視相当職の一般職員を含む。）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

前記第４の４の（３）のコに定める運用要領について、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は、当該運用要領に従うものとする。

５　警察情報セキュリティポリシーの見直し

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場合は、情報セキュリティ管理者がこれを裁定する。

前　文（抄）（平成31年３月29日群本例規第９号（情管））

平成31年４月１日から施行する。

別表（第４関係）

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　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
11　当該情報システムの設計・開発及び運用・保守に関する事項
12　民間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