兵庫県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（例規甲）

〔平成28年９月20日
兵警情例規甲第30号本部長〕

〔沿革〕　平成30年２月兵警情例規甲第７号、31年２月第６号、３月第14号、令和４年10月第26号改正

兵庫県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を下記のように定め、平成28年10月１日から実施する。

記

第１　総則

１　目的

この通達は、兵庫県警察における情報セキュリティに関する訓令（平成23年兵庫県警察本部訓令第１号。以下「訓令」という。）第５条第２項及び第８条の規定に基づき、兵庫県警察における管理対象情報の分類及び兵庫県警察における情報セキュリティを維持するために必要な管理体制に関し必要な事項を定めるものとする。

２　定義規定等の適用

訓令、兵庫県警察情報システムの利用及び管理対象情報の取扱いに係る警察職員の遵守事項について（平成28年兵警情例規甲第31号）及び兵庫県警察情報システムの情報セキュリティ要件について（平成28年兵警情例規甲第32号）に定めるところによる定義規定及び略称規定は、この通達において適用する。

３　定義

この通達において、次に掲げる用語の意義は、それぞれに定めるところによる。

(1)　兵庫県警察情報セキュリティポリシー　訓令及び訓令に基づく規程に規定された情報セキュリティに関する事項をいう。

(2)　システムドキュメント　次に掲げる文書、図画及び電磁的記録（作成中のものを含む。）をいう。

ア　システム仕様書（情報の処理に必要な機能、項目等を定義した記録をいう。）

イ　システム設計書（情報の処理手順並びに機器及びプログラムの構成の概要の記録をいう。）

ウ　プログラム仕様書（情報の処理手順の概要の記録をいう。）

エ　プログラムリスト（情報の処理手順を電子計算機に指示した記録をいう。）

オ　操作指示書（情報システムの維持管理に伴う機器の設定方法等を説明した記録をいう。）

(3)　取扱説明書　情報システムを利用する者が業務を行う上で参照する機器の操作の方法を説明した記録をいう。

(4)　ドキュメント　警察情報システムに関するシステムドキュメント及び取扱説明書をいう。

(5)　外部記録媒体　フラッシュメモリ、外付けハードディスクドライブ、光ディスク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。

(6)　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。

(7)　ネットワーク機器　情報システムを構成するルータ、スイッチング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。
(8)　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。
(9)　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。
(10) 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。
(11) 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。
(12) 要安定情報　可用性２（高）情報に分類される管理対象情報をいう。
(13) ドメイン　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グループをいう。
(14) ドメイン名　ドメインの名前であり、英数字及び一部の記号を用いて表したものをいう。
(15) 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。
(16) 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。
(17) 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。
(18) 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。
(19) 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。
(20) 情報システム台帳　情報システムにおける情報セキュリティ対策に係る情報及びセキュリティ要件に係る事項を記録し、又は記載したものをいう。

第２　管理対象情報の分類及び取扱制限

１　訓令第５条第１項の規定による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（特定秘密の保護に関する法律（平成25年法律第108号）第３条第１項の規定により指定された特定秘密をいう。）又は秘密文書（兵庫県警察における秘密文書の取扱いに関する訓令（平成13年兵庫県警察本部訓令第20号）第２条第１項に規定するものをいう。）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、情報公開条例（平成12年兵庫県条例第６号。以下「情報公開条例」という。）第６条各号における非公開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、情報公開条例第６条各号における非公開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）情報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）情報に分類される以外のもの

２　訓令第６条の規定による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、必要に応じて管理対象情報に設ける取扱制限は次のとおりとする。

(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指定する。

(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指定する。

(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指定する。

(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指定する。

(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指定する。

(6)　公開予定なし　当該情報について、直ちに一般に公開することを前提としていない場合に指定する。

(7)　前記(1)から(6)までに掲げるもののほか、取扱制限が必要と認めるときは、適宜必要な取扱制限を指定するものとする。

第３　管理体制

１　情報セキュリティ管理者

情報セキュリティ管理者の遵守事項は、次のとおりとする。

(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、職員に兵庫県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、教養を実施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（優先度が高い業務の継続性を確保するために必要な事項を定めたものをいう。以下同じ。）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又は維持改善等を行う際に、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、問題点又は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)　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、所要の措置をとらなければならない。

(7)　情報セキュリティ管理者は、職員に情報セキュリティについての自己点検を

実施させなければならない。

(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。

(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、兵庫県警察が整備した全ての情報システムに対して、別記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。

2　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、兵庫県警察庁舎管理規程（平成９年兵庫県警察本部訓令第15号）第３条第４号に規定する本部庁舎、同条第５号に規定する本部所属庁舎、同条第６号に規定する警察署庁舎又は兵庫県警察が使用し、若しくは管理する部屋、建物及びこれに附属する工作物並びに敷地（以下「庁舎」という。）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までに分類する。

イ　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く。

ウ　区域の分類の方法及び各区域の区域情報セキュリティ管理者として充てる者は次のとおりとする。

(ｱ)　クラス０

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

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、当該庁舎を管理する者をもって充てる。

(ｳ)　クラス２

庁舎の各室は、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、当該所属の長をもって充てる。

(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もって充てる。

(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行う。

(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、次に掲げる対策を実施しなければならない。

(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には、確認ができない時間帯に施錠するなどの措置をとること。

c　職員以外の者を立ち入らせるときは、その者の氏名、会社名又は住所、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ときは、総務部長が別に定める場合を除き、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　無人となるときは施錠すること。

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とること。

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並びに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留意すること。

e　クラス０の区域と接するときは、当該境界において前記(ｱ)に規定する対策を講ずること。

(ｳ)　クラス３の管理対策

a　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。なお、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とること。

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とること。

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。また、持ち込みが許可された機器については、許可を受けていることを確認できるような措置をとること。

g　自然災害の発生等に起因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と認めるときは、当該区域において実施する個別の対策を講じなければならない。

(4)　管理対策の実施が困難な場合の措置

区域情報セキュリティ管理者は、所管する区域において、前記(3)に規定する管理対策の実施が困難と認めたときは、情報セキュリティ管理者の承認を得た上で、別に庁舎を管理する者がいる場合は当該庁舎を管理する者と連携し、前記(3)の規定に準じて、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実施しなければならない。

3　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

ア　警察情報システムごとに、システムセキュリティ責任者を置く。

イ　システムセキュリティ責任者は、警察情報システムの整備を担当する部又は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。

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又は管理の定め（以下「基盤となる情報システムの運用管理規程等」という。）に基づき、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が情報セキュリティ要件を満たしているかについて、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。

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の導入時、稼働中及び廃棄時の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について、次に掲げるもの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。

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策定しなければならない。この場合において、当該警察情報システムの運用要領等には、次に掲げる事項を含めるものとする。

(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、ソフトウェアの追加等）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

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について、情報セキュリティに係るぜい弱性情報（ぜい弱性の原因、影響範囲及び対策方法並びにぜい弱性を悪用する不正プログラムの流通状況を含む。以下同じ。）を適宜入手するとともに、ぜい弱性情報（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、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、必要な措置をと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、可能な限り兵庫県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にはその見直しを行い、必要な措置をと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を運用するときは、既知の種類のぜい弱性を排除するための対策が講ぜられているか定期的に確認し、対策が十分でないと認めたときは必要な措置をと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と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を運用する場合は、基盤となる情報システムの運用管理規程等に基づき、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。

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、総務部長が別に定める。

4　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

ア　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、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、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。

イ　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。

ウ　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とらなければならない。

エ　システムセキュリティ維持管理者は、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。

オ　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、定期的にぜい弱性情報に係る対策、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するとともに、これを分析し、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。

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、規範意識等の向上を目的とした教養を適宜実施しなければならない。

ク　システムセキュリティ維持管理者は、兵庫県警察情報セキュリティポリシー、所管する警察情報システムの運用要領等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、総務部長が別に定める。

5　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

運用管理者は、職員に対して兵庫県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。

6　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、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、管理の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、ぜい弱性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に分類されている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、外部記録媒体又はシステムドキュメントを、クラス２以下に分類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。

オ　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、あらかじめ試験環境を構築し検証するなど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。

カ　システム管理担当者は、システム管理に関する業務を行う目的以外の目的で管理者権限を使用してはならない。

7　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真に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、管理の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、ぜい弱性情報を入手したときには、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。

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。

エ　ネットワーク管理担当者は、ネットワーク管理に関する業務を行う目的以外の目的で管理者権限を使用してはならない。

8　媒体利用管理者

(1)　媒体利用管理者の設置

ア　外部記録媒体を利用する所属に媒体利用管理者を置く。

イ　媒体利用管理者は、警部以上の階級にある警察官又は警部相当職以上の一般職員をもって充てる。

ウ　運用管理者は、必要があると認めるときは、前記イの規定によらず、警部補の階級にある警察官又は警部補相当職の一般職員を媒体利用管理者に指名することができる。この場合において、運用管理者は、総務部長が別に定める方法により、その状況を明らかにしておかなければならない。

(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４　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、総務部長が別に定める。

第５　分掌

運用管理者は、情報セキュリティ管理者の許可を受けたときは、遠隔地の庁舎に勤務する警視以上の階級にある警察官又は警視相当職以上の一般職員を指名し、自身の権限に属する事務を当該庁舎において分掌させることができる。

第６　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。

第７　管理体制の代替措置

前記第３の３の(3)のコに定める運用要領等については、兵庫県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（警察庁と接続している警察情報システムにあっては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。

別記

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職名
３　システムセキュリティ維持管理者の職名
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
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は、次に掲げる事項を含む内容についても記載すること。
(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

注　９はインターネット回線、専用線、広域イーサネット（有線）、携帯電話網（閉域網）等の例により記載すること。