部長及び参事官　　情管発第５４号
殿　　（生企、刑企、交企、備－）
所　属　長　　平成28年２月10日
10年保存（口訓）
本　部　長

（沿革）　平成28年12月７日情管発第363号改正
（沿革）　平成30年２月26日情管発第37号改正
（沿革）　平成31年３月１日情管発第49号改正
（沿革）　令和２年３月24日情管発第100号改正

高知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（通達甲）

県警察における情報セキュリティに係る管理体制に関し「高知県警察情報セキュリティに係る管理体制の制定について（例規）」（平成25年12月25日情管発第467号）を制定しているところであるが、高知県警察公文書管理規程（平成27年６月本部訓令第18号）の施行により公文書種別から例規をなくすることに伴い、当該管理体制に関し次のとおり定め、平成28年２月10日から実施することとしたので、誤りのないようにされたい。

記

第１　総則

１　趣旨

この通達甲は、高知県警察における情報セキュリティに関する訓令（平成16年６月本部訓令第10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、県警察における情報セキュリティを確保するための管理体制に関し必要な事項を定めるものとする。

２　管理対象情報の分類

高知県警察情報システム（以下「県警察情報システム」という。）において取り扱われ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（高知県警察における特定秘密の保護に関する訓令（平成26年12月本部訓令第26号）第１条に定めるものをいう。）又は秘密文書（高知県警察公文書管理規程（令和２年３月本部訓令第５号）第２条第10号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

イ　機密性２（中）情報

管理対象情報のうち、高知県情報公開条例（平成２年高知県条例第１号。以下「情報公開条例」という。）第６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、情報公開条例第６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）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

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

高知県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、別に定める場合を除き、次のとおりとする。

(1)　高知県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

県警察情報システム及び管理対象情報を取り扱う高知県警察職員をいう。

(3)　要機密情報

機密性３（高）又は機密性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)　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を含む。）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)　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。

(10) 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。

(11) 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。

(12) 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。

(13) 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。

(14) 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。

(15) 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。

(16) 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。

(17) 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。

(18) 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。

(19) 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。

(20) 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。

(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) 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。

(23) 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。

(24) 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。

(25) 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。

(26) 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。

(27) 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。

(28) 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。

(29) 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。

(30) 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。

(31) 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。

(32) 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。

(33) 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もの又は電磁的記録媒体が内蔵されているものをいう。

(34) クラウドサービス

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。

(35) 約款による外部サービス

民間事業者等が約款に基づきインターネット上で提供する電子メール、ファイルストレージ、グループウェア等の情報処理サービスであって、当該サービスを提供するサーバにおいて利用者が情報の作成、保存、送信等を行うものをいう。ただし、クラウドサービスに該当するものは除く。

(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) 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。

(38) 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。

(39) 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。

(40) 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、ウェブコンテンツ等の総称をいう。

第２　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ときは、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、職員に高知県警察情報セキュリティポリシー（以下「県警察情報セキュリティポリシー」という。）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、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県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、県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は、県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　情報セキュリティ管理者は、災害時等において、県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、県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、県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、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。

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県警察情報システムについて、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県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、全ての県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。

12　情報セキュリティ管理者は、県警察情報システムを新規に構築し、又は更改する際には、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。

第3　情報セキュリティアドバイザー

1　情報セキュリティアドバイザーの設置

県警察に情報セキュリティアドバイザーを置き、情報管理課長をもって充

てる。

２　情報セキュリティアドバイザーの責務

情報セキュリティアドバイザーは、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ものとする。

３　情報セキュリティアドバイザーの遵守事項

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)　県警察情報セキュリティポリシーの整備

(2)　県警察情報システムに係る技術的事項

(3)　県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

(4)　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４　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、県警察の管理する庁舎、施設及びその敷地内における各区域を態様ごとに分割し、当該分割した区域をクラス０から３までに分類する。

(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は、次に掲げる基準により行うものとする。

ア　クラス０

県警察の管理する庁舎、施設及びその敷地内であって、職員以外の者が自由に立ち入ることのできる区域は、一の区域としてクラス０に分類する。

イ　クラス１

庁舎における廊下等の職員の共用区域は、一の区域としてクラス１に分類し、その区域情報セキュリティ管理者に、当該庁舎を管理する所属の長を指名する。

ウ　クラス２

執務室は、所属ごとに一の区域としてクラス２に分類し、その区域情報セキュリティ管理者に、当該執務室を使用する所属の長を指名する。ただし、所属の執務室が複数の庁舎にわたる場合は、執務室ごとに区域情報セキュリティ管理者を指名することができる。この場合において、当該区域情報セキュリティ管理者には、所属の長以外の者を指名するこ

とができる。

エ　クラス３

県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てクラス３に分類し、その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、次のアからウまでに定める管理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識別証を身に付けさせるなどして、職員と職員以外の者と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の区域への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、合同庁舎等他の機関が管理する施設等に執務室がある場合において、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及び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。

(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、職員の立合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、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は、１(3)の基準による運用が困難であると認めたときは、当該基準によらない区域を設けることができる。この場合において、情報セキュリティ管理者は、３に定める管理対策を参考にして、関係する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。

第５　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

県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、整備する県警察情報システムに必要な情報セキュリティ要件を備え、当該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県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、県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、所管する県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、所管する県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、所管する県警察情報システムの運用及び保守において、当該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、所管する県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、主体から県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県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、暗号化を行う県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県警察情報システムにおいて、暗号化

又は電子署名のために選択された暗号アルゴリズムの危殆化及びプロトコルの脆弱性に関する情報を定期的に入手しなければならない。

(10) システムセキュリティ責任者は、所管する県警察情報システムごとに、当該システムを利用する業務の主管課の長と連携の上、当該システムの運用要領を策定するなどして、職員が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。

なお、遵守すべき事項には、次に掲げる事項を示すものとする。

ア　当該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

(11) システムセキュリティ責任者は、必要に応じて、所管する県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。

(12) 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。

(13) システムセキュリティ責任者は、所管する県警察情報システムについて、公開された情報セキュリティに係る脆弱性情報（原因、影響範囲、対策方法及び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、脆弱性情報を入手したときは、情報セキュリティ管理者に報告しなければならない。

(14) システムセキュリティ責任者は、(13)で入手した脆弱性情報が所管する県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。

(15) 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。

(16) システムセキュリティ責任者は、所管する県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。

(17) システムセキュリティ責任者は、要安定情報を取り扱う県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。

(18) 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。

(19) システムセキュリティ責任者は、所管する県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。

(20) 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ないかを定期的に確認し、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。

(21) 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。

(22) 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。

(23) 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県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、適切に県警察情報システムを運用しなければならない。

(24) システムセキュリティ責任者は、県警察情報セキュリティポリシーに定めるもののほか、所管する県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県警察情報システムの運

用保守に必要な事項については、別に定める。

第６　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

県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、担当する県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、管理者権限を適正に運用しなければならない。

(2)　システムセキュリティ維持管理者は、主体が県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。

(3)　システムセキュリティ維持管理者は、維持管理する県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。

(4)　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。

(5)　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て確認及び分析するとともに、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も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。

(6)　システムセキュリティ維持管理者は、県警察情報セキュリティポリシー又は第５の３(10)の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県警察情報システムの運用保守に必要な事項については、別に定める。

第７　運用管理者

1　運用管理者の設置

県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、所属における県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、それ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、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、職員の(1)及び(2)の教養受講状況について、情報セキュリティ管理者に報告しなければならない。

第８　運用管理補助者

1　運用管理補助者の設置

県警察情報システムを運用する所属に運用管理補助者を置き、それぞれ当該所属の次長（次長が二人の所属は、次長（第一）の職にある者とする。）又は副署長をもって充てる。

2　運用管理補助者の責務

運用管理補助者は、運用管理者を補佐する。

第９　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、維持管理する県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、担当する県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、県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県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、県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。

第10　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、維持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、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。

第11　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、外部記録媒体の管理及び点検を行うとともに、外部記録媒体を利用した管理対象情報の入出力の管理及び端末管理に係る事務を行うものとする。

第12　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には、当該分庁舎の警視相当職以上の職員（警視相当職以上の職員がいない場合は警部相当職以上の職員）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５の３(10)の運用要領について、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の確認を受けた場合には、当該運用要領に従うものとする。

5　県警察情報セキュリティポリシーの解釈

県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、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　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、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