兵庫県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（一般甲）

（令和６年10月30日
兵警情一般甲第91号）

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対策の基準は、令和６年11月１日から兵庫県警察における情報セキュリティに関する対策基準（別添）に基づき実施することとしたので、各所属長は、所属職員に周知徹底の上、適切な情報セキュリティの維持に努められたい。

別添

兵庫県警察における情報セキュリティに関する対策基準

第１　総則

１　目的

この対策基準は、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情報セキュリティを維持するために必要な対策の基準について定めるものとする。

２　定義規定等の適用

訓令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　用語の定義

この対策基準において、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)　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。

(2)　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。

(3)　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。

(4)　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。

(5)　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。

(6)　兵庫県警察ＣＳＩＲＴ　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。

(7)　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。

(8)　外部委託　業務委託及びクラウドサービスをいう。

(9)　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。

(10)　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。

(11)　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。

(12)　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。

(13)　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。

(14)　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。

(15)　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。

(16)　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。

(17) 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。
(18) 業務委託　警察の業務（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。）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。
(19) 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ものをいう。
(20) 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。
(21) 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をいう。
(22) 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。
(23) 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。
(24) 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、又は電磁的記録媒体が内蔵されているものをいう。
(25) 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。
(26) 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。
(27) ドメインネームシステム　クライアント等からの問合せを受けて、ドメイン名又はホスト名と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。
(28) 名前解決　ドメイン名又はホスト名とＩＰアドレスを変換することをいう。
(29) 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。
(30) 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。
(31) 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。
(32) 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。
(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、動画共有サイト等利用者が情報を発信し、形成していくものをいう。

4　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、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。

5　兵庫県警察情報システムの分類等

(1)　兵庫県警察情報システムの分類及び分類基準

兵庫県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し、又は他の重要度（高）システムに影響を与えるもの

イ　重要度（中）システム　要保護情報を取り扱い、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もの（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）システム以外のもの

(2)　兵庫県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

兵庫県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は、次のとおりとする。

ア　基本セキュリティ対策　兵庫県警察情報システムの構成要素及び兵庫県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、全ての兵庫県警察情報システムが実施すべき対策

イ　追加セキュリティ対策　兵庫県警察情報システムの構成要素及び兵庫県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、重要度（高）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対策。ただし、重要度（高）システム以外のものについても、必要に応じて実施を検討すること。

第２　情報セキュリティ対策の基本的枠組み

1　導入及び計画

(1)　体制の整備

ア　情報セキュリティ管理者等の設置

(ｱ)　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、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、建物及びこれに付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。

(ｲ)　運用管理者の設置

a　兵庫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。

b　運用管理者は、所属における兵庫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。

(ｳ)　システムセキュリティ責任者の設置

a　兵庫県警察情報システムの整備を担当する部（サイバーセキュリティ・捜査高度化センターを含む。）又は所属にシステムセキュリティ責任者を置き、それぞれ当該部又は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、整備する兵庫県警察情報システムが必要なセキュリティ要件を備え、当該兵庫県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。

(ｴ)　システムセキュリティ維持管理者の設置

a　兵庫県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、担当する兵庫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。

(ｵ)　システム管理担当者の設置

a　システムセキュリティ維持管理者は、その管理する兵庫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。

b　システム管理担当者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、情報セキュリティ管理者が認める兵庫県警察情報システムにあっては、この限りでない。

c　システム管理担当者は、担当する兵庫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。

(ｶ)　ネットワーク管理担当者の設置

a　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。

b　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。

(ｷ)　媒体利用管理者の設置

a　外部記録媒体及び公費携帯電話機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。

b　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。

c　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及び公費携帯電話機の管理に係る事務を行うものとする。

イ　情報セキュリティ対策推進体制の整備

(ｱ)　総務部情報管理課に、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、総務部情報管理課長をもって充てる。

(ｳ)　情報セキュリティ対策推進体制の構成員は、総務部情報管理課長が指名する。

ウ　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、兵庫県警察に兵庫県警察ＣＳＩＲＴを置く。

(ｲ)　兵庫県警察ＣＳＩＲＴの長は、総務部情報管理課長をもって充てる。

(ｳ)　兵庫県警察ＣＳＩＲＴの運営に係る事項については、情報セキュリティ管理者が別途定める。

エ　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。

オ　その他

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た上で分掌させることができる。

(2)　リスク評価の実施

情報セキュリティ管理者は、自己点検結果、情報セキュリティ監査結果等を踏まえ、兵庫県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

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。）

を定めること。

イ　対策推進計画の内容

前記アの対策推進計画には、兵庫県警察の業務、兵庫県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及び重点並びに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)　兵庫県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の結果を踏まえた対策への取組

(ｶ)　前記(ｱ)から(ｵ)まで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　運用

(1)　情報セキュリティ関係規程の違反への対処

ア　職員は、兵庫県警察情報セキュリティポリシー又は第５の１の(2)のアによ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、兵庫県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、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、兵庫県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、合理的な理由がある場合は、後記(ｲ)、イ、ウ及び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。

(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、情報セキュリティ管理者とする。

イ　例外措置の運用

(ｱ)　申請者は、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、許可者に対して事前に申請を行うこと。

なお、例外措置の適用期間は、最長１年間とする。

(ｲ)　システムセキュリティ責任者は、所管する兵庫県警察情報システムの運用において、例外措置の適用が必要と認める場合は、適用を受けようとする業務等の範囲をあらかじめ定めた上で、許可者に申請し、包括許可を受けることができる。

なお、包括許可による例外措置の適用期間は、最長５年間とする。

(ｳ)　許可者は、申請内容を審査し、情報セキュリティ上の影響及び対処方法を検討し、その検討結果を記録すること。

(ｴ)　許可者は、前記(ｳ)の検討を基に許可の可否を決定し、審査の結果を申請者に通

知すること。

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、この対策基準に定める事項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、当該事項にかかわ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、兵庫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、兵庫県警察情報セキュリティポリシーに定める事項にかかわらず、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、特定の兵庫県警察情報システムについて、この対策基準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、情報セキュリティ管理者と協議の上、当該兵庫県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　教養体制の整備及び教養実施計画の策定

(ｱ)　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こと。

(ｲ)　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、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箇月以内に実施すること。

(ｲ)　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。

(ｳ)　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ること。また、運用管理者は、兵庫県警察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。

(ｴ)　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。

(ｵ)　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適宜実施すること。

(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)　情報セキュリティインシデントの可能性がある事案のうち、兵庫県警察ＣＳＩＲＴの長への報告を要するもの（以下「要報告インシデント」という。）は、次に掲げるものとする。

ａ　情報流出事案　管理対象情報の流出事案

ｂ　重大障害事案　兵庫県警察情報システムにおいて発生した障害であって、30分以上にわたって警察業務に重大な影響を及ぼす事案

ｃ　不正プログラム感染事案、不正アクセス事案及びサイバー攻撃事案　次の事案に該当するもの

(a)　兵庫県警察情報システムにおける不正プログラム感染事案

(b)　兵庫県警察情報システムに対する不正アクセス事案

(c)　兵庫県警察情報システムに対するサイバー攻撃事案（(a)及び(b)に掲げるものを除く。）

ｄ　兵庫県警察情報システムの不正使用事案　あらかじめ定められた目的以外の目的で当該兵庫県警察情報システムを不正に使用した事案

ｅ　個人所有の機器等の不正使用事案　管理対象情報を個人所有の機器等において不正に処理した事案

ｆ　外部委託先等における情報流出事案　次の事案に該当するもの

(a)　兵庫県警察情報システムに係る外部委託先における事案

(b)　兵庫県警察情報システムに係る外部委託について、契約に至らずとも契約を前提としてやり取りを行った事業者における事案

(c)　その他の外部委託について、情報セキュリティインシデントに当たる又はその可能性のある事案

ｇ　その他社会的反響が大きいと予想される事案　兵庫県警察情報システム及び管理対象情報に係る情報セキュリティを損なう事案であって、前記ａからｆまでに掲げるものを除き、報道されるなど社会的反響が大きいと予想されるもの

(ｲ)　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兵庫県警察情報システムについて、緊急連絡先、連絡手段、連絡内容等を含む緊急連絡網を整備すること。

(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兵庫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すること。

(ｴ)　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)　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)　兵庫県警察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、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する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、直ちに運用管理者、システムセキュリティ維持管理者及び兵庫県警察ＣＳＩＲＴの長に報告し、指示に従うこと。

(ｲ)　兵庫県警察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。

(ｳ)　兵庫県警察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、遅延なく情報セキュリティ管理者に報告すること。

(ｴ)　兵庫県警察ＣＳＩＲＴの長は、関係する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システムセキュリティ責任者等に確認を指示すること。

(ｵ)　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兵庫県警察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。

(ｶ)　兵庫県警察ＣＳＩＲＴの長は、要報告インシデントが、兵庫県警察における情報セキュリティの維持に重大な支障を及ぼし、又は及ぼすおそれがあると認めるときは関係する所属の長（以下「関係所属長」という。）に、社会的な反響が大きいと予想されるときは関係所属長及び総務部県民広報課長にその概要を連絡（総務部県民広報課報道第一係、報道第二係又は報道第三係経由）をすること。この場合において、当該要報告インシデントが大規模サイバー攻撃事態に該当するおそれがあるときは、前段の規定による連絡に併せて警備部公安第一課長及びサイバーセキュリティ・捜査高度化センターサイバー捜査課長にその概要を連絡すること。

(ｷ)　兵庫県警察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及び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に該当するおそれがあるときは、総務部県民広報課長に連絡（総務部県民広報課県民情報センター経由）し、対応について助言を受けること。

(ｸ)　兵庫県警察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。

ウ　情報セキュリティインシデントの再発防止及び教訓の共有

(ｱ)　運用管理者は、兵庫県警察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、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)　兵庫県警察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、情報セキュリティ管理者、運用管理者等に対して共有を図ること。また、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。

3　情報セキュリティ対策の自己点検

(1)　自己点検計画の策定及び実施手順の準備

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

イ　情報セキュリティ管理者は、年度自己点検計画に基づき、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　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は、当該年度自己点検計画を見直すこと。

(2)　自己点検の実施

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、職員に対し、自己点検を実施させること。

(3)　自己点検結果の評価等

ア　情報セキュリティ管理者は、兵庫県警察に共通の課題の有無についての観点から自己点検結果を分析し、評価すること。

イ　情報セキュリティ管理者は、前記アの規定による評価の結果により明らかになった問題点について、運用管理者に改善を指示するとともに、その改善結果について報告を受けること。

4　情報セキュリティ対策の見直し

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並びに自己点検及び監査の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、情報セキュリティ対策について定期的に見直しを行うこと。

第３　管理対象情報の取扱い

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、兵庫県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部外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、上位の職員であって、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（夜間及び休日にあっては宿直責任者を含む。以下同じ。）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、部外に管理対象情報を提供する場合は、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及び保存

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し、又は入手しないこと。

(ｲ)　管理対象情報を不正に利用し、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（運用管理者以上の者を除く。）は、庁舎外において機密性３（高）情報を利用する場合は、後記(5)のウの(ｲ)に定める手続を行うこと。

ウ　職員は、情報セキュリティ管理者が別途定める場合を除き、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は、第８の１の(1)のウの規定に従うこと。

カ　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兵庫県警察情報システムを除き、外部回線に接続する兵庫県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。

キ　職員は、兵庫県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及び公表

ア　職員は、管理対象情報を公表する場合は、当該情報が機密性１（低）情報に分類されるものであ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は、後記(5)の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、管理対象情報を部外者に電磁的記録で提供する場合は、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及び送信

ア　職員は、要機密情報を運搬し、又は送信する場合は、情報漏えいを防止するため、必要に応じて次に掲げる措置を講ずること。

(ｱ)　運搬し、又は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、暗号化機能等を備える外部記録媒体を利用する。

イ　職員は、要保護情報が記載された記録媒体の庁舎外への運搬を第三者へ依頼する場合は、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（運用管理者より上位の職にある者を除く。）は、要機密情報について、庁舎外への持ち出しを行う場合は、前記(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、次に掲げる事項を遵守すること。

(ｱ)　機密性２（中）情報を庁舎外に持ち出す場合は、上位の職員であって、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に報告すること。

(ｲ)　機密性３（高）情報を庁舎外に持ち出す場合は、運用管理者の許可を受けること。

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、必要に応じて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。

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、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、前記(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、前記(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維持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　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

情報セキュリティ管理者は、業務委託に際し、次に掲げる基準に関する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)　兵庫県警察情報システムに関する業務委託

ア　兵庫県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、兵庫県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　兵庫県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)　兵庫県警察情報システムのセキュリティ要件の適切な実装

(ｲ)　警察情報セキュリティの観点に基づく試験の実施

(ｳ)　兵庫県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　兵庫県警察情報システムの運用又は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、兵庫県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、当該兵庫県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兵庫県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、兵庫県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した上で、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に限る。）

情報セキュリティ管理者は、次に掲げる事項に関する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及び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に限る。）

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、次に掲げる事項に基づき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又は地域
(ｳ)　クラウドサービスで取り扱う情報の廃棄の方法
(ｴ)　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、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に限る。）

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及び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、仕様の内容を契約に含めること。

(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に限る。）

ア　システムセキュリティ責任者及び運用管理者は、クラウドサービスを利用する場合は、情報セキュリティ管理者にクラウドサービスの利用申請を行うこと。

イ　情報セキュリティ管理者は、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　情報セキュリティ管理者は、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。

(5)　クラウドサービスの利用（要機密情報を取り扱う場合に限る。）

ア　クラウドサービスの利用に係る運用規定の整備

(ｱ)　情報セキュリティ管理者は、クラウドサービスの特性及び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兵庫県警察情報システムを導入し、又は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)　情報セキュリティ管理者は、クラウドサービスの特性及び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兵庫県警察情報システムを運用し、

又は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)　情報セキュリティ管理者は、クラウドサービスの特性及び責任分界点に係る考え方を踏まえ、次に掲げる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、前記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、前記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兵庫県警察情報システム導入時及び構築時の対策

(ｱ)　クラウドサービス管理者は、前記イの(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、その実施状況を確認し、記録すること。

(ｲ)　クラウドサービス管理者は、兵庫県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、クラウドサービスの運用開始前までに次に掲げる事項の実施手順を運用要領に整備すること。

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兵庫県警察情報システムの運用時及び監視時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し、又は利用することが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兵庫県警察情報システムの運用時及び保守時の対策

(ｱ)　クラウドサービス管理者は、前記アの(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及び保守を適切に実施すること。また、その実施状況を定期的に確認し、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について修正又は変更等を行う必要がある場合は、情報システム台帳及び情報システム関連文書を更新し、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宜検討し、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兵庫県警察情報システムの更改時及び廃棄時の対策

(ｱ)　クラウドサービス管理者は、前記アの(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又は廃棄に際し、必要な対策を講ずること。

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

(6)　クラウドサービスの選定及び利用（要機密情報を取り扱わない場合に限る。）

情報セキュリティ管理者は、次に掲げる事項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及び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に限る。）

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は、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情報セキュリティ管理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　情報セキュリティ管理者は、前記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　情報セキュリティ管理者は、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、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。

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

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。この場合において、情報セキュリティ管理者は、必要に応じ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ように管理がなされ、その管理状況について確認するために必要な項目を加えること。

(2)　機器等の納入時の確認及び検査手続の整備

情報セキュリティ管理者は、機器等の納入時の確認手続及び検査手続を整備すること。

第5　兵庫県警察情報システムのライフサイクル

1　兵庫県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　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、情報システム台帳を整備すること。

イ　システムセキュリティ責任者は、兵庫県警察情報システムを構築し、更改し、又は変更する場合は、情報システム台帳に記録し、当該内容について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、所管する兵庫県警察情報システムごとに、当該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、当該情報システムの運用要領等を制定すること。

イ　職員は、前記アに定める運用要領等について、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の確認を受けた場合は、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、所管する兵庫県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、次に掲げる事項に関する文書を整備すること。

(ｱ)　当該兵庫県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)　当該兵庫県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)　当該兵庫県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)　当該兵庫県警察情報システムが停止した際の復旧手順

2　兵庫県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)　兵庫県警察情報システムの企画及び要件の策定

ア　兵庫県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、兵庫県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兵庫県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、兵庫県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、次に掲げる事項を含む兵庫県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　兵庫県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　兵庫県警察情報システム運用時の監視等の運用管理機能要件

ｃ　兵庫県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　兵庫県警察情報システムの可用性に関する対策要件

ｅ　兵庫県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兵庫県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（平成30年２月28日に経済産業省により策定された、デジタル複合機等の製品分野ごとに考慮すべきセキュリティ上の脅威とそれに対抗するためのセキュリティ要件をまとめたものをいう。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、構築する兵庫県警察情報システムが取り扱う情報、兵庫県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て高度な情報セキュリティ対策を要すると認める兵庫県警察情報システムについては、兵庫県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のうち、上位の情報セキュリティ対策をセキュリティ要件とする必要性について検討すること。

イ　その他

(ｱ)　システムセキュリティ責任者は、兵庫県警察情報システムについてプログラムの開発を行うときは、情報セキュリティを維持するために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、兵庫県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)　兵庫県警察情報システムの調達時及び構築時の対策

ア　システムセキュリティ責任者は、兵庫県警察情報システムの構築時において、情報セキュリティの維持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、兵庫県警察情報システムを新規に構築し、又は更改する場合は、兵庫県警察情報システムの分類基準に基づいて兵庫県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し、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が発生した場合における業務への影響、脅威の動向等を踏まえ、兵庫県警察情報システムの分類の適用について変更することが適当であると認める場合は、システムセキュリティ責任者にその変更の指示を行うこと。

エ　情報セキュリティ管理者は、兵庫県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)　兵庫県警察情報システムの分類基準及び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に確認し、必要に応じて見直しを行うこと。

(ｲ)　全ての兵庫県警察情報システムについて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、構築した兵庫県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維持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兵庫県警察情報システムの

受入れ時の確認又は検査にあっては、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、兵庫県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)　兵庫県警察情報システムの運用時及び保守時の対策

ア　システムセキュリティ責任者は、所管する兵庫県警察情報システムの運用及び保守を行う場合は、当該兵庫県警察情報システムに実装されたセキュリティ機能（監視機能を含む。）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、不正な行為及び意図しない兵庫県警察情報システムへのアクセス等の事象が発生した場合に追跡することができるように、運用及び保守に係る作業についての記録を管理し、運用及び保守によって機器の構成、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について確認し、必要に応じて見直すこと。

ウ　システムセキュリティ責任者は、兵庫県警察情報システムの運用時及び保守時において、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は、情報システム台帳及び情報システム関連文書を更新し、又は修正すること。

エ　システムセキュリティ責任者は、所管する兵庫県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適宜に見直しを行い、必要に応じて適切な対応を行うこと。

オ　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及び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。

カ　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、担当する兵庫県警察情報システムの維持管理を行うこと。

(4)　兵庫県警察情報システムの更改時及び廃棄時の対策

システムセキュリティ責任者は、兵庫県警察情報システムの更改又は廃棄を行う場合は、当該兵庫県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　兵庫県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　兵庫県警察情報システム廃棄時の管理対象情報の抹消

(5)　兵庫県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、所管する兵庫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、情報セキュリティ管理者から示された改善が必要な事項について、適切な措置を講ずること。この場合において、当該措置の結果について、情報セキュリティ管理者に報告すること。

3　兵庫県警察情報システムの業務継続計画の整備及び整合的運用の確保

(1)　システムセキュリティ責任者は、所管する兵庫県警察情報システムについて、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。）の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、可能な限り兵庫県警察情報セキュリティポリシーとの整合を図ること。

(2)　情報セキュリティ管理者は、兵庫県警察情報システムの業務継続計画の教養訓練並びに維持及び改善を行う場合は、危機的事象の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について定期的に確認すること。

第６　兵庫県警察情報システムの構成要素

1　端末等に係る対策

(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、端末において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を認め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、兵庫県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。

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、端末において利用を認めるソフトウェアについて、追加又は継続の適否について定期的に見直しを行うこと。

(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、脆弱性検査等の結果により必要があると認める場合は、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し、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、これを確認し、及び分析すること。

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、兵庫県警察情報システムの更改又は廃棄を行う

場合は、当該兵庫県警察情報システムの端末が運用終了後に再利用された時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、その分類及び取扱制限を考慮した上で、第５の２の(4)に掲げる措置を適切に講ずること。

エ　モバイル端末及び公費で整備された携帯電話機（以下「公費携帯電話機」という。）の導入時及び利用時の対策

(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)　システムセキュリティ責任者は、公費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が漏えいす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、モバイル端末及び公費携帯電話機の導入時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、前記(1)のアに掲げる対策を準用する。

(ｲ)　システムセキュリティ責任者は、障害、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兵庫県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とき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、前記(1)のイに掲げる対策を準用する。

(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、危機的事象の発生時に適切な対処を行うことができるよう運用すること。

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、前記(1)のウの対策を準用する。

(3)　複合機及び特定用途機器

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場合は、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、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　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　電子メール等に係る対策

(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兵庫県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対策を講ずること。

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兵庫県警察情報システムへのウェブサーバ等の導入時及び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、不要な機能を停止し、又は制限すること。

イ　ウェブサーバからの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ウェブコンテンツが公開されることの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漏えい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

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兵庫県警察情報システムへのドメインネームシステムの導入時等に次に掲げる対策を講ずること。

ア　ドメインネームシステムの導入時の対策

(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、兵庫県警察のみで使用する名前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　ドメインネームシステムの運用時の対策

(ｱ)　系統間で同期す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時及び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　電気通信回線等に係る対策

(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について留意した上で必要な検討を行うこと。

(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兵庫県警察情報システムを電気通信回線に接続する場合に、通信内容の秘匿性の確保が必要であると認めるときは、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、次に掲げるａからｃまで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兵庫県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場合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保守又は診断が行われる場合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、兵庫県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場合に、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兵庫県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は、次に掲げる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。

(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兵庫県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、兵庫県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、消去及び改ざんが行われないように管理すること。

(ｲ)　前記１の(1)のイの(ｲ)及び(ｴ)の規定は、電気通信回線の運用時の対策について準用する。この場合において、「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、所管する兵庫県警察情報システムの情報セキュリティの維持が困難な事由が発生した場合は、当該兵庫県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、電気通信回線及び通信要件の変更を行う場合並びに定期的に、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、前記１の(1)の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、前記１の(1)の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、要保護情報を送受信するため、無線ＬＡＮ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、通信内容の漏えい及び改ざんを防止するための措置を講ずること。

４　兵庫県警察情報システムの基盤の管理又は制御をするソフトウェアに係る対策

(1)　兵庫県警察情報システムの基盤の管理又は制御を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兵庫県警察情報シ

ステムの基盤の管理又は制御を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)　兵庫県警察情報システムの基盤の管理又は制御を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)　兵庫県警察情報システムの基盤の管理又は制御を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場合の対処手順

(2)　兵庫県警察情報システムの基盤の管理又は制御を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、兵庫県警察情報システムの基盤の管理又は制御をするソフトウェアを運用し、又は保守する場合は、次に掲げるセキュリティ対策を実施すること。

ア　兵庫県警察情報システムの基盤の管理又は制御を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　脅威及び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・コンテンツに係る対策

(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部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・コンテンツの開発又は作成を業務委託する場合は、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を開発する場合は、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くことがないよう、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、脆弱性が発覚した場合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及びウェブコンテンツにアプリケーション及び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　地方公共団体ドメイン名の使用

(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、公費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、「lg.jp」等の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。

(ｲ)　システムセキュリティ責任者は、部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、職員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　兵庫県警察情報システムのセキュリティ要件

１　兵庫県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、兵庫県警察情報システム及び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は、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、県民及び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兵庫県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、主体認証を行う兵庫県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、兵庫県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、主体が兵庫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、兵庫県警察情報システムの特性、当該兵庫県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、維持管理する兵庫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、主体から兵庫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ときの被害を最小化するための措置並びに内部からの不正操作及び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。

(4)　ログの取得及び管理

ア　システムセキュリティ責任者は、兵庫県警察情報システムにおいて、兵庫県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、兵庫県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、兵庫県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)　暗号及び電子署名

ア　暗号化機能及び電子署名機能の導入

システムセキュリティ責任者は、兵庫県警察情報システムで取り扱う情報の漏えい、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兵庫県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、技術的その他の理由により暗号化が困難であるもの

ｃ　公費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兵庫県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、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」（以下「暗号リスト」という。）に基づき、兵庫県警察情報システムで使用する暗号及び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)　兵庫県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は、やむを得ない場合を除き、暗号リストに記載されたアル

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、適用が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　暗号化及び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兵庫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に安全な方法で提供すること。

(ｲ)　暗号化を行う兵庫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兵庫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安全性の低下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、兵庫県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、兵庫県警察情報システムの運用において、兵庫県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、兵庫県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　兵庫県警察情報システムの設置時又は運用開始時に、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も、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宜に確認すること。

エ　脆弱性情報が、所管する兵庫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兵庫県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兵庫県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、後記ウ及び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を講ずること。

イ　外部回線に接続された兵庫県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、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。

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

情報セキュリティ管理者は、複数の兵庫県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、複数の兵庫県警察情報システム間で横断的な対策の企画、推進及び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は、動的アクセス制御の対象とする兵庫県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に関する事項（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　兵庫県警察情報システム等の利用等

１　兵庫県警察情報システム等の利用時の対策

(1)　兵庫県警察情報システム等の利用時の基本的対策

ア　兵庫県警察情報システム

(ｱ)　職員は、定められた目的以外の目的で兵庫県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、兵庫県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、兵庫県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兵庫県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、ソフトウェアの追加等をいう。）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、兵庫県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は、システムセキュリティ責任者が定めた当該兵庫県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、情報セキュリティ管理者が別途定める場合を除き、機器等を庁舎外に不正に持ち出さないこと。

(ｷ)　職員は、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、兵庫県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場合は、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、兵庫県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、アクセスすることが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。

イ　公費携帯電話機

(ｱ)　職員は、共用で利用する公費携帯電話機（音声通話機能のみを使用するものを

除く。）を庁舎外に持ち出す場合は、媒体利用管理者の許可を受けること。

(ｲ)　職員は、公費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、公費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は、速やかに当該管理対象情報を消去すること。

ウ　外部記録媒体

職員は、外部記録媒体を庁舎外に持ち出す必要がある場合は、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、媒体利用管理者の許可を受けること。

なお、機密性３（高）情報を持ち出す場合は、運用管理者の許可を受けること。

エ　個人所有の機器等

(ｱ)　職員は、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、職員が前記(ｱ)の情報セキュリティ管理者が別途定める場合において、個人所有の機器等において管理対象情報を処理するときは、当該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、前記(ｲ)の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。

(2)　電子メール及び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は、警察が管理及び運用（業務委託による場合を含む。）をする電子メール機能又は公費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、公費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は、電子署名により当該ソフトウェア（電子署名が付与されていないものを除く。）の配布元を確認すること。

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は当該情報を暗号化し、暗号化が困難である場合は主体認証を設定すること。

ケ　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。

コ　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。

サ　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。

(3)　識別コード及び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、兵庫県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。

(4)　暗号及び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。

(5)　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。

(6)　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、情報を発信しようとする場合は、第４の２の(7)のアに定める手続を行うこと。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)　要安定情報の県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、兵庫県

警察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。

第９　その他

この対策基準の細目的事項については、情報セキュリティ管理者が別途定める。