○埼玉県警察情報セキュリティ対策基準

令和５年３月30日

情　管　第　８１１号

警　察　本　部　長

埼玉県警察情報セキュリティ対策基準の制定について（通達）

みだしのことについては、別添のとおり埼玉県警察情報セキュリティ対策基準を制定し、令和５年４月１日から実施するので、運用上誤りのないようにされたい。

なお、警察情報セキュリティ監査実施要領の制定について（平成19年情管第3707号）、警察情報セキュリティの維持に関する例外措置の適用について（平成23年情管第2548号）、警察情報セキュリティ管理要綱の制定について（平成26年情管第795号）、警察情報システム及び管理対象情報の取扱要領の制定について（平成26年情管第796号）、警察情報システムにおける情報セキュリティ要件の制定について（平成26年情管第797号）、警察情報システムに係る機器持ち出し要領の制定について（平成26年情管第798号）、外部記録媒体管理要領の制定について（平成26年情管第799号）及び公用携帯電話機管理要領の制定について（平成31年情管第586号）は、令和５年３月31日限り、廃止する。

別添

埼玉県警察情報セキュリティ対策基準

第１　総則

１　趣旨

この通達は、警察情報セキュリティに関する規程（平成19年埼玉県警察本部訓令第40号。以下「セキュリティ訓令」という。）第３条第２項、第８条第２項、第９条第２項及び第10条の規定に基づき、埼玉県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対策の基準を定めるものとする。

２　管理対象情報の分類及び取扱制限

(1)　管理対象情報の分類

セキュリティ訓令第８条第１項に規定する管理対象情報の分類は、次のとおりとする。

ア　機密性

(ｱ)　機密性３（高）情報　管理対象情報のうち、特定秘密（埼玉県警察における特定秘密の保護に関する規程（平成26年埼玉県警察本部訓令第49号）第１条第１項に定めるものをいう。）又は秘密文書（埼玉県警察文書管理規程（平成14年埼玉県警察本部訓令第25号）第48条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、埼玉県情報公開条例（平成12年埼玉県条例第77号。以下「情報公開条例」という。）第10条各号に規定す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10条各号に規定す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

イ　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、改ざんされ、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）に分類される情報以外のもの

ウ　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）情報に分類される情報以外のもの

(2)　管理対象情報の取扱制限

ア　職員は、管理対象情報の分類に応じて、適正な取扱制限の指定を行わなければならない。

イ　前記アに規定する取扱制限の例は、次のとおりとする。

(ｱ)　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。

(ｲ)　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。

(ｳ)　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。

(ｴ)　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。

(ｵ)　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「所属長限り」等の指定をする。

3　定義

この通達において使用する用語は、セキュリティ訓令において使用する用語の例によるほか、次に掲げる用語の意義は、それぞれ定めるところによる。

(1)　警察情報セキュリティポリシー　セキュリティ訓令及びセキュリティ訓令に基づき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職員（会計年度任用職員及び臨時的任用職員を含む。）をいう。

(3)　要機密情報　機密性３（高）情報又は機密性２（中）情報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）情報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）情報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該当する管理対象情報をいう。

(7)　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。

(8)　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。

(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) 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。）又は運用しているものをいう。

(11) 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。

(12) 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。

(13) 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汎用電子計算機をいう。

(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) 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。

(16) 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（一の機関でハードウェアからアプリケーションまで管理又は運用している情報システムを除く。）をいう。

(17) 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。

(18) 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総務省及び経済産業省が策定した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（以下「ＣＲＹＰＴＲＥＣ暗号リスト」という。）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。

(19) 業務委託　委任、準委任、請負等の契約形態を問わず、警察の一部又は全部の業務（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。）を契約により外部の者に実施させることをいう。

(20) 外部サービス　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（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。）を提供するものをいう。

(21) 外部委託　業務委託及び外部サービスをいう。

(22) 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及び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を経由してアクセスする方法で提供されるサービスであり、かつ、利用者によって自由にリソースの設定及び管理並びに情報セキュリティに係る十分な条件設定が可能であるものをいう。

(23) ウェブ会議サービス　専用のアプリケーション又は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（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除く。）をいう。

(24) 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。

(25) 外部サービス管理者　利用を承認された外部サービスに係る管理を行う者として許可権限者から指名された者をいう。

(26) 外部サービス提供者　外部サービスを提供する事業者（警察に対し外部サービスを利用して独自のサービスを提供する事業者を除く。）をいう。

(27) 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。

(28) 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。

(29) 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。

(30) 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。

(31) 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。

(32) 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。

(33) 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。

(34) 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。

(35) 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。

(36) 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。

(37) 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。

(38) 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。

(39) 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。

(40) 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。

(41) 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。

(42) テレワーク　情報通信技術を活用した、場所及び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勤務公署と異なる警察施設において行う勤務をいう。

(43) モバイル勤務　情報通信技術を活用した、場所及び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及び出先で業務を行うことをいう。

第２　情報セキュリティ対策の基本事項

１　体制の整備

(1)　情報セキュリティ管理者

情報セキュリティ管理者は、セキュリティ訓令第４条第２項に定める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（(3)に規定する者をいう。）及びシステムセキュリティ維持管理者（(4)に規定する者をいう。）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)　区域情報セキュリティ管理者

ア　情報セキュリティ管理者は、それぞれ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、区域情報セキュリティ管理者の指名等については、別に定める。

(3)　システムセキュリティ責任者

ア　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、当該所属の長をもって充てる。

イ　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に必要な事務を処理するものとする。

(4)　システムセキュリティ維持管理者

ア　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、当該所属の長をもって充てる。

イ　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に必要な事務を処理するものとする。

(5)　埼玉県警察ＣＳＩＲＴ

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、埼玉県警察本部に、埼玉県警察ＣＳＩＲＴを置く。

イ　埼玉県警察ＣＳＩＲＴの長（以下「ＣＳＩＲＴ長」という。）は総務部情報管理課長（以下「情報管理課長」という。）をもって充てる。

ウ　埼玉県警察ＣＳＩＲＴの運営に関し必要な事項は、別に定める。

(6)　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、次の役割を兼務してはならない。

(ｱ)　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。）

(ｲ)　セキュリティ訓令第９条に規定する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に関する監査（以下「情報セキュリティ監査」という。）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、又は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。

(7)　分庁舎等における事務

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及びシステムセキュリティ維持管理者は、それぞれの事務のうち分庁舎等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、当該分庁舎等に勤務する警視以上の階級の警察官又はこれと同等の職にある一般職員を指名した上で担当させることができる。

２　情報セキュリティ委員会

(1)　構成

ア　セキュリティ訓令第３条に規定する情報セキュリティ委員会（以下「委員会」という。）は、委員長、副委員長及び委員をもって構成する。

イ　委員長は警察本部長（以下「本部長」という。）、副委員長は総務部長をもって充てる。

ウ　委員は、警務部長、生活安全部長、地域部長、刑事部長、交通部長、警備部長、さいたま市警察部長、警察学校長及び各方面本部長並びに関東管区警察局埼玉県情報通

信部長をもって構成する。

(2)　任務

委員会の任務は、次に掲げる事項の審議を任務とする。

ア　管理対象情報の分類及び対策の基準

イ　遵守事項に対する例外措置の適用の申請を審査するための手続

ウ　前記ア及びイに定める事項の見直しを行う必要性の有無

エ　情報セキュリティ管理者が作成した年度ごとの情報セキュリティ監査の実施計画

オ　情報セキュリティ監査の結果（以下「監査結果」という。）に基づく対策

カ　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が侵害された場合の再発防止対策

キ　その他警察における情報セキュリティに関する事項で、委員長が重要と認めるもの

(3)　専門部会

ア　委員会に、委員長から付託された警察情報システムに係る情報セキュリティに関する事項を調査し、又は審議するため、情報セキュリティ専門部会（以下「専門部会」という。）を置く。

イ　専門部会は、部会長、副部会長及び部会員をもって構成する。

ウ　部会長は総務部長、副部会長は情報管理課長をもって充てる。

エ　部会員は、総務部総務課長、同部財務局会計課長、警務部警務課長、生活安全部生活安全総務課長、地域部地域総務課長、刑事部刑事総務課長、交通部交通総務課長及び警備部公安第一課長並びに第一方面本部副本部長並びに警察学校副校長並びに総務部情報管理課情報セキュリティ対策室長及び警務部警務課企画調整室長並びに関東管区警察局埼玉県情報通信部通信庶務課長をもって構成する。

オ　部会長は、専門部会の調査又は審議状況を委員会に報告するものとする。

(4)　分科会

ア　専門部会に、特定の事項を調査し、又は研究するため、情報セキュリティ分科会（以下「分科会」という。）を置く。

イ　分科会に分科会長を置き、情報管理課長をもって充てる。

ウ　分科会は、分科会長が指定する者をもって組織する。

(5)　運営

ア　委員会、専門部会及び分科会の会議は、各会の長が必要に応じて招集し、議事を主宰する。

イ　各会の長は、必要があると認めるときは、定められた構成員以外の者に対し各会への出席を求めることができる。

ウ　前記ア及びイに規定するもののほか、委員会、専門部会及び分科会の運営に関し必要な事項は、各会の長が定める。

(6)　庶務

委員会、専門部会及び分科会の庶務は、総務部情報管理課において処理する。

3　運用

(1)　情報セキュリティ対策

ア　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には、速やかに警察庁情報セキュリティ管理者（警察庁長官官房技術企画課長）に報告すること。

イ　職員は、警察情報セキュリティポリシー又は第５の１(2)アに規定する運用要領に違反する行為を認知したときは、運用管理者を経て、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。

ウ　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又は第５の１(2)アに規定する運用要領への重大な違反を認知した場合は、情報管理課長を経て、情報セキュリティ管理者に報告するとともに、違反者及び関係者等に情報セキュリティの維持に必要な措置を講じさせなければならない。

(2)　例外措置

ア　趣旨

警察情報セキュリティポリシーで定められた情報セキュリティの維持に関する事項（以下この(2)において「情報セキュリティ維持事項」という。）を遵守することが困難であり、かつ合理的理由がある場合は、イ及びウに定めるところにより、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。

なお、例外措置の適用に際しては、情報セキュリティ維持事項の趣旨に鑑み、可能な限り代替の措置を講じるものとする。

イ　例外措置の適用の申請

(ｱ)　システムセキュリティ責任者又は運用管理者は、情報セキュリティ維持事項について履行することが困難な場合において、業務を推進するために必要と認めるときは、情報管理課長を経て情報セキュリティ管理者に例外措置の適用を申請しなければならない。

(ｲ)　緊急を要する場合は、システムセキュリティ責任者又は運用管理者の許可を受けることで例外措置の適用を受けたものとみなす。この場合において、例外措置を適用した後、速やかに情報セキュリティ管理者に申請すること。

(ｳ)　例外措置の適用期間は、１年以内の範囲で定めること。ただし、申請の対象となる警察情報システムの整備目的を踏まえ情報セキュリティ管理者が特に認めた場合は、１年を超える期間とすることができる。

(ｴ)　情報セキュリティ管理者は、前記(ｱ)の申請内容を審査し、情報セキュリティ上の影響と対処方法を検討の上、許可の可否を決定し、システムセキュリティ責任者又は運用管理者に対し通知するものとする。

(ｵ)　当該申請に係る手続等については、別に定める。

ウ　緊急事態等への対応等

(ｱ)　職員は、大規模災害、重大テロ等（以下このウにおいて「緊急事態等」という。）において、本通達の規定によることが困難なときは、運用管理者等の指示により、これらの規定によ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、緊急事態等において、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、所要の措置を講じること。

エ　その他

システムセキュリティ責任者は、特定の警察情報システムについて、第６に規定する情報セキュリティ要件を適用することが困難であると認めたときは、情報セキュリティ管理者と協議の上、当該警察情報システムの情報セキュリティ要件について、別に定めるために必要な措置をとるものとする。

(3)　教養の実施

ア　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。

イ　情報セキュリティ管理者は、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。

ウ　職員は、別に定める教養実施計画に従って、適切な時期に教養を受講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、業務の責務に即した必要な範囲において管理権限を付与したシステム管理担当者（第６の１(3)エに規定する者をいう。）及びネットワーク管理担当者（第６の１(3)キに規定する者をいう。）に対して、規範意識等の醸成及びセキュリティ機能の利用方法等に係る教養を実施しなければならない。

(4)　情報セキュリティインシデントへの対処

ア　事案発生時の措置

(ｱ)　職員は、情報セキュリティインシデントの可能性がある事案を認知したときは、運用管理者に速やかに報告しなければならない。

(ｲ)　運用管理者は、前記(ｱ)の事案を認知したときは、システムセキュリティ責任者及びＣＳＩＲＴ長に速やかに報告しなければならない。

(ｳ)　ＣＳＩＲＴ長は、前記(ｲ)により報告された事案について、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ものとする。

(ｴ)　ＣＳＩＲＴ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、遅滞なく情報セキュリティ管理者に報告しなければならない。

(ｵ)　ＣＳＩＲＴ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、埼玉県警察ＣＳＩＲＴ、情報セキュリテインシデントが発生した所属その他関連所属の役割分担を調整するものとする。

(ｶ)　ＣＳＩＲＴ長は、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運用管理者に対し、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ものとする。

(ｷ)　情報セキュリティ管理者及び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、別に定める対処手順及びＣＳＩＲＴ長からの指示又は助言に従って、適切に対処しなければならな

い。

(ｸ)　情報セキュリティ管理者及び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際に、当該事案が「政府共通プラットフォーム」等の基盤となる情報システムに関するものであり、当該基盤となる情報システムの情報セキュリティ対策に係る運用管理規定等が定められている場合は、その規定に従い、適切に対処しなければならない。

(ｹ)　ＣＳＩＲＴ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、必要な事項を記録しておかなければならない。

(ｺ)　埼玉県警察ＣＳＩＲＴによる情報セキュリティインシデントへの対処状況を検証するため、ＣＳＩＲＴ長は、委員会に活動状況を報告しなければならない。

イ　警察庁ＣＳＩＲＴ等への報告

ＣＳＩＲＴ長は、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、次に掲げるものは、警察庁ＣＳＩＲＴの長及び関東管区警察局情報通信部情報技術解析課長に速やかに報告しなければならない。

(ｱ)　情報流出事案

管理対象情報の流出事案

(ｲ)　重大障害事案

警察情報管理システム等（警察情報管理システム等運用管理規程（平成23年埼玉県警察本部訓令第32号）第２条第１号に定めるものをいう。ただし、警察庁が整備する情報システムと接続しているものに限る。）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

(ｳ)　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

ａ　警察情報システムにおける不正プログラム感染事案

ｂ　警察情報システムに対する不正アクセス事案

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

(ｴ)　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警察情報システムを不正に使用した事案

(ｵ)　個人所有の機器の不正使用事案

a　管理対象情報を、個人所有の機器において不正に処理した事案

b　個人所有の機器を警察情報システムに不正に接続した事案

(ｶ)　外部委託先等における情報流出事案

a　警察情報システムに係る外部委託先における事案

b　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、重大なインシデントに当たる可能性のある事案

d　その他の外部委託について、重大なインシデントに当たると認められない事案

(ｷ)　その他社会的反響が大きいと予想される事案

前記(ｱ)から(ｶ)までに掲げるもののほか、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、報道されるなど社会的反響が大きいと予想されるもの

ウ　連絡及び訓練体制

(ｱ)　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の発生に備え、業務の遂行のために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。

(ｲ)　情報セキュリティ管理者は、業務の遂行のために特に重要と認めた警察情報システムについて、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、訓練内容及び体制を整備しなければならない。

エ　再発防止

情報セキュリティ管理者は、警察庁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、これを踏まえ、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、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。

オ　情報共有

ＣＳＩＲＴ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、関係所属と情報の共有を図らなければならない。

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ものについても、注意喚

起等が必要と認められるときには、関係する者に情報共有を図るものとする。

4　自己点検

(1)　自己点検の実施

ア　情報セキュリティ管理者は、自己点検実施計画を策定し、職員に自己点検を実施させなければならない。

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の発生状況等を踏まえ、適宜、自己点検実施計画を見直すものとする。

(2)　自己点検結果の評価

情報セキュリティ管理者は、前記(1)アで実施した自己点検の結果を評価し、明らかになった問題点について所要の措置を講じるものとする。

5　情報セキュリティ監査

(1)　情報セキュリティ監査の種類

情報セキュリティ監査の種類は、通常監査及び特別監査とする。

(2)　通常監査

ア　実施計画

情報セキュリティ管理者は、年度ごとに実施計画を定め、本部長の承認を得るものとする。

イ　実施の通知

情報セキュリティ管理者は、実施日、実施要領その他必要事項について、通常監査を受ける所属の長に通知するものとする。

ウ　監査官の指名等

(ｱ)　情報セキュリティ管理者は、通常監査の実施に当たっては、警察本部所属の課長補佐級以上の職にある者の中から、監査官を指名するものとする。

(ｲ)　監査官に係る細目事項等については、別に定める。

エ　情報セキュリティ監査の実施

監査官は、通常監査を実施するに当たっては、次に掲げる事項に留意しなければならない。

(ｱ)　取り扱う情報の保秘を徹底すること。

(ｲ)　厳正かつ公平を旨とすること。

(ｳ)　資料及び情報を十分に収集し、正確な事実の把握に努めること。

(ｴ)　必要な限度を超えて関係者の職務に支障を及ぼさないよう注意すること。

オ　実施結果の報告及び通知

(ｱ)　監査官は、通常監査の実施結果を取りまとめ、総合的に点検した上で評価し、情報セキュリティ管理者に報告しなければならない。

(ｲ)　情報セキュリティ管理者は、実施結果に基づき、改善を求める事項その他必要と認める事項について、情報セキュリティ監査を受けた所属の長に通知するものとする。

(ｳ)　情報セキュリティ管理者は、情報セキュリティ監査を受けた所属以外の所属においても共通の改善を必要とする課題若しくは問題点がある可能性が高い、又は緊急に課題若しくは問題点があることを確認する必要があると判断した場合は、情報セキュリティ監査を受けた所属以外の所属の長に対し、課題又は問題点の有無を確認するよう通知するものとする。

(ｴ)　情報セキュリティ監査を受けた所属の長は、前記(ｲ)の通知に改善事項があった場合は、速やかに必要な措置を講じるものとする。

なお、速やかな措置が困難な事項については、その影響を低減させるための補完的な措置を検討した上で改善計画を策定し、措置結果又は改善計画を情報セキュリティ管理者に報告しなければならない。

(ｵ)　前記(ｳ)の通知を受けた所属の長は、当該通知の内容を踏まえ、速やかに必要な措置をとり、その措置結果を情報セキュリティ管理者に報告するものとする。

(3)　特別監査

ア　実施

情報セキュリティ管理者は、特に必要があると認める場合は、特別監査の対象となる所属、監査項目及び実施要領を定め、本部長の承認を得て特別監査を実施するものとする。

イ　通常監査に関する規定の準用

特別監査については、前記(2)ウからオまでの規定を準用する。

6　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監査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。

第３　管理対象情報の取扱い

管理対象情報の取扱いについては、個人情報の保護に関する法律（平成15年法律第57号）、埼玉県警察文書管理規程（平成14年埼玉県警察本部訓令第25号）等別の定めによる適正な管理を行うほか、次に定めるところにより行うものとする。

１　管理対象情報の目的外での利用等の禁止

職員は、担当する業務の遂行のために必要な範囲を超えて、警察情報システム及び管理対象情報を取り扱ってはならない。

２　管理対象情報の分類及び取扱制限の決定、明示等

(1)　職員は、管理対象情報を作成し、又は職員以外の者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なければならない。

(2)　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情報公開条例第10条各号に規定す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であるときを除き、上職者（警察本部の課長補佐（室長補佐、隊長補佐及び科長を含む。）、さいたま市警察部及び各方面本部の補佐官、警察学校の校長補佐若しくは警察署の課長（課長代理及び課長を置かない場合の係長を含む。）以上の職にある職員又は埼玉県警察処務規程（昭和38年埼玉県警察本部訓令第12号。以下「処務規程」という。）第32条に規定する総括管理者をいう。）の承認を得なければならない。

(3)　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しなければならない。

(4)　職員は、職員以外の者に管理対象情報を提供する場合は、別に定めるものを除き、管理対象情報の機密性の分類及び取扱制限を明示しなければならない。

(5)　職員は、管理対象情報を作成し、又は複製する場合で、参照した管理対象情報又は入手した管理対象情報に分類及び取扱制限の決定が既になされているときは、元となる管理対象情報の機密性に係る分類及び取扱制限を継承しなければならない。

(6)　職員は、管理対象情報の修正、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、当該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さなければならない。

3　管理対象情報の利用及び保存

(1)　職員は、管理対象情報を取り扱う場合は、次に掲げる事項を遵守しなければならない。

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。

(2)　職員は、別に定める場合を除き、警察庁舎外に設置されている機器に要機密情報を保存してはならない。

(3)　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しなければならない。

(4)　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警察情報システムを除き、外部回線に接続する警察情報システムにおいて、要機密情報を取り扱ってはならない。

(5)　職員は、警察が維持管理を行っていない機器に機密性３（高）情報を保存してはならない。

4　管理対象情報の提供及び公表

(1)　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）情報に分類されることを確認しなければならない。

(2)　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には、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じなければならない。

(3)　職員は、管理対象情報を職員以外の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しなければならない。

5　管理対象情報の持ち出し

(1)　職員は、要保護情報が記録され、又は記載された記録媒体の警察庁舎外への運搬を第三者に依頼する場合は、管理対象情報の分類及び取扱制限に応じて、適切な措置を講じなければならない。

(2)　職員（所属長以上の者を除く。）は、要機密情報について、警察庁舎外への持ち出し

を行う場合は、前記２(6)に規定する当該情報の分類及び取扱制限の見直しを行った上で、別に定める事項を遵守しなければならない。

(3)　職員は、機密性２（中）情報を外部回線を用いた電子メールにより送信する場合は、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、適切な措置を講じなければならない。

(4)　職員は、機密性３（高）情報を外部回線を用いた電子メールで送信してはならない。

6　管理対象情報の消去

(1)　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しなければならない。

(2)　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しなければならない。

なお、端末、サーバ等をリース契約で調達する場合は、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、必要な対策を講じなければならない。

(3)　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しなければならない。

7　管理対象情報のバックアップ

(1)　職員は、要保全情報又は要安定情報を持ち出すときは、運用管理者の許可を得るとともに、必要に応じてバックアップを取得しなければならない。

(2)　職員は、取得した管理対象情報のバックアップについて、前記２(5)の規定に基づき管理対象情報の機密性に係る分類及び取扱制限に従って、適切に管理しなければならない。

8　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

情報セキュリティ管理者は、前記第２の１(2)アの規定に基づき分類した区域について、各区域の特性に応じた対策の基準を定めるものとする。

(2)　区域ごとの対策の決定

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確保のための管理対策を講じなければならない。

(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しなければならない。

また、職員が行うべき対策については、職員が認識できる措置を講じなければならない。

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じなければならない。

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しなければならない。

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するよう求めなければならない。

第４　外部委託

１　業務委託

(1)　業務委託に係る契約

ア　システムセキュリティ責任者は、次に掲げる事項を例として、情報セキュリティ対策の実施を委託先の選定条件とし、仕様書等に盛り込まなければならない。

(ｱ)　委託先に提供する管理対象情報の委託先における目的外利用の禁止

(ｲ)　委託先における情報セキュリティ対策の実施内容及び管理体制

(ｳ)　委託事業の実施に当たり、委託先事業者若しくはその従業員、再委託先又はその他の者による意図しない変更が加えられないための管理体制

(ｴ)　委託先の資本関係並びに役員等の情報、委託事業の実施場所、委託事業従事者の所属、専門性（情報セキュリティに係る資格、研修実績等）、実績及び国籍に関する情報提供

(ｵ)　情報セキュリティインシデントへの対処方法

(ｶ)　情報セキュリティ対策その他の契約の履行状況の確認方法

(ｷ)　情報セキュリティ対策の履行が不十分な場合の対処方法

イ　システムセキュリティ責任者は、委託する業務において取り扱う管理対象情報の分類等を勘案し、必要に応じて次に掲げる事項を仕様書等に記載しなければならない。

(ｱ)　情報セキュリティ監査の受入れ

(ｲ)　サービスレベルの保証

ウ　システムセキュリティ責任者は、外部委託によって情報セキュリティが損なわれることのないよう、十分に検討の上、委託先には事業継続性を有すると認められる事業者を選定しなければならない。

エ　システムセキュリティ責任者は、委託先がその役務内容を一部再委託する場合は、再委託されることで生じる脅威に対して情報セキュリティが十分に確保されるよう、前記アからウまでの措置の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を委託先に報告させるなどにより、適切に対策が実施されているかどうか確認するために必要な情報をシステムセキュリティ責任者に提供し、システムセキュリティ責任者の承認を受けるよう、仕様書等に記載しなければならない。

オ　システムセキュリティ責任者は、委託先によるアクセスを認める情報及び情報システムの範囲を適切に判断しなければならない。

カ　システムセキュリティ責任者は、あらかじめ当該委託に係る作業を監督する職員の任務を定めるとともに、情報セキュリティの観点から委託先に遵守させるべき事項を仕様書等に盛り込まなければならない。

(2)　業務委託における情報の取扱い

ア　職員は、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しなければならない。

イ　職員は、提供した要保護情報が委託先において不要になった場合は、これを確実に返却又は抹消させなければならない。

ウ　職員は、委託した業務において、情報セキュリティインシデント、情報の目的外利用等を認知した場合は、速やかにシステムセキュリティ責任者又は運用管理者に報告しなければならない。

(3)　業務委託における対策の実施

ア　システムセキュリティ責任者は、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認しなければならない。

イ　システムセキュリティ責任者は、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職員から受けた場合は、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なければならない。

ウ　システムセキュリティ責任者は、委託した業務の終了時に、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され、又は抹消されたことを確認しなければならない。

2　外部サービス

(1)　要機密情報を取り扱う外部サービス

ア　クラウドサービスの選定

(ｱ)　システムセキュリティ責任者又は運用管理者は、利用するクラウドサービスを選定するに当たっては、次に掲げる事項に従ってクラウドサービスを選定しなければならない。

a　取り扱う管理対象情報の分類及び取扱制限を踏まえ、別に定める利用判断基準を利用条件としてクラウドサービスの利用を検討し、利用する場合は、必要な手続をとること。

なお、利用の検討に当たっては、リスク及びその低減措置を考慮すること。

b　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を踏まえ、別に定める外部サービス提供者の選定基準に従って選定するとともに、業務に特有のリスクが存在する場合は、必要な情報セキュリティ対策を外部サービス提供者の選定条件に含めること。

c　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て情報セキュリティ要件を定めること。

(ｲ)　クラウドサービスの選定については、前記1(1)ウの規定を準用する。この場合において、「システムセキュリティ責任者」とあるのは「システムセキュリティ責任者又は運用管理者」と読み替えるものとする。

(ｳ)　システムセキュリティ責任者又は運用管理者は、情報を取り扱う場所並びに契約に定める準拠法及び裁判管轄を国内に指定しなければならない。この場合において、情報の開示が懸念される場合は、警察が管理する暗号鍵で情報を暗号化するなどの措置を検討しなければならない。

(ｴ)　職員は、情報セキュリティ管理者が認めた場合を除き、クラウドサービスで機密

性３（高）情報を取り扱ってはならない。

(ｵ)　システムセキュリティ責任者又は運用管理者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることで生じる脅威に対して情報セキュリティが十分に確保されるよう、次に掲げる事項に留意しなければならない。

ａ　外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させること。

ｂ　再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報をシステムセキュリティ責任者に提供して承認を受けることを、外部サービス提供者の選定条件に含めること。

ｃ　外部サービスの利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断すること。

イ　クラウドサービス以外の外部サービスの選定

(ｱ)　システムセキュリティ責任者又は運用管理者は、取り扱う管理対象情報の分類及び取扱制限を踏まえ、別に定める利用判断基準を利用条件として、クラウドサービス以外の外部サービス（以下この２において「その他の外部サービス」という。）の利用を検討し、利用する場合は、必要な手続をとること。

(ｲ)　システムセキュリティ責任者又は運用管理者は、その他の外部サービスで取り扱う管理対象情報の分類及び取扱制限を踏まえ、別に定める外部サービス提供者の選定基準に従い外部サービス提供者を選定しなければならない。

(ｳ)　システムセキュリティ責任者又は運用管理者は、その他の外部サービスの中断又は終了時に円滑に業務を移行するための対策を検討の上、外部サービス提供者を選定しなければならない。

(ｴ)　その他の外部サービスの選定については、前記１(1)ウ並びに２(1)ア(ｳ)及び(ｵ)の規定を準用する。この場合において、前記１(1)ウの「システムセキュリティ責任者」とあるのは「システムセキュリティ責任者又は運用管理者」と読み替えるものとする。

(ｵ)　システムセキュリティ責任者又は運用管理者は、取り扱う管理対象情報の分類及び取扱制限に応じて情報セキュリティに係る国際規格等と同等以上の水準となる情報セキュリティ要件を定め、その他の外部サービスを選定しなければならない。

(ｶ)　システムセキュリティ責任者又は運用管理者は、その他の外部サービスの情報セキュリティ要件を定めるに当たっては、その他の外部サービスの特性を考慮するとともに、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た上で、その他の外部サービスが提供する部分を含む流通経路全般で情報セキュリティが適切に確保されるようにしなければならない。

(ｷ)　システムセキュリティ責任者又は運用管理者は、その他の外部サービスに対する情報セキュリティ監査による報告書の内容、各種認定又は認証制度の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的かつ客観的に評価した上で、利用の可否を判断しなければならない。

ウ　外部サービスの利用に係る調達及び契約

(ｱ)　システムセキュリティ責任者又は運用管理者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めた情報セキュリティ要件を仕様書に記載しなければならない。

(ｲ)　システムセキュリティ責任者又は運用管理者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが仕様書の内容を満たすことを契約までに確認し、当該仕様書の内容を契約に含めなければならない。

(ｳ)　外部サービスの利用に係る調達及び契約については、前記１(2)及び(3)の規定を準用する。この場合において、「システムセキュリティ責任者は」とあるのは「システムセキュリティ責任者又は運用管理者は」と読み替えるものとする。

エ　外部サービスの利用承認

(ｱ)　外部サービスの利用申請の許可権限者は次のとおりとする。

ａ　クラウドサービス

情報セキュリティ管理者（警察庁が整備した情報システム又は警察庁が整備する情報システムと接続された情報システムについては、警察庁情報セキュリティ管理者）

ｂ　その他の外部サービス

情報セキュリティ管理者

(ｲ)　システムセキュリティ責任者又は運用管理者は、外部サービスを利用する場合は、利用申請の許可権限者に外部サービスの利用申請を行わなければならない。

(ｳ)　利用申請の許可権限者は、職員による外部サービスの利用申請を審査し、利用の可否を決定しなければならない。

(ｴ)　許可権限者は、前記(ｳ)の審査で利用を承認したときは、当該外部サービスについて記録し、申請者を外部サービス管理者として指名しなければならない。

オ　外部サービスを利用した警察情報システムの導入及び構築時の対策

(ｱ)　システムセキュリティ責任者又は運用管理者は、外部サービスを利用して警察情報システムを構築する場合は、外部サービスの特性、責任分界点等を踏まえ、次に掲げる事項を遵守しなければならない。

ａ　不正なアクセスを防止するためのアクセス制御を行うこと。

ｂ　取り扱う情報の機密性を保護するための暗号化を行うこと。

ｃ　開発時における情報セキュリティ対策を講じること。

ｄ　設計及び設定時における誤りを防止すること。

(ｲ)　システムセキュリティ責任者又は運用管理者は、前記(ｱ)に掲げる事項について対応したときは、その実施状況を確認し、記録しておかなければならない。

(ｳ)　外部サービスを利用した警察情報システムの導入又は構築時の対策については、前記１(1)オ及びカの規定を準用する。

カ　外部サービスを利用した警察情報システムの運用及び保守時の対策

(ｱ)　外部サービス管理者は、外部サービスを利用した情報システムの運用又は保守に際し、必要な対策を講じなければならない。

(ｲ)　外部サービス管理者は、外部サービスで情報セキュリティインシデントを認知した場合は、前記第２の３(4)ア(ｱ)、(ｲ)、(ｷ)及び(ｸ)の規定に基づき、適切に対処しなければならない。

(ｳ)　外部サービス管理者は、前記(ｱ)及び(ｲ)に定める事項について、運用又は保守時にその実施状況を定期的に確認し、記録しておかなければばらない。

キ　外部サービスを利用した警察情報システムの更改及び廃棄時の対策

(ｱ)　外部サービス管理者は、外部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、必要な対策を講じなければならない。

(ｲ)　外部サービス管理者は、前記(ｱ)に定める事項について、外部サービスの利用終了時に実施状況を確認し、記録しておかなければならない。

(2)　要機密情報を取り扱わない外部サービス

ア　職員は、要機密情報を取り扱わない外部サービスを利用する場合は、サービスの約款、提供条件等から、利用に当たってのリスクが許容できる範囲であることを確認しなければならない。

イ　職員は、要機密情報を取り扱わない外部サービスを利用する場合は、必要な手続をとるとともに、承認時に指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講じなければならない。ただし、ウに定める場合又は検索サービス等のその他の外部サービスによりインターネット上に掲出された情報を閲覧する場合（アカウントの取得を必要としない場合に限る。）は、この限りでない。

ウ　職員は、検索サービス等のその他の外部サービスによりインターネット上に掲出された情報を閲覧する場合（アカウントの取得を必要とする場合に限る。）は、取り扱う管理対象情報をアカウントの登録に必要な情報に限定した上で、運用管理者の許可を得なければならない。

エ　職員は、前記イ及びウにおける情報の閲覧の場合であっても、検索する情報が当該外部サービスの提供側において収集及び分析され関心事項が把握される可能性があることに留意しなければならない。

オ　要機密情報を取り扱わない外部サービスの利用については、それぞれ次の規定を準用する。

(ｱ)　クラウドサービスを利用する場合

前記１及び２(1)エ

(ｲ)　その他の外部サービスを利用する場合

前記１(1)オ及びカ並びに２(1)エ

第５　警察情報システムのライフサイクル

１　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

情報セキュリティ管理者は、埼玉県警察が整備した全ての情報システムについて、別に定める情報システム台帳を整備しなければならない。

(2)　情報システム関連文書の整備等

ア　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を主管する所属の長と連携し、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と情報セキュリティ管理者の確認を受けた上で、当該警察情報システムの運用要領等（以下「運用要領」という。）を制定するために必要な措置をとらなければならない。

イ　運用要領には、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ものとする。

(ｱ)　取り扱うことが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)　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)　新たな機器の接続、ソフトウェアの追加等職員が独自の判断で行うことのできる改造の範囲

(ｴ)　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

ウ　システムセキュリティ責任者は、前記ア及びイのほか、別に定める情報システム関連文書の整備等をしなければならない。

2　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)　警察情報システムの企画及び要件定義

ア　実施体制の確保

(ｱ)　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を確保するように努めなければならない。

(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管理規程等で求められる事務を処理するものとする。

イ　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、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及び取扱制限、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。

(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、標的型攻撃をはじ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しなければならない。

(ｳ)　システムセキュリティ責任者は、経済産業省が公開するＩＴ製品の調達におけるセキュリティ要件リストを参照し、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情報セキュリティ要件を策定しなければならない。

(ｴ)　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に、基盤となる情報システムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリティ要件を適切に策定しなければならない。

ウ　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、警察情報システムの構築を業務委託する場合は、次に掲げる事項を仕様書に記載するなどして、委託先に適切に実施させなければならない。

(ｱ)　警察情報システムのセキュリティ要件を適切に実装すること。

(ｲ)　警察情報セキュリティの観点に基づく試験を実施すること。

(ｳ)　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を講じること。

(ｴ)　前記イ(ｱ)並びに(2)イ(ｲ)、(4)ア及び第６の２(1)アに定める事項

エ　警察情報システムの運用及び保守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、警察情報システムの運用又は保守を業務委託する場合は、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、委託先が適切に実施するよう仕様書に記載するなどしなければならない。

また、委託先が実施する情報セキュリティ対策によって当該警察情報システムの内容に変更が生じるときは、速やかに報告するよう求めること。

オ　その他留意事項

(ｱ)　システムセキュリティ責任者は、警察情報システムについてプログラム開発を行うときは、情報セキュリティを維持するために必要な対策を講じなければならない。

(ｲ)　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)　警察情報システムの調達及び構築

ア　機器等の選定時の対策

システムセキュリティ責任者は、機器等の選定に当たっては、次に掲げる事項に配意するものとする。

(ｱ)　機器の選定に当たっては、当該機器及び当該機器の製造者に係る情報の入手に努めること。

(ｲ)　前記(ｱ)で入手した情報等を基に、情報セキュリティの確保に必要な機能及び信頼性を有する機器を選定すること。

(ｳ)　委託先の選定に当たっては、「ＩＴ調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」（平成30年12月10日関係省庁申合せ）に係る所要の措置を講じること。

(ｴ)　機器の選定に当たっては、警察情報システムのセキュリティ要件の適切な実装ができること。

(ｵ)　前記(ｱ)から(ｴ)までのほか、別に定める対策を講じること。

イ　警察情報システムの構築時の対策

(ｱ)　システムセキュリティ責任者は、警察情報システムの構築において、情報セキュリティの観点から必要な措置を講じなければならない。

(ｲ)　システムセキュリティ責任者は、警察情報システムの運用開始の手順及び環境を定めるに当たっては、情報セキュリティを損なうことのないよう留意するとともに、必要に応じて試験を実施すること。

ウ　納品検査時の対策

(ｱ)　システムセキュリティ責任者は、警察情報システムを構築する機器の調達に当たっては、必要に応じて機器の納入時に検査等を実施すること。

(ｲ)　システムセキュリティ責任者は、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ついて、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しなければならない。

(3)　警察情報システムの運用及び保守

ア　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。

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により、基盤となる情報システムの運用管理規程等に従って、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。

ウ　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こと。この場合において、不正な通信等を認知したときは、速やかに必要な対応を行わなければならない。

エ　システムセキュリティ維持管理者は、情報システムの構成又は情報の処理手順を変更するなどの維持管理作業等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かなければならない。

オ　システムセキュリティ維持管理者は、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。

(4)　警察情報システムの更改又は廃棄

システムセキュリティ責任者は、警察情報システムの更改又は廃棄を行う場合は、保存されている管理対象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じなければならない。

ア　警察情報システムを移行する際は、管理対象情報の移行作業において情報セキュリティ対策をとること。

イ　警察情報システムを廃棄する際は、不要な管理対象情報を抹消すること。

(5)　対策の見直し

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ときは、必要な措置を講じなければならない。

3　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)　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。

(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について、非常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。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。

(3)　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を行うときなどに、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検討しなければならない。

第6　警察情報システムの情報セキュリティ要件

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について、必要に応じてシステムセキュリティ維持管理者等に指示するなどして、次に定める技術的要件を満たさなければならない。

1　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、ログイン時に主体認証を行う機能を設けなければならない。

(ｲ)　システムセキュリティ責任者は、国民又は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しなければならない。

(ｳ)　システムセキュリティ責任者は、主体認証を行う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じなければならない。

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、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じなければならない。

(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じなければならない。

(2)　アクセス制御機能

ア　システムセキュリティ責任者は、警察情報システムの特性、当該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、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。

(3)　権限の管理

ア　システムセキュリティ責任者は、主体からの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。

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ときは、主体の識別コード及び主体認証情報が、第三者等に窃取された際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じなければならない。

ウ　システムセキュリティ維持管理者は、管理者権限を適正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、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。

オ　前記エ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た上で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ついては、この限りでない。

カ　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。

キ　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。

ク　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。

(4)　証跡の取得及び管理

ア　システムセキュリティ責任者は、警察情報システムにおいて、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、証跡を取得し、保管する機能を設けなければならない。

イ　システムセキュリティ責任者は、警察情報システムにおいて、その特性に応じて証跡を取得する目的を設定した上で、証跡を取得する対象の機器、証跡として取得する情報項目、証跡の保存期間等について、適切に証跡を管理しなければならない。

ウ　システムセキュリティ責任者は、警察情報システムにおいて、取得した証跡を定期的に点検又は分析をする機能を設けなければならない。

エ　システムセキュリティ責任者は、警察情報システムに対する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、前記ウの機能を用いて定期的に点検又は分析をしなければならない。

(5)　暗号及び電子署名

ア　暗号化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、警察情報システムで取り扱う情報の漏えい、改ざん等を防止するため、次に掲げる措置を講じること。

(ｱ)　管理対象情報を取り扱う警察情報システムについては、暗号化機能を設けなければならない。ただし、次に掲げるものは、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、技術的に又は運用上暗号化が困難であるもの

ｃ　公費により購入し配分された携帯電話機（以下「公用携帯電話機」という。）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ことの必要性を検討し、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については、情報セキュリティ管理者（警察庁が整備した情報システム又は警察庁の情報システムと接続された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）の許可を受けた場合を除き、ＣＲＹＰＴＲＥＣ暗号リストに掲げたものを使用しなければならない。

(ｴ)　警察情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合は、やむを得ないときを除き、ＣＲＹＰＴＲＥＣ暗号リストに記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用しなければならない。

(ｵ)　暗号化及び電子署名に使用する暗号アルゴリズムが危殆化した場合、又はそれを利用したプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めなければならない。

(ｶ)　暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定めなければならない。

(ｷ)　電子署名の目的に合致し、かつ、適用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しなければならない。

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、暗号化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じなければならない。

(ｱ)　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、署名検証者に安全な方法で提供しなければならない。

(ｲ)　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。

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じなければならない。

ア　警察情報システムの設置又は運用開始時に、当該システム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じなければならない。

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。

ウ　サーバ等、端末及びネットワーク機器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確認する時間間隔を可能な限り短くしなければならない。

エ　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、必要な措置を講じなければならない。

(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じなければならない。

ア　電子計算機には、当該電子計算機上で動作するウイルス対策ソフトウェアが存在しない場合を除き、ウイルス対策ソフトウェアを導入しなければならない。

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、ウイルス対策ソフトウェア等により対策を講じなければならない。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、ウイルス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、必要な対処を行わなければならない。

(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じなければならない。

ア　要安定情報を取り扱う外部回線に接続された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、端末及びネットワーク機器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じなければならない。

イ　サーバ等、端末、ネットワーク機器又は電気通信回線から監視対象を特定し、監視しなければならない。

ウ　外部回線に接続する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、別に定める措置を講じなければならない。

(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じなければならない。

ア　標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講じなければならない。

イ　外部回線に接続された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（内部対策及び出口対策）を講じなければならない。

(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、別に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　アプリケーション・コンテンツの作成及び提供

(1)　アプリケーション・コンテンツの作成時の対策

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自組織外の情報セキュリティ水準を低下させないため、アプリケーション・コンテンツの仕様書等に次に掲げる事項を記載しなければならない。

(ｱ)　提供するアプリケーション・コンテンツが不正プログラムを含まないこと。

(ｲ)　提供するアプリケーション・コンテンツが脆弱性を含まないこと。

(ｳ)　実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。

(ｴ)　電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。

(ｵ)　提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのＯＳ、ソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、ＯＳ、ソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。

(ｶ)　サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなど、サービス利用に当たって必須ではない機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。

イ　システムセキュリティ責任者は、アプリケーション・コンテンツの開発及び作成を業務委託する場合は、前記アに掲げる内容を仕様書等に記載しなければならない。

(2)　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

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、外部サービスを利用する場合、公用携帯電話機を使用する場合、及び情報セキュリティ管理者が例外として認める場合を除き、地方公共団体であることが保証されるドメイン名（「pref.saitama.jp」、「lg.jp」等。以下「保証ドメイン名」という。）を使用しなければならない。

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埼玉県警察のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講じなければならない。

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じなければならない。

(ｲ)　職員は、警察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等の有効性を保たなければならない。

第７　警察情報システムの構成要素

１　端末、サーバ等、複合機及び特定用途機器

(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、表示用デバイスの盗み見等物理的な脅威から保護するための対策を講じなければならない。

(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で脆弱性による危険性が増大することを防止するため、端末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なければならない。

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について、定期的に見直しを行わなければならない。

(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、必要な措置を講じなければならない。

(ｳ)　システムセキュリティ維持管理者は、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。

(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、及び分析しなければならない。

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、警察情報システムの更改又は廃棄を行う場合は、当該警察情報システムの端末が運用終了後に再利用されたとき、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、前記第５の２(4)の規定を準用し、必要な措置講じなければならない。

エ　モバイル端末及び公用携帯電話機の導入及び利用時の対策

(ｱ)　システムセキュリティ責任者は、モバイル端末及び公用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窃取されることを防止するための対策を講じなければならない。

(ｲ)　システムセキュリティ責任者は、モバイル端末及び公用携帯電話機の導入及び利用時の対策について、第８に定める対策を講じることができるように情報セキュリティ要件を検討しなければならない。

オ　個人所有の機器の導入及び利用時の対策

職員は、第８の１(2)オただし書きにより個人所有の機器を利用して管理対象情報を処理する場合は、個人所有の機器の導入及び利用時の対策について、盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための必要な対策を講じなければならない。

(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)アの規定を準用する。この場合において、「端末」とあるのは「サーバ等」と読み替えるものとする。

(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しなければならない。

(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際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じなければならない。

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)イの規定を準用する。この場合において、「端末」とあるのは「サーバ等」と読み替えるものとする。

(ｲ)　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発生を監視する必要があると認めた場合は、監視のために必要な機能を設けなければならない。

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)ウの規定を準用する。この場合において、「端末」とあるのは「サーバ等」と読み替えるものとする。

(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て、適切な情報セキュリティ要件を満たさなければならない。

(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おける情報セキュリティ対策を講じなければならない。

(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際には、複合機の電磁的記録媒体の全ての管理対象情報を抹消しなければならない。ただし、別に定める

場合は、この限りではない。

イ　ＩｏＴ機器を含む特定用途機器

システムセキュリティ責任者は、ＩｏＴ機器を含む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じなければならない。

2　電子メール、ウェブ等

(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警察情報システムへの電子メールの導入に当たっては、次に掲げる対策を講じなければならない。

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策を講じること。

エ　第８の１(3)キに定める対策を講じることのできるよう情報セキュリティ要件を検討すること。

(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警察情報システムへのウェブサーバ等の導入時等に当たっては、次に掲げる対策を講じなければならない。

ア　ウェブサーバの導入及び運用時の対策

(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)　ウェブコンテンツの編集作業を担当する主体を限定すること。

(ｳ)　公開してはならない、又は意味の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。

(ｴ)　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。

(ｵ)　インターネットを介して転送される管理対象情報については、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により、盗聴及び改ざんを防止すること。

(ｶ)　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。

イ　ウェブアプリケーションの開発及び運用時の対策

ウェブアプリケーションの開発及び運用時において、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、必要な措置を講じなければならない。

(3)　ドメインネームシステム（ＤＮＳ）

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警察情報システムへのドメインネームシステム（ＤＮＳ）の導入等に当たっては、次に掲げる対策を講じなければならない。

ア　ドメインネームシステム（ＤＮＳ）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こと。

(ｲ)　キャッシュサーバにおいて、名前解決の要求に適切に応答すること。

(ｳ)　コンテンツサーバにおいて、組織内部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を外部に漏えいさせないこと。

イ　ドメインネームシステム（ＤＮＳ）の運用時の対策

(ｱ)　系統間で同期をと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及び運用に当たっては、次に掲げる対策を講じなければならない。

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権限管理を行うこと。

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こと。

エ　データベース及びデータベースに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

(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の観点から、次に掲げる順序で検討を行わなければならない。

a　拠点間の回線　専用回線（有線回線に限る。）、広域イーサネット（有線回線であって事業者閉域網のものに限る。）、ＩＰ－ＶＰＮ（有線回線であって事業者閉域網のものに限る。）、携帯電話回線（事業者閉域網のものに限る。）の順

b　庁舎内回線　有線回線、無線回線の順

(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しなければならない。

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ネットワーク機器を利用することにより、アクセス制御及び経路制御を行わなければならない。

(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警察情報システムを電気通信回線に接続する場合で、通信内容の秘匿性の確保が必要と認められるときは、通信内容の秘匿性を確保するための措置を講じなければならない。

(ｴ)　システムセキュリティ責任者は、ネットワーク機器を警察が管理する区域に設置しなければならない。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じなければならない。

(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は、次に掲げるａからｃまでの順序で導入を検討すること。この場合において、当該回線が次に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なければならない。

ａ　一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、次に掲げる対策が講じられていること。

(a)　情報システム内の他の機器への不正な接続を制限すること。

(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こと。

(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、IDS/IPS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した場合は、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しなければならない。

(ｷ)　ソフトウェアの利用及び禁止については、前記１(1)ア(ｲ)の規定を準用する。この場合において、「端末」とあるのは「ネットワーク機器」と読み替えるものとする。

(ｸ)　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。

(ｹ)　保守又は診断については、前記１(2)ア(ｳ)の規定を準用する。この場合において、「サーバ等」とあるのは「ネットワーク機器」と読み替えるものとする。

イ　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わなければならない。また、監視により得られた結果は、消去又は改ざんが行われないように管理しなければならない。

(ｲ)　電気通信回線の運用時の対策については、前記１(1)イ(ｲ)及び(ｴ)の規定を準用する。この場合において、「端末」とあるのは「電気通信回線及びネットワーク機

器」と読み替えるものとする。

(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の情報セキュリティの確保が困難な事由が発生した場合は、当該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。

ウ　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(1)ウの規定を準用する。この場合において、「端末」とあるのは「ネットワーク機器」と読み替えるものとする。

エ　無線ＬＡＮ環境導入時の対策

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ため、無線ＬＡＮ技術を利用して電気通信回線を構築する場合は、前記アからウまでに規定する対策に加えて、通信内容の秘匿性を確保するための通信路の暗号化を行わなければならない。

(2)　ＩＰｖ６通信回線

ア　ＩＰｖ６通信を行う警察情報システムに係る対策

(ｱ)　システムセキュリティ責任者は、ＩＰｖ６技術を利用する通信を行う警察情報システムを構築する場合において、IPv6 Ready Logo Programに基づくPhase-2準拠製品を調達することが可能なときは、これを選択しなければならない。

(ｲ)　システムセキュリティ責任者は、ＩＰｖ６通信の特性等を踏まえ、ＩＰｖ６通信を想定して構築する警察情報システムにおいては、次の事項を含む脅威又は脆弱性に対する検討を行い、必要な措置を講じなければならない。

ａ　グローバルＩＰアドレスによる直接の到達性における脅威

ｂ　ＩＰｖ６通信環境の設定不備等に起因する不正アクセスの脅威

ｃ　ＩＰｖ４通信とＩＰｖ６通信を情報システムにおいて共存させる際のＩＰｖ６通信の制御の不備に起因する脆弱性の発生

ｄ　ソフトウェアにおけるＩＰｖ６アドレスの取扱いの不備に起因する脆弱性の発生

イ　意図しないＩＰｖ６通信の抑止及び監視

システムセキュリティ責任者は、端末、サーバ等及びネットワーク機器をＩＰｖ６通信を想定していない通信回線に接続する場合は、自動トンネリング機能で想定外のＩＰｖ６通信パケットが到達する脅威等当該通信回線から受ける不正なＩＰｖ６通信による情報セキュリティ上の脅威を防止するため、ＩＰｖ６通信を抑止するなどの措置を講ずること。

第８　警察情報システムの利用

１　警察情報システムの利用

(1)　規定遵守を支援するための対策

ア　システムセキュリティ責任者は、職員による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ警察情報システムを構築しなければならない。

イ　システムセキュリティ責任者は、簿冊により管理することとされている事項その他の警察情報セキュリティポリシーに定める手続について、システム構築等の技術的措置による電子化を検討し、事務負担の軽減に努めるものとする。

ウ　前記イの規定に基づき電子化する手続は、警察情報セキュリティポリシーに定める手続と同等以上の管理水準であることについて情報セキュリティ管理者（警察庁が整備した情報システム又は警察庁が整備する情報システムと接続された情報システムについては、警察庁情報セキュリティ管理者）の確認を受けることにより、警察情報セキュリティポリシーによらないことができる。

(2)　利用時の基本的対策

ア　運用管理担当者等

(ｱ)　運用管理担当者

a　外部記録媒体、公用携帯電話機、モバイル端末等を利用する所属の運用管理者は、警察本部の課長補佐（室長補佐、隊長補佐及び科長を含む。）、さいたま市警察部及び各方面本部の補佐官、警察学校の校長補佐若しくは警察署の課長（課長代理及び課長を置かない場合の係長を含む。）以上の職にある職員又は処務規程第32条に規定する総括管理者から、運用管理担当者を指名するものとする。

b　運用管理担当者は、外部記録媒体及び公用携帯電話機の管理並びにモバイル端末等の持ち出しに関する管理を行うものとする。

(ｲ)　運用管理補助者

ａ　運用管理者は、運用管理担当者による外部記録媒体及び公用携帯電話機の管理が困難な場合は、係長以上の職にある職員から、運用管理補助者を指名することができる。

ｂ　運用管理補助者は、運用管理担当者の指示の下、外部記録媒体及び公用携帯電話機の管理を補助するものとする。

イ　警察情報システム

(ｱ)　職員は、あらかじめ定められた目的以外の目的で警察情報システムを使用してはならない。

(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、警察情報システムを外部回線に接続してはならない。

(ｳ)　職員は、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警察情報システムを接続してはならない。

(ｴ)　職員は、システムセキュリティ責任者の許可なく、運用要領に規定する改造の範囲を超えて警察情報システムを構成する機器の改造をしてはならない。

(ｵ)　職員は、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ってはならない。

(ｶ)　職員は、別に定める場合を除き、機器を警察庁舎外に持ち出してはならない。

(ｷ)　職員は、別に定める場合を除き、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てはならない。

(ｸ)　職員は、警察情報システムを利用するときは、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しなければならない。特に、主体認証情報を入力するときは、権限のない者に視認されていないことを確認しなければならない。

(ｹ)　職員は、他の者にアクセスさせる必要がない管理対象情報については、アクセスできないよう設定しなければならない。

(ｺ)　職員は、電子計算機又はネットワーク機器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しなければならない。

(ｻ)　職員は、この通達に定めるもののほか、取り扱う警察情報システムについて別の定め又は指示事項があるときは、それを遵守しなければならない。

ウ　公用携帯電話機

(ｱ)　職員は、公用携帯電話機内の要機密情報を必要最小限にした上で、公用携帯電話機の警察庁舎外への持ち出しを行うことができる。ただし、共用で利用する公用携帯電話機（音声通話機能のみを使用するものを除く。）については、運用管理担当者の許可を得なければならない。

(ｲ)　職員は、公用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には、主体認証情報入力等の主体認証を求められるよう設定しなければならない。

(ｳ)　職員は、公用携帯電話機を適正に管理しなければならない。

(ｴ)　職員は、要機密情報を取り扱った公用携帯電話機を廃棄する場合は、情報の抹消を実施しなければならない。

エ　外部記録媒体

(ｱ)　職員は、外部記録媒体を適正に管理しなければならない。

(ｲ)　職員は、外部記録媒体を警察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、運用管理担当者の許可を得なければならない。

オ　個人所有の機器

職員は、個人所有の機器において管理対象情報を処理してはならない。ただし、別に定める場合は、この限りでない。

(3)　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、警察が管理又は運用する（業務委託による場合を含む。）電子メール機能又は公用携帯電話機の電子メール機能を利用しなければならない。

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、保証ドメイン名を使用しなければならない。ただし、前記第４の２に規定する外部サービスを利用するとき、公用携帯電話機を使用するとき、又は特別な事情があるときは、この限りではない。

ウ　職員は、不審な電子メールを受信したときは、当該電子メールを開封することなく、直ちに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　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ってはならない。

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で、電子署名が付与されているときは、電子署名により当該ソフトウェアの配布元を確認しなければならない。

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しなければならない。

(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　職員が機密性２（中）情報を電子メールにより外部に送信する場合については、前記第３の５(3)の規定を準用する。この場合において、当該情報に主体認証情報を設定し、又は暗号化しなければならない。

ク　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しなければならない。

ケ　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しなければならない。

コ　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てはならない。ただし、やむを得ない事由がある場合は、この限りでない。

サ　職員は前記コただし書きの規定により、電子メールにより外部から受信した要機密情報を、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たときは、外部記録媒体を用いて外部回線と接続されていない端末に取り込むなどした後、速やかに削除しなければならない。

(4)　識別コード及び主体認証情報の取扱い

ア　職員は、付与された識別コード以外の識別コードを用いて、警察情報システムを使

用してはならない。

イ　職員は、付与された主体認証情報を権限のない者に知られないよう適切に管理しなければならない。

(5)　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てはならない。

イ　職員は、必要に応じて、鍵のバックアップを取得するものとする。この場合において、取得したバックアップは、オリジナルの鍵と同等の安全管理を実施するものとする。

(6)　不正プログラム感染防止

職員は、不正プログラム感染防止に関し、次に掲げる事項を遵守しなければならない。

ア　不正プログラム感染を回避するため、ウイルス対策ソフトウェア等により不正プログラムとして検知された実行プログラム形式のファイルを実行してはならない。

また、不正プログラムとして検知されたデータファイルを、アプリケーション等で読み込んではならない。

イ　外部から受領し、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警察情報システムを構成する電子計算機に接続するときは、当該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しなければならない。

(7)　ウェブ会議サービスの利用時の対策

ア　職員は、職務上ウェブ会議サービスを利用しようとする場合は、前記第４の２(1)ア(ｱ) a 若しくはイ(ｱ)又は第４の２(2)イに定める手続をとらなければならない。この場合において、ウェブ会議の参加者及び取り扱う管理対象情報に応じた情報セキュリティ対策を講じなければならない。

イ　職員は、ウェブ会議を主催するときは、会議に関係のない者を参加させてはならない。

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で情報を発信する場合は、次に掲げる対策を講じなければならない。

(1)　職務上ソーシャルメディアサービスを利用して情報発信をしようとする場合は、前記

第４の２(2)アに定める確認をしなければならない。

なお、当該サービスの利用において、要機密情報を取り扱ってはならない。

(2)　ソーシャルメディアサービスを用いて要安定情報を発信する場合は、埼玉県警察ホームページに当該情報を掲載して参照できるようにしなければならない。

3　テレワーク及びモバイル勤務

(1)　実施環境における対策

ア　システムセキュリティ責任者は、テレワーク及びモバイル勤務の実施により外部回線を経由して警察情報システムにリモートアクセスをする形態となる警察情報システムを構築する場合は、通信経路及びリモートアクセス特有の攻撃に対する情報セキュリティを確保しなければならない。

イ　システムセキュリティ責任者は、リモートアクセスに対し多要素主体認証を行わなければならない。

ウ　システムセキュリティ責任者は、リモートアクセスをするに当たっては、許可された端末に限定する措置を講じなければならない。

エ　システムセキュリティ責任者は、リモートアクセスをする個人所有の端末を最新の脆弱性対策、不正プログラム対策等が施されている端末に限定しなければならない。

(2)　実施時における対策

ア　職員は、テレワーク及びモバイル勤務の実施前及び実施後に別に定める項目について確認しなければならない。

イ　職員は、画面ののぞき見及び盗聴を防止できるようテレワーク又はモバイル勤務の実施場所を選定しなければならない。

また、自宅以外の場所でテレワーク又はモバイル勤務を実施する場合は、離席時の盗難等に注意しなければならない。

ウ　職員は、テレワーク及びモバイル勤務時において警察情報システムへの接続に利用する回線については、別に定める回線を使用しなければならない。

第９　その他

本通達の実施に必要な細部事項については、別に定める。

実施日

1　この通達は、令和５年４月１日から実施する。

2　この通達で定める事項は、この通達の施行の際、現に整備済みでこの通達に定める事項を満たしていない警察情報システムについては、当分の間、適用を猶予することができる。この場合において、システムセキュリティ責任者は、可能な限り早期に要件を満たすことができるよう努めるとともに、情報セキュリティを確保するための代替手段を講じなければならない。