保 存 期 間 ５ 年

通達乙情管第213号

令和６年３月22日

本部内各部課長

警 察 学 校 長　殿

各 警 察 署 長

警　　務　　部　　長

（情報セキュリティ管理者）

茨城県警察における情報セキュリティに関する対策基準の細目について

茨城県警察における情報セキュリティに関する対策基準の細目については、茨城県警察における情報セキュリティに関する対策基準の細目（令和５年３月23日付け通達乙情管発第332号別添。以下「旧通達」という。）に基づき実施してきたところであるが、この度、その一部を改め、令和６年４月１日から実施することとしたので、事務処理上誤りのないようにされたい。なお、旧通達は、令和６年３月31日限り、廃止する。

記

主な改正点

１　業務委託先に求める対策を明確化した。

２　クラウドサービス利用時のセキュリティ対策を明確化した。

３　個人所有携帯電話機の特例利用申請の際に必要となる対策を変更した。

別添

令和６年４月

茨城県警察における情報セキュリティに関する対策基準の細目

目次

第１　情報セキュリティ対策の基本的枠組み

１　情報セキュリティアドバイザーが行う助言

「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」（令和６年３月22日付け通達甲情管発第212号。以下「対策基準」という。）第２の１(2)イにおける情報セキュリティアドバイザーが行う助言について、次のとおり定める。

(1)　警察情報セキュリティポリシーの整備

(2)　警察情報システムに係る技術的事項

(3)　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)　(1)から(3)までに掲げるもののほか、情報セキュリティ対策に係る事項

２　情報セキュリティ対策推進事務局の事務

対策基準第２の２(1)ア(ｱ)に基づき、情報セキュリティ対策推進事務局が遂行する事務について、次のとおり定める。

(1)　警察情報セキュリティポリシーの策定に係る事務

(2)　警察情報セキュリティポリシーの運用に係る事務

(3)　警察情報セキュリティポリシーの遵守事項に関する例外措置に係る事務

(4)　情報セキュリティ対策の教養の実施に係る事務

(5)　(1)から(4)までに掲げるもののほか、情報セキュリティ管理者が必要と認める事務

３　県警ＣＳＩＲＴの運営に係る事項

対策基準第２の１(1)エ(ｳ)に基づき、県警ＣＳＩＲＴの運営に係る事項について、次のとおり定める。

(1)　県警ＣＳＩＲＴの構成

県警ＣＳＩＲＴに総括、解析班及び支援班を置く。

(2)　総括班

ア　総括班の構成員は、それぞれ次の者をもって充てる。

(ｱ)　班長

警務部情報管理課管理官（企画・指導）

(ｲ)　班員

警務部情報管理課課長補佐（企画・指導）以下の職員

イ　総括班の任務は、次に掲げるものとする。

(ｱ)　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（以下「発生所属等」という。）に対する指導又は助言

(ｲ)　情報の集約と関係所属への周知及び警察庁への報告

(ｳ)　被害拡大の防止及び証拠保全の方針の決定

(ｴ)　県警ＣＳＩＲＴ内の総合調整

(ｵ)　広報対応における関係所属との連携

(ｶ)　サイバー戦略推進室、生活安全部サイバー犯罪対策課及び警備部公安課との連携

ウ　対処体制の保持

イで掲げる総括班の任務遂行に必要な場合には、構成員以外の情報管理課の職員についてもあらかじめ指名するなどして、実効ある対処体制を保持すること。

(3)　解析班

ア　解析班の構成員は、それぞれの次の者をもって充てる。

(ｱ)　班長

警務部情報管理課管理官（情報システム）

(ｲ)　班員

警務部情報管理課課長補佐（情報管理・運用）以下の職員

警務部情報管理課課長補佐（システム開発）以下の職員

イ　解析班の任務は、次に掲げるものとする。

情報セキュリティインシデントに関する電磁的記録の解析及びそれに基づく当該インシデントの分析並びにこれらの実施に係る指導

ウ　対処体制の保持

イで掲げる解析班の任務遂行に必要な場合には、構成員以外の職員についてもあらかじめ指名するなどして、実効ある対処体制を保持すること。

(4)　支援班

ア　支援班の構成員は、それぞれ次の者をもって充てる。

(ｱ)　班長

関東管区警察局茨城県情報通信部情報技術解析課長

(ｲ)　班員

関東管区警察局茨城県情報通信部情報技術解析課員

イ　支援班は、県警ＣＳＩＲＴの長からの依頼により、情報セキュリティインシデントに関する電磁的記録の解析及びそれに基づく当該インシデントの分析並びにこれらの実施に係る指導に関し支援を行うことを任務とする。

4　例外措置

(1)　例外措置手続

対策基準第２の２(2)ア(ｱ)に基づき、例外措置手続について、次のとおり定める。

ア　例外措置の変更

申請者は、例外措置の適用の許可を受けた後、申請内容に変更が生じた場合は、申請内容を修正し、速やかに再申請すること。

イ　例外措置終了後の報告

申請者は、例外措置の適用期間が終了した場合、当該例外措置の適用の許可を受けた際に、許可者から報告を行うよう求められた事項について、許可者に報告すること。また、許可者は、例外措置の適用期間の終了後、申請者から報告がない場合には、申請者にその状況を報告させ、必要な対応を行うこと。ただし、対策基準第２の２(2)イ(ｲ)及び(ｳ)の審査及び許可の際に、報告を要しないとされた場合は、この限りでない。

ウ　庶務

例外措置の適用の審査等に係る庶務は、警務部情報管理課（以下「情報管理課」という。）において処理する。

エ　その他

対策基準第２の２(2)イ(ｱ)における例外措置の適用申請については、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、システムセキュリティ責任者又は運用管理者が許可者に対して包括的に行うことができる。

(2)　例外措置の運用

対策基準第２の２(2)イ(ｱ)及び(ｳ)に基づく例外措置適用申請書及び審査結果通知書の様式等については、別に定める。

5　情報セキュリティインシデントへの対処

対策基準第２の２(4)イ(ｲ)及びウ(ｱ)における要報告インシデント及び再発防止策の報告について、次のとおり定める。

(1)　報告先

要報告インシデント及び再発防止策に係る情報管理課への報告先は、別に定める。

(2)　様式

要報告インシデントに係る報告の様式については、別に定める。

(3)　対策基準第２の２(4)ア(ｶ)に定める事案について、事業者から報告等を受けた所属は、情報管理課及び会計部門等関係所属に当該事案について速やかに報告を行うこと。

６　情報セキュリティ監査

対策基準第２の３(3)における監査補助者の指名等について、監査責任者は、通常監査の実施に当たって、情報管理課の職員の中から監査補助者を指名すること。このほか、監査補助者の独立性が保たれるよう留意すること。

第２　管理対象情報の取扱い

１　管理対象情報の取扱い

(1)　管理対象情報の分類及び取扱制限の決定・明示

ア　対策基準第３の１(2)イにおける自所属の上級の職員については、自所属の上級の職員であって警部相当職以上の者（夜間・休日にあっては当直長及び副当直長を含む。）とする。

イ　対策基準第３の１(2)エにおける管理対象情報の機密性の分類及び取扱制限の明示を必要としないものについて、次のとおり定める。

(ｱ)　秘密文書又は特定秘密に関する規程に基づき、秘密文書又は特定秘密である旨が表示されているもの

(ｲ)　捜査資料取扱保管要綱（令和５年２月17日付け通達甲刑総第２号別添）３(1)に定義されている「捜査資料」及び証拠物件

(ｳ)　法令その他の規程により様式等の定めがあり、その取扱いが明らかであるもの

(ｴ)　(ｲ)及び(ｳ)のほか、管理対象情報の機密性の分類及び取扱制限を明示す

ることが不適当なものとして、運用管理者が認めたもの

(ｵ) 広報資料、ウェブサイト掲載資料その他の公開する情報であって、その取扱いが明らかであるもの

ウ イに掲げる管理対象情報の機密性の分類及び取扱制限を明示する必要がない場合であっても、当該管理対象情報の機密性の分類及び取扱制限に応じて、ファイル名や当該ファイルを添付したメールの件名・本文中に取扱上の留意事項を記載するなどの方法により、当該管理対象情報が提供先においても適切に取り扱われるよう努めること。

(2) 管理対象情報の利用・保存

対策基準第３の１(3)ウに基づき、警察の庁舎外に設置されている機器等に要機密情報を保存する必要がある場合には、事件主管課長が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と協議して別に定めるところにより、当該機器等に保存することができることとする。

(3) 管理対象情報の運搬・送信

ア 対策基準第３の１(5)イにおける要保護情報が記録又は記載された記録媒体の警察の庁舎外への運搬を第三者へ依頼する場合の措置については、次のとおり定める。

(ｱ) 要保護情報が記録又は記載された記録媒体の警察の庁舎外への運搬を第三者へ依頼する場合には、必要に応じて受領印が必要となる書留郵便や、専用車両による配達サービス、配達状況の追跡が可能なサービス等の手段により運搬すること。

(ｲ) 要安定情報を運搬するときは、運搬中の滅失、紛失等を防止するため、必要に応じて、同一の情報を異なる経路手段で運搬するなど適切な措置を講ずること。

イ 対策基準第３の１(5)ウにおける要機密情報を警察の庁舎外に持ち出す場合については、次に掲げる事項を遵守すること。

(ｱ) 機密性２（中）情報を持ち出す場合は、その旨を１(1)アに定める所属内の上級の職員に報告（口頭による報告を含む。）すること。

(ｲ) 機密性３（高）情報を持ち出す場合は、機密性３（高）情報提供・持出簿（以下「提供・持出簿」という。）に氏名、当該機密性３（高）情報を

識別できる事項（文書番号、件名等）、提供等区分、提供日又は持出期間、目的及び提供・持出開始日時を記録した上で、運用管理者の許可を得ること。ただし、法令その他の規程により様式等の定めがある場合は、その規程によること。

なお、職務上緊急に機密性３（高）情報を持ち出す必要があって運用管理者が不在の場合には、運用管理者があらかじめ指名した当該管理者の職責を代行する警視相当職以上の者の許可を得ることとする。

(ｳ) (ｲ)の提供・持出簿の様式等は、別に定める。

(4) 管理対象情報の消去

対策基準第３の１(6)イにおける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、次に掲げる事項を例とする対策を講ずること。

ア リース契約の仕様書に記載し、契約内容にも含める。

イ リース契約終了に伴う情報の抹消について、役務提供契約を別途締結する。

(5) 管理対象情報のバックアップ

対策基準第３の１(7)イにおけるバックアップの保存場所については、災害や情報セキュリティインシデント等の危機的事象により生ずる業務上の支障を考慮し、適切な保存場所を選定すること。要保全情報又は要安定情報である電磁的記録のバックアップについては、必要に応じ、バックアップ取得元の警察情報システム等と同時に破壊されない保存場所を選定すること。

２ 管理対象情報を取り扱う区域の管理

(1) 区域の分類

対策基準第３の２(1)における各区域の特性に応じた対策を行うため、区域の分類を下表のとおり定める。

表１ 区域の分類

クラス３	情報セキュリティを確保するための対策を実施する必要がある区域（要管理対策区域）のうち、警察情報システムに係る機械室であり、室ごとの区域
クラス２	クラス３以外の要管理対策区域であり、執務室等、

	職員以外の者の立入りを制限する必要がある所属ごとの区域
クラス１	クラス３、クラス２以外の要管理対策区域であり、各庁舎における職員が共用する廊下等の一の区域
クラス０	各庁舎の敷地内であり、職員以外の者が自由に立ち入ることのできる要管理対策区域外の一の区域

(2) 区域における対策の基準等

区域情報セキュリティ管理者の指名の方法及び対策の基準について、次のとおり定める。

ア クラス３

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し、次に掲げる対策を講ずること。

(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講ずること。

(ｳ) 当該区域に立ち入る者の氏名とその入退室の時刻を記録すること。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、職員の立会いや監視カメラ等により監視するなどの措置を講ずること。

(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。

イ クラス２

区域情報セキュリティ管理者に、各所属の長を指名し、次に掲げる対策を講ずること。

(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講ずること。

(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、機器等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講ずること。

(ｵ)　クラス０に分類される区域と接するときは、当該境界においてウに定める対策を講ずること。

ウ　クラス１

区域情報セキュリティ管理者に、当該庁舎の庁舎管理に関する事務を処理する者を指名し、次に掲げる対策を講ずること。

(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講ずること。

(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カードを身に付けさせるなどして、職員とそれ以外の者を視覚上区別できるようにすること。

(3)　区域ごとの対策の決定

対策基準第３の２(2)イにおける情報セキュリティの確保のための管理対策については、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、(2)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することとする。

(4)　区域における対策の実施

対策基準第３の２(3)における管理する区域に対して定めた対策については、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、(2)及び(3)において定めた対策を実施すること。

なお、情報セキュリティ管理者が、(2)の基準による運用を困難と認めたときは、当該基準によらない区域を設けることができる。このとき、情報セキュリティ管理者は、(2)の規定を参考として、関係する他の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ずること。

第３　外部委託

１　業務委託

(1)　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

(ｱ)　委託先の選定条件を含む仕様の策定

システムセキュリティ責任者又は運用管理者は、対策基準第４の１(1)ア(ｲ)における委託先の選定条件を含む仕様の策定において、次のａからｅに掲げる情報セキュリティ対策の実施を選定条件とし、仕様にも含めること。また、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、必要に応じて次のｆ及びｇに掲げる事項を仕様に含めること。

ａ　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

ｂ　委託先（再委託先を含む。）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

ｃ　情報セキュリティインシデントへの対処方法

ｄ　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

ｅ　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

ｆ　情報セキュリティ監査の受入れ

ｇ　サービスレベルの保証

(ｲ)　仕様に基づく委託先の選定

システムセキュリティ責任者又は運用管理者は、対策基準第４の１(1)ア(ｳ)における仕様に基づく委託先の選定において、委託先がその役務内

容を一部再委託する場合には、再委託されることにより生ず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を委託先に求めること。また、委託判断基準及び委託先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。

a　再委託先における情報セキュリティ対策の実施

b　再委託先の情報セキュリティ対策の実施状況の把握

(ｳ)　管理対象情報の取扱い

システムセキュリティ責任者又は運用管理者は、対策基準第４の１(1)ア(ｴ)の契約の締結に当たり、委託先との情報の受渡し方法や、委託業務終了時の情報の廃棄方法等を含む情報の取扱手順について委託先と合意し、定められた手順により情報を取り扱うこと。

(ｴ)　情報セキュリティ対策の履行状況確認

システムセキュリティ責任者又は運用管理者は、対策基準第４の１(1)ア(ｴ)の契約の締結に当たり、次に掲げる事項を含む委託先における情報セキュリティ対策の遵守方法、情報セキュリティ管理体制等に関する確認書を提出させること。

なお、確認書にあっては、別紙１の別記様式に示す情報セキュリティ対策履行状況確認書を参考とし、変更があった場合は、速やかに再提出させること。

a　委託する業務に携わる者の特定

b　委託する業務に携わる者が実施する具体的な情報セキュリティ対策の内容

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、対策基準第４の１(1)イ(ｱ)における管理対象情報の適正な取扱いのための情報セキュリティ対策について、委託業務における管理対象情報の適正な取扱いを委託先に担保させるため、次に掲げる内容を含む情報セキュリティ対策を委託先との契約に含めた上で、委託期間を通じて、管理対象情報の分類等に応じた実施を求めること。また、別紙１に掲げる内容を参考として、守秘義務の担保、再委託管理、業務管理等に係る事項についても契約に含め実施を求めること。

(ｱ)　情報セキュリティインシデント等への対処能力の確立・維持

(ｲ)　情報にアクセスする主体の識別とアクセスの制御

(ｳ)　ログの取得・監視

(ｴ)　情報を取り扱う機器等の物理的保護

(ｵ)　情報を取り扱う要員への周知と統制

(ｶ)　情報セキュリティの脅威に対処するための資産管理・リスク評価

(ｷ)　委託先が取り扱う情報及び当該情報を取り扱う情報システムの完全性の保護

(ｸ)　情報セキュリティ対策の検証・評価・見直し

(2)　警察情報システムに関する業務委託

ア　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

対策基準第４の１(2)アにおける委託先の選定条件については、次に掲げる事項を含めること。

(ｱ)　委託業務の実施に当たり、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

(ｲ)　委託先の資本関係・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

イ　警察情報システムの構築を業務委託する場合の対策

(ｱ)　対策基準第４の１(2)イ(ｲ)の警察情報セキュリティの観点に基づく試験について、次に掲げる対策を含めること。

ａ　ソフトウェアの作成及び試験を行う警察情報システムについては、情報セキュリティの観点から運用中の警察情報システムに悪影響が及ばないように、運用中の警察情報システムと分離すること。

ｂ　必要な試験がある場合には、試験項目及び試験方法を定め、これに基づいて試験を実施すること。

ｃ　実施した試験の実施記録を保存すること。

(ｲ)　対策基準第４の１(2)イ(ｳ)における警察情報システムの開発工程における情報セキュリティ対策について、次に掲げる対策を含めること。

ａ　ソースコードが不正に変更されることを防ぐために、次に掲げる事項

を含むソースコードの管理を適切に行うこと。

(a)　ソースコードの変更管理

(b)　ソースコードの閲覧制限のためのアクセス制御

(c)　ソースコードの滅失、き損等に備えたバックアップの取得

b　警察情報システムに関連する脆弱性についての対策要件として定めたセキュリティ実装方針に従うこと。

c　セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビュー及びソースコードレビューを実施すること。

d　コーディングに関する規定を整備すること。

ウ　警察情報システムの運用・保守を業務委託する場合の対策

対策基準第４の１(2)ウ(ｱ)における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、次に掲げる要件を含めること。

(ｱ)　警察情報システムの運用環境に課せられるべき条件の整備

(ｲ)　警察情報システムのセキュリティ監視を行う場合の監視手順や連絡方法

(ｳ)　警察情報システムの保守における情報セキュリティ対策

(ｴ)　運用中の警察情報システムに脆弱性が存在することが判明した場合の情報セキュリティ対策

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)　対策基準第４の１(2)エ(ｱ)における業務委託サービス特有の選定条件について、次のとおり定める。

a　業務委託サービスの中断や終了時に円滑に業務を移行するための対策として、次の事項を例とする情報セキュリティ対策を実施することを委託先の選定条件に加えること。

(a)　取り扱う管理対象情報の可用性の分類に応じた、業務委託サービス中断時の復旧要件

(b)　取り扱う管理対象情報の可用性の分類に応じた、業務委託サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法

b　業務委託サービスの利用を通じて取り扱う管理対象情報に対して国内法以外の法令及び規制が適用されるリスクを評価して委託先を選定し、必要に応じて管理対象情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を委託先の選定条件に加えること。

(ｲ)　対策基準第４の１(2)エ(ｲ)における業務委託サービスに係るセキュリティ要件について、取り扱う管理対象情報の分類及び取扱制限に応じて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。また、業務委託サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めること。

(ｳ)　対策基準第４の１(2)エ(ｳ)における委託先の信頼性の判断について、委託先が業務委託サービス利用者に提供可能な第三者による監査報告書の内容、各種の認定・認証制度の適用状況等から、委託先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判断すること。

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）

ア　システムセキュリティ責任者及び運用管理者は、クラウドサービスの利用に当たっては、必要に応じて次に掲げる事項を踏まえクラウドサービスの利用を判断すること。

(ｱ)　クラウドサービス利用者がクラウドサービスを利用する際の接続方法（テレワーク等により、外部回線から直接クラウドサービスにアクセスすることの可否等）

(ｲ)　クラウドサービス特有の脅威を踏まえて、クラウドサービスを利用して行うことが可能な業務や利用不可とする業務

(ｳ)　クラウドサービスで取り扱う情報の分類、取扱制限等に応じた、情報の保存を許可（又は禁止）する国・地域

(ｴ)　クラウドサービス特有の脅威やクラウドサービスを利用して行う業務の特性等を踏まえて、ＩＳＭＡＰのみを許容又はＩＳＭＡＰ－ＬＩＵも含めて許容

イ　ＩＳＭＡＰクラウドサービスリスト又はＩＳＭＡＰ－ＬＩＵクラウドサービスリストから選定すること。

(2)　クラウドサービスの利用に係る手続（要機密情報を取り扱う場合）

ア　クラウドサービスの利用申請の利用手続について、クラウドサービスを利用する場合、警察情報システム又はその一部として調達・導入されるクラウドサービスについてはシステムセキュリティ責任者が、その他の利用者自身の登録のみで利用可能なクラウドサービスについては運用管理者が、利用しようとするサービスの約款その他の提供条件等から、利用のリスクが許容できることを確認した上で、次に掲げる事項を明らかにして対策基準第４の２(3)エに定める承認権限者に申請を行うこと。この場合において警察情報システム上でクラウドサービスを利用する場合には、運用管理者は事前にシステムセキュリティ責任者と協議の上、申請を行うこと。

なお、申請内容に変更が生じた場合には、速やかに承認権限者に連絡すること。

(ｱ)　ＩＳＭＡＰ等クラウドサービスリストの登録番号

(ｲ)　クラウドサービスの名称（必要に応じて機能名までを含む。）

(ｳ)　クラウドサービスリストの区分（ＩＳＭＡＰ又はＩＳＭＡＰ－ＬＩＵ）

(ｴ)　クラウドサービス提供者の名称

(ｵ)　利用目的（業務内容）

(ｶ)　利用可能な警察情報システムの範囲

(ｷ)　取り扱う管理対象情報の分類

(ｸ)　クラウドサービスの利用規約（契約）内容

(ｹ)　取得するアカウント（クラウドサービス利用者、管理者及びその他）及び主体認証情報

(ｺ)　接続方法（外部回線から直接クラウドサービスに接続することの可否）

(ｻ)　利用期間

(ｼ)　利用申請者（所属・氏名）

(ｽ)　クラウドサービス利用者の範囲

(ｾ)　選定時の確認結果

(ｿ)　利用において講ずべき対策

イ　アの規定にかかわらず、次に掲げる場合は、それぞれで定める手続によりクラウドサービスを利用することができる。

(ｱ) 犯罪捜査において約款や規約等によるクラウドサービスを利用する特段の必要がある場合は、当該事務を所掌する警察庁の所属の長が警察庁情報セキュリティ管理者と協議して別に定めるところにより、利用することができる。

(ｲ) 情報技術の解析において約款や規約等によるクラウドサービスを利用しようとする場合は、次に掲げる事項を満たす場合に限り、利用することができる。

a 取り扱う管理対象情報は、必要最小限とすること。

b 不要となったアカウント、アプリケーション及び情報は速やかに削除すること。

c 不審なサービス及びアプリケーションを調査する際には、調査実施前及び実施後に資機材の初期化を実施すること。

d アカウントの登録には、ドメイン名に「go.jp」を含むメールアドレス及び個人所有のメールアドレスを使用しないこと。

(ｳ) 電気等の契約において約款や規約等によるクラウドサービスを利用しようとする場合は、次に掲げる用途に限り、運用管理者にアに掲げる内容の届出を行うことにより利用することができる。

a 当該サービスを提供する事業者自身が保有する情報を閲覧等すること。

b 当該サービスを利用して、当該事業者に対して情報を送信すること。

ウ その他

検索サービス等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で、取り扱う管理対象情報がアカウントの登録に必要な情報又は当該アカウントに限定される場合は、運用管理者の許可のみで利用できるものとする。ただし、検索する情報が当該クラウドサービスの提供側において収集、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すること。

(3) クラウドサービス利用状況等の管理（要機密情報を取り扱う場合）

利用申請の承認権限者は、クラウドサービス管理者の指名とクラウドサービスの利用状況の管理について、次に掲げる事項を管理すること。

ア 申請ごとにクラウドサービス管理者を指名すること。

イ　利用承認したクラウドサービスは、その内容を遅滞なく記録するよう運用ルールを定め、常に最新のクラウドサービスの利用状況を把握できるようにし、必要に応じて自組織内で共有すること。

(4)　クラウドサービスの選定に係る要件（要機密情報を取り扱う場合）

システムセキュリティ責任者又は運用管理者は、対策基準第４の２(1)イにおけるセキュリティ要件について、次に掲げる事項を含めること。

ア　ＩＳＭＡＰ管理基準の管理策基準が求める対策と同等以上の水準

イ　業務に特有のリスクを踏まえ、クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法、クラウドサービスに求めるサービスレベル等

ウ　ＩＳＭＡＰ等クラウドサービスリストの詳細情報等を用いて、セキュリティ要件を満たしていることの確認

(5)　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）

対策基準第４の２(3)イにおける利用申請の審査については、(4)に規定のクラウドサービスの選定に係る要件のほか、クラウドサービス提供者が、業務に特有のリスクを踏まえたクラウドサービス提供者の選定条件を満たしていることを審査し、利用の可否を決定すること。

(6)　クラウドサービスの利用（要機密情報を取り扱う場合）

ア　クラウドサービスの利用に係る運用規定の整備

クラウドサービスの利用に係る情報セキュリティ対策の基本方針は、次のとおりとする。

(ｱ)　クラウドサービスを利用して警察情報システムを導入・構築する際の情報セキュリティ対策の基本方針は表２のとおりとする。

表２　クラウドサービスを利用して警察情報システムを導入・構築する際の情報セキュリティ対策の基本方針

基本方針名	対策
アクセス制御に係る基本方針	・　クラウドサービスを利用する際にクラウドサービス提供者が付与又はクラウドサービス利用者が登録する識別コードの作成から廃棄に至るまでのライフサイクルにおける管理 ・　クラウドサービスを利用する際に使用するネッ

	トワークに対するサービスごとのアクセス制御 ・　クラウドサービスを利用する警察情報システムの管理者権限を保有するクラウドサービス利用者に対する強固な認証技術の利用 ・　クラウドサービス提供者が提供する主体認証情報の管理機能が要求事項を満たすことの確認及び要求事項を満たすための措置の実施 ・　クラウドサービス上に保存する管理対象情報やクラウドサービスの機能に対してアクセス制御できることの確認及び適切なアクセス制御の実施 ・　クラウドサービス利用者によるクラウドサービスに多大な影響を与える操作の特定と誤操作の抑制 ・　クラウドサービス上で構成される仮想マシンに対する適切なセキュリティ対策の実施 ・　インターネット等の外部回線から内部ネットワークを経由せずにクラウドサービス上に構築した警察情報システムにログインすることの要否の判断と認める場合の適切な情報セキュリティ対策の実施 ・　クラウドサービス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の必要なログの管理
暗号化に係る基本方針	・　クラウドサービス内及び通信経路全般における暗号化の確認及び適切な実施 ・　警察情報システムで利用する暗号化方式の遵守度合いに係る法令や規則の確認
開発時のセキュリティ対策に係る基本方針	・　クラウドサービスを利用する場合のクラウドサービス提供者へのセキュリティを保つための開発手順等の情報の要求とその活用

	・　クラウドサービス上に他ベンダが提供するソフトウェア等を導入する場合のそのソフトウェアのクラウドサービス上におけるライセンス規定
設計・設定時の誤り防止に係る基本方針	・　クラウドサービスを利用する際のクラウドサービス提供者への設計、設定、構築等における知見等の情報の要求とその活用 ・　クラウドサービスを利用する際の設定の誤りを見いだすための対策 ・　クラウドサービス上に構成された警察情報システムのネットワーク設計におけるセキュリティ要件の異なるネットワーク間の通信の監視 ・　利用するクラウドサービス上の警察情報システムが利用するデータ容量や稼働性能についての監視と将来の予測 ・　利用するクラウドサービス上で要安定情報を取り扱う場合の可用性を考慮した設計 ・　クラウドサービス内における時刻同期の方法の確認

(ｲ)　クラウドサービスを利用して警察情報システムを運用・保守する際の情報セキュリティ対策の基本方針は表３のとおりとする。

表３　クラウドサービスを利用して警察情報システムを運用・保守する際の情報セキュリティ対策の基本方針

基本方針名	対策
利用に係る基本方針	・　責任分界点を意識したクラウドサービスの利用 ・　利用承認を受けていないクラウドサービスの利用禁止 ・　クラウドサービス提供者に対する定期的なサービスの提供状態の確認 ・　利用するクラウドサービスに係る情報セキュリ

	ティインシデント発生時の連絡体制
教養に係る基本方針	・　クラウドサービス利用のための規定及び手順について ・　クラウドサービス利用に係る情報セキュリティリスクとリスク対応について ・　クラウドサービス利用に関する適用法令や関連する規制等について
クラウドサービスで取り扱う資産の管理に係る基本方針	・　クラウドサービス上で利用するIT資産の適切な管理 ・　クラウドサービス上に保存する管理対象情報に対する適切な分類・取扱制限の明示 ・　クラウドサービスの機能に対する脆弱性対策について、クラウドサービス利用者の責任範囲の明確化と対策の実施
アクセス制御に係る基本方針	・　管理者権限をクラウドサービス利用者に割り当てる場合のアクセス管理と操作の確実な記録 ・　クラウドサービス利用者に割り当てたアクセス権限に対する定期的な確認による見直し ・　クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合の機能の確認と利用者の制限 ・　利用するクラウドサービスの不正利用の監視
暗号化に係る基本方針	・　暗号化に用いる鍵の管理者と鍵の保管場所等の鍵管理機能 ・　鍵管理機能をクラウドサービス提供者が提供する場合の鍵管理手順と鍵の種類の情報の要求とリスク評価 ・　鍵管理機能をクラウドサービス提供者が提供する場合の鍵の生成から廃棄に至るまでのライフサイクルにおける情報の要求とリスク評価

通信の制御に係る基本方針	・　利用するクラウドサービスのネットワーク基盤が他のネットワークと分離されていることの確認
設計・設定時の誤りの防止に係る基本方針	・　クラウドサービスの設定を変更する場合の設定の誤りを防止するための対策 ・　クラウドサービス利用者が行う可能性のある重要操作の手順書の作成と監督者の指導の下での実施
警察情報システムの事業継続に係る基本方針	・　不測の事態に対してサービスの復旧を行うために必要なバックアップの確実な実施又はクラウドサービス提供者が提供する機能を利用する場合は、その実施の確認 ・　要安定情報をクラウドサービスで取り扱う場合の十分な可用性の担保、復旧に係る手順の策定と定期的な訓練の実施 ・　クラウドサービス提供者からの仕様内容の変更通知に関する内容確認と復旧手順の確認 ・　クラウドサービスで利用しているデータ容量、性能等の監視

(ｳ)　クラウドサービスを利用した警察情報システムを更改・廃棄する際の情報セキュリティ対策の基本方針は、表４のとおりとする。

表４　クラウドサービスを利用した警察情報システムを更改・廃棄する際の情報セキュリティ対策の基本方針

基本方針名	対策
クラウドサービス利用終了手順に係る基本方針	・　クラウドサービスの利用を終了する場合の移行計画書又は終了計画書の作成 ・　移行計画書又は終了計画書のクラウドサービス利用者への事前通知
管理対象情報の廃棄に係る基本方針	・　管理対象情報の廃棄方法 ・　暗号化消去が実施できない場合の基盤となる物

	理機器の廃棄方法
アカウントの廃棄に係る基本方針	・　作成されたクラウドサービス利用者アカウントの削除 ・　利用したクラウドサービスにおける管理者アカウントの削除又は返却と再利用の確認 ・　クラウドサービス利用者アカウント以外の特殊なアカウントの削除と関連情報の廃棄

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

クラウドサービスの利用に係るセキュリティ要件等は、表５のとおりとする。

表５ クラウドサービスの利用に係るセキュリティ要件

基本方針名	対策
クラウドサービス利用に係る内容の確認項目	・　クラウドサービス提供者が提供する主体認証情報の管理機能が自組織の要求事項を満たすこと。 ・　クラウドサービス上に保存する管理対象情報やクラウドサービスの機能に対してアクセス制御できること。 ・　クラウドサービス利用者によるクラウドサービスに多大な影響を与える操作の特定 ・　クラウドサービス内及び通信経路全般における暗号化 ・　クラウドサービス上に他ベンダが提供するソフトウェア等を導入する場合のそのソフトウェアのクラウドサービス上におけるライセンス規定 ・　クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合の機能 ・　鍵管理機能をクラウドサービス提供者が提供する場合の鍵管理手順と鍵の種類の情報の要求とリスク評価

	・　鍵管理機能をクラウドサービス提供者が提供する場合の鍵の生成から廃棄に至るまでのライフサイクルにおける情報の要求とリスク評価 ・　利用するクラウドサービスのネットワーク基盤が他のネットワークと分離されていること。 ・　クラウドサービス提供者が提供するバックアップ機能を利用する場合、求める要求事項が満たされること。
クラウドサービスを利用するアカウント管理に関するセキュリティ機能要件	・　クラウドサービス提供者が付与又はクラウドサービス利用者が登録する識別コードの作成から廃棄に至るまでのライフサイクルにおける管理 ・　クラウドサービスを利用する管理者権限を保有するクラウドサービス利用者に対する強固な認証技術 ・　クラウドサービス提供者が提供する主体認証情報の管理機能が要求事項を満たすための措置
アクセス制御に関するセキュリティ機能要件	・　クラウドサービス上に保存する管理対象情報やクラウドサービスの機能に対して適切なアクセス制御 ・　インターネット等の外部回線から内部ネットワークを経由せずにクラウドサービス上に構築した警察情報システムにログインすることを認める場合の適切なセキュリティ対策
権限管理に関するセキュリティ機能要件	・　クラウドサービス利用者によるクラウドサービスに多大な影響を与える誤操作の抑制 ・　クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合の利用者の制限
ログ管理に関するセキュリティ機能要件	・　クラウドサービス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必要なログの管理
暗号化に関するセキュリティ機能要件	・　クラウドサービス内及び通信経路全般における暗号化の適切な実施 ・　警察情報システムで利用する暗号化方式の遵守度合いに係る法令や規則の確認 ・　暗号化に用いる鍵の保管場所等の管理に関する要件 ・　クラウドサービスで利用する暗号鍵に関する生成から廃棄に至るまでのライフサイクルにおける適切な管理
設計・設定時の誤り防止に関するセキュリティ要件	・　クラウドサービス上で構成される仮想マシンに対する適切な情報セキュリティ対策 ・　クラウドサービス提供者へのセキュリティを保つための開発手順等の情報の要求とその活用 ・　クラウドサービス提供者への設計、設定、構築等における知見等の情報の要求とその活用 ・　クラウドサービスの設定の誤りを見いだすための対策
運用時の監視等の運用管理機能要件	・　クラウドサービス上に構成された警察情報システムのネットワーク設計におけるセキュリティ要件の異なるネットワーク間の通信の監視 ・　利用するクラウドサービス上の警察情報システムが利用するデータ容量や稼働性能についての監視と将来の予測 ・　クラウドサービス内における時刻同期の方法 ・　利用するクラウドサービスの不正利用の監視
可用性に関する機能要件	・　利用するクラウドサービス上で要安定情報を取り扱う場合の可用性を考慮した設計
情報セキュリティインシデントが発生した際の復旧に関す	・　不備の事態に対してサービスの復旧を行うために必要なバックアップの確実な実施

る対策要件	

ウ　クラウドサービスを利用した警察情報システムの導入・構築時の対策

(ｱ)　クラウドサービス管理者は、対策基準第４の２(4)イ(ｳ) a における情報セキュリティ水準の維持に関する手順について、次の実施手順を整備すること。

a　クラウドサービス利用のための責任分界点を意識したクラウドサービス利用手順

b　クラウドサービス利用者が行う可能性のある重要操作の手順

(ｲ)　クラウドサービス管理者は、対策基準第４の２(4)イ(ｳ) b 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について、次に掲げる事項を含む実施手順を整備すること。

a　クラウドサービス提供者との責任分界点を意識した責任範囲の整理

b　利用するクラウドサービスごとの情報セキュリティインシデント対処に関する事項

c　利用するクラウドサービスに係る情報セキュリティインシデント発生時の連絡体制

(ｳ)　クラウドサービス管理者は、対策基準第４の２(4)イ(ｳ) c におけるクラウドサービスが停止又は利用できなくなった際の復旧手順について、要安定情報をクラウドサービスで取り扱う場合の十分な可用性を担保した復旧に係る手順を整備すること。

エ　クラウドサービスを利用した警察情報システムの運用・保守時の対策

クラウドサービス管理者は、対策基準第４の２(4)ウ(ｱ)におけるクラウドサービスに係る運用・保守の適切な実施について、次に掲げる情報セキュリティ対策を実施すること。

(ｱ)　クラウドサービス提供者に対する定期的なサービスの提供状態の確認

(ｲ)　クラウドサービス上で利用するＩＴ資産の適切な管理

(ｳ)　クラウドサービスで利用するアカウント管理、アクセス制御、管理権限

a　管理者権限をクラウドサービス利用者に割り当てる場合のアクセス管理と操作の確実な記録

b　クラウドサービス利用者に割り当てたアクセス権限に対する定期的な確認による見直し

(ｴ)　クラウドサービスで利用する機能に対する脆弱性対策

(ｵ)　クラウドサービスを運用する際の設定変更に関する情報セキュリティ対策

a　クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合の利用者の制限

b　クラウドサービスの設定を変更する場合の設定の誤りを防止するための対策

c　クラウドサービス利用者が行う可能性のある重要操作に対する監督者の指導の下での実施

(ｶ)　利用するクラウドサービスへの不正利用を検知することが可能な監視機能

a　利用するクラウドサービスの不正利用の監視

b　クラウドサービスで利用しているデータ容量、性能等の監視

(ｷ)　クラウドサービスを運用する際の可用性に関する情報セキュリティ対策

a　不測の事態に対してサービスの復旧を行うために必要なバックアップの確実な実施

b　要安定情報をクラウドサービスで取り扱う場合の十分な可用性の担保、復旧に係る定期的な訓練の実施

c　クラウドサービス提供者からの仕様内容の変更通知に関する内容確認と復旧手順の確認

(ｸ)　クラウドサービスで利用する暗号鍵に関する生成から廃棄に至るまでのライフサイクルにおける適切な管理の実施

オ　クラウドサービスを利用した警察情報システムの更改・廃棄時の対策

クラウドサービス管理者は、対策基準第４の２(4)エ(ｱ)におけるクラウドサービスを利用した警察情報システムの更改・廃棄時の対策について、次に掲げる情報セキュリティ対策を実施すること。

(ｱ)　クラウドサービスで取り扱った管理対象情報の廃棄

(ｲ)　暗号化消去が行えない場合の基盤となる物理機器の廃棄

(ｳ)　作成されたクラウドサービス利用者アカウントの削除

(ｴ)　利用したクラウドサービスにおける管理者アカウントの削除又は返却

(ｵ)　クラウドサービス利用者アカウント以外の特殊なアカウントの削除と関連情報の廃棄

(7)　クラウドサービスの選定・利用（要機密情報を取り扱わない場合）

ア　クラウドサービスを利用可能な業務の範囲

要機密情報を取り扱わない場合のクラウドサービスを利用可能な業務の範囲について、利用に当たって入力又は提供する情報が当該クラウドサービス提供側に収集、分析等され、警察業務の遂行に支障を及ぼすおそれがある業務には利用できないものとする。ただし、情報セキュリティ対策により、情報セキュリティリスクが十分に軽減される場合は、この限りでない。

イ　クラウドサービスの利用に係る手続

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手続については、(2)の要機密情報を取り扱う場合のクラウドサービスの利用手続に準じて、承認権限者に申請を行うこと。ただし、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　クラウドサービスの利用状況等の管理

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状況等の管理については、(3)の要機密情報を取り扱う場合のクラウドサービスの利用状況等の管理に準じて管理すること。

エ　クラウドサービスの利用に係る運用要領等の整備

対策基準第４の２(5)エにおける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に係る運用要領等について、次に掲げる事項を例に定めること。

(ｱ)　サービス利用中の安全管理に係る規定

a　適切な主体認証、アクセス制御の管理の実施

b　サービス機能の設定（例えば情報の公開範囲）に関する定期的な内容確認

c　情報の滅失、破壊等に備えたバックアップの取得

d　利用者への定期的な注意喚起（禁止されている要機密情報の取扱いの有無の確認等）

(ｲ)　情報セキュリティインシデント発生時の連絡体制

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

対策基準第４の３(1)における機器等の調達に係る機器等の選定基準に、サプライチェーン・リスクを低減するための要件として、次に掲げる事項を含めること。

ア　調達した機器等に不正な変更が見つかったときに、必要に応じて追跡調査や立入検査等、自組織と調達先が連携して原因を調査・排除できる体制を整備していること。

イ　「ＩＴ調達に係る国等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）に基づき、サプライチェーン・リスクに対応する必要があると判断されるものについては、必要な措置を講ずること。

ウ　調達する機器等において、設計書の検査によるセキュリティ機能の適切な実装の確認、開発環境の管理体制の検査、脆弱性テスト等、第三者によるセキュリティ機能の客観的な評価を必要とする場合には、ISO/IEC15408に基づく認証を取得しているか否かを調達時の評価項目とすることを機器等の選定基準として定めること。

(2)　機器等の納入時の確認・検査手続の整備

対策基準第４の３(2)における機器等の納入時の確認・検査手続について、次に掲げる事項を確認できる手続を定めること。

ア　調達時に指定したセキュリティ要件の実装状況

イ　機器等に不正プログラムが混入していないこと。

第４　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

対策基準第５の１(1)における情報システム台帳について、記載すべき項目

を次のとおり定める。

ア　情報システム名

イ　システムセキュリティ責任者の役職名

ウ　システムセキュリティ維持管理者の役職名

エ　システム管理担当者の氏名及び連絡先

オ　ネットワーク管理担当者の氏名及び連絡先

カ　運用開始年月日

キ　運用終了予定日

ク　情報システム構成図

ケ　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。）

(ｱ)　インターネット回線

(ｲ)　専用線

(ｳ)　広域イーサネット（有線）

(ｴ)　携帯電話網（閉域網）

(ｵ)　その他（具体的に）

コ　通信回線装置

サ　アプリケーション

シ　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

ス　当該警察情報システムの設計・開発、運用・保守に関する事項

セ　情報システムの利用目的

ソ　警察情報システムの分類

タ　民間事業者等が提供するクラウドサービス等を利用して警察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。

(ｱ)　クラウドサービス等の名称（クラウドサービスの場合、必要に応じて機能名まで含む。）

(ｲ)　クラウドサービス等の提供者の名称

(ｳ)　利用期間

(ｴ)　クラウドサービス等の概要

(ｵ)　ドメイン名

(ｶ)　クラウドサービス等で取り扱う情報の格付及び取扱制限に関する事項

(ｷ)　情報の暗号化に用いる鍵の管理主体（機関等管理かクラウドサービス等の提供者管理か）

(ｸ)　クラウドサービス等で取り扱う情報が保存される国・地域

(ｹ)　サービスレベル

チ　その他上記以外の情報システムに関連する文書名等

(2)　情報システム関連文書の整備

対策基準第５の１(2)における情報システム関連文書の整備について、次のとおり定める。

ア　システムセキュリティ責任者は、対策基準第５の１(2)アの運用要領等に、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こと。

(ｱ)　当該警察情報システムにおいて取り扱うことのできる管理対象情報の機密性、完全性及び可用性の分類の範囲

(ｲ)　当該警察情報システムにおいて利用を認めるソフトウェア及び利用を禁止するソフトウェア

(ｳ)　当該警察情報システムにおいて職員が独自の判断で行うことのできる改造（新たな機器等の接続、ソフトウェア追加等）の範囲

イ　システムセキュリティ責任者は、対策基準第５の１(2)イ(ｱ)における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について、次に掲げる事項を含めること。

(ｱ)　サーバ等及び端末の機種並びに利用しているソフトウェアの種類、名称及びバージョン、サポート体制等

(ｲ)　サーバ等及び端末で利用するソフトウェアを動作させるために用いられる他のソフトウェアであって、次に掲げる事項を含むものの種類、名称及びバージョン、入手先、サポート体制等

a　動的リンクライブラリ等、ソフトウェア実行時に読み込まれて使用されるもの

b　フレームワーク等、ソフトウェアを実行するための実行環境となるもの

ｃ　プラグイン等、ソフトウェアの機能を拡張するもの

ｄ　静的リンクライブラリ等、ソフトウェアを開発する際に当該ソフトウェアに組み込まれるもの

ｅ　インストーラー作成ソフトウェア等、ソフトウェアを開発する際に開発を支援するために使用するもの

(ｳ)　サーバ等及び端末の仕様書又は設計書

(ｴ)　システムセキュリティ責任者は、必要に応じて、(ｱ)及び(ｲ)の情報を収集するため、自動でソフトウェアの種類やバージョン等を管理する機能を有するＩＴ資産管理ソフトウェアを導入すること。

ウ　システムセキュリティ責任者は、対策基準第５の１(2)イ(ｲ)における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について、次に掲げる事項を含めること。

(ｱ)　通信回線装置の機種並びに利用しているソフトウェアの種類、名称及びバージョン、サポート体制等

(ｲ)　電気通信回線及び通信回線装置の仕様書又は設計書

(ｳ)　通信回線装置におけるアクセス制御の設定

(ｴ)　電気通信回線を利用する機器等の識別コード、サーバ等及び端末の利用者と当該利用者の識別コードとの対応

(ｵ)　電気通信回線の利用部門

エ　システムセキュリティ責任者は、対策基準第５の１(2)イ(ｳ)における警察情報システムの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について次に掲げる事項を含めること。

(ｱ)　サーバ等及び端末のセキュリティの維持に関する手順

(ｲ)　電気通信回線を介して提供するサービスのセキュリティの維持に関する手順

(ｳ)　インターネット等の外部回線経由で利用するサービスのセキュリティの維持に関する手順

(ｴ)　電気通信回線及び通信回線装置のセキュリティの維持に関する手順

(ｵ)　端末、サーバ等、通信回線装置等において利用するソフトウェアのセキュリティの維持に関する手順

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・要件定義

対策基準第５の２(1)イにおける警察情報システムのセキュリティ要件の具体的な対策について、次のとおり定める。

ア　システムセキュリティ責任者は、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル（内閣官房内閣サイバーセキュリティセンター)」を活用し、警察情報システムが提供する業務及び取り扱う情報、利用環境等を考慮した上で、脅威に対抗するために必要となるセキュリティ要件を適切に策定すること。

イ　システムセキュリティ責任者は、開発する警察情報システムが運用される際に想定される脅威の分析結果並びに当該警察情報システムにおいて取り扱う情報の分類及び取扱制限に応じて、セキュリティ要件を適切に策定し、仕様書に記載すること。

ウ　システムセキュリティ責任者は、必要に応じて、整備する警察情報システムのセキュリティ要件の設計について第三者機関によるＳＴ（Security Target：セキュリティ設計仕様書）評価・ＳＴ確認を受けること。

エ　システムセキュリティ責任者は、警察情報システム運用時の監視等の運用管理機能要件を明確化し、警察情報システム運用時に情報セキュリティ確保のために必要となる管理機能や監視のために必要な機能を仕様書に記載すること。

オ　システムセキュリティ責任者は、開発する警察情報システムに関連する脆弱性への対策が実施されるよう、次に掲げる事項を含む対策を仕様書に記載すること。

(ｱ)　既知の脆弱性が存在するソフトウェアや機能モジュールを警察情報システムの構成要素としないこと。

(ｲ)　開発時に警察情報システムに脆弱性が混入されることを防ぐためのセキュリティ実装方針を定めること。

(ｳ)　セキュリティ侵害につながる脆弱性が警察情報システムに存在することが発覚した場合に修正が施されること。

(ｴ)　ソフトウェアのサポート期間又はサポート打切り計画に関する情報提供

を行うこと。

カ　システムセキュリティ責任者は、開発する警察情報システムに意図しない不正なプログラム等が組み込まれないよう、次に掲げる事項を含む対策を実施すること。

(ｱ)　警察情報システムで利用する機器等を調達する場合は、意図しない不正なプログラム等が組み込まれていないことを確認すること。

(ｲ)　アプリケーション・コンテンツの開発時に意図しない不正なプログラム等が混入されることを防ぐための対策を講ずること。

(ｳ)　警察情報システムの構築を委託する場合は、委託先において意図しない変更が加えられないための管理体制を求めること。

キ　システムセキュリティ責任者は、要安定情報を取り扱う警察情報システムを構築する場合は、許容される停止時間に応じた次に掲げる事項を含むセキュリティ要件について、警察情報システムを構成する要素ごとに策定し、仕様書に記載すること。

(ｱ)　端末、サーバ等及び通信回線装置等の冗長化に関する要件

(ｲ)　端末、サーバ等及び通信回線装置並びに取り扱われる情報に関するバックアップの要件

(ｳ)　警察情報システムを中断することのできる時間を含めた復旧に関する要件

ク　システムセキュリティ責任者は、開発する警察情報システムのネットワーク構成に関する要件について、次に掲げる事項を含む要件を調達仕様書等に明記すること。

(ｱ)　インターネットやインターネットに接点を有する警察情報システム（クラウドサービスを含む。）から分離することの要否の判断とインターネットから分離するとした場合の要件

(ｲ)　端末、サーバ等及び通信回線装置上で利用するソフトウェアを実行するのに必要な通信要件

(ｳ)　インターネット上のクラウドサービス等のサービスを利用する場合の通信経路全般のネットワーク構成

(ｴ)　外部回線を経由して機器等に対してリモートメンテナンスすることの要

否の判断とリモートメンテナンスすることとした場合の要件

ケ　システムセキュリティ責任者は、構築する警察情報システムの構成要素のうち、製品として調達する機器等について、当該機器等に存在する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ために、次に掲げる事項を実施すること。

(ｱ)　セキュリティ要件リストを参照し、リストに掲載されている製品分野の「セキュリティ上の脅威」が自身の運用環境において該当する場合には、「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件を調達時のセキュリティ要件とすること。ただし、セキュリティ要件リストの「セキュリティ上の脅威」に挙げられていない脅威にも対抗する必要がある場合には、必要なセキュリティ要件を策定すること。

(ｲ)　セキュリティ要件リストに掲載されていない製品分野においては、調達する機器等の利用環境において対抗すべき脅威を分析し、必要なセキュリティ要件を策定すること。

(2)　警察情報システムの調達・構築時の対策

ア　システムセキュリティ責任者は、対策基準第５の２(2)アにおける情報セキュリティ対策について、次に掲げる事項を含む対策を講ずること。

(ｱ)　警察情報システム構築の工程で扱う要保護情報への不正アクセス、滅失、き損等に対処するために開発環境を整備すること。

(ｲ)　セキュリティ要件が適切に実装されるようにセキュリティ機能を設計すること。

(ｳ)　警察情報システムで使用する機器やソフトウェア等においては、設定の誤りを防止するため、提供者が提示している推奨設定や業界標準、ベストプラクティス等を参照し、警察情報システムの各種設定を行うこと。

(ｴ)　警察情報システムへの脆弱性の混入を防ぐために定めたセキュリティ実装方針に従うこと。

(ｵ)　セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビューやソースコードレビュー等を実施すること。

(ｶ)　脆弱性検査を含む情報セキュリティの観点での試験を実施すること。

(ｷ)　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すること。

イ　システムセキュリティ責任者は、対策基準第５の２(2)イにおける警察情報システムの分類について、次に掲げる場合は、警察情報システムの分類を行うこと。

(ｱ)　警察情報システムの構築又は更改が発生した場合

(ｲ)　警察情報システムで取り扱う情報に変更が発生した場合

(ｳ)　情報セキュリティ管理者から分類の再実施を指示された場合

ウ　情報セキュリティ管理者は、対策基準第５の２(2)ウにおける警察情報システムの分類の修正指示について、自組織で所管する警察情報システムの分類結果を確認し、次に掲げる例に該当する場合、報告を受けた警察情報システムの分類結果の上位への修正指示の要否を検討すること。

(ｱ)　業務特性やシステム特性、取り扱う情報等を踏まえると上位の警察情報システムの分類の適用が望ましいと判断される場合

(ｲ)　類似する自組織の警察情報システムで上位の警察情報システムの分類が適用されていた場合

エ　システムセキュリティ責任者は、対策基準第５の２(2)エにおける警察情報システムの運用保守段階に移行するに当たり、次に掲げる事項を含む情報セキュリティ対策を行うこと。

(ｱ)　情報セキュリティに関わる運用保守体制の整備

(ｲ)　運用保守要員へのセキュリティ機能の利用方法等に関わる教養の実施

(ｳ)　情報セキュリティインシデントを認知した際の対処方法の確立

オ　システムセキュリティ責任者は、対策基準第５の２(2)オにおける機器等の納入時又は警察情報システムの受入れ時の確認・検査等を実施する場合は、次に掲げる事項を含む検査を実施すること。

(ｱ)　警察情報システムの構築時に使用し、運用時に不要となる識別コードが削除されていること。

(ｲ)　機器等において初期値として設定されている主体認証情報が残っていないこと。

(ｳ)　機器等において公開された脆弱性について対策を実施していること。

(ｴ)　機器等において不要なポートが開放されていないこと。

(ｵ)　機器等において不要なサービスが起動していないこと。

(ｶ)　機器等において、利用を認めていないソフトウェアが動作していないこと。

(3)　警察情報システムの運用・保守時の対策

対策基準第５の２(3)における警察情報システムの運用・保守時の対策について、次のとおり定める。

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について、監視を行う場合には、次に掲げる事項を含む監視手順を定め、適切に監視運用すること。

(ｱ)　監視するイベントの種類や重要度

(ｲ)　監視体制

(ｳ)　監視状況の報告手順や重要度に応じた報告手段

(ｴ)　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の報告手順

(ｵ)　監視運用における情報の取扱い（機密性の確保）

イ　システムセキュリティ責任者は、所管する警察情報システムについて、外部環境が大きく変化した場合等には、次に掲げる事項を例とした確認を適宜実施し、当該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ていることを確認すること。

(ｱ)　機器等のパラメータ設定の確認

(ｲ)　物理的な設置環境の確認

(ｳ)　ネットワーク環境の確認

(ｴ)　人的な運用体制の確認

ウ　システムセキュリティ責任者は、所管する警察情報システムにおいて取り扱う管理対象情報について、当該管理対象情報の分類及び取扱制限が適切に守られていることを確認すること。

エ　システムセキュリティ責任者は、警察情報システムで不要となった識別コードや過剰なアクセス権限等の付与がないか適宜見直すこと。

オ　システムセキュリティ責任者は、運用中の警察情報システムにおいて定期的に脆弱性対策の状況を確認すること。

カ　システムセキュリティ責任者は、運用中の警察情報システムの脆弱性の存在が明らかになった場合には、情報セキュリティを確保するための措置を講ずること。

キ　対策基準第５の２(3)カにおける整備すべきドキュメント及び記録簿について、表６のとおり定める。この場合において、障害記録簿に記録されなければならない事項を作業記録簿に記録するときは、障害記録簿の作成は要しない。

表６　システム運用管理等記録簿の名称・記録事項等

記録簿等の名称	記録されなければならない事項	最低保管期間
システム・ネットワーク管理担当者指名簿	電子計算機名又は通信回線装置名 指名を受けた者の所属、官職及び氏名 担当させるシステムの範囲 指名年月日 指名解除年月日	紙媒体又は電磁的記録により当該指名が解除された日から５年
管理者権限が設定できる各ソフトウェアの管理者権限保有者名簿	ソフトウェア 指名を受けた者の所属、官職及び氏名 指名年月日 指名解除年月日	
暗号化装置の設定	鍵共有等の暗号化装置の設定 使用開始年月日	次の設定をするまでの間
管理者パスワード変更記録簿	変更年月日 変更作業者 変更した管理者パスワードに係る電子計算機、ネットワーク機器、管理者権限が設定できるソフトウェア等	紙媒体又は電磁的記録により５年
主体認証情報格納装置交付管理簿	主体認証情報格納装置を交付された者の所属及び氏名 交付の理由 交付年月日 返納年月日	

機械室等入室許可者名簿（職員）	クラス３に分類された区域に係る入室許可者の所属及び氏名 許可した年月日 許可を取り消した年月日 許可の有効期間 入室事由
機械室等入室許可者名簿（部外者）	クラス３に分類された区域に係る入室許可者の事業者名及び氏名 許可した年月日及び許可の有効期間 入室許可証の交付年月日及び返納年月日 許可取消した年月日 入室事由
フィルタリング等設定表	ファイアウォール、ＩＤＳ等、ルータ、スイッチングハブ等の名称及び型番、設置場所 設定の内容（ＩＰアドレス、ＭＡＣアドレス、（対象とするネットワーク機器の通過を許可するパケット又は許可しないパケットを送信元又は送信先により設定した内容等）
入退室管理簿 （入退室の記録が自動的に収集できない場合）	入退室者の所属及び氏名 入室年月日時分 退室年月日時分 （部外者の場合）立会者の氏名
障害記録簿	障害を認知した年月日 認知した者の所属及び氏名 障害の内容 対処した者の所属及び氏名 対処の内容
作業記録簿	作業年月日

	作業を行った者の所属及び氏名 作業の依頼元及び作業の概要 管理者権限によりログインした場合はそのサーバ等の名称及びログ等の確認結果	
システム設定等変更記録簿（クラス３に分類された区域内の装置ごと）	作業年月日 設定変更の依頼元・設定変更の内容 作業を行った者の所属及び氏名	
機械室物品の持ち出し記録簿	クラス３に分類された区域内の機器に係る持ち出した者の所属、官職及び氏名 持ち出しの理由 持ち出した物の名称 持ち出し年月日 返戻年月日	
機器等管理台帳（システム構成図及び電気通信回線系統図を含む。）	機器等の名称、型番及び設置年月日 設置場所、ＩＰアドレス及びＭＡＣアドレス、ホスト名等機器等を特定するのに必要となる情報 アクセス制限等があるときはその内容 インストールされているソフトウェア	紙媒体又は電磁的記録により該当するシステムの使用終了後５年
プログラム関係のドキュメント	ソースコード 設計レビュー及びソースコードレビューの結果 試験結果	当該プログラムの利用を終了するまでの間

ク　システム管理担当者は、警察情報システムに係るドキュメント及び記録簿について、事務に関係のない者は、閲覧できないように保管すること。また、原本の保管その他記載されている記録の完全性を担保する以外の目的で複写しないこと。

ケ　システム管理担当者は、クラス３に指定された区域に設置されている警察

情報システムを構成する機器、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、その状況を記録すること。

コ　ネットワーク管理担当者は、担当する通信回線装置について、データ伝送に関する監視及び制御を行うこと。

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警察情報システムについて、次に掲げる事項を含む運用をすること。

(ｱ)　警察情報システムの各構成要素及び取り扱われる管理対象情報に関する適切なバックアップの取得及びバックアップ要件の確認による見直し

(ｲ)　警察情報システムの構成や設定の変更等が行われた際及び定期的に、警察情報システムが停止した際の復旧手順の確認による見直し

(4)　警察情報システムの更改・廃棄時の対策

対策基準第５の２(4)における警察情報システムの更改・廃棄時の対策について、次のとおり定める。

ア　システム管理担当者は、警察情報システムの構成の変更等の作業（軽微なものを除く。）を行う場合において、情報セキュリティの観点から、あらかじめその影響を確認するとともに、その作業を監視し、必要な対応を行うこと。

イ　ネットワーク管理担当者は、ネットワークの構成の変更等の作業（軽微なものを除く。）を行う場合において、情報セキュリティの観点から、あらかじめその影響を確認するとともに、その作業を監視し、必要な対応を行うこと。

３　警察情報システムの業務継続計画の整備・整合的運用の確保

対策基準第５の３(3)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、次のとおり定める。

(1)　情報セキュリティ管理者は、情報セキュリティに係る対策事項及び実施手順が運用可能であるか確認するため、次の事項を例とする訓練の実施を検討すること。

ア　警察情報システム復旧訓練

イ　警察情報システム切替え訓練

ウ　実施手順書確認訓練

エ　シナリオ非提示型訓練

(2)　情報セキュリティ管理者は、次に掲げる事項を踏まえ、情報セキュリティに係る対策事項及び実施手順を見直すこと。

ア　危機的事象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が運用可能であるかの確認結果

イ　危機的事象発生時の対処結果

ウ　警察情報システムの構成や利用環境、利用方法、取り扱う管理対象情報の変化

第５　警察情報システムの構成要素

１　端末・サーバ等

(1)　端末

ア　端末の導入時の対策

(ｱ)　対策基準第６の１(1)ア(ｱ)における物理的な脅威から保護するための対策について、次のとおり定める。

ａ　モバイル端末及び支給携帯電話機を除く端末については、原則としてクラス２以上に指定された区域に設置すること。

ｂ　物理的に持ち出しが困難であるもの、鍵のかかる保管庫やクラス３に保管しているもの及び管理対象情報を保存できないようにするための機能を設けたものを除き、全ての端末にセキュリティワイヤを取り付けること。

ｃ　15分間操作のない状態が続くと再び主体認証を求める機能を設けること。また、当該設定は一般利用者の権限では変更できないようにすること。ただし、特定の業務を行うための端末であって、即時の対応を求められるなど主体認証の失敗による操作の遅れが職務遂行に当たって非常に大きな妨げとなるおそれのあるものについては、この機能を適用しないことができる。このとき、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。

(a)　当該端末が、許可された者以外は立ち入ることができない執務室等に設置されていること。

(b)　許可された者が常駐する、許可された者が不在となる際は当該端末が設置された執務室等を施錠するなど、当該端末の不正操作が困難な環境が整えられていること。

(c)　のぞき見防止フィルタを取り付けるなど、当該端末の画面が、部外者から視認することができない措置が講じられていること。

(d)　このほか、不正な利用を防ぐための代替措置等、当該端末の情報セキュリティ確保に関し必要な事項を定めた規程を策定し、当該規程に基づく運用を徹底すること。

d　設置環境を踏まえ、必要に応じて画面に視野角を制限するのぞき見防止フィルタを取り付けること。

(ｲ)　対策基準第６の１(1)ア(ｲ)における端末で利用を認めるソフトウェアについては、次に掲げる事項を考慮した上で、ソフトウェアのバージョンも含め定めること。

なお、特定の業務や端末のみに利用を認めるなどの条件を付す場合は、その旨を含めること。

a　ソフトウェアベンダ等のサポート状況

b　ソフトウェアと外部との通信の有無及び通信する場合は、プロトコル（バージョンを含む。）、使用するポート、暗号化の有無

c　インストール時に同時にインストールされる他のソフトウェア

d　その他、ソフトウェアの利用に伴う情報セキュリティリスク

イ　端末の運用時の対策

(ｱ)　対策基準第６の１(1)イ(ｱ)における端末で利用を認めるソフトウェアの見直しについては、職員からの利用申請を受けて利用の適否を判断した結果等を反映すること。

(ｲ)　対策基準第６の１(1)イ(ｴ)における確認、分析の結果、不適切な状態にある端末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すること。また、対処の結果については速やかにシステムセキュリティ責任者に報告すること。

ウ　対策基準第６の１(1)エにおけるモバイル端末及び支給携帯電話機の導入及び利用時の対策について、次のとおり定める。

(ｱ) モバイル端末

a 庁舎外で使用するモバイル端末については、盗み見されるおそれがある場合に、画面に視野角を制限するのぞき見防止フィルタを取り付けるなどの対策を講ずること。

b 盗難等の際に第三者により情報窃取されることを防止するため、モバイル端末に保存される管理対象情報を暗号化するため次に掲げるいずれかの機能を設けること。

(a) モバイル端末にハードディスク等の内蔵された電磁的記録媒体を暗号化する機能を設ける。

(b) モバイル端末にファイルを暗号化する機能を設ける。

(c) タブレット端末等を使用する場合、高度なセキュリティ機能（電磁的記録媒体全体を自動的に暗号化する機能又は電磁的記録媒体に保存されている情報を遠隔からの命令等により暗号化消去する機能等）を備えたＯＳを搭載するものを使用する。

c モバイル端末の盗難・紛失が発生した際の緊急対応手順を設けること。

d 外部回線に接続するモバイル端末は、次に掲げる事項を例とする、利用者が当該端末に管理対象情報を保存できないようにするための機能を設けること。

(a) シンクライアント等の仮想デスクトップ技術を活用した、モバイル端末に管理対象情報を保存させないリモートアクセス環境を構築する。

(b) セキュアブラウザ等を活用した、モバイル端末に管理対象情報を保存させないリモートアクセス環境を構築する。

(c) ファイル暗号化等のセキュリティ機能を持つアプリケーションを活用したリモートアクセス環境を構築する。

(d) ハードディスク等の内蔵された電磁的記録媒体に保存されている管理対象情報を遠隔から暗号化消去する機能（遠隔データ消去機能）を設ける。

e モバイル端末であることが判別できる目印を貼付するなどして、他の

電子計算機との混同を防止するための措置を講ずること。

f　モバイル端末に別表に示す対策を講ずること。

g　要機密情報を取り扱わないモバイル端末については、ａ、ｂ、ｄ及び第６の１(1)ア(ｲ)の規定を適用しない。

h　内蔵された電磁的記録媒体に要機密情報を保存しないモバイル端末については、ｂの規定を適用しない。また、一定回数以上主体認証に失敗した際及び遠隔操作により、認証を不能とする機能を設けることにより、第６の１(1)ア(ｲ)の規定を適用しないことができる。

ｉ 外部回線に接続したモバイル端末を内部ネットワークに接続する場合は、当該端末から内部ネットワークを経由して警察情報システムが不正プログラムに感染することを防止するための対策を講ずること。

(ｲ)　支給携帯電話機

a　庁舎外で使用する際等、盗み見されるおそれがある場合に、画面に視野角を制限するのぞき見防止フィルタを取り付けるなどの対策を講ずること。

b　盗難等の際に第三者により情報の窃取されることを防止するため、技術的に困難である場合を除き、次に掲げるいずれかの機能を設けること。

(a)　支給携帯電話機に内蔵された電磁的記録媒体を暗号化する機能

(b)　支給携帯電話機にファイルを暗号化する機能

c　スマートフォンを使用する場合、可能な限り高度なセキュリティ機能（電磁的記録媒体全体を自動的に暗号化する機能又は電磁的記録媒体に保存されている情報を遠隔からの命令等により暗号化消去する機能等）を備えたＯＳを搭載するものを使用すること。

d　可能な限り、支給携帯電話機の紛失時に当該携帯電話機をロックするサービスを契約すること。

e　支給携帯電話機の盗難・紛失が発生した際の緊急対応手順を設けること。

f　支給携帯電話機においては、情報セキュリティ管理者の許可を受けた場合を除き、移動通信事業者が提供する移動通信サービスを使用すること。

g　支給携帯電話機において外部回線を用いた電子メール機能等を使用する場合は、移動通信事業者が提供する外部回線を使用し、公衆無線ＬＡＮ（移動通信事業者が提供するものを除く。）等の外部回線を使用しないこと。

h　支給携帯電話機（音声通話機能のみを使用する場合を除く。）に別表に示す対策を講ずること。

i　要機密情報を取り扱わない、又は音声通話機能のみを使用する支給携帯電話機については、ａ、ｂ、ｃ、ｇ及び対策基準第７の２(2)アに掲げる規定を適用しない。

(2)　サーバ等

ア　サーバ等の導入時の対策

対策基準第６の１(2)アにおけるサーバ等の導入時の対策について、次のとおり定める。

(ｱ)　サーバ等については、原則としてクラス３に指定された区域に設置すること。ただし、機密性１（低）情報のみを取り扱うサーバ等にあっては、クラス２に指定された区域に設置することができる。

(ｲ)　サーバ等の導入時の対策は、(1)ア(ｱ)ｂ、ｃ及びｄを準用する。

(ｳ)　(ｱ)においてクラス３に設置することと定められたサーバ等のうち、重要度（中）又は（低）システムであり、次に掲げる事項を満たすものについては、クラス２に指定された区域に設置することができる。

a　サーバ等を施錠可能なラック等で管理すること。

b　ラック扉の開閉を行う者の氏名とその開閉時の時刻を記録すること。また、当該記録については、クラス３の区域に係る入退室管理簿と同様に管理を行うこと。

c　第６の１(4)ウ及び２(5)に定める外部記録媒体の利用に係る要件を満たすこと。

d　運用要領等において、管理手順等を定めること。

(ｴ)　対策基準第６の１(2)ア(ｳ)における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

の対策について、次に掲げる事項を例とする対策を講ずること。

a　リモートメンテナンス端末の機器番号等の識別コードによりアクセス制御を行う。

b　主体認証によりアクセス制御する。

c　通信内容の暗号化により秘匿性を確保する。

d　ファイアウォール等の通信制御のための機器に例外的な設定を行う場合には、その設定により脆弱性が生じないようにする。

(ｵ)　対策基準第６の１(2)ア(ｱ)において準用する対策基準第６の１(1)ア(ｲ)に基づくサーバ等で利用を認めるソフトウェアについては、次に掲げる事項を考慮した上で、ソフトウェアのバージョンも含め定めること。

なお、特定の業務やサーバ等のみに利用を認めるなどの条件を付す場合は、その旨を含めること。

a　ソフトウェアベンダ等のサポート状況

b　ソフトウェアと外部との通信の有無及び通信する場合は、プロトコル（バージョンを含む。）、使用するポート、暗号化の有無

c　インストール時に同時にインストールされる他のソフトウェア

d　その他、ソフトウェアの利用に伴う情報セキュリティリスク

イ　サーバ等の運用時の対策

対策基準第６の１(2)イにおけるサーバ等の運用時の対策について、次のとおり定める。

(ｱ)　システムセキュリティ責任者は、要保全情報に係るサーバ等のバックアップについては、必要に応じて、一定の期間ごとに、当該サーバ等から離れた場所に移して保管すること。

(ｲ)　対策基準第６の１(2)イ(ｱ)において準用する対策基準第６の１(1)イ(ｴ)に基づく確認、分析の結果、不適切な状態にあるサーバ等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すること。また、対処の結果については速やかにシステムセキュリティ責任者に報告すること。

(ｳ)　システムセキュリティ責任者は、要保全情報又は要安定情報に係るサーバ等については、定期的にバックアップを取得すること。

(ｴ)　システムセキュリティ責任者は、要安定情報に係るサーバ等については、障害に備えて、次に掲げる事項をあらかじめ定め、適切に見直しを行うこと。

a　障害発生の認知からシステムセキュリティ責任者への報告の方法

b　応急措置の方法

c　ログの保存の方法

d　データのバックアップの方法

e　復旧の手順

f　保守業者等への連絡手続

(ｵ)　システムセキュリティ責任者は、クラス３の区域に設置された要機密情報に係るサーバ等及びそのバックアップをクラス２以下の区域に持ち出し、又はクラス２以下の区域に設置された電子計算機に要機密情報を送信する場合には、暗号化すること。また、クラス２の区域に設置された要機密情報に係るサーバ等及びそのバックアップを、設置された区域から持ち出す場合には、要機密情報を暗号化すること。

(ｶ)　サーバ等のバックアップを取得する場合は、第７の１(2)カ(ｳ) f の規定を適用しない。

(3)　複合機・特定用途機器

ア　複合機

対策基準第６の１(3)アにおける複合機について、次のとおり定める。

(ｱ)　システムセキュリティ責任者は、複合機について、利用環境に応じた適切なセキュリティ設定を行うこと。

(ｲ)　システムセキュリティ責任者は、複合機が備える機能のうち利用しない機能を停止すること。

(ｳ)　システムセキュリティ責任者は、印刷された書面の取り忘れ等により他者に閲覧等される場合には、複合機が備える操作パネルで主体認証が成功した者のみ印刷が許可される機能等を活用すること。

(ｴ)　システムセキュリティ責任者は、複合機をインターネットに直接接続しないこと。

(ｵ)　システムセキュリティ責任者は、リモートメンテナンス等の目的で複合

機がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行うこと。

(ｶ) システムセキュリティ責任者は、利用者ごとに許可される操作を適切に設定すること。

(ｷ) 対策基準第６の１(3)ア(ｳ)に基づき、運用を終了する複合機が管理対象情報を抹消するための機能を備えていない場合は、委託先との契約時に委託先に複合機内部に保存されている管理対象情報の漏えいが生じないための対策を講じさせることを契約内容に含むようにするなどの別の手段で対策を講ずること。

イ　ＩｏＴ機器を含む特定用途機器

対策基準第６の１(3)イにおける特定用途機器について、次のとおり定める。ただし、特定用途機器の機能上の制約により講ずることができない対策を除く。

(ｱ) 主体認証情報を初期設定から変更した上で、適切に管理すること。

(ｲ) 特定用途機器にアクセスする主体に応じて必要な権限を付与し、管理すること。

(ｳ) 特定用途機器が備える機能のうち利用しない機能は停止すること。

(ｴ) インターネットと通信を行う必要のない特定用途機器については、当該特定用途機器をインターネットに接続させず、インターネットに接点を有する情報システムに接続する場合は、当該特定用途機器がインターネットに接続されないように適切に通信制御を行うこと。

(ｵ) 特定用途機器がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行うこと。

(ｶ) 特定用途機器のソフトウェアに関する脆弱性の有無を確認し、脆弱性が存在する場合は、バージョンアップ、セキュリティパッチの適用、アクセス制御等の対策を講ずること。

(ｷ) 特定用途機器に対する不正な行為、無許可のアクセス等の意図しない事象の発生を監視すること。

(ｸ) 使用しない場合は電源をオフにすること。

(ｹ) 廃棄する場合は、内蔵された電磁的記録媒体に保存されている全ての情

報を抹消すること。

(ｺ) 庁舎外で使用する場合は、利用環境に応じて、特定用途機器に対する不正な行為等の防止対策を講ずること。

(ｻ) 特定用途機器を他の警察情報システムと接続する場合には、当該警察情報システムのシステムセキュリティ責任者と調整し、警察情報システムの情報セキュリティを維持できるよう必要な対策を講ずること。

(ｼ) 特定用途機器のうち、電子計算機としても使用できるものについては、別表に示す対策を講ずること。機能要件上、技術的要件を満たすことができないものについては、情報セキュリティ管理者と協議の上、代替措置を講ずるなどして情報セキュリティ上の対策を講ずること。

(ｽ) 特定用途機器について、利用環境に応じた適切なセキュリティ設定を行うこと。

2 電子メール・ウェブ等

(1) 電子メール

ア 対策基準第６の２(1)イにおける主体認証を行う機能について、電子メールの受信時に限らず、送信時においても不正な利用を排除するためにＳＭＴＰ認証等の主体認証機能を導入すること。

イ 対策基準第６の２(1)ウにおけるなりすましの防止策について、次のとおり定める。

(ｱ) 送信ドメイン認証技術による次に掲げる防止策を講ずること。

a ＤＭＡＲＣによる送信側の対策を行うこと。ＤＭＡＲＣによる送信側の対策を行うためには、ＳＰＦ、ＤＫＩＭのいずれか又は両方による対策を行う必要がある。

b ＤＭＡＲＣによる受信側の対策を行うこと。ＤＭＡＲＣによる受信側の対策を行うためには、ＳＰＦ、ＤＫＩＭの両方による対策を行う必要がある。

(ｲ) 必要に応じて、Ｓ／ＭＩＭＥ等の電子メールにおける電子署名の技術による防止策を講ずること。

(ｳ) 職員が自組織外の者と電子メールを送受信する場合には、政府ドメイン

名を取得できない場合を除き、政府ドメイン名を使用した電子メールアドレスが利用される機能を備えること。

ウ　対策基準第６の２(1)エにおける暗号化について、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、次に掲げる事項を例とする電子メールに関する通信の暗号化を行うこと。

(ｱ)　ＳＭＴＰによる電子メールサーバ間の通信をＴＬＳにより保護する。

(ｲ)　Ｓ／ＭＩＭＥ等の電子メールにおける暗号化及び電子署名の技術を利用する。

(2)　ウェブ

対策基準第６の２(2)における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の導入・運用時の対策について、次のとおり定める。

ア　システムセキュリティ責任者は、ウェブサーバが備える機能のうち、必要な機能のみを利用するために、次に掲げる事項を含むウェブサーバの管理や設定を行うこと。

(ｱ)　ＣＧＩ機能を用いるスクリプト等は必要最低限のものに限定し、ＣＧＩ機能を必要としない場合は設定でＣＧＩ機能を使用不可とする。

(ｲ)　ディレクトリインデックスの表示を禁止する。

(ｳ)　ウェブコンテンツ作成ツールやコンテンツ・マネジメント・システム（ＣＭＳ）等における不要な機能を制限する。

(ｴ)　ウェブサーバ上で動作するソフトウェアは、最新のものを利用するなど、既知の脆弱性が解消された状態を維持する。

イ　システムセキュリティ責任者は、ウェブサーバからの不用意な情報漏えいを防止するために、次に掲げる事項を含むウェブサーバの管理や設定を行うこと。

(ｱ)　公開を想定していないファイルをウェブ公開用ディレクトリに置かない。

(ｲ)　初期状態で用意されるサンプルのページ、プログラム等、不要なものは削除する。

(ｳ)　ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認する。

(ｴ)　ウェブクライアントに攻撃の糸口になり得る情報を送信しないよう設定すること。

ウ　システムセキュリティ責任者は、ウェブコンテンツの編集作業を行う主体の限定として、次に掲げる事項を含むウェブサーバの管理や設定を行うこと。

(ｱ)　ウェブサーバ上のウェブコンテンツへのアクセス権限は、ウェブコンテンツの作成や更新に必要な者以外に更新権を与えない。

(ｲ)　ＯＳやアプリケーションのインストール時に標準で作成される識別コードやテスト用に作成した識別コード等、不要なものは削除する。

エ　システムセキュリティ責任者は、通信時の盗聴による第三者への情報の漏えい及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするための措置として、次に掲げる事項を含むウェブサーバの実装を行うこと。

(ｱ)　ＴＬＳ機能を適切に用いる。

(ｲ)　ＴＬＳ機能のために必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いる。

(ｳ)　暗号技術検討会及び関連委員会（ＣＲＹＴＲＥＣ）により作成された「ＴＬＳ暗号設定ガイドライン」に従って、ＴＬＳサーバを適切に設定する。

オ　システムセキュリティ責任者は、利用者が、ウェブクライアントの情報セキュリティレベル設定を低下させることなく利用できるようにすること。

カ　システムセキュリティ責任者は、公開する必要がなくなったウェブサイトは閉鎖し、また、利用しないポートは閉鎖すること。

(3)　ドメインネームシステム（ＤＮＳ）

ア　ＤＮＳの導入時の対策

(ｱ)　対策基準第６の２(3)ア(ｱ)における名前解決を停止させないための措置について、次に掲げる事項を例とする措置を講ずること。

ａ　コンテンツサーバを冗長化する。

b　通信回線装置等で、コンテンツサーバへのサービス不能攻撃に備えたアクセス制御を行う。

c　ＩＳＰ等が提供するマネージドＤＮＳサービスやＤＤｏＳ（Distributed Denial of Servic）対策サービスを利用する。

d　ＵＤＰ及びＴＣＰの両方でサービスを提供する。

(ｲ)　対策基準第６の２(3)ア(ｲ)における名前解決の要求への適切な応答をするための措置について、自組織外からの名前解決の要求に応じる必要性がないと判断される場合は、自組織内からの名前解決の要求のみに応答をするよう、次に掲げる事項を例とする措置を講ずること。

a　キャッシュサーバの設定でアクセス制御を行う。

b　ファイアウォール等でアクセス制御を行う。

(ｳ)　対策基準第６の２(3)ア(ｲ)における名前解決の要求への適切な応答をするための措置について、ＤＮＳキャッシュポイズニング攻撃から保護するため、次の事項を例とする措置を講ずること。

a　ソースポートランダマイゼーション機能を導入する。

b　ＤＮＳＳＥＣを利用する。

(ｴ)　対策基準第６の２(3)ア(ｳ)における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について、次の事項を例とする措置を講ずること。

a　外部向けのコンテンツサーバと別々に設置する。

b　ファイアウォール等でアクセス制御を行う。

イ　ＤＮＳの運用時の対策

対策基準第６の２(3)イ(ｳ)における名前解決の要求への適切な応答を維持するための措置について、次のとおり定める。

(ｱ)　キャッシュサーバにおいて、ルートヒントファイル（ＤＮＳルートサーバの情報が登録されたファイル）の更新の有無を定期的に確認し、最新のＤＮＳルートサーバの情報を維持すること。

(ｲ)　キャッシュサーバにおいてＤＮＳＳＥＣを利用する場合、電子署名を検証する起点となるＤＮＳＳＥＣトラストアンカーを最新の状態に保つため、自動更新機能を有効にする又は更新の有無を定期的に確認すること。

(4)　データベース

対策基準第６の２(4)におけるデータベースの導入・運用時の対策について、次のとおり定める。

ア　システムセキュリティ責任者は、必要に応じて、警察情報システムの管理者権限を付与する職員とデータベースの管理者権限を付与する職員を別の者にすること。

イ　システムセキュリティ責任者は、管理者権限を付与された職員のうち、データベースに格納されているデータにアクセスする必要のない者に対して、データへのアクセス権を付与しないこと。

ウ　システムセキュリティ責任者は、データベースの管理に関する権限の不適切な付与を検知できるよう、措置を講ずること。

エ　システムセキュリティ責任者は、職務を遂行するに当たって不必要なデータの操作を検知できるよう、次に掲げる事項を例とする措置を講ずること。

(ｱ)　一定数以上のデータの取得に関するログを記録し、警告を発する。

(ｲ)　データを取得した時刻が不自然であるなど、通常の職務によるデータベースの操作から逸脱した操作に関するログを記録し、警告を発する。

オ　システムセキュリティ責任者は、データベースにアクセスする機器上で動作するプログラムに対して、ＳＱＬインジェクションの脆弱性を排除すること。必要に応じて、次に掲げる事項を例とする対策の実施を検討すること。

(ｱ)　ウェブアプリケーションファイアウォールの導入

(ｲ)　データベースファイアウォールの導入

カ　システムセキュリティ責任者は、データベースに格納されているデータに対して暗号化を実施する場合には、バックアップデータやトランザクションデータ等についても暗号化を実施すること。

３　電気通信回線

(1)　電気通信回線の導入時の対策

対策基準第６の３(1)アにおける電気通信回線の導入時の対策について、次のとおり定める。

ア　システムセキュリティ責任者は、警察情報システムで用いる電気通信回線については、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)　権限のない者又は権限のない電子計算機が当該回線を使用できないこと。

(ｲ)　権限のない者が当該接続に関する設定変更を行えないこと。

(ｳ)　利用する用途に応じて、帯域保証、不通の際の事前連絡等、可用性を確保するための措置が講じられていること。

(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には、当該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、当該事業者と契約時に取り決めておくこと。

(ｵ)　機能要件上必要がある場合を除き、他のシステムと論理的に接続しないこと。

イ　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(庁舎内有線回線を除く。）にあっては、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)　論理的に警察以外の機関と接続していない閉域網であること（警察以外の機関と要機密情報を送受信するために外部回線と接続された警察情報システムであって、論理的に他の情報システムと分離している場合を除く。以下同じ。)。

(ｲ)　システムセキュリティ責任者は、通信経路における盗聴及び情報の改ざん等の脅威への対策として、通信内容の秘匿性を確保するための機能を設けること。電気通信回線の秘匿性確保の方法として、ＴＬＳ、ＩＰｓｅｃ等による暗号化を行うこと。また、その際に使用する暗号アルゴリズム及び鍵長については､「電子政府推奨暗号リスト」を参照し決定すること。

(ｳ)　外部からの侵入等の現実的な脅威がないこと。

(ｴ)　端末認証の記録を取得し、適正に管理すること（専用回線等、端末認証が不要である場合を除く。)。

ウ　システムセキュリティ責任者は、内部ネットワークへの接続を許可された警察情報システムであることを確認し、無許可の情報システムが当該内部ネットワークに接続することを拒否するための機能として、対策を講ずること。

(ｱ)　当該警察情報システムのＭＡＣアドレス等の端末を一意に識別できる情

報により接続機器を識別する。

(ｲ)　クライアント証明書により接続機器の主体認証を行う。

エ　システムセキュリティ責任者は、電気通信回線を暗号化する装置については、次の事項を満たすこと。

(ｱ)　当該装置は、クラス３に分類された区域に設置すること。ただし、次に掲げる事項を満たす場合はクラス２又はクラス１に設置することができる。

ａ　破壊、取り外し、入替え等が検知できること。

ｂ　容易に取り外し等ができないように固定されていること。

ｃ　不要な接続口を塞ぐなど不正な接続を防止する措置が講じられていること。

ｄ　暗号に係る設定等の情報が不正に抽出できない仕組みとなっていること。

(ｲ)　(ｱ)において、クラス３以外に重要度（高）システムに係る暗号化装置を設置する際には、(ｱ)に掲げる事項を満たしていることについて警察庁情報セキュリティ管理者の確認を受けること。

(ｳ)　当該装置は、筐体の開閉、内部回路の入れ替え等情報セキュリティの侵害のおそれがある事案があった場合において､そのログを残す機能を有し、又は封印シールを貼付するなどの措置が講じられていること。

オ　システムセキュリティ責任者は、電気通信回線に接続された警察情報システムについては、サイバー攻撃に備えて、必要に応じて、管理対象情報の漏えい、管理対象情報の改ざん、なりすまし、標的型攻撃、サービス不能攻撃等を防ぐため、暗号装置、ファイアウォール、ウェブアプリケーションファイアウォール、リバースプロキシ、通信回線装置による特定の通信プロトコルの利用の制限、ＩＤＳ／ＩＰＳ等による対策を講ずること。

カ　対策基準第６の３(1)ア(ｹ)における遠隔地から通信回線装置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について、次に掲げる事項を例とする対策を講ずること。

(ｱ)　リモートメンテナンス端末の機器番号等の識別コードによりアクセス制御を行う。

(ｲ)　主体認証によりアクセス制御する。

(ｳ)　通信内容の暗号化により秘匿性を確保する。

(ｴ)　ファイアウォール等の通信制御のための機器に例外的な設定を行う場合には、その設定により脆弱性が生じないようにする。

キ　システムセキュリティ責任者は、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、個人情報又は機密性３（高）情報が保存されたサーバ等と接続された警察情報システムにあっては、無線回線（携帯電話回線（事業者閉域網のものに限る。）を除く。）を利用しないこと。

(2)　外部回線の接続時の対策

対策基準第６の３(1)イにおける外部回線の接続時の対策について、次のとおり定める。

ア　システムセキュリティ責任者は、内部ネットワークに、インターネット回線や公衆通信回線等の外部回線を接続する場合には、外部からの不正アクセスによる被害を防止するため､次に掲げる事項を例とする対策を講ずること。

(ｱ)　ファイアウォール、ＷＡＦ、プロキシやリバースプロキシ、次世代ファイアウォール等により通信制御を行う。

(ｲ)　通信回線装置による特定の通信プロトコルの利用を制限する。

(ｳ)　ＩＤＳ／ＩＰＳにより不正アクセスを検知及び遮断する。

(ｴ)　不審なメールの受信や不審なウェブサイトへのアクセスを遮断する。

(ｵ)　サンドボックス型の標的型攻撃対策をする。

イ　インターネット回線等の外部回線を用いたクラウドサービスへのアクセスがある場合、クラウドサービスへのアクセスを可視化し、適切な利用を把握するための対策を検討すること。

ウ　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警察庁が整備したサーバ等に接続された内部ネットワークの不正な通信の有無を監視するため、次に掲げる事項について、監視を行うこと。

(ｱ)　自組織外と電気通信回線で接続している箇所における外部からの不正アクセスの監視

(ｲ)　不正プログラム感染や踏み台に利用されること等による自組織外への不正な通信の監視

(ｳ)　不正プログラム等の感染による拡大防止のため、警察庁が整備したサーバ等に接続された内部ネットワークに接続された機器等における不審な通信の監視

エ　システムセキュリティ責任者は、特定した監視対象について、監視方法及び監視記録の保存期間を定め、監視記録を保存し、適切に保護、管理すること。

オ　システムセキュリティ責任者は、外部回線からの保守又は診断のためのリモートメンテナンスを必要と認める場合は、セキュリティ確保のために、次に掲げる事項を含む対策を講ずること。

(ｱ)　リモートメンテナンスを行う主体の認証において多要素主体認証を行う。

(ｲ)　リモートメンテナンスを行う端末等を制限するアクセス制御を行う。

(ｳ)　主体認証によるアクセス制御を行う。

(ｴ)　通信内容の暗号化により秘匿性を確保する。

(ｵ)　ファイアウォール等の通信制御のための機器に例外的な設定を行う場合は、その設定により脆弱性が生じないように措置する。

(3)　電気通信回線の運用時の対策

対策基準第６の３(1)ウにおける電気通信回線の運用時の対策について、次のとおり定める。

ア　システムセキュリティ責任者は、要安定情報を取り扱う警察情報システムを構成する通信回線装置については、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すること。

イ　対策基準第６の３(1)ウ(ｲ)において準用する対策基準第６の１(1)イ(ｴ)に基づく確認、分析の結果、不適切な状態にある通信回線装置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すること。また、対処の結果については速やかにシステムセキュリティ責任者に報告すること。

ウ　システムセキュリティ責任者は、外部回線から保守又は診断のためのリモートメンテナンスに関する次に掲げる事項について、定期的な確認による見直しを行うこと。

(ｱ)　リモートからのアクセスが必要な主体

(ｲ)　リモートメンテナンスを行う端末

(ｳ)　ファイアウォール等の通信制御のための機器に例外的な設定を行った場合の設定

(4)　通信回線装置

対策基準第６の３(2)における通信回線装置の対策について、システムセキュリティ責任者は、３(1)エ(ｱ)を例とする対策を講ずること。

(5)　無線ＬＡＮ環境導入時の対策

対策基準第６の３(3)における無線ＬＡＮ技術を利用して電気通信回線を構築する場合は、要保護情報を送受信する無線ＬＡＮ回線は、次に掲げる事項を満たしていることについて警察庁情報セキュリティ管理者の確認を受けること。

なお、ウ及びエについては、WPA2-Enterprise又はWPA3-Enterprise相当の機能により実現すること。また、エ及びオについては、当該事項が担保されるよう、必要に応じて、管理外の無線ＬＡＮ装置及び端末がないかどうか確認すること。

ア　無線ＬＡＮ装置の出力を必要最小限に調整し、可能な限り電波を外部に漏えいさせないこと。また、不要時には無線ＬＡＮ装置の出力を停止すること。

イ　論理的に警察以外の機関と接続していない閉域網であること。

ウ　通信の暗号化を適切に行うこと。

エ　あらかじめ定めた以外の端末が接続されないように、端末認証の記録を取得し、適正に管理すること。

オ　端末が、あらかじめ定めた以外の無線ＬＡＮ装置に接続されないこと。

カ　庁舎外で利用する場合においては、次に掲げる対策を講ずること。

(ｱ)　警察庁情報セキュリティ管理者の許可を受けること。

(ｲ)　他のシステムと論理的に接続していないこと。

(ｳ)　一時的に利用する回線であること。

(ｴ)　次に掲げる事項を例としたアからオの代替となる対策を講ずること。

a　IEEE 802.1xにより無線ＬＡＮへのアクセス主体を認証する。

b　無線ＬＡＮ装置のＳＳＩＤ及びＰＳＫを使用のたびに変更する。

c　暗号化の方式として、脆弱なものを使用しない。

d　無線ＬＡＮ装置と機器等との接続を行う際に、想定外の機器等と接続がなされていないかを確認する。

e　自動接続を行う設定とする場合には、ＰＳＫをネットワーク管理担当者が管理し利用者に通知しない。

f　公衆無線ＬＡＮのアクセスポイント等、警察が管理していない無線ＬＡＮアクセスポイントへの接続を禁止する。

4　警察情報システムの基盤を管理又は制御するソフトウェア

(1)　対策基準第６の４(2)アにおけるソフトウェアの情報セキュリティを維持するための対策として、権限設定やアクセス制御、セキュリティ設定が適切であるか定期的に確認すること。

(2)　対策基準第６の４(2)イにおける脅威や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として、次に掲げる対策を実施すること。

ア　警察情報システムの基盤を管理又は制御するソフトウェアの利用のための情報セキュリティ水準の維持に関する手順に基づく教養の実施

イ　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に基づく訓練

5　アプリケーション・コンテンツ

(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

対策基準第６の５(1)アのセキュリティ要件については、次に掲げる事項を含めること。

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　自組織外に提供するアプリケーションに、アプリケーションの仕様に反するプログラムコードが含まれていないことを確認すること。

ウ　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ように開発すること。

エ　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。

オ　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をアプリケーション・

コンテンツの提供先に与えること。

カ　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や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や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。

キ　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、次に掲げる事項を仕様に含め開発すること。

(ｱ)　自組織外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことをＨＴＭＬソースを表示させるなどして確認すること。必要があって当該機能を含める場合は、自組織外のウェブサイト等のサーバへのアクセスが情報セキュリティ上安全なものであることを確認すること。

(ｲ)　本来のサービス提供に必要のない自組織外へのアクセスを自動的に発生させる機能を含めないこと。

(2)　ウェブアプリケーションの開発時の対策

対策基準第６の５(2)におけるウェブアプリケーションの開発時の対策について、次のとおり定める。

ア　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開発において、次に掲げる事項を含む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。

(ｱ)　ＳＱＬインジェクション脆弱性

(ｲ)　ＯＳコマンドインジェクション脆弱性

(ｳ)　ディレクトリトラバーサル脆弱性

(ｴ)　セッション管理の脆弱性

(ｵ)　アクセス制御欠如と認可処理欠如の脆弱性

(ｶ)　クロスサイトスクリプティング脆弱性

(ｷ)　クロスサイトリクエストフォージェリ脆弱性

(ｸ)　クリックジャッキング脆弱性

(ｹ)　メールヘッダインジェクション脆弱性

(ｺ)　ＨＴＴＰヘッダインジェクション脆弱性

(ｻ)　ｅｖａｌインジェクション脆弱性

(ｼ)　レースコンディション脆弱性

(ｽ)　バッファオーバーフロー及び整数オーバーフロー脆弱性

(ｾ) サーバサイドリクエストフォージェリ（ＳＳＲＦ）脆弱性

イ　システムセキュリティ責任者は、ウェブアプリケーションを運用段階に移行する前に警察情報システムの分類に基づき、開発したウェブアプリケーションに対して脆弱性診断の実施を検討し、必要に応じて実施すること。

(3)　アプリケーション・コンテンツの運用時の対策

対策基準第６の５(3)におけるアプリケーション・コンテンツ運用時の対策について、システムセキュリティ責任者は、利用者に強制するＯＳやソフトウェア等のサポート状況や脆弱性情報等を確認し、サポートが終了する又は脆弱性が存在するバージョンのＯＳやソフトウェア等の利用を強制するなど情報セキュリティ水準を低下させる設定変更等をＯＳやソフトウェア等の利用者に要求することがないよう、アプリケーション及びウェブコンテンツの提供方式等を見直すこと。

(4)　アプリケーション・コンテンツの提供時の対策

対策基準第６の５(4)におけるアプリケーション・コンテンツ提供時の対策について、次のとおり定める。

ア　不正なウェブサイトへの誘導防止

(ｱ)　自組織外向けに提供するウェブサイトに対して、次に掲げる事項を例とする検索エンジン最適化措置（ＳＥＯ対策）を講ずること。

a　クローラからのアクセスを排除しない。

b　cookie機能を無効に設定したブラウザでも正常に閲覧可能とする。

c　適切なタイトルを設定する。

d　不適切な誘導を行わない。

(ｲ)　システムセキュリティ責任者は、自組織外向けに提供するウェブサイトに関連するキーワードで定期的にウェブサイトを検索し、検索結果に不審

なサイトが存在した場合は、速やかにその検索サイト業者に報告するとともに、不審なサイトへのアクセス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、自組織のウェブサイトなどになりすました不審なウェブサイト等が存在していることの連絡を受け付ける体制を整備するとともに、不審なウェブサイトに対し必要な措置を講ずること。

イ アプリケーション・コンテンツの告知

(ｱ) 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、ＵＲＬ等を用いて直接誘導することを原則とし、検索サイトで指定の検索語を用いて検索することを促す方法その他の間接的な誘導方法を用いる場合であっても、ＵＲＬ等と一体的に表示すること。また、短縮ＵＲＬを用いないこと。

(ｲ) アプリケーション・コンテンツを告知するに当たって、ＵＲＬを二次元コード等に変換して印刷物等に表示して誘導する場合には、当該コードによる誘導先を明らかにするため、アプリケーション・コンテンツの内容に係る記述を当該コードと一体的に表示すること。

(ｳ) 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等の有効性を保つため、次に掲げる措置を講ずること。

a 告知するアプリケーション・コンテンツを管理する組織名を明記する。

b 告知するアプリケーション・コンテンツの所在場所の有効性（リンク先のＵＲＬのドメイン名の有効期限等）を確認した時期又は有効性を保証する期間について明記する。

第６ 警察情報システムのセキュリティ要件

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

対策基準第７の１(1)アにおける主体認証機能について、次のとおり定める。

(ｱ)　システムセキュリティ責任者は、利用者が正当であることを検証するため、次に掲げる認証方式を例に主体認証機能を導入すること。

なお、可能な限り主体認証情報として生体情報を用いること。

ａ　知識（パスワード等、利用者本人のみが知り得る情報）による認証

ｂ　所有（電子証明書を格納するICカード、ワンタイムパスワード生成器、利用者本人のみが所有する機器等）による認証

ｃ　生体（指紋や静脈等、本人の生体的な特徴）による認証

(ｲ)　システムセキュリティ責任者は、内部ネットワークへリモートアクセスを必要とする主体、インターネット等から直接アクセスが可能なクラウドサービス等の管理者権限を有する主体、モバイル端末にログインする主体など厳格な主体認証が必要な場合、認証の強度として２つ以上の主体認証方式を組み合わせる多要素主体認証方式等の強固な認証技術を用いること。

(ｳ)　システムセキュリティ責任者は、サーバ等へのアクセスについて、利用者及び端末の主体認証機能を設けること。

(ｴ)　システムセキュリティ責任者は、主体認証情報の漏えい等による不正なアクセスを防止するため、次に掲げる事項を含む措置を講ずること。

ａ　原則として、機器等において初期値として設定されている識別コードを使用しない。

ｂ　不要な識別コードを無効にする。

(ｵ)　システムセキュリティ責任者は、主体認証情報としてパスワードを使用し、主体認証情報を付与された主体自らがパスワードを設定することを可能とする場合には、辞書攻撃等によるパスワード解析への耐性を考慮し、強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用することを利用者に守らせる機能を設けること。

(ｶ)　システムセキュリティ責任者は、職員自身がパスワードを変更できる機能を設けること。

(ｷ)　システムセキュリティ責任者は、職員にパスワードを定期的に変更するよう促す機能を設ける場合には、有効期限が切れたパスワードによるログインを停止できる機能を設けること。

(ｸ)　システムセキュリティ責任者は、主体認証情報が第三者に対して明らかにならないよう、次の方法を用いて適切に管理すること。

ａ　主体認証情報を送信又は保存する場合には、その内容を暗号化する。

ｂ　主体認証情報に対するアクセス制限を設ける。

ｃ　主体認証情報に対するアクセスに関するログを保存し、アクセスした主体を確認する。

(ｹ)　システムセキュリティ責任者は、主体認証情報を他の主体に不正に利用され、又は利用されるおそれを認識した場合の対策として、不正利用を防止するため、次に掲げる機能を設けること。

ａ　当該主体認証情報及び対応する識別コードの利用を停止する機能

ｂ　主体認証情報の再設定を利用者に要求する機能

イ　識別コード及び主体認証情報の管理

対策基準第７の１(1)イにおける識別コード及び主体認証情報の管理について、次のとおり定める。

(ｱ)　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を利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与（発行、更新及び変更を含む。以下同じ。）すること。

(ｲ)　システムセキュリティ維持管理者は、識別コードを付与するに当たっては、次に掲げる事項を例とする措置を講ずること。

ａ　単一の情報システムにおいて、ある主体に付与した識別コード（共用識別コードを除く。）を別の主体に対して付与することの禁止

ｂ　主体への識別コードの付与に関する記録を消去する場合のシステムセキュリティ責任者からの事前の許可

(ｳ)　システムセキュリティ維持管理者は、主体以外の者が識別コード又は主体認証情報を設定する場合に、主体へ安全な方法で主体認証情報を配布するよう、措置を講ずること。

(ｴ)　システムセキュリティ維持管理者は、識別コード及び知識による主体認証情報を付与された主体に対し、初期設定の主体認証情報を速やかに変更するよう、促すこと。

(ｵ)　システムセキュリティ維持管理者は、知識による主体認証方式を用いる

場合には、他の警察情報システムで利用している主体認証情報を設定しないよう主体に注意を促すこと。

(ｶ)　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を利用する主体ごとに識別コードを個別に付与すること。ただし、次に掲げる場合であって、システムセキュリティ維持管理者の判断の下、システムセキュリティ責任者と協議し、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関する規定を整備し、その規定に従って付与する場合はこの限りでない。

a　システムの運用上の制約により、やむを得ず一般利用者に共用識別コードを付与する必要がある場合

b　システムの機能上の制約により、当該システムを更改するまでの間、やむを得ず管理者に共用識別コードを付与する必要がある場合

(ｷ)　共用識別コードを用いて共用の端末装置を使用したときは、共用端末使用簿に使用日、使用時間、使用者及び使用目的を記載すること。また、当該使用簿は、月に１回以上、運用管理者又は運用管理者が指名する当該任務を代行する警視相当職以上の者の確認を受けること。

なお、当該使用簿の様式等については、別に定める。

(ｸ)　システムセキュリティ維持管理者は、主体認証情報の不正な利用を防止するために、主体が維持管理する警察情報システムを利用する必要がなくなった場合には、次に掲げる事項を例とする措置を講ずること。

a　当該主体の識別コードを無効にする。

b　当該主体に交付した主体認証情報格納装置を返還させる。

c　無効化した識別コードを他の主体に新たに発行することを禁止する。

(ｹ)　システムセキュリティ維持管理者は、管理者権限を持つ識別コードのうち、不要なものは削除すること。

(2)　アクセス制御機能

対策基準第７の１(2)におけるアクセス制御機能について、次のとおり定める。

ア　システムセキュリティ責任者は、主体の属性、アクセス対象の属性に基づきアクセス制御機能の要件を定めること。

イ　システムセキュリティ責任者は、主体の属性、アクセス対象の属性に基づくアクセス制御の要件の定期的な確認による見直しを行うこと。

(3)　権限の管理

対策基準第７の１(3)における権限の管理について、次のとおり定める。

ア　システムセキュリティ責任者は、管理者と一般利用者の権限を分割し、管理者権限は必要最小限の者のみが運用すること。ただし、携帯電話機、タブレット端末等の機能上、権限を分割できないものについては、個別のアプリケーションごとに管理者と一般利用者の権限を分割するなどして、可能な限り管理者と一般利用者の権限を分割すること。

イ　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ないこと。

ウ　システムセキュリティ責任者は、初期値として利用可能な管理者権限を有する識別コードには、管理者権限を付与しない又は無効化すること。

エ　システム管理担当者及びネットワーク管理担当者は、警察情報システムを管理する目的以外の目的で管理者権限を使用しないこと。

オ　システムセキュリティ責任者は、所管する警察情報システムの管理者権限について、システムセキュリティ維持管理者による運用状況を定期的に把握し、改善の必要が認められる場合には、必要な措置を講ずること。

(4)　ログの取得・管理

対策基準第７の１(4)におけるログの取得・管理について、次のとおり定める。

ア　時刻設定

(ｱ)　システムセキュリティ責任者は、サーバ等の時刻設定を正確なものとすること。

(ｲ)　システムセキュリティ責任者は、通信回線装置の時刻設定を正確なものとすること。

(ｳ)　システムセキュリティ責任者は、警察情報システムに含まれる構成要素のうち、時刻設定が可能なものについては、警察情報システムにおいて基準となる時刻に、当該構成要素の時刻を同期させ、ログに時刻情報も記録されるよう設定すること。

イ　ログ（外部記録媒体関係のものを除く。）

(ｱ)　システムセキュリティ責任者は、職員に対し、ログを保管すること、その分析を行う可能性があること等をあらかじめ周知すること。

(ｲ)　システムセキュリティ責任者は、取得したログについては、不正な消去、改ざん及びアクセスを防止するため、適切なアクセス制御を含む、ログの保全方法を定め、管理させること。

(ｳ)　システムセキュリティ責任者は、要保護情報を保存するサーバ等へのアクセスについては、アクセスした日時及び職員を特定できる情報をログとして取得し、５年以上保管できる仕様とすること。

(ｴ)　システムセキュリティ責任者は、電子計算機、通信回線装置等については、その特性に応じて、ログを取得する目的を設定した上で、表７に掲げる項目の中から必要と認めたものについて、ログの保存期間、取扱方法、ログが取得できなくなった場合の対処方法等を定め、ログを適切に保管できる仕様とすること。

表７　ログ（外部記録媒体関係のものを除く。）の項目

利用者のログイン・ログアウトの記録	ログイン・ログアウトした日時（年月日時分秒）
	ログイン・ログアウトしたユーザを特定できる情報（識別コード、ユーザ名等）
	ログイン・ログアウトした電子計算機を特定できる情報（ホスト名、ＩＰアドレス等）
電子メールの送受信の記録	送受信日時（年月日時分秒）
	送受信者を特定できる情報（識別コード、メールアドレス等）
	件名
	宛先（Ｔｏ、Ｃｃ、Ｂｃｃの別を含む。）
	添付ファイルの名前及びファイルサイズ
	送受信した電子計算機を特定できる情報（ホスト名、ＩＰアドレス等）
印字出力の記録	印字出力の時刻（年月日時分秒）
	印字出力した者を特定できる情報（識別コード、ユーザ名等）
	印字出力した電子計算機を特定できる情報（ホスト名、Ｉ

	Ｐアドレス等）
	印字出力したファイル名
	印字出力先の印字装置を特定できる情報（ホスト名、ＩＰアドレス等）
	印字出力した枚数又はページ数
	印字出力したファイルの保存場所（ファイルパス）
ファイル操作（参照、保存、名前変更、削除及びコピー）の記録	ファイル操作日時（年月日時分秒）
	操作した者を特定できる情報（識別コード、ユーザ名等）
	操作した電子計算機を特定できる情報（ホスト名、ＩＰアドレス等）
	操作したファイル名（拡張子を含む。）
	操作したファイルの保存場所（ファイルパス）
ネットワークに係る記録	通信パケットの内容
システム管理に係る記録	識別コードの発行等の管理記録 職員、管理者等へシステムから通知した内容

(ｵ)　システムセキュリティ責任者は、必要に応じて、電子メールの送受信、外部のウェブサイトの閲覧等の履歴を保管するとともに、管理対象情報の漏えい防止その他の情報セキュリティの観点から当該履歴を確認する場合があり得ることを職員に周知すること。

ウ　外部記録媒体関係のログ

(ｱ)　媒体利用管理者は、次に掲げる場合においては、ファイル名及びファイルサイズに係るログの確認を不要とすることができる。ただし、警察が管理する電子計算機以外の電子計算機では技術的に復号できない暗号化機能を利用して、外部回線に接続されていない電子計算機から出力したファイルを外部回線に接続されている電子計算機に入力した場合は、その出力又は入力のいずれかに係るログを確認することとする。

ａ　システムセキュリティ責任者が、次の(a)から(c)まで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た警察情報システムにおいてファイルを入力した場合

(a)　不正プログラム対策ソフトウェアが適切に導入されているとともに、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できる環境を整えていること。

(b)　次に掲げる事項を満たしていること。

なお、光ディスクに限っては、次に掲げる事項のいずれかを満たしていること。

・　警察情報システムに未登録の外部記録媒体は、その種類によらず、媒体利用管理者の許可がなければ利用できないよう技術的措置が講じられていること。

・　入力に係るログを抽出し検証が行えること。

(c)　外部記録媒体の自宅への持ち帰り防止対策等、外部記録媒体によって本来の目的以外の情報が入出力されることを防ぐための対策が講じられていること。

b　警察が管理する電子計算機以外の電子計算機では技術的に復号できない暗号化機能を利用してファイルを入出力した場合

(ｲ)　システムセキュリティ責任者は、次に掲げる項目について外部記録媒体の利用のログを取得し、５年以上保管できる機能を設けること。

a　入出力日時

b　操作した者を特定できる情報（識別コード、ユーザ名等）

c　操作した電子計算機を特定できる情報（ホスト名、ＩＰアドレス等）

d　入出力したファイルの名前（拡張子を含む。）及びサイズ

e　入出力の別

f　出力時の平文、暗号文の別

(ｳ)　システムセキュリティ責任者は、次に掲げる項目について可能な限り外部記録媒体の利用のログを取得し、5年以上保管できる機能を設けること。

a　利用外部記録媒体のＩＤ等の固有情報

b　外部記録媒体に出力したファイルの元の保存場所（ファイルパス）

(ｴ)　システムセキュリティ責任者は、次に掲げる項目について外部記録媒体の利用の許可のログを取得し、１年以上保管できる機能を設けること。

a　利用の許可の期間

b　利用許可者を特定できる情報（識別コード、ユーザ名等）

(ｵ)　システムセキュリティ責任者は、(ｲ)に掲げるログについては媒体利用管理者が、(ｴ)に掲げるログについては媒体利用管理者の第２の１(1)アに定める所属の上級の職員（夜間・休日の当直責任者を除く。）が、それぞれ印刷物又は情報システム上で確認できる機能を設けること。

(ｶ)　対策基準第５の２(5)ウにおける警察情報システムの運用・保守に係る代替手段として、システムセキュリティ責任者は、(ｲ)及び(ｴ)に示すログが取得できない電子計算機について、外部記録媒体を接続するたびに職員名、日時、その外部記録媒体の管理番号、目的等を外部記録媒体利用簿に記載しなければならない旨を担当職員に周知すること。

なお、外部記録媒体利用簿の様式等については、別に定める。

エ　その他

(ｱ)　システムセキュリティ責任者は、ＲＰＡ等において職員の識別コード及び主体認証情報を用いた自動処理を行うときは、ＲＰＡサーバ等において自動的な処理が行われたログを取得し、適切な期間保管するなど、可能な限り情報システムを利用していた主体を特定できる仕組みを設けること。

(ｲ)　システムセキュリティ責任者は、所管する警察情報システムにおいて、ログが取得できなくなった場合の対処方法を定めること。

(ｳ)　システムセキュリティ責任者は、警察情報システムの分類に応じて、取得したログを効率的かつ確実に点検及び分析に資するため、警察情報システムの分類に応じて、次に掲げる対策を講ずること。

a　当該作業を支援するため、ログ情報のソフトウェア等による集計、時系列での表示、報告書を生成するなどの自動化機能を導入すること。

b　追加セキュリティ対策として、必要に応じて、上記ａの機能の導入に加え、リアルタイムでログの調査・分析を行うための機能の導入を検討すること。

(ｴ)　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に係る管理者権限を使用した者を特定可能なサーバ等のログ等により、管理者権限に係る接続元のＩＰアドレス、アクセス日時等を定期的に確認すること。

(5)　暗号・電子署名

対策基準第７の１(5)における暗号・電子署名について、次のとおり定める。

ア　暗号化機能・電子署名機能の導入

(ｱ)　電子署名の付与又は検証を行う機能については、次に掲げる機能を設けること。

ａ　暗号リストに掲げるハッシュ関数を使用し、当該情報が改ざんされた場合に自動的に検知する仕組みとすること。

ｂ　暗号リストに掲げる公開鍵暗号を使用し、自動的に相互認証を実施する仕組みとすること。

(ｲ)　復号又は電子署名の付与に用いる鍵の管理については、次に掲げる事項を満たすこと。

ａ　暗号鍵を警察独自に設定できること。

ｂ　暗号鍵を更新できる仕組みがあること。また、自動更新できるものについては１日に１回以上更新する設定とすること。

ｃ　復号又は電子署名の付与に用いる鍵について、鍵の生成手順、有効期限、廃棄手順、鍵が露呈した場合の対応手順等を定めること。

ｄ　新たに作成された共通鍵を共有するために配送するときは、その共通鍵を暗号化すること。ただし、その暗号化に使用する暗号鍵は、必要に応じて速やかに変更できるようにすること。

ｅ　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。

ｆ　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。

(ｳ)　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(たい)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ること。

イ　暗号化・電子署名に係る管理

署名検証者が、電子署名の正当性を容易に検証するための情報を入手できるよう、次に掲げる事項を例とする方法により、当該情報の提供を可能とすること。

(ｱ)　信頼できる機関による電子証明書の提供

(ｲ)　自組織の窓口での電子証明書の提供

(6)　監視機能

対策基準第７の１(6)における監視機能について、次のとおり定める。

ア　システムセキュリティ責任者は、監視のために必要な機能について、次に掲げる事項を例とする機能を仕様書に記載すること。

(ｱ)　自組織外と電気通信回線で接続している箇所における外部からの不正アクセスやサービス不能攻撃を監視する機能

(ｲ)　不正プログラム感染や踏み台に利用されること等による自組織外への不正な通信を監視する機能

(ｳ)　端末等の内部ネットワークの末端に位置する機器及びサーバ等において不正プログラムの挙動を監視する機能

(ｴ)　内部ネットワークへの端末の接続を監視する機能

(ｵ)　端末への外部記録媒体の挿入を監視する機能

(ｶ)　サーバ等の機器の動作を監視する機能

(ｷ)　ネットワークセグメント間の通信を監視する機能

イ　システムセキュリティ責任者は、暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を仕様書に記載すること。

ウ　システムセキュリティ責任者は、所管する警察情報システムについて、監視を行う場合には、次に掲げる事項を含む監視手順を定め、適切に監視運用すること。また、追加セキュリティ対策として、必要に応じて、警察情報システム運用時の監視において、ＳＯＣ（Security Operation Center）やＮＯＣ（Network Operations Center）等のセキュリティ監視を専門の外部事業者に業務委託することを検討すること。

(ｱ)　監視するイベントの種類

(ｲ)　監視体制

(ｳ)　監視状況の報告手順

(ｴ)　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の報告手順

(ｵ)　監視運用における情報の取扱い（機密性の確保）

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

対策基準７の２(1)におけるソフトウェアに関する脆弱性対策について、次のとおり定める。

ア　脆弱性診断の実施

(ｱ)　システムセキュリティ責任者は、インターネット向けにサービスを公開しているサーバ等や直接インターネットから到達可能なサーバ等、端末及び通信回線装置に対し、設置又は運用開始時に脆弱性診断を実施すること。また、その他のサーバ等、端末及び通信回線装置については、警察情報システムの分類や保有する情報、システム特性等を踏まえ、脆弱性診断の実施を検討すること。

(ｲ)　システムセキュリティ責任者は、サーバ等、端末及び通信回線装置に対する追加セキュリティ対策として、必要に応じて、ペネトレーションテスト、ＴＬＰＴ（脅威ベースのペネトレーションテスト）等の高度な脆弱性診断の実施を検討すること。

イ　脆弱性情報の入手

(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について、構成要素ごとにソフトウェアのバージョン等を把握し、当該ソフトウェアの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、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（広報、報道等が行われているものを除く。）を入手したときは、情報セキュリティ管理者に連絡すること。

(ｲ)　システムセキュリティ責任者は、サポート期間を考慮して利用するソフトウェアを選定し、サポートが受けられないソフトウェアは可能な限り利用しないこと。

(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構成要素ごとにソフトウェアのバージョン等を把握し、脆弱性対策の状況を確認すること。

(ｴ)　システム管理担当者及びネットワーク管理担当者は、管理対象となる電

子計算機又は通信回線装置に関連する脆弱性情報の入手に努めること。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すること。

ウ　脆弱性対策の実施

(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について脆弱性対策計画を策定する場合には、次に掲げる事項について、検討すること。

a　対策の必要性

b　対策方法

c　対策方法が存在しない場合又は対策が完了するまでの期間に対する一時的な回避方法

d　対策方法又は回避方法が警察情報システムに与える影響

e　対策の実施予定時期

f　対策試験の必要性

g　対策試験の方法

h　対策試験の実施予定時期

(ｲ)　システムセキュリティ責任者は、脆弱性対策を講ずる場合には、少なくとも次に掲げる事項を記録し、これらの事項のほかに必要事項があれば適宜記録すること。

a　実施日

b　実施内容

c　実施者

(ｳ)　システムセキュリティ責任者は、ネットワーク境界にある通信回線装置や認証サーバ、要機密情報を保有するサーバ等のサイバーセキュリティリスクが高い機器等について、セキュリティパッチの適用又はソフトウェアのバージョンアップ等の措置を講じないと判断した場合には、リスク評価結果の記録を残すこと。

(ｴ)　システムセキュリティ責任者は、脆弱性対策が計画どおり実施されていることについて、実施予定時期の経過後、遅滞なく確認すること。

(ｵ)　システムセキュリティ責任者は、セキュリティパッチ、バージョンアッ

プソフトウェア等の脆弱性を解決するために利用されるファイルは、信頼できる方法で入手し、完全性を検証すること。

(ｶ)　システムセキュリティ責任者は、追加セキュリティ対策として、必要に応じて、警察情報システムを構成する機器へのセキュリティパッチの適宜の適用を前提とした運用設計を行うこと。

エ　その他

システムセキュリティ責任者は、サポート期間を考慮して利用するソフトウェアを選定し、サポートが受けられないソフトウェアは可能な限り利用しないこと。

(2)　不正プログラム対策

対策基準第７の２(2)における不正プログラム対策について、次のとおり定める。

ア　システムセキュリティ責任者は、不正プログラム対策ソフトウェア及びそのパターンファイルについて、その運用状況に応じた頻度で、最新の状態に更新すること。

イ　システムセキュリティ責任者は、不正プログラム対策ソフトウェアの設定変更権限については、システムセキュリティ維持管理者が一括管理し、利用者に当該権限を付与しないこと。

ウ　システムセキュリティ責任者は、不正プログラム対策ソフトウェアによる不正プログラムの自動検査機能を有効にするとともに、定期的に不正プログラムの有無を確認するよう設定すること。不正プログラムの有無の確認を自動的に行えない場合には、定期的に手動で行うよう職員に指示すること。

エ　システムセキュリティ責任者は、想定される全ての感染経路を特定し、不正プログラム対策ソフトウェア等の導入による感染の防止、端末の接続制限及び機能の無効化等による感染拡大の防止等の必要な対策を行うこと。

オ　システムセキュリティ責任者は、次に掲げる電子計算機については、アからエ及び対策基準第７の２(2)の規定を適用しない。

(ｱ)　当該電子計算機で外部記録媒体を利用できないよう技術的又は物理的な措置が講じられているものであって、当該電子計算機とネットワーク接続された全ての電子計算機において同様の措置が講じられているもの

(ｲ)　スタンドアロン端末であって、ＵＳＢメモリ型の不正プログラム対策ソフトウェアを用いて定期的な不正プログラムの有無を確認すべき旨が職員に周知されているもの

(ｳ)　当該電子計算機内で実行されるアプリケーションが、ホワイトリストにより制限されているもの

(ｴ)　不正プログラムの解析又は調査・研究の用に供するもの

カ　システムセキュリティ責任者は、追加セキュリティ対策として、必要に応じて、ＥＤＲ（Endpoint Detection and Response）ソフトウェア等を利用し、端末やサーバ等（エンドポイント）の活動を監視し、感染した機器等を早期にネットワークから切り離す機能の導入を検討すること。

(3)　サービス不能攻撃対策

対策基準第７の２(3)に基づき、サービス不能攻撃対策の実施について、次のとおり定める。

ア　システムセキュリティ責任者は、直ちに警察情報システムを外部ネットワークから遮断する、又は電気通信回線の通信量を制限する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責任者は、次に掲げる事項を例とするサービス不能攻撃対策を講ずること。

(ｱ)　サービス不能攻撃の影響を排除又は低減するための専用の対策装置やサービスの導入

(ｲ)　サーバ等、端末、通信回線装置又は電気通信回線の冗長化

ウ　システムセキュリティ責任者は、追加セキュリティ対策として、必要に応じて、次に掲げる事項を例とする対策を検討すること。

(ｱ)　外部回線に接続している電気通信回線の提供元となる事業者やクラウドサービス提供者が別途提供する、サービス不能攻撃に係る通信の遮断等の対策

(ｲ)　コンテンツデリバリーネットワーク（ＣＤＮ）サービスの利用

エ　システムセキュリティ責任者は、攻撃への対処を効率的に実施できる手段の確保について検討すること。

オ　システムセキュリティ責任者は、特定した監視対象については、監視方法

及び監視記録の保存期間を定め、監視記録を保存すること。

(4)　標的型攻撃対策

対策基準第７の２(4)における標的型攻撃対策について、次のとおり定める。

ア　システムセキュリティ責任者は、情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される、認証サーバやファイルサーバ等の重要なサーバについて、次に掲げる事項を含む対策を講ずること。

(ｱ)　重要なサーバについては、内部ネットワークを複数セグメントに区切った上で、重要なサーバ類専用のセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定する。また、インターネットに接続する必要がある場合は、必要最小限のプロトコルやポートのみに限定し、インターネットに接続する必要がない場合はインターネットから分離を行う。

(ｲ)　認証サーバについては、利用者端末から管理者権限を狙う攻撃（辞書攻撃、ブルートフォース攻撃等）を受けることを想定した対策を講ずること。

イ　システムセキュリティ責任者は、端末の管理者権限を有する識別コードについて、次に掲げる事項を含む対策を講ずること。

(ｱ)　不要な管理者権限を有する識別コードは削除する。

(ｲ)　管理者権限を有する識別コードのパスワードは、容易に推測できないものに設定する。

ウ　システムセキュリティ責任者は、追加セキュリティ対策として、必要に応じて、次に掲げる事項を例とする対策を講ずること。

(ｱ)　プロキシサーバ等により、Ｃ＆Ｃサーバ等への不正な通信を監視し、遮断する。

(ｲ)　警察情報システムの管理者が利用する警察情報システム管理用の専用端末を用意し、他のセグメントと分離した運用管理セグメントを構築し、当該セグメントにシステム管理用の専用端末を接続する。

(ｳ)　認証サーバに管理者権限でログインできる端末をシステム管理用の専用端末に制限する。

(ｴ)　職員が利用する端末間でのファイル共有機能を停止する又は職員が利用する端末間の直接通信を遮断する。

(5)　外部記録媒体の利用に係る対策

対策基準第７の２(5)における外部記録媒体の利用に係る対策の実施について、次のとおり定める。

ア　入力の制限

電子計算機は、次のうち少なくとも一方の規定を満たすこと。

(ｱ)　媒体利用管理者の許可なしに外部記録媒体からのファイルの入力が技術的に行えないよう設定すること。また、媒体利用管理者が行う許可は、管理者権限とは別の権限によって行うこと。

(ｲ)　警察情報システムに登録済みの外部記録媒体以外の外部記録媒体には技術的にアクセスできないよう設定すること。ただし、光ディスク媒体に限りファイルの入力が行えることは妨げない。

イ　出力の制限

(ｱ)　外部記録媒体への出力を、自己復号型暗号又は警察が管理する電子計算機以外の電子計算機では技術的に復号できない暗号により行う機能を設けること。

(ｲ)　媒体利用管理者の許可なしに外部記録媒体への出力が技術的に行えいよう設定すること。ただし、警察が管理する電子計算機以外の電子計算機では技術的に復号できない暗号による出力については、媒体利用管理者の許可なく行うことができる。

(ｳ)　媒体利用管理者による許可は、管理者権限とは別の権限によって行うこと。また、警察が管理する電子計算機以外の電子計算機では技術的に復号できない暗号による出力を許可したときは、平文又は自己復号型暗号による出力が行えないよう制限する機能を設けること。

(ｴ)　警察情報システムに登録済みの外部記録媒体以外の外部記録媒体への出力が技術的に行えないよう設定すること。ただし、光ディスク媒体に限りファイルの出力が行えることは妨げない。

ウ　許可

ア及びイの許可は、許可の期間、電子計算機又は対象とする情報システム及び利用者を指定した上で行えるようにすること。

エ　例外

次に掲げる事項に該当する電子計算機については、アからウ及び１(4)ウ

(ｲ)から(ｵ)までの規定を適用しない。ただし、(ｵ)にあっては１(4)ウ(ｲ)から(ｵ)までに定めるログを取得すること。

(ｱ)　内蔵された電磁的記録媒体に要機密情報を保存しないもの

(ｲ)　クラス３に指定された区域に設置されたもの（端末を除く。）

(ｳ)　当該電子計算機で外部記録媒体を利用できないよう技術的又は物理的な措置が講じられているもの（端末の利用者に付与している権限で解除できないものに限る。）

(ｴ)　支給携帯電話機、タブレット端末等であって、技術的にアからウ及び１(4)ウ(ｲ)から(ｵ)の規定を満たすことが困難であるもの

(ｵ)　専ら証拠品等の外部記録媒体の確認のみを行うもの

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

対策基準第７の３(1)における動的なアクセス制御の実装時の対策について、次のとおり定める。

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対象とするシステムの範囲や優先度を検討し、動的なアクセス制御の対象とするシステムを特定すること。

イ　システムセキュリティ責任者は、動的なアクセス制御の導入方針の検討時において、特定した警察情報システムの利用形態等を基に次に掲げる事項を例とする区分で警察情報システムのリソースを識別すること。また、動的なアクセス制御の実装に当たっては同事項を例とするリソースの信用情報を整理すること。

(ｱ)　ユーザアカウント

(ｲ)　機器

(ｳ)　アプリケーション

(ｴ)　データ

ウ　システムセキュリティ責任者は、識別したリソースを基にアクセスパターンを整理すること。

エ　システムセキュリティ責任者は、整理したアクセスパターンに対するリスク評価を実施し、動的なアクセス制御を実装するアクセスパターンを特定す

ること。

オ　システムセキュリティ責任者は、動的なアクセス制御を実現するための構成について検討すること。

カ　システムセキュリティ責任者は、リソースの信用情報の変化を踏まえて、リソースの信用情報を収集する頻度・機会について定めること。

キ　システムセキュリティ責任者は、リソースの認証・認可において、アクセス制御ポリシーに基づき、セッションが確立していない操作ごとに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

対策基準第７の３(2)における動的なアクセス制御の運用時の対策について、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、アクセスパターンやアクセス先のリソースの変化があった場合は、変化が影響する箇所に対し再度リスク評価を行い、アクセス制御ポリシーの見直しを行うこと。

第７　警察情報システムの利用

１　警察情報システムの利用

(1)　警察情報システム利用者の規定の遵守を支援するための対策

対策基準第８の１(1)における警察情報システム利用者の規定の遵守を支援するための対策について、次のとおり定める。

ア　システムセキュリティ責任者は、職員がウェブサイトを閲覧するための警察情報システムについては、次に掲げる事項を例として、閲覧できる範囲を制限する機能を導入すること。また、当該機能に係る設定や条件について定期的に見直すこと。

(ｱ)　ウェブサイトフィルタリング機能

(ｲ)　事業者が提供するウェブサイトフィルタリングサービスの利用

イ　システムセキュリティ責任者は、不審な電子メールを受信することによる被害をシステム的に抑止するため、次に掲げる事項を例とする機能を導入すること。

(ｱ)　受信メールに対するフィルタリング機能

(ｲ)　受信メールをテキスト形式で表示する機能

(ｳ)　スクリプトを含む電子メールを受信した場合において、当該スクリプトが自動的に実行されることがない電子メールクライアント

(ｴ)　受信メールに添付されている実行プログラム形式のファイルを削除等することで実行させない機能

ウ　システムセキュリティ責任者は、受信した電子メールを表示するに当たって、プログラムが自動的に起動しないよう設定しておくこと。

エ　職員は、対策基準第８の１(1)イ及びウにおける手続について、技術的措置を講ずるに当たっては、次の事項に留意すること。

(ｱ)　技術的措置が警察情報セキュリティポリシーに定める手続に適合していることについて、必要に応じて情報セキュリティ管理者の確認を受けること。

(ｲ)　警察情報セキュリティポリシーによらない独自の手続を技術的措置により実現しようとする場合は、十分な期間をもって情報セキュリティ管理者の確認を受けること。

(2)　警察情報システム等の利用時の基本的対策

ア　警察情報システム

対策基準第８の１(2)アにおける警察情報システムの利用時の基本的対策について、次のとおり定める。

(ｱ)　職員は、物理的に持ち出しが困難であるもの及びセキュリティワイヤの取り付けられたものを除き、全ての電子計算機を鍵のかかる保管庫に保管するなどして、紛失又は盗難がないよう適正に管理すること。

(ｲ)　職員は、警察情報システムを不正操作から保護するため、スクリーンロックの設定、利用後のログアウトの徹底等必要な措置を講ずること。

(ｳ)　対策基準第８の１(2)ア(ｵ)により、運用管理者は、警察情報システムを構成する機器の改造を行おうとするときは、電子計算機接続等許可申請書を作成し、システムセキュリティ責任者に申請すること。

イ　モバイル端末の管理

運用管理者は、次の(ｱ)から(ｵ)までに掲げる事項を記載したモバイル端末管理簿を作成し、保管すること。また、当該管理簿は、モバイル端末の増減のあった都度、変更のないときも年１回以上、更新すること。

(ｱ)　モバイル端末の管理番号

(ｲ)　モバイル端末の種別

(ｳ)　モバイル端末の管理者（使用者）

(ｴ)　使用開始日及び使用終了日

(ｵ)　その他の所要事項

ウ　機器等の持ち出し

対策基準第８の１(2)ア(ｷ)に基づき、機器等の持ち出し時の対策について、次のとおり定める。

(ｱ)　モバイル端末の持ち出し

a　モバイル端末を持ち出すときは、内蔵された電磁的記録媒体の要機密情報を必要最小限にすること。また、警察が管理する区域以外に持ち出すときは、外部記録媒体・端末等持出簿（以下「持出簿」という。）に氏名、モバイル端末の管理番号、端末種別、持出期間、目的及び持出開始日時を記載し、自所属の上級の職員であって警部相当職以上の者（夜間・休日にあっては当直長及び副当直長を含む。）の許可を得ること。ただし、本部執行隊における分駐隊、警察署における交番等（以下「分駐隊等」という。）庁舎内に警部相当職以上の者が配置されていない場合は、当該分駐隊等の最上位の者の許可を得ることで足りる。

b　モバイル端末の警察が管理する区域以外への持ち出しが終了したときは、持出簿に持出終了日時を記載し、持出時に許可を与えた者から紛失のない旨の確認を受けること。

(ｲ)　モバイル端末等以外の機器等の持ち出し

a　次に掲げる場合を除き、モバイル端末及び支給携帯電話機以外の機器等を持ち出さないこと。

(a)　機器等の内部に要機密情報が保存されていないことを自所属の上級の職員であって警部相当職以上の者（夜間・休日の当直長及び副当直長を除く。）が確認した場合

(b)　修理、廃棄、保管場所変更、保守作業等のためであって、職員が運搬し、常に職員の管理下にある場合

(c)　(a)及び(b)に掲げるもののほか、やむを得ない事情があるとして、

システムセキュリティ責任者の許可を得た場合

b　a(a)から(c)までの場合においてモバイル端末及び支給携帯電話機以外の機器等を持ち出すときは、システム管理担当者の許可を得るとともに、必要最小限の情報を残して機器等内の要機密情報を削除し、持出簿に氏名、機器の管理番号、持出期間、目的及び持出開始日時を記載した上で運用管理者の許可を得ること。ただし、警察が管理する区域以外には持ち出さない場合は、運用管理者の許可を自所属の上級の職員であって警部相当職以上の者（夜間・休日の当直長及び副当直長を除く。）の許可で足りることとし、持出簿への記載は不要とする。

c　モバイル端末及び支給携帯電話機以外の機器等を運搬業者に運搬させるときは、システムセキュリティ責任者の許可を得るとともに、保秘に関する取決めを行うこと。

d　警察が管理する区域以外への持ち出しが終了したときは、持出簿に持出終了日時を記載し、持ち出し時に許可を与えた者から紛失のない旨の確認を受けること。

e　持ち出しを前提として整備された特定用途機器を持ち出すときは、モバイル端末の持ち出し時の手続に準拠した手続で持ち出すことができる。

(ｳ)　盗難・紛失に対する対策

持ち出し中における機器等の盗難・紛失に対する対策として、利用状況に応じて次に掲げる事項を例とした対策を講ずること。

a　機器等の放置の禁止

b　利用時以外のシャットダウン及びネットワークの切断

c　機器等を常時携帯すること

d　常に身近に置き、目を離さないこと

(ｴ)　持出簿の確認

持出簿について月に１回以上運用管理者又は運用管理者が指名する当該任務を代行する警視相当職以上の者の確認を受けること。

エ　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の

内部ネットワークへの接続

対策基準第８の１(2)ア(ｸ)に基づ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へファイアウォール等を介さずに直接接続する場合には、次に掲げる事項を満たすこと。

(ｱ)　警察が管理する区域以外での端末の利用時において、外部回線を通じて警察情報システムのみにアクセスできる設定としたものであること。

(ｲ)　当該外部回線は、内部ネットワークに接続中には第５の３(1)イの規定を満たす回線であること。

(ｳ)　第５の１(1)ウ(ｱ)ｄに規定された、管理対象情報を保存できないようにするための機能を設けたモバイル端末であること。

オ　支給携帯電話機

対策基準第８の１(2)イにおける支給携帯電話機（複数の職員が共用する支給携帯電話機（以下「共用支給携帯電話機」という。）を含む。）の利用時の基本的対策について、次のとおり定める。

(ｱ)　支給携帯電話機の管理

ａ　運用管理者は、次の(a)から(g)までに掲げる事項を記載した支給携帯電話機管理簿を作成すること。また、当該管理簿は支給携帯電話機の増減のあった都度、変更のないときも年１回以上、更新すること。

(a)　支給携帯電話機の管理番号

(b)　支給携帯電話機の電話番号

(c)　支給携帯電話機を支給する職員の役職又は氏名（共用支給携帯電話機にあっては、共用支給携帯電話機を管理する職員の役職又は氏名）

(d)　支給携帯電話機で使用するメールアドレス（電子メール機能を使用するものに限る。）

(e)　支給携帯電話機の機種

(f)　使用開始日及び使用終了日

(g)　その他所要の事項

ｂ　職員は、支給携帯電話機について、紛失又は盗難がないよう適正に管理すること。

c　共用支給携帯電話機の管理者は、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場合は、この限りでない。

d　共用支給携帯電話機の管理者は、共用支給携帯電話機を使用しない場合は、鍵のかかる保管庫に保管するなどの措置を講ずること。また、可能な限り集中保管すること。

e　支給携帯電話機の管理者は、月に１回以上、支給携帯電話機の所在を点検するとともに、点検結果を運用管理者に電子決裁システムの起案文にて年度管理の１年保存文書として報告すること。ただし、クラス３に分類された区域内で鍵のかかる保管庫に保管されている場合は、年に１回の点検で足りることとする。

なお、個人に支給されている支給携帯電話機の点検結果については、当該支給携帯電話機の管理者の所属の上級の職員であって、警部相当職以上の者が点検することを妨げない。

(ｲ)　支給携帯電話機の使用

a　職員は、職務上必要がある場合は、支給携帯電話機の音声通話機能、電子メール機能、写真撮影機能等を使用することができる。

b　職員は、支給携帯電話機において外部回線を用いて要機密情報を取り扱う場合は、情報の暗号化、符丁の活用等の情報漏えい対策を講ずること。

c　職員は、支給携帯電話機の電子メール機能を使用する場合は、可能な限りグループ機能を使用するなど、情報の誤送信を防止するための対策を講ずること。

d　職員は、支給携帯電話機に保存された管理対象情報を電子計算機に取り込む必要がある場合は、自所属の上級の職員であって警部相当職以上の者（夜間・休日の当直長及び副当直長を含む。）に報告（口頭による報告を含む。）した上で、不正プログラムが侵入しないよう安全な方法で当該管理対象情報を電子計算機に取り込んだ後、速やかに支給携帯電話機本体から管理対象情報を削除すること。

(ｳ)　共用支給携帯電話機の持ち出し

a　持ち出し時の手続

対策基準第８の１(2)イ(ｱ)において共用支給携帯電話機を警察の庁舎外に持ち出す場合は、持出簿に氏名、共用支給携帯電話機の管理番号、端末種別、持出期間、目的及び持出開始日時を記載し、自所属の上級の職員であって警部相当職以上の者（夜間・休日の当直長及び副当直長を含む。）の許可を得ること。

b　持ち出しの特例

職員は、ａの規定にかかわらず、次に掲げるいずれかの場合は、持出簿への記載を省略することができる。

(a)　職員は、警察署等において、課長等が休暇や出張等により不在で同室に警部相当職以上の者が配置されていない場合であって、別室（他の課等）の警部相当職以上の者の許可を得ることが困難である場合は、当該課長等が指名した警部補相当職の者に、一時的に持ち出しに係る許可を得ることができる。

(b)　当直勤務に従事する職員が、当直勤務用として指定された共用支給携帯電話機を持ち出す場合。この場合において、当該共用支給携帯電話機は、原則として、当直勤務を取りまとめる所属において管理すること。また、当直長は、当直勤務において当該共用支給携帯電話機を使用する者を指名するとともに、当直勤務の終了後の報告時に、併せて当該共用支給携帯電話機を当直勤務を取りまとめる所属に返却すること。

(c)　交替制勤務に従事する職員が、交替制勤務用として指定された共用支給携帯電話機を持ち出す場合。この場合において、当該職員の所属の上級の職員であって警部相当職以上の者は、定期的に当該共用支給携帯電話機の管理状況を確認すること。

c　持ち出し終了時の手続

職員は、共用支給携帯電話機の持ち出しが終了した場合は、持出簿に持出終了日時を記載し、持ち出し時に許可を与えた者から持ち出し終了の確認を受けること。

d　持出簿の確認

職員は、持出簿について、月に１回以上運用管理者又は運用管理者が

指名する当該任務を代行する警視相当職以上の者の確認を受けること。

カ　外部記録媒体

対策基準第８の１(2)ウにおける外部記録媒体の利用時の基本的対策について、次のとおり定める。

(ｱ)　外部記録媒体の管理

a　運用管理者は、次の(a)から(f)までに掲げる事項を記載した外部記録媒体管理簿を作成し、保管すること。また、当該管理簿について、外部記録媒体の増減のあった都度、変更のないときも年１回以上、更新すること。

なお、外部記録媒体には、管理番号を記載したラベルを貼付すること。ただし、本体が小さいなどの理由により貼付することが困難なときは、略番号を記載したラベルを貼付することができる。このとき、外部記録媒体管理簿の備考欄に当該略番号を記載しておく。

(a)　外部記録媒体の管理番号

(b)　外部記録媒体の媒体種別

(c)　外部記録媒体の利用目的

(d)　外部記録媒体の媒体利用管理者

(e)　使用開始日及び使用終了日

(f)　その他所要の事項

b　職員は、外部記録媒体を利用しないときは、鍵のかかる保管庫に保管するなどして、紛失又は盗難がないよう適正に管理すること。

c　職員は、可能な限り外部記録媒体を集中保管すること。

d　媒体利用管理者は、月に１回以上、外部記録媒体の所在を点検するとともに、点検結果をを運用管理者に電子決裁システムの起案文にて年度管理の１年保存文書として報告すること。ただし、クラス３に分類された区域内で鍵のかかる保管庫に保管されている場合は、年に１回の点検で足りることとする。

e　デジタルカメラ、ボイスレコーダ等、情報を記録でき、電子計算機に接続して情報を入出力することができる機器等は、外部記録媒体とみなす。ただし、規定上、警察情報システムに接続することを禁止したもの

及び内蔵された電磁的記録媒体に管理対象情報を保存することを禁止したものにあっては、この限りでない。

f　次に掲げる外部記録媒体については、aからdまでの規定を適用しない。

(a)　未使用のもの

(b)　一度情報が書き込まれ、これ以上の情報の書き込みが技術的に不可能なものであって、内部に記録された管理対象情報が機密性１（低）情報のもの

(c)　法令その他の規程により、管理方法が別に定められているもの

g　運用管理者は、分駐隊等庁舎内に警部相当職以上の者が配置されていない場合は、当該分駐隊等の最上位の者を媒体利用管理者に指名して外部記録媒体を管理させることができる。

(ｲ)　外部記録媒体の持ち出し

a　持ち出し時の手続

対策基準第８の１(2)ウ(ｲ)において外部記録媒体を持ち出すときは、持出簿に氏名、媒体の管理番号、媒体種別、持出期間、目的及び持出開始日時を記載し、自所属の上級の職員であって警部相当職以上の者（夜間・休日の当直長及び副当直長を含む。）の許可を得ること。ただし、分駐隊等庁舎内に警部相当職以上の者が配置されていない場合は、当該分駐隊等の最上位の者の許可を得ることで足りる。

なお、(ｱ)eに掲げる外部記録媒体については、次に掲げる事項を満たしている場合に限り、持ち出し時の許可を不要とすることができる。

(a)　管理対象情報が記録されていない外部記録媒体の持ち出しであること。

(b)　持ち出したその日のうちに持ち出しが終了する見込みであること。

(c)　持出簿への記載内容について媒体利用管理者が指名する当該任務を代行する警部補相当職以上の者から確認を受けること。

(d)　媒体利用管理者が、少なくとも１日のうちに１回は、当該外部記録媒体の管理状況を目視により確認すること。

b　外部記録媒体の持ち出しの特例

(a)　職員は、警察署等において、課長等が休暇や出張等により不在で同室に警部相当職以上の者が配置されていない場合であって、別室（他の課等）の警部相当職以上の者の許可を得ることが困難である場合は、当該課長等が指名した警部補相当職の者に、一時的に持ち出しに係る許可を得ることができる。

(b)　職員は、外部記録媒体の持ち出しが保管場所と同一の敷地内であり、持ち出したその日のうちに持ち出しが終了する見込みの場合に限っては、持ち出しに係る手続を、持出簿によらず口頭により行うことができる。

(c)　職員は、ａの規定にかかわらず、次に掲げる場合は、持出簿への記載を省略することができる。ただし、デジタルカメラで撮影した写真の活用について（令和４年２月７日付け通達乙刑総発第78号ほか）に規定するものを除く。

・　あらかじめ外部記録媒体管理簿において外部記録媒体を持ち出す職員が一に指定されている場合であって、当該職員が当該外部記録媒体を持ち出したその日のうちに持ち出しが終了する見込みである場合。ただし、持ち出し中に、その日のうちに持ち出しが終了しないことが判明した場合には、当該持ち出しについて、ａに規定する手続を執ること。また、当該外部記録媒体は、使用しない場合は、媒体利用管理者が鍵のかかる保管庫において集中管理し、さらに、媒体利用管理者が、少なくとも１日のうち１回は、当該外部記録媒体等の管理状況を目視により確認すること。

・　当直勤務に従事する職員が、当直勤務用として指定された外部記録媒体を持ち出す場合。この場合において、当該外部記録媒体は、原則として、当直勤務を取りまとめる所属において管理すること。また、当直長は、当直勤務において当該外部記録媒体を使用する者を指名するとともに、当直勤務の終了後の報告時に、併せて当該外部記録媒体を当直勤務を取りまとめる所属に返却すること。

・　交替制勤務に従事する職員が、交替制勤務用として指定された外部記録媒体を持ち出す場合。この場合において、当該職員の所属の

上級の職員であって、警部相当職以上の者は、定期的に当該外部記録媒体の管理状況を確認すること。

c　警察以外の機関の電子計算機への接続

職員は、外部記録媒体を警察以外の機関の電子計算機に接続する予定があるときは、持ち出す前に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すること。

d　持ち出し終了時の手続

職員は、外部記録媒体の持ち出しが終了したときは、職務上必要がある管理対象情報を電子計算機に取り込んだ後、速やかに当該外部記録媒体から管理対象情報を削除すること。また、持出簿に持出終了日時を記載し、持ち出し時に許可を与えた者から紛失のない旨の確認を受けること。

なお、b(a)の手続により持ち出したときは、前記のほか、課長等から事後の確認も受けなければならない。

e　持出簿の確認

職員は、持出簿について、月に1回以上運用管理者又は運用管理者が指名する当該任務を代行する警視相当職以上の者の確認を受けること。

(ｳ)　外部記録媒体の利用

a　職員は、外部記録媒体を電子計算機に接続する際には、平文・暗号文の別、目的、外部記録媒体を接続する電子計算機を明らかにし、媒体利用管理者に申請した上で利用すること。また、外部記録媒体に管理対象情報を出力する際の平文・暗号文の別については、cからeまでに定めるところにより、選択すること。

なお、外部記録媒体の利用が技術的に制限されていない場合には、この限りでない。

b　aに係る申請を受けた媒体利用管理者は、必要最小限の範囲で許可すること。

c　職員は、管理対象情報を外部記録媒体に出力するときは、警察が管理する電子計算機以外の電子計算機では技術的に復号できない暗号化機能を用いること。

d　職員は、暗号化を行う電子計算機と復号を行う電子計算機とで同一の暗号化ソフトウェアが導入されていないときは、cの規定にかかわらず、自己復号型暗号化機能を用いることができる。

e　職員は、次に掲げる場合は、c及びdの規定にかかわらず、平文で出力することができる。

(a)　機密性１（低）情報を出力するとき。

(b)　電子計算機に暗号化機能が設けられていないとき。

(c)　一の電子計算機に保存された管理対象情報を同一の庁舎内に設置された他の電子計算機に移すために出力するとき。

f　職員は、外部記録媒体の利用が終了したときは、職務上必要がある管理対象情報を電子計算機に取り込んだ後、速やかに当該外部記録媒体から管理対象情報を削除すること。

g　媒体利用管理者は、職員が外部記録媒体を用いて入出力したファイル名及びファイルサイズに係るログを定期的に確認すること。

h　媒体利用管理者は、bに係る許可について、自所属の上級の職員（夜間・休日の当直責任者及び副当直長を除く。）による確認を受けること。

i　職員は、g及びhの検証結果について、情報セキュリティ管理者が別に定める方法により行うこと。

j　職員は、管理対象情報を取り扱った外部記録媒体を廃棄する場合には、情報の抹消を実施すること。

キ　個人所有の機器等

対策基準第８の１(2)エに基づき、個人所有の機器等の利用時の基本的対策について、次のとおり定める。

(ｱ)　個人所有の機器等の職務上の利用禁止

a　職員は、(ｳ)aに定める場合を除き、個人所有の機器等に管理対象情報を保存しないこと。

b　職員は、(ｳ)に定める場合を除き、個人所有の機器等を警察情報システムに接続しないこと。

c　職員は、(ｳ)に定める場合を除き、個人所有の機器等において、管理対象情報の処理を行わないこと。

(ｲ)　個人所有の機器等の利用時の対策

職員は、(ｳ)ａ又はｂに基づき個人所有の端末を利用する場合は、次に掲げる対策を実施すること。

ａ　主体認証情報による端末ロックの常時設定

ｂ　主体認証情報の厳格な管理

ｃ　ＯＳやアプリケーションへの最新のセキュリティパッチの適用

ｄ　不正プログラム対策ソフトウェアの導入及び最新のパターンファイルの適用並びに定期的な不正プログラム検査の実施（有効な不正プログラム対策ソフトウェアが提供されていない場合を除く。）

ｅ　警察が提供する業務専用アプリケーションの利用（業務専用アプリケーションを提供する場合のみ）

ｆ　次に掲げる事項を例とする禁止事項の遵守

(a)　ＯＳ、警察が提供する業務専用アプリケーション等の改造

(b)　安全性が確認できないアプリケーションのインストール及び利用

(c)　利用が禁止されているソフトウェアのインストール及び利用

(d)　許可されない電気通信回線サービスの利用（利用する回線を限定する場合に限る。）

ｇ　次に掲げる事項を例とする情報漏えい対策

(a)　盗み見に対する対策（のぞき見防止フィルタの利用等）

(b)　盗難・紛失に対する対策（端末の放置の禁止、利用時以外のシャットダウン及びネットワークの切断等）

(c)　利用する場所や時間の限定

(d)　端末の盗難・紛失が発生した際の緊急対応手順の把握

(ｳ)　個人所有の機器等の利用に係る特例

ａ　個人所有の携帯電話機

(a)　職員は、職務上やむを得ず個人所有の携帯電話機（以下「個人所有携帯電話機」という。）を使用（音声通話機能のみを使用するものを除く。）することが想定されるときは、あらかじめ運用管理者の許可を得ること。

(b)　運用管理者は、(a)に係る許可を与えた個人所有携帯電話機につい

て、職員の氏名、電話番号、メールアドレス、端末の製造業者名、機種名、スマートフォン等のＯＳの種類及びバージョンを記載した個人所有携帯電話機管理簿を作成し、保管すること。また、当該管理簿は、個人所有携帯電話機の増減のあった都度、更新すること。

(c)　職員は、(a)に係る許可を受けた個人所有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の閲覧時にパスワード等の主体認証情報の入力を求められるよう設定すること。また、当該個人所有携帯電話機については共用・貸与（家族との共用等を含む。）しないこと。

(d)　職員は、職務上の理由により管理対象情報を伝達する必要があるときは、(a)に係る許可を受けた個人所有携帯電話機の電子メール機能、写真撮影機能、その他警察庁情報セキュリティ管理者が認めた機能を使用することができる。

なお、伝達する情報が機密性２（中）情報であり、伝達手段が複数存在する場合には、警察庁情報セキュリティ管理者が定めた基準に従い、より安全な手段を用いて伝達すること。

(e)　職員は、(d)の規定に従って個人所有携帯電話機を使用する場合、取り扱う管理対象情報は機密性２（中）情報までとし、職務上不要となった管理対象情報は速やかに消去すること。

なお、写真撮影機能の使用に当たって、個人所有携帯電話機本体に画像情報等を保存することが困難であるときは、個人所有携帯電話機に付属する外部記録媒体に、一時的に画像情報等を保存することができる。

(f)　職員は、(d)の規定に従って個人所有携帯電話機を使用した後に、当該個人所有携帯電話機に保存された管理対象情報を電子計算機に取り込む必要があるときは、自所属の上級の職員であって警部相当職以上の者（夜間・休日の当直責任者及び副当直長を除く。）に報告(口頭による報告を含む。)した上で、不正プログラムが侵入しないよう安全な方法で当該管理対象情報を電子計算機に取り込んだ後、速やかに個人所有携帯電話機本体及び付属する外部記録媒体から管理対象情

報を削除すること。

(g)　職員は、(a)に係る許可を受けた個人所有携帯電話機を用い、犯罪捜査において個人所有携帯電話機で約款や規約等によるクラウドサービスを利用する特段の必要がある場合には、第３の２(2)イ(ｱ)に基づき別に定めるところにより、利用することができるものとする。

(h)　職員は、大規模災害、重大テロ等の緊急事態（訓練を含む。）において、職務上緊急に管理対象情報を伝達する必要がある場合は、個人所有携帯電話機を使用することができる。

なお、本項における個人所有携帯電話機の使用にあっては、(a)に規定する運用管理者の許可を得たものとみなすとともに、(ｲ)、(b)及び(c)の規程を適用しない。

b　テレワーク及びモバイル勤務に使用する個人所有端末

テレワーク及びモバイル勤務において個人所有の端末を使用する場合には、次に掲げる事項を遵守すること。ただし、ｃ(a)の場合はこの限りでない。

(a)　職員は、第５の１(1)ウ(ｱ) d (a)から(c)までに掲げる機能（警察が整備したものに限る。）を用いる場合に限り、個人所有の端末をテレワーク及びモバイル勤務で利用することができる。

(b)　職員は、テレワーク及びモバイル勤務において個人所有の端末を利用する際は、次に掲げる項目を明らかにして運用管理者に申請すること。また、運用管理者は当該申請に係る手続の内容を記録しておくこと。

・　テレワークの申請者の氏名、所属、連絡先

・　利用する端末の契約者の名義（スマートフォン等の通信事業者と契約を行う端末の場合）

・　利用する端末の製造業者名、機種名、ＯＳの種類及びバージョン

・　利用目的、取り扱う情報の概要、要機密情報の利用の有無等

・　利用する電気通信回線サービス

・　利用する期間

(c)　運用管理者は、利用状況に応じて、次に掲げる事項を例とした利用

許諾条件を示し、利用者の同意を承諾書へのサイン等により証拠として残しておくこと。

・　管理対象情報の分類及び取扱制限に応じた取扱いの遵守

・　定められた安全管理措置の遵守

・　組織による利用状況の情報収集の承諾

・　組織による利用端末の制御及び端末の設定変更の承諾

・　情報セキュリティインシデントの可能性を認知した際の迅速な届出

・　機種変更や端末交換の際の再届出の遵守

・　個人所有の端末の第三者（家族等の同居するものを含む。）への貸与の禁止の遵守

・　その他、システムセキュリティ責任者等の管理責任者の指示の遵守

(d)　職員は、テレワーク及びモバイル勤務において利用中の個人所有の端末に紛失・盗難が発生した場合は、対策基準第２の２(4)ア(ｱ)に規定する情報流出事案と同様の手続を執ること。

(e)　職員は、(b)の申請内容に変更が生じた場合は、遅滞なく再申請すること。

(f)　職員は、(b)の申請による利用が終了した際には、運用管理者に報告すること。

c　その他

(a)　職員は、モバイル勤務及び自宅でのテレワークにおいて個人所有の機器等を使用して、インターネット上の情報の閲覧・保存・印字を行うことができる。

(b)　職員は、個人所有のイヤホン及びヘッドセットを警察情報システムに接続して使用することができる。ただし、アナログ端子により接続するものに限る。

ク　簿冊の様式及び保存期間

ア、イ、ウ、オ、カ及びキに定める各簿冊の様式等については、別に定める。

(3)　識別コード・主体認証情報の取扱い

対策基準第８の１(4)における識別コード・主体認証情報の取扱いについて、次のとおり定める。

ア　職員は、自己に付与された識別コードを適切に管理するため、次に掲げる措置を講ずること。

(ｱ)　知る必要のない者に知られるような状態で放置しない。

(ｲ)　他者が主体認証に用いるために付与又は貸与しない。

(ｳ)　識別コードを利用する必要がなくなった場合には、定められた手続に従い、識別コードの利用を停止する。

イ　職員は、知識による主体認証情報を用いる場合には、次の管理を徹底すること。

(ｱ)　自己の主体認証情報を他者に知られないように管理する。

(ｲ)　自己の主体認証情報を他者に教えない。

(ｳ)　主体認証情報を忘却しないように努める。

(ｴ)　主体認証情報を設定する場合には、容易に推測されないものにする。

(ｵ)　異なる識別コードに対して、共通の主体認証情報を用いない。

(ｶ)　異なる警察情報システムにおいて、識別コード及び主体認証情報についての共通の組合せを用いない（シングルサインオンの場合を除く。）。

(ｷ)　識別コード及び主体認証情報を他の職員と共用している場合であって、当該他の職員が異動等により当該識別コードを利用する必要がなくなった場合には、当該主体認証情報を速やかに変更する。

ウ　職員は、ＩＣカード等の主体認証情報格納装置による主体認証を行う場合には、次の管理を徹底すること。

(ｱ)　主体認証情報格納装置を本人が意図せずに使われることのないように安全措置を講じて管理する。

(ｲ)　主体認証情報格納装置を権限のない者に付与又は貸与しない。

(ｳ)　主体認証情報格納装置を紛失しないよう管理する。紛失した場合には、定められた手続に基づき、直ちにその旨を報告する。

(ｴ)　主体認証情報格納装置を利用する必要がなくなったときは、システムセキュリティ責任者又は運用要領等に定められた担当部署に返納する。

(4)　不正プログラム感染防止

対策基準第８の１(6)における不正プログラム感染防止について、次のとおり定める。

ア　職員は、不正プログラム感染を回避するため、不正プログラム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ないこと。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まないこと。

イ　職員は、外部から情報やソフトウェアを端末及びサーバ等に取り込む場合又は外部に情報やソフトウェアを提供する場合には、不正プログラム感染の有無を確認すること。

ウ　職員は、不審なウェブサイトの閲覧等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利用する場合を除き、不正プログラムに感染するリスクを低減する警察情報システムの利用方法として、次に掲げる措置を講ずること。

(ｱ)　不審なウェブサイトを閲覧しない。

(ｲ)　アプリケーションの利用において、マクロ等の自動実行機能を無効にする。

(ｳ)　安全性が確実でないソフトウェアをダウンロード又は実行しない。

エ　職員は、不正プログラムに感染したおそれがある場合には、直ちにネットワークケーブルを切り離すなどして回線を切断するとともに、対策基準第２の２(4)に定める方法により、担当部署に連絡すること。

(5)　ウェブ会議サービスの利用時の対策

対策基準第８の１(7)におけるウェブ会議サービスの利用時の対策について、次のとおり定める。

ア　職員は、ウェブ会議サービスの利用に当たり、次に掲げる情報セキュリティ対策を実施すること。

(ｱ)　警察が管理する電子計算機を利用すること。

(ｲ)　自組織において利用を許可されたウェブ会議サービスを利用すること。

(ｳ)　利用するウェブ会議サービスのソフトウェアが、最新の状態であることを確認すること。

(ｴ)　可能な限りエンドツーエンドの暗号化を行うこと。

(ｵ)　ウェブ会議サービスの議事録作成機能、自動翻訳機能、録画機能等、エンドツーエンドの暗号化を利用できなくなる機能は可能な限り使用しないこと。

イ　職員は、ウェブ会議に無関係な者を参加させないために、次に掲げる事項を例とする対策を行うこと。

(ｱ)　会議室にアクセスするためのパスワード等をかける。

(ｲ)　会議の参加者に会議室にアクセスするためのパスワード等を通知する際は、第三者に知られないよう安全な方法で通知する。

(ｳ)　会議を非公開にする。

(ｴ)　待機室を設けて参加者と確認できた者だけを会議室に入室させる。

(ｵ)　ウェブ会議の主催者が事前に登録した者だけを会議室に入室させる。

(ｶ)　なりすましや入れ替わりが疑われるなどの不審な参加者を会議室から退室させる。

2　ソーシャルメディアサービスによる情報発信

対策基準第８の２におけるソーシャルメディアサービスによる情報発信時の対策について、次のとおり定める。

(1)　職員は、アカウント運用ポリシーを策定し、ソーシャルメディアのアカウント設定における自由記述欄又はソーシャルメディアアカウントの運用を行っている旨の表示をしている警察のウェブサイト上のページに、アカウント運用ポリシーを掲載すること。特に専ら情報発信に用いる場合には、その旨をアカウント運用ポリシーに明示すること。

(2)　職員は、ＵＲＬ短縮サービスにおいて、利用するソーシャルメディアサービスが自動的にＵＲＬを短縮する機能を持つ場合等、その使用が避けられない場合を除き、使用しないこと。

(3)　職員は、警察のアカウントによる情報発信が実際の警察のものであると認識できるようにするためのなりすまし対策として、次に掲げる対策を講ずること。

ア　警察からの情報発信であることを明らかにするために、自組織のウェブサイト内において、利用するソーシャルメディアのサービス名と、そのサービスにおけるアカウント名又は当該アカウントページへのハイパーリンクを明

記するページを設けること。

イ　警察からの情報発信であることを明らかにするために、アカウント名やアカウント設定の自由記述欄等を利用し、警察が運用していることを利用者に明示すること。

ウ　運用しているソーシャルメディアのアカウント設定の自由記述欄において、当該アカウントの運用を行っている旨の表示をしている自組織のウェブサイト上のページのＵＲＬを記載すること。

エ　ソーシャルメディアの提供事業者が、アカウント管理者を確認し、それを表示等する、認証アカウント（公式アカウント）等のアカウントの発行を行っている場合には、可能な限りこれを取得すること。

(4)　職員は、第三者が何らかの方法で不正にログインを行い、偽の情報を発信するなどのアカウント乗っ取りを防止するため、ソーシャルメディアのログインパスワードや認証方法については、次に掲げる対策を講ずること。

ア　ログインパスワードには十分な長さと複雑さを持たせた容易に推測されないものを設定するとともに、パスワードを知る担当者を限定し、パスワードの使い回しをしないこと。

イ　二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用すること。

ウ　ソーシャルメディアへのログインに利用する端末を紛失した又は当該端末が盗難に遭った場合は、当該端末を悪用され、アカウント乗っ取りの可能性があるため、当該端末の管理を厳重に行うこと。

エ　ソーシャルメディアへのログインに利用する端末が不正アクセスされることを防止するため、当該端末には適切な情報セキュリティ対策を講ずること。

(5)　職員は、なりすましや不正アクセスを確認した場合は、次のとおり対処すること。

ア　自組織のウェブサイト内において、なりすましアカウントが存在することや当該ソーシャルメディアを利用していないこと等の周知を行い、信用できる機関やメディアを通じて注意喚起を行うこと。

イ　アカウント乗っ取りを確認した場合には、被害を最小限にするため、ログインパスワードの変更やアカウントの停止を速やかに実施し、自組織のウェ

ブサイト等で周知を行うとともに、対策基準第２の２(4)イ(ｱ)、(ｲ)及び(ｷ)に基づき、適切に対処すること。

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

対策基準第８の３(1)におけるテレワーク及びモバイル勤務の実施環境における対策について、次のとおり定める。

ア　システムセキュリティ責任者は、ＶＰＮ回線等を整備してリモートアクセス環境を構築する場合は、次に掲げる事項を例とする対策を講ずること。

(ｱ)　利用開始及び利用停止時の申請手続の整備

(ｲ)　通信を行う端末の識別又は認証

(ｳ)　利用者の認証

(ｴ)　通信内容の暗号化

(ｵ)　主体認証ログの取得及び管理

(ｶ)　アクセス可能な情報システムの制限

(ｷ)　リモートアクセス中の他の電気通信回線との接続禁止

(ｸ)　不正な通信の有無の監視

(ｹ)　端末画面の接写対策並びに、情報の持ち出し及び印字の禁止（端末で対策されている場合は除く。）

イ　システムセキュリティ責任者は、なりすましの対策として、リモートアクセスする端末が、許可されたものであるかどうかを確認するために、次に掲げる事項を例とする対策を行うこと。

(ｱ)　証明書による端末確認

(ｲ)　ソフトウェア認証による端末確認

ウ　システムセキュリティ責任者は、リモートアクセスする個人所有の端末を最新の脆弱性対策や不正プログラム対策が施されている端末に限定するために、次に掲げる事項を例とする対策を行うこと。

(ｱ)　テレワーク及びモバイル勤務で利用する警察情報システムに接続する前に、端末に脆弱性や不正プログラムの対策が行われているかを確認できる、検疫ネットワークの整備

(ｲ)　テレワーク及びモバイル勤務で利用する端末の脆弱性や不正プログラム

の対策の状況を自動的に確認するための、ＩＴ資産管理の自動化

(2)　実施時における対策

対策基準第８の３(2)におけるテレワーク及びモバイル勤務の実施時における対策について、次のとおり定める。

ア　職員は、テレワークの実施申請及び承認並びにテレワークの実施報告については、職員の勤務管理のために別途定められたテレワークの実施に係る規程に従うこと。

イ　職員は、モバイル勤務の実施申請及び承認並びにモバイル勤務の実施報告については、１(2)ウ(ｱ)及び対策基準第３の１(5)ウの手続を実施すること。

ウ　職員は、テレワークで取り扱うことができる管理対象情報については、職員の勤務管理のために別途定められたテレワークの実施に係る規程に従うこと。また、モバイル勤務で取り扱うことができる管理対象情報については、利用するモバイル端末について定められた規定に従うこと。

エ　職員は、端末で利用する、内蔵された電磁的記録媒体や外部記録媒体等には原則として要機密情報を保存しないこと。他に手段がなく保存が必要な場合は、文書ファイルにパスワードを設定するなどの暗号化の措置を講ずること。

オ　対策基準第８の３(2)アにおけるテレワーク及びモバイル勤務の実施前並びに実施後に確認すべき項目について、次に掲げる事項を例とする。ただし、システムセキュリティ責任者が技術的に担保できていると判断した項目については、確認を不要とすることができる。

(ｱ)　実施前にチェックする項目

a　管理対象情報の管理

b　脆弱性対策

c　情報漏えい対策

d　不正プログラム対策

e　情報セキュリティインシデント対策

(ｲ)　実施後に行うチェックの項目

a　不正プログラム対策

b　管理対象情報の管理

ｃ 情報漏えい対策

カ　職員は、次に掲げる項目を例とする画面ののぞき見や盗聴から発生する情報漏えい対策を講ずること。

(ｱ)　背後に人が立たないよう背後に通路がない場所で壁を背にする位置に座りテレワーク又はモバイル勤務を行う。

(ｲ)　ウェブ会議等、音声を扱う場合は、ヘッドセットを使用するなど、内容が周囲に漏れないよう注意する。

(ｳ)　同居する者に対し知り得た情報を他人に漏らさないよう協力を求める。

(3)　警察情報システムへの接続に利用する電気通信回線

対策基準第８の３(2)ウに基づき、警察情報システムへの接続に利用する回線について、次のとおり定める。

ア　テレワーク及びモバイル勤務時の、個人等が契約したインターネット回線を利用した警察情報システムへの接続中には、第５の３及び対策基準第６の３のうち、第５の３(1)キ及び(5)並びに対策基準第６の３(1)ア(ｱ)及び(ｵ)の要件を適用しない。ただし、無線ＬＡＮ回線を利用する場合は、次に掲げる対策を追加して実施すること。

(ｱ)　WPA2-Personal又はWPA3-Personal相当の機能により認証を行うこと(脆弱な暗号化方式は利用しない。)。

(ｲ)　無線ＬＡＮ装置のＳＳＩＤを推測困難なものに設定すること（メーカー名や名前などを設定しない。)。

(ｳ)　ＰＳＫをランダムで長いものに設定すること。

(ｴ)　モバイルWi-Fiルータや携帯電話機のテザリング機能を利用する場合、不要時には無線ＬＡＮ装置の出力を停止すること。

イ　テレワーク及びモバイル勤務時に、警察情報システムへの接続に利用する回線については、自宅用に契約した電気通信回線や公費で整備した電気通信回線等、信頼性の高い電気通信回線を使用し、次に掲げる電気通信回線を例とした情報セキュリティ対策の内容が不明又は不十分なものは使用しないこと。

(ｱ)　公衆無線ＬＡＮ

(ｲ)　宿泊施設等が提供する無料ネットワーク　　＜別紙・別表省略＞