

保存期間 5 年

通達乙情管第332号

令和 5 年 3 月 23 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」（令和 5 年 3 月 23 日付け通達乙情管発第331号ほか別添）第 9 に基づき、別添のとおり「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」を定め、令和 5 年 4 月 1 日から実施することとしたので、事務処理上遺漏のないようにされたい。

なお、本通達の実施に伴い、以下の通達は、令和 5 年 3 月 31 日限り、廃止する。

- 1 警察情報システムにおける運用保守に係る細目の改正について（令和 4 年 3 月 28 日付け情管発第334号）
- 2 警察情報システム及び管理対象情報の取扱いに係る細目の改正について（令和 4 年 3 月 28 日付け通達乙情管発第335号）
- 3 警察情報システムの情報セキュリティ要件に係る細目の改正について（令和 4 年 3 月 28 日付け通達乙情管発第336号）
- 4 情報セキュリティインシデント対処要領に係る細目の改正について（令和 4 年 3 月 28 日付け通達乙情管発第338号）

令和5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
1	情報セキュリティアドバイザーが行う助言	1
2	情報セキュリティ対策推進事務局の事務	1
3	県警CSIRTの運営に係る事項	1
(1)	県警CSIRTの構成	1
(2)	総括班	1
(3)	解析班	2
(4)	支援班	2
4	例外措置	3
(1)	例外措置手続	3
(2)	例外措置の運用	3
5	情報セキュリティインシデントへの対処	4
(1)	報告先	4
(2)	様式	4
6	情報セキュリティ監査	4
第2	管理対象情報の取扱い	4
1	管理対象情報の取扱い	4
(1)	管理対象情報の分類及び取扱制限の決定・明示	4
(2)	管理対象情報の利用・保存	5
(3)	管理対象情報の運搬・送信	5
(4)	管理対象情報の消去	6
2	管理対象情報を取り扱う区域の管理	6
(1)	区域における対策の基準	6
(2)	区域ごとの対策の決定	8
(3)	区域における対策の実施	8
第3	外部委託	8
1	業務委託	9
(1)	業務委託に係る契約	9

(2) 業務委託における情報の取扱い	9
2 外部サービスの利用	9
(1) 外部サービスの利用に係る手続	9
(2) 要機密情報を取り扱う場合	10
(3) 要機密情報を取り扱わない場合	20
第4 警察情報システムのライフサイクル	20
1 警察情報システムに係る文書等の整備	20
(1) 情報システムに係る台帳等の整備	20
(2) 情報システム関連文書の整備	21
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	22
(1) 警察情報システムの企画・要件定義	22
(2) 警察情報システムの調達・構築	23
(3) 警察情報システムの運用・保守	23
(4) 警察情報システムの更改・廃棄	27
第5 警察情報システムの情報セキュリティ要件	27
1 警察情報システムの情報セキュリティ機能	27
(1) 主体認証機能	27
(2) アクセス制御機能	30
(3) 権限の管理	31
(4) 証跡の取得・管理	31
(5) 暗号・電子署名	36
2 情報セキュリティの脅威への対策	37
(1) ソフトウェアに関する脆弱性対策	37
(2) 不正プログラム対策	38
(3) サービス不能攻撃対策	39
(4) 標的型攻撃対策	40
(5) 外部記録媒体の利用に係る対策	40
3 アプリケーション・コンテンツの作成・提供	41
(1) 不正なウェブサイトへの誘導防止	42

(2) アプリケーション・コンテンツの告知	42
第6 警察情報システムの構成要素	42
1 端末・サーバ等	42
(1) 端末	42
(2) サーバ等	47
(3) 複合機・特定用途機器	49
2 電子メール・ウェブ等	50
(1) 電子メール	50
(2) ウェブ	50
(3) ドメインネームシステム（DNS）	52
(4) データベース	52
3 電気通信回線	53
(1) 電気通信回線の導入時の対策	53
(2) 電気通信回線の運用時の対策	55
(3) 無線LAN環境導入時の対策	56
第7 警察情報システムの利用	57
1 警察情報システムの利用	57
(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	57
(2) 警察情報システム等の利用時の基本的対策	58
(3) 識別コード・主体認証情報の取扱い	71
(4) 不正プログラム感染防止	72
(5) ウェブ会議サービスの利用時の対策	73
2 ソーシャルメディアサービスによる情報発信	74
3 テレワーク及びモバイル勤務	75
(1) 実施環境における対策	75
(2) 実施時における対策	76
(3) 警察情報システムへの接続に利用する回線	78
別紙1 契約の相手方に遵守させるべき事項の例	
別紙2 機器等の調達時に仕様書・契約書等に記載すべき事項の例	

別表 (第6の1(1)ウ(ア) e、(イ) g、(3)イ(ク)及び3(1)イ(イ)関係)

## 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5年3月23日付け通達甲情管発第331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書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(4)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C S I R T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

イで掲げる連絡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。

(7) 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C S I R T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(7)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) c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・休日にあつ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) 捜査情報の保秘及び捜査資料管理の徹底について（平成19年7月24日付け刑総発第488号ほか）2(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當なものとして、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つて、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)ア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じること。

イ 対策基準第3の1(5)イ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、次の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つ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、次の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。

### 2 管理対象情報を取り扱う区域の管理

#### (1) 区域における対策の基準

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の基準として、区域の分類、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 0

各庁舎の敷地内であつて、職員以外の者が自由に立ち入ることのできる区域は、一の区域とし、クラス 0 に分類する。

##### イ クラス 1

各庁舎における廊下等、職員の共用の区域は、一の区域とし、クラス 1 に分類するとともに、区域情報セキュリティ管理者に、当該庁舎の庁舎管理に関する事務を処理する者を指名し、次の対策を講ずること。

(ア) 職員以外の者が不正に立ち入ることがないように壁、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。

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つては、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。

#### ウ クラス2

執務室は、所属（茨城県警察処務に関する訓令（昭和46年茨城県警察本部訓令第50号）第2条第1号に規定する所属をいう。以下同じ。）ごとに一の区域とし、クラス2に分類するとともに、区域情報セキュリティ管理者に、各所属の長を指名し、次の対策を講ずること。

- (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、機器の持込みによる不正な撮影及び録音が行わ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、当該境界においてイに定める対策を講ずること。

#### エ クラス3

警察情報システムに係る機械室は、室ごとに一の区域とし、クラス3に分類するとともに、区域情報セキュリティ管理者に、当該機械室を管理する所属の長を指名し、次の対策を講ずること。

- (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。
- (キ) 自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策を講ずること

## (2) 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、(1)に定める対策のみでは安全性が確保できない場合は、当該区域において実施する個別の対策を決定することとする。

## (3) 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、(1)及び(2)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、(1)の基準による運用を困難と認めるときは、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、(1)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) 業務委託に係る契約

ア 対策基準第4の1(1)カにおける委託の相手方に遵守させるべき事項について、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を仕様書等に盛り込むこと。

イ 対策基準第4の1(1)における業務委託に係る契約について、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、委託先の情報セキュリティ水準の評価を行うこと。

(ア) ISO/IEC 27001等の国際規格とそれに基づく認証制度の活用

(イ) 情報セキュリティガバナンスの確立促進のために開発された自己評価によるツール等の応用

### (2) 業務委託における情報の取扱い

対策基準第4の1(3)での業務委託における情報の取扱いについて、職員は、一般に公開する仕様書の作成に当たっては、次に掲げる情報の記載の是非を検討すること。

ア 情報システムへの不正な侵入を容易にする情報

(ア) OS又はウイルス対策ソフトウェアの名称、電子計算機本体の型番等ソフトウェアを特定させる情報

(イ) ネットワークの構成、アドレス体系を特定させる情報

イ 暗号の種類、鍵長、暗号装置の名称、暗号装置の製造業者名等暗号の解読を容易にする情報

## 2 外部サービスの利用

### (1) 外部サービスの利用に係る手続

対策基準第4の2(1)ア(ア)a、イ(ア)及び(2)アにおける手続について、外部サービスを利用する場合には、警察情報システム又はその一部として調達・導入される外部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外部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、次の事項を明らかにして対策基準第4の2(1)エ(エ)に定める許可権限者に申請を行うこと。ただし、警察情報システム上で外部サ

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。また、申請内容に変更が生じた場合には、速やかに許可権限者に連絡すること。

ア 外部サービスの名称（必要に応じて機能名までを含む。）

イ 外部サービスの種類（クラウドサービス、その他の外部サービスの別）

ウ 外部サービス提供者の名称

エ 利用目的（業務内容）

オ 利用可能な警察情報システムの範囲

カ 取り扱う管理対象情報の分類

キ 外部サービスの利用規約（契約）内容

ク 取得するアカウント（外部サービス利用者、管理者及びその他）及び主体  
認証情報

ケ 接続方法（外部回線から直接外部サービスへ接続することの可否）

コ 利用期間

サ 利用申請者（所属・氏名）

シ 外部サービス利用者の範囲

ス 選定時の確認結果

セ 利用において講ずべき対策

## (2) 要機密情報を取り扱う場合

ア 外部サービスの選定（クラウドサービスの場合）

(ア) 対策基準第4の2(1)ア(ア)aにおける利用判断基準について、次に掲げる事項をクラウドサービスの利用条件として、利用可能な業務及び警察情報システムの範囲を判断した上で、(1)に定める手続により許可を得ること。

a 情報セキュリティ管理者と協議の上、講ずべき対策を定めること。

b 次に掲げる事項を含む対策を講じること。

(a) (イ)、(ウ)a及び(エ)に定めるクラウドサービスの選定

(b) 対策基準第4の2(1)ウに定める外部サービスの利用に係る調達・  
契約

(c) オ及び対策基準第4の2(1)オに定める外部サービスを利用した警

#### 警察情報システムの導入・構築時の対策

(d) カ及び対策基準第4の2(1)カ(イ)に定める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

(e) 対策基準第4の2(1)キに定める外部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

c 次に掲げる事項に留意すること。

(a) サーバ等の故障や外部サービス提供者の運用手順誤り等により、サーバ等に保存されている情報が滅失して復元不可能となるおそれがあること。

(b) サーバ装置上の要保全情報が第三者等により改ざんされ、復元が困難となるおそれがあること。

(c) サービスが突然停止されるおそれがあること。

(d) 約款や利用規約等が予告なく一方的に変更され、セキュリティ設定が変更されるおそれがあること。

(e) 情報の取扱いが保証されず、一旦記録された情報を確実に消去することができないおそれがあること。

(f) 入力した情報を蓄積し、関心事項等が分析されるおそれがあること。

(イ) 対策基準第4の2(1)ア(ア) aにおけるリスク及びその低減措置について、次のとおり定める。

a 外部サービスは、そのサービス提供の仕組みの詳細を利用者が知ることがなくても手軽に利用できる反面、外部サービス提供者の運用の詳細が公開されないために情報セキュリティ対策の運用において必要な情報の入手が困難であること。

b オンプレミスと外部サービスの併用や外部サービスと他の外部サービスの併用等、多様な利用形態があるため、利用者と外部サービス提供者との間の責任分界点やサービスレベルの合意が容易でないこと。

c 外部サービス提供者が所有する資源の一部を利用者が共有し、その上に個々の利用者が管理する情報システムが構築されるなど、不特定多数の利用者の情報やプログラムを一つの外部サービス基盤で共用することとなるため、情報が漏洩するリスクがあること。

- d 外部サービスで提供される情報が国外で分散して保存・処理されている場合、裁判管轄の問題や国外の法制度が適用されることによるコントリーリスクが存在すること。
  - e サーバ等の整備環境が外部サービス提供者の都合で急変する場合、サプライチェーン・リスクへの対策の確認が容易でないこと。
- (ウ) 対策基準第4の2(1)ア(ア) bにおける外部サービス提供者の選定基準について、次のとおり定める。
- a 「政府情報システムのためのセキュリティ評価制度（ISMAP）」（以下「ISMAP」という。）の管理基準のうち、ガバナンス基準及びマネジメント基準における全ての基準、管理策基準における統制目標（3桁の番号で表現される項目）及び末尾にBが付された詳細管理策（4桁の番号で表現される項目）を原則として全て満たすこと。
  - b 1(1)イに定める委託先の情報セキュリティ水準の評価を行うこと。
  - c 対策基準第4の1(1)アの各号に掲げる事項を例とした対策を実施可能なこと。
  - d 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、必要に応じて対策基準第4の1(1)イの各号に掲げる事項を実施可能なこと。
- (エ) 対策基準第4の2(1)ア(ア) cにおける情報セキュリティ要件の策定に当たっては、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を求めること。
- イ 外部サービスの選定（クラウドサービス以外の場合）
- (ア) 対策基準第4の2(1)イ(ア)における利用判断基準について、ア(ア) a から c（b(a)を除く。）をその他の外部サービスの利用条件として、利用可能な業務及び警察情報システムの範囲を判断した上で、(1)に定める手続により許可を得ること。
  - (イ) 職員は、事業者等が不特定多数の利用者に対して提供する、画一的な約款や規約等への同意のみで利用可能となる外部サービス（以下「約款や規約等による外部サービス」という。）を利用しようとする場合は、機密性1（低）情報のみを取り扱うものとする。
  - (ウ) 職員は、(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

る手続により利用することができる。

a 犯罪捜査において約款や規約等による外部サービスを利用する特段の必要がある場合は、(イ)の規定にかかわらず、当該事務を主管する所属の長が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。

b 情報技術の解析において約款や規約等による外部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」、「lg.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。

c 電気等の契約において約款や規約等による外部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(1)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。

(エ) 対策基準第4の2(1)イ(イ)における外部サービス提供者の選定基準について、次のとおり定める。

a 外部サービス提供者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い手順について外部サービス提供者と合意し、定められた手順により情報を取り扱うこと。

b サービスの中断や終了時に際し、円滑に業務を移行するための対策として、次に掲げる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その他の外部サービスの選定条件とし、仕様書等に盛り込むこと。

(a) 取り扱う管理対象情報の可用性区分の分類に応じた、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区分の分類に応じた、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

c その他の外部サービスが提供する部分を含む情報の流通経路全般にわたる情報セキュリティ対策を構築すること。また、当該対策を実現するために、次に掲げる事項を例とする情報セキュリティ要件をその他の外部サービスに求め、契約内容にも含めること。

(a) その他の外部サービスに係るアクセスログ等の証跡の保存及び提供

(b) その他の外部サービスのインターネット接続点の通信の監視

(c) 外部サービス提供者による情報の管理・保管の実施内容の確認

(d) その他の外部サービス上の脆弱性対策の実施内容の確認

(e) その他の外部サービス上の情報に係るRPO（Recovery Point Objective：復旧時点目標）等の指標

(f) その他の外部サービス上で取り扱う管理対象情報の暗号化

(g) 外部サービス利用者の意思による外部サービス上で取り扱う管理対象情報の確実な削除・廃棄

(h) 外部サービス利用者が求める情報開示請求に対する開示項目や範囲の明記

d 1 (1)イに定める委託先の情報セキュリティ水準の評価を行うこと。

e 対策基準第4の1(1)アの各号に掲げる事項を例とした対策を実施可能なこと。

f 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、必要に応じて対策基準第4の1(1)イの各号に掲げる事項を実施可能なこと。

#### ウ 外部サービスの利用に係る調達・契約

(7) 対策基準第4の2(1)ウ(イ)において、仕様書の内容を契約に含める際、外部サービス提供者との情報セキュリティに関する役割及び責任の範囲が明確になっていることを確認すること。

(イ) システムセキュリティ責任者又は運用管理者は、対策基準第4の2(1)ウにおける外部サービスの利用に係る調達・契約において、一般に公開する仕様書の作成に当たっては、1(2)の各号に掲げる情報の記載の是非を検

討すること。

エ 外部サービスの利用承認

(ア) 対策基準第4の2(1)エ(イ)における利用申請の審査について、次のとおり定める。

a 利用申請されたサービスが、外部サービス提供者の選定基準と外部サービスの情報セキュリティ要件の両者を満たしていること。

b 審査は、可能な限り外部サービスの契約前までに行うこと。

(イ) 対策基準第4の2(1)エ(ウ)における外部サービスの記録について、2(1)の各号（キからケ及びスを除く。）に定める事項及び外部サービス管理者を記録し、自組織内で共有すること。

オ 外部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) 対策基準第4の2(1)オ(ア) aにおけるアクセス制御について、必要に応じて次に掲げる対策を講ずること。

a 外部サービスを利用する際に外部サービス提供者が付与又は外部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

b 外部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

c 外部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外部サービス利用者に対する強固な認証技術の利用

d 外部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

e 外部サービス上に保存する管理対象情報や外部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

f 外部サービス利用者による外部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

g 外部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の実施

h 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外部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可否の判

断と認める場合の適切な情報セキュリティ対策の実施

(イ) 対策基準第4の2(1)オ(ア) bにおける暗号化について、必要に応じて次に掲げる対策を講ずること。

a 外部サービス内及び通信経路全般における暗号化の確認

b 関連する法令や規則において暗号化方式を定めている情報システムについて当該定めへの遵守度合いの確認

(ウ) 対策基準第4の2(1)オ(ア) cにおける情報セキュリティ対策について、必要に応じて次に掲げる対策を講ずること。

a 警察情報システムの構築において外部サービスを利用する場合の外部サービス提供者への情報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

b 警察情報システムの構築において、外部サービス上に他の事業者が提供するソフトウェア等を導入する場合の当該ソフトウェアの外部サービス上におけるライセンス規定の確認

(エ) 対策基準第4の2(1)オ(ア) dにおける設計・設定時の誤りの防止について、必要に応じて次に掲げる対策を講ずること。

a 外部サービス上に情報システムを構築する際の外部サービス提供者への設計、構築における知見等の情報の要求とその活用

b 外部サービス上に警察情報システムを構築する際の設定の誤りを見いだすための対策

c 外部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情報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

d 利用する外部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

e 利用する外部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

f 外部サービス内における時刻同期の方法の確認

カ 外部サービスを利用した警察情報システムの運用・保守時の対策対策基準第4の2(1)カ(ア)における対策について、必要に応じて、次に掲げる事項を遵守すること。

- (ア) 責任分界点を意識して外部サービスを利用すること。
- (イ) 利用承認を受けていない外部サービスを利用しないこと。
- (ウ) 外部サービス提供者に対して、契約時に同意した事項又は次に掲げる事項を例とした事項について、定期的にサービスの提供状態を確認すること。
  - a 情報の保存方法、保存場所、伝送経路
  - b 情報の廃棄状況
  - c ログ情報の収集と保存状況
  - d 時刻同期の状況
  - e バックアップの実施状況
  - f 不正アクセスの監視状況
- (エ) 利用する外部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について、事前に確認すること。
- (オ) 外部サービス利用者に外部サービス利用に必要な知識を習得させるため、必要に応じて次に掲げる事項を含む教養を受けさせること。
  - a 外部サービス利用のための規定及び手順
  - b 外部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
  - c 外部サービス利用に関する適用法令や関連する規制等
- (カ) 外部サービス上で利用するIT資産を適切に管理すること。
- (キ) 外部サービス上に保存する管理対象情報に対して、適切に分類し、取扱制限を明示すること。
- (ク) 外部サービスの機能に対する脆弱性対策について、外部サービス利用者の責任範囲を明確化し、適切に情報セキュリティ対策を実施すること。
- (ケ) 外部サービスにおける管理者権限を持つ者の操作等について、適切に記録され保存されていることを確認すること。
- (コ) 外部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見直しを実施すること。
- (サ) 外部サービスのリソース（ネットワーク、仮想マシン等）の設定を変更する機能を使用する場合は、当該機能を確認し、外部サービス利用者を適切に制限すること。
- (シ) 利用する外部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に

より、監視を行うこと。

- (ス) 通信の暗号化について、外部サービス提供者が提供するサービスを利用する場合は、次に掲げる事項を例とする詳細な情報を外部サービス提供者に要求し、リスク評価を行った上で使用すること。
  - a 暗号化に用いる鍵の管理者と鍵の保管場所
  - b 鍵管理機能を外部サービス提供者が提供する場合は鍵管理手順と鍵の種類
  - c 鍵管理機能を外部サービス提供者が提供する場合は鍵の生成から廃棄に至るまでのライフサイクルに関する情報
- (セ) 利用する外部サービスのネットワーク基盤が、当該外部サービスを利用するに当たって必要となるもの以外のネットワークから論理的に分離されていることを確認すること。
- (ソ) 外部サービスの設定を変更する場合における設定の誤りを防止するため、次に掲げる事項を例とする対策を講じること。
  - a 定期的な設定の確認
  - b 外部サービス提供者が提供するセキュリティ設定・監視ツールの利用
  - c 設定権限を与える外部サービス利用者の限定
  - d 外部サービス利用者側の責任範囲の明確化
  - e 開発プロセスへの情報セキュリティ対策の組み込み
  - f 外部サービスの機能追加に係る設定の見直し
- (タ) 外部サービス利用者の操作により利用中の外部サービスに重大な障害をもたらすことが予想される操作については、その操作手順を文書化し、実施の際は外部サービス管理者が指名した監督者の監視の下、実施すること。
- (チ) 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を確実に実施すること。また、外部サービス提供者が提供する機能を利用する場合は、実施状況を確認すること。
- (ツ) 要安定情報を外部サービスで取り扱う場合の十分な可用性を担保するため、復旧に係る手順を策定し、定期的な訓練を実施すること。
- (テ) 外部サービス提供者によるサービス内容の変更が行われる際の事前通知を受けた場合は、その影響範囲、影響度を確認し、サービス停止等が発生

した場合の復旧手順を確認すること。

キ 外部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

対策基準第4の2(1)キ(ア)における対策について、次のとおり定める。

(ア) 外部サービスの利用終了において、外部サービス利用者への影響を考慮して移行計画書又は終了計画書を作成し、外部サービスの利用の許可権限者に承認を得た上で外部サービス利用者に提示すること。また、計画書には、次に掲げる事項を例として記載すること。

a 当該外部サービス名

b サービスの利用終了日時

c 管理対象情報の廃棄日時

d 他の外部サービスへの移行を行う場合は、移行先の外部サービス名及び移行手順

(イ) 作成した移行計画書又は終了計画書は当該サービスを利用する利用者に対して十分な余裕を持って通知すること。

(ウ) 次に掲げる事項を例として、取り扱った全ての情報が外部サービス基盤上から確実に削除されていることを確認すること。

a 仮想リソース（仮想マシン、仮想ストレージ、仮想ネットワーク機器等）

b ファイル（ストレージサービスに格納したファイル、各サービスのログ、開発関連ファイル、設定ファイル等）

c 暗号化された情報の復号に用いる鍵

d ドメイン情報

(エ) 外部サービス提供者が、外部サービスの基盤となる装置等の情報セキュリティを保った処分又は再利用のための方針及び手順を確実に実施していることを確認すること。

(オ) 作成された外部サービス利用者のアカウントを全て削除すること。

(カ) 作成した外部サービス利用者のアカウントが全て削除されていることを確認した上で可能であれば外部サービス管理者のアカウントを削除し、外部サービス提供者に返却すること。また、外部サービス管理者のアカウントについては再利用されないことを外部サービス提供者に確認すること。

(キ) 外部サービス利用者のアカウント以外の特異なアカウント（ストレージアカウント等）を作成した場合は、サービス利用終了時に確実に削除すること。また、当該アカウントを利用して作成された情報についても廃棄されていることを確認すること。

(3) 要機密情報を取り扱わない場合

ア 外部サービス管理者は、クラウドサービスを利用する場合は、次に掲げる事項を例として運用要領等を定めること。

(ア) サービス機能の設定（情報の公開範囲等）に関する定期的な内容確認

(イ) 情報の滅失、破壊等に備えたバックアップの取得

(ウ) 外部サービス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 外部サービス上において要機密情報を取り扱わない場合に適用される規定について、次のとおり定める。

(ア) クラウドサービスを利用する場合

1、2(1)、(2)ア(ア) a、c、(ウ) c、d 及び(2)エの規定を適用する。

(イ) その他の外部サービスを利用する場合

1、2(1)、(2)ア(ア) a、c、イ(ア)、(イ)、(ウ) 及びエの規定を適用する。

#### 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) 情報システムに係る台帳等の整備

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 ネットワーク機器

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 事業者等が提供する情報処理サービスにより情報システムを構築する場合には、次に掲げる事項を含む内容についても台帳として整備すること。

- (ア) 情報処理サービス名
- (イ) 契約事業者
- (ウ) 契約期間
- (エ) 情報処理サービスの概要
- (オ) ドメイン名
- (カ) 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

ソ 情報セキュリティインシデント発生時に報告する内容のうち、情報システムに関する事項

(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、所管する警察情報システムについて、次の関連文書等を整備すること。

- (ア) サーバ等及び端末の仕様書又は設計書
- (イ) 電気通信回線及びネットワーク機器の仕様書又は設計書

イ システムセキュリティ責任者は、必要に応じて、所管する警察情報システムを構成する機器のソフトウェアの名称、バージョン等に関する情報を自動

で収集し、管理する機能を導入すること。

ウ 対策基準第5の2(3)エにおけ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に閲覧できないよう保管すること。

エ 対策基準第5の2(3)エにおけるドキュメント及び記録簿について、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。

## 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

#### ア 警察情報システムのセキュリティ要件の策定

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

#### イ 警察情報システムの構築を業務委託する場合の対策

アは、警察情報システムの構築を業務委託する場合の対策に準用する。

#### ウ その他

対策基準第5の2(1)オ(ア)における警察情報システムについてプログラム開発を行うときの対策について、次のとおり定める。

(ア) プログラムの開発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こと。また、必要に応じて、運用中の警察情報システムと分離された環境とすること。

(イ) 情報セキュリティの観点に基づく試験において、次に掲げる事項を実施すること。

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情報システムに悪影響が及ばないように、運用中の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。

(ウ) ソースコードが不正に変更されることを防ぐために、次に掲げる事項を適切に実施すること。

- 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

(エ) 情報セキュリティ機能が適切に実装されていること及び情報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。

(オ) コーディングに関する規定を整備すること。

## (2) 警察情報システムの調達・構築

### ア 機器等の選定時の対策

対策基準第5の2(2)ア(1)における機器等の選定時の対策について、次のとおり定める。

(ア) 調達を行う製品について、意図しない変更が加えられた機器等が組み込まれることのないよう、必要に応じて、別紙2に掲げる内容を参考として、仕様書、契約書等の内容を検討すること。

(イ) 調達する機器等において、情報セキュリティ機能の適切な実装を確認するための設計書の検査、開発環境の管理体制の検査、脆弱性試験等、第三者による情報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/IEC 15408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。

### イ 情報システムの構築時の対策

対策基準第5の2(2)イにおける警察情報システムの構築時の対策について、システムセキュリティ責任者は、システム管理担当者及びネットワーク管理担当者に対して、セキュリティ機能の利用方法等に関わる教養を実施すること。

## (3) 警察情報システムの運用・保守

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
- (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）

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 対策基準第5の2(3)エ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1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1 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	電子計算機名又はネットワーク機器名 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により当該指名が除された日から5年
管理者権限が設定できる各ソフトウェア	ソフトウェア 指名を受けた者の所属、官職及び氏名	

の管理者権限保有者 名簿	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、IPアドレス及びMACアド レス	

	設定の内容（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証跡等の確認結果	
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	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	紙媒体又は電磁的記録により該当す

電気通信回線系図を含む。)	レス 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	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

オ システム管理担当者は、警察情報システムに係るドキュメントを適正に管理すること。

カ 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。

キ ネットワーク管理担当者は、担当するネットワーク機器について、データ伝送に関する監視及び制御を行うこと。

#### (4) 警察情報システムの更改・廃棄

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。

## 第5 警察情報システムの情報セキュリティ要件

### 1 警察情報システムの情報セキュリティ機能

#### (1) 主体認証機能

## ア 主体認証機能の導入

対策基準第6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、可能な限り主体認証情報として生体情報を用いること。知識による主体認証情報を用いるときは、必要に応じて主体認証情報格納装置と組み合わせるなどして、主体認証の機能を強化すること。
- (イ) システムセキュリティ責任者は、ネットワーク端末については、必要に応じて直ちに特定の利用者によるログインを禁止できる機能を設けること。
- (ウ) システムセキュリティ責任者は、モバイル端末の主体認証においては、次に掲げる認証方式のうち少なくとも2つ以上を併用すること。また、主体認証情報格納装置をモバイル端末から抜き取った場合には、操作を禁止する機能を設けること。
  - a 知識による認証
  - b 主体認証情報格納装置を用いた認証
  - c 生体情報による認証
- (エ) 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。
- (オ) システムセキュリティ責任者は、パスワードは、可能な限り英数字・記号を含む8文字以上の文字列とし、これを満たさないパスワードを設定できないよう技術的な対策を講ずること。
- (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、当該機能及び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のほか、次に掲げる事項を例とする機能を設けること。
  - a 職員がパスワードを定期的に変更しているか否かを確認する機能
  - b 以前に設定したパスワードの再設定を防止する機能

(ク) システムセキュリティ責任者は、パスワードを送信又は保存する場合には、暗号化、アクセス制限等の措置を施し、パスワードが第三者に知られることのないように対策を講ずること。

(ケ) システムセキュリティ責任者は、一定回数以上、パスワードによる主体認証に失敗した際に認証を一定時間停止する機能を設けるなど、総当たり攻撃への対策を講ずること。

#### イ 識別コード及び主体認証情報の管理

対策基準第6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。

(コ) 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に対するパスワードは、容易に推測できないものに設定すること。

## (2) アクセス制御機能

対策基準第6の1(2)におけるアクセス制御機能について、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要件を定め、必要に応じて、次に掲げる事項を例とする機能を利用者ごとに設けること。

ア 利用時間又は利用時間帯によるアクセス制限

イ 同一主体による複数アクセスの制限

ウ IPアドレスによる端末のアクセス制限

エ 分割したネットワークセグメントに基づくアクセス制限

オ 暗号化されたファイルに対するアクセス制御機能を有するサーバによる利用者の主体認証に基づくアクセス制限

カ 主体の操作に対する常時アクセス判断・許可アーキテクチャ（ゼロトラストアーキテクチャ、ゼロトラストセキュリティ等）での制御

### (3) 権限の管理

対策基準第6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 対策基準第6の1(3)イにおける措置については、次に掲げる事項を例とする。

(ア) 職務上必要な場合に限定する。

(イ) 必要最小限の権限のみ付与する。

(ウ) 管理者権限を行使できる端末をシステム管理担当者等の専用の端末とする。

ウ 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

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) 証跡の取得・管理

対策基準第6の1(4)における証跡の取得・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。

(イ) システムセキュリティ責任者は、ネットワーク機器の時刻設定を正確な

ものとする。

- (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、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、証跡に時刻情報も記録されるよう設定すること。

イ 証跡（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、証跡を保管すること、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、取得した証跡については、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、証跡の保全方法を定め、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証跡として取得し、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、ネットワーク機器等については、その特性に応じて、証跡を取得する目的を設定した上で、表2に掲げる項目の中から必要と認めたものについて、証跡の保存期間、取扱方法、証跡が取得できなくなった場合の対処方法等を定め、証跡を適切に保管できる仕様とすること。

表2 証跡（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、IP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、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証跡を取得し、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。
- (カ) 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証跡

(7) 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証跡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証跡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全て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) ウイルス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) 次に掲げる事項を全て満たしていること。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。

- ・ 入力に係る証跡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

(4) 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証跡を取得し、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証跡を取得し、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証跡を取得し、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)に掲げる証跡については媒体利用管理者が、(エ)に掲げる証跡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)イ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)に示す証跡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度に職員名、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

- (7) 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、証跡が取得できなくなった場合の対処方法を定めること。
- (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、取得した証跡を効率的かつ確実に点検及び分析し、その結果を報告するために、証跡情報をソフトウェア等により集計し、時系列で表示し、報告書を生成するなどの作業を自動化するなど、当該作業を支援する機能を導入すること。
- (ウ) 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証跡等により、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6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) 暗号化又は電子署名を行う警察情報システムにおいては、次に掲げる事項を例とした措置を講ずること。

a 複数の暗号アルゴリズム及びそれに基づいた安全なプロトコルを選択することが可能な構成とする。

b 選択した暗号アルゴリズムがソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された管理対象情報の復号又は電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護されることを確実にするため、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択する。

c 暗号化された管理対象情報の復号又は電子署名の付与に用いる鍵については、耐タンパ性を有する暗号モジュールへ格納する。

d 機密性3（高）情報を取り扱う警察情報システムを新規に構築する場合は、安全なプロトコルを選択し、長期的な秘匿性を保証する観点を考慮する。

(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、次の事項を満たすこと。

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) 電子署名の付与又は検証を行う機能については、対策基準第6の1(5)ア(キ)のほか、次に掲げる事項を満たすこと。

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 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

## 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

対策基準第6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 システムセキュリティ責任者は、所管する警察情報システムについて、情報セキュリティに係る脆弱性情報（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は、管理対象となる電子計算機に関連する脆弱性情報の入手に努めること。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。

オ ネットワーク管理担当者は、管理対象となるネットワーク機器に関連する脆弱性情報の入手に努めること。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。

カ 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。

(ア) 対策の必要性

(イ) 対策方法

(ウ) 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

(エ) 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

(オ) 対策の実施予定

(カ) 対策試験の必要性

(キ) 対策試験の方法

(ク) 対策試験の実施予定

キ システムセキュリティ責任者は、脆弱性対策を講じる場合には、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必要事項があれば適宜記録すること。

(ア) 実施日

(イ) 実施内容

(ウ) 実施者

ク 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。

(2) 不正プログラム対策

対策基準第6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、ウイルス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、ウイルス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、ウイルス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、次に掲げる電子計算機については、アからウ及び(4)並びに対策基準第6の2(2)ア及びイ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メモリ型のウイルス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

(3) サービス不能攻撃対策

対策基準第6の2(3)イに基づき、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、サーバ等、端末及びネットワーク機器に設けられている機能を有効にするだけではサービス不能攻撃の影響を排除又は低減できない場合には、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) サービス不能攻撃の影響に係る通信の遮断等の対策

(ウ) サーバ等、端末、ネットワーク機器又は電気通信回線の冗長化

(エ) コンテンツデリバリーネットワーク（CDN）サービスの利用

ウ 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。

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6の2(4)における標的型攻撃対策について、システムセキュリティ責任者は、外部記録媒体を利用した組織内部への侵入を低減するため、次に掲げる事項を例とする対策を講ずること。

ア 自動再生（オートラン）機能を無効化する。

イ 外部記録媒体内にあるプログラムを一律に実行拒否する設定とする。

ウ 使用を想定しないUSBポートを無効化する。

#### (5) 外部記録媒体の利用に係る対策

対策基準第6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な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)にあつては1(4)ウ(イ)から(オ)までに定める証跡を取得する機能を設けること。

- (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) 支給された携帯電話機（以下「支給携帯電話機」という。）、タブレット端末等であつて、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 アプリケーション・コンテンツの作成・提供

対策基準第6の3(2)イ及びウ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。

(1) 不正なウェブサイトへの誘導防止

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。

ア クローラからのアクセスを排除しない。

イ 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。

ウ 適切なタイトルを設定する。

エ 不適切な誘導を行わない。

(2) 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。

(ア) 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。

(イ) 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構成要素

### 1 端末・サーバ等

#### (1) 端末

ア 端末の導入時の対策

対策基準第7の1(1)アにおける端末の導入時の対策について、次のとおり定める。

- (7) 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。
- (イ) 物理的に持ち出しが困難であるもの及び鍵のかかる保管庫やクラス3に保管しているものを除き、全ての端末にセキュリティワイヤを取り付けること。
- (ウ) 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、次に掲げる事項を全て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。
- (エ) 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 端末の運用時の対策

対策基準第7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 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

対策基準第7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、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) 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) 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 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、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、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。
- d 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。

- e モバイル端末に別表に示す対策を講ずること。
- f 要機密情報を取り扱わないモバイル端末については、a から c 及び第 5 の 1 (1)ア(ウ)の規定を適用しない。
- g 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 5 の 1 (1)ア(ウ)の規定を適用しないことができる。

(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を設ける。
  - (b) 支給携帯電話機にファイルを暗号化する機能を設ける。
- 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。
- f 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。
- g 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。

- h 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、f及び対策基準第6の2(2)アに掲げる規定を適用しない。

エ 個人所有の機器の導入及び利用時の対策

対策基準第7の1(1)オにおける個人所有の機器の導入及び利用時の対策について、次のとおり定める。

(ア) 個人所有の携帯電話機に係る特例

第7の1(2)キ(イ)aに係る許可を受けた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しておくとともに、当該機種において動作するセキュリティ対策ソフトウェア又はセキュリティ対策サービスが存在しない場合を除き、導入すること。

(イ) 個人所有の機器に係る特例

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。

- a ウ(ア)c(a)から(c)までに掲げる機能（警察が整備したものに限る。）を用いて、個人所有の端末をテレワーク及びモバイル勤務で使うことができる。
- b 個人所有の端末を利用する場合は、次に掲げる措置を例とした対策を実施すること。
- (a) パスワード等による端末ロックの常時設定
  - (b) 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
  - (c) ウイルス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
  - (d) 警察が提供する業務専用アプリケーションの利用
  - (e) 次に掲げる事項を例とする禁止事項の遵守
    - ・ OS、警察が提供する業務専用アプリケーション等の改造
    - ・ 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
    - ・ 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

- ・ 許可されない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。）

## (2) サーバ等

### ア サーバ等の導入時の対策

対策基準第7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つては、クラス2に指定された区域に設置することができる。
- (イ) (1)アの(イ)、(ウ)及び(エ)は、サーバ等の導入時の対策に準用する。
- (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、機密性3（高）情報を取り扱わないものについては、対策基準第2の2(2)ウ(ウ)の規定による協議の上、クラス2に指定された区域に設置することができる。ただし、次に掲げる事項を全て満たすこと。
  - a 接続される端末及びサーバ等が同じ区域に設置されていること。
  - b サーバ等を施錠可能なラック等で管理すること。
  - c 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。
  - d 第5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。
  - e 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7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。

イ サーバ等の運用時の対策

対策基準第7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7の1(2)イ(ア)において準用する対策基準第7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ること。
  - a 障害発生時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 証跡の保存の方法
  - 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7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、庁内通信回線とファクシミリ等に使用する公衆通信回線が、複合機の内部において接続されないようにすること。
- (オ) 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。
- (カ) 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。
- (キ) 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。
- (ク) 対策基準第7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7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) 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。

- (イ) 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。
- (ウ) 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。
- (エ) 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。
- (オ) 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。
- (カ) 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。
- (キ) 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。
- (ク) 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。
- (ケ) 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

対策基準第7の2(1)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電子メールの導入時の対策について、次のとおり定める。

ア 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。

イ 管理するドメインについてSPFレコードを登録するなど、電子メールのなりすましの防止対策を講ずること。

### (2) ウェブ

## ア ウェブサーバの導入・運用時の対策

対策基準第7の2(2)ア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、ウェブサービスを提供するために設置されるウェブサーバの管理を行うに当たっては、次に掲げる事項を遵守すること。
  - a 必要に応じて多重化すること。
  - b ウェブサーバが利用者からの文字列等の入力を受ける場合には、当該文字列等に対して特殊文字の無害化を実施するとともに、当該通信を暗号化すること。
  - c 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。
  - d 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。
- (イ) 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。

## イ ウェブアプリケーションの開発時・運用時の対策

対策基準第7の2(2)イにおけるウェブアプリケーションの開発時・運用時の対策について、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) S Q Lインジェクション脆弱性
- (イ) O S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) メールヘッド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
  - (カ) 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
- (3) ドメインネームシステム (DNS)

対策基準第7の2(3)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ドメインネームシステム(DNS)の導入時及び運用時の対策について、次のとおり定める。

ア DNSの導入時の対策

システムセキュリティ責任者は、DNSサーバ(外部回線に接続されたものに限る。)については、次に掲げる事項を遵守すること。

- (ア) 必要に応じて多重化すること。
- (イ) DNSサーバについて、サービス不能攻撃、DNSキャッシュポイズニング攻撃等を防止するための措置を講ずること。
- (ウ) 外部に公開しないサーバ等の名前解決を行うDNSサーバにおいて、当該DNSサーバで管理する管理対象情報の漏えいを防止するため、次に掲げる事項を例とする措置を講ずること。
  - a 外部向けのDNS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

システムセキュリティ責任者は、キャッシュサーバにおいて、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。

(4) データベース

対策基準第7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

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証跡を記録し、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証跡を記録し、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7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、次に掲げる事項を全て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、拠点間において要機密情報を送受信する電気通信回線にあつては、次に掲げる事項を全て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つて、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) 利用する電気通信回線の終端間で別表の要件を満たす暗号により暗号化されていること。

(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、次に掲げる事項を例とする対策を講ずること。

(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、当該装置の筐体の開閉及び当該装置の取り外し等、情報セキュリティ侵害のおそれがある事案を検知した場合に、暗号に係る設定を消去するなどの仕組みを構築するときは、この限りでない。

なお、一時的に使用する電気通信回線を暗号化する装置であつて、職員

が常時当該装置の状況を視認できるものについては、区域にかかわらず設置することができる。

- (イ) 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、その証跡を残す機能を有し、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、ネットワーク機器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7の3(1)ア(ケ)における遠隔地からネットワーク機器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、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つては、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) 電気通信回線の運用時の対策

対策基準第7の3(1)イ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ネットワーク機器については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管すること。

イ 対策基準第7の3(1)イ(イ)において準用する対策基準第7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ネットワーク機器を把握した場合には、システムセキュリティ責任者に報告し、指示を受けて適切に対処すること。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。

(3) 無線LAN環境導入時の対策

対策基準第7の3(1)エにおける無線LAN技術を利用して電気通信回線を構築する場合は、要機密情報を送受信する無線LAN回線は、次に掲げる事項を全て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。

なお、ア(エ)及び(オ)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、ア(カ)及び(キ)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 庁舎内で利用する場合

- (ア) 無線LAN装置と端末とが同一庁舎内にあること。
- (イ) 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れいさせないこと。また、不要時には無線LAN装置の出力を停止すること。
- (ウ) 論理に警察以外の機関と接続していない閉域網であること。
- (エ) 通信の暗号化を適切に行うこと。
- (オ) 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。
- (カ) 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。

イ 庁舎外で利用する場合

- (ア) 他のシステムと論理的に接続していないこと。
- (イ) 一時的に利用する回線であること。
- (ウ) (ア)及び(イ)のほか、次に掲げる事項を例としたア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を使用の度に変更する。
- 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装置と機器との接続を行う際に、想定外の機器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運用要領等により禁止する。

## 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開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の的に抑止するため、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 機器の持ち出し

対策基準第8の1(2)ア(キ)に基づき、警察の庁舎外への機器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とともに、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・休日にあつ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 モバイル端末の持ち出しが終了したときは、持出簿に持出終了日を記載し、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を持ち出さないこと。

(a) 機器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つて、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、持出先が警察の庁舎である場合は、

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する。

- c モバイル端末及び支給携帯電話機以外の機器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 持ち出しが終了したときは、持出簿に持出終了日を記載し、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 対策基準第8の1(2)ア(ウ)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が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、次に掲げる事項を全て満たすこと。

- (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6の3(1)イの規定を満たす回線であること。
- (ウ) 第6の1(1)ウ(ア) c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。

### (7) 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つては、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た電子メール機能を使用する場合は、情報の暗号化、符丁（略語、符号等）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（支給区分）、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（警察署にあっては課）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、巡視等に合わせて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。

(7) 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により足りる。

なお、(ア) e に掲げる外部記録媒体については、次に掲げる事項を全て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（警察署にあつては課）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。
- ・ 交番等における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つて、警部相当職以上の者は、交番の巡視等に合わせて当該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 持出簿の確認及び保管

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証跡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、要機密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

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

##### (ア) 個人所有機器の職務上の使用禁止

- a 職員は、(イ)に定める場合を除き、個人所有の機器に管理対象情報を保存しないこと。
- b 職員は、(イ)、(ウ)又は3(3)に定める場合を除き、個人所有の機器を警察情報システムに接続しないこと。
- c 職員は、(イ)、(ウ)又は3(3)に定める場合を除き、個人所有の機器において、管理対象情報の処理を行わないこと。

##### (イ) 個人所有の携帯電話機に係る特例

- 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携帯電話機について、第6の1(1)エ(7)に定める対策を講ずること。

d 職員は、職務上緊急に管理対象情報を伝達する必要があつて、警察が整備した機器等による代替手段が他にないとき又はテレワーク及びモバイル勤務時に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及び写真撮影機能を使用することができる。

なお、電子メール機能の使用に当たっては、運用管理者が認めた場合を除き、移動通信事業者が提供する電子メール機能を使用するものとし、当該電子メール機能で取り扱う管理対象情報は機密性2(中)情報までとする。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。

e 職員は、dの規定に従つ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つて警部相当職以上の者に報告(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。

f 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外部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(ウ)a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。

なお、当該別に定めるところによる個人所有携帯電話機の利用は、dに定める代替手段には該当しない。

g 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つては、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、b及びcの規程を適用しない。

(ウ) 個人所有の機器に係る特例

a テレワーク及びモバイル勤務に使用する個人所有の端末に必要な対策  
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、bの場合はその限りでない。

(a) 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使用する際は、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。

- ・ 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
- ・ 利用する通信回線サービス
- ・ 利用する期間

(b) 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

(c) 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)aに規定する情報流出事案と同様の手続を執ること。

(d) 職員は、(a)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。

(e) 職員は、(a)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。

(f) 職員は、テレワーク及びモバイル勤務で使用する個人所有の端末について、第6の1(1)エ(イ)に定める対策を講ずること。

(g) 職員は、個人所有の端末を利用する場合は、次に掲げる措置を例とした対策を講ずること。

- ・ 盗み見に対する対策（のぞき見防止フィルタの利用等）
- ・ 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）
- ・ 利用する場所や時間の限定
- ・ 端末の盗難・紛失が発生した際の緊急対応手順の把握

b 個人所有機器を使用したインターネット上の情報の閲覧等

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。

c 個人所有のイヤホン及びヘッドセットに係る特例

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。

キ 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、自己に付与されたユーザ I D 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) ユーザ I D を利用する必要がなくなった場合には、定められた手順に従い、ユーザ I D 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) 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。

(イ) 異なるユーザ I D に対して、共通の主体認証情報を用いない。

(ウ) 異なる警察情報システムにおいて、ユーザ I D 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。）。

(エ) ユーザ I D 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ユーザ I D 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、I C 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、本人が意図せずに使われることのないように管理すること。

エ 職員は、主体認証情報格納装置を紛失しないよう管理し、権限のない者に付与又は貸与しないこと。また、紛失した場合には、定められた手順に基づき、直ちにその旨を報告すること。

オ 職員は、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こと。

#### (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、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) 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。
- (エ) 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短縮サービスは、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や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通信回線との接続禁止
- (ク) 端末画面の接写対策並びに、情報の持出及び印字の禁止（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)イ (ア)及び対策基準第3の1 (5)イ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、以下の事項を例とする。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として、「持ち出した機器は全てそろっているか」
- b 脆弱性対策として、「OSやアプリケーション等のソフトウェアが最新の状態に保たれているか」、「サポート切れのソフトウェアを利用していないか」、「自宅のネットワークルータをはじめとした、ネットワーク上の機器は最新のファームウェアに更新されているか」
- c 情報漏えい対策として、「のぞき見防止フィルタが装着されているか」、「背後にのぞき見可能なスペースがないか」、「スクリーンロックは設定されているか」
- d 不正プログラム対策として、「ウイルス対策ソフトウェアのパターンファイルが最新の状態になっているか」、「作業前にウイルスチェックをしたか」、「ウイルス対策ソフトウェアがリアルタイムスキャンを行うように設定されているか」
- e 情報セキュリティインシデント対策として、「情報セキュリティインシデント発生時の連絡先を把握しているか」

(イ) 実施後に行うチェックの項目

- a 不正プログラム対策として、「ウイルスチェックを行い不正プログラ

ムに感染していないことを確認したか」

b 管理対象情報の管理として、「持ち出した機器は全てそろっているか」

c 情報漏えい対策として、「端末に保存した要機密情報が暗号化されているか」

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。

キ テレワーク及びモバイル勤務に係る機器の技術的な要件については、対策基準第8の3(1)を参照すること。

(3) 警察情報システムへの接続に利用する回線

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6の3及び対策基準第7の3のうち、第6の3(1)キ及び(3)並びに対策基準第7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。

(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・別表略>