兵庫県警察情報システムの情報セキュリティ要件について（例規甲）

〔平成28年９月20日
兵警情例規甲第32号本部長〕

［沿革］　平成30年２月兵警情例規甲第９号、平成31年２月第８号改正

兵庫県警察情報システムの情報セキュリティ要件についてを下記のように定め、平成28年10月１日から実施する。

記

第１　総則

１　目的

この通達は、兵庫県警察における情報セキュリティに関する訓令（平成23年兵庫県警察本部訓令第１号。以下「訓令」という。）第５条第２項及び第８条の規定に基づき、兵庫県警察情報システムの情報セキュリティ要件に関し必要な事項を定めるものとする。

２　定義規定等の適用

訓令、兵庫県警察における情報セキュリティに係る管理体制について（平成28年兵警情例規甲第30号）及び兵庫県警察情報システムの利用及び管理対象情報の取扱いに係る警察職員の遵守事項について（平成28年兵警情例規甲第31号。以下「遵守事項通達」という。）に定めるところによる定義規定及び略称規定は、この通達において適用する。

３　定義

この通達において、次の各号に掲げる用語の意義は、それぞれの当該各号に定めるところによる。

(1)　モバイル端末　一の警察の庁舎内から移動して運用するものとして整備された電子計算機（公費整備携帯電話機を除く。）をいう。

(2)　データベース　サーバのうち、特にデータの管理に特化し、専用の装置とデータベースファイルを合わせたもので、要保護情報を保管するものをいう。

(3)　複合機　プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器をいう。

(4)　特定用途機器　テレビ会議システム、ＩＰ電話システム、ネットワークカメラシステム、監視カメラ等の特定の用途に使用される情報システム特有の構成要素となる機器であって、電気通信回線に接続され、又は電磁的記録媒体が内蔵されているものをいう。

(5)　クラウドサービス　事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに係る十分な条件設定の余地があるものをいう。

第２　技術的要件

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

１　物理的対策

(1)　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又はクラス３に保管しているものを除き、全ての電子計算機にセキュリティワイヤーを取り付けなければならない。
(2)　設置環境を踏まえ、必要に応じて画面に視野角を制限し、のぞき見を防止するフィルタを取り付けなければならない。
(3)　サーバ等については、原則としてクラス３に分類された区域に設置しなければならない。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に分類された区域に設置することができる。
(4)　モバイル端末及び公費整備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しなければならない。
(5)　物理的対策については、前記(1)から(4)までに定めるもののほか、総務部長が別に定める要件を満たさなければならない。

２　主体認証及びアクセス制御

(1)　ログイン時に主体認証を行う機能を設けなければならない。
(2)　管理者と一般利用者の権限を分割し、管理者権限を必要最小限の者のみに付与しなければならない。
(3)　管理者権限を持つ識別コードを付与した者には、管理者としての職務遂行時に限定して、当該識別コードを利用させなければならない。
(4)　識別コードについては、職員ごとに発行することとし、複数の職員が共有する識別コードを発行してはならない。ただし、業務上支障がある場合はこの限りでない。
(5)　主体認証及びアクセス制御の機能については、前記(1)から(4)までに定めるもののほか、総務部長が別に定める要件を満たさなければならない。

３　暗号及び電子署名

(1)　内蔵された電磁的記録媒体に記録される管理対象情報を暗号化する機能を設けなければならない。ただし、次に掲げるものについては、この限りでない。
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電子計算機
イ　技術上又は運用上暗号化が困難であるサーバ等
(2)　復号又は電子署名の付与に用いる鍵をインターネットに接続された電子計算機に保存してはならない。
(3)　暗号及び電子署名については、前記(1)及び(2)に定めるもののほか、総務部長が別に定める要件を満たさなければならない。

４　ネットワーク

(1)　ネットワーク機器の時刻設定を正確なものとする機能を設けなければならない。
(2)　ネットワークの監視を行う機能を設けなければならない。また、監視により得られた結果は、消去又は改ざんが行われないように管理する機能を設けなければならない。
(3)　ネットワークについては、前記(1)及び(2)に定めるもののほか、総務部長が別に定める要件を満たさなければならない。

５　サーバ等

(1)　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、アクセス権を必要最小限としなければならない。
(2)　サーバ等の時刻設定を正確なものとする機能を設けなければならない。
(3)　サーバ等については、前記(1)及び(2)に定めるもののほか、総務部長が別に

定める要件を満たさなければならない。

6　データベース

(1)　データベースに対する職員の不正を防止するため、管理者権限を持つ識別コードの適正な権限管理を行う機能を設けなければならない。

(2)　データベースに格納されているデータにアクセスした利用者を特定できるよう、措置をとらなければならない。

(3)　データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講じなければならない。

(4)　データベース及びデータベースへアクセスする機器等のぜい弱性を悪用した、データの不正な操作を防止するための対策を講じなければならない。

(5)　データの窃取、電磁的記録媒体の盗難等による管理対象情報の流出を防止する必要がある場合は、適切に暗号化しなければならない。

(6)　データベースについては、前記(1)から(5)までに定めるもののほか、総務部長が別に定める要件を満たさなければならない。

7　不正プログラム対策

警察情報システムを構成する機器には、総務部長が別に定めるところにより、不正プログラムへの対策を講じなければならない。

8　電子メール及びウェブ

(1)　インターネットに接続された情報システムについては、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かなければならない。

(2)　インターネットに接続された情報システムのうち職員以外の者に電子メールを送信することを目的とした情報システム及びウェブサイト（外部委託する場合を含む。）については、遵守事項通達第７の規定により約款による外部サービスを利用する場合、公費整備携帯電話機を使用する場合又は特別な事情がある場合を除き、「lg.jp」等行政機関であることが保証されるドメイン名を使用しなければならない。

(3)　インターネットに接続された情報システムの電子メール及びウェブについては、前記(1)及び(2)に定めるもののほか、総務部長が別に定める要件を満たさなければならない。

9　外部記録媒体の利用

総務部長が別に定めるところにより、外部記録媒体の利用を制限する機能を設けなければならない。

10　証跡の取得

(1)　総務部長が別に定める項目について、証跡を取得し、保管する機能を設けなければならない。

(2)　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させなければならない。

11　モバイル端末

モバイル端末については、前記１から10までに定めるもののほか、総務部長が別に定める要件を満たさなければならない。

12　公費整備携帯電話機

公費整備携帯電話機については、前記２、３、７、８及び９に定めるもののほか、総務部長が別に定める要件を満たさなければならない。ただし、音声通話機能のみを使用する公費整備携帯電話機については、前記２、３、７、８及び９に

定める規定は適用しない。

13　複合機

(1)　複合機が備える機能、設置環境及び取り扱う管理対象情報の分類に応じ、適切な情報セキュリティ要件を満たさなければならない。

(2)　複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティ対策をとらなければならない。

(3)　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わなければならない。

(4)　複合機については、前記(1)から(3)までに定めるもののほか、総務部長が別に定める要件を満たさなければならない。

14　特定用途機器

(1)　取り扱う管理対象情報、利用方法、電気通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じた対策を講じなければならない。

(2)　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わなければならない。

(3)　特定用途機器については、前記(1)及び(2)に定めるもののほか、総務部長が別に定める要件を満たさなければならない。

第３　設計、調達、運用及び廃棄

１　共通事項

(1)　システムセキュリティ責任者は、警察情報システムの設計に当たっては、前記第２に定める要件のほか、用途や設置環境に応じた情報セキュリティ対策をとらなければならない。

(2)　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ＳＴ（Security Target：セキュリティ設計仕様書）評価及びＳＴ確認を受けなければならない。

(3)　システムセキュリティ責任者は、警察情報システムの設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開されたぜい弱性についての対策を講じなければならない。

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

(5)　システムセキュリティ責任者は、警察情報システムの移行又は廃棄を行う場合には、当該警察情報システムに保存されている管理対象情報について、当該情報の分類及び取扱制限を考慮した上で、次に掲げる措置を適切にとらなければならない。

ア　警察情報システム移行時の管理対象情報の移行作業における情報セキュリティ対策

イ　警察情報システム廃棄時における物理的な破壊、データ消去ソフトウェアの利用等による不要な管理対象情報を復元させないための措置

(6)　システムセキュリティ責任者は、必要に応じて、所管する警察情報システムを構成する機器のソフトウェアの名称、バージョン等に関する情報を自動で収集し、管理する機能を導入しなければならない。

２　機器の調達

システムセキュリティ責任者は、警察情報システムを構成する機器の調達に当たっては、次に掲げる事項を遵守しなければならない。

(1)　機器の選定に当たっては、当該機器及び当該機器の製造者に係る情報の入手に努め、入手した情報等を基に、情報セキュリティの確保に必要な機能及び信頼性を有するものを選定すること。

(2)　ＩＴ製品の調達におけるセキュリティ要件リスト（平成30年２月28日に経済産業省により策定された、デジタル複合機等の製品分野ごとに考慮すべきセキュリティ上の脅威とそれに対抗するためのセキュリティ要件をまとめたものをいう。）を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するための情報セキュリティ設計を行うこと。

(3)　必要に応じて、機器の納入時に検査等を実施すること。

(4)　機器の調達については、前記(1)から(3)までに定めるもののほか、総務部長が別に定める事項を遵守しなければならない。

３　プログラム開発

システムセキュリティ責任者は、警察情報システムについてプログラム開発を行うときは、総務部長が別に定める事項を遵守しなければならない。

４　外部委託

システムセキュリティ責任者は、警察情報システムの設計、運用又は廃棄の外部委託に当たっては、次に定める事項を遵守しなければならない。

(1)　外部委託によって情報セキュリティが損なわれることのないよう、十分に検討の上、委託先には事業継続性を有すると認められる事業者を選定すること。

(2)　次に掲げる情報セキュリティ対策又はこれらと同等以上のセキュリティが認められる対策の実施を、委託先の選定条件とした上、仕様書等に盛り込むこと。

ア　委託先に提供する管理対象情報の委託先における目的外利用の禁止

イ　委託先における情報セキュリティ対策の実施内容及び管理体制

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

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

オ　情報セキュリティインシデントへの対処方法

カ　情報セキュリティ対策その他の契約の履行状況の確認方法

キ　情報セキュリティ対策の履行が不十分な場合の対処方法

ク　前記アからキまでに掲げるもののほか、実施することが必要と認められる情報セキュリティ対策

(3)　委託する業務において取り扱う管理対象情報の分類等を勘案し、必要に応じて次に掲げる事項を仕様書等に盛り込むこと。

ア　情報セキュリティ監査の受入れ

イ　サービスレベルの保証

(4)　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、前記(1)から(3)までの措置の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報をシステムセキュリティ責任者に提供し、システムセキュリティ責任者の承認を受けるよう、仕様書等に盛り込むこと。

(5)　警察情報システムの開発事業者から運用業者又は保守業者に引き継がれる項

目に、情報セキュリティ対策に必要な内容が含まれていることを確認すること。

(6)　あらかじめ当該委託に係る作業を監督する職員の任務を定めるとともに、前記(1)から(5)までに定める事項のほか、情報セキュリティの観点から委託の相手方に遵守させるべき事項を仕様書等に盛り込むこと。

(7)　クラウドサービスを利用するに当たっては、次に掲げる事項

ア　取り扱う管理対象情報は、機密性１（低）情報に限ること。

イ　取り扱う管理対象情報の取扱制限を踏まえ、当該クラウドサービスの利用の可否を判断すること。

ウ　取り扱う管理対象情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定すること。

エ　クラウドサービスの中断や終了時に円滑に職務を移行するための対策を検討し、委託先を選定する際の要件とすること。

オ　クラウドサービスの特性を考慮した上で、クラウドサービス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が適切に確保されるよう、情報の流通経路全般を見渡した形で情報セキュリティ設計を行うこと。

カ　クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し、利用の可否を判断すること。

(8)　前記(1)から(7)までに定めるもののほか、総務部長が別に定める事項

第４　ドキュメント及び記録簿

システムセキュリティ維持管理者は、総務部長が別に定めるところにより、情報システムの構成や情報の処理手順を変更するなどの維持管理作業に必要なドキュメント及び記録簿を整備しなければならない。

第５　情報セキュリティ要件を適用することが困難な場合の措置

システムセキュリティ責任者は、特定の警察情報システムについて、この通達に定めた情報セキュリティ要件を適用することが困難であると判断したときは、情報セキュリティ管理者（警察庁と接続している警察情報システムにあっては警察庁情報セキュリティ管理者）と協議の上、当該警察情報システムの情報セキュリティ要件について、別の定めを置くことができる。