

警 情 甲 達 第 7 号
平成30年4月23日
〔 改正 令和元年9月30日 〕
警 情 甲 達 第 30号

各部、課、隊、所、校、署長 殿

福 井 県 警 察 本 部 長

福井県警察情報システム等の情報セキュリティ要件の制定について

福井県警察情報システム等の情報セキュリティ要件については、福井県警察情報システム等の情報セキュリティ要件の制定について（平成26年警情甲達第17号。以下「旧通達」という。）により実施してきたところであるが、情報セキュリティをめぐる各種情勢の変化等を踏まえ、別添のとおり制定し、平成30年5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、平成30年4月30日をもって廃止する。

別添

福井県警察情報システム等の情報セキュリティ要件

第1 総則

1 目的

この通達は、福井県警察における警察情報セキュリティに関する訓令（平成19年福井県警察本部訓令第3号。以下「訓令」という。）第14条の規定に基づき、福井県警察情報システム等の情報セキュリティ要件を定めることを目的とする。

2 用語の定義

この通達における用語の意義は、訓令及び福井県警察における情報セキュリティに係る管理体制の制定について（平成30年警情甲達第4号）に定めるところによる。

第2 技術的要件

システムセキュリティ責任者は、整備する福井県警察情報システム等（以下「警察情報システム」という。）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、鍵のかかる保管庫に保存されているもの及びクラス3の区域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するのぞき見防止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に指定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に指定された区域に設置することができる。
- (4) モバイル端末及び支給又は貸与された携帯電話機（以下「支給携帯電話機」という。）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、（1）から（4）までに定めるもののほか、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、管理者権限は必要最小限の者のみが運用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された場合には、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しなければならない。
- (4) 業務上支障がある場合を除き、識別コードは警察職員ごとに発行することとし、複数の警察職員が共有する識別コードを発行してはならない。
- (5) 主体認証及びアクセス制御の機能については、（1）から（4）までに定めるもののほか、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 サーバ等であって、技術的又は運用上暗号化が困難であるもの
- (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、(1)及び(2)に定めるもののほか、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しなければならない。
- (2) ネットワークの監視を行わなければならない。また、監視により得られた結果は、消去や改ざんが行われないように管理しなければならない。
- (3) ネットワークについては、(1)及び(2)に定めるもののほか、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しなければならない。
- (3) サーバ等については、(1)及び(2)に定めるもののほか、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内部不正を防止するため、管理者権限を持つ識別コードの適正な権限管理を行わなければならない。
- (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、措置を執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脆弱性を悪用した、データの不正な操作を防止するための対策を講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漏えい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、(1)から(5)までに定めるもののほか、情報セキュリティ管理者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、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

次に定める要件は、インターネットに接続された情報システムについて適用される。

- (1) 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) 警察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、「福井県警察情報システム等及び管理対象情報の取扱要領の制定について」（平成30年警情甲達第6号）第7に規定する約款による外部サービスを利用する場合、支給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、行政機関であることが保証されるドメイン名（「g o . j p」、「l g . j p」等）を使用しなければならない。
- (3) 電子メール及びウェブについては、（1）及び（2）に定めるもののほか、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

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（外部記録媒体関係のものを除く。）の取得

- (1) 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) （1）に定める証跡は、必要に応じて分析し、適切な措置を執らなければならない。
- (3) 警察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しなければならない。
- (4) 得られた証跡は、消去や改ざんが行われないように管理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、1から10までに定めるもののほか、別に定める要件を満たさなければならない。

12 支給携帯電話機

支給携帯電話機については、2、3、7、8及び9に定めるもののほか、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支給携帯電話機については、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講じなければならない。
- (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、（1）から（3）までに定めるもののほか、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、（1）及び（2）に定めるもののほか、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、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講じなければならない。
- (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S T（セキュリティ設計仕様書）評価・S T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執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の不要な管理対象情報の抹消

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なければならない。
- (2) 機器の選定に当たっては、（1）において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しなければならない。
- (3) 「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日経産省）を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するための情報セキュリティ要件を策定しなければならない。
- (4) 必要に応じて、機器の納入時に検査等を実施すること。
- (5) 機器の調達については、（1）から（4）までに定めるもののほか、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、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・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しなければならない。
- (2) 次に掲げる事項を例として、情報セキュリティ対策の実施を委託先の選定条件とし、仕様書等に盛り込まなければならない。
 - ア 委託先に提供する管理対象情報の委託先における目的外利用の禁止
 - イ 委託先における情報セキュリティ対策の実施内容及び管理体制
 - ウ 委託事業の実施に当たり、委託先企業又はその従業員、再委託先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
- (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まなければならない。
 - ア 情報セキュリティ監査の受入れ
 - イ サービスレベルの保証
- (4) 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しなければならない。
- (5) 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、(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、仕様書等に盛り込まなければならない。
- (6) あらかじめ当該委託に係る作業を監督する警察職員の任務を定めるとともに、当該委託に係る業務の実施の場所及び方法、(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明記した仕様書等に盛り込まなければならない。
- (7) クラウドサービスを利用するに当たっては、次に掲げる事項を遵守しなければならない。
 - ア 取り扱う管理対象情報の分類は、機密性1（低）情報に限ること。
 - イ 取扱制限を踏まえ、管理対象情報の取扱いを委ねること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った上で情報セキュリティ要件を定めること。

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) 外部委託に当たっては、(1) から (7) までに定めるもののほか、別に定める事項を遵守しなければならない。

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、情報セキュリティ管理者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、その内容を常に最新のものとしておかなければならない。

第5 その他

1 経過措置

この通達が施行された時点で整備済みの警察情報システムであって、この通達に定められた事項を満たしていないものに限り、当該事項について、適用を猶予することができる。この場合において、システムセキュリティ責任者は可能な限り早期に要件を満たすことができるよう努めるとともに、別に定める代替手段その他必要に応じて情報セキュリティを確保するための代替手段を講じなければならない。

2 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、別段の定めを置くことができる。