情第365号
平成26年３月26日

各所属長　殿

岐阜県警察本部長

岐阜県警察における警察情報システムの情報セキュリティ要件の制定について（通達）

岐阜県警察における情報セキュリティについては、「岐阜県警察情報セキュリティ対策基準」（平成22年12月24日付け情第1042号）及び「外部記録媒体等の情報セキュリティ対策の強化について」（平成22年12月24日付け情第1043号）により実施してきたところであるが、この度、岐阜県警察情報セキュリティポリシーの体系を見直すこととし、岐阜県警察情報セキュリティに関する訓令（平成16年岐阜県警察訓令第15号）第８条の規定に基づき、警察情報システムを整備するに当たり、情報セキュリティを維持するために必要な要件について、別添のとおり「岐阜県警察における警察情報システムの情報セキュリティ要件」を定め、平成26年４月１日より運用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。

別添

岐阜県警察における警察情報システムの情報セキュリティ要件

第１　総則

１　目的

この要件は、岐阜県警察情報セキュリティに関する訓令（平成16年岐阜県警察訓令第15号）第８条の規定に基づき、警察情報システムの情報セキュリティ要件を定めるものである。

２　用語の定義

この要件における用語の意義は、「岐阜県警察情報セキュリティ管理要綱」（平成26年３月26日付け情第362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やクラス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）の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、情報セキュリティ管理者が別で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。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。

(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、別で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、技術的に又は運用上暗号化が困難であるもの

ウ　支給携帯電話機であって、技術的に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、別で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、別で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、別で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、データベースへアクセスする機器等の脆弱(ぜい)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、別で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、別で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)　職員以外の者に電子メールを送信することを目的とした情報システム及びウェブサイト（業務委託する場合を含む。）については、「岐阜県警察における警察情報システムの情報取扱要領」（平成26年３月26日付け情第363号）第７に規定す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（「go.jp」、「lg.jp」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、別で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

電子計算機には、別で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)　電子計算機及びサーバ等には、別で定めるところにより、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)　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、別で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、情報セキュリティ管理者が別途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、別で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、別で定める要件を満たさなければならない。

15　テレワーク及びモバイル勤務の実施環境における対策

(1)　テレワーク及びモバイル勤務の実施により外部回線を経由して警察情報システムへリモートアクセスする形態となる警察情報システムを構築する場合は、通信経路及びリモートアクセス特有の攻撃に対する情報セキュリティを確保しなければならない。
(2)　リモートアクセスに対し多要素主体認証を行わなければならない。
(3)　リモートアクセスする端末を許可された端末に限定する措置を講じなければならない。
(4)　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しなければならない。
(5)　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は、(1)から(4)までに定めるもののほか、別で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、廃棄等

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、警察情報システムの整備に当たり、必要な事項を記載した台帳を作成し、情報セキュリティ管理者に報告しなければならない。
(3)　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・ＳＴ確認を受けなければならない。
(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脆弱性についての対策を講じなければならない。
(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。
(6)　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日経済産業省）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、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、別で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、別で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、廃棄等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)　次のアからキまでに掲げる事項を参考に、情報セキュリティ対策の実施を委託先の選定条件とし、仕様書等に盛り込まなければならない。

ア　委託先に提供する管理対象情報の委託先における目的外利用の禁止

イ　委託先における情報セキュリティ対策の実施内容及び管理体制

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

エ　委託先の資本関係、役員等の情報、委託事業の実施場所並びに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実施及び結果報告

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保守事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委託先に報告させるなどにより、適切に対策が実施されているかどうか確認するために必要な情報をシステムセキュリティ責任者に提供し、システムセキュリティ責任者の承認を受けるよう、仕様書等に盛り込まなければならない。

(6)　次に掲げる事項を参考にして、委託先の情報セキュリティ水準の評価を行わなければならない。

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

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

(8)　委託先によるアクセスを認める情報及び情報システムの範囲を適切に判断しなければならない。

(9)　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、(1)から(8)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まなければならない。

(10) 外部サービスを利用して警察情報システムを構築する場合は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、次に掲げる事項を遵守し、構築時に実施状況を確認・記録しなければならない。ただし、外部サービスにおいて要機密情報を取り扱わない場合はこの限りでない。

ア　不正なアクセスを防止するためのアクセス制御

イ　取り扱う情報の機密性保護のための暗号化

ウ　開発時における情報セキュリティ対策

エ　設計・設定時の誤りの防止

(11) 外部委託に当たっては、(1)から(10)までに定めるもののほか、別で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、別で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

システムセキュリティ責任者は、この要件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、この要件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。このとき、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、別途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、例外の措置を行うことができる。

附　則（平成26年３月26日付け情第365号）

この要件は、平成26年４月１日から運用する。

附　則（平成28年５月16日付け情第689号）

この要件は、平成28年５月16日から運用する。

附　則（平成30年５月23日付け情第664号）

この要件は、平成30年６月１日から運用する。

附　則（平成31年２月27日付け情第279号）

この要件は、平成31年４月１日から運用する。

附　則（令和４年７月１日付け情第564号）

この要件は、令和４年７月１日から運用する。