○　警察情報システムの情報セキュリティ要件について

（平成26年３月18日岩警務第62号、岩生安第53号、岩刑事第62号、岩交通第25号、岩警備第18号警察本部長）

[沿革]平成27年12月岩警務第75号、岩生安第107号、岩刑事第92号、岩交通第95号、岩警備第55号改正

各　　部　　長
首 席 監 察 官
各　所　属　長

岩手県警察における情報セキュリティについては、岩手県警察情報セキュリティ対策基準の制定について（平成23年５月24日付け岩警務第17号、岩生安第33号、岩刑事第28号、岩交通第30号、岩警備第14号）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、岩手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、この度、岩手県警察情報セキュリティに関する訓令（平成18年岩手県警察本部訓令第３号）第５条第２項及び第８条の規定に基づき、別添のとおり「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日から施行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。

別添

警察情報システムの情報セキュリティ要件

第１　総則

１　趣旨

この例規は、岩手県警察情報セキュリティに関する訓令（平成18年岩手県警察本部訓令第３号）第５条第２項及び第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とする。

２　用語の定義

この例規において、用語の意義は、岩手県警察情報セキュリティに関する訓令及び岩手県警察情報セキュリティに係る管理体制について（平成26年３月18日付け岩警務第60号、岩生安第51号、岩刑事第60号、岩交通第23号、岩警備第16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、次に定める要件を満たさなければならない。この場合において、次に定める要件は、特に断りのない限り、ネットワーク端末、インターネット端末、スタンドアロンパソコン、モバイル端末、複合機、特定用途機器及びサーバ等並びにこれらの機器により構成されるシステムに適用されるものとする。

１　物理的対策

(1)　電子計算機は、物理的に持出しが困難であるもの並びに鍵のかかる保管庫及び区域に保管しているものを除き、全てのもの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)　電子計算機は、その設置環境に鑑み、必要に応じて画面に視野角を制限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、機密性低の情報のみを取り扱うサーバ等にあっては、この限りでない。

(4)　物理的対策については、(1)から(3)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。

２　利用者認証

次に定める要件は、電子計算機について適用されるものとする。

(1)　ログイン時に認証する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)　業務上支障がある場合を除き、ＩＤは職員ごとに発行することとし、複数の職員が共有するＩＤを発行してはならない。

(4)　利用者認証の機能については、(1)から(3)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。

3　暗号

(1)　内蔵記憶装置に記録される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　要機密情報を内蔵記憶装置に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

(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)　暗号については、(1)及び(2)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。

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。この場合において、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、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。

5　サーバ等

(1)　サーバ等へのアクセスについて、利用者認証及び端末認証の機能を設け、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、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。

6　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、情報セキュリティ管理者が別に定めるところにより、コンピュータ・ウイルス等不正プログラムへの対策を講じなければならない。

7　電子メール及びウェブ

インターネットに接続されたシステムにおける電子メール及びウェブは、次に定める要件を満たさなければならない。

(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システムについては、特別な事情があるときを除き、行政機関であることが保証されるドメイン名（「pref.iwate.jp」、「lg.jp」等をいう。）を取得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、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。

8　外部記録媒体の利用

情報セキュリティ管理者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。

9　証跡（外部記録媒体に係るものを除く。）の取得

(1)　情報セキュリティ管理者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)　(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。

10　モバイル端末

モバイル端末については、１から９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。ただし、携帯電話機については、１から９までに定める要件は適用されない。

11　複合機

(1)　複合機が備える機能、設置環境及び取り扱う情報の分類に応じ、適切な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執らなければならない。

(3)　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、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。

12　特定用途機器

(1)　取り扱う情報、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)　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、(1)及び(2)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。

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、用途及び設置環境に応じた情報セキュリティ対策を執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機能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をいう。以下同じ。）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。

(4)　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に当たっては、情報の消去及び保存並びに警察情報システムの再利用について必要性を検討し、適切な措置を執らなければならない。情報を消去するに当たっては、物理的な破壊、データ消去ソフトウェアの利用等により、情報を復元できないよう措置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)　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)　必要に応じて、機器の納入時、検査等を実施すること。

(3)　機器の調達については、(1)及び(2)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、情報セキュリティ管理者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、運用及び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)　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、当該委託に係る業務の実施の場所及び方法、当該委託に係る業務に従事する者の範囲、委託先によるアクセスを認める範囲その他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を作成しなければならない。

(3)　外部委託に当たっては、(1)及び(2)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、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、この例規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、この例規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、情報セキュリティ管理者が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　例外

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、この例規に定められた事項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。