○石川県警察情報セキュリティ対策基準の全部改正について

〔平成23年３月25日情甲達第４号、務甲達第23号、生企甲達第35号、刑企甲達第31号、交企甲達第24号、公甲達第18号
警察本部長から部課署長あて〕

対号　平成20年４月25日付け情甲達第16号、務甲達第91号、県相甲達第３号、会甲達第128号、生企甲達第36号、捜一甲達第38号、交企甲達第20号、公甲達第19号「石川県警察情報セキュリティ対策基準の制定について（通達）」

石川県警察における警察情報システムの情報セキュリティについては、対号により実施してきたところであるが、このたび、警察庁において政府統一基準に準拠するため、警察情報セキュリティ対策基準の改正が行われたことに伴い、「石川県警察情報セキュリティ対策基準」を別添のとおり全部改正し、平成23年４月１日から実施することとしたので、事務処理上遺憾のないようにされたい。

なお、対号は平成23年４月１日をもって廃止する。

別添

石川県警察情報セキュリティ対策基準

第１　総則

１　目的

この対策基準は、石川県警察における情報セキュリティに関する訓令（平成17年石川県警察本部訓令第15号。以下「訓令」という。）第５条第２項の規定に基づき、警察情報システムの情報セキュリティの維持に関し必要な事項を定めるものとする。

２　用語の定義

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

(1) 警察情報セキュリティポリシー

訓令及び訓令に基づいて定められた情報セキュリティに関する事項をいう。

(2) 入出力資料

警察情報システムに入力された又は警察情報システムにより出力された情報を記録した文書、図画及び電磁的記録（作成中のものを含む。）をいう。

(3) ドキュメント

警察情報システムに関する次に掲げる文書、図画及び電磁的記録（作成中のものを含む。）をいう。

ア　システムドキュメント

(ｱ) システム仕様書

(ｲ) システム設計書（情報の処理手順並びに機器及びプログラムの構成の概要の記録をいう。）
(ｳ) プログラム仕様書（情報の処理手順の概要の記録をいう。）
(ｴ) プログラムリスト
(ｵ) 操作指示書（システムの維持管理に伴う機器の設定方法等を説明した記録をいう。）

イ　取扱説明書

システムを利用する者が業務を行う上で参照する機器の操作の方法を説明した記録をいう。

(4) 外部記録媒体

フロッピーディスク、フラッシュメモリ、ＤＶＤ規格媒体等、情報を記録する電磁的記録媒体をいう。

(5)　デジタル機器

デジタルカメラ、デジタルビデオなど、画像、動画及び音声等の情報をデジタル方式で本体の内蔵メモリ又は外部記録媒体に記録できる機器をいう。

(6) 画像等情報記録媒体

デジタル機器で記録専用に使用する外部記録媒体をいう。

(7) 情報

入出力資料、ドキュメント、デジタル機器、外部記録媒体又は画像等情報記録媒体若しくは警察情報システム内部に記録された情報をいう。

(8) アクセス

警察情報システムにデータを入力し、又は警察情報システムからデータを出力することをいう。

(9) アクセス権者

アクセスを行う権限を与えられた者をいう。

(10) アクセス範囲

アクセス権者ごとにその者が行うことができるアクセスの範囲をいう。

(11) ユーザＩＤ

アクセス権者を識別するためにアクセス権者ごとに一意に付与された文字列をいう。

(12) パスワード

警察情報システムを利用しようとする者がアクセス権者本人であるかどうかを検証するため用いられる文字列をいう。

(13) 認証

ユーザＩＤ、パスワード等を警察情報システムに入力することなどにより、アクセス権者が正当な者であるか否かを検証することをいう。

(14)　データベース装置

警察情報システムを構成するメインフレーム、サーバ等の電子計算機及びこれらに附置されるシステム管理を行う電子計算機をいう。

(15) ネットワーク機器

警察情報システムを構成するルータ、レイヤ３スイッチ、スイッチングハブ

等の機器若しくは伝送通信装置又はこれらから出力されるデータを利用することによりネットワークを管理する機能を有する機器をいう。

(16) 持ち出し用パソコン

警察情報システムのうち、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したものをいう。

(17) 外部回線

警察機関の管理が及ばない電子計算機が論理的に接続され、当該電子計算機の通信に利用されるインターネットその他の電気通信回線をいう。

第２　管理体制

１　情報セキュリティ管理者

(1) 情報セキュリティ管理者（訓令第３条に規定する情報セキュリティ管理者をいう。以下同じ。）は、最高情報セキュリティ管理者（警察庁情報通信局長をいう。）が行う調整の下、石川県警察における情報セキュリティに係る事務を統括する。

(2) 情報セキュリティ管理者は、警察庁情報セキュリティ管理者（警察庁情報通信局情報管理課長をいう。）の統括のもと業務を行う。

(3) 情報セキュリティ管理者は、情報セキュリティに係る事務を統括するに当たり、その事務に関係する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の意見を聞き、十分検討した上で処理しなければならない。

２　システムセキュリティ責任者

(1) 警察情報システムの整備を担当する課（課に相当する室、所、隊及び警察学校を含む。以下同じ。）にシステムセキュリティ責任者を置き、それぞれ当該課の長をもって充てる。

(2) 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関して、システムセキュリティ維持管理者及び運用管理者が３の(2)及び４の(2)の事務を処理するに当たって必要なセキュリティ要件を当該警察情報システムが備えるための事務を処理するとともに、整備した警察情報システムにおけるシステムセキュリティ維持管理者が行う事務を統括する。

３　システムセキュリティ維持管理者

(1) 警察情報システムを構成する電子計算機及びネットワーク機器の管理者権限を保有する課に、システムセキュリティ維持管理者を置き、それぞれ当該課の長をもって充てる。

(2) システムセキュリティ維持管理者は、担当する警察情報システムの維持管理時における情報セキュリティに係る事務を処理する。

４　運用管理者

(1) 警察情報システムを運用する所属に運用管理者を置き、所属長をもって充てる。

(2) 運用管理者は、所属における警察情報システムの運用に関し、情報セキュリティの維持その他の警察情報システムによる処理に係る情報の適正な取扱いを確保するために必要な事務を処理する。

５　システム管理担当者

(1) システムセキュリティ維持管理者は、その管理する電子計算機ごとにシステム

管理担当者を指名し、業務の責務に即した必要な範囲において、管理者権限を付与しなければならない。

(2) システム管理担当者は、担当する電子計算機その他の警察情報システムの情報セキュリティに係るシステム管理に関する事務を行う。

(3) システム管理担当者は、同一の者が複数の電子計算機に関して重複して指名されることを妨げない。

6　ネットワーク管理担当者

(1) システムセキュリティ維持管理者は、その管理するネットワーク機器ごとにネットワーク管理担当者を指名し、業務の責務に即した必要な範囲において、管理者権限を付与しなければならない。ただし、ネットワーク機器の維持管理に係る事務が軽微であると認められる場合は、システムセキュリティ維持管理者は、当該事務をシステム管理担当者に行わせることができる。

(2) ネットワーク管理担当者は、担当するネットワーク機器その他の警察情報システムに係るデータ伝送に関する監視及び制御その他の情報セキュリティに係るネットワーク管理に関する事務を行う。

(3) ネットワーク管理担当者は、同一の者が複数のネットワーク機器に関して重複して指名されることを妨げない。

第３　情報の分類及び取扱い

１　情報の分類

訓令第５条第１項の情報の分類は、別表第１のとおり実施する。

２　分類が異なる情報の取扱い

機密性、完全性又は可用性のいずれかの情報の分類が異なる情報を一の警察情報システムで取り扱うことについては、次のいずれかに該当するときに限り認めるものとする。

(1) 当該警察情報システムにおいて取り扱う情報のうち、最も上位の分類に応じた情報の管理が可能であるとき。

(2) 情報セキュリティ管理者の承認を受けたとき。

３　情報の分類及び通知

(1) 情報セキュリティ管理者は、警察情報システムで取り扱われる情報について、当該情報に係る業務を主管する所属の長及び当該情報を取り扱う警察情報システムのシステムセキュリティ責任者と協議の上、分類するものとする。

(2) 情報セキュリティ管理者は、(1)の規定に基づく情報の分類を関係所属に通知するものとする。

(3) 情報セキュリティ管理者は、情報の分類を変更する必要がある場合には、当該情報に係る業務を主管する所属の長及び当該情報を取り扱う警察情報システムのシステムセキュリティ責任者と協議し、必要な見直しを行わなければならない。

(4) 情報セキュリティ管理者は、(1)の規定に基づく情報の分類を警察庁情報セキュリティ管理者に報告しなければならない。

４　情報の取扱い

(1) 一般的な措置

情報の取扱いについては、この項に定めるもののほか、石川県警察文書管理規程（平成13年石川県警察本部訓令第２号）に定めるところによる。

ア　情報の作成、入手及び利用

(ｱ) 職員は、情報を不正に作成し、利用し、又は処分若しくはき損してはならない。

(ｲ) 職員は、情報を不当な目的で入手し、複製し、又は他の者に提供してはならない。

(ｳ) 職員は、情報を警察の庁舎外に不正に持ち出してはならない。

(ｴ) 職員は、情報セキュリティ管理者が認めた場合を除き、情報の分類を他の者が認識できる方法を用いて明示しなければならない。

イ　情報の管理

(ｱ)　職員は、情報の分類に応じて、警察情報システム、外部記録媒体、デジタル機器、画像等情報記録媒体、ドキュメント及び入出力資料の紛失、盗難の防止に対して十分に配意し、適切に管理しなければならない。

(ｲ)　職員は、運用管理者が認めた場合を除き、担当する業務に必要な情報以外の情報を保有してはならない。

ウ　情報の提供

(ｱ) 職員は、情報を公表する場合には、当該情報が別表第１において機密性低に分類される情報であることを確認しなければならない。

(ｲ) 職員は、情報を電磁的記録で公表又は提供する場合には、当該情報の付加情報等からの不用意な情報漏えいを防止するための措置を執らなければならない。

エ　情報の消去

(ｱ) システムセキュリティ責任者は、電子計算機及びネットワーク機器を廃棄し、又は利用を終了する場合には、システム管理担当者又はネットワーク管理担当者に、データ消去ソフトウェア又はデータ消去装置の利用、物理的又は磁気的な破壊等の方法を用いて、すべての情報を復元できないように措置させなければならない。また、システムセキュリティ責任者又はシステムセキュリティ維持管理者は当該情報が復元できないことを確認しなければならない。

(ｲ) 職員は、電子計算機、ネットワーク機器、デジタル機器、外部記録媒体及び画像等情報記録媒体を他の者へ提供する場合には、これらに保存されていた情報を復元できない状態にする必要性の有無を検討し、必要があると認めた情報について、データ消去ソフトウェア又はデータ消去装置等を用いて、当該情報を復元できないように措置し、システムセキュリティ維持管理者又は運用管理者はこれを確認しなければならない。

(ｳ) 職員は、情報を廃棄する場合には、裁断、データの消去その他の方法により当該情報を復元できないように措置しなければならない。

(2) 情報の分類に応じた措置

情報の分類に応じた措置は、別表第２のとおり実施する。

第４　警察情報システムの構成要素についての対策

1　設置環境、維持管理等

(1) 別表第１において機密性高に分類される情報若しくは機密性中に分類される情報に係るデータベース装置若しくはネットワーク機器（施錠された筐体に収容されているものであって電気通信回線から切り離された場合に直ちにそのことが検知できる仕組みを有するもの及び電子計算機（データベース装置を除く。(2)において同じ。）に近接して設置する必要のあるネットワーク機器を除く。）を設置し、又はそれらの装置若しくは機器に係るシステムドキュメントを保管する室（以下「警察情報システム機械室等」という。）は、人及び物の出入りを確実に管理することができ、外部からの侵入及び内部の視認が容易にできない構造の区域としなければならない。また、警察情報システム機械室等には、立入りが認められた者以外の者が立ち入ることができないよう必要な措置を執らなければならない。

(2) 別表第１において機密性低、完全性低及び可用性低に分類される情報以外の情報（以下「要保護情報」という。）を取り扱う電子計算機を設置し、それらの機器に係るシステムドキュメントを保管し、又は要保護情報に係る入出力資料、デジタル機器、外部記録媒体及び画像等情報記録媒体を取り扱う場所は、人及び物の出入りを管理することができるように区画された区域とし、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しなければならない。また、その区域には、立入りが認められた者以外の者が立ち入ることができないよう必要な措置を執らなければならない。

(3) 情報セキュリティ管理者は、警察情報システム機械室等に立ち入ることができる者の範囲をあらかじめ定め、システムセキュリティ維持管理者又は運用管理者は、そのうち、必要な者に許可を与えなければならない。また、職員以外の者が警察情報システム機械室等に立ち入るときは、職員を立ち会わせなければならない。

(4) 警察情報システム機械室等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警察情報システム機械室等の外に持ち出そうとする者は、システム管理担当者又はネットワーク管理担当者の立会いの下でこれを行い、その状況を記録しなければならない。

(5) システムセキュリティ維持管理者は、警察情報システムの構成又は情報の処理手順の変更その他の維持管理等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。また、システム管理担当者及びネットワーク管理担当者は、警察情報システムの構成又は情報の処理手順の変更その他の維持管理等に必要な作業（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、必要な対応を行わなければならない。

(6) 情報セキュリティ管理者は、警察情報システムについて一元的に把握し管理するため、必要な事項を記載した台帳を整備しなければならない。

2　電子計算機

(1) 共通対策

ア　職員は、警察情報システムを構成する機器、デジタル機器、外部記録媒体、画像等情報記録媒体及びドキュメントを適正に管理しなければならない。

イ　職員は、警察情報システムを構成する機器、デジタル機器、外部記録媒体、画像等情報記録媒体及びドキュメントを他の者に不正に交付し又は利用させてはならない。

ウ　職員は、警察情報システムを構成する機器、デジタル機器、外部記録媒体及び画像等情報記録媒体として、個人所有の機器、デジタル機器、外部記録媒体及び画像等情報記録媒体を利用してはならない。

エ　職員は、あらかじめ定められた目的以外の目的で不正に警察情報システムを利用してはならない。また、システムセキュリティ責任者が認めた場合を除き、警察情報システムを構成する機器に電子計算機等を接続又は増設し、若しくは警察情報システムを構成する機器を交換してはならない。

オ　職員は、システムセキュリティ責任者が認めた場合を除き、警察情報システムを構成する機器の改造を行い、又はソフトウェアの追加、削除若しくは変更をしてはならない。

カ　職員は、情報セキュリティ管理者が認めた場合を除き、警察情報システムを構成する機器、デジタル機器、外部記録媒体及び画像等情報記録媒体を警察の庁舎外に持ち出してはならない。

キ　システムセキュリティ責任者は、電子計算機（データベース装置を除く。）について、必要な対策を執らなければならない。

ク　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は、データベース装置について、許可のない者が容易に操作できないように所要の措置を執らなければならない。

ケ　システムセキュリティ責任者は、電気通信回線を経由してデータベース装置の保守作業を行う場合は、送受信される情報を暗号化する機能の必要性の有無を検討し、必要があると認めた場合は、当該機能を設けなければならない。また、システムセキュリティ維持管理者は、当該保守作業を行う場合には、送受信される情報を暗号化する必要性を検討し、必要があると認めたときは、暗号化しなければならない。

コ　システムセキュリティ責任者は、電子計算機にインストールしてもよいソフトウェア及び警察情報システムの維持管理に利用するソフトウェアを定めなければならない。また、システムセキュリティ維持管理者は、これに該当しないソフトウェアが稼働していることを認知した場合は、当該ソフトウェアを停止し、利用を定めたソフトウェアであっても、利用しない機能は無効化しなければならない。

サ　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、盗難及び設置場所からの不正な持ち出しを防止するための措置を執らなければならない。

シ　システム管理担当者は、データベース装置の時刻設定を正確なものとしなければならない。

(2) 持ち出し用パソコン対策

ア　システムセキュリティ責任者は、持ち出し用パソコンについて、必要な対策を執らなければならない。

イ　職員は、持ち出し用パソコンを警察の庁舎外に持ち出す必要がある場合には、持ち出し期間を明らかにし、システムセキュリティ維持管理者又は運用管理者の許可を得なければならない。また、庁舎外に持ち出すことを終了した場合には、当該許可者に対して、その旨を報告しなければならない。さらに、当該許可者は、持ち出し期間が満了しているにもかかわらず終了の報告がない場合は、その状況を確認し、必要な対応を講じなければならない。

ウ　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は、警察の庁舎外で持ち出し用パソコンから無線回線を利用してその他の警察情報システムにアクセスする仕組みを構築してはならない。

(3) 外部記録媒体対策

ア　外部記録媒体の利用制限

システムセキュリティ責任者は、職員が許可なく外部記録媒体を利用して情報を入出力できないようにするため、必要な措置を講じなければならない。

イ　外部記録媒体に記録する情報の暗号化機能の付与

(ｱ)　システムセキュリティ責任者は、外部記録媒体に記録する情報を自動的に暗号化する機能（以下「媒体自動暗号化機能」という。）を電子計算機に設けなければならない。

(ｲ)　システムセキュリティ責任者は、媒体自動暗号化機能を用いない場合に備え、自己復号型の暗号措置（特定のソフトウェアを使用することなく、あらかじめ設定された文字列を入力することにより暗号化されたファイルの復号が可能となる暗号措置のことをいう。以下同じ。）を行う機能又は当該機能と同等以上のセキュリティ基準を満たすと情報セキュリティ管理者が認める暗号措置を行う機能を電子計算機に設けなければならない。

ウ　外部記録媒体の利用状況の証跡取得機能の付与

システムセキュリティ責任者は、外部記録媒体に対する情報の入出力操作及び外部記録媒体の利用の許可に関する証跡を取得する機能を電子計算機に設けなければならない。

エ　電子計算機の内蔵ハードディスクの自動暗号化機能の付与

システムセキュリティ責任者は、電子計算機の内蔵ハードディスクに記録される情報を自動的に暗号化する機能を当該電子計算機に設けなければならない。

3　電子メール及びウェブ

(1) 職員は、業務遂行に係る情報を含む電子メールを送受信する場合には、警察が運営又は外部委託した電子メール機能を利用しなければならない。また、受信した電子メールについては、適切な方法により当該内容を表示しなければならない。

(2) システムセキュリティ責任者は、電子メールの送受信時に認証を行う機能を設けなければならない。

(3) 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は、電子メ

ールを保管、送受信又は中継するために設置される電子計算機及びウェブサービスを提供するために設置される電子計算機を不正に使用されることのないように構築し、管理しなければならない。

(4) 職員及びシステムセキュリティ責任者は、電子メール機能の利用及びウェブサービスの提供に当たって、利用者の情報セキュリティが損なわれることのないように必要な措置を執らなければならない。また、職員以外の者に電子メールの送受信又はウェブサービスを提供する場合には、情報セキュリティ管理者が認めた場合を除き、地方自治体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。

4　電気通信回線

(1) 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は、電気通信回線を利用するに当たっては、当該接続による情報セキュリティの維持に係るリスクを検討しなければならない。

(2) 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は、警察情報システムを構成する電気通信回線として、警察庁情報セキュリティ管理者が認めた回線を利用しなければならない。

(3) 職員は、情報セキュリティ管理者が認めた場合を除き、警察情報システムを構成する機器を外部回線に接続し、又は外部回線から警察情報システムにアクセスする仕組みを構築してはならない。

(4) 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は、ネットワーク機器について、許可のない者が容易に操作できないように所要の措置を執らなければならない。

(5) ネットワーク管理担当者は、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。

(6) ネットワーク管理担当者は、警察情報システムを構成する電気通信回線の監視をシステム管理担当者と協力して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。

第５　情報セキュリティ要件の明確化に基づく対策

1　情報セキュリティについての機能

(1) アクセス制御機能等

ア　システムセキュリティ責任者は、アクセス権者以外の者によるアクセス及びアクセス権者によるアクセス範囲を越えたアクセスを防止するために、整備する警察情報システムごとに認証、アクセス制御及び権限管理を行う機能を設けなければならない。また、アクセス権者及び各アクセス権者のアクセス範囲を定める場合は、当該警察情報システムで取扱う情報に係る業務を主管する所属の長と協議の上、整備する警察情報システムごとに、必要な手続を明確化し、業務上の責務と必要性を勘案して、必要最小限の範囲に限らなければならない。

イ　職員は、自己のユーザＩＤ以外のユーザＩＤを用いて、警察情報システムを利用してはならない。

ウ　職員は、自己のユーザＩＤ及びパスワード（以下「ユーザＩＤ等」とい

う。）を他の者に知らせてはならない。また、自己のユーザＩＤ等を他の者に知られないように適切に管理しなければならない。ただし、人事異動、長期休暇等に伴う引継ぎのために特に設定したユーザＩＤ等及びあらかじめ複数の者が共用することをシステムセキュリティ責任者又はシステムセキュリティ維持管理者が認めたものについては、この限りでない。

エ　職員は、ＩＣカード等による認証を用いる場合には、ＩＣカード等を本人が意図せずに使用されることがないように安全措置を執るとともに、紛失しないよう管理し、他の者に付与又は貸与してはならない。ただし、あらかじめ複数の者が共有することをシステムセキュリティ責任者又はシステムセキュリティ維持管理者が認めたものについては、この限りでない。また、ＩＣカード等を利用する必要がなくなった場合には、これをシステムセキュリティ維持管理者に返納するなどの適切な措置を執らなければならない。

オ　職員は、警察情報システムに設けられた機能を用いて、当該警察情報システムに保存される情報の分類に従って、必要なアクセス制御の設定をしなければならない。

カ　システムセキュリティ維持管理者は、遠隔地から制御又は監視する警察情報システムについて権限のない者が遠隔地から当該機器の制御又は監視を行うことがないよう厳重に管理しなければならない。

キ　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及びネットワーク管理担当者の権限を、個別の者に付与しなければならない。また、これを他の職員に代理させることはできない。

(2) 証跡管理

ア　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、証跡管理を行う必要性の有無を検討し、必要があると認めた警察情報システムには、証跡を取得する機能を設けなければならない。

イ　システムセキュリティ維持管理者は、警察情報システムに設けられた機能を利用して、事象ごとに必要な項目を証跡として記録し、管理しなければならない。また、その記録を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。

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、ネットワーク管理担当者及び職員に対して、証跡の管理、分析等を行う可能性があることをあらかじめ周知しなければならない。

エ　運用管理者は、所属の警察情報システムのアクセス権者及びアクセス範囲を適正に管理しなければならない。

(3) 暗号と電子署名

ア　情報セキュリティ管理者は、暗号化又は電子署名の付与に用いることができるアルゴリズムを、別途定めるとともに、当該アルゴリズムの安全性を随時評価し、必要な変更を行わなければならない。

イ　システムセキュリティ責任者は、警察情報システムにおいて暗号化又は電子署名の付与に用いるアルゴリズムをアで定められたものから選定するとともに、暗号化された情報の復号又は電子署名の付与に用いる鍵の管理につ

いて定めなければならない。

ウ　システムセキュリティ維持管理者は、電子署名の付与を行う必要があると認めた警察情報システムについて、電子署名の正当性を検証するための情報又は手段を署名検証者へ提供しなければならない。

エ　職員は、暗号化された情報の復号又は電子署名の付与に用いる鍵の管理を適正に行わなければならない。

2　特定脅威等への対策

(1) セキュリティホール対策

ア　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は、電子計算機及びネットワーク機器の構築及び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セキュリティホールについて対策を講じなければならない。

イ　システム管理担当者及びネットワーク管理担当者は、管理対象となる電子計算機及びネットワーク機器に関連する公開されたセキュリティホールの情報の入手に努めなければならない。また、その情報を入手した場合には、システムセキュリティ維持管理者に報告しなければならない。

ウ　システムセキュリティ責任者は、入手したセキュリティホールに関連する情報から、当該セキュリティホールが警察情報システムにもたらすリスクを分析した上で、セキュリティホール対策計画を作成し、これに基づいたセキュリティホール対策を講じるとともに、随時職員に周知しなければならない。

エ　システムセキュリティ維持管理者は、定期的にセキュリティホール対策及びソフトウェア構成の状況を記録し、これを確認、分析するとともに、不適切な状態にある電子計算機及びネットワーク機器を把握した場合には適切に対処しなければならない。

オ　システムセキュリティ責任者は、入手したセキュリティホールに関連する情報及び対策方法に関して、必要に応じ、システムセキュリティ維持管理者及び他のシステムセキュリティ責任者と共有しなければならない。

(2) 不正プログラム対策

ア　職員は、コンピュータ・ウイルス等不正プログラムが電子計算機、デジタル機器、外部記録媒体及び画像等情報記録媒体に存在していないことを確認しなければならない。また、不正プログラムが発見された場合には、直ちに拡散の防止のための措置を執らなければならない。

イ　情報セキュリティ管理者は、不正プログラム感染の回避を目的とした職員に対する留意事項を含む日常的実施事項を定めなければならない。

ウ　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は、不正プログラムから電子計算機（当該電子計算機で動作可能なコンピュータ・ウイルス対策ソフトウェア等が存在しないものを除く。）を保護するための対策を講じなければならない。また、不正プログラム対策の状況を適宜把握し、その見直しを行わなければならない。

(3) IPv6 技術を利用する通信への対策

ア　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は、警

察情報システムに IPv6 技術を利用する通信（以下「IPv6 通信」という。）の機能を導入する場合には、他の警察情報システムの情報セキュリティが損なわれることのないように必要な措置を執らなければならない。

イ　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は、IPv6 通信を想定していない電気通信回線に接続するすべての電子計算機及びネットワーク機器について、IPv6 通信を停止するための機能を有している場合には、当該機能の設定を適切に行わなければならない。

(4) 踏み台対策

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は、外部回線に接続する警察情報システムが、不正アクセス等の中継地点として使用されることを防止するため、(1)及び(2)に掲げるもののほか、必要な措置を執らなければならない。また、不正アクセス等の中継地点として使用された場合の影響が最小となるように警察情報システムを構築しなければならない。

3　警察情報システムのセキュリティ要件

(1) 警察情報システムの計画・設計

ア　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は、警察情報システムについて、その構築から運用管理にわたり、情報セキュリティを維持することが可能な体制の確保を情報セキュリティ管理者に求めることができる。

イ　システムセキュリティ責任者は、警察情報システムのセキュリティ要件を決定し、その要件を満たすために機器等の購入（購入に準ずる賃貸借契約を含む。）及びプログラム開発において必要な対策、情報セキュリティについての機能の設定、情報セキュリティについての脅威への対策、並びに警察情報システムの構成要素についての対策について定めなければならない。

ウ　システムセキュリティ責任者は、構築する警察情報システムに重要なセキュリティ要件があると認めた場合には、当該警察情報システムの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）評価・ＳＴ確認を受けなければならない。ただし、警察情報システムを改修する場合であって、見直し後のセキュリティ設計仕様書において重要なセキュリティ要件の変更が軽微であると認めたときはこの限りでない。

エ　システムセキュリティ責任者は、構築した警察情報システムの運用を開始するに当たって、情報セキュリティの観点から実施する運用開始のための手順及び環境を定めなければならない。

(2) 警察情報システムのセキュリティ要件

ア　警察情報システムの構築、運用及び監視

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は、警察情報システムの構築、運用及び監視に際しては、セキュリティ要件に基づき定めた情報セキュリティ対策を行わなければならない。

イ　警察情報システムの移行又は廃棄

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は、警

察情報システムの移行又は廃棄を行う場合は、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。

ウ　警察情報システムの見直し

システムセキュリティ責任者は、警察情報システムの情報セキュリティ対策について見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行い、必要な措置を執らなければならない。

4　外部委託

(1) 外部委託に当たっては、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) 職員は、警察情報システムの開発、運用管理、維持管理等を外部委託する場合は、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警察情報システムの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。また、契約に当たっては、当該事項を遵守させるための措置を定めるなど情報セキュリティの維持に関し所要の措置を執らなければならない。

(3) 職員は、警察情報システムに係る仕様書で一般に公開されるものを作成する場合は、当該仕様書が情報セキュリティの観点から支障のないものであることについて、あらかじめ情報セキュリティ管理者の指定する者の確認を受けなければならない。

5　業務継続計画との整合的運用の確保

情報セキュリティ管理者、システムセキュリティ責任者、システムセキュリティ維持管理者及び運用管理者は、業務継続計画（優先度が高い業務の継続性を確保するために必要な事項を定めたものをいう。以下同じ。）を策定する場合には、業務継続計画と警察情報セキュリティポリシーの整合的な運用が可能となるよう必要な措置を執らなければならない。

第6　事案発生時の措置

1　対処方法等の策定及び周知

情報セキュリティ管理者は、障害・事故等の事案について、その態様、対処方法、連絡体制、報告手順等当該事案を迅速かつ的確に措置するために必要な事項を定め、職員に周知しなければならない。

2　職員等の責務

情報セキュリティ管理者、システムセキュリティ責任者、システムセキュリティ維持管理者、運用管理者及び職員は、障害・事故等の事案発生時に、情報セキュリティ管理者が定める事項に基づき、必要な措置を執らなければならない。

3　事案の原因調査と再発防止策

情報セキュリティ管理者は、障害・事故等の事案が発生した場合には、当該事案の原因を調査し再発防止策を策定しなければならない。また、その調査結果を

警察庁情報セキュリティ管理者を通じて最高情報セキュリティ管理者に報告しなければならない。

4　警察情報セキュリティポリシー違反時の対応

情報セキュリティ管理者は、障害・事故等の事案が、職員が警察情報セキュリティポリシーに違反して警察情報システムを使用したことによる場合には、期間を定め、当該職員に警察情報システムを使用させないことができる。

第7　自己点検及び教養

1　自己点検

(1) 情報セキュリティ管理者は、職員の警察情報セキュリティポリシーにおける職務に応じた自己点検票及び自己点検の実施手順を定め、職員に対して自己点検の実施を指示しなければならない。

(2) 職員は、情報セキュリティ管理者の指示に従い、自己点検を実施し、その結果自身が改善すべき事項があった場合は改善し、その結果について情報セキュリティ管理者の評価を受けなければならない。

(3) 情報セキュリティ管理者は、自己点検の結果について、最高情報セキュリティ管理者の評価を受けなければならない。

(4) 情報セキュリティ管理者は、最高情報セキュリティ管理者より、評価による改善指示を受けた場合は、適切に措置しなければならない。

(5) 情報セキュリティ監査においては、自己点検の適正性の確認を行うものとする。

2　教養

情報セキュリティ管理者は、警察情報セキュリティポリシーを正しく理解し、これを確実に実施できるようにするため、職員に対し、職務に応じた教養を行うための体制を整備しなければならない。

第8　その他

1　警察情報セキュリティポリシーに係る情報の管理

職員は、警察情報セキュリティポリシーのうち、公知となることによって警察情報システムに係る犯罪、不正行為等による情報の漏えいその他の情報セキュリティの侵害事案の発生が懸念され、又は公知となることによって既存の警察情報システムに新たな情報セキュリティに係る対策を講じる必要が生じるもの（警察情報システム関係通達の内容の一部又は全部、個々の警察情報システムの構成、機能及び性能が明らかになる項目等）については、部外に公開してはならない。

2　警察情報セキュリティポリシーの見直し

警察情報セキュリティポリシーの規定については、見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行わなければならない。

3　細目的事項

この対策基準に定めるもののほか、警察情報システムに係る情報セキュリティの維持に関し必要な細目的事項は、別に定める。

附　則

この対策基準は、平成23年4月1日から施行する。

別表（略）