○　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号警察本部長）

[沿革]平成27年12月岩警務第73号、岩生安第105号、岩刑事第90号、岩交通第93号、岩警備第53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。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情勢の変化を踏まえ、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「岩手県警察情報セキュリティに係る管理体制」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。

なお、本通達の施行に伴い、旧通達は、廃止する。

別添

岩手県警察情報セキュリティに係る管理体制

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。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、警察情報セキュリティを確保するために必要な管理体制を定めるものとする。

２　情報の分類

情報の分類は次のとおりとする。

(1)　機密性

ア　機密性高

情報のうち、秘密文書（岩手県警察秘密文書の取扱いに関する訓令（平成13年岩手県警察本部訓令第24号）第２条第１項に定める秘密文書をいう。）の内容に相当する情報その他の機密性が損なわれることによる影響が大きいもの。

イ　機密性中

情報のうち、直ちに一般に公開することを前提としていないもの。

ウ　機密性低

情報のうち、機密性高又は機密性中に分類されるもの以外のもの。

(2)　完全性

ア　完全性高

情報のうち、改ざん又は滅失した場合に業務の的確な遂行に支障を及ぼすおそれがあるもの。

イ　完全性低

情報のうち、完全性高に分類されるもの以外のもの。

(3)　可用性

ア　可用性高

情報のうち、その情報が使用できないときに業務の安定的な遂行に支障を及ぼすおそれがあるもの。

イ　可用性低

情報のうち、可用性高に分類されるもの以外のもの。

３　用語の定義

警察情報セキュリティポリシーにおいて、次に掲げる用語の意義は、それぞれ次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)　要機密情報

機密性高又は機密性中に分類される情報をいう。

(3)　外部記録媒体

フロッピーディスク、フラッシュメモリ、ＤＶＤ規格媒体等電子計算機に接続し

情報を入出力する電磁的記録媒体をいう。

(4)　ネットワーク機器

システムを構成するルータ、ハブ等の機器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。

(5)　外部回線

警察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。

(6)　ネットワーク端末

ネットワークを介して他の電子計算機と接続された端末装置であって、インターネットに接続されていないものをいう。

(7)　インターネット端末

インターネットに接続された端末装置をいう。

(8)　スタンドアロンパソコン

他の電子計算機と接続されていない電子計算機をいう。

(9)　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した電子計算機（携帯電話機を含む。）をいう。

(10)　サーバ等

情報を体系的に記録し、検索し、又は編集する機能を有するサーバ及びメインフレームをいう。

(11)　自己復号型暗号

特定のソフトウェアをインストールすることなく復号することのできる暗号をいう。

(12)　警察暗号

警察が管理する電子計算機以外の電子計算機では技術的に復号できない暗号をいう。

(13)　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。

(14)　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ている、又は内蔵記憶装置を備えているものをいう。

(15)　約款による外部サービス

民間事業者等が約款に基づきインターネット上で提供する電子メール、ファイルストレージ、グループウェア等の情報処理サービスであって、約款への同意及び簡易なアカウントの登録により当該機能が利用可能となるサービスをいう。

第２　情報セキュリティ管理者

１　情報セキュリティ管理者の責務

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。）及び東北管区警察局情報セキュリティ管理者（東北管区警察局情報通信部情報技術解析課長をいう。）が行う調整の下、岩手県警察における情報セキュリティに係る事務を総括整理するものとする。

2　情報セキュリティ管理者の遵守事項

(1)　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総括整理するに当たっては、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聴き、十分検討した上で処理しなければならない。

(2)　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。

(3)　情報セキュリティ管理者は、職員に警察情報セキュリティポリシーを正しく理解させ、確実に遵守させるため、職員に対し、職務に応じた教養を実施しなければならない。

(4)　情報セキュリティ管理者は、災害時等において、警察情報システムの復旧、通信手段の確保等のためにやむを得ないときは、警察情報セキュリティポリシーの規定にかかわらず、所要の措置を執るものとする。

第３　区域情報セキュリティ管理者

1　区域情報セキュリティ管理者の設置

(1)　情報セキュリティ管理者は、岩手県警察の庁舎の敷地を複数の区域に分割し、当該区域をクラス０からクラス３までに分類する。

(2)　クラス０の区域を除く各区域に区域情報セキュリティ管理者を置き、情報セキュリティ管理者が指名する者をもって充てる。

(3)　区域の分類及び区域情報セキュリティ管理者の指名の方法は次の基準による。

ア　クラス０

各庁舎の敷地内であって、職員以外の者が自由に立ち入ることのできる区域は、一の区域とし、クラス０に分類する。

イ　クラス１

各庁舎における廊下等、職員の共用の区域は、一の区域とし、クラス１に分類するとともに、当該区域の区域情報セキュリティ管理者に、当該庁舎の庁舎管理に関する事務を処理する者を指名する。

ウ　クラス２

執務室は、所属ごとに一の区域とし、クラス２に分類するとともに、当該区域の区域情報セキュリティ管理者に、当該所属の長を指名する。

エ　クラス３

警察情報システムに係る機械室は、室ごとに一の区域とし、クラス３に分類するとともに、当該区域の区域情報セキュリティ管理者に、当該機械室を管理する所属の長を指名する。

2　区域情報セキュリティ管理者の責務

区域情報セキュリティ管理者は、当該区域における情報セキュリティの確保のための管理対策を行うものとする。

3　区域情報セキュリティ管理者の遵守事項

区域情報セキュリティ管理者は、関係する他の区域情報セキュリティ管理者、情報セキュリティ管理者等と連携し、次に定める対策を実施しなければならない。

(1)　クラス１の管理対策

ア　職員以外の者が不正に立ち入ることがないよう対策を執らなければならない。

イ　職員以外の者を立ち入らせるときは、その者の氏名、所属、訪問目的及び訪問相手を確認しなければならない。ただし、継続的に立ち入りを許可された者にあっては、この限りでない。

ウ　職員以外の者を立ち入らせるときは、職員とは種別の異なるカードを身に付けさせるなどして、職員とそれ以外の者を視覚上区別できるようにしなければならない。

(2)　クラス２の管理対策

ア　下位区域との境界を施錠可能な扉等によって仕切らなければならない。

イ　無人となるときは施錠しなければならない。

ウ　職員以外の者を立ち入らせるときは、区域内に設置された電子計算機の画面の不正な視認や、機器の持込みによる不正な撮影及び録音がされないよう必要に応じ措置しなければならない。

エ　クラス０に分類される区域と接するときは、当該境界において(1)に定める対策を実施しなければならない。ただし、合同庁舎等において、他の機関が(1)と同等以上の対策を実施しているときは、この限りでない。

(3)　クラス３の管理対策

ア　下位区域との境界の扉等を常時施錠し、区域内に立ち入ることができる者の名簿を作成しなければならない。この場合において、名簿に記載された者以外の者が立ち入る必要があるときは、区域情報セキュリティ管理者の承認を得なければならない。

イ　区域内に立ち入る者の氏名及び入退室の時刻を記録しなければならない。この場合において、当該記録は、可能な限り電磁的に記録させなければならない。

ウ　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。

エ　職員以外の者が立ち入っている間は、職員が立ち会わなければならない。

オ　区域情報セキュリティ管理者が認めた場合を除き、電子計算機及び外部記録媒体を持ち込んではならない。

カ　自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策を講じなければならない。

４　例外

情報セキュリティ管理者が、１(3)の基準による運用を困難と認めたときは、当該基準によらない区域を設けることができる。この場合において、情報セキュリティ管理者は、３の規定を参考として、関係する他の情報セキュリティ管理者等と連携の上、可能な限り情報セキュリティの確保のための管理対策を行わなければならない。

第４　システムセキュリティ責任者

1　システムセキュリティ責任者の設置

警察情報システムの整備を担当する所属にシステムセキュリティ責任者を置き、当該所属の長をもって充てる。

2　システムセキュリティ責任者の責務

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が必要な情報セキュリティ要件を備えるための事務を処理するものとする。

3　システムセキュリティ責任者の遵守事項

(1)　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の情報セキュリティ要件について、あらかじめ情報セキュリティ管理者の確認を受けなければならない。

(2)　システムセキュリティ責任者は、所管する警察情報システムごとに、当該システムを利用する業務の主管課の長と連携の上、当該システムの運用要領を策定するなどして、職員が当該システムを取り扱う際に遵守すべき事項を職員に周知するとともに、情報セキュリティ管理者に通知しなければならない。この場合において、遵守すべき事項には、次に掲げる事項を含めなければならない。

ア　当該システムにおいて取り扱うことのできる情報の機密性の分類の範囲

イ　当該システムにおいて、職員が独自の判断で行うことのできる改造（新たな機器の接続、ソフトウェア追加等をいう。）の範囲

(3)　システムセキュリティ責任者は、所管する警察情報システムについて、情報セキュリティに係る脆弱性に関する情報（以下「脆弱性情報」という。）を入手したときは、情報セキュリティ管理者に連絡するとともに、当該脆弱性情報が警察情報システムにもたらすリスクを分析した上で、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、所管する警察情報システムについて、災害時等においても継続して運用できるよう十分検討し、必要に応じて業務継続計画を策定しなければならない。この場合において、当該業務継続計画は、可能な限り警察情報セキュリティポリシーとの整合を図らなければならない。

(5)　システムセキュリティ責任者は、所管する警察情報システムの情報セキュリティ対策について脆弱性検査等により見直しを行う必要性の有無を適宜検討し、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。

第５　システムセキュリティ維持管理者

1　システムセキュリティ維持管理者の設置

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所属に、システムセキュリティ維持管理者を置き、当該所属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の責務

システムセキュリティ維持管理者は､システムセキュリティ責任者の指示等を受け、担当する電子計算機及びネットワーク機器の維持管理のための事務を処理するものとする。

3　システムセキュリティ維持管理者の遵守事項

(1)　システムセキュリティ維持管理者は、管理者権限を適正に運用しなければならな

い。

(2)　システムセキュリティ維持管理者は、各種ソフトウェアのうち利用しない機能は無効化しなければならない。

(3)　システムセキュリティ維持管理者は、定期的に脆弱性情報に係る対策、導入したソフトウェアのバージョンアップ等の状況を記録し、これを確認及び分析するとともに、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。

(4)　システムセキュリティ維持管理者は、警察情報セキュリティポリシー又は運用要領に違反する行為を認知したときは、速やかにシステムセキュリティ責任者に連絡しなければならない。

第６　運用管理者

１　運用管理者の設置

警察情報システムを運用する所属に運用管理者を置き、当該所属の長をもって充てる。

２　運用管理者の責務

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ものとする。

第７　運用管理補助者

１　運用管理補助者の設置

警察情報システムを運用する所属に運用管理補助者を置き、当該所属の副署長又は次長等をもって充てる。

２　運用管理補助者の責務

運用管理補助者は、運用管理者の処理する事務を補助するものとする。

第８　取扱責任者

１　取扱責任者の設置

警察情報システムを運用する所属に取扱責任者を置き、警察本部にあっては運用管理者が指名する課長補佐等（警部以上の階級にある警察官又は同相当職の一般職員をいう。）、警察署にあっては各課長をもって充てる。ただし、やむを得ない事情があるときはこの限りでない。

２　取扱責任者の責務

取扱責任者は、取扱者である部下職員を指導監督するものとする。また、外部記録媒体を利用した情報の入出力の管理に係る事務を行うものとする。

第９　システム管理担当者

１　システム管理担当者の設置

システムセキュリティ維持管理者は、その管理するシステムごとにシステム管理担当者を指名し、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の責務

システム管理担当者は、担当するシステムに係るシステム管理に関する業務を行うものとする。

3　システム管理担当者の遵守事項

(1)　システム管理担当者は、権限のない者にＩＤを発行してはならない。

(2)　システム管理担当者は、警察情報システムに係るドキュメントを適正に管理しなければならない。

(3)　システム管理担当者は、担当する電子計算機に関連する脆弱性情報の入手に努めなければならない。この場合において、脆弱性情報を入手した場合には、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に報告しなければならない。

(4)　システム管理担当者は、クラス３に指定された区域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、クラス２以下に指定された区域に持ち出すときは、その状況を記録しなければならない。

(5)　システム管理担当者は、システムの構成の変更等の作業（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。

第10　ネットワーク管理担当者

1　ネットワーク管理担当者の設置

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ごとにネットワーク管理担当者を指名し、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　ネットワーク管理担当者の責務

ネットワーク管理担当者は、担当するネットワーク機器に係るネットワーク管理に関する業務を行うものとする。

3　ネットワーク管理担当者の遵守事項

(1)　ネットワーク管理担当者は、担当するネットワーク機器に関連する脆弱性情報の入手に努めなければならない。この場合において、脆弱性情報を入手した場合には、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に報告しなければならない。

(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について、データ伝送に関する監視及び制御を行わなければならない。

(3)　ネットワーク管理担当者は、ネットワークの構成の変更等の作業（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。

第11　情報セキュリティ対策委員会

1　情報セキュリティ対策委員会の設置

情報セキュリティに関する組織管理を図るため、所属に情報セキュリティ対策委員会（以下「対策委員会」という。）を設置する。

2　情報セキュリティ対策委員会の組織

対策委員会は、委員長、副委員長、委員、推進員及び委員会庶務をもって組織し、それぞれ次に掲げる者をもって充てる。

(1)　委員長は、運用管理者をもって充てる。

(2)　副委員長は、運用管理補助者をもって充てる。
(3)　委員は、取扱責任者をもって充てる。
(4)　推進員は、本部所属は所属内で２名以上、警察署は各課１名以上とし、委員長が指名する者をもって充てる。
(5)　委員会庶務は、所属内で１名とし、委員長が指名する者をもって充てる。この場合において、委員又は推進員と委員会庶務を兼務させることができるものとする。

3　委員長等の責務

(1)　委員長は、対策委員会の事務を管理監督するものとする。
(2)　副委員長は、委員長を補佐し、対策委員会の事務を各員に指示、遂行させるものとする。
(3)　委員は、対策委員会の事務を確実に遂行し、情報セキュリティに関する事項を部下職員に指導監督するものとする。
(4)　推進員は、委員を補佐し、対策委員会の事務が滞りなく遂行されるように推進するものとする。
(5)　委員会庶務は、各委員が遂行する対策委員会の事務についての取りまとめ及び連絡調整を行うものとする。

4　情報セキュリティ対策委員会の所掌事務

対策委員会の所掌事務は、次に掲げるものとする。

(1)　情報セキュリティの教養の実施に関すること。
(2)　情報セキュリティ関係の手続に関すること。
(3)　警察情報システム機器等の維持管理及び障害対応に関すること。
(4)　(1)から(3)までに掲げるもののほか、所属の情報セキュリティの維持に関すること。

5　委員会選定状況の報告

(1)　対策委員会は、対策委員会の各委員等の選定状況及び取扱責任者を指名する場合の指名状況について、情報セキュリティ対策委員会選定報告書（様式）により、毎年４月10日までに情報セキュリティ管理者へ報告しなければならない。
(2)　対策委員会は、対策委員会の各委員等の選定状況及び取扱責任者を指名する場合の指名状況に変更があった場合は、都度、情報セキュリティ対策委員会選定報告書（様式）により情報セキュリティ管理者へ報告しなければならない。

6　対策委員会の事務に係る留意事項

対策委員会は、事務の遂行に当たり、推進員、委員会庶務等の特定の者に事務が集中することのないよう努めなければならない。

第12　その他

1　情報セキュリティインシデント発生時の措置

不正プログラム感染等の情報セキュリティインシデント（情報セキュリティの維持を困難とする事案をいう。）が発生した際の措置については、別に定める。

2　分掌

区域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、それぞれの事務のうち分庁舎において処理される

ものについて、当該分庁舎の警視相当職以上の職員に分掌させることができる。

3　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宜検討し、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。

4　警察情報セキュリティポリシーの解釈

警察情報セキュリティポリシーの解釈に関し疑義があるときは、情報セキュリティ管理者がこれを裁定する。

様式（第11の５関係）

保存	１年
廃棄	.

情報セキュリティ管理者　殿
（　警　務　部　長　）

運　用　管　理　者
（　　）

情報セキュリティ対策委員会選定報告書

みだしのことについて、　　年度の委員を下記のとおり選定したから報告する。

記

委員名	役　職	階　級	氏　名	備　考[注]

注：委員であって、取扱責任者として指名した者については、備考欄にその旨記載すること。

【この係：　　】