通達甲（総．情．セ１）第１０号
平成２６年５月２７日
存　　続　　期　　間

各　　所　　属　　長　　殿

総　　務　　部　　長

警視庁警察情報システム整備要綱の制定について

このたび、別添のとおり、警視庁警察情報システム整備要綱を制定し、平成２６年６月１日から実施することとしたから、運用上誤りのないようにされたい。

別添

警視庁警察情報システム整備要綱

第１　目的

この要綱は、警視庁情報セキュリティに関する規程（平成２６年５月２７日訓令甲第２２号。以下「セキュリティ規程」という。）の施行に関し、警察情報システム（外部記録媒体及び特定用途機器を含む。以下同じ。）の整備及び維持管理について、必要な事項を定めることを目的とする。

第２　用語の定義

１　この要綱における用語の意義は、次のとおりとする。

(1)　特定用途機器　電気通信回線に接続され、又は内蔵記憶装置を備えている機器であって、警視庁情報管理システム及び警視庁情報処理システムのいずれにも属さないものをいう。

(2)　ネットワーク機器　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。

(3)　システムドキュメント　警察情報システムに係る仕様書、設計書等警察情報システムの整備又は維持管理のために必要な文書、図画及び電磁的記録をいう。

(4)　システムドキュメント等　システムドキュメント並びに警察情報システムを維持管理するために記録しなければならないものとして情報セキュリティ管理補佐官が指定した文書及び電磁的記録をいう。

(5)　所属独自ネットワークシステム　警視庁情報処理システムのうち、所属において独自に構築するものをいう。

２　前１に規定するもののほか、この要綱において使用する用語は、セキュリティ規程において使用する用語の例による。

第３　警視庁情報管理システム又は警視庁情報処理システムの整備を担当する所属における管理体制

１　システムセキュリティ責任者の任務

(1)　システムセキュリティ責任者は、警視庁情報管理システム又は警視庁情報処理システム（以下単に「システム」という。）の運用に関し、必要な事項を定め、その適正を図らなければならない。

(2)　システムセキュリティ責任者は、所管するシステムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保に努めなければならない。

(3)　システムセキュリティ責任者は、所管するシステムについて、次の仕様書等を整備しなければならない。

ア　サーバ等及び端末の仕様書又は設計書

イ　電気通信回線及びネットワーク機器の仕様書又は設計書

(4)　システムセキュリティ責任者は、所管するシステムの運用及び保守において、当該システムに実装されたセキュリティ機能を適切に運用しなければならない。

(5)　システムセキュリティ責任者は、警察情報システム及び管理対象情報に対するアクセスの権限を適切に管理しなければならない。

(6)　システムセキュリティ責任者は、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。）を入手した場合は、情報セキュリティ管理補佐官に連絡するとともに、必要な措置を講じなければならない。

(7)　システムセキュリティ責任者は、システムについて、業務の継続に重大な支障を来し、又は国民の安全及び利益に重大な脅威となる事態を想定し、当該事態に対応するための計画を定めなければならない。

(8)　システムセキュリティ責任者は、システムにおける情報セキュリティの維持のための対策を随時検証し、見直しを行う等必要な措置を講じなければならない。

(9)　システムセキュリティ責任者は、システム管理担当者及びネットワーク管理担当者に対して、セキュリティ機能の利用方法等に関わる教養を実施しなければならない。

(10)　システムセキュリティ責任者は、システムの運用に関し、情報セキュリティの維持のために、職員に対する指導教養を行うとともに、当該システムの管理運用状況について点検しなければならない。

(11) システムセキュリティ責任者は、可用性高情報を取り扱うシステムを構成するネットワーク機器については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しなければならない。

(12) システムセキュリティ責任者は、基盤となる情報システムを利用してシステムを整備する場合は、基盤となる情報システムに係る運用通達等で求められる事務を処理するとともに、基盤となる情報システムの運用通達等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切に警察情報システムを運用しなければならない。

(13)　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設置環境、取り扱う管理対象情報の分類、管理対象情報を取り扱う者等に応じて、必要な対策を講じなければならない。

(14)　システムセキュリティ責任者は、必要に応じて、所管する警察情報システムを構成する機器のソフトウェアの名称、バージョン等に関する情報を自動で収集し、管理する機能を

導入しなければならない。

(15) システムセキュリティ責任者は、必要に応じて、所管する警察情報システムにおける不正な通信等を監視するとともに、不正な通信等を認知した場合は、速やかに必要な対応を行わなければならない。

(16) その他システムセキュリティ責任者が遵守すべきシステムの運用及び保守に必要な事項については、別に定める。

2　システム管理担当者

(1)　システム管理担当者の設置

システムの整備を担当する所属にシステム管理担当者を置き、警察署以外の所属にあっては課長代理又はこれに相当する職にある者、警察署にあっては課長又はこれに相当する職にある者のうち、システムセキュリティ責任者が指定する者をもって充てる。

(2)　システム管理担当者の任務

システム管理担当者は、システムセキュリティ責任者を補佐し、システムを構成する機器（ネットワーク機器を除く。ウ及びエにおいて同じ。）及び当該システムで取り扱われる情報の管理を行うものとする。この場合において、システム管理担当者は、次の事項に留意しなければならない。

ア　システムに係る管理者権限を、任務に即した必要な範囲において適正に付与しなければならない。

イ　システムに係るシステムドキュメント等を適正に管理しなければならない。

ウ　システムを構成する機器に関連する脆弱性情報の入手に努め、当該脆弱性情報を入手した場合は、システムセキュリティ責任者に報告しなければならない。

エ　クラス３（警視庁情報セキュリティ対策実施要綱（平成２６年５月２７日通達甲（総．情．セ１）第９号）第３の１の（１）に規定するものをいう。以下同じ。）の区域に設置されているシステムを構成する機器、外部記録媒体又はシステムドキュメントを、クラス３以外の区域に持ち出す場合は、その状況を記録しなければならない。

オ　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、事前にその影響を確認するとともに、当該作業を監視し、必要な対応を行わなければならない。

3　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

システムの整備を担当する所属にネットワーク管理担当者を置き、警察署以外の所属にあっては課長代理又はこれに相当する職にある者、警察署にあっては課長又はこれに相当する職にある者のうち、システムセキュリティ責任者が指定する者をもって充てる。

(2)　ネットワーク管理担当者の任務

ネットワーク管理担当者は、システムセキュリティ責任者を補佐し、システムを構成するネットワーク、ネットワーク機器及び当該ネットワーク機器で取り扱われる情報の管理を行うものとする。この場合において、ネットワーク管理担当者は、次の事項に留意しなければならない。

ア　ネットワークに係る管理者権限を、任務に即した必要な範囲において適正に付与しなければならない。

イ　システムを構成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、当該脆弱性情報を入手した場合は、システムセキュリティ責任者に報告しなければならない。

ウ　システムを構成するネットワークについて、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。

エ　システムを構成するネットワーク又はネットワーク機器の変更等の作業（軽微なものを除く。）を行う場合は、情報セキュリティの観点から、事前にその影響を確認するとともに、当該作業を監視し、必要な対応を行わなければならない。

第４　システムの整備

１　警視庁情報管理システムの整備

(1)　システムセキュリティ責任者は、警視庁情報管理システムを構築し、又は変更しようとする場合は、次の事項について、事前に情報セキュリティ管理補佐官と協議をし、決定した事項について情報セキュリティ管理者の承認を受けなければならない。

ア　当該警視庁情報管理システムの目的

イ　当該警視庁情報管理システムの設計

ウ　当該警視庁情報管理システムの管理体制

エ　当該警視庁情報管理システムにおいて取り扱う情報の分類

オ　当該警視庁情報管理システムにおける登録又は照会の手順

カ　当該警視庁情報管理システムにおけるアクセス権の範囲

キ　当該警視庁情報管理システムにおける情報の保存期間

ク　当該警視庁情報管理システムの管理運用に関すること。

ケ　当該警視庁情報管理システムにおける入出力資料の取扱いに関すること。

コ　当該警視庁情報管理システムにおいて取り扱う個人情報照会に関する記録の確認に関すること。

サ　当該警視庁情報管理システムと他の警視庁情報管理システムとの統廃合の可否に関すること。

シ　当該警視庁情報管理システムに係るシステムドキュメントの作成及び保管に関すること。

ス　その他当該警視庁情報管理システムにおける情報セキュリティの維持に関すること。

(2)　システムセキュリティ責任者は、警視庁情報管理システムを廃止しようとする場合は、次の事項について、事前に情報セキュリティ管理補佐官と協議をし、決定した事項について情報セキュリティ管理者の承認を受けなければならない。

ア　当該警視庁情報管理システムの廃止に伴う業務への影響に関すること。

イ　当該警視庁情報管理システムの情報の整理に関すること。

２　警視庁情報処理システムの整備

(1)　所属独自ネットワークシステム

ア　システムセキュリティ責任者は、所属独自ネットワークシステムを構築し、又は変更

しようとする場合は、次の事項について、事前に情報セキュリティ管理補佐官と協議をし、決定した事項について情報セキュリティ管理者の承認を受けなければならない。

(ｱ)　当該所属独自ネットワークシステムの目的

(ｲ)　当該所属独自ネットワークシステムに接続される機器の構成

(ｳ)　当該所属独自ネットワークシステムの管理体制

(ｴ)　当該所属独自ネットワークシステムにおいて取り扱う情報の分類

(ｵ)　当該所属独自ネットワークシステムにおける登録又は照会の手順

(ｶ)　当該所属独自ネットワークシステムにおけるアクセス権の範囲

(ｷ)　当該所属独自ネットワークシステムにおける情報の保存期間

(ｸ)　当該所属独自ネットワークシステムの管理運用に関すること。

(ｹ)　当該所属独自ネットワークシステムにおける入出力資料の取扱いに関すること。

(ｺ)　当該所属独自ネットワークシステムにおける個人情報照会に関する記録の確認に関すること。

(ｻ)　当該所属独自ネットワークシステムに係るシステムドキュメント等の作成及び保管に関すること。

(ｼ)　その他当該所属独自ネットワークシステムにおける情報セキュリティの維持に関すること。

イ　システムセキュリティ責任者は、所属独自ネットワークシステムを廃止しようとする場合は、事前に情報セキュリティ管理補佐官に通知しなければならない。

(2)　インターネット端末

ア　システムセキュリティ責任者は、インターネット端末を構築し、又は変更しようとする場合は、次の事項について、事前に情報セキュリティ管理補佐官と協議をし、決定した事項について情報セキュリティ管理者の承認を受けなければならない。

(ｱ)　当該インターネット端末の目的

(ｲ)　当該インターネット端末の管理体制

(ｳ)　当該インターネット端末を接続させるネットワークの種類

(ｴ)　当該インターネット端末におけるアクセス権の範囲

(ｵ)　当該インターネット端末において取り扱う情報の分類

(ｶ)　当該インターネット端末における情報の保存方法及び伝送方法

(ｷ)　当該インターネット端末において障害が発生した場合の復旧方法

(ｸ)　当該インターネット端末及びそれに付帯する周辺機器の管理運用に関すること。

(ｹ)　当該インターネット端末に係るシステムドキュメント等の作成及び保管に関すること。

(ｺ)　その他当該インターネット端末における情報セキュリティの維持に関すること。

イ　システムセキュリティ責任者は、インターネット端末を廃止しようとする場合は、事前に情報セキュリティ管理補佐官に通知しなければならない。

(3)　スタンドアロンパソコン

ア　システムセキュリティ責任者は、スタンドアロンパソコンを構築し、又は変更しよう

とする場合は、次の事項について、事前に情報セキュリティ管理補佐官と協議をし、決定した事項について情報セキュリティ管理者の承認を受けなければならない。

(ｱ)　当該スタンドアロンパソコンの目的

(ｲ)　当該スタンドアロンパソコンの管理体制

(ｳ)　当該スタンドアロンパソコン及びそれに付帯する周辺機器の管理運用に関すること。

(ｴ)　当該スタンドアロンパソコンに係るシステムドキュメント等の作成及び保管に関すること。

(ｵ)　その他当該スタンドアロンパソコンにおける情報セキュリティの維持に関すること。

イ　システムセキュリティ責任者は、スタンドアロンパソコンを廃止しようとする場合は、事前に情報セキュリティ管理補佐官に通知しなければならない。

3　システムの維持管理

システムセキュリティ責任者は、次の事項に留意してシステムの維持管理を行わなければならない。

(1)　情報セキュリティ管理補佐官が指定する方法で、システムを構成する機器に管理番号を付与すること。

(2)　他所属にシステムを配備する場合は、管理番号ごとに配備先を明らかにすること。

(3)　システムの運用方法に関して必要な事項を定めること。

(4)　システムにアクセスできる権限の範囲を明示すること。

4　システムの検証

(1)　システムセキュリティ責任者は、定期的にシステムの運用実態を調査し、業務の効率性及び経済性の観点から当該システムの有効性について検証した上で、見直す必要があると認める場合は、必要な措置を講じなければならない。

(2)　情報セキュリティ管理補佐官は、必要に応じて、システムセキュリティ責任者に対し、前（１）による調査を依頼し、その結果に基づきシステムの有効性について評価を行うものとする。この場合において、システムセキュリティ責任者は、当該評価に基づき、当該システムの統廃合又は変更について必要な措置を講じなければならない。

第５　警察庁情報管理システムの維持管理

1　システムセキュリティ維持管理者の設置

警察庁情報管理システムを維持管理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任務

システムセキュリティ維持管理者は、前記第３の２及び３の規定に準じて、システム管理担当者及びネットワーク管理担当者を指定し、警察庁情報管理システムの維持管理を行うものとする。この場合において、警察庁システムセキュリティ責任者（警察における情報セキュリティに係る管理体制について（平成２９年１月３１日警察庁丙情管発第５号ほか）第６の１の規定により警察庁に置かれるシステムセキュリティ責任者をいう。（６）において同

じ。）が定める運用要領等に従うとともに、次の事項に留意しなければならない。

(1)　管理者権限を適正に運用しなければならない。

(2)　利用者が警察庁情報管理システムを利用しなくなった場合は、当該利用者のユーザＩＤ及びパスワード等の不正な利用を防止するための措置を速やかに講じなければならない。

(3)　許可のない利用者による警察庁情報管理システム及び警察庁情報管理システム内の情報へのアクセスを制限するために、アクセス制御機能を適切に運用しなければならない。

(4)　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。

(5)　定期的に脆弱性情報に係る対策、警察庁情報管理システムに導入されたコンピュータ・ウイルス対策ソフトウェアのウイルス定義ファイルの更新状況及びソフトウェアのバージョンアップ等の状況を確認し、不適切な状態にある当該警察庁情報管理システムを構成する機器を把握した場合は、適切に対処しなければならない。

(6)　警察庁システムセキュリティ責任者が定める運用要領、セキュリティ規程、警視庁情報セキュリティ対策実施要綱その他情報セキュリティに係る規程の規定に違反する行為を認知した場合は、速やかに当該警察庁システムセキュリティ責任者及び情報セキュリティ管理補佐官に報告しなければならない。

３　警察庁情報管理システムの維持管理上の留意事項

システムセキュリティ維持管理者は、次の事項に留意して警察庁情報管理システムの維持管理を行わなければならない。

(1)　情報セキュリティ管理補佐官が指定する方法で、警察庁情報管理システムを構成する機器に管理番号を付与すること。

(2)　他所属に警察庁情報管理システムを配備する場合は、管理番号ごとに配備先を明らかにすること。

(3)　警察庁情報管理システムの運用方法に関して必要な事項を定めること。

(4)　警察庁情報管理システムにアクセスできる権限の範囲を明示すること。

第６　システムの技術的要件

システムセキュリティ責任者は、整備を担当するシステムが、別に定める技術的要件を満たすように整備を行わなければならない。

第７　警察情報システムに係るシステムドキュメント等の管理

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、次の事項に留意して警察情報システムに係るシステムドキュメント等を管理しなければならない。

１　当該システムドキュメント等の内容を常に最新のものとしておくこと。

２　当該システムドキュメント等を、関係のない者が閲覧することができないよう施錠設備のある保管庫に保管すること。

３　当該システムドキュメント等は、原本の保管その他記載されている記録の完全性を担保する目的以外の目的で複写しないこと。

第８　外部記録媒体等の配備等

１　外部記録媒体の配備

(1)　同一機会に複数の所属に対し配備する目的で外部記録媒体を調達しようとする所属長

は、事前に情報セキュリティ管理補佐官と次の事項について協議の上、当該外部記録媒体に管理番号を付与し､配備先の所属に対し必要な指示をした上で配備しなければならない。この場合において、当該所属長は、当該外部記録媒体を配備した旨を当該管理番号とともに、情報セキュリティ管理補佐官に通知しなければならない。

ア　当該外部記録媒体の管理運用に関すること。

イ　別に定める「外部記録媒体管理システム」の登録に関すること。

ウ　当該外部記録媒体の返納及び廃棄に関すること。

エ　その他当該外部記録媒体における情報セキュリティの維持に関すること。

(2)　所属からの要望に応じて外部記録媒体を配備する所属長は、次の事項について、配備先の所属に対して指示をした上で配備しなければならない。

ア　当該外部記録媒体の配備に係る上申手続に関すること。

イ　当該外部記録媒体の管理運用に関すること。

ウ　外部記録媒体管理システムの登録に関すること。

エ　当該外部記録媒体の返納及び廃棄に関すること。

オ　その他当該外部記録媒体における情報セキュリティの維持に関すること。

2　外部記録媒体の廃棄

(1)　前１により外部記録媒体を他所属に配備した所属長（以下「媒体配備所属長」という。）は、配備した外部記録媒体を廃棄する場合は、当該外部記録媒体を配備先の所属から回収し、消去用ソフトの使用、消去装置の利用、物理的破壊等の方法により、当該外部記録媒体に保存されていた情報を復元できないような措置を講じた上で廃棄しなければならない。

(2)　媒体配備所属長は、配備した外部記録媒体に保存されている情報の消去が容易な方法で行うことができるものと認める場合は、配備先の所属に対し、当該外部記録媒体の廃棄方法について必要な指示をした上で廃棄させることができる。

3　デジタルカメラ、ボイスレコーダ等の配備

(1)　デジタルカメラ、ボイスレコーダ、デジタルビデオカメラ等内蔵記憶装置に情報を保存することが可能であり、又は、電子計算機に接続して情報を入出力することが可能である機器（以下「デジタルカメラ等」という。）を他所属に配備しようとする所属長は、事前に情報セキュリティ管理補佐官と次の事項について協議の上、配備先の所属に対し、必要な指示をした上で配備しなければならない。

ア　当該デジタルカメラ等の運用管理に関すること。

イ　その他当該デジタルカメラ等における情報セキュリティの維持に関すること。

(2)　デジタルカメラ等を配備する所属長は、当該デジタルカメラ等に付属する外部記録媒体について、前１及び２による措置を講じなければならない。

(3)　デジタルカメラ等を配備しようとする所属長は、当該デジタルカメラ等の内蔵記憶装置に情報を保存することを認めるものとして配備する場合又は当該デジタルカメラ等を警察情報システムに接続することを認めるものとして配備する場合は、事前に情報セキュリティ管理補佐官と協議の上、情報セキュリティ管理者の承認を受けなければならない。

第９　特定用途機器の配備等

１　特定用途機器を配備しようとする所属長は、当該特定用途機器の運用に関し、必要な事項を定め、その適正を図らなければならない。この場合において、当該所属長は、次の事項について、事前に情報セキュリティ管理補佐官と協議をし、決定した事項について情報セキュリティ管理者の承認を受けなければならない。

(1)　当該特定用途機器の管理運用に関すること。

(2)　その他当該特定用途機器における情報セキュリティの維持に関すること。

２　前１の協議に当たっては、当該特定用途機器の利用方法、取り扱う情報の分類、電気通信回線への接続形態その他当該特定用途機器の特性及び利用環境に応じたセキュリティ対策を検討しなければならない。