通達甲（総．情．セ１）第９号
平成２６月５月２７日
存　　続　　期　　間

各　　所　　属　　長　　殿

総　　務　　部　　長

警視庁情報セキュリティ対策実施要綱の制定について

このたび、別添のとおり、警視庁情報セキュリティ対策実施要綱を制定し、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

警視庁情報セキュリティ対策実施要綱

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、警視庁における情報セキュリティを維持するための対策その他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)　庁舎　警視庁の各所属が使用している庁舎（敷地を含む。）をいう。

(2)　端末等　ネットワーク端末、インターネット端末及びスタンドアロンパソコンをいう。

(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)　入力資料　警察情報システムを構成するサーバ等により処理される情報を記録した文書、図画及び電磁的記録をいう。

(5)　出力資料　警察情報システムを構成するサーバ等により処理された情報を記録した文書、図画及び電磁的記録をいう。

(6)　モバイルパソコン　スタンドアロンパソコンのうち、庁舎から持ち出して使用することを前提として整備を行ったものをいう。

(7)　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。

(8)　電子メール　インターネット端末において、外部回線を通じて文字情報、画像情報等を伝達する手段をいう。

(9)　モバイルインターネット端末　インターネット端末のうち、庁舎から持ち出して使用するものとして整備を行ったもの又はインターネットに接続することができる公用の携帯電話機をいう。

(10)　ＫＩＩＳ端末　インターネットに接続し、職務の遂行上必要となる情報の収集、提供又は共有を行うため各所属に共通の基盤を提供することを目的とし、情報管理課が設置するサーバ、端末、通信機器及びこれらを接続する電気通信回線並びにこれらの用に供するプ

ログラムを組み合わせたものにおいて用いる電子計算機をいう。

(11) 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、当該サービスを提供するサーバにおいて利用者が情報の作成、保存、送信等を行うものをいう。

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　管理体制

１　区域における管理体制

(1)　庁舎の分類及び分割並びに区域情報セキュリティ管理者の設置

庁舎（当庁以外の行政機関その他の団体が使用している部分を除く。）を、別表第１の「区域における管理体制」により、区域に分類し、及び分割し、各区域（クラス０の区域を除く。）に区域情報セキュリティ管理者を置くものとする。

(2)　区域情報セキュリティ管理者の任務

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を確保するとともに、関係する他の区域情報セキュリティ管理者と連携し、別に定める管理対策を実施しなければならない。

２　所属における管理体制

所属長は、所属における情報セキュリティの確保のため、別表第２の「所属における管理体制」により、情報管理責任者、情報管理者、情報管理補助者、セキュリティ指導員及びセキュリティ準指導員を指定するものとする。ただし、これにより難い場合は、情報セキュリティ管理補佐官と協議の上、これに代わるべき措置を講ずるものとする。

第４　情報の分類及び管理の基準

１　情報の分類及び管理の基準は、別表第３の「情報の分類及び管理の基準」のとおりとする。

２　情報管理者は、職員が情報を作成し、又は入手した場合は、その分類及び取扱制限を決定しなければならない。

３　職員以外の者に情報を提供する場合には、別に定める場合を除き、その機密性の分類及び取扱制限を明示しなければならない。

４　情報の分類及び取扱制限の継承

情報を作成し、又は複製する際に、参照した情報又は入手した情報に分類及び取扱制限の決定が既になされている場合には、元となる情報の機密性の分類及び取扱制限を継承しなければならない。

５　情報の分類及び取扱制限の見直し

情報管理者は、情報の修正、追加、削除その他の理由により、情報の分類及び取扱制限を見直す必要があると認める場合は、速やかに当該情報の分類及び取扱制限を見直さなければならない。

第５　警察情報システムの取扱い

１　機器の管理

(1)　情報管理責任者は、所属における機器（警察情報システムを構成する機器であって、

外部記録媒体以外のものをいう。第５において同じ。）の管理について指導及び調整を行うものとする。

(2)　情報管理責任者は、所属に配備された全ての端末等の管理番号、種別等の必要事項を、端末等配備状況管理システム（所属に配備された端末等を一元的に管理するためのシステムをいう。）に登録するとともに、情報管理者に当該端末等を適正に管理させるものとする。

(3)　情報管理者は、担当する部署に別に定める「端末等配備状況管理表」を備え付けなければならない。

(4)　情報管理者は、システムセキュリティ責任者が定めた範囲内で、担当する部署の職員に端末等を使用させるものとする。

２　機器の配備等

(1)　システムセキュリティ責任者は、機器を他所属に配備する場合は、情報セキュリティ管理補佐官と協議の上、必要な措置を講ずるものとする。

(2)　所属長は、機器の新設、増設、移設、返納、修理又は変更の必要がある場合は、関係するシステムセキュリティ責任者と協議の上、必要な措置を講じなければならない。

(3)　所属長は、配備された機器が職員の配置換え等により不要となった場合は、速やかに情報セキュリティ管理補佐官及び関係するシステムセキュリティ責任者の指示を受け、返納の措置を講じなければならない。

３　機器の持ち出し

(1)　モバイルパソコン等（モバイルパソコン及びモバイルインターネット端末をいう。３において同じ。）を庁舎外に持ち出す場合は、内蔵記憶装置の要機密情報を必要最小限にし、情報漏えいの防止に努めるとともに、別に定める場合を除き、情報管理者の承認を受けなければならない。

(2)　所属長は、職員が他の所属においてモバイルパソコン等を継続して使用する場合には、持ち出し先の所属の長に対し当該モバイルパソコン等の管理を依頼しなければならない。

(3)　モバイルパソコン等以外の機器を庁舎外に持ち出す場合は、当該機器を整備したシステムセキュリティ責任者に連絡の上、指示を受けなければならない。

４　不正プログラム対策

情報管理者は、システムセキュリティ責任者が指定する方法により、担当する部署の端末等で動作するコンピュータ・ウイルス対策ソフトウェア（以下「ウイルス対策ソフト」という。）のウイルス定義ファイルを遅滞なく更新し、その状況を確認しなければならない。

５　アクセス権管理

所属長は、所属における警察情報システムにアクセスする権限を、適正に管理しなければならない。

６　アクセス制御

(1)　他の職員のユーザＩＤを不正に用いて、警察情報システムにアクセスしてはならない。

(2)　自己のアクセスできる権限の範囲を超えて、警察情報システムにアクセスしてはならない。

(3)　他の者にアクセスさせる必要がない情報については、当該情報にパスワードを設定する

等他の者がアクセスすることができないような措置を講じなければならない。

(4)　自己の認証情報を権限のない者に知られないよう適切に管理しなければならない。

(5)　認証機器のうち別に指定するものを使用する場合は、別に定める方法により必要な措置を講じなければならない。

(6)　保守又は試験を行う場合を除き、職員以外の者に警察情報システムを操作させてはならない。

　また、保守又は試験のため職員以外の者に警察情報システムを操作させる場合は、職員が立ち会わなければならない。

7　電子メール及びウェブ

(1)　情報を送受信する場合は、別に定める場合を除き、警察情報システムを利用しなければならない。

(2)　別に定める場合を除き、電子メールにより要機密情報を取り扱ってはならない。

(3)　不審な電子メールを受信した場合は、速やかに情報セキュリティ管理補佐官及び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。

(4)　別に定める場合を除き、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信してはならない。

第６　外部記録媒体の取扱い

1　外部記録媒体の管理

(1)　情報管理責任者は、所属における外部記録媒体の管理について指導及び調整を行うものとする。

(2)　情報管理責任者は、所属の全ての外部記録媒体の管理番号、種別等の必要事項を、外部記録媒体管理システム（所属に配備された外部記録媒体及びＵＩＤを一元的に管理するためのシステムをいう。）に登録するとともに、情報管理者に当該外部記録媒体を適正に管理させるものとする。

(3)　情報管理者は、担当する部署に別に定める「外部記録媒体管理表」を備え付けなければならない。

2　外部記録媒体の使用

(1)　外部記録媒体を使用する場合は、別に定める場合を除き、情報管理者の承認を受けなければならない。

(2)　情報を外部記録媒体に保存する場合は、別に認める場合を除き、暗号化しなければならない。

(3)　外部記録媒体を機器に接続する場合は、当該外部記録媒体に不正プログラムが記録されていないことを確認しなければならない。

第７　ＵＩＤの取扱い

　ＵＩＤの管理及び使用については、前第６の１及び２の（１）の規定を準用する。

第８　デジタルカメラ等の取扱い

1　デジタルカメラ等の管理

(1)　情報管理責任者は、所属におけるデジタルカメラ、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。）の管理について指導及び調整を行うものとする。

(2)　情報管理責任者は、所属における全てのデジタルカメラ等の管理番号、種別等の必要事項を、デジタルカメラ等管理システム（デジタルカメラ等を一元的に管理するシステムをいう。）に登録するとともに、情報管理者に当該デジタルカメラ等を適正に管理させるものとする。

(3)　情報管理者は、担当する部署に別に定める「デジタルカメラ等管理表」を備え付けなければならない。

2　デジタルカメラ等の使用

(1)　デジタルカメラ等を使用する場合は、別に定める場合を除き、情報管理者の承認を受けなければならない。

(2)　情報セキュリティ管理者が個別に認めた端末等を除き、デジタルカメラ等を警察情報システムに接続してはならない。

(3)　別に定める場合を除き、デジタルカメラ等の内蔵記憶装置に情報を保存してはならない。

(4)　デジタルカメラ等を情報セキュリティ管理者が認める機器以外のものに接続した場合は、当該デジタルカメラ等に不正プログラムが記録されていないことを確認しなければならない。

第９　機器等の点検

１　情報管理者は、前記第５から第７までの機器及びデジタルカメラ等の管理状況について、別に定める場合を除き、毎月１回以上点検を行い、所属長に報告しなければならない。

２　情報管理者及び情報管理補助者は、職員が使用した機器及びデジタルカメラ等の返納状況を確認しなければならない。

第 10　携帯電話機（付属する外部記録媒体を含む。）の取扱い

１　業務における公用の携帯電話機の使用

(1)　業務において携帯電話機を使用する場合は、公用の携帯電話機を使用するものとする。

(2)　業務で使用する公用の携帯電話機については、当該携帯電話機に保存されている通話履歴、送受信メール履歴、電話帳等のデータのうち、要機密情報に該当するものを閲覧する際に、パスワード入力等の認証を求められるよう設定しなければならない。

(3)　業務で使用する公用の携帯電話機に前（２）で設定した認証情報を、権限のない者に知られることがないよう適切に管理しなければならない。

(4)　業務で使用する公用の携帯電話機で情報の処理（通話を除く。以下同じ。）をした場合は、業務に支障がない限り、速やかに当該携帯電話機の内蔵記憶装置から当該情報を消去しなければならない。この場合において、当該携帯電話機で処理した情報を警察情報システムに取り込む必要があるときは、別に指定する方法により端末等に取り込むことができる。

２　業務における個人所有の携帯電話機の使用

(1)　個人所有の携帯電話機を使用して情報の処理を行うことが想定される場合は、事前に当

該携帯電話機の電話番号、メールアドレス及び機種を所属長に報告の上、承認を受けなければならない。

(2)　前（１）の承認を受けた携帯電話機について、当該携帯電話機において動作するウイルス対策ソフトが存在しない場合を除き、ウイルス対策ソフトを導入しなければならない。

(3)　前記（１）の承認を受けた携帯電話機について、前１の（２）及び（３）に規定する措置を講じなければならない。

(4)　業務において緊急に情報を伝達する必要があり、かつ、他に代替手段がないときに限り、前記（１）の承認を受けた携帯電話機を使用して情報の処理を行うことができる。

(5)　前記（１）の承認を受けた携帯電話機を使用して情報の処理を行った場合は、速やかに当該携帯電話機の内蔵記憶装置から当該情報を消去し、情報管理者の確認を受けなければならない。この場合において、当該携帯電話機で処理した情報を警察情報システムに取り込む必要があるときは、情報管理者に報告した上で、別に指定する方法により端末等に取り込むことができる。

第 11　約款による外部サービスの取扱い

情報発信のために約款による外部サービスを利用する場合には、事前に情報セキュリティ管理補佐官、システムセキュリティ責任者及び業務を主管する所属長等と協議を行い、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得なければならない。

第 12　職員の責務

１　情報又はプログラムを不正に保持し、作成し、利用し、毀損し、廃棄し、又は改ざんしてはならない。

２　定められた目的以外の目的で警察情報システムを使用してはならない。

３　警察情報システムに、システムセキュリティ責任者の許可を受けていない機器を接続してはならない。

４　個人所有の機器（携帯電話機を除く。）を事務室に持ち込んではならない。

５　情報セキュリティに係る不正を認知した場合は、直ちに所属長に報告しなければならない。

第13　情報セキュリティインシデント発生時の措置

１　所属長は、次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。以下同じ。）の発生を認知した場合は、直ちに情報セキュリティ管理者に報告しなければならない。

(1)　情報流出事案

(2)　重大障害事案

(3)　不正プログラム感染、不正アクセス事案等

(4)　警察情報システムの不正使用事案

(5)　個人所有の機器の不正使用事案

(6)　機器の紛失事案

(7)　その他社会的反響が大きいと予想される事案

２　所属長は、警視庁ＣＳＩＲＴの長が情報セキュリティインシデントの発生又はそのおそれがあると判断して調査を行う場合は、職員に対して指定された日時及び場所に出頭させ、説

明させ、又は資料若しくは個人所有の機器の提出を求めるなど、これに協力しなければならない。

3　情報セキュリティ管理者は、前記１による報告をした所属長に対し、必要な指導を行うものとする。

第 14　教養等

1　情報セキュリティ管理補佐官は、警察情報システムに関する知識及び技能の向上並びに情報セキュリティに関する教養計画を策定し、これに基づいた教養を推進するとともに、必要により職員を招致して指導又は助言を行うものとする。

2　システムセキュリティ責任者は、整備を担当する警視庁情報管理システム又は警視庁情報処理システムごとに、職員が当該警視庁情報管理システム又は警視庁情報処理システムを取り扱う際に遵守すべき事項について教養を推進するものとする。

3　所属長は、所属における情報セキュリティについて教養を行うものとする。

第 15　緊急事態に係る特例

1　システムセキュリティ責任者又は所属長は、この要綱に定める規定によることが業務に著しく支障を及ぼす場合又は技術的に困難な場合は、情報セキュリティ管理補佐官と協議の上、この要綱に定める規定と同水準の対策を講じ、情報セキュリティ管理者の承認を得た場合に限り、この要綱に定める規定によらないことができる。

2　職員は、大規模災害、重大テロ等の緊急事態であって、この要綱に定める規定によることが困難な場合は、所属長の指示により、これらの規定によらずに情報を処理することができる。

別表第１

区域における管理体制

区域	分類の基準	分割の基準	区域情報セキュリティ管理者
クラス０	職員以外の者が自由に立ち入ることのできる場所	庁舎ごと	なし
クラス１	職員が自由に立ち入ることのできる共用の場所	庁舎ごと	警視庁庁舎管理規程（昭和５７年１２月１日訓令甲第２７号。以下「庁舎管理規程」という。）第３条第２項に規定する庁舎管理責任者
クラス２	事務室（クラス３に分類されるものを除く。）	所属ごと	事務室を管理する所属の長
クラス３	警察情報システムに係るサーバ等を設置した室	室ごと	室を管理する所属の長

別表第２

所属における管理体制

	警察署	警察署以外の所属	任務
情報管理責任者	副署長（島部警察署にあっては次長）	庶務担当課長代理又はこれに相当する職にある者	所属内の情報セキュリティの維持に関すること。
情報管理者	課長（島部警察署にあっては次長、その他の警察署で課長の配置のない課にあっては課長代理）	課長代理又はこれに相当する職にある者（配置のない部署にあっては係長）	担当する部署の情報セキュリティの維持に関すること。
情報管理補助者	課長代理（島部警察署にあっては係長）	係長又はこれに相当する職にある者	情報管理者の任務の補助に関すること。
セキュリティ指導員	情報セキュリティに関する知識を有する巡査部長以上の階級（同相当職を含む。）にある者のうち、情報管理責任者が適任と認めたもの		情報管理責任者が行うべき事務の処理の補助に関すること。
セキュリティ準指導員	情報セキュリティに関する知識を有する者のうち、情報管理者が適任と認めたもの		情報管理者が行うべき事務の処理の補助に関すること。

別表第３

情報の分類及び管理の基準

	分類の基準	管理の基準
機密性高	情報のうち、特定秘密（特定秘密の保護に関する法律（平成２５年法律第１０８号）第３条第１項の規定により指定された特定秘密をいう。）又は秘密文書（警視庁秘密文書取扱規程（平成２４年１２月２７日訓令甲第２８号）第２条第１項第１号に規定するものをいう。）に相当する機密性を有する情報を含むもの	１　別に認める場合を除き、庁舎外に設置され、若しくは警察が維持管理を行っていない機器に保存し、又は庁舎外に設置され、若しくは警察が維持管理を行っていない機器により作成してはならない。 ２　別に認める場合を除き、インターネット端末において取り扱ってはならない。 ３　職員以外の者へ提供する場合は、所属長の承認を受けるとともに、提供先に対して適正な取扱いを求めなければならない。 ４　庁舎外に持ち出す場合は、所属長の承認を受けなければならない。 ５　別に認める場合を除き、複製し、又は配布してはならない。 ６　廃棄する場合は、復元できない方法により行わなければならない。
機密性中	情報のうち、東京都情報公開条例（平成１１年３月１９日東京都条例第５号）第７条各号における非開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、機密性高情報以外のもの	１　別に認める場合を除き、庁舎外に設置され、若しくは警察が維持管理を行っていない機器に保存し、又は庁舎外に設置され、若しくは警察が維持管理を行っていない機器により作成してはならない。 ２　別に認める場合を除き、インターネット端末において取り扱ってはならない。 ３　職員以外の者へ提供する場合は、所属長の承認を受けるとともに、提供先に対して適正な取扱いを求めなければならない。 ４　前３の場合を除き、庁舎外に持ち出す場合は、情報管理者の承認を受けなければならない。 ５　必要以上に複製し、又は配布してはならない。 ６　廃棄する場合は、復元できない方法により行わなければならない。
機密性低	情報のうち、東京都情報公開条例第７条各号における非開示情報に該当すると判断される蓋然性の高い情報を含まないもの	１　インターネット端末において、取り扱うことができる。 ２　公表する場合は、要機密情報に分類されていないことを情報管理者が確認しなければならない。
完全性高	情報（書面に記載された情報を除く。）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	１　必要に応じてバックアップを取得しなければならない。 ２　庁舎外に持ち出す場合は、所属長の承認を受けるとともに、滅失、紛失等を防止するため、適切な措置を講じなければならない。
完全性低	情報（書面に記載された情報を除く。）のうち、完全性高に分類されるもの以外のもの	改ざん又は滅失を防止するための措置を検討しなければならない。
可用性高	情報（書面に記載された情報を除く。）のうち、その情報が利用できない場合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	１　必要に応じて、システム障害等に備えた機器の二重化、バックアップシステムの構築等により可用性を確保しなければならない。 ２　庁舎外に持ち出す場合は、所属長の承認を受けるとともに、滅失、紛失等を防止するため、適切な措置を講じなければならない。
可用性低	情報（書面に記載された情報を除く。）のうち、可用性高に分類されるもの以外のもの	可用性が確保されない場合の代替手段をあらかじめ定めておかなければならない。