兵庫県警察情報システムの利用及び管理対象情報の取扱いに係る警察職員の遵守事項について（例規甲）

〔平成28年９月20日
兵警情例規甲第31号本部長〕

〔沿革〕　平成30年２月兵警情例規甲第８号、31年２月第７号、令和３年１月兵警総例規甲第３号、４年10月兵警情例規甲第27号、５年３月兵警広例規甲第23号改正

兵庫県警察情報システムの利用及び管理対象情報の取扱いに係る警察職員の遵守事項についてを下記のように定め、平成28年10月１日から実施する。

記

第１　総則

１　目的

この通達は、兵庫県警察における情報セキュリティに関する訓令（平成23年兵庫県警察本部訓令第１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、兵庫県警察情報システムの利用及び管理対象情報を取り扱う際に、職員が遵守すべき事項を定めるものとする。

２　定義規定等の適用

訓令、兵庫県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28年兵警情例規甲第30号。以下「管理体制通達」という。）及び兵庫県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28年兵警情例規甲第32号）に定めるところによる定義規定及び略称規定は、この通達において適用する。

３　定義

この通達において、次に掲げる用語の意義は、それぞれに定めるところによる。

(1)　要機密情報　警察情報システムにおいて取り扱われる機密性３（高）情報又は機密性２（中）情報に分類される管理対象情報をいう。

(2)　要保全情報　完全性２（高）情報に分類される管理対象情報をいう。

(3)　要保護情報　要機密情報、要保全情報又は要安定情報のいずれかに該当する管理対象情報をいう。

(4)　暗号化消去　情報を電磁的記録媒体に暗号化して記録した上で、当該情報の復号に用いる鍵を抹消することにより情報の復号を不可能にし、情報を利用不能にする論理的削除方法をいう。

(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)　主体認証情報格納装置　ＩＣカード等主体認証情報を格納した装置であって、正当な主体に所有させ、又は保持させる装置をいう。

(7)　携帯電話機　フィーチャーフォン、スマートフォン等回線（電気通信役務としての移動通信サービスに係る無線局を自ら開設し、開設された無線局に係る免許人等の地位を承継し、又は運用している電気通信事業者が設置する回線をいう。）を利用し音声通話及び情報の処理を行うための端末をいう。

(8)　平文　暗号化されていない文字、画像、音声等のデータをいう。

(9)　暗号文　暗号化された文字、画像、音声等のデータをいう。

(10) 業務委託　警察情報システムの開発、構築及び運用に係る業務についてリース契約を行う等警察の業務（管理対象情報が取り扱われる場合に限る。）の一部又は全部について、契約をもって外部の者に実施させることをいう。
(11) アプリケーション・コンテンツ　情報の提供、行政手続、意見の募集等の行政サービスを行うことを目的として利用者に提供するアプリケーションプログラム、ウェブコンテンツ等の総称をいう。
(12) 外部サービス　クラウドサービス、ウェブ会議サービス、ソーシャルメディアサービス等部外の者が一般に対して情報システムの一部又は全部の機能を提供するもの(管理対象情報を取り扱うものに限る。)をいう。
(13) クラウドサービス　外部サービスのうち、事業者によって定義されたインタフェースを用いた、拡張性及び柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワークを経由してアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに係る十分な条件設定の余地があるものをいう。
(14) 約款、規約等による外部サービス　外部サービスのうち、事業者等が不特定多数の利用者に対して提供する、画一的な約款、規約等への同意のみで利用可能となるものをいう。

第２　管理対象情報の分類及び取扱制限の決定、明示等

１　管理対象情報の分類及び取扱制限の決定

職員は、管理対象情報を作成し、又は部外から入手したときは、当該情報の機密性、完全性及び可用性の分類を定めるとともに、必要により当該分類に応じた取扱制限を定めなければならない。

２　機密性１（低）情報の分類

職員（運用管理者以上の職にある者を除く。）は、管理対象情報を機密性１（低）情報に分類する場合には、当該情報が明らかに非公開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であるときを除き、所属の上級の職員であって、警部以上の階級にある警察官又は警部相当職以上の一般職員（夜間・休日にあっては宿直責任者（兵庫県警察本部宿直勤務規程（昭和49年兵庫県警察本部訓令第19号）第７条に規定する一般宿直責任者及び業務別宿直責任者を除く。以下同じ。））の承認を得なければならない。

３　管理対象情報の分類及び取扱制限の明示

職員は、管理対象情報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。ただし、次に掲げる場合はこの限りでない。

(1)　部内において管理対象情報を取り扱う場合で、管理対象情報の機密性の分類及び取扱制限が明らかであるとき。
(2)　部外に管理対象情報を提供する場合で、総務部長が当該明示の必要がないものとして別に定める場合に該当するとき。

４　管理対象情報の分類及び取扱制限の継承

職員は、管理対象情報を作成し、若しくは複製する際に参照した管理対象情報又は入手した管理対象情報に、分類及び取扱制限の決定が既になされている場合には、元となる管理対象情報の機密性に係る分類及び取扱制限を継承しなければならない。

５　管理対象情報の分類及び取扱制限の見直し

職員は、修正、追加、削除その他の理由により、管理対象情報の分類又は取扱制限を見直す必要がある場合には、当該情報の分類及び取扱制限の決定者等と協

議の上、見直さなければならない。

第３　管理対象情報の取扱い

１　準拠

管理対象情報の取扱いについては、兵庫県警察公文書管理規程（令和３年兵庫県警察本部告示第17号）、個人情報の保護に関する法律（平成15年法律第57号）その他別に定める規程によるほか、本項目に定めるところにより適正に管理を行うものとする。

２　管理対象情報の利用

(1)　職員は、管理対象情報を不正に作成又は入手してはならない。

(2)　職員は、管理対象情報を不正に利用又は毀損してはならない。

(3)　職員は、要保護情報を放置してはならない。

(4)　職員は、要機密情報を必要以上に配布してはならない。

(5)　職員は、要機密情報を必要以上に複製してはならない。

３　管理対象情報の提供・運搬

(1)　職員は、管理対象情報を公表する場合には、当該情報が機密性１（低）情報に分類されることを確認しなければならない。

(2)　職員は、管理対象情報を部外に電磁的記録で提供する場合には、ファイルの属性情報等からの情報漏えいを防止しなければならない。

(3)　職員（運用管理者以上の職にある者を除く。）は、機密性２（中）情報について、閲覧可能な範囲外の者に提供し、又は警察の庁舎外への持ち出しを行う場合は、第２の５の規定に基づき当該情報の分類及び取扱制限の見直しを行った上で、その旨を所属の上級の職員であって、警部以上の階級にある警察官又は警部相当職以上の一般職員（夜間又は休日にあっては宿直責任者）に報告（口頭による報告を含む。以下同じ。）しなければならない。

(4)　職員（運用管理者以上の職にある者を除く。）は、機密性３（高）情報について、閲覧可能な範囲外の者に提供し、又は警察の庁舎外への持ち出しを行う場合は、第２の５の規定に基づき当該情報の分類及び取扱制限の見直しを行った上で、総務部長が別に定める手続により許可を得なければならない。

(5)　職員は、要機密情報について、閲覧可能な範囲外の者に提供する場合には、第２の５の規定に基づき当該情報の分類及び取扱制限の見直しを行った上で、提供先において、当該情報に付された分類及び取扱制限に応じて適切に取り扱われるよう、取扱上の留意事項を確実に伝達するなどの措置をとらなければならない。

(6)　職員は、要保護情報が記録され、又は記載された記録媒体の運搬（同一庁舎内への運搬を除く。）を部外の者に依頼する場合には、必要に応じて、受領印が必要となる書留郵便での郵送、専用車両による配達サービス、配達状況の追跡が可能なサービス等の手段により運搬しなければならない。

４　管理対象情報の保存

(1)　職員は、警察の庁舎外に設置されている機器に要機密情報を保存してはならない。ただし、総務部長が別に定めるところにより保存する場合はこの限りではない。

(2)　職員は、要機密情報の取扱いが認められた警察情報システムを除き、外部回線に接続する警察情報システムにおいて、要機密情報を取り扱ってはならない。

(3)　職員は、警察が維持管理を行っていない機器に、機密性３（高）情報を保存してはならない。

(4)　職員は、保存する管理対象情報にアクセス制限を設定するなど、管理対象情報の分類及び取扱制限に従って管理対象情報を適切に管理しなければならない。

5　管理対象情報の廃棄

(1)　職員は、電磁的記録媒体に保存された管理対象情報が職務上不要となった場合には、速やかに当該情報を消去しなければならない。

(2)　職員は、電磁的記録媒体を廃棄する場合は、当該記録媒体内に管理対象情報が残存した状態とならないよう、全ての管理対象情報を復元できないように抹消し、又は電磁的記録媒体を物理的に破壊しなければならない。

(3)　職員は、要機密情報が記載された書面を廃棄する場合は、復元が困難な状態にしなければならない。

6　管理対象情報を取り扱う区域における対策

職員は、クラス１からクラス３までの区域に立ち入るときは、区域情報セキュリティ管理者が定めた対策に従わなければならない。また、職員以外の者を立ち入らせるときには、当該職員以外の者にも当該区域で定められた対策に従わせなければならない。

第４　警察情報システムの取扱い

1　共通事項

(1)　職員は、警察情報システムにおいて管理対象情報を取り扱う場合には、当該警察情報システムのシステムセキュリティ責任者が定めた機密性、完全性及び可用性の範囲を超えた管理対象情報を取り扱ってはならない。

(2)　職員は、警察情報システムの利用時には、利用環境に配意し、関係のない者に管理対象情報を視認されないよう留意しなければならない。特に、知識による主体認証情報を入力する際には、権限のない者に視認されていないことを確認しなければならない。

(3)　職員は、定められた目的以外の目的で使用するなど警察情報システムを不正に使用してはならない。

(4)　職員は、管理体制通達第３の３の(3)のコの（ウ）に該当する場合を除き、システムセキュリティ責任者の許可なく、警察情報システムを構成する機器の改造（新たな機器の接続、ソフトウェアの追加等をいう。）をしてはならない。

(5)　職員は、警察情報システムで利用される電気通信回線に、当該電気通信回線を管理するシステムセキュリティ責任者の許可を受けていない警察情報システムを接続してはならない。

(6)　職員は、警察情報システムを不正操作から保護するため、スクリーンロックの設定、利用後のログアウトの徹底等必要な措置をとらなければならない。

(7)　職員は、外部回線に接続することを前提として整備された場合を除き、警察情報システムを外部回線に接続してはならない。

(8)　職員は、外部回線から電子計算機にソフトウェアをダウンロードする場合には、当該ソフトウェアの配布元を確認しなければならない。

(9)　職員は、不正プログラムの解析、犯罪の証拠となるファイルの取り扱い等を目的として整備された警察情報システムを除き、不正プログラム感染を回避するため、ウイルス対策ソフトウェア等により不正プログラムとして検知された実行プログラム形式のファイルを実行してはならない。また、不正プログラムとして検知されたデータファイルをアプリケーション等で読み込んではならない。

(10) 職員は、部外から情報やソフトウェアを端末及びサーバ等に取り込む場合又は部外に情報やソフトウェアを提供する場合には、不正プログラム感染の有無を確認しなければならない。

(11) 職員は、不審なウェブサイトの閲覧等が認められるものとして整備された警察情報システムを利用する場合を除き、不正プログラムに感染するリスクを低減する警察情報システムの利用方法として、次に掲げる措置をとらなければならない。

ア　不審なウェブサイトを閲覧しないこと。

イ　安全性が確実でないソフトウェアをダウンロード又は実行しないこと。

ウ　アプリケーションの利用において、マクロ等の自動実行機能を無効にすること。

2　事案発生時の措置

職員は、不正プログラムに感染したおそれがある場合には、直ちにネットワークケーブルを切り離すなどして回線を切断するとともに、総務部長が別に定める方法により、対応しなければならない。

3　アクセス制御

(1)　職員は、自己のユーザＩＤ以外のユーザＩＤを不正に用いて、警察情報システムを使用してはならない。

(2)　職員は、自己に付与されたユーザＩＤを適切に管理するため、次に掲げる措置をとらなければならない。

ア　知る必要のない者に知られるような状態で放置しないこと。

イ　他者が主体認証に用いるために付与又は貸与しないこと。

ウ　ユーザＩＤを利用する必要がなくなった場合には、定められた手続に従い、ユーザＩＤの利用を停止すること。

(3)　職員は、自己の主体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。

(4)　職員は、知識による主体認証情報を用いる場合には、次の管理を徹底しなければならない。

ア　主体認証情報を設定する場合には、容易に推測されないものにすること。

イ　異なるユーザＩＤに対して、共通の主体認証情報を用いないこと。

ウ　異なる警察情報システムにおいて、ユーザＩＤ及び主体認証情報については共通の組合せを用いないこと。ただし、シングルサインオン（共通のユーザＩＤ及び主体認証情報により複数の情報システムの認証を行うよう設計された認証方式をいう。）による認証の場合はこの限りでない。

エ　ユーザＩＤ及び主体認証情報を他の職員と共用している場合で、当該他の職員が異動等により当該ユーザＩＤを利用する必要がなくなったときは、当該主体認証情報を速やかに変更しなければならない。

(5)　職員は、ＩＣカード等の主体認証情報格納装置による主体認証を行う場合には、本人が意図せずに使われることのないように管理しなければならない。

(6)　職員は、主体認証情報格納装置を紛失しないよう管理し、権限のない者に付与し、又は貸与してはならない。また、紛失した場合には、システムセキュリティ責任者が定めた手続により、直ちにその旨を報告しなければならない。

(7)　職員は、主体認証情報格納装置を利用する必要がなくなったときは、システムセキュリティ責任者又は当該システムの運用要領等に定められた担当部署に返納しなければならない。

(8)　職員は、他の者からアクセスさせる必要がない管理対象情報については、アクセスできないよう設定しなければならない。

(9)　職員は、公費整備された携帯電話機（以下「公費整備携帯電話機」という。）について、送受信メール、電話帳等の情報のうち、要機密情報に当たるものを閲覧するときは、主体認証情報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。

4　電子メール及びウェブ

(1)　職員は、管理対象情報を含む電子メールを送受信する場合には、警察の運営又は業務委託に係る電子メール機能又は公費整備携帯電話機の電子メール機能を利用しなければならない。

(2)　職員は、多数の者に電子メールを一斉送信するときは、Ｂｃｃ（Blind carb on copy）等の機能を用いて、受信者のメールアドレスが漏えいすることのないようにしなければならない。ただし、受信者同士でメールアドレス情報を共有する必要がある場合又はメールアドレス情報が共有されている場合は、この限りではない。

(3)　職員は、機密性２（中）情報を電子メールにより部外に送信する場合には、当該情報に主体認証情報を設定し、又は暗号化しなければならない。

(4)　職員は、機密性３（高）情報を外部回線を用いた電子メールにより送信してはならない。

(5)　職員は、機密性２（中）情報を電子メールにより部外に送信したときは、やむを得ない場合を除き、送信後直ちに端末に内蔵された電磁的記録媒体から当該情報を消去しなければならない。

(6)　職員は、要機密情報を電子メールにより部外から受信したときは、当該情報を外部回線に接続された端末に内蔵された電磁的記録媒体に保存してはならない。ただし、やむを得ず一時的に保存したときは、外部記録媒体を用いて外部回線と接続されていない端末に取り込むなどして、当該情報を可能な限り速やかに削除しなければならない。

(7)　職員は、不審な電子メールを受信したときは、開封せずにシステム管理担当者に連絡しなければならない。

(8)　職員は、閲覧しているウェブサイトに表示されるフォームに機密性２（中）情報を入力して送信する場合は、次に掲げる事項を確認しなければならない。

ア　送信内容が暗号化されること。

イ　当該ウェブサイトが送信先として想定している組織のものであること。

(9)　職員は、アプリケーション・コンテンツを告知する場合には、当該アプリケーション・コンテンツに係るＵＲＬ（短縮ＵＲＬを除く。以下同じ。）等を表示して直接的に誘導する方法により行うことを原則とし、検索サイトで検索するための指定の用語を表示する等間接的に誘導する方法により行う場合においても、当該アプリケーション・コンテンツに係るＵＲＬ等を一体的に表示しなければならない。

(10)　前記(9)の場合において、告知するアプリケーション・コンテンツが部外の者が提供するものであるときは、表示するＵＲＬ等の有効性を保つため、次に掲げる措置をとらなければならない。

ア　告知するアプリケーション・コンテンツを管理する組織名を明記すること。

イ　告知するアプリケーション・コンテンツの所在場所の有効性を確認した時

期又は有効性を保証する期間を明記すること。

(11) 職員は、前記(9)の規定による告知を行う場合において、ＵＲＬを二次元コード等に変換して表示するときは、告知するアプリケーション・コンテンツの内容を併せて表示する等の方法により当該二次元コード等による誘導先を明らかにしておかなければならない。

5　機器の取扱い

(1)　機器の管理

職員は、警察情報システムを構成する機器について、各システムセキュリティ責任者が定めるところにより、適正に管理しなければならない。

(2)　機器の紛失防止

職員は、物理的に持ち出しが困難であるもの及びセキュリティワイヤーの取り付けられたものを除き、全ての電子計算機を鍵のかかる保管庫に保管するなどして、紛失又は盗難がないよう適正に管理しなければならない。

(3)　可用性への配慮

職員は、電子計算機又はネットワーク機器の取扱いに当たっては、設置環境を踏まえ、障害等により可用性を損なわないよう配慮しなければならない。

(4)　機器の持ち出し

職員は、警察情報システムを構成する機器を警察の庁舎外に持ち出す必要がある場合には、総務部長が別に定める手続により許可を得なければならない。

第５　公費整備携帯電話機の取扱いに係る特例

１　公費整備携帯電話機の取扱いについては、第４に定めるもののほか、次に定めるところによる。

(1)　公費整備携帯電話機の管理については、システムセキュリティ責任者が定める場合を除くほか、総務部長が定めるところによる。

(2)　職員は、第４の５の(4)の規定にかかわらず、公費整備携帯電話機に記録する要機密情報を必要最小限にした上で、公費整備携帯電話機を警察の庁舎外に持ち出すことができる。ただし、共用で利用する公費整備携帯電話機（音声通話機能のみを使用するものを除く。）については、総務部長が別に定める手続により許可を得なければならない。

２　前記１のほか､公費整備携帯電話機の取扱いに係る特例の細目事項については、総務部長が別に定める。

第６　外部記録媒体の取扱い

１　外部記録媒体の管理

職員は、外部記録媒体について、総務部長が別に定める方法により、適正に管理しなければならない。

２　外部記録媒体の持ち出し

職員は、外部記録媒体を警察の庁舎外に持ち出す必要がある場合には、外部記録媒体内の要機密情報を必要最小限にするとともに、総務部長が別に定める手続により許可を得なければならない。

３　外部記録媒体の利用

(1)　部外から受領した外部記録媒体の利用

職員は、警察活動に伴い部外から受領した外部記録媒体又は部外の電子計算機に接続して利用した本県警察の整備による外部記録媒体を電子計算機に接続するときは、安全な方法によって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。

(2)　外部記録媒体の利用の申請

ア　職員は、外部記録媒体を電子計算機に接続するときは、平文・暗号文の別、目的及び外部記録媒体を接続する電子計算機を明らかにした上で、媒体利用管理者に申請しなければならない。

イ　職員は、外部記録媒体に管理対象情報を出力する際の平文・暗号文の別について、総務部長が別に定めるところにより、選択しなければならない。ただし、外部記録媒体の利用が技術的に制限されていない場合は、この限りでない。

(3)　外部記録媒体の利用の許可

前記(2)のアの規定による申請を受けた媒体利用管理者は、必要最小限の範囲で当該利用の申請を許可しなければならない。

(4)　管理対象情報の削除

職員は、外部記録媒体の利用が終了したときは、業務上必要がある管理対象情報を電子計算機に取り込んだ後、直ちに当該外部記録媒体から管理対象情報を削除しなければならない。

4　外部記録媒体の利用状況の検証

(1)　利用の証跡の検証

媒体利用管理者は、システムセキュリティ責任者が策定する運用要領等に基づき、職員が外部記録媒体を用いて入出力したファイル名及びファイルサイズに係る証跡を定期的に確認しなければならない。

(2)　許可の証跡の検証

媒体利用管理者は、前記３の(3)に係る許可について、定期的に確認を受けなければならない。

(3)　検証結果の保存

職員は、前記(1)及び(2)の規定による確認の結果について、総務部長が別に定めるところにより保存しなければならない。

5　外部記録媒体の廃棄

職員は、要機密情報を取り扱った外部記録媒体を廃棄する場合には、裁断、データの消去、暗号化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。

第７　外部サービスの取扱い等

1　外部サービスの取扱い

職員は、業務で外部サービスを利用しようとする場合には、総務部長が別に定める手続により申請を行わなければならない。ただし、検索サービスその他の外部サービスによりインターネット上の情報を閲覧する場合（アカウントの取得を必要としないときに限る。）はこの限りではない。

2　管理対象情報の取扱い

外部サービスのうち、次に掲げるものを利用する場合における管理対象情報の取扱いは、それぞれに定めるところによるものとする。

(1)　クラウドサービス　機密性３（高）情報を取り扱ってはならない。ただし、情報セキュリティ管理者が必要と認める場合はこの限りでない。

(2)　約款、規約等による外部サービス　要機密情報を取り扱ってはならない。ただし、情報セキュリティ管理者が必要と認める場合はこの限りでない。

3　外部サービスを利用する際の留意事項

職員は、インターネット上の情報の閲覧その他の外部サービスの利用をすると

きは、検索する情報が当該外部サービスの提供側において収集、分析され関心事項が把握される可能性があることに留意しなければならない。

第８　個人所有の機器の取扱い

職員は、総務部長が別に定める場合を除き、個人所有の機器において管理対象情報を処理してはならない。

第９　自己点検

職員は、情報セキュリティ管理者の指示により、情報セキュリティに関する事項について、自己点検を実施しなければならない。

第10　緊急事態に係る特例

職員は、大規模災害、重大テロ等の緊急事態であって、この通達に定める規定を遵守することが困難なときは、運用管理者等の指示により、これらの規定によらずに管理対象情報を処理することができる。