警情甲達第６号
平成３０年４月２３日
（改正　令和４年３月１８日
警務甲達第１２号）

各部、課、隊、所、校、署長　　殿

福井県警察本部長

福井県警察情報システム等及び管理対象情報の取扱要領の制定について

福井県警察における情報の取扱については、福井県警察情報システム等における情報の取扱要領の制定について（平成２６年警情甲達第１６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、警察情報セキュリティポリシーの体系を見直すことに伴い、福井県警察における警察情報セキュリティに関する訓令（平成１９年福井県警察本部訓令第３号）第１４条に基づき、別添のとおり「福井県警察情報システム等及び管理対象情報の取扱要領」を制定し、平成３０年５月１日から実施することとしたので、事務処理上誤りのないようにされたい。

なお、旧通達は、平成３０年４月３０日をもって廃止する。

別添

福井県警察情報システム等及び管理対象情報の取扱要領

第１　総則

１　目的

この要領は、福井県警察における警察情報セキュリティに関する訓令（平成１９年福井県警察本部訓令第３号。以下「訓令」という。）第１４条の規定に基づき、福井県警察情報システム等（以下「警察情報システム」という。）及び管理対象情報を取り扱う際に情報セキュリティ上遵守すべき事項を定めることを目的とする。

２　用語の定義

この要領における用語の意義は、訓令及び福井県警察における情報セキュリティに係る管理体制の制定について（平成３０年警情甲達第４号。以下「管理体制通達」という。）に定めるところによる。

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

警察職員は、管理対象情報を作成し、又は警察職員以外の者から入手したときは、当該情報の分類及び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

警察職員は、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不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である場合を除き、部内の警部相当職（警部以上の階級にある者（同相当職を含む。）をいう。以下同じ。）（夜間・休日にあっては当直責任者を含む。）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

(1)　警察職員は、部内においては、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場合を除き、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。

(2)　警察職員は、警察職員以外の者に管理対象情報を提供する場合には、（３）に掲げるものを除き、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。

(3)　管理対象情報の機密性の分類及び取扱制限の明示を必要としないものについて、次のとおり定める。

ア　特定秘密又は秘密文書に関する規程に基づき、特定秘密又は秘密文書である旨が表示されているもの

イ　「捜査資料の管理の徹底について」（平成１９年刑捜一甲達第３３号）の１に定義されている「捜査資料」及び証拠物件

ウ　個別の法令又は規程等により様式等の定めがあり、その取扱いが明らかであるもの

エ　イ及びウに掲げるもののほか、管理対象情報の機密性の分類及び取扱制限を明示することが不適当なものとして、運用管理者が認めたもの

オ　広報資料、ウェブサイト掲載資料その他の公開する情報であって、その取扱いが

明らかであるもの

(4)　警察職員は、（３）に掲げる管理対象情報の機密性の分類及び取扱制限を明示する必要がないものであっても、当該管理対象情報の機密性の分類及び取扱制限に応じて、ファイル名や当該ファイルを添付したメールの件名・本文中に取扱上の留意事項を記載するなどの方法により、当該管理対象情報が提供先においても適切に取り扱われるよう努めなければならない。

４　管理対象情報の分類及び取扱制限の継承

警察職員は、管理対象情報を作成し、又は複製する際に、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

警察職員は、修正、追加、削除その他の理由により、管理対象情報の分類及び取扱制限を見直す必要がある場合には、管理対象情報の分類及び取扱制限の決定者等に確認し、その結果に基づき見直さなければならない。

第３　管理対象情報の取扱い

管理対象情報の取扱いについては、文書管理規程、個人情報保護に関する規程等別に定める規程による適正な管理を行うほか、本項目に定めるところにより行うものとする。

１　管理対象情報の利用

(1)　警察職員は、管理対象情報を不正に作成し、又は入手してはならない。

(2)　警察職員は、管理対象情報を不正に利用し、又は毀損してはならない。

(3)　警察職員は、要保護情報を放置してはならない。

(4)　警察職員は、要機密情報を必要以上に配布してはならない。

(5)　警察職員は、要機密情報を必要以上に複製してはならない。

２　管理対象情報の提供・運搬

(1)　警察職員は、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）に分類されることを確認しなければならない。

(2)　警察職員は、管理対象情報を警察職員以外の者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)　警察職員（運用管理者以上の職位の者を除く。）は、機密性２（中）情報について、閲覧可能な範囲外の者への提供又は警察庁舎外への持ち出しを行う場合には、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、警部相当職又は当直責任者に報告（口頭による報告を含む。以下同じ。）しなければならない。

(4)　警察職員（運用管理者以上の職位の者を除く。）は、機密性３（高）情報について、閲覧可能な範囲外の者への提供又は警察庁舎外への持ち出しを行う場合には、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、次の手続により許可を得なければならない。

ア　警察職員（運用管理者以上の職位の者を除く。）は、イに定める場合を除き、機密性３（高）情報を閲覧可能な範囲外の者へ提供し、又は警察庁舎外へ持ち出すときは、当該機密性３（高）情報を識別できる事項（文書記号、管理番号、件名

等)、提供日又は持ち出し期間及び目的を記録した上で、運用管理者の許可を得なければならない。

イ　警察職員（運用管理者以上の職位の者を除く。）は、運用管理者が不在時に職務上緊急に機密性３（高）情報を提供し、又は持ち出す必要がある場合には、運用管理者があらかじめ指名した当該管理者の職責を代行する警視（同相当職を含む。）以上の者の許可を得なければならない。

(5)　警察職員は、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執らなければならない。

(6)　警察職員は、要保護情報が記録され、又は記載された記録媒体の警察庁舎外への運搬を第三者へ依頼する場合には、必要に応じて受領印が必要となる書留郵便や、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。

３　管理対象情報の保存

(1)　警察の庁舎外に設置されている機器への要機密情報の保存

ア　警察職員は、イの場合を除き、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。

イ　警察職員は、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する必要がある場合には、事件主管課長が情報セキュリティ管理者及びシステムセキュリティ責任者と協議して別に定めるところにより、当該機器に保存することができるものとする。

(2)　警察職員は、外部との電子メールの送受信等、要機密情報の取扱い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)　警察職員は、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)　警察職員は、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。

４　管理対象情報の廃棄

(1)　警察職員は、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、速やかに当該管理対象情報を消去しなければならない。

(2)　警察職員は、電磁的記録媒体を廃棄する場合には、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なければならない。

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

５　管理対象情報を取り扱う区域における対策

警察職員は、利用する区域について区域情報セキュリティ管理者が定めた対策に従って利用しなければならない。また、警察職員以外の者を立ち入らせるときには、当

該警察職員以外の者にも当該区域で定められた対策に従って利用さ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)　警察職員は、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、システムセキュリティ責任者が定めた当該警察情報システムにおいて取り扱うことのできる機密性、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)　警察職員は、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、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)　警察職員は、定められた目的以外の目的で警察情報システムを不正に使用してはならない。

(4)　警察職員は、管理体制通達第３の３（１０）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、ソフトウェア追加等）をしてはならない。

(5)　警察職員は、警察情報システムで利用される電気通信回線に、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)　警察職員は、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執らなければならない。

(7)　警察職員は、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)　警察職員は、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、電子署名により当該ソフトウェアの配布元を確認しなければならない（電子署名が付与されていないものを除く。）。

(9)　警察職員は、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)　警察職員は、外部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外部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)　警察職員は、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、次に掲げる措置を執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。

イ　安全性が確実でないソフトウェアをダウンロードし、又は実行しない。

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。

２　事案発生時の措置

警察職員は、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、福井県警察情報システム等における情報セキュリティインシデント対処要領の制定について（平成３０年警情甲達第９号。以下「インシデント通達」という。）に定める方法により、担当部署に連絡しなければならない。

３　アクセス制御

(1)　警察職員は、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)　警察職員は、自己に付与されたユーザＩＤを適切に管理するため、次に掲げる措置を執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。

イ　他者が主体認証に用いるために付与し、又は貸与しない。

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。

(3)　警察職員は、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)　警察職員は、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。

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。

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の共通の組合せを用いない（シングルサインオンの場合を除く。）。

エ　ユーザＩＤ及び主体認証情報を他の警察職員と共用している場合であって、当該他の警察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場合には、当該主体認証情報を速やかに変更する。

(5)　警察職員は、ＩＣカード等の主体認証情報格納装置による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)　警察職員は、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、定められた手続に基づき、直ちにその旨を報告しなければならない。

(7)　警察職員は、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、別に定めがある場合を除き、システムセキュリティ責任者に返納しなければならない。

(8)　警察職員は、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)　警察職員は、支給又は貸与された携帯電話機（以下「支給携帯電話機」という。）について、送受信メール履歴、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場合には、主体認証情報入力等の主体認証を求められるよう設定しなければならない。

４　外部回線による電子メール及びウェブ

(1)　警察職員は、管理対象情報を含む電子メールを送受信する場合には、警察が管理

し、運用（外部委託による場合を含む。）する電子メール機能又は支給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)　警察職員は、多数の者に電子メールを一斉送信するときは、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を除き、Ｂｃｃ（ブラインド・カーボン・コピー）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。

(3)　警察職員は、機密性２（中）情報を電子メールにより外部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)　警察職員は、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)　警察職員は、要機密情報を電子メールにより外部に送信したときは、やむを得ない場合を除き、送信後直ちに端末に内蔵の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)　警察職員は、要機密情報を電子メールにより外部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の電磁的記録媒体に保存してはならない。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、可能な限り速やかに削除しなければならない。

(7)　警察職員は、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)　警察職員は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、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。

5　機器の取扱い

(1)　機器の管理

警察職員は、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。

(2)　可用性への配慮

警察職員は、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。

(3)　モバイル端末の持ち出し

ア　持ち出し時の手続

警察職員は、モバイル端末を警察庁舎外に持ち出すときは、内蔵された電磁的記録媒体の要機密情報を必要最小限にするとともに、外部記録媒体・端末等持ち出し簿（別記様式第１号）に持ち出し期間、目的等を記載し、警部相当職又は当直責任者の許可を得なければならない。

イ　持ち出し終了時の手続

警察職員は、モバイル端末の持ち出しが終了したときは、外部記録媒体・端末等持ち出し簿に持ち出し終了日を記載し、持ち出し時に許可を与えた者から紛失

のない旨の確認を受けなければならない。

(4)　モバイル端末等以外の機器の持ち出し

ア　警察職員は、次に掲げる場合を除き、モバイル端末及び支給携帯電話機（以下「モバイル端末等」という。）以外の機器を警察の庁舎外に持ち出してはならない。

(ｱ)　機器の内部に要機密情報が保存されていないことを警部相当職が確認した場合

(ｲ)　修理、廃棄、保管場所変更、保守作業等のためであって、警察職員が運搬し、常に警察職員の管理下にある場合

(ｳ)　（ア）及び（イ）に掲げるもののほか、やむを得ない事情があるとして、システムセキュリティ責任者の許可を得た場合

イ　警察職員は、ア（ア）からア（ウ）までの場合においてモバイル端末等以外の機器を持ち出すときは、システム管理担当者の許可を得るとともに、必要最小限の情報を残して機器内の要機密情報を削除し、外部記録媒体・端末等持ち出し簿に持ち出し期間、目的等を記載した上で警部相当職の許可を得なければならない。

ウ　警察職員は、モバイル端末等以外の機器を運搬業者に運搬させるときは、システムセキュリティ責任者の許可を得るとともに、保秘に関する取決めを行わなければならない。

エ　持ち出し終了時の手続

警察職員は、持ち出しが終了したときは、外部記録媒体・端末等持ち出し簿に持ち出し終了日を記載し、持ち出し時に許可を与えた者から紛失のない旨の確認を受けなければならない。

オ　警察職員は､持ち出しを前提として整備された特定用途機器を持ち出すときは、モバイル端末の持ち出し時の手続に準拠した手続で持ち出すことができる。

(5)　完全性及び可用性の確保

ア　警察職員は、要保全情報又は要安定情報が保存された機器を庁舎外に持ち出すときは、運用管理者の許可を得るとともに、必要に応じてバックアップを取得しなければならない。

イ　警察職員は、要安定情報が保存された機器を運搬するときは、運搬中の滅失、紛失等を防止するため、必要に応じて、同一の情報を異なる経路手段で運搬するなど適切な措置を執らなければならない。

(6)　外部記録媒体・端末等持ち出し簿の確認

警察職員は、外部記録媒体・端末等持ち出し簿について月に１回以上運用管理者の確認を受けなければならない。

(7)　外部記録媒体・端末等持ち出し管理システムの利用

外部記録媒体・端末等持ち出し管理システムで機器の持ち出し許可を得たものについては、当該システムで確認を受けるものとし、外部記録媒体・端末等持ち出し簿への記載を省略することができる。

第５　支給携帯電話機の取扱い

１　支給携帯電話機の管理

警察職員は、支給携帯電話機について、次のとおり適正に管理しなければならない。

(1)　運用管理者は、次のアからキに掲げる事項を記載した支給携帯電話機管理簿（別記様式第２号）を作成し、第８に定める期間、保管しなければならない。また、当該管理簿は支給携帯電話機の増減のあった都度、変更のないときも年１回以上、更新しなければならない。

ア　支給携帯電話機の管理番号

イ　支給携帯電話機の電話番号

ウ　支給携帯電話機を支給する警察職員の役職及び氏名（複数の警察職員が共用する支給携帯電話機（以下「共用支給携帯電話機」という。）にあっては、共用支給携帯電話機を管理する警察職員の役職及び氏名）

エ　支給携帯電話機で使用するメールアドレス（電子メール機能を使用するものに限る。）

オ　支給携帯電話機の機種

カ　使用開始日及び使用終了日

キ　その他所要の事項

(2)　警察職員は、支給携帯電話機について、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)　共用支給携帯電話機を管理する警察職員は、警部相当職以上の警察職員とする。ただし、やむを得ない事情がある場合は、この限りでない。

(4)　共用支給携帯電話機を管理する警察職員は、共用支給携帯電話機を使用しない場合は、鍵のかかる保管庫に保管するなどしなければならない。また、可能な限り集中保管しなければならない。

(5)　支給携帯電話機を管理する警察職員は、月に１回以上、支給携帯電話機の所在を点検するとともに、点検結果を外部記録媒体等点検簿として、第７に定める期間、保管しなければならない。ただし、クラス３に分類された区域内で鍵のかかる保管庫に保管されている場合は、年に１回の点検で足りることとする。

２　支給携帯電話機の使用

警察職員による支給携帯電話機の使用については、次のとおり定める。

(1)　警察職員は、職務上必要がある場合は、支給携帯電話機の音声通話機能、電子メール機能、写真撮影機能等を使用することができる。

(2)　警察職員は、支給携帯電話機において外部回線を用いた電子メール機能を使用する場合は、情報の暗号化、符丁の活用等の情報漏えい対策を講じなければならない。

(3)　警察職員は、支給携帯電話機の電子メール機能を使用する場合は、可能な限りグループ機能を使用するなど、情報の誤送信を防止するための対策を講じなければならない。

(4)　警察職員は、支給携帯電話機に保存された管理対象情報を電子計算機に取り込む必要がある場合は、部内の上級の警察職員であって、警部相当職以上の者に報告（口頭による報告を含む。）した上で、不正プログラムが侵入しないよう安全な方法で当該管理対象情報を電子計算機に取り込んだ後、速やかに支給携帯電話機本体から管理対象情報を削除しなければならない。

３　支給携帯電話機の持ち出し

警察職員は、支給携帯電話機内の要機密情報を必要最小限にした上で、支給携帯電話機の警察の庁舎外への持ち出しを行うことができる。ただし、共用支給携帯電話機（音声通話機能のみを使用するものを除く。）については、次に定める手続により許可を得なければならない。

(1)　持ち出し時の手続

警察職員は、共用支給携帯電話機を警察の庁舎外に持ち出す場合は、あらかじめ、外部記録媒体・端末等持ち出し簿に、共用支給携帯電話機の管理番号、使用者及び目的を記載し、部内の上級の警察職員であって、警部相当職以上の者（夜間・休日にあっては当直責任者を含む。（２）において同じ。）の許可を得なければならない。

(2)　持ち出し終了時の手続

警察職員は、共用支給携帯電話機の持ち出しが終了した場合は、外部記録媒体・端末等持ち出し簿に持ち出し終了日を記載し、警部相当職以上の者から持ち出し終了の確認を受けなければならない。

(3)　外部記録媒体・端末等持ち出し簿の確認

媒体利用管理者は、外部記録媒体・端末等持ち出し簿について、月に１回以上運用管理者の確認を受けなければならない。

第６　外部記録媒体の取扱い

１　外部記録媒体の管理

(1)　運用管理者は、外部記録媒体の管理番号、媒体の種別、利用目的、媒体利用管理者、使用開始日及び使用終了日を記載した外部記録媒体管理簿（別記様式第３号）を作成しなければならない。また、当該管理簿について、外部記録媒体の増減のあった都度、変更のないときも年１回以上、確認しなければならない。

なお、外部記録媒体管理システムに登録されたものについては、外部記録媒体管理簿への記載を省略することができる。また、他の規程に基づき適切に管理されている外部記録媒体についても同様とする。

(2)　媒体利用管理者は、外部記録媒体を利用しないときは、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)　警察職員は、可能な限り外部記録媒体を集中保管しなければならない。

(4)　媒体利用管理者は、月に１回以上、外部記録媒体等点検簿（別記様式第４号）により外部記録媒体等の所在を点検しなければならない。

なお､クラス３に分類された区域内で鍵のかかる保管庫に保管されている場合は、年に１回の点検で足りることとする。

(5)　デジタルカメラ、ボイスレコーダ等、情報を記録でき、電子計算機に接続して情報を入出力することができる機器は、外部記録媒体とみなす。ただし、規定上、警察情報システムに接続することを禁止したもの及び内蔵された電磁的記録媒体に管理対象情報を保存することを禁止したものについては、この限りでない。

(6)　次に掲げる外部記録媒体については、（１）から（４）までの規定は、適用しない。

ア　未使用のもの

イ　一度情報が書き込まれ、これ以上の情報の書き込みが技術的に不可能なもので

あって、内部に記録された管理対象情報が機密性１（低）情報のもの

２　外部記録媒体の持ち出し

警察職員は、外部記録媒体を警察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、次の手続により許可を得なければならない。

(1)　持ち出し時の手続

警察職員は、外部記録媒体を持ち出すときは、外部記録媒体・端末等持ち出し簿に持ち出し期間、目的等を記載し、媒体利用管理者又は当直責任者の許可を得なければならない。

このとき、外部記録媒体に機密性３（高）情報が含まれる場合には、第３の２（４）の規定に基づき、運用管理者の許可を得なければならない。ただし、第６の１（５）に掲げる外部記録媒体については、次に掲げる事項を全て満たしている場合に限り、持ち出し時の許可を不要とすることができる。

ア　管理対象情報が記録されていない外部記録媒体の持ち出しであること。

イ　持ち出したその日のうちに持ち出しが終了する見込みであること。

ウ　外部記録媒体・端末等持ち出し簿への記載内容について媒体利用管理者が指名する当該任務を代行する警部補（同相当職を含む。）の者から確認を受けていること。

エ　媒体利用管理者が、少なくとも１日のうちに１回は、持ち出した外部記録媒体の管理状況を目視により確認すること。

(2)　デジタルカメラの持ち出しの特例

警察職員は、（１）の規定にかかわらず、次に掲げる場合は、外部記録媒体・端末等持ち出し簿への記載を省略することができる。ただし、「画像ファイル媒体の活用要領の制定について」（平成２８年刑鑑甲達第１号）に規定するものを除く。

ア　あらかじめ外部記録媒体管理簿においてデジタルカメラ（当該デジタルカメラで使用する外部記録媒体を含む。以下同じ。）を持ち出す警察職員が一に指定されている場合であって、当該警察職員が当該デジタルカメラを持ち出すとき。ただし、持ち出したその日のうちに持ち出しが終了する見込みである場合に限り、持ち出し中に、その日のうちに持ち出しが終了しないことが判明した場合には、当該持ち出しについて、（１）に規定する手続を執らなければならない。また、当該デジタルカメラは、使用しない場合は、媒体利用管理者が鍵のかかる保管庫において集中管理し、さらに、媒体利用管理者が、少なくとも１日のうち１回は、当該デジタルカメラの管理状況を目視により確認しなければならない。

イ　当直勤務に従事する警察職員が、当直勤務用として指定されたデジタルカメラを持ち出す場合。この場合において、当該デジタルカメラは、原則として、当直勤務を取りまとめる所属（警察署にあっては課）において管理するものとする。また、当直責任者は、当直勤務において当該デジタルカメラを使用する者を指名するとともに、当直勤務の終了後の報告時に、併せて当該デジタルカメラを返却しなければならない。

ウ　交番における交代制勤務に従事する警察職員が、交番勤務用として指定された

デジタルカメラを持ち出す場合。この場合において、媒体利用管理者は、交番の巡視等に合わせて当該デジタルカメラの管理状況を確認しなければならない。

(3)　警察以外の機関の電子計算機への接続

警察職員は、外部記録媒体を警察以外の機関の電子計算機に接続する予定があるときは、持ち出す前に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。

(4)　持ち出し終了時の手続

外部記録媒体の持ち出しが終了したときは、職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、速やか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。また、外部記録媒体・端末等持ち出し簿に持ち出し終了日を記載し、持ち出し時に許可を与えた媒体利用管理者から紛失のない旨の確認を受けなければならない。

(5)　外部記録媒体・端末等持ち出し簿の確認

媒体利用管理者は、外部記録媒体・端末等持ち出し簿について、月に１回以上運用管理者の確認を受けなければならない。

(6)　外部記録媒体・端末等持ち出し管理システムの利用

外部記録媒体・端末等持ち出し管理システムで外部記録媒体の持ち出し許可を得たものについては、当該システムで確認を受けるものとし、外部記録媒体・端末等持ち出し簿への記載を省略することができる。

３　外部記録媒体の利用

(1)　外部から受領した外部記録媒体の利用

警察職員は、外部から受領した外部記録媒体又は外部の電子計算機に接続して利用した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

警察職員は、外部記録媒体を電子計算機に接続する際には、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た上で利用しなければならない。また、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は、（３）アからウまでの中から、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には、この限りでない。

(3)　平文・暗号文の区別

ア　警察職員は、管理対象情報を外部記録媒体に出力するときは、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化機能を用いなければならない。

イ　警察職員は、暗号化を行う電子計算機と復号を行う電子計算機とで同一の暗号化ソフトウェアが導入されていないときは、アの規定にかかわらず、自己復号型暗号化機能を用いることができる。

ウ　警察職員は、次に掲げる場合は、ア及びイの規定にかかわらず、平文で出力することができる。

(ｱ)　機密性１（低）情報を出力するとき。
(ｲ)　電子計算機に暗号化機能が設けられていないとき。
(ｳ)　一の電子計算機に保存された管理対象情報を、同一の庁舎内に設置された他の電子計算機に移すために出力するとき。

(4)　外部記録媒体の利用の許可

（２）に係る申請を受けた媒体利用管理者は、必要最小限の範囲で許可しなければならない。

(5)　管理対象情報の削除

警察職員は、外部記録媒体の利用が終了したときは、職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、速やか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、警察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。ただし、システムセキュリティ責任者は、次に掲げる事項を全て満たしていることについて情報セキュリティ管理者の確認を受けた場合には、入力に係る証跡の確認を不要とすることができる。

なお、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化機能を利用して入出力したファイルについては、証跡の確認を要しない。

ア　ウイルス対策ソフトウェアが適切に導入されているとともに、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できる環境を整えていること。

イ　次の（ア）及び（イ）を全て満たしていること。光ディスクに限っては、（ア）又は（イ）のいずれかを満たしていること。

(ｱ)　警察情報システムに未登録の外部記録媒体は、その種類によらず、媒体利用管理者の許可がなければ利用できないよう技術的措置が執られていること。

(ｲ)　入力に係る証跡を抽出し、検証が行えること。

ウ　外部記録媒体の自宅への持ち帰り防止対策等、外部記録媒体によって本来の目的以外の情報が入出力されることを防ぐための対策が講じられていること。

(2)　許可の証跡の検証

媒体利用管理者は、３（４）に係る許可について、定期的に上司による確認を受けなければならない。

(3)　警察職員は、（１）及び（２）の検証結果について、保存しなければならない。

５　外部記録媒体の廃棄

警察職員は、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、情報の抹消を実施しなければならない。

第７　約款による外部サービスの取扱い

１　共通事項

(1)　警察職員は、職務上約款による外部サービスを利用してはならない。ただし、検

索サービスその他の約款による外部サービスによりインターネット上に掲出された情報を閲覧する場合（アカウントの取得を必要としない場合に限る。）及び次の２から４までの利用の場合はこの限りではない。

(2)　警察職員は、（１）における情報の閲覧の場合であっても、検索する情報が当該約款による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。

(3)　警察職員は、個人所有の機器により、職務上約款による外部サービスを利用してはならない。

２　広報における利用

(1)　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、利用する警察職員の上級の警察職員であって警部相当職以上の者（以下「利用責任者」という。）が、利用しようとするサービスの約款その他の提供条件等から、利用のリスクが許容できることを確認した上で、次の事項を明らかにして運用管理者に申請を行わなければならない。

ア　利用する約款による外部サービス

イ　利用目的

ウ　約款による外部サービスの利用規約内容

エ　取得するアカウント及び主体認証情報

オ　利用する警察職員及び電子計算機

カ　利用期間

(2)　（１）の申請を受けた運用管理者は、利用を許可する場合には、情報セキュリティ管理者及びシステムセキュリティ責任者と協議の上、講ずべき対策を定めなければならない。

(3)　警察職員は、申請した約款による外部サービスの利用が許可された場合には、運用管理者から指示された対策を講じなければならない。

(4)　利用責任者は、アカウントの利用状況を適切に管理しなければならない。

(5)　利用責任者は、（１）のイからカまでに掲げる事項に変更が生じた場合には、運用管理者に届出を行わなければならない。ただし、利用する電子計算機を他の警察情報システムに変更する場合には、（１）の申請を行わなければならない。

(6)　（５）の届出を受けた運用管理者は、当該届出の内容を速やかに情報セキュリティ管理者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。

(7)　利用責任者は、不要なアカウントが生じた場合には、当該アカウントを速やかに削除するとともに、運用管理者にその旨を届け出なければならない。

(8)　警察職員は、不正アクセス等を防止するため、主体認証情報や主体認証方法を適切に運用管理しなければならない。

(9)　警察職員は、なりすましや不正アクセスを確認した場合には、速やかにインシデント通達に定める方法により、担当部署に連絡しなければならない。

(10)　警察職員は、許可された約款による外部サービスにおいて、要機密情報を取り扱ってはならない。

(11)　警察職員は、許可された約款による外部サービスにおいて、要安定情報を取り扱

う場合には、自組織のウェブサイト等に当該要安定情報を掲載して参照可能としなければならない。

(12)　利用責任者は、発信する情報が自組織のものであることを明らかにするため、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講じなければならない。

3　犯罪捜査における利用

警察職員は、犯罪捜査において約款による外部サービスを利用する特段の必要がある場合には、当該事務を所掌する本部所属の長が情報セキュリティ管理者と協議して別に定めるところにより、利用することができるものとする。

4　その他の場合における利用

警察職員は、２及び３に定めるもののほか、職務上約款による外部サービスを利用する特段の必要がある場合には、運用管理者に申請を行うものとする。この場合において、２（１）から２（１０）までの規定を適用するものとする。

第８　簿冊の保管期間

各簿冊の最低保管期間については、会計年度で次のとおり定める。

なお、各簿冊を電磁的記録により管理することを妨げない。

１　外部記録媒体・端末等持ち出し簿　５年

２　支給携帯電話機管理簿　５年

３　外部記録媒体管理簿　５年

４　外部記録媒体等点検簿　１年未満

５　確認証跡簿　１年未満

６　外部記録媒体利用簿　５年

（ただし、外部記録媒体利用簿は、福井県警察情報システム等の情報セキュリティ要件に係る細目の制定について（平成３０年警情甲達第８号。以下「セキュリティ細目」という。）第１９に定める経過措置を適用する場合のみ作成する必要がある。）

第９　個人所有の機器の取扱い

１　警察職員は、情報セキュリティ管理者が別に定める場合を除き、管理対象情報を個人所有の機器及び外部記録媒体において処理してはならない。

２　警察職員は、個人所有の機器及び外部記録媒体を警察情報システムに接続してはならない。

３　個人所有の端末に係る特例

警察職員は、テレワーク（自宅（警察職員が自ら居住するための住宅であり、警察職員の生活の本拠となっているものをいう。）でモバイル端末等の機器等を利用して勤務することをいう。以下同じ。）を実施するため、セキュリティ細目第１１の５（１）から（３）に掲げる機能（警察が整備したものに限る。）を用いて、個人所有の機器を使用することができる。ただし、テレワークの実施に関し定められた手続を執らなければならない。

４　細目的事項の委任

その他個人所有の機器の取扱いについては、別に定める。

第 10　教養及び自己点検

1　警察職員は、教養実施計画に従って、適切な時期に教養を受講しなければならない。

2　警察職員は、情報セキュリティ管理者から指示された自己点検の手順を用いて自己点検を実施しなければならない。

第11　その他

1　運用要領等

警察職員は、この通達に定めるもののほか、取り扱う警察情報システムについて運用要領等の別に定められた文書や指示事項があるときは、それを遵守しなければならない。

2　緊急事態に係る特例

警察職員は、大規模災害、重大テロ等の緊急事態であって、この要領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。

3　技術的措置の推奨

(1)　簿冊により管理することとされている事項その他の警察情報セキュリティポリシーに定める手続について、システム構築等の技術的措置による電子化を検討し、事務負担の軽減に努めること。

なお、手続を電子化する際は、技術的措置が警察情報セキュリティポリシーに定める手続に適合していることについて、必要に応じて情報セキュリティ管理者の確認を受けること。

(2)　技術的措置により電子化する手続は、警察情報セキュリティポリシーに定める手続と同等以上の管理水準であることについて情報セキュリティ管理者の確認を受けることにより、警察情報セキュリティポリシーによらないことができる。ただし、この場合は十分な期間をもって情報セキュリティ管理者の確認を受けること。

別記様式省略