原議保存期間	5年（令和9年3月31日まで）
有効期間	一種（令和9年3月31日まで）

庁内各局部課長
各附属機関の長
各地方機関の長　殿
各都道府県警察の長

警察庁 丙情管発第46号、丙企画発第57号
丙生企発第106号、丙刑企発第67号
丙組企発第25号、丙交企発第107号
丙備企発第164号、丙外事発第48号
丙備一発第22号

令和３年10月５日

警察庁情報通信局長
警察庁長官官房長
警察庁生活安全局長
警察庁刑事局長
警察庁交通局長
警察庁警備局長

警察情報システム及び管理対象情報の取扱いについて（通達）

警察における情報セキュリティについては、警察における情報セキュリティに関する訓令（平成15年警察庁訓令第３号）第６条第２項及び第９条の規定に基づき、「警察情報システム及び管理対象情報の取扱いについて（通達）」（平成30年９月11日付け警察庁丙情管発第45号ほか。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各種情勢の変化等を踏まえ別添のとおり「警察情報システム及び管理対象情報の取扱い」を定め、令和３年10月15日から実施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、本通達の実施に伴い、旧通達は、廃止する。

別添

警察情報システム及び管理対象情報の取扱い

第１　総則

１　目的

この文書は、警察における情報セキュリティに関する訓令（平成15年警察庁訓令第３号）第６条第２項及び第９条の規定に基づき、警察情報システム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ものとする。

２　用語の定義

この文書において、用語の意義は、「警察における情報セキュリティに係る管理体制」（令和３年10月５日付け警察庁丙情管発第45号ほか別添。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

職員は、管理対象情報を作成又は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

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、部内の上級の職員であって警部（警察庁内部部局にあっては警視）相当職以上の者（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)　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)　職員は、職員以外の者に管理対象情報を提供する場合には、警察庁情報セキュリティ管理者が別途定めるものを除き、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。

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

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)　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き損してはならない。

(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。

2　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)　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、その旨を部内の上級の職員であって、警部（警察庁内部

部局にあっては警視）相当職以上の者（夜間・休日にあっては当直責任者を含む。）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、警察庁情報セキュリティ管理者が別途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執らなければならない。

(6)　職員は、要保護情報が記録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)　職員は、警察庁情報セキュリティ管理者が別途定める場合を除き、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。

(2)　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)　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。

４　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、速やかに当該管理対象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。また、端末やサーバ等をリース契約で調達する場合は、契約終了に伴う返却時の情報の抹消方法及び履行状況の確認手段について、次に掲げる事項を例とする対策を行わなければならない。

ア　リース契約の調達仕様書に記載し、契約内容にも含める。

イ　リース契約終了に伴う情報の抹消について、役務提供契約を別途締結する。

(3)　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

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、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)　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)　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)　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)　職員は、管理体制通達第７の３(11)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)　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)　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)　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、警察庁情報セキュリティ管理者が別途定める場合を除き、警察が管理する区域以外において外部回線に接続したことのある端末を、内部ネットワークに直接接続してはならない。

(9)　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。）。

(10) 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。

(11) 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。

(12) 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

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、最高情報セキュリティ管理者が別途定める方法により、担当部署に連絡しなければならない。

3　アクセス制御

(1)　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)　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。

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職員と共用している場合であって、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場合には、当該主体認証情報を速やかに変更する。

(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)　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、支給された携帯電話機（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　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、警察が管理・運用（業務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)　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（Blind carbon 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。

(3)　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)　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、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された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)　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。

(9)　職員は、アプリケーション・コンテンツを告知する場合は、告知する対象となるアプリケーション・コンテンツに利用者が確実に誘導されるよう、ＵＲＬ等を用いて直接誘導することを原則とし、検索サイトで指定の検索語を用いて検索することを促す方法その他の間接的な誘導方法を用いる場合であっても、ＵＲＬ等と一体的に表示しなければならない。また、短縮ＵＲＬを用いてはならない。

(10)　職員は、アプリケーション・コンテンツを告知するに当たって、ＵＲＬを二次元コード等に変換して印刷物等に表示して誘導する場合には、当該コードによる誘導先を明らかにするため、アプリケーション・コンテンツの内容に係る記述を当該コードと一体的に表示しなければならない。

(11)　職員は、警察以外の者が提供するアプリケーション・コンテンツを告知する場合は、告知するＵＲＬ等の有効性を保つため、次に掲げる措置を講じなければならない。

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。

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（リンク先のＵＲＬのドメイン名の有効期限等）を確認した時期又は有効性を保証する期間について明記する。

５　機器の取扱い

(1)　機器の管理

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

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)　機器の持ち出し

機器を警察庁舎外に不正に持ち出してはならない。持ち出すときの手続等については、警察庁情報セキュリティ管理者が別途定める。

第５　支給携帯電話機の取扱い

１　支給携帯電話機の管理

職員は、支給携帯電話機について、警察庁情報セキュリティ管理者が別途定める方法により、適正に管理しなければならない。

２　支給携帯電話機の使用

職員は、警察庁情報セキュリティ管理者が別途定めるところにより、支給携帯電話機を使用することができる。

３　支給携帯電話機の持ち出し

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、共用で利用する支給携帯電話機（音声通話機能のみを使用するものを除く。）については、警察庁情報セキュリティ管理者が別途定める手続により許可を得なければならない。

４　支給携帯電話機の廃棄

職員は、要機密情報を取り扱った支給携帯電話機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、警察庁情報セキュリティ管理者が別途定める方法により、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、警察庁情報セキュリティ管理者が別途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)　外部から受領した外部記録媒体の利用

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

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、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、警察庁情報セキュリティ管理者が別途定めるところにより、選択しなければならない。

なお、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)　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。

(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、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、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)　利用の証跡の検証に係る例外

次に掲げる場合においては、ファイル名及びファイルサイズに係る証跡の確認を不要とすることができる。ただし、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、外部回線に接続されていない電子計算機から出力したファイルを外部回線に接続されている電子計算機に入力した場合は、その出力又は入力のいずれかに係る証跡を確認することとする。

ア　システムセキュリティ責任者が、次の(ｱ)から(ｳ)に掲げる事項を全て満たしていることについて警察庁情報セキュリティ管理者の確認を受けた警察情報システムにおいてファイルを入力した場合

(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)　次に掲げる事項を全て満たしていること。光ディスクに限っては、次に掲げる事項のいずれかを満たしていること。

・　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。

・　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。

イ　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ファイルを入出力した場合

(3)　許可の証跡の検証

媒体利用管理者は、３(3)に係る許可について、定期的に部内の上級の職員による確認を受けなければならない。

(4)　検証結果の保存期間

職員は、(1)及び(3)の検証結果について、証跡確認簿として警察庁情報セキュリティ管理者が別途定める期間、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、情報の抹消を実施しなければならない。

第７　外部サービスの取扱い

1　職員は、職務上外部サービスを利用しようとする場合には、警察庁情報セキュリティ管理者が別途定める手続により申請を行わなければならない。ただし、２に定める場合及び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。）はこの限りでない。

2　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する場合に限る。）には、取り扱う管理対象情報をアカウントの登録に必要な情報に限定した上で、運用管理者の許可を得なければならない。

3　職員は、１及び２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。

4　職員は、最高情報セキュリティ管理者が認めた場合を除き、クラウドサービスで機密性３（高）情報を取り扱ってはならない。

第８　個人所有の機器の取扱い

職員は、警察庁情報セキュリティ管理者が別途定める場合を除き、管理対象情報を個人所有の機器において処理してはならない。

第９　テレワーク及びモバイル勤務の取扱い

職員は、テレワーク及びモバイル勤務を実施する場合には、警察庁情報セキュリティ管理者が別途定めるところにより実施しなければならない。

第10　教養及び自己点検

1　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　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票及び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　都道府県警察が設置する情報システム（警察情報システムに該当するものを除く。）及び当該情報システムで取り扱われる情報の取扱い

都道府県警察の長が、この文書の規定に準じて対策を講ずるものとする。

2　運用要領等

職員は、この文書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途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。

3　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、この文書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。

4　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。

(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警察庁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。