

○北海道警察情報管理システム等運営要領の制定について

令和6年2月20日
道本情第6952号

／警察本部各部、所属の長／警察学校長／各方面本部長／各警察署長／宛て
みだしのことについては、「北海道警察情報管理システム運営要領の策定について」（令
3. 3. 26道本情第5852号。以下「旧通達」という。）に基づき運用してきたところであ
るが、警察共通基盤システムの運用開始に伴い、所要の見直しを行い、別添「北海道警察
情報管理システム等運営要領」を制定し、令和6年3月1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、旧通達は、同日付けで廃止する。

別添

北海道警察情報管理システム等運営要領

第1 総則

1 趣旨

この要領は、警察情報管理システム運営規程（令和3年警察本部訓令第14号。以下
「運営規程」という。）第7条及び第8条の定めに基づき、北海道警察情報管理シス
テム等（北海道警察情報管理システム、警察共通基盤システム及び警察情報管理シス
テムをいう。以下同じ。）のサービス・業務企画、設計・開発、運用・保守その他の
運営に関し、必要な事項を定めるものとする。

2 用語の定義

この要領において、次に掲げる用語の意義は、それぞれ当該各号に定めるほか、運
営規程並びに警察情報セキュリティポリシー（北海道警察情報セキュリティに関する
訓令（平成16年警察本部訓令第7号）及び当該訓令に基づいて定められた情報セキュ
リティに関する事項をいう。以下同じ。）に定めるところによる

ア 対象業務等 対象業務及び対象業務以外の北海道警察情報管理システム等を利用
して行う情報の利用及び管理に係る業務をいう。

イ 個人情報 個人に関する情報であつて、当該情報に含まれる氏名、生年月日そ
の他の記述又は個人別に付された番号、記号その他の符号により当該個人を識別
できるもの（当該情報のみでは識別できないが、他の情報と容易に照合すること
ができ、それにより当該個人を識別できるものを含む。）をいう。

ウ 入力資料 北海道警察情報管理システム等を構成するサーバ等により処理する
ことを目的として作成した文書、図画及び電磁的記録をいう。

エ 出力資料 北海道警察情報管理システム等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。

オ 個人情報入力資料 個人情報に記載され、又は個人情報が電磁的方法（電子的
方法、磁気的方法その他の人の知覚によって認識することができない方法をいう。
以下同じ。）により記録された入力資料をいう。

カ 個人情報出力資料 個人情報に記載され、又は個人情報が電磁的方法により記
録された出力資料（北海道警察の職員又は職員であつた者に係る出力資料であつ
て、専らその人事、給与若しくは福利厚生に関する事項又はこれらに準ずる事項
を記録するものを除く。）をいう。

- キ サーバ等 物理サーバ又はメインフレームをいう。
- ク 相互接続 電子計算機接続及び端末接続をいう。
- ケ システムドキュメント 北海道警察情報管理システムに関する次に掲げる文書、図画及び電磁的記録（作成中のものを含む。）をいう。
- (ア) システム仕様書
 - (イ) システム設計書
 - (ウ) プログラム仕様書
 - (エ) プログラムリスト
 - (オ) 操作指示書（システムの維持管理に伴う機器の設定方法等を説明した記録をいう。）
- コ 取扱説明書 北海道警察情報管理システム等を利用する者が対象業務等を行う上で参照する機器の操作の方法を説明した記録をいう。
- サ アクセス 北海道警察情報管理システム等にデータを入力し、又は北海道警察情報管理システム等からデータを出力することをいう。
- シ アクセス権者 アクセスを行う権限を与えられた者をいう。
- ス アクセス範囲 アクセス権者ごとにその者が行うことができるアクセスの範囲をいう。
- セ 照会 北海道警察情報管理システム等を構成するサーバ等に特定の事項が記録されているか否かに関する情報又は当該サーバ等に記録された事項の内容に関する情報を得るため、北海道警察情報管理システム等を利用することをいう。
- ソ 照会者 照会を行う者をいう

第2 準拠

北海道警察情報管理システム等のサービス・業務企画、設計・開発、運用・保守その他の運営については、警察本部長及び対象業務等に関係のある部長が別に定める場合を除き、この要領の定めるところによる。

第3 管理体制

1 システム管理者

- (1) 警察本部にシステム管理者を置き、情報管理課長をもって充てる。
- (2) システム管理者は、システム総括責任者の事務を補佐する。

2 所属における管理体制

(1) 運用管理者

ア 所属に運用管理者を置き、「北海道警察における情報セキュリティに関する対策基準について」（令5. 3. 22道本情第8100号。以下「対策基準」という。）第2の1の(1)のイの(ア)に定める運用管理者をもって充てる。

イ 運用管理者は、所属における対象業務等の実施に関し、第5の1、第8の5から7まで及び第10の2に定める事務その他の対象業務等の適正かつ円滑な実施を確保するために必要な事務を処理する。

(2) 管理責任者

ア 所属に管理責任者を置き、対策基準第2の1の(1)のウの(ア)に定める管理責任者をもって充てる。

イ 管理責任者は、運用管理者を補佐するものとする。

(3) 管理補助者

ア 所属に管理補助者を置き、対策基準第8の1の(2)のウの(ウ)に定める管理補助者

をもって充てる。

イ 管理補助者は、第5の1、第8の5から7まで及び第10の2に定める事務に関し、運用管理者を補佐するものとする。

第4 対象業務等に係る検討事項及び実施方法の策定等

1 対象業務等に係る検討事項

北海道警察情報管理システムのサービス・業務企画及び設計・開発に当たっては、対象業務等及びその周辺業務の現状把握と分析を行った上、それら業務の見直し・改善を図りつつ、次の各号に掲げる事項について検討を行わなければならない。

- (1) 対象業務等を新設し、又は変更する必要性に関する事項
- (2) 対象業務等の実施による警察事務全般への影響に関する事項
- (3) 対象業務の業務要件（業務実施手順、システム化の範囲等）に関する事項
- (4) システムの設計・開発及び対象業務の実施に必要な人員、組織及び経費に関する事項
- (5) 対象業務等の実施に当たり必要な安全性の確保に関する事項
- (6) システム間のデータ連携及び公開可能な情報のオープンデータとしての活用を容易にするために必要となる次に掲げる事項
 - ア 文字の取扱いに関する事項
 - イ データの標準化に関する事項
- (7) その他対象業務の実施に関する事項

2 実施方法の策定

運用主管課長は、その所管に属する対象業務等について、警察庁の運用主管課長が定める事項を踏まえ、システム総括責任者の承認を得た上で、次のアからカまでに掲げる事項のほか、対象業務等の特性を踏まえ、必要に応じてキからサまでに掲げる事項を定めなければならない。

- ア 対象業務の目的に関する事項
- イ 対象業務の運用の体制に関する事項
- ウ 対象業務において利用するファイルに関する事項
- エ 対象業務における登録、照会等の手順に関する事項
- オ 対象業務に係るアクセス範囲に関する事項
- カ 自宅型テレワーク（自宅（職員が自ら居住するための住宅であり、職員の生活の本拠となっているものをいう。）において行うテレワークをいう。）における対象業務の実施に関する事項（実施の可否等）
- キ 個人情報照会（個人情報を対象とする照会をいう。以下同じ。）に関する記録の確認方法に関する事項
- ク 対象業務に係る入力資料及び出力資料の取扱いに関する事項
- ケ 対象業務に係る部外への委託に関する事項
- コ 対象業務に係る取扱説明書の取扱いに関する事項
- サ その他対象業務の適正かつ円滑な実施に必要な事項

3 実施方法の周知及び指導等

- (1) 運用主管課長は、2の規定により定める対象業務等の実施方法を関係職員に周知しなければならない。
- (2) 運用主管課長は、関係職員に対して、対象業務等が適正かつ円滑に行われるよう、

その実施方法について適切に指導しなければならない。

- (3) (1)及び(2)に掲げるものほか、運用主管課長は、所管する対象業務等を適正かつ円滑に行うために必要な措置を取らなければならない。

第5 アクセス権の付与等

1 アクセス権の申請

- (1) 運用管理者は、所属の職員にアクセス権(アクセスを行う権限をいう。以下同じ。)を付与する必要がある場合は、対象業務等を行う上で必要なアクセス範囲に限定し、運用主管課長にアクセス権の付与の申請を行うものとする。
- (2) 運用主管課長は、(1)に定める申請によるアクセス権の付与が必要と認める場合は、システム総括責任者に当該アクセス権の付与の申請をするものとする。

2 アクセス権の付与

システム総括責任者は、1の事項の申請に基づき、必要と認める場合は、アクセス権を付与するものとする。

3 アクセス権の付与の委任

(1) 委任の条件

対象業務以外の北海道警察情報管理システムを利用して行う業務のアクセス権に係る事務及び警察共通基盤システムの対象業務で運用要領で定められた臨時的アクセス権に係る事務については、次に掲げる条件を満たした場合には、運用主管課長が処理することができる。

ア アクセス権の付与基準の策定

運用主管課長が、対象業務等における所属、係、官職、役職等によって登録、照会、印字等ができるアクセス権の付与基準をあらかじめシステム管理者と協議した上で定め、システム総括責任者の承認を得ていること。

イ アクセス権の付与範囲

アクセス権の付与基準を満たし、かつ必要最小限の範囲であること。

(2) 留意事項

ア 委任を可能とした場合であっても、そのうち特異なもの、重要なもの等について、その都度の判断でシステム総括責任者の承認を得ること。

イ システム総括責任者はアクセス権の付与に係る事務について、受任者を総括すること。

ウ 委任を可能とした場合、受任者において、登録・削除等の作業を実施した際は、その都度、受任者はシステム総括責任者へ登録・削除等の情報を提供すること。

4 認証情報の管理

システム総括責任者は、システムに登録された認証情報(ユーザID、パスワード、個人に特有の生体的特徴その他のアクセス権者を識別又は検証するための情報をいう。以下同じ。)を適切に管理しなければならない。

5 利用の制限

システム総括責任者は、アクセス権者が北海道警察情報管理システム等の情報セキュリティを損なわせる行為を行っていること又は対象業務等の目的以外の目的で不正に北海道警察情報管理システム等を利用していることを認めた場合は、当該アクセス権者に対し、北海道警察情報管理システム等の利用を制限することができる。

6 アクセス権者の責務等

(1) 不正なアクセスの禁止

ア アクセス権者以外の者は、アクセスをしてはならない。

イ アクセス権者は、対象業務等の目的以外の目的で不正にアクセスをしてはならない。

(2) 不正な照会及び情報の利用等の禁止

ア 照会者は、対象業務等の目的以外の目的で不正に照会をしてはならない。

イ 照会者は、照会により得た情報を対象業務の目的以外の目的で不正に利用し、又は提供してはならない。

(3) 認証用媒体の管理等

認証用媒体(認証情報を記録した I C カード等の外部記録媒体をいう。以下同じ。)を利用するアクセス権者は、自己の認証用媒体により他人にアクセスをさせ、又は他のアクセス権者の認証用媒体を用いてアクセスをしてはならない。

(4) 識別コードの管理等

識別コードを利用するアクセス権者は、自己の識別コードにより他人にアクセスをさせ、又は他のアクセス権者の識別コードを用いてアクセスをしてはならない。

(5) パスワード管理の徹底

識別コード及びパスワードを付与されたアクセス権者は、パスワードが他に漏れないように適正に管理しなければならない。

7 アクセスに関する記録等

(1) アクセスに関する記録

システム総括責任者は、北海道警察情報管理システム等を構成するサーバ等に対するアクセスの日時及び内容並びに当該アクセスを行ったアクセス権者の氏名又は識別コードを電磁的方法により記録しておかなければならない。

(2) アクセスに関する記録の保存

システム総括責任者は、(1)による記録を当該記録をした日から起算して5年間保存しておかなければならない。

(3) アクセスに関する確認

システム総括責任者は、(1)による記録に基づき、必要に応じ、アクセスが適正に行われたか否かを確認するものとする。

第6 個人情報照会に関する記録等

1 個人情報照会に関する記録

システム総括責任者は、個人情報照会の日時、目的及び内容並びに当該個人情報照会を行った者の氏名(職員の職員番号その他当該照会者を識別できる符号を含む。以下同じ。)を電磁的方法により記録しておかなければならない。

2 個人情報照会に関する記録の保存

システム総括責任者は、1による記録を当該記録がされた日から起算して5年間保存しておかなければならない。

3 個人情報照会に関する確認

(1) 運用主管課長は、対象業務において利用する情報の機密性に鑑み、第4の2のキにより、必要に応じ、1及び2により保存される個人情報照会の記録の確認の方法を定めるものとする。

(2) システム総括責任者は、1及び2の事項による記録に基づき、必要に応じ、個人

情報照会が適正に行われたか否かを確認するものとする。

第7 個人情報入力資料を含む入力資料の取扱い

1 入力資料の取扱い

- (1) 入力資料は、これを対象業務等に関係のない者に不正に交付し、又は遺棄し、若しくは毀損してはならない。
- (2) 入力資料は、これを亡失しないよう厳重に管理しなければならない。

2 個人情報入力資料の作成等

個人情報入力資料の作成及び個人情報入力資料に記載され、又は記録された情報に係る北海道警察情報管理システム等へのデータの inputs は、対象業務等の目的に従いあらかじめ定められた手続により正確に行わなければならない。

3 用済み後の個人情報入力資料の取扱い

- (1) 個人情報入力資料は、用済み後速やかにこれを返却し、又は廃棄し（当該個人情報入力資料が電磁的記録である場合は廃棄し、若しくはこれに電磁的方法により記録された個人情報を削除し）なければならない。
- (2) 個人情報入力資料の廃棄は、細断、焼却等の復元できない方法により行わなければならない。

4 個人情報入力資料の保管

書面又は外部記録媒体である個人情報入力資料を保管する場合は、施錠のできる所定の保管庫等を用いて保管しなければならない。

5 個人情報入力資料の管理

2から4までに掲げるもののほか、個人情報入力資料は、第4の2の規定により運用主管課長が定める取扱いに関する事項その他のあらかじめ定められた手続に従い、適正に管理しなければならない。

第8 個人情報出力資料を含む出力資料の取扱い

1 出力資料の取扱い

- (1) 出力資料は、これを対象業務に関係のない者に不正に交付し、又は遺棄し、若しくは毀損してはならない。
- (2) 出力資料は、これを亡失しないよう厳重に管理しなければならない。

2 個人情報出力資料の作成

個人情報出力資料は、次の各号に掲げる場合を除き、これを作成してはならない。

ア 対象業務等の目的に従いあらかじめ定められた手続により作成する場合

イ 5の(1)のイの規定により個人情報出力資料を交付するため作成する場合

ウ 北海道警察情報管理システム等の保守又は試験を行うため作成する場合

エ システム総括責任者が別に定める臨時的な出力に係る手続により作成する場合

3 用済み後の個人情報出力資料の取扱い

- (1) 個人情報出力資料は、用済み後速やかにこれを返却し、又は廃棄し（当該個人情報出力資料が電磁的記録である場合は廃棄し、若しくはこれに電磁的方法により記録された個人情報を削除し）なければならない。
- (2) 個人情報出力資料の廃棄は、細断、焼却等の復元できない方法により行わなければならない。

4 個人情報出力資料の保管

書面又は外部記録媒体である個人情報出力資料を保管する場合は、施錠のできる所

定の保管庫等を用いて保管しなければならない。

5 個人情報出力資料の交付

(1) 個人情報出力資料は、次に掲げる場合を除き、これを交付（出力資料を取り扱う警察職員から、その他の者に対して当該資料又は当該資料に記録された情報を提供することをいう。以下同じ。）してはならない。

ア 対象業務等の目的に従いあらかじめ定められた者に交付する場合

イ 法令の規定により交付を求められ、又は交付することが許されている場合において、当該資料に記録された情報を保有するシステム総括責任者の承認を得て交付する場合

ウ 北海道警察情報管理システム等の保守又は試験のため交付する必要がある者に交付する場合

エ システム総括責任者が別に定める臨時的な出力に係る手続により作成し、交付する場合

(2) 個人情報出力資料を交付するときは、運用管理者は、当該個人情報出力資料が交付の目的以外の用に供されないよう適切にこれを管理させるとともに、用済み後は、これを返却させ、又は廃棄させ（当該個人情報出力資料が電磁的記録である場合は廃棄させ、若しくはこれに電磁的方法により記録された個人情報を削除させ）なければならない。

(3) 書面又は外部記録媒体である個人情報出力資料の交付を送付の方法により行うときは、運用管理者は、職員にこれを携行させなければならない。ただし、職員にこれを携行させることが困難である場合においてシステム総括責任者が特に認めたときは、書留郵便により、又はこれを封かんした容器に入れ、個人情報の漏えいを防止するために必要な特約を締結した者に託して送付することができる。

(4) 個人情報出力資料の交付を通信の手段により行うときは、その手段としてファイルサーバ又は電子メールを使用するものとし、交付又は受入れを行う所属の運用管理者は、対象業務ごとに交付又は受入れを担当する職員（以下「交付等担当者」という。）を指定するとともに、その手段ごとに次に掲げる事項を遵守しなければならない。ただし、システム総括責任者及び運用主管課長が特に認めた場合は、これによらない方法で交付することができる。

なお、ファイルサーバ又は電子メールの手段により難しい場合は、ファクシミリを使用することができる。

ア ファイルサーバを使用する場合

(ア) 電子計算機の指定

対象業務等を行う上で必要な範囲で交付又は受入れに使用する電子計算機を指定（交番、駐在所等に整備される電子計算機は除く。）するとともに、指定した電子計算機以外の電子計算機で交付又は受入れを行う個人情報出力資料を取り扱わないようにさせなければならない。

(イ) 作成する共有フォルダへのアクセスの制限

運用管理者の所属及び対象業務等ごとの共有フォルダを作成させ、当該対象業務等に係る交付等担当者以外の者がアクセスできないよう技術的な対策を講じさせなければならない。

(ウ) 交付する資料の暗号化

(イ)の事項により作成する共有フォルダに個人情報出力資料を保存する場合は、パスワードを利用して暗号化させるとともに、当該パスワードを交付等担当者以外の者に知られないようにさせなければならない。

(エ) 交付又は受入れ後の資料の削除

個人情報出力資料を交付し、又は受け入れた後は、(イ)の事項により作成する共有フォルダから速やかにこれを削除させなければならない。

イ 電子メールを使用する場合

(ア) 電子メールの限定

交付又は受入れに使用する電子メールは、メールサーバにおいて送受信の履歴が収集でき、かつ、警察機関の内部に閉じた電気通信回線を使用するものに限定させなければならない。

(イ) 電子計算機の指定

対象業務等を行う上で必要な範囲で交付又は受入れに使用する電子計算機を指定（交番、駐在所等に整備される電子計算機は除く。）するとともに、指定した電子計算機以外の電子計算機で交付又は受入れを行う個人情報出力資料を取り扱わないようにさせなければならない。

(ウ) 交付する情報の暗号化

交付する個人情報出力資料は、パスワードを利用して暗号化させるとともに、当該パスワードを交付等担当者以外の者に知られないようにさせなければならない。

(エ) 交付又は受入れ後の資料の削除

個人情報出力資料を交付し、又は受け入れた後は、送信用又は受信用のメールサーバから速やかにこれを削除させなければならない。

(オ) 誤送信防止

交付先のメールアドレスを事前に登録させなければならない。

ウ ファクシミリを使用する場合

(ア) 交付する個人情報出力資料の限定

ファクシミリにより交付する個人情報出力資料は、次に掲げるものに限定させなければならない。

a 照会記録資料（個人情報照会に関する記録事項の通知資料をいう。）

b 重要犯罪、重要窃盗犯、銃器・薬物犯罪及びひき逃げ事件の捜査並びに逮捕事件の送致等の事案であって、これらの事案処理のため緊急に必要な個人情報出力資料

(イ) 使用するファクシミリの指定

対象業務等を行う上で必要な範囲で交付又は受け入れに使用するファクシミリ（送受信の履歴が収集できるものに限る。）を指定（交番、駐在所等に整備されるファクシミリは除く。）しなければならない。

(ウ) 誤送信防止

(イ)の規定により指定した交付に使用するファクシミリについては、一般加入回線への発信を停止した警察電話回線に接続させるとともに、事前に交付先のファクシミリの番号を登録させ、又は短縮ダイヤルを設定させなければならない。

(エ) 交付等担当者の相互の連絡

交付先のファクシミリにおいて個人情報出力資料を受信した後、交付等担当者が速やかにこれを受領するよう、交付等担当者の相互の連絡を緊密に行わせなければならない。

(オ) メモリ送信及びメモリ受信

メモリ送信の機能は利用させてはならない。

また、ファクシミリが用紙切れ等によりメモリ受信した場合は、記録内容を印字した後、当該記録がメモリから削除されていることを確認させなければならない。

6 個人情報出力資料の複写

(1) 個人情報出力資料は、次に掲げる場合を除き、これを複写してはならない。

ア 対象業務等を行う上で複写する必要があるものとして運用管理者が認める場合

イ 北海道警察情報管理システム等の保守又は試験のため複写する必要がある場合

(2) (1)の規定により個人情報出力資料を複写した物は、個人情報出力資料とみなして3から5まで、6(1)及び7の規定を適用する。

7 個人情報出力資料の作成等に関する記録

(1) 運用管理者は、個人情報出力資料の作成、交付、受入れ、複写、返却又は廃棄若しくはこれに電磁的方法により記録された個人情報の削除（(3)において「作成等」という。）の日時及び目的、当該個人情報出力資料を取り扱う警察職員の氏名並びに当該個人情報出力資料の概要及び数量を簿冊に記載させ、又はこれらの事項を電磁的方法により記録させておかななければならない。

(2) 運用管理者は、(1)の簿冊を最終の記載がされた日から起算して5年間保管し、又は(1)の事項による記録を当該記録がされた日から5年間保存しておかななければならない。

(3) 運用管理者は、(1)の簿冊又は(1)の事項による記録に基づき、個人情報出力資料の作成等が適正に行われたか否かを確認しなければならない。

また、システム総括責任者は、(1)の簿冊又は(1)の事項による記録に基づき、必要に応じ、個人情報出力資料の作成等が適正に行われたか否かを確認するものとする。

8 個人情報出力資料の作成等に関する記録に係る特例措置

運用管理者は、システム総括責任者が、次に規定した事項を全て満たしていることの警察庁システム総括責任者（警察庁長官官房参事官（情報化及び技術革新に関する総合調整担当）をいう。以下同じ。）による確認を受けた場合、7の規定に基づく記録を不要とすることができる。

なお、本特例措置の適用は、一の対象業務中、全部又は一部の個人情報出力資料の作成等に関する記録に対して行うことができるものとする。

(1) システムに係る要件

ア 警察庁システム総括責任者が別に定めるところにより、個人情報出力資料の印字出力及びファイル出力に関する証跡その他の個人情報出力資料の作成等に関する証跡等をサーバ等又は端末装置に記録していること。

イ 警察庁システム総括責任者が別に定めるところにより、印字出力又はファイル出力する個人情報出力資料に出力日時、出力した者の所属その他の個人情報出力資料の作成等に関する情報を明示できること。

(2) 個人情報出力資料の取扱いに係る要件

ア 交付時における幹部による確認

警察職員が個人情報出力資料を5の(1)のア、ウ又はエにより交付する場合は、警部以上の階級にある警察官又はこれに相当する一般職員（夜間・休日にあつては当直責任者を含む。）の確認を受けること。

イ 個人情報出力資料の管理

印字出力した個人情報出力資料のうち、出力当日中に廃棄又は捜査書類として利用するもの以外は、各機関における文書に関する規定に基づいた方法により管理すること。

第9 保守

1 適切な保守のための措置

システム総括責任者は、北海道警察情報管理システム等が適切に保守されるよう必要な措置を執らなければならない。

2 設備等の保守

北海道警察情報管理システム等を構成するサーバ等及びこれに附帯する電源設備等（以下「設備等」という。）は、次の各号に掲げるところにより、これを適切に保守しなければならない。

ア 設備等の保守・点検の方法を定めること。

イ 設備等の重要度に応じて、予備機器の整備等に努めること

ウ 保安装置の整備等安全性の確保に努めること。

第10 ドキュメント等の取扱い

1 ドキュメント等の取扱い

(1) システムドキュメント及びプログラム並びに取扱説明書（以下「ドキュメント等」という。）は、これを対象業務等に関係のない者に不正に交付し、又はこれを遺棄し、若しくは毀損してはならない。

(2) ドキュメント等は、これを亡失しないよう厳重に管理しなければならない。

2 ドキュメント等の亡失等の防止

(1) システムドキュメント及びプログラム

システムドキュメント及びプログラムは、その亡失若しくは毀損又はこれに記載され、若しくは記録された北海道警察情報管理システム等の安全上秘密を要する事項の漏えいのないよう、これらを管理する所属の長は、資料の名称、作成、交付、受入れ、複写、返却、保管、廃棄等管理の状況を簿冊に記載させ、又はこれらの事項を電磁的方法により記録させるとともに、当該ドキュメント等が書面又は外部記録媒体の場合は、施錠のできる所定の保管庫等を用いて保管させなければならない。

(2) 取扱説明書

北海道警察情報管理システム等の安全上秘密を要する事項が記載され、又は記録されているなど特に管理が必要なものとして、第4の2のロの事項により運用主管課長が定める取扱説明書については、運用管理者は、資料の名称、交付、受入れ、複写、返却、保管、廃棄等管理の状況を簿冊に記載させ、又はこれらの事項を電磁的方法により記録させるとともに、当該説明書が書面又は外部記録媒体の場合は、施錠のできる所定の保管庫等を用いて保管させなければならない。

第11 安全の確保

1 端末装置の表示

北海道警察情報管理システム等の端末装置は、対象業務等に関係のない者がそのディスプレイ等に表示された内容を容易に見ることができない場所に設置しなければならない。

また、照会した結果を表示する画面にはウォーターマークを挿入するなど、画面に表示された内容の不適正な接写を防止するために必要な措置を執らなければならない。

2 警察職員以外の者への業務の委託

対象業務等の一部、北海道警察情報管理システム等を構成するサーバ等又は端末装置の保守、試験等北海道情報管理システム等に関する業務を警察職員以外の者に委託する者は、次の各号に掲げるところによりこれを行わなければならない。

- (1) あらかじめ当該委託に係る業務の実施の場所及び方法、当該委託に係る業務に従事する者（以下「委託先担当者」という。）の範囲、個人情報又は北海道警察情報管理システム等の安全上秘密を要する事項の漏えいを防止するために執るべき措置等を明確に定めた特約を締結すること。
- (2) 委託先担当者にアクセス権を貸与する場合は、業務上必要な範囲に限定するとともに、当該委託先による個人情報照会に関する記録を随時確認するなど、北海道警察情報管理システム等の不正な利用を防止するために必要な措置を執ること。
- (3) 委託先担当者が取り扱う個人情報入力資料又は個人情報出力資料の廃棄（当該資料が電磁的記録である場合は廃棄、又はこれに電磁的方法により記録された個人情報の削除）に当たっては、その状況を職員に確認させるなど、当該資料の不正な利用を防止するために必要な措置を執ること。

3 情報セキュリティ

北海道警察情報管理システム等の情報セキュリティに関して実施する運用管理対策、物理的対策、技術的対策その他の事項については、この要領に定めるもののほか、警察情報セキュリティポリシーに定めるところによる。

4 事故発生時の措置

システム総括責任者は、北海道警察情報管理システム等に関する事故が発生した場合において執るべき措置を定め、あらかじめこれを関係職員に周知するとともに、事故が発生した場合は、速やかにその状況及び原因を調査し、適切な措置を執らなければならない。

5 相互接続

相互接続に当たっては、警察庁長官官房長が定める技術的基準に従い、安全性の確保に努めなければならない。

第12 細目的事項に関する委任

この要領に定めるもののほか、北海道警察情報管理システム等の設計並びに運用及び維持管理に関し必要な細目的事項は、システム総括責任者が定めるものとする。