別紙10

情報管理規程（ひな型③）

【事業者の責任者を含む複数名が、犯罪事実確認記録等を通じて、従事者の犯歴情報を確認し、こども性暴力防止法関連システム以外にも犯罪事実確認記録等の記録・保存等を行う場合】

※　本ひな型は標準的措置をベースに記載している。各事業者は、別紙1の考え方を十分理解した上で、必要に応じて最低限求められる措置も参照しつつ、その実情に合わせて本ひな型を適宜改変した上で活用されたい。

※　法関連システムとは、こども性暴力防止法（以下「法」という）の運用のために、こども家庭庁で新たに開発するシステムをいう。また、情報システムとは、各事業者における人事管理等に用いている独自のシステムをいう。

第１章　総論

（1）　基本的事項

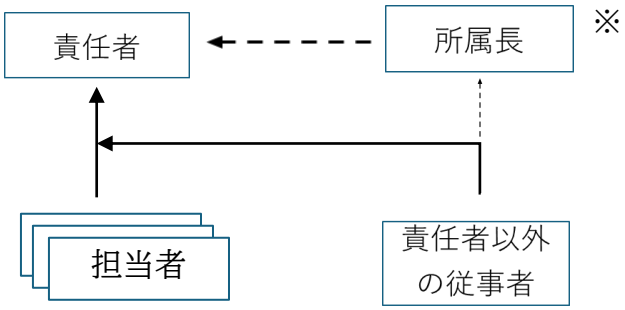
- 責任者は犯罪事実確認記録等の取扱いに関する基本方針を、次のとおり定める。
  - 犯罪事実確認記録等の取扱者は必要最小限とする
  - 犯罪事実確認書の記載内容について、別に記録・保存することを極力避ける
  - やむを得ず記録・保存する場合は、リスクに応じた情報管理措置を行う
  - 情報機器の種類や環境、ネットワークの状況等に応じた情報管理措置を講じる
  - 犯罪事実確認記録等の取扱いの手順に応じて必要な対応を行う
  - 組織の長自ら情報管理の重要性を理解し、組織として点検・改善を実施する
  - 法に定める情報管理措置に関する規定を遵守する

第２章　組織的情報管理措置

（1）　組織体制の整備

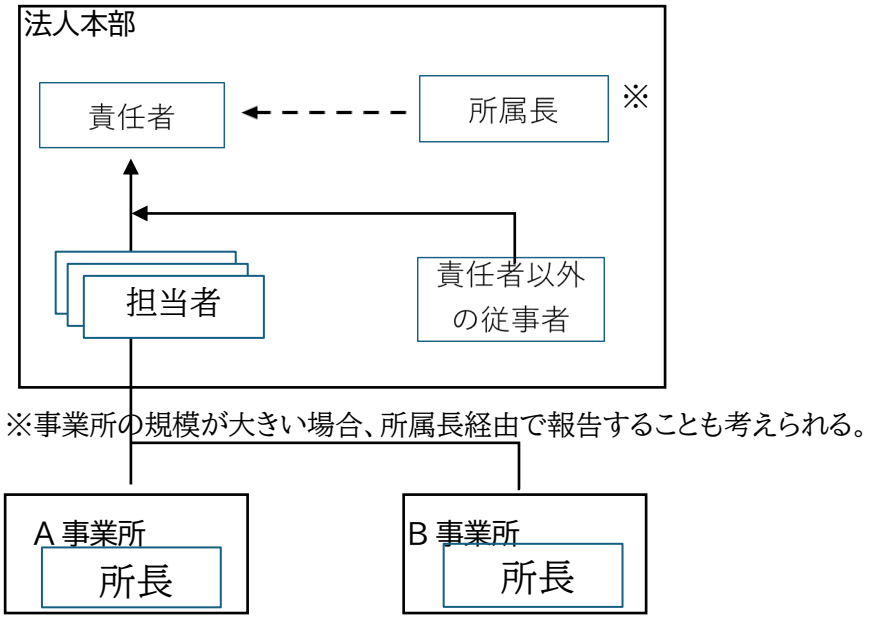
- 犯罪事実確認記録等の取扱いに関する責任者（以下「責任者」という。）を設置することとし、●●長をもって充てる。
- 責任者は、犯罪事実確認記録等の管理に関する事務を総括するとともに、自ら本規程に定められた事項を遵守し、かつ従事者に遵守させるために、本規程に定める措置その他必要な措置を実施する責任を負う。
- 責任者は、犯罪事実確認記録等の管理に関する担当者（以下「担当者」という。）を任命し、その権限の一部を担当者に委譲する。担当者は●●…をもって充てる。
- 責任者は、犯罪事実確認記録等の管理に関する監査を行う者を設置することとし、●●をもって充てる。
- 責任者、担当者、監査を行う者に加えて、犯罪事実確認記録等を取り扱うことができる者を置く場合は、責任者が認めた者に限り、その都度任命する。
- 責任者は、漏えい等の事案の発生又は兆候を把握した場合、こども家庭庁の対応マニュアルに基づき対応する。また、その対応を行うための体制を整備する。
- 責任者は、漏えい等の事案の発生又は兆候を把握した場合の報告連絡体制及び法や情報管理規程に違反している事実又は兆候を把握した場合の報告連絡体制を次のように定める。

（報告連絡体制図：単一事業所内で完結する場合）



※事業所の規模が大きい場合、所属長経由で報告することも考えられる。

（報告連絡体制図：事業者内に事業所が複数ある場合）



※事業所の規模が大きい場合、所属長経由で報告することも考えられる。

- 事業者内外（事業者内の関係者のほか、IT 製品のメーカー、保守ベンダー、保護者等）の緊急連絡先・伝達ルートを整備し、関係者へ周知を行う。
- 事案発生時に業務システムが使えず連絡先が確認できない場合を想定した、連絡の代替手段をあらかじめ確認する。
- 犯罪事実確認記録等を複数の部署で取り扱う場合の各部署の任務分担と責任を次のように定める。（複数の部署で取り扱わない場合は、定めは不要。）

部署・役割名	任務分担	責任
法人本部 ・責任者／担当者	・ 法人全体の犯罪事実確認書の申請事務取りまとめ・閲覧 ・ 法関連システムの ID 発行事務・管理 ・ 犯罪事実確認記録等の管理体制の整備・利害関係者への伝達	・ 法人全体の犯罪事実確認書の情報管理措置 ・ 法関連システムの ID 発行事務・管理 ・ 犯罪事実確認記録等の管理体制の整備・利害関係者への伝達

A 事業所 ・責任者	・ A 事業所の従事者の犯罪事実確認書の閲覧、法関連システムの利用 ・ 法関連システムの ID 管理	・ A 事業所の従事者に関する犯罪事実確認書の情報管理措置 ・ 法関連システムの ID 管理

（2） 運用状況に関する記録の整備

- 責任者は、情報管理規程に基づく運用を確保するため、システムログその他の犯罪事実確認記録等の取扱記録を作成し、適切かつ安全に管理されていることを定期的に確認する。
  - 紙で交付された犯罪事実確認書の閲覧の状況
  - 犯罪事実確認書の情報を転記した犯罪事実確認記録の作成・閲覧の状況
  - 犯罪事実確認記録等が記録された媒体等の持ち運び等の状況
  - 犯罪事実確認記録等の伝達の状況（法により認められた事業者間の情報共有の場合に限る。）
  - 犯罪事実確認記録等の消去・廃棄の状況（消去・廃棄を委託した場合の消去・廃棄を証明する記録を含む。）

    ※ 法関連システム上の犯罪事実確認書については、同システムで消去
- 責任者は、次の項目について、犯罪事実確認記録等の取扱状況を確認する手段を整備し、記録を行うことにより、取扱状況を把握する。

  （記録する情報）
  - 犯罪事実確認書
  - 犯罪事実確認記録

  （記録項目）
  - 記録する情報ごとの取扱責任者・取扱部署、アクセス権者
  - 犯罪事実確認記録の所在（バックアップがある場合はその所在を含む。）
  - 利用目的

（3） 点検等

- 責任者は、法や情報管理規程の遵守状況につき、犯罪事実確認記録等の取扱記録等に基づいて、定期的に自己点検及び他部署等による監査を実施する。
- 自己点検の際、責任者は担当者と取扱いの不備、情報漏えいの発生の危険性、改善すべき点等について、意見交換し、見直し及び改善に取り組むとともに、必要に応じて規程を変更する。

第 3 章 人的情報管理措置

（1） 研修・訓練等

- 責任者、担当者その他の犯罪事実確認記録等を取り扱うことができる者は、犯罪事実確認記録等の取扱いに関する次の内容について、着任時及び定期的に研修等を受講する。
  - 犯罪事実確認記録等の管理の重要性
  - 情報管理措置の基本原則及び具体的措置
  - 法違反、漏えい等の事実又はおそれを把握した場合の対応
  - 関係法令や事業者内規程等の変更があった場合にはその内容
  - 禁止事項と罰則
- 責任者は、研修の実施記録を作成し、定期的に確認する。
- 責任者は、犯罪事実確認記録等の取扱い、法違反、漏えい等の事実又は兆候を把握した場合の対応について、従事者に対し、着任時に研修等を行う。
- 責任者は、上述の研修以外にも、人事異動の多い時期等に定期的に意識啓発を行う。
- 犯罪事実確認記録等の秘密保持、情報管理規程に違反した際の人事上の取扱い等に関する就

業規則は次のとおり。
・ 就業規則第●条 ……

- 責任者は、担当者等が退職する際、永久的に犯罪事実確認記録等に記載された情報を漏らしてはならないことを確認する。

第 4 章 物理的情報管理措置

（1） 犯罪事実確認記録等を取り扱う区域の管理

- 犯罪事実確認記録等の管理区域を（本部●●部執務室及び●事業所●●室）に限定し、次の対策を行う（複数選択可）。
  - ・ 権限を有しない者が入室、閲覧しないように施錠
  - ・ 管理者による鍵の管理・入退室の際の鍵の貸出しの許可制
  - ・ 入退室管理
  - ・ 警備システムの導入、警備員の配置
  - ・ 持ち込む機器等の制限

- 責任者は、取扱区域（本部●●部執務室内の●●で指定されるエリア及び●事業所●●室の●●で指定されるエリア）を限定し、次の措置を講じ、取扱区域において権限を有しない者による犯罪事実確認記録等の閲覧等を防止するため、次の措置を講じる（複数選択可）。
  - ・ 権限を有しない者が入室、閲覧しないための施錠
  - ・ 管理者による鍵の管理・入退室の際の鍵の貸出しの許可制の導入
  - ・ 入退室管理
  - ・ 警備システムの導入、警備員の配置
  - ・ 責任者の承認のない記録媒体、カメラ等の持込みの制限
  - ・ 間仕切り等の設置
  - ・ 座席配置の工夫
  - ・ のぞき込みを防止する措置の実施

（2） 機器及び電子媒体等の盗難等の防止

- 責任者は、犯罪事実確認記録等を取り扱う機器、犯罪事実確認記録等が記録された電子媒体及び書類等の盗難又は紛失等を防止するため、次の措置を講じる（複数選択可）。
  - ・ 犯罪事実確認記録等を取り扱う機器をセキュリティワイヤーで固定する（又は使用者の不在時にノートPC等を机の引出しやロッカー等に格納・施錠する）
  - ・ 犯罪事実確認記録等を取り扱う機器、犯罪事実確認記録が記録された電子媒体又は犯罪事実確認記録が記載された書類等を、施錠できるキャビネット・書庫等に保管する

- 責任者は、盗難、紛失時に情報漏えい等を防止するために、次の措置を講じる（複数選択可）。
  - ・ 犯罪事実確認記録等の電子ファイルは暗号化、パスワードによる保護等を行った上で保存する
  - ・ 携帯端末の紛失時の端末の位置の特定
  - ・ 携帯端末の紛失時の遠隔操作による端末の保護
  - ・ 携帯端末の紛失時の遠隔操作によるデータの消去

- 責任者は、従事者等が犯罪事実確認記録等を取り扱う機器を紛失した場合、即時、法関連システム及び情報システムのアクセス権の解除を行うとともに、情報システムのログインパスワードを変更する。

（3） 電子媒体又は紙媒体等を持ち運ぶ場合の漏えい等の防止

- 責任者は、次のような紛失・盗難等を防ぐための安全な方策を講じた上で、やむを得ない場合に限り、犯罪事実確認記録等が記載された電子媒体や書類等の持ち運びを行うことを認める。この場合において、持ち運びや伝達等の状況に係る取扱記録の作成を求め、責任者が定期的に確認する（複数選択可）。
  - データを暗号化する
  - パスワードを設定する
  - 封筒に封入し、鞄に入れて搬送する
  - 公共交通網などを利用する場合は、網棚等を使用せず手元から離さない
  - 自家用車を利用する場合は車内に放置せず、身体から離さずに移動する
  - 封緘、目隠しシールの貼付けを行う
  - 施錠できる搬送容器を利用する
  - 紙媒体へ記録せざるを得ない場合には、権限を有する従事者であっても、利用終了後、速やかに回収し、廃棄又は厳重に保管する等、組織的な管理を徹底する
  - 情報の持ち運びを行う場合は、その従事者に対し、退社時の荷物検査を行い、情報持ち出しのチェック等の対策を講じる
- 犯罪事実確認記録を電子媒体に記録する場合、責任者は、その電子媒体の管理状況の確認を定期的に行う。

（4） 犯罪事実確認記録等の削除及び機器、電子媒体等の廃棄

- 責任者は、犯罪事実確認記録等が記録された書類・ファイルや記録媒体等の廃棄、犯罪事実確認記録等が保存された電子データの消去を行う場合、次の点に留意して、紙媒体については復元不可能な状態にして廃棄し、電子媒体については容易には復元できない形にして廃棄・消去する。その上で、犯罪事実確認記録等を削除したこと、又は犯罪事実確認記録等が保存された機器、電子媒体等を廃棄したことの取扱記録を作成し、責任者が確認する。
  - 犯罪事実確認記録が記録された機器、電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等を行う
  - 紙媒体については、適切なシュレッダー処理、焼却等の復元不可能な手段を採用する

第 5 章　技術的情報管理措置

（1）　アクセス制御

- 責任者は、犯罪事実確認記録等を取り扱うことのできる機器及び当該機器を取り扱うことのできる従事者を明確化して限定する。
- 責任者は、情報システムに犯罪事実確認記録を保存する場合、次のような保存場所の分離等を行った上で、アクセス権を有する者の ID からのみアクセスできるようにする（複数選択可）。
  - アクセス権を有する者の ID でログインしたPC等からのみ、その電子データを閲覧できる状態にする。
  - 犯罪事実確認記録等を取り扱う機器のサーバの物理的分離（専用サーバの設定）、サーバの仮想化による論理的分離（1台のサーバを複数の仮想サーバに分割し、専用サーバを設定）。
  - 情報システムで犯罪事実確認記録を保存する場合は、ネットワークの分離を行う。
- 責任者は、異動又は退職する者等について、即時、法関連システム及び情報システムからアクセス権を解除する。
- 責任者は、定期的に適切にアクセス権が付与されているかを確認し、アクセスが不要な者がいた場合、即時、法関連システム及び情報システムへのアクセス権の解除及びアカウントの削除を行う。

（2）　外部からの不正アクセス等の防止

- 責任者は、犯罪事実確認記録等を取り扱う機器(主に PC)にアンチウイルスソフトウェア等を導入し、不正ソフトウェアの有無を確認する。
- 責任者は、犯罪事実確認記録等を取り扱う情報システムのオペレーティングシステム(OS)やアプリケーションは、サポート期限切れにならない製品を利用し、最新のバージョンを維持する。
- 責任者は、ウイルスの侵入や情報漏えいを防止するため、次に掲げる方法により、業務上不要なインターネット通信を制限する(複数選択可)。
  - 情報システムと外部ネットワークとの接続箇所へのファイアウォールの設置
  - フィルタリング機能を有するOS標準ソフトウェアの利用
  - 通信キャリアやインターネットプロバイダの提供するオプションサービス、複数のセキュリティサービスを提供するソフトウェア製品等の活用
  - ネットワークの分離及び犯罪事実確認記録等を取り扱う回線の専用ネットワーク化
- 責任者は、情報システムにおけるログ等を定期的に分析し、不正アクセス等を検知する。
- 責任者は、次に掲げる方法を組み合わせて、多層防御を実施する(複数選択可)。
  - ファイアウォールの設置
  - ネットワークの分離
  - ファイルや通信データの暗号化
  - IDS、IPS などによる不正アクセスの検知又は遮断
  - DLP を用いた情報の漏えい、滅失又は毀損の防止
- 責任者は、情報システムに犯罪事実確認記録を保存する際、外部ネットワークから遮断された領域において保存する等の方法により、外部からの不正アクセス等を防止する。

(3) 情報システムの使用に伴う漏えい等の防止

- 責任者は、情報システムの使用に伴う犯罪事実確認記録等の漏えい等を防止するため、情報システムの設計時に安全性を確保し、継続的に見直す。(情報システムの脆弱性を突いた攻撃への対策を講ずることも含む。)
- 犯罪事実確認記録等を含む通信の経路及び内容を暗号化する。
- 移送する犯罪事実確認記録等について、パスワード等による保護を行う。
- 保存場所の分離等を行った上で、アクセス権を有する者の ID からのみアクセスできるようにする。
- 犯罪事実確認記録等を取り扱う情報システムにアクセスする従事者に対して、ユーザーID による識別を行い、パスワード、磁気・IC カード、生体認証(指紋認証、虹彩認証、静脈認証等)、ワンタイムパスワード、PIN 入力の付与等を組み合わせた多要素認証を行う。
- ISMAP 基準を満たし、国内法が適用される拠点にデータを保存できるクラウドサービスを選定する。
- (既に海外拠点にデータを保存するクラウドサービスを利用しており、利用サービスを変更することでかえって漏えい等のリスクが高まる等、やむを得ず海外拠点にデータを保存するクラウドサービスを引き続き利用する場合)当該外国の個人情報の保護に関する制度等を把握し、犯罪事実確認記録等の情報管理のために〇〇等の必要かつ適切な措置を講じる。