【情報管理措置】こども性暴力防止法に基づく「情報管理措置」とは

■なぜ厳格な情報管理が必要なのか？

「犯罪事実確認記録等」は、従事者の特定性犯罪事実を含む極めて機微性の高い個人情報です 。万が一漏えいが発生した場合、対象者の権利を著しく侵害するだけでなく、制度全体への信頼を揺るがし、こどもたちの安全を守る取り組みに支障をきたす恐れがあります 。そのため、法に基づき厳格な管理と罰則規定が設けられています 。

■情報管理の5つの基本義務

対象事業者等には、以下の5つの対応が義務付けられています。

① 適正な管理
管理責任者を置き、必要な措置を講じること 。

② 目的外利用・第三者提供の禁止
裁判所の手続や捜査等の例外を除き、提供・利用は禁止 。

③ 重大事態の報告
漏えい等の事案が発生した際は、直ちにこども家庭庁へ報告すること 。

④ 廃棄・消去の徹底
定められた期限（後述）までに確実に廃棄・消去すること 。

⑤ 機微情報の保護
被害児童等から聴取した情報も、犯罪事実に準じて厳格に取り扱うこと 。

■組織として取り組むべき「情報管理規程」の策定

事業者は、適正な管理を行うために「情報管理規程」を定め、遵守しなければなりません 。

【基本原則】
・情報を取り扱う者は必要最小限に限定する 。
・犯罪事実確認書の内容の記録・保存は極力避ける 。
・やむを得ず保存する場合は、漏えいリスクに応じた措置を講じる 。

【管理体制の整備】
・「管理責任者」を設置し、役割と責任を明確にする 。
・法や規程に違反する兆候を把握した際の報告連絡体制を整える 。

■4つの安全管理措置（具体的な実施事項）

① 組織的情報管理措置

取扱記録の作成	システムログや閲覧状況などの記録を作成し、管理者が定期的に確認する 。
自己点検・監査	適正に管理されているか、定期的に評価・見直しを行う 。

② 人的情報管理措置

研修の実施	従事者の着任時および定期的に、情報管理の重要性やルールに関する研修を行う 。
秘密保持の周知	就業規則等に秘密保持義務や違反時の懲戒規定を盛り込む 。退職後も秘密を保持することを再確認する 。

③ 物理的情報管理措置

区域管理	情報システムや書類を取り扱う区域を適切に管理し、盗難や紛失を防止する 。
復元不可能な廃棄	書類や電子媒体を廃棄する際は、シュレッダーや消去ソフト等で復元不可能な状態にする 。

④ 技術的情報管理措置

アクセス制限	正当な権限を持つ者のみがアクセスできるよう、ID・パスワードや多要素認証（GビズID等）を活用する 。
不正アクセス対策	OSを最新の状態に保ち、ウイルス対策ソフトの導入などセキュリティ対策を徹底する 。

■情報の保存期間と廃棄ルール

犯罪事実確認記録等は、以下のいずれか早い方の期限が経過する日までに廃棄・消去しなければなりません 。

○犯罪事実確認の日から5年後の年度末から起算して30日以内 。
○本人の離職等の日から30日以内 。
○事業者が対象事業者に該当しなくなった日から30日以内 。

■罰則規定

犯罪事実確認書に記載された情報をみだりに他人に知らせたり、不当な目的で利用・提供したりした場合には、刑罰が科されます 。事業者の社会的信用を失墜させないためにも、徹底した管理が求められます。

【出典】「こども性暴力防止法施行ガイドライン」P244-P290「Ⅷ. 情報管理措置」より