Ⅷ. 情報管理措置

１．総則

（１）情報管理措置の全体像

○　犯罪事実確認記録等（※）は、個人の特定性犯罪事実を含む情報であり、漏えい等が発生した場合には、従事者個人の権利利益を著しく侵害し、その生活にも影響を与え得る過度な批判等が生じる可能性がある。また、制度全体への信頼が揺らぎ、本制度を通じて児童等の安全を守ることに支障が生じる可能性や、対象事業者等の信頼や事業継続性にかかわる問題となり、結果として、児童等の教育、保育等に影響が出ることもあり得る。

※　犯罪事実確認記録等とは、次に掲げるものをいう。

- 犯罪事実確認書
- 犯罪事実確認書に記載された情報に係る記録（以下「犯罪事実確認記録」という。）

（特定性犯罪事実の有無及びそれを直接的に示唆する内容（「黒」・「白」と表現するなど）は、犯罪事実確認書の内容と同義であるため、該当する。）

○　このため、法においては、対象事業者等に対して、犯罪事実確認記録等の適正な管理を求めるとともに、対象事業者等、その従事者等が、みだりに特定性犯罪事実等に関する情報を他人に知らせたとき等の様々な場合について、罰則を規定している。特に、対象事業者等の数が多く、その事業内容もさまざまである中で、業務を通じて特定の従事者の特定性犯罪事実を知り得た者が、第三者に不用意にその情報を漏らしてしまうなどのリスクには特に注意を払うべきであることから、対象事業者等は、犯罪事実確認書を閲覧できる者を必要最小限に限定することや、犯罪事実確認書の内容の記録・保存を極力避けること等の、必要な情報管理を徹底する必要がある。

○　対象事業者等には、情報管理措置として、具体的に、次の①から⑤までに掲げる事項への対応が求められる。

①　犯罪事実確認記録等の適正な管理

○　犯罪事実確認実施者等（※）は、犯罪事実確認記録等を適正に管理しなければならない（法第14条）。

※　犯罪事実確認実施者等とは、次に掲げる者をいう。

- 学校設置者等
- 施設等運営者
- 県費負担教職員の犯罪事実確認記録の提供を受けた市町村教育委員会

○　犯罪事実確認記録等を適正に管理するため、犯罪事実確認実施者等は、犯罪事実確認記録等の管理責任者の設置その他の犯罪事実確認記録等を適正に管理するために必要な措置を実施しなければならない（法第11条、規則第12条）。

○　認定事業者等についても、同等の措置が求められている（法第 20 条第１項第６号及び第 27 条第１項）。

②　目的外利用・第三者提供の禁止

○　犯罪事実確認実施者等は、次に掲げる場合を除き、犯罪事実確認記録等を犯罪事実確認若しくは防止措置を実施する目的以外の目的のために利用し、又は第三者に提供してはならない（法第 12 条）。

・　都道府県教育委員会と市町村教育委員会との間（県費負担教職員の場合）及び学校設置者等と施設等運営者との間で、防止措置の実施に必要な限度において提供する場合（同条第１号）
・　訴訟等の裁判所手続又は刑事事件の捜査のために提供する場合（同条第２号）
・　情報公開・個人情報保護審査会の求めに応じて提示する場合（同条第３号）
・　法、児童福祉法等の規定に基づき、報告徴収・立入検査等に応じる場合（同条第４号）

○　認定事業者等についても、同等の措置が求められている（法第 27 条第２項）。

○　また、犯罪事実確認書受領者等（※）又はその役員、従事者等は、犯罪事実確認書に記載された情報について、みだりに他人に知らせ、又は不当な目的に利用してはならないこととされている（法第 39 条）。これに違反した場合や、犯罪事実確認書に記載された情報を自己又は第三者の不正な利益を図る目的で提供したときは、刑罰が科される（法第 43 条及び第 45 条第２項）。

※　犯罪事実確認書受領者等とは、次に掲げる者をいう。

・　犯罪事実確認書の交付を受けた対象事業者
・　法第９条第２項（県費負担教職員）、第 10 条第２項（施設等運営者）又は第 26 条第７項（共同認定）の規定により犯罪事実確認書の提供を受けた者

③　漏えい等の重大事態のこども家庭庁への報告

○　犯罪事実確認実施者等は、犯罪事実確認書に記載された情報の漏えいその他の犯罪事実確認記録等の管理が適正に行われていないと認められる事態であって個人の権利利益を害するおそれが大きいものが生じたときは、直ちにその旨をこども家庭庁に報告しなければならない（法第 13 条）。

○　認定事業者等についても、同等の措置が求められている（法第 27 条第２項）。

④　犯罪事実確認記録等の廃棄・消去

○　犯罪事実確認書受領者等は、犯罪事実確認記録等について、

・　犯罪事実確認の確認日から５年後の属する年度の末日から起算して 30 日
・　離職等の日から起算して 30 日
・　対象事業者に該当しなくなった日から起算して 30 日

を経過する日までに廃棄・消去しなければならない（法第 38 条）。

⑤　安全確保措置等を通じて収集した機微性の高い情報の取扱い

○　犯罪事実確認実施者等及び認定事業者等が、こども性暴力防止法に基づく安全確保措置等を通じて収集した機微性の高い情報（①特定性犯罪事実関連情報及び②児童等から聴取した児童対象性暴力等のおそれ等の情報）は、法において特別な情報管理を求める犯罪事実確認記録等には該当しないが、犯罪事実確認記録等に準じた厳格な情報管理が必要となる。

（２）個人情報保護法との関係

○　個人情報の保護に関する一般法である個人情報保護法においては、事業者に対する情報保護に係る規律が定められており、犯罪事実確認実施者等及び認定事業者等が犯罪事実確認記録等を取り扱う場合も、当該規律は適用される。

○　一方、犯罪事実確認記録等は、個人情報の中でも特に配慮が必要な機微性の高い個人情報であり、漏えい等した場合の権利利益の侵害や制度に対する信頼の喪失のおそれが大きいため、法においては、個人情報保護法上の規律に加えて、より厳格な規制を課すことが必要であるとの考えの下、前述の①から④までの規定が置かれている。

○　法において特別な情報管理を求める犯罪事実確認記録等には該当しない⑤の機微性の高い情報も含めて、情報管理措置の具体的内容については、このような考え方を踏まえるとともに、個人情報保護法における規律との整合性を図ることとしている。

○ 本章では、上述の内容も踏まえ、情報管理措置に関する具体的な対応事項や留意点等を示す。

２．犯罪事実確認記録等の適正な管理（法第 11 条、第 14 条、第 20 条第１項第６号及び第 27 条第１項関係）

法第 11 条、第 14 条、第 20 条第１項第６号及び第 27 条第１項

（犯罪事実確認記録等の管理に関する措置）

第十一条　第四条（第九条第一項又は前条第一項の規定により読み替えて適用する場合を含む。）の規定により犯罪事実確認を行わなければならない者及び第九条第二項の規定により犯罪事実確認記録の提供を受ける市町村の教育委員会（以下この章において「犯罪事実確認実施者等」という。）は、犯罪事実確認記録等（第三十八条第一項に規定する犯罪事実確認記録等をいう。以下この章及び次章において同じ。）の管理責任者の設置その他の犯罪事実確認記録等を適正に管理するために必要な措置として内閣府令で定めるものを講じなければならない。

（犯罪事実確認記録等の適正な管理）

第十四条　犯罪事実確認実施者等は、犯罪事実確認記録等を適正に管理しなければならない。

（認定の基準等）

第二十条　内閣総理大臣は、認定の申請に係る前条第三項第二号の民間教育保育等事業及び同項第四号の業務の内容がそれぞれ民間教育保育等事業及び教育保育等従事者の業務に該当し、かつ、当該申請が次に掲げる基準に適合すると認めるときでなければ、認定をしてはならない。

一～五　（略）

六　認定を受けようとする民間教育保育等事業者が犯罪事実確認記録等を適正に管理するために必要な措置として内閣府令で定めるものを講じていること。

２　（略）

（犯罪事実確認記録等の適正な管理）

第二十七条　認定事業者等は、犯罪事実確認記録等を適正に管理しなければならない。

２　（略）

規則第 12 条

（法第十一条等の内閣府令で定める措置）

第十二条　法第十一条及び第二十条第一項第六号（法第二十一条第三項において準用する場合を含む。）の内閣府令で定める措置は、管理責任者を設置し、及び犯罪事実確認記録等（法第三十八条第一項に規定する犯罪事実確認記録等をいう。以下同じ。）の管理に関する措置（以下「情報管理措置」という。）に係る規程（以下「情報管理規程」という。）を定め、これを遵守すること並びに民間教育保育等事業者（法第二条第五項に規定する民間教育保育等事業者をいう。以下同じ。）にあっては、その事業に従事する者を二人以上置くこととする。

２　情報管理規程には、次の各号に掲げる事項を記載しなければならない。

一　基本的事項次のイからホまでに掲げる事項

イ　犯罪事実確認記録等を取り扱う者の範囲を必要最小限とすること。

ロ　犯罪事実確認書の内容の記録及び保存を極力避けるとともに、やむを得ず犯罪事実確認書の内容を記録し、又は保存する場合には、漏えい等（次条第一号及び第二号に規定する漏えい、

滅失若しくは毀損又は第三者への提供をいう。）のリスクに応じた情報管理措置を講ずること。

ハ　情報機器の種類、ネットワークの利用状況等に応じた情報管理措置を講ずること。

ニ　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こと。

ホ　組織の長が情報管理の重要性を理解し、組織的に点検及び改善を実施すること。

二　次に掲げる措置として内閣総理大臣が定めるもの

イ　組織的情報管理措置

ロ　人的情報管理措置

ハ　物理的情報管理措置

ニ　技術的情報管理措置

3　施設等運営者がある場合の学校設置者等及び施設等運営者又は共同認定（法第二十一条第一項に規定する共同認定をいう。以下同じ。）を受けようとする民間教育保育等事業者及び事業運営者（法第十九条第一項に規定する事業運営者をいう。以下同じ。）にあっては、情報管理規程に、前項に定める事項に加え、同項各号に掲げる事項に係るそれぞれの役割分担を記載しなければならない。

4　犯罪事実確認実施者等（法第十五条第一項に規定する犯罪事実確認実施者等をいう。第十四条を除き、以下同じ。）は、当該情報管理規程に係る学校設置者等に係る事業において、初めて交付申請を行う前に、電子情報処理組織（こども家庭庁の使用に係る電子計算機（入出力装置を含む。以下同じ。）と当該犯罪事実確認実施者等の使用に係る電子計算機とを電気通信回線で接続した電子情報処理組織をいう。以下この項において同じ。）を使用して、情報管理規程を内閣総理大臣に提出しなければならない。ただし、電気通信回線の故障、災害その他の理由により電子情報処理組織を使用することが困難であると認められる場合は、電子情報処理組織を使用しないで当該提出を行うことができる。

5　施設等運営者がある場合の学校設置者等及び施設等運営者が前項の規定により情報管理規程の提出を行うに当たっては、その双方が内容を確認し、及び合意しなければならない。

6　犯罪事実確認実施者等は、第四項の規定により提出した情報管理規程を変更しようとするときは、あらかじめ、次に掲げる事項を記載した届出書を内閣総理大臣に提出しなければならない。ただし、第二十四条第三項で定める軽微な変更をしようとするときは、この限りでない。

一　犯罪事実確認実施者等の氏名又は名称及び住所又は所在地並びに法人にあっては、その代表者の氏名

二　変更の内容（新旧の対照を明示すること。）及び変更の理由三変更後の情報管理規程の実施予定日

7　前項の届出は、電子情報処理組織（こども家庭庁の使用に係る電子計算機と当該届出をしようとする犯罪事実確認実施者等の使用に係る電子計算機とを電気通信回線で接続した電子情報処理組織をいう。以下この項において同じ。）を使用して行うものとする。ただし、電気通信回線の故障、災害その他の理由により電子情報処理組織を使用することが困難であると認められる場合で、かつ、電子情報処理組織を使用しないで当該届出を行うことができると認められる場合は、この限りでない。

8　施設等運営者がある場合の学校設置者等及び施設等運営者が第六項の規定により届出を行うに

当たっては、その双方が内容を確認し、及び合意しなければならない。

学校設置者等及び民間教育保育等事業者による児童対象性暴力等の防止等のための措置に関する法律施行規則第十二条第二項第二号の規定に基づきこども家庭庁長官が定める措置（令和七年こども家庭庁告示第 10 号）

1　学校設置者等及び民間教育保育等事業者による児童対象性暴力等の防止等のための措置に関する法律施行規則（令和七年内閣府令第 104 号。以下「規則」という。）第十二条第二項第二号イの組織的情報管理措置は、次に掲げるものとする。

一　情報管理措置（規則第十二条第一項に規定する情報管理措置をいう。以下同じ。）を講ずるための組織体制を整備すること。

二　犯罪事実確認記録等（学校設置者等及び民間教育保育等事業者による児童対象性暴力等の防止等のための措置に関する法律（令和六年法律第六十九号。以下「法」という。）第三十八条第一項に規定する犯罪事実確認記録等をいう。以下同じ。）が適切に取り扱われるよう、情報管理規程（規則第十二条第一項に規定する情報管理規程をいう。）を遵守し、及び犯罪事実確認記録等を取り扱う者に遵守させるために必要な措置をとること。

三　犯罪事実確認書（法第三十三条第一項に規定する犯罪事実確認書をいう。第三項第三号において同じ。）の内容を記録し、又は保存する場合には、その運用状況を事後的に確認できるようにするため、犯罪事実確認記録等の取扱いに係る記録に記載する項目を整理し、当該項目に従って犯罪事実確認記録等の取扱いに係る記録を作成すること。

四　漏えい等（規則第十二条第二項第一号ロに規定する漏えい等をいう。以下同じ。）の事案の発生又はその兆候を把握した場合に適切かつ迅速に対応するための体制を整備すること。

五　犯罪事実確認記録等の取扱状況を把握し、情報管理措置の評価、見直し及び改善に取り組むこと。

2　規則第十二条第二項第二号ロの人的情報管理措置は、犯罪事実確認記録等を取り扱う者に対し、その適正な取扱いについての周知及び必要な研修を行うこととする。

3　規則第十二条第二項第二号ハの物理的情報管理措置は、次に掲げるものとする。

一　犯罪事実確認記録等を取り扱うサーバー、コンピュータ等の重要な情報システムを管理する区域及び犯罪事実確認記録等を取り扱う事務を行う区域について、それぞれ適切な管理を行うこと。

二　犯罪事実確認記録等を取り扱う機器、電子媒体、書類等の盗難、紛失等を防止するために、適切な管理を行うこと。

三　犯罪事実確認書の内容を記録し、又は保存する場合には、犯罪事実確認記録等が記録された電子媒体、書類等の持ち運びに当たって犯罪事実確認記録等の漏えい等を防止するための方策を講ずること。

四　犯罪事実確認記録等の廃棄若しくは消去をし、又は犯罪事実確認記録等が記録された機器、電子媒体等の廃棄をする場合には、復元不可能な手段で行うこと。

4　規則第十二条第二項第二号ニの技術的情報管理措置は、次に掲げるものとする。

一　犯罪事実確認記録等を取り扱う情報システムにおいて、当該システムを使用する者が正当なアクセス権を有する者であることを識別し、当該識別した結果に基づき認証する機能を具備すること。
二　犯罪事実確認記録等を取り扱う者の範囲を限定するために、適切なアクセス制御を行うこと。
三　犯罪事実確認記録等を取り扱う情報システムを、不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用すること。
四　犯罪事実確認記録等を取り扱う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の措置を講じ、適切に運用すること。

（１）犯罪事実確認記録等を適正に管理するために必要な措置の全体像

○　法第 14 条においては、犯罪事実確認実施者等は、犯罪事実確認記録等を適正に管理しなければならないこととされており、同条の規定を具体的に担保するため、法第 11 条においては、犯罪事実確認実施者等は、犯罪事実確認記録等の管理責任者の設置その他の犯罪事実確認記録等を適正に管理するために必要な措置を講じなければならないとされている。

○　認定事業者等についても、同等の措置が求められており（法第 20 条第１項第６号及び第 27 条第１項）、これに違反した場合は適合命令及び是正命令の対象（法第 30 条）や認定取消事由（法第 32 条）に該当する。

○　犯罪事実確認記録等を適正に管理するために必要な措置の具体的内容は次の①から③までに掲げるとおり（規則第 12 条第１項及び第２項）。

①　犯罪事実確認書受領者等及び認定事業者等に求められる情報管理措置として、適正な情報管理に必要な措置が盛り込まれた情報管理規程を策定するとともに、当該規程を適切に遵守すること。

②　情報管理規程には、次のアからオまでに掲げる事項を盛り込むこと（具体的な内容については、後述の（２）において示す）。

ア　基本的事項
イ　組織的情報管理措置
ウ　人的情報管理措置
エ　物理的情報管理措置
オ　技術的情報管理措置

③　犯罪事実確認書受領者等及び認定事業者等は、②のイからオまでの措置について、次の（ア）又は（イ）に掲げる２つの水準に基づく措置から選択して情報管理規程に盛り込むこと。可能な限り、（ア）の標準的措置に基づく規程とするとともに、これを満たすように努めること。

（ア）　標準的措置

実施に困難をきたすなどの特別な事由がない限りは、相応に実施されるべき基本的水準の措置。

（イ） 最低限求められる措置

小規模事業者等の負担に配慮し、（ア）の水準を一部緩和した水準の措置（個人情報保護法における安全管理措置の水準と同等以上)。全ての事業者が、施設・事業単位で満たすべきもの。

（２）犯罪事実確認記録等を適正に管理するために必要な措置の具体的内容

○ 情報管理規程において定める（１）②アからオまでに掲げる事項等について、その具体的内容を順次示す。

ア 基本的事項

○ 基本的事項として、次の(ア)から(キ)までの基本原則を遵守しなければならない（規則第 12 条第２項)。特に、情報漏えい等のリスクに鑑み、(ア) 及び (イ) を徹底することが重要である。

（ア） 犯罪事実確認記録等の取扱者は必要最小限とすること

（イ） 犯罪事実確認書の内容の記録・保存を極力避けること

（ウ） やむを得ず記録・保存する場合には、リスクに応じた情報管理措置を行うこと

（エ） 情報機器の種類、ネットワークの状況等に応じた情報管理措置を講じること

（オ） 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こと

（カ） 組織の長自ら情報管理の重要性を理解し、組織的に点検・改善を実施すること

（キ） 法に定める情報管理措置に関する規定を遵守すること

○ (ウ)及び(エ)の具体的内容については、次の(一)から(三)までに掲げるとおり。

(一) 使用する情報機器の要件（(エ)関係）

・ 業務用端末であること（専用端末の使用を推奨、私用端末は不可）

・ 端末 OS 及びアプリケーションは、最新のバージョンを維持し、提供ベンダーのサポート期間が切れたものは利用しないこと

・ 複数のセキュリティ対策を組み合わせることで、一定のセキュリティ水準を確保すること（アンチウイルスソフトウェア（特に PC）等の導入、キャリア通信会社やインターネットプロバイダのセキュリティサービスの活用など)

(二) ネットワークの要件（(エ)関係）

・ ウイルスの侵入や情報漏えいを防止するため、業務上不要なインターネット通信を制限すること

・ 事業者の組織的な管理下にあるネットワークを活用する場合には、複数の対策を行う多層防御を実施すること

(三) クラウドサービスの要件（(ウ)・(エ)関係）

・ クラウドサービスの活用は、真にやむを得ない場合に限り認めることとし、利用に当たっては、アクセス管理、セキュリティ設定、データの暗号化等の必要な対策を講じること

・　ISMAP 基準[35]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ことを原則とすること

○　（オ）の具体的内容については、次の図表のとおり。

図表 79 犯罪事実確認記録等の取扱いの手順に応じた必要な対応

※網掛けは法関連システムで処理する手続

手順	情報管理措置の主な留意点
①事前準備	・　犯罪事実確認記録等にアクセスできる者を最小限に限定・明確化する。
②犯罪事実確認書の交付申請	・　法関連システム上での申請を原則とする。 ・　不正ログイン等を防ぐため、ログインに当たっては、Ｇビズ ID・認証用アプリによる多要素認証を原則とする。
③従事者への事前通知（犯歴ありの場合）	・　法関連システム上での通知を原則。 ・ 従事者本人の真正性を可能な限り高めるため、マイナンバーカードなどの多要素認証を活用した身元確認及び当人認証を原則とする。 ・　本人通知書の様式は、犯罪事実確認書の様式と同じものを活用する。
④犯罪事実確認書の交付	・　法関連システム上での閲覧により交付を受けることを原則とする。 ・　犯罪事実確認書については、万が一のぞき見、漏えい等があった場合に備え、本人が特定できる氏名等の情報は記載せず、法関連システムで別管理している従事者の識別番号（申請番号を想定）のみを記載し、事業者が別途従事者名と照合できるようにする。
⑤（やむを得ない場合の） ・犯罪事実確認記録の作成 ・犯罪事実確認記録等の事業者間又は事業者内での伝達・利用 ・犯罪事実確認記録等の保存	・　法関連システムにログインすれば、法で定める期限内に限り、いつでも何度でも犯罪事実確認書を閲覧することを可能とし、情報の転記等による電子ファイル又は紙の記録・保存・伝達・利用は極力行わない。 ※　事業者内での伝達・利用においても、あらかじめ閲覧権限を設定された者が法関連システムにログインして確認できるようにする。 ※　県費負担教職員、施設等運営者又は共同認定の場合に事業者間で情報共有する際には、法関連システム内での権限設定により閲覧できるようにするとともに、閲覧できる者にアクセス制限をかける。 ・　やむを得ず記録等を作成・伝達・利用・保存する場合には、リスクに応じた管理措置を求める。
⑥犯罪事実確認記録等の廃棄・消去	・　法関連システム内で保管する犯罪事実確認書は、法で定める期限に、自動で消去される機能を付加する。 ただし、離職等の場合は、国においてその時期を把握することが難しく、事業者において消去の手続が必要。 ・　犯罪事実確認記録等は法により第三者提供を禁止されているため、廃棄を委託

[35] ISMAP（イスマップ、Information system Security Management and Assessment Program）基準は、国際標準等を踏まえ、クラウドサービスに対して要求する情報セキュリティ管理・運用の基準をいう。

	することはできない。
⑦帳簿の作成	・　帳簿には犯罪事実確認書の受領日等の情報が含まれ、法関連システム上で自動生成される。
⑧定期報告	・　情報管理措置の「標準的措置」及び「最低限求められる措置」の実施状況（必須報告事項）やその他の事項（任意報告事項）を、情報管理措置の報告事項と併せて報告する。 ・　報告方法は年に一度、法関連システムにおいて、チェックボックス形式を基本とする報告により行う。
⑨漏えい等が発生した際の対応	・　漏えいその他の内閣総理大臣に報告すべき事案は、①犯罪事実確認記録等の漏えい等、②法第 12 条違反の事案、③特定性犯罪事実関連情報の漏えい等（高度に暗号化されたものの漏えい等を除く）
⑩その他	・　情報管理措置の変更の届出、是正命令への対応完了報告も、基本的に法関連システム上で対応する。

※　適切な運用を確保するため、犯罪事実確認記録等の取扱記録（犯罪事実確認書の閲覧日時・者、犯罪事実確認記録の作成状況等）を作成し、適切かつ安全に管理されていることを責任者が定期的に確認するとともに、取扱状況の検証を可能とすることが重要。

イ　組織的情報管理措置

○　組織的情報管理措置として、次の(ア)から(オ)までの措置を講じなければならない。

（ア）　組織体制の整備

○　情報管理措置を講ずるための組織体制を整備しなければならない。本措置を達成するための手段・方法を次の表の「標準的措置」及び「最低限求められる措置」に示す（下線部は、「標準的措置」及び「最低限求められる措置」の主な違いを指す。以下同じ。）。

図表 80　組織体制の整備

標準的措置	最低限求められる措置
(イ) 犯罪事実確認記録等の取扱いに関する責任者を設置し、事業者における情報管理を統括する。	(イ)　犯罪事実確認記録等の取扱いに関する責任者を設置し、事業者における情報管理を統括する。
(ロ)　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（責任者が担当者を兼ねることもあり得る）。	(ロ)　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（責任者が担当者を兼ねることもあり得る）。
(ハ)　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。	
(ニ)　犯罪事実確認記録等を取り扱う責任者、担当者、その他従事者（以下「取扱者」という。）を特	(ハ)　犯罪事実確認記録等を取り扱う責任者、担当者、その他従事者（以下「取扱者」という。）を特

標準的措置	最低限求められる措置
定し、その役割・業務を明確化する。なお、その際、犯罪事実確認記録等を取り扱う従事者は、業務実施に必要となる最低限の者にとどめ、業務実施に不要な者が犯罪事実確認記録等を取り扱うことがないようにする。 （責任者、担当者以外に犯罪事実確認記録等を取り扱う者の例） ・　人事部門のうち、責任者が認めた者 ・　情報システム部門のうち、責任者が認めた者 ・　各部署のマネージャーのうち、責任者が認めた者 （ホ）　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責任者への報告連絡体制を整備する。 （ヘ）　犯罪事実確認記録等の漏えい等の事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための報告連絡体制を整備する。 （ト）　犯罪事実確認記録等を複数の部署で取り扱う場合、各部署の役割分担及び責任を明確化する。	定し、その役割・業務を明確化する。なお、その際、犯罪事実確認記録等を取り扱う従事者は、業務実施に必要となる最低限の者にとどめ、業務実施に不要な者が犯罪事実確認記録等を取り扱うことがないようにする。 （責任者、担当者以外に犯罪事実確認記録等を取り扱う者の例） ・　人事部門のうち、責任者が認めた者 ・　情報システム部門のうち、責任者が認めた者 ・　各部署のマネージャーのうち、責任者が認めた者 （ニ）　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責任者への報告連絡体制を整備する。 （ホ）　犯罪事実確認記録等の漏えい等の事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための報告連絡体制を整備する。 （ヘ）　犯罪事実確認記録等を複数の部署で取り扱う場合、各部署の役割分担及び責任を明確化する。

（イ）　情報管理規程に基づく運用

○　情報管理規程に基づき犯罪事実確認記録等を取り扱わなければならない。また、その運用状況を事後的に確認できるようにするため、取扱記録を作成することが重要である。本措置を達成するための手段・方法を次の表の「標準的措置」及び「最低限求められる措置」に示す。

図表 81　情報管理規程に基づく運用

標準的措置	最低限求められる措置
（イ）　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責任者が定期的に確認するとともに、犯罪事実確認記録等の取扱いの検証を可能とする。 （整備すべき取扱記録の例） ・　犯罪事実確認書の閲覧の状況（法関連システムで自動記録） ・　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の状況 ・　犯罪事実確認記録を情報システムで取り扱う場	（イ）　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責任者が定期的に確認する。 （整備すべき取扱記録の例） ・　犯罪事実確認書の閲覧の状況（法関連システムで自動記録） ・　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の状況 ・　犯罪事実確認記録を情報システムで取り扱う場

標準的措置	最低限求められる措置
合、その利用状況（状況に応じ、ログイン実績・アクセスログ等） ・　犯罪事実確認記録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伝達の場合に限る） ・　犯罪事実確認記録等の廃棄・消去の状況（犯罪事実確認書については、法関連システムで消去）	合、その利用状況（状況に応じ、ログイン実績・アクセスログ等） ・　犯罪事実確認記録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伝達の場合に限る） ・　犯罪事実確認記録等の廃棄・消去の状況（犯罪事実確認書については、法関連システムで消去）

（ウ）　犯罪事実確認記録等の取扱記録の記載項目の整理

○　犯罪事実確認記録等の取扱記録に記載する項目を整理しなければならない。例えば、犯罪事実確認記録等の種類、責任者・取扱部署、アクセス権を有する者、犯罪事実確認記録等の所在等をあらかじめ明確化しておくことにより、犯罪事実確認記録等の取扱状況を把握可能とすることが重要である。本措置を達成するための手段・方法を次の表の「標準的措置」及び「最低限求められる措置」に示す。また、取扱記録の様式は資料編別紙６を参照すること。

図表 82　犯罪事実確認記録等の取組記録の記載項目の整理

標準的措置	最低限求められる措置
（イ）　事業者において取り扱う犯罪事実確認記録等の種類ごとに、以下のような項目をあらかじめ明確化しておくことにより、取扱状況を把握可能とする。 （記録対象情報の種類） ・　犯罪事実確認書 ・　犯罪事実確認記録 （記録項目） ・　記録対象情報ごとの取扱責任者・取扱部署、アクセス権者 ・　犯罪事実確認記録等の所在（バックアップがある場合はその所在を含む） ・　利用目的 等	（イ）　事業者において取り扱う犯罪事実確認記録等の種類ごとに、以下のような項目をあらかじめ明確化しておくことにより、取扱状況を把握可能とする。 （記録対象情報の種類） ・　犯罪事実確認書 ・　犯罪事実確認記録 （記録項目） ・　記録対象情報ごとの取扱責任者・取扱部署、アクセス権者 ・　犯罪事実確認記録等の所在（バックアップがある場合はその所在を含む） ・　利用目的 等

（エ）　漏えい等の事案に対応する体制の整備

○　漏えい等の事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための体制を整備しなければならない。本措置を達成するための手段・方法を次の表の「標準的措置」及び「最低限求められる措置」に示す。なお、漏えい等の事案への対応事項詳細は本章「４．漏えい等の重大事態のこども家庭庁への報告（法第 13 条及び第 27 条第２項関係）」を参照すること。

図表 83　漏えい等の事案に対応する体制の整備

標準的措置	最低限求められる措置
（イ）　組織の長が主導して、漏えい等の事案の発生時の対応を行うための体制を整備するとともに、対応手順を明確化する。 （漏えい等の事案の発生時の対応の例） ・　情報漏えいの事実の確認 ・　被害の拡大防止 ・　影響範囲の特定 ・　影響を受ける可能性のある本人への通知 ・　こども家庭庁等への報告 ・　事実関係の調査及び原因の究明 ・　再発防止策の検討及び決定 ・　（必要に応じて）事実関係及び再発防止策等の公表	（イ）　組織の長が主導して、漏えい等の事案の発生時の対応を行うための体制を整備するとともに、対応手順を明確化する。 （漏えい等の事案の発生時の対応の例） ・　情報漏えいの事実の確認 ・　被害の拡大防止 ・　影響範囲の特定 ・　影響を受ける可能性のある本人への通知 ・　こども家庭庁等への報告 ・　事実関係の調査及び原因の究明 ・　再発防止策の検討及び決定 ・　（必要に応じて）事実関係及び再発防止策等の公表

（オ）　犯罪事実確認記録等の取扱状況の把握及び情報管理措置の見直し

○　犯罪事実確認記録等の取扱記録等に基づき、情報管理措置の評価、見直し及び改善に取り組まなければならない。具体的には、情報管理措置の内容に従って、適正に情報管理が行われているかを定期的に評価し、問題等が発見された場合には速やかに内容の見直しや運用の改善に取り組むことが重要である。本措置を達成するための手段・方法を次の表の「標準的措置」及び「最低限求められる措置」に示す。

図表 84　犯罪事実確認記録等の取扱状況の把握及び情報管理措置の見直し

標準的措置	最低限求められる措置
（イ）　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。 （ロ）　自己点検の際、責任者は犯罪事実確認記録等の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、必要に応じ規程を変更する。 ※　責任者以外の点検者（取扱者である必要はない）が参加することが望ましい。 （監査の方法の例） ・　事業者内の犯罪事実確認記録等を取り扱う部署とは別の部署による内部監査を実施 ・　外部の主体による監査活動がある場合には、外部監査活動と合わせて監査を実施 ・　情報処理安全確保支援士等のセキュリティ資格	（イ）　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、定期的に自己点検又は他部署等による監査を実施する。 （ロ）　自己点検の際、責任者は犯罪事実確認記録等の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、必要に応じ規程を変更する。 ※　責任者以外の点検者（取扱者である必要はない）が参加することが望ましい。 （監査の方法の例） ・　事業者内の犯罪事実確認記録等を取り扱う部署とは別の部署による内部監査を実施

標準的措置	最低限求められる措置
を保有する者が実施	

ウ　人的情報管理措置

○　従事者に、犯罪事実確認記録等の適正な取扱いを周知徹底するとともに、適切な研修を行うことが求められる。本措置を達成するための手段・方法を次の表の「標準的措置」及び「最低限求められる措置」に示す。

図表 85　講ずべき人的情報管理措置の内容

標準的措置	最低限求められる措置
（イ）　犯罪事実確認記録等の取扱いに関する留意事項について、従事者に着任時及び定期的に研修等を行う。	（イ）　犯罪事実確認記録等の取扱いに関する留意事項について、従事者に着任時及び定期的に研修等を行う。
（ロ）　研修を実施した旨は、記録し、責任者が定期的に確認する。	（ロ）　研修を実施した旨は、記録し、責任者が定期的に確認する。
（ハ）　研修以外でも（人事異動の多い時期などに）定期的に意識啓発を行う。	（ハ）　研修以外でも（人事異動の多い時期などに）定期的に意識啓発を行う。
（ニ）　犯罪事実確認記録等についての秘密保持に関する事項や犯罪事実確認記録等の情報管理規程に違反した場合の人事上の取扱いを就業規則等に盛り込む。	（ニ）　犯罪事実確認記録等についての秘密保持に関する事項や犯罪事実確認記録等の情報管理規程に違反した場合の人事上の取扱いを就業規則等に盛り込む。
（ホ）　退職時に、退職後も永久的に情報を漏らしてはならないことを確認する。 ※　従事者の就業形態（ボランティア、その他派遣職員等）が複雑な構成となっている場合、研修、規則等の管理も複雑となるが、各形態に係る制度や実情を踏まえて適切に対応する。	（ホ）　退職時に、退職後も永久的に情報を漏らしてはならないことを確認する。 ※　従事者の就業形態（ボランティア、その他派遣職員等）が複雑な構成となっている場合、研修、規則等の管理も複雑となるが、各形態に係る制度や実情を踏まえて適切に対応する。
（研修等の内容の例） ・　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内容 ・　情報管理規程違反若しくは漏えい等の事実又は兆候を把握した場合の責任者への報告連絡体制 ・　関係法令や社内規程等の変更があった場合はその内容 ・　禁止事項と罰則 ※　事業所で独自に評価した想定リスクとその対処方法等を盛り込んだ説明資料を作成しておくと効果的である。必要に応じて、こども家庭庁が作成する研修教材や情報処理推進機構（IPA）等公的機関が無料で公開している情報セキュリティの研修用ドキュメント等も活用	（研修等の内容の例） ・　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内容 ・　情報管理規程違反若しくは漏えい等の事実又は兆候を把握した場合の責任者への報告連絡体制 ・　関係法令や社内規程等の変更があった場合はその内容 ・　禁止事項と罰則 ※　こども家庭庁が作成する研修教材や情報処理推進機構（IPA）等公的機関が無料で公開している情報セキュリティの研修用ドキュメント等を活用することも可能。

標準的措置	最低限求められる措置
する。 （研修等の実施方法の例） ・　入社時、昇進時等、配転時研修などの一環として実施。 ・　関係法令や社内規程の改正等に伴う研修の一環 ・　e-ラーニングによる実施（理解度確認付 e-ラーニングなど、従事者等全員の受講が確認できるように工夫することも考えられる。） ・　研修会の実施（可能であれば座学だけでなくディスカッションやロールプレイ、訓練、理解度確認テスト等を実施することが望ましい。） （研修以外での意識啓発の例） ・　定例の会議等での説明資料の配布、社内電子掲示板等への掲示、電子メールでの送付 ・　定期的に行われる朝礼や会議等での、犯罪事実確認記録等の取扱いに関する注意喚起・意識の共有	（研修等の実施方法の例） ・　入社時、昇進時等、配転時研修などの一環として実施。 ・　関係法令や社内規程の改正等に伴う研修の一環 ・　e-ラーニングによる実施（理解度確認付 e-ラーニングなど、従事者等全員の受講が確認できるように工夫することも考えられる。） ・　研修会の実施（可能であれば座学だけでなくディスカッションやロールプレイ、訓練、理解度確認テスト等を実施することが望ましい。） （研修以外での意識啓発の例） ・　定例の会議等での説明資料の配布、社内電子掲示板等への掲示、電子メールでの送付 ・　定期的に行われる朝礼や会議等での、犯罪事実確認記録等の取扱いに関する注意喚起・意識の共有

エ　物理的情報管理措置

○　物理的情報管理措置として、次の(ア)から(エ)までの措置を講じなければならない。

（ア）　犯罪事実確認記録等を取り扱う区域の管理

○　犯罪事実確認記録が保存されるデータベース等を取り扱うサーバ、メインコンピュータ等の重要な情報システムを管理する区域（以下「管理区域」という。）及び犯罪事実確認記録等を取り扱う事務を行う区域（以下「取扱区域」という。）について、それぞれ適切な管理を行わなければならない。本措置を達成するための手段・方法を次の表の「標準的措置」と「最低限求められる措置」に示す（下線部は、「標準的措置」と「最低限求められる措置」の主な違いを指す）。

図表 86　犯罪事実確認記録等を取り扱う区域の管理

標準的措置	最低限求められる措置
（イ）　管理区域がある場合、権限を有しない者の管理区域への立入りの防止等、適切な管理を行う。 （管理区域の管理手法の例） ・　権限を有しない者が入室・閲覧しないように施錠（同時に、権限を有しない者が入室・閲覧しないように視線を配るなど、視認性を高める） ・　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（IC カード、ナンバーキー等による	（イ）　管理区域がある場合、権限を有しない者の管理区域への立入りの防止等、適切な管理を行う。 （管理区域の管理手法の例） ・　権限を有しない者が入室、閲覧しないように施錠（同時に、権限を有しない者が入室・閲覧しないように視線を配るなど、視認性を高める） ・　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（IC カード、ナンバーキー等による

標準的措置	最低限求められる措置
入退室管理システムの設置等） ・　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 ※　入退室管理システムの認証方法としては、ICカード認証、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入力の付与等があり、アンチパスバック機能[36]も併用できる。なお、これらのシステムのうち、製品によっては、入退出者や入退出時刻等を記録する機能を持つものもあるが、その記録を保存することは「視認性の確保」にもつながる。	入退室管理システムの設置等） ・　持ち込む機器等の制限 ※　入退室管理システムの認証方法としては、ICカード認証、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入力の付与等があり、アンチパスバック機能も併用できる。なお、これらのシステムのうち、製品によっては、入退出者や入退出時刻等を記録する機能を持つものもあるが、その記録を保存することは「視認性の確保」にもつながる。
（ロ）　取扱区域を限定し、権限を有しない者の取扱区域への立入りや、犯罪事実確認記録等の閲覧等の防止等、適切な管理を行う。	（ロ）　取扱区域を特定し、権限を有しない者による犯罪事実確認記録等の閲覧等の防止等、適切な管理を行う。
（取扱区域の管理手法の例） ・　権限を有しない者が入室、閲覧しないように施錠（同時に、権限を有しない者が入室・閲覧しないように視線を配るなど、視認性を高める） ・　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 ・　持込む機器等の制限 ・　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	（取扱区域の管理手法の例） ・　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 ※　場所の制約等により区域の限定が困難な場合は、区域を特定して、時間帯で利用を区切るなどの工夫をするとともに、後述の「（イ）機器及び電子媒体等の盗難等の防止等」の項目に基づいて、アクセス権を有しない者が容易に犯罪事実確認記録等を閲覧等できないような措置を講ずる。

（イ）　機器及び電子媒体等の盗難等の防止

○　犯罪事実確認記録等を取り扱う機器、電子媒体、書類等の盗難、紛失等を防止するために、適切な管理を行わなければならない。本措置を達成するための手段・方法を次の表の「標準的措置」及び「最低限求められる措置」に示す。

[36] 入室していないＩＤでは退室できず、退室していないＩＤでは入室できないなどの機能。これにより、同じＩＤで、2回連続で入室又は2回連続で退室ができないなど、共連れを防止できる。

図表 87　機器及び電子媒体等の盗難等の防止

標準的措置	最低限求められる措置
(イ)　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、紛失等を防止するための措置を講じる。 （盗難、紛失等を防止するための措置の例） ・　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し、もしく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。	(イ)　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、紛失等を防止するための措置を講じる。 （盗難、紛失等を防止するための措置の例） ・　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し、もしく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。
(ロ)　盗難、紛失時に情報漏えいを防止するための措置を講じる。 （盗難、紛失時に情報漏えいを防止するための措置の例） ・　犯罪事実確認記録等の電子ファイルの暗号化、パスワードによる保護等を行った上での保存 ・　（携帯端末の場合）紛失時の端末の位置の特定 ・　（携帯端末の場合）紛失時の遠隔操作による端末の保護 ・　（携帯端末の場合）紛失時の遠隔操作によるデータの消去	(ロ)　盗難、紛失時に情報漏えいを防止するための措置を講じる。 （盗難、紛失時に情報漏えいを防止するための措置の例） ・　犯罪事実確認記録等の電子ファイルの暗号化、パスワードによる保護等を行った上での保存 ・　（携帯端末の場合）紛失時の端末の位置の特定 ・　（携帯端末の場合）紛失時の遠隔操作による端末の保護 ・　（携帯端末の場合）紛失時の遠隔操作によるデータの消去
(ハ)　犯罪事実確認記録等を取り扱う機器を紛失した場合は、即時に法関連システム及び情報システムのログインパスワードを変更するとともに、アクセス権の解除を行う。	(ハ)　犯罪事実確認記録等を取り扱う機器を紛失した場合は、即時に法関連システム及び情報システムのログインパスワードを変更するとともに、アクセス権の解除を行う。

（ウ）　電子媒体等を持ち運ぶ場合の漏えい等の防止

○　犯罪事実確認記録等が記録された電子媒体、書類等を持ち運ぶ場合に、情報の漏えいを防止するための安全な方策を講じなければならない。本措置を達成するための手段・方法を次の表の「標準的措置」及び「最低限求められる措置」に示す。

○　なお、持ち運びがやむを得ない場合とは、事業所の機器が災害、障害等により一時的に情報の閲覧ができない状態の場合において、早急に当該情報を用いた対応が求められる際に電子媒体や書類等による記録の伝達・利用を行うことなどが考えられる。

図表 88　電子媒体等を持ち運ぶ場合の漏えいの防止

標準的措置	最低限求められる措置
（イ）　やむを得ない場合のみ、紛失・盗難等を防ぐための安全な方策を講じた上で、犯罪事実確認記録が記載された電子媒体や書類等の持ち運びを行う。その際、持ち運びや伝達等の状況に係る取扱記録を作成し、責任者が定期的に確認する。	（イ）　やむを得ない場合のみ、紛失・盗難等を防ぐための安全な方策を講じた上で、犯罪事実確認記録が記載された電子媒体や書類等の持ち運びを行う。その際、持ち運びや伝達等の状況に係る取扱記録を作成し、責任者が定期的に確認する。
（ロ）　犯罪事実確認記録を電子媒体に記録する場合、その電子媒体の管理状況の確認を定期的に行う。	（ロ）　犯罪事実確認記録を電子媒体に記録する場合、その電子媒体の管理状況の確認を定期的に行う。
（紛失・盗難等を防ぐための措置の例） ・　データの暗号化 ・　パスワードの設定 ・　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（資料に、通し番号を付すことで遺漏なく回収することが可能となる）。従事者等の手元に紙媒体を残させないことにより、紙媒体を持ち出すことができない状態にする。 ・　情報の持ち運びを行う場合は、対象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。	（紛失・盗難等を防ぐための措置の例） ・　データの暗号化 ・　パスワードの設定 ・　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（資料に、通し番号を付すことで遺漏なく回収することが可能となる）。従事者等の手元に紙媒体を残させないことにより、紙媒体を持ち出すことができない状態にする。

（エ）　犯罪事実確認記録等の破棄及び消去並びに機器・電子媒体等の廃棄

○　犯罪事実確認記録等の廃棄及び消去並びに犯罪事実確認記録等が記録された機器・電子媒体等の廃棄を行う場合は、復元不可能な手段で行わなければならない。本措置を達成するための手段・方法を次の表の「標準的措置」及び「最低限求められる措置」に示す。

図表 89　犯罪事実確認記録等の廃棄及び消去並びに機器・電子媒体等の廃棄

標準的措置	最低限求められる措置
（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、犯罪事実確認記録が保存された電子データの消去を行う場合） 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復元できない形にし	（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、犯罪事実確認記録が保存された電子データの消去を行う場合） 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復元できない形にし

標準的措置	最低限求められる措置
て消去する。その際、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についての取扱記録を作成し、責任者が定期的に確認する。 （容易に復元できない状態での機器、電子媒体等の廃棄方法の例） ・　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の手段を採用する。 ※　記録媒体からデータを消去しただけでは復元されるおそれがあるため （復元不可能な手段での書類等の廃棄方法の例） ・　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。 ・　犯罪事実確認記録等の重要度に応じて、より復元を困難とするため、クロスカット（縦方向と横方向の両方から裁断する）方式のシュレッダーを利用するなど、かけることができる予算も踏まえながら、シュレッダーの機能性について検討する。 ・　犯罪事実確認記録等を廃棄するまで保管するゴミ箱は、取り出すことができない鍵付きゴミ箱に限定する。	て消去する。その際、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についての取扱記録を作成し、責任者が定期的に確認する。 （容易に復元できない状態での機器、電子媒体等の廃棄方法の例） ・　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の手段を採用する。 ※　記録媒体からデータを消去しただけでは復元されるおそれがあるため （復元不可能な手段での書類等の廃棄方法の例） ・　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。

オ　技術的情報管理措置

○　技術的情報管理措置として、次の(ア)から(エ)までの措置を講じなければならない。

（ア）　アクセス者の識別及び認証

○　犯罪事実確認記録等を取り扱う情報システムにおいては、①組織の中でも業務上必要な者のみにアクセス権限を付与し、アクセス者として識別した上で、②正当なアクセス権を有する者であることを認証する機能を具備しなければならない。本措置を達成するための手段・方法を次の表の「標準的措置」及び「最低限求められる措置」に示す。

図表 90　アクセス者の識別及び認証

標準的措置	最低限求められる措置
（イ）　法関連システム及び情報システムを使用する従事者の識別及び認証を行う。 （識別及び認証手法の例） ・　犯罪事実確認記録等を取り扱う法関連システム及び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、	（イ）　法関連システム及び情報システムを使用する従事者の識別及び認証を行う。 （識別及び認証手法の例） ・　犯罪事実確認記録等を取り扱う法関連システム及び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、

標準的措置	最低限求められる措置
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。 ※　パスワードを設定する際は、容易に推測可能なものは避け、一定の複雑性を持たせたうえで、同一のパスワードを複数のシステムやアプリケーションで使いまわさないこと。	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。 ※　パスワードを設定する際は、容易に推測可能なものは避け、一定の複雑性を持たせたうえで、同一のパスワードを複数のシステムやアプリケーションで使いまわさないこと。

（イ）　アクセス制御

○　犯罪事実確認記録等の取扱者の範囲を限定するために、適切なアクセス制御を行わなければならない。本措置を達成するための手段・方法を次の表の「標準的措置」及び「最低限求められる措置」に示す。

図表 91　アクセス制御

標準的措置	最低限求められる措置
（イ）　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し、アクセス制御を行う。	（イ）　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し、アクセス制御を行う。
（ロ）　情報システムに犯罪事実確認記録を保存する場合、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アクセス制御を行う。 （アクセス制御の例） ・　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設定 ・　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（複数のネットワークを構築し、犯罪事実確認記録等を取り扱う回線については専用ネットワークとする等）を実施する。 ※　ネットワークを分離することで、１つのネットワークに不正アクセス等があった場合でも、その他のネットワークに保管される犯罪事実確認記録等へは直接アクセスできないため、不正アクセスやウイルス感染に対する被害の拡散防止につながる。	（ロ）　情報システムに犯罪事実確認記録を保存する場合、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アクセス制御を行う。 （アクセス制御の例） ・　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設定
（ハ）　異動又は退職する者等が発生した際には、即時に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ための手続を行う。	（ハ）　異動又は退職する者等が発生した際には、即時に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ための手続を行う。

標準的措置	最低限求められる措置
（異動又は退職する者等が発生した際のアクセス制御の例） ・　定期的にアクセス権を有する者の管理状況の確認を実施し、不要な者がいた場合、即時に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	（異動又は退職する者等が発生した際のアクセス制御の例） ・　定期的にアクセス権を有する者の管理状況の確認を実施し、不要な者がいた場合、即時に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

（権限者及び権限の整理）

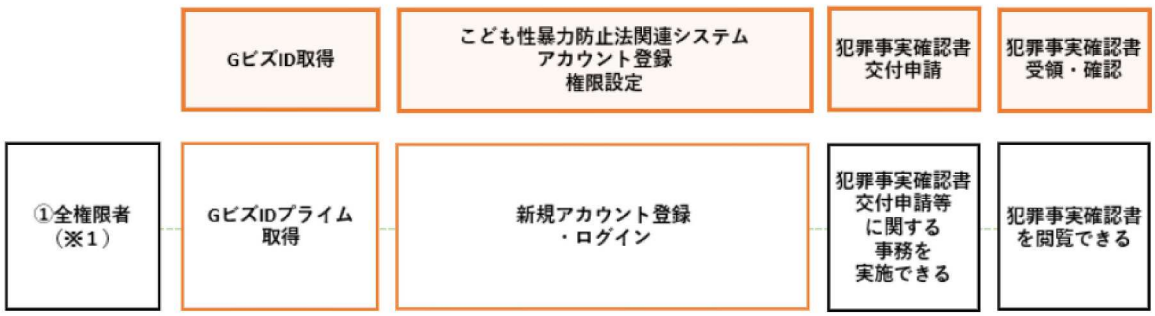
○　こども性暴力防止法関連システムにおいて、犯罪事実確認書の閲覧等を行うに当たっては、事業規模や情報管理の在り方に応じて、次の図表を参考としつつ、「犯罪事実確認書の閲覧」「権限設定」「事務手続」の３つの階層に応じた権限設定を行うとともに、初期のアカウント登録等を行う。

○　次の図表中「権限設定」の権限を有する者（全権限者又は権限設定権者）が、事業者内で法に基づく事務等を行う従事者について、いずれの権限者となるか設定する。犯罪事実確認書の閲覧権限は、事業者内で最小限の人数となるよう留意すること（小規模事業者においては１人に限るなど）。より詳細な権限者及び権限の整理については、別紙７を参照すること。

図表 92　権限者及び権限

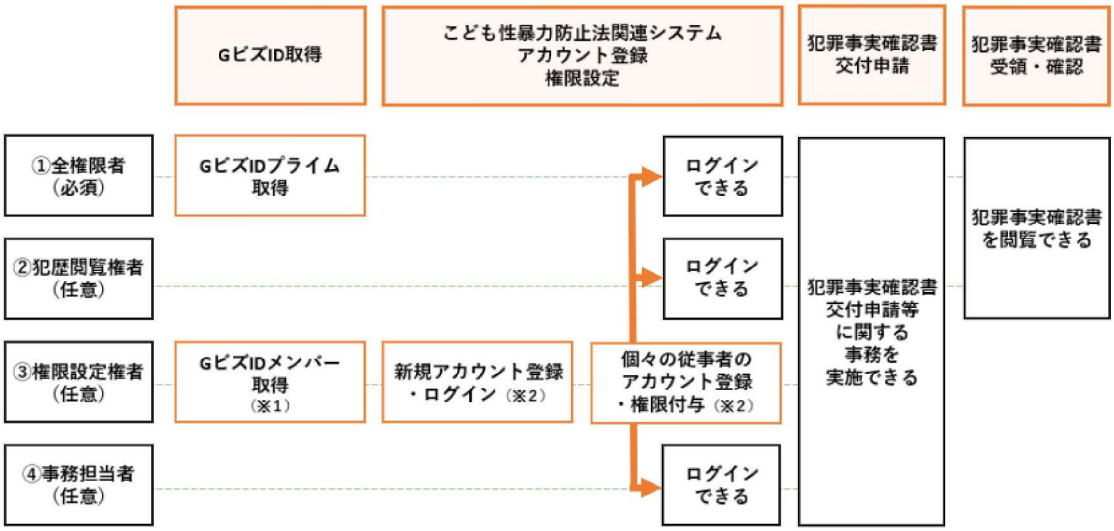
権限者	権限	権限が割り当てられる者の職務のイメージ
①全権限者	**犯罪事実確認書の閲覧** **権限設定** 申請手続等の事務	組織の総責任者、準責任者 （行政の人事担当部長、法人理事長等）
②犯歴確認権者	**犯罪事実確認書の閲覧** 申請手続等の事務	現場責任者 （公立学校の校長、複数園を運営する法人内の園長等）
③権限設定権者	**権限設定** 申請手続等の事務	情報システムの責任者
④事務担当者	申請手続等の事務	その他の従事者 （人事担当等）

図表 93　権限者ごとに行う事務フロー①
全権限者が一人で犯罪事実確認書の閲覧その他の事務を行う場合



※１　犯罪事実確認を含む法に基づく手続について統括的な責任を有する者を、事業者で１名設置する。法人の場合は理事長等の法人代表者、法人以外の場合は事業主等が想定される。

図表 94　権限者ごとに行う事務フロー②
全権限者を含む複数名が犯罪事実確認書の閲覧その他の事務を行う場合



※１　Ｇビズ ID メンバーの第一管理者を取得する。

※２　アカウント登録・ログイン、個々の従事者のアカウント登録・権限付与についても、全権限者が行うことは可能。

（ウ）　外部からの不正アクセス等の防止

○　犯罪事実確認記録等を取り扱う情報システムを、外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用しなければならない。本措置を達成するための手段・方法を次の表の「標準的措置」及び「最低限求められる措置」に示す。

図表 95　外部からの不正アクセス等の防止

標準的措置	最低限求められる措置
（イ）　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、使用期間において提供ベンダーの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。	（イ）　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、使用期間において提供ベンダーの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。
（ロ）　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。	（ロ）　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。
（ハ）　ウイルスの侵入や情報漏えいを防止するため、業務上不要なインターネット通信を制限する。	（ハ）　ウイルスの侵入や情報漏えいを防止するため、業務上不要なインターネット通信を制限する。

標準的措置	最低限求められる措置
(ニ)　ログ等の定期的な分析により、不正アクセス等を検知する。 （不要なインターネット通信制限の例） ・　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、セキュリティソフトウェア製品等の活用 ・　ネットワークの分離（複数のネットワークを構築し、犯罪事実確認記録等を取り扱う回線については専用ネットワークとする等）及びアクセス制限を実施 ※　ネットワークを分離することで、１つのネットワークに不正アクセス等があった場合でも、その他のネットワークに保管される犯罪事実確認記録等へは直接アクセスできないため、不正アクセスやウイルス感染に対する被害の拡散防止につながる。	(ニ)　責任者によるログ等の定期的な確認により、不正アクセス等を検知する。 （不要なインターネット通信制限の例） ・　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、セキュリティソフトウェア製品等の活用
(ホ)　組織的に管理されたネットワークを設置している場合は、「(ウ) 外部からの不正アクセスの防止」の(イ)～(ハ)を含む複数の対策を組み合わせた多層防御を実施する。 （多層防御を構成する対策の例） ・　ファイアウォールの設置 ・　ネットワークの分離及びアクセス制限 ・　ファイルや通信データの暗号化 ・　IDS[37]／IPS[38]等による不正アクセスの検知又は遮断 ・　DLP[39]を用いた情報の漏えい、滅失又は毀損の防止 （上記以外に外部からの不正アクセス等を防止するための措置の例） ・　情報システムに犯罪事実確認記録を保存する場合は、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。	(ホ)　組織的に管理されたネットワークを設置している場合は、「(ウ) 外部からの不正アクセスの防止」の(イ)～(ハ)を含む複数の対策を組み合わせた多層防御を実施する。 （多層防御を構成する対策の例） ・　ファイアウォールの設置 ・　ネットワークの分離及びアクセス制限 ・　ファイルや通信データの暗号化

[37] Intrusion Detection System：侵入検知システム。システムやネットワークに対する不正なアクセスなどを検知して管理者に通知する技術。
[38] Intrusion Prevention System：侵入防御システム。システムやネットワークに対する不正なアクセスなどを検知して自動的に遮断する技術。
[39] Data Loss Prevention：データ漏えい防止機能。機密情報や重要なデータを監視し、情報の漏えい、滅失又は毀損を防止する技術。

（エ） 情報システムの使用に伴う漏えい等の防止

○ 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の措置を講じ、適切に運用しなければならない。本措置を達成するための手段・方法を次の表の「標準的措置」及び「最低限求められる措置」に示す。

図表 96 情報システムの使用に伴う漏えい等の防止

標準的措置	最低限求められる措置
（イ） 情報システムの使用に伴う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。）。	（イ） 情報システムの使用に伴う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。）。
（ロ） 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。	（ロ） 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。
（ハ） 移送する犯罪事実確認記録について、パスワード等による保護を行う。	（ハ） 移送する犯罪事実確認記録について、パスワード等による保護を行う。
（クラウドサービスの使用に伴う漏えい等の防止措置） ・ 情報システムに犯罪事実確認記録を保存する場合、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。 ・ 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。 ・ 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には、当該外国の個人情報の保護に関する制度等を把握した上で、犯罪事実確認記録等の情報管理のために必要かつ適切な措置を講じる。	（クラウドサービスの使用に伴う漏えい等の防止措置） ・ 情報システムに犯罪事実確認記録を保存する場合、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。 ・ 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。 ・ 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には、当該外国の個人情報の保護に関する制度等を把握した上で、犯罪事実確認記録等の情報管理のために必要かつ適切な措置を講じる。

（３）情報管理規程

○　上述の内容を盛り込んだ情報管理規程のひな型は、資料編別紙８から 10 までのとおり。なお、ひな型において複数選択可と記載されている項目については、可能な限り複数の方法を選択し、実施することが望ましい。

・　ひな型①（別紙８）
事業者における責任者一人（理事長、人事担当部長等）のみが、法関連システム上のみで犯罪事実確認書を確認し、それ以外では犯罪事実確認記録等の記録・保存等を行わない場合
・　ひな型②（別紙９）
事業者の責任者を含む複数名が、法関連システム上のみで犯罪事実確認書を確認し、それ以外では犯罪事実確認 記録等の記録・保存等を行わない場合
・　ひな型③（別紙 10）
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、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

※　「犯罪事実確認記録等の記録・保存」は、犯罪事実確認書に記載された内容の記録・保存をいい、犯罪事実確認を実施済みか否かについての情報の記録・保存は、これに当たらない。

○　犯罪事実確認実施者等（国公立を除く。）は、情報管理規程のひな型を必要に応じて参考にしながら、規程を作成し、一人目の従事者の犯罪事実確認までに、作成した情報管理規程を提出する（規則第 12 条第４項）。
※　情報管理規程の内容が法令の規定に違反していると認められる場合は、違反を是正するために必要な措置をとるべきことを命令され、その措置が講じられたと認められるまでの間は、犯罪事実確認書の交付が留保される（法第 35 条第３項）。

○　届出の方法及び留意点は、次の①及び②に掲げるとおり。
①　手続は、原則としてこども性暴力防止法関連システムを介してオンラインで行うこと（規則第 12 条第４項）
※　具体的なこども性暴力防止法関連システムを介した手続方法や必要な様式等は、別途マニュアルにおいて示す。
②　施設等運営者がある場合には、情報管理規程に、上述のアからオまでに掲げる事項に加え、各事項に係る役割分担を記載するとともに、学校設置者等及び施設等運営者の両方が内容を確認・合意した上で届け出ること（規則第 12 条第３項及び第５項）

（４）情報管理規程の変更の届出

○　犯罪事実確認実施者等は、規則第 12 条第４項の規定により提出した情報管理規程を変更しようとするときは、あらかじめ、次の①から③までに掲げる事項を記載した届出書をこども家庭庁に提出しなければならない（規則第 12 条第６項）。

① 犯罪事実確認実施者等の次の情報

ア 氏名又は名称

イ 住所又は所在地

ウ 代表者の氏名（法人の場合）

② 変更の内容及び理由（変更の内容については、新旧の対照を明示すること）

③ 変更後の情報管理規程の実施予定日

※ ただし、次の(ア)から(ウ)までに掲げる場合は、軽微な変更として、届出の必要はない。

（ア） 情報管理規程の内容の実質的な変更を伴わないもの（例：部署名・役職名の形式的な変更など）

（イ） 情報管理措置の水準を維持する変更であって、具体的な手法の変更にとどまるもの（例：例示されている手法の変更など）

（ウ） 情報管理措置の水準を向上させる変更（例：最低限求められる措置から標準的措置への変更など）

○ 届出の方法及び留意点は、次の①及び②に掲げるとおり。

① 手続は、原則としてこども性暴力防止法関連システムを介してオンラインで行うこと（規則第 12 条第７項）

※ 具体的なこども性暴力防止法関連システムを介した手続方法や必要な様式等は、別途マニュアルにおいて示す。

② 施設等運営者がある場合には、学校設置者等及び施設等運営者の両方が内容を確認・合意した上で届け出ること（規則第 12 条第８項）

（５）個人情報保護法との関係

○ 個人情報保護法第 23 条においては、個人情報取扱事業者[40]（※）に対し、個人データの安全管理のために必要かつ適切な措置（安全管理措置）を講ずる義務を課しており、その具体的内容については「個人情報の保護に関する法律についてのガイドライン（通則編）」（平成 28 年 11 月（令和７年６月一部改正）個人情報保護委員会。以下「個人情報保護法ガイドライン」という。）等において示されている[41]。

○ 個人情報保護法ガイドラインにおいては、個人情報取扱事業者が講ずべき安全管理措置として、次の①及び②に掲げる措置を求めている。

① 基本方針を策定すること

② 次のアからオまでの措置を盛り込んだ個人データの取扱に係る規律を整備すること

ア 組織的安全管理措置

[40] 個人情報データベース等[21]を事業に用いている事業者をいう（国の機関、地方公共団体、独立行政法人等、地方独立行政法人を除く。個人情報保護法第 16 条第２項）

[41] 個人情報を含む情報の集合物であって、特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの、又は特定の個人情報を容易に検索することができるようにしたもの（個人情報保護法第 16 条第１項）。個人情報データベース等を構成する個人情報のことを「個人データ」という（個人情報保護法第 16 条第３項）。

イ　人的安全管理措置
ウ　物理的安全管理措置
エ　技術的安全管理措置
オ　外的環境の把握

○　個人情報保護法ガイドラインに基づく組織的安全管理措置、人的安全管理措置、物理的安全管理措置及び技術的安全管理措置の策定項目と、法に基づく情報管理規程に盛り込む犯罪事実確認記録等を適正に管理するために必要な措置として、個人情報保護法との整合性を踏まえて整理されている組織的情報管理措置、人的情報管理措置、物理的情報管理措置及び技術的情報管理措置の策定項目については、次の表のとおり整理される。

（個人情報保護法ガイドライン及び犯罪事実確認記録等を適正に管理するために必要な措置の策定項目の対照表）

個人情報保護法ガイドライン	犯罪事実確認記録等を適正に管理するために必要な措置
1　組織的安全管理措置	（1）　組織的情報管理措置
ⅰ　組織体制の整備	(i)　組織体制の整備
ii　個人データの取扱いに係る規律に従った運用	(ii)　情報管理規程に基づく運用
iii　個人データの取扱状況を確認する手段の整備	(iii)　犯罪事実確認記録等の取扱記録の記載項目の整理
iv　漏えい等事案に対応する体制の整備	(iv)　漏えい等事案に対応する体制の整備
v　取扱状況の把握及び安全管理措置の見直し	(v)　犯罪事実確認記録等の取扱状況の把握及び安全管理措置の見直し
2　人的安全管理措置 従業者の教育	（2）　人的情報管理措置 従業者の研修・訓練等
3　物理的安全管理措置	（3）　物理的情報管理措置
ⅰ　個人データを取り扱う区域の管理	(i)　個人データを取り扱う区域の管理
ii　機器及び電子媒体等の盗難等の防止	(ii)　機器及び電子媒体等の盗難等の防止
iii　電子媒体等を持ち運ぶ場合の漏えい等の防止	(iii)　電子媒体等を持ち運ぶ場合の漏えい等の防止
iv　個人データの削除及び機器、電子媒体等の廃棄	(iv)　個人データの削除及び機器、電子媒体等の廃棄
4　技術的安全管理措置	（4）　技術的安全管理措置
ⅰ　アクセス制御	(i)　アクセス制御
ii　アクセス者の識別と認証	(ii)　アクセス者の識別と認証
iii　外部からの不正アクセス等の防止	(iii)　外部からの不正アクセス等の防止
iv　情報システムの使用に伴う漏えい等の防止	(iv)　情報システムの使用に伴う漏えい等の防止

○　なお、既に施設・事業所内における個人情報保護法に基づく基本方針を策定している場合は、法に基づく基本的事項が漏れなく含まれるよう、既存の基本方針を改定する等の対応が求められる（別途、法に基づく情報管理規程を定める場合の改定等は不要）。

３．目的外利用・第三者提供の禁止（法第 12 条、第 27 条第２項、第 39 条、第 43 条、第 45 条第２項、第 47 条及び第 48 条関係）

法第 12 条、第 27 条第２項、第 39 条、第 43 条、第 45 条第２項、第 47 条及び第 48 条

（利用目的による制限及び第三者に対する提供の禁止）

第十二条　犯罪事実確認実施者等は、次に掲げる場合を除き、犯罪事実確認記録等を犯罪事実確認若しくは第六条（第九条第一項又は第十条第一項の規定により読み替えて適用する場合を含む。）の措置を実施する目的以外の目的のために利用し、又は第三者に提供してはならない。

一　第九条第二項又は第十条第二項の規定により提供する場合

二　訴訟手続その他の裁判所における手続又は刑事事件の捜査のために提供する場合

三　情報公開・個人情報保護審査会設置法（平成十五年法律第六十号）第九条第一項の規定により情報公開・個人情報保護審査会に提示する場合

四　第十六条第一項、児童福祉法第二十一条の五の二十二第一項、第二十四条の十五第一項、第三十四条の十七第一項、第三十四条の二十五第一項若しくは第四十六条第一項又は認定こども園法第十九条第一項若しくは第三十条第三項の規定により報告若しくは提出若しくは提示を求められ、又は質問若しくは検査に応じる場合

（犯罪事実確認記録等の適正な管理）

第二十七条　（略）

２　第十二条及び第十三条の規定は、認定事業者等について準用する。この場合において、第十二条中「第六条（第九条第一項又は第十条第一項の規定により読み替えて適用する場合を含む。）の措置」とあるのは「第二十六条第七項に規定する防止措置」と、同条第一号中「第九条第二項又は第十条第二項」とあるのは「第二十六条第七項」と、同条第四号中「第十六条第一項、児童福祉法第二十一条の五の二十二第一項、第二十四条の十五第一項、第三十四条の十七第一項、第三十四条の二十五第一項若しくは第四十六条第一項又は認定こども園法第十九条第一項若しくは第三十条第三項」とあるのは「第二十九条第一項」と、「提出若しくは提示」とあるのは「提出」と読み替えるものとする。

（職員等の秘密保持義務）

第三十九条　犯罪事実確認書受領者等（その者が法人である場合にあっては、その役員）若しくはその職員若しくは従業者又はこれらであった者は、その業務に関して知り得た犯罪事実確認書（第三十五条第四項第二号に定める事項が記載されたものに限る。第四十五条第二項において同じ。）に記載された情報の内容をみだりに他人に知らせ、又は不当な目的に利用してはならない。

（情報不正目的提供罪）

第四十三条　犯罪事実確認書受領者等（その者が法人である場合にあっては、その役員）若しくはその職員若しくは従業者又はこれらであった者が、その業務に関して知り得た犯罪事実確認書に記載された情報を自己又は第三者の不正な利益を図る目的で提供したときは、二年以下の拘禁刑若しくは百万円以下の罰金に処し、又はこれを併科する。

（虚偽表示罪及び情報漏示等罪）

第四十五条　（略）

２　第三十九条の規定に違反して、その業務に関して知り得た犯罪事実確認書に記載された情報の内容をみだりに他人に知らせ、又は不当な目的に利用した者は、一年以下の拘禁刑若しくは五十万円以下の罰金に処し、又はこれを併科する。

（国外犯）

第四十七条　第四十三条及び第四十五条第二項の規定は、日本国外においてこれらの規定の罪を犯した者にも適用する。

（両罰規定）

第四十八条　法人の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関し、第四十三条、第四十四条、第四十五条第一項又は第四十六条の違反行為をしたときは、行為者を罰するほか、その法人又は人に対して各本条の罰金刑を科する。

（１）目的外利用・第三者提供の禁止

○　犯罪事実確認実施者等は、次の①から④までに掲げる場合を除き、犯罪事実確認記録等を犯罪事実確認若しくは防止措置を実施する目的以外の目的のために利用し、又は第三者に提供してはならない（法第 12 条）。

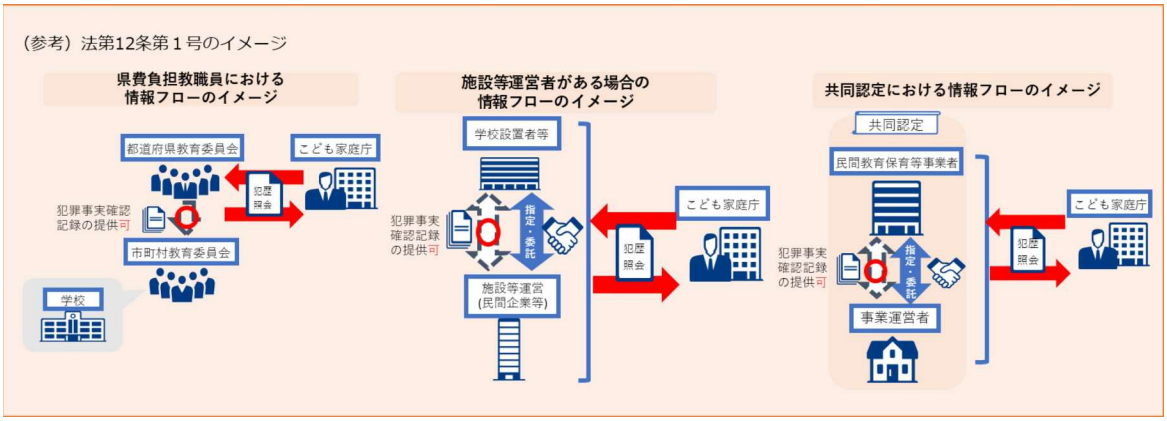
①　都道府県教育委員会と市町村教育委員会との間（県費負担教職員の場合）及び学校設置者等と施設等運営者との間で、防止措置の実施に必要な限度において提供する場合（同条第１号）

②　訴訟等の裁判所手続又は刑事事件の捜査のために提供する場合（同条第２号）

③　情報公開・個人情報保護審査会の求めに応じて提示する場合（同条第３号）

④　法、児童福祉法等の規程に基づき、報告徴収・立入検査等に応じる場合（同条第４号）

図表 97　①（法第 12 条第１号）に該当する場合のイメージ



○　認定事業者等についても、同等の措置が求められており（法第 27 条第２項）、これに違反した場合は適合命令及び是正命令の対象（法第 30 条）や認定取消事由（法第 32 条）に該当する。

（２）目的外利用に当たらない場合

○　犯罪事実確認実施者等及び認定事業者等が、防止措置を実施することを目的として、次のア又はイに掲げる措置を行う場合には、法第 12 条に定める犯罪事実確認書の目的外利用には当たらない。

ア　具体的な防止措置の検討・実施に当たり、同一事業者内（例：教育委員会と学校）で、犯罪事実確認記録を必要最低限の関係者間で共有すること

イ　犯罪事実確認記録等を端緒に、従事者本人と改めて面談の場を設ける等により、犯罪事実確認書の情報だけでは足りない特定性犯罪事実関連情報を追加的に得ること

※　なお、特定性犯罪事実関連情報の詳細については、本章「６．安全確保措置等を通じて収集した機微性の高い情報の取扱い」を参照すること。

（３）第三者提供の禁止に該当する場合

○　第三者提供に当たる主な例とその留意点は次に掲げるとおり。

・　保護者からの問い合わせを受けて、特定の従事者の特定性犯罪事実の有無を回答する場合

※　特定の従事者が犯罪事実確認の対象か否かを回答することは、犯罪事実確認記録等の提供に当たらないが、基本的には開示を控えること。

・　派遣元等に対して、特定性犯罪事実の有無に関する情報を提供する場合

※　派遣労働者の交代等を派遣元等に求める場合には、特定性犯罪事実に限定しない形で「法第６条等の防止措置を講ずる必要があるため」といった直接的ではない形の伝達を行うことが考えられる。

・　法に定める犯罪事実確認記録等の情報管理業務を、他の事業者に委託する場合

（４）県費負担教職員への犯罪事実確認記録等の提供

○　県費負担教職員に係る市町村教育委員会への犯罪事実確認記録等の提供については、当該情報を取り扱う犯罪事実確認書受領者等における取扱者を必要最小限とするため、システム上での閲覧権限を付与することをもって実施することを原則とする。

○　このとき、犯罪事実確認記録等の適正管理義務は都道府県教育委員会、市町村教育委員会の双方にかかり、後述の情報不正目的提供罪（法第 43 条）及び情報漏示等罪（第 45 条第２項）の罰則が適用される場合は、両罰規定（法第 48 条）により当該罰則適用の対象者が所属している組織に対しても罰則が適用される。

（５）職員等の秘密保持義務

○　犯罪事実確認書受領者等又はその役員、従事者等は、犯罪事実確認書に記載された特定性犯罪事実がある場合の情報をみだりに他人に知らせ、又は不当な目的に利用してはならない（法第 39 条）。

○　犯罪事実確認書受領者等又はその役員、従事者等が、法第 39 条の規定に違反した場合（情報漏示等罪）や、犯罪事実確認書に記載された情報（特定性犯罪事実がない場合を含む。）を自己又は第三者の不正な利益を図る目的で提供したとき（情報不正目的提供罪）は、刑罰が科される（法第 43 条及び第 45 条第２項）。

○　情報不正目的提供罪及び情報漏示等罪に関する規定は、日本国外においてこれらの罪を犯した者にも適用される（法第 47 条）。

○　法人の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関し、上述の情報不正目的提供罪及び情報漏示等罪に係る違反行為をしたときは、刑罰が課されるほか、その法人又は人に対して情報不正目的提供罪及び情報漏示等罪における刑罰が科される（法第 48 条）。

○　このように、犯罪事実確認の情報を取り扱う責任者・担当者が従事者の犯罪事実確認記録等の内容を第三者に提供、開始、漏えいした場合、法に基づく刑罰が科され得るほか、当該従事者個人を被害者とする名誉毀損罪等に該当する可能性がある。また、責任者・担当者や事業者が当該従事者個人に対し民事上の損害賠償義務を負う可能性がある。

○　対象事業者等は、このような法違反時に、刑罰が科され得ることや、民事責任の対象になる可能性があることを、犯罪事実確認記録等を取り扱う従事者に対しても、研修等を通じて十分に周知するとともに、これらの行為について就業規則の服務規律（禁止事項）や懲戒事由に定めることで、事前防止を図る必要がある。