別紙

情報管理措置の具体的な内容

1 基本方針の策定

事業者は、情報管理規程の全体に関わる基本方針を定めるものとする。
基本方針は情報管理措置の基本原則の内容を含むものとする。
具体的な内容については、表1の「標準的措置」と「最低限求められる措置」に示す。

表1 講ずべき基本的事項

講じなければならない措置	想定リスク	標準的措置	最低限求められる措置
○ 犯罪事実確認記録等の取扱いに係る基本方針の整備	全リスク共通	■事業者において、犯罪事実確認記録等を取り扱うに当たり、以下の内容を含む基本方針を策定する。 ・ 犯罪事実確認記録等の取扱者は必要最小限とする ・ 犯罪事実確認書の内容の記録・保存を極力避ける ・ 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 ・ 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 ・ 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	■事業者において、犯罪事実確認記録等を取り扱うに当たり、以下の内容を含む基本方針を策定する。 ・ 犯罪事実確認記録等の取扱者は必要最小限とする ・ 犯罪事実確認書の内容の記録・保存を極力避ける ・ 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 ・ 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 ・ 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

2 組織的情報管理措置

事業者は、組織的情報管理措置として、次の(1)～(5)に掲げる措置を講じることが求められる。

(1) 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。

(2) 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。

(3) 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。

(4) 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。

(5) 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。

上記(1)～(5)に掲げる措置を達成するための手段・方法を以下表２の「標準的措置」と「最低限求められる措置」に示す。

表2 講ずべき組織的情報管理措置の内容

講じなければならない措置	想定リスク	標準的措置	最低限求められる措置
(1) 組織体制の整備	全リスク共通	■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。 ■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)。 ■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。 ■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 ■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	■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。 ■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)。 ■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 ■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

講じなければならない措置	想定リスク	標準的措置	最低限求められる措置
		連絡体制を整備する。 ■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。 ■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。	連絡体制を整備する。 ■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。 ■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。
(2) 情報管理規程に基づく運用	全リスク共通	■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	■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

講じなければならない措置	想定リスク	標準的措置	最低限求められる措置
		テムで消去）	テムで消去）
（3）犯罪事実確認記録等の取扱記録の記載項目の整理	全リスク共通	■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	■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
（4）漏えい等の事案に対応する体制の整備	全リスク共通	■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	■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

講じなければならない措置	想定リスク	標準的措置	最低限求められる措置
		等の公表	等の公表
(5) 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	全リスク共通	■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を保有する者が実施	■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。 ■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

3 人的情報管理措置

● 従事者の研修・訓練等

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。

上記措置を達成するための手段・方法を以下表3の「標準的措置」と「最低限求められる措置」に示す。

なお、こども家庭庁において、次年度以降に研修教材[1]を作成し、提供する予定。

[1]現時点では、以下の内容を含む、平易で具体的な内容の教材を想定。
・情報セキュリティの初歩的な事項
・日常的に意識して履行すべき事項（関連業務に従事しなくなる者のアクセス権解除、利用端末紛失時の対応等）
・様々な規模の事業者において、漏えい等が発生した場合に起こりうる事態と対処の例
・犯罪事実確認記録等の漏えいによる様々な影響（プライバシーの権利の侵害、組織の信用失墜、損害賠償請求の可能性等）

表3 講ずべき人的情報管理措置の内容

講じなければならない措置	想定リスク	標準的措置	最低限求められる措置
(1) 従事者の研修・訓練等	・ 権限のない従事者による電子ファイル等の無断持ち出し・情報漏えい ・ 権限のある管理者の故意・過失による目的外利用 ・ 異動又は退職する者等による情報の持ち出し、不正侵入による情報漏えい ・ 従事者の出力紙、手書きメモの置き忘れ、紛失等過失による情報漏えい ・ 権限のある従事者からその他の者（権限のない従事者、従事者以外の者）への会話による情報漏えい（例：日々の業務上／業務外の会話、会食での会話、電車内やエレベータ内での会話を聞かれてしまう等） ・ 従事者による SNS・チャットアプリ等インターネットでの電子ファイル、撮影画像、メッセージ等による情報漏えい（故意・過失を含む） ・ 従事者の過失で組織内の情報共有ツールへ情報が共有されることによる情報漏えい ・ ビジネスメール詐欺による情報窃取（例：こども家庭庁になりすまして情報を得る等） ・ クラウドサービスの認証情報	■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。 ■研修を実施した旨は、記録し、責任者が定期的に確認する。 ■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。 ■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。 ■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	■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。 ■研修を実施した旨は、記録し、責任者が定期的に確認する。 ■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。 ■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。 ■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 ※こども家庭庁が作成する研修教材や情

講じなければならない措置	想定リスク	標準的措置	最低限求められる措置
	が、メールやSMS等フィッシング詐欺により窃取されることによる情報漏えい 等	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	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。 （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

4 物理的情報管理措置

事業者は、物理的情報管理措置として、次の(1)～(4)に掲げる措置を講じることが求められる。

(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。

(2) 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。

(3) 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。

(4) 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

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。

上記(1)～(4)に掲げる措置を達成するための手段・方法を表4の「標準的措置」と「最低限求められる措置」に示す。

表4 講ずべき物理的情報管理措置の内容

講じなければならない措置	想定リスク	標準的措置	最低限求められる措置
(1) 犯罪事実確認記録等を取り扱う区域の管理	・ 権限のない従事者によるファイル・紙媒体等の無断持ち出し・情報漏えい ・ 権限のある管理者の故意・過失によるファイル・紙媒体等の無断持ち出し・情報漏えい ・ 異動又は退職する者等による情報の持ち出し、不正侵入による情報漏えい ・ 権限のない従事者又は悪意のある第三者によるショルダーハッキング(盗み見)、盗聴等による情報漏えい ・ 端末・電子記録媒体の紛失・盗難による情報漏えい ・ 権限のない従事者の内部犯行による情報の改ざん ・ 悪意のある第三者の侵入による情報の改ざん 等	■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[2]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。 ■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。	■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。 ■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。

[2] 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。

講じなければならない措置	想定リスク	標準的措置	最低限求められる措置
		（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、以下の「（2）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。
（2）機器及び電子媒体等の盗難等の防止	・ 従事者による端末・記録媒体の紛失・盗難等による情報漏えい ・ 従事者による紙媒体の紛失・盗難による情報漏えい ・ 従事者の出力紙、手書きメモの置き忘れ、紛失等過失による情報漏えい ・ 従事者又は悪意のある第三者による端末・記録媒体の持ち出しによる情報漏えい 等	■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。 ■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。	■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。 ■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。

講じなければならない措置	想定リスク	標準的措置	最低限求められる措置
		（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 ■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。	（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 ■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。
（3）電子媒体等を持ち運ぶ場合の漏えい等の防止	・ 従事者による端末・記録媒体の紛失・盗難等による情報漏えい ・ 従事者の移送中の紛失・盗難等による情報漏えい 等	■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[3]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。 ■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	■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。 ■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

[3] 犯罪事実確認記録等を管理区域又は取扱区域の内外をまたいで移動させることをいう。なお、事業者内の移動等であっても、個人データの紛失・盗難等に留意する必要がある。

講じなければならない措置	想定リスク	標準的措置	最低限求められる措置
		□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。	□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。
（4）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	・ 内部犯又は悪意のある第三者による情報の復元・窃取 ・ 書類の誤廃棄による情報漏えい 等	■（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	■（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

講じなければならない措置	想定リスク	標準的措置	最低限求められる措置
		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。	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） □犯罪事実確認記録等が記録された機器、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。

5 技術的情報管理措置

事業者は、技術的情報管理措置として、次の(1)～(4)に掲げる措置を講じることが求められる。

(1) 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。

(2) 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。

(3) 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。

(4) 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。

上記(1)～(4)に掲げる措置を達成するための手段・方法を表5の「標準的措置」と「最低限求められる措置」に示す。なお、事業者独自の情報システムを保有していない場合は、特段の措置は不要である。

表5 講ずべき技術的情報管理措置の内容

講じなければならない措置	想定リスク	標準的措置	最低限求められる措置
(1) アクセス者の識別及び認証	・ 権限のない従事者又は悪意のある第三者による、アクセス権者へのなりすましによる情報の窃取 ・ 従事者又は悪意のある第三者による端末・記録媒体の持ち出しによる情報漏えい ・ 権限のない従事者のアクセスによる情報漏えい ・ 犯罪事実確認の担当外のシステム管理者のアクセスによる情報漏えい ・ 異動又は退職する者等による電子ファイルの情報の持ち出し・不正アクセスによる情報漏えい ・ 権限を持たない従事者の内部犯行による電磁記録情報の改ざん ・ 等	■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、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。	■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、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。
(2) アクセス制御	(同上)	■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。 ■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。	■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。 ■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。

講じなければならない措置	想定リスク	標準的措置	最低限求められる措置
		（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。 ■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。 （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	（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 ■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。 （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

講じなければならない措置	想定リスク	標準的措置	最低限求められる措置
		除	
(3) 外部からの不正アクセス等の防止	・ 悪意のある第三者の不正アクセスによる情報漏えい ・ 悪意のある第三者の不正アクセスによる情報の改ざん ・ ビジネスメール詐欺による情報窃取(例:こども家庭庁になりすまして情報を得る等) 等	■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。 ■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。 ■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。 ■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	■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。 ■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。 ■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。 ■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

講じなければならない措置	想定リスク	標準的措置	最低限求められる措置
		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。 ■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、「(3)外部からの不正アクセスの防止」の■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[4]／IPS[5]等による不正アクセスの検知又は遮断 □DLP[6]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。	■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、「(3)外部からの不正アクセスの防止」の■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
(4) 情報システムの使用に伴う漏えい等の防止	・ マルウェア感染した端末へ情報が記録・保存された結果、外部への不正通信が	■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	■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

[4] 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。
[5] 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。
[6] 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。

講じなければならない措置	想定リスク	標準的措置	最低限求められる措置
	行われることによる情報漏えい ・ 従事者の過失により組織内で情報共有ツールへ情報が共有されることによる情報漏えい ・ クラウドサービスが不正アクセス等のサイバー攻撃を受けることによる情報漏えい ・ クラウドサービスの設定不備による情報漏えい 等	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

講じなければならない措置	想定リスク	標準的措置	最低限求められる措置
		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。	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。