

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

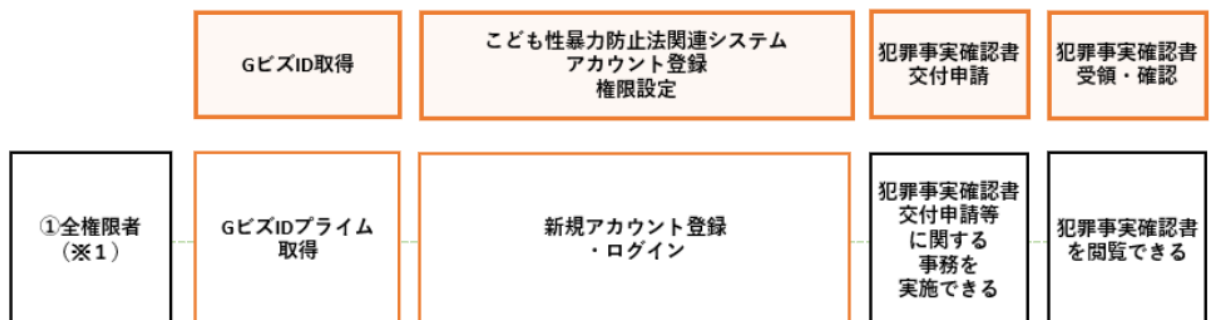
(権限者及び権限の整理)

- 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

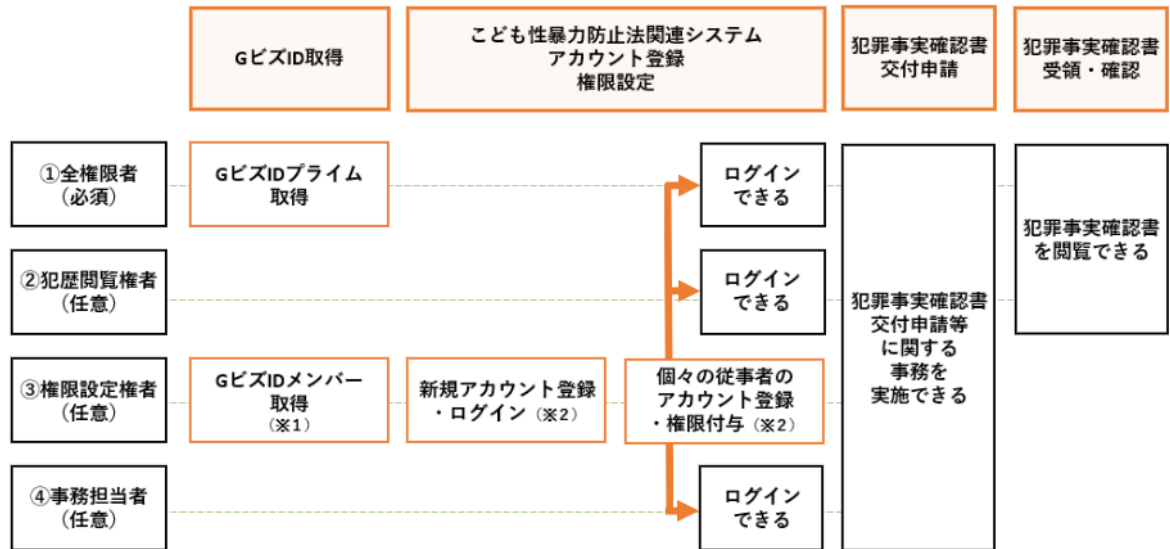
権限者	権限	権限が割り当てられる者の職務のイメージ
①全権限者	犯罪事実確認書の閲覧 権限設定 申請手続等の事務	組織の総責任者、準責任者 (行政の人事担当部長、法人理事長等)
②犯歴確認権者	犯罪事実確認書の閲覧 申請手続等の事務	現場責任者 (公立学校の校長、複数園を運営する法人内の園長等)
③権限設定権者	権限設定 申請手続等の事務	情報システムの責任者
④事務担当者	申請手続等の事務	その他の従事者 (人事担当等)

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 Biz 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。