ProcessMind監査ログおよびSIEMに関する声明

発効日：2026年11月12日

本声明は、ProcessMind B.V.が顧客データに対して実行されたセキュリティ上重要な操作および管理操作をどのように記録するか（「監査ログ」）について説明します。本声明は、セキュリティ対策、データ処理付属書、顧客契約およびサブプロセッサー一覧を補足するものです。

---

1. 適用範囲

1.1 単一の監査ログ。 ProcessMindは、顧客データおよびProcessMindサービスに対して実行されたセキュリティ上重要な操作および管理操作について、単一の監査ログを維持します。監査ログは、運用（アプリケーション）ログ、HTTPアクセスログおよび製品のアクティビティフィードとは別個のものであり、これらのストリームはそれぞれ異なる目的を果たすもので、監査証跡として扱われるものではありません。

1.2 該当しないもの。 監査ログは、顧客データのすべての読み取りを記録するものではなく、プロセスモデル、図、ドキュメントまたはシミュレーションに関する製品の変更履歴でもありません。これらは、製品内で利用可能なプロセス変更履歴に記録されます。

---

2. 各監査記録に含まれる内容

2.1 フィールド。 各記録には以下のフィールドが含まれます。フィールドの集合は記録スキーマによって固定されており、この一覧にないフィールドが記録に追加されることはなく、アクションがレジストリで宣言していないフィールドを追加することもできません。

- *schemaVersion*（数値）：記録スキーマのバージョン。現在は1です。
- *eventId*（文字列）：一意の記録識別子。新しい記録にはULIDを使用します。以前のストアから移行された行は、元のUUIDを保持します。
- *occurredAt*、*ingestedAt*（タイムスタンプ）：アクションが発生した時刻、および監査ログ書き込みコンポーネントが記録を保存した時刻。いずれ

もUTCです。

- *eventClass*（列挙型）：security、auth、admin、data、api、aiまたはplatformです。
- *action*（列挙型）：クローズドで審査済みのアクションレジストリにあるコードのいずれか。例：auth.login.blockedまたはapi.key.revokedです。
- *outcome*（列挙型）：success、failure、deniedまたはerrorです。
- *severity*（列挙型）：info、notice、warningまたはcriticalで、結果に基づいて決定されます。成功したアクションにはレジストリの既定値（アクションに別段の定めがない限りinfo）が使用され、failureはnotice、deniedまたはerrorはwarningとして記録されます。
- *actor*（オブジェクト）：操作を行った主体。type（user、apiKey、service、systemまたはanonymous）、id、email、displayName、および別のアカウントのためにアクションが実行された場合のonBehalfOfとonBehalfOfEmailです。
- *actorContext*（オブジェクト）：操作を行ったセッション。sessionId、authMethod（oidc、password、loginToken、apiKeyまたはnone）およびサポートセッションのフラグです。
- *organizationId*、*tenantId*（識別子、null可）：アクションが属する組織および環境です。顧客に関係しない記録、または環境より上位の記録ではnullです。
- *resource*（オブジェクト、null可）：影響を受けたオブジェクト。type、idおよびnameを含み、typeはapiKey、artifact、connection、database、datatable、export、lead、model、organization、process、role、session、setting、storage、tenantまたはuserのいずれかです。
- *source*（オブジェクト）：記録が生成された場所。service（api、externalApi、superadminApi、worker、cronまたはwebSocket）、functionおよびversionです。
- *stage*、*region*（文字列）：記録を生成したデプロイ環境（例：prod）およびAWSリージョン（顧客記録の場合はeu-central-1）です。
- *correlation*（オブジェクト）：requestId、traceIdおよびparentEventIdを含み、記録を、その原因となったリクエストおよび同じフロー内の先行記録に関連付けます。

- *network*（オブジェクト、null可）：sourceIpおよびuserAgentです。レジストリの項目で記録が有効化されているアクション（サインイン、アクセス判断、管理および設定の変更、データのアップロード、ダウンロードおよびエクスポート、APIキーの変更、AIポリシーの変更）についてのみ取得されます。
- *detail*（オブジェクト）：アクション固有のペイロードであり、そのアクションのスキーマに照らして検証されます。値はプリミティブ（文字列、数値、ブール値、null）のみであるため、記録のクエリおよび編集が可能な状態に保たれます。

2.2 クローズドな語彙。 アクションは、固定された審査済みのアクションコード一覧から選択されます。監査記録に自由記述のメッセージは含まれません。また、各アクションは追加で含めることのできるフィールドを宣言するため、記録に新たな種類の内容がひそかに追加されることはありません。

---

3. 記録されるアクション

3.1 現在記録されるもの。 ProcessMindは、特に以下を記録します。

- **認証：**サインインの成功および失敗、ブロックされたサインイン（アカウントのロック、許可されていないドメイン、未確認のプロバイダーのメールアドレス）、サインアウト、ログイントークンの発行および引き継ぎ。
- **認可：**アクセス拒否。外部APIの認証情報、スコープおよびテナントの状態に関するすべての拒否、ならびにオリジン（CORS）による拒否を含みます。
- **サポートアクセス：**顧客アカウントに対するProcessMindサポートセッションの開始。担当者および影響を受けるアカウントの両方を記録します。
- **API認証情報：**APIキーの作成、スコープの変更および失効。付与されたスコープを含みます。
- **アカウントおよびロールの管理：**ユーザーの作成、招待、管理者プロフィールの編集、削除、ロールの付与および失効、ならびにテナントまたは組織のメンバーシップの変更。
- **組織のライフサイクル：**作成、削除、復元、削除のスケジュール設定およびキャンセル、ならびに完了した消去。

- **データのアップロード、ダウンロードおよびエクスポート：**アーティファクトのアップロード、ダウンロードおよび削除、表形式データのアップロードおよび更新、エクスポートのダウンロード、データテーブルの削除、ならびにWebhook（接続）の作成、変更および削除。
- **請求状態：**プランの変更、支払いに起因する一時停止および復旧、ならびにサブスクリプションのキャンセル。
- **ProcessMindのプロバイダーコンソール：**特権クエリの実行、ユーザーおよび組織の管理、設定および機能の変更、請求同期リクエスト、ならびに移行。
- **ProcessMindのスケジュール済みジョブによる管理操作および破壊的操作：**テナント、組織、ユーザーおよびリードの削除、保持期間に基づく一括処理、ならびにパイプラインの失敗。
- **監査ログの完全性：**監査ログ自体の書き込み処理の失敗。

3.2 ワークスペース内の編集。 ワークスペース内の編集（プロセスモデル、ドキュメント、シミュレーション、ダッシュボード、コメントおよびブックマーク）は、監査ログではなく、製品独自のプロセス変更履歴に記録されます。監査ログには、誰がデータをアップロード、ダウンロード、エクスポートまたは削除したかが記録され、変更履歴にはモデル内で何が変更されたかが記録されます。記録対象のアクションコードの最新一覧は、ProcessMindに請求することで入手できます。

---

4. 記録されない情報

パスワード、認証トークン、APIキーの値、Cookie、認可ヘッダー、リクエストまたはレスポンスの本文、ファイルの内容、署名付きURL、ならびにAIプロンプトまたは生成結果は、監査ログに記録されません。監査記録には、帰属の特定に必要な個人データとして、操作主体のメールアドレス、およびレジストリの項目で記録が有効化されているアクション（サインイン、アクセス判断、管理および設定の変更、データの移動、APIキーおよびAIポリシーの変更）に関する送信元IPアドレスとユーザーエージェントが含まれる場合があります。許可されるフィールドはアクションごとに定義され、アクションの追加時に審査されます。

---

5. 完全性

5.1 追記専用。 監査ログは追記専用です。いずれのアプリケーションロールにも更新または削除の権限はなく、データベース制約により両方の操作が拒否されます。

5.2 単一の書き込みコンポーネント。 記録は、書き込み前にアクションコードおよびそのペイロードを検証する単一のコンポーネントによって書き込まれます。検証に失敗した記録は、一部だけを書き込むのではなく、拒否されて報告されます。

5.3 失敗への対応。 監査ログへの書き込みが失敗しても、記録対象の業務上のアクションが失敗することはありません。書き込みの失敗は、アラームが設定された運用経路で記録され、記録自体は復旧できるよう二次コピーに保存されます。

---

6. 保持および保管場所

6.1 保持期間。 監査記録は、イベント発生日から少なくとも10年間保持されます。

6.2 保管場所および暗号化。 監査記録は欧州連合（ドイツ、フランクフルト、`eu-central-1`）に保管され、保存時には顧客管理のAWS KMSキーで暗号化されます。また、インシデント発生中に調査できるよう、稼働中のコピーがアクセス制御されたAmazon CloudWatchロググループにも書き込まれます。

6.3 リージョン間レプリケーションなし。 監査記録は欧州連合の外部に複製されません。

---

7. 監査記録へのアクセス

7.1 利用資格。 アプリ内監査ログは、Process Architectureプラン以上に含まれます。組織管理者は組織全体を読み取ることができ、テナントの範囲に限定された管理者は自身のテナントを読み取ることができます。範囲は認証済みセッションから導出され、クエリの前に確認されるため、リクエストによって別のテナントまたは組織に範囲を拡大することはできません。

7.2 ProcessMindの担当者。 ProcessMindの担当者は、サポート、インシデント対応または法的義務のために必要な場合に限り、知る必要のある範囲で監査記録に

アクセスします。顧客間のアクセスは専用のサポートロールに制限され、そのようなアクセス自体も管理操作として記録されます。

7.3 記録の取得方法。 組織管理者およびテナント管理者は、アプリ内監査ログで自身の監査記録を読み取り、外部APIを通じて取得またはエクスポートできます。大規模なリクエストまたは支援を要するリクエストについては、ProcessMindサポートが、指定された組織、テナントおよび期間の記録をCSVまたはJSON形式で提供します。標準的なリクエストについては、5営業日を目標とします。

---

8. 監査記録の削除

8.1 請求に基づく削除。 書面による請求が確認された場合、ProcessMindは顧客組織に属する監査記録を監査ストアから消去し、消去したことを書面で確認します。運用上のCloudWatchコピーは記録ごとに編集できず、独自の保持期間に従って失効します。

8.2 保持される情報。 消去が行われたことを示す記録（組織識別子、日付、請求者、理由および削除された記録の件数）は、プラットフォームレベルの監査記録として保持され、顧客データは含まれません。いずれの顧客にも属さない記録（ProcessMindプラットフォームのイベント）は、顧客による消去請求の影響を受けません。

8.3 個人による消去請求。 引き続き有効な顧客内の個人に関する請求の場合、GDPR第17条第3項(b)および(e)で認められる範囲で、法的請求の確立、行使または防御のためにセキュリティ記録を保持します。この根拠は、処理活動の記録およびプライバシーポリシーに記載されます。

---

9. SIEM連携およびエクスポート

9.1 利用可能性。 不変の監査アーカイブはEnterpriseオプションであり、顧客組織からの請求に応じて有効化されます。組織ごとのプレフィックスの下にあるObject-Locked（WORM）S3バケットに、マニフェストおよび夜間照合とともに、圧縮されたNDJSONオブジェクトを毎日書き込みます。

9.2 現在の提供方法。 ProcessMindは現在、ネイティブSIEMコネクタまたはプッシュフィードを提供していません。提供は、次の3つの方法によるプル方式です。読み取りAPI（`GET /v1/tenant/{tenantId}/audit`）、制限付きエクスポートジョブ（`POST /v1/tenant/{tenantId}/audit/exports`を使用して作成し、ステータス呼び出しから結果を取得します。ステータス呼び出しは有効期間の短いダウンロードURLを返します）、およびEnterpriseアーカイブを利用する場合は、顧客のSIEMがアクセス手段を通じて読み取る、Object-Lockedバケット内の組織専用プレフィックス下にある日次オブジェクトです。ProcessMindは、顧客が指定する場所に、独自のスケジュールで記録を配信することはありません。

9.3 ProcessMind独自の監視。 ProcessMindのセキュリティ監視も同じ記録を利用します。監査ログへの書き込み失敗、認証失敗の急増、権限の変更および破壊的な管理操作により、内部アラームが発生します。

---

10. 顧客が利用できる証拠

請求に応じて、該当する場合は秘密保持を条件として、ProcessMindは本声明、セキュリティ対策、データ処理付属書、サブプロセッサー一覧、監査記録の編集済みサンプル、およびアクセス請求と消去請求に用いる手順を提供します。

---

11. 制限事項

疑義を避けるために明記すると、ProcessMindは、すべての組織について追記専用の監査ストアを維持し、監査アーカイブの利用資格が有効な場合には、夜間のマニフェスト照合を伴うObject-Locked（WORM）コピーを維持します。
ProcessMindは現在、ハッシュチェーン、ネイティブのリアルタイムSIEMプッシュコネクタ、ユーザー単位での監査記録の編集、この管理策を対象とするISO 27001またはSOC 2の保証、あるいは顧客データのすべての読み取りを対象とすることを表明していません。顧客は、アプリ内監査ログおよび外部APIを通じて、セルフサービスで記録を読み取り、エクスポートできます。