ProcessMind Security Measures

発効日：2026年9月14日

本書は、ProcessMind B.V.がCustomer Dataの機密性、完全性および可用性を保護するために維持する技術的および組織的な対策（「TOM」）について説明します。ProcessMindは、多層防御のアプローチに従っており、ネットワークおよびインフラストラクチャから、アイデンティティ、認可、データ分離、暗号化、監視およびソフトウェア開発に至るまで、あらゆるレベルで複数の独立したセキュリティ層によりCustomer Dataを保護しています。これらの対策は、Data Processing Addendum、Privacy PolicyおよびSaaS Hosting Policyを補完するものです。ProcessMindは、これらの対策を少なくとも年1回、確認および更新します。

Customer Dataが第三者に販売されること、第三者と共有されること、または第三者が自己の目的のために使用することは一切ありません。

---

1. インフラストラクチャセキュリティ

1.1 クラウドプラットフォーム。ProcessMindは、EU（ドイツ・フランクフルト、`eu-central-1`）のAmazon Web Services（AWS）上でのみhostingされています。AWSは、ISO 27001、ISO 27017、ISO 27018、SOC 1/2/3およびPCI DSSの認証を維持しています。完全な一覧については、AWS Compliance Programsをご覧ください。

1.2 サーバーレスアーキテクチャ。ProcessMindのアプリケーションロジックは、AWS LambdaおよびAWSマネージドサービス上で実行されます。ProcessMindは、顧客が管理する長期間稼働するアプリケーションサーバーを運用していないため、オペレーティングシステムのパッチ適用およびサーバー強化に関する作業の大部分が不要になります。

1.3 ネットワーク境界。ProcessMindは、データベースおよびネットワーク制御のためにAWS VPCを維持しています。Aurora PostgreSQLはインターネットへのegressがないプライベートサブネットで実行され、公開アクセスはできず、VPCフローログが有効化されています。ProcessMindは、デフォルトではアプリケーションLambda関数をVPC内に配置していません。Lambdaは、IAMおよびSecrets

Manager認証を使用し、TLS経由のAWS RDS Data APIを通じてAuroraに接続します。

1.4 コンテンツ配信およびエッジ制御。顧客向けウェブサイト、フロントエンドSPAおよび公開リソースのトラフィックは、Amazon CloudFrontを通じて提供されます。すべてのCloudFrontディストリビューションでは、TLS 1.2（2021）以上の最低TLSポリシーが適用されます。ウェブサイトおよびフロントエンドSPAのディストリビューションには、HTTP Strict Transport Security（HSTS）、Content Security Policy（CSP）、`frame-ancestors 'none'`、`X-Frame-Options: DENY`、`X-Content-Type-Options`、referrer policyおよびpermissions policyを含むセキュリティレスポンスヘッダーも追加されます。公開リソースのディストリビューションでは、CloudFront Origin Access Controlを使用してオリジンバケットを非公開にしています。顧客向けAPIトラフィックはAmazon API Gatewayを通じて別途処理されます。HTTPSのリクエスト／レスポンストラフィックは専用APIサブドメイン上のHTTP APIを通じて提供され、リアルタイムのクライアント接続は専用WebSocketサブドメイン上の別個のAPI Gateway WebSocket APIを通じて提供されます。

1.5 環境の分離。本番環境と開発環境では、別個のAWSアカウント、別個のデータベースおよび別個のインフラストラクチャスタックを使用します。開発者の認証情報では、本番環境のCustomer Dataにアクセスできません。

---

2. データ暗号化

2.1 転送中の暗号化。クライアントとProcessMindのサービス間で送信されるすべてのデータは、TLS 1.2以上を使用して暗号化されます。顧客向けエンドポイントはHTTPS経由で公開されます。ProcessMindが直接作成するS3バケット、SNSトピックおよびSQSキューでは、SSLのみのアクセスが適用されます。RDS Data APIを通じたデータベースアクセスおよびその他のAWSサービス呼び出しでは、HTTPS／TLSが使用されます。

2.2 保存時の暗号化。Aurora PostgreSQLは、顧客管理のAWS KMSキーを使用し、自動キーローテーションを有効にして保存時に暗号化されます。ProcessMindが直接作成する顧客データおよび運用用のS3バケット（アップロード、リソースおよびアクセスログのバケットを含みます）では、顧客管理のKMSキーを使用します。ProcessMindが直接作成するCloudWatchロググループ、SNSトピックおよび

SQSキューでも、顧客管理のKMSキーを使用します。SSTが管理するウェブサイトおよびフロントエンドのオリジンバケットでは、顧客管理のKMSキーではなく、AWS管理のS3サーバー側暗号化（SSE-S3／AES-256）を使用します。

2.3 キー管理およびSecrets。データベース暗号化キーはAWS KMSを通じて一元管理され、キーへのアクセスは最小権限の原則に従うIAMポリシーによって管理されます。データベース認証情報はAWS Secrets Managerに保存されます。Auroraのマスターsecretおよび制限付きアプリケーションユーザーSecretは、30日ごとに自動的にローテーションされます。本番環境のキーおよびSecretがソースコードに保存されることはありません。開発専用の認証情報は本番環境から分離されています。一部のAWS／CDK／SST管理の補助リソースでは、サービスまたはフレームワークが顧客管理キーの設定を公開していない場合、引き続きAWS管理の暗号化を使用します。

---

3. データ分離およびデータ所在地

3.1 テナント分離。各顧客テナントには、専用で分離されたデータベースインスタンスが割り当てられます。Customer Dataがデータベースレベルで他の顧客のデータと混在することはありません。共有メタデータ（アカウントレコード、請求情報、ユーザーとテナントのマッピングなど）は、厳格なアクセス制御を備えた別個のマルチテナントデータベースに保存されます。テナントおよび組織を対象範囲とする共有テーブルは、リクエスト単位のデータベースコンテキストを通じて適用されるPostgreSQLの行レベルセキュリティ（RLS）ポリシーによってさらに保護されます。

3.2 データ所在地。データベース、ファイルアップロード、バックアップおよびクエリ結果を含むすべてのCustomer Dataは、EU（ドイツ・フランクフルト）域内にのみ保存されます。EEA域外に所在するsub-processorが特定の処理活動（例えば、AIモデル処理または決済処理）のために関与する場合、移転はData Processing Addendumに記載された適切な移転メカニズムによって対象とされ、sub-processorおよびその処理場所はSub-processor Listに記載されます。

3.3 データの保持および削除。保持および削除の期間は、Data Processing Addendumの第6項に定められています。Customerは、アプリケーションを通じて、またはProcessMindに連絡することにより、いつでもデータを削除できます。

バックアップコピーは、該当するバックアップ保持期間が満了すると削除されます（第7.1項）。

---

4. アイデンティティおよびアクセス管理

4.1 認証。ProcessMindは、Microsoft Entra ID（Azure AD）、Google OAuth 2.0／OIDCおよびLinkedIn OAuth 2.0／OIDCを介したSingle Sign-On（SSO）をサポートします。ProcessMindはrelying partyとして機能し、ユーザーのパスワードを保存しません。多要素認証はidentity providerによって適用されます。例えば、組織がMicrosoft Entra ID（Azure AD）を接続する場合、その組織独自のMFAおよびアクセス・ポリシーが適用されます。

4.2 セッション管理。ブラウザセッションでは、SameSiteおよびSecureフラグを備えた安全なHttpOnly Cookieを介して送信される署名付きJSON Web Token（JWT）を使用します。トークン署名は、認証された各リクエストで検証されます。

4.3 認可モデル。ProcessMindは、コアアプリケーションAPIについてAPI Gatewayのネイティブauthorizerに依存していません。認可は、ビジネスロジックの実行前にセッション状態およびテナント範囲を検証する共有Lambdaハンドララッパーで適用されます。公開ルートは、認証されないフロー、webhook、イベント取り込みおよびCORS preflightのために明示的にallowlist化されています。外部APIエンドポイントでは専用の認証ハンドラを使用します。Customer Dataへのアクセスは、認証されたテナントまたは組織のコンテキストに限定されます。

4.4 最小権限。内部システムは、最小権限の原則に従います。IAMロールは、フレームワークが正確な範囲設定を許可する場合、必要な最小限のリソースに限定されます。一部のSST／CDK生成ロールでは、バインディングおよびランタイム運用のために、より広範な管理ポリシーまたはインラインポリシーを使用します。これらのケースは確認され、可能な場合はリソース範囲が設定され、明示的な例外として追跡されます。

4.5 従業員アクセス制御。内部システムへの従業員アクセスは、SSOおよび必須MFAを備えたActive Directoryを通じて管理されます。ロールベースアクセス制御

（RBAC）により、Customer Dataへのアクセスは、知る必要がある承認済み担当者に限定されます。アクセス権は定期的に確認されます。

---

5. ロギング、監視および監査

5.1 一元化されたロギング。HTTP APIアクセスログおよびWebSocketアクセスログは、構造化されたJSONフィールドを備えて有効化され、Amazon CloudWatch Logsに1週間保持されます。これらのアクセスロググループは、顧客管理のAWS KMSキーで暗号化されます。アプリケーションログは、顧客管理のAWS KMSキーで暗号化されたAmazon CloudWatchロググループに一元化され、10年間保持されます。別個の監査ロググループおよびテレメトリロググループも、顧客管理のAWS KMSキーで暗号化され、10年間保持されます。Aurora PostgreSQLエンジンのログエクスポートグループは1週間保持されます。

5.2 ログに記録されるものと記録されないもの。ProcessMindは、リクエスト時刻、リクエスト識別子、ルートまたはパス、レスポンスステータス、レイテンシー、送信元IPおよびユーザーエージェントを含むHTTP APIおよびWebSocketのアクセスイベントをログに記録します。ProcessMindは、認証イベント、非同期の失敗経路および補助的なLambdaアプリケーション活動も、一元化されたCloudWatchロググループに記録します。VPCフローログは有効化されています。ProcessMindは現在、ウェブサイト、フロントエンドSPAまたは公開リソースのディストリビューションでCloudFront標準アクセスログを有効化していません。

5.3 監視およびアラート。CloudWatchアラームおよびダッシュボードは、システムの健全性、デッドレターキューおよびセキュリティに関連する障害を監視します。非同期処理の障害は、暗号化されたデッドレターキュー（保持期間14日、thumbnailおよびsearch-indexキューは2日）に送られ、DLQアラームは調査のためにSNS通知を発します。さらに、ProcessMindは、フロントエンドのエラー追跡、パフォーマンス監視およびセッションリプレイにSentryを使用します。セッションリプレイは、エラーが発生したセッションについてのみ記録され、リプレイではテキスト、フォーム入力およびメディアがマスクまたはブロックされます。SentryデータはEU（フランクフルト）で取り込まれ、ProcessMind Usage Data（ブラウザエラー、パフォーマンストレース、デバイスメタデータおよびマスクさ

れたリプレイ記録）に限定されます。Sentryはsub-processor listに記載されています。

5.4 ログの保護。ログは、専用のアクセス制御されたCloudWatchロググループに保存され、保存時に暗号化されます。本番環境と開発環境のログは、環境およびアカウントの境界によって分離されます。

---

6. 自動化された管理策の検証および脆弱性管理

6.1 ProcessMindが行うこと。ProcessMindは、複数の業界ルールパック（AWS Solutions、NIST 800-53およびPCI DSSを含みます）を使用し、インフラストラクチャの合成およびデプロイワークフローの一環として`cdk-nag`を実行します。スタックごとのレポートが生成され、インフラストラクチャ変更管理の一環として確認されます。検出事項は、修正済み、受容したリスクまたは計画された改善としてトリアージされます。

6.2 例外の管理方法。抑制は、フレームワークが許可する場合は中央レジストリに記録され、影響を受けるスタックに範囲を限定され、書面による正当化を必要とします。スタックにインライン抑制が含まれる場合は、そのスタックと併せて文書化されます。検出事項が是正された場合、対応する抑制は更新または削除されます。ProcessMindは、抑制をレビューからの包括的なオプトアウトとはみなしません。

6.3 ProcessMindが現在行っていないこと。ProcessMindは、重要なインフラストラクチャ管理策の例外を追跡および確認しています。主なものは以下のとおりです。

- デフォルトでは、アプリケーションのLambdaはVPC内に配置されておらず、TLS経由のRDS Data APIを通じて、IAMおよびSecrets Manager認証によりAuroraに接続します
- WebSocket APIおよび静的配信はAWS WAFの背後にありません（WebSocket接続では短期間有効なHMACトークンを使用し、決済関連の地域制限は決済システムで適用されます）。また、静的配信ではCloudFront標準アクセスログを有効にしていません

- データベースの復旧は、別個のAWS BackupプランまたはAurora Enhanced Monitoringではなく、Auroraの自動バックアップおよびポイントインタイムリカバリに依存します
- 変更可能なバケットについて、リージョン間S3レプリケーションまたはS3 Object Lockはありません
- 一部のAWS/CDK/SST管理の補助リソースでは、サービスが顧客管理の代替手段を提供していない場合、AWS管理の暗号化または生成された、より広範なIAMポリシーを使用します

完全な抑制レジストリはインフラストラクチャコードと併せて維持されており、請求に応じて提供できます。`cdk-nag`ルールパックの使用は、エンジニアリングによる統制の検証であり、HIPAA、NISTまたはPCI DSSの外部認証、監査意見または法的証明ではありません。

6.4 依存関係管理。ソフトウェア依存関係について、既知の脆弱性を継続的に監視します。重大度がCriticalまたはHighの脆弱性は、7日以内を目標として修正します。依存関係は定期的なサイクルで更新します。

6.5 セキュアソフトウェア開発ライフサイクル（SDLC）。ProcessMindは、ソフトウェア開発において多層防御のアプローチを採用しています。本番環境へのすべての変更は、デプロイ前に複数の独立した自動検証レイヤーを通過する必要があります。

- **静的解析および型安全性：**TypeScriptのstrictモードおよびESLintにより、コンパイル時に型の正確性、null安全性およびセキュリティに関連するコーディングパターンを適用します。
- **AI支援コードレビュー：**AI支援分析により、プルリクエストに対する追加のレビュー観点を提供し、自動テストを補完しながら、セキュリティリスク、ロジックエラーおよび規約からの逸脱を特定します。
- **単体テストおよび統合テスト：**包括的なVitestテストスイートにより、開発環境の実際のAWSリソースに対して、ビジネスロジック、データアクセスパターン、APIの動作およびエラー処理を検証します。
- **エンドツーエンドテスト：**Playwrightベースのブラウザテストにより、認証、データアップロード、プロセスモデリング、シミュレーションおよびマルチテナント分離を含む重要なユーザーワークフローを検証します。

- **インフラストラクチャコンプライアンススキャン：**`cdk-nag`変更のたびに、複数のコンプライアンスフレームワークに照らしてInfrastructure as Codeを検証します。
- **依存関係の脆弱性スキャン：**自動化された依存関係監査により、既知の重大度がCriticalまたはHighの脆弱性が本番環境に到達することを阻止します。

人的レビューは、行単位のコード検査ではなく、アーキテクチャ、セキュリティ境界および設計レベルの判断に重点を置きます。構造、セキュリティまたはインフラストラクチャに関わる変更については、自動検証に加えて、明示的な人的承認が必要です。

すべての検証レイヤーは、mainブランチへの変更に必要なマージゲートとしてCIを通じて適用されます。緊急の本番修正ではCIゲートを回避できますが、24時間以内に完全なパイプライン実行およびインシデント後レビューを実施しなければなりません。

---

7. バックアップおよび災害復旧

7.1 自動バックアップ。Amazon Auroraは、7日間の保持期間で継続的かつ自動的なバックアップを実行します。バックアップは、ソースデータベースと同じ顧客管理KMSキーを使用して暗号化されます。

7.2 ポイントインタイムリカバリ。Auroraは、バックアップ保持期間内の任意の秒時点へのポイントインタイムリカバリをサポートし、データ破損または誤削除が発生した場合の迅速な復元を可能にします。

7.3 S3の耐久性およびバージョニング。ファイルアップロードおよび運用アーティファクトは、99.999999999%（イレブンナイン）の耐久性を提供するAmazon S3に保存されます。復旧およびロールバックをサポートするため、uploadsバケットおよびresourceバケットではバージョニングが有効になっています。ウェブサイトおよびフロントエンドのデプロイバケットは再現可能なビルドアーティファクトであり、バックアップシステムとして扱いません。ProcessMindは現在、リージョン間S3レプリケーションを有効にしていません。

7.4 事業継続性。災害復旧手順は文書化され、定期的にテストされています。概要はDisaster Recovery, Business Continuity & Incident Response文書で確認できます。アーキテクチャは`eu-central-1`リージョン内のAWS管理サービスに依存しており、AWSはこれらを複数のアベイラビリティゾーンにわたって運用しています。Auroraクラスターは現在、単一の書き込みインスタンスで稼働しているため、データベースの復旧はリージョン内のスタンバイではなく、自動バックアップおよびポイントインタイムリカバリに依存します。Auroraバックアップ、S3の耐久性、デッドレターキューおよびソースから再構築可能な静的アセットは、復旧戦略の一部です。

---

8. インシデント対応

8.1 インシデント通知。DPAで定義されるセキュリティインシデントが発生した場合、ProcessMindは、不当な遅延なく、また可能な場合にはインシデントを認識してから72時間以内に、影響を受ける顧客に通知します。

8.2 インシデント処理。ProcessMindは、特定、封じ込め、根絶、復旧およびインシデント後レビューを対象とする、文書化されたインシデント対応手順を維持しています。概要はDisaster Recovery, Business Continuity & Incident Response文書で確認できます。インシデントから得られた教訓は、セキュリティ統制およびプロセスに反映されます。

8.3 コミュニケーション。インシデント通知には、インシデントの性質および範囲、影響を受けたデータのカテゴリー、インシデントを封じ込めるために講じた措置ならびに顧客に推奨する対応を含めます。

---

9. 組織的措置

9.1 情報セキュリティ管理。ProcessMindは、ISO 27001の原則に沿った情報セキュリティ管理システムを維持しています。ProcessMindは、ISO 27001認証およびSOC 2 Type II保証報告に向けた認証方針を選択していますが、正式な認証プロセスはまだ開始していません。

9.2 セキュリティ意識。Customer Dataへのアクセス権を有するすべての人員は、セキュリティ意識向上研修を受けます。セキュリティのベストプラクティス

は、オンボーディング、開発ワークフローおよび運用手順に組み込まれています。

9.3 ベンダーおよびサブプロセッサー管理。サブプロセッサーは、本書に記載するものと同等のデータ保護基準を契約上遵守する義務を負います。ProcessMindは公開のサブプロセッサーリストを維持し、新たなサブプロセッサーを起用する少なくとも30日前に通知します。サブプロセッサーについて、コンプライアンスを年1回確認します。

9.4 機密保持。Customer Dataの処理を許可されたすべての人員は、書面による機密保持義務を負います。

---

10. コンプライアンスおよび認証

フレームワーク／標準	状況
GDPR（EU一般データ保護規則）	準拠
EUデータレジデンシー（ドイツ、フランクフルト）	適用済み
AWSインフラストラクチャ認証（ISO 27001、SOC 2、PCI DSS）	AWSを通じて継承
ISO 27001（ProcessMind）	予定 ー 認証方針を選択済み、正式なプロセスは未開始
SOC 2 Type II（ProcessMind）	予定 ー 認証方針を選択済み、正式なプロセスは未開始
自動化されたインフラストラクチャ統制の検証（cdk-nagAWS Solutions、HIPAA Security、NIST 800-53 R4/R5、PCI DSS 3.2.1、Serverlessにわたる）	認証ではなく、エンジニアリングによる統制の検証として実施済み
国際移転に関する標準契約条項（SCC）	実施済み（DPAを参照）

フレームワーク／標準	状況
Data Processing Addendum（DPA）	公開済み

cdk-nagルールパックの使用は、ProcessMindがHIPAA、NISTまたはPCI DSSについて正式な認証を取得していること、または独立した監査を受けていることを意味しません。これらのルールパックは、インフラストラクチャ設計を検証し、ギャップを明示的に追跡するためのエンジニアリング上のガードレールとして使用されます。

セキュリティ、コンプライアンスに関する質問、または監査報告書や記入済みセキュリティ質問票などの文書の請求については、**support@processmind.com**までご連絡ください。