ProcessMind災害復旧、事業継続およびインシデント対応

発効日：2026年9月14日

本書は、ProcessMind B.V.のクラウドサービスに関する災害復旧（「DR」）、事業継続（「BCP」）およびセキュリティインシデント対応手順の概要を示すものです。本書は、セキュリティ対策、SaaSホスティングポリシー、サービスレベル契約およびデータ処理補遺を補足するものです。

本書は当社の現在のアプローチを説明するものであり、適用される契約、DPAまたはSLAに明示的に定められている場合を除き、別個の契約上の復旧時間目標、復旧時点目標、データ耐久性保証、通知期限、サービスレベルまたは責任基準を設定するものではありません。

---

1. 目的および適用範囲

ProcessMindは、以下の目的でこれらの手順を維持しています。

- 障害事象中に顧客データの機密性、完全性および可用性を保護する
- ProcessMindが管理するシステムの障害後に、重要な本番サービスコンポーネントを復旧する
- サービスの中断中も、インシデント管理、顧客とのコミュニケーションおよび運用上の意思決定を継続する
- 文書化された手順およびソース管理されたインフラストラクチャ定義を使用して、インフラストラクチャ、デプロイ、アプリケーションまたはデータ層の障害から復旧する
- セキュリティインシデントを特定および評価し、脅威を封じ込め、根本原因を排除し、影響を受けたシステムを復旧し、必要に応じて連絡を行い、得られた教訓を記録する

これらの手順は、本番ProcessMindクラウドサービス、およびサービスに影響を及ぼし、ProcessMindが合理的に調査および管理できる範囲において、サブプロセッサーまたはクラウドサービスに関係するセキュリティ事象に適用されます。開発環境およびテスト環境は分離されており、顧客向け本番に関する取り組みの復旧対象とはみなされません。

---

2. レジリエンス戦略

2.1 リージョン設計。本番サービスはAWS EU（ドイツ、フランクフルト、`eu-central-1`）でホスティングされています。アーキテクチャは、AWSが複数のアベイラビリティゾーンにわたって運用する当該リージョン内のAWSマネージドサービスに依存しています。Auroraクラスターは現在、単一のライター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。ProcessMindは現在、顧客データ用の第2のアクティブリージョンを運用していません。

2.2 マネージドサービスおよびサーバーレスサービス。ProcessMindは、AWS Lambda、Amazon API Gateway、Amazon CloudFront、Amazon Aurora PostgreSQL、Amazon S3、Amazon SQS、Amazon SNSおよびAmazon CloudWatchに依存しています。これにより、顧客が管理する長期稼働サーバーへの依存が軽減され、アプリケーションおよび静的コンポーネントについて、ソースから再構築する復旧が可能になります。

2.3 環境分離。本番環境と開発環境は、別個のデータベースおよびインフラストラクチャスタックを備えた別個のAWSアカウントで運用されています。これにより、開発活動が本番の復旧運用に影響を及ぼすリスクが軽減されます。

2.4 監視および検出。CloudWatchアラーム、ダッシュボード、デッドレターキューのアラート、集中ログおよび合成サービス監視により、インシデントの検出、トリアージおよびエスカレーションを支援します。潜在的なインシデントは、サポート受付、従業員からの報告、ベンダーからの通知その他の調査の契機を通じて特定されることもあります。

---

3. 復旧の優先順位

重大なインシデントが発生した場合、ProcessMindの復旧の優先順位は、通常、以下のとおりです。

1. 顧客データの完全性を保護し、さらなる損害を防止する。
2. インシデントを封じ込め、影響を受けたシステムを安定化する。
3. 中核となる本番アクセス経路および重要なワークフローを復旧する。

4. 復旧完了を宣言する前に、サービスの動作、データの完全性および監視を検証する。
5. 状況の更新、顧客への影響およびフォローアップ措置を伝達する。

正確な順序は、データの完全性、顧客アクセス、非同期処理またはサポートインフラストラクチャのいずれに影響するかを含め、インシデントの性質に応じて異なることがあります。

---

4. 災害復旧手順

4.1 インシデントの宣言および調整。重大なサービス中断およびセキュリティインシデントは、インシデント対応手順を通じてトリアージされます。ProcessMindは、インシデントリードを指名し、対応への参加を承認された担当者に限定し、重大度および範囲を評価し、技術対応者を調整し、インシデントが解決または格下げされるまで復旧措置を追跡します。

4.2 封じ込め。ProcessMindは、より広範な復旧を開始する前に、継続中の影響を停止または軽減するため、商業上合理的な努力を行います。障害モードに応じて、封じ込め措置には、最近の変更のロールバック、影響を受けた経路の無効化、誤動作しているコンポーネントの隔離、完全性チェック中のバックグラウンド処理の一時停止、認証情報の失効またはローテーション、悪用行為のブロックなどが含まれることがあります。

4.3 根絶。直ちに生じた影響が安定した後、ProcessMindは根本原因または寄与した状態の除去に取り組みます。これには、コードまたは設定の修正の適用、悪意のあるアーティファクトの削除、シークレットのローテーション、信頼できる設定の復元、公開されたアクセス経路の閉鎖などが含まれることがあります。

4.4 データベースの復旧。Aurora PostgreSQLは、7日間の保持期間で継続的な自動バックアップを実行し、ポイントインタイムリカバリをサポートします。データベースレベルの障害、破損事象または誤った破壊的変更により復元が必要となった場合、ProcessMindは、適切な最新のバックアップから、または選択した時点まで復元し、復元された環境を検証した上で、アプリケーションのトラフィックを復旧したデータベース経路に戻すことがあります。

4.5 オブジェクトおよびアーティファクトの復旧。顧客によるファイルのアップロードおよび運用アーティファクトは、Amazon S3に保存されます。アップロードバケットおよびリソースバケットでは、誤削除または上書きのシナリオからの復旧を支援するため、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アーティファクトとして扱われ、バックアップから復元するのではなく、ソースから再構築されることがあります。

4.6 非同期ワークロードの復旧。非同期処理経路では、調査のために失敗したイベントを保持するデッドレターキューを使用します。復旧には、失敗したメッセージの再試行、処理ロジックの再実行、または基礎となるワークフローが安全な再処理をサポートする場合の作業の再生が含まれることがあります。

4.7 アプリケーションおよびインフラストラクチャの再構築。インフラストラクチャは、ソース管理されたInfrastructure as Code定義を通じて管理されます。アプリケーションインフラストラクチャまたは静的アセットを再作成する必要がある場合、ProcessMindは、バージョン管理された定義およびビルドアーティファクトから影響を受けたコンポーネントを再構築および再デプロイできます。

4.8 サービス復帰前の検証。インシデントを終了する前に、ProcessMindは、利用可能な監視、ログ、合成チェックおよび対象を絞った機能検証を使用してサービスの健全性を検証し、検証済みのデプロイ、復旧およびインフラストラクチャ手順を使用して影響を受けた機能を復元します。インシデントにデータの復元またはデータ完全性のリスクが関係していた場合、追加のレビューが実施されることがあります。

---

5. 事業継続措置

5.1 運用継続。ProcessMindは、障害事象中もインシデント対応、顧客サポートの受付、エンジニアリング対応および意思決定を継続できるよう、文書化された運用手順を維持しています。

5.2 コミュニケーション。重大な本番インシデントについて、ProcessMindは、顧客サポートチャネルおよび、適切な場合には公開ステータスページprocessmind.com/statusを通じて更新情報を提供するため、商業上合理的な努力を行います。

5.3 管理された変更管理。複数の独立した自動検証レイヤー、管理されたデプロイ、集中監視およびインシデント後のレビューを備えた多層防御型のソフトウェア開発ライフサイクルを使用し、回避可能な停止を減らし、時間の経過とともに継続性を向上させています。

5.4 復旧中のセキュリティ。復旧措置は、通常の運用中に適用されるものと同じ一般的なセキュリティ原則に従って実施されます。これには、最小権限アクセス、可能な場合の運用活動の記録、本番システムおよびデータへのアクセス管理が含まれます。

---

6. バックアップおよびデータ保護の概要

6.1 データベースのバックアップ。Auroraの自動バックアップは暗号化され、7日間保持されます。この保持期間内では、ポイントインタイムリカバリを利用できます。

6.2 S3 Protections. Amazon S3は、保存されたオブジェクトに高い耐久性を提供します。変更可能な顧客データバケットは、プライマリリージョン内の耐久性およびバージョニングに依存します。ProcessMindは、現在、これらのバケットについてリージョン間S3レプリケーションを有効にしていません。

6.3 Logs and Diagnostics. 集中管理されたログ、アラームおよびテレメトリは、障害の調査および復旧の検証を支援します。これらの仕組みは継続運用を支援しますが、それ自体が別個のバックアップ製品として提示されるものではありません。

---

7. インシデントの特定およびトリアージ

7.1 初期評価。 報告された事象について、Security Incidentの定義に該当するか、影響を受ける可能性のあるシステムまたはデータ、想定される範囲および重大度、ならびに直ちに封じ込めが必要かどうかを判断するため、トリアージを実施します。証拠の保全は、インシデントの性質および関係するシステムに適した方法で取り扱います。

7.2 オンコールおよびエスカレーション。 ProcessMindは、本番環境のインシデントについてオンコール対応を維持しており、インシデントをいつでも受領確認し、

トリアージできるよう、Criticalインシデント（Service Level Agreementに定義されるもの）については24時間365日の対応を含みます。

7.3 文書化。 ProcessMindは、重要な調査結果、対応措置および復旧に関する判断を文書化し、インシデントの経過およびその結果としての是正措置を事後に確認できるようにします。

---

8. コミュニケーションおよび通知

8.1 内部コミュニケーション。 ProcessMindは、インシデントのライフサイクル全体を通じて技術的対応と顧客とのコミュニケーションの整合性を維持できるよう、対応担当者、意思決定者およびサポートチャネルを調整します。

8.2 顧客への通知。 DPAまたは適用法に基づく通知が必要なSecurity Incidentが発生した場合、ProcessMindは、影響を受ける顧客に不当な遅延なく、また可能な場合にはインシデントを認識してから72時間以内に通知します。通知には通常、インシデントの性質および範囲、判明している場合は影響を受けたデータのカテゴリー、インシデントの封じ込めおよび是正のために講じた措置、ならびに関連する場合は顧客に推奨される対応が含まれます。

8.3 継続的な更新。 インシデントが継続している場合、または重要な事実に変更がある場合、ProcessMindは、追加の検証済み情報が利用可能になり次第、続報を提供します。より広範な本番サービスの障害については、ProcessMindは顧客サポートチャネルおよび、適切な場合には公開ステータスページ（processmind.com/status）も使用することがあります。

---

9. テスト、レビューおよび保守

ProcessMindは、これらの手順を少なくとも年1回、ならびに重大なインシデントまたは重要なアーキテクチャ変更の後にレビューし、対応および復旧のアプローチに関連する要素（バックアップの復元、デプロイメントの再構築、監視、アラートおよびインシデントコミュニケーションなど）を定期的に演習し、得られた教訓をセキュリティ、信頼性および継続性に関する手順に反映します。

---

10. 制限および契約上の境界

本書は高レベルの概要であり、すべての内部ランブック、エスカレーション経路、調査方法または証拠取扱い手順を運用上の詳細まで記載するものではありません。本書は、適用される契約または注文書に明示的に記載されている範囲を超えて、別個のリージョン間フェイルオーバー設計、すべての変更可能なバケットについての不変ストレージ保持、または独立したRTO/RPO保証をProcessMindに義務付けるものではありません。

本書と、適用されるCustomer Agreement、Data Processing Addendum、Service Level Agreementまたは強行法規との間に矛盾がある場合は、それらの定めが優先します。