SailPoint

SailPoint Identity Security Cloud

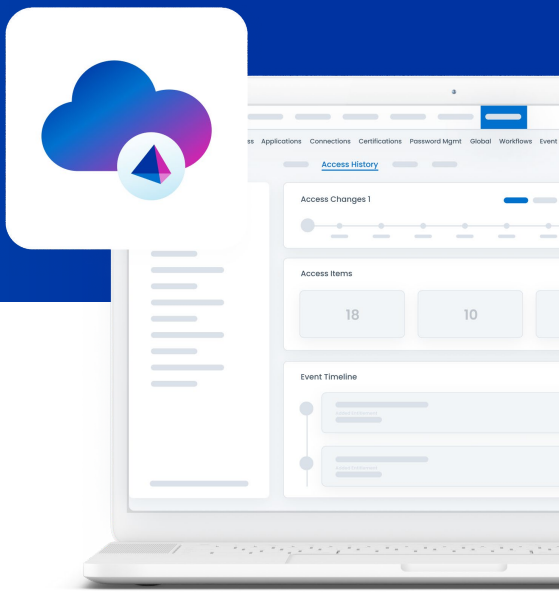
アイデンティティ管理にも ガバナンスを

エンタープライズ セキュリティの 要にアイデンティティを

ユニファイド アイデンティティ セキュリティ ソリューションで最小権限を確保

先進的な企業は、経営幹部や取締役会からの圧力だけでなく、外部からの規制要求に応じるためにサイバー セキュリティ対策を講じると同時に、従業員の生産性向上や運用コストの削減、利益の増大を追求しています。変化の激しい環境の中で、何千ものアイデンティティと、重要なアプリケーションへのアクセス権限を管理することは、セキュリティを強化するうえで極めて重要な要素です。しかしながら、アイデンティティとセキュリティの各チームは、アクセス権限の制御とガバナンスへの対応に苦慮している現実があります。サイロ化したシステムでは手作業を排除することが難しく、過剰なアクセス権限を付与することにつながり、結果としてコンプライアンス違反や不要なリスクを引き起こします。

SailPoint Identity Security Cloud は、信頼性の高いアイデンティティ セキュリティ プログラムを企業が効率的に構築できるように設計されています。



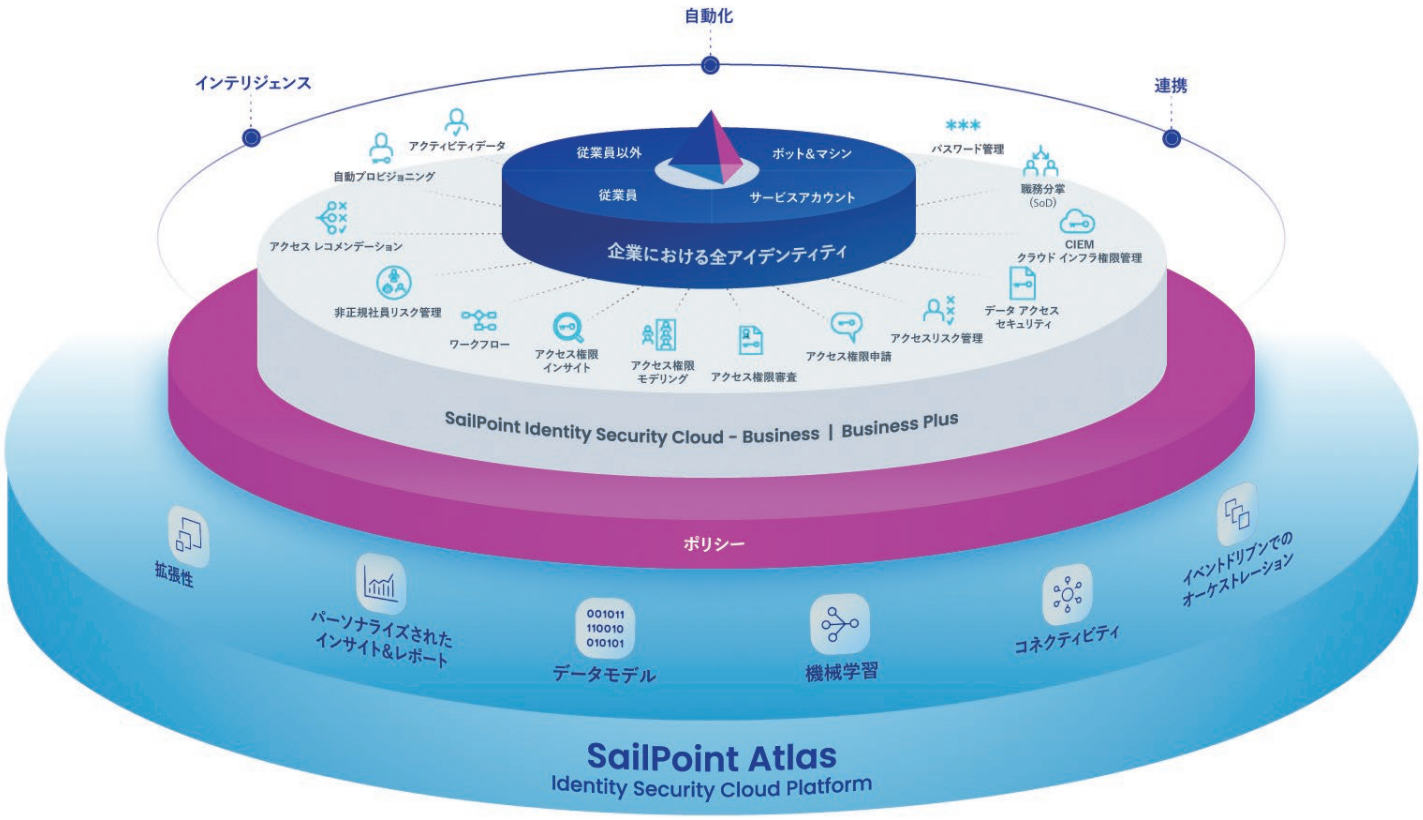
AI と機械学習の技術を活用することで、優れたインテリジェンス、円滑な自動化に加え、アイデンティティに関する包括的な統合連携を実現。企業は、SailPoint Identity Security Cloud によって、企業における全てのアイデンティティの重要なデータやアプリケーションへのアクセス権限をリアルタイムで管理・保護できます。SailPoint は、大手のグローバル顧客企業と共に歩んできた経験から、ユーザーが業務を遂行するうえで必要となるアクセス権限の最小権限を確保するための要件の理解を深めてきました。それは、領域に特化した、単一のユニファイド ソリューションとして機能する SaaS ベースの製品です。

SailPoint Atlas のプラットフォームを基盤とした SailPoint ソリューションは、昨今の複雑な IT 環境に求められる柔軟性、導入のしやすさ、ユーザー中心の設計を提供。アイデンティティ セキュリティへの取り組みのあらゆる段階で、組織が求めるニーズを満たすように設計されており、アイデンティティ要件の規模や対象範囲の拡大、複雑さの増大に合わせて、より高度な機能を提供します。

ユニファイド
インテリジェント
パワフル

SailPoint Atlas
Identity Security Platform

SailPoint Atlas は、次世代のアイデンティティ プラットフォームであり、組織がアイデンティティ セキュリティにおける新たな課題に取り組む際に、ソリューションを再構築することなく対応できるように設計された製品です。このユニファイド プラットフォームは、最先端の AI、ユニファイド アプローチ、拡張性に優れたアーキテクチャを 1 つにしたもので、アイデンティティ セキュリティを再定義するものです。SailPoint Atlas は、SailPoint Identity Security Cloud ソリューションの基盤であり、統合連携の強化、さらなる柔軟な設定、メンテナンス費用の削減を実現。これにより、組織は短期間でその価値を享受でき、より適切なアプローチでの導入、さらにはユーザー エクスペリエンスの改善が可能になります。また、独自のインサイトとガバナンスの合理化により、アクセス制御、ポリシー、プロセスの強化を行い、動的なデジタル環境におけるセキュリティ、効率性、適応性を確保することで企業を包括的に強化します。



製品モジュール

変化するアイデンティティ セキュリティのニーズに対応する機能

SailPoint Identity Security Cloud ソリューションは、次に挙げる 4 つの製品モジュールから構成されています。現代のアイデンティティ セキュリティのニーズに合わせて設計された独自の機能を提供しつつ、将来のニーズにも対応する優れた拡張性を備えています。

ライフサイクル管理

アイデンティティのライフサイクルの自動化と管理を実現

コンプライアンス管理

アイデンティティ プロセスの合理化と、アクセスガバナンスを強化

アクセス権限モデリング

アクセス権限のグループ（ロール）を、ニーズに合わせて構築

アナリティクス

アイデンティティに関する実用的なインサイトで、より適切にアクセス権限に関わる意思決定を支援

アイデンティティ セキュリティを進化させる SailPoint Identity Security Cloud

適切なアクセス権限の付与：

- 最小権限の原則（PoLP）モデルに基づき、すべてのアイデンティティに適切なアクセス権限をタイムリーに付与することで、生産性を向上
- 属性に応じた柔軟な設定のアプローチでアクセス権限モデルを構築し、セキュリティの確保と、適切なアクセス権限の付与を両立

アイデンティティのリスク管理：

- セキュリティ担当者が、アイデンティティとアクセス権限における潜在的なリスクの特定・管理が可能に
- 脅威と脆弱性に対して先手を打つことで、セキュリティ態勢を強化し、侵害による被害を最小化

アクセス権限に関する意思決定の迅速化：

- 事業部門のマネージャーやアプリケーション管理者が、アクセス権限に関する意思決定を、情報に基づいて迅速に実施可能に
- 個別のインサイトと自動化されたワークフローにより、複数部門にまたがるプロセスの迅速化と効率化を実現

コンプライアンス対応業務の簡素化：

- 社内の監査担当者に、コンプライアンスの遵守状況を容易に証明できる使いやすいツールを提供
- コンプラインス対応のための業務プロセスを簡素化することで、シームレスで正確な監査が実施され、規制要件への遵守を証明可能に

特権管理タスクの自動化：

- 特権管理に関わる反復的なタスクを自動化し、効率性に加えて、セキュリティとガバナンスを強化
- 特権のセッションを開始したり、クレデンシャルを共有することなく、特権管理に関わるタスクの実行を委任
- 特権管理に関わる認証の集約と、タスクの委任と実行のためのレポジトリー

SailPoint Identity Security Cloud 製品パッケージ

Standard

- ✓ 手動によるロールの割り当てとサポート
- ✓ アクセス権限の自動プロビジョニング
- ✓ アクセス権限の申請・付与
- ✓ アクセス権限審査（棚卸）
- ✓ 職務の分離（SoD）
- ✓ アクセス インテリジェンス センター - 既製のダッシュボード
- ✓ アクセス権限履歴

Add-ons

- ＋ クラウド インフラ権限管理（CIEM）

Business

Standard に記載されているもの全てに加え

- ✓ アプリケーション オンボーディング
- ✓ ロールと共通アクセス権限の検出
- ✓ アクセス権限のリクエスト管理
- ✓ アクセス権限審査（棚卸）のリコメンデーション
- ✓ アイデンティティの外れ値 - 閲覧のみ
- ✓ アクセス インテリジェンス センター - オーサリング
- ✓ アクティビティ インサイトによるアクセス権限履歴

Add-ons

- ＋ クラウド インフラ権限管理（CIEM）
- ＋ 非正規社員リスク管理(NERM)
- ＋ データ アクセス セキュリティ
- ＋ パスワード管理
- ＋ GRC とアクセスリスク管理
- ＋ マシン アイデンティティ セキュリティ (MIS)

Business Plus

Business に記載されているもの全てに加え

- ✓ エンタイトルメントの説明文を生成 AI で作成
- ✓ アクティビティ インサイトによるロール検出と共通アクセス検出
- ✓ アクティビティ インサイトによるアクセス権限審査（棚卸）
- ✓ クラウド インフラ権限管理（CIEM）
- ✓ アイデンティティの外れ値 - スコアリング、コンテキストインサイト、ワークフロー

Add-ons

- ＋ 非正規社員リスク管理(NERM)
- ＋ データ アクセス セキュリティ
- ＋ パスワード管理
- ＋ GRC とアクセスリスク管理
- ＋ マシン アイデンティティ セキュリティ (MIS)

アドオン機能

多彩なアイデンティティ全体に、セキュリティを拡充

SailPoint Identity Security Cloud は、個別のユース ケースに対応したアドオン機能も提供。アイデンティティ プログラムのレベルを引き上げるのに役立つ重要な機能により、アイデンティティ エコシステム全体にセキュリティを拡張できます。

クラウド インフラ権限管理 (CIEM)

「SailPoint クラウド インフラ権限管理 (CIEM)」は、明確に定義されたポリシーを適用し、IaaS のアクセス権限のライフサイクル管理を自動化。単一のアプローチでマルチクラウド インフラストラクチャを管理できるようになります。アイデンティティ重視のアプローチに基づくこのソリューションは、クラウドにアクセスできるエンタイトルメントの検出と権限審査 (棚卸) の統制を支援します。

非正規社員リスク管理 (NERM)

「非正規社員リスク管理 (NERM)」は、契約社員や提携パートナーなどの非正規社員を対象に、リスクに基づいたアクセス権限管理とライフサイクル戦略を実現。オペレーションを効率化することで、新たな営業活動の促進、法規制遵守のサポート、非正規社員によるリスクの低減を支援します。

データ アクセス セキュリティ

「データ アクセス セキュリティ」は、重要な非構造化データを検出、統制、保護する機能です。リスクを最小限に抑えつつ、自動化されたワークフローと組込み済みのポリシーで生産性を向上させ、重要なデータへのアクセス権限に関する詳細なインサイトとアラートを活用して、コンプライアンス要件への対応を実現します。

GRC とアクセス リスク管理

「GRC とアクセス リスク管理」は、アクセス権限のリスク ガバナンスを一元化して、GRC とのシームレスなインテグレーションを実現。アクセス権限を全方位的に可視化することで、職務分掌 (SoD) の違反を防止すると共に、アクセス権限レビューの自動化、リスク軽減対策の文書化、緊急アクセスの監視、先を見越したリスク シミュレーションの実施などにより、コンプライアンス対応を効率化します。

パスワード管理

「SailPoint のパスワード管理機能」は、パスワード ポリシーを効率的に使用して強力なパスワード要件を適用。同期グループとパスワード ディクショナリを通じてリスクを最小限に抑えながらコントロールを強化します。これにより、ユーザーの生産性を高めながら、IT 部門の負荷を最小化できます。

マシン アイデンティティ セキュリティ (MIS)

「SailPoint マシン アイデンティティ セキュリティ (MIS)」は、サービス アカウントやボット、RPA など、人以外のマシン アイデンティティを管理。マシン アカウントの検出から分類・タグ付けを効率的に行い、状況が変化する中でも、常に責任者 (オーナー) を割り当てることが可能です。人のアイデンティティと同等の可視化と制御のもとでガバナンスを確立し、アイデンティティ セキュリティ プロセスを合理化しながら包括的な管理を実現します。

アイデンティティ セキュリティの道のりを共に歩むパートナーに SailPoint が選ばれています

SHIONOGI　セブン銀行　MOTION & CONTROL NSK　LINEヤフー

Allianz　PHILIPS　HARVARD UNIVERSITY　SAMSUNG BIOLOGICS

（一部抜粋）

選ばれる理由があります

ビジネスインパクト

90%
IT 関連の効率性が向上

90%
アイデンティティ関連のタスクを自動化

アクセス権限審査（棚卸）

1 年 > **1** ヶ月

新規ユーザーのプロビジョニング

14 時間 > **2.5** 分

アカウントのプロビジョニング解除（デプロビジョニング）

30+ 日 > **0** 日

80 万 US ドルのコスト削減

SailPoint について

SailPoint は、現代の先進的な企業が、アプリケーションやデータの安全な利用を、アイデンティティの観点から、スピードと拡張性を持って、継ぎ目のない一枚岩のプラットフォーム上で管理・保護することを支援しています。アイデンティティ セキュリティのカテゴリー リーダーである SailPoint は、企業のシステム環境の安全性を確保する基盤としてのアイデンティティ セキュリティを、これからも進化させ続けていきます。SailPoint が提供するインテリジェントで拡張性が高い包括的なユニファイド プラットフォームは、アイデンティティを標的にしたダイナミックなサイバー脅威から組織を保護するとともに、企業の生産性と効率性を向上させます。企業が、ビジネス変革を牽引する安全なテクノロジー エコシステムを先進的で高度に作り上げる支援を提供していきます。

sailpoint.com/ja

SP2488-2412