SailPoint が提案する SAP 向け アイデンティティ セキュリティ

異なるビジネス プロセスを統合する場合、企業の多くが SAP の ERP ツールやシステムを利用しています。SAP 環境は非常に複雑で、モジュール、アプリケーション サーバー、レガシー インターフェース、カスタマイズ環境のほか、複数のシステム ランドスケープで構成されています。

この複雑な環境を可視化できる機能、特に SAP のシステムやアプリケーションへのユーザー アクセスを容易に管理・統制できる機能は、組織のセキュリティ対策を強化し、生産性とオペレーションを向上させる上で非常に重要です。SAP によるビジネス変革の潮流や、複雑さを増す SAP 環境も、セキュアで包括的なアクセス ソリューションがますます求められる要因となっています。

- SAP が発表した「クラウドファースト戦略」に加え、オンプレミスの SAP Enterprise Central Component（SAP ECC）からクラウドベースの S/4HANA への移行を背景に、従来のオンプレミス ソリューションではなく、クラウドベースのプラットフォームを使用した SAP 製品サービスの開発、提供、強化が優先されている現状があります。
- SAP 環境には、オンプレミス、クラウド、ハイブリッドのアプリケーションに加え、カスタムビルドのアプリケーションやソリューションが多数あり、SAP 環境内外に複雑なデータフローが存在しています。
- SAP のシステムやアプリケーションへの不正アクセスを防ぐには、一元化されたポリシーの適用が欠かせないため、組織は SAP 環境へのアクセスを保護すると共に、S/4HANA への移行やクラウドベースのソリューション導入に伴うリスクを軽減できるソリューションを求めています。

- 企業は SAP アプリケーションを含むすべてのアプリケーションに対してエンド ツー エンドのセキュリティ対策を実施して、アクセスを制御する必要もあります。SAP アイデンティティ管理（SAP IdM）をはじめとして、SAP がこれまで提供してきたアイデンティティ セキュリティ システムのサポート終了が迫る中、組織はビジネスの保護、クラウド移行のサポート、厳格な規制要件やコンプライアンス要件、ポリシー要件への対応を可能にする他のソリューションを検討しています。

SAP 環境における アイデンティティ セキュリティの課題

SAP ユーザーと管理者は、アイデンティティ セキュリティに関して以下のような個別の課題にも直面しています。これらの課題は、複雑な SAP 環境全体のガバナンスやコンプライアンスに影響を与える可能性があります。

- 一元化されたセキュリティ ポリシーの理解と設定
- SAP が提供するオンプレミス、クラウド、ハイブリットの各モジュールとアプリケーション全体における複雑なアクセス権限と制御の管理。ユーザーに対するアクセス権限の設定を誤ると不正アクセスにつながり、重大なセキュリティ リスクが生じる可能性があります。
- 多くの SAP アプリケーションに対するプロビジョニングは手動で行われており、自動化と効率化が必要な状況
- 頻繁に行われる組織変更における、正確なユーザー記録の維持ライフサイクル管理を自動化しない場合、ユーザーのエンタイトルメントを更新するには手間がかかり、エラーが発生しやすい
- 職務分掌（SoD）の実施や、違反の監視、アクセス権限審査（棚卸）など、ガバナンス、リスク、コンプライアンスへの対応。これらの違反を放置すると、社内の不正行為やコンプライアンス違反につながる可能性があります。
- 既存のアイデンティティ ガバナンスのフレームワークに従って SAP システムとの統合を行う場合、シームレスな相互運用性と包括的な監視を実現させるには、専門知識と多くのリソースを必要とすることが少なくありません。
- 「従来型」のアイデンティティ セキュリティ管理者と SAP 管理者間の調整。企業全体のアクセス権限を適切に管理するには、両者が、アイデンティティ セキュリティとゼロトラストの施策に取り組む必要があります。

SailPoint の SAP 向けアイデンティティ セキュリティ：システム最適化に対応したソリューション

SailPoint が提供する企業向けアイデンティティ セキュリティ機能は、ユーザーと業務上不可欠なアプリケーションやリソースへのアクセスの管理、統制を支援します。これにより、アクセス権限の一元管理と制御、一貫したポリシーの適用、脅威の検知、リスクの把握が可能になります。

SailPoint の SAP 向けアイデンティティ セキュリティ機能は、SAP のオンプレミス、クラウド、ハイブリット環境へのセキュアなアクセスを確保すると共にアクセス権限監査を支援します。また、SAP アプリケーション、インフラ、サービス全体のアクセス経路に関する詳細な情報を取得して、職務分掌（SoD）とガバナンス、リスク、コンプライアンス（GRC）のニーズに応えます。

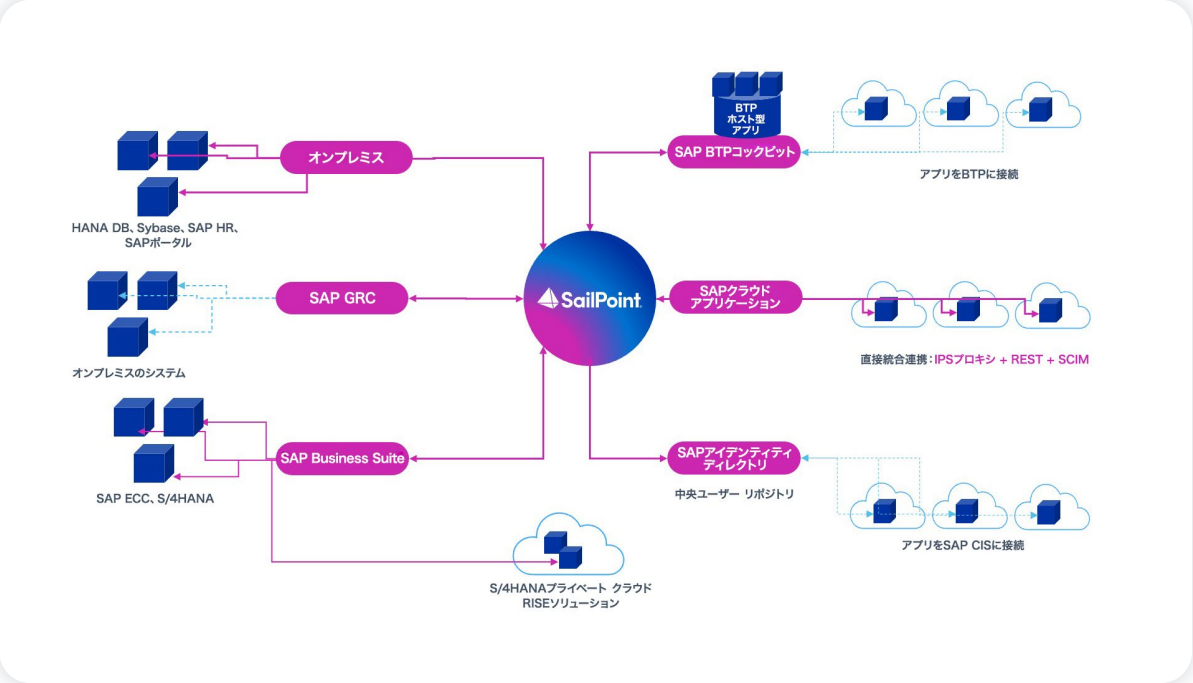


図 1：SailPoint の SAP 向けアイデンティティ セキュリティ

これらのソリューションは、複雑な SAP 環境に対し、ガバナンス、セキュリティ、デジタル トランスフォーメーションなどの課題解決を支援するために設計されています。

- **SAP の最新クラウド インフラ サービスを包括的に適用して迅速な導入を促進：**SAP の最新クラウド インフラに対応する統合機能が含まれており、SAP のリファレンス アーキテクチャに沿って、SAP Business Technology Platform（SAP BTP）や SAP Identity Directory / IdentityAuthentication Service（IAS）などによるユーザー管理の一元化、SAP Cloud Identity Services（CIS）による 40 以上の SAP アプリケーションのプロビジョニングなどが行えます。
- **SAP クラウドのビジネス アプリケーションとサービスへのアクセスの管理と保護機能：**SuccessFactors、SAP HR、Concur、Ariba、Fieldglass など、最も重要な SAP クラウドのビジネス アプリケーションとの統合機能を搭載しているだけでなく、さらに SAP Identity Provisioning Services（SAP IPS）を活用すると、迅速かつ拡張可能な統合を実現でき、ビジネス ニーズに合わせたカスタマイズが可能です。
- **クラウド移行を進めているお客様がアイデンティティ セキュリティの継続性を実現できる統合機能：**オンプレミスの SAP Business Suite アプリケーションと S/4HANA クラウドに対応する包括的なアイデンティティ セキュリティを適用することに加え、SAP RISE に移行する SAP ECC アプリケーションのサポート、職務分掌（SoD）チェックを実行するための SAP GRC および SAP Identity Access Governance（SAP IAG）との統合を実現します。
- **SAP のオンプレミスおよびハイブリット環境をセキュアにサポート：**SAP ECC、S/4HANA、SAP GRC などのオンプレミスの SAP のアプリケーションに対応する高度なガバナンス機能を提供するとともに、SAP のハイブリット環境全体におけるリスク分析、プロビジョニング、アクセス権限審査（棚卸）、職務分掌（SoD）チェックを行うことで、一元化されたアイデンティティ セキュリティとアクセスに対するエンド ツー エンドの透明性を確保します。
- **職務分掌(SoD) に関するニーズを満たすソリューション：**アプリケーション全体に一元化されたセキュリティ ポリシーを適用し、リスク、ポリシー違反、アクセス権限審査（棚卸）をチェックする必要がある企業は、SailPoint の GRC とアクセス リスク管理（ARM）、SAP GRC との統合を実現します。また、SAP GRC と SAP IAG を使用してハイブリッド エコシステム内の SAP アプリケーションに対するプロビジョニングと職務分掌（SoD）分析を行っている場合は、SAP GRC-IAG bridge との統合を実現するなど、複数の選択肢があります。

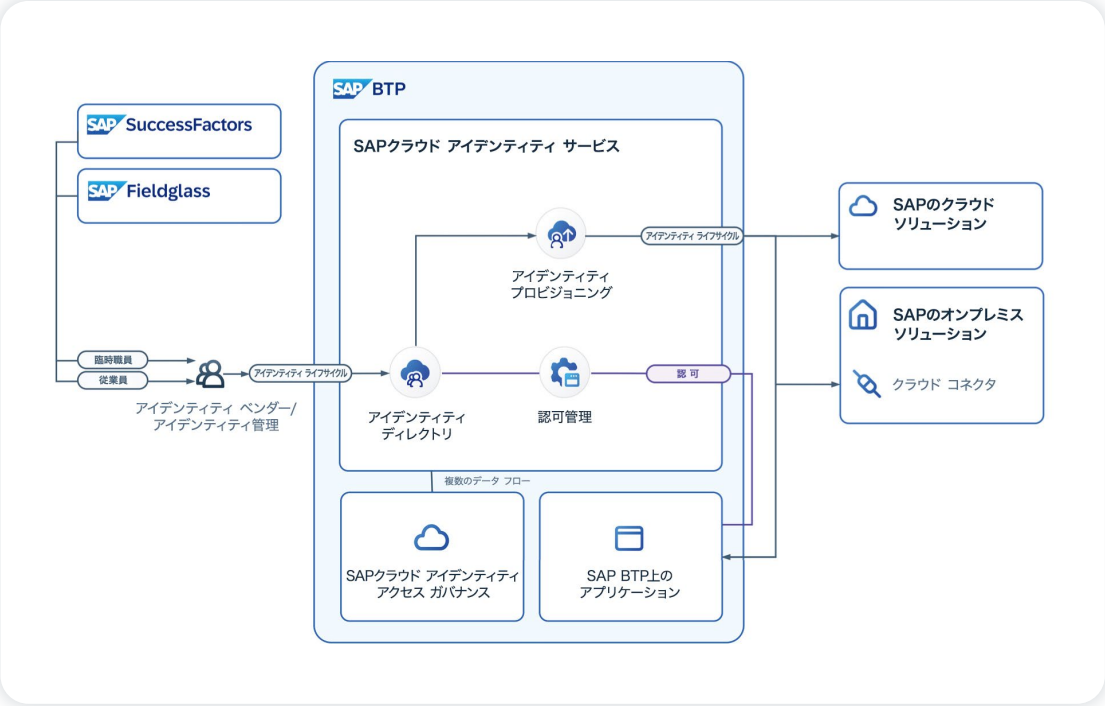
SailPoint の SAP 向けアイデンティティ セキュリティ ソリューションは、デジタル トランスフォーメーションをあらゆる段階でサポートし、SAP のクラウド、オンプレミス、ハイブリットのアプリケーションやサービスへのアクセスを可視化、制御、管理する機能を提供します。またビジネス ニーズに応じて職務分掌(SoD)やアクセス権限審査（棚卸）の機能も実装できます。

クラウドへの移行：
SAP に準拠したシステム最適化ソリューション

SailPoint は、1,100 以上のエンタープライズ アプリケーションと 20,000 以上のカスタム アプリケーションをサポートしています。当社のテクノロジーにより、お客様は主要なアイデンティティ セキュリティ機能と日常的に使用する重要なビジネス アプリケーションを、単一のアイデンティティ セキュリティ プラットフォーム上に拡張、接続、統合できるようになります。これにより、アイデンティティ セキュリティの価値を実感するまでの時間を短縮できます。

SailPoint が SAP と戦略的に技術提携しているのは、このためです。SailPoint の SAP 向けアイデンティティ セキュリティ ソリューションは、業界のベスト プラクティスと SAP の技術要件の両方に準拠しており、重要なアクセスに対するセキュリティを強化したい組織を支援し、クラウド移行における安心感を提供します。

SailPoint が SAP アプリケーション向けアイデンティティ セキュリティに採用しているアプローチは、SAP の戦略的ビジョンをはじめ、リファレンス アーキテクチャ、取り扱い製品、統合連携環境、方法論、ロードマップに準拠しています。たとえば、SailPoint のアプリケーション統合機能は、SAP Identity Provisioning Service（IPS）API を活用しており、最も広く利用されている SAP クラウド アプリケーションにアイデンティティ セキュリティを迅速に拡張できます。



出典：SAP CIO Guide：Identity Lifecycle in SAP Landscapes（P30）

ここで紹介しているアイデンティティ セキュリティの主要な機能には、アクセス権限付与、アクセス承認、ライフサイクル管理、社内の権限審査（棚卸）、インサイトが含まれており、オンプレミスかクラウドかを問わず、SAP の基幹アプリケーションに高度なガバナンスを提供します。また、必要に応じてフレームワークを拡張してお客様固有の要件に対応し、より高度なコンテキストやガバナンスを提供するほか、REST、SCIM、SOAP などの標準的な接続オプションを介した拡張性のサポートも含まれます。

さらに、SAP BTP のサービス群の一つとして提供される SAP CIS との統合、SAP の RISE マネージド サービスとの相互運用性により、SailPoint の企業向けアイデンティティ セキュリティ機能が SAP システムに追加され、SAP のアプリケーションとサービス全体にシームレスなユーザー アクセス権限管理機能を提供すると同時にセキュアなアクセスを確保します。

SailPoint では、SAP GRC および SAP GRC/IAG Bridge との高度な統合機能も提供しています。どちらの統合モジュールも、プロビジョニング リクエストに対するリスク分析機能を提供するだけでなく、論理アクセスと職務分掌（SoD）違反に関する IT ガバナンスの課題を解決してくれます。

また、SailPoint Identity Security Cloud で利用できる、数千種類に及ぶ Connectivity ソリューションでは、Salesforce、Workday、Microsoft Entra などの SAP 以外の基幹アプリケーションへのアクセスを制御でき、アイデンティティ セキュリティの適用範囲を企業全体へとさらに拡大させることが可能です。

SailPoint では、SAP のシステムとアプリケーションに対するスケーラブルな接続性と拡張性に重点を置くことで、企業は競争力とセキュリティを維持し、デジタル トランスフォーメーションの目標を達成し、最新の企業システムの迅速な導入を促進するために必要なコンプライアンス要件、セキュリティ要件、アイデンティティ管理要件への対応を強化できます。

SailPoint

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。