

分散するIDを可視化し、権限情報などの一元管理を実現

SailPoint Identity Security Cloud

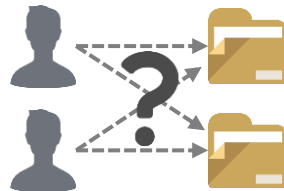
クラウドシフトに伴い、従業員のIDがオンプレミスやクラウドに分散して存在するようになったため、ID管理の負荷が増大しています。煩雑なID管理は内部不正や不正アクセスにつながることもあり、対策が必要です。

SailPoint Identity Security Cloudは、企業が利用しているシステムのIDとアクセス権限を可視化し、一元的に管理。ID管理の負荷軽減とセキュリティ強化を実現します。

このような課題はありませんか？



オンプレミスとクラウドに分散するIDの管理や、非正規社員IDなどの手動管理により、管理者の負担が増大



ユーザーにどのようなアクセス権限を付与しているかの把握が困難



ユーザーに付与していた権限情報をさかのぼって確認できないため、インシデントの原因究明が難航

SailPoint Identity Security Cloudが適切なID・アクセス権管理を支援

- オンプレミス/クラウドのシステムや社員/非正規社員などに関わらず、IDとアクセス権を一元的に管理でき、管理者負担を軽減。
- ユーザーに付与しているアクセス権限を可視化・監視。過剰な権限を用いた不正行為を防ぎ、セキュリティリスクを低減。
- アクセス権の変更履歴を期間の制限なく保存できるため、インシデント発生時の原因究明に有効。

従来のID管理製品との違い

従来のID管理製品	SailPoint Identity Security Cloud
クラウドシステムへの対応が限定的	多くのクラウドシステムに対応可能
権限の棚卸には別途作り込みが必要	権限の棚卸機能が標準装備
人に紐づかないID（マシンID）は手作業での管理	人に紐づかないID（マシンID）も含めて管理可能
管理者への重い負担	ID管理負担を軽減

機能

高度なプロビジョニング

ユーザーの入社や退職、異動などに合わせ、IDの作成、削除、変更を自動化。

アクセス権限をロールで管理

アクセス権限をロールとして管理でき、ユーザーは必要なロールを直接申請可能。

コンプライアンス準拠を支援

過剰な権限の付与など、内部規制・コンプライアンスに違反したユーザーを検知。

職掌の分離

相反する権限の付与を禁止するなど、さまざまな条件のポリシーを設定可能。

アクセス権の変更履歴を可視化

アクセス権限の変更履歴を保存し、過去の付与状況や現在との差分を確認可能。

AIによるロール作成支援

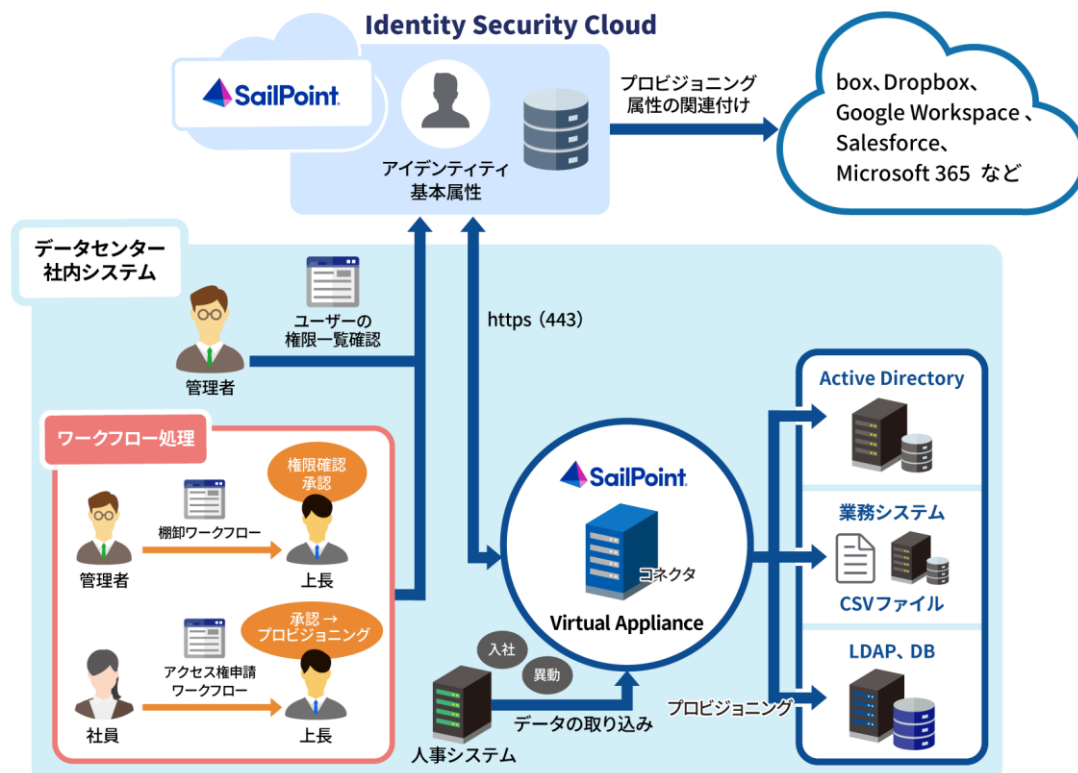
AIがユーザーの役職や権限などを分析し、割り当てるロールの候補を提案。

IDとアクセス権限の可視化

IT部門が未承認のものも含め、利用中のシステムのIDとアクセス権限を可視化。



利用イメージ



※ SailPointは、SailPoint Technologies, Inc.の米国およびその他の国における商標または登録商標です。※本リーフレット中の会社名、商品名は各社の商標、または登録商標です。
※ Google Workspace は、Google LLC の商標です。※ Microsoft (Active Directory 、 Microsoft 365)は、マイクロソフトのグループ企業の、米国およびその他の国における商標または登録商標です。※本文中および図中では、TMマーク、®マークは表記していません。※製品の仕様は、改良のため、予告なく変更する場合があります。※本製品を輸出される場合には、外国為替及び外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認のうえ、必要な手続きをお取りください。なお、ご不明な場合は、当社担当営業にお問い合わせください。※本リーフレット中の情報は、作成時点のものです。

株式会社 日立ソリューションズ

www.hitachi-solutions.co.jp

本リーフレット掲載商品・サービスの詳細情報

<https://www.hitachi-solutions.co.jp/sailpoint/>

