SailPoint

サイバーリスクを回避するには？

アイデンティティ セキュリティの成熟度がレジリエンスを左右する

組織内にアイデンティティの数と種類が増えれば、セキュリティ上の脆弱性が高まるだけでなく、コンプライアンスへの取り組みにより多くの負荷がかかり、サイバー保険料も上昇します。

↑30+%
今後 3 ～ 5 年間における
マシン アイデンティティ
の増加率

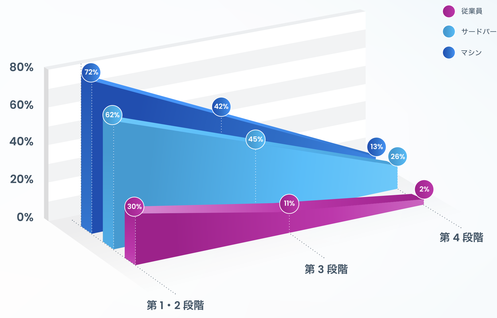
↑14%
今後 3 ～ 5 年間における
デジタル アイデンティティ
の増加率

↑77%
過去 3 年間における
サイバー保険料の上昇率

↑7倍
アイデンティティ
関連規制の強化
（2010 年以降）

アイデンティティ アクセス管理（IAM）およびセキュリティの意思決定者約350名を対象とした最近の調査では、2024年においてもガバナンスが効いていないところからのアクセスが、依然として重大な問題を抱えていることが明らかになりました。

ガバナンスが効いていないところからのアクセス（アイデンティティ種類別）



第 1・2 段階
手作業：基本的なアイデンティティ処理は手作業で管理されており、効率の低下やセキュリティ上の不備につながることが多い。

第 3 段階
デジタル化：アカウントのプロビジョニングを自動化して正確性を向上させ、手作業による作業負荷を軽減。

第 4 段階
高度なツールと予測ユース ケース：人工知能（AI）を活用したソリューションを導入し、インテリジェントな意思決定と先を見越したアイデンティティ管理を実現。

セキュリティ リスクの最大要因はマシン アイデンティティであり、その数は人間の10倍以上の数に及ぶことが多い

セキュリティ リスクやコンプライアンス違反を未然に防ぐには、
専門的なマシン管理が必要です。

66%
マシン アイデンティティの管理には
より多くの手作業が必要 *

60%
マシン アイデンティティに起因した
監査上の問題があった *

72%
休眠状態のマシン アイデンティティを
意図的に保持している *

* マシン アイデンティティの危機：手作業によるプロセスと隠れたリスク

すべてのアイデンティティをセキュアに保護する すべてのアクセス権限を管理する

アイデンティティ アクセス管理（IAM）に戦略的に投資する組織は、アイデンティティ関連のセキュリティ問題とインシデントによる影響範囲を縮小させると同時に、全社的なサイバー レジリエンスの向上を実現しています。

約40%
成熟度が第 4 段階以上の
組織で、AI により
サイバー攻撃の検知と
対応が迅速化

83%
アイデンティティ
セキュリティに
2023 年に投資した結果、
アイデンティティ関連の
セキュリティ問題が減少

40%
サイバー保険会社の
損失が減少
（サイバー リスクの
管理向上を示している）

数字で見るリスク低減の成功事例

3倍
サイバー リスクの低減、約 6,000 の
アカウントに適切な特権を設定することで実現

12,000名
非正規社員のうち
セキュアなアクセス権限を付与された
アイデンティティの数

14万 4,000件
アカウントの変更と検証を自動化することで
低減された潜在的なセキュリティ脅威の件数

300万ドル以上
堅牢なアイデンティティ セキュリティにより
ランサムウェアを未然に防いだことで
阻止できた支払額

現状を把握して、サイバー レジリエンスを向上させましょう。

「アイデンティティ セキュリティ調査レポート 2024-2025」では、そのフレームワークと評価方法について説明しています。成熟した組織によるセキュリティの強化方法、業務の簡素化、コンプラインスの遵守方法をご確認いただけます。

調査結果の詳細はこちら

本書に記載されているすべてデータは、別途記載のない限り、レポート「アイデンティティ セキュリティ調査レポート 2024-2025」からの引用です。

SailPoint

sailpoint.com/ja

IN2634-2504