SailPoint

サイバー攻撃の経済学：サードパーティに起因するリスク

サードパーティのアクセス権限を安全に確保するために、
アイデンティティ ファースト戦略が求められる理由とは

9.5 兆 US ドル
2024 年に予測される
サイバー犯罪関連
コスト[1]

サイバー犯罪を 1 つの
国家と見なすと、
その経済規模は、米国と
中国に次いで第 3 位

主要な違法薬物の
世界中での取引額を
合算した金額よりも、
収益性が高い

63%
非正規社員に付与している
アクセス権限を可視化できていない
企業の割合[2]

54%
非正規社員に不適切な
アクセス権限が付与されていることで
セキュリティの課題に直面している
企業の割合[3]

59%
サードパーティが関与した
情報漏洩を経験した
企業の割合[4]

攻撃チェーンは ここから始まる

下記の方法で、攻撃者に認証情報を盗まれ、アクセス管理が不十分に：
- クレデンシャル スタッフィング攻撃
- キー ロギング マルウェア
- フィッシング
- ソーシャル エンジニアリング

内部の攻撃者

外部の攻撃者

サイバー攻撃により甚大なる被害を被った **41%** の企業が、その攻撃がサードパーティのアクセス権限に起因していたと回答[6]

契約社員

サプライ チェーン パートナー

ベンダー

関連会社

サードパーティの非正規社員を活用する企業は増加している

非正規社員は従業員ではないが、企業の最も重要な資産に対するアクセス権限を有している

97% の企業が、サードパーティの非正規社員にアクセス権限を付与[5]

アプリ | **データ** (001011 110010 010101) | **DevOps** | **IaaS/PaaS** | **オンプレミス** | **SaaS**

特権アカウント

サイバー攻撃者が非正規社員を標的にする理由は、サードパーティのセキュリティ プロトコルにはギャップが存在する、セキュリティ トレーニングのレベルが低い、アクセス権限の制御や監視が厳格でない、など

わずか **13%** の企業のみがサードパーティのセキュリティ リスクを継続的に監視[7]

情報漏洩 | **ランサムウェア** | **ビジネスの中断**

429 万 USドル

サードパーティが関与する情報漏洩の平均コスト[8]

absa

サードパーティのセキュリティ戦略は、広がり続ける企業のネットワークの安全性を確保する上で不可欠になっています。Absa銀行が、SailPointを活用して実現：

12,000 名
安全性が担保されている
アイデンティティを持つ非正規社員

15 日
オンボーディング期間を削減し
迅速なアクセスを実現

300 USドル
非正規社員 1 人の
オンボーディング に関わる削減効果

事例を読む

SailPoint

1. eSentire
2. Imprivata
3. SailPoint
4. RiskRecon
5. SailPoint
6. 世界経済フォーラム
7. Panorays
8. IBM

sailpoint.com/ja

IN2493-2412