# SaaSのセキュリティリスク・設定不備を可視化・検出・修復

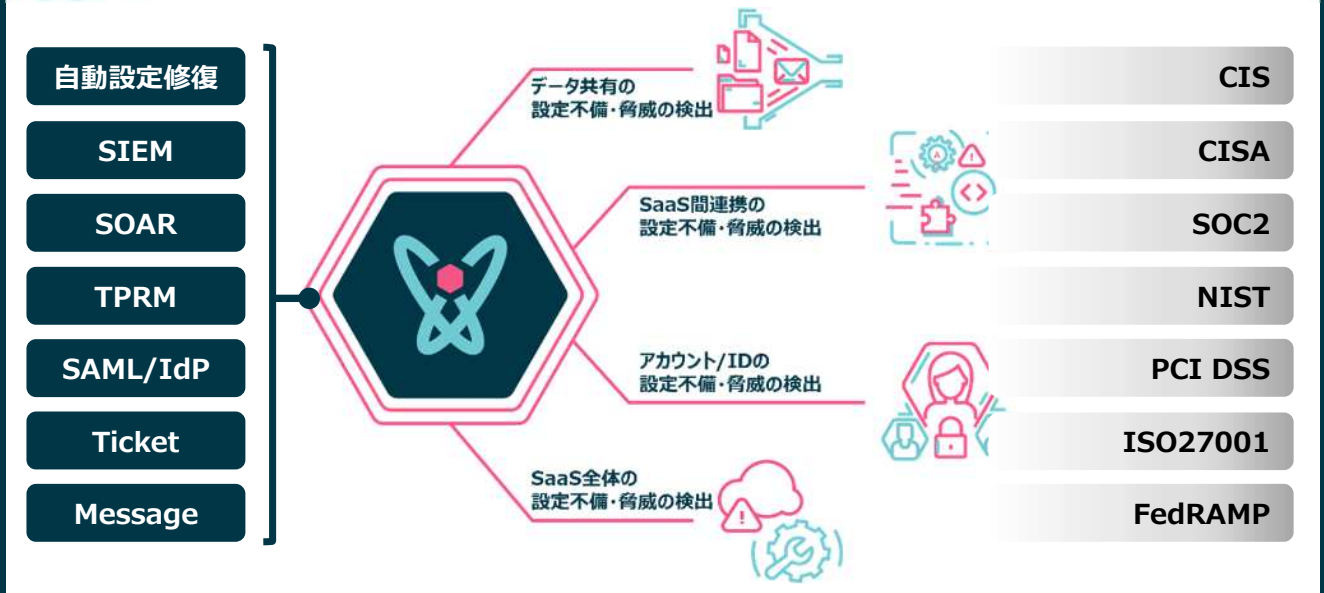
# Valence

## SaaS利活用が普及する中で、こんなお悩みありませんか？

- 多要素認証（MFA）が徹底出来ているか不安
- 意図しないアカウントに管理者権限が付与されている
- 退職者や協力会社向けのアカウントが放置されている
- 誰でもアクセスできる形でファイルをWebに公開し続けている
- SaaSのAPI間連携が無秩序に有効化されている

などなど……

## SaaSの設定ミスによるセキュリティリスクを自動で検出！機密情報の漏えい、サイバー攻撃被害を未然に防ぎます。


東京エレクトロン デバイス

# 代表的なSaaSセキュリティリスクの例

## セキュリティ設定の不備

SaaSアプリケーションは高いカスタマイズ性を備えていますが、その柔軟性ゆえに設定ミスが発生しやすく、情報漏えいのリスクを高める要因となります。

## 脆弱なID管理体制

強固なID管理体制（Identity Posture）を維持することは、アカウントの乗っ取りやトークンの窃取による被害を防ぐうえで極めて重要となります。

## データの過剰共有

ユーザーが外部関係者とファイルやデータを過剰に共有し、URLさえ知っていれば誰でもアクセス可能なリンクを開放したまま放置してしまうケースが多く見られます。

## リスクの高いSaaS間連携

APIやOAuth、サービスアカウントなどのNHI（非人間ID）により、外部サービスや生成AI/AIエージェントが機密データや管理者権限にアクセスできてしまうリスクがあります。

## シャドーSaaSの存在

ユーザーがセキュリティ担当者の許可なく導入したSaaS（特にAI機能を持つもの）は、組織にとって新たなセキュリティ上の脅威となっています。

### セッションの無期限化

Oktaアカウントにセッションタイムアウトが設定されておらず、トークンが無期限に有効な状態となっている。

### コンプライアンスリスク

Microsoft 365の重大度が高いNIST CSFセキュリティチェックのうち、68%がコンプライアンスに非準拠。

### MFA（多要素認証）の未設定

グループウェアのSaaSアカウントで、MFA（多要素認証）またはSSO（シングルサインオン）が適用されていない。

### アカウント削除の不備

OktaやAzure ADからアカウント削除しても、SaaS上でアカウントが削除されておらず、ローカルアカウントが有効なまま残存。

### 個人アカウントへのファイル共有

大量のファイルが個人メールアドレスへ共有されている。また共有されたファイルの94%が使用されていない。

### 意図しない共有設定

機密性/秘匿性の高いファイルがリンクを知っていれば誰でも閲覧可能な状態で外部に共有されてしまっている。

### 使用していないSaaS連携

大量のSaaS間連携がされていることが確認され、そのうち86%が90日以上未使用となっており、ライフサイクル管理の不備が原因。

### 権限リスク

管理者権限を付与されたIDaaS連携が存在しているが、最小権限の原則が適用されていないケースが多数見られる。

### 生成AIの無許可利用

生成AI/AIエージェントの利用規定が定められていない。定められていたとしても、準拠していない生成AI/AIエージェントを利用している。

### サプライチェーンリスク

セキュリティ担当者の承認無く、ユーザーにより無許可で導入されたSaaSアプリケーションが多数確認。

Valenceを活用することで、機密情報の漏えいやセキュリティ侵害のリスクに先手を打ち、SaaSに潜む課題を事前に発見・修復することができます。いま見えていないリスクが、**明日のセキュリティインシデント**を引き起こすかもしれません。
セキュリティ対策の第一歩は、“知らないリスク”をゼロにするところから始めましょう。



東京エレクトロン デバイス株式会社
CN BU
https://cn.teldevice.co.jp/
本社：〒150-6234 東京都渋谷区桜丘町１番１号
渋谷サクラステージ SHIBUYAタワー35階

名古屋：〒451-0045 愛知県名古屋市西区名駅2-27-8
名古屋プライムセントラルタワー8階

大阪:〒530-0001
大阪市北区梅田3-2-123イノゲート大阪 17階