

\ SaaSテナントからの情報漏洩を防止 /

# SSPMサービス AppOmni

SSPM : SaaS Security Posture Management

SaaSの使い方を誤ることで、さまざまな情報漏洩事件が起こっています

Microsoft 365の  
パスワードポリシーの設定が  
弱く、不正ログイン

Salesforceの仕様変更  
に気づかず、ゲストユーザーから  
情報アクセス可能に

GitHubから開発ソースや  
システムの認証IDが流出

**! 取引先情報や顧客情報が流出!**

AppOmniがお客さまの**SaaSテナントが安全か常時監視します!**

セキュリティ設定不備

過剰なアクセス権限

不要な3rdパーティ  
サービスからのアクセス許可

不要なアカウントの放置

## AppOmni **4**つの強み



### きめ細かく診断

各SaaSの機能に応じた専門の診断項目で  
きめ細かく診断します。また、検出したリスクに対  
し、対策方法などについても具体的にアドバイス。  
診断内容のカスタマイズも可能です。



### 疑わしいアクセスも検知

ログ解析により、お客さまのSaaS環境がブル  
ートフォース攻撃や匿名ネットワークからの不審な  
アクセスを受けていないかを監視できます。  
アクセスのブロックや対策強化に役立ちます。



### SaaSの仕様変更 に自動追従

エキスパート機能が刻々と変化するSaaSの  
仕様やセキュリティ設定に合わせて、セキュリ  
ティの弱点を監視します。運用者は監視  
ルール  
の調整を気にせず運用できます。



### 簡単導入・運用

エージェントレスで簡単に導入でき、サービ  
スが用意するベストプラクティスのセキュリ  
ティポリシー  
ですぐに診断・監視を始められます。開発プラ  
ットフォームで独自のSaaSも統合監視  
できます。

# AppOmniでできること

セキュリティ対策不備の監視  
(セキュリティ設定・権限・アカウント管理など)

コンプライアンス基準での評価

レポート

セキュリティ設定・アクセス権限・  
接続サービスなどのビュー

疑わしいアクセスの検知

ポリシーのカスタマイズ

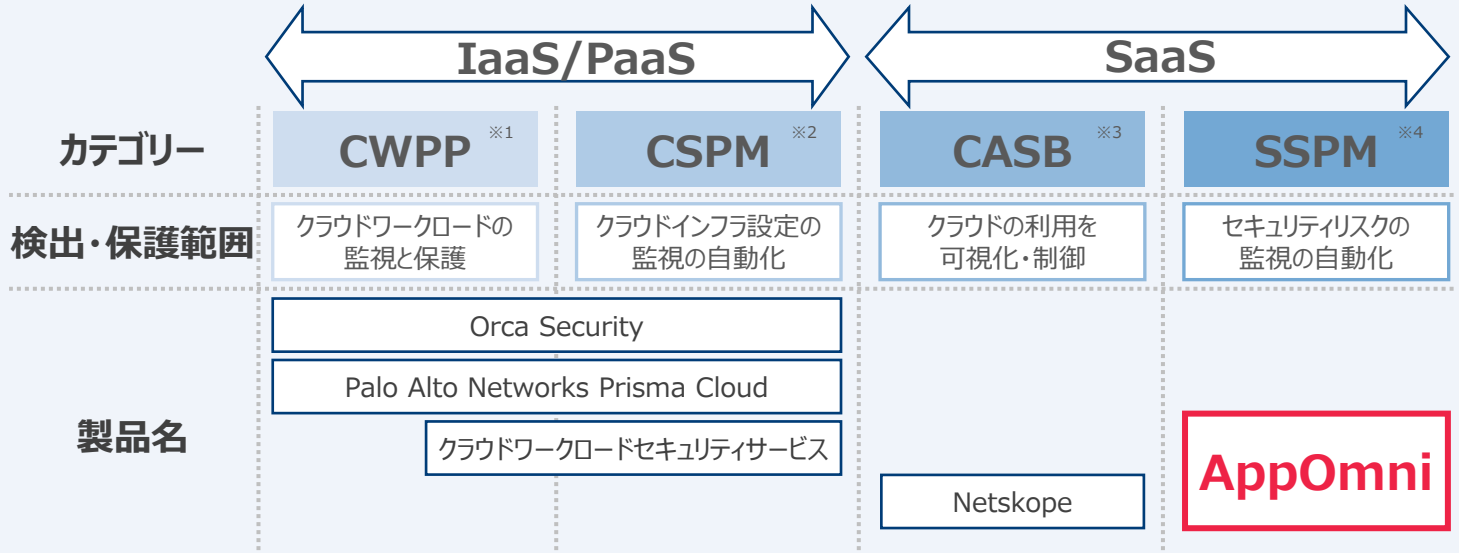
## 多数のSaaSに対応！順次拡大中

- Google Workspace
- Microsoft 365
- Salesforce
- ServiceNow
- Jira Software
- Microsoft Intune
- Box
- monday.com
- Okta
- Microsoft OneDrive
- GitHub
- Tableau
- Zoom
- Zendesk
- Microsoft Teams
- Slack
- Auth0
- Workday
- ...and more

2024年2月時点  
対応SaaS **38**種類

## CSPM/CWPPと組み合わせて クラウドのセキュリティを万全に

日立ソリューションズではさまざまな脅威に対応する多彩なソリューションをご提供しています。



※1 Cloud Workload Protection Platform : クラウドワークロード保護プラットフォーム

※2 Cloud Security Posture Management : クラウドセキュリティポスチャ管理

※3 Cloud Access Security Broker : クラウドアクセスセキュリティブローカー

※4 SaaS Security Posture Management : サーズセキュリティポスチャ管理

※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。 ※本文中および図中では、TMマーク、®マークは表記しておりません。 ※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上、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  
www.hitachi-solutions.co.jp/appomni/

