

## クラウド セキュリティ監視サービス

高度な分析と優れた脅威インテリジェンスを組み合わせた常時監視により、お使いのクラウドおよびハイブリッドのIT環境の業務負荷を軽減

Secureworks のクラウドセキュリティ監視サービスは、社内に追加の専門の担当者を用意することなく、コスト削減と対応スピードの高速化を実現し、クラウドの防御態勢を強化します。Secureworks のカウンター・スレット・プラットフォーム (Counter Threat Platform™: CTP) を活用し、Secureworks の専門家がお客様のクラウド上のデータを 24 時間 365 日常時監視し、相関分析を行います。また誤検知を除去し、本当に脅威となり得るセキュリティイベントを特定して、修復を支援します。

### クラウドでの脅威を可視化

大切なデータやアプリケーションをクラウドへ移行するということは攻撃者からの防御の必要性が増すということでもあります。この移行段階でクラウドセキュリティの対策が不十分だと、コンプライアンスへの不適合や脆弱性の危険にさらされることになりかねません。

しかし、正しいプロセスとテクノロジーを用いて適切な人材が適切に監視すれば、クラウド環境には脅威状況の可視化を強化するための様々な新しいデータ・ソースが提供されています。問題は 24 時間 365 日常時大量のログ・データを解析するプロセスやプラットフォームに従事するクラウドセキュリティの専門家を探し出し、確保することです。また、これは複雑な業務であるため、特に高度な分析や脅威インテリジェンスを持ち合わせていなければ、セキュリティ上の欠陥が残る可能性があります。

### Secureworksが解決します

Secureworks は、企業組織が安心してクラウドへと移行できるよう、恒常的な可視性を提供します。リアルタイムでの監視と可視化を行うことで、ユーザーが注意すべきセキュリティイベントに狙いが定められ、侵害やデータ流出が発生する前に実際の脅威に対して迅速に対応することができます。

Secureworks のクラウドセキュリティ監視サービスは Secureworks のカウンター・スレット・プラットフォーム™(Counter Threat Platform : CTP) を活用し、Secureworks お客様ポータルにより使いやすいレポートを提供しています。これは監査の簡素化や、生産性の向上にも役立ちます。Secureworks のサービスは、ログ監視にかかる運用、維持の負担を軽減する支援をします。これにより、お客様は優先度の高い本来のビジネスに集中することが可能となり、また、場所や時間にとられない生産的なツールを採用することによる組織的なリスクの低減も実現します。

### お客様のメリット

- 継続的な監視によりクラウドへの侵害リスクを低減
- 誤検知を減らし、それにかかる時間や工数の削減
- ログの監視にかかるコスト高のクラウド環境のコンプライアンス・ギャップを解消
- 社内の人員などのリソースを本来のビジネスの戦略的業務に注力

### サービスの特長

- 24 時間 365 日、クラウド内のアプリケーション、デバイス及びサーバーを監視
- Secureworks のカウンター・スレット・プラットフォームを活用し、高度な分析とイベントの相関分析を実施
- カウンター・スレット・ユニット (Counter Threat Unit™ : CTU™) による優れた脅威インテリジェンス
- 早期のエスカレーションと通知
- クラウド型とオンプレミス型の脅威情報を一元管理
- 使いやすいレポート機能でコンプライアンス遵守の簡素化

## アマゾン ウェブ サービス (AWS) のための クラウドセキュリティ監視

Secureworks は、AWS のアドバンスドテクノロジー パートナーであり、業界をリードするセキュリティ・サービスのプロバイダーとしてお客様の AWS 環境をおびやかす脅威を 24 時間 365 日常時監視しています。カウンター・スレット・プラットフォームを活用し、様々な AWS のログの出力元やサービス（例えば CloudTrail、VPC フローログ、論理デバイスなど）からデータを収集、分析し、お客様の環境のスケールアップ/ダウンに関わらず、セキュリティで保護されている状態を維持できるよう努めています。高度な脅威の検知については、Secureworks が提供する “エンドポイントの高度な脅威検知 :AETD Red Cloak” サービスが有効です。

## AWS 上のファイアウォールを監視

昨今の常時接続、モバイル、クラウドファーストといった環境において、仮想ファイアウォールはデータトラフィックの安全を守るための主要なセキュリティ対策です。ですが、これらのファイアウォールはかなりの量のログ・データの生成も行います。疑わしいデータを調査、評価するスタッフや専門知識を持たない企業組織であっても、Secureworks がお客様の代わりに監視、脅威の相関性分析を行い、またその専門知識を提供することが可能です。

## Secureworks について

グローバルのサイバーセキュリティ・サービス業界をリードする Secureworks® (NASDAQ: SCWX) は、デジタル化が進む社会において、企業組織をサイバーの脅威から保護し続けています。

当社は、数千社におよぶお客様から集積したデータと人工知能（AI）、そして独自のカウンター・スレット・プラットフォーム (Counter Threat Platform™ : CTP) の自動化による可視性と、お客様の環境を保護する強固なネットワーク効果を創出する当社の卓越したリサーチとアナリスト集団から提供される実践的な分析結果を統合してサービスに反映させます。

データの種別や出所を問わず集積・分析を行うことで、セキュリティ侵害の防御、悪意ある活動のリアルタイムによる検知、深刻化する脅威の迅速な対応と予見を実現し、サイバーの脅威への対抗策をお客様に提供します。

もっと上手に組み合わせれば、セキュリティは飛躍できる™

Amazon Web Services は、Amazon.com, Inc. の米国およびその他の国における商標です。Microsoft Office365® Azure、Exchange Online、SharePoint Online、Azure Active Directory は、Microsoft Corporation の米国およびその他の国における登録商標または商標です。

## Microsoft Azure のための クラウドセキュリティ監視

Azure Active Directory、Azure Activity、Azure Security Center アラートなどからのセキュリティログを 24時間x365日常時監視し、相関分析や、高度な分析を提供します。

また、Azure 上の ファイアウォールや、WAF デバイスの監視も実施します。

高度な脅威の検知については、Secureworks が提供する “エンドポイントの高度な脅威検知 :AETD Red Cloak” サービスが有効です。

## Office 365 のための クラウドセキュリティ監視

Secureworks は、お客様が安心して Office 365® に移行できるよう、24 時間 365 日常時、脅威状況の可視性を提供します。

強固なデータ・ログシステム、監視、レポート機能により、Exchange Online や SharePoint Online、Azure Active Directory など主要サービスへの侵害や不正アクセスをお客様にアラートします。Secureworks は、お客様が適切にデータを管理し、実際に被害が発生する前に不正なユーザーや脅威活動の検知できるよう支援します。

## 対応クラウド



## パートナーシップ

Microsoft  
Partner

aws partner  
network  
Advanced  
Technology  
Partner



より詳細な内容に関しては、下記のメールアドレスにご連絡ください。

[SCWX\\_PreSales@secureworks.com](mailto:SCWX_PreSales@secureworks.com)

代表 03-6893-2317

[secureworks.jp](http://secureworks.jp)

SecureWorks Japan 株式会社