AWS、Azure
などに対応

パブリッククラウド環境に潜むリスクを早期に発見

3ステップで導入可能な新しい手法とは?

IaaS/PaaS上で業務システムを稼働する企業が増える中、設定やセキュリティ対策の不備に起因するリスクが新たな課題になっている。こうした状況に対して日立ソリューションズが提案するのが、「Orca Security」だ。CSPM（Cloud Security Posture Management）の進化形ともいうべきこのサービスは、独自技術にもとづくリスクの可視化・管理により、安全・安心なIaaS/PaaS環境の実現を強力に支援する。

クラウドの設定不備がセキュリティリスクの温床に

デジタルトランスフォーメーション（DX）を推進するため、多くの企業が既存のIT資産を最新技術に対応させるITモダナイゼーションに取り組んでいる。その中でも重要課題の1つとなるのが、システムのクラウド化だ。オンプレミスで稼働してきたさまざまな業務システムをIaaS/PaaS環境へ移行し、運用コストの削減、柔軟性向上を図る。また、新規システムの構築に際してはクラウドファーストを徹底し、ビジネススピードを加速するといった取り組みだ。

一方、ここで切実な問題として浮上してきているのが情報セキュリティである。

株式会社日立ソリューションズ
クロスインダストリソリューション事業部
セキュリティソリューション本部
セキュリティプロダクト第1部 担当部長
河浦 直人氏

「既存システムの移行と新規システムの構築、どちらのケースでもリスクの温床となっているのが、クラウド環境の設定不備です。スピーディーなクラウド化をめざすあまり、ユーザーごとのアクセス権限やセキュリティ対策などを適切に設定・管理しないまま活用をスタートしてしまっているのです」と日立ソリューションズの河浦 直人氏は指摘する。

また、仮にこの点に気付いていたとしても課題はある。クラウド環境の確実な設定、および維持・管理を行うには相応の工数とコストが必要で、対策は容易でないからだ。

例えばセキュリティ対策では、マルウェア対策、脆弱性対策、不正アクセス対策など、目的に応じた複数のツールを、インフラ、OS、アプリケーションといったクラウドの各レイヤーに適用しなければならない。もちろん、対策実施による業務への影響を極小化するには、事前の綿密な調査も不可欠だ。既存のオンプレミスのシステムに実施してきたのと同様の工数・コストが、クラウドでも新たに発生することになる。

「また、最近は『Amazon Web Services（AWS）』や『Microsoft Azure（Azure）』『Google Cloud Platform（GCP）』などのクラウドサービスを目的ごとに使い分けるマルチクラウドでの活用も増えています。そうなると、クラウドごとにツールを導入する必要性が生じるほか、そのための知識とスキルを備えた人員も不可欠です。企業の負荷は大きく高まってしまうでしょう」と河浦氏は言う。

4つのレイヤーをまたぐ可視化と管理を可能にする

そこで、これらの課題を解決するサービスとして日立ソリューションズが提案するのが、「Orca Security」だ（図1）。

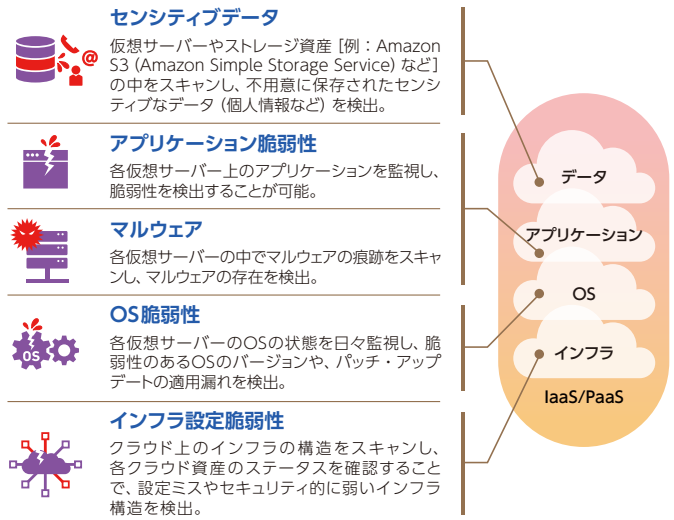
これは、イスラエルのスタートアップ企業、オルカセキュリティ（Orca Security, Inc.）が提供するCSPM（Cloud Security Posture Management）サービス。CSPMとは、IaaS/PaaS環境におけるポリシー設定、ネットワークの設定などを可視化し、継続的にチェックすることで、セキュリティリスクや不具合の存在、異常発生などの速やかな検知を支援するものである。

「そもそもオルカセキュリティは、イスラエル軍でサイバー攻撃関連の諜報活動を担う組織のメンバーが創業した企業です。知識や技術力は折り紙付きであり、グローバルで多くのユーザー企業を抱えています。このオルカセキュリティと日立ソリューションズのノウハウを融合することで、IaaS/PaaS環境の可視化にもとづく効率的なセキュリティ対策の実施をご支援します」と河浦氏は説明する。

Orca Securityの特長は大きく3つだ。

1つ目が「トータルな可視化・管理機能を提供できること」。一般には目的ごとに個別のツールやソリューションが必要になるインフラ、OS、アプリケーション、データという4つのレイヤー

図1　Orca Securityが検出するセキュリティリスクの例



インフラからOS、アプリケーション、データまでの4つのレイヤーを網羅したトータルなセキュリティ管理を実現する

株式会社日立ソリューションズ
クロスインダストリソリューション事業部
セキュリティソリューション本部
セキュリティプロダクト第1部 主任
山口 拓人氏

の可視化・管理を、単一のサービスで実行できる。「AWS、Azure、GCPというメジャーなパブリッククラウドサービスに対応しています。お客様のマルチクラウド環境において、統合的かつ詳細な可視化・管理が実現できます」と日立ソリューションズの山口 拓人氏は述べる。

可視化できる情報も多岐にわたる。例えばインフラレイヤーでは、設定の問題などを検出可能。OSレイヤーでは各仮想サーバーのOSを管理し、パッチ適用漏れによる脆弱性を検出したり、OSのサポート切れを指摘したりできる。また、仮想サーバー内のマルウェアも検知することが可能だ。

アプリケーションレイヤーでは、クロスサイトスクリプティング（XSS）やSQLインジェクションといったサイバー攻撃につながるような脆弱性を把握できる。データレイヤーでは、機密データが不適切な形で扱われていないかどうかを可視化。また、仮想サーバー上に存在する個人情報やID・パスワード情報なども検出できるという。

「レイヤー横断型の可視化・管理が行えるため、組織内部に侵入した脅威がネットワーク経由で複数の仮想サーバーを水平移動するラテラルムーブメントによる侵害範囲拡大につながるようなセキュリティリスクも検出できます。また、コンテナやサーバーレスといった最新のインフラ技術に対応している上、リスクの内容に応じて攻撃ルートを図示するなど分かりやすく表示します。これらは、Orca Securityならではの強みといえるでしょう」と河浦氏は強調する。要因や危険度レベルごとに分かりやすく表示された結果をもとに、運用負荷削減を図りつつ、迅速な対応を進めることができるだろう。

独自技術によりシステム環境に影響を与えない管理を実現

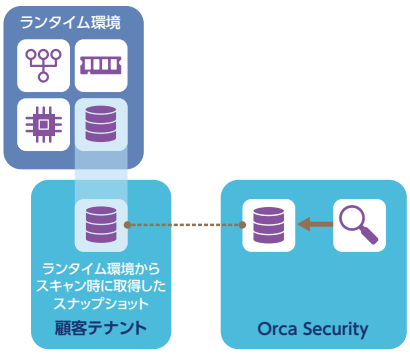
2つ目は「エージェントレス」である。対象となる顧客環境にエージェントをインストールする必要がない。これを可能にしているのが、オルカセキュリティの独自技術「SideScanning」だ（図2）。

「チェック対象のクラウド環境全体のスナップショットを、対象のクラウド環境が存在するリージョンの一時領域に取得し、取得したスナップショットをスキャンすることで、稼働中のお客様環境、およびお客様の業務に影響を及ぼすことなく可視化・管理が行えるのです」（山口氏）

これにより、CSPMサービス利用時やマルウェアスキャンの課題になりがちなユーザー環境のCPUパワー消費、I/Oの発生による処理遅延などは起こらない。セキュリティチェックのための追加リソースも不要だ。対象のクラウドアカウントを指定するだけで、その環境のセキュリティチェックを継続的に実施することができるという。

なお、実は1つ目の特長で紹介したトータルな可視化・管理も、

図2　オルカセキュリティの独自技術「SideScanning」



スナップショットを取得し、それをスキャンすることで顧客環境に影響を及ぼすことなく可視化・管理を実現する

このSideScanning技術によって支えられている。顧客システム全体のスナップショットをスキャンすることで、レイヤー横断的な可視化・管理を可能にしている。

3つのステップによる数分程度の作業で導入が完了

3つ目の特長が「導入の容易さ」である。わずか3ステップの操作で利用を開始できる。AWS環境への導入を例に紹介しよう。

まず、①Orca Securityのダッシュボード上で、AWSアカウントにログインする。②ダッシュボード上で「クラウドフォーメーションテンプレート」を開き、所定の情報を入力。「クラウドフォーメーションテンプレート」により、Orca Securityからの読み込み権限設定、およびユーザーのAWS環境とOrca Securityを接続するための情報を生成する。そして、③生成された情報をフォームに入力し、ボタンをクリック。これだけで、設定作業は完了となり、AWS環境のセキュリティチェックをすぐに開始できる。

「操作は多少異なりますが、AzureやGCPでも同じく3ステップで利用開始できます。数分程度の簡単な作業で使い始めることができるでしょう」と山口氏は言う。

加えて日立ソリューションズは、導入時の事前コンサルティングや運用支援などのサービスを幅広く提供する。高度な知見を備えたホワイトハッカー人材が、Orca Securityで確認したアラートに対し、具体的な対策方針の立案や支援などを行うことで、顧客のIaaS/PaaS環境のセキュリティ対策の実施を支援するという。

「オルカセキュリティが実施した調査※によると、パブリッククラウド上でシステムを運用する企業の約8割が、外部公開サーバーのうち少なくとも1つはパッチ未適用やサポート切れのOSを利用しており、外部公開サーバーの約4割が内部環境に侵入されるラテラルムーブメントのリスクを自社クラウド内に抱えています。内部環境にある仮想環境は、77%の組織のうち10%以上のワークロードでパッチ未適用やサポート切れのOSを利用している状況であったため、外部から侵入を許すと機密情報にアクセスされるリスクを抱えています。リスクは他人事ではありません。自社のクラウド環境の可視化と管理に今すぐ取り組むことをお勧めします」と山口氏は最後に語った。

※Orca Security 2020 State of Public Cloud Security Report