Orca Security

｜導入事例｜ 株式会社日立ソリューションズ

日立ソリューションズ

所在地	東京都品川区東品川四丁目12番7号
設立	1970年9月21日
従業員数	4,914名（2022年9月末現在）
事業内容	ソフトウェアサービス事業、 情報処理機器販売事業
URL	https://www.hitachi-solutions.co.jp/

クラウド環境のセキュリティレベルを高めつつ インテリジェントな仕組みでリスク管理の負荷を軽減

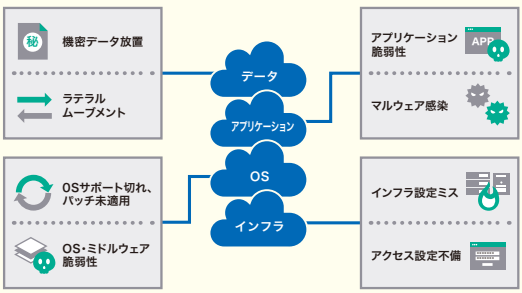
システムインテグレーション企業の日立ソリューションズは、クラウドシフトが加速する現状に対し、よりインテリジェントにパブリッククラウド環境のセキュリティリスクを検出できる仕組みを求めて「Orca Security」を導入。セキュリティの統制部門と各システム管理者の双方にとって運用負荷の少ない方法で、セキュリティ対策の強化を実現しています。

課題	導入後
めまぐるしく変化する脅威に対し、手作業による セキュリティチェック・対応は限界がある	パブリッククラウド環境のセキュリティリスクを 継続的かつ広範囲に自動で検出するため、運用負荷を軽減
大量のアラートの情報精査に追われ、 対策の優先度を判断しにくい	アラートをトリアージして、対応優先度とともに 可視化することで効率的な対策を支援
診断ツールの導入にあたっては、 稼働システムへの影響が懸念される	エージェントレスのため、 稼働システムを止めずに導入が可能

SOLUTION

パブリッククラウド環境におけるセキュリティ対策を効率化

- パブリッククラウド環境のセキュリティリスクを幅広く自動検出し、一元管理を実現
- エージェントレスのため既存環境を変更することなく、15分程度の権限設定で利用を開始
- インフラの設定ミスから機密データの検知、ラテラルムーブメント対策まで対応
- サーバーレス環境やコンテナ環境を含め1つの製品で対応し、運用コストを削減



既存環境に影響なく、4つのレイヤーにまたがって セキュリティリスクを幅広く自動で検出

株式会社 日立ソリューションズ

| 導入事例 |

株式会社日立ソリューションズ INTERVIEW

グループ協創推進本部　情報セキュリティ・リスク統括センタ

セキュリティアナリスト
佐藤 広志

技師
下倉 正幸

背景 クラウドシフトに伴う脅威への対応に課題

日立グループのデジタル事業をけん引する中核企業として、さまざまな分野で人々の社会生活や企業活動を支えてきた日立ソリューションズ。「未知の扉をひらく。ゆるぎないチカラとともに。」を経営ビジョンに掲げ、確かな技術力で自社製品・サービスを開発するとともに、米国にも拠点を設置し、世界中の最先端デジタル技術を積極的に採り入れています。

クラウドシフトが急速に進展する昨今、当社においてもAWSやAzureなどのパブリッククラウド環境を利用したシステムの開発・リリースが増え、クラウドセキュリティの重要性はますます高まっています。日立ソリューションズグループ全体の情報セキュリティの統制とリスク対策をミッションとする当社の情報セキュリティ・リスク統括センタの担当者は、次のように語ります。

「クラウド環境は、オンプレミス環境とは異なる観点でのセキュリティ対策が必要です。しかし、めまぐるしく変化する脅威に対し、各システムの管理者が人手でセキュリティリスクをチェックし対応することは大きな負担となります。また、日々の運用の中で発生する誤検知対応や、大量のアラート情報精査・必要な対応の優先度付けといった作業も負荷が高く、セキュリティ対策に精通した技術者を擁する当社であっても、多忙な業務とセキュリティ管理の両立には限界があると感じていました。我々統制部門からの一方通行ではなく、各システム管理者との協力体制のもとでセキュリティ対策をより強固に進めていくには、さらなるセキュリティレベルの向上を図ると同時に各システム管理者の負荷を軽減できる施策が不可欠だと考えました」（佐藤）

取り組み 最小限の手間でリスクを可視化する仕組みを検討

パブリッククラウド環境のセキュリティリスクへの対応に向けて、的確かつ効率よく監視・運用できる仕組みの確立が急務として、新しい製品の導入検討へと踏み出した当社。クラウドシフトに伴い見えないセキュリティリスクが増大しつつあることは、各システムの管理者も日々の運用を通じて十分に認識しており、新しい仕組みの導入に抵抗感を示す声はありませんでした。

製品の選定を進めるにあたっては、各システム管理者との協力体制を築くための要件として、導入が容易であることに加え、統制部門とシステム管理者の双方の運用工数を最小化できること、開発・本番環境への影響を最小限に抑えられることを重視。セキュリティ製品を扱う部門やシステム管理者の協力を得て評価を進めた結果、要件を満たす製品として選定されたのが、パブリッククラウド環境のセキュリティリスク管理を支援する「Orca Security」でした。エージェントレスでありながら機能が豊富であること、サーバーレス環境やコンテナ環境を含め1つの製品で対応できることなども決め手となりました。

効果 緊急度の高い真に重要なアラートへの対応に集中

「Orca Security」は、検出した問題を一般的な高・中・低でリスク分類するのではなく、関連するすべてのクラウドリソースの性質やつながりを加味した緊急度に応じて、アラートを通知します。本稼働に向けて2022年3月から20システムで試行を開始する中で、改めて認識された同製品の優位性は次のとおりです。

「『Orca Security』はよくできており、必要なタイミングで的確にセキュリティインテリジェンスを提供してくれます。当初は検出されたアラートのすべてをシステム管理者に通知する計画でしたが、製品の信頼性の高さから、絶対に見逃してはならない緊急度の高い問題のみを通知し、それ以外は『Orca Security』の画面上で適宜確認してもらうことにしました。これにより通知件数が顕著に減り、システム管理者の負荷は大きく軽減されており、対応にかかる時間は80%ほど削減できています。アラートや誤検知に追われて点検が形骸化する心配もなく、軽減された作業時間を本来の業務に注力できるようになりました」（佐藤）

システム管理者側の反応も予想以上に好感触だったとのことです。

「インシデントにつながる前段階でリスクを確実に検出してくれる『Orca Security』に十分な手応えを感じているようです。クラウド上のシステムで構成変更が行われた際、顕在化するリスクがある場合には速やかに通知されます。また、『Orca Security』の画面上でもシステム構成情報が視覚的に分かりやすく表示されるので、検出内容についてシステム管理者側とのコミュニケーションも取りやすくなり、より迅速に対策が行えるようになりました。我々統制部門にとっても、『Orca Security』の画面上でシステム構成と検出内容との因果関係を容易に把握できるようになり、多くの気づきが得られています」（下倉）

人手のみでは追い切れないパブリッククラウド上のセキュリティリスクが可視化され、使うごとに蓄積されていくナレッジにも期待を寄せています。

展望 全社導入で大幅なコスト削減効果に期待

一部のシステムで本稼働がスタートした当社では、引き続き全社規模での導入をめざす計画です。各稼働システムに影響を与えることなく1システム当たり15分程度で導入できる容易さも、全社展開を大きく後押しすることになりそうです。また、すべての導入が完了すれば、全社規模で「Orca Security」が担う領域が増え、大幅な業務負荷の軽減とコスト削減につながることは間違いありません。

なにより、「自ら実践することで蓄積されたナレッジをもとに、お客様にはリアリティのある、よりよい提案ができると考えています」と佐藤が語るように、システムインテグレーション企業の日立ソリューションズとして、「Orca Security」で手にしたアドバンテージをお客様のビジネスに還元していく考えです。

本事例のwebページはこちら
www.hitachi-solutions.co.jp/cspm/case01/

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/cspm/

J22S-06-00　2023.03