SOPHOS

CUSTOMER CASE STUDY **日鉄ソリューションズ株式会社**

あらゆる企業にデジタルイノベーションが求められる時代にあって、“鉄のDNA”を継承し、自ら考え行動できる人材を育成している日鉄ソリューションズは、ITで顧客企業の幅広い課題を解決してきた。同社の流通・サービスソリューション事業本部アドバンストテクノロジー部では、開発環境として需要が増大するパブリッククラウドのセキュリティ対策を強化するために、ソフォスのCloud Optixを採用した。

CUSTOMER-AT-A-GLANCE

NS Solutions

日鉄ソリューションズ株式会社
東京都港区虎ノ門一丁目17番1号
虎ノ門ヒルズビジネスタワー

社員数
6,639名（連結）[2020年3月期]

Webサイト
https://www.nssol.nipponsteel.com/

ソフォスソリューションズ
Sophos Cloud Optix

パブリッククラウドでは、セキュリティが低いまま、安易に開発環境を構築してしまう危険があります。そして、運用規模が大きくなると、チェックする項目や対象が多岐にわたるので、管理しきれなくなります。

日鉄ソリューションズ
流通・サービスソリューション事業本部　アドバンストテクノロジー部
プロフェッショナル　外崎　則夫氏

日鉄ソリューションズの流通・サービスソリューション事業本部では、流通小売業の業務高度化に向けた各種ソリューションや、AIにIoX※やRFIDさらには5Gなどの最新技術を活用した最新テクノロジーを提供している。同事業本部では、ECサイトの構築から販売物流系システム構築に、流通業界向けの基幹システムや販売分析など、多岐にわたる最先端のITソリューションを提供している。同事業本部のアドバンストテクノロジー部では、ITソリューションを開発する事業部の開発者に対して、横断的な活動を推進している。その活動の一環として、パブリッククラウドを開発者が安全に利用できるように、ソフォスのCloud Optixを採用し、利用状況のスマートな可視化やアラート機能により、安全で的確な運用・監視を実現した。

※IoXとは、「IoT:モノのインターネット」に「IoH:ヒトのインターネット」を加えた日鉄ソリューションズの考え方「Internet of X」に由来する日鉄ソリューションズの登録商標です。

ビジネスチャレンジ

「パブリッククラウドに潜むセキュリティリスクを重視」

日鉄ソリューションズの流通・サービスソリューション事業本部　アドバンストテクノロジー部が、パブリッククラウドの利用におけるセキュリティ対策の強化に取り組んできた背景について、プロフェッショナルの外崎則夫氏は次のように切り出す。

「数年前から、社内でも開発環境にAWSやAzureなどのパブリッククラウドを利用する

CloudOptixではネットワークのトラフィックレベルで、外部回線からのアクセスをリアルタイムでチェックできます。また、監視対象のデータが可視化されているので、問題を容易に発見できるようになりました。

日鉄ソリューションズ
流通・サービスソリューション事業本部　アドバンストテクノロジー部
エキスパート　伊藤　春氏

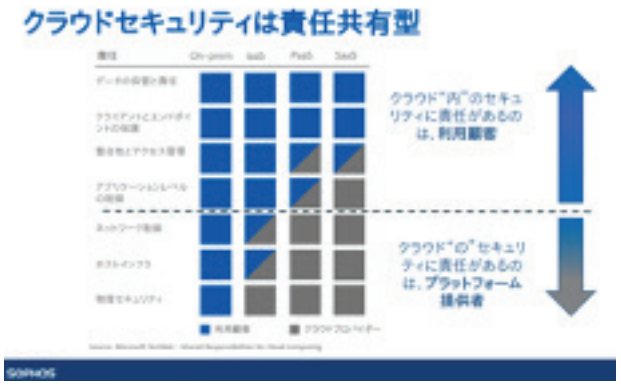
ケースが増えてきました。パブリッククラウドでは、新規のハードウェア導入やネットワーク施設などが不要なので、手軽に開発に着手できます。その一方で、セキュリティに対する意識がないままに、安易に開発環境を構築してしまう危険もあります。例えば、デフォルトのパスワードを変更しないで利用してしまうとか、通信のセキュリティを考慮していないと、攻撃される危険性が高くなります。そこで、当部門ではパブリッククラウド開発環境に対するセキュリティのルールを独自に設けて、外部からの侵入や攻撃を防ぐ取り組みを強化してきました」

パブリッククラウドを開発基盤に採用し、サービスの提供を推進する企業が増えている。その一方で、パブリッククラウドに潜む脆弱性を狙った攻撃や被害も増えている。海外では、侵入されたパブリッククラウドが、仮想通貨のマイニングに悪用される被害も起きている。

同事業本部では、早くからパブリッククラウドのセキュリティリスクに備えるために、簡易的な監視ツールを利用してきた。しかし、この監視ツールにはいくつかの課題があった。外崎氏は「従来使用していた監視ツールは、利用するパブリッククラウドの規模が小さいときには、問題なく運用ができました。しかし、パブリッククラウドを開発環境として使用するプロジェクトが増え、運用規模が大きくなると、チェックする項目や対象が多岐にわたるので、管理しきれなくなりました」と説明する。

パブリッククラウドでのセキュリティ対策では、データの保管やクライアントとエンドポイントの保護など、利用者の責任となっているチェック項目は多い。SaaSやPasSの一部では、アプリケーションレベルの制御やアクセス管理などは、サービス事業者も責任の一端を担う。だが、IaaSのような開発環境で

は、利用者の責任範囲は広くなる。こうした多岐に渡るセキュリティ対策を簡易の監視ツールで的確にチェックするのは難しい。簡易ツールでは、設定したルールに従ってメールを通知するだけなので、構成が複雑化した場合には対象の特定や修正すべきポイントの洗い出しが煩雑になってしまい、運用が難しくなってしまう。こうした背景から、同事業本部では本格的なパブリッククラウドの監視ツールの導入を検討した。



テクノロジーソリューション

「大規模な運用にも対応できるスマートな可視化やアラート機能を評価」

アドバンストテクノロジー部のエキスパート伊藤春氏は、パブリッククラウドの監視ツールとしてCloud Optixを選定し導入した経緯について、次のように振り返る。

「大規模なパブリッククラウドの運用にも対応できる監視ツールを探しているときに、Cloud Optixを紹介してもらいました。そこで、約1ヶ月かけて機能を検証しました。検証にあたっては、AWSなどの脆弱性対策として利用できるか、Cloud Optixの可視性やインシデント対応の性能を確認しました。例えば、AWSのセキュリティグループに対して、正しくポリシーをかけているかどうか、指定したリソースに対して問題が発生したときに適格に通知されるかなど、実際の運用を想定した機能を検証しました」

パブリッククラウドのセキュリティ対策では、すべてのエンドポイントのデータを厳重に管理する必要がある。その重要性について伊藤氏は「例えば、Cloud Optixではネットワークのトラフィックレベルで、外部回線からのアクセスをほぼリアルタイムでチェックできます。セキュリティホールを発見する上で、トラフィックレベルでのチェック機能は重要です。また、監視対象のデータが可視化されているので、問題を容易に発見できるようになりました」と指摘する。

同部では、Cloud Optixの直感的でわかりやすいダッシュボードをはじめとして、スマートな可視性や継続的なコンプライアンスのチェック機能、限られた管理者でも大規模な運用を監視できるAIを活用したアラート対応などの性能を総合的に評価して、採用を決めた。

導入した結果

「危機の予兆を事前に検知でき開発者のセキュリティ意識も向上」

Cloud Optixの運用を担当している小野晋也氏は、導入の成果について次のように評価する。

「実運用がスタートしてから、我々の部署では10以上の環境を管理しています。運用してみて便利だと感じているのは、管理者としての使いやすさです。直感的でわかりやすい

ダッシュボードが表示されるので、状況の確認が容易になりました。また、アラートが発生するタイミングが速いので、対応も迅速になりました。さらに、継続的な監視とアラートによりパブリッククラウドを利用している開発者のセキュリティ意識も向上したと感じています」

Cloud Optixの導入により、流通・サービスソリューション事業本部の開発チームは、パブリッククラウドでの開発におけるセキュリティリスクの可視化を実現し、迅速な検知とアラートにより、安全な運用体制を確立した。

今後の展望

「新機能がこれまでだと月1回くらいのペースでリリースされているので、今後の性能向上にも期待」

Cloud Optixを活用しているエキスパートの栗栖直士氏は、今後の取組について次のように計画している。

「まずは、パブリッククラウドに対するセキュリティ意識を社内で高めていく必要があります。その意味では、Cloud Optixの利用は効果が期待できると思います。また、社内の開発チームだけではなく、社外についてもCloud Optixの利用を推奨できるケースがあるだろうと考えています」

導入から数ヶ月が経過して、日々の運用に取り組んでいる小野氏は「Cloud Optixの導入当初は、アラートを受信できるアプリが限定されていたのですが、しばらくしてメールによる受信が可能になりました。我々がほしいと思う機能が、毎月のようにリリースされるので、今後も便利な機能や性能の向上に期待しています」と話す。

SOPHOS

日鉄ソリューションズ
流通・サービスソリューション事業本部
アドバンストテクノロジー部
エキスパート　栗栖　直士氏

日鉄ソリューションズ
流通・サービスソリューション事業本部
アドバンストテクノロジー部
小野　晋也氏