お客様事例 › 顧客接点の高度化

SCSK

KubernetesをベースにしたプラットフォームにSysdig Secureを導入 セキュリティの可視化によりシステムの安定と利用者の安心を実現

株式会社インターネットイニシアティブ（IIJ）様

専門家以外でも使える操作性に優れたGUIと プリセット済みの豊富なルールが魅力

事例のポイント

IIJ様の課題

- Kubernetesを用いたサービス共通プラットフォームのセキュリティを強化したい
- FalcoやOSS版Sysdigではルールづくりなどの手間がかかる上、高度で専門的な知識も必要
- 専門知識のない事業部の担当者にもツールから得られるセキュリティ情報を役立ててほしい

課題解決の成果

- セキュリティが可視化されたことで安定したシステムが実現し、利用者の安心感にもつながる
- あらかじめ豊富なルールが用意されているため、手間をかけずに導入できた
- 操作性に優れたGUIにより、専門知識のない事業部の担当者でもセキュリティ情報の活用が可能に

導入ソリューション Sysdig Secure

「IIJ Kubernetes Engine(IKE)にSysdig Secureを導入したことで、テナント側とクラスタ側との間で責任分界点を明確化した上で、インシデントに対処することが可能になりました」

ネットワーク本部 SRE推進部長　田口 景介 氏

背景・課題

KubernetesをベースにしたプラットフォームのSRE利用に際してセキュリティの強化が課題に

日本におけるインターネットの黎明期より、サービスプロバイダとしてさまざまなサービスを提供してきたインターネットイニシアティブ（以下 IIJ）。同社は設立以来の基本方針である「高い品質と信頼性」を、クラウド上のインフラにおいても実現するため、2018年からSRE（Site Reliability Engineering）推進部が中心となって、サービス共通プラットフォームの構築に取り組んでいる。

その取り組みの中で生まれたIKE（IIJ Kubernetes Engine）という名前のこのプラットフォームは、いま話題のコンテナ管理技術であるKubernetesを用いており、社内システムの運用環境や各事業部門が提供するサービスの共通基盤となることが期待されている。プロジェクトをリードするSRE推進部長 田口景介氏はKubernetesを採用した理由について「今日では多くの企業がクラウドを活用していますが、パブリッククラウドごとにインターフェースが異なるため、クラウド事業者の変更や使い分けが困難です。その点、サーバー側においてOSのような役割を果たすKubernetesは、ベアメタルサーバー上やさまざまなパブリッククラウド上で、まったく同じパッケージが動かせるのが大きな魅力です」と語る。つまり、KubernetesをIKEのベースにすることで、インフラの種類を問わず同一パッケージによるアプリケーションのデプロイや、環境に依存しない同一オペレーションによる運用が可能になり、リリース速度やスケーラビリティ、サービス品質が向

お客様プロフィール

IIJ Internet Initiative Japan

株式会社インターネットイニシアティブ

所 在 地：東京都千代田区富士見2-10-2 飯田橋グラン・ブルーム

U R L：https://www.iij.ad.jp/

1992年、国内初のインターネット接続事業者として設立される。以来、日本におけるインターネット企業のパイオニアとして、技術面を中心にイニシアティブをとり続けてきた。現在は、インターネット接続事業で培った高い技術力をベースに、クラウドをはじめとするアウトソーシングサービスやWANサービス、システムインテグレーションなどのトータルソリューションプロバイダとして事業領域を拡大し、ネットワークに関する顧客のあらゆる要望へワンストップで応える企業グループとして成長を続けている。

株式会社インターネットイニシアティブ
ネットワーク本部
SRE推進部長
田口 景介 氏

株式会社インターネットイニシアティブ
ネットワーク本部 SRE推進部
シニアエンジニア
牧野 泰光 氏

株式会社インターネットイニシアティブ（IIJ）様

上するとともに、システムリソースのコスト削減が期待できるというわけだ。

しかし、IKEの構築時にはひとつ大きな課題があった。セキュリティである。IIJでは、Kubernetesを利用するために各種ドライバやトラフィックマネージャ、さらにはアプリケーションやアカウントを管理するためのポータル／モニタリングツールなどを自社で開発したり、OSSのコンポーネントを組み込んだりしていた。それにより、本番運用に向けてセキュリティを強化する必要があったが、利用できるコンポーネントがなかったのである。そこでSRE推進室は、2021年春ごろからセキュリティ対策の導入に向けて本格的な検討を開始した。

左からSCSK 姜（きょう）、SCSK 川杉、IIJ 田口 氏、IIJ 牧野 氏、SCSK 石川、SCSK 奥

解決策と効果

採用の決め手は操作性に優れたGUIと豊富なルール SCSKの高度で専門的な製品知識と 日本語サポートも評価

Kubernetesのセキュリティコンポーネントとしては、Falcoがよく知られている。しかし、Falcoを活用する際にはルールづくりなどの手間がかかるだけでなく、高度で専門的な製品知識も求められる。

「SRE推進部のメンバーは皆Kubernetesの専門家ですが、セキュリティに必ずしも精通している、というわけではありませんし、メンバーの数に限りがある中で、Falcoだけに貴重な人的リソースを割くわけにもいきません」（田口氏）

そこでSRE推進部が注目したのが統合型エンタプライズセキュリティ「Sysdig Secure」だった。Sysdig社がFalcoやOSS版Sysdigの開発元であることに加え、SCSKが2019年11月から商用版の国内総販売代理店となったことから、日本語による手厚いサポートが期待できる点に注目したのである。

「かねてよりSCSKはブログなどを通じてSysdig Secureの情報を積極的に発信しており、製品に対する十分な知識を持っていると考えました」（田口氏）

2021年4月、SRE推進部はSysdig Secureの採用を決断、6月から利用をスタートした。実際の導入・構築にあたったSRE推進部 シニアエンジニアの牧野泰光氏は、採用のポイントについて「ひとつはFalcoやOSS版Sysdigと異なり、操作性に優れたGUIを備えており、専門家以外の担当者でも使いやすいこと。もうひとつが、脆弱性や不正アクセスなどを検出するためのルールが豊富にプリセットされており、ゼロからルールを作る必要がなかったことです」と振り返り、田口氏も「Kubernetesのメリットを最大限に生かし、付加価値を高めるには、いわゆるマルチテナントが望ましいと考えていて、IKEもその前提で構築しています。ここにSysdig Secureを導入したことで、テナント側とクラスタ側との間で責任分界点を明確化した上で、インシデントに対処することが可能になりました」とその意義を強調する。

また、2021年12月、Javaベースのロギングユーティリティ「Apache Log4J」に深刻な脆弱性が発見されるということがあったが、このとき大きな手応えを感じたと導入の効果について話す。

「脆弱性が公表されたのが金曜日だったため、週末に攻撃を受けてしまった事業者が多かったようですが、当社はSysdig Secureのルールを追加することで迅速に対処できました。結果的に不正なアクセスはなかったのですが、インシデントが発生していないことを確認できたのは安心感につながりました」（田口氏）

さらに、SCSKの提供するサポートは期待以上のもので、導入前に実施されたハンズオンや勉強会に加え、導入後も最新の情報が逐次提供されている。メンバーの知識習得やスキル向上に大いに役立っているということだ。

今後の展望

Sysdig Secureのさらなる活用を検討 IKEの利用拡大に合わせ、 SCSKのきめ細かいサポートを期待

今後、IIJがサービス共通プラットフォームとしてIKEの活用を進めていく中、Sysdig Secureによるセキュリティの可視化は、システムの安定性はもちろん、利用者の安心感にもつながることだろう。同社では、システムのデプロイ前にはクラスタのスキャンや、SaaSとの連携などの機能も活用していくことを検討している。

そして、現時点では25ノードで稼働しているIKEだが、近日中に50ノードまで増やし、将来的には100ノード以上に拡大していく方針だ。

「IKEの利用が広がっていくことで、今後さらに多くのサーバーが置き換わっていくことでしょう。これに伴い事業部の担当者に使ってもらうケースも増えると思いますので、SCSKには機能制限などよりきめ細かい対応を期待しています」（牧野氏）

プラットフォーム事業グループ
ITエンジニアリング事業本部
ミドルウェアソリューション部
川杉 喜彦

SCSK担当者からの声

IIJ様のIKE（IIJ Kubernetes Engine）のようなクラウドネイティブなプラットフォームは、従来の境界型防御だけではセキュリティの確保が難しいため、ワークロードにフォーカスしたセキュリティ対策が非常に重要です。Sysdig Secureはワークロードを監視し、マルウェア攻撃などによる怪しい振る舞いを可視化します。稼働中のアプリケーション環境がセキュアであることを証明するためにはワークロードセキュリティ対策が必須です。SCSKでは今後もIIJ様とともにSysdigを利用したセキュリティ対策の取り組みを推進し、アプリケーションにとって安心安全な環境の実現に貢献してまいります。

SCSK株式会社

● ソリューションの詳細情報・お問い合わせ先

PickUpソリューション　顧客接点の高度化
「Sysdig Secure」

▶URL：www.scsk.jp/pickup/contactpoint/index.html
▶URL：https://www.scsk.jp/sp/sysdig/

● 本件に関するお問い合わせ先

▶Mail：sysdig-sales@scsk.jp

（2022年4月 初版）