お客様事例 > 顧客接点の高度化

SCSK

フリマアプリ「メルカリ」を支えるKubernetesクラスタにおいて Sysdig Secure DevOps Platformが強固なセキュリティを確立

株式会社メルカリ 様

さまざまなセキュリティレベルのマイクロサービスが同一のクラスタ上で同居する環境の監視を実現

事例のポイント

お客様（メルカリ様）の課題

- 一般論としてKubernetesはSecure by defaultではなく仕様上、セキュリティのリスクを考慮して使う必要のあるプロダクト
- マイクロサービス化で開発者の操作を想定したセキュリティ対策も必要に

課題解決の成果

- Kubernetesへの不正侵入の監視と操作ログ保存が実現した
- 不正侵入に備えた不審なアクティビティの監視が可能に
- 全操作ログが簡単に残せるようになり、トラブルの際も後から確認できる

導入ソリューション　Sysdig Secure DevOps Platform

「不審なアクティビティがあった際には通知が来るので、迅速な対応が可能です。また、開発者の操作ログの記録が容易になったことが安心感につながっています」

Security Engineeringチーム 末澤 裕希 氏

お客様プロフィール

mercari

株式会社メルカリ

所 在 地：東京都港区六本木6-10-1
U R L：https://www.mercari.com/jp/

2013年2月設立。同社のビジネスの主軸を担うフリマアプリ「メルカリ」は、月間利用者数が1,755万人と、フリマアプリとしては日本でも最大規模であり、年間流通総額は6,259億円を超える。2014年9月からは米国でもサービスをスタート。また、2019年2月には子会社のメルペイが、非接触型決済サービス「メルペイ」の提供を開始。事業の多角化に乗り出している。

株式会社メルカリ
Security Engineeringチーム
末澤 裕希 氏

背景・課題

「メルカリ」の機密情報を守る上でKubernetesクラスタのモニタリングとログ管理が課題に

「新たな価値を生みだす世界的なマーケットプレイスを創る」をミッションに、2013年2月に設立されたメルカリ。同社が運営するフリマアプリ「メルカリ」は、同種サービスの代表格といえる存在にまで成長している。2019年2月には、子会社であるメルペイが非接触型決済サービス「メルペイ」の提供を開始。これらのサービスの展開を通じ、限りある資源を循環させ、より豊かな社会をつくることを目指している。

もともとメルカリでは、サービスプラットフォームをモノリシックなアーキテクチャで構成していた。しかしながら、サービス数が増え、大人数が同時並行で開発を進めるようになると、さらなる生産性の向上が課題になってきた。そこで2017年末、同社はメルカリのマイクロサービス化を決断。クラウド基盤にGoogle Cloud Platform（GCP）、コンテナ管理ツールにGoogle Kubernetes Engine（GKE）を採用し、順次マイクロサービスアーキテクチャに移行した。

その中、マイクロサービス化により開発組織のあり方も変わり、バックエンドエンジニアが、開発から運用まで責任を持つようになった。その結果、開発者がインフラを触る可能性を前提とした新たなセキュリティ対策が必要になった。Kubernetesクラスタ上では、複数のマイクロサービスが稼働する。それゆえ、各マイクロサービスが影響を及ぼす範囲を最小限にする必要がある。

メルカリでは、一般的に現状のKubernetesは、Secure by defaultなプロダクトとは言えず、そもそもコンテナ間でカーネルを共有するという性質上、セキュリ

株式会社メルカリ 様

ティのリスクをよく考慮して使う必要のあるプロダクトと考えていた。メルカリでは対策を行っているものの、たとえばデフォルト環境のままKubernetesを使ってしまうと、容易に権限昇格が出来るなどの問題がある。この点についてSecurity Engineeringチームの末澤裕希氏は「私たちが防ぎたい攻撃は、外部からの脆弱性を突いた攻撃や重要端末の盗難などによるコンテナへの不正侵入です。ノードに権限昇格されると、他コンテナ上のクレデンシャルの取得が可能になります」と語る。

メルカリにおける膨大な量の取引情報を扱っている同社において、機密情報の保護は最優先の課題だ。そこで同社はKubernetesのセキュリティ対策として、独自の侵入テストや、クラスタの堅牢化など、さまざまな取り組みを実施してきた。その中でさらなるセキュリティ強化の手段として浮上してきたのが、モニタリングと操作ログの記録だった。

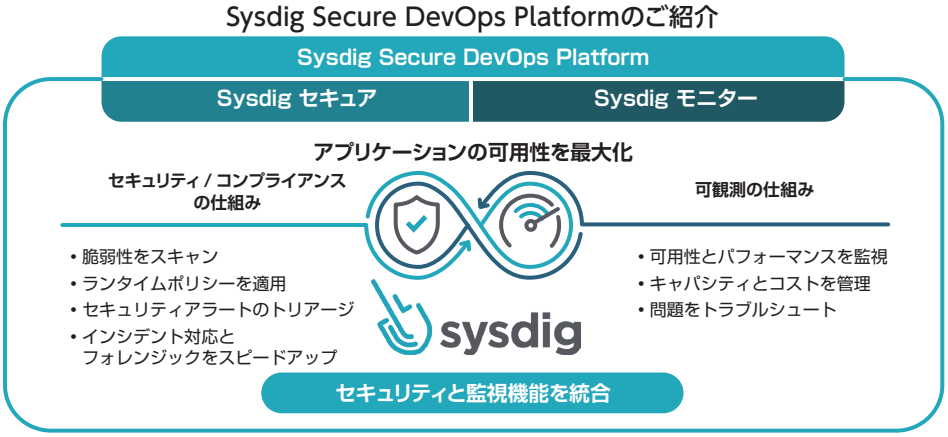
「モニタリングすることでインフラとアプリケーションに対する不正侵入を即時検知して対応すること、Kubernetes上の操作ログを取得し記録できることがリスクの緩和のために必要だと考え、新たな対策を検討することにしました」（末澤氏）

解決策と効果

不正検知能力が高く、運用管理の負担も少ない「Sysdig Secure DevOps Platform」を採用 不正侵入の監視が実現

メルカリでは、3つの観点からコンテナ管理専用のセキュリティ対策を検討。3製品に対してPoCを実施し、「不正検知能力」「記録能力」「運用管理」の3つの項目で点数化した。その中で、総合点数が最も高かったコンテナ・Kubernetes環境向けセキュリティ・モニタリング プラットフォーム「Sysdig Secure DevOps Platform（以下、Sysdig）」の採用を決めた。

「メルカリではPoCにあたり、把握しているKubernetesへの攻撃を全て試しました。たとえば脆弱なコンテナの作成や、Kubernetesを操作するためのCredential盗難などのシナリオなどを含みます。その中でSysdigはPoCにおいて「不正検知能力」の成績がトップでした。また、安定したSaaS版が提供されていることも大きかったですね。Sysdigはクラウドネイティブな環境に適したかたちで提供されており、Kubernetes上にエージェントをデプロイするだけで導入できます。自社での運用も不要で、コンソールから容易に管理可能です」（末澤氏）



このほか、Sysdig社が主に開発しているオープンソースのKubernetes監視ツールである「Falco」がKubernetesコミュニティに深く関わりながら改善を続けていることも評価したと言う。また、Sysdig自体は有償ツールだが、様々な周辺ツールはオープンソースで開発されており、メルカリからの依頼をすぐに反映したり、メルカリからの貢献を取り込んだりというプロセスがあったことも高く評価された。

今回の選定やPoCの実施にあたっては、国内総販売代理店のSCSKがサポートにあたった。比較した3製品はいずれも海外のツールだったが、Sysdigのみがコンテナセキュリティについての深い議論が可能だったことや、SCSKがSysdig本社とのパイプを通して、新たな機能追加の要望を伝えることができることもポイントになった。

「セキュリティのプロダクトは日本では利用ユーザに対する対応が代理店のみに限定されてしまうものもあります。Sysdigについては、SCSKとSysdigの日本法人の2社から共同で対応していただき、製品に対する理解が深まりました。当社の開発チームが普段から利用している『Slack』を使い、スピーディなやり取りができたのも有り難かったですね」（末澤氏）

Sysdigの導入は、約1カ月で完了した。本作業は社内のKubernetesを管理しているチームが行ったが、パフォーマンスへ与える影響を考慮し、段階的にKubernetesクラスタに対して、Sysdigのエージェントのデプロイを行っていった。その際、大きなパフォーマンス影響は確認できなかったという。

同社はSysdigを導入したことで、不正侵入の監視が実現し、Kubernetesクラスタのセキュリティレベルを大幅に高めることができた。

「不正侵入があった際にはすぐに通知が来るので、迅速な対応が可能です。たとえば、先ごろLinuxの新しい脆弱性（CVE-2020-14386）が発見された際には、セキュリティチームで攻撃手法を解析し、即座にSysdigによる防御を実施することができました。また、開発者の操作ログが分かりやすく残るため、トラブルが起きた際に簡単に確認が可能になったことが安心感につながっています」（末澤氏）

今後の展望

パフォーマンスや可用性を監視する Sysdig Monitorの導入も予定

「Googleは、Secure by defaultかつ、コンテナ間の分離を高めたコンテナオーケストレーションを実現するために、gVisorというコンテナランタイムを作っています。gVisorを使うと、不正侵入を受けたあとの権限昇格などは防げる場面も大きくなりますが、それでも不正侵入自体の監視の必要性は残り続けると思っています。ネットワーク等一部の監視などが今のSysdigの仕組みでは難しくなるかもしれない認識をしていますが、こうした取り組みを追った上で、新しい仕組みに可能な限り追従していただけたらと思います」（末澤氏）

同社とSCSK、Sysdigの3社は、今後も密に連携しながらセキュリティ課題の解決に取り組んでいく。

ITエンジニアリング事業本部
ミドルウェア第二部 第一課
石川 愛彦

SCSK担当者からの声

「Sysdig Secure DevOps Platform」は、クラウド・ネイティブなシステムを下支えする基盤であり、かつ、コンテナ・セキュリティの起点であるとも考えています。メルカリ様への本製品導入支援を通じて、コンテナ・セキュリティに対する必要性が着実に高まっている状況を目のあたりにし、他の多くの企業様にもこのプラットフォームの価値を感じていただきたいと思っております。SCSKは、今後もSysdigソリューションの提供を通じて、お客様サービスにおけるコンテナやKubernetes活用への取り組みを、最大限支援してまいります。

SCSK株式会社

● ソリューションの詳細情報や問い合わせ先はこちら

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

▶URL：https://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

（2020年11月 初版）