顧客事例


# ゴールドマン・サックス：マイクロサービス化でビジネスを加速

## 概要：

ゴールドマン・サックスにとって、ソフトウェア革新のスピードは非常に重要です。それは、企業としての競争力を持ち続けるには、有益なインサイトを顧客に提供するためのソフトウェアアプリケーションが彼らの有能なチームに必要だからです。ゴールドマン・サックスのエンジニアリング部門は、世界経済が変化する中で顧客へのアドバイスに必要なツールを最前線で同社のプロフェッショナルに提供しています。

このことを念頭に、ゴールドマン・サックスはDevOpsの原則とマイクロサービスを採用し、オンプレミスとクラウド環境においてコンテナ化されたアプリケーションを大規模に配信しています。そして、ゴールドマン・サックスはソフトウェア配信を加速し、2週間に1回のビルドから1日あたり1,000回以上までに開発スピードの高速化に成功しました。マイクロサービスの採用にあたり、ゴールドマン・サックスはSysdigからホストとコンテナのモニタリングとセキュリティ・ソリューションを採用し、同社の成長が促進されました。

## 課題：

ゴールドマン・サックスでは、スピードが重要な目標である一方で、コンプライアンスとセキュリティにも妥協は許されません。規制が厳しい業界に属する同社は、コンテナ化されたアプリケーションとデータを確実に監視する方法を求められています。さらに、ソフトウェアでビジネスを展開しているため、パフォーマンスと可用性は基本中の基本です。

## 効果：

Sysdigは、ゴールドマン・サックスのクラウドチームがマイクロサービスを大規模に監視する上で重要な役割を担っています。Sysdigを使用することで、ゴールドマン・サックスは以下を実現しました。

- 業務上重要なサービスのパフォーマンスと可用性の最適化
- インシデントレスポンスとトラブルシューティングの迅速化

ゴールドマン・サックスは、クラウドネイティブテクノロジーにより、DevOpsチームの効率を大幅に向上させることができました。コンテナを使用することで、ソフトウェア開発の加速、事業継続の自動化、インフラ管理の簡素化が実現したのです。同時に、セキュリティとコンプライアンスプロセスも効果が出るよう変更しなければなりませんでした。ゴールドマン・サックスは、可視性を確保できる適切なツールが事業運営に必要でした。

「クラウドプロバイダーとオンプレミスでのデータセンターにまたがる変化の激しい環境での、セキュリティ、モニタリング、トラブルシューティングは、今までにない新しい次元の業務になりました」と、ゴールドマン・サックスのエンジニアリング担当バイスプレジデント、Chetan Mehendiratta氏は説明します。

「私たちの環境で稼働しているサービスを最適化し、安全性を確保する事が私たちの使命です。例えば、通信パターンやクラスタの使用状況を把握し、不正な動作やセキュリティイベントを特定し、アプリケーションの使用率が低いか高いかを知る必要があるのです。これらの目標の達成には、詳細なテレメトリーに加え、アプリケーションのコンテキストが必要となり、解決するのが難しい問題です。」

ゴールドマン・サックスは2016年後半にSysdigと契約し、同社独自の一連の要件に適合するかどうかを判断するために、厳格な技術評価に着手しました。ゴールドマン・サックスは、セキュリティとコンプライアンスを同社のDevOpsワークフローに統合しながら、必要な可視性を実現するSysdigを見つけました。ゴールドマン・サックスはSysdigを活用することで、監視、トラブルシューティング、スキャン、コンプライアンス、脅威の検出、監査など数多くのユースケースに、大規模に対応できるようになりました。

**ゴールドマン・サックスはSysdigを使用することで、監視、トラブルシューティング、スキャン、コンプライアンス、脅威の検出、監査など数多くのユースケースに、大規模に対応できるようになりました。**

ゴールドマン・サックスは、Sysdigを導入し、大規模な環境の監視とセキュリティ確保を行い、9,000人以上の開発者をサポートしています。

## アプリケーションの大規模なモニタリング

ゴールドマン・サックスのモニタリングチームは、変化が激しく大規模なマルチクラウド環境において、ホスト、コンテナ、オーケストレーターの自動検出と監視にSysdigを使用しています。同チームは、オンプレミスとパブリッククラウドにまたがるアプリケーションとコンテナを容易に特定することができます。収集されたテレメトリーは、アプリケーション、インフラストラクチャー、プロセスレベルのアクティビティにまたがり、毎秒数百万のコンテナをポーリングするという前例のないスケールで行われます。

ゴールドマン・サックスは、豊富なデータを活用して、特定のアプリケーションに属するコンテナとプロセスを特定し、どのサービスが他のサービスと通信しているかを詳細に示す、カスタムサービス接続マップを構築することができます。さらに、これらのマップは、スタック全体の問題の特定とトラブルシューティングに役立つ、きめ細かいアクティビティデータで強化されています。

## クラウド上の不正な接続とトップトーカーを特定

監視チームはSysdigを使用して、エンティティ、データセンター、地域、クラウド間の何百万ものネットワーク接続を追跡し、ネットワーク使用量をコンテナに割り当てています。どのプロセスとコンテナがトップトーカーであるかを把握することで、ゴールドマン・サックスはより効率的に作業を進めることができます。

- 最も多くのネットワークデータを使用しているアプリケーションを分離
- セキュリティ侵害を示す不正な接続を識別
- コンテナ・プロセスとネットワークの使用状況を関連付けて、より良いキャパシティ・プランニングを実現
- トラブルシューティングの実行による可用性の最大化

## クラウドネイティブ環境におけるMITRE ATT&CKの検知機能

Sysdig Secureを使用することで、ゴールドマン・サックスはセキュリティ検出ポリシーを利用して、プロセス、ファイル、ネットワークI/O、ユーザーの行動を完全に可視化することができます。予め用意されたルールに加え、カスタマイズ可能なルールも使い、一般的な不正行為や侵害の可能性を検出することができます。さらに、ゴールドマン・サックスのセキュリティチームは、コミュニティ主導のルールや、Sysdigの脅威リサーチチームが提供する最新の検出結果を利用することができます。

優れたセキュリティ戦略には、セキュリティチームをある標準に適合させることが含まれます。ゴールドマン・サックスのGSIRT（シーサートチーム）は、MITRE ATT&CKフレームワークを使用して、検出戦略の調整や、ツールの選択プロセスでの比較を行いました。

ゴールドマン・サックスのセキュリティ・インシデント・レスポンス担当のグローバル長であるWes Williams氏は次のように述べています。「セキュリティはベストプラクティスを中心に推進されており、当社のチームが日々のセキュリティプロセスに統合されているMITRE ATT&CKプラクティスを効率的に適用する方法を必要としていたのです。

ゴールドマン・サックスは、既存のログ記録ツールや、Sysdigが元々作成したオープンソースのクラウドネイティブ・ランタイムセキュリティプロジェクトであるFalcoを含むオープンソースソリューションを評価しました。評価の結果、GSIRTは、ロギングでは必要な一連の検出を十分にサポートできない、と結論づけました。

**ゴールドマン・サックスは、FalcoをベースにしたSysdig Secureによって、インシデントを検出し、コンテキストを持ったきめ細かいデータを使用して迅速に対応する能力がチーム内で拡がったことを認識しました。**

ゴールドマン・サックスは、FalcoをベースにしたSysdig Secureによって、インシデントを検出し、コンテキストと共にきめ細かいデータを使用して迅速に対応できるようになりました。誤検出のノイズを最小限に抑える堅牢な検出機能により、チームの効率と信頼性が向上しました。

## エフェメラルワークロードの監査とフォレンジックの記録

Sysdigが監査とフォレンジックのために収集したデータは、ゴールドマン・サックスの戦略を実現するための重要な要素となっています。これらのデータ・ソースにより、アナリストはイベントが発生した時点からユーザーとシステムのアクティビティを確認することができます。これには、実行されたユーザー・コマンド、確立または試行されたすべてのネットワーク接続、およびホストが実行されていない場合でも、あらゆるI/Oアクティビティを掘り下げることができます。将来的には、GSIRTはコンプライアンスとセキュリティイベントのために、現在のホスト監視に加え、コンテナの監視にもSysdig Secureを活用する予定です。

「私たちの規模では、たとえコンテナが数秒しか経たなかったとしても、完全な記録を残すことが重要です」とWilliams氏は説明します。「そして、フォレンジック調査だけでなく、セキュリティ監査も行うために、このデータを大規模に取得できる必要があるのです。」

インシデントレスポンスチームは、Sysdig Secureが提供する30以上の組み込み検出機能を通じて、即座に価値を引き出しています。Sysdigのデータにより、ゴールドマン・サックスは活動の完全な記録を保持し、監査用に粒度の細かいレベルでイベントを再構築することができます。

> **「私たちの規模では、たとえコンテナが数秒しか経たなかったとしても、完全な記録を残すことが重要です」とWilliams氏は説明します。「そして、フォレンジック調査だけでなく、セキュリティ監査も行うために、このデータを大規模に取得できる必要があるのです。」**
>
> **- ゴールドマン・サックス**
> **セキュリティ・インシデント・レスポンス部門**
> **グローバル長 Wes Williams氏**

**Sysdigは、ゴールドマン・サックスのLinux、コンテナ、クラウド環境において不可欠な存在となりつつあり、イノベーションを加速し、競争力を維持し続けるために貢献しています。**

**Sysdigについての詳細は www.sysdig.jp**

**Sysdig Japan合同会社**
**〒107-0052 東京都港区赤坂7-9-4 赤坂Vetoro 3階**
**https://sysdig.jp/company/contact-us/**

sysdig




CS-GOLDMANSACHS-JA Rev. A 8/22