sysdig

顧客事例

SAP Concurについて：
企業や政府機関に出張・経費管理、請求書管理クラウドサービスを提供する世界的な大手企業

ビジネスニーズ：
- セキュアな会計アプリをグローバルに提供
- 常時アクセス可能なプラットフォームの確保
- 競争力を失わないために、安全なアプリケーションをスピーディに提供

課題：
- Prometheusは運用面で負担が大きかった
- 手動でのスキャンに手間がかかり、業務が滞っていた
- トラブルシューティングやコンプライアンス監査に必要なデータが不足していた

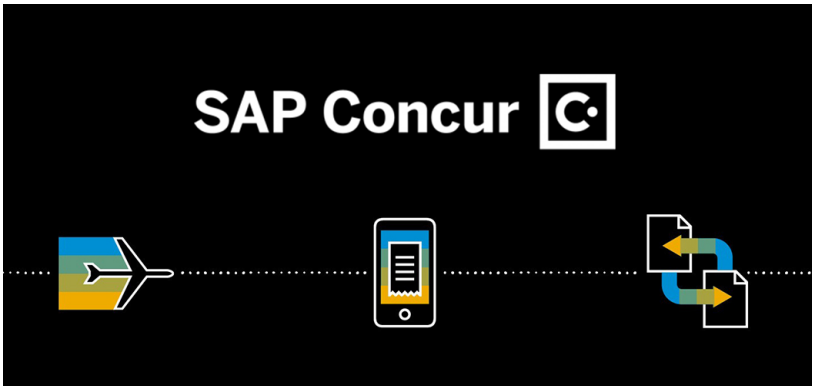
SYSDIG採用のビジネス効果：
SAP Concurは、セキュリティとコンプライアンス要件を満たした常時アクセス可能なプラットフォームを、グローバルで提供しています。新しいサービスも、より早く市場に投入することができるようになりました。

SYSDIGプラットフォームのメリット：
- 自動化により10,000時間以上を節約
- セキュアなDevOpsアプローチ、シングルエージェントでコスト効率を向上
- コンテナがなくなってもフォレンジック対応が可能
- 設立以来20倍に増えているKubernetesの成長に合わせて拡張可能なプラットフォーム
- 監査証跡により、監査の負担を軽減

インフラストラクチャー：
オンプレミス上でのAWS

オーケストレーション：
Kubernetes

SAP Concur



SAP Concur、全世界で7,800万人を超えるエンドユーザーに安全かつコンプライアンスに準拠したソリューションを提供

概 要：

SAP Concurは、出張・経費管理、請求書管理クラウドサービスを企業や政府機関に提供しています。北米だけでも中小から大企業まで25,000社以上のグローバルな顧客基盤を持つSAP Concurは、大規模なインフラを運用しています。SAP Concurにとって新しい、信頼性の高いサービスに常にアクセスできるよう、そしてできるだけ安全に展開することは、最も重要です。

SAP Concurは、アプリケーションをより速く提供するための柔軟性を求めて、モノリシックなアーキテクチャからマイクロサービスへの移行を決めました。その決断から4年後、SAP Concurのチームは現在20人に増え、本番で2,000以上のノードからなるコンテナ・エコシステムを担当しています。

課 題：

SAP Concurは、小規模の特別チームでマイクロサービス構築を始めました。SAP ConcurのDirector EngineeringであるMike Luedke氏は、「草の根的活動から始まった」と語ります。「異なるチームから数人が集まり、当初はクラスターを構築していました。最終的には、Concur社内のアーリーアダプターに開放しました。その後、急速に普及が進みました。最初は非公式なグループによる管理でしたが、次第にConcurの将来像がはっきりと見えてきました。その時点で、正式なチーム編成を開始したのです。」

SAP Concurのスタックは、オープンソースでスタートしました。特に、従来のインフラと新しいコンテナ環境のセキュリティを比較した場合、セキュリティと可視性のギャップがすぐに明らかになりました。

シニア開発マネジャーのTiziano Tarolla氏は述べています。「オープンソースのPrometheusで100ノードに到達した頃、より良いスケーリング戦略を考えなければならない変曲点にさしかかったのです。私たちは、リソースに窮していました。社内アプリケーション・チームのニーズである拡張に忙しく、Prometheusのスケーリング・ソリューションを考えるための余剰サイクルがあまりなかったため、商用オプションを検討し始めました。Sysdig MonitorのマネージドPrometheusサービスはオープンスタンダードに基づいているため、私たちの監視環境を再構築する必要はありませんでした」

SAP ConcurがSysdigを採用した理由：

Luedke氏は、選択肢を探す際、「Concurは、スタックに導入する商用ソリューションについて、多くの時間をかけて熟慮し、選択しました。スタックの他の部分はすべて無料のオープンソースだったからです」

よく知られている複数の商用監視・セキュリティツールを比較検討した結果、SAP ConcurがSysdigを選択した理由は下記の通りです。

- セキュリティに対するKubernetesファーストのアプローチ
- ソリューションのルーツがオープンソース
- システムコールを活用した独自技術
- セキュリティ、コンプライアンス、モニタリングが統合されている
- PromQLをサポート
- カーネルレベルの深いメトリクスをすぐに利用でき、あらゆる方法でスライスが可能

数千時間を節約し、毎日のリリースが可能に

Sysdigの採用前は、SAP Concurはコードを本番環境にプッシュする前に手動でレビューを行っていました。Luedke氏によると、「Sysdigで、手動レビューの多くを自動化することができました。パイプラインにSysdigを組み込み、本番環境に移行する際にコンテナの脆弱性チェックとコンプライアンスチェックを実行しています。これらのチェックが自動化された事で、私たちの活動がよりスピーディになりました。

さらに、レビューのプロセスと、現在の規模でSysdigがなければどうなるかをLuedke氏は説明してくれました。「脆弱性の手動レビューや手動スキャンは、チェックインごとに10分かかることもあります。以前の脆弱性スキャンのオプションはオープンソースのClairを使用していたので、私のチームは別のインターフェースで結果を確認しに行かなければならず、時間がかかっていました。Sysdigを使えば、チームがデプロイを行う際にパイプラインの一部として、これらすべてが自動的に行われるようになるのです。現在、私たちは1日あたり数千のマージを処理しています。1件あたり平均10分かかり、1日に何千件も処理することになると考えると、Sysdigなしでは同じスピードで処理することはできないでしょう。」

セキュリティと可視性のギャップを取り除く

Sysdigは、唯一のセキュリティ、コンプライアンス、監視が統合されたプラットフォームです。そして、開発、DevOps、セキュリティチーム間の情報のサイロ化解消に繋がる信頼できる唯一の情報源を提供します。このアプローチにより、企業は、クラウドとKubernetesのコンテキストに自動的に関連付けられた粒度の高いシステムデータを分析でき、問題をより迅速に解決することができます。また、DevOpsチームがセキュリティの責任を負うことも可能になります。

Sysdigは、SAP Concurのアプリケーション、運用、インフラ、DevOps、セキュリティチームなど多くのチームで活用されています。1つのツールで複数のユースケースに対応することで、全員がセキュリティに責任を持ち、安全なDevOpsを採用することが可能になりました。Luedke氏は、「Sysdigを使うことで、何が起きているのかを直接把握することができます。Sysdigをトラブルシューティングツールとして使用することにより、アプリケーション開発者がアプリケーションのDevOpsを行うことができるようになりました。運用チームやインフラチームに連絡しなくても、Sysdigにアクセスするだけで何が起こっているかを確認できるのです。」

「脆弱性の手動レビューや手動スキャンは、チェックインごとに10分かかることもあります。[...] Sysdigを使えば、チームがデプロイを行う際にパイプラインの一部として、これらすべてが自動的に行われるようになるのです。現在、私たちは1日あたり数千のマージを処理しています。1件あたり平均10分かかると考えると、[...] Sysdigなしでは同じスピードで処理することはできないでしょう。」

Luedke氏はさらに続けます。「Sysdigは、アプリケーション開発者だけでなく、インフラチーム、すべての人の時間を節約してくれます。このように、データを可視化することで、ハードルを下げることができるのです。何かを見たいと思ったときに、余分なオーバーヘッドがなく、ただ見に行くだけでいいのです。インフラで何が起こっているのか、よりよく理解できるようになった、と思います。」

また、Luedke氏は、統一されたプラットフォームは安全性を高めるだけでなく、リソースとコストを削減することができる、と説明しました。「モニタリングの全体像を把握できるひとつのソリューションを利用することで、シンプルになります。つまり、インフラ運用の監視とセキュリティの監視を同時に行うことができるのです。これには大きな価値があります。より戦術的な観点からは、1つのエージェントがすべてを報告することで、コストを大幅に削減できます。なぜなら、エージェントごとに処理能力が必要だからです。Sysdigで得られるものを他で得るには、2つのツールが必要で、エージェントの数が2倍になってしまいます。

企業規模でのPrometheusメトリクス

SAP ConcurがSysdigを選択する前、チームはモニタリングにPrometheusを使用していました。Luedke氏によると、「メトリクス側では、Prometheusがあったので問題はなかったのです。しかし、スケーラビリティの面で問題がありました。規模が大きくなるにつれて、スケーリングの問題からPrometheusのデータベースが定期的に失われていました。ある時点では、1時間分のデータしか保存できないのです。1時間以上前に何かが起こると、収集したデータ量に見合うだけの損失が発生してしまうのです。時には、データベースが完全に失われてクラッシュすることもありました。データがまったくないのです。私たちは目が見えない状態で空を飛んでいたようなものです。

Sysdigは、Prometheusと完全な互換性を持つ唯一のソリューションです。Prometheus Query Language（PromQL）をサポートし、高度なメトリッククエリーの実行、ダッシュボードの構築、アラートの作成が可能です。Sysdigは、Prometheusモニタリングの組織的な導入の妨げとなっている、規模、データ保持、企業内アクセス制御といった問題に対処します。

イメージスキャンの活用で、セキュリティをシフトレフト

イメージスキャンにより、DevOpsプロセスの早い段階で脆弱性や設定ミスを発見し、修正することで、企業はセキュリティリスクを管理することができます。SAP ConcurはSysdigを利用して、レジストリやCI/CDパイプライン内、および実稼働中のイメージを継続的にスキャンしています。これにより、Kubernetesベースのアプリケーションに脆弱性を独自にマッピングすることで、時間を節約しています。

Luedke氏によると、「私たちは、コンテナの脆弱性スキャンと侵入検知を行うためにSysdigに依存しています。Sysdig以前は、ノード上でホストベースの侵入検知を実行していましたが、コンテキストがありませんでした。どのプロセスが影響を受けたかを教えてくれるだけで、それは単にDocker IDのように見えるだけでした。大規模なマルチテナント環境では、Kubernetesのメタデータと混在させないと、そのコンテナが何に属しているのかが分からないのです。その情報を取得できないわけではありませんが、その作業を定期的に行うのは本当に骨が折れることでした。Sysdigは、セキュリティイベントやその他の低レベルの情報をコンテキストに沿って表示する、実に迅速な方法を提供してくれました。」

「会社の成長に伴い、Sysdigの使い方や私たちの環境のセキュリティ対策は増え続けています。以前は、商業界のお客様にかなり注力していましたが、最近では、公共部門のビジネスの成長が大きくなっています。それに伴い、新たなコンプライアンス義務も発生しました。Sysdigを活用することで、これらのコンプライアンス項目にもチェックが入るようになりました。しかし、私たちのコンプライアンス要件がKubernetes環境とともに大きくなるにつれて、手作業で調査することができなくなりました。現在のような規模になると、Sysdigなしでは運用できなくなります。このようなソリューションがなければ、単にKubernetesを使うことができなかっただけです。」

「Sysdigを当社のパイプラインに組み込んでいます。私たちの環境に導入されたコンテナに対して、コンテナ脆弱性チェックとコンプライアンスチェックを実行するパイプラインにSysdigを組み込んでいます。これらのチェックが自動化された事で、私たちの活動がよりスピーディになりました。

コンプライアンスレポートの簡素化

アクティビティ監査では、Sysdigはコンテナのアクティビティをキャプチャし、アプリケーションのコンテキストや、Kubernetesのユーザーやサービスと情報を関連付けます。この機能は、監査の際など、何百回となく重宝してきました。

Luedke氏は、「監査証跡があることで、多くの場面で役立っています。あるとき、監査役が私たちの言うとおりの環境を運用しているかどうかを 確認したい、と言ってきたことがありました。インフラを動かしている特定のコンテナのプロセス情報を要求されたのですが、そのコンテナはdistrolesssを動かしていて、シェルがないんです。必要なものだけにロックされているので、非常に安全ですが、その分、実行することでプロセス情報を取得するようなことはできないわけです。Sysdigを使ってそのコンテナを可視化し、監査人に証拠を提供することができたのです。」

Luedke氏はさらに続けます。「私はそのインスタンスのトッププロセスのメトリクスビューでダッシュボードを見て、彼らが必要とするものを提供しただけです」と述べました。また、私たちがこの義務を果たしている、と伝えたので、私たちのコンテナがイミュータブルであることを確認するためのフォローアップの質問もありました。Sysdigを使用することで、実行中のコンテナが起動以来変更されていないことを証明することができました。Sysdigの監査イベントを使用して、コンテナ上のファイルシステムとシェルのアクティビティを示すだけで、それを証明できました。」

コンテナが存在しなくなってもフォレンジックが可能

コンプライアンス監査に有用なアクティビティ監査証跡は、異常な振る舞いがあった場合に非常に貴重です。Sysdigを利用すれば、たとえコンテナが存在しなくなったとしても、フォレンジック用にすべてのアクティビティ情報をキャプチャファイルに取り込むことができます。

SAP Concurでは、Luedke氏は「Sysdigがトラブルシューティングのヒントになったことが何度もあります」と説明します。「Sysdigはトラブルシューティングのヒントを何度も与えてくれました。Sysdigを使うことで、問題の所在をピンポイントで把握することができます。これは、私たちがSysdigを使う価値を最も感じる機能のひとつです。」

Luedke氏によると、キャプチャ以外にも、「様々な属性で指標をスライスして表示できることは、非常に便利です。私たちは前例のない問題によく遭遇しますが、その問題を必要な方法で表示する定型ビューがない場合、そのビューをすばやく構築することができます。何かが計画通りに進まないときに、この機能がどれほど役に立つか、説明しきれません」。

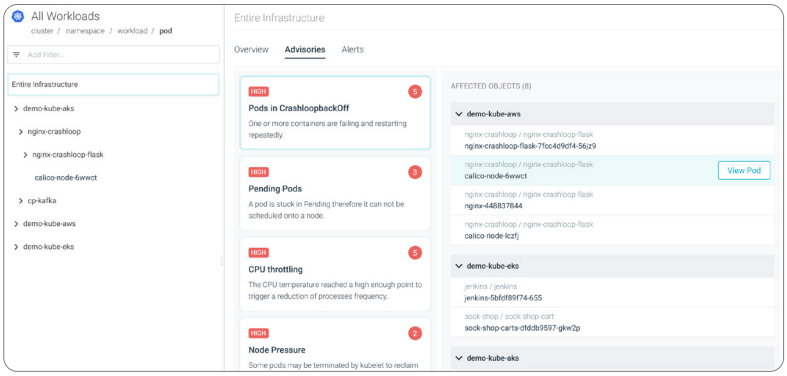
ディープカーネルデータで比類なき可視性を実現

Sysdigはシステムコールを使って、コンテナ内で何が起きているかを報告します。ユーザースペースとカーネルがやり取りする主要なメカニズムであるシステムコールは、プログラムが何をしているのかについての素晴らしいインサイトを提供し、トラブルシューティング、監視、ボトルネックの特定に非常に役立ちます。

Luedke氏によると、「私たちはSysdigのアプローチを気に入りました。Sysdigのアプローチと、実際にデータを収集する方法は、他の選択肢と比較して、優れたセキュリティ監視ソリューションであると感じました。他のセキュリティツールは、Kubernetesの機能を拡張するために多くの残存機能を提供しています。Kubernetesの隙間を埋めているようなものですが、Kubernetesも成熟してくると、その隙間はすでに含まれているか、上流で処理されているものなのです。私たちは、カーネルからメトリクスを取り出す方法を強く信じています。これは非常に堅実な戦略です。私はいつも、Sysdigから得られるすぐに使えるメトリクスに感心しています。これは非常に低レベルフォーマットのデータで、他のソリューションと比較して非常に広範であるため、進行中の問題の奥深くまで見ることができます。

ハイブリッドクラウド基盤における可用性の最大化

SAP Concurの環境は、AWSクラウドとオンプレミスのインフラにまたがっています。Sysdigを利用することで、SAP Concurはすべてのインフラで同じ表示体験を得られるため、クロスプラットフォームに依存するマイクロサービスの問題を容易に予測することができます。問題が発生した場合、システム全体を可視化することで、より迅速な解決が可能になります。



Luedke氏は、「Sysdigでは、AWSとオンプレミスの両方にまたがる問題のスコープと検索を1つのビューで行うことができます」と述べています。「Sysdigでは、AWSとオンプレミスの両方の問題を1つの画面で確認することができます。ダッシュボードのスマートなグループ化により、必要なコンテキストで意味のある方法でメトリックの異なる属性をグループ化することができます。Kubernetesやネームスペースのビュー、より物理的なビュー、あるいはクラスターのビューなど、欲しいビューを得るためにデータの範囲を設定することで詳しく分析できるようになり、それをSysdigのコンテキストで煮詰めれば、インフラ全体で何が起こっているかを本当に理解できるようになりました。」

オープンでコミュニティベースのSysdig

SAP Concurのチームは、選定段階でSysdigがオープンソースの基盤上に構築されていることに惹かれたと、いいます。Luedke氏によると、「Sysdigがオープンソースを採用し、またオープンソースに貢献していることが気に入りました。それは我々にとって重要なことでした」

今日、オープンソースはクラウドを牽引しています。Sysdig Inspect、Falco、Prometheusなどのオープンソースツール上に構築されているため、Sysdigはより速く、より安全なソフトウェアを提供することができます。

Luedke氏は、「Sysdigがオープンソースを採用しているため、新しい機能を追加する必要がある場合にも容易に対応できる」と述べています。「Prometheusのようなオープンスタンダードを迅速かつ容易に利用できることが役立っています。例えば、すぐに使える統合機能がない場合でも、Prometheusのエンドポイントを使って、必要な機能を構築することができます。簡単で迅速、本当に素晴らしいことです。」

オープンソースをベースとする企業であることは、Sysdigがコラボレーションを重要視していることも意味しています。Sysdigの立ち上げ以来、製品チームは顧客の声に耳を傾け、彼らのニーズをロードマップに反映させるために何時間も費やしてきました。長年のユーザーであるLuedke氏にとって、このようなサービスのレベルは非常に重要です。「Sysdigは、私たちにとって良いパートナーです。私たちのニーズの変化に常に敏感で、大小にかかわらず、私たちのためのソリューションを見つける手助けをしてくれました。彼らは我々と一緒に現場にいるのです。」

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/

CS-SAPCONCUR-JA Rev. A 9/22