sysdig | 株式会社NTTドコモ

CUSTOMER STORY

8,000万ユーザーのAPIサービス基盤「RAFTEL」の運用とコンプライアンスをSysdigで支える

株式会社NTTドコモ ネットワーク本部 サービスデザイン部
（左から）
アプリケーション基盤 担当部長　加藤 雅俊 氏
アプリケーション基盤　担当　伊藤 泰平 氏
アプリケーション基盤 担当課長　山口 範和 氏
アプリケーション基盤　主査　福田 訓之 氏

「Sysdigが止まったらどうなるのか？私たちのAPI基盤サービスRAFTELは約60を超える社内の各組織で使われており、そのサービスの利用者、約8,000万人に大きな影響が出るでしょう。」とおっしゃるのは株式会社NTTドコモの加藤雅俊氏です。「RAFTELの安定稼働をSysdigが支えているのです。」

株式会社NTTドコモ（以下、NTTドコモ）は日本の移動体通信サービスのリーディングプレイヤーとして日本国内に約8,700万の携帯電話ユーザーを持つ企業です。単に携帯電話への接続サービスを提供するだけではなく近年では光通信サービス、衛星電話、動画や音楽、ショッピングなどのコンテンツサービス、更にペイメントサービスから子会社であるNTTコミュニケーションズによる法人向けサービスなど多方面に展開されています。今回はそのNTTドコモのサービス間連携を実現するAPI基盤RAFTELにおいてSysdigが導入された経緯をネットワーク本部 サービスデザイン部 アプリケーション基盤グループの加藤氏、山口氏、福田氏、伊藤氏の4名からお話を伺いました。

NTT docomo

株式会社NTTドコモ

事業内容

- コンシューマ通信事業：
  個人向け通信サービス（5G・LTE等携帯電話サービス、光ブロードバンドサービス、国際サービス）、各サービスの端末機器販売など
- スマートライフ事業：
  金融決済サービス、コンテンツライフスタイルサービス（動画・音楽・電子書籍等配信サービス・ドコモでんきなど）、マーケティングソリューション、あんしん系サポート（ケータイ補償サービスなど）など
- その他の事業（法人通信など）：
  法人向け通信サービス（5G・LTE等携帯電話サービス、ユビキタスサービス、衛星電話サービス、光ブロードバンドサービス、国際サービス）、各サービスの端末機器販売、オフィスリンクなど

導入効果

- セキュリティインシデント対応の精密化
- Kubernetesの仕様にマッチしたセキュリティ
- 厳しい要求に耐えられるコンプライアンス機能

導入前の課題

- パブリッククラウド上でのセキュリティ対応
- 現実にマッチしないコンプライアンス

選定理由

- Wiresharkの開発者が開発したオープンソースを基盤としたKubernetesに最適なセキュリティ製品

API基盤、RAFTELをGoogle Kubernetes Engine上に再構築

RAFTEL API基盤チームではインフラストラクチャーチームがセキュリティの実装とコンプライアンスにSysdig Secure、運用チームがSysdig Monitorを使っています。

NTTドコモでは主にAmazon Web Services（AWS）をパブリッククラウドとして活用していましたが、社内向けAPI基盤を提供する際にGoogle CloudのAPI基盤サービス「Apigee」を使い始めました。そこから仮想マシンによるアプリケーション実装からコンテナ環境に移行し、コンテナオーケストレーションのデファクトスタンダード、Kubernetesを使ったGKE（Google Kubernetes Engine）をプラットフォームとして採用しました。

RAFTELの開発リーダーである伊藤泰平氏はSysdigの採用経緯について伺いました。「AWSに馴れていたこともあってGoogle Cloudについては難しく感じることがありました。Google Cloud上でのセキュリティを検討するにあたり、クラウドのリスクを一元的に把握できるSysdig候補にあがりました。」

> 私たちの API 基盤サービス「RAFTEL」は約 60 を超える社内の各組織で使われており、 この基盤上のサービスを 8,000 万人のユーザに利用いただいています。 RAFTEL の安定稼働を Sysdig が支えているのです。
>
> アプリケーション基盤 担当部長
> **加藤 雅俊 氏**

選定理由

インシデントを原因まで辿れるモニタリング機能と使用中コンポーネントに絞り込むアラートのフィルター機能

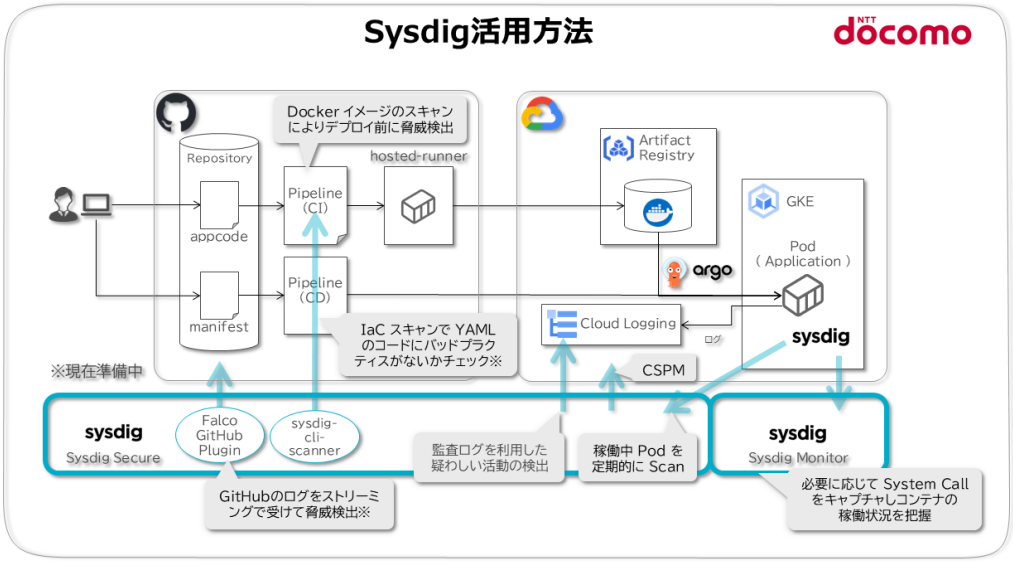
Sysdig採用の検討を行った同グループの福田訓之氏は、その採用理由をこう語られています。

アプリケーション基盤 主査
福田 訓之 氏

「他のベンダーの製品やGoogleの製品も比較しましたが、チームのエンジニアでWiresharkを知っていた人がおり、彼が「Wiresharkを開発した人が作っている製品だから間違いない」、と熱く語っていたのです。Sysdigの米国本社を訪問して直接説明を受けました。そのインパクトは大きかったですね。SysdigのCTOであり、Wiresharkの開発者であるLoris Degioanniが直接デモと解説をしてくれましたから。あと細かい話ですが、脆弱性のチェックを行う時に使っているコンポーネントを優先して結果を見せてくれる「In-Use」の機能はパブリッククラウドにはない機能で、優れていますね」（福田氏）

また伊藤氏は開発に直接携わった経験から「セキュリティのインシデントが発生した時にモニタリングの機能の中からタイムラインを辿って原因に到達できるのは使いやすいですね。またRAFTELが使うKubernetesの設計思想にフィットしています」とその使いやすさについて感想を述べています。「Sysdig Monitorの中からネットワーク診断のツールであるtcpdumpの細かいところまでドリルダウンできる機能もエンジニアからは高い評価を受けています。」（伊藤氏）Sysdigは、自社プロダクトをKubernetes上で開発し、ユーザーとして使いやすさを追及していることもあり、Kubernetesのモニタリングについてはユーザー目線でニーズを掴んでいることも利点となっているようです。

アプリケーション基盤 担当
伊藤 泰平 氏



導入効果

日々アップデートされるコンプライアンス要件にSysdig Secureで対応

実際にSysdigを採用してみると思わぬ発見もあったようです。

「社内にIT基盤に関するコンプライアンスは確立されていたのですが、実際にGKEでサービスを構築してSysdig Secureを導入してコンプライアンスをチェックしてみると実態に合わないことや抜けている項目が見つかったのです。」（加藤氏）

アプリケーション基盤 担当課長
山口 範和 氏

ツールの機能以上に業務改善のヒントが見つかったというのは嬉しい驚きかもしれません。担当課長である山口範和氏は「IT基盤が進歩するに従ってコンプライアンスとしてチェックしなければいけない項目は増えています。『世間ではこんな攻撃が発生した。NTTドコモ社内は大丈夫か？』というリクエストに応えるために部内の仕事量は増えてしまってますが、Sysdigのコンプライアンス機能に助けられています」と、コンプライアンスの徹底について話されました。

また伊藤氏からは「Sysdig Secureのコンプライアンスはかなり細かな部分までカバーしてくれています。ただし実際にはユーザーが触れる領域ではない部分、つまりGoogleのプラットフォーム側の領域までチェックしてしまうのでそれに関しては分けて評価できるようになると良いとは思います」とSysdig Secureが包括的にコンプライアンスチェックを行っていることを評価されました。

RAFTELのサービス更新を支えるインフラ基盤の開発と運用を効率化するSysdig Sage活用へ

アプリケーション基盤 担当部長
加藤 雅俊 氏

加藤氏は「RAFTELはパブリッククラウドだけではなくオンプレミスでの実装も検討しましたが、総合的なコンシューマー向けのサービスを実現しようとするとどうしてもスピードが重要になります。想定外のアクセスが発生することも良くありますし、NTTドコモの動画サービスのLeminoでもコンテンツに対して短い時間の中で集中的にアクセスが来るケースが多くあります。そういうニーズがある中で選択したのがパブリッククラウドだったのです」とインターネットサービス実装の難しさを語る場面もありました。また山口氏は「特にコンプライアンス面では我々のサービス、そしてプラットフォームについて様々なチェックが随時必要となりますが、それを毎回エンジニアがマニュアルで行うのは工数がかかる作業になります。それに対して生成AIを使って「このサービスはこのコンプライアンス項目に適合しているか？」を問い合わせできるような機能があると助かりますね」と、Sysdigが新たに発表したSysdig Sageに対する期待を寄せています。

> “ IT基盤が進歩するに従ってコンプライアンスとしてチェックしなければいけない項目は増えています。『世間ではこんな攻撃が発生した。NTTドコモ社内は大丈夫か？』というリクエストに応えるために部内の仕事量は増えてしまってますが、Sysdigのコンプライアンス機能に助けられています。
>
> アプリケーション基盤 担当課長
> **山口 範和 氏**

今後への展開

冒頭の「約8千万人が使うドコモのサービスを支えるSysdig」に対する期待は大きく、現状は満足が期待を上回っています。今後の活用の拡がりとして、セキュリティだけではなくドコモのAPIサービス全体のモニタリングにもSysdig Monitorの適用を検討されています。

株式会社NTTドコモの詳細は、**www.docomo.ne.jp/**をご覧ください。

株式会社NTTドコモ

主な事業内容：

コンシューマ通信事業
スマートライフ事業
その他の事業（法人通信など）

インフラ基盤

Google Cloud

オーケストレーション

Kubernetes

ソリューション

Sysdig Monitor, Sysdig secure

Sysdigについて

クラウド環境では、1秒1秒が重要となります。攻撃は驚くほどの速さで進行するため、セキュリティチームはビジネスを減速させることなく、攻撃から守る必要があります。Sysdigは、ランタイムインサイトとオープンソースのFalcoを利用することで、リスクにおける変化を即座に検知し、クラウド攻撃をリアルタイムで阻止します。Sysdigは、クラウドのワークロード、アイデンティティ、サービス全体におけるシグナルを相互に関連付けることで、隠れた攻撃経路を明らかにすると共に、真のリスクに優先順位を付けます。予防から防御に至るまで、Sysdigは企業がイノベーションという最重要事項に集中できるよう支援します。

Sysdig. Secure Every Second.

Sysdigの詳細は、**sysdig.jp**をご覧ください。

デモを依頼 →

sysdig

CUSTOMER STORY

CS-DOCOMO-JA REV. A 9/24