CLOMO を支えるプラットフォームとその進化

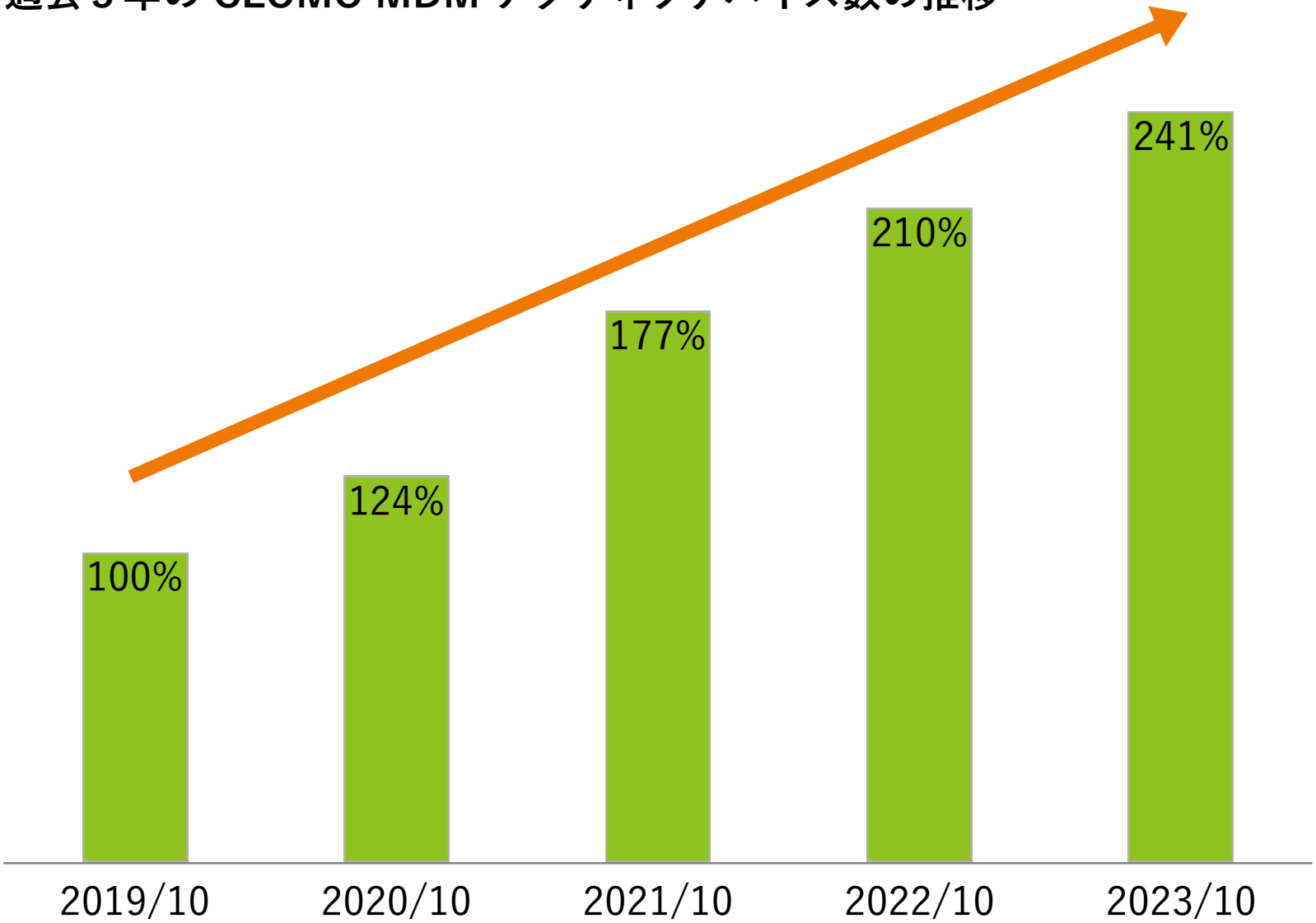
2023年12月14日

株式会社アイキューブドシステムズ
製品開発運用本部 プラットフォーム運用部
田中 孝憲

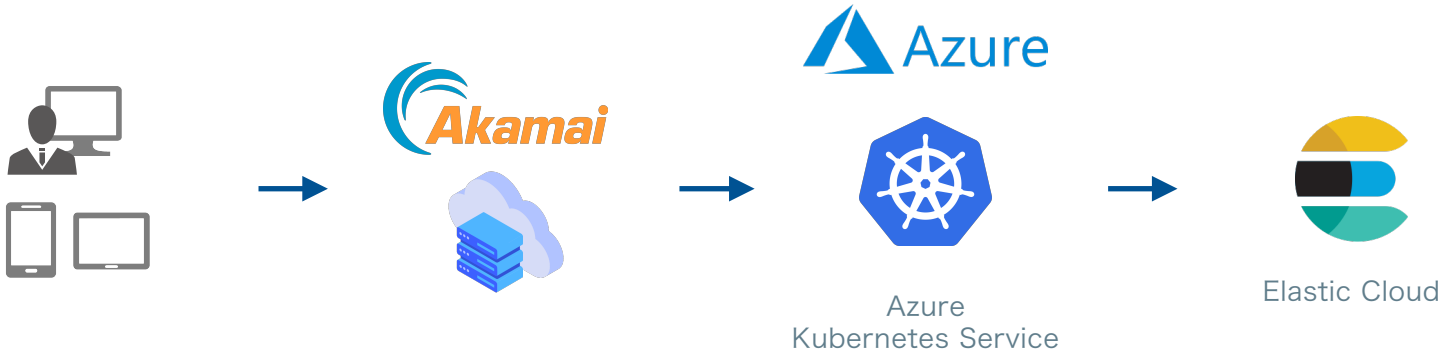
CONTENTS

1. CLOMO を支えるインフラストラクチャ

過去５年の CLOMO MDM アクティブデバイス数の推移

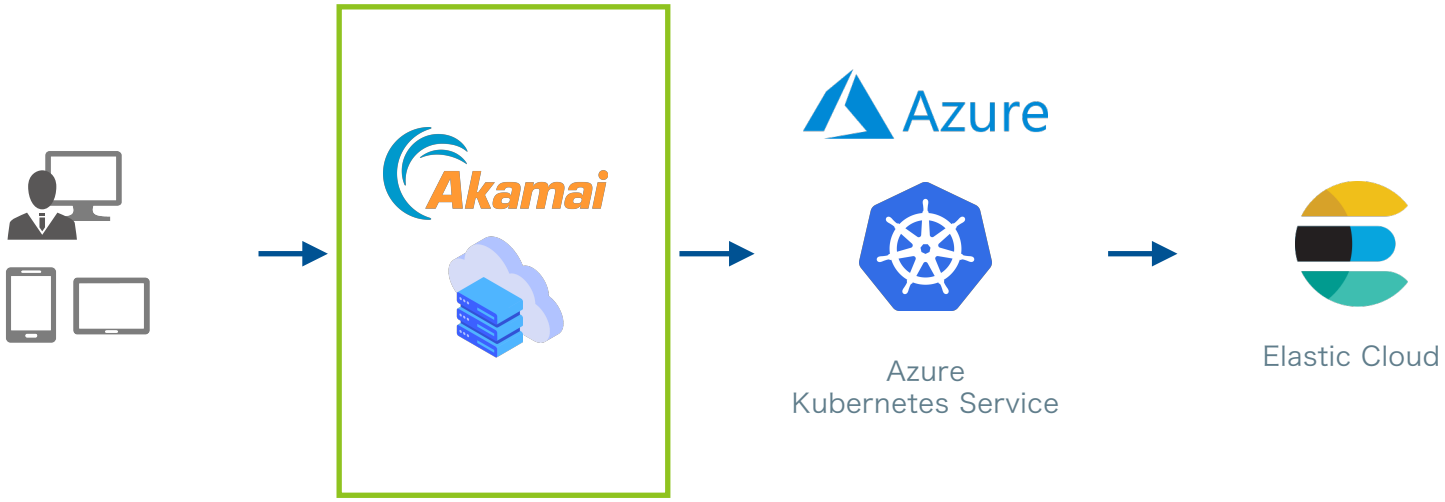


CLOMO システム構成



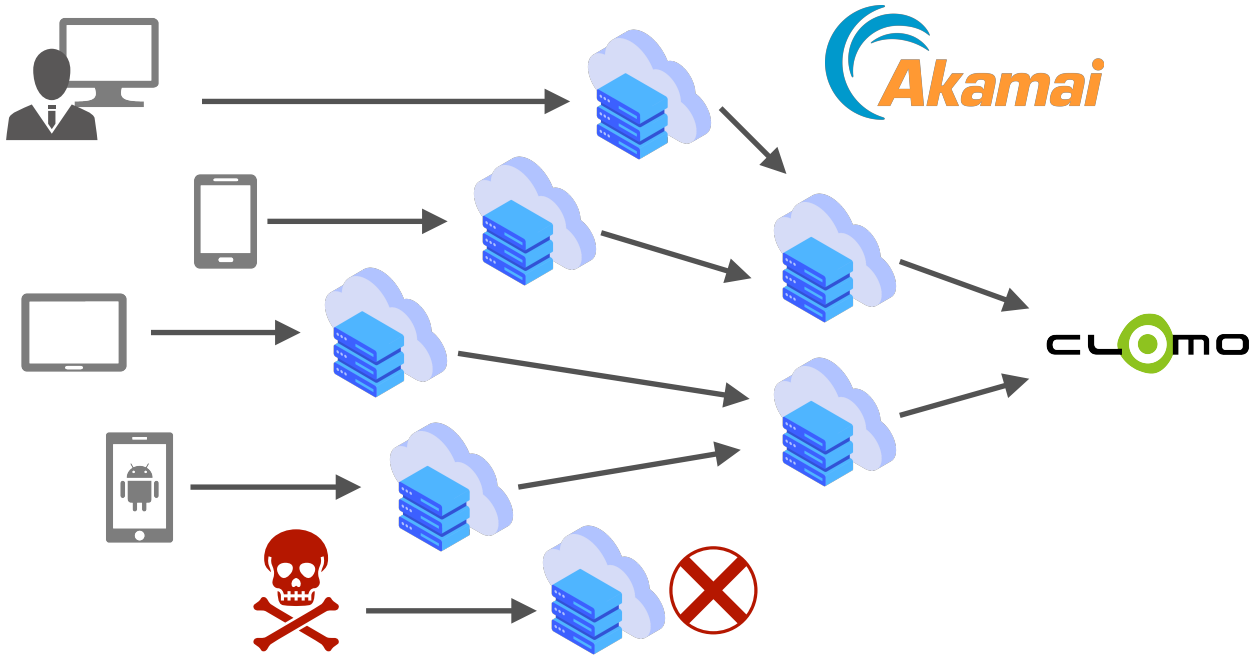
CLOMO システム構成

- Akamaiによる外部セキュリティ防衛



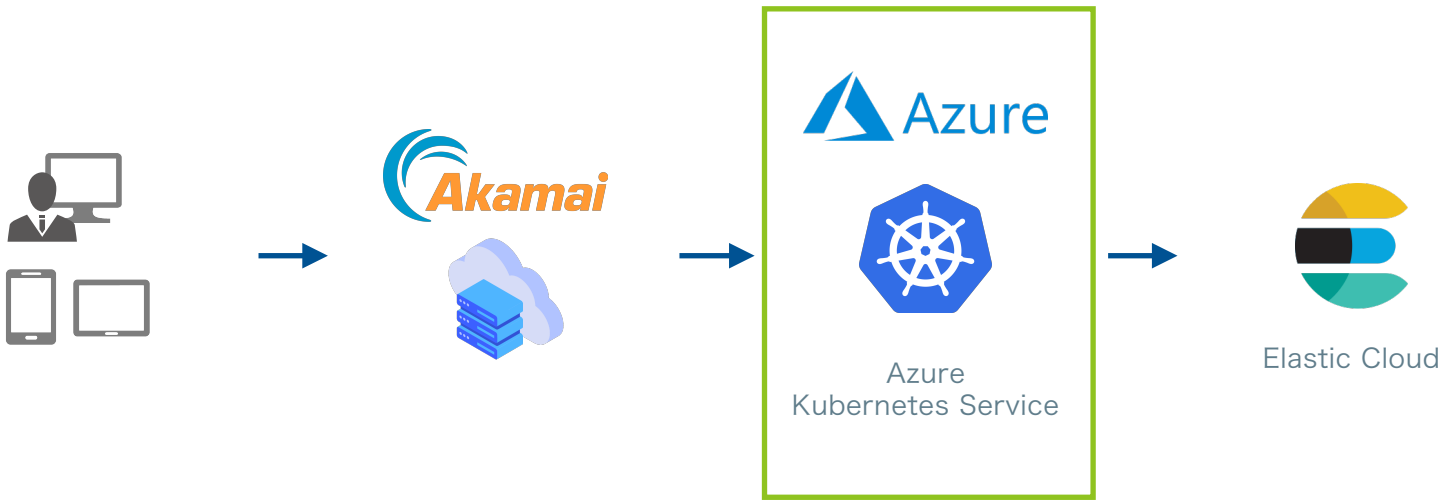
Akamai による外部セキュリティ防衛

- Web Application Firewallを導入
- DDoS攻撃やSQLインジェクションなどを遮断
- Akamai専門スタッフによるコンサルティング・最新のルールを適用



CLOMO システム構成

- インフラはMicrosoft社のAzureを使用
- Kubernetesでスケーラブルに



インフラは Microsoft 社の Azure を使用

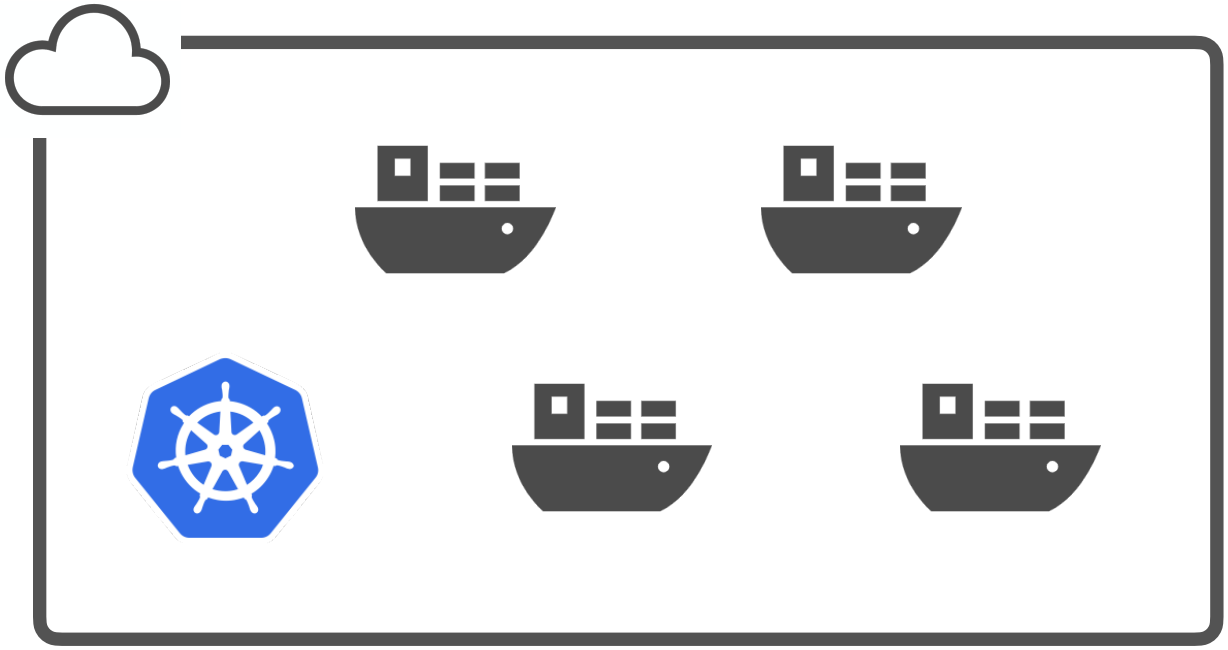
90を超えるコンプライアンス認定資格

【 例 】

- ISO / IEC 27001:2013
- FISC（金融機関向けコンピューターシステムに関するセキュリティガイドライン）

Kubernetes でスケーラブルに

- Azure提供のAzure Kubernetes Serviceを利用
- サービスを自動で迅速にスケーリング



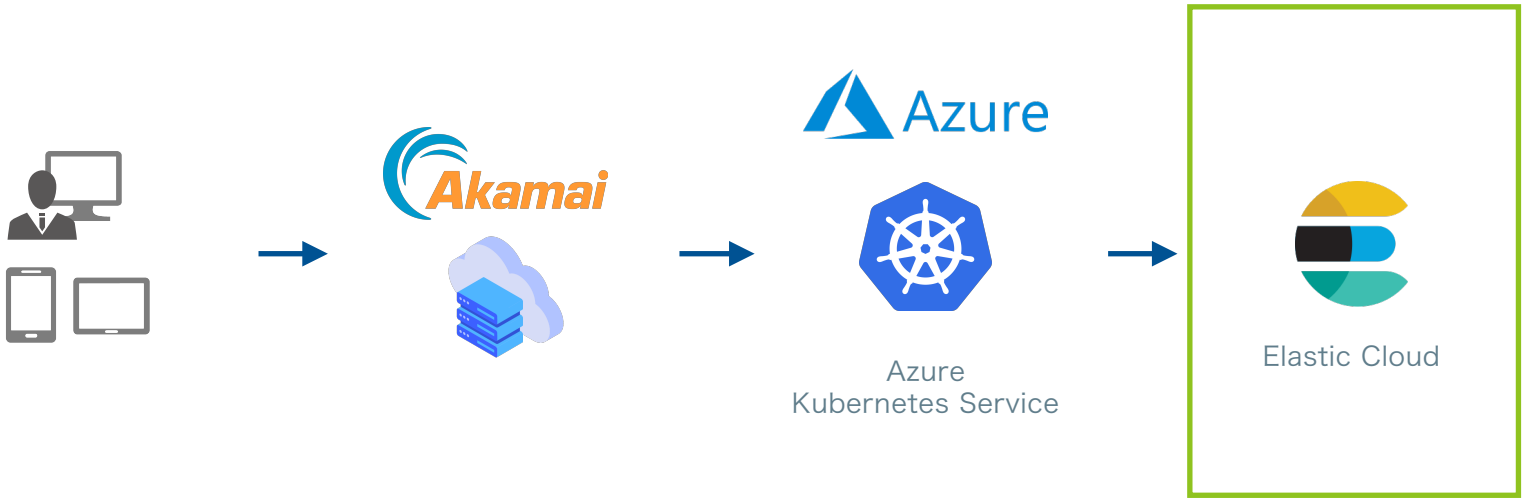
Falco で Kubernetes のセキュリティをより強固に

Kubernetesのセキュリティ監視のスタンダード「falco」の導入

- OSのシステムコールを分析しKubernetesのアクティビティを可視化
- Kubernetes上で誰がどこで何をしたのかを正確に理解できるように
- Elastic Cloudに結果を保存
- 運用チームにアラートを通知

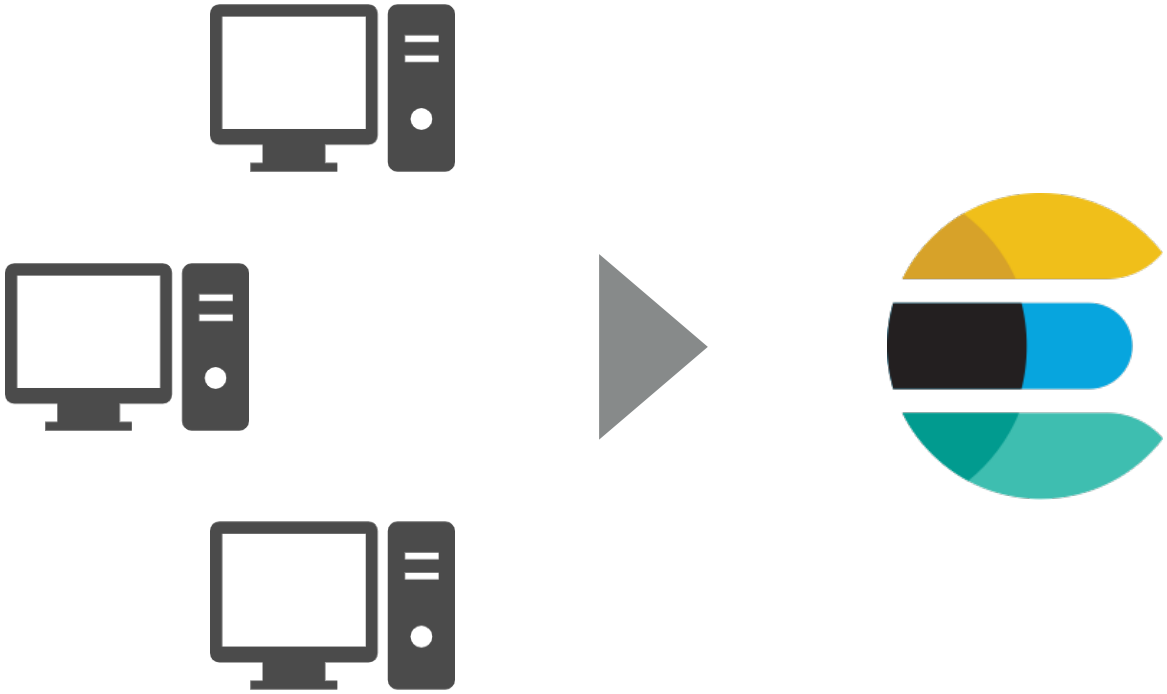
CLOMO システム構成

- Elastic Cloudによる効率的なログ検索



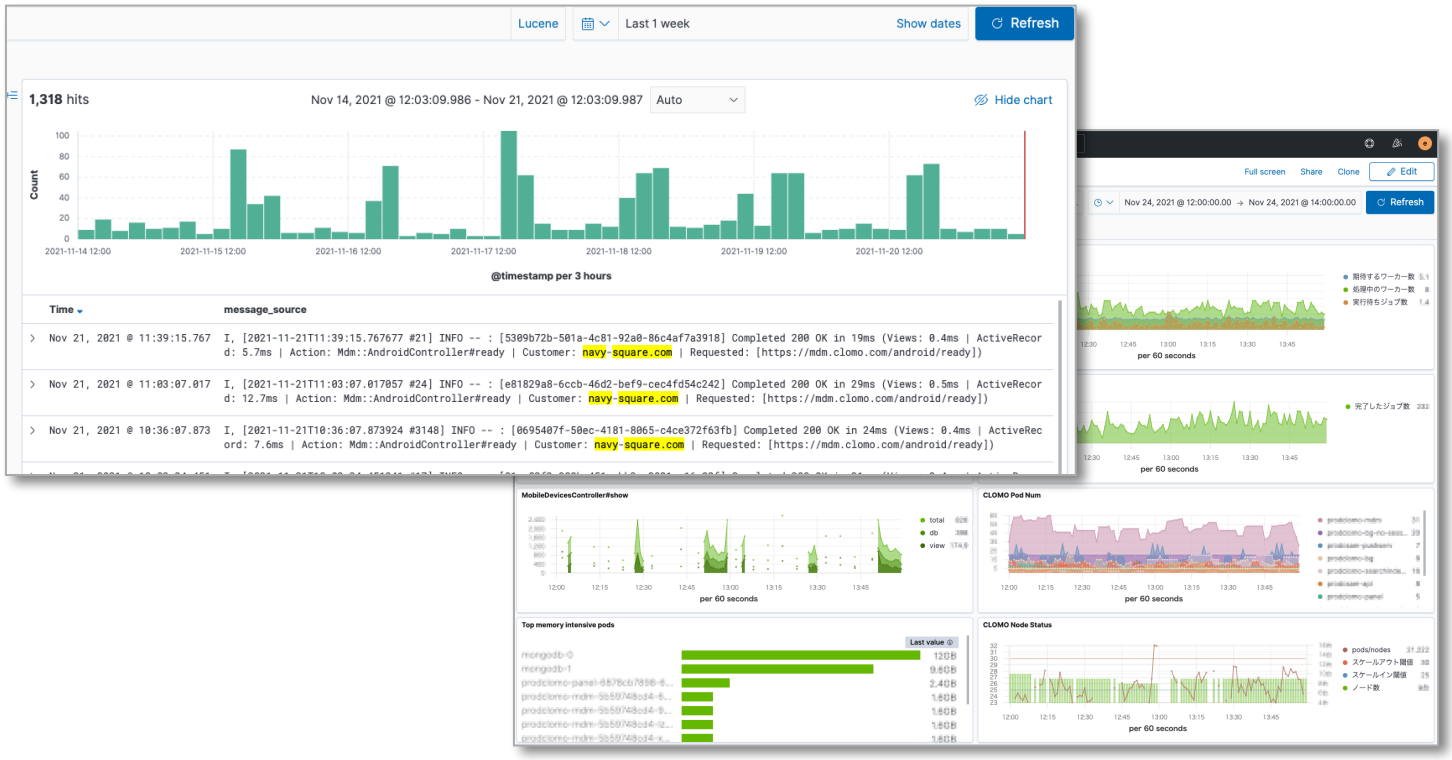
Elastic Cloud による効率的なログ検索

- 分散したログを一箇所に集約



検索・可視化による迅速なサポート対応

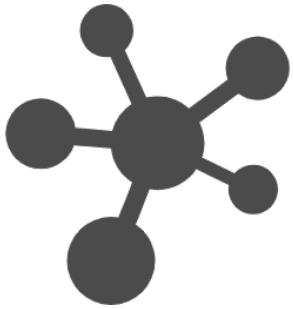
- 横断的に素早くログを検索 → お客様の問い合わせに迅速に回答
- 集約したログ・メトリクスを解析・グラフ化してひと目で状態を確認



Elastic の機械学習によるアノマリ検知

Elastic機械学習を利用することで、
運用異常を自動検知

- しきい値設定を明示的にしなくても柔軟な異常検知が可能
- しきい値をスパイク的に超過してしまったような偽陽性を排除
- 今後、サーバー状態の異常検知以外にも役立てられる可能性も模索



Kubernetes 環境を運用する体制

- 運用メンバーはKubernetes専門資格を保持

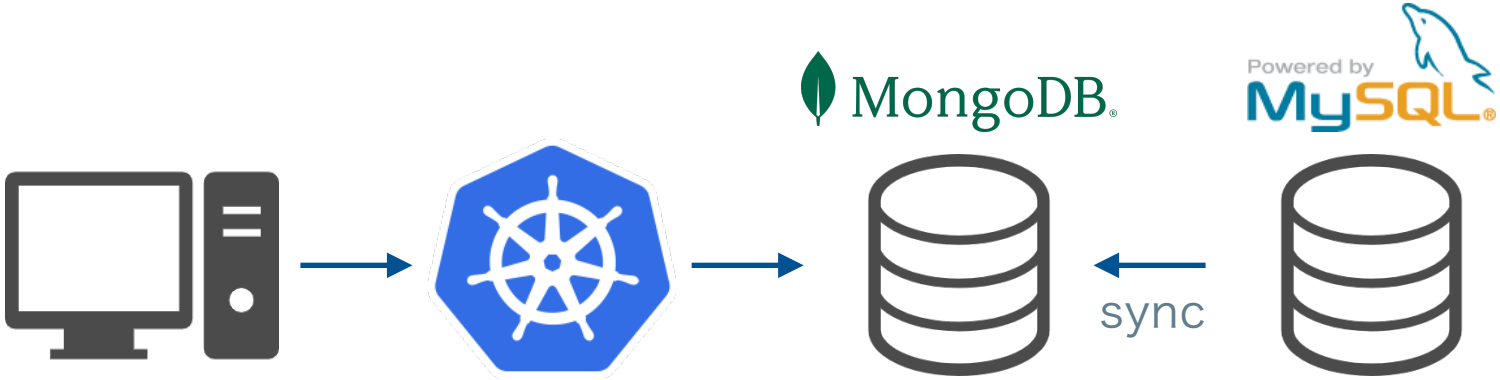
2. CLOMO 内部アーキテクチャの進化

CLOMO PANEL の高速化

- デバイス一覧取得における旧来の処理

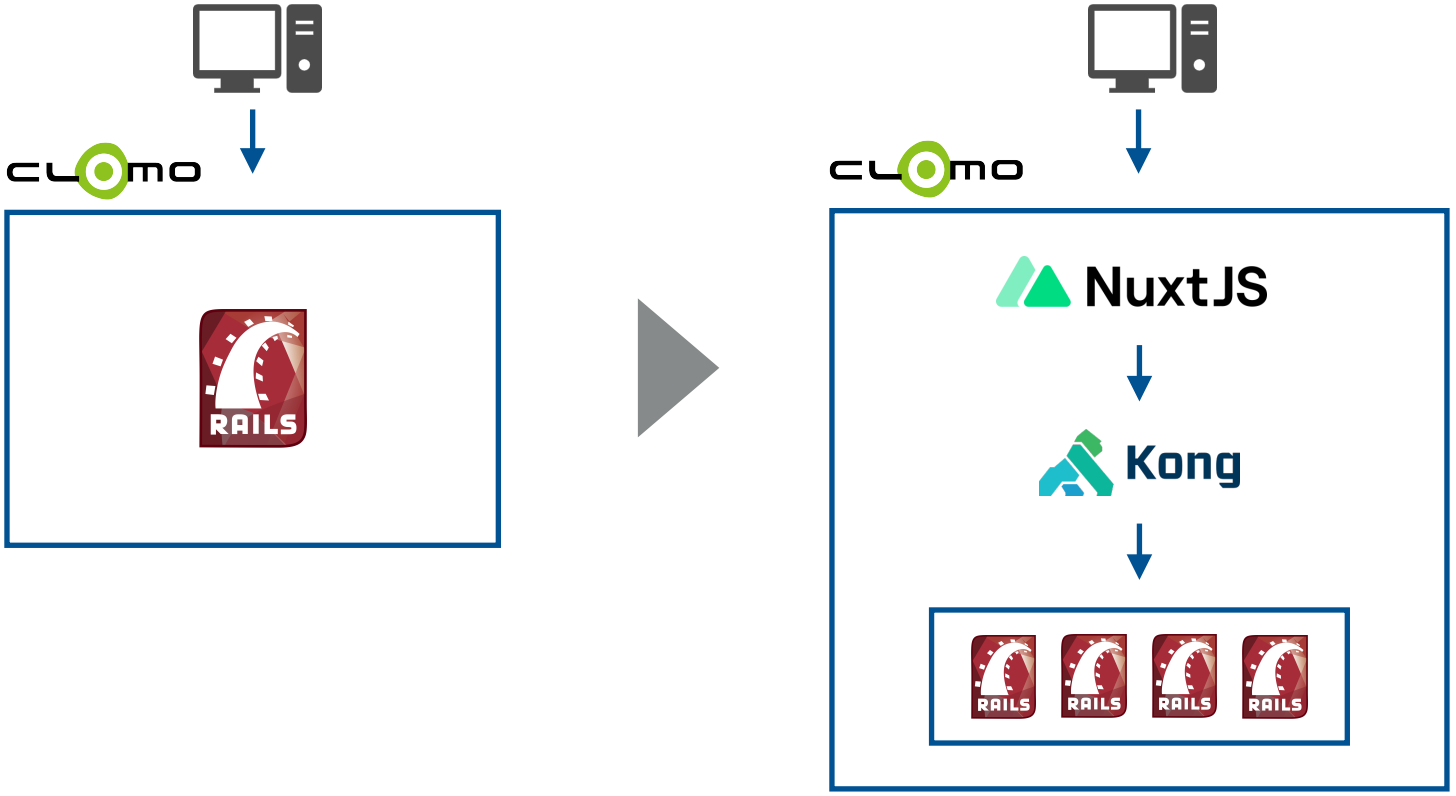
CLOMO PANEL の高速化

- MongoDBによるデバイス一覧用データ作成機構の追加
- デバイス一覧画面・詳細検索・デバイス情報エクスポート（現在も進行中）



CLOMO PANEL 内部アーキテクチャの進化

- Ruby on Rails単一のアーキテクチャから
  フロントエンドにNuxt.jsを使用したモダンな構成へ
- バックエンドもKubernetesと親和性のあるマイクロサービスアーキテクチャにより
  再構成（現在も進行中）



3. 監視とセキュリティの取り組み

CLOMO システムの運用・監視

- 24/365 有人監視

システム負荷アラートチェック

平日・定時：プラットフォーム部
休日・夜間：外部パートナー → プラットフォーム部

CLOMO 機能チェック

お客様の利用を想定した動作正常性確認

- アプリケーションインストール・削除
- VPPライセンス付与・剥奪
- プロファイル自動適用・解除　など

外部ベンダーAPIの正常性確認

- Apple DEP API / VPP API
- Google EMM API　など

ブラウザオートメーションを利用した監視の充実

実際のブラウザ動作によるサービス正常性チェックを実施

- ログイン等のブラウザ操作を伴うサービス正常性チェックを実施
- ブラウザでJavaScriptまで動作した上でのページ内容のチェック（改ざん検知など）
- 弊社のエンジニアが個人OSS活動にて開発したライブラリ「puppeteer-ruby」を活用

第三者機関によるセキュリティ診断

Webアプリケーション診断・
プラットフォーム診断を実施

- CLOMOのアプリケーション・システムに脆弱性が存在していないか、第三者機関により定期的に診断

内部のセキュリティへの取り組み

人の手で行う取り組みも確実に実施

- JPCERT/CCによる最新の脆弱性情報を確認
- Azure等の運用サービス・サーバーの
  監査ログの定期確認
- サービス運用アカウント・権限設定の定期確認
- 既定のフローに従い全ての作業を記録

4. まとめ

安心して CLOMO を利用していただくために

より柔軟に、より迅速に、より安全に

CLOMO プラットフォームは
止まらない、止まらせない。

これからも CLOMO をよろしくお願いいたします


CLOMO