NTT DATA
Trusted Global Innovator

デジタルペイメント開発におけるコンテナとSysdigの活用紹介

2021年3月2日

株式会社NTTデータ　技術革新統括本部　システム技術本部 クラウド技術センタ
佐藤 優太

自己紹介

佐藤　優太
Sato, Yuta

NTTデータ　技術革新統括本部　システム技術本部
生産技術部 クラウド技術センタ 主任

現在の業務内容

- デジタルペイメント開発室のSRE（Site Reliability Engineer）
- ハイブリッドクラウド基盤の設計構築

専門領域

- Kubernetesでのコンテナ基盤構築
- クラウド（AWS, GCP）環境構築・運用

デジタルペイメント開発室の紹介

NTT DATA

カード&ペイメント事業部の紹介

カード＆ペイメント事業部は、CAFISを中心として決済システムを提供している
代表となるCAFISは1984年から稼働する国内最大規模の決済ネットワークである

参考URL https://solution.cafis.jp/

課題感

デジタル化

- レガシーシステムが多く新たな技術が取り入れられない
- 従来の開発プロセスではサービス化にスピード感がない

ビジネス変革

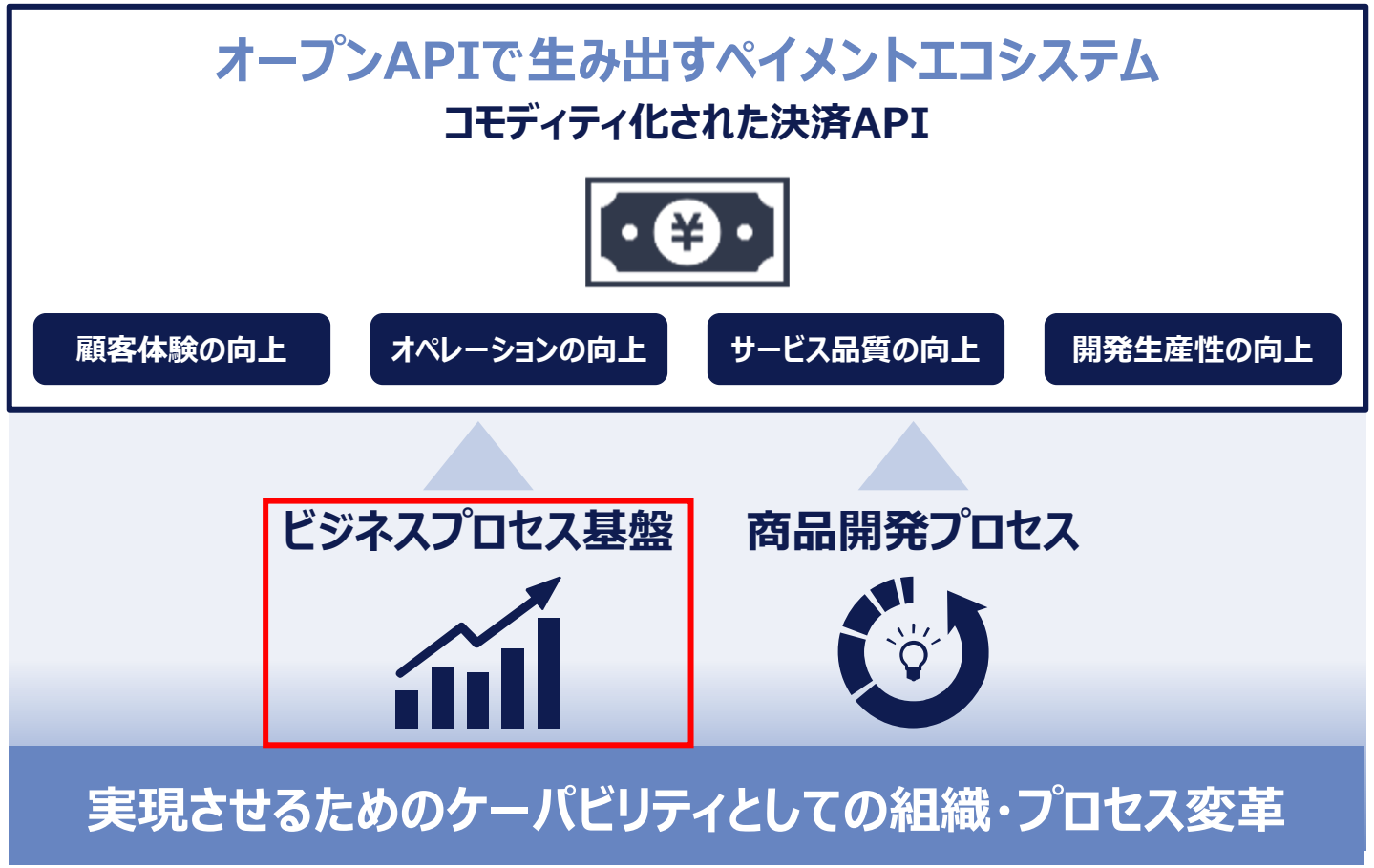
- 新しいビジネスが生まれない
- 顧客体験の向上が達成できない

セキュリティ

- セキュリティは高度化しており、セグメント化する従来方式では担保が困難
- ゼロトラストセキュリティへの切り替えが必要な状況

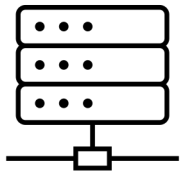
デジタルCAFIS ～デジタルペイメント開発室での取り組み～

デジタルCAFISはビジネスモデルを変革するデジタル商品とそれを実現するための施策として
価値創造、**サービス提供**、**事業運営プロセス**、**商品開発プロセス**にて構成される複合施策である。
ビジネスモデル、顧客体験、組織内部をそれぞれ変革しデジタルトランスフォーメーションを達成する。

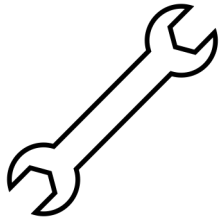


ビジネスプロセス基盤（Digital Platform）

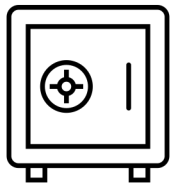
組織のデジタルトランスフォーメーションのために必要な基盤を整備する。
アジリティと決済APIのための安定した基盤とセキュリティを両立させる。



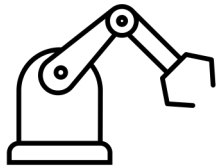
ITインフラ



マネジメントツール



セキュリティ



CI/CD

アジェンダ

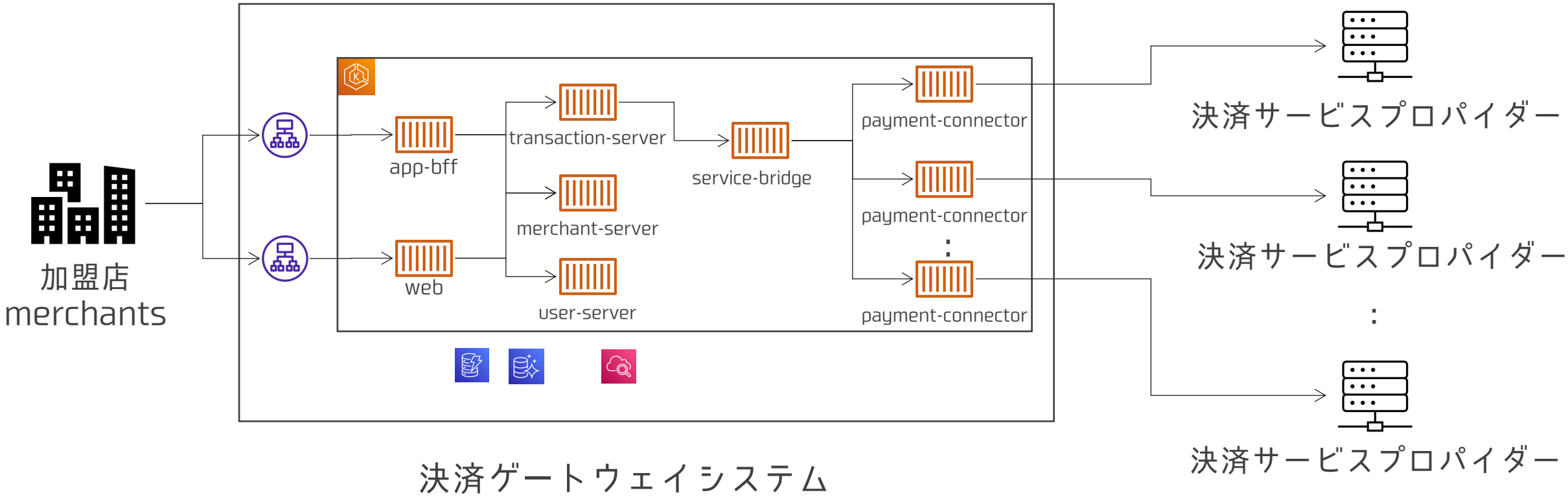
- ペイメントエコシステム
- Monitoring
- Security

デジタルペイメント開発における取り組み

NTT DATA

ペイメントエコシステム　～決済ゲートウェイ～

加盟店様は多様な決済手段に対応して販売機会の損失を減少できるようになるとともに、
お客様はより多くの店舗でより利便性の高い決済手段を選択して利用できるようになります

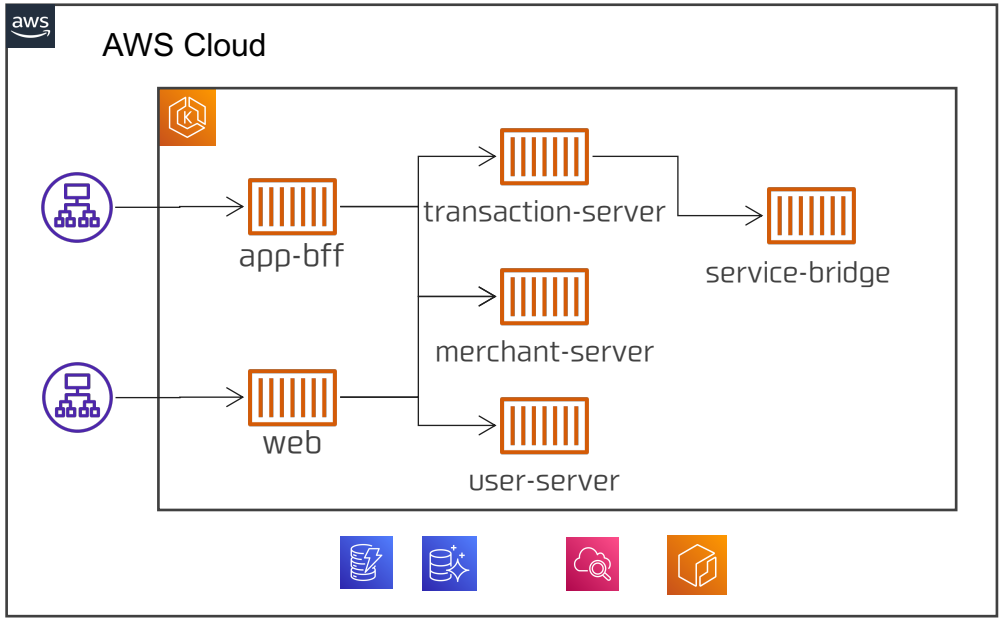


※本図は決済ゲートウェイサービズに関して示したものであり、CAFISはクラウド上で動作していません

ペイメントエコシステムを支えるテクノロジー

Cloudベース、Microservice architectureの技術を使って開発のスピード感を向上させる

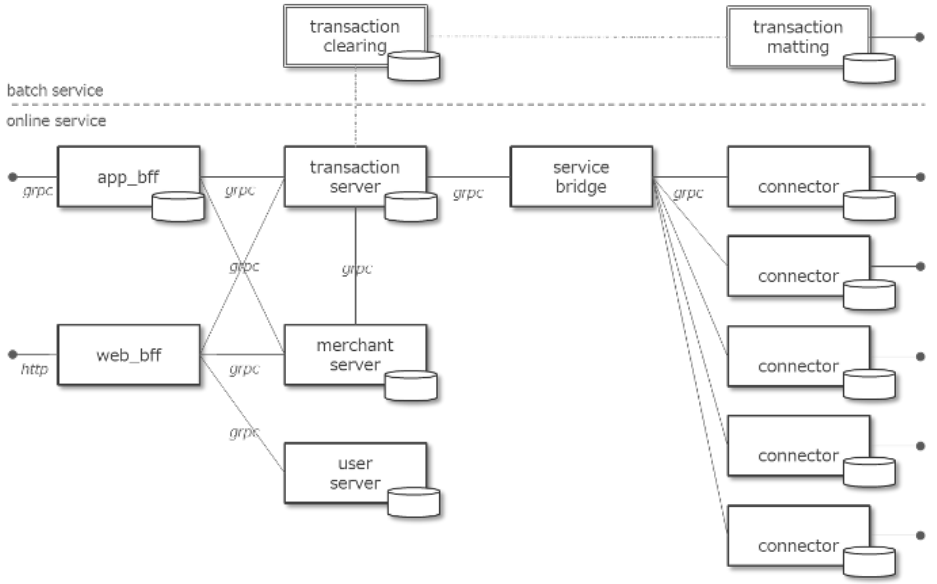
Cloud technologies



パブリッククラウド

コミュニティクラウド

Microservices Architecture



Go

Java

kubernetes

※本図は決済ゲートウェイサービスに関して示したものであり、CAFISはクラウド上で動作していません

インテグレーションにおける重点事項

■ Agility	スピード感のあるサービス提供 CI/CD, IaC
■ Availability	可用性を確保するためのシステム設計と モニタリング機構
■ Consistency	ハイブリッドクラウドを見据えての Kubernetesを中心としたインフラ環境
■ Security	決済インフラとしての高いセキュリティ要件

Agility

開発アジリティ向上のため、プロセスとインフラの両面で施策を実施

開発プロセス・組織運営

- Scaled Agile Framework (SAFe) による大規模アジャイルの実践
- マイクロサービスによる並行開発

CI/CD・IaC

- アプリケーション自動ビルド・自動テスト
- Git-OpsによるKubernetesへのデプロイ自動化
- SREチームにて標準となるterraform moduleを作成してインフラ設計・構築を高速化

マネジメントツール

- コミュニケーションツール
- インシデント管理ツール
- 構成管理ツール

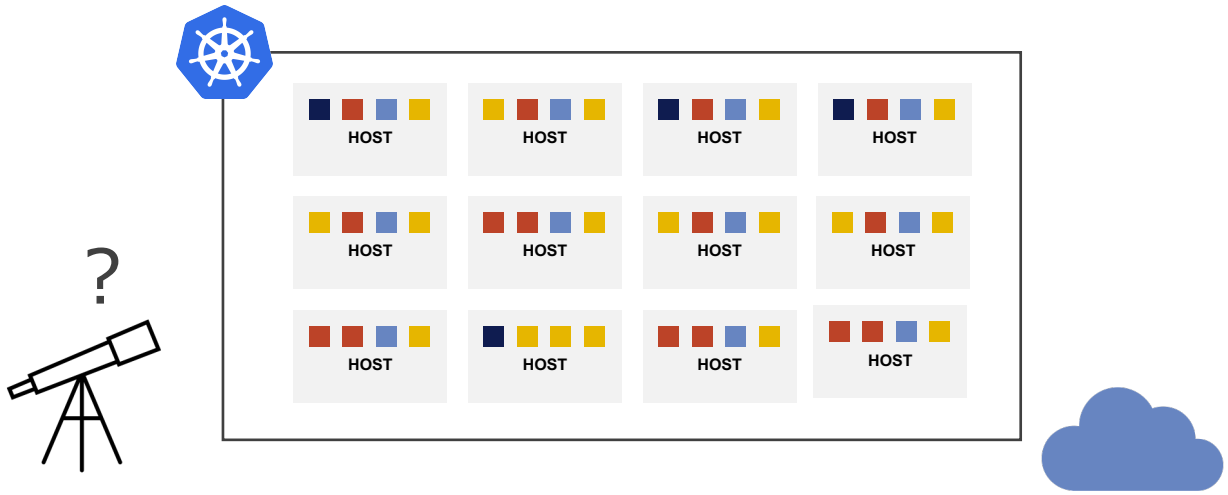
Availability & Consistency

Kubernetes

- コンテナの可搬性の特徴を活かして環境を問わず一貫したデプロイが可能
- Kubernetesのオートヒーリング機能により安定したアプリケーション実行が可能

Monitoring

- 従来の監視方法ではコンテナの挙動を追跡することが困難なため新たな方式が必要となる
- 複数のKubernetesクラスタで一貫したMonitoringを行いたい



Security

脆弱性対応・ベンチマーク

- ビルドしたコンテナイメージやランタイム中のコンテナの検疫が必要
- Kubernetes Benchmarkの実行とレポート作成

フォレンジック

- コンテナ内のアクティビティ追跡手段が必要

セキュリティ基準(PCI-DSS)への対応

- 業界標準のセキュリティ基準・監査要件への対応が必要

モニタリング＆セキュリティにおける課題

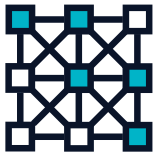
開発アジリティ向上のため大規模アジャイルとマイクロサービスにより並行開発を行う一方で、
コンテナやKubernetesに関して技術的な課題が発生しています。

コンテナ

Go, Node.js, Javaなど様々なタイプのコンテナが動作しています。コンテナはエフェメラルであり問題が発生したコンテナはすでに消え去っています。

アプリケーションに依存しない
モニタリング方法が必要

マイクロサービス



学習コストの高いKubernetesのスキルレベルは担当者により異なります。
複雑度が高く、故障解析には多くの情報が必要です。

Kubernetesのスキルに依存しない
管理の仕組みが必要

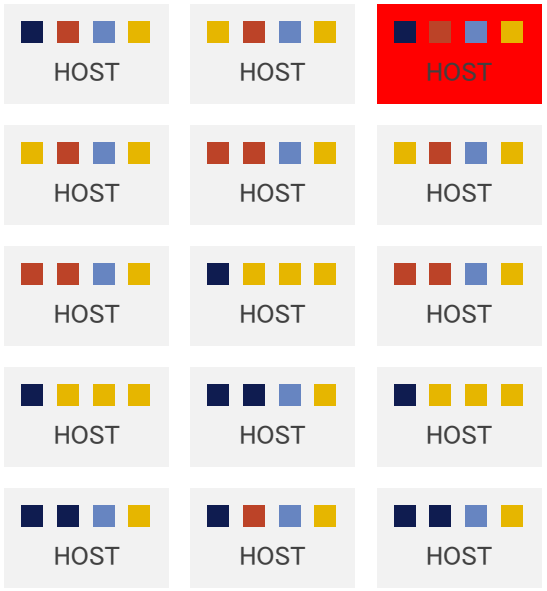
マルチクラウド

異なるクラウドにおいても統一的なモニタリングとセキュリティー確保で統制が必要です。

決済セキュリティの確保と
統一的なダッシュボードが必要

モニタリング課題の例

Kubernetesでのトラブルシュートをできる人が限られ、情報収集にも時間を要する



外形監視、コンテナログ、限定的なメトリクスから
影響範囲と原因を究明するには時間がかかる

```
$ kubectl get pod
NAME                              READY STATUS RESTARTS AGE
details-v1-5974b67c8-qpptg        2/2   Running 0        57m
productpage-v1-64794f5db4-5z25g 2/2   Running 0        57m
ratings-v1-c6cdf8d98-hfqvk        2/2   Running 1        11h
reviews-v1-7f6558b974-wh69t       2/2   Running 0        57m
reviews-v2-6cb6ccd848-j6ckf       2/2   Running 0        57m
reviews-v3-cc56b578-d7fs6         2/2   Running 0        11h

$ kubectl describe pod
...
```

モニタリング＆セキュリティプラットフォームとしてのSysdig

☑ コンテナ環境の真のモニタリング＆セキュリティプラットフォーム

- Wiresharkの創作者によって開発
- OSのシステムコールを可視化する特許技術により、コンテナ内部やコンテナ間の通信状況を完全にモニタリング/視覚化
- コンテナに潜む脆弱性の発見や、不正アクセス・サイバー攻撃などの異常検知、コマンドの実行履歴をすべて記録

➡ フルフォレンジックによるトラブルシューティングを実現

Sysdig活用方針

❶ kubernetesスキルに依存せず、
障害復旧を早く行える仕組みを整備する

❷ コンテナ環境のセキュリティ対応を行う

モニタリング課題

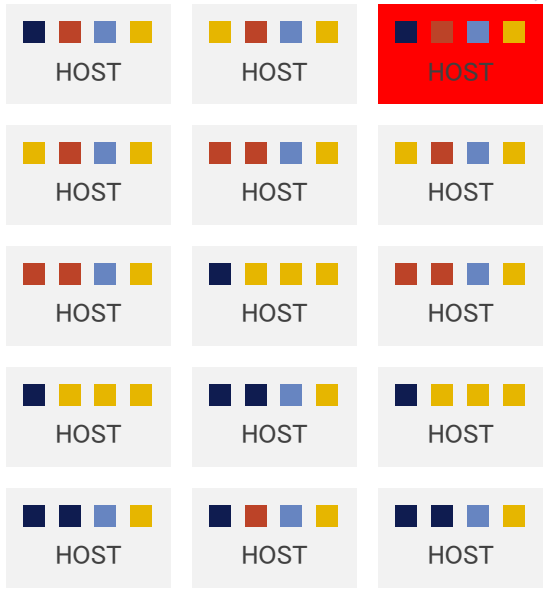
Kubernetesでのトラブルシュートをできる人が限られ、情報収集にも時間を要する

課題

- 大量のログから故障のレイヤーの判別が瞬時にできない
- ログ基盤は大量ログ発生時に遅延が発生する
- Kubernetes内部の解析ができるひと人が限られる

Sysdigによるモニタリング課題への対応

Sysdigに情報を集約し、チーム単位のダッシュボードやビューを活用して情報収集の初動を高速化



sysdig

チーム単位のダッシュボード

トポロジーマップで影響範囲、
コンテナの相互関係を確認

Explorer機能でメトリクスを
様々な切り口で確認

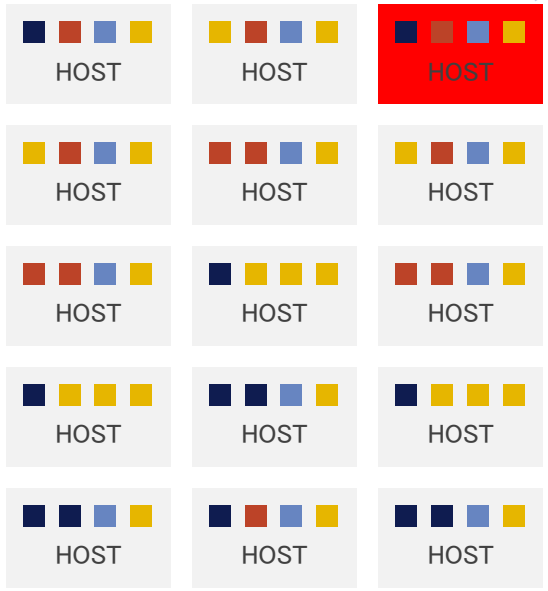
オンコールのインシデント管理システムや
チャットとネイティブに連携

NTT DATA

Sysdigとチャット・オンコール連携

チャットシステムやオンコールシステムともネイティブに連携でき、
故障に迅速に対応できる組織づくりに繋がる

ノード/コンテナ
で故障が発生



sysdig

チャットツール

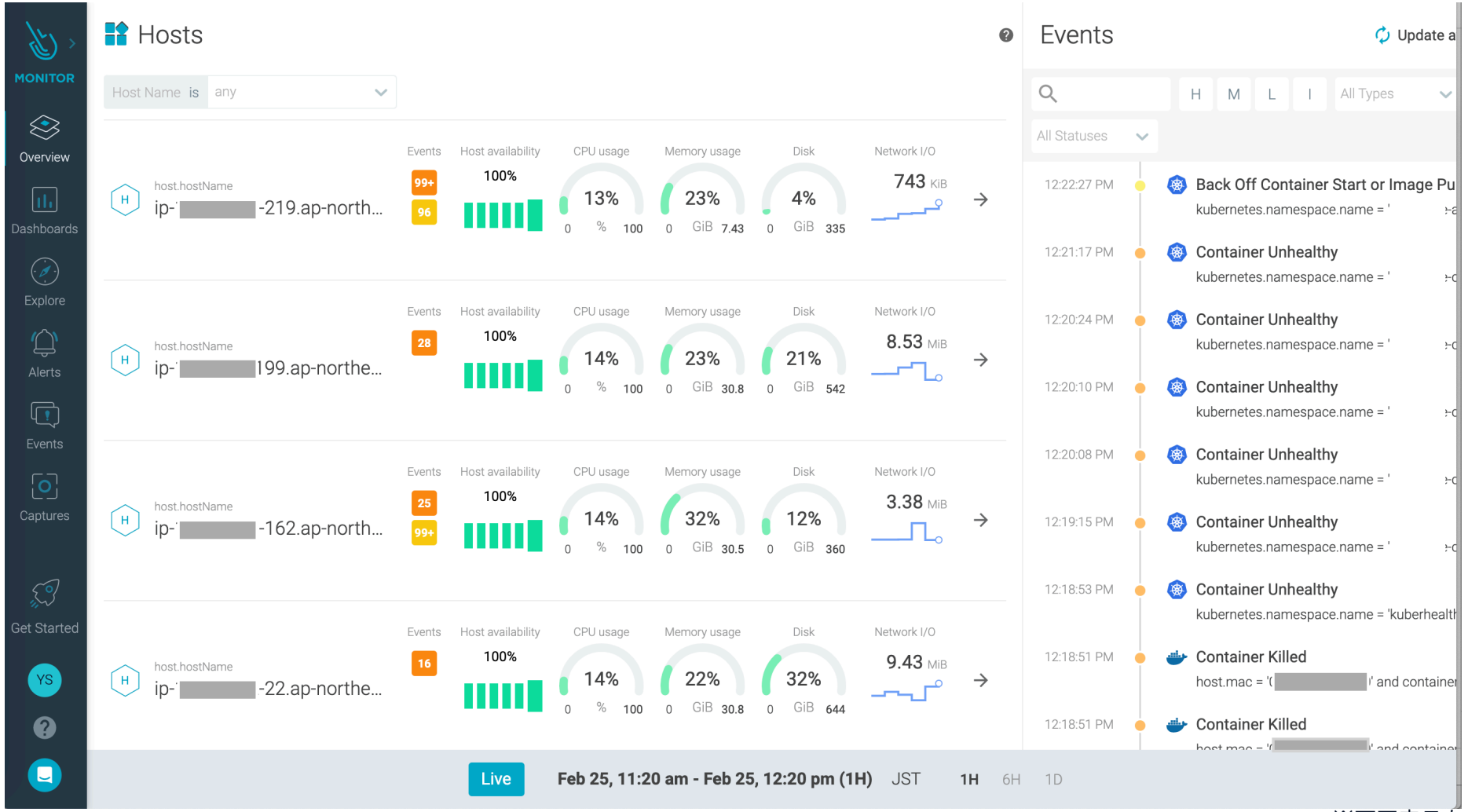
Pagerduty

オンコール

NTT DATA

Sysdig Monitor活用 ～Overview～

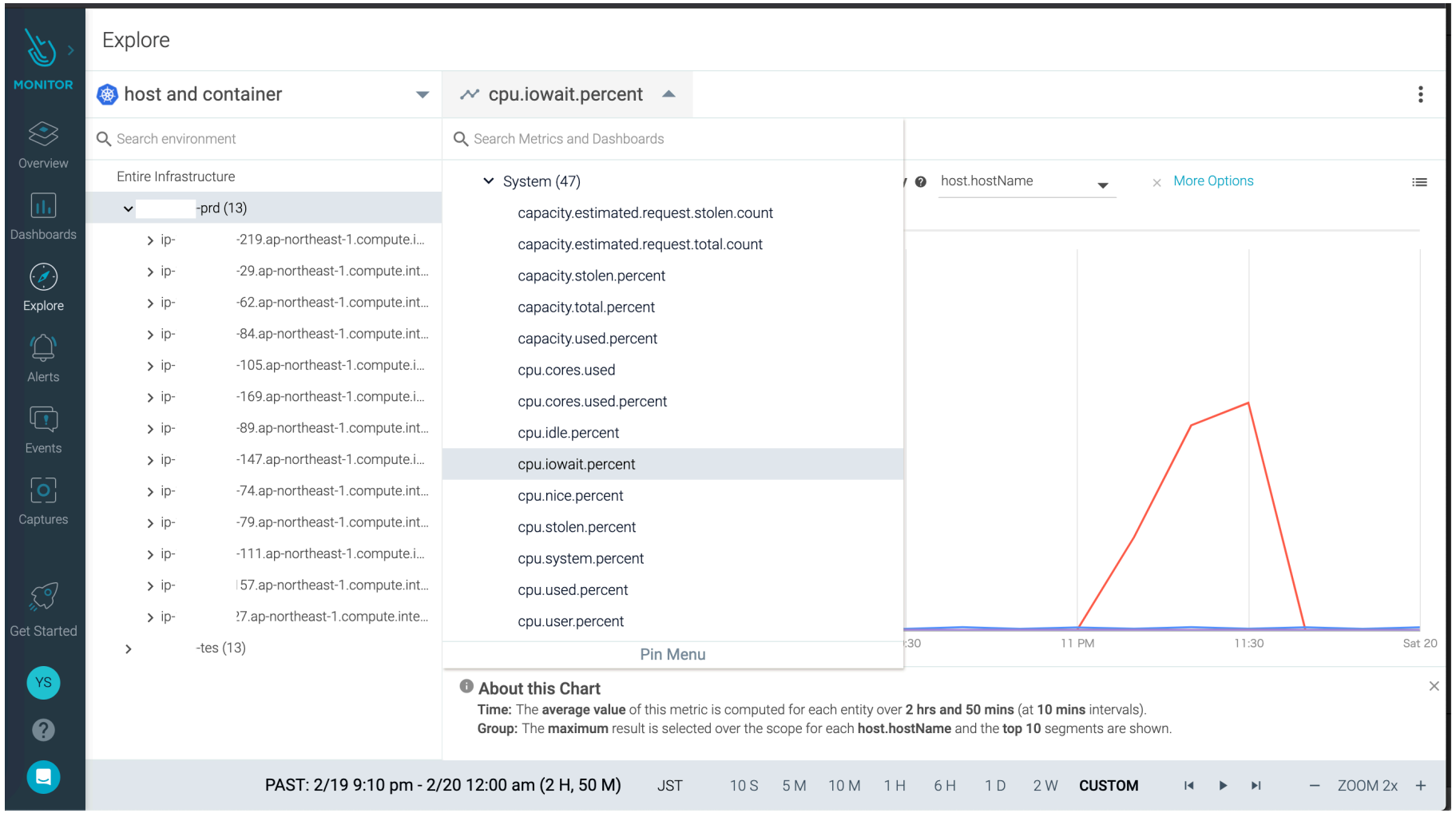
Overviewページでホストとコンテナイベントの概況を確認できる



※画面表示を一部マスクしています

Sysdig Monitor活用 ～Explorer～

Explorer機能でメトリクスを個別に確認して原因を調査できる
必要に応じてSystem callのCaptureと解析がWeb UIからできる



※画面表示を一部マスクしています

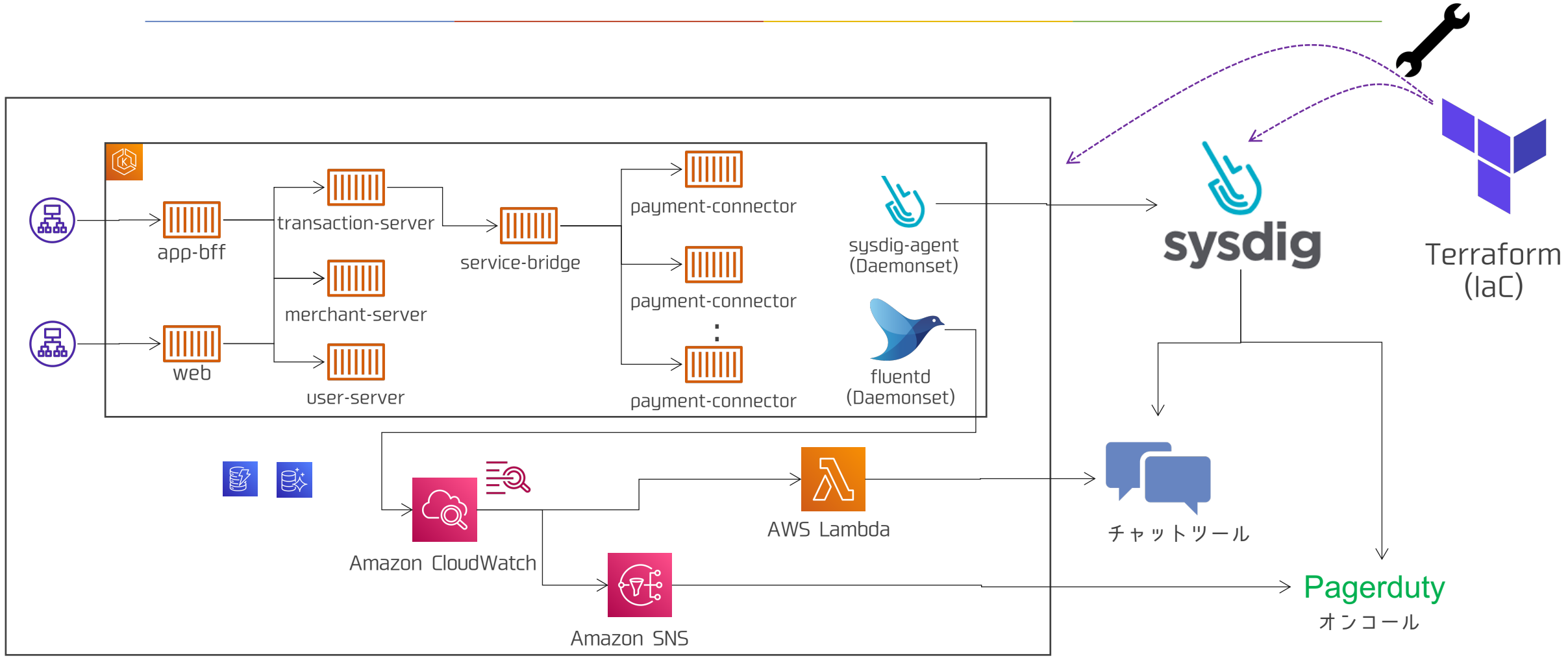
Sysdig Monitor 活用の取り組み

❶ kubernetesスキルに依存せず、障害復旧を早く行える仕組みを整備する

課題	Sysdig活用の取り組み
組織作り SREチームだけでなく、SOC/CSIRTチーム、アプリケーションチームもKubernetesのトラブルシュートが出来る組織作り	PromQL互換のダッシュボードを使用したMicroservice & Application モニタリング
システムの可視化 障害の予知・通知、トラブルシューティング、性能予兆検知、性能試験結果の解析、リソース最適化	システムダッシュボード、Kubernetes健全性およびパフォーマンスモニタリング アラーティングとオンコールシステムとの連携 異常時のシステムメタデータ（ネットワーク、システムコール）のキャプチャ リソース過不足の特定とリソース最適化 トポロジービューによるサービスの相互作用の把握

モニタリング全体像

Sysdigのアラート設定、AWS設定はterraformによるIaC管理を実施



※1 図は抜粋して表記しています
※2 本図は決済ゲートウェイシステムに関して示したものであり、CAFISはクラウド上で動作していません

【再掲】Security

脆弱性対応・ベンチマーク

- ビルドしたコンテナイメージやランタイム中のコンテナの検疫が必要
- Kubernetes Benchmarkの実行と

フォレンジック

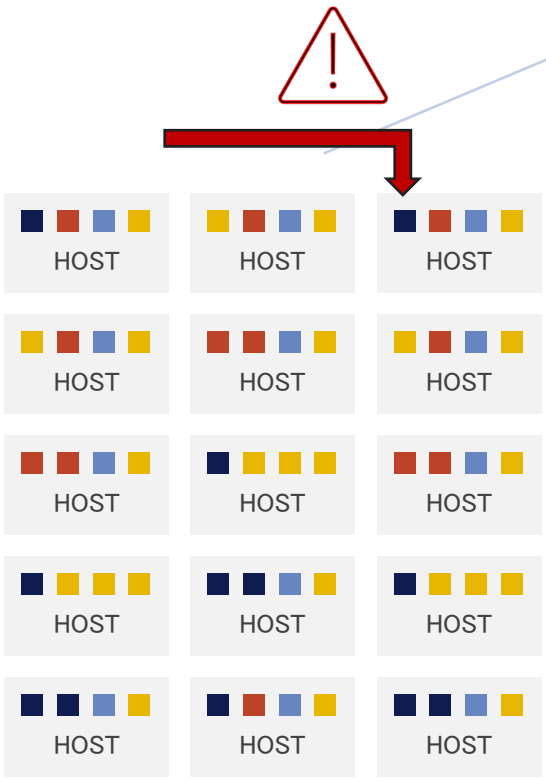
- コンテナ内のアクティビティ追跡手段が必要

セキュリティ基準(PCI-DSS)への対応

- 業界標準のセキュリティ基準・監査要件への対応が必要

Security課題の例

KubernetesのPod内への不正アクセスが発生した際に、
どのようなアクティビティが行われたかのフォレンジックが困難である



コンテナでの不正な
アクティビティが発生

課題

- Kubernetes audit loggingからAPI実行履歴は確認できるが、コンテナ内で何が行われたかの確認ができない
- kubectl logsではPID 1プロセスの標準出力ログしか確認できない
- アプリログが出力されずKubernetes API 実行もない場合に検知する方法が無い

SysdigによるSecurity課題への対応

Image ScanとRuntime Policyでインフラを保護
Activity Audit Logによりフォレンジック用のログを収集

Container Registry & Runtime Container Imageのスキャン

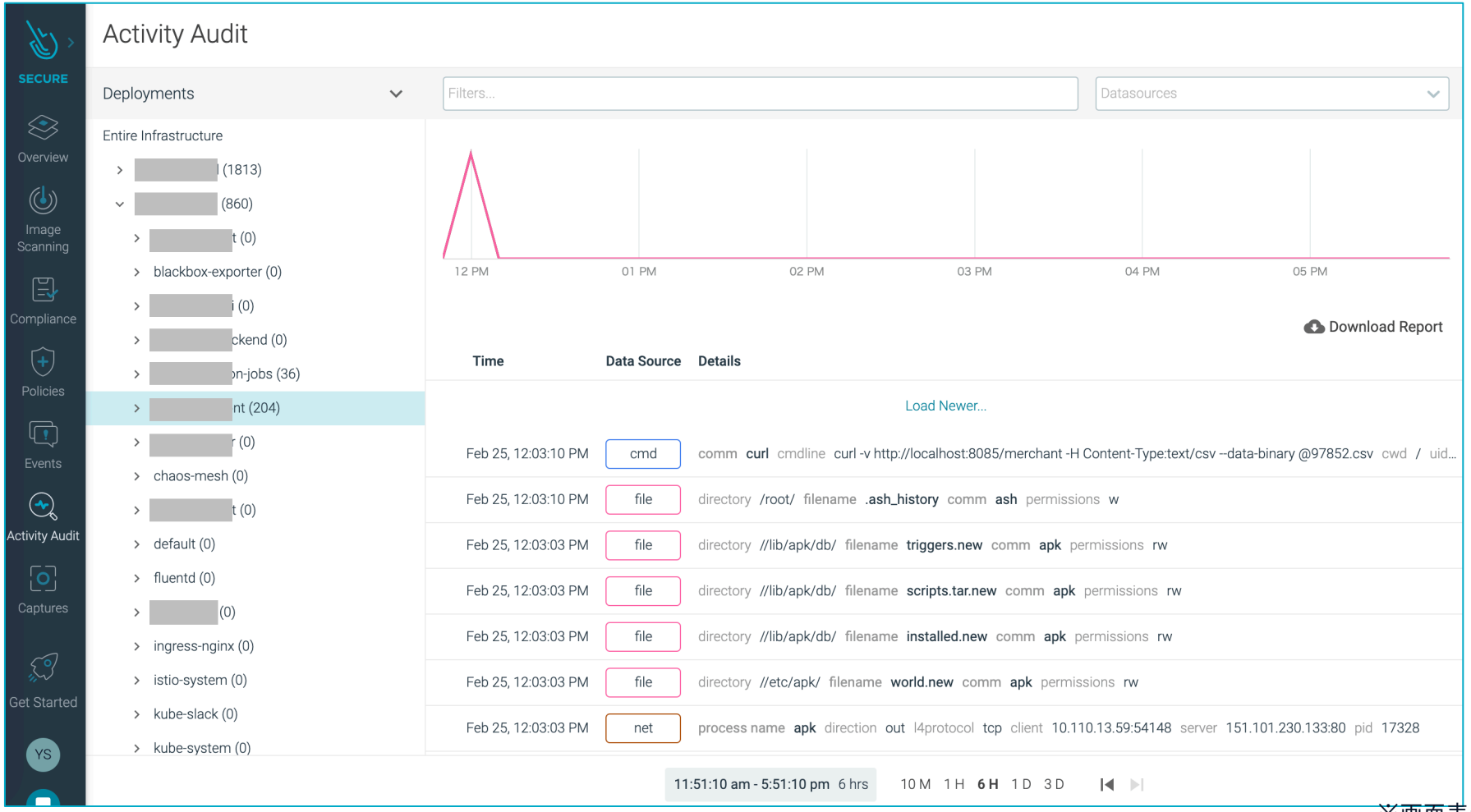
Falco RuleでのPolicy逸脱の検出

Activity Audit Log によるフォレンジック用データの取集

PCI-DSSのコンプライアンスReportの生成

Sysdig Secure活用 ～Activity Audit Log～

コンテナ内でのコマンド実行履歴やファイル変更履歴といったActicity
の収集によりフォレンジックが行えるようになる



※画面表示を一部マスクしています

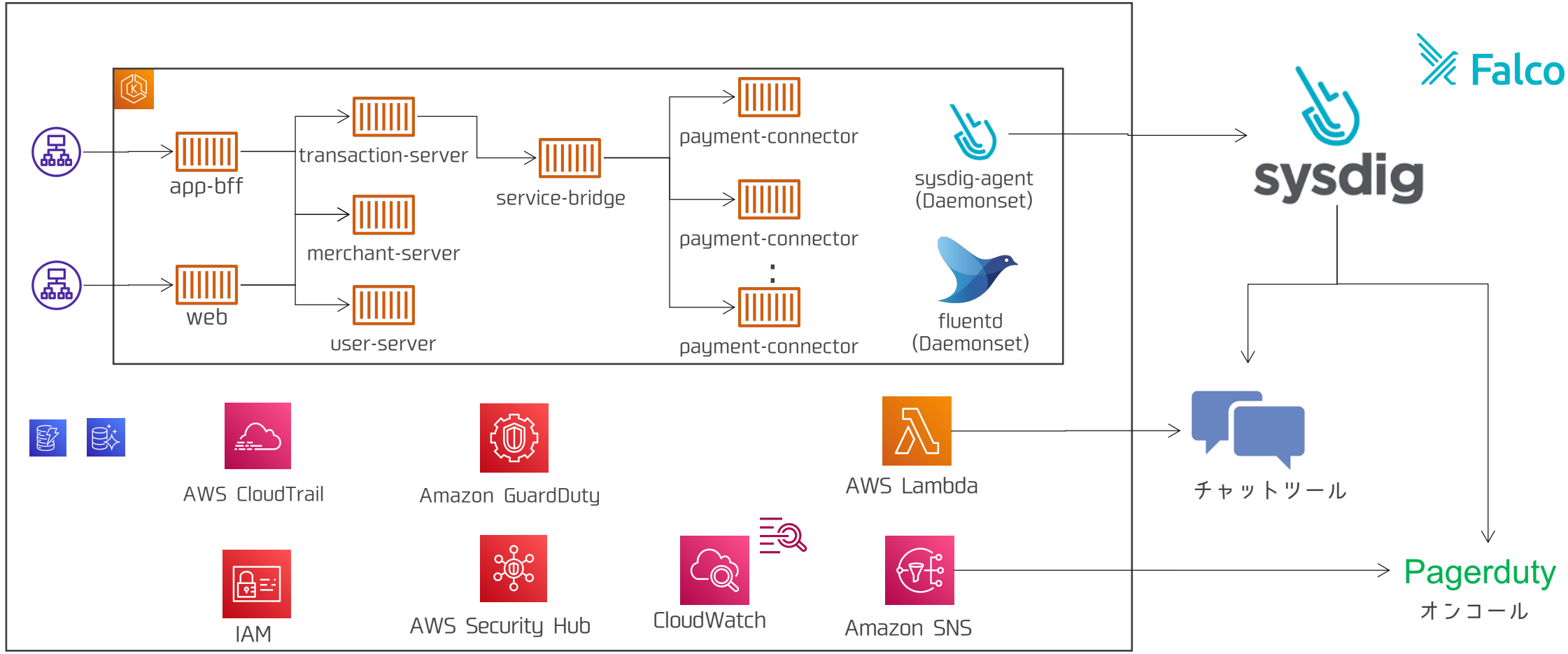
Sysdig Secure活用の取り組み

❷ コンテナ環境のセキュリティ対応を行う

課題	Sysdig活用の取り組み
プロアクティブなユースケース • コンテナイメージの脆弱性スキャン • セキュリティコンプライアンスチェック	CI/CDパイプライン・レジストリと連動したイメージスキャン ランタイムイメージのスキャン
リアクティブなユースケース • コンテナへのセキュリティ侵害検知 • セキュリティ侵害のフォレンジック	Kubernetes Benchmarkによるセキュリティコンプライアンスチェック Falcoを活用したコンテナランタイム脅威の検出
セキュリティ基準(PCI-DSS)への対応 • PCI-DSS準拠のセキュリティイベント対応・監査ログ取得、インシデント対処	Activity Auditを活用した、コマンド、ファイルI/O、ネットワークアクティビティ、Kubernetes実行ログを含む完全なアクティビティのキャプチャ SIEMプラットフォームおよび通知システムとの統合

Security 全体像

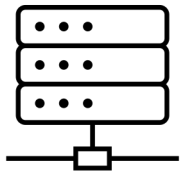
クラウド基盤とコンテナ実行環境のセキュリティを保護



※1 図は抜粋して表記しています
※2 本図は決済ゲートウェイサービスに関して示したものであり、CAFISはクラウド上で動作していません

まとめ

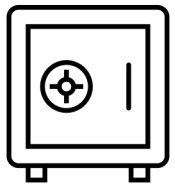
アジリティと決済APIのための安定した基盤とセキュリティを両立させる
コンテナ環境のモニタリングとセキュリティにSysdig Platformを活用



ITインフラ

ダッシュボードを活用して情報収集を高速化

詳細なデータ収集と分析



セキュリティ

脆弱性スキャンとポリシー逸脱の検出

フォレンジック用データの取集

商標について

本資料に記載されている会社名、商品名、又はサービス名は、各社の登録商標又は商標です。

本資料に記載されている情報は2021年3月1日時点のものです。

NTT DATA

Trusted Global Innovator