

JIG-SAW

2025

JIG-SAW **OP5**

⋮

JIG-SAW株式会社  
アカウントマネジメント本部  
岡田龍征  
Mail : ryusei.okada@jp.jig-saw.com  
Tell : 070-1417-3505

JIGSAW

# 会社概要

## 社名

JIG-SAW株式会社

## ISMS認証

IR0038

(ISO/IEC27001:2013,JIS Q 27001:2014)

## 設立

2001年11月1日

## 上場市場

東京証券取引所グロース

(証券コード3914)

## 本社

東京都中央区八重洲二丁目2番1号

東京ミッドタウン八重洲 八重洲セントラルタワー 33階

## 本店

北海道札幌市北区北8条西3丁目32

## 海外拠点

JIG-SAW US, INC.(米国サンフランシスコ・サンタモニカ)

JIG-SAW CA, INC.(カナダ・トロント)



# JIG-SAW OPSとは

## モニタリング



24時間365日の自動モニタリング、最適なモニタリングの設計、設定を支援しシステムの異常、予兆、停止を正確に検知します。

## 最適化支援



システムの安定稼働、パフォーマンスの最適化や冗長化、可用性の向上等システムの課題に合わせた支援を行います。

## インシデント 対応



インフラのプロフェッショナルエンジニアによるインシデント対応を提供、必要に応じて問題の根本原因を突き止め解決策を提示します。

## 構築支援



オンプレミス、クラウド問わずプロフェッショナルエンジニアによるベストプラクティスな設計を提案、環境構築まで支援します。

# JIG-SAW OPSサポート範囲(一部)



# サービス 提供範囲

## システムを包括的に支援

システムの設計から構築、本番稼働後の運用はもちろんのこと、コストやシステムの最適化、セキュリティ対策、技術的なサポートまで包括的に支援します。



### マネージドサービス

オンプレミス、クラウド問わず環境の最適化、標準化を支援しシステムの安定稼働とコストの最適化、運用負荷を無くします。



### セキュリティ

脆弱性の診断から脅威の検知、保護や防御等、お客様の課題に合わせた最適な解決ソリューションを提案します。



### クラウド構築

クラウドエンジニアによるベストプラクティスに則った最適な設計を提案、稼働後の運用まで考えられた環境を構築し引き渡します。



### クラウド請求代行

日本円建て請求書払いを手数料無料、6%割引からご提供。お客様のクラウド環境のコスト削減を支援します。

# 監視体制

弊社にお任せいただくことで、監視運用の質の向上や万全なセキュリティを確保したセンターからのサポートが実現できます。

## グローバルな2拠点の監視センター

- SCC（札幌コントロールセンター）  
専任のサーバエンジニアが常駐する**国内最大級**の監視センター
- TCC（トロントコントロールセンター）  
時差12時間のトロント拠点で**夜間帯**の業務依頼も安心対応



## 監視センター内 セキュリティ

- すべての作業が見える位置に**監視カメラ**を設置
- カードキーによる**入退出管理**
- **個人ロッカー**を設置し、センターへの私物持ち込みを禁止
- USBメモリ等の**外部媒体利用禁止**

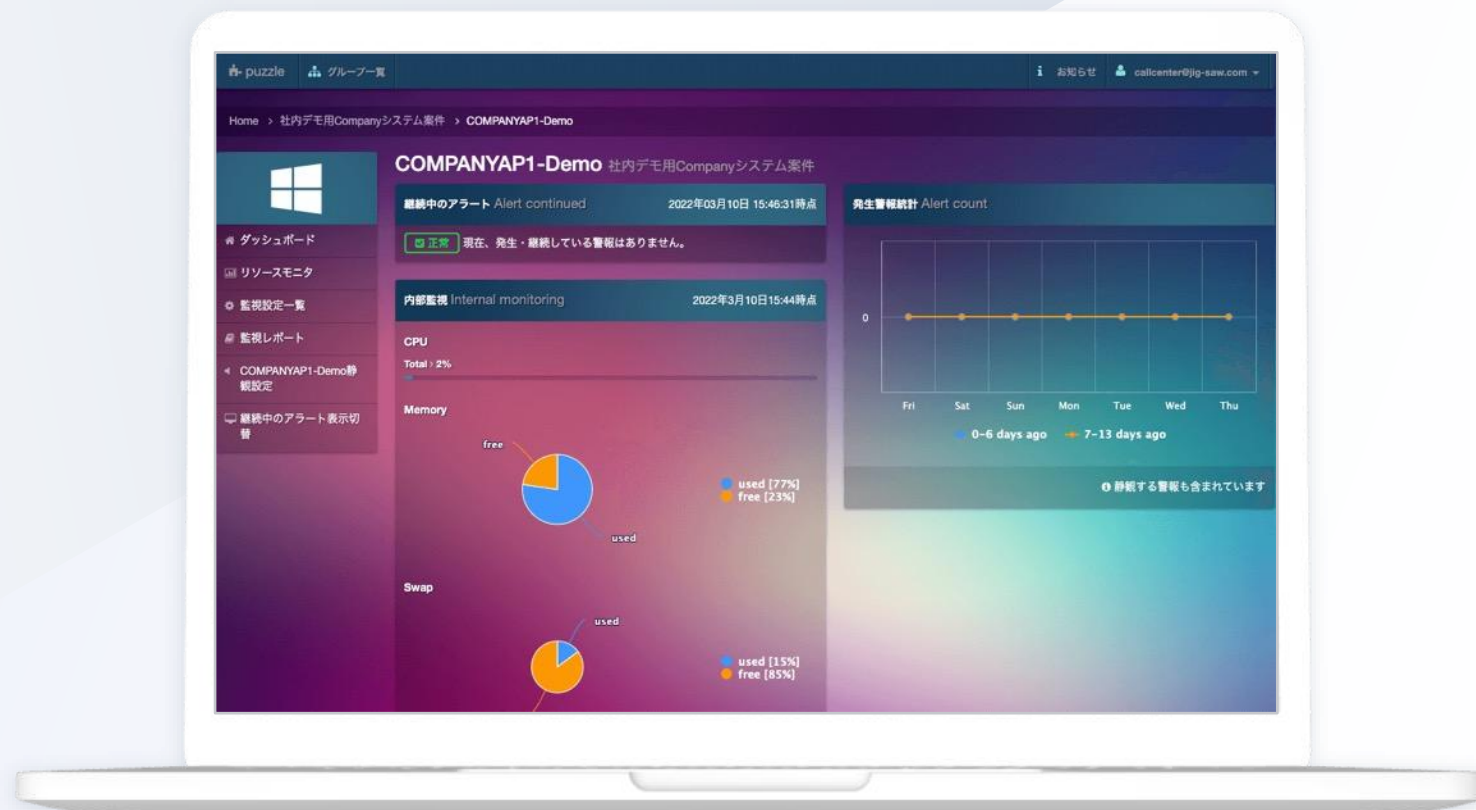
# データコントロールセンター



# puzzle

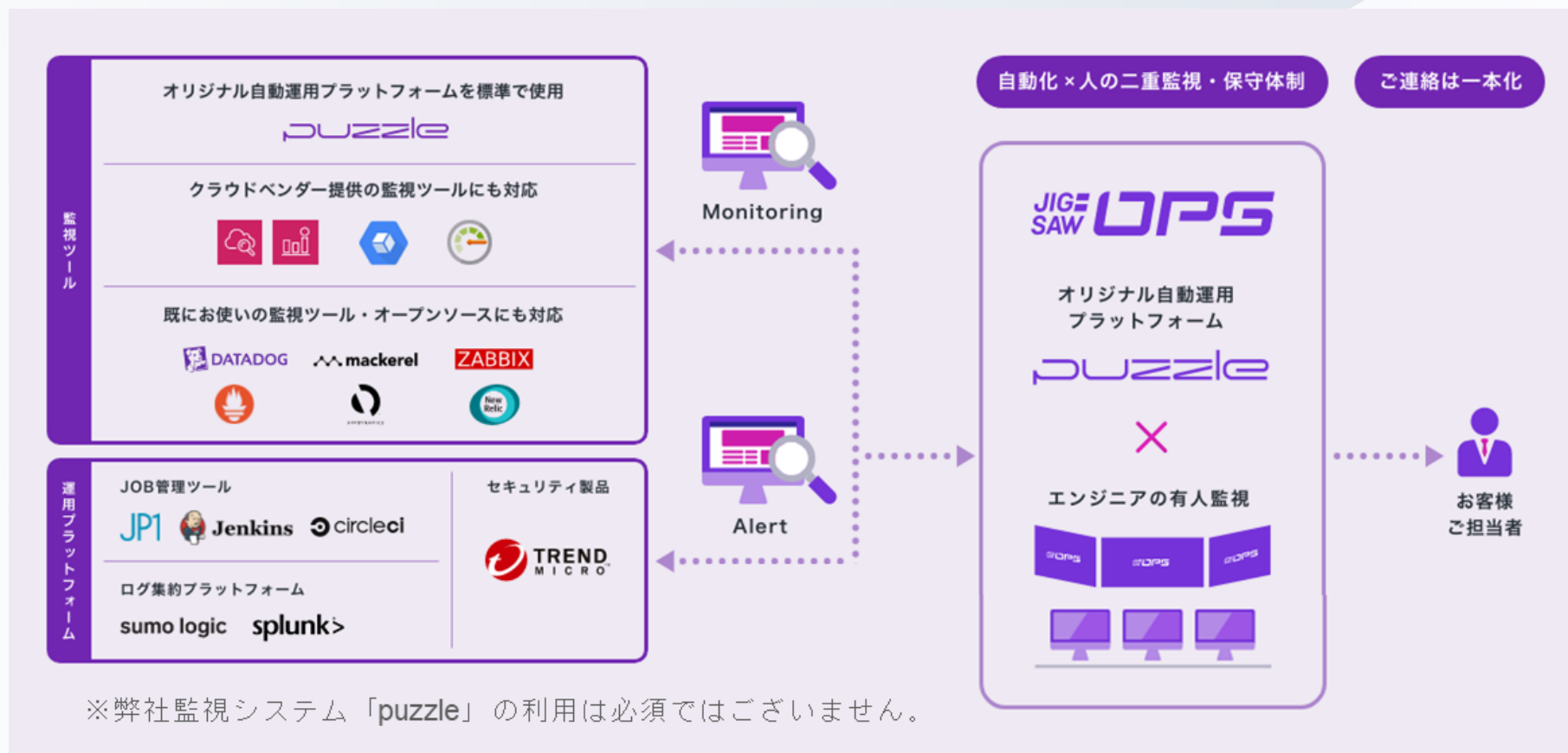
## データ・コントロール プラットフォーム

Puzzleは自社開発の運用プラットフォームです。  
検知・取得する膨大なビッグデータの動き・揺らぎを検知するだけでなく、優先順位の判断、指示までのすべてを自動で実現しています。



# 監視イメージ / 対応監視システム

既にお客様がご利用中の各種運用プラットフォームや監視ツールも、そのままご利用いただくことが可能です。各種ツールやサービスからのアラートをJIG-SAW OPSが全て吸収することで、お客様へのご連絡は一本化されます。



# JIG-SAW OPS が解決する課題

## 様々な課題に対応、高品質な運用へ

システム運用のプロフェッショナルである

JIG-SAWではお客様の抱える様々な

システム運用の課題に対応することができます。



1

### 24時間365日の体制が構築できない エンジニア不足

24時間365日エンジニアによる有人のモニタリング体制を提供しエンジニア不足を解消します。



2

### システムのコスト 運用のコストの肥大化

システム稼動状況を見直し、最適化することにより不必要な支出を無くします。またオペレーションを標準化、自動化することによって人的なコストも大幅に削減します。



3

### パフォーマンスや信頼性が 低いシステム

異常、予兆、停止を正確に検知する仕組みを設計し提供、インシデントが発生した際にシステムが抱える問題を分析し根本的な解決策を提案、改善することをパフォーマンスや信頼性を向上します。

# 導入実績企業ロゴ (一部)

TOYOTA

NTT docomo



NTT DATA

子どもたちに誇れるしごとを。  
SHIMIZU CORPORATION  
清水建設

パーソルキャリア  
PERSOL

BANDAI NAMCO

ZENRIN  
DataCom

A D A S T R I A  
Play fashion!

富士急行

cybozu

0TELWANDS

Tabio  
tradition in motion

PARCO DIGITAL MARKETING



Benefit one

PLAZA CREATE

BEING

GDO

人と音楽の新しい関係をデザインする。  
レコチョク

心かよう 夢かなう  
南海国際旅行

Wedding Park

C BIRD

CU サイバー大学  
Cyber University

Forum  
Engineering  
Inc.

もっと素敵な伝え方を。  
Jstream

SHIFT  
SOLVE, EVOLVE then SHIFT.

アルク

# Appendix



# 導入の流れ



## お見積り

運用の要件やシステム環境をヒアリングさせていただきプランとお見積りをご提示いたします。



## ご注文・ご契約

お見積りの内容に合意いただきご注文いただきます。



## 設計/構築/導入

ご契約後弊社エンジニアがシステム設計、運用設計、監視設計を行い構築から導入までを行います。

お客様でご用意の手順書やフローにつきまして受け入れを行います。



## 運用開始

環境の構築が完了し運用フロー、手順、体制の準備が整いましたら24時間365日の運用を開始します。

## ユースケース

# 某大手保険グループ会社

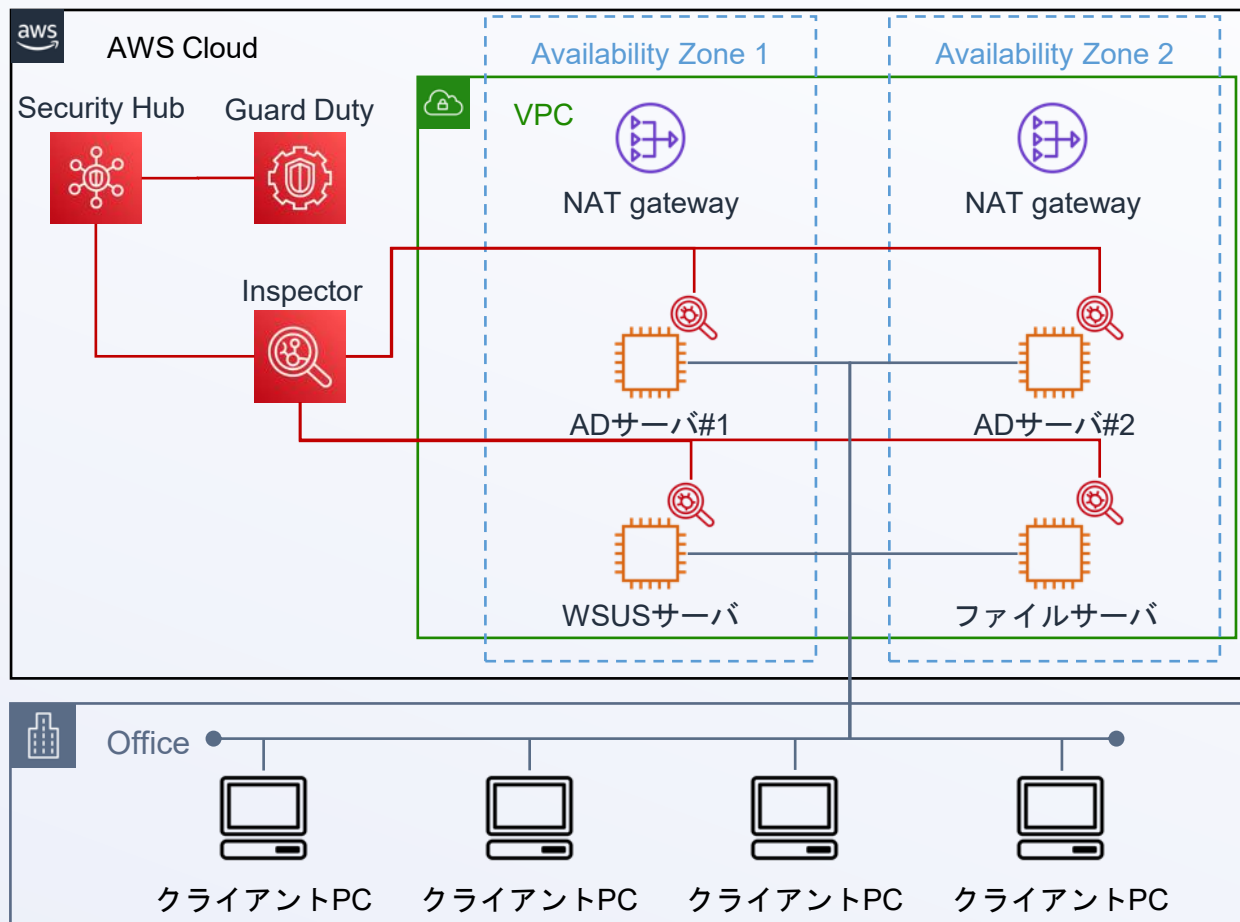
## オフィスLAN環境のクラウド化と運用事例

### 【抱えていた課題】

- ・ オンサイト対応の為、復旧まで時間がかかっていた。
- ・ 過剰なスペックのマシンを使ってコスト負担となっていた。
- ・ WindowsServerのバージョンアップは夜間、休日にオンサイトで対応していた為、対応者の負担が大きかった。

### 【解決/改善】

- ・ クラウド化によりオンサイト対応が不要になった。
- ・ 障害時対応を委託することにより自社での対応が不要になった。
- ・ 構成の提案を受け、高可用性で有りながらも低コスト且つセキュアな環境を実現。
- ・ クライアントPC、WindowsServerのパッチ適用作業を運用委託し自社でのパッチ適用作業が不要になった。
- ・ プラットフォームの定期脆弱診断や脅威や攻撃の検知が可能になった。



## ユースケース

# 某コミックアプリ分析基盤

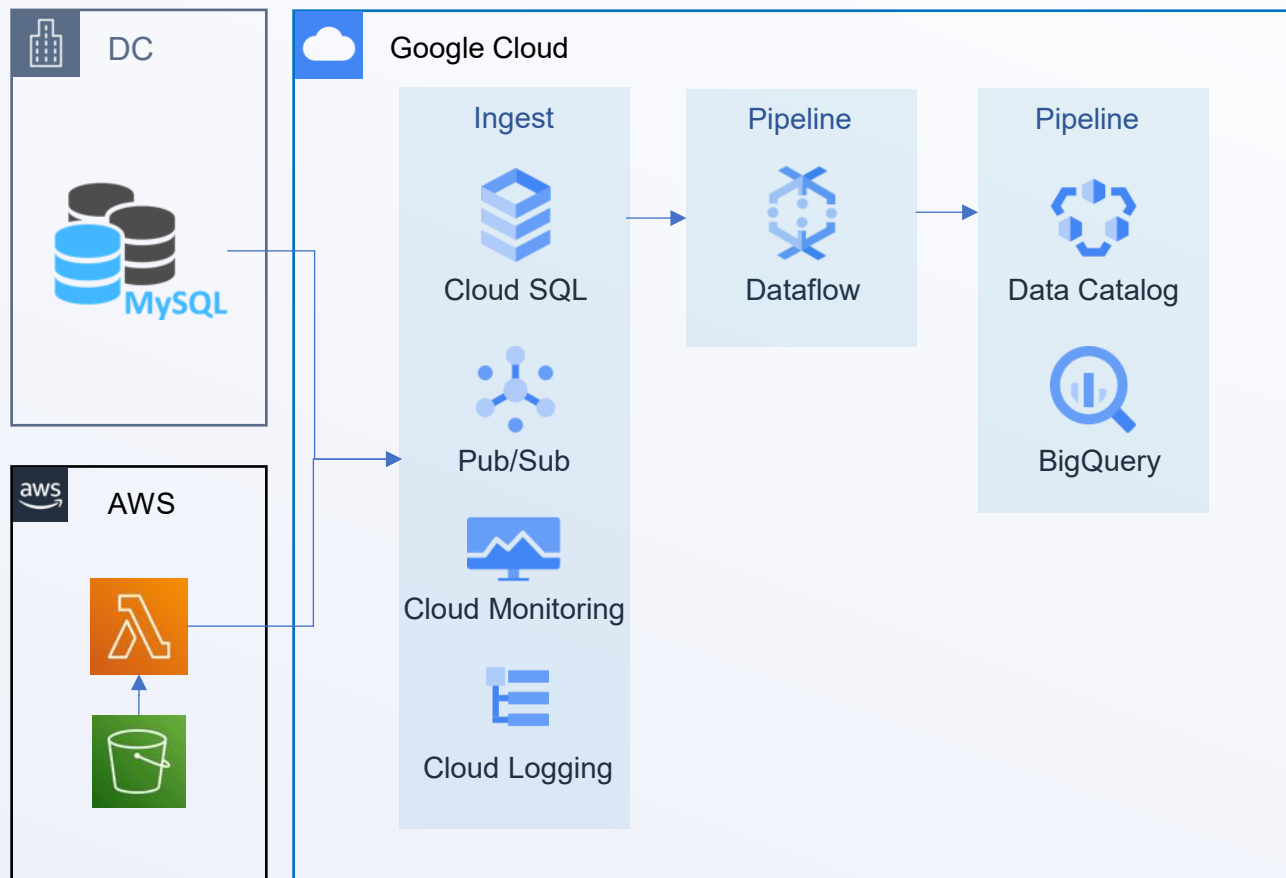
## マルチクラウド構成の分析基盤運用事例

### 【抱えていた課題】

- 高額なライセンスのETLサーバを使いコストが課題となっていた。
- パフォーマンスが悪く必要な時にデータを取得できず業務に影響がでていた。
- 障害時に大量のデータの洗い替えが必要で非常に時間もかかる状況であった。

### 【解決/改善】

- 従量課金で低コストな環境を提案いただきパフォーマンスも改善。
- ジョブの実行エラー時の対応を委託し調査や夜間帯の再実行対応が不要に。



# WEBサイトシナリオ監視サービスのご紹介

WEBサイトシナリオ監視サービスは、JIG-SAW OPS独自の監視用ロボットを利用して、Webサイトやコンテンツの自動監視を行うサービスです。

## ○特徴

通常のURL応答監視だけでは捉えきれない、アプリケーションのエラーやWebブラウザの表示崩れなどを確実かつ迅速にキャッチします。特にECサイトや会員登録などの処理を必要とするWebサイトを運営されているサイト管理者の皆様にご活用いただきたいサービスです。

### 導入前

システムご担当者様



目視確認

Webサイト



- ・ 人手で確認が必要なため1日数回の確認が限界
- ・ エラー発生時の状況をリアルタイムで確認することが難しく、どこに問題があったか把握できない

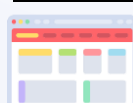
### 導入後

JIG-SAW



自動確認

Webサイト



異常時



システムご担当者様



- ・ デフォルト10分周期で自動確認
- ・ 異常発生時にはメールでご連絡
- ・ エラー発生時の画面はWEBモニタにて閲覧可能（スクリーンショット確認も可能）

# シナリオ監視STEPの概念

Webシナリオ監視では、「人が行うブラウザ操作と同様の操作」を行うことを1STEPとして定義します。監視の設定は1STEP毎に行います。また料金体系もSTEP数単位での価格となります。

○以下のようにSTEPは何らかのアクションを実行する単位となります。

- ページ内のリンクをクリック
- 指定のWeb要素のフォームに文字を入力する
- マウスオーバーでメニューを表示
- ドラッグ&ドロップで音量バーをコントロールする
- プルダウンメニューから選択
- 商品検索結果が〇〇件以上であることを確認する

## STEPの例

STEP1	https://monitor.jig-saw.com/login/ にアクセス
STEP2	Email address欄にメールアドレスを入力
STEP3	Password欄にパスワードを入力
STEP4	Log Inボタンをクリック
STEP5	ページ右上に入力したメールアドレスが表示されていることを確認する

# シナリオ監視ユースケース

ユーザがログインできるか		ショッピングカートに商品が入るか		チケット予約ができるか		ポイント残高が表示されるか	
1	ログインページを開く	1	商品ページを開く	1	ログインページを開く	1	ログインページを開く
2	ユーザのIDを入力する	2	商品数を選択する	2	ユーザのIDを入力する	2	ユーザのIDを入力する
3	パスワードを入力する	3	カートに入れるボタンをクリック	3	パスワードを入力する	3	パスワードを入力する
4	ログインボタンをクリック	4	所定の商品がショッピングカート内に存在するか	4	ログインボタンをクリック	4	ログインボタンをクリック
5	所定のユーザ情報が表示されているか	5	商品をショッピングカートから削除できるか	5	所定のユーザ情報が表示されているか	5	所定のユーザ情報が表示されているか
				6	予約ページを開く	6	ポイント残高ページに移動
				7	予約日時(例: 実行時の日時から1週間後の日付など)を選択	7	決められたポイント残高が表示されているか
				8	確認ボタンをクリック		
				9	予約ボタンをクリック		
				10	確認ページ内に所定の予約情報が表示されているか		

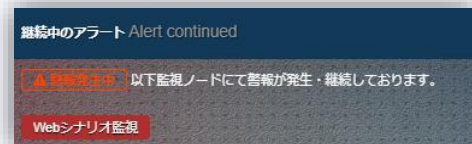
# puzzle WEBモニタの画面

## ■ 閲覧できるもの

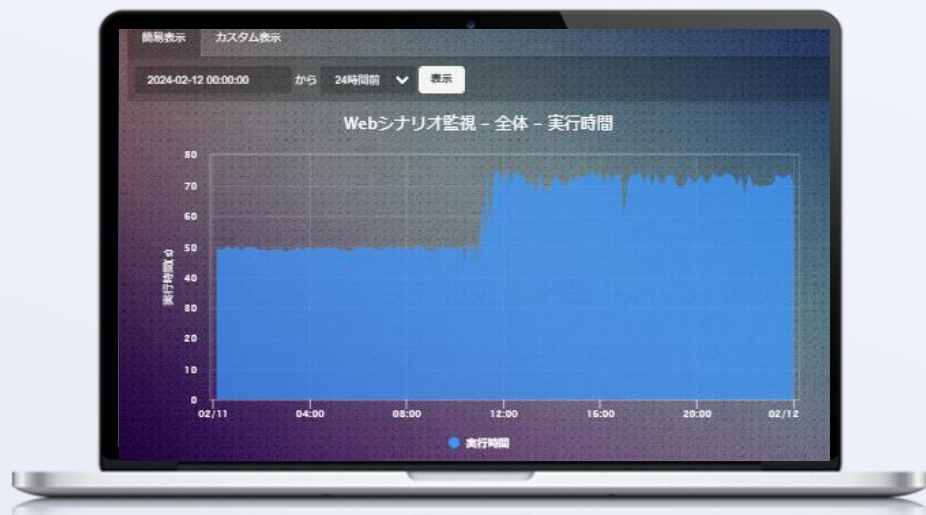
- ・発生中の警報一覧
- ・シナリオ実行時間のグラフ ※1
- ・STEPごとの実行状況の詳細
  - ・STEPごとの実行時間
  - ・操作エラー時の原因
- ・静観設定画面
- ・監視レポート（1か月単位で自動出力）

※1)

STEP毎のレスポンスタイムのグラフ表示させる場合はデータ量増加の関係で費用が通常より上がるため、個別でご相談となります。



## ▼シナリオ全体の実行状況



## ▼STEPごとの実行状況

STEP0 : ブラウザ起動	
結果	OK
実行時間	0.72秒
操作名	ブラウザ起動
操作詳細	閉じる 操作詳細1 結果 OK 実行時間 0.72秒 操作名 ブラウザを起動
入力パラメータ	> 開く
操作後のDump値	-
STEP1 : https://httpbin.org/delay/5	
結果	OK
実行時間	6.06秒 (内スクリーンショット取得時間 : 0.2秒)
操作名	URLアクセス
操作詳細	> 開く
入力パラメータ	> 開く
操作後のDump値	> 開く
スクリーンショット	> 開く
STEP2 : /html/body/pre	
結果	OK (エラーを無視)
実行時間	10.34秒 (内スクリーンショット取得時間 : 0.21秒)
操作名	クリック (ページ遷移あり)
操作詳細	> 開く
入力パラメータ	> 開く
操作後のDump値	> 開く

# puzzleについて



## 設定不要で 簡単導入

puzzleエージェントイン  
ストールや監視設定は  
弊社で実装



## 外部・内部監視 が可能

外からの監視とエージェントを  
用いた内からの監視が可能



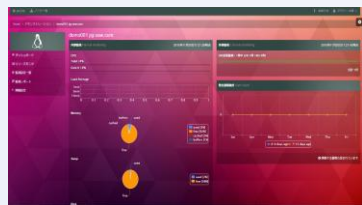
## API連携で PaaS監視も対応

API連携することで、  
PaaSサービスの監視が可能  
※主にAWSに対応



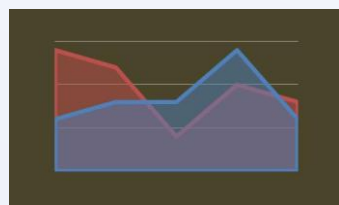
## 柔軟な通知方法

SlackやChatworkへの通知、  
曜日/時間帯毎の設定が可能



## リソース状況の 確認が可能

WEBモニタを閲覧するこ  
とで障害状況やリソース  
状況の確認が可能



## グラフの可視化 で分析

毎月1回のグラフの生成  
でシステムの動向も分析



## オートコールで 迅速通知

自動電話通知機能で  
一斉通知、優先順通知が可能



## オートコマンド 実行で自動化

障害発生時にお客さまの  
サーバでコマンドを実行  
し負荷軽減で業務改善

# puzzleについて

**接続方法**：インターネット(GIP)経由 / VPN経由 / 専用回線経由

**内部監視経路**：ファイアーウォール設定にて、監視対象からJIG-SAW向けのOutbound方向に443ポートの接続許可が必要となります。

**その他**：バックエンドのDBなどインターネットと直接接続されていないサーバは、

フロント側にあるWebサーバ、踏み台サーバ等からNAT設定をさせていただきます。

エージェントをインストールできないアーキテクチャについてはCloudWatch等からAPIを利用し、メトリクスを取得して監視させていただきます。

監視タイプ	監視項目		
エージェントレス監視 (外部監視)	Ping監視	死活応答監視	
	URL応答監視	HTTPステータスコード、コンテンツ内文字列パターンマッチング、レスポンスタイム他	
	SNMP監視	SNMPポーリング監視	
	SMTP応答監視	SSL/TLS、SMTP-Auth対応も含む	
	POP3/IMAP応答監視	SSL/TLS対応	
	SSL証明書期限監視	証明書期限の監視	
	TCP応答監視	ポート応答監視	
	DB応答監視	Oracle、MS-SQL、MySQL、PostgreSQL他、レスポンス監視も可	
エージェント監視 (内部監視)	リソース監視	CPU	CPU全体およびCPUコア毎の使用率
		メモリ	メモリ使用率
		ディスク	パーティションごとに異なる閾値を設定可(共通の閾値も設定可)
		ロードアベレージ	1分、5分、15分それぞれの項目別に閾値を設定可
		スワップ	スワップ使用率
		ネットワーク	インタフェースごとに異なる閾値を設定可能
		inode	パーティションごとに異なる閾値を設定可
	プロセス監視	アプリケーション	コマンドラインオプションも含めた正規表現でのパターンマッチング監視 検知した個数で閾値を設定
		ミドルウェア	
	ログ監視	検知パターンと除外パターンの組み合わせで監視周期内にマッチした行数を閾値に設定	

# Safingサービス概要

- Safingは、AWS環境の脆弱性や脅威を一元管理できるサービス
- 知見がないと使いこなしにくいAWSセキュリティサービスの活用をサポート
- 脆弱性や脅威の検出だけでなく、対処方法まで見える化することにより、セキュリティ課題解決を支援



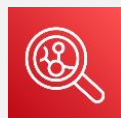
# Safingが活用するAWSセキュリティサービスの詳細

- Safingは、4種類のAWSセキュリティサービスを有効化し、Safing Consoleに脆弱性や脅威の情報を集約する仕組み
- Safingのご利用にあたり、有効化されるAWSセキュリティサービスは下記の通り



AWS Security Hub

- AWS のセキュリティチェックの自動化とセキュリティアラートの一元化をする機能
- S3の公開設定のミスやルートアカウントへのMFA設定漏れなどを可視化できる



Amazon Inspector

- CVE情報を元にリスクスコアを作成
- EC2 インスタンス、コンテナ（ECR）、Lambda 関数の脆弱性や、意図しないネットワークの露出がないか、自動でスキャン

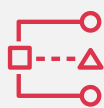


Amazon GuardDuty

- 不正なアクティビティやマルウェアの感染を自動で検出
- 人による作業やサードパーティーのツールを必要とすることなく、AWS アカウントの脅威検出が可能



AWS IAM



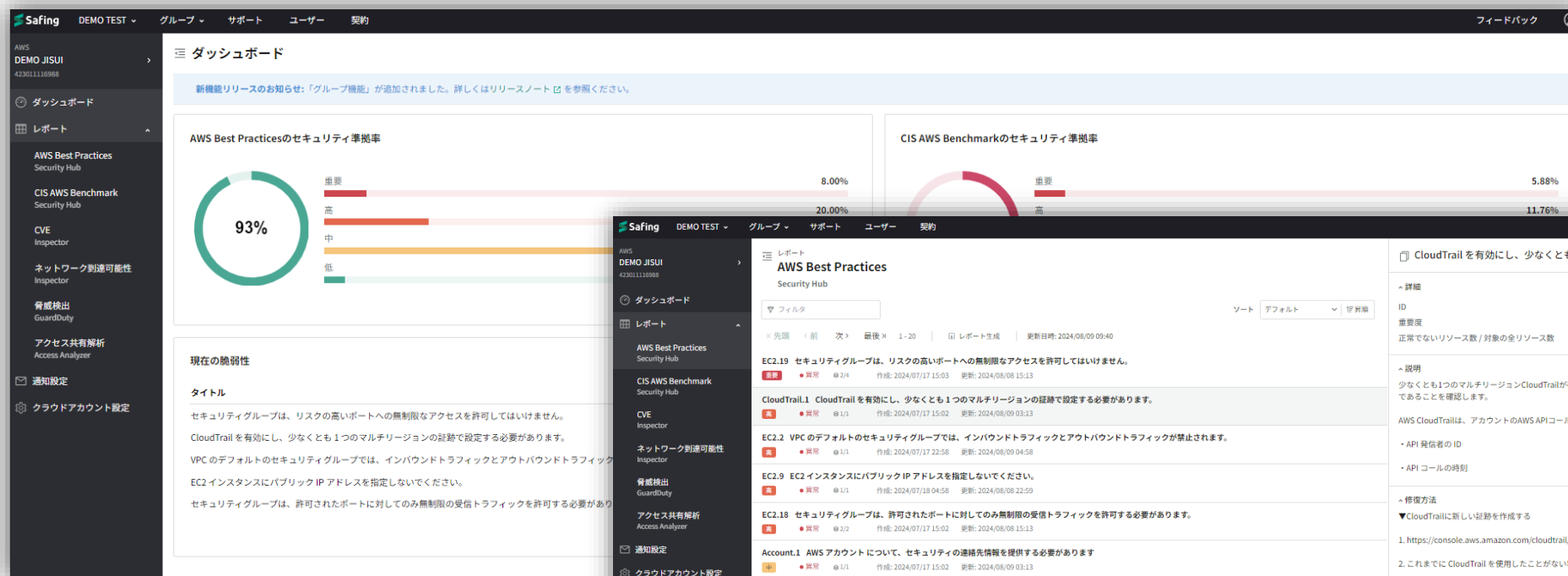
IAM Access  
Analyzer

- IAM Access AnalyzerはAWS IAMの一機能
- AWSリソースに紐づいているポリシーを検査し、管理者として意図していない公開設定・IAM権限が設定がされていないか、自動で検出

# Safingで出来ること

- Security HubやInspectorの内容を、分かり易くダッシュボードで表示
- 脆弱性の詳細だけでなく、修復方法の詳細も記載されているため、運用課題の解決につながる
- メールアドレスや電話番号を入れるだけで、GuardDutyやIAM Access Analyzerのアラートを受け取れる（※）
- アラートの設定ミスなく、インシデントにいち早く気づき対処をすることが可能

※通知機能はビジネスプラン以上で利用可能



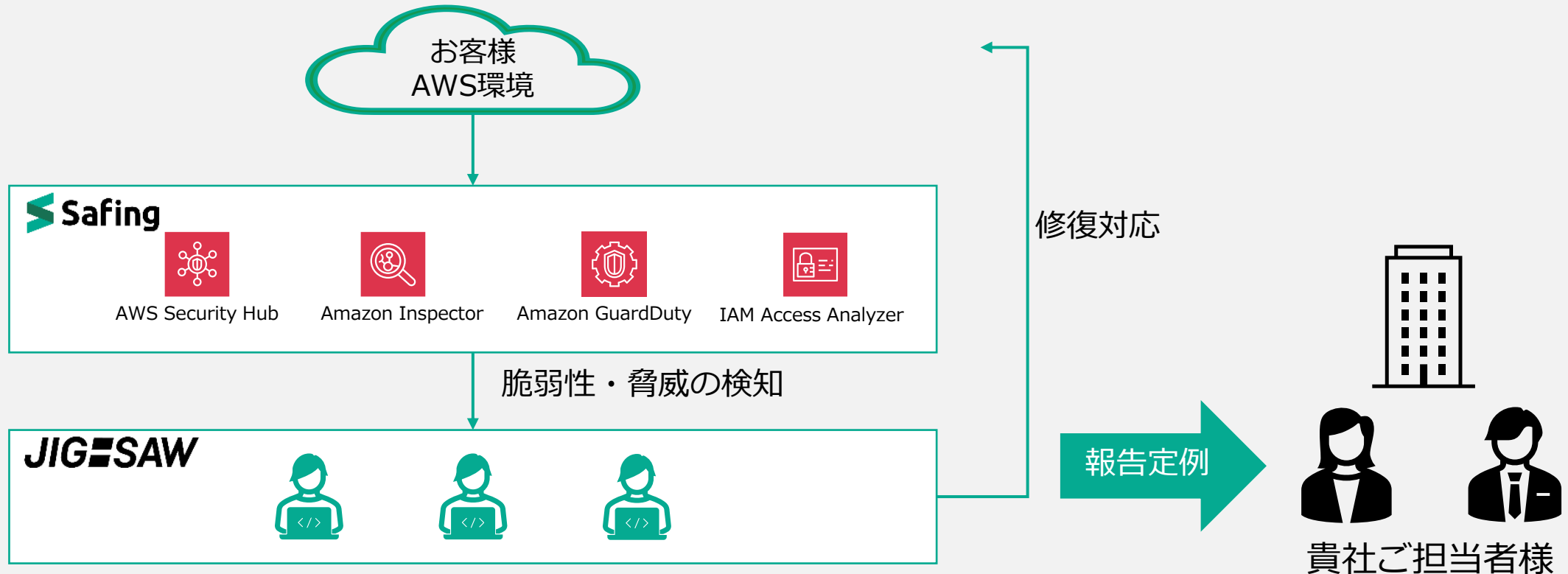
This screenshot shows a detailed report from Safing titled 'AWS Best Practices Security Hub'. The report lists several security findings with their severity levels and remediation instructions. The findings include:

- EC2.19** セキュリティグループは、リスクの高いポートへの無制限なアクセスを許可してはいけません。 (Security groups should not allow unrestricted access to high-risk ports.)
- CloudTrail.1** CloudTrail を有効にし、少なくとも1つのマルチリージョンの証跡を設定する必要があります。 (Enable CloudTrail and configure at least one multi-region trail.)
- EC2.2** VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックとアウトバウンドトラフィックが禁止されます。 (In the default VPC security group, inbound and outbound traffic is prohibited.)
- EC2.9** EC2 インスタンスにパブリック IP アドレスを指定しないでください。 (Do not specify a public IP address for EC2 instances.)
- EC2.18** セキュリティグループは、許可されたポートに対してのみ無制限の受信トラフィックを許可する必要があります。 (Security groups must only allow unrestricted inbound traffic for permitted ports.)
- Account.1** AWS アカウントについて、セキュリティの連絡先情報を提供する必要があります。 (Provide security contact information for the AWS account.)
- EC2.3** アタッチされた EBS ボリュームは、保管時に暗号化する必要があります。 (Attached EBS volumes must be encrypted at storage.)
- EC2.6** すべての VPC で VPC フローログ記録を有効にする必要があります。 (Enable VPC flow log recording for all VPCs.)
- EC2.7** EBS デフォルト暗号化を有効にする必要があります。 (Enable EBS default encryption.)

The right side of the report shows details for the 'CloudTrail.1' finding, including its ID, severity (Critical), and remediation steps such as enabling CloudTrail and configuring multi-region trails.

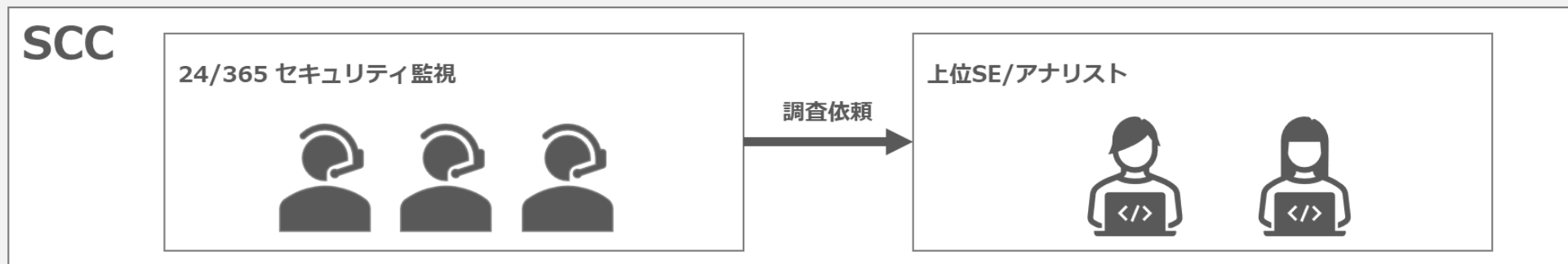
# Safing運用 (CSPM)

- セキュリティ課題に対して、弊社がお客様の運用を通じて得た知見を元に、セキュリティ運用サービスをご提供
- CSPM (Cloud Security Posture Management) サービスを提供中
- 設定ミスなどによる脆弱性を弊社スタッフが確認することで、いち早く脆弱性の検出・修復が可能



# セキュリティサービス：SOC（Security Operation Center）サービス

- 弊社の運用監視体制を活用し、セキュリティインシデントにも備える体制を実現
- セキュリティインシデント後の支援ができる体制を築く



## セキュリティエンジニアチーム

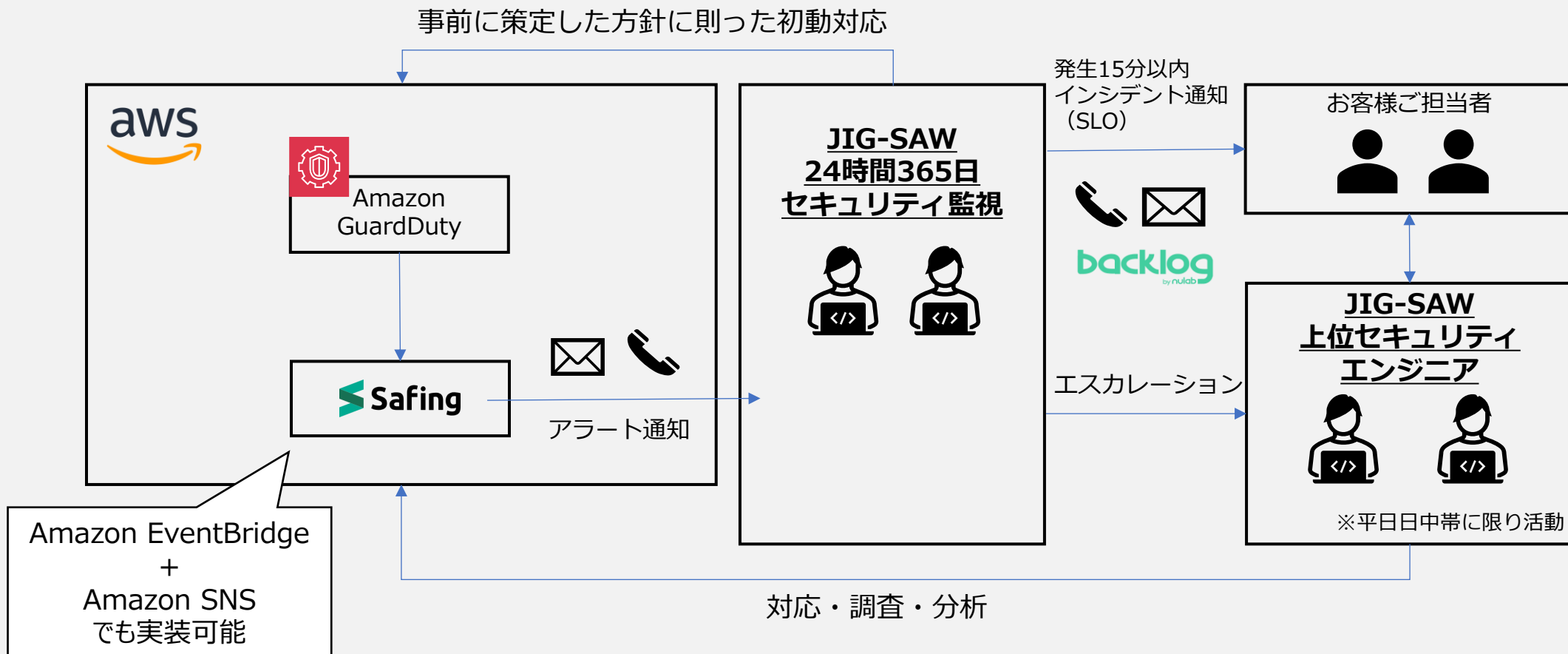
- 役割
  - ・ 24時間365日セキュリティ監視、運用
  - ・ セキュリティインシデント発生時15分以内連絡
- 業務
  - ・ ログ監視
  - ・ インシデント切り分け
  - ・ インシデント一次報告

## 上位SE/アナリストチーム

- 役割
  - ・ インシデント分析、調査対応
  - ・ セキュリティ強化のアドバイザリ
- 業務
  - ・ ログ分析
  - ・ 経路分析
  - ・ 影響調査
  - ・ セキュリティアドバイザリ

# Amazon GuardDuty運用（Safing活用）

- Amazon GuardDutyからの通知を起点に、JIG-SAWのエンジニア体制で受け取り、24時間365日体制で検知・対応を実施
- 発生した通知に対して、事前に策定した方針に則った初動対応のほか、上位セキュリティエンジニアによる調査・分析が可能



# NEWS

## 2024年12月より東京本社が移転となりました！

JIG-SAWは今後の大幅な事業拡大に向け、現在の大手町本社オフィスと丸の内オフィスの東京2拠点を1つに統合・集約しました。

移転先である新オフィスの面積は、従来の2倍以上となります。  
※登記上の本店は変わらず北海道札幌市のSCC N83となります。

### [本社移転先の名称及び所在地]

(1) 名称

東京ミッドタウン八重洲  
八重洲セントラルタワー 33階

(2) 所在地

東京都中央区八重洲二丁目2番1号

### [JIG-SAWコントロールセンター一覧] ※変更なし

- ・ SCC N44 (新設札幌コントロールセンター：札幌市中央区)
- ・ SCC N83 (既存札幌コントロールセンター：札幌市北区)
- ・ SCC サテライト (データセンター：札幌市中央区)
- ・ TCC (北米トロントコントロールセンター：カナダ・トロント)



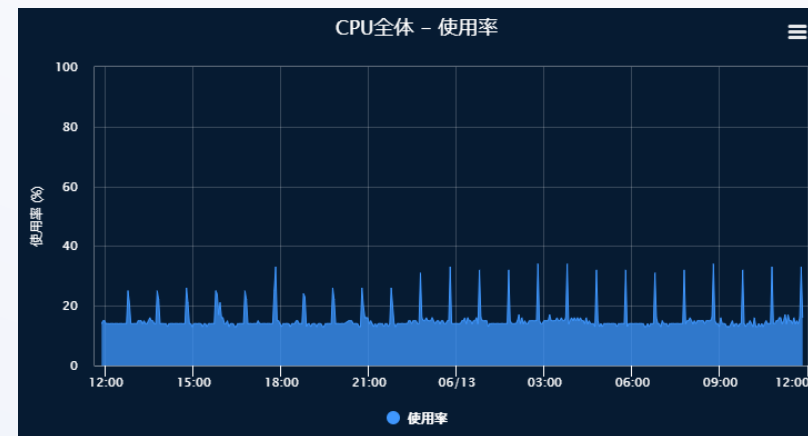
## NEWS

# puzzle WEBモニタにリソースグラフのAI分析機能が搭載されました

弊社監視ツールpuzzleについて、AIとの連携機能の開発を進めております。  
第一弾として、取得した監視データに対し生成AIによる分析を行う機能をリリースいたしました。  
ユーザ様側でより手軽にサーバのリソース状況を分析できる機能となります。  
今後もAI活用は積極的に進めてまいります。



グラフの期間のCPU全体使用率について  
分析、洞察、提案をしてください。



### 【分析】

ほとんどの時間帯でCPUの使用率は14%前後で安定していますが、いくつかのピークが見られます。  
特に、最大使用率が26%を超えることが数回あります。

### 【洞察】

ピーク時の使用率が30%を超える状況が散見されるため、突発的な負荷がかかっている可能性があります。  
また、使用率が一定の時間帯で急上昇している点も気になります。

### 【提案】

特定の時間帯での負荷の原因を特定し、必要であればその時間帯に対策を講じることをお勧めします。  
また、負荷分散やリソースの追加を検討する必要があります。

puzzle

今日を知り、明日を変えるシステム運用メディア

# Ops Today

最新のITトレンドやセキュリティ対策の  
情報をお届けします。

> [Ops Todayを見る](https://ops-today.com/)



**THANK YOU**

⋮