

## 1. サービス概要

### 1.1. サービス概要

- 本サービスは Amazon Web Services (以下、AWS) を対象とした有人によるサービス監視、障害対応、定常運用作業代行サービスです。
- クラスメソッド株式会社 (以下、クラスメソッド) と JIG-SAW 株式会社 (以下、JIG-SAW) が、お客様に代わり24時間365日体制で、作業負荷の軽減と安心をご提供いたします。

### 1.2. 提供サービス

本サービスでは、以下のサービスを提供いたします。

- 障害発生時のご連絡および一次対応
- 障害二次対応
- 定常運用作業代行
- 月次対応レポート作成
- 脆弱性情報アナウンス
- ( puzzle 利用時のみ ) Webポータルサイト
  - puzzle は JIG-SAW が提供する監視サービスです。

## 2. 対象とするお客様

- ビジネス課題に注力したい
- 夜間 / 土日はゆっくり休みたい
- 定常作業をまるっと任せたい
- 障害発生時の一次対応を対応してほしい
- 障害原因を調査してほしい
- もっと安く安定した環境にしたい

## 3. サービス内容

### 3.1. 有人によるサービス監視

監視対象項目を定義しメール通知をトリガーに、サービス状況確認・障害対応を行います。

#### 3.1.1 対象監視システム

お客様で保有されている既存監視システムのご利用も可能です。既存監視システムがない場合はクラスメソッドの提供する監視サービス「監視オプション ( Mackerel ) または JIG-SAW の提供する監視サービス ( puzzle ) のご提供が可能です。ただし、特定のメールアドレスへのメール通知および通知内容 ( 件名 ) のご共有が前提条件となります。

### 3.2. 障害発生時のご連絡および一次対応

24/365 サポートチームが、監視項目ごとの緊急度（高 / 低 の設定可能）により、メールまたは電話での連絡を行います。

- アラート検知
- エスカレーション対応（電話 / メール）
- 再起動対応
- 障害一次対応（手順書対応）

## 障害一次対応サンプル

### URL応答警報検知時

#### 1. サイト表示確認

- ブラウザにて該当のURLを開き表示を確認する
  - [https://\\*\\*\\*\\*.\\*\\*\\*\\*.com](https://****.****.com) 
- URLが表示され復旧を検知しているか確認
  - 復旧を検知している場合：静観
  - アラートが継続している場合：以降の手順を実施

#### 2. 該当サーバへログイン

- 該当サーバへSSH接続をします

#### 3. apacheプロセスの再起動

apacheプロセスの再起動

```
# systemctl status httpd

# ps auxwf | grep httpd | grep -v grep
*apacheプロセスが稼働していることを確認

# systemctl stop httpd

# ps auxwf | grep httpd | grep -v grep
*apacheプロセスが停止していることを確認

# systemctl start httpd


# ps auxwf | grep httpd | grep -v grep
*apacheプロセスが稼働していることを確認

# netstat -anpt | grep LISTEN | grep httpd
*httpdに関するポートが開いていることを確認
```

ログの確認

```
# tail -f /var/log/httpd/access_log
*ステータス200のログが流れている及び400番台・500番台のログが頻発していないことを確認
```

## 4. サイト表示確認&一次対応後連絡

- ブラウザにて該当のURLを開き表示を確認する
  - `https://****.****.com` 
- URLが表示され復旧を検知しているか確認
  - 復旧を検知している場合：一次対応後に復旧した旨をメール連絡
  - アラートが継続している場合：電話連絡

## apacheプロセス警報検知時

### 1. 該当サーバへログイン

- 該当サーバへSSH接続をします

### 2. apacheプロセスの再起動

apacheプロセスの再起動

```
# systemctl status httpd

# ps auxwf | grep httpd | grep -v grep
*apacheプロセスが稼働していることを確認

# systemctl stop httpd

# ps auxwf | grep httpd | grep -v grep
*apacheプロセスが停止していることを確認

# systemctl start httpd

# ps auxwf | grep httpd | grep -v grep
*apacheプロセスが稼働していることを確認

# netstat -anpt | grep LISTEN | grep httpd
*httpdに関するポートが開いていることを確認
```

### 3. 動作確認

- プロセスが復旧しているか確認
  - 復旧を検知している場合：一次対応後に復旧した旨をメール連絡
  - アラートが継続している場合：インスタンス再起動

### 4. インスタンス再起動

- マネジメントコンソールにログイン
  - EC2 インスタンス画面へ移動
  - 対象インスタンスを選択
  - 対象のインスタンスを停止
  - 対象のインスタンスを起動

- apacheの状況確認

該当サーバへSSH接続をします

```
# systemctl status httpd

# ps auxwf | grep httpd | grep -v grep
*apacheプロセスが稼働していることを確認
```

## 5. 一次対応後連絡

- 復旧を検知している場合：インスタンス再起動後に復旧した旨をメール連絡
- アラートが継続している場合：電話連絡

### 3.3. 二次対応

24/365 サポートチームが障害復旧および再発防止のために、一次対応の結果をもとに対応を行います。

- 原因調査（障害発生から5日間で4時間程度の支援）
  - 例：ログ調査、知見・技術によるベストエフォートな支援
- 障害復旧サポート
  - 例：バックアップからのデータリストア・インスタンス再作成
- 手順書対応（事前に共有済みの手順をもとに実施）
  - 例：インスタンスタイプ変更、悪意のあるIPアドレスのブラックリスト登録

### 3.4. 定常運用作業代行

事前に手順・日時をご指定いただいた内容で、サポートチームが作業を実施します。

- ネットワーク周りの設定変更
- AWSマネージメントコンソールからの各種設定変更
- AWS Systems Manager から行う作業
- サーバのスペックアップ・ダウン作業
- サーバのスケールアウト・イン作業
- バックアップ取得

### 補足事項

- マネジメントコンソール以外にも、awscli、Powershell、SystemsManager Automation 等を利用した作業が可能です。詳しくはお問い合わせください。
- 作業代行は1か月あたり契約台数の回数まで、1回あたりの作業時間は最大2時間を目安とします。3営業日以内に作業を開始します。
- 作業の依頼はBacklogを利用して行っていただきます。

### 作業代行サービスの範囲例（AWS）

カテゴリ	サービス	作業内容	対応可否	備考
コンピューティング	EC2	インスタンスの Start・Stop		
		EBSのバックアップ・リストア		
		AMIからのインスタンス作成		基本的には復旧作業のみとなります

		Role のアタッチ・デタッチ		
	ELB	ELBへのEC2インスタンスの登録・解除		
		TimeOut、Connection Draining等の設定変更		
		SSL証明書の登録・更新		
		新規ELBの作成		
		アクセスログ取得設定		
	AutoScaling	起動数 ( DesiredCapacity ) の変更		
		新規AutoScalingの構成		AMI作成時のデプロイは行なっておりません
	Route53	レコードの追加・変更・削除		
		レジストラへ権威サーバー変更作業	×	
		ドメインの取得・更新		
		他DNSからのDNSレコードの移行		zoneファイルをいただきましたら可能です
	EMR	設定変更作業全般	×	
ネットワーキング	セキュリティグループ	セキュリティグループへの設定変更		
	VPN	設定変更作業全般		
	Direct Connect	設定変更作業全般		
	NACL	新規追加		
		ルールの追加・削除		
	ルートテーブル	ルートの追加・削除		

ストレージ・コンテンツ配信	S3	バケットの作成		
		LifeCycleの設定変更		
	Glacier	ファイルの復元		
	CloudFront	新しいディストリビューションの作成		
		CloudFront に地域制限を適用する		
		アクセスログ取得設定		
	Storage Gateway	設定変更作業全般		
	Import Export	設定変更作業全般		
データベース	RDS	インスタンスのリポート・フェイルオーバー		
		インスタンスタイプの変更		
		ディスクサイズの変更		
		スナップショット保存世代数の変更		
		スナップショットからのDBインスタンス作成		
		バージョンアップ		
	ElastiCache	新規クラスター作成		
		ノードの追加 ( memcachedのみ )		
	DynamoDB	テーブルの作成		
	Redshift	ノードタイプの変更		
		ノードの数の変更		
		自動スナップショット保存期間の変更		
		スナップショットからのクラスター作成		
		EIP の付け替え		

		スナップショット作成		
デプロイ & マネジメント	Elastic Beanstalk	設定変更作業全般		
	OpsWorks	設定変更作業全般	×	
	CloudFormation	スタックのアップデート	×	
	IAM	ユーザー・グループの作成、削除		
		パスワードのリセット		
		IAM Role の作成		
	Data Pipeline	設定変更作業全般	×	
	CloudHSM	設定変更作業全般	×	
アプリケーションサービス	CloudSearch	設定変更作業全般	×	
	Elastic Transcoder	設定変更作業全般	×	
	SES	プロダクション申請		
		ドメイン・メールアドレス認証		
	SNS	トピック作成・変更		
	SQS	キュー作成・変更		
	SWF	設定変更作業全般	×	
管理ツール	CloudWatch	メトリクスフィルタ作成		
		CloudWatch アラーム作成		
シェル・aws-cli	aws-cli	スクリプトサンプルの提供	×	

#### 作業代行サービスの作業範囲例（OS、ミドルウェア）

作業対象	作業内容	対応可否	備考
Linux	OSユーザーアカウントの作成		
	OSユーザーアカウントパスワードリセット		

	iptablesの設定		
	EBS追加後の新規ボリュームの作成		
Windows	RDP を使ってログインしての作業		
	Systems Manager の Run Command による作業		コマンド作成は都度のご相談とさせていただきます
	AMI からのインスタンス作成		
	EC2 の Stop / Start		
	AMI および スナップショットの作成		
Apache	httpd.conf の変更		調査の伴う変更につきましては都度のご相談とさせていただきます
	アクセスログ、エラーログの抽出		
	VirtualHostの追加・変更		
PHP	php.ini の変更		調査の伴う変更につきましては都度のご相談とさせていただきます
ミドルウェア	yumによるパッケージインストール・アップデート		
	お客さま指示の手順書に基づいたパッケージインストール		
	ソースからのビルド、商用パッケージ製品のインストール		ソースからのビルドが不可となります。
その他	お客さま指示の手順書に基づいた作業		

## 定常作業代行サンプル



## セキュリティグループ設定変更

---

### 1. 作業開始連絡 (30分前)

---

Backlog (想定) で、予定時刻より作業を開始することを依頼者へご連絡

[確認点]

- Backlog で、正常にコメント内容が保存されている
- 通知先が依頼者となっている

[中止基準]

- Backlog 障害等で連絡が取れない
- 上記 [確認点] がクリアされない

[巻き戻し]

- 後続作業を中止する
- 連絡が可能となった段階でご報告を行う

### 2. 対象アカウントへログイン

---

マネジメントコンソールで、作業対象となる AWS アカウント (12桁) へログインします。

[確認点]

- 正しいアカウント、ユーザーでログインが行えている
- 対象リソースのあるリージョンが表示されている

[中止基準]

- AWS 障害等でログインできない
- 上記 [確認点] がクリアされない

[巻き戻し]

- 後続作業を中止する
- お客様へ状況をご連絡を行う

### 3. 対象リソースの確認

---

EC2 から セキュリティグループへ 移動をし、作業対象リソースをグループ名で検索します

[確認点]

- 対象リソースが存在している

[中止基準]

- マネジメントコンソールが表示されない (権限不足)
- 上記 [確認点] がクリアされない

[巻き戻し]

- 後続作業を中止する
- お客様へ状況をご連絡を行う

## 4. 現在設定と作業内容の確認

対象リソースを選択し、「インバウンド」または「アウトバウンド」を確認します



### [ 確認点 ]

作業種別によって以下の内容を確認します。

- 追加：追加予定の内容が存在していないこと
- 削除：追加予定の内容が存在していること
- 変更：追加予定の内容が存在している、変更後の内容と異なること

### [ 中止基準 ]

- 上記 [ 確認点 ] がクリアされない

### [ 巻き戻し ]

- 後続作業を中止する
- お客様へ状況をご連絡を行う

## 5. 変更作業

対象リソースの「インバウンド」または「アウトバウンド」を選択し、「編集」を選択します。

「ルール追加」から新しいルールの追加、または「X」にてルールの削除、またはルール内容を変更し、「保存」を選択します



### [ 確認点 ]

- 変更を行った内容が反映されている

### [ 中止基準 ]

- 上記 [ 確認点 ] がクリアされない

### [ 巻き戻し ]

- 後続作業を中止する
- お客様へ状況をご連絡を行う

## 6. 作業完了連絡

Backlog（想定）で、作業終了を依頼者へご連絡

### [ 確認点 ]

- Backlog で、正常にコメント内容が保存されている
- 通知先が依頼者となっている

### [ 中止基準 ]

- Backlog 障害等で連絡が取れない
- 上記 [ 確認点 ] がクリアされない

### [ 巻き戻し ]

- 連絡が可能となった段階でご報告を行う

## RDS インスタンスタイプ変更

### 1. 作業開始連絡 (30分前)

Backlog (想定) で、予定時刻より作業を開始することを依頼者へご連絡

### 2. 変更作業

AWS CLI を利用して即時に変更します  
(例: db.t2.micro へ即時変更)

```
$ aws rds modify-db-instance --db-instance-identifier database-1 --db-instance-class db.t2.micro --apply-immediately
```

対象DB の以下の項目に結果が反映されたことを確認します。

```
$ aws rds describe-db-instances --db-instance-identifier database-1
```

- DBInstanceClass: db.t2.small
- DBInstanceStatus: available

### 3. 作業完了連絡

Backlog (想定) で、作業終了を依頼者へご連絡

## 3.5. 月次対応レポート作成

以下の6項目を記載したレポートを報告いたします。

- お客様情報
- マネジメントサービス 対象ホスト
- 作業実績報告
- 作業実績詳細
- 警報一次対応報告
- 特記事項・その他ご報告

## 3.6. 脆弱性情報アナウンス

サービス提供側で、影響が広範囲・深刻と判断した脆弱性情報について 連絡用ツールにて、ご案内いたします。

お客様にカスタマイズしたご案内 (特定製品、案内方法・内容) は行っておりません。

## 3.7. Webポータルサイト ( puzzle 利用時のみ )

ご契約いただいたお客様に Web ポータルサイトをこ用意します。Web ポータルサイトでは、以下の機能を提供いたします。

- サービス提供対象機器における稼働状況の閲覧
- メンテナンス作業等に伴う監視の静観設定

## 4. サービス申込み～利用開始

- ご契約からサービス開始まで2～4週間程度を想定ください。
- 対象項目、対応内容（手順）によって、サービス開示時期が変動することがございます。

お客様作業	クラスメソッド及び JIG-SAW 作業
見積依頼 <ul style="list-style-type: none"> <li>・ 保護対象台数</li> <li>・ 定常作業想定所要時間</li> </ul>	
	見積作成・送付
契約書への記入	
	受付 各種記入用ファイル送付
マネジメント対象一覧 への記入 <ul style="list-style-type: none"> <li>・ 障害、定常作業対象リソース情報 (AWS サービス、リージョン、名前、ユーザ情報等) ) 記入</li> <li>・ (共有可能であれば) システム構成図</li> </ul>	
ヒアリングシート への記入 <ul style="list-style-type: none"> <li>・ 連絡先 (メールアドレス、電話番号)</li> <li>・ 通知情報 (アラート件名、本文、一次対応、復旧件名)</li> </ul>	
各種代行手順のご準備	
	監視システム導入の場合 <ul style="list-style-type: none"> <li>・ 監視項目選定 (項目、閾値、対応内容)</li> <li>・ 監視エージェントのインストール</li> <li>・ (Systems Manager エージェントのインストール)</li> <li>・ 監視システム側の設定</li> </ul>
監視設定の動作検証をしていただきます。(推奨) <ul style="list-style-type: none"> <li>・ 監視項目、閾値の確認</li> <li>・ メール通知、電話通知の確認</li> </ul>	同左
サービス開始	同左

## 5. サービス提供条件

### 5.1. 提供リージョン

- AWSの全リージョンでご利用可能です。

### 5.2. 提供条件

- AWSアカウントのメンバーズ プレミアムプラン契約が必要です。
- 障害対応作業、作業代行にあたり、IAM RoleやOSユーザーが必要になります。
  - 最低限必要な権限は弊社よりご連絡いたします。
- ログインするための認証情報は、クラスメソッドとJIG-SAWで管理します。
- (作業内容に応じて) 監視対象サーバーにAWS Systems Managerエージェントのインストールを行います。この際、対象サーバーの管理者権限が必要になります。
  - サービス開始後もエージェントのアップデートが必要になる場合がございます。
- 監視システムからの通知先として、メールアドレスが最低1つ必要になります。
- 障害対応には通知される内容(件名、本文)を予め共有いただく必要がございます。

### 5.3. サーバー要件

- Amazon Linux, Amazon Linux 2
  - CentOS
  - Windows Server 2012以降
- 上記以外のOSについて希望される際はご相談ください。

### 5.4. 管理者の登録

- 本サービスでは、ご契約時に管理者情報を登録していただきます。
- 管理者情報とは、監視サービス仕様に基づく障害発生を検知した場合のご連絡先です。
- メール、電話ともに最大5つまでご登録いただくことが可能です。
- お電話でご連絡する場合、優先度の高い方からご連絡し、ご連絡が取れた段階で、優先度下位の方にはご連絡いたしません。
- メールでのご連絡は、ご登録いただいた方すべてに同報でお送りいたします。ご連絡先が2つ以上の場合は、別途ご相談ください。
- なお管理者情報につきましては、保守ヘンタ様の情報でも問題ございませんか、ご登録いただいた管理者様は、本サービスの内容について十分理解しているものいたします。

### 5.5. Webポータル画面利用要件

- Chrome 最新版
  - Firefox 最新版
  - Internet Explorer 10以上
- FirefoxまたはChromeでの利用を推奨しております。

### 5.6. 連絡用ツール

問い合わせ・作業依頼に関する連絡方法は、サービス提供側が用意する [Backlog\[1\]](#) の利用をお願いいたします。

お客様の規則等で利用できない場合は、別途ご相談ください。

### 5.7. システム情報一覧

サービスを開始する上で必要となる情報です。

- AWSアカウントID(数字12桁)
- AWS環境構築作業用IAM Role

- AWS環境調査用IAM Role
- AWS環境障害対応作業用IAM Role
- OS障害対応作業用ユーザー（Linux または Windows）

## 5.8. IAM Role

AWS リソースに対する読み取り・変更作業を行うため、以下を作成させていただきます。

種別	IAM Role名	権限	用途
AWS環境調査用IAM Role	JIG-SAW_ReadOnly	AWSサービス全般に対する参照権限	問い合わせ等対応時の環境調査のため
AWS環境障害対応作業用IAM Role	JIG-SAW_Operation	EC2、ELB、RDS等監視対象リソースに対する操作権限	障害対応作業のため

## 5.9. 言語

日本語で実施します。

## 6. サービス費用

価格はすべて税別です。

台数は運用サービス対象のEC2、RDS、ElastiCache、Fargate（サービス単位）のインスタンス数が対象になります。

AutoScaling の台数は desired capacity に指定し起動している台数分になります。月20時間までのスケールアウトはカウントしません。

### 6.1. 最小構成（5台）での費用イメージ

#### 6.1.1 運用代行オプションのみ利用

項目	内容	費用	備考
初期費用・・・	運用初期設定	100,000円	
月額費用・・・	運用代行オプションサービス利用料	100,000円	5ノード 構成例 ・ EC2（仮想サーバー）本番2台 ・ EC2（仮想サーバー）開発1台 ・ RDS（データベース）本番1台 ・ RDS（データベース）開発1台
初月合計	+	200,000円	

2ヶ月目以降 合計		100,000円	
-----------	--	----------	--

### 6.1.2 監視オプションとの併用利用

項目	内容	費用	備考
初期費用・・・	運用初期設定	100,000円	
初期費用・・・	監視初期設定	50,000円	監視システムとして監視オプションを利用した場合 10,000円/台
月額費用・・・	AWSサービス監視	25,000円	監視システムとして監視オプションを利用した場合 5,000円/台
月額費用・・・	運用代行オプションサービス利用料	100,000円	5ノード 構成例 ・ EC2 (仮想サーバー) 本番2台 ・ EC2 (仮想サーバー) 開発1台 ・ RDS (データベース) 本番1台 ・ RDS (データベース) 開発1台
初月合計	+ + +	275,000円	
2ヶ月目以降 合計	+	125,000円	

### 6.2. 月額費用

項目	費用
サービス利用料 (最小契約台数: 5台)	100,000円
以降 台数1台追加あたり	20,000円

### 6.3. 初期費用

サービス提供側に初期作業を委託する場合は以下の通りとなります。

項目	費用
----	----

AWS 環境準備 アカウント準備 管理対象情報記入 連絡情報記入 監視設定（puzzle 利用時に限る） 障害・定常作業代行手順作成	月額費用1ヶ月分
---	----------

本サービスと合わせて監視オプションによる監視を行う際には別途費用がかかります。

## 6.4. その他の費用

運用における課題に関して以下のサービスを提供しております。ご希望の際はお問い合わせください。

項目	費用	備考
継続的なシステム構成最適化の相談	10,000円/時間	フートアドバイザー契約
IDS/IPSシステムの導入	月額 20,000円～	フートセキュリティ契約

## 7. サービス契約

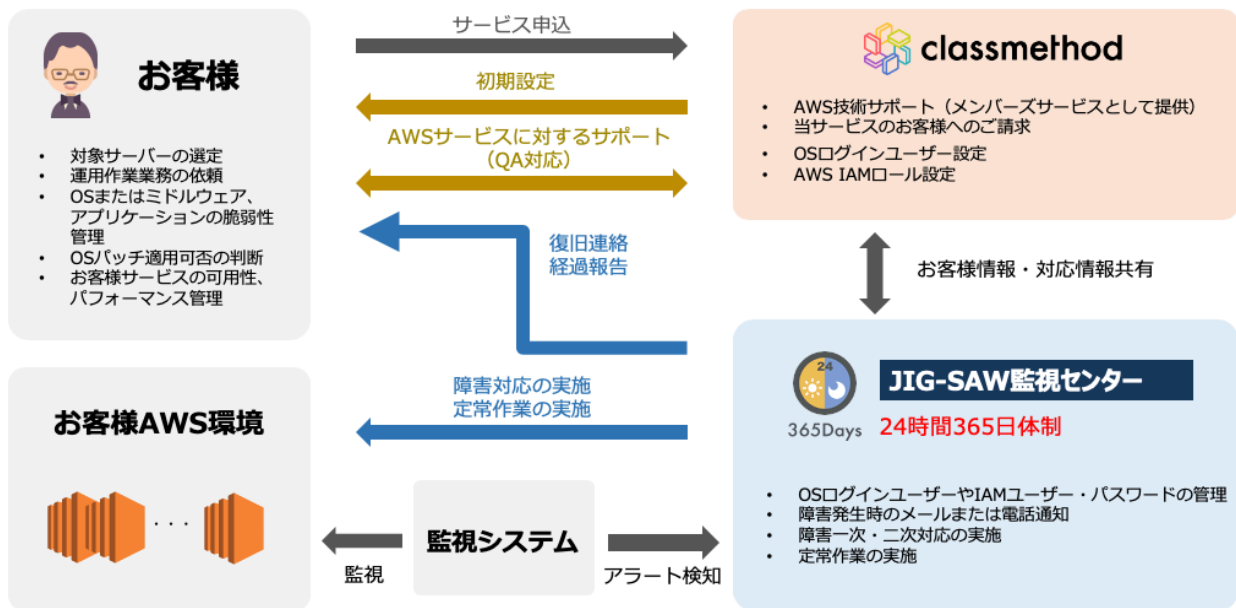
最低利用期間	課金開始月より 3ヶ月間 (3ヶ月未満で解約した場合、残り期間の費用を請求させていただきます)
課金開始日	お客様指示の開始月1日より ・増加：日割り計算 ・解約、減小：月割り計算
支払条件	弊社への支払い条件は、お客様と弊社で締結している「取引基本契約」(若しくは、両社間の取引支払い条件を取り交わしている基本の契約)に準ずるものとしします。
解約申し込み	解約60日前に書面にて申請いただきます。 なお解約時、過去に蓄積されたデータについてはご提供いたしません。
監視システムの管理責任	本サービスで提供する監視システム (Webポータルサイトおよびそれが稼働するサーバー) についての管理責任はJIG-SAWにあります。 ・監視システムの可用性管理、セキュリティ対策 ・収集したデータの保全管理 ・Webポータルサイトにログインするためのお客様ま固有アカウントおよびパスワードの管理 また下記設定およびスクリプトについての管理責任はクラスメソッドにあります。 ・本サービスで利用するIAMクレデンシャルの管理 ・Linuxサーバーのssh鍵の管理、Windowsサーバーのパスワード管理



<p>お客様機器の管理責任</p>	<p>保護対象サーバーやサービスに対する管理責任はお客様にあります。</p> <ul style="list-style-type: none"> <li>保護対象サーバーの可用性管理、セキュリティ管理</li> </ul>
<p>その他</p>	<ul style="list-style-type: none"> <li>サービス提供対象機器とお客様が所有する他製品との問題切り分けは、本サービスに含まれません。</li> <li>本サービスの全部または一部を弊社外部へ再委託する場合があります。</li> <li>本サービスは全ての不正アクセスを検知するものではありません。</li> <li>本サービスは不正アクセスに関する防御を保障するものではありません。</li> <li>本サービスの内容を予告なく変更をさせていただきます。</li> </ul>

## 8. サービス運用形態

### 8.1. サービス体制



### 8.2. サービス提供用アクセス経路（アドレス帯、ポート）

障害・定常作業代行を実施する際に、JIG-SAW よりお客様環境へアクセスするため以下の接続元IPアドレスから作業に必要なポートの許可設定が必要となります。

- 221.245.250.58/32
- 210.229.179.170/32
- 211.128.86.128/27
- 203.141.136.194/32
- 124.38.245.90/32
- 221.115.122.18/32

監視システム（puzzle）を利用する際、監視対象サーバから下記 IP アドレスおよびポート番号に対して、Outbound のインターネット接続が可能であることが必要となります。

通信は TLS 接続により暗号化（AES256）されるため監視データを盗聴される恐れはありません。

接続先IPアドレス	接続先ポート番号	備考
211.128.86.141	TCP 443	主経路
221.245.235.253	TCP 443	副経路

### 8.3. サービス開始時の提供物

作業依頼用フォーム画面ログイン情報（Backlog）

### 8.4. サービス対応時間

区分	項目	対応時間	リードタイム
初期設定	受付	24時間365日	翌3営業日
	Mackerelライセンス発注作業	毎日 9:00-18:00	即日
	（監視オプション）監視環境初期設定	毎日 9:00-18:00	5営業日程度
監視	監視	24時間365日	-
問い合わせ	本サービスに関する問い合わせ	毎日 9:00-18:00	-
	障害に関する問い合わせ	24時間365日	-
	作業依頼	24時間365日	3営業日以内に実施
報告	Webポータルサイト	24時間365日	-

### 8.5. お問い合わせ先

本サービスに関するお問い合わせは以下の窓口をお願いいたします。

障害・定常作業依頼の連絡は、連絡用ツールにて行います。

サービス開始前のお問い合わせ	営業部	aws-sales@classmethod.jp
サービス開始後のお問い合わせ	AWS オペレーションチーム	メンバーズポータルサイトのお問い合わせフォームをご利用ください

電話でのお問い合わせは受け付けておりません。

## 9. セキュリティとサービス品質

## 9.1. 監視システムのセキュリティ対策

- お客様AWS環境から監視システムへの通信は TLS 接続により暗号化 (AES256) されています。
- ブラウザによるWebポータルサイトへのアクセスはHTTPSを利用してあります。
- Webポータルサイトへログインするためのパスワードについては暗号化してデータベースに格納されます。
- 監視システムへのログインアカウントは徹底した管理と運用を実施してあります。
- 監視センターは、特定の者のみ許可される入室制限、入退室記録、監視カメラによる管理を行っております。

## 9.2. お客様AWS環境のセキュリティ対策

- 監視対象サーバーとCloudWatchエンドポイント間の通信はHTTPSで暗号化されています。
- 監視対象サーバーにログイン作業する場合はsshまたはRDPを利用し通信は暗号化されています。

## 9.3. 情報セキュリティ

お客様から提供いただいた各種情報は、ISMS の情報資産管理規定に則り、適切に管理いたします。

## 9.4. メンテナンスによるサービス一時停止

障害発生等によるサービス停止の他、監視システム等のメンテナンス時 (AWSインフラ要因を含む監視設備メンテナンス、監視項目の追加、変更など) に一時的にサービスが停止する場合があります。

サービス停止日時が特定できる場合のみ、予めお客様連絡先へご連絡いたします。

## 改訂履歴

版数	日付	改訂履歴
初版	2018/08/28	初版作成
第二版	2019/07/08	文言修正 (フットモニタリング、フットオペレーション)
第三版	2019/07/30	5.6. 連絡用ツール を追加
第四版	2019/08/01	3.3. 二次対応 を追加
第五版	2020/02/18	サービス内容見直しにより該当箇所を修正
第六版	2020/03/31	Fargate に関する課金単位を修正

## リンク

[1] Backlog, <https://backlog.com/ja/>