メンバーズサービス仕様書

リリース ***2024-05-29***

Classmethod, Inc.

2024 年 05 月 29 日

目 次

第1章　はじめに

1.1 目的

このドキュメントでは、クラスメソッドメンバーズ（以下、メンバーズ）が提供する各種サービスの仕様について説明します。

記載範囲については、次のとおりとなります。

- メンバーズの概要
- メンバーズが提供する各種サービス
- 各種サービスが作成・管理する AWS リソース

1.2 対象

本書は次の利用者を対象としています。

- メンバーズに所属する AWS アカウントの管理者
- メンバーズが提供する各種サービスの利用者

1.3 構成

このドキュメントは次の構成となります。

- メンバーズの概要
  - メンバーズの基本サービスや構成システム、料金についての説明を行います
- 各種サービス情報
  - メンバーズに付随する各種サービスやオプション、そのほか当社で提供しているサービスについてご案内します
- 作成される AWS リソース
  - メンバーズに加入することで作成される AWS リソースについての説明を行います
  - 各リソースの役割や変更の可否、注意点などを説明します

第2章　メンバーズの概要

メンバーズは、クラスメソッド株式会社（以下、当社）が提供する AWS クラウド環境に対する総合支援サービスです。メンバーズのご利用開始に際しましては、本書と併せて クラスメソッドメンバーズ利用規約 もご確認下さい。

本サービスでは、お客様に対して AWS 利用費の割り引きやセキュリティチェック、技術サポートなどを提供しています。プレミアムサービスに加入した場合、AWS に関する技術コンサルティングや構築支援、24/365 での運用監視サービスなどもご利用いただけます。

また、上記のほかに当社が提供する AWS に関連した各種サービスをご利用いただけます。

2.1 構成

ここでは、メンバーズを構成する各要素について説明します。

2.1.1 システム構成

メンバーズサービスは主に次の三種類のシステムで構成されています。

- メンバーズポータル
- 請求システム
- アカウントメンテナンスシステム

それぞれのシステムと提供されるサービスの構成は以下となります。

ここからは、各サービスの主な役割について説明します。

メンバーズポータル

お客様の管理する AWS アカウントの一覧や利用状況、RI の期限切れチェックなどの情報を提供します。また、メンバーズに関するお知らせや、技術的な問い合わせ・申請依頼を行うための問い合わせフォームなども提供しています。

メンバーズポータルへのアクセスは次の URL から行えます（アクセスには専用の ID ／パスワードが必要です）。

- https://members.classmethod.net

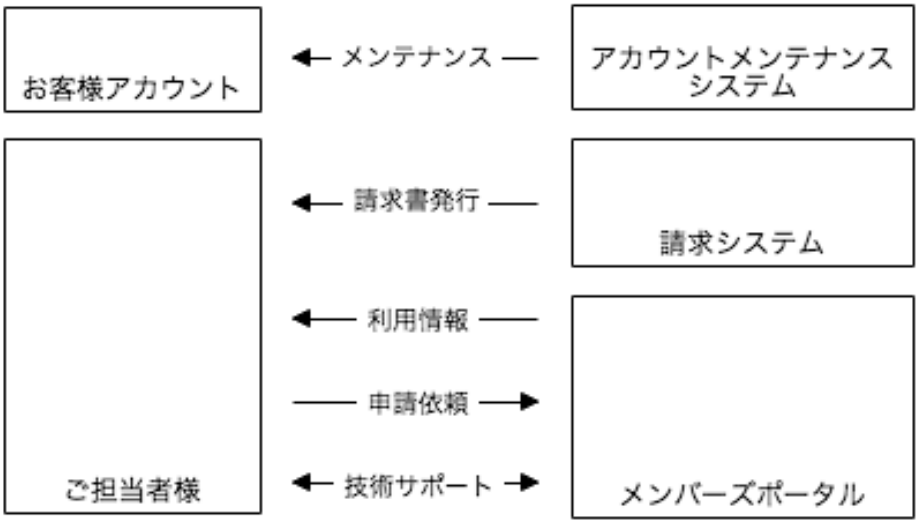

図 1: サービスの構成

請求システム

AWS 利用費や割り引き額、各種オプション利用料の集計を行い、その結果をもとにお客様へ請求書発行を行います。

アカウントメンテナンスシステム

AWS アカウントに対して、メンバーズをご利用いただくためのメンテナンスを行います。メンバーズ加入時に行われる初回メンテナンス（初期設定）と、週末に行われる定期メンテナンスの二種類があります。

メンテナンスにより、お客様の AWS アカウントには各種サービスを利用するための AWS リソースが作成されます。利用可能なサービス、および AWS リソースの詳細については、以下をご確認ください。

- 各種サービス情報
- 作成される *AWS* リソース

2.1.2 AWS アカウントと「組織」について

ご契約いただくプランによって AWS Organizations の利用可否を選択いただけます。

主に「一律割引プラン v2（7%）、クレジットカードプラン v2（4%）、バウチャープラン v2（7%）、 EC2・CDN 割引プラン」（以下、まとめて「標準プラン」と呼称）か、「組織管理プラン v2（4 %）」かによって分かれます。

※メンバーズのプランについては **参考資料** または AWS 総合支援サービス「クラスメソッドメンバーズ」を参照してください。

プランの総称	標準プラン	組織管理プラン
含まれるプラン	・一律割引プラン v2（7%） ・クレジットカードプラン v2（4%） ・バウチャープラン v2（7%） ・EC2・CDN 割引プラン	・組織管理プラン v2（4 %）
AWS Organizations の利用	不可	可能

標準プランの場合

標準プランでは、お客様の AWS アカウントは、当社が管理する AWS Organizations 上の「組織」に所属するメンバーアカウントとなります。これら AWS アカウントは、クロスアカウント機能によって、複数の AWS アカウントを連携させることが可能です。また、プランは AWS アカウント単位で選ぶことができます。

管理アカウントは当社が管理するため、「組織」や管理アカウントを意識することなく、AWS クラウド環境をご利用いただくことが可能です。

その他、作成される AWS リソースや制限事項の詳細は以下をご確認ください。

- **作成される *AWS* リソース**
- **【標準プラン】制限事項**

組織管理プランの場合

組織管理プランでは、お客様はメンバーアカウントとあわせて管理アカウントも使用できます。そのため、AWS Organizations を前提としたマルチアカウント管理・機能をご利用いただけます。なお、組織管理プランの場合、同じ「組織」内のメンバーアカウントは、全て同じプランしか選ぶことができません。

その他、作成される AWS リソースや制限事項の詳細は以下をご確認ください。

- **作成される *AWS* リソース** （ **【組織管理プラン】補足事項** を含む）
- **【組織管理プラン】制限事項**

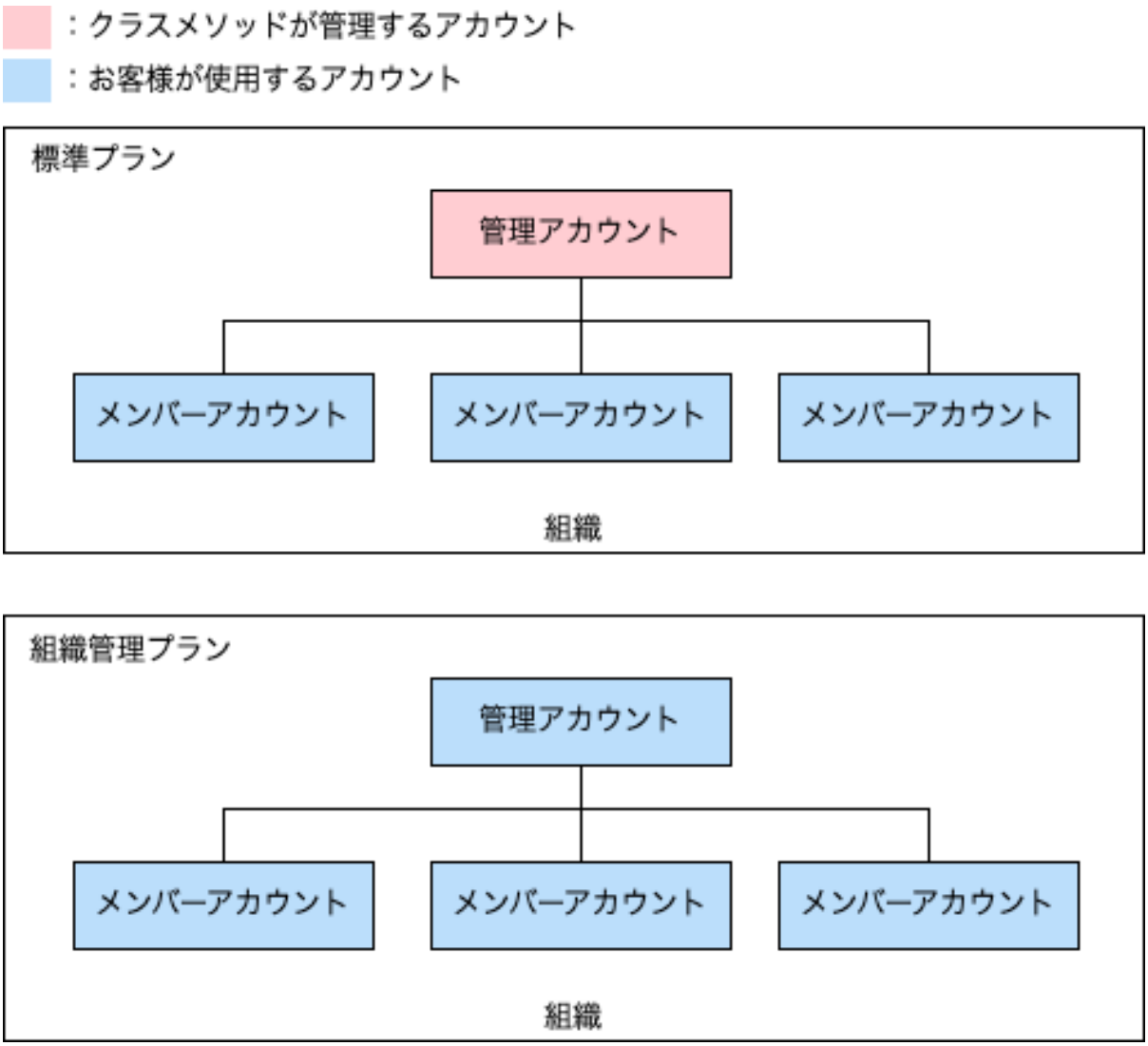
：クラスメソッドが管理するアカウント
：お客様が使用するアカウント
標準プラン
管理アカウント
メンバーアカウント
メンバーアカウント
メンバーアカウント
組織
組織管理プラン
管理アカウント
メンバーアカウント
メンバーアカウント
メンバーアカウント
組織

図 2: 構成図

2.2 料金

ここでは、メンバーズに所属する AWS アカウントの料金および請求について説明します。

2.2.1 料金および請求書発行

月毎の AWS 利用費が確定した場合、AWS から各アカウントへの請求処理は当社が一括して代行します。

当社からは、各アカウントの利用費に対し割り引きを適用した後、プレミアムサービスの手数料やその他サービス利用費などをまとめた請求書をプロジェクト単位で発行します。

割り引きの適用は、料金確定後の請求の際に行われます。割り引き額の詳細については次のリンクよりご確認ください。

- https://classmethod.jp/services/members/invoice/

現在実施中のキャンペーンにつきましては次のリンクよりご確認ください。

- https://docs.classmethod.jp/tos/cm_members_campaign.pdf

メンバーズにおける料金請求の流れは次のとおりです。

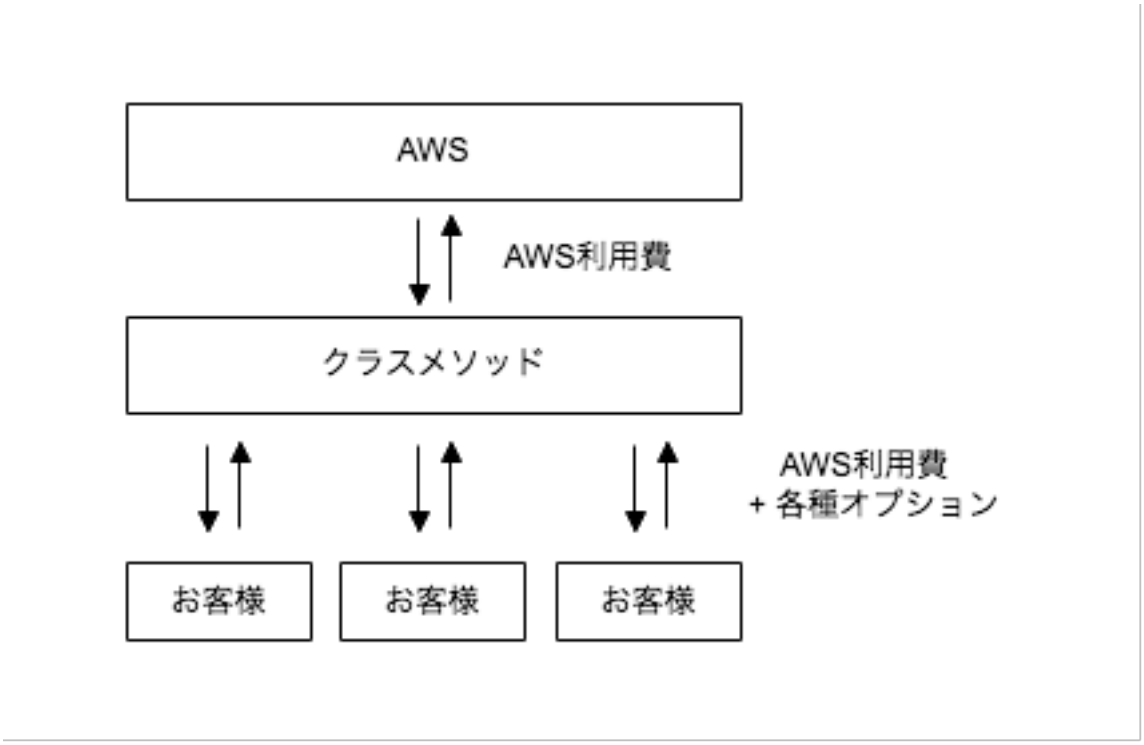

図 3: 料金請求の流れ

2.2.2 料金の確認方法

AWS アカウントの利用費については、 メンバーズポータル よりご確認いただけます。

メンバーズに加入した場合、AWS アカウントが AWS Organizations 上の組織の所属となる関係から、AWS 上の利用額（マネジメントコンソール、Cost Explorer 等およびそれらに関する API）と実際の利用額が異なります。また不定期に AWS アカウントの組織を変更することがございます。その場合 AWS 上の過去の料金情報にアクセスできなくなります。そのため、実際の利用額についてはメンバーズポータルよりご確認ください。なおメンバーズポータルへの料金反映はマネジメントコンソール等より遅れることがあります。

2.2.3 AWS とメンバーズポータルとの料金の差異について

AWS の利用料金については AWS マネジメントコンソール等でもご確認いただけますが、メンバーズポータル上の金額と異なる場合があります。この金額差は、主に AWS Organizations の一機能である「組織の一括請求」の影響により発生します。

「組織の一括請求」の下ではリザーブドインスタンス（RI）および Savings Plans（SP）はアカウント間で共有されます。その際、余剰となった RI・SP は購入者以外のアカウントに対してランダムに適用されます。また、ボリュームディスカウントについても同様に全体の利用量に応じて変化するため、個別アカウントで規定量に満たない場合でも割り引きを受ける場合があります。

メンバーズポータルではこれらの割り引きを通常価格に戻したうえで、当社規定の割り引きプランを適用しています。結果として AWS マネジメントコンソール等よりも高い金額が表示されますが、お客様のメンバーズポータルでの利用料金は通常の AWS の利用料金をベースとしたものであることをご了承ください。

「組織の一括請求」についての詳細は、以下をご確認ください。

- 組織の一括請求について
- ボリューム割引
- リザーブドインスタンス
- Savings Plans

2.2.4 AWS 利用費の換算レートと支払い

AWS 利用費の日本円での請求費用の算出方法は次のとおりとなります。

- 換算レートは、三菱 UFJ リサーチ&コンサルティングの 月中平均 TTS（MonthlyAverageTTS） に準拠します
- 円換算後、一円未満切り捨てとなります

2.2.5 AWS Marketplace でのサードパーティーコンテンツの購入について

お客様は、メンバーズに所属する AWS アカウントを介して、サードパーティーが AWS Marketplace に出品するソフトウェア、サービス等（以下、サードパーティーコンテンツ）を購入することができ、この場合、AWS Marketplace の利用については AWS が定める AWS Customer Agreement、AWS Service Terms、及び Privacy Notice が適用されます。

サードパーティーコンテンツは、サードパーティーが定める EULA、その他の利用規約等に基づきお客様へ直接利用許諾されます。AWS Marketplace の購入手順に従い、サードパーティーが定める利用規約等にお客様が同意することが、ご購入の条件となります。

メンバーズに所属する AWS アカウントを介して、お客様が AWS Marketplace でサードパーティーコンテンツを購入された場合、クラスメソッドは、その購入金額に課税される税金を加算してお客様に請求します。

2.3 利用している AI サービス

ここではメンバーズサービスのサポート窓口運用のために利用している AI サービスを説明します。

- Amazon Bedrock
  - お客様よりいただいたご質問への回答、および回答内容の改善のために利用します
  - AWS の利用規約
- Azure OpenAI Service
  - お客様よりいただいたご質問への回答、および回答内容の改善のために利用します
  - Azure OpenAI Service の利用規約

2.4 利用している外部サービス

ここではメンバーズサービス運用のために利用している外部サービスを説明します。

- Zendesk
  - サポート窓口の運用に利用しています
  - Zendesk の利用規約

第3章　各種サービス情報

メンバーズにご加入のお客様へ提供する主なサービスの一覧です。各サービスはお客様の契約状況によって利用できるものと、そうでないものがあります。

メンバーズのサービス体系については AWS 総合支援サービス「クラスメソッドメンバーズ」 を参照してください。

3.1 提供されるサービス

メンバーズのどのプランでも提供される基本的なサービスです。

3.1.1 サポート窓口

テクニカルサポート、カスタマーサポートをご提供します。AWS に関する技術的なお問い合わせ、ベストエフォートでのサードパーティアプリケーション（一般的な OS・DB・Web サーバー）、発生している障害に関してはテクニカルサポート窓口で対応します。また、メンバーズに関する請求・契約変更、AWS 上限緩和申請、新規 AWS アカウント発行などテクニカルサポート以外の問い合わせについてはカスタマーサポート窓口で対応します。

- 費用
  - 無料
- 申込方法
  - お申込みは不要です
- 受付時間
  - テクニカルサポート：24 時間 365 日（英語／日本語）
  - カスタマーサポート：平日 9:00〜18:00（日本語）
- 初回応答目標時間（テクニカルサポートのみ）
  - 通常のお問い合わせ：24 時間以内
  - 障害／開発中の急ぎの問い合わせ：12 時間以内
  - 発生中の障害：4 時間以内
  - 発生中の障害（ビジネスへの影響大）：1 時間以内
- 利用方法

  - メンバーズポータルからご利用いただけます

3.1.2 AWS ユーザー向け保険

AWS の障害に起因する損害賠償責任に対する補償や損害発生時にかかる各種費用に対する補償、情報漏えいにかかる各種費用に対する補償などに対応します。加入者による保険加入手続きは不要です。

- 費用
  - 無料
- 申込方法
  - お申込みは不要です
- 資料
  - クラスメソッド メンバーズ 付帯損害保険のご紹介

3.1.3 AWS アカウント初期設定／継続メンテナンス

お客様のアカウントを新規発行する際にご指定のセキュリティ設定オプション（ベーシック／セキュア）に基づいて、メンバーズ推奨の設定にて各種 AWS サービスを有効化します。また管理ポータルサイトのメンバーズサービス設定画面でオプトインすることによって、継続的にメンテナンスを実施し最新の設定に保つことができます。設定方法の詳細については メンバーズサービス設定 を参照してください。

- 費用
  - 設定費用：無料
  - 各 AWS サービスご利用料金は別途発生します
- 申込方法
  - 新規アカウント申し込みフォーム
  - 管理ポータルサイトのメンバーズサービス設定画面
- 各種ドキュメント
  - **作成される *AWS* リソース**

3.1.4 AWS マネジメントコンソール

AWS が提供している AWS マネジメントコンソール は加入後も Administrator 権限で使用できます。

- 費用
  - 無料
- 申込方法

  - お申し込みは不要です。メンバーズ契約時に権限が付与された AWS アカウントを発行します

- 備考
  - 既存の AWS アカウントをメンバーズに移管した場合、作成済みの IAM ユーザーなどは引き続きご利用いただけます

3.1.5 管理ポータルサイト

料金明細やお問い合わせ、各種設定を行う、クラスメソッドメンバーズポータル（CMP） を提供します。詳細は、CMP の ユーザーガイド をご覧ください。

- 費用
  - 無料
- 申込方法
  - お申し込みは不要です。メンバーズ契約時に CMP アカウントを発行します

3.1.6 AWS 申請代行

ELB の暖機、上限緩和、負荷テストなど各種 AWS の申請を、弊社オペレーターが代行します。

- 費用
  - 無料
- 申込方法
  - CMP の お問い合わせ より申し込みください

3.1.7 コストと使用状況レポート（CUR）

AWS で利用されたサービスの利用量とコストについての時間単位での明細です。CSV 形式で、おおむね 1 日 2 回、所定の S3 バケットへ出力されます。

- 費用
  - 設定費用：無料
  - S3 のストレージ料金が別途発生します
- 申込方法
  - CMP の ユーザーガイド をご参照ください

3.1.8 AWS アカウントの追加

AWS アカウントの追加については、下記のガイドをご参照ください

- AWS アカウントの追加方法を教えてください

3.1.9 Classmethod Cloud Guidebook（CCG）

Classmethod Cloud Guidebook（CCG）は組織内における AWS ガバナンスの支援を目的としています。複数の AWS 活用時の管理方法やセキュリティ対策の検討・判断に役立つ情報をまとめています。

- 費用
  - 無料
- 申込方法
  - お申し込みは不要です。メンバーズ契約時に発行するクラスメソッドメンバーズポータル（CMP）アカウントを利用します
- 利用方法
  - Classmethod Cloud Guidebook にクラスメソッドメンバーズポータル（CMP）のユーザー名/パスワードを入力してログインしてください
- 各種ドキュメント
  - クラスメソッドメンバーズのお客様向けに公開している「Classmethod Cloud Guidebook (CCG)」の使い方 | DevelopersIO

3.2 プレミアムサービス（基本）

プレミアムサービスで提供されるサービスです。弊社の子会社である代理店を通じて申し込みを行う場合にはご利用いただけませんので、予めご了承ください。

3.2.1 RI・SP 購入代行

リザーブドインスタンス（RI）および Savings Plans（SP）の購入を、弊社オペレーターが代行します。

- 本サービスの対象
  - リザーブドインスタンス
    - EC2
    - RDS
    - Redshift
    - ElastiCache

        - OpenSearch Service (旧 Elasticsearch Service)
    - Savings Plans
        - Compute Savings Plans
        - EC2 Instance Savings Plans
- 費用
    - 無料
- 申込方法
    - CMP の お問い合わせ より申し込みください
- 各種ドキュメント
    - リザーブドインスタンス（RI）購入の流れ
    - Savings Plans（SP）購入の流れ
- 制限事項
    - 代理購入は弊社営業日の実施となります
    - 購入内容の確定および弊社での確認が完了して 3 営業日後が最短の購入日となります
    - 営業日以外の購入をご希望の場合は、正常に購入が完了しているかを当日に確認できません
        - 次営業日に購入確認し、購入できていなかった場合はその日中に購入いたします
    - 購入する時間はご指定いただけません
    - 購入完了後にお客様側でも購入内容のチェックをお願いいたします
    - 止むを得ない事情により購入日が変更になる場合があります
        - 例）購入予定だったインスタンスタイプの廃止
        - 例）AWS 障害により当日購入ができなかった
    - AWS の価格改定によりご依頼時と購入時で金額が異なった場合は、購入時の金額を正とします
    - AWS のサービス仕様により、購入後のキャンセルはできません
    - RI や SP の残債がある場合は AWS アカウントの解約ができなくなります
    - 購入した RI・SP をマーケットプレイスで売却することはできません

3.2.2 IAM ユーザー作成代行

IAM ユーザーの作成を弊社オペレーターが代行します。また同時に、IAM グループの作成と割り当ても可能です。

- 費用
  - 無料
- 申込方法
  - CMP の お問い合わせ より申し込みください
- 作業範囲外の項目
  - IAM ポリシーの作成
  - アクセスキーの生成

3.2.3 AWS 利用改善レポート

お客様 AWS 環境の利用状況を分析し、コストとセキュリティに関しての改善提案をメールで通知します。

- 費用
  - 無料
- 申込方法
  - お申込みは不要です
- チェック項目
  - 使用率の低い Amazon EC2 インスタンス
  - 利用頻度の低い Amazon EBS ボリューム
  - 使用率の低い Amazon Redshift クラスター
  - 無制限にアクセスを許可しているセキュリティグループ
  - IAM パスワードポリシー
  - AWS CloudTrail ロギング
  - IAM ユーザの MFA
  - アクセスキー漏洩時のリスクが高い IAM ユーザ
  - 各種ログ設定（ELB ／ CloudFront ／ S3 静的ウェブサイトホスティング）

3.3 プレミアムサービス（オプション）

プレミアムサービスに追加できるオプションサービスです。弊社の子会社である代理店を通じて申し込みを行う場合にはご利用いただけませんので、予めご了承ください。

3.3.1 AWS コンサルティング

弊社エンジニアをアサインし、お客様の AWS 環境をサポート・コンサルティングをします。また AWS を新規に導入される場合も不明点や懸念事項を解決する提案を行い、構築支援や運用支援、運用コストの最適化も合わせてコンサルティングします。

- サービス概要およびお問い合わせ

3.3.2 AWS 環境構築

弊社エンジニアによる AWS 環境の構築作業を実施します。AWS クラウド環境の設計、環境構築に関わる各種手続き代行、サーバー OS に関する初期設定、ミドルウェアの初期インストール、AWS 環境と環境定義書のご提供までを行います。

3.3.3 監視オプション

24 時間 365 日体制でシステムの無人監視を行うサービスです。簡単な設定をしていただくだけで導入でき、AWS 環境の安定稼働、障害復旧の高速化を実現します。月額費用であるホスト数の計算は Mackerel に準拠します。詳細は各種ドキュメントのリンク先の FAQ を参照してください。

- サービス概要およびお問い合わせ
- 各種ドキュメント
  - 利用規約 （更新日：2020/10/15）
  - サービス仕様 （更新日：2019/05/01）
  - ご利用の手引き（マニュアル） （更新日：2022/01/18）
  - 請求対象となるホスト数の計算方法について （Mackerel のサイトが開きます）
  - プラン上限超過時のホスト台数換算について （Mackerel のサイトが開きます）

3.3.4 脆弱性診断オプション

OS/ミドルウェア/Web アプリケーションの脆弱性や設定不備を識別する脆弱性診断サービスです。

- サービス概要およびお問い合わせ

3.3.5 フルマネージド DeepSecurity オプション

Trend Micro Cloud One Workload Security を利用したセキュリティ監視運用サービスです。Workload Security のログを株式会社アズジェントのセキュリティ監視センターにて 24 時間／ 365 日監視します。

- サービス概要およびお問い合わせ
- 各種ドキュメント
  - サービス仕様書 （更新日：2020/03/31）

3.3.6 AWS 技術アドバイザー

AWS プロフェッショナル資格をもつエンジニアがお客様の専任となり、AWS に関するアドバイスや各種相談に対応します。お客様が AWS 環境を自ら効率的に運用していくことを支援するために、オンラインミーティングを実施します。その場で Q&A を実施し、豊富なノウハウから即時ご回答します。

- サービス概要およびお問い合わせ

3.3.7 運用代行オプション

24 時間 365 日の有人監視・運用代行・障害対応をワンストップで代行するサービスです。事前のヒアリングシートの内容に基づき、高度な専門知識を持ったエンジニアが作業を実施します。

- サービス概要およびお問い合わせ
- 各種ドキュメント
  - サービス仕様書 `JIG-SAW` 版 （更新日：2020/03/31）
  - サービス仕様書 運用アシスタント版 （更新日：2020/10/01）

3.3.8 AWS トレーニングサービス

AWS から認定を受けた弊社トレーナーが AWS 公式トレーニングをお客様にご提供します。

- 各種ドキュメント
  - サービス概要およびお申し込み方法

3.3.9 セキュアアカウント インシデント自動調査機能

お客様のセキュリティ運用を支援するための、クラスメソッドメンバーズのオプションサービスです。現状では AWS の脅威検知サービスである GuardDuty について、クラスメソッドの知見を提供しつつ、1 次調査を支援しお客様の AWS セキュリティに関するナレッジ・人的コストの削減を支援します。

- 各種ドキュメント
  - セキュアアカウント インシデント自動調査機能サービス仕様書
- 申込方法
  - 導入をご検討のかたは お問い合わせ からご連絡ください

3.3.10 モダンアプリコンサルティング

AWS にも精通した開発エンジニアが、お客様のクラウドネイティブなアプリケーション開発の内製化をご支援します。

- サービス概要およびお問い合わせ

3.3.11 スタートパッケージ for Amazon Connect

予めパッケージ化されたクラウドコンタクトセンター環境一式を短納期でご提供するサービスです。

- サービス概要およびお問い合わせ

3.4 その他

3.4.1 opswitch（オプスイッチ）

AWS リソースに対してよく行う処理にスケジュールを設定し、定期的に自動実行する Web サービスです。

- 費用
  - 無料
- 申込方法
  - お申込みは不要です。 こちら よりアカウントを作成しご利用開始できます
- 各種ドキュメント
  - 利用規約
  - ユーザーガイド
  - FAQ
  - お問い合わせ

第4章　作成されるAWSリソース

メンバーズでは、セキュリティおよびメンバーズサービス提供のためいくつかの AWS サービスを有効化しリソースを作成します。このドキュメントではメンバーズご契約時に作成される主なリソースを説明します。

リソースには CM 管理リソースとオプションリソースの 2 種類があります。

CM 管理リソースについては、お客様で削除および変更はできません。

オプションリソースはセキュリティ設定オプションによって設定される内容が異なります。メンバーズでは初期設定時に「ベーシック」か「セキュア」を選択できます。このドキュメントでは共通のものと個別のものでそれぞれ説明します。それらのリソースについては、お客様の判断で設定変更や削除をしても問題ありません。

ベーシック設定では次のリソースを初期設定で有効化します。

- メンバーズ基本サービスの各種リソース
- ベーシック設定の各種リソース

セキュア設定では次のリソースを初期設定で有効化します。

- メンバーズ基本サービスの各種リソース
- セキュア設定の各種リソース

初期設定で有効化するいくつかのリソースについて、メンバーズポータル上のメンバーズサービス設定画面でオプトインを提供しています。オプトインすると、メンテナンス時にそのリソースを再有効化および一部設定をメンバーズの推奨設定に上書きします。そのため、お客様独自の設定を行う場合、オプトインしないことを推奨します。オプトインに対応しているリソースには オプトイン ラベルを付与しています。

- ベーシック設定ではオプトインは **デフォルト OFF** となっています
- セキュア設定ではオプトインは **デフォルト ON** となっています
- ベーシック設定でアカウントの初期設定を行なった場合でも、セキュア設定のリソースをオプトイン可能です

特殊なリソースにはラベルを付与しています。ラベルのないリソースは初期設定となり、お客様独自の設定が可能です。AWS 上のタグ設定が可能なリソースには、次のタグが設定されています。

- `CM` 管理 ラベル
  - メンバーズサービスを提供する上で必須のリソース。設定変更などを行うとサービス提供に支障が出る可能性があります
  - cm:Members=Managed

- ラベルのないリソース
  - アカウント提供時に有効になっているリソース
  - ベーシック設定および共通で有効化されるリソース
    - cm:Members=Initialized
  - セキュア設定で有効化されるリソース
    - cm:Members=SecureAccount

4.1 メンバーズ基本サービス

4.1.1 AWS Identity and Access Management（IAM）

ユーザー

次のような初期ユーザーが作成されています。新しいユーザーを作成したあとであれば削除しても問題ありません。

- initial-admin-user-<アカウント ID>
  - 「admin-group-<アカウント ID>」グループに追加

グループ

次のような初期グループが作成されています。適切なポリシーがアタッチされたユーザーやグループを作成したあとであれば削除しても問題ありません。

- admin-group-<アカウント ID>
  - 「AdministratorAccess」ポリシーをアタッチ

ロール

- AWSServiceRoleForOrganizations
  - メンバーズでは AWS Organizations を利用しており、お客様のアカウントはメンバーアカウントとして作成しています。このロールは AWS によってメンバーアカウントに自動的に作成されます
  - AWS Organizations の仕様で削除することはできません
- `CM` 管理 cm-helpdesk
  - 弊社オペレーションチームがお客様環境へアクセスするために使用します
  - 作業の実施にあたり、一時的にポリシーの修正を行うことがあります

  - アタッチされている AWS 管理ポリシー
    - ReadOnlyAccess
  - アタッチされているインラインポリシー
    - ContentProtectedReadOnlyPolicy
    - ExplicitDenyActionPolicy
    - RIPurchasePolicy
    - ViewBillingPolicy
    - OrganizationMovingPolicy

- CM 管理 cm-membersportal
  - メンバーズポータルがお客様環境へアクセスするために使用します
  - アタッチされている AWS 管理ポリシー
    - ReadOnlyAccess
  - アタッチされているインラインポリシー
    - ContentProtectedReadOnlyPolicy
    - ExplicitDenyActionPolicy
    - OrganizationAccountAccessPolicy

- CM 管理 cm-policymaintainer
  - IAM ロール、ポリシーおよびメンバーズサービスで有効にしているサービスのメンテナンスを実施するために使用します
  - アタッチされているインラインポリシー
    - CMMaintenancePolicy

- CM 管理 cm-config-role-all-regions
  - AWS Config で使用します
  - アタッチされている AWS 管理ポリシー
    - AWS_ConfigRole
  - アタッチされているインラインポリシー
    - CMConfigPolicy

アカウント設定

- オプトイン パスワードポリシー
  - パスワードの最小長
    - 8 文字
  - 少なくとも 1 つの大文字が必要
    - ON
  - 少なくとも 1 つの小文字が必要
    - ON
  - 少なくとも 1 つの数字が必要
    - ON
  - 少なくとも 1 つの英数字以外の文字が必要
    - ON
  - ユーザーにパスワードの変更を許可
    - ON

4.1.2 Amazon S3

S3 バケットを誤って公開しないようにアカウントレベルのパブリックアクセスブロックを設定します。

このアカウントのブロックパブリックアクセス設定

- パブリックアクセスをすべてブロック
  - オン

4.1.3 AWS CloudFormation

スタック

次の CloudFormation スタックが作成されています。こちらは AWS アカウント新規発行時に「お客様向け IAM ユーザー」「管理者権限 IAM グループ」を作成する際に弊社で作成したものです。不要でしたら削除して問題ありません。

- cm-Initial-IAM

4.1.4 オプトイン AWS Compute Optimizer 有効化

アクティブな各リージョンで有効化します。

Compute Optimizer

- オプトイン
  - 有効

IAM ロール

- AWSServiceRoleForComputeOptimizer
  - Compute Optimizer で使用します

4.1.5 オプトイン AWS IAM Access Analyzer 有効化

アクティブな各リージョンで有効化し、次の設定を行います。

アナライザー

- cm-access-analyzer
  - タイプ
    - アカウント

アーカイブルール

- ArchiveRule-CmHelpdesk
  - リソース
    - cm-helpdesk
- ArchiveRule-CmMembersportal
  - リソース
    - cm-membersportal
- ArchiveRule-CmPolicymaintainer
  - リソース
    - cm-policymaintainer

IAM ロール

- AWSServiceRoleForAccessAnalyzer
  - IAM Access Analyzer で使用します

4.2 ベーシック設定

4.2.1 オプトイン AWS CloudTrail 有効化

東京リージョンで「すべてのリージョンに適用される証跡」を作成し有効化します。証跡は各リージョンに対して 5 個が上限となっています。そのためすでに上限の証跡が存在している場合、証跡は作成されません。証跡を新たに作成するためには、既存の証跡を 5 個未満にする必要があります。また S3 バケットを作成するため、バケット数が上限となっている場合は不要なバケットを削除するか上限緩和の申請を行ってください。次の設定を行います。

CloudTrail 証跡

- Members
  - Trail settings
    - 証跡情報を全てのリージョンに適用
      - Yes
  - 管理イベント
    - 読み込み/書き込みイベント
      - すべて
  - ストレージの場所
    - S3 バケット
      - cm-members-cloudtrail-<アカウント ID>
  - ログファイルの検証を有効化
    - はい

S3 バケット

AWS CloudTrail のログ配信先として東京リージョンに作成します。

- cm-members-cloudtrail-<アカウント ID>
  - パブリックアクセスのブロック（バケット設定）
    - パブリックアクセスをすべてブロック
      - オン
  - バケットのバージョニング
    - 有効
  - デフォルトの暗号化
    - サーバー側の暗号化
      - 有効
    - 暗号化キータイプ
      - Amazon S3 マネージドキー（SSE-S3）
  - オブジェクトロック
    - デフォルトの保持期間
      - 1 年
    - デフォルトの保持モード
      - コンプライアンス
  - リクエスタ支払い
    - リクエスタ支払い
      - 無効
  - ライフサイクルルール
    - オブジェクトの完全削除
      - 3 年後
    - 不完全なマルチパートアップロード
      - 7 日後

4.2.2 オプトイン AWS Config 有効化

アクティブな各リージョンで AWS Config を有効化します。また S3 バケットを作成するため、バケット数が上限となっている場合は不要なバケットを削除するか上限緩和の申請を行ってください。

AWS Config 配信チャネルおよび設定レコーダー

- default
  - 配信チャネル
    - S3 バケット
      - cm-members-config-<アカウント ID>
  - 設定レコーダー
    - IAM ロール
      - cm-config-role-all-regions
    - 記録するリソースタイプ
      - 詳細は次項をご確認ください

記録するリソースタイプ

ベーシック設定では一部のリソースのみを記録します。リソースタイプには特定リージョンのみ記録可能なものがあります。また、グローバルリソース（AWS IAM リソースなど）は東京リージョンのみ記録します。

- 東京
- バージニア北部
- オレゴン
- その他のリージョン

AWS Config に関する注意点

記録対象となっているリソースは、あくまでメンバーズの初期設定となります。セキュリティをより強化する目的で記録対象を追加する（あるいは **すべてのリソース** を記録対象とする）ことは問題ありません。その場合、AWS Config の利用費も増加するため注意してください。

また、利用費軽減の目的で記録対象からリソースを削除する（あるいは **記録をオフ** にする）ことも問題ありません。ただし変更管理ができなくなるため、本当に削除してもよいのかは十分に検討してください。

一時的に記録対象からリソースを削除する（あるいは **記録をオフ** にする）ケースとして、検証目的などで頻繁にリソースの作成、変更、削除を行う場合が考えられます。AWS Config は **記録対象となっているリソースの変更を記録する料金** が利用費として発生するため、仮に検証目的であってもリソースの作成、変

更、削除を行うと利用費が発生します。検証時などに AWS Config の利用費が多く見込まれる場合、記録が不要なリソースを記録対象から一時的に削除することをご検討ください。

S3 バケット

AWS Config のログ配信先として東京リージョンに作成します。

- cm-members-config-<アカウント ID>
  - パブリックアクセスのブロック（バケット設定）
    - パブリックアクセスをすべてブロック
      - オン
  - デフォルトの暗号化
    - サーバー側の暗号化
      - 有効
    - 暗号化キータイプ
      - Amazon S3 マネージドキー（SSE-S3）
  - リクエスタ支払い
    - リクエスタ支払い
      - 無効
  - ライフサイクルルール
    - オブジェクトの完全削除
      - 3 年後
    - 不完全なマルチパートアップロード
      - 7 日後

4.3 セキュア設定

4.3.1 AWS Key Management Service (KMS)

S3 バケットに保存する AWS CloudTrail および AWS Config のログを暗号化するためにカスタマーマスターキー（CMK）を作成します。

KMS キー

- alias/cm-members-logs-key
  - リージョン
    - 東京
  - キーのタイプ
    - 対称

4.3.2 デフォルト VPC 削除

意図せず必要以上の公開範囲でリソースを晒してしまう可能性があるため、アクティブな各リージョンのデフォルト VPC を削除します。

4.3.3 オプトイン AWS CloudTrail 有効化

東京リージョンで「すべてのリージョンに適用される証跡」を作成し有効化します。証跡は各リージョンに対して 5 個が上限となっています。そのためすでに上限の証跡が存在している場合、証跡は作成されません。証跡を新たに作成するためには、既存の証跡を 5 個未満にする必要があります。また S3 バケットを作成するため、バケット数が上限となっている場合は不要なバケットを削除するか上限緩和の申請を行ってください。次の設定を行います。

CloudTrail 証跡

- Members
  - Trail settings
    - 証跡情報を全てのリージョンに適用
      - Yes
  - 管理イベント
    - 読み込み/書き込みイベント
      - すべて
  - ストレージの場所
    - S3 バケット
      - cm-members-cloudtrail-<アカウント ID>
  - ログファイルの SSE-KMS 暗号化
    - 有効

        * KMS エイリアス
            · alias/cm-members-logs-key
    - ログファイルの検証を有効化
        * はい

S3 バケット

AWS CloudTrail のログ配信先として東京リージョンに作成します。

- cm-members-cloudtrail-<アカウント ID>
    - パブリックアクセスのブロック（バケット設定）
        * パブリックアクセスをすべてブロック
            · オン
    - バケットのバージョニング
        * 有効
    - デフォルトの暗号化
        * サーバー側の暗号化
            · 有効
        * 暗号化キータイプ
            · AWS Key Management Service キー（SSE-KMS）
        * AWS KMS キー
            · alias/cm-members-logs-key
        * バケットキー
            · 有効
    - オブジェクトロック
        * デフォルトの保持期間
            · 1 年
        * デフォルトの保持モード
            · コンプライアンス
    - リクエスタ支払い
        * リクエスタ支払い
            · 無効
    - ライフサイクルルール

        * オブジェクトの完全削除
            - 3 年後
        * 不完全なマルチパートアップロード
            - 7 日後

4.3.4 オプトイン AWS Config 有効化

アクティブな各リージョンで AWS Config を有効化します。また S3 バケットを作成するため、バケット数が上限となっている場合は不要なバケットを削除するか上限緩和の申請を行ってください。

AWS Config 配信チャネルおよび設定レコーダー

- default
    - 配信チャネル
        * S3 バケット
            - cm-members-config-<アカウント ID>
    - 設定レコーダー
        * IAM ロール
            - cm-config-role-all-regions
        * 記録するリソースタイプ
            - サポートされているすべてのリソース
        * グローバルリソースを含める
            - 東京のみ有効

S3 バケット

AWS Config のログ配信先として東京リージョンに作成します。

- cm-members-config-<アカウント ID>
    - パブリックアクセスのブロック（バケット設定）
        * パブリックアクセスをすべてブロック
            - オン
    - デフォルトの暗号化
        * サーバー側の暗号化
            - 有効

        * 暗号化キータイプ
            - AWS Key Management Service キー（SSE-KMS）
        * AWS KMS キー
            - alias/cm-members-logs-key
        * バケットキー
            - 有効
    - リクエスタ支払い
        * リクエスタ支払い
            - 無効
    - ライフサイクルルール
        * オブジェクトの完全削除
            - 3 年後
        * 不完全なマルチパートアップロード
            - 7 日後

4.3.5 オプトイン Amazon EBS デフォルト暗号化の有効化

ブロックストレージである Amazon EBS をデフォルトで暗号化します。セキュアアカウント発行時のデフォルトの暗号化キーは AWS マネージドキーを指定していますが、お客様で発行したカスタマーマスターキー（CMK）に変更することも可能です。データを保管するストレージを CMK で暗号化することで、暗号化キーの削除による暗号化消去（Cryptographic Erase）が可能です。お客様が暗号化消去を行うことで、AWS 上からデータを論理的に削除したことが説明できます。安全なデータ破棄の考え方は クラウドにおける安全なデータの廃棄 も参照してください。

EBS 暗号化

- 常に新しい EBS ボリュームを暗号化
    - 有効
- デフォルトの暗号化キー
    - alias/aws/ebs

4.3.6 オプトイン Amazon GuardDuty 有効化

AWS 上の脅威検知サービスとして各リージョンで Amazon GuardDuty を有効化します。攻撃者による不正な AWS ログインやコインマイニング、S3 データ漏洩などを検知します。

GuardDuty

- S3 保護
  - 有効
- EKS 保護
  - EKS 監査ログのモニタリング
    - 有効
  - EKS ランタイムモニタリング
    - 有効
  - エージェントを自動的に管理する
    - 有効
- マルウェア保護
  - 有効
- RDS 保護
  - 有効
- Lambda 保護
  - 有効

4.3.7 オプトイン AWS Security Hub 有効化

AWS 上の危険な設定を検知するために AWS Security Hub によるスタンダードをアクティブな各リージョンで設定します。うっかり Security Group の SSH ポートを `0.0.0.0/0` で開放したり、S3 バケットを公開してしまったりという誤設定を検知します。Security Hub を有効化するためには AWS Config が有効になっている必要があります。事前に AWS Config を有効化しておくか、両方のリソースをオプトインしてください。

Security Hub 有効化にあたっては、次のドキュメントも参照してください。

- コントロール検出結果の生成に必要な AWS Config リソース
- Security Hub コントロールのリファレンス

Security Hub

- 検出結果の集約
  - 集約リージョン
    - アジアパシフィック（東京）／ ap-northeast-1
  - 将来のリージョンを自動的にリンク
    - オン
- セキュリティスタンダード
  - AWS 基礎セキュリティのベストプラクティス v1.0.0
  - 無効化項目
    - Account.1
    - IAM.6
    - EC2.8
    - CloudTrail.5
    - Config.1（東京リージョン以外）
- コントロール
  - 統合されたコントロールの検出結果
    - オン
- オートメーション
  - Suppress KMS.2 for cm-config-role-all-regions
    - RuleOrder
      - 100
    - IsTerminal
      - false
    - 条件

.

キー	演算子	値
RecordState	EQUALS	ACTIVE
WorkflowStatus	EQUALS	NEW
GeneratorId	EQUALS	aws-foundational-security-best-practices/v/1.0.0/KMS.2
ResourceId	EQUALS	arn:aws:iam::<アカウント ID>:role/cm-config-role-all-regions

        * 自動アクション

.

ASFF 属性	値
ワークフローステータス	SUPPRESSED

招待による管理者アカウントとの関連付けについて

招待による管理者アカウントとの関連付けがされていた場合、メンテナンス時に自動的に解除します。手動での関連付けを維持したい場合は、オプトインしないでください。

4.3.8 オプトイン Amazon Detective 有効化

インシデントが発生した場合に脅威を可視化するためにアクティブな各リージョンで有効化します。ログの詳細な調査や可視化を簡単に実現できます。Detective を有効化するためには GuardDuty が有効になっている必要があります。事前に GuardDuty を有効化しておくか、両方のリソースをオプトインしてください。

- Detective の前提条件と推奨事項

4.3.9 オプトイン Amazon EventBridge 有効化

Amazon GuardDuty ／ AWS Security Hub ／ AWS IAM Access Analyzer で検知した各種セキュリティアラートをメールや Slack などに転送するために作成します。通知を受け取るためには セキュリティアラート通知設定 の手順に沿って設定を行ってください。

イベントバス

- cm-security-alert-aggregator-bus
  - 整形後のセキュリティアラートを集約します
  - お客様が通知設定することで通知を受け取ることが可能です
  - 通知設定は ユーザーガイド を参照してください

ルール

- cm-guardduty-alert-rule
  - 各リージョンの GuardDuty 検知結果を集約しステートマシンに送ります
  - リージョン
    * 東京
  - ターゲット

        * cm-sharping-security-alert-machine

- cm-guardduty-<region_name>-alert-rule
  - 各リージョンの GuardDuty 検知結果を東京リージョンに転送します
  - リージョン
    * 東京以外
  - ターゲット
    * cm-guardduty-aggregate-alert-rule
- cm-securityhub-alert-rule
  - 各リージョンの Security Hub 検知結果を集約しステートマシンに送ります
  - リージョン
    * 東京
  - ターゲット
    * cm-sharping-security-alert-machine
- cm-accessanalyzer-alert-rule
  - 各リージョンの Access Analyzer 検知結果を集約しステートマシンに送ります
  - リージョン
    * 東京
  - ターゲット
    * cm-sharping-security-alert-machine
- cm-accessanalyzer-<region_name>-alert-rule
  - 各リージョンの Access Analyzer 検知結果を東京リージョンに転送します
  - リージョン
    * 東京以外
  - ターゲット
    * cm-accessanalyzer-alert-rule

AWS Step Functions ステートマシン

Amazon EventBridge から送られてきた各種セキュリティアラートを整形してメールや Slack などに転送できるフォーマットに加工します。東京リージョンに作成します。

- cm-sharping-security-alert-machine
- 整形後のセキュリティアラート転送先
  - cm-security-alert-aggregator-bus

IAM ロール

セキュア設定では各種セキュリティアラート関連リソースのため次の IAM ロールが作成されます。

- cm-alert-eventrule-role
  - 各種セキュリティアラートを検知してステートマシンに転送するルールで利用します
- cm-alert-forward-eventrule-role
  - 各種セキュリティアラートを検知して東京リージョンに転送するルールで利用します
- cm-alert-statemachine-role
  - 各種セキュリティアラートを受け取り整形するステートマシンで利用します

4.4 【組織管理プラン】補足事項

上記は組織管理プランにおける管理アカウント・メンバーアカウントについても同様ですが、いくつか補足事項がございます。

4.4.1 管理アカウント

組織管理プランの場合、お客様は管理アカウントもご利用いただけますが、セキュリティおよびメンバーズサービス提供のためいくつかの AWS サービスを有効化しリソースを作成します。

前提として、AWS Organizations はデフォルトの機能セット（すべての機能）で有効化します。

AWS Organizations 組織単位 (OU)

- `CM` 管理 MembersDefaultOU
  - Root 直下の OU はクラスメソッド管理の OU となり、当該 OU が実質的にお客様の Root としてご利用いただけます
- `CM` 管理 AllowASAOU
  - AWS Shield Advanced を利用する AWS アカウントがある場合にのみ、ご利用いただけます

- CM 管理 AccountLeavableOU
  - AWS アカウントを別の組織に移管する場合にのみ、使用します
- CM 管理 MembersControlTowerOU（※ AWS Control Tower 利用時のみ作成）
  - AWS Control Tower 登録済み OU として、当該 OU が実質的にお客様の Root としてご利用いただけます
- CM 管理 SecurityOU（※ AWS Control Tower 利用時のみ作成）
  - AWS Control Tower の基礎 OU として作成します

AWS Organizations サービスコントロールポリシー (SCP)

- CM 管理 CM-Root
  - Root に適用します
- CM 管理 CM-MembersDefaultOU
  - MembersDefaultOU に適用します
- CM 管理 CM-AllowASAOU
  - AllowASAOU に適用します
- CM 管理 CM-AccountLeavableOU
  - AccountLeavableOU に適用します
- CM 管理 CM-MembersControlTowerOU（※ AWS Control Tower 利用時のみ作成）
  - MembersControlTowerOU に適用します
- CM 管理 CM-SecurityOU（※ AWS Control Tower 利用時のみ作成）
  - SecurityOU に適用します

AWS IAM ロール

メンバーズ基本サービスの *IAM* ロール（*CM* 管理のみ） に加え、以下リソースを作成します。

- CM 管理 cm-ActAdministrator
- CM 管理 cm-ActManager
- CM 管理 cm-ActMember
- CM 管理 cm-SupportMember
  - 弊社オペレーションチームがお客様環境へアクセスするために使用します
- CM 管理 cm-managementaccount-maintainer
  - メンバーズサービスのメンテナンスを実施するために使用します

- CM 管理 cm-membersportal-billing
  - メンバーズポータルがお客様環境へアクセスするために使用します

4.4.2 メンバーアカウント

AWS Control Tower 利用時における変更点

AWS Control Tower アカウントファクトリーにより発行された AWS アカウントには、次の AWS リソースは作成・メンテナンスされません。

- AWS CloudTrail
- AWS Config
- AWS IAM ユーザー/グループ
  - initial-admin-user-<アカウント ID> および admin-group-<アカウント ID>

AWS Control Tower を利用しているかの判定にはご利用の AWS アカウント内に IAM ロール `aws-controltower-AdministratorExecutionRole` が存在するかをチェックします。

そのため AWS Control Tower を利用していないにもかかわらず、上記 AWS リソースがメンテナンスされない場合、正常に設定されるよう当該 IAM ロールを削除してください。

第5章　【標準プラン】制限事項

メンバーズに加入いただいた AWS 環境では、当社サービス提供品質の維持のため、またお客様の安全な利用のため、いくつか制限事項がございます。

5.1 メンバーアカウントに関する制限・注意事項

トラブル防止を目的として、メンバーアカウントに対し一部操作の制限を行っています。制限をしている操作は次のものです。

制限内容	対象アクション	補足
組織からの脱退	`organizations:LeaveOrganization`	
AWS Shield Advanced の有効化	`shield:CreateSubscription`	ご利用の際は、CMP の お問い合わせ より申し込みください
サポートケースの起票	`support:CreateCase`	起票を希望される場合、まずは **サポート窓口** へお問い合わせください
AWS Elemental Link の購入制限	`elemental-appliances-software:Creat` `elemental-appliances-software:Submi`	メンバーズ加入後にライブ動画送信デバイス Elemental Link をご購入頂くことはできません
AWS Artifact	`artifact:*`	AWS とお客様との間で直接の契約がある場合を除き、AWS Artifact をご利用いただくことはできません
サポートプランの変更	`supportplans:StartSupportPlanUpdate`	
EC2 の一部インスタンスタイプの起動	`ec2:RunInstances` サイズが 16xlarge 以上 or ベアメタル（サイズが metal） or P3 など P ファミリー	制限解除を希望される場合、CMP の お問い合わせ より申し込みください
Savings Plans の返却	`savingsplans:returnSavingsPlan`	

第6章　【組織管理プラン】制限事項

メンバーズに加入いただいた AWS 環境では、当社サービス提供品質の維持のため、またお客様の安全な利用のため、いくつか制限事項がございます。

6.1 メンバーアカウントに関する制限・注意事項

トラブル防止を目的として、メンバーアカウントに対し一部操作の制限を行っています。制限をしている操作は次のものです。

制限内容	対象アクション	補足
組織からの脱退	`organizations:LeaveOrganization`	
AWS Shield Advanced の有効化	`shield:CreateSubscription`	ご利用の際は、CMP の お問い合わせ より申し込みください
サポートケースの起票	`support:CreateCase`	起票を希望される場合、まずは **サポート窓口** へお問い合わせください
AWS Elemental Link の購入制限	`elemental-appliances-software:Create` `elemental-appliances-software:Submit`	メンバーズ加入後にライブ動画送信デバイス Elemental Link をご購入頂くことはできません
AWS Artifact	`artifact:*`	AWS とお客様との間で直接の契約がある場合を除き、AWS Artifact をご利用いただくことはできません
サポートプランの変更	`supportplans:StartSupportPlanUpdate`	
Savings Plans の返却	`savingsplans:returnSavingsPlan`	

6.2 管理アカウントに関する制限・注意事項

6.2.1 当社管理のメンバーアカウントについて

当社が組織管理プランを提供するために使用する AWS アカウントを作成します。当該 AWS アカウントにて発生する利用費は当社負担となります。お客様の AWS 環境への影響はございません。

6.2.2 請求関連のページについて

AWS マネジメントコンソール、および API 等によるご利用はできません。

6.2.3 制限される AWS アカウントの操作について

- 既存 AWS アカウントの招待（*InviteAccount*）
- 新規 AWS アカウントの作成（*CreateAccount*）
- 既存 AWS アカウントの離脱（*LeaveAccount*）
- AWS アカウントの代替の連絡先情報（請求・操作・セキュリティ）への登録

6.2.4 制限される管理アカウントの操作について

- 請求・料金に関する設定は変更しないでください
- **管理アカウントのクラスメソッド管理用 *IAM* ロール（*cm-XXX*）** を削除しないでください

上記が守られていない状態が発覚した場合は、IAM の Permission Boundary を使用して管理アカウントのルートユーザーにて配下の IAM ユーザーの権限を厳しく制限します。

6.2.5 管理アカウントで発生する費用について

利用料金を取得するためにデータ（CUR）を保管する費用が一定程度かかります。

6.2.6 AWS Organizations 利用における制限

組織単位（OU）利用について

- MembersDefaultOU のみを使用してください
- MembersDefaultOU の子 OU を作成して利用することは可能です
- クラスメソッド管理の OU、および付随する SCP に対して改変は行わないでください

サービスコントロールポリシー（SCP）利用について

以下に対して制限しないでください。

- ルートユーザー
- メンバーアカウントのクラスメソッド管理用 *IAM* ロール（*cm-XXX*）
- アカウント作成時、AWS の標準機能として存在する IAM ロール（OrganizationAccountAccessRole、および Control Tower 利用環境の場合は AWSControlTowerExecution も含む）

AWS Control Tower が作成するガードレール/コントロールに対しては原則上記対応は不要ですが、メンバーズサービスの提供に支障をきたした場合は削除が必要となる可能性がございます。

6.2.7 AWS Control Tower 利用における制限

- AWS Control Tower の有効化/利用開始は、お客様自身では行えません。ご希望の場合は当社にご連絡ください
- アカウントファクトリーによるメンバーアカウントの発行は、お客様自身では行えません。申込フォームで申請ください

組織単位（OU）について

- AWS Control Tower が作成する必須の OU 名は SecurityOU にする必要があります
- AWS Control Tower に登録された任意の OU として、MembersControlTowerOU のみを使用してください
- MembersControlTowerOU の子 OU を作成して利用することは可能です

6.2.8 制限や注意事項が守られていない場合

当社は上記について適切な管理が行われているかどうか定期的に監査し、違反があった場合には是正させていただく可能性がございます。

第7章　参考資料

7.1 プラン比較表

プラン名	一律割引プラン v2（7%）	クレジットカードプラン v2（4%）	バウチャープラン v2（7%）	EC2・CDN 割引プラン	組織管理プラン v2（4％）
プランの総称	標準プラン	標準プラン	標準プラン	標準プラン	組織管理プラン
管理アカウントのルートユーザー管理者	クラスメソッド	クラスメソッド	クラスメソッド	クラスメソッド	クラスメソッド
メンバーアカウントのルートユーザー管理者	クラスメソッド	クラスメソッド	クラスメソッド	クラスメソッド	クラスメソッド
メンバーズ支払い方法	銀行振込	クレジットカード	バウチャー（前払い）	銀行振込	銀行振込
総額からの割引	総額から 7% 割引	総額から 4%割引	総額から 7% 割引	適用なし	総額から 4% 割引
EC2 オンデマンド割引	適用なし	適用なし	適用なし	適用あり	適用なし
データ転送割引	適用なし	適用なし	適用なし	適用あり	適用なし
S3 割引	適用なし	適用なし	適用なし	適用あり	適用なし
CloudFront アウトバウンド通信割引	適用なし	適用なし	適用なし	適用あり	適用なし
CloudFront リクエスト料金割引	適用なし	適用なし	適用なし	適用あり	適用なし
RI/SP 組織内共有	提供なし	提供なし	提供なし	提供なし	利用可能
AWS Organizations の利用	提供なし	提供なし	提供なし	提供なし	利用可能
セキュア設定	利用可能	利用可能	利用可能	利用可能	利用可能
Resold ES（*1）	提供なし	提供なし	提供なし	提供なし	利用可能

*1 AWS 直接契約となる AWS サポートを有償で提供します。

第8章　よくある質問

ここでは、よくお問い合わせいただくご質問についての回答をまとめてあります。問題が解決しない場合は、お手数ですが メンバーズポータル よりお問い合わせください。またご契約のプランによりご質問に対する回答が異なる場合がございます。現在ご契約中のプランが該当するかご確認ください。

8.1 AWS サポートに直接問い合わせしたいが、可能か？

全プラン共通

貴社および AWS 社間でサポート契約が締結されていないため、弊社を介さず直接問い合わせいただくことはできません。

8.2 AWS アカウントを解約したい（解約を実施したが動作しない）

全プラン共通

AWS アカウントの解約をご希望の場合は、まずは弊社までお問い合わせください。

メンバーズサービスに所属されている場合、誤操作防止のために AWS アカウント解約に関する一部の操作を制限しています。メンバーズの解約が完了するとともに、AWS アカウントの解約が実施できます。

8.3 AWS Billing Console にある解約ボタンを誤って押した場合、どのような対応が必要か

全プラン共通

解約に関わる操作は制限されているため、誤って解約ボタンを押した場合でもアカウントの解約処理は実行されません。解約をご希望の場合は、弊社までお問い合わせください。

8.4 プランを変更したい

全プラン共通

プランの変更は月単位で行うことが可能です。詳細は、下記のリンクをご確認ください。

- [新メンバーズポータル] 契約プランを変更したい

※旧メンバーズポータルをご利用の方は、下記をご確認ください。

- メンバーズプラン切替のお申し込み

8.5 メンバーズ加入時に作成される AWS リソース（S3 バケット, CloudTrail など）の設定を変更したい

全プラン共通

CM 管理 ラベルがないリソースであれば、自由に削除や設定変更を行えます。ただし オプトイン ラベルがあるものについて、メンバーズサービス設定画面でオプトインすると一部設定を上書きすることがございます。

8.6 AWS マネージメントコンソールのアカウント設定ページから「代替の連絡先」にメールアドレスを追加したい

全プラン共通

申し訳ございませんがお客様によって任意のメールアドレスを追加することはできかねます。

8.7 AWS Trusted Advisor のメール通知先として「代替の連絡先」を指定したい

全プラン共通

「代替の連絡先」は設定できないため、大変ご不便をおかけしますが CloudWatch への通知などをご検討ください。またプレミアムプランにご加入いただいている場合には、弊社から定期的にお送りしている「AWS ご利用改善レポート」メールを代替手段としてご利用下さい。

- Trusted Advisor のチェック結果を CloudWatch で通知する - DevelopersIO

8.8 購入したリザーブドインスタンス（RI）を Reserved Instance Marketplace で販売したい

全プラン共通

申し訳ございませんが、お客様が購入したリザーブドインスタンス（RI）を Reserved Instance Marketplace で販売することはできかねます。

8.9 メンバーズ設定で作成される AWS リソースのオプトインを無効化した場合、AWS リソースは自動的に削除されますか

全プラン共通

AWS リソースは削除されません。オプトインを無効化した場合その AWS リソースはメンテナンスの対象外となります。不要であればお客様で削除していただきますようお願いいたします。

- 【セキュアアカウントサービス】環境の切り戻しに関するご案内 - DevelopersIO

8.10 AWS リソースのオプトインを設定しました。いつ頃 AWS リソースは有効化されますか

全プラン共通

定期メンテナンスは、毎週土曜日の 2:00 (JST) 以降、週末にわたって順次実行されます。週明けに AWS リソースが作成されていることを確認してください。

8.11 メンテナンスで設定される項目に変更がある場合、事前に告知はありますか

全プラン共通

はい、通常であれば 1 週間程度前に変更のお知らせを行います。影響度が高いと判断されたものはそれより以前にお知らせすることもあります。

8.12 提供されているオプトインを利用して Security Hub などを特定リージョンのみ有効化することはできますか

全プラン共通

いいえ、特定リージョンのみ有効化はできません。オプトインを利用した場合、すべてのリージョンでサービスが有効化されます。特定リージョンのみ有効化したい場合、お手数ですがお客様でサービスを有効化してください。

8.13 AWS Organizations の ServiceControlPolicy を利用したい

標準プラン

申し訳ございませんが ServiceControlPolicy はご利用いただけません。また、ServiceControlPolicy の個別設定につきましても承ることはできかねます。

第9章　お問い合わせ

メンバーズサービスに関するご質問やご依頼については、メンバーズポータル 内の「お問い合わせ」ページよりお問い合わせいただけます。

メンバーズポータルの「お問い合わせ」ページがご利用いただけない場合は、お手数ですが support@classmethod.jp までメールにてご連絡ください。

第10章　改訂履歴

次の表は、メンバーズサービス仕様書に関する重要なアップデートについてまとめたものです。

改訂版	改訂内容
2024-05-29	制限事項に Savings Plans の返却を追加しました。
2024-04-08	新プラン提供に伴いプラン情報を更新しました。
2024-01-25	組織管理プランサービス仕様書と統合し、それに伴う整合性の調整を行いました。利用している AI サービスの記載を追加しました。
2023-05-29	提供サービスにインシデント自動調査を追加、WafCharm を削除しました。
2022-12-02	メンバーズ加入時の制限事項としてサポートプランの変更を追加しました。
2022-08-10	提供サービスに WafCharm を追加しました。
2022-06-10	作成される AWS リソースから cm-job ロールを削除しました。
2022-05-18	第 3 版をリリースしました。
2022-01-31	セキュア設定に関する項目を追加しました。
2020-06-15	英語版のサービス仕様書をリリースしました。
2020-03-26	第 2 版をリリースしました。
2019-11-08	提供サービスに IAM ユーザー作成代行を追加しました。
2019-11-08	初期設定として作成される IAM ユーザーと IAM グループの名前を変更しました。
2019-10-09	提供サービスにコストと利用状況レポート（CUR）を追加しました。
2019-09-25	監視オプションの料金情報やドキュメントを更新しました。
2019-08-21	オペレーション自動実行サービス終了に伴い、項目を削除しました。
2019-08-01	提供サービスに opswitch を追加しました。
2019-07-01	メンバーズのプラン改定に伴い、一部表記等を改めました。
2019-01-28	DDoS 攻撃対策オプションの加入時に運用代行オプションの加入が不要となりました。
2018-12-06	監視オプションをリニューアルしました。
2018-11-21	メンバーズで有効にする CloudTrail の仕様を変更しました。
2018-11-14	運用代行オプションの提供範囲を見直しました。
2018-10-04	提供サービスに運用代行オプションを追加しました。
2018-08-03	初版をリリースしました。