アカウントを複数に分ける理由

マルチアカウントの管理方法について紹介する前に、そもそもアカウントを複数に分けなければならない理由について考えてみます。

アカウントを複数に分ける理由としては、一般的に開発/ステージング/本番といった利用用途や部署やプロジェクト等の使用者の違いによって分けるのが一般的ではないでしょうか。 これは勿論当然の理由であり、利用者のポリシーでアカウントを分割することは必要であると言えます。 一方でAWSの機能的な制約からアカウントを分けた方がいいケースがございます。

AWSの機能的な制約からアカウントを分けた方がいいケースは課金情報を完全に分離する必要がある場合です。AWSの従量は課金配分タグ機能を利用することで1つのアカウントの内部でもある程度分解することが可能です。 しかしながら、課金配分タグは全ての従量課金に対応しているわけではありません。
例えば、ネットワーク通信料には対応しておらず、せっかくEC2にタグを設定しても、そこから送信されたトラフィックに対する通信料には課金タグが付与されません。 このようにある程度課金情報を分離すればいいだけであれば、課金配分タグにて対応可能ですが、厳密に分けたい場合は、AWSアカウントを分ける必要があります。

もうひとつは、リソースを完全に分離したい場合です。
AWSではIAMとタグを設定することによって、ユーザやグループ単位でアクセスできるサービスやリソースを制御することが可能です。 しかしながら、IAMでは閲覧の権限を付与すると、そのサービス内のリソースは全て表示され、本来他のユーザに見せたくないリソースを制限することはできません。 また、それなりに利用するリソースが増えてくるとIAMポリシーの設定やタグの管理が煩雑になる恐れがあります。 そのため、リソースを完全に分離したい場合もAWSアカウント自体を分ける必要があります。

マルチアカウント管理

複数のアカウントを管理する機能としてAWS社からはAWS Organizationsが提供されています。
AWS Organizationsを利用すると大きく請求の統合とマルチアカウントに対する一元管理/統制を行うことが可能となります。

AWS Organizationsでは、1つの管理アカウント（旧マスターアカウント）と複数のメンバーアカウント（旧連結アカウント）で構成されます。AWS Organizationsを利用する場合、まず管理アカウントを作成し、管理アカウント内で組織を作成し、組織内にメンバーアカウントを作成したり、 既存で存在するAWSアカウントに招待して、組織のメンバーとして登録することができます。

また、組織内には組織単位（OU）というグループを作成し、メンバーアカウントをグループ化し、グループ単位で管理を行うことができます。そして、組織、OU単位で様々な制御を行うことができます。

一括請求（コンソリデーティッドビリング）

AWS Organizationsで組織を構成すると一括請求によってAWSの従量に対してさまざまなメリットを享受することが可能となります。

AWSからの請求が纏まる

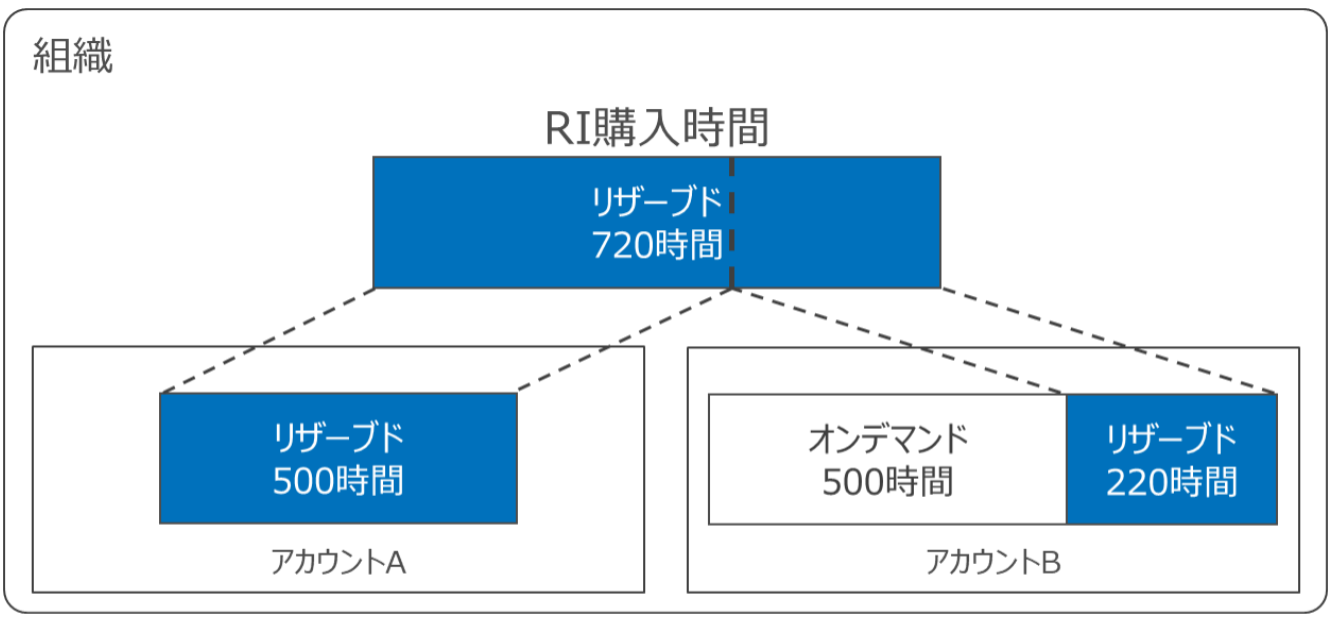
1つめのメリットはAWS社からの請求を1つに纏めることができる点です。
通常AWS社からの請求はアカウント単位で請求書が作成され、アカウント単位で支払いを実施しなければなりません。 AWS Organizationsで組織に統合すると組織内のメンバーアカウントで発生した従量は管理アカウントに集約され、 管理アカウントに纏めて請求が行われるため、アカウントが増えれば、増えるほど請求処理の手間を削減することが可能となります。

課金情報の一元管理

2つめのメリットは課金情報の一元管理ができる点です。
管理アカウントは名前の通り全てのメンバーアカウントを管理できるため、 管理アカウント請求書情報やCost Explorerからは全てのメンバーアカウントの課金情報を閲覧することができます。

各種ディカウントの共有

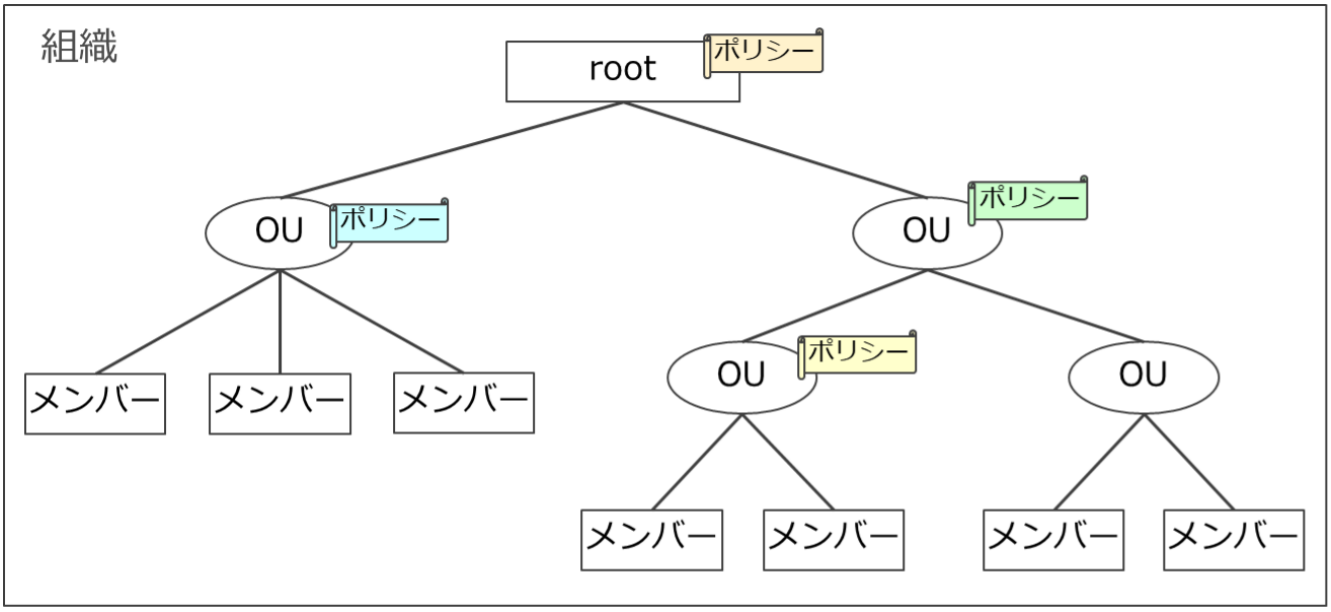
3つめのメリットは各種ディカウントの共有ができる点です。
AWS Organizationsで組織を構成すると、組織内のすべてのアカウントの使用量を結合し、 料金のボリューム割引を組織単位で受けることができる様になります。また、Amazon EC2やRDSを1年/3年単位で購入することで割引を受けることができる リザーブドインスタンスやSavings Plansを共有し、無駄なく利用することもできます。



Service Control Policy

AWS OrganizationsのService Control Policy（SCP）を使用するとOU単位で利用可能なAWSサービスの 制御を行うことができるため、マルチアカウント環境での統制を容易に実施することができます。

SCPはIAMと同じ形式でポリシーを作成し、作成したポリシーを組織全体またはOU単位で適用します。そうすることによって、複数のAWSアカウントに対して、利用してほしくないAWSサービスの利用を禁止したり、 アカウント内の特定のIAMユーザ/ロールからしかAWSサービスを利用できない様にすることが可能となります。



AWS Organizationsと連携するAWSサービス

ここ数年でAWS Organizationsと連携し、組織全体やOU単位で利用可能なAWSサービスが増えてきています。例えば、AWS CloudTrailは組織全体の監査ログを管理アカウントで取得し、 管理アカウントから一元的に組織内のイベント履歴の管理を行うことができます。

また、AWS Configを利用すれば、組織全体のリソースに対する設定の監視、変更履歴の記録、 設定に対する監査を行うことができ、組織全体のコンプライアンス維持を行うことが可能です。 その他AWS Organizationsと連携する機能として下記の様なものがあります。

サービス	機能
Amazon GuardDuty	悪意のあるアクティビティや不正な動作等による脅威の検出
AWS Backup	AWS リソースの自動バックアップ
AWS CloudFormation StackSets	複数のアカウントに対してCloudFormation Stackの作成、更新、削除
AWS Control Tower	複数のアカウントに対する管理ルールの適用
AWS Directory Service	組織内でAWS Managed Microsoft AD ディレクトリの共有
AWS Firewall Manager	アカウントおよび複数のリソース間で AWS WAF 管理
AWS Resource Access Manager	Amazon VPC等のリソースを組織内で共有
AWS Single Sign-On	組織内のアカウントにシングルサインオン
タグポリシー	リソース全体でタグを標準化

（上記サービスにはAWS Organizationsと連携する一部の機能取ります）

さいごに

この様にAWS Organizationsと連携することでマルチアカウントでの利用に対する利便性は確実に向上しており、 今後もさまざまなAWSサービスがAWS Organizationsと連携していくことが予想されます。

そのため、複数のアカウントを管理しなければならないシステム管理者様はAWS Organizationsを積極的に活用し、 マルチアカウント環境での管理に対する労力を削減して頂ければと思います。