AWS Firewall Manager を用いた マルチアカウントでの AWS WAF の管理手法

AWS Black Belt Online Seminar

文珠 啓介
Solutions Architect
2022/06

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

AWS Black Belt Online Seminar とは

- 「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分け、アマゾン ウェブ サービス ジャパン合同会社が主催するオンラインセミナーシリーズです
- AWS の技術担当者が、AWS の各サービスについてテーマごとに動画を公開します
- お好きな時間、お好きな場所でご受講いただけるオンデマンド形式です
- 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます

内容についての注意点

- 本資料では 2022 年 06 月時点のサービス内容および価格についてご説明しています。
  最新の情報は AWS 公式ウェブサイト (http://aws.amazon.com) にてご確認ください。

- 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます。

- 価格は税抜表記となっています。
  日本居住者のお客様には別途消費税をご請求させていただきます。

- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at http://aws.amazon.com/agreement/. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

自己紹介

❑ 名前

文珠 啓介 (Keisuke Monju)

❑ ロール

ソリューション アーキテクト

❑ 経歴

- オンプレミスのインフラ構築・運用
- AWS へのマイグレーション対応・運用

❑ 好きなAWSサービス

Amazon CloudFront 、AWS WAF 、AWS Firewall Manager

本セミナーの対象者

- 中規模以上のマルチアカウントを管理されている方で、セキュリティサービスの設定に関する一元管理に興味がある方
- Amazon Firewall Manager を既にご利用の方で、より理解を深めたい技術者の方

アジェンダ

1. AWS Firewall Manager とは
2. AWS Firewall Manager をはじめるには (AWS Organizations との連携)
3. AWS Firewall Manager による AWS WAF 用のポリシー設定
4. AWS Firewall Manager のその他の設定
5. AWS Firewall Manager と AWS Security Hub との連携
6. AWS Firewall Manager の色々な使い方
7. AWS Firewall Manager のクォータについて
8. AWS Firewall Manager の料金について
9. 参考情報
10. まとめ

アジェンダ

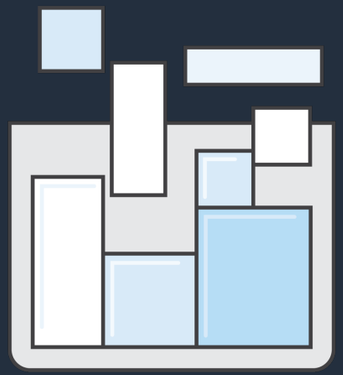
1. AWS Firewall Manager とは
2. AWS Firewall Manager をはじめるには (AWS Organizations との連携)
3. AWS Firewall Manager による AWS WAF 用のポリシー設定
4. AWS Firewall Manager のその他の設定
5. AWS Firewall Manager と AWS Security Hub との連携
6. AWS Firewall Manager の色々な使い方
7. AWS Firewall Manager のクォータについて
8. AWS Firewall Manager の料金について
9. 参考情報
10. まとめ

こんなお困りごとありませんか？

大量のアカウントやリソース

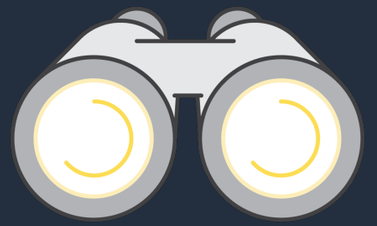
全てのアカウントやリソースに対するセキュリティポリシーの集約管理・維持が大変

作られ続けるアプリケーション



全てのアプリケーションが追加された瞬間から常時保護するのが困難

組織全体に渡る脅威対策の可視化

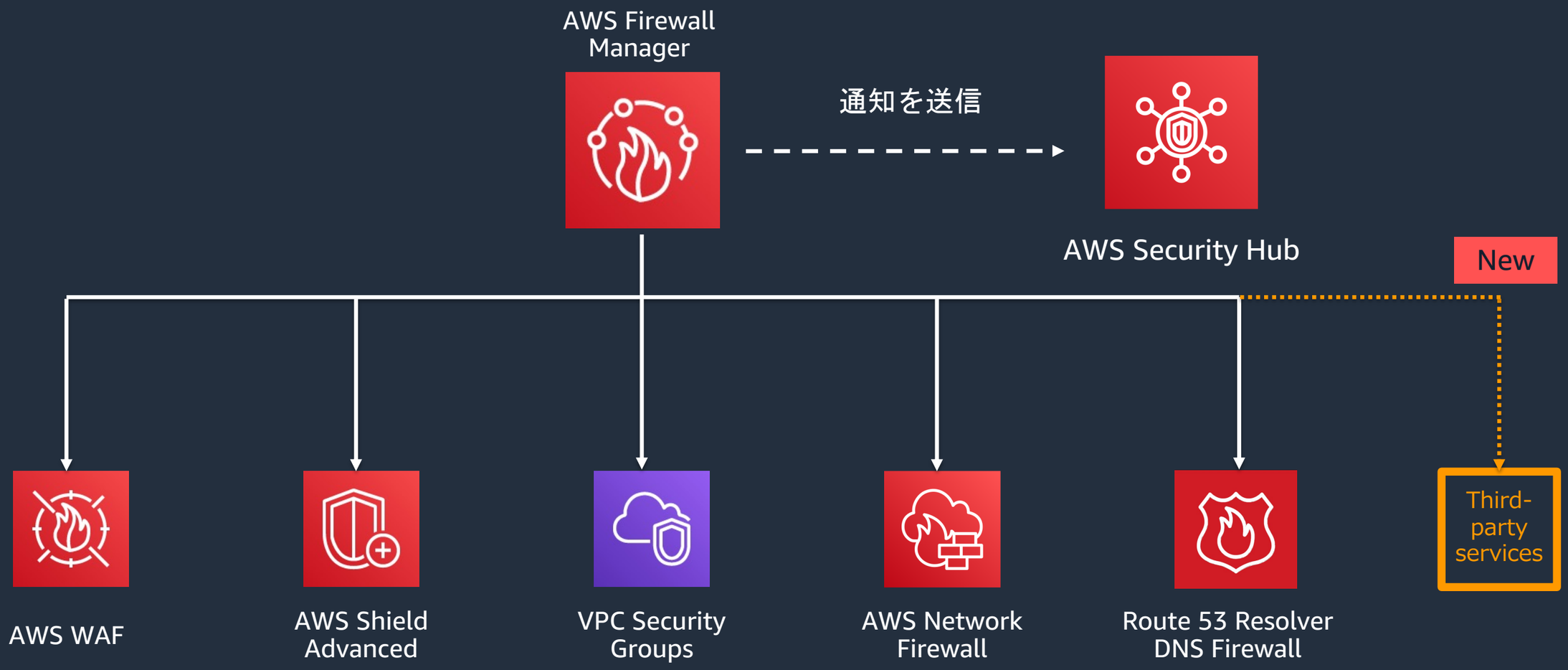


組織横断的に脅威の対策を監視し対応することができていない

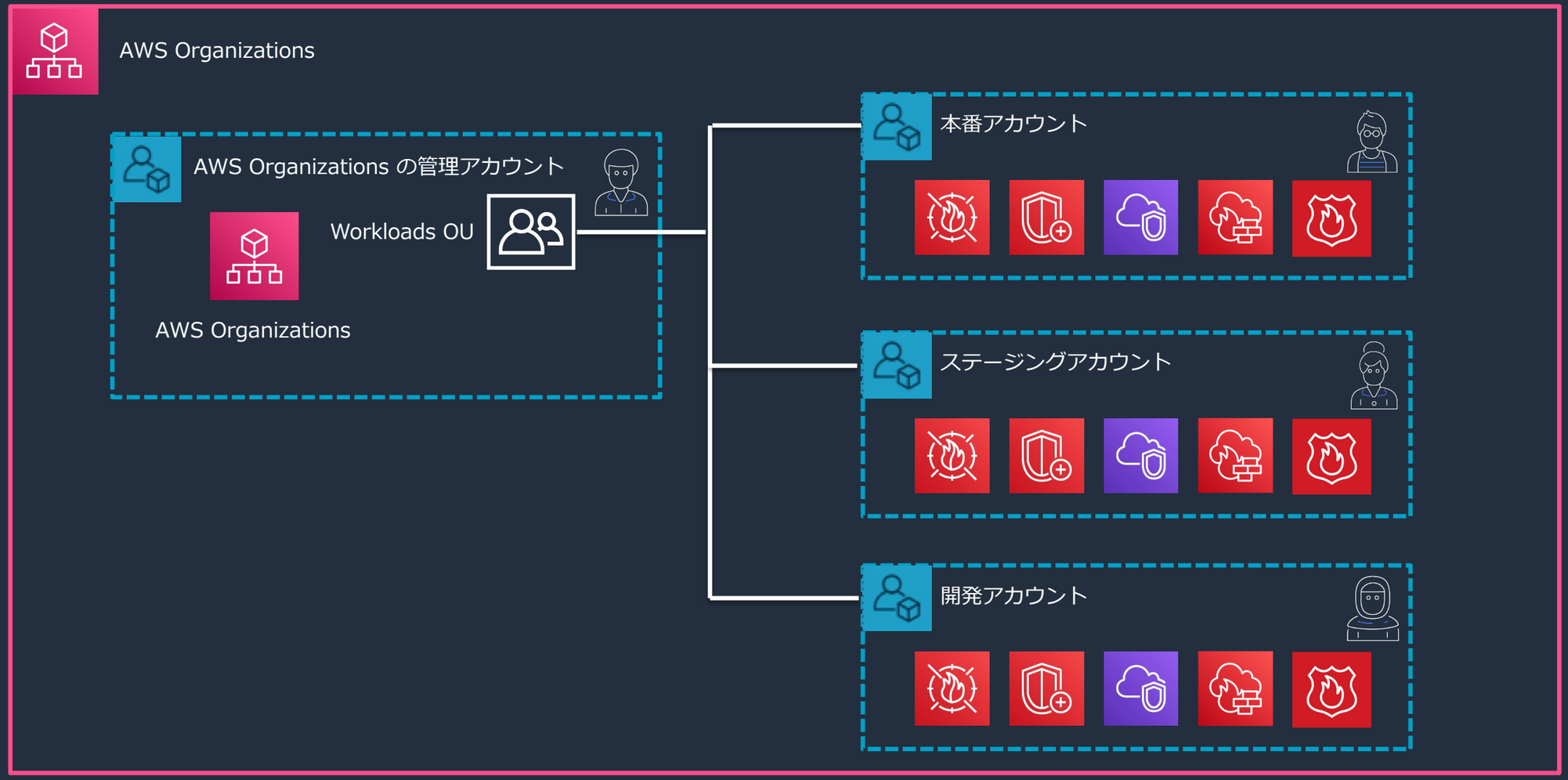
AWS Firewall Manager とは

AWS Firewall Manager とは AWS Organizations 配下で
管理されている AWS アカウント内のいくつかの
セキュリティサービスを中央集権的に設定、管理するための
セキュリティマネージメントサービスです。

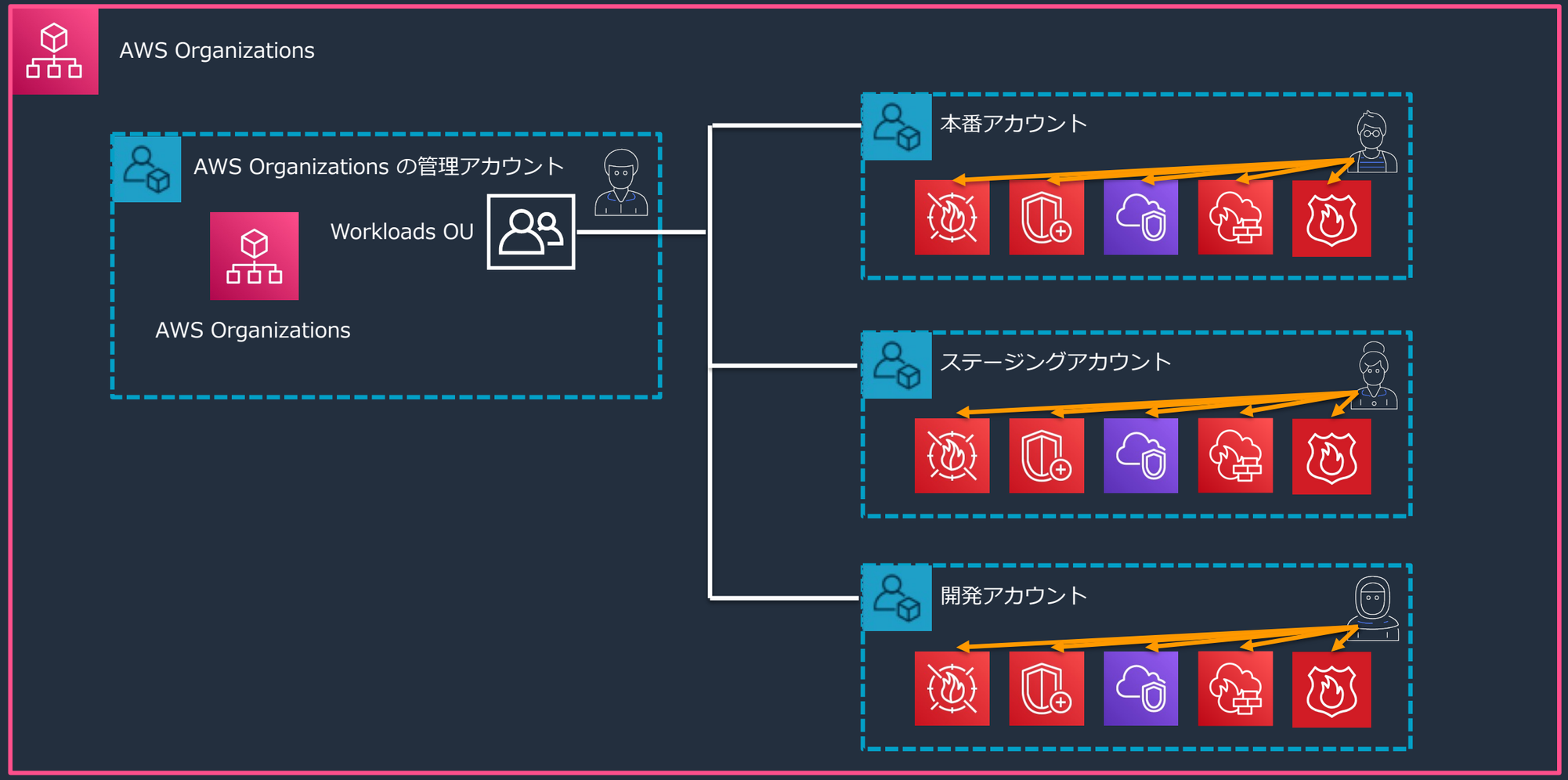
AWS Firewall Manager が中央集権的に管理するサービス



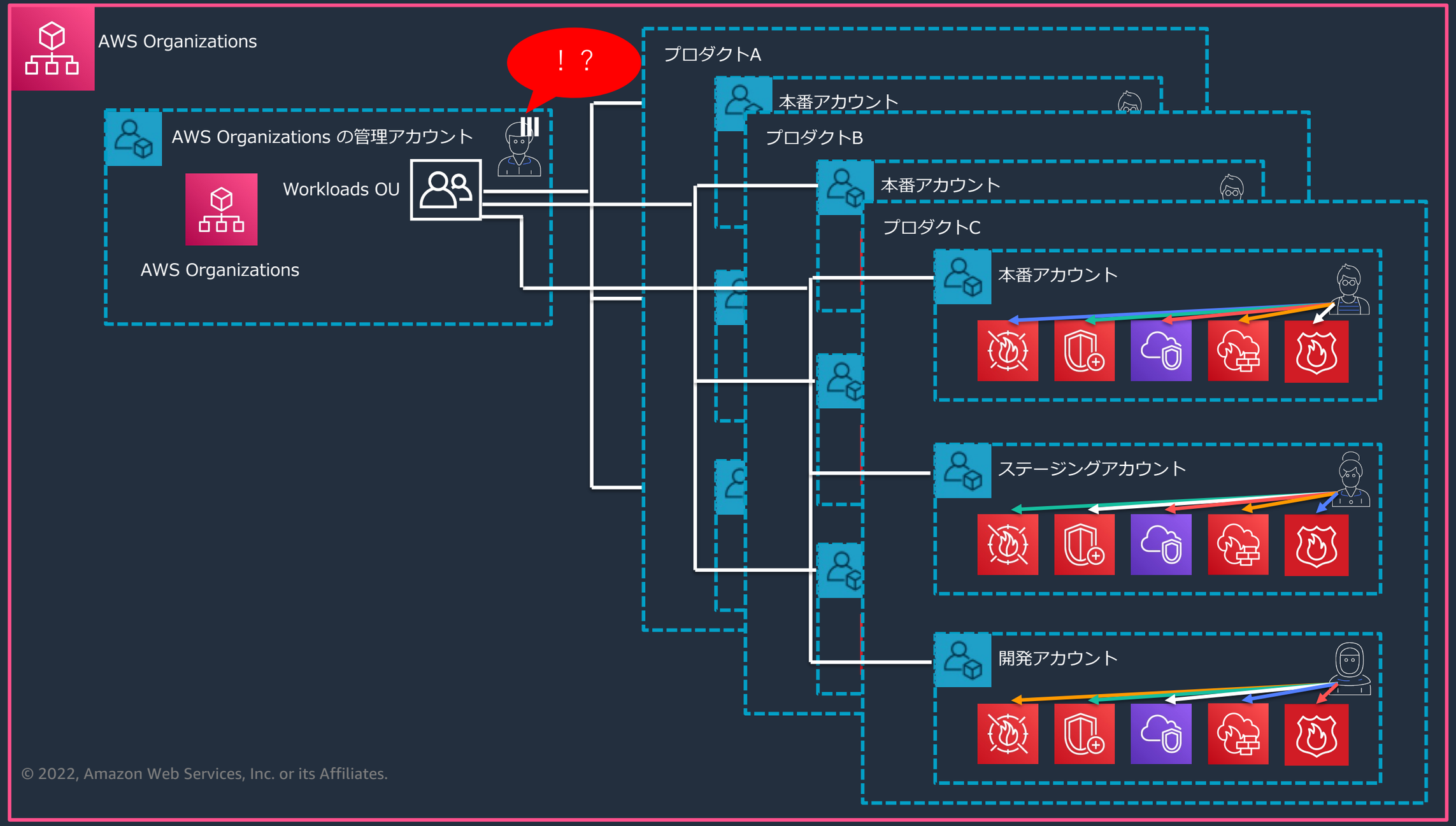
AWS Firewall Manager のイメージ



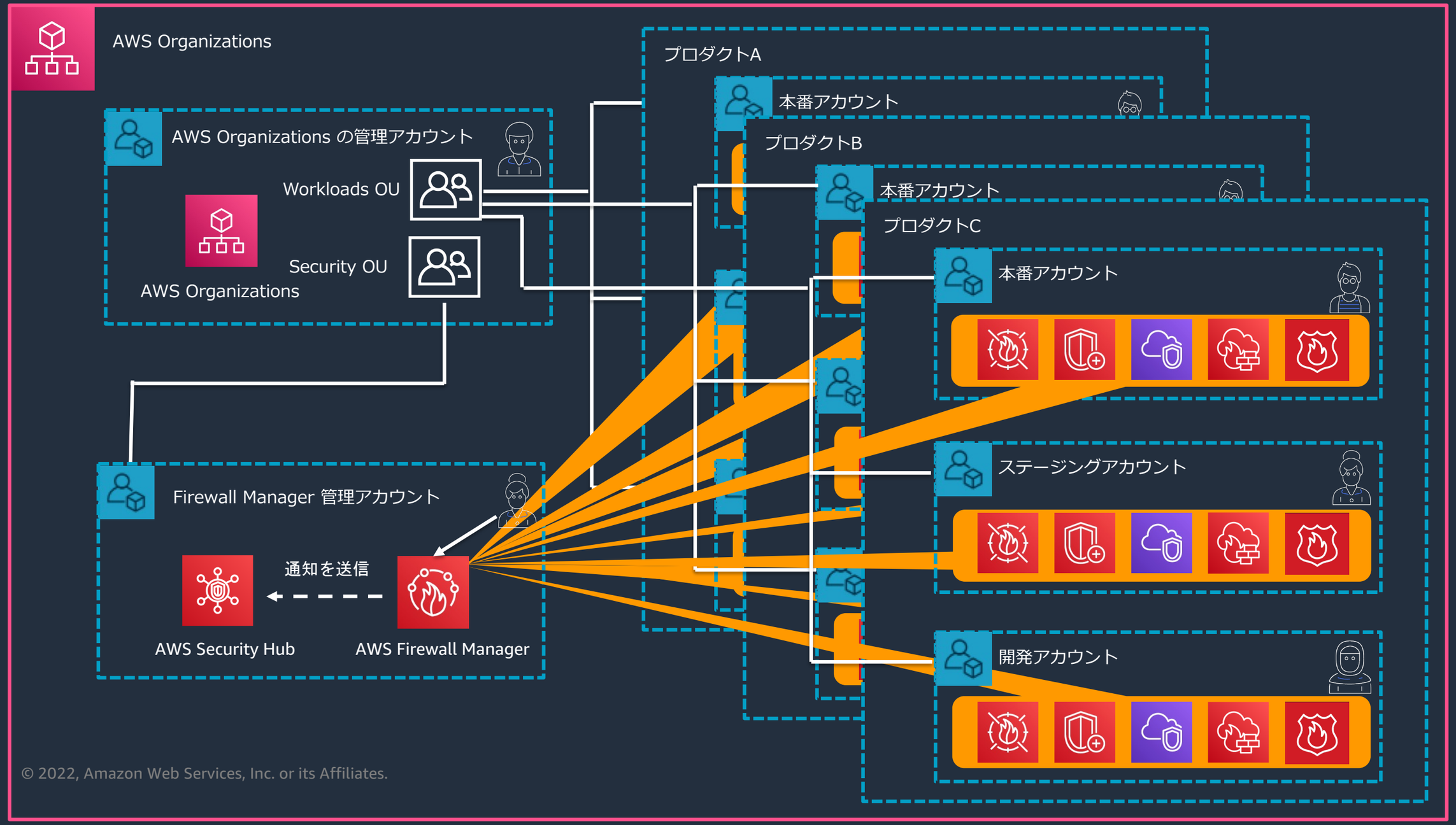
AWS Firewall Manager のイメージ



AWS Firewall Manager が解決する課題について



AWS Firewall Manager が解決する課題について



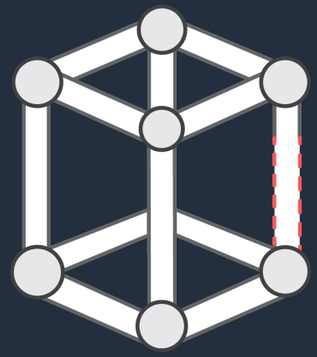
AWS Firewall Manager が解決する課題について

ファイアウォールポリシーの一元管理

AWS Organizations と統合されており、AWS Network Firewall、AWS WAF、AWS Shield、セキュリティグループ、Route 53 Resolver DNS Firewall を一元的に管理

ベースラインセキュリティポリシーの設定

WAF ルールやセキュリティグループのベースラインを管理者アカウントから簡単に作成・適用



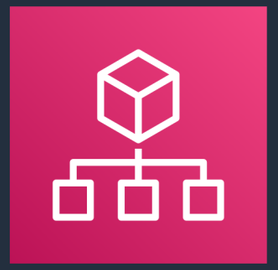
コンプライアンス違反の検出と修正

ポリシーベースのセキュリティグループ管理により、リソースを発見し、設定の逸脱を回避

アジェンダ

1. AWS Firewall Manager とは
2. AWS Firewall Manager をはじめるには (AWS Organizations との連携)
3. AWS Firewall Manager による AWS WAF 用のポリシー設定
4. AWS Firewall Manager のその他の設定
5. AWS Firewall Manager と AWS Security Hub との連携
6. AWS Firewall Manager の色々な使い方
7. AWS Firewall Manager のクォータについて
8. AWS Firewall Manager の料金について
9. 参考情報
10. まとめ

AWS Firewall Manager をはじめるには



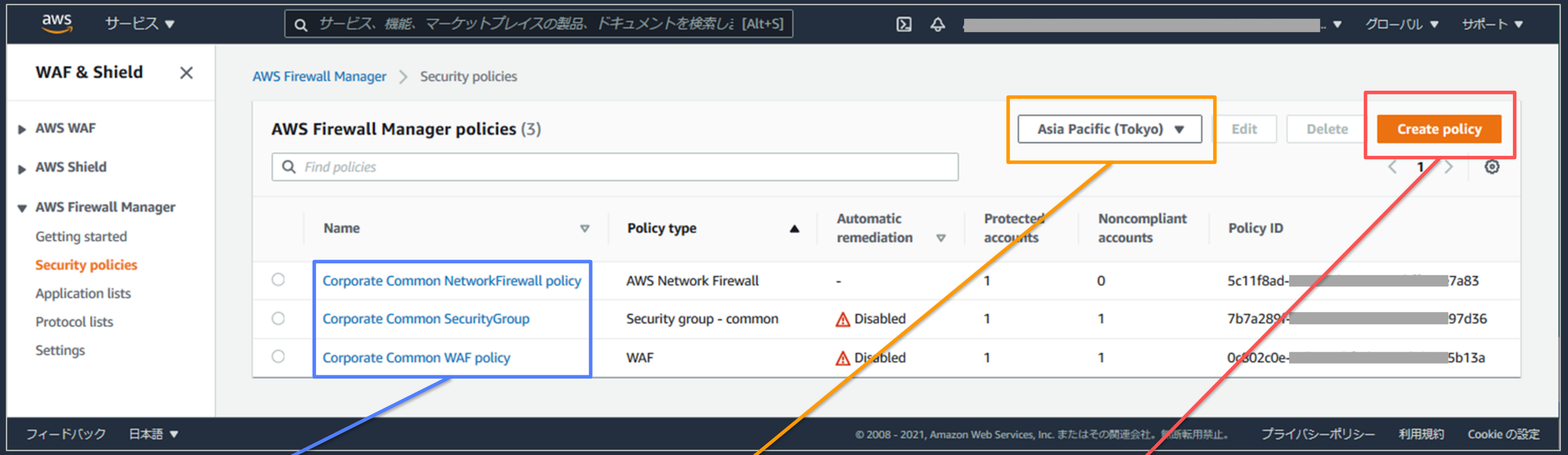
AWS Organizations にて全ての機能を有効化

すべての AWS アカウントで AWS Config を有効化

Firewall Manager 管理者を指定

・AWS Firewall Manager の前提条件 (具体的な設定手順)
https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/fms-prereq.html

AWS Firewall Manager の設定画面



(作成済みの)
Firewall Manager
ポリシーの一覧

対象リージョンを指定

Firewall Manager
ポリシーを作成

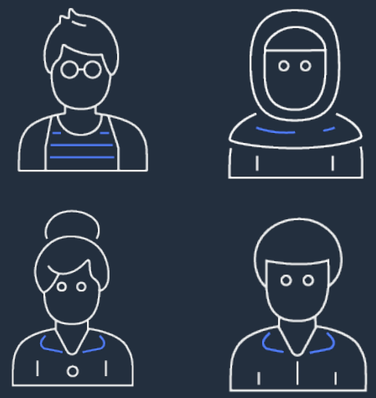
AWS Firewall Manager ポリシーとリージョンの立ち位置

AWS Firewall Manager ポリシーの設定内容

AWS Firewall Manager ポリシー

ルール

アクション



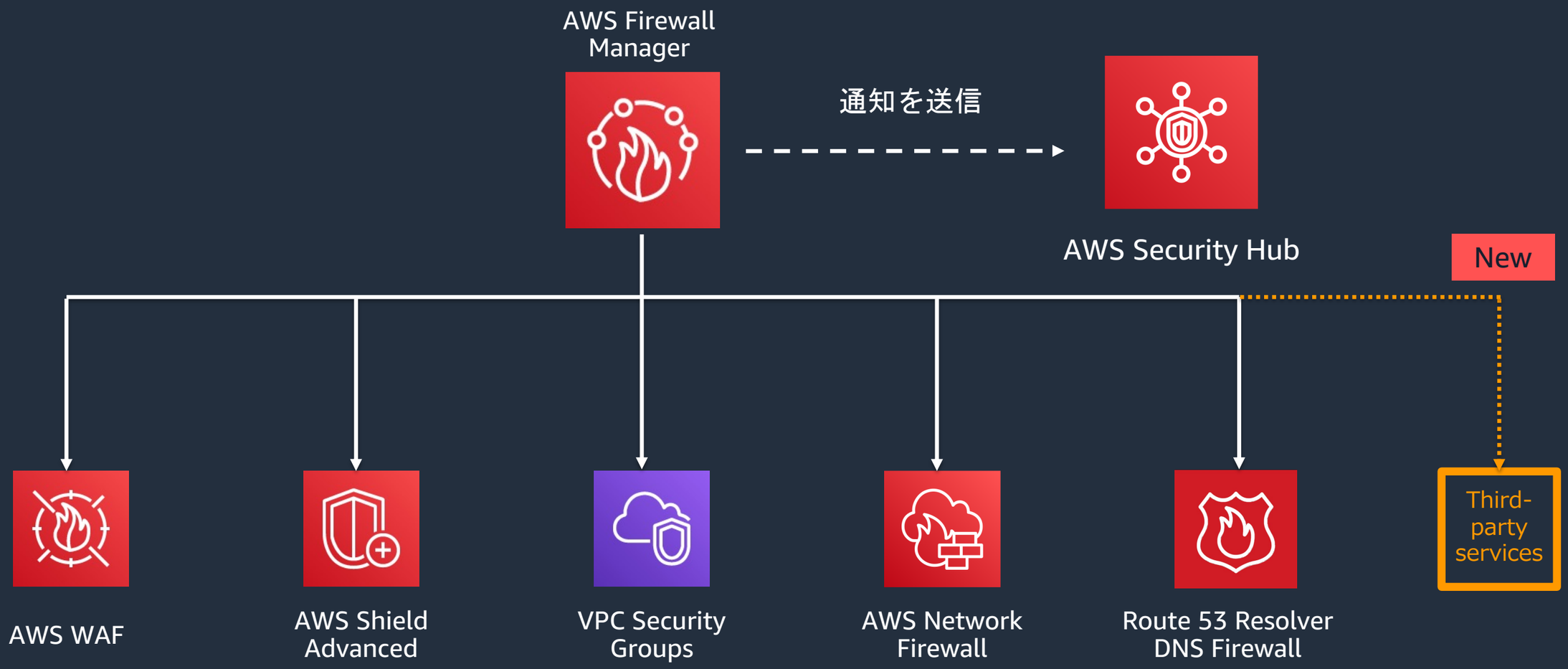
スコープ

アジェンダ

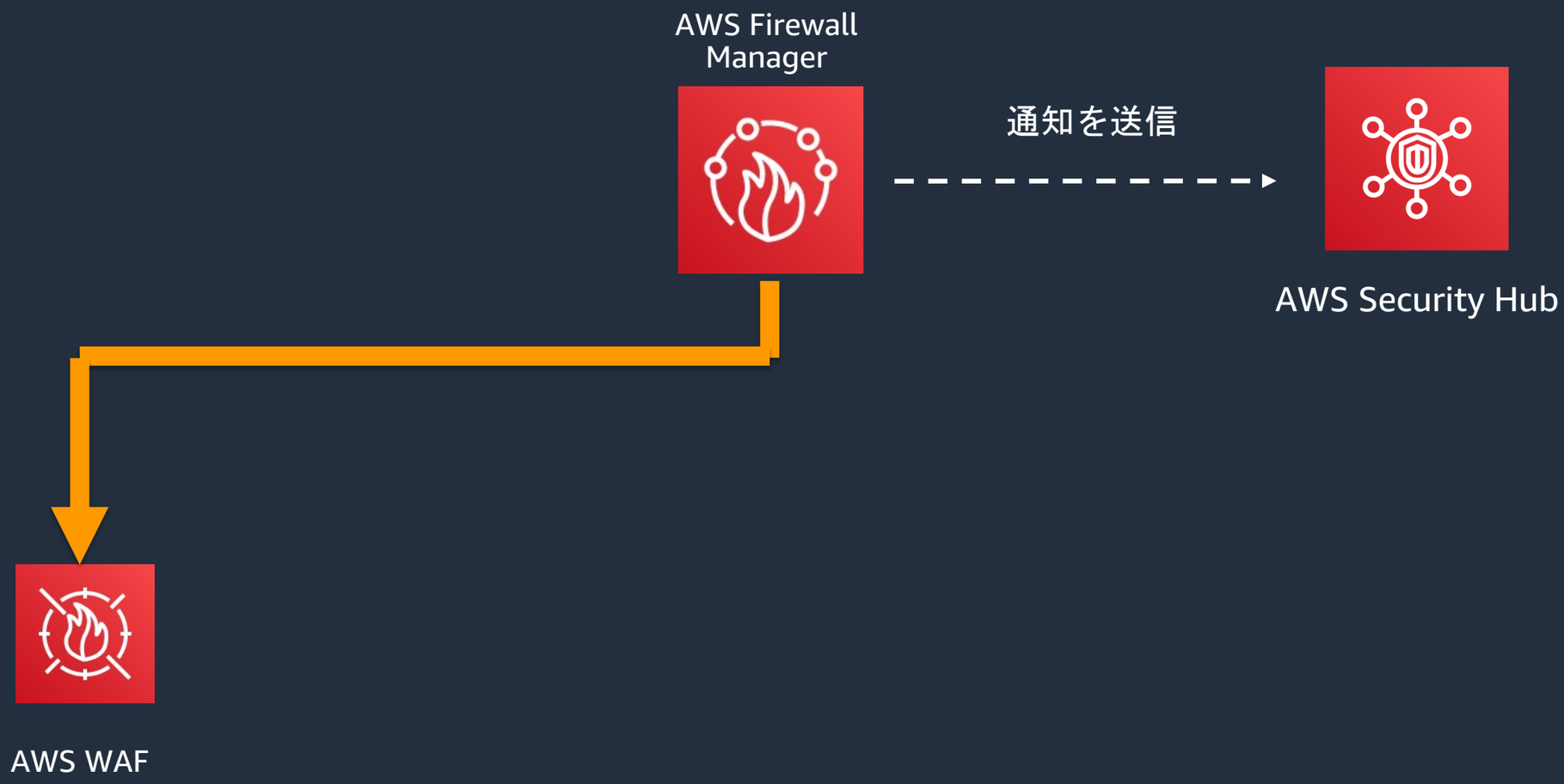
1. AWS Firewall Manager とは
2. AWS Firewall Manager をはじめるには (AWS Organizations との連携)
3. AWS Firewall Manager による AWS WAF 用のポリシー設定
4. AWS Firewall Manager のその他の設定
5. AWS Firewall Manager と AWS Security Hub との連携
6. AWS Firewall Manager の色々な使い方
7. AWS Firewall Manager のクォータについて
8. AWS Firewall Manager の料金について
9. 参考情報
10. まとめ

再掲

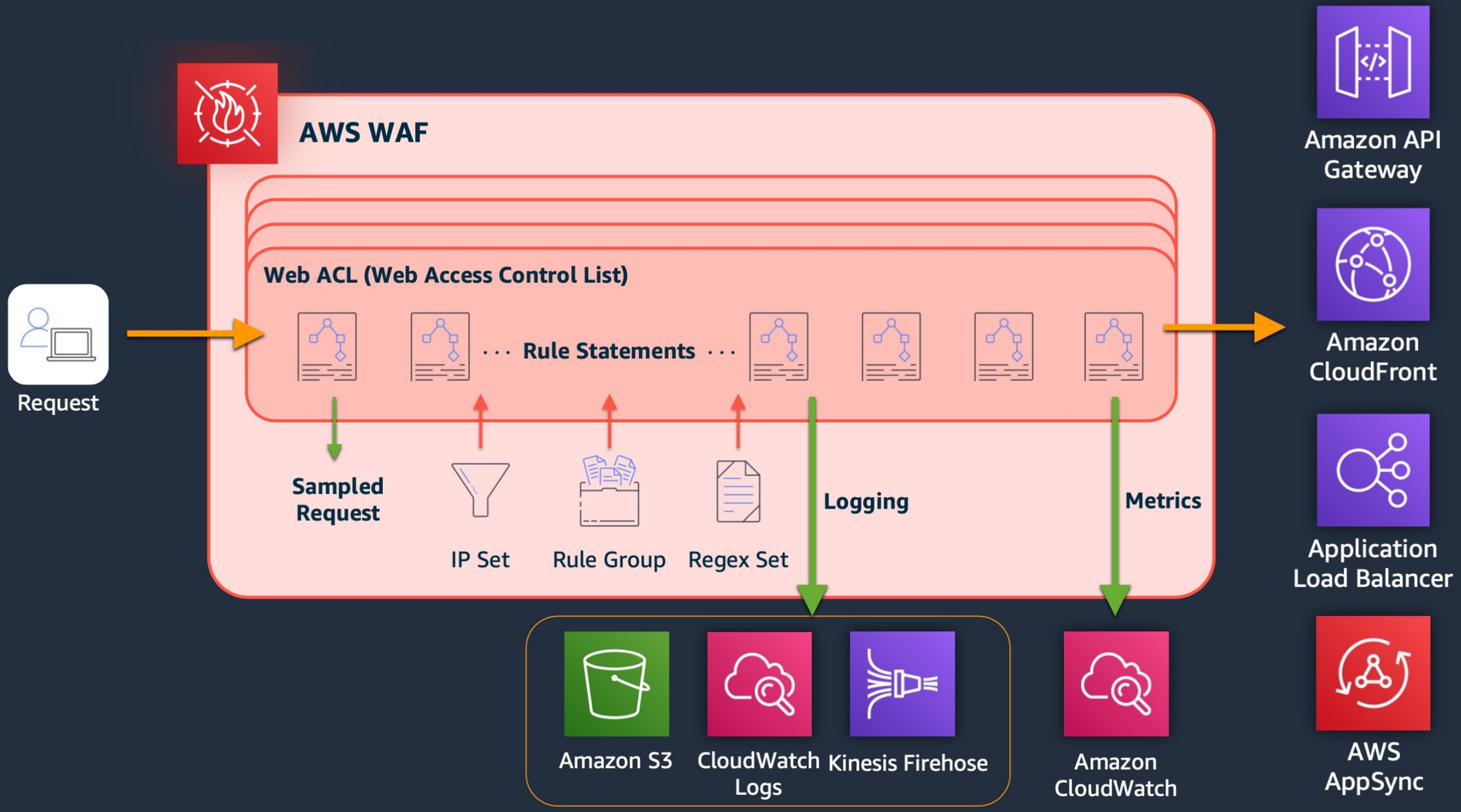
AWS Firewall Manager が中央集権的に管理するサービス



AWS Firewall Manager が中央集権的に管理するサービス



AWS WAFとは？



(抜粋) [AWS Black Belt Online Seminar] AWS WAF アップデート
https://d1.awsstatic.com/webinars/jp/pdf/services/20200324_AWS_BlackBelt_AWS_WAF_Update.pdf

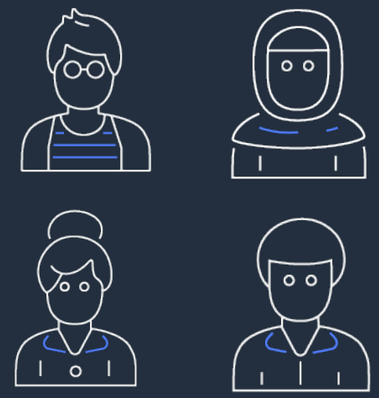
再掲

AWS WAF 用の Firewall Manager ポリシーの設定概要

AWS Firewall Manager ポリシー

ルール

アクション



スコープ

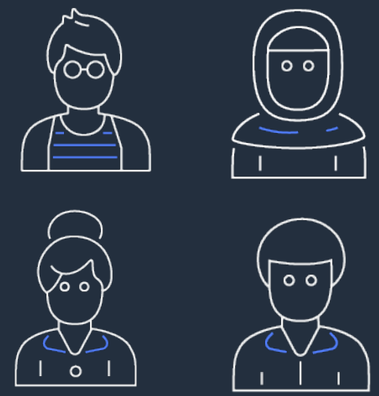
再掲

AWS WAF 用の Firewall Manager ポリシーの設定概要

AWS Firewall Manager ポリシー

ルール

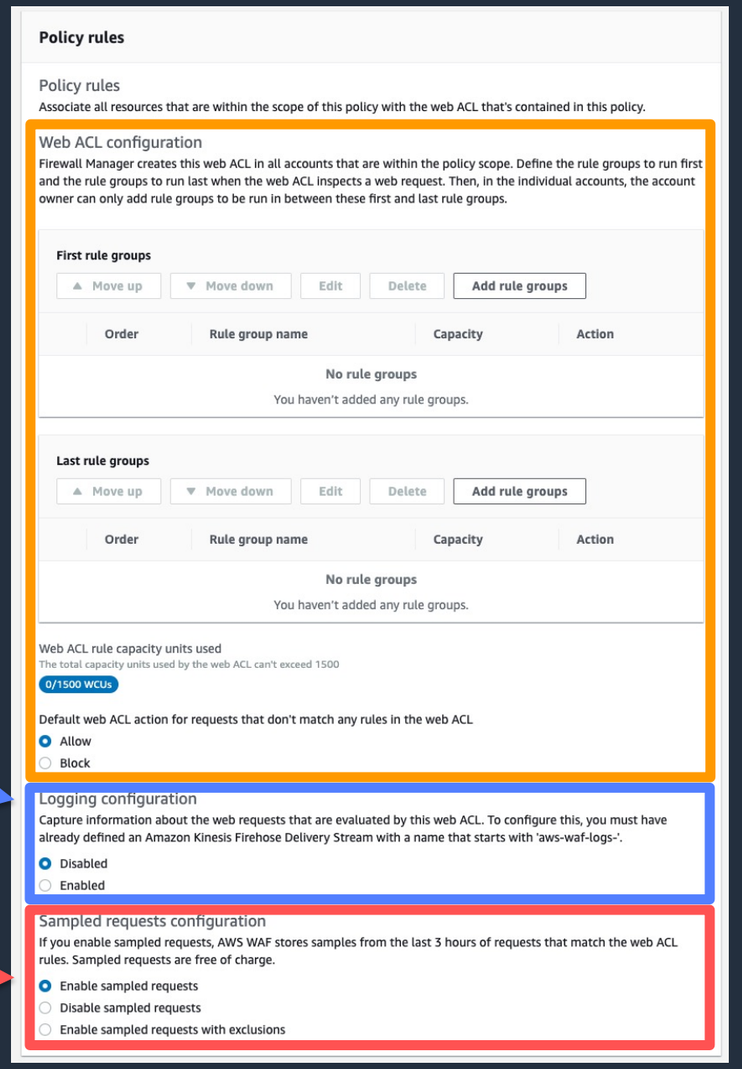
アクション



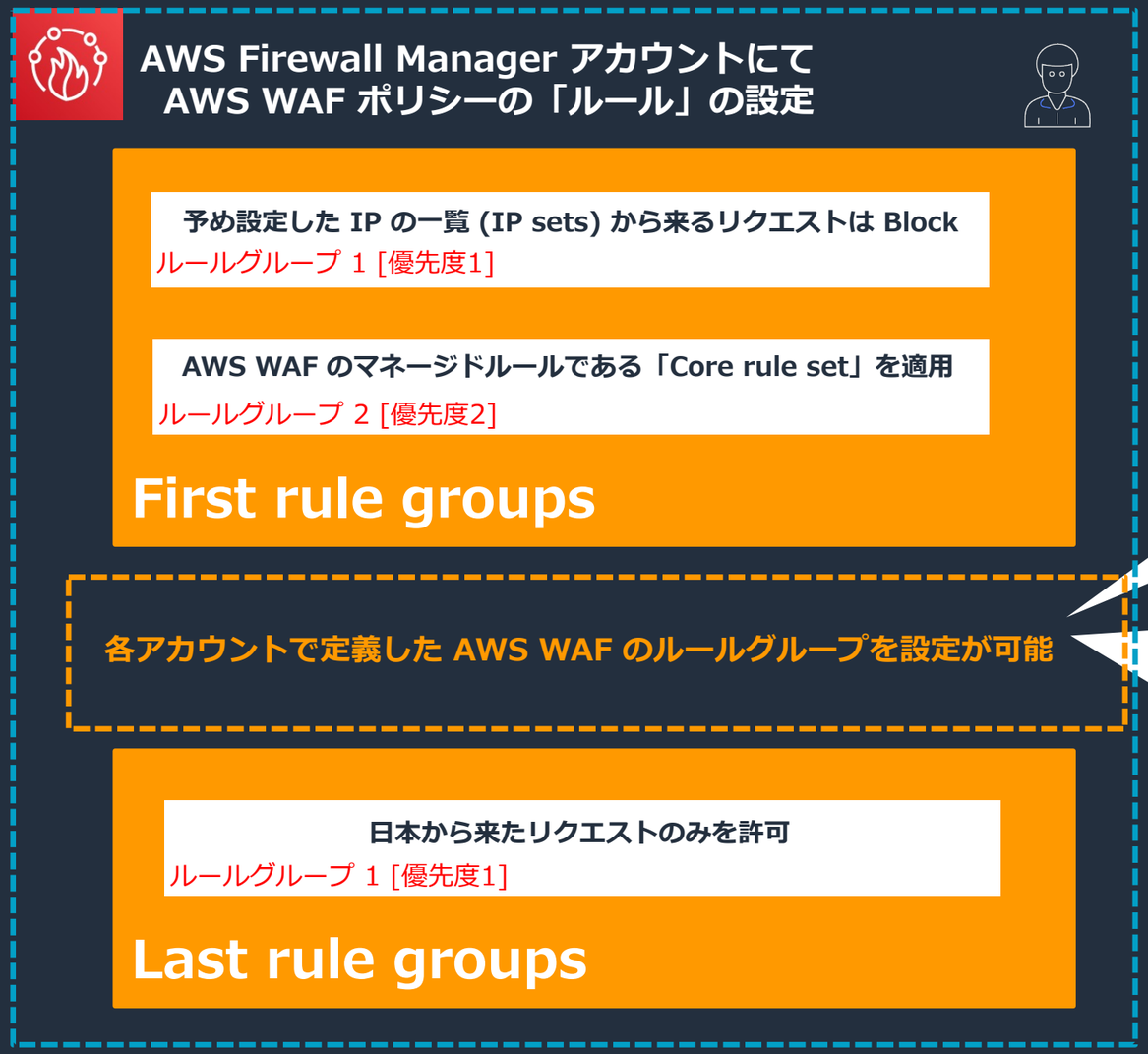
スコープ

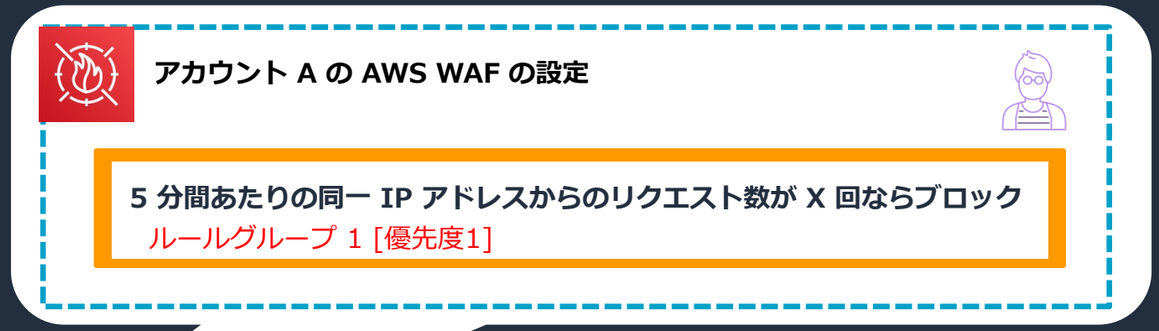
AWS WAF 用のポリシーの「ルール」について

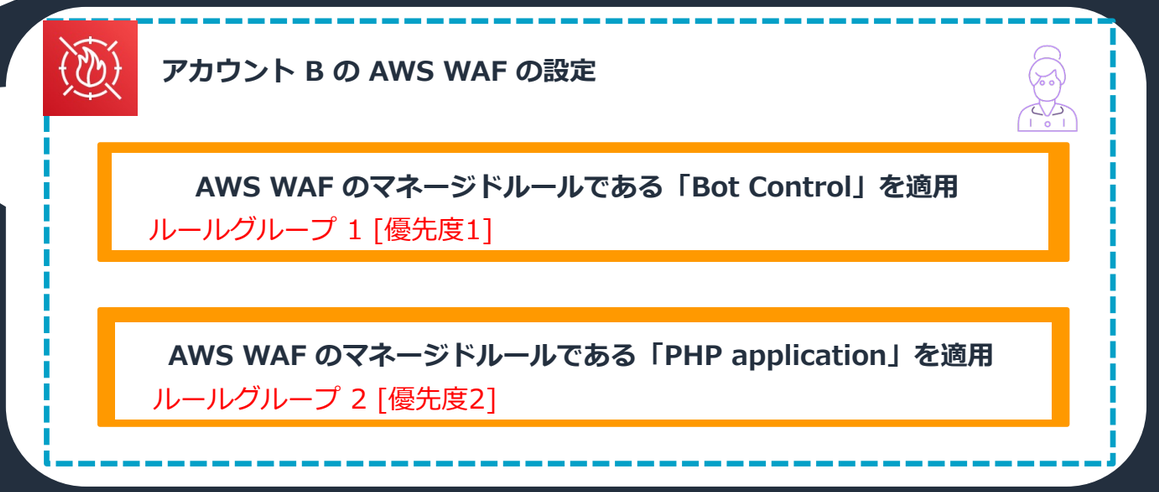
- 3つのセクション
  - Web ACL configuration
    AWS WAF の Web ACL についての設定
  - Logging configuration
    AWS WAF の ログについての設定
  - Sampled requests configuration
    サンプルリクエストについての設定



「Web ACL configuration」の設定について



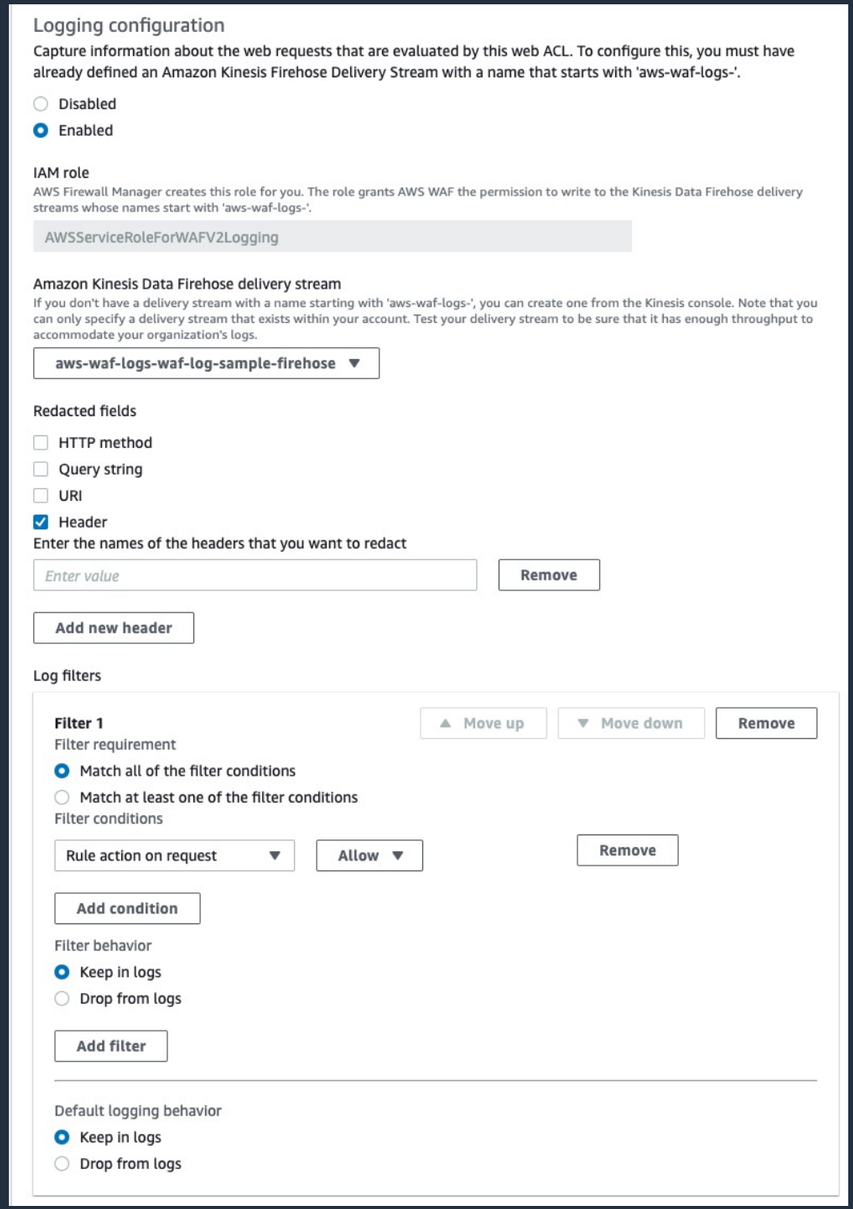




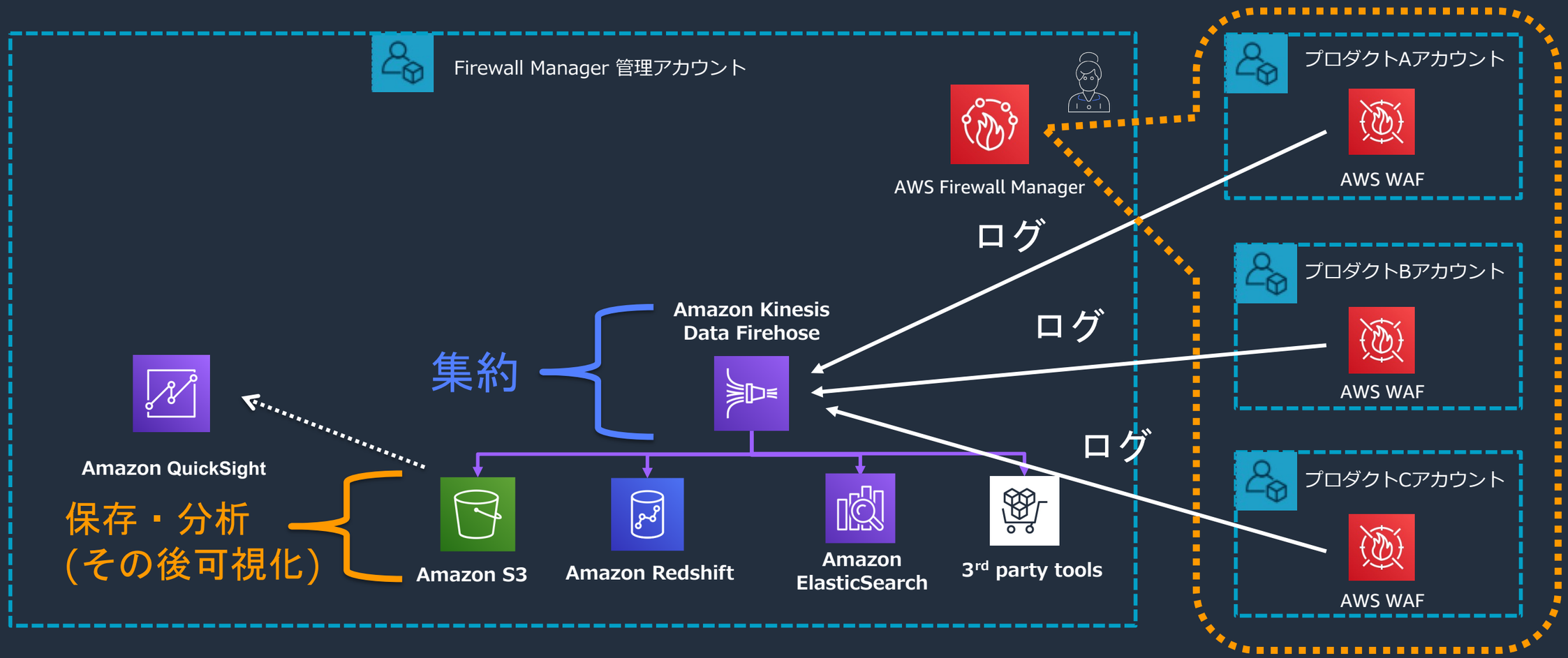
全てのルールにマッチしなかったら「Allow」 or 「Block」を設定可能

「Logging configuration」について

- Kinesis Data Firehose を介して、選択した宛先に JSON 形式でログを送出
- 記録されたすべてのリクエストには、一致したリクエストヘッダーと RuleID が含まれる
- Cookie や認証ヘッダなど、センシティブな情報をログから除外可能
- リクエストのどこで (ヘッダ/クエリ/Body) どの値がルールに合致してブロックされたかを確認可能
- **ログフィルタリングの設定も可能**
- **各アカウントで発生したログはここで指定した Kinesis Data Firehose に集約**

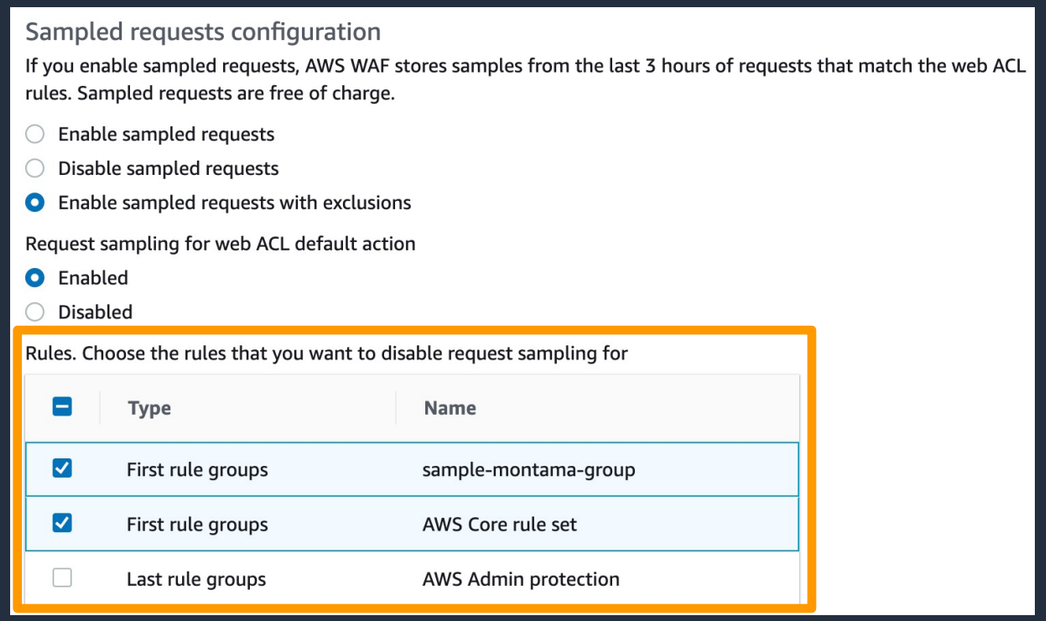


「 Logging configuration 」について

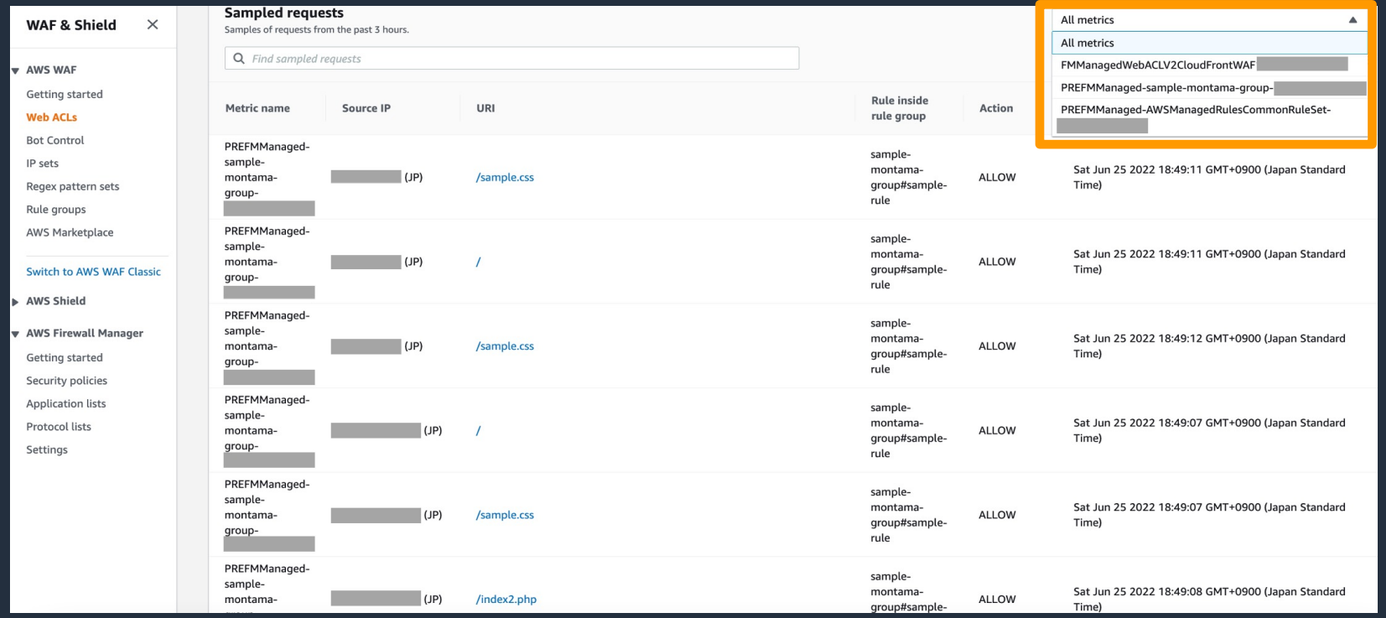


「Sampled requests configuration」について

- 過去 3 時間以内の保護対象リソースに対するリクエストで Web ACL のルールとマッチしたもののサンプリングを AWS WAF 側で保存するか否かを設定する項目
- サンプリングされたリクエストの内容 (ソース IP 、URI 、Action など) を確認可能



設定画面



サンプルの閲覧画面
(AWS WAF側)

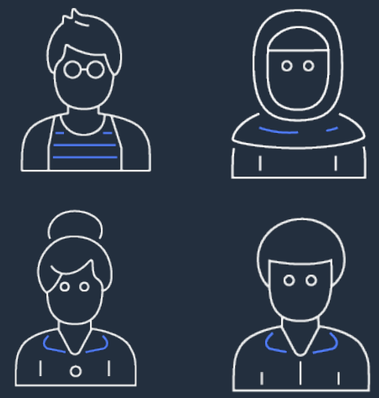
再掲

AWS WAF 用の Firewall Manager ポリシーの設定概要

AWS Firewall Manager ポリシー

ルール

アクション

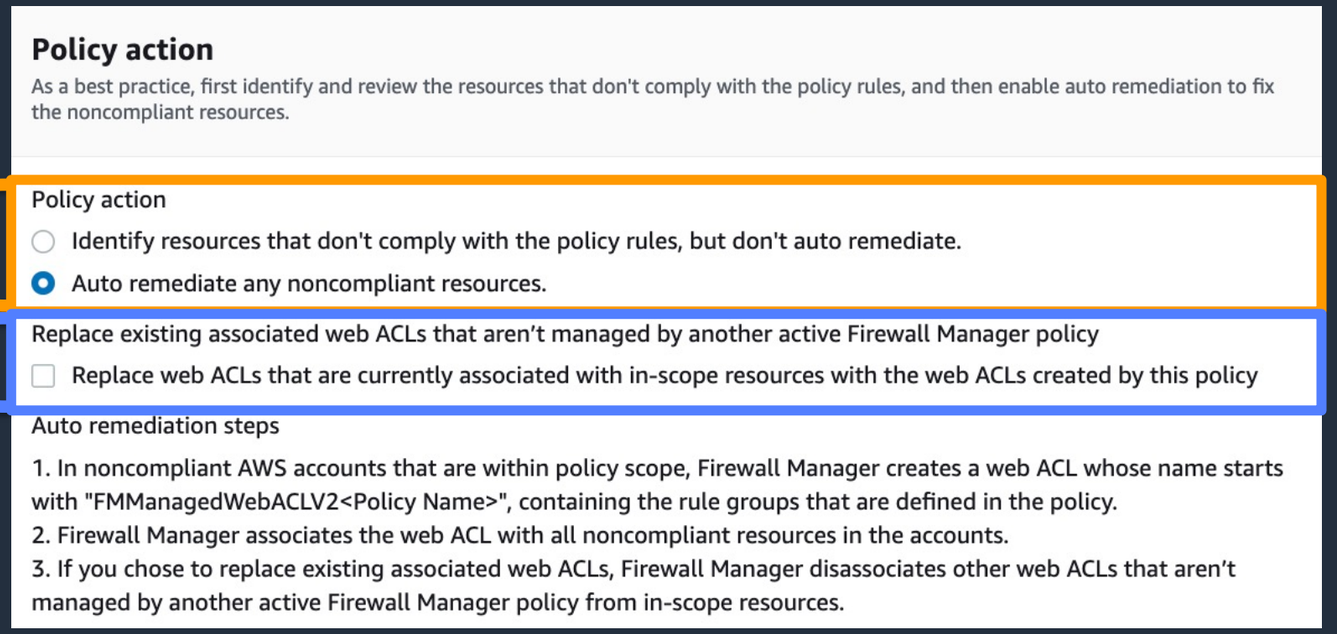


スコープ

AWS WAF 用のポリシーの「アクション」について

Firewall Manager の AWS WAF ポリシーが作成した Web ACL が紐付いていないリソースを発見した場合の挙動を設定 (自動設定 or 検知のみ)

Firewall Manager のAWS WAF ポリシーが作成した Web ACL 以外が紐付いているリソースを発見した場合の挙動を設定 (自動リアサイン or 検知のみ)



※検知モードでポリシーに準拠していないリソースの一覧を確認した後に Auto で割り当てるか否かの検討する流れを推奨

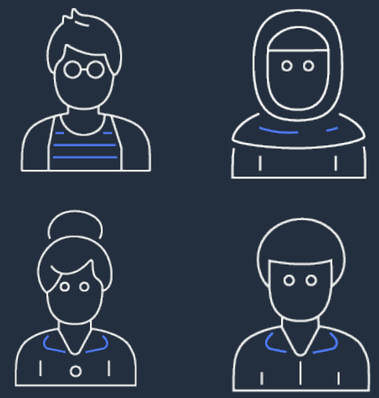
再掲

AWS WAF 用の Firewall Manager ポリシーの設定概要

AWS Firewall Manager ポリシー

ルール

アクション



スコープ

aws

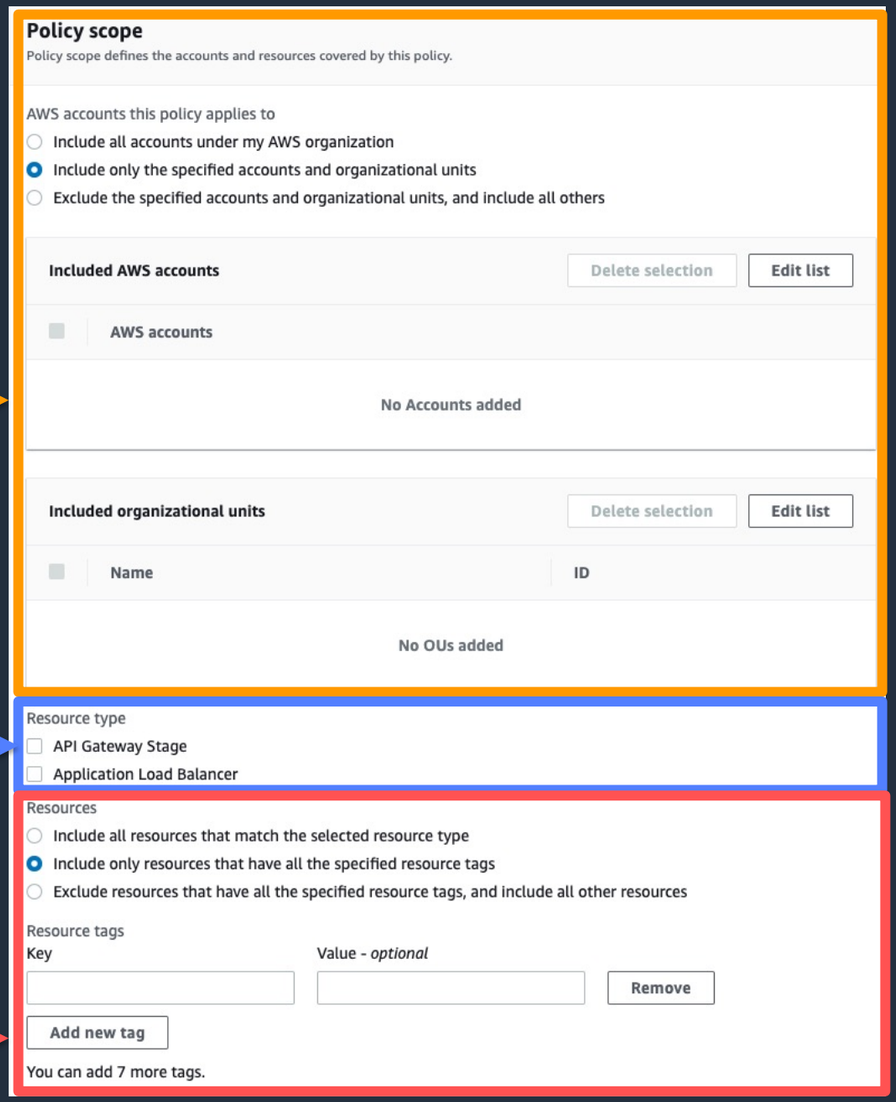
AWS WAF のポリシーの「スコープ」について

- **3つのセクション**
  - AWS accounts this policy applies to

    このポリシーを設定する対象のアカウント
    もしくは OU を指定 (WhiteList　or BlackList)
  - Resource type

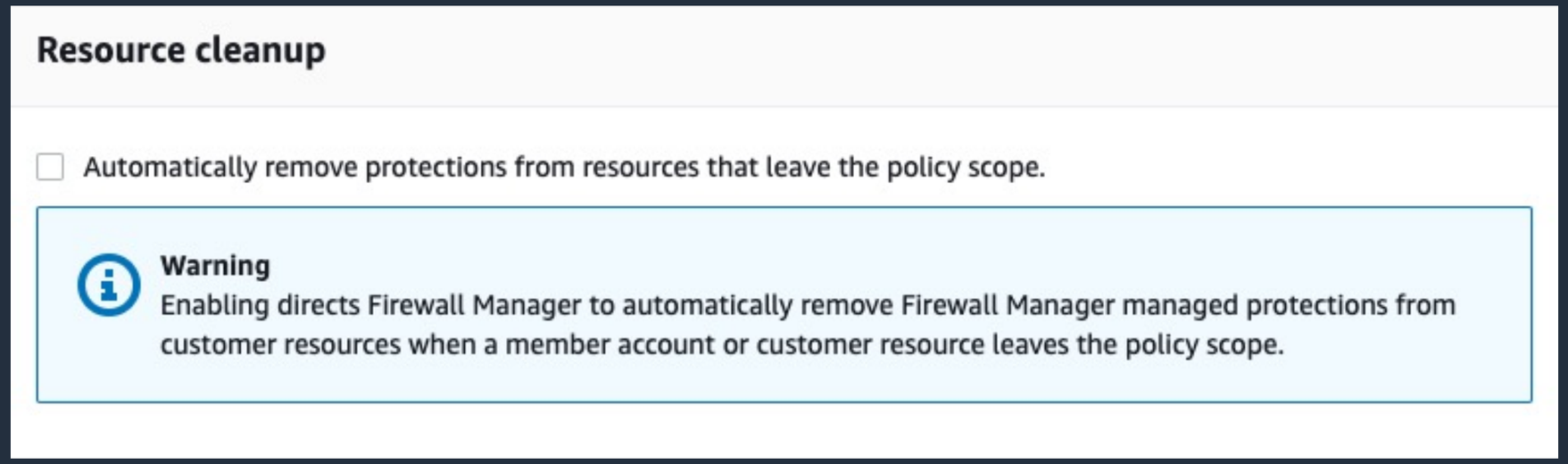
    対象となるリソースタイプを指定
    (CloudFront は Global リージョンを選択)
  - Resources

    対象となるリソースに紐づくタグを指定



「リソースのクリーンアップ」について

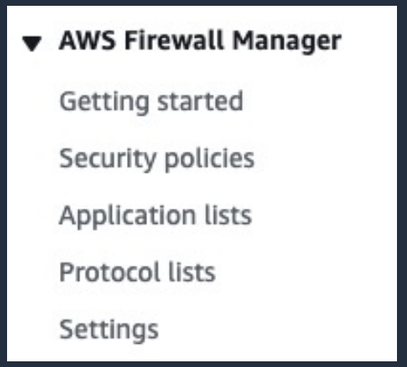
AWS WAF ポリシーのスコープから対象のリソースが外れた時の挙動を設定
(スコープから外れた際に AWS WAF の Web ACL も自動的にデタッチさせることが可能)



アジェンダ

1. AWS Firewall Manager とは
2. AWS Firewall Manager をはじめるには (AWS Organizations との連携)
3. AWS Firewall Manager による AWS WAF 用のポリシー設定
4. AWS Firewall Manager のその他の設定
5. AWS Firewall Manager と AWS Security Hub との連携
6. AWS Firewall Manager の色々な使い方
7. AWS Firewall Manager のクォータについて
8. AWS Firewall Manager の料金について
9. 参考情報
10. まとめ

その他の設定について



- Application lists
  - SecurityGroup (Auditing and enforcement of security group rules) 用のポリシーで自動制御する対象となるアプリケーションを指定する際に利用する
- Protocol lists
  - SecurityGroup (Auditing and enforcement of security group rules) 用のポリシーで自動制御する対象となるプロトコルを指定する際に利用する
- Settings
  - AWS Firewall Manager administrator account の設定
  - AWS Firewall Manager から直接通知する際の SNS の設定
  - Third party 製品との連携の設定

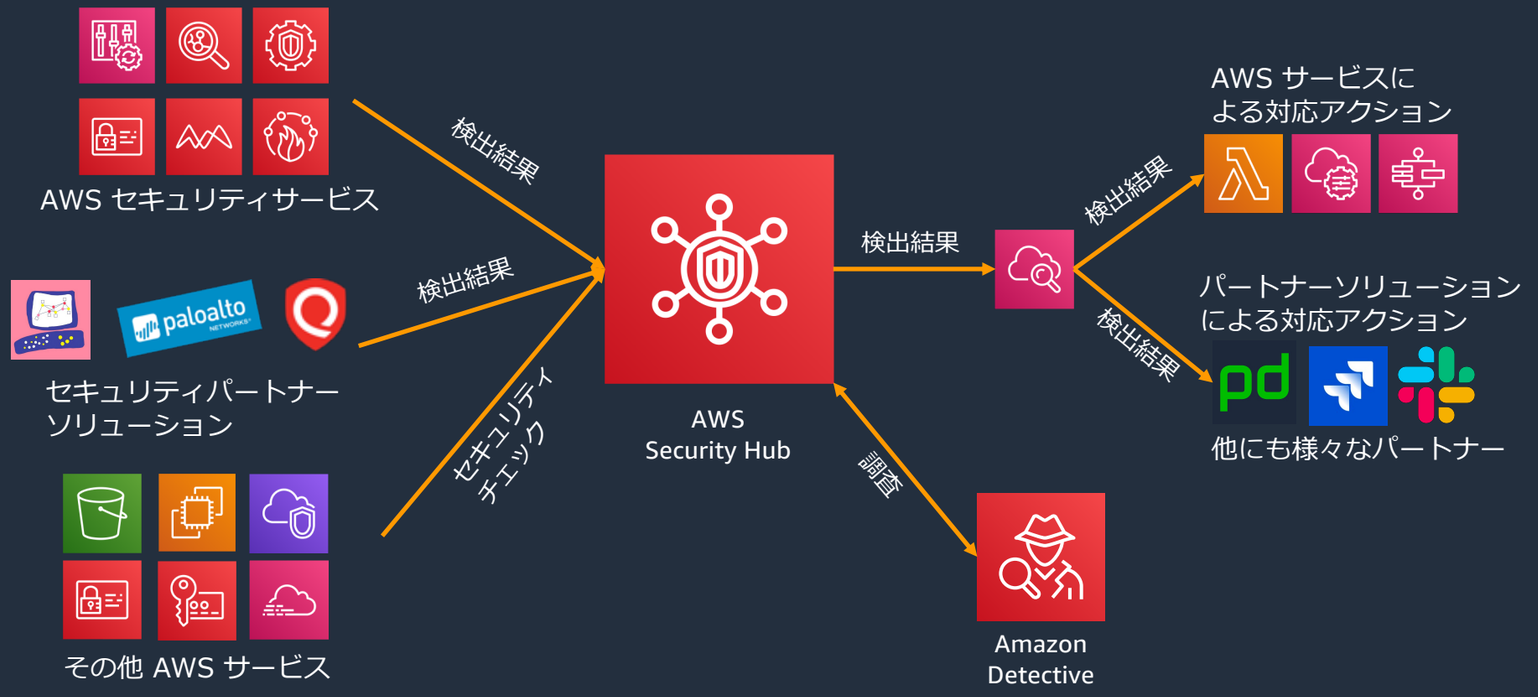
マネージドリスト
https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/working-with-managed-lists.html

アジェンダ

1. AWS Firewall Manager とは
2. AWS Firewall Manager をはじめるには (AWS Organizations との連携)
3. AWS Firewall Manager による AWS WAF 用のポリシー設定
4. AWS Firewall Manager のその他の設定
5. AWS Firewall Manager と AWS Security Hub との連携
6. AWS Firewall Manager の色々な使い方
7. AWS Firewall Manager のクォータについて
8. AWS Firewall Manager の料金について
9. 参考情報
10. まとめ

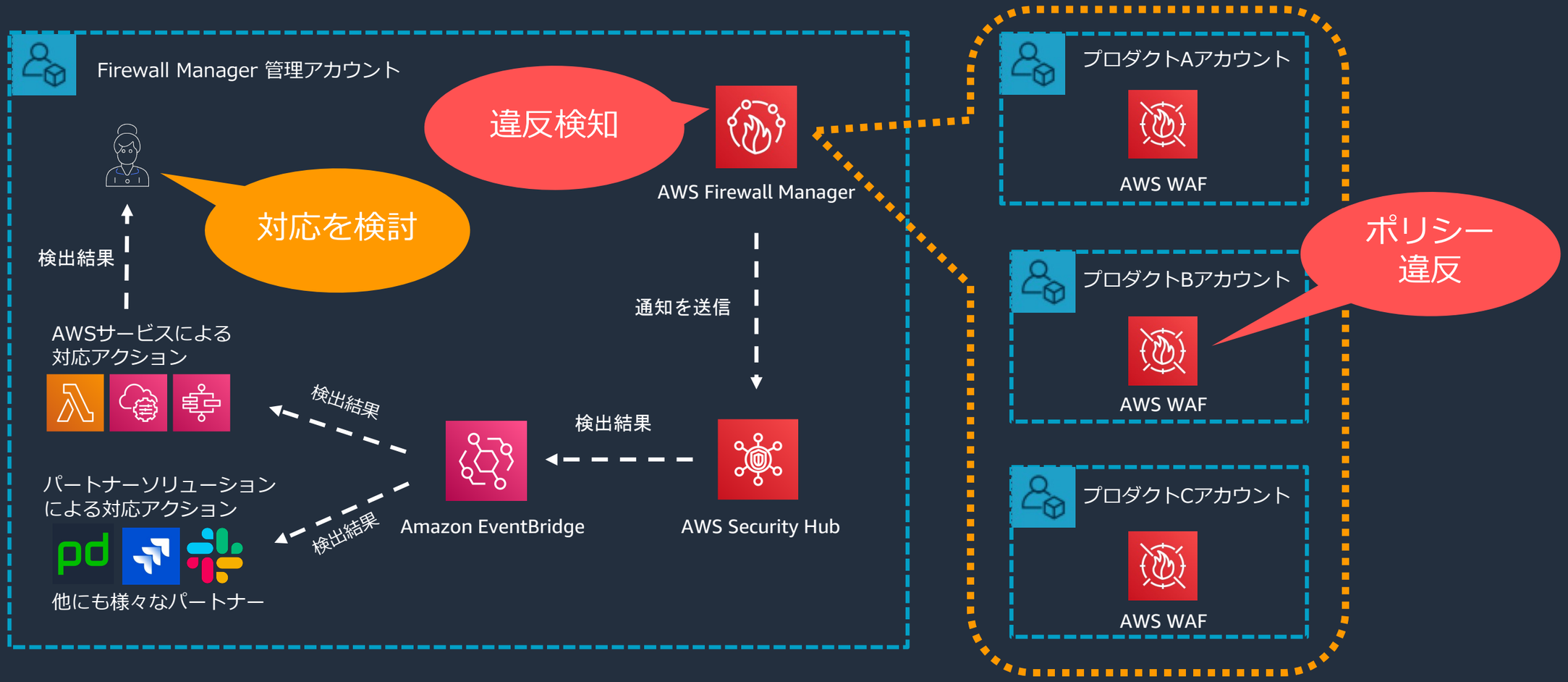
AWS Security Hub とは？

組織内の様々なセキュリティデータを集約して、一元的に
可視化するためのサービス



(抜粋) [AWS Black Belt Online Seminar] AWS Security Hub
https://d1.awsstatic.com/webinars/jp/pdf/services/20201013_AWS-BlackBelt-AWSSecurityHub.pdf

AWS Firewall Manager と AWS Security Hub との連携



※Firewall Manager はデフォルトで Security Hub と連携

アジェンダ

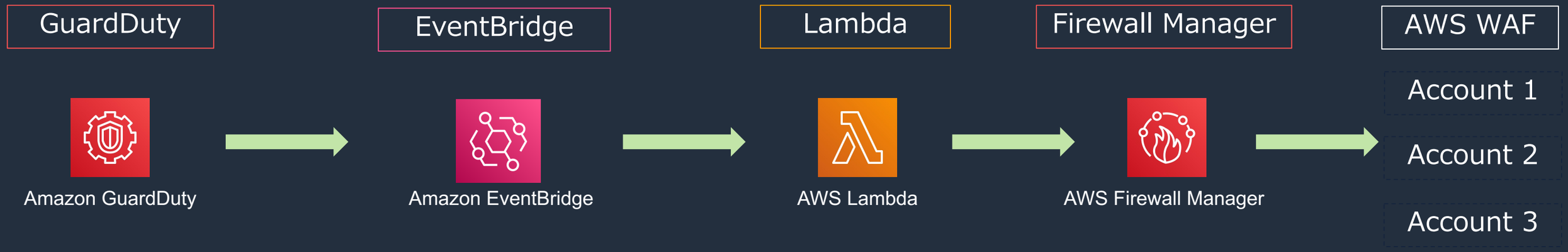
1. AWS Firewall Manager とは
2. AWS Firewall Manager をはじめるには (AWS Organizations との連携)
3. AWS Firewall Manager による AWS WAF 用のポリシー設定
4. AWS Firewall Manager のその他の設定
5. AWS Firewall Manager と AWS Security Hub との連携
6. AWS Firewall Manager の色々な使い方
7. AWS Firewall Manager のクォータについて
8. AWS Firewall Manager の料金について
9. 参考情報
10. まとめ

セキュリティのベースラインを整える

- 自社セキュリティのベースラインを Firewall Manager で担保する
- 世の中の脆弱性に関する情報や Security Hub の検出結果を元に
  ポリシーの更新を行い、アジリティを損なわせずにセキュアな環境を担保する

インターネットからの攻撃に対する迅速な対応

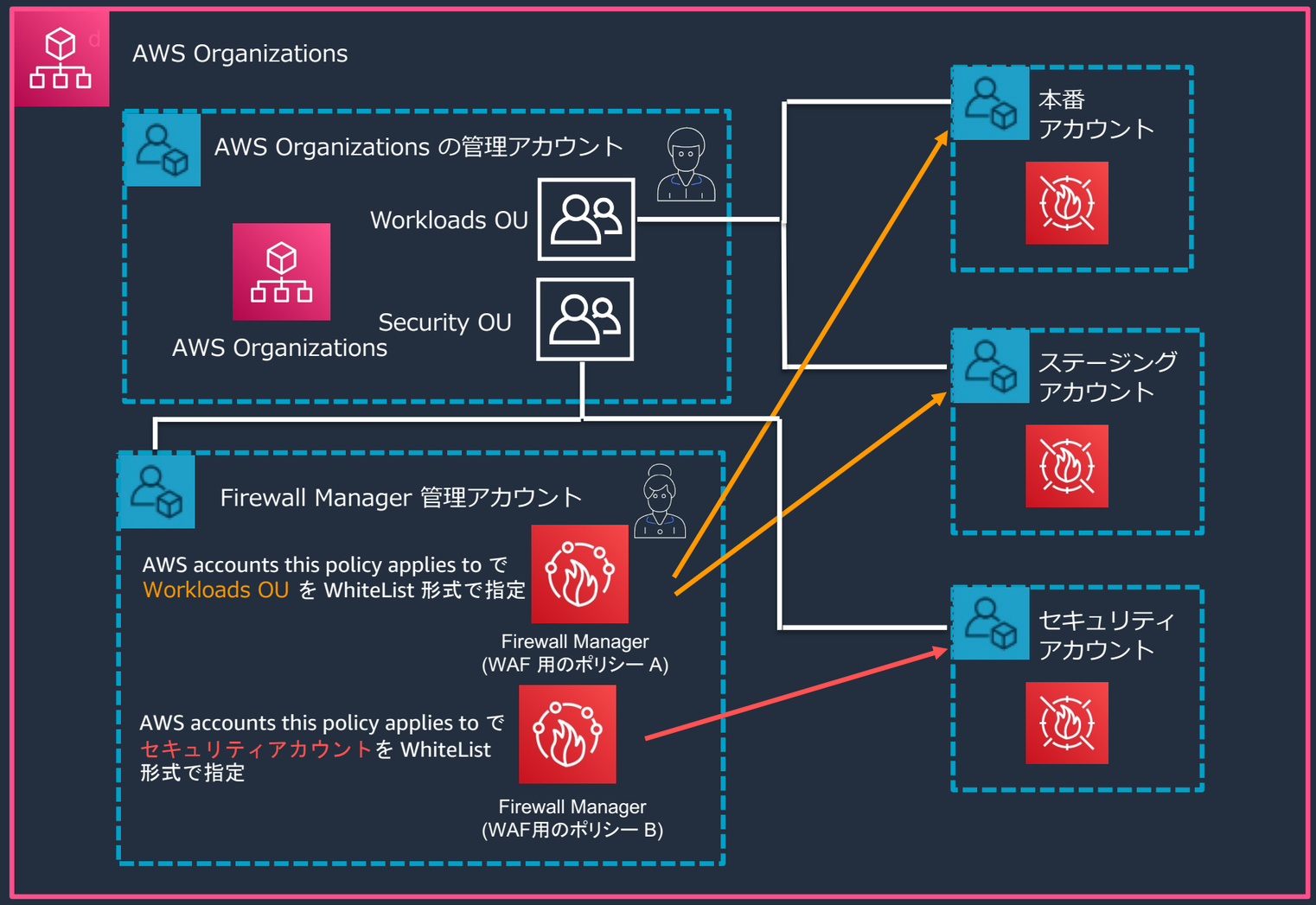
- セキュリティ管理者はコンソールから脅威情報をリアルタイムに把握し、数分以内に対応できる
- 組織内の全てのアプリケーションの脆弱性に対するパッチを素早く適応したり、GuardDuty で検知された不正な IP アドレスとの通信をブロックする



アカウント別に運用ポリシーを変更

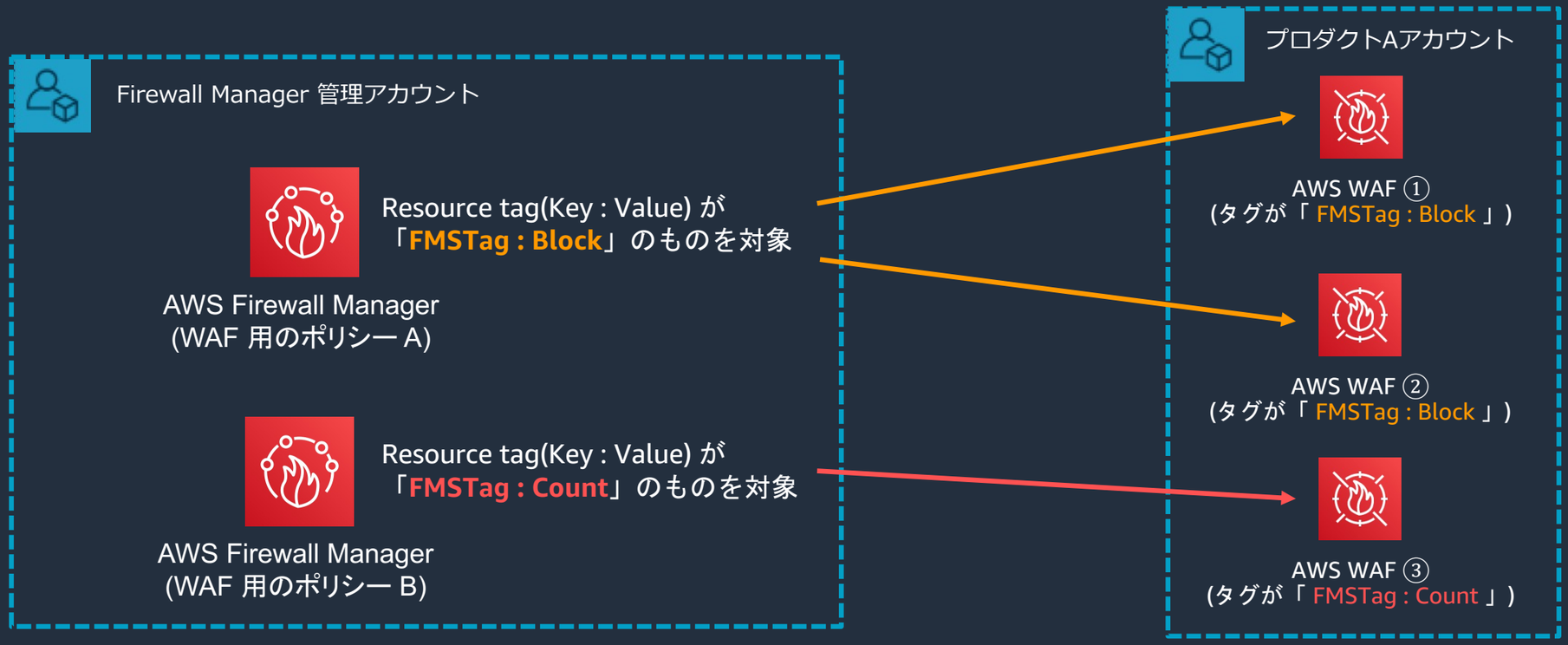
・アカウントもしくは OU を指定してポリシーの適用アカウントを指定することが可能

・逆に指定したアカウントもしくは OU だけにポリシーを適用しないという指定方法も可能



タグを用いた更に柔軟な運用

- タグを用いることでアカウントの中で更に細かい制御が可能
- Count モードで運用したいリソースと Block モードで運用したいリソースを
  下記のように柔軟に運用が可能 (ただし、作りすぎると多重管理になるので注意)



簡単に Firewall Manager を自社環境にデプロイする (AWS Firewall Manager Automations for AWS Organizations)

AWS Firewall Manager のオートメーション (実装ガイド)
https://d1.awsstatic.com/Solutions/ja_JP/automations-for-aws-firewall-manager.pdf

アジェンダ

1. AWS Firewall Manager とは
2. AWS Firewall Manager をはじめるには (AWS Organizations との連携)
3. AWS Firewall Manager による AWS WAF 用のポリシー設定
4. AWS Firewall Manager のその他の設定
5. AWS Firewall Manager と AWS Security Hub との連携
6. AWS Firewall Manager の色々な使い方
7. AWS Firewall Manager のクォータについて
8. AWS Firewall Manager の料金について
9. 参考情報
10. まとめ

AWS Firewall Manager のクォータ関連

代表的な AWS Firewall Manager の引き上げ可能なクォータ

リソース	デフォルトのクォータ
AWS Organizations の組織ごとの Firewall Manager ポリシー	20
Firewall Manager ポリシーあたりの範囲内の組織単位	20
Firewall Manager ポリシーの範囲内にあるアカウント (個々のアカウントを明示的に含めたり除外したりする場合)	200
Firewall Manager ポリシーの範囲内にあるアカウント (個々のアカウントを明示的に含めたり除外したりしない場合)	2500
Firewall Manager ポリシーごとのリソースを含む、または除外するタグ	8
Firewall Manager 管理者アカウントあたりの AWS WAF ルールグループ	100
AWS WAF ポリシー別のルールグループ	50

- Web サイトから上限緩和申請可能

  https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/fms-limits.html

アジェンダ

1. AWS Firewall Manager とは
2. AWS Firewall Manager をはじめるには (AWS Organizations との連携)
3. AWS Firewall Manager による AWS WAF 用のポリシー設定
4. AWS Firewall Manager のその他の設定
5. AWS Firewall Manager と AWS Security Hub との連携
6. AWS Firewall Manager の色々な使い方
7. AWS Firewall Manager のクォータについて
8. AWS Firewall Manager の料金について
9. 参考情報
10. まとめ

AWS Firewall Manager 価格

- **AWS Network Firewall 保護ポリシー**
  全パブリックリージョン： 100.00USD / ポリシー / リージョン
- **Amazon VPC セキュリティグループ保護ポリシー**
  全パブリックリージョン：100.00USD / ポリシー / リージョン
- **Amazon Route 53 Resolver DNS Firewall の保護ポリシー**
  全パブリックリージョン：100.00USD / ポリシー / リージョン
- **AWS WAF 保護ポリシー**
  全パブリックリージョン、グローバル (Amazon CloudFront ロケーション) ともに：
  100.00USD / ポリシー / リージョン (Shield Advanced の利用料に含まれる)
- **AWS Shield Advanced 保護ポリシー** (*1,*3)
  全パブリックリージョン、グローバル (Amazon CloudFront ロケーション) ともに：
  100.00USD / ポリシー / リージョン (Shield Advanced の利用料に含まれる)

アジェンダ

1. AWS Firewall Manager とは
2. AWS Firewall Manager をはじめるには (AWS Organizations との連携)
3. AWS Firewall Manager による AWS WAF 用のポリシー設定
4. AWS Firewall Manager のその他の設定
5. AWS Firewall Manager と AWS Security Hub との連携
6. AWS Firewall Manager の色々な使い方
7. AWS Firewall Manager のクォータについて
8. AWS Firewall Manager の料金について
9. 参考情報
10. まとめ

参考URL

- AWS Firewall Manager のデベロッパーガイド
  https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/fms-chapter.html
- Architecting for HIPAA Security and Compliance on Amazon Web Services
  https://d0.awsstatic.com/whitepapers/compliance/AWS_HIPAA_Compliance_Whitepaper.pdf
- AWS Services in Scope by Compliance Program
  https://aws.amazon.com/compliance/services-in-scope/
- AWS Firewall Manager のよくある質問
  https://aws.amazon.com/jp/firewall-manager/faqs/
- AWS Firewall Manager API Reference
  https://docs.aws.amazon.com/ja_jp/fms/2018-01-01/APIReference
- AWS Firewall Manager の価格
  https://aws.amazon.com/jp/firewall-manager/pricing/

アジェンダ

1. AWS Firewall Manager とは
2. AWS Firewall Manager をはじめるには (AWS Organizations との連携)
3. AWS Firewall Manager による AWS WAF 用のポリシー設定
4. AWS Firewall Manager のその他の設定
5. AWS Firewall Manager と AWS Security Hub との連携
6. AWS Firewall Manager の色々な使い方
7. AWS Firewall Manager のクォータについて
8. AWS Firewall Manager の料金について
9. 参考情報
10. まとめ

まとめ

- ✓ AWS Organizations との統合によるアカウント間保護ポリシー
- ✓ ポリシー不正変更の継続的監視とルールの自動修正
- ✓ リソースタイプやタグを用いたマルチアカウントのリソースグループ
- ✓ 階層ルールの適用 - 必須のグローバルルールとカスタマイズ可能なローカルルール
- ✓ 監査用コンプライアンス通知ができるダッシュボード
- ✓ コンプライアンス非準拠イベントの SNS 経由でのリアルタイム通知
- ✓ 組織全体に渡る脅威を一元集約して可視化

本資料に関するお問い合わせ・ご感想

- 技術的な内容に関しましては、有料の AWS サポート窓口へ
  お問い合わせください
  - https://aws.amazon.com/jp/premiumsupport/
- 料金面でのお問い合わせに関しましては、カスタマーサポート窓口へ
  お問い合わせください （マネジメントコンソールへのログインが必要です）
  - https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service
- 具体的な案件に対する構成相談は、後述する個別技術相談会をご活用ください

ご感想は Twitter へ！ハッシュタグは以下をご利用ください
#awsblackbelt

AWS の日本語資料の場所 「AWS 資料」 で検索

https://amzn.to/JPArchive

AWS のハンズオン資料の場所 「AWS ハンズオン」 で検索

https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/

AWS 個別相談会

- 毎週 「AWS 個別相談会」 を実施中
  - AWS のソリューションアーキテクト （SA） に対策などを相談することも可能

- 申込みは下記の URL から
  - https://pages.awscloud.com/JAPAN-event-SP-Weekly-Sales-Consulting-Seminar-2021-reg-event.html

AWS 個別相談会 で[検索]

ご視聴ありがとうございました