



# 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 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おります。  
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

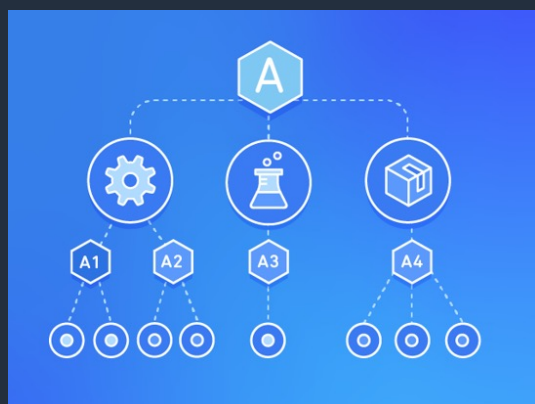
1. AWS Firewall Manager とは
2. AWS Firewall Manager をはじめるには (AWS Organizations との連携)
3. AWS Firewall Manager による AWS WAF 用のポリシー設定
4. AWS Firewall Manager のその他の設定
5. AWS Firewall Manager と AWS Security Hub との連携
6. AWS Firewall Manager の色々な使い方
7. AWS Firewall Manager のクォータについて
8. AWS Firewall Manager の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

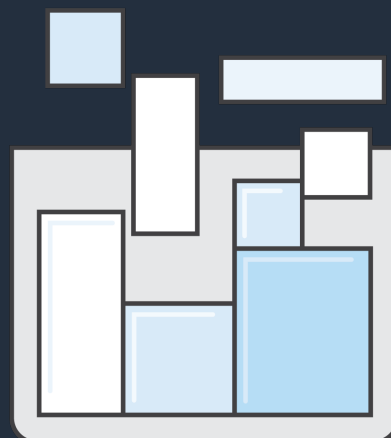
# こんなお困りごとありませんか？

大量のアカウントや  
リソース



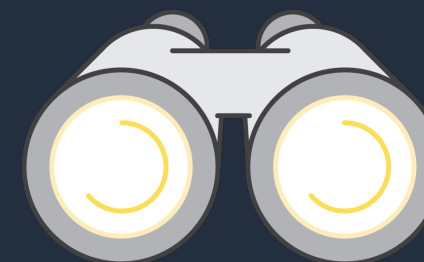
全てのアカウントや  
リソースに対する  
セキュリティポリシーの  
集約管理・維持が大変

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

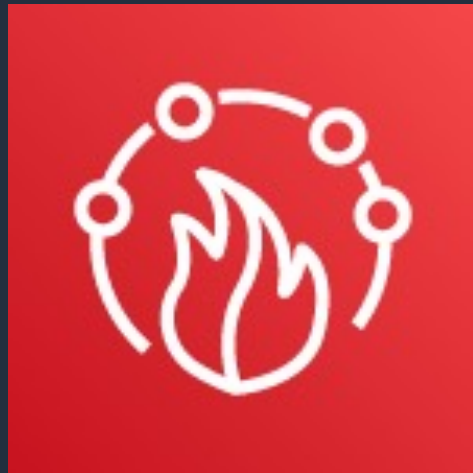
組織全体に渡る  
脅威対策の可視化



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

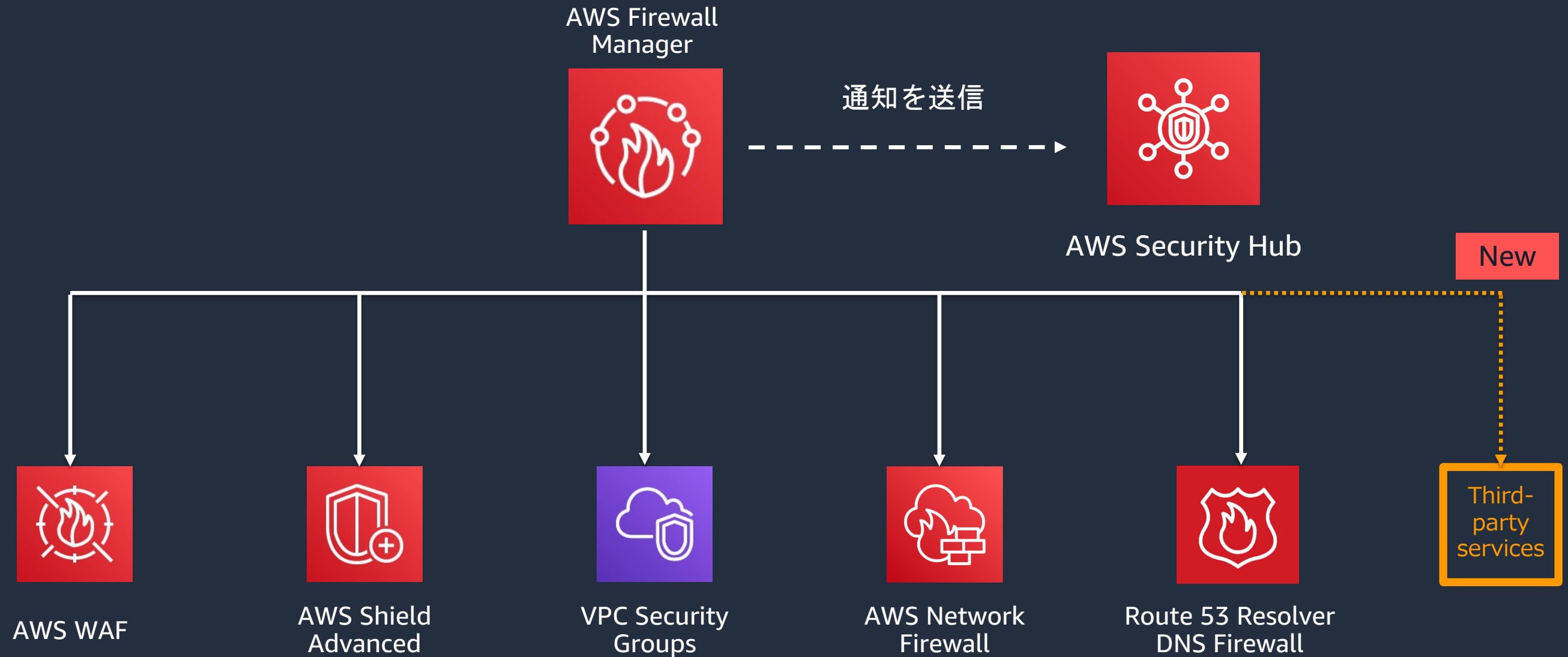


# AWS Firewall Manager とは

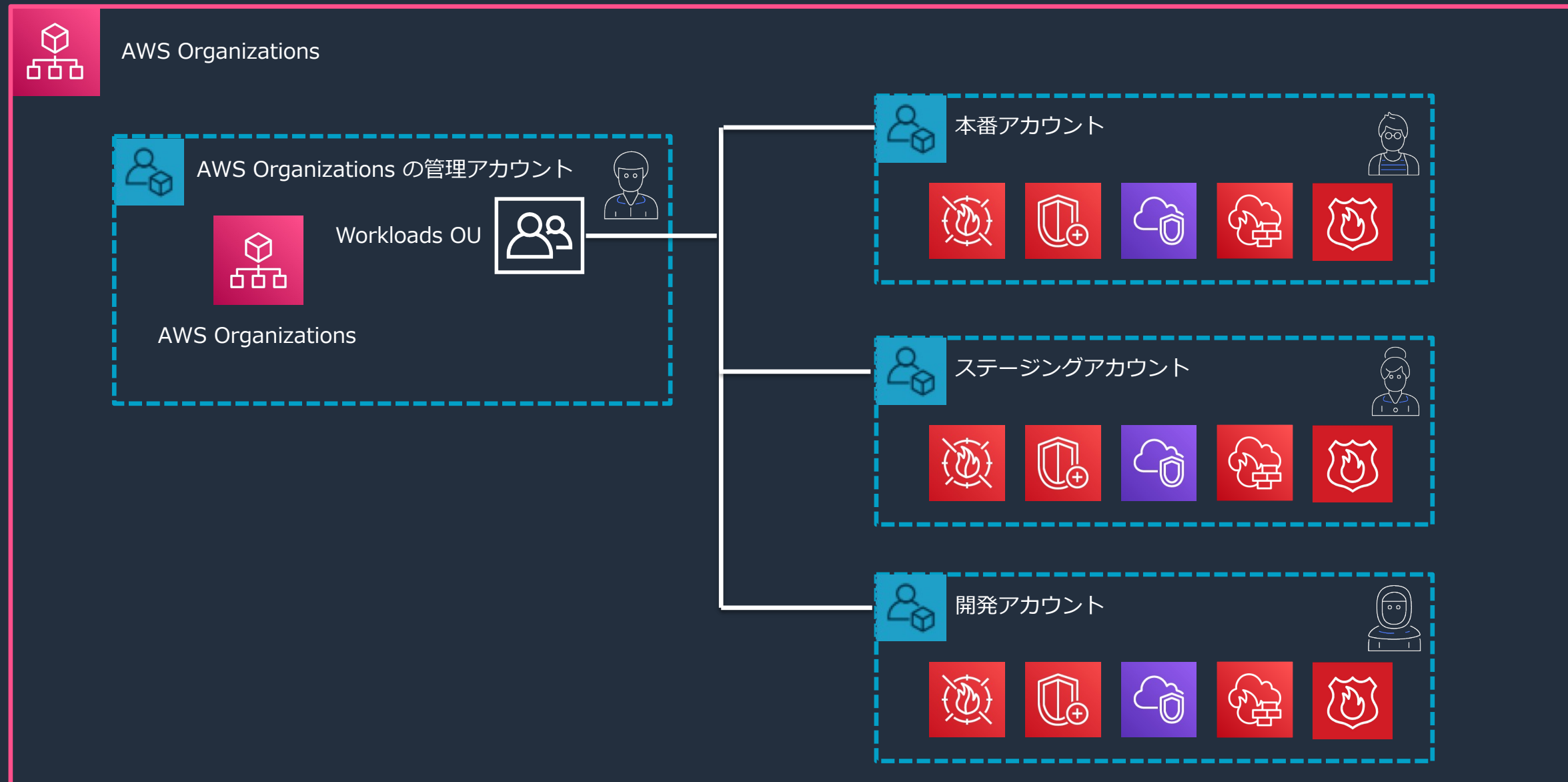


AWS Firewall Manager とは AWS Organizations 配下で管理されている AWS アカウント内のいくつかのセキュリティサービスを中央集権的に設定、管理するためのセキュリティマネージメントサービスです。

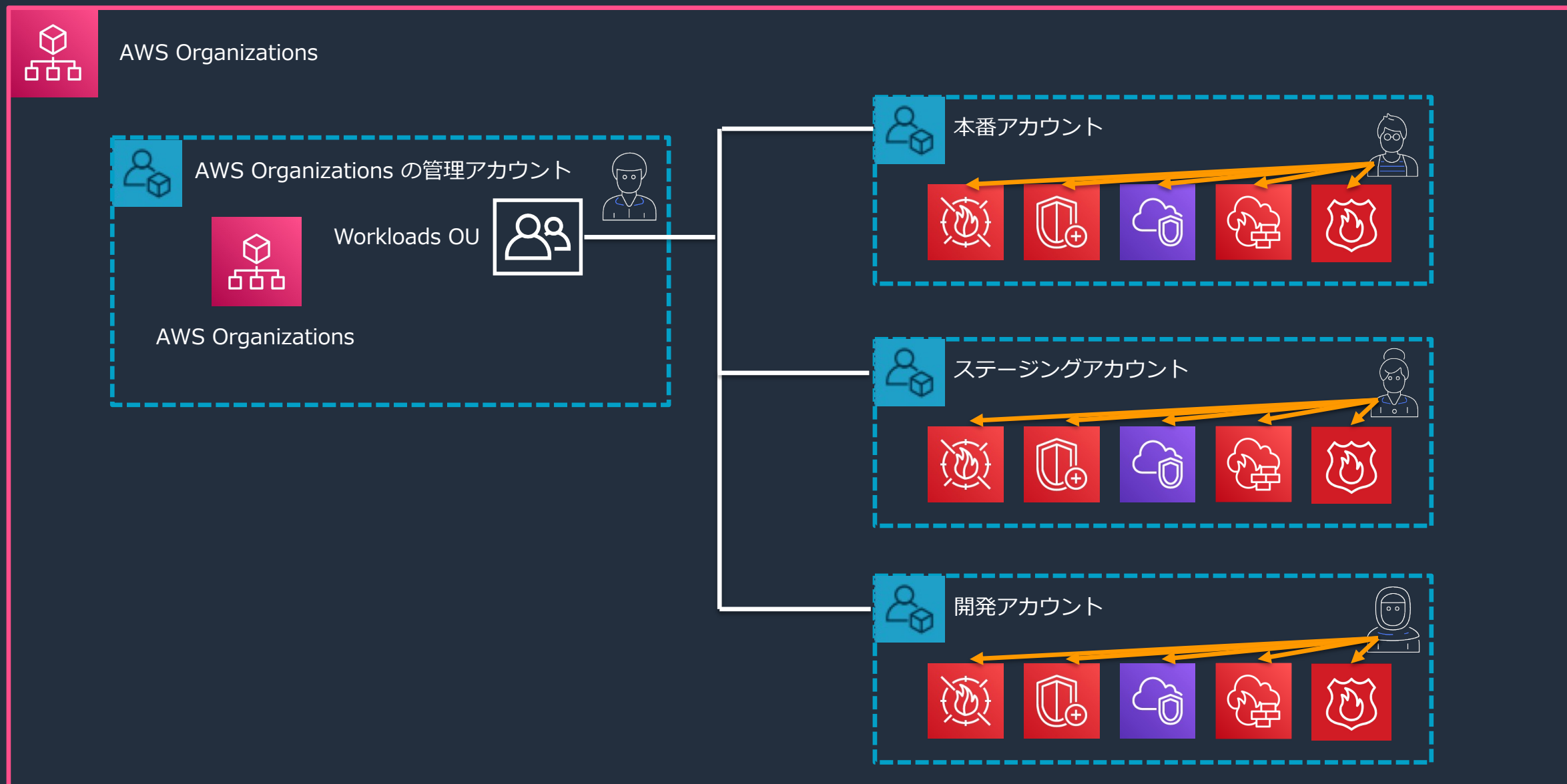
# AWS Firewall Manager が中央集権的に管理するサービス



# AWS Firewall Manager のイメージ



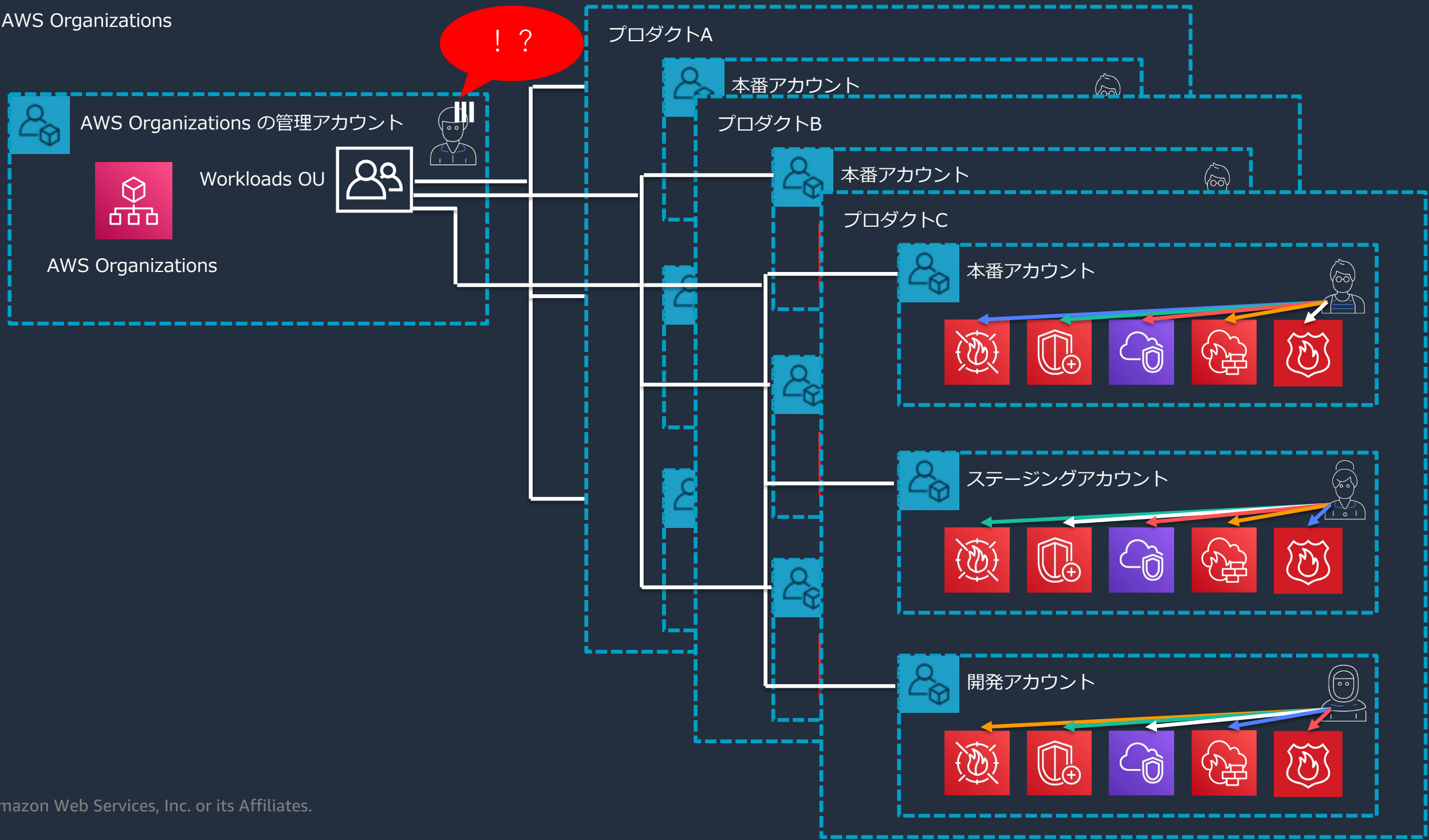
# AWS Firewall Manager のイメージ



# AWS Firewall Manager が解決する課題について



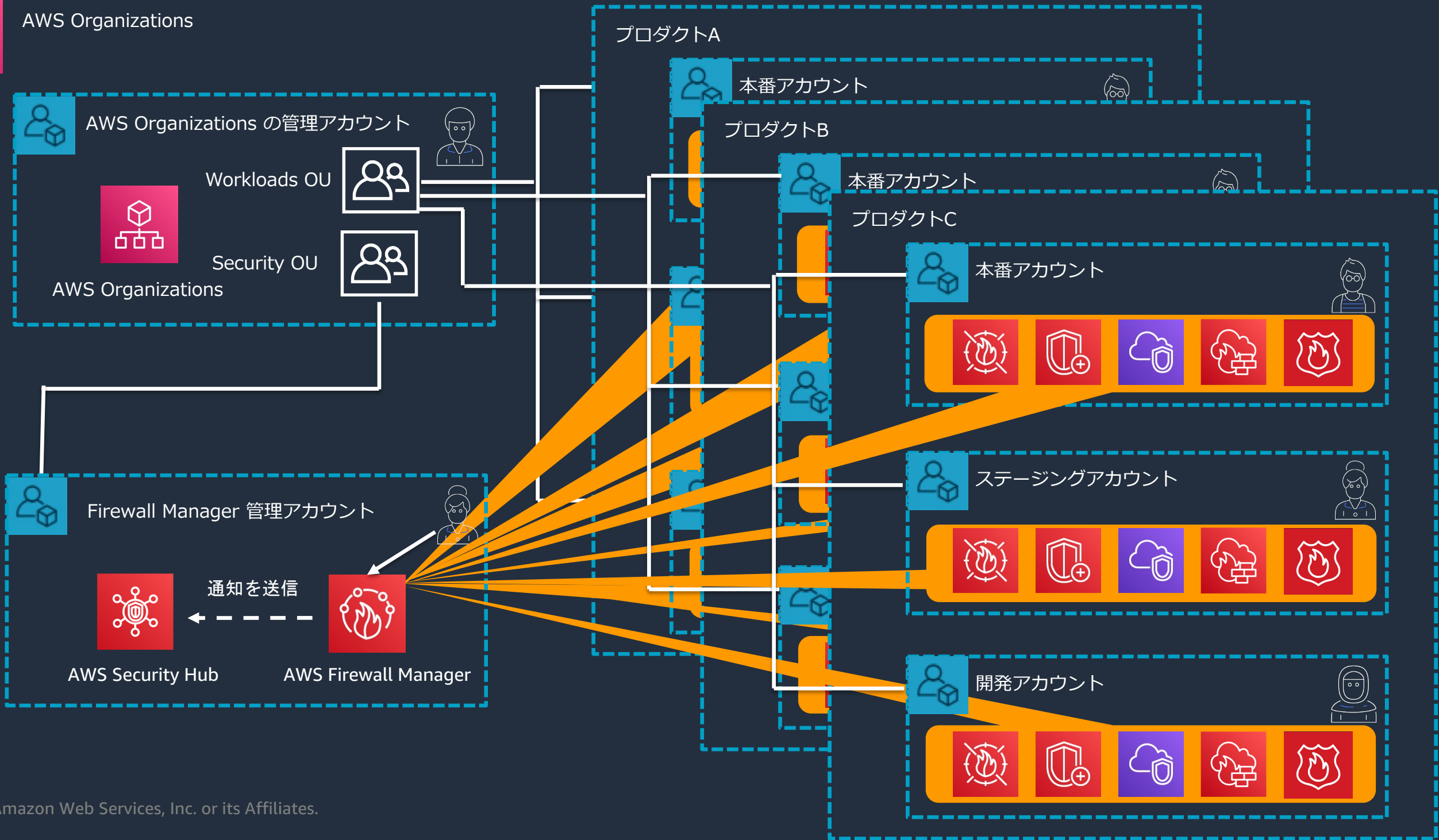
AWS Organizations



# AWS Firewall Manager が解決する課題について



AWS Organizations



# AWS Firewall Manager が解決する課題について



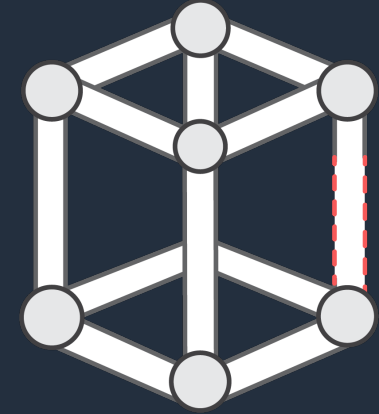
## ファイアウォールポリシー の一元管理

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

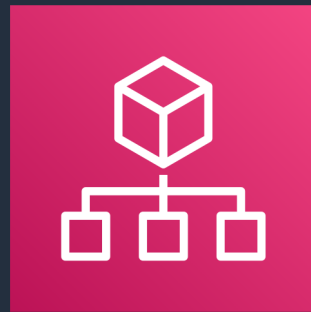
ポリシーベースのセキュリティグループ管理により、リソースを発見し、設定の逸脱を回避

# アジェンダ

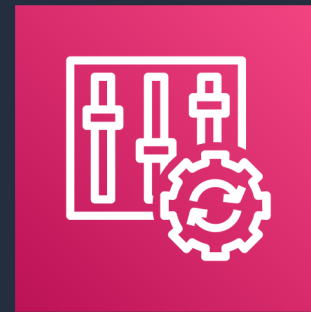
1. AWS Firewall Manager とは
2. AWS Firewall Manager をはじめるには (AWS Organizations との連携)
3. AWS Firewall Manager による AWS WAF 用のポリシー設定
4. AWS Firewall Manager のその他の設定
5. AWS Firewall Manager と AWS Security Hub との連携
6. AWS Firewall Manager の色々な使い方
7. AWS Firewall Manager のクォータについて
8. AWS Firewall Manager の料金について
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](https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/fms-prereq.html)

# AWS Firewall Manager の設定画面

WAF & Shield

AWS Firewall Manager > Security policies

AWS Firewall Manager policies (3)

Find policies

	Name	Policy type	Automatic remediation	Protected accounts	Noncompliant accounts	Policy ID
<input type="radio"/>	Corporate Common NetworkFirewall policy	AWS Network Firewall	-	1	0	5c11f8ad-...7a83
<input type="radio"/>	Corporate Common SecurityGroup	Security group - common	⚠ Disabled	1	1	7b7a289f-...97d36
<input type="radio"/>	Corporate Common WAF policy	WAF	⚠ Disabled	1	1	0c302c0e-...5b13a

Asia Pacific (Tokyo) Edit Delete Create policy

フィードバック 日本語

© 2008 - 2021, Amazon Web Services, Inc. またはその関連会社。無断転用禁止。 プライバシーポリシー 利用規約 Cookie の設定

(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 のマネージメントコンソール ( Global )



バージニア北部リージョン用



用のポリシー①

AWS WAF



用のポリシー②

AWS WAF



用のポリシー

AWS Shield Advanced



シンガポールリージョン用



用のポリシー③

AWS WAF



用のポリシー

VPC Security Groups



東京リージョン用



用のポリシー

AWS Network Firewall



用のポリシー

Route 53 Resolver DNS Firewall



# AWS Firewall Manager ポリシーの設定内容



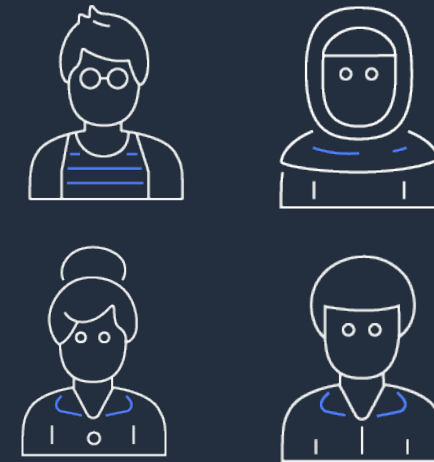
## AWS Firewall Manager ポリシー



ルール



アクション

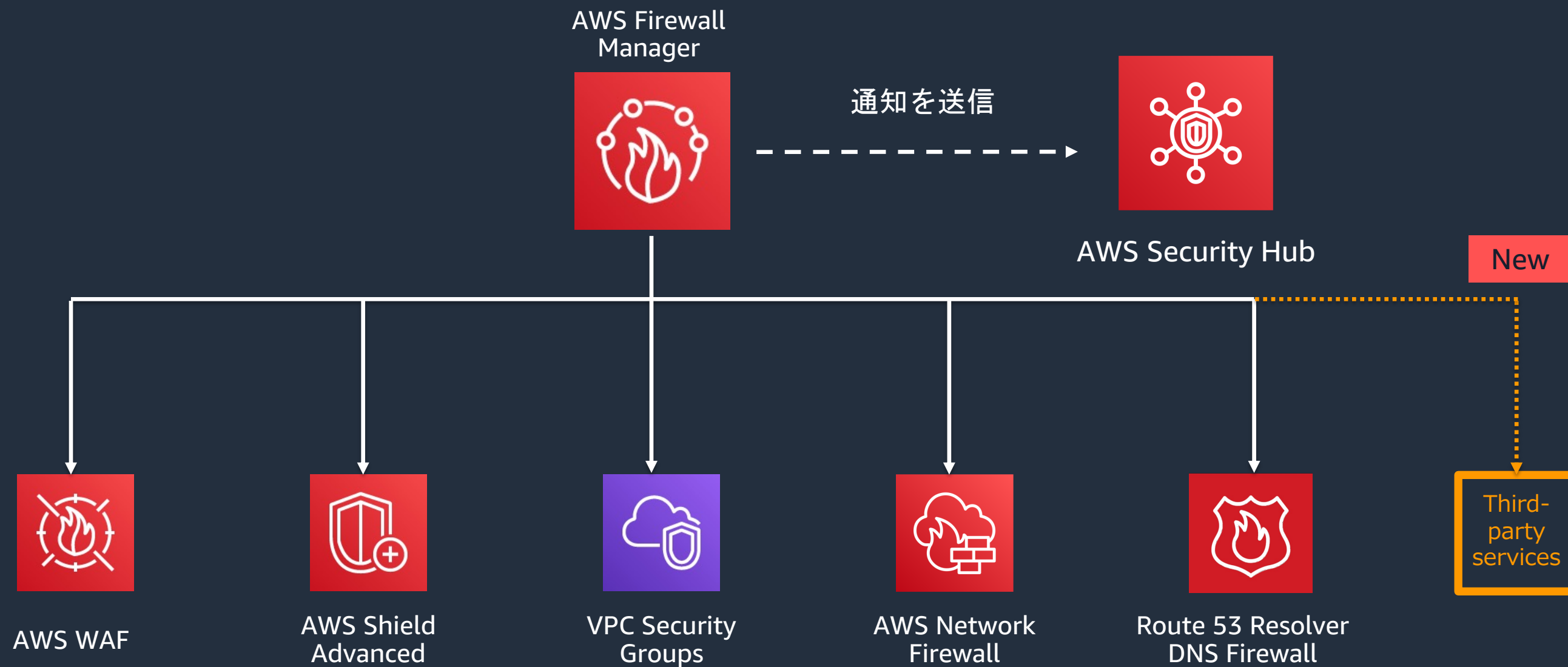


スコープ

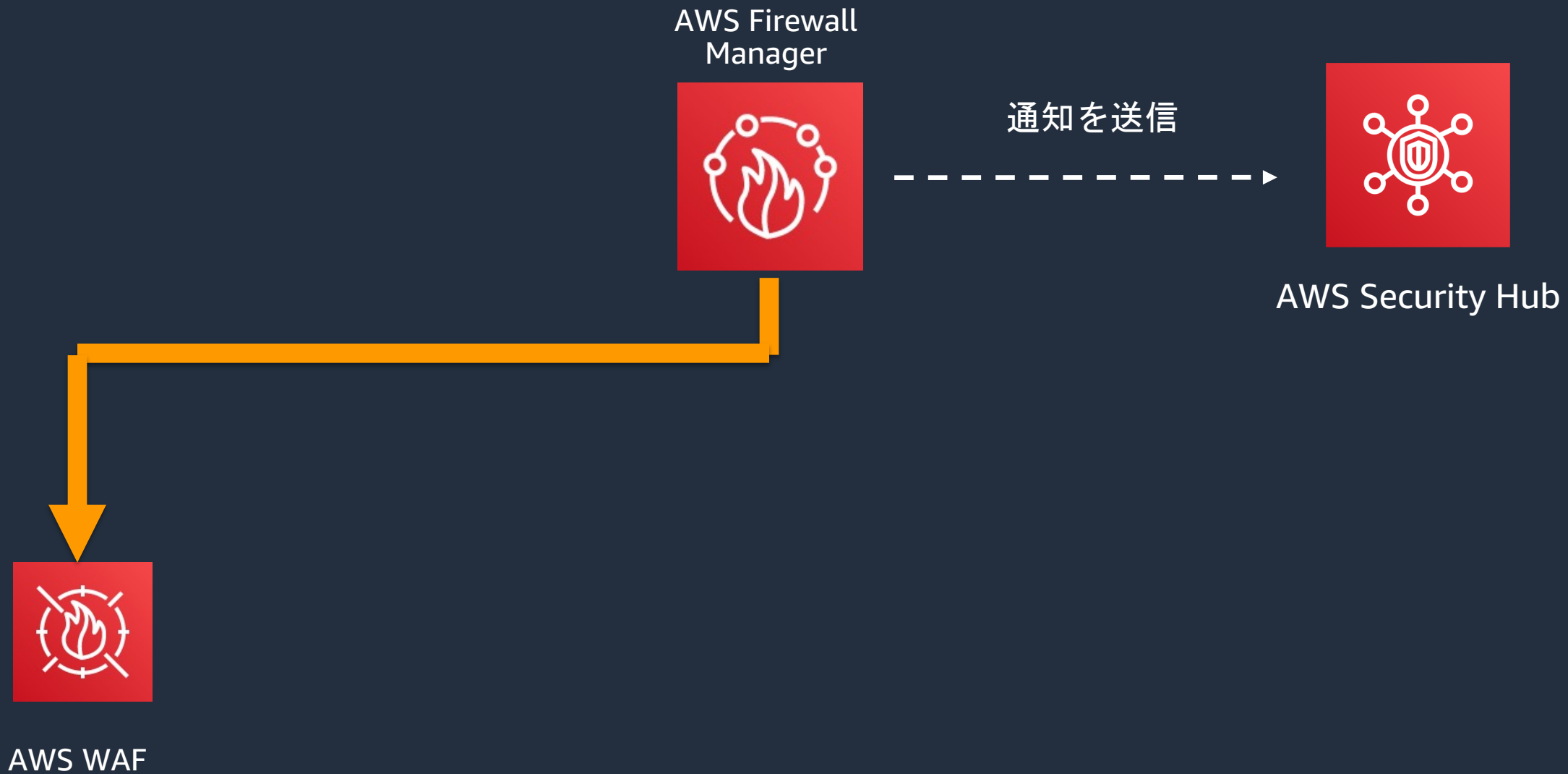
# アジェンダ

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

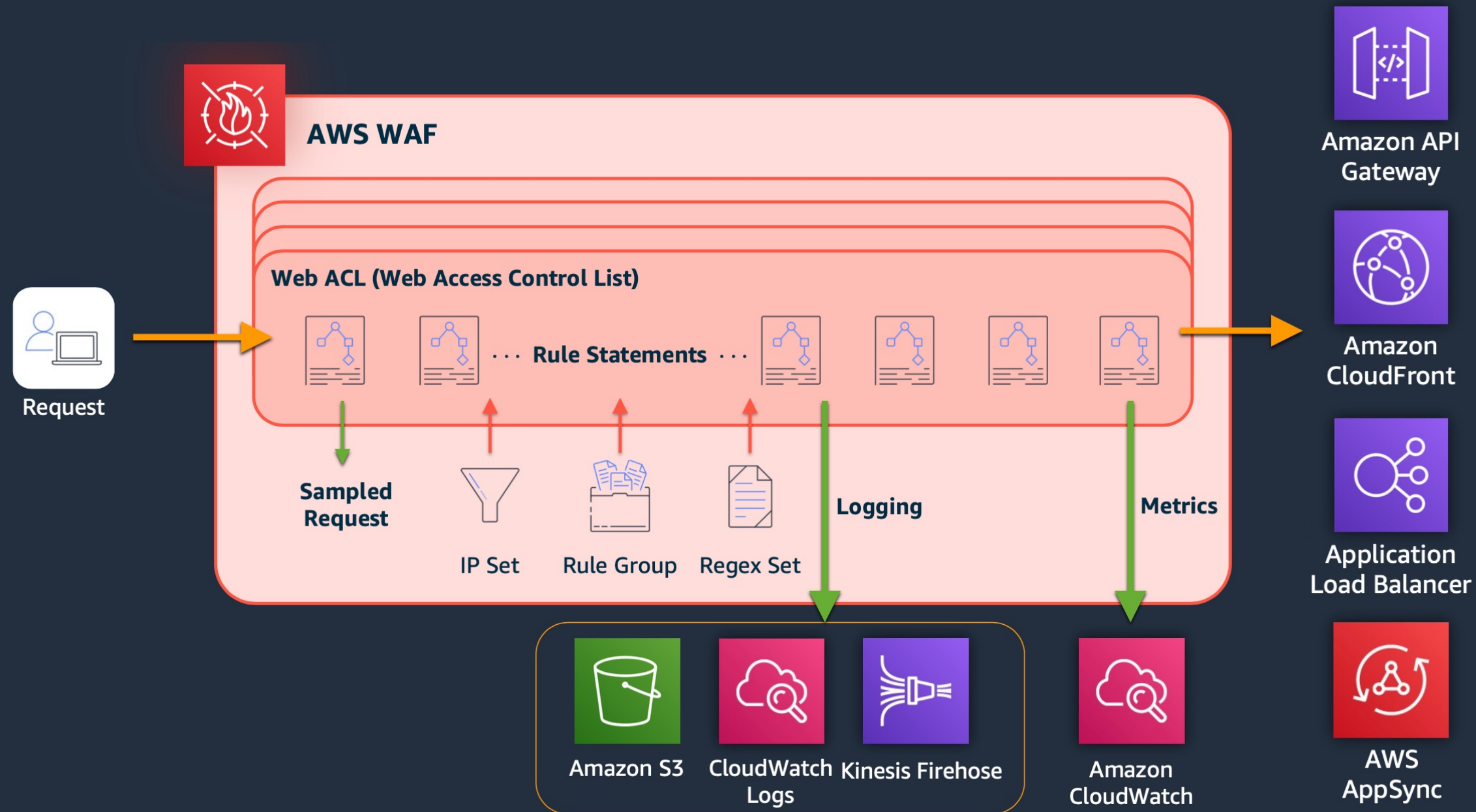
# AWS Firewall Manager が中央集権的に管理するサービス



# 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](https://d1.awsstatic.com/webinars/jp/pdf/services/20200324_AWS_BlackBelt_AWS_WAF_Update.pdf)



# AWS WAF 用の Firewall Manager ポリシーの設定概要



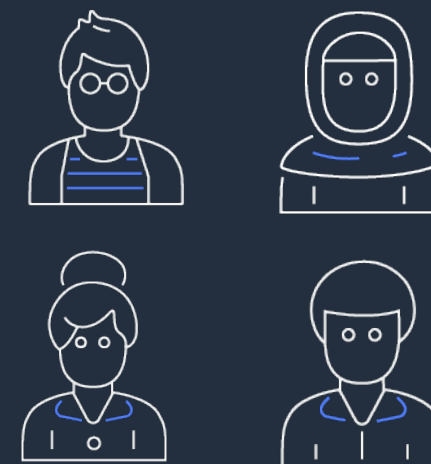
## AWS Firewall Manager ポリシー



ルール



アクション



スコープ

# AWS WAF 用の Firewall Manager ポリシーの設定概要



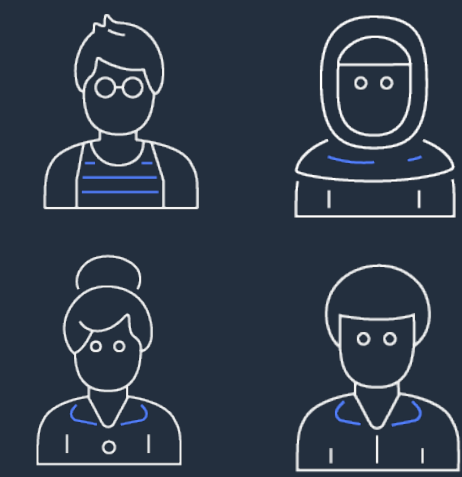
## AWS Firewall Manager ポリシー



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

**Policy rules**

Policy rules  
Associate all resources that are within the scope of this policy with the web ACL that's contained in this policy.

**Web ACL configuration**  
Firewall Manager creates this web ACL in all accounts that are within the policy scope. Define the rule groups to run first and the rule groups to run last when the web ACL inspects a web request. Then, in the individual accounts, the account owner can only add rule groups to be run in between these first and last rule groups.

**First rule groups**

▲ Move up ▼ Move down Edit Delete Add rule groups

Order	Rule group name	Capacity	Action
No rule groups You haven't added any rule groups.			

**Last rule groups**

▲ Move up ▼ Move down Edit Delete Add rule groups

Order	Rule group name	Capacity	Action
No rule groups You haven't added any rule groups.			

**Web ACL rule capacity units used**  
The total capacity units used by the web ACL can't exceed 1500  
0/1500 WCUs

**Default web ACL action for requests that don't match any rules in the web ACL**

Allow  
 Block

**Logging configuration**  
Capture information about the web requests that are evaluated by this web ACL. To configure this, you must have already defined an Amazon Kinesis Firehose Delivery Stream with a name that starts with 'aws-waf-logs-'.  
 Disabled  
 Enabled

**Sampled requests configuration**  
If you enable sampled requests, AWS WAF stores samples from the last 3 hours of requests that match the web ACL rules. Sampled requests are free of charge.  
 Enable sampled requests  
 Disable sampled requests  
 Enable sampled requests with exclusions

# 「Web ACL configuration」の設定について



AWS Firewall Manager アカウントにて  
AWS WAF ポリシーの「ルール」の設定



予め設定した IP の一覧 (IP sets) から来るリクエストは Block  
ルールグループ 1 [優先度1]

AWS WAF のマネージドルールである「Core rule set」を適用  
ルールグループ 2 [優先度2]

First rule groups

各アカウントで定義した AWS WAF のルールグループを設定が可能

日本から来たリクエストのみを許可  
ルールグループ 1 [優先度1]

Last rule groups



アカウント A の AWS WAF の設定



5 分間あたりの同一 IP アドレスからのリクエスト数が X 回ならブロック  
ルールグループ 1 [優先度1]



アカウント B の AWS WAF の設定



AWS WAF のマネージドルールである「Bot Control」を適用  
ルールグループ 1 [優先度1]

AWS WAF のマネージドルールである「PHP application」を適用  
ルールグループ 2 [優先度2]



# 「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

Capture information about the web requests that are evaluated by this web ACL. To configure this, you must have already defined an Amazon Kinesis Firehose Delivery Stream with a name that starts with 'aws-waf-logs-'.

Disabled  
 Enabled

**IAM role**  
AWS Firewall Manager creates this role for you. The role grants AWS WAF the permission to write to the Kinesis Data Firehose delivery streams whose names start with 'aws-waf-logs-'.

AWSServiceRoleForWAFV2Logging

**Amazon Kinesis Data Firehose delivery stream**  
If you don't have a delivery stream with a name starting with 'aws-waf-logs-', you can create one from the Kinesis console. Note that you can only specify a delivery stream that exists within your account. Test your delivery stream to be sure that it has enough throughput to accommodate your organization's logs.

aws-waf-logs-waf-log-sample-firehose

**Redacted fields**

HTTP method  
 Query string  
 URI  
 Header

Enter the names of the headers that you want to redact

Enter value

**Log filters**

**Filter 1**

Filter requirement

Match all of the filter conditions  
 Match at least one of the filter conditions

Filter conditions

Rule action on request

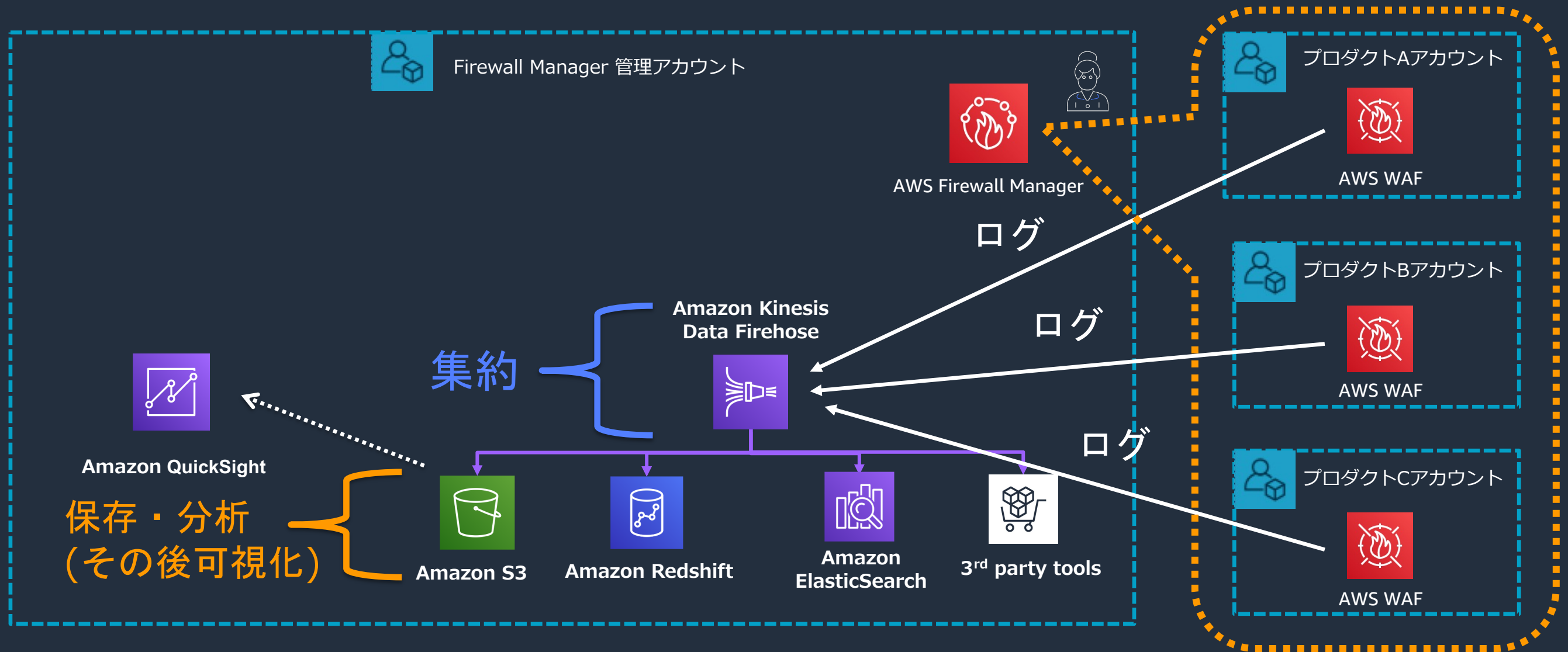
Filter behavior

Keep in logs  
 Drop from logs

**Default logging behavior**

Keep in logs  
 Drop from logs

# 「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

Sampled requests configuration

If you enable sampled requests, AWS WAF stores samples from the last 3 hours of requests that match the web ACL rules. Sampled requests are free of charge.

Enable sampled requests

Disable sampled requests

Enable sampled requests with exclusions

Request sampling for web ACL default action

Enabled

Disabled

Rules. Choose the rules that you want to disable request sampling for

Type	Name
<input checked="" type="checkbox"/> First rule groups	sample-montama-group
<input checked="" type="checkbox"/> First rule groups	AWS Core rule set
<input type="checkbox"/> Last rule groups	AWS Admin protection

設定画面

WAF & Shield

Sampled requests

Samples of requests from the past 3 hours.

Find sampled requests

Metric name	Source IP	URI	Rule inside rule group	Action	
PREFManaged-sample-montama-group-	(JP)	/sample.css	sample-montama-group#sample-rule	ALLOW	Sat Jun 25 2022 18:49:11 GMT+0900 (Japan Standard Time)
PREFManaged-sample-montama-group-	(JP)	/	sample-montama-group#sample-rule	ALLOW	Sat Jun 25 2022 18:49:11 GMT+0900 (Japan Standard Time)
PREFManaged-sample-montama-group-	(JP)	/sample.css	sample-montama-group#sample-rule	ALLOW	Sat Jun 25 2022 18:49:12 GMT+0900 (Japan Standard Time)
PREFManaged-sample-montama-group-	(JP)	/	sample-montama-group#sample-rule	ALLOW	Sat Jun 25 2022 18:49:07 GMT+0900 (Japan Standard Time)
PREFManaged-sample-montama-group-	(JP)	/sample.css	sample-montama-group#sample-rule	ALLOW	Sat Jun 25 2022 18:49:07 GMT+0900 (Japan Standard Time)
PREFManaged-sample-montama-	(JP)	/index2.php	sample-montama-group#sample-	ALLOW	Sat Jun 25 2022 18:49:08 GMT+0900 (Japan Standard Time)

All metrics

- All metrics
- FMMManagedWebACL2CloudFrontWAF
- PREFManaged-sample-montama-group-
- PREFManaged-AWSManagedRulesCommonRuleSet-

サンプルの閲覧画面  
(AWS WAF側)

# AWS WAF 用の Firewall Manager ポリシーの設定概要



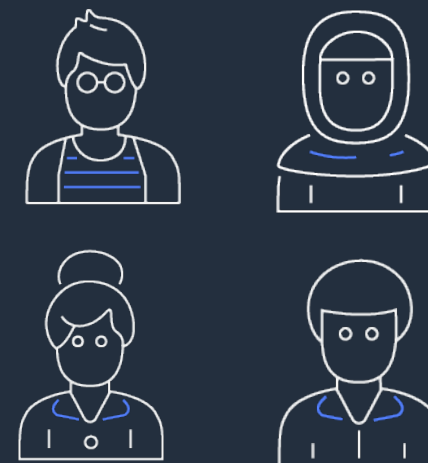
## AWS Firewall Manager ポリシー



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)

## Policy action

As a best practice, first identify and review the resources that don't comply with the policy rules, and then enable auto remediation to fix the noncompliant resources.

### Policy action

- Identify resources that don't comply with the policy rules, but don't auto remediate.
- Auto remediate any noncompliant resources.

### Replace existing associated web ACLs that aren't managed by another active Firewall Manager policy

- Replace web ACLs that are currently associated with in-scope resources with the web ACLs created by this policy

### Auto remediation steps

1. In noncompliant AWS accounts that are within policy scope, Firewall Manager creates a web ACL whose name starts with "FMManagedWebACLV2<Policy Name>", containing the rule groups that are defined in the policy.
2. Firewall Manager associates the web ACL with all noncompliant resources in the accounts.
3. If you chose to replace existing associated web ACLs, Firewall Manager disassociates other web ACLs that aren't managed by another active Firewall Manager policy from in-scope resources.

※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

# AWS WAF 用の Firewall Manager ポリシーの設定概要



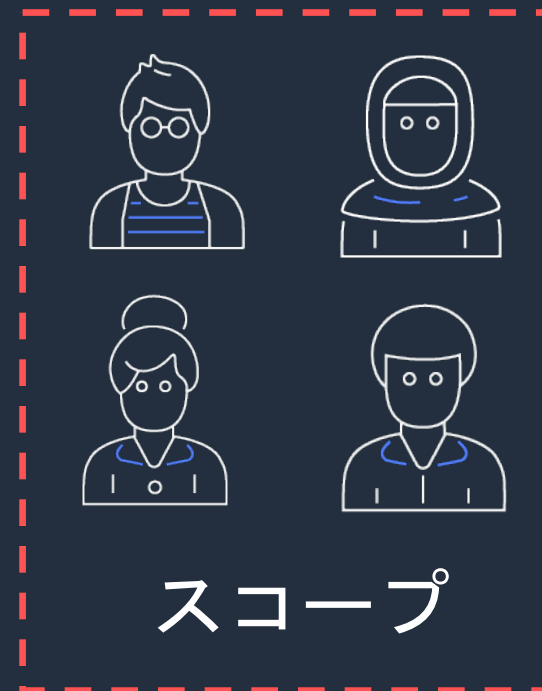
## AWS Firewall Manager ポリシー



ルール



アクション



スコープ

# AWS WAF 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

**Policy scope**  
Policy scope defines the accounts and resources covered by this policy.

AWS accounts this policy applies to

- Include all accounts under my AWS organization
- Include only the specified accounts and organizational units
- Exclude the specified accounts and organizational units, and include all others

Included AWS accounts Delete selection Edit list

AWS accounts

No Accounts added

Included organizational units Delete selection Edit list

Name	ID
No OUs added	

**Resource type**

- API Gateway Stage
- Application Load Balancer

**Resources**

- Include all resources that match the selected resource type
- Include only resources that have all the specified resource tags
- Exclude resources that have all the specified resource tags, and include all other resources

Resource tags

Key	Value - optional	
<input type="text"/>	<input type="text"/>	<span>Remove</span>

Add new tag


You can add 7 more tags.

# 「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)

**Resource cleanup**

Automatically remove protections from resources that leave the policy scope.

 **Warning**  
Enabling directs Firewall Manager to automatically remove Firewall Manager managed protections from customer resources when a member account or customer resource leaves the policy scope.

# 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

## ▼ AWS Firewall Manager

Getting started

Security policies

Application lists

Protocol lists

Settings

- 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

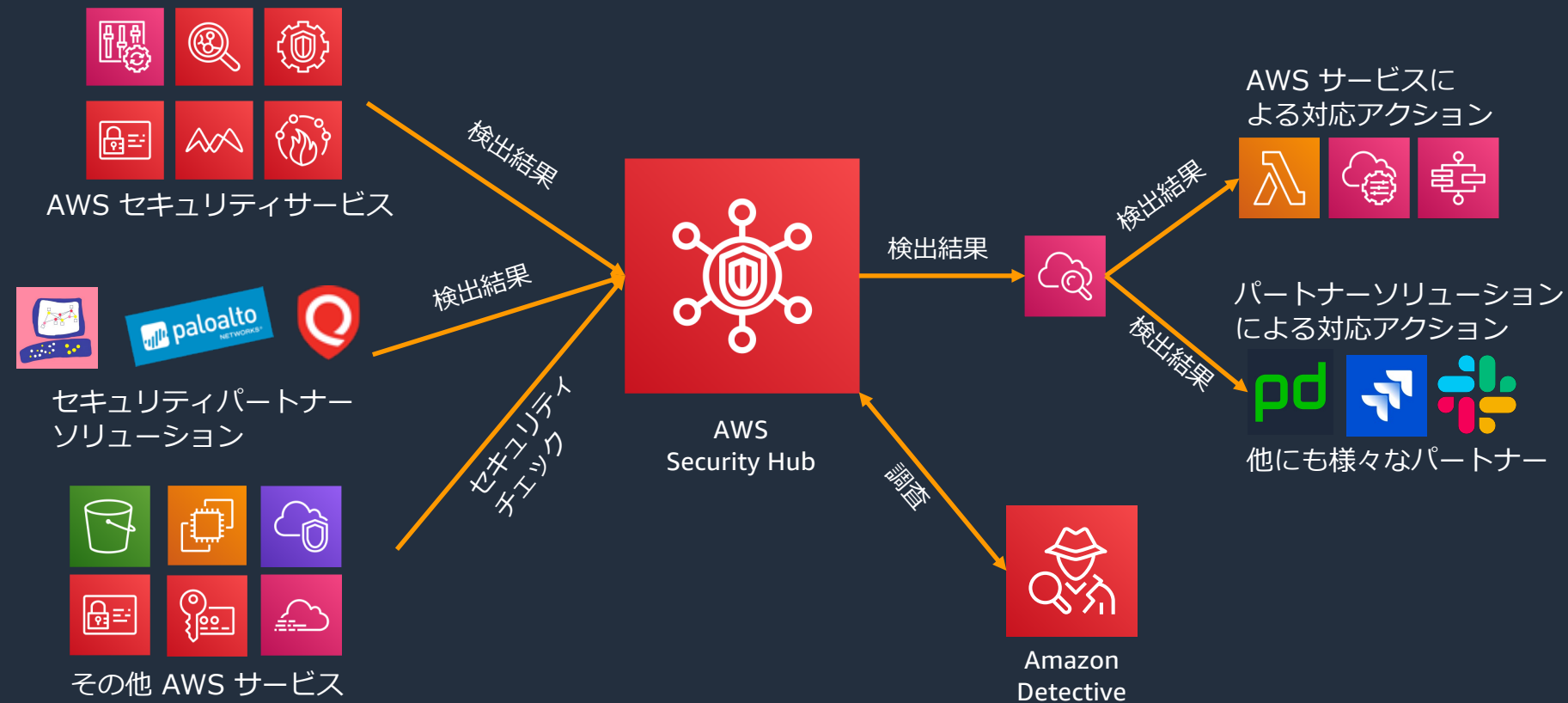
[https://docs.aws.amazon.com/ja\\_jp/waf/latest/developerguide/working-with-managed-lists.html](https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/working-with-managed-lists.html)

# 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

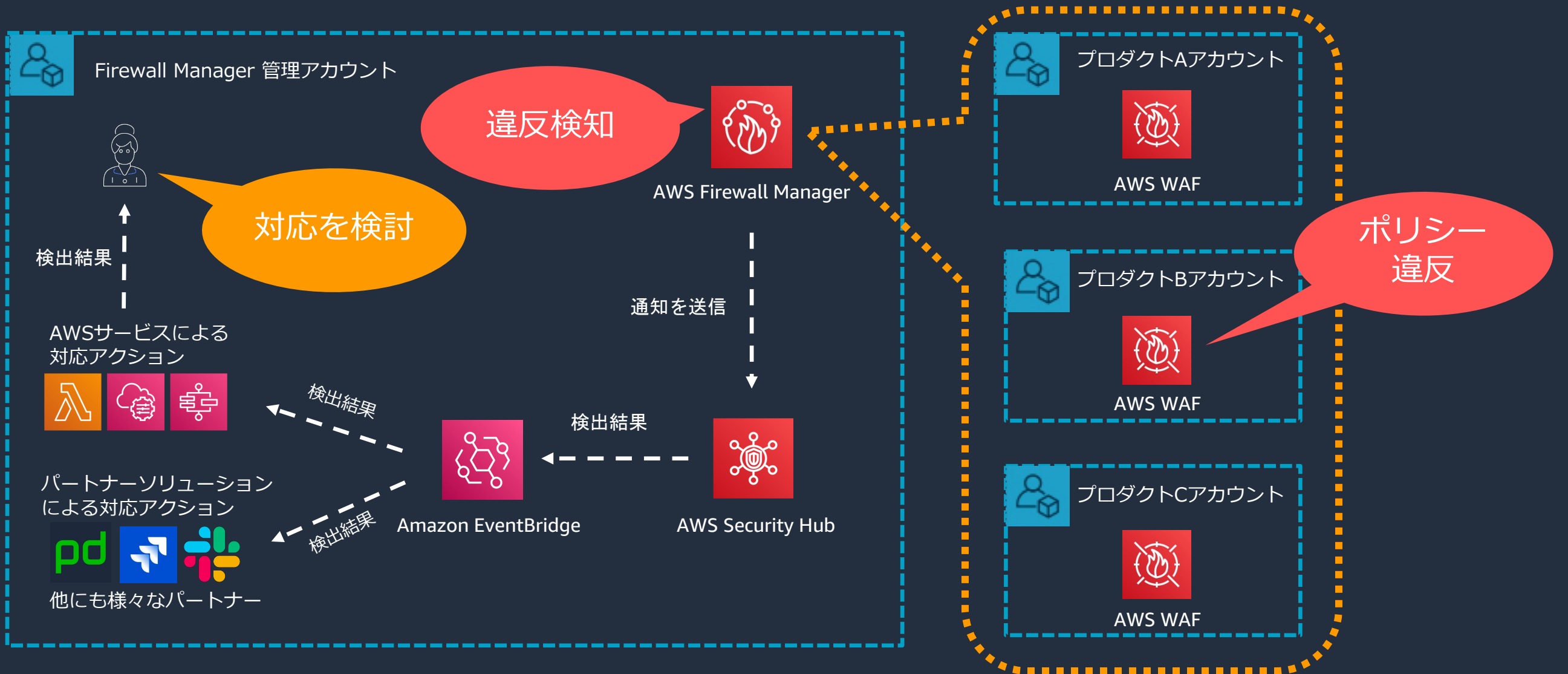


(抜粋) [AWS Black Belt Online Seminar] AWS Security Hub

[https://d1.awsstatic.com/webinars/jp/pdf/services/20201013\\_AWS-BlackBelt-AWSSecurityHub.pdf](https://d1.awsstatic.com/webinars/jp/pdf/services/20201013_AWS-BlackBelt-AWSSecurityHub.pdf)



# AWS Firewall Manager と AWS Security Hub との連携



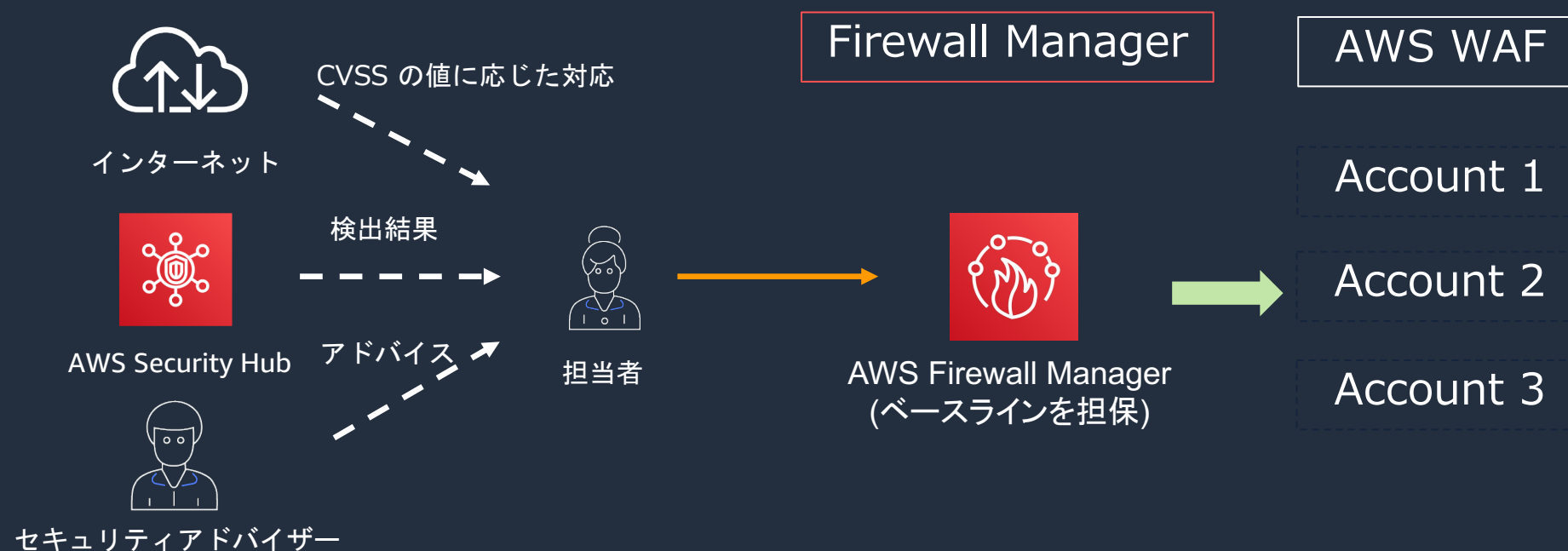
※Firewall Manager はデフォルトで Security Hub と連携

# 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

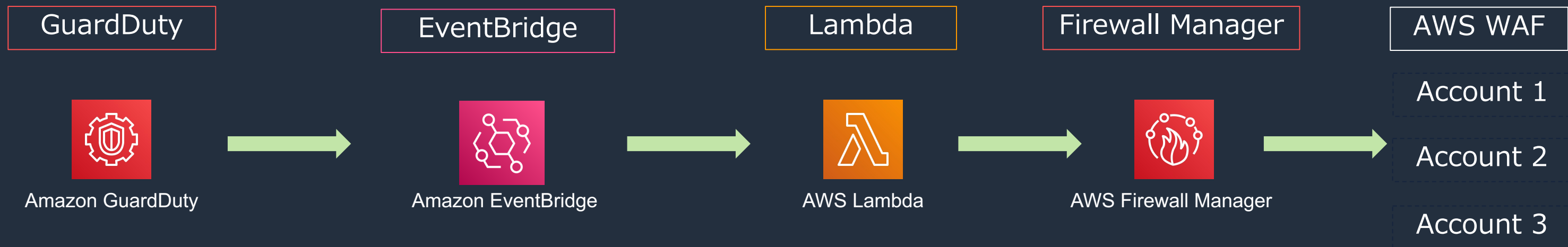
# セキュリティのベースラインを整える

- 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

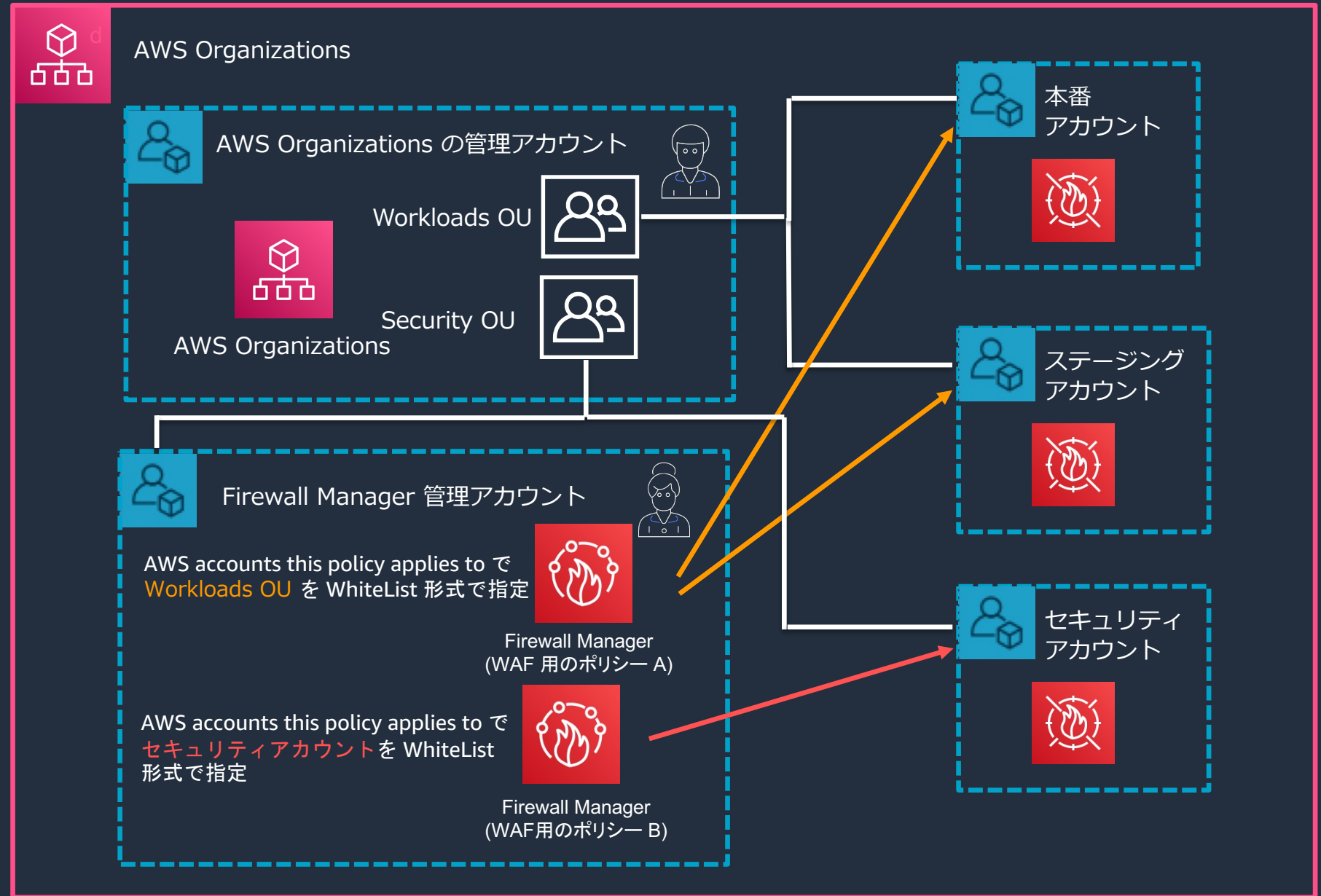
- セキュリティ管理者はコンソールから脅威情報をリアルタイムに把握し、数分以内に対応できる
- 組織内の全てのアプリケーションの脆弱性に対するパッチを素早く適応したり、GuardDuty で検知された不正な IP アドレスとの通信をブロックする



# アカウント別に運用ポリシーを変更

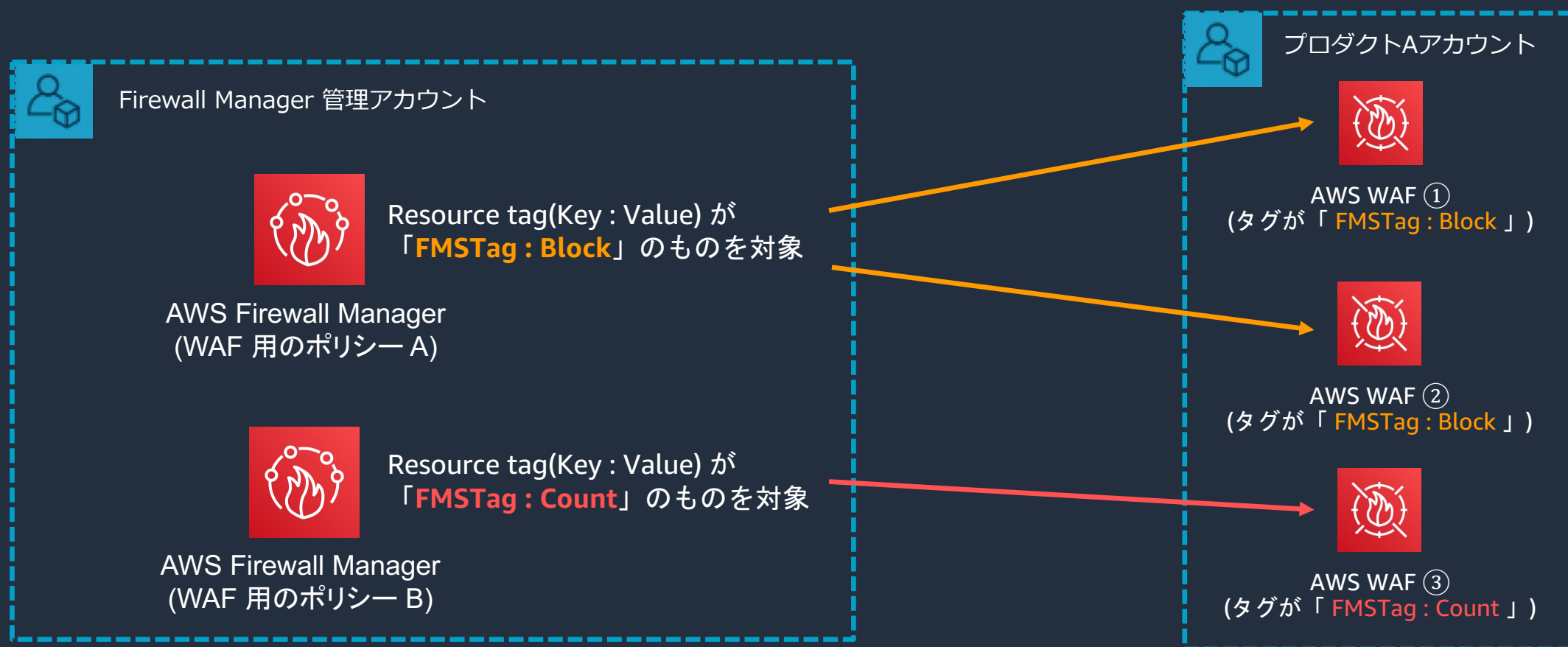
- ・アカウントもしくは OU を指定してポリシーの適用アカウントを指定することが可能

- ・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

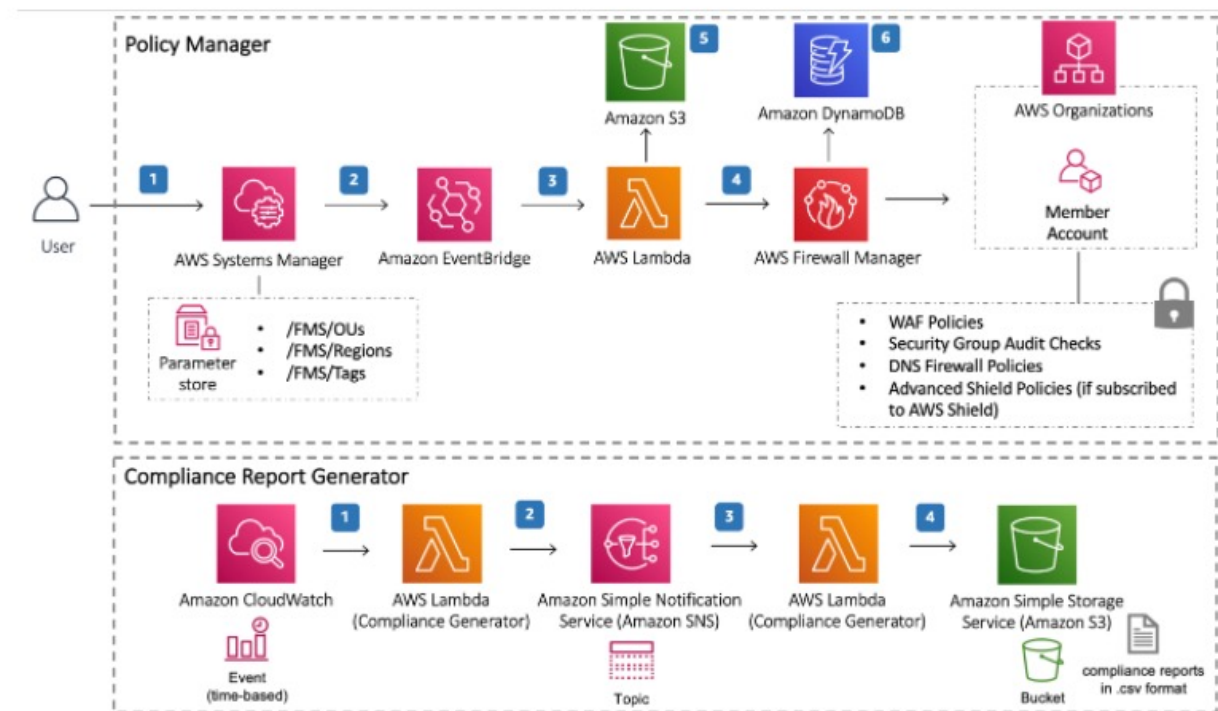
- タグを用いることでアカウントの中で更に細かい制御が可能
- Count モードで運用したいリソースと Block モードで運用したいリソースを下記のように柔軟に運用が可能 (ただし、作りすぎると多重管理になるので注意)



# 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 ソリューションの概要

下の図表は、このソリューションの実装ガイドと付属の AWS CloudFormation テンプレートを使用して、自動的にデプロイできるアーキテクチャを示しています。



[拡大イメージを見る](#)

## AWS Organizations 向けの AWS Firewall Manager のオートメーション

バージョン 2.0.1

最終更新日: 2022 年 4 月

作成者: AWS

見積りデプロイ時間: 3 分

[予想費用](#)

[ソースコード](#)

[CloudFormation テンプレート](#)

実装ガイドを表示

AWS コンソールで起動する

AWS IQ エキスパートでデプロイする

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](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](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](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](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](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



The screenshot shows the AWS Japanese website header with the logo and navigation links. The main content area features a large heading 'AWS クラウドサービス活用資料集トップ' and a paragraph of introductory text. Below the text are four buttons: 'AWS Webinar お申込', 'AWS 初心者向け', 'サービス別資料', and 'ハンズオン資料'.

aws お問い合わせ サポート ▼ 日本語 ▼ アカウント ▼ [今すぐ無料サインアップ »](#)

製品 ソリューション 料金 ドキュメント 学ぶ パートナーネットワーク AWS Marketplace イベント さらに詳しく見る 🔍

## AWS クラウドサービス活用資料集トップ

アマゾン ウェブ サービス (AWS) は安全なクラウドサービスプラットフォームで、ビジネスのスケールと成長をサポートする処理能力、データベースストレージ、およびその他多種多様な機能を提供します。お客様は必要なサービスを選択し、必要な分だけご利用いただけます。それらを活用するために役立つ日本語資料、動画コンテンツを多数ご提供しております。(本サイトは主に、AWS Webinar で使用した資料およびオンデマンドセミナー情報を掲載しています。)

[AWS Webinar お申込 »](#) [AWS 初心者向け »](#) [サービス別資料 »](#) [ハンズオン資料 »](#)

<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



## AWS ハンズオン資料

AWS をステップバイステップでお試しいただくのに役立つ動画および資料を掲載しています。

その他の資料は以下をご覧ください。

[初心者向けの資料](#) »

[サービス別の資料](#) »

[AWS オンラインセミナースケジュール](#) »

[AWS クラウドサービス活用資料集トップ](#) »

### AWS 初心者向けハンズオン

AWS 初心者向けに「AWS Hands-on for Beginners」と題し、初めて AWS を利用する方や、初めて対象のサービスに触る方向けに、操作手順の解説動画を見ながら自分のペースで進められるハンズオンをテーマごとにご用意しています。

<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