AWS Managed Rules for AWS WAF の活用

AWS Black Belt Online Seminar

岡　豊
Solutions Architect, Edge Services
2022/03

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3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

- 岡　豊（おか　ゆたか）
- 所属：Edge サービス担当ソリューションアーキテクト
- 担当サービス：
  - Amazon CloudFront
  - AWS Global Accelerator
  - AWS WAF
  - AWS Shield Advanced
  - AWS Firewall Manager

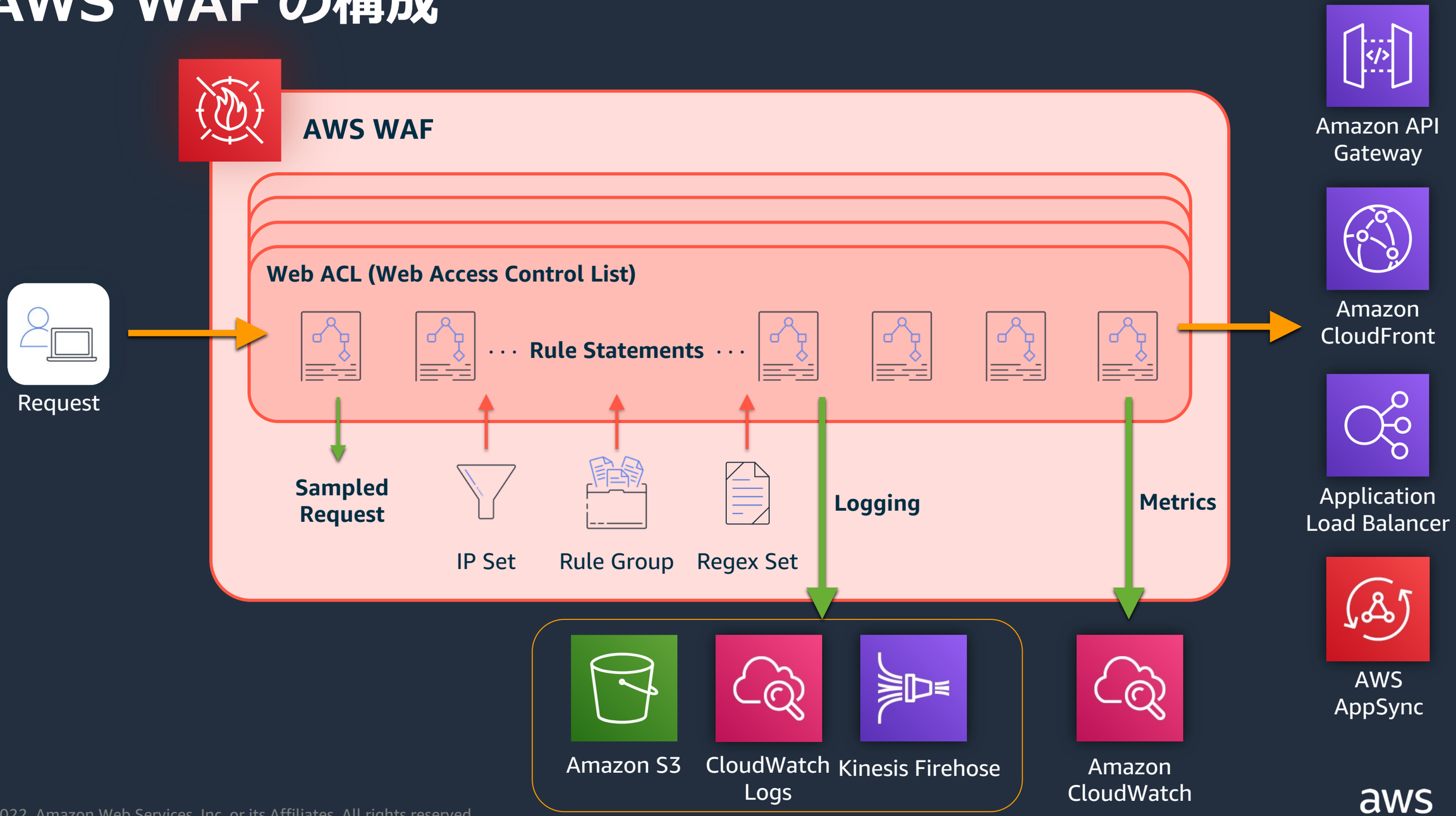
本セミナーの対象者

- WAF の一般的な知識をお持ちの方で、これから AWS Managed Rules for AWS WAF をご利用予定の方
- AWS Managed Rules for AWS WAF を既にご利用の方で、設定方法について更に理解を深めたい方

アジェンダ

1. AWS Managed Rules for AWS WAF の概要
2. マネージドルールの活用に役立つ新しい機能
3. 導入ステップとチューニング
4. まとめ

AWS WAF の構成

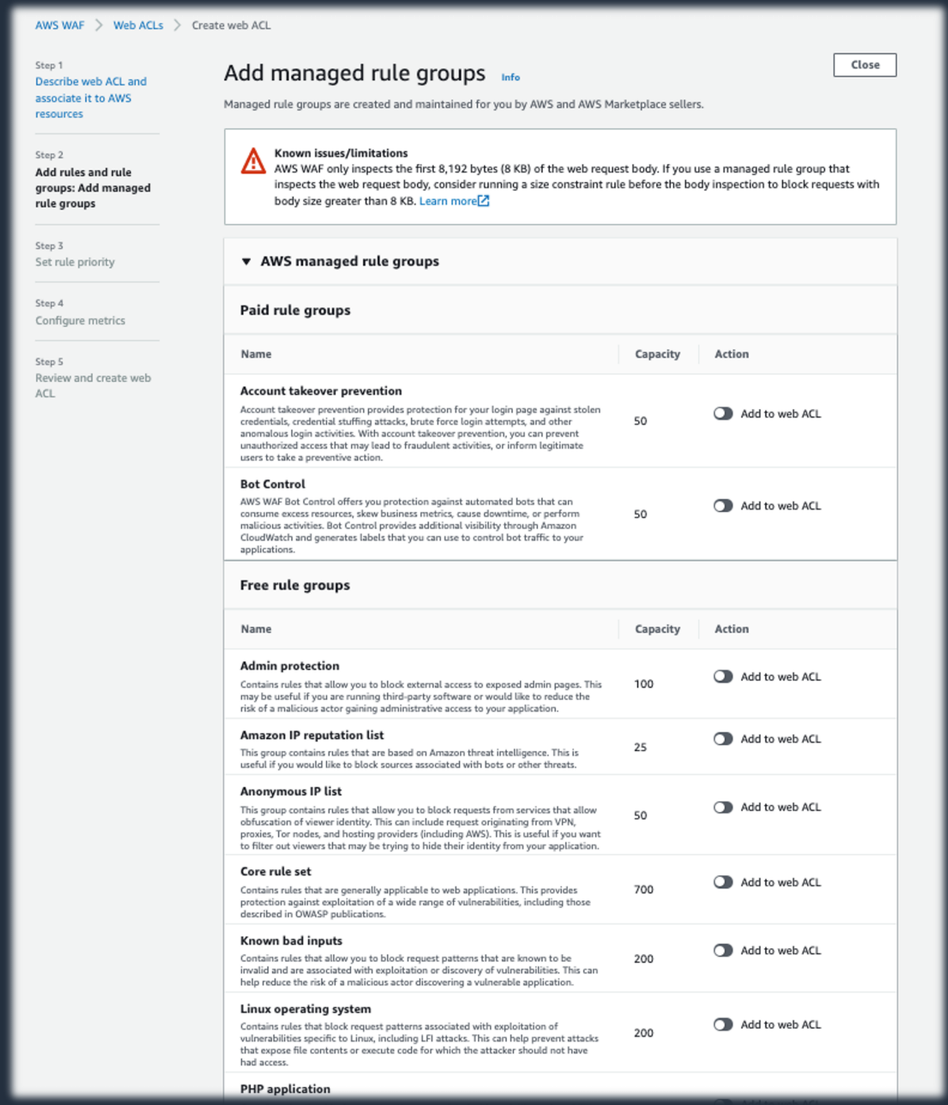


AWS Managed Rules for AWS WAF とは

お客様のアプリケーションに利用可能な事前に構成済みのルールセット

- 様々な脅威や高リスクな脆弱性に対する攻撃手法などに幅広く対応
- 脅威リサーチチームによる作成及びメンテナンスを実施
- ボット対策や不正なログイン試行の対策のルールも提供

一部のルールを除き、追加費用無しで利用可能



AWS WAF に導入可能なルールの種類

マネージドルール

- AWS が提供するマネージドルール (AWS Managed Rules for AWS WAF)
- パートナー提供のマネージドルール

独自のカスタムルール

- お客様が独自に作成可能なルール
- マネージドルールと組み合わせてカスタムルールを作成することが可能

AWS Managed Rules for AWS WAF の概要

AWS Managed Rules for AWS WAF の種類

- ベースラインルールグループ
- ユースケース別のルールグループ
- IP レピュテーションルールグループ
- Bot Control ルールグループ
- Account Takeover Prevention ルールグループ

ベースラインルールグループ

Free rule groups

- 様々な既知の脅威に対する一般的な対策ルールを提供
- これらのルールグループのうち1つ以上を選択して、対象のアプリケーションを保護する為のベースラインとなるルールを設定

Ruleset	Description
Core rule set (CRS)	OWASP Top 10 の脅威に基づく、一般的なウェブアプリケーションに適用可能な防御ルール
Admin protection	公開されている管理ページへの外部アクセスをブロックするためのルール
Known bad inputs	無効であることがわかっており、脆弱性の悪用または探索に関連するリクエストパターンをブロックするルール

ユースケース別ルールグループ

Free rule groups

- AWSWAF を利用する様々なユースケースに合わせた追加の保護対策を提供
- 保護対象のオペレーティングシステムやミドルウェア、アプリケーションによって、適切なルールを選択

Ruleset	Description
SQL database	SQL インジェクション攻撃など、SQL データベースの悪用に関連するリクエストパターンをブロックするルール
Linux operating system	Linux 固有のローカルファイルインクルージョン (LFI) 攻撃など、Linux 固有の脆弱性の悪用に関連するリクエストパターンをブロックするルール
PHP application	安全でない PHP 関数のインジェクションなど、PHP に固有の脆弱性の悪用に関連するリクエストパターンをブロックするルール
WordPress application	WordPress サイト特有の脆弱性の悪用に関連するリクエストパターンをブロックするルール
POSIX operating system	POSIX および POSIX と同等のオペレーティングシステムに固有の脆弱性の悪用 (ローカルファイルインクルージョン (LFI) 攻撃など) に関連するリクエストパターンをブロックするルール
Windows operating system	PowerShell コマンドのリモート実行など、Windows 固有の脆弱性の悪用に関連するリクエストパターンをブロックするルール

IP レピュテーションルールグループ

Free rule groups

- アプリケーションのアクセス元のソース IP アドレスに基づいてリクエストをブロック
- 不正なボットトラフィックや攻撃に利用されている IP アドレスからのアクセスを制限したい場合や、アクセス元の隠蔽を試みるアクセスからの制限が可能

Ruleset	Description
Amazon IP reputation list	ボットやその他の脅威に関連づけられている IP アドレスをブロックする、Amazon 内部の脅威インテリジェンスに基づくルール
Anonymous IP list	VPN、プロキシ、Tor ノード、ホスティングプロバイダー などのビューワーIDの難読化を許可するサービスからのリクエストをブロックするルール

Bot Control ルールグループ

Paid rule groups

ボットと判断されるトラフィックを検知し、それに基づいたアクションを行う

- ボットに特化した マネージドルールを提供
- リクエストによってボットの種別を表すラベルを追加
  - ラベル内にボットの種類と特徴（シグナル）を表す情報を付加

AWS WAFを利用する全てのユーザーは、Bot Control のルールグループを有効にせずとも、一定の可視性が得られる

- Bot Control ルールグループを利用した場合の効果を事前に取得し、利用の可否を決めることができる

https://aws.amazon.com/waf/features/bot-control/

aws

Account Takeover Prevention ルールグループ

Paid rule groups

ログインページに対する不正なアクセスから保護するためのルールグループ

- 盗まれた認証情報を利用したログイン試行を可視化及び制御
  - クレデンシャルスタッフィング攻撃
  - ブルートフォース攻撃
  - その他の異常なログイン試行
- POST されたデータを盗まれたクレデンシャルのデータベースと照合
- アプリケーション統合 SDK の利用で検知能力を向上（オプション）
  - JavaScript、iOS/Android SDK

https://docs.aws.amazon.com/waf/latest/developerguide/waf-atp.html

マネージドルールの活用に役立つ新しい機能

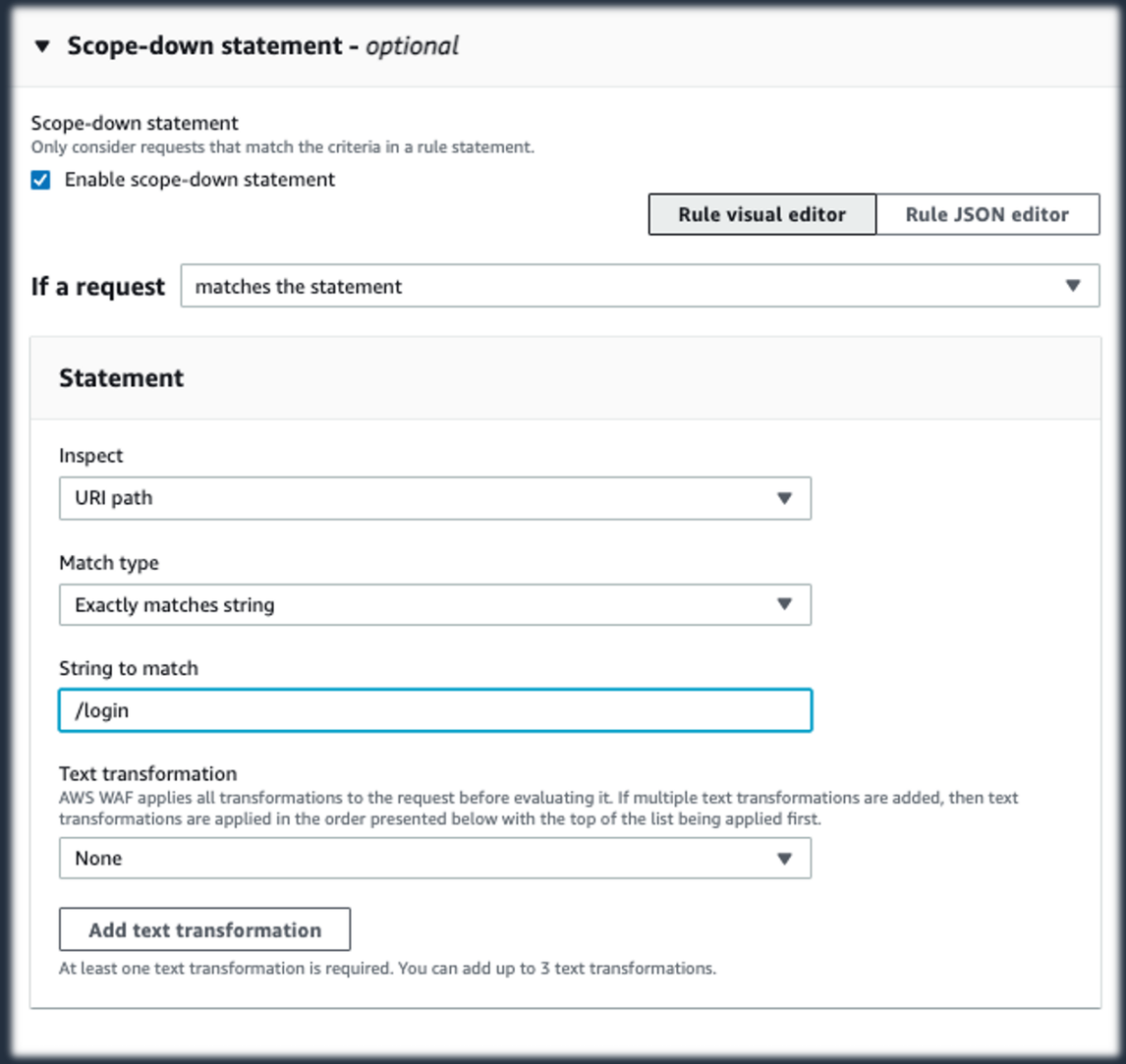
マネージドルールの利用に役立つ新しい機能

- スコープダウンステートメント
- ラベル
- カスタムレスポンス
- カスタムリクエストヘッダー
- バージョニングと通知

スコープダウンステートメント

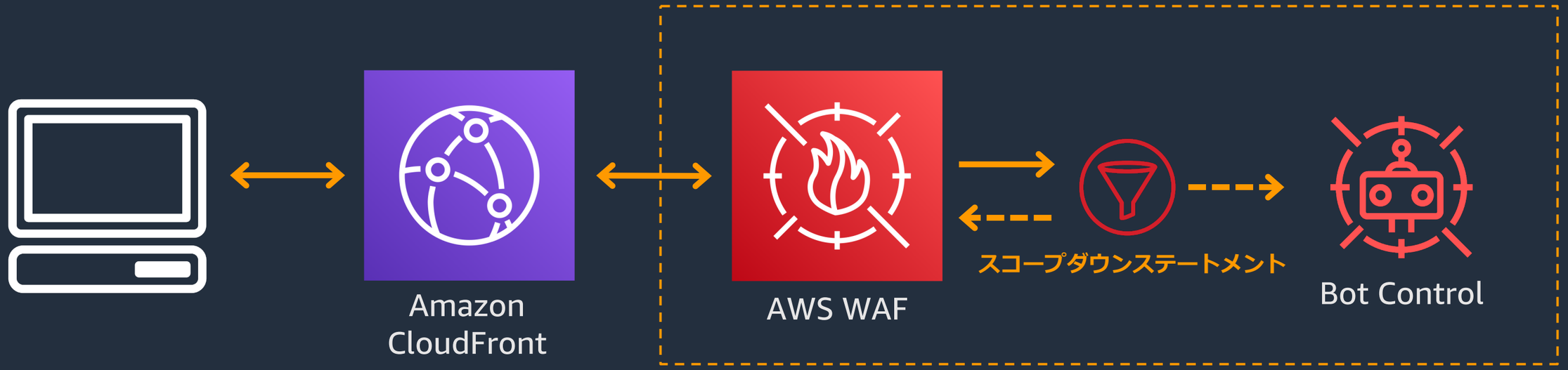
ルールグループの適用範囲を限定する機能を提供

- 特定のリクエストパターンのみルールグループを適用する場合、または除外する場合に活用出来る機能
- 全てのマネージドルールグループ で利用可能



スコープダウンステートメントの使用例

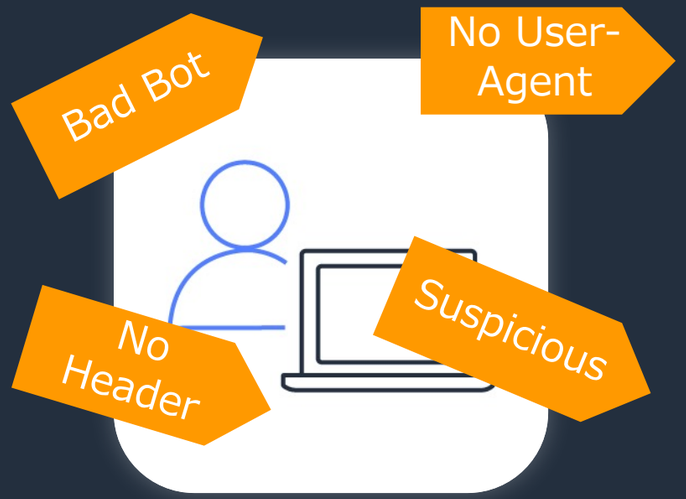
- Bot Control によって評価したいリクエストパターンを特定し、ルールを適用する
- ボットの影響を受けないトラフィック（画像など）は評価しない
- Bot Control のコストは評価対象のリクエストのみ



ラベル

リクエストに対して追加されるメタデータ

- ラベルの値によってルールを実行させることが可能
- アクションに依存せず設定することが可能
- CloudWatch メトリクスやログに追加される

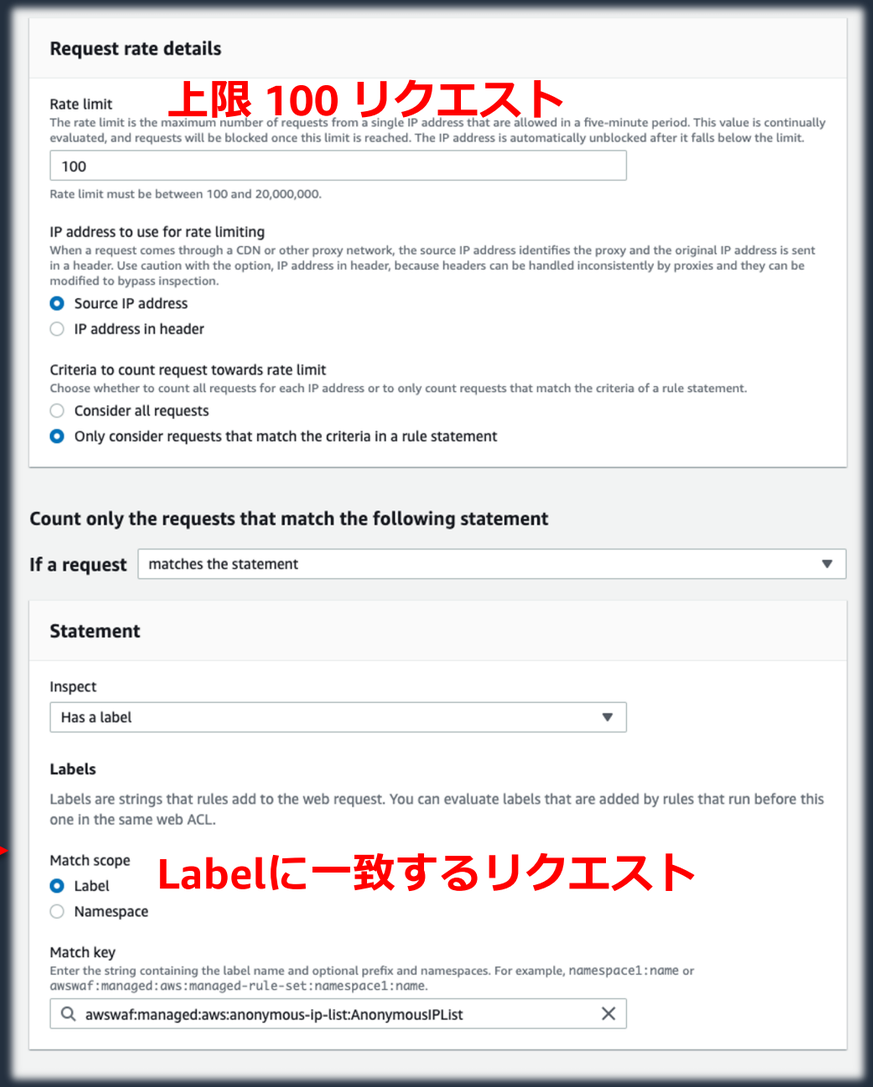


ラベル の使用例

マネージドルールのラベル機能を使ったレートベースルールの設定

- レートベースルールに条件として指定したいマネージドルールを Count に設定
- 該当のラベルが付加されたリクエストを後続のレートベースルールでブロック

Anonymous IP のラベルが付与されたリクエストが 5 分間に100 リクエストを超えたらブロック

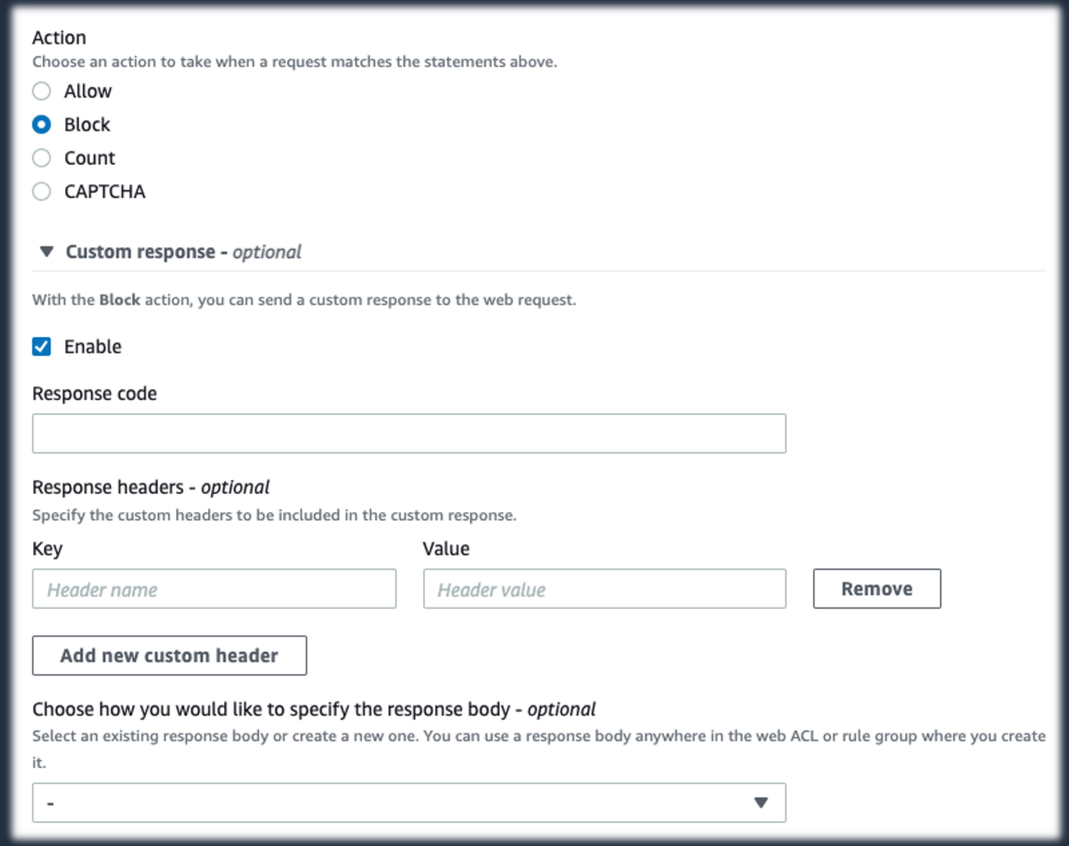


カスタムレスポンス

WAF ルールによって ブロック された際にカスタムレスポンスを返却
以下のカスタマイズが可能:

- Response code
- Headers in the response
- Response body

マネージドルールで利用する場合は
ラベル機能を利用



カスタムレスポンスの使用例

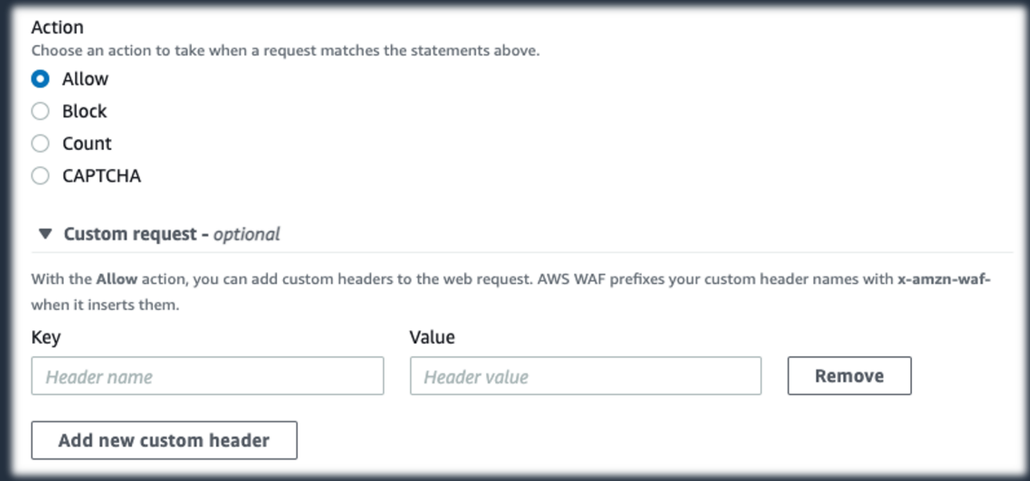
マネージドルールのラベル機能を使って、特定のマネージドルールのアクションをカスタマイズ

IP ReputationList のラベルが付与されたリクエストは、特定のページへリダイレクト

カスタムリクエストヘッダー

WAF ルールによって Allow / Count された際に任意のリクエストヘッダーを挿入

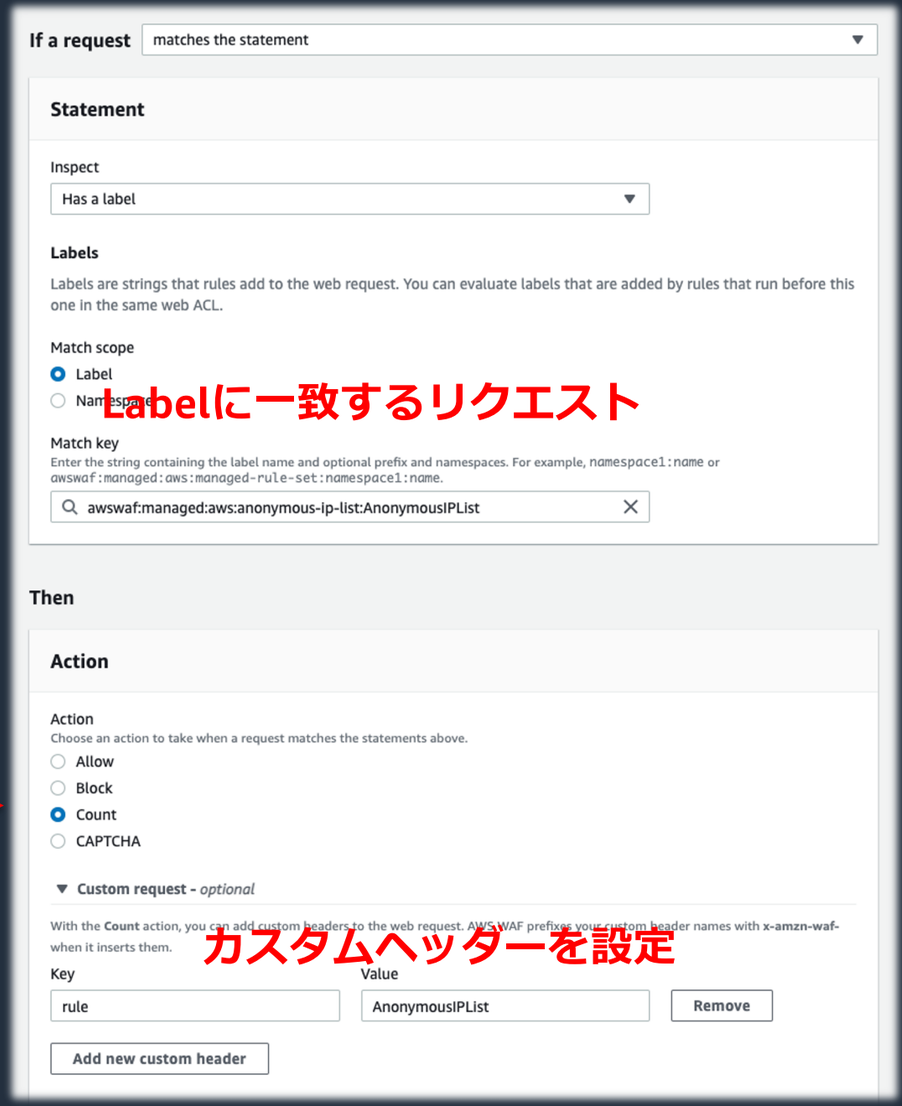
- “x-amzn-waf-” の prefix が付与される
- 既存のリクエストヘッダーの変更は不可



カスタムリクエストヘッダーの使用例

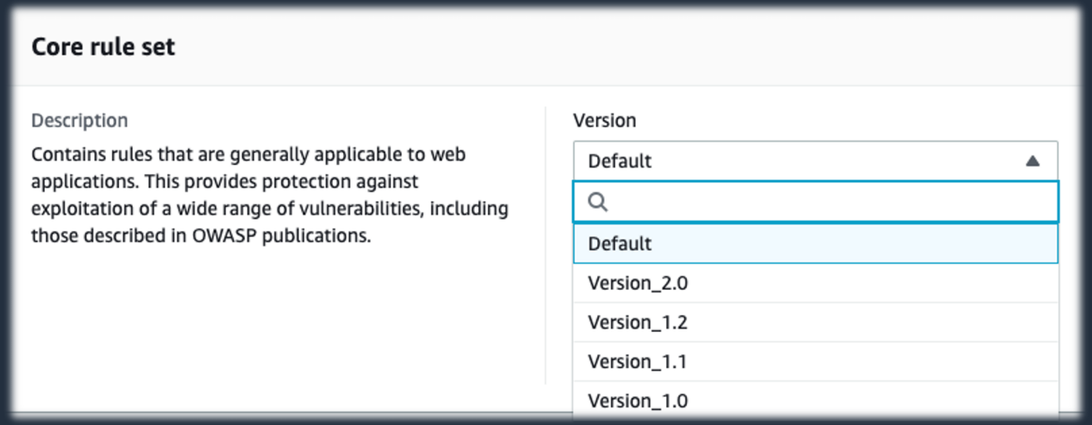
マネージドルールのラベル機能を使って、特定のマネージドルールに合致するリクエストにカスタムヘッダーを挿入

AnonymousIPList のラベルが付与されたリクエストは、カスタムヘッダーを挿入　（アプリケーション側でヘッダーによって動作を変える場合などに利用できる）



マネージドルールの自動更新の制御

- マネージドルールグループで特定のバージョンに設定し、自動更新させないようにすることが可能
- テスト環境等で新しいルールの評価後にルールを更新したり、以前のバージョンにロールバックすることが可能
  - デフォルトでは、マネージドルールグループ内のルールが自動更新される
- Amazon Simple Notification Service (Amazon SNS) を通じて、ルールの更新を事前に受信することが可能

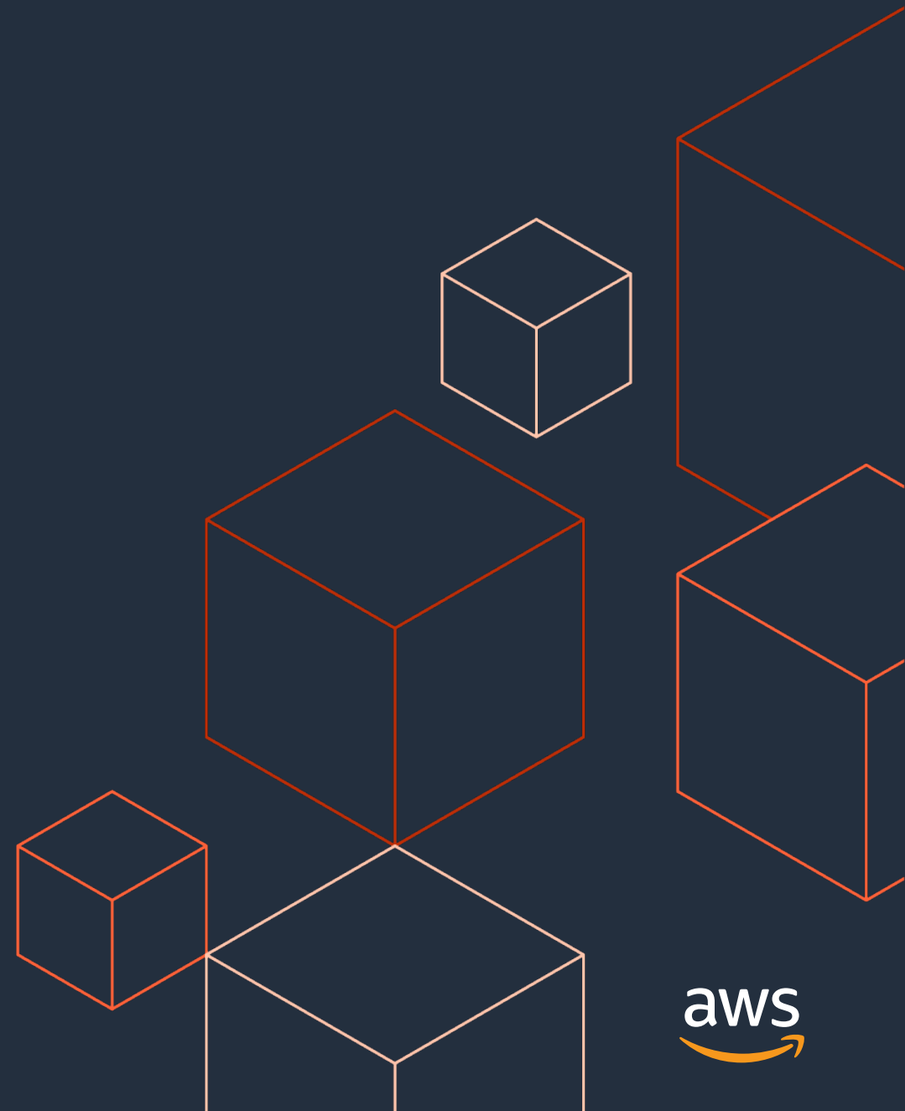


バージョンの期限切れアラートの設定

- バージョンを指定する運用にした場合に、バージョンの有効期限に近づいた時に通知を送信するように設定
- CloudWatch の DaysToExpiry メトリクスでモニタリング可能
- バージョンの有効期限が切れると、マネージドルールグループは自動的に最新のデフォルトバージョンに切り替わる
- 重要な更新の見落とし防止に役立つ

ManagedRuleGroup (2)	Vendor	Version	Metric name
AWSManagedRulesAdminProtectionRuleSet	AWS	Version_1.1	DaysToExpiry
AWSManagedRulesCommonRuleSet	AWS	Version_2.0	DaysToExpiry

導入ステップとチューニング



導入ステップ

最初はルールアクションを Count にしてモニタリングを実施。検知率や誤検知の有無を確認後、ルールアクションを Block へ変更する

Count

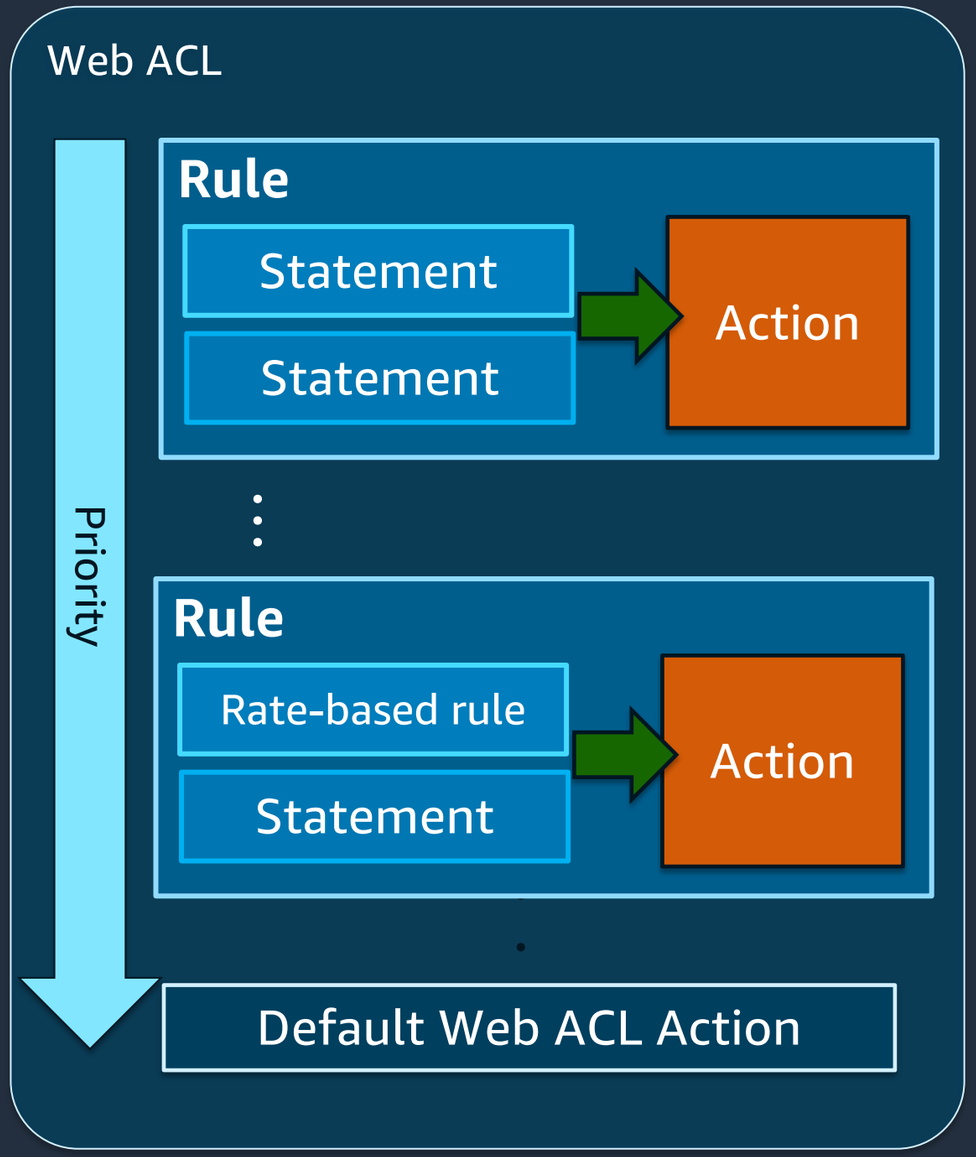
- CloudWatchメトリクスでルールを評価
- 誤検知が発生しないかサンプルレポートやログを確認
- レートベースのルールの閾値を調整

Block

- 誤検知がないことを確認後、Block へ変更
- ルール毎に段階的に Block モードへ変更することも可能
- サンプルリクエストレポートで確認
- ブロックされたリクエストをログから解析

Web ACL のルールの評価の流れ

- Web ACL 内のルールの優先度の順にリクエストの検査が実行される
- ルール内のステートメントでリクエストを検査するための条件を定義、アクションによって条件に一致したリクエストの処理が実行される
- どのルールにも一致しない場合、デフォルト Web ACL Action が実行される

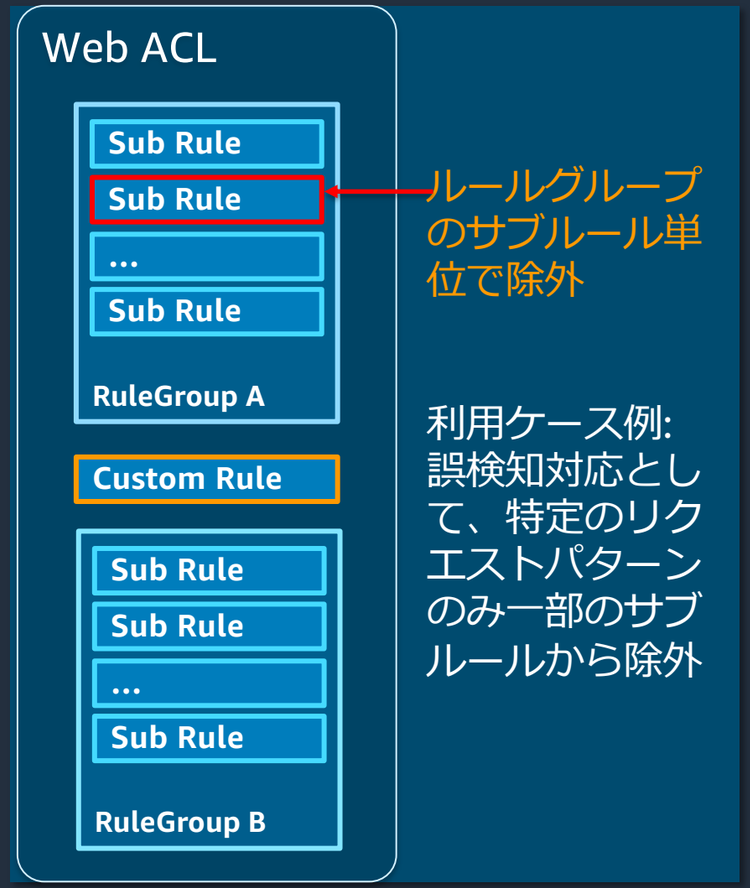


マネージドルールグループから特定の条件のリクエストを除外

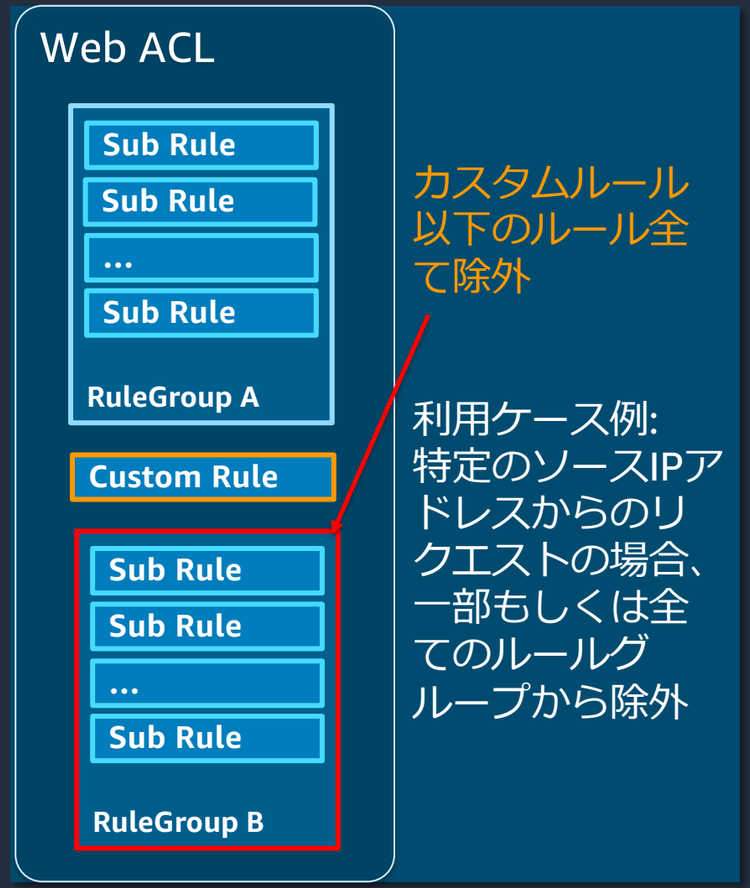
もし正規のリクエストが マネージドルールグループで 検知される場合、またリクエストのパターンによって一部のルールを適用したく無い場合、複数の方法で特定の条件のリクエストを除外することが可能

除外パターン１

除外パターン２



除外パターン３

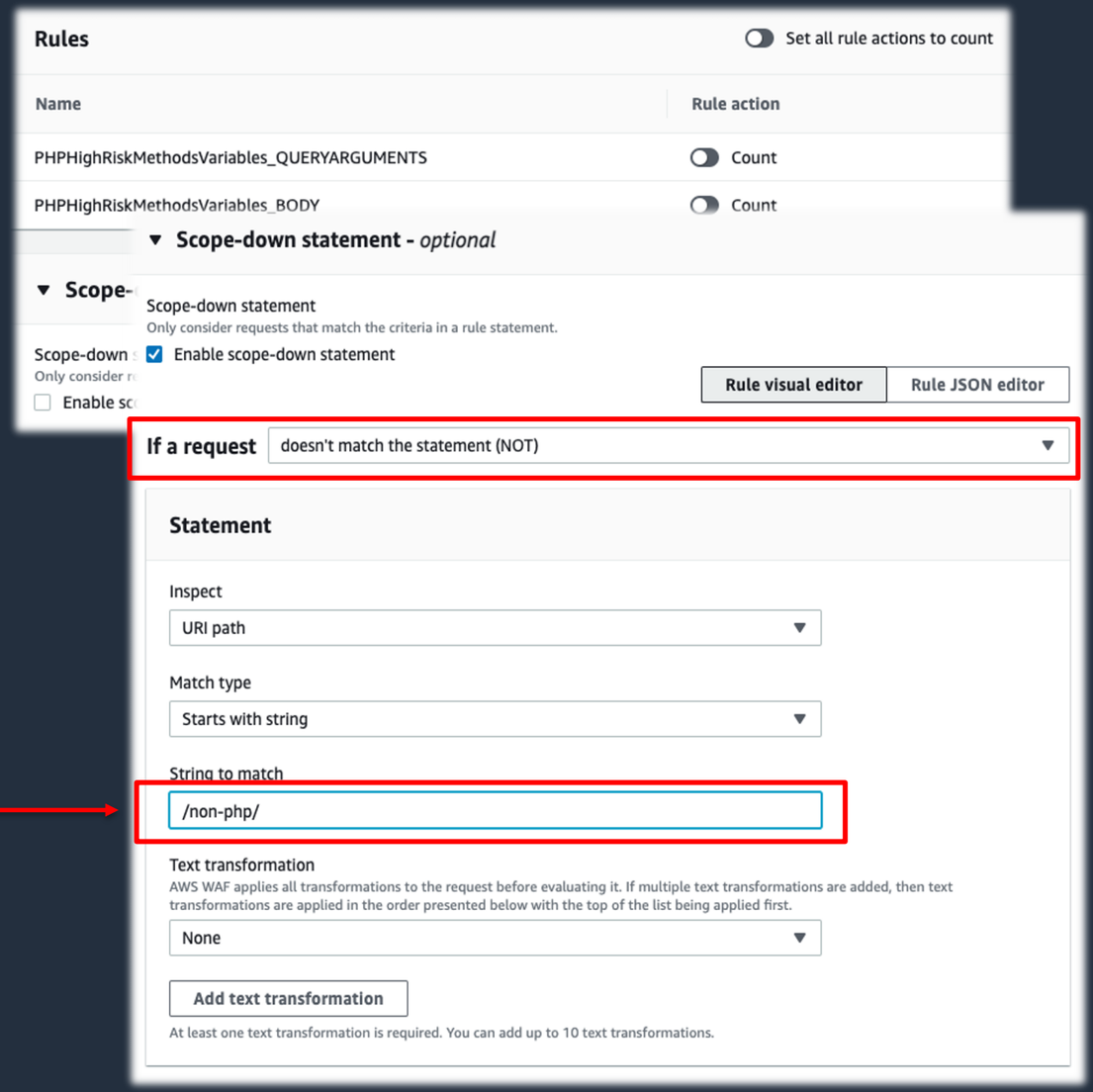


1. ルールグループ単位で特定のリクエスト条件を除外

スコープダウンステートメントを利用

- “doesn’t match the statement (NOT)” を選択し、除外したい条件を指定
- AND を使って、複数の除外パターンを定義することが可能

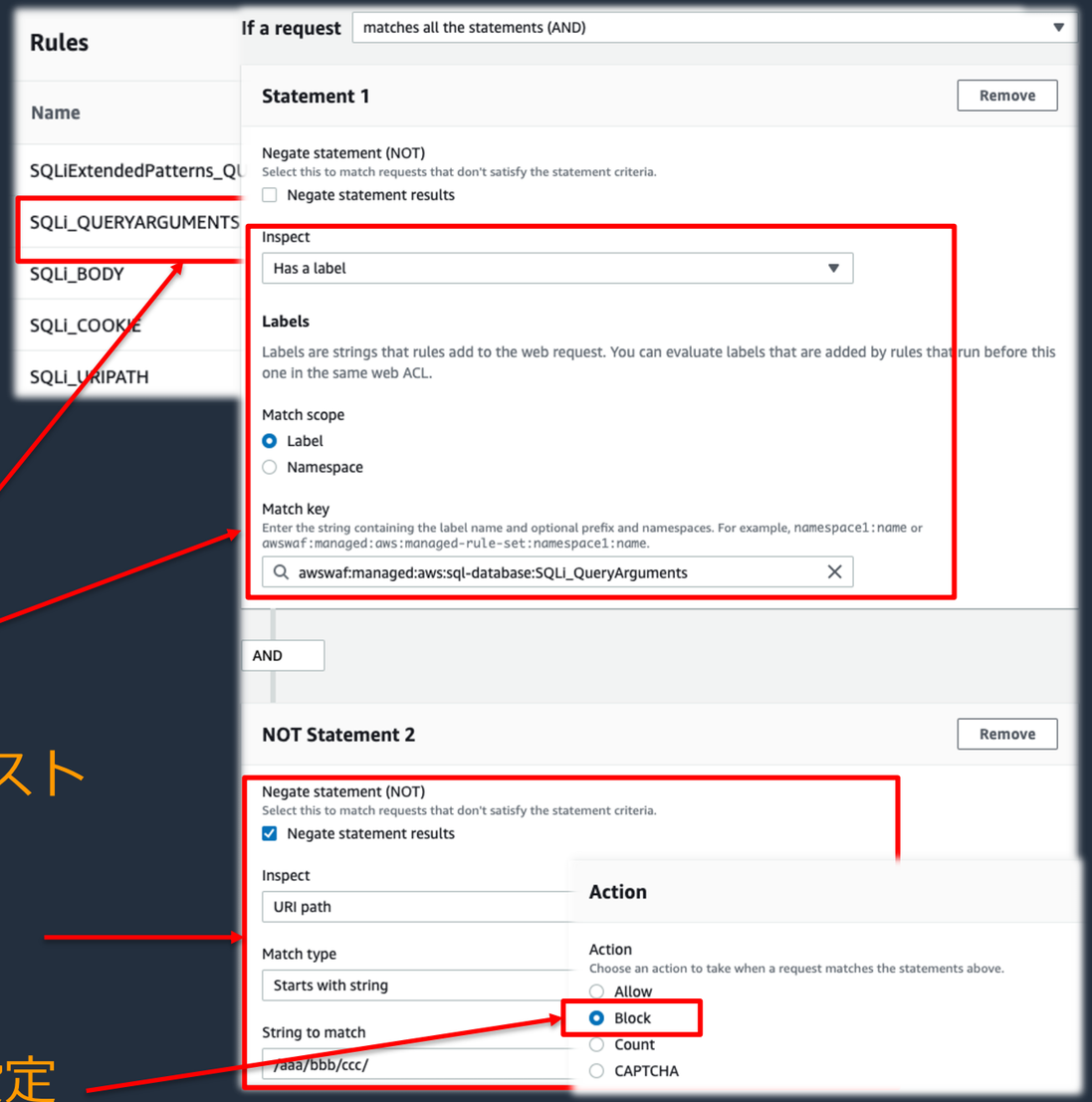
AWS-AWSManagedRulesPHPRuleSet から特定の URI パターンを除外



2. ルールグループの サブルール単位で特定リクエスト条件を除外

ルールのラベルを利用

- 対象のサブルールを Count に設定し、そのラベルが付加されたリクエストを後続のカスタムルールで除外条件を指定してブロック



サブルールを Count に設定

AWS-AWSManagedRulesSQLiRuleSet の
SQLi_QueryArgumentsのラベルが付与されたリクエスト

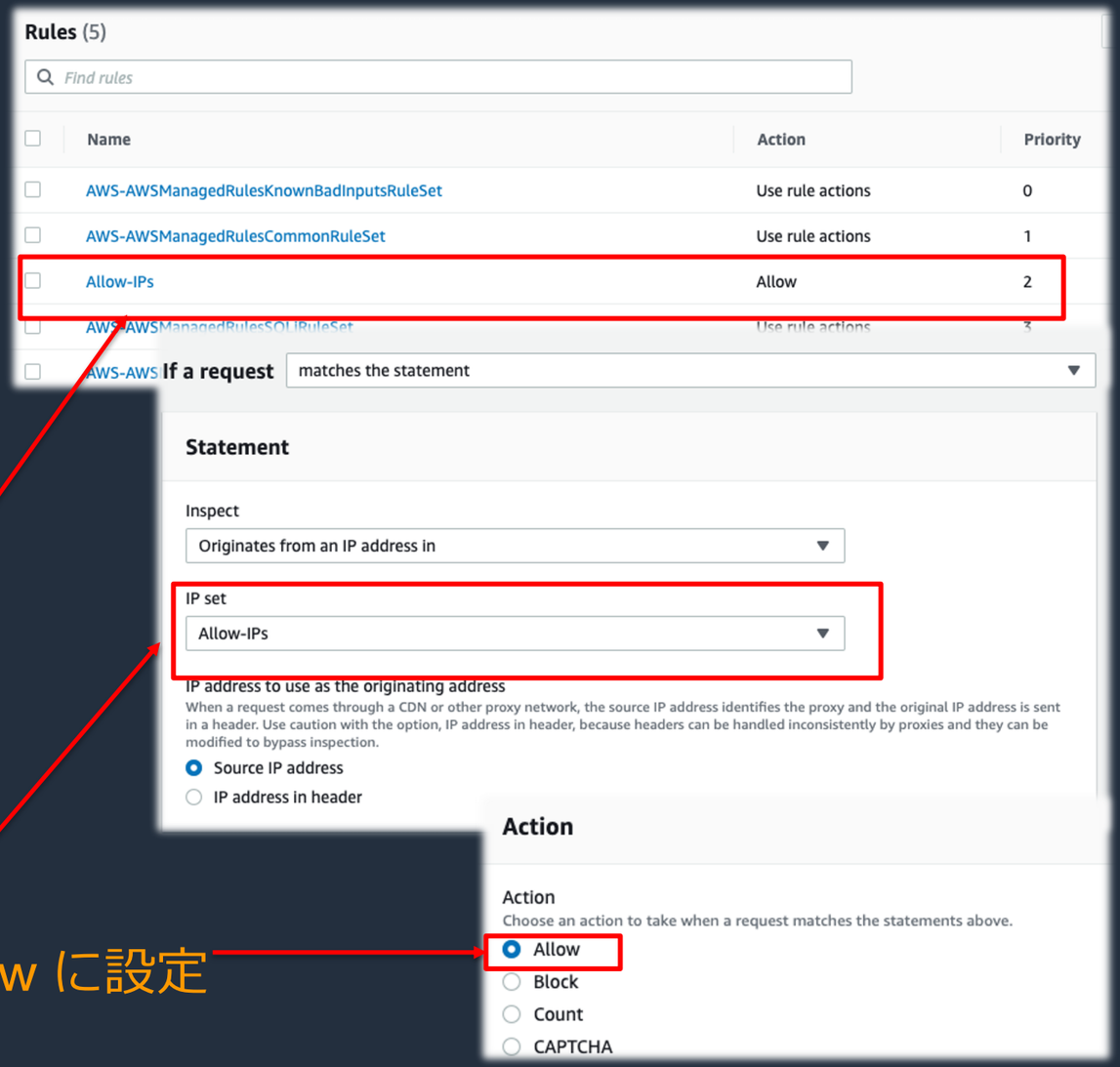
特定のパスパターンを除外

Action を Block に設定

3. カスタムルール以下のルールグループ全体から特定リクエストを除外

優先度の高い除外用カスタムルールを利用

- 除外条件を指定したカスタムルールを作成し、Actionを Allowにする。それを除外したいルールグループよりも高い優先度に設定する



カスタムルールを作成

許可するIPアドレスのリストを指定

Action を Allow に設定

導入後の運用

Block への切り替え後、モニタリングを継続して実施

- CloudWatchメトリクスによるアラーム通知
  - 異常を速やかに把握
- Athena や CloudWatch Log insights を利用したログ解析
  - ブロックされたトラフィックを定期的に確認
  - 誤検知が疑われる場合、ログからリクエストのパターンを特定
- マネージドルールの更新通知を設定し、更新状況を把握
  - 自動更新にしない場合はバージョンの期限切れアラートを設定

まとめ

- AWS Managed Rules for AWS WAF は様々な事前構成済みのルールセットの中から直ぐに導入可能なマネージドルール
- ラベルの機能により、マネージドルールにカスタムレスポンスやカスタムヘッダー、レートベースルールを組み合わせて利用することが可能
- マネージドルールのバージョンの指定により、任意のタイミングでルールの更新が可能
- バージョンの期限切れアラートを設定することにより、重要な更新の見落としを防止
- スコープダウンステートメントやラベルを活用することによって、特定のリクエスト条件の除外設定が柔軟に対応可能

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