



このコンテンツは公開から3年以上経過しており内容が古い可能性があります
最新情報については[サービス別資料](#)もしくはサービスのドキュメントをご確認ください

[AWS Black Belt Online Seminar] AWS WAF アップデート

サービスカットシリーズ

Solutions Architect

岡 豊

2020/03/24

AWS 公式 Webinar

<https://amzn.to/JPWebinar>



過去資料

<https://amzn.to/JPArchive>



自己紹介

岡 豊 (おか ゆたか)

所属 :

アマゾン ウェブ サービス ジャパン
Edge サービス担当ソリューションアーキテクト

好きなAWSのサービス :

Amazon CloudFront
AWS WAF
AWS Certificate Manager



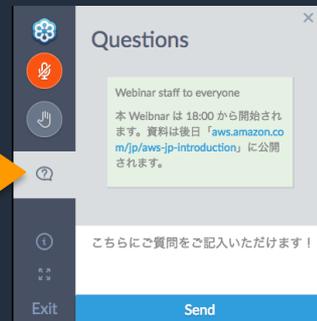
AWS Black Belt Online Seminar とは

「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かれて、アマゾンウェブ サービス ジャパン株式会社が主催するオンラインセミナーシリーズです。

質問を投げることができます！

- 書き込んだ質問は、主催者にしか見えません
- 今後のロードマップに関するご質問は
お答えできませんのでご了承下さい

- ① 吹き出しをクリック
- ② 質問を入力
- ③ Sendをクリック



Twitter ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- 本資料では2020年03月24日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.

本セッションの目的

2019年にAWS WAFが大幅にアップデートされました
AWS WAFを以前からご利用の方には、そのアップデートで何が変わったのか、また、AWS WAFをまだお使いでない方には、AWS WAFの全体像を把握いただき、何が出来るのかをご理解いただく

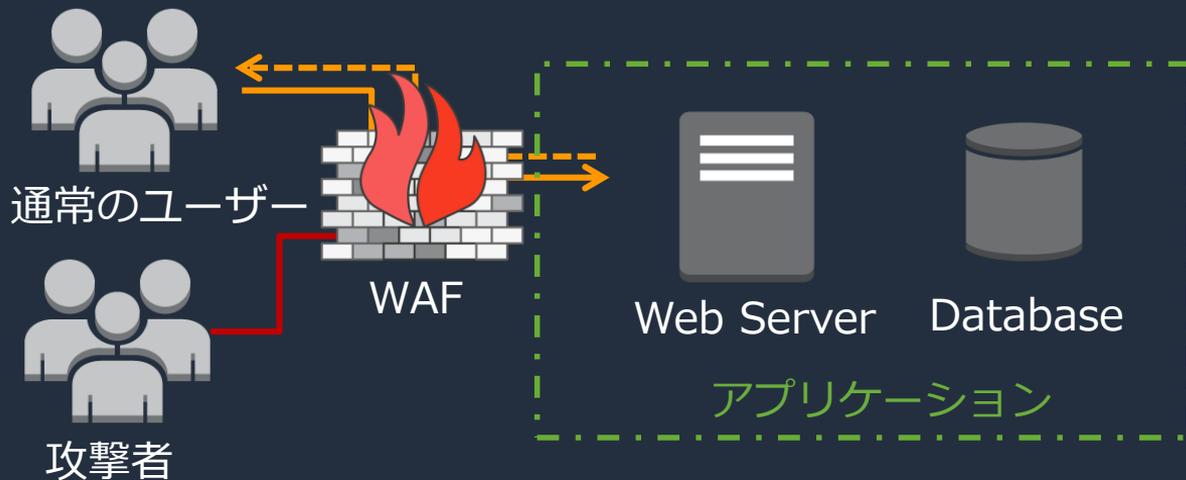
本日のアジェンダ

1. Web Application Firewall(WAF)とは
2. AWS WAFの機能
3. アップデートによる主な変更点
4. AWS WAFの詳細
5. AWS Managed Rules for AWS WAF
6. Web ACL作成の流れ
7. ログとモニタリング
8. AWS WAF利用のための考慮事項
9. 料金体系
10. まとめ

Web Application Firewall (WAF)とは

ウェブアプリケーションの通信内容を検査し、不正なアクセスを遮断する
ルールセットを持つセキュリティ対策

ウェブアプリケーションの脆弱性を悪用した攻撃などからウェブアプリケーションを保護することが目的



様々な攻撃手法

DDoS

Reflection and amplification

Slowloris

Layer 3 & 4 floods

SSL abuse

HTTP floods

Bots and probes

SQL injection

XSS

Application exploits

RFI/LFI

CSRF

Authorization exploits

Spear phishing

Certificate hijacking

Targeted attacks

Web Application Firewall
AWS WAF

様々な攻撃手法

DDoS

Reflection and amplification

Slowloris

Layer 3 & 4 floods

SSL abuse

HTTP floods

Bots and probes

SQL injection

XSS

Application exploits

RFI/LFI

CSRF

Authorization exploits

Spear phishing

Certificate hijacking

Targeted attacks

- Amazon CloudFront
- Elastic Load Balancing
- AWS Shield Standard
- AWS Shield Advanced

**Web Application Firewall
AWS WAF**

- Amazon Inspector
- Amazon Macie
- Amazon Certificate Manager (ACM)
- AWS Marketplace: IDS/IPS, anti-malware

ウェブアプリケーションの欠陥に対する攻撃を軽減

- WAFは根本的な欠陥を修正するものではなく、それらを悪用する能力を制限
- 様々なHTTPのリクエストパターンを検証
- 攻撃の変化に対応するためにルール構成を迅速に変更する機能が必要



本日のアジェンダ

1. Web Application Firewall(WAF)とは
2. AWS WAFの機能
3. アップデートによる主な変更点
4. AWS WAFの詳細
5. AWS Managed Rules for AWS WAF
6. Web ACL作成の流れ
7. ログとモニタリング
8. AWS WAF利用のための考慮事項
9. 料金体系
10. まとめ

AWS WAFが提供する機能

悪意のあるリクエストのブロック



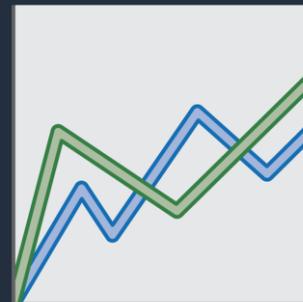
- SQLインジェクション
- クロスサイトスクリプト
- AWS、またはパートナー提供のマネージドルール

カスタムルールに基づいたWeb トラフィックのフィルタ



- Rate-based rules
- IP & Geo-IP filters
- 正規表現パターン、文字列
- サイズ制限
- アクション：許可/拒否

モニタリングとチューニング



- Amazon CloudWatch
- メトリクス/アラーム
- サンプルログ
- Full logs
- カウントアクションモード（検知モード）

AWS WAFの特徴

Launch



容易なデプロイ



迅速なインシデントレスポンス



フルAPIサポート



セキュリティオートメーション

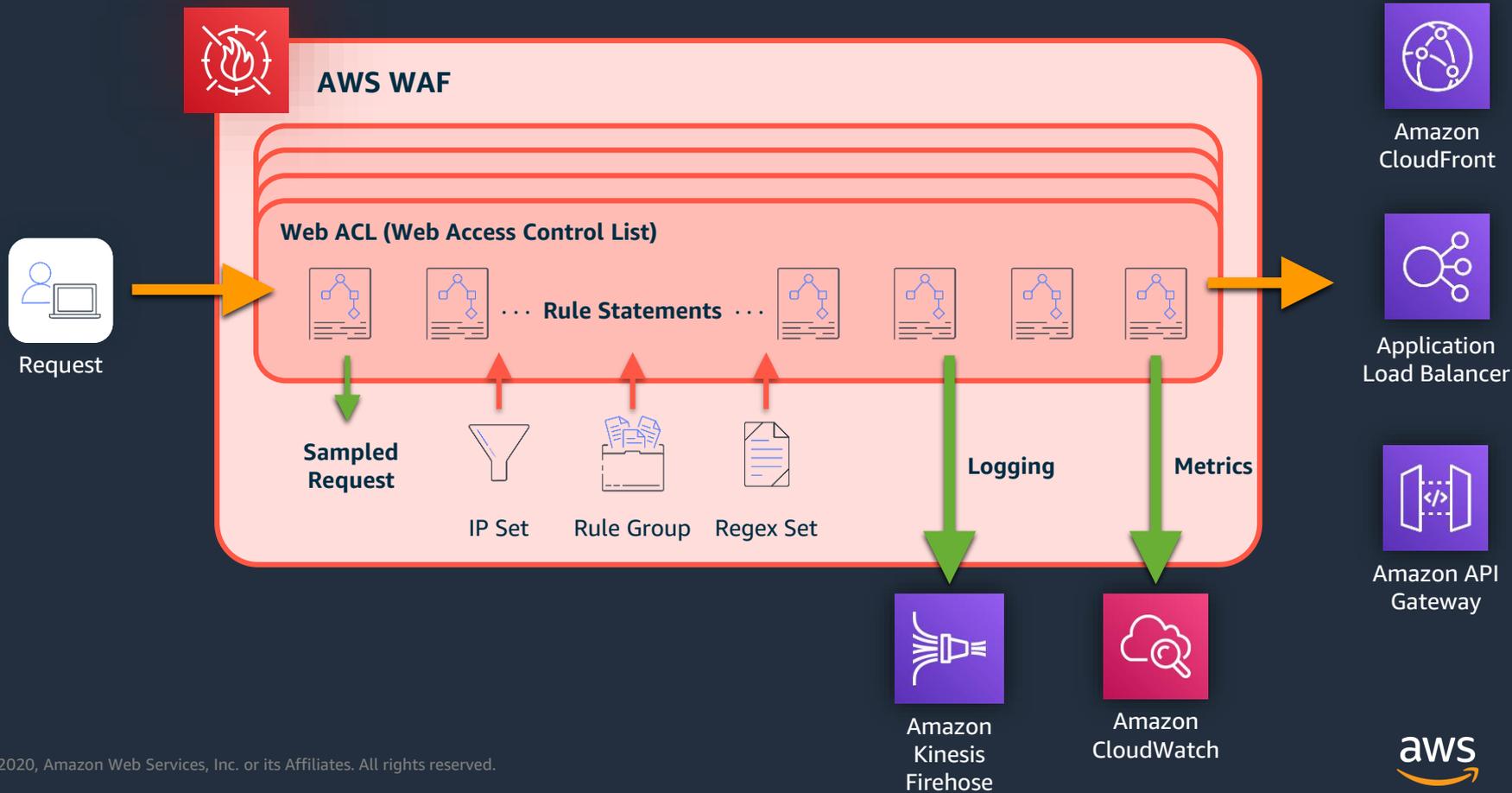


廉価



マネージドルール

AWS WAFの全体像



AWS WAF 機能拡張の歴史



- 2015年10月 AWS WAF リリース
- 2015年12月 CloudFormationに対応

2015



2016



- 2016年1月 HTTP Bodyの検査に対応
- 2016年1月 リクエストサイズの長さ制限の条件に対応
- 2016年3月 Cross-Site Scripting (XSS)ルール条件に対応
- 2016年4月 AWS CloudTrailに対応
- 2016年7月 PCI DSS 3.2 Merchant Level 1にAWS WAFが含まれる
- 2016年10月 IPv6に対応
- 2016年12月 Application Load Balancer (ALB)に対応

- 2017年5月 AWS WAF on ALBがAWS CloudTrailに対応
- 2017年5月 IP setの上限を1000から10000へ増加
- 2017年5月 AWS WAF on ALBがAWS CloudFormationに対応
- 2017年6月 HIPAA コンプライアンスプログラムの対象となる
- 2017年6月 レートベースのルールに対応
- 2017年10月 正規表現のルールに対応
- 2017年10月 地域別の制御に対応
- 2017年11月 パートナーマネージドルールに対応

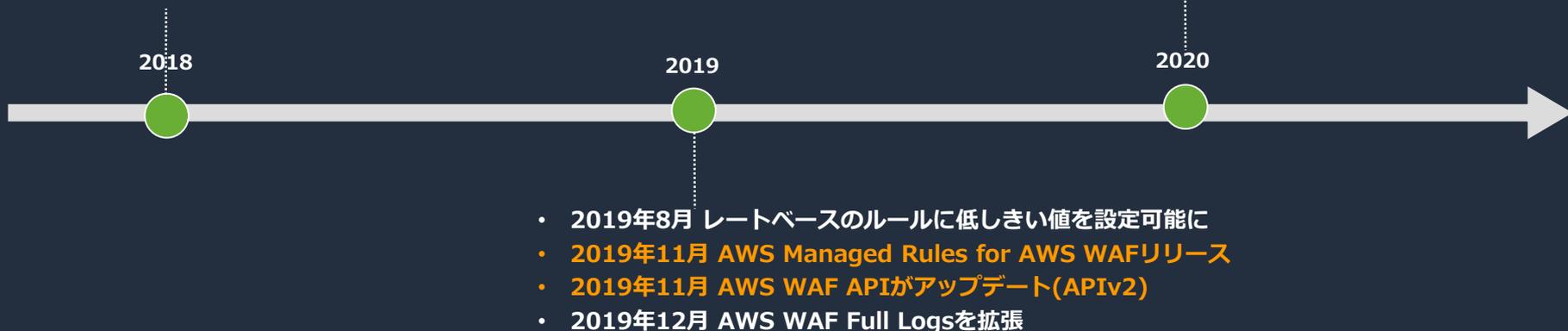
2017



AWS WAF 機能拡張の歴史(続き)

- 2018年2月 AWS Config が AWS WAF ルールグループをサポート
- 2018年6月 クエリ文字列とのパターンマッチングを強化
- 2018年6月 Non-octet CIDR boundariesをサポート
- 2018年8月 AWS WAF Full logsが新たに利用可能に
- 2018年11月 AWS API Gatewayに対応

- 2020年3月 AWS マネージドルールにAnonymous IP リスト追加



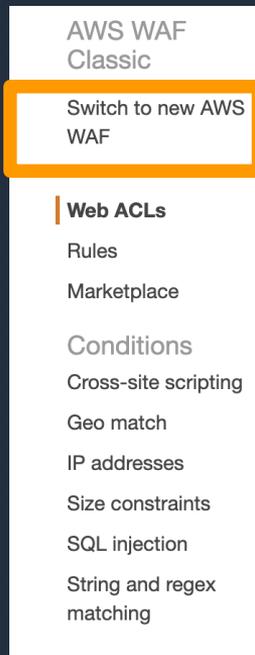
本日のアジェンダ

1. Web Application Firewall(WAF)とは
2. AWS WAFの機能
3. アップデートによる主な変更点
4. AWS WAFの詳細
5. AWS Managed Rules for AWS WAF
6. Web ACL作成の流れ
7. ログとモニタリング
8. AWS WAF利用のための考慮事項
9. 料金体系
10. まとめ

従来のAWS WAFはAWS WAF Classicへ名称変更

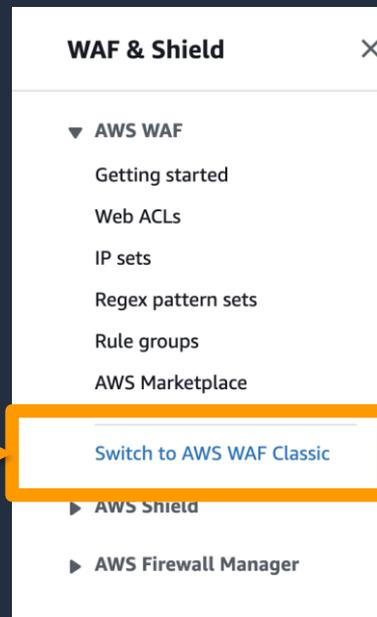
2019年11月末のアップデートにより、従来のAWS WAFはAWS WAF Classicへ名称を変更しました。AWSマネージメントコンソールの左のメニューから切り替え可能です。

AWS WAF Classic



切り替え

AWS WAF



AWS WAF 直近の主なアップデート

AWS WAFの新しいAPIの仕組み

- namespace: “wafv2”が付与される
- “waf” や “waf-regional”という区別なく、APIでの操作が可能

ルールの記述方法も拡張

- これまで異なっていたルールタイプ毎の記述方法が統一化
- JSON フォーマットのドキュメントベースのルール記述
- 一つのJSONファイル内にすべてのルールを記載し、UpdateWebACL を呼ぶだけで反映

WAF Capacity Unit (WCU)を新たに利用

- Web ACLあたりの上限10 ルールの制限は撤廃
- その他諸々の制限の緩和 (例:フィルタ数の上限など)

AWS WAF 直近の主なアップデート

コンソール画面の変更

- コンソールをシンプル化し、より簡単に利用できるように

ルール記述の柔軟化

- OR、複数のトランスフォーム、CIDR表記

ビルトインのマネージドルール: AWS Managed Rules for AWS WAF

- AWS Threat Research Team が作成及びメンテナンスを実施
- OWASP Top 10 や IP reputation listなどが含まれる

AWS WAF Full logsの拡張

- 誤検知発生時のトラブルシューティングに有用となる新しいログフィールドの追加

AWS WAFとAWS WAF Classicの主な違い

| 機能 | WAF Classic | 新 AWS WAF |
|-----------------------|---|--|
| AWSマネージドルールグループ | No | Yes |
| AWS パートナーマネージドルールグループ | Yes | Yes |
| Web ACL毎のルール上限 | 10 | WAF Capacity Unit (WCU)の上限 1500 WCU |
| Web ACL毎のルールグループ数の上限 | 2 | WAF Capacity Unit (WCU)の上限 1500 WCU |
| ルールの論理条件 | AND and NOT | AND, OR, and NOT |
| API の利用 | CloudFrontとALB,API GWで異なる名前スペースを指定 (namespace "waf") (namespace "waf-regional") | 名前スペースは"WAFv2"に統一 |
| IP setのCIDRサポート | /8, /16-/32 | /1-/32 |

本日のアジェンダ

1. Web Application Firewall(WAF)とは
2. AWS WAFの機能
3. アップデートによる主な変更点
4. AWS WAFの詳細
5. AWS Managed Rules for AWS WAF
6. Web ACL作成の流れ
7. ログとモニタリング
8. AWS WAF利用のための考慮事項
9. 料金体系
10. まとめ

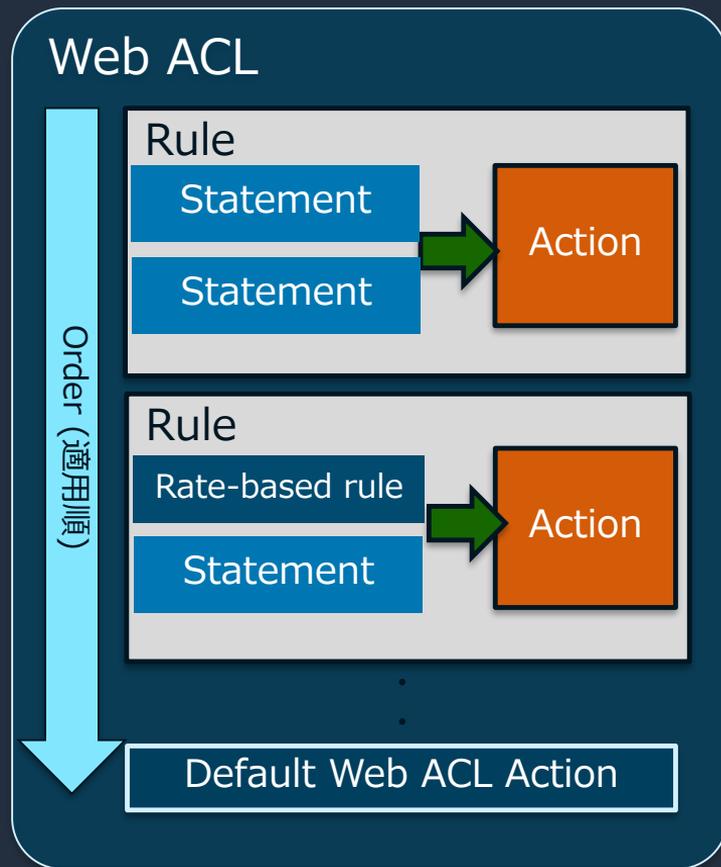
AWS WAFのコンポーネント

- Web ACL (Web Access Control List)
- Rules
- Statement
- Rate-based rule
- Actions
- Managed Rule
- Rule Group
- AWSリソース (CloudFront, ALB, API Gateway)
- レポート
- AWS WAF Full logs

Web ACL

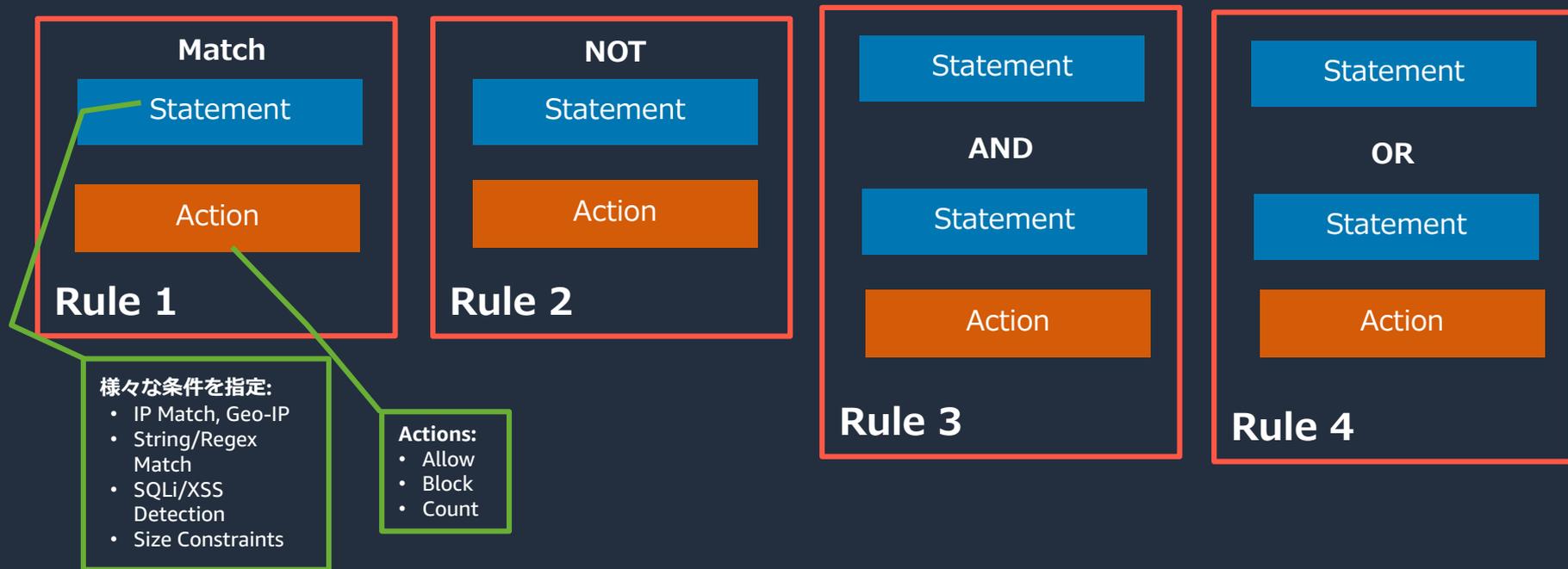
Web ACL を作成し、ルールを追加して攻撃に対する戦略を定義します。ルール内のステートメントにより、リクエストを検査するための条件が定義され、アクションによって条件に一致したリクエストの処理方法が指定されます。

- Web Capacity Unit(WCU)がWeb ACLで設定できるルールの上限となります。(WCUについては後述)
- Web ACL内のルールの優先度を指定可能です。
- Web ACL全体のデフォルトActionを指定(どのルールにも一致しない場合のアクション) します。



Ruleの中身

リクエストに対する検査方法と、リクエストが検査条件に一致した場合の処理を定義



ステートメントで定義可能な条件の種類

| 一致条件 | 内容 |
|---------------|--|
| リクエスト発生国の一致 | リクエストの送信元の国を検査 |
| 送信元IPアドレスの一致 | IPアドレスがマッチしているかどうかのリストを設定（CIDRで設定） |
| サイズの制約 | サイズの制約にマッチしているかどうか |
| SQL injection | SQLインジェクション攻撃かどうか |
| XSS injection | クロスサイトスクリプティング攻撃かどうか |
| 文字列の一致 | 文字列がマッチしているかどうか Header / HTTP Method / Query String / URI / Body 以下のMatchに対応 Contains / Exact / Begins with / Ends with / Contains word |
| 正規表現パターンセット | 正規表現パターンを指定されたリクエストコンポーネントと比較 |

リクエストの検査をする対象コンポーネントの種類

| コンポーネント | 内容 |
|--------------|---|
| リクエストヘッダー | 特定のリクエストヘッダー。このオプションでは、[Header type (ヘッダータイプ)] フィールドでヘッダーの名前 (User-Agent、Referer など) も選択 |
| HTTPメソッド | HTTP メソッドを検査する |
| クエリ文字列 | URL 内で "?" 文字の後に続く部分 (ある場合) XSS一致条件の場合は、[Query string (クエリ文字列)] ではなく [All query parameters (すべてのクエリパラメータ)] を選択することを推奨 |
| 単一クエリパラメータ | 指定されたパラメータの値を検査する |
| すべてのクエリパラメータ | クエリ文字列に含まれるすべてのパラメータの値を検査する |
| URI | URL 内でリソースを識別する部分 (例: images/daily-ad.jpg) |
| Body | リクエストヘッダーの直後に続くリクエストボディの部分。これには、フォームからのデータなど、ウェブリクエストに必要な追加データが含まれる |

利用可能なテキスト変換の種類

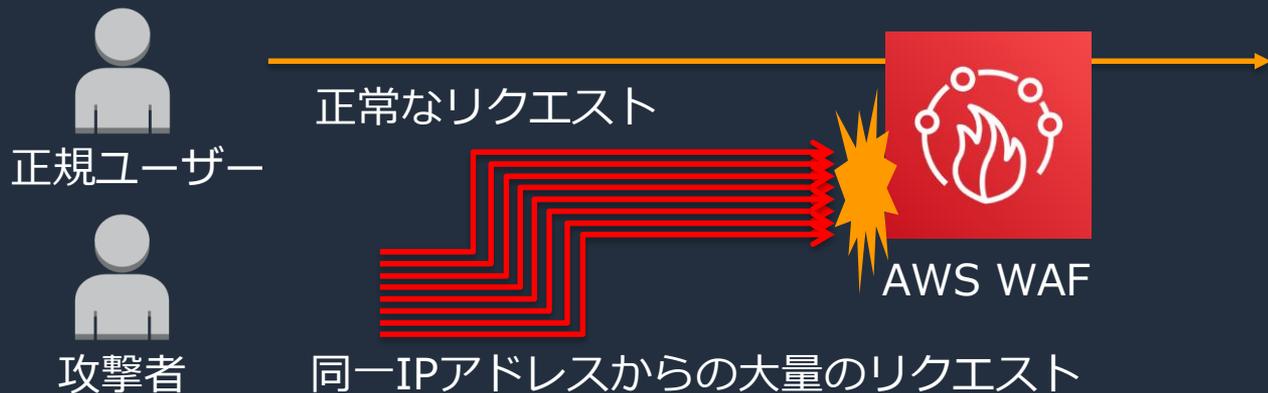
| テキスト変換 | 内容 |
|-----------------------|--|
| None | 変換せず、そのままリクエストを検査 |
| Convert to lowercase | 大文字の A-Z を小文字の a-z に変換 |
| HTML decode | HTML エンコードされた文字をエンコードされていない文字に置き換え |
| 空白の正規化 | 複数のスペースを 1 つのスペースに置換、以下の文字を空白文字（10 進数の 32）に置き換え ¥f、フォームフィード、10 進数の 12 ¥t、タブ、10 進数の 9 ¥n、改行、10 進数の 10 ¥r、キャリッジリターン、10 進数の 13 ¥v、垂直タブ、10 進数の 11 改行なしスペース、10 進数 160 |
| Simplify command line | 攻撃者がオペレーティングシステムのコマンドを挿入した際、異常なフォーマットを使用して、コマンドの一部またはすべてを偽装するのを防ぐ |
| URL decode | URL エンコードされたリクエストをデコード |

論理ルールステートメントの種類

| 論理ステートメント | 内容 |
|-----------|--|
| ANDロジック | ステートメントを AND ロジックと組み合わせる (API ステートメント - AndStatement) |
| NOTロジック | ステートメントの結果を否定 (API ステートメント - NotStatement) |
| ORロジック | ステートメントを OR ロジックと組み合わせる (API ステートメント - OrStatement) |

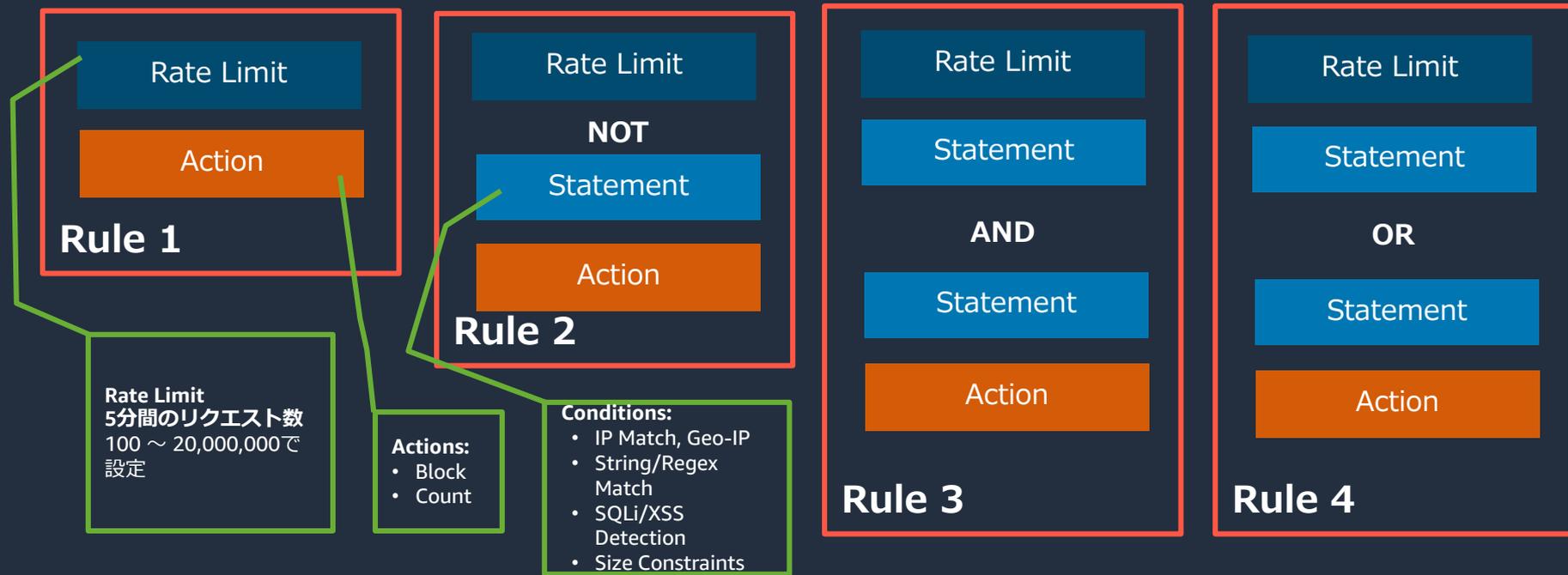
レートベースのルール

- 5 分間あたりの同一IPアドレスからのリクエスト数が設定された閾値を超過したら、Block/Countする。
- 5 分間あたりの閾値の設定範囲は、100 ~ 20,000,000 で設定
- ルール作成時にRate-based Ruleを選択
- 全てのリクエストを対象にするか、ステートメント内の条件に一致したリクエストだけを対象にするかを選択可能



Ruleの中身 (Rate-based ruleのパターン)

リクエストレートの制限を適用する条件を指定 (All, NOT, OR, AND)



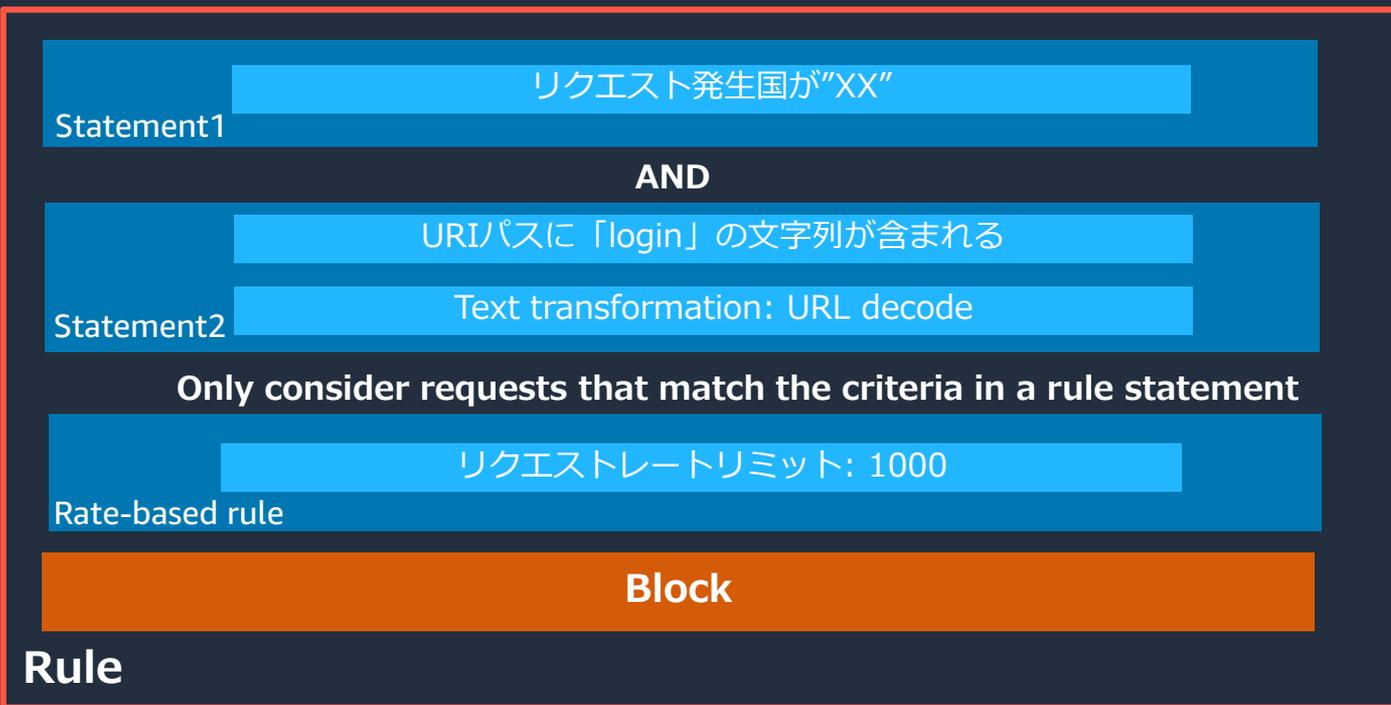
ルール設定例 1

クエリパラメータにadminの文字列を含むリクエストに対し、リクエストBodyがクロスサイトスクリプティング攻撃かどうかをチェックし、ブロック



ルール設定例 2

特定の国からのリクエストのURIパスに「login」を含む場合において、リクエストのレートが1,000 を超えたらブロックする



WAF Capacity Unit (WCU)とは

WAFのルールに対する処理コストの考え方。それぞれのルールの中身に応じて処理コストを計上、その合計がWeb ACLの Capacity を超えない範囲でルールを登録可能

注意点：

- Web ACLのWCUの上限は 1500 となる
- 文字列のマッチ条件の処理内容によって、WCUの使用量が異なる
- 正規表現のルール数の上限はこれまで通り10 個まで (Regex pattern sets)
- Web ACLの画面に合計利用WCUの値が表示される

Web ACL rule capacity units used

The total capacity units used by the web ACL can't exceed 1500.

900/1500 WCUs

Web ACLで消費されるWCUリソース

より複雑なルールはより多くのWCUを利用

| Match Statement | Description | WCUs |
|----------------------|--|------------------------------|
| IP Set Match | リクエストの送信元を一連の IP アドレスおよびアドレス範囲と比較 | 1 |
| Regex Pattern Set | 正規表現パターンを指定されたリクエストコンポーネントと比較 | 25 per pattern set |
| Size Constraint | 指定されたリクエストコンポーネントに対してサイズ制約をチェック | 1 |
| SQLi Attack | 指定されたリクエストコンポーネント内の悪意のある SQL コードを検査 | 20 |
| String Match | 指定されたリクエストコンポーネントと文字列を比較 | Depends on the type of match |
| XSS Scripting Attack | 指定されたリクエストコンポーネントでのクロスサイトスクリプティング攻撃を検査 | 40 |

ルールグループも作成が可能（含まれるルールの合算WCUが消費される）

Web ACLにおけるWCUの計算例

- 文字列マッチルール
 - Bodyに対する 10 個の文字列フィルタ → $10 \times 10 \text{ WCU} = 100 \text{ WCU}$
 - Bodyに対する空白の正規化 → 10 WCU
- SQLi 検出ルール
 - URL, cookie header, と bodyに適用 → $3 \times 20 \text{ WCU} = 60 \text{ WCU}$
- 正規表現ルール
 - 10 個の正規表現を含むパターンセット → $1 \times 25 \text{ WCU} = 25 \text{ WCU}$
- 3 つのIPセットルール
 - 3 つの IPセット (10,000 IPまで指定可能) → $3 \times 1 = 3 \text{ WCU}$
- AWS Managed Rules
 - Core ruleset → 700 WCU

合計 WCU :898 WCU

WCU 残:1,500 - 898 = 602 WCU



ルールグループ

- 個別のルール以外にも複数のルールを組み合わせたルールグループも自分で作ることが可能
- Web ACL内でグループ単位で優先度を設定したり、グループ内の個別ルールのアクションをオーバーライドすることが可能
- ルールグループ作成時にWCUの値を設定
 - 将来的にルールグループをメンテナンスしていくときにWCUの上限を超えないように事前に予約するための機能
 - 含まれるルール自体はWCU22 だがルールグループの設定は 200 など設定できる（包含しているものより大きい値が設定可能）
 - 1 回設定したら変えられない



本日のアジェンダ

1. Web Application Firewall(WAF)とは
2. AWS WAFの機能
3. アップデートによる主な変更点
4. AWS WAFの詳細
5. AWS Managed Rules for AWS WAF
6. Web ACL作成の流れ
7. ログとモニタリング
8. AWS WAF利用のための考慮事項
9. 料金体系
10. まとめ

AWS Managed Rules for AWS WAF (AMR)とは

AWS WAFに組み込み可能なビルトインルールセット

- AWS Threat Research Team (TRT)が作成及びメンテナンスを実施
- OWASP Top 10 をメインに対応を実施

追加費用は不要

- WAF Capacity Unit (WCU)は消費するがそれ以外の追加費用は不要

| Category | Ruleset | Description |
|----------|------------------------|---|
| CRS | Core Ruleset | Based on OWASP Top 10 |
| EXR | Admin Protection | Blocks common administrative access |
| EXR | SQL DB | Predefined SQL injection detection |
| EXR | Linux | Linux based path traversal attempts |
| EXR | Known Bad Inputs | Well known bad request indicators |
| EXR | PHP | PHP specific exploits |
| EXR | WordPress | WordPress specific exploits |
| EXR | Posix | Posix based path traversal attempts |
| EXR | Windows | Windows based path traversal attempts |
| IP List | AWS IP Reputation List | Blocks IP that is known to have bot activities |
| IP List | Anonymous IP list | VPN, proxies, Tor nodes, and hosting providers. |



AWS Managed Rules for AWS WAF ルール一覧

(2020/3/24現在)

| Name | Description | Capacity Unit |
|---------------------------|---|---------------|
| Admin protection | 管理者保護ルールグループには、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が含まれる。これは、サードパーティーのソフトウェアを実行している場合や、悪意のあるアクターがアプリケーションへの管理アクセスを得るリスクを軽減したい場合に有効 | 100 |
| Amazon IP reputation list | このグループには、Amazon の内部脅威インテリジェンスに基づくIPレピュテーションリストが含まれる。これは、通常、ボットやその他の脅威に関連付けられている IP アドレスをブロックする場合に有効。これらの IP アドレスをブロックすることで、ボットを軽減し、悪意のあるアクターが脆弱なアプリケーションを発見するリスクを軽減できる。 | 25 |
| Anonymous IP list | このグループには、匿名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ためのルールが含まれる。これには、VPN、プロキシ、Torノード、およびホスティングプロバイダからの要求が含まれる。アプリケーションからアイデンティティを隠そうとしている可能性のあるビューアを除外する場合に有効。 | 50 |
| Core rule set | コアルールセット (CRS) ルールグループには、ウェブアプリケーションに一般的に適用可能なルールが含まれる。これらは、OWASP の出版物や多くの共通脆弱性識別子 (CVE) に記載されているものを含め、幅広い脆弱性の悪用から保護するのに有用。すべての AWS WAF ユースケースでこのルールグループを使用することの検討を推奨 | 700 |
| Known bad inputs | 既知の不正な入力ルールグループには、無効且つ脆弱性の悪用または発見に関連するリクエストパターンをブロックするルールが含まれる。これにより、悪意のあるアクターが脆弱なアプリケーションを発見するリスクを軽減可能 | 200 |
| Linux operating system | Linux オペレーティングシステムルールグループには、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が含まれる。これにより、攻撃者がアクセスしてはならないファイルの内容を公開したり、コードを実行したりする攻撃を防ぐ。アプリケーションの一部が Linux で実行されている場合は、このルールグループを評価する必要がある。また、このルールグループは、POSIX オペレーティングシステムルールグループと組み合わせて使用する必要がある。 | 200 |

AWS マネージドルール ルールグループ のリスト

https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/aws-managed-rule-groups-list.html

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

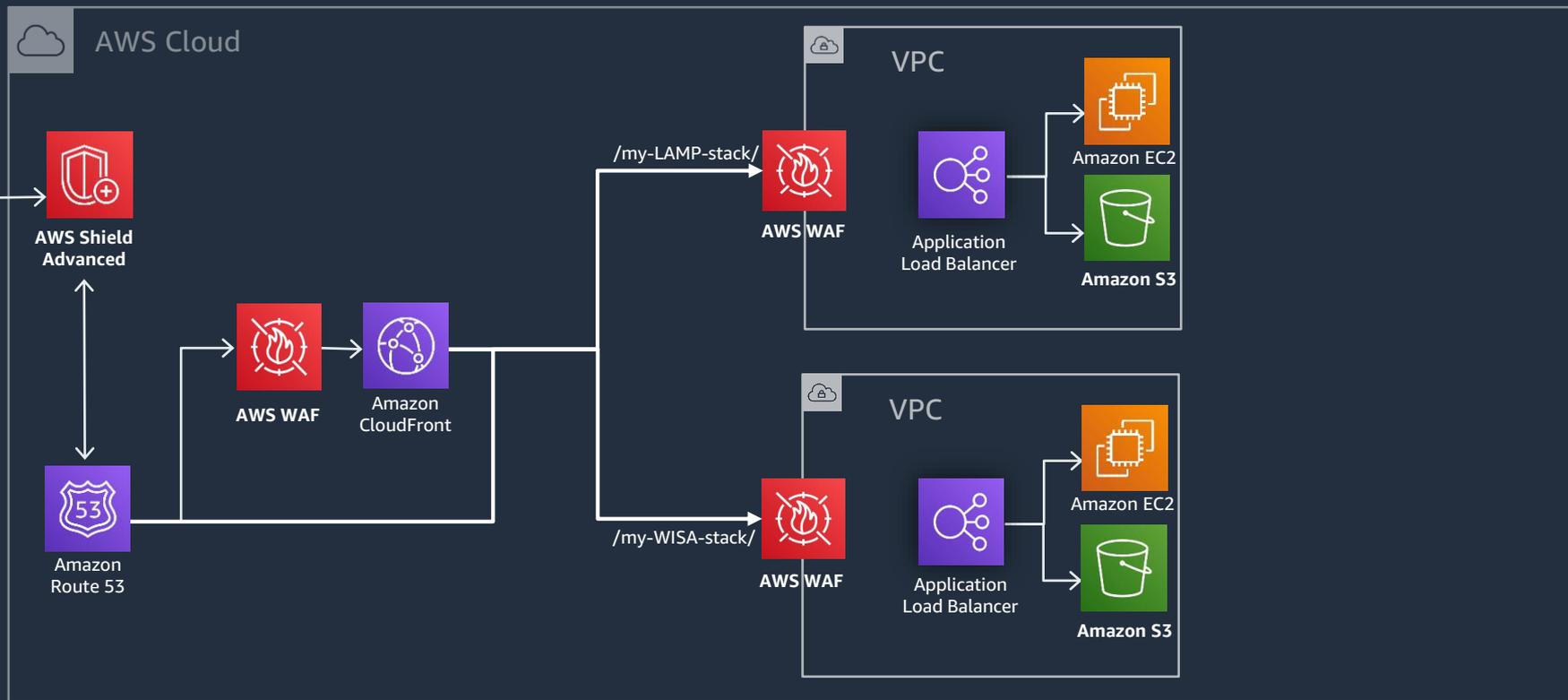


AWS Managed Rules for AWS WAF ルール一覧

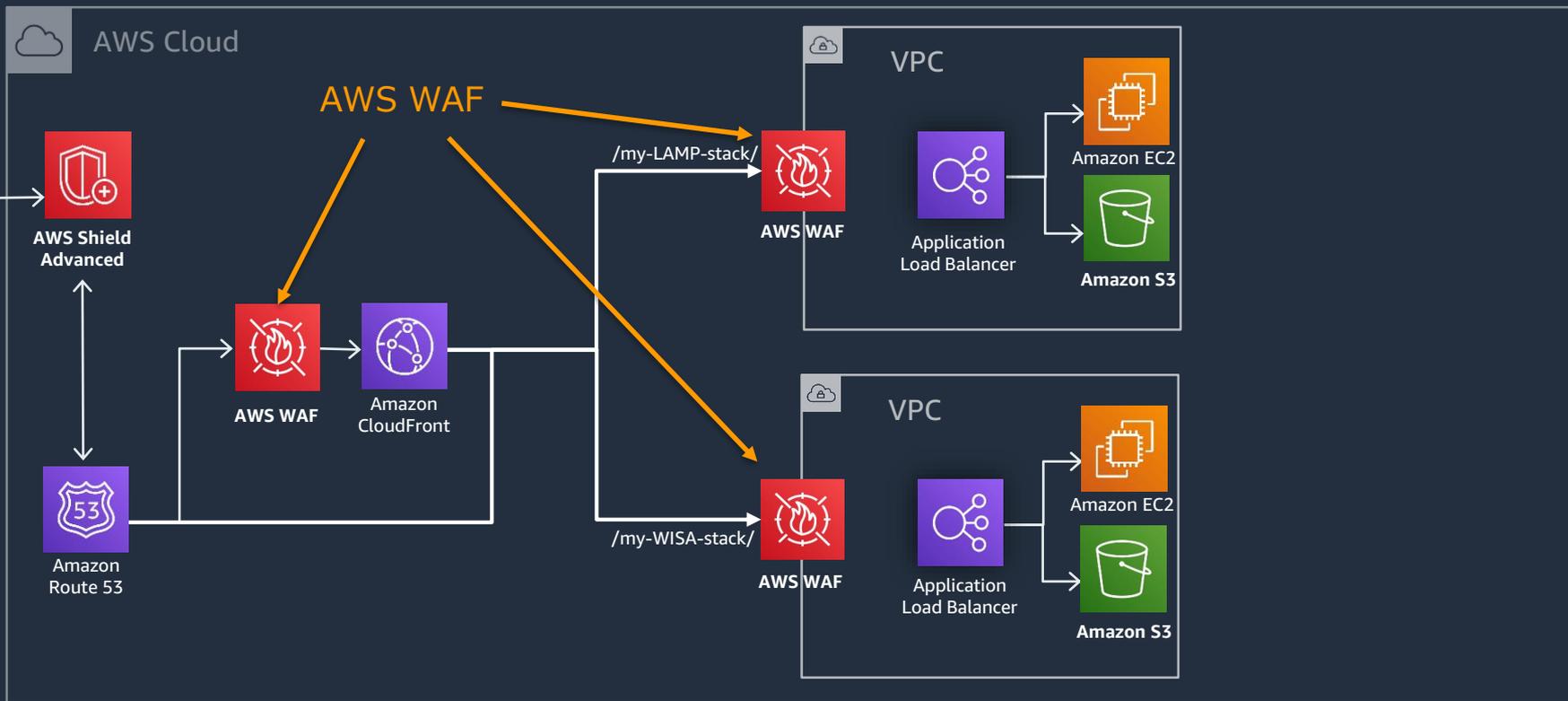
(2020/3/24現在)

| Name | Description | Capacity Unit |
|--------------------------|--|---------------|
| PHP application | PHP アプリケーションルールグループには、安全でない PHP 関数のインジェクションなど、PHP プログラミング言語の使用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が含まれる。これにより、攻撃者が許可されていないコードまたはコマンドをリモートで実行できる脆弱性の悪用を防ぐ。アプリケーションが連結するサーバーに PHP がインストールされている場合は、このルールグループを使用することの検討を推奨 | 100 |
| POSIX operating system | POSIX オペレーティングシステムルールグループには、ローカルファイルインクルージョン (LFI) 攻撃を含む 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に関連するリクエストパターンをブロックするルールが含まれる。これにより、攻撃者がアクセスしてはならないファイルの内容を公開したり、コードを実行したりする攻撃を防ぐことが可能。アプリケーションの一部が、Linux、AIX、HP-UX、macOS、Solaris、FreeBSD、OpenBSD、その他多くのものを含む POSIX または POSIX と同等のオペレーティングシステムで実行されている場合は、このルールグループを使用することの検討を推奨。 | 100 |
| Windows operating system | Windows オペレーティングシステムのルールグループには、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が含まれる。これにより、攻撃者が不正なコマンドを実行したり、悪意のあるコードを実行したりする脆弱性の悪用を防ぐことが可能。アプリケーションの一部が Windows オペレーティングシステムで実行されている場合は、このルールグループを使用することの検討を推奨。 | 200 |
| SQL database | SQL Database ルールグループには、SQL インジェクション攻撃などの 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が含まれる。これにより、不正なクエリのリモートインジェクションを防ぐことが可能。アプリケーションが SQL データベースと連結している場合は、このルールグループを使用することの検討を推奨。 | 200 |
| WordPress application | WordPress アプリケーショングループには、WordPress サイト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が含まれる。WordPress を実行している場合は、このルールグループを使用することの検討を推奨。このルールグループは、SQL データベースおよび PHP アプリケーションルールグループと組み合わせて使用が必要がある。 | 100 |

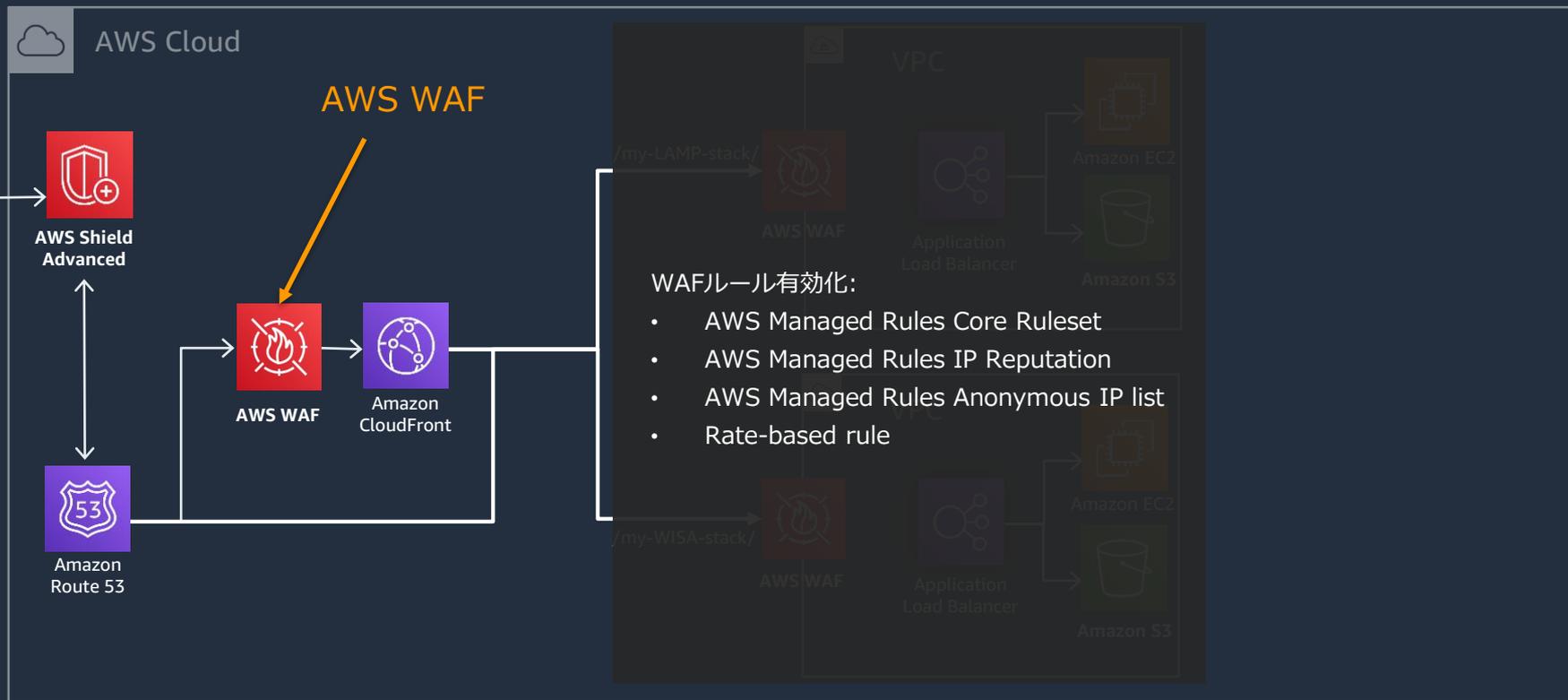
ユースケース: AWS Managed Rulesを利用した多段防御



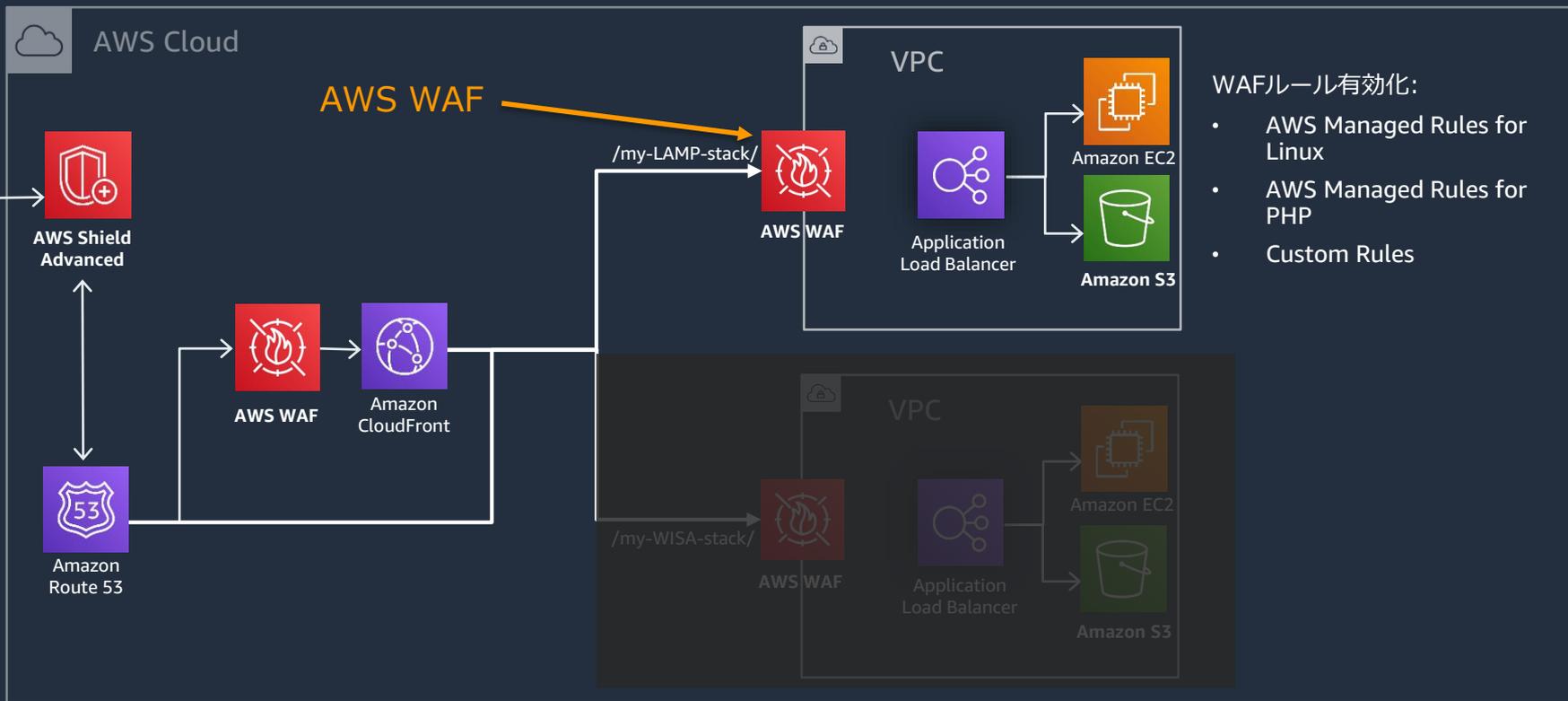
ユースケース: AWS Managed Rulesを利用した多段防御



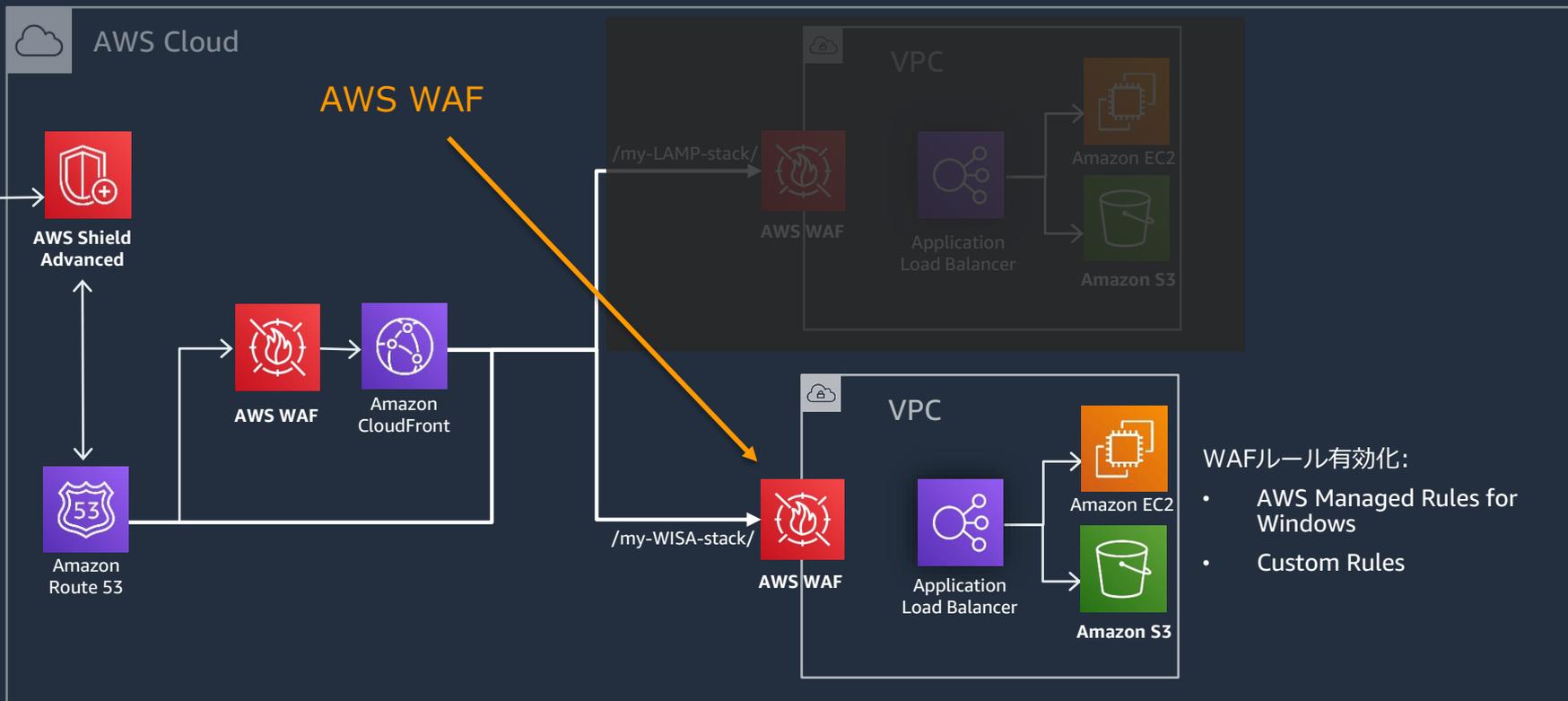
ユースケース: AWS Managed Rulesを利用した多段防御



ユースケース: AWS Managed Rulesを利用した多段防御



ユースケース: AWS Managed Rulesを利用した多段防御



本日のアジェンダ

1. Web Application Firewall(WAF)とは
2. AWS WAFの機能
3. アップデートによる主な変更点
4. AWS WAFの詳細
5. AWS Managed Rules for AWS WAF
6. Web ACL作成の流れ
7. ログとモニタリング
8. AWS WAF利用のための考慮事項
9. 料金体系

Web ACL名の設定と対象リソースの選択

Web ACLの名称の設定

AWS WAFを適用するリソースの選択

Step 1
Describe web ACL and associate it to AWS resources

Step 2
Add rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Describe web ACL and associate it to AWS resources [Info](#)

Web ACL details

Name

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Description - optional

The description can have 1-256 characters.

CloudWatch metric name

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Resource type
Choose the type of resource to associate with this web ACL.

CloudFront distributions

Regional resources (Application Load Balancer and API Gateway)

Region
Choose the AWS region to create this web ACL in.

Global (CloudFront) ▾

Associated AWS resources - optional Remove Add AWS resources

< 1 > ⌘

| Name | Resource type | Region |
|---------------------------------|---------------|--------|
| No results | | |
| There are no results to display | | |

Cancel Next

利用するルールを選択

使用するルールを選択する
(ルール設定の子ウィザード
が起動)

Step 1
Describe web ACL and
associate it to AWS resources

Step 2
Add rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Add rules and rule groups [Info](#)

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

Rules
If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

Edit Delete **Add rules** ▼

- Add managed rule groups
- Add my own rules and rule groups

| <input type="checkbox"/> | Name | Action |
|---------------------------------|------|--------|
| No rules. | | |
| You don't have any rules added. | | |

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

Default action

- Allow
- Block

Cancel Previous **Next**

AWSマネージドルールールの追加

Managed Rule Group内で
利用するルールを選択

Step 1
Describe web ACL and
associate it to AWS resources

Step 2
Add rules and rule groups:
Add managed rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Add managed rule groups [Info](#)

Managed rule groups are created and maintained for you by AWS and AWS Marketplace sellers.

| Name | Capacity | Action |
|--|----------|---|
| Admin protection Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application. | 100 | <input checked="" type="radio"/> Add to web ACL <input type="radio"/> Set rules action to count |
| Amazon IP reputation list This group contains rules that are based on Amazon threat intelligence. This is useful if you would like to block sources associated with bots or other threats. | 25 | <input checked="" type="radio"/> Add to web ACL <input checked="" type="radio"/> Set rules action to count |
| Core rule set Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications and common Common Vulnerabilities and Exposures (CVE). | 700 | <input checked="" type="radio"/> Add to web ACL <input type="radio"/> Set rules action to count |
| Known bad inputs Contains rules that allow you to block request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of | 200 | <input type="radio"/> Add to web ACL |

デフォルトアクションの選択

選択されたルールを確認

WCUの合計を確認

デフォルトアクションを
許可 (Allow) か拒否
(Block) ションを選択

Step 1
Describe web ACL and associate it to AWS resources

Step 2
Add rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Add rules and rule groups [Info](#)

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

Rules

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

[Edit](#) [Delete](#) [Add rules](#)

| <input type="checkbox"/> | Name | Capacity | Action |
|--------------------------|---|----------|------------------|
| <input type="checkbox"/> | AWS-AWSManagedRulesAdminProtectionRuleSet | 100 | Use rule actions |
| <input type="checkbox"/> | AWS-AWSManagedRulesAmazonIpReputationList | 25 | Use rule actions |
| <input type="checkbox"/> | AWS-AWSManagedRulesCommonRuleSet | 700 | Use rule actions |
| <input type="checkbox"/> | AWS-AWSManagedRulesKnownBadInputsRuleSet | 200 | Use rule actions |
| <input type="checkbox"/> | AWS-AWSManagedRulesPHPRuleSet | 100 | Use rule actions |
| <input type="checkbox"/> | AWS-AWSManagedRulesSQLiRuleSet | 200 | Use rule actions |

Web ACL rule capacity units used
The total capacity units used by the web ACL can't exceed 1500.
1325/1500 WCU

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

Default action

Allow
 Block

[Cancel](#) [Previous](#) [Next](#)

ルールの優先度の設定

ルールの優先度（適用順序）
を指定

AWS WAF > Web ACLs > Create web ACL

Step 1
Describe web ACL and associate it to AWS resources

Step 2
Add rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Set rule priority [Info](#)

Rules
If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

| | | | |
|----------------------------------|---|-----|------------------|
| <input type="radio"/> | AWS- AWSManagedRulesAdminProtectionRuleSet | 100 | Use rule actions |
| <input checked="" type="radio"/> | AWS- AWSManagedRulesAmazonIpReputationList | 25 | Count |
| <input type="radio"/> | AWS-AWSManagedRulesCommonRuleSet | 700 | Use rule actions |
| <input type="radio"/> | AWS-AWSManagedRulesWindowsRuleSet | 200 | Count |
| <input type="radio"/> | AWS-AWSManagedRulesSQLiRuleSet | 200 | Use rule actions |

CloudWatchメトリクスの設定

CloudWatchメトリクス名を指定（デフォルトはルール名がそのまま適用される）

AWS WAF > Web ACLs > Create web ACL

Step 1
Describe web ACL and associate it to AWS resources

Step 2
Add rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Configure metrics [Info](#)

Amazon CloudWatch metrics

CloudWatch metrics allow you to monitor web requests, web ACLs, and rules. You incur charges for each metric that AWS WAF emits to CloudWatch.

| | | |
|-------------------------------------|---|--------------------------------------|
| <input checked="" type="checkbox"/> | AWS-AWSManagedRulesAdminProtectionRuleSet | AWS-AWSManagedRulesAdminProtectionRu |
| <input checked="" type="checkbox"/> | AWS-AWSManagedRulesAmazonIpReputationList | AWS-AWSManagedRulesAmazonIpReputatio |
| <input checked="" type="checkbox"/> | AWS-AWSManagedRulesCommonRuleSet | AWS-AWSManagedRulesCommonRuleSet |
| <input checked="" type="checkbox"/> | AWS-AWSManagedRulesWindowsRuleSet | AWS-AWSManagedRulesWindowsRuleSet |
| <input checked="" type="checkbox"/> | AWS-AWSManagedRulesSQLiRuleSet | AWS-AWSManagedRulesSQLiRuleSet |

Cancel Previous Next

設定レビューとWeb ACL作成

設定した内容をレビューし、
Web ACLを作成

AWS WAF > Web ACLs > Create web ACL

Review and create web ACL Info

Step 1: Describe web ACL and associated AWS resources Edit

Web ACL details

| | | | |
|------------------------|---------------|--------|------------|
| Name | TestACL121001 | Scope | CLOUDFRONT |
| Description | | Region | global |
| CloudWatch metric name | TestACL121001 | | |

Steps 2 and 3: Add rules and set rule priority Edit

Rules

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

| Name | Capacity | Action |
|---|----------|------------------|
| AWS-AWSManagedRulesAdminProtectionRuleSet | 100 | Use rule actions |
| AWS-AWSManagedRulesAmazonipReputationList | 25 | Use rule actions |
| AWS-AWSManagedRulesCommonRuleSet | 700 | Use rule actions |
| AWS-AWSManagedRulesKnownBadInputsRuleSet | 200 | Use rule actions |
| AWS-AWSManagedRulesLinuxRuleSet | 200 | Use rule actions |
| AWS-AWSManagedRulesPHPRuleSet | 100 | Use rule actions |

Web ACL rule capacity units used
The total capacity units used by the web ACL can't exceed 1500.

1325/1500 WCUs

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

Default action

Allow

Block

Step 4: Configure metrics Edit

Amazon CloudWatch metrics

| Rules | CloudWatch metric name |
|---|---|
| AWS-AWSManagedRulesAdminProtectionRuleSet | AWS-AWSManagedRulesAdminProtectionRuleSet |
| AWS-AWSManagedRulesAmazonipReputationList | AWS-AWSManagedRulesAmazonipReputationList |
| AWS-AWSManagedRulesCommonRuleSet | AWS-AWSManagedRulesCommonRuleSet |
| AWS-AWSManagedRulesKnownBadInputsRuleSet | AWS-AWSManagedRulesKnownBadInputsRuleSet |
| AWS-AWSManagedRulesLinuxRuleSet | AWS-AWSManagedRulesLinuxRuleSet |
| AWS-AWSManagedRulesPHPRuleSet | AWS-AWSManagedRulesPHPRuleSet |

Cancel Previous **Create web ACL**

自分で作成したルールを追加する

IPセットルール、ルールビルダー、ルールグループから選択

ルールの整合性チェック

ステートメントを設定

ルールのアクションを選択

The screenshot shows the 'Add rule' page in the AWS WAF console. The breadcrumb trail is 'AWS WAF > Web ACLs > reinvent_recap_ACL001 > Add rule'. The 'Rule type' section has three options: 'IP set' (unselected), 'Rule builder' (selected), and 'Rule group' (unselected). Below this is a 'Validate' button. The 'If a request' dropdown is set to 'matches the statement'. The 'Statement' section has an 'Inspect' dropdown set to 'Choose an inspection option'. The 'Then' section has an 'Action' dropdown set to 'Block'. At the bottom right are 'Cancel' and 'Add rule' buttons.

自分で作成したルールを追加する(JSON editor)

複雑なネスト条件を定義する場合にJSON editorで直接JSON形式でルールを記述可能 (Visual editorでは一つのネストのみ対応)

The screenshot shows the 'Add new rule' interface in the AWS IAM console. The 'Rule builder' section is active, and the 'JSON editor' tab is selected. The JSON editor contains the following rule definition:

```
1 {
2   "Matcher": {
3     "Type": "OrMatch",
4     "Matcher1": {
5       "Type": "ByteMatch",
6       "Haystack": "Header:UserAgent",
7       "Needle": "[\"firefox\",WW-Mechanize",
8         "WWW-Mechanize",
9         "x22Mozilla",
10        "x22Mozilla"]",
11     },
12     "Transformations": [
13       "lowercase"
14     ],
15     "Matcher2": {
16       "Type": "ByteMatch",
17       "Haystack": "Header:Referrer",
18       "Needle": "[\"firefox\",WW-Mechanize",
19         "spam-referrer",
20         "content-copier"]",
21     },
22     "Transformations": [
23       "lowercase"
24     ],
25     "Action": {
26       "Type": "BLOCK"
27     }
28   }
29 }
```

APIによるWebACLの作成と更新



JSON形式でweb ACLを定義し、APIを呼び出す

web ACL: **CreateWebACL** または **UpdateWebACL** を利用

- シンタックスのチェックを行い、作成/更新を実施
- エラーが発生した場合は、以下のようなエラーメッセージが出力される
 - 例: WebACL has exceeded WCU capacity, rule statement is illogical

RuleGroup: **CreateRuleGroup** または **UpdateRuleGroup**

IP set: **CreateIPSet** または **UpdateIPSet**

Regex set: **CreateRegexPatternSet** または **UpdateRegexPatternSet**

WAFv2 APIでサポートされるアクション一覧

AssociateWebACL
CreateIPSet
CreateRegexPatternSet
CreateRuleGroup
CreateWebACL
DeleteIPSet
DeleteRegexPatternSet
DeleteRuleGroup
DeleteWebACL
DisassociateWebACL
GetIPSet
GetManagedRuleSet
GetRateBasedStatementManagedKeys

GetRegexPatternSet
GetRuleGroup
GetWebACL
GetWebACLForResource
ListIPSets
ListManagedRuleSets
ListRegexPatternSets
ListResourcesForWebACL
ListRuleGroups
ListWebACLs
UpdateIPSet
UpdateRegexPatternSet
UpdateRuleGroup
UpdateWebACL

AWS WAFV2
APIリファレンス

https://docs.aws.amazon.com/waf/latest/APIReference/API_Operations.html

※ CLIで利用する場合は単語に-を付与
例) ListIPSets → list-ip-sets
aws wafv2 list-ip-sets --scope=REGIONAL

APIによるWeb ACLの作成例

```
// web ACLの作成例（作成するが関連付けはしない/別API）
{
  "Name": "foo",           // web ACLの名前
  "Scope": "CLOUDFRONT", // web ACLのリージョンまたはCloudFront (Global)
  "DefaultAction": {     // web ACLでルールがトリガーされなかった場合のデフォルト動作
    "Block": {}          // 1つ選ぶ
    "Allow": {}
  },
  "Description": "foo", // web ACLのDescription
  "Rules": [ // ルール記載ブロック
    {
      <Rule #1>
    }, {
      <Rule #2>
    }
  ],
  "VisibilityConfig": { // CloudWatch とSampledRequests の設定
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "TestMetric"
  }
}
```

ルールの記述例

// conditionを組み合わせてルールを作成する

```
"Rules": [  
  {  
    "Name": "foo",  
    "Priority": 1, // トリガーされる順序 (プライオリティ)  
    "Statements": {  
      <Condition> // conditions (SQLInjectionを検知した場合、など)を定義  
    },  
    "Action": {  
      "Block": {}  
      "Allow": {}  
      "Count": {}  
    },  
    "VisibilityConfig": { // CloudWatch とSampledRequests の設定  
      "SampledRequestsEnabled": true,  
      "CloudWatchMetricsEnabled": true,  
      "MetricName": "TestMetric"  
    }  
  }  
] // 必要な内容を継続して記載
```

ステートメントの記述例 (XSS and SQLi)

```
"Statement": {
  "OrStatement": {
    "Statements": [{
      "XssMatchStatement": {
        "FieldToMatch": {
          "QueryString": {}
        },
        "TextTransformations": [
          {"Priority": 1, "Type": "URL_DECODE"},
          {"Priority": 2, "Type": "LOWERCASE"}
        ]
      },
      {
        "SqliMatchStatement": {
          "FieldToMatch": {
            "Body": {}
          },
          "TextTransformations": [
            {"Priority": 1, "Type": "HTML_ENTITY_DECODE"},
            {"Priority": 2, "Type": "NONE_COMPRESS_WHITE_SPACE"}
          ]
        }
      }
    ]
  }
}
```

テキスト変換の種類:

- NONE
- COMPRESS_WHITE_SPACE
- HTML_ENTITY_DECODE
- LOWERCASE
- CMD_LINE
- URL_DECODE

本日のアジェンダ

1. Web Application Firewall(WAF)とは
2. AWS WAFの機能
3. アップデートによる主な変更点
4. AWS WAFの詳細
5. AWS Managed Rule for AWS WAF
6. Web ACL作成の流れ
7. ログとモニタリング
8. AWS WAF利用のための考慮事項
9. 料金体系
10. まとめ

モニタリング

- Amazon CloudWatchを利用してAWS WAFのメトリクスをモニタリング、アラートの設定が可能
- サンプルリクエストからリクエスト内容の詳細(ソースIP、URI、リクエストBodyなど)を確認可能

Sample request

| Source IP | Matches rule | Action | Time |
|-----------|--------------|--------|--|
| | - | ALLOW | Thu Feb 27 2020 22:03:14 GMT+0900 (日本標準時) |

URI
/index.html

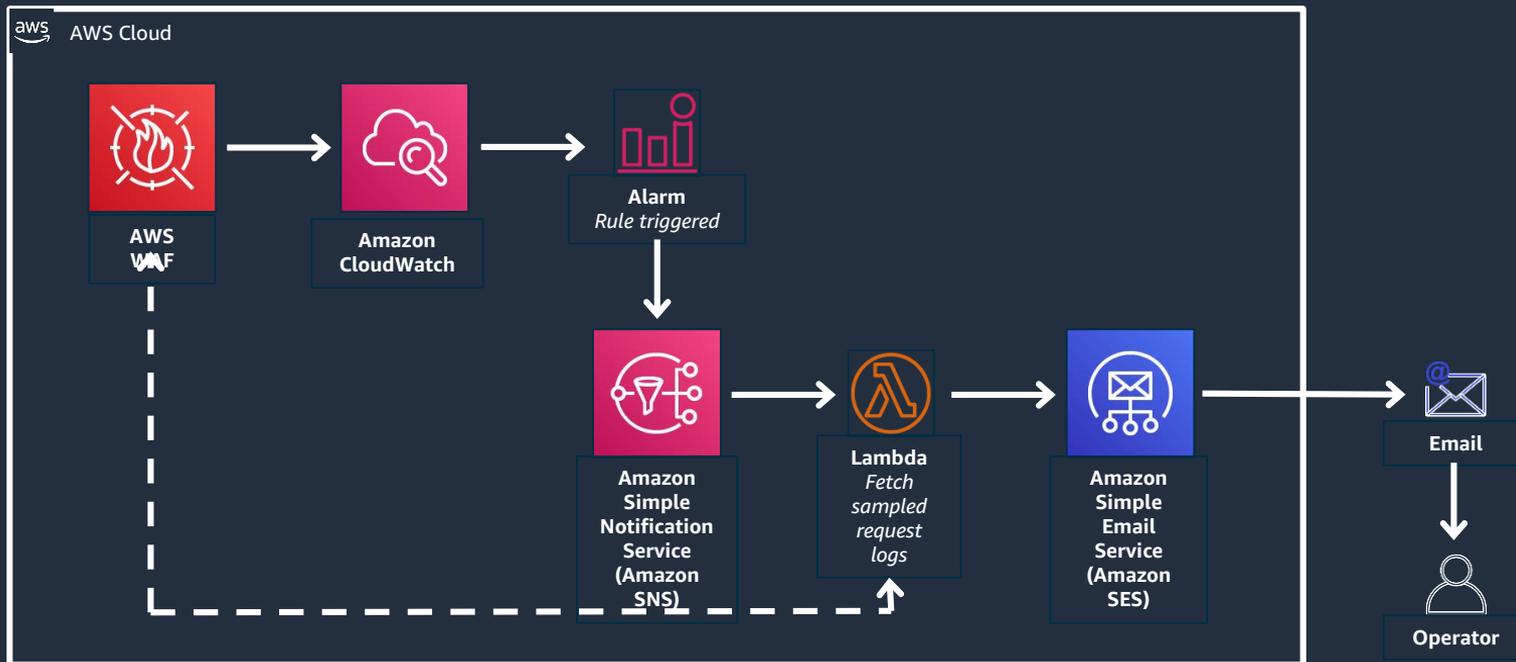
Request body

```
GET /index.html
Host:
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/75.0.3738.0 Safari/537.36 CloudWatchSynthetics/arn:aws:synthetics:us-east-1]
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
accept-encoding: gzip, deflate, br
accept-language: en-US
```

Close



参考: Amazon CloudWatchによるインシデントレポート



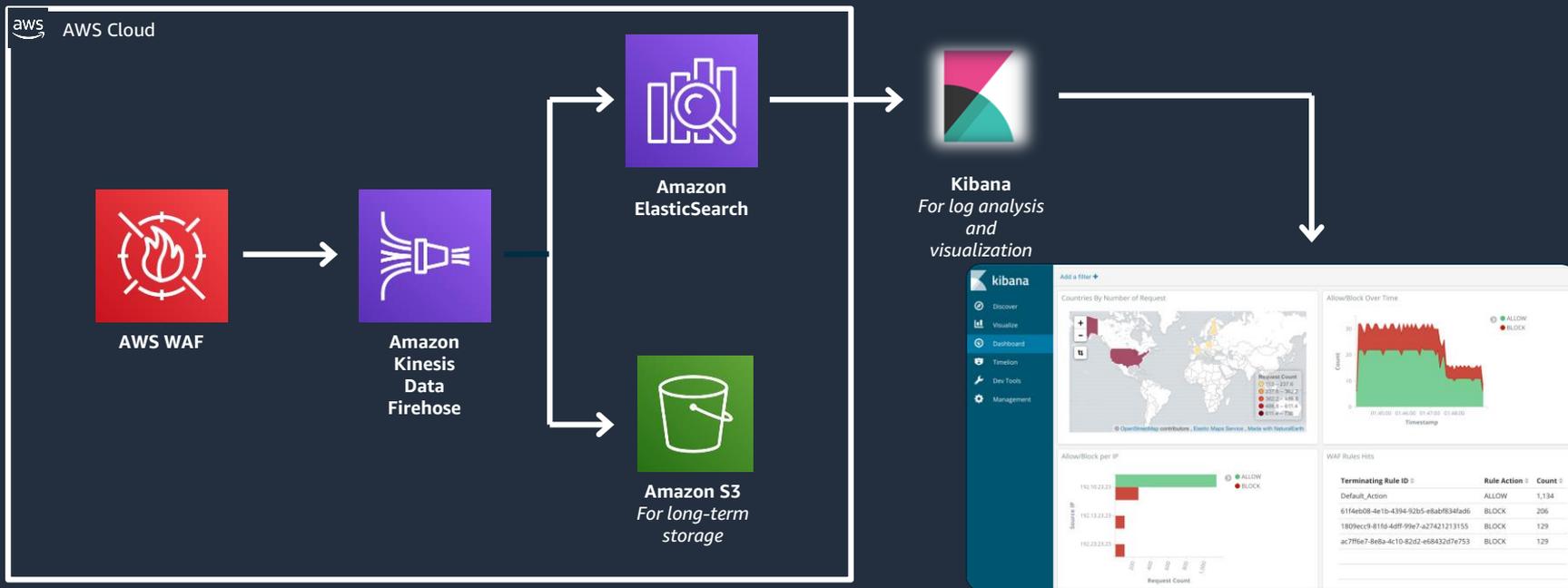
AWS WAF Full logs

- 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

```
"terminatingRuleId": "STMTTest_SQLi_XSS",  
"terminatingRuleType": "REGULAR",  
"action": "BLOCK",  
"terminatingRuleMatchDetails": [  
  {  
    "conditionType": "SQL_INJECTION",  
    "location": "HEADER",  
    "matchedData": [  
      "10",  
      "AND",  
      "1"  
    ]  
  }  
]
```



参考 : Amazon Elasticsearch and Kibanaによるログ分析



How to analyze AWS WAF logs using Amazon Elasticsearch Service
<https://aws.amazon.com/blogs/security/how-to-analyze-aws-waf-logs-using-amazon-elasticsearch-service/>

参考: カスタムエラーページ(Block時に任意のページを表示)

WAFのBlock時にカスタムエラーページを表示したい場合、CloudFrontの“Custom Error Response”から任意のエラーページを設定可能

注意点:

- CloudFrontのみ設定可能 (CloudFrontのカスタムエラーページの機能を利用)
- オリジンによって返された 403と、AWS WAFが返す 403 を区別できません
- ステータスコード 403 で複数のエラーページを表示できません。
アプリケーションが出す 403とAWS WAFが出す 403 は同じエラーページを表示することになります。

参考: パートナーマネージドルール

パートナー提供のマネージドルールも利用可能

AWS Marketplaceでパートナー提供のマネージドルールグループをサブスクライブすることで、AWS WAFからそのマネージドルールグループを使用可能



AWS Marketplace

<https://aws.amazon.com/marketplace/solutions/security/waf-managed-rules>



本日のアジェンダ

1. Web Application Firewall(WAF)とは
2. AWS WAFの機能
3. アップデートによる主な変更点
4. AWS WAFの詳細
5. AWS Managed Rules for AWS WAF
6. Web ACL作成の流れ
7. ログとモニタリング
8. AWS WAF利用のための考慮事項
9. 料金体系
10. まとめ

AWS WAF利用のための考慮事項 1 - ルールポリシー

ブラックリスト型 (ネガティブ)

- デフォルトのアクションは許可
- ルールに合致した不正なリクエストをブロック
- 一般的なWebサイトではこちらが多い

ホワイトリスト型 (ポジティブ)

- デフォルトのアクションはブロック
- ルールに合致したリクエストのみを許可
- 全てのリクエストパターンが事前に把握できる場合のみ
- 限られた利用者がアクセスするケース

AWS WAF利用のための考慮事項 2 - ルールの運用

セルフサービス

- テンプレートなどを利用してルールを構築
- ログの分析やルールのアップデートを継続実施
- 誤検知が発生した場合は、ルールの見直しを自身で実施

マネージド

- AWSパートナーのマネージドルールまたは、AWS Managed rules for AWS WAFを利用する
- ルールのアップデートはManaged Ruleの提供ベンダーに任せる
- 誤検知が発生した場合はルールに合致した文字列を正規表現ルールに設定して、部分的にトラフィックを通す。または該当ルールをCountモードへ切り替え

参考

マネージドルール内の個別のルールを Countモードに切り替える

Rules (4)

Find rules

Edit Delete Add rules

| Name | Action | Priority |
|--|--------|----------|
| <input type="checkbox"/> AWS-AWSManagedRulesAmazonIpReputationList | Count | 0 |
| <input checked="" type="checkbox"/> AWS-AWSManagedRulesCommonRuleSet | Count | 1 |
| <input type="checkbox"/> AWS-AWSManagedRulesLinuxRuleSet | Count | 2 |
| <input type="checkbox"/> AWS-AWSManagedRulesSQLIRuleSet | Count | 3 |

AWS WAF > Web ACL > WebACL_Test > Edit rule

Core rule set

Description
Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications and common Common Vulnerabilities and Exposures (CVE).
Capacity: 700

Action
 Enable count mode

| Name | Override rules action |
|-------------------------------------|--|
| NoUserAgent_HEADER | <input checked="" type="radio"/> Override rules action |
| UserAgent_BadBots_HEADER | <input checked="" type="radio"/> Override rules action |
| SizeRestrictions_QUERYSTRING | <input checked="" type="radio"/> Override rules action |
| SizeRestrictions_Cookie_HEADER | <input checked="" type="radio"/> Override rules action |
| SizeRestrictions_BODY | <input checked="" type="radio"/> Override rules action |
| SizeRestrictions_URI_PATH | <input checked="" type="radio"/> Override rules action |
| EC2MetaDataSSRF_BODY | <input checked="" type="radio"/> Override rules action |
| EC2MetaDataSSRF_COOKIE | <input checked="" type="radio"/> Override rules action |
| EC2MetaDataSSRF_URI_PATH | <input checked="" type="radio"/> Override rules action |
| EC2MetaDataSSRF_QUERYARGUMENTS | <input checked="" type="radio"/> Override rules action |
| GenericLFI_QUERYARGUMENTS | <input checked="" type="radio"/> Override rules action |
| GenericLFI_URI_PATH | <input checked="" type="radio"/> Override rules action |
| GenericLFI_BODY | <input checked="" type="radio"/> Override rules action |
| RestrictedExtensions_URI_PATH | <input checked="" type="radio"/> Override rules action |
| RestrictedExtensions_QUERYARGUMENTS | <input checked="" type="radio"/> Override rules action |
| GenericRFI_QUERYARGUMENTS | <input checked="" type="radio"/> Override rules action |
| GenericRFI_BODY | <input checked="" type="radio"/> Override rules action |
| GenericRFI_URI_PATH | <input checked="" type="radio"/> Override rules action |
| CrossSiteScripting_COOKIE | <input checked="" type="radio"/> Override rules action |
| CrossSiteScripting_QUERYARGUMENTS | <input checked="" type="radio"/> Override rules action |
| CrossSiteScripting_BODY | <input checked="" type="radio"/> Override rules action |
| CrossSiteScripting_URI_PATH | <input checked="" type="radio"/> Override rules action |

AWS WAF利用のための考慮事項 2 - ルールの運用

セルフサービス

- テンプレートなどを利用してルールを構築
- ログの分析やルールのアップデートを継続実施
- 誤検知が発生した場合は、ルールの見直しを自身で実施

マネージド

- AWSパートナーのマネージドルールまたは、AWS Managed rules for AWS WAFを利用する
- ルールのアップデートはManaged Ruleの提供ベンダーに任せる
- 誤検知が発生した場合はルールに合致した文字列を正規表現ルールに設定して、部分的にトラフィックを通す。または該当ルールをCountモードへ切り替え

AWS WAF利用のための考慮事項3 - 導入ステップ

Countモード

- 開発環境等でテストを実施
- 誤検知が発生しないかサンプルリクエストレポートで確認
- CloudWatchメトリクスでルールを評価
- Full Logを確認



Blockモード

- 誤検知がないことを確認後、Blockモードへ変更
- 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
- Blockされたリクエストは、Full logでWebACLsルールにマッチした内容を確認できる

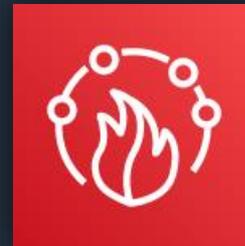
AWS WAFとの組み合わせ



AWS WAF



AWS Shield
Advanced



AWS Firewall
Manager

本日のアジェンダ

1. Web Application Firewall(WAF)とは
2. AWS WAFの機能
3. アップデートによる主な変更点
4. AWS WAFの詳細
5. AWS Managed Rules for AWS WAF
6. Web ACL作成の流れ
7. ログとモニタリング
8. AWS WAF利用のための考慮事項
9. 料金体系
10. まとめ

AWS WAFの料金

Web ACL

- \$5 /月 (1web ACLあたり/1500 WCUを含む)

ルール

- \$1 /月 (1ルールあたり)

リクエスト数

- \$0.60 /百万リクエスト
- 全てのリージョンで同一価格

料金計算ツール

aws pricing calculator

Feedback

Configure AWS Web Application Firewall (WAF) [Info](#)

サービスの設定

使用されたウェブアクセスコントロールリスト (ウェブ ACL) の数

多くの場合、これは AWS WAF を使用して保護したい AWS リソースの数です。同じリージョン内の複数の AWS リソース間でウェブ ACL を共有することに注意してください。

/月

ウェブ ACL ごとに追加するルールの数

/月

ウェブ ACL ごとのルールグループの数

This only includes custom Rule Groups that you create. It does not include Managed Rule Groups.

/月

各ルールグループ内のルールの数

/月

Number of Managed Rule Groups

Managed Rule Groups from AWS Marketplace are charged additional fees as per the seller.

/月

受信したウェブリクエストの数

100 万/月

▼ Show calculations

2 Web ACLs per month x 5.00 USD = 10.00 USD (WAF Web ACLs cost)

4 Rules added per Web ACL + 1 Managed Rule Groups = 5.00 Total billable Rules

5.00 Billable Rules per month x 1.00 USD = 5.00 USD (WAF Rules cost)

1 requests per month x 1000000 multiplier for million x 0.0000006 USD = 0.60 USD (WAF Requests cost)

料金計算ツール

<https://aws.amazon.com/jp/waf/pricing/>

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



本日のアジェンダ

1. Web Application Firewall(WAF)とは
2. AWS WAFの機能
3. アップデートによる主な変更点
4. AWS WAFの詳細
5. AWS Managed Rules for AWS WAF
6. Web ACL作成の流れ
7. ログとモニタリング
8. AWS WAF利用のための考慮事項
9. 料金体系
10. まとめ

まとめ

- マネージドルールにより、実践的なルールセットをすぐに導入可能
- フレキシブルにルールをカスタマイズ可能
- 全ての機能がAPIでコントロール可能
- モニタリングやログにより迅速に攻撃状況を把握可能
- 今すぐ使い始められて、使った分だけの料金

参考資料

- AWS WAF 開発者ガイド
https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/waf-chapter.html
- AWS マネージドルール ルールグループ のリスト
https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/aws-managed-rule-groups-list.html
- AWS マネージドルール変更履歴
<https://docs.aws.amazon.com/waf/latest/developerguide/aws-managed-rule-groups-changelog.html>
- AWS WAF V2 APIリファレンス
https://docs.aws.amazon.com/waf/latest/APIReference/API_Operations.html
- 料金計算ツール
<https://aws.amazon.com/jp/waf/pricing/>

Q&A

お答えできなかったご質問については

AWS Japan Blog 「<https://aws.amazon.com/jp/blogs/news/>」にて
後日掲載します。

AWS の日本語資料の場所「AWS 資料」で検索



日本担当チームへお問い合わせ サポート 日本語 ▼ アカウント ▼

コンソールにサインイン

製品 ソリューション 料金 ドキュメント 学習 パートナー AWS Marketplace その他 🔍

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 »](#)

[業種・ソリューション別資料 »](#)

[サービス別資料 »](#)

<https://amzn.to/JPArchive>



AWS Well-Architected 個別技術相談会

毎週“W-A個別技術相談会”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

- 申込みはイベント告知サイトから

(<https://aws.amazon.com/jp/about-aws/events/>)

AWS イベント

で[検索]



ご視聴ありがとうございました

AWS 公式 Webinar

<https://amzn.to/JPWebinar>



過去資料

<https://amzn.to/JPArchive>

