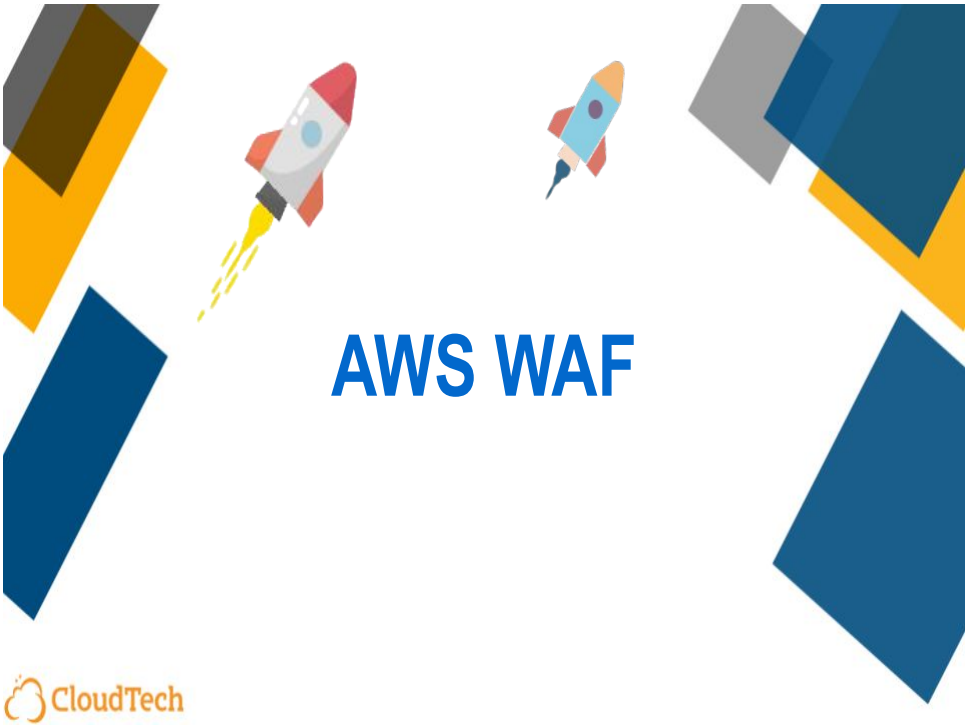
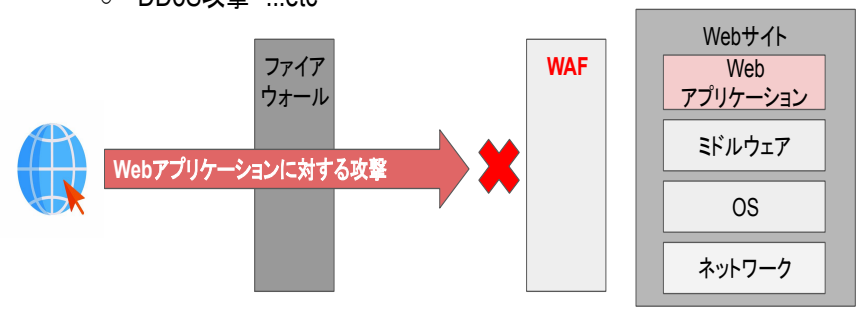


- AWS WAFは、Webアプリケーションに対する攻撃から保護をするためのサービスです。

WAF（Web Application Firewall）とは

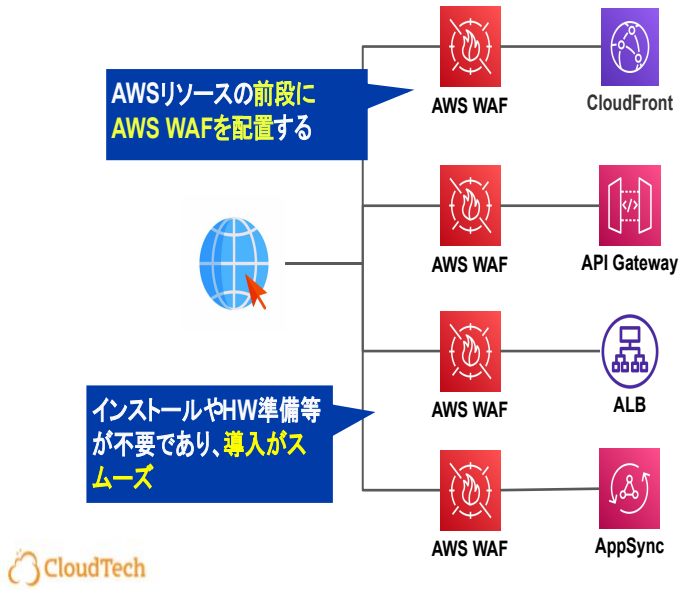
- Webアプリケーションに対する攻撃から保護するセキュリティソリューション
  - SQLインジェクション
  - クロスサイトスクプティング
  - DDoS攻撃　...etc



CloudTech

- 前提知識として、WAF（Web Application Firewall）とは
  - Webアプリケーションの脆弱性を突いた攻撃から守るためのセキュリティ対策ソリューションです。
    - 関連レッスンがありますので、詳細はご覧いただきたいのですが、
      - オンプレなどではファイアーウォールを通過したHTTP(S) リクエストをモニタリングし、
      - OSI参照モデルの7層(アプリケーション層)を防御し、
        - SQLインジェクション
        - クロスサイトスクリプティング
        - DDoS攻撃などの攻撃を防ぐために利用されます。

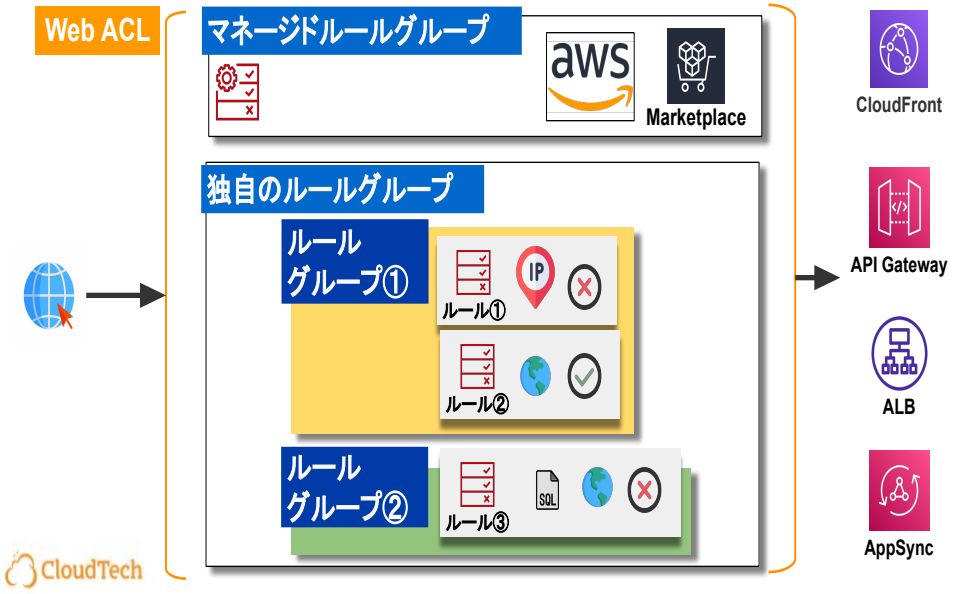
AWS WAFの配置



- AWS WAFがどのように働くのか構成図をもとに説明していきます。
  - インターネットからAWSリソースに通信がくる際に、WAFで待ち受けます。
    - WAFをCloudFrontの前面に配置し、CloudFrontで配信しているWebディストリビューションのコンテンツを保護をするような使い方です。
  - また、他にも保護対象の リソースとして
  - API Gatewayや
  - ALB
  - APPSyncなどがあります。

- AWS WAFはマネージドサービスですので、
  - ソフトウェアのインストールやハードウェアの準備は不要であり、導入がスムーズです。

AWS WAF（Web ACL）



- WAFの理解には、Web ACLが大変重要です。
  - ACL … Access Control List ですね。
  - インターネットから受信したアクセスをコントロールして、AWS リソースを保護するための、ルールの集合体です。
    - ルールには大きく
      - マネージドルールグループと
      - 独自のルールグループがあります。

    - 後ほど詳しく見ていきますが、ルールにはどんな基準値を設けるかのステートメントがあり、
      - 基準を満たした場合にブロックするなどのアクションがあります。
        - また、各ルールはルールグループ、と呼ばれる単位で

- ひとまとめにできます。
- では、まずはマネージドルールグループの中身を詳しく見ていきましょう。

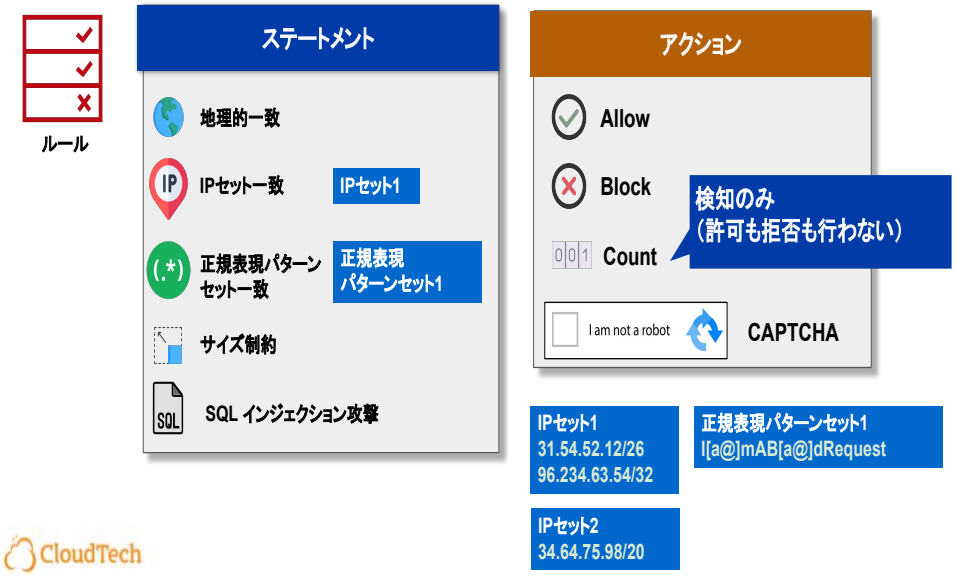
（1-Web ACLのスライド）では、続いては独自のルールグループについて、まずはこの、ルールの中身を詳しく見ていきましょう。
（2-Web ACLのスライド）さて、Web ACLの中身を詳しく見てきました。
全体像を把握するために、スライドでは複数のルールを組み入れていますが、実際の現場では、まずはマネージドルールをひとつ設定し、運用していくのが良いでしょう。
複数のルールを設定した場合、どのルールを優先させるか、優先度も設定できます。
こちら、概念としては非常にシンプルなので、参考記事のリンクを載せておきます。
さて、実は各ルールにはキャパシティという、ルールの複雑さを表す単位が存在します。
最後にこれを確認しましょう。

AWS WAF（マネージドルールグループ）

- マネージドルールについて
  - 設定画面を元に解説します。
    - WAFにはマネージドで素早く設定できるルールが用意されており、SQLインジェクションやクロスサイトスクリプティングの攻撃など、一般的な攻撃のパターンがルール化されています。
  - マネージドルールは新しい問題が出てくると自動的に更新されるため、アプリケーションの構築に集中できます。
    - 通常、セキュリティ関連のルール作成には専門知識や、管理の手間やコストが必要ですが、これを抑えることができます。

- マネージドルールには 2種類あります。
- AWSが提供するマネージドルール
    - こちらは使用開始時の初期料金などはありません。
    - 一般的な既知の攻撃手法の多くに対処できます。
        - （ CVE ）記載の脆弱性への対応、他
        - LinuxやWindows、OS 固有の脆弱性に対処するもの
        - WordPress などプラットフォーム固有の脆弱性に対処するものなど、多岐に渡ります。
- そして、AWS Marketplace の販売者が提供するマネージドルールがあります。
    - F5やFortinetなど、NW系ベンダーが提供するものもありますね。
        - より専門的なルールが存在します。
    - こちらを使用するには、ルールに応じた月額料金のサブスク料金が必要となります。

AWS WAF（ルール・ステートメント・アクション）



- ルールとは、攻撃してきたリクエストに、どう対処するのかを定義する設定です。
  - 各ルールには、リクエストを検査するステートメントと、
  - リクエストがその検査の条件を満たした場合に実行するアクション、例えば
    - 通信を許可するのか、
    - ブロックするのか（403を返します）

- ステートメントはさまざまあり、適切なものを選択します。例えば、
  - 地理的一致ステートメント
    - リクエストの送信元の国が、この国だったら …

      アクションをブロックする、など
    - 特定の国を基準とします。
  - IPセット一致ステートメントでは

- 特定のIPアドレスからのアクセスを拒否したいとか、許可したいとかいった場合に使用します。
    - なお、設定の際には、IPアドレスやIPアドレスのCIDRの範囲をあらかじめ「 IPセット」という設定項目で定義しておき、
    - ルール設定の際には「どの IPセットを使用するか？」を選択します。

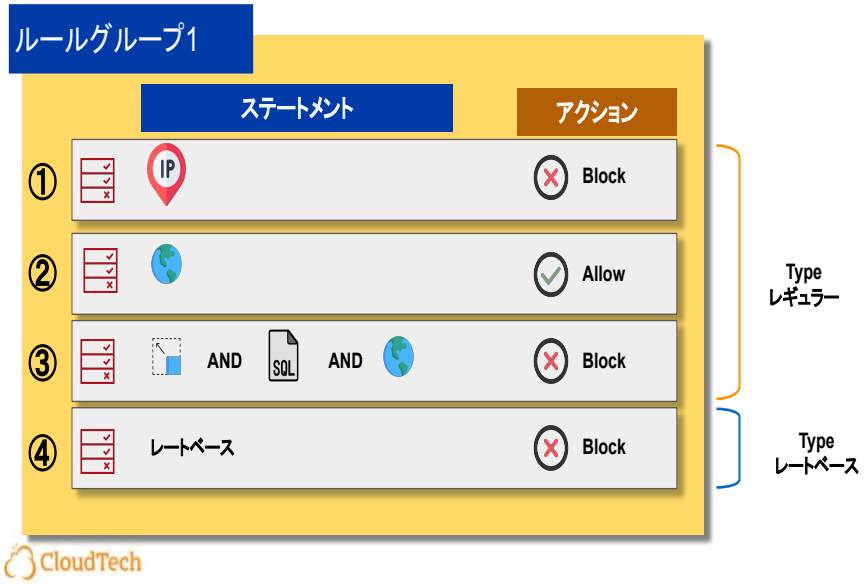
■ 続いて、正規表現パターンセット一致
- リクエストの一部に含まれる文字列が一致するか、または正規表現 で一致するかで判断します。
    - こちらも、設定の際には、どのような正規表現かをあらかじめ「正規表現パターンセット」という設定項目で定義しておき、
    - ルール設定の際には「どの正規表現パターンセットを使用するか？」を選択します。

■ 他、リクエストのサイズを基準にするサイズ制約ステートメントや、

■ 悪意のあるSQLコード（SQL インジェクション）が含まれている可能性があるか？
- などなど、これら目的に合った適切なステートメントを使用して、
    - リクエストのIPアドレスやHTTPヘッダー、HTTPのボディ、カスタムURIなどを対象に、
    - ステートメントで指定した条件で検査することができます。

- アクションについて、
    - 許可や拒否の他にも
        - カウントが選択できます。
            - これは、ルール一致時に検知はしますが「許可」も「拒否」も行わず、
            - 何のリクエストがステートメントにヒットしているのか、などを知ることができます。
            - 誤検知で正常なリクエストをブロックしてしまうのを防ぐのにも有用です。
        - CAPTCHAを設定もできます。
            - CAPTCHAとは、コンピュータと人間を判別するためのテストのことです。
            - よく、自動車の画像を選択してください、などログインの時にでてくるあれですね。

AWS WAF（ルールグループ）



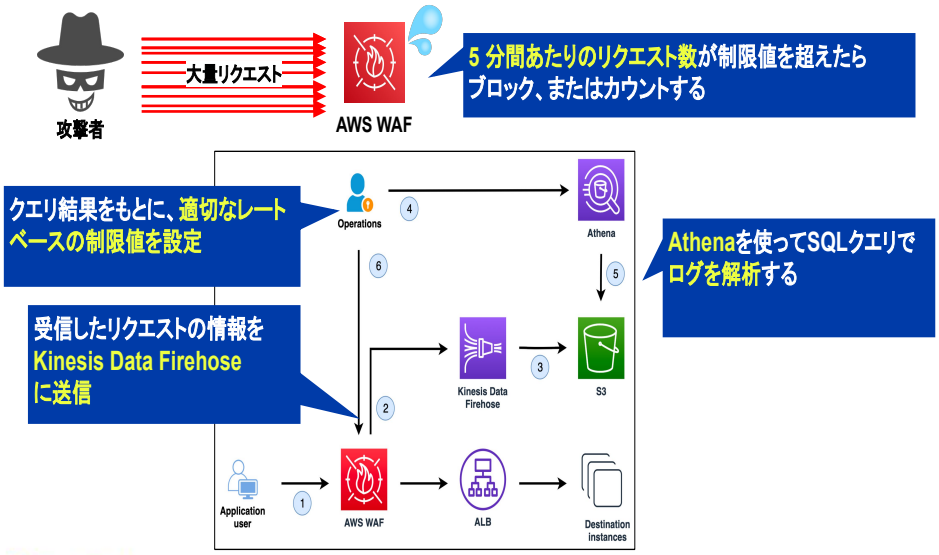
- 続いて、ルールグループについて
- ルールの設定方法は様々考えられました。例えば、
  - このIPアドレスはブロックする、
  - この国からのリクエストは許可するなど、
    - このように、単発のステートメントで設定もできますし、
      - ステートメントを複数使用して、AND条件やOR条件、NOT条件で組み合わせることも可能です。

- これら複数のルールをひとまとめにして設定しておくことができます。
  - それが、ルールグループです。
    - 複数のルールをまとめて管理する際の単位のことですね。任意の名前をつけて保存しておけます。

なお、ルールには2タイプあり、

- これまで見てきたのはレギュラールールというタイプで、もうひとつが、、
- レートベースのタイプです。
    - これを詳しく見ていきましょう。

AWS WAF（レートベースのルール）



CloudTech https://aws.amazon.com/jp/blogs/security/three-most-important-aws-waf-rate-based-rules/

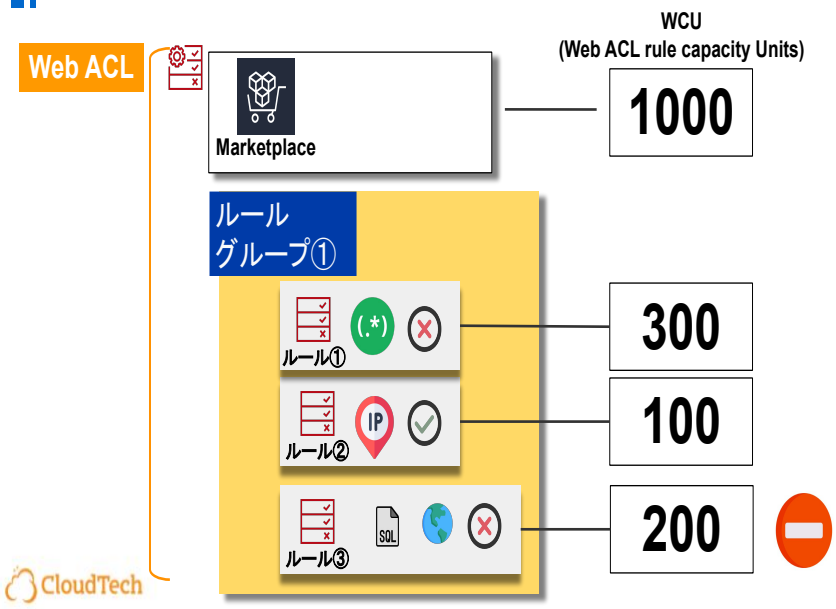
- レートベースのルールは、AWS WAFが送信元 IP アドレスからのリクエストのレート追跡、（要はどの程度リクエストがあったのか数をカウント）し、
  - 送信されたリクエストが、設定した制限値を超えると、そのIP はブロックするなどのアクションを実行できます。
    - 即ブロックといきたいところですが、ひとまずカウントで様子見、という手もありますね。
  - 制限は、5 分間あたりのリクエスト数として設定します。
    - レートベースのルールを使用すると、過剰なリクエストを送信している IP アドレスからのリクエストを一時的にブロックできます。

レートベースルールの閾値は 100～2千万まで設定ができます。

では、閾値はどの程度設定するのが良いのでしょうか？
こちらはAWS公式ブログからの引用です。
レートベースを使った閾値を決定していく流れを見てみましょう。

ユーザーがアプリケーションに対してリクエストを行う
AWS WAFは受信したリクエストの情報を取得して Kinesis Data Firehoseに送信する
Kinesis Data FirehoseはログをS3バケットに保存する
運用チームはAthenaを使ってSQLクエリでログを解析する
AthenaはS3バケット内のログにクエリを発行し、クエリ結果を表示する
運用チームはクエリ結果をもとに、適切な AWS WAFのレートベースルールを決定する。
参考にしてみてください。

AWS WAF（Web ACLのWCU制限について）



- Web ACL のキャパシティについて
  - WAFには、ルールごとに（WCUs: Web ACL rule capacity Units）が設定されています。
    - 通常、Web ACLを設定する場合は、Web ACLごとに1500 WCU 以内に納まるようにルールを選定する必要があります。
      - 単純なルールはWCUが少なく、複雑なルールは多くの WCUが設定されています。
      - マネージドルールは基本的にWCUを多く消費する特徴があります。
    - 要は、なんでもかんでも、ルールを追加していってしまうと、WCUが1500をオーバーすることになり、設定できません。
      - この例では、4つめのルールで1500を超え、1600に

        - なってしまうので、作成することはできません。
    - この1500以内の制限は、AWSへのクォーターのリクエストで引き上げることができますが、
    - ほとんどのユースケースでは 1500以内で十分となります。
        - このWCUの制限にも気をつけてWeb ACLを設定していきましょう。

■関連レッスン
WAFとは / IDS,IPS / WAFとFWの防御レイヤーの違い【 6:28】
https://kws-cloud-tech.com/topic/waf%e3%81%a8%e3%81%af-idsips-waf%e3%81%a8fw%e3%81%ae%e9%98%b2%e5%be%a1%e3%83%ac%e3%82%a4%e3%83%a4%e3%83%bc%e3%81%ae%e9%81%95%e3%81%84%e3%80%90628%e3%80%91

公式ドキュメント
・Web ACLのルールの優先度について
ウェブ ACL でのルールおよびルールグループの処理順序
https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/web-acl-processing-order.html

・ルールステートメントリスト
https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/waf-rule-statements-list.html

公式ブログ（英語）
・レートベースのルールの運用について

The three most important AWS WAF rate-based rules
https://aws.amazon.com/jp/blogs/security/three-most-important-aws-waf-rate-based-rules/