

cloudbric

Cloudbric Rule Set for AWS WAF

設定ガイド v1.3 2023.08

FOR ENDUSER(PUBLIC)

変更履歴

更新日	担当者	更新内容	ページ	備考
2023.05	仲田慶也	ラベルを使用したルールの例外処理に関する内容を追加	14, 16, 21, 22	v1.1
2023.06	仲田慶也	Tor IP Detection Rule Set の紹介、Rule Set のバージョン設定、アップデートの通知設定及び削除関連の内容追加	4, 5, 10~11, 12~14, 15, 19~20	v1.2
2023.08	仲田慶也	Bot Protection Rule Set に関する紹介内容を追加	5	v1.3

目次

1. Overview	4
- 1.1 Cloudbric Rule Set とは.....	4
- 1.2 Cloudbric Rule Set のタイプ	5
2. Cloudbric Rule Set 設定方法.....	5
- 2.1 Cloudbric Rule Set サブスクリプション	5
- 2.2 Cloudbric Rule Set の適用.....	7
- 2.3 Cloudbric Rule Set バージョンの選択.....	11
- 2.4 Cloudbric Rule Set のアップデート通知	13
3. Cloudbric Rule Set 解除方法.....	16
- 3.1 Cloudbric Rule Set サブスクライブ解除	16
- 3.2 Cloudbric Rule Set の削除.....	18
- 3.3 Cloudbric Rule Set アップデート通知の削除	20
4. Cloudbric Rule Set 例外処理.....	22
- 4.1 Rule Action 「Count」の設定	22
- 4.2 Label 基盤の例外処理の Rule 追加.....	25
5. 付録.....	29
- 5.1 よくある質問 (FAQ)	29
- 5.2 Cloudbric OWASP Top 10 Rule.....	33

1. Overview

本文書はクラウドブリック株式会社より AWS Marketplace で提供する AWS WAF 用 Managed Rule Groups である「Cloudbric Rule Set」をサブスクライブし Web ACL に適用する際の設定方法につき説明するため作成されました。

1.1 Cloudbric Rule Set とは

Cloudbric Rule Set とは、クラウドブリックが開発した AWS WAF 用 Managed Rules です。クラウドブリックはアマゾン・ウェブ・サービス（AWS : Amazon Web Service）の厳格な技術的評価を通過した韓国初でありながら唯一の AWS WAF Ready Program ローンチパートナーでもあります。また、Cloudbric Rule Set は 20 年以上の豊富なセキュリティ経験と蓄積されたノウハウにて開発され、安定したセキュリティ水準を維持するために持続的な更新及び管理を行っています。

AWS WAF Managed Rule とは？

AWS Marketplace 販売者が作成および管理する、事前に構成された AWS 用セキュリティ Rule Set です。AWS WAF ユーザが自らルールを作成する必要はなく AWS Marketplace にてサブスクリプション型ですぐ使用でき、一般的な脅威から Web アプリケーションまたは、API を素早く保護することができます。

1.2 Cloudbric Rule Set のタイプ

Rule set	説明
OWASP Top 10 Rule Set 購読ページへ	アジアパシフィック(APAC)マーケットシェア No.1 の Web アプリケーション ファイアウォール 検知エンジンを搭載した Cloudbric WAF+のインテリジェンス検知モジュールを実装し、数百万のログから異常パターンを正確に感知することで OWASP Top 10 SQL Injection, Cross Site Scripting(XSS) 等の脆弱性から保護します。
Malicious IP Reputation Rule Set 購読ページへ	Cloudbric Labs のブロックチェーン基盤脅威インテリジェンスは、95 ヶ国 700,000 サイトより収集される脅威情報を活し、多様な脅威を識別する時間を短縮させ、また、危険度が高い IP を事前に遮断します。
Tor IP Detection Rule Set 購読ページへ	分散型のリレーネットワークを通じ、インターネットトラフィックをルーティングし、トラフィックの出どころを匿名化する Tor ブラウザが、非合法的な目的で使用される場合、Web サイト、Web アプリケーションに対する脅威を減らすことができます。
Bot Protection Rule Set 購読ページへ	悪意ある反復作業や特定の作業を実行する悪性 Bot のトラフィックを検知及び遮断し、アカウントの乗っ取り（ATO、Account Takeover）、スクラッピング、アプリケーション層への DDoS 攻撃など広範囲にわたり悪性 Bot による攻撃を防衛し、被害を予防します。

2. Cloudbric Rule Set 設定方法

AWS WAF で Cloudbric Rule Set を設定するためには、AWS Marketplace から Cloudbric Rule Set をサブスクライブして下さい。サブスクライブしてから AWS WAF コンソールにて Web ACL に Cloudbric Rule Set を適用することが可能になります。また Cloudbric Rule Set のバージョン選択と Amazon SNS（Simple Notification Service）を通じたアップデート通知を設定することができます。

2.1 Cloudbric Rule Set サブスクリプション

• Step 1

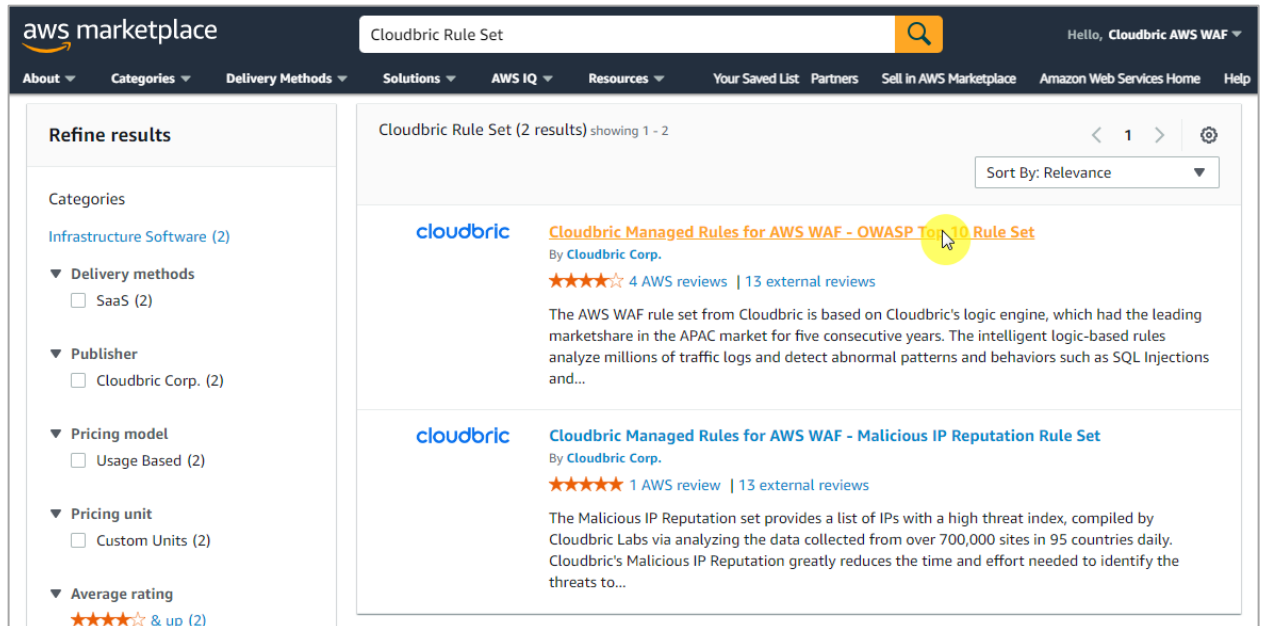
AWS Marketplace にアクセスした後 AWS アカウントを入力しログインします。

※ AWS Marketplace : <https://aws.amazon.com/marketplace/>



- Step 2

検索ボックスに「Cloudbric Rule Set」を検索し、サブスクリプションが必要な Rule Set 名をクリックします。



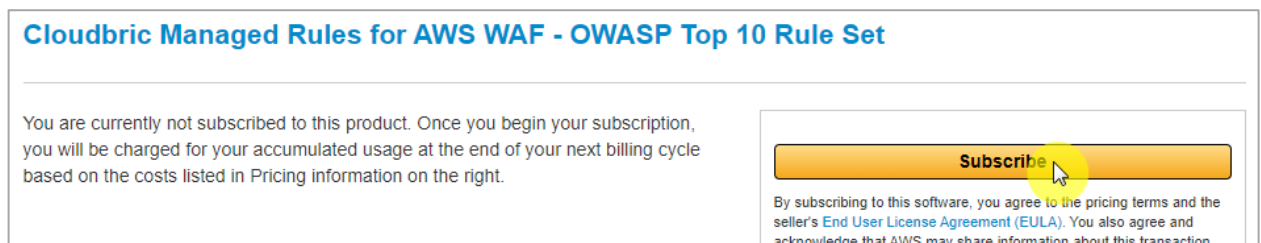
- Step 3

選択した Rule Set の詳細内容を確認した後、「Continue to Subscribe」をクリックします。



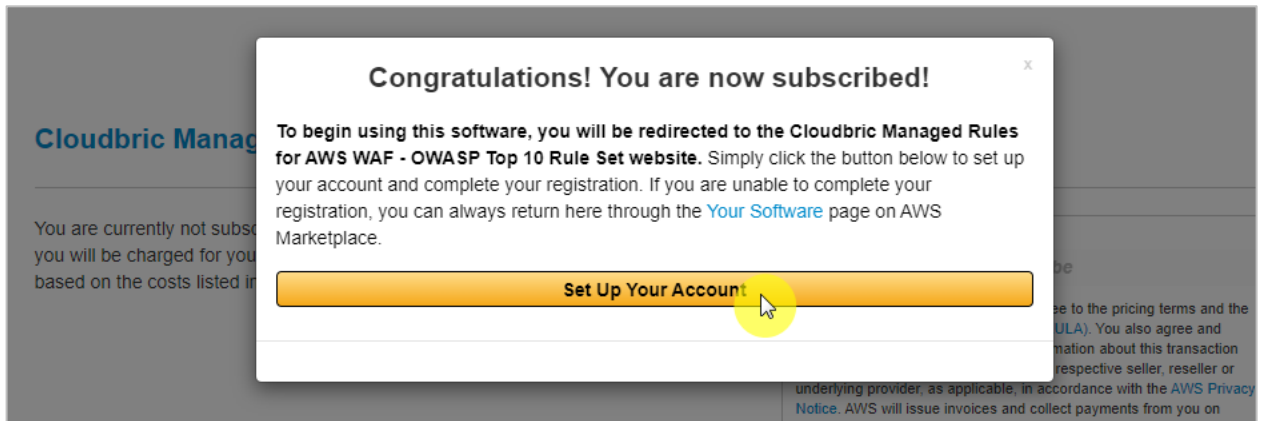
- Step 4

サブスクリプションの約款と価格情報を確認した後、「Subscribe」をクリックします。



- Step 5

Cloudbric Rule Set のサブスクリプションが完了しました。Cloudbric Rule Set 利用のために「**Set Up Your Account**」をクリックし AWS WAF コンソールに移動します。



cloudbric

2.2 Cloudbric Rule Set の適用

- Step 1

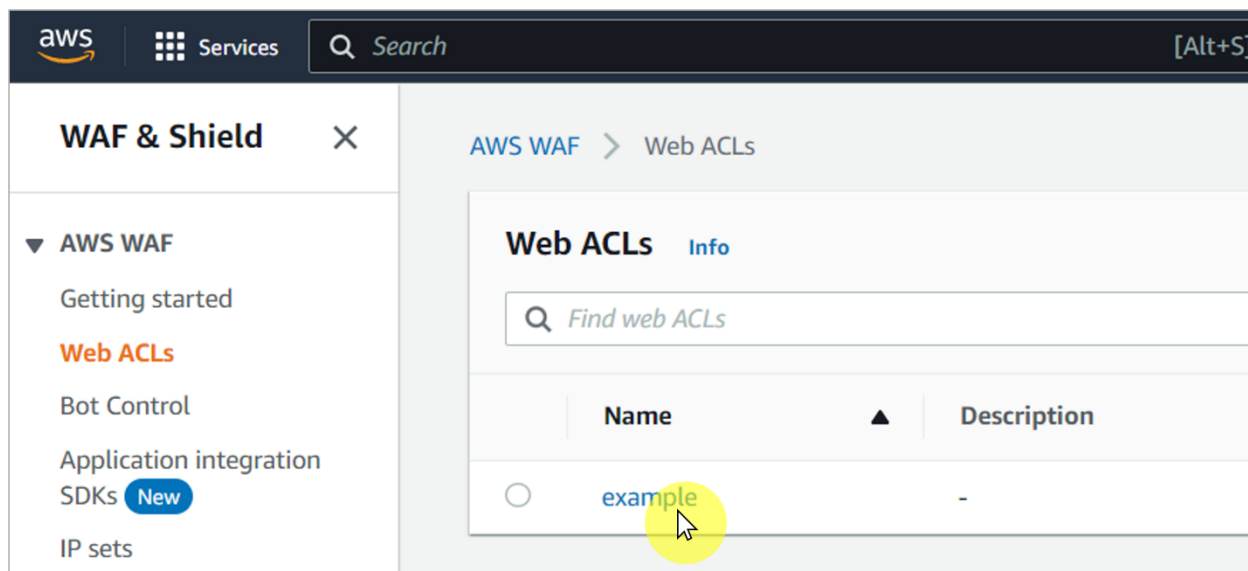
AWS WAF コンソールにアクセスします。

※ AWS WAF コンソール : <https://console.aws.amazon.com/wafv2/>



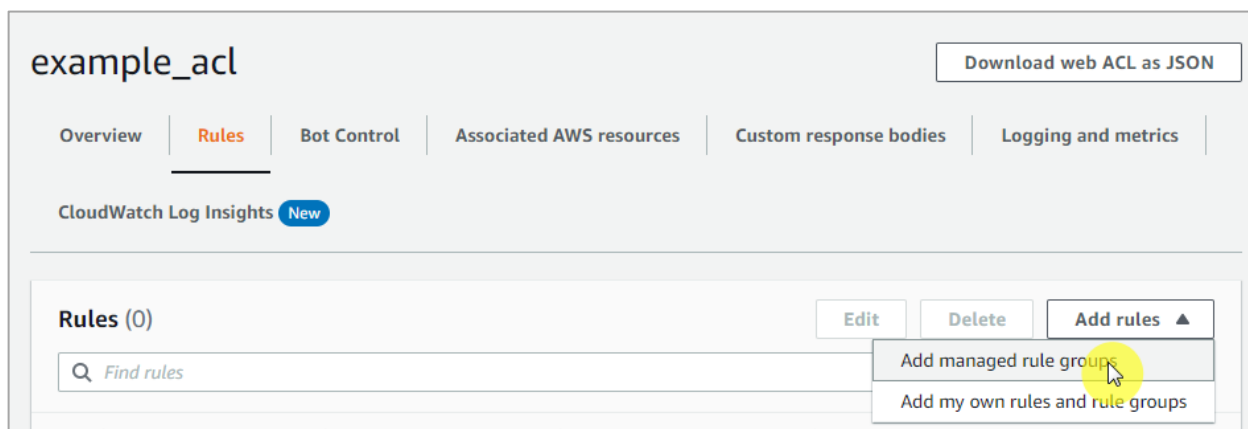
- Step 2

Web ACL メニューにて Cloudbric Rule Set を適用する Web ACL 名をクリックします。



- Step 3

Web ACL の「Rules」メニューに移動した後、「Add rules」から「Add managed rule groups」を選択します。



- Step 4

「Cloudbric Corp」にてサブスクリプションした Cloudbric Rule Set を有効化し、「Add rules」をクリックします。

※ Rule Set テストを行うためには「Edit」をクリックし Rule の Action を count として再定義してください。

Add managed rule groups

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

▶ AWS managed rule groups

▼ Cloudbric Corp. managed rule groups

Name	Capacity	Action
Malicious IP Reputation Rule Set Cloudbric Labs provides a comprehensive list of Malicious IP Reputation based on threat intelligence gathered from over 700,000 sites in 95 countries, reducing the amount of time required for identifying and processing, and in turn, helping minimizing the damages caused by these threats.	6	<input checked="" type="radio"/> Add to web ACL
OWASP Top 10 Rule Set Cloudbric utilizes a logic-based intelligent WAF engine that was voted as Asia Pacific's no.1 for 5 consecutive years. Automated updates ensures it protects against the OWASP Top 10 vulnerabilities and new threats.	1400	<input type="radio"/> Add to web ACL <input type="button" value="Edit"/>

Cancel

- Step 5

Cloudbric Rule Set 2 つを全て有効化する場合、**Malicious IP Reputation Rule Set** が優先的に適用されるようにルール of 優先順位を設定した後、「**Save**」をクリックし、ルールの適用を完了します。

Set rule priority [Info](#)

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

	Name	Capacity	Action
<input checked="" type="radio"/>	CloudbricCorp-Cloudbric_MaliciousIPReputationRuleSet	6	Use rule actions
<input type="radio"/>	CloudbricCorp-Cloudbric_OWASPTop10RuleSet	1400	Use rule actions

Cancel

- Step 6

Web ACL の「Rules」メニューより **Cloudbric Rule Set** が適用されていることを確認します。

Success

You successfully updated the web ACL example_acl.

AWS WAF > Web ACLs > example_acl

example_acl

Download web ACL as JSON

Overview Rules Bot Control Associated AWS resources Custom response bodies Logging and metrics CloudWatch Log Insights New

Rules (2)

Find rules

Edit Delete Add rules

	Name	Action	Priority	Custom response
<input type="checkbox"/>	CloudbricCorp-Cloudbric_MaliciousIPReputationRuleSet	Use rule actions	0	-
<input type="checkbox"/>	CloudbricCorp-Cloudbric_OWASPTop10RuleSet	Use rule actions	1	-

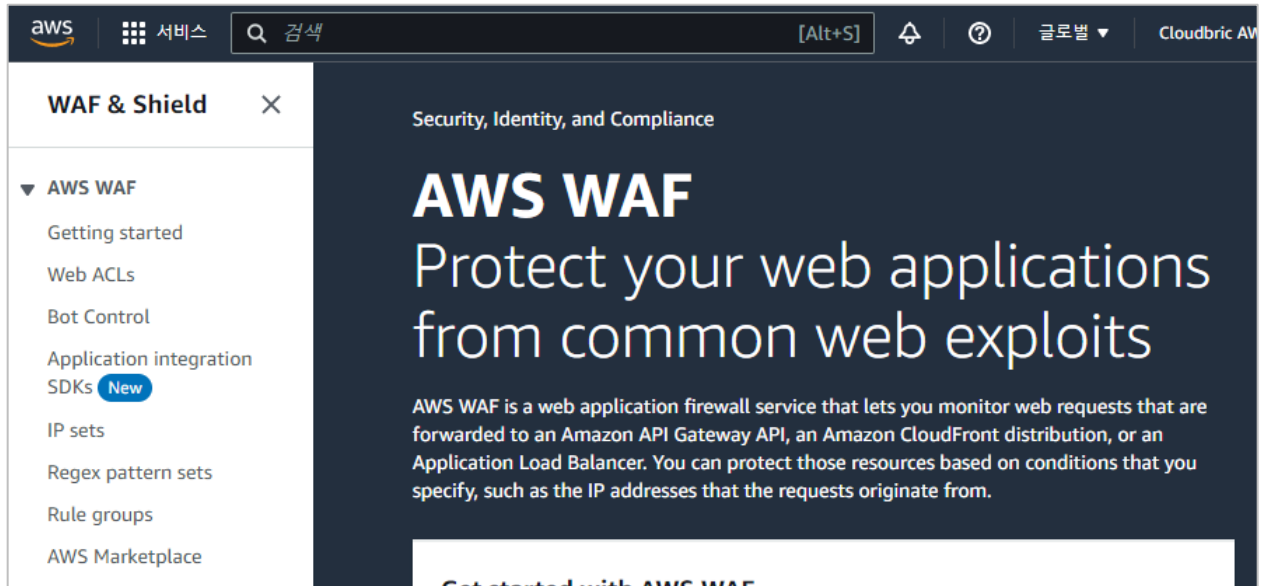
cloudbric

2.3 Cloudbric Rule Set バージョンの選択

- Step 1

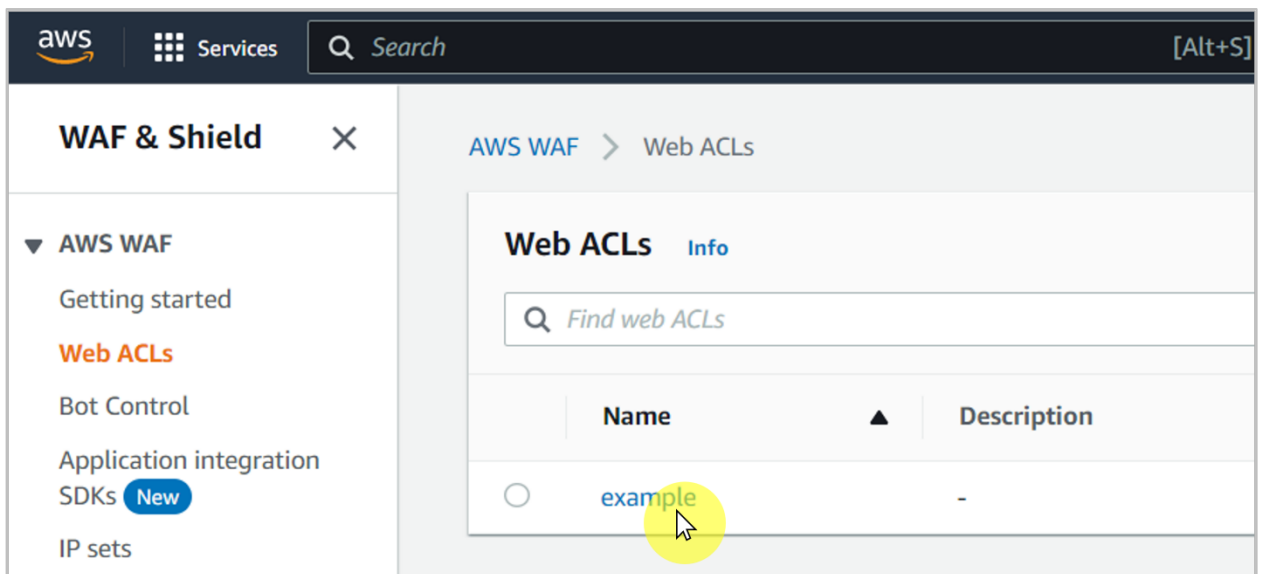
AWS WAF コンソールにアクセスします。

※ AWS WAF コンソール : <https://console.aws.amazon.com/wafv2/>



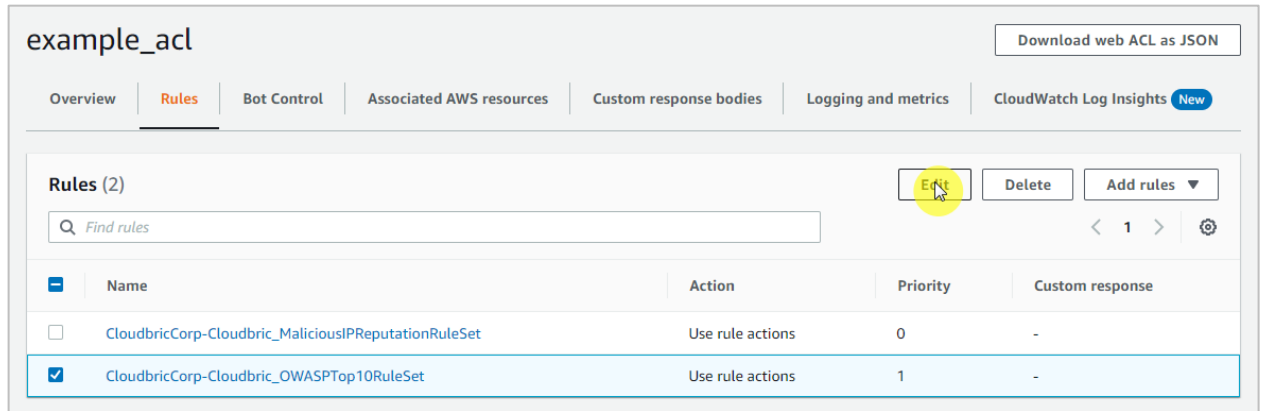
- Step 2

Web ACL メニューにて Cloudbric Rule Set のバージョンを選択する Web ACL 名をクリックします。



- Step 3

当該の Web ACL の「Rule」タブに移動し、Cloudbric Rule Set にチェックをし、「Edit」ボタンをクリックします。



example_acl

Download web ACL as JSON

Overview Rules Bot Control Associated AWS resources Custom response bodies Logging and metrics CloudWatch Log Insights New

Rules (2)

Find rules

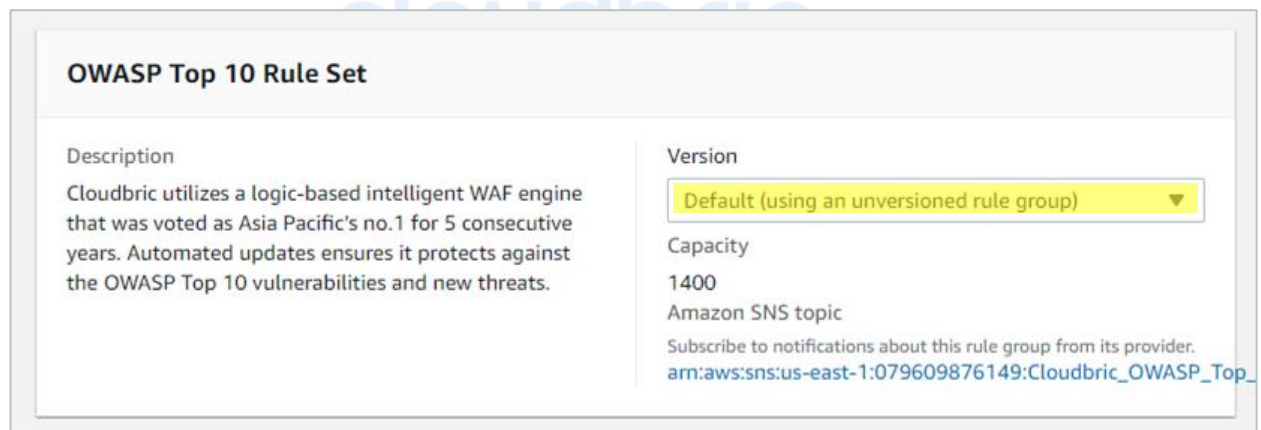
Edit Delete Add rules ▼

	Name	Action	Priority	Custom response
<input type="checkbox"/>	CloudbricCorp-Cloudbric_MaliciousIPReputationRuleSet	Use rule actions	0	-
<input checked="" type="checkbox"/>	CloudbricCorp-Cloudbric_OWASPTop10RuleSet	Use rule actions	1	-

※ 現在バージョン設定機能は OWASP Top 10 に限り、提供しています。

- Step 4

利用される Cloudbric Rule Set のバージョンを選択後、「Save rule」を選択し、設定を完了します。



OWASP Top 10 Rule Set

Description

Cloudbric utilizes a logic-based intelligent WAF engine that was voted as Asia Pacific's no.1 for 5 consecutive years. Automated updates ensures it protects against the OWASP Top 10 vulnerabilities and new threats.

Version

Default (using an unversioned rule group) ▼

Capacity

1400

Amazon SNS topic

Subscribe to notifications about this rule group from its provider.

arn:aws:sns:us-east-1:079609876149:Cloudbric_OWASP_Top_10

※ 現在は Default（最新バージョン）のみ提供しており、今後 Rule のアップデートにより従来のバージョンをご提供する予定です。

2.4 Cloudbric Rule Set のアップデート通知

- Step 1

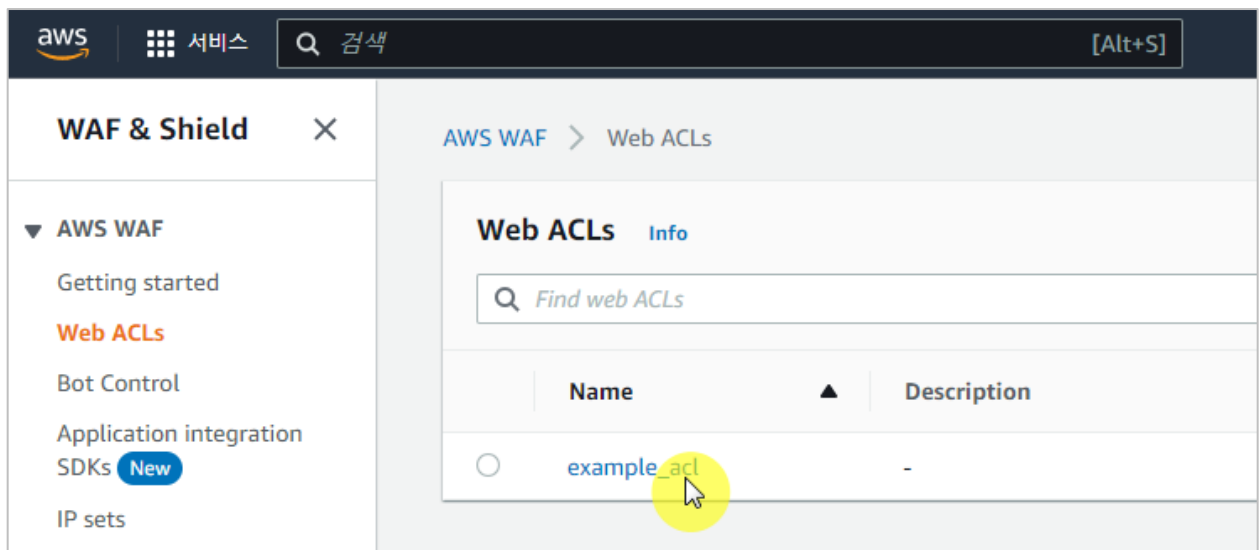
AWS WAF コンソールにアクセスします。

※ AWS WAF コンソール : <https://console.aws.amazon.com/wafv2/>



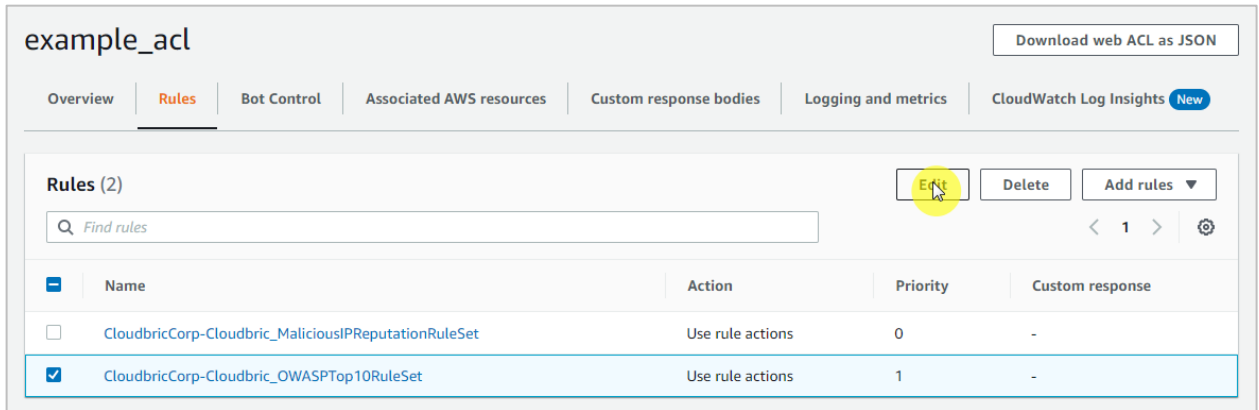
- Step 2

Web ACL メニューにて Cloudbric Rule Set のバージョンを選択する Web ACL 名をクリックします。



- Step 3

当該の Web ACL の「Rule」タブに移動し、Cloudbric Rule Set にチェックをし、「Edit」ボタンをクリックします。

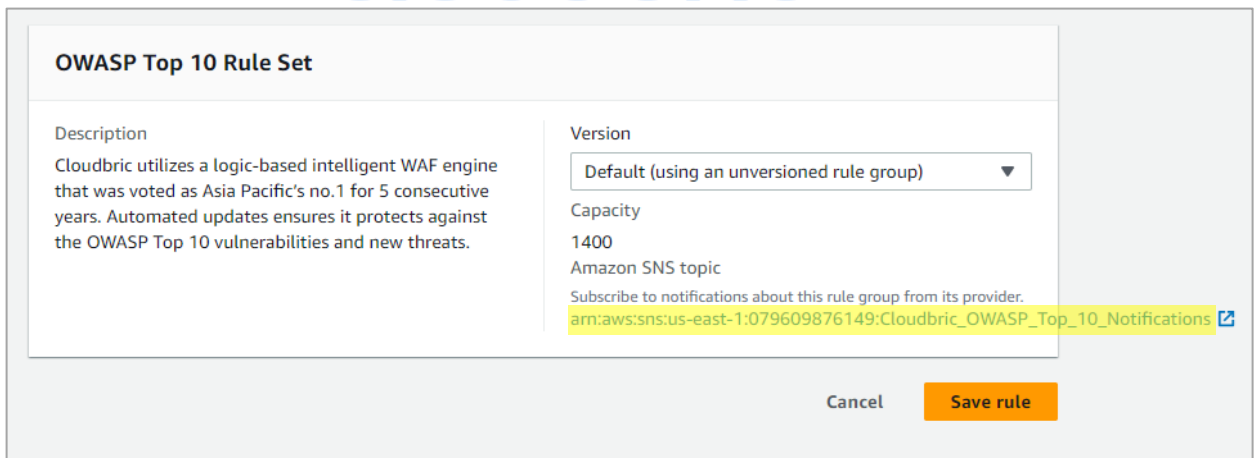


The screenshot shows the AWS WAF console interface for a Web ACL named 'example_acl'. The 'Rules' tab is selected, displaying a list of rules. The 'Edit' button is highlighted with a yellow circle.

Name	Action	Priority	Custom response
CloudbricCorp-Cloudbric_MaliciousIPReputationRuleSet	Use rule actions	0	-
CloudbricCorp-Cloudbric_OWASPTop10RuleSet	Use rule actions	1	-

- Step 4

Cloudbric Rule Set の Amazon SNS (Simple Notification Service) topic ARN (Amazon Resource Name) をドラッグしコピーした後、Amazon SNS topic ARN を選択し、Amazon SNS のアップデート通知の登録ページに移動します。



The screenshot shows the 'OWASP Top 10 Rule Set' configuration page. The Amazon SNS topic ARN is highlighted in yellow.

OWASP Top 10 Rule Set

Description
Cloudbric utilizes a logic-based intelligent WAF engine that was voted as Asia Pacific's no.1 for 5 consecutive years. Automated updates ensures it protects against the OWASP Top 10 vulnerabilities and new threats.

Version
Default (using an unversioned rule group)

Capacity
1400

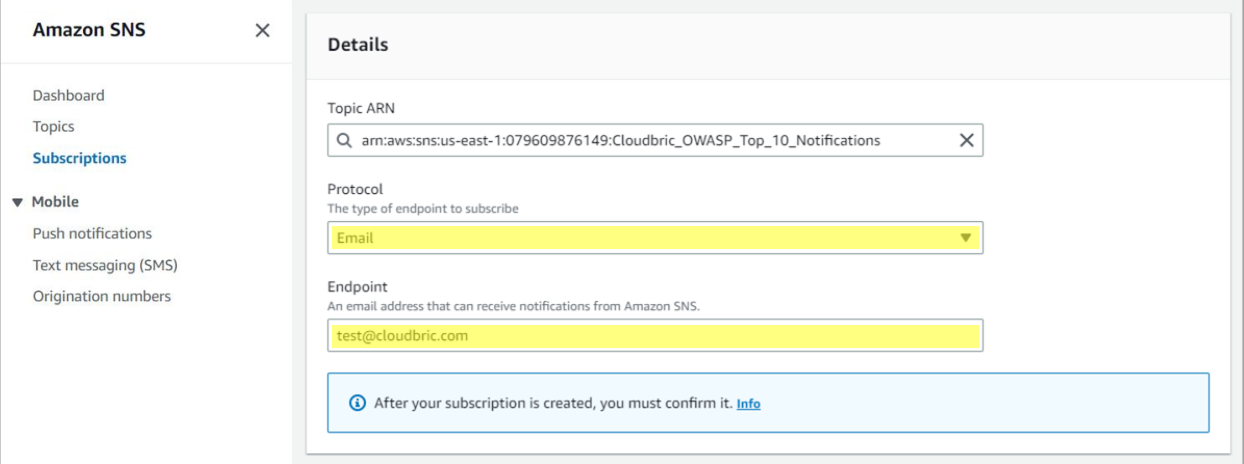
Amazon SNS topic
Subscribe to notifications about this rule group from its provider.
arn:aws:sns:us-east-1:079609876149:Cloudbric_OWASP_Top_10_Notifications

Buttons: Cancel, Save rule

- **Step 5**

Cloudbric Rule Set のアップデート通知を受け取るための Protocol と Endpoint を入力します。

- Topic ARN : コピーした Cloudbric Rule Set の Amazon SNS topic ARN を入力
- Protocol : Email を選択
- Endpoint : アップデート通知を受信されるメールアドレスを入力

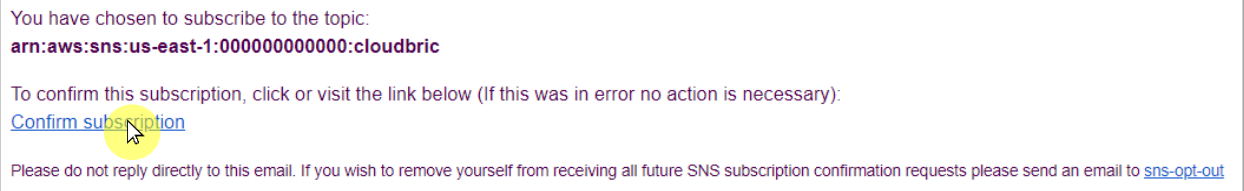


The screenshot shows the Amazon SNS console interface. On the left is a navigation menu with 'Dashboard', 'Topics', 'Subscriptions', and a 'Mobile' section containing 'Push notifications', 'Text messaging (SMS)', and 'Origination numbers'. The main area is titled 'Details' and contains three input fields: 'Topic ARN' with the value 'arn:aws:sns:us-east-1:079609876149:Cloudbric_OWASP_Top_10_Notifications', 'Protocol' set to 'Email', and 'Endpoint' with the value 'test@cloudbric.com'. A blue information box at the bottom states: 'After your subscription is created, you must confirm it. Info'.

※ Email 以外の Protocol にてアップデートを受け取る場合には、設定した Protocol に合う Endpoint を入力してください。

- **Step 6**

入力したメールアドレスに転送された AWS の認証メールにて「**Confirm subscription**」を選択し、アップデート通知の設定を完了します。



The screenshot shows an email confirmation message from AWS. It states: 'You have chosen to subscribe to the topic: arn:aws:sns:us-east-1:000000000000:cloudbric'. Below this, it says: 'To confirm this subscription, click or visit the link below (If this was in error no action is necessary): Confirm subscription'. The link 'Confirm subscription' is highlighted with a yellow circle and a mouse cursor. At the bottom, it says: 'Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to sns-opt-out'.

3. Cloudbric Rule Set 解除方法

Cloudbric Rule Set の利用を中止し Rule Set のサブスクリプションを解約するためには、AWS Marketplace のサブスクリプション取り消しと共に AWS WAF コンソールの全ての Web ACL から Cloudbric Rule Set を削除する必要があります。また Cloudbric Rule Set のアップデート通知を受け取られている場合、通知に対する課金が発生しないよう Amazon SNS (Simple Notification Service) にて Cloudbric Rule Set のアップデート通知を削除する必要があります。

※ サブスクリプションのみ取り消し Web ACL に適用した Cloudbric Rule Set が残っている場合、課金が続きます。

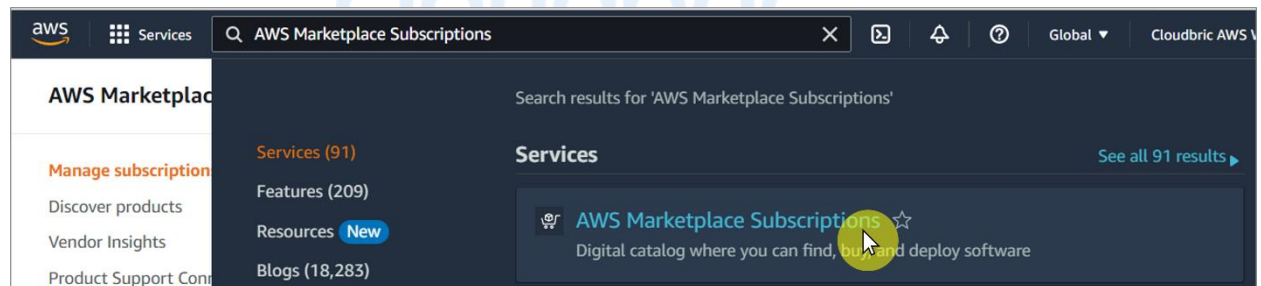
※ Amazon SNS (Simple Notification Service) にて Cloudbric Rule Set のアップデート通知を削除されない場合、通知設定に対する費用請求が発生する場合があります。

3.1 Cloudbric Rule Set サブスクリプション解除

- Step 1

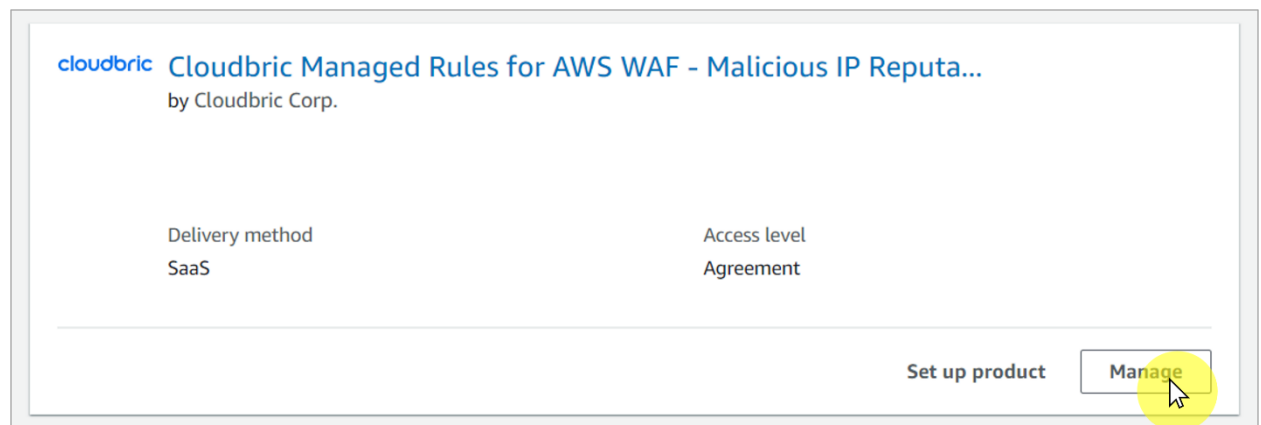
AWS Marketplace のサブスクリプション管理コンソールにアクセスします。

※ AWS WAF コンソール : <https://console.aws.amazon.com/marketplace/home#/subscriptions>



- Step 2

「manage」メニューにてサブスクリプションを解除する Cloudbric Rule Set の「manage」をクリックします。



- Step 3

「Agreement」の右側の「Actions」にて「Cancel subscription」を選択します。

Summary

Product	Delivery method	Product ID
Cloudbric Managed Rules for AWS WAF - Malicious IP Reputation Rule Set	SaaS	53cd6a3b-5461-413f-857e-058aef62c219

Agreement

Seller	Access level
Cloudbric Corp. [link]	Agreement

Product

- Set up product
- Usage instructions
- Write review

Subscription

- View terms
- Cancel subscription

Actions

- Step 4

データを復元できないことを確認し、チェックボックスにチェックを入れた後、「Yes, cancel subscription」を選択します。

Your AWS Marketplace subscriptions are now available as license entitlements in AWS License Manager. You will be able to manage these entitlements on this page. To enable this feature, go to the AWS License Manager Console.

Cancel subscription

Are you sure that you want to cancel your subscription to **Cloudbric Managed Rules for AWS WAF - Malicious IP Reputation Rule Set**? Canceling your subscription means that you lose access to the software.

Warning: All resources and data related to this subscription **will be deleted**. Once deleted, this data **cannot be recovered**.

☒ I understand that canceling my subscription will delete all Cloudbric Managed Rules for AWS WAF - Malicious IP Reputation Rule Set resources and data, and this data cannot be recovered.

No, don't cancel **Yes, cancel subscription**

3.2 Cloudbric Rule Set の削除

- Step 1

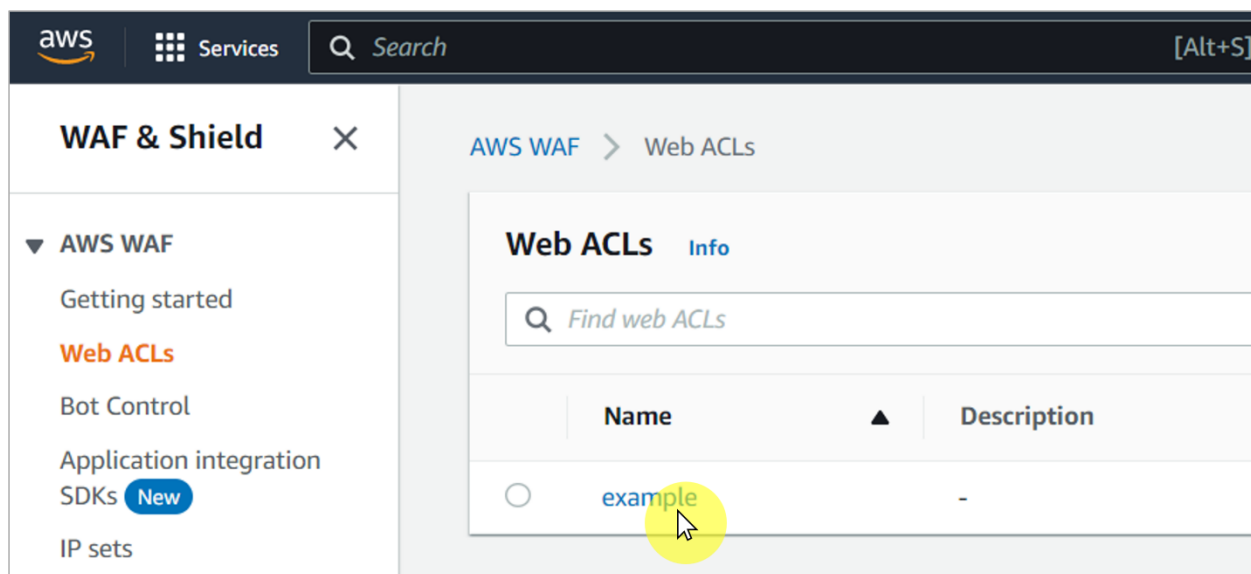
AWS WAF コンソールにアクセスします。

※ AWS WAF コンソール : <https://console.aws.amazon.com/wafv2/>



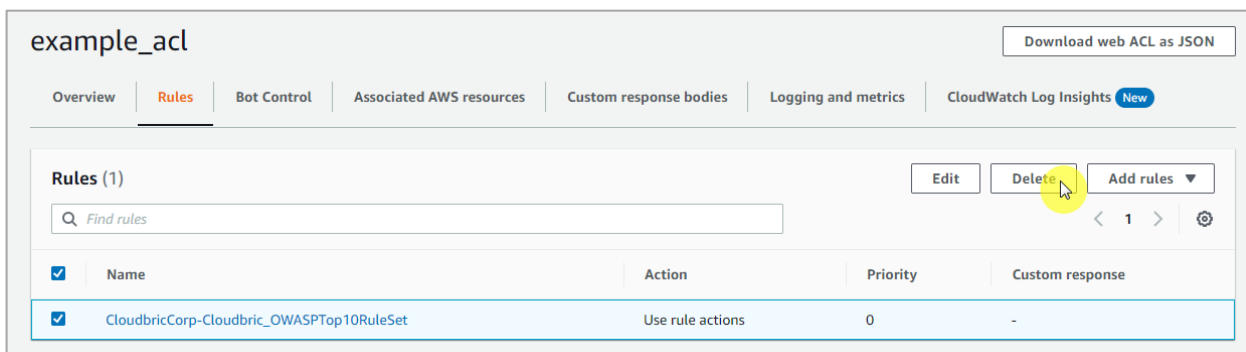
- Step 2

Web ACL メニューにて Cloudbric Rule Set を削除する Web ACL を選択します。



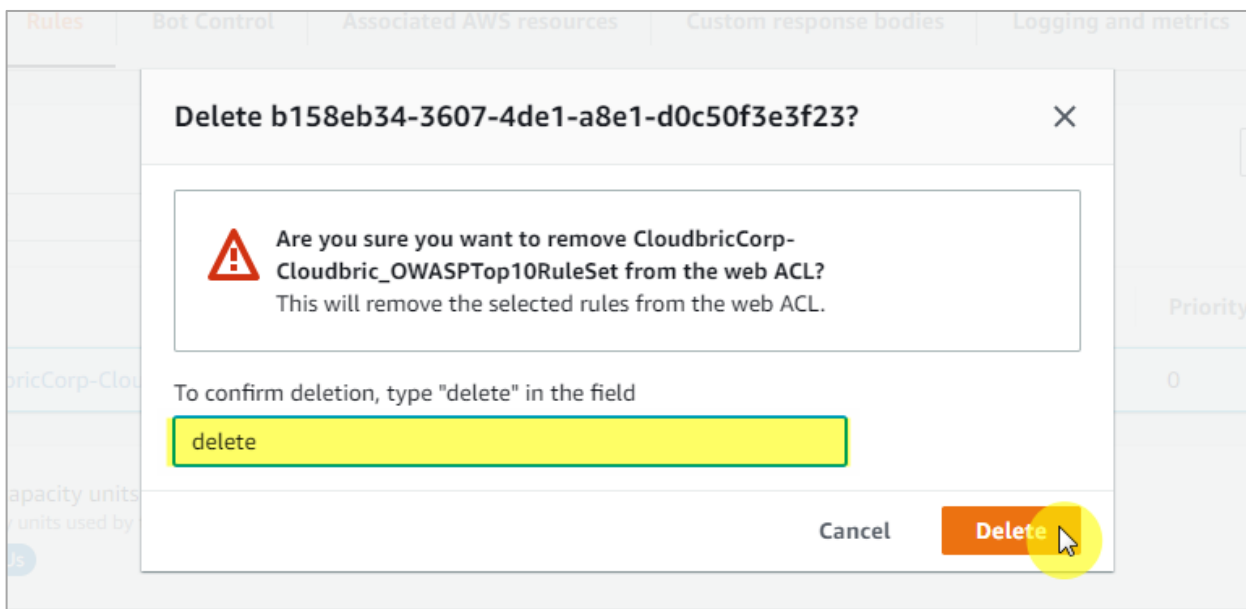
- Step 3

「Rules」タブに移動し、削除する Cloudbric Rule Set にチェックを入れ「Delete」をクリックします。



- Step 4

delete 文字を入力し、「Delete」をクリックし削除します。

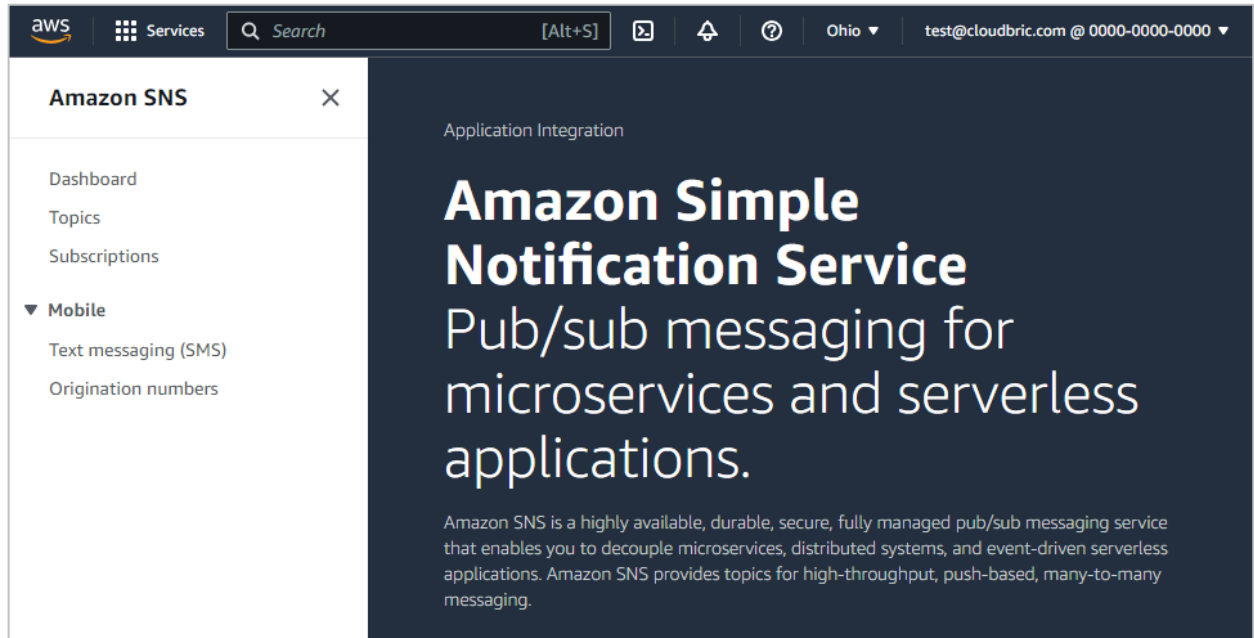


3.3 Cloudbric Rule Set アップデート通知の削除

- Step 1

Amazon SNS (Simple Notification Service) コンソールにアクセスします。

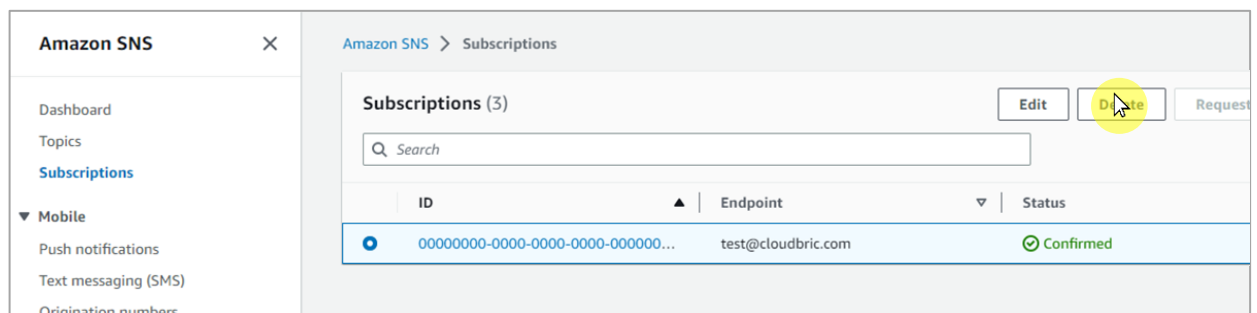
※ Amazon SNS (Simple Notification Service) コンソール : <https://console.aws.amazon.com/sns/home>



- Step 2

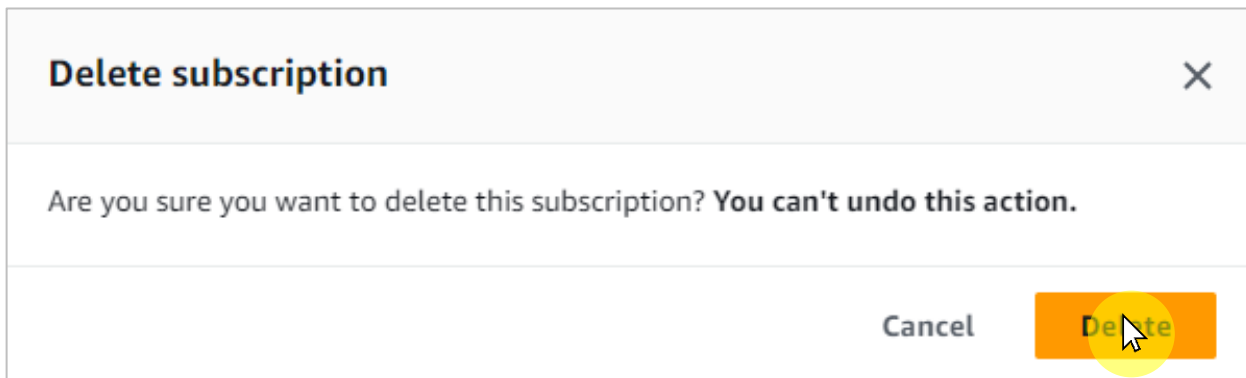
Subscriptions メニューにて Cloudbric Rule Set のアップデート通知を受け取られている ID を選択後、

「Delete」を選択します。



- **Step 3**

アップデート通知に関する削除確認のウィンドウが表示されたら「**Delete**」を選択し、アップデート通知の削除を完了します。



cloudbric

4. Cloudbric Rule Set 例外処理

Cloudbric Rule Set において正常なリクエストをブロックする誤検知が発生した場合、誤検知が発生した特定の Rule の Action を「Count」にて再定義し、ブロックしないように例外処理をする必要があります。しかし、それにより悪意あるリクエストまで許可されてしまう恐れがあります。Rule 例外処理前と同様に、機能を最大限維持し、誤検知が発生した特定のパターンのみ例外処理するためには、Label 基盤のユーザ定義の Rule Set を追加し、例外処理ポリシーを再定義する必要があります。

※ Cloudbric OWASP Top10 の Rule Set のすべての Rule には Label が設定されています。

※ IP 基盤の Cloudbric Rule Set は IP アドレスリストの動的な特性により別途 Label が設定されていません。例外処理が必要な IP がある場合、当該の IP を許可している Rule を生成してください。

4.1 Rule Action 「Count」の設定

- Step 1

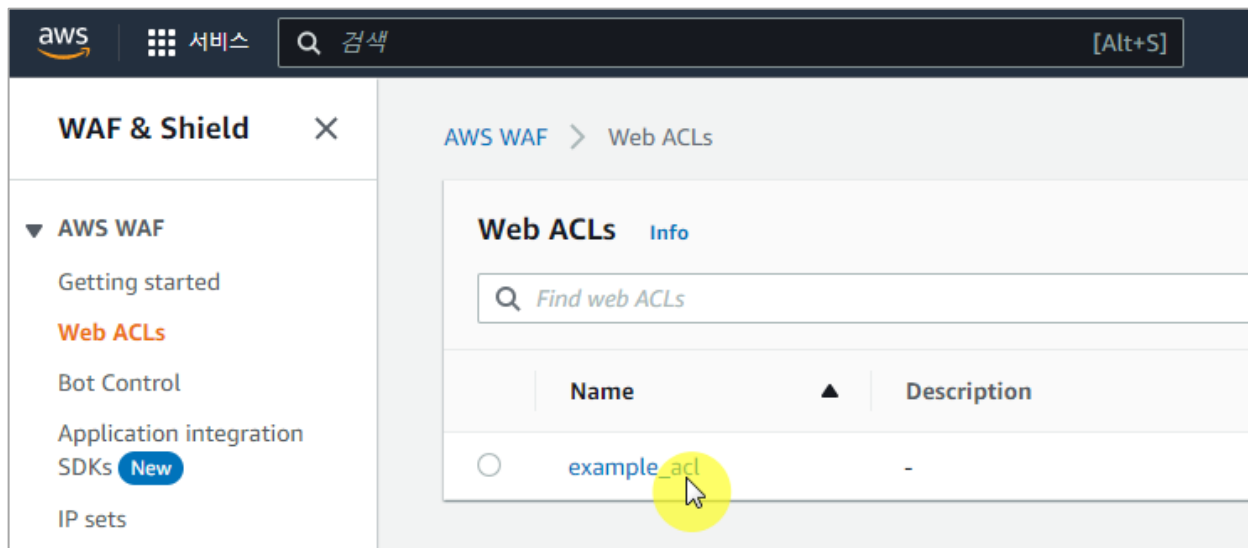
AWS WAF コンソールにアクセスします。

※ AWS WAF コンソール : <https://console.aws.amazon.com/wafv2/>



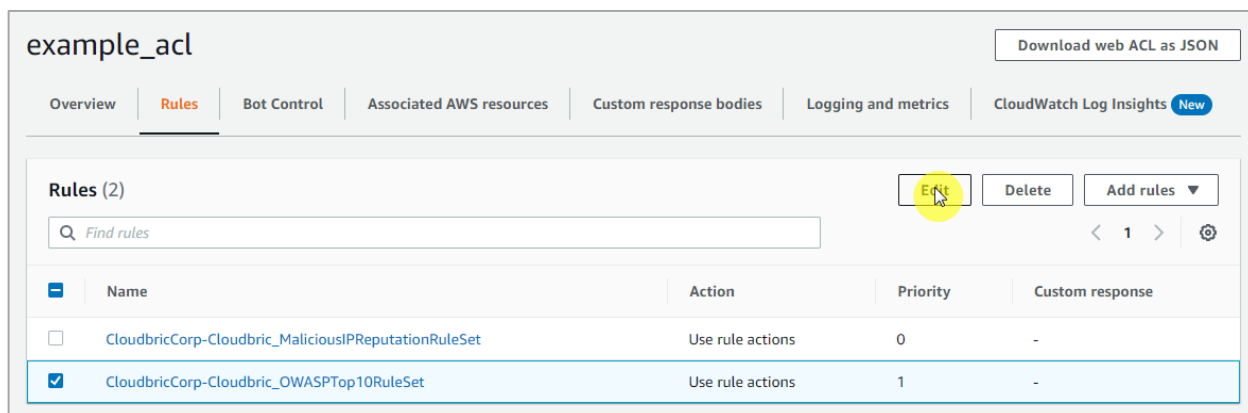
- Step 2

Web ACL 메뉴より Cloudbric Rule Set を適用する Web ACL を選択します。



- Step 3

「Rules」タブに移動し、例外処理する Rule Set にチェックを入れ「Edit」をクリックします。



- Step 4

例外処理が必要な Rule の Action を Count に再設定した後、「Save rule」を選択し例外処理します。

OWASP Top 10 Rule Set Rules

You can override rule actions for all rules and for individual rules. For a single rule, use the dropdown to specify an override action or to remove an override.

Override all rule actions

Choose rule action override ▼

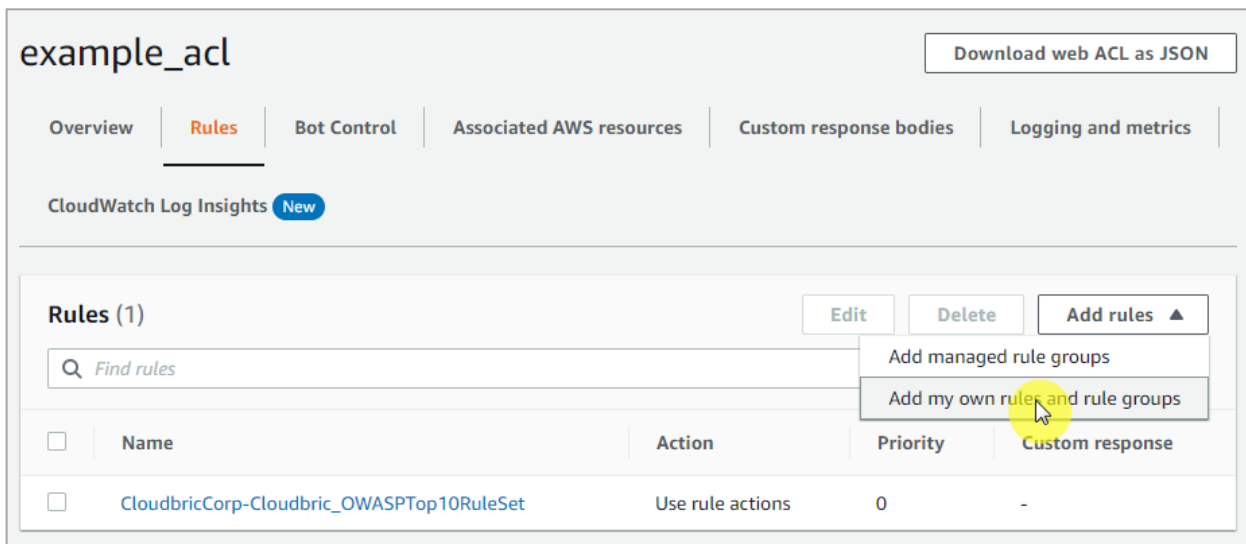
Remove all overrides

Cloudbric_BufferOverFlow	Cloudbric_XSS_1	Cloudbric_XSS_2
<div>Choose rule action override ▼</div>	<div>Choose rule action override ▲</div>	<div>Choose rule action override ▼</div>
	<div>Q </div>	
	Allow	
	Block	
	Count	
	CAPTCHA	
	Challenge	
	↶ Remove Override	
Cloudbric_SQLInjection_URL		Cloudbric_SQLInjection_Header_1
<div>Choose rule action override ▼</div>		<div>Choose rule action override ▼</div>
Cloudbric_SQLInjection_Header_2		Cloudbric_RequestMethodFiltering
<div>Choose rule action override ▼</div>		<div>Choose rule action override ▼</div>
Cloudbric_RequestHeaderFiltering		Cloudbric_StealthCommanding_Body_1
<div>Choose rule action override ▼</div>		<div>Choose rule action override ▼</div>

4.2 Label 基盤の例外処理の Rule 追加

- Step 1

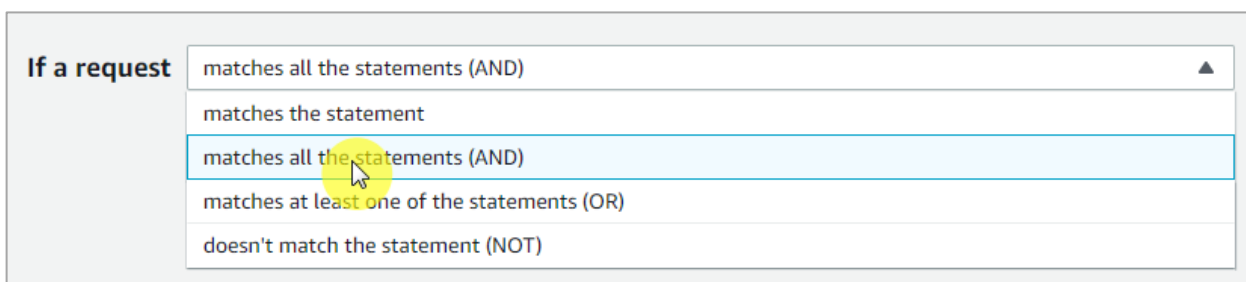
Web ACL の「Rules」ページに移動し、「Add Rules」ボタンで「Add my own rules and rule group」を選択し新規 Rule を生成します。



- Step 2

2 つの statement を充足したら一致するようにオーバーラップ条件「AND」を選択します。

- If a request: matches all the statements (AND)



- Step 3

Statement 1 は「4.1」にて例外処理した Rule と一致するリクエストを対象に検査するように定義します。

- Inspect : Has a label 選択
- Match key : 例外処理した Rule に設定した「Label 名」を選択

If a request matches all the statements (AND) ▼

Statement 1 Remove

Negate statement (NOT)
Select this to match requests that don't satisfy the statement criteria.
☐ Negate statement results

Inspect
Has a label ▼

Labels
Labels are strings that rules add to the web request. You can evaluate labels that are added by rules that run before this one in the same web ACL.

Match scope
☒ Label
☐ Namespace

Match key
Enter the string containing the label name and optional prefix and namespaces. For example, namespace1:name or aws:waf:managed:aws:managed-rule-set:namespace1:name.
aws:waf:managed:cloudbric:owasp:XSS_1 X

※ Cloudbric OWASP Top 10 Rule Set の Label 名の構造 : aws:waf:managed:cloudbric:owasp:[Rule 名]

- 例 : Rule 名が「Cloudbric_XSS_1」の場合、「aws:waf:managed:cloudbric:owasp:XSS_1」にて生成されます。

- **Step 4**

Statement2 は「4.1」で例外処理された Rule で誤検知が発生したリクエストの検知条件を除外するように定義します。

- Negate statement results : 当該の構文に定義されている検知条件を除外するようにチェック設定
- Inspect : 誤検知が発生する条件を設定

AND

NOT Statement 2 Remove

Negate statement (NOT)
Select this to match requests that don't satisfy the statement criteria.

☒ Negate statement results

Inspect
Choose an inspection option ▼

※ SQL injection 及び XSS(Cross Site Scripting)攻撃を検知する Rule に限り、AWS WAF 「ruleMatchDetails」ログフィールドでリクエストが一致した検知条件を確認することができます。

※ その以外の Rule で誤検知が発生した場合にはログ情報と共に awsmkp@cloudbric.com へお問い合わせください。

- **Step 5**

Rule と一致する場合、ブロックするよう Rule の Action を「**Block**」に設定し、「**Add Rule**」ボタンを選択し、Rule を追加します。

Action

Action
Choose an action to take when a request matches the statements above.

☐ Allow

☒ Block

☐ Count

☐ CAPTCHA

☐ Challenge

- Step 6

「4.1」で例外処理した Rule より後に適用されるように優先順位（Priority）を設定した後、「Save」ボタンを選択し、例外処理 Rule 設定を完了します。

Set rule priority [Info](#)

Rules

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

▲ Move up▼ Move down

	Name	Capacity	Action
<input type="radio"/>	CloudbricCorp-Cloudbric_OWASPTop10RuleSet	1400	Use rule actions
<input checked="" type="radio"/>	MyExceptionRule_xss_1	2	Block

CancelSave

cloudbric

5. 付録

5.1 よくある質問 (FAQ)

Q. リクエストを遮断した Rule を確認できますか。

Rule Set が適用された Web ACL の [Sampled requests] > [Rule inside rule group] にて確認できます。Web ACL ロギングを設定した場合、[RuleId] ログフィールドでも確認できます。

※ Sampled requests は直前 3 時間の間のリクエストの中、最大 100 個のログを確認できます。詳しい内容につきましては、以下の AWS デベロッパーガイドをご参照下さい。

https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/web-acl-testing-view-sample.html

Rule が確認できるログフィールドとログファイルの例です。

- **terminatingRuleId**: リクエストを終了した Rule ID です。
リクエストが終了した Rule がない場合、この値は Default_Action となります。

ex)

```
{
  "timestamp": 1576280412771,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:ap-southeast-2:111122223333:regional/webacl/STMTTest/1EXAMPLE-2ARN-3ARN-4ARN-123456EXAMPLE",
  "terminatingRuleId": "STMTTest_SQLi_XSS",
  "terminatingRuleType": "REGULAR",
  "action": "BLOCK",
  "terminatingRuleMatchDetails": [
    {
      "conditionType": "SQL_INJECTION",
      "sensitivityLevel": "HIGH",
      "location": "HEADER",
      "matchedData": [
```

- **RuleId**: リクエストに一致し、終了していない nonTerminatingMatchingRules の Rule ID です。

ex)

```
{
  "timestamp": 1592357192516
  , "formatVersion": 1
  , "webaclId": "arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
  , "terminatingRuleId": "Default_Action"
  , "terminatingRuleType": "REGULAR"
  , "action": "ALLOW"
  , "terminatingRuleMatchDetails": []
  , "httpSourceName": "-"
  , "httpSourceId": "-"
  , "ruleGroupList": []
  , "rateBasedRuleList": []
  , "nonTerminatingMatchingRules":
  [{
    "ruleId": "TestRule"
    , "action": "COUNT"
    , "ruleMatchDetails":
```

※ 詳細内容は AWS デベロッパーガイドのログの例を参照下さい。

ログの例: https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/logging-examples.html

Q. Cloudbric Rule Set が正しく適用できているか確認する方法はありますか。

AWS WAF は Block に設定されている Rule とリクエストが一致すると、基本的に 403 Forbidden エラーを返します。

以下のように XSS 攻撃をブラウザに入力し、Rule Set に適用されているかご確認下さい。

- [http://your-domain/<script>alert\('XSS'\)</script>](http://your-domain/<script>alert('XSS')</script>)

Q. Cloudbric Rule Set の検知条件を確認する方法はありますか。

基本的に AWS WAF Managed Rules の検知位置やパターンなどの詳細条件は、AWS Marketplace 販売者の知的財産権でありこれを公開する場合、Rule の迂回などのハッキングに悪用される恐れがあるため、公開していません。

しかしながら SQL Injection 及び XSS (Cross Site Scripting) 攻撃を検知する Rule に限り、AWS WAF 「ruleMatchDetails」ログフィールドでリクエストが一致した検知条件を確認することができます。

- SQL Injection 攻撃と一致する Rule の検知条件ログの例：

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

, "nonTerminatingMatchingRules":
[
  {
    "ruleId": "TestRule",
    "action": "COUNT",
    "ruleMatchDetails": [
      {
        "conditionType": "SQL_INJECTION",
        "sensitivityLevel": "HIGH",
        "location": "HEADER",
        "matchedData": [
          "10",
          "and",
          "1"
        ]
      }
    ]
  }
]
```

(左図)リクエストを終了した Rule の場合 / (右図)リクエストを終了していない Rule の場合

Q. Rule Set に含まれている各 Rule の詳細情報を確認できますか。

Rule の検知情報は AWS Marketplace 販売者の知的財産権で、また、Rule の詳細情報を公開する場合、ハッキングなどにも悪用される恐れがあるため、公開しておりません。

Q. 誤検知及び過剰検知が発生する場合、Cloudbric Rule Set の検知条件を変更する方はありますか。

AWS では Managed Rules 独自の検知条件を変更する機能を提供していません。

しかし AWS WAF Managed Rules は一般的に多くのユーザで見受けられる脅威を基盤に作成されているため使用する環境により誤検知や過剰検知が発生する場合があります。そのため Cloudbric Rule Set を本番環境に適用する 2～4 週間はモニタリングを実施し、運用環境に合わせ「4. Cloudbric Rule Set 例外処理」をご参考いただき、例外処理後に適用することを推奨いたします。

ユーザの環境に合う Rule 設定が難しい場合、クラウドブリックの AWS WAF セキュリティポリシー運用及び管理サービスである Cloudbric WMS を提案いたします。

- Cloudbric WMS サービス : <https://www.cloudbric.jp/cloudbric-wms/>
- お問い合わせ : <https://www.cloudbric.jp/inquiry/>

Q. Cloudbric Rule Set の更新内容はどこで確認できますか。

クラウドブリックホームページにて Cloudbric Rule Set の変更内容を案内しております。

※ IP 基盤の Rule Set の場合、IP リストの動的特性により Rule に適用された IP リストの変更内容は案内していません。

Cloudbric Rule Set for AWS WAF リリースノート

- JP : <https://www.cloudbric.jp/managed-rules-for-aws-waf-release-notes/>

Q. Cloudbric Rule Set の月額料金はど計算しますか。

AWS Marketplace の AWS WAF Managed Rule 料金は
Cloudbric Rule Set が適用された Web ACL 基準で以下 2 つの単位を基準として請求されます。

- ① **Region:** Web ACL の Region 数
- ② **Requests:** 各 Region に 100 万件単位で Web ACL に受信された Requests 数

Cloudbric OWASP Top 10 Rule Set 料金の例

- OWASP Top 10 Rule Set 料金:

計算単位	料金
Region 当たり	\$25/月 (時間で案分)
各 Region の 100 万 Requests 当たり	\$1/月

- 例 A:

1 つのリージョン(例: us-east-1)に作成した Web ACL 2 つに Cloudbric Rule Set を適用し
2 つの Web ACL に 1 カ月間受信された Web Requests が 1,000 万件の場合

us-east-1 Region

① **Region 料金:** $\$25.00 * 1 = \25.00

② **Requests 料金:** $\$1.00(100 \text{ 万件当たり}) * 10 \text{ Requests}(1,000 \text{ 万件}) = \10.00

= 合計(①+②): \$35.00

- 例 B:

2 つのリージョン(例: us-east-1, us-west-2)に Web ACL を 2 つずつ作成し Cloudbric Rule Set を適用して、

Web ACL に 1 カ月間受信された Web Requests が各リージョンに 1,000 万件の場合

us-east-1 Region

① **Region 料金:** $\$25.00 * 1 = \25.00

② **Requests 料金:** $\$1.00(100 \text{ 万件当たり}) * 10 \text{ Requests}(1,000 \text{ 万件}) = \10.00

us-west-2 Region

③ **Region 料金:** $\$25.00 * 1 = \25.00

④ **Requests 料金:** $\$1.00(100 \text{ 万件当たり}) * 10 \text{ Requests}(1,000 \text{ 万件}) = \10.00

= 合計(①+②+③+④): \$70.00

5.2 Cloudbrix OWASP Top 10 Rule

Rule	説明
Buffer Overflow	Web サーバーに対しメモリ上の領域をオーバーさせるような、制限値より大きなサイズのデータが含まれているリクエストを遮断
Cross Site Scripting (XSS)	クライアント側で実行可能な悪意あるスクリプトを挿入する試みを遮断
SQL Injection	データベースに対し不正な SQL クエリを送り付ける試みを遮断
Directory Traversal	Web サーバーのディレクトリおよびファイルにアクセスを試みるリクエストを遮断
Request Method Filtering	安全ではない HTTP リクエストのメソッドを遮断
Request Header Filtering	Web ブラウザにより発行された正常な HTTP リクエストとは異なり、ヘッダの一部の情報が抜けているか、もしくは自動化されたツールによる不正なアクセスの場合遮断
Stealth Commanding	多くの Web アプリケーションは、機能を実行するために OS や外部プログラムを使用します。Web アプリケーションが HTTP リクエストを受信して外部プログラムに情報を送信する場合、攻撃者は情報を改ざんし、悪意のあるコマンドを挿入させます。その後、OS や外部プログラムがこの改ざん情報を実行させることにより、トロイの木馬を植え付けたり、悪質なコードの実行を強制します。
File Upload	Web サーバーで実行可能なファイルのアップロードを遮断
XXE Injection	XML ドキュメントの External entity を用いて、ローカルファイルの閲覧などを起こす攻撃を遮断します。