

AWS WAF Managed Rules
ルールグループの例外機能マニュアル
Ver 1.0

目次

1. [機能概要](#)
2. [ご利用頂くための前提条件](#)
3. [ルールグループの例外機能を有効にする方法](#)
4. [ルールグループの例外機能のご利用](#)
 - 4.1. [Managed Rules の一覧および例外設定状態を確認する方法](#)
 - 4.2. [Managed Rules の全体および個別ルールのAction を変更する方法](#)
 - 4.3. [Action 変更に関する操作のステータスを確認する方法](#)
5. [補足](#)
 - 5.1. [Managed Rules ページで可能な操作](#)
 - 5.2. [Action Override](#)
 - 5.3. [Action](#)
 - 5.4. [Task](#)
 - 5.5. [Status](#)

1. 機能概要

AWS WAF Managed Rules のルールグループの例外機能を
AWS マネジメントコンソール を利用せず、WafCharm管理画面にて容易に設定できる機能です。

※ルールグループの例外機能とは

AWS WAF Managed Rules でルール単位での
COUNT(検知) / BLOCK(遮断) モードの切り替えができる機能です。

※ AWS WAF Managed Rules とは

多数のルールで構成されるルールセットで、AWS マーケットプレイスにて購入いただけます。
提供されているルールは下記からご確認いただけます。

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

The logo for Waf Charm features the text "Waf Charm" in a bold, sans-serif font. The word "Waf" is in black, and "Charm" is in a dark grey. A small blue dot is positioned above the letter "a" in "Charm".

2. ご利用頂くための前提条件

WafCharm でルールグループの例外機能をご利用いただくには、下記設定が必要となります。

- 2.1 以下のリンクより弊社が提供する、Managed Rules を Subscribe してください。
[Cyber Security Cloud Managed Rules for AWS WAF -HighSecurity OWASP Set-](#)
- 2.2 上記 Managed Rules を WafCharm にご登録の Web ACL に設定してください。
- 2.3 Entry Plan のお客様は WafCharm でのルールグループの例外機能はご利用いただけません。

3. ルールグループの例外機能を有効にする方法

3.1 Web ACL Config の設定

3.1.1 WafCharm 管理画面にログインしてください。

3.1.2 Managed Rules を適用しているWeb ACL Config 画面を開いてください。

3.1.3 Web ACL Config の設定をされていない方は以下のブログを参考にしてください。

<https://www.wafcharm.com/blog/check-wafcharm-setting-jp/>

The screenshot shows the WafCharm management interface. At the top, there is a dark navigation bar with the WafCharm logo and menu items: Web ACL Config (highlighted), Web Site Config, and Managed Rules. On the right side of the navigation bar, it says 'TEST USER' with a dropdown arrow. Below the navigation bar, the main heading is 'Web ACL Config'. Underneath the heading, there are two links: '< Back' and '+ Add ACL'. The main content area displays a table with two columns: 'Web ACL ID' and 'Web ACL Name'. The table contains one row with a long alphanumeric ID and the name 'TEST'. To the right of the 'TEST' name, there are two icons: a share icon and a settings gear icon.

Web ACL ID	Web ACL Name
560274851-4756-4547-0461-117095000001	TEST

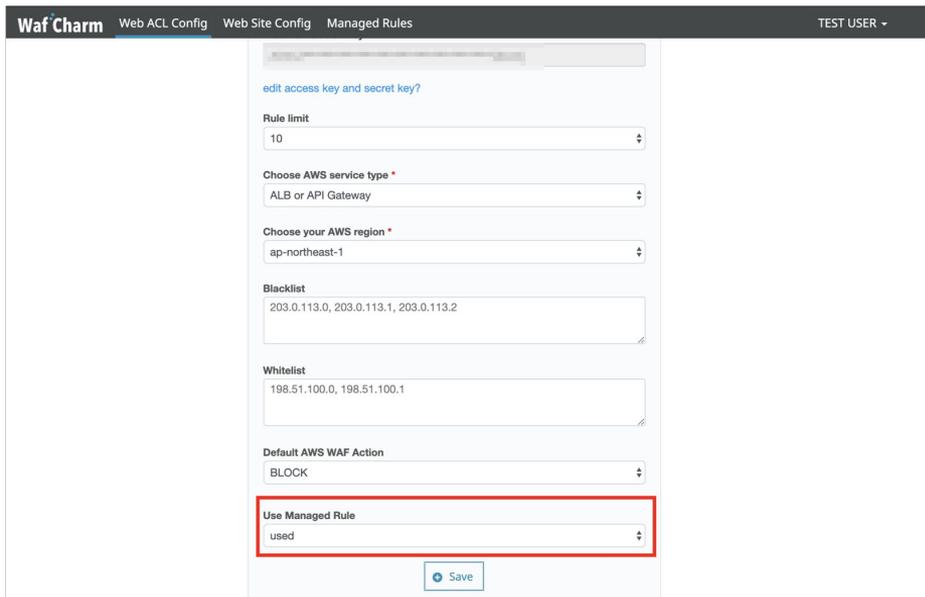
3.2 ルールグループの例外機能の有効化

3.2.1 Web ACL Config の Edit 画面を開いてください。

3.2.2 Use Managed Rule 項目を unused から used に変更してください。

3.2.3 Save ボタンをクリックしてください。

※設定はいつでも変更可能です。



The screenshot shows the 'Waf Charm' configuration interface. The top navigation bar includes 'Waf Charm', 'Web ACL Config', 'Web Site Config', 'Managed Rules', and 'TEST USER'. The main content area is titled 'edit access key and secret key?'. Below this, there are several configuration sections:

- Rule limit:** A dropdown menu set to '10'.
- Choose AWS service type:** A dropdown menu set to 'ALB or API Gateway'.
- Choose your AWS region:** A dropdown menu set to 'ap-northeast-1'.
- Blacklist:** A text input field containing '203.0.113.0, 203.0.113.1, 203.0.113.2'.
- Whitelist:** A text input field containing '198.51.100.0, 198.51.100.1'.
- Default AWS WAF Action:** A dropdown menu set to 'BLOCK'.
- Use Managed Rule:** A dropdown menu set to 'used', which is highlighted with a red rectangular box.

At the bottom of the form is a 'Save' button with a blue circular icon containing a plus sign.

ルールグループの例外機能を有効化完了

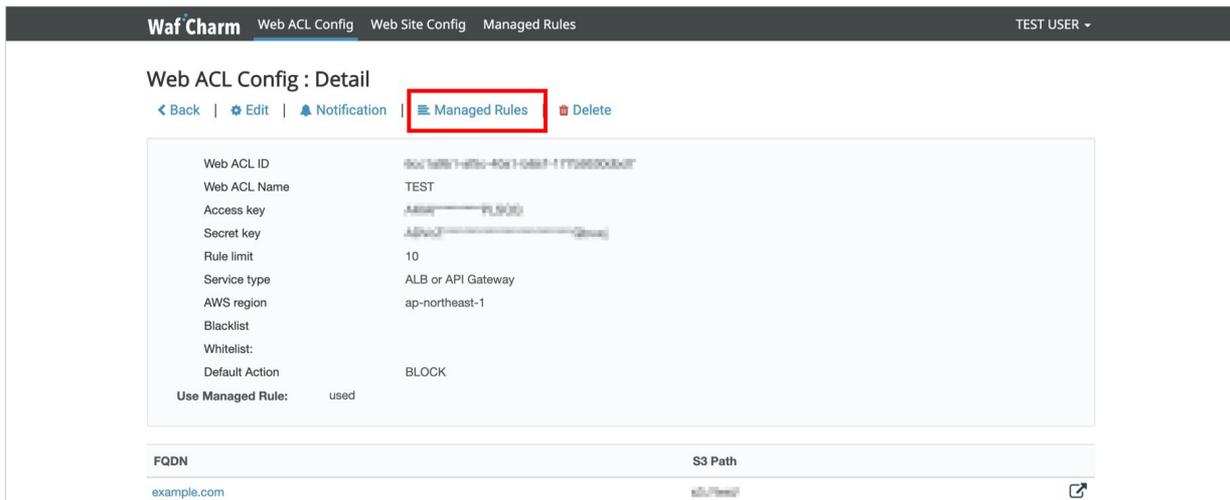
以上でルールグループの例外機能をご利用いただけるようになります。

4. ルールグループの例外機能のご利用

4.1 Managed Rules の一覧および例外設定状態を確認する方法

4.1.1 Managed Rules 画面へ遷移

「Managed Rules」を押下し、Managed Rules 画面に遷移してください。



The screenshot shows the 'Web ACL Config : Detail' page in the Waf Charm interface. The 'Managed Rules' tab is selected and highlighted with a red box. The page displays configuration details for a Web ACL named 'TEST'.

Property	Value
Web ACL ID	50c7a8b1-a7b0-40d1-0a87-17709000b0f7
Web ACL Name	TEST
Access key	AKIAI44QH8DHBVS3LH536
Secret key	AKIAI44QH8DHBVS3LH536
Rule limit	10
Service type	ALB or API Gateway
AWS region	ap-northeast-1
Blacklist	
Whitelist	
Default Action	BLOCK
Use Managed Rule:	used

FQDN	S3 Path
example.com	s3://test/

4.1 Managed Rules の一覧および例外設定状態を確認する方法

4.1.3 Managed Rules 画面(弊社 Managed Rulesの状態取得後)

下記の画面にてお客様 AWS WAF に適用されている弊社 Managed Rules の状態と同一の状態をご確認いただけます。

お客様の AWS WAF に適用されている弊社の Managed Rules の状態の取得が完了した後は、下記赤枠の Action Override のように現在の Managed Rules の状態が反映されます。

The screenshot shows the Waf Charm interface with the 'Managed Rules' section selected. The 'Action Override' column in the table is highlighted with a red box, showing 'No override' for the selected rule group.

Waf Charm Web ACL Config Web Site Config Managed Rules TEST USER ▾

Managed Rules

Web ACLs > Web ACL: TEST

[Edit](#) [Waiting Tasks](#) [Completed Tasks](#) [Refresh Status](#)

Rule Group Section

Managed Rule Group Name	Action Override
Cyber Security Cloud Managed Rules for AWS WAF -HighSecurity OWASP Set-	No override

Individual Rules Section

No	Rule Id	Name	Attack Type	Field Type	Action Override	Action
1	arn:aws:wafv2::aws:managed-rule-groups/111111111111:rule-groups/111111111111	bad_useragent-header-001	bad_useragent	header	No	⊞ BLOCK
2	arn:aws:wafv2::aws:managed-rule-groups/111111111111:rule-groups/111111111111	bad_useragent-header-002	bad_useragent	header	No	⊞ BLOCK

4.1 Managed Rules の一覧および例外設定状態を確認する方法

4.1.4 AWS マネジメントコンソール上のAWS WAFの状態

Managed Rules 画面とAWS マネジメントコンソール上の Action の状態が一致していることをご確認いただけます。

The screenshot shows the AWS WAF console interface. On the left, the 'Web ACLs' section is expanded, showing a list of rules. The main area displays the 'Rules' tab for a specific Web ACL. The table below shows the configuration of the rules:

Order	Rule	Type	Action
1	[Redacted]	Regular	Count requests
2	[Redacted]	Regular	Count requests
3	[Redacted]	Regular	Count requests
4	[Redacted]	Regular	Count requests
5	[Redacted]	Regular	Count requests
6	Cyber Security Cloud Managed Rules for AWS WAF - HighSecurity OWASP Set-	Group	No override

Below the table, the 'Default action' is set to 'Allow all requests that don't match any rules'. At the bottom, the 'Status' for the rule group is '0 rule(s) excluded'.

4.2 Managed Rules の全体および個別ルール の Action を変更する方法

4.2.1 Actionの変更 (Edit 画面)

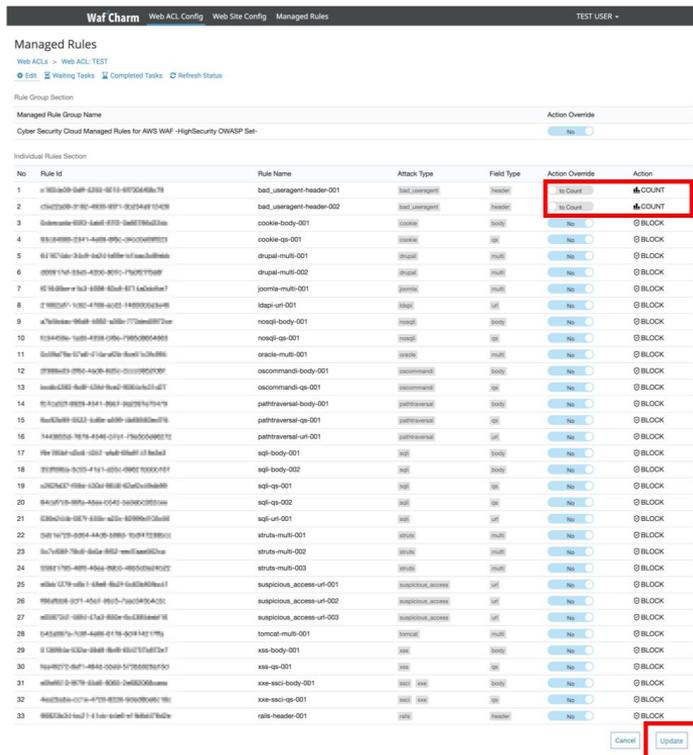
Action Override 部分の Action をクリックし、Update ボタンを押下してください。

(BLOCK の場合は、Action Override 項目を [No] に、COUNT の場合は、[to Count] となるよう設定してください。)

※設定の反映には 10分程度時間がかかります。

※右記 Managed Rules 画面では弊社の Managed Rules に含まれる全てのルールが表示されている訳ではなく、お客様にて制御可能なルールのみ表示されております。

その他、変更を希望するルールがあった場合は [サポート](#)にご連絡ください。



4.2 Managed Rules の全体および個別ルール の Action を変更する方法

4.2.2 Managed Rules 画面の状態確認

AWS マネジメントコンソール上の弊社 Managed Rules への Action の変更を実施後、左記 Managed Rules 画面に適用した状態が反映されるまで 10分程度かかります。

Waf Charm [Web ACL Config](#) [Web Site Config](#) [Managed Rules](#) TEST USER ▾

Managed Rules

[Web ACLs](#) > [Web ACL: TEST](#)

[Edit](#) [Waiting Tasks](#) [Completed Tasks](#) [Refresh Status](#)

Rule Group Section

Managed Rule Group Name	Action Override
Cyber Security Cloud Managed Rules for AWS WAF -HighSecurity OWASP Set-	No override

Individual Rules Section

No	Rule Id	Name	Attack Type	Field Type	Action Override	Action
1	arn:aws:wafv2:us-east-1:123456789012:managed-rule-group/HighSecurityOWASPSet/bad-useragent-header-001	bad_useragent-header-001	bad_useragent	header	to Count	📊 COUNT
2	arn:aws:wafv2:us-east-1:123456789012:managed-rule-group/HighSecurityOWASPSet/bad-useragent-header-002	bad_useragent-header-002	bad_useragent	header	to Count	📊 COUNT
3	arn:aws:wafv2:us-east-1:123456789012:managed-rule-group/HighSecurityOWASPSet/cookie-body-001	cookie-body-001	cookie	body	No	🚫 BLOCK
4	arn:aws:wafv2:us-east-1:123456789012:managed-rule-group/HighSecurityOWASPSet/cookie-qs-001	cookie-qs-001	cookie	qs	No	🚫 BLOCK

4.2 Managed Rules の全体および個別ルール の Action を変更する方法

4.2.3 AWS マネジメントコンソール画面の状態

Action 変更結果を AWS マネジメントコンソールでも確認可能です。

AWS マネジメントコンソール画面に Managed Rules 内の COUNT モードにしたいルールが反映されています。
(下記赤枠部分)

The screenshot shows the AWS WAF console interface. On the left, the 'Web ACLs' section is expanded, and the 'Rules' tab is selected. The main area displays a table of rules with columns for Order, Rule, Type, and Action. Below this table, a section titled 'If a request doesn't match any rules, take the default action' shows the default action as 'Allow all requests that don't match any rules'. At the bottom, a table lists the rule group name and its status. The status for the 'Cyber Security Cloud Managed Rules for AWS WAF - HighSecurity OWASP Set-' rule group is '2 rule(s) excluded', which is highlighted with a red box. Another red box highlights the individual rules listed below.

Order	Rule	Type	Action
1	[Redacted]	Regular	Count requests
2	[Redacted]	Regular	Count requests
3	[Redacted]	Regular	Count requests
4	[Redacted]	Regular	Count requests
5	[Redacted]	Regular	Count requests
6	Cyber Security Cloud Managed Rules for AWS WAF - HighSecurity OWASP Set-	Group	No override

Rule group name	Status
Cyber Security Cloud Managed Rules for AWS WAF - HighSecurity OWASP Set-	2 rule(s) excluded

4.3 Action 変更に関する操作のステータスを確認する方法

4.3.1 操作のステータス確認

Waiting Tasks リンクを押下することで、現在処理待ちのステータスをご確認いただけます。

Waiting Tasks 画面

Waf Charm [Web ACL Config](#) [Web Site Config](#) [Managed Rules](#) TEST USER ▾

Managed Rules

[Web ACLs](#) > [Web ACL: TEST](#)

[Edit](#) [Waiting Tasks](#) [Completed Tasks](#) [Refresh Status](#)

Target	Rule ID	Name	Task	Status	Accepted
Group		Cyber Security Cloud Managed Rules for AWS WAF -HighSecurity OWASP Set-	Refresh Status	Waiting	2019-06-05 10:20:57 +0900

4.3 Action 変更に関する操作のステータスを確認する方法

4.3.2 操作完了のステータス確認

Completed Tasks リンクを押下することで、処理が完了したステータスをご確認いただけます。

Completed Tasks 画面

Waf Charm [Web ACL Config](#) [Web Site Config](#) [Managed Rules](#) TEST USER ▾

Managed Rules

[Web ACLs](#) > [Web ACL: TEST](#)

[Edit](#) [Waiting Tasks](#) [Completed Tasks](#) [Refresh Status](#)

Target	Rule ID	Name	Task	Status	Accepted	Completed
Rule	e1904e89-0c25-4c55-8215-827884958178	bad_useragent-header-001	Update to Override to Count	Success	2019-06-05 12:07:45 +0900	2019-06-05
Rule	e1904e89-0c25-4c55-8215-827884958178	bad_useragent-header-002	Update to Override to Count	Success	2019-06-05 12:07:45 +0900	2019-06-05

ルールグループの例外機能のご利用

ルールグループの例外機能のご利用に関しては以上となります。

5. 補足

5.1 Managed Rules ページで可能な操作

Managed Rules ページで用意している下記メニューについて説明します。



Managed Rules

[Web ACLs](#) > [Web ACL: TEST](#)

[Edit](#) [Waiting Tasks](#) [Completed Tasks](#) [Refresh Status](#)

名称	役割
Edit	各ルールのアクションやManaged Rules 全体の Action を変更する際に使用します。
Waiting Tasks	現在処理待ちのタスク一覧をご確認いただけます。
Completed Tasks	処理が完了したタスク一覧をご確認いただけます。
Refresh Status	AWS マネジメントコンソール上の弊社Managed Rules と状態を合わせる際に使用します。AWS マネジメントコンソール側で弊社 Managed Rules の Action を変更した場合は、こちらを押下して状態を合わせてください。

5.2 Action Override

Rule Group Section と Individual Rules Section に表示される Action Override について説明します。

Waf Charm Web ACL Config Web Site Config Managed Rules TEST USER ▾

Managed Rules

[Web ACLs](#) > [Web ACL: TEST](#)

[Edit](#) [Waiting Tasks](#) [Completed Tasks](#) [Refresh Status](#)

Rule Group Section

Managed Rule Group Name	Action Override
Cyber Security Cloud Managed Rules for AWS WAF -HighSecurity OWASP Set-	No override

Individual Rules Section

No	Rule Id	Name	Attack Type	Field Type	Action Override	Action
1	01400000-0140-0000-0001-000000000000	bad_useragent-header-001	bad_useragent	header	to Count	COUNT
2	01400000-0140-0000-0001-000000000000	bad_useragent-header-002	bad_useragent	header	to Count	COUNT

5.2.1 Rule Group Section における Action Override の違い

- Rule Group Section では、Managed Rules 全体の動作を設定することができます。
 - 以下の動作を選択することができます。

Action Override	検知時の動作
No override	BLOCK
Override to count	COUNT

5.2.2 Individual Rules Section における Action Override の違い

- Individual Rules Section では、ルール毎に動作を設定することができます。
 - 以下の動作を選択することができます。

Action Override	検知時の動作
No	BLOCK
to Count	COUNT

5.3 Action

- Action 列には、AWS 上で動作する際の Action が表示されます。
 - AWS 上で動作する際の Action とは Rule Group Section の Action Override と Individual Rules Section の Action Override の組み合わせにより決定される Action です。
※組み合わせのパターンは次ページを参照ください。

The screenshot shows the AWS WAF console interface for Waf Charm. The top navigation bar includes 'Waf Charm', 'Web ACL Config', 'Web Site Config', 'Managed Rules', and 'TEST USER'. The main content area is titled 'Managed Rules' and shows the configuration for 'Web ACL: TEST'. Under the 'Rule Group Section', the 'Managed Rule Group Name' is 'Cyber Security Cloud Managed Rules for AWS WAF -HighSecurity OWASP Set-', and the 'Action Override' is set to 'No override'. Under the 'Individual Rules Section', there are two rules: 'bad_useragent-header-001' and 'bad_useragent-header-002', both with 'Attack Type' 'bad_useragent' and 'Field Type' 'header'. Both rules have an 'Action Override' of 'to Count' and an 'Action' of 'COUNT'.

Rule Group Section	
Managed Rule Group Name	Action Override
Cyber Security Cloud Managed Rules for AWS WAF -HighSecurity OWASP Set-	No override

Individual Rules Section					
No	Rule Id	Name	Attack Type	Field Type	Action
1	AWASACL001-100-4000-0001-000000000000	bad_useragent-header-001	bad_useragent	header	COUNT
2	AWASACL001-100-4000-0002-000000000000	bad_useragent-header-002	bad_useragent	header	COUNT

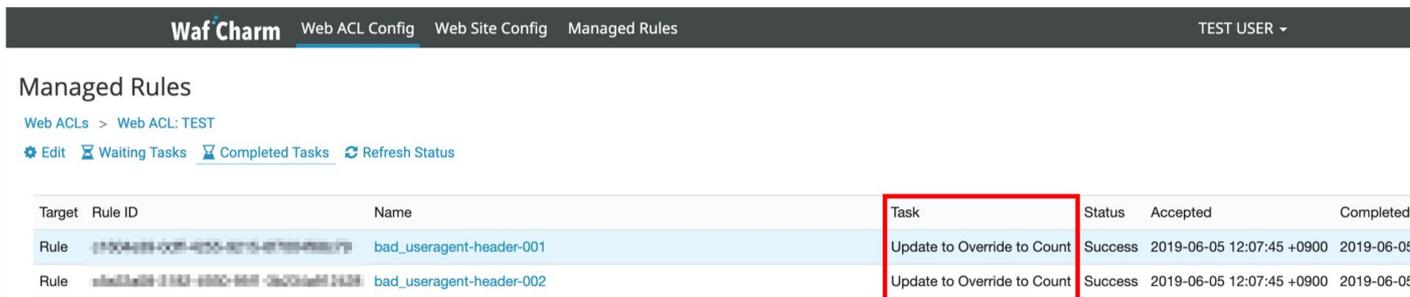
5.3.1 Action Override の組み合わせパターン

例) Rule Group Section の Action Override で Override to count をご選択の場合は、Individual Rules Section の Action を No にしていた場合も、Action は COUNT になります。

Rule Group Section Action Override	Individual Rules Section Action Override	Action
No override	No	BLOCK
No override	to Count	COUNT
Override to count	No	COUNT
Override to count	to Count	COUNT

5.4 Task

Action Override の更新をすると、WafCharm は AWS WAF への指示を Task として非同期実行するため、実行状態を赤枠部分にて確認いただく事が出来ます。



WafCharm Web ACL Config Web Site Config Managed Rules TEST USER ▾

Managed Rules

Web ACLs > Web ACL: TEST

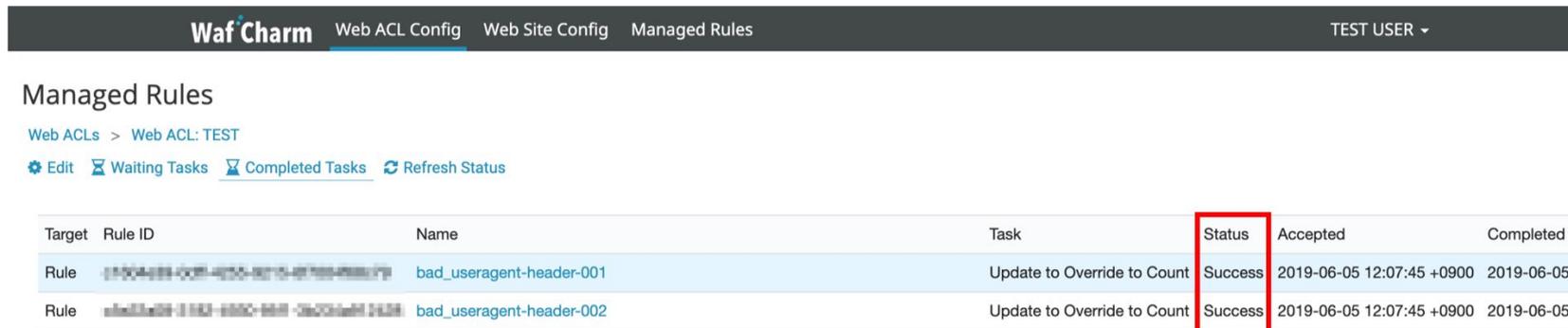
[Edit](#) [Waiting Tasks](#) [Completed Tasks](#) [Refresh Status](#)

Target	Rule ID	Name	Task	Status	Accepted	Completed
Rule	12345678-9012-3456-7890-123456789012	bad_useragent-header-001	Update to Override to Count	Success	2019-06-05 12:07:45 +0900	2019-06-05
Rule	12345678-9012-3456-7890-123456789012	bad_useragent-header-002	Update to Override to Count	Success	2019-06-05 12:07:45 +0900	2019-06-05

Task名	処理内容
Update to Override to Count	COUNTモードに変更
Update to No Override	BLOCKモードに変更
Refresh Status	AWS マネジメントコンソール上のManaged Rulesの状態取得

5.5 Status

Task の処理状態を表すものが 下記赤枠の Status です。



The screenshot shows the WafCharm interface with the 'Managed Rules' section. The breadcrumb is 'Web ACLs > Web ACL: TEST'. There are navigation links for 'Edit', 'Waiting Tasks', 'Completed Tasks', and 'Refresh Status'. A table lists two rules, both with a 'Success' status in the 'Status' column, which is highlighted with a red box.

Target	Rule ID	Name	Task	Status	Accepted	Completed
Rule	[REDACTED]	bad_useragent-header-001	Update to Override to Count	Success	2019-06-05 12:07:45 +0900	2019-06-05
Rule	[REDACTED]	bad_useragent-header-002	Update to Override to Count	Success	2019-06-05 12:07:45 +0900	2019-06-05

Status の値は処理状況に対応して値が設定されます。種類に関しては、次ページにて記載しています。

5.5.1 Statusの種類 (1/2)

Status	意味	対応策
Success	成功	-
Failed(Permission error)	設定されている権限が不足しています。	権限に関する IAM 設定は下記ページを参照ください。 https://www.wafcharm.com/blog/aws-iam-setting-for-wafcharm-jp/
Failed(Managed Rule not found)	Managed Rules が Web ACL にアタッチされていません。	1. 弊社 Managed Rules が Web ACL にアタッチされているかご確認ください。 2. ご利用頂くための前提条件 をご確認ください。

5.5.1 Statusの種類 (2/2)

Status	意味	対応策
Failed(Unknown error happened)	不明なエラーが発生	<ol style="list-style-type: none">1.再度ルールグループの例外機能が使えないかお試しください。2.手順1で状況が改善しない場合は、発生状況等を含めて、下記サポートにご連絡ください。 wafcharm-support@cscloud.co.jp
Failed(Max retry was over)	リトライ処理が上限に達したため、エラーが発生	<ol style="list-style-type: none">1.再度ルールグループの例外機能が使えないかお試しください。2.手順1で状況が改善しない場合は、発生状況等を含めて、下記サポートにご連絡ください。 wafcharm-support@cscloud.co.jp

ご不明な点がございましたら
wafcharm-support@cscloud.co.jp までご連絡をお願いいたします。

Waf Charm