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

Waf Charm

目次

Waf Charm

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

WafCharm

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。

WafCharm

3.　ルールグループの例外機能を有効にする方法

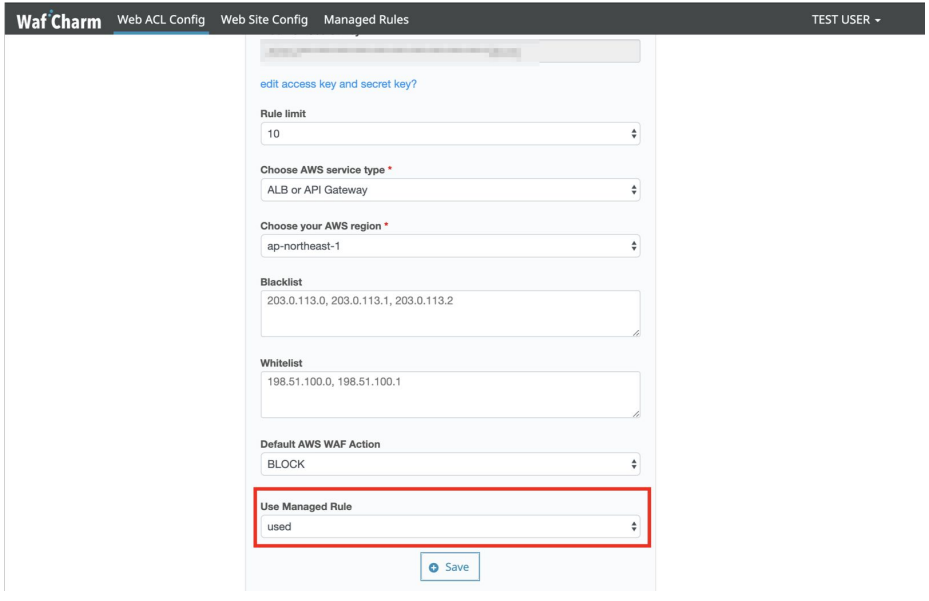
Waf Charm

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/

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。



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。

Waf Charm

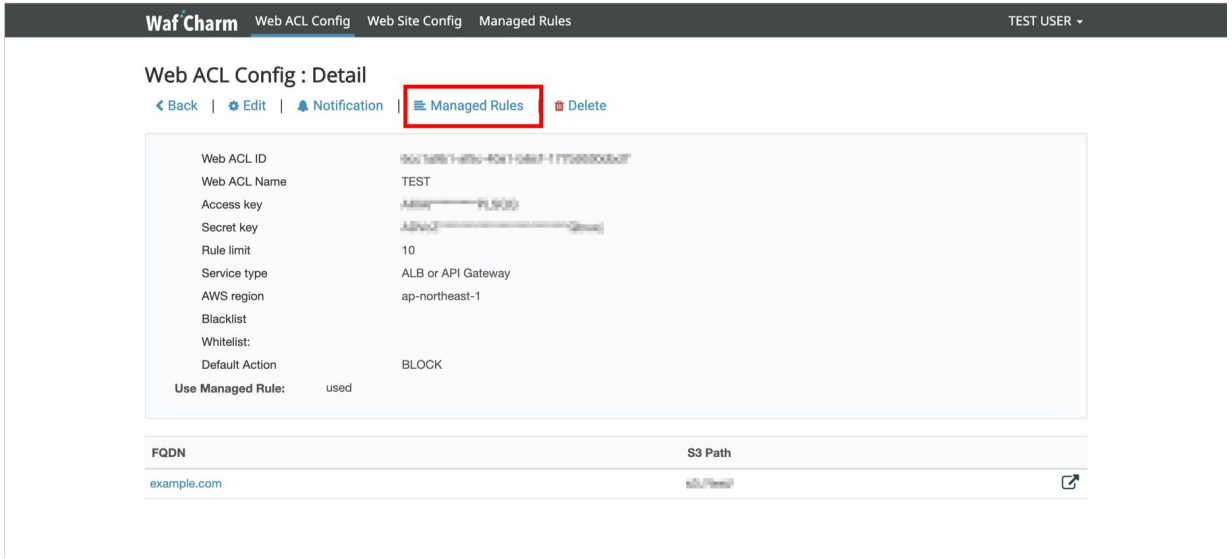
4. ルールグループの例外機能のご利用

Waf Charm

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。

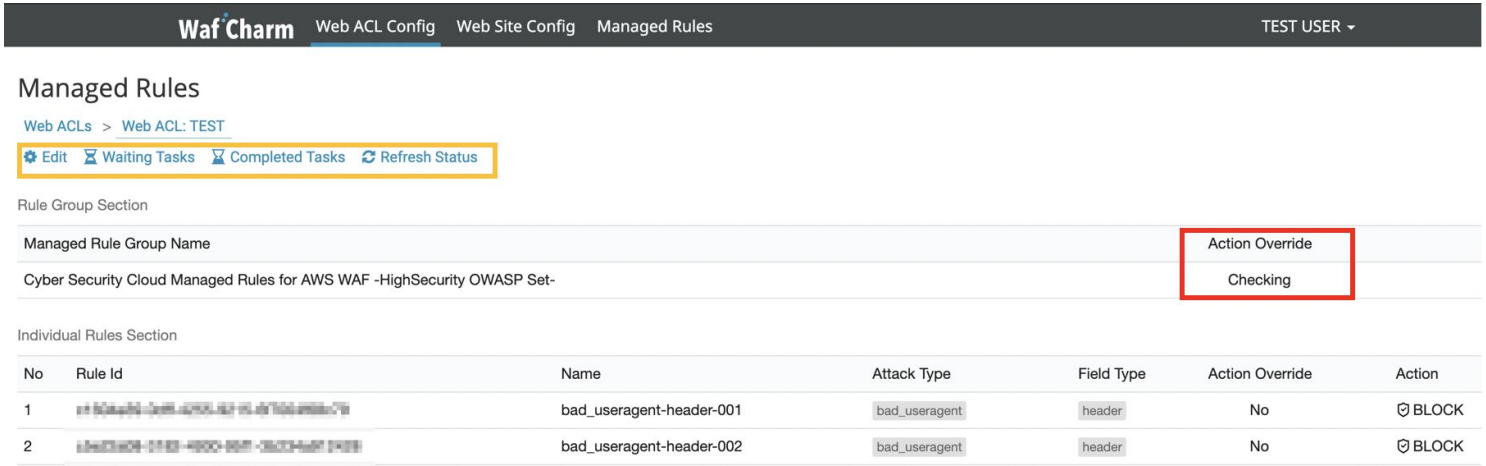


4.1 Managed Rules の一覧および例外設定状態を確認する方法

4.1.2 Managed Rules 画面

下記の画面にて Managed Rules の一覧をご確認いただけます。
下記黄色枠の詳細は補足ページ (Managed Rules ページで可能な操作)をご覧ください。

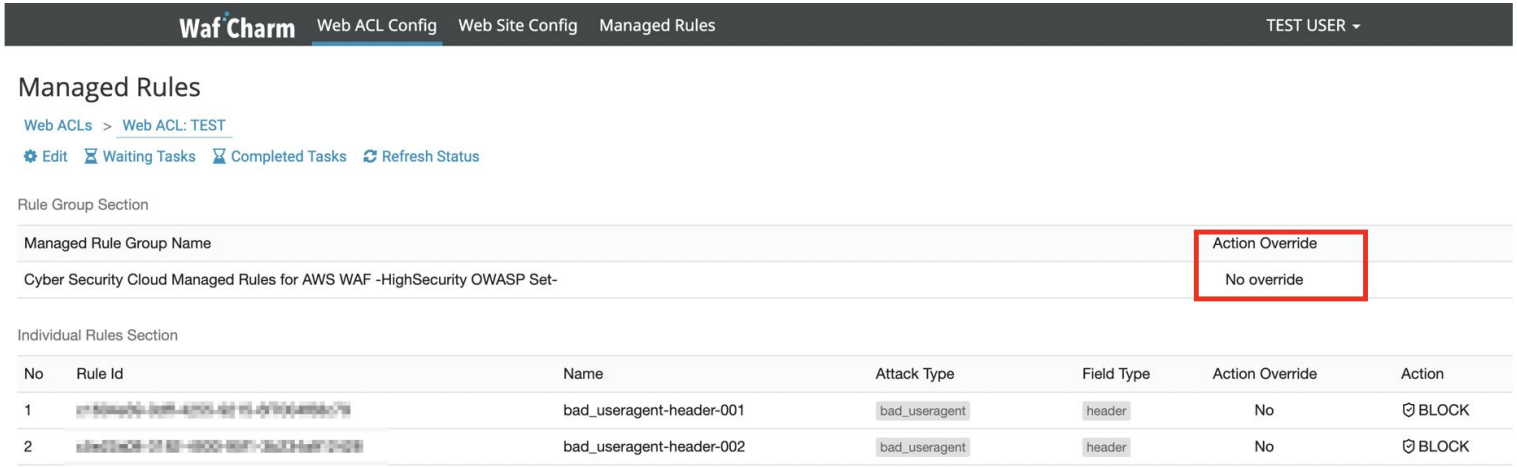
※初めてルールグループの例外機能をご使用になる場合は、下記赤枠　Action Override の部分が Checking になっています。
お客様の AWS WAF に適用されている弊社の Managed Rules の状態を取得している状態ですので、状態が反映されるまでお待ちください。
（10分程度）



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)

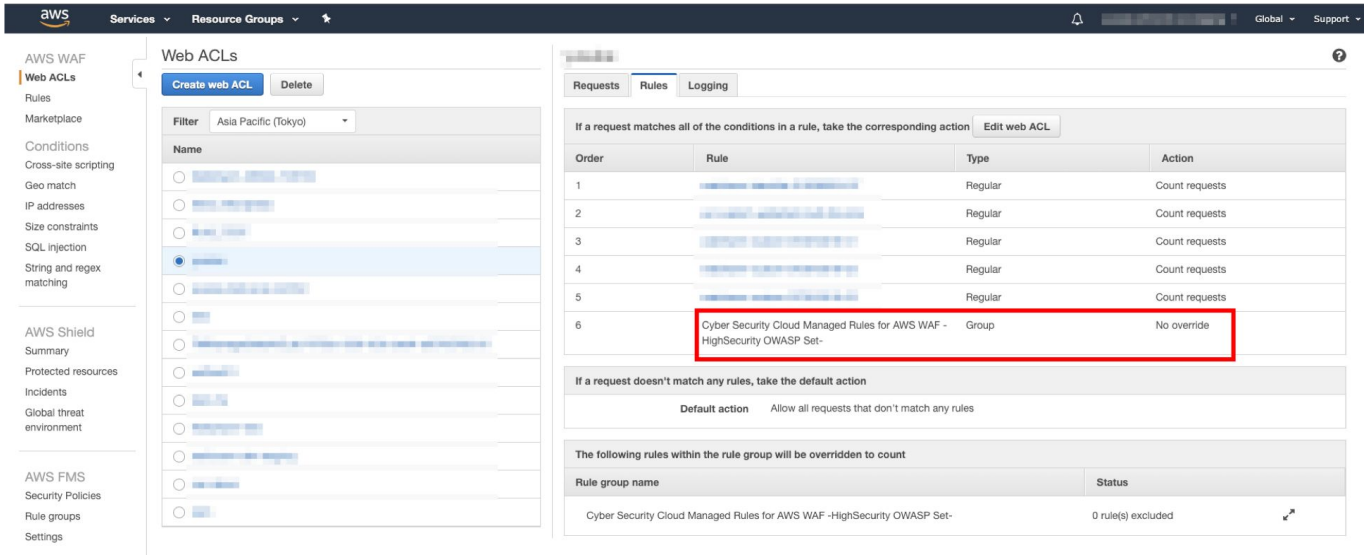
下記の画面にてお客様 AWS WAF に適用されている弊社 Managed Rules の状態と同一の状態をご確認いただけます。
お客様の AWS WAF に適用されている弊社の Managed Rules の状態の取得が完了した後は、下記赤枠の Action Override のように現在の Managed Rules の状態が反映されます。



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。



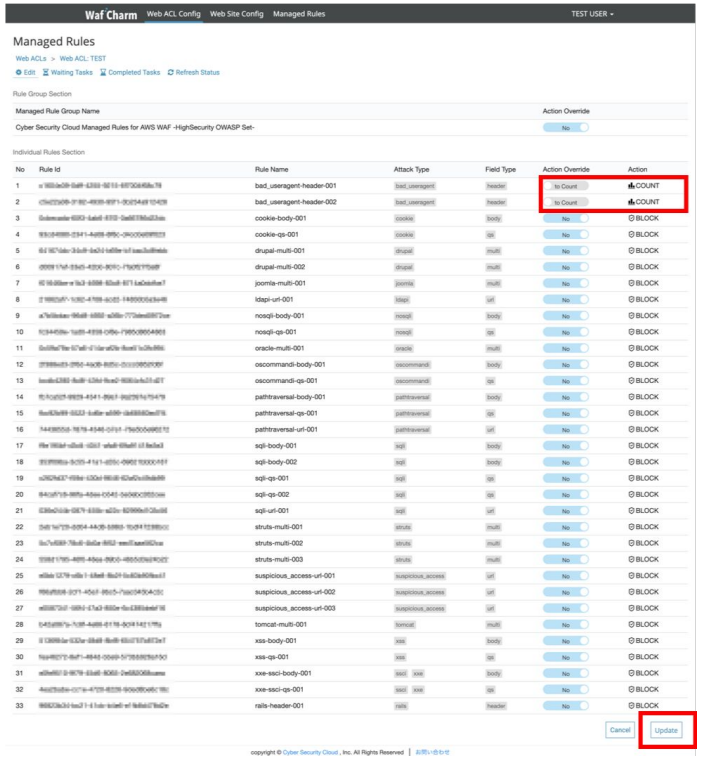
4.2 Managed Rules の全体および個別ルールの Action を変更する方法

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。)

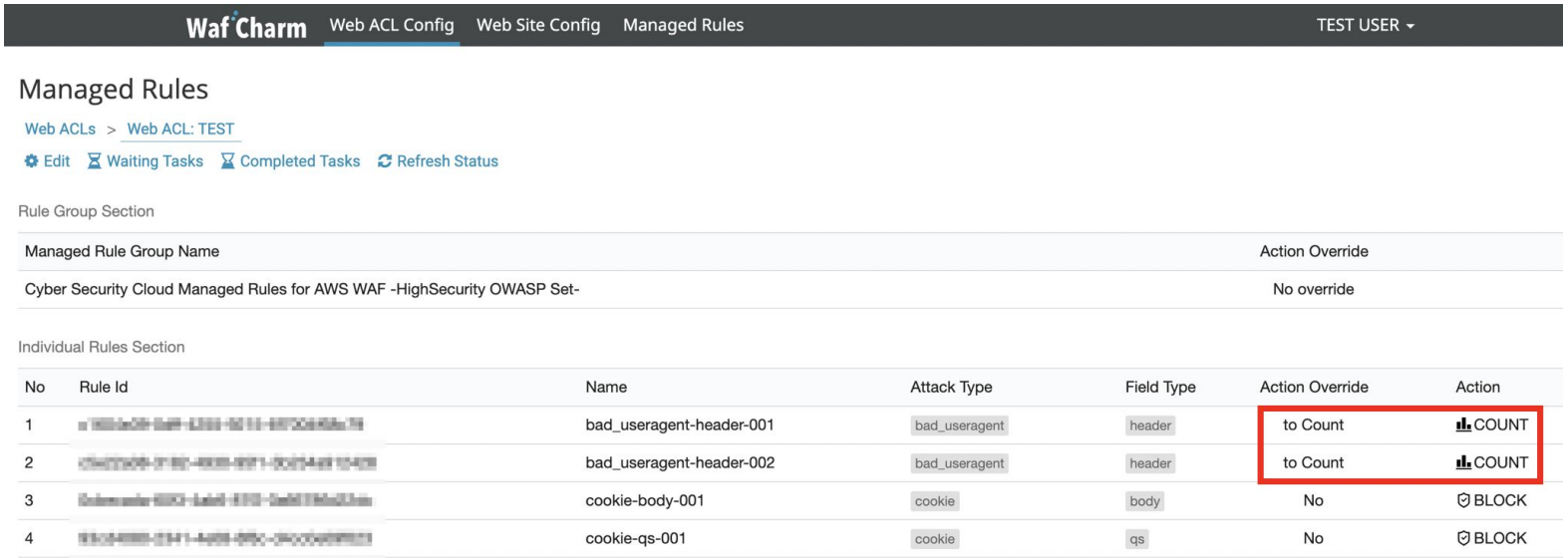
※設定の反映には 10分程度時間がかかります。
※右記 Managed Rules 画面では弊社の Managed Rules に含まれる全てのルールが表示されている訳ではなく、お客様にて制御可能なルールのみ表示されております。
その他、変更を希望するルールがあった場合は サポートにご連絡ください。



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

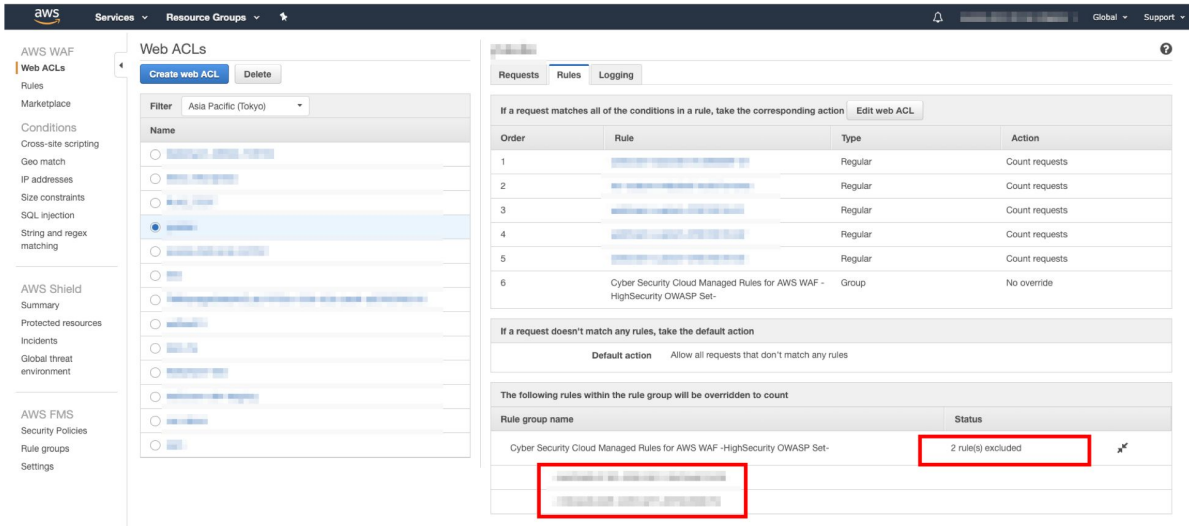
AWS マネジメントコンソール上の弊社 Managed Rules への Action の変更を実施後、左記 Managed Rules 画面に適用した状態が反映されるまで 10分程度かかります。



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)

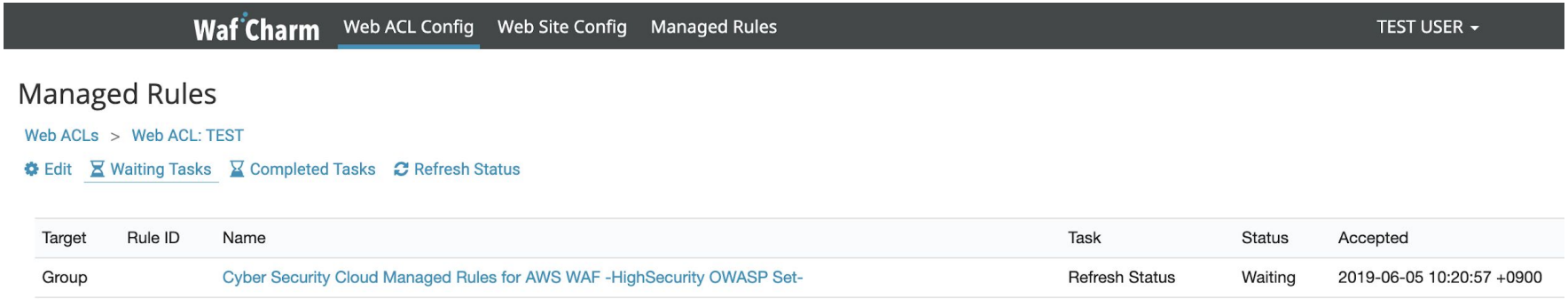


4.3 Action 変更に関する操作のステータスを確認する方法

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

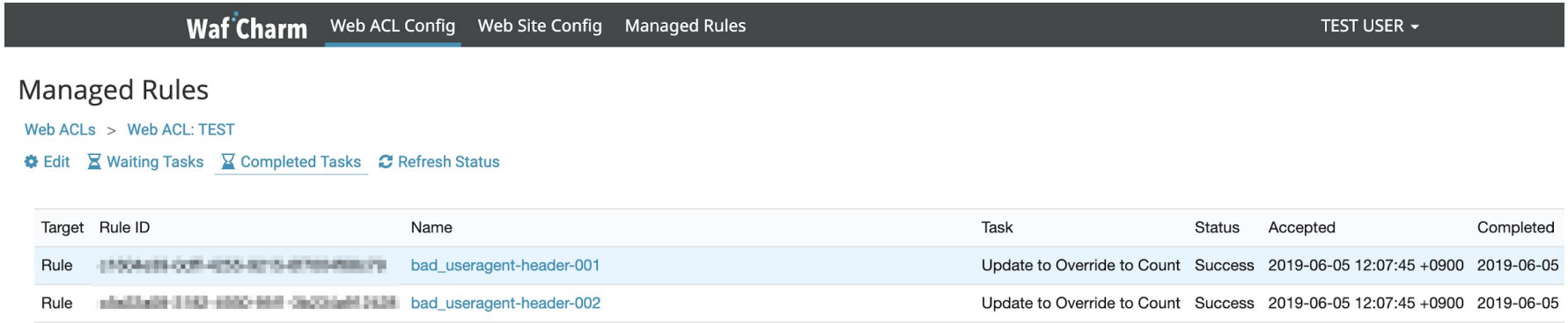


4.3 Action 変更に関する操作のステータスを確認する方法

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



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。

Waf Charm

5. 補足

Waf Charm

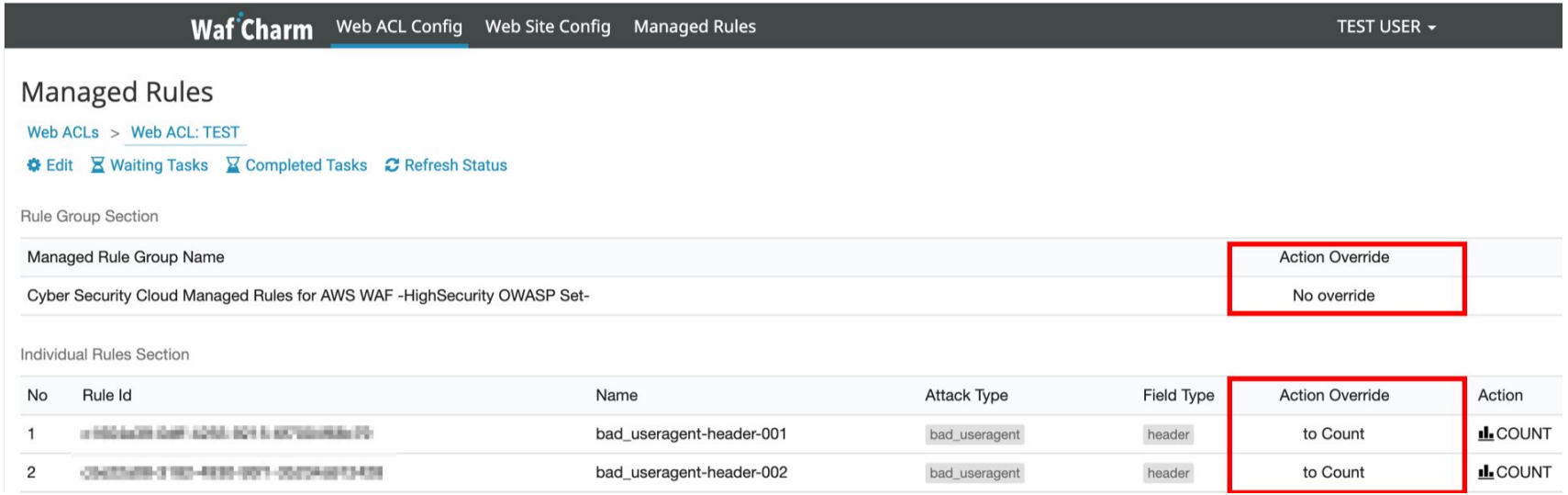
5.1 Managed Rules ページで可能な操作

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。

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。



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

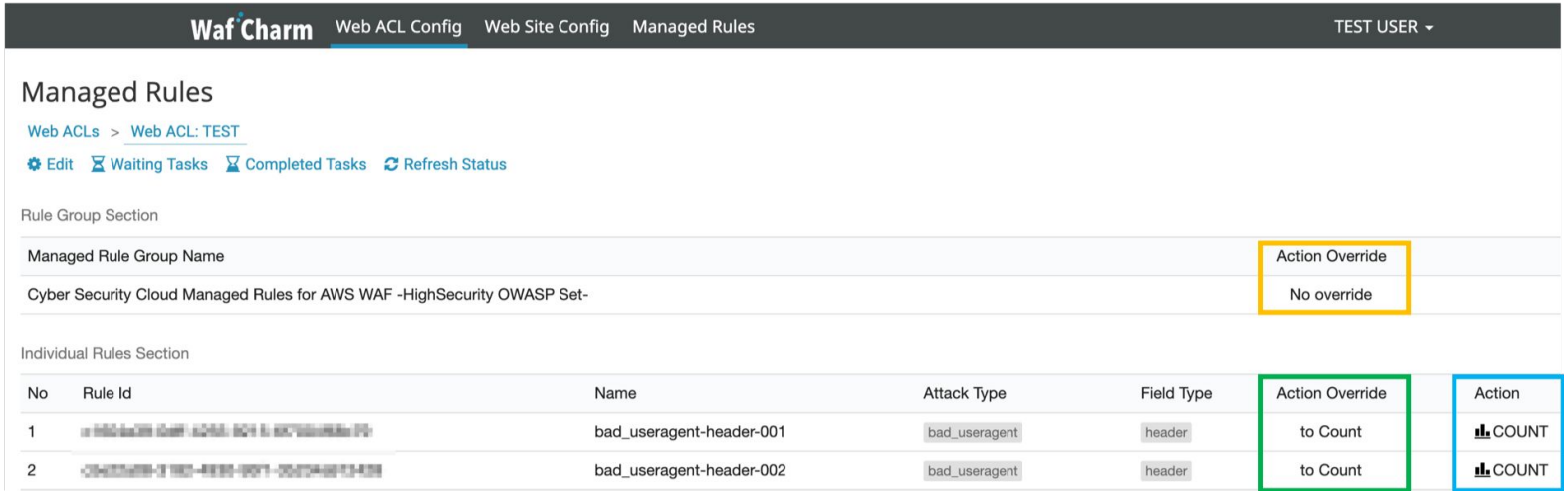
5.2.2 Indivdual Rules Section における Action Overrideの違い

- 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。



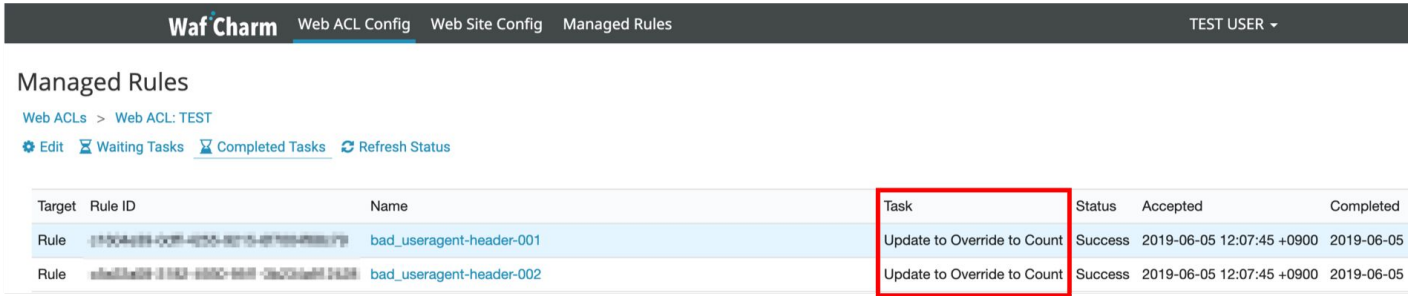
5.3.1 Action Override の組み合わせパターン

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

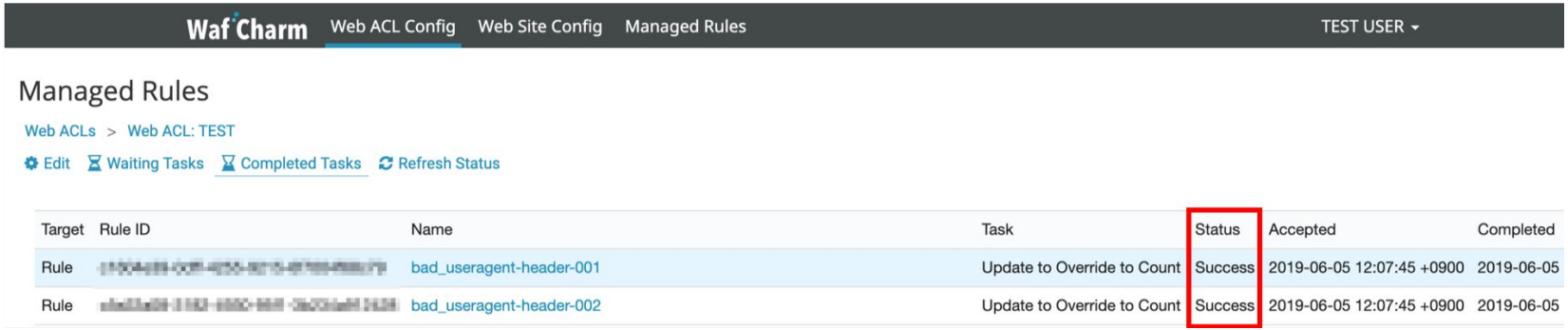
Action Override の更新をすると、WafCharm は AWS WAF への指示を Task として非同期実行するため、実行状態を赤枠部分にて確認いただく事が出来ます。



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。



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	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	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