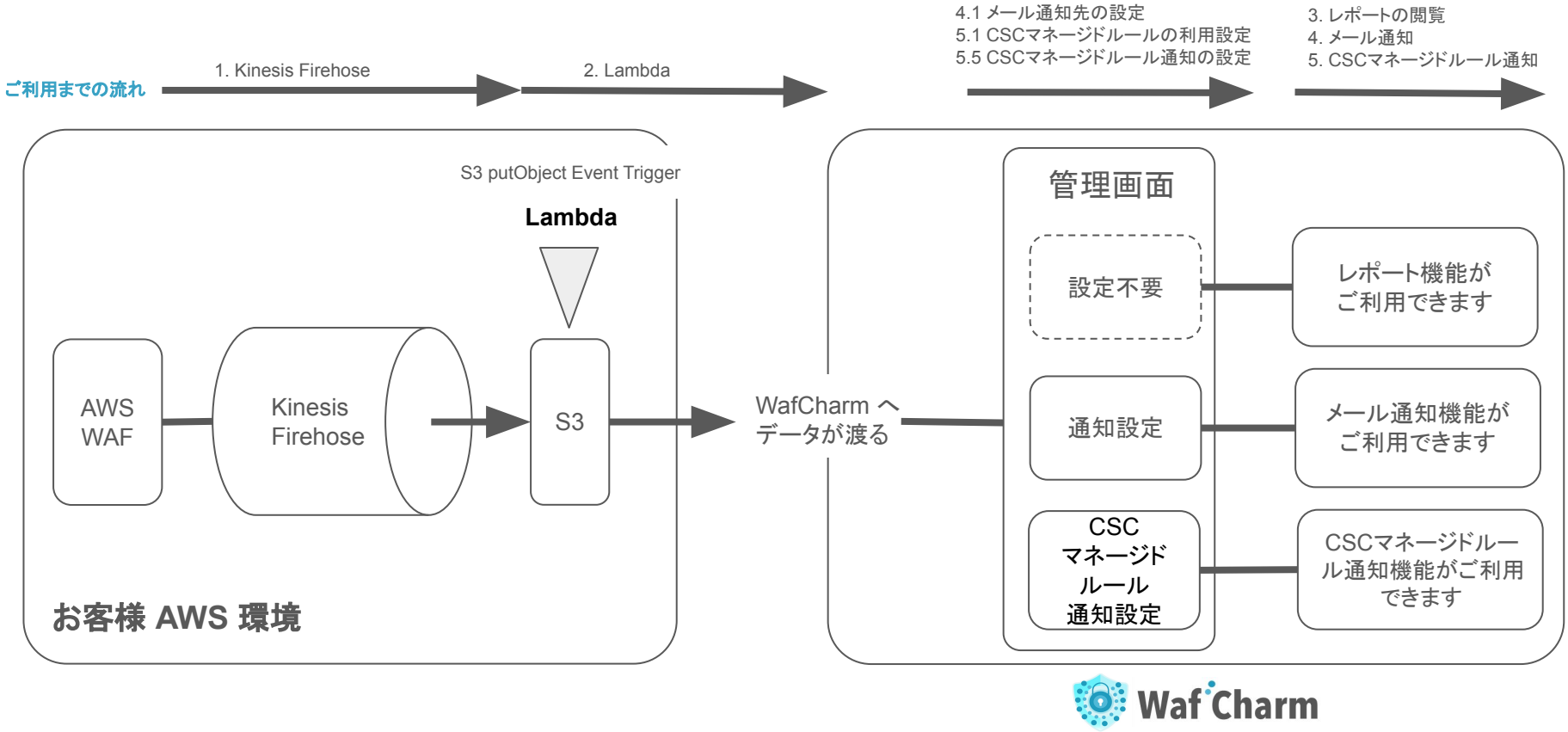
レポート機能/通知機能 利用マニュアル
AWS WAF Classic
Ver 1.6

Waf Charm

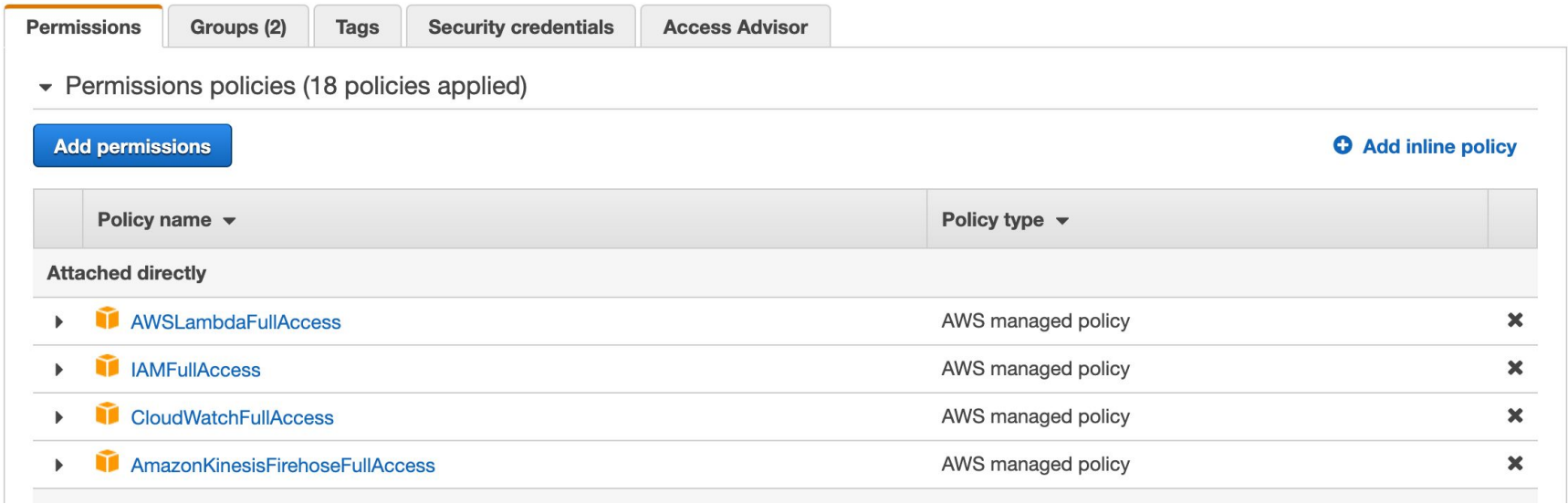
レポート機能/通知機能のアーキテクチャ概要



Waf Charm

本手順を実施頂く上で必要な権限

AWSにおいてデフォルトで用意されている権限ポリシーをご利用される場合の例となります



レポート機能/通知機能の作業概要 (1/2)

レポート機能、および通知機能をご利用されたい場合には、まずはお客様 AWS環境にて下記 1 と 2 の作業を完了させる必要があります

1. Kinesis Firehose
    - Kinesis Firehose の構築/設定
    - Kinesis Firehose 実行用の role 設定
    - Kinesis FirehoseとAWS WAFとの連携設定
    - 1章の完了確認
2. Lambda
    - WAFLog 出力先 S3 の read 権限 policy 作成
    - WafCharm 連携用 S3 の put 権限 policy 作成
    - WafCharm 連携用 Lambda の role 作成
    - Lambda 構築/設定
3. レポート機能をご利用される場合
    - WafCharm 管理画面にて、月次レポートの閲覧

レポート機能/通知機能の作業概要 (2/2)

１と２の作業が完了しましたら、ご利用されたい機能別に設定すべき事項が異なりますので、本マニュアルに沿って機能をご利用ください

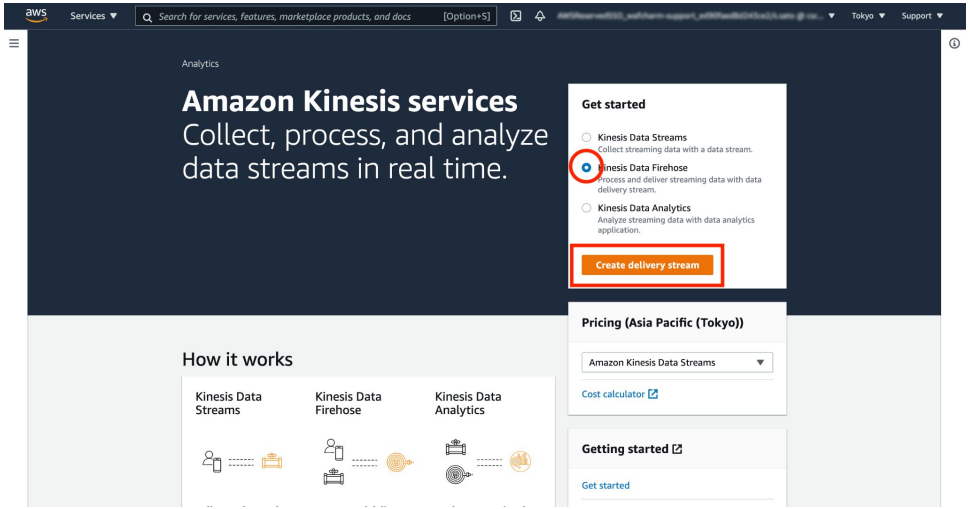
4. メール通知機能をご利用される場合
    - メール通知先の設定
    - メール通知の設定
    - メール通知内容
5. CSCマネージドルール通知機能をご利用される場合
    - CSC マネージドルールの利用設定
    - CSC マネージドルール通知の設定
    - メール通知内容
6. 通知機能に関する補足事項
7. その他補足事項

1. Kinesis Firehose

WAF ログを S3 に転送する Kinesis Firehose を設定

- Kinesis Firehose の構築/設定
- Kinesis Firehose 実行用の Role 設定
- Kinesis Firehose と AWS WAF との連携設定
- 1 章の完了確認

1.1. Kinesis Firehose 設定

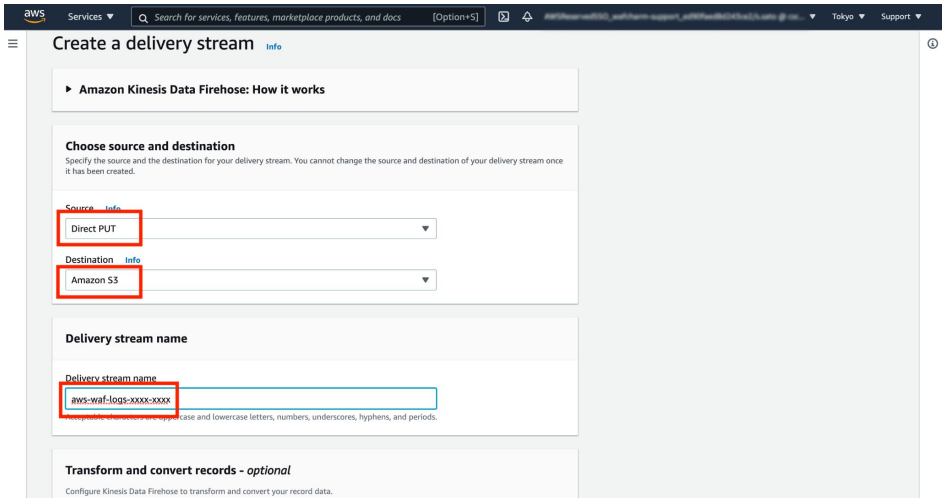


「Get started」より「Kinesis Data Firehose」を選択し、「Create delivery Stream 」をクリックします

適用予定のAWS WAF(Web ACL) と同じリージョンで作成

※ CloudFront でのご利用の方はリージョンを「バージニア」にして作業を進めてください

1.2. Kinesis Firehose 設定



「Choose source and destination」

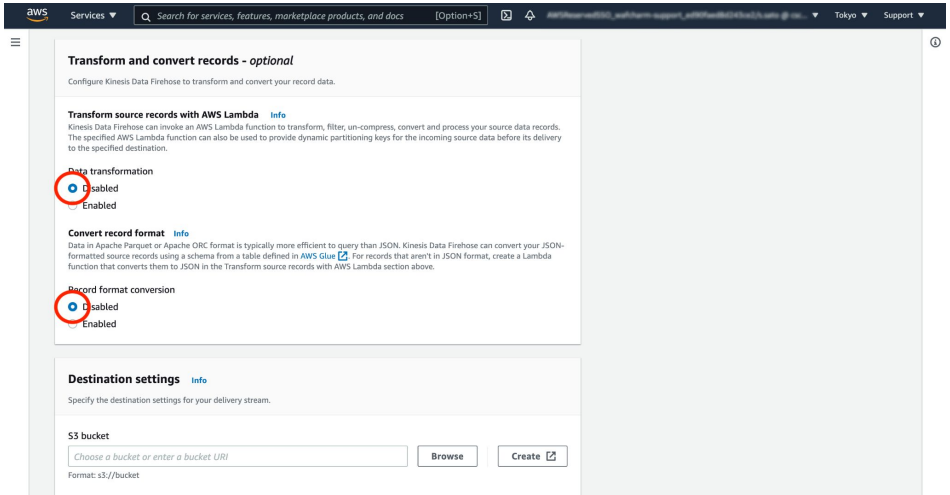
Source：Direct PUT

Destination：Amazon S3

Delivery Stream Name :
aws-waf-logs-<任意の文字列>

※ Delivery Stream Name は、先頭に ”aws-waf-logs-” を付けるという制限がありますので、ご注意ください

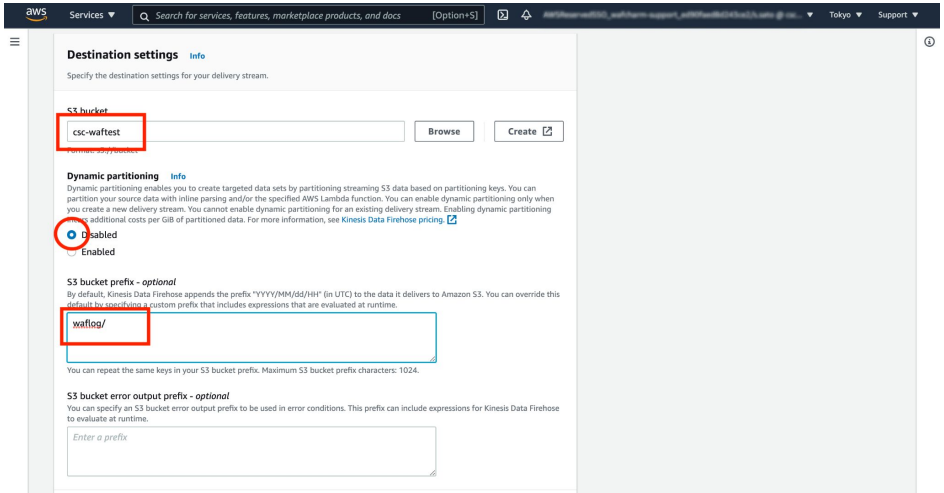
1.3. Kinesis Firehose 設定



下記は使用しません（Disabled）

- Transform source records with AWS Lambda
- Convert record format

1.4. Kinesis Firehose 設定

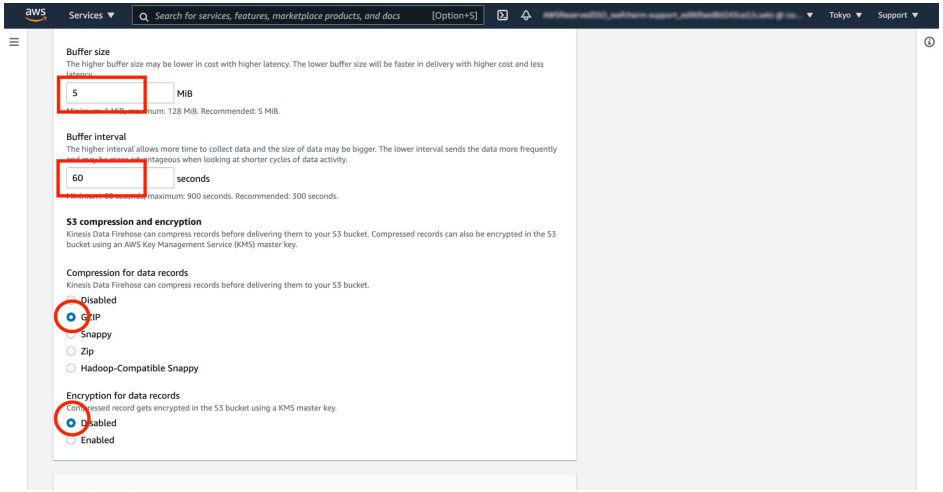


S3 bucket :
任意の S3bucket を指定 (ex : csc-waftest)

Prefix :
任意の Prefix を指定 (ex : waflog/)

※ Prefix は、「 waflog/ 」というように必ず「 / 」を付けるようにしてください

1.5. Kinesis Firehose 設定



Buffer intervals :
推奨は 60 seconds

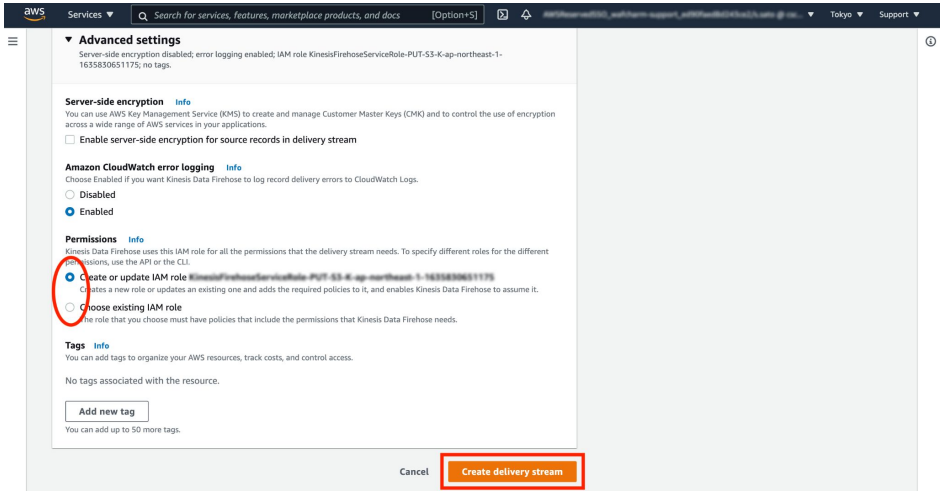
Buffer size :
推奨は 5 MB

※ Buffer intervals、またはBuffer size に達した時点で S3 にログが作成されます

S3 compression :
GZIP

S3 encryption :
Disable

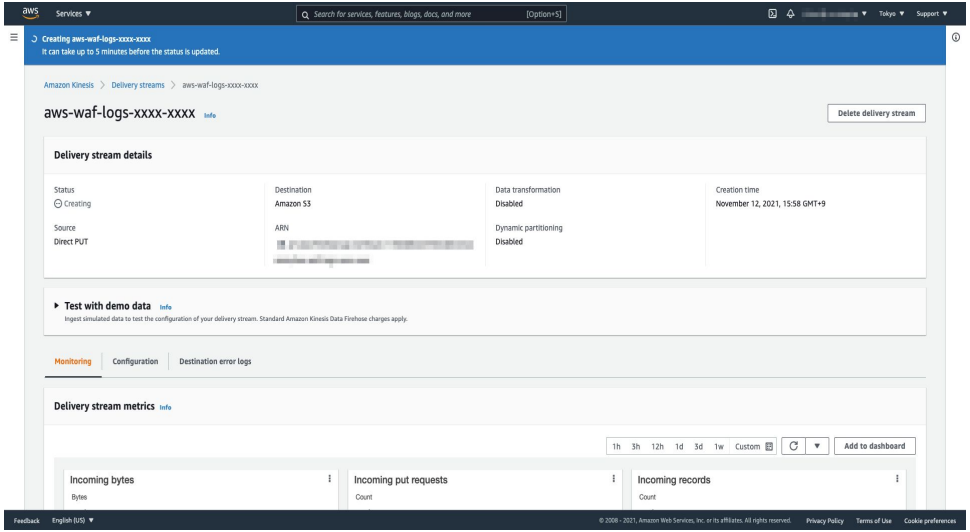
1.6. IAM role 設定



IAM Role : 新しいIAM ロールの作成 or 選択

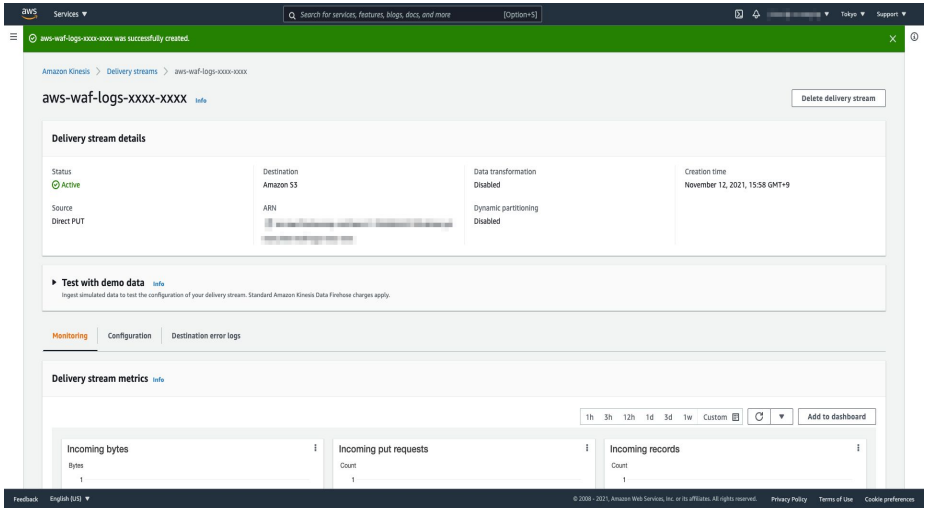
「Create delivery stream」

1.7. Kinesis Firehose 設定



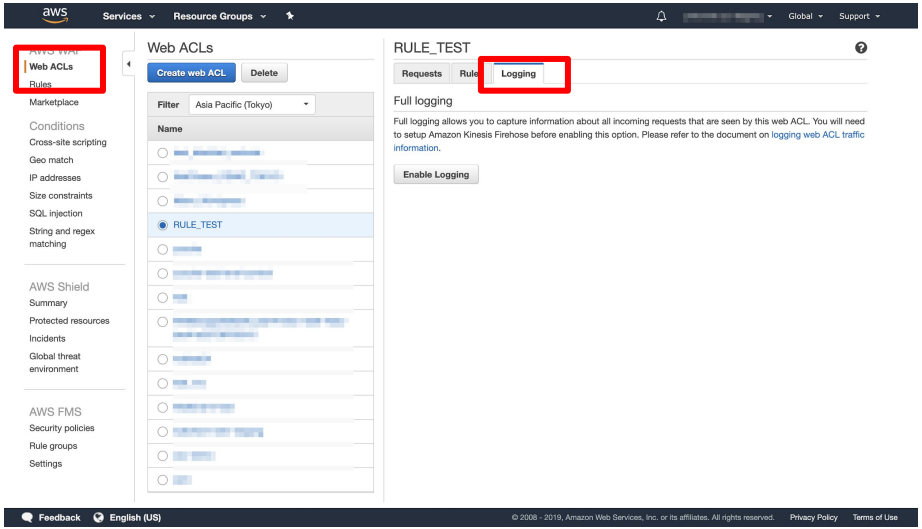
待機

1.8. Kinesis Firehose 設定



完了

1.9. Kinesis Firehose と AWS WAF との連携設定

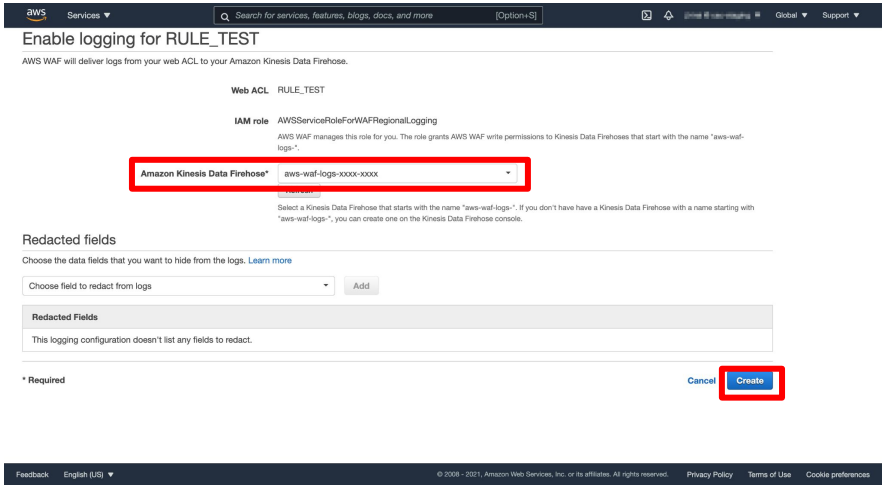


サービス “AWS WAF” に戻り

“Web ACLs” > “Logging” を選択

「Enable Logging 」

1.10. Kinesis Firehose と AWS WAF との連携設定

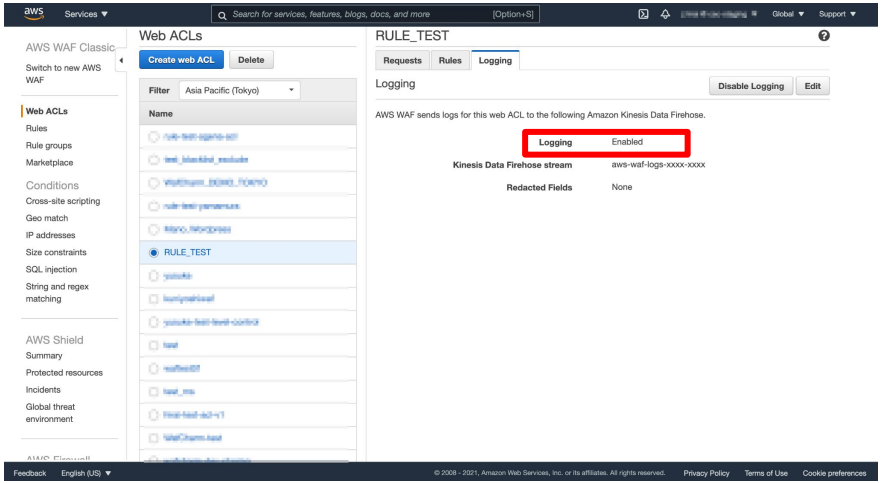


Amazon Kinesis Data Firehose には自身で命名した Delivery Stream Name を選択

※ 1.2 で指定したもの

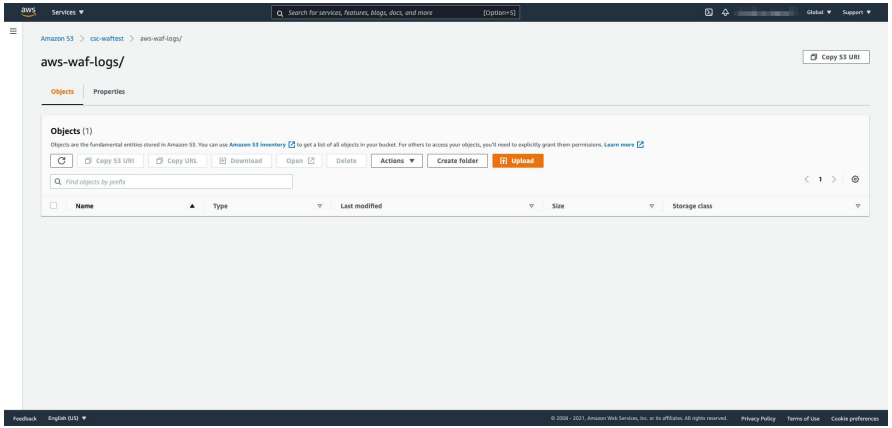
「Create」

1.11. Kinesis Firehose と AWS WAF との連携設定



Logging が、”Enabled” になっていることを確認

1.12. 1 章の完了確認

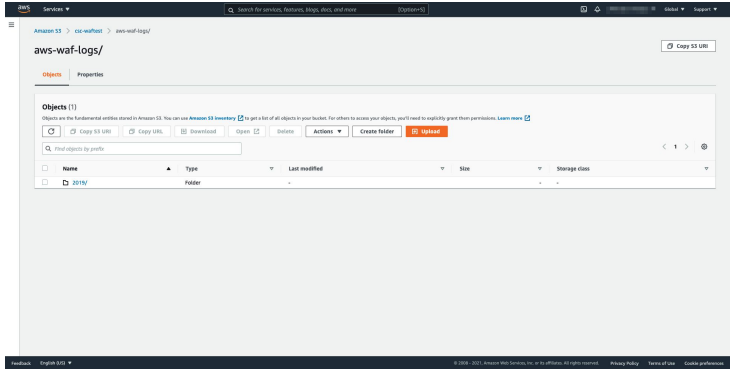


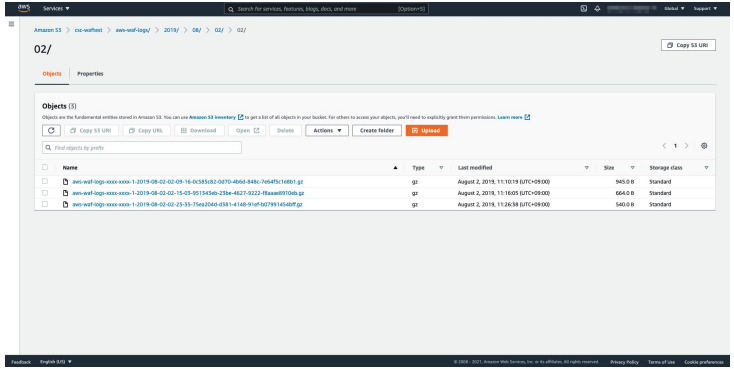
S3 に WAF ログファイルが生成されているか確認

※ 1.4 で指定したもの

左記の状態ではまだ検知がされておらず、ファイルが生成されていない状態

1.13. 1 章の完了確認





左記のようなファイルが生成されれば

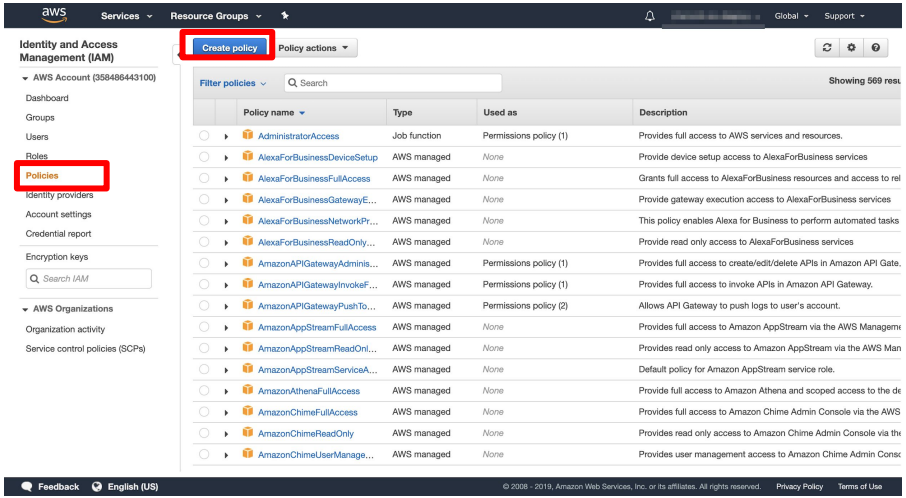
1 章の作業は完了

2. Lambda

顧客側の S3 に出力されたファイルを CSC 側の S3 に転送する設定

- WAFLog 出力先 (顧客側 S3) の read 権限 policy 作成
- WafCharm 連携用 (CSC 側 S3) の put 権限 policy 作成
- WafCharm 連携 Lambda 用の role 作成
- Lambda 構築
- CloudWatch ログ設定変更 (Lambda 出力ログ) ※ 任意

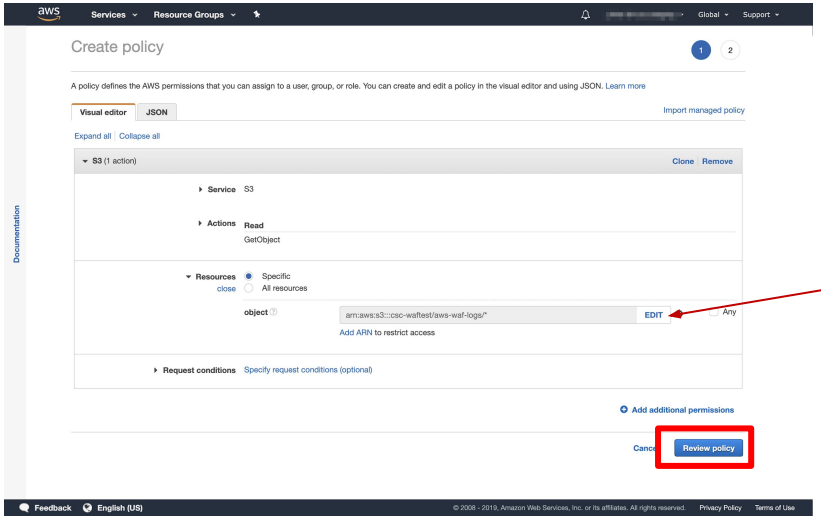
2.1. WAFLog 出力先 read 権限 policy 作成



サービス “IAM” より

“Policy” > “Create policy” を選択

2.2. WAFLog 出力先 read 権限 policy 作成



Service : S3

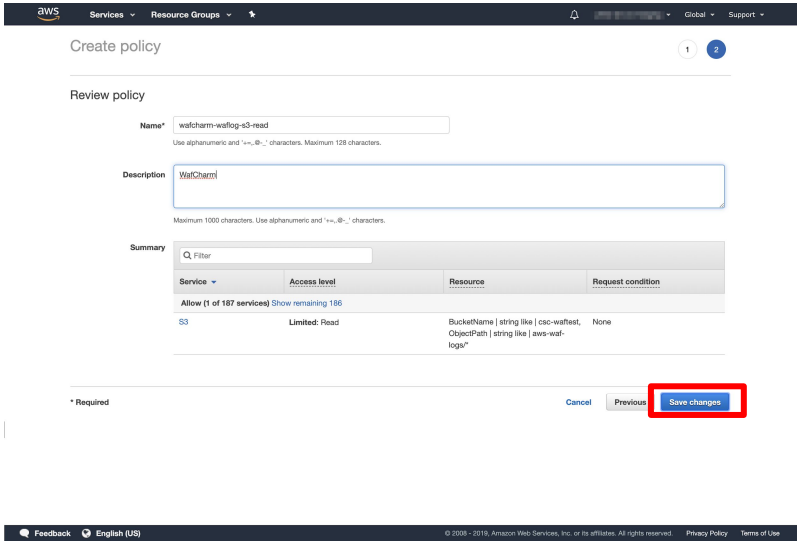
Action : GetObject

Resources :
arn:aws:s3:::csc-waftest/waflog/*
※ 1.4 で設定した内容

※ Resources に指定するパスには必ず “ /* ”を付けること

「Review policy」

2.3. WAFLog 出力先 read 権限 policy 作成

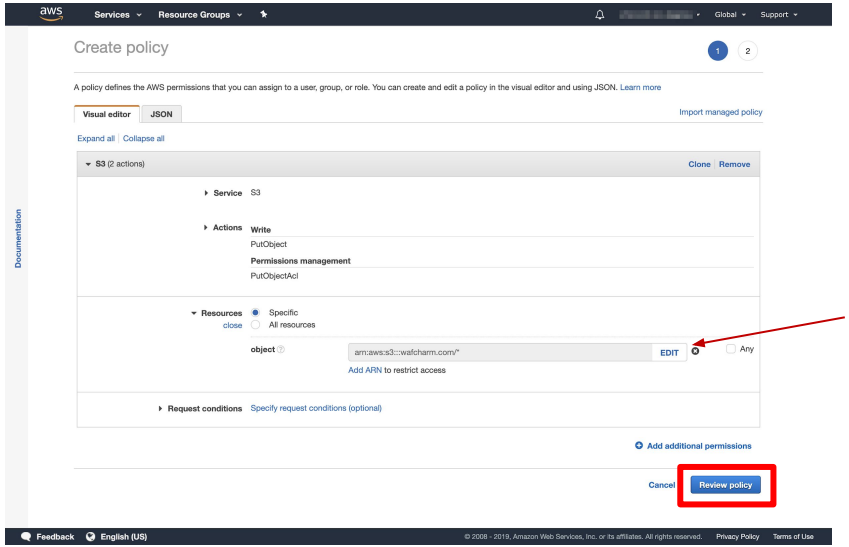


Name:
wafcharm-waflog-s3-read (任意の名前)

Description : WafCharm (任意)

「Create policy」

2.4. WafCharm 連携用 put 権限 policy 作成



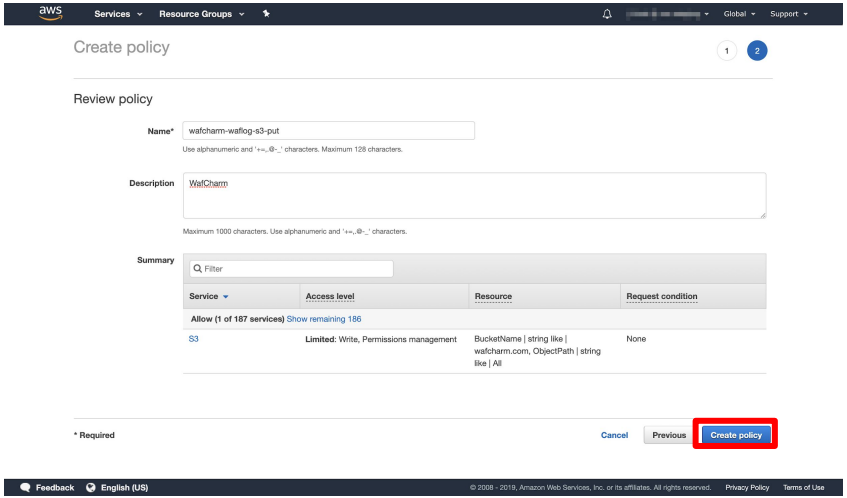
Service : S3

Action : PutObject, PutObjectACL

Resources :
arn:aws:s3:::wafcharm.com/*
※ CSC 側の S3 に対する権限

「Review policy」

2.5. WafCharm 連携用 put 権限 policy 作成

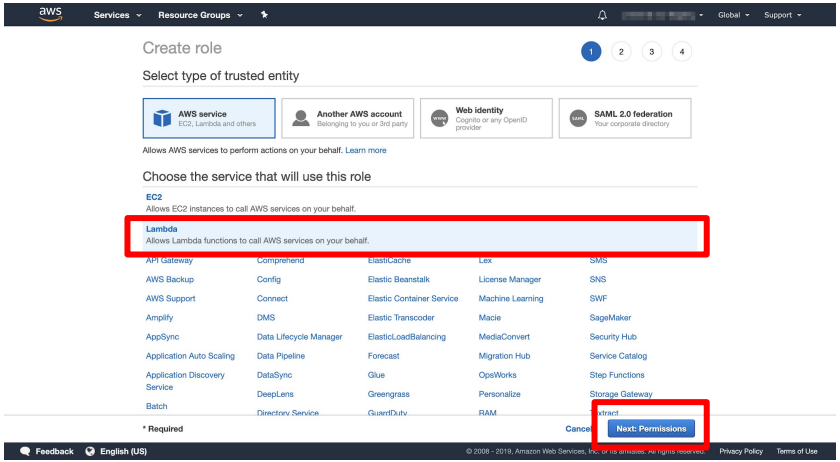


Name :
wafcharm-waflog-s3-put (任意の名前)

Description : WafCharm (任意)

「Create policy」

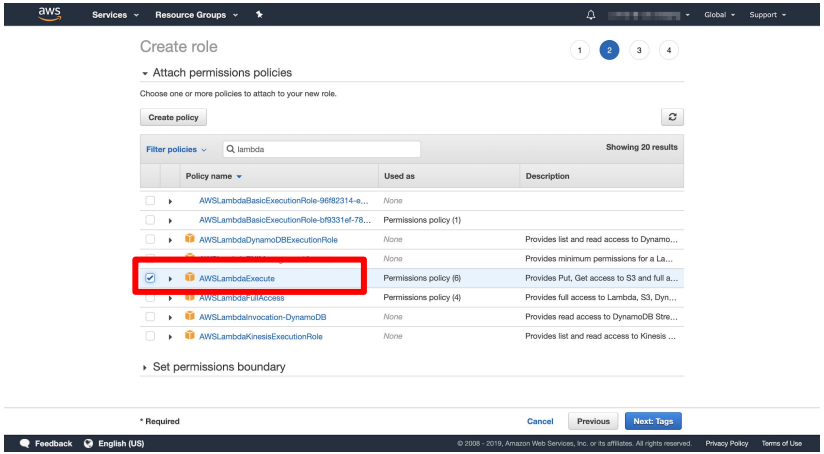
2.6. WafCharm 連携 Lambda 用 role 作成



このロールを使用するサービスを選択 ：Lambda

「Next: Permissions」

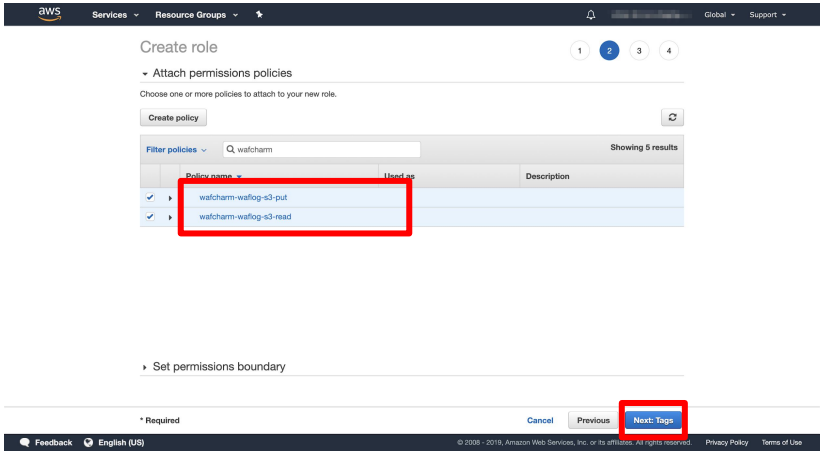
2.7. WafCharm 連携 Lambda 用 role 作成



フィルターに「lambda」を入力し、一覧の中から

「AWSLambdaExecute」を選択

2.8. WafCharm 連携 Lambda 用 role 作成



フィルターに「wafcharm」を入力し、一覧の中から

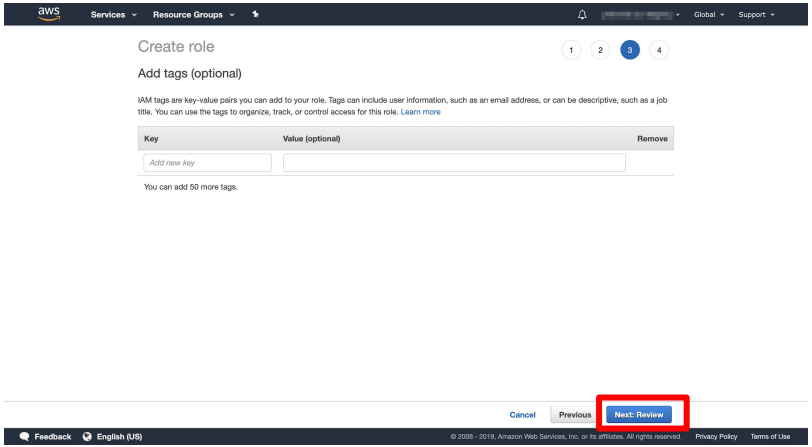
「wafcharm-waflog-s3-put」
「wafcharm-waflog-s3-read」

を選択

※ 2.3, 2.5で作成した policy

「Next: Tags」

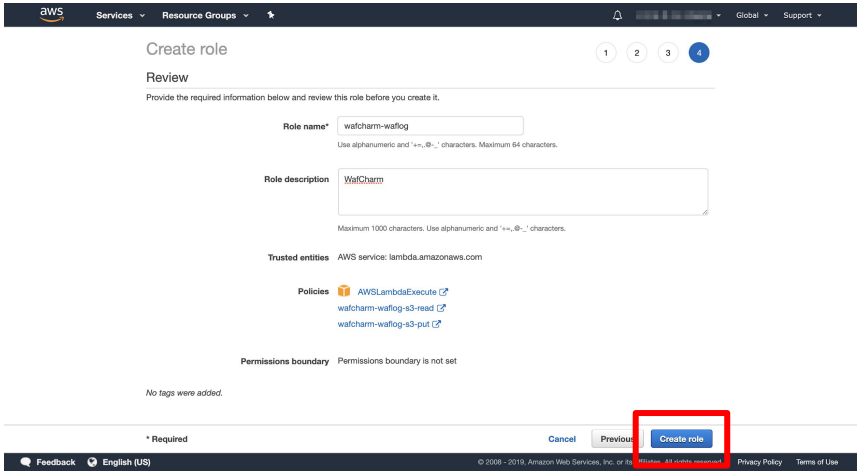
2.9. WafCharm 連携 Lambda 用 role 作成



タグの追加は任意

「Next: Review」

2.10. WafCharm 連携 Lambda 用 role 作成

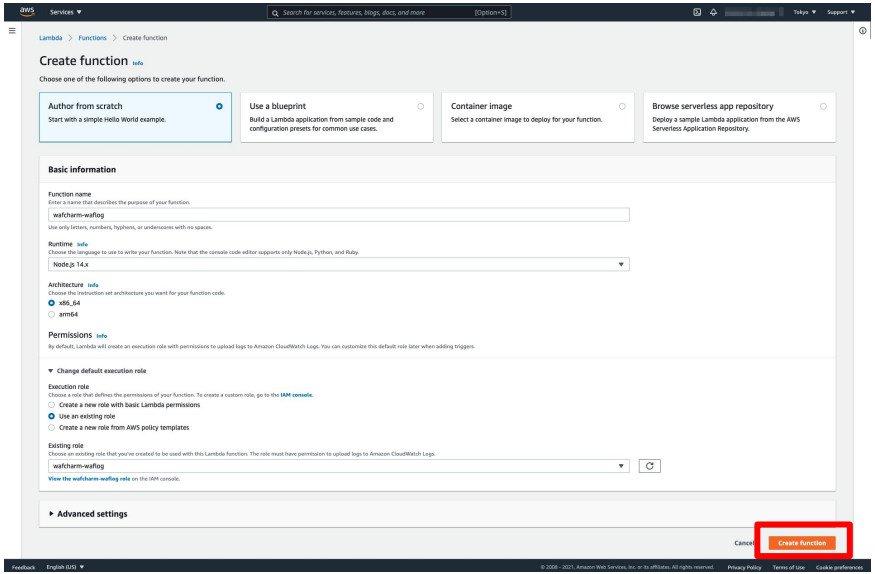


Role name:
wafcharm-waflog (任意)

Role description :
WafCharm (任意)

「Create role」

2.11. Lambda 構築



名前：wafcharm-waflog (任意)

Runtime : Node.js 12.x ~ Node.js 18.x

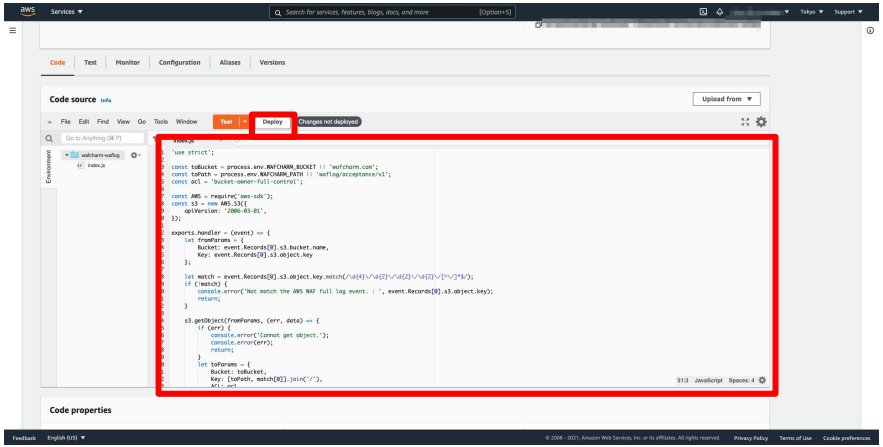
Execution Role : Use an existing role

既存のロール：wafcharm-waflog
※ 2.10 で作成したもの

※ 1.4 で指定した S3 のバケットと同じリージョンで作成してください

「Create function」

2.12. Lambda 構築 (関数コード)



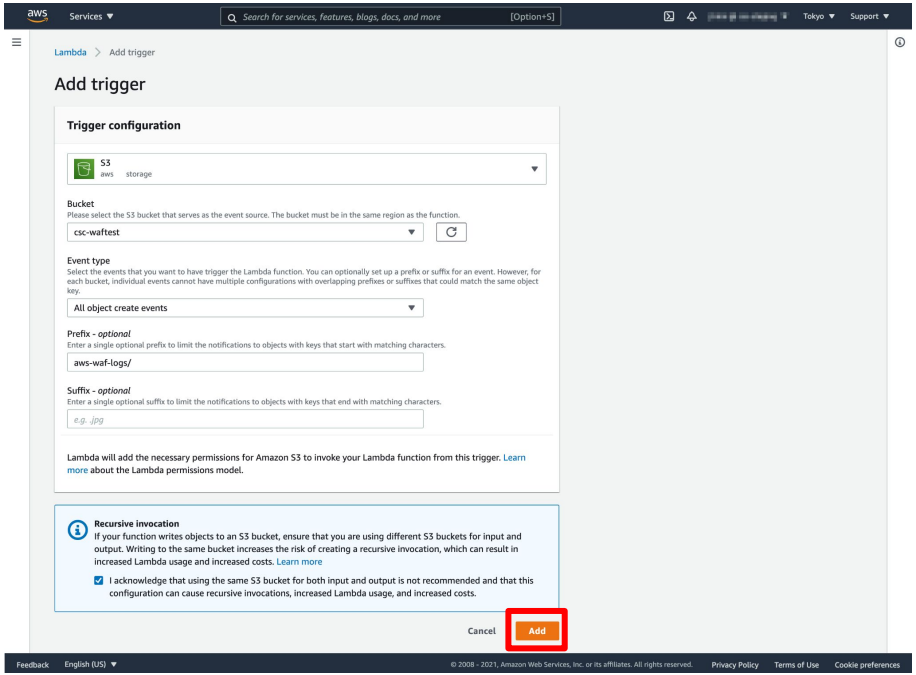
Code source:
以下のソースを貼り付け
http://docs.wafcharm.com/manual/classic_aws_waf/index.js

※ ソースは AWS WAF のバージョンで異なりますのでご注意ください

※ Node.js 18.xをご利用頂く場合にはファイル名をindex.mjs から index.js へ変更してください。

「Deploy」

2.13. Lambda 構築 (トリガー)



Add trigger :
トリガーに S3 を選択

トリガーの設定

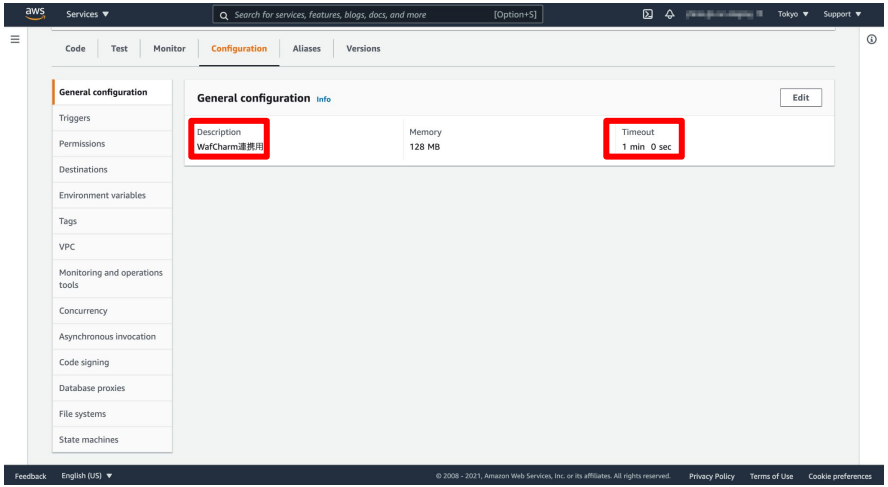
バケット: 1.4 で設定した S3 bucket

イベントタイプ：オブジェクトの作成（すべて）

プレフィックス：1.4 で設定した prefix

「Add」

2.14. Lambda 構築

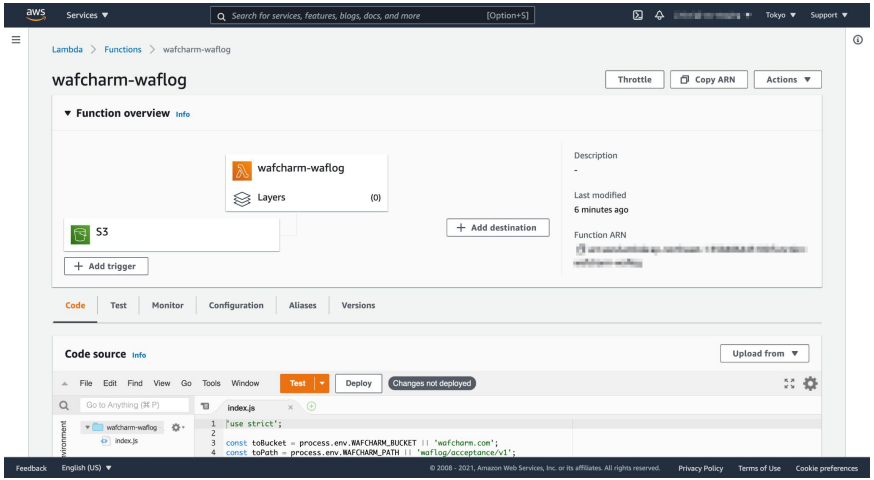


General configuration:

Timeout : 1 分

Description : WafCharm 連携用 (任意)

2.15. Lambda 構築



完了

2.16. CloudWatch

Lambda 関数実行後でないと作成されません

AWS コンソール > CloudWatch > ロググループを選択

“次の期間経過後にイベントを失効 “カラムの値が

デフォルト値：“失効しない”

となっているため

必要に応じてログの保存期間を変更してください

3. レポート機能をご利用される場合

レポート機能をご利用頂くには、以下の条件が満たされる必要があります

1. １～２章までの設定が完了している

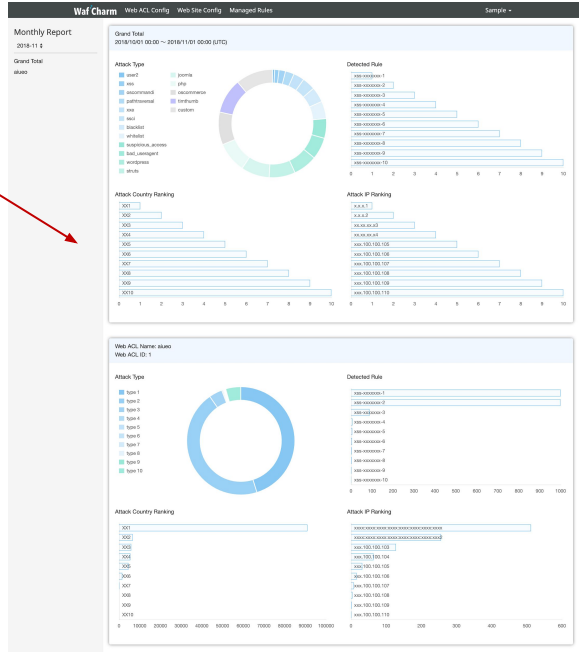
2. 前月に検知があった

※ 前月に検知がなかった方 -> 月次レポートが作成されません

3.1. WafCharm 管理画面にて月次レポートの閲覧

WafCharm 管理画面

右上のメニューより、「Report」を選択



※ レポートは、毎月初旬に前月分が閲覧可能

※ 上記レポートはイメージです

4. メール通知機能をご利用される場合

1 ～ 2 章までの設定が完了し、さらに WafCharm 管理画面にて通知先の設定、通知 ON にするとメールによる検知内容の通知が開始されます

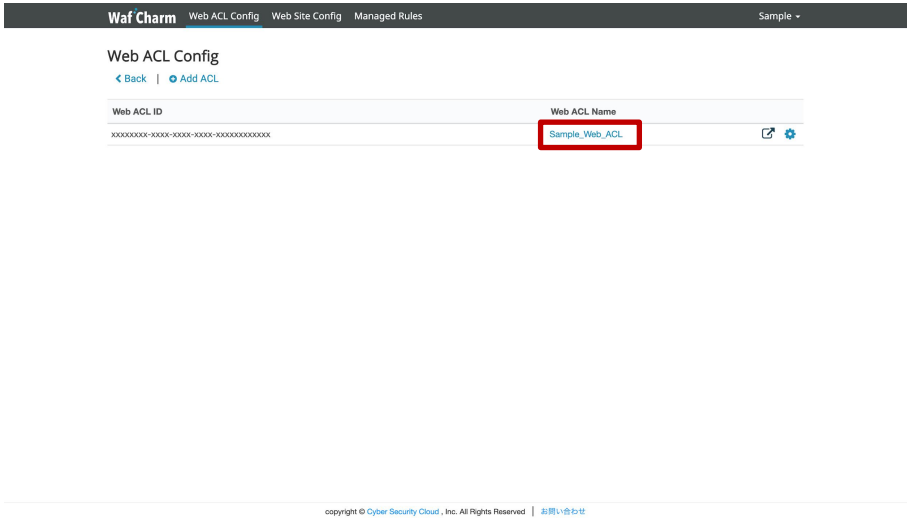
- メール通知先の設定
- メール通知の設定
- メール通知内容

4.1. メール通知先の設定

WafCharm 管理画面

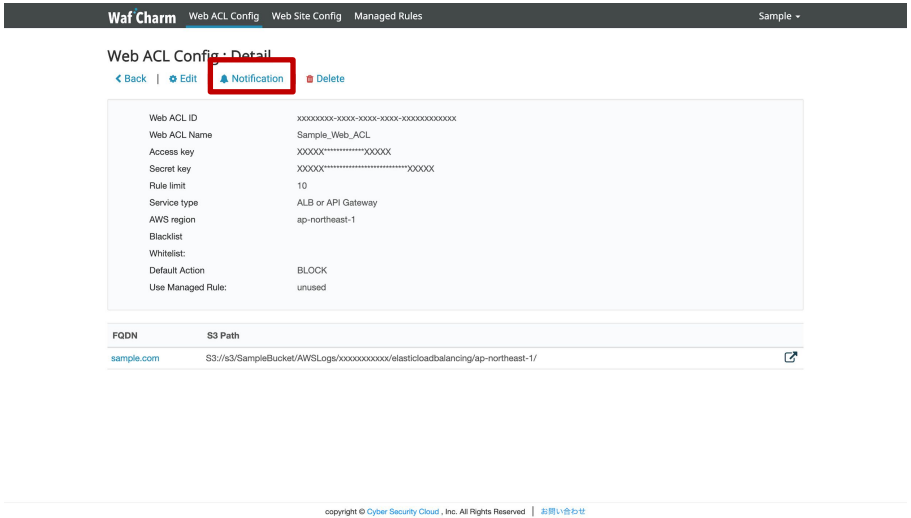
上部メニューより、「Web ACL Config」を選択

4.2. メール通知先の設定



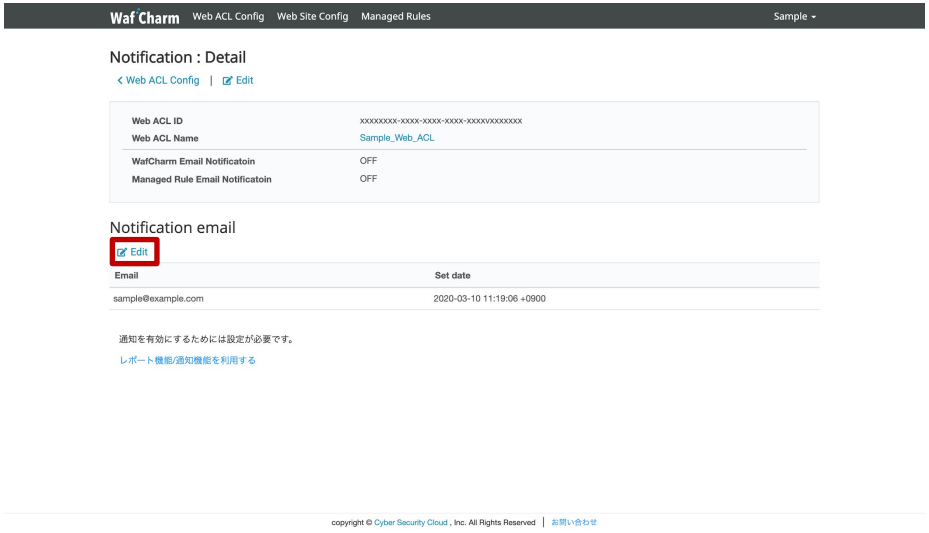
対象の「Web ACL Name」を選択

4.3. メール通知先の設定



「Notification」を選択

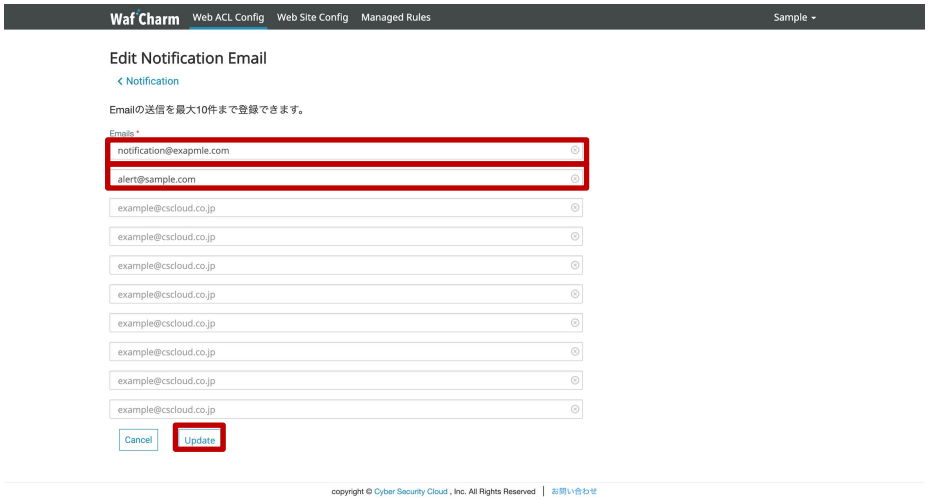
4.4. メール通知先の設定



「Notification email」の「Edit」を選択

※ デフォルトは WafCharm 管理画面へのログイン用メールアドレスが設定されています

4.5. メール通知先の設定

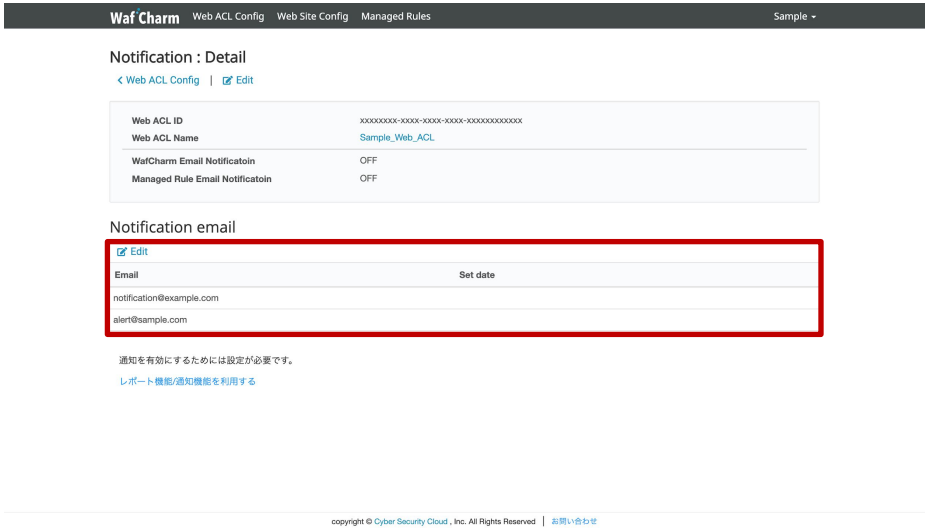


「Emails」に任意のメールアドレスを設定し、

「Update」

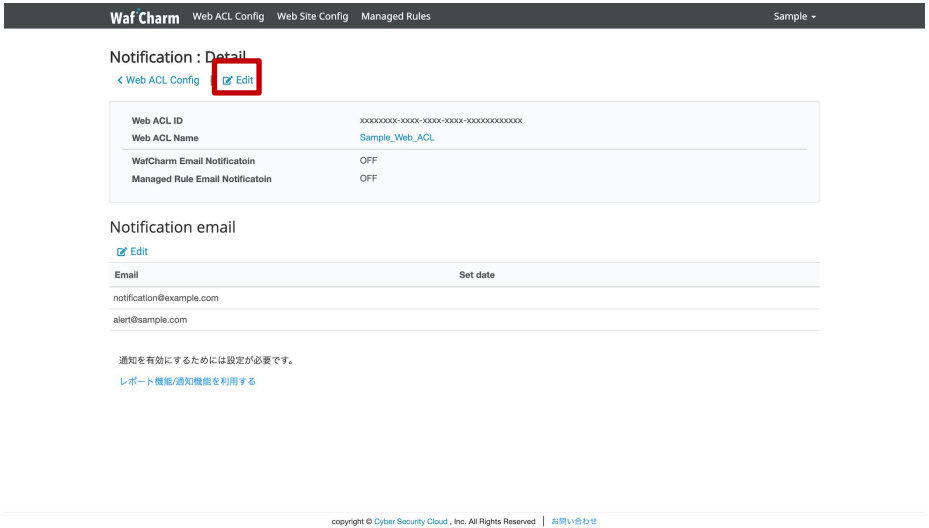
※ 最大 10 件まで登録可

4.6. メール通知先の設定



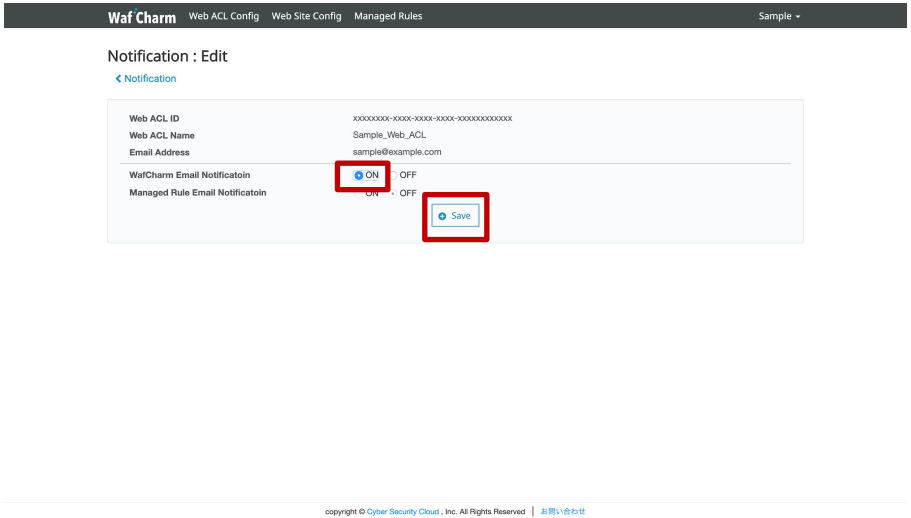
「Notification email」が設定したメールアドレスに更新されていることを確認

4.7. メール通知の設定



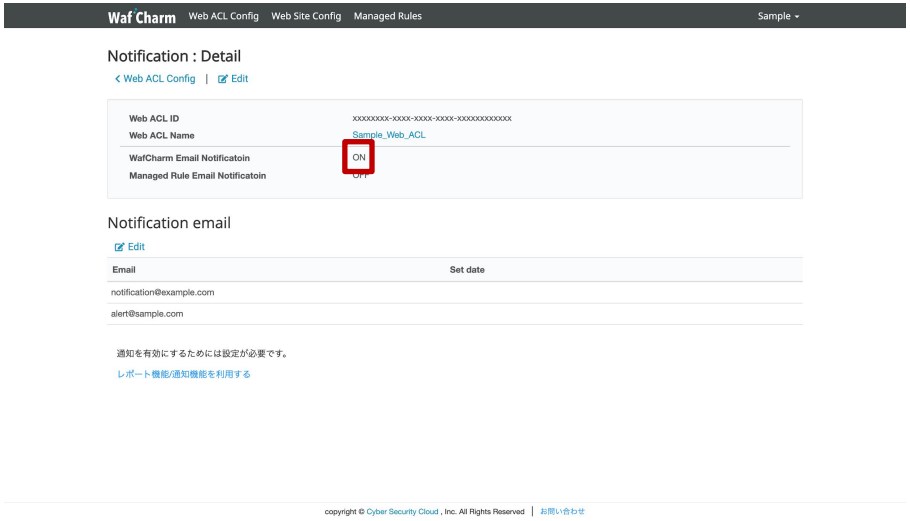
「Edit」を選択

4.8. メール通知の設定



「WafCharm Email Notificaition」を「ON」に変更し、「save」

4.9. メール通知の設定



「WafCharm Email Notificaition」が「ON」になっていることを確認

4.10. メール通知内容

検知 (BLOCK/COUNT) された場合、下記のメールが送信されます

- メールタイトル： WafCharm Attack Detected.
- メール差出人：WafCharm Notification wafcharm-notification@cscloud.co.jp
- メール宛先：WafCharm Notification wafcharm-notification@cscloud.co.jp
- メールBCC先：「Notification email」に登録されているメールアドレス (4.6)

Attacks as follows were detected.
This report includes up to 10 attacks detected in every buffer interval.
If you need to check more information and attacks, visit your AWS console.

WebACL Name(Web ACL ID): < お客様 のWeb ACL Name> (< お客様 のWeb ACL ID>)

Matches Rule: wafcharm-blacklist-010090004-07 (<Rule ID>)
Time(UTC): Thu, 01 Apr 2020 20:20:00 GMT
Source IP: XXX.XXX.XXX.XXX
Source Country: JP
URI: /

5. CSC マネージドルール通知機能をご利用される場合

1 章 (Kinesis Firehose) 、2 章 (Lambda) の設定が完了し、CSC のマネージドルール (Cyber Security Cloud Managed Rules for AWS WAF Classic -OWASP Set-) をご利用頂いている場合、WafCharm 管理画面にて設定及び、通知 ONにするとメールによる検知内容の通知が開始されます

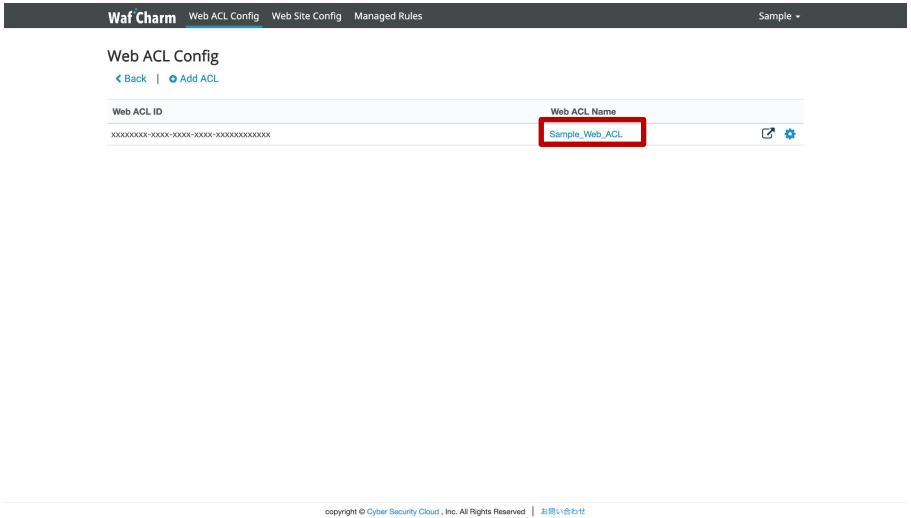
- CSC マネージドルールの設定
    - AWS WAF Managed Rules ルールグループの例外機能マニュアル（p4)
- CSC マネージドルール通知の設定
- メール通知内容

5.1. CSC マネージドルールの利用設定

WafCharm 管理画面

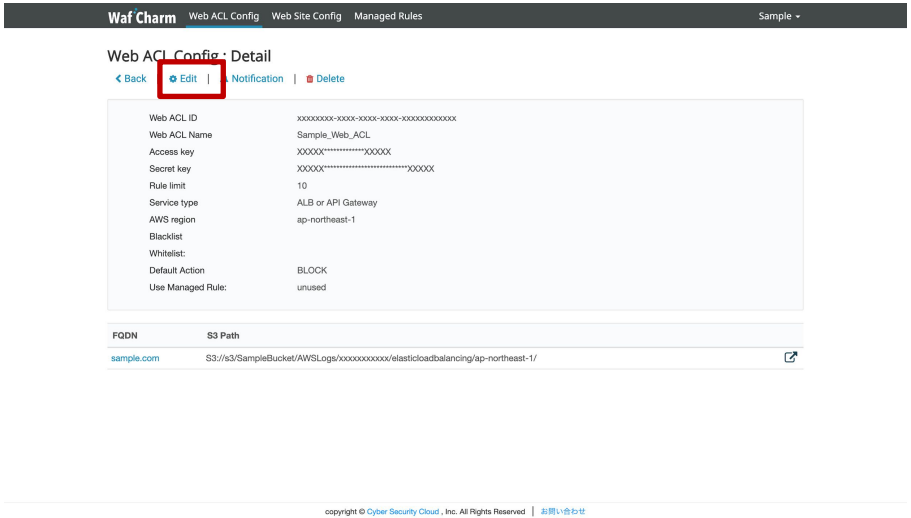
上部メニューより、「Web ACL Config」を選択

5.2. CSC マネージドルールの利用設定



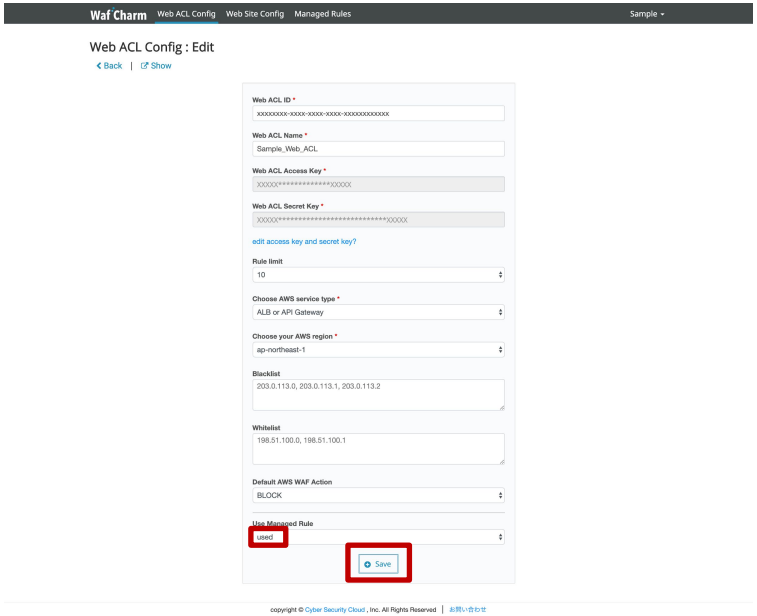
対象の「Web ACL Name」を選択

5.3. CSC マネージドルールの利用設定



「Edit」を選択

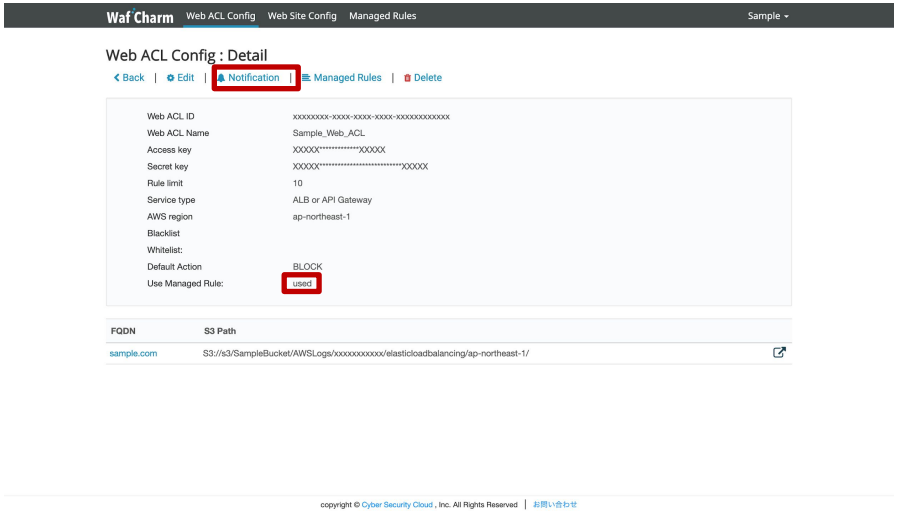
5.4. CSC マネージドルールの利用設定



「Use Managed Rule」を「used」へ変更し、

「Save」をクリック

5.5. CSC マネージドルール通知の設定



「Use Managed Rule」が「used」になっている
ことを確認

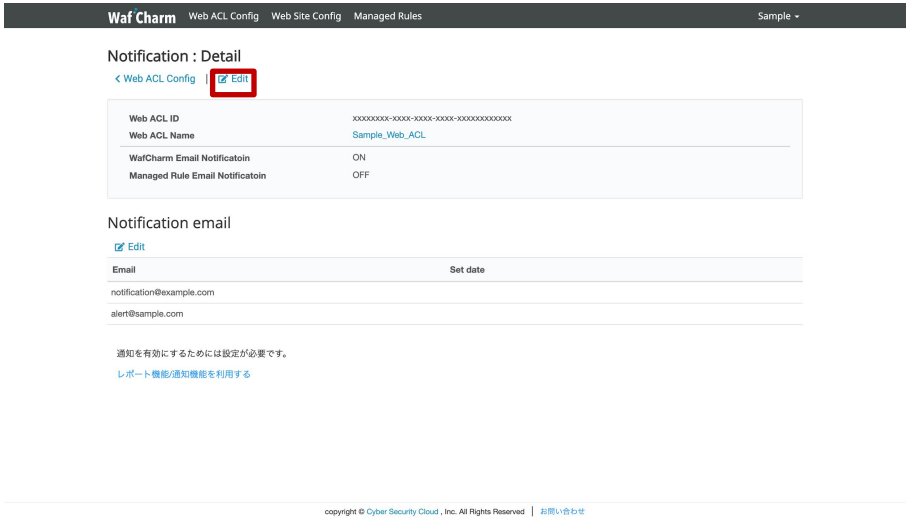
※お客様の CSC マネージドルールの利用確認に
5 ~ 10分程度かかります

設定反映確認には以下ページ参照

AWS WAF Managed Rules ルールグループの例外機能マニュアル (p11 ~ 13)

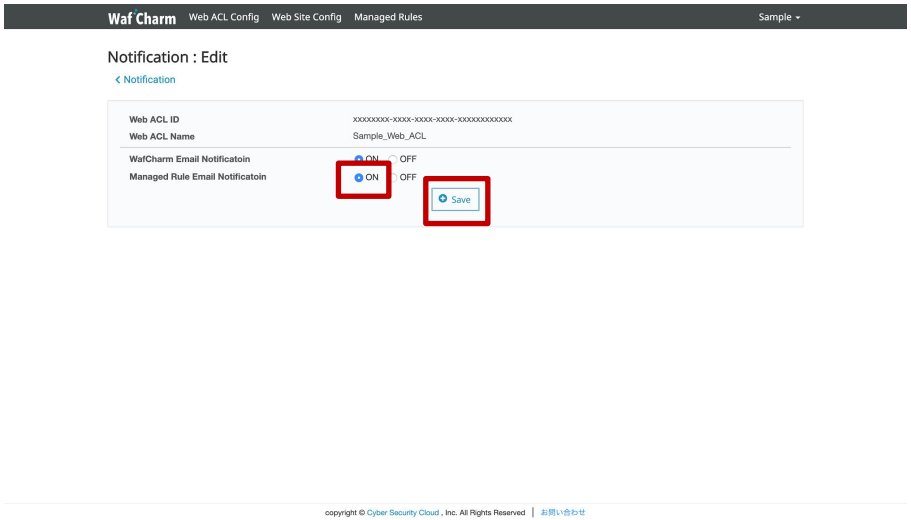
設定反映確認後、メニュー上部の「 Notification」を選択

5.6. CSC マネージドルール通知の設定



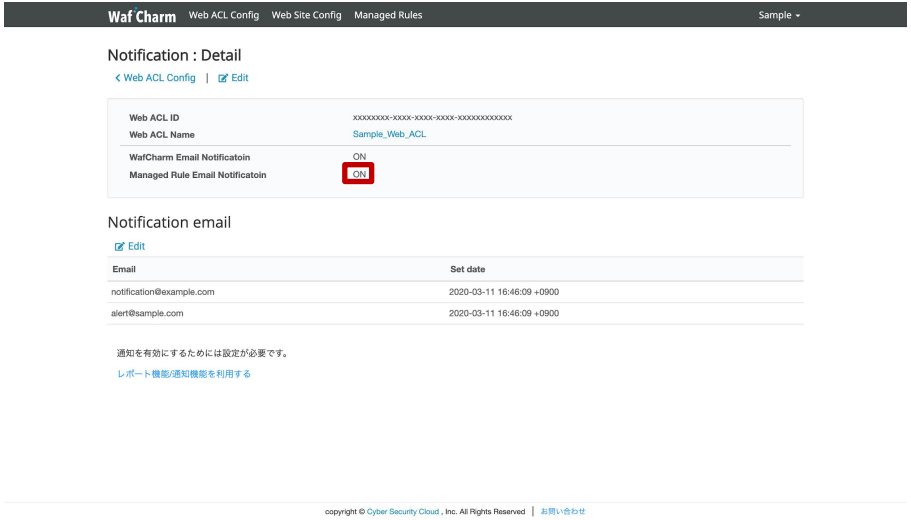
「Edit」を選択

5.7. CSC マネージドルール通知の設定



「Managed Rule Email Notificaition」を「ON」に変更し、「save」

5.8. CSC マネージドルール通知の設定



「Managed Rule Email Notificaition」が「ON」になっていることを確認

5.9. メール通知内容

検知 (BLOCK/COUNT) された場合、下記のメールが送信されます

- メールタイトル： CSC Managed Rules Attack Detected.
- メール差出人 : WafCharm Notification wafcharm-notification@cscloud.co.jp
- メール宛先 : WafCharm Notification wafcharm-notification@cscloud.co.jp
- メールBCC先 :「Notification email」に登録されているメールアドレス (4.6)

Attacks as follows were detected.
This report includes up to 10 attacks detected in every buffer interval.
If you need to check more information and attacks, visit your AWS console.

WebACL Name(Web ACL ID): < お客様 のWeb ACL Name> (< お客様 のWeb ACL ID>)

Managed Rule: Cyber Security Cloud Managed Rules for AWS WAF -HighSecurity OWASP Set-
Attack Type: suspicious_access
Field Type: url
Matches Rule Name: sample_suspicious_access-url-001
Matches Rule ID:<Rule ID>
Time(UTC): Thu, 1 Apr 2020 20:20:00 GMT
Source IP: XXX.XXX.XXX.XXX
Source Country: JP
URI: /

6. 通知機能に関する補足事項

- 以下条件が揃った場合、WafCharm の通知機能は「CSC 管理外のルールグループによる検知」として通知します
  - CSC マネージドルールを利用している
    - (Cyber Security Cloud Managed Rules for AWS WAF Classic -OWASP Set-)
  - メール通知機能 ：ON
  - CSC マネージドルール通知機能 ：OFF
  - CSC マネージドルールで検知

- 通知間隔は、1.5 Kinesis Firehose 設定 の Buffer intervals、Buffer size で設定した値に応じて変化します

- 1 メール(ログファイル)につき最大 10 件まで検知内容が記載されます

7. その他補足事項

- お客様の S3 に出力されたログファイルは必要に応じてライフサイクル機能等を用いて定期的(1ヶ月毎等) に S3 Glacier への退避や削除することを推奨します

- AWS にて対象の IP アドレスの地域を特定できていない場合、月次レポートの国名に「 - 」と出力されることがあります

- 弊社への WAF ログ転送確認をご希望の際は、事前に下記 2 点をご確認の上、1.2 にて設定した「Delivery Stream Name」と対象の Web ACL ID を共有ください
  - Kinesis Data Firehose にて指定した S3 に WAF ログが出力されていること
  - CloudWatch のイベントログに ERROR が出力されていないこと (START/END/REPORTの3行は都度出力されている)
    - ERROR の確認方法

      CloudWatch -> Log groups -> /aws/lambda/Lambda 関数名 (マニュアルの場合 : wafcharm-waflog)

      -> 最新(一番上)のLog Stream を選択 -> ERROR のメッセージ有無確認

7. その他補足事項

- Lambda 起動後にロール(ポリシー)の権限を編集した場合、動作中の Lambda に変更点が反映されない可能性があるため、index.js の最終行に空白行の追加等を行い、再度デプロイを実施してください

- WafCharm に AWS WAF のバージョンが異なる Web ACL を登録し、各 Web ACL にて本機能を利用する場合、Kinesis Data Firehose、及び Lambda はバージョン毎に作成してください
    - 同じバージョンの場合、Kinesis Data Firehose、及び Lambda を共有することは可能です