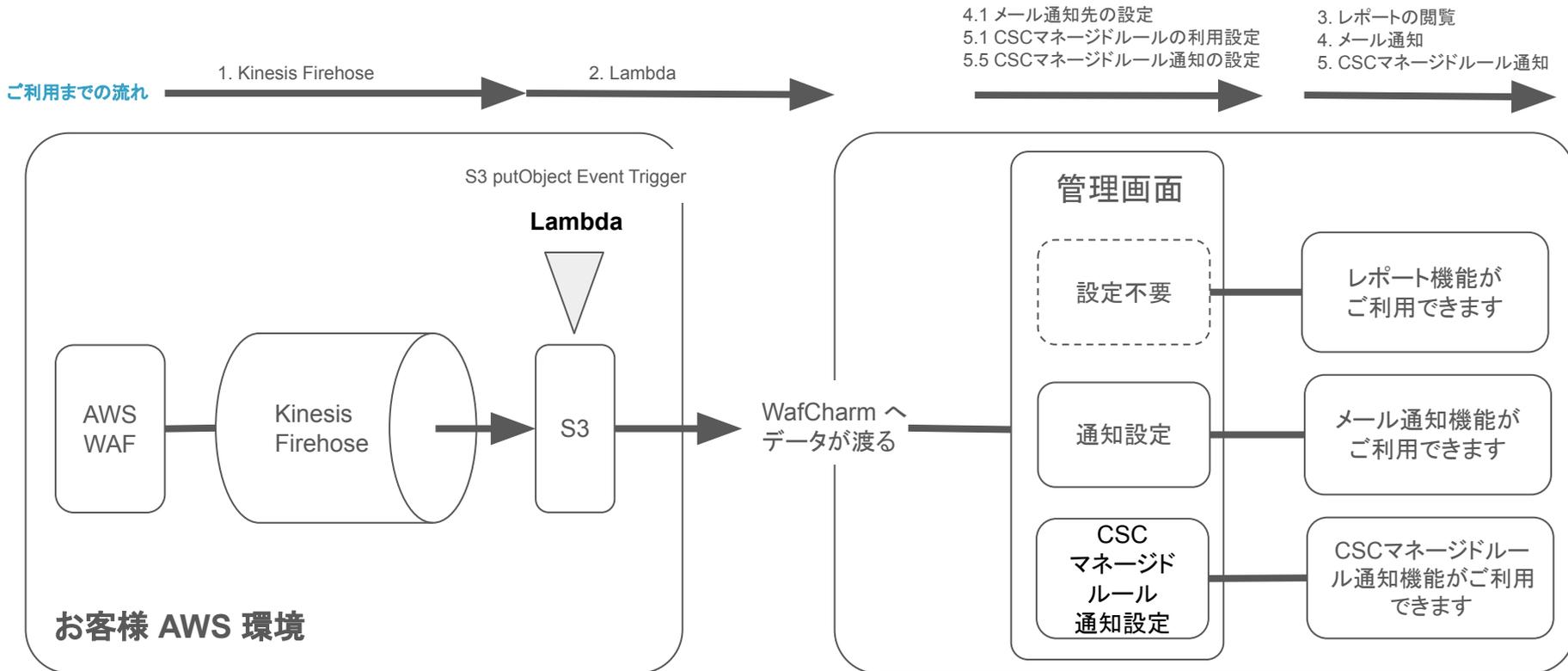


レポート機能/通知機能 利用マニュアル
AWS WAF Classic
Ver 1.6

レポート機能/通知機能のアーキテクチャ概要



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

Permissions Groups (2) Tags Security credentials Access Advisor

▼ Permissions policies (18 policies applied)

[Add permissions](#) [+ Add inline policy](#)

Policy name ▼	Policy type ▼	
Attached directly		
▶  AWSLambdaFullAccess	AWS managed policy	✕
▶  IAMFullAccess	AWS managed policy	✕
▶  CloudWatchFullAccess	AWS managed policy	✕
▶  AmazonKinesisFirehoseFullAccess	AWS managed policy	✕

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

The screenshot displays the AWS Management Console interface for Amazon Kinesis services. The main heading is 'Amazon Kinesis services' with the subtext 'Collect, process, and analyze data streams in real time.' Under the 'Get started' section, three options are listed: 'Kinesis Data Streams', 'Kinesis Data Firehose' (which is selected and circled in red), and 'Kinesis Data Analytics'. Below these options, the 'Create delivery stream' button is highlighted with a red rectangular box. The page also includes a 'Pricing (Asia Pacific (Tokyo))' section with a dropdown menu set to 'Amazon Kinesis Data Streams' and a 'Cost calculator' link. At the bottom, there is a 'Getting started' section with a 'Get started' link.

「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

aws Services Search for services, features, marketplace products, and docs [Option+S] Tokyo Support

Create a delivery stream [Info](#)

▶ Amazon Kinesis Data Firehose: How it works

Choose source and destination

Specify the source and the destination for your delivery stream. You cannot change the source and destination of your delivery stream once it has been created.

Source [Info](#)
Direct PUT

Destination [Info](#)
Amazon S3

Delivery stream name

Delivery stream name
aws-waf-logs-xxxx-xxxx

Transform and convert records - *optional*
Configure Kinesis Data Firehose to transform and convert your record data.

「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

The screenshot shows the AWS Kinesis Firehose console interface. The main section is titled "Transform and convert records - optional" and contains three sub-sections:

- Data transformation:** This section has a radio button for "Disabled" selected and circled in red, and an "Enabled" option that is unselected.
- Convert record format:** This section has a radio button for "Disabled" selected and circled in red, and an "Enabled" option that is unselected.
- Record format conversion:** This section has a radio button for "Disabled" selected and circled in red, and an "Enabled" option that is unselected.

Below these sections is the "Destination settings" section, which includes a text input field for "S3 bucket" with the placeholder text "Choose a bucket or enter a bucket URI", a "Browse" button, and a "Create" button with an external link icon. The format is specified as "Format: s3://bucket".

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

Destination settings [Info](#)

Specify the destination settings for your delivery stream.

S3 bucket

Dynamic partitioning [Info](#)

Dynamic partitioning enables you to create targeted data sets by partitioning streaming S3 data based on partitioning keys. You can partition your source data with inline parsing and/or the specified AWS Lambda function. You can enable dynamic partitioning only when you create a new delivery stream. You cannot enable dynamic partitioning for an existing delivery stream. Enabling dynamic partitioning may incur additional costs per GB of partitioned data. For more information, see [Kinesis Data Firehose pricing](#).

Enabled
 Disabled

S3 bucket prefix - optional

By default, Kinesis Data Firehose appends the prefix "YYYY/MM/dd/HH" (in UTC) to the data it delivers to Amazon S3. You can override this default by specifying a custom prefix that includes expressions that are evaluated at runtime.

You can repeat the same keys in your S3 bucket prefix. Maximum S3 bucket prefix characters: 1024.

S3 bucket error output prefix - optional

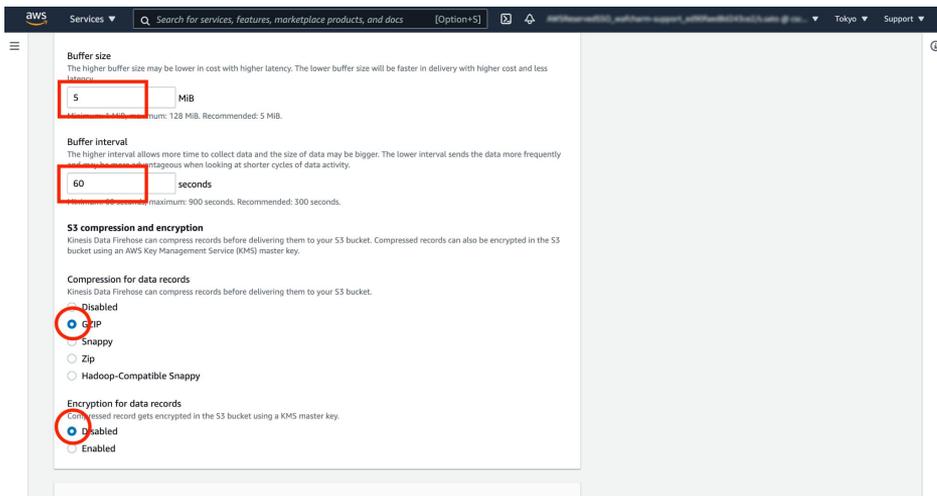
You can specify an S3 bucket error output prefix to be used in error conditions. This prefix can include expressions for Kinesis Data Firehose to evaluate at runtime.

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

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

The screenshot shows the 'Advanced settings' configuration page for an IAM role in the AWS IAM console. The page includes sections for 'Server-side encryption', 'Amazon CloudWatch error logging', 'Permissions', and 'Tags'. The 'Permissions' section has two radio button options: 'Create or update IAM role' (which is selected and circled in red) and 'Choose existing IAM role'. At the bottom of the page, there are two buttons: 'Cancel' and 'Create delivery stream' (which is circled in red).

IAM Role : 新しいIAM ロールの作成 or 選択

「Create delivery stream」

1.7. Kinesis Firehose 設定

The screenshot displays the AWS Management Console interface for configuring a Kinesis Firehose delivery stream. The top navigation bar includes the AWS logo, 'Services' dropdown, a search bar, and the user's location 'Tokyo'. The main content area shows the 'Creating aws-waf-logs-xxx-xxxx' status, with a note that it can take up to 5 minutes before the status is updated. The 'Delivery stream details' section provides the following information:

Property	Value
Status	Creating
Destination	Amazon S3
Data transformation	Disabled
Creation time	November 12, 2021, 15:58 GMT+9
Source	Direct PUT
ARN	arn:aws:kinesis:ap-northeast-1:123456789012:delivery-stream/xxx-xxxx
Dynamic partitioning	Disabled

Below the details, there is a 'Test with demo data' section with a link to 'info' and a note: 'Inject simulated data to test the configuration of your delivery stream. Standard Amazon Kinesis Data Firehose charges apply.'

The 'Monitoring' tab is selected, showing 'Delivery stream metrics'. The metrics section includes three panels: 'Incoming bytes' (Byes), 'Incoming put requests' (Count), and 'Incoming records' (Count). The time range is set to '1h'.

At the bottom of the console, there is a footer with 'Feedback', 'English (US)', and copyright information: '© 2009 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences'.

待機

1.8. Kinesis Firehose 設定

The screenshot displays the AWS Management Console interface for a Kinesis Data Firehose delivery stream. The stream name is 'aws-waf-logs-xxxx-xxxx'. The status is 'Active'. The destination is 'Amazon S3'. The data transformation is 'Disabled'. The creation time is 'November 12, 2021, 15:58 GMT+9'. The source is 'Direct PUT'. The dynamic partitioning is 'Disabled'. The console also shows a 'Test with demo data' button and a 'Delivery stream metrics' section with three gauges: 'Incoming bytes', 'Incoming put requests', and 'Incoming records', all showing a count of 1.

aws-waf-logs-xxxx-xxxx was successfully created.

Amazon Kinesis > Delivery streams > aws-waf-logs-xxxx-xxxx

aws-waf-logs-xxxx-xxxx [Info](#) Delete delivery stream

Delivery stream details

Status Active	Destination Amazon S3	Data transformation Disabled	Creation time November 12, 2021, 15:58 GMT+9
Source Direct PUT	ARN arn:aws:kinesis:us-east-1:123456789012:stream/aws-waf-logs-xxxx-xxxx	Dynamic partitioning Disabled	

Test with demo data [Info](#)
Ingest simulated data to test the configuration of your delivery stream. Standard Amazon Kinesis Data Firehose charges apply.

Monitoring | Configuration | Destination error logs

Delivery stream metrics [Info](#)

1h 3h 12h 1d 3d 1w Custom [Add to dashboard](#)

Incoming bytes Bytes 1	Incoming put requests Count 1	Incoming records Count 1
-------------------------------------	--	---------------------------------------

Feedback English (US) © 2009 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences

完了

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

The screenshot shows the AWS WAF console interface. On the left, the navigation menu has 'Web ACLs' highlighted with a red box. The main content area shows a list of Web ACLs with 'RULE_TEST' selected. On the right, the 'Logging' tab is highlighted with a red box, and the 'Enable Logging' button is visible below the 'Full logging' section.

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

The screenshot shows the AWS console interface for enabling logging for a WAF rule named 'RULE_TEST'. The page title is 'Enable logging for RULE_TEST'. Below the title, it states 'AWS WAF will deliver logs from your web ACL to your Amazon Kinesis Data Firehose.' The 'Web ACL' is 'RULE_TEST'. The 'IAM role' is 'AWSServiceRoleForWAFRegionalLogging'. A dropdown menu for selecting a Kinesis Data Firehose is highlighted with a red box, showing 'Amazon Kinesis Data Firehose' and 'aws-waf-logs-xxxx-xxxx'. Below this, there is a 'Redacted fields' section with a 'Choose field to redact from logs' dropdown and an 'Add' button. At the bottom right, there are 'Cancel' and 'Create' buttons, with the 'Create' button highlighted by a red box. The footer contains 'Feedback', 'English (US)', '© 2018 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.', 'Privacy Policy', 'Terms of Use', and 'Cookie preferences'.

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

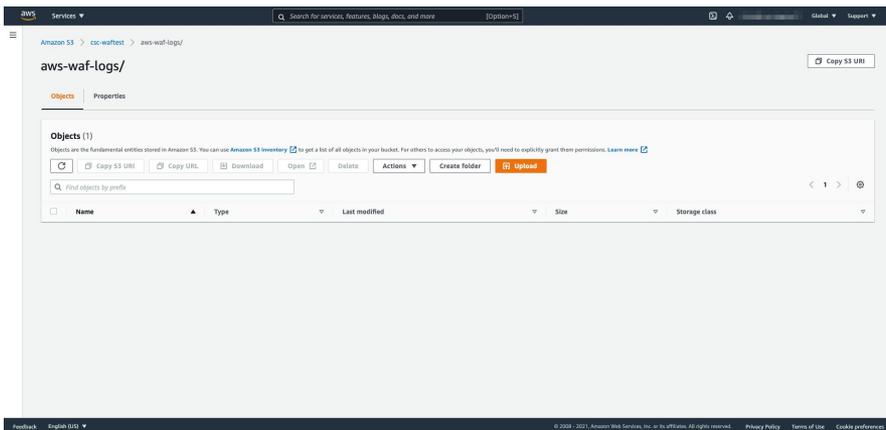
The screenshot shows the AWS WAF console interface. On the left, there is a navigation menu with options like 'Web ACLs', 'Rules', 'Rule groups', 'Marketplace', 'Conditions', 'Cross-site scripting', 'Geo match', 'IP addresses', 'Size constraints', 'SQL injection', 'String and regex matching', 'AWS Shield', 'Summary', 'Protected resources', 'Incidents', and 'Global threat environment'. The main content area is titled 'Web ACLs' and shows a list of Web ACLs. The 'RULE_TEST' rule is selected. The right-hand pane shows the configuration for 'RULE_TEST', with tabs for 'Requests', 'Rules', and 'Logging'. The 'Logging' tab is active, showing a table with columns for 'Logging' and 'Kinesis Data Firehose stream'. The 'Logging' column contains the text 'Enabled', which is highlighted with a red box. The 'Kinesis Data Firehose stream' column contains the text 'aws-waf-logs-xxxx-xxxx'. Below the table, there is a 'Redacted Fields' section with the value 'None'.

Logging	Kinesis Data Firehose stream
Enabled	aws-waf-logs-xxxx-xxxx

Redacted Fields: None

Logging が、“Enabled” になっていることを確認

1.12. 1 章の完了確認

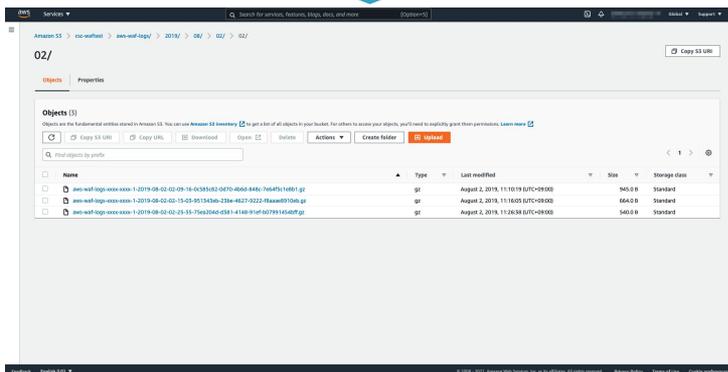
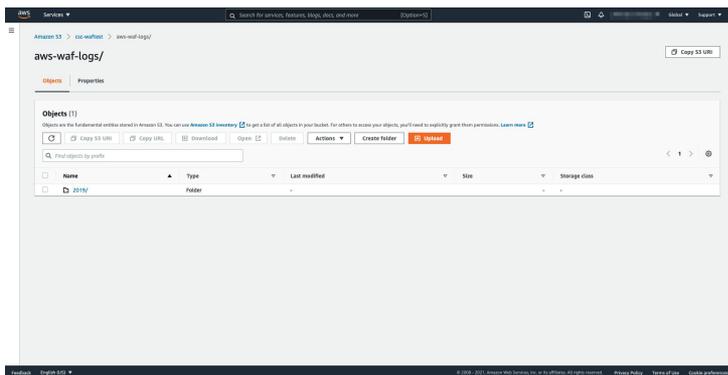


S3 に WAF ログファイルが生成されているか確認

※ 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

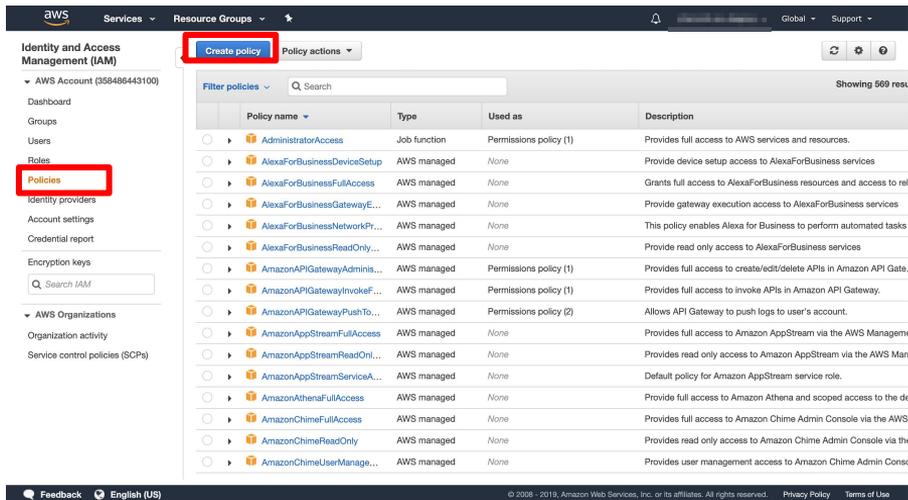
1 章の作業は完了

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



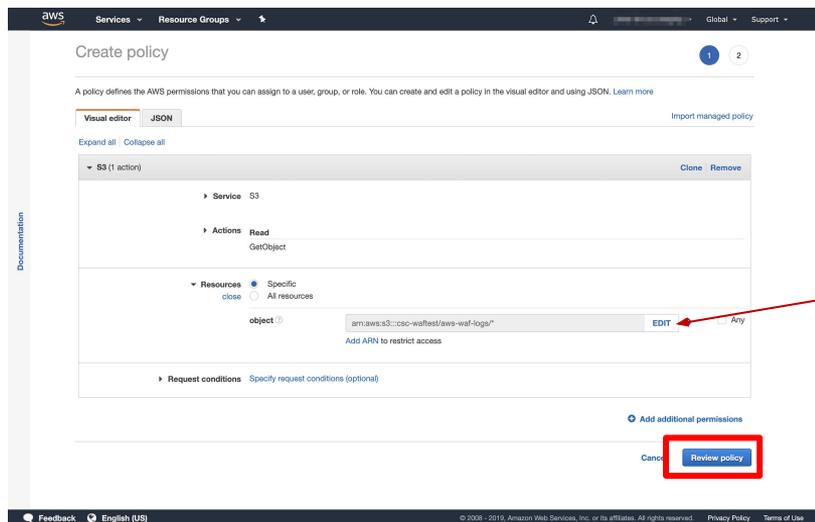
The screenshot shows the AWS IAM console interface. In the left-hand navigation pane, the 'Policies' menu item is highlighted with a red box. In the main content area, the 'Create policy' button is also highlighted with a red box. Below the navigation pane, a table lists various AWS managed policies. The table has columns for Policy name, Type, Used as, and Description.

Policy name	Type	Used as	Description
AdministratorAccess	Job function	Permissions policy (1)	Provides full access to AWS services and resources.
AlexaForBusinessDeviceSetup	AWS managed	None	Provides device setup access to AlexaForBusiness services
AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness resources and access to re
AlexaForBusinessGatewayE...	AWS managed	None	Provide gateway execution access to AlexaForBusiness services
AlexaForBusinessNetworkPr...	AWS managed	None	This policy enables Alexa for Business to perform automated tasks
AlexaForBusinessReadOnly...	AWS managed	None	Provide read only access to AlexaForBusiness services
AmazonAPIGatewayAdminis...	AWS managed	Permissions policy (1)	Provides full access to create/edit/delete APIs in Amazon API Gate.
AmazonAPIGatewayInvokeF...	AWS managed	Permissions policy (1)	Provides full access to invoke APIs in Amazon API Gateway.
AmazonAPIGatewayPushTo...	AWS managed	Permissions policy (2)	Allows API Gateway to push logs to user's account.
AmazonAppStreamFullAccess	AWS managed	None	Provides full access to Amazon AppStream via the AWS Manage
AmazonAppStreamReadOnl...	AWS managed	None	Provides read only access to Amazon AppStream via the AWS Man
AmazonAppStreamServiceA...	AWS managed	None	Default policy for Amazon AppStream service role.
AmazonAthenaFullAccess	AWS managed	None	Provide full access to Amazon Athena and scoped access to the de
AmazonChimeFullAccess	AWS managed	None	Provides full access to Amazon Chime Admin Console via the AWS
AmazonChimeReadOnly	AWS managed	None	Provides read only access to Amazon Chime Admin Console via the
AmazonChimeUserManage...	AWS managed	None	Provides user management access to Amazon Chime Admin Cons

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

aws Services Resource Groups

Create policy

Review policy

Name* wafcharm-waflog-s3-read
Use alphanumeric and "+, -, @_" characters. Maximum 128 characters.

Description WafCharm
Maximum 1000 characters. Use alphanumeric and "+, -, @_" characters.

Summary

Service	Access level	Resource	Request condition
Allow (1 of 187 services) Show remaining 186			
S3	Limited: Read	BucketName string like csc-wafset, None ObjectPath string like aws-waf-logs*	

* Required

Cancel Previous **Save changes**

Feedback English (US) © 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

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

aws Services Resource Groups

Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor JSON Import managed policy

Expand all Collapse all

S3 (2 actions) Clone Remove

- Service S3
- Actions
 - Write
 - PutObject
 - Permissions management
 - PutObjectAcl
- Resources
 - Specific (selected)
 - All resources
 - object
 - arn:aws:s3:::wafcharm.com/*
 - Add ARN to restrict access
- Request conditions Specify request conditions (optional)

Add additional permissions

Cancel Review policy

Feedback English (US) © 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Service : S3

Action : PutObject, PutObjectACL

Resources :

arn:aws:s3:::wafcharm.com/*

※ CSC 側の S3 に対する権限

ARN の追加

Amazon リソースネーム (ARN) は、AWS リソースを一意に識別します。リソースは各サービスに固有です。 [詳細はこちら](#)

S3_object の ARN の指定 [ARN を手動でリスト](#)

arn:aws:s3:::wafcharm.com/*

Bucket name * wafcharm.com すべて

Object name * * すべて

キャンセル 追加

「Review policy」

2.5. WafCharm 連携用 put 権限 policy 作成

Create policy

Review policy

Name: wafcharm-waflog-s3-put
Use alphanumeric and "+=,@-." characters. Maximum 128 characters.

Description: WafCharm
Maximum 1000 characters. Use alphanumeric and "+=,@-." characters.

Summary

Service	Access level	Resource	Request condition
Allow (1 of 187 services) Show remaining 186			
S3	Limited: Write, Permissions management	BucketName string like wafcharm.com, ObjectPath string like All	None

* Required

Cancel Previous **Create policy**

Feedback English (US) © 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

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

The screenshot shows the AWS IAM console 'Create role' page. The 'Select type of trusted entity' section has four options: 'AWS service', 'Another AWS account', 'Web identity', and 'SAML 2.0 federation'. The 'Choose the service that will use this role' section is expanded to show a list of services. The 'Lambda' service is highlighted with a red box. At the bottom of the page, the 'Next: Permissions' button is also highlighted with a red box.

Create role

Select type of trusted entity

Choose the service that will use this role

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

API Gateway	Comprehend	ElasticCache	Lex	SMS
AWS Backup	Config	Elastic Beanstalk	License Manager	SNS
AWS Support	Connect	Elastic Container Service	Machine Learning	SWF
Amplify	DMS	Elastic Transcoder	Macie	SageMaker
AppSync	Data Lifecycle Manager	ElasticLoadBalancing	MediaConvert	Security Hub
Application Auto Scaling	Data Pipeline	Forecast	Migration Hub	Service Catalog
Application Discovery Service	DataSync	Glue	OpsWorks	Step Functions
Batch	DeepLens	Greengrass	Personalize	Storage Gateway
	Directory Service	GuardDuty	RAM	Amazon

* Required

Next: Permissions

このロールを使用するサービスを選択 : Lambda

「Next: Permissions」

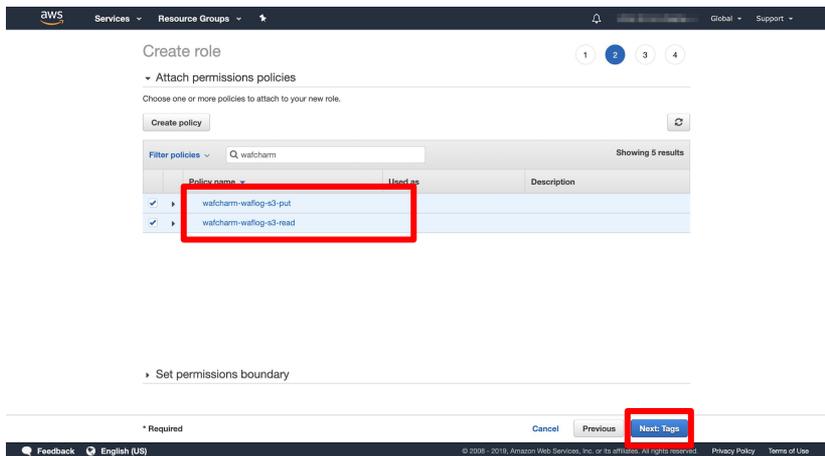
2.7. WafCharm 連携 Lambda 用 role 作成

The screenshot shows the AWS IAM console interface for creating a role. The 'Attach permissions policies' step is selected. A search filter 'lambda' is applied to the policy list. The 'AWSLambdaExecute' policy is selected and highlighted with a red box.

Policy name	Used as	Description
<input type="checkbox"/> AWSLambdaBasicExecutionRole-96f82314-e...	None	
<input type="checkbox"/> AWSLambdaBasicExecutionRole-bf9331ef-78...	Permissions policy (1)	
<input type="checkbox"/> AWSLambdaDynamoDBExecutionRole	None	Provides list and read access to Dynamo...
<input type="checkbox"/> AWSLambdaExecute	Permissions policy (8)	Provides minimum permissions for a La...
<input type="checkbox"/> AWSLambdaFullAccess	Permissions policy (4)	Provides Put, Get access to S3 and full a...
<input type="checkbox"/> AWSLambdaInvocation-DynamoDB	None	Provides full access to Lambda, S3, Dym...
<input type="checkbox"/> AWSLambdaKinesisExecutionRole	None	Provides read access to DynamoDB Stre...
<input type="checkbox"/> AWSLambdaKinesisExecutionRole	None	Provides list and read access to Kinesis ...

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

aws Services Resource Groups

Create role 1 2 3 4

Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="Add new key"/>	<input type="text"/>	<input type="button" value="Remove"/>

You can add 50 more tags.

Cancel Previous **Next: Review**

Feedback English (US) © 2009 - 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

タグの追加は任意

「Next: Review」

2.10. WafCharm 連携 Lambda 用 role 作成

The screenshot shows the 'Create role' page in the AWS IAM console, specifically the 'Review' step. The page contains the following information:

- Role name:** wafcharm-waflog
- Role description:** WafCharm
- Trusted entities:** AWS service: lambda.amazonaws.com
- Policies:** AWSLambdaExecute, wafcharm-waflog-s3-read, wafcharm-waflog-s3-put
- Permissions boundary:** Permissions boundary is not set

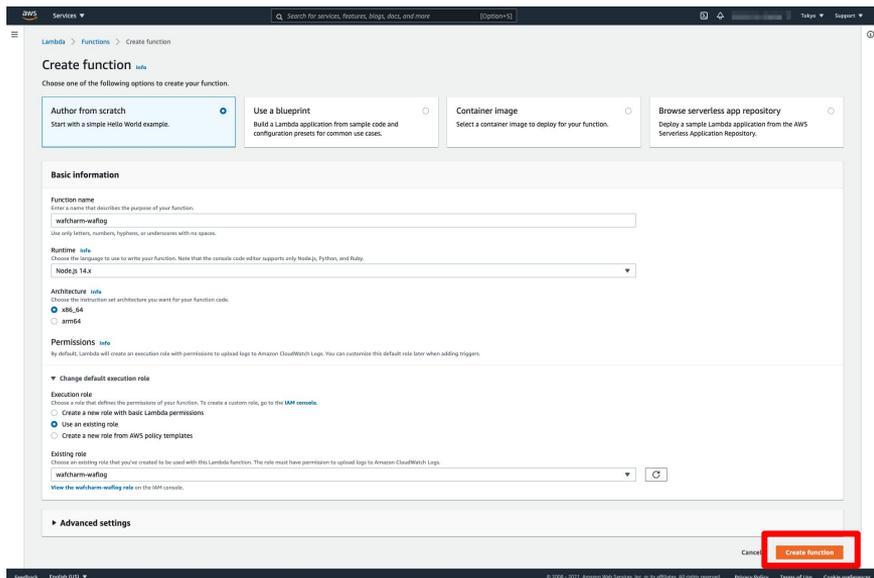
At the bottom of the page, there are three buttons: 'Cancel', 'Previous', and 'Create role'. The 'Create role' button is highlighted with a red box.

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」

2.13. Lambda 構築 (トリガー)

aws Services Search for services, features, blogs, docs, and more [Option+S] Tokyo Support

Lambda > Add trigger

Add trigger

Trigger configuration

S3 storage

Bucket
Please select the S3 bucket that serves as the event source. The bucket must be in the same region as the function.
csc-wafest

Event type
Select the events that you want to have trigger the Lambda function. You can optionally set up a prefix or suffix for an event. However, for each bucket, individual events cannot have multiple configurations with overlapping prefixes or suffixes that could match the same object key.
All object create events

Prefix - optional
Enter a single optional prefix to limit the notifications to objects with keys that start with matching characters.
aws-waf-logs/

Suffix - optional
Enter a single optional suffix to limit the notifications to objects with keys that end with matching characters.
e.g. .jpg

Lambda will add the necessary permissions for Amazon S3 to invoke your Lambda function from this trigger. [Learn more about the Lambda permissions model.](#)

Recursive invocation
If your function writes objects to an S3 bucket, ensure that you are using different S3 buckets for input and output. Writing to the same bucket increases the risk of creating a recursive invocation, which can result in increased Lambda usage and increased costs. [Learn more](#)

I acknowledge that using the same S3 bucket for both input and output is not recommended and that this configuration can cause recursive invocations, increased Lambda usage, and increased costs.

Cancel **Add**

Feedback English (US) © 2008 - 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences

Add trigger :
トリガーに S3 を選択

トリガーの設定

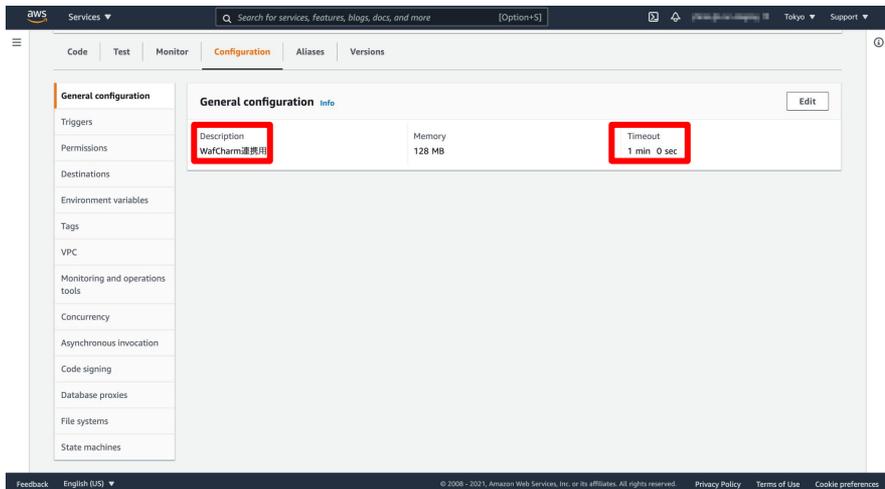
バケット: 1.4 で設定した S3 bucket

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

The screenshot displays the AWS Lambda console interface for a function named 'wafcharm-waflog'. The top navigation bar includes the AWS logo, 'Services', a search bar, and regional information (Tokyo). The breadcrumb trail shows 'Lambda > Functions > wafcharm-waflog'. The function name 'wafcharm-waflog' is prominently displayed at the top, along with buttons for 'Throttle', 'Copy ARN', and 'Actions'. Below this, the 'Function overview' section shows a diagram of the function's architecture, including a 'wafcharm-waflog' function box, a 'Layers' box with '(0)' layers, and an 'S3' trigger box. A '+ Add destination' button is visible. To the right, a metadata panel lists 'Description' (empty), 'Last modified' (6 minutes ago), and 'Function ARN'. The 'Code source' section is active, showing a code editor with a file explorer on the left containing 'wafcharm-waflog' and 'index.js'. The code in 'index.js' is as follows:

```
1 use strict;
2
3
4 const toBucket = process.env.WAFCHARM_BUCKET || 'wafcharm.com';
5 const toPath = process.env.WAFCHARM_PATH || 'waflog/acceptance/V1';
```

The bottom of the console shows the footer with 'Feedback', 'English (US)', and copyright information: '© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences'.

完了

2.16. CloudWatch

Lambda 関数実行後でないとは作成されません

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

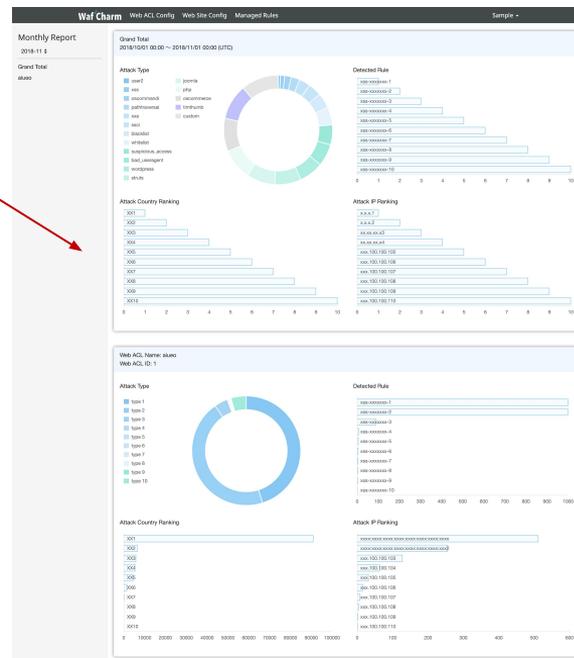
1. 1～2章までの設定が完了している
2. 前月に検知があった

※ 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

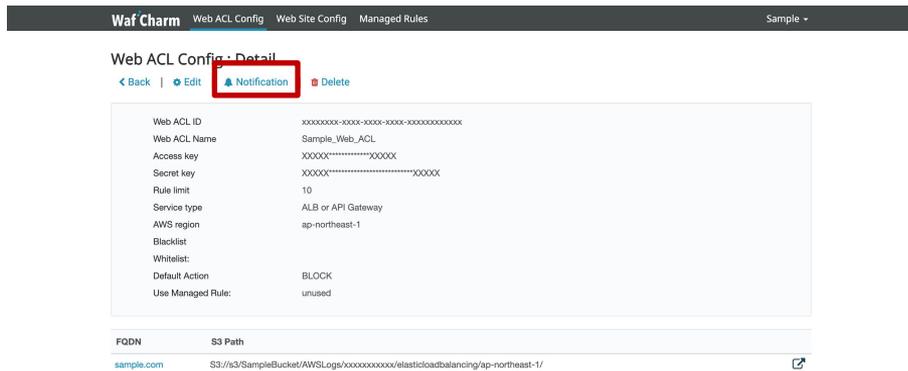
4.2. メール通知先の設定

The screenshot shows the 'Web ACL Config' page in the Waf Charm interface. The breadcrumb navigation includes 'Web ACL Config', 'Web Site Config', and 'Managed Rules'. Below the title, there are links for '< Back' and 'Add ACL'. A table lists the configured Web ACLs:

Web ACL ID	Web ACL Name	
xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxx	Sample_Web_ACL	 

対象の「Web ACL Name」を選択

4.3. メール通知先の設定



WafCharm Web ACL Config Web Site Config Managed Rules Sample ▾

Web ACL Config - Detail

[Back](#) | [Edit](#) | **Notification** | [Delete](#)

Web ACL ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Web ACL Name	Sample_Web_ACL
Access key	XXXXXXXXXXXXXXXXXXXX
Secret key	XXXXXXXXXXXXXXXXXXXXXXXXXXXX
Rule limit	10
Service type	ALB or API Gateway
AWS region	ap-northeast-1
Blacklist	
Whitelist	
Default Action	BLOCK
Use Managed Rule:	unused

FQDN	S3 Path
sample.com	S3://s3/SampleBucket/AWSLogs/xxxxxxxxxx/elasticloadbalancing/ap-northeast-1/ ↗

「Notification」を選択

4.4. メール通知先の設定

WafCharm Web ACL Config Web Site Config Managed Rules Sample -

Notification : Detail
[< Web ACL Config](#) | [Edit](#)

Web ACL ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Web ACL Name	Sample_Web_ACL
WafCharm Email Notificatoin	OFF
Managed Rule Email Notificatoin	OFF

Notification email
[Edit](#)

Email	Set date
sample@example.com	2020-03-10 11:19:06 +0900

通知を有効にするためには設定が必要です。
[レポート機能/通知機能を利用する](#)

「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

Waf Charm Web ACL Config Web Site Config Managed Rules Sample ▾

Edit Notification Email

[< Notification](#)

Emailの送信を最大10件まで登録できます。

Email *

notification@exampl.com	⊗
alert@sample.com	⊗
example@cscloud.co.jp	⊗

copyright © Cyber Security Cloud, Inc. All Rights Reserved | お問い合わせ

「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

Waf Charm Web ACL Config Web Site Config Managed Rules Sample -

Notification : Detail
[< Web ACL Config](#) | [Edit](#)

Web ACL ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Web ACL Name	Sample_Web_ACL
WafCharm Email Notificatoin	OFF
Managed Rule Email Notificatoin	OFF

Notification email

[Edit](#)

Email	Set date
notification@example.com	
alert@sample.com	

通知を有効にするためには設定が必要です。
[レポート機能/通知機能を利用する](#)

「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

Notification : Detail

[< Web ACL Config](#) [Edit](#)

Web ACL ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Web ACL Name	Sample_Web_ACL
WafCharm Email Notificatoin	OFF
Managed Rule Email Notificatoin	OFF

Notification email

[Edit](#)

Email	Set date
notification@example.com	
alert@sample.com	

通知を有効にするためには設定が必要です。

[レポート機能/通知機能を利用する](#)

「Edit」を選択

4.8. メール通知の設定

WafCharm Web ACL Config Web Site Config Managed Rules Sample ▾

Notification : Edit
[← Notification](#)

Web ACL ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Web ACL Name	Sample_Web_ACL
Email Address	sample@example.com
WafCharm Email Notificaitoin	<input checked="" type="checkbox"/> ON OFF
Managed Rule Email Notificaitoin	<input type="checkbox"/> ON OFF

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

4.9. メール通知の設定

Waf Charm Web ACL Config Web Site Config Managed Rules Sample ▾

Notification : Detail
[Web ACL Config](#) | [Edit](#)

Web ACL ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Web ACL Name	Sample_Web_ACL
WafCharm Email Notificaiton	<input checked="" type="checkbox"/> ON
Managed Rule Email Notificaiton	<input type="checkbox"/> OFF

Notification email
[Edit](#)

Email	Set date
notification@example.com	
alert@sample.com	

通知を有効にするためには設定が必要です。
[レポート機能/通知機能を利用する](#)

「WafCharm Email Notificaiton」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

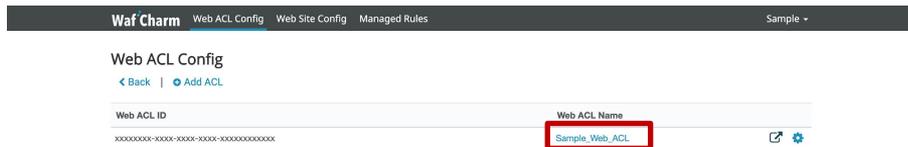
5.1. CSC マネージドルールの利用設定



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



Waf Charm Web ACL Config Web Site Config Managed Rules Sample ▾

Web ACL Config
◀ Back | Add ACL

Web ACL ID	Web ACL Name	
xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxx	Sample_Web_ACL	🔗 ⚙️

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

WafCharm Web ACL Config Web Site Config Managed Rules Sample ▾

Web ACL Config: Detail

[← Back](#) [Edit](#) | [Notification](#) | [Delete](#)

Web ACL ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Web ACL Name	Sample_Web_ACL
Access key	XXXXXXXXXXXXXXXXXXXX
Secret key	XXXXXXXXXXXXXXXXXXXXXXXXXXXX
Rule limit	10
Service type	ALB or API Gateway
AWS region	ap-northeast-1
Blacklist	
Whitelist	
Default Action	BLOCK
Use Managed Rule:	unused

FQDN	S3 Path
sample.com	S3://s3/SampleBucket/AWSLogs/xxxxxxxxxx/elasticloadbalancing/ap-northeast-1/ ↗

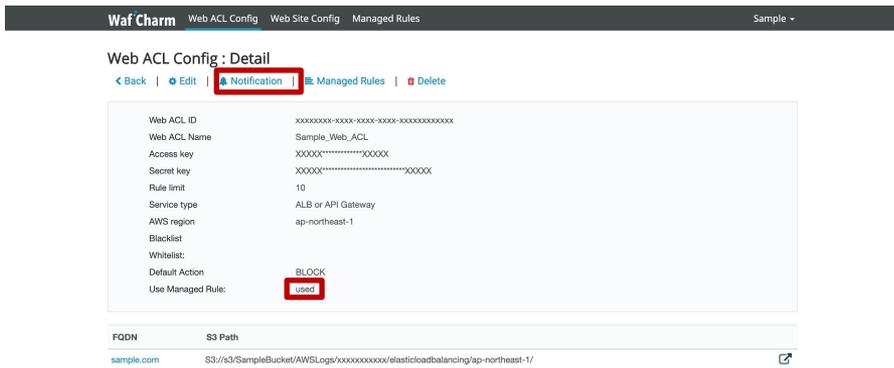
「Edit」を選択

5.4. CSC マネージドルールの利用設定

The screenshot shows the 'Web ACL Config: Edit' page in the Waf Charm interface. The page has a dark header with 'Waf Charm' and navigation links for 'Web ACL Config', 'Web Site Config', and 'Managed Rules'. Below the header, there are navigation links for 'Back' and 'Show'. The main content area contains a form with several fields: 'Web ACL ID *', 'Web ACL Name *', 'Web ACL Access Key *', and 'Web ACL Secret Key *'. Below these are sections for 'Rule limit', 'Choose AWS service type *', 'Choose your AWS region *', 'Blacklist', and 'Whitelist'. At the bottom of the form, there is a 'Default AWS WAF Action' dropdown set to 'BLOCK' and a 'Use Managed Rule' dropdown set to 'used'. The 'used' option and the 'Save' button are highlighted with red boxes. The footer contains the copyright notice: 'copyright © Cyber Security Cloud, Inc. All Rights Reserved | お問い合わせ'.

「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



WafCharm Web ACL Config Web Site Config Managed Rules Sample ▾

Web ACL Config: Detail

< Back | Edit | **Notification** | Managed Rules | Delete

Web ACL ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Web ACL Name	Sample_Web_ACL
Access key	XXXXXXXXXXXXXXXXXXXX
Secret key	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Rule limit	10
Service type	ALB or API Gateway
AWS region	ap-northeast-1
Blacklist:	
Whitelist:	
Default Action	BLOCK
Use Managed Rule:	<input checked="" type="checkbox"/> used

FGDN	S3 Path
sample.com	S3://s3/SampleBucket/AWSLogs/xxxxxxxxxx/elasticloadbalancing/ap-northeast-1/

「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

Notification : Detail

[Web ACL Config](#) | [Edit](#)

Web ACL ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Web ACL Name	Sample_Web_ACL
WafCharm Email Notificatoin	ON
Managed Rule Email Notificatoin	OFF

Notification email

[Edit](#)

Email	Set date
notification@example.com	
alert@sample.com	

通知を有効にするためには設定が必要です。

[レポート機能/通知機能を利用する](#)

「Edit」を選択

5.7. CSC マネージドルール通知の設定

The screenshot shows the WafCharm interface with the following elements:

- Header: WafCharm | Web ACL Config | Web Site Config | Managed Rules | Sample ▾
- Page Title: Notification : Edit
- Back Link: < Notification
- Form Fields:
 - Web ACL ID: xxxxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
 - Web ACL Name: Sample_Web_ACL
 - WarCharm Email Notificaiton: ON OFF
 - Managed Rule Email Notificaiton: ON OFF
- Buttons: A "Save" button is located at the bottom right of the form area.

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

5.8. CSC マネージドルール通知の設定

Waf Charm Web ACL Config Web Site Config Managed Rules Sample ▾

Notification : Detail
[< Web ACL Config](#) | [Edit](#)

Web ACL ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Web ACL Name	Sample_Web_ACL
WafCharm Email Notification	ON
Managed Rule Email Notification	ON

Notification email
[Edit](#)

Email	Set date
notification@example.com	2020-03-11 16:46:09 +0900
alert@sample.com	2020-03-11 16:46:09 +0900

通知を有効にするためには設定が必要です。
[レポート機能/通知機能を利用する](#)

「Managed Rule Email Notification」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