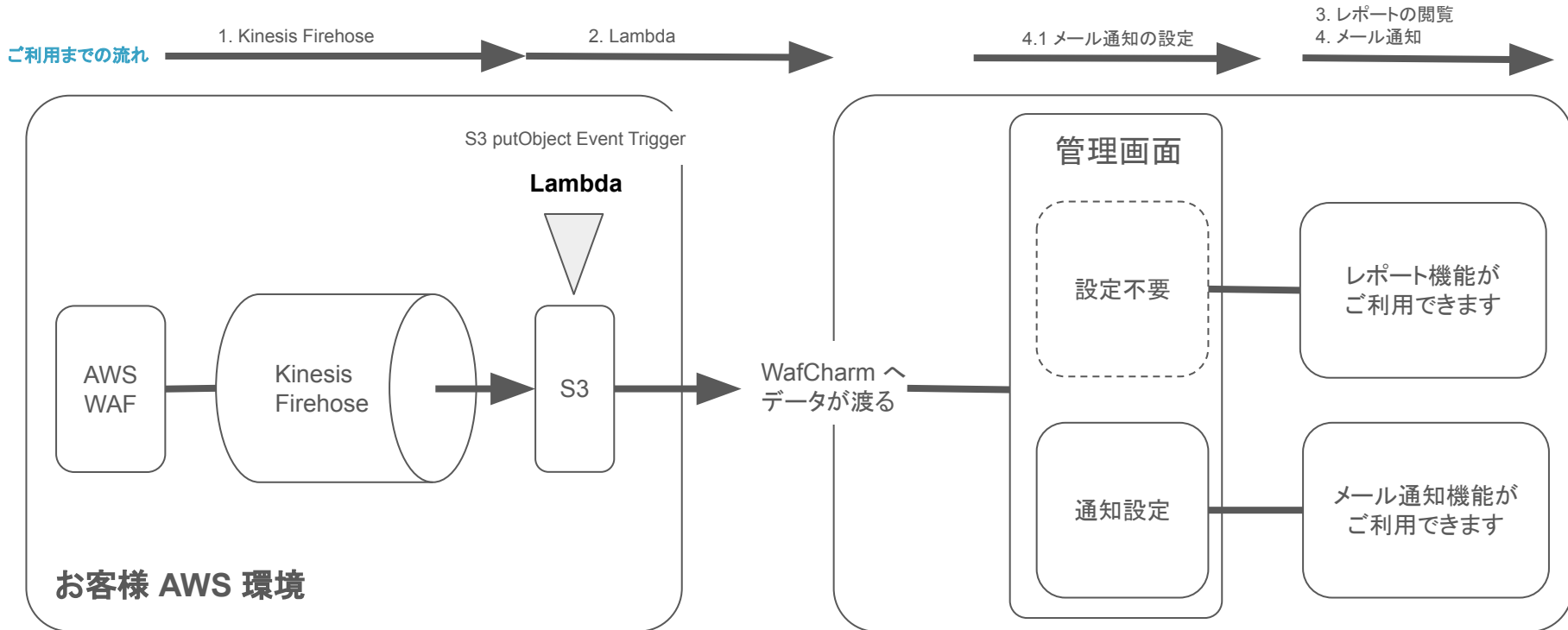


レポート機能/通知機能 利用マニュアル
new AWS WAF
Ver 1.0

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. 通知機能に関する補足事項

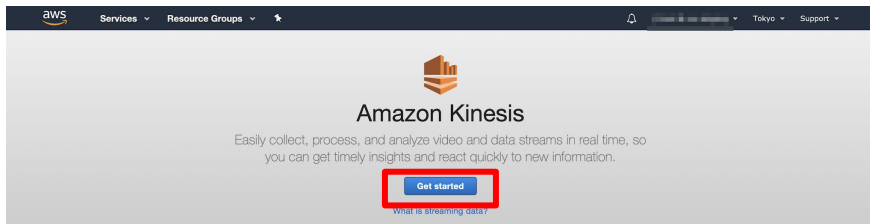
6. その他補足事項

1. Kinesis Firehose

WAF ログを S3 に転送する Kinesis Firehose を設定

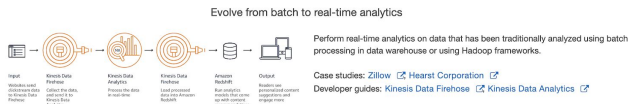
- Kinesis Firehose の構築/設定
- Kinesis Firehose 実行用の Role 設定
- Kinesis Firehose と AWS WAF との連携設定
- 1 章の完了確認

1.1. Kinesis Firehose 設定



「Get started」をクリックします

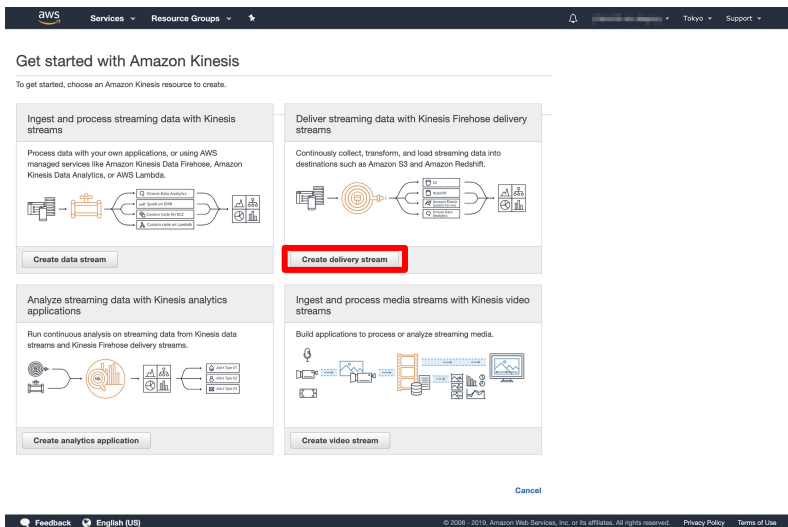
What can you build with Amazon Kinesis?



Build real-time applications

Create utility into what your customers' applications and products see about you

1.2. Kinesis Firehose 設定



「Create delivery stream」

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

1.3. Kinesis Firehose 設定

Kinesis Firehose - Create delivery stream

Step 1: Name and source

New delivery stream

Delivery streams load data, automatically and continuously, to the destinations that you specify. Kinesis Firehose resources are not covered under the AWS Free Tier, and usage-based charges apply. For more information, see Kinesis Firehose pricing.

Delivery stream name*

Letters, numbers, underscores, hyphens, and periods.

Choose source

Choose how you would prefer to send records to the delivery stream.

Firehose data flow overview

```
graph LR
    subgraph Source
        S1[ ]
        S2[ ]
    end
    subgraph Firehose_delivery_stream [Firehose delivery stream]
        SR[Source records]
        PR[Processed records]
    end
    subgraph Destination
        D1[ ]
        D2[ ]
    end
    S1 --> SR
    S2 --> SR
    SR --> PR
    PR --> D1
    PR --> D2
```

----- Optional

Source* Direct PUT or other sources

Choose this option to send records directly to the delivery stream, or to send records from AWS IoT, CloudWatch Logs, or CloudWatch Events.

Kinesis stream

Direct PUT or other sources

After creating the delivery stream, send source records using the Firehose PUT API or the Amazon Kinesis Agent.

Firehose PUT APIs

Use the Firehose PutRecord() or PutRecordBatch() API to send source records to the delivery stream. [Learn more](#)

Amazon Kinesis Agent

The Amazon Kinesis Agent is a stand-alone Java software application that offers an easy way to collect and send source records to Firehose. [Learn more](#)

AWS IoT

Create AWS IoT rules that send data from MQTT messages. [Learn more](#)

CloudWatch Logs

Use subscription filters to deliver a real-time stream of log events. [Learn more](#)

CloudWatch Events

Create rules to indicate which events are of interest to your application and what automated action to take when a rule matches an event. [Learn more](#)

* Required

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

「Next」

※ 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

1.4. Kinesis Firehose 設定

Kinesis Firehose - Create delivery stream

Step 1: Name and source
Step 2: Process records
Step 3: Choose destination
Step 4: Configure settings
Step 5: Review

Process records

Kinesis Firehose can transform records or convert record format before delivery.

Process records data flow overview

Source records → Processed records

Transform source records → Convert record format

Invoke AWS Lambda function → Refer to AWS Glue table for schema

Optional

Transform source records with AWS Lambda

To return records from AWS Lambda to Kinesis Firehose after transformation, the Lambda function you invoke must be compliant with the required record transformation output model. [Learn more](#)

Record transformation: Disabled
 Enabled

Convert record format

Data in Apache parquet or Apache ORC format is typically more efficient to query than JSON. Kinesis Data Firehose can convert your JSON-formatted source records using a schema defined in AWS Glue. [If](#) For records that aren't in JSON format, create a Lambda function that converts them to JSON in the [Transform source records with AWS Lambda](#) section above. [Learn more](#)

Record format conversion: Disabled
 Enabled

If record format conversion is enabled, Firehose can deliver data to Amazon S3 only. Record format conversion will be configured using the `Opport_JSON_SerDe`. For other options use the [AWS CLI](#).

* Required

Cancel Previous **Next**

© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

「Next」

下記は使用しません

- Transform source records with AWS Lambda
- Convert record format

1.5. Kinesis Firehose 設定

Kinesis Firehose - Create delivery stream

Step 1: Name and source
Step 2: Process records
Step 3: Choose destination
Step 4: Configure settings
Step 5: Review

Select destination

Destination* Amazon S3
Amazon S3 is an easy-to-use object storage, with a simple web service interface to store and retrieve any amount of data from anywhere on the web.

Amazon Redshift
Amazon Redshift is a fast, fully managed, petabyte-scale data warehouse that makes it simple and cost-effective to analyze all your data using your existing business intelligence tools.

Amazon Elasticsearch Service
Elasticsearch is an open-source search and analytics engine for use cases such as log analytics, real-time application monitoring, and click stream analytics.

Splunk
Splunk is an operational intelligence tool for analyzing machine-generated data in real-time.

Firehose to S3 data flow overview

Source → Firehose delivery stream → S3 bucket (destination)
Processed records
Optional → S3 bucket (optional backup)
If processing fails

S3 destination
Choose a destination in Amazon S3 where your data will be stored. Amazon S3 is object storage built to store and retrieve any amount of data from anywhere. [Learn more](#)

S3 bucket*

S3 prefix
By default, Kinesis Data Firehose appends the prefix "YYYYMMDDHH" (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.

If your custom prefix doesn't include expressions, Kinesis Data Firehose uses your prefix and appends "YYYYMMDDHH". If your custom prefix includes a Firehose random string or timestamp expression, Kinesis Data Firehose doesn't append "YYYYMMDDHH". [Learn more](#)

Prefix

S3 error prefix
You can specify an S3 bucket prefix to be used in error conditions. This prefix can include expressions for Kinesis Data Firehose to evaluate at runtime. [Learn more about the rules for specifying prefix expressions](#)

Error prefix

* Required

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

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

「Next」

1.6. Kinesis Firehose 設定

The screenshot shows the 'Configure settings' step of the 'Create delivery stream' process in the AWS Kinesis Firehose console. The page is divided into several sections:

- Configure settings:** A header section with a sub-header 'Configure buffer, compression, logging, and IAM role settings for your delivery stream.'
- S3 buffer conditions:** A section with a description: 'Firehose buffers incoming records before delivering them to your S3 bucket. Record delivery will be triggered once either of these conditions has been satisfied. Learn more.' It contains two input fields: 'Buffer size' set to 5 MB and 'Buffer interval' set to 60 seconds. Both fields are highlighted with a red box.
- S3 compression and encryption:** A section with a description: 'Firehose can compress records before delivering them to your S3 bucket. Compressed records can also be encrypted in the S3 bucket using a KMS master key. Learn more.' It contains two radio button groups: 'S3 compression' with 'GZIP' selected, and 'S3 encryption' with 'Disabled' selected. Both groups are highlighted with a red box.
- Error logging:** A section with a description: 'Firehose can log record delivery errors to CloudWatch Logs. If enabled, a CloudWatch log group and corresponding log streams are created on your behalf. Learn more.' It contains a radio button group with 'Enabled' selected.
- Tags (optional):** A section with a description: 'You can add tags to organize your AWS resources, track costs, and control access. Learn more.' It contains input fields for 'Key' and 'Value' and a 'Remove tag' button.
- IAM role:** A section with a description: 'Firehose uses an IAM role to access your specified resources, such as the S3 bucket and KMS key. Learn more.' It contains a button labeled 'Create new or choose' which is highlighted with a red box.

At the bottom of the page, there are 'Cancel', 'Previous', and 'Next' buttons, and a '* Required' label.

Buffer intervals :
推奨は 60 seconds

※ 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

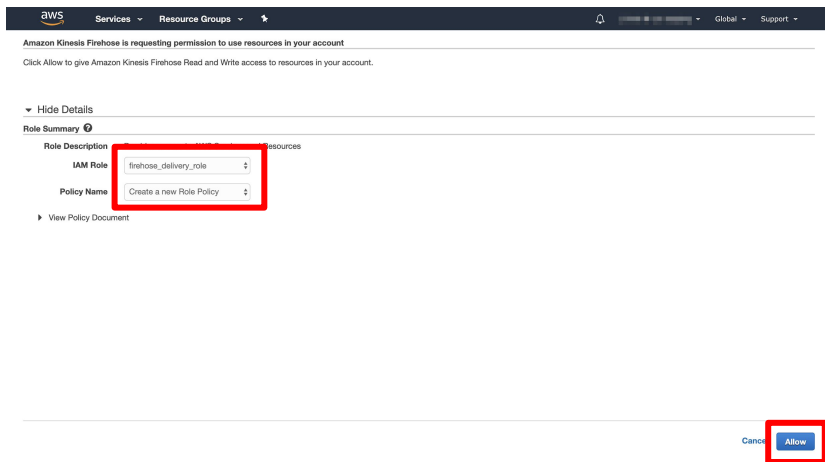
Buffer size :
推奨は 5 MB

S3 compression :
GZIP

S3 encryption :
Disable

「Create new or choose」

1.7. IAM role 設定



Role Description :
任意

IAM Role :
新しいIAM ロールの作成 or 選択

Policy Name :
新しいロールポリシーの作成 or 選択

「Allow」

1.8. Kinesis Firehose 設定

aws Services Resource Groups

Kinesis Firehose - Create delivery stream

Step 1: Name and source
Step 2: Process records
Step 3: Choose destination
Step 4: Configure settings
Step 5: Review

Configure settings

Configure buffer, compression, logging, and IAM role settings for your delivery stream.

S3 buffer conditions

Firehose buffers incoming records before delivering them to your S3 bucket. Record delivery will be triggered once either of these conditions has been satisfied. [Learn more](#)

Buffer size* 5 MB
Specify a buffer size between 1-128 MB

Buffer interval* 60 seconds
Specify a buffer interval between 60-900 seconds

S3 compression and encryption

Firehose can compress records before delivering them to your S3 bucket. Compressed records can also be encrypted in the S3 bucket using a KMS master key. [Learn more](#)

S3 compression* Disabled
 GZIP
 Snappy
 Zip

S3 encryption* Disabled
 Enabled

Error logging

Firehose can log record delivery errors to CloudWatch Logs. If enabled, a CloudWatch log group and corresponding log streams are created on your behalf. [Learn more](#)

Error logging* Disabled
 Enabled

Tags (optional)

You can add tags to organize your AWS resources, track costs, and control access. [Learn more](#)

Key Value - optional
Enter key Enter value

*You can add 48 more tags

IAM role

Firehose uses an IAM role to access your specified resources, such as the S3 bucket and KMS key. [Learn more](#)

IAM role* firehose_delivery_role

* Required

「Next」

1.9. Kinesis Firehose 設定

The screenshot shows the AWS Management Console interface for creating a Kinesis Firehose delivery stream. The page is titled 'Kinesis Firehose - Create delivery stream' and is in the 'Review' step. The configuration details are as follows:

- Name and source:** Delivery stream name is 'aws-waf-logs-wafcham-waflog'. Source is 'Direct PUT or other sources'.
- Process records:** Source record transformation is 'Disabled' and Record format conversion is 'Disabled'.
- Destination:** Destination is 'Amazon S3', S3 bucket is 'csc-wafest', S3 bucket prefix is 'aws-waf-logs', and S3 bucket error prefix is 'no error prefix specified'.
- Settings:** S3 buffer conditions are '5 MB or 60 seconds', Compression is 'GZIP', Encryption is 'Disabled', Error logging is 'Enabled', Tags are 'no tags specified', and IAM role is 'firehose_delivery_role'.

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

「Create delivery stream」

1.10. Kinesis Firehose 設定

Amazon Kinesis

Firehose delivery streams

Kinesis Firehose delivery streams continuously collect, transform, and load streaming data into the destinations that you specify.

Creating delivery stream **aws-waf-logs-wafcharm-waflog**
It can take up to a minute before the status is updated.

Create delivery stream Test with demo data Delete

Filter Firehose delivery streams

Name	Status	Created	Source	Record transformation	Destination
aws-waf-logs-wafcharm-dev-staging	Active	2019-02-28T13:22+0900	Direct PUT and other sources	Disabled	Amazon S3 csc-wafstest

© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

待機

1.11. Kinesis Firehose 設定

Firehose delivery streams

Kinesis Firehose delivery streams continuously collect, transform, and load streaming data into the destinations that you specify.

Successfully created delivery stream **aws-waf-logs-wafcham-waflog**
Next, send records directly to the delivery stream using the [Amazon Kinesis Agent](#) or the [Firehose API](#) using the [AWS SDK](#), or send records from [AWS IoT](#), [CloudWatch Logs](#), or [CloudWatch Events](#). [Learn more](#)

Create delivery stream Test with demo data Delete

Filter Firehose delivery streams

Name	Status	Created	Source	Record transformation	Destination
aws-waf-logs-wafcham-waflog	Active	2019-09-02T11:01+0900	Direct PUT and other sources	Disabled	Amazon S3 cs-wafteet

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

完了

1.12. 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 the 'Web ACLs' page with a 'Create web ACL' button and a 'Delete' button. Below this, there is a list of Web ACLs with a filter set to 'Asia Pacific (Tokyo)'. The 'RULE_TEST' Web ACL is selected. On the right, the 'Logging' tab is highlighted with a red box, and the 'Enable Logging' button is visible.

サービス “AWS WAF” に戻り

“Web ACLs” > “Logging” を選択

1.13. 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, there is a section for 'Web ACL' and 'IAM role'. The 'IAM role' section shows 'AWSServiceRoleForWAFRegionalLogging'. A dropdown menu for 'Amazon Kinesis Data Firehose' is highlighted with a red box, showing the selected value 'aws-waf-logs-wafcharm-waflog'. Below this, there is a 'Refresh' button and a note about selecting a Kinesis Data Firehose. The 'Redacted fields' section allows choosing fields to hide from logs. At the bottom right, there are 'Cancel' and 'Create' buttons, with the 'Create' button highlighted by a red box.

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

※ 1.3 で指定したもの

「Create」

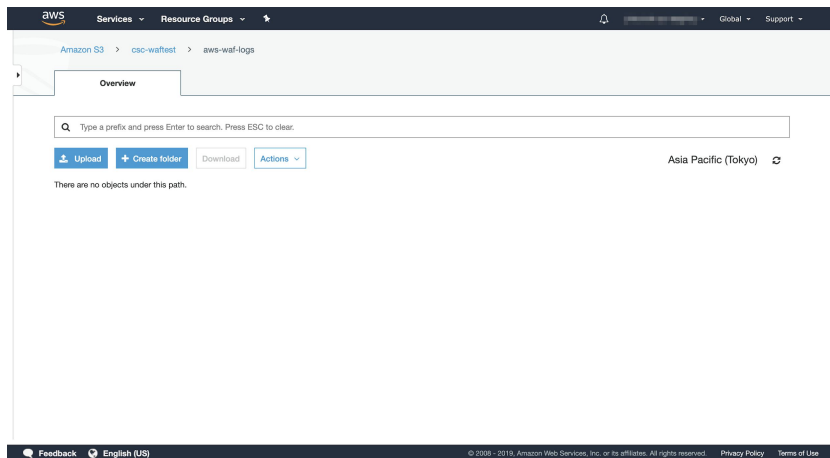
1.14. Kinesis Firehose と AWS WAF との連携設定

Logging が、“Enabled” になっていることを確認

The screenshot shows the AWS Management Console interface for configuring logging on a Web ACL. At the top, a green notification banner states: "Successfully enabled logging for this web ACL. AWS WAF will send the logs to your Kinesis Data Firehose." The left sidebar lists various AWS services, with "AWS WAF" selected. The main area is divided into two sections: "Web ACLs" and "RULE_TEST".

In the "Web ACLs" section, a list of Web ACLs is shown with "RULE_TEST" selected. In the "RULE_TEST" section, the "Logging" tab is active. The "Logging" section shows a toggle switch labeled "Logging" which is currently in the "Enabled" position. This toggle is highlighted with a red rectangular box. Below the toggle, it indicates that logs are sent to the "aws-waf-logs-wafcham-waflog" Kinesis Data Firehose stream. The "Redacted Fields" are listed as "None".

1.15. 1 章の完了確認

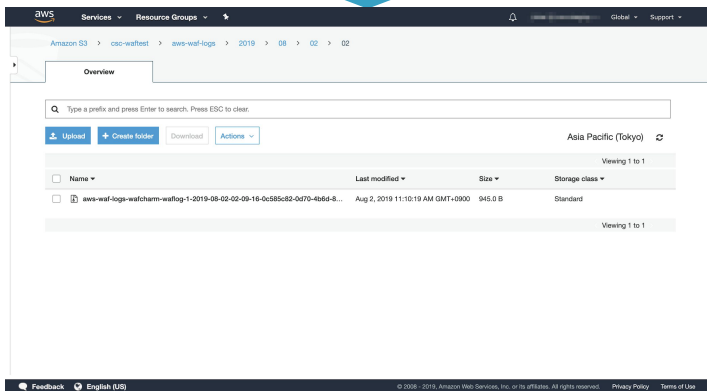
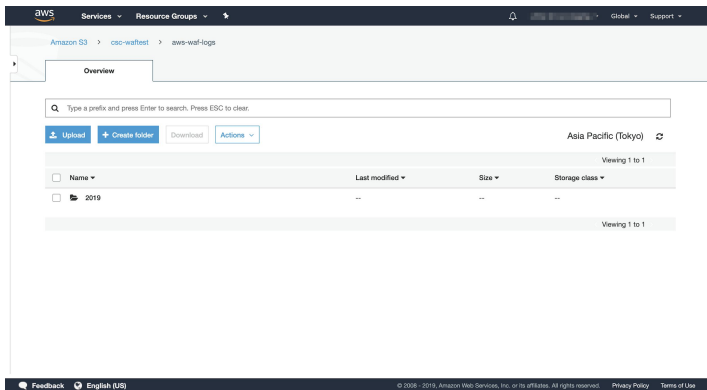


S3 にフルログファイルが生成されているか確認

※ 1.5 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

1.16. 1章の完了確認



左記のようなファイルが生成されれば

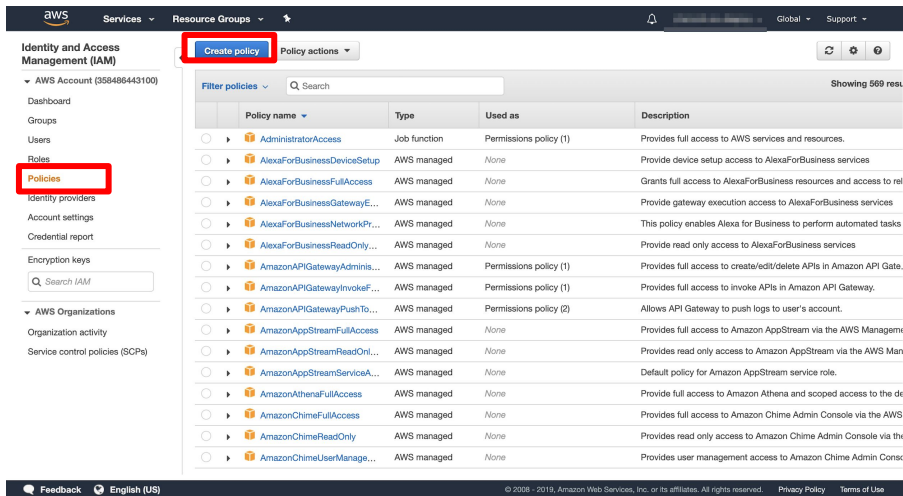
1章の作業は完了

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
- WacCharm 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



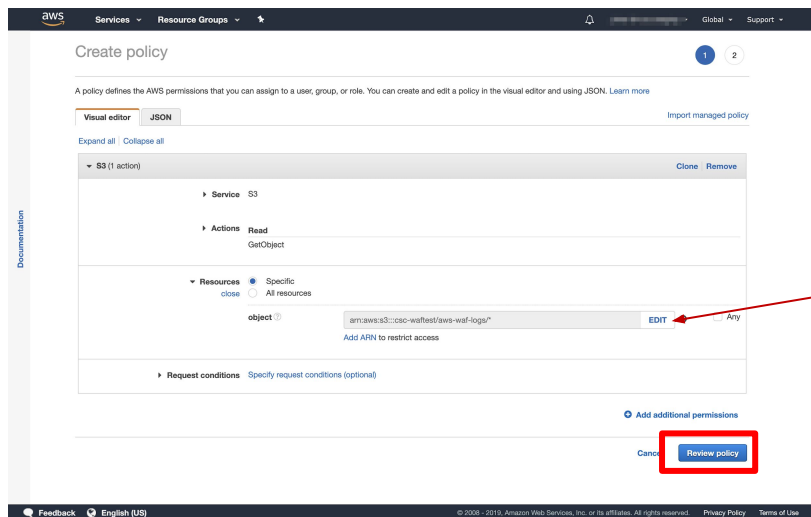
The screenshot shows the AWS IAM console interface. In the left-hand navigation menu, the 'Policies' option is highlighted with a red box. In the main content area, the 'Create policy' button is also highlighted with a red box. Below this, a table lists various AWS managed policies. The table has columns 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/*

※ 1.5 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 EDIT Any

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](#)

Bucket name * 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
S3	Limited: Write, Permissions management	BucketName string like wafcharm.com, ObjectPath string like All	None

* Required

Cancel Previous **Create policy**

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 'AWS service' selected. The 'Choose the service that will use this role' section has 'Lambda' selected. The 'Next: Permissions' button is highlighted.

1 2 3 4

Create role

Select type of trusted entity

AWS service
EC2, Lambda and others

Another AWS account
Belonging to you or 3rd party

Web identity
Cognito or any OpenID provider

SAML 2.0 federation
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

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

Cancel **Next: Permissions**

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

このロールを使用するサービスを選択 : Lambda

「Next: Permissions」

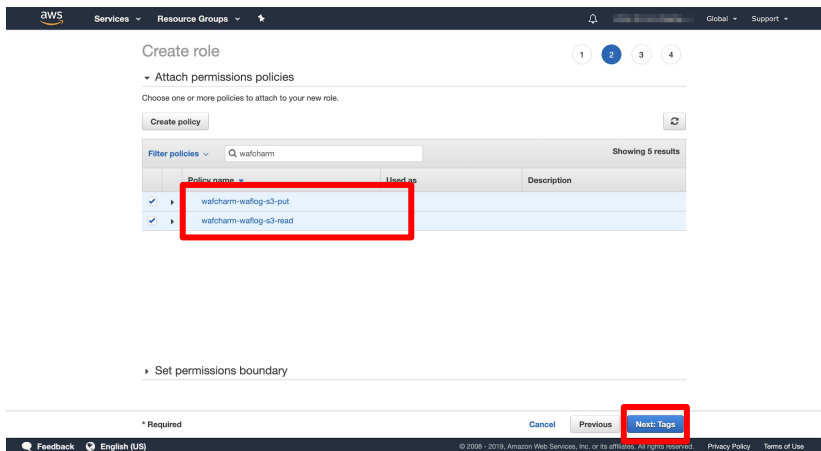
2.7. WafCharm 連携 Lambda 用 role 作成

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

「次のステップ: タグ」

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

The screenshot shows the AWS Lambda console interface for creating a new function. The 'Create function' page is displayed with the following details:

- Options:** Three options are available: 'Author from scratch' (selected), 'Use a blueprint', and 'Browse serverless app repository'.
- Basic information:**
 - Function name:** 'wafcharm-waflog' (with a note: 'Use only letters, numbers, hyphens, or underscores with no spaces.')
 - Runtime:** 'Node.js 10.x' (selected from a dropdown menu).
 - Permissions:** 'Use an existing role' is selected under the 'Choose or create an execution role' section. The existing role 'wafcharm-waflog' is chosen from a dropdown.
- Buttons:** 'Cancel' and 'Create function' (highlighted with a red box) are located at the bottom right.

名前 : wafcharm-waflog (任意)

Runtime : Node.js 10.x 以上

Role : Use an existing role

既存のロール : wafcharm-waflog

※ 2.10 で作成したもの

※ 1.5 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)

The screenshot displays the AWS Lambda console configuration for a function named 'wafcharm-waflog'. The 'Function code' section is highlighted with a red box and labeled '関数コード'. The code is a JavaScript file named 'index.js' containing WafCharm configuration. The 'Basic settings' section is also highlighted with a red box and labeled '基本設定', showing the function description 'WafCharm連携用', memory size of 128 MB, and a timeout of 1 minute.

```
1 'use strict';
2
3 const toBucket = process.env.WAFCHARM_BUCKET || 'wafcharm.com';
4 const toPath = process.env.WAFCHARM_PATH || 'waflog/acceptance/v1';
5 const url = `bucket-${toBucket}-${toPath}`;
6
7 const AWS = require('aws-sdk');
8 const s3 = new AWS.S3();
9
10 const VERSION = '2006-03-01';
11
12
```

Function code :

以下のソースを貼り付け

http://docs.wafcharm.com/manual/new_aws_waf/index.js

Basic settings

Description : WafCharm 連携用 (任意)

Timeout : 1 分

2.13. Lambda 構築 (トリガー)

The screenshot shows the 'Add trigger' configuration page in the AWS Lambda console. The 'Trigger configuration' section is expanded, showing the following settings:

- Trigger configuration:** S3 (aws storage)
- Bucket:** csc-waf-test
- Event type:** All object create events
- Prefix:** aws-waf-logs/
- Suffix:** (empty)
- Enable trigger:** Enable trigger now, or create it in a disabled state for testing (recommended).

The 'Add' button at the bottom right of the configuration form is highlighted with a red box.

Designer :
トリガーに S3 を選択

トリガーの設定

バケット: 1.5 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 : 1.5 で設定した prefix

トリガーの有効化 : check

「追加」

2.14. Lambda 構築

The screenshot displays the AWS Lambda console configuration page for the function 'wafcharm-waflog-hiraitest'. The top navigation bar includes 'AWS', 'Services', 'Resource Groups', and the current region 'Tokyo'. The breadcrumb trail shows 'Lambda > Functions > wafcharm-waflog-hiraitest'. The function's ARN is 'arn:aws:lambda:ap-northeast-1:358486443100:function:wafcharm-waflog-hiraitest'. Below the breadcrumb, there are controls for 'Throttle', 'Qualifiers', 'Actions', and a 'Test' button. A red box highlights the 'Save' button. The main configuration area is divided into 'Configuration' and 'Monitoring' tabs. The 'Designer' section shows a visual representation of the function's execution path, including an S3 trigger, the function 'wafcharm-waflog-hiraitest', and destinations for Amazon CloudWatch Logs and Amazon S3. The 'S3' section below shows the function is enabled and has access to the 'csc-waf-test' bucket, with details for the event type 'ObjectCreated', notification name, and prefix.

「保存」

2.15. Lambda 構築

The screenshot displays the AWS Lambda console interface for the function 'wafcharm-waflog-hiraitest'. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and a user profile. The breadcrumb trail shows 'Lambda > Functions > wafcharm-waflog-hiraitest'. The function's ARN is 'arn:aws:lambda:ap-northeast-1:358486443100:function:wafcharm-waflog-hiraitest'. Action buttons include 'Throttle', 'Qualifiers', 'Actions', 'Select a test event', 'Test', and 'Save'. The 'Configuration' tab is active, showing a 'Designer' section with a diagram of the function's configuration. The diagram includes a 'wafcharm-waflog-hiraitest' function box with a 'Layers' section containing '(0)' layers. A trigger box labeled 'S3' is connected to the function. Below the trigger, there are sections for 'Amazon CloudWatch Logs' and 'Amazon S3'. The 'Amazon S3' section shows a resource named 'csc-wafitest' with an 'Enabled' toggle and a 'Delete' button. The event type is 'ObjectCreated', the notification name is '87230023-181b-4761-a04d-6aee094047b3', and the prefix is 'aws-waf-logs/'. The footer contains 'Feedback', 'English (US)', and copyright information for Amazon Web Services, Inc. (2008-2019).

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

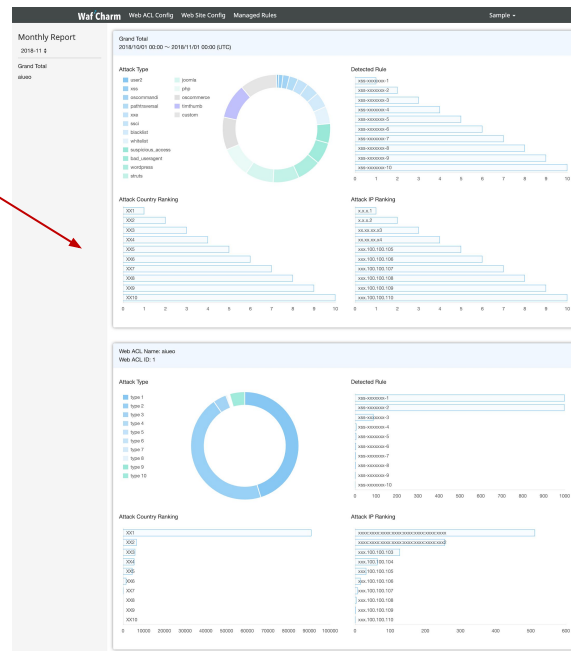
1. 1～2章までの設定が完了している
2. 前月に検知があった

※ 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

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

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	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
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

WafCharm 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@example.com	⊗
alert@sample.com	⊗
example@cscloud.co.jp	⊗
example@cscloud.co.jp	⊗
example@cscloud.co.jp	⊗
example@cscloud.co.jp	⊗
example@cscloud.co.jp	⊗
example@cscloud.co.jp	⊗
example@cscloud.co.jp	⊗
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

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

The screenshot shows the WafCharm configuration page. At the top, there is a navigation bar with 'WafCharm', 'Web ACL Config', 'Web Site Config', 'Managed Rules', and 'Sample'. Below this, the 'Notification : Detail' section is visible, with a breadcrumb trail '< Web ACL Config | Edit'. A table lists configuration items: 'Web ACL ID' (xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx), 'Web ACL Name' (Sample_Web_ACL), 'WafCharm Email Notification' (ON, highlighted with a red box), and 'Managed Rule Email Notification' (OFF). Below the table is the 'Notification email' section, which includes an 'Edit' link and a table with columns 'Email' and 'Set date'. The 'Email' column contains 'notification@example.com' and 'alert@sample.com'. At the bottom of the page, there is a footer with the text 'copyright © Cyber Security Cloud, Inc. All Rights Reserved | お問い合わせ'.

「WafCharm Email Notification」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 Name: wafcharm-blacklist-685

Time(UTC): Thu, 01 Apr 2020 20:20:00 GMT

Source IP: 153.156.84.123

Source Country: JP

Action: BLOCK

URI: /

5. 通知機能に関する補足事項

- 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
- 通知間隔は、[1.6 Kinesis Firehose 設定](#) の Buffer intervals、Buffer size で設定した値に応じて変化します
- new AWS WAF 仕様の WafCharm では CSC マネージドルールとの連携機能はないため、AWS WAF Classic 仕様で利用可能な CSC マネージドルール専用の通知機能はありません
- お客様作成のルールグループを使用していないルールでの COUNT 検知は通知されません

6. 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、[1.3](#) にて設定した「Delivery Stream Name」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
 - 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