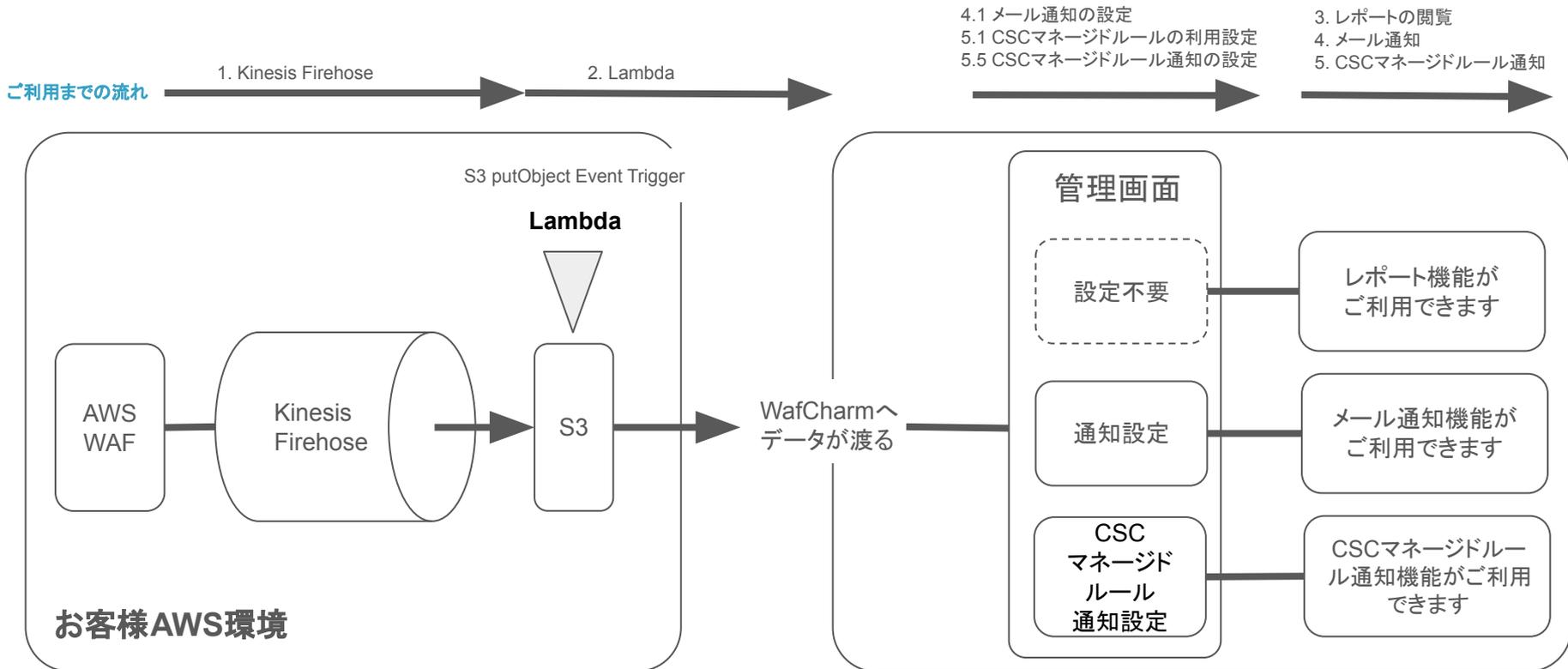


レポート機能/通知機能 利用マニュアル
Ver 1.5

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

The screenshot shows the AWS IAM console interface for a user. At the top, there are tabs for 'Permissions', 'Groups (2)', 'Tags', 'Security credentials', and 'Access Advisor'. The 'Permissions' tab is active, showing a dropdown for 'Permissions policies (18 policies applied)'. Below this, there is a blue 'Add permissions' button and a '+ Add inline policy' link. A table lists the attached policies, categorized under 'Attached directly'. The table has two columns: 'Policy name' and 'Policy type'. Each row includes a right-click icon (X) for removal.

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 full 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

- WafCharm管理画面にて、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

- WafCharm管理画面にて、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

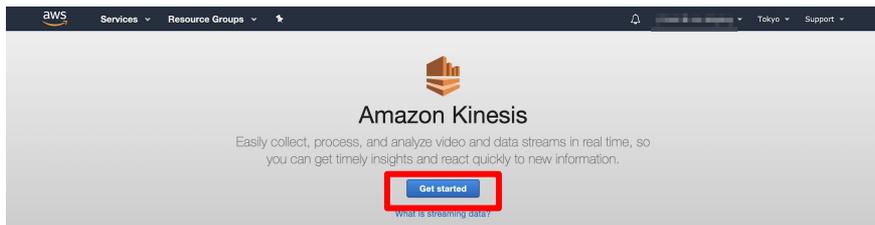
7. その他補足事項

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」をクリックします

What can you build with Amazon Kinesis?

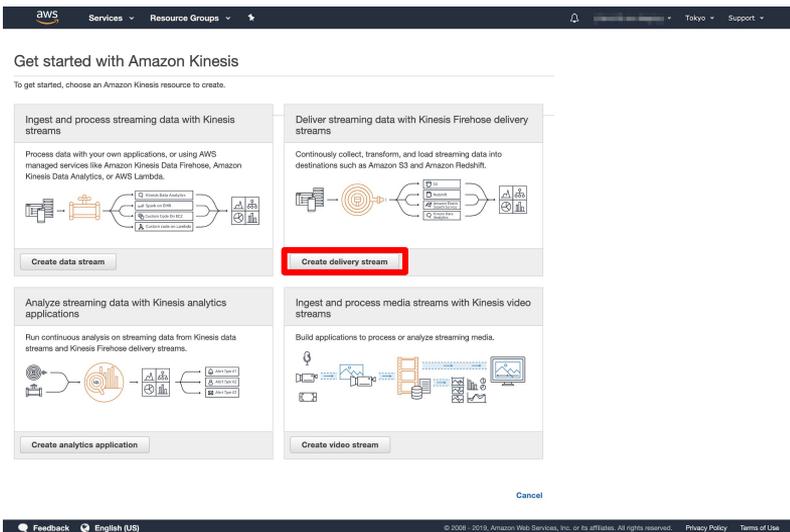
Evolve from batch to real-time analytics



Build real-time applications



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
    Source[Source] --> Firehose[Firehose delivery stream]
    subgraph Firehose
        direction TB
        SR[Source records]
        PR[Processed records]
        SR --- PR
    end
    Firehose --> Destination[Destination]
```

..... 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

The screenshot shows the AWS Kinesis Firehose console interface for creating a delivery stream. The page is titled "Kinesis Firehose - Create delivery stream" and is on "Step 2: Process records".

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

Process records data flow overview

The flow overview diagram shows the following steps:

- Source records (represented by three document icons) flow into Processed records.
- Under "Processed records", there are two sub-steps: "Transform source records" and "Convert record format".
- Arrows indicate the flow from Source records to Transform source records, then to Convert record format, and finally to the final destination (represented by three document icons).
- Below "Transform source records", it says "Invoke AWS Lambda function".
- Below "Convert record format", it says "Refer to AWS Glue table for schema".
- A dashed box labeled "Optional" encloses the "Transform source records" and "Convert record format" steps.

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 from a table defined in AWS Glue (F). 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 OpenT_JSON SerDe. For other options use the AWS CLI.

* Required

Buttons: Cancel, Previous, **Next** (highlighted with a red box)

「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)
Source records → Processed records → S3 bucket (destination)
If processing lags → S3 bucket (optional backup)

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-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

「Next」

1.6. 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

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
 Zp

S3 encryption* Disabled
 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 Remove tag

Add tag
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 Create new or choose (f)

* Required Cancel Previous Next

Feedback English (US) © 2018 - 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

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

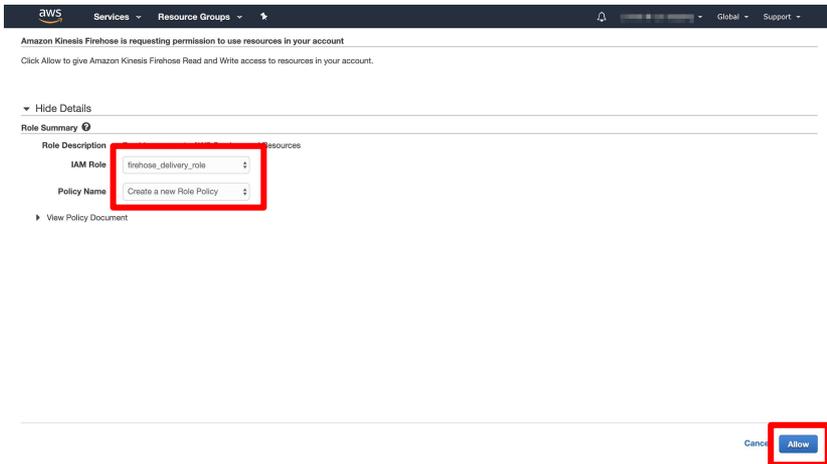
Buffer size :
推奨は 5 MB

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 Tokyo Support

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

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

Review
Review your configuration details before creating your delivery stream.

Name and source [Edit](#)

Delivery stream name aws-waf-logs-wafchrm-waflog

Source Direct PUT or other sources
After creating the delivery stream, send records directly to the delivery stream, or send records from AWS IoT, CloudWatch Logs, or CloudWatch Events.

Process records [Edit](#)

Source record transformation Disabled

Record format conversion Disabled

Destination [Edit](#)

Destination Amazon S3

S3 bucket [csc-wafest](#)

S3 bucket prefix aws-waf-logs/

S3 bucket error prefix no error prefix specified

Settings [Edit](#)

S3 buffer conditions 5 MB or 60 seconds

Compression GZIP

Encryption Disabled

Error logging Enabled

Tags no tags specified

IAM role [firehose_delivery_role](#)

[Cancel](#) [Previous](#) [Create delivery stream](#)

「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 aws-waflogs

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 configuration for a Web ACL named 'RULE_TEST'. The 'Logging' tab is selected and highlighted with a red box. Below the 'Full logging' section, 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: RULE_TEST' and an 'IAM role' section. In the 'IAM role' section, a dropdown menu is open, showing 'Amazon Kinesis Data Firehose' as the selected option, which is highlighted with a red rectangular box. Below this, there is a 'Refresh' button and a note about selecting a Kinesis Data Firehose. The 'Redacted fields' section is visible below, with a note that no fields are currently redacted. At the bottom right of the form, there are 'Cancel' and 'Create' buttons, with the 'Create' button highlighted by a red rectangular box. The footer of the console shows 'Feedback', 'English (US)', and copyright information.

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

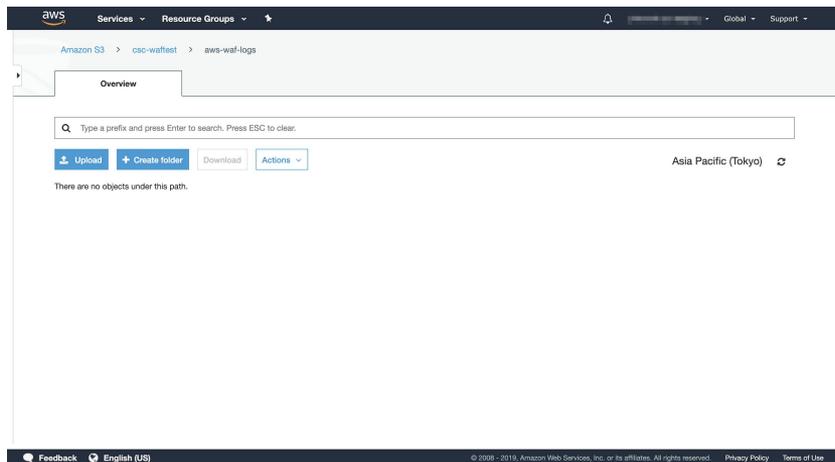
「Create」

1.14. Kinesis FirehoseとAWS WAFとの連携設定

The screenshot shows the AWS WAF console interface. 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." Below this, the "Web ACLs" section is visible, with a list of web ACLs. The "RULE_TEST" web ACL is selected. The "Logging" tab is active, showing the configuration for logging. The "Logging" status is set to "Enabled", which is highlighted with a red box. The "Kinesis Data Firehose stream" is set to "aws-waf-logs-wafcham-waflog". The "Redacted Fields" are set to "None".

Loggingが、“Enabled”になっていることを確認

1.15. 1章の完了確認

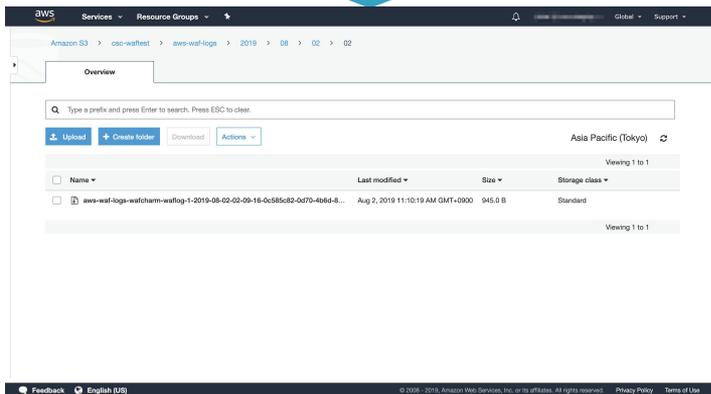
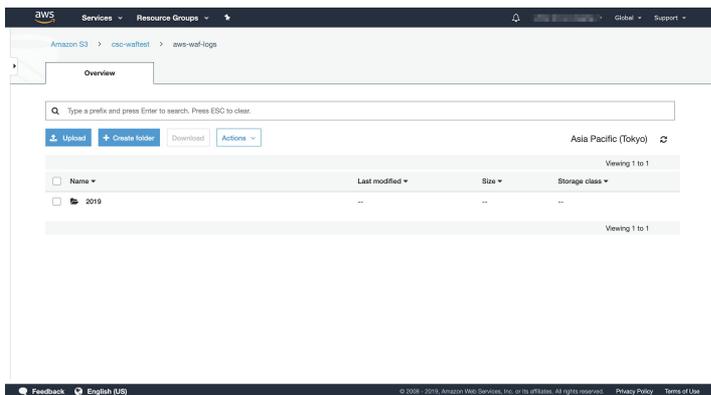


S3にフルログファイルが生成されているか確認

※ 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full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

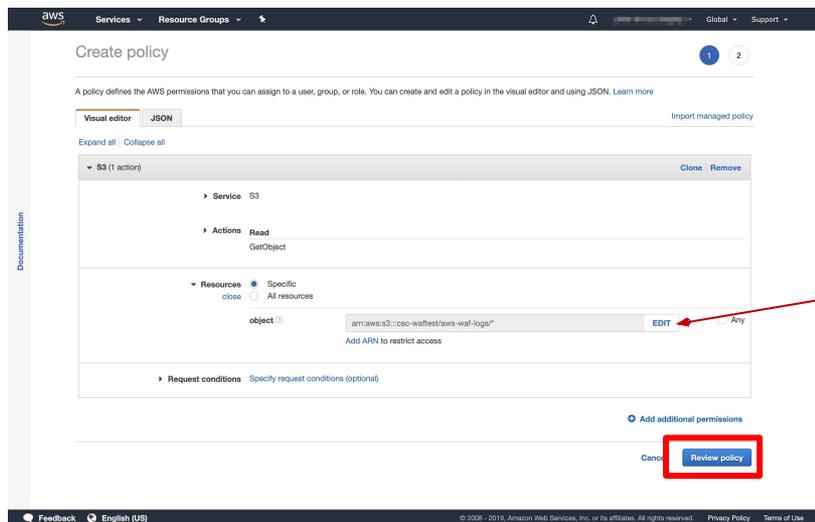
The screenshot shows the AWS IAM console interface. In the left-hand navigation pane, the 'Policies' menu item is highlighted with a red box. In the main content area, the 'Create policy' button is highlighted with a red box. Below this, a table lists various AWS managed policies. The table has the following columns: Policy name, Type, Used as, and Description. The table contains 15 rows of policies, including AdministratorAccess, AlexaForBusinessDeviceSetup, AlexaForBusinessFullAccess, AlexaForBusinessGatewayE..., AlexaForBusinessNetworkPr..., AlexaForBusinessReadOnly..., AmazonAPIGatewayAdmin..., AmazonAPIGatewayInvokeF..., AmazonAPIGatewayPushTo..., AmazonAppStreamFullAccess, AmazonAppStreamReadOnl..., AmazonAppStreamServiceA..., AmazonAthenaFullAccess, AmazonChimeFullAccess, AmazonChimeReadOnly, and AmazonChimeUserManage...

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
AmazonAPIGatewayAdmin...	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-wafest/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**

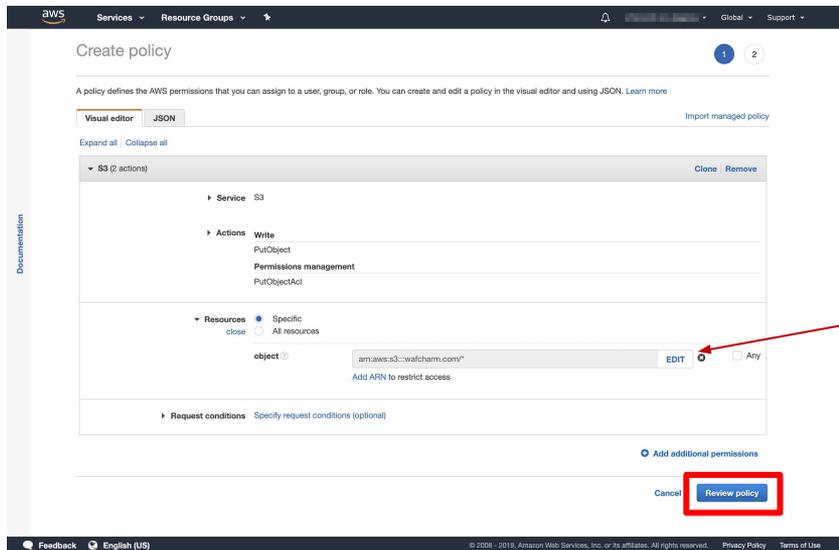
Feedback English (US) © 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Name:
wafcharm-waflog-s3-read (任意の名前)

Description : WafCharm (任意)

「Create policy」

2.4. WafCharm連携用full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full権限policy作成

Create policy

Review policy

Name*
Use alphanumeric and "+=,@-." characters. Maximum 128 characters.

Description
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

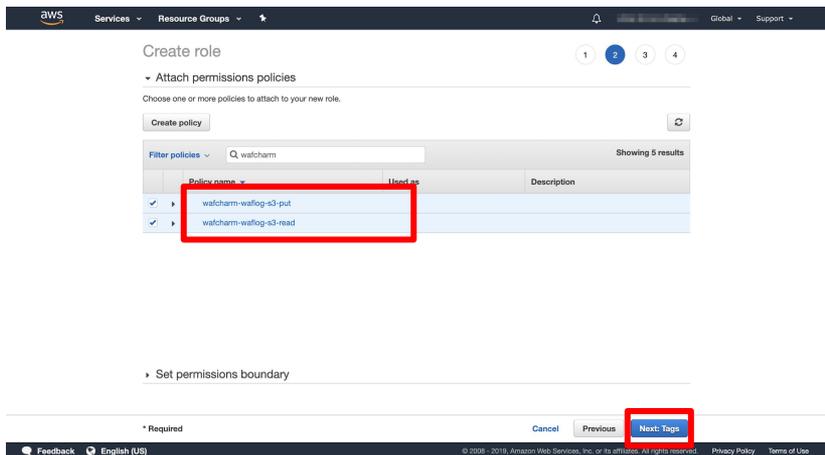
The screenshot shows the AWS IAM console 'Create role' page. The 'Select type of trusted entity' section has four options: 'AWS service', 'Another AWS account', 'Web identity', and 'SAML 2.0 federation'. The 'Choose the service that will use this role' section is expanded to show a list of services.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

Service	Service	Service	Service	Service
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

このロールを使用するサービスを選択 :Lambda

「Next: Permissions」

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

※2.2., 2.4.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"/>	

You can add 50 more tags.

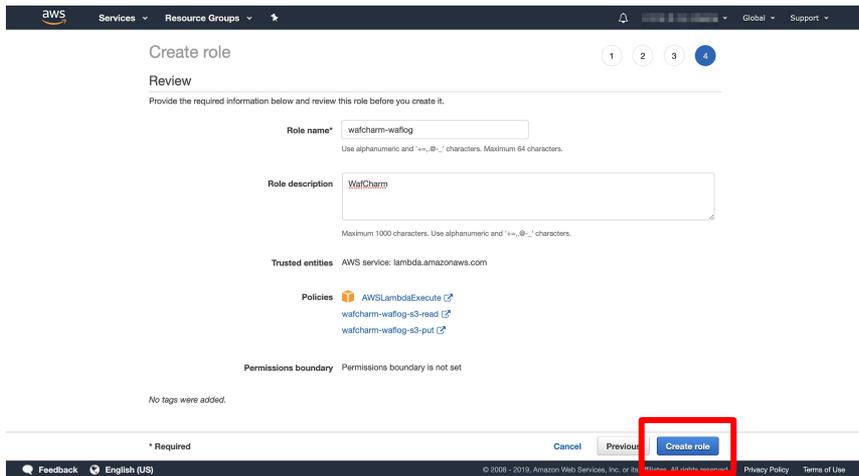
Cancel Previous **Next: Review**

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 has a dark header with the AWS logo and navigation menus. Below the header, there are four numbered steps (1, 2, 3, 4) with step 4 being the active one. The main content area is titled 'Review' and contains the following fields:

- Role name:** A text input field containing 'wafcharm-waflog'. Below it, a small note says 'Use alphanumeric and '+, -, @, _' characters. Maximum 64 characters.'
- Role description:** A text area containing 'WafCharm'. Below it, a small note says 'Maximum 1000 characters. Use alphanumeric and '+, -, @, _' characters.'
- Trusted entities:** A dropdown menu showing 'AWS service: lambda.amazonaws.com'.
- Policies:** A list of three policies: 'AWSLambdaExecute', 'wafcharm-waflog-s3-read', and 'wafcharm-waflog-s3-put', each with a link icon.
- Permissions boundary:** A dropdown menu showing 'Permissions boundary is not set'.

At the bottom of the form, there are three buttons: 'Cancel', 'Previous', and 'Create role'. The 'Create role' button is highlighted with a red rectangular box. Below the buttons, there is a footer with 'Feedback', 'English (US)', and copyright information.

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
 - Runtime:** Node.js 10.x
 - Permissions:** Use an existing role (selected). The existing role is wafcharm-waflog.
- 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

※ 2.8.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 interface 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 snippet for WafCharm. The 'Basic settings' section is also highlighted with a red box and labeled '基本設定', showing the description 'WafCharm連携用', memory 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   apiVersion: '2006-03-01',
10 });
```

Function code :

以下のソースを貼り付け

<http://docs.wafcharm.com/manual/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 interface for the function 'wafcharm-waflog-hiraitest'. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and the current region 'Tokyo'. The function's ARN is shown as 'arn:aws:lambda:ap-northeast-1:358486443100:function:wafcharm-waflog-hiraitest'. Below the navigation, there are controls for 'Throttle', 'Qualifiers', 'Actions', and a 'Save' button, which is highlighted with a red rectangle. The main area is divided into 'Configuration' and 'Monitoring' tabs, with 'Configuration' selected. Under the 'Designer' section, a visual diagram shows the function 'wafcharm-waflog-hiraitest' with a 'Layers' section containing '(0)' layers. Below this, there are sections for 'S3' (with an 'Add trigger' button) and 'Amazon CloudWatch Logs' (with an 'Amazon S3' sub-section). At the bottom, the 'S3' section details a log group 'csc-wafitest' with an 'Enabled' toggle and a 'Delete' button. The event type is 'ObjectCreated', the notification name is '87230023-181b-4761-a044-6aee09404763', and the prefix is 'aws-waf-logs/'.

「保存」

2.15. Lambda構築

The screenshot displays the AWS Lambda console configuration page for the function 'wafcharm-waflog-hiraitest'. The interface includes a navigation bar with 'Services', 'Resource Groups', and 'Tokyo' (region). The function's ARN is shown as 'arn:aws:lambda:ap-northeast-1:35846443100:function:wafcharm-waflog-hiraitest'. Below the function name, there are controls for 'Throttle', 'Qualifiers', 'Actions', 'Select a test event', 'Test', and 'Save'. The 'Configuration' tab is active, showing a 'Designer' section with a visual diagram of the function's configuration. The diagram includes a central function box 'wafcharm-waflog-hiraitest' with a 'Layers' section below it. To the left, an 'S3' trigger is connected to the function. Below the trigger, there is an 'Add trigger' button. To the right, 'Amazon CloudWatch Logs' and 'Amazon S3' are listed as resources. Below the resources, there is a section for 'S3' with a table listing a bucket named 'csc-waf-test' with an 'Enabled' toggle and a 'Delete' button. The table row contains: 'csc-waf-test', 'arn:aws:s3:::csc-waf-test', 'Event type: ObjectCreated', 'Notification name: 87230023-181b-4761-a04d-6aee094047b3', and 'Prefix: aws-waf-logs/'. The footer of the console shows '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

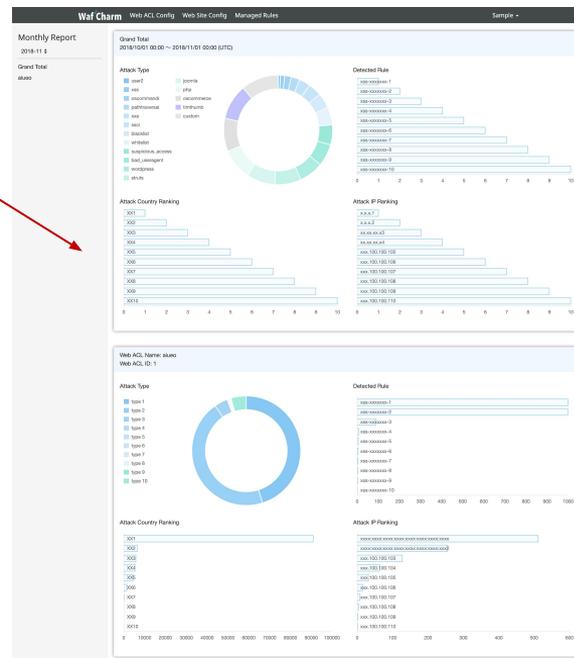
1. 1～2章までの設定が完了している
2. 前月に検知があった

※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

- WafCharm管理画面にて、メール通知の設定
- メール通知内容

4.1. メール通知の設定



WafCharm管理画面

上部メニューより、「WebACL Config」を選択

4.2. メール通知の設定

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'. The page title is 'Web ACL Config' with links for '< Back' and 'Add ACL'. A table lists the configuration details for a specific Web ACL. The 'Web ACL Name' column contains the value 'Sample_Web_ACL', which is highlighted with a red rectangular box. To the right of the table row are icons for a link and a settings gear.

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

対象の「Web ACL Name」を選択

4.3. メール通知の設定

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
Email Address	sample@example.com
WafCharm Email Notificatoin	OFF
Managed Rule Email Notificatoin	OFF

「Edit」を選択

4.5. 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」

4.6. メール通知の設定

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
Email Address	sample@example.com
WafCharm Email Notification	<input checked="" type="checkbox"/> ON
Managed Rule Email Notification	<input type="checkbox"/> OFF

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

4.7. メール通知内容

検知されると、下記メールが WafCharm 管理画面アカウントのメールアドレス宛てに通知されます

- 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 管理画面アカウントのメールアドレス

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(WebACL 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 Aug 2019 09:21:03 GMT

Source IP: 192.0.2.0

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 HighSecurity 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

- WafCharm管理画面上での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
- 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', 'Managed Rules', and 'Sample'. Below the header, there are navigation links for 'Back' and 'Show'. The main content area contains a form with the following fields:

- Web ACL ID * (text input)
- Web ACL Name * (text input)
- Web ACL Access Key * (password input)
- Web ACL Secret Key * (password input)
- edit access key and secret key? (link)
- Rule limit (dropdown menu)
- Choose AWS service type * (dropdown menu)
- Choose your AWS region * (dropdown menu)
- Blacklist (text input)
- Whitelist (text input)
- Default AWS WAF Action (dropdown menu)
- Use Managed Rule (dropdown menu with 'used' selected)
- Save button (highlighted with a red box)

At the bottom of the page, there is a 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機能の設定

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機能の設定

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
Email Address	sample@example.com
WafCharm Email Notificatoin	<input checked="" type="checkbox"/> ON
Managed Rule Email Notificatoin	<input type="checkbox"/> OFF

「Edit」を選択

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](#)

5.7. CSCマネージドルール通知機能の設定

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 Notificaiton	<input checked="" type="radio"/> ON <input type="radio"/> OFF
Managed Rule Email Notificaiton	<input checked="" type="radio"/> ON <input type="radio"/> OFF

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

5.8. CSCマネージドルール通知機能の設定

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
Email Address	sample@example.com
WafCharm Email Notificaiton	ON
Managed Rule Email Notificaiton	ON

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

5.9. CSCマネージドルール通知内容

検知されると、下記メールが WafCharm 管理画面アカウントのメールアドレス宛てに通知されます

- 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 管理画面アカウントのメールアドレス

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(WebACL 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): Tue, 19 Feb 2019 02:09:35 GMT

Source IP: 192.0.2.0

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 の通知機能は対象の Web ACL Config における通知機能 の ON / OFF に関わらず検知内容を通知します
 - 本マニュアルにて作成した 1 つの Kinesis Firehose を複数の Web ACL に連携している
 - 上記連携をしている Web ACL を 2 つ以上 WafCharm に登録している
 - 上記 Web ACL の内 1 つでも WafCharm の通知機能を ON にしている

- 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 (Cyber Security Cloud Managed Rules for AWS WAF HighSecurity OWASP Set) を利用している
 - 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

6. 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
- アカウントに登録されているメールアドレス以外に通知することはできません
 - 現在、機能拡張検討中

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