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		
- Permissi	ons policies (18 polici	es applied)			
Add permise	sions					• Add inline policy
Policy	name 🔻				Policy type 👻	
Attached dire	ectly					
AW:	SLambdaFullAcc	ess			AWS managed policy	×
) 🧵 🚺 IAM	FullAccess				AWS managed policy	×
File Cloud	udWatchFullAcce	ess			AWS managed policy	×
🕨 🧵 Ama	azonKinesisFireh	oseFullAcc	ess		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. <u>CSCマネージドルール通知機能をご利用される場合</u>
 - 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. <u>その他補足事項</u>

1. Kinesis Firehose

WAF ログを S3 に転送する Kinesis Firehose を設定

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

1.1. Kinesis Firehose 設定



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

適用予定のAWS WAF(Web ACL) と同じリージョン で作成

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

1.2. Kinesis Firehose 設定

aws	Services 🔻	Q Search for services, features, marketplace products, and docs	[Option+S]	〕 ⇔	tearved550_walchern-support_w890%w686045xs2/Losto @ co	Tokyo
=	Create a	delivery stream Info				
	► Amazon	Kinesis Data Firehose: How it works				
	Choose sou Specify the source it has been create	rrce and destination e and the destination for your delivery stream. You cannot change the source and rd.	ind destination of your delive	very stream once		
	Source Info Direct PUT]	•			
	Destination I Amazon S3		•			
	Delivery str	ream name				
	Delivery stream	n name 	periods.			
	Transform a	and convert records - <i>optional</i>				

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

aws	Services 🔻	Q Search for services, features, marketplace products, and docs	[Option+S]	∑ \$	ANTINUM	red50,eAhem spp	rt_e690faed8d343cs2/Lasts @ csc.	🔻 Tokyo 🔻	-
=	Transform Configure Kinesis	and convert records - optional Is Data Firehose to transform and convert your record data.							
	Transform sou Kinesis Data Firef The specified AW to the specified d	urce records with AWS Lambda Info hose can invoke an AWS Lambda function to transform, filter, un-compress, cr VS Lambda function can also be used to provide dynamic partitioning keys for destination.	onvert and process your the incoming source da	source data rec ta before its del	ords. livery				
	Bata transform Babled Enabled	mation							
	Convert record Data in Apache P formatted source function that con	rd format info Parquet or Apache ORC format is typically more efficient to query than JSON. excends using a schema from a table defined in AWS Glue [2]. For records th nverts them to JSON in the Transform source records with AWS Lambda sectio	Kinesis Data Firehose ca at aren't in JSON forma in above.	n convert your . , create a Lamb	ISON- da				
	Enabled	t conversion							
	Destination	n settings Info							
	S3 bucket	mation settings for your octively su carff.							
	Choose a buck	cket or enter a bucket URI	Browse	Create	Ľ				

∞ 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

	aws	Services 🔻	Q Search for services, features, marketplace products, and docs [Option+S] D
≡		Destination Specify the destin	settings Info ation settings for your delivery stream.
		S3 bucket csc-waftest	Browse Create 🖸
	j.	Dynamic partition Dynamic partition partition your sou you create a new s additional e Dsabled Enabled	ioning Info mg enables provides participated data sets by partitizating dreaming 53 data based on partitioning keys. You can be a set of the partition of the specified AMS Landak function. You can enable remaining participations only when delivery stram. You can enable dynamic partitioning for an existing dynamic partitioning costs per GiB of partitioned data. For more information, see Kinelis Data Firehose pricing. C
		S3 bucket prefi By default, Kinesis default by specify waflog/	x - optionol Duba Fierbeas appends the prefix "YYY/MM(dd/MH" (in UTC) to the data it delivers to Amazon SS. You can override this an autom prefix that includes expressions that are evaluated at runtime.
		You can repeat th S3 bucket error You can specify an to evaluate at run	e same keys in your S3 bucket prefix. Maximum S3 bucket prefix characters: 1024. output prefix - optional S3 bucket prefix to be used in error conditions. This prefix can include expressions for Kinesis Data Firehose time.
		Enter a prefix	

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

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

upport 🔻

※ 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

	Q Search for services, features, marketplace products, and docs [Option+S] 🔰 🗛 🔹 🔻 Tokyo 🔻 Supp
Buffer size The higher buff	e may be lower in cost with higher latency. The lower buffer size will be faster in delivery with higher cost and less MIB man: 128 MIB. Recommended: 5 MIB.
Buffer interva The higher inte	illows more time to collect data and the size of data may be bigger. The lower interval sends the data more frequently an tageous when looking at aborter cycles of data activity.
60	seconds
L	maximum: 900 seconds. Recommended: 300 seconds.
Kinesis Data Fir bucket using an	c an compress records before delivering them to your 53 bucket. Compressed records can also be encrypted in the 53 Key Management Service (IO45) master key.
Compression Kinesis Data Fir Disabled Grup	Stat records can compress records before delivering them to your 53 bucket.
Compression Kinesis Data Fir Disabled GrIP Snappy	Sata records can compress records before delivering them to your 53 bucket.
Compression Kinesis Data Fir Disabled Grup Snappy Zip Hadoop-C	atar records and a second seco
Compression Kinesis Data Fir Disabled OrtP Snappy Zip Hadoop-C Encryption for Compressed ree	Jata records can compress records before delivering them to your 53 bucket.

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



aws	Services 🔻	Q Search for services, features, marketplace products, and docs [Option+S] D A Tokyo V Support V
=	 Advance Server-side e 1635830651 	d settings morphing enabled; UM role KinesisFirehousServiceRole-PUT-S3-K-ap-northeast-1- 175; no tags.
	Server-side en You can use AWS across a wide ran	kcryption info Kcry Nanapament Service (OHS) to create and manage Customer Master Koys (CMR) and to control the use of encryption get AVM Sarvices in your applications.
	Enable serv	ver-side encryption for source records in delivery stream
	Amazon Cloud Choose Enabled i	dWatch error logging Info If you want Kinesis Data Firehose to log record delivery errors to CloudWatch Logs.
	O Disabled	
	Enabled	
	Permissions Kinesis Data Firef	Info hose uses this MM role for all the permissions that the delivery stream needs. To specify different roles for the different the API or the CLL
	Create or u Creates a new	pdate IAM role w role or updates an existing one and adds the required policies to it, and enables Kinesis Data Firehose to assume it.
	O Choose exist the role that	sting IAM role you choose must have policies that include the permissions that Kinesis Data Firehose needs.
	Tags Info	
	You can add tags	to organize your AWS resources, track costs, and control access.
	No tags associa	ated with the resource.
	Add new ta	ag
	You can add up to	a 50 more tags.
		Cancel Create delivery stream

IAM Role : 新しいIAM ロールの作成 or 選択

Create delivery stream

1.7. Kinesis Firehose 設定

Cale base water base base as a log data		Q Search for services, features, blogs, docs, and more	[Option+S]	∑ 🗘 ▼ Tekyo ▼ Support ♥
Anazon Kones, Delevery stream i zer-verifogo-sox sox sox aws-waf-logs-xxxx-xxxx is better delivery stream	Creating aws-waf-logs-xxxx-xxxx it can take up to 5 minutes before the status is updated.			0
exters-waf-logs-xxxx-xxxx betweey stream	Amazon Kinesis > Delivery streams > aws-waf-logs-xxxx-xxxx			1
Delivery stream details Destruction Conting Destruction Maxees 53 Destruction Deaded Creation thine Newmetr 12, 2021, 15.58 (0H*9 Source Direct rUT ARI Dipatic partitioning Deaded Dipatic partitioning Deaded Creation thine Newmetr 12, 2021, 15.58 (0H*9 I Test with demo data Image: 10 to the the configuration of the conf	aws-waf-logs-xxxx-xxxx 🗤			Delete delivery stream
Status Destruction Ann Disbade Creating Source T Ann Disbade Disbade Porter T Ann Disbade Disbade * Test with demo data two Destruction the endpointer of port delary stream. Reacted Amazen Rises Data Freiner charges upply Destruction the endpointer of port delary stream. Reacted Amazen Rises Data Freiner charges upply * Test with demo data two Configuration Destruction the endpointer of port delary stream. Reacted Amazen Rises Data Freiner charges upply * Test with demo data two Destruction the endpointer of port delary stream. Reacted Amazen Rises Data Freiner charges upply * Test with demo data two Destruction the endpointer of port delary stream. Reacted Amazen Rises Data Freiner charges upply * Test with demo data two Destruction the endpointer of port delary stream. Reacted Amazen Rises Data Freiner charges upply * Test with demo data two Destruction the endpointer of port delary stream. Reacted Amazen Rises Data Freiner charges upply * Test with demo data two Destruction the endpointer of port delary stream. Reacted Amazen Rises Data Freiner charges upply * Test with demo data two Destruction the endpointer of port delary stream. Reacted Amazen Rises Data Freiner charges upply * Test with demo data two Destruction the endpointer of port delary stream. Reacted Amazen Rises Data Freiner charges upply * Test with demo data two Distruction the endpointer of port delary stream. React	Delivery stream details			
Contraining Anazon 53 Diabled Newmetrer 12, 2021, 1536 60f1+9 Source of the contraining of the contr	Status	Destination	Data transformation	Creation time
Source Direct PUT ANI ANI Direct PUT Dynamic participant Deabled De	⊖ Creating	Amazon S3	Disabled	November 12, 2021, 15:58 GMT+9
Direct HyT Disologies of your difference of your di	Source	ARN	Dynamic partitioning	
	Direct PUT	 A statistical statistic metallicity and statistical 	Disabled	
Delivery stream metrics une In 3h 12h 1d 3d 1w Custom B C v Add to dishbeard Incoming pytes I Incoming put requests I Bytes Court Court				
Incoming pytes I Incoming put requests I Incoming records I Bytes Own Court Court I	Test with demo data Info Ingest simulated data to test the configuration of your delivery stream. S Monitoring Configuration Destination error logs	Randard Amazon Kinesis Data Firehose charges apply.		
Incoming bytes Incoming put requests Incoming records I Bytes Count Count Count Count	Test with demo data wise byper simulated data to test the configuration of your datavey stream. S Honoteching Configuration Destination error logs Delivery stream metrics mole	landard Amazon Kinesis Data Finknos charges apply.		
Bytes Court Court	Y Test with demo data and the undependent of your delany stream 5. Honotaning Configuration Destination error logs Delivery stream metrics tota	Sandard Annuant Kinedis Data Freihene obergei apply		1h 3h 12h 1d 3d 1w Custom (B) C ▼ Add to dashbeard
	Y Test with demo data were available of your delivery stream 5 Honotoxing Configuration Detivation error logs Delivery stream metrics wo Incoming bytes	Iandard Annaen Kinela Bata Finhee durges apply		1h 3h 12h 1d 3d 1w Custom IB O T Add to dashbeard 1 Incoming records 1

1.8. Kinesis Firehose 設定

Services V					
vs-waf-logs-xxxx-xxxx was su	ccessfully created.				
nazon Kinesis > Delivery	streams > aws-waf-logs-xxxx-xxxx				
ws-waf-logs-x	XXX-XXXX info				Delete delivery stream
Delivery stream deta	nils				
Status		Destination	Data transformation		Creation time
		Amazon S3	Disabled		November 12, 2021, 15:58 GMT+9
Source		ARN	Dynamic partitioning		
Discost Di IT			Dirablad		
			UISBUREU		
Test with demo da Ingest desided data to ten Monitoring Configure	ta sete the configuration of your delivery stream. I ation Destination error logs	Standard Annuan Stands Data Fahren charges again	USURU		
Test with demo da Ingest simulated data to ten Monitoring Configur Delivery stream met	ta tofo the configuration of your delivery stream. I action Destination error logs rrics note	Standard Annuard David Data Fashare sharper apply.			
Test with demo da Inget smaller data to te Monttering Configur Delivery stream met	tta solo the configuration of your delivery stream : attom Destination error logs rfcs solo	Standard Ansaan Clineis Data Fanhase dergan agaiy	In	. 3h 12h 1d 3d	Tw Cuttom (E) (C (v) Add to doubloared
Test with demo da Ingent simulated der to ten Monttoring Configur Delivery stream met Incoming bytes	te inte antigonation of your delaway stream. I attem Destination error logs rics inte	Standard Ansans Clinesis Data Fanhass charges agains	unner In In	3h 12h 1d 3d Incoming record	Tw Conton (E) (C) v (Add to dashboard)
Test with demo da Ingent simulated data to ten Menitarting Configur Delivery stream met Incoming bytes Bytes	tta solo. Like soliganition of your delivery stream. 1 zation Destination error logs trices sole	Iterated Ansaec Dees Data Ferbers charges apply.	1 1 1	3h 12h 1d 3d Incoming record Cont	Tw Contom D C V Add to disableared ds I

完了

1.9. Kinesis Firehose とAWS WAF との連携設定



サービス "AWS WAF" に戻り

"Web ACLs" > "Logging"を選択

[Enable Logging]

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

aws Services V	Q Search for	services, features, blogs, docs, and more	[Option+S]	D	÷	Dies Branning M.	Global 🔻	Support
Enable logging for F	RULE_TEST							
AWS WAF will deliver logs from your w	ab ACL to your Amazon Kin	esis Data Firehose.						
	Web ACL	RULE_TEST						
	IAM role	AWSServiceRoleForWAFRegionalLogging						
		AWS WAF manages this role for you. The role grants AWS logs-*.	WAF write permissions to Kinesis	s Data Firehoses that sta	irt with th	ne name "aws-waf-		
Amazor	n Kinesis Data Firehose*	aws-waf-logs-xxxx-xxxx	~					
Redacted fields		Select a Kinesis Data Firehose that starts with the name " "aws-waf-logs-", you can create one on the Kinesis Data	aws-waf-logs-*. If you don't have Firehose console.	have a Kinesis Data Fire	hose with	h a name starting with		
Choose the data fields that you want to	hide from the logs. Learn r	nore						
Choose field to redact from logs		- Add						
Redacted Fields								
This logging configuration doesn't lis	t any fields to redact.							
* Required						Cancel Create		

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

eedback English (US) 🔻

© 2008 - 2021, Amszon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie pref

「Create」

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



Logging が、"Enabled" になっていることを確認

1.12.1 章の完了確認

aws	Senices 🔻		Q Search for services, fea	ures, blogs, docs, and more	[Option+S]		۵ ¢	Glabal	♥ Support ♥
=	Amazon S3 > csc-waftest > a	ws-waf-logs/							
	aws-waf-logs/							0	opy \$3 URI
	Control Lawrence								
	repertes								
	Objects (1)								
	Objects are the fundamental entities	stored in Amazon 53. You can use	Amazon S3 inventory 🛃 to get a list of all object	s in your bucket. For others to access yo	ur objects, you'll need to explicitly	part then permissions. Learn more [
	C Copy S3 URI	🖞 Copy URL	Download Open 🖸 Deleb	Actions V Creat	e folder 🕞 Upload				
	Q. Find objects by prefix							<u> </u>	/ 0
	Name	 Туре 	⊽ Last	nodified		Size V	Storage class		~
Feedback	English (US) 🔻					© 2008 - 2021, Amazon Web Services, Inc. or its	affiliatos. All rights reserved. Privacy Pol	icy Terms of Use	Cookie preferences

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

ave-wat-logs-occ-voor-1-2019-08-02-02-25-35-75ea204d-d381-4148-91ef-b07991454bff.gz

Septer 11
Perela • Regela •
Spenzo* 200 of Chancer Market and and and a final spent for the spend to an end of the spend to an end to an end of the spend to an end to an end of the spend to an end to an
type20.* Type
ngentati segentati Segent to gentation and setting allow and s
ngel30*
typeSQL* Type
ngellet ¹ New York was an excellence of a star back was an excel
agende 4 en en en en de la martin de la ma
hýzkla) * (100 200 moreklekal overvele klenne i formal i klenne klenne klenne klenne i klenne klenne i klenne klenne i klenne
by http:///
spekale*
Servers * Q Servers (Q Server (
Service · · · · · · · · · · · · · · · · · · ·
Sector Q and for marked large large data and mark and mar
Sector * Quest to intervice Autom page data guestions Page of the sector Autom page data guestions Page of the sector Autom page data guestions Sector * Quest to intervice Autom page data guest page data
Secure
Sector
Server () Control to con
Service 1 Q Service for any Control Q Servic
Sector 7 Q Alexa Cut Kinkson, Nature, Na
Sector C Q and the sector to be expected to expect to be expected to expect to and the sector to be expected to and the sector to and
Verified Control of the first field of the first fi
Anna S1) Concentral () Server Regn () S27(1) (S0() C0()
A manufactory of a strategy of
22/
22/ Ø com Columnia Inspecting III Objects III Inspecting IIII (IIIII) The construction of the column behaviored Biology Biology and Line IIIII (IIIIIIIII) Inspecting IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
Add Image: The provides Objects (1) Statement (1) Constraints (1) Statement (1) <
Objects Properties Objects (2) (Conceptor by the concept of the concept of the conceptor data, performed on the conceptor
Objects (3) The most field with the start (3 to use an indexed 3 to leaver (2 to up to list), to obtain to user your days, put final to solidly per time services (second 2) ① ① opposition (2 to up to list) ① been (2 to up to list) ① dependent (second 2) ① ① opposition (2 to up to list) ① been (2 to up to list) ① dependent (second 2) ① dependent (second 2) ② ① opposition (2 to up to list) ① been (2 to up to list) ① dependent (second 2) ① dependent (second 2)
Objects (1) Charge (1) Congress to the charge of the congress of the congres of the congress of the congress of the congres of
Objects (3)
Objects (3) @ dot cost of location of location of locations (2) locat
Objects (1) Construction (1) Construction (1) Construction (1) Construction (1) Construction (1) Construction (1) Construction (1) Construction (1) Construction (1) Construction (1) Construction (1) Construction (1) Construction (1) Construction (1) Construction (1) Construction (1) Construction (1)
Security Constraints of the second se
Object set for example and an example and an example and and a set of a se
Ø Ø (ary \$1) (0) Ø (ary \$10) B baselood Opto D Actions ▼ Oreter hilder E topland Q. Tradingten try prefe
Q. The default by prefix (1)
Q, that digites by serific
□ nærre ▲ Type ♥ Last medified ♥ Size ♥ Storage dass
A 265-062 (2023) 12:0159 (05-02-02-05-16-0535/02-0070-4666-8486-766455(10001.02) 42 44
D memory management of the second

August 2, 2019, 11:26:38 B/TC+09:000

ar

540.0 8 Standard

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

aws Services -	Resource Gr	oups 🗸 🛠			Global → Support →
lentity and Access lanagement (IAM)	Create	e policy Policy actions 👻			
AWS Account (358486443100)	Filter p	oolicies v Q Search			Showing 569 re
Dashboard					
Groups		Policy name 👻	Туре	Used as	Description
Users	0,	AdministratorAccess	Job function	Permissions policy (1)	Provides full access to AWS services and resources.
Roles	0.	 AlexaForBusinessDeviceSetup 	AWS managed	None	Provide device setup access to AlexaForBusiness services
Policies	0.	AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness resources and access to
dentity providers	0.	AlexaForBusinessGatewayE	AWS managed	None	Provide gateway execution access to AlexaForBusiness service
Account settings	0.	AlexaForBusinessNetworkPr	AWS managed	None	This policy enables Alexa for Business to perform automated ta
Credential report	0,	AlexaForBusinessReadOnly	AWS managed	None	Provide read only access to AlexaForBusiness services
Encryption keys	0.	AmazonAPIGatewayAdminis	AWS managed	Permissions policy (1)	Provides full access to create/edit/delete APIs in Amazon API 0
Q Search IAM	0,	AmazonAPIGatewayInvokeF	AWS managed	Permissions policy (1)	Provides full access to invoke APIs in Amazon API Gateway.
AWS Organizations	0.	AmazonAPIGatewayPushTo	AWS managed	Permissions policy (2)	Allows API Gateway to push logs to user's account.
Organization activity	0.	AmazonAppStreamFullAccess	AWS managed	None	Provides full access to Amazon AppStream via the AWS Mana
Service control policies (SCPs)	0.	MazonAppStreamReadOnl	AWS managed	None	Provides read only access to Amazon AppStream via the AWS
	0,	AmazonAppStreamServiceA	AWS managed	None	Default policy for Amazon AppStream service role.
	0,	AmazonAthenaFullAccess	AWS managed	None	Provide full access to Amazon Athena and scoped access to the
	0,	AmazonChimeFullAccess	AWS managed	None	Provides full access to Amazon Chime Admin Console via the
	0,	AmazonChimeReadOnly	AWS managed	None	Provides read only access to Amazon Chime Admin Console vi
	0,	AmazonChimeUserManage	AWS managed	None	Provides user management access to Amazon Chime Admin C

サービス "IAM" より

"Policy" > "Create policy"を選択

🗨 Feedback 🛛 😵 English (US)

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

2.2. WAFLog 出力先 read 権限 policy 作成

With Services ~ Resource Groups ~ * Create policy	² Service : S3	
A poley driftes the XMD permissions that you can assign to a user, group, or role. You can ceste and edit a poley in the visual editor and using JSON. Learn more Expand all Colleges all	Action : GetObject Resources : arn:aws:s3:::csc-waftest/waflog/* ※ 1.4 で設定した内容	ARN の追加 × Arnazon リソースネーム (ARN) は、AVIS リソースを一意に講顾します。リソースは各 ワービスに回有です。詳細はとちら ♂ メントレスを一意に講顾します。リソースは各 マービスに回有です。詳細はとちら ♂ S3_object Ø ARN Ø唐芝 arnzwesiGitocie-walhest/walfog* ARN を手動でリスト arnzwesiGitocie-walhest/walfog* Bucket name* csc-walhest/walfog Object name* マ すべて
Request conditions (spicoral) Add additional permission Cano Revelator English (US) C 2001 - 2013, Ansaon Web, Services, etc. or its utilitates. All rights memory. Prevelator Prevelator Prevelator C 2001 - 2013, Ansaon Web, Services, etc. or its utilitates. All rights memory. Prevelator Pr	。 ? ? [*] ***** ※ Resources に指定するパスには	**>** =================================

[Review policy]

2.3. WAFLog 出力先 read 権限 policy 作成

aws	Services - Reso	urce Groups 👻 🛠		4		Global 👻	Support +
	Create policy					1 2)
	Review policy						
	Name*	wafcharm-waflog-s3-read					
		Use alphanumeric and '+=,.@+_' chars	cters. Maximum 128 characters.				
	Description	WafCharm					
	Summan	Maximum 1000 characters. Use alphe	numeric and '+=,, &' characters.				1
	Summary	Q, Filter					
		Service 👻	Access level	Resource	Request condition		
		Allow (1 of 187 services) Sho	w remaining 186				
		83	Limited: Read	BucketName string like csc-waftest, ObjectPath string like aws-waf- logs/"	None		
	Nequirou			Cano	ei Previous	ave changes	
	* Required			Cano	el Previous S	ave changes	

edback 🚱 English (US)

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

Create policy 2 2	Service : S3	
Valual editor VSON Import managed policy Espand all Colargee all S3 (2 actions) Clone Remove S savide S3 Savide S3	Action : PutObject, PutObjectACL	
Actions Write PuDQyet: PuDQyet: Pormissions management PuDQyet/dcl PodSystMcl Socific	ARN © 2501 Resources : arn:aws:s3:::wafcharm.com/*	× 食に識別します。リソースは各 ARN を手動でリスト
	※ CSC 側の S3 に対する権限	ा रूर रूर ⊽र्र 🥑
Add additional permissions Cancel Review policy		キャンセル 追加

ж

2.5. WafCharm 連携用 put 権限 policy 作成

Services - Reso Create policy	urce Groups 👻 🕈		Δ.		Global +
Review policy					
Name*	wafcharm-waflog-s3-put Use alphanumeric and '+=,,@'	characters. Maximum 128 characters.			
Description	WafCharm				
	Maximum 1000 characters. Use	alphanumeric and '+=, \mathfrak{D}_{-} ' characters.			8
Summary	Q, Filter	Access level	Resource	Request condition	
	Allow (1 of 187 services)	Show remaining 186			
	83	Limited: Write, Permissions management	BucketName string like wafcharm.com, ObjectPath string like All	None	
* Required			Can	cel 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

aws Services - Reso	urce Groups 👻	*			Δ	- Global - Su	ippor
Creat	te role				1 2 3 4		
Select	type of truste	ed entity					
Û.	AWS service EC2, Lambda and other	Another AW Belonging to y	VS account ou or 3rd party Well Cog prov	b identity nito or any OpenID ider	SAML 2.0 federation Your corporate directory		
Allows AW Choos EC2	'S services to perfor	that will use this ro	n more le				
Lambda Allows La	umbda functions to c	all AWS services on your behail.	ut.				
API Gatev	way	Comprehend	ElastiCache	Lex	SMS	•	
AWS Bac	kup	Config	Elastic Beanstalk	License Manager	SNS		
AWS Sup	port	Connect	Elastic Container Service	Machine Learning	SWF		
Amplify		DMS	Elastic Transcoder	Macie	SageMaker		
AppSync		Data Lifecycle Manager	ElasticLoadBalancing	MediaConvert	Security Hub		
Applicatio	on Auto Scaling	Data Pipeline	Forecast	Migration Hub	Service Catalog		
Applicatio Service	on Discovery	DataSync	Glue	OpsWorks	Step Functions		
Batch		DeepLens	Greengrass	Personanze	Storage GateWay	1	
* Required	d	Directory Service	GuardDuty	C	ancel Next: Permissions		
edback 🚱 English (US)			(2008 - 2019, Amazon Web Serv	ices. Inc. or its annales, wi nams reserved	Privacy Policy	Term

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

upport -

Terms of Use

aws Services - Re	esource Groups 👻 🕏		🗘 - Global - S
Cre	eate role		1 2 3 4
- Att	ttach permissions policies		
Choose	e one or more policies to attach to your new role.		
Crea	ate policy		8
Filter	r policies 🐱 🔍 Q, lambda		Showing 20 results
	Policy name 💌	Used as	Description
	AWSLambdaBasicExecutionRole-96f82314-e	None	
	AWSLambdaBasicExecutionRole-bf9331ef-78	Permissions policy (1)	
	 AWSLambdaDynamoDBExecutionRole 	None	Provides list and read access to Dynamo
		None	Provides minimum permissions for a La
	 AWSLambdaExecute 	Permissions policy (6)	Provides Put, Get access to S3 and full a
	AWSLambdaFullAccess	Permissions policy (4)	Provides full access to Lambda, S3, Dyn
	 AWSLambdalnvocation-DynamoDB 	None	Provides read access to DynamoDB Stre
	 AWSLambdaKinesisExecutionRole 	None	Provides list and read access to Kinesis
› Se	et permissions boundary		
* Requ	uired		Cancel Previous Next: Tags
🗨 Feedback 🛛 🚱 English (US)		© 2008 - 2019, Ama	zon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy

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

WS Services	- Resource Groups 👻 🕏	Ciobal -
	Create role	1 2 3 4
	 Attach permissions policies 	
	Choose one or more policies to attach to your new role.	
	Create policy	0
	Filter policies ~ Q wafcharm	Showing 5 results
	Policy name * Used as Descrip	ation
	✓ ▶ wafcharm-waflog-s3-put	
	✓ → wafcharm-waflog-s3-read	

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

 Set permissions boundary 	
* Required	Cancel Previous Noxt: Tags
🗨 Feedback 🛛 🚱 English (US)	© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

※ 2.3, 2.5で作成した policy

「Next: Tags」

2.9. WafCharm 連携 Lambda 用 role 作成

ws	Services	- Resource Groups - 🔸		A	100	-	Global +	Support
		Create role		(1)	2	3 4		
		Add tags (optional)						
		IAM tags are key-value pairs you can title. You can use the tags to organize	add to your role. Tags can include user information, such as an email address, or track, or control access for this role. Learn more	can be des	criptive,	such as a job		
		Key	Value (optional)			Remove		
		Add new key						
		You can add 50 more tags.						

タグの追加は任意

「Next: Review」



2.10. WafCharm 連携 Lambda 用 role 作成

AWS Services - Resource Groups - +	↓ Global × Support ×	
Create role		Role name:
Review		
Provide the required information below and review	this role before you create it.	wafcharm-wa
Role name*	wafcharm-waflog	
	Use alphanumeric and '++,.@+_' characters. Maximum 64 characters.	
Role description	WafCharm	Dele descripti
		Role descripti
	Maximum 1000 characters. Use alphanumeric and '+=,, Φ_{-1}^{-} characters.	WofCharm (4
Trusted entities	AWS service: lambda.amazonaws.com	
Policies	AWSLambdeExecute C	
	wafcharm-waflog-s3-read 17	
	wafcharm-waflog-s3-put [2]	
Permissions boundary	Permissions boundary is not set	
No tags were added.		
		Create rale (
* Required	Cancel Previous Create role	r Create role
Feedback (English (US)	© 2008 - 2019, Amazon Web Services, Inc. or Its Withtee All violete researced Privacy Policy Terms of Use	

name: narm-waflog (任意)

description : harm (任意)

2.11. Lambda 構築

Services 🔻	Q Search for services, features, blogs, docs, and more	[Option+S]	🕲 🚓 🛛 Takya 🔻 Support 🔻
Lambda > Functions > Create function			٥
County formation			
Create function into			
Choose one of the following options to create your function.			
Author from scratch O Start with a simple Helio World example.	Use a blueprint OBUID a Lambda application from sample code and configuration presets for common use cases.	Container image Select a container image to deploy for your function.	Browse serverless app repository Deploy a sample Lambda application from the AWS Serverless Application Repository.
Basic information			
Function name Enter a name that describes the purpose of your function.			
wafcharm-waflog			
Use only letters, numbers, hyphens, or underscores with no spaces.			
Ruttime infe Choose the languages to use to write your function. Note that the convolution	de editor supports only Node Jr. Python, and Puby.		
Node,is 14.x			•
Coose the instruction set architecture you want for your function code.	lage te Amazon Claudhistels Lage You can existenize this default raie later when a	däng triggers.	
Change default execution role Execution role Cores and role the default execution of user function	ere mile, en ta the IAM operatio		
 Create a new role with basic Lambda permissions 			
 Use an existing role 			
 Create a new role from AWS policy templates 			
Existing role Choose an existing role that you've created to be used with this Lambda fun	tion. The role must have permission to upload logs to Amazon CloudWatch Logs.		
wafcharm-waflog			• C
View the wafeharm-waffing role on the IAM console.			
► Advanced settings			
			Cancel Create function
English (US) 🔻		ID 2008 - 2021, Amazon Web Servi	cos, Inc. or Its athlistes. All rights reserved. Privacy Policy Terms of Use Cashie preferences

名前:wafcharm-waflog (任意)

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

Execution Role : Use an existing role

既存のロール: wafcharm-waflog ※ 2.10 で作成したもの

※ 1.4 で指定した S3 のバケットと同じリージョンで作 成してください

「Create function」

2.12. Lambda 構築 (関数コード)

	Q. Search for services, features, blogs, docs, and more [Option+5]	E ↓ Takya ▼ Takya ▼
	0 ^m	
Code Test Monitor	Configuration Allases Versions	
Code source Info		Upload from v
	Tools Window Test Test Deploy Charges not displayed	8.0
() VINC2 () VINC2	<pre>Weight</pre>	

Code source: 以下のソースを貼り付け <u>http://docs.wafcharm.com/manual/classic_aws_w</u> <u>af/index.js</u>

※ ソースは AWS WAF のバージョンで異なりますのでご注意ください

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

[Deploy]

2.13. Lambda 構築 (トリガー)

	Q Search for Services, reactires, blogs, b	ca, una more copuon	<u>ग</u>	A
Lambda > Add trigger				
Add trigger				
Trigger configurat	ion			
S3 aws storage		•		
Bucket Please select the S3 bucket t	hat serves as the event source. The bucket must be in the same r	egion as the function.		
csc-waftest		▼ C		
Event type Select the events that you w each bucket, individual even key.	ant to have trigger the Lambda function. You can optionally set u ts cannot have multiple configurations with overlapping prefixes	up a prefix or suffix for an event. However, for or suffixes that could match the same object		
All object create event	s	•		
Prefix - optional Enter a single optional prefit	to limit the notifications to objects with keys that start with ma	tching characters.		
aws-waf-logs/				
Suffix - optional Enter a single optional suffic	to limit the notifications to objects with keys that end with mate	hing characters.		
		and characters		
e.gjpg				
e.gjpg				
e.gjpg Lambda will add the neo more about the Lambda	essary permissions for Amazon S3 to invoke your Lamb permissions model.	da function from this trigger. Learn		
e.gjpg Lambda will add the nec more about the Lambda	essary permissions for Amazon S3 to invoke your Lamb permissions model.	da function from this trigger. Learn		
C.g., Jpg Lambda will add the nec more about the Lambda for the Lambda for function w output. Writing te increased Lambda I acknowledge I acknowledge	essary permissions for Amazon S3 to invoke your Lamb permissions model.	da function from this trigger. Learn different 53 buckets for input and ve invocation, which can result in uut is not recommended and that this		
C.g. Jpg Lambda will add the nec more about the Lambda for the Lambda for function w output. Writing te increased Lambda I acknowledge configuration	essary permissions for Amazon S3 to invoke your Lamb permissions model. ion rifes objects to an S3 bucket, ensure that you are using a bucket increases the risk of creating a recursi usage and increased costs. Learn more that using the same S3 bucket for both input and outp can cause recursive invocations, increased Lambda usag	da function from this trigger. Learn different 53 buckets for input and ve invocation, which can result in ut is not recommended and that this re, and increased costs.		
Co. Jpp Lambda will add the nec more about the Lambda figure function w output. Writing to increased Lambda Z Lacknowledge configuration	essary permissions for Amazon S3 to invoke your Lamb permissions model.	da function from this trigger. Learn different 53 buckets for input and ve invocation, which can result in e, and increased costs.		

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]

Cookie preference



aws	Services 🔻	Q Search for services, features, blogs, docs, and	more [Option+S]	D	A landar sector and a sector	Tokyo 🔻	Support 🔻
=	Code Test Monito	or Configuration Aliases Versions					٩
	General configuration	General configuration Info				Edit]
	Triggers	Description	Mamaaa	Toront	-		
	Permissions	WafCharm連携用	128 MB	1 min 0 s	20		
	Destinations						_
	Environment variables						
	Tags						
	VPC						
	Monitoring and operations tools						
	Concurrency						
	Asynchronous invocation						
	Code signing						
	Database proxies						
	File systems						
	State machines						
Feedback	English (US) 🔻				d. Privacy Policy Terr	ns of Use Cor	kie preferences

General configuration:

Timeout:1分

Description : WafCharm 連携用 (任意)



aw	S Services 🔻	Q Search for services, features, blogs, docs, and more	[Option+S]	∑	•
=	Lambda > Functions > wafcharm-	waflog			٩
	wafcharm-waflog			Throttle Copy ARN Actions V	
	▼ Function overview Info				
	S3 + Add trigger	Configuration Allases Versions	+ Add destination	Description - Last modified 6 minutes ago Function ARN	
	Code source Info			Upload from 🔻	
	Go to Anything (# P)	indow Test Changes not	deployed	22.42	
	v wafcharm-waflog & v	<pre>1 'use strict'; 2 const toBucket = process.env.WAFCHARM_BUCKET ' 4 const toPath = process.env.WAFCHARM_BUCKET 'mafl</pre>	'wafcharm.com'; log/acceptance/v1';		
Feedba	sk English (US) ▼	0	2008 - 2021, Amazon Web Services, Inc. o	r its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie prefere	ences

完了

2.16. CloudWatch

Lambda 関数実行後でないと作成されません

AWS コンソール > CloudWatch > ロググループを選択

"次の期間経過後にイベントを失効 "カラムの値が

デフォルト値: "失効しない"

となっているため

必要に応じてログの保存期間を変更してください

3. レポート機能をご利用される場合

レポート機能をご利用頂くには、以下の条件が満たされる必要があります

1. 1~2章までの設定が完了している

2. 前月に検知があった

※前月に検知がなかった方 -> 月次レポートが作成されません

3.1. WafCharm 管理画面にて月次レポートの閲覧



WafCharm 管理画面

※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

Waf Charn Web ACL Config Veb Site Config Managed Rules

Sample 🗸

WafCharmへようこそ

下記リンク先を参考に設定を行ってください。

https://www.wafcharm.com/blog/check-wafcharm-setting-jp/

さらに、メール通知機能と月次レポート機能をご利用されたいお客様はHelpページの 「レポート機能/通知機能を利用する」をご参照の上、必要なセッティングを実施して ください。

Helpページ

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 Co	onfig					
Web ACL ID				Web ACL Name		
xxxxxxxxxxxxxxxxxxxxxx	0<->000<->00000000000000000000000000000	DX		Sample_Web_ACL	6 🕈	

対象の「Web ACL Name」を選択

4.3.メール通知先の設定

Waf Charm Web ACL Config Web Site Config Managed Rules Web ACL Config : Detail K Back | O Edit A Notification 💼 Delete Web ACL ID Web ACL Name Sample Web ACL XXXXXX Access key Secret key XXXXXX******XXXXXX 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/xxxxxxx/elasticloadbalancing/ap-northeast-1/

「Notification」を選択

4.4.メール通知先の設定

レポート機能/通知機能を利用する

Notification : Detail		
< Web ACL Config 🖻 Edit		
Web ACL ID	XXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXXXX	
Web ACL Name	Sample_Web_ACL	
WafCharm Email Notificatoin	OFF	
Managed Rule Email Notificatoin	OFF	
Notification email		
Votification email		
🕼 Edit		
Email	Set date	
sample@example.com	2020-03-10 11:19:06 +0900	

「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。

notification@exapmle.com	8
alert@sample.com	0
example@cscloud.co.jp	

「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 V	Veb Site Config	Managed Rules	Sample 🗸
Notification : Detail			
< Web ACL Config Z Edit			
Web ACL ID		X0000000-X000-X000-X000-X0000-X0000-X000000	
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

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

「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

Waf Charm Web ACL Config Web Site	Config Managed Rules	Sample +	■ 「Edit」を選択
Web ACL ID Web ACL Name WafCharm Email Notificatoin Managed Rule Email Notificatoin	20000000 - 20000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000 - 2000		
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			

4.8.メール通知の設定

Waf Charm Web ACL Config Web Site C	onfig Managed Rules	Sample +
Notification : Edit		
Web ACL ID Web ACL Name	xxxxxxxxx-xxxx-xxxx-xxxxxxxxxxxxxxxxxx	
Email Address WafCharm Email Notificatoin Managed Rule Email Notificatoin	Sample@example.com	
	O Save	

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

4.9.メール通知の設定

Wat Charm Web ACL Config	Web Site Config Managed Rules	Sample 👻
Notification : Detail		
< Web ACL Config 🕑 Edit		
Web ACL ID	X0000000X-X000X-X000X-X0000000000000	
Web ACL Name	Sample_Web_ACL	
WafCharm Email Notificatoin	ON	
Managed Rule Email Notificatoin		
Notification email		
Le Foit		
Email	Set date	
Email notification@example.com	Set date	
Email notification@example.com	Set date	
LS EQIT Email notification@example.com alert@aample.com 適知を有効にするためには設定が必要で	Set date	

「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: 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
 - <u>AWS WAF Managed Rules ルールグループの例外機能マニュアル (p4)</u>
- 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

Waf Charn Web ACL Config / eb Site Config Managed Rules

Sample 🗸

WafCharmへようこそ

下記リンク先を参考に設定を行ってください。

https://www.wafcharm.com/blog/check-wafcharm-setting-jp/

さらに、メール通知機能と月次レポート機能をご利用されたいお客様はHelpページの 「レポート機能/通知機能を利用する」をご参照の上、必要なセッティングを実施して ください。

Helpページ

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

Sample 🗸

Waf Charm Web ACL Config Web Site Config Managed Rules Web ACL Config < Back | O Add ACL Web ACL ID Web ACL Name 6 5 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

Waf Charm Web ACL Config Web Site Config Managed Rules Sample 🗸 Web ACL Config : Detail 「Edit」を選択 O Edit < Back Notification 📔 🍵 Delete Web ACL ID ******* Web ACL Name Sample Web ACL XXXXXX Access key Secret key XXXXXX******XXXXXX Bule 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 Z sample.com S3://s3/SampleBucket/AWSLogs/xxxxxxx/elasticloadbalancing/ap-northeast-1/

5.4. CSC マネージドルールの利用設定

Web ACL ID •	
Web ACL Name *	
Sample_Web_ACL	
Web ACL Access Key *	
200000(*************00000)	
Web ACL Secret Key	
XXXXXX.*******************************	
edit access key and secret key?	
Bule limit	
10 \$	
Change AMQ service ture *	
ALB or API Gateway \$	
Choose your AWS region *	
ap-normeast-1	
Blacklist	
203.0.113.0, 203.0.113.1, 203.0.113.2	
Whitelist	
198.51.100.0, 198.51.100.1	
Default AWS WAF Action	
BLOCK \$	
Use Managed Rule	

「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

Back OF Edit	Notification E Managed Rules C Delete	
Web ACL ID	X0000000x-X00X-X000x-X0000000000X	
Web ACL Name	Sample_Web_ACL	
Access key	X0000X*******X0000X	
Secret key	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	
Rule limit	10	
Service type	ALB or API Gateway	
AWS region	ap-northeast-1	
Blacklist		
Whitelist:		
Default Action	BLOCK	
Use Managed Rule	used	
ooo managoa maa		
FQDN S3 I	ath	
sample.com \$3:/	3/SampleBucket/AWSLogs/xxxxxxxxx/elasticloadbalancing/ap-northeast-1/	C

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

「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

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

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

Waf Charm Web ACL Config Web Si	te Config Managed Rules	Sample 🕶
Notification : Detail		
Notification . Detail		
K Web ACL Config 😰 Edit		
Web ACL ID	100000001-10001-10001-10001-000010000000	
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

Waf	Charm	Web ACL Config	Web Site Config	Managed Rules	Sample 🗸
Noti < No	ficatior tification	n : Edit			
w	leb ACL ID leb ACL Nar	ne		xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	
M	fafCharm Er lanaged Rul	nail Notificatoin e Email Notificatoir		O ON OFF	

「Managed Rule Email Notification」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 V	Web Site Config Managed Rules	Sample 🗸
Notification : Detail		
Web ACL ID Web ACL Name	xaacaaaax-xaax-xaax-xaax-xaaaaaaaaaaaaa	
WafCharm Email Notificatoin Managed Rule Email Notificatoin	ON ON	
Notification email		
Email	Set date	
notification@example.com	2020-03-11 16:46:09 +0900	

レポート機能/通知機能を利用する

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

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

5.9.メール通知内容

検知 (BLOCK/COUNT) された場合、下記のメールが送信されます

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

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、<u>1.5 Kinesis Firehose 設定</u>の Buffer intervals、Buffer size で設定した値に応じて変化しま
- 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、<u>1.2</u> 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