AWS Black Belt Online Seminar

# AWS SAW

## セルフサービスなトラブルシューティング
## Amazon Simple Storage Service (Amazon S3) + AWS Lambda 編

石川 直哉 / 藤原 弘樹

Cloud Support Engineer
2024/03

# AWS Black Belt Online Seminar とは

- 「サービス別」「ソリューション別」「業種別」などのテーマに分け、アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- AWS の技術担当者が、 AWS の各サービスやソリューションについてテーマごとに動画を公開します
- 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます
  - https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/
  - https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY

ご感想は X (Twitter) へ！ハッシュタグは以下をご利用ください
#awsblackbelt

# 内容についての注意点

- 本資料では 2024 年 2 月時点のサービス内容および価格についてご説明しています。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (https://aws.amazon.com/) にてご確認ください
- 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます
- 技術的な内容に関しましては、有料の AWS サポート窓口へお問い合わせください
- 料金面でのお問い合わせに関しましては、カスタマーサポート窓口へお問い合わせください (マネジメントコンソールへのログインが必要です)

# 本セミナーの概要

- 本セミナーの対象者
  - Amazon S3 や AWS Lambda を利用した運用を実施されている方
  - Amazon S3 や AWS Lambda、Amazon S3 と AWS Lambda を組み合わせて使用する際のトラブルシューティングの効率化に興味のある方
- 本セミナーの Goal
  - Amazon S3、AWS Lambda 向けに利用可能な4つの AWS Support Automation Workflows(SAW) について利用ユースケース及び概要を理解する
- 本セミナーの前提知識
  - AWS Black Belt Online Seminar (Amazon S3) 入門編 (PDF/YouTube)
  - AWS Black Belt Online Seminar (AWS Lambda) (PDF/YouTube)
  - AWS Black Belt Online Seminar AWS SAW - セルフサービスなトラブルシューティングと運用の自動化 入門編 (PDF/YouTube)

# 自己紹介

名前：石川 直哉 (Naoya Ishikawa)

所属：アマゾン ウェブ サービス ジャパン合同会社

技術支援本部 クラウドサポートエンジニア

好きな AWS サービス：

Amazon
CloudFront

# 自己紹介

名前：藤原 弘樹 (Hiroki Fujiwara)

所属：アマゾン ウェブ サービス ジャパン合同会社

技術支援本部 クラウドサポートエンジニア

好きな AWS サービス：

AWS Lambda

AWS IoT Core

# アジェンダ

- Amazon S3 のよくあるお問い合わせと SAW の紹介
  - S3 バケットへのパブリックアクセスが許可されているかを判定する
    - AWSSupport-TroubleshootS3PublicRead
  - S3 バケットに対して、同一アカウントの IAM ユーザー/ロールがアクセスを行うことができるかを判定する
    - AWSSupport-TroubleshootS3AccessSameAccount
  - S3 イベントに指定した AWS Lambda 関数がトリガーされない原因を特定・修正する
    - AWSSupport-RemediateLambdaS3Event
  - VPC に接続した Lambda 関数からインターネットアクセスができない原因を特定する
    - AWSSupport-TroubleshootLambdaInternetAccess
- まとめ

# Amazon S3 と AWS Lambda の よくあるお問い合わせと SAW の紹介

# Amazon S3 と AWS Lambda でよくあるお問い合わせ

- 機能について
  - Amazon S3 の各種機能、ストレージクラス、ライフサイクルルール、レプリケーション、オブジェクトロック、S3イベントなどについてのお問い合わせ
- トラブルシューティング
  - Amazon S3 へのリクエスト 403 (AccessDenied) が発生する
  - S3 イベントに指定した AWS Lambda 関数がトリガーされない
  - VPC 接続した Lambda 関数からインターネット経由のアクセスができない

# Amazon S3 と AWS Lambda でよくあるお問い合わせ

- 機能について
  - Amazon S3 の各種機能、ストレージクラス、ライフサイク
    ション、オブジェクトロック、S3イベントなどについての
- トラブルシューティング
  - Amazon S3 へのリクエスト 403 (AccessDenied) が発生する
  - S3 イベントに指定した AWS Lambda 関数がトリガーされない
  - VPC 接続した Lambda 関数からインターネット経由のアクセスができない

SAW によって解析や関連情報収集ができる範囲

# Amazon S3 と AWS Lambdaで利用可能な SAW(ランブック)

| 名称 | 概要 |
| --- | --- |
| AWSSupport-TroubleshootS3PublicRead | S3 バケットへのパブリックアクセスが許可されているかを判定する |
| AWSSupport-TroubleshootS3AccessSameAccount | S3 バケットに対して、同一アカウントの IAM ユーザー/ロールがアクセスを行うことができるかを判定する |
| AWSSupport-RemediateLambdaS3Event | S3 イベントに指定した AWS Lambda 関数がトリガーされない原因を特定・修正 |
| AWSSupport-TroubleshootLambdaInternetAccess | VPC に接続した Lambda 関数からインターネットアクセスができない原因を特定する |

*パブリック：アクセス許可の対象を IAM ユーザー/ロールや AWS プリンシパル、
特定の IP アドレス等に限定していない状態。

# AWSSupport-TroubleshootS3PublicRead

# AWSSupport-TroubleshootS3PublicRead

- 利用ユースケース
  - S3 バケットに対するパブリックアクセスが可能かを確認したいとき
    - 具体例
      - S3 バケット内のオブジェクトを公開したい
      - オブジェクト URL を使用した S3 バケット内のオブジェクトへのアクセスに失敗する
        - 403 エラー (Access Denied) が発生

# AWSSupport-TroubleshootS3PublicRead

- SAW(ランブック)が確認するポイント
  - バケットポリシーが設定されているか
  - バケットポリシーでパブリックアクセスが許可されているか
  - ACL でパブリックアクセスが許可されているか
  - バケットレベルのブロックパブリックアクセス設定
  - アカウントレベルのブロックパブリックアクセス設定

# SAW(ランブック)入力パラメーター (1/3)

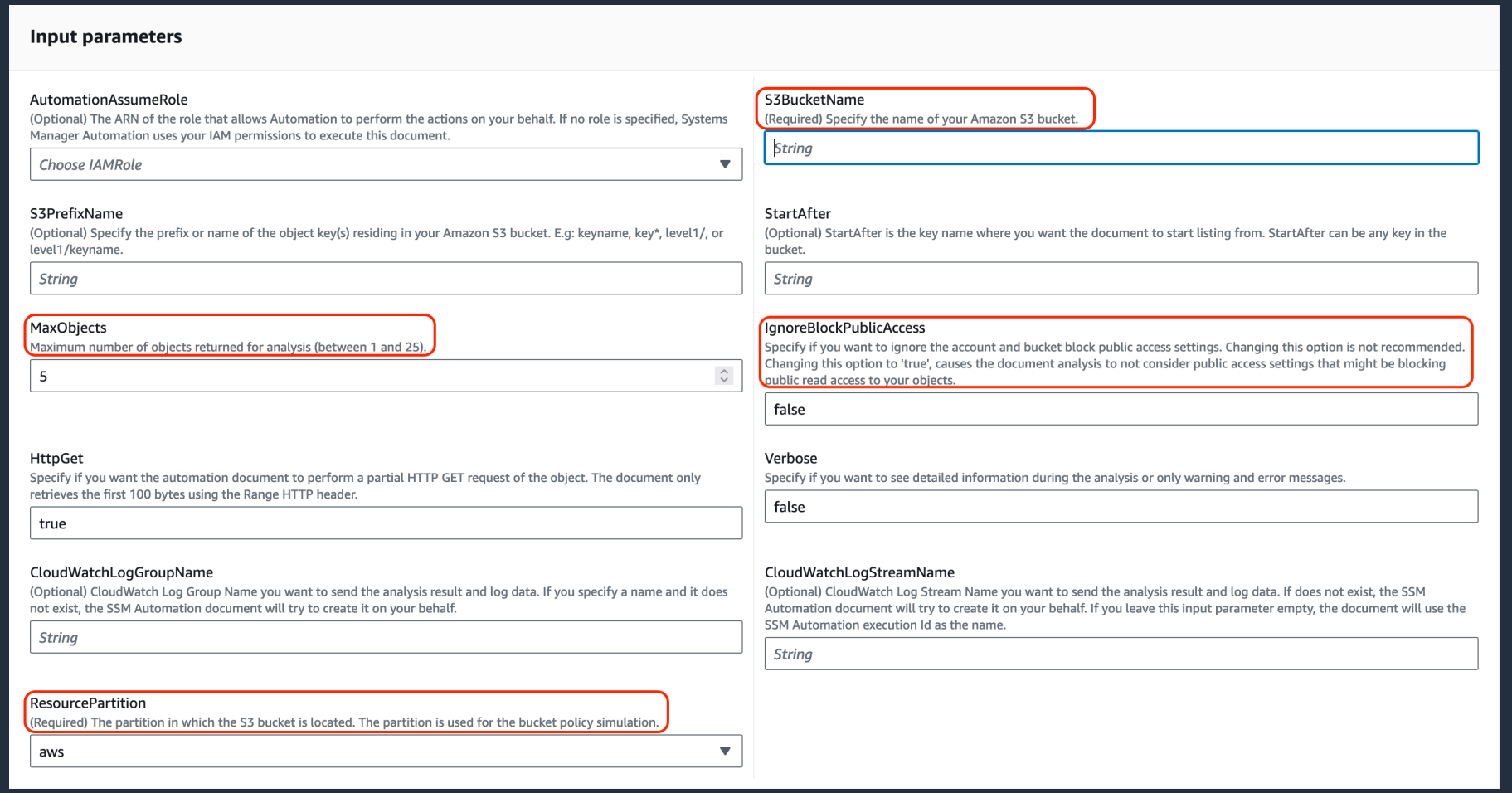
- AutomationAssumeRole : 操作しているユーザとは別にランブックのアクションを実行する IAM ロールを指定したい場合に使用
- S3BucketName(必須) : S3 バケット名
- S3PrefixName : プレフィックス
- StartAfter : オブジェクトの分析を開始するオブジェクトキー名
- MaxObjects(必須) : 分析対象とするオブジェクトの数 (デフォルト 5 個で 1 - 25 個を指定可能)
- IgnoreBlockPublicAccess(必須) : 対象 S3 バケットのパブリックアクセスブロック設定を無視するかどうか

# SAW(ランブック)入力パラメーター (2/3)

- HttpGet(必須) : Range リクエストを行なって最初のバイトのみを返すかどうか
- Verbose (必須) : Warning や Error メッセージ以外の詳細な情報を返すかどうか
- CloudWatchLogGroupName : 出力を送信するロググループ
- CloudWatchLogStreamName : 出力を送信するログストリーム
- ResourcePartition (必須) : S3 バケットのあるパーティション
  aws/aws-us-gov/aws-cn

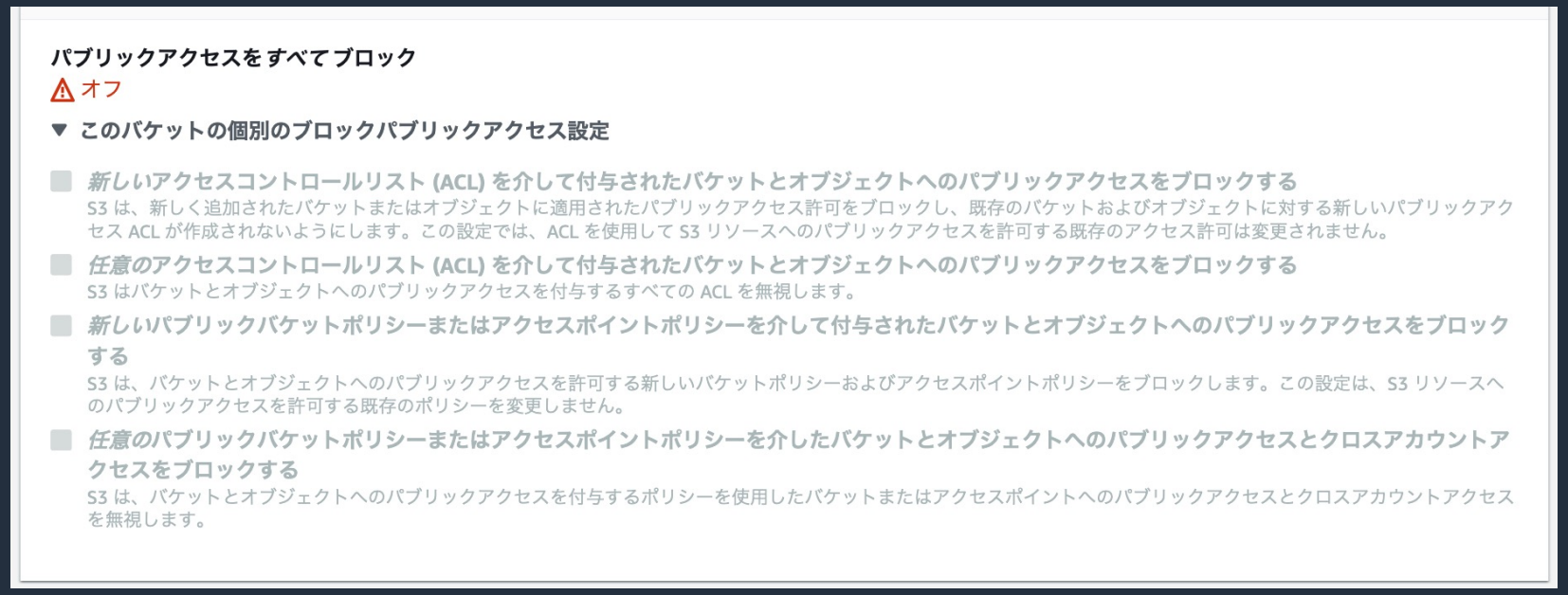
# SAW(ランブック)入力パラメーター (3/3)

- 赤枠の項目が必須パラメーター



# SAW(ランブック)実行例1

- 状況
  - バケットポリシー/ACL : パブリックアクセスを許可
  - バケット・アカウントレベルのブロックパブリックアクセス設定 : オフ



# SAW(ランブック)実行例1

▼ 出力

AnalyzeObjects.bucket

AnalyzeObjects.objects

```
[info ] [I09] HTTP GET request status:206, reason:Partial Content.
[info ] [I09] HTTP GET request status:206, reason:Partial Content.
[info ] [I09] HTTP GET request status:206, reason:Partial Content.
[info ] [I09] HTTP GET request status:206, reason:Partial Content.
[info ] [I09] HTTP GET request status:206, reason:Partial Content.
```

実行されたステップ (11)

Find Steps

1 2

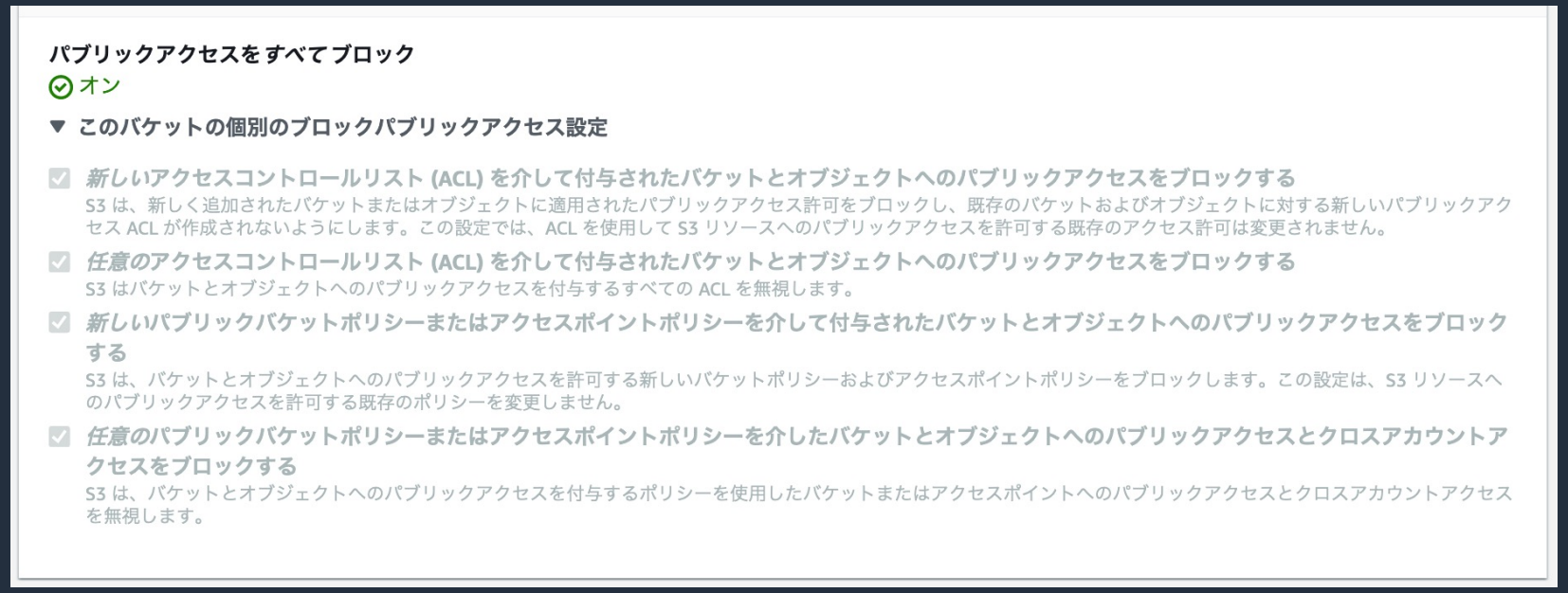
| ステップ ID | ステップ番号 | ステップ名 | アクション | ステータス |
|---|---|---|---|---|
| | 1 | TestBucketAccess | aws:assertAwsResourceProperty | 成功 |
| | 2 | GetBucketInformation | aws:executeScript | 成功 |
| | 3 | GetBlockPublicAccess | aws:executeScript | 成功 |
| | 4 | CheckBucketPayer | aws:assertAwsResourceProperty | 成功 |
| | 5 | GetBucketPolicyStatus | aws:executeScript | 成功 |
| | 6 | GetBucketPolicy | aws:executeAwsApi | 成功 |
| | 7 | GetContextKeys | aws:executeAwsApi | 成功 |
| | 8 | SimulateBucketPolicy | aws:assertAwsResourceProperty | 成功 |
| | 9 | GetBucketAcl | aws:executeAwsApi | 成功 |
| | 10 | CreateLogandStream | aws:executeScript | 成功 |

実行ステータス

| 全体的なステータス | 実行されたすべてのステップ | # 成功 |
|---|---|---|
| 成功 | 11 | 11 |
| **# 失敗** | **# キャンセル済み** | **# TimedOut** |
| 0 | 0 | 0 |

# SAW(ランブック)実行例2

- 状況
  - バケットポリシー/ACL：パブリックアクセスを許可
  - バケット・アカウントレベルのブロックパブリックアクセス設定：オン



# SAW(ランブック)実行例2

(参考訳) S3 バケットまたはアカウントブロックのパブリックアクセス設定は、パブリック ACL とパブリックバケットポリシーを無視するように設定されています。

▼ 出力

AnalyzeObjects.objects

-

AnalyzeObjects.bucket

```
[warn ] [W13] S3 bucket block public access settings are configured to ignore public ACLs.
[warn ] [W14] S3 bucket block public access settings are configured to ignore any public bucket
[error] [E01] S3 bucket or account block public access settings are configured to ignore publi                d any public bucket policy.
```

**実行ステータス**

| 全体的なステータス | 実行されたすべてのステップ |
|---|---|
| 成功 | 11 |
| # 失敗 | # キャンセル済み |
| 1 | 0 |

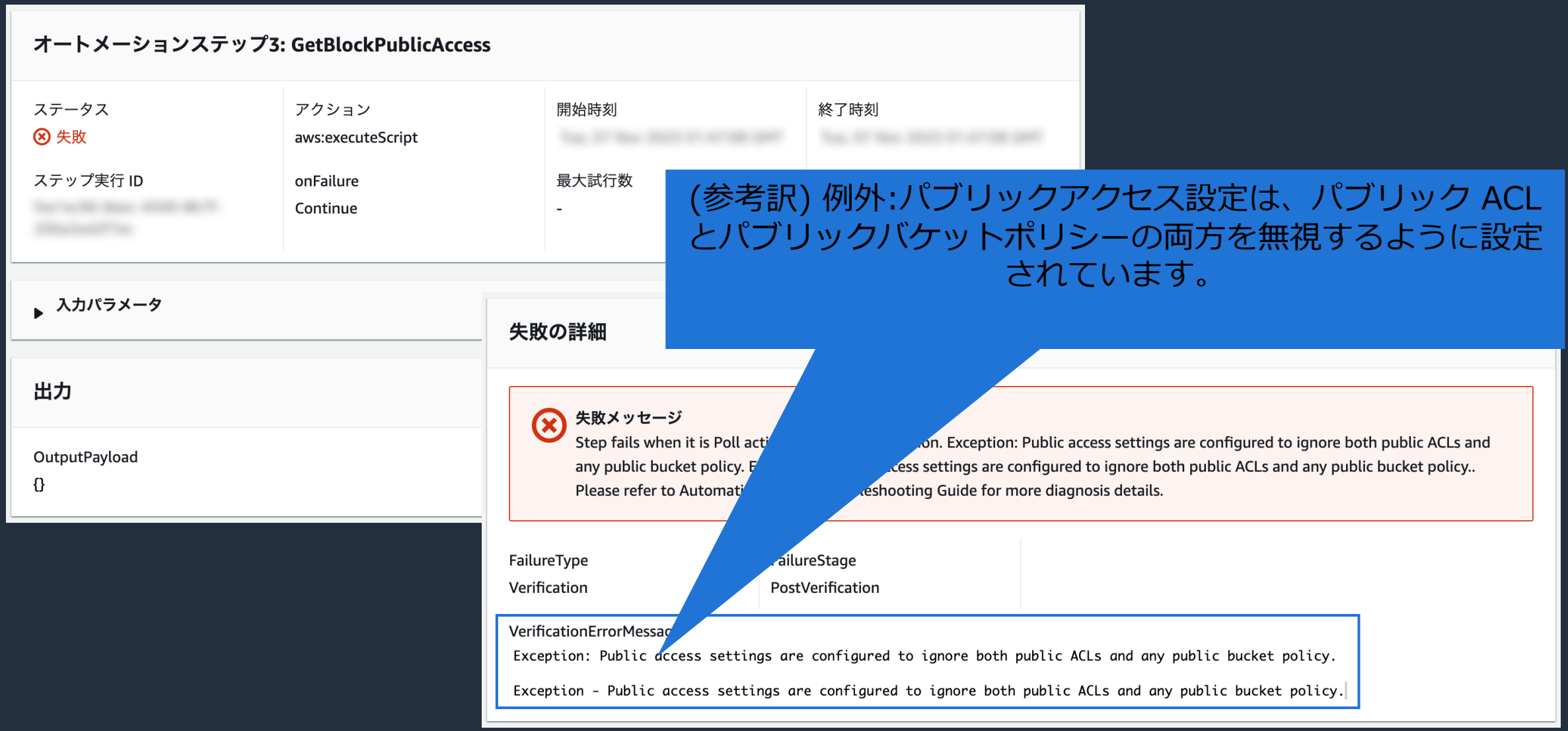
**実行されたステップ** (11)

Find Steps

1 2

| ステップ ID | ステップ番号 | ステップ名 | アクション | ステータス |
|---|---|---|---|---|
| | 1 | TestBucketAccess | aws:assertAwsResourceProperty | 成功 |
| | 2 | GetBucketInformation | aws:executeScript | 成功 |
| | 3 | GetBlockPublicAccess | aws:executeScript | 失敗 |
| | 4 | CheckBucketPayer | aws:assertAwsResourceProperty | 成功 |
| | 5 | GetBucketPolicyStatus | aws:executeScript | 成功 |
| | 6 | GetBucketPolicy | aws:executeAwsApi | 成功 |
| | 7 | GetContextKeys | aws:executeAwsApi | 成功 |
| | 8 | SimulateBucketPolicy | aws:assertAwsResourceProperty | 成功 |
| | 9 | GetBucketAcl | aws:executeAwsApi | 成功 |
| | 10 | CreateLogandStream | aws:executeScript | 成功 |

# SAW(ランブック)実行例2




(参考訳) 例外:パブリックアクセス設定は、パブリック ACL とパブリックバケットポリシーの両方を無視するように設定されています。

# その他

- 留意点
  - 対象リソースとしては S3 バケット名を入力
    - ARN 形式ではない

# AWSSupport-TroubleshootS3AccessSameAccount

# AWSSupport-TroubleshootS3AccessSameAccount

- 利用ユースケース
  - 同一アカウントの IAM ユーザー/ロールで S3 に対するアクションが拒否される場合
    - 具体例
      - IAM ユーザーに対して IAM ポリシーで GetObject 権限を付与したが、S3 オブジェクトのダウンロードに失敗する
      - バケットポリシーに変更を加えたところ、以前はできていた操作ができなくなった

# AWSSupport-TroubleshootS3AccessSameAccount

- SAW(ランブック)が確認するポイント
  - IAM ユーザー/ロールが持つ権限
  - S3 バケットの ACL 設定
  - 対象リソースの暗号化設定
  - バケットポリシー
  - VPC エンドポイントポリシー
  - KMS キーのキーポリシー
  - サービスコントロールポリシー (SCP)

# SAW(ランブック)入力パラメーター (1/3)

- AutomationAssumeRole :ランブックのアクションを実行する IAM ロール
- S3ResourceArn(必須) : 対象の S3 リソース (バケット/オブジェクト) の ARN
- S3Action(必須) : 評価の対象とする S3 アクション
- RequesterArn(必須) : アクセス権の有無を確認されたい IAM ユーザー/ロールの ARN
- RequesterRoleSessionName : RequesterArn にて IAM ロールを指定した際に、ロールを引き受ける際のセッション名

# SAW(ランブック)入力パラメーター (2/3)

- S3ObjectVersionId : S3 オブジェクトのバージョン ID
- KmsKeyArn : 対象リソースの暗号化に使用している KMS キーの ARN
- VpcEndpointId : VPC エンドポイントの ID
- ContextKeyList : 評価において必要な条件キーとそれに対する値
- SCPPolicy : AWS Organizations にて設定されている SCP

# SAW(ランブック)入力パラメーター (3/3)

- 赤枠の項目が必須パラメーター

**Input parameters**

AutomationAssumeRole
(Optional) The ARN of the role that allows the Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses your user context IAM permissions to run this document.
*Choose IAMRole*

S3Action
(Required) The S3 Action for which you want the runbook to evaluate the access context for. Make sure you provide the corresponding S3 resource type (bucket or object) for the specific action.

RequesterRoleSessionName
(Optional) The session name of the assumed role, in case the IAM ARN is a role and you want to provide a specific session name.
*String*

KmsKeyArn
(Optional) The KMS Key ARN if it is relevant to the action, example: 'CompleteMultipartUpload','CopyObject','CreateMultipartUpload','PutObject', etc., and the type of resource (bucket or object) for which you want to evaluate the access context.
*String*

ContextKeyList
(Optional) Condition keys list and corresponding values with respect to the policy evaluation. For example: [{"ContextKeyName":"aws:PrincipalArn","ContextKeyValues":["arn:aws:iam::123456789012:root"],"ContextKeyType":"string"}, {"ContextKeyName":"aws:SourceIp","ContextKeyValues":["54.240.143.0/24"],"ContextKeyType":"ip"}] (Please remove any new lines, tabs, or white spaces when you input a value) For more information please see the context-entries parameter in https://docs.aws.amazon.com/cli/latest/reference/iam/simulate-principal-policy.html
[]

S3ResourceArn
(Required) The ARN of your Amazon S3 resource (bucket or key). For object operations such as PutObject or GetObject, please provide the ARN of the object. Example: arn:aws:s3:::bucket_name, or arn:aws:s3:::bucket_name/key_name.
*String*

RequesterArn
(Required) The IAM Principal (user or role) ARN for which you want to find the access level on the specific S3 resource. For example: arn:aws:iam::123456789012:user/user_name or arn:aws:iam::123456789012:role/example-role.
*String*

S3ObjectVersionId
(Optional) If the object has multiple versions, this parameter allows you to specify the specific version of the object you want to evaluate the access context.
*String*

VpcEndpointId
(Optional) The virtual private cloud (VPC) endpoint ID related to the access evaluation. Amazon S3 bucket policies can control access to buckets from specific virtual private cloud (VPC) endpoints.
*String*

SCPPolicy
(Optional) The AWS Organizations Service Control Policy (SCP) in case you want the runbook to evaluate the input against a particular SCP policy. This is not needed and ignored when you run this runbook from the organization's management account. (Please remove any new lines, tabs, or white spaces when you input a value).
{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Action":"*","Resource":"*"}]}

# SAW(ランブック)実行例1

- 状況
  - バケットポリシーにて IAM ユーザーからの GetObject/PutObject を許可
  - IAM ユーザーの IAM ポリシーでは S3 に関する記述はなし
  - S3 バケットの ACL は無効
  - S3 バケット内のオブジェクトに対する GetObject に成功するかを評価

# SAW(ランブック)実行例1

**実行ステータス**

| 全体的なステータス | 実行されたすべてのステップ | # 成功 |
|---|---|---|
| 成功 | 14 | 14 |
| **# 失敗** | **# キャンセル済み** | **# TimedOut** |
| 0 | 0 | 0 |

▼ 出力

EvaluatePolicy.denied_statements_array

-

EvaluatePolicy.allowed_statements_array


```
{
  "Decision": "Bucket Policy",
  "MatchedStatement": {
    "Sid": "Statement1",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::
      ]
    },
    "Action": [
      "s3:GetObject",
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3:::
    ]
  }
}
```


EvaluatePolicy.final_decision

- allowed for S3 action **The output policy will be similar to a statement in your policy, but may not be exact. Please check the Actions and the Sid of your policy to match the exact statement. The Resource section of the IAM Policy and the Principal & Resource sections of the Resource Policy may be a little differing from the actual statement in the policy.**

EvaluatePolicy.final_decision – allowed for S3 action (許可)

# SAW(ランブック)実行例2

- 状況
  - バケットポリシーにて IAM ユーザーからの GetObject/PutObject を許可
  - IAM ユーザーの IAM ポリシーで対象リソースに対するアクションを拒否
  - S3 バケットの ACL は無効
  - S3 バケット内のオブジェクトに対する GetObject に成功するかを評価

# SAW(ランブック)実行例2

▼ 出力

EvaluatePolicy.allowed_statements_array


```
{
  "Decision": "Bucket Policy",
  "MatchedStatement": {
    "Sid": "Statement1",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::
      ]
    },
    "Action": [
      "s3:GetObject",
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3:::
    ]
  }
}
```


EvaluatePolicy.denied_statements_array


```
{
  "Decision": "IAM Policy",
  "MatchedStatement": {
    "Sid": "Statement1",
    "Effect": "Deny",
    "Action": [
      "s3:*"
    ],
    "Resource": [
      "arn:aws:s3:::
    ]
  }
}
```


EvaluatePolicy.final_decision

- explicitDeny for S3 action **The output policy will be similar to a statement in your policy, but may not be exact. Please check the Actions and the Sid of your policy to match the exact statement. The Resource section of the IAM Policy and the Principal & Resource sections of the Resource Policy may be a little differing from the actual statement in the policy.**

**実行ステータス**

| 全体的なステータス | 実行されたすべてのステップ | # 成功 |
|---|---|---|
| ✓ 成功 | 14 | 14 |
| # 失敗 | # キャンセル済み | # TimedOut |
| 0 | 0 | 0 |

EvaluatePolicy.final_decision - explicitDeny for S3 action (明示的な拒否)

# その他

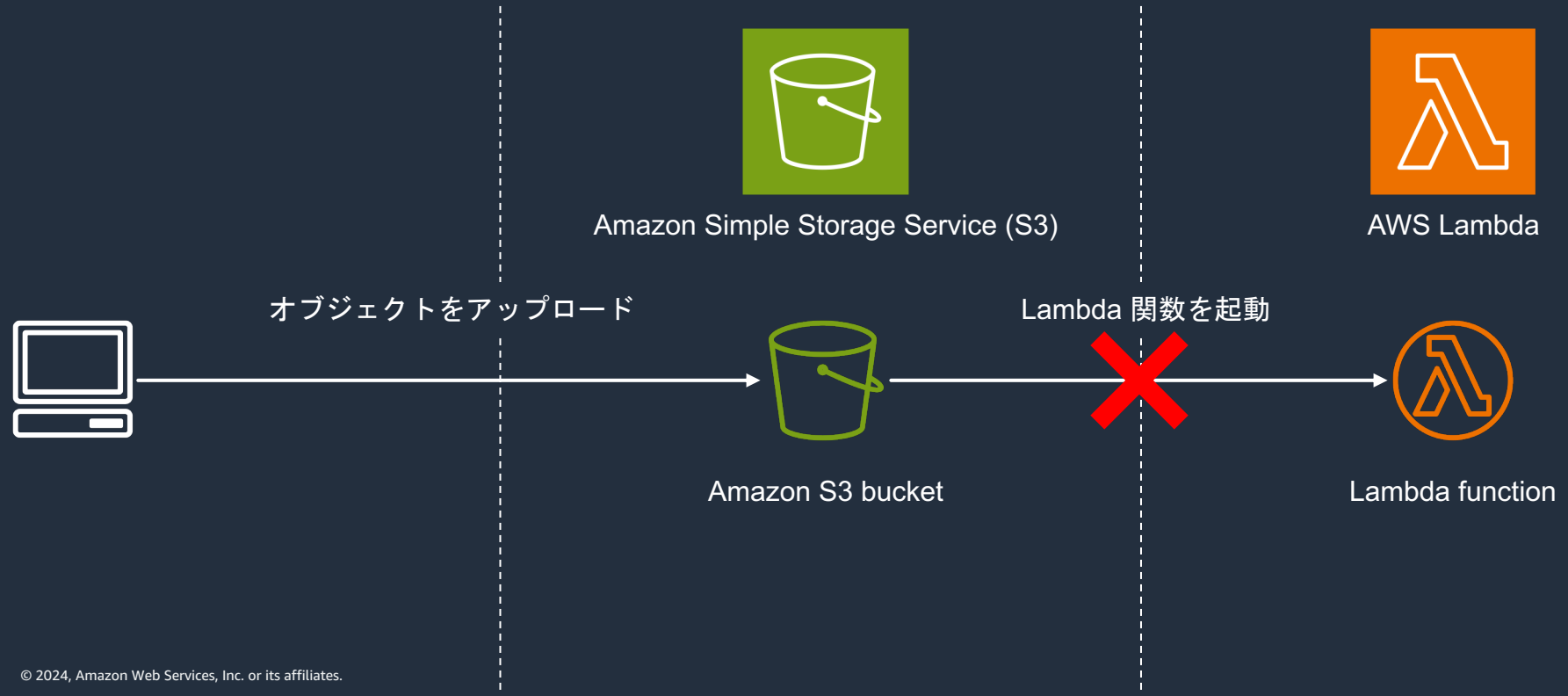
- 留意点
  - 対象リソースは ARN で入力する必要がある
  - オブジェクトレベルのアクションについて評価を行う場合には、対象リソースもオブジェクトレベルで指定する必要がある
    - GetObject/PutObject の評価を行う場合には、S3 オブジェクトの ARN を指定する必要がある

# AWSSupport-RemediateLambdaS3Event

# AWSSupport-RemediateLambdaS3Event

- 利用ユースケース
  - S3 イベントを用いて、Lambda 関数を起動するように設定したが、対象のLambda関数が起動しない

S3 イベントを利用した Lambda 関数の起動 (イメージ)



# AWSSupport-RemediateLambdaS3Event

- 利用ユースケース
  - AWSSupport-RemediateLambdaS3Event ランブックは、AWS ナレッジセンターの記事で説明されている手順を自動化するソリューションを提供します。
    - Lambda を呼び出すように Amazon S3 イベント通知を設定する | AWS re:Post
    - Amazon S3 イベント通知を作成する際のエラーのトラブルシューティング | AWS re:Post
  - S3 のイベント通知が、設定した Lambda 関数をトリガーできなかった理由を特定して修正するのに役立ちます。

# AWSSupport-RemediateLambdaS3Event

- 問題事象確認方法
  - S3 イベントを設定し、ファイルをバケットにアップロード


# AWSSupport-RemediateLambdaS3Event

- 問題事象確認方法
  - 設定したイベントタイプに該当する操作を行ったにも関わらず、Lambda 関数が呼び出されていない
    - 対象の Lambda 関数のログ出力がない
    - Invoke メトリクスが記録されない

# AWSSupport-RemediateLambdaS3Event

- SAW(ランブック)が確認するポイント
  - S3 イベントの有無
  - Lambda 関数のリソースベースのポリシー

# SAW(ランブック)入力パラメーター

- LambdaFunctionArn (必須)
  - 調査対象の Lambda 関数の ARN
- S3BucketName (必須)
  - 調査対象の S3 バケット名
- アクション [Troubleshoot or Remediate] (必須)
  - Troubleshoot: 問題の検出のみ行う
  - Remediate: 問題の修正も行う
- AutomationAssumeRole
  - Automation が各種 API を呼び出す際に利用するロール名
  - 必要な権限はドキュメント参照
  - 指定しない場合、ランブックを利用した IAM ユーザーの権限を利用

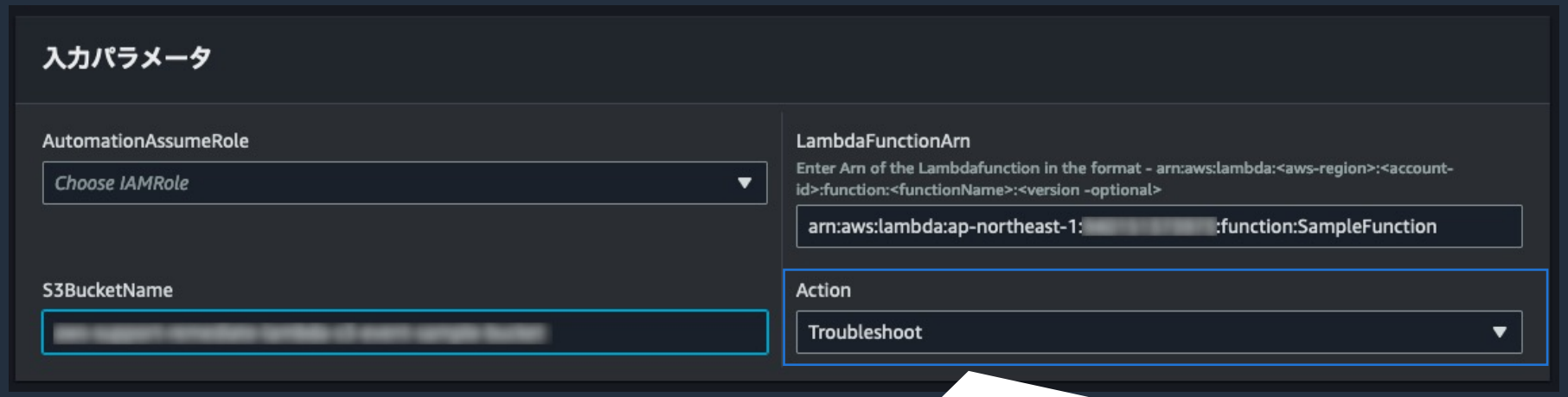
https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/automation-awssupport-remediatelambdas3event.html

# SAW(ランブック)実行例1 (Lambda関数のポリシー誤りの検出)

- 状況
  - S3 イベントの設定を行い、S3 バケットで対応する操作を行ったが、Lambda 関数が起動しない

# SAW(ランブック)実行例1 (Lambda関数のポリシー誤りの検出)

- ランブック実行のためのパラメーター指定

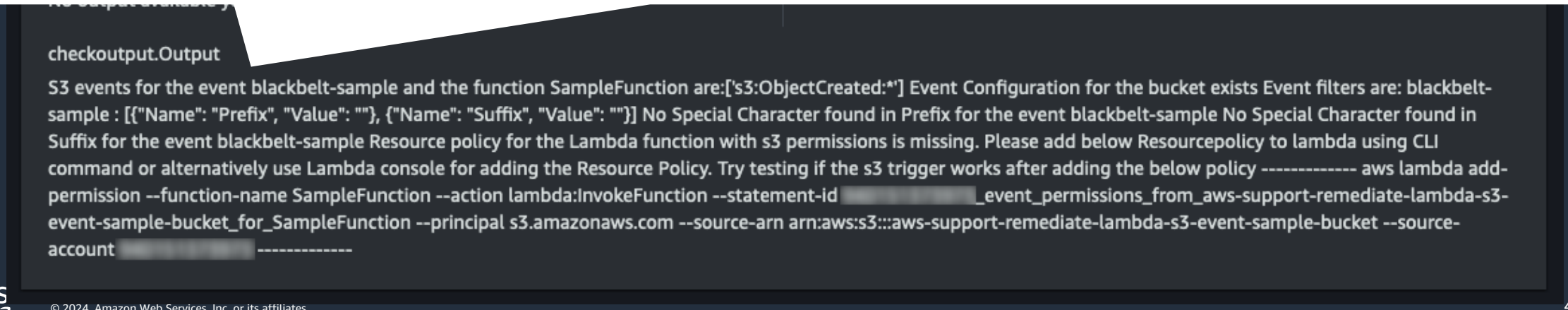



検出のみ行う場合は、Action で「Troubleshoot」を選択

# SAW(ランブック)実行例1 (Lambda関数のポリシー誤りの検出)

- ランブック実行結果
  - Lambda 関数のリソースベースのポリシーに S3 向けの権限が不足している旨が出力される
  - 必要な権限をポリシーに追加するための AWS CLI コマンドも出力される

… Resource policy for the Lambda function with s3 permissions is missing. Please add below Resourcepolicy to lambda using CLI command or alternatively use Lambda console for adding the Resource Policy. Try testing if the s3 trigger works after adding the below policy …

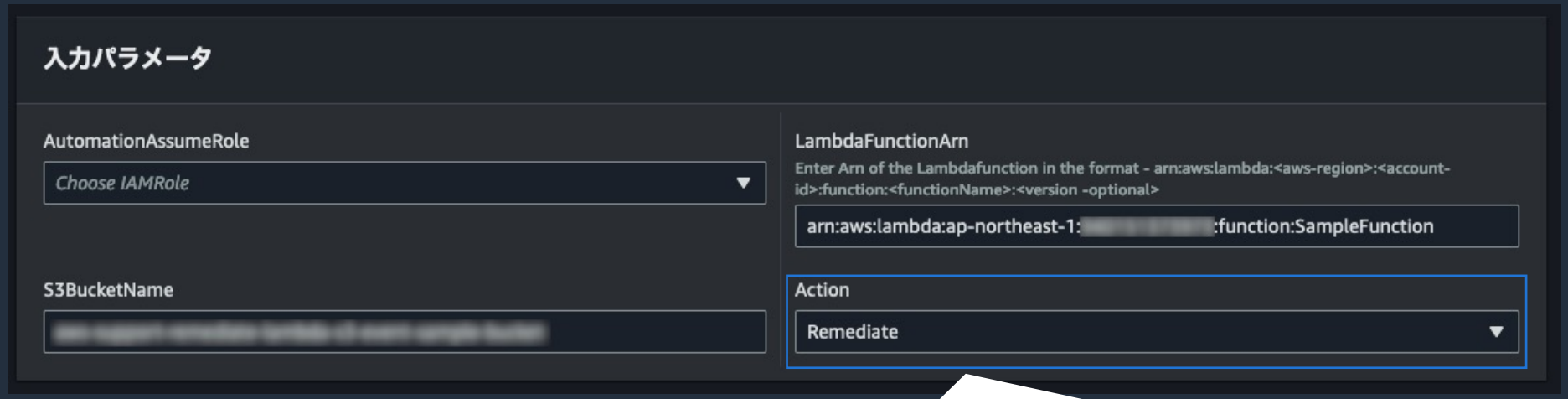


# SAW(ランブック)実行例2 (Lambda関数ポリシーの自動修正)

- 状況
  - S3 イベントの設定を行い、S3 バケットで対応する操作を行ったが、Lambda 関数が起動しない
  - Action 「Troubleshoot」でランブックを実行し、Lambda 関数のリソースベースのポリシーに問題があることが分かった
  - ランブックから、対象の Lambda 関数のリソースベースのポリシーを自動で修正したい

# SAW(ランブック)実行例2 (Lambda関数ポリシーの自動修正)

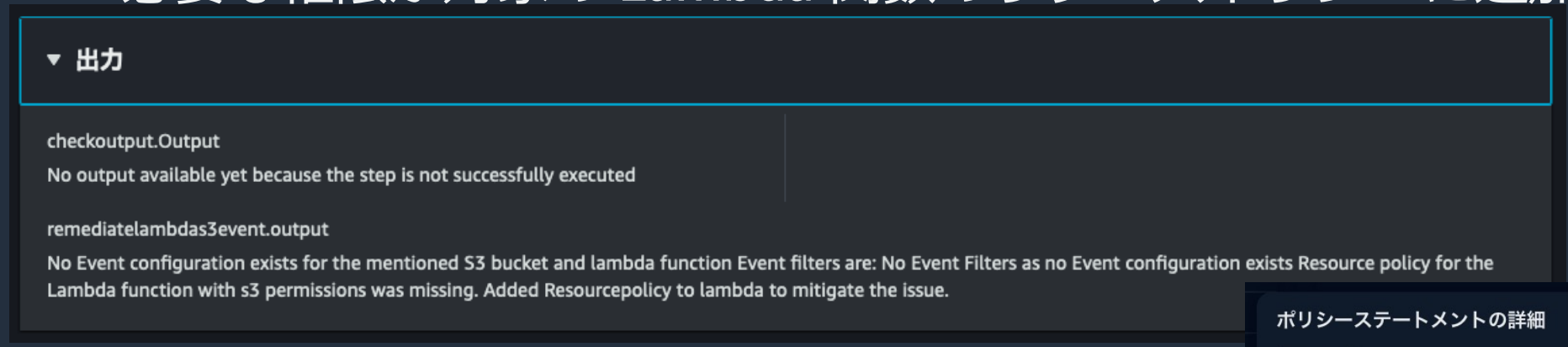
- ランブック実行のためのパラメーター指定

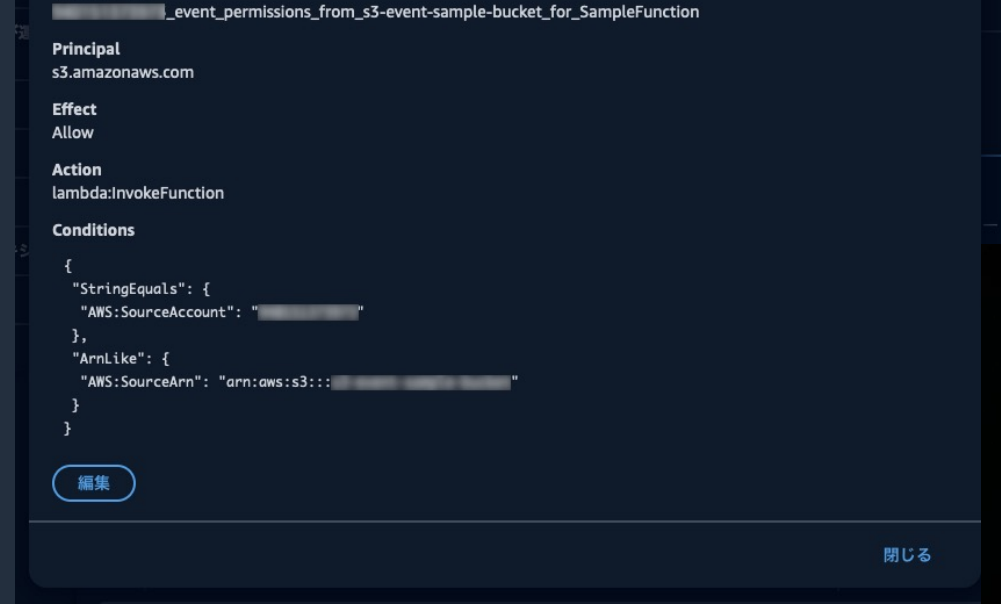



修正も行う場合は、Action で「Remediate」を選択

# SAW(ランブック)実行例2 (Lambda関数ポリシーの自動修正)

- ランブック実行結果
  - 必要な権限が対象の Lambda 関数のリソースポリシーに追加される



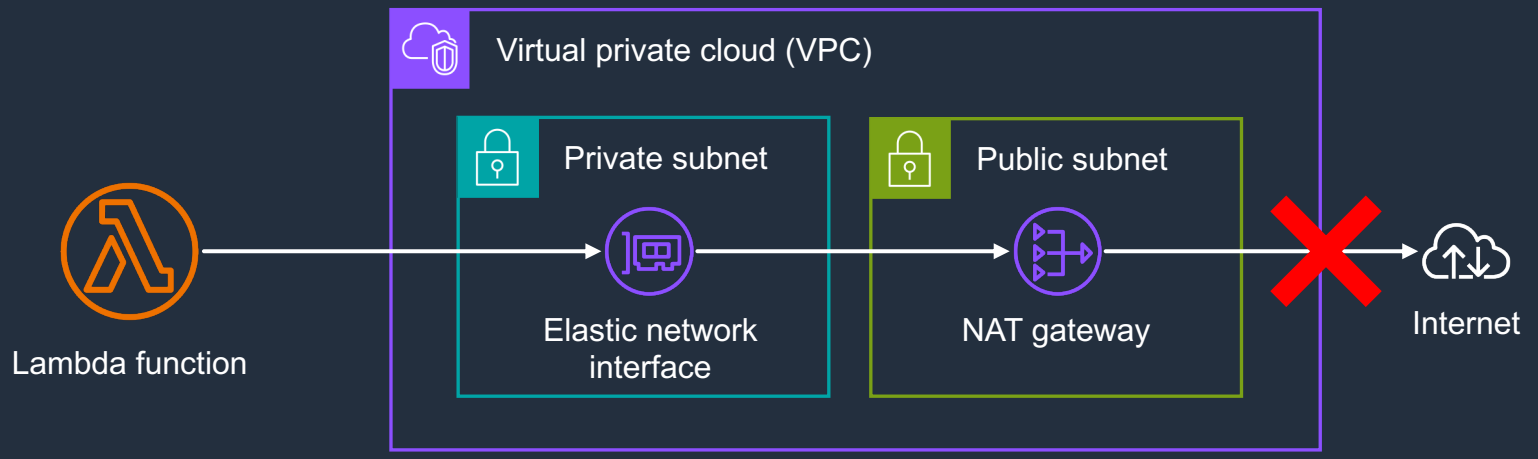
# その他

- 留意点
  - S3 イベントの設定内容に起因する問題は範囲外
    - 例えば、下記のパターンは非対応
      - s3:ObjectCreated:CompleteMultipartUpload が指定されておらず、マルチパートアップロードされた場合に Lambda 関数が起動しない
      - S3 イベントでプレフィックスを指定したが、アップロード対象のオブジェクトが該当せず、Lambda 関数が起動しない
        - 例) プレフィックスに .jpg を指定し、example.png がアップロードされた場合

# AWSSupport-TroubleshootLambdaInternetAccess

# AWSSupport-TroubleshootLambdaInternetAccess

- 利用ユースケース
  - VPC に接続された Lambda 関数において、インターネットアクセスができない



# AWSSupport-TroubleshootLambdaInternetAccess

- 問題事象確認方法
  - インターネット経由で通信を行うコードを VPC に接続した Lambda 関数で実行

```
import requests

def lambda_handler(event, context):
  res = requests.get('https://example.com', timeout=10)
  print(res.status_code)
```

  - 設定に問題があり、インターネット経由で example.com にアクセスする際

```
START RequestId: 63e269e6-7301-4cc3-8ae3-8caf0a2cec5b Version: $LATEST
[ERROR] ConnectTimeout: HTTPSConnectionPool(host='example.com', port=443): Max retries exceeded with url: / (Caused by ConnectTimeoutError(<urllib3.connection.HTT'Connection to example.com timed out. (connect timeout=10)'))PSConnection object at 0x7fa46bf08150>,
…
```

# AWSSupport-TroubleshootLambdaInternetAccess

- SAW(ランブック)が確認するポイント
  - セキュリティグループ
  - サブネットのネットワークACL
  - サブネットのルートテーブル

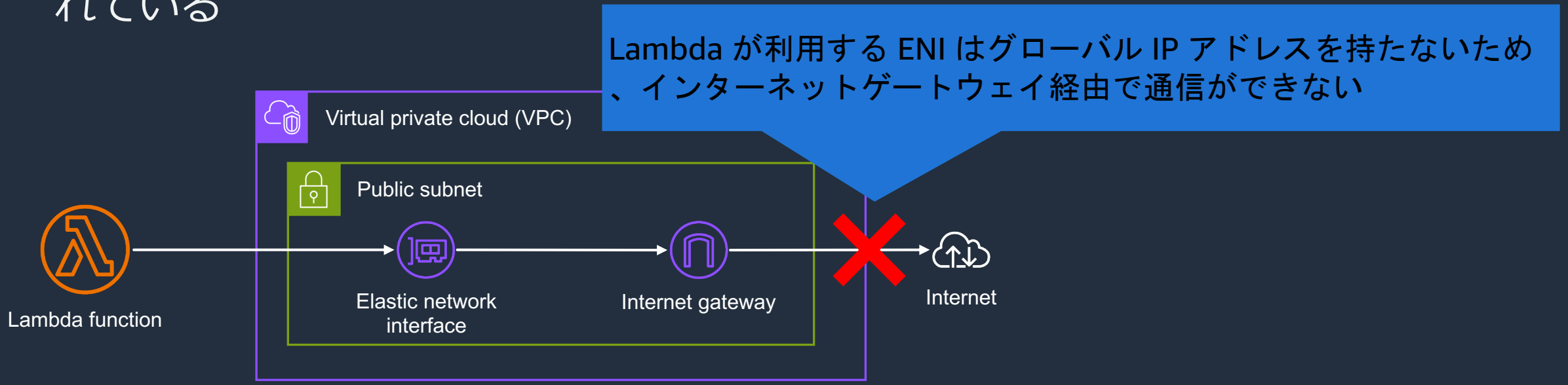
# SAW(ランブック)入力パラメーター

- FunctionName (必須)
  - 調査対象の Lambda 関数名
- destinationIp (必須)
  - Lambda 関数のアクセス先 IP アドレス
- destinationPort
  - Lambda 関数のアクセス先ポート番号
- AutomationAssumeRole
  - 「AWSSupport-RemediateLambdaS3Event」と同様

https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/AWSSupport-TroubleshootLambdaInternetAccess.html

# ランブック実行例

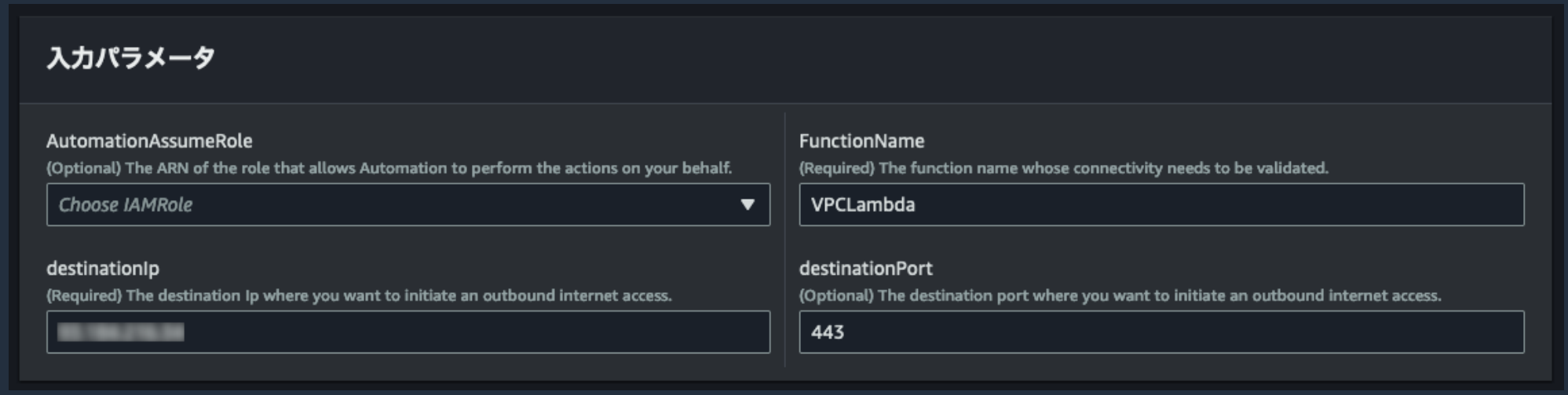
- 状況
  - ルートテーブルのデフォルトルートにインターネットゲートウェイが指定されている




| 送信先 | ターゲット |
|---|---|
| 10.0.0.0/16 | local |
| 0.0.0.0/0 | インターネットGW |

# ランブック実行例

- ランブック実行のためのパラメーター指定



# ランブック実行例1 (Lambda関数のポリシー誤りの検出)

- ランブック実行結果

▼ 出力

checkVpc.securityGroups

sg-[redacted], sg-[redacted]

checkVpc.subnet

subnet-[redacted]

checkVpc.vpc

vpc-[redacted]

checkNACL.NACL


```
{
  "subnet-[redacted]": {
    "NACL": "acl-[redacted]",
    "destinationIp_Egress": "Allowed",
    "destinationIp_Ingress": "Allowed",
    "Analysis": "This NACL has both Egress and Ingress rule allowing your desired destination IP / destionation port"
  }
}
```


checkSecurityGroups.secgrps


```
{
  "sg-[redacted]": {
    "Status": "Allowed",
    "Analysis": "This security group has allowed destintion IP and port
  },
  "sg-[redacted]": {
    "Status": "Allowed",
    "Analysis": "This security group has allowed destintion IP and port in its outbuond rule."
  }
}
```


ルートテーブルにインターネットゲートウェイの経路があること、インターネットゲートウェイではなく、NAT ゲートウェイを利用すべきである点が出力される

checkSubnet.subnets


```
{
  "subnet-[redacted]": {
    "Route": {
      "DestinationCidrBlock": "0.0.0.0/0",
      "GatewayId": "igw-[redacted]",
      "Origin": "CreateRoute",
      "State": "active"
    },
    "Analysis": "This Route Table has an internet gateway route for your destination. However, route should be pointed to NAT gateway. Correct this route entry to NAT gateway.",
    "RouteTable": "rtb-[redacted]"
  }
}
```

# その他

- 留意点
  - 名前解決に関する問題は範囲外

# まとめ

# まとめ

- SAW を使うことでお客様自身でトラブルシューティングを行うことができる
  - 自動化された分析によってヒューマンエラーの削減および作業の効率化
  - 問題解決までの時間を削減
- 問題解決しない場合には通常通り、サポートケースを起票いただき、AWS サポートまでお問い合わせください
- SAW を実行しても問題解決しなかった場合、実行頂いた SAW のランブック名、関連する SSM Automation の実行 ID、SAW の実行結果なども通常起票時に必要な情報と併せて記載頂けますと幸いです

# Thank you!