



【AWS Black Belt Online Seminar】

AWS Identity and Access Management

(AWS IAM)

アマゾンウェブサービスジャパン株式会社
プロフェッショナルサービス本部 高田 智己
2016.09.21

内容についての注意点

- 本資料では2016年9月21日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。最新の情報はAWS公式ウェブサイト(<http://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が東京リージョンを使用する場合、別途消費税をご請求させていただきます。

AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at <http://aws.amazon.com/agreement/>. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

アジェンダ

- IAMの概要
- IAMによる認証 (Authentication)
- IAMによる権限設定 (Authorization)
- IAMによる監査 (Audit)
- AWS Security Token ServiceとIAMロール
- IAMによるFederation
- まとめ



アジェンダ

- IAMの概要
- IAMによる認証 (Authentication)
- IAMによる権限設定 (Authorization)
- IAMによる監査 (Audit)
- AWS Security Token ServiceとIAMロール
- IAMによるFederation
- まとめ



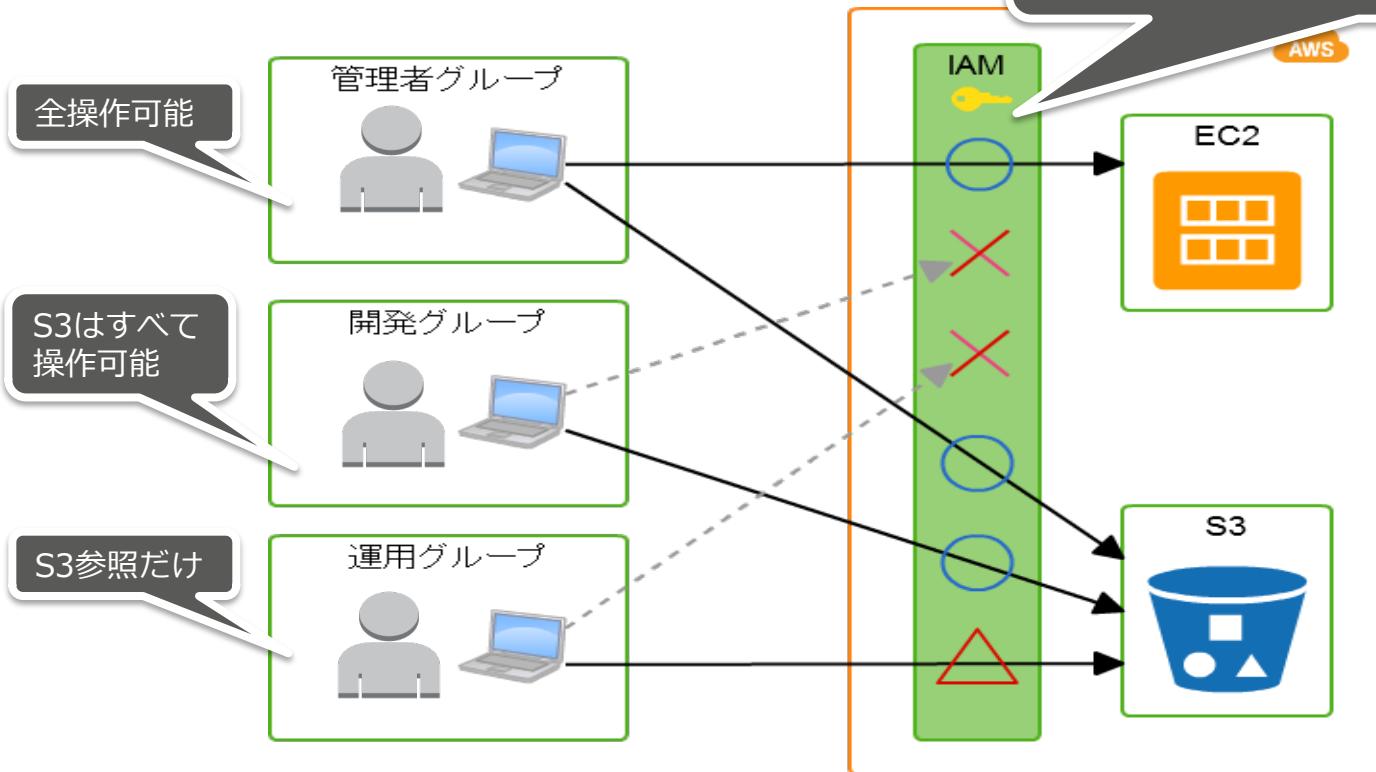
AWS Identity and Access Management (IAM)

- AWS操作をよりセキュアに行うための認証・認可の仕組み
- AWS利用者の認証と、アクセスポリシーを管理
 - AWS操作のためのグループ・ユーザー・ロールの作成が可能
 - グループ、ユーザーごとに、実行出来る操作を規定できる
 - ユーザーごとに認証情報の設定が可能



IAM動作イメージ

APIやマネジメントコンソールからの
アクセスに対して、権限をチェック



AWSアカウント (root) ユーザー

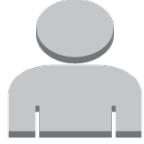
- AWSアカウント作成時のID
- アカウントの全ての AWS サービスとリソースへの完全なアクセス権限を持つ
- アカウントの作成に使用したメールアドレスとパスワードでサインイン
- 日常的なタスクには、それが管理者タスクであっても、root ユーザーを使用しないことを強く推奨

AWSのroot権限が必要な操作の例

以下の操作にはAWSのルート権限が必要となります。 (2016年9月現在)

- AWS ルートアカウントのメールアドレスやパスワードの変更
- IAMユーザーの課金情報へのアクセスに関するactivate/deactivate
- 他のAWSアカウントへのRoute53のドメイン登録の移行
- CloudFrontのキーペアの作成
- AWSサービス（サポート等）のキャンセル
- AWSアカウントの停止
- コンソリディテッドビリングの設定
- 脆弱性診断フォームの提出
- 逆引きDNS申請

IAMユーザー



- AWS操作用のユーザー
 - 1AWSアカウントで5000ユーザーまで作成可能
- ユーザーごとに設定可能な情報
 - ユーザー名
 - IAMユーザーの識別と、マネジメントコンソールへのログインに使用
 - 64文字までのアルファベット、数字、+=,.@-_
 - パス（オプション）
 - ユーザーにオプションとしてセットできる情報
 - パスを元にユーザーの検索が可能
 - 組織階層やプロジェクトなどをセット（例）/aws/sa/
 - 512文字までのBasic Latin文字（アルファベット、数字、!"#\$%&'()=~|-^¥@`{[]}*:+;?_）
 - 開始と終了が/であること
 - 所属グループ
 - 10のグループまで設定可能
 - パーミッション
 - AWSサービスへのアクセス権限
 - JSON形式でポリシーを記述

IAMグループ



- IAMユーザーをまとめれるグループ
 - 1AWSアカウントで100グループまで作成可能
- グループに設定可能な情報
 - グループ名
 - グループの識別に使用。最大128文字。
 - パス（オプション）
 - 組織階層などをセット 例) /aws/
 - パーミッション
 - グループに設定したパーミッションは、IAMユーザーに付与したパーミッションと同時に評価
 - 評価方法は後述

アジェンダ

- IAMの概要
- IAMによる認証 (Authentication)
- IAMによる権限設定 (Authorization)
- IAMによる監査 (Audit)
- AWS Security Token ServiceとIAMロール
- IAMによるFederation
- まとめ



IAMで使用する認証情報

- アクセスキーID/シークレットアクセスキー
 - REST,Query形式のAPI利用時の認証に使用
 - 2つまで生成可能
 - Active/Inactiveの切り替え
 - 情報の置き場には注意
 - GitHub
 - AMIの中への埋め込み
 - ワード文書等に記述
 - 非暗号化メールの中に記述
 - コードの中への直接書き込み
 - AWS 認証情報ファイル
 - 環境変数
- X.509 Certificate
 - SOAP形式のAPIリクエスト用
 - OpenSSLなどで証明書を作りアップロード

Access Key ID	Created	Last Used	Last Used Service	Last Used Region	Status
AKIAJPBCSRVV4	2014-07-25 13:25 UTC+0900	N/A	N/A	N/A	Inactive (Make Active Delete)
AKIAI7ZJG6Y24N	2015-04-21 19:11 UTC+0900	N/A	N/A	N/A	Active (Make Inactive Delete)

□ X.509 Certificates

Note: You can have a maximum of two X.509 certificates (active or inactive) at a time.

Created	Deleted	Thumbprint	Status	Actions
Apr 16th 2014		Y26KDMVOINFRS2LJWKLUGDP4PNWXRDFW	(Download Certificate)	Active Make Inactive Delete
Create New Certificate Upload Your Own Certificate				

IAMで使用する認証情報

- AWSマネジメントコンソールへのログインパスワード

- デフォルトは未設定（ログインできない）
 - 128文字までのBasic Latin文字
 - パスワード変更時のポリシー設定が可能
 - AWSアカウントごとに設定
 - 最低パスワード長、大文字小文字等

- MFA(多要素認証)

- ハードウェアMFA、仮想MFA、SMS MFAより選択
 - ハードウェアMFA
 - Gemalto社からAWS用のデバイスを購入
 - Tokenタイプ
 - カードタイプ **(2016年9月現在利用できません)**
 - 仮想MFA
 - スマートフォンやPCにインストール
 - Google Authenticatorなど、TOTP実装のソフトが利用可能
 - SMS MFA (プレビュー)
 - モバイルデバイスのSMSを利用



強度の強いパスワードポリシーの利用

- AWSの管理コンソールにログインするために必要となるIAMユーザーのパスワードには以下ののようなパスワードポリシーを持たせることが可能

- パスワードの最小文字数
- 大文字英字の要求
- 小文字英字の要求
- 数字を含めることの要求
- 特殊文字の要求
- ユーザー自身によるパスワード変更の許可
- パスワードの有効期限の設定
- パスワードの再利用の制限
- パスワードが期限切れになった場合管理者によるリセットの有無

▼ パスワードポリシー

パスワードポリシーは、IAMユーザーが設定できるパスワードの種類を定義するルールのセットです。パスワードポリシーの詳細については、「IAM の使用」の「[パスワードの管理](#)」を参照してください。

以下の既存のパスワードポリシーを変更します。

パスワードの最小長:

少なくとも 1 つの大文字が必要 ⓘ

少なくとも 1 つの小文字が必要 ⓘ

少なくとも 1 つの数字が必要 ⓘ

少なくとも 1 つの英数字以外の文字が必要 ⓘ

ユーザーによるパスワードの変更を許可 ⓘ

パスワードの失効を許可 ⓘ

パスワードの有効期間(日数):

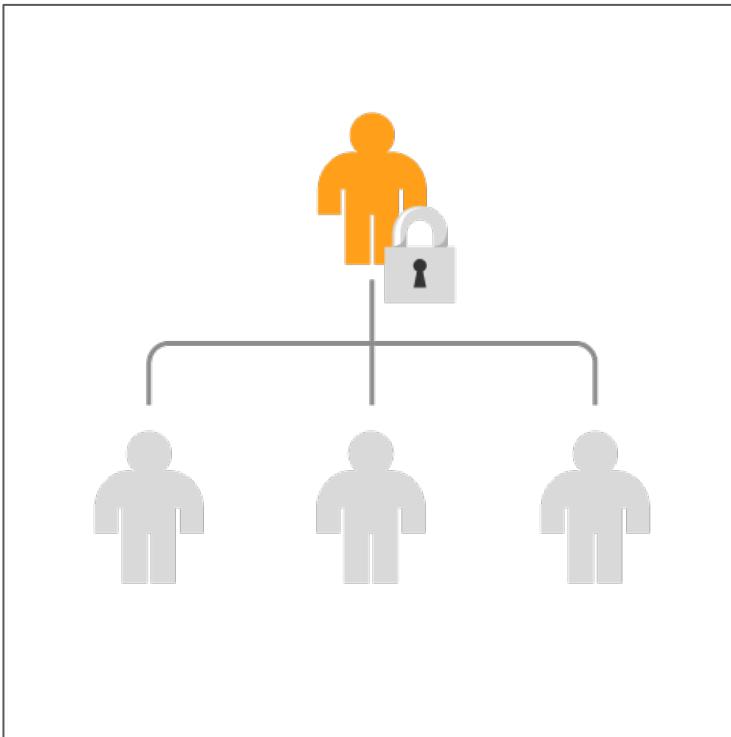
パスワードの再利用を禁止 ⓘ

記憶するパスワードの数:

パスワードの有効期限で管理者のリセットが必要 ⓘ

AWSルートアカウントには適用されないことに注意

AWSルートアカウントは極力利用しない



- AWSルートアカウントは**IAMで設定するアクセスポリシーが適用されない**強力なアカウント
- 十分に強度の強いパスワードを設定した上、通常は極力利用しないような運用を
- Security CredentialのページからAccess Keyの削除（ただしAccess Keyを使用していないか確認が必要）

S Edit Tomomi Takada ▾ Global ▾ Support ▾

Your Security Credentials

This page allows you to manage your AWS security credentials. To manage credentials for AWS Identity and Access Management (IAM), see the IAM User Guide.

To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

[My Account](#) [Billing & Cost Management](#) [Amazon CloudWatch Metrics](#) [AM Console](#) [Security Credentials](#) [Sign Out](#)

Access Keys (Access Key ID and Secret Access Key)

You use access keys to sign programmatic requests to AWS services. To learn how to sign requests using your access keys, see the [signing documentation](#). For your protection, store your access keys securely and do not share them. In addition, AWS recommends that you rotate your access keys every 90 days.

Note: You can have a maximum of two access keys (active or inactive) at a time.

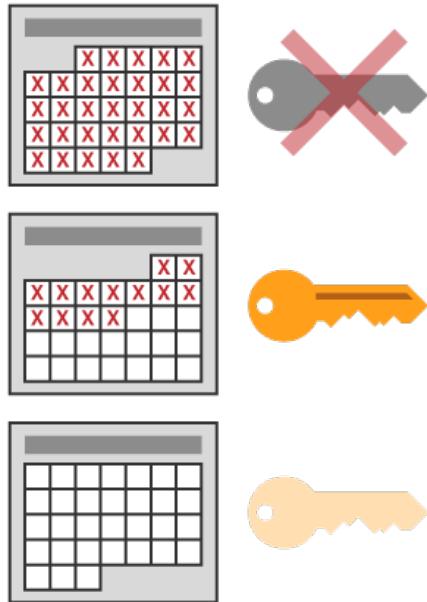
Created	Deleted	Access Key ID	Last Used	Last Used Region	Last Used Service	Status	Actions
Sep 15th 2013		AKIAIJLB47XDTJTVZAA	2015-04-23 09:22 UTC+0900	N/A	s3	Active	Make Inactive Delete
Nov 17th 2013		AKIAJ7LBKK7GAI5RMNA	N/A	N/A	N/A	Active	Make Inactive Delete
Sep 2nd 2013	Nov 17th 2013	AKIAI3DKSUQ6F7XQ4D1Q	N/A	N/A	N/A	Deleted	

MFAによるアカウントの保護

- 多要素認証（MFA）によるなりすましの防止
- AWSルートアカウントはMFAで保護し通常利用しない運用に
- 2016年9月現在カード型のハードウェアMFAは利用できません。

	ハードウェア	ソフトウェア (認証情報コピー不可)	ソフトウェア (認証情報コピー可能)	SMS (プレビュー)
製品	Gemalto	Google Authenticator	Authy	N/A
形式	トークン型／（カード型）	スマホアプリ	スマホアプリ	モバイルデバイスのSMS
コスト	有料（2,000円程度）	無料	無料	SMS料金/データ料金
保管	持ち歩くことも可能だし、金庫などに厳重に保管も可能	常に持ち歩く	常に持ち歩く	常に持ち歩く
交換	紛失／故障時は、再登録 交換のために予備の準備が必要	紛失／機種変更時は、再登録	機種交換時に認証情報を引き継げる	同じ電話番号を持つ新しいモバイルフォンを取得する場合支障なし
ルートアカウント	サポート	サポート	サポート	サポートしていない
IAMユーザー	サポート	サポート	サポート	サポート

認証情報の定期的なローテーション



- IAMユーザーのパスワードやAccess Key/Secret Access Keyは定期的にローテーションすることを推奨
- 認証情報の利用状況はIAMのCredential Report機能で確認可能
 - ユーザーの作成日時
 - 最後にパスワードが使われた日時
 - 最後にパスワードが変更された日時
 - MFAを利用しているか
 - Access KeyがActiveか
 - Access Keyのローテートした日時
 - Access Keyを最後に使用した日時
 - Access Keyを最後に利用したAWSサービス
 - 証明書はActiveか
 - 証明書のローテートした日時

IAM認証情報レポート (Credential Report)

The screenshot shows the AWS IAM console interface. On the left, there's a sidebar with links like Dashboard, Details, Groups, Users, Roles, Policies, Identity Providers, Account Settings, and Credential Report. The Credential Report link is highlighted with a red box. Below the sidebar, a main panel displays the 'Welcome to Identity and Access Management' message and various statistics: Users: 15, Groups: 3, Roles: 26, and Customer Managed Policies: 4. A 'Security Status' section shows a progress bar at 4 out of 5 complete. Below this, there are three items with checkboxes: 'Delete your root access keys' (unchecked), 'Activate MFA on your root account' (checked), and 'Create individual IAM users' (checked). A large orange box highlights the 'Credential Report' button at the bottom of the main panel.

レポートは4時間毎に一回生成可能

- ・ パスワードやアクセスキーのローテーションなど、認証情報ライフサイクルの要件の結果を監査可能
- ・ 認証情報レポートは、カンマ区切り値 (CSV) ファイルとしてダウンロード可能
- ・ 使用していない認証情報は削除！

The screenshot shows a Microsoft Excel spreadsheet titled 'status_reports_2015-05-14T06-25'. The table has columns labeled A through H. Column A contains user IDs, column B contains ARNs, column C contains creation times, column D contains password hashes, column E contains last used dates, column F contains last change dates, column G contains next rotation dates, and columns H and I contain status and access information. The table is filled with data for multiple users, including 'root_account', 'adftest', 'admin-test', 'cloudberry', 'sengard', 'kkk', 'restiam', 'takizawa', 'yo1', 'yo1private', 'yo1t', and 'yoicht'. A green box highlights the 'password_next_rotation' column for the 'root_account' row.

A	B	C	D	E	F	G	H	I
user	arn	user_creation_time	password_hash	password_last_used	password_last_changed	password_next_rotation	mfa_active	access
<root_account>	arn:aws:iam::123456789012:root	2014-10-02T11:12:58+00:00	not_supp	2015-05-14T02:17:24+00:00	not_supported	not_supported	TRUE	
adftest	arn:aws:iam::123456789012:user/adftest	2015-07T09:12:18+00:00	FALSE	N/A	N/A	N/A	FALSE	
admin-test	arn:aws:iam::123456789012:user/admin-test	2015-04-14T06:34:15+00:00	FALSE	2015-04-14T06:37:11+00:00	N/A	N/A	TRUE	
cloudberry	arn:aws:iam::123456789012:user/cloudberry	2014-11-25T02:42:20+00:00	FALSE	N/A	N/A	N/A	FALSE	
sengard	arn:aws:iam::123456789012:user/sengard	2015-03-12T04:41:26+00:00	FALSE	N/A	N/A	N/A	FALSE	
kkk	arn:aws:iam::123456789012:user/kkk	2014-11-20T05:24:30+00:00	FALSE	N/A	N/A	N/A	FALSE	
restiam	arn:aws:iam::123456789012:user/restiam	2015-03-27T13:57:45+00:00	TRUE	2015-03-27T14:26:53+00:00	2015-03-27T13:58:30+00:00	N/A	FALSE	
takizawa	arn:aws:iam::123456789012:user/takizawa	2015-04-23T06:47:03+00:00	TRUE	2015-04-23T07:04:46+00:00	2015-04-23T06:48:52+00:00	N/A	TRUE	
yo1	arn:aws:iam::123456789012:user/yo1	2014-10-06T05:13:42+00:00	TRUE	2015-05-08T06:24:40+00:00	2014-11-14T02:37:24+00:00	N/A	TRUE	
yo1private	arn:aws:iam::123456789012:user/yo1private	2015-01-06T13:17:42+00:00	FALSE	N/A	N/A	N/A	FALSE	
yo1t	arn:aws:iam::123456789012:user/testing/yo1t	2015-05-07T00:51:17+00:00	TRUE	2015-05-07T00:59:42+00:00	2015-05-07T00:52:21+00:00	N/A	TRUE	
yoicht	arn:aws:iam::123456789012:user/yoicht	2014-10-10T11:10:53+00:00	TRUE	2014-11-13T05:28:03+00:00	2014-11-13T05:27:19+00:00	N/A	FALSE	

IAMユーザーのパスワードローテーション

The screenshot shows the AWS IAM Management Console with the URL https://console.aws.amazon.com/iam/home?region=ap-northeast-1#account_settings. The left sidebar has 'Account Settings' selected. The main area is titled 'Password Policy' and contains the following information:

- A note: "Password policy is a set of rules that define the complexity requirements for passwords assigned to IAM users. For more information about password policies, see 'Using IAM' > 'Managing' > 'Passwords'."
- A note: "The following existing password policy will be updated." Below it is a text input field with the value "6".
- A list of checkboxes for password complexity:
 - At least one uppercase letter is required ⓘ
 - At least one lowercase letter is required ⓘ
 - At least one digit is required ⓘ
 - At least one non-alphanumeric character is required ⓘ
 - Allow users to change their own password ⓘ
- A red box highlights the following settings:
 - Allow users to change their own password ⓘ
 - Set password expiration (days):
 - Prevent reuse of previous passwords ⓘ
 - Number of previous passwords to remember:
 - Require password change at next login ⓘ
- Buttons at the bottom: "Password Policy Apply" and "Password Policy Delete".

- IAMのパスワードポリシーでユーザーがパスワードを変更できるように設定
- パスワードに有効期限を設けることで利用者が自分で定期的にパスワードをローテーションできるようにする

アクセスキーのローテーション

認証情報

アクセス認証情報

アクセスキー:

AKIAINOCQBSBO44YE65Q
Active
Created 2014-10-06 14:13 UTC+0900
Last Used N/A
Last Used Region N/A
Last Used Service N/A
AKIAIKC65YH2CWLP5BVQ
Active
Created 2014-10-14 19:13 UTC+0900
Last Used N/A
Last Used Region N/A
Last Used Service N/A

- IAMユーザーの「認証情報」の「アクセスキー」から「アクセスキーの管理」を選択
- 「アクセスキーの作成」で新しい認証情報の作成（2つまで）

アクセスキーの管理

AWS サービス API にセキュアな REST またはクエリプロトコルリクエストを行うには、アクセスキーを使用します。

アクセスキー ID	作成日	Last Used	Last Used Service	Last Used Region	ステータス
AKIAINOCQBSBO44YE65Q	2014-10-06 14:13 UTC+0900	N/A	N/A	N/A	Active (無効化 削除)
AKIAIKC65YH2CWLP5BVQ	2014-10-14 19:13 UTC+0900	N/A	N/A	N/A	Active (無効化 削除)

注意: 保護のため、誰ともシークレットキーを共有しないでください。また、業界のベストプラクティスでは頻繁なキー更新が推奨されています。

› アクセスキーの詳細は[こちら](#)

キャンセル アクセスキーの作成

アジェンダ

- IAMの概要
- IAMによる認証 (Authentication)
- IAMによる権限設定 (Authorization)
- IAMによる監査 (Audit)
- AWS Security Token ServiceとIAMロール
- IAMによるFederation
- まとめ



IAMポリシー

- AWSアクセスに対する権限設定
- JSON形式のアクセスポリシー言語でアクセス条件を記述
 - http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/policy-reference.html

このブロックを1条件として、
アクセス権限をチェック

```
{  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "s3>ListBuckets",  
        "s3:Get *"  
      ],  
      "Resource": [  
        "arn:aws:s3:::mybucket"  
      ],  
      "Condition": {  
        "IpAddress": {  
          "aws:SourceIP": ["176.32.92.49/32"]  
        }  
      }  
    }  
  ]  
}
```

管理ポリシーとインラインポリシー

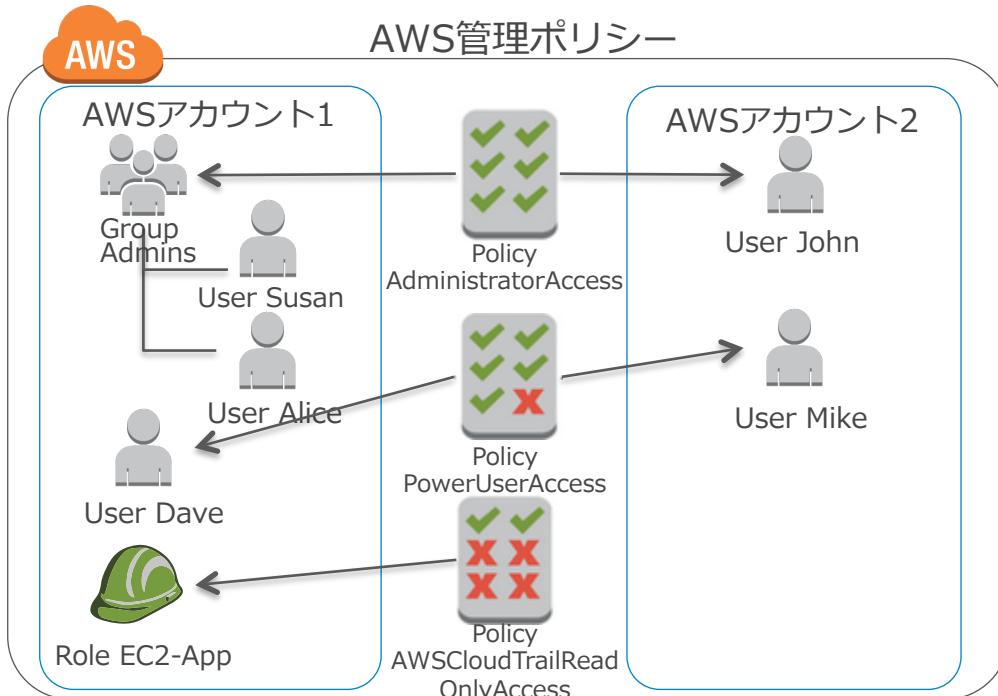
2015年より従来からのインラインポリシーに加え管理ポリシーがIAMポリシーの分類として追加。管理ポリシーは独立したポリシーであり複数のユーザーやグループ等にアタッチして利用することが可能。

分類	詳細
管理ポリシー： AWS アカウント内の複数のユーザー、グループ、およびロールに最大10個までアタッチできるスタンダードアロンポリシー。5世代まで変更を保管でき、ロールバックも可能。	AWS管理ポリシー： AWS が作成および管理する管理ポリシー
インラインポリシー： 従来のIAMポリシーと同じ内容	カスタム管理ポリシー： AWS アカウントで作成および管理する管理ポリシー

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/policies-managed-vs-inline.html

AWS管理ポリシー

AWS管理ポリシーは、AWSが作成および管理するスタンダードアロンポリシー。一般的なユースケースに基づいたAWS管理ポリシーが用意されており、利用者は事前に定義されたAWS管理ポリシーを選択して利用することが可能。



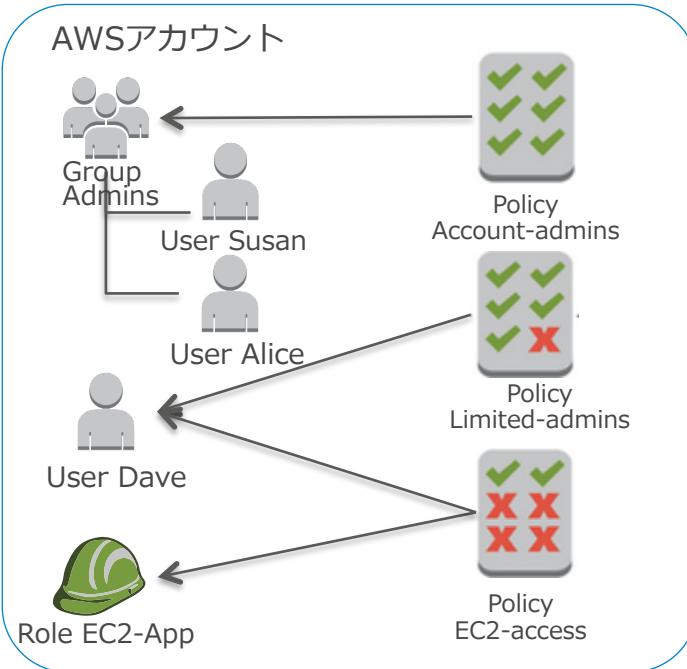
- 管理者用（すべてのアクセス）、パワーユーザー用（IAMを除くすべてのアクセス）、および AWSサービスへのその他のさまざまなレベルアクセス用の一般的なアクセス権限を定義
- 新しいAWSサービスがリリースされたり、既存のサービスで新しいAPIが利用できるようになったり、ポリシーに新しいサービスまたはAPIのアクセス権限を含める必要が発生した場合に、AWS管理ポリシーが対応
- 事前定義されているものなので、1つのAWS管理ポリシーを複数のAWSアカウントのIAMエンティティに、また1つのAWSアカウントの複数のIAMエンティティにアタッチ可能

カスタマー管理ポリシー

カスタマー管理ポリシーは、自身のAWSアカウントで管理できるスタンダードアロンポリシー。AWSアカウントの複数のIAMエンティティにカスタマー管理ポリシーをアタッチすることが可能。

カスタマー管理ポリシー

AWSアカウント



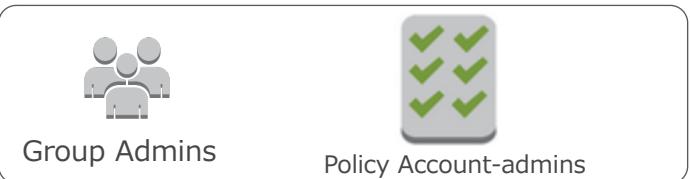
- 利用者がカスタム可能な管理ポリシー
- 同じポリシーを複数のIAMエンティティにアタッチできる
- 用意されているポリシーでは要件を満たせない場合等にカスタマー管理ポリシーを適用

インラインポリシー

インラインポリシーは、1つのIAMエンティティ（ユーザー、グループ、またはロール）に埋め込まれたポリシー。IAMエンティティの一部であり、IAMエンティティの作成時、またはそれ以降に、ポリシーを作成してIAMエンティティに埋め込まれる。

インラインポリシー

AWSアカウント



User Susan User Alice

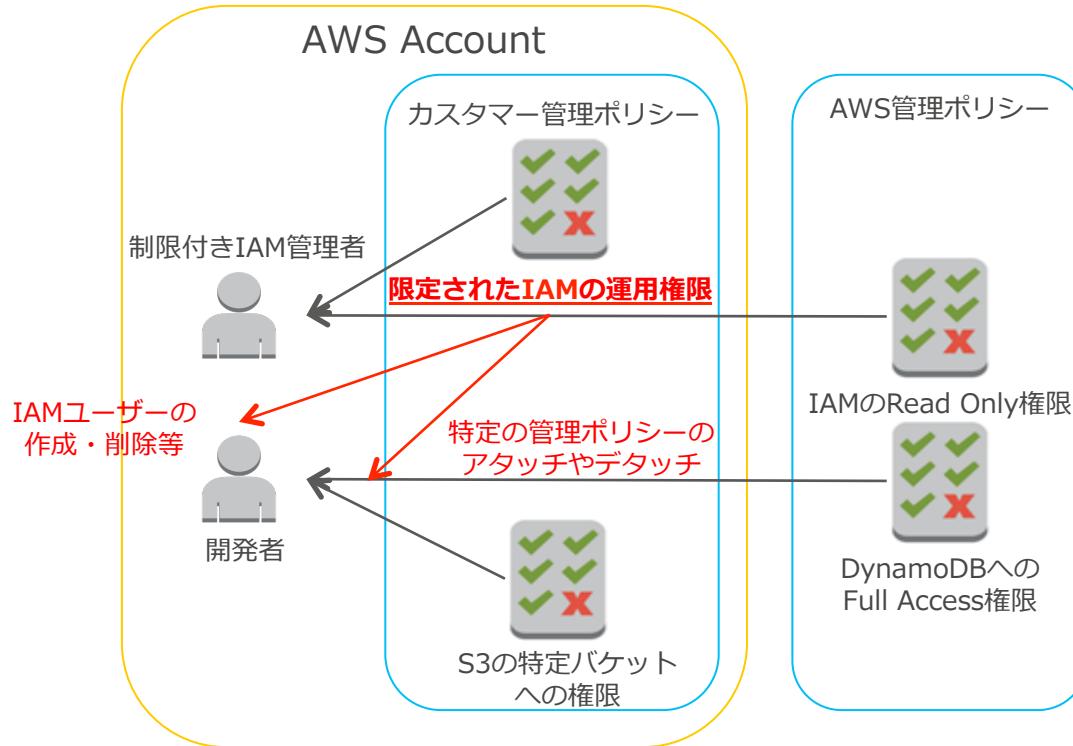


- ・ユーザー、グループ、またはロールの一部
- ・一つのポリシーを共有することはできない
- ・ポリシーの変更に関して、該当するインラインポリシー全てを個々に変更する必要がある

管理ポリシーの使い分け

- 管理ポリシーのメリット
 - 再利用性
 - 変更管理の一元化
 - バージョニングとロールバック
 - AWS管理ポリシーの自動更新
- 管理ポリシーの制限
 - AWS アカウントあたりのカスタマー管理ポリシー数: 1000
 - 管理ポリシーあたりのバージョン数: 5
 - IAM のユーザー、グループ、ロールごとにアタッチされる管理ポリシー数: 10
- 管理ポリシーに関する留意点
 - 管理ポリシーの制限が問題となるケース
 - 意図しないIAMエンティティに管理ポリシーが誤ってアタッチされるリスクを許容できないケース
 - AWS管理ポリシーに関しては、AWSによる変更が問題となるケース

管理ポリシーの使用例（アクセス権限管理の委任）



- ユーザーの作成や削除等IAMの運用・管理の一部を委任する場合
- ベースラインになるIAMのRead Only権限は事前定義されているAWS管理ポリシーを利用
- 委譲したい特定業務はカスタマー管理ポリシーを作成
- どの管理ポリシーを操作できるといった細かいアクセスコントロールも可能

アクセス条件の記述

```
{  
  "Effect": "Allow",  
  "Action": [  
    "s3>ListBuckets",  
    "s3:Get *"  
  ],  
  "Resource": [  
    "arn:aws:s3:::mybucket"  
  ],  
  "Condition": {  
    "IpAddress": {  
      "aws:SourceIP":  
        ["176.32.92.49/32"]  
    }  
  }  
}
```

Effect:
許可の設定なら"Allow"
拒否の設定なら"Deny"

Action:
対象となるAWS操作を指定

Resource:
対象となるAWSリソースを指定

Condition:
このアクセス制御が有効になる
条件の設定

この例の場合、
「アクセス元IPが176.32.92.49だったら、S3のListBucketsとGet系の操作を許
可する」という意味

Action



- 「Action」は、操作**自体**に対する設定
 - ec2:runInstances
 - ec2:AttachVolume
 - s3>CreateBucket
 - s3>DeleteObject
- ワイルドカード指定可能
 - 例) ec2:Describe*
- 指定の操作以外の場合は「NotAction」を使用
 - 例) "NotAction": "iam:*" (IAMの操作以外を許可する)

```
"Action": [  
    " s3>ListBuckets",  
    " s3:Get*"  
]
```

Resource



- 「Resource」は操作対象を指定する設定
 - EC2インスタンス
 - EBSボリューム
 - S3バケット
 - S3オブジェクト
- ARN(Amazon Resource Name)で記述
 - “arn:aws:”で始まる文字列
 - arn:aws:*service:region:account:resource*
 - 例) arn:aws:s3:::mybucket
- 指定リソース以外の場合は「NotResource」を使用
 - 例) “NotResource”：“arn:aws:s3:::hoge”

```
"Resource": [  
    "arn:aws:s3:::mybucket"  
]
```

http://docs.aws.amazon.com/ja_jp/general/latest/gr/aws-arns-and-namespaces.html

Condition



- Resourceに対するActionを許可（もしくは拒否）するかどうかの条件設定
- ポリシー変数（条件キー）に対して、演算子を用いて条件を指定

```
"Condition": {  
    "IpAddress": {"aws:SourceIP": "176.32.92.49/32" }  
}
```

演算子

ポリシー変数

条件値

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/AccessPolicyLanguage_ElementDescriptions.html#Condition

ポリシー変数

- 全てのリクエストで利用できるキー

ポリシー変数	用途
aws:CurrentTime	日時の確認
aws:EpochTime	エポック (UNIX) 時間で表した日付
aws:TokenIssueTime	一時的認証情報が発行された日付
aws:MultiFactorAuthPresent	MFAの確認
aws:MultiFactorAuthAge	MFA認証済み認証が発行された時間
aws:principaltype	プリンシパルタイプの確認
aws:Referer	クライアントブラウザーの確認
aws:SecureTransport	SSLによるリクエストの確認
aws:SourceIp	接続元IPの確認
aws:SourceArn	ソースのARNの確認
aws:SourceVpc	ソースのVPCの確認
aws:UserAgent	クライアントアプリケーション
aws:userid	ユーザーID
aws:username	ユーザー名

- AWSサービス固有のキーの例

ポリシー変数	用途
s3:prefix	Prefixの確認
sns:Protocol	配信プロトコルの確認
ec2:ResourceTag/tag名	タグ名の確認

```
"Condition": {  
    "IpAddress":  
        {"aws:SourceIP":  
            "176.32.92.49/32"}  
}
```

例えば、API呼び出し/コンソール利用を指定のIPアドレスだけに絞りたい場合に利用。
注) コンソールに関してはログインはできても操作する権限がないという状態になります。

Conditionの演算子

- 文字列
 - 完全一致、部分一致など
- 数値
 - 一致、以上、以下など
- 日付および時間
 - 一致、日付の後先など
- Boolean
- バイナリ
- IP アドレス
 - 指定のアドレス、指定範囲など
- Amazon リソース名
 - 完全一致、部分一致など
- ...IfExists
 - 上記演算子に付与。変数がない場合無視
- 条件キーの有無

```
"Condition": {  
    "StringEquals":  
        {"ec2:ResourceTag/stack":  
            "prod"}  
}
```

```
"Condition": {  
    "streq":  
        {"ec2:ResourceTag/stack":  
            "prod"}  
}
```

複数Conditionの"OR"と"AND"

AND

AND

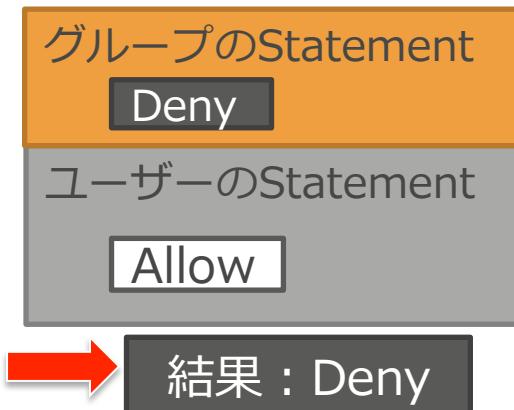
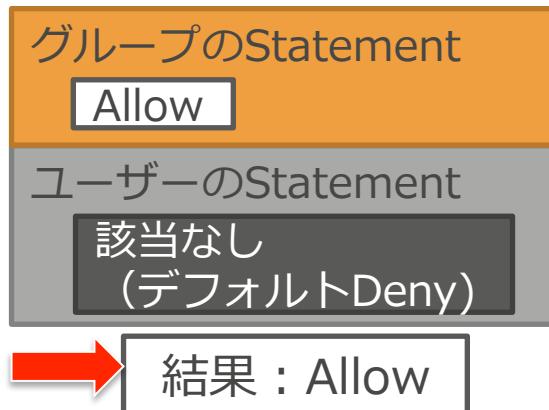
```
"Condition" : {  
    "DateGreaterThanOrEqual" : {  
        "aws:CurrentTime" : "2013-07-16T12:00:00Z"  
    },  
    "DateLessThan": {  
        "aws:CurrentTime" : "2013-07-16T15:00:00Z"  
    },  
    "IpAddress" : {  
        "aws:SourceIp" : ["192.168.176.0/24","192.168.143.0/24"]  
    }  
}
```

OR

- Condition下のブロックはAND、演算子に対する値はOR
- この例の場合、「2013/7/16の12:00から15:00の間に、ソースIP192.168.176.0/24もしくは192.168.143.0/24のネットワークからアクセスしたリクエスト」を意味する

アクセス可否の決定ロジック

- アクセス制御の条件は複数設定可能
 - ユーザー・グループごとに複数。相反する条件の設定も可能
- すべてのアクセスはデフォルトで拒否(**デフォルトDeny**)
 - アクセス権限に“Allow”的な条件があった場合、アクセス許可
 - ただしアクセス権限に1つでも“Deny”的な条件があった場合、アクセス拒否(明示的なDeny)
 - **デフォルトDeny < Allow < 明示的なDeny**



IAMと連携するAWSサービス

連携のカテゴリ	内容
アクションレベルの アクセス許可	ポリシーのAction エレメントでの個別のアクションの指定をサポート
リソースレベルの アクセス許可	ポリシーのResource要素での個別のリソースの指定 (ARN を使用) をサ ポートする 1 つ以上の APIがある
リソースベースの アクセス許可	IAM ユーザー、グループ、ロールに加えて、サービスのリソースにもポ リシーをアタッチ可能
タグベースの アクセス許可	Condition エレメントのリソースタグのテストをサポート
一時的なセキュリティ 認証のサポート	ユーザーは AssumeRole または GetFederationToken などの AWS STS API を呼び出して取得した一時的なセキュリティ認証情報を使用してリク エストを作成

IAMと連携するAWSサービス

サポートされるアクセス権限のカテゴリは各AWSサービスによって異なるため、ドキュメントにて最新の状況を確認するようにして下さい。

コンピューティングサービスの例（2016年9月現在）

サービスおよび関連する IAM 情報	次のアクセス権限をサポートします				
	アクションレベル	リソースレベル	リソースベース	タグベース	一時認証情報
Amazon Elastic Compute Cloud (Amazon EC2)	Yes	Yes ¹	No	はい ¹	Yes
Amazon EC2 Container Service (Amazon ECS)	Yes	Yes ²	No	No	Yes
Auto Scaling	Yes	No	No	No	Yes
Elastic Load Balancing	Yes	Yes ³	No	No	Yes
AWS Lambda	Yes	Yes ⁴	Yes	No	Yes

IAMと連携するAWSサービス

リソースレベルやタグベースのアクセス許可は、各AWSサービスのアクションによりサポート状況が異なるためドキュメントでの確認を行ってください。

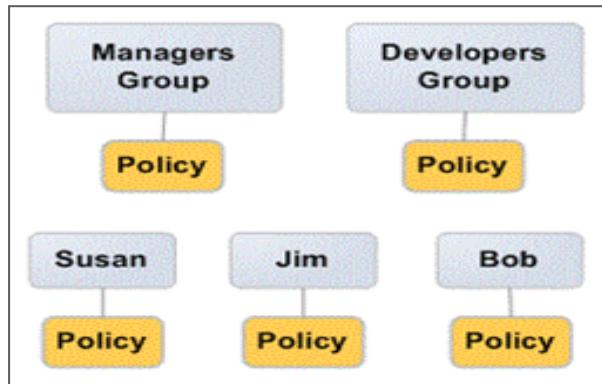
Amazon EC2 API アクションでサポートされるリソースレベルのアクセス許可の例（2016年9月現在）

StopInstances	インスタンス arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/ <i>instance-id</i>	ec2:Tenancy ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:Region ec2:ResourceTag/ <i>tag-key</i> ec2:RootDeviceType ec2:Tenancy
TerminateInstances	インスタンス arn:aws:ec2:region:account:instance/* arn:aws:ec2:region:account:instance/ <i>instance-id</i>	ec2:AvailabilityZone ec2:EbsOptimized ec2:InstanceProfile ec2:InstanceType

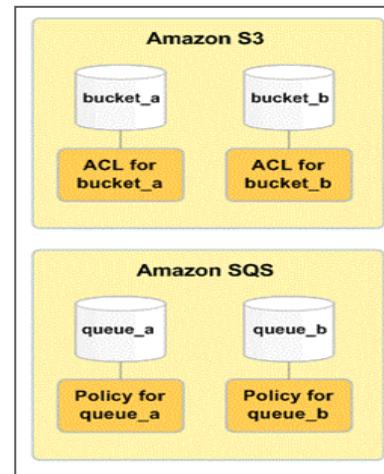
StopInstanceがサポートするリソースと条件キー

ユーザーベースとリソースベース

- ポリシーは、ユーザーやグループ以外に、リソースにも紐付け可能
- S3バケット、SQSのキューなどに対してポリシーが適用可能
 - 「特定のIPアドレスからしかアクセスできないバケット」などの設定が可能



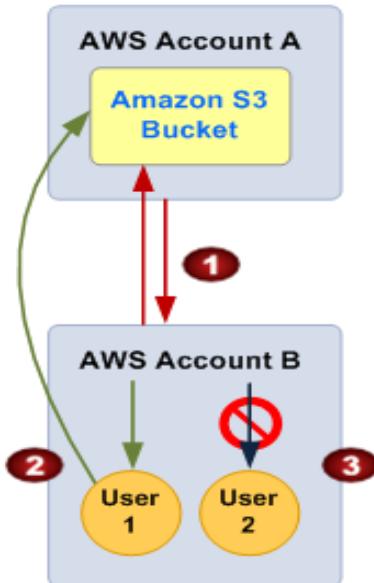
ユーザーベース



リソースベース

リソースベースのポリシーによるクロスアカウントアクセス

- AWSアカウントを超したアクセス許可
 - S3,SQS,SNSなどで利用可能



1. Account Aのバケットに以下のポリシーを設定

```
{  
    "Statement": {  
        "Effect": "Allow",  
        "Principal": {  
            "AWS": "arn:aws:iam::Account Bの番号:root"  
        },  
        "Action": "s3:*",  
        "Resource": "arn:aws:s3:::mybucket/*"  
    }  
}
```

Principalは、実行を
しているユーザーに
対する条件設定

2. Account Bに、mybucketへアクセス権限付与

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/roles-resourcebasedpolicies-compare.html

IAMポリシーの作成を支援するツール群

- AWS Policy Generator : <http://awspolicygen.s3.amazonaws.com/policygen.html>
 - AWSのサービスについて、必要情報を入力するとポリシー文書を自動作成してくれるツール
- ポリシー言語の文法チェック機能
 - ポリシー保管時にポリシー言語の文法チェック、自動フォーマットを実施
 - 「Validate Policy」により明示的な確認が可能
- IAM Policy Validator
 - 自動的に既存の IAMポリシーを調べ、IAMポリシーの文法に準拠しているか確認
 - ポリシーに対する推奨の変更を提示
 - Policy Validator を使用できるのは、準拠していないポリシーがある場合のみ
- IAM Policy Simulator : <https://policysim.aws.amazon.com/home/index.jsp>
 - プロダクションへの実装前にポリシーをテスト可能
 - パーミッションのトラブルシューティング
 - Condition、ポリシー変数、リソースベースのポリシーを入れたテスト

アジェンダ

- IAMの概要
- IAMによる認証 (Authentication)
- IAMによる権限設定 (Authorization)
- IAMによる監査 (Audit)
- AWS Security Token ServiceとIAMロール
- Federation
- まとめ

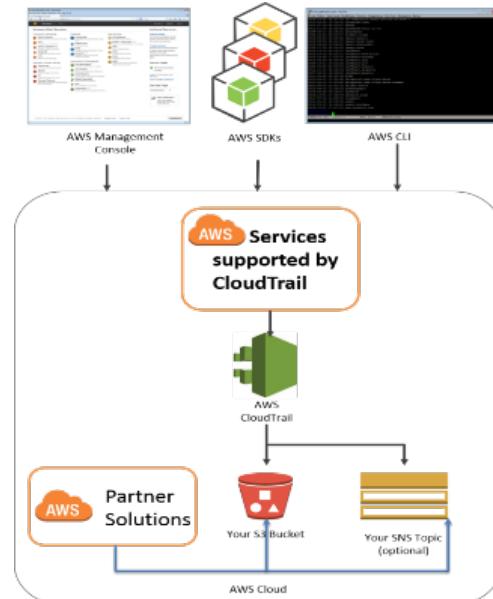


ユーザーのアクティビティの記録

AWS CloudTrailはAWSアカウントで利用されたAPI Callを記録し、S3上にログを保存するサービス。AWSのリソースにどのような操作が加えられたか記録に残す機能であり全リージョンでの有効化を推奨。
適切なユーザーが与えられた権限で環境を操作しているかの確認と記録に使用。

記録される情報には以下のようなものが含まれる

- APIを呼び出した身元 (Who)
- APIを呼び出した時間 (When)
- API呼び出し元のSource IP (Where)
- 呼び出されたAPI (What)
- APIの対象となるAWSリソース (What)
- 管理コンソールへのログインの成功・失敗
(rootアカウントの失敗は2016年9月現在未サポート)



Access AdvisorとService Last Accessed Data

- IAM エンティティ (ユーザー、グループ、ロール) が、最後に AWS サービスにアクセスした日付と時刻を表示する機能
- IAMの最小限の特権に関する設定に利用
 - IAM ポリシー内で未使用または最近使用されていないアクセス許可を識別
 - 未使用のサービスに関するアクセス許可を削除したり、類似の使用パターンを持つユーザーをグループに再編成
 - アカウントのセキュリティを改善

The screenshot shows the AWS IAM User Details page for a user named 'Admin'. The left sidebar has a red box around the 'Users' option under the 'Details' section. The main content area shows the 'Summary' tab with user information and creation time. Below it is the 'Access Advisor' tab, which is highlighted with a red box. This tab displays a table of services last accessed by the user, with columns for Service Name, Policies Granting Permissions, and Last Accessed. The table shows entries for Amazon CloudWatch and Amazon EC2, both last accessed 17 days ago.

Service Name	Policies Granting Permissions	Last Accessed
Amazon CloudWatch	AdministratorAccess	17 days ago
Amazon EC2	AdministratorAccess	17 days ago

Service Last Accessed Dataは下記のリージョンでは
2016年9月現在提供されていません。

- 中国（北京）(cn-north-1)
- AWS GovCloud (US) (region-gov-us-west-1)

Service Last Accessed Dataの利用例

- ユーザーや、グループ、ロールに与えられた権限で利用されていないものを見

AWS Directory Service	AdministratorAccess	19 days ago
Elastic Load Balancing	AdministratorAccess	19 days ago
AWS Key Management Service	AdministratorAccess	19 days ago
AWS Billing	AdministratorAccess	24 days ago
AWS IoT	AdministratorAccess	Not accessed in the tracking period
Amazon API Gateway	AdministratorAccess	Not accessed in the tracking period
AWS Certificate Manager	AdministratorAccess	Not accessed in the tracking period
AWS Database Migration Service	AdministratorAccess	Not accessed in the tracking period
Amazon Storage Gateway	AdministratorAccess	Not accessed in the tracking period

- IAMポリシーの利用状況と利用しているエンティティの識別

Access Advisor

Access advisor shows the service permissions granted to this user and when those services were last accessed. You can use this information to revise your policies. [Learn more](#)

Note: recent activity usually appears within 4 hours. Access Advisor tracking began on Oct 1, 2015. [Learn more](#)

Service Name	Access by Entities	Last Accessed
AWS Identity and Access Management	lambda_basic_execution and 1 more	Today
Amazon CloudWatch Logs	lambda_basic_execution and 1 more	Today
AWS Config	lambda_basic_execution and 1 more	Today
Amazon S3	lambda_basic_execution and 1 more	Today

Access by Entities

Service Name: AWS Identity and Access Management
Policy: AdministratorAccess

Name	Type	Last accessed
lambda_basic_execution	Role	2016-09-18 10:00-11:00 UTC+0900
Admin	User	2016-08-31 19:00-20:00 UTC+0900
Platform	User	Not accessed in the tracking period
CFnGenerator	Role	Not accessed in the tracking period

IAMポリシーを利用しているのが誰で最後にアクセスしたのがいつか簡単に識別可能

IAM認証情報レポート (Credential Report)

- ユーザーの作成日時
- 最後にパスワードが使われた日時
- 最後にパスワードが変更された日時
- MFAを利用しているか
- Access KeyがActiveか
- Access Keyのローテートした日時
- Access Keyを最後に使用した日時
- Access Keyを最後に利用したAWSサービス
- 証明書はActiveか
- 証明書のローテートした日時

	A	B	C	D	E	F	G	H	
1	user	arn	user_creation_time	password	password_last_used	password_last_changed	password_next_rotation	mfa_active	access
2	<root_account>	arn:aws:iam::123456789012:root	2014-10-02T11:12:58+00:00	not_supported	2015-05-14T02:17:24+00:00	not_supported	not_supported	TRUE	
3	adftest	arn:aws:iam::123456789012:user/adftest	2015-07-07T09:12:18+00:00	FALSE	N/A	N/A	N/A	FALSE	
4	admin-test	arn:aws:iam::123456789012:user/admin-test	2015-04-14T06:34:15+00:00	FALSE	2015-04-14T06:37:11+00:00	N/A	N/A	TRUE	
5	cloudberry	arn:aws:iam::123456789012:user/cloudberry	2014-11-25T02:42:20+00:00	FALSE	N/A	N/A	N/A	FALSE	
6	isengard	arn:aws:iam::123456789012:user/isengard	2015-03-12T04:41:26+00:00	FALSE	N/A	N/A	N/A	FALSE	
7	kkk	arn:aws:iam::123456789012:user/kkk	2014-11-20T05:24:30+00:00	FALSE	N/A	N/A	N/A	FALSE	
8	restiam	arn:aws:iam::123456789012:user/restiam	2015-03-27T13:57:45+00:00	TRUE	2015-03-27T14:26:53+00:00	2015-03-27T13:58:30+00:00	N/A	FALSE	
9	takizawa	arn:aws:iam::123456789012:user/takizawa	2015-04-23T06:47:03+00:00	TRUE	2015-04-23T07:04:46+00:00	2015-04-23T06:48:52+00:00	N/A	TRUE	
10	yo1	arn:aws:iam::123456789012:user/yo1	2014-10-06T05:13:42+00:00	TRUE	2015-05-08T06:24:40+00:00	2014-11-14T02:37:24+00:00	N/A	TRUE	
11	yo1private	arn:aws:iam::123456789012:user/yo1private	2015-01-06T13:17:42+00:00	FALSE	N/A	N/A	N/A	FALSE	
12	yo1t	arn:aws:iam::123456789012:user/testing/yo1t	2015-05-07T00:51:17+00:00	TRUE	2015-05-07T00:59:42+00:00	2015-05-07T00:52:21+00:00	N/A	TRUE	
13	yoicht	arn:aws:iam::123456789012:user/yoicht	2014-10-10T11:10:53+00:00	TRUE	2014-11-13T05:28:03+00:00	2014-11-13T05:27:19+00:00	N/A	FALSE	
14									

AWS ConfigのIAMサポート

- IAMのUser、Group、Role、Policyに関して変更履歴、構成変更を管理・確認することが可能

The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

The screenshot shows the IAM Role inspector interface. At the top, there is a message indicating the image cannot be displayed due to memory constraints or corruption. Below this, the title "IAM Role inspector" is displayed along with the date and time of the inspection: "on September 18, 2016 10:54:21 AM (UTC+09:00)". On the right side, there are buttons for "Manage resources" and a refresh icon. A navigation bar at the bottom allows for navigating through changes, with arrows pointing left and right, and a "Now" button. The main area displays a timeline of changes for the role "inspector". There are three visible change entries:

- 17th April 2016 7:49:09 PM: This entry has a circled "1" and a "Change" link.
- 21st August 2016 4:05:57 PM: This entry has a circled "1" and a "Change" link.
- 22nd August 2016 9:06:07 PM: This entry has a circled "1" and a "Change" link.

Below the timeline, there is a section titled "Configuration Details" with a "View Details" link. The details listed are:

Amazon Resource Name	arn:aws:iam::336580663284:role/inspector	Role Name	inspector
Resource type	AWS::IAM::Role	Trust Relationships	Document
Resource ID	AROAJIMX2KEEQRW57LCCA	Inline Policy Details	oneClick_inspector_1447334619937 oneClick_inspector_1471762879566 oneClick_inspector_1471867256220
Availability zone	Not Applicable		
Created on	November 12, 2015 10:23:51 PM		

アジェンダ

- IAMの概要
- IAMによる認証 (Authentication)
- IAMによる権限設定 (Authorization)
- IAMによる監査 (Audit)
- AWS Security Token ServiceとIAMロール
- IAMによるFederation
- まとめ



IAMロールとは？

- AWSサービスやアプリケーション等、エンティティに対してAWS操作権限を付与するための仕組み
 - 例えば実行するアプリケーションにロールを付与する事で、そのアプリケーションからAWSを操作出来るようになる
- IAMユーザーやグループには紐付かない
- 設定項目は、ロール名とIAMポリシー
- EC2ほか、Beanstalk, Data Pipelineなどでも利用



EC2にはIAMロールを利用

EC2のようなAWSサービスに対してAWS操作権限を付与するための仕組み。

IAMユーザーの認証情報のようなものをOS/アプリケーション側に持たせる必要がなく、認証情報の漏えいリスクを低減可能。 IAMロールによる認証情報はAWSが自動的にローテーション。

IAMロール利用の利点

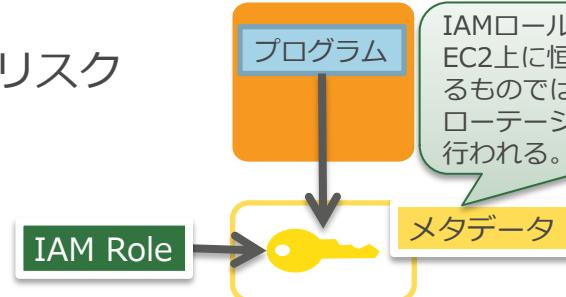
- EC2上のアクセスキーの管理が容易
- 認証情報はSTS(Security Token Service)で生成
- 自動的に認証情報のローテーションが行われる
- EC2上のアプリケーションに最低権限を与えることに適している
- AWS SDK及びAWS CLIのサポート
- IAMユーザーの認証情報を外部に漏えいしてしまうリスクを低減させる

IAMユーザー利用



認証情報をEC2内に持たせる。認証情報の保管・ローテーション等の検討が必要

IAMロール利用



IAMロールによる権限はEC2上に恒久的に保管されるものではなくテンポラリ。ローテーション等は自動で行われる。

メタデータからの認証情報取得

- IAM Roleを設定したEC2インスタンス内から取得

```
curl http://169.254.169.254/latest/meta-data/iam/security-credentials/EC2_Admin
```

```
{  
    "Code" : "Success",  
    "LastUpdated" : "2016-09-18T05:15:39Z",  
    "Type" : "AWS-HMAC",  
    "AccessKeyId" : "ASIAJY2YJ5S2ZYK25BLQ",  
    "SecretAccessKey" : "Kp1NbIz7mov/4ln7GLu8dqvN5GztXXXXXXXXXXXXXX",  
    "Token" : "AQoDYXdzELP//////////wEa0ANmvPx2CpTfOWjuPSMQ+/XXXXXXXXXXXXXX",  
    "Expiration" : "Expiration" : "2016-09-18T11:27:40Z"  
}
```



Role名

有効期限

STSのセッショントークン

- AWS SDKを利用する場合、認証情報取得と有効期限切れ前の再取得を自動的に実施可能

```
AWSCredentials credentials =  
    new BasicAWSCredentials("アクセスキー","シークレットキーID");  
AmazonEC2 ec2 = new AmazonEC2Client(credentials);  
ec2.describeInstances();
```



IAM Role利用後

```
AmazonEC2 ec2 = new AmazonEC2Client();"  
ec2.describeInstances();
```

- AWS CLIはIAM Roleに対応済み
 - <http://aws.amazon.com/jp/cli/>

IAM Role適用のインスタンス上では、認証情報の設定が不要

AWS Security Token Service(STS)とは

- 一時的に利用するトークンを発行するサービス
- 動的にIAMユーザーを作成し、ポリシーを適用できる
- IAM Role for EC2は、このSTSを利用

Temporary Security Credentialsとは

- AWSに対する、一時的な認証情報を生成する仕組み
 - 期限付きの認証情報（認証チケット）
- ユーザーに対して、以下の3つのキーを発行
 - アクセスキー：(ASIAJTNDEWXXXXXXX)
 - シークレットアクセスキー：(HQUdrMFbMpOHJ3d+Y49SOXXXXXXX)
 - セッショントークン (AQoDYXdzEHQakAOAEHxwpf/ozF73gmp9vZDWDPkgFnzwSG/3ztBw9Z4IUsINNn503+3SeN0nwI3wcdLR8y8Ulv9cnksMrBGjRVrJl2xg+/CRnI9nJ1tteHp6yso3sP0BVvnxLpNwyIUpHrcTHt+8v2P6Y9/VX2zI8Hc/cy6La0r1/GuiHb9NEwqt6VIgjPWCZzHXzX8XsUObKhMnAUkY2IdTMrNKXcqVk8VbC6BNTqWsMIIIfQPz9fDjKK1ifAFmHVSWvUxio94n+ebXXpy1NuHnt5JEGV34VPLMsrpZ86b+eulKNE1suoQ8TM5E1O66rYwizkq6w+cJovUnMxg6ESASBvolsrEioLiP+SE7cX1i8gRrSG9/KT59GYTIhTzStjjFroCAqZu4KYplGUMCDI1g0twrdXeymsu3GG70Qwu0wSi3WjkW8VPiajahJXCEgp6gIgXElwkrBO01H5Y9NNDEyQaq8ocOGBPVRu+DS9LMs9SHASXimnnVeIN+1FVkXXXXXXXXXXXXXXXXXXXXXX)



IAMの権限階層

AWSアカウント

- ・ 全てのサービスへのアクセス
- ・ 課金設定へのアクセス
- ・ 管理コンソールおよびAPIへのアクセス
- ・ カスタマーサポートへのアクセス

DO NOT USE
after initial set-up



ドアキー

IAMユーザー

- ・ 許可されたサービスへのアクセス
- ・ 管理コンソールおよびAPIへのアクセス
- ・ カスタマーサポートへのアクセス



従業員
バッジ

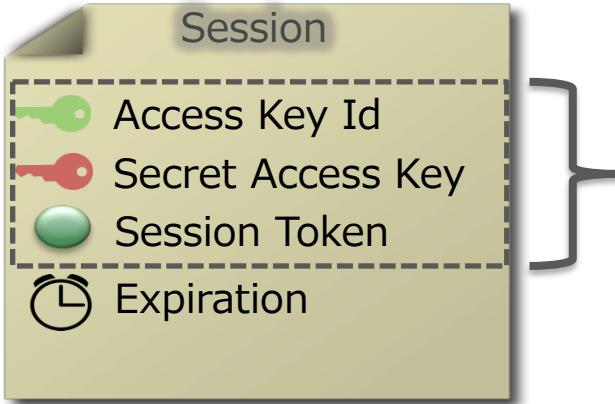
Temporary Security Credentials / IAM Roles

- ・ 許可されたサービスへの一時的なアクセス
- ・ 管理コンソールおよびAPIへのアクセス

ホテルキー



認証情報を取得する方法



Temporary
Security
Credentials

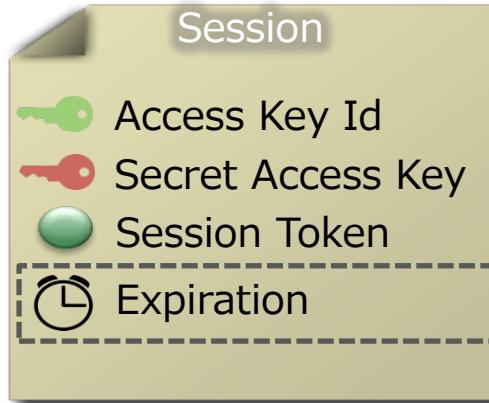


- Self-sessions (GetSessionToken)
- Federated sessions (GetFederationToken)
- Assumed-role sessions
 - AssumeRole
 - AssumeRoleWithWebIdentity
 - AssumeRoleWithSAML

認証情報取得のためのAPI

STSで利用できるAPI Action	概要
GetSessionToken	自身で利用するIAMユーザーのtemporary security credentialsを取得するためのアクション
GetFederationToken	認証を受けたFederatedユーザーのtemporary security credentialsを取得するためのアクション
AssumeRole	既存のIAMユーザーの認証情報を用いて、IAM Roleのtemporary security credentialsを取得するためのアクション。
AssumeRoleWithWebIdentity	AmazonやFacebook、Googleによる承認情報を使用してロールを引き受け、temporary security credentialsを取得するためのアクション
AssumeRoleWithSAML	IdPによる認証とSAMLのアサーションをAWSにポストすることでロールを引き受けtemporary security credentialsを取得するためのアクション

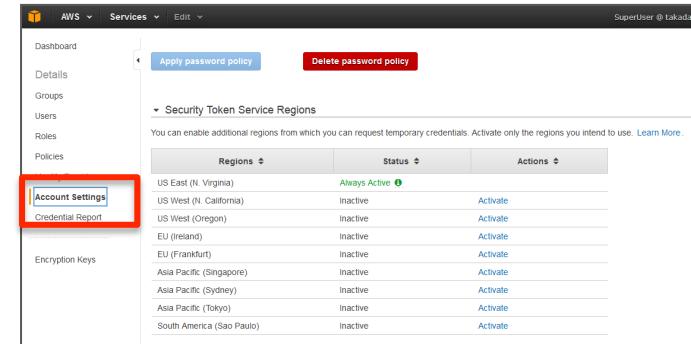
認証情報の有効期限



- トークンのタイプにより有効期限は様々 [Min/Max/Default]
 - Self (Account) [15 min / 60 min / 60 min]
 - Self (IAM User) [15 min / 36 hrs / 12 hrs]
 - Federated [15 min / 36 hrs / 12 hrs]
 - Assumed-role [15 min / 60 min / 60 min]
- 発行したチケットは延長や期間短縮は出来ない
- 即座にアクセス制御したい場合は、発行に使用したIAMユーザー或はIAMロールの権限を変更する

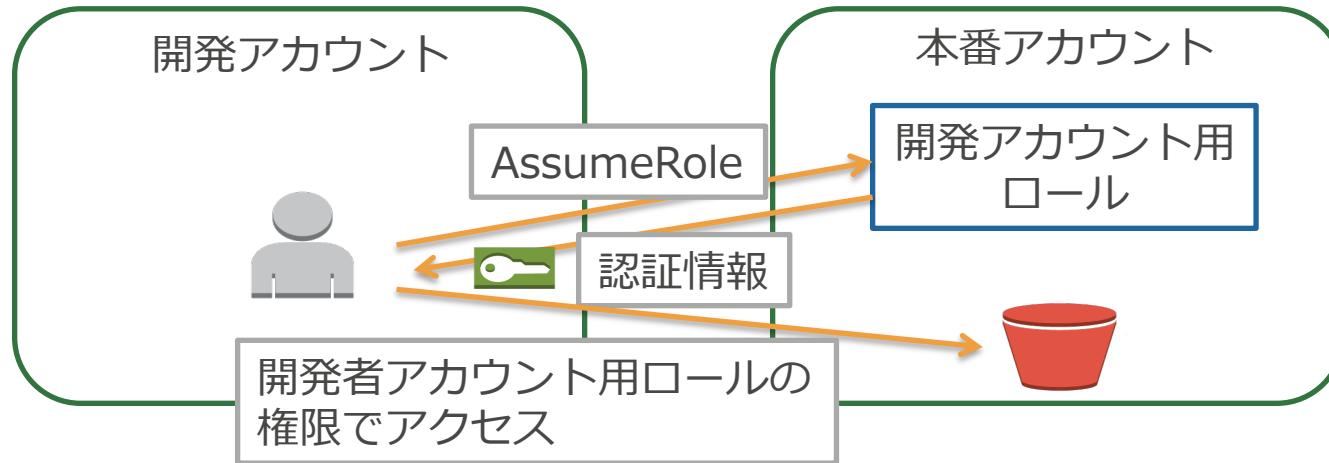
AWS STS in all AWS regions

- STSのエンドポイントが全リージョンに拡張
- デフォルトではSTSはグローバルサービスとして利用
 - 単一エンドポイント : <https://sts.amazonaws.com>
- IAMのAccount Settingsより各リージョンでSTS機能をアクティベート可能
 - レイテンシーの低減
 - 冗長性の構築
- 有効化したリージョンでのCloudTrailの使用を忘れない

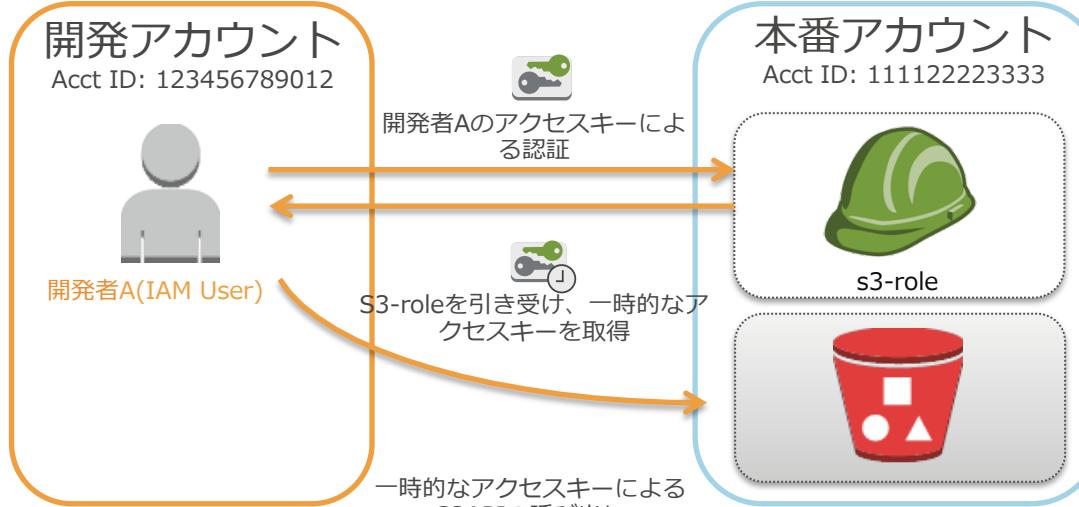


ユースケース: IAMロールによるクロスアカウントアクセス

- あるアカウントのユーザーに別のアカウントのIAMロールに紐づける機能
- 例えば開発アカウントを使って、本番環境のS3データを更新するようなケースで利用



IAMロールによるクロスアカウントアクセスの動作



s3-roleに付与されているポリシー

```
{ "Statement": [ { "Effect": "Allow", "Action": "s3:*", "Resource": "*" } ] }
```

```
{ "Statement": [ { "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "arn:aws:iam::111122223333:role/s3-role" } ] }
```

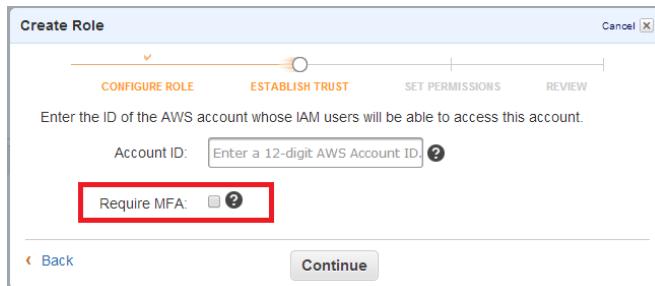
本番アカウントのs3-roleの引き受けを許可するポリシーを開発者Aに設定

```
{ "Statement": [ { "Effect": "Allow", "Principal": {"AWS": "arn:aws:iam::123456789012:root"}, "Action": "sts:AssumeRole" } ] }
```

S3-roleを誰が引き受けられるか定義したポリシーをs3-roleに設定

クロスアカウントアクセスのためのMFA保護

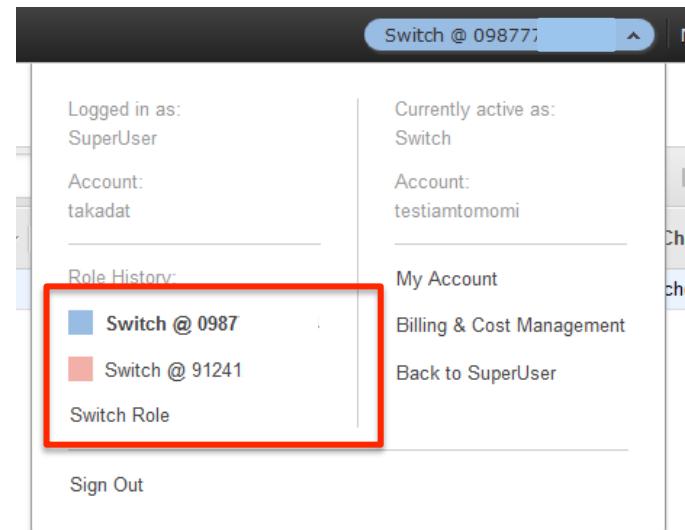
- AWSアカウント間でのアクセスのためのMFA保護を追加する機能
- AWSマネージメントコンソールでroleを作成する際に、Require MFAのチェックボックスを選択することで設定可能
- MFA認証されたユーザーのみが認証情報を受けとることが可能に
 - AssumeRole
 - GetSessionToken



```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {"AWS": "Parent-Account-ID"},  
      "Action": "sts:AssumeRole",  
      "Condition": {"Null": {"aws:MultiFactorAuthAge": false}}  
    }  
  ]  
}
```

Switch Role

- IAMユーザーからクロスアカウントアクセス用IAMロールにコンソールから切替が可能
 - 必ずしも別アカウントである必要はなく、同じアカウントでもOK
- 必要な時のみIAMユーザーの権限を“昇格”させる
 - IAMユーザーには読み取り権限のみを付与
 - IAMロールには更新権限を付与



<https://aws.amazon.com/blogs/aws/new-cross-account-access-in-the-aws-management-console/>

アジェンダ

- IAMの概要
- IAMによる認証 (Authentication)
- IAMによる権限設定 (Authorization)
- IAMによる監査 (Audit)
- AWS Security Token ServiceとIAMロール
- IAMによるFederation
- まとめ



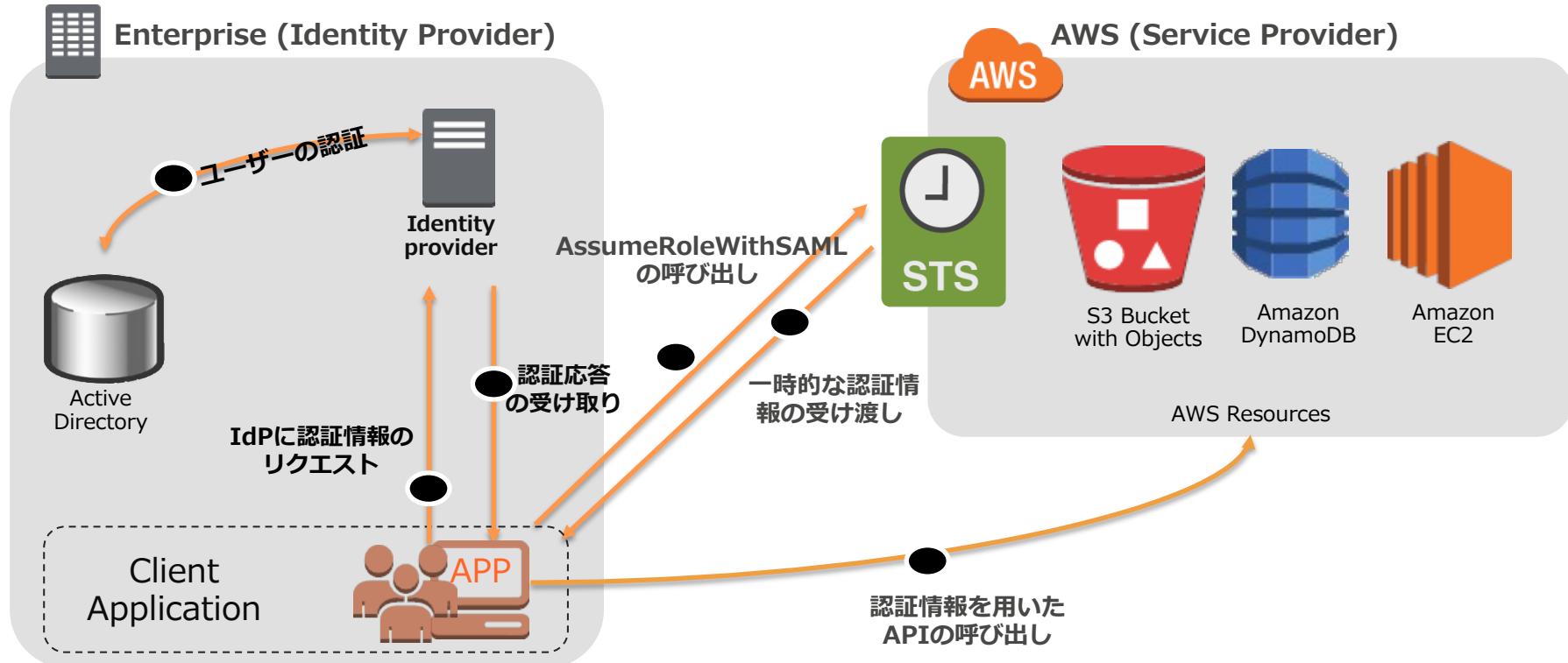
Identity Federation (ID連携) とは

- 企業・組織の認証機能と、AWSの認証を紐づける機能
- 例えばLDAP認証したユーザーに対してS3のアクセス権をつける、といった連携が可能
- 認証したユーザーごとにTemporary Security Credentials (一時的なアクセスキー) を発行
- IAMは、OpenID ConnectまたはSAML 2.0 (Security Assertion Markup Language 2.0) と互換性のある IdP をサポート

ユースケース: SAML2.0ベースのFederation

- SAML2.0を使用した IDフェデレーション
- 組織内の全員についてIAMユーザーを作成しなくても、ユーザーは AWSを利用可能
- 組織で生成した SAMLアサーションを認証レスポンスの一部として使用し、一時的セキュリティ認証情報を取得
- ユーザーは一時的セキュリティ認証情報でAWSのリソースにアクセス

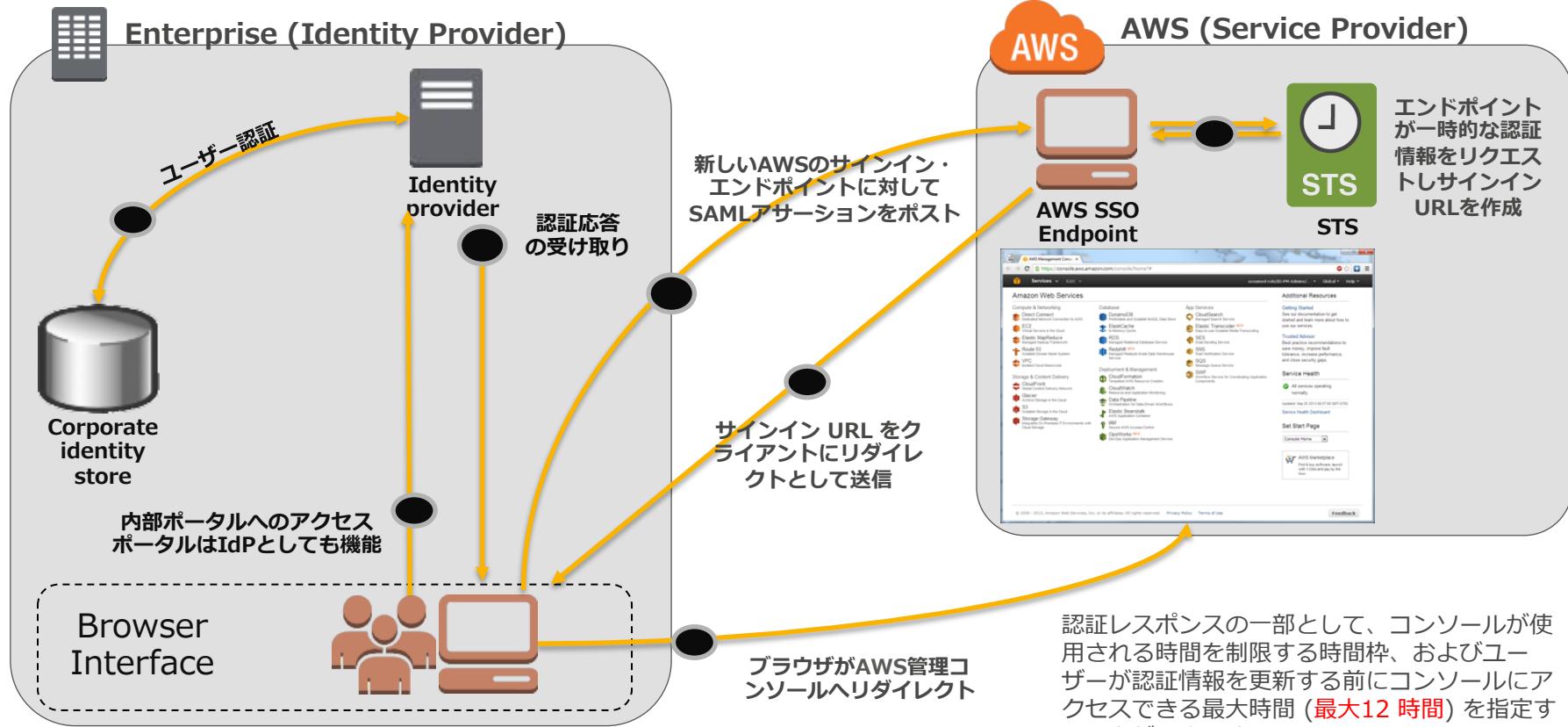
SAML2.0ベースのFederation動作例



ユースケース: SAML2.0によるSSO Federation

- SAML 2.0互換IdPおよびIAMロールを使用した管理コンソールへのフェデレーションアクセス
- AssumeRoleWithSAML APIを直接呼び出す代わりに、AWS SSOエンドポイントを使用
- エンドポイントはユーザーの代わりにAPIを呼び出し、URL を返すと、それによってユーザーのブラウザーがAWSマネジメントコンソールへ自動的にリダイレクト

SAMLによるConsole Federationの動作例

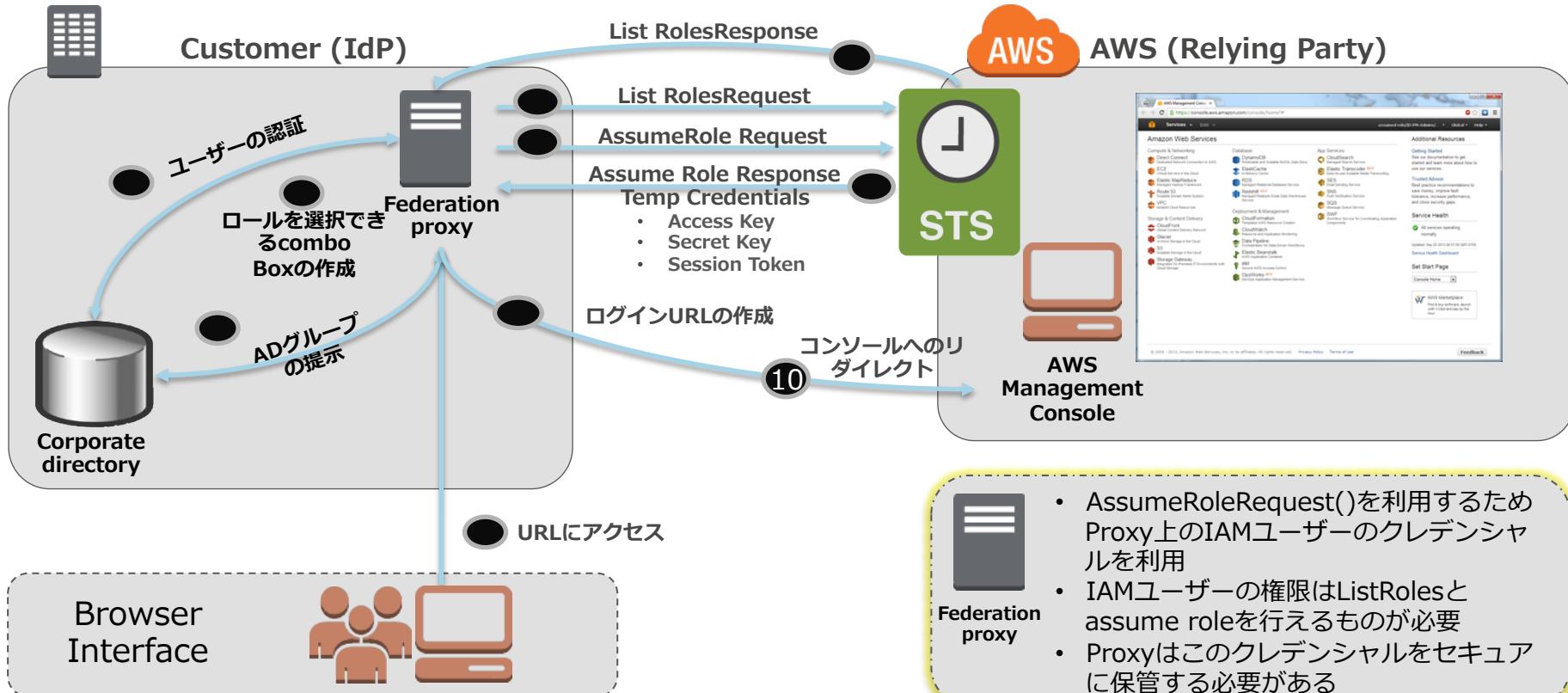


ユースケース: Console Federation

(Sample - <http://aws.amazon.com/code/4001165270590826>)

- 既存のIdPによる管理コンソールへのシングルサインオン
- STSより一時的な認証情報を取得するためのカスタムフェデレーションブローカーを利用
- AssumeRole APIの利用

Console Federationの動作例



Console Federationのメリット

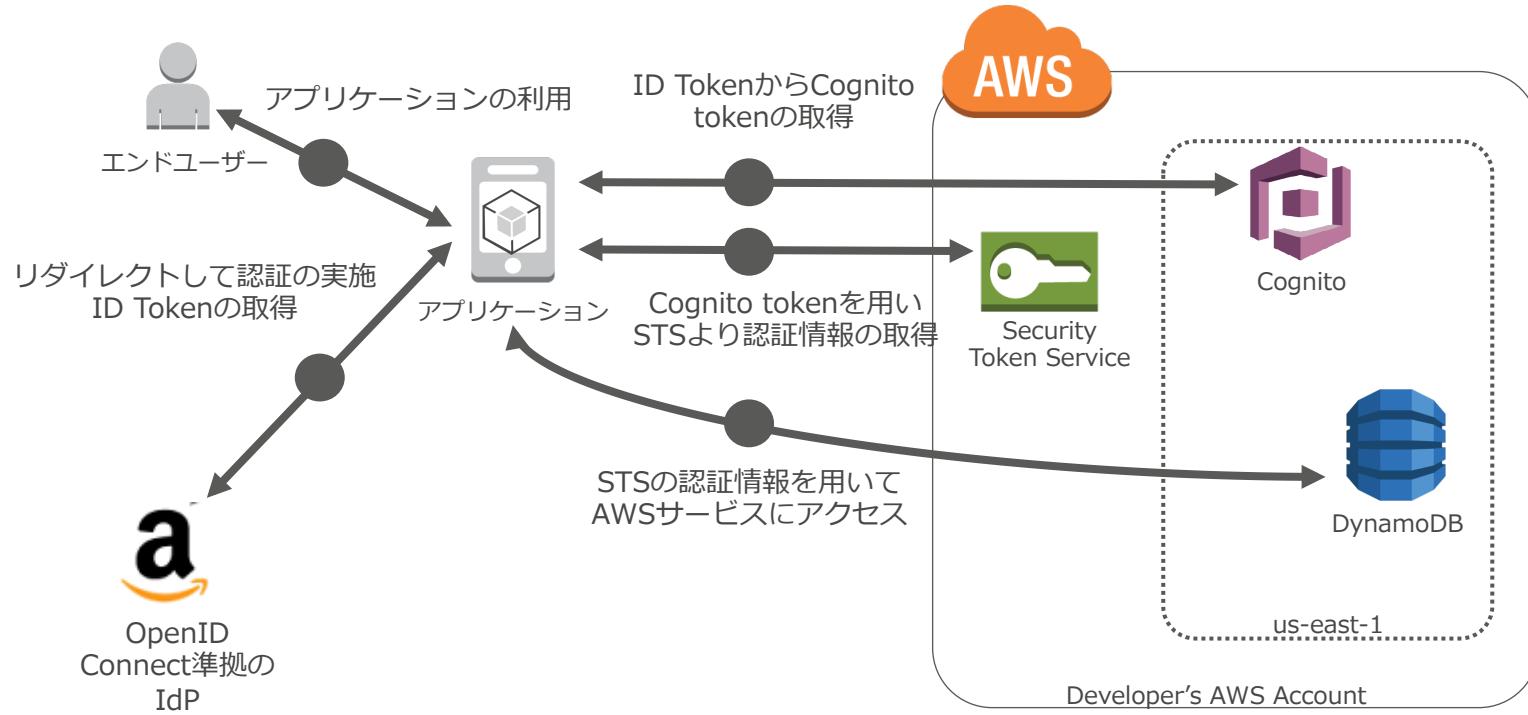
- アカウント管理が統合され、リスクが低減する
- 既存のユーザ情報をそのまま利用
- 既存の権限ベースでの管理が可能
- 既存と同様のポリシーの利用が可能
 - アカウントロックポリシーや、パスワード管理ポリシー
- 入退社など一元的な管理が可能
- イントラネットからのみアクセス可能なログイン画面

ユースケース: Web Identity Federation

- モバイルアプリから一時的なAWSセキュリティ認証情報を必要に応じて動的にリクエスト
- 認証を確認するサーバが不要
 - 例えばスマートフォンアプリとS3だけでシステムが作成可能
- 現在Google,Facebook,Amazon(Login with Amazon), twitter, Amazon Cognito及びOIDC準拠のIdPに対応



モバイルアプリへのAmazon Cognitoの使用例



https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_roles_providers_oidc_cognito.html

Federation/SSOを提供するパートナーソリューション

<http://aws.amazon.com/jp/iam/partners/>



One Global Identity to Drive Business in a Distributed World



アジェンダ

- IAMの概要
- IAMによる認証 (Authentication)
- IAMによる権限設定 (Authorization)
- IAMによる監査 (Audit)
- AWS Security Token ServiceとIAMロール
- IAMによるFederation
- まとめ



IAMのベストプラクティス

1. AWS アカウント（ルート）のアクセスキーをロックする
2. 個々の IAM ユーザーを作成する
3. IAM ユーザーへのアクセス許可を割り当てるためにグループを使います。
4. 最小限の特権を認める。
5. ユーザーのために強度の高いパスワードポリシーを設定する。
6. 特権ユーザーに対して、MFA を有効化する。
7. Amazon EC2 インスタンスで作動するアプリケーションに対し、ロールを使用する。
8. 認証情報を共有するのではなく、ロールを使って委託する。
9. 認証情報を定期的にローテーションする。
10. 不要な認証情報の削除
11. 追加セキュリティに対するポリシー条件を使用する。
12. AWS アカウントのアクティビティの監視
13. IAM ベストプラクティスについてのビデオ説明。

まとめ

- IAMを利用してすることで、よりセキュアにAWSサービスを利用できます
 - 権限を適切に設定することで、セキュリティが向上し、オペレーションミスも低減できます
- STSをうまく利用すると、AWSサービスをアプリケーションやモバイルから直接扱えます
 - サーバコストの削減が可能
- IAM自体には利用料が必要ありません
 - 積極的に活用を！

追加のリソース

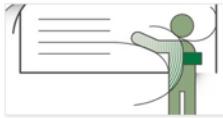
- IAMドキュメント群
 - <http://aws.amazon.com/jp/documentation/iam/>
- IAMベストプラクティス
 - <http://docs.aws.amazon.com/IAM/latest/UserGuide/IAMBestPractices.html>
- AWS Security Blog
 - <http://blogs.aws.amazon.com/security/>

オンラインセミナー資料の配置場所

- AWS クラウドサービス活用資料集
 - <http://aws.amazon.com/jp/aws-jp-introduction/>

日本語資料のカテゴリー一覧

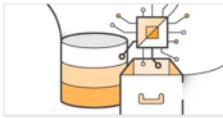
本資料集では、この利便性を皆様に活用していただけるよう、トレーニング、ソリューション/事例、プロダクト別、セキュリティ・コンプライアンス、その他という5つのカテゴリーで資料をご用意いたしております。



トレーニング資料



ソリューション・事例紹介資料



製品・サービス別資料

はじめてAWSをご利用いただくお客様向けに、AWSの概要、アカウント作成に関するご案内をいたします。

実際に他のお客様がどのようにAWSをご活用いただいているかをご覧いただける参考資料をご覧いただけます。

無料オンラインセミナー「AWS Black Belt Tech Webinar」や各種セミナーで紹介された、ソリューションアーキテクトによる各サービスの解説資料をご覧いただけます。

- AWS Solutions Architect ブログ
 - 最新の情報、セミナー中のQ&A等が掲載されています
 - <http://aws.typepad.com/sajp/>

公式Twitter/Facebook AWSの最新情報をお届けします



@awscloud_jp



検索

もしくは
<http://on.fb.me/1vR8yWm>

最新技術情報、イベント情報、お役立ち情報、
お得なキャンペーン情報などを日々更新しています！

AWSの導入、お問い合わせのご相談

- AWSクラウド導入に関するご質問、お見積り、資料請求をご希望のお客様は、以下のリンクよりお気軽にご相談ください

<https://aws.amazon.com/jp/contact-us/aws-sales/>

The screenshot shows a web form titled "日本担当チームへのお問い合わせ" (Inquiry to Japan Support Team). On the left, there is a sidebar with links: "お問い合わせ" (Inquiry), "日本担当チームへのお問い合わせ" (selected), "関連リンク" (Related Links), and "フォーラム" (Forum). The main content area has a heading "日本担当チームへのお問い合わせ" and text explaining that inquiries about AWS Cloud adoption can be made via this form. It also specifies that for sales inquiries, contact the Japan office directly. Below this, there is a note about contacting for account-related questions. The form includes fields for "姓*" (Last Name*) and "名*" (First Name*), both represented by input boxes.