

# 初めてのAWS Session Manager (SSM)

AWS 初心者 session-manager

## 概要

---

いまさらですが、先日開催されたJAWS DAYS 2019でSSH使わずにEC2に接続できるSession Managerを知り、現状自社サービスにおいてもSSH管理が課題になっていましたので、さっそく試してみました

いつ、だれが、何をしたのはすべてログ（実行結果も含めて）に保存されるので、問題発生時にトレース用としても使えます！

設定自体は非常に簡単なので、どんなものなのかを試してみたい方は是非試してみてる価値はあります！

※以下の手順は新規インスタンスにSSM用ロールを追加していますが、既存インスタンスに追加する場合は[こちら](#)を参照ください

※すぐに試してみたい方向けの内容なので権限設定等はガバガバなのでご注意ください！

# 手順

## ロールの作成

### 1. 「IAM」 - 「ロール」 - 「ロール作成」

The screenshot shows the AWS IAM console interface. On the left sidebar, the 'Roles' link is highlighted with a red box. The main content area displays the 'IAM Role Overview' page. At the bottom of the main content area, the 'Create Role' button is highlighted with a red box. Below the buttons is a search bar and a table header for roles.

**IAM の検索**

ダッシュボード  
グループ  
ユーザー  
**ロール**  
ポリシー  
ID プロバイダー  
アカウント設定  
認証情報レポート

暗号化キー

**ロール**

**IAM ロールの概要**

IAM ロールは信頼できるエンティティにアクセス権限を付与する安全な方法です。エンティティの例には次のようなものがあります。

- 別のアカウントの IAM ユーザー
- AWS のリソースでアクションを実行する必要がある、EC2 インスタンスで実行されるアプリケーションコード
- 機能を提供するためにお客様のアカウントのリソースを操作する必要がある AWS のサービス
- SAML を使用した ID フェデレーションを使用する企業内ディレクトリからのユーザー

IAM ロールは短期間のみ有効なキーを発行し、より安全にアクセス権限を付与します。

**その他のリソース:**

- IAM ロールのよくある質問
- IAM ロールのドキュメント
- チュートリアル: クロスアカウントアクセスのセットアップ
- ロールの一般的なシナリオ

**ロールの作成**    ロールの削除

Q 検索

ロール名 ▼	説明	信頼されたエンティティ
--------	----	-------------

## 2. 「AWSサービス」 - 「EC2」 ロールを選択

### ロールの作成

1 2 3 4

信頼されたエンティティの種類を選択

**AWS サービス**  
EC2、Lambda、およびその他

**別の AWS アカウント**  
お客様またはサードパーティーに属しています

**ウェブ ID**  
Cognito または任意の OpenID プロバイダ

**SAML 2.0 フェデレーション**  
企業ディレクトリ

AWS のサービスによるアクションの代行を許可します。 [詳細はこちら](#)

このロールを使用するサービスを選択

**EC2**  
Allows EC2 instances to call AWS services on your behalf.

**Lambda**  
Allows Lambda functions to call AWS services on your behalf.

API Gateway	CodeBuild	EKS	Lambda	SMS
AWS Backup	CodeDeploy	EMR	Lex	SNS

## 3. ポリシーから「AmazonEC2RoleforSSM」を選択

権限の絞り込みをしたい場合は、「ポリシーの作成」から作成してください

### ロールの作成






1 2 3 4

▼ Attach アクセス権限ポリシー

新しいロールにアタッチするポリシーを 1 つ以上選択します。

**ポリシーの作成**

**ポリシーのフィルタ**  8 件の結果を表示中

	ポリシー名 ▼	次として使用	説明
<input checked="" type="checkbox"/>	 AmazonEC2RoleforSSM	Permissions policy (2)	Default policy for Amazon EC2 Role for ...
<input type="checkbox"/>	 AmazonSSMAutomationApproverAccess	なし	Provides access to view automation exe...
<input type="checkbox"/>	 AmazonSSMAutomationRole	なし	Provides permissions for EC2 Automatio...
<input type="checkbox"/>	 AmazonSSMFullAccess	なし	Provides full access to Amazon SSM.
<input type="checkbox"/>	 AmazonSSMMaintenanceWindowRole	なし	Service Role to be used for EC2 Mainten...

## 4. タグやロール名を付けて作成

# EC2の作成

Session Managerからコントロールするためには、EC2に`ssm-agent`がインストールされている必要があります。最新のAmazon Linux 2のAMIであれば最初から入っています

1. インスタンスを新規作成し、インスタンスの詳細の設定で作成したIAMロールを選択すればOK！

1. AMI の選択   2. インスタンスタイプの選択   3. インスタンスの設定   4. ストレージの追加   5. タグの追加   6. セキュリティグループの設定   7. 確認

## 手順 3: インスタンスの詳細の設定

要件に合わせてインスタンスを設定します。同じ AMI からの複数インスタンス作成や、より低料金を実現するためのスポットインスタンスのリクエスト、インプができます。

インスタンス数	①	1	Auto Scaling グループに作成する	①
購入のオプション	①	<input type="checkbox"/> スポットインスタンスのリクエスト		
ネットワーク	①	████████ (デフォルト)	🔄	新しい VPC の作成
サブネット	①	優先順位なし (アベイラビリティゾーンのデフォルト)		新しいサブネットの作成
自動割り当てパブリック IP	①	サブネット設定を使用 (有効)		
配置グループ	①	<input type="checkbox"/> インスタンスをプレースメントグループに追加します。		
キャパシティの予約	①	開く	🔄	新しいキャパシティ予約の作成
IAM ロール	①	SSM_Test	🔄	新しい IAM ロールの作成
シャットダウン動作	①	停止		
削除保護の有効化	①	<input type="checkbox"/> 誤った削除から保護します		

# Session Manager

## 1. サービス「Systems Manager」 - 「セッションマネージャー」 - 「セッションの開始」

※実行中のセッションがあれば、セッションマネージャーの一覧に表示される

## 2. 前述で作成したEC2インスタンスを選択し、「セッションの開始」

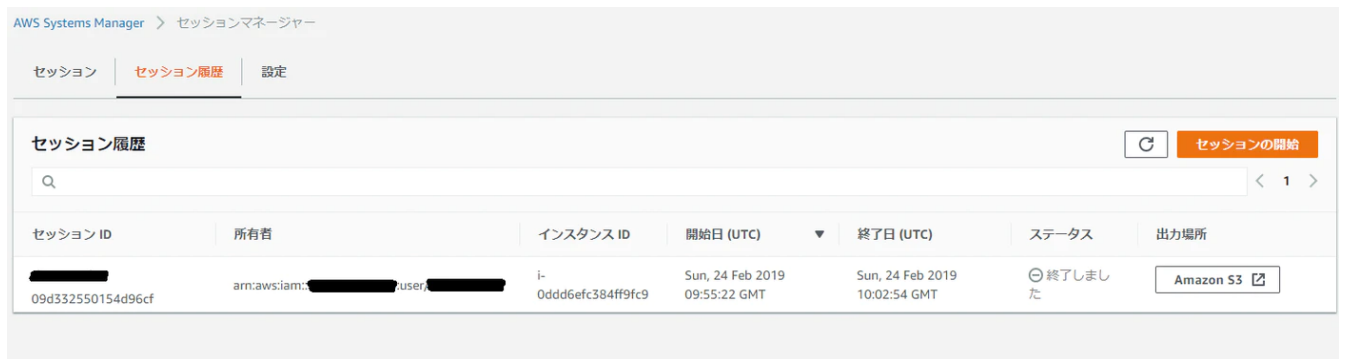


## 3. 新しいタブにターミナルが立ち上がる（若干動作がもっさり）

接続ユーザはssm-userになるが、sudo実行が許可されている

※参考：[小ネタ]新機能Session Managerで使うssm-userの権限が気になった話

4. ターミナルの「終了」を押下するとセッションが終了され、セッション履歴が保存されます
- 操作ログをS3出力設定していれば、S3の指定していたバケットにログファイルが出力されます



セッション履歴						
セッション ID	所有者	インスタンス ID	開始日 (UTC)	終了日 (UTC)	ステータス	出力場所
09d332550154d96cf	arn:aws:iam::[redacted]:user/[redacted]	i-0ddd6efc384ff9fc9	Sun, 24 Feb 2019 09:55:22 GMT	Sun, 24 Feb 2019 10:02:54 GMT	☹ 終了しました	Amazon S3

## 操作ログ（サンプル）

以下のように標準出力された内容がすべてログファイルに出力されます

```
ssm-log
```

```
Script started on 2019-02-24 10:00:54+0000
```

```
[?1034hsh-4.2# /usr/bin/ssm-session-logger /var/lib/amazon/ssm-session/orchestration/xxxxx-xxxxxxx/Standard_Stream/ipcTempFile.log false
```

```
Error occurred fetching the seelog config file path: open /etc/seelog.conf: No such file or directory
Initializing new seelog logger
```

## New Seelog Logger Creation Complete

```
sh-4.2$ ls -la
```

```
total 127096
```

```
dr-xr-xr-x  2 root root      24576 Feb 24 09:54 .
```

```
drwxr-xr-x 13 root root      155 Jan 14 18:29 ..
```

```
-rwxr-xr-x  1 root root    41344 Jul 31  2018 [
```

```
-rwxr-xr-x  1 root root   107744 Sep 12 22:17 a2p
```

```
-rwxr-xr-x  1 root root    28712 Aug  2  2018 ac
```

```
-rwxr-xr-x  1 root root    28976 Jan  3 20:00 addr2line
```

```
～中略～
```

```
-rwxr-xr-x  2 root root   189440 Jul 27  2018 zipinfo
```

```
-rwxr-xr-x  1 root root    95896 Aug  1  2018 zipnote
```

```
-rwxr-xr-x  1 root root    99968 Aug  1  2018 zipsplit
```

```
-rwxr-xr-x  1 root root     2041 Jul 27  2018 zless
```

```
-rwxr-xr-x  1 root root          2859 Jul 27  2018 zmore

-rwxr-xr-x  1 root root          5343 Jul 27  2018 znew

lrwxrwxrwx  1 root root          6 Jan 14 18:29 zsoelim -> so

sh-4.2$ sh-4.2# exit
exit
```

Script done on 2019-02-24 10:02:40+0000

## 注意点

---

SSMで接続すると `/var/log/ssm/` 配下にSSM接続時の操作ログが残ります。

なので、このログでディスク容量が圧迫される可能性もあるので、ログサイズとローテーションの設定を必ずしておきましょう！

[https://docs.aws.amazon.com/ja\\_jp/systems-manager/latest/userguide/monitoring-ssm-agent.html](https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/monitoring-ssm-agent.html)