



プライベートサブネットのインスタンスに SSH? EC2 Instance Connect Endpoint を試してみる！

Hiroki Yamazaki

Amazon Web Services Japan G.K.
Solutions Architect

2023/09/06

山崎 宏紀 (Yamazaki Hiroki)

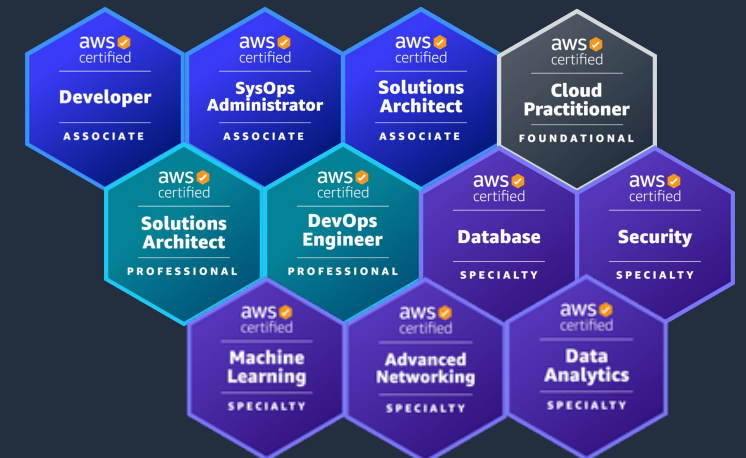
Amazon Web Services Japan ソリューションアーキテクト
ソフトウェア・SaaS を開発されている皆様をご支援します！

得意分野:

- 組合せ最適化, 離散アルゴリズム
- Infrastructure as Code, Serverless

好きな AWS サービス: AWS CDK, AWS Step Functions

趣味: 将棋, ボードゲーム, ボルダリング



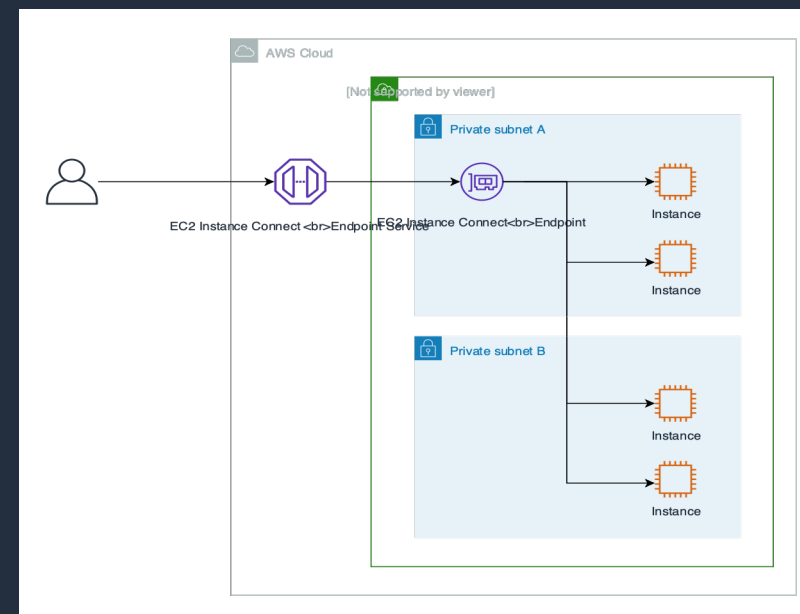
Agenda

- EC2 Instance Connect Endpoint (EIC Endpoint) 概要
- EC2 Instance Connect とは？
- Session Manager との違いを確認
- デモ
- おわりに
- Appendix

EC2 Instance Connect Endpoint (EIC Endpoint) 概要

- 2023/06: Public IP を持たないインスタンスに対し SSH/RDP 接続ができる **EC2 Instance Connect Endpoint** が発表
- 従来、インスタンスへの SSH/RDP での接続には Public IP や踏み台インスタンスを用意する必要があった

- EIC Endpoint の使用料金は**無料** (別途データ転送料は発生)
- IAM・セキュリティグループによる**アクセス制御**
- AWS CloudTrail による**監査**
- インスタンスのセキュリティグループでは EIC Endpoint からの SSH/RDP を許可



EC2 Instance Connect とは？

- インスタンスに **SSH** でアクセスするための機能
- SSH キーを自身で **共有・管理する必要なし**
- マネジメントコンソール・CLI **両対応**
- 仕組み
 - Instance Connect API で SSH 公開鍵をインスタンスメタデータにプッシュ
 - インスタンスメタデータから取得した公開鍵でユーザーを認証

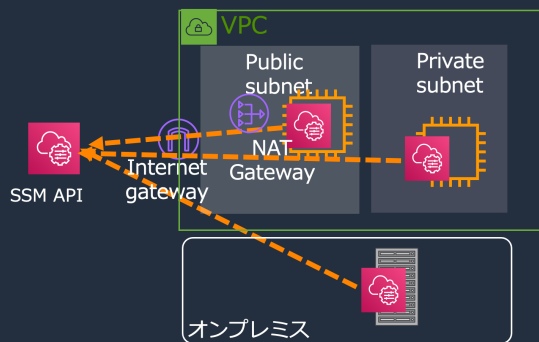
The screenshot shows the AWS Management Console interface for connecting to an EC2 instance. The page title is "インスタンスに接続" (Connect to Instance). Below the title, there are four tabs: "EC2 Instance Connect" (selected), "セッションマネージャー", "SSH クライアント", and "EC2 シリアルコンソール". The "EC2 Instance Connect" tab is active, showing the "接続タイプ" (Connection Type) section with two radio button options: "EC2 Instance Connect を使用して接続する" (selected) and "EC2 Instance Connect エンドポイントを使用して接続する". Below this, there are fields for "パブリック IP アドレス" (Public IP Address), "ユーザー名" (Username) with the value "ec2-user", and a "接続" (Connect) button. A note at the bottom states: "注意: ほとんどの場合はデフォルトのユーザー名 ec2-user に間違いはありませんが、AMI の使用手順を読んで AMI の所有者がデフォルトの AMI ユーザー名を変更していないか確認してください。"

Session Manager との違いを確認

- インスタンスにアクセスするための **AWS Systems Manager** の一機能
- セキュリティグループでの **Inbound 許可不要**
- セッション中のコマンドと出力を記録可能
- インスタンス内 SSM Agent から SSM API への **接続経路**が必要

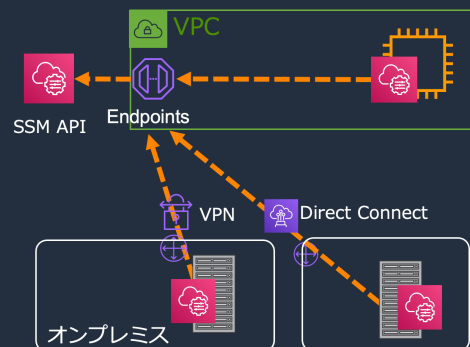
1, インターネット経由

- パブリックサブネットや NAT Gateway を使用



2, VPC エンドポイント経由

- プライベートネットワークによる接続が可能
- オンプレミスからも AWS Direct Connect や VPN 経由で閉域網経由のアクセスが可能



Outbound 設定の構成例

The screenshot shows the AWS Management Console interface for Session Manager. The breadcrumb navigation is "EC2 > インスタンス > [Instance ID] > インスタンスに接続". The main heading is "インスタンスに接続 情報". Below the heading, there is a text block: "これらのオプションのいずれかを使用してインスタンス i-0f100b0660ac8ec9f (ec2-instance-connect-demo-prod/Instance) に接続する". There are three tabs: "EC2 Instance Connect", "セッションマネージャー" (selected), "SSH クライアント", and "EC2 シリアルコンソール". Under "セッションマネージャー", there is a section "Session Manager の使用:" with the following bullet points:

- Connect to your instance without SSH keys, a bastion host, or opening any inbound ports.
- セッションは AWS Key Management Service キーを使用してセキュア化されています。
- セッションのコマンドと詳細は、Amazon S3 バケットまたは CloudWatch Logs のロググループに記録できます。
- Configure sessions on the Session Manager [Preferences](#) page.

At the bottom right, there are two buttons: "キャンセル" and "接続".

デモ

おわりに

- Public IP や踏み台なしで EC2 インスタンスに SSH/RDP 接続できる **EC2 Instance Connect Endpoint** を紹介
- 利用料金は**無料**で IAM やセキュリティグループによる **アクセス制御**に対応
- 2023/08 時点のクォータ
 - VPC ごと・サブネットごとに1つまで
- Multi-AZ 構成を利用している場合は Session Manager と適切な使い分けを！

Appendix



EIC Endpoint と Session Manager の比較観点 (2023/08 時点)

- 費用
 - EIC Endpoint: 無料
 - Session Manager: 無料。ただし、Private Subnet 内のインスタンスで利用する場合 SSM API への接続経路として NAT Gateway や VPC Endpoint が必要
- 可用性
 - EIC Endpoint: クォータの制約上、単一 AZ にのみ作成可能
 - Session Manager: NAT Gateway/VPC Endpoint を接続経路として利用する場合、Multi-AZ 構成可能
- 動作環境
 - EIC Endpoint: Amazon Linux 2 全てのバージョン, Ubuntu 16.04 以降
 - Session Manager: AWS Systems Manager の対応状況に準拠