



【AWS Hands-on for Beginners】

Network 編 #1-1

AWS上にセキュアなプライベートネットワーク空間を作成

アマゾン ウェブ サービス ジャパン合同会社
パートナー ソリューション アーキテクト

江口 智 / Tomo Eguchi

(収録日: 2022/5/8)

自己紹介



- 名前: 江口 智
- 役割: Partner Solutions Architect
- 役割:
 - コンサルティングパートナー様の技術支援を担当
 - パートナー様のAWSビジネスを成功させることが私の喜び
- 好きな AWS サービス



Amazon VPC



AWS Direct Connect



AWS Transit Gateway

AWS Hands-on for Beginners とは



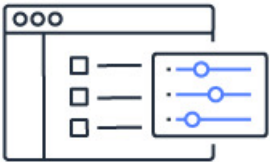
実際に手を動かしながら AWS の各サービスを学んでいただきます



初めてそのサービスを利用される方がメインターゲットです



好きな時間、好きな場所でご視聴いただけるオンデマンド形式



テーマごとに合計1～2時間の内容 & 細かい動画に分けて公開
スキマ時間の学習や、興味のある部分だけの視聴も可能

内容についての注意点

- 本資料では2022年5月8日収録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、資料とAWS公式ウェブサイトとで記載内容に相違があった場合、AWS公式ウェブサイトの記載を優先させていただきます。
- マネージメントコンソールについても、収録時点のものとなります。差異がある場合がございますので、ご注意ください。
- ハンズオンでは、AWS の各種サービスの利用、リソースの作成を行います。無料枠を超えるコースもございますが、その場合、ご利用料金が発生することをあらかじめご認識ください。
- 学習後のリソースの削除についても、お客様の責任でご実施いただくようお願いいたします。

本コースのゴール/前提条件・知識

- 本コースのゴール
 - Amazon VPC の基本を理解する
 - Amazon VPC を使ってAWS上にプライベートネットワーク空間を作成する
 - Amazon VPC とインターネットの接続をコントロールする方法を理解する
 - VPCエンドポイントを使ってAWSマネージドサービスに接続する方法を理解する
- 本コースの前提条件・知識
 - AWS アカウントをお持ちであること
 - ハンズオンの作業が同一AWSアカウントの他のリソースに影響が出る場合があります。
 - ハンズオン用にAWSアカウントを取得していただくことをオススメします。
 - TCP/IP、ルーティングといったネットワークの基礎知識をお持ちであること

このコースの Agenda

1. AWS

1. 前提知識の確認
2. AWSでのネットワークの考え方
3. 本ハンズオンの最終構成図

2. Amazon VPC ハンズオン

1. Amazon VPC ハンズオン① Amazon VPC の作成とインターネット接続環境の構築
2. Amazon VPC ハンズオン② ルートテーブルによる経路設定を理解する
3. Amazon VPC ハンズオン③ プライベートサブネットからインターネットへのアクセス方法
4. Amazon VPC ハンズオン④ VPC外サービスへの接続方法 - 1
5. Amazon VPC ハンズオン⑤ VPC外サービスへの接続方法 - 2

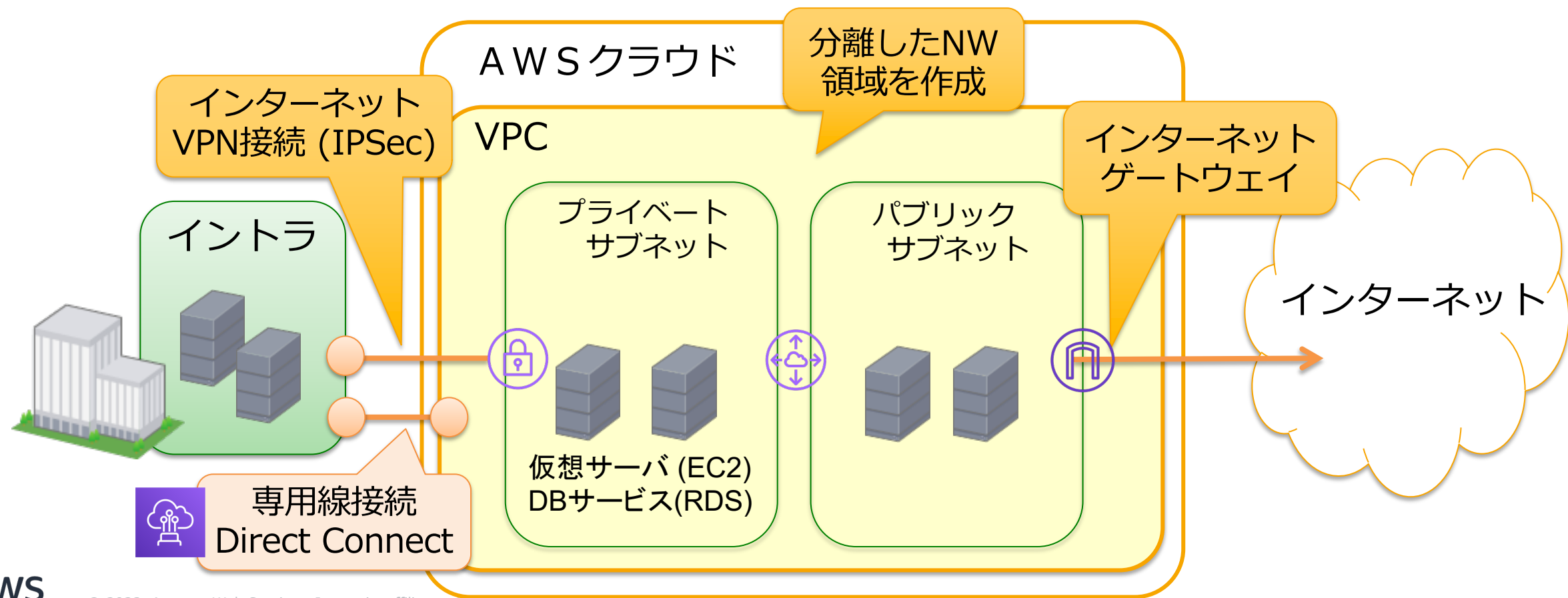
3. 本コースのまとめ



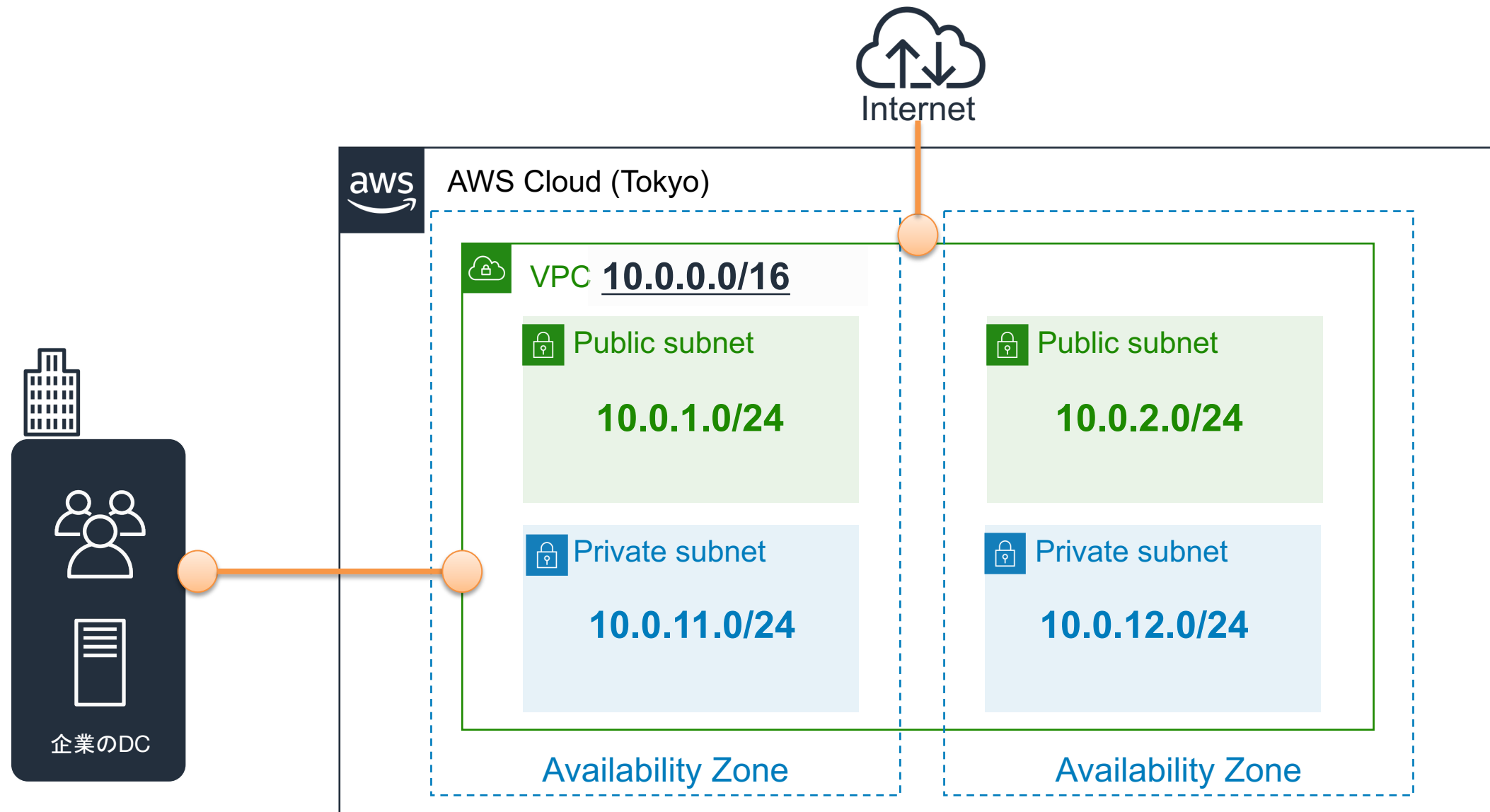


Amazon VPC (Virtual Private Cloud)

クラウド内に**プライベートネットワーク**を構築
既存データセンターの延長としてAWSを利用

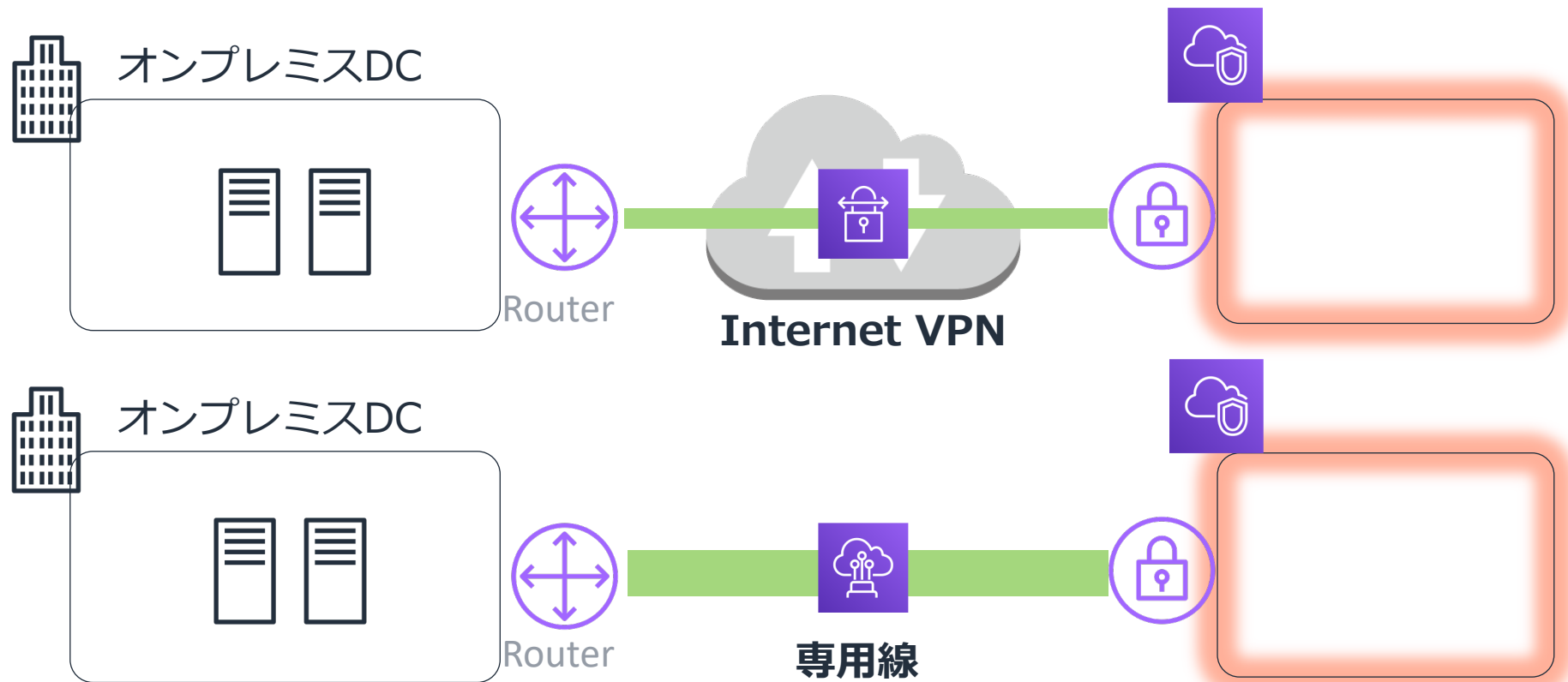


VPCをAZにまたがって作成し可用性を担保（マルチAZ構成）

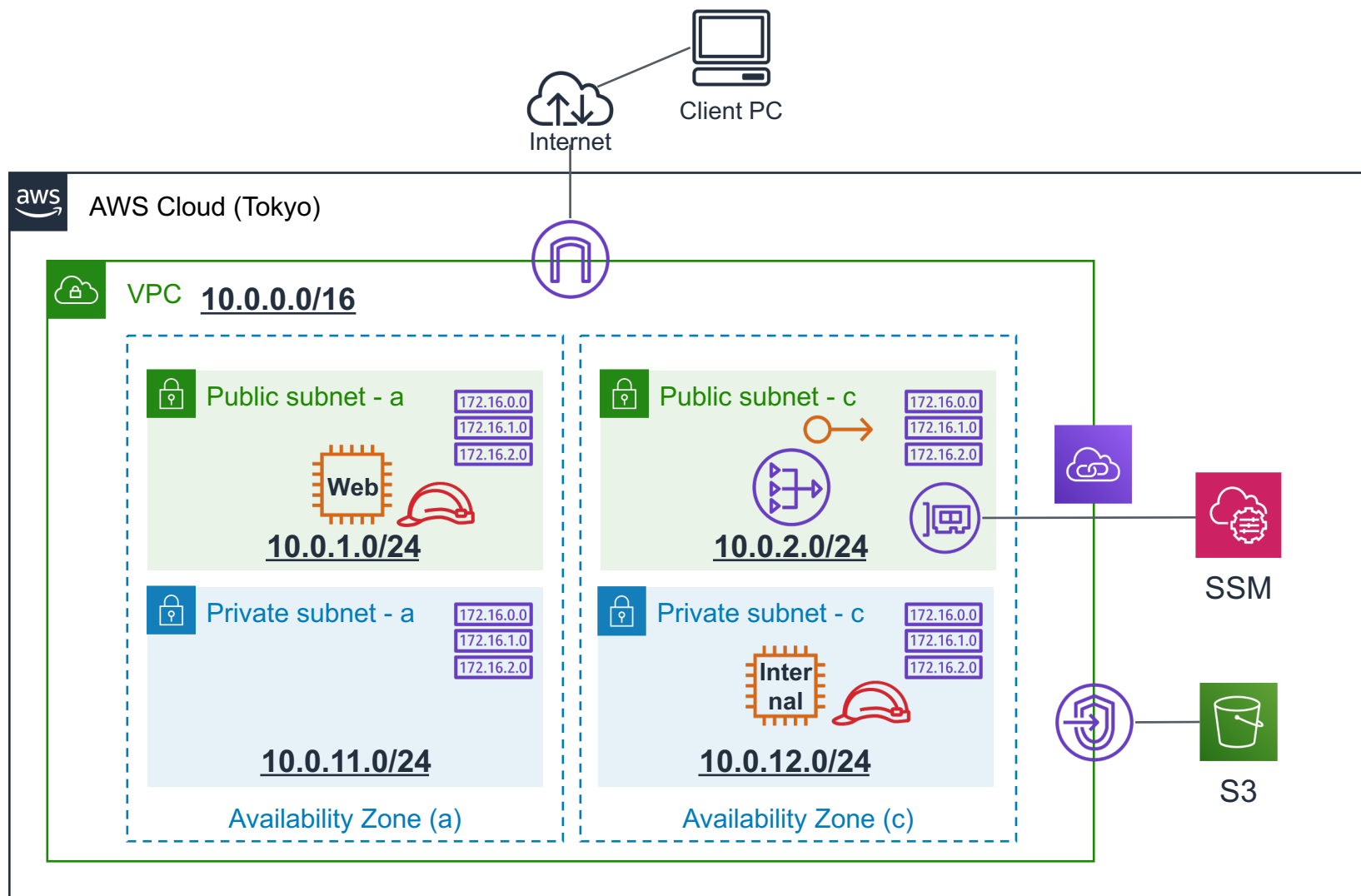


オンプレミスとAWSの接続

VPNや専用線を使った標準技術で、クラウド環境と接続することが可能



本ハンズオンの最終構成図



ハンズオンで学ぶサービス・機能



Amazon VPC



Public/Private Subnet



Internet gateway



Route table



NAT gateway



Endpoints



PrivateLink



Elastic IP address

ハンズオンの中で関わるサービス・機能



AWS Systems Manager



Amazon EC2



Amazon S3



IAM Role



【AWS Hands-on for Beginners】

Network 編 #1-2

AWS上にセキュアなプライベートネットワーク空間を作成

アマゾン ウェブ サービス ジャパン合同会社
パートナー ソリューション アーキテクト

江口 智 / Tomo Eguchi

(収録日: 2022/5/8)

このコースの Agenda

1. AWS

1. 前提知識の確認
2. AWSでのネットワークの考え方
3. 本ハンズオンの最終構成図

2. Amazon VPC ハンズオン

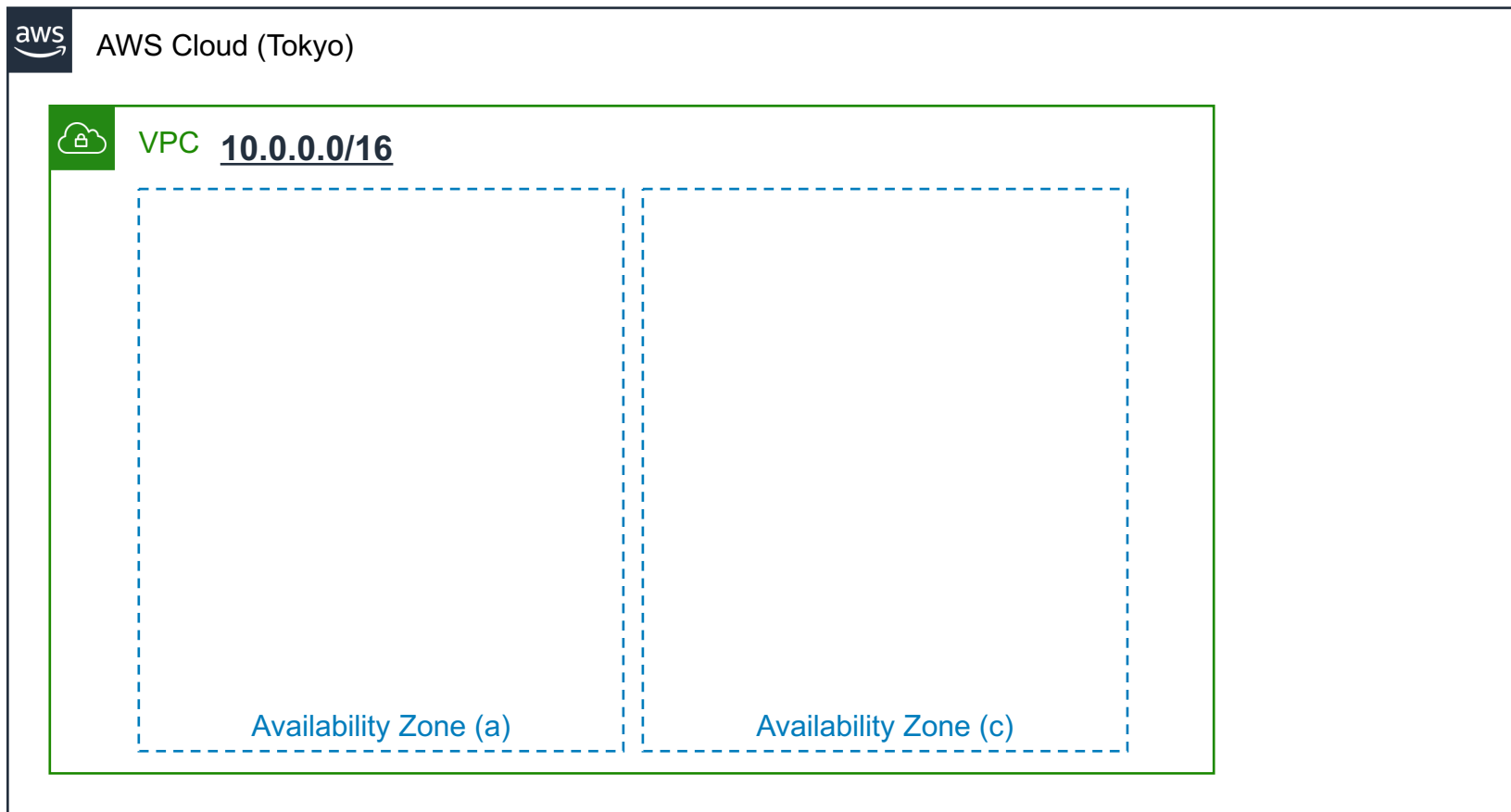
- 1. Amazon VPC ハンズオン① Amazon VPC の作成とインターネット接続環境の構築**
2. Amazon VPC ハンズオン② ルートテーブルによる経路設定を理解する
3. Amazon VPC ハンズオン③ プライベートサブネットからインターネットへのアクセス方法
4. Amazon VPC ハンズオン④ VPC外サービスへの接続方法 - 1
5. Amazon VPC ハンズオン⑤ VPC外サービスへの接続方法 - 2

3. 本コースのまとめ



ハンズオンの流れ

VPCを作成する



ハンズオンで学ぶサービス・機能



Amazon VPC

ハンズオンの中で関わるサービス・機能



VPCを作成する

VPC全体で利用するIPアドレス空間は余裕を持つこと
設定可能なネットマスクは 16bit ~ 28bit



AWS Cloud (Tokyo)



VPC 10.0.0.0/16

Availability Zone (a)

Availability Zone (c)

ハンズオンで学ぶサービス・機能

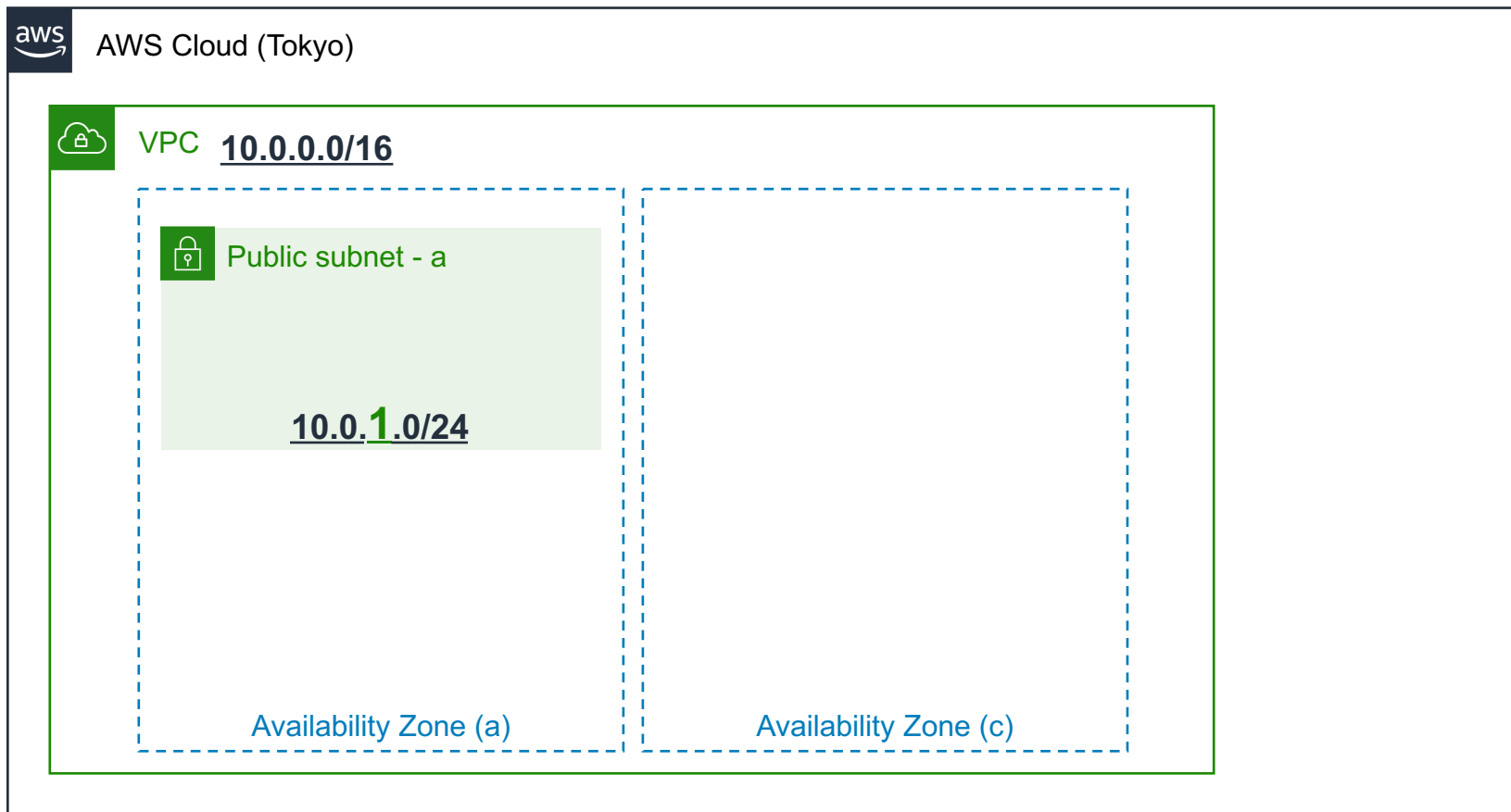


Amazon VPC

ハンズオンの中で関わるサービス・機能



VPC内にサブネットを作成する



ハンズオンで学ぶサービス・機能



Amazon VPC

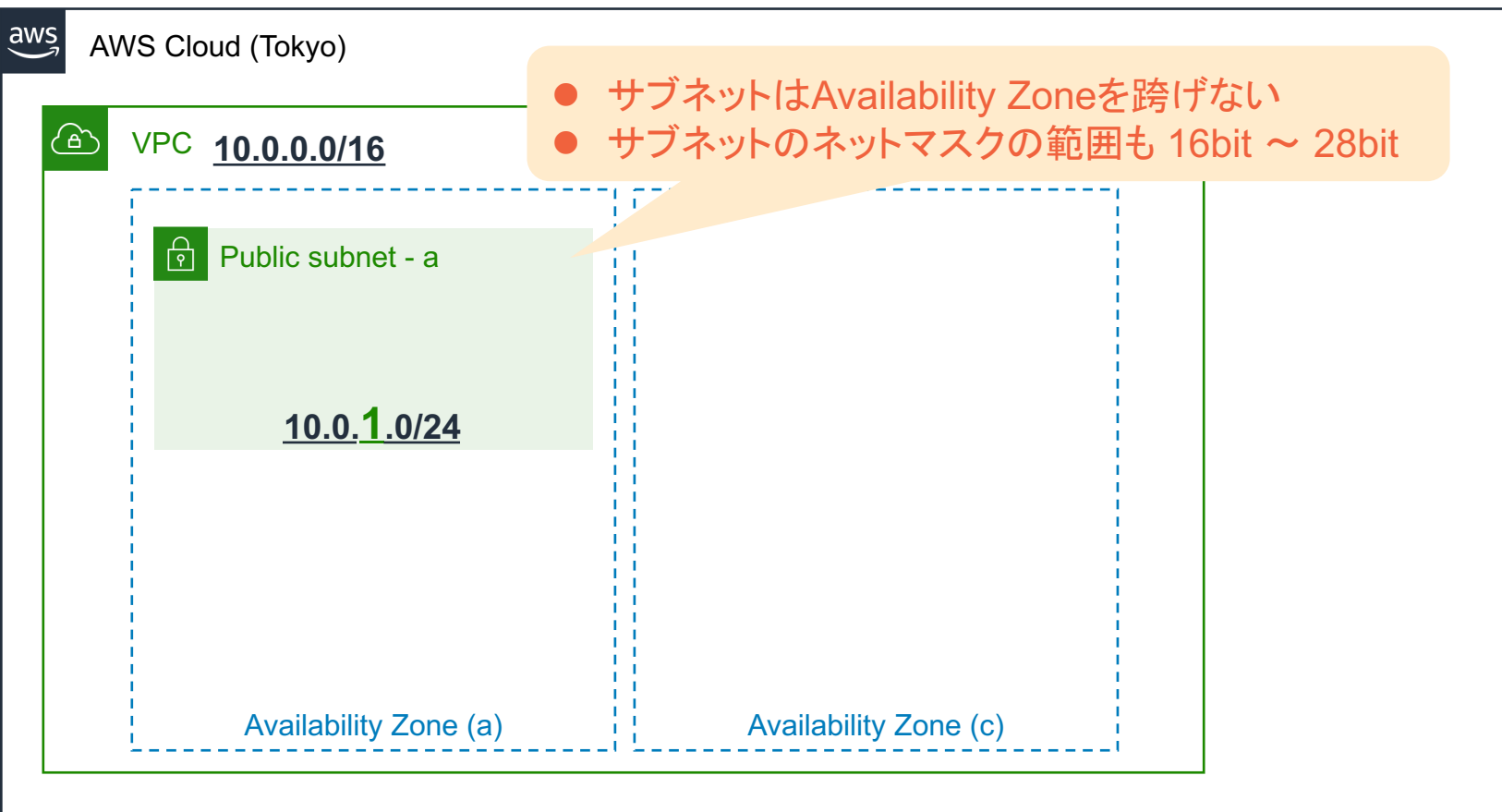


Public/Private Subnet

ハンズオンの中で関わるサービス・機能



VPC内にサブネットを作成する



ハンズオンで学ぶサービス・機能



Amazon VPC



Public/Private Subnet

ハンズオンの中で関わるサービス・機能

VPC内にサブネットを作成する

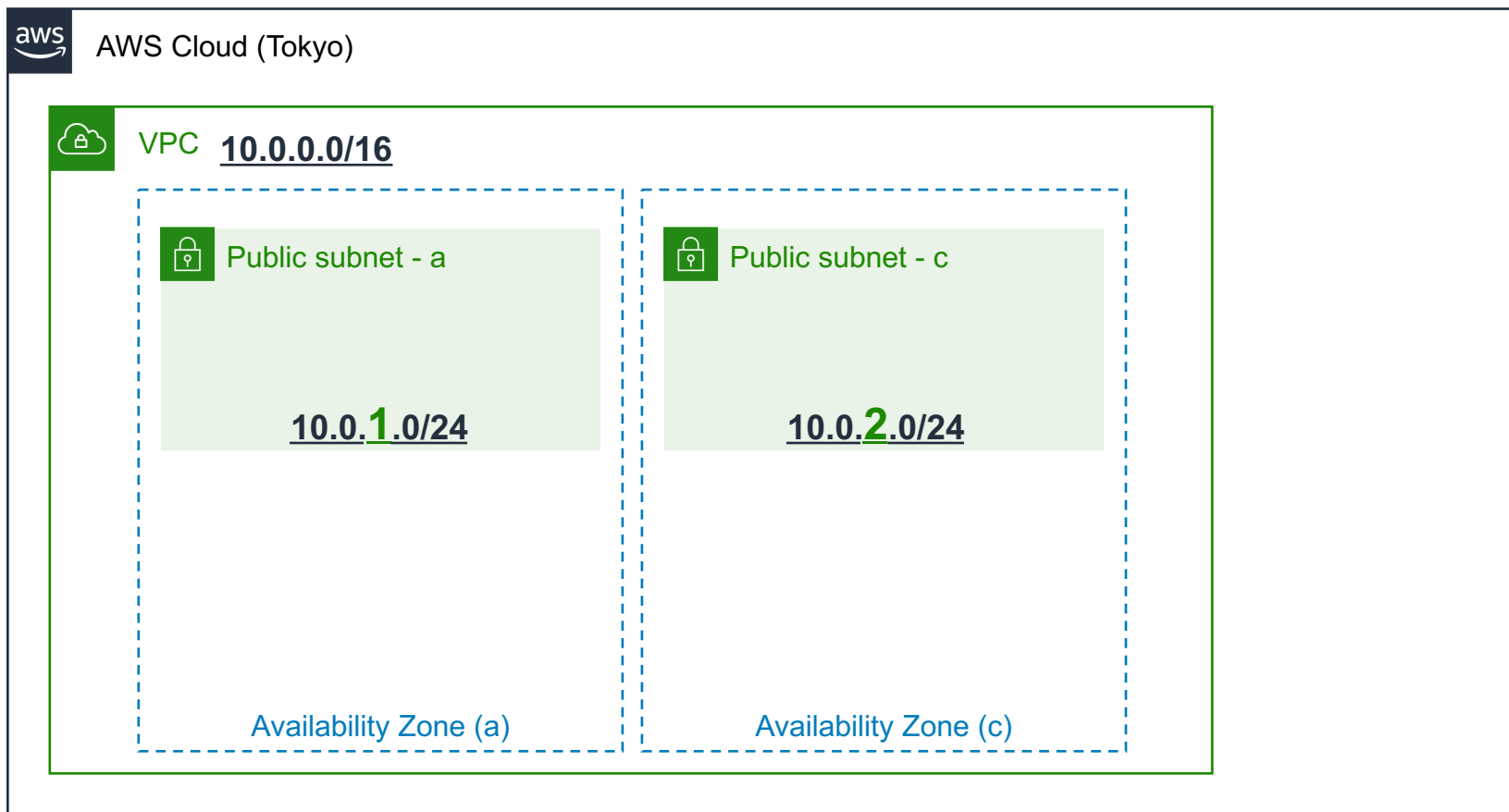
ハンズオンで学ぶサービス・機能



Amazon VPC



Public/Private Subnet



ハンズオンの中で関わるサービス・機能



VPC内にサブネットを作成する

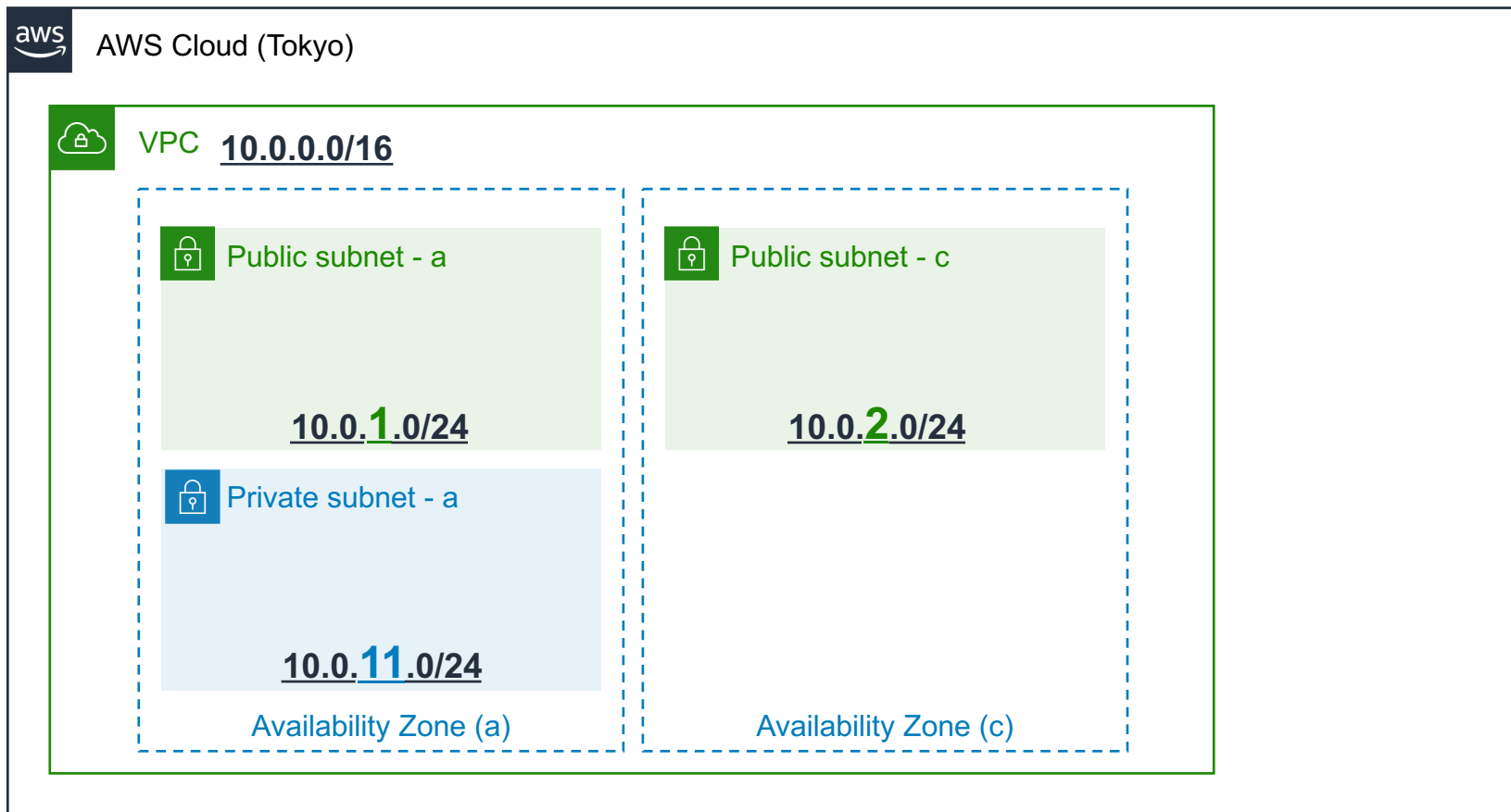
ハンズオンで学ぶサービス・機能



Amazon VPC



Public/Private Subnet



ハンズオンの中で関わるサービス・機能



VPC内にサブネットを作成する

ハンズオンで学ぶサービス・機能



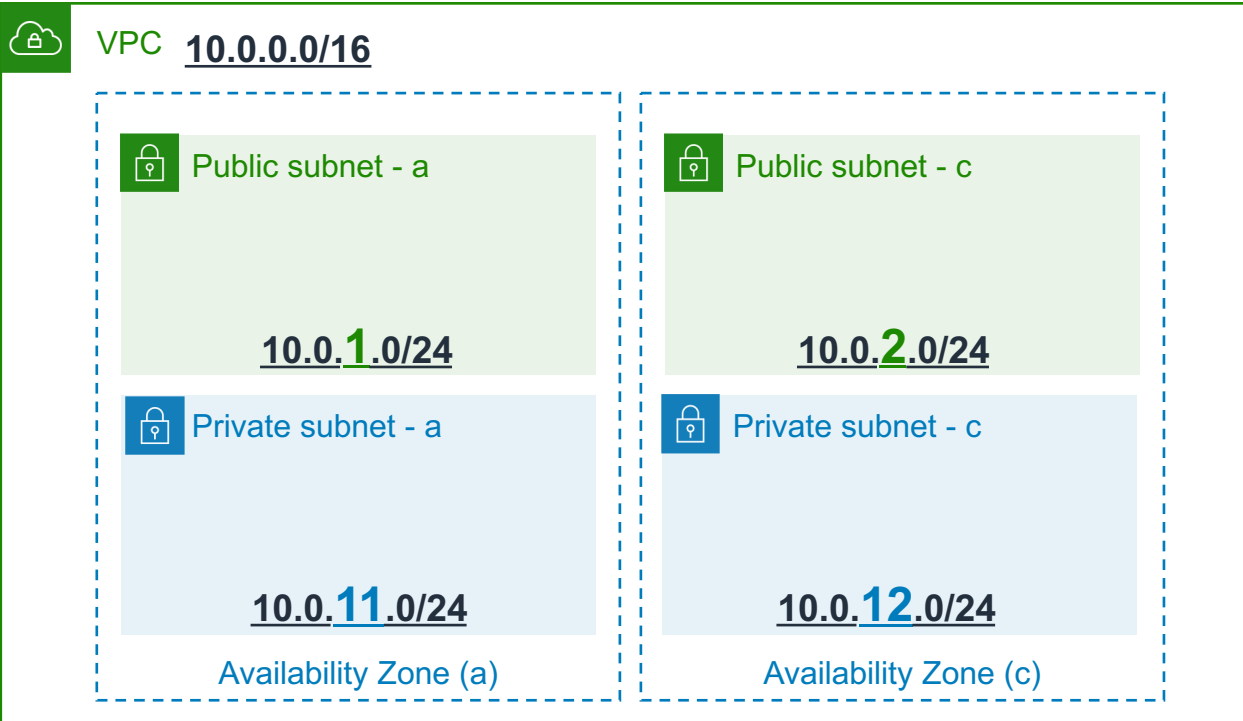
Amazon VPC



Public/Private Subnet



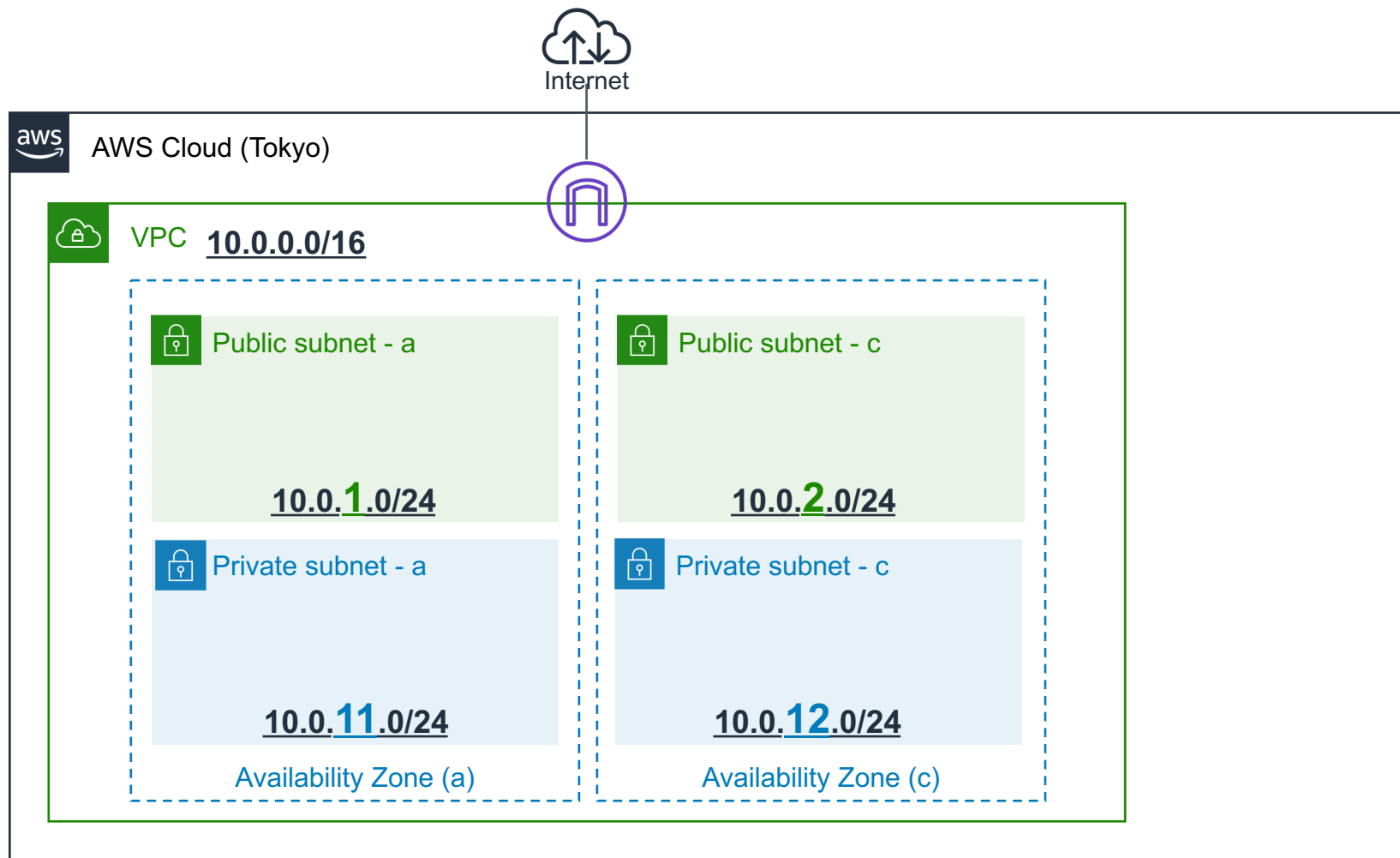
AWS Cloud (Tokyo)



ハンズオンの中で関わるサービス・機能



Internet Gatewayの作成とアタッチ



ハンズオンで学ぶサービス・機能



Amazon VPC



Public/Private Subnet



Internet gateway

ハンズオンの中で関わるサービス・機能



【AWS Hands-on for Beginners】

Network 編 #1-3

AWS上にセキュアなプライベートネットワーク空間を作成

アマゾン ウェブ サービス ジャパン合同会社
パートナー ソリューション アーキテクト

江口 智 / Tomo Eguchi

(収録日: 2022/5/8)

このコースの Agenda

1. AWS

1. 前提知識の確認
2. AWSでのネットワークの考え方
3. 本ハンズオンの最終構成図

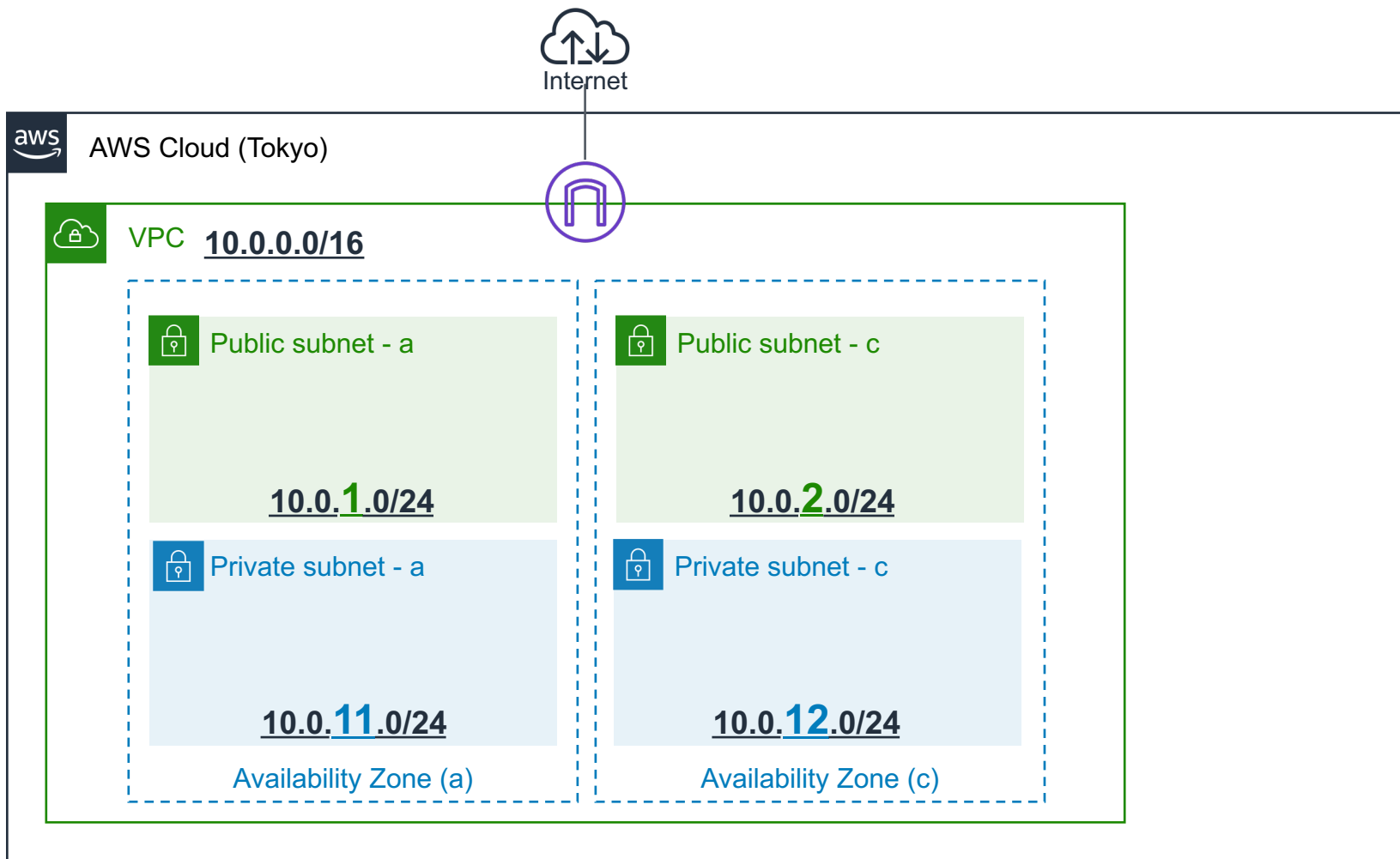
2. Amazon VPC ハンズオン

- 1. Amazon VPC ハンズオン① Amazon VPC の作成とインターネット接続環境の構築**
2. Amazon VPC ハンズオン② ルートテーブルによる経路設定を理解する
3. Amazon VPC ハンズオン③ プライベートサブネットからインターネットへのアクセス方法
4. Amazon VPC ハンズオン④ VPC外サービスへの接続方法 - 1
5. Amazon VPC ハンズオン⑤ VPC外サービスへの接続方法 - 2

3. 本コースのまとめ



ハンズオンで作成する環境



ハンズオンで学ぶサービス・機能



Amazon VPC



Public/Private Subnet

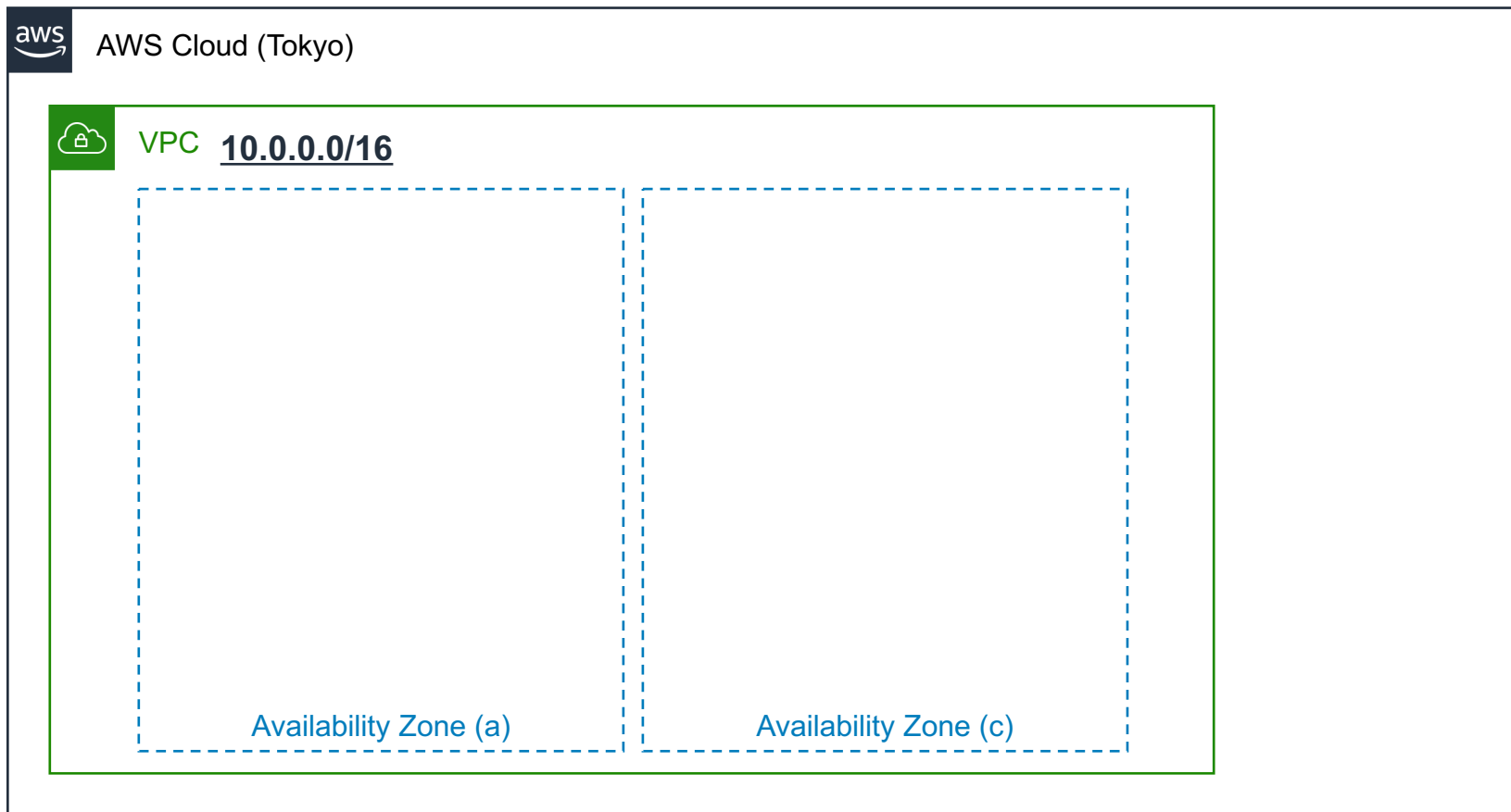


Internet gateway

ハンズオンの中で関わるサービス・機能



VPCを作成する



ハンズオンで学ぶサービス・機能

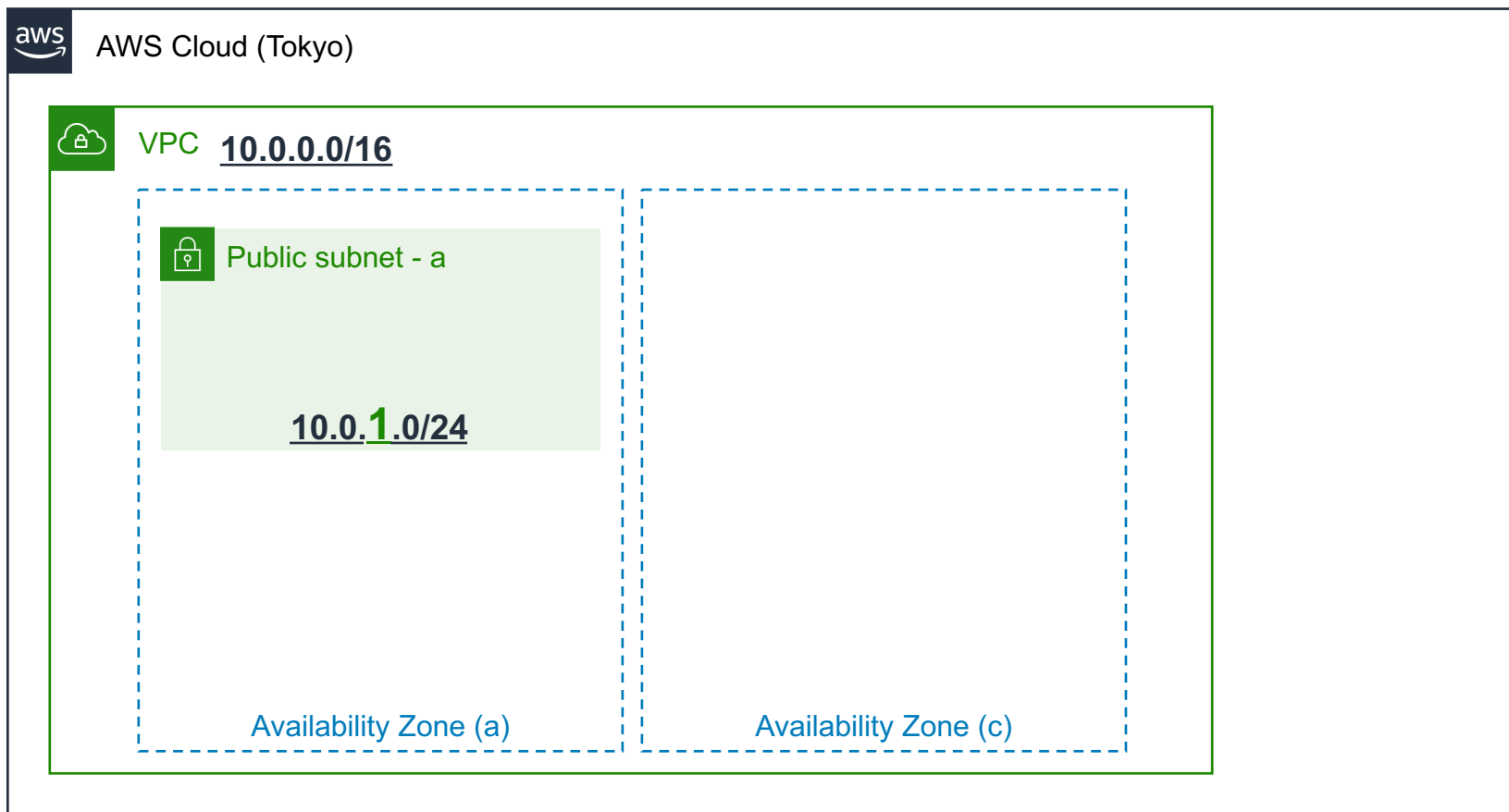


Amazon VPC

ハンズオンの中で関わるサービス・機能



VPC内にサブネットを作成する



ハンズオンで学ぶサービス・機能



Amazon VPC



Public/Private Subnet

ハンズオンの中で関わるサービス・機能



VPC内にサブネットを作成する

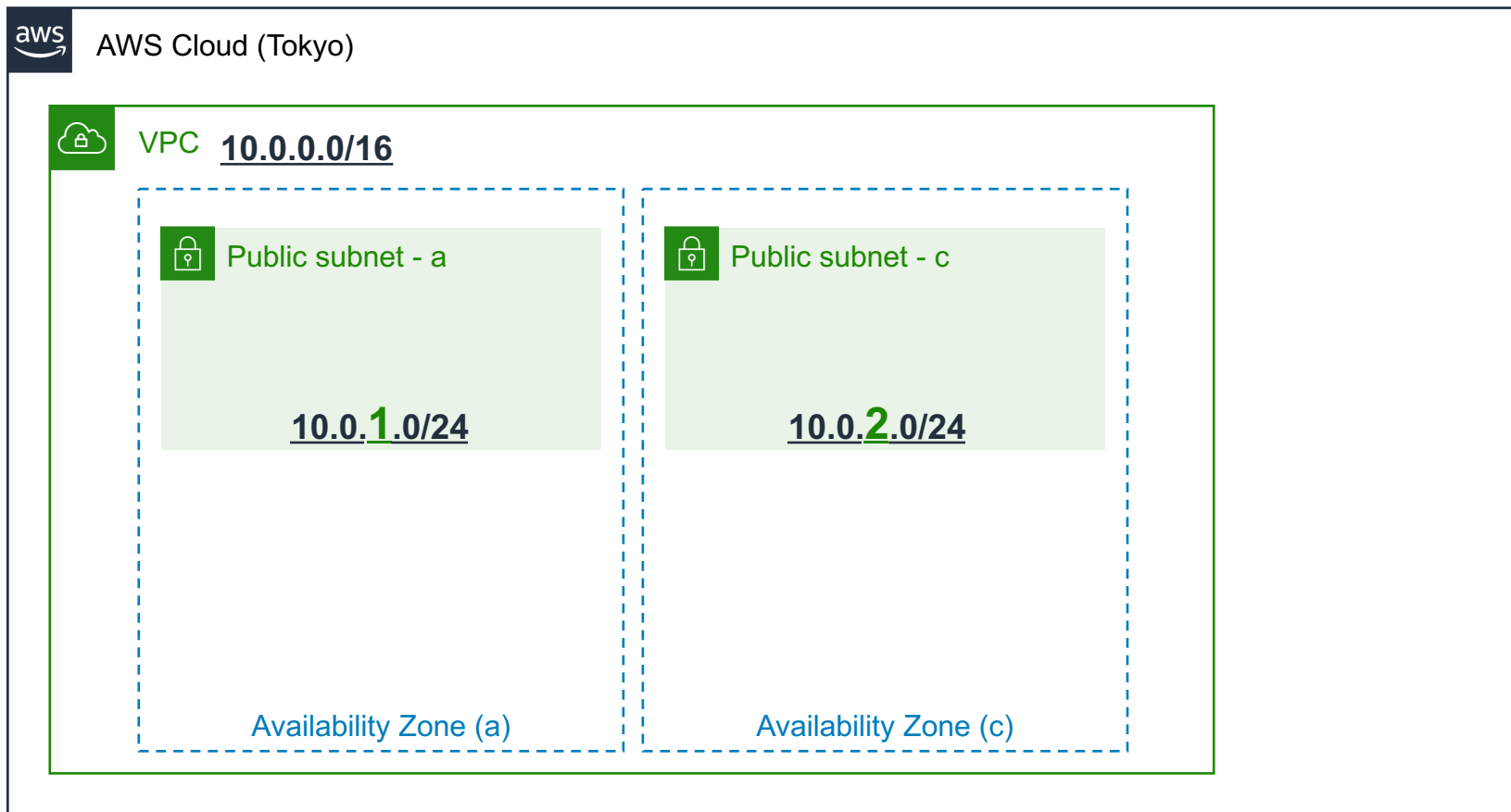
ハンズオンで学ぶサービス・機能



Amazon VPC



Public/Private Subnet



ハンズオンの中で関わるサービス・機能



VPC内にサブネットを作成する

ハンズオンで学ぶサービス・機能



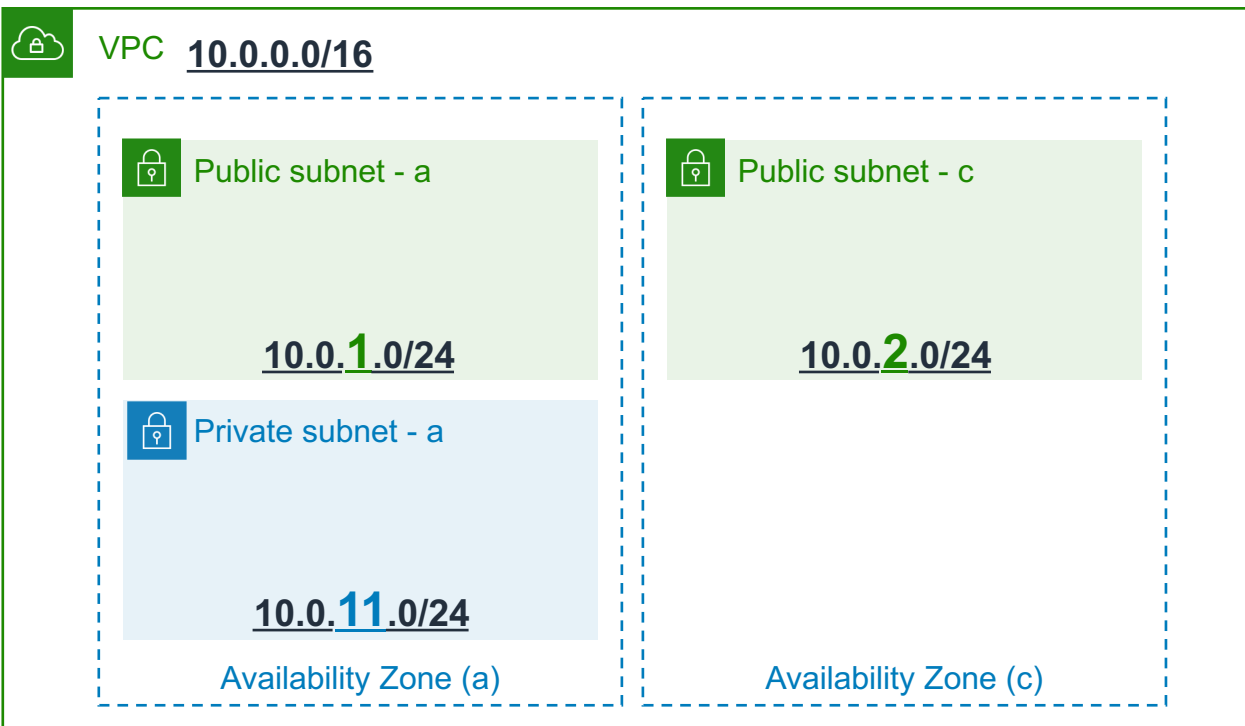
Amazon VPC



Public/Private Subnet



AWS Cloud (Tokyo)



ハンズオンの中で関わるサービス・機能



VPC内にサブネットを作成する

ハンズオンで学ぶサービス・機能



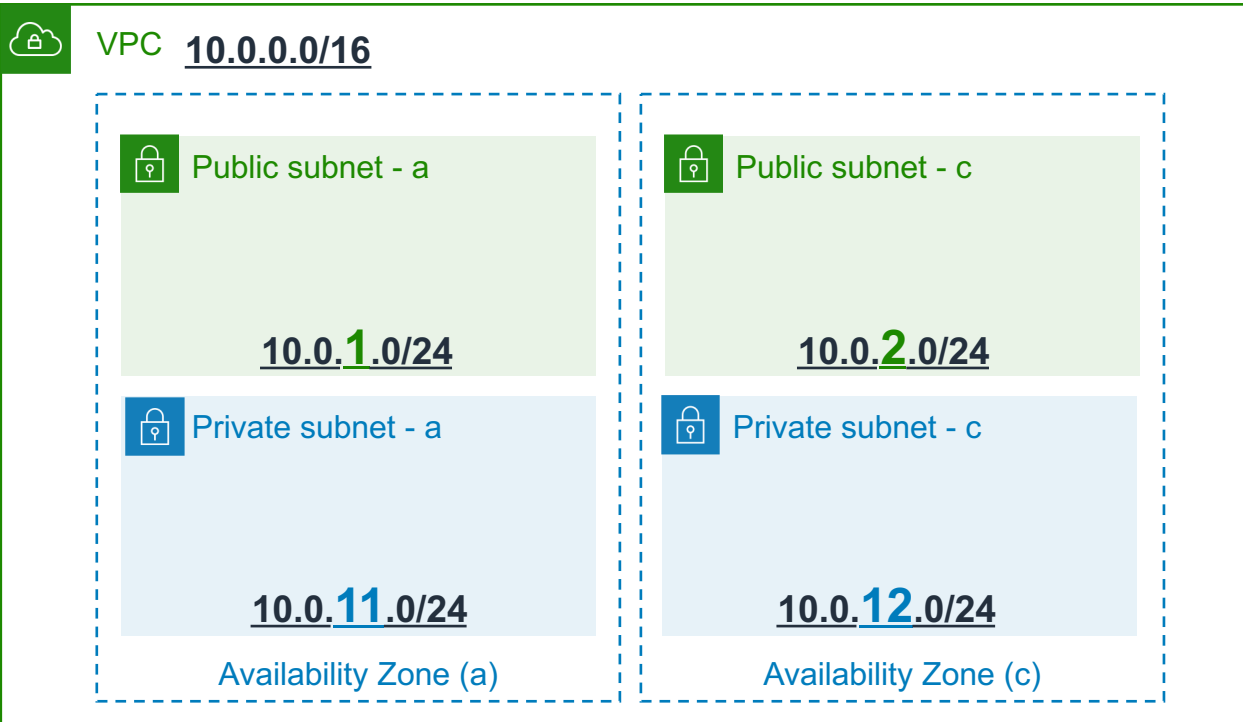
Amazon VPC



Public/Private Subnet



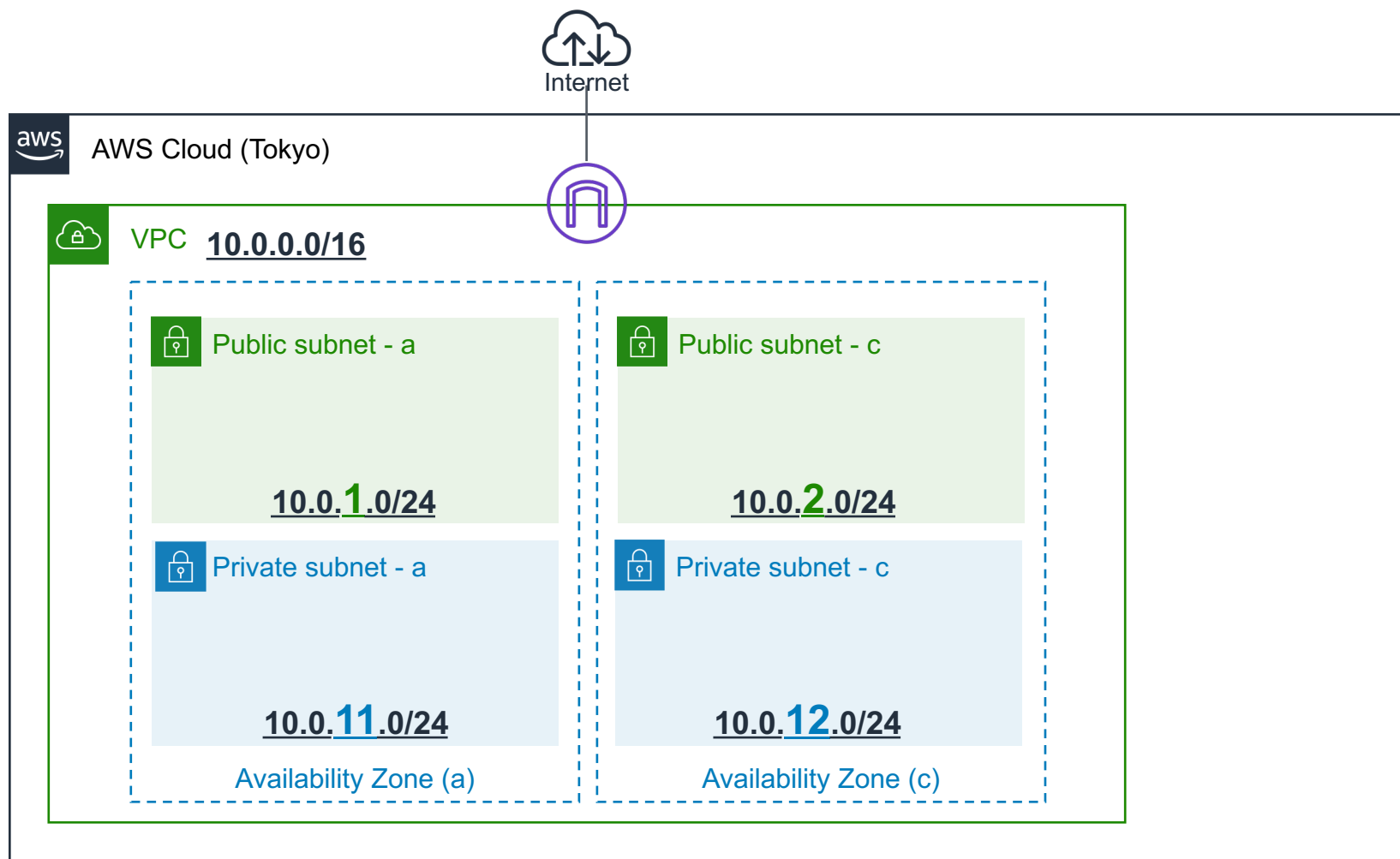
AWS Cloud (Tokyo)



ハンズオンの中で関わるサービス・機能



Internet Gatewayの作成とアタッチ



ハンズオンで学ぶサービス・機能



Amazon VPC



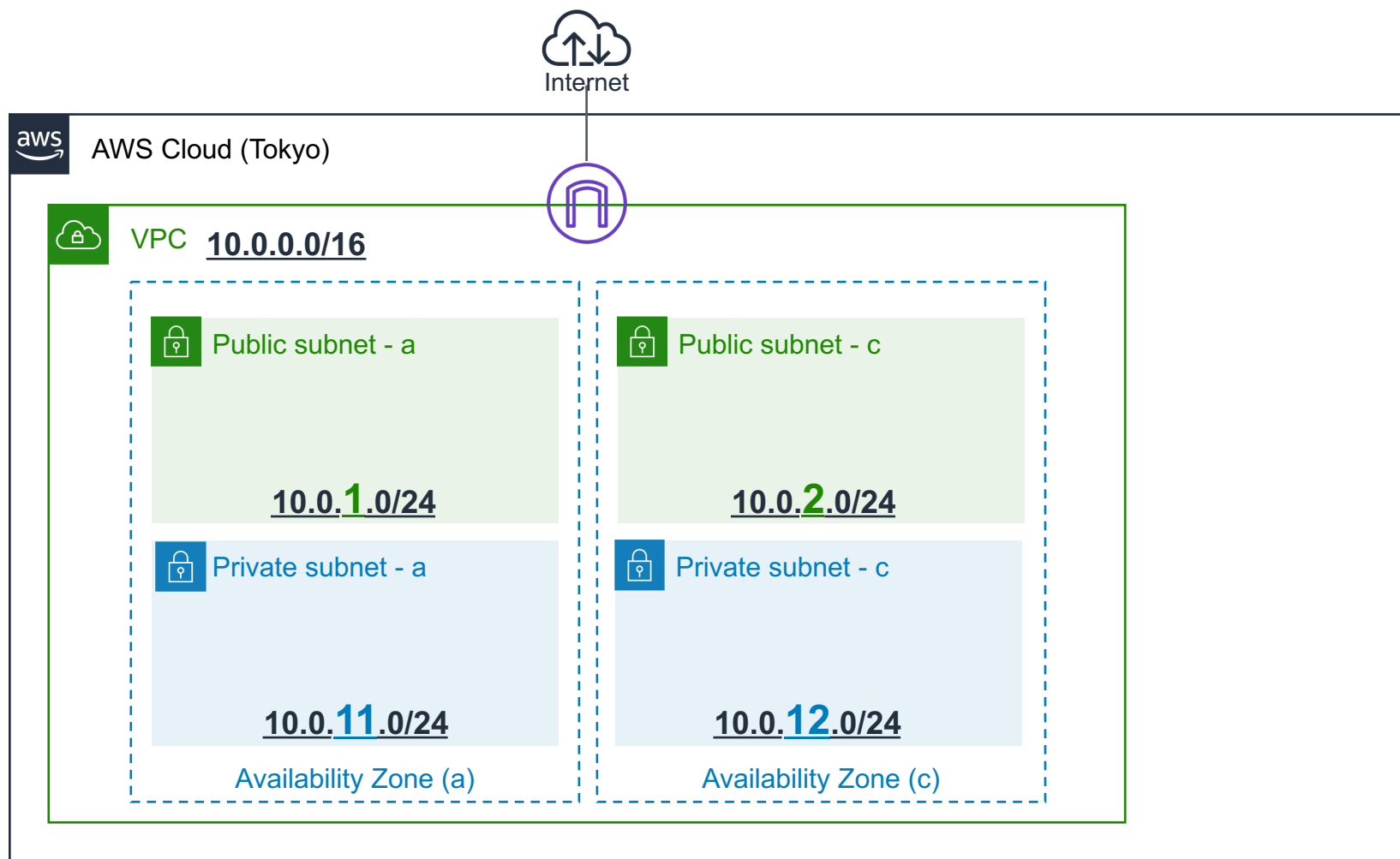
Public/Private Subnet



Internet gateway

ハンズオンの中で関わるサービス・機能

Internet Gatewayの作成とアタッチ



ハンズオンで学ぶサービス・機能



Amazon VPC



Public/Private Subnet



Internet gateway

ハンズオンの中で関わるサービス・機能

ルートテーブルの作成と関連付け

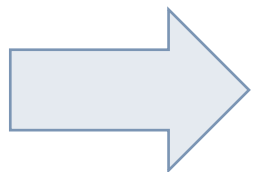
パブリックサブネット と プライベートサブネット

- パブリックサブネット

- ルーティングテーブルにインターネットゲートウェイへのエントリがあり、インターネットとインバウンド/アウトバウンドのアクセスが可能

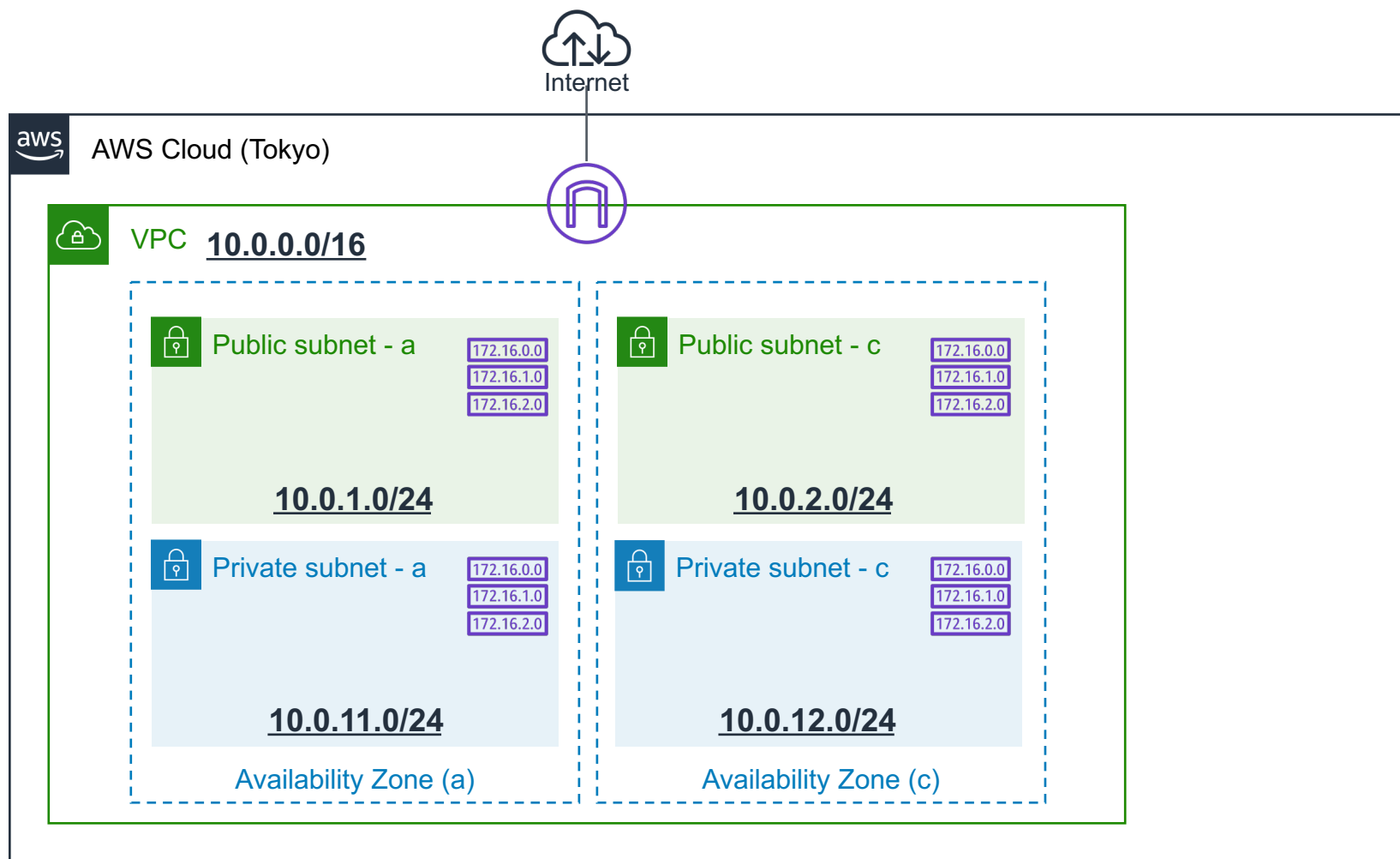
- プライベートサブネット

- ルーティングテーブルにインターネットゲートウェイへのエントリはなく、インターネットから直接アクセスできない



ルートテーブルでコントロール

Route tableの作成と関連付け



ハンズオンで学ぶサービス・機能



Amazon VPC



Public/Private Subnet



Internet gateway



Route table

ハンズオンの中で関わるサービス・機能



ルートテーブルで理解しておくこと

- ルートテーブルとは、ネットワークトラフィックの経路を決定する**ルート**と呼ばれる一連のルールが定義されたテーブル情報
- 各サブネットに**ルートテーブルを関連付ける**ことにより、サブネットのネットワークルーティング（通信経路）が決定



【AWS Hands-on for Beginners】

Network 編 #1-4

AWS上にセキュアなプライベートネットワーク空間を作成

アマゾン ウェブ サービス ジャパン合同会社
パートナー ソリューション アーキテクト

江口 智 / Tomo Eguchi

(収録日: 2022/5/8)

このコースの Agenda

1. AWS

1. 前提知識の確認
2. AWSでのネットワークの考え方
3. 本ハンズオンの最終構成図

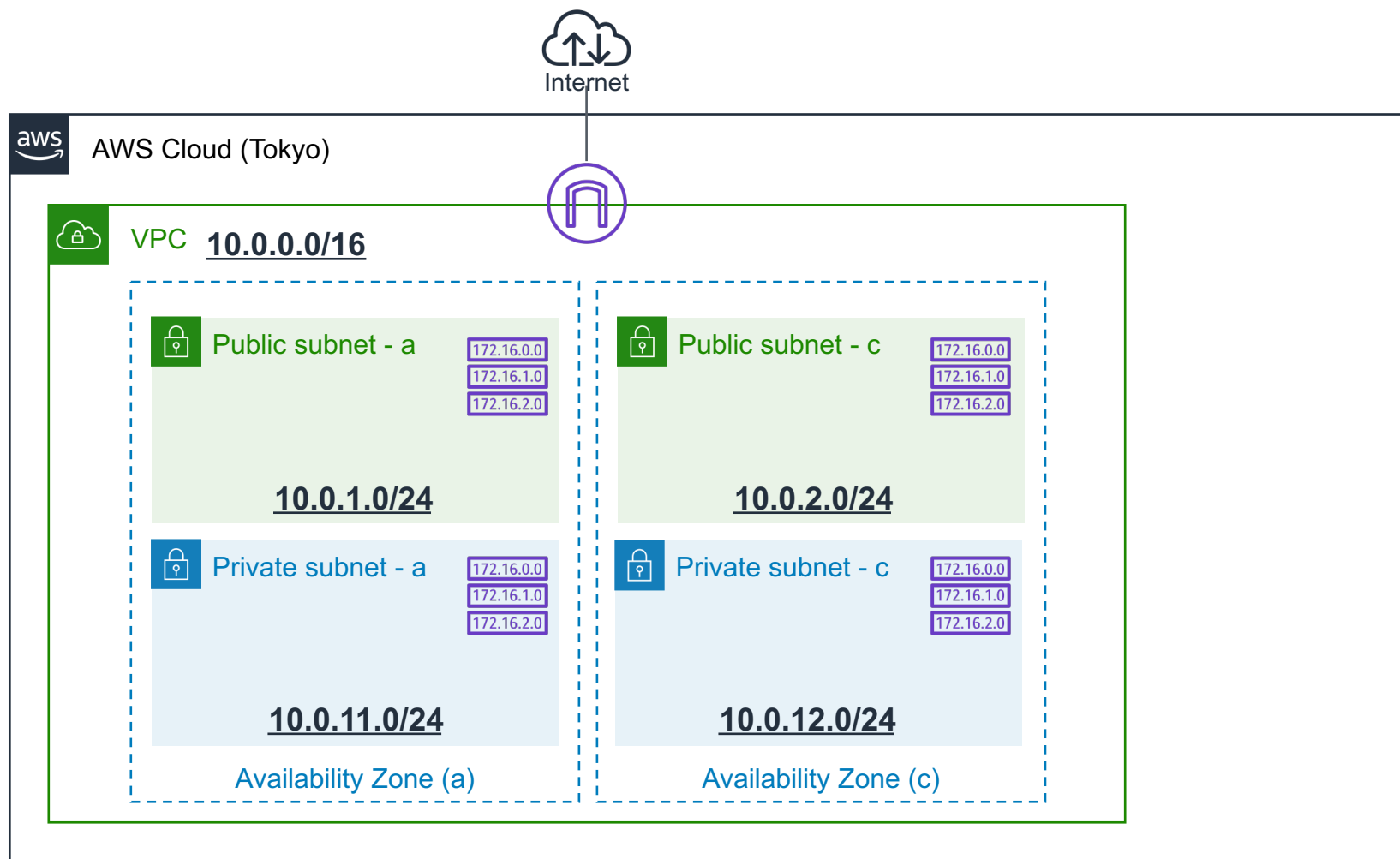
2. Amazon VPC ハンズオン

- 1. Amazon VPC ハンズオン① Amazon VPC の作成とインターネット接続環境の構築**
2. Amazon VPC ハンズオン② ルートテーブルによる経路設定を理解する
3. Amazon VPC ハンズオン③ プライベートサブネットからインターネットへのアクセス方法
4. Amazon VPC ハンズオン④ VPC外サービスへの接続方法 - 1
5. Amazon VPC ハンズオン⑤ VPC外サービスへの接続方法 - 2

3. 本コースのまとめ



Route tableの作成と関連付け



ハンズオンで学ぶサービス・機能



Amazon VPC



Public/Private Subnet



Internet gateway



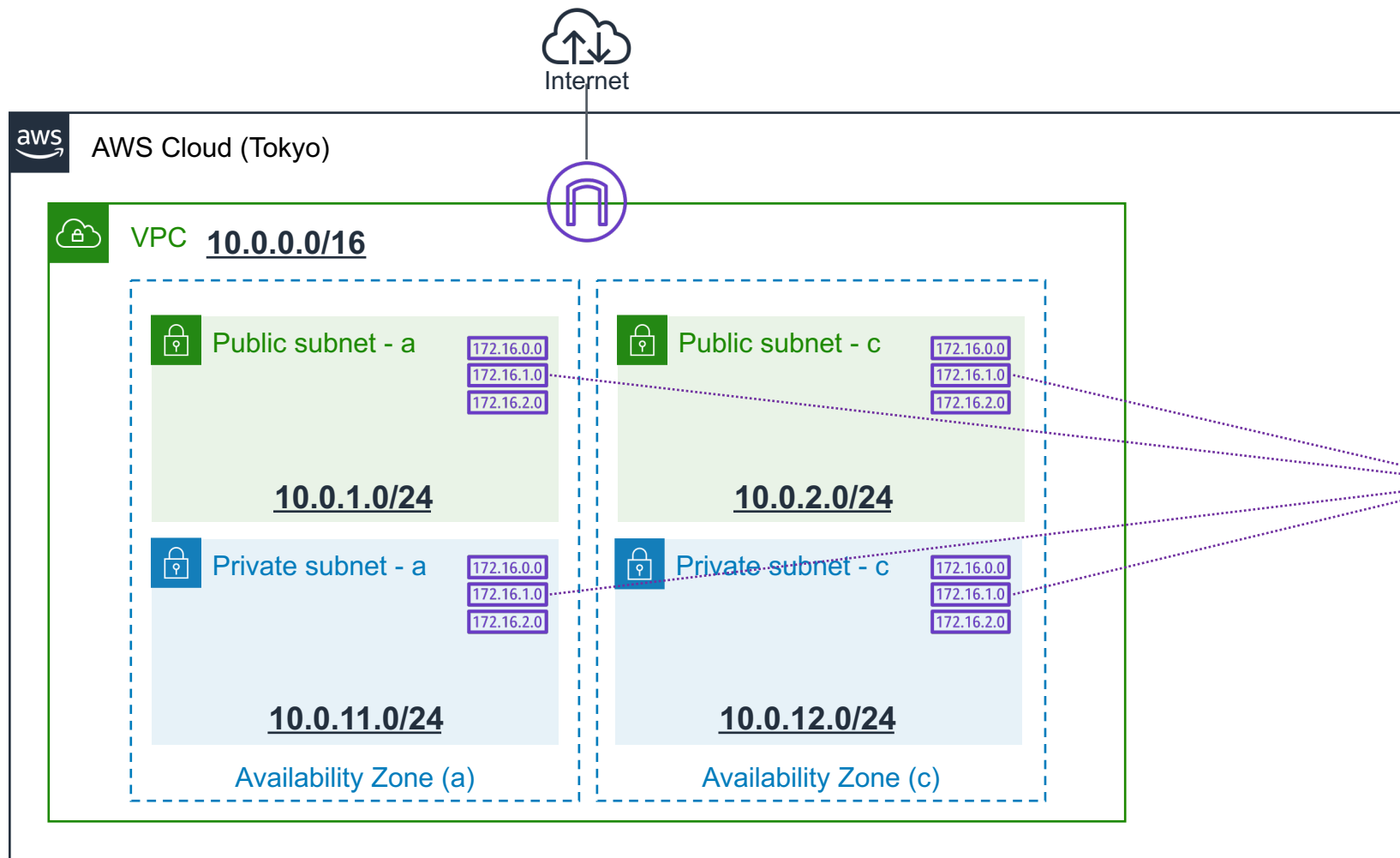
Route table

ハンズオンの中で関わるサービス・機能



ハンズオンの流れ

Route tableの作成と関連付け

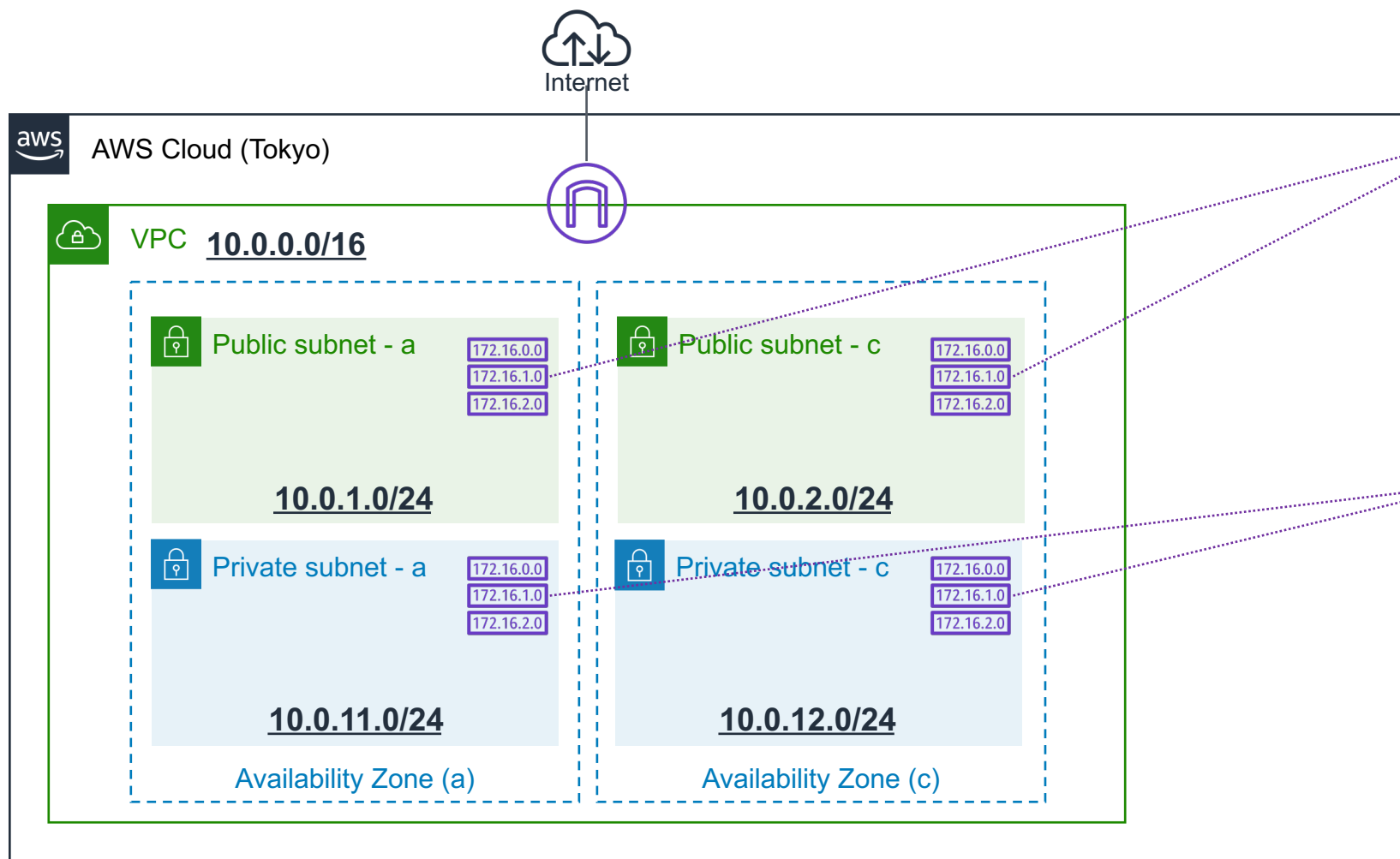


Route Table(メイン)

送信先	ターゲット
10.0.0.0/16	local

“local”という表現は、
VPC内通信という意味

Route tableの作成と関連付け（設定イメージ）



Public Route Table

送信先	ターゲット
10.0.0.0/16	local
0.0.0.0/0	Internet Gateway

Private Route Table(メイン)

送信先	ターゲット
10.0.0.0/16	local

ルーティングの優先度

- ルートテーブル内に定義された**最も具体的なルート**が優先されます。
(最長プレフィックス一致、ロングストマッチ)

Public Route Table

送信先	ターゲット
10.0.0.0/ 16	local
0.0.0.0/ 0	Internet Gateway

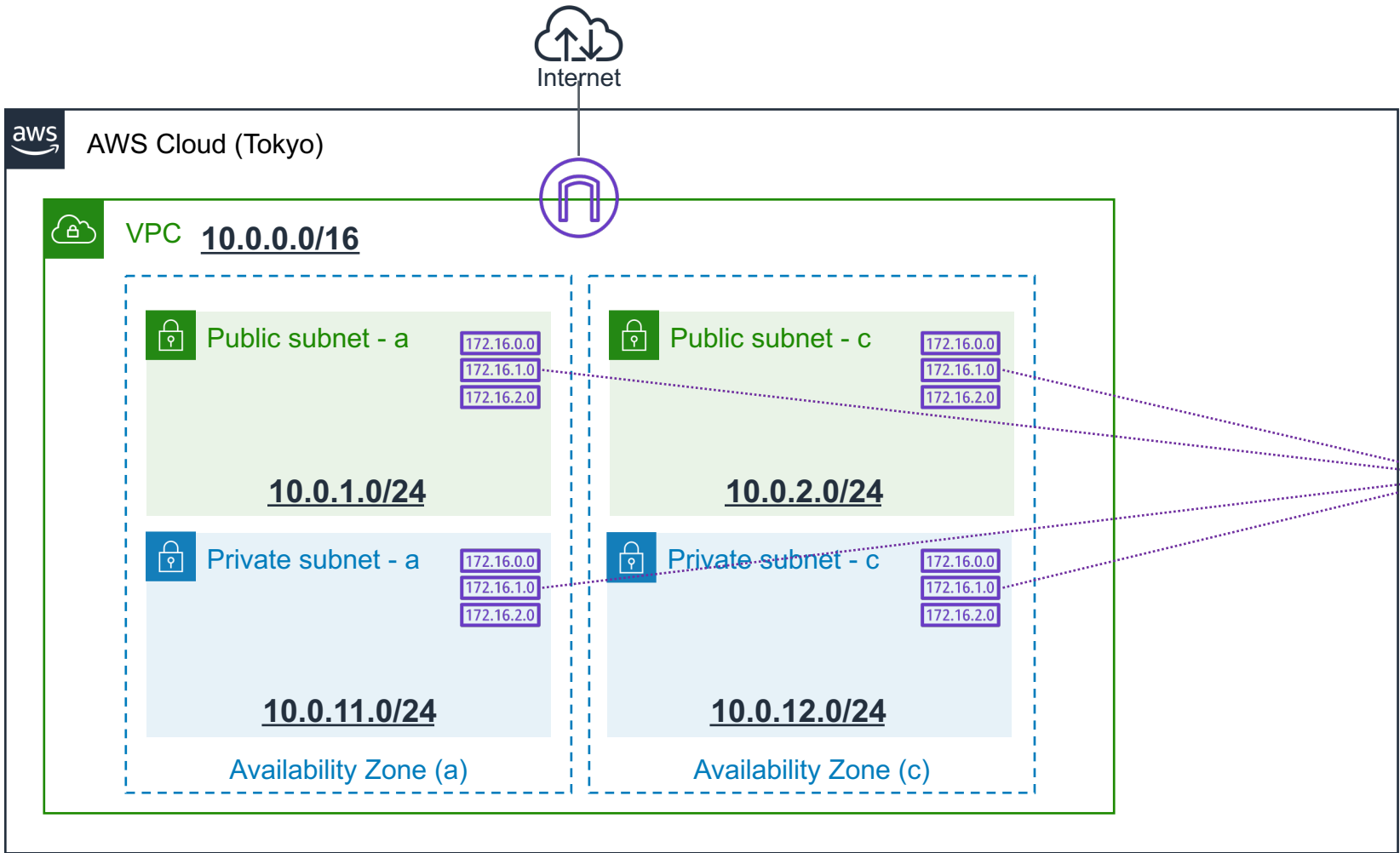
→ 10.0.0.0 ~ 10.0.255.255

→ 0.0.0.0 ~ 255.255.255.255

例)

送信先が10.0.10.111のトラフィックを受信した場合、ターゲットは「local」が選択される。

Route tableの作成と関連付け



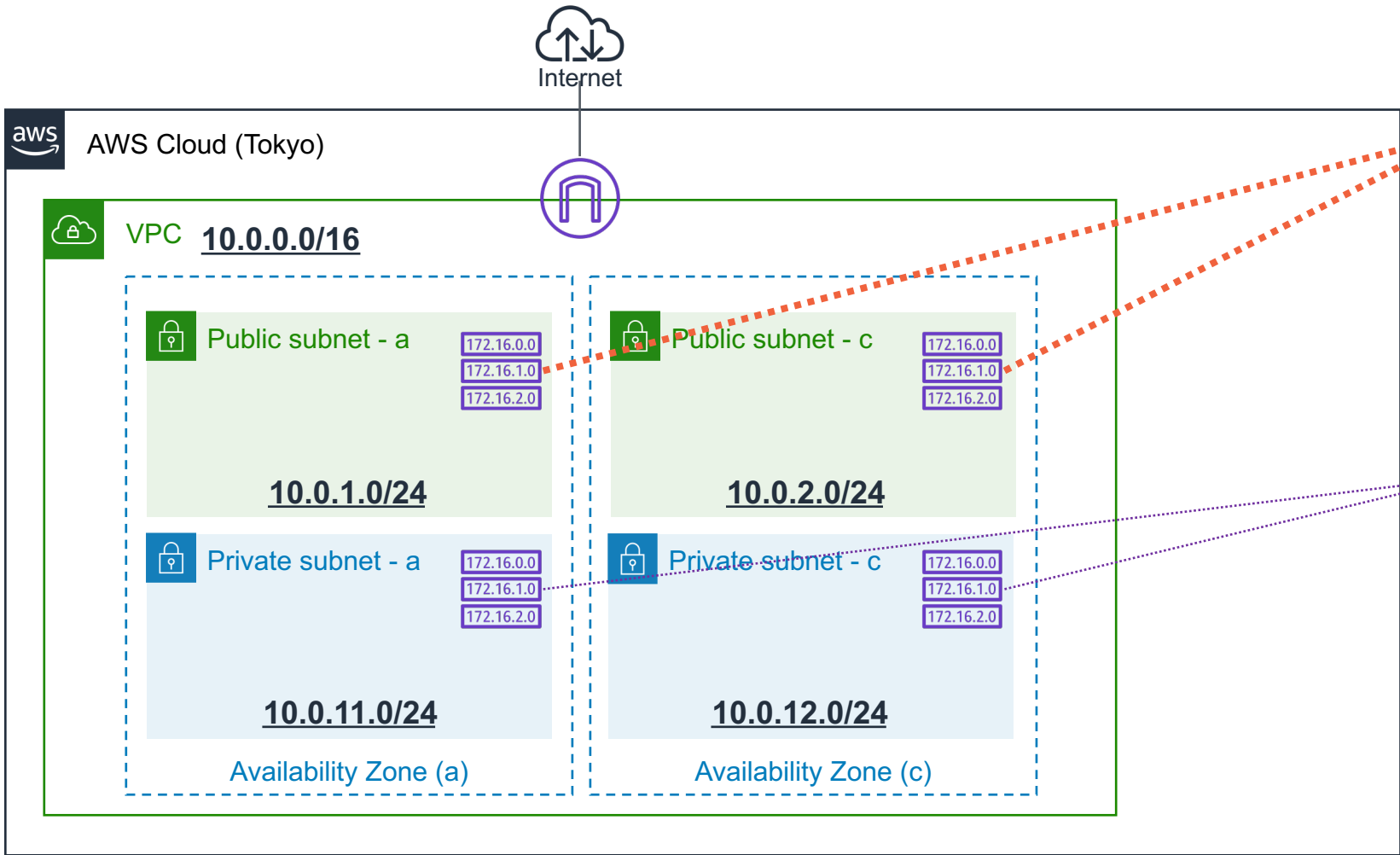
Public Route Table

送信先	ターゲット
10.0.0.0/16	local
0.0.0.0/0	Internet Gateway

Private Route Table (メイン)

送信先	ターゲット
10.0.0.0/16	local

Route tableの作成と関連付け



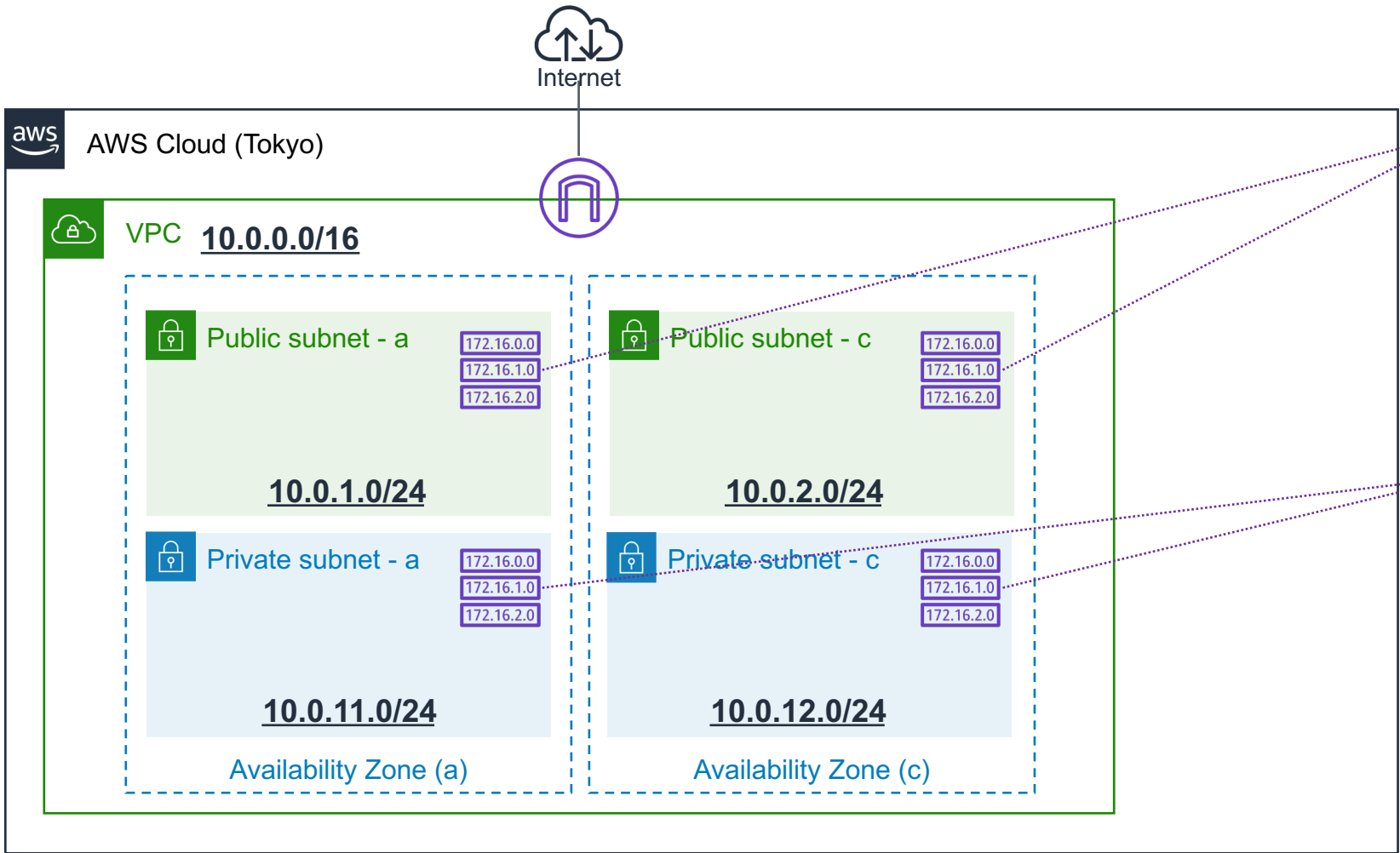
Public Route Table

送信先	ターゲット
10.0.0.0/16	local
0.0.0.0/0	Internet Gateway

Private Route Table(メイン)

送信先	ターゲット
10.0.0.0/16	local

Route tableの作成と関連付け



Public Route Table

送信先	ターゲット
10.0.0.0/16	local
0.0.0.0/0	Internet Gateway

Private Route Table(メイン)

送信先	ターゲット
10.0.0.0/16	local

Route table 設定のまとめ

- VPCの各サブネットは必ず1つのルートテーブルが関連付け(アソシエート)されている
- 1つのルートテーブルに異なる複数のサブネットを関連づけることが可能
- ルートテーブルにはメインが存在する。
ルートテーブルを明示的に関連付けていないサブネットは、メインルートテーブルが関連付く。
(新規でサブネットを作成した際もメインルートテーブルが関連付く)
- ルートテーブルの経路選択は最長プレフィックス一致（ロングストマッチ）にて、
経路の優先度が決まる



【AWS Hands-on for Beginners】

Network 編 #1-5

AWS上にセキュアなプライベートネットワーク空間を作成

アマゾン ウェブ サービス ジャパン合同会社
パートナー ソリューション アーキテクト

江口 智 / Tomo Eguchi

(収録日: 2022/5/8)

このコースの Agenda

1. AWS

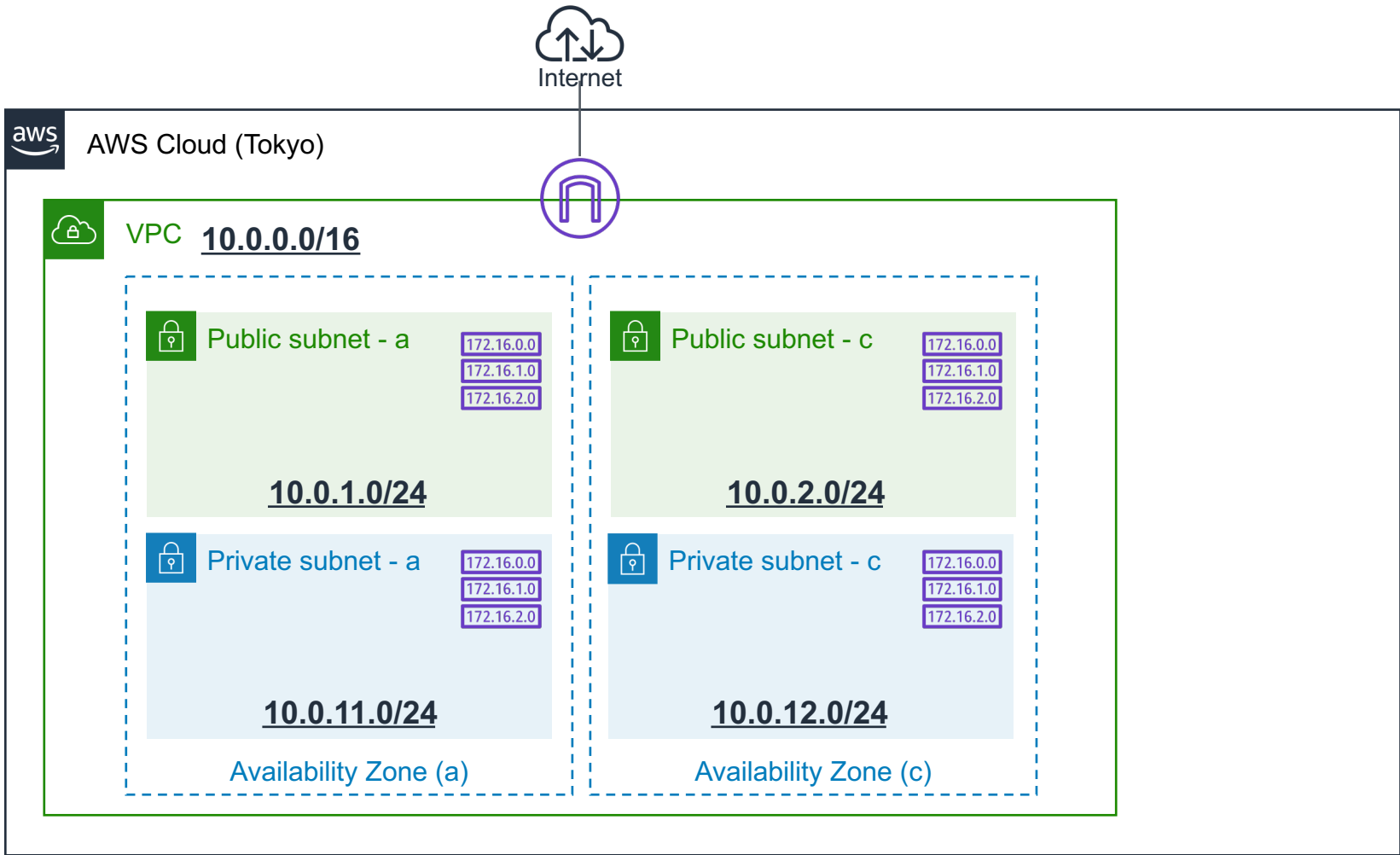
1. 前提知識の確認
2. AWSでのネットワークの考え方
3. 本ハンズオンの最終構成図

2. Amazon VPC ハンズオン

1. Amazon VPC ハンズオン① Amazon VPC の作成とインターネット接続環境の構築
- 2. Amazon VPC ハンズオン② ルートテーブルによる経路設定を理解する**
3. Amazon VPC ハンズオン③ プライベートサブネットからインターネットへのアクセス方法
4. Amazon VPC ハンズオン④ VPC外サービスへの接続方法 - 1
5. Amazon VPC ハンズオン⑤ VPC外サービスへの接続方法 - 2

3. 本コースのまとめ

動作確認方法



ハンズオンで学ぶサービス・機能



Amazon VPC



Public/Private Subnet



Internet gateway

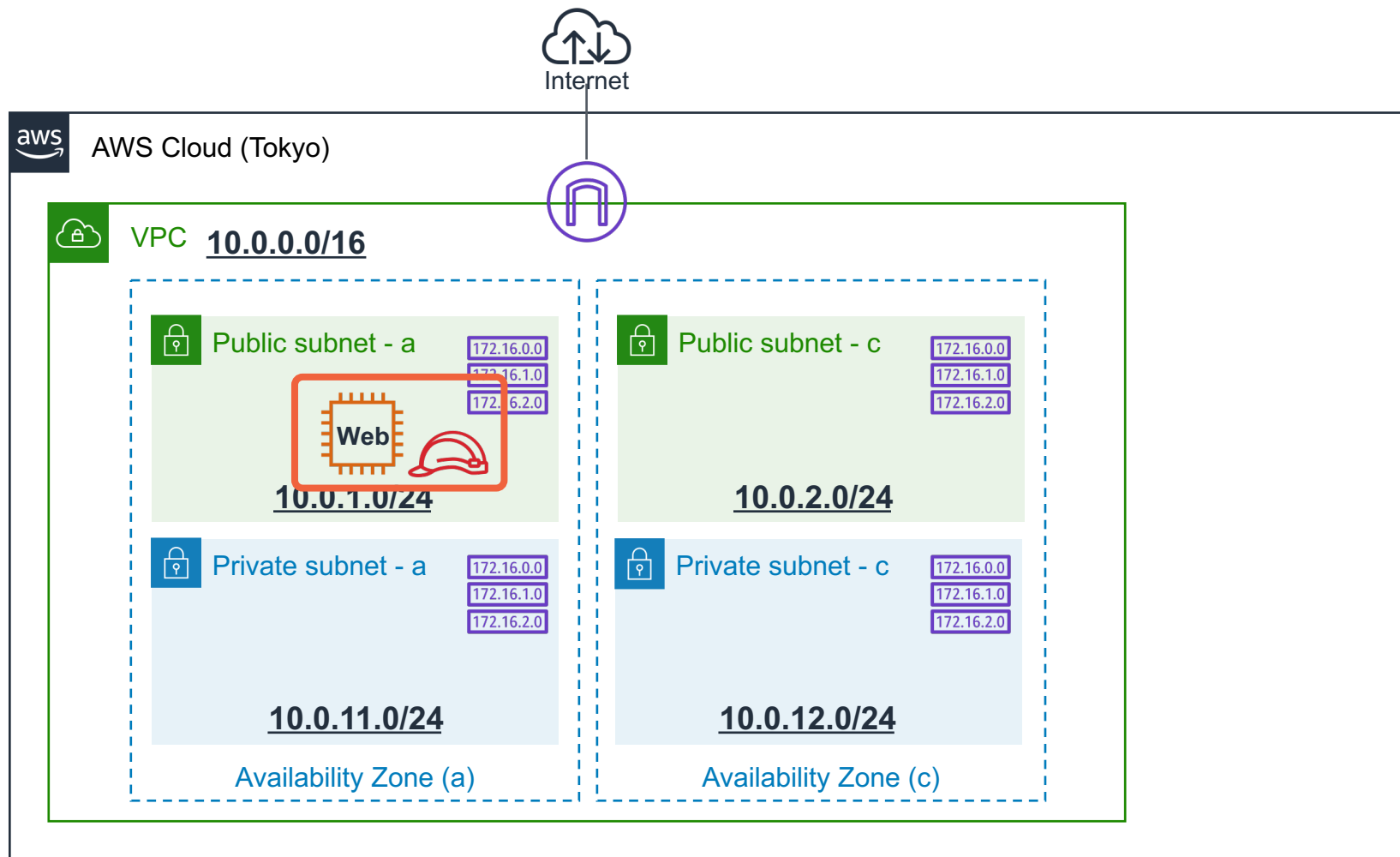


Route table

ハンズオンの中で関わるサービス・機能



動作確認方法



ハンズオンで学ぶサービス・機能



Amazon VPC



Public/Private Subnet



Internet gateway



Route table

ハンズオンの中で関わるサービス・機能



AWS Systems Manager

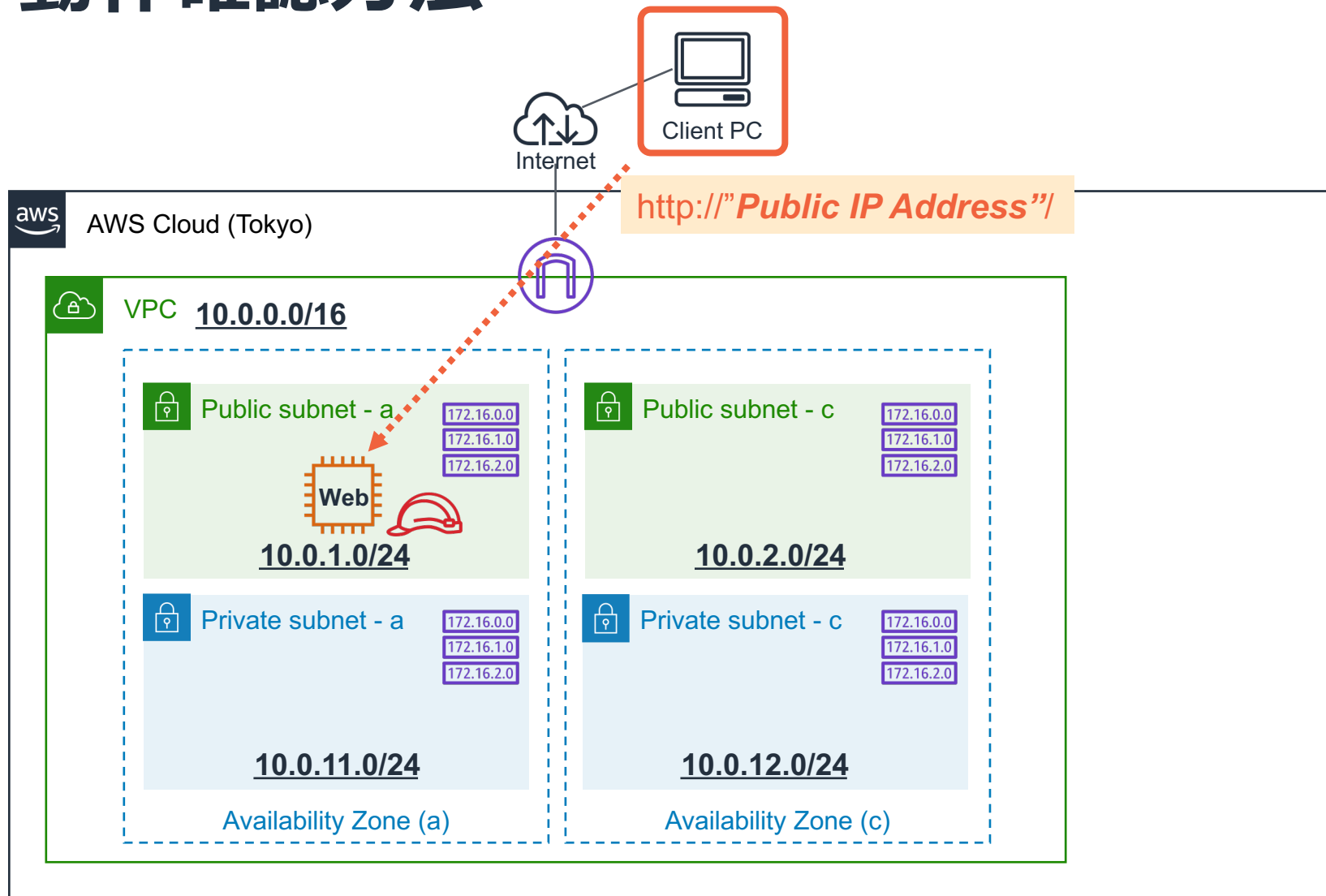


Amazon EC2



IAM Role

動作確認方法



ハンズオンで学ぶサービス・機能



Amazon VPC



Public/Private Subnet



Internet gateway



Route table

ハンズオンの中で関わるサービス・機能



AWS Systems Manager

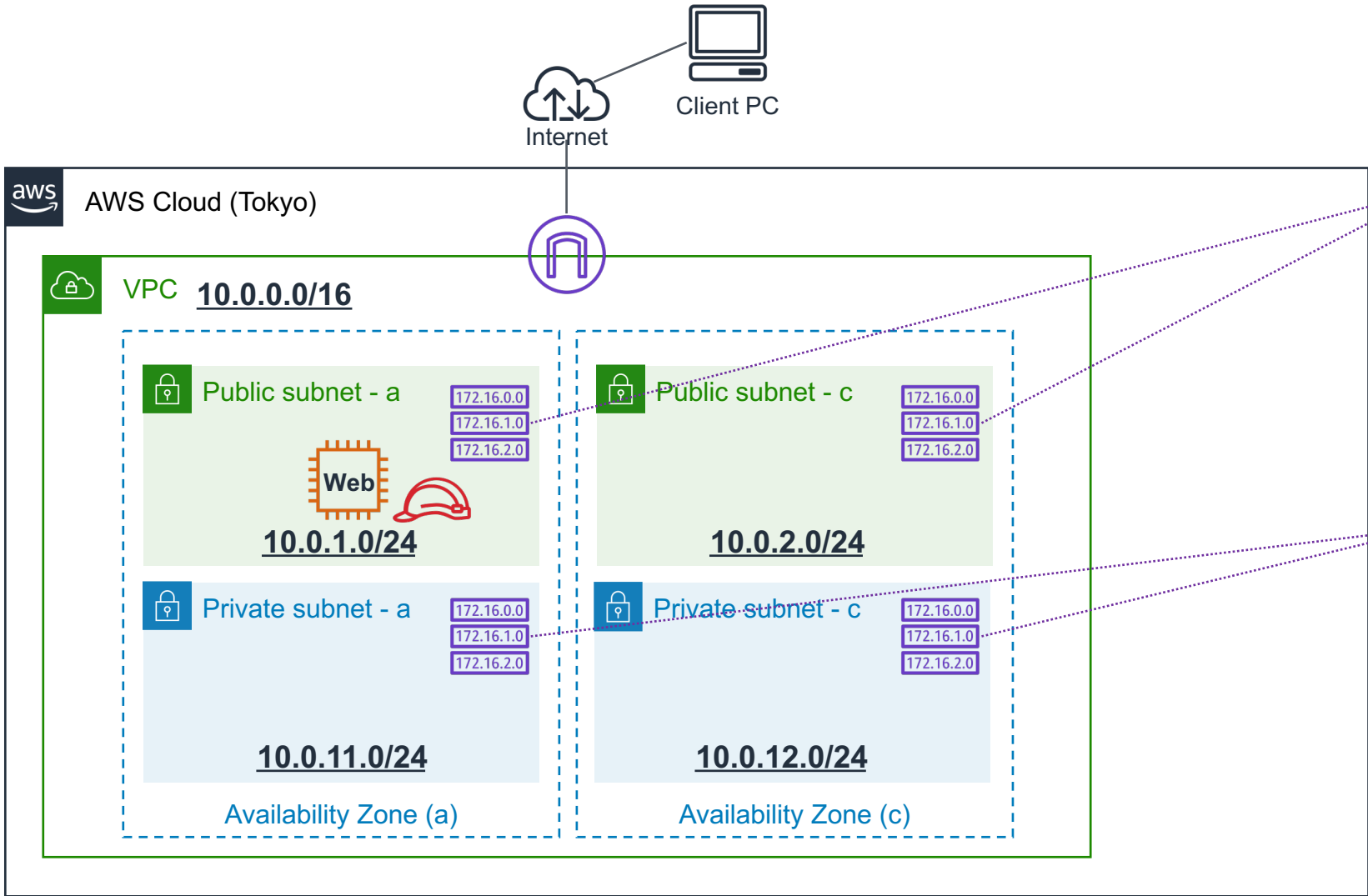


Amazon EC2



IAM Role

動作確認の実施手順



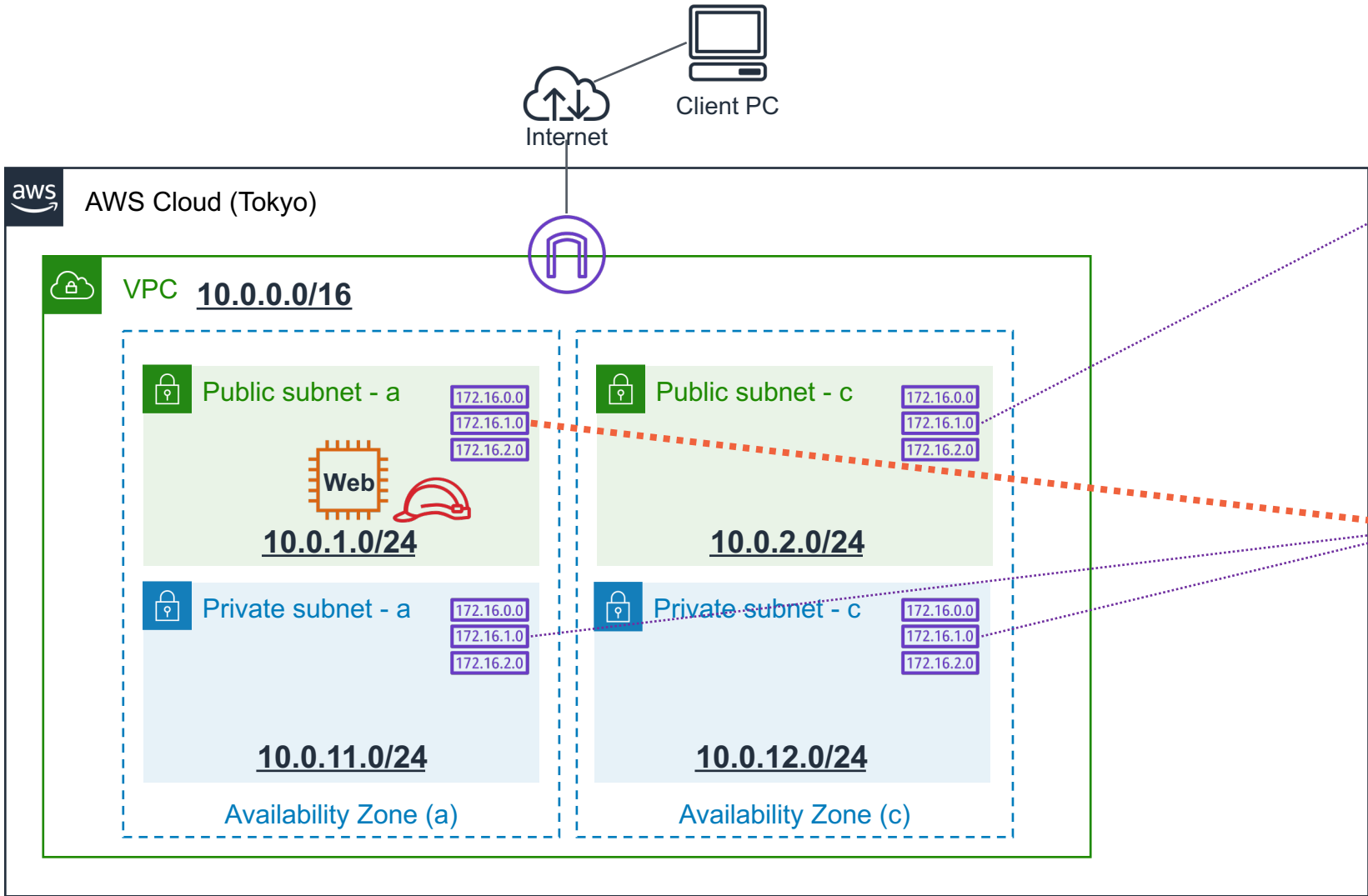
Public Route Table

送信先	ターゲット
10.0.0.0/16	local
0.0.0.0/0	Internet Gateway

Private Route Table(メイン)

送信先	ターゲット
10.0.0.0/16	local

動作確認の実施手順



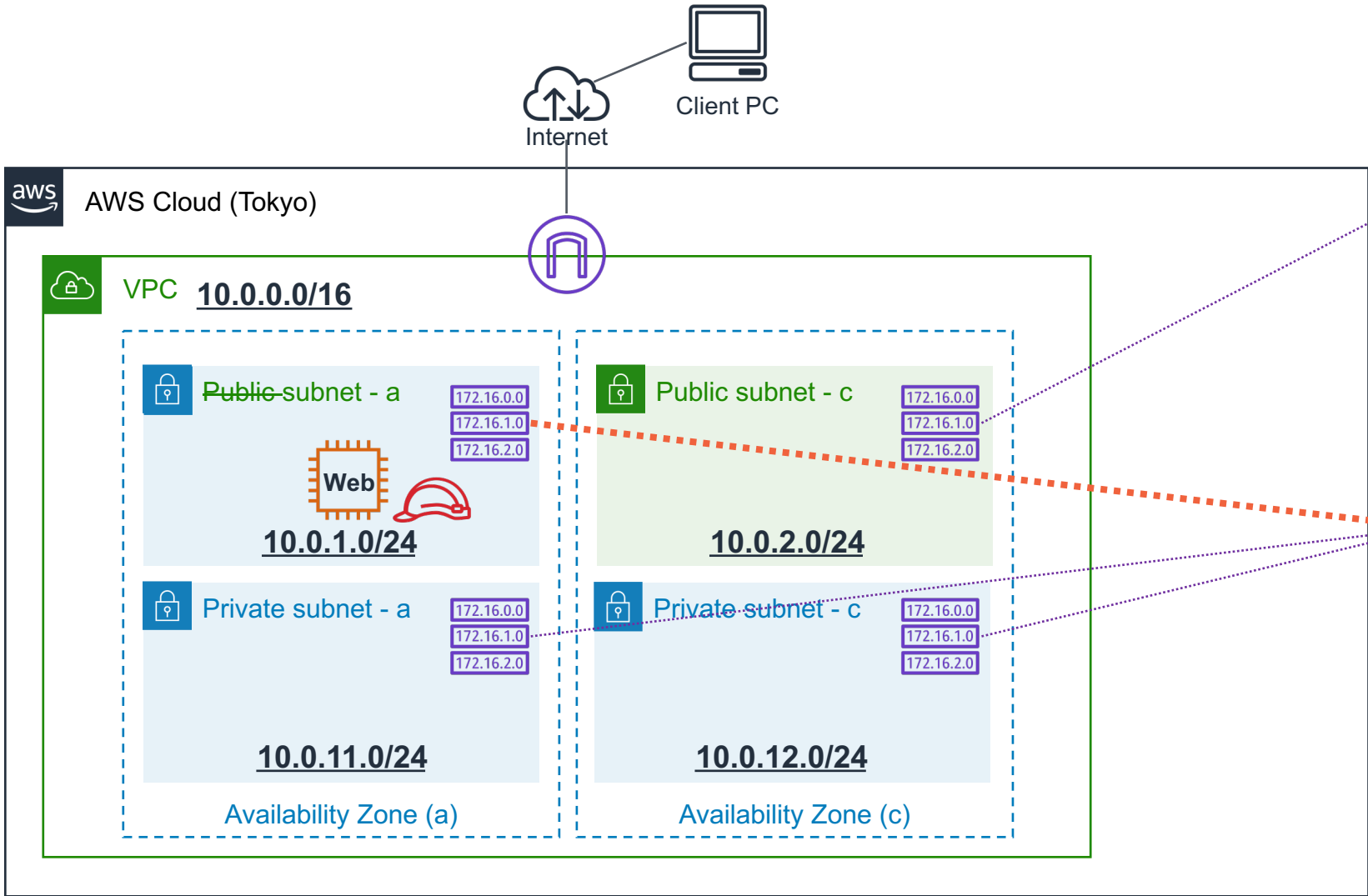
Public Route Table

送信先	ターゲット
10.0.0.0/16	local
0.0.0.0/0	Internet Gateway

Private Route Table(メイン)

送信先	ターゲット
10.0.0.0/16	local

動作確認の実施手順



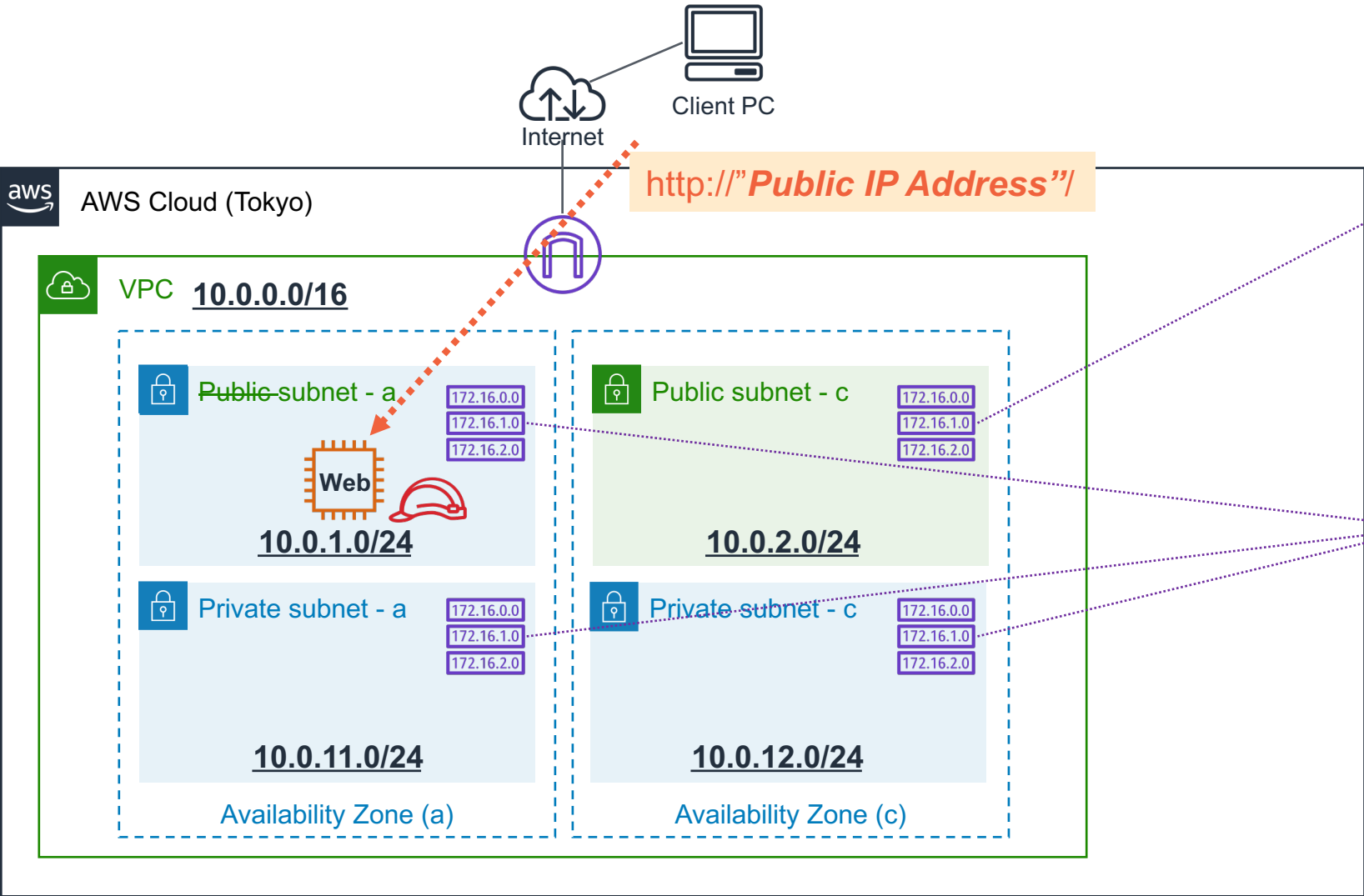
Public Route Table

送信先	ターゲット
10.0.0.0/16	local
0.0.0.0/0	Internet Gateway

Private Route Table(メイン)

送信先	ターゲット
10.0.0.0/16	local

動作確認の実施手順



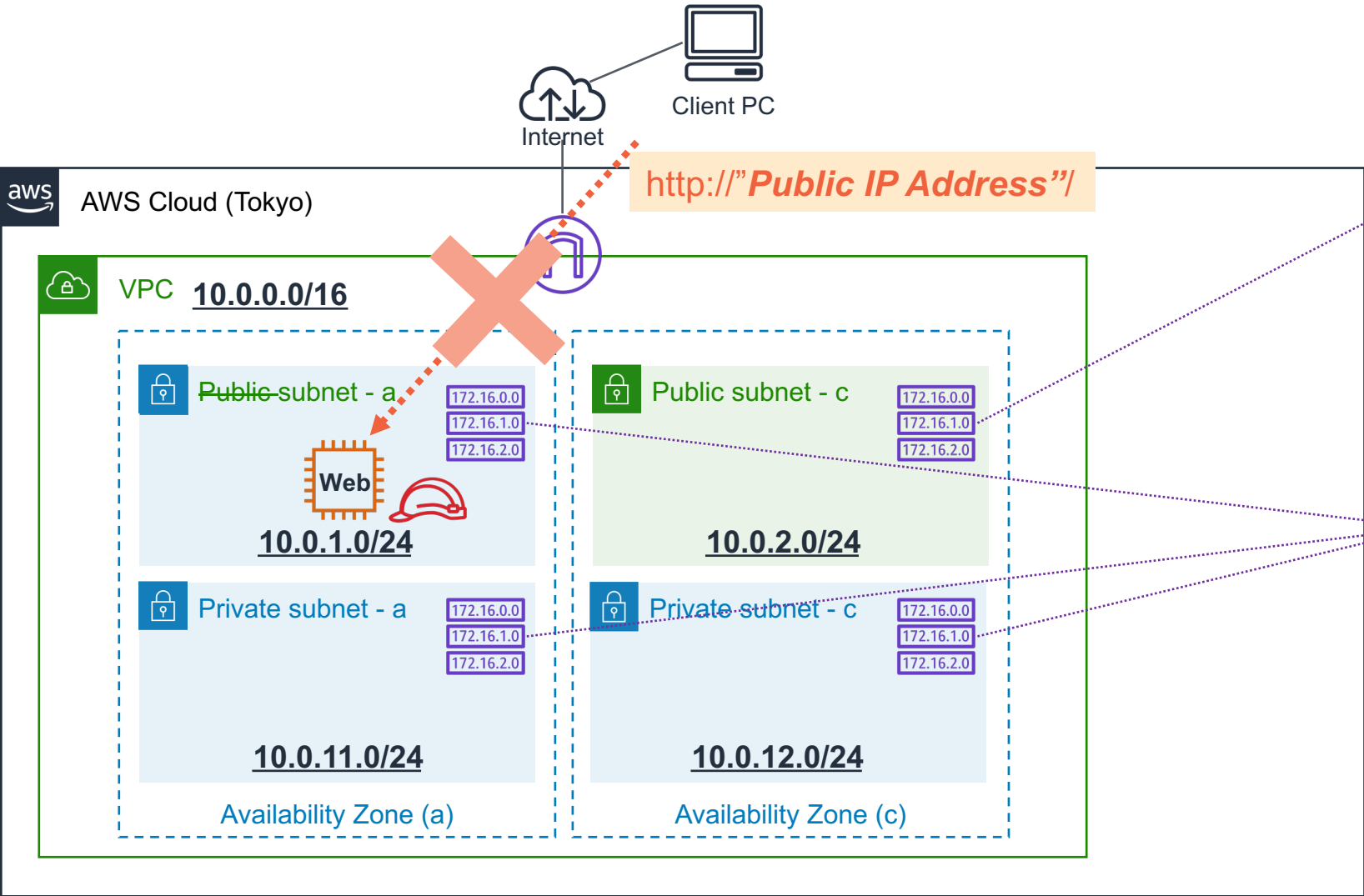
Public Route Table

送信先	ターゲット
10.0.0.0/16	local
0.0.0.0/0	Internet Gateway

Private Route Table(メイン)

送信先	ターゲット
10.0.0.0/16	local

動作確認の実手順



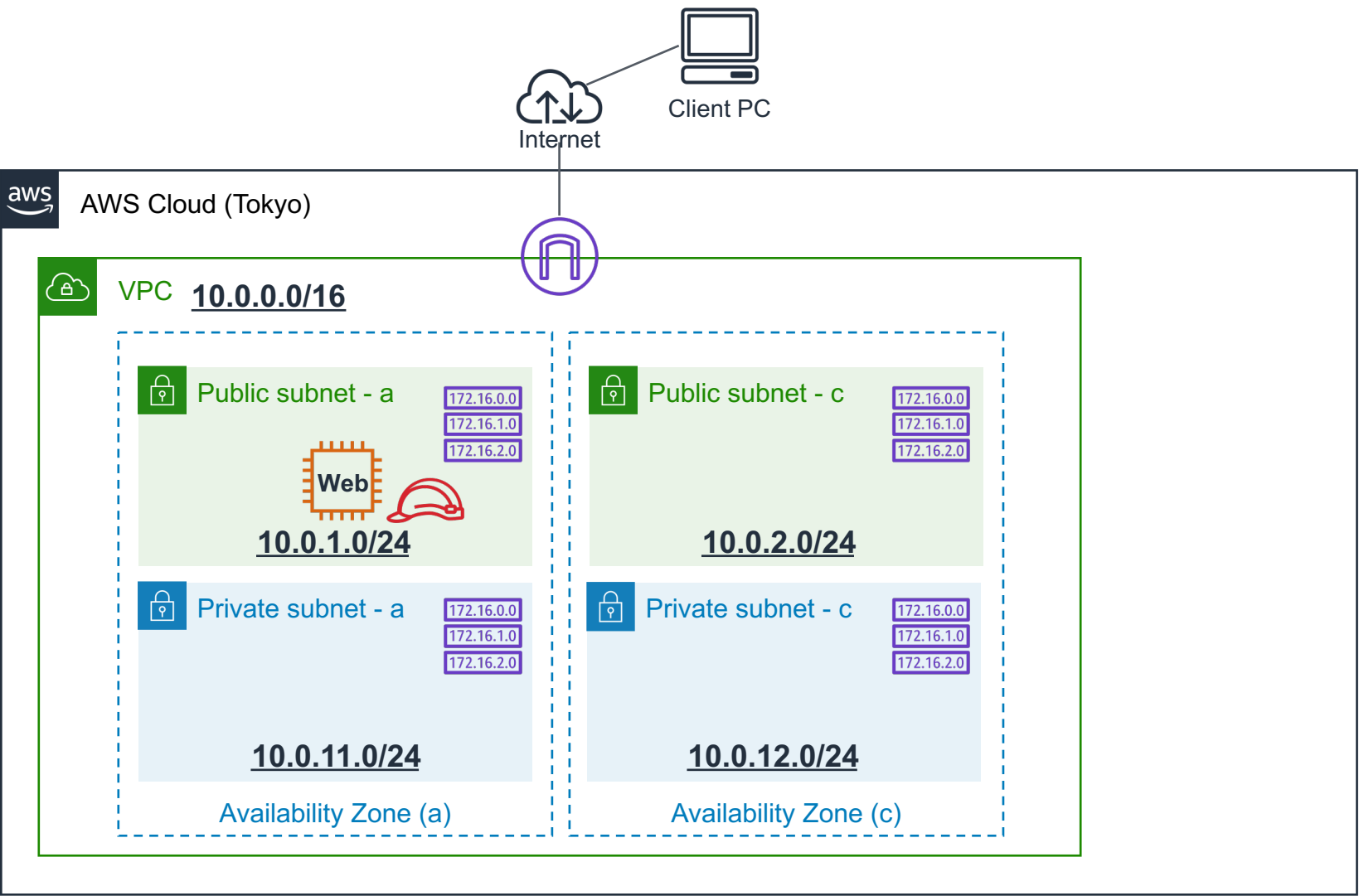
Public Route Table

送信先	ターゲット
10.0.0.0/16	local
0.0.0.0/0	Internet Gateway





Private Route Table(メイン)

送信先	ターゲット
10.0.0.0/16	local




現在の構成



ハンズオンで学ぶサービス・機能

-  Amazon VPC
-  Public/Private Subnet
-  Internet gateway
-  Route table

ハンズオンの中で関わるサービス・機能

-  AWS Systems Manager
-  Amazon EC2
-  IAM Role

パブリックサブネット と プライベートサブネット

- パブリックサブネット

- ルーティングテーブルにインターネットゲートウェイへのエントリがあり、インターネットとインバウンド/アウトバウンドのアクセスが可能

- プライベートサブネット

- ルーティングテーブルにインターネットゲートウェイへのエントリはなく、インターネットから直接アクセスできない



【AWS Hands-on for Beginners】

Network 編 #1-6

AWS上にセキュアなプライベートネットワーク空間を作成

アマゾン ウェブ サービス ジャパン合同会社

パートナー ソリューション アーキテクト

江口 智 / Tomo Eguchi

(収録日: 2022/5/8)

このコースの Agenda

1. AWS

1. 前提知識の確認
2. AWSでのネットワークの考え方
3. 本ハンズオンの最終構成図

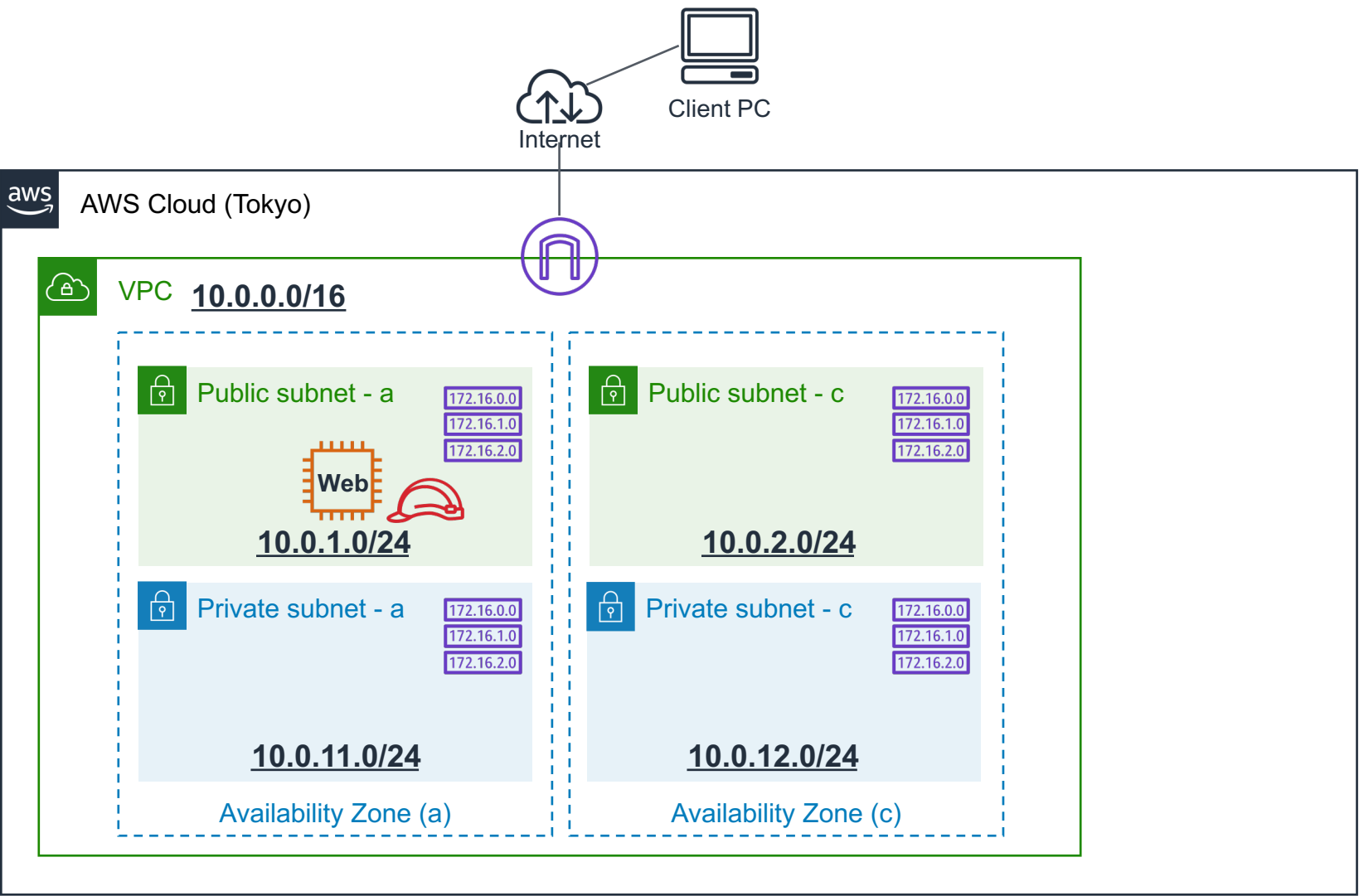
2. Amazon VPC ハンズオン

1. Amazon VPC ハンズオン① Amazon VPC の作成とインターネット接続環境の構築
2. Amazon VPC ハンズオン② ルートテーブルによる経路設定を理解する
- 3. Amazon VPC ハンズオン③ プライベートサブネットからインターネットへのアクセス方法**
4. Amazon VPC ハンズオン④ VPC外サービスへの接続方法 - 1
5. Amazon VPC ハンズオン⑤ VPC外サービスへの接続方法 - 2





3. 本コースのまとめ






現在の構成



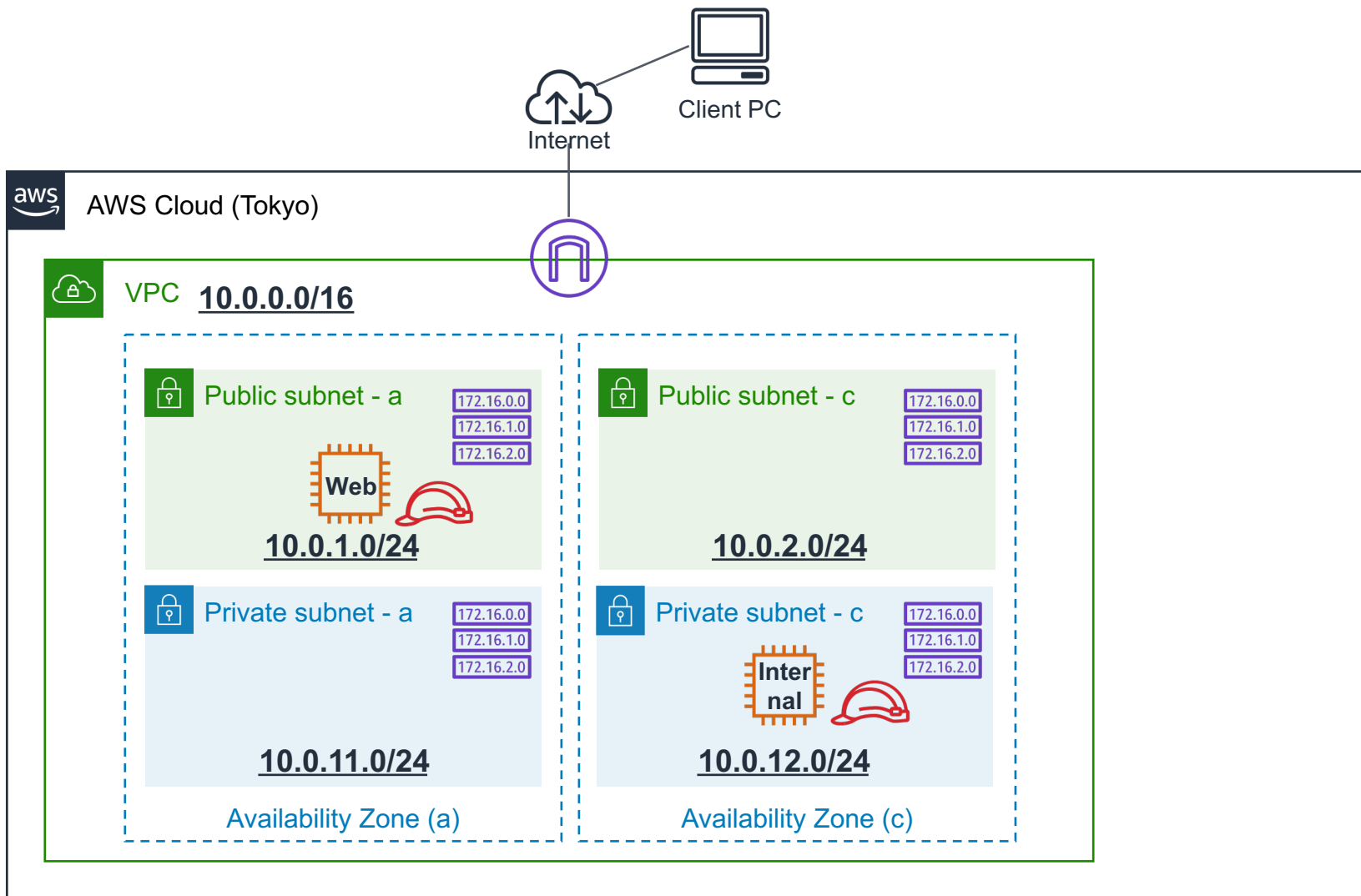
ハンズオンで学ぶサービス・機能

-  Amazon VPC
-  Public/Private Subnet
-  Internet gateway
-  Route table

ハンズオンの中で関わるサービス・機能

-  AWS Systems Manager
-  Amazon EC2
-  IAM Role

プライベートサブネットへの配置



ハンズオンで学ぶサービス・機能



Amazon VPC



Public/Private Subnet



Internet gateway



Route table

ハンズオンの中で関わるサービス・機能



AWS Systems Manager

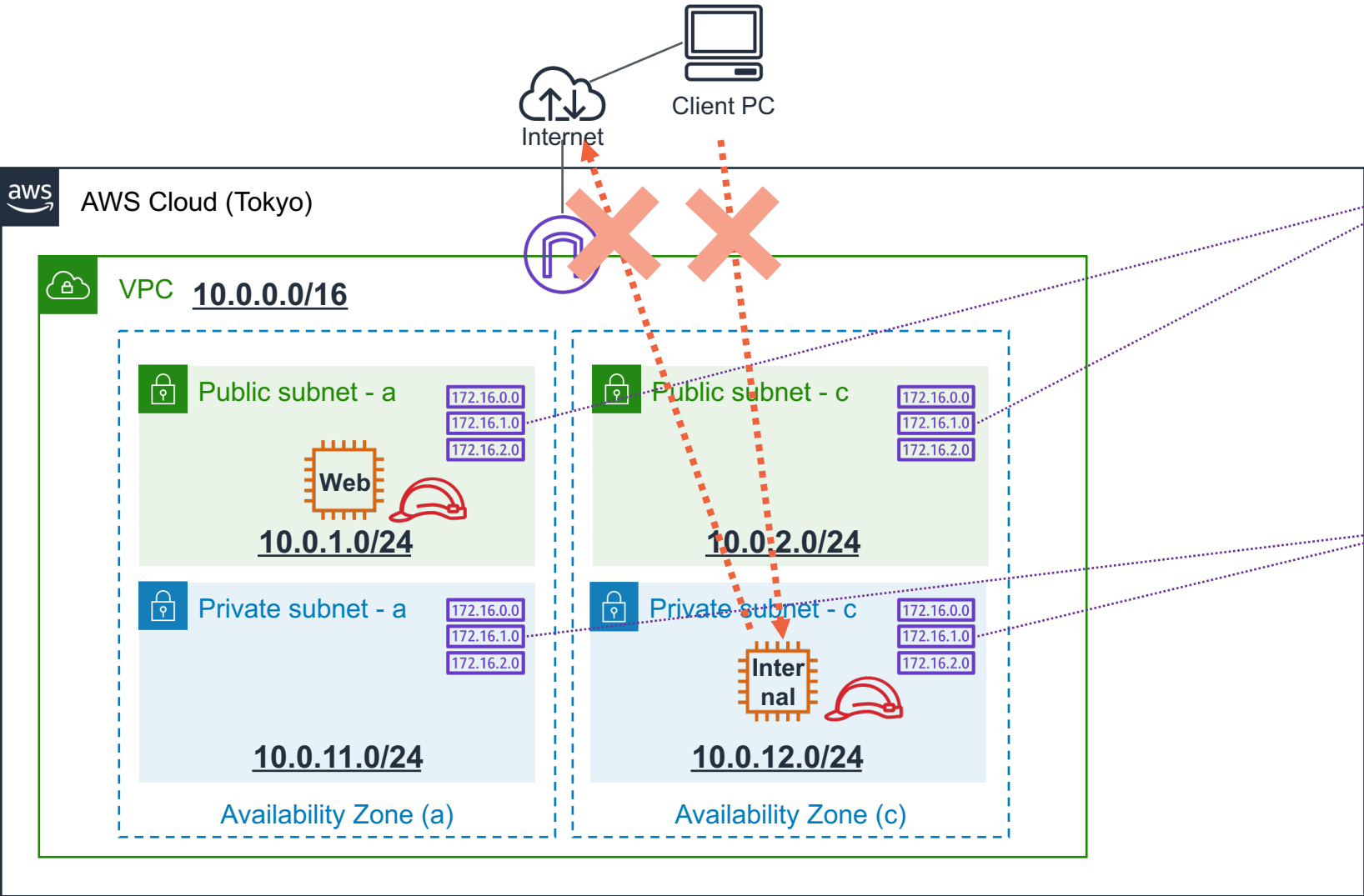


Amazon EC2



IAM Role

プライベートサブネットへの配置



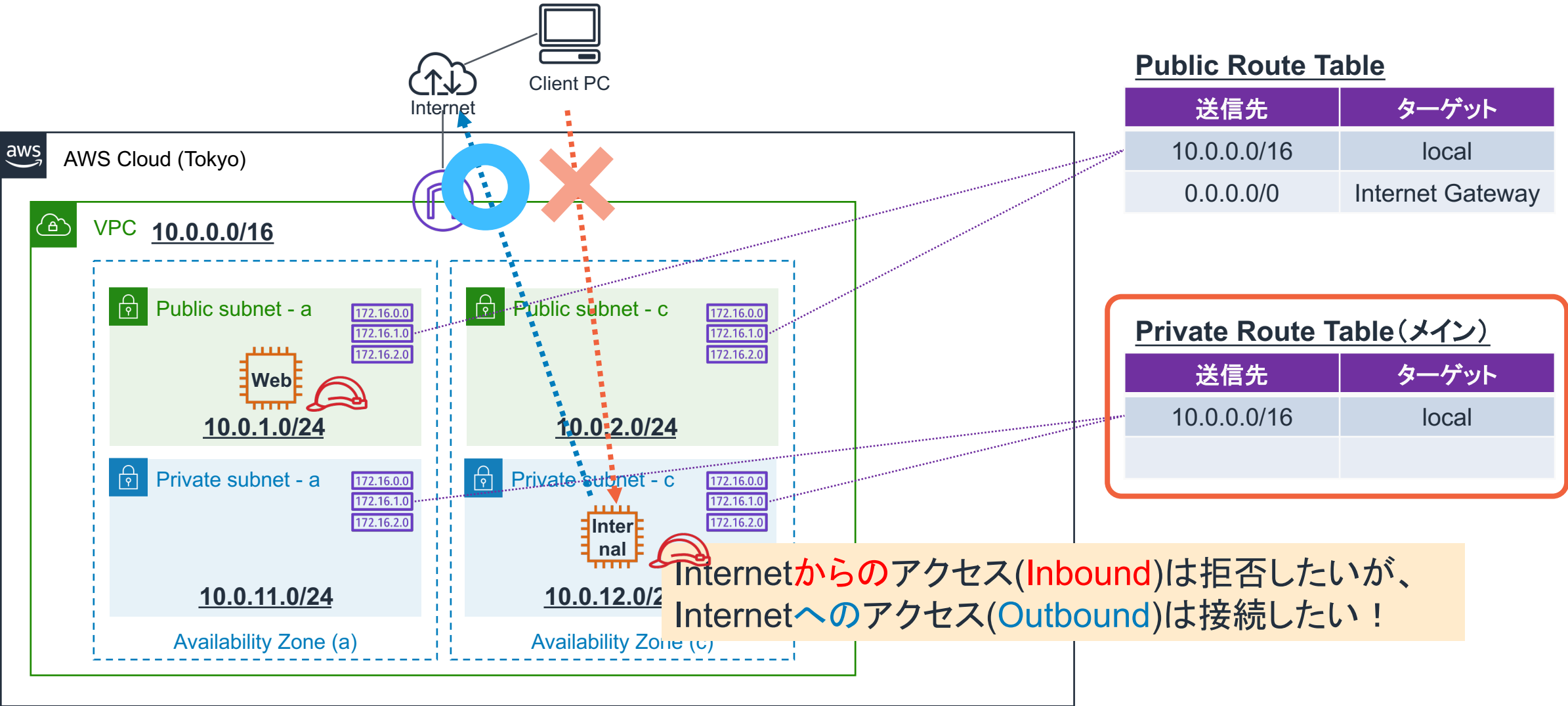
Public Route Table

送信先	ターゲット
10.0.0.0/16	local
0.0.0.0/0	Internet Gateway

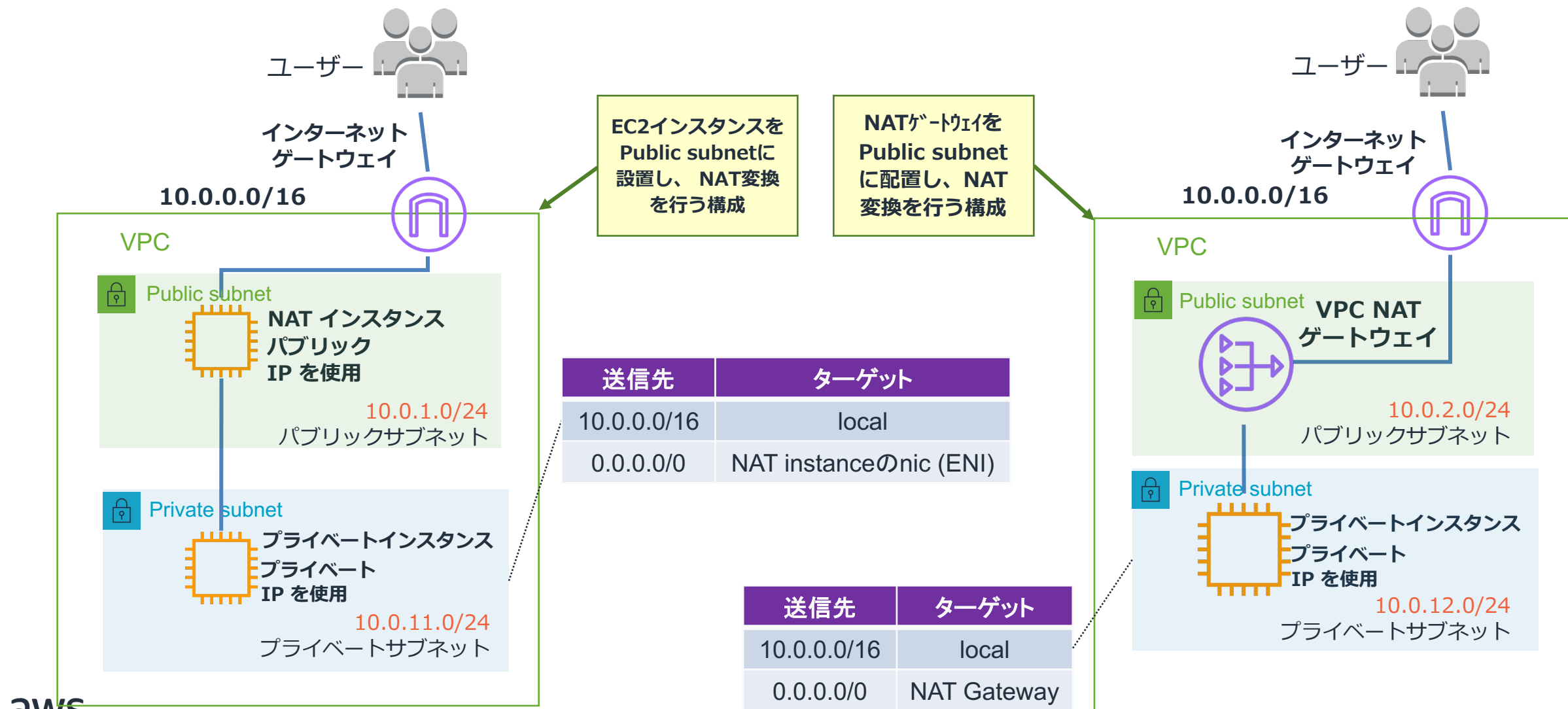
Private Route Table(メイン)

送信先	ターゲット
10.0.0.0/16	local

プライベートサブネットへの配置（実現したいこと）



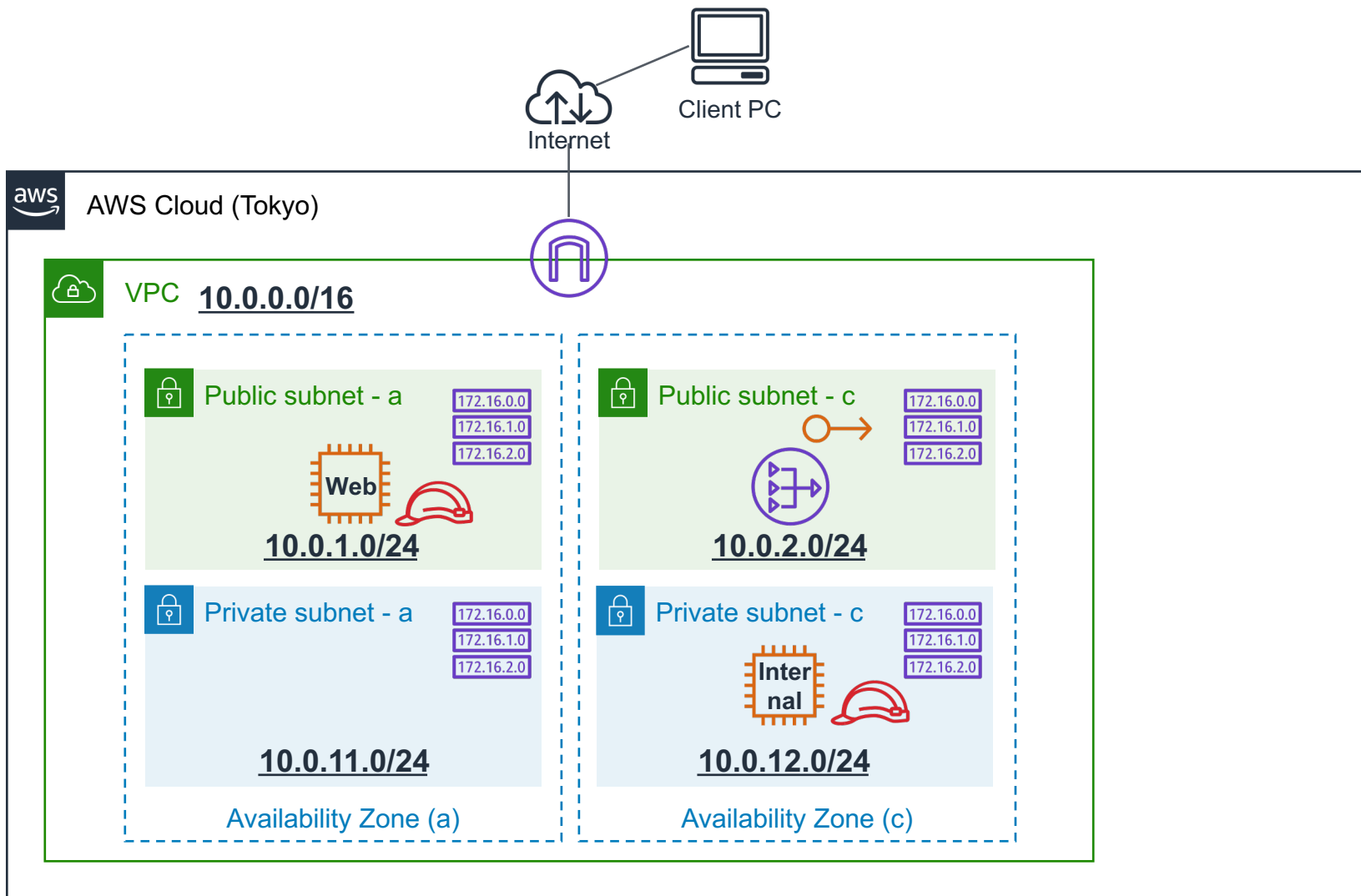
NAT instance / NAT Gateway



NAT instance / NAT Gateway 機能比較

	NAT インスタンス	NAT ゲートウェイ
可用性	スクリプトを使って フェイルオーバーを管理	デフォルトで可用性が高い
帯域幅	インスタンスタイプの 帯域幅に基づく	5 Gbps 45 Gbps まで自動的に拡張
メンテナンス	自分で管理	AWS で管理
セキュリティ	セキュリティグループと NACL	NACL
ポートフォワーディング	サポートあり	サポートなし
範囲	アベイラビリティーゾーン	アベイラビリティーゾーン

プライベートサブネットへの配置



ハンズオンで学ぶサービス・機能



Amazon VPC



Public/Private Subnet



Internet gateway



Route table



NAT Gateway



Elastic IP address

ハンズオンの中で関わるサービス・機能



AWS Systems Manager

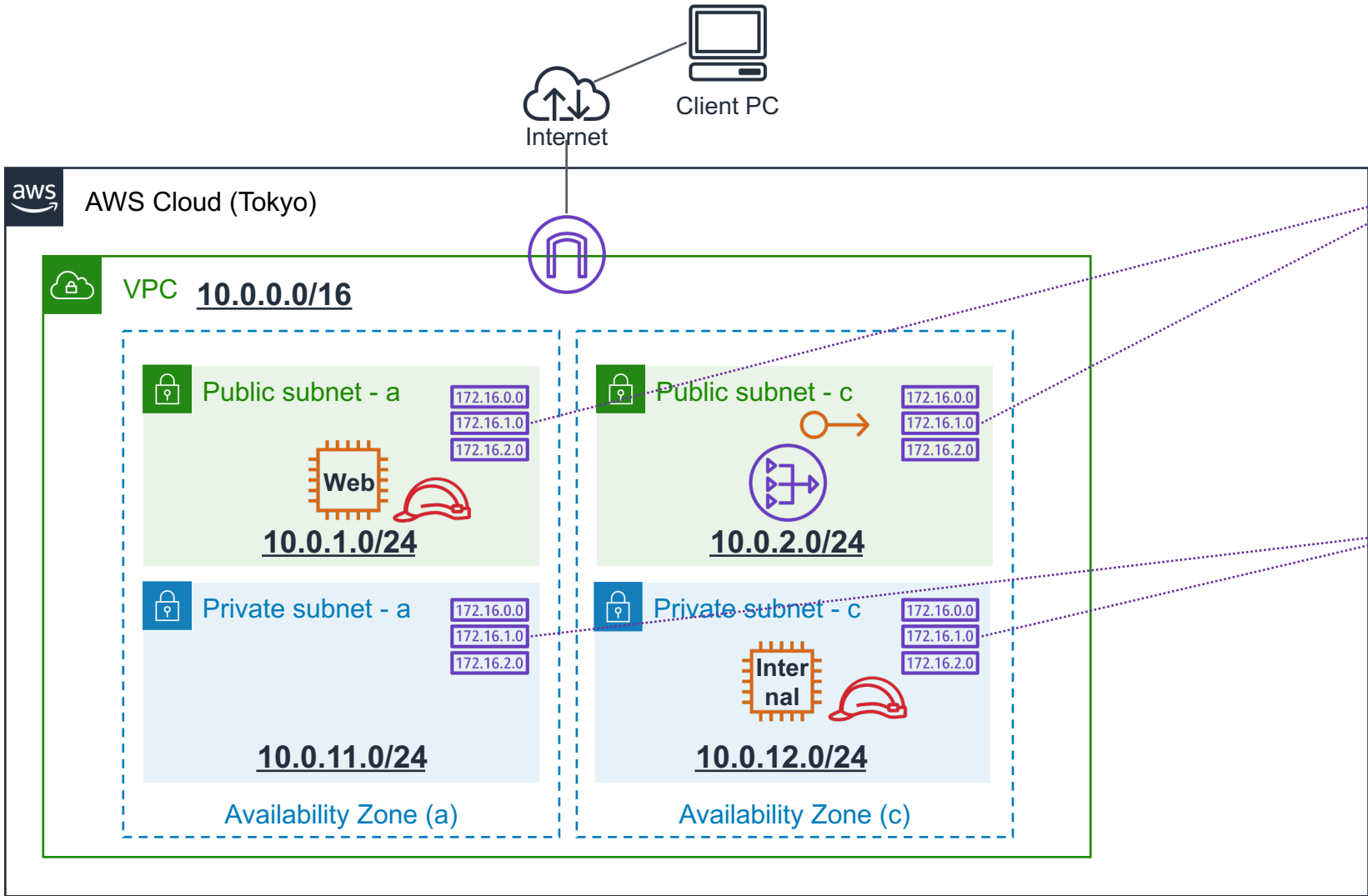


Amazon EC2



IAM Role

プライベートサブネットへの配置



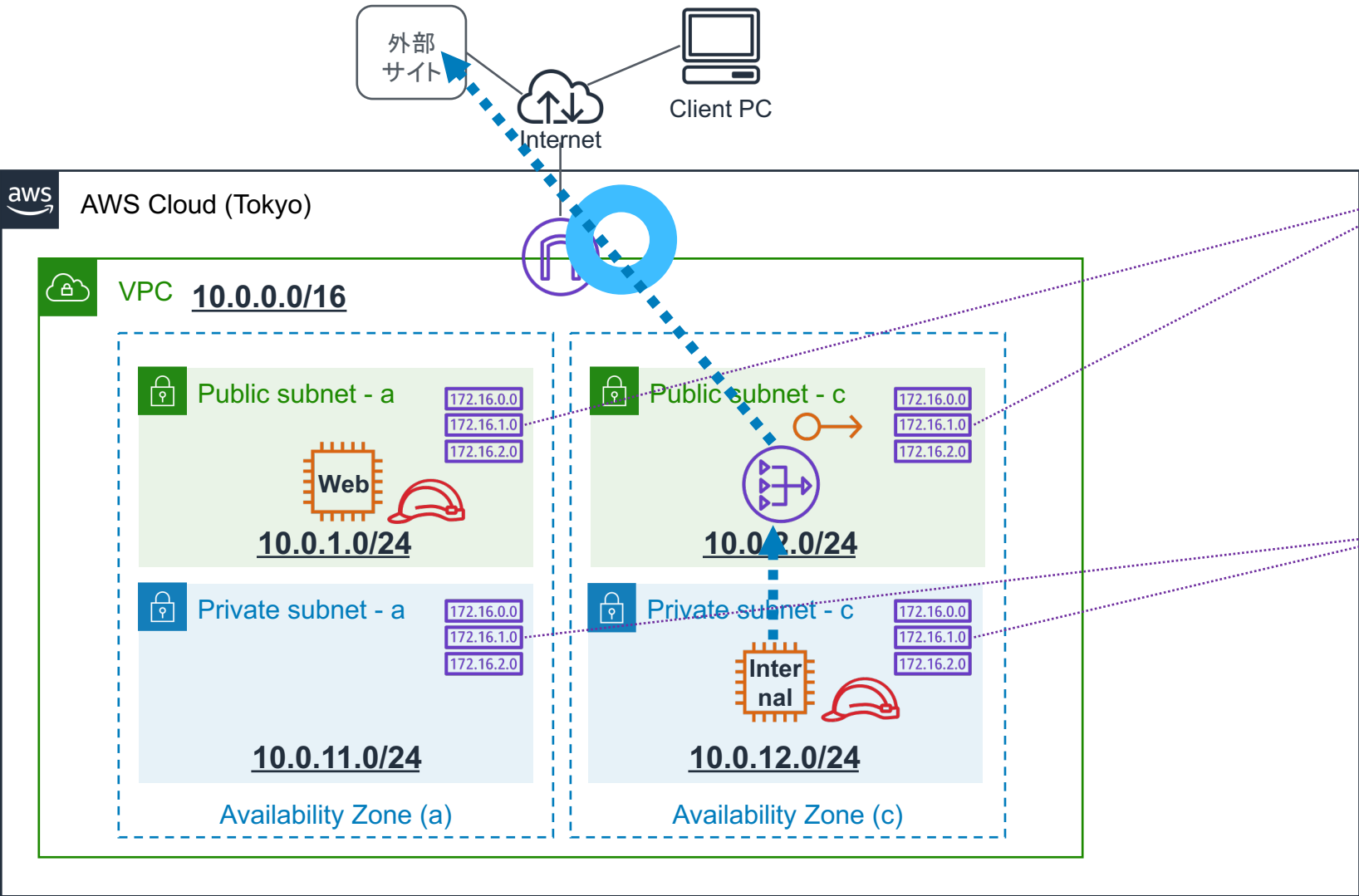
Public Route Table

送信先	ターゲット
10.0.0.0/16	local
0.0.0.0/0	Internet Gateway

Private Route Table (メイン)

送信先	ターゲット
10.0.0.0/16	local
0.0.0.0/0	Nat Gateway

プライベートサブネットへの配置



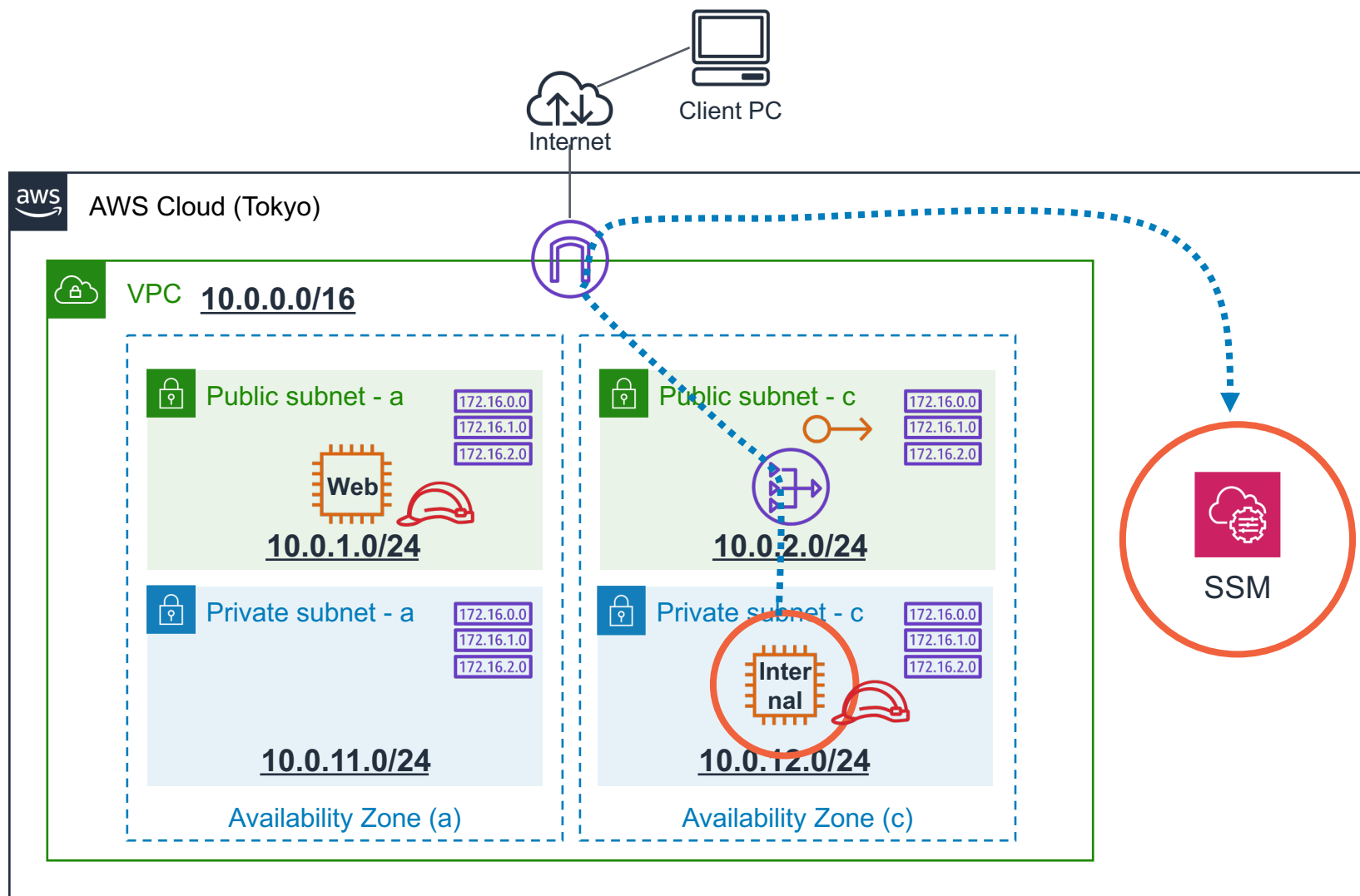
Public Route Table

送信先	ターゲット
10.0.0.0/16	local
0.0.0.0/0	Internet Gateway






Private Route Table(メイン)

送信先	ターゲット
10.0.0.0/16	local
0.0.0.0/0	Nat Gateway

VPC外マネージドサービスへの接続






ハンズオンで学ぶサービス・機能

-  Amazon VPC
-  Public/Private Subnet
-  Internet gateway
-  Route table
-  NAT Gateway

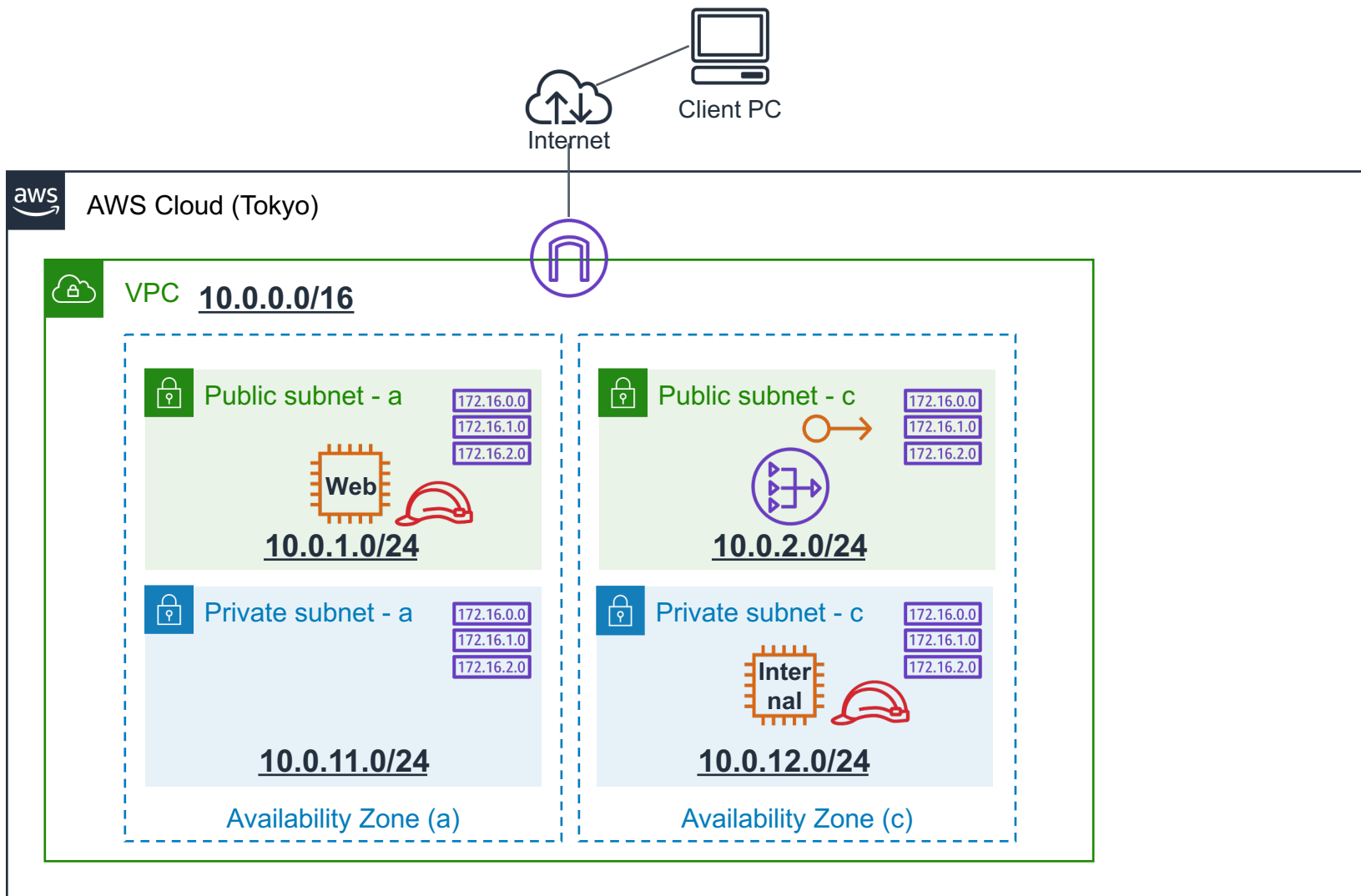
 Elastic IP address

SSM

ハンズオンの中で関わるサービス・機能

-  AWS Systems Manager
-  Amazon EC2
-  IAM Role

プライベートサブネットへの配置



ハンズオンで学ぶサービス・機能



Amazon VPC



Public/Private Subnet



Internet gateway



Route table



NAT Gateway



Elastic IP address

ハンズオンの中で関わるサービス・機能



AWS Systems Manager

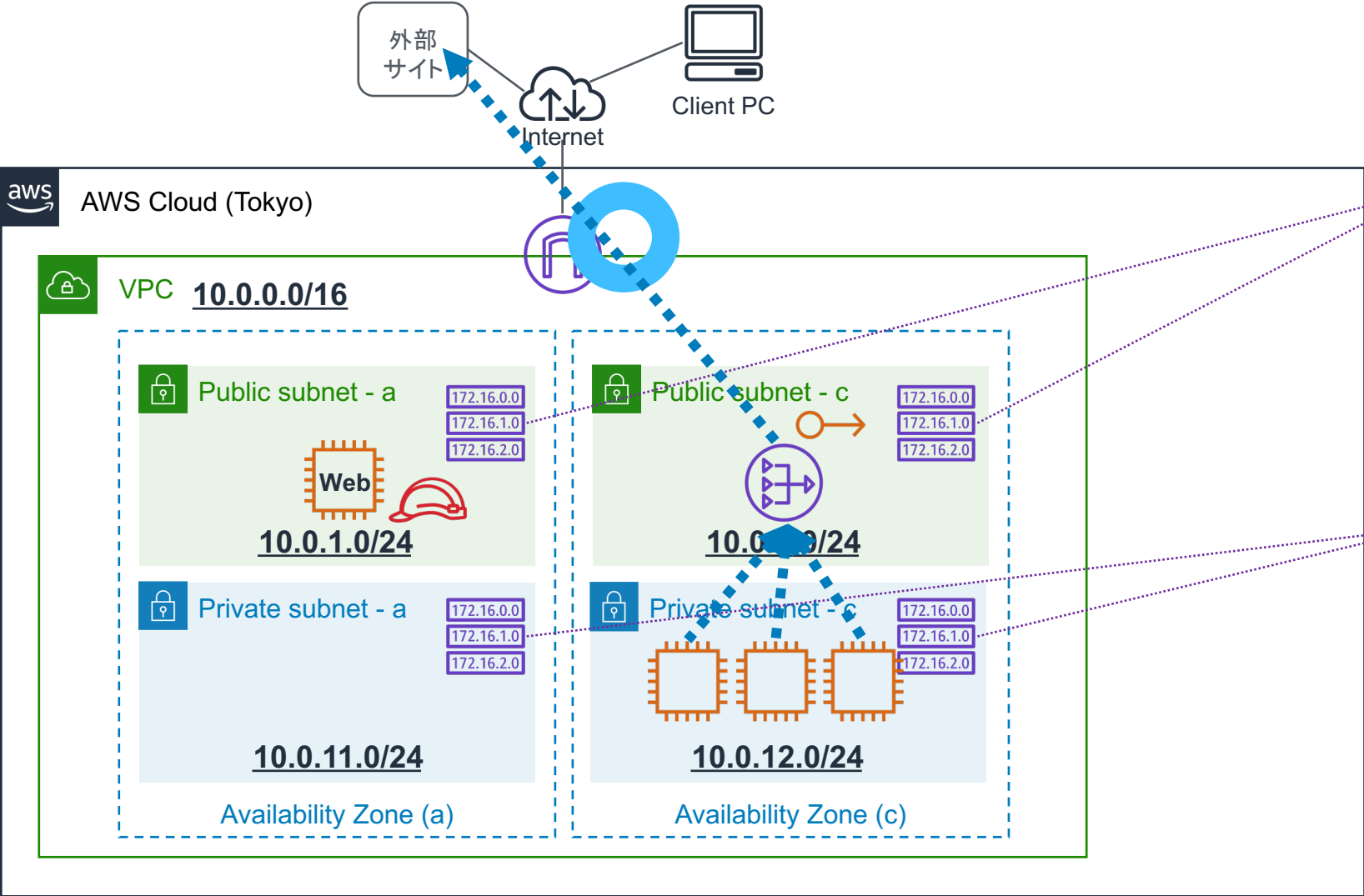


Amazon EC2



IAM Role

プライベートサブネットへの配置



Public Route Table

送信先	ターゲット
10.0.0.0/16	local
0.0.0.0/0	Internet Gateway

Private Route Table(メイン)

送信先	ターゲット
10.0.0.0/16	local
0.0.0.0/0	Nat Gateway

パブリックサブネット と プライベートサブネット (更新)

- パブリックサブネット

- ルーティングテーブルにインターネットゲートウェイへのエントリがあり、インターネットとインバウンド/アウトバウンドのアクセスが可能

- プライベートサブネット

- ルーティングテーブルにインターネットゲートウェイへのエントリはなく、インターネットから直接アクセスできない

- パブリックサブネットに設置したNATやプロキシを経由することで、インターネットへのアウトバウンドのアクセスが可能



【AWS Hands-on for Beginners】

Network 編 #1-7

AWS上にセキュアなプライベートネットワーク空間を作成

アマゾン ウェブ サービス ジャパン合同会社

パートナー ソリューション アーキテクト

江口 智 / Tomo Eguchi

(収録日: 2022/5/8)

このコースの Agenda

1. AWS

1. 前提知識の確認
2. AWSでのネットワークの考え方
3. 本ハンズオンの最終構成図

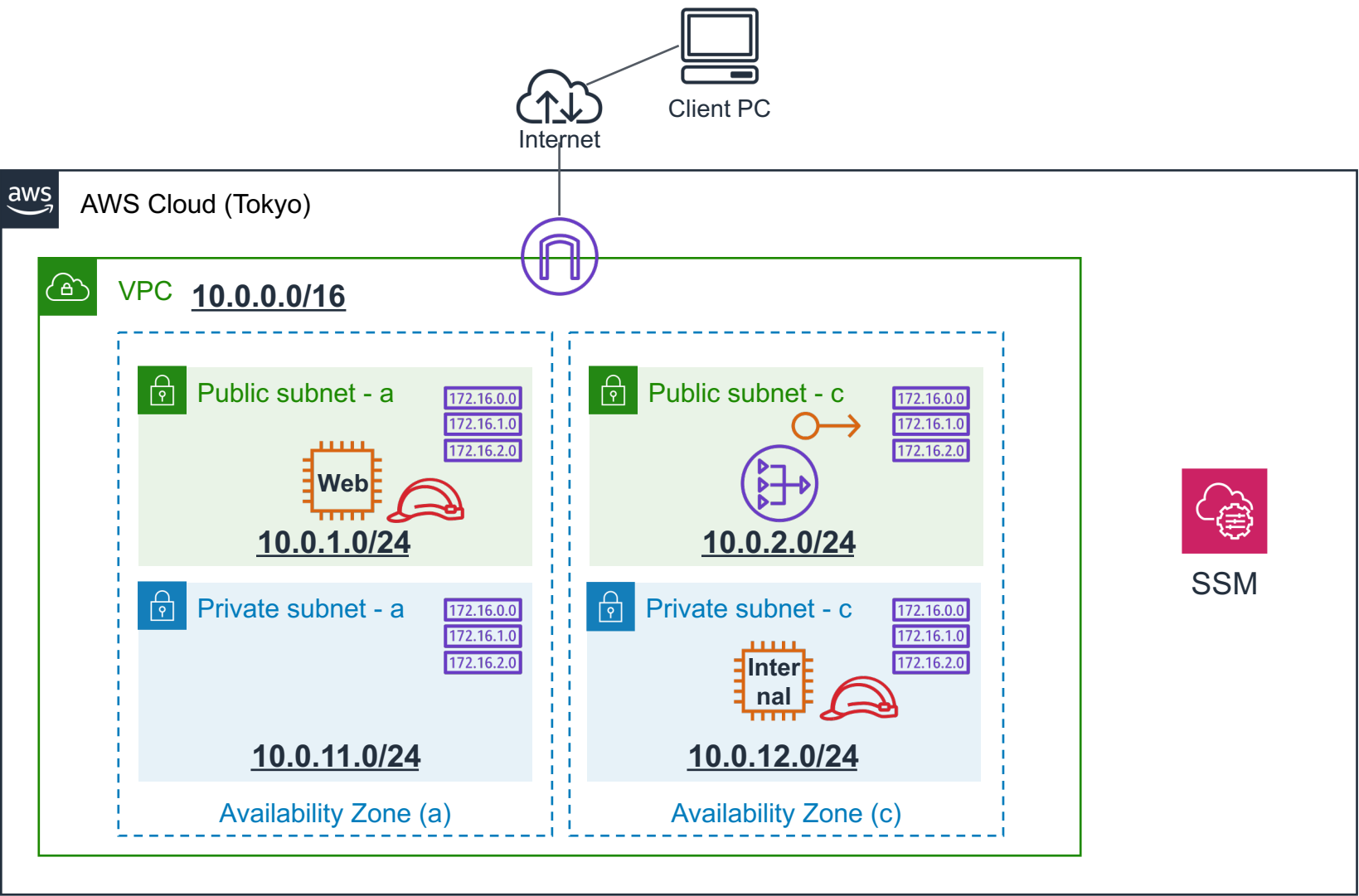
2. Amazon VPC ハンズオン

1. Amazon VPC ハンズオン① Amazon VPC の作成とインターネット接続環境の構築
2. Amazon VPC ハンズオン② ルートテーブルによる経路設定を理解する
3. Amazon VPC ハンズオン③ プライベートサブネットからインターネットへのアクセス方法
- 4. Amazon VPC ハンズオン④ VPC外サービスへの接続方法 - 1**
5. Amazon VPC ハンズオン⑤ VPC外サービスへの接続方法 - 2

3. 本コースのまとめ



現在の構成



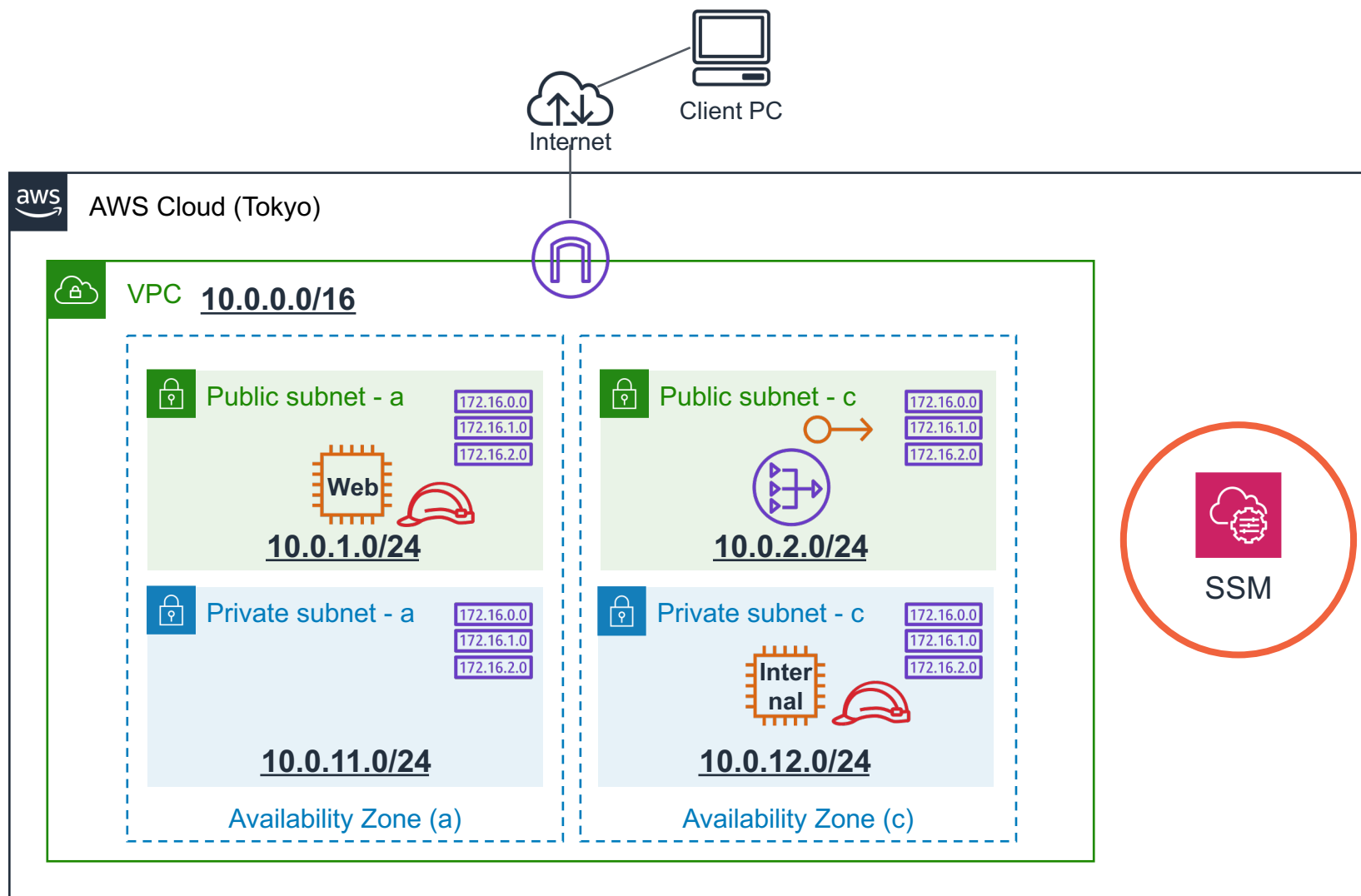
ハンズオンで学ぶサービス・機能

- Amazon VPC
- Public/Private Subnet
- Internet gateway
- Route table
- NAT gateway
- Elastic IP address

ハンズオンの中で関わるサービス・機能

- AWS Systems Manager
- Amazon EC2
- IAM Role

VPC外マネージドサービスへの接続



ハンズオンで学ぶサービス・機能



Amazon VPC



Public/Private Subnet



Internet gateway



Route table



NAT gateway



Elastic IP address

ハンズオンの中で関わるサービス・機能



AWS Systems Manager

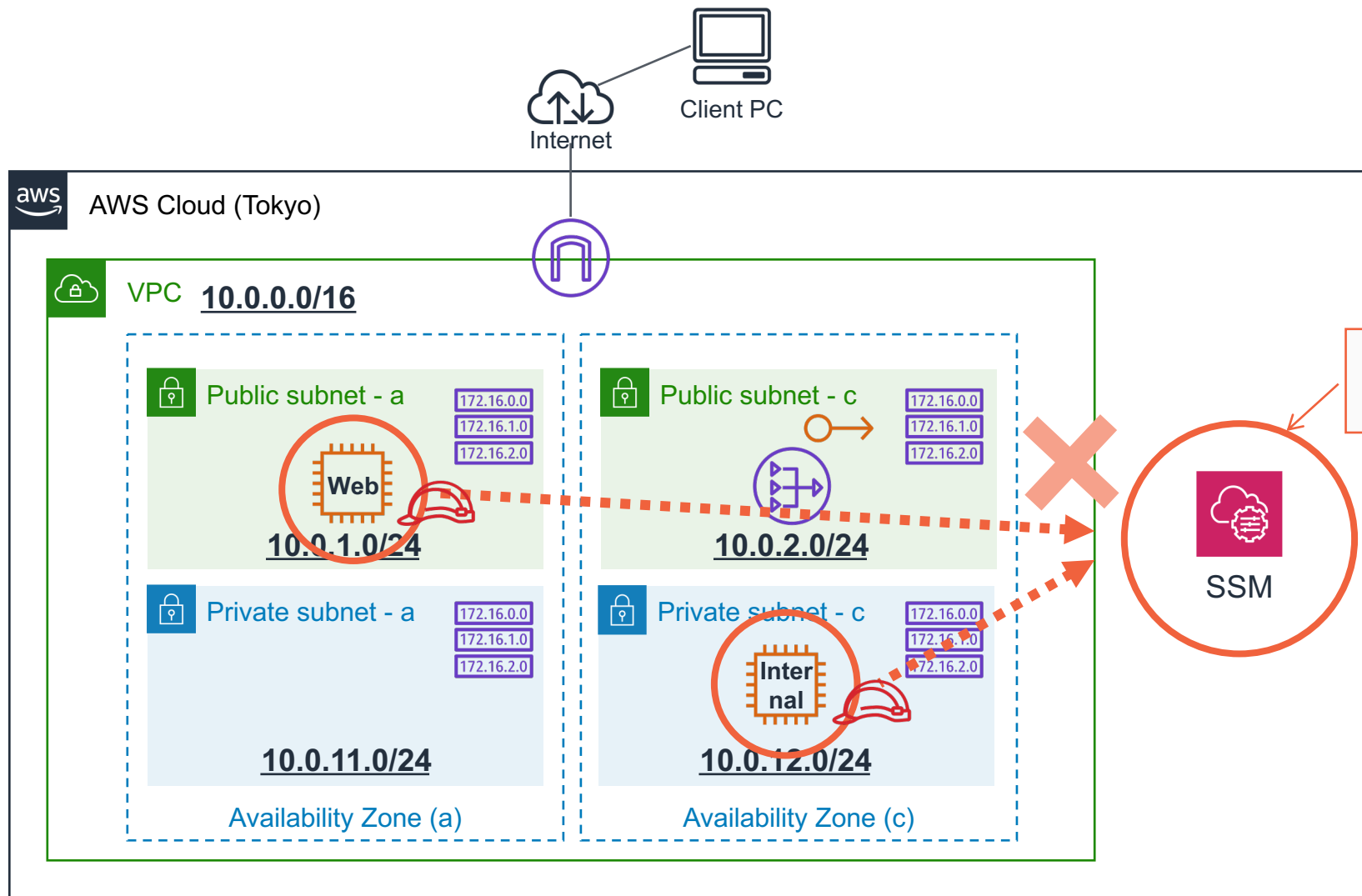


Amazon EC2








IAM Role

VPC外マネージドサービスへの接続



ハンズオンで学ぶサービス・機能


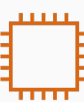

-  Amazon VPC
-  Public/Private Subnet
-  Internet gateway
-  Route table
-  NAT gateway

接続口(エンドポイント)はVPC外

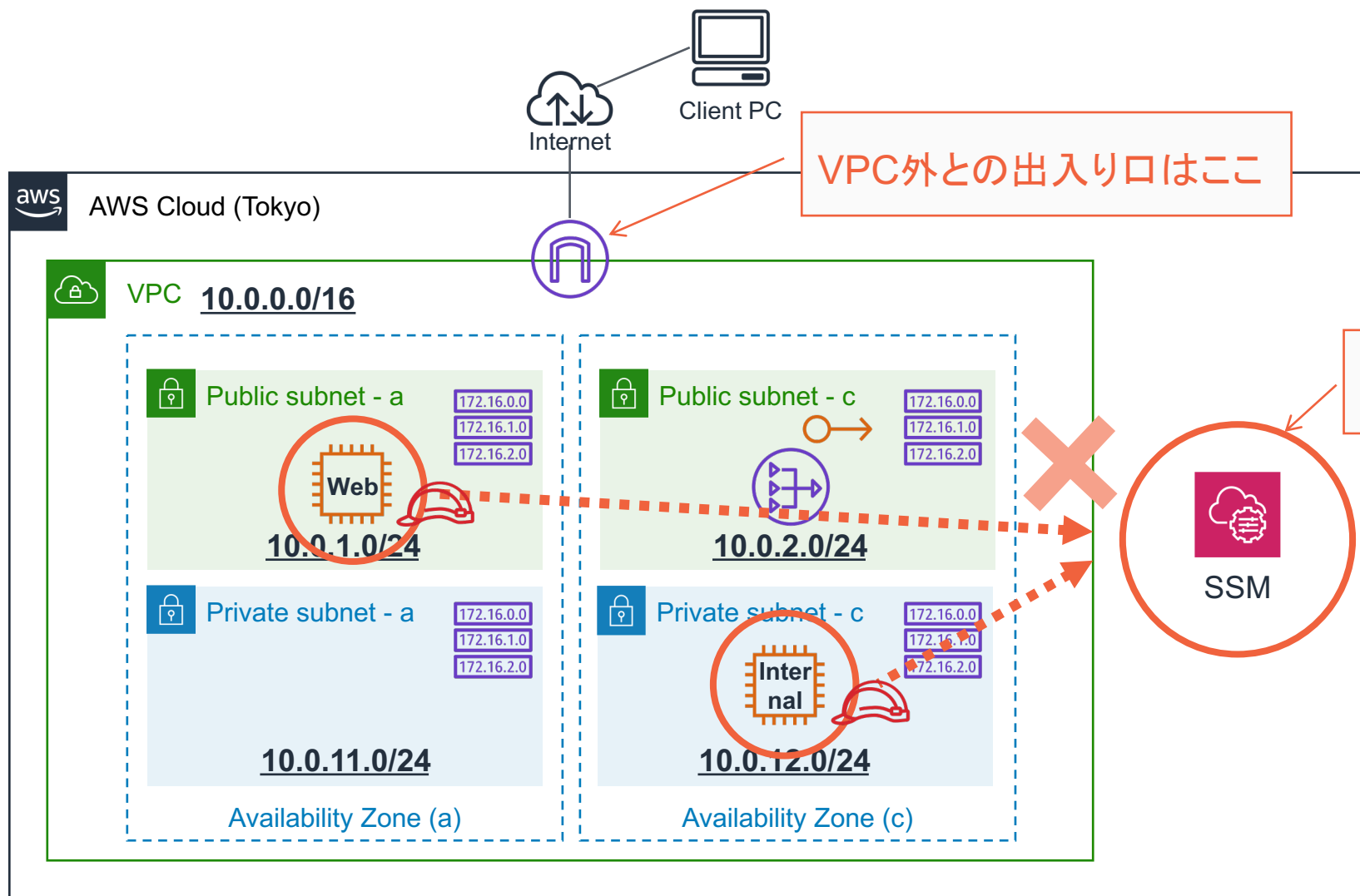
 Elastic IP address

SSM






ハンズオンの中で関わるサービス・機能

-  AWS Systems Manager
-  Amazon EC2
-  IAM Role

VPC外マネージドサービスへの接続






ハンズオンで学ぶサービス・機能

-  Amazon VPC
-  Public/Private Subnet
-  Internet gateway
-  Route table
-  NAT gateway

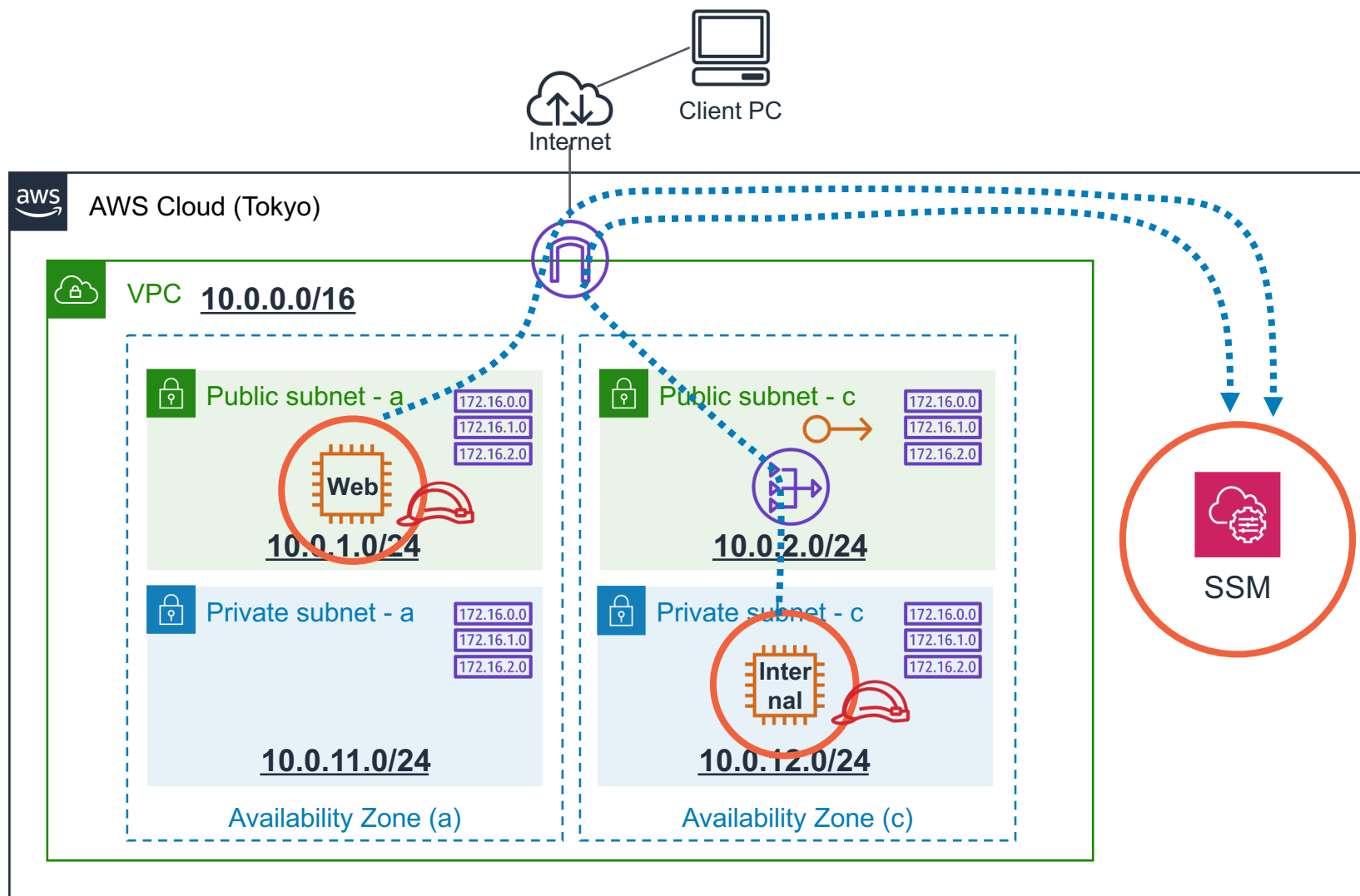
接続口(エンドポイント)
はVPC外

 Elastic IP address






ハンズオンの中で関わるサービス・機能

-  AWS Systems Manager
-  Amazon EC2
-  IAM Role

VPC外マネージドサービスへの接続




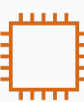

ハンズオンで学ぶサービス・機能

-  Amazon VPC
-  Public/Private Subnet
-  Internet gateway
-  Route table
-  NAT gateway

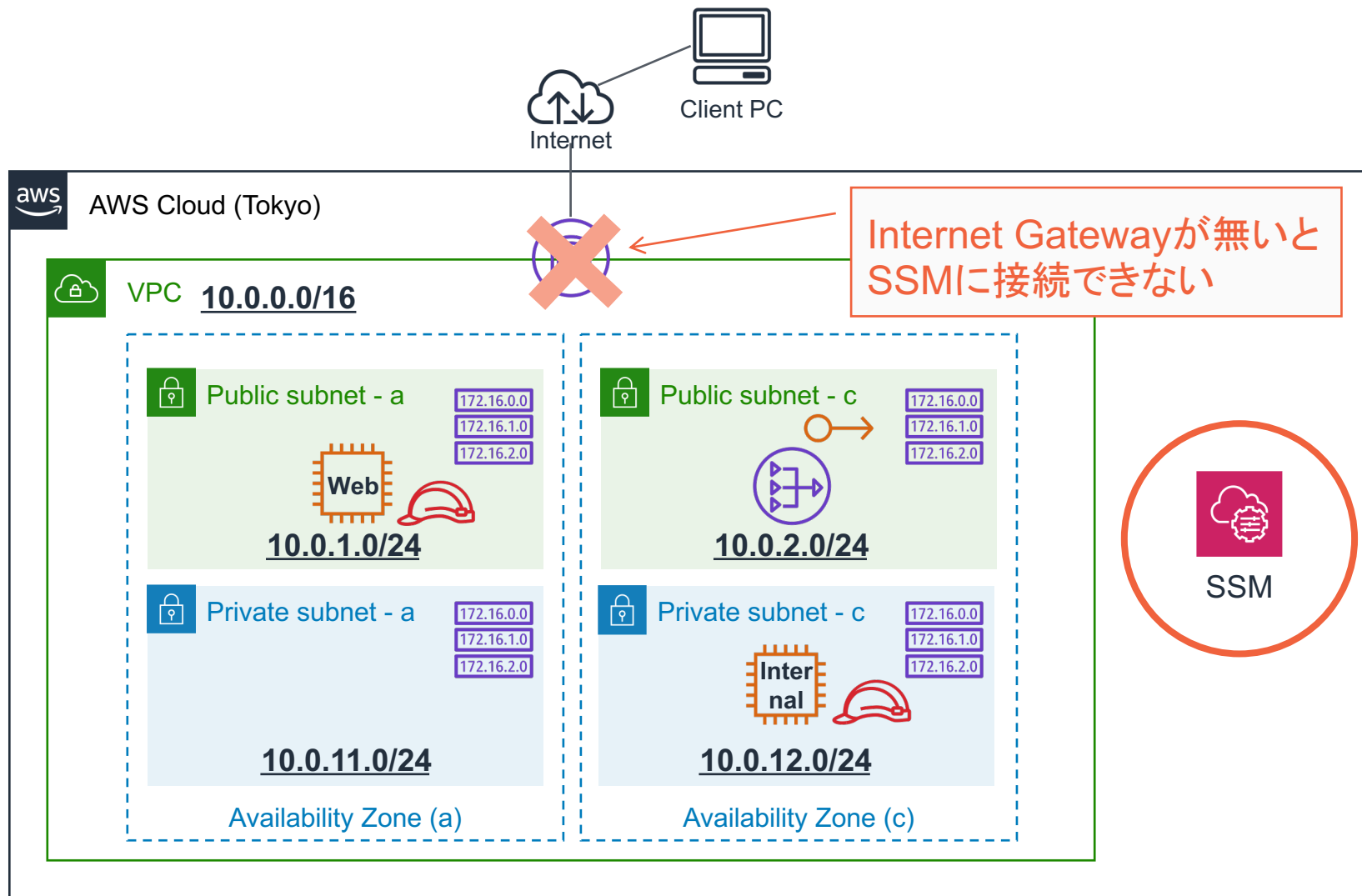
 Elastic IP address

SSM






ハンズオンの中で関わるサービス・機能

-  AWS Systems Manager
-  Amazon EC2
-  IAM Role

VPC外マネージドサービスへの接続


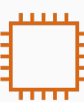



ハンズオンで学ぶサービス・機能

-  Amazon VPC
-  Public/Private Subnet
-  Internet gateway
-  Route table
-  NAT gateway

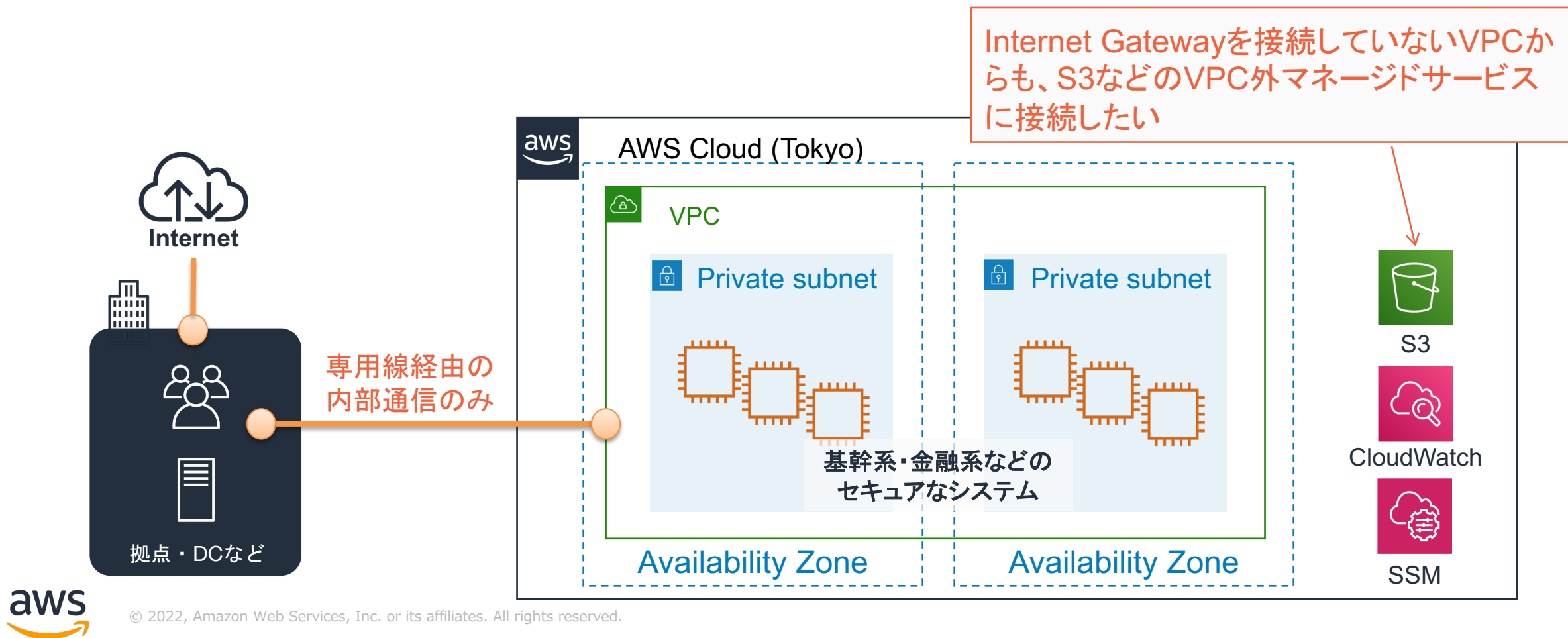
 Elastic IP address

ハンズオンの中で関わるサービス・機能

-  AWS Systems Manager
-  Amazon EC2
-  IAM Role

VPC外マネージドサービスへの接続

セキュアなシステムでは、Private Subnetのみ構成し、VPCからインターネットに接続性を持たせない構成を取る場合も多数あり



VPC Endpoint、AWS PrivateLink

VPC内Subnet上で稼働するサービスから、Internet Gateway、NAT Gateway、NATインスタンスを経由せずに**VPC外サービスと直接通信**させることが可能



Endpoints

➤ Gateway

S3、DynamoDBとの接続方式

➤ Interface

SSM、CloudWatch、S3など、その他サポートされているサービス



AWS PrivateLink

https://docs.aws.amazon.com/ja_jp/vpc/latest/userguide/vpc-endpoints.html

VPC Endpoint、AWS PrivateLink

VPC内Subnet上で稼働するサービスから、Internet Gateway、NAT Gateway、NATインスタンスを経由せずに**VPC外サービスと直接通信**させることが可能



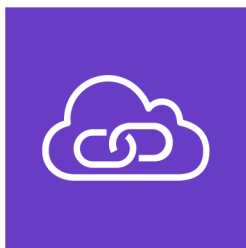
Endpoints

➤ Gateway

S3、DynamoDBとの接続方式

➤ Interface

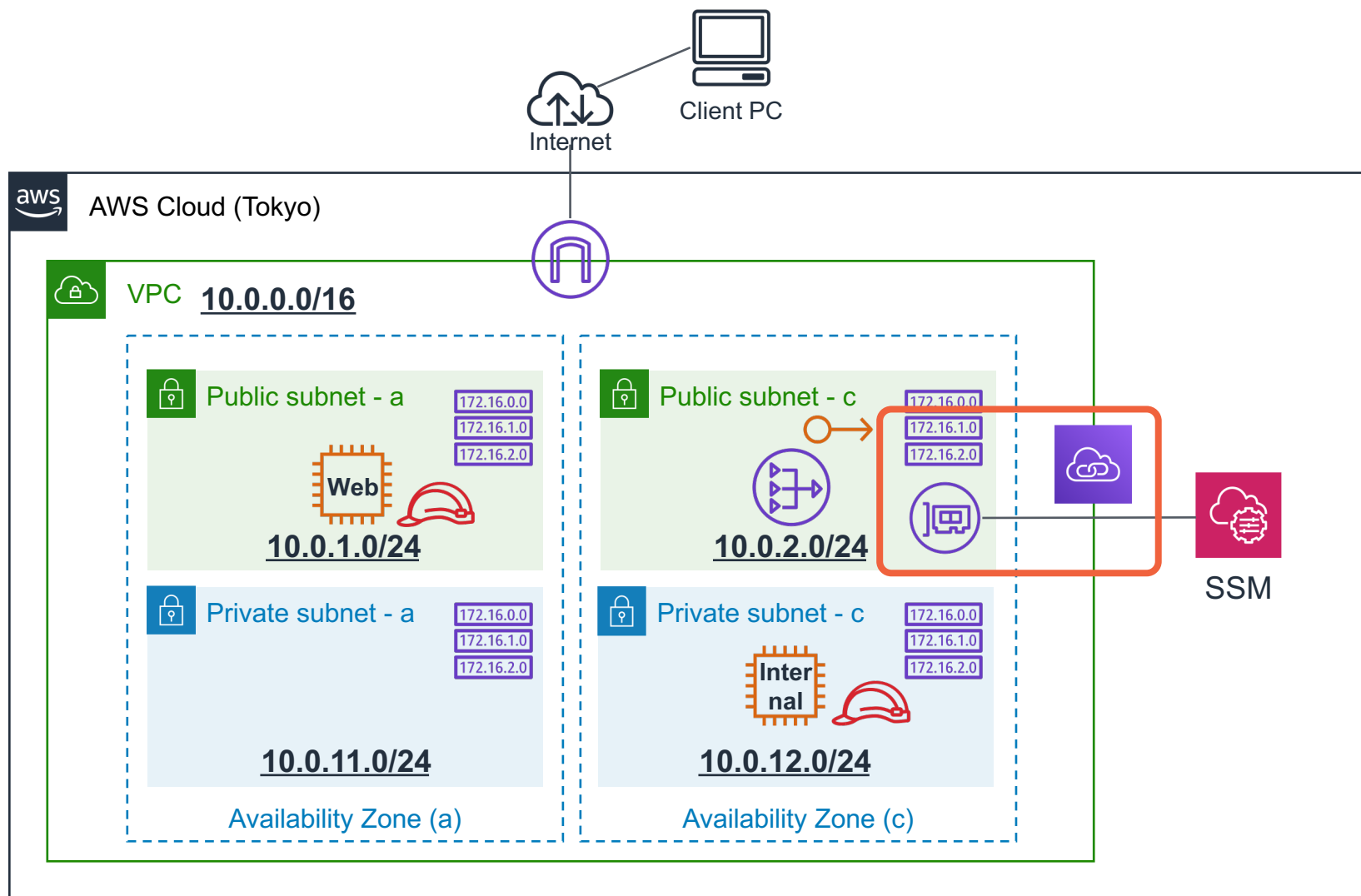
SSM、CloudWatch、**S3**など、その他サポートされているサービス



AWS PrivateLink

https://docs.aws.amazon.com/ja_jp/vpc/latest/userguide/vpc-endpoints.html

VPC外マネージドサービスへの接続



ハンズオンで学ぶサービス・機能



Amazon VPC



Public/Private Subnet



Internet gateway



Route table



NAT gateway



PrivateLink



Elastic IP address

ハンズオンの中で関わるサービス・機能



AWS Systems Manager

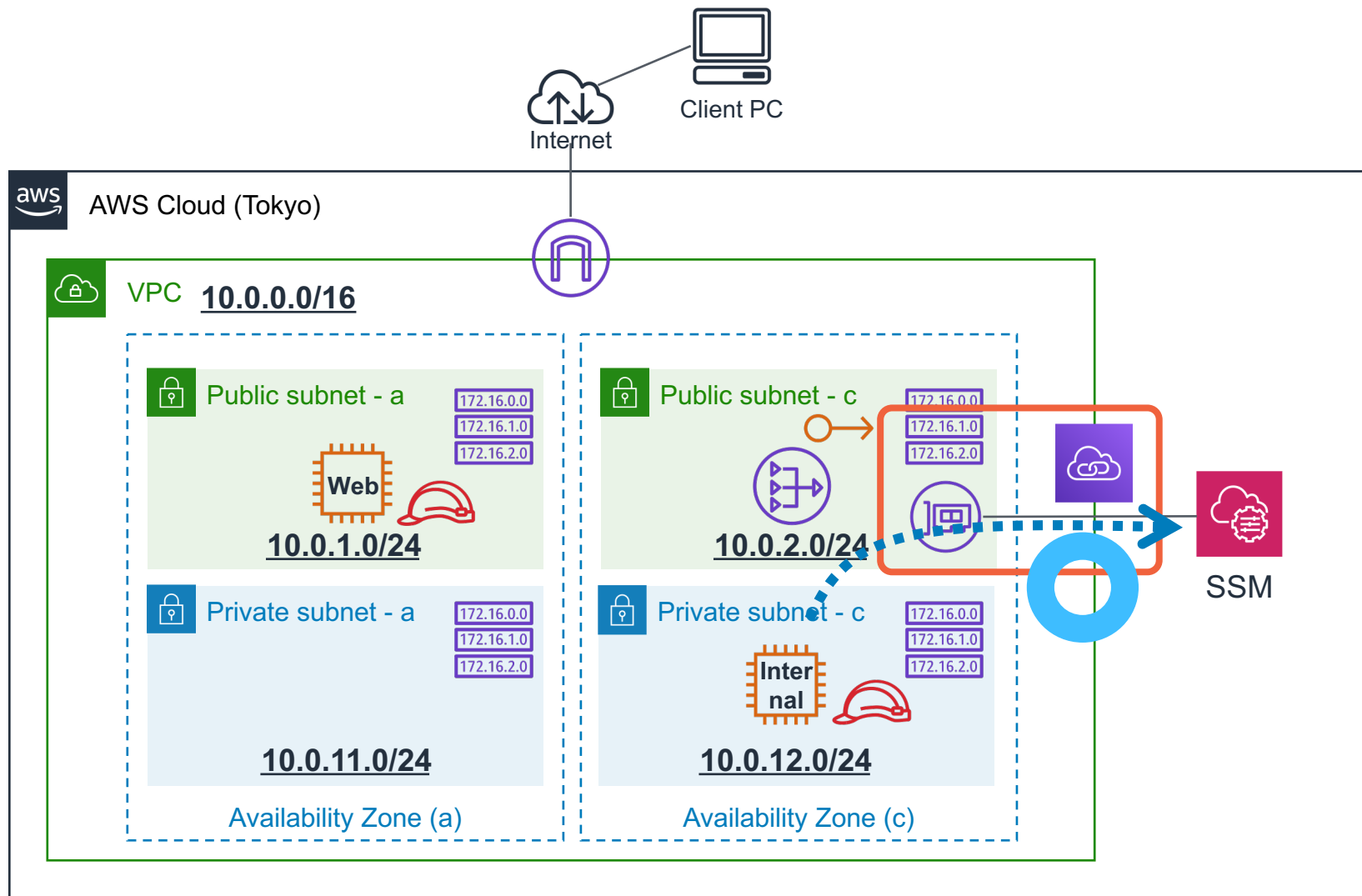


Amazon EC2










IAM Role




VPC外マネージドサービスへの接続



ハンズオンで学ぶサービス・機能

-  Amazon VPC
-  Public/Private Subnet
-  Internet gateway
-  Route table
-  NAT gateway
-  PrivateLink
-  Elastic IP address

ハンズオンの中で関わるサービス・機能

-  AWS Systems Manager
-  Amazon EC2
-  IAM Role



【AWS Hands-on for Beginners】

Network 編 #1-8

AWS上にセキュアなプライベートネットワーク空間を作成

アマゾン ウェブ サービス ジャパン合同会社

パートナー ソリューション アーキテクト

江口 智 / Tomo Eguchi

(収録日: 2022/5/8)

このコースの Agenda

1. AWS

1. 前提知識の確認
2. AWSでのネットワークの考え方
3. 本ハンズオンの最終構成図

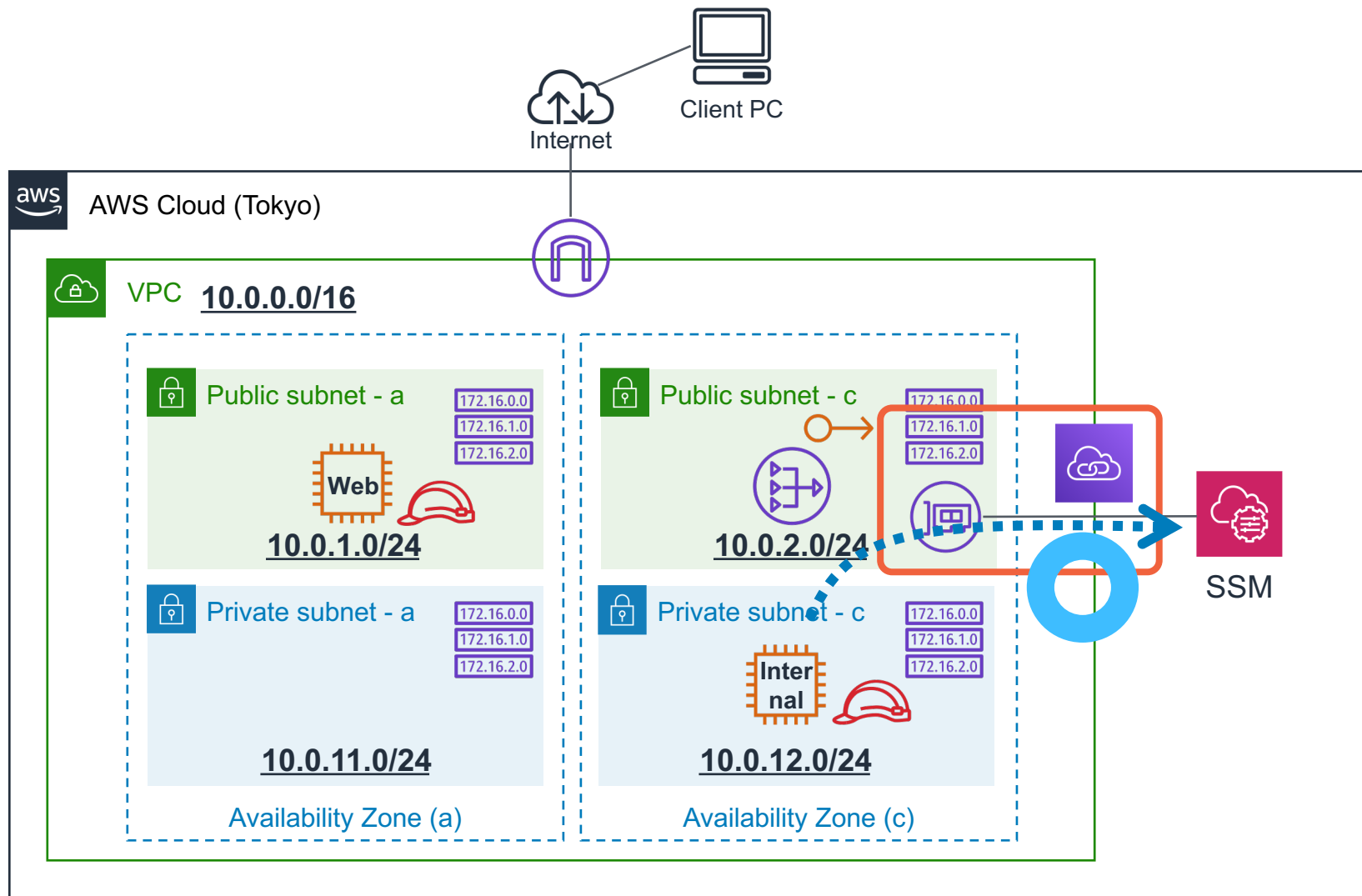
2. Amazon VPC ハンズオン

1. Amazon VPC ハンズオン① Amazon VPC の作成とインターネット接続環境の構築
2. Amazon VPC ハンズオン② ルートテーブルによる経路設定を理解する
3. Amazon VPC ハンズオン③ プライベートサブネットからインターネットへのアクセス方法
- 4. Amazon VPC ハンズオン④ VPC外サービスへの接続方法 - 1**
5. Amazon VPC ハンズオン⑤ VPC外サービスへの接続方法 - 2








3. 本コースのまとめ






VPC外マネージドサービスへの接続



ハンズオンで学ぶサービス・機能

-  Amazon VPC
-  Public/Private Subnet
-  Internet gateway
-  Route table
-  NAT gateway
-  PrivateLink
-  Elastic IP address

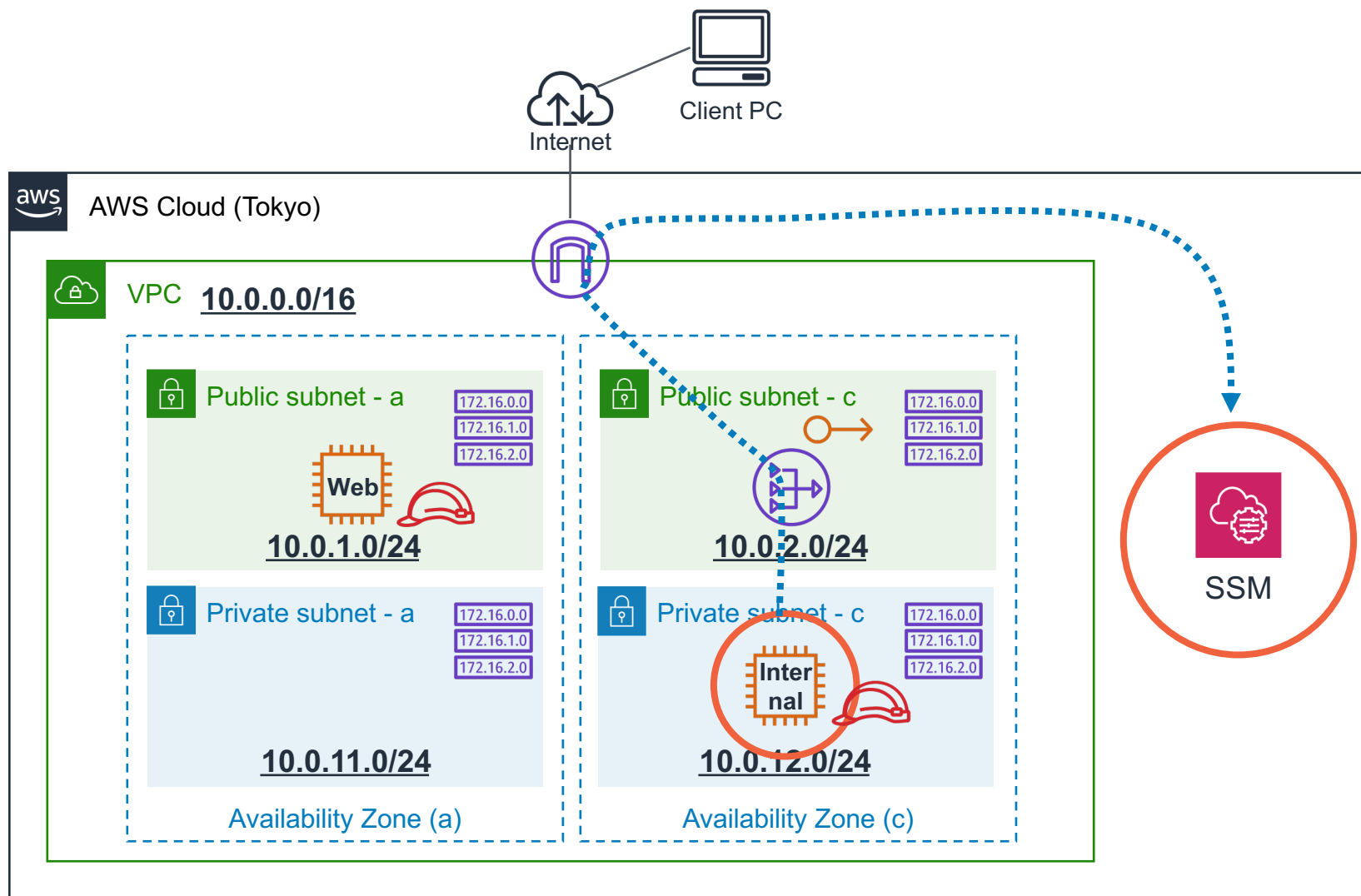
ハンズオンの中で関わるサービス・機能

-  AWS Systems Manager
-  Amazon EC2
-  IAM Role






ハンズオン



VPC外マネージドサービスへの接続






ハンズオンで学ぶサービス・機能

-  Amazon VPC
-  Public/Private Subnet
-  Internet gateway
-  Route table
-  NAT gateway

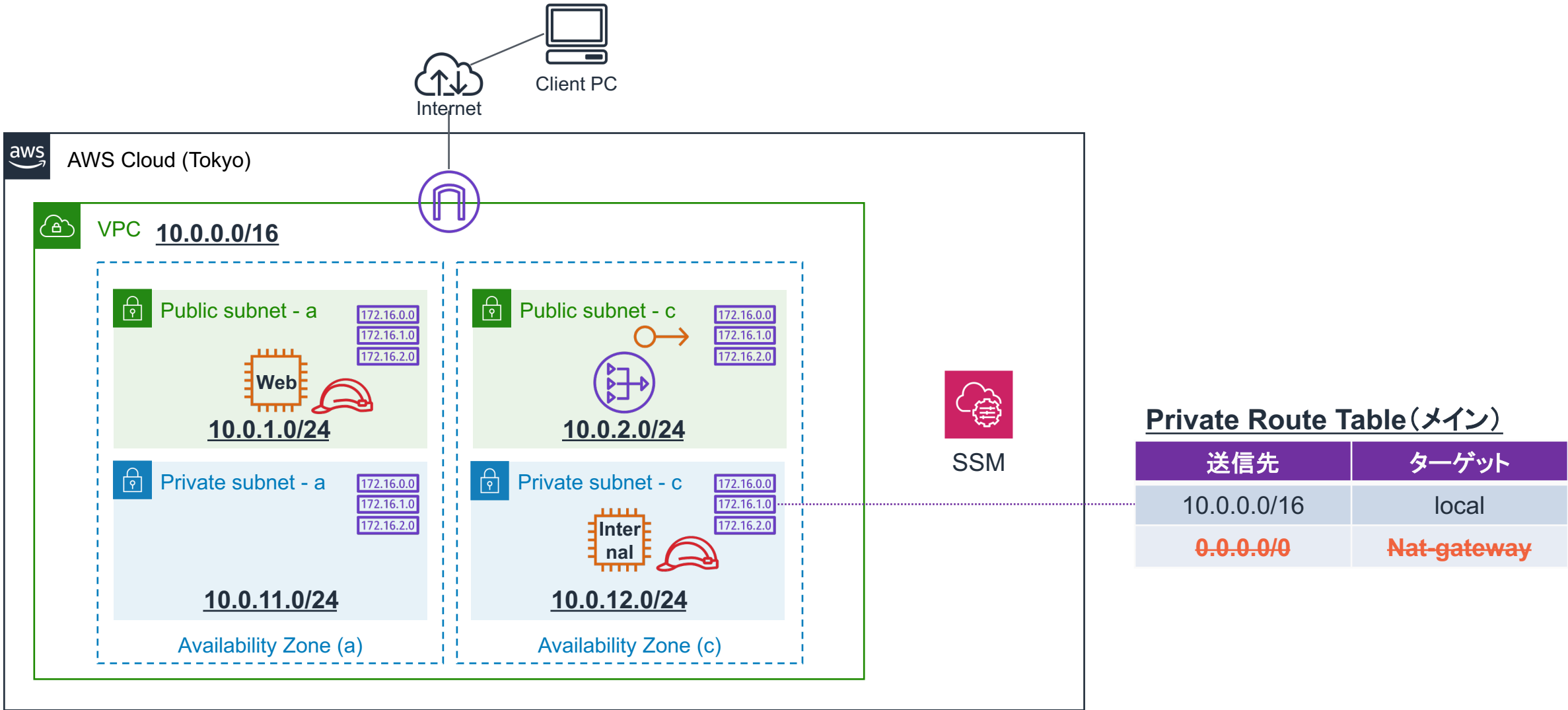
 Elastic IP address

SSM

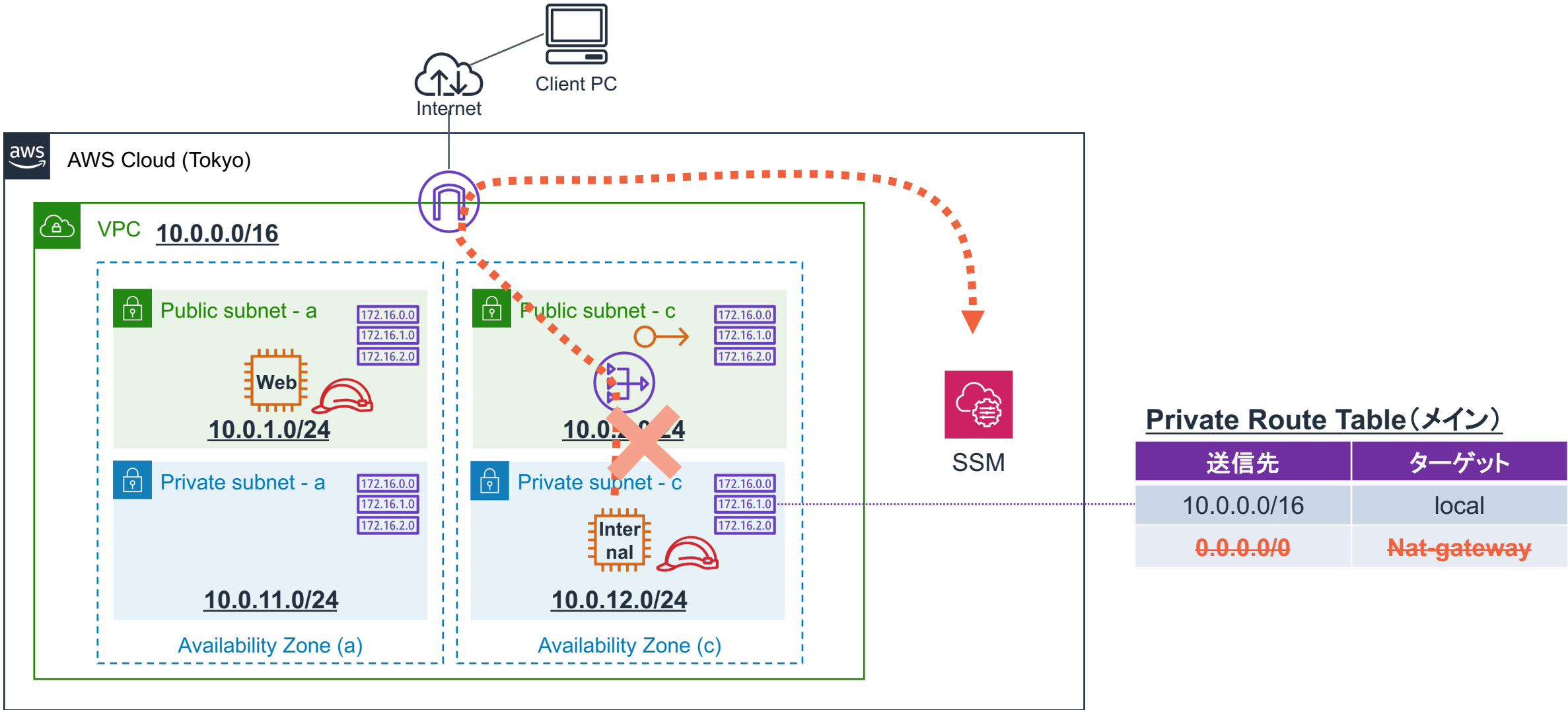
ハンズオンの中で関わるサービス・機能

-  AWS Systems Manager
-  Amazon EC2
-  IAM Role

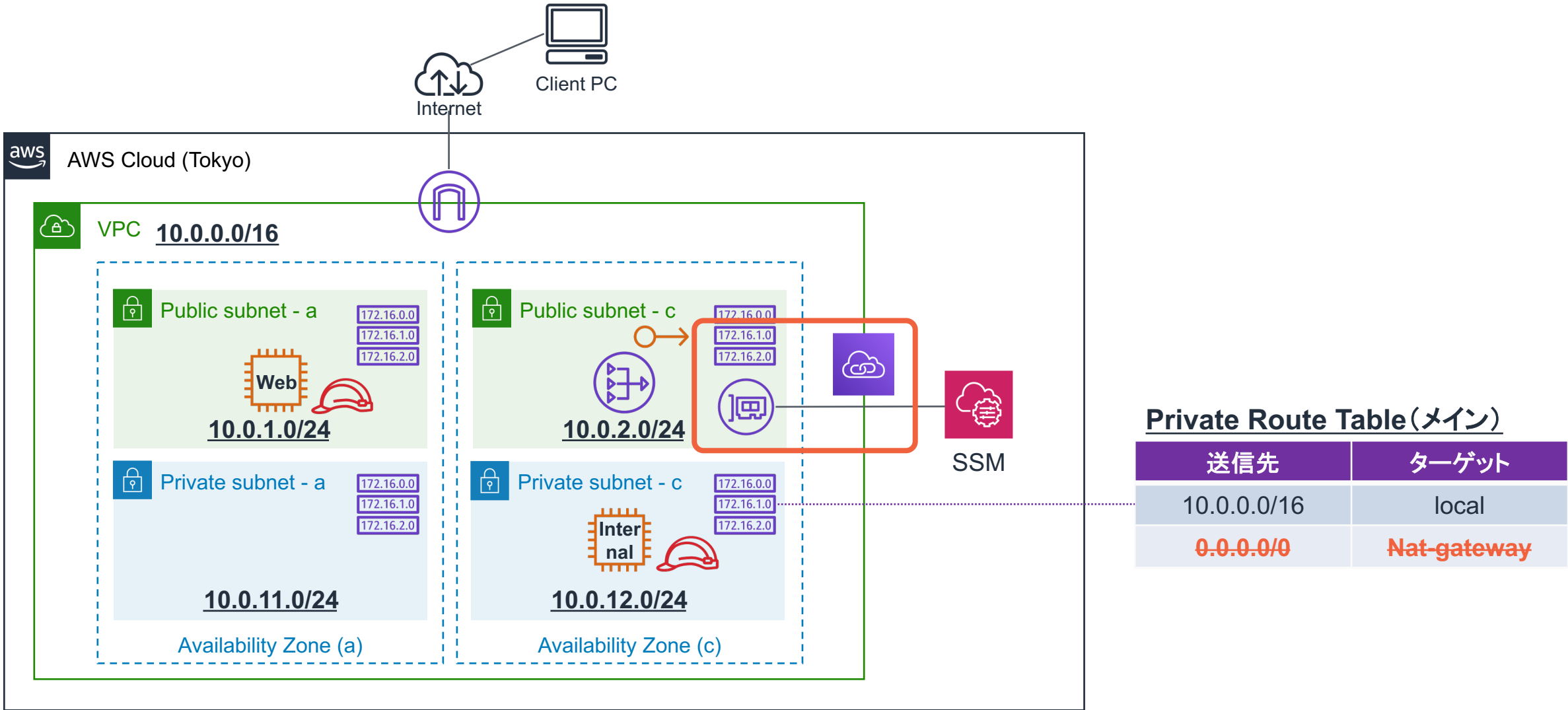
VPC外マネージドサービスへの接続



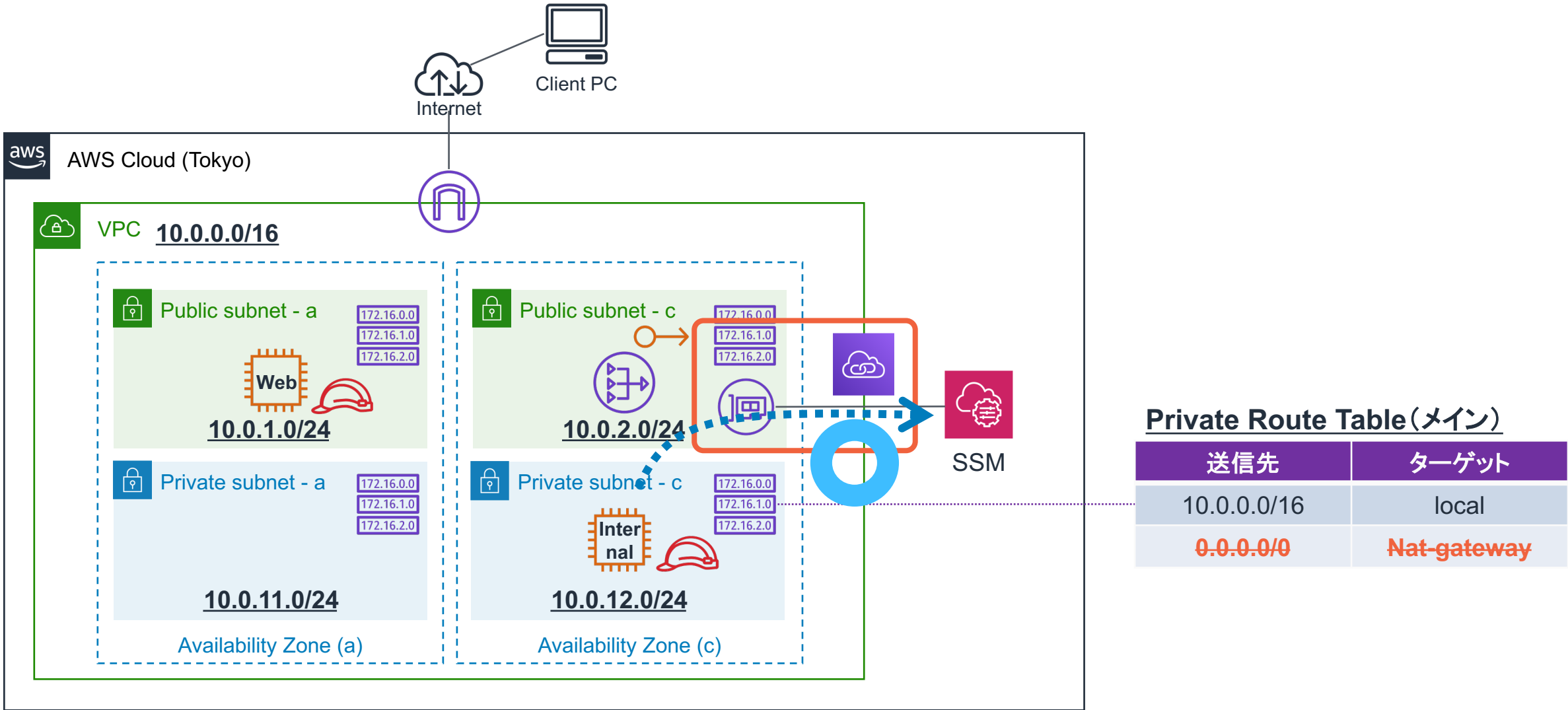
VPC外マネージドサービスへの接続



VPC外マネージドサービスへの接続



VPC外マネージドサービスへの接続





【AWS Hands-on for Beginners】

Network 編 #1-9

AWS上にセキュアなプライベートネットワーク空間を作成

アマゾン ウェブ サービス ジャパン合同会社
パートナー ソリューション アーキテクト

江口 智 / Tomo Eguchi

(収録日: 2022/5/8)

このコースの Agenda

1. AWS

1. 前提知識の確認
2. AWSでのネットワークの考え方
3. 本ハンズオンの最終構成図

2. Amazon VPC ハンズオン

1. Amazon VPC ハンズオン① Amazon VPC の作成とインターネット接続環境の構築
2. Amazon VPC ハンズオン② ルートテーブルによる経路設定を理解する
3. Amazon VPC ハンズオン③ プライベートサブネットからインターネットへのアクセス方法
4. Amazon VPC ハンズオン④ VPC外サービスへの接続方法 - 1
- 5. Amazon VPC ハンズオン⑤ VPC外サービスへの接続方法 - 2**

3. 本コースのまとめ

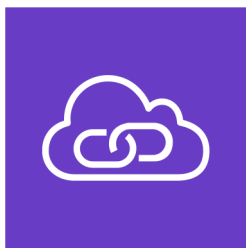


VPC Endpoint、AWS PrivateLink

VPC内Subnet上で稼働するサービスから、Internet Gateway、NAT Gateway、NATインスタンスを経由せずに**VPC外サービスと直接通信**させることが可能



Endpoints



AWS PrivateLink

➤ Gateway

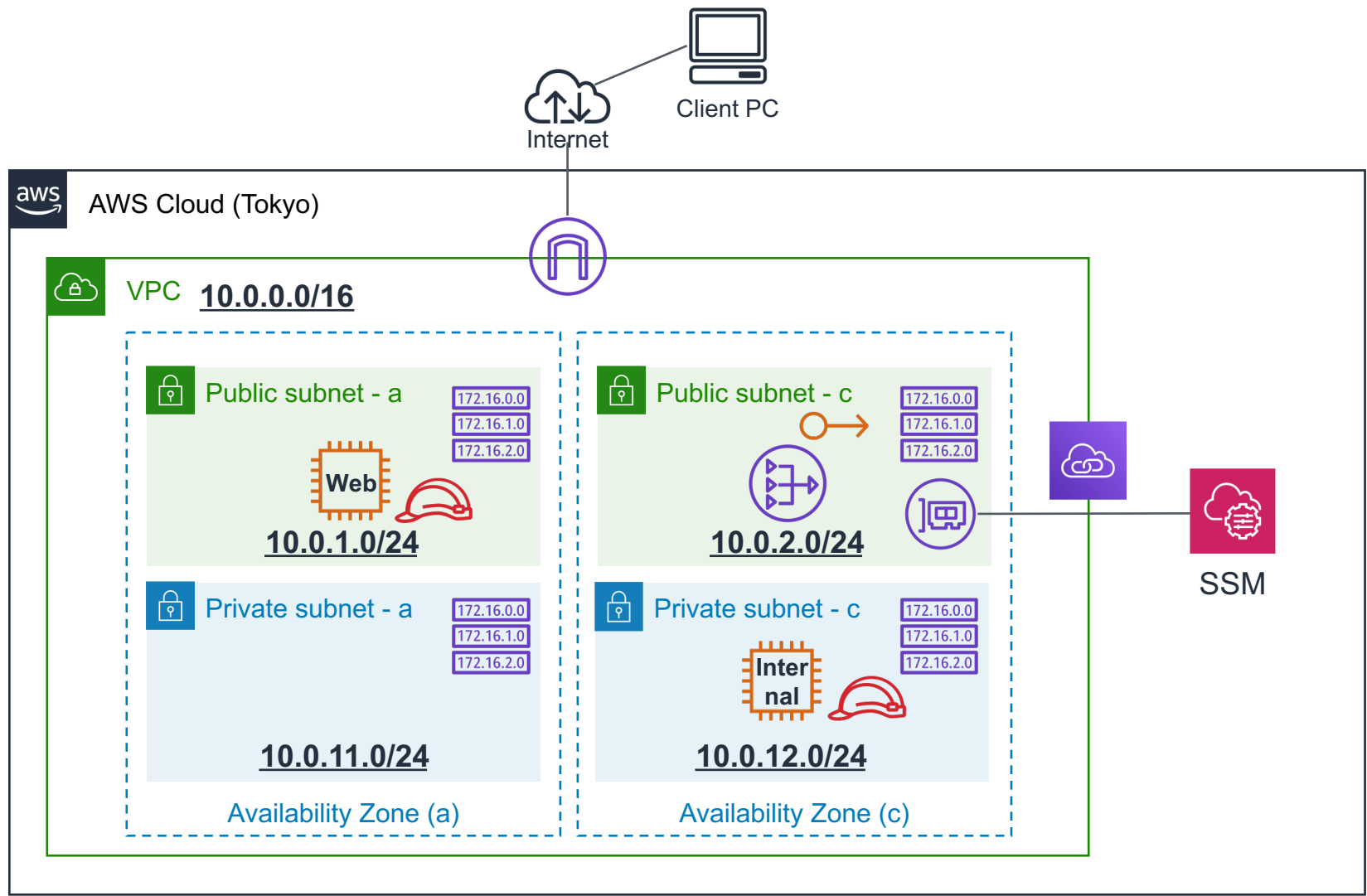
S3、DynamoDBとの接続方式

➤ Interface

SSM、CloudWatch、S3など、その他サポートされているサービス

https://docs.aws.amazon.com/ja_jp/vpc/latest/userguide/vpc-endpoints.html

現在の構成



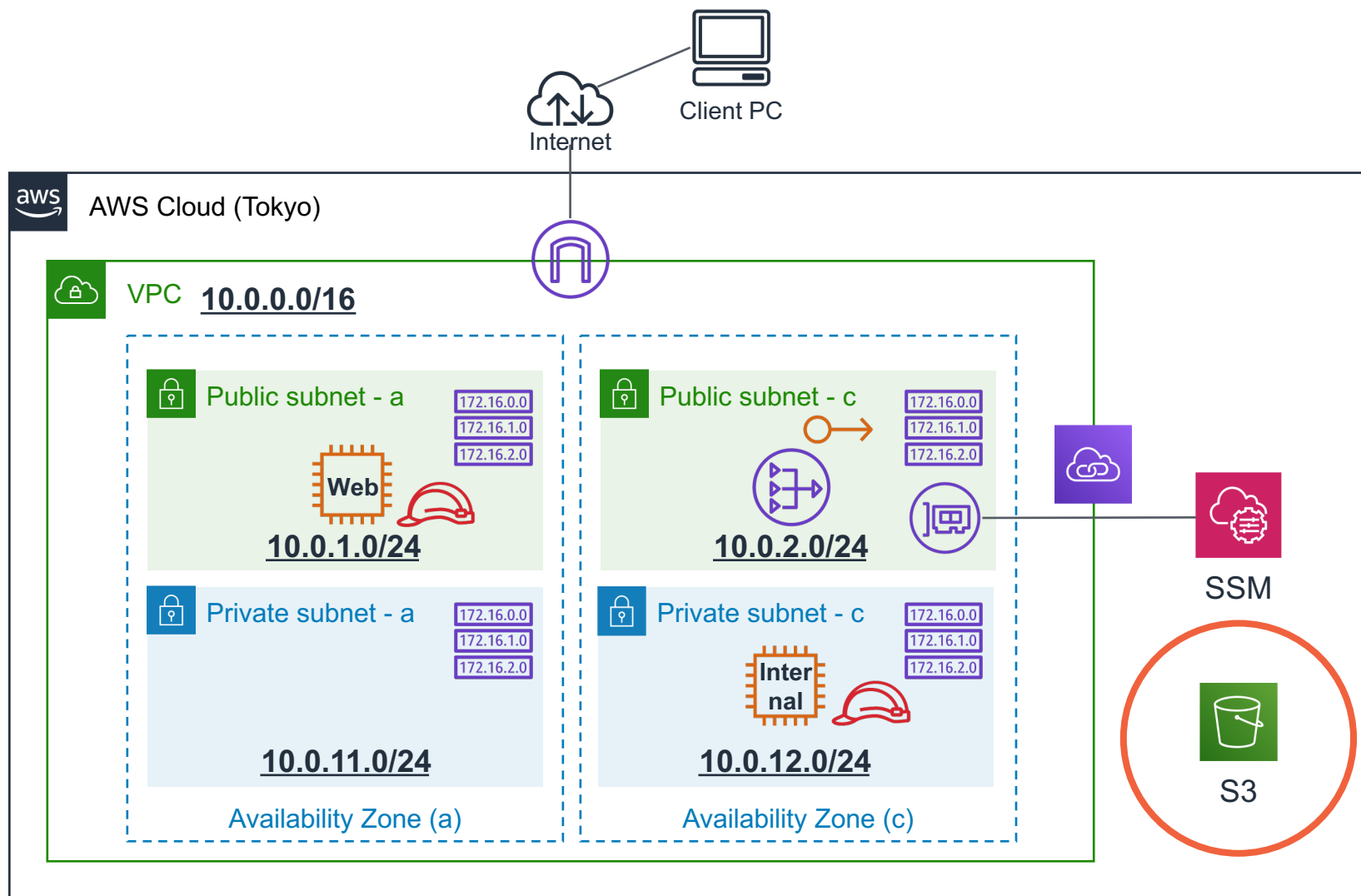
ハンズオンで学ぶサービス・機能

- Amazon VPC
- Public/Private Subnet
- Internet gateway
- Route table
- NAT gateway
- PrivateLink
- Elastic IP address








ハンズオンの中で関わるサービス・機能

- AWS Systems Manager
- Amazon EC2
- IAM Role





VPC外マネージドサービスへの接続



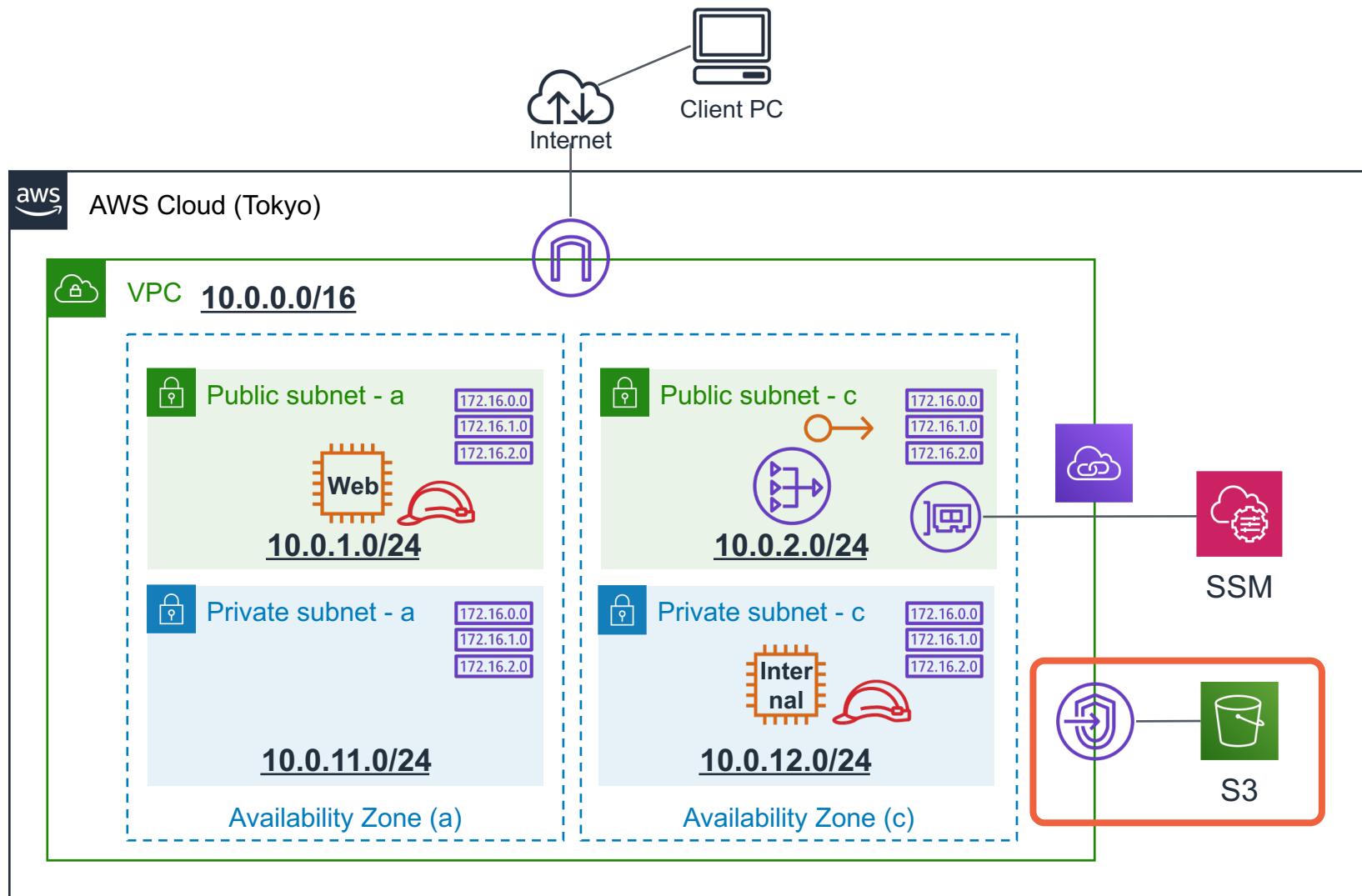
ハンズオンで学ぶサービス・機能

-  Amazon VPC
-  Public/Private Subnet
-  Internet gateway
-  Route table
-  NAT gateway
-  PrivateLink
-  Elastic IP address









ハンズオンの中で関わるサービス・機能

-  AWS Systems Manager
-  Amazon EC2
-  Amazon S3
-  IAM Role





VPC外マネージドサービスへの接続



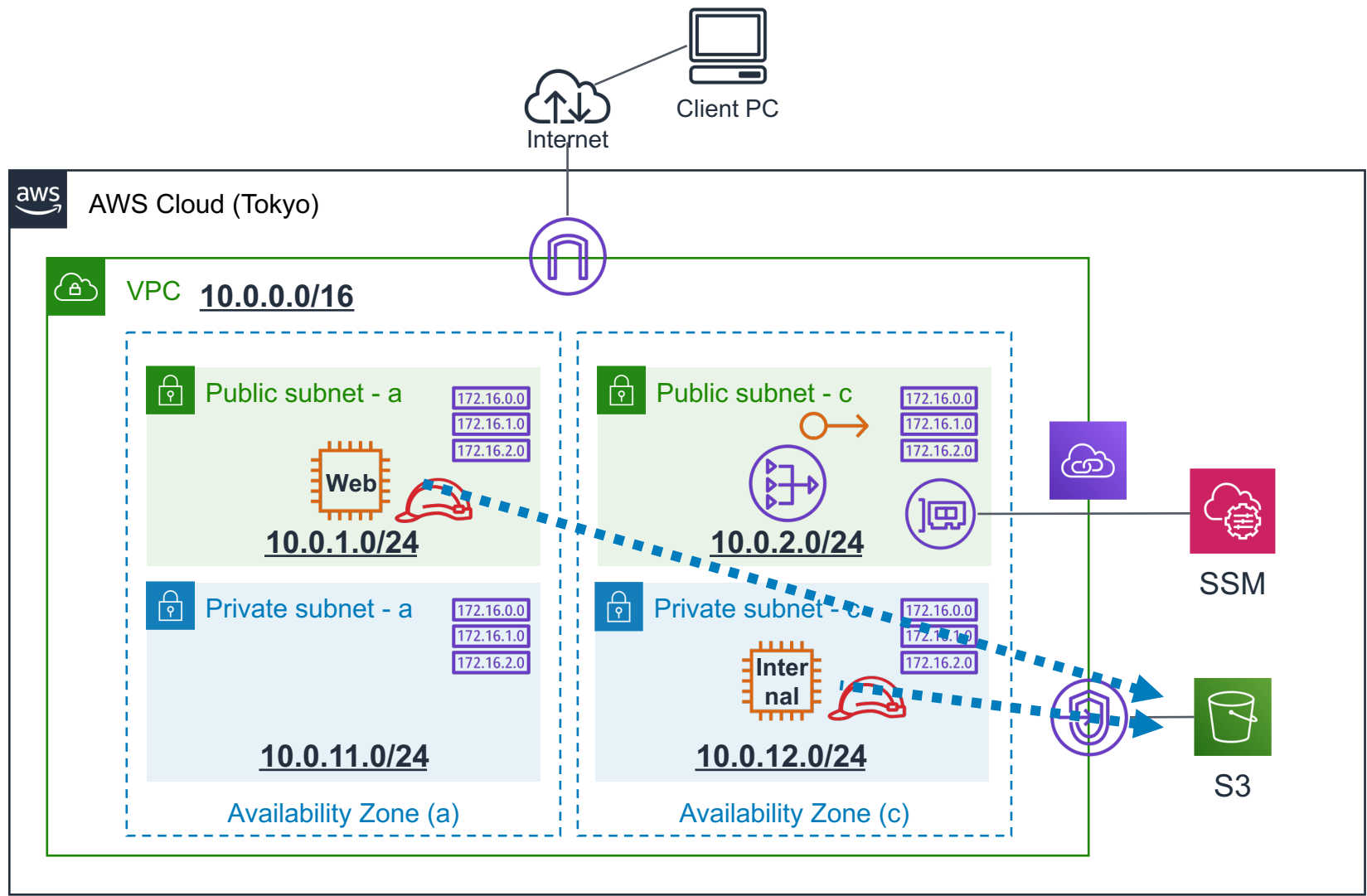
ハンズオンで学ぶサービス・機能

-  Amazon VPC
-  Public/Private Subnet
-  Internet gateway
-  Route table
-  NAT gateway
-  PrivateLink
-  Endpoints
-  Elastic IP address

ハンズオンの中で関わるサービス・機能

-  AWS Systems Manager
-  Amazon EC2
-  Amazon S3
-  IAM Role

現在の構成



ハンズオンで学ぶサービス・機能

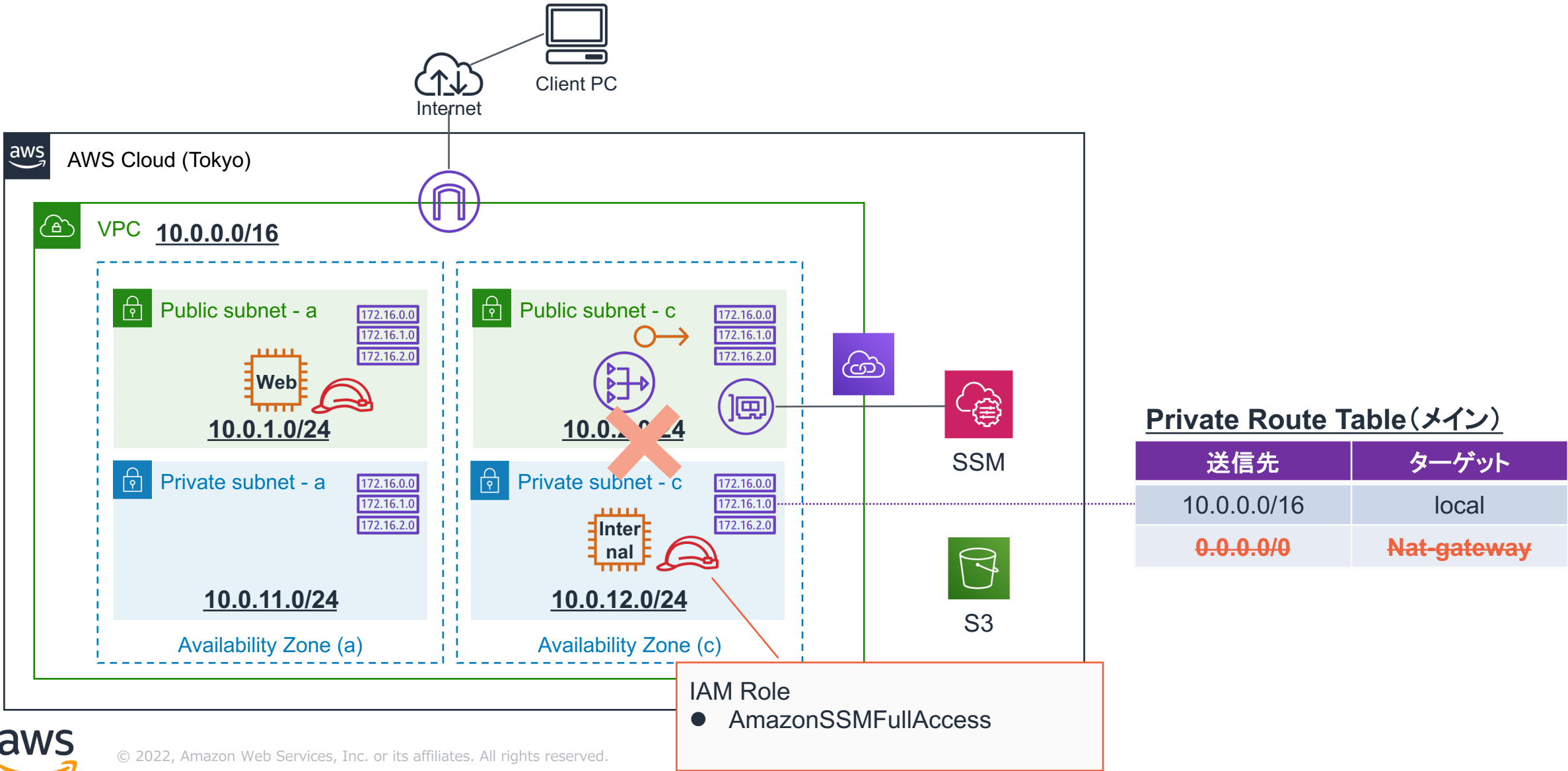
- Amazon VPC
- Public/Private Subnet
- Internet gateway
- Route table
- NAT gateway
- PrivateLink
- Endpoints
- Elastic IP address

ハンズオンの中で関わるサービス・機能

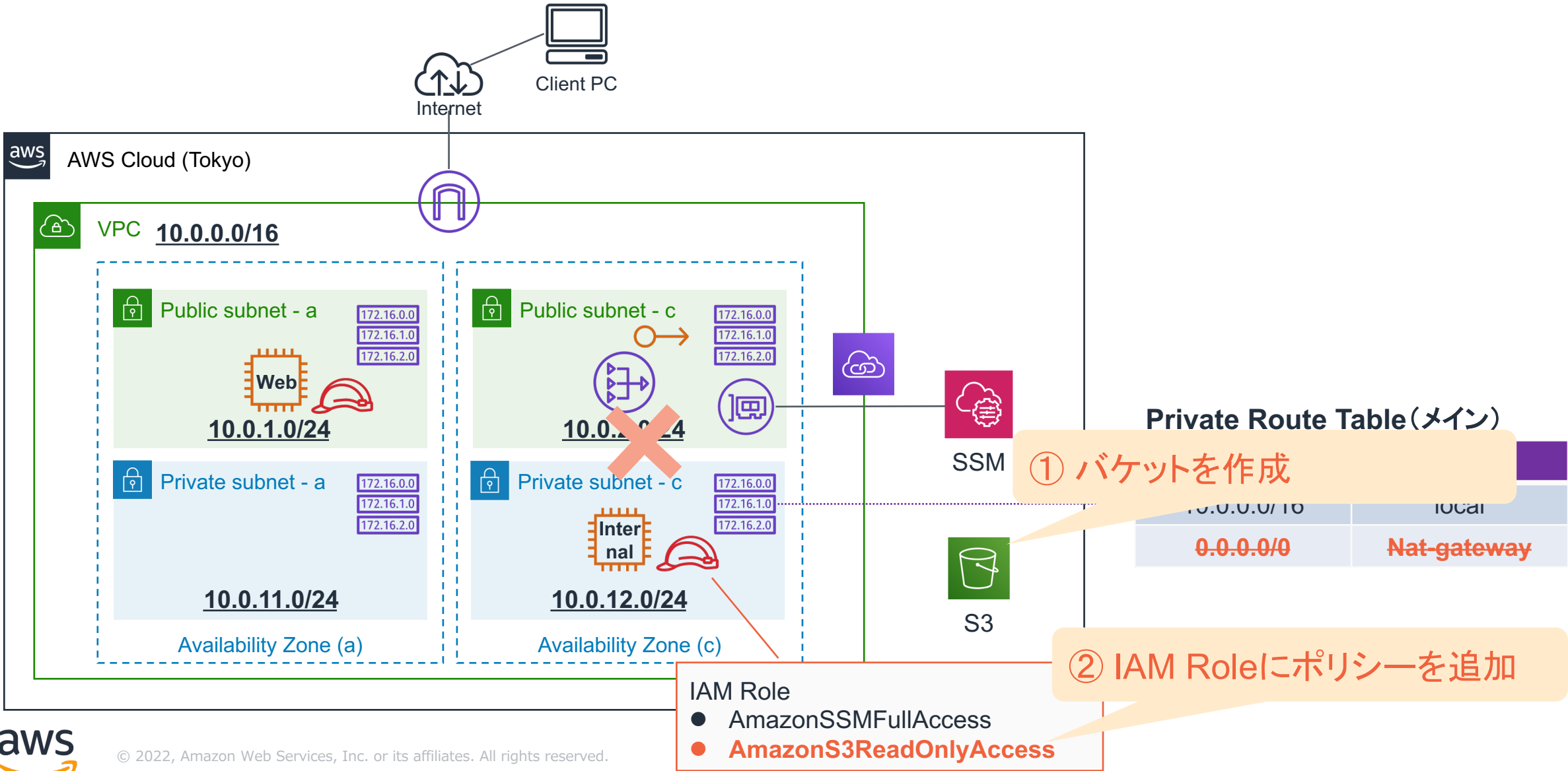
- AWS Systems Manager
- Amazon EC2
- Amazon S3
- IAM Role

ハンズオンの流れ

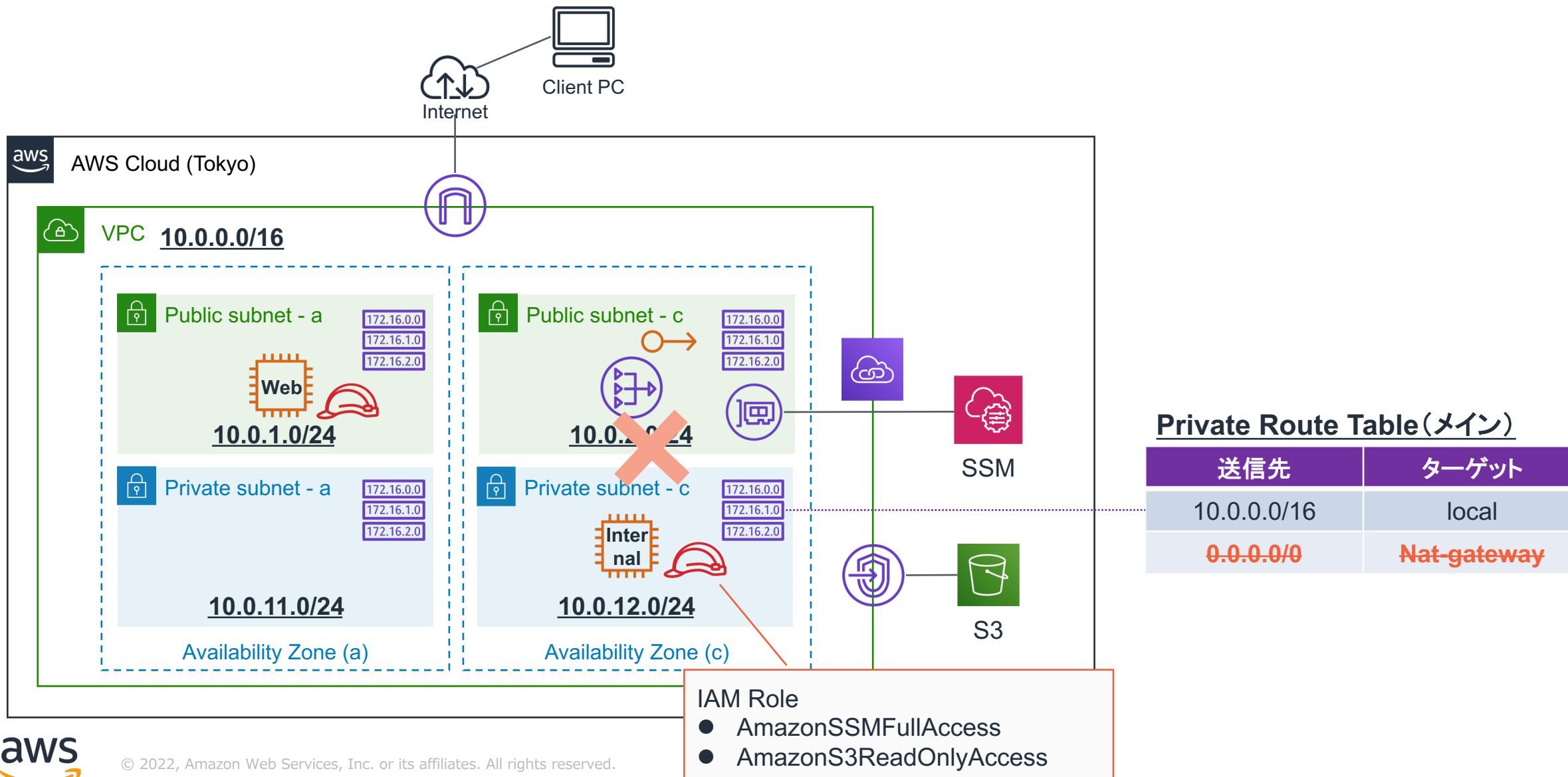
VPC外マネージドサービスへの接続



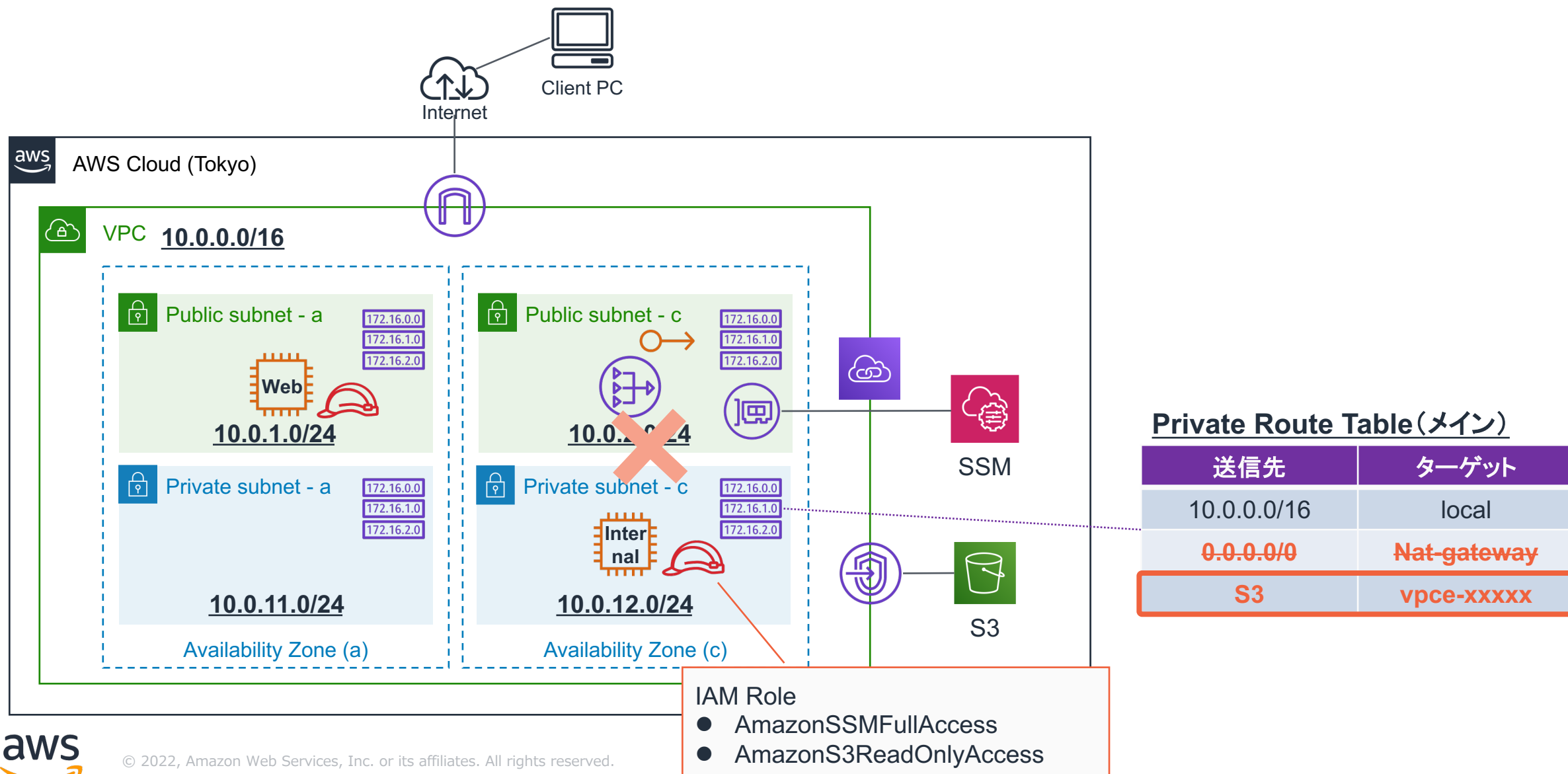
VPC外マネージドサービスへの接続



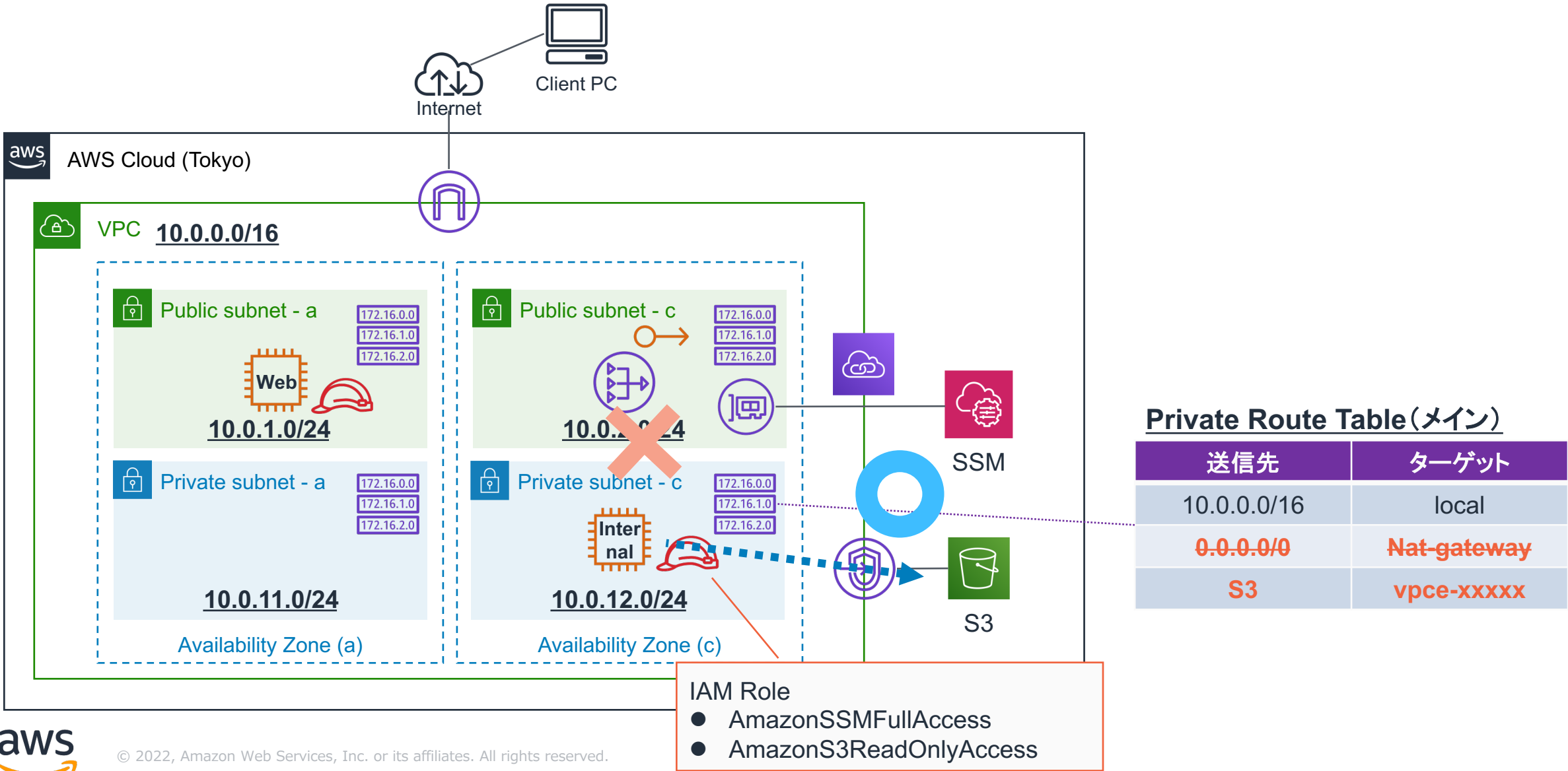
VPC外マネージドサービスへの接続



VPC外マネージドサービスへの接続



VPC外マネージドサービスへの接続





【AWS Hands-on for Beginners】

Network 編 #1-10

AWS上にセキュアなプライベートネットワーク空間を作成

アマゾン ウェブ サービス ジャパン合同会社

パートナー ソリューション アーキテクト

江口 智 / Tomo Eguchi

(収録日: 2022/5/8)

このコースの Agenda

1. AWS

1. 前提知識の確認
2. AWSでのネットワークの考え方
3. 本ハンズオンの最終構成図

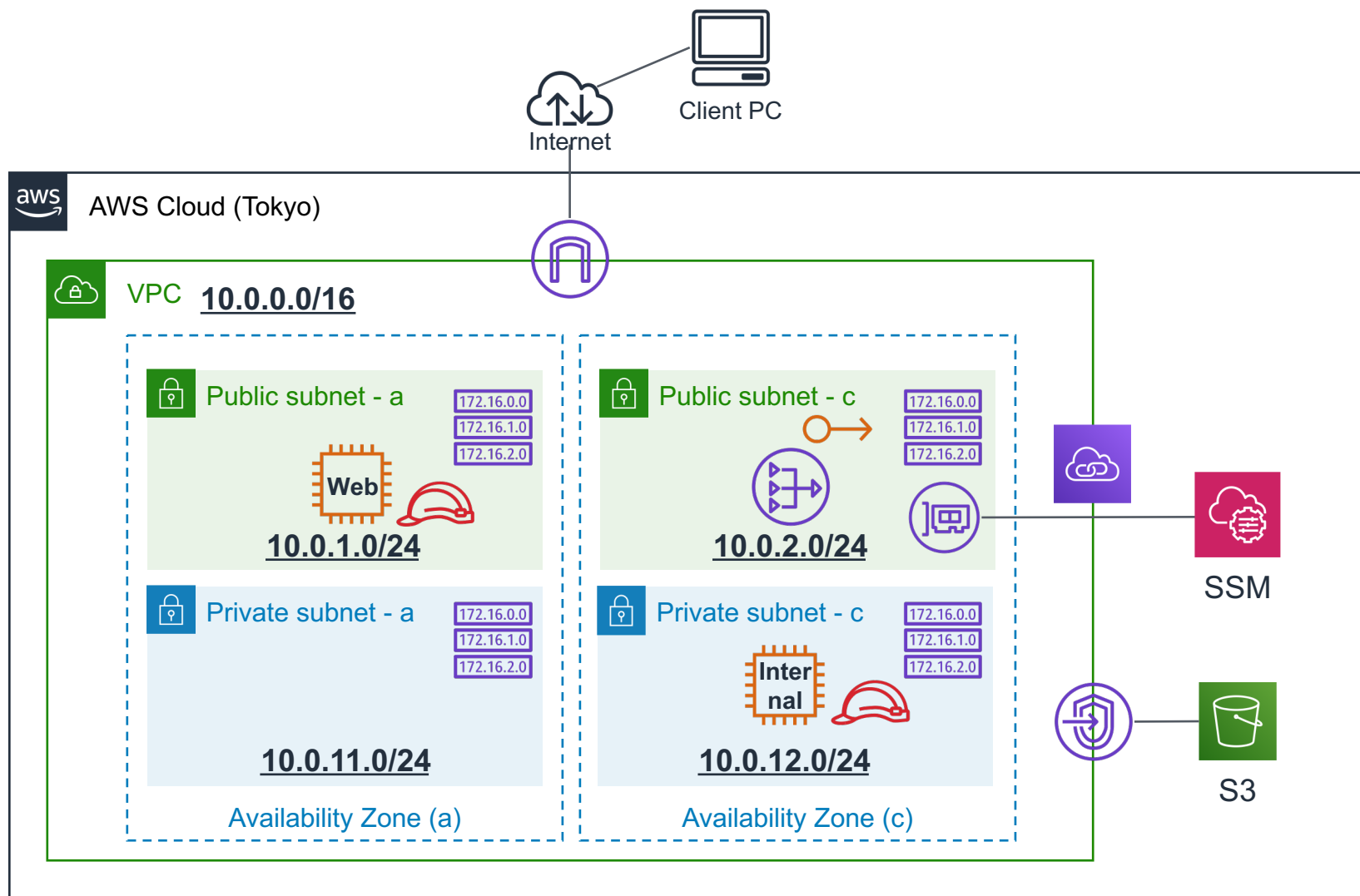
2. Amazon VPC ハンズオン

1. Amazon VPC ハンズオン① Amazon VPC の作成とインターネット接続環境の構築
2. Amazon VPC ハンズオン② ルートテーブルによる経路設定を理解する
3. Amazon VPC ハンズオン③ プライベートサブネットからインターネットへのアクセス方法
4. Amazon VPC ハンズオン④ VPC外サービスへの接続方法 - 1
5. Amazon VPC ハンズオン⑤ VPC外サービスへの接続方法 - 2









3. 本コースのまとめ







最終構成図



ハンズオンで学ぶサービス・機能

-  Amazon VPC
-  Public/Private Subnet
-  Internet gateway
-  Route table
-  NAT gateway
-  Endpoints
-  PrivateLink
-  Elastic IP address

ハンズオンの中で関わるサービス・機能

-  AWS Systems Manager
-  Amazon EC2
-  Amazon S3
-  IAM Role

本コースのまとめ

- Amazon VPC を使ってAWS上にセキュアなプライベートネットワーク空間を作成できることを学んでいただきました
- 実際に手を動かし、Amazon VPCを中心としたネットワークに関する機能を学んでいただきました
- NAT gateway、VPC endpoint を活用し、AWS上でセキュアなネットワークを構成する方法を学んでいただきました

参考資料

- BlackBelt: Amazon Virtual Private Cloud (VPC)
 - https://d1.awsstatic.com/webinars/jp/pdf/services/20201021_AWS-BlackBelt-VPC.pdf
 - https://www.youtube.com/watch?v=JAzsGRS_o4c
- Amazon VPC 料金
 - <https://aws.amazon.com/jp/vpc/pricing/>
- Amazon VPC のよくある質問
 - <https://aws.amazon.com/jp/vpc/faqs/>





【AWS Hands-on for Beginners】

Network 編 #1-11

AWS上にセキュアなプライベートネットワーク空間を作成

アマゾン ウェブ サービス ジャパン合同会社
パートナー ソリューション アーキテクト

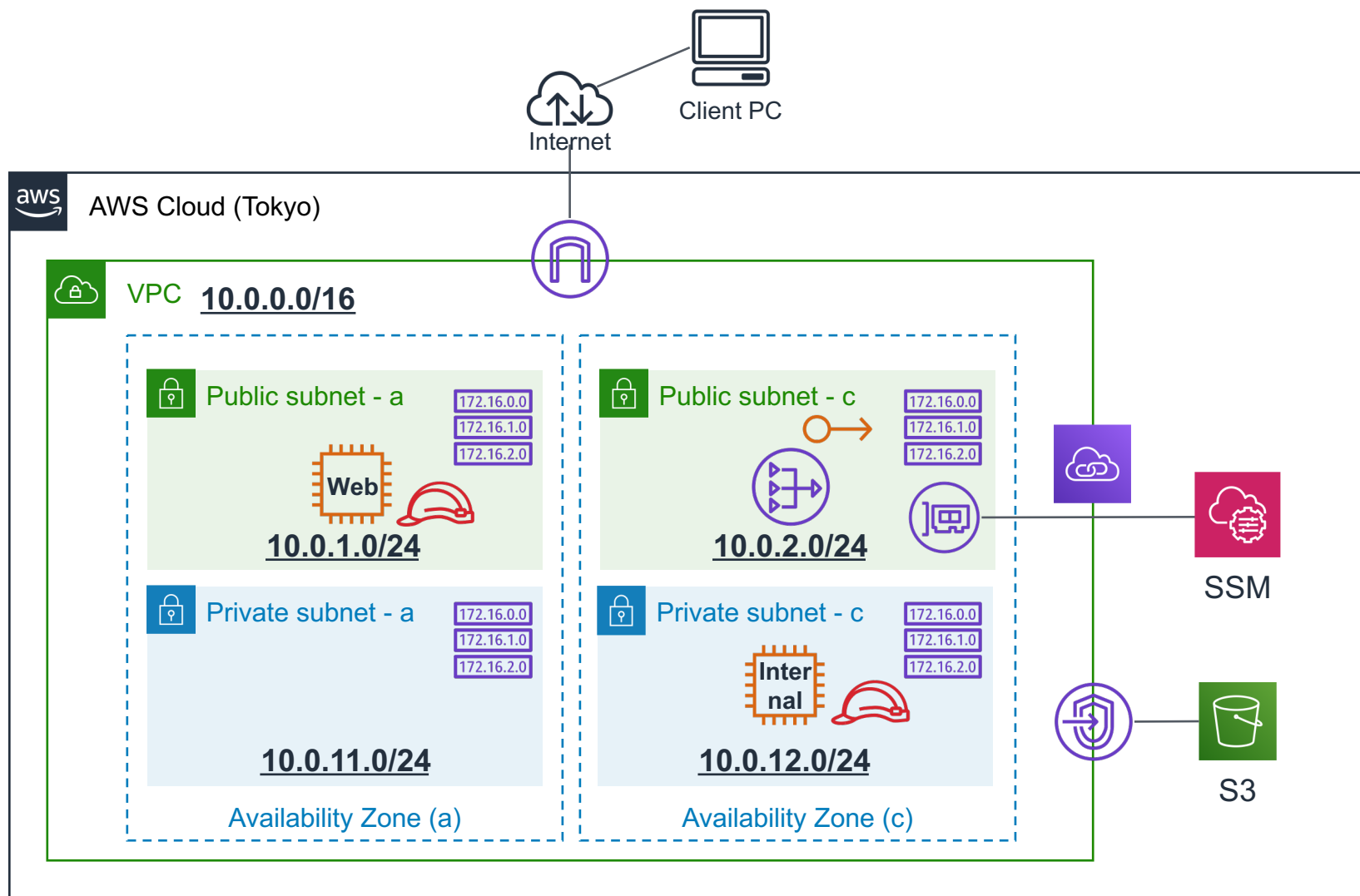
江口 智 / Tomo Eguchi

(収録日: 2022/5/8)









後片付け







最終構成図



ハンズオンで学ぶサービス・機能

-  Amazon VPC
-  Public/Private Subnet
-  Internet gateway
-  Route table
-  NAT gateway
-  Endpoints
-  PrivateLink
-  Elastic IP address

ハンズオンの中で関わるサービス・機能

-  AWS Systems Manager
-  Amazon EC2
-  Amazon S3
-  IAM Role

ハンズオンで設定した流れ

1. Amazon VPC の作成とインターネット接続環境の構築

1. VPC 作成
2. サブネット 作成
3. Internet Gateway 作成
4. Route table 作成
5. IAM Role 作成
6. EC2 (web) 作成
7. Security Group 作成

2. プライベートサブネットからインターネットへのアクセス方法

1. NAT Gateway 作成
2. EC2 (Internal)

3. VPC外サービスへの接続方法

1. VPC Endpoint Interface型 (SSM) 作成
2. S3 バケット 作成
3. Gateway型 (S3) 作成

環境削除手順

1. VPC Endpoint 削除
2. S3バケット 削除
3. EC2 削除
4. Security Group 削除
5. IAM Role 削除
6. NAT Gateway 削除
7. Elastic IP 削除（解放）
8. VPC 削除

