VPC

レクチャー	レクチャーで学ぶ内容
VPCの概要	VPCの基本的な機能や仕組みについて理解します。
VPCとの接続	VPCと外部機器やVPC同士などの接続方法について理解します。
VPCの設計	今回ハンズオンで実施するVPC構成の設計を確認します。
VPCとサブネットを設定する(ハンズオン)	VPCにパブリックサブネットとプライベートサブネットを設置する構成を作成します。
VPC／サブネットにサーバーを設定する(ハンズオン)	設置したサブネットにサーバーを設置してサーバー間通信の設定を行います。

VPC

レクチャー	レクチャーで学ぶ内容
ネットワークACL（ハンズオン）	ネットワークACLによるアクセス制御で特定のIPアドレスからのアクセスを拒否する設定を行います。
VPCエンドポイント（ハンズオン）	プライベートサブネットにあるDBサーバーからS3に対して、エンドポイントを通してアクセスする設定を行います。
VPC Flow Logs	VPCのトラフィックデータのログ取得する設定を行います。

VPCの概要

Virtual Private Cloud（VPC）

VPCはAWSクラウド内に論理的に分離されたセクションを作り、ユーザーが定義した仮想ネットワークを構築するサービス

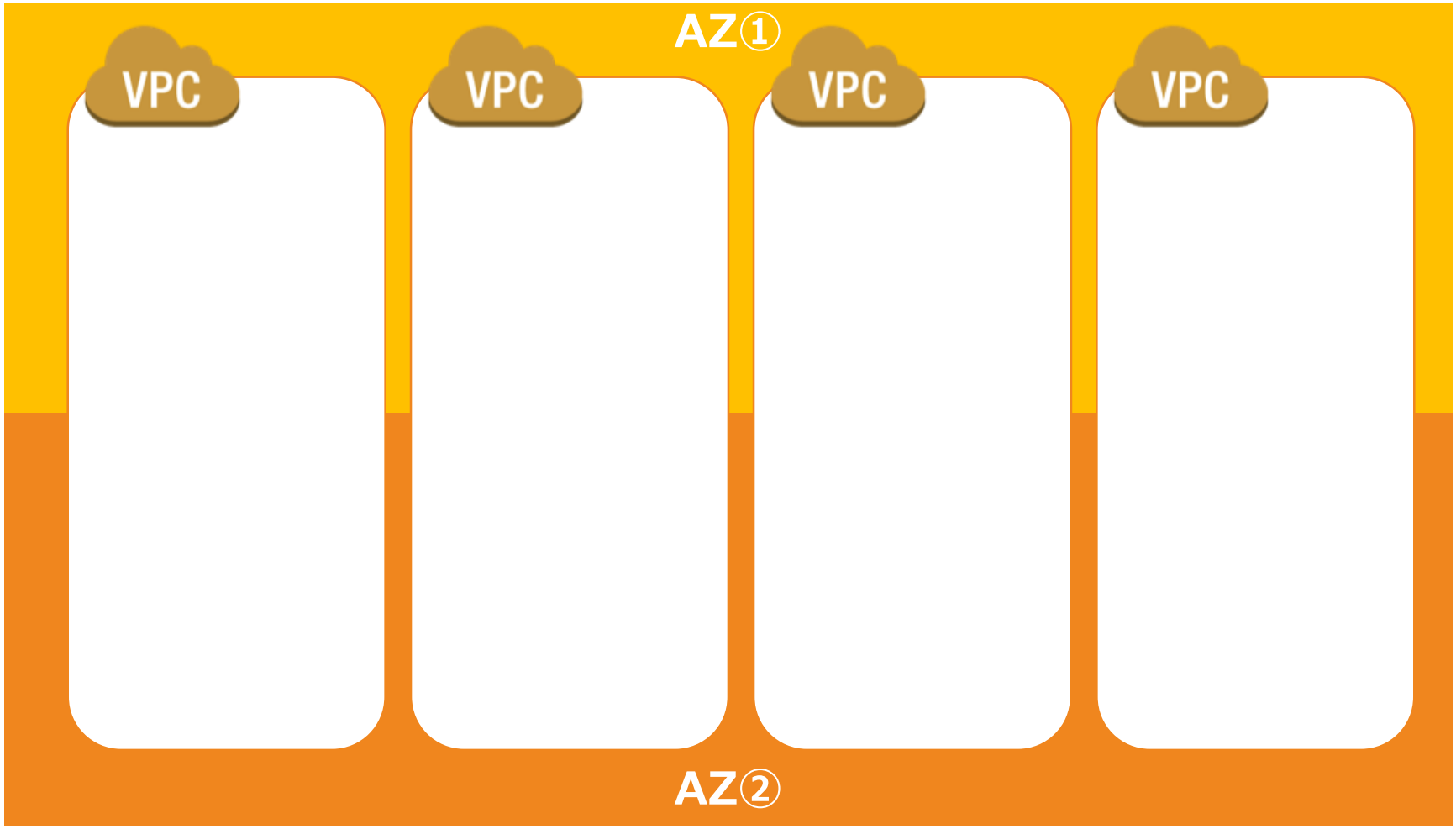
- ✓ 任意の IP アドレス範囲の選択して仮想ネットワークを構築
- ✓ サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など仮想ネットワーキング環境を完全に制御可能
- ✓ 必要に応じてクラウド内外のネットワーク同士を接続することも可能
- ✓ 複数の接続オプションが利用可能
  - -インターネット経由
  - -VPN/専用線(Direct Connect)

Virtual Private Cloud（VPC）

単一のVPCを構築すると単一AZの範囲に設定される。

Virtual Private Cloud（VPC）

同一リージョン内ではVPCは複数のAZにリソースを含めることが可能



サブネットとVPC

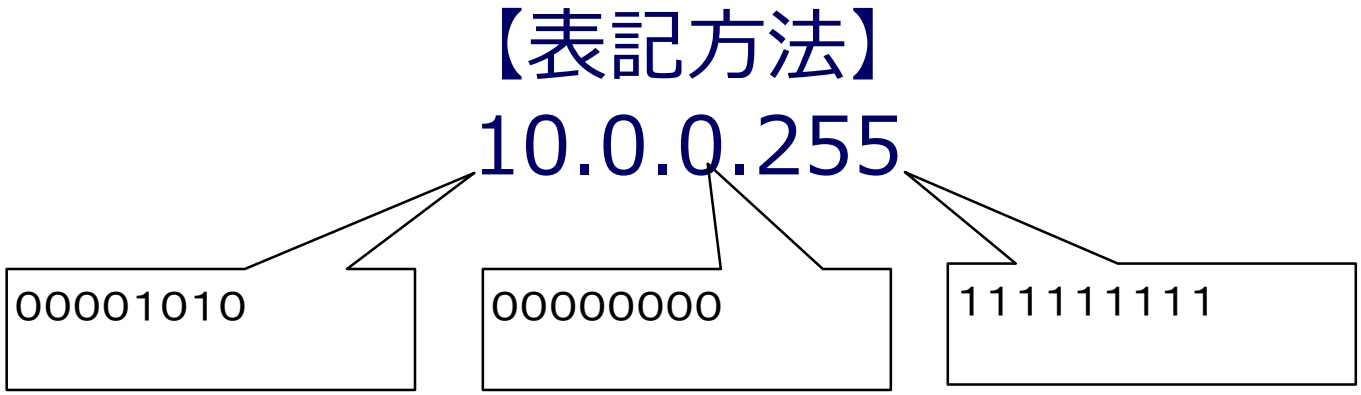
VPCとサブネットの組合せでネットワーク空間を構築する
VPCはサブネットとのセットが必須

VPC設定手順


CIDR方式で
アドレス
レンジを選択
AZの
サブネット
を選択
インターネット
経路を選択
VPCへの
トラフィック
許可の設定

IPアドレス

IPアドレスは3桁（0～255）×4つの組合せで、各桁が8つのバイナリ値の集合を表す



CIDR（Classless Inter-Domain Routing）

サブネットマスクの値を設定し、同じネットワークとして扱う
IPアドレスの個数を調整できるIPアドレスの設定方法

【表記方法】

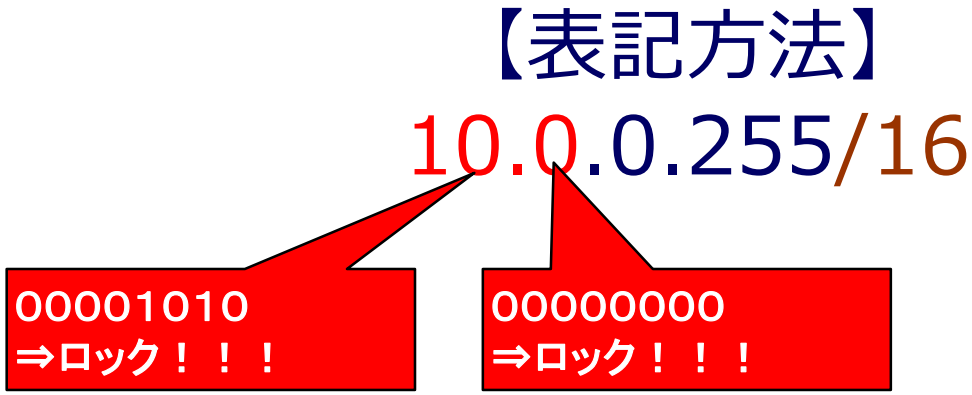
196.51.100.XXX/16

サブネット

左から16桁目までが同じネットワーク範囲と指定

CIDR（Classless Inter-Domain Routing）

左16桁分が利用できないようにロックされて変更不可となる

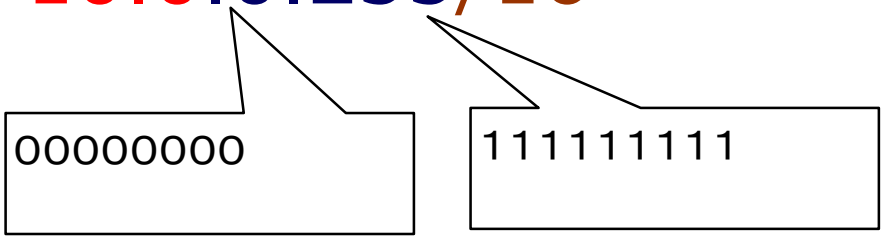


CIDR（Classless Inter-Domain Routing）

ロックされていない16桁分のビットの間が有効なIPアドレスとして活用できる

【表記方法】

10.0.0.255/16



CIDR（Classless Inter-Domain Routing）

ロックされていない16桁分のビットの間が有効なIPアドレスとして活用できる

【最小値】
10.0.0.0

【最大値】
10.0.255.255

CIDR

IPアドレスの範囲は今後の拡張も踏まえて十分な余裕がありつつ、多すぎないレンジを指定する

10.0.0.255/16

推奨レンジ（65,534アドレス）

CIDR

VPCは/16　~　/28のCIDR範囲を使用できる

/16　~　/28

CIDR

CIDRに/16を設定した際に設定可能となるサブネット数とIPアドレス数の組合せ

サブネットマスク	サブネット数	サブネット当たりのIPアドレス数
/18	4	16379
/20	16	4091
/22	64	1019
/24	256	251
/26	1024	59
/28	16384	11

CIDR

既に利用されているなどして設定できないアドレスもある（/24の例）

ホストアドレス	用途
.0	ネットワークアドレス
.1	VPCルータ
.2	Amazonが提供するDNSサービス
.3	AWSで予約されているアドレス
.255	ブロードキャストアドレス

サブネット

サブネットはCIDR範囲で分割したネットワークセグメント

パブリックサブネット
10.0.1.0/24

EC2

トラフィックがインターネットゲートウェイにルーティングされるサブネット

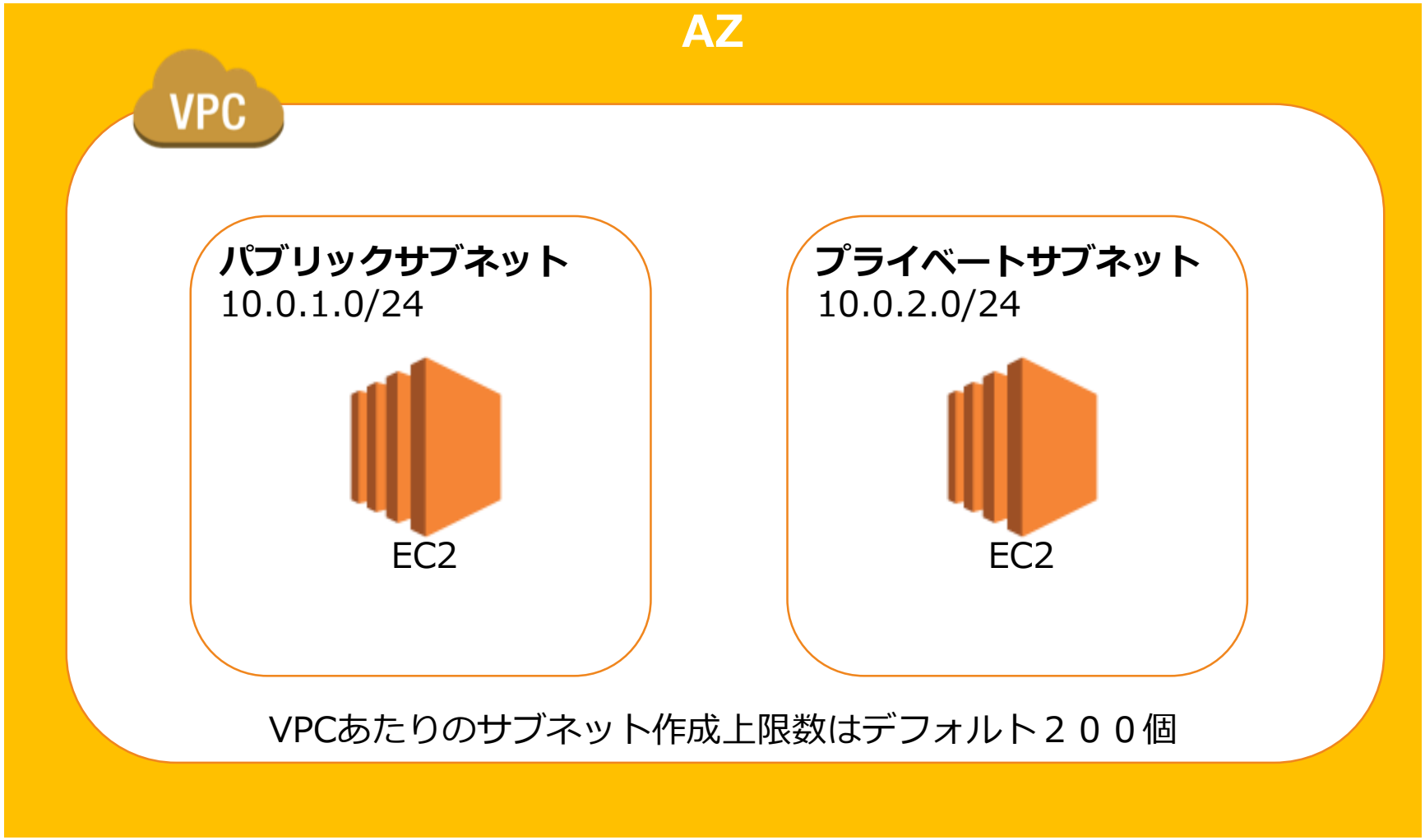
プライベートサブネット
10.0.2.0/24

EC2

インターネットゲートウェイへのルートがないサブネット

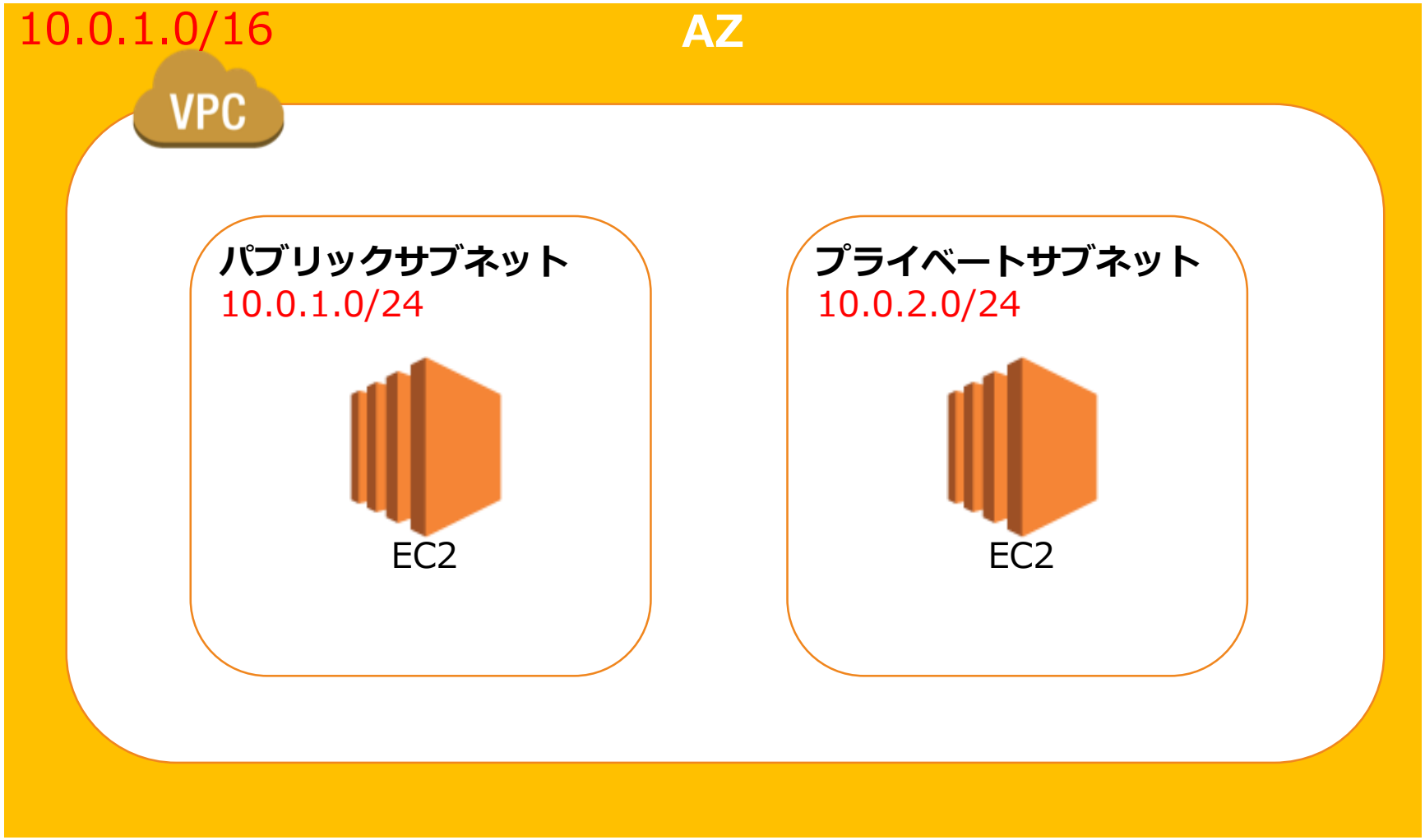
サブネット

サブネットはVPC内に複数設置でき、プライベートとパブリックに分かれる



IPアドレスの付与

VPCとサブネットにはIPアドレスが付与され識別される



サブネット

インターネットゲートウェイへのルーティング有無でサブネットのタイプが分かれる

パブリックサブネット
10.0.1.0/24

EC2

トラフィックがインターネットゲートウェイにルーティングされるサブネット

プライベートサブネット
10.0.2.0/24

EC2

インターネットゲートウェイへのルートがないサブネット

サブネット

サブネットはインターネットアクセス範囲を定義するために利用する

パブリックサブネット
10.0.1.0/24

EC2

インターネットと接続が必要なリソースを揃える

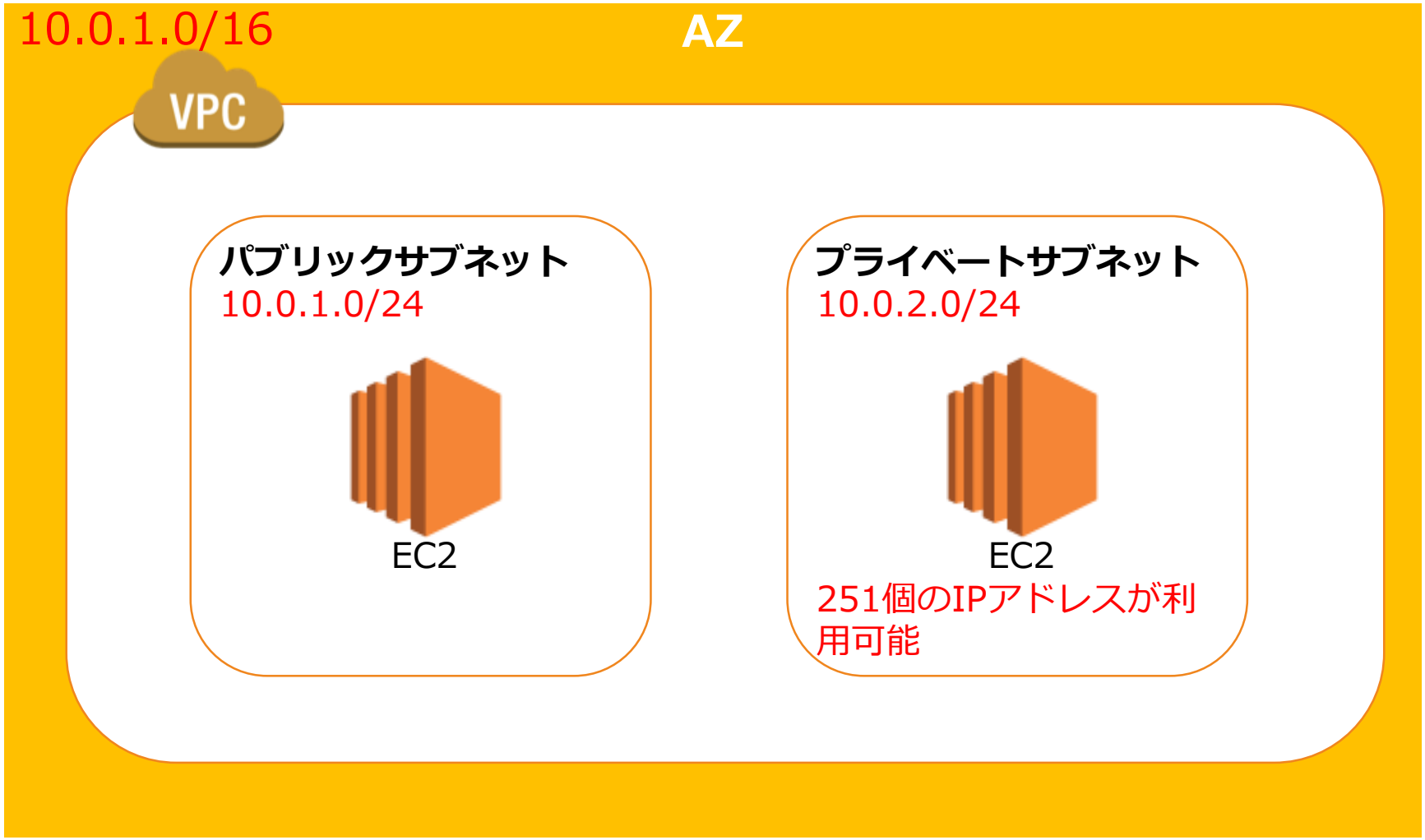
プライベートサブネット
10.0.2.0/24

EC2

インターネットから隔離することでセキュリティを高める

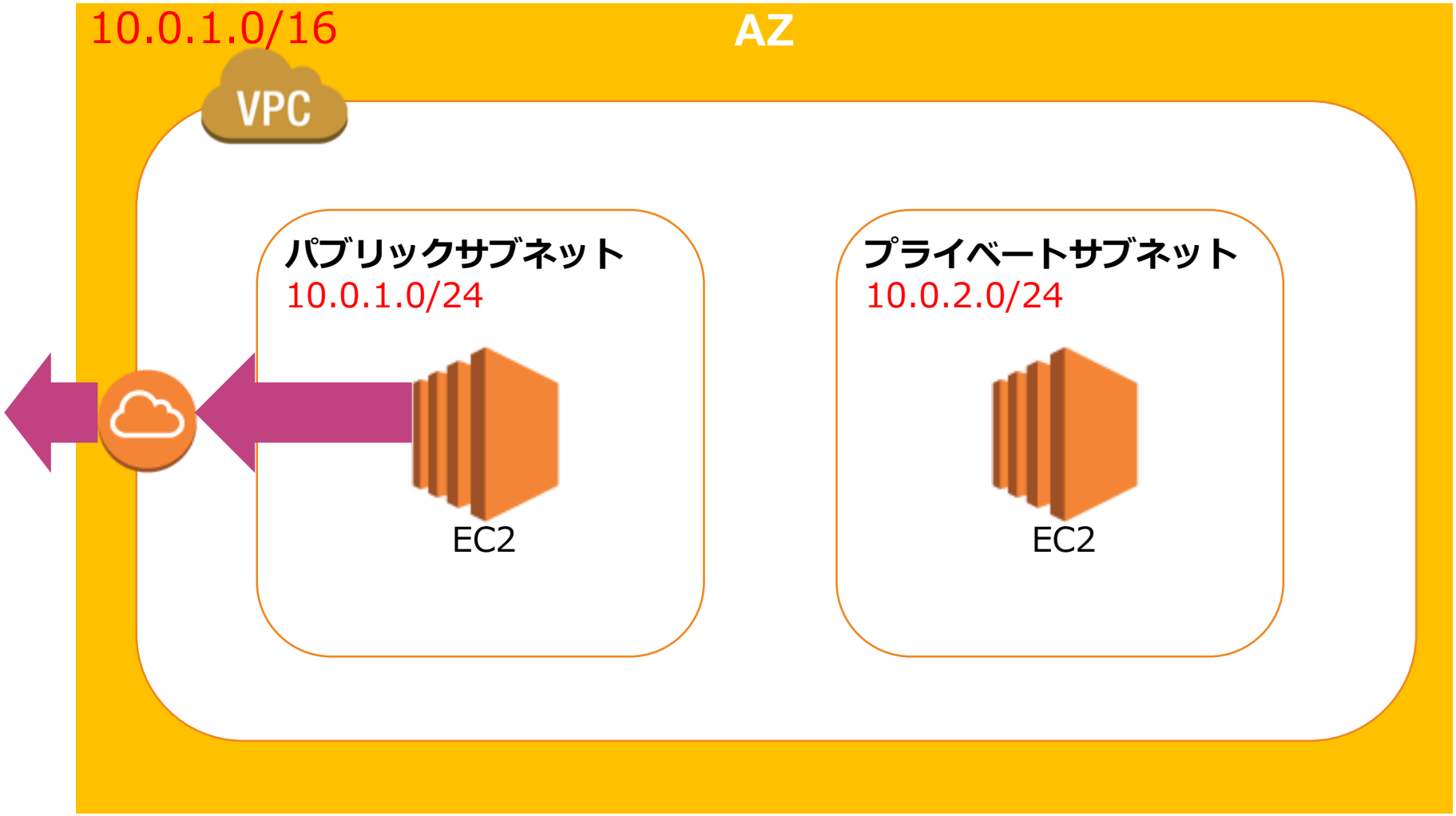
VPCにサブネットを設定

VPCにCIDR/16を設定し、サブネットに/24の設定を推奨



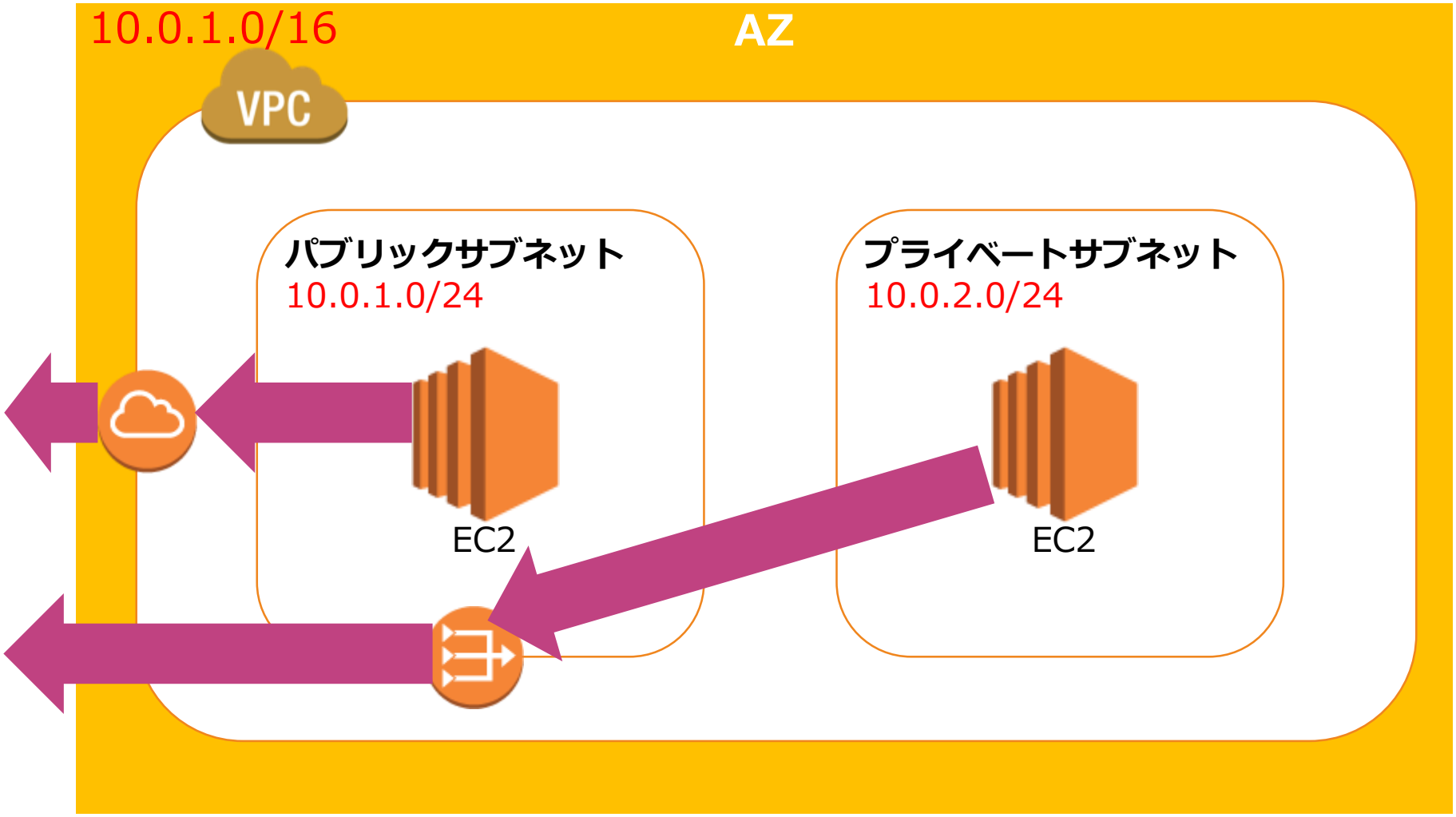
VPC外部接続

パブリックサブネットからインターネットに接続するにはインターネットゲートウェイが必要



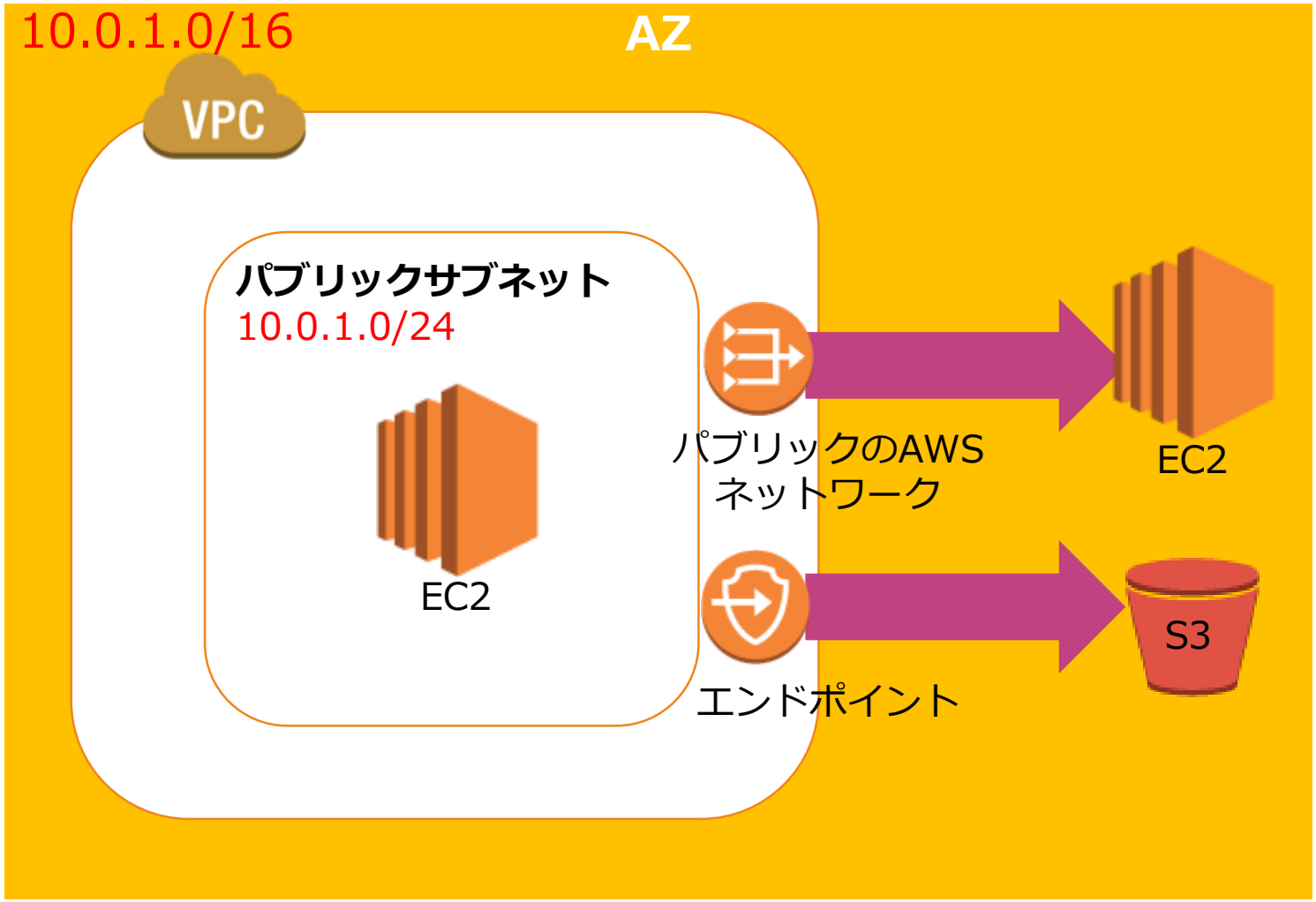
VPC外部接続

プライベートサブネットからインターネットに接続するには
NATゲートウェイがパブリックサブネットに必要



VPC外部接続

VPCの外側にあるリソースとの通信にはパブリックのAWSネットワークかエンドポイントを利用する



インターネット経路を設定

ルートテーブルとCIDRアドレスでルーティングを設定する

- ルートテーブルでパケットの行き先を設定
- VPC作成時にデフォルトで１つルートテーブルを作成
- VPC内はCIDRアドレスでルーティング

VPCトラフィック設定

トラフィック設定はセキュリティグループまたはネットワークACLを利用する

セキュリティグループ設定

- ステートフル：戻りトラフィックの考慮がいらない
- サーバー単位で適用
- 許可のみをIn/outで指定
- デフォルトでは同じセキュリティグループ内通信のみ許可
- 必要な通信は許可設定が必要
- 全てのルールを適用

ネットワークACLs設定

- ステートレス：戻りトラフィックも許可設定が必要
- サブネット単位で適用
- 許可と拒否をIn/outで指定
- デフォルトでは全ての送信元IPを許可
- 番号の順序通りに適用

VPC設計ポイント

- 設計時には将来の拡張も見据えたアドレッシングや 他ネットワークとの接続性も考慮する
- CIDR(IPアドレス)は既存のVPC、社内のDCやオフィスと被らないアドレス帯を設定し、組織構成やシステム構成の将来像も考えながら前もって計画する
- VPC構成は自社業務に合せたVPC単体ではなくVPC全体の関係性も視野に入れる
- 組織とシステム境界からVPCをどのように分割するか将来構成も考慮して検討する
- 複数AZを利用して可用性の高いシステムを構築
- サブネットは大きいサブネットを使い、パブリック/プライベートサブネットへのリソースの配置をインターネットアクセス可否から検討する
- セキュリティグループを使ってリソース間のトラフィックを適切に制御する
- 実装や運用を補助するツールも有効利用し、VPC Flow Logsを使ってモニタリングできるようにする