御社の IT インフラを拡張

Amazon Virtual Private Cloud で

***2010* 年 *1* 月**

最終更新 *2012* 年 *9* 月

amazon web services

目次

はじめに

Amazon Virtual Private Cloud（Amazon VPC）では、アマゾン ウェブ サービス（AWS）クラウドの分離したプライベートセクションをプロビジョニングし、ここで、お客様が定義した仮想ネットワークで AWS リソースを起動することができます。Amazon VPC では、お客様のデータセンターで運用されている従来型のネットワークを正確に模して、仮想ネットワークのトポロジーを定義することができます。独自の IP アドレス範囲の選択、サブネットの作成、ルートテーブル、ネットワークゲートウェイの設定など、仮想ネットワーク環境を完全にコントロールできます。例えば、VPC を使用すると以下のことが可能です。

- 既存のオンプレミスインフラストラクチャの容量を拡大する。
- 災害対策のためにお客様の環境のバックアップスタックを開始する。
- PCI-DSS（Payment Card Industry Data Security Standard）に準拠した、安全な決済が可能なウェブサイトを開設する。
- 独立した開発およびテスト環境を構築する。
- お客様の企業ネットワーク内で仮想デスクトップアプリケーションを提供する。

これらのユースケースを実現する際、従来型の方法では、独自のデータセンターの建設、必要なハードウェアのプロビジョニング、必要なセキュリティ証明書の取得、システム管理者の採用、諸般の運用に多額の事前投資が必要です。AWS の VPC では、事前投資がほとんど必要なく、必要に応じてインフラストラクチャの規模を変化させることができます。安全な環境によるすべてのメリットを追加費用なしで手に入れることができます。AWS のセキュリティ制御、証明書、認可、および機能は、最高レベルの思慮とセキュリティ意識を備えた大企業や政府機関のお客様が定めたセキュリティ基準を満たすものです。証明書と認証の詳細については、AWS Security and Compliance Center[1] をご覧ください。

このドキュメントでは、Amazon VPC および関連サービスの一般的ユースケースとベストプラクティスについて説明します。

Amazon Virtual Private Cloud について

概要

Amazon VPC は、お客様が定義する仮想ネットワーク内で AWS リソースを起動することができる、AWS Cloud の安全でプライベートな独立したセクションです。VPC を作成するときは、VPC 内のインスタンスが使用するプライベート IP アドレスのセットを指定します。このアドレスのセットは、Classless Inter-Domain Routing[2]（CIDR）ブロックの形式で、10.0.0.0/16 のように指定します。ブロックサイズは、/28（16 個の IP アドレス）から /16（65,536 個の IP アドレス）の間で割り当てることができます。

Amazon VPC では、Amazon EC2 の各インスタンスのデフォルトネットワークインターフェイスに Amazon VPC ネットワークのプライマリプライベート IP アドレスが割り当てられられます。追加の Elastic Network

[1] http://aws.amazon.com/security/
[2] http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing

Interfaces（ENI）を作成して、お客様の VPC 内の任意の EC2 インスタンスにアタッチできます。各 ENI は、それぞれ独自の MAC アドレスを持ちます。ENI は複数のプライベート IP アドレスを持つこともでき、特定のセキュリティグループに割り当てることができます。1 つのインスタンスでサポートされる ENI とプライベート IP アドレスの数の合計は、インスタンスタイプ[3]によって決まります。ENI は同じアベイラビリティーゾーン内の複数のサブネット内に作成し、低コストの管理ネットワークやネットワークおよびセキュリティアプライアンスなどをビルドする 1 つのインスタンスにアタッチすることができます。セカンダリ ENI およびプライベート IP アドレスは同じサブネット内で他のインスタンスに移動でき、これによって低コスト、高可用性のソリューションを実現できます。各プライベート IP アドレスに対してパブリックの Elastic IP アドレス（EIP）を割り当てて、そのインスタンスにインターネットからアクセスできるようにすることができます。複数の IP および EIP がサポートされているため、1 つのサーバーに対して複数の SSL 証明書を使用し、各証明書に特定の IP アドレスを割り当てることもできます。

VPC でデプロイできるコンポーネントの数には、Amazon Virtual Private Cloud User Guide[4] で説明されているようにデフォルトでいくつかの制限があります。この制限数の増加をご希望の場合は、Amazon VPC 制限フォームに記入してください。[5]

ネットワーク分離レベルについて

VPC サブネットは、パブリック、プライベート、または *VPN* のみに設定できます。パブリックサブネットを設定するには、そのサブネットからインターネットへのトラフィックが、VPC に関連付けられているインターネットゲートウェイを経由するようにルーティングテーブルを設定する必要があります。そのサブネット内のインスタンスに EIP アドレスを割り当てると、そのアドレスはインターネットからもアクセスできるようになります。ベストプラクティスは、サブネットのネットワーク ACL[6]（ネットワークアクセスコントロールリスト）とインスタンスのセキュリティグループ[7]を設定することにより、これらのインスタンスに関する送受信トラフィックを制限することです。

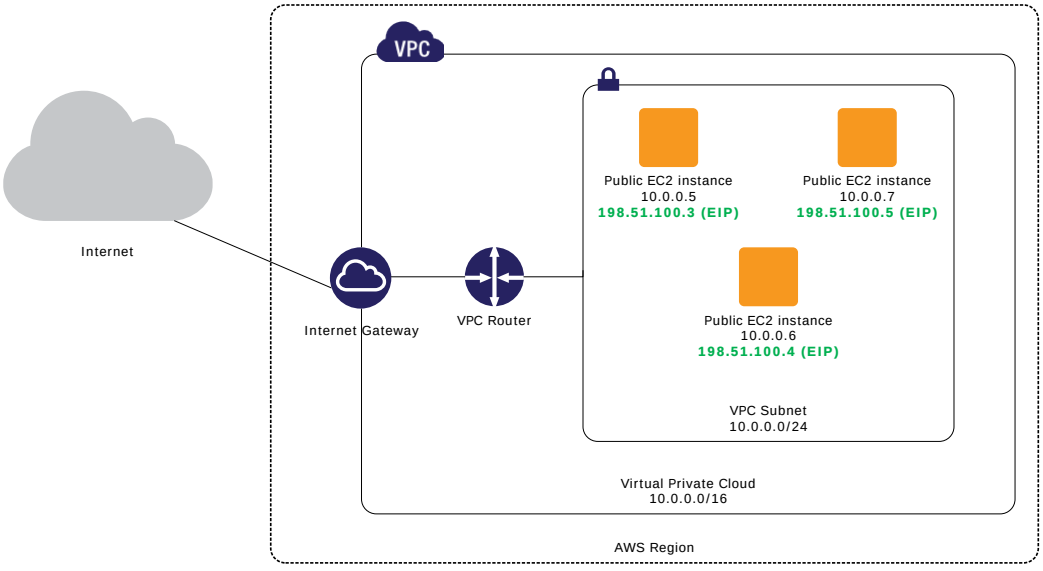

図 1 – パブリックサブネットだけを持つ VPC の例

[3] http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/instance-types.html
[4] http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html
[5] http://aws.amazon.com/contact-us/vpc-request/
[6] http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html
[7] http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

プライベートサブネットの場合、インターネットへのトラフィックは、パブリックサブネット内の、パブリック EIP が割り当てられた特殊な NAT（Network Address Translation）インスタンスを経由してルーティングする必要があります。この設定では、プライベートサブネット上のリソースは、EIP を割り当てることも直接受信接続を受け入れることもせずに、送信トラフィックをインターネットに接続することができます。AWS には、お客様が使用できるように事前設定された NAT サーバーイメージが用意されています。

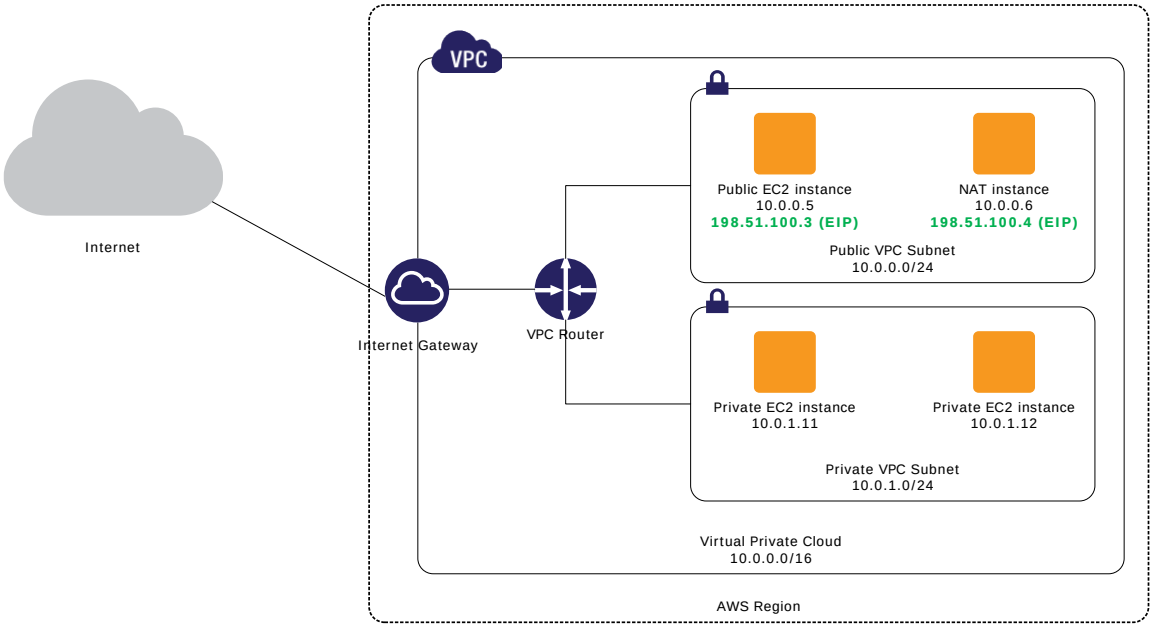

図 2 – パブリックおよびプライベートサブネットを持つ VPC の例

お客様の VPC に仮想プライベートゲートウェイをアタッチすることにより、お客様の VPC とお客様独自のデータセンターとの間に VPN 接続を作成できます。VPN 接続では、業界標準の IPsec をトンネルモードで使用（IKEv1-PSK、AES-128、HMAC-SHA-1、PFS）することにより、ゲートウェイ間の相互認証を実現し、データ送信中の盗聴や改変から保護します。IPsec では、カプセル化により追加されるオーバーヘッドは最小限にとどまります。冗長化のために、各 VPN 接続には 2 つのトンネルがあり、それぞれのトンネルが固有の仮想プライベートゲートウェイのパブリック IP アドレスを使用します。

VPN 接続の設定には、Border Gateway Protocol[8]（BGP）と静的ルーティングの 2 つのルーティングオプションがあります。BGP の場合、IP アドレスと、それを VPC にアタッチするためのカスタマーゲートウェイの BGP Autonomous System Number（ASN）が必要です。この情報を提供すると、サポートされているカスタマーゲートウェイのハードウェアアプライアンスの設定ファイルをダウンロードし、両方の VPN トンネルを設定することができます。BGP をサポートしていないデバイスの場合は、VPC 接続の設定時に当該の CIDR 範囲を指定して、オンプレミスネットワークに対して 1 つ以上の静的ループバックを設定します。次に、お客様の VPC に対するトラフィックを IPsec トンネル経由でルーティングするために、VPN Customer Gateway および他の内部ネットワークデバイスに静的ルートを設定します。

オンプレミスネットワークとの接続のある仮想プライベートゲートウェイのみを選択した場合、インターネット経由のトラフィックを VPN 上にルーティングし、セキュリティポリシーと組織のファイアウォールによって受信トラフィックをコントロールできます。

[8] http://en.wikipedia.org/wiki/Border_Gateway_Protocol

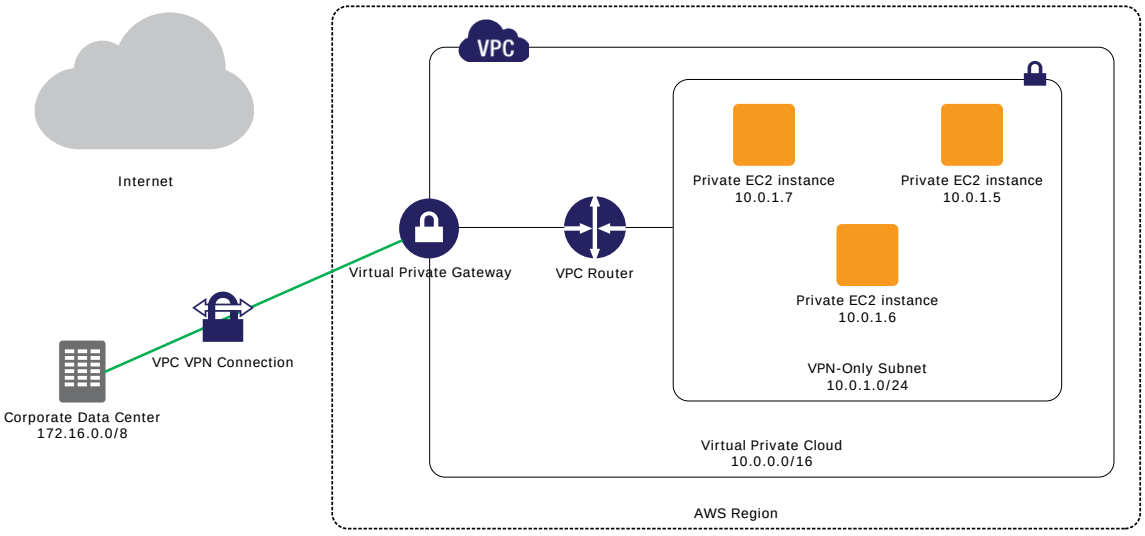

図 3 – インターネットから切り離され、VPN 経由でコーポレートデータセンターに接続されている VPC の例

AWS Direct Connect を使用して、オンプレミスのネットワークからお客様の Amazon VPC に直接、プライベート論理接続を確立できます。AWS Direct Connect は、お客様のネットワークと VPC の間にプライベートの広帯域ネットワーク接続を提供します。複数の論理接続を使用することにより、複数の VPC へのプライベート接続を確立すると共に、ネットワークの独立性を維持できます。

AWS Direct Connect を使用すると、AWS と任意の AWS Direct Connect ロケーション [9]との間に 1 Gbps または 10 Gbps の専用ネットワーク接続を確立できます。1 つの専用接続を、業界標準の 802.1q VLAN を使用して複数の論理接続に分割できます。これにより、同じ接続を使用して、パブリック IP アドレス空間を使用する、Amazon Simple Storage Service（Amazon S3）に格納されているオブジェクトなどのパブリックリソースにも、プライベート IP 空間を使用して VPC 内で実行される Amazon Elastic Compute Cloud（Amazon EC2）インスタンスのようなプライベートリソースにもアクセスでき、その際常にパブリック環境とプライベート環境の間のネットワーク分離を維持できます。WAN サービスプロバイダ [10]のエコシステムから選んで、AWS Direct Connect ロケーションにある AWS Direct Connect エンドポイントをリモートネットワークに統合することができます。Figure 4 に、一般的な AWS Direct Connect 設定を示します。

[9]サポートされている Direct Connect ロケーションおよびサービスプロバイダについては、http://aws.amazon.com/directconnect/ をご覧ください。
[10] http://aws.amazon.com/directconnect/#details

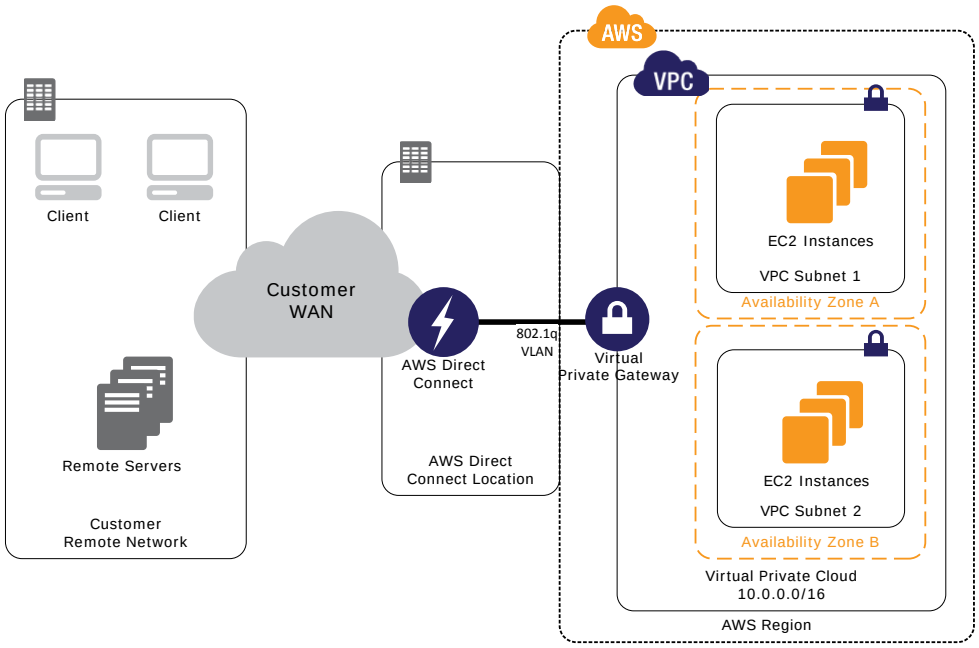

図 4 – カスタマーリモートネットワークと接続された VPC Direct Connect

これらのさまざまな機器を統合することができます。例えば、仮想プライベートゲートウェイを備えた既存のデータセンターに VPC をアタッチし、追加のパブリックサブネットを設定して、Amazon S3、Amazon Simple Queue Service（Amazon SQS）、Amazon Simple Notification Service（Amazon SNS）など、その VPC 内で実行されていない他の AWS サービスに接続できます。その場合、これらのサービスに対して専用の AWS Identity and Access Management（IAM）ユーザーを設定し、それらのユーザーが NAT サーバーの Elastic IP アドレスだけを受け入れるように IAM ポリシーを設定する必要があります。

シナリオ例

Amazon VPC が本来的に備えている柔軟性により、多様なユースケースにおけるお客様のビジネスおよび IT セキュリティの要件を適確に満たす仮想ネットワークトポロジーを設計できます。Amazon VPC の潜在力を正しく理解していただくために、以下に示すいくつかの最も一般的なユースケースをご覧ください。

- PCI 準拠の e コマースウェブサイトをホストする
- 開発およびテスト環境を構築する
- 災害対策およびビジネス継続のための計画を立てる
- データセンターをクラウドに拡張する
- ブランチオフィスとビジネスユニットのネットワークを構築する
- 仮想デスクトップインフラストラクチャを構築する

PCI 準拠の e コマースウェブサイトをホストする

e コマースウェブサイトでは、クレジットカード情報、ユーザープロフィール、購入履歴などの機密データを扱うことがあります。そのため、これらのサイトでは、顧客の機密データを保護するために PCI DSS（Payment Card Industry Data Security Standard）に準拠したインフラストラクチャが必要です。

AWS は Payment Card Industry Data Security Standard（PCI DSS）でレベル 1 のサービスプロバイダとして認定されているため、PCI に準拠したテクノロジーインフラストラクチャ上でお客様のアプリケーションを実行して、クラウド内でクレジットカード情報を格納、処理、送信できます。お客様は販売業者として、引き続き独自の PCI 証明書を管理する必要がありますが、認定済みのインフラストラクチャサービスプロバイダを使用することで、インフラストラクチャレベルでの PCI への準拠は考慮しなくて済みます。PCI 準拠の詳細については、AWS セキュリティセンターをご覧ください。[11]

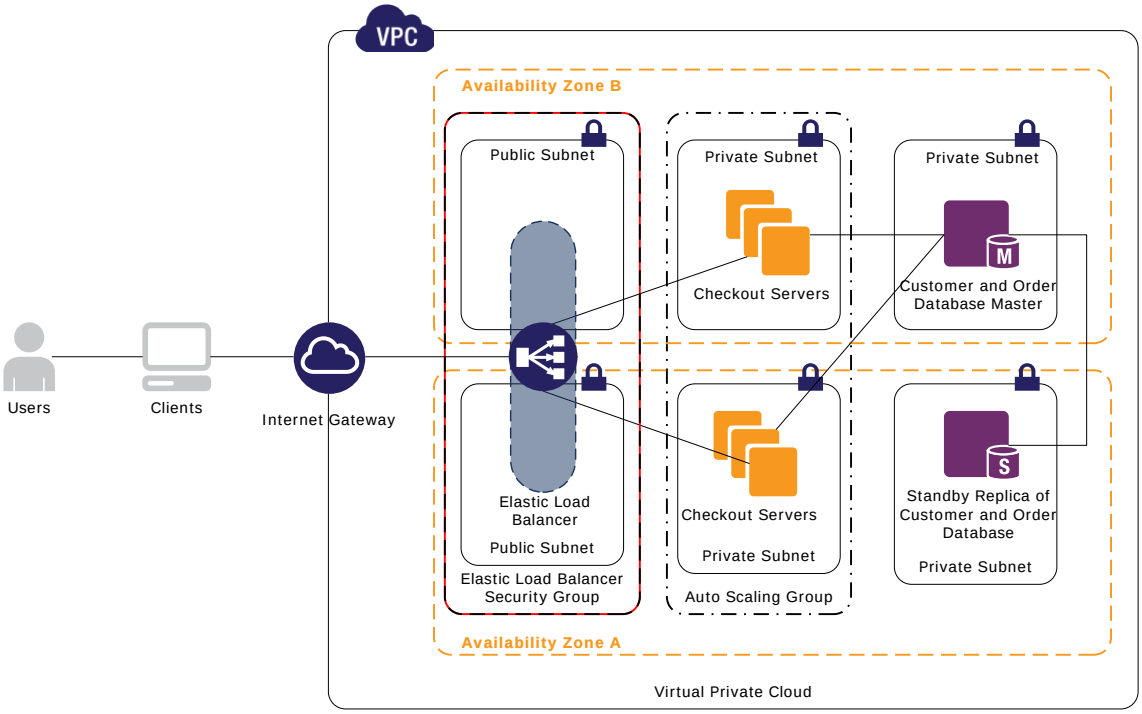

図 5 – チェックアウトアーキテクチャの例

例えば、カスタマーデータベースをホストし、e コマースウェブサイトのチェックアウトプロセスを管理する VPC を作成するとします。高度な可用性を実現するために、1 つのリージョン内のアベイラビリティーゾーンごとにプライベートサブネットを設定し、各アベイラビリティーゾーン内でカスタマーおよび注文の管理データベースをデプロイします。お客様の複数のチェックアウトサーバーは、複数のアベイラビリティーゾーン内の複数のプライベートサブネットに渡る 1 つの Auto Scaling グループに含まれます。これらのサーバーは、使用されるすべてのアベイラビリティーゾーンに渡るパブリックサブネットを対象としたエラスティックロードバランサーの背後に置かれます。VPC、サブネット、ネットワーク ACL、およびセキュリティグループを統合することにより、AWS インフラストラクチャを細かく制御できます。e コマースウェブサイトの中で最も対応の難しい、スケーラビリティ、セキュリティ、伸縮自在性、可用性という主要な課題に対して備えが用意されています。

[11] http://aws.amazon.com/security/#certifications

開発およびテスト環境を構築する

ソフトウェア環境は、新しいバージョンのリリース、機能の追加、パッチ、アップデートにより、絶えず変化します。ソフトウェアの変更は迅速にデプロイする必要があり、回帰テストを実行する時間はほとんどありません。本稼働環境をそっくりそのまま複製してテストラボとし、これに更新を適用してから負荷テストを実施できれば申し分ありません。ソフトウェアのアップデートまたは新バージョンがすべてのテストに合格すれば、一層の自信を持って本稼働環境に導入できます。

このようなテストラボを社内で構築するには大量のハードウェアを用意する必要がありますが、そのほとんどは普段眠らせておくことになります。しかも、そのようなハードウェアは往々にして本稼働用のハードウェアとして転用され、必要なときにテストラボを構築できなくなります。Amazon VPC を使用すると、最新の本稼働環境をシミュレートし、本稼働環境に影響を与えることなく新しい機能をテストできる、経済的で機能的なテストラボを構築できます。テスト環境は必要に応じて開始でき、テストが終わったらシャットダウンできます。高価なハードウェアを購入する必要はなく、環境の変化にも柔軟かつ迅速に対応できます。テスト環境は、LDAP、メッセージング、およびモニタリングを使用することによってお客様のオンプレミスネットワークと透過的に対話できます。また、支払いは実際に使用した AWS に対してのみ発生します。このプロセスは、全面的に自動化することも、お客様のソフトウェア開発プロセスに組み込むこともできます。

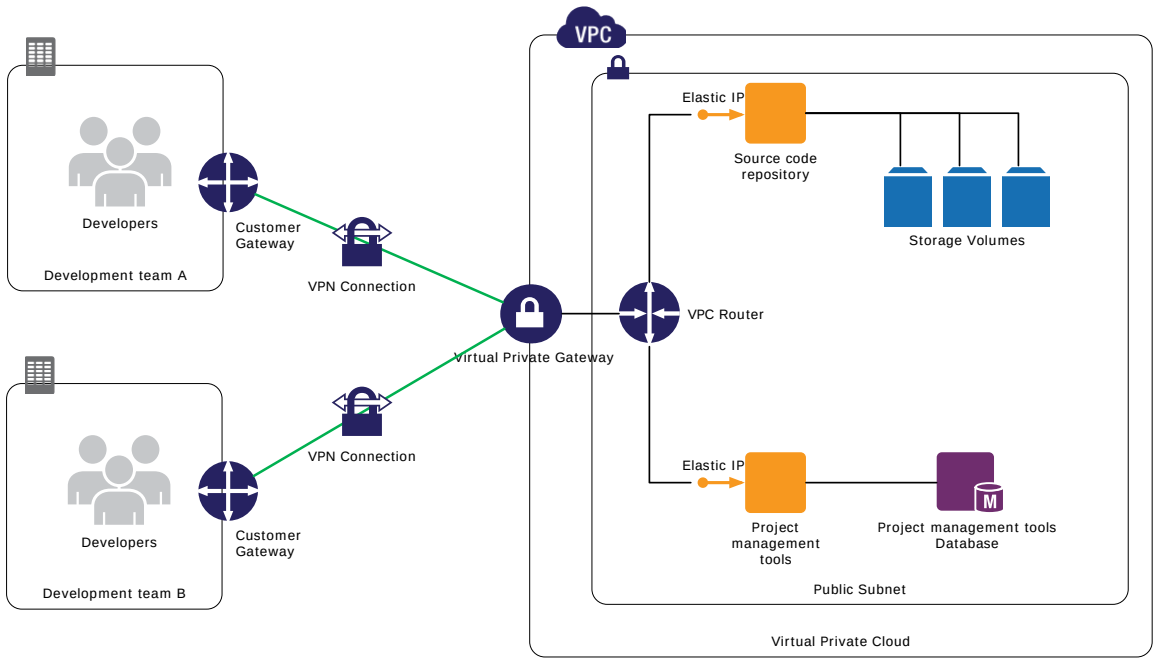

図 6 – 開発およびテスト環境の例

同様のロジックが実験的なアプリケーションにも適用されます。本稼働環境から切り離しておきたい新しいソフトウェアパッケージを評価する際は、VPC 内のテスト環境でいくつかの Amazon EC2 インスタンスにインストールし、一部の内部ユーザーを選んでアクセスを許可します。すべてが正しく動作したら、それらのイメージを本稼働環境に移行し、不要なリソースを終了します。

災害対策および事業継続のための計画を立てる

災害がお客様のデータセンターに与える影響は、そのような事態に備えておかなかった場合、お客様のビジネスにとって壊滅的なものになるおそれがあります。そのような事態が発生したときにオペレーションが受ける影響を最小限に抑えるための戦略を考えることは、時間をかける価値のあることです。災害復旧

に対する従来のアプローチでは、通常労働集約的なバックアップと高価なスタンバイ装置を必要とします。代わりに、御社の災害回復計画に Amazon VPC の導入を検討してください。AWS の弾力性のあるダイナミックな特性は、リソース要件が突然上昇する災害シナリオに最適です。

最初に、御社のビジネスで最も重要な IT 資産を特定します。このドキュメントですでに説明したテスト環境のように、本稼働環境の複製を自動化して重要なアセットの機能をコピーすることができます。自動化プロセスを使用すると、本稼働データを Amazon EBS ボリュームや Amazon S3 バケットにバックアップできます。宣言型の AWS CloudFormation テンプレートを記述して VPC インフラストラクチャスタックを表し、任意の AWS リージョンまたはアベイラビリティーゾーン内で自動的に開始することができます。

災害が発生した際は、VPC 内の環境ですぐに複製を起動し、ビジネスのトラフィックがそちらのサーバーに向かうようにします。災害によって社内のサーバーからデータが失われた場合は、バックアップストレージとして使用していた Amazon EBS データボリュームから復元できます。

詳細については、AWS アーキテクチャセンター[12]の「Using Amazon Web Services for Disaster Recovery」をご覧ください。

データセンターをクラウドに拡張する

データセンターの構築に投資した場合は、変化し続ける容量の要件に追随していくという課題に直面することが考えられます。不定期に発生する大きな需要が総容量を超えることもあり得ます。事業が順調であれば、定型的なオペレーションさえもやがてはデータセンターの容量の限界に達し、その容量をどのようにして拡張するか決断しなければなりません。新しいデータセンターを構築することも 1 つの方法ですが、費用だけでなく時間もかかり、プロビジョニングが需要を下回る、または上回るリスクが高くなります。いずれの場合も、Amazon VPC はお客様のデータセンターの拡張として利用できます。

クラウドのリソースは、安全に保たれること、およびユーザーからオンプレミスのリソースと同じように見え、動作することが重要です。お客様の環境と AWS クラウドの間の接続が適切に実装されていることは、これらの要件が満たされるのに役立ちます。オンプレミスのネットワークを VPC 内の AWS リソースに接続するために、データセンター内にカスタマーゲートウェイ、VPC に仮想プライベートゲートウェイをそれぞれ作成できます。これらのゲートウェイは、VPN によって接続されます。VPC は、インターネットから隔離するためにインターネットゲートウェイを使用せずに作成することが考えられます。

オプションで、AWS Direct Connect を使用して、プライベート、低遅延、広帯域の VPC への接続を実現できます。VPC をブランチオフィスと同様に扱って、独自の IP アドレス範囲を VPC に割り当てることができます。データセンターに物理ハードウェアを追加することなく、コーポレートアプリケーションを VPC に移動したり、追加のウェブサーバーを開始したり、コンピューティング能力をネットワークに追加することができます。VPC はお客様のファイアウォールの内側でホストすることが可能なため、これらのアプリケーションに対するユーザーのアクセス方法を変更することなく、シームレスに IT リソースをクラウドに移行することができます。データセンターの VPC を拡張する設定の例については、Figure 3 このドキュメントのここまでの記述をご覧ください。

[12] http://aws.amazon.com/architecture/

ブランチオフィスとビジネスユニットのネットワークを構築する

現在ローカルネットワークと相互接続しているが、分離する必要のあるブランチオフィスが御社にある場合は、Amazon VPC 内部にリソースを配置し、各オフィスにそのサブネットを割り当てることを検討してください。VPC サブネット内のアプリケーションは、適用する VPC セキュリティグループに応じて相互にオープンでコミュニケーションを行えます。また、アプリケーションは、バーチャルルーターを通じてサブネット全体でコミュニケーションを行えます。サブネット内、またはサブネット間のフローを制限する必要がある場合は、相互にコミュニケーションを行えるサーバーを定義するセキュリティグループまたはネットワーク ACL を設定できます。この同じ考え方をビジネスユニット機能に従ってグループアプリケーションにも適用できます。特定のビジネスユニットに固有のアプリケーションは、別のサブネットに、各ユニットに 1 つずつインストールできます。

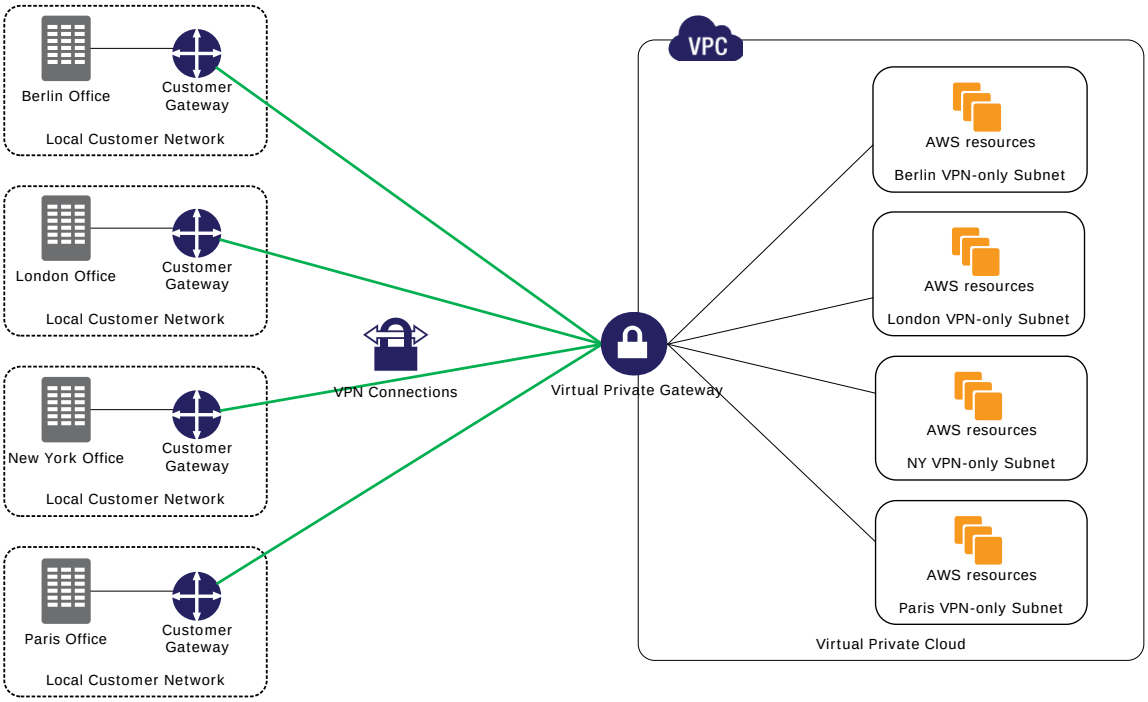

図 7 – ブランチオフィスで VPC および VPN を使用するシナリオ

ブランチオフィスで専用のオンプレミスハードウェアをプロビジョニングすることと比較した場合の Amazon VPC を使用することの主なメリットは、他の場所で説明したものと似ています。すなわち、需要に合うようにリソースを伸縮自在に増減したり、追加、削除したりして、プロビジョニング不足や過剰プロビジョニングを避けられることです。容量の追加は、カスタムの Amazon マシンイメージ（AMI）から追加の Amazon EC2 インスタンスを開始するだけで簡単に実行できます。容量を減らす必要があるときは、単に不要なインスタンスを手動で終了するか、Auto Scaling ポリシーを使用して自動的に終了します。アセットを適切に実行し続けるための運用タスクは同じですが、専任のリモートスタッフが不要になり、使用した分だけを支払う価格モデルによって費用を節約できます。

仮想デスクトップインフラストラクチャを構築する

いくつかのベンダーが、Amazon EC2 でホストできるクライアント仮想化およびアプリケーションストリーミングのためのソリューション（Citrix 社の XenApp など）を提供しています。仮想デスクトップ、または VPC からのストリームクライアントアプリケーションをホストすると、例えば、御社の標準に沿った仮想

デスクトップをオンサイトの契約作業者が実行できるようにしたり、会社の VPN に接続した遠隔地の従業員や自宅作業者にオフィスと同じ環境を提供することができます。

例えば、社内セミナーを開催し、参加者が使用するために多数のクライアント PC の導入が必要な場合は、シンクライアントコンピュータをリースして、御社の VPC からロードするカスタマイズしたバーチャルデスクトップを実行すれば、コストを最小限に抑えることができます。短期間デスクトップ PC を必要とするプロジェクトやプログラムは、バーチャルデスクトップやアプリケーションストリーミングに適しています。たとえば、バーチャルデスクインフラ(VDI)を使用して、新規またはアップデートしたクライアントアプリケーションを導入前にテストすることが可能です。御社環境から隔離したまま特定のアプリケーションを実行するビジネス要件がある場合、VDI は効果的なサンドボックスを提供できます。

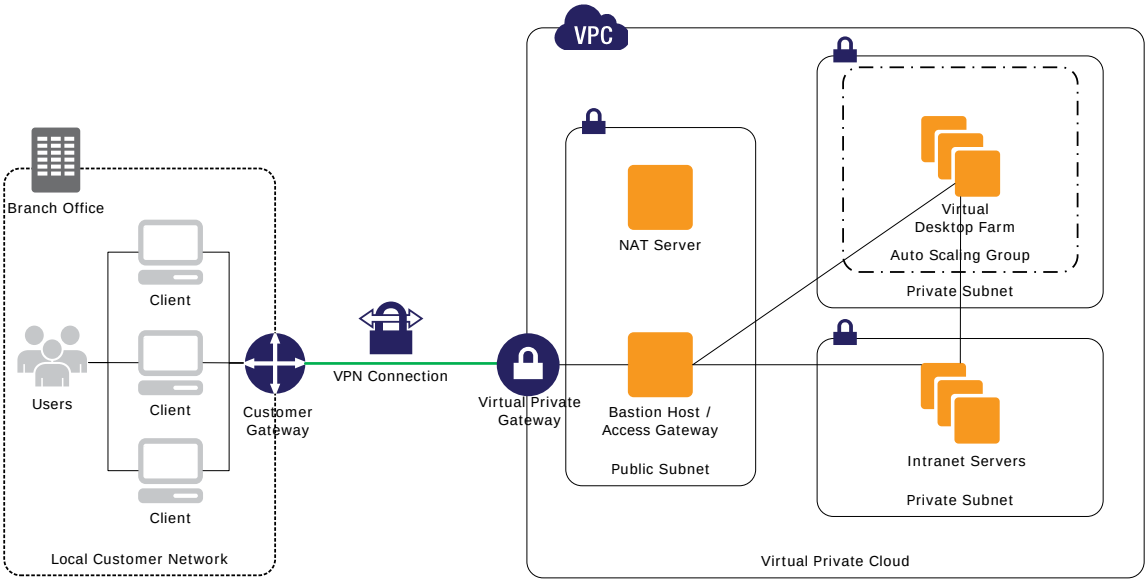

図 8 – 簡略化した VDI アーキテクチャの例

固定的なユーザーにとっても、仮想デスクトップインフラストラクチャとしての利点はあります。コンピューティングの負荷を Amazon VPC に移動することで、既存のクライアントハードウェアの寿命を延ばし、不要な資本支出を避けることができます。一元管理される VDI ソリューションにより、オペレーティングシステムに対する更新およびパッチ適用や新しいクライアントアプリケーションのデプロイが簡略化されます。さらに、移動することがない従業員が在籍する高度に統制された業界では、一元管理される VDI ソリューションによりデータ損失やマルウェアの伝染リスクが大幅に減少されます。

Amazon VPC 使用のベストプラクティス

インフラストラクチャのデプロイを自動化する

インフラストラクチャの手動管理は、面倒でエラーが発生しやすく、時間も費用もかかります。例えば、災害対策の場合、計画に含める手動ステップはプロセスを遅延させるため、少なく抑えます。開発およびテスト環境など、それほど差し迫っていないユースケースでも、スタンバイ環境を確実に本稼働環境の正確な複製にすることをお勧めします。本稼働環境を手動で複製することは非常に難しい場合があり、デプロイされている要素の相互依存関係によっては、バグが混入したりバグを見逃したりする危険が高まります。

AWS CloudFormation によってデプロイを自動化することにより、テンプレートを記述してインフラストラクチャを宣言的に表すことができます。テンプレートを使用すると、いずれの AWS リージョンでもきわめて短い時間で定義済みのスタックをデプロイできます。テンプレートにより、サブネット、ルーティング情報、およびセキュリティグループの作成、AWS リソースのプロビジョニングなど、必要なあらゆることを全面的に自動化できます。AWS Cloudformation ヘルパーを使用することによって標準の Amazon マシンイメージ（AMI）を使用できます。AMI は、デプロイ環境で要求されるすべての正しいバージョンのソフトウェアを、Amazon EC2 インスタンスの開始時にインストールします。

インフラストラクチャの自動化されたデプロイは、御社のプロセスに完全に組み込む必要があります。自動化スクリプトは、御社の標準とポリシーに沿ったテストとメンテナンスが必要なソフトウェアと同じように扱ってください。ほとんどの VPC ユースケースは、優れた自動化戦略の恩恵を受けるはずです。多くの場合、完全にテストされた自動化プロセスは多数の手動ステップに依存するプロセスよりも高速で、低費用で、信頼性が高く、安全です。

高可用性のために VPC でマルチ AZ 配置を使用する

高可用性を実現するように設計されたアーキテクチャは、通常、AWS リソースを同一リージョン内の複数のアベイラビリティーゾーンに渡って冗長に配布します。1 つのアベイラビリティーゾーンでサービスが中断した場合は、他のアベイラビリティーゾーンにトラフィックをリダイレクトして中断の影響を限定します。この一般的なベストプラクティスは、Amazon VPC を含むアーキテクチャにも当てはまります。

VPC は複数のアベイラビリティーゾーンを対象にすることができますが、VPC 内の各サブネットは 1 つのアベイラビリティーゾーンに制限されます。例えばマルチ AZ で Amazon RDS DB インスタンスをデプロイするためには、最初に、データベースインスタンスを開始するリージョン内の各アベイラビリティーゾーンで VPC サブネットを設定する必要があります。Auto Scaling グループおよびエラスティックロードバランサーは、各ゾーンの VPC サブネットに渡ってデプロイすることにより、複数のアベイラビリティーゾーンを対象にすることができます。

セキュリティグループとネットワーク ACL を使用する

Amazon VPC は、パブリック AWS クラウドに対して追加のセキュリティ機能を備えています。EC2 セキュリティグループに追加の機能を提供するネットワーク ACL および VPC セキュリティグループを定義することができます。例えば、VPC セキュリティグループを使用すると、送受信トラフィックを制御（EC2 セキュリティグループでは受信のみを制御）でき、すべてのプロトコルおよびポートについてルールを定義できます（EC2 セキュリティグループでルールを定義できるのは TCP、UDP、ICMP のみ）。Amazon EC2 と Amazon VPC におけるセキュリティグループの違いに関する全体的な概要については、Amazon Virtual Private Cloud User Guide をご覧ください [13]。Amazon EC2 と Amazon VPC セキュリティグループは、どちらもステートフルなファイアウォールです。

ネットワーク ACL は、セキュリティの追加的なレイヤーであり、サブネットを出入りするトラフィックを制御するファイアウォールとして機能します。サブネットごとにアクセスコントロールのルールを定義できます。VPC セキュリティグループはインスタンスレベルで動作しますが、ネットワーク ACL はサブネッ

[13] http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

トレベルで動作します。ネットワーク ACL では、送受信に対して *allow* と *deny* の両方のルールを指定できます。ネットワーク ACL は NACL とも呼ばれ、ステートレスなファイアウォールです。

ベストプラクティスとして、インフラストラクチャは複数の防御レイヤーで保護する必要があります。VPC 内でインフラストラクチャを実行することにより、インターネットに対してどのインスタンスが最初に公開されるかを決めることができ、また、インフラストラクチャをインフラストラクチャとサブネットのレベルでさらに保護するためのセキュリティグループとネットワーク ACL を定義できます。また、オペレーティングシステムレベルのファイアウォールによってインスタンスを保護し、セキュリティに関して AWS Security and Compliance Center で説明している他のベストプラクティスに従う必要があります [14]。

IAM ユーザーとのロールの分離

AWS Identity and Access Management（IAM）により、アカウント内にユーザーを作成し、管理できます。AWS とやり取りする必要がある人またはアプリケーションをユーザーにすることができます。IAM を使用すると、アカウントのユーザー、セキュリティ認証情報（アクセス認証情報など）、およびユーザーがアクセスできる AWS リソースを制御するアクセス許可を集中管理できます。通常、IAM ユーザーはユーザー向けに作成し、アプリケーションに対しては IAM ロールを使用します。

IAM を使用して、最小限の特権というセキュリティ戦略を実装することをお勧めします。例えば、メインの AWS ユーザーアカウントを使用して AWS インフラストラクチャのすべての要素を管理することは避けます。代わりに、AWS で実行する必要があるタスクの違いに応じたユーザーグループを定義し、各ユーザーはそのロールを実行するために AWS が必要とする機能だけに制限します。例えば、IAM 内にユーザーのネットワーク管理者グループを作成し、そのグループだけに VPC を作成および変更する管理を与えます。ユーザーグループごとに制限のためのポリシーを定義し、それによって各ユーザーにそのユーザーの必要とするサービスへのアクセスだけを与えます。組織内の許可された人だけがこれらのユーザーにアクセスできるようにし、インフラストラクチャが侵害されるリスクを低くするために、認証情報は一定間隔で変更します。

IAM のユーザーおよびポリシーを定義する方法の詳細については、Amazon Virtual Private Cloud User Guide をご覧ください [15]。

Amazon Cloudwatch を使用して VPC インスタンスおよび VPN リンクの正常性をモニタリングする

パブリック Amazon EC2 インスタンスの場合と同様に、Amazon CloudWatch を使用することにより、VPC 内で実行されているインスタンスのパフォーマンスをモニタリングできます。Amazon CloudWatch を使用すると、CPU 使用率、ディスクの読み書き、ネットワークトラフィックなどを含め、リソースの使用状況、運用のパフォーマンス、全体的な需要パターンを知ることができます。情報は AWS マネジメントコンソールに表示され、CloudWatch API を通じて入手することもできるため、既存の管理ツールと統合できます。

VPN 接続は、AWS マネジメントコンソールまたは *vgw-telemetry* API アクションを使用することによってモニタリングできます。これらのツールには、どちらかのトンネルが停止中の場合、各 VPN トンネルの状態およびエラーメッセージ（アップ/ダウン）を含む、VPN 接続ステータスが表示されます。

[14] http://aws.amazon.com/security/
[15] http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPC_IAM.html

まとめ

Amazon VPC には、AWS インフラストラクチャを細かく制御できる幅広いツールが用意されています。VPC 内では、サブネットとルーティングテーブルを定義することによって独自のネットワークトポロジーを定義できます。また、ネットワーク ACL によってサブネットレベルで、VPC セキュリティグループによってリソースレベルで、それぞれアクセスを制限できます。リソースをインターネットから分離し、VPN を通じて自社のデータセンターに接続することができます。一部のインスタンスに Elastic IP アドレスを割り当て、インフラストラクチャの他の部分はプライベートサブネットにとどめたまま、それらのインスタンスをインターネットゲートウェイ経由でパブリックのインターネットに接続できます。VPC では、AWS の柔軟性、スケーラビリティ、伸縮自在性、パフォーマンス、可用性、および「使用した分だけ支払う」価格モデルに関するメリットを保ったまま、AWS リソースを容易に保護することができます。

参考文献

1. **Amazon VPC 製品ページ**: http://aws.amazon.com/vpc/
2. **Amazon VPC ドキュメント:** http://aws.amazon.com/documentation/vpc/
3. **AWS Direct Connect 製品ページ:** http://aws.amazon.com/directconnect/
4. **AWS Direct Connect ドキュメント:** http://aws.amazon.com/documentation/directconnect/
5. **AWS Architecture Center:**http://aws.amazon.com/architecture/
6. **AWS Security and Compliance Center:**http://aws.amazon.com/security/
7. **災害復旧目的での AWS の使用白書**、 http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf
8. **AWS クラウドアーキテクチャのベストプラクティスに関する白書、** http://media.amazonwebservices.com/AWS_Cloud_Best_Practices.pdf

改訂履歴

最新版（2010 年 1 月）からの変更

- Amazon VPC の新機能を反映するための大規模な改訂
- VPC の新しいユースケースを追加
- 「Amazon Virtual Private Cloud について」の項を追加
- 「Amazon VPC 使用のベストプラクティス」を追加