障害復旧を目的とした Amazon Web Services の使用

2011 年 10 月

更新: 2012 年 1 月

Glen Robinson、Ianni Vamvadelis、Attila Narin

amazon web services™

目次

要約

障害が発生した場合も、Amazon Web Services（AWS）で迅速にリソースを起動して、ビジネスの継続性を確保することができます。このホワイトペーパーでは、関連する AWS 機能および DR プロセスで活用できるサービスについて説明し、障害から復旧する方法のシナリオを紹介します。さらに、DR プランを向上させ、障害復旧プロセスで AWS の可能性を最大限に活用する方法に関する推奨事項を提供します。

はじめに

障害復旧（DR）とは、障害に備えること、また、障害から回復することです。ビジネスの継続性または財務状況に悪影響を及ぼす事象が障害と呼ばれ、例えば、ハードウェアまたはソフトウェアの障害、ネットワーク停止、停電、火災／洪水などによる建物への物理的損傷、人為的なミス、またはその他の大きな災害などがあります。

ビジネスに対する障害の影響を最小限に抑えるために、企業はこうした事象に対処するプロセスの計画、準備、実践、文書化、トレーニング、および更新に時間とリソースを費やしています。特定のシステムの障害復旧計画にどの程度投資するかは、発生する可能性のある停止によるコストによって大きく異なってきます。このホワイトペーパーでは、最小限の投資事例から最大規模の可用性および耐障害性まで、標準的なアプローチについて説明します。

DR の準備は必ず適切に行わなければなりません。このホワイトペーパーでは、DR プランと計画を向上させるためのベストプラクティスをいくつか取り上げ、その概要を説明します。

ビジネスとシステムは進化します。したがって、障害復旧プロセスでは、継続的な分析および改善が行われます。顧客は、ビジネスサービスごとに許容できる復旧ポイントと時間を設定し、適切な DR ソリューションを策定する必要があります。

従来の物理環境における標準のアプローチの障害シナリオでは、インフラストラクチャを複製することで、予備容量を確保しました。予想される容量要件に対処できるようにするには、このインフラストラクチャを入手、インストール、および維持する必要があります。通常の運用環境では、このインフラストラクチャがあまり活用されていないか、あるは過剰にプロビジョニングされていることが少なくありません。

AWS を使用すると、インフラストラクチャを必要な場合にのみ拡張できます。Amazon がウェブサイトの独自のグローバルネットワークを実行する際に使用しているものと同じ、拡張性と信頼性に優れた安全で高速、かつコストがかからないインフラストラクチャにアクセスでき、支払いは使った分に対してのみ発生します。障害復旧（DR）ソリューションでは、これが大きなコスト削減につながります。また、DR シナリオでリソースの変更や最適化をより迅速に行うこともできます。

システムのダウンタイムは、ほとんどの場合、人為的なミスが原因で発生します。AWS には、役割を分類して*最小限の権限*[1]の原則を適用するためのツールが用意されています。また、AWS を使用すると、環境全体を自動的に展開し、予測しながら繰り返し設定を行うことができます。非常に迅速にセットアップできる DR テスト環境は、使い捨てのリソースとして処理できます。これにより組織は設定変更を本番環境に取り入れる前に、再現環境でテストできます。あまり利用されることのないテスト専用の大規模な環境を構築する必要はありません。

[1] http://en.wikipedia.org/wiki/Principle_of_least_privilege

復旧時間目標と復旧ポイント目標

このホワイトペーパーでは、障害復旧プランに関して 2 つの一般的な業界用語を使用します。

復旧時間目標（RTO）[2]：ビジネスが中断することで許容できない結果が発生しないようにするために、障害（中断）が発生してから、ビジネスプロセスが規定のサービスレベルに復旧するまでに必要な時間のことをいいます。例えば、障害が午後 12 時（正午）に発生し、RTO が 8 時間の場合、DR プロセスでは、午後 8 時までに許容できるサービスレベルに復旧します。

復旧ポイント目標（RPO）[3]：どの程度のデータ紛失を許容できるかを時間で表します。例えば、RPO が 1 時間の場合、障害が発生したのは正午なので、復旧後のシステムには午前 11 時以降のデータのみが含まれることになります。

通常、許容できる RTO および RPO は、システムが使用できなくなった場合のビジネスに対する経済的な影響に基づいて決まります。経済的な影響を判断するには、ビジネス上の損失、ダウンタイムによる評価の失墜、システムの可用性が低下など、様々な要因を検討します。

そして、IT 組織は、RTO によって確立されたタイムラインとサービスレベル内で、RPO に基づいてコスト効率よくシステムを復旧させるソリューションを計画します。

従来の DR 投資プラクティス

DR に対する従来のアプローチでは、データおよびインフラストラクチャを、現場から離れて様々なレベルで再現します。このインフラストラクチャで重要なビジネスサービスをセットアップして維持し、定期的にテストします。障害復旧環境の場所とソースインフラストラクチャは、物理的にかなり離れた場所になければなりません。これは、ソースサイトに影響を及ぼす可能性がある障害から、その障害復旧環境が確実に切り離されるようにするためです。

再現環境をサポートするのに必要なインフラストラクチャには次のものが含まれます。ただし、これに限定されません。

- 電源および冷却装置を備えたインフラストラクチャを持つ施設。
- 資産を物理的に保護するためのセキュリティ。
- 環境の拡大に対応できる適切な容量。
- インフラストラクチャの修復、交換、変更のサポート。
- 最大読み込み時に再現環境で帯域幅を使用し続けられるインターネット接続の提供に関して合意した、インターネット サービス プロバイダとの契約。
- ファイヤウォール、スイッチ、ロードバランサーなどのネットワークインフラストラクチャ。

---

[2] http://en.wikipedia.org/wiki/Recovery_time_objective から引用

[3] http://en.wikipedia.org/wiki/Recovery_point_objective から引用

- ミッションクリティカルなサービスすべてを実行できるだけのサーバー容量。このミッションクリティカルなサービスには、アプリケーションおよびバックエンドサービス（ユーザー認証、ドメイン ネームシステム（DNS）、DHCP（動的ホスト構成プロトコル）、モニタリング、アラートなど）を実行するためのデータおよびサーバーをサポートするストレージアプライアンスが含まれます。

サービス容量によっては、耐障害性を考えて再現環境を構成できます。これを行うには、通常、上記のインフラストラクチャ全体を再現する必要があります。

障害復旧を目的とした AWS サービスと機能の基本

DR に対する様々なアプローチについて説明するにあたり、まず重要なのは、障害復旧と関連が深い AWS サービスと機能について確認していくことでしょう。このセクションでは、これについてを簡単に説明していきます。

DR の準備フェーズでは、データ移行と耐久性のあるストレージをサポートするサービスと機能の使用について検討することが重要です。このようなサービスと機能によって、バックアップ済みの重要なデータを災害発生時に AWS に復元することが可能になるからです。AWS でシステムの展開を縮小または拡大するシナリオについては、コンピュートリソースも必要です。

障害に対応する場合、重要なのは、AWS でシステムを実行するようにコンピュートリソースにすばやく処理を委任するか、AWS で既に実行されているリソースにフェールオーバーするよう調整することです。ここでは、DNS、ネットワーク機能、様々な Amazon Elastic Compute Cloud（Amazon EC2）の機能など、インフラストラクチャの重要な要素の一部について説明します。

リージョン

Amazon Web Services は、複数のリージョンで使用できるので、障害復旧サイト、およびシステムを完全に展開するサイトとして最適な場所を選択できます。このホワイトペーパーの執筆時点では、米国東部（バージニア北部）、米国西部（北カリフォルニア）、EU（アイルランド）、アジアパシフィック（シンガポール）、およびアジアパシフィック（東京）の５つのリージョンで利用可能です。

ストレージ

Amazon Simple Storage Service（Amazon S3）は、ミッションクリティカルで重要なデータストレージのための設計された、耐久性に優れたストレージインフラストラクチャです。オブジェクトは、リージョン内の複数の施設の複数のデバイスに冗長的に保存されます。AWS は、Amazon S3 のバージョン管理機能、AWS Multi-Factor Authentication、バケットポリシー、および Identity and Access Management（IAM）を介してデータ保存とアーカイブを提供し、さらなる保護を実現します。

Amazon Elastic Block Store（Amazon EBS）では、データボリュームのポイントインタイムスナップショットを作成できます。このスナップショットは、新しい Amazon EBS ボリュームを立ち上げるときにも、データを長期間格納するときにも役立ちます。作成されたボリュームは、実行中の Amazon EC2 インスタンスに接続できます。Amazon EBS ボリュームは、インスタンスの運用状況には左右されない永続性のあるストレージを提供します。

AWS Import/Export により、転送用のポータブル記憶装置を用いて、AWS 内外への大容量データの転送を高速化できます。AWS なら、Amazon の高速内部ネットワークを駆使し、インターネットを使うことなくデータを直接記憶装置に転送できます。データセットのサイズがかなり大きい場合は、AWS Import/Export の方がインターネット転送より高速で、通信環境をアップグレードするよりも経済的です。AWS Import/Export を使用すると、Amazon S3 バケットに、または Amazon S3 バケットからデータを移行できます。また、Amazon EBS スナップショットにデータを移行することも可能です。

AWS Storage Gateway を利用すると、AWS のクラウドストレージとオンプレミスアプリケーションとの間のシームレスなデータ移行が可能になります。AWS Storage Gateway では、ボリュームデータがユーザー企業のインフラストラクチャ内でローカルに保管されるほか、AWS にも保管されます。したがって、既存のオンプレミスアプリケーションのデータを AWS のコスト効果、セキュリティ、および耐久性に優れたストレージインフラストラクチャにシームレスに保管できるだけでなく、このデータへのアクセスにおける待ち時間の短さも維持されます。

コンピュート

Amazon Elastic Compute Cloud（Amazon EC2）は、クラウド内でサイズ変更可能な計算処理能力を提供します。数分で EC2 インスタンスを作成できます。このインスタンスは、完全にコントロールできる仮想マシンです。コントロールできる仮想マシンを迅速に作成するこの機能は、DR では非常に重要です。このドキュメントでは、Amazon EC2 のすべての機能について説明することはできません。ここでは、Amazon EC2 の中でも DR に関連する部分を中心に説明していきます。

Amazon マシンイメージ（AMI）はオペレーティングシステムで事前設定されています。事前設定された AMI の中には、アプリケーションスタックが含まれるものもあります。独自の AMI を設定することもできます。DR では、復旧プロセスの一部として AMI を起動できるように独自の API を設定し、特定することを強くお勧めします。こうした AMI は、選択したオペレーティングシステムと、アプリケーションスタックの適切な要素で事前設定する必要があります。

Amazon EC2 Reserved Instances は、EC インスタンスの実行コストを大幅に削減する際に使用されることが多く、特に DR に関連するもう 1 つの利点があります。Reserved Instances は、必要な容量を必要なときに利用できるようにするのに役立ちます。

利用可能ゾーンは、他のゾーンからの影響を受けないようにそれぞれが独立しており、同一リージョンの他の利用可能ゾーンに対して、待ち時間が短くコストのかからないネットワーク接続を提供します。独立した利用可能ゾーンでインスタンスを起動することにより、1 つの場所で発生した障害からアプリケーションを保護することができます。リージョンは 1 つ以上の利用可能ゾーンで構成されます。

Amazon EC2 VM Import 機能を使用すると、既存の環境から Amazon EC2 インスタンスに仮想マシンのイメージをインポートできます。

ネットワーク

障害に対応するにあたり、他のサイトにフェールオーバーするときに、ネットワーク設定を変更しなければならないことはよくあるでしょう。

Amazon Route 53 は、可用性と拡張性の高いドメイン ネーム システム（DNS）ウェブサービスです。このサービスの目的は、開発者やビジネスに対して、信頼性と費用対効果に優れた方法でエンドユーザーをインターネットアプリケーションにルーティングする方法を提供することです。

Elastic IP アドレスは、ダイナミック クラウド コンピューティング用に設計された固定 IP アドレスサービスです。従来の静的な IP アドレスとは異なり、Elastic IP アドレスでは、パブリックな IP アドレスを、特定のリージョンのアカウントのインスタンスにプログラム的に再マッピングすることにより、インスタンスまたは利用可能ゾーンの障害にマスクをかけることができます。DR では、最も重要なシステムの IP アドレスを事前に割り当てることもできるので、障害が発生する前に IP アドレスを認識できます。これにより、DR プランの実行を簡素化できます。

Elastic Load Balancing は、複数の Amazon EC2 インスタンス間で、アプリケーショントラフィックの負荷を自動的に分散します。これは耐障害性に優れたアプリケーション運用を可能にし、流入するアプリケーショントラフィックに対応した負荷分散能力を、シームレスに提供するものです。Elastic IP アドレスを事前に割り当てることができるように、Elastic Load Balancer も事前割り当てが可能なので DNS 名を認識でき、これにより DR プランの実行を簡素化できます。

Amazon Virtual Private Cloud（Amazon VPC）では、Amazon Web Services クラウドのプライベートで孤立したセクションをプロビジョニングできます。ここでは、定義済みの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。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るので、企業のデータセンターと自分の VPC 間に VPN 接続を作成し、AWS クラウドを企業のデータセンターの拡張機能として活用することができます。DR との関連では、Amazon VPC を使用して、既存のネットワークトポロジをクラウドに拡張できます。これは、通常は内部ネットワークにある企業アプリケーションの復旧に特に適しています。

Amazon Direct Connect により、構内から AWS への専用ネットワーク接続を簡単に確立できます。多くの場合、これによりネットワークコストが削減し、帯域幅スループットが向上します。また、インターネットベースの接続よりも一貫したネットワークエクスペリエンスが実現します。

データベース

データベースのニーズに応じて、次の AWS サービスの使用について検討してください。

Amazon Relational Database Service（Amazon RDS）を使用すると、クラウドで簡単にリレーショナルデータベースを設定、操作、および拡張できます。Amazon RDS は、DR の準備フェーズで使用して、重要なデータを既に実行されているデータベースで保持するか、あるいは、復旧フェーズで使用して、本番データベースを実行します。

Amazon SimpleDB は、可用性と柔軟性に優れ、データベース管理の負担を軽減する、非リレーショナル データストアです。これは、DR の準備フェーズおよび復旧フェーズでも使用できます。

Amazon EC2 でデータベースソフトウェアを選択してインストールおよび実行し、様々な主要データベースシステムから選択することもできます。

AWS のデータベースオプションの詳細については、「Running Databases on AWS」を参照してください。

展開の調整

Amazon EC2 では、展開の自動化および起動後のソフトウェアのインストール／設定プロセスおよびツールを使用できます。この分野に投資することを強くお勧めします。これは、復旧フェーズで必要なリソースを自動的に作成する際に役立ちます。

AWS CloudFormation は、関連する AWS リソースを収集し、整った予測可能な方法でそれらをプロビジョニングする簡単な方法を開発者やシステム管理者に提供します。環境用にテンプレートを作成し、関連するリソースのコレクション（スタックと呼ばれます）を必要に応じて展開することができます。

セキュリティ

AWS サービスにはセキュリティ関連の機能が多数あります。セキュリティについては、「Security Best Practices」ホワイトペーパーをご覧になることをお勧めします。また、AWS の「AWS セキュリティセンター」で、リスクとコンプライアンスに関する詳細情報を確認することもできます。このホワイトペーパーでは、セキュリティについては詳しく説明していません。

AWS での障害復旧シナリオ

このセクションでは、AWS を使用する 4 つの DR シナリオを取り上げ、AWS を従来の DR 方法と比較します。

- バックアップと復元
- AWS への簡単な復旧を目的としたパイロットライト
- ウォーム スタンバイ ソリューション
- 複数サイトソリューション

Amazon Web Services を使用すると、ここで示す DR 戦略の例をコスト効率よく実施することができます。ここで紹介するアプローチは単なる例に過ぎないこと、そして、様々な組み合わせやバリエーションが考えられることを忘れないようにしてください。

バックアップと復元

従来の環境では、ほとんどの場合、テープにデータがバックアップされ、定期的にサイトに送信されます。この方法を使用すると、復旧にかなりの時間がかかります。Amazon S3 は、 1 年にわたり 99.999999999%（イレブンナイン）のオブジェクト耐久性を実現するように設計されてるので、データのバックアップには最適です。Amazon S3 とのデータのやり取りは、通常、ネットワーク経由で行われるため、どこからでもアクセスできます。また、Amazon S3 をサポートする市販およびオープンソースのバックアップソリューションは多数存在します。AWS Import/Export サービスを使用すると、ストレージデバイスを直接 AWS に送ることで、非常に大きなデータセットを転送できます。

AWS Storage Gateway サービスを利用すると、オンプレミスのデータボリュームのスナップショットをバックアップ目的で透過的に Amazon S3 にコピーすることができます。このスナップショットから、ローカルボリュームや AWS EBS ボリュームを作成できます。

AWS で実行されているシステムについては、お客様が Amazon S3 にバックアップすることもできます。Amazon S3 には、Elastic Block Store（EBS）ボリュームのスナップショットと Amazon RDS のバックアップが保存されています。また、ファイルを直接 Amazon S3 にコピーすることも、バックアップファイルを作成して Amazon S3 にコピーすることもできます。Amazon S3 にバックアップデータを保存するバックアップソリューションは多数あり、こうしたソリューションは、Amazon EC2 システムからも使用できます。

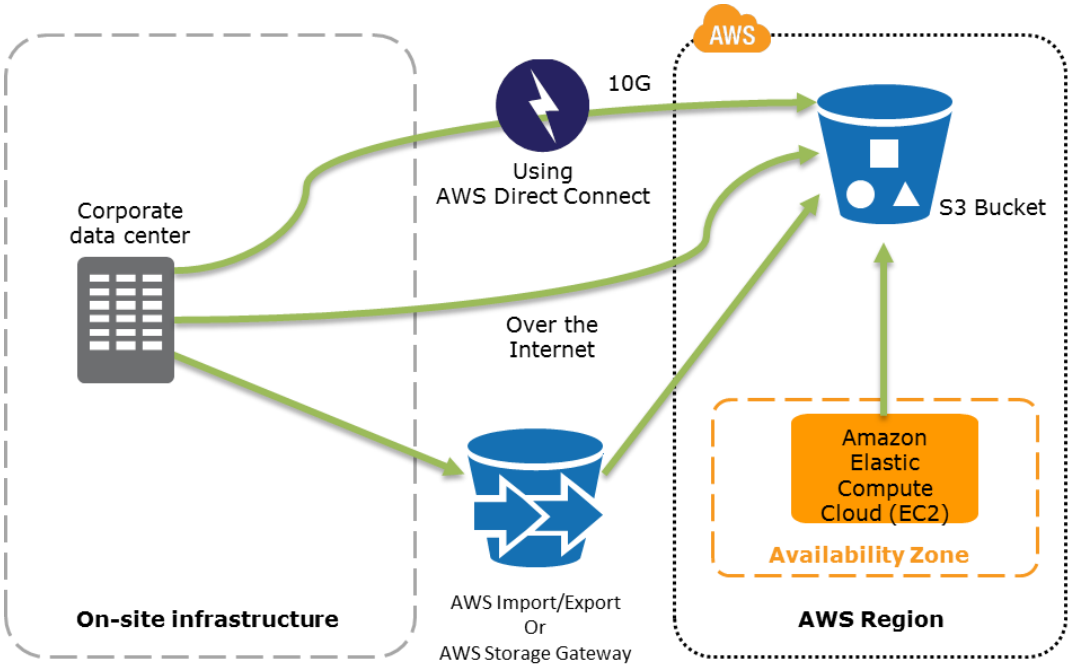

図 1 : 施設内インフラストラクチャまたは AWS から S3 へのデータ バックアップ オプション。

データをバックアップしても、それは、まだ道半ばに過ぎません。障害復旧シナリオでは、データの復旧をすばやく確実にテストし、復旧したデータをアーカイブする必要があります。また、データが適切に保持され、データのセキュリティが適切に確保されるようシステムを設定するほか、システムでデータ復旧プロセスをテストする必要もあります。

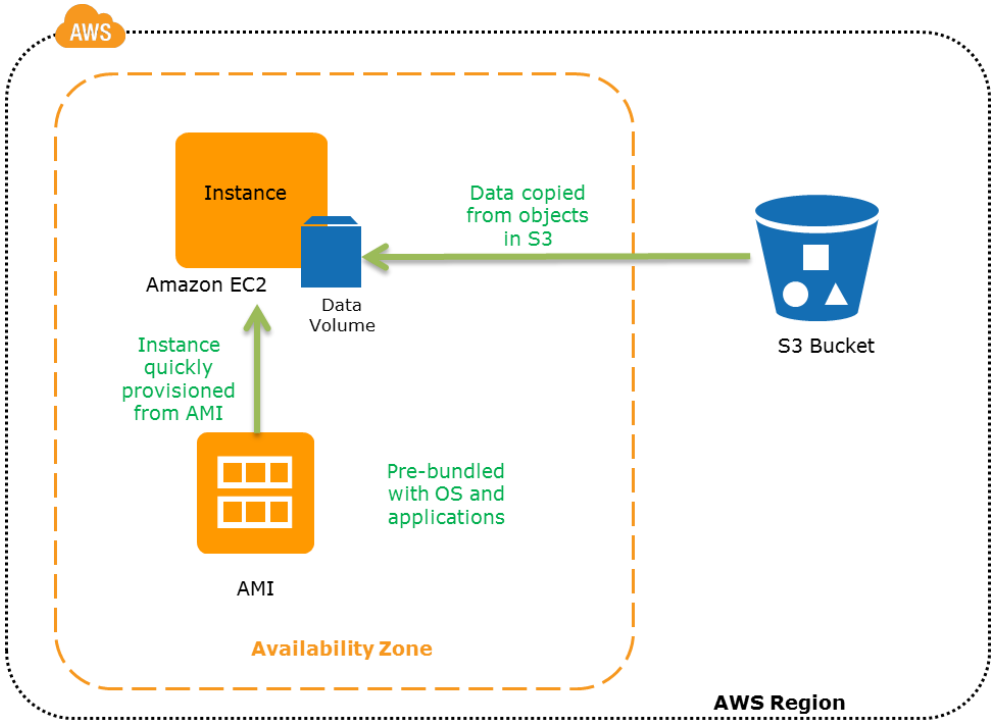

図 2 : S3 バックアップから AWS EC2 へのシステムの復旧

バックアップおよび復元の主な手順は次のとおりです。

- 適切なツールまたはメソッドを選択し、データを AWS にバックアップします。
- このデータに適切な保存ポリシーがあることを確認します。
- このデータに、暗号化、アクセスポリシーなど、適切なセキュリティ対策が適用されていることを確認します。
- このデータの復旧とシステムの復元を定期的にテストします。

AWS への迅速な復旧を目的としたパイロットライト

パイロットライトは、ガスストーブに例えた言葉です。ガスストーブでは、常に点いてる小さな炎が火炉全体をすばやく点火し、必要に応じて家を暖めます。このシナリオはバックアップおよび復元シナリオに似ていますが、システム内で中核を成す非常に重要な要素を設定し、AWS で実行しておく必要があります（パイロットライト）。そして復旧時に、その重要な要素に基づいて、大規模な本番環境を迅速にプロビジョニングします。

パイロットライト自体のインフラストラクチャ要素には、通常、データベースサーバーが含まれます。このデータベースサーバーはデータを Amazon EC2 にレプリケートします。システムによっては、AWS にレプリケートする必要がある重要なデータが他にも、データベース外に存在することがあります。これがシステムの重要な部分（パイロットライト）で、これに基づいて、AWS 内のすべてのインフラストラクチャ要素（火炉の他の部分）をすばやくプロビジョニングし、システム全体を復元できます。

インフラストラクチャの残りの部分をプロビジョニングしてビジネスクリティカルなサービスを復元するために、通常、事前設定されたサーバーバンドル Amazon マシンイメージ（AMI）が用意されています。このバンドルはすぐに起動することができます。復旧を開始すると、この AMI のインスタンスがすぐに起動し、パイロットライトに基づいて展開内でその役割を見つけます。ネットワークの観点から言うと、Elastic IP アドレス（DR の準備フェーズで事前割り当てが可能）を使用して、そのアドレスをインスタンスに関連付けるか、Elastic Load Balancing を使用して、トラフィックを複数のインスタンスに分散します。その後、CNAME を使用して、Amazon EC2 インスタンスまたは Elastic Load Balancing を指定するように DNS レコードを更新します。

それほど重要でないシステムについては、すべてのインストールパッケージや設定情報を、例えば EBS スナップショットの形式で、AWS で確実に利用できます。複数のボリュームを複数の利用可能ゾーンに作成できるので、アプリケーションサーバーのセットアップの速度が上がり、EC2 インスタンスに接続されます。その後、それに応じて、インストールおよび設定できます。

パイロットライト手法では、システムで中核を成す要素が既に実行されており、常に最新の状態が保たれているため、上記の「バックアップおよび復元」シナリオよりも復旧時間が短くなります。アプリケーションを完全に復旧するためのインストールおよび設定作業はまだ他にもあります。AWS を使用すると、インフラストラクチャリソースのプロビジョニングおよび設定を自動化できます。これは、時間を短縮したり人為的なミスを防いだりするには非常に有用です。

準備フェーズ：

次の図は準備フェーズを示しています。このフェーズでは、定期的に変更されるデータをパイロットライトにレプリケートする必要があります。この小さな中核となる要素に基づいて、復旧フェーズで環境全体が開始されます。オペレーティングシステムやアプリケーションなどの更新頻度が少ないデータについては、Amazon マシンイメージ（AMI）として定期的に更新および保存できます。

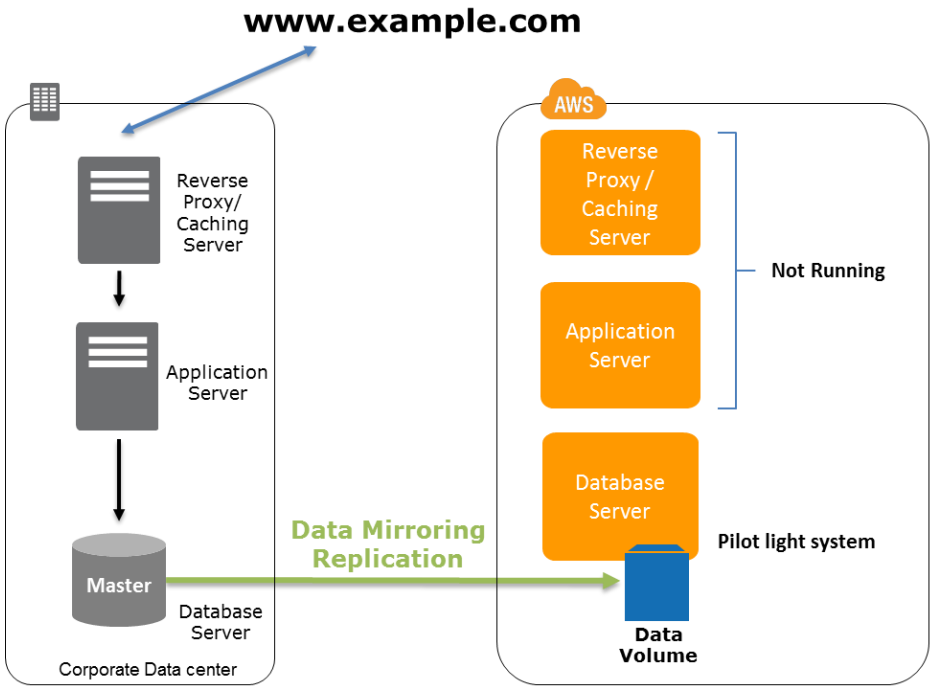

図 3：パイロット ライト シナリオの準備フェーズ

準備に関する重要ポイント：

- EC インスタンスをセットアップして、データをレプリケートまたはミラー化します。
- サポート カスタム ソフトウェア パッケージすべてが AWS で使用できることを確認します。
- 高速復旧が必要な主要サーバーの Amazon マシンイメージ（AMI）を作成および維持します。
- このサーバーを定期的に実行およびテストし、ソフトウェア更新および設定変更を適用します。
- AWS リソースのプロビジョニングの自動化を検討します。

復旧フェーズ：

パイロットライトに基づいて残りの環境を復旧するために、適切なインスタンスタイプで Amazon マシンイメージ（AMI）からシステムを開始します。動的なデータサーバーについては、サイズを変更して、必要に応じて本番ボリュームを処理するか、容量を追加できます。水平拡張（可能な場合）は、システムの容量を追加するためのアプローチとしては最もコスト効率がよく、拡張性に優れていますが、より大きな EC2 インスタンスタイプを選択することによって垂直拡張を行うこともできます。ネットワークの観点から言うと、DNS 更新を必要とするすべての処理を並行して実行できます。

一度復旧されたら、なるべく早く冗長性を確保する必要があります。本番環境で障害が発生した後すぐに、DR 環境で障害が発生することは考えにくいと思われますが、念のためこのリスクについても考慮しておく必要があります。システムのバックアップを定期的に取り続け、データレイヤーで追加の冗長性を確保することを検討してください。

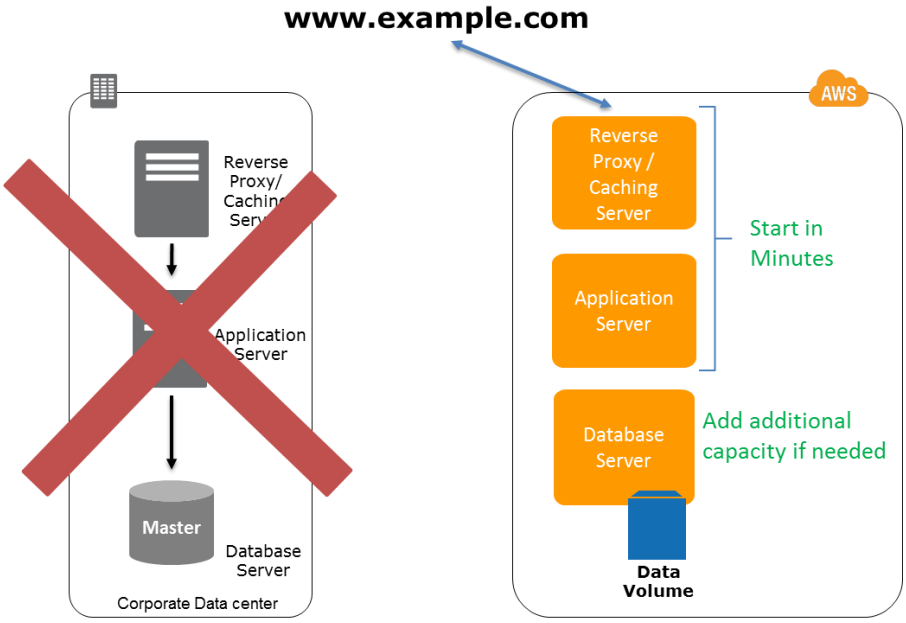

図 4：パイロット ライト シナリオの復旧フェーズ。

復旧に関する重要ポイント：

- カスタム AMI からアプリケーション EC2 インスタンスを開始します。
- データベース／データストアインスタンスのサイズ変更や拡張を、必要に応じて行います。
- EC2 サーバーを指定するように DNS を変更します。
- AMI ベース以外のシステムを（理想的には自動的に）インストールおよび設定します。

AWS でのウォーム スタンバイ ソリューション

ウォーム スタンバイソリューションにより、パイロットライトの要素と準備が拡張されます。この場合は一部のサービスが常に実行されているので、復旧時間が短縮されます。ビジネスクリティカルなシステムを特定して AWS に完全に復元し、常時稼働させておきます。

これらのサーバーは、最小サイズの EC2 インスタンスのフリートで、できるだけ小さなサイズで実行できます。このソリューションが、本番環境のすべての負荷を担うために拡張されることはありませんが、完全な機能は備えています。テスト、品質保証、内部使用など、本番以外の作業に使用される場合もあります。

障害が発生した場合、システムは迅速に拡張され、本番環境の負荷を処理します。AWS でこれを行うには、ロードバランサーにインスタンスを追加したり、より大きな EC2 インスタンスタイプで実行されるように小容量サーバーのサイズを変更したりします。既に説明したように、多くの場合、垂直拡張よりも水平拡張（使用できる場合）の方が優先されます。

準備フェーズ：

次の図は、ウォーム スタンバイ ソリューションの準備フェーズを示しています。このフェーズでは、施設内のソリューションと AWS ソリューションが並んで実行されています。

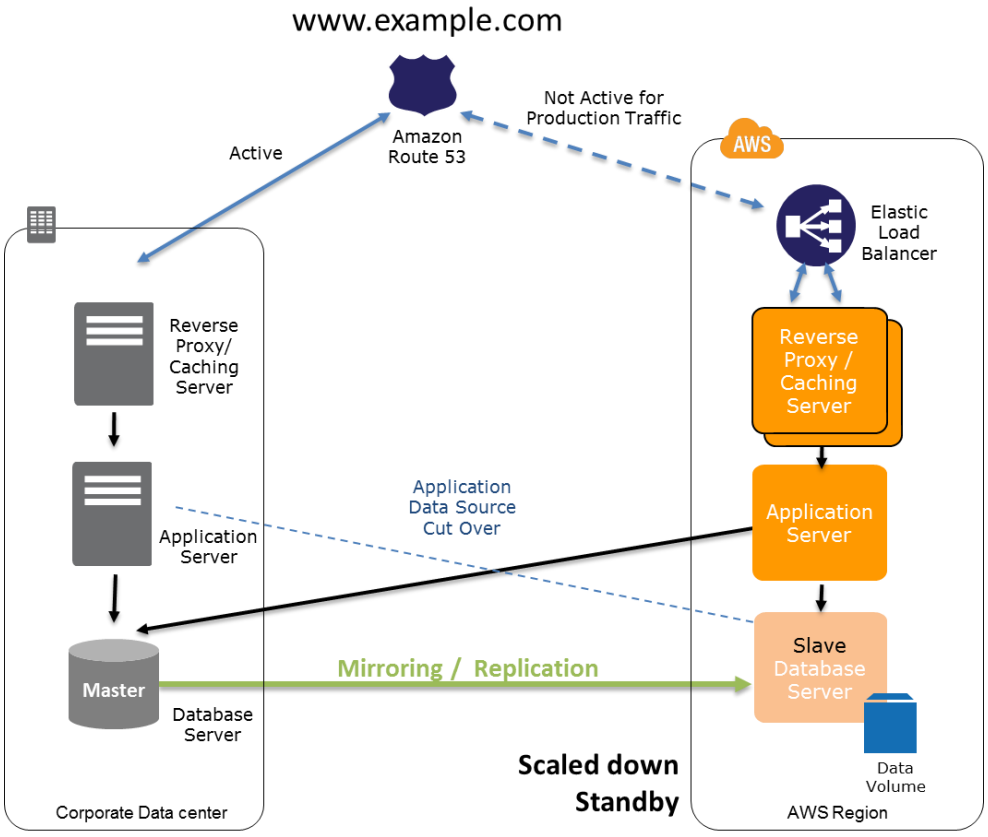

図５：「ウォームスタンバイ」シナリオの準備フェーズ。

準備に関する重要ポイント：

- EC インスタンスをセットアップして、データをレプリケートまたはミラー化します。
- Amazon マシンイメージ（AMI）を作成して維持します。
- EC2 インスタンスまたは AWS
  インフラストラクチャの占有領域を最小限に抑えてアプリケーションを実行します。
- 本番環境に従ってソフトウェアおよび設定ファイルにパッチまたは更新を適用します。

復旧フェーズ：

本番システムで障害が発生すると、本番環境の負荷に対応するためにスタンバイ環境が拡大し、すべてのトラフィックが AWS にルーティングされるように DNS レコードが変更されます。

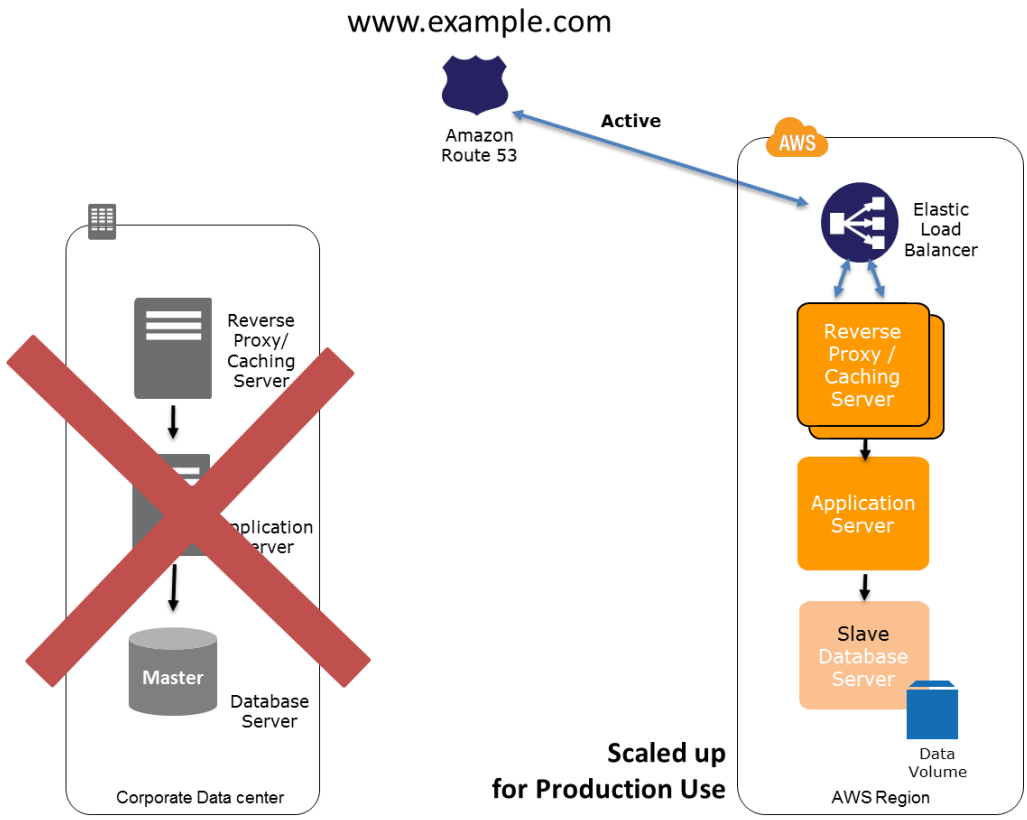

図 6：「ウォームスタンバイ」シナリオの復旧フェーズ。

復旧に関する重要ポイント：

- 必要に応じて、より大きな EC2 インスタンスタイプでアプリケーションを開始します（垂直拡張）。
- Load Balancer で、サービスの EC2 フリートのサイズを増やします（水平拡張）。
- すべてのトラフィックが AWS 環境にルーティングされるように DNS レコードを変更します。
- 自動拡張を使用してフリートを適切なサイズに調整し、より高い負荷に対応できるようにすることを検討します。

AWS および施設内に展開された複数サイトソリューション

複数サイトソリューションは、AWS およびアクティブ - アクティブ構成の施設内インフラストラクチャで実行されます。使用するデータレプリケーション方法は、選択する復旧ポイント（上記の RPO を参照）によって決まります。様々なレプリケーション方法があります（以下を参照）。

本番トラフィックを様々なサイトにルーティングするときに使用されるのは、Amazon Route 53 などの重み付けされた DNS サービスです。ある割合のトラフィックが AWS のインフラストラクチャに送られ、残りは施設内インフラストラクチャに送られます。

施設内で障害が発生した場合は、DNS 重み付けを調整し、すべてのトラフィックを AWS サーバーに送信できます。AWS サービスの容量は、本番環境のすべての負荷を処理できるように迅速に増やすことができます。このプロセスを自動化するには、EC2 Auto Scaling を使用します。主要データベースサービスの障害を検出し、AWS で並行して実行されているデータベースサービスにカットオーバーするには、AWS アプリケーションロジックが必要になる場合があります。

このシナリオのコストは、通常の稼働状況で AWS が処理できる本番トラフィックの量によって決まります。復旧フェーズでは、追加で使用した量と、DR 環境全体が必要だった期間に対してのみ支払いが発生します。「常時稼働」 AWS サーバーに対して Reserved Instances を購入すると、コストを削減できます。

準備フェーズ：

以下の図では、DNS を使用して、トラフィックの一部を AWS サイトにルーティングしています。AWS のアプリケーションは、施設内の本番システムのデータソースにアクセスできます。データは、AWS インフラストラクチャにレプリケートまたはミラー化されています。

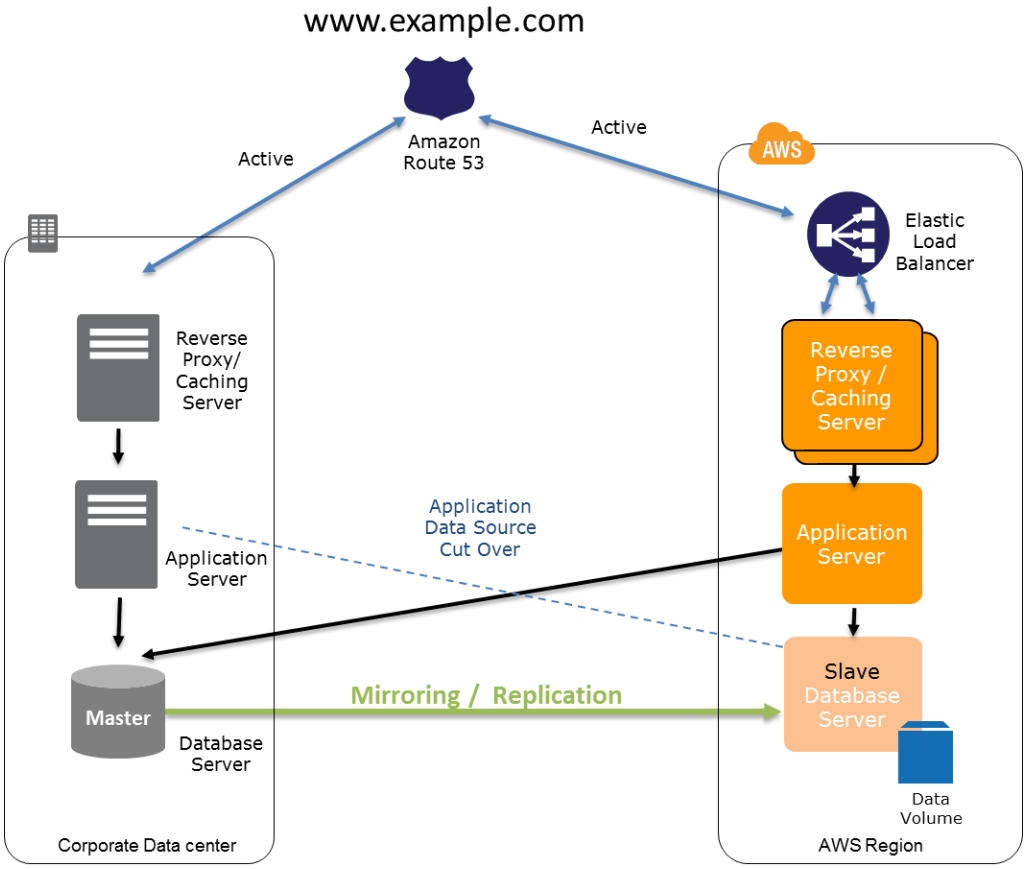

図 7：「複数サイト」シナリオの準備フェーズ。

準備に関する重要ポイント：

- AWS 環境をセットアップし、本番環境を再現します。
- DNS 重み付けまたは同様のテクノロジーをセットアップし、受信リクエストを両方のサイトに配信します。

復旧フェーズ：

以下の表は、施設内で障害が発生した場合の状況を示しています。DNS を更新することで、トラフィックが AWS インフラストラクチャにカットオーバーされています。

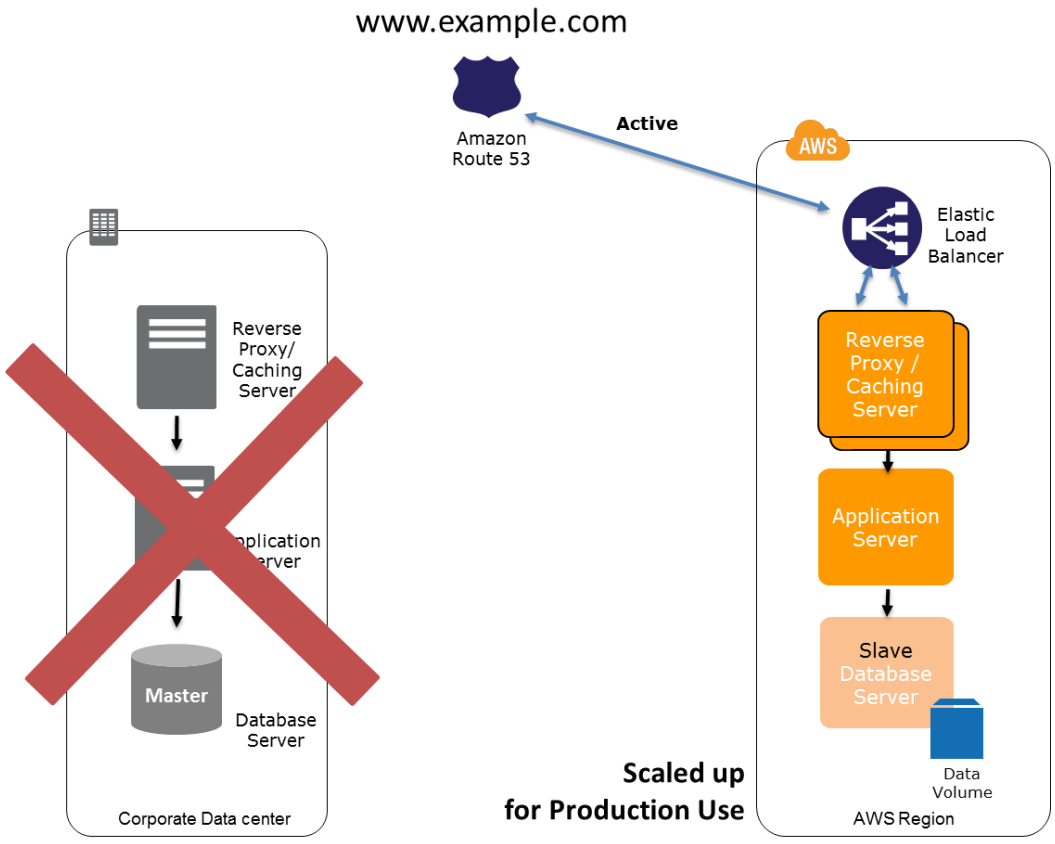

図 8：施設内および AWS インフラストラクチャにおける「複数サイト」シナリオの復旧フェーズ。

復旧に関する重要ポイント：

- DNS 重み付けを変更します。これにより、すべてのリクエストが AWS サイトに送信されます。
- フェールオーバーのアプリケーションロジックによってローカル AWS データベースサーバーが使用されるように指定します。
- 自動拡張を使用して AWS フリートを適切なサイズに調整することを検討します。

複数サイトソリューションの可用性を高めるには、Multi-AZ アーキテクチャを設計します。複数の利用可能ゾーンにわたるアプリケーションを設計する方法の詳細については、「Designing Fault-Tolerant Applications in the AWS Cloud」ホワイトペーパーをご覧ください。

データのレプリケーション

リモートの場所にデータをレプリケートするとき、考慮すべき事項がいくつかあります。

- サイト間の距離：距離が長くなると、通常、遅延時間が長くなりイライラします。
- 使用できる帯域幅：相互接続の幅と変動はどうでしょうか？
- アプリケーションに必要なデータ転送速度：データ転送速度は、使用できる帯域幅を下回っている必要があります。
- 並行レプリケーションテクノロジーを使用する必要があります（これにより、ネットワークを効率的に使用できます）。

データのレプリケーションは、主に同期と非同期の 2 つの方法で行うことができます。

同期レプリケーション

データが複数の場所で細かく更新されます。このためネットワークのパフォーマンスと可用性に依存します。

非同期レプリケーション

データが複数の場所で細かく更新されません。データは、ネットワークのパフォーマンスと可用性によって許可されている場合に転送されます。アプリケーションは、レプリケーションが完了していないデータも書き込み続けます。

データベースの多くが非同期データレプリケーションをサポートしています。データベース複製はリモートに配置できます。この複製は、主要データベースサーバーと完全に同期している必要はありません。これは、バックアップソース、レポート作成／読み取り専用使用事例など、多くのシナリオで使用できます。

ソフトウェアソリューションで採用されているレプリケーションテクノロジーについてよく理解しておくことをお勧めします。このホワイトペーパーでは、レプリケーションテクノロジーについては詳しく分析していません。

AWS では、リージョン内の利用可能ゾーンは適切に連携していますが、物理的には離れた場所にあります。例えば、「Multi-AZ」モードで展開した場合、Amazon Relational Database Service は同期レプリケーションを使用して、2 番目の利用可能ゾーンのデータを再現します。したがって、主要利用可能ゾーンが使用できなくなっても、データは失われません。

AWS リージョンはお互いに完全に独立していますが、リージョンへのアクセス方法や使用方法に違いはありません。これにより、大陸をまたがる距離ほど離れている場合でも、通常かかりそうなコストや問題を発生させずに障害復旧プロセスを作成することができます。データおよびシステムを 2 つ以上の AWS リージョンにバックアップできるので、特に大規模な障害が発生してもサービス復元が可能です。AWS リージョンを使用すると、複雑度が比較的低い運用プロセスによって、世界中に広がる自身のお客様に対応できます。

DR プランの改善

しっかりした DR プランを策定するには、従わなければならない重要な手順がいくつかあります。このセクションでは、その手順のいくつかについて説明します。

テスト

DR ソリューションの準備ができたら、テストが必要です。「ゲームデー」は、DR 環境へのフェールオーバーに向けてのトレーニングを実施するときです。実際に何か起こるに備えて、十分なドキュメントを用意し、プロセスはできるだけシンプルにします。ゲームデーのシナリオをテストするために、AWS ではコスト効率よく、かつ迅速に再現環境を始動できます。また、通常は、本番環境に手を加える必要はありません。AWS CloudFormation を使用すると、環境全体を AWS に展開できます。これはテンプレートを使用して、環境全体を構築する際に必要な AWS リソースと、関連する依存関係またはランタイムパラメータを記述します。

多種多様な障害に対応できるように、様々なテストを行うことが重要です。「ゲームデー」シナリオの例を以下に示します。

- サイトまたは一連のコンピュータに対する電力の損失
- １つのサイトへの ISP 接続の切断
- 主要ビジネスサービスのウィルス感染が複数サイトに影響
- データ損失によって発生したユーザーエラーによりポイントインタイムリカバリが必要

モニタリングとアラート

サーバー障害および接続やアプリケーションの問題が DR 環境に影響を及ぼす場合に警告されるように、定期的にチェックを実行し、十分なモニタリングを行う必要があります。Amazon CloudWatch を使用すると、AWS リソースの評価指標にアクセスできます。任意の評価指標のに定義された閾値に基づいてアラームを設定し、予期せぬ動作が発生した場合は、必要に応じて Amazon Simple Notification Service メッセージで警告することができます。AWS では任意のモニタリングソリューションを使用できます。

会社が使用している既存のモニタリングおよびアラートツールを引き続き使用して、インスタンスの評価指標、OS の統計値、アプリケーションの状態をモニタリングすることもできます。

バックアップ

DR 環境に切り替えたら、引き続き通常のバックアップを行う必要があります。バックアップと復元を定期的にテストすることは、フォールバックソリューションとして非常に重要です。

AWS は、DR インフラストラクチャを「常時稼働」しなくても、DR テストを頻繁に、かつ低コストで行うための柔軟性を備えています。

ユーザーアクセス

DR 環境のリソースに安全にアクセスするには、AWS Access Management（IAM）を使用します。このようにして、DR 環境で作業しながら、ユーザーの責務を分類する役割／ユーザーベースのセキュリティポリシーを作成できます。

自動化

AWS ベースのサーバーおよび組織内サーバーへのアプリケーションの展開を自動化するには、設定管理または調整ソフトウェアを使用します。これにより、両方の環境で、アプリケーションおよび設定変更の管理を簡単に処理できます。使用できる一般的な調整ソフトウェアオプションは複数あります。使用できるソリューションプロバイダについては、ソリューションプロバイダのページ[4]をご覧ください。AWS CloudFormation は複数のツールと連携し、インフラストラクチャサービスを自動的にプロビジョニングします。ユーザーデータは、初回起動時にインスタンスに渡されます。その後、インスタンスタイプまたは役割を判断するために設定管理ツールに渡され、適切なソフトウェアと設定が確実に展開されます。全体的な目的は、インスタンスをできるだけ自動的に実行できる最終的な状態に持っていくことです。

自動拡張を使用すると、インスタンスのプールが、CloudWatch で指定された評価指標に基づいた需要を満たすよう確実かつ適切にサイズ調整されます。つまり、DR 状況では、ユーザーベースがさらに環境を使用し始めると、この需要の増加を満たすためにソリューションを動的に拡張できます。ある事象が終わり、使用量が減少する可能性がある場合は、最小レベルのサーバーにまでソリューションを縮小できます。

ソフトウェアライセンスと DR

AWS 環境のライセンスが適切に付与されていることは、他の環境へのライセンス供与と同じくらい重要です。Amazon では、ライセンスを管理しやすいように様々なモデルをご用意しています。例えば、複数のソフトウェアコンポーネントまたはオペレーティングシステムに対して [Bring Your Own License] を使用できます。ライセンスのコストが 1 時間の料金に含まれているソフトウェアも複数あります。これは、[License included] と呼ばれます。

[Bring your Own License] を使用すると、障害発生時に既存のソフトウェアへの投資を利用できます。[License included] を有効にすると、毎日は使用されない、つまり DR テストの際に DR サイトで最初に支払うコストを最小限に抑えることができます。

ライセンス自体、および AWS へのライセンスの適用方法に関してご不明な点がある場合はいつでも、ライセンスリセラーにお問い合わせください。

まとめ

DR には多くのオプションやバリエーションがあります。このホワイトペーパーでは、簡単なバックアップおよび復元から、耐障害性を備えた複数サイトソリューションまで、一般的なパターンをいくつか取り上げて説明しています。AWS を使用すると、DR の目標（RTO および RPO）と予算を指定したうえで、きめ細やかな管理を実現し、多数の構成要素で適切な DR ソリューションを構築できます。AWS サービスはオンデマンドで使用でき、支払いは使った分に対してのみ発生します。重要なインフラストラクチャをすぐに必要とするが、必要なのは障害発生時にのみ限られる DR にとって、これは重要なメリットです。

このホワイトペーパーでは、皆様がより効果的な DR プランを作成できるように、AWS がどのように柔軟でコスト効率のよいインフラストラクチャソリューションを提供しているかについて説明しました。

---

[4]ソリューションプロバイダについては、http://aws.amazon.com/solutions/solution-providers/ をご覧ください。

詳細情報

- S3 Getting Started Guide：http://docs.amazonwebservices.com/AmazonS3/latest/gsg/
- EC2 Getting Started Guide：http://docs.amazonwebservices.com/AWSEC2/latest/GettingStartedGuide/
- Find an AWS Solution Provider：http://aws.amazon.com/solutions/solution-providers/
- Designing Fault-Tolerant Applications in the AWS Cloud
  ホワイトペーパー：http://aws.amazon.com/whitepapers/
- AWS Security and Compliance Center：http://aws.amazon.com/security/
- AWS Architecture Center：http://aws.amazon.com/architecture
- AWS Technical ホワイトペーパー：http://aws.amazon.com/whitepapers