

エンタープライズ AWS 導入ガイド

第 1.1 版 (2014/12/22)

エンタープライズ AWS 導入ガイド製作者一同

利用許諾条件

第1条（定義）

1. 「本件ドキュメント」とは、アクセンチュア株式会社、アビームコンサルティング株式会社、伊藤忠テクノソリューションズ株式会社、株式会社サーバーワークス、日本ユニシス株式会社、株式会社日立製作所（総称して以下「当六社」という。）を提供元とする「エンタープライズ AWS 導入ガイド」を意味します。
2. 「利用」とは、以下を意味します。
 - (1) 本件ドキュメントの全部又は一部を忠実に複製すること（本件ドキュメントのダウンロードを含む。）。
 - (2) 本利用許諾条件、当六社の著作権表示、その利用につき本利用許諾条件が適用される旨を記載したうえで、本件ドキュメント（複製物を含む）を頒布すること。
 - (3) 著作権法上の定めに従い引用すること。
3. 「ユーザ」とは、本件ドキュメントを利用する個人（個人がその所属する法人等の団体の業務のために本件ドキュメントを利用する場合には、当該法人等の団体）を意味します。

第2条（本件ドキュメントの利用）

1. 当六社は、ユーザが本利用許諾条件を遵守することを条件として、ユーザに対し、本件ドキュメントをユーザの責任において利用するための非独占的権利を許諾します。なお、本件ドキュメントの利用につき、当六社は一切責任を負いません。
2. ユーザは、本ドキュメントを改変することはできません。ユーザが改変して本件ドキュメントを頒布した場合、その一切の責任はユーザが負うものとします。
3. ユーザは、本件ドキュメント（複製物を含む）を第三者へ頒布する場合、当該第三者に対し本利用許諾条件の内容を遵守させるものとし、又、当該第三者に対するすべての責任を負うものとします。

第3条（本件ドキュメント及び本利用許諾条件の内容変更）

本件ドキュメント及び本利用許諾条件の内容は、ユーザにあらかじめ通知することなく変更されることがあります。この場合、ユーザが本利用許諾条件の変更後に本件ドキュメントを利用する際には変更が適用されるものとし、ユーザは変更に同意したものとみなされます。

第4条（本件ドキュメントの提供停止等）

本件ドキュメントの提供は予告なく停止又は中断することがあり、ユーザはそれに同意するものとします。

第5条（保証及び責任）

当六社は、本件ドキュメントを現状有姿にてユーザに提供し利用許諾するものであり、本件ドキュメントに瑕疵が存しないこと、本件ドキュメントが第三者の権利を侵害していないこと、本件ドキュメントが商用性を有していること、本件ドキュメントの機能がユーザの要求を満たすことを含め、明示的であると黙示的であることを問わず一切保証しません。また、本件ドキュメントの評価、業務への適用、その他の処置については、ユーザがすべての責任を負うものとします。

第6条（知的財産権）

ユーザは、本件ドキュメントが当六社又は当六社のライセンサーの財産であり、かつその一切の知的財産権は当六社又は当六社のライセンサーに帰属していることを了解します。

第7条（損害賠償）

当六社は、本件ドキュメントの利用によりユーザ又は第三者が被った直接的、又は間接的ないかなる損害についても責任を負わないものとします。

第8条（利用の終了）

1. ユーザが本利用許諾条件のいずれかの条項に違反した場合、第2条に基づく利用の許諾は直ちに終了します。
2. ユーザは、前項によって第2条に基づく利用の許諾が終了した場合、本件ドキュメントを利用することは認められず、速やかに本件ドキュメント及びその複製物のすべてを廃棄又は消去するものとします。

第9条（輸出管理）

ユーザは、本件ドキュメント及びそれに含まれる技術を海外に持ち出し、又は非居住者に提供する場合は、経済産業大臣の輸出許可を取得する等、関連法規に基づき適正な手続きをとるものとします。

第10条（合意管轄）

本利用許諾条件に関し、訴訟の必要が生じた場合には、東京地方裁判所を第一審の専属的合意管轄裁判所とします。

以上

本利用許諾条件に同意できない場合、本件ドキュメントを利用することはできません。本件ドキュメントを利用した場合、本利用許諾条件に同意したものとみなされます。

本書1～2ページの利用許諾契約書にご同意を頂けない場合、部分利用か又は全部利用かを問わず、本書を利用することはできません。

目次

第1部	AWSによるエンタープライズシステムの幕開け.....	5
第1章	はじめに.....	5
第1節	目的.....	5
第2節	背景・トレンド.....	6
第3節	AWS 概要.....	7
第4節	AWS クラウドの付加価値.....	8
第5節	典型的なエンタープライズシステムの定義.....	10
第2章	AWS サービスの概要.....	11
第2部	AWSによるエンタープライズシステム実現の勘所.....	16
第3章	エンタープライズシステム構成例.....	16
第1節	重要度別のシステム構成例.....	16
第1項	システムに求められる重要度分類.....	16
第2項	ノンプライムシステムのシステム構成例.....	17
第3項	プライムシステムのシステム構成例.....	19
第4項	ミッションクリティカルシステムのシステム構成例.....	21
第2節	システムの広がりを考慮したシステム構成例.....	23
第1項	ハイブリッドシステムのシステム構成例.....	23
第2項	海外拠点グローバルシステム連携のシステム構成例.....	26
第3節	ユースケースごとのシステム構成例.....	28
第1項	SAP を用いた基幹系システムのシステム構成例.....	28
第2項	情報系システムのシステム構成例.....	30
第4章	システム・運用要件.....	33
第1節	基本サービス要件.....	34
第2節	可用性／信頼性要件.....	36
第3節	性能/拡張性要件.....	38
第4節	セキュリティ要件.....	41
第5節	運用要件.....	45
第6節	コンプライアンス要件.....	47
第7節	ベンダー要件.....	50
第5章	移行.....	51
第1節	データ移行.....	52
第2節	サーバー移行.....	53
第3節	ネットワーク移行.....	54

本書1～2ページの利用許諾契約書にご同意を頂けない場合、部分利用か又は全部利用かを問わず、本書を利用することはできません。

第6章	調達	57
第1節	予算管理	57
第2節	コストモデル	57
第3節	サイジング	58
第1項	オンプレミスでのサイジングの考え方	58
第2項	定期的なサイジング	59
第4節	見積もり	60
第1項	企業のITコストにおけるAWS利用料の位置づけ	60
第2項	簡易見積ツールと見積もりのポイント	60
第5節	契約	62
第1項	契約上のポイント	62
第2項	契約モデル	63
第3項	SLA	64

※本書に記載されている製品名などの固有名詞は、各社の商標または登録商標です。（詳細は巻末に記載）

※本書では、記載されているシステム名、製品名等には、必ずしも商標表示（(C)、(R)、TM）を付記していません。

※本書では、説明等の便宜のために製品名、会社名等を掲載する場合がありますが、それらの商標権の侵害を行う意志や目的はありません。

※本書に記載された内容に関して執筆者一同はいかなる保証を行うものではなく、またこの文書を明示的または暗黙的に利用した結果について責任を負うものではありません。

本書は、Amazon Web Services (AWS) をエンタープライズでいかに活用するかに焦点を当て、日本の AWS パートナーネットワークのメンバーである 6 社で共同執筆した書籍である。

本書は、二部構成になっており、第一部は AWS の概要やメリットを知りたい方を対象としており、第二部は AWS のシステム・運用、移行、契約といったより詳細な情報を知りたい情報システム部の方を対象としている。

Amazon Web Services, Inc. のサービスは日々新しいソリューションをリリースしているが、本書は 2014 年 11 月現在の情報をベースに執筆している。

本書が AWS の利用を検討しているエンタープライズのお客様の一助となれば幸いである。

2014年12月

エンタープライズ AWS 導入ガイド製作者一同

第1部 AWSによるエンタープライズシステムの幕開け

第1章 はじめに

第1節 目的

「The Network is The Computer」を掲げて Sun Microsystems が創業したのが 1982 年。その 11 年後、当時の Sun の CEO であった Eric Schmidt 氏は「ネットワークがプロセッサ並みに高速になれば、コンピューターはネットワークに拡散し、ネットワークがコンピューターになる」と語った。その翌年の 1994 年、Jeff Bezos 氏により Amazon.com の前身となる Cadabura.com が創業。インターネット上の書店から始まった Amazon.com はいまや世界最大規模のネット小売業に成長を遂げ、その成長の過程で Amazon Web Services, Inc. が誕生した。2006 年のことである。



AWS とは、仮想サーバー、データベース、ストレージ、ロードバランサーなどの多種に亘るインフラストラクチャーサービスを、初期費用のない安価な従量課金モデルで提供しているクラウドサービスのことである。最初のサービスが提供開始された 2006 年以降、クラウドコンピューティングの急速な発展・浸透とともに、クラウドコンピューティングにおけるリーダーとして圧倒的な存在感を示すこととなった。米国東海岸からスタートした後、西海岸、欧州、シンガポールとリージョン（リージョンとは、複数のデータセンター群の集合体を指す）を拡大し、2011 年 3 月 2 日、待望の東京リージョンが日本に設立された。東京リージョンの設立に合わせ、日本向けのサポートサービスも拡充され、従来問題となっていた地理的制約の解消とともに、より一層日本での AWS の利用促進に拍車がかかったといえる。教育機関、官公庁などのパブリックセクターのみならず、業種業態、企業規模を問わず、非常に幅広い企業群において AWS が活用され始めているその様は、まさにキャズムを超え、メインストリーム市場へ移行していることを示唆している。今後もオンプレミスやプライベートクラウドに存在する企業の情報技術基盤がパブリッククラウド、特に AWS に急加速で移行していくことが想像される。

本書は、これまで数多くの AWS 導入支援を行ってきた APN (AWS パートナーネットワーク) コンサルティングパートナー企業 (AWS 上での顧客の新規アプリケーションの設計、移行、または構築を支援するプロフェッショナルサービス企業) の有志が一堂に会し、企業が自身の情報技術基盤を AWS クラウド上に構築する際、頻出するであろう問題点・心配点・注意点・課題などをまとめ、より効果的かつ円滑な AWS 導入の一助となるガイドラインを提示することを目的としている。本書が、AWS のメリット、セキュリティ、移行方法などに関する正しい理解につながり、AWS クラウドを活用する企業にとって成長への一助となれば望外の喜びである。

第2節 背景・トレンド

昨今、より競争力のあるビジネスの基盤として「AWS をエンタープライズ分野でも利用したい」という声が非常に大きな高まりを見せている。

エンタープライズ AWS 導入ガイド制作委員会の一社である(株)サーバーワークスでは、2008年より AWS における SI サービスの提供を開始したが、2011年まではかなり販売に苦勞していた。ところが、以下に掲げる 3つの大きな進展によって、国内の企業でも AWS の採用が進むことになった。

1. 国内向けネットワークサービスの相次ぐ提供

2011年3月に東京リージョンが開設され、遅延の問題が解決した。続く8月に VPC (Virtual Private Cloud/AWS 上のネットワークにプライベートなアドレスを割り当て、インターネット VPN で接続することができるサービス) が、2012年1月には専用線を引き込める「AWS Direct Connect」というサービスが東京リージョンで提供され始めたことによって、ネットワークに関する課題がほぼ解消された。

2. セキュリティ不安の払拭

AWS にとってセキュリティの確保はトッププライオリティであり、2006年のサービス開始以来、AWS は一度もセキュリティインシデントを発生させていない。

3. 国内事例の発表

2011年3月の東日本大震災直後、AWS とエンタープライズ AWS 導入ガイド製作者の一社である(株)サーバーワークスでは、日本赤十字社に対して、3,200億円もの義援金をインターネット経由で集めて管理するためのアプリケーションをわずか48時間で構築し、提供した。この事例が広く知られるようになり、震災のように予見不能なケースでも、AWS が、安全に個人情報を格納するセキュリティと、想定外のアクセスにも耐えられるという俊敏性を併せ持つことが広く認識されるようになった。

そして「AWS のエンタープライズ用途での適用」という流れを決定づけたのが、2013年の2月～6月にかけての事例発表である。2013年2月に日経 SYSTEMS で「クラウド・ファースト」という特集が生まれ、企業の IT 戦略として「オンプレミスと決別する」戦略が大々的に紹介されただけでなく、続く2013年6月に行われた AWS Summit Tokyo においてそうした戦略を実際に実行している企業の大規模な AWS 活用事例が発表されるに至り、現在の「エンタープライズ用途における AWS クラウド利用」という大きなトレンドにつながった。

第3節 AWS 概要

AWS とは、2006 年に開始したクラウドコンピューティングサービスである。

世界各国にデータセンター群を保有し、2011 年 3 月からは日本にも東京リージョンと呼ばれるデータセンター群を構え、サービスを提供している。

全世界に数十万の利用者がおり、日本でもユーザーの利用が急増しており、2013 年 6 月の時点で、既に 2 万以上の利用者数となっている。

AWS の特徴の 1 つとして、「地理的に分散された複数のロケーションを利用できる」という点がある。執筆時点で世界 11 拠点のリージョンが提供されており、さらにリージョンの中で、物理的に離れているデータセンター群が複数存在している。

例えば、異なるデータセンター群にまたがってシステムを構築することにより、データセンターレベルの障害にも対応できるシステムを構築できる。AWS はこれらのリージョンの中で数多くのサービスを提供しており、仮想サーバーやストレージといった基本的なサービスから、データウェアハウスやコンテンツ配信サービスも提供している。またシステム構築や運用の自動化を行うサービスや、操作権限管理のサービスなど、エンタープライズに必要とされるさまざまなサービスを提供しており、これらをシステム要件に応じて組み合わせることで、サーバー 1 台だけで稼働する開発用のシステムから、数百のアプリケーションから成り立つミッションクリティカルなシステムまで、柔軟に構築することができる。

AWS が提供するサービスは従量課金モデルで提供されており、初期費用を払うことなくシステム構築を開始できる。各サービスは数分で利用を開始することができるため、システム負荷やビジネス成長に合わせて、柔軟にシステムの処理能力を変更できる。例えば今この瞬間に、100 台のサーバーからなる業務システムが必要であったとしても、それを調達することができる。また次の瞬間、そのサーバーを破棄して課金を止めることもできる。これがビジネススピードやコストにもたらす恩恵は、想像に易いだろう。

例え定常的に使うシステムであったとしても、AWS は提供するサービスに対して執筆時点までに 38 回の値下げが行われており、ユーザーはその都度恩恵を受けることができる。これは今までの IT にはないメリットであるといえる。

また、これら新しい概念がありながらも、既存の IT 資産を活かせるサービス体系となっている。例えば、仮想サーバーであれば Windows や Red Hat Enterprise Linux といった OS を利用でき、アプリケーションや言語は今までのものを利用することができる。また、商用パッケージであったとしても、Oracle や SAP のようなグローバルベンダーのパッケージをはじめ、JP1 や HULFT のような国産パッケージも、AWS への持ち込みや AWS 上でのサポートを許諾しており、既存のシステムを無駄にせず、新たな価値をエンタープライズのシステムに付与することができる。

本書 1～2 ページの利用許諾契約書にご同意を頂けない場合、部分利用か又は全部利用かを問わず、本書を利用することはできません。

まとめると、AWS とは従来の IT 資産を活かしつつ、利用者のシステムやビジネスに付加価値を付けることができるサービスといえる。クラウドのもたらす付加価値については、次節で説明する。

第 4 節 AWS クラウドの付加価値

一般的にクラウドのメリットといわれるのは、「コストが下がる」「基盤の構築・変更が短期間で可能」といったことである。

クラウド活用は、「IT コスト削減」「新ビジネス立ち上げ」「BCP 見直し」「グローバル化への対応」などのビジネス課題に貢献する可能性がある。

システム観点では、クラウドをどこに適用するのかという視点で、享受できるメリットが変わってくる。

クラウドのメリット

ビジネス課題	メリット	利用例
IT コスト削減	スケールアップ、アウトが容易	<ul style="list-style-type: none"> 本番稼働後でもスペックを柔軟に変更できる(繁忙期のみ、システムを高スペックで稼働させることができる。)
	ハードウェアの管理が不要	<ul style="list-style-type: none"> パッケージソフトのサポート期間とハードウェアの更新を常に 考えなくてはならず煩雑だったが、ソフトウェア部分にフォーカスできる 開発・テスト時には、必要なときだけサーバーリソースを立ち上げて利用できる。必要でないときは停止してコストを削減できる。
新規ビジネス立ち上げ時のリードタイム短縮	新サービスの早期立ち上げ	<ul style="list-style-type: none"> 従来は、「ビジネスのアイデア」→「IT 部門による企画」→「利用者需要の把握」→「サーバー、アプリケーションの調達」→「サービス開始」と各調達プロセスを踏まなくてはいけなかったが、「ビジネスのアイデア」からすぐに「サービス開始」が可能となる

BCP の見直し	ディザスターリカバリー（災害対策）サイトであれば、すぐに作成できる	<ul style="list-style-type: none"> ・ 日本の国内でも距離の離れたデータセンター群を用いた、マルチクラスターサイトを構成することができる。 ・ さらに、海外データセンターに、容易に環境を立ち上げることができ、国外サイトを含めたディザスターリカバリーが可能
グローバル化への対応	海外展開が容易	<ul style="list-style-type: none"> ・ 日本国内で立ち上げたシステムを、海外リージョンに容易にコピーできる ・ 日本の国内から、ネットワーク(インターネットや VPN、広域 WAN 等)経由でどここの海外リージョンにでもアクセス可能

第5節 典型的なエンタープライズシステムの定義

本書では「エンタープライズシステム」を以下のように定義することにした。

[エンタープライズシステムの定義]

- ・大企業（資本金 10 億円超）が保有する社内/外を含めた全ての IT システム
- ・中堅企業（資本金 1 億円～10 億円）が保有する社内 IT システム

エンタープライズシステムの例

	システム例
基幹系	財務管理システム 人事管理システム 販売管理システム 購買管理システム 生産管理システム 会計システム EC サイト など
情報系	社内ポータル 電子メール ファイルサーバ データウェアハウス(DWH) ビジネスインテリジェンス グループウェア 営業支援ツール など

大企業であれば、社内システムはもちろんのこと、Web サイト1つをとっても、高い可用性に堅牢なセキュリティレベル、そして事前に規定されたプロシージャに基づく情報の更新など、企業レベルに相応しいさまざまな検討事項が存在する。これは一般論として会社規模に依るところが大であるから、大企業が持つシステムについては、それが社内向け用途か社外向け用途かを問わず、「エンタープライズシステム」と呼ぶことにした。

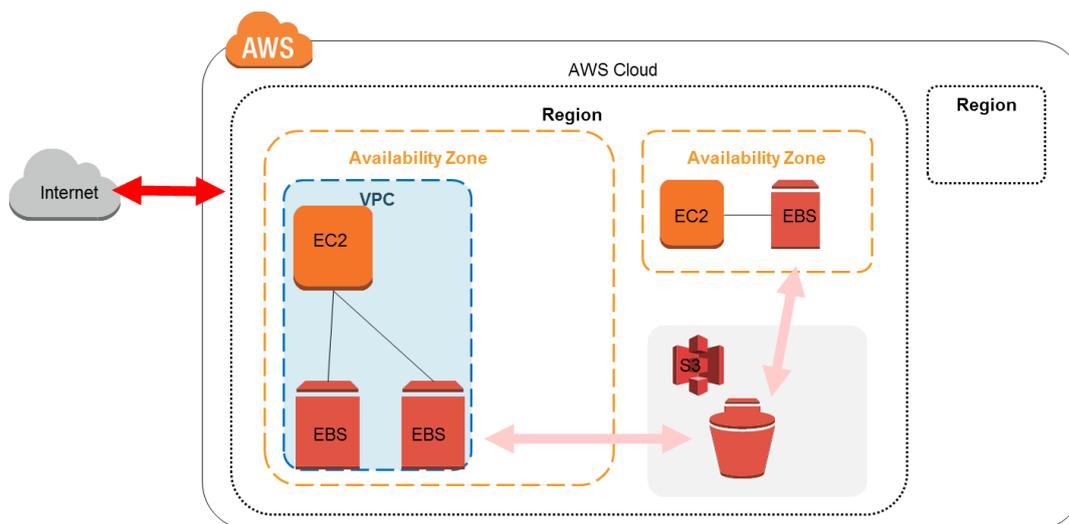
また、中堅企業であっても、社内システムが企業活動に与える影響の度合い、考慮すべき事項が大企業の保有するシステムに準ずることが容易に想像されることから、ここまでを範囲に含めることにした。

本書が以上の前提で構成されていることを、読者各位には注意されたい。

 本書 1～2 ページの利用許諾契約書にご同意を頂けない場合、部分利用か又は全部利用かを問わず、本書を利用することはできません。

第 2 章 AWS サービスの概要

AWS はコンピュータリソースといったインフラストラクチャーサービスからワークフロー管理などのアプリケーションサービス開発・管理といった広い範囲でサービスを提供している。まず、エンタープライズで利用する主なサービスを紹介する。



※Availability Zone はそれぞれ物理的に相当な距離を離れた独立したデータセンターを指し、1つのリージョンには必ず2つ以上の Availability Zone がある。

図 2 - 1

	名称 (略称)	概要説明
コンピューター	Amazon Elastic Compute Cloud (EC2)	<ul style="list-style-type: none"> 台数やスペックを柔軟に変更可能な仮想サーバー 必要な時に、必要な台数を時間課金で利用可能 コア数、メモリ容量が選べる VM Import/Export を使用することにより、オンプレミスにある仮想化環境の VM を、AWS にインポート/エクスポートすることが可能

ストレージ	Amazon Elastic Block Store (EBS)	<ul style="list-style-type: none"> ・ EC2 からマウントする仮想ドライブ ・ スナップショット(ディスクイメージのバックアップ)を取得可能 ・ スナップショットをリージョン間で転送可能
	Amazon Simple Storage Services (S3)	<ul style="list-style-type: none"> ・ 容量無制限のオンラインストレージ ・ 自動的に複数 DC にデータを保存し、高い耐久性を実現 ・ バックアップ、別の環境構築のテンプレートなどに利用できる
ネットワーク	Amazon Virtual Private Cloud (VPC)	<ul style="list-style-type: none"> ・ パブリッククラウドであってもプライベートクラウドのように利用することができるサービス ・ 社内ネットワークから AWS に VPN/専用線で接続
	AWS Direct Connect	<ul style="list-style-type: none"> ・ AWS クラウドへの専用線接続サービス ・ 1Gbps,10Gbps の物理ポートを利用可能 ・ サービスプロバイダーに依頼して、より多くのオプションを利用する事が可能

上記以外にもさまざまなサービスが提供されており、下記のサービスを組み合わせて利用することで、より効果的に AWS を利用することができる。

	名称(略称)	概要説明
コンピューター処理	Auto Scaling	<ul style="list-style-type: none"> ・ CPU 負荷や接続数などに応じて、EC2 のインスタンス数を自動的に増減 ・ 時間指定での増減も可能
ストレージ	Amazon Glacier	<ul style="list-style-type: none"> ・ 容量無制限のアーカイブストレージ ・ Amazon S3 と比べて約 10 分の 1 のコスト ・ 自動的に複数データセンターにデータを保存し、S3 と同等の高い耐久性を実現
	AWS StorageGateway	<ul style="list-style-type: none"> ・ オンプレミスおよび EC2 上に設置するアプライアンス ・ ディスクやテープをエミュレート

本書 1～2 ページの利用許諾契約書にご同意を頂けない場合、部分利用か又は全部利用かを問わず、本書を利用することはできません。

データベース	Amazon Relational Database Service (RDS)	<ul style="list-style-type: none"> マネージドの RDB(Relational Database)サービス AZ を跨いだマスター/スレーブ構成や自動バックアップ、自動パッチ適用などが利用可能 DB エンジンとして、Oracle Database、Microsoft SQL Server、MySQL、PostgreSQL が選択可能
	Amazon DynamoDB	<ul style="list-style-type: none"> スループット性能指定可能な高速 NoSQL サービス 3カ所のデータセンターの SSD でデータを保持 後から、スループットを変更可能
	Amazon Redshift	<ul style="list-style-type: none"> DWH 用のマネージドデータベース 最大 1600 コア/1.6PB まで拡張可能 スモールスタートでき、必要に応じて拡張できる
ネットワーク	Elastic Load Balancing(ELB)	<ul style="list-style-type: none"> AWS 提供の自動でスケールするロードバランサー 高信頼で低価格。SSL、ヘルスチェックなどを完備
	Amazon Route53	<ul style="list-style-type: none"> SLA100%の DNS サービス シンプルに使える GUI が提供されており、低価格で利用可能
データ転送	AWS Import/Export	<ul style="list-style-type: none"> 大量のデータを AWS へ入出力するサービス 物理媒体を AWS へ送付してデータを入出力
	AWS Data Pipeline	<ul style="list-style-type: none"> AWS サービス間のデータ転送を定期処理するサービス オンプレミスと AWS 間のデータ転送も可能
アプリケーションサービス	Amazon Elastic MapReduce(EMR)	<ul style="list-style-type: none"> ハードウェア購入不要の分散処理(Hadoop)サービス MapR,Hbase の利用が可能
	Amazon CloudFront	<ul style="list-style-type: none"> データ配信量に応じた低額な時間課金の CDN 世界 48ヶ所(東京・大阪含む)のエッジロケーション
	Amazon ElastiCache	<ul style="list-style-type: none"> Memached と Redis 互換のキャッシングサービス 利用時間×利用台数に応じた支払い
	Amazon Simple Email Service(SES)	<ul style="list-style-type: none"> メール送信を行えるサービス 送信サーバーの管理不要。バウンス情報などの取得が可能
	Amazon Simple Notification Service (SNS)	<ul style="list-style-type: none"> イベント発生時に、指定の通知先へ通知 通知方法はメール、HTTP、SQS、モバイル Push

アプリケーションサービス	Amazon Simple Queue Service (SQS)	<ul style="list-style-type: none"> メッセージをキューイングするサービス メッセージが取得されるまで、メッセージは冗長化して保管される
	Amazon Simple Workflow (SWF)	<ul style="list-style-type: none"> ワークフローの実行エンジンを提供するサービス フローを開発する「Flow Framework」を提供
	Amazon Cloud Search	<ul style="list-style-type: none"> 投入したデータに対する検索機能を提供するサービス 文字列、数値、ファセットなどで検索が可能
	Amazon Elastic Transcoder	<ul style="list-style-type: none"> 動画のエンコードサービス 指定の S3 バケットに置くだけで、変換を実行
	Amazon AppStream	<ul style="list-style-type: none"> 負荷の高いアプリケーションの処理を AWS 上で行い、クライアント端末へストリーミング配信するサービス 端末能力に依存せず、複雑なアプリケーションの実行が可能
管理・配備	AWS Elastic Beanstalk	<ul style="list-style-type: none"> Web アプリケーション実行環境を提供する PaaS ライクなサービス Java、PHP、.NET、node.js、Ruby、Python のコンテナが選択可能
	AWS CloudFormation	<ul style="list-style-type: none"> AWS のサービスをテンプレートから構築できるサービス テンプレート化することで、システム構成の再利用が可能
	AWS OpsWorks	<ul style="list-style-type: none"> Chef を使用した運用自動化サービス システムをレイヤーで管理できる
	AWS Identity and Access Management (IAM)	<ul style="list-style-type: none"> AWS 操作グループ/ユーザーの管理サービス グループ/ユーザーごとに、サービス操作権限の付与が可能 SAML をサポート
	AWS Directory Service	<ul style="list-style-type: none"> オンプレミスの Active Directory と連動可能なディレクトリサービス。AWS クラウド上にスタンドアロンで構築も可能 既存の認証システムに AWS クラウドのリソースを容易に組み込むことが可能
	AWS Management Console	<ul style="list-style-type: none"> ウェブベースの AWS の管理ツール 自身の利用する様々な AWS のサービスや構成を一元管理する事が可能
	Amazon CloudWatch	<ul style="list-style-type: none"> AWS クラウドリソースと カスタムメトリックにて設定できる AWS 上でユーザーが実行する OS・アプリケーションなどのモニタリングサービス

管 理・ 配 備	AWS CloudHSM	<ul style="list-style-type: none"> AWS クラウド内の専用ハードウェアセキュリティモジュール (HSM) アプライアンスを使用し、データセキュリティに対する企業コンプライアンス要件、および法令遵守の要件を満たすことができるサービス
	AWS CloudTrail	<ul style="list-style-type: none"> アカウントに対する AWS API 呼び出しを記録し、ログファイルを配信するウェブサービス。アカウントのセキュリティ分析、リソース変更の追跡、コンプライアンスの監査を行うことが可能
	AWS SDK、IDE およ びコマンドラインツ ール	Java、Python、PHP、.NET、Ruby、node. js、JavaScript、iOS、Android、AWS Toolkit for VisualStudio、AWS Tools for Windows PowerShell、CLI

第2部 AWSによるエンタープライズシステム実現の勘所

第3章 エンタープライズシステム構成例

本章ではAWS上でエンタープライズシステムを実現するための構成例を示す。

エンタープライズシステムには小規模システムにはないさまざまなシステム要件が求められるが、本章ではそれら要件を大きく下記の3つの観点に分類しシステム構成例を示す。

- ・ システムの重要度
- ・ グローバルへの展開や既存システムとの連携等のシステムの広がり
- ・ ユースケース

第1節 重要度別のシステム構成例

第1項 システムに求められる重要度分類

エンタープライズシステムの実現においては、そのシステムが支えるビジネスの特性に応じて重要度が設定される。

ここではエンタープライズシステムを3つの重要度に分類し、それぞれに求められる一般的な要件を示す。

重要度	概要	求められる要件	可用性			主なケース
			障害復旧時間	復旧ポイント	災害対応	
ノンプライムシステム	事業の効率化やビジネスの促進を支えるシステム	目標稼働率 99% 標準的なセキュリティ対応	24 時間	前日バックアップ	非対応	情報系システム
プライムシステム	事業の根幹を支えるシステム	目標稼働率 99.99% 高度なセキュリティ対応	30 分	障害発生直前	非対応	基幹系システム
ミッションクリティカルシステム	グローバル規模に展開する事業の根幹を支えるシステム	目標稼働率 99.99% 高度なセキュリティ対応	30 分	障害発生直前	対応	大規模基幹系システム

第2項 ノンプライムシステムのシステム構成例

AWS Architecture Model – ノンプライムシステム

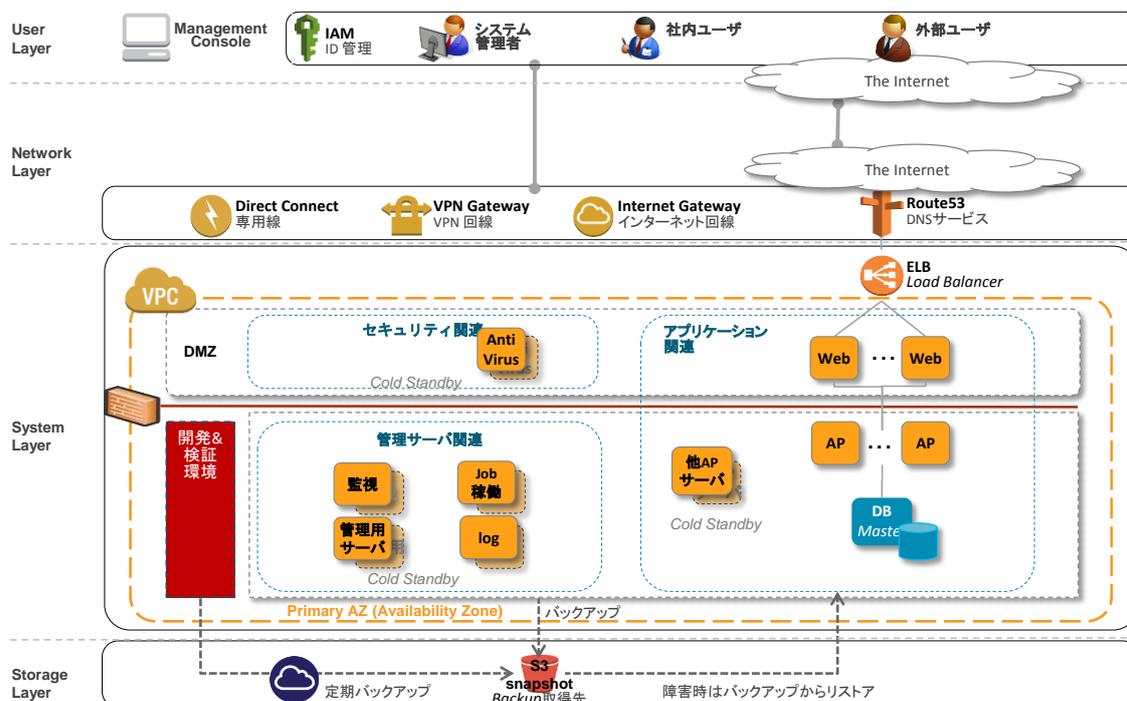


図 3-1

■ 概要

会社経営の効率化やビジネスの促進に貢献することを主な目的とするノンプライムシステムは、システムが停止したとしても事業継続自体に大きな影響を及ぼさない。しかしビジネスの成長を支えるシステムである以上、ある一定の稼働率を実現する必要がある。

AWS においてはインスタンスの故障発生時には新しいインスタンスを起動し復旧することができるため、低コストで十分な可用性を確保することが可能と考える。

■ 特徴

【基本的な稼働率の実現】

オンプレミスでは機器障害発生時には、障害の調査や機器交換などに時間がかかり、稼働率を減少させる主な要因となることが多い。そのため、あらかじめ余分に機器を調達しておき、平時はコールドスタンバイとしておくことで、障害に備えることが一

一般的である。

一方 AWS を利用する場合、インスタンスに障害が発生した時点でインスタンスを再起動する、または他のインスタンスを起動することで迅速な復旧が可能と考える。また、普段はインスタンスを停止しておくことで課金が発生しないため、コストを削減することが可能と考える。

【標準的なセキュリティの実現】

AWS はセキュリティに関する各種サービスを標準機能として提供しており、それらサービスを組み合わせることで、標準的なセキュリティを実現可能と考える。

- ・ VPC によるプライベートでセキュアなネットワーク空間の実現と、VPN や Direct Connect による VPC への暗号化経路を通じたセキュアな接続の実現
- ・ Network Access Control List やセキュリティグループ等、柔軟に設定が可能なファイアウォール機能により外部または内部からの不正侵入を防止
- ・ IAM 機能を用いて AWS を操作するための ID やロールの細かい設定を行うことで、誤操作や不適切なユーザーによる操作を防止

【低コストでのデータバックアップの実現】

大規模障害発生時において、一般的にノンプライムシステムではプライムシステムのように数十分以内という短時間での復旧は求められないが、それでも効率的に障害から復旧できるようバックアップデータや OS イメージを保存しておく必要がある。

これらの仕組みをオンプレミスで用意する場合、バックアップ用のストレージやテープドライブなどのハードウェアを調達する必要があるが、AWS では AWS が提供しているストレージサービスを利用することで実現可能と考える。また、システムの運用とともにバックアップデータが増大していくことが一般的であり、オンプレミスではあらかじめ運用期間を考慮した最大ストレージ容量を確保しておくことが一般的であるが、AWS においてはバックアップデータ量に応じて柔軟にストレージ容量を増強可能であり、初期投資を削減することが可能と考える。

具体的なバックアップ方式を以下に示す。

- ・ 各サーバーのシステムバックアップを AMI のイメージスナップショットとして、構成変更のたびに S3 に保存する
- ・ 各サーバーのデータバックアップを EBS のスナップショットとして S3 上に定期的に保存する
- ・ 取得した AMI からコールドスタンバイとしてインスタンスを作成し、インスタンスは停止の状態にしておき、障害時にはスナップショットから作成した EBS を、スタンバイのサーバーにマウントして起動させることで復旧が可能と考える。

第3項 プライムシステムのシステム構成例

AWS Architecture Model – プライムシステム

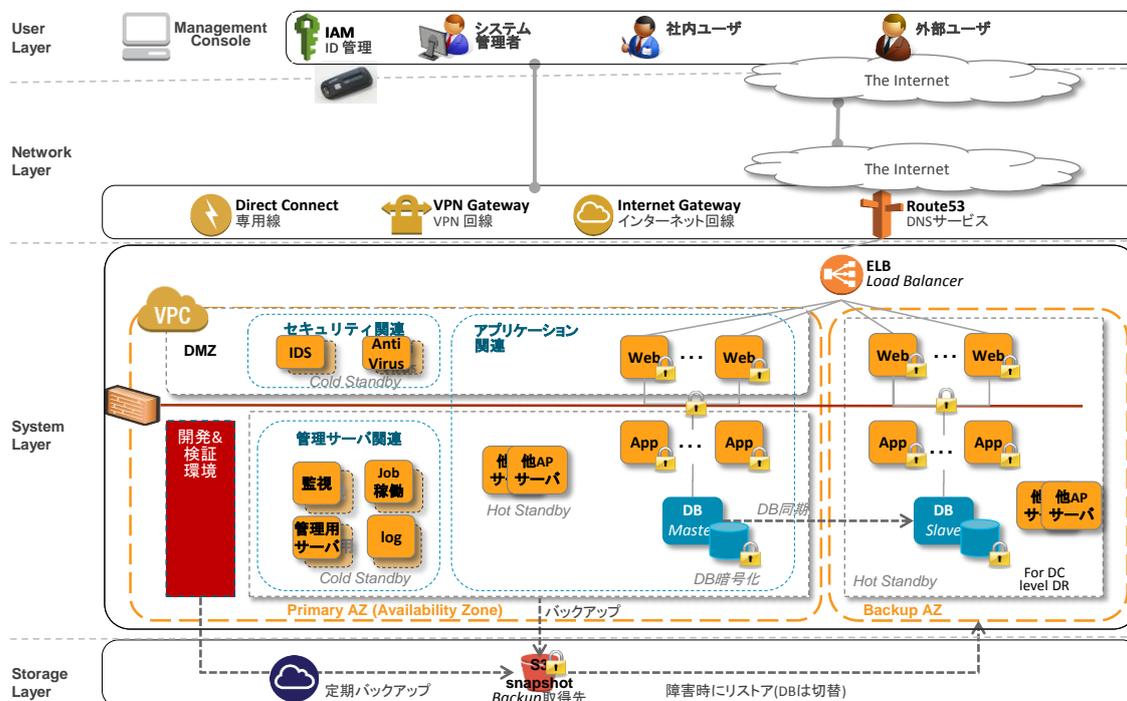


図 3-2

■ 概要

事業の根幹を支えるプライムシステムには、大規模な障害やデータセンターレベルの障害発生時においても、システムが継続的に利用可能であることが求められる。

また、企業のビジネスの中核をなす重要なデータを扱うことが多く、高度なセキュリティの実現も必要不可欠である。

AWS では、複数のアベイラビリティゾーンとデータの暗号化ソリューションなどを組み合わせることで、これらの要件に対応したシステムを実現可能と考える。

■ 特徴

【大規模障害やデータセンターレベル障害への対応】

複数のアベイラビリティゾーンに亘るシステムを構成し、外部からのアクセスを ELB で分配することで、容易に可用性の高いシステムを実現可能と考える。

データ層に関しては、AWS のデータレプリケーションの機能を利用することで、こちらも複雑な構築に工数をかけずに、複数のデータセンターにまたがってデータベース

のリアルタイムデータコピーが実現可能と考える。

障害発生時には、アプリケーションサーバーからのデータベースへの接続は自動的にスレーブへ接続が切り替わるため、システムの稼働が継続される。

【障害発生直前までのデータ復旧】

プライムシステムでは常に大量のデータが作成、更新されるため、万が一の事態に備え、障害発生直前のデータを復旧できる仕組みを組み込んでおく必要がある。前述の通り、複数のデータセンターにデータをコピーすることで耐障害性を高め、常に最新のデータを復旧することが可能と考える。

【高度なセキュリティ】

プライムシステムにおいては、ノンプライムシステム以上にセキュリティを考慮した構成を実現する必要がある。AWS では AWS が備えるセキュリティ関連オプション機能の利用やサードベンダーソリューションを利用することで、高度なセキュリティを実現可能と考える。

- ・ データベースの表領域や特定のテーブルの列を暗号化し、データベースへの不正アクセスやデータの抜き取りに対する対策を行う。Amazon RDS では暗号化機能を備えた RDB が利用可能であり、その機能を利用する事ができる。また、RDS ではなく、仮想サーバー上にデータベースを独自でインストールする場合は、データベース暗号化ソリューションと組み合わせることが可能である。
- ・ データストレージである S3 の暗号化も AWS のセキュリティオプションで実現可能である。
- ・ 通常、Management Console へのログインは、ユーザーID とパスワードによる認証となっているが、認証にハードウェア MFA (Multi-Factor Authentication) を適用することで、万が一のユーザーID やパスワードが漏えいした場合にも、認証用ハードウェアを所持していなければログインできないような仕組みを構築でき、不正アクセスの防止が可能と考える。
- ・ サードベンダー製の侵入検知 (IDS)、侵入防止 (IPS) 製品を導入することで、サーバーへの不正侵入の検知と対応が実現可能と考える。
- ・ CloudTrail により、AWS API の呼び出しを記録することが可能であると考えられる。履歴には、Management Console、AWS SDK、コマンドラインツール、AWS CloudFormation などを使用した API の呼び出しが含まれる。CloudTrail で生成される履歴を利用して、セキュリティの分析、リソース変更の追跡、およびコンプライアンスの監査が実現可能と考える。

第4項 ミッションクリティカルシステムのシステム構成例

AWS Architecture Model – ミッションクリティカル システム

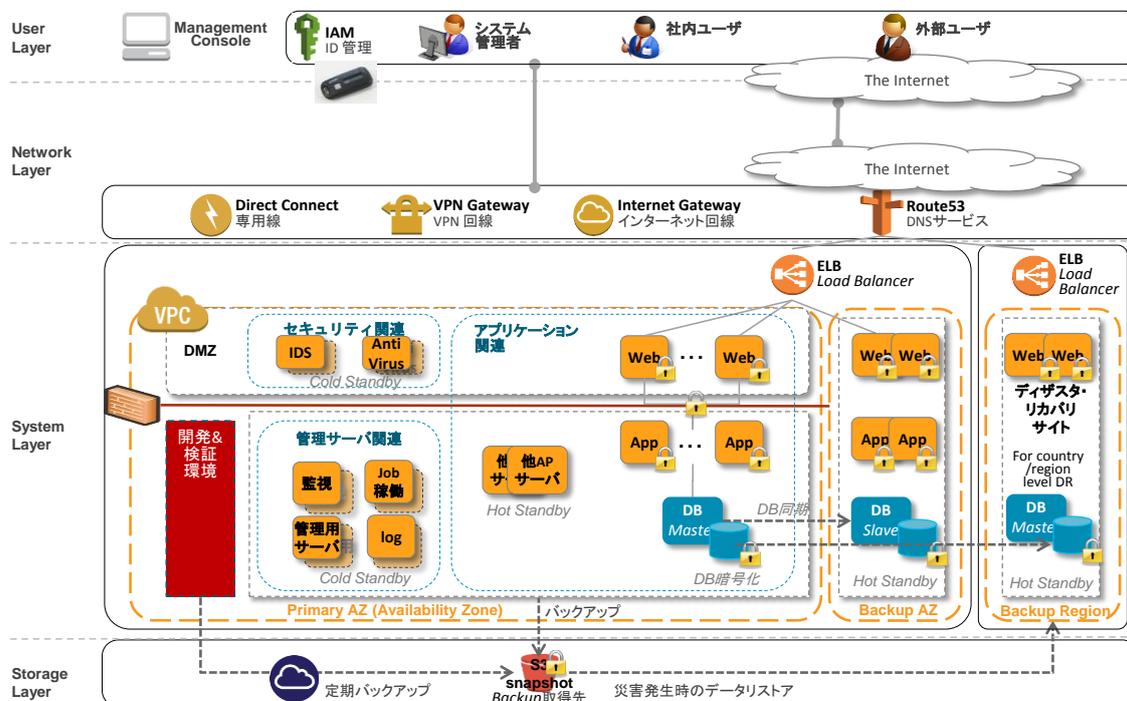


図 3-3

■ 概要

グローバルに事業を展開する企業では、万が一の大規模災害の発生時においても、被災地域以外での業務の継続が必須であり、業務の根幹を支えるミッションクリティカルシステムは、どのような状況下においてもその継続性が求められる。

AWS では世界中に存在する複数のリージョンを活用することで、大規模災害発生時においても迅速に他の地域でシステムを使えるように対応可能であり、グローバル規模での事業の継続を実現可能と考える。

■ 特徴

【グローバル規模のディザスタリカバリーの実現】

ミッションクリティカルなシステムの場合、大規模災害によってグローバルレベルでのディザスタリカバリーが必要となる場合でも、短時間でフェールオーバーを完了することが求められる。

オンプレミスのシステムであれば海外のデータセンター上に同様の環境を構築し、何

らかの方法でデータ同期を行い、バックアップサイトを構築する必要がある。

AWS では、バックアップリージョンに AMI からインスタンスを作成しておき、データベースのデータを Oracle Data Guard や Geographic Replication 等でバックアップサイトへ同期しておく。

災害発生時には Route53 (DNS サービス)の設定を変更し、アクセスをバックアップリージョンヘルレーティングするだけでフェールオーバーを行うことが可能となる。

バックアップサイトのインスタンスは復旧時間とコストのバランスを検討し、最短の復旧時間を実現するために常時インスタンスを起動しておくことも可能ではあるが、なるべくコストを削減するため、インスタンスを停止した状態にしておき、災害発生時に起動するという構成も可能と考える。

第2節 システムの広がり を考慮したシステム構成例

本節では、システムの広がり を考慮したシステム構成例として、オンプレミスと AWS によるハイブリッド環境のシステム構成例とグローバルにシステムの利用が広がるようなユースケースでのシステム構成例を示す。

第1項 ハイブリッドシステムのシステム構成例

AWS Architecture Model - オンプレミス・AWSクラウドハイブリッドシステム

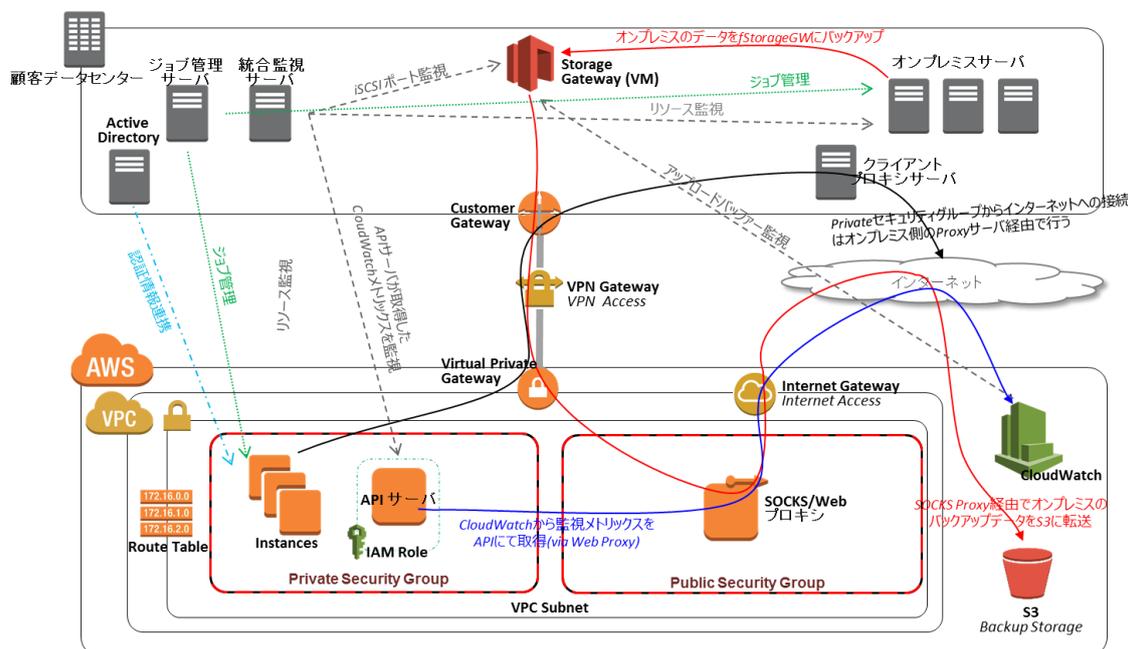


図 3-4

■ 概要

短期間、低コストで社内システムを拡張する必要が生じた場合、AWS クラウド基盤を利用したシステム拡張が有効な手段として考えられる。既存のシステム資産と AWS 上のシステムとのシームレスな統合を実現し、システム整備のスピードとコストのバランスを最適化することを指向するアーキテクチャーを「ハイブリッド型アーキテクチャー」と定義する。

■ 特徴

【シームレスでセキュアなネットワーク】

社内システムの高度化に伴い、リソースが不足してきた場合や、新規機能を開発した

い場合、AWS を利用することでスピーディかつ低コストで実現可能と考える。一方で、クライアントのセキュリティポリシーにより、外部への社内情報保管が許容されず、クラウド基盤の利用を躊躇するケースが存在する。こうしたセキュリティ要件には、VPC によりセキュアなプライベートクラウドを構築することで対応可能と考える。この VPC はサブネットなども全てオンプレミスと整合性のある形で構築でき、オンプレミスとセキュアかつシームレスに統合することができる。

また、VPC 内では柔軟に通信経路の設定を行うことができる。図 3-4 では、ルーティングルールとして S3、CloudWatch などの AWS サービスへ通信する際には VPC から直接インターネットへ接続する経路を通り、その他オンプレミスと同様の運用用途（パッチ適用等）でインターネット接続する場合にはオンプレミス側のプロキシサーバーを経由するよう指定している。この設定により、AWS 環境上のサーバーは全てオンプレミス環境と同様の運用手順が適用でき、VPC をオンプレミスの延伸と捉えることが可能となるため、サーバーからの Web アクセスポリシーなどの、企業の個別のセキュリティポリシーにも対応することが可能と考える。

【既存資産の活用】

オンプレミスとセキュアに接続した上で、企業が保有する既存システム資産を活用することが可能である。例えば、EC2 は多くのジョブ管理および監視製品に対応しており、オンプレミス側のジョブ管理サーバー、監視サーバーと連携可能である。AWS 上にシステムを拡張した場合でも、既存の管理/監視システムを用い、従来の方法で各リソースを一元的に管理できる。また、オンプレミス環境に Active Directory が存在する場合は、AWS 上のシステムと連携してシングルサインオンを実現する事も可能と考える。さらに、マネージドサービスである AWS Directory Service の AD Connector ディレクトリタイプは、オンプレミス環境の Active Directory に対する認証機能のプロキシとして利用が可能であり、複雑なアカウント情報同期のテクノロジーやフェデレーション処理なしで、オンプレミス環境とのシングルサインオンが実現可能と考える。

【リソースの増減対応（月末、年末、ピーク時など）】

AWS リソースは、業務量の増減が大きいシステムにおいてコストメリットを発揮する。企業の業務システムは、業務の特性上、ある一定期間にシステム利用量が増大し、サーバーに負荷がかかるケースが多い。例えば、「月末に大きな月次処理が走る」、「年末に年次処理を行うために極端に業務量が増加する」、「全業務ユーザーがアクセスする時間帯が存在する」などが考えられる。こうした場合、オンプレミスではこの負荷増大時を見越してリソースのサイジングを行うことが一般的であるため、普段はリソースに余剰がある状態となるが、AWS では負荷状況に応じてリソースの増減（スケー

ルアップ、スケールアウト)が可能である。従量課金制である料金体系により、コストが最適化され余剰リソースに対してコストを支払う必要がなくなる。

第2項 海外拠点グローバルシステム連携のシステム構成例

AWS Architecture Model – グローバルシステム

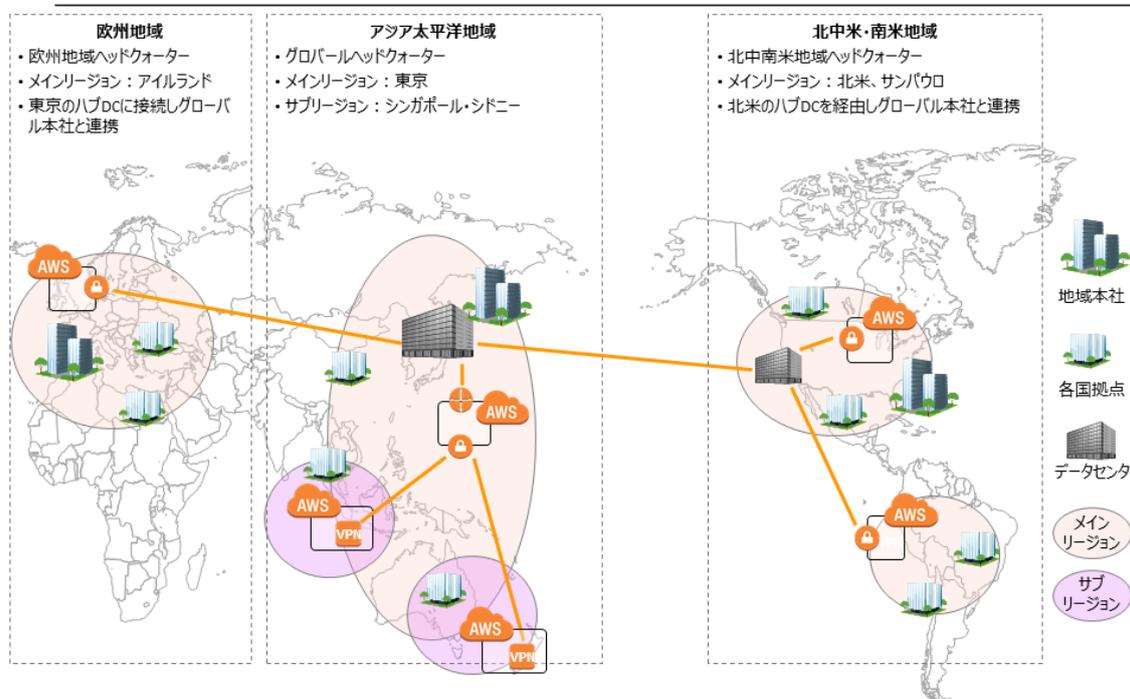


図 3-5

■ 概要

グローバルに事業を展開する企業において、業務遂行上必要となるシステムを対象地域に配置することは必須であるが、単純にその地域にデータセンターを配置しシステムを構築した場合、地域ごとにシステムがサイロ化し業務上の非効率やガバナンスの不全につながる可能性がある。そのため、地理的に分散しながらもシステム間の連携性を十分に担保することは重要な課題であるといえる。また新興国に展開する場合、データセンターを調達するにあたっては先進国と比較して大きな時間とコストが必要となり、場合によってはその地域への展開の足かせとなりうる。AWS では多くの国・地域をカバーする複数のリージョンが配置されており、それらを相互に接続することが可能であるため、このようなグローバル展開におけるシステム課題への解となりうる。

■ 特徴

【地理的に分散したシステム間での連携】

本書 1～2 ページの利用許諾契約書にご同意を頂けない場合、部分利用か又は全部利用かを問わず、本書を利用することはできません。

地理的に分散したシステム間での連携を担保するためのデータセンター間の接続方式としては MPLS などのキャリア国際網、およびインターネット VPN が一般的である。AWS ではこのいずれの方式もサポートしており、AWS リージョン間、およびオンプレミスのデータセンターと AWS リージョンとの間での接続を構築できる。構成としては、オンプレミスのデータセンターが存在する場合にそれを複数の AWS リージョンに対するハブとして利用する構成、および複数の AWS リージョンを相互に接続する構成が考えられる。オンプレミスデータセンターをハブにする構成では DirectConnect (MPLS の場合)または VPN 接続 (インターネット VPN)を用いてデータセンターと複数の AWS リージョンを接続する。AWS リージョン同士を接続する方式では、一方のリージョンにソフトウェア VPN をインストールし、そこに対して他方のリージョンから VPN で接続する。いずれの構成でも、複数のリージョンを 1 つのネットワークとして構成し、システム間連携を行うことが可能と考える。

【海外拠点でのスピーディなシステム構築】

新たに海外拠点を立ち上げる場合には現地での事業内容に応じて業務システムの配備が必要となる。AWS では東南アジア、南米などの新興国地域を含む 9 つのリージョンが配備されており、展開先の地域に応じて選択することができる。特に新興国地域においては、AWS は現地でのデータセンターの調達と比較して極めて迅速かつ低コストで調達できるため、海外での事業展開におけるリスクの低下につながると考える。また、他の地域のシステムが AWS 上で稼働している場合、新たな展開先において他地域のシステム資産を活用することが容易になり、これも同様にリスク低下要因と考える。また、一般に海外展開の初期段階では展開されるシステムは最小の構成となっており、その他の機能は本社側のシステムを利用するというケースが多い。このようなケースでは現地で必要となる最低限のシステムを拠点に近いリージョン (サブリージョン) に配備し、その他の機能は前述のリージョン間接続を通じて本社側のリージョン (メインリージョン) を利用するという構成も可能と考える。

第3節 ユースケースごとのシステム構成例

本節ではエンタープライズシステムの代表的なユースケースとして、SAP とアナリティクスシステムの AWS を活用した構成例を示す。

第1項 SAP を用いた基幹系システムのシステム構成例

AWS Architecture Model – 大規模基幹システム SAP on AWS

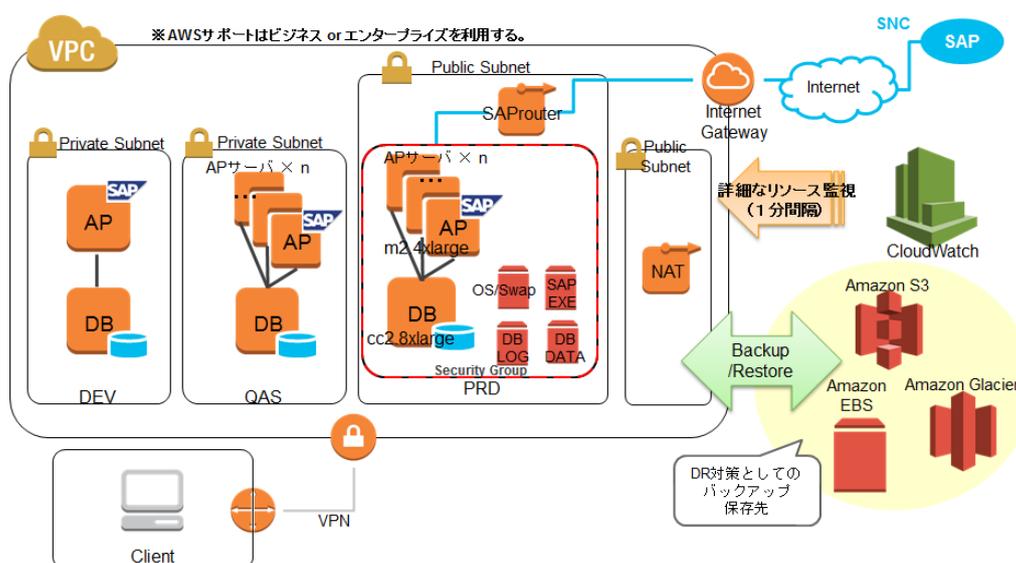


図 3-6

■ 概要

大規模基幹系システム向けパッケージとして広く利用されている SAP は、従来はオンプレミスで利用されてきたが、近年では次第にクラウド化のニーズが高まっている。基幹システムのクラウド化は、国内企業の海外進出時あるいは海外企業買収時にスピーディに現地の基幹システムを構築し、また撤退時のコスト最小化を実現する。SAP社の定義するパブリッククラウドでサポートされている唯一のクラウド基盤として AWS が挙げられ、本番環境への導入実績が増えつつある。SAP の基本的な構成を AWS 上で構築するアーキテクチャーモデルを記載する。

■ 特徴

【海外拠点における基幹システムの短期構築】

企業が海外に支社を新規設立する場合や、海外企業を買収する際に国内で使用している SAP による基幹システムと同等の機能を現地に速やかに構築したい場合、AWS を

利用することが有効である。AWS 上での SAP の動作は SAP 社によりサポートされており、オンプレミスと同機能のシステムを AWS で構築可能と考える。海外進出時に今後の展望が予測困難であったとしても、AWS 環境であれば構築作業および撤退作業が容易かつ低コストで実施できるため、低リスクでシステム構築が可能と考える。

【高い拡張性によりシステム性能を柔軟に変更】

AWS では、システムの利用状況（アクセス数等）に応じて柔軟に性能を変更可能であり、例えば、毎月末にシステムの利用が通常時の 3 倍になる場合はその期間のみ SAP の処理能力を追加することができる。具体的にはアプリケーション層は通常時は 1 台のサーバーで処理を行い、月末の高負荷条件下においては 2 台以上にサーバー台数を増加（スケールアウト）させることができる。データベース層は通常時は低スペックのサーバーで実行し、高負荷が想定される場合は高スペックのサーバーに切り替える（スケールアップ）ことが可能である。オンプレミスで利用する際には高負荷時に合わせてシステムリソースのサイジングを行うため、通常時にはリソースの余剰分が存在する状態となりコストも高額となる。一方で、AWS は負荷状況に応じスケールアップ/スケールアウトができるため、従量課金制のコストメリットを享受できると考える。

第2項 情報系システムのシステム構成例

AWS Architecture Model
 - Redshiftを活用したアナリティクスシステム

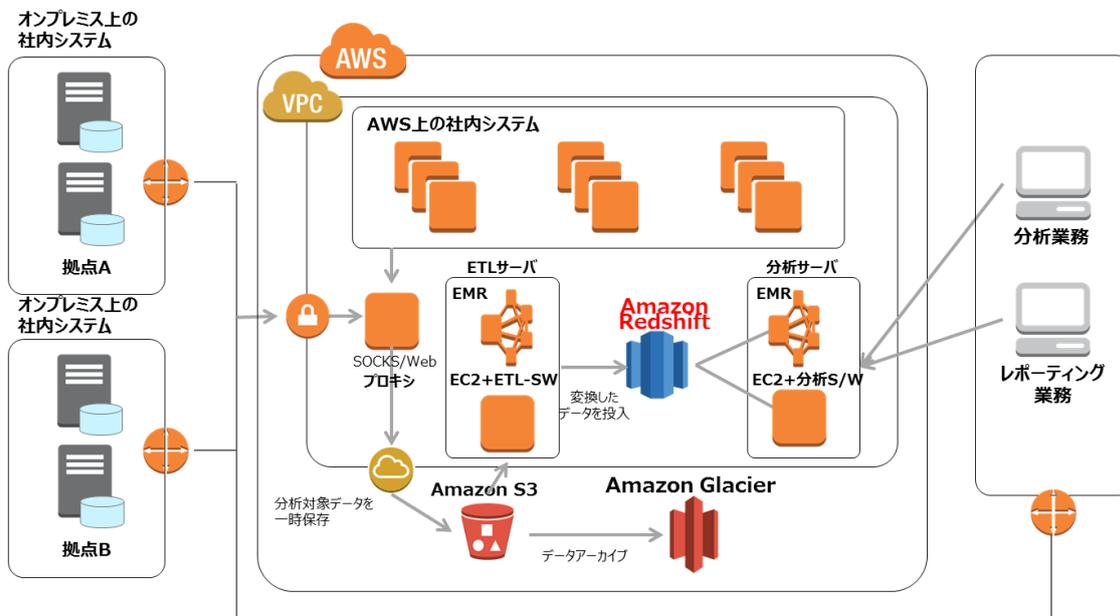


図 3 - 7

AWS Architecture Model
 - Data Pipelineを活用したアナリティクスシステム

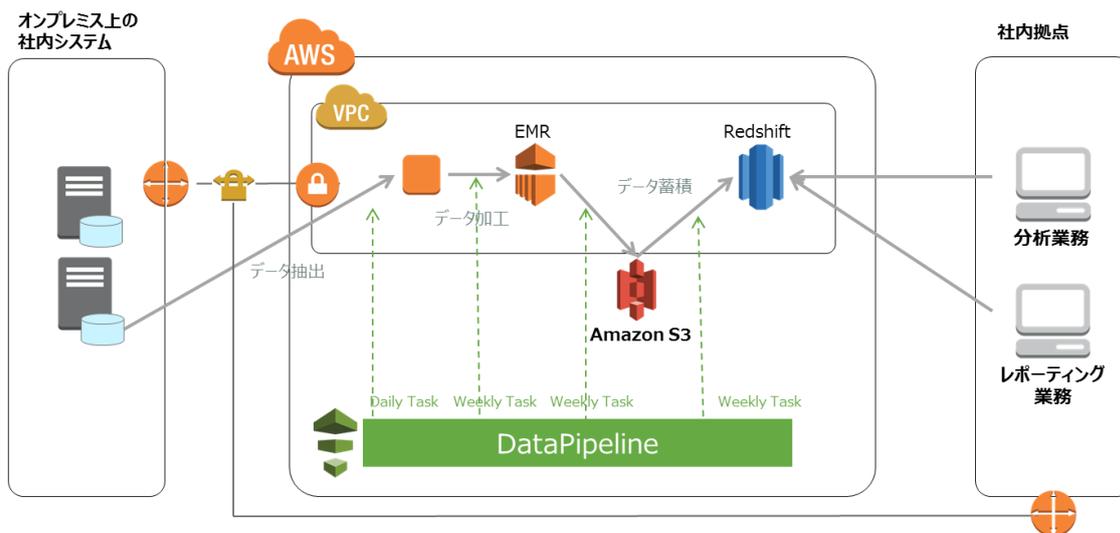


図 3 - 8

本書 1~2 ページの利用許諾契約書にご同意を頂けない場合、部分利用か又は全部利用かを問わず、本書を利用することはできません。

■ 概要

企業内外に存在するデータを蓄積し、有効活用するニーズが高まっている。特にそれらデータを迅速に分析し経営戦略に活かすため、ビッグデータやアナリティクスが注目を集めているが、オンプレミスで実現する場合、一般的にその初期投資が高額なものになっていた。AWS では低価格のデータウェアハウスとして Redshift を提供しており、AWS 対応の分析ツールと併用することで、少ない初期投資でアナリティクス環境を構築することが可能と考える。

■ 特徴

【スモールスタート可能で従量課金制のサービス】

Redshift は、高いパフォーマンスのデータウェアハウス機能を安価に提供している。クラウドの特徴の1つである高い拡張性を備えており、データの少ない状態では定額の課金でスモールスタートを実現し、必要に応じてスケールアップすることが可能である。これにより、ビジネスの状況の変化でデータ量が増大した場合でも、性能を落とさずに稼働させることが可能と考える。オンプレミスで導入しようとする機器調達のリードタイムや将来的なデータ量増大を見込んだサイジングを考慮する必要があり、また初期費用も比較的高額になるなど、データウェアハウスの導入に至るまでは検討事項が多く存在する。一方で、低額のスモールスタートが可能な Redshift を利用する場合にはこれらの検討事項は考慮不要であり、企業のデータウェアハウス導入の敷居を大幅に下げるソリューションといえる。

【多くのサードパーティー製品の対応】

規模の大きな企業は、各部門や各拠点に大量の業務データを持ち、データウェアハウスを採用しなければ全てのデータを集中・統合することは現実的でない。図 3-7 では、クライアント本社システムは AWS 上で稼働しており、一方で拠点システムはオンプレミスに置かれているようなケースにおいて、Redshift を利用する際の構成例を示している。多様なデータソースから Redshift にデータを取り込むためには ETL (Extract/Transform/Load) ツールが必要となるが、EC2 上では多くの製品がサポートされており、AWS 上にさまざまな体系のデータを変換可能な ETL サーバーを構築可能と考える。Redshift からデータを取得し分析を行うツールとしては、SAS や Congnos、Pentaho、Tableau 等多くの製品をサポートしている。ETL、分析ツールのいずれについても、AWS の並行処理アーキテクチャーである EMR を利用することで高いパフォーマンスでのデータ変換処理や分析処理を実現可能と考える。

また、AWS Data Pipeline サービスを利用する事で、S3、RDS、DynamoDB、Elastic

MapReduce のような AWS サービスやオンプレミス環境に分散されているデータを効率よく連携させ、信頼性のあるデータ処理やデータ移動、および指定した間隔での自動実行も実現可能と考える。

第4章 システム・運用要件

本章は、エンタープライズシステムを企画・設計する際に、一般的に考慮すべきと考えられる要件について、AWS でどのような対応が可能かについてまとめたものである。以降に記載する要件リストでは、エンタープライズ AWS 導入ガイド製作委員会への参加各社が実際に顧客からよく問い合わせを受ける項目をリスト化している。これは下記に参考を示すようなさまざまな業界団体のガイドや基準を完全に満たすものではないが、実際のエンタープライズシステムの構築を手がけてきたエンタープライズAWS導入ガイド製作委員会への参加各社の知見ならびに経験に基づくものであるため、必要最小限のリーズナブルな要件リストであると考えられる。

さらに厳しい基準を満たす必要がある場合には、下記のガイドや基準を参考にされたい。

- ・ クラウドサービス利用のための情報セキュリティマネジメントガイドライン（経済産業省）
- ・ データセンターの安全・信頼性に係る情報開示指針 第2版（総務省）
- ・ IaaS・PaaSの安全・信頼性に係る情報開示指針（総務省）
- ・ 非機能要求グレード（独立行政法人 情報処理推進機構）
- ・ クラウド情報セキュリティ管理基準（特定非営利活動法人日本セキュリティ監査協会）
- ・ 金融分野における個人情報保護に関するガイドライン（金融庁）
- ・ 金融機関等コンピューターシステムの安全対策基準（FISC 安全対策基準）

第1節 基本サービス要件

ユーザー企業が一般的にパブリッククラウドサービスを選択する際に、サービス提供事業者を求める基本的なサービス仕様および要件について列挙し、AWSにおける回答を記載する。AWSの場合、サービス種別も多い上、各サービスの要件・オプション・課金体系も非常に多岐に亘り、アップデート頻度もかなり高い。従って、AWSを利用する際は、リアルタイムでより正確にサービス要件の理解・把握に努める必要がある。

項目	要件	回答
1-1 提供プラットフォーム種別	提供スペック/ゲスト OS/データベースエンジン/契約体系/ストレージサービス	AWS における、提供可能なインスタンスタイプ (EC2/RDS)、選択可能なゲスト OS 種別 (EC2)、選択可能なデータベースエンジン (RDS) は、多岐に渡る。各インスタンスの契約体系もオンデマンド/リザーブド/スポットの 3 種類から選択可能である。 また、ストレージサービスも 4 種類から選択可能で、用途や予算等に応じて、うまく使い分けることが重要となる。
1-2 リソース準備までの時間	新規アカウント作成/リソース準備までの時間	AWS は、オンデマンド性/拡張性に優れたサービスで、Management Console および AWS コマンドラインツール (API 連携) 経由で、柔軟になおかつ迅速に、システムリソースの伸縮が可能である。
1-3 管理ポータル機能	機能概要/制御・確認が可能な機能/閲覧可能な統計情報	AWS では、管理ポータル機能として、「Management Console」が用意されている。Management Console では、数多くの AWS のサービスについて制御・確認が可能である。 また、仮想サーバーや ELB / RDS などの統計情報も、Management Console にて閲覧可能である。
1-4 API 連携	API 連携	AWS では、数多くのプログラミング言語またはプラットフォーム用の SDK が用意されており、Management Console を経由せずに、コマンドラインでも各種 AWS サービスが操作可能である。

1-5 災害対策	日本国内/グローバルレベルでの災害対策	<p>AWS を利用した災害対策として、以下の 3 種類に大別される。</p> <ul style="list-style-type: none"> ・ AWS のみを利用する場合(日本国内の災害対策) ・ オンプレミス環境のディザスターリカバリー先として AWS を利用する場合(同上) ・ AWS のみを利用する場合(グローバルレベルでの災害対策) <p>災害対策に関わるシステム要件と予算等の諸条件を考慮して、AWS のサービスを選択していくことが重要となる。</p>
1-6 持ち込み可能ライセンス (BYOL)	Red Hat /Microsoft 製品 /Oracle 製品 /その他製品の BYOL	<p>AWS 環境への持ち込み可能ライセンス (BYOL)として、よく議題に上る Red Hat Enterprise Linux/Microsoft 製品/Oracle 製品について、詳細を別途「付録」に記載する。</p> <p>また、その他のソフトウェア製品でも 1,000 をはるかに超えるソフトウェアのライセンス提供や BYOL が可能で、AWS Marketplace や AWS の Web サイトにて詳細確認することが可能である。</p>
1-7 ネットワーク	IPアドレス/負荷分散/Firewall/リモートアクセス/他システム連携	<p>AWS で割り当て可能なプライベート IP アドレスやパブリック IP アドレス、AWS における負荷分散機能 (ELB) や Firewall 機能 (セキュリティグループ)、AWS 環境へのリモートアクセスや AWS 環境との他システム連携について、詳細を別途「付録」に記載する。</p>
1-8 その他	時刻同期 /DNS/CDN	<p>AWS 環境における時刻同期 (NTP) 設定、外部 DNS (Route 53) / 内部 DNS 機能、CDN サービス (CloudFront) について、詳細を別途「付録」に記載する。</p>
1-9 責任範囲	利用者とサービス提供者の責任範囲	<p>一般的に (AWS に限らず) クラウドサービスを利用する場合は、サービスメニューに提示された内容とその責任範囲に対して、設定されたサービスレベル保証 (SLA) に基づいてサービスを利用することとなる。</p> <p>AWS においても、AWS と利用者における責任範囲について、事前に理解を深める必要がある。</p> <p>なお、AWS を利用する際、利用者責任範囲の業務の支援を得るために、認定パートナー (APN コンサルティングパートナー (SI)) を活用することが推奨される。</p>

第2節 可用性／信頼性要件

エンタープライズシステムにおいては、必ずといっても過言ではないぐらい、高い可用性と信頼性が要求されることになる。ここでは、AWS サービスにおける SLA、レイヤーごとの可用性、AWS 上システムにおけるバックアップ方式・ディザスタリカバリー方式などについて要件項目を列挙し、その回答を記載する。

項目	要件	回答
2-1 稼働率	AWS サービスの稼働率に基づく SLA	<p>AWS では、いくつかのサービスにおいて、稼働率が保証されている。</p> <p>ペナルティが設定されている EC2/RDS/S3/CloudFront/Route53 の SLA について、詳細を別途「付録」に記載する。</p> <p>ミッションクリティカルシステムやプライムシステムに区分されるようなシステムでは、各サービス単一の SLA では要件を満たせない可能性があるため、個別に耐障害性をより強く意識した構成を検討する必要がある。</p>
2-2 可用性	レイヤーごとの可用性確保のための機能・対策	<p>AWS では、以下のレイヤーごとに可用性を確保するための機能・対策が施されている。</p> <ul style="list-style-type: none"> ・ アプリケーション層 (AMI/Elastic IP/Multi-AZ/Auto-Scaling) ・ データベース層 (RDS/Redshift/DynamoDB/ EC2+DB) ・ ストレージ (EBS/S3/Glacier) ・ ファシリティ(データセンター構成/物理的セキュリティ/防火・湿温度管理/電力設備/回線設備)
2-3 バックアップ方式/範囲	実現方式/対象範囲/データの整合性	<p>AWS 環境における代表的なバックアップの方式として、以下の 4 種類が考えられる。バックアップ取得対象やデータの整合性確保等の要件を鑑み、方式を取捨選択することが重要になる。</p> <ul style="list-style-type: none"> ・ 各種サードパーティー製品と組み合わせた S3/Glacier へのバックアップ ・ StorageGateway 経由での S3 へのバックアップ ・ EBS スナップショット ・ AMI(Amazon Machine Image)によるイメージバックアップ

2-4 ディザスターリ カバリー方式 /範囲	実現方式 /利点/注意点	AWS で実現できるディザスターリカバリーの方式として、以下の4種類が考えられる。ここでは、各方式での実現方式/利点/注意点にフォーカスを当てて、詳細を別途「付録」に記載する。 <ul style="list-style-type: none"> ・ S3/Glacier へのバックアップ+リストア ・ コールドスタンバイ ・ ウォームスタンバイ ・ マルチサイトホットスタンバイ
2-5 ディザスターリ カバリー復旧 目標	RPO/RTO /コスト感	AWS で実現できるディザスターリカバリーの4種類の方式における、RPO(目標復旧地点)・RTO(目標復旧時間)・コスト感について記載する。2-4 で記載した実現方式/利点/注意点に加え、RPO/RTO要件とコストを考慮し、方式を取捨選択することが重要になる。 <ul style="list-style-type: none"> ・ S3/Glacier へのバックアップ+リストア ・ コールドスタンバイ ・ ウォームスタンバイ ・ マルチサイトホットスタンバイ

第3節 性能/拡張性要件

本節では、AWS で提供されるコンピューター、ストレージ、ネットワークの性能/拡張性要件に関する対応について記載する。クラウドコンピューティングでは、オンプレミスと比較してCPU、メモリ等を柔軟に変更できるという特徴がある。設計段階でシステム構成の詳細が決定していなくても、実際の使用状況に合わせてシステム構成の変更を柔軟に行うことができる。

項目	要件	回答
3-1 CPU 性能(仮想コア数)	コア数/増減単位	<p>EC2 は複数のインスタンスタイプが提供されており、それぞれのインスタンスタイプはさまざまな CPU、メモリ、ストレージ、ネットワークキャパシティの組み合わせによって構成されている。</p> <p>東京リージョンでは 1 仮想コア～32 仮想コア のインスタンスタイプが提供されている。</p> <p>仮想コア数の変更はインスタンスタイプを変更することで可能である。インスタンスタイプを変更するにはシステムの停止が必要である。</p> <p>※ 1 ECU は、1.0-1.2 GHz 2007 Opteron または 2007 Xeon プロセッサの CPU 能力と同等の能力を提供する。</p>
3-2 メモリ量	メモリサイズ/増減単位	<p>CPU 性能と同じく、EC2 で複数提供されているインスタンスタイプはさまざまなメモリサイズで構成されている。</p> <p>東京リージョンでは 0.613～244GiB のインスタンスタイプが提供されている。</p> <p>メモリサイズの変更はインスタンスタイプを変更することで可能である。インスタンスタイプを変更するにはシステムの停止が必要となる。</p>

<p>3-3 ディスク量/性能</p>	<p>ディスクサイズ /増減単位 /IOPS</p>	<p>EC2 に直接アタッチ可能なブロックストレージとして以下の 2 つのストレージが提供されている。</p> <p>▼インスタンスストア</p> <p>EC2 インスタンスで使用するための一時ストレージを提供する。ほとんどのインスタンスタイプには、このインスタンスストアボリュームが標準で付属している。インスタンスストアボリュームのサイズは最大 48 TB までで、インスタンスタイプによって異なるが、基本的には大きなインスタンスタイプほどサイズが大きくなる。また中には高性能な SSD を搭載したタイプもある。特徴としてはインスタンスを停止／起動するとインスタンスストアボリュームに保存されていたデータは消失する。またデタッチして他のインスタンスに再アタッチすることはできない。そのため、一時的なデータの保存に適している。</p> <p>▼EBS</p> <p>EC2 のインスタンス存続期間とは無関係に永続的に使用可能である。1GB～1 TB のストレージボリュームを作成して、EC2 インスタンスにデバイスとしてアタッチすることができる。複数の EBS ボリュームを同じインスタンスにアタッチすることが可能である。</p> <p>また EBS ボリュームは、General Purpose ボリューム、Provisioned IOPS ボリューム、Magnetic ボリュームの 3 種類から選択可能である。General Purpose ボリュームは、最大 3,000IOPS までバーストが可能なボリュームである(最低 3 IOPS/GB の性能が保証される)。Provisioned IOPS ボリュームは、ボリューム作成時に IOPS レートを指定でき、ボリュームの存続期間中はそのレートに従って IOPS 性能がプロビジョニングされる。</p>
<p>3-4 ネットワーク帯域/速度</p>	<p>帯域</p>	<p>AWS のサービス内でのネットワーク帯域は保証されていないが、クラスター内の全インスタンス間において高帯域で低レイテンシーのネットワークで構成されたクラスタープレースメントグループが提供されている。クラスタープレースメントグループに登録されたインスタンスは、クラスター内の全インスタンス間において高帯域(10Gbps)で低レイテンシーのネットワークを提供する論理クラスターに配置される。クラスターネットワークは、特に並列プログラミングに標準的な MPI ライブラリーを使用する、高性能分析システム、多くの科学および工学応用に適している。</p>

本書 1～2 ページの利用許諾契約書にご同意を頂けない場合、部分利用か又は全部利用かを問わず、本書を利用することはできません。

3-5 ネットワーク機器の持ち込み /ネットワーク 利用	ネットワーク機器の持ち込み /ネットワーク 利用	AWS へネットワーク機器等を持ち込むことはできない。 ネットワークに関してはユーザーネットワークと専用線で接続する Direct Connect というサービスがある。Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができる。これにより、ネットワークのコストを削減し、帯域幅のスループットを向上させることが可能となる。
---------------------------------------	--------------------------------	--

第4節 セキュリティ要件

本節では、AWS で提供されるコンピューター、ストレージ、ネットワークのセキュリティ要件に関する対応について記載する。パブリッククラウドの利用を検討する場合においても、必ずセキュリティの確保が課題となる。AWS ではAWS の定義する責任分担モデルのもと、以下の対応が行われている。利用者責任範囲の OS、アプリケーション、OS ファイアウォールは従来通りの方式にて利用者側での対応となる。また、AWS のセキュリティグループ、ネットワーク設定、アカウント管理に関しては、AWS から提供される機能を利用者側で設定することにより対応することになる。

項目	要件	回答
4-1 ユーザー認証 /利用制限 [IaaS/PaaS]	認証方式、アクセス制限	<p>IAM を使用すると AWS サービスおよびリソースへのアクセスをコントロールすることが可能である。</p> <p>IAM を使用すると、AWS のユーザーとグループを作成および管理し、権限を使用して AWS リソースへのアクセスを許可および拒否することが可能である。</p> <p>また、AWS ウェブサイトにサインインする際に多要素認証デバイス (MFA デバイス) による認証を行うことも可能である。</p> <p>その他、OS レベル、アプリケーションレベルの認証については、従来通りの方式が利用可能である。</p>
4-2 データセキュリティ/完全性	データ暗号化方式(伝送データ)	ELB は標準で証明書管理機能を持っており、SSL の利用が可能である。
	データ暗号化方式(蓄積データ)	<p>EBS ボリュームおよびそれに関連づけられたスナップショットを暗号化する仕組みが提供されている。</p> <p>S3 については、サーバー側の暗号化 (SSE)、または S3 に格納する前に独自の暗号化ライブラリを使用してデータを暗号化することが可能である。</p>

4-3 ネットワーク領域の保護/分離	ネットワーク制御方式	VPCを使用して、AWSクラウド環境の論理的に分離したセクションをプロビジョニングし、ユーザーが定義する仮想ネットワークで AWS リソースを起動することができる。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ユーザーが設定することが可能である。
	ファイアウォール機能	<p>ファイアウォール機能として以下の 2 つの機能が提供されている。</p> <p>▼セキュリティグループ</p> <p>EC2、RDS、ElastiCache のファイアウォールとして動作し、インバウンドトラフィックとアウトバウンドトラフィックの両方をインスタンスレベルでコントロールする。</p> <p>▼ネットワークアクセスコントロールリスト(ネットワーク ACL)</p> <p>ネットワーク ACL はそれに関連付けられたサブネットのファイアウォールとして動作し、インバウンドトラフィックとアウトバウンドトラフィックの両方をサブネットレベルでコントロールする。</p>
	ネットワーク領域の保護	ネットワーク領域の保護の方法として、VPN 接続と Direct Connect による接続の 2 種類の方法がある。
4-4 侵入検知/不正検知	IDS/IPS/WAF の設置等	標準では提供されていないが、OSS、サード パーティ製品等を使用して個別に構築することが可能である。
	ログの取得/保管/保護の範囲/内容	<p>CloudTrail を使用すると Management Console、AWS Command Line Interface の AWS API に対するコールを記録することが可能である (ただし執筆時点では東京リージョン未対応)。特定のユーザーがある期間に行った操作、特定のリソースに対してどの AWS ユーザーが操作を実行したか、ある操作に対してどの IP アドレスから行われたかを確認することが可能である。</p> <p>また、OS、ミドルウェア、アプリケーション等の監査ログについては従来通り個別に取得することができる。</p>

4-5 ネットワークセキュリティ	DoS/DDoS 攻撃対策	インフラに対する分散サービス妨害 (DDoS) 攻撃への対応として標準的な緩和策は導入されている。DoS/DDoS 攻撃の対応をユーザー側で行うことも可能である。
	介入者 (MITM) 攻撃対策	すべての AWS API は、サーバー認証による SSL で保護されたエンドポイント経由で利用可能である。
	IP スプーフィング対策	EC2 インスタンスは、なりすましを受けたネットワークトラフィックを送信できない。
	ポートスキャン対策	EC2 の顧客による許可のないポートスキャンは、AWS のポリシーで禁止されている。AWS に事前申請することにより、ユーザー自身のインスタンスに対してポートスキャンを実施することが可能である。
	第三者によるパケットスニフing対策	無差別モード (プロミスクラス・モード) で実行中の仮想インスタンスが、異なる仮想インスタンス向けトラフィックの受信や、「傍受」することは不可能である。
4-6 ウイルス/マルウェア対策	ウイルス/マルウェア対策	標準では提供されていないが、OSS、サード パーティ製品等を使用して個別に構築することが可能である。
4-7 物理環境の占有		EC2 の「ハードウェア占有インスタンス (Amazon EC2 Dedicated Instance)」が利用可能である。

4-8 データセンターのセキュリティ	物理的セキュリティ	ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入り口とその周辺両方において、物理的アクセスを厳密に管理している。全ての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行う。
	電力	AWS のデータセンターの電力システムは、完全に冗長性を持ち、運用に影響を与えることなく管理が可能となっている。電力障害時には無停電電源装置(UPS)がバックアップ電力を供給する。データセンターは、発電機を使用して施設全体のバックアップ電力を供給する。
	データセンターの可用性	各アベイラビリティゾーンは、一般的な都市地域内で物理的に分離されており、洪水の影響が及ばないような場所にある(洪水地域の分類はリージョンによって異なる)。ユーザーは複数のアベイラビリティゾーンにアプリケーションを配信することによって、自然災害やシステム障害など、ほとんどの障害に対して、その可用性を保つことができる。
	ストレージデバイスの廃棄	AWSではストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスを実行している。DoD 5220.22-M(米国国防省方式)またはNIST 800-88(媒体サニタイズに関するガイドライン)に従ったプロセスが存在する。
	データの保存場所	リージョン間のデータのレプリケートはユーザーが能動的に実行しない限り行われず。利用可能な地理的司法管轄域内のリージョンをユーザーが選択することによって、欧州データプライバシー指令のような、地域に依存する個人情報およびコンプライアンス要件に適合する堅牢な環境が提供される。 リージョン間の通信はパブリックなインターネットインフラストラクチャを介して行われる。重要なデータをリージョン間で送受信する場合は、ユーザーが適切な暗号化手段を使用して保護することが必要となる。

第5節 運用要件

ユーザー企業やシステム規模の大小やシステム用途等を問わず、パブリッククラウド等の外部サービスを利用する場合は、運用要件を把握することも重要となる。ここでは、AWS サービスにおける運用スケジュールや運用窓口、AWS 上のシステムにおける運用監視・リソース変更やソフトウェア更新/パッチ適用等の運用要件に関わる項目を列挙し、その回答を記載する。

項目	要件	回答
5-1 運用スケジュール	インフラの運用 時間帯	<p>AWS では、グローバルレベルで 24 時間 365 日体制にてサービス提供されており、ミッションクリティカルシステムでも利用することが可能である。</p> <p>※コスト最適化の一環として、平日夜間帯や土日祝日等のシステム利用が見込まれていない、もしくはアクセスが少ないタイミングで、システムリソースを意図的に停止・縮小させることも可能である。</p>
5-2 計画停止スケジュール	実施頻度/期間、事前アナウンス	<p>AWS では、定期的な計画停止作業はない。必要に応じて、不定期でメンテナンス作業は適宜実施される。メンテナンス作業時は、事前に利用者に対して、Web コンソール経由もしくはメールにて通知される。</p> <p>※月間の平均稼働率として 99.95%以上を求められるミッションクリティカルシステムやプライムシステムに区分されるようなシステムでは、メンテナンス作業の影響を受けないようなシステム構成をあらかじめ検討することを推奨する。</p>
5-3 運用窓口	言語、問い合わせ方法/対応時間、回答リードタイム/アーキテクチャ・サポートレベル	<p>AWS における運用サポートサービス(AWS サポート)は、サービスレベル別に以下の 4 種類用意されている。詳細を別途「付録」に記載する。</p> <ul style="list-style-type: none"> ・ ベーシック ・ 開発者 ・ ビジネス ・ エンタープライズ <p>なお、いずれの形態であれ、日本語での問い合わせ対応が可能。</p>

本書 1～2 ページの利用許諾契約書にご同意を頂けない場合、部分利用か又は全部利用かを問わず、本書を利用することはできません。

5-4 運用監視	運用監視の対象/範囲(各レイヤー)/システム(プロセス)/ネットワーク(パケット等)、監視間隔、利用可能な運用監視ツール	AWS では、監視機能を有する CloudWatch というサービスが標準提供される。また、CloudWatch Logs を使用することで OS、アプリケーションやカスタムのログファイルを監視対象にすることができる(執筆時点では東京リージョンは未対応のため対応リージョンにログを保管する等の工夫が必要)。OS 以上のレイヤーの監視要件を満たす必要がある場合は、Zabbix/Hinemos/JP1 などの運用監視ツールを使った監視システムを個別に構築する必要がある。 また、仮想サーバーの負荷分散機能を有する ELB では、Web サーバーのヘルスチェックが可能である。
5-5 リソース変更	仮想サーバー ストレージ、 ネットワーク	AWS では、以下の各種リソースの変更を必要なタイミングで、比較的容易に実施することが可能である。 <ul style="list-style-type: none"> ・ 仮想サーバー(起動・停止、スケールアップ/ダウン、スケールアウト/イン) ・ ストレージ(容量拡張/縮小、IOPS の変更) ・ ネットワーク(セキュリティグループ/ネットワークアクセスコントロールリスト/ルートテーブル、サブネット、インターネットゲートウェイ、DHCP オプションの変更)
5-6 サーバーソフトウェア更新/ ソフトウェア更新/ パッチ適用	ソフトウェア更新/ パッチ適用 の実施方針/ 範囲	AWS で稼働する EC2 上で動作する OS/ミドルウェア/アプリケーションの各種ソフトウェア更新/パッチ適用をリモートで実施することが可能である。

第6節 コンプライアンス要件

エンタープライズ系でのコンプライアンス要件としては、法令遵守、法規制などへの取り組み、災害、パンデミックにおける事業継続性、管理、監督、監査から、企業の社会的責任（CSR）などのコーポレートガバナンスの徹底、リスクとセキュリティについての考慮が挙げられる。これらの対策として、環境面での配慮、各種認証取得、手順の標準化などにおいて、エビデンス（根拠）を確認することが重要と考える。

なお、コンプライアンスに関する解釈や開示できる情報の範囲は、個々の利用者の背景や条件（守秘義務契約等）に応じて異なるため、詳細については AWS APN コンサルティングパートナー各社にご相談願いたい。

項目	要件	回答
6-1 拠点（データセンター）所在地と仕様	クラウドサービス（IaaS、PaaS、SaaS）の稼働拠点（データセンター）	<ul style="list-style-type: none"> 提供拠点（データセンター）が日本国内に立地している リージョン外へのデータ移行などはない
	災害被害に関する立地条件	<ul style="list-style-type: none"> 各アベイラビリティゾーンは、独立した障害ゾーンとして設計し、災害によりサービス停止するような事態に陥らない立地を考慮している 物理的に分離（洪水の影響を考慮）している 電力供給の障害可能性の考慮をしている
	災害被害に関する施設条件	施設条件として地震等の災害により iDC 自身が被害を受けサービスが停止するような事態に陥らないために、通信設備等の二重化などの考慮している。
	電源・空調の障害に関するファシリティ条件	電源・空調設備の障害により、機器等（そのサービス）が停止するような事態に陥らないように電源の二重化など冗長性確保を考慮している。
	不法侵入や妨害破壊行為などに関する物理セキュリティ条件	不法侵入防御、アクセス管理など物理的セキュリティを確保している。
運用体制に関する条件	データセンター・設備の維持・管理作業関係として連絡窓口、定期点検体制などを考慮している。	

6-2 データ所在の把握/特定(国/地域)	<ul style="list-style-type: none"> クラウドサービスが取り扱う企業・機関の機密情報やセンシティブ情報の保持場所についての把握 情報が事前に指定した(国家・地方などの)地域の国内法が及ぶ範囲限定であることについて 	<ul style="list-style-type: none"> 格納データの所在はリージョン指定にて日本国内に限定が可能 データとサーバーを配置する物理的なリージョンは、ユーザーが指定して、ユーザーに通知することなく、ユーザーが選択したリージョンからサービス利用者コンテンツを移動しない。
6-3 法令/業界規制/社内基準/標準化	<ul style="list-style-type: none"> 刑法、著作権法、不正アクセス禁止法、個人情報保護法等各種法令/規制への対応 IPAでのガイドラインで取り上げられている項目について 公的認証機関等のガイドラインまたは認定基準の準拠 	<p>規制、標準、およびベストプラクティスに準拠するように設計、管理されている。</p> <p>各種法令に遵守し、設計上、また運用上の有効性が証明されている第三者の監査人が作成したレポート、証明書および認定書をリクエストすることができる。</p>
個人情報保護法の遵守		インフラストラクチャーに関する箇所は AWS が SOC1, SOC2, PCI DSS 等の複数の第三者認証の取得や監査を実施しているため、セキュリティやプライバシーに関連する各項目について確認が可能であり、インフラストラクチャー上に構築されるアプリケーション部分に関してはパートナー各社のサービスやお客様自身での対応が必要となる。
ISMS(JIS Q 27001 : 2006、ISO/IEC 27001:2005)対応状況		AWS は、ISO 27001 認証、PCI DSS Level 1 Provider の認証を取得している。米国基準としては FedRAMP 認証を取得しており、FISMA Moderate レベルでの運用が可能となっている。
物理ストレージの破棄方法		AWS ではストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスを実行している。DoD 5220.22-M(米国国防省方式)、NIST 800-88(媒体サニタイズに関するガイドライン)に従ったプロセスが存在する。

6-4 監査基準対応	立ち入り検査などの監査対応について 利用者からの要請に応じて、監査対応に必要な各種情報の収集	立ち入り検査はできないが、SOC1 などの監査レポートや認証の提示が可能。 <ul style="list-style-type: none"> ・ インスタンス上に残る各種ログと、サービスが提供するログを収集可能 ・ CloudTrail サービスにより操作履歴の記録が可能 ・ SOC1の認証により、管理体制について第三者による監査が行われたことを証明することができる。
6-5 その他の要件	AWS 公開情報にはない情報	コンプライアンスに関する要件は、リーガルアドバイスに関わるケースバイケースの問題となるが多いためパートナーにご相談ください。
6-6 コンプライアンス情報	コンプライアンス関連文書	AWS コンプライアンスに関する最新の情報に関しては下記を参照。 <ul style="list-style-type: none"> ・ AWS セキュリティセンター, Amazon Web Services, Inc. http://aws.amazon.com/jp/security/ ・ AWS コンプライアンス, Amazon Web Services, Inc. http://aws.amazon.com/jp/compliance/ ・ ホワイトペーパー(リスクとコンプライアンス) 2012年7月, Amazon Web Services, Inc. Risk and Compliance White paper

第7節 ベンダー要件

ベンダー要件とは、企業の競争力・収益力の向上を総合的に捉え、企業価値を増大化するためのコーポレートガバナンス遂行のために必要とされる要件であり、ベンダーが備えるべき要求事項と考える。

項目	要件	回答
7-1 グローバル 対応/標準 化	グローバルな拠点で均一なサービスの利用	<ul style="list-style-type: none"> 全世界共通のコンソールサービスを展開 均一なサービス仕様を提供。基本的なサービスはどのリージョンでも提供
7-2 事業継続	災害発生時、パンデミック発生時の事業継続のための対応手順、体制	サービスを提供するプロセス(運用や体制など)について、プロセス基準書を定義し、障害災害対応手順書や体制を整備し、訓練計画書に沿って、定期的な訓練を実施している。

第5章 移行

既存のシステムを AWS クラウドに移行する場合、新規に AWS クラウドを利用する場合の留意事項に加えて、論理サーバー、データなどの移行を合わせて考慮する必要がある。

実際の AWS クラウド移行では、下記の方法論やシステム特性を考慮しながら移行計画を立てて実際の移行を行うことになる。その際、AWS クラウドでは「リハーサル環境を作り、試験するということが非常に簡単に行える」ことを強調しておきたい。これまでのシステム移行では、物理的なハードウェアの移動を伴うケースが多いことから、「本番環境と全く同じ環境を事前に用意して試験すること」が非常に難しかった。ところが、AWS クラウドでは本番環境と同じ環境を簡単に用意することができ、そこで十分な試験を行い、必要がなくなればそれらを破棄することで以降のコスト発生を抑制することができる。つまり、試験や移行リハーサルが非常にやりやすく、その分既存システムの移行と比べてもリスクを減じることができるといえる（図5-1参照）。

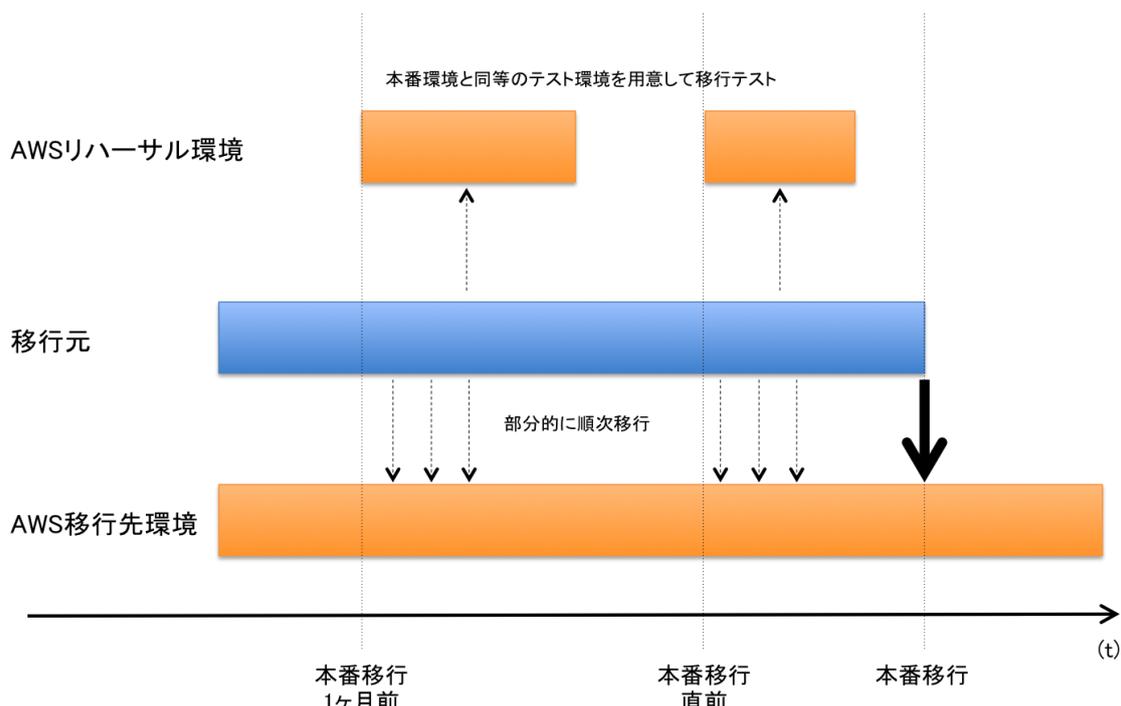


図5-1. 移行リハーサル環境を併用しながらの本番環境への移行

こうした AWS クラウドならではの利点を踏まえ、既存のシステムを AWS クラウドに移行するためのアプローチとその設計手法について概説する。

第 1 節 データ移行

既存の環境から AWS へデータを移行するためには、データの性質などによって様々な方法がある。データの転送自体は既存システムのやり方となんら変わらないためここでは割愛するが、データ移行のパフォーマンスを高めたり、コスト効率をあげる方法について 2 つほどアイデアを提示したい。

〔転送速度の向上〕

EBS ボリュームに対するデータ転送にかかる時間を短縮したい場合、AWS クラウドでは「EBS 最適化インスタンス」を利用することができる。このタイプのインスタンスと、IOPS 速度の保証をつけるオプション(プロビジョンド IOPS)を合わせて使うことで、EBS ボリュームで利用できる帯域幅を確保することができる。

大量のデータを AWS に転送する場合、こうしたオプションを用いることで一時的に帯域を確保しておき、データ転送が終わったらインスタンスタイプを通常のタイプに戻すことで、データ転送にかかる時間を短縮しつつコストを節約するということも可能である。

〔Storage Gateway の利用〕

1TiB を超える大量のデータを AWS クラウドに移行する場合、Storage Gateway を利用するというオプションも検討に加えるべきである。オンプレミスの VMware または HyperV 環境 AWS が提供する仮想マシンをインストールすることで、Storage Gateway が利用できる。Storage Gateway が提供する iSCSI ボリュームにデータをコピーすることで、Storage Gateway が圧縮・暗号化して、データを S3 にコピーしてくれる。iSCSI ボリュームにデータをコピーする部分はオンプレミス-オンプレミス間なので高速にコピーが行われ、かつ Storage Gateway が既存のネットワーク回線を圧迫しないよう、指定されたスケジュールに基づき、指定された帯域幅を使いながらアップロードを実行するので、データ移行用に別な回線を利用しなくても大量のデータを AWS クラウドへ移行することができる(ただし、帯域幅を制限すればその分時間がかかることにも留意されたい)。

Storage Gateway のインストールやセットアップの手間を軽減するために、プリインストールされたアプライアンスがサードパーティーから提供されている。自社に Storage Gateway 環境を構築することが負担になる場合、こうした選択肢も検討されたい。また合わせて WAN 高速化のソフトウェアの利用や AWS Direct Connect といった広帯域な専用線接続の利用も考えられる。

第2節 サーバー移行

サーバーを AWS クラウドに移行する方法は、移行元サーバーの状態（物理マシンか、仮想マシンか）また OS の種類によってやり方が異なるため、一般的には場合分けを行った上で個別に検討することになる。

1. 物理マシンの場合

(1) Windows の場合

一般的に移行元が物理マシンの場合、AWS クラウド上に新規に構築することが前提となる。特に AWS で提供されている Windows のバージョン、bit 数に適合するかを確認しながら移行の実現可能性を考慮する必要がある。

■AWS が準備する Windows AMI (2014 年 10 月現在)

	32bit	64bit
Windows Server 2003	×	×
Windows Server 2003 R2	△(*)	○
Windows Server 2008	△(*)	○
Windows Server 2008 R2	×	○
Windows Server 2012	×	○
Windows Server 2012 R2	×	○

(*) t2.micro, t2.small のみ

(2) Linux の場合

Linux 物理サーバー環境の場合、AWS クラウド上に環境を再構築するアプローチが一般的である。AWS クラウドには、AWS が提供している Red Hat ベースのディストリビューション「Amazon Linux」が存在する。AWS へ Linux 環境を移行する場合によく使われるディストリビューションでもあるので、こうした選択肢も検討されたい。

2. 仮想マシンの場合

(1) Windows の場合

移行元の Windows サーバーが、VMware ESX か VMware Workstation の VMDK イメージ、Citrix Xen の VHD イメージ、Microsoft Hyper-V の VHD イメージのいずれかで、かつ Windows のバージョンが 2003, 2003R2, 2008, 2008R2 の場合、AWS が提供する VM Import という機能を利用することで仮想マシンイメージをそのまま EC2 仮想マシンとして移行することができる。

上記の条件に合致する場合、まずは VM Import によるサーバー移行を検討すべきである。

(2) Linux の場合

移行元の Linux サーバーが下記の条件に合致する場合、VM Import を使って EC2 仮想マシンに移行することができる。

- ① 以降元の仮想マシンが、VMware ESX か VMware Workstation の VMDK イメージ、Citrix Xen の VHD イメージ、Microsoft Hyper-V の VHD イメージのいずれかであること
- ② 以降元 Linux のディストリビューションが Red Hat Enterprise Linux 5.1 - 6.5, CentOS 5.1 - 6.5, Ubuntu 12.04, 12.10, 13.04, 13.10, Debian 6.0.0 - 6.0.8, 7.0.0 - 7.2.0 のいずれかであること (REHL6.0 はサポートされないことに注意されたい)
- ③ 以降元 Linux サーバーのファイルシステムが ext2, ext3, ext4, Btrfs, JFS, もしくは XFS のいずれかであること
- ④ /boot パーティションと / 以下が同じディスク上にあること

また、執筆時点では、移行先の EC2 インスタンスタイプが限定されることにも注意が必要である。

移行計画に際しては、新規に AWS クラウド上に構築する場合のコストと、VM Import を行う場合とのコストとを比較して最適な移行計画を立てることが重要である。

物理・仮想サーバーに関係なく留意すべき事項として、データベースなどプロプライエタリなアプリケーションがインストールされたサーバーを AWS クラウド上に移行する場合は、AWS クラウド上での稼働が許諾されているバージョンであるかを事前に確認しておくことが望ましい。

第3節 ネットワーク移行

(1) 回線

既存システムを AWS クラウドに順次移行する場合、オンプレミスなど既存ネットワークと AWS クラウドとを並行運用する期間が発生する。これまで物理的に 1 カ所だったものを 2 カ所に分散させることになるので、その間のネットワークは VPN (IPsec) もしくは閉域網接続によってセキュリティを確保することが望ましい (図 5-2 の黄色線部)。

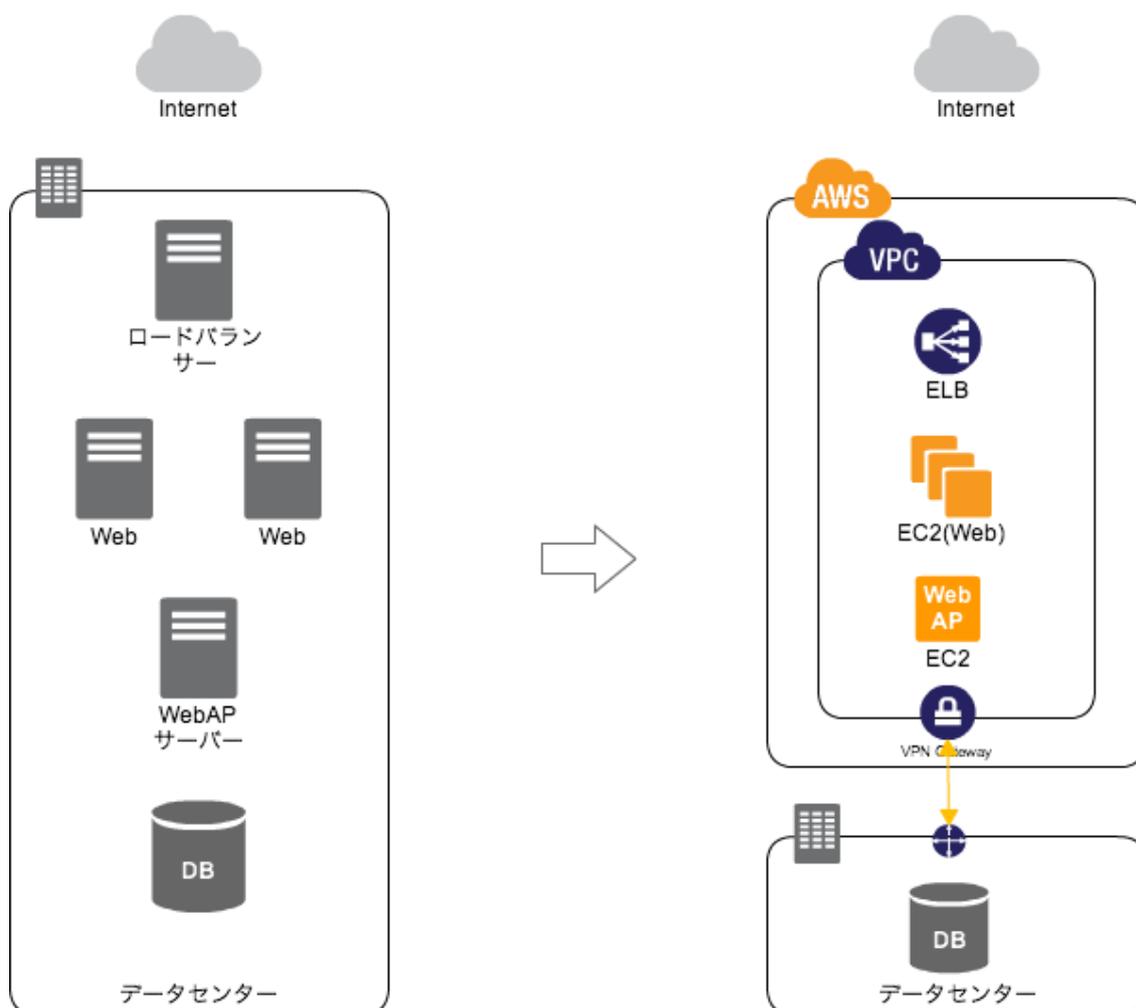


図 5-2. フロント部分を先に AWS 化し、データベース部分を後から移行するケース

一般的に、オンプレミス側ネットワークにおけるインターネットとの出入口のトラフィックはよく監視されており、発生するトラフィックについても把握されているケースが多いが、内部サーバー間のトラフィック（図 5-2 でいうとアプリケーションサーバーとデータベースサーバーのトラフィックなど）については測定されていないケースも散見される。

VPC を用いて並行運用する場合、論理的には 1 つのシステムのままでも、物理的にオンプレミス・AWS クラウドと分散することが想定されるため、結合部分のトラフィックがボトルネックになる可能性が予想される。このため、物理的に分離する箇所については事前にトラフィックを測定しておき、十分なキャパシティをもって設計することが望まれる。

参考までに、B フレッツ（ベストエフォートで最大 100Mbps の回線）と YAMAHA 社ルーターを用いた IPsec による VPC 環境へのトラフィックは、執筆時点で東京 23 区内の環境では平均的に 30～50Mbps 程度のスピードが出ているようである。当然ベストエフォ

本書 1～2 ページの利用許諾契約書にご同意を頂けない場合、部分利用か又は全部利用かを問わず、本書を利用することはできません。

ト回線であることから、この回線速度は約束される性質のものではない。システムの性質や流れるデータ量、移行にかけられるコストなどを総合的に勘案して適切なメディアを選択すべきである。

もし、並行運用のために十分なトラフィック、もしくは安定的にスピードが求められる場合は、**Direct Connect** を検討すべきである。これは、AWS が指定する **POI(Point of Interface)**まで専用線を引き込むことで、AWS クラウドまで専用線で接続することができるというものである。

AWS と直接 **Direct Connect** の契約をする場合、執筆時点では **1Gbps** か **10Gbps** という選択肢しか存在しないが、**Direct Connect** のサービスをより使いやすいものに仲介するサードパーティーが複数社存在している。こうした事業者は、**10Mbps** から **Direct Connect** を契約できるようにしていたり、事業者のネットワークまで **IP-VPN** など（専用線以外の）安価なサービスで AWS クラウドへ閉域網接続できるサービスを提供している。システムの性質やかけられるコストによっては、こうしたサービスも検討に加えるべきである。

(2) トポロジー

エンタープライズシステムを AWS クラウドに移行する場合、**VPC** と呼ばれる仮想ネットワークの機能を使う場合が大半を占めると考えられる。**VPC** によって仮想のネットワークングが実現でき、既存システムと同等のトポロジーを展開することができるが、以下の特性を踏まえて設計することが望まれる。

① ゾーン理解とサブネットの設計

AWS クラウド上にシステムを移行する場合、可用性を考慮して **Multi-AZ** と呼ばれる「複数アベイラビリティゾーンにまたがって仮想サーバーを配置する」構成をとることが一般的である。この場合、アベイラビリティゾーン毎に別なサブネットが必要となるため、その点を考慮してサブネットを設計する必要がある。

② IP アドレスの制限

VPC 内サブネットでは、いくつかのアドレスがシステム用に予約されていて使用できなくなっている。こうした点を踏まえて **IP** アドレスの配置を設計する必要がある。

AWS クラウドを用いることにより、その豊富な機能をコスト効率良く利用できるだけでなく、テストのやりやすさによって移行リスクを減じることができ、移行後もシステム全体の品質向上が期待できるというメリットについても重ねて強調しておきたい。

本書 1～2 ページの利用許諾契約書にご同意を頂けない場合、部分利用か又は全部利用かを問わず、本書を利用することはできません。

第6章 調達

第1節 予算管理

AWSは時間単位での課金となるため、オンプレミス環境と異なる予算管理が必要になる。AWSの費用には、固定分と変動分の費用があるので、固定分と変動分を分けて予算を確保し、変動分については見積もりに対し利用用途によって安全係数をかけておく。

変動費	EC2インスタンス EBS ボリューム EBSスナップショット Elastic IP データ転送量
固定費	ダイレクトコネクト VPC ルータ保守費 回線費用

	EC2 インスタンス	EBSボリ ューム	EBSスナッ プショット	Elastic IP	データ転 送量	システム 単位のコ スト合計
xxxシステム	リ ソ ン ス 単 位 の コ ス ト	システム単位のコスト				¥xxxx
yyyシステム		¥xxxx	¥xxxx	¥xxxx	¥xxxx	¥xxxx
zzzシステム		¥xxxx	¥xxxx	¥xxxx	¥xxxx	¥xxxx
システム共 通		¥xxxx	¥xxxx	¥xxxx	¥xxxx	¥xxxx
合計		¥xxxx	¥xxxx	¥xxxx	¥xxxx	¥xxxx

図6-1. AWSの費用区分の代表例

図6-2. コストイメージ

変動費については、利用用途単位でタグ付けし、利用目的ごとのコストを管理できる仕組み作りを行うことにより、システム単位のコストを把握し予算管理を行うことができる。また、AWSの特徴として、時間単位での課金になるため、検証機、開発機の夜間自動停止、利用者自身で起動する仕組み作りを行うことにより、コストセーブを行うことができる。AWSを活用することにより、費用に柔軟性を持たせることができるが、予算管理においては各部門への配賦が年度単位での調整になるのが現実的といった予算の仕組みが制約となることがある。

第2節 コストモデル

AWSのコストモデルには「オンデマンド」、「リザーブド」、「スポット」の大きく3つのモデルが用意されている。

オンデマンドは1時間ごとに課金される従量課金制であり、リザーブドは、1年もしくは3年単位での契約となり、前払い金を払うことにより、低価格でインスタンスが利用できるサービスである。また、スポットは予備のEC2インスタンスを入札により購入できる仕組みである。

リザーブドインスタンスの種類

種類	特徴	割引率
Light	予約金は小さいが、時間単位の値引きも小さい	1年:42% 3年:56%
Medium	予約金は Light より大きく、時間単位の値引きも Light より大きい	1年:31% 3年:54%
Heavy	予約金は Medium よりも大きく、時間単位の値引きも Medium よりも大きい。 但し、Reserved の間はインスタンスを起動しなくても請求される。	1年:37% 3年:60%

システムの特徴に合わせて、オンデマンド、リザーブドインスタンスを組み合わせる使用することにより、よりコストメリットを受容することができる。

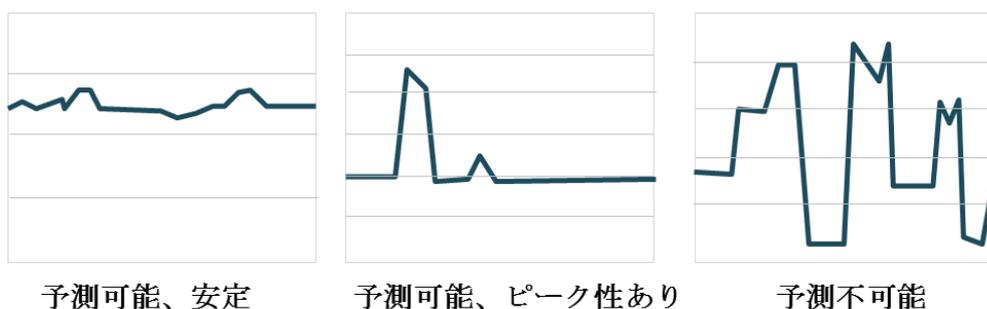


図 6-3

システム利用タイプ	例	インスタンスのタイプ例
予測可能、安定型システムの場合	コーポレートサイト 業務アプリケーション	リザーブドインスタンスを利用
予測可能、ピーク性ありの場合	Web サイト	リザーブドインスタンスとオンデマンド利用
予測不可能の場合	新規ビジネス、ソーシャル系	オンデマンドを利用

第3節 サイジング

第1項 オンプレミスでのサイジングの考え方

エンタープライズシステムにおけるサイジングは、負荷のピークに合わせて行うことが一般的である。

クラウドサービスの利点である柔軟性を生かし、リソースの最適利用によるコスト低減を目指す場合はこの考え方では不十分であり、最大利用状態と、通常状態の最低 2 つの状態

本書 1~2 ページの利用許諾契約書にご同意を頂けない場合、部分利用か又は全部利用かを問わず、本書を利用することはできません。

をサイジングする必要がある。

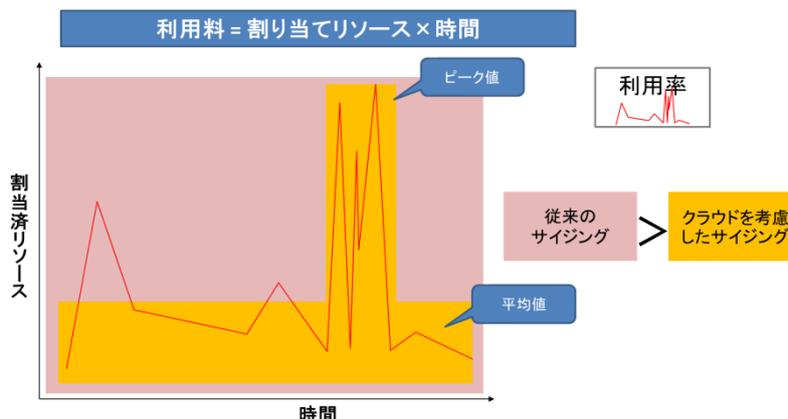


図 6-4

第 2 項 定期的なサイジング

従来のエンタープライズシステムの導入時は、機器を調達する際に機器のスペックを決定する必要があり、調査や関係者間の合意形成に多大な時間と労力を費やしていた。そのためサイジングの見直しタイミングが機器調達時や拠点や複数部門への展開の時等に限られ、結果としてリソースの余剰や不足を招く事態となっていた。

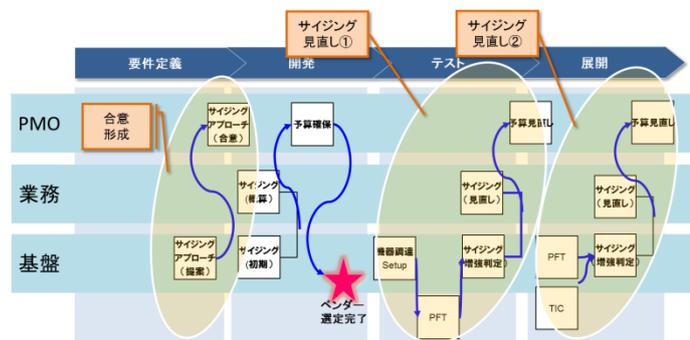


図 6-5

クラウド環境では、テストや展開期間において定期的なサイジングの見直しを行うことで、適切な構成に調整することが可能である。サイジングの振れ幅が小さくなるため、導入初期におけるサイジングの精度をあまり高くする必要がなく、サイジングに対する労力を将来の予測よりも測定と調整のサイクルを多くこなすことに注力する方が得策である。

第4節 見積もり

第1項 企業のITコストにおけるAWS利用料の位置づけ

一般的にITに関する費目は多岐に渡るが、クラウド環境はデータセンター設備、サーバー機器、ソフトウェアライセンス、運用費用等に影響する。アプリケーションレベルのSI費用はクラウド・オンプレミスに関わらず必要であるが、環境構築費用（ハードウェア環境構築やソフトウェアインストール作業）はクラウドサービスに含まれる場合がある。初期コストがかからないことがクラウドサービスの大きな利点であるが、エンタープライズシステムにおいては閉域網による接続など、一定の初期費用が発生する場合があることに留意する必要がある。また、ソフトウェアライセンスについてはクラウドサービスとして利用料を支払う形態と、自社で保有しているライセンスを持ち込む（BYOL）形態が存在する。

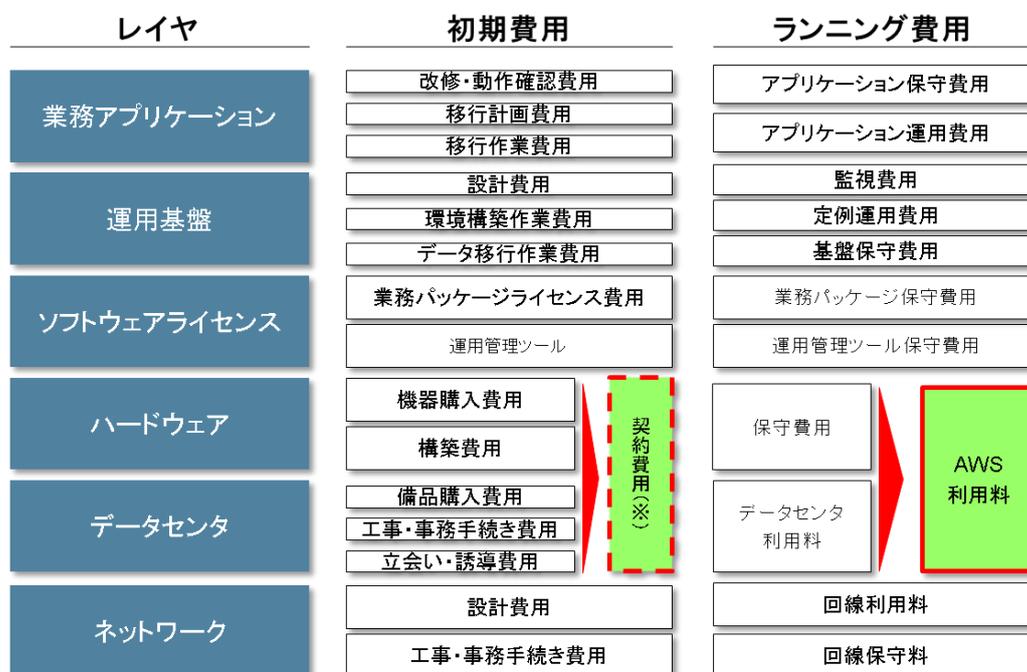


図6-6

第2項 簡易見積ツールと見積もりのポイント

オンプレミス導入では、ハードウェアベンダーに見積もりを依頼する際、構成の複雑さによるものの、回答に1週間以上かかることが多い。AWSでは、Webで簡易見積もりツール(Simple Monthly Calculator)が公開されており、誰でもすぐにコストをシミュレーションすることができる。その為、第1節のコストモデルを考慮した算出を行うことで、将来の予測について条件を変えながら自由にリアルタイムに試算が可能になる。

本書1～2ページの利用許諾契約書にご同意を頂けない場合、部分利用か又は全部利用かを問わず、本書を利用することはできません。

簡易見積もりツール画面の左ペインから使用したい Amazon サービスを選択し、右ペインに利用予定の数量や、使用数・使用率などを入力することで月額費用が自動で算出される。また、見積もり結果は Web 上に保存して置くことができ、いつでも条件を変更してコストを算出し直すことができる。

Amazon AWS SIMPLE MONTHLY CALCULATOR

URL : http://calculator.s3.amazonaws.com/calc5.html?lng=ja_JP

① EC2・S3、VPC 等の利用予定のサービスを選択する。

② サービス毎のタイプや、利用数・利用率など条件に合わせて、入力する。

説明	インスタンス	使用量	タイプ	料金計算オプション	1か月あたりコスト
【本番】Relay S	1	100 使用率/月	Windows, m1.large	3年重度リザーブ	\$ 128.84
【本番】Afaria I	1	100 使用率/月	Windows, m1.large	3年重度リザーブ	\$ 128.84
【本番】Afaria S	2	100 使用率/月	Windows, m1.large	3年重度リザーブ	\$ 257.68
【開発】Relay S	1	25 使用率/月	Windows, m1.small	3年中度リザーブ	\$ 9.15
【開発】Afaria I	1	25 使用率/月	Windows, m1.small	3年中度リザーブ	\$ 9.15
【開発】Afaria S	1	25 使用率/月	Windows, m1.small	3年中度リザーブ	\$ 9.15

図 6-7

見積もりにあたっては、次節で説明する固定費・変動費を意識して算出する必要があるが、固定費として計上する EC2 インスタンス使用料でも、オプションの選択によって、大きく見積額が変わってくるので、注意が必要である。中でも、EC2 では、費用が大きく変動する要素が多いため、代表的な要素を以下に記載する。

要素	説明	選択時の注意点
使用量	月・週・日単位の使用量。単位時間当たりの使用率や使用量(時間)を選択	コストモデルに応じて、使用量・使用率を選択する
タイプ	仮想コア数、メモリ、ストレージ容量がセットになった EC2 仮想サーバーのインスタンスタイプを small、large 等から選択	稼働後に変更することができるため、極端に余分なサイジングは行わない。
料金計算オプション	事前予約の設定。期間は1年、3年から選択が可能。期間を予約することでランニング費用を抑える事ができる。	期間の使用が確実な場合にはリザーブドを選択した方が総コストの抑制になる。ただし、リザーブドを選択した場合、稼働率による調整ができなくなるので注意が必要である。

第5節 契約

第1項 契約上のポイント

AWS 利用に際し、契約上理解すべき重要なポイントは(1)均一なサービス、(2)米国法への対応、(3)支払い方法の制約である。

(1)均一なサービス

AWS は提供するサービス内容を均一化することで高品質と低価格を実現する方針を採っている。そのため IT システムの調達で一般的な相対取引ではなく、同一条件・同一価格による取引となることを理解する必要がある。特に障害が発生した際の損害賠償や優先対応といった個別契約を結ぶことができない。契約者側に、複数リージョンへの分散配置やオンプレミス/別のクラウド環境へのデータ退避といった最悪の事態に対する備えが求められる。

(2)米国法の下での契約

AWS を利用する場合は、サービスの主体である米国人の Amazon Web Services, Inc. との契約となる。このため、契約内容における齟齬あるいは訴訟などにおいては、米国法を準拠法として定めている。従って、AWS に対して契約内容に疑義が生じた場合は、米国ワシントン州キングス郡州裁判所あるいは連邦裁判所での係争となる。このため、米国法での係争にリスクがあると判断する場合において、日本法を準拠法とした契約が必要な場合は、一部の AWS のパートナーとの間で日本法での契約を行うことで、直接的なリスクを回避することができる。

本書 1～2 ページの利用許諾契約書にご同意を頂けない場合、部分利用か又は全部利用かを問わず、本書を利用することはできません。

(3)支払い方法の制約

基本的には AWS の利用料金はクレジットカード決済であるが、以下の 2 つの方法でクレジットカード決済から別の支払い方法へ変更することができる。

1. AWS への口座送金を利用する

利用料金が大きい場合、クレジットカードの与信枠を超えてしまうケースも多いことから、利用料の多い利用者（おおよそ月額 2,000 ドル程度）は AWS から請求書（PDF）を電子送付してもらい、お客様より AWS の口座へ入金できる仕組みがある

この場合は、米ドル決済となり、海外送金となる。

AWS の国内営業窓口に連絡することにより、請求書払いが可能となる。

2. AWS のパートナー経由で AWS を利用する

AWS のパートナーの中には、AWS の運用やサポートと合わせて、AWS の利用料についても一緒に請求処理をしてくれるサービスを提供されているパートナーがいる。

詳しくは日本の AWS パートナー一覧をご覧ください、請求代行サービスを行っているパートナーへ相談する。

第 2 項 契約モデル

クラウドサービスを利用するにあたり、AWS 社との契約モデルは 2 パターン存在する。

- ・ パターン A：利用企業が AWS 社と運用委託先を別々に契約する
- ・ パターン B：運用委託先が AWS 社と契約する。（利用企業は運用委託先とのみ契約する）

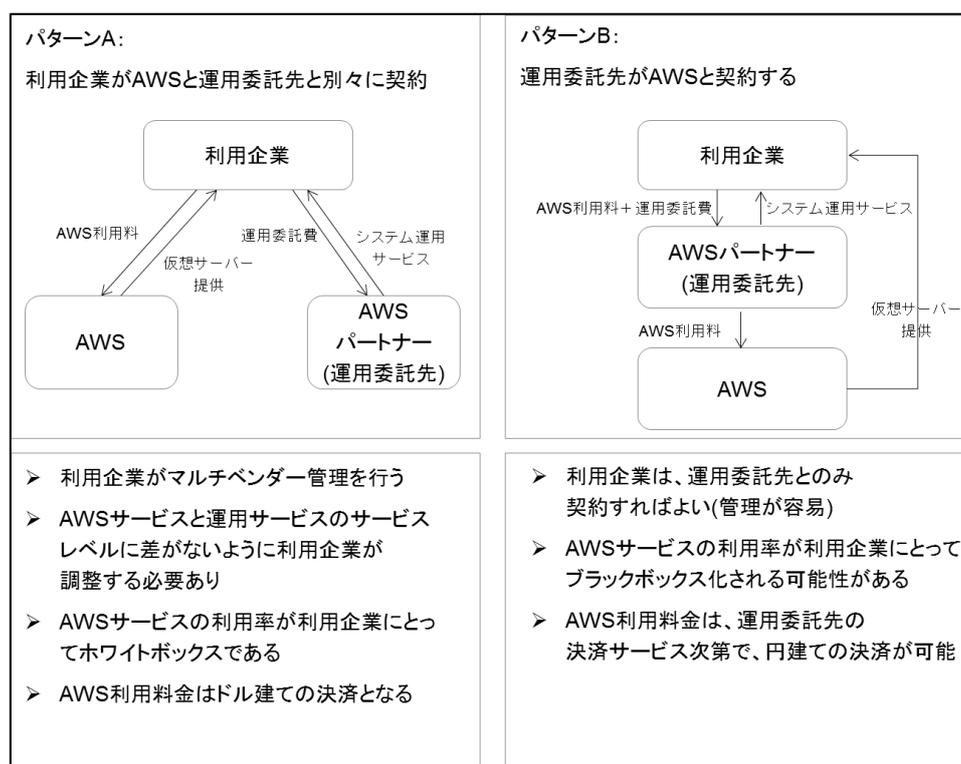


図 6-8

パターン A はより AWS によるメリットを享受することが可能であるが、同時にいくつかのリスクへ利用者に対応する必要がある。これに対しパターン B では AWS パートナー企業との契約の中で、第一項で挙げたリスクをヘッジすることも可能であり、自社の IT や法務部門の体制に合った契約モデルを選択することが重要である。

第 3 項 SLA

AWS はサービスごとに SLA を規定しており、例えば EC2 の場合、あるリージョンにおいて可用性が「99.95%以上で使用できるようにするため商業的に合理的な努力をする」方針を採っており（「サービスコミットメント」）、独自の仮想技術、徹底した運用の自動化、サービスの均等化によりこれを実現している。

この方針に従い、SLA を満たさなかった場合に将来の支払に充当可能な「サービスクレジット」を利用者が受け取ることができる。

以下に AWS が提供する代表的なサービスの SLA とサービスクレジットを記載する。

月間使用可能時間割合	サービスクレジット率		
	EC2	RDS	S3
99.0%以上 99.95%未満	10%	10%	-
99% 以上 99.9% 未満	-	-	10%
99.0%未満	30%	25%	25%

Route 53 の使用可能時間割合が 100%でなかった期間	サービスクレジット付与
5～30 分	1 日分
31 分～4 時間	7 日分
4 時間以上	30 日分

図 6-9. 主なサービスのサービスコミットメントとサービスクレジット

このように SLA の観点からも AWS は信頼のおけるサービスであるということ是可以する。しかしながらここでも「サービス内容を均一化することで高品質と低価格を実現する」という AWS の方針に注意が必要である。具体的には個々の利用企業のサービス復旧に対する個別対応を AWS 社と結ぶことはできず、システム全体の復旧は利用者側が最終的な責任を持つ必要があるという点である。

インフラ保守を内製化せず、ベンダーに任せる方針のもと AWS を運用する場合は、適切な AWS パートナーを選定することが重要となる。各サービスの SLA を適切に理解し、複数のサービスを適切に組み合わせることで可用性、耐用性の高いシステムを構築することが必要である。

終わりに

クラウドサービスの登場により、調達・資産管理業務の軽減や迅速なシステム提供といった面から、IT 部門やユーザーがより多くの時間を IT の活用検討に割くことができるようになることが予想され、90 年代のダウンサイジングや 2000 年代のオープン化以上のインパクトを持つと考えられる。また、2012 年の SAP 社による認定や 2013 年の AWS Summit における先進企業の活用事例等、急速にエンタープライズシステムの AWS 利用環境が整えられて来ており、導入のハードルは確実に低くなって来ている。

一方で、本書で述べた通り、適切なサービスレベルやデータのセキュリティの確保、コンプライアンス対応等、エンタープライズシステムをクラウドサービス上で運用する上で重要なポイントが多数存在する。

本書を作成するにあたり、AWS のパートナーである 6 社が一堂に集まり、数か月に亘り多くのディスカッションを重ねた。その中でも、ユーザーが持っている不安を解消するためにクラウドについて正しく伝えることを心がけた。

本書がユーザー企業によるエンタープライズシステムにおけるクラウドサービス導入の一助となれば幸いである。

2014年12月

エンタープライズ AWS 導入ガイド製作者一同

エンタープライズ AWS 導入ガイド制作委員(以下 50 音順)

- ・ アクセンチュア株式会社(表紙、第 3 章担当)
- ・ アビームコンサルティング株式会社(第 1 章第 4 節、2 章、6 章担当)
- ・ 伊藤忠テクノソリューションズ株式会社(第 4 章第 1 節、2 節、5 節担当)
- ・ 株式会社サーバーワークス(第 1 章第 1 節、2 節、3 節、5 節、第 5 章担当)
- ・ 日本ユニシス株式会社(第 4 章第 6 節、7 節担当)
- ・ 株式会社 日立製作所(第 4 章第 3 節、4 節担当)

本書で使用されている登録商標または商標を以下に列挙いたします。ただしここに含まれないものも特定の法人または個人の登録商標または商標である可能性があります。

- Linux は、Linus Torvalds 氏の日本およびその他の国における登録商標または商標です。
- Red Hat および Red Hat Enterprise Linux は、米国またはその他の国における Red Hat, Inc. の登録商標です。
- Microsoft は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。
- Oracle は、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における商標または登録商標です。
- Zabbix はラトビア共和国にある Zabbix SIA の商標です。
- Hinemos は、株式会社 NTT データの登録商標です。
- JP1 は、株式会社日立製作所の日本における商品名称(商標または登録商標)です。
- Opteron は Advanced Micro Devices, Inc. の商標です。
- Xeon はアメリカ合衆国および / またはその他の国における Intel Corporation の商標です。
- Amazon Web Services、AWS、Amazon EC2、Amazon EBS、Amazon S3、Amazon VPC、AWS Direct Connect、Auto Scaling、Amazon Glacier、AWS Storage Gateway、Amazon RDS、Amazon ELB、Amazon Route53、Amazon Dynamo DB、Amazon Redshift、Amazon CloudFront、Amazon ElastiCache、AWS IAM、AWS Management Console、Amazon CloudWatch、Amazon CloudTrail、AWS SDK は、米国その他の諸国における、Amazon.com, Inc. またはその関連会社の商標です。

本書で引用されている文章、画像、図表等の出典と著作権の説明を以下に列挙いたします。

- 表紙の画像はアクセンチュア株式会社が Fotolia.com より許諾を受け使用しています。画像の著作権は bigfoot - Fotolio.com に帰属します。