National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-146

クラウドコンピューティングの概要と推奨事項

米国国立標準技術研究所による推奨

Lee Badger
Tim Grance
Robert Patt-Corner
Jeff Voas

NIST Special Publication 800-146

クラウドコンピューティングの概要と推奨事項

米国国立標準技術研究所による推奨

Lee Badger
Tim Grance
Robert Patt-Corner
Jeff Voas

コンピュータセキュリティ

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

2012 年 5 月

米国商務省　長官

John Bryson

米国国立標準技術研究所 標準技術担当次官兼所長

Patrick D. Gallagher

コンピュータシステムの技術に関する報告書

米国国立標準技術研究所 (NIST: National Institute of Standards and Technology、以下、NIST と称す)の情報技術ラボラトリ (ITL: Information Technology Laboratory、以下、ITL と称す)は、国家の測定および標準に関する基盤において技術的リーダーシップを提供することにより、米国の経済と公共福祉に貢献している。ITL は、テストの開発、テスト技法の開発、参照データの作成、概念実証の実施および技術的分析を通じて、情報技術の開発と生産的利用の発展に努めている。ITL の責務には、連邦政府のコンピュータシステムにおいて、機密ではないものの機微な情報に対する費用対効果の高いセキュリティとプライバシーを実現するための、技術面、物理面、管理面および運用面での標準およびガイドラインを策定することが含まれる。本 Special Publication 800 シリーズでは、コンピュータセキュリティに関する ITL の調査、ガイダンスおよびアウトリーチの努力、ならびに業界団体、政府機関および学術機関との共同活動について報告する。

NIST Special Publication 800-146、81 頁
(2012 年 5 月)

この文書中で特定される商業的組織、装置、資料は、実験的な手順または概念を適切に説明するためのものである。したがって、NIST による推薦または保証を意味するものではなく、これら組織、資料、または装置が、その目的に関して得られる最善のものであると意味しているわけでもない。

謝辞

本文書の著者である Lee Badger (NIST)、Timothy Grance (NIST)、Robert Patt-Corner (Global Tech, Inc)、および Jeff Voas (NIST)は、本文書のドラフトをレビューし、技術的な内容に寄与してくださった方々に感謝の意を表する。また、コメントを寄せてくださった個人および団体にも深く感謝する。彼らのコメントによって、本文書の全体的な質が高められた。

商標について

目次

図

表

付録

Executive Summary

クラウドコンピューティングにより、コンピュータユーザは十分な機能を有するアプリケーション、ソフトウェアの開発・実装環境、ならびにネットワーク経由でアクセスできるデータストレージおよび処理能力などに対する利用権を使い勝手よくレンタルすることができる。

本文書は NIST によるクラウドコンピューティングの定義をレビューし、クラウドコンピューティングがもたらすメリットと未解決の問題を記述し、クラウドテクノロジーの主な分類の概要を示し、クラウドコンピューティングがもたらす相対的な機会とリスクを組織がどう捉えるべきかについてのガイドラインと推奨を示すものである。クラウドコンピューティングに関しては、これまでにも数多くの解説書が出されてきた。しかしながら、クラウドコンピューティングを一般的な用語で表そうとする試みは、問題をはらんできた。なぜならば、クラウドコンピューティングは単一の種類のシステムではなく、クラウドコンピューティングを支える技術、可能な構成、サービスモデル、および実装モデルまで、その各々について広がりを持つからである。本文書ではクラウドシステムについて説明し、その長所と短所について論じている。

組織にとって適切な技術および構成は、その組織の要件によって変わってくる。クラウドシステムの広がりの中で、組織がそのニーズに最も適したものを把握するには、クラウドをどのように実装できるか（実装モデル）、どのようなサービスが顧客に提供されるか（サービスモデル）、クラウドサービスの利用がもたらす経済的な機会とリスク（経済的考察）、パフォーマンスや信頼性など、クラウドサービスの技術特性（運用面での特性）、一般的なサービス条項（SLA（サービスレベル契約））、およびセキュリティ面での機会とリスク（セキュリティ）を考慮しなければならない。

実装モデル。クラウドコンピューティングシステムは、プライベートに実装、つまり、クラウド利用者の施設内にホストされたり、信頼のおける限られた数のパートナー間で共有されたり、第三者によってホストされたり、あるいは一般からアクセス可能なサービス（すなわち、パブリッククラウド）であったりする。実装の種類によっては、クラウドが利用できるコンピューティングリソースが、限られたプライベートリソースであったり、リモートでアクセス可能な大量のリソースであったりする。また、リソースの規模、コスト、および可用性のコントロール、ならびにリソース自体を利用者がどのようにコントロールできるかについても、異なる実装モデル間でいくつかのトレードオフが存在する。

サービスモデル。クラウドは、電子メールやオフィス生産性向上ツールなどのソフトウェアアプリケーションに対するアクセス(Software as a Service (SaaS)サービスモデル)、利用者が独自のソフトウェアを構築・運用するのに利用できる環境(Platform as a Service (PaaS)サービスモデル)、処理能力およびストレージなどの従来のコンピューティングリソースに対するネットワークアクセス(Infrastructure as a Service (IaaS)サービスモデル)を提供する。それぞれのサービスモデルには、異なる長所があり、どのような利用者や事業目的に適しているかも異なる。一般的に、利用者ワークロードの相互運用性と移行可能性に関しては、IaaS サービスモデルの方が他のモデルよりも実現しやすい。なぜならば、IaaS サービスでは、例えばネットワークプロトコル、CPU の命令セット、レガシーデバイスインターフェースなどの構成要素が、比較的明確に定義されているからである。

経済的考察。外部委託型およびパブリック実装型モデルでは、コンピューティングリソースを都合に合わせてレンタルする機会がクラウドコンピューティングによって提供される。利用者はサービスを利用した分だけサービス料金を支払うことになるが、高い調達費用を初期投資してコンピューティング基盤を構築する必要はない。初期投資が不要となれば、パイロットプロジェクトおよび実験的取り組みに伴うリスクを減らすことができ、組織の柔軟性または敏捷性に対する障壁を削減することができる。外部委託型およびパブリック実装型モデルでは、拡張性（すなわち、利用者がリソースを必要なだけ即座に要求し、受け取り、後に開放できること）もクラウドコンピューティングによってもたらされる。拡張可能なクラウドの利用により、利用者はオー

バープロビジョニング（すなわち、ピーク需要に備えて十分な処理能力を構築したものの、ピーク時以外にはそれだけの処理能力を使わないこと）に起因する過度のコストを回避することができる。組織にとって、クラウドコンピューティングの利用が全体的なコストの削減につながるか否かの判断には、クラウドへの移行にかかる費用（および、必要な場合はクラウドからの移行にかかる費用）を含む、運用、法令順守、およびセキュリティにかかる総コストの慎重な分析が必要となる。

運用面での特性。クラウドコンピューティングは、独立した小さなパーツに分割できるアプリケーションを好む。通常、クラウドシステムはネットワークに依存するため、ネットワーク上のあらゆる制限、例えばデータのインポート／エクスポートにおけるボトルネックやサービスの中断などは、とりわけ、中断に対する耐性がないアプリケーションでは、クラウドの有用性を低下させる。

サービスレベル契約(SLA)を含む、サービス契約。組織は、クラウド利用者とクラウドプロバイダとの間の法律上の関係について規定する、サービス契約のサービス条項を理解する必要がある。組織は、クラウドサービスを利用する前に、利用者側の責任とサービス提供者の責任を理解する必要がある。

セキュリティ。組織は、クラウドコンピューティングに存在するセキュリティ問題と、該当する NIST 刊行物（例：NIST Special Publication (SP) 800-53）について知っておくべきである。複雑なネットワークシステムであるクラウドは、データの機密性、データの完全性、およびシステムの可用性の提供など、従来からのコンピュータおよびネットワークセキュリティ問題の影響を受ける。クラウドでは、一元的な管理の実践を適用することにより、セキュリティアップデートおよびレスポンスに関する問題の一部を改善できる可能性がある。しかしながらクラウドでは、前例のないほどの大量かつ多様な利用者データをクラウドデータセンタに集約する可能性があり、このような脆弱性から、クラウド提供者が利用者データの隔離と保護を維持することに対する高い信頼性と透明性が求められる。一方、クラウドの利用者および管理者は、ウェブブラウザに大きく依存するため、ブラウザのセキュリティ上の欠陥がクラウドのセキュリティ侵害につながる可能性がある。クラウドコンピューティングのプライバシーとセキュリティは、基本的に、利用者が望む堅固なセキュリティ管理策および健全なプライバシーポリシーをクラウドサービス提供者が実装したか、利用者がその実践について目視確認できるか、および当該サービスの管理がどの程度行き届いているかによって決まる。

本質的に、クラウドコンピューティングへの移行はビジネス上の意思決定であり、ビジネス判断では関連要素を考慮しなければならない。対象としては、例えば、既存のアプリケーションがクラウドに実装できるようになっているかどうか、移行にかかる費用とライフサイクル全体を通してかかる費用、既存のインフラストラクチャにおけるサービス指向の成熟度、ならびにその他の要素（セキュリティおよびプライバシー要件など）がある。

1. はじめに

1.1 文書の効力

米国国立標準技術研究所 (NIST: National Institute of Standards and Technology、以下 NIST と称する)は、2002 年施行の連邦情報セキュリティマネジメント法 (FISMA: Federal Information Security Management Act、以下、FISMA と称す)、公法 107-347 に基づくその法的責任を果たすために、この文書を作成した。

NIST は、連邦政府機関のすべての業務および資産に適切な情報セキュリティをもたらすために、最低限の要求事項を含んだ標準およびガイドラインを作成する責務がある。ただし、このような標準およびガイドラインは国家安全保障にかかわるシステムには適用されない。このガイドラインは、行政管理予算局の通達 A-130 (OMB: Office of Management and Budget, Circular A-130)、第 8b(3)項、『政府機関の情報システムの保護 (Securing Agency Information Systems)』の要求事項に一致しており、これは A-130 の付録 IV「重要部門の分析」で分析されているとおりである。 補足情報は、A-130、付録 III に記載されている。

このガイドラインは連邦政府機関が使用する目的で作成されている。政府以外の組織が自由意志で使用することもでき、著作権の制約はないが、出典明記を求む。[1]

本文書における一切は、商務長官が法的権威に基づき連邦政府機関に対して適用と順守を義務づけた標準およびガイドラインを否定するものと解釈してはならない。また、本書に示すガイドラインは、商務長官、行政管理予算局長、または他のすべての連邦政府当局者による既存の公式文書に変更を加えたり、これらに取って代わるものと解釈してはならない。

1.2 目的および適用範囲

本文書の目的は、クラウドコンピューティングの技術領域を分かりやすい言葉で説明し、IT に関する意思決定を行う方々に対する推奨事項を示すことにある。

クラウドコンピューティングは発展途上の領域であり、その長所と短所については十分な調査、文書化およびテストがいまだ行われておらず、結論が得られていない。本文書では、クラウドコンピューティングがいつどのような場合に適切なツールとなるかについて提言し、現時点での知識の限界と、今後分析が必要な領域を示す。

1.3 対象と想定する読者

本文書は、最高情報責任者、情報システム開発者、プロジェクトマネージャ、システム設計者、システムプログラマ、アプリケーションプログラマ、システム・ネットワークアドミニストレータ、情報システムセキュリティ責任者、およびシステムオーナーを含む、企業内のさまざまな情報システム専門家の一助となることを目指している。

1.4 本文書の構成

本文書は以降、次のような主な章で構成する。

■ **第 2 章**では、NIST によるクラウドコンピューティングの定義を示す。

1t著作権に関するこの記述は、SP800−146 の英語の原文のことを言っており、日本語へ翻訳した本書の著作権は、独立行政法人 情報処理推進機構に帰属する。

- **第 3 章** では、クラウドコンピューティングシステムの商用利用の典型的な条件について探る。
- **第 4 章**では、クラウドコンピューティングソリューションの実装方法の分類を示し、それぞれの実装方法の一般的な特徴を記述する。
- **第 5 章**では、SaaS クラウドの仕組みの概要を示す。
- **第 6 章**では、PaaS クラウドの仕組みの概要を示す。
- **第 7 章**では、IaaS クラウドの仕組みの概要を示す。
- **第 8 章**では、未解決の問題を示す。
- **第 9 章**では、推奨事項を示す。

本文書には、補足資料として、付録も付している。

- **付録 A** では、セキュリティ管理策の実装に関する提供者と利用者間の責任の分担を示す。
- **付録 B** では、本文書内で使用されている略語の一覧を示す。
- **付録 C** では、本文書内で使用されている用語の解説を示す。
- **付録 D** では、本文書内で参照される外部情報源の一覧を示す。
- **付録 E** では、本文書内で参照される NIST 刊行物の一覧を示す。

2. クラウドコンピューティングの定義

本文書は、クラウドコンピューティングの特徴を説明するために、NIST SP800-145『NIST によるクラウドコンピューティングの定義』を使用する。読者の便宜上、以下を NIST SP800-145 から抜粋した。

クラウドコンピューティングは、共用の構成可能なコンピューティングリソース（ネットワーク、サーバー、ストレージ、アプリケーション、サービス）の集積に、簡便に、必要に応じて、ネットワーク経由でアクセスすることを可能とするモデルであり、最小限の利用手続きまたはサービスプロバイダとのやりとりで速やかに割当てられ提供されるものである。このクラウドモデルは 5 つの基本的な特徴と 3 つのサービスモデル、および 4 つの実装モデルによって構成される。

基本的な特徴:

オンデマンド・セルフサービス(On-demand self-service)。ユーザは、各サービスの提供者と直接やりとりすることなく、必要に応じ、自動的に、サーバーの稼働時間やネットワークストレージのようなコンピューティング能力を一方的に設定できる。

幅広いネットワークアクセス(Broad network access)。コンピューティング能力は、ネットワークを通じて利用可能で、標準的な仕組みで接続可能であり、そのことにより、様々なシンおよびシッククライアントプラットフォーム（例えばモバイルフォン、タブレット、ラップトップコンピュータ、ワークステーション）からの利用を可能とする。

リソースの共用(Resource pooling)。サービスの提供者のコンピューティングリソースは集積され、複数のユーザにマルチテナントモデルを利用して提供される。様々な物理的・仮想的リソースは、ユーザの需要に応じてダイナミックに割り当てられたり再割り当てされたりする。物理的な所在場所に制約されないという考え方で、ユーザは一般的に、提供されるリソースの正確な所在地を知ったりコントロールしたりできないが、場合によってはより抽象的なレベル（例：国、州、データセンタ）で特定可能である。リソースの例としては、ストレージ、処理能力、メモリ、およびネットワーク帯域が挙げられる。

スピーディな拡張性(Rapid elasticity)。コンピューティング能力は、伸縮自在に、場合によっては自動で割当ておよび提供が可能で、需要に応じて即座にスケールアウト／スケールインできる。ユーザにとっては、多くの場合、割当てのために利用可能な能力は無尽蔵で、いつでもどんな量でも調達可能のように見える。

サービスが計測可能であること(Measured Service)。クラウドシステムは、計測能力 [2]を利用して、サービスの種類（ストレージ、処理能力、帯域、実利用中のユーザアカウント数）に適した管理レベルでリソースの利用をコントロールし最適化する。リソースの利用状況はモニタされ、コントロールされ、報告される。それにより、サービスの利用結果がユーザにもサービス提供者にも明示できる。

サービスモデル:

SaaS（ソフトウェア・アズ・ア・サービス（サービスの形で提供されるソフトウェア））。利用者に提供される機能は、クラウドのインフラストラクチャ [3]上で稼動しているプロバイダ由来のアプリケーションである。アプリケー

[2] 通常、従量課金(pay-per-use)または従量請求(charge-per-use)ベースで計算される。

[3] クラウドのインフラストラクチャは、クラウドコンピューティングの 5 つの基本的な特徴を可能にするためのハードウェアとソフトウェアの集合である。クラウドのインフラストラクチャは、物理レイヤーと抽象レイヤーの両方を含むものと考えられる。物理レイヤーは、提供されるクラウドサービスをサポートするのに必要なハードウェアリソースからなり、通常、サーバー、ストレージ、およびネットワークコンポーネントを含む。抽象レイヤーは、物理レイヤー上に配備されたソフトウェアからなり、クラウドの基本的な特徴を明白に示す部分である。概念上は、抽象レイヤーは物理レイヤーの上に位置する。

ションには、クライアントの様々な装置から、ウェブブラウザのようなシンクライアント型インターフェイス（例えばウェブメール）、またはプログラムインターフェイスのいずれかを通じてアクセスする。ユーザは基盤にあるインフラストラクチャを、ネットワークであれ、サーバーであれ、オペレーティングシステムであれ、ストレージであれ、各アプリケーション機能ですら、管理したりコントロールしたりすることはない。ただし、ユーザに固有のアプリケーションの構成の設定はその例外となろう。

PaaS（プラットフォーム・アズ・ア・サービス（サービスの形で提供されるプラットフォーム））。利用者に提供される機能は、クラウドのインフラストラクチャ上にユーザが開発したまたは購入したアプリケーションを実装することであり、そのアプリケーションはプロバイダがサポートするプログラミング言語やツールを用いて生み出されたものである [4]。ユーザは基盤にあるインフラストラクチャを、ネットワークであれ、サーバーであれ、オペレーティングシステムであれ、ストレージであれ、管理したりコントロールしたりすることはない。一方ユーザは自分が実装したアプリケーションと、場合によってはそのアプリケーションをホストする環境の設定についてコントロール権を持つ。

IaaS（インフラストラクチャ・アズ・ア・サービス（サービスの形で提供されるインフラストラクチャ））。利用者に提供される機能は、演算機能、ストレージ、ネットワークその他の基礎的コンピューティングリソースを配置することであり、そこで、ユーザはオペレーティングシステムやアプリケーションを含む任意のソフトウェアを実装し走らせることができる。ユーザは基盤にあるインフラストラクチャを管理したりコントロールしたりすることはないが、オペレーティングシステム、ストレージ、実装されたアプリケーションに対するコントロール権を持ち、場合によっては特定のネットワークコンポーネント機器（例えばホストファイアウォール）についての限定的なコントロール権を持つ。

実装モデル:

プライベートクラウド (Private cloud)。クラウドのインフラストラクチャは、複数の利用者（例：事業組織）から成る単一の組織の専用使用のために提供される。その所有、管理、および運用は、その組織、第三者、もしくはそれらの組み合わせにより行われ、存在場所としてはその組織の施設内または外部となる。

コミュニティクラウド (Community cloud)。クラウドのインフラストラクチャは共通の関心事（例えば任務、セキュリティの必要、ポリシー、法令順守に関わる考慮事項）を持つ、複数の組織からなる成る特定の利用者の共同体の専用使用のために提供される。その所有、管理、および運用は、共同体内の1つまたは複数の組織、第三者、もしくはそれらの組み合わせにより行われ、存在場所としてはその組織の施設内または外部となる。

パブリッククラウド (Public cloud)。クラウドのインフラストラクチャは広く一般の自由な利用に向けて提供される。その所有、管理、および運用は、企業組織、学術機関、または政府機関、もしくはそれらの組み合わせにより行われ、存在場所としてはそのクラウドプロバイダの施設内となる。

ハイブリッドクラウド (Hybrid cloud)。クラウドのインフラストラクチャは二つ以上の異なるクラウドインフラストラクチャ（プライベート、コミュニティまたはパブリック）の組み合わせである。各クラウドは独立の存在であるが、標準化された、あるいは固有の技術で結合され、データとアプリケーションの移行可能性を実現している（例えばクラウド間のロードバランスのためのクラウドバースト）。

本文書において「クラウド」または「クラウドシステム」という用語がそのまま使用されている箇所については、4つの実装モデルのすべてに当てはまると解釈されるべきである。ある表記が4つのすべての実装モデルに当てはまらない場合は、特定の実装モデルを指定するよう、注意が払われている。

[4] この機能は必ずしも他の供給源からの互換性のあるプログラミング言語、ライブラリ、サービス、およびツールの利用を排除するものではない。

本文書では、さらなる明確化のために、以下の用語を一貫して使用している。

クラウド利用者または利用者：クラウドの利用者である個人または組織。クラウド利用者がクラウドであったり、複数のクラウドが互いにサービスを提供することもあることに留意すること。

クライアント：（おそらく利用者の代わりに）ネットワーク接続を介してクラウドにアクセスするコンピュータまたはソフトウェアアプリケーション。

クラウド提供者または提供者：クラウドサービスを提供する組織。

3. 商取引における典型的なサービス条項

利用者にとってのクラウドのサービス条項は、両者（利用者と提供者）間の法的拘束力のある合意により決定され、多くの場合、(1) サービス契約書、および (2) サービスレベル契約(SLA) 書の二つで構成される。通常、サービス契約書は、利用者と提供者間の法的契約の決め事を明記した法的ドキュメントであり、SLA は技術的パフォーマンスに関する提供者側の約束（契約の不履行に対する補償を含む）を明記した、サービス契約書よりも短いドキュメントである。本文書では、便宜上、これらの 2 つのドキュメントの組み合わせをサービス契約書と称している。[5]

さまざまな種類のサービス契約書が存在する。サービス契約書は、提供される IT サービスが組織の任務目的に適合することを確実にするために、企業の情報システムユニットとその他のユニットの間で内部的に使用される場合がある。サービス契約書は、通常、ある政府機関から別の政府機関に渡るようなサービスの契約には使用されない。その場合、サービス条項の成文化には、(MOU（覚書）や IAA（省庁間の取り決め）が代わりに使用されることが多い。

第 3 章では、商用クラウドの典型的なサービス契約に含まれる項目のうち、クラウド提供者が提供するサービスとセキュリティの質について直接述べているいくつかの項目について説明する。第 2 章で定義されている、クラウドのセルフサービスの要素は、利用者が (1) 提供者の価格設定とサービス条項を受け入れるか、あるいは (2) より受け入れやすいサービス条項を掲げる別の提供者を探すことになることを示唆している。ただし、クラウドリソースを多量に使うことを想定している利用予定者は、より好ましいサービス条項を交渉できる可能性がある。しかし、通常の利用者は、クラウドの価格体系やサービス契約について交渉することはできない。

利用者と提供者間のサービス契約があらかじめ決められた条件のものである場合は、通常、「解約理由に基づく」例えば利用者がクラウドの利用規定に違反した場合とか、利用者が期限内に料金を支払わないことにより、いずれかの当事者によっていつでも終了となりうる。さらに、理由もないのに契約が終了となることもある。利用者は、提供者が掲げる契約終了およびデータ保全方針を分析する必要がある。

クラウド提供者側の保証は、その限度に関する明示的通知とともに、サービス契約書に明記される。クラウド提供者のサービス契約書は、(1) 利用者に対する一連の保証、(2) 利用者に提供されない一連の保証の明記（すなわち、制限条項）、および (3) 利用者が受け入れなければならない一連の義務、という 3 つの部分によって構成される。

3.1 保証

通常、提供者は利用者に対して 4 つの主な保証を提示する。

- **可用性。**通常、クラウド提供者は可用性に対する保証として、稼働率 99.5 ないし 100.0 パーセントを謳っている。これは頼もしい主張ではあるが、これらのパーセンテージがどのように算出されているかについては注意が必要である。多くの場合、パーセンテージは、支払請求単位期間（あるいは 1 年などのより長い期間）内に、設定されたタイムインターバルにわたってサービスが「アップ」していない状態が何回発生したかをもとに算出される。著名なクラウド提供者は、このタイムインターバルを 5 分、15 分、1 時間などに設定している。例えば、あるクラウド提供者がサービスが利用可能であるタイムインターバルを 15 分に設定した場合、仮に 14 分間にわたってサービスが中断したとしても、この測定方法では 100 パーセントの可用性が記録される。通常、「アップ」の定義は、直感的にサービスが反応していることとして

[5] クラウド提供者によっては、従来からサービス契約書を提供しなかったり、大口の利用者または上得意の利用者にのみサービス契約書を提供してたりする。サービス契約書はクラウド提供者側の提供する保証を理解するうえで極めて重要である。

定義されるが、場合によっては、クラウドが利用可能でないと判断される以前に、クラウドのの複数のサブシステムが機能不全に陥っているはずである。また、クラウド提供者は、特定の機能または仮想マシン (VMs)に限定した障害の場合には、可用性の保証を制限することもある。

- **稼動停止に対する補償。**利用者に対して約束した可用性を提供できない場合には、クラウド提供者は将来のクラウドサービス利用に対するサービスクレジットをもって、誠心誠意、利用者に補償すべきである。サービスクレジットはさまざまな方法によって算出できるが、通常は、特定の支払請求単位期間内でサービスが中断した期間の長さによって決まる。通常、サービスクレジットは、ダウンタイムが発生した支払請求単位期間において、利用者が負担する費用の一定の割合を超えないように設定される。提供者によって異なるが、通常は、利用者が負担するその時点の費用の 10 パーセントから 100 パーセントの間に設定されている。通常、サービスクレジットを取得する責任は利用者側にある。その際利用者はサービス中断の種類と中断期間について、タイムリーな情報を提供しなければならない。クラウド提供者がサービスの中断について自発的に利用者に通知するか否かは定かでない。最近調査したクラウド提供者の内、稼動停止に対する払い戻しまたはその他の補償について、(標準化されたサービス契約の中で)謳っている提供者は一つもなかった。パフォーマンスに関する評判がよくないと長期的なビジネス利益も望めないことを、すべてのクラウド提供者が理解すべきである。

- **データの保護。**利用者によるクラウドサービスへのアクセスが「解約理由による」、すなわち、利用者がクラウドの利用規定に違反したり、料金を支払わなかったりした場合には打ち切りとなることがあるが、このような場合にはクラウドストレージに残っている利用者データを保護する義務はないと主張するクラウド提供者が殆どである。さらに、通常、クラウド提供者は、利用者が自発的にクラウドの利用を中止した場合には、その日から数えて 30 日間は利用者のデータを意図的に消去することはないと主張する。クラウド提供者によっては、利用者データのスナップショットのみを保持したり、利用者に対して (1) データを別のクラウド提供者のクラウドにバックアップする、あるいは (2) データをローカルにバックアップすることを推奨している。

- **利用者情報の法的取り扱い。** 通常、クラウド提供者は、法的な要請に応じる場合を除き、利用者のデータを販売、ライセンス供与、または開示しないことを保証している。しかしながら、通常、クラウド提供者は、クラウド上での利用者のアクションをモニタリングする権利を有し、モニタリングを支援するために利用者が使用しているソフトウェアのコピーを要求する場合さえある。

3.2 除外規定

通常、クラウド提供者のポリシーには、5 つの主な除外規定が含まれる。

- **サービスの計画的停止。**クラウド提供者がサービスの計画的な停止をアナウンスする場合には、サービスの停止は稼動停止としてはカウントされない。クラウド提供者によっては、停止が事前にアナウンスされたり、停止時間の長さが示される。

- **不可抗力事象。**通常、クラウド提供者は、自身が現実的にコントロールできない事象に関しては、すべての責任を拒否する。そのような事象には、停電、自然災害、利用者と提供者間のネットワーク接続障害などが含まれる。

- **サービス契約に対する変更。**通常、クラウド提供者は、サービス契約のサービス条項をいつでも変更できる権利と、簡単な事前通知により価格を変更する権利を有する。標準的なサービス契約の変更では、通常、クラウド提供者がウェブサイトに変更内容を掲載することによって通知を行う。そして、クラウド提供者のウェブサイトを定期的に参照してサービス契約に変更がないかを確認するのは、利用者側の責任である。変更は即座に有効になる場合や、数週間後に有効になる場合がある。特定の利用者のアカウントに影響を与える変更の場合、電子メールや宅配サービスによって通知がなされる場合もある。

- **セキュリティ。**通常、クラウド提供者は、セキュリティ、すなわち、利用者データの正規の権限によらない変更または開示、あるいは悪意のある行為によるサービスの中断に関しては責任を負わないと主張する。通常、サービス契約は、セキュリティリスクは利用者が負うことを明白に述べている。場合によってはクラウド提供者が利用者データを保護するために最善を尽くすことを約束することもあるが、今回調査したすべてのクラウド提供者が、データの侵害、データの消失、またはサービスの中断に対するセキュリティ上の責任は負わないとし、約束した可用性を満たせなかった場合の補償をサービスクレジットに限定していることが判明した。さらに、サービスの中断が悪意のある行為によるものなのか、それとも他に要因があるのかを利用者側で判断するのが、どれだけ容易であるかは定かでない。

- **サービス API に対する変更。**通常、クラウド提供者は、サービス API をいつでも変更または削除できる権利を有する。

3.3 義務

通常、利用者は 3 つの主な義務に同意しなければならない。

- **利用規定。**通常、利用者は、児童ポルノなどの違法コンテンツを保存しないこと、ならびに (1) 賭博、(2) スパム送信、(3) セキュリティ攻撃（例：サービス妨害またはハッキング）の実施、(4) スパイウェアの配信、(5) 侵害的なモニタリング、および (6) クラウドシステムインフラストラクチャの破壊を試みることなどの、違法行為を行わないことに同意しなければならない。利用規定は、プロバイダ間で異なる。

- **ソフトウェアライセンス。**すべてのクラウド提供者が、自社のクラウド上で稼働するサードパーティーのソフトウェアに対して、ソフトウェアのライセンス条項を順守することを要求している。場合によっては、クラウド提供者側でそうしたソフトウェアを用意して、ライセンス上の義務が守られるようモニタリングする仕組みを組み込むこともある。

- **タイムリーな支払い。**クラウドサービスの費用は、一般的に、支払請求単位期間内に段階的に課金され、料金は期間末に支払い義務が生じる。通常、支払猶予期間が過ぎても支払いがなされなかった場合には、その利用者に対するサービスが「解約理由による」停止または終了となり、利用者のデータも消失する可能性がある。

3.4 推奨事項

- **用語。** 利用者はサービス契約書内で使用されている用語に細心の注意を払うべきである。一般用語についても、クラウド提供者側で、提供するサービスに特化する形で再定義する可能性がある。

- **補償。**クラウド提供者との間で具体的なサービス契約が交渉されない限り、あらゆる不履行に対する補償は極めて限られる可能性が高い。利用者は自身が被る可能性のある損害に見合った補償が組み入れられることを望むであろう。

- **法令順守。**利用者は、利用者データの規制に関する十分な範囲の法規制について、提供者が順守することが、サービス契約書に明記されているか否かを慎重に確認すべきである。

- **セキュリティ、重要度、およびバックアップ。**利用者は、セキュリティまたは極めて重要な処理に関連する免責条項がサービス契約書に含まれていないかを慎重に確認すべきである。また、クラウドに格納されているデータのクラウド外でのバックアップを提供者が推奨しているかどうかも確認すべきである。

- **交渉によるサービス契約。**デフォルトのサービス契約のサービス条項が利用者のすべてのニーズに対応していない場合には、クラウドの利用を開始する前に、サービス契約書の修正についてクラウド提供者と話し合うべきである。

4. 一般的なクラウド環境

本分書の執筆時点で、既に多くの個人および組織がクラウドコンピューティングとその長所・短所について一般的なコメントを寄せていた。しかしながら、重要なことは、「クラウドコンピューティング」という用語はさまざまなシステムと技術に加えて、サービスモデルと実装モデル、およびビジネスモデルを含むことを理解することである。クラウドコンピューティングについて数多く寄せられるコメントには、例えば「拡張できる」とか「資本支出を減らして運営経費に形を変えることができる」などがあるが、これらは一部の種類のクラウドシステムにしか当てはまらない。本章の目的は、クラウドコンピューティングシステムの 5 つの重要なシナリオへの区分けについて分かりやすく説明し、シナリオごとに、スケーラビリティなどのクラウドコンピューティングに関する一般的な事柄について説明し、それらの事柄がそのシナリオにどのように当てはまるかを示すことにある。[6]

NIST によるクラウドコンピューティングの定義で示されたように、クラウドシステムは顧客（すなわちクラウド利用者）がネットワーク経由でアクセスできるコンピューティングリソースの集積である。一般的に言うと、クラウドシステムとその利用者はクライアントサーバーモデル [Com88] を使用することになる。つまり、利用者（クライアント）がメッセージをネットワーク経由でサーバーコンピュータに送り、サーバーは受け取ったメッセージに応じて作業を行う。

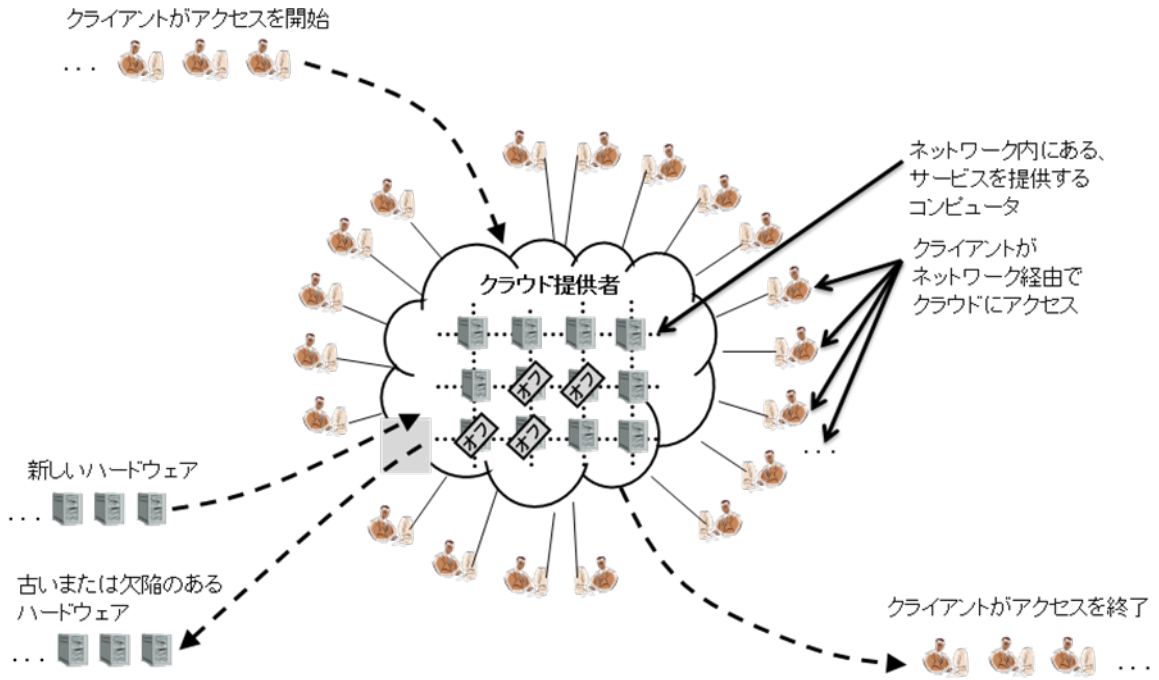

図1: クラウドと利用者との結びつきの一般的な図

クラウドとクライアントとの結びつきを一般的な図で示すと図１のようになる。クラウドのコンピューティングリソースは格子の中のコンピュータシステムによって描写されていて、クライアントはネットワーク接続を介してクラウドにアクセスする。図で示されているように、新規クライアントが参入したり、既存のクライアントが離脱したりするため、クラウドを利用するクライアントの数は常に変動する。同様にクラウドは、コストを最小限

[6] 本章では、クラウドシステムと利用者がどのように結びつくかを物理的ネットワークの視点から示している。クラウドソフトウェアについて、また、従来のソフトウェア「スタック」のどの部分をクラウド利用者が利用できるかについて理解することも重要である。これについては第 5,6、章および第 7 章で説明する。

に抑えつつ最大限のサービスを提供できるよう、自身が管理するハードウェアリソースの集積を維持管理する。また、予想されるコンポーネントの障害や耐用年数の超過を踏まえたうえで可用性の高いサービスを維持するために、必要に応じて新しいハードウェアコンポーネントを組み入れたり、古いまたは欠陥のあるコンポーネントを切り離したりする。さらに、サービスをコスト効率よく提供するために、ハードウェアリソースの集積を調整して、リソース効率の向上を図る。利用者の需要減少期間にクラウド提供者が採用する戦略の一つに、使用されていないコンポーネントの電源をオフにすることがある。電力管理のためであれ、ハードウェアリフレッシュのためであれ、利用者ワークロード（データストレージおよび処理能力）をある物理的コンピュータから他の物理的コンピュータに移行すること[Chr05, Shr10, VMw11, Mic10, Red99]は、利用者に不便を感じさせることなくハードウェアをリフレッシュしたり、ワークロードを整理するうえで重要な戦略となる。

図1から、クラウドコンピューティングに関する一般的なステートメントがいくつか推察される（例：長所と制約、パフォーマンス特性）。クラウドコンピューティングの利用を考えている組織は、以下にリスト化されている一般的なステートメントについて考慮しなければならない。クラウドについて一般的になされる多くのステートメント、例えば「クラウドは非常に大きなワークロード向けに拡張可能である」または「クラウドは資本支出を減らして運営経費に形を変えることができる」は、一部の種類のクラウドにしか当てはまらない。混乱を避けるために、本文書ではそうしたステートメントの各々を、適合するクラウドの種類によって明示的に区別している（すなわち、各ステートメントには「スコープ」がある）。表 1 に、本文書内で使用されているスコープの一覧を示す。

表 1: クラウドについてなされたステートメントに対するスコープ区分

スコープ名	適用範囲
共通 (general)	すべてのクラウド実装モデルに適合する。
オンサイトプライベート (on-site-private)	利用者の施設内に実装されるプライベートクラウドに適合する。
外部委託型プライベート (outsourced-private)	サーバー側がホスティング会社に外部委託されるプライベートクラウドに適合する。
オンサイトコミュニティ (on-site-community)	コミュニティクラウドを構成する利用者の施設内に実装されるコミュニティクラウドに適合する。
外部委託型コミュニティ (outsourced-community)	サーバー側がホスティング会社に外部委託されるコミュニティクラウドに適合する。
パブリック (public)	パブリッククラウドに適合する。

各スコープについては、以下で説明する。以下のステートメントのスコープは「共通 (general)」であり、実装モデルやサービスモデルにかかわらず、すべての種類のクラウドに適合する。

- **ネットワークへの依存性（共通）。** クライアントである利用者は、正常に機能しているセキュアなネットワークを使ってクラウドにアクセスする必要がある。利用者の観点からすれば、ネットワークが信頼できなければ、クラウドも信頼できないだろう。
- **利用者にも IT スキルが求められる（共通）。** サーバーコンピュータの運用はクラウド提供者が行うため、利用者組織の IT スタッフの必要性が減少すると考えられるが、利用者は自身が施設内で管理するクライアントシステムからクラウドにアクセスするため、クライアントシステムの維持管理やセキュリティの確保などが必要になる。

- **ワークロードの所在場所は動的に割り当てられるため、クライアントからは見えない（共通）。** クラウドのハードウェアリソースを効率よく管理するには、クラウド提供者がマシン間の利用者ワークロードの移行をクライアントに不便を感じさせることなく、すなわち、変更に対する追随と適応をクライアントに求めたり、移行をクライアントに意識させることなく行う能力が求められる。[7]

- **マルチテナント（複数利用者による共同利用）に伴うリスク（共通）。** 複数の異なるクライアントのそれぞれのワークロードが同じシステムおよびローカルネットワーク上に同時に存在し、クラウド提供者のソフトウェアが実施するアクセスポリシーによってのみ隔離が行われる場合がある。その実装に、またはプロバイダの運用管理ポリシーおよび手順に欠陥があると、利用者のセキュリティが侵害される恐れがある。

- **データのインポート／エクスポート、およびパフォーマンスの限界（共通）。** 利用者はネットワーク経由でクラウドにアクセスするため、オンデマンドでの大量データのインポート／エクスポートが、データをタイムリーに運ぶネットワークの能力を上回る可能性がある。さらに、リアルタイムな処理または極めて重要な処理は、ネットワークの遅延やその他の制限によって阻害される可能性がある。

クラウドコンピューティングの利用を考えている組織は、これらの一般的なステートメントと、これらのステートメントが組織の任務およびビジネスモデルに及ぼす影響について考慮しなければならない。ただし、一般的なステートメントのみを考慮すれば十分であるわけではない。クラウドは、表 1 にリスト化されているスコープの内、「共通」以外の1つまたは複数のスコープによって表されることもある。クラウドコンピューティングの利用を考えている組織は、利用を考えている種類のクラウドに関する詳細なステートメントについても考慮が必要となる。それぞれの選択肢については、具体的なスコープに焦点を当てて分類された以降の各章にて説明する。[8]

4.1 クラウドのリソースを誰がコントロールするかを理解する

クラウドコンピューティングでは、従来の施設内のコンピューティングとは異なり、利用者が 2 つの重要な能力をクラウド提供者に委譲するという指摘がある。

- **コントロール:**利用者のデータおよびプログラムにアクセスできる人またはモノを高い信頼性を持って決定すること、ならびにデータの削除やネットワークの切断などのアクションを、アクションが実施されたことと、利用者の意図に反する余計なアクションは一切実施されていないこと（例：利用者からのデータオブジェクトの消去依頼が、消去前にこっそりコピーを作成する行為によって阻害されないようにしなければならない）に対する高い信頼性を持って実施すること。

- **可視性:**利用者のデータとプログラムに関して、ステータス、および誰がどのようにアクセスしているかを高い信頼性を持ってモニタリングすること。

しかしながら、利用者がコントロールと可視性をどの程度委譲するかは、物理的所有や、利用者のコンピューティングリソースのアクセス境界防御メカニズムを（高い信頼性を持って）設定する能力を含む、いくつかの因子によって決まる。

本文書では、アクセス境界の概念を用いて異なるクラウド実装モデルを整理し、特徴づけている。図 2 に、境界とコントロールに関連するコンピュータセキュリティの重要な概念である、セキュリティ境界 [TIS94,

[7] ワークロードが移行に先立ち特定期間にわたって特定の場所に存在する場合もあれば（例：第 7 章に記載されている IaaS サービスモデル）、ワークロードが根本的に分散されたエンティティとして存在し、データも地理的に分散されたデータストア内に存在し、利用者向けのシーケンシャルな処理が（場合によっては、複数の異なるサーバー上で）実行される場合もある（例：第 6 章に記載されている PaaS サービスモデル）。

[8] 本文書は、基本的に同じ記述を繰り返さない。ただし、特定の種類のクラウドについては追加の説明が必要な場合がある。このような場合には、共通ステートメントの名称を再び使った上でその種類のクラウドに特化した説明を加えている。

Gas88] を示す。この図に示されているように、セキュリティ境界はアクセスに対するバリア（障壁）である。セキュリティ境界の内側にあるエンティティは、セキュリティ境界の内側にあるリソースを自由にアクセスできる。一方、セキュリティ境界の外側に位置するエンティティは、アクセスに関するポリシーを実施する境界制御装置がアクセスを許可した場合のみ、セキュリティ境界の内側にあるリソースにアクセスできる。セキュリティ境界という用語は、ファイアウォールやネットワークについて論じる際によく使われるが、セキュリティ境界の概念は実際にはより一般的であり、例えば、稼働中のソフトウェアの異なる特権レベル間の境界（例：アプリケーションとオペレーティングシステムとの間）を示すのに使用することができる。セキュリティ境界は、それ自体が十分なセキュリティメカニズムであるわけではないが、境界コントロールはセキュアなシステムを実現するための重要な構成要素である。

典型的な境界制御装置には、ファイアウォール[TIS94, Che94]、ガード[Eps99]、および仮想プライベートネットワーク[Ros99]が含まれる。重要なリソースの周りにセキュリティ境界を実装することで、それらのリソースの利用をコントロールするための手段と、リソースに対するアクセスをモニタリングするための手段が組織に与えられる。[9] さらに、設定変更を通じて、組織がセキュリティ境界を変化するニーズに適応させることも可能である（例：変化するビジネス状況に応じてプロトコルやデータフォーマットをブロックまたは許可する）。NISTによるクラウドの定義に含まれる種々のクラウド実装モデルは、利用者が管理するセキュリティ境界の設置場所と、クラウドに外部委託するリソースに対する利用者側のコントロールレベルに影響を与える。

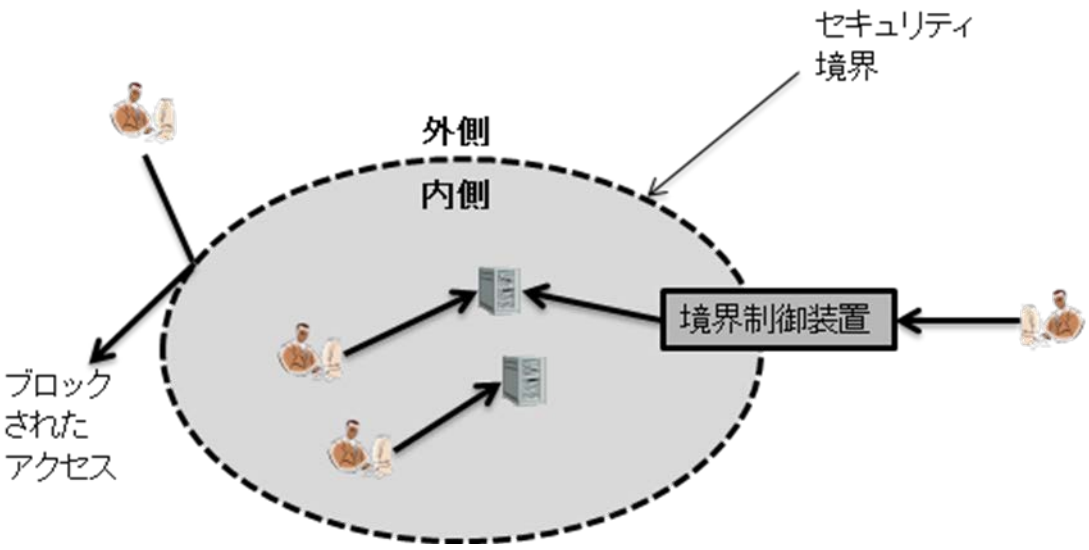

図2: セキュリティ境界

NIST によるクラウドの定義は、プライベート、コミュニティ、パブリック、およびハイブリッドの 4 つの実装モデルを列挙している。プライベートとコミュニティ実装モデルには、それぞれオンサイトと外部委託型の 2 つの異型があり、これらはセキュリティ境界に影響を与えるため個別に論じる必要がある。ハイブリッド実装モデルは異なる実装モデルの組み合わせから成る。したがって、ハイブリッド実装モデルは、すべての構成要素の特徴と、複数のシステムからなるより複雑な統合システムの特徴を有する場合がある。

[9] コンピューティングリソースに自由にアクセスできるパスが存在する場合、セキュリティ境界の効果が弱まるか、あるいは、まったく存在しない状態に陥ることすらある。例えば、広範囲なワイヤレス通信は、外部エンティティと内部エンティティとの間に境界制御装置を確実に設置するすべがないため、セキュリティ境界にとって脅威となる。同様に、モバイルデバイスを使用して組織のセキュリティ境界内に接続できるようにしている組織も多いが、移動中などは直に脅威に晒される場合がある。

4.2 オンサイトプライベートクラウドのシナリオ

オンサイトプライベートクラウドを簡単な図で示すと図 3 のようになる。この図が示すように、セキュリティ境界は利用者のオンサイトリソースとプライベートクラウドのリソースの周りに広がる。プライベートクラウドは、単一の利用者の施設に集約される場合もあれば、複数の利用者の施設に分散される場合もある。セキュリティ境界は、利用者側で実装しない限り存在しない。セキュリティ境界が実装されていることで、プライベートクラウドのリソースに対するコントロール権が保障されるわけではないが、オンサイトプライベートクラウドに組み込まれたリソースについては、コントロールを行使する機会が利用者にもたらされる。

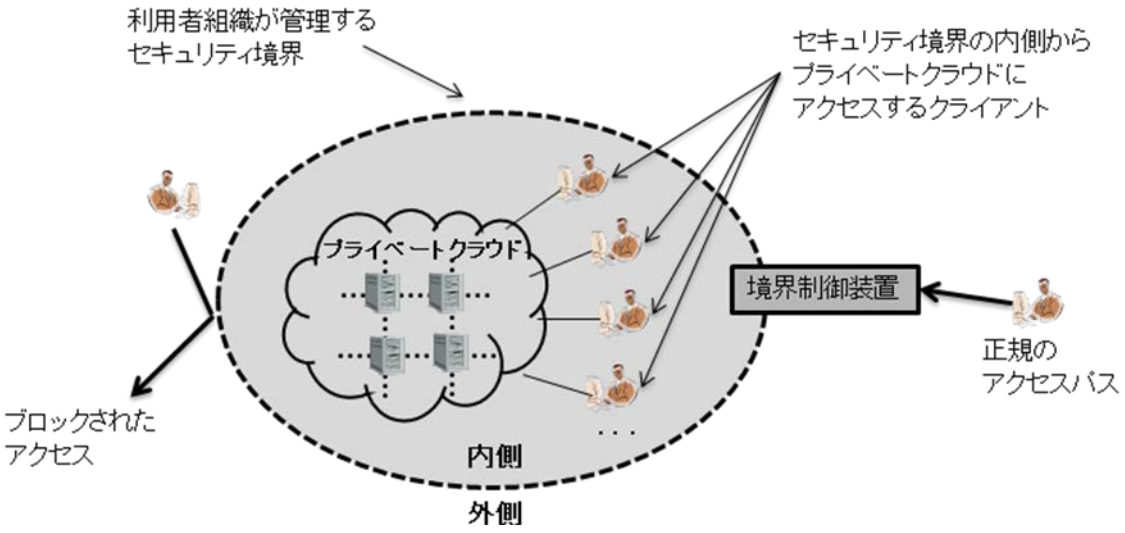

図3: オンサイトプライベートクラウド

オンサイトプライベートクラウドには共通の特徴が当てはまるが、それ以外にもオンサイトプライベートクラウドの利用を考えている組織が考慮すべき追加の、細部にわたる特性がある。

- **ネットワークへの依存性（オンサイトプライベート）。** オンサイトプライベートクラウドでは、例えば、単一の物理的施設や保護されたクラウドネットワークなど構成によっては、ネットワークへの依存性は利用者がコントロールできるネットワークリソース（例：ローカルエリアネットワーク）に依存する範囲に限定される。このシナリオでは、インターネットの混雑または遠隔のインターネット DNS とのやりとり[Moc87-1, Moc87-2]など、大規模ネットワークにありがちな問題を回避できるだろう。

  しかしながら、利用者組織が複数の物理的施設に跨っていて、それぞれの施設から同じプライベートクラウドにアクセスすることを望む場合には、その利用者組織が暗号化された専用回線などのコントロールされた施設間通信媒体を用意するか、あるいは、公衆インターネットなどのコントロールレベルが劣る通信媒体を使用する場合には暗号化技術（例えば VPN と共に）を使用する必要がある。これらのオプションは、いずれもプライベートクラウドのネットワークの可用性とセキュリティに対するリスクを招く。なぜならば、利用者の施設から離れた場所にある、利用者の直接の管理下にないリソースに対するパフォーマンス依存の問題があり、暗号化メカニズムの実装と設定がうまくいかなかった場合に外部からのアクセスを許してしまう可能性があるからである。利用者組織は、遠隔の施設が、プライベートクラウドに適したセキュリティレベルで維持されることと、セキュリティレベルの相違を防ぐために境界制御装置がインストールされることを確実にしなければならない。

- **利用者にも IT スキルが求められる（オンサイトプライベート）。** 利用者組織には、プライベートクラウドにアクセスするユーザデバイスを管理するのに必要な従来の IT スキルと、クラウドを扱うための IT スキルが求められる。オンサイトプライベートクラウドを使い始めた段階では、評価期間中はクラウドとクラウド以外のシステムを並行して運用したいと考える利用者組織もある。そのような評価期間には、従来の IT スキルが必要になるだろう。また、評価期間が過ぎても、レガシーなライセンス契約、特定のハードウェア要件またはシステム要件、特定プロジェクトに特化したセキュリティニーズ、および設備やトレーニングに対する従来からの投資を管理するために、従来の IT スタッフが必要となるだろう。

  さらに、クラウドを扱うための新たなスキルも必要となる。例えば、コンピュータを駆使した業務を行う組織では、クラウドのリソース上で高レベルの並列処理による業務の遂行を実現するために、最終的にそれらの業務の再編成が必要となる場合もある[Dea04]。クラウドで大規模なデータセットを処理する組織では、クラウドベースのストレージを扱うためのスキルの育成が必要となるだろう [Cha06, Ghe03, Ama06, SNI10, Msf11] 。[10]

- **ワークロードの所在地はクライアントからは見えない（オンサイトプライベート）。**「共通」のケースと同様に、クラウドのハードウェアリソースを管理するには、プライベートクラウドがマシン間のワークロードの移行をクライアントに不便を感じさせることなく、すなわち、移行をクライアントに意識させることなく行えることが前提となる。場合によっては、単一障害点が生成されるのを回避するために、地理的に分散された場所にクラウド施設を設けて運用する必要がある。しかしながら、オンサイトプライベートクラウドでは、プライベートクラウドが稼働する物理的インフラストラクチャを利用者組織が選択する。したがって、ワークロードの地理上の設置場所も利用者組織によって決定される。個々のクライアントは、ある時点で自身のワークロードが利用者組織のインフラストラクチャ内のどこに物理的に存在するかを知ることができない可能性がある一方で、利用者組織はワークロードが動作できる場所について知ることとコントロールすることができる。

- **複数利用者による共同利用(multi-tenancy)がもたらすリスク（オンサイトプライベート）。**「共通」のケースと同様に、複数の異なるクライアントのそれぞれのワークロードが同じシステムおよびローカルネットワーク上に同時に存在し、クラウド提供者のソフトウェアが実施するアクセスポリシーによってのみ隔離が行われる場合がある。その実装またはプロバイダの運用管理ポリシーおよび手順に欠陥があると、利用者組織のセキュリティポリシーに反してクライアントのワークロードが互いに見える状態になり、利用者組織のセキュリティが侵害される恐れがある。例えば VPN ルーティングなど、ネットワークレイヤーにおける論理的な隔離の技法は、リスクの軽減に役立つ。オンサイトプライベートクラウドでは、攻撃する可能性のある人間の数を最小限に抑えることによって、これらのリスクをある程度軽減することができる。オンサイトプライベートクラウドでは、通常、すべてのクライアントが利用者組織のメンバーであるか、あるいは、権限を与えられたゲストまたはパートナーであるが、それでも権限は与えられているが同時に悪意を持つ内部関係者による攻撃に対しては脆弱である。そうしたセキュリティ上の欠陥が原因で、給料計算、機微な個人情報の保存、知的財産の生成など、当該組織の異なる機能がマージされ、一定の秘密度のデータが権限のないユーザによってアクセスされ、オンサイトプライベートクラウドから外へデータが開示されてしまうことも考えられる。

- **データのインポート／エクスポート、およびパフォーマンスの限界（オンサイトプライベート）。**「共通」のケースと同様に、オンデマンドでの大量データのインポート／エクスポートはオンサイトプライベートクラウドのネットワーク容量によって制限され、リアルタイムな処理または極めて重要な処理はネットワークの制限によって阻害される可能性がある。しかしながら、オンサイトプライベートクラウドのシナリオでは、利用者のインフラストラクチャ内に高性能および／または高信頼性のネットワークを配備することによって、これらの制限を排除することはできないものの、緩和することができる。とりわけ、オンサイトプライ

[10] 注釈：クラウドストレージシステムの包括的なリストを指しているわけではない。

ベートクラウドに対して単一の施設からのみアクセスする場合には、WAN を使用する場合よりも実際に高いパフォーマンスを提供するローカルネットワークを配備してもよい。

- **外的脅威に対する堅固なセキュリティを実現できる可能性がある（オンサイトプライベート）。** オンサイトプライベートクラウドでは、十分に堅固なセキュリティ境界を実装することによって、クラウド以外のリソースに対して実現できるセキュリティと同レベルのセキュリティを確保し、プライベートクラウドのリソースを外的脅威から保護するといった選択肢もある。影響度が低位のデータおよび処理では、市販のファイアウォールのルールセットと VPN によってセキュリティ境界を構築してもよい。影響度が高位のデータでは、より厳しいファイアウォールポリシー[Zwi00, Ran99]、多要素認証[SP-800-63]、暗号化[Sch94, Ros99]、侵入検知・防止、および場合によっては物理的な隔離によって、セキュリティ境界を構築することもできる。

- **クラウドへの移行にかかる初期費用は、「やや高めから高いの間」である（オンサイトプライベート）。** オンサイトプライベートクラウドでは、利用者組織内のコンピュータシステムにクラウドマネジメントソフトウェアをインストールする必要がある。大量のプロセスまたはデータを扱うワークロードをサポートするためにクラウドを利用する場合、マネジメントソフトウェアは多数の市販システムにインストールするか、あるいは、より限られた数の高性能システムにインストールする必要があるだろう。クラウドソフトウェアのインストールと、インストール作業の管理は、クラウドソフトウェア自体が無料であっても、かつ、ハードウェアの多くが利用者組織に既にあるものでまかなえたとしても、かなりの初期費用が必要になる。以下に、プライベートクラウドを実現するための候補となる、3 つのアプローチを示す。

  データセンタの新設: 利用者にとって最もダイレクトなアプローチは、データセンタを手配して、クラウドソフトウェアを実装することである。この場合、従来のデータセンタを手配する場合と同様の初期費用が発生し、利用者は予想されるワークロードに対応できるデータセンタを用意することができる。

  データセンタへの改装: 新しいデータセンタを手配する以外にも、既存のデータセンタの一部または全部をオンサイトプライベートクラウド向けに改装するといった選択肢がある。ただし、このアプローチでは、初期評価期間にクラウドとクラウド以外のシステムを平行して運用することができないことも考えられる。

  リソースをかき集める: 上記以外にも、クラウドソフトウェアを主に組織内の既存のコンピュータにインストールするといったアプローチがある[Nur-08, Nur-08-2]。このシナリオでは、クラウドシステムがハードウェアリソースを占有するわけではなく、他の用途と共有するため、従来なら無駄になる可能性のあるサイクルを取り除くことができる。このアプローチは、ハードウェアに対する大規模な投資を行うことなく試験的にクラウドサービスを利用できるといったメリットをもたらす。しかしながら、そうした構成で利用できるハードウェアリソースは、組織のインフラストラクチャ内の余剰リソースに限られるだろう（他の用途に使用されていたハードウェアリソースがクラウドに譲る形で開放されない限り）。さらなる制限として、(1) オンサイトプライベートクラウドに組み入れなければならないハードウェアリソースは、効率化のために一か所に集められているわけではなく、利用者組織のインフラストラクチャ内のあらゆる場所から（ネットワークを介して）かき集めることになる、(2) 利用できるハードウェアが一様でなく、管理がいくらか困難になる可能性がある、といったことが挙げられる。

- **リソースが限られている（オンサイトプライベート）。** オンサイトプライベートクラウドでは、予想されるワークロードとコスト制限に対応するように調節された固定の処理能力とストレージ容量が、どの時点においても維持される。十分に多様なワークロードをサポートする大規模組織では、オンサイトプライベートクラウドが利用者組織内のクライアントに拡張性をもたらす可能性がある一方で、より小規模のオンサ

イトプライベートクラウドは従来のデータセンタのものに類似した最大能力上限を示すだろう。オンサイトプライベートクラウドでは、例えば設備の導入など、なんらかの費用を当初に支払う必要がある。

4.3 外部委託型プライベートクラウドのシナリオ

外部委託型プライベートクラウドを図で表すと図 4 のようになる。この図が示すように、外部委託型プライベートクラウドには、2 つのセキュリティ境界があり、片方はクラウド利用者によって実装され（右側）、もう片方はクラウド提供者によって実装される[11]（左側）。この 2 つのセキュリティ境界は、保護された通信リンクによって結ばれる。この図で明らかなように、外部委託型プライベートクラウドで実施される処理とデータのセキュリティは、セキュリティ境界と保護された通信リンクの両方の強度と可用性に依存する。そこで、クラウド提供者は、クラウド提供者によって実装されるべきセキュリティ境界を実施する責任と、プライベートクラウドリソースが、クラウド提供者によって管理されるセキュリティ境界の外側にあるその他のクラウドリソースと混在しないようにする責任を受け入れる。プライベートクラウドリソースとその他のクラウドリソースとの間で適切な強度での隔離を実現するための種々のメカニズムの適切性は、利用者のセキュリティ要求事項によって左右される。使用できるメカニズムは、例えば、仮想ローカルエリアネットワーク(VLAN)、仮想プライベートネットワーク(VPN)、ネットワークセグメントを分ける、クラスタなど、いくつか存在するが、それぞれのメカニズムには隔離の強度とコスト／利便性との間のさまざまなトレードオフが伴う。ただし、このシナリオでは、パブリッククラウドで利用者間を隔離するために使用される通常のメカニズム（例：ハードウェアの仮想化、VLAN）である隔離メカニズムのみを使用することは許されない。仮に、それらのメカニズムだけが使用された場合、本シナリオは本質的にパブリッククラウドのシナリオと同一になるだろう。

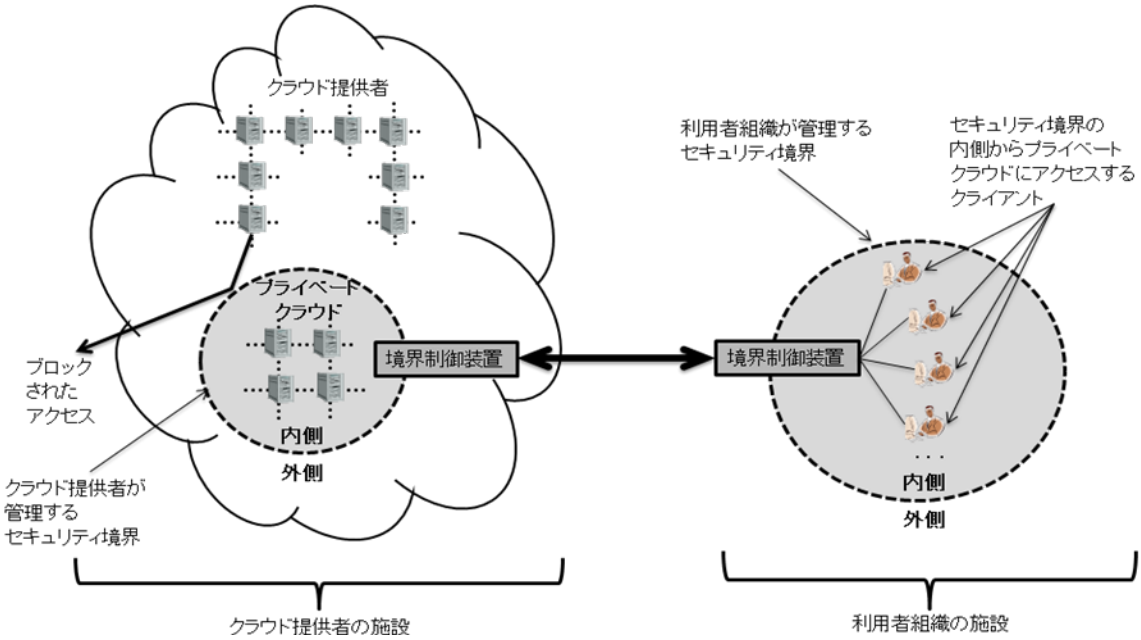

図4: 外部委託型プライベートクラウド

外部委託型プライベートのシナリオには共通ステートメントが当てはまるが、それ以外にも外部委託型プライベートクラウドの利用を考えている組織が考慮すべき、共通ステートメントの一部についてのより詳細な解釈と、追加のステートメントがある。

[11] 設定は、おそらく利用者が行うだろうが。

- **ネットワークに依存する（外部委託型プライベート）。** 外部委託型プライベートのシナリオでは、利用者は提供者との間に、保護された信頼性の高い専用の通信リンクを手配するといった選択肢もある。ネットワーク依存は避けられないと思われるが、本シナリオでは価格の交渉によりネットワーク依存の影響を改善することが可能である（例：パフォーマンス、信頼性、およびセキュリティの向上を支援する、専用回線によるネットワーク接続）。

- **ワークロードの所在地はクライアントからは見えない（外部委託型プライベート）。**「共通」のケースと同様に、クラウドのハードウェアリソースを管理するには、外部委託型プライベートクラウドがマシン間のワークロードの移行をクライアントに不便を感じさせることなく、すなわち、移行をクライアントに意識させることなく行えることが前提となる。しかしながら、外部委託型プライベートクラウドのシナリオでは、ワークロードの所在地に対するある程度の可視性とコントロールを有する機会が利用者組織に与えられる。クラウド提供者が利用者組織との間で合意したセキュリティ境界を忠実に実施すると仮定すると、利用者組織のワークロードの移動は、合意されたセキュリティ境界の内側でしか行われない。境界を実施するために選ばれたメカニズムによっては、外部委託型プライベートクラウドに割り当てられたリソースの物理的な位置（例：クラスタ、ネットワークセグメント）をクライアントは知りえないとしても、利用者組織が知ることが可能な場合がある。

- **複数利用者による共同利用(multi-tenancy)がもたらすリスク（外部委託型プライベート）。** 内容は、オンサイトプライベートクラウドの場合と同じである。FISMA と OMB ポリシーは、連邦政府に代わって連邦情報を取り扱っている、または情報システムを運用している外部プロバイダに対して、連邦政府機関と同等のセキュリティ要件を満たすことを要求している。

- **データのインポート／エクスポート、およびパフォーマンスの限界（外部委託型プライベート）。**「共通」のケースと同様に、オンデマンドでの大量データのインポート／エクスポートは提供者と利用者間のネットワーク容量によって制限され、リアルタイムな処理または極めて重要な処理はネットワークの制限によって阻害される可能性がある。外部委託型プライベートクラウドのシナリオでは、提供者と利用者間に高性能および／または高信頼性のネットワークを配備することによって、これらの制限を排除することはできないものの、緩和することができる。ただし、このような配備では特別な契約が必要となり、かなりの費用が発生する。

- **外的脅威に対する堅固なセキュリティを実現できる可能性がある（外部委託型プライベート）。** オンサイトプライベートクラウドのシナリオの場合と同様に、セキュリティ境界を強化するためのさまざまなテクニックが存在する。オンサイトプライベートクラウドとの主な違いは、それらのテクニックを利用者のネットワーク境界と提供者のネットワーク境界の両方に適用しなければならないことと、通信リンクを保護しなければならないことである。

- **クラウドへの移行にかかる初期費用は、「妥当からやや高めの間」である（外部委託型プライベート）。** クラウドの運用を開始する前に、物理的なコンピューティングリソースを利用者側で用意する、あるいはかき集める必要があるオンサイトプライベートクラウドと異なり、外部委託型プライベートクラウドのシナリオでは、リソースは提供者側が用意し、利用者側の初期費用は主に以下の要素に左右される：(1) SLA のサービス条項について交渉する（例：適切な保護メカニズムについての合意）、(2) 場合によっては、外部委託型プライベートクラウドに接続するために利用者のネットワークをアップグレードする、(3) 従来のアプリケーションからクラウドがホストされるアプリケーションに移行する、(4) 既存の非クラウドオペレーションをクラウドに移植する、および (5) トレーニング。これらの費用は、サーバー側の設備や基盤にあるインフラストラクチャの費用は含まないにもかかわらず、高額になることもある。

- **大規模なリソースを利用できる（外部委託型プライベート）。** リソースを利用者側で前もって用意する必要があるオンサイトプライベートクラウドと異なり、外部委託型プライベートクラウドでは、利用者は提供者が提供するリソースをどんな量でもレンタルすることができる。拡張可能なコンピューティング設備を

提供・運用することは、クラウド提供者に求められる必須の能力である。したがって、クラウド提供者は、比較的大規模なプライベートクラウドを必要に応じて提供できる可能性が高い。オンサイトプライベートクラウドと同様に外部委託型プライベートクラウドにおいても、利用できる処理能力はどの時点においても一定であり、十分に多様なワークロードを備えた大規模なクラウドでなければ、クライアントに拡張性を提供することはできない。また、オンサイトプライベートクラウドと同様に外部委託型プライベートクラウドにおいても、従来のデータセンタの場合と同じように、最大容量制限が提示されるであろう。

4.4 オンサイトコミュニティクラウドのシナリオ

オンサイトコミュニティクラウドを図で表すと図 5 のようになる。この図に示されたコミュニティは、一連の参加組織によって構成されている。それぞれの参加組織は、クラウドサービスを提供する側、クラウドサービスを利用する側、あるいはその両方に分類される。コミュニティクラウドが機能するには、少なくとも 1 人のコミュニティメンバーがクラウドサービスを提供することが必要となる。この図では、クラウドサービスを提供するメンバー（サービスを利用することもある）を左側に、サービスを利用するだけのメンバーを右側に示している。各組織がセキュリティ境界を実装すると仮定した場合、それらの参加組織は、セキュリティ境界を介してアクセス可能な、境界制御装置間のリンクによって接続される。これ以外にも、追加のセキュリティ境界を実装して、ローカルクラウドリソースをその他のローカルリソースから隔離するといった選択肢もある。考えられるネットワーク構成は多岐にわたる。図では、追加のセキュリティ境界が、ある組織の「クラウド以外の」セキュリティ境界の内側に設置されているが、外部に設置することも可能である。どのような設定であれ、境界制御装置は、クラウドリソースに対する適切なアクセスをローカルクライアントとその他の参加組織のクライアントの両方に与えらなければならない。重要なことは、ローカルクラウドリソースに対するアクセスを与えることによって、クラウド以外のリソースに対するアクセスも与えてしまうことがないようにすることである（ただし、そうすることが特定のポリシーの目的である場合を除く）。

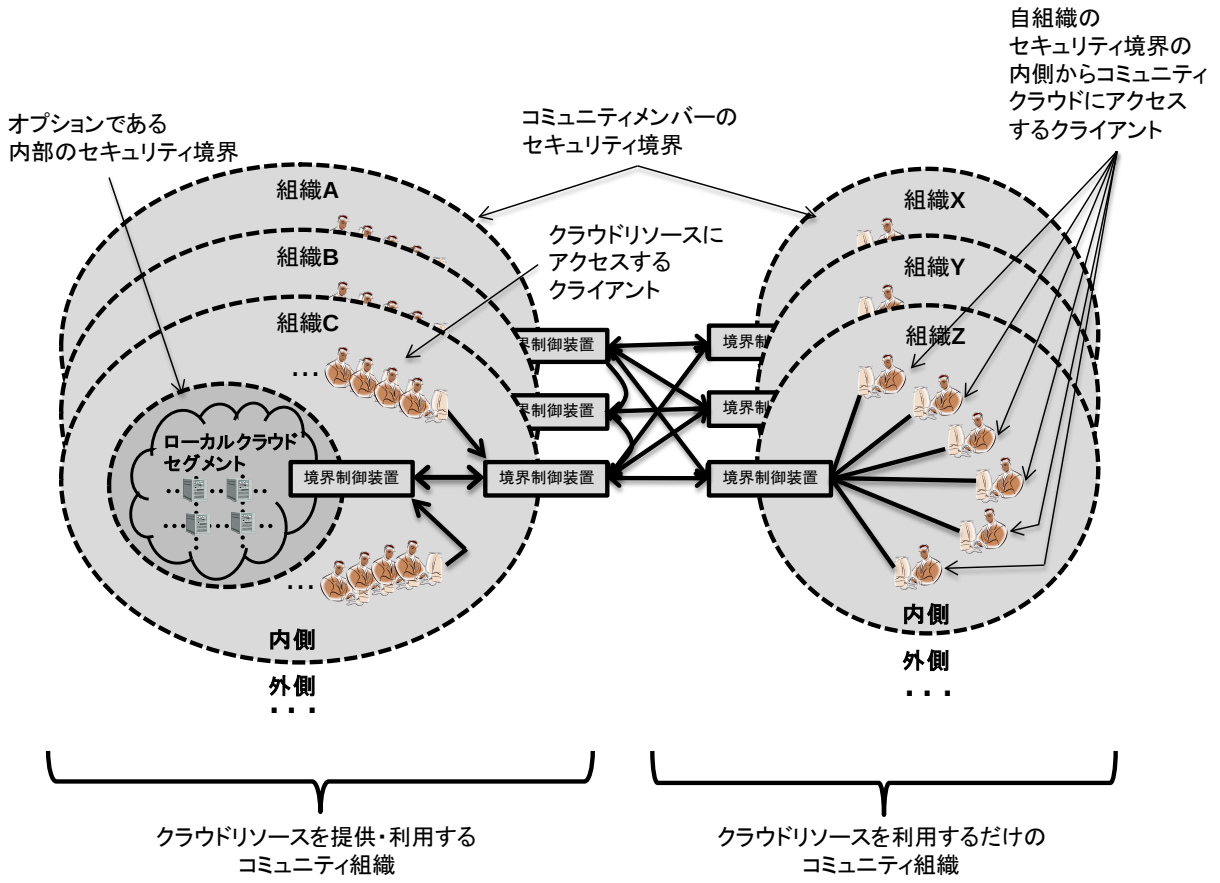

図5: オンサイトコミュニティクラウド

図 5 から、コミュニティクラウドのアクセスポリシーが複雑になることが容易に伺える。コミュニティが N 人のメンバーで構成されている場合、1人のメンバーのローカルクラウドリソースをその他の各メンバーとどのように共有するかについて、明示的であれ、暗黙であれ、決める必要がある。共有ポリシーは、例えば、XACML などの標準を使用した任意のアクセス制御[Mos05]、ロールベースのアクセス制御[Fer92]、属性ベースのアクセス制御[Kar09]など、いくつかのポリシー記述技法を使用して表現できる。さらに、このシナリオでは、リソースに対するアクセスコントロール以外にも、複数の参加組織のクライアントが共有のリソース集積にアクセスするため、ID 管理 [Oid11, Rag08, Oix10]が重要となる。

オンサイトプライベートクラウドや外部委託型プライベートクラウドと同様に、オンサイトコミュニティのシナリオも共通ステートメントが当てはまるが、それ以外にもオンサイトコミュニティクラウドの利用を考えている組織が考慮すべき、共通ステートメントの一部についてのより詳細な解釈と、追加のステートメントがある。

- **ネットワークへの依存性(オンサイトコミュニティ)。** 組織が複数の施設に跨るオンサイトプライベートクラウドと同様に、オンサイトコミュニティクラウドの利用者も、コントロールされた施設間通信リンクを用意するか、あるいは、公衆インターネットなどのコントロールレベルが劣る通信媒体を使用する場合には暗号化技術を使用する必要がある。オンサイトコミュニティクラウドの信頼性とセキュリティは、通信リンクの信頼性とセキュリティに依存するだろう。パフォーマンス、信頼性、およびセキュリティの向上を支援するために、専用回線によるネットワーク接続を使用するこができる。これ以外にも、オンサイトコミュニティの場合、参加組織が複数であることと、クラウドインフラストラクチャに障害が発生した(例:オフラインになる)場合に、いずれかの組織が損害を被る可能性があるため、メンバー組織間の実際の依存関係

の理解に注意を払うべきである。さらに、ローカルクラウドはメンテナンスのためにオフラインにせざるをえない場合が多いと予想されるが、互いに提供するサービスレベルと互いに求めるサービスレベルについての明確な理解を実現するためにも、コミュニティメンバー間の事前の通知が重要になる。

- **利用者にも IT スキルが求められる（オンサイトコミュニティ）。** オンサイトコミュニティクラウドでは、参加組織が、コミュニティにクラウドサービスを提供する組織と、クラウドリソースを利用するだけの組織の 2 種類に分類されると考えられる。クラウドリソースを提供する参加組織には、オンサイトプライベートクラウドのシナリオと同様の IT スキルが求められるが、クラウドの全体的な構成がより複雑である場合には、より高レベルのスキルが求められる。リソースを利用するだけの参加組織には、クラウドサービスを提供する参加組織が複数である場合を除き、「共通」のケースと同様の IT スキルが求められる。クラウドサービスを提供する組織が複数である場合、サービスを利用する側の設定がより複雑になり、例えば、クライアントが複数の認証情報を維持管理しなくてはならない、あるいは、ID マネジメントフレームワークに委ねざるをえなくなることも考えられる。

  参加組織間の ID およびアクセス制御の設定は、複雑になる可能性がある。コミュニティクラウドの利用を考えている組織は、当該コミュニティクラウドに導入される予定のアクセスポリシーついて、参加組織の IT スタッフが交渉し、明確に文書化していることを確認すべきである。

- **ワークロードの所在地はクライアントからは見えない（オンサイトコミュニティ）。** 外部委託型プライベートクラウドのシナリオと同様に、参加組織がセキュリティ境界を忠実に実装し、ワークロードを施設内に留めるポリシーを実施している場合には、ワークロードは参加組織内に留まることになる。しかしながら、このシナリオにはいくつかのバリエーションが考えられる。例えば、コミュニティクラウドにクラウドサービスを提供する組織が、実装戦略の一環として外部委託型プライベートクラウドの採用を望む可能性がある。ワークロードの所在地について知りたいと考える組織は、コミュニティクラウドに参加する前に、考えられる外部委託の構成について話し合い、外部委託ポリシーが明確に文書化され参加組織が閲覧できる状態であることを確認すべきである。

- **複数利用者による共同利用(multi-tenancy)がもたらすリスク（オンサイトコミュニティ）。** オンサイトプライベートのシナリオと同様に、オンサイトコミュニティのシナリオにおいても、攻撃する可能性のある人間の数を最小限に抑えることによって、マルチテナントに伴うリスクの一部を軽減することができる。しかしながら、オンサイトコミュニティのシナリオでは、より多くの組織がクラウドに含まれるため、攻撃する可能性のある人間の数を抑えるといっても、オンサイトプライベートのシナリオ程には抑えられないだろう。

- **データのインポート／エクスポート、およびパフォーマンスの限界（オンサイトコミュニティ）。** コミュニティクラウドでは、さまざまな参加組織間を結ぶ通信リンクの性能、セキュリティおよび信頼性は、参加組織のニーズに応じてさまざまなレベルで提供される。したがって、ネットワークベースの制限は、外部委託型プライベートクラウドのシナリオとものと類似する。

- **外的脅威に対する堅固なセキュリティを実現できる可能性がある（オンサイトコミュニティ）。** コミュニティクラウドの外的脅威に対するセキュリティは、参加組織のすべてのセキュリティ境界のセキュリティと、通信リンクの強度に依存する。これらの依存性は、根本的には外部委託型プライベートクラウドのシナリオと同じだが、コミュニティクラウドはより多くのリンクとセキュリティ境界を持っているため、設定がより複雑になる。

- **クラウドへの移行にかかる初期費用は、かなりのばらつきがある（オンサイトコミュニティ）。** オンサイトコミュニティクラウドに参加する組織が負担する初期費用は、その組織がクラウドサービスを利用するだけであるか、それとも、クラウドサービスの提供も行うかによって大きく変わってくる。利用のみのシナリオでは、外部委託型プライベートクラウドの場合と同様の初期費用で済むと考えられる（すなわち、妥当からやや高めの間）。一方、コミュニティクラウド内でクラウドサービスを提供するのであれば、オンサイ

トプライベートクラウドのシナリオと同様の初期費用が必要になると考えられる（すなわち、やや高めから高いの間）。

- **リソースが限られている（オンサイトコミュニティ）。** オンサイトプライベートクラウドのシナリオと同様に、オンサイトコミュニティクラウドにおいても、リソースをローカルで調達またはかき集める必要がある。したがって、オンサイトプライベートクラウドと同様のリソース制限が存在すると考えられる（すなわち、比較的限られている）。

4.5 外部委託型コミュニティクラウドのシナリオ

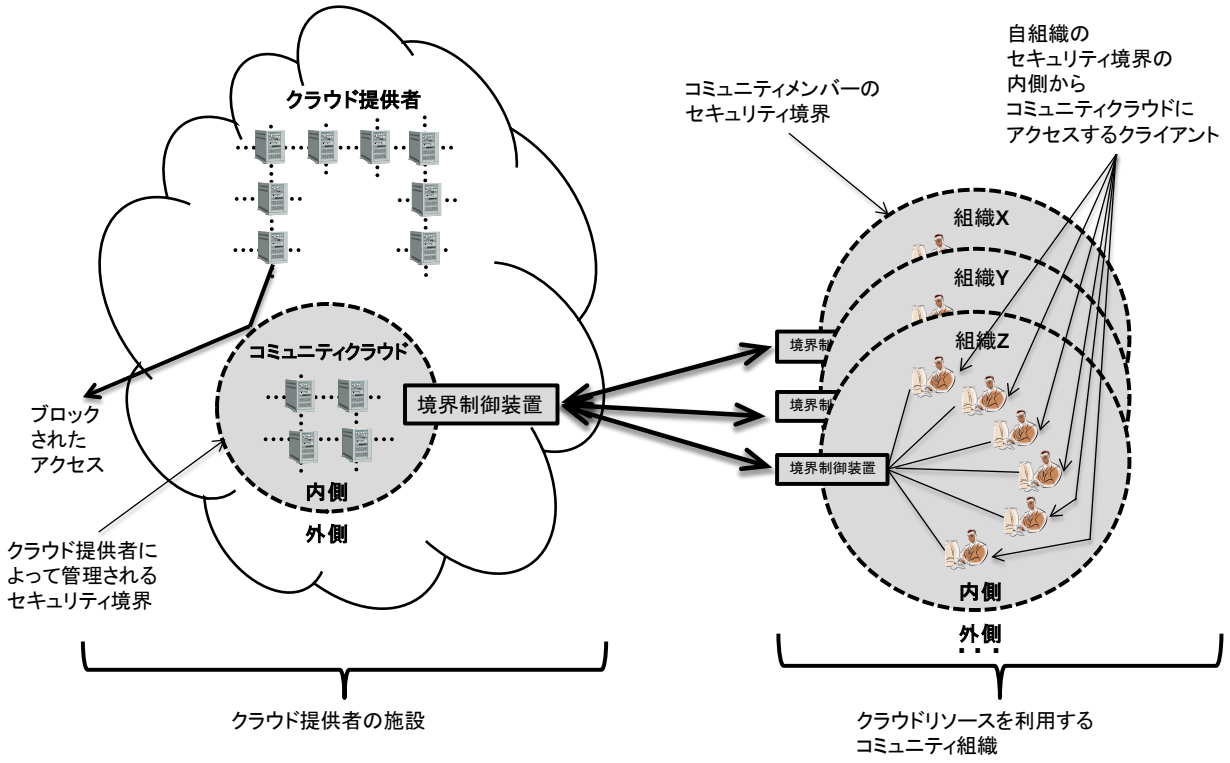

図6: 外部委託型コミュニティクラウド

外部委託型コミュニティクラウドを図で表すと図 6 のようになる。この図に示されたコミュニティは、クラウドサービスを利用する一連の参加組織によって構成される。本シナリオは、外部委託型プライベートクラウドのシナリオに非常に似ている。つまり、クラウド提供者がサーバー側の責務を管理し、セキュリティ境界の実装を行い、コミュニティクラウドのリソースが、クラウド提供者によって管理されるセキュリティ境界の外側にあるその他のクラウドリソースと混在しないようにする。大きな違いは、外部委託型コミュニティクラウドでは、場合によっては、クラウド提供者による参加組織間の共有ポリシーの強制適用が必要となることである。

外部委託型コミュニティクラウドのシナリオには共通ステートメントが当てはまるが、それ以外にも以下に示すような、共通ステートメントの一部についての細部にわたる特性がある。

- **ネットワークへの依存性（外部委託型コミュニティ）。** 図 6 を見ても分かるように、外部委託型コミュニティクラウドのネットワークに対する依存性は、外部委託型プライベートクラウドのものと似ている。主な違いは、保護された複数の通信リンクがコミュニティメンバーからクラウド提供者の施設へと結ばれることである。

- **ワークロードの所在地はクライアントからは見えない（外部委託型コミュニティ）。** 内容は、外部委託型プライベートクラウドのシナリオと同じである。
- **複数利用者による共同利用(multi-tenancy)がもたらすリスク（外部委託型コミュニティ）。** 内容は、オンサイトコミュニティクラウドのシナリオと同じである。
- **データのインポート／エクスポート、およびパフォーマンスの限界（外部委託型コミュニティ）。** 内容は、外部委託型プライベートクラウドのシナリオと同じである。
- **外的脅威に対する堅固なセキュリティを実現できる可能性がある（外部委託型コミュニティ）。** 内容は、オンサイトコミュニティクラウドのシナリオと同じである。
- **クラウドへの移行にかかる初期費用は、「妥当からやや高めの間」である（外部委託型コミュニティ）。** 内容は、外部委託型プライベートクラウドのシナリオと同じである。
- **大規模なリソースを利用できる（外部委託型コミュニティ）。** 内容は、外部委託型プライベートクラウドのシナリオと同じである。

4.6 パブリッククラウドのシナリオ

パブリッククラウドを図で表すと図 7 のようになる。この図は、セキュリティ境界を実装している利用者施設が描かれている点を除き、基本的には図 1 と似ている。しかしながら、パブリッククラウドの場合、図 1 をベースにした場合よりも多くのステートメントがなされることが、下の図から伺える。例えば、パブリック環境では、クラウド提供者のコンピューティングおよびストレージリソースが大規模である可能性があり、通信リンクは公衆インターネット上に実装されると考えられ、さまざまなクライアント層に（場合によっては攻撃者にも）サービスが提供される。

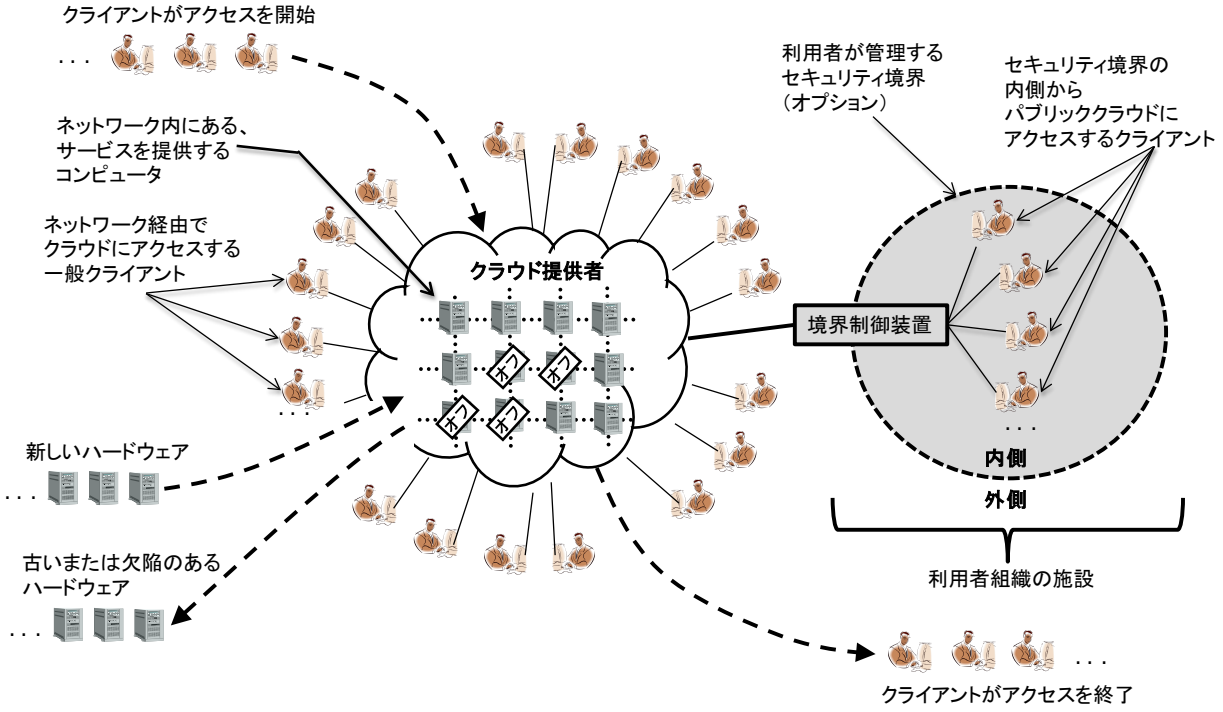

図7: パブリッククラウド

他のシナリオと同様に、パブリッククラウドのシナリオにも共通ステートメントが当てはまるが、それ以外にも共通ステートメントの一部についてより細部にわたる特性がある。

- **ネットワークへの依存性（パブリック）。** パブリックのシナリオでは、利用者は公衆インターネットを介してクラウド提供者に接続する。したがって、接続の信頼性は、インターネットの DNS サーバーのインフラストラクチャ、ルータのインフラストラクチャ、およびルータ間のリンクに依存する。したがって、これらのコンポーネントの設定ミス[Opp03]や機能不全、ならびにネットワークの混雑または攻撃によって、接続の信頼性が損なわれる場合がある。さらに、利用者には、しばしば「ラストマイル」と表されるインターネットサービスプロバイダ(ISP)を介した接続が求められる。この接続がうまくいっていないと、パブリッククラウドをオンラインで利用できない。

- **ワークロードの所在地はクライアントからは見えない（パブリック）。**パブリッククラウドのシナリオでは、処理能力であれ、データであれ、利用者のワークロードを提供者がいつでも移転できる。パブリッククラウドコンピューティングにおける費用効率に関する主な議論の一つに、データセンタ（およびワークロード）を低コストの場所にを設置できることがある。通常、パブリッククラウドにおけるワークロードは、クラウド提供者が（オプションとして）ロケーション制限ポリシーを提供していて、利用者が特定のロケーション制限をリクエストするよう自身のアカウントを設定している場合を除き、クラウド提供者がいつでも、どこにでも移動できる。通常、パブリッククラウドにおけるロケーション制限は、例えば「米国の東海岸に」など、幾分きめが粗い。制限が実際に実施されていることに対する信頼は、利用者の登録情報が保護されているか（例：アカウントがハイジャックされていないか、その設置場所の選択が変更されていないか）、およびクラウド提供者が公示しているポリシーをどれだけ忠実に実施しているかによって決まる。通常、利用者は、ロケーション制限が実施されているか否かを確認できる立場にない。

- **複数利用者による共同利用(multi-tenancy)がもたらすリスク（パブリック）。**パブリッククラウドでは、一台のコンピュータが任意の組み合わせの利用者のワークロードによって共有される可能性がある。これは、実際に、ある利用者のワークロードが競争相手または敵のワークロードと同じ場所に置かれる可能性があることを意味する。共通ステートメントに要約されているように、そうした状況は信頼性に対するリスクとセキュリティリスクの両方を招き、いずれかの利用者によって障害を引き起こされたり、攻撃をしかけられる可能性がある。パブリッククラウドでは、利用者とリソースの規模の増加に合わせて拡張できるという点が重要な戦略の一つであり、これにより低コストと拡張性(elasticity)を実現できる。しかしながら、この拡張性が実現されれば、攻撃する可能性のある人間の規模も増加すると考えられる。

- **セキュリティに関するデータに対する可視性とコントロールが限られている（パブリック）。**クラウド提供者によるシステム運用の詳細は、通常、機密情報とみなされ、利用者には開示されない。多くの場合、クラウド提供者が使用するソフトウェアは提供者に帰属し、利用者が点検することはできない。したがって、（本文書の執筆時点で）利用者には、クラウド内の提供者のリソースをモニタリングできる決まった方法や、リソースに対するアクセス権が与えられていない。クラウド提供者が利用者のリクエストを実施しようと真剣に努める場合もあり、一部のクラウド提供者がモニタリングサービスを提供する場合もあるが、利用者からしてみれば、クラウド提供者が業務を忠実に遂行することを信頼するか、あるいは、クラウド提供者が第三者監査機関と契約を結んでいる場合には、正確でタイムリーな監査が行われることを信頼するしかない。このような制約の例として、現在のところ、クラウド提供者のシステムからデータが完全に消去されたか否かを利用者が確認できないことが挙げられる。

- **クラウドへの移行にかかる初期費用は、少なくて済む（パブリック）。**内容は、外部委託型プライベートクラウドのシナリオと同じであると考えられる。

- **拡張性：リソースを無尽蔵に調達できるような錯覚を覚える（パブリック）。**通常、パブリッククラウドでは、所在地とサイズに制約がない。さらに、通常は、固定的なセキュリティ境界による制約を受けることなくマルチテナントを利用できるため、利用可能なリソースに合わせて利用者ワークロードを高い柔軟性を

持って移動できる可能性がある。したがって、パブリッククラウドは拡張性を実現するうえでのユニークな利点を備えていて、利用者はリソースを無尽蔵に調達できるような錯覚を覚える。

- **制約の多いお仕着せの SLA（パブリック）。**パブリッククラウドのデフォルトの SLA には、利用者に対する提供者側の限られた保証が明記され、利用者に対する補償の制限と利用者側の義務の概要が示される。
- マーケティング資料がクラウドシステムの信頼性およびセキュリティなどについての大まかな記述を含むこともあるが、サービス契約のサービス条項はクラウド提供者が果たすべき実際の（法的）義務を規定する。これらのサービス条項については、第 3 章で、より詳細に説明している。

4.7 ハイブリッドクラウドのシナリオ

第 2 章のクラウドの定義にもあるように、ハイブリッドクラウドはプライベートクラウド、コミュニティクラウド、パブリッククラウドのうち、2 つ以上のクラウドの組み合わせからなる。本章にて示されように、プライベート実装モデルとコミュニティ実装モデルは、いずれもオンサイトと外部委託型の 2 つの有意な異型を有する。オンサイトと外部委託型では、パフォーマンス、信頼性、およびセキュリティ特性が異なるため、このバリエーションは重要である。したがってハイブリッドクラウドでは、それを構成する各クラウドが、前述の 5 つの異型のうちのいずれかに当てはまる。ハイブリッドクラウドでは、考えられる構成が数多くあり、それらをすべて列挙するのは現実的でない。ただし、可能な構成の例と、考えられる課題を例示することは可能である。

図 8 に、実装モデルのすべての異型を代表するクラウドを使用したハイブリッドクラウドの構成例を示す。この図では、ハイブリッドクラウドを構成するクラウドへのアクセスポイントと、それらのクラウド間の（すべての）接続が示されている。情報の流れとリソースに対するアクセスに関するセキュリティポリシー、例えば、個々の構成クラウドによって適用されるポリシーに基づいた、さまざまな方法で実装することができる。さらに、ハイブリッドクラウドにおける ID 管理や認証および情報保護のための共通化された標準などのグローバルな問題は、図に示されていない。また、構成クラウドの追加や離脱による、時間の経過に伴うハイブリッドクラウドの変化といったより複雑な問題も、図に示されていない。

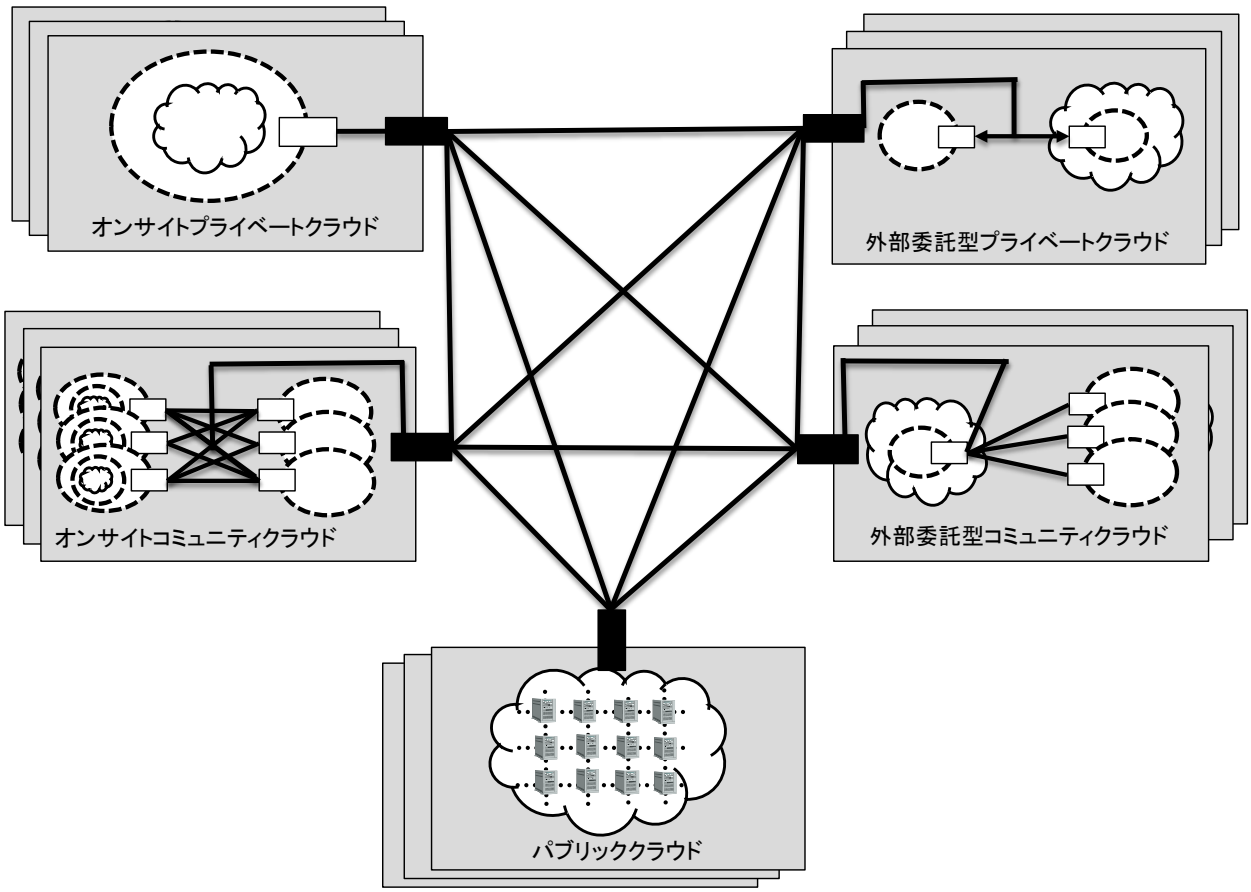

図8: ハイブリッドクラウド

図 8 が示すように、ハイブリッドクラウドは非常に複雑になる場合がある。しかしながら、より単純で有用性の高いハイブリッドクラウド構成も多く存在する。例えば、よく論じられるコンセプトの１つである「クラウドバースト」では、利用者が通常のワークロードにはプライベートクラウドを利用し、需要が高い期間には代替の 1 つまたは複数の外部クラウドにアクセスする。他にもハイブリッドクラウドでは、ある種類のクラウドを別の種類のクラウドのバックアップリソースとして使用したり[SNI09]、あるクラウドを別のクラウドの災害復旧用として使用すること[SNI09]も可能である。クラウドプラットフォーム上で実行できるように特別に開発された新しいソフトウェア（例：[Msf11-2, Goo11, Sal11]）は、マルチクラウド構成になる可能性がある（あるいは、その可能性が高い）。例えば、ウェブリクエストを扱うプラットフォームクラウド（第 6 章を参照）が、ウェブアプリケーションを低コストで継続的に利用できるようにするうえで非常に有効であるのに対し、アプリケーションをサポートするのに必要なバックグラウンド処理の実施には、オンサイトまたはコミュニティインフラストラクチャクラウドの方がより適しているだろう。組織の機能や役割によっては、異なるクラウド実装モデルが適している場合もある。例えば、給与情報のような機微なデータは外部委託型プライベートクラウドで処理し、新しいソフトウェアの開発とテストにはパブリッククラウドを利用することを、組織が選択することも考えられる。

5. ソフトウェア・アズ・ア・サービス(SaaS)環境

本章の目的は、クラウドコンピューティング環境におけるソフトウェア・アズ・ア・サービス (SaaS)のアーキテクチャと基本的な動作を示すことにある。この情報は、SaaS クラウドサービスが特定の信頼性、法令順守、またはセキュリティ要求事項を満たすか否かを評価する必要がある読者にとって、また、SaaS クラウドサービスの動作の仕組みを理解したいと考える読者にとって重要である。

SaaS という用語は 1990 年代、すなわち、クラウドコンピューティングが出現する前から使われている。SaaS は、一般的に「ウェブサービス」としても知られている。SaaS システムは、いくつかの異なる方法で実装することができる。[Cho06]の SaaS 成熟度モデルを用いて得られた SaaS の最新アーキテクチャは、NIST によるクラウドコンピューティングの定義を満たすと考えられる。SaaS に関してはわずかに異なる定義がいくつも出現する可能性があるが、シンプルで有用な定義が既になされている。

「ホストされるサービスとして実装されるソフトウェアであり、インターネット経由でアクセスされる。」[Cho06]

基本的にクラウドコンピューティングは、コンピューティングリソースを適宜レンタルできる機会を提供する。これらのリソースは、通常、ネットワーク経由で利用者によってアクセスされ、ユニットで計測され、

SaaS

誰がサービスを利用するか？

1. 職場でよく使われるソフトウェアアプリケーション、たとえば、生産性向上のためのアプリケーションや電子メールアプリケーションに対するアクセスを職員に与えている組織
2. 自身のために、あるいは組織に代わってソフトウェアアプリケーションを直接使用するエンドユーザ
3. エンドユーザ向けにアプリケーションの設定を行うソフトウェアアプリケーションアドミニストレータ

利用者は何を得るか？ 特定のアプリケーションをオンデマンドで利用する権利、およびバックアップや利用者間のデータ共有などのアプリケーションデータの管理。

利用料金はどのように算出されるか？ 通常は、利用者の数、利用時間、実行回数、処理されたレコードの数、利用したネットワーク帯域、および保存するデータの量と保存期間を基に算出される。

特定の利用者に個別に割り当てることが可能で、料金はそのユニットを誰が、どのくらいの期間にわたって、どのように使用したかなどに基づいて算出される。SaaSの場合、レンタルされるのはアプリケーションに対するアクセスである[Sii01]。通常、アプリケーションに対するアクセスは、SaaS提供者と利用者を結ぶネットワークを介して行われる。パブリックまたは外部委託型SaaSの場合、アプリケーションプログラムロジックの大半はクラウド提供者のサーバー上で実行される。利用者のブラウザ [12]は、(1) 利用者のキーストロークやその他のインプットを受け取り、グラフィック／サウンドの形式でアウトプットを生成するためのユーザインターフェース、および (2) データをUSBデバイスまたはプリンタなどのローカルストレージデバイスに出力するためのデータエクスポート機能を提供する。利用者のブラウザとクラウド提供者との間でネットワークを介してやりとりされるアプリケーションデータを保護するには、暗号化が必要となる。通常、利用者のブラウザとクラウド提供者のサーバーは、いくつかある標準鍵交換プロトコルのうちのいずれか（例：TLS[Die08]またはSSL[Net96]）を用いて共有鍵を取り決めたうえで、セッションを開始する。次に、利用者のブラウザとクラウド

[12] SaaS クラウドとのやりとりには、ブラウザまたはその他のシンクライアントアプリケーションを使用できるが、実際には、追加のインストールを必要としないブラウザが使用されることが多い。本文書では、便宜上、利用者側のソフトウェアを単に「ブラウザ」と称している。

提供者は、その鍵を使用して通信を暗号化する[13]。その後、利用者と提供者は認証情報を交換して、互いに身元を確かめる。通常、利用者はアカウント名とパスワード、あるいはその他の認証情報、例えば、時間ベースのハードウェアトークン値を提示する。

利用者に対する SaaS 提供者の主な責任は、自身が供給するソフトウェアがしっかりサポートされ、テストされることを確実にすることである。次第に増加する利用者ワークロードに合わせて SaaS アプリケーションを拡張できることも、重要な要件となる。セキュアな環境で利用者に提示した稼働率を保ちながら上記を実施できるインフラストラクチャを維持管理することは、極めて重要な側面である。多くの利用者が組織の重要なデータをクラウドに保存して、その情報の一部が専有であったり、業務上機微な情報であったりするため、セキュアな環境が必要不可欠となる。

以下の 6 つのサブセクションでは、SaaS サービスのいくつかの重要な特性である、抽象的な相互作用ダイナミクス、ソフトウェアスタックおよび提供者／利用者が有するコントロールの範囲、メリット、問題と懸念、候補となるアプリケーションクラス、ならびに推奨事項について説明する。

5.1 抽象的な相互作用ダイナミクス

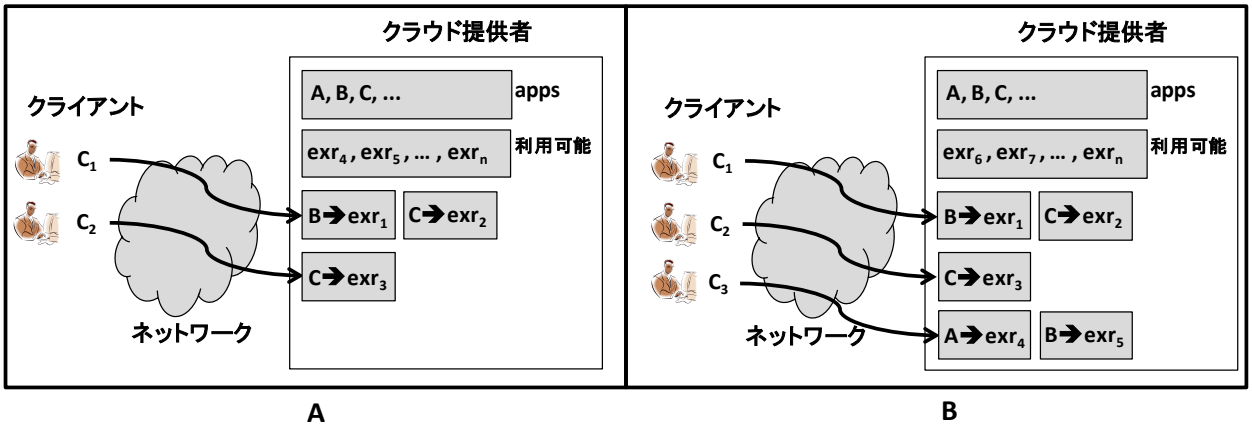

図9: SaaS における提供者／利用者間の相互作用ダイナミクス

本章では、SaaS クラウドサービスについての理解を読者にもたらすために、典型的な利用者組織のクライアントと SaaS クラウドサービス間の相互作用ダイナミクスをシンプルなモデルによって抽象的に説明する。図 9 に、そうしたモデルの一例を示す。図 9 の A には、C_1 と C_2 の 2 人のクライアントにサービスを提供するクラウドが描かれている。プライベートクラウドでは、すべてのクライアントは単一の利用者組織に所属する（あるいは関連する）。その他の実装モデルでは、第 4 章で触れたように、クライアントは異なる利用者組織を代表する場合がある。概念上は、クラウド提供者がクライアントに提供する、ネットワーク経由で利用可能なソフトウェアアプリケーションのインベントリ（図中の「apps」）は、クラウド提供者が所有する。また、アプリケーションの実行に必要なリソース（図中の「exr」とラベル付けされたもの）も、クラウド提供者が保有（またはレンタル）する。図 9 の A では、クライアント C_1 が 2 つのアプリケーション（B と C）を同時に使用している。クライアント C_1 向けのそれらのアプリケーションを実行できるよう、クラウド提供者は 2 つの実行リソース、exr_1 と exr_2 を割り当てている。この内、exr_1 は、アプリケーション B を実行するための処理能力とその他のリソース（図中の「B-> exr_1」）を提供し、exr_2 は、アプリケーション C を実行するための処理能力とその他のリソース（図中の「C-> exr_2」）を提供する。実行リソース（例えば、物理的なコンピュータであったり、仮想マシン

[13] こうした保護は、リスクがまったくないわけではない。なぜならば、過去に誤った実装やプロトコルの欠陥を突いた中間割込み(man-in-the-middle)攻撃が成功裏に行われ、利用者のクラウドリソースがアタッカーによってハイジャックされる可能性が示されたからである[Mar09]。

（第 7 章に記載）であったり、あるいは、クライアントのリクエストを処理するサーバープログラムであったりする）は、仮想マシンを起動する、もしくはコンピューティングサイクルとストレージを他の組織からレンタルすることさえも可能である。同様に、クライアント C_2 は、実行リソース exr_3 によってサポートされるアプリケーション C を使用している。クラウド提供者がアプリケーションをサポートする実行リソースを集めて整理(marshal)できれば、同じアプリケーション（この場合 C）を複数のクライアントに同時にレンタルすることも可能である。図 9.B に示されたように、クラウド上のアプリケーションをリクエストするクライアントが 1 人増えた場合、クラウド提供者は、リクエストされたアプリケーションをサポートする追加の実行リソースを割り当てる。

5.2 ソフトウェアスタックおよび提供者／利用者が有するコントロールの範囲

SaaS では、ソフトウェアスタックの大半をクラウド提供者がコントロールする。図 10 に、コントロールとマネジメントに関する責任の分担を示す。図の中央には、ハードウェア、オペレーティングシステム、ミドルウェア、およびアプリケーションの層から成る、従来のソフトウェアスタックが描かれている。この図には、クラウド提供者と利用者のいずれか、または両方に対する責任の割り当ても示されている。

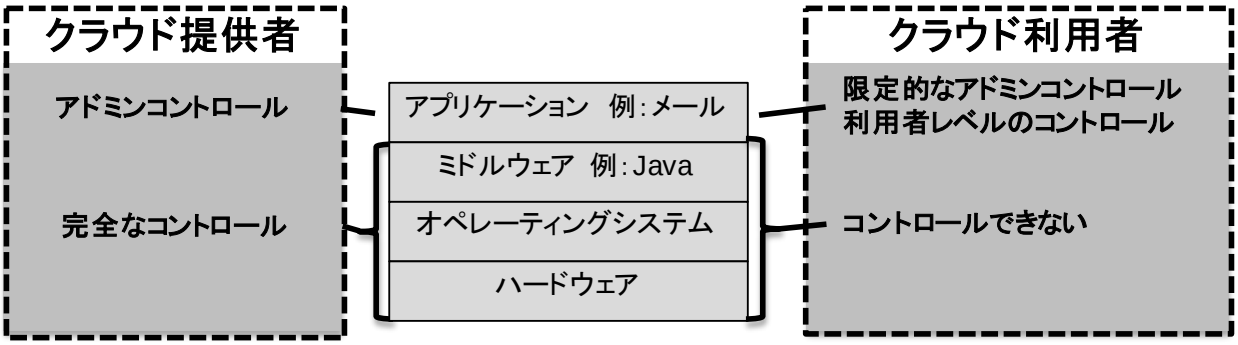

図10: SaaS において提供者／利用者が有するコントロールの範囲

SaaS サービスモデルでは、SaaS アプリケーションが提供するアプリケーションのためのリソースを利用者がコントロールする。例えば、クラウド提供者が電子メールアプリケーションを提供している場合、通常、利用者は電子メールメッセージを作成、送信し、保存することができるだろう。図 10 では、これを「利用者レベル」のコントロールと表記している。場合によっては、利用者がアプリケーションに対する限定的な管理的コントロールを有することもある。例えば、電子メールアプリケーションの例では、他の利用者の電子メールアカウントを作成したり、他の利用者の活動をレビューする権限が、特定の利用者に与えられることもある。

その一方で、アプリケーションレベルの管理的コントロールに関しては、クラウド提供者がかなり多くの割合でコントロールを有するのが通常である。クラウド提供者は期待されるレベルのサービスを利用者に提供するために、アプリケーションの実装、設定、更新、および運用の管理に責任を負う。クラウド提供者の責任には、利用規定の実施、利用料金の請求、問題の解決なども含まれる。これらの義務を果たすために、クラウド提供者はアプリケーションに対する最終的な権限を行使する必要がある。利用者が限られた管理的コントロールを有することもあるが、利用者が有するコントロールは、クラウド提供者の裁量によってのみ存在する。

図 10 に描かれているミドルウェア層は、アプリケーションにソフトウェアを構築するための構成要素を提供する。ミドルウェア層は、(1) 従来のソフトウェアライブラリから、(2) ソフトウェアインタプリタ（例：Java 仮想マシン[Lind99]または Python ランタイム環境[Pyt11]または共通言語インフラストラクチャの実装[ISO/IEC 23271:2006]）や、(3) リモートネットワークサービスの起動まで、いくつかの形態をとる。ミドルウェアコンポーネントはデータベースサービス、ユーザ認証サービス、ID 管理、アカウント管理などを提供する場合がある。

通常、クラウド利用者がこの層に直接アクセスする必要はなく、直接アクセスすることもできない。同様に、オペレーティングシステム層とハードウェア層についても、利用者が直接アクセスする必要はなく、直接アクセスすることもできない。1つの選択肢として、クラウド提供者が仮想マシンモニター (VMM)をソフトウェアスタックの一部として使用することもある。この場合（図 10 には示されていないが）、仮想マシンモニターはハードウェア層とオペレーティングシステム層の間に設置される。仮想マシンモニターは、クラウド提供者による利用可能なハードウェアリソースの管理を支援する便利なツールではあるが、SaaS の利用者が直接アクセスする必要はなく、通常は直接アクセスすることもできない。

5.3 メリット

コンピュータとソフトウェアを各自に配布する従来のソリューションに比べて、SaaS クラウドは拡張性を提供し、利用者側の大きな負担を提供者側に移行するため、効率の向上と、場合によってはパフォーマンスの向上のための多くの機会が与えられる。以降の各章では、SaaS クラウドの 5 つの主なメリットについて説明する。

5.3.1 ソフトウェアツールの 占有面積が小さくて済む

インタラクティブなコンテンツを効率的に表示できるブラウザが広く提供されてどこでも手に入ることから、SaaS アプリケーションの実装はますます便利に、かつ効率的になり、クライアント側のソフトウェアをほとんど、あるいは全く必要としなくなった。このような価値命題に寄与する因子は、いくつかある。

- 市販のソフトウェアアプリケーションと違って、SaaS アプリケーションは複雑なインストール手順を踏まなくても利用できる。
- クライアントコンピュータ上で SaaS アプリケーションが占める面積は非常に小さいため、クライアントコンピュータ上の各アプリケーションの設定が互いに干渉するリスクを軽減できる。
- ソフトウェアの配布コストを根本的に削減することができる。[Cho06]で論じられているように、配布コストが下がれば、利用者の数が少ない場合にも、ソフトウェア機能を経済的に開発・実装できる。

5.3.2 ソフトウェアライセンスの効率的利用

SaaS を使用すれば、ライセンス管理におけるオーバーヘッドを大幅に減らすことができる。[Sii01]で述べたように、利用者はシングルライセンスを複数のコンピュータ上で異なる時間に適用することができる。それぞれに異なるコンピュータごとに追加のライセンスを購入する必要がないため、使われない可能性のあるコンピュータへのライセンスの供給、すなわち、ライセンスの過剰供給を回避できる。さらに、ソフトウェアはクラウド提供者のインフラストラクチャ内で稼働し、利用量は直接計測されて請求されるため、アプリケーション開発者の知的財産を保護するための従来のライセンス管理プロトコルやライセンスサーバーは必要でない。

5.3.3 管理とデータの集中化

パブリックおよび外部委託型のシナリオにおける SaaS サービスモデルは、アプリケーションによって管理されるデータの大半がクラウド提供者のサーバー上に置かれることを意味する。クラウド提供者がこのデータを分散して保管することによって、冗長性と信頼性を確保することもある（利用者からは 1 箇所に保管されているように見えるが）。このような論理的なデータ集中化は、利用者にとって重要な意味を持つ。一つには、パブリックおよび外部委託型のシナリオでは、SaaS 提供者がデータの専門的な管理、例えば、法令順守チェック、セキュリティスキャン、バックアップ、および災害復旧を行うことがある。パブリックおよび外部委託型のシナリオでは、これらのサービスが利用者の施設から離れた場所から提供されるため、SaaS によるデー

タの管理は、利用者の施設とデータの両方を単一の大災害で破壊される可能性から利用者を保護する。ただし、このようなメリットは、SaaS 提供者が自身の施設を壊滅的な打撃やその他の有害事象から保護していることが前提となる。オンサイトプライベートおよびコミュニティ SaaS クラウドにおいても、集中的管理により同様のメリットがもたらされるが、不測の事態が発生した場合の壊滅的損失に対しては、そのような不測の事態に対処するための計画を利用者が明確に立てていない限り、耐性(resilience)は劣る。SaaS アプリケーションの「オンデマンド」ネットワークアクセスは、環境によっては利用者がデータを携行する必要がないため、データの損失または盗難のリスクが軽減される可能性がある。アプリケーションのロジックによってサポートされる場合、遠隔でのデータ管理は他の利用者間との共有も容易にする。

5.3.4 クラウド提供者によって管理されるプラットフォーム関連事項

通常、外部委託型またはパブリック SaaS クラウドでは、クラウド提供者のインフラストラクチャの管理に利用者が関わる必要はない。例えば、どのようなオペレーティングシステム、ハードウェアデバイス、構成の選択肢、あるいはソフトウェアライブラリのバージョンが SaaS アプリケーションの下層にあるかを、利用者が意識する必要はない。とりわけクラウド提供者はバックアップ、システムメンテナンス、セキュリティパッチの適用、電力の管理、ハードウェアのリフレッシュ、物理的な施設のセキュリティなど、運用上の問題に責任を負う。プロバイダは、また、アプリケーションレベルで既知の悪用から保護するための現場サービスも提供する義務がある。さらに、利用者が、これらのタスクを実施するための自社内 IT サポートを維持する必要もない（ただし、利用者のブラウザを安全にネットワークにつなぐには、自社内 IT サポートが必要となる）。アプリケーションの新しい機能の実装と、それらの機能を実施するサーバー側のハードウェアの調達は SaaS 提供者が行うため、新しい機能の導入については SaaS 提供者が管理することになり、利用者側でそれらの新しい機能を使用するためにハードウェアシステムをアップグレードする必要はない。

5.3.5 初期費用の節減

外部委託型およびパブリック SaaS クラウドでは、設備を調達するための初期費用を負担することなく、利用者はアプリケーションの利用を開始できるが、利用料金が経常的に発生する。さらに、クラウド提供者は、個々の利用者よりも効率的に、かつ、拡張できる形でハードウェア、電力、およびその他のコンピューティングリソースを提供できなければならない。これが、（競争市場を想定すれば）利用者側のコスト削減の基礎をもたらす。購入とレンタルのどちらを選ぶかについての判断には、他のケースと同様に、予想される将来の価格を含む、コストに関するすべての考慮すべき事項について慎重な分析が必要となる。

5.4 問題と懸念

コンピュータとソフトウェアを各自に配布する従来のソリューションと比較すると、外部委託型およびパブリック SaaS クラウドでは、アプリケーションレベルのロジックが、クラウド提供者の施設でより多く実施される。すべてのシナリオで言えることだが、SaaS クラウドは利用者のブラウザがセキュアで、かつ信頼性が高いことに大きく依存する。これらの制約はいくつかの問題と懸念を生じさせ、SaaS に適したアプリケーションの種類に影響を与える。

5.4.1 ブラウザベースのリスクおよびリスク改善

ブラウザは、クラウド提供者との間の通信を暗号化するが、それでも巧妙な情報開示が行われる可能性がある。例えば、メッセージトラフィックが極端に多いまたは少ないこと、送信されたメッセージのサイズ、あるいは送信元の所在地から、一部の利用者にとって直接は関係ないものの重要な情報が漏れる可能性がある。また、堅固な暗号技術も誤った実装によりもろくなることがある。よくある誤りに、強度が低下する形で鍵またはパスワードを生成してしまい、その結果、総当りの推測攻撃に対して暗号技術が脆弱になるといったことが挙げられる。さらに、ブラウザが使用する暗号プロトコルに対する中間割込み(man-in-the-middle)攻

撃[Mar09]により、アタッカーが利用者のクラウドリソースをハイジャックすることも考えられる。これらのリスクはクラウド以外の環境にも当てはまるが、クラウドコンピューティングでは、エンドユーザであるクライアントアプリケーションとネットワークの安全性に対する依存度がより大きいと考えられる。

SaaS アプローチでは、ソフトウェアアプリケーションのインターフェースに関して利用者のブラウザに依存することになるため、利用者が悪質なウェブサイトにアクセスしてブラウザがウイルスに感染した場合、その後利用者が SaaS アプリケーションにアクセスするだけで利用者のデータが侵害されるといったリスクがある。別のリスクとして、利用者のウェブブラウザ内の利用者システム上に、異なる SaaS アプリケーションのデータが混在してしまうことが挙げられる。例えば図 9 では、クライアント C_1 がアプリケーション B と C を同時に稼働している。アプリケーション B と C が処理するデータによっては、それぞれのアプリケーションのデータを別々に保管することが重要になる。また、図 9 ではアプリケーション B と C が同一のクラウド提供者によって供給されているが、別のシナリオでは複数の異なる組織によって供給され、慎重なデータの隔離が必要になる場合がある。著名なウェブブラウザは、ウェブページ（およびウェブページに含まれる対話型プログラム）を互いに隔離するためのサンドボックスなどの機能を提供するが、サンドボックスはウェブブラウザが攻撃に対して強い耐性を有することに依存する。残念なことに、数々の競技会で証明されたように[Por10, Mar09]、ウェブブラウザは悪質なウェブサイトに対して脆弱であることが多い。この問題の回避方法の１つとして、複数のブラウザを用意して、その内の特定のブラウザを重要な SaaS アプリケーション専用とし、それらのブラウザを、攻撃に晒す可能性のある一般的な目的でのウェブサーフィンを行わないことが挙げられる別の回避方法として、クラウドのホストされたアプリケーションに接続する際に仮想デスクトップを使用することが挙げられる。そうすることで、クラウドに接続した状態で、他にアクセスできるモノとできないモノを制限するための厳格なポリシーによって管理される、完全に機能的な作業用プラットフォームが提供される。

5.4.2 ネットワークに対する依存

SaaS アプリケーションの可用性は、信頼性のある、継続的に利用可能なネットワークに依存する。パブリック SaaS クラウドのシナリオでは、クラウド利用者とクラウド提供者のいずれもネットワークの信頼性を保証することはできない。なぜならば、インターネットは彼らの管理下にないからである。外部委託型のプライベートまたはコミュニティ SaaS のシナリオでは、保護された専用の通信リンクを使用することによってネットワークのセキュリティと信頼性を実現できるが、費用がかかる。SaaS アプリケーションにはネットワーク故障時に処理を継続させるための「非接続モード」が含まれる場合があるが、SaaS の基本構成ではアプリケーションロジックがクラウド提供者のサーバー上で実施されるため、アプリケーションが実際に機能するかどうかは、アプリケーションが信頼できるネットワークにアクセスできるかどうかに左右されるだろう。

5.4.3 SaaS クラウド間の移行可能性の欠如

SaaS における移行可能性は、ある SaaS クラウドから別の SaaS クラウドにワークロードを移行する際に問題となる。データをエクスポート／インポートする際のフォーマットについては、SaaS クラウド間で完全な互換性が保証されていない。長い期間をかけてカスタマイズされたワークフローや業務ルール、ユーザインターフェースおよびアプリケーションの設定、支援スクリプト、データ拡張、アドオンも、プロバイダに固有のものであったり、容易に移行できない場合がある。

5.4.4 隔離対効率（セキュリティ対コストのトレードオフ）

図 9 に示されている実行リソース exr_1～exr_5 は抽象的であり、SaaS アプリケーションソフトウェアが SaaS 提供者によって実際にどのように実行されるか、また、利用者のために SaaS 提供者がソフトウェアを実行する方法が固定か可変かについては示されていない。図 11 に、そうした実行を成し遂げるための 1 つの方法のより具体的な図を示す（いくつかのオプションが[Cho08]に記載されている）。

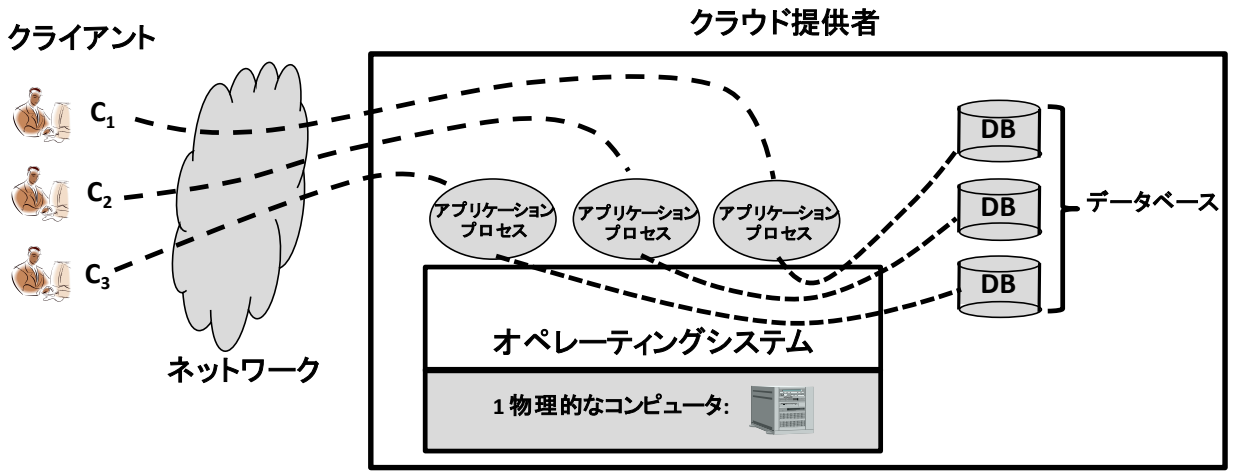

図11: SaaS における隔離対効率：隔離を重視したモデル

図 11 に示されているシナリオでは、クラウド提供者がクライアントごとにアプリケーションのインスタンス（アクティブなコピー）を個別に起動し、アプリケーションインスタンスが互いに干渉することなく単一の物理コンピュータ上に共存できるよう、必要に応じてそれらのインスタンスの設定を行っている。SaaS アプリケーションはクライアントの代わりにデータを保管する（あるいは、少なくとも選択された設定を保存する）ことが多いため、上の図には個々のアプリケーションインスタンスに接続された個々のデータベースシステムも示されている。基本的に、各クライアントにはアプリケーションのランニングコピーとデータストアが個別に割り当てられ、クライアント間の隔離はオペレーティングシステムによってもたらされる。隔離はオペレーティングシステムを使用してさまざま方法で提供できるが、それぞれの方法には隔離の強度と実施にかかる費用とのさまざまなトレードオフが伴う。異なる仮想マシン上で、または異なる物理コンピュータ上で各アプリケーションを稼働することによって、より高い信頼性が得られる可能性もあるが、そうしたアプローチでは費用も高くなる。図 11 の例では、単一の物理コンピュータが数人のクライアントに同時にサービスを提供することが可能だが、このアプローチではアクティブなクライアントごとに、アプリケーションのコピーとデータベースのオーバーヘッドコストが発生するため、費用はやはり高くなる。

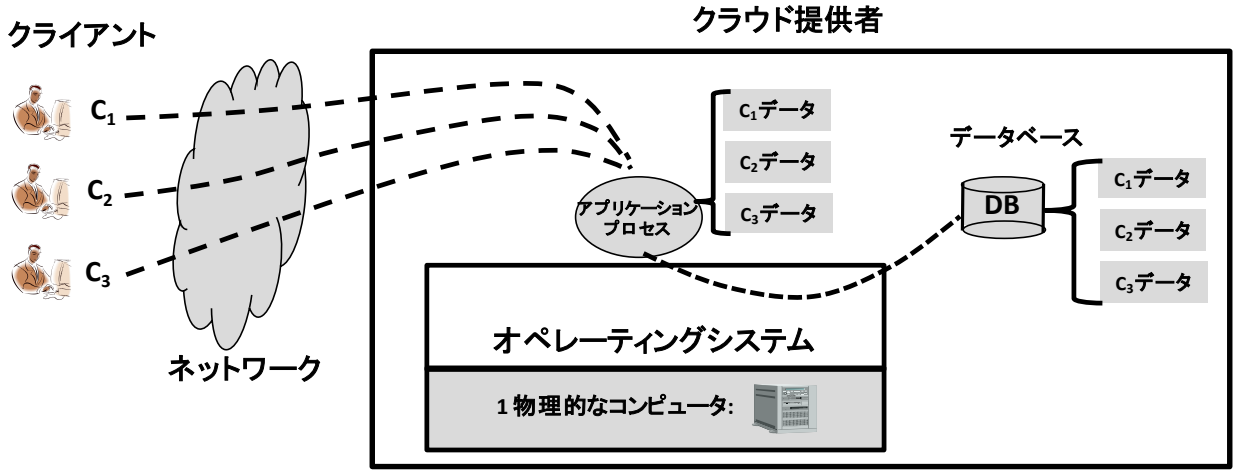

図12: SaaS における隔離対効率：効率を重視したモデル

図 12 に、より効率的なアプローチを示す。このアプローチでは、一体化されたデータベースにデータを保存し、複数のクライアントに同時にサービスを提供できるように、提供者が SaaS アプリケーションを改良して

いる。図 12 に示されている、クライアントの処理とデータの隔離のアプローチでは、アプリケーションが複数のクライアントに属するデータを同時に処理することも考えられるため、慎重なアプリケーション設計が必要となる。さらに、アプリケーションは、悪意のあるなしにかかわらず、1 人のクライアントの行為がパフォーマンスの低下を引き起こし他のクライアントに迷惑がかからないように、スケジュール問題を管理しなければならない。図 12 のアプローチは、単一のプログラムとデータベースをこのような方法で共有することで、クラウド提供者側のコストを削減する（利用者側のセキュリティリスクは増加するが）。処理とデータストレージが SaaS 提供者によってどのように実施されるかによって、考えられるその他の設計上のトレードオフがいくつか存在するため、注意が必要である。例えば、多くの異なる SaaS アプリケーションが、統合された単一のアプリケーションプロセスおよびデータストレージシステム上で並列に実行されることもある。さらに、実際のコンピューティングリソース（物理コンピュータ上で実行されているプロセス）をどのように調達するかは、SaaS 提供者のデータセンタから直接供給を受けることから、IaaS クラウド提供者からハードウェアをレンタルするに至るまで多岐にわたる。これら異なる種類のサービス構成は、利用者データの保護メカニズムと、クライアントのプログラムとデータの所在地に影響を及ぼすため、利用者ワークロードのセキュリティにも影響を与える。さらに、SaaS アプリケーション間に一定レベルの互換性と相互運用性がなければ、ワークロードの移行可能性は成立しない。SaaS アプリケーションの設計上のトレードオフに関する全般的な考察は、[Cho08] に記載されている。

5.5 候補となるアプリケーションクラス

SaaS アプリケーションは、期待される分量の利用者データをインポート／エクスポートするのに十分な帯域幅を持ち、遅延が少なく信頼の高いネットワークが備わっていれば、うまく機能する（ただし、サービス妨害などの悪質な攻撃を受けた場合を除く）。遅延やデータ転送速度といったパフォーマンス特性は、アプリケーションの種類によって異なる。例えば、以下に示す広い分野に数多くの SaaS サービスが存在する。

- **ビジネスロジック。**この分野におけるアプリケーションは、企業と、サプライヤー、職員、投資者、およびサービス加入者とを結びつける。これには、例えば、請求書の送付、資金の送金、在庫管理、およびサービス利用者管理がある。

- **協働。**この分野におけるアプリケーションは、組織内または組織間の、人によるチーム間の連携を支援する。これには、例えば、スケジュール管理システム、電子メール、画面共有、共同ドキュメントオーサリング、会議管理、およびオンラインゲームが含まれる。

- **職場の生産性。**この分野におけるアプリケーションは、ワードプロセッサー、表計算プログラム、プレゼンテーションプログラム、およびデータベースプログラムなどの、オフィス環境を代表するアプリケーションを実行する。これらのアプリケーションが SaaS として提供される場合、従来のオフィス生産性向上アプリケーションにはないコラボレーション機能を提供することが多い。

- **ソフトウェアツール。**この分野におけるアプリケーションは、セキュリティまたは互換性に関する問題を解決し、新規ソフトウェアの開発を支援する。これには、例えば、フォーマット変換ツール、セキュリティスキャンおよび分析、法令順守チェック、ならびにウェブ開発が含まれる。

重要なことは、SaaS 実装モデルは広範囲にわたって適用可能であり、上に列挙したもの以外のソフトウェアグループにも使用されていることを強調することである。インターネットの普及とパフォーマンスの向上により、SaaS はほぼ普遍的に適用されるようになった。しかしながら、以下の 3 つのクラスのソフトウェアは、パブリック SaaS に適さないだろう。

- **リアルタイムなソフトウェア。** 飛行管制システムまたは工場ロボット制御のように、タスク完了の正確なタイミングが求められるアプリケーションは SaaS に適さない。なぜならば、SaaS システムではレスポンス

タイムにばらつきがあり、SaaS 利用者とクラウド提供者間で送受信されるメッセージの往復遅延を通常は避けられないからである。

- **大量の利用者データ。** 医療機器のモニタリングまたはその他の身体的現象のモニタリングを行うアプリケーションなど、一部のアプリケーションでは、データが利用者の身体に関わるものであり、データ量も非常に大きくなる場合がある。そのような場合、データをリアルタイムに広域ネットワーク系経由で SaaS 提供者に送信できない可能性がある。

- **重要機能のソフトウェア。** ソフトウェアの障害により人命が失われたり、重要な財産が失われる可能性がある場合には、そのソフトウェアは「重要機能を持つ」とラベル付けされる。重要機能のソフトウェアの障害は、間違ったことをしたり、正しいこと行うのに時間をかけすぎる（あるいは早すぎる）ことによって発生する。重要機能のソフトウェアにおいて許容できる信頼性を確保することについては、現在研究が進められているが、主な設計アプローチの1つに、重要機能のソフトウェアの複雑さを軽減することがある。しかしながら、SaaS アプリケーションは、その性質上、ネットワークを含む大規模で複雑なソフトウェアスタックが正しく機能することに依存する。パブリック SaaS の場合、ネットワークをコントロールすることはできないため、ネットワークが許容レベルのサービスを提供し続ける保証はない。

これらの問題は、オンサイト SaaS、外部委託型 SaaS、またはコミュニティ SaaS のように、明確なネットワークプロビジョニングが実施され、ネットワークの品質が必要なレベルの保証をもって保障されるサービスを利用することによって、改善することが可能である。

さらに、利用者のディスプレーに対して高リフレッシュレートを要求するアプリケーションもある。SaaS は高リフレッシュレートをサポートするが、サポートできるリフレッシュレートは、SaaS 提供者と利用者間の距離が長くなるにつれて低下する。経験則的に、長距離ネットワークでは遅延が多く発生するため、高リフレッシュレートを継続的に実現することは難しいだろう。

5.6 SaaS に関する推奨事項

連邦政府の情報システム、および米国政府の代わりとなる他の組織によって運用される情報システムで SaaS システムを使用する場合には、2002 年施行の FISMA と、関連する NIST 標準および特定発行文書（例: FIPS199、FIPS200、SP800-53 など）が適用される。以下に、SaaS システムに関する追加の推奨事項を示す。

- **データの保護。** SaaS 提供者のデータ保護メカニズム、データロケーション設定およびデータベース編成／トランザクション処理技術を分析し、その SaaS アプリケーションを利用することになっている組織の機密性、法令順守、完全性および可用性のニーズが満たされているか否かを評価すること。

- **クライアントデバイス／アプリケーションの保護。** FIPS199 が定義する処理対象データの影響度レベルに準拠して、クラウド利用者のクライアントデバイス（例：ウェブブラウザが稼働しているコンピュータ）を保護し、攻撃にさらされないように管理すること。

- **暗号化。** 利用する SaaS アプリケーションがアプリケーション間のやりとりや転送されるデータの機密性を必要とする場合には常に、堅固なアルゴリズムと必要な強度を有する鍵の組み合わせによる強力な暗号化を用いてウェブセッションを確立するよう要求すること。また、保存されているデータについても、同様の措置を行うよう要求すること。連邦政府機関は、暗号化と電子署名に政府認可の暗号アルゴリズムを使用し、その実装は FIPS 140-2 に準拠しなければならない。暗号鍵がどのように管理され、誰がアクセス権を有するかについて理解すること。また、暗号鍵が適切に保護されるようにすること。

- **データの消去。** クラウド提供者に対して、利用者のリクエストに応じてデータを確実に消去するためのメカニズムの提供を要求すること。

6. プラットフォーム・アズ・ア・サービス(PaaS)環境

プラットフォーム・アズ・ア・サービス (PaaS)クラウドは、多数の利用者をサポートし、膨大な量のデータを処理できるよう構造化され、インターネット上のどのポイントからもアクセスできる可能性があるアプリケーションソフトウェアを適宜、開発、実装、管理するためのツールキットを提供する。通常、PaaS クラウドは高品質で拡張可能なアプリケーションの構築を容易にするための一連のソフトウェア構成要素と、プログラム言語や支援ランタイム環境などの一連の開発ツールを提供する。さらに、通常、PaaS クラウドは新規アプリケーションの実装を支援するツールも提供する。新規のソフトウェアアプリケーションを PaaS クラウドに実装することは、ウェブサーバーにファイルをアップロードするのと同じくらい容易であることもある。通常、PaaS クラウドは、利用者のアプリケーションの稼働に必要なコンピューティングリソース(例:処理能力、ストレージ、およびネットワーク)も提供・維持する。つまり、PaaS クラウドは、ソフトウェアアプリケーションをプラットフォームに合せて開発し、そのプラットフォーム上で実行できるという点で、従来のあらゆるコンピューティングシステム(すなわち、プラットフォーム)と似ている。

PaaS

誰がサービスを利用するか？

1. アプリケーション開発者、すなわち、アプリケーションのソフトウェアを設計し、実装する者。
2. アプリケーションテスター、すなわち、アプリケーションをさまざまな(場合によってはクラウドベースの)テスト環境で実行する者。
3. アプリケーション実装者、すなわち、完成した(あるいはアップデートされた)アプリケーションをクラウドに実装し、複数の異なるバージョンのアプリケーション間で生じる衝突を管理する者。
4. アプリケーションアドミニストレータ、すなわち、プラットフォーム上のアプリケーションのパフォーマンスを設定、調整し、モニタリングする者。
5. アプリケーションのエンドユーザ、すなわち、PaaS クラウド上に実装されたアプリケーションを利用する者。エンドユーザにとって、アプリケーションに対するアクセスは、SaaS クラウドを利用する場合と同じである。

利用者は何を得るか？ PaaS クラウド提供者が提供する、アプリケーションを開発、テスト、実装、管理するためのツールと実行リソースの利用。

利用料金はどのように算出されるか？ 通常は、利用者の数、利用者の種類(例:開発者か、あるいはアプリケーションのエンドユーザか)、ストレージ、処理能力、あるいは、そのプラットフォームが消費したネットワークリソース、処理されたリクエスト、およびプラットフォームの使用時間を基に算出される。

従来のシステムの場合と異なり PaaS は拡張可能なアプリケーションを作成するための基盤を開発者に提供する。パブリック PaaS クラウド向けアプリケーションには、(1) 大量のコンピューティングリソースを必要に応じて調達できる、(2) 大量のデータを必要に応じて処理できる、(3) ほぼ即座に実装できる、(4) IT に関わる多くの作業から利用者を解放する、および (5) 追加的に購入できる(従来のように設備や IT スタッフのトレーニングに初期費用をかけることもなく、使用に伴う料金を支払うだけで済む)といったメリットがある。外部委託型 PaaS クラウドも、外部委託の条件によって拡張性が制限される場合があるが、同様の機能を提供する。外部委託型でないプライベートまたはコミュニティ PaaS クラウド(第 4.2 章と 4.4 章を参照)では、データセンタのリソースによって拡張性が制限される。

以下の 6 つのサブセクションでは、PaaS サービスのいくつかの重要な特性である、抽象的な相互作用ダイナミクス、ソフトウェアスタックと、提供者／利用者によるコントロールの範囲、メリット、問題と懸念、候補となるアプリケーションクラス、ならびに推奨事項について説明する。

6.1 抽象的な相互作用ダイナミクス

PaaS クラウドの相互作用ダイナミクスを簡易化された（4 つのステップの）図で示すと、図 13 のようになる。図 13.A には、クライアント C_1 に代わって 2 つのアプリケーションを実行している PaaS クラウドが描かれている。図 13.A では、実装された 3 つのアプリケーションの現行のインベントリ("apps")を PaaS 提供者が保有している。クラウド提供者は一連の開発ツール（図中の「開発ツール」）と一連の実行環境（図中の「exr」で始まる文字列）も保有する。第 5 章で前述した SaaS 提供者の場合と同様に、実行環境は物理的なコンピュータであったり、仮想マシン（第 7 章に記載）であったり、あるいは、クライアントのリクエストを処理するサーバープログラムであったりする。そして仮想マシンを起動したり、コンピューティングサイクルとストレージを他の組織からレンタルすることさえも可能である。図 13.A には、2 つのアクティブなアプリケーション、B-> exr_1 と C-> exr_2 が描かれていて、（SaaS 環境の場合とまったく同じように）アプリケーション B と C が異なる実行環境で稼働しているのが示されている。

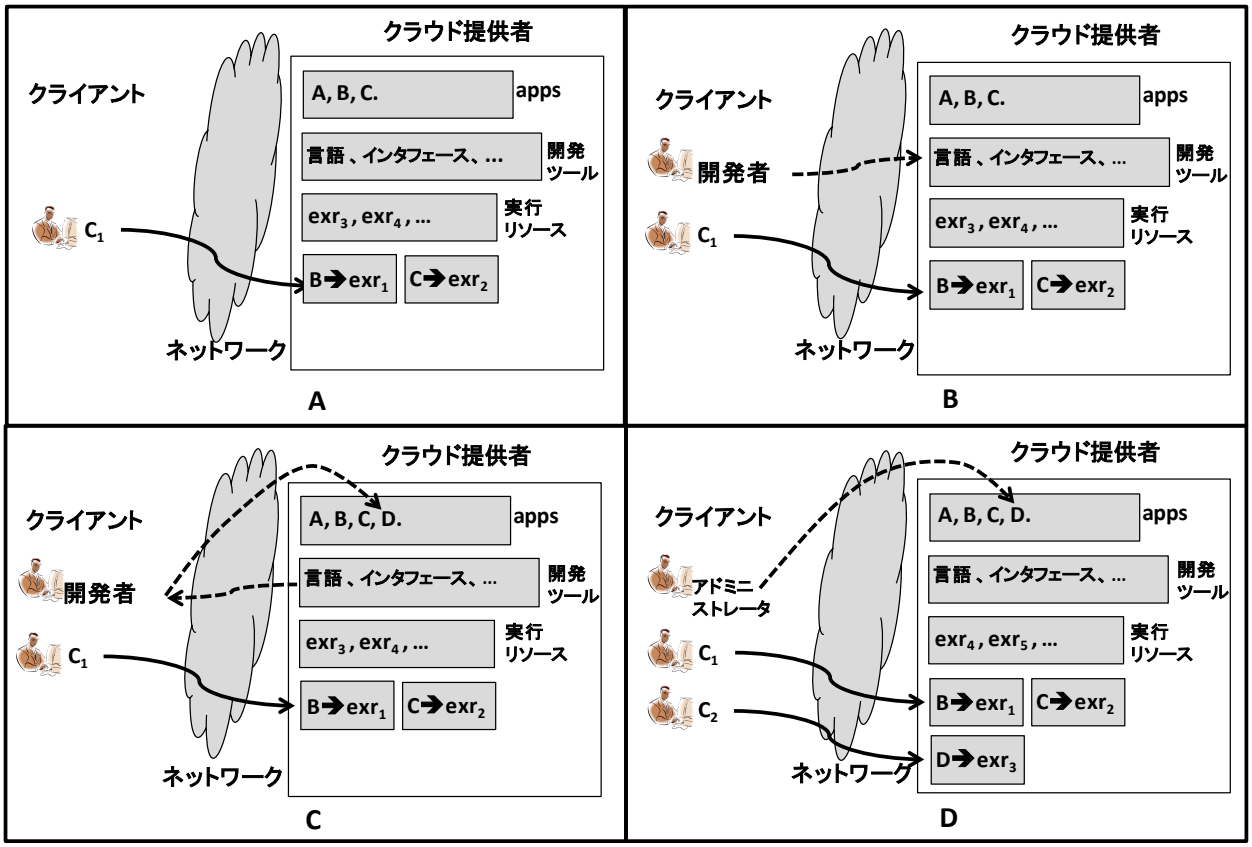

図13: PaaS における提供者／利用者間の相互作用ダイナミクス

図 13.B では、新規の開発者クライアントがクラウド提供者の開発ツールにアクセスしている。開発ツールには、例えば、プログラミング言語、コンパイラ、インターフェース、テストツール、およびこれらの工程を経た後にアプリケーションを実装するためのメカニズムが含まれる。

図 13.C は、開発者によるツールの利用を図解している。開発者は、ツールをダウンロードして自身のインフラストラクチャ内（すなわち、ローカル）で使用したり、単純にクラウド提供者のインフラストラクチャ内のツールにアクセスすることができる。いずれの場合も、開発者の行いによって生成されるのは、図で示されているとおり、クラウド提供者のインフラストラクチャに実装される新規のアプリケーション D である。

図 13.D には、利用できる状態になった新規アプリケーションの設定を行っているアドミニストレータと、新規アプリケーションを使用している新規クライアント C_2 が描かれている。

図 13 は、PaaS クラウドがどのように機能するかについて簡単に図解しているが、以下のような、PaaS クラウドの重要な側面も示している：PaaS クラウドは、ソフトウェアを開発し、ソフトウェアを実装し、ライフサイクル全体にわたってソフトウェアを稼働させることができるプラットフォームである。この基本的なシナリオには多くのバリエーションがある。例えば、開発者は新規のアプリケーションを作成する代わりに、既存のアプリケーションを修正してもよい。この場合、テスト、バージョン管理、廃棄フェーズを含むソフトウェア開発の通常のフェーズを省略できる。

6.2 ソフトウェアスタックおよび提供者／利用者が有するコントロールの範囲

PaaS では、より特権的な、ソフトウェアスタックの下位層に対するコントロールをクラウド提供者が有する。図 14 に、コントロールおよびマネジメントに関する責任の分担を示す。図の中央には、ハードウェア、オペレーティングシステム、ミドルウェア、およびアプリケーションの層から成る従来のソフトウェアスタックが描かれている。この図には、クラウド提供者と利用者のいずれか、または両方に対する責任の割り当ても示されている。

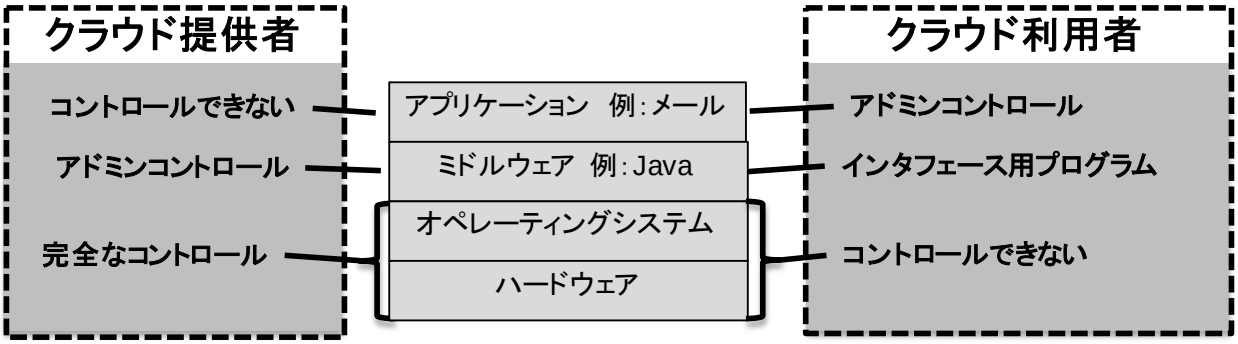

図14: PaaS におけるコンポーネントスタックおよびコントロールの範囲

クラウド提供者は最下層、すなわち、オペレーティングシステム層とハードウェア層を操作しコントロールする。ここに内在するのは、データセンタ間の LAN やルータなどのネットワークインフラストラクチャに対するコントロールである。ミドルウェア層では、利用者が利用できるプログラミングおよびユーティリティインターフェースがクラウド提供者によって提供される。これらのインターフェースは、利用者のアプリケーションが稼働する実行環境と、必要なリソース、たとえば、CPU サイクル、メモリ、不揮発性ストレージ、データストア、データベース、ネットワーク接続などに対するアクセスを提供する。クラウド提供者は、プログラミングモデル、すなわち、利用者のアプリケーションコードが実行状態になる条件を決定し、課金のために利用者プログラムの活動をモニタリングする。利用者がアプリケーションを実装・配備するために PaaS クラウドの装備を使用した時点で、アプリケーションは基本的に SaaS 実装（第 5 章に記載）と同一になる。第 3 章に記載されているように、クラウド提供者が利用規定に基づいてサポートを提供する範囲において、利用者はアプリケーション本体に対する管理的コントロールを実施できる。

6.3 メリット

パブリックおよび外部委託型 PaaS のシナリオでは、クラウド提供者がクラウドインフラストラクチャを低コストの場所に自由に設置することができ、利用者はオープンなインターネット経由でクラウドサービスにアクセスする。すべてのシナリオに当てはまるが、PaaS 提供者は図 14 が示すようにソフトウェアスタックのより下位の層に対するコントロールを保持することになるため、それらの下位層を管理することができ、PaaS 利用者はプラットフォームコンポーネントの選択、インストール、メンテナンス、運用といった責務からを開放される。PaaS が何らかの形でインフラストラクチャリソースを消費することから、PaaS サービスにはインフラストラクチャ料金が暗に存在するが、このインフラストラクチャ料金は PaaS の実行環境リソース（例：CPU、帯域幅、ストレージ）に対して課せられる料金に含まれる。

PaaS は、第 5.3 章で説明した SaaS のメリットの多くを共有する。

- ソフトウェアツールの占有面積が小さくて済む (5.3.1)、
- 管理とデータの集中化 (5.3.3)、
- クラウド提供者によって管理されるプラットフォーム関連事項(5.3.4)、および
- 初期費用の節減 (5.3.5)。

6.3.1 拡張可能なアプリケーションの開発と実装が容易である

PaaS は、アプリケーションを低コストで開発・実装するための手段を提供する。PaaS アプリケーションを開発し、そのアプリケーションをサーバー側はデータストアとサーバー側の処理フレームワーク（例: [Msf11-2, Goo11, Sal11, Red10, Ama12]）によって、クライアント側はシンクライアントと、とりわけブラウザベースの処理フレームワーク（例：[Gar05, Ado11, Goo11-2, Mic11, Dja11,]）によってサポートするためのさまざまなツールキットが存在する。これらのテクニックは、エンタープライズアプリケーションを開発・実装し、それらのアプリケーションの運用と、アプリケーションによって処理されるデータの集中的管理を維持する手段を組織に提供する。通常、PaaS アプリケーション開発フレームワークは、高レベルの拡張性をサポートするデザインパターンを提供するため、需要の大きな変動にもスムーズに対応できる、しっかりした PaaS アプリケーションの作成を可能にする。オンサイトのシナリオでは、拡張性が、利用者のデータセンタによって提供されるリソースに限定されるだろう。一方、外部委託型のシナリオでは、クラウド提供者の施設のリソースを利用することになり、オンサイトよりも多くのリソースを利用できる場合がある。とりわけパブリックのシナリオでは、しっかりした PaaS アプリケーションを多数の利用者向けに迅速に提供し、膨大な量のデータおよびプロセッシングサービスを提供することが可能である。

6.4 問題と懸念

第 5 章で説明した SaaS クラウドと同様に、PaaS クラウドでも、従来のコンピューティングソリューションと比較すると、より多くの割合でアプリケーションレベルのロジックがクラウド提供者の施設で実施される。また、PaaS 実装では、提供者システムとの間で信頼できるセキュアな接続を維持し、異なる PaaS アプリケーションおよびアカウント間の隔離を維持することに関して、重大な役割が利用者のブラウザ（あるいはシンクライアント）に課せられる。したがって、PaaS クラウドは、第 5.4 章で説明した SaaS に関する問題と懸念を共有する。

- ブラウザベースのリスクおよびリスク改善 (5.4.1)、
- ネットワークに対する依存 (5.4.2)、および
- 隔離対効率 (5.4.3)。

これ以外にも、PaaS クラウド特有の問題がいくつかある。

6.4.1 PaaS クラウド間の移行可能性の欠如

PaaS における移行可能性は、新規アプリケーションの開発時に、とりわけ、プラットフォームが独自の言語とランタイム環境を必要とする場合には問題になる。標準言語が使用されている場合でも、プラットフォームサービスの実装はクラウド提供者間で大きく異なる可能性がある。例えば、あるプラットフォーム上のファイル、キュー、またはハッシュテーブルインターフェースが、他のプラットフォーム上のものとは互換性がない場合がある。新規アプリケーションを作成する利用者は、特定のプラットフォーム提供者に特化した実装方法を編み出す代わりに、プラットフォームサービスに対する汎用のインターフェースを作成することによって、移行可能性のリスクを軽減してもよい。ただし、そうした戦略はコストが発生し、リスクも完全に軽減することはできない。なぜならば、提供者に特化したバリエーションを隠す汎用のインターフェースは、提供者特有の付加価値機能の使用を制限するため、アプリケーション機能は「最小限の待遇」しか受けられない。

6.4.2 イベントベースのプロセッサースケジューリング

PaaS アプリケーションには、HTTP メッセージからなるイベントによる、イベント駆動型である場合がある。こうした設計は、突出したリクエストがなければリソースはほとんど消費されないため、とりわけ費用効率が高い。しかしながら、この方式は、アプリケーションに対してリソースの制約をもたらす。つまり、コンピュータは、個々のリクエストに対して所定の時間内に応答するか、長くかかるリクエスト処理を続けるときは、生成されたメッセージをキューに入れて順次処理するからである。また、ローカルアプリケーションでは迅速に実行されるタスクも、PaaS アプリケーションでは同等のパフォーマンスを得られない可能性がある。

6.4.3 PaaS アプリケーションのセキュリティエンジニアリング

PaaS アプリケーションの開発者は、数々のセキュリティ上の危険を管理しなければならない。隔離された環境でローカルなリソースのみを使用して稼働できるアプリケーションの場合と異なり、PaaS アプリケーションは本質的にネットワークにアクセスする。さらに、PaaS アプリケーションは暗号技術を明示的に使用しなければならず、アウトプットを利用者に提供する一般のウェブブラウザのプレゼンテーション機能と情報をやりとりしなければならない。通常、PaaS アプリケーションは、例えば HTML, Java, JavaScript, XML, HTTP, .Net、ウェブリソースアーカイブフォーマットなどの複数の言語とフォーマットを使う必要がある。

6.5 候補となるアプリケーションクラス

PaaS ツールキットおよびサービスは、SaaS として使用できる多種多様なアプリケーションを開発するために使用できる。したがって、PaaS に適したアプリケーションクラスは、基本的には SaaS に適したアプリケーションクラス（第 5.5 章に記載）と同じである。

6.6 PaaS に関する推奨事項

連邦政府の情報システム、および米国政府のために運用される情報システムで PaaS システムを使用する場合には、2002 年施行の FISMA と、関連する NIST 標準および特定発行文書（例： FIPS199、 FIPS200、SP800-53 など）が適用される。クラウドコンピューティングサービスに関する共通の推奨事項は、第 9 章に記載している。利用者とクラウドプロバイダの役割と責任の分担について解説している付録 A も参照のこと。以下に、PaaS システムに関する追加の推奨事項を示す。

- **一般的なインターフェース。** パブリック PaaS クラウドプラットフォーム上で新規のアプリケーションを開発することを決定する前に、そのプラットフォームで提供されるアプリケーションインフラストラクチャイン

ターフェース（ファイル向け、キュー向け、ハッシュテーブル向けなど）が、そのアプリケーションの移行可能性と相互運用性をサポートするのに十分な一般性を備えているか、もしくは備えることが可能かを評価することが推奨される。一般的なンターフェースをサポートする PaaS クラウドの利用が望ましい。

- **標準的な言語およびツール。** 専有の言語とツールしか使えない PaaS システムが唯一の実際的な選択肢である場合を除き、標準の言語とツールを使用して作成できる PaaS システムを選択すること。
- **データアクセス。** できれば、標準のデータアクセスプロトコル（例：SQL）に対応した PaaS システムを選択すること。
- **データの保護。** PaaS 提供者のデータ保護メカニズム、データロケーション設定およびデータベース編成／トランザクション処理技術を分析し、その PaaS アプリケーションを利用することになっている組織の機密性、法令順守、完全性および可用性のニーズが満たされているか否かを評価すること。
- **アプリケーションフレームワーク。** 入手可能なら、セキュリティ上の脆弱性を軽減するための、アーキテクチャとツールをを持ったアプリケーション開発フレームワークを提供する、PaaS システムを選択すること。
- **コンポーネントのテスト。** パブリック PaaS クラウドプラットフォーム上に新規のアプリケーションを実装する（あるいは、場合によっては、PaaS クラウド提供者が提供する構成要素を使用してアプリケーションを構築する）ことを決定する前に、コンパイルフェーズに含まれるソフトウェアライブラリ、または実行フェーズにおいてコールされるソフトウェアライブラリが、機能とパフォーマンスの両方の観点から意図したとおりに機能することを確認すること。
- **セキュリティ。** PaaS アプリケーションが安全に稼働するように構成する（例：専用の VLAN セグメントを使用し、クライアントとサーバー間の通信には暗号技術を使用する）ことが可能であるか、また、識別および認可(identification and authorization)などの既存の企業／政府機関セキュリティフレームワークと統合でき、企業／政府機関セキュリティポリシーを適用できるかどうかを確認すること。
- **データの安全な消去。** クラウド提供者に対して、利用者のリクエストに応じてデータを確実に消去するためのメカニズムの提供を求めること。

7. インフラストラクチャ・アズ・ア・サービス(IaaS)環境

本章の目的は、インフラストラクチャ・アズ・ア・サービス (IaaS)クラウドのアーキテクチャと基本的な動作を示すことにある。この情報は、IaaS クラウドが特定の信頼性、法令順守、およびセキュリティ要求事項を満たすか否かを評価する必要がある読者、および IaaS クラウドサービスの動作の仕組みを理解したいと考える読者にとって重要である。ただし、重要なことは、パブリッククラウドの構成の多くは各々に固有であり、運用上の詳細は一般に公開されていないことに留意することである。

IaaS

誰がサービスを利用するか？

システムアドミニストレータ

利用者は何を得るか？

仮想コンピュータ、ネットワーク経由でアクセスできるストレージ、ファイアウォールなどのネットワークインフラストラクチャコンポーネント、およびコンフィギュレーションサービスに対するアクセス。

利用料金はどのように算出されるか？

通常、CPU 時間、1 時間当たりに保存されたデータ量（ギガバイト）、利用したネットワーク帯域、1 時間当たりに使用したネットワークインフラストラクチャ（例：IP アドレス）、使用した付加価値サービス（例：モニタリング、自動スケーリング）を基に算出される。

本章に含まれる技術情報は、以下の3つの情報源から抽出した情報である：(1) 一部のクラウド提供者が活用していることを公的に認めた「ハードウェアの仮想化」[Pop74]などの、一般向けに公開されている、基盤技術に対する技術的な取り組み、(2) 一般向けに公開されているクラウドシステムインターフェース（例：[Ama10, Ama06]）から抽出したインターフェース、および (3) 設計文書やソースコードを利用できるようにした、いくつかのオープンソースクラウドプロジェクトから得られた洞察（例：[Can11, Nas10, War09]）。したがって、本章では、IaaS クラウドがどのように動作するかを、特定の条件下ではなく一般的に、説明している。本章では、特定のクラウドコンピューティングプロジェクトを名前で言及しているが、これらの参考文献を推奨するわけではないことに留意すること。

以下の 6 つのサブセクションでは、IaaS サービスのいくつかの重要な特性である、抽象的な相互作用ダイナミクス、ソフトウェアスタックおよび提供者／利用者が有するコントロールの範囲、IaaS クラウドの運用面、メリット、問題と懸念、ならびに推奨事項について説明する。

7.1 抽象的な相互作用ダイナミクス

図 15 に、IaaS クラウド内の情報のやりとりの簡易化した図を示す。図 15A には、ネットワーク経由で IaaS クラウドとやりとりしているクライアントが描かれている。クラウド提供者は、クライアントに割り当てが可能な仮想マシン(vm)を数多く所有する。この図では、クライアント A が vm_1 と vm_2 に対するアクセスを有し、クライアント B が vm_3 に対するアクセスを有する。クラウド提供者は vm_4 から vm_n までを予備として保持しているが、ここで n は、いずれかのクライアントがリクエストすることが予想される、最高 vm 数を上回ると考えられる。図 15B は、新規クライアント C が、追加の 3 つの vm に対するアクセスをリクエストして受け取った直後の状況を示している。この時点で、クライアント C が vm_4、vm_5 と vm_6 に対するアクセスを有し、クラウド提供者は vm_7 から vmn までしか保持していないことになる。図 15 は、確かに、IaaS クラウドが実際にどのように機能するかを極めて簡単に示したものであるが、それでも、IaaS クラウドを機能させるために取り組むべき、いくつかの技術上の問題を示すには十分である。さらに、図 15 では、（提供者による）仮想マシンの割り

当てと、(利用者による)情報のやりとりのみが示されている。リリース時にデフォルト値にリセットされる、シンプルな仮想マシンのみを提供する IaaS クラウドを構築することも可能だが、そうしたクラウドは限られた機能しか持たないだろう。実用的な IaaS クラウドシステムは、不揮発性データストレージと、安定したネットワーク接続も提供する。それらのシステムは、金銭的コストが発生するリソースの使用を計測し、それらのコストを利用者に請求する必要がある。

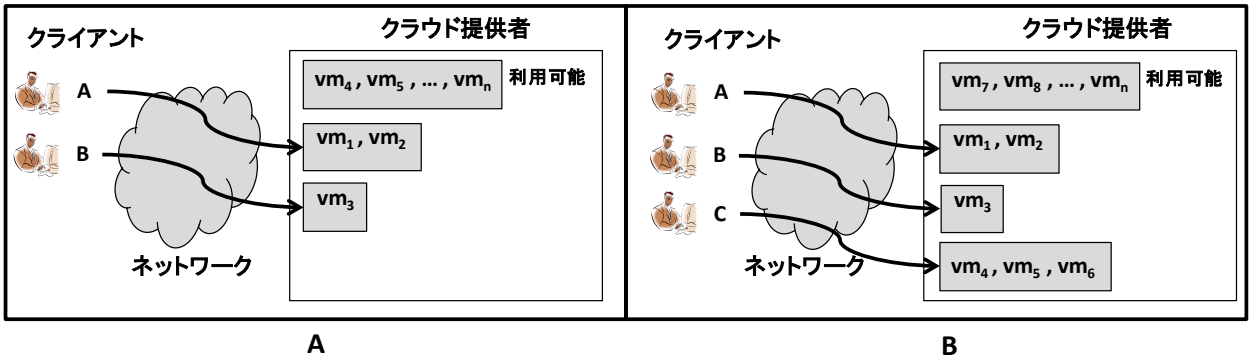

図15: IaaS における提供者／利用者間の相互作用ダイナミクス

7.2 ソフトウェアスタックおよび提供者／利用者が有するコントロールの範囲

IaaS では、より特権的な、ソフトウェアスタックの下位層に対するコントロールをクラウド提供者が有する。図 16 に、コントロールおよびマネジメントに関する責任の分担を示す。図の中央には、ハードウェア、オペレーティングシステム、ミドルウェア、およびアプリケーションの層から成る従来のソフトウェアスタックが描かれている。IaaS の場合、オペレーティングシステムによって通常は占められる層は、2 つの層に分割される。下位の(かつ、より特権的な)層は、ハイパーバイザとも呼ばれる仮想マシンモニター(VMM)によって占められる。ハイパーバイザはハードウェアを使用し、1 つまたは複数の仮想マシン(VM)を生成する。各仮想マシンは「実在するマシンの複製であり、実能力を備え、他と分離されている」[Pop73]。つまり、利用者が仮想マシンに対するアクセスをレンタルする場合、利用者にとっては仮想マシンが、ネットワーク経由でクラウド提供者に送信されるコマンドを介して管理(例:電源のオン／オフ、周辺機器の設定)できる、実在するコンピュータハードウェアのように見える。仮想マシン内で稼働するオペレーティングシステムは、ゲストオペレーティングシステムと呼ばれる。クラウド提供者がフルセットの仮想技術(NIST SP800-125 参照)を使用している場合、利用者はサポートされるオペレーティングシステムソフトウェアのうち、望ましいものを自由に仮想マシンにロードすることができる。

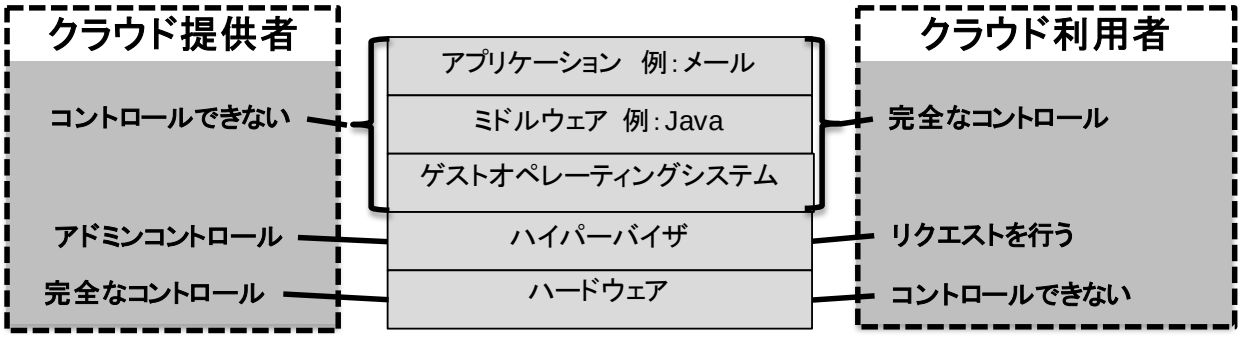

図16: IaaS におけるコンポーネントスタックおよびコントロールの範囲

図 16 に示されたように、クラウド提供者は物理的なハードウェアに対する総合的なコントロールと、ハイパーバイザ層に対する管理的コントロールを維持する。利用者は、クラウド（ハイパーバイザ層を含む）に対して、新規の仮想マシンの作成と管理をリクエストすることができるが、これらのリクエストはリソースの割り当てに関するクラウド提供者のポリシーに適合する場合にのみ、受け入れられる。通常、クラウド提供者はハイパーバイザを介して、ネットワーク機能に対するインターフェース（仮想ネットワークスイッチなど）を提供し、利用者はこれを使用して、クラウド提供者のインフラストラクチャ内のカスタム仮想ネットワークの設定を行う。通常、利用者は、各仮想マシン上のゲストオペレーティングシステムと、その上のすべてのソフトウェア層の操作に対する完全なコントロールを維持する。この構造は、ソフトウェアスタックに対するかなりのコントロールを利用者に与える一方で、これら従来からのコンピュータリソースをセキュリティと信頼性がを確保されるように運用、アップデートおよび設定する責任は、最終的に利用者が負うことになる。この構造は、これらの問題の多くが利用者に意識させることなく対処される SaaS と PaaS とは対照的である。

7.3 運用面

独自技術によるクラウドの提供者は、自身のシステムアーキテクチャまたはアルゴリズムに関する詳細な技術情報を公開しない。しかしながら、Eucalyptusソースコードに基づく 3 つのオープンソースシステム (Ubuntu Enterprise Cloud [War09], NASA Nebula[Nas10], Eucalyptus [Nur08, Nur08-2])は、特定のシステムアーキテクチャに関する詳細な技術情報を提供している。[14] 本章では、IaaSクラウドの構造と運用の論理的な図を示す。この論理的な図は、EucalyptusおよびUbuntu Enterprise Cloudプロジェクト関連の資料によって十分に知られているものである。[15] しかしながら、ここに示されるインフォーマルなモデルは、より抽象的かつ一般的である。このモデルは、IaaSクラウドサービスの提供についての直感的な制限(intuitive constraints)に基づいている。IaaSクラウドには、集中的な管理およびサービスを中断させることなくスケールアップする能力を維持する一方で、上述のリソースをパフォーマンスと費用効果の両方が満たされる形で提供することが求められる。これらの制約から、IaaSクラウドシステムにおける自然な 3 つのレベルの階層、すなわち、集中的な管理に責任を負う最上層、互いに地理的に離れている可能性のあるコンピュータクラスタの集合（大規模になる場合がある）の管理に責任を負う中間層、仮想マシンが作成されるホストコンピュータシステムの稼働に責任を負う最下層の存在が示唆される。

図 17 に、この階層化された抽象的なモデルを示す。最上層にあるのはクラウドマネージャである。マネージャは、ユーザアカウントと、クラウド内での高レベルのリソース割り当てに責任を負う。中間層にあるのは、クラスタマネージャである。クラスタマネージャは、多数のコンピュータと、それらのコンピュータ間の相互接続に責任を負う。最下層にあるのはコンピュータマネージャである。構成によっては、パフォーマンスを理由に分割され、いくつかのコンポーネントが並列に処理されたり、さらなる調整のためにより多くの中間層が導入されたり、あるいは、本モデルに示されたネットワークとは異なるネットワーク上にストレージが配置される場合がある。

[14] 他にも、Eucalyptus をベースとしないものを含むオープンソースプロジェクトが進行中である。
[15] これらのプロジェクトを推奨するわけではないことに留意願いたい。

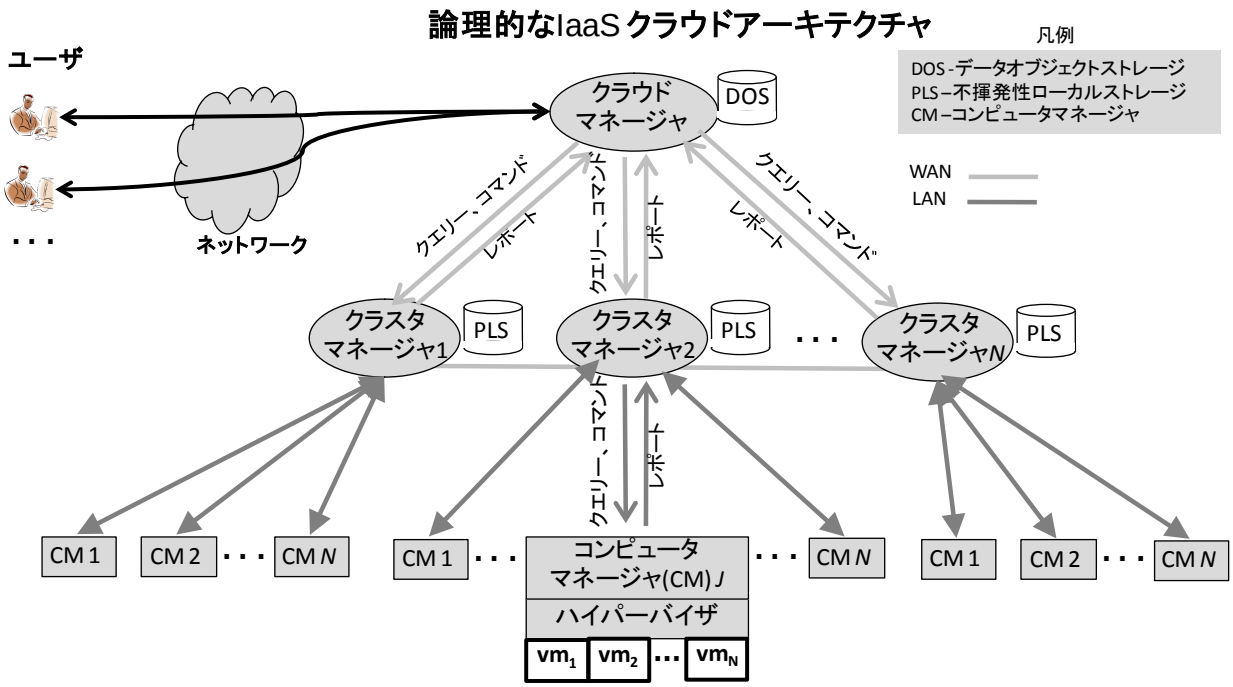

図17: ローカル IaaS クラウドアーキテクチャ

IaaS クラウドは動的にリソースをレンタルするためのコンピュータシステムである。通常、ユーザのクエリーとコマンドはシステムの最上層に投入され、それらのクエリーに答える、またはコマンドを実行する下位層へと転送される。ステータスレポートは利用者に向けて逆方向に流れる。通常、図 17 に示されたクラウドマネージャとクラスタマネージャは、IP ルータの高速ネットワークによって接続される。これは、クラウドが拡張するにつれて、新規のデータセンタの形で処理能力を追加する必要があることを反映している。これとは対照的に、コンピュータマネージャ間の通信は、局所的で非常に高速(例:10 ギガバイトのイーサネット)である傾向にある。クラウド内のこれらのすべてのリンクを高速のローカルネットワーク上に実装することを阻むものは何もないが、このアプローチではクラウドを拡張することができず、例えば自然災害などのサービスを中断させる局所的イベントに対して脆弱になる。同様に、クラウドを広域のリンク上に完全に分散させることを阻むものは何もないが、そうしたクラウドはパフォーマンス上の不利益を被る可能性がある。

以降の各サブセクションでは、クラウドマネージャ、クラスタマネージャ、およびコンピュータマネージャの 3 つの主な層の働きについての要約を示す。

7.3.1 クラウドマネージャの働き

クラウドマネージャはクラウドに対するパブリックアクセスポイントであり、利用者はこのポイントからアカウントにサインアップし、自身がクラウドからレンタルするリソースを管理し、クラウドに格納されているデータにアクセスする。クラウドマネージャには、利用者認証メカニズムと、仮想マシンとやりとりする際に利用者が採用するアクセス認証情報(例:暗号鍵)を生成し確認するためのメカニズムが含まれる。クラウドマネージャは、トップレベルのリソース割り当ても行う。利用者がいくつかのリソースをレンタルするためにコマンドを発行した場合、クラウドマネージャは、そのリクエストを満たすのに十分な未使用のリソースがあるか、また、そうだとしたら、そのリソースの一部または全部をどのクラスタマネージャ(もしくはマネージャ)が所有しているかを判断しなければならない。リクエストが通った場合、クラウドマネージャは、参加しているクラスタマネージャ上のリソースの割り当てを行い、仮想ネットワークのセットアップの調整を行い、利用者がすべてのリ

ソースに均一にアクセスできるようにする。クラウドマネージャは、リソースのリクエストに関するクラウドグローバルポリシーも実施することになるだろう。

図 17 には、クラスタマネージャとの間の調整に加えて、クラウドのデータオブジェクトストレージ（DOS）のレポジトリに接続されたクラウドマネージャも描かれている。実際の実装では、DOS は分散されるか、あるいは異なるネットワーク上に設置される。しかしながら DOS サービスは、クラウド内で稼働している仮想マシンと、クラウドの外部のシステムの両方から利用できなければならず、有効な利用者 ID を記録し、正規の利用者に DOS に対する管理行為を許可し、請求を可能にするためにも、クラウドマネージャとの十分な調整が必要になる。これらの制約が意味するものは、DOS とクラウドマネージャとの間に緊密なつながりがあり、かつ、DOS が広域ネットワークを介して稼働中の仮想マシンと外部システムの両方にアクセスするといった構造である。

7.3.2 クラスタマネージャの働き

各クラスタマネージャは、高速のローカルエリアネットワークによって接続されるコンピュータの集合を運用することに責任を負う。コンピュータクラスタは、数百または数千のコンピュータを含む可能性がある。クラスタマネージャは、リソースの割り当てに関するコマンドやクエリーをクラウドマネージャから受け取り、そのコマンドの一部もしくは全部をクラスタ内のコンピュータのリソースを使って満たすことができるか否かを計算する。クラスタマネージャは、クラスタ内の各コンピュータのコンピュータマネージャに問い合わせて、リソースの可用性を判断し、リクエストの一部もしくは全部をクラスタ内で満たすことができるか否かについてのメッセージをクラウドマネージャに返す。その後、クラウドマネージャから指示があった場合、クラスタマネージャはコンピュータマネージャに対して、リソースの割り当ての実施と、均一のアクセスを利用者に与えるための仮想ネットワークインフラの再設定を指示する。

図 17 には、LAN リンクを介して個々のコンピュータに接続することに加えて、不揮発性ローカルストレージ（PLS）に接続されている各クラスタマネージャも描かれている。上述したように、仮想マシンは、割り当ての解除とその後の再割り当ての間にも作業内容が保持されるよう、不揮発性のディスクのようなストレージを必要とする。このストレージは、仮想マシンに対する高速接続が可能な場所に設置するのが最も自然であるが、ストレージが特定のコンピュータシステムに固定的につながるような場所であってはならない。

7.3.3 コンピュータマネージャの働き

階層の最下層にあるコンピュータマネージャは、クラスタ内の各コンピュータシステム上で稼働するハイパーバイザと連携する。コンピュータマネージャは、クラスタマネージャからのクエリーに応じて、稼働している仮想マシンの数と、追加で起動できる仮想マシンの数を含む情報を返す。コンピュータマネージャは、クラスタマネージャから発行されたコマンドに応じて、ハイパーバイザのコマンドインターフェースを使用して仮想マシンを起動、停止、一時停止、再設定し、ローカルの仮想ネットワークの設定を行う。ハイパーバイザの技術によっては、同一のハイパーバイザ上で稼働する異なる仮想マシン間で送受信されるネットワークパケットを、高性能のメモリ内メッセージに実装することによって、パフォーマンスを向上させることが可能である。コンピュータマネージャは、そうした最適化の設定に責任を負う。上述したように、異なる利用者のために稼働する仮想マシンは、見かけ上互いに独立していなければならない。各コンピュータシステムのコンピュータマネージャは、ハイパーバイザの機能を使用してこの有用な幻想を最大限に作り出すことに責任を負う。

図 17 に図解されているように、IaaS クラウドの運用は、利用者のリクエストが階層の最上層に投入され、下位層に転送されてから、レスポンスが利用者に返されるまでの、周期的なプロセスである。仮想マシンの運転に加えて、利用者は、クラウド内のデータストレージサーバーに直接アクセスすることができる。ユーザ需要の合計値の山谷は個々の利用者の需要の山谷よりも緩やかであるにも拘らず、クラウドが十分に利用されない場合もある。コンピュータシステム間、さらにはクラスタ間の利用者ワークロードの移行は一つの戦

略手段で、利用者のワークロードを使用率が高い一連のコンピュータ上に集中させて他のコンピュータの電源をオフにすることによって運用コストの一部を削減することや、あるいはメンテナンス作業を実施できるようにすることができる。図 17 には、コンピュータシステムとネットワークの静的構造が示されているが、実際には物理的ハードウェアは劣化したり、故障したりすることがあるため、クラウドの構造とアルゴリズムには、広範囲にわたってサービスを中断させることなくハードウェアの交換を可能にすることが求められる。仮想マシンに内在する移動性は、ハードウェアの交換といった不可欠なニーズに対応するための重要な手段であることに留意願いたい。さらに、クラウド提供者は仮想化を使用して、クラスタ内にコンピュータを追加する形で、あるいはクラスタを追加する形で透過的に新たな処理能力を追加することによって、クラウドサービスの需要の増加に対処することができる。

7.4 メリット

SaaS クラウドや PaaS クラウドと同様に、パブリックおよび外部委託型 IaaS シナリオでは、クラウド提供者がクラウドインフラストラクチャを低コストの場所に自由に設置することができ、利用者はオープンなインターネット経由でクラウドサービスにアクセスする。低コストのインフラストラクチャによるコストの節減は、サービス料金の引き下げという形で、利用者との間で共有されるだろう。さらに、パブリックおよび外部委託型 IaaS クラウドは、パブリックおよび外部委託型 SaaS クラウドや PaaS クラウドと同様に、初期費用の節減を可能にする。

- 初期費用の節減 (5.3.5)。

通常、IaaS ではシステムの管理責任が、SaaS または PaaS よりも多く利用者に課せられる。利用者は仮想マシンおよび仮想化されたインフラストラクチャを管理し、システムアドミニストレータとしての作業を実施する必要がある。クラウド提供者が丁寧に構築されたオペレーティングシステムイメージとサービス、複製機能つきストレージ、暗号技術、ファイアウォール、モニタリング、需要に基づく仮想マシンの自動スタートアップ／シャットダウン機能などを提供する場合があるが、ハイパーバイザ上のすべてのソフトウェア層の運用に対する責任は、主に利用者側にある。これは、利用者のスキルセットや特定のニーズによってメリットにもなれば、懸念事項にもなる。

以降の各章では、主なメリットについて説明する。

7.4.1 仮想マシンに対する管理的アクセスを介した、コンピュータリソースの完全コントロール

通常、IaaS クラウドリソースに対する利用者からのアクセスは、第三者による傍受または改ざんを防ぐため暗号技術を使用する標準ネットワークプロトコルを使って行われる。ネットワークを経由したクラウドリソースに対するアクセスは、基本的に 3 つの異なる形式をとる。すなわち、(i) 利用者がクラウド提供者に対して管理コマンド、例えば、仮想マシンを稼働するための、またはデータをクラウドのサーバーに保存するためのリクエスト、を発行する、(2) 稼働中の特定の仮想マシンに対する管理的アクセスを行う利用者（すなわち、現時点でそれらの仮想マシンをレンタルしている利用者）が、それらの仮想マシンに対して管理コマンド、例えば、仮想マシン上でウェブサーバーを起動するための、または新規のアプリケーションをインストールするためのコマンドを発行する、および (3) 仮想マシンに対するパブリックネットワークインターフェースに対するアクセスを行うあらゆる利用者（匿名の利用者を含む場合がある）が、利用者が以前に使用可能にした仮想マシン上で稼働するネットワークサービスを利用する。1 つの例として、UNIX 型の仮想マシンでは、通常、管理的アクセスを行う利用者が管理特権アカウントを持ち、セキュアシェル(Secure Shell)などのネットワークプロトコルを介してアクセスする[Ylo06]。

7.4.2 コンピュータハードウェアの柔軟かつ効率的なレンタル

基本的に、クラウドコンピューティングは、コンピュータリソースをレンタルするサービスである。これらのリソースは、通常、ネットワーク経由で利用者によってアクセスされ、利用者各々に個別に割り当てられるユニットで計測され、、利用者がリソースを占有している時間の長さに基づいて課金される。IaaS クラウドの場合、割り当てられるリソースの主なユニットは仮想マシン、ネットワーク帯域、ストレージ、および IP アドレス（に対する管理的アクセス）である。これ以外のリソースには、モニタリングサービス、ファイアウォール、キューなどの同期化メカニズム、データベースなどが含まれる。仮想マシンに対する管理的アクセスを有することの大きな強みは、利用者が望むほぼすべてのソフトウェア（カスタムオペレーティングシステムを含む）を実行できることである。

パブリックおよび外部委託型 IaaS クラウドは、ハードウェアに直にアクセスする機能を提供するのに加えて、多数の仮想マシンまたはその他のクラウドリソースを即座にレンタルし開放する能力も提供する。これにより利用者は、大規模ネットワークを迅速にセットアップして利用者が選択したソフトウェアを稼働することができ、結果として必要なハードウェアの購入と維持に費用をかけることなく、大きな問題を解決することができる。

7.4.3 レガシーアプリケーションの移行可能性と相互運用性

IaaS クラウドは、利用者が選択したオペレーティングシステムを利用者がインストールし走らせることを可能にするため、レガシーアプリケーションと IaaS クラウド内のワークロード間の高レベルの互換性を保つことができる。例えば、自身が所有するサーバーのハードウェア上で通常稼働させている従来型のネットワークアプリケーション（例：ウェブサーバー、電子メールサーバー、データベース）のうち、ほとんどすべてのネットワークアプリケーションを IaaS クラウド内の仮想マシンから起動できる。さらに、エンドユーザ向けアプリケーションの多くについても、仮想デスクトップ技術によって、IaaS クラウド内で稼働させることが可能である。アプリケーションの多くは、仮想マシンにスピーディに移行できるが、そうでないアプリケーションもある。例えば、特定のハードウェアサポートを必要とするアプリケーションは、移行には向いていない。

7.5 問題と懸念

第 5 章で説明した SaaS クラウドや PaaS クラウドと同様に、IaaS クラウドはセキュアで信頼性の高いネットワークに依存し、また、アカウントの管理にセキュアで信頼性の高いブラウザに依存することが多い。

- ネットワークに対する依存性 (5.4.2)、および
- ブラウザベースのリスクおよびリスク軽減（5.4.1）

さらに、IaaS クラウド特有の問題がいくつかある。

7.5.1 レガシーなセキュリティ上の脆弱性との互換性

IaaS クラウドは、利用者がレガシーソフトウェアシステムをクラウド提供者のインフラストラクチャ内で稼働することを可能にするが、この場合利用者は、それらのレガシーソフトウェアシステムのセキュリティ上のすべての脆弱性に晒される。

7.5.2 仮想マシンの不規則な広がり

IaaS クラウドは、利用者が多くの仮想マシンを生成し、場合によってはさまざまな状態（例：実行、一時停止、休止）で保持することを可能にする。アクティブでない仮想マシンは、重要なセキュリティアップデートに

関して遅れをとる可能性がある。仮に、古くなった仮想マシンがアクティブになった場合、そうした仮想マシンは侵害される可能性がある。原理上は、クラウド提供者が利用者の代わりにアクティブでない仮想マシンをアップデートすることが可能だが、そうしたアップデートのメカニズムは複雑であり、通常、セキュリティアップデートの維持管理は利用者側の責任になる。

7.5.3 IaaS クラウド提供者のウェブサイトが本物であるかを確認する

第 7.2 章で概説した機能は、IaaS クラウド提供者のリソースに対するセキュアなセッションの確立を可能にするが、例えば第三者による認証サービスなど、何らかの手段を使ってクラウド提供者のウェブサイトが本物であるかを確認する責任は、利用者側にある。通常、利用者のブラウザは、公開鍵暗号[Mar08, Die08] を使用して、クラウド提供者に対するプライベートリンクを確立するだろう。ただし、クラウドのウェブサイトの身元を確認して、プライベートリンクが偽のサイトにつながっていないことを確かめるのは、利用者側の責任になる。

7.5.4 仮想マシンレベルの隔離の堅牢性

図 15 に図解されているように、仮想マシンは共有のリソースの集積から異なる利用者に割り当てられる。利用者は、他の利用者（悪意を持っている場合がある）による傍受または改ざんの可能性から保護されなければならない。つまり、利用者は、ネットワークを介してやりとりすることを望む場合を除き、互いに独立していなければならない。通常、IaaS クラウドは、（ソフトウェア層である）ハイパーバイザを、仮想化をサポートするハードウェア（例：AMD-V や Intel VT-x）と組み合わせて使用することにより、それぞれの物理的なコンピュータを複数の仮想マシンに分割する。仮想マシンの隔離は、ハイパーバイザの正しい実装と設定に依存する。ハイパーバイザによって提供されるハードウェアの仮想化[Per08]は、独立した、またはサンドボックス機能を備えたコンピュータ環境を提供するために広く用いられている技術であるが、高度な技術を有する攻撃者が存在する状況においては、隔離の強度は上未解決の研究課題となる。

7.5.5 隔離をもたらすための動的なネットワーク設定機能

図 15 からは明らかでないが、稼働中の各仮想マシンをサポートするネットワークインフラストラクチャ(例：ルータ、ケーブル、ネットワーク帯域など)も、ネットワークリソースの共有の集積から割り当てられる。仮想マシンがクラウドによって利用者に割り当てられた時、仮想マシンがその利用者と通信し、場合によってはインターネット上の任意の外部エンティティとも通信できるよう、ネットワークパスをクラウド提供者のインフラストラクチャを介して構成しなければならない。利用者間の望ましくない相互作用を防ぐために、クラウド内でいずれかの利用者によって送信されたパケットが他の利用者の目に止まる事がないようにしなければならない。また各利用者が期待されるレベルのサービスを受けられるように、十分な帯域幅が確保されるようにしなければならない。通常、仮想マシンは、ほんの数分間で割り当てられる。対応するネットワーク設定も同程度に速やかに実施されなければならない。仮想 LAN（VLAN）やオーバーレイネットワークなどのいくつかの技術は、論理的にネットワークトポロジーが見えるようにし、迅速な再構成わ可能にする。異なる利用者に属するネットワーク間の干渉を防ぐためには、これらの機能の慎重な設定が（および、おそらくハイパーバイザにおけるサポートも）必要となる。

7.5.6 データ消去の実施

仮想マシンは、クラウド提供者によって維持管理されるディスクリソースにアクセスする。利用者がそうしたリソースを開放した時、クラウド提供者は、そのリソースを次にレンタルする者から、前利用者の残存データが見えることがないようにしなければらなない。強力なデータ消去ポリシー（例：ディスクブロックを数回にわたって上書きする）の実施は多くの時間を要し、利用者が変わる時には高いパフォーマンスは望めないと考えられる。データの複製およびバックアップの実行も、データ消去作業を複雑にする。

7.6 IaaS に関する推奨事項

連邦政府の情報システム、および米国政府の代わりとなる他の組織によって運用される情報システムで IaaS システムを使用する場合には、2002 年施行の FISMA と、関連する NIST 標準および特定発行文書（例: FIPS199、FIPS200、SP800-53 など）が適用される。クラウドコンピューティングサービスに関する共通の推奨事項は、第 9 章に記載している。利用者とクラウドプロバイダの役割と責任の分担について解説している付録 A も参照のこと。以下に、IaaS システムに関する追加の推奨事項を示す。

- **複数利用者による共同利用。** IaaS クラウド提供者が仮想マシンの形でコンピューティングリソースを提供するに際して、(a) 同一の物理ホスト上の他の仮想マシンからの攻撃、(b) 物理ホストからの攻撃に加えて、(c) ネットワークを介した攻撃から仮想マシンを保護するためのメカニズムを、クラウド提供者が実施していることを確認すること。攻撃の検知・防止メカニズムの典型的な例には、仮想ファイアウォール、仮想 IDS/IPS などに加えて、VLAN などのネットワーク分割技法が含まれる。
- **データの保護。**IaaS 提供者のデータ保護メカニズム、データロケーション設定および処理技術を分析し、そのプロバイダのインフラストラクチャを利用することになっている組織の機密性、法令順守、完全性および可用性のニーズが満たされているか否かを評価すること。
- **データの安全な消去。** クラウド提供者に対して、利用者のリクエストに応じてデータを確実に消去するためのメカニズムの提供を求めること。
- **管理的アクセス。** IaaS クラウド提供者から仮想マシンまたは物理サーバーの形でコンピューティングリソースをレンタルする場合、（利用者組織の）トレーニングを受けた／信頼のおけるユーザの範囲に対してのみ、それらのリソースに対する管理的アクセスを与えること。
- **仮想マシンの移行。**仮想マシンとそれに対応するストレージの、将来の代替クラウド提供者間の移行についての戦略を策定すること（例：OVF 標準は、そうした戦略の部分的なベースとなりうる）
- **仮想化の最良慣行。** 従来型のシステムおよびネットワークの管理についての最良慣行（ベストプラクティス）と、仮想化の利用についての最良慣行（すなわち、NIST SP800-125『Guide to Security for Full Virtualization Technologies』）に従うこと。

8. 未解決の問題

クラウドコンピューティングは、IT サービスのすべての利用者にとってのソリューションであるわけではなく、すべてのアプリケーションに適しているわけでもない。新興技術であるクラウドコンピューティングは、いつくかの問題を含んでいて、そのすべてがクラウドに固有のものではなく、IT をホストするすべてのサービスにとって懸念となるものもある。本章の目的は、ローカルで管理される IT コンピューティングサービスと外部委託型の IT コンピューティングサービスの両方における未解決の問題に、クラウドコンピューティングがどのように関連するかを読者に示すことにある。

これらの問題の一部は従来の分散型コンピューティングに関するトピックでもあり、数十年にわたって未解決のままであるが、クラウドコンピューティングの登場により、今ではより身近な問題になっている。その他の問題はクラウドコンピューティングに特有のものと考えられる。

複雑なコンピューティングシステムは、障害やセキュリティ侵害に遭いやすい。さらに、同時並行性、動的設定、および大規模な計算処理などの、複雑な要求事項に対応しなければならないソフトウェアは、従来の商用グレードのソフトウェアよりも高い欠陥の密度を示すと考えられる。このことを考慮すると、クラウドシステムは、すべての複雑なコンピューティングシステムと同様に欠陥を含み、障害やセキュリティ侵害に遭うこともあることを理解することが重要になる。だからといって、クラウドシステムが重要な業務を実施するのに向いていないわけではないが、クラウドを広範囲に適用する際には、障害を検知し、そのもたらす結果を把握し、その影響を遮断し、それらから回復するための技術が重要となる。

クラウドコンピューティングには、コンピューティングリソースの迅速なリース提供を通じて、より効率的なマーケットを育成できる可能性がある。クラウドコンピューティングを使用することで、利用者は、さまざまなサービス料金と引き換えに資本支出（例:コンピューティングセンターを社内に構築するための）から解放される。したがってクラウドは、利用者に、IT 関連の資金支出の削減の可能性をもたらす。クラウド提供者の観点からすれば、クラウドコンピューティングは、初期投資後に、資本支出の効果でプラスの収益流入となって還ってくることを可能にする。こうしたことは、よく知られている経済的概念であるが、ネットワークおよびシステム構成の複雑さに加えて、データおよびソフトウェア資産を外部の者に触らせることによる通常のリスクが伴う。

約束した品質のサービスを提供するための技術手段は、通常、利用者には開示されない。このため、約束された品質のサービスが提供されていることを利用者がどのように確認するのか、といった問題が浮上する。さらに、市場の効率は、複数のサービスを実際に比較することを利用者ができるかどうかにかかっている。サービス契約のすべてが標準の評価指標、技術、および語彙に準拠しているわけではないため、それは難しい。

要するに、クラウドコンピューティングはさまざまな問題を提起し、それらの問題は本章の残りの部分で扱う 5 つの分野、すなわち、コンピュータ性能（第 8.1 章）、クラウドの信頼性（第 8.2 章）、経済的目標（第 8.3 章）、法令順守（第 8.4 章）、および情報セキュリティ（第 8.5 章）に分類することができる。

8.1 コンピュータ性能

求められるシステム性能のレベルは、アプリケーションの種類によって異なる。例えば、電子メールの場合、通常、短時間のサービスの中断には耐えられるが、工業オートメーションやリアルタイムな処理では、通常、高いパフォーマンスと高いレベルの予測可能性の両方が求められる。クラウドコンピューティングには、パフォーマンス関連のいくつかの課題が伴い、それらは、他の分散型コンピューティングのパフォーマンス関連の課題と異なるとは限らない。しかしながら、これは注目に値する。

8.1.1 遅延

遅延とは、リクエストを処理する際にシステムが経験する時間的な遅延のことをいう。クラウド利用者が経験する遅延には、通常は少なくとも1つのインターネットの往復時間、すなわち、リクエストメッセージがクラウド提供者にたどり着くまでの時間と、レスポンスメッセージを利用者が受け取るまでの時間の合計が含まれる。通常、インターネットの往復時間が単純な予測できる数値であるわけではなく、一定の幅を持った値であって、混雑、誤った構成、または障害に起因する数多くの変数の合成である。これらの要因については、クラウド提供者または利用者がコントロールできないことが多い。しかしながら、広域ネットワークの最適化技術やウェブアプリケーションを加速化させるサービスもあり、これらを許容できないパフォーマンスの改善に使用することができる。アプリケーションがそうした環境に適しているか否かの判断には、そのアプリケーションの重要度、ネットワークサービスのレスポンスタイムの変動に対して備わっている耐性、事後に適用可能な是正措置についての慎重な分析が必要となる。この最後のステートメントは、クラウドに限ったことではないことに留意すること。

8.1.2 オフラインでのデータの同期化

クラウドに保存されているドキュメントに対するアクセスは、利用者がネットワークに接続できない場合には問題になる。ドキュメントがクラウドに保存されていて、利用者がオフラインになっている間に、ドキュメントの同期化とデータの処理を行えることが、とりわけ SaaS クラウドでは望ましい。そうした同期化を実現するには、バージョン管理、グループ間の協力、およびクラウド内のその他の同期化機能が必要となる場合がある。

8.1.3 拡張可能なプログラミング

MapReduce [Dea04]、BigTable [Cha06]、あるいは拡張可能なキューサービスなどのツールキットを使用する「大規模な」プログラミングでは、アプリケーション開発作業の新たな検討が必要となる。追加のコンピュータ能力を動的にリクエストする機能により、グリッドコンピューティングや並列処理などのよく研究されたコンピュータモデルを科学研究所内に留めず、より一般的なコンピュータ使用にも適用することが可能になる。クラウド利用者は、データの並列処理とタスクの並列処理を通じて、追加のコンピュータ能力をうまく利用できると同時に、コンピュータを駆使したタスクを遂行するためにクラウドを拡張できる。しかしながら、オンデマンドで調達可能な新規のコンピュータ能力のメリットを最大限に引き出すには、アプリケーションを改良する必要があるだろう。

8.1.4 データストレージの管理

クラウド環境におけるデータストレージについて考える場合、利用者は、(1) オンデマンドで追加のストレージ容量を供給する、(2) 保存されているデータの物理的な所在地を把握し、限定する、(3) データがどのように消去されたかを確認する、(4) データストレージハードウェアを安全に廃棄するための文書化されたプロセスに対するアクセスを有する、および (5) データに対するアクセス制御を管理することを要求するが、データが外部の者（組織）によってホストされる場合には、これらはすべて難題となる。

8.2 クラウドの信頼性

信頼性とは、システムが特定の環境の範囲内で特定期間にわたって障害のないサービスを提供することについての確率である。クラウドにおける信頼性は、大まかにいえば、4 つの個別のコンポーネント、すなわち、(1) クラウド提供者が提供するハードウェアおよびソフトウェア設備、(2) クラウド提供者側の職員、(3) 提供されるサービスに対する接続性、ならびに (4) 利用者側の職員、についての信頼性をもとに算出される。

特定のクラウドの信頼性を提供者側または利用者側が測定するのは、以下の主な 2 つの理由により、難しいことに留意願いたい。第一に、クラウドはさまざまなコンポーネントによって構成されるが、各コンポーネントが単独で測定された時の各々の信頼性の度合いを引き継いでいることが挙げられる。これらのコンポーネントが組み合わさった場合、最終的な信頼性は予想するのが困難であり、あいまいに終わる可能性がある。第二に、信頼性の測定はその環境の関数によるものであり、クラウドが稼働する環境のすべてを十分に理解することは不可能な場合がある。前述したように、信頼性に対する従来の定義は、状況（環境）および故障せずに動作する期間の予測値にもとづく。クラウド、およびかなりの規模のシステムの大半では、それぞれのコンポーネントが特定の状況において特定の信頼性を有するため、それらの状況を組み合わせたものを把握するのは複雑であり、場合によっては手に負えないこともある。

8.2.1 ネットワークに対する依存

クラウドコンピューティングだけでなく、企業アプリケーションの大半は、ネットワークの接続性に依存する。大半のクラウドでは、利用者がサービスを利用するには、インターネットが継続的に利用できる状態であることが求められる。利用者がプロバイダを利用してパブリックネットワークサービスを確保する場合には、その依存性は通常のホスティングと同様になる。なぜならば、パブリックネットワークサービスのアクセスは通常インターネット越しに行われるからである。クラウドに依存する利用者向けアプリケーション（例：ウェブメール）では、アプリケーションが継続的なサービスの提供を必要とする場合には常に、このような依存性がリスクとなる。極めて多くの場合において、範囲の限界（例：地下鉄、飛行機、遠隔地）により、あるいはネットワーク途絶の影響を受けやすいが故に、利用者のアプリケーションがクラウドにアクセスできないといった事態が発生する。

ネットワークに対する依存性は、すべてのアプリケーションがネットワークアプリケーションであり、その構造が比較的複雑である（すなわち、エラーやセキュリティ上の脆弱性のリスクは、ネットワークでつながれていないスタンドアロン型のアプリケーションの場合よりも高い）ことを意味する。例えば、クラウドアプリケーションでは、通常、クラウド提供者に対するリクエストに暗号を使って署名する必要があり、伝送中の利用者データについても、暗号を使って保護する必要がある。このような依存性により、通常の停電もしくはサービスエリアの外であることだけでなく、アプリケーションが健常に動作するかどうかは、(1) インターネットルーティングおよび名前解決インフラストラクチャの健全性、(2) ローカルネットワークリソースの奪い合い、および (3) 不可抗力事象によっても左右されることになる。

サービス妨害攻撃、ウェブサーバーへのウイルスの侵入、ワームによる DNS サーバーの停止、海底ケーブルの障害、および地震やそれに続く土砂崩れによる光ファイバーケーブルの損傷に起因する、インターネットの地域的な機能停止に関して広く報道された事例がいくつかある。このような機能停止は比較的珍しいが、ネットワーク接続に数時間にわたって影響を及ぼす場合がある。まれにしか発生しないが、深刻になるケースも多いこれらの機能停止に対する異常対処計画の策定は、組織の IT 戦術計画の一環として実施されるべきである。今では、かなり多くのアプリケーションが、クラウドコンピューティングを採用しているか否かにかかわらず、インターネットを使用している。したがって、読者は、クラウドの利用を避けることによってインターネットの機能停止に関連するリスクを自動的に回避できると考えるべきではない。

8.2.2 クラウド提供者によるサービス供給停止

サービス契約書の条項が利用者に対する高い可用性と最小休止時間を示していても、人的要因（例：悪質な攻撃またはアドミニストレータによる故意によらないミス）、あるいは自然災害（例：洪水や竜巻など）によるサービスやユーティリティの供給停止は避けられない。

供給停止に関して利用者が考慮すべき問題は、供給停止の頻度と復旧時間の予測値にもとづくと考えられる。以下に、主な 2 つの考慮事項を示す。

- 業務プロセスに悪影響を及ぼすことなく利用者が許容できる供給停止の頻度と期間は？
- 供給停止が長引いた場合を含む不測の事態に利用者が利用できる、機能を維持するための代替策にはどのようなものがあるか？

8.2.3 安全性が重視される処理

ハードウェアであれ、ソフトウェアであれ、安全性が重視されるシステムとは、通常は政府当局によって規制される部類のシステムである。例としては、航空電子機器、核物質、および医療機器をコントロールするシステムが挙げられる。通常、そうしたシステムは人命の喪失または財産の損失のリスクを伴う。

そうしたシステムは、システムのコントロール、開発、およびテストに関する規制の副産物としての「血統」を受け継ぐ。（クラウドは多くの異なるサブコンポーネントによって構成またはサポートされるため）クラウド内でこれらのシステムのいずれかの「血統」を評価するには現時点では能力不足であり、このクラスのアプリケーションのホストとしてクラウドテクノロジーを採用することは推奨されない。だからといって、安全性が重視されるシステムの開発をサポートする目的でクラウドテクノロジーを利用する（例：クラウドを採用して、開発中の安全性が重視されるシステムのシミュレーションを行う）ことを検討すべきではないといっているわけではない。

影響度が高位のシステムに関する詳細な情報は、NIST FIPS 199 に記載されている。

8.3 経済的目標

パブリックおよび外部委託型のシナリオにおけるクラウドコンピューティングは、小額または妥当な初期費用でコンピューティングリソースを利用する機会を利用者に提供する。さらに、クラウドコンピューティングは、試験的な取り組みにかかる費用を削減することによって業務の敏捷性を促進すると同時に、利用者が負担する費用を規模の経済を通じて削減できる可能性がある。これにより、十分なメリットが得られる場合もあるが、いくつかの経済的なリスクについても考慮が必要である。

8.3.1 事業継続性に関するリスク

施設内のシステムの場合、ベンダーがサポートを中断したり、倒産した場合にも、利用者は製品を使い続けることが可能である。一方、パブリックまたは外部委託型のクラウドコンピューティングでは、利用者は、提供者によるサービスのほぼリアルタイムな提供に依存する。どんな市場でも事業の倒産を回避できない場合あるが、このような依存性は、スピードを重視したコンピューティングを必要とする利用者にとってはリスクになる。このリスクを軽減するのに利用できるアプローチは、例えば、冗長なクラウドを採用する、クラウド提供者の業務の健全性をモニタリングする、あるいはハイブリッドクラウドを採用するなど、多岐にわたる。

8.3.2 サービス契約の評価

第 3 章でも述べたが、サービス契約では、可用性やセキュリティなどの用語については、定義が固有かつ限定的である可能性がある。さらに、サービス契約における変更の追跡と、サービス契約を再評価するタイミングの決定に関して利用者側に課せられる責任は、しばしば変化する。

利用者には、サービス契約を評価・比較するための実践的な技術が求められる。現在のところ、サービス契約は人によって作成され、人によって利用される。しかしながら、最近のサービス契約に見られる共通点から、サービス契約用語の一部の標準化のためのベースが存在することがわかる。実際に共通のサービス契約用語を含むサービス契約テンプレートをどのように設計するかは、1 つの未解決の問題である。そうし

たテンプレートの仕様ができれば、サービス契約の一部を機械的に評価することができ、これにより、利用者側のコストを削減し、実際にクラウドサービスが提供するものについての理解を深めることが可能になる。

サービス契約を共通のオントロジーを使用して機械可読フォーマットで記述することは、契約条件の自動評価を支援する有効なステップになりうる。共通要素を定義するテンプレートはクエリーインターフェイスを支援する可能性があり、その場合、利用を検討中の者は詳細な契約条件の手動での評価に労力を注ぐ前に、重要なコンポーネントを迅速にチェックし比較することが可能になる。これは、より効率的なクラウド市場の構築を支援することにつながる。テンプレートには、利用者が各サービスを客観的に比較することを可能にする標準化された性能測定基準が含まれる可能性がある。

8.3.3 ワークロードの移行可能性

クラウドの適用を妨げる第一の障壁は、ローカルにあるワークロードをクラウド提供者のインフラストラクチャに移動しなければならないことである。クラウド提供者が必要に応じてワークロード（例：データワークロードまたは完全にカプセル化されたコンピュータ／ストレージ／ネットワークワークロード）を利用者の施設に戻すための実用的な方法を提供する場合には、利用者にとってこの意思決定のリスクは少ない。もう1つの問題として、利用者は、必要に応じてワークロードをあるクラウド提供者から他のクラウド提供者に移行できなければならないことがある。これらの 2 つのニーズは、クラウド市場の競争を促すだろう。

移行可能性は、標準化されたインターフェースとデータフォーマットに依存する。クラウドコンピューティングは合意形成と事実上の業界標準（TCP/IP、XML、WSDL、IA-64、x509、PEM、DNS、SSL/TLS、SOAP、REST など）の両方に依存する。従来のコンピューティングリソース（仮想マシンまたはディスクストレージなど）をレンタルするクラウドサービス（すなわち IaaS）は、既存の標準と密接に関係するので、移行可能性を示す利用シナリオは、既存の標準用語を使用して表現すことができる場合もある。

IaaS システムでは、デバイスインターフェースなどの低レベルの詳細がむき出しになるため、そうしたインターフェース間の相違が障害となり、移行可能性を実現するのが困難であろう。一方、ミドルウェアスタックに対するアクセス(PaaS)や、提供されるアプリケーションを使用する権利(SaaS)などの、生成されたエンティティをレンタルするクラウドサービスでは、現在の標準を用いてもさほどうまく記述されないため、そうしたエンティティがあるクラウド提供者から他のクラウド提供者にどのように移行されるかについて記述する共通の用語が不足している。デバイスインターフェースなどの低レベルの詳細の一部は、クラウド提供者によって秘匿されるため、移行可能性は高まるが、リソースの定義はベンダーに固有のものである場合が多い。

8.3.4 クラウド提供者間の相互運用性

クラウド提供者間で仮想マシンイメージやデータを転送するなどのオペレーションでは、転送されるデータに適用する標準化されたフォーマット、料金請求、ID 管理が必要となる。オープン仮想フォーマット(Open Virtualization Format)[DMT09]やクラウドデータマネジメントインターフェース(Cloud Data Management Interface)[SNI10]などの一部の標準が、既に開発されているが、クラウド提供者間の相互運用コストを削減するためには、さらなる開発と経験が必要である。セキュリティに関する1つの例として、クラウド提供者は、利用者から資産の転送リクエストを受けてから利用者の資産を転送する前に、適切な認証情報を転送先のクラウド提供者に掲示できなければらななないことが挙げられる。さらに、認証が確認されたら次に、転送されるオブジェクトのフォーマットに互換性がなければならない。

8.3.5 災害復旧

災害復旧は利用者の資産に対する物理的災害および電子的災害の両方を含む。自然災害に対する備えとして、地理的に分散した場所にデータの複製を保管することが推奨される。ハードウェアの盗難など、そ

他の物理的災害に対しては、司法の関与が唯一の救済策となるだろう。電子的災害に対しては、どのような電子的災害から保護するかによって、冗長性、複製、および多様性などの耐障害性アプローチを適用することができる。災害復旧計画は、ホストされるすべての IT サービスに適用することができるが、文書化と迅速に実行できることが必要である。自身のワークロードがどこにホストされているかを利用者が知らないこともあるため、これらの従来からの問題はすべて複雑である。

8.4 法令順守

データまたは処理能力がクラウドに移行された場合、法令順守の最終的な責任は利用者にとどまるが、クラウド提供者は（データに直接アクセスできるため）法令順守に関するルールを実行する最良の立場にあると考えられる。法令順守を複雑にする要因はいつくかあり、契約による対処が必要となる。NIST およびその他の米国政府機関は、利用者における法令順守問題を支援する道筋（例：FEDRAMP [Fed10]）を開発中である。第 3 章と付録 B も参照のこと。

8.4.1 可視性の欠如

利用者が、クラウドがどのように機能するかについての可視性を十分に得られない可能性がある。その場合、サービスが安全に実施・提供されているとはいい切れない可能性が高い。クラウドサービスのモデルが異なれば、利用者が有するコントロールのレベルも増えたり減ったりし、可視性の度合いも異なってくる。しかしながら、クラウド提供者の施設に追加のモニタリングメカニズムを配備するよう利用者がリクエストするといった選択肢は、現在、クラウド以外のさまざまなシステムにおいて用いられているが、現実的ではない。

8.4.2 物理的なデータロケーション

クラウド提供者は、いくつかのパラメータをもとに、データセンタを物理的にどこに設置するかについてのビジネス上の意思決定を行う。そうしたパラメータには、例えば、建設費、エネルギー費、安全とセキュリティ上の関心事、教育を受けた労働力を確保できるか、雇用コスト、および公共インフラストラクチャの品質が含まれる。

一方、利用者は、データを特定の物理的範囲または境界の外に保管することを禁止する国際的な、または連邦政府の、もしくは州の法律および指示に従わなければならない。技術によってデータを論理的にコントロールしたり、暗号メカニズムを採用して正規の権限によらない開示のリスクを軽減することも可能だが、それでも利用者は、これらの法規制に従わなければならない[NIST SP800-144]。

8.4.3 司法管轄権および規制

利用者は、さまざまな法規制、例えば SOX（Sarbanes-Oxley Act：サーベンスオクスリー法）、PCI DSS（Payment Card Industry Data Security Standard：クレジットカード業界のセキュリティ基準）、HIPAA（Health Insurance Portability and Accountability Act：医療保険の相互運用性と責任に関する法律)、2002 年施行の FISMA（Federal Information Security Management Act：連邦政府情報セキュリティ管理法）、または GLBA（Gramm-Leach-Bliley Act：グラムリーチブライリー法）などに準拠しなければらない。クラウド提供者のシステム上で処理されるデータに対する最終的な責任を負う利用者は、適切な法規制の順守に関して、クラウド提供者からの支援が得られる保証を要求する必要があるだろう。

利用者は、また、クラウドサービスに対する適切な法管轄が存在することに対する保証を要求する。これにより、クラウド提供者が法規制を順守しなかった場合にとられる法的措置について、前もって把握することができる。クラウド提供者は、自身が提供するサービスの実装と設定については知的財産を構成する情報とみなすのが通常であり、そうした詳細についての可視性を利用者に提供しないため、これらのニーズは複

雑になる。こうした可視性の欠如は、クラウド提供者が信頼できる第三者による独立監査を受けない限り、クラウド提供者による法規制の順守を利用者が確信するのを困難にしている。それでも、クラウドシステムは気付かないうちに法令順守からそれる可能性があるため、第三者による監査の頻度によっては、提供される総合的な保証が限られる場合がある。この場合、クラウドの設定と健全性を継続的にモニタリングすることが推奨される。

8.4.4 フォレンシックに対するサポート

インシデント対応の取り組みの一環としてのデジタルフォレンシックの目的は、(1) 何が起きたかを理解する、(2) システムのどの部分が影響を受けたかを把握する、(3) そうしたインシデントの再発をどのように防止するかについて学ぶ、および(4) 将来にわたる法的措置についての情報を収集する、ことにある。しかしながら、クラウドにおけるフォレンシックは、例えば以下のようないつくかの新しい問題を提起する。

- サービス契約では、インシデント対応に関する責任がどのように定義されているか？（付録 A を参照）
- 一連のイベントを再現することを支援するために、複数のデータセンタのクロックをどのように合せるか？
- データ流出・漏えいについての通知に関する法律が異なる国家間でどのように扱われるか？
- 共有のハードドライブのイメージをとらえた時に、クラウド提供者にはどのようなデータが見えるか？
- 監査ログの内、利用者に閲覧が許可されているものは何か（例：他のクラウド利用者に関連する情報は保護されているか？）
- PaaS モデルにおけるインシデントの報告に関して、利用者はどのような責任を負うか？
- 間接的な契約関係しかない（例：利用者が 3 層構造になっている）場合に、自身のクラウド内のアプリケーションに対する攻撃を止めるために、クラウド提供者は合法的に介入できるか？

SaaS モデルにおけるフォレンジック分析については、クラウド提供者が全面的に責任を負う可能性がある一方で、IaaS モデルにおけるフォレンジック分析については、利用者が（提供者からのなんらかの協力を得て）主に責任を負う可能性がある。PaaS モデルでは、利用者と提供者が責任を分担すると考えられる。

8.5 情報セキュリティ

情報セキュリティは、データの機密性と完全性を保護し、データの可用性を確保することに関連する。IT 事業を所有し運営する組織は、通常、以下のようなデータセキュリティ対策を実施するだろう。

- データ関連の作業、例えば、データの作成、アクセス、開示、伝送、および破棄をだれが実施できるかを規定する組織的／管理的コントロール
- ストレージ媒体とストレージデバイスを収容する施設の保護に関連する物理的コントロール
- 本人確認及びアクセス管理(IAM)、保存中のデータと伝送中のデータの暗号化、ならびに法的要求事項を順守するための、その他のデータ監査の扱いについての順守要件に関する技術的コントロール

組織がクラウドを利用する場合、生成・処理されるすべてのデータは、クラウド提供者が所有し運営する施設内に物理的に置かれる。この状況において基本的な問題となるのは、提供者が実施しないのなら利用者が実施すると考えられる管理策と同じまたは同等の管理策を提供者が実施することについて、利用者が

提供者から保証を得ることができるか否かである。これらの管理策についての保証を得ようとする際には、以下の問題が立ちはだかる。

- 利用者がクラウドに移行しようとしているデータに関する法令順守義務が、特定のレベルと精度の監査ログ、アラートの生成、活動報告、およびデータ保持を求める場合がある。これらはクラウド提供者が提供する標準のサービス契約には含まれない可能性があるため、利用者が(1) これらの手続きを契約上のデータ保護責任の一環として含め、かつ (2) 標準の運用手順の一環として実施する意思があるかが問題になる。

- 契約上の義務や運用上の設定を通じてクラウド提供者が利用者のデータの保護に関する要求事項を満たす場合であっても、クラウド提供者は、要求事項が継続して満たされているか否かを評価するための手段を利用者に提供すべきである。

- 保存中のデータの暗号に関しては、暗号アルゴリズムスイートの強度、クラウド提供者がサポートする鍵管理方式、および各データ所有者が持つことになる鍵（個別鍵または共通鍵）の数を各データ所有者が把握すべきである。

パブリッククラウドで処理されるデータとパブリッククラウド上で稼働するアプリケーションは、施設内でホストされる環境の場合とは異なるセキュリティ上の危険に遭う可能性がある。クラウド内のデータと実施されるプロセスのセキュリティに影響を与える課題がいくつかある。例えば、クラウドの実装の質、クラウドに対する攻撃の矢面、攻撃者の集合の可能性、システムの複雑さ、およびクラウドアドミニストレータの専門知識のレベルは、クラウドシステムのセキュリティに影響を与える課題の例である。

残念なことに、これらの課題はいずれも、クラウドセキュリティに関してはっきり判っているわけではなく、クラウド以外のシステムとクラウドシステムのどちらが実際により安全であるかを比較しようとしても、明白な答えがあるわけではない。しかしながら、クラウドシステムに存在する1つの課題に、利用者ワークロードの「物理的な隔離」ではない「論理的な隔離」による耐性と、利用者のリソースを保護するための論理メカニズムの使用がある。多くの従来型のシステムでも論理的な隔離を採用しているが、そうしたシステムは物理的な隔離（例：物理的に隔離されたネットワークまたはシステム）も採用していて、論理的な隔離は物理的な隔離と同じくらい信頼できるわけではないことが証明されている（例：過去に、一部の仮想システムがストレステストにおいて機能不全を起こした[Orm07]）。以降のサブセクションでは、いくつかのセキュリティ問題について簡単に説明する。NIST SP800-144 も、パブリッククラウドにおけるセキュリティ問題について論じている。

8.5.1 意図しないデータ開示のリスク

政府の機密扱いされていないシステムは、単一のシステムを使用して個人情報、公用に限る情報、または専有情報に加えて、機微でない公開情報も処理するといった形で運用されることが多い。典型的なシナリオでは、ユーザは機微な情報とそうでない情報を1つのシステム上の異なるディレクトリに、あるいは、1つの電子メールサーバー上の異なるメールメッセージに保存するであろう。そうすることで、機微な情報が慎重に管理され、意図しない配信が回避されることが期待される。利用者が機微でないコンピューティングにクラウドコンピューティングを使用し、機微なコンピューティングには施設内のリソースのセキュリティ上の利点を利用することを望む場合には、機微なデータを暗号化して保存するよう、注意を払わなければならない。

8.5.2 データプライバシー

プライバシーは、例えば、システム上で処理される情報の所有者である利用者またはその他の者などの、特定の主体に属するデータの機密性に対する取り組みである。プライバシーは、法律および義務に関わる問題を抱えていて、技術的な課題としてだけでなく、法律および倫理に関わる課題としてとらえるべきである。あらゆるコンピューティングシステムにおいてプライバシーを保護することは、技術的な課題である。クラウド

環境では、クラウドが分散型の性質を有し、データの保存場所やアクセス権を有する（またはアクセスできる）者について利用者が知らない可能性があるため、この課題が複雑になる。

8.5.3 システム保全

クラウドは、クラウドの機能性の内部からの破壊または妨害行為に対する保護を必要とする。クラウド内には、利用者、提供者、およびさまざまなアドミニストレータといった、利害関係者がいる。悪質な攻撃を防止する一方で、これらのグループのそれぞれにアクセス権を分配する能力は、悪質な攻撃を防ぐ一方でクラウドの完全性を維持するための、重要な特性となる。クラウド環境では、クラウドのメカニズムに対する可視性の欠如が、クラウドによってホストされるアプリケーションの完全性を利用者がチェックすることをより困難にする。

8.5.4 複数利用者による共同利用(multi-tenancy)

クラウドコンピューティングでは、提供者側のリソースを共有することによって、かなりの経済的効率を享受できる。IaaS クラウドでは、異なる仮想マシンがハイパーバイザを介してハードウェアを共有する可能性があり、PaaS クラウドでは、異なるプロセスがオペレーティングシステムや支援データおよびネットワークサービスを共有する可能性があり、SaaS クラウドでは、異なる利用者が同一のアプリケーションまたはデータベースを共有する可能性がある。

提供者側が採用する共有メカニズムは、各利用者ワークロードの隔離に関して、複雑なユーティリティに依存するため、隔離に失敗するリスクが存在する。過去に、論理的な隔離の欠陥がドキュメント化されている[Orm07].。

論理的な隔離が物理的な隔離の代わりとして適していることへの信頼の確立は、長期にわたる研究課題であるが、この問題はデータをクラウドに移行する前にデータを暗号化することによって、いくらか緩和される。（データが暗号化される場合、そのデータを処理するには、暗号の復号化が必要になる。）計算を行うクラウドでは、クラウドで処理するデータの種類を限定するか、あるいは仮想マシン（単一のテナント）、仮想プライベートネットワーク(VPN)、セグメント化されたネットワーク、または最新のアクセス制御をレンタルする代わりにコンピュータシステム全体をレンタルするなどの、特殊な隔離メカニズムを提供する提供者と契約を結ぶことによって、リスクを軽減できる。

8.5.5 ブラウザ

多くのクラウドアプリケーションは、利用者のブラウザをグラフィカルインターフェースとして使用する。例えば、ソフトウェアをクラウドインフラストラクチャ内で稼働しているにもかかわらず、ローカルで稼働しているように感じさせるクラウド体験を、利用者のブラウザによってもたらすための技術（例：[Gar05, Ado11, Goo11-2, Mic11, Dja11]）がいつくか存在する。クラウドを管理するためのクライアントツールをクラウド提供者が配布する場合もあるが、利用者アカウントの設定およびリソースの管理（アカウントを開設・使用するのに必要な財務情報の提供者への提供を含む）にブラウザが使用されることもある。残念なことに、ブラウザは初期のオペレーティングシステムの複雑さと同じくらい複雑であり、セキュリティ上の欠陥を有し、ほぼすべてのパブリックセキュリティ課題（例：[Por10, Mar09]）において脆弱であることが既に示されている。クラウド提供者は、利用者のさまざまな種類やバージョンのブラウザとやりとりし、利用者が管理する端末システムおよびブラウザは、セキュリティ面で適切に管理されない、あるいいは最新でない可能性がある。利用者のブラウザが侵害された場合、クラウド提供者に外部委託された利用者のすべてのリソースがリスクに晒される。

ブラウザがクラウドに対するアクセスポイントである場合、ブラウザが侵害されていないことについての信頼の確立が重要になる。信頼の確立には、アプリケーションゲートウェイまたはネットワークパケットフィルタ

リングファイアウォールを介してクラウドにアクセスする、クラウドにアクセスすることを認可するブラウザの種類を限定する、クラウドに対するアクセスを提供するブラウザに対するブラウザプラグインを限定する、ブラウザを確実に最新にする、およびブラウザを介してクラウドにアクセスするシステムをロックダウンするなど、さまざまなアプローチをとることができる。これらの技術の大半は実用的で有用であるが、コストの増加、機能性の低下、または利便性の低下を引き起こす。

8.5.6 信頼性を確保するためのハードウェアサポート

一部のシナリオでは、ハードウェアサポートを通じて、リモートシステムが信頼できることを利用者に理解させることができる。1つの例として、トラステッドプラットフォームモジュール（TPM）の目的は、システムの起動時に生成される一連のチェックサムを保存し、要請があった場合には、そのシステムが実際に既知のコンポーネントから起動されたことを証明することにある。仮想マシンを移行する場合、トラステッドプラットフォームモジュールのトラストチェーンが断ち切られると考えられる。これまでにもさまざまなグループが、トラステッドプラットフォームモジュールの仮想化や、停止状態を解除された仮想マシンが異なるハードウェア上でトラストを再構築できるといった議論の構築を試みたが、この問題は未解決のままである。

8.5.7 鍵管理

利用者の暗号鍵の適切な保護には、クラウド提供者からのなんらかの協力が必要であると考えられる。問題は、専用のハードウェアとは異なりクラウドでは、以下の条件下では、メモリバッファをゼロで埋めても鍵は消去されない可能性がある：(1) メモリをがハイパーバイザによってバックアップされ、不揮発化される、(2) リカバリ目的で仮想マシンのスナップショットを撮っている、あるいは (3) 異なるハードウェアへの移行に備えて仮想マシンをシリアル化している。クラウドの内部から暗号技術をいかに安全に使用するかは、未解決の問題である。

9. 一般的な推奨事項

連邦政府の情報システム、および米国政府のために運用される情報システムでクラウドシステムを使用する場合には、2002 年施行の FISMA と、関連する NIST 標準および特定発行文書（例: FIPS199、FIPS200、SP800-53 など）が適用される。クラウドコンピューティングの環境では、以下のような追加の一般的な推奨事項があり、これらは読みやすさのために、マネジメント、データガバナンス、セキュリティと信頼性、仮想マシン、ならびにソフトウェアおよびアプリケーションの 5 つのグループに分類されている。

9.1 マネジメント

- **クラウドへのデータの移行およびクラウドからのデータの移行。**利用者は、クラウドへのデータ移行とクラウドからのデータの移行に適したリソースを特定すべきである。リソースは、例えば、(1) 電子メール、(2) 共有ドキュメントなどのデータレポジトリ、あるいは (3) 仮想環境で稼働するシステムなどのサービスであったりする。利用者は、クラウドへのデータ移行とクラウドからのデータの移行の両方に関する計画と、クラウドに移行されたデータとのやりとりに関する計画を作成すべきである。利用者は、調達の段階で、万一提供者からのサービスが終了した場合対処するための計画も策定し、資産がどのように利用者に返却されるべきかを明確にすべきである。利用者は、クラウド間の移行に関する計画も作成すべきである。

- **業務の継続性。** アプリケーションに対するアクセスを失うことの代償が深刻である場合、提供者が特定の種類のサービスの途絶に起因する所定の損害に対する代償を支払うことに同意する意思がない限り、利用者はその業務をローカルで実施することが推奨される。利用者は、提供者の事業継続計画と冗長性アーキテクチャを精査し、彼らが掲示している可用性の目標がサポートされているか否かを把握すべきである。利用者は、提供者が信頼性の高いシステムアップデート、データ転送、およびその他の施設の変更のための確立された内部運用手順およびサービスマネジメント技術を適用することについて、保証を要請すべきである。利用者は、通常サービス契約に謳われていることは、サービスが中断した場合の利用者に対する賠償として、提供者はサービスの中断に起因する実際の損害に対して補償するのでなく、サービス料金を返還するだけであることを考慮すべきである。クラウドサービスの可用性のレベルと、データのバックアップと災害復旧についての能力は、クラウドサービスが中断した場合に、必要に応じて代替のサービス、設備、場所を使用して中断されたサービスを復旧できるようにするためにも、組織の異常対処計画と事業継続計画にて取り扱うべきである。

- **法令順守。**利用者は、(1) 必要な管理策を定義するための能力が特定のクラウド提供者にあるか、(2) それらの管理策が適切に実施されているか、および (3) それらの管理策が文書化されているかについて判断しなければならない。 従来の直接的なアセスメントは実施できない可能性があり、その場合、必要な情報およびシステムアクセスを得るために、あるいは第三者による監査により十分なレベルの保証を確保するために、クラウドプロバイダと協力することになるだろう。また、利用者は、あらゆる認証（例: ISO 27001）または監査報告書（例:SAS 70）を精査し、その適用範囲を確認すべきである。[16]

- **運営管理スタッフ。** 利用者は、クラウド提供者側のアドミニストレータの業務上の責任を、利用者側のアドミニストレータの責任に対して区分するためのプロセスが実施されていることを確認すべきである。内部関係者によるセキュリティ脅威は、殆どの組織にとって既知の問題であり、内部関係者にはクラウドプロバイダの職員も含まれる。したがって、利用者は、悪意のある内部関係者から保護するためのクラウドプロバイダのポリシー、手順、管理策が適切であるかどうかを確認しなければならない。

[16] Federal Risk and Authorization Management Program は、クラウドコンピューティングサービスおよび製品のアセスメントと認可を行う際に利用できる、標準化されたアプローチを提供するために確立された。このアプローチにより、共通のセキュリティリスクモデルに関して、複数のクラウドプロバイダによる共同認可が可能になる。発行された共同認可は、そのセキュリティリスクモデルが適用可能なクラウドコンピューティング実装において、連邦政府機関全体を通して再利用し、活用することができる。

- **法的要件。**利用者は、(1) 司法による証拠の凍結などの電子証拠開示、および (2) データとメタデータの保存を命ずる偶発的な法的要請に提供者が対応できるか否かを調査すべきである。

- **運営方針。**利用者は、提供者の運営方針を精査し、(1) 提供者が外部監査とセキュリティ認証を受ける意思があるか、(2) 法医学的分析能力を含む、提供者のインシデント対応とリカバリの手順／実務、(3) IT リソースの不正な、または不適切な使用に関する提供者側の内部調査手順、および (4) 提供者側のシステムおよびネットワークアドミニストレータなどの特権ユーザに対する信用度調査に関するポリシーについて、確認すべきである。

- **利用規定。**利用者は、利用者側のすべての職員が提供者の利用規定を読んで理解することを確実にするとともに、同意済みの利用規定の違反に対する解決策について、前もって提供者と交渉を行い合意しておくべきである。さらに、利用者が、利用規定の違反に関する両者間（利用者と提供者）の紛争を解決するためのプロセスを前もって知っていることが重要である。

- **ライセンス。**利用者は、クラウドにインストールされているあらゆる知的財産権のあるソフトウェアについて、提供者と利用者の両方が適切にライセンスしていることを確実にすべきである。

- **パッチマネジメント。**利用者と提供者は、アプリケーションをオフラインにするために利用者が実施する必要がある一連の手順（ソフトウェアパッチのインストールを提供者が行うか、あるいは利用者が行うかにかかわらず）、アプリケーションが意図したとおりに機能し続けることを確実にするために実施するテスト、およびアプリケーションをオンラインに戻すために必要な手続きについて、合意しなければならない。システムメンテナンス計画は、サービス契約書に含まれていなければならない。

9.2 データガバナンス

- **データアクセス標準。**クラウド上で新規のアプリケーションを開発することを決定する前に、そのクラウド上のアプリケーションインフラストラクチャインターフェースが一般性を備えているか、あるいは少なくともアプリケーションの移行可能性と相互運用性に大きな影響が及ばないようデータアダプターを開発することが可能であるかを確認すべきである。利用者は、きちんと文書化されたデータアクセスプロトコルに対応するクラウドを選択すべきである。

- **データの隔離。**異なるレベルの機微さを有するデータをクラウドで処理する場合、複数の異なるクラウドを同時に使用することによって、機微なデータとそうでないデータに対して異なるレベルの保護を施すことが可能である。このアプローチを取った場合、提供者側の機微なデータとそうでないデータを隔離するための保護メカニズムを利用者は求めるべきである。

- **データの完全性。**利用者は、データの完全性を確保するためのチェックサムと複製技術を採用すべきである。クラウドで扱うデータのチェックサムを求めて、使用に際して有効性を確認し、各チェックサムを別々に保存することによって、データを正規の権限によらない変更から保護することが可能になる。

- **データの規制。**利用者は、データ関連の法規制に関するすべての順守事項に最終的な責任を負うため、自身のデータをクラウドに処理させる、またはクラウドに格納することに伴うリスクを評価すべきである。利用者は、クラウドプロバイダに対して、国際、連邦政府、または州の法律と指令（例：特定の物理的な境界の外側にデータを保管することを禁じるもの）に従うことを要求すべきである。

- **データの廃棄。**利用者は、クラウド提供者に対して、リクエストに応じて利用者データを確実に消去するためのメカニズムを用意し、データが消去されたことの証拠を提供するよう求めるべきである。

- **データのリカバリ。**利用者は、(1) データのバックアップ、(2) アーカイビング、および (3) リカバリに関する提供者の能力を検証できなければならない。

9.3 セキュリティと信頼性

- **利用者側の脆弱性。**利用者は、利用者プラットフォームのセキュリティと強化に関する最良慣行（ベストプラクティス）を採用することによって、ウェブブラウザやその他のクライアントデバイスが攻撃に遭う可能性を最小限に抑えると同時に、悪質かもしれないなウェブサイトにブラウザがさらされるリスクを最小限に抑えるべきである。

- **暗号化。**利用者は、レンタルするアプリケーションが他のアプリケーションとのやりとりや転送されるデータの機密性を必要とする場合には常に、堅固な（FIP 140-2 に準拠）暗号化を用いてウェブセッションを確立するよう求めるべきである。また、利用者は、保存されているデータについても、同様の措置を行うよう要求するべできある。

- **物理的な。**利用者は、クラウド提供者を選択する際に、リスクに関する全般的な考慮の一環として、提供者の施設における物理的施設向けのセキュリティの実践および計画について考慮すべきである。物理的な攻撃に対しては、サイバー攻撃と同様に、バックアップ計画が必要になる。利用者は、そうした攻撃からの復旧計画を文書化すべきである。利用者は、また、候補となるクラウド提供者が、提供者が運営するサイトに対して冗長性を持たせているかについても調査し、自然災害やその他の途絶を想定して、地理上の特定の場所に結びついていない別の場所の選択を考慮すべきである。

- **認証。**利用者は、アカウントのハイジャックやその他の種類の悪用のリスクを軽減するために一部のクラウド提供者が提供する、適切な最新の認証の利用を検討すべきである。

- **ID およびアクセス管理。**利用者は、以下に示す提供者の能力について把握していなければならない: (1) 提供者のインフラストラクチャがサポートする認証およびアクセス管理メカニズム、(2) 認証情報を提供するために利用者が利用できるツール、および (3) 提供者による仲介を要することなく、利用者組織のユーザとアプリケーションの権限付与（情報）を入力・管理するためのツール。

- **パフォーマンス要件。**利用者は、アプリケーションをクラウド提供者の施設に実装する前に、アプリケーションの現在のパフォーマンススコアを測定し、主要パフォーマンススコアに関する要求事項を決定べきである。主要パフォーマンススコアには、対話型のユーザアプリケーションに対する応答性能と、大量のデータを継続的にインプット／アウトプットするアプリケーションの大量データの転送に関するパフォーマンスが含まれる。

- **可視性。**利用者は、特定の利用者のデータまたはそのデータに対する操作に影響を与えるオペレーティングサービスに対する可視性を提供するよう、クラウド提供者に対して求めるべきである。

9.4 仮想マシン

- **仮想マシン の脆弱性。** クラウド提供者がコンピューティングリソースを仮想マシンの形式で提供する場合、利用者は、仮想マシンを (1) 同一の物理ホスト上の他の仮想マシンからの攻撃、(2) 物理ホストからの攻撃、および (3) ネットワークを介した攻撃から保護するためのメカニズムを提供者が有することを確認すべきである。攻撃の検知・防止メカニズムの典型的な例には、仮想ファイアウォール、仮想 IDS/IPS、および VLAN などのネットワーク分割技法が含まれる。

- **仮想マシン の移行。** 利用者は、代替が可能なクラウド提供者間での仮想マシンおよび関連するストレージの移行に関する、戦略を策定すべきである。

9.5 ソフトウェアおよびアプリケーション

- **スピードが重視されるソフトウェア。**タスク完了の正確なタイミングが求められるアプリケーションは、パブリッククラウドコンピューティング、および一部の外部委託型クラウドコンピューティングのシナリオには適さないと考えられる。なぜならば、そうしたシステムではレスポンスタイムにばらつきがあり、予期しない、かつやむを得ない往復遅延に遭う可能性があるからである。利用者は、スピードが重視されるアプリケーションにクラウドを使用すべきではない。

- **安全性が重視されるソフトウェア。**現時点で、安全性が重視されるアプリケーションにクラウドテクノロジーを採用するのは、クラウドを構成するすべてのサブシステムの「血統」を十分に評価する能力が不足していることと、ネットワークにばらつきがあることから、推奨されない。

- **アプリケーション開発ツール。**利用者は、利用可能な場合は、セキュリティ上の脆弱性を軽減するためのアーキテクチャとツールを含む、アプリケーション開発フレームワークを提供するクラウドを選択すべきである。セキュリティポリシーの直感的なオーサリングおよび保守を支援し、システムライフサイクル全体をカバーする統合されたアプリケーション開発環境を提供するツールは、セキュリティ認定を容易にするためにも望ましい。利用者は、また、そうしたツールが FIPS 140-2 の該当する安全要求を満たすことを確実にしなければならない。

- **アプリケーションランタイムサポート。** クラウド上に新規のアプリケーションを実装することを決定する前に、あるいはクラウド提供者が提供する構成要素を使用してアプリケーションを構築する場合には、コンパイルフェーズに含まれるライブラリ、または実行フェーズにおいてコールされるライブラリが、機能とパフォーマンスの両方の観点から意図したとおりに機能することを利用者は確認すべきである。

- **アプリケーションの設定。**利用者は、アプリケーションが安全に稼働するように構成する（例：専用の VLAN セグメントを使用する）ことが可能であるか、また、（例えば識別および認可(identification and authorization)などの）既存の企業／政府機関セキュリティフレームワークと結合でき、企業／政府機関セキュリティポリシーの実施を適用できるかどうかを確認すべきである。

- **標準プログラミング言語。**利用者は、実現可能であれば、標準化された言語とツールに対応するクラウドを選択すべきである。

付録 A－役割と責任

クラウドの設計、構築、実装、および運用における提供者－利用者間の協力関係は、適切なセキュリティとプライバシーの保護を提供するうえで新しい課題を提起する。必要な管理策の実施に関する責任の共有は、提供者－利用者間の協力によるプロセスとなる。

クラウドビジネスモデルは、クラウド内で提供されるコンピューティングリソースの管理者責任を決定する。提供者と利用者が同一の組織体であるプライベートクラウドの場合、責任の分担について話し合うことが、クラウドに実装されるシステムの所有者にとって有効である。これは、管理者が、提供者の論理的な役割と利用者の論理的な役割との協力にもとづいて包括的な運用計画を策定するのに役立つ。

セキュリティ管理策の実施に関する役割と責任をどのように割り振るかといった質問に答えることは、組織が (1) クラウドのセキュリティ要求事項に取り組むための詳細なセキュリティ計画を定義する、(2) 開発中に適切なセキュリティ対策を開発または入手する、(3) クラウド提供者を客観的に比較・評価する、および (4) 開発中および運用段階の全体を通して、セキュリティプロトコルを実施する、ことを支援するうえで、重要である。さらに、提供者－利用者間の協力は、クラウドが特定のセキュリティ要求事項および法的要求事項、とりわけ、政府機関の業務をサポートする要求事項を確実に満たすことに役立つ。

この簡潔な付録では、NIST の SP 800-53 から抜粋した技術面での主要なセキュリティ管理策の概要を示すことによって、これらの問題について論じた後に、セキュリティ上の責任を共有するためのさまざまな提供者－利用者関係のパターンを考慮することによって、それらの管理策をクラウドに適用するためのロードマップを示している。

クラウドに実装されるシステムのライフサイクルと寿命は、役割と責任の記述方法に関する別の視点をもたらす。システム開発者とインテグレータは、開発時にシステムに組み込まれるべきセキュリティ管理策の実装に責任を負う。システムアドミニストレータと運営担当者は、運用時に実施されるセキュリティ管理策の実装に責任を負う。

SaaS クラウドでは、提供者が開発者／インテグレータであると同時に、アドミニストレータ／運営担当者である場合がある。その場合、セキュリティ管理策の実施に関する責任の大半を提供者が負うのが一般的である。IaaS クラウドでは、利用者は開発者／インテグレータであると同時に、アドミニストレータ／運営担当者でもあるため、通常、利用者はより多くの責任を負う。ただし、利用者がコントロール権を持たないインフラストラクチャレベルでの保護の提供に関しては、IaaS クラウドの提供者が責任を負うことになるだろう。PaaS クラウドでは、両極端の混在が発生する。すなわち、開発者／インテグレータである利用者は、アプリケーションレベルの必要なセキュリティ管理策をシステムに組み込む必要があり、提供者は、システムレベルのすべての保護の提供に責任を負う。（ここで妥協案として、第三者によるクラウドセキュリティサービスを利用することが考えられる。その場合、システム全体に対する保護を提供する責任について、すべての関係者間が話し合うべきである。）

SP 800-53 は、IT システムを保護するためのセキュリティ管理策の包括的なリストを定義している。各セキュリティ管理策は、システムに実装される機能であるか、あるいはセキュリティを実施するために組織が実施する一連の手続きまたは活動のいずれかである。SP 800-53 は、また、組織の特定のニーズを満たすために、あるいはシステムの特異性に対応するために、セキュリティ管理策リストをどのように調整するかについてのガイダンスも提供する。

セキュリティ管理策は、セキュリティ要求事項の各分野にもとづいて、17 ファミリに分類されている。さらに、セキュリティ管理策の実施に関する、責任の論理的領域の割り当てについて検討する際の出発点として、管理策ファミリは管理面、技術面、および運用面での管理策といった 3 つの大まかなクラスに分類されている。表 2 は、17 ファミリと、それぞれのファミリが属するクラスの一覧である。

表 2: 800-53 管理策ファミリおよびクラス

技術面	運用面	管理面
アクセス制御	意識向上およびトレーニング	承認、運用認可、セキュリティ評価
監査および責任追跡性	構成管理	計画
識別および認証	緊急時対応計画	リスクアセスメント
システムおよび通信の保護	インシデント対応	システムおよびサービスの調達
	保守	
	記録媒体の保護	
	物理的および環境的な保護	
	人的セキュリティ	
	システムおよび情報の完全性	

SP 800-53 に現在記載されている NIST のベースラインは、クラウドアプリケーションおよびサービス、ならびにそれらのアプリケーションやサービスを提供する情報システムにとって、良い出発点となる。SP 800-53 は、クラウドコンピューティング環境への対応を可能にする修整ガイダンスを提供する。SP 800-53 に現在記載されているセキュリティ管理策は、技術とポリシーの観点から記述されているため、より低い抽象レベルの追加のガイダンスが必要となるだろう。

現在、追加のガイダンスを策定するための作業が進められている。それらの結果には、以下の 3 つの主要な見解が含まれる。

- ポリシーおよび手順に関連する技術面でのセキュリティ管理策に関しては、通常、利用者側の責任になる。提供者は、それらのポリシーと手順の実施の実現可能性およびコストに対するインプット（とりわけ、それらを実施することに提供者が責任を負うか否か）を提供する可能性が高い。システム機能に関連する管理策に関しては、構築時には機能の開発者が、運用時にはアドミニストレータが責任を負う。例えば、IaaS クラウドにおける特権ユーザに対する「アカウント管理」管理策は、通常、IaaS クラウド提供者によって実施されるが、IaaS 環境に実装されるアプリケーションのアプリケーションユーザアカウントの管理に関しては、提供者の責任ではない。利用者の組織は、アカウントの管理に全面的に責任を負うことが多い（ただし、利用者が、その責任を第三者である ID 管理仲介業者に外部委託する場合を除く）。
- 運用面でのセキュリティ管理策ファミリは、ポリシー、手順、およびプロセスを扱う。利用者は通常、それらの定義に関して責任を負い、提供者は（運用上のパートナーであるため）実施時に責任を共有する。しかしながら、この協力の性質は、これらの管理策が適用可能な範囲に影響を及ぼすだろう。例えば、職員に対して定期的に開催されるセキュリティトレーニングが必要か否か、あるいは実現可能か否かに

ついては、提供者が決定権を持つ必要があるだろう。これらの運用面でのセキュリティ管理策は、提供者が掲示する価格を比較する際に、また、サービス契約の交渉時に利用者が使用できる、チェックリストとなる。

- 表 2 に示されている管理クラスの 4 つのセキュリティ管理策ファミリは、運用クラスのセキュリティ管理策と似ており、利用者側の責任になる。ここで提供者は、これらの要求事項を満たすのに必要なドキュメントと証拠を提供することによって、利用者を支援する補助的な役割を果たす。クラウド提供者によっては、セキュリティマネジメントに関する利用者からの要求事項の一部を満たすために、自身の業務プロセスと技術的解決法を変更する可能性がある。

付録 B－略語

本ガイド内で使用されている頭字語と略語の中から選択されたものの定義を以下に示す。

AJAX	group of Web development methods（一群のウェブ開発方式）
API	Application Programming Interface
CPU	Computer Processing Unit（中央処理装置）
DBMS	Database Management System（データベースマネジメントシステム）
DNS	Domain Name System（ドメインネームシステム）
FISMA	Federal Information Security Management Act（連邦情報セキュリティマネジメント法）
HTML	Hypertext Markup Language（ハイパーテキストマークアップ言語）
HTTP	Hypertext Transfer Protocol（ハイパーテキスト転送プロトコル）
HTTPS	Hypertext Transfer Protocol Secure（ハイパーテキスト転送プロトコルセキュア）
IaaS	Infrastructure as a Service（サービスの形で提供されるインフラストラクチャ）
IDS/IPS	Intrusion Detection Systems/Intrusion Prevention Systems（侵入検知システム／侵入防止システム）
ISO	International Standards Organization（国際標準化機構）
IT	Information Technology（情報技術）
ITL	Information Technology Laboratory（情報技術ラボラトリ）
IA-64	64-bit Intel Itanium architecture（64 ビットインテルアイテニアムアーキテクチャ）
IP	Internet Protocol（インターネットプロトコル）
JVM	Java Virtual Machine（Java 仮想マシン）
NIST	US National Institute of Standards and Technology（米国国立標準技術研究所）
PaaS	Platform as a Service（サービスの形で提供されるプラットフォーム）
OMB	Office of Management and Budget（行政管理予算局）
OVF	Open Virtualization Format（オープン仮想化フォーマット）
PEM	Privacy Enhanced Mail（暗号化された電子メール）

SaaS	Software as a Service（サービスの形で提供されるソフトウェア）
SP	Special Publication （特定発行文書）
SQL	Structured Query Language（構造化された問い合わせ言語）
SSL/TLS	Secure Socket Layer/Transport Layer Security （セキュアソケットレイヤー／トランスポートレイヤーセキュリティ）
TCP	Transmission Control Protocol（通信制御プロトコル）
VLAN	Virtual Local Area Network（仮想ローカルエリアネットワーク）
VM	Virtual Machine（仮想マシン）
VMM	Virtual Machine Monitor（仮想マシンモニター）
VPN	Virtual Private Networks（仮想プライベートネットワーク）
VRF	VPN Routing and Forwarding （仮想プライベートネットワークのルーティングとフォワーディング）
WSDL	Web Services Description Language（ウェブサービス記述言語）
XML	Extensible Markup Language（拡張マークアップ言語）

付録 C－用語集

本刊行物内で使用されている用語の中から選択されたものの定義を以下に示す

認証(Authentication): 多くの場合、情報システムのリソースに対するアクセスを許可するための前提条件として、ユーザ、プロセス、またはデバイスの身元を確認すること。

証明書(Certificate): 情報のデジタル表現であり、少なくとも (1) 証明書を発行する認証機関を識別し、(2) 利用者の名前を挙げるまたは利用者を識別する、(3) 利用者の公開鍵を含む、(4) 証明書の有効期間を識別する、および (5) 証明書を発行する認証機関によってデジタル署名される。

法令順守(Compliance): 職務上の要求事項を満たすための順守行為。

IaaS: 「NIST によるクラウドコンピューティングの定義」に定義されていて、そこから抜粋したものを第 2 章に記載している。

PaaS: 「NIST によるクラウドコンピューティングの定義」に定義されていて、そこから抜粋したものを第 2 章に記載している。

公開鍵暗号(Public key cryptography): 公開鍵とプライベート鍵の 2 つの鍵を使用する暗号方式。通常、利用者は、自身の公開鍵を配布するが、プライベート鍵は自分が所持する。この方式は、「非対称暗号」としても知られている。

SaaS: 「NIST によるクラウドコンピューティングの定義」に定義されていて、そこから抜粋したものを第 2 章に記載している。

サービス契約書(Service agreement): クラウド利用者とクラウド提供者間の法的契約の決め事を明記した法的ドキュメント。

サービス契約書(Service-level agreement): 技術的パフォーマンスに関するクラウド提供者側の約束と、紛争をどのように発見し処理するか、および契約の不履行に対する補償について明記したドキュメント。

仮想マシン(Virtual machine (VM)): 実在するマシンの複製であり、実能力を備え、他と分離されている[Pop74]。

仮想化(Virtualization): ソフトウェアおよび／またはハードウェアをシミュレーションしたものであり、そこで他のソフトウェアを稼働できる[NIST SP 800-125]。

付録 D－参考文献

以下の一覧は、有用なリソースの例を示すものである。

[Ado11] Adobe Systems Inc., "Adobe Flex Framework Technologies", 2011, http://labs.adobe.com/technologies/flex.

[Ama06] Amazon Web Services, "Amazon Simple Storage Service API Reference," Copyright @ 2010 Amazon Web Services LLC or its affiliates, http://awsdocs.s3.amazonaws.com/S3/latest/s3-api.pdf.

[Ama10] Amazon Web Services, "Amazon Elastic Compute Cloud API Reference API Version 2010-11-15", 2010, http://aws.amazon.com/documentation/ec2.

[Ama12] Amazon Web Services, “Amazon Elastic Beanstalk,” Copyright @ 2012 Amazon Web Services LLC or its affiliates, http://aws.amazon.com/elasticbeanstalk.

[Can11] Canonical Ltd., Bazaar branches of Eucalypus (source code), 2011, [Online] https://code.launchpad.net/eucalyptus.

[Cha06] Fay Chang, Jeffrey Dean, Sanjay Ghemawat, Wilson C. Hsieh, Deborah A. Wallach, Mike Burrows., Tushar Chandra, Andrew Fikes, Robert E. Gruber, "Bigtable: A Distributed Storage System for Structured Data," 2006, Proceedings of the 7th USENIX Symposium on Operating Systems Design and Implementation, Nov. 6-8, Seattle, WA.

[Che94] William R. Cheswick, Steven M. Bellovin, "Firewalls and Internet Security: Repelling the Wily Hacker," 1994, Addison-Wesley, ISBN B000OOQ4R0.

[Chr05] Christopher Clark, Keir Fraser, Steven Hand, Jacob Gorm Hansen, Eric Jul, Christian Limpach, Ian Pratt, Andrew Warfield, "Live Migration of Virtual Machines," Proceedings of the 2nd Symposium on Networked Systems Design and Implementation, May 2-4, 2005, Boston MA.

[Cho06] Frederick Chong and Gianpaolo Carraro, "Architecture Strategies for Catching the Long Tail," Microsoft Corporation, April 2006. http://msdn.microsoft.com/en-us/library/aa479069.aspx.

[Com88] Douglas Comer, "Internetworking with TCP/IP Principles, Protocols, and Architectures," Prentice-Hall, Inc., 1988, ISBN 0-13-470154-2.

[Dea04] Jeffrey Dean and Sanjay Ghemawat, "MapReduce: Simplified Data Processing on Large Clusters," Proceedings of the 6'th USENIX Symposium on Operating Systems Design and Implementation, Dec. 6-8, 2004, San Francisco, CA.

[Die08] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2,” 2008, IETF RFC 5246, http://www.ietf.org/rfc/rfc5246.txt.

[Dja11] Django Software Foundation, "django The Web framework for perfectionists with deadlines," 2011, http://www.djangoproject.com.

[DMT09] Distributed Management Task Force, "Open Virtualization Format Specification, Version 1.0.0", 2009, online: http://www.dmtf.org/sites/default/files/standards/documents/DSP0243_1.0.0.pdf.

[Eps99] Jeremy Epstein, "Architecture and Concepts of the ARGuE Guard," Proceedings of the 1999 Annual Computer Security Applications Conference, Dec. 6-10, 1999, Phoenix, Arizona.

[Fed10] CIO Council, "Proposed Security Assessment and Authorization for U.S. Government Cloud Computing, Draft version 0.96, Nov. 2010. Online: www.FedRAMP.gov.

[Fer92] David F. Ferraiolo and D.R. Kuhn, "Role Based Access Control," Proceedings of the 15th National Computer Security Conference, Oct 13-16, 1992, pp. 554-563.

[Gar05] Jesse James Garrett, "Ajax: A New Approach to Web Applications," 2005, http://www.adaptivepath.com/ideas/essays/archives/000385.php.

[Gas88] Morrie Gasser, "Building a Secure Computer System," 1988, Van Nostrand Reinhold Company Inc., ISBN 0-442-23022-2.

[Ghe03] Sanjay Ghemawat, Howard Gobioff, and Shun-Tak Leung, "The Google File System," SOSP '03, Oct 19-22, 2003, Bolton Landing, New York, USA.

[Goo11] Google, "Google App Engine", Copyright 2011 Google, http://code.google.com/appengine.

[Goo11-2] Google, "Google Web Toolkit", Copyright 2011, http://code.google.com/Webtoolkit.

[ISO/IEC 23271:2006] Information technology -- Common Language Infrastructure (CLI) Partitions I to VI, 2006, JTC1/SC22, online: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

[Kar09] A. H. Karp, H. Haury, and M. H. Davis, “From ABAC to ZBAC: the Evolution of Access Control Models,” Tech. Report HPL-2009-30, HP Labs, Feb. 21, 2009, http://www.hpl.hp.com/techreports/2009/HPL-2009-30.pdf.

[Lind99] Tim Linkholm and Frank Yellin, "The Java Virtual Machine Specification Second Edition," 1999, online, http://java.sun.com/docs/books/jvms/second_edition/html/VMSpecTOC.doc.html.

[Mar09] Moxie Marlinspike, "New Tricks for Defeating SSL In Practice," 2009, http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf.

[Mat08] Jeanna N. Matthews, Eli M. Dow, Todd Deshane, Wenjin Hu, Jeremy Bongio, Patrick F. Wilbur, Brendan Johnson, "Running Xen a Hands-On Guide to the Art of Virtualization," Pearson Education, Inc., 2008, ISBN-13: 978-0-132-34966-6.

[Mic10] Microsoft, "Hyper-V: Using Live Migration with Cluster Shared Volumes in Windows Server 208 R2," Microsoft TechNet August 25, 2010. http://technet.microsoft.com/en-us/library/dd446679(WS.10).aspx.

[Mic11] Microsoft, "Microsoft Silverlight," 2011, http://www.microsoft.com/silverlight.

[Moc87-1] Paul Mockapetris, "Domain Names - Concepts and Facilities," IETF RFC 1034, 1987, http://tools.ietf.org/html/rfc1034.

[Moc87-2] Paul Mockapetris, "Domain Names - Implementation and Specification," IETF RFC 1035, 1987, http://tools.ietf.org/html/rfc1035.

[Mos05] Tim Moses, "eXtensible Access Control Markup Language (XACML) Version 2.0," OASIS Standard, Feb. 1, 2005, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf.

[Msf11] Microsoft, "Windows Azure Storage Services REST API Reference," Copyright 2011 Microsoft, http://msdn.microsoft.com/en-us/library/dd179355.aspx.

[Msf11-2] Microsoft, "Windows Azure," Copyright 2011 Microsoft, http://msdn.microsoft.com/en-us/library/dd179367.aspx.

[Nas10] NASA Nebula IaaS Team, "NASA Nebula IaaS", 2010, http://nebula.nasa.gov.

[Net96] Netscape, "The SSL Protocol: Version 3.0," Netscape/Mozilla, 1996. http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt.

[Nur08] Nurmi, Daniel, Rich Wolski, Chris Grzegorczyk, Graziano Obertelli, Sunil Soman, Lamia Youseff, Dmitrii Zagorodnov, "The Eucalyptus Open-source Cloud-computing System," in Proceedings of the 2009 IEEE/ACM International Symposium on Cluster Computing and the Grid, May 2009.

[Nur08-2] Nurmi, Daniel, Rich Wolski, Chris Grzegorczyk, Graziano Obertelli, Sunil Soman, Lamia Youseff, Dmitrii Zagorodnov, "Eucalyptus A technical report on an elastic utility computing architecture linking your programs to useful systems," UCSB Technical Report, 2008-10.

[Oid11] The OpenID Foundation, "OpenID," 2011, http://openid.net.

[Oix10] Open Identity Exchange, "An Open Market Solution for Online Identity Assurance," Copyright 2010 OIX Corporation, http://openidentityexchange.org/sites/default/files/oix-white-paper-2010-03-02.pdf.

[Opp03] David Oppenheimer, Archana Ganapathi, and David A. Patterson, "Why do Internet services fail, and what can be done about it?" Proceedings of the 4th Usenix Symposium on Internet Technologies and Systems, 2003.

[Orm07] T. Ormandy, "An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments," CanSecWest, 2007, Vancouver, British Columbia.

[Per08] R. Perez, L. van Doorn, R. Sailer, "Virtualization and Hardware-Based Security," Security and Privacy, IEEE , vol.6, no.5, pp.24-31, Sept.-Oct. 2008; URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4639019&isnumber=4639007

[Pop74] Gerald Popek and Robert Goldberg, "Formal Requirements for Virtualizable Third Generation Architectures," July 1974, Communications of the ACM, Vol. 17.

[Por10] Aaron Portnoy, "Pwn2Own2010", 2010, TippingPoint Digital Vaccine Laboratories, online: http://dvlabs.tippingpoint.com/blog/2010/02/15/pwn2own-2010.

[Pyt11] Python Software Foundation, "Extending and Embedding the Python Interpreter," copyright 2011, The Python Software Foundation, online, http://docs.python.org/py3k/extending/index.html#extending-index.

[Rag08] N. Ragouzis et al., "Security Assertion Markup Language (SAML) V2.0 Technical Overview," OASIS Committee Draft, March 2008, http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf.

[Ran99] Marcus Ranum, "Installing the Trusted Information Systems Internet Firewall Toolkit," 1996, http://www.fwtk.org/fwtk/docs/mjr-slides.

[Red10] Redhat, "RED HAT PaaS: Bringing open choice & application portability to the cloud," 2010, http://www.jboss.com/pdf/RedHatPaaSWhitepaper.pdf.

[Red99] Redhat Emerging Technology, "KVM Migration," last updated: June 2009, http://www.linux-kvm.org/page/Migration.

[Ros99] E. Rosen, Y. Rekhter, "BGP/MPLS VPNs," IETF RFC 2547, 1999, http://www.ietf.org/rfc/rfc2547.txt.

[Sal11] salesforce, "Force.com," copyright 2011 salesforce.com, http://www.salesforce.com/platform.

[Sch94] Bruce Schneier, "Applied Cryptography," John Wiley and Sons, Inc., 1994, ISBN 0-471-59756-2.

[Shr10] Gautam. Shroff, "Enterprise Cloud Computing Technology, Architecture, Applications," Cambridge University Press, 2010, ISBN 978-0-521-76095-9.

[Sii01] Software and Information Industry Association, "Strategic Backgrounder: Software as a Service," 2001, [Online] http://www.siia.net/estore/pubs/SSB-01.pdf.

[SNI09] SNIA, "Cloud Storage Use Cases Version 0.5 rev 0," Trial-Use Draft, Copyright 2009 Storage Networking Industry Association, http://www.snia.org/tech_activities/publicreview/CloudStorageUseCasesv0.5.pdf.

[SNI10] SNIA, "Cloud Data Management Interface Version 1.1f," Work In Progress, Copyright 2010 Storage Networking Industry Association, http://www.snia.org/tech_activities/publicreview/CDMI_Spec_v1.01f_DRAFT.pdf.

[TIS94] Trusted Information Systems, "TIS Firewall Toolkit," June 30, 1994, http://www.fwtk.org/fwtk/docs/overview.pdf.

[Vmw11] VMware, "VMware vSphere VMWARE VMOTIONTM Migrate Virtual Machines with Zero Downtime," 2011, http://www.vmware.com/products/vmotion.

[War09] Simon Wardley, Etienne Goyer and Nick Barcet, "Ubuntu Enterprise Cloud Architecture," 2009, online:

http://www.canonical.com/sites/default/files/active/Whitepaper-UbuntuEnterpriseCloudArchitecture-v1.pdf.

[Ylo06] T. Ylonen and C. Lonvick, "The Secure Shell (SSH) Protocol Architecture," 2006, IETF RFC 4251, http://www.ietf.org/rfc/rfc4251.txt.

[Zwi00] Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman, "Building Internet Firewalls," 2000 O'Reilly and Associates, Inc. ISBN 1-56592-871-7.

付録 E－NIST 刊行物

NIST 800 Series Special Publications は、http://csrc.nist.gov/publications/nistpubs/index.htmlから入手できる。

NIST FIPS Publications は、http://csrc.nist.gov/publications/PubsFIPS.htmlから入手できる。

[SP 800-41] NIST Special Publication 800-41, Revision 1, *Guidelines on Firewalls and Firewall Policy*, 2009 年 9 月.

[SP 800-53] NIST Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, 2010 年 5 月 1 日.

[SP 800-63] NIST Special Publication 800-63, *Electronic Authentication Guideline*, 2006 年 4 月.

[SP 800-125] NIST Special Publication 800-125, *Guide to Security for Full Virtualization Technologies*, 2011 年 1 月.

[SP 800-144] NIST Special Publication 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, 2011 年 11 月.

[SP 800-145] NIST Special Publication 800-145, *The NIST Definition of Cloud Computing*, 2011 年 9 月.

[FIPS 200] NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, 2006 年 3 月.

[FIPS 199] NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, 2004 年 2 月.

[FIPS 140] NIST FIPS 140-2, *Security Requirements for Cryptographic Modules*, 2002 年 12 月.