



**National Institute of
Standards and Technology**

U.S. Department of Commerce

Draft Special Publication 800-144

パブリッククラウドコンピューティングの セキュリティとプライバシーに関する ガイドライン

Wayne Jansen
Timothy Grance

Draft NIST Special Publication

パブリッククラウドコンピューティングの
セキュリティとプライバシーに関するガイドライン

Wayne Jansen
Timothy Grance

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

2011 年1 月



米国商務省 長官

Gary Locke

米国国立標準技術研究所 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ー (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。

米国国立標準技術研究所、Special Publication 800-144、60 頁

(2011 年 1 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。

本レポートは、原典に沿ってできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありません。翻訳監修主体は本レポートに記載されている情報より生じる損失または損害に対して、いかなる人物あるいは団体にも責任を負うものではありません。

要旨

クラウドコンピューティングが意味するものは、人によってさまざまである。ほとんどのクラウドに共通の特性としては、信頼性の高いコンピューティングリソースの集積を、必要なときに必要な規模で利用できること、サービスが計測可能でどこからも安全に利用できること、データを組織の内部から外部に移行できることなどが挙げられる。これらの特性の諸側面はある程度まで実現しているが、クラウドコンピューティングは、いまだ、発展途上にあるといえる。本文書は、パブリッククラウドコンピューティングのセキュリティとプライバシーに関する課題を概説し、組織がデータ、アプリケーションおよびインフラをパブリッククラウド環境にアウトソースする際に考慮すべき事項を示すものである。

キーワード: クラウドコンピューティング; コンピュータセキュリティおよびプライバシー; IT のアウトソーシング

目次

EXECUTIVE SUMMARY	VI
1. はじめに.....	1
1.1 作成機関.....	1
1.2 目的および適用性.....	1
1.3 対象となる読者.....	1
1.4 本文書の構成.....	2
2. 背景.....	3
3. パブリッククラウドサービス.....	7
3.1 サービスアレンジメント.....	7
3.2 セキュリティに関する利点.....	8
3.3 セキュリティ上のデメリット.....	10
4. セキュリティおよびプライバシーに関する重要な問題.....	13
4.1 ガバナンス.....	13
4.2 コンプライアンス.....	14
4.3 トラスト.....	16
4.4 アーキテクチャ.....	19
4.5 アイデンティティとアクセスの管理.....	22
4.6 ソフトウェアの隔離.....	23
4.7 データの保護.....	24
4.8 可用性.....	26
4.9 インシデント対応.....	28
4.10 推奨事項のまとめ.....	28
5. パブリッククラウドのアウトソーシング.....	30
5.1 一般的な懸念事項.....	31
5.2 事前の実施事項.....	33
5.3 契約開始と契約期間中の実施事項.....	35
5.4 終了のための実施事項.....	36
5.5 推奨事項のまとめ.....	36
6. むすび.....	38
7. 参考文献.....	39
付録 A – 略語.....	51
付録 B – オンライン参考文献.....	52

EXECUTIVE SUMMARY

NIST の定義によると、クラウドコンピューティングとは、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[Mel09]。クラウドコンピューティングテクノロジーは、多様なアーキテクチャによって実装することができ、選択可能なサービスモデルや実装モデルも複数存在する。また、その他のテクノロジーやソフトウェアデザインアプローチと併用することもできる。クラウドコンピューティングにおいてセキュリティを確保するのは容易でない。とりわけ、パブリッククラウドでは、そのインフラとコンピューティングリソースの所有者がそれらのサービスを一般向けに販売する外部の者となるため、なおさら厄介である。

クラウドコンピューティングの出現によって、連邦政府機関およびその他の組織のシステムとネットワークに広範な影響がもたらされると期待される。一方、クラウドコンピューティングを魅力的にする機能の多くは、従来のセキュリティモデルや管理策が適用できない可能性がある。本文書は、パブリッククラウドコンピューティングの概要と、考慮すべきセキュリティおよびプライバシー問題を示すことを主な目的としている。具体的には、パブリッククラウド環境における脅威、技術上のリスク、保護対策、およびそれらにどう対処すべきかについて記述する。

以下は、本文書から抽出された主要なガイドラインの要約である。連邦政府の各省庁および機関には、これらのガイドラインを適用することが推奨される。

クラウドコンピューティングのソリューションを利用する前に、セキュリティとプライバシーの諸側面について慎重に企画すること

クラウドコンピューティングでは、他の新しい IT 分野と同様にデータの機微度 (sensitivity) に十分配慮する必要がある。計画作成は、コンピューティング環境の安全性を最大限に確保し、組織の関連するすべてのポリシーへの準拠を確実にし、データプライバシーの維持を確実にすることに役立つ。また、IT への支出の効用を最大限に引き出せるようにすることに役立つ。

IT サービスをアウトソーシングすべきか否かの判断、とりわけ、組織のデータやアプリケーションなどのリソースをパブリッククラウドコンピューティング環境に移行すべきか否かの判断では、組織のセキュリティ目的が重要な決定因子となる。アプリケーションの開発とサービスの提供に関するポリシー、手順、標準、ならびに実装された、または稼働中のサービスの設計、実施、テスト、モニタリングに関する組織の IT 実践規範は、クラウドコンピューティング環境にも適用されるべきである。

費用を最小限に抑えつつ最大限の効果を得るには、システムの開発ライフサイクルの初期プランニングの段階からセキュリティとプライバシーを考慮する必要がある。システムの導入・展開後にセキュリティに取り組むことは、はるかに困難であり費用も高くなるばかりか、リスク度も増す。

そのクラウドプロバイダが提供するパブリッククラウドコンピューティング環境を理解し、クラウドコンピューティングというソリューションが組織のセキュリティおよびプライバシー要件を満たすことを確認すること

一般的に、クラウドプロバイダは特定の組織のセキュリティおよびプライバシーニーズを把握していない。組織の要求条件を満たすために、クラウドコンピューティング環境は調整できるようにされていると期待される。組織は、選択したパブリッククラウドコンピューティング環境に対して、組織のセキュリティやプライバシーなどの要求条件を満たすよう設定、実装、管理されることを要求するべきである。

パブリッククラウドコンピューティングでは、交渉の余地のないサービス契約、すなわち、クラウドプロバイダがサービス条項を一方的に定めるような契約が一般的である。交渉によるサービス契約も可能である。交渉による契約では、政府機関による従来型の IT アウトソーシング契約と同様に、セキュリティおよびプライバシーの細部にわたる組織の関心事を盛り込むことができる。これには、職員に対する信用度調査、データの所有権とその停止の権利、利用者アプリケーション間の隔離、データの暗号化と分別、サービスの有効性の測定と報告、法規制の順守、連邦政府または国家の標準(例:FIPS140)を満たす製品の利用などが含まれる。

重要なデータおよびアプリケーションをパブリッククラウドで使用する場合、交渉ベースのサービス契約を結ぶことが必要だろう。しかしながら、交渉内容によっては、交渉の余地のないサービス契約によってパブリッククラウドコンピューティングにもたらされるスケールメリット(規模の経済)が損なわれ、変更結果が費用対効果を下げるといった結果を招く恐れがある。そこで組織は、代替案として、パブリッククラウドサービスでは不足することが判明した部分を補うために補完的管理策を採用してもよい。もう一つの代替案は、より適した実装モデル(例えば、プライベートクラウド)を選択することである。それにより、セキュリティとプライバシーをより厳密に監視・コントロールできるようになる。

クライアント側のコンピュータ環境が、組織のクラウドコンピューティングに関するセキュリティおよびプライバシー要件を満たすことを確認すること

クラウドコンピューティングは、サーバー側とクライアント側で構成される。通常、サーバー側に重きが置かれるため、クライアント側はおろそかになりがちである。クライアント側の物理的および論理的セキュリティを維持することは、とりわけスマートフォンなどの組み込み携帯機器の場合には、困難を伴う。そうした機器のサイズと持ち運び可搬なことで、物理的なコントロールが不可能な場合がある。あらかじめ組み込まれているセキュリティ機能は使われないことが多く、知識の豊富な者によって容易に破られたり、すり抜けられ、装置のコントロールを奪われる可能性がある。

ウェブブラウザは広く提供されてどこでも手に入ることから、クラウドコンピューティングサービスへのクライアント側からのアクセスの主たる手段となっている。クライアントからサービスにアクセスするためには、小さな軽量のアプリケーションをデスクトップまたは携帯機器に装着してもよい。ウェブブラウザ向けに用意されたさまざまなプラグインや拡張機能はセキュリティが問題になっている。ブラウザのアドオンの多くはまた、自動的アップデート機能を持たないため、既存の脆弱性が解消されずに残っている可能性を高めている。同様の問題が他の種類のクライアントにも存在する。

ソーシャルメディア、パーソナルウェブウェブメール、およびその他の一般に利用可能なサイトの提供と利用の増加は、関連するリスクがあり、1つの懸念材料である。なぜなら、ソーシャルエンジニアリング攻

撃を受けた場合に、クライアントだけでなく、そのベースとなるプラットフォームや利用対象のクラウドサービスにまで悪影響が及ぶ可能性があるからである。また、アタッカーが、クライアントデバイス上で、バックドアを仕込むトロイの木馬、キーストロークロガー、その他のマルウェアを動作させるのに成功すれば、クラウドまたはその他のウェブベースのサービスのセキュリティを損なわせることができる。クラウドコンピューティングの全体的なセキュリティアーキテクチャの一環として、組織には、既存の対策の見直しを行い、必要であれば追加の対策を実施して、クライアント側のセキュリティを確保することが求められる。

パブリッククラウドコンピューティング環境に導入・展開されているデータおよびアプリケーションのプライバシーとセキュリティに対する説明責任を満たすこと

組織は、クラウドコンピューティングに対する適切なセキュリティマネジメントの実践と管理を展開すべきである。強力なマネジメントの実践は、セキュアなクラウドコンピューティングのソリューションを運用し維持管理するうえで不可欠である。セキュリティおよびプライバシーに関する実践規範には、組織の情報システム資産のモニタリングと、ポリシー、標準、手順、ガイドラインの適用状況を評価して情報システムリソースの機密性、完全性、可用性を確立し維持することが含まれる。

クラウドコンピューティングシステムにおけるリスクを評価し管理することは、困難な課題と言える。リスク分析では、質的要素と量的要素の両方を考慮しなければならない。リスクは、利用可能な技術面、管理面、運用面での保護対策に照らして慎重に評価しなければならない。リスクを受容可能なレベルまで軽減するために必要な手立てを講じなければならない。組織はまた、セキュリティおよびプライバシー管理策が正しく導入されていること、意図したとおりに運用されていること、組織の要求条件を満たしていることを確実にしなければならない。

クラウドサービス環境について一定レベルの信頼を確立できるかどうかは、そのサービスの提供者が、組織のデータおよびアプリケーションを保護するのに必要なセキュリティ管理策を配備することができるかと、それらの管理策の有効性を立証できるかによる[Jcf10]。しかし、サブシステムが正しく機能していることと、セキュリティ管理策が有効であることを自組織内のシステムに対する検証と同じように詳細に検証することができない場合がある。このような場合、第三者による監査など、他の手段によって信頼を確立することも必要である。最終的に、提供されるサービスの信頼の度合いが期待を下回る場合で、かつ、組織が補完的管理策を採用できない場合には、そのサービスを利用しない、または、より高いレベルのリスクを受容することになる。

一般的に、組織は、クラウドベースのアプリケーションに対して、そのアプリケーションが組織内に展開された場合と同等またはそれ以上のセキュリティ管理策を実施する必要がある。クラウドコンピューティングは、その多くの構成要素、例えばセルフサービス、割り当て量の管理、リソースの計測のための要素に加え、ハイパーバイザ、ゲスト仮想マシン、サポートミドルウェア、実装されたアプリケーション、データストレージなどの構成要素各々のセキュリティに大きく依存する。簡易化されたインターフェースおよびサービスの抽象化の多くは、セキュリティに影響を与える内部の複雑さを覆い隠す。組織は、実現可能な範囲で、これらの構成要素のすべてがセキュアであり、健全なセキュリティ実践規範に基づいてセキュリティが維持されていることを確実にしなければならない。

1. はじめに

クラウドコンピューティングでは、コンピューティングリソースを低価格で柔軟に調達することができ、しかも可用性が高いことから、近年、急速に関心を集めている。しかしながら、パブリッククラウドコンピューティング環境へのアプリケーションの移行を検討している政府機関や他の組織にとっては、セキュリティとプライバシーに関する問題があり、このことが本文書を作成する背景となっている。

1.1 作成機関

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が、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(翻訳者注: 著作権に関するこの記述は、SP800-144 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)。

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遵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ではない。また、これらのガイドラインは、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の既存の権威に変更を加えたり、これらに取って代わるものと解釈してはならない。

1.2 目的および適用性

本文書の目的は、パブリッククラウドコンピューティングについて概説し、セキュリティおよびプライバシーに関する課題を示すことにある。本文書は、パブリッククラウド環境における脅威、技術上のリスク、保護対策について記述するものであり、これらの課題に対する IT の観点からの意思決定を十分な情報に基づいて行うための知識を提供するものである。

1.3 対象となる読者

本文書の対象と想定する読者には、以下の分野の人が含まれる。

-
- クラウドコンピューティングの推進について意思決定を行う者(システムマネージャ、経営層、情報管理責任者)
 - セキュリティの専門家(セキュリティ責任者、セキュリティ管理者、監査人、その他 IT セキュリティに責任を持つ者、など)
 - クラウドコンピューティングのセキュリティおよびプライバシー対策に携わる IT プログラムマネージャ
 - システムおよびネットワーク管理者
 - パブリッククラウドコンピューティングサービスのユーザ

本文書の内容は必然的に技術的なものになるが、読者が内容を理解しやすいように背景説明も提供している。本文書は、読者が OS およびネットワークに関する最低限の専門知識と、クラウドコンピューティングに関する基礎知識を有することを前提にしている。クラウドコンピューティングにおけるセキュリティおよびプライバシー問題は日々変化するため、他の情報源も活用して、より詳細でかつ最新の情報を入手することを推奨する。他の情報源としては、本文書内で参照したりリスト化されている多彩な刊行物を含む。その多くは、インターネット上で入手可能である。

1.4 本文書の構成

本文書は以降、次のように構成されている。

- **第 2 章**では、パブリッククラウドコンピューティングを概説する。
- **第 3 章**では、セキュリティおよびプライバシーの観点からパブリッククラウドサービスのメリットとデメリットについて記述する。
- **第 4 章**では、パブリッククラウドコンピューティングにおけるセキュリティおよびプライバシーに関する主な問題点と、それらの問題を緩和するための予防措置を記述する。
- **第 5 章**では、データとアプリケーションの管理をクラウドプロバイダにアウトソーシングする際のセキュリティおよびプライバシー問題に対処するためのガイダンスを示す。
- **第 6 章**では、結論を手短かに述べる。
- **第 7 章**では、参考文献の一覧を示す。

本文書には、補足資料として、付録も用意されている。付録 A には略語の一覧が、付録 B にはその他の参考文献の一覧が記載されている。

2. 背景

NIST の定義によると、クラウドコンピューティングとは、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[Mel09]。クラウドコンピューティングは、インターネットまたはその他のコンピューターネットワークを介して利用できるオンデマンドサービスであり、一つまたは複数の階層で抽象化されたコンピュータインフラの利用を可能にするという意味において、コンピュータの新しいパラダイムであると考えられることができる。クラウドコンピューティングは、より低いコストでより大きな柔軟性と利用可能性が得られると期待されることから、近年、高い関心と呼ぶテーマとなっている。

クラウドコンピューティングサービスでは、リソースを広範に利用できること、専門特化できること、その他の実用的な効率性によって、スケールメリットを享受することができる。とはいうものの、クラウドコンピューティングは、発展途上の分散型コンピューティングの一形態であり、まだ幼年期段階である。クラウドコンピューティングという用語は現在よく使われているが、その意味と解釈は多岐にわたる[Fow09]。クラウドコンピューティングについての記述の多くは、定義に関するものである。その目指すところは、クラウドコンピューティングの利用に関する主要なパラダイムを定義することと、サービスの重要な諸相の概念整理をするために汎用性のある分類を提供することにあり。

パブリッククラウドコンピューティングは、定義づけがなされているいくつかの実装モデルの内の、ひとつである。パブリッククラウドは、その構成要素であるクラウド基盤とその他のコンピューティングリソースを一般の人々がインターネット経由で利用できるようにしたモデルである。パブリッククラウドは、そのクラウドサービスを販売するクラウドプロバイダが所有者であり、その定義上必然的に、組織の外部に存在する。それとは正反対のモデルとして、プライベートクラウドがある。プライベートクラウドでは、コンピュータ環境が特定の組織のためだけに運転される。その管理はその組織自身または第三者により行われ、存在場所としてはその組織のデータセンタにホストされるか、またはその組織の外部となる。プライベートクラウドでは、パブリッククラウドよりも幅広い、クラウド基盤とコンピューティングリソースに対するコントロールが可能である。

パブリッククラウドとプライベートクラウドの間に属する他の二つの実装モデルとして、コミュニティクラウドとハイブリッドクラウドがある。コミュニティクラウドはプライベートクラウドに似ているが、クラウド基盤とコンピューティングリソースは、単一の組織によって独占的に使用されるわけではなく、プライバシー、セキュリティ、規制に関する共通の関心事を持つ複数の組織によって共用される。ハイブリッドクラウドは、二つ以上のクラウド(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、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、相互運用を実現している。

クラウドのコンピュータ環境に対する組織の管理範囲とコントロールは、実装モデルによって異なるが、同様に、クラウドが提供するサービスモデルによっても異なる。以下に、広く知られている使用頻度の高い三つのサービスモデル[Lea09, Vaq09, You08]を示す。

- **Software-as-a-Service (SaaS)**。 ソフトウェア・アズ・ア・サービス (SaaS)は、ソフトウェア提供モデルの1つである。単一または複数のアプリケーションと、それらのアプリケーションを稼働させるためのコンピューティングリソースを即座に使えるサービスとしてオンデマンドで提供する。このモデルの主な目的は、ハードウェアとソフトウェアの開発、メンテナンス、運用にかかる総費用を減らすことにある。セキュリティの構築は、主にクラウドプロバイダが行う。クラウド利用者は、好みの設定や一部の管理上のアプリケーション設定を除き、ベースとなるクラウド基盤または個々のアプリケーションの管理・制御を行うことはない。
- **Platform-as-a-Service (PaaS)**。 プラットフォーム・アズ・ア・サービス (PaaS)は、ソフトウェア提供モデルの1つである。コンピューティングプラットフォームをオンデマンドで提供し、その上でアプリケーションを開発し走らせることができる。このモデルの主な目的は、ベースとなるハードウェアおよびソフトウェアコンポーネント(必要なプログラムおよびデータベースの開発ツールを含む)の調達、ハウジング、管理に伴う費用と手間を減らすことにある。通常、構築される開発環境は、特定の用途に用いられる。その用途はクラウドプロバイダが設定し、そのプラットフォームのデザインとアーキテクチャに合わせて調整される。クラウド利用者は、プラットフォーム上のアプリケーションとそれらのアプリケーションの環境設定に対する管理を行うことができる。セキュリティの構築は、プロバイダとユーザの各々に分割される。
- **Infrastructure-as-a-Service (IaaS)**。 インフラストラクチャ・アズ・ア・サービスは、ソフトウェア提供モデルの1つである。サーバー、ソフトウェアおよびネットワーク装置からなるコンピューティング基盤をオンデマンドで提供し、その基盤上にアプリケーションを開発・実行するためのプラットフォームを構築できる。このモデルの主な目的は、基本的なハードウェア・ソフトウェア基盤用コンポーネントの調達、ハウジング、管理を行うことなく、そのようなリソースをサービスインターフェースを介して制御可能な仮想オブジェクトをリソースとして手に入れることにある。通常、クラウド利用者は OS とその上に載る開発環境を自由に選択することができる。ベースとなる基盤以外に必要なセキュリティの構築は、主にユーザが受け持つことになる。

図1に、上述のサービスモデルごとの、クラウド利用者とプロバイダ間の管理範囲とコントロールの違いを示す。図の中央にあるのは、一般化されたクラウド環境の概念化された5つのレイヤであり、パブリッククラウドをはじめとする、各実装モデルに適合する。図の左右にある矢印は、各サービスモデルのクラウド環境に対する管理範囲とコントロールのおおまかな範囲を、ユーザとプロバイダについて示している。一般的に、クラウドプロバイダから得られるサポートのレベルが高いほど、システムに対するクラウド利用者の管理範囲とコントロール領域が狭くなる。

下位の2つのレイヤは、クラウド環境における物理エレメントである。これらは、選択されたサービスモデルにかかわらず、クラウドプロバイダによってコントロールされる。最下位のレイヤである「ファシリティ」レイヤは、施設に必要な暖房・換気・空調 (HVAC)、電力、通信その他の物理的プラント構成要素によって構成される。一方、「ハードウェア」レイヤは、コンピュータ、ネットワークおよびストレージのコンポーネントと、その他の物的コンピューティング基盤構成要素によって構成される。

残りのレイヤは、クラウド環境における論理エレメントである。「仮想化基盤」レイヤは、ハイパーバイザ、仮想マシン、仮想データストレージ、サポートミドルウェアコンポーネントなどのソフトウェアエレメントによって構成され、

コンピューティングプラットフォームの構築に必要なクラウド基盤を実現するために使用される。通常このレイヤでは、仮想マシンテクノロジーが使用されるが、その他の手段を使って必要なソフトウェアの抽象化を提供することも可能である。同様に、「プラットフォームアーキテクチャ」レイヤは、コンパイラ、ライブラリ、ユーティリティ、ならびにアプリケーションの実装に必要なその他のソフトウェアツールおよび開発環境によって構成される。「アプリケーション」レイヤは、エンドユーザであるソフトウェア利用者に向けて提供されたソフトウェアアプリケーションまたはその他のプログラムを示す。これらのアプリケーションとプログラムは、クラウドを介して利用に供される。

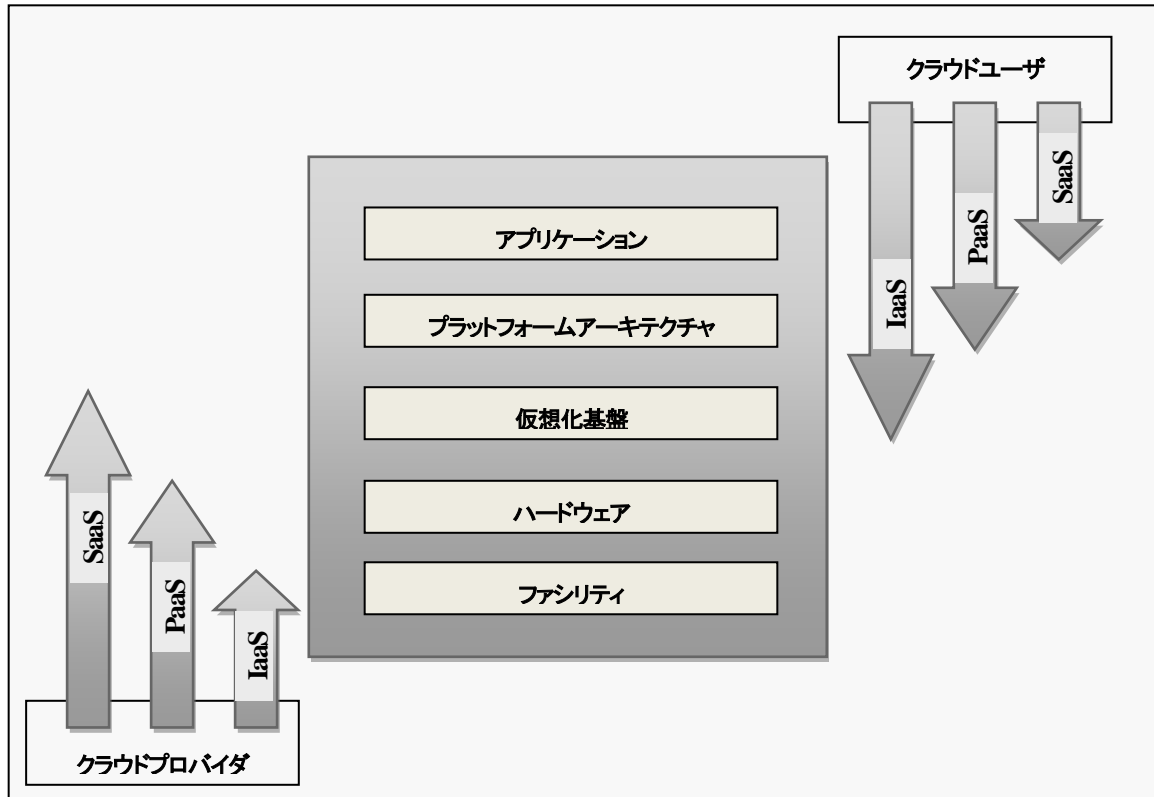


図1:クラウドサービスモデルによる管理範囲およびコントロールの違い

IaaS と PaaS の違いが曖昧だと主張する人もいる。実際に多くの商用サービスにおける両者の関係は、異なるというよりは似ているといえる[Arm10]。とはいえものの、「IaaS」と「PaaS」という用語は役に立っている。ごく基本的な支援環境と、より高レベルの支援を提供する環境との区別を示し、そのことによって、IaaS と PaaS ではクラウド利用者およびクラウドプロバイダに割り当てられるコントロールと責任の範囲が異なることを示している。

クラウドコンピューティングは、特定の組織専用組織内プライベートクラウドとして実装することができるが、本来の目的は、その環境の一部を、外部の存在に対してパブリッククラウドとして、アウトソーシングに供するための手段を提供することにある。他の IT サービスのアウトソーシングと同様に、クラウドコンピューティングにも、コンピュータセキュリティおよびプライバシーに関する懸念が存在する。主な問題としては、重要なアプリケーションまたはデータを組織のコンピューティングセンタの内側から一般の人々が簡単にアクセスできる別組織の環境(すなわち、パブリッククラウド)に移すことによって生じるリスクが中心となる。

パブリッククラウドに移行する一番の動機は、コストを下げ高い効率性を実現することにあるが、セキュリティに対する責任を軽減するための移行であってはならない。最終的に、組織は、アウトソーシングしたサービスの全般的なセキュリティに対して責任がある。発生するセキュリティ問題をモニタリングし、それらの問題に対処することは、パフォーマンスや可用性などの他の重要な問題を監視するのと同様に組織の責務である。クラウドコンピューティングは、新たなセキュリティ課題をもたらすため、クラウドプロバイダがどのようにしてコンピューティング環境のセキュリティを確保し、その環境を維持管理し、データを保護するかについて、組織が監視し管理することが必要不可欠である。

3. パブリッククラウドサービス

クラウドコンピューティングサービスの様相は、組織間で大きく異なる場合がある。なぜならば、組織の目的、保有する資産、公開レベル、直面する脅威、リスク許容度は組織ごとに異なるからである。たとえば、国民一人一人に関するデータを主に扱う政府機関と、そうでない政府機関とでは、セキュリティ目的が異なる。同様に、一般に利用されるための情報を作成し配布する政府機関と、組織内でのみ利用に限定した機密情報を主に扱う政府機関の間にも相違がある。リスクの観点から考えると、ある組織にクラウドサービスが向いているかどうかの判断には、組織の業務の流れと、組織が直面する可能性の高い脅威がもたらす影響についての理解が不可欠である。

従って、IT サービスをアウトソーシングすべきか否かの判断、とりわけ、組織のリソースをパブリッククラウドコンピューティングおよび特定プロバイダのサービスやサービスアレンジメントに移行すべきか否かの判断では、組織のセキュリティ目的が重要な決定因子となる。ある組織で役に立つものが、他の組織でも役に立つとは限らない。また、実際問題としてすべてのコンピュータリソースと資産を可能な限り高いレベルで保護することはコスト面で不可能であるとする組織が多く、結果として組織は、選択可能なオプションに対してコスト、重大性 (criticality)、機密性 (sensitivity) に基づいた優先順位付けを行うことになる。パブリッククラウドコンピューティングがもたらすメリットを判断する際には、組織のセキュリティ目的を頭に入れ、それに基づいて判断することが重要になる。最終的に、クラウドコンピューティングに関する決定は、そこに発生するトレードオフに対するリスク分析に基づいて行われることになる。

3.1 サービスアレンジメント

パブリッククラウドサービスの仕様とサービスについての取り決めは、通常サービスレベル契約 (Service Level Agreement SLA) と呼ばれる。SLAは、期待されるサービスレベルと、プロバイダがそのレベルのサービスを提供できなかった場合に利用者が受け取る補償に関して、利用者とプロバイダの間でなされる合意を意味する。しかしながら、通常、SLAといった場合には、サービス契約またはサービス合意書が規定するサービス条項の一部を示すことが多い。サービス条項には、他の重要な詳細内容、例えばサービスの使用許可、使用基準、サービスの停止と契約終了、免責条項、プライバシーに関するポリシー、サービス条項の変更規定などが含まれる。本文書では、サービス契約全般を示す用語として「SLA」を使用している。¹

SLA には、あらかじめ定められた交渉の余地のない契約と、交渉による契約の二種類がある[Bra10, UCG10]。交渉の余地のない契約は、いろいろな面でパブリッククラウドコンピューティングが発揮するスケールメリットの基となる。サービス条項はクラウドプロバイダによって、一部の例外を除いて一方的に定められるだけでなく、利用者に直接通知することなく、(例: インターネット上に更新版が掲示されるだけ) 一方的に変更が行われる[Bra10]。交渉可能な SLA は、従来型の IT アウトソーシング契約に近い。交渉可能な SLA は、セキュリティおよびプライバシーに関するポリシー、手順、技術的管理策についての組織の要望、たとえば、職員に対する信用度調査、データの所有権とその停止の権利、利用者アプリケーション間の隔離、データの暗号化と分別、サービ

¹ 状況によっては、SLA が単なるサブセットではなく、サービス合意または契約全般を意味することもある[Kan09]。

スの有効性の測定と報告、法規制の順守(例:FISMA)、国家標準または国際標準(例:FIPS140-2)を満たす製品の利用などが扱われる。

重要なデータおよびアプリケーションをパブリッククラウドで使用する場合、交渉可能な SLA を結ぶことが必要だろう[Wall0]。しかしながら、交渉内容によっては、交渉の余地のない SLA がもたらすスケールメリットが著しく阻害され負の影響を受けるため、通常、交渉可能な SLA は交渉の余地のない SLA よりも費用対効果で劣る。交渉の成果は、組織の規模や影響力にも左右される。SLA がどちらのタイプであれ、法律面および技術面での適切なアドバイスを得ることは、サービス条項が組織のニーズを十分に満たすことを確実にするために推奨される。

3.2 セキュリティに関する利点

パブリッククラウドコンピューティングにとって最大の障害はセキュリティであるが、クラウドコンピューティングのパラダイムは、セキュリティサービスを提供し技術革新の機会をもたらす、組織全体のセキュリティを向上させる可能性がある。その恩恵を最大に受けるのは、IT アドミニストレータとセキュリティ担当者の数が不足していたり、大規模なデータセンタを有する大きな組織が享受するようなスケールメリットを得られないような小さな組織であるといえるだろう。

パブリッククラウドコンピューティング環境に移行することによってセキュリティ上のメリットを得られる可能性のある分野には、以下ものがある。

- **職員の専門性 (Staff Specialization)**。大規模なコンピュータ設備を有する組織と同様に、クラウドプロバイダのスタッフには、組織にとって興味と関心が深いセキュリティおよびプライバシーなどの分野を専門に扱う機会が与えられる。コンピューティングの規模が大きいほど、より専門性が求められるため、セキュリティ担当者は、他の職務を切り捨ててセキュリティ問題に専念することが許される。専門性が高まることによって、職員は、自身の経験を深め、是正措置を実施し、セキュリティを向上させる機会を、多様な業務を抱えている場合よりも簡単に得ることができる。
- **プラットフォームの強度 (Platform Strength)**。通常、クラウドコンピューティングプラットフォームの構造は、多くの従来型のコンピューティングセンタよりも均一的である。均一性と同一性が高ければ、プラットフォームの強化を実現したり、セキュリティマネジメントの作業(プラットフォームコンポーネントに対する設定管理、脆弱性テスト、セキュリティ監査、セキュリティパッチの適用)の自動化を改良したりすることが容易になる。情報保証およびセキュリティレスポンス業務も、故障管理、ロードバランシング、システムメンテナンスなどのシステムマネジメント業務と同様に、クラウド基盤の均一性と同一性の恩恵を受ける。クラウドプロバイダの多くが、業務上の遵守事項を定めた基準や認証標準を満たしている。具体的には：健康医療分野における、医療保険の携行性と責任に関する法律 (Health Insurance Portability And Accountability Act (HIPAA))、金融分野における、クレジットカード業界のデータセキュリティ基準 (Payment Card Industry Data Security Standard (PCI DSS))、会計監査における、監査基準書 No.70 (Statement on Auditing Standards No. 70 (SAS 70))が挙げられる。

-
- **リソースの可用性 (Resource Availability)**。クラウドコンピューティング設備は拡張が可能であるため、他の設備よりも可用性が高い。クラウドコンピューティング環境には冗長性や災害復旧機能があらかじめ備わっていて、オンデマンドによりリソースが提供される機能は、サービスの需要の増加やDDoS(分散型サービス妨害)攻撃に直面した場合の体制を高められるし、あるいは深刻な事故からの早期復旧にも有効である。インシデント発生時には、実稼働環境に影響を与えずにより詳細な情報を即座に取得することが可能になる。しかしながら、場合によっては、そのような耐障害性があたとなることがある。例えば、分散サービス拒否攻撃が失敗に終わっても、防御に必要な大量のリソースが短時間で消費されてしまい、使用料が跳ね上がり、組織にとっては金銭上の大きな損失となることが考えられる。
 - **バックアップおよびリカバリ (Backup and Recovery)**。クラウドサービスのバックアップおよびリカバリに関するポリシーと手順は、利用者組織が有するものよりも優れていると考えられ、コピーが地理的に散らばって保管されている場合はより堅固であるといえるだろう。クラウド内にあるデータは、色々な状況において、従来型のデータセンタに置かれる場合に比べて可用性が高く、迅速に復旧でき、信頼性も高い。したがって、組織のデータセンタのためのオフサイトバックアップストレージの手段として、従来型のテープベースのオフサイトストレージの代わりにクラウドサービスを使用することも考えられる[Kum08]。しかしながら、インターネット経由のネットワークのパフォーマンスと取り扱うデータの量は、復旧を遅らせる要素となる。
 - **モバイルのエンドポイント (Mobile Endpoints)**。クラウドコンピューティングアーキテクチャには、サービスの末端で、ホストされたアプリケーションにアクセスするのに使われるクライアントも含まれる。クラウドのクライアントにはブラウザベースとアプリケーションベースがある。必要なコンピューティングリソースの主なものはクラウドプロバイダが保有するため、通常、クライアントは軽量のコンピューティング機能であり、ラップトップコンピュータ、ノートパソコン、ネットブックで簡単に利用可能な他、スマートフォン、タブレット、PDAなど組み込みデバイスでも利用できる。²
 - **データの集中管理 (Data Concentration)**。外勤職員を抱える組織にとっては、データをクラウドで保管・処理する方が、同じデータをポータブルコンピューターやリムーバブルメディアに保存して外に持ち出すよりもリスクが少ない。なぜならば、日常的に発生するデバイスの盗難や紛失の可能性を排除できるからである。多くの組織がすでに、ワークフローの管理の向上をはじめとする業務効率の改善を目的として、自組織のデータにモバイル機器からアクセスできる変更を実施している。

パブリッククラウドサービスは、コンピューティングプラットフォームを提供し、自社所有のアプリケーションの代わりに提供するが、それ以外にも以下に示すように、他のコンピューティング環境にセキュリティを提供するために使用することができる。

- **データセンタ向け**。クラウドサービスは、データセンタのセキュリティを向上させるために使用することができる。例えば、電子メールをメールエクステンジ(MX)レコードを介してクラウドプロバイダにリダイレクトし、他のデータセンタからの同様のトランザクションをまとめて検査・分析することによって、広範囲に

²これ自体がセキュリティ上のメリットとなるわけではないが、次の項目に関連していることに留意願いたい。

及ぶスパム、フィッシング、マルウェア活動を検知し、単一の組織が行う場合よりもより包括的に是正措置を取る(例: 疑わしいメッセージやコンテンツを検疫する)といったことが可能である。研究者たちは、ホストベースのアンチウイルスソリューションに代わるものとして、クラウドベースのアンチウイルスサービスを提供するシステム構成の実証に成功している[Obc08b]。

- **クラウド向け。**クラウドサービスは、他のクラウド環境のセキュリティを向上させるために使用することができる。例えば、リバースプロキシ製品を使うと、SaaS 環境内のデータを暗号化した状態で保ちながら、SaaS 環境に自由にアクセスできる[Nav10]。また、クラウドベースのアイデンティティマネジメントサービスも存在する。これは、クラウドユーザの識別・認証に使用される組織のディレクトリサービスに対する追加または代替として利用することができる。

3.3 セキュリティ上のデメリット

パブリッククラウドコンピューティングは、従来型のデータセンタに見られるコンピューティング環境と比較すると、セキュリティとプライバシー関連のさまざまなメリットだけでなく、懸念される事項ももたらすと考えられる。基本的な懸念事項には、以下のものが含まれる。

- **システムの複雑さ (System Complexity)。**パブリッククラウドコンピューティング環境は、従来型のデータセンタと比べると極めて複雑である。パブリッククラウドは多くのコンポーネントによって構成されるため、攻撃の矢面が広がる。パブリッククラウドのコンポーネントには、一般的なコンピューティングのためのコンポーネント(実装されたアプリケーション、仮想マシンモニタ、ゲスト仮想マシン、データストレージ、サポートミドルウェアなど)の他に、管理のための後方機能(セルフサービス、リソースの計測、割り当て量の管理、データの複製とリカバリ、作業負荷管理、およびクラウドバースト³など)を構成するコンポーネントがある。クラウドサービスは、他のクラウドプロバイダが提供するサービスとの入れ子構造化や階層構造化によって実現することもできる。クラウドを構成するコンポーネントは、アップグレードや機能の改良に伴って、時間の経過とともに変わるため、問題がさらに複雑になる。

セキュリティは、多くのコンポーネントの正確さと有効性だけでなく、それらのコンポーネント間の相互作用にも左右される。コンポーネント間の相互作用の数は、コンポーネントの数の二乗にふくれ上がるため、複雑さが増す。通常、複雑さはセキュリティに反比例するため、複雑さが増すことによって脆弱性が生じる[Avo00, Gee08, Sch00]。

- **複数テナントによって共有される環境 (Shared Multi-tenant Environment)。**プロバイダによって提供されるパブリッククラウドサービスには、深刻なややこしさが内在している。つまり、利用者は、通常、コンポーネントとリソースを未知の他の利用者と共有する。ネットワークおよびコンピューティング基盤に対する脅威は年を追うごとに増大し、より高度なものへと進化している。自分の知らない第三者とコンピューティング基盤を共有しなければならないということは、アプリケーションによっては重大な障害となりうる。そして、論理的な分離のために使用されるセキュリティメカニズムの強度に関して高レベルの保証が必

³クラウドバーストは、組織のデータセンタにおけるコンピューティングリソースが飽和状態に陥った場合に、クラウドにアプリケーションを実装しアプリケーションを起動したうえで、リダイレクトされるリクエストに応じる。

要となる。クラウドコンピューティングに限ったことではないが、論理的な分離の問題を侮ってはいけな
い。クラウドコンピューティングの規模なら、なおさらである。設定ミスやソフトウェアエラーが原因で、組
織のデータやリソースに対するアクセスが他のユーザにも見えてしまうことがある。アタッカーが利用者
になりすましてクラウド環境の内側から脆弱性を突く攻撃を仕掛け、不正アクセスを行う可能性もある。

- **インターネットを介したサービス (Internet-facing Services)**。パブリッククラウドサービスは、インターネット
を介して提供されるが、アカウントをセルフサービスで作成することを可能にする管理インターフェースと、
ユーザとアプリケーションが他のサービスにアクセスすることを可能にするインターフェースの両方を、
インターネットにさらすことになる。以前に組織のイントラネットの内側でアクセスされていたアプリケーシ
ョンとデータをクラウドに移行した場合、かつては組織のイントラネットの境界で防ぐことが可能だったネ
ットワーク上の脅威と、露出されたインターフェースを狙う新たな脅威による、リスクの増大に直面する。
その影響は、組織のイントラネットの境界にワイヤレスアクセスポイントを設置した場合にその技術がも
たらす問題と類似する。クラウドプロバイダによって保有される組織の資産を管理するための唯一の手
段として、管理のためのリモートアクセスを要求することは、プラットフォームに対する管理のためのアク
セスをダイレクト接続または内部接続に限定できる従来型のデータセンタに比べてリスクが高い。
- **コントロールの喪失 (Loss of Control)**。クラウドコンピューティングサービスにおけるセキュリティおよび
プライバシー問題は、従来型のクラウド以外のサービスにおける問題と似ているが、クラウドでは組織
の資産が外部の者によって管理されることと、誤った管理がなされる可能性によって問題が深刻化す
る。パブリッククラウドへの移行では、組織の管理下にあった情報およびシステムコンポーネントをクラ
ウドプロバイダの管理下に置きかえることが必要となる。システムとデータの物理的・論理的コントロ
ールの喪失は、状況認識の維持、現行のものと代替のものとの比較検討、優先順位の設定、組織の最
優先事項であるセキュリティとプライバシーに関する変更の実施といった、組織の能力を低下させる。

次章では、上述の基本的な懸念事項から生じるセキュリティおよびプライバシー問題について、より詳細に論
じることとする。

どんな技術でも同じことが言えるが、クラウドコンピューティングサービスも不適切または不正な行為に利用さ
れる可能性がある。以下に、すでに発生した注目すべき事件をいくつか示す。これらの事例を通じて、将来にわ
たってどのようなことが起きうるかを知ることができる。

- **ボットネット (Botnets)**。ハッカーによって構築されコントロールされるボットネットは、いろいろな意味でク
ラウドコンピューティングの原型である。低コスト、ダイナミックな割り当て、冗長性、セキュリティをはじめ、
クラウドコンピューティングの多くの特性がボットネットにもある。ボットネットはスパムの送信、ログイン
登録情報の不正取得、ウェブサイトに対するインジェクション攻撃などに利用されてきた[Pro09]。ボット
ネットは、クラウドプロバイダの基盤に対するサービス拒否攻撃にも利用できる。クラウドサービスがボ
ットネットに組み込まれる可能性はすでに現実のものになっている。2009年に、IaaS クラウド上で稼働して
いる司令塔(コマンドアンドコントロール)ノードが発見されている[Mcm09a, Whi09]。スパム攻撃を行う者

はまた、クラウドサービスを直接購入してフィッシング攻撃を仕掛け、ソーシャルエンジニアリング手法を使って受信者にマルウェアを仕掛けた[Kre08]。

- **メカニズムのクラッキング (Mechanism Cracking)**。WPA (WiFi Protected Access: ワイファイプロテクトドアクセス)を攻撃するクラッカーの例では、クラウドサービスに対しては侵入試験をしているように装い、オンデマンドで調達できるクラウドリソースを束ねて使い、ワイアレスネットワークの保護に使用される暗号化されたパスワードを解読する。クラウドコンピューティングを利用することによって、単一のコンピュータ上で5日間かかる作業を400台の仮想マシンを使ってたったの20分で終わることが可能になる[Rag09]。暗号技術は認証、データの機密性と完全性、およびその他のセキュリティメカニズムにおいて広く使われているため、暗号鍵をクラッキングするクラウドサービスが使用された場合に、実際問題として、その仕組みの有効性が損なわれてしまう。クラウドベースのシステムと、従来型のシステムの両方が、標的となりうる。クラウドサービスを利用するクラッキングには、CAPTCHAクラッキングというものもある。これは、自動化ソフトウェアを使ってインターネットサービスを無制限に利用されるのを阻止するための検証の仕組みをクラウドサービスを使ってすり抜けるものである。⁴

⁴CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart: キャプチャ)は、サービスを提供する前にユーザに対する簡易テストを行うことによって、自動化された迷惑アクセスを阻止する仕組みである。

4. セキュリティおよびプライバシーに関する重要な問題

クラウドコンピューティングは登場して間もないが、セキュリティの重要な側面に対する洞察は、クラウドコンピューティングを早期に導入していた人々の経験の報告と、クラウドプロバイダが提供するプラットフォームと関連テクノロジーについて分析・実験を行ってきた研究者から得ることができる。以下のセクションでは、クラウドコンピューティングにとって長期にわたる課題となるプライバシーおよびセキュリティ問題を明らかにする。一つの課題を説明するにあたって、可能な場合にはすでに発生または経験した問題の事例も示す。IT のアウトソーシングに関するセキュリティおよびプライバシー問題については、次の章で取り扱い、以下の記述への補足となる。

クラウドコンピューティングはいくつかのテクノロジー（サービス指向型アーキテクチャ、仮想化、Web2.0、ユーティリティコンピューティングを含む）が融合したところから生まれたものである。このため、クラウドにおけるプライバシーおよびセキュリティ問題の多くは、決して真新しいものではなく、既知の問題が新しい形の中にはめ込まれたものであるといえる。しかしながら、個々の問題が組み合わさることの重要性を軽視してはならない。クラウドコンピューティングは、思考力を刺激するパラダイムシフトを引き起こし、従来の規範の枠を超えて組織のインフラの境界を組み替える。極端な例では、アプリケーションをある組織のインフラから別の組織のインフラに移動したものの、移動先で悪意のある者が用意したアプリケーションが稼働しているといったことも考えられる。

4.1 ガバナンス

ガバナンスとは、アプリケーション開発のためのポリシー、手順、標準に対するコントロールと監視、ならびに実装されたサービスの設計、実施、テスト、モニタリングを意味する。クラウドコンピューティングサービスが広く利用されている状況で、そうしたサービスに現場判断中心で従事する職員に対する十分なコントロールがなされないということは問題である。クラウドコンピューティングではプラットフォームの調達容易であるが、だからといってガバナンスの必要性が減少するわけではなく、むしろ増加するといった反対の影響ももたらされる。

クラウドコンピューティングのメリットの一つに、資本投資を減らして運営経費に形を変えることができることがある。クラウドコンピューティングは新たなサービスの実装にかかる初期費用を減らし、実際の利用に対応した支出にすることができる。⁵ しかしその結果、コンピューティングリソースを資本支出扱いで調達することに対して組織が定めた正規のプロセスと手順を、部署や個人が無視してしまい、リソースの調達を運営経費なみの扱いにかいくぐらせてしまう可能性がある。そうした行為を組織が取り締まらない限り、プライバシー、セキュリティ、および監視のポリシーと手順が無視され、組織がリスクにさらされる可能性がある。例えば、脆弱なシステムが実装される、法的規制が無視される、費用は短期間に受容できないレベルにまで積み上がる、リソースが許されない目的に使用される、あるいはその他の悪影響が生じる、といったことが起こる。

欧州と米国の 900 名以上の IT 専門家を対象にした研究では、各組織のほかの部署が知らない間にクラウドコンピューティングサービスが実装されている可能性への強い懸念が、参加者から示された[Pon10]。この問題は、組織のインフラにたちのよくないワイヤレスアクセスポイントを個人が勝手に接続した場合に似ている。この

⁵多くの事業主は税金に対する考慮から、資本支出よりも運営経費に比重を置く傾向にある（例えば、資本コストのコントロールをよりうまく行って会計期間の運営経費の控除にすると、それは費用として計上できるが、資本投資の場合は複数期間の減価償却を行うことになる。）。

場合、適切なガバナンスが実施されない結果、その組織のコンピュータ基盤は、セキュリティが確保されていないサービスの無秩序で管理が困難な集合と化してしまう可能性がある。アプリケーションの開発とサービスの提供に関するポリシー、手順、標準、ならびに実装された、または稼働中のサービスの設計、実施、テスト、モニタリングに関する組織の実践規範は、クラウドコンピューティング環境にも適用されるべきである。

クラウドサービスを取り扱うにあたっては、関連する役割と責任、とりわけリスクの管理に関して、注意を払う必要がある。システムのセキュリティを確保し、リスクの管理を確実にすることは、いかなる環境においても困難であるが、クラウドコンピューティングではなおさら困難である。データがどのように保管、保護、使用されるのかを特定し、サービスの有効性を判断し、ポリシーの遵守状態を検証するには、監査のためのメカニズムとツールが必要となる。また、絶え間なく進化と変化を遂げるリスクの世界に対応できるような柔軟なリスクマネジメントプログラムも備えなければならない。

4.2 コンプライアンス

コンプライアンスには、定められた仕様、標準、規制、または法律の遵守を含む。セキュリティおよびプライバシーに関する法規制は、国ごとに、国家、州、ローカルのレベルでさまざま存在する。このためクラウドコンピューティングにおけるコンプライアンスは、複雑な問題となる可能性がある。

- **データの所在地 (Data Location)**。組織が直面する最も一般的なコンプライアンス問題の一つは、データの所在地である[Bin09, Kan09, Ove10]。社内のコンピューティングセンタを使用することによって、組織は、自身のコンピューティング環境を構築し、データの格納場所と、データの保護に使用されている保護対策について詳しく知ることができる。これとは対照的に多くのクラウドコンピューティングサービスが有する特徴として、組織のデータの所在地についての詳細な情報は得られない、あるいはサービスの利用者には開示されないといったことがある。このような状況下では、十分な保護対策が実施されていることと、法規制上のコンプライアンスが満たされていることの確認が困難である。この問題は、外部の者による監査およびセキュリティ認証によってある程度緩和されるが、これらは万能薬ではない[Mag10]。

情報が国境を超えた場合、適用されるプライバシーや規制に関する制度が不明瞭となり、さまざまな懸念が生じる可能性がある(例:[CBC04])。その結果、機微なデータが国境を超えて流れることに対する制約と、データ保護に関する要件が、プライバシーおよびセキュリティに関する国家および地域の法規制の主題となる[Eis05]。問題としては、データが収集された管轄区域の法律がデータの転送を許容するか、データ転送後も引き続きそれらの法律が適用されるか、転送先が設ける法律がなんらかの追加的なリスクまたはメリットをもたらすかなどがある[Eis05]。よく当てはまるケースとしては、アクセスコントロールなどの技術面、物理面および管理面での保護対策がある。例えば、欧州のデータ保護法が、米国に転送されたデータの取り扱いと処理に関して追加的な義務を課す可能性がある[Doc00]。

国境を超えるデータのフローに関する主なコンプライアンス問題は、データが収集された管轄区域の法律がデータの転送を許容するか、データ転送後も引き続きそれらの法律が適用されるか、転送先が設ける法律がなんらかの追加的なリスクまたはメリットをもたらすかなどがある[Eis05]。よく当てはまるケースとしては、アクセスコントロールなどの技術面、物理面および管理面での保護対策がある。例えば、欧州のデータ保護法が、米国に転送されたデータの取り扱いと処理に関して追加的な義務を課す可能

性がある [Doc00]。[訳注:このパラグラフは、原文自体が、ほとんど前パラグラフの最後の2文の繰り返しとなっている。]

- **法令 (Laws and Regulations)**。米国連邦政府機関にとってのセキュリティおよびプライバシーに関する主なコンプライアンス課題には、1996年施行のクリンガー・コーエン (Clinger-Cohen) 法、行政管理予算局通達 A-130 号 (OMB Circular No. A-130) – 特に付録 III –、1974年施行のプライバシー法 (Privacy Act)、2002年施行の連邦政府情報セキュリティ管理法 (Federal Information Security Management Act (FISMA)) が含まれる。これ以外にも重要なのが、米国国立公文書館 (National Archives and Records Administration (NARA)) 関連の法令、特に連邦記録法 (Federal Records Act) (合衆国法典 44 号、第 21, 29, 31, 33 章)、および NARA 規則 (連邦規則集のタイトル 36、第 XII 編、第 B 章) である。

クリンガー・コーエン法は、連邦政府内のコンピュータシステムの効率、セキュリティ、プライバシーに関する責任の割り当てを行い、政府機関による情報リソースの調達と管理を向上させる包括的なアプローチを実現させる。クリンガー・コーエン法が定める OMB の権限に基づいて、さまざまな通達が発行されている。通達 A-130 号は、連邦情報リソースの管理ポリシーを定めるものであり、これらのポリシーの特定部分を実施するための手続きおよび分析用ガイドラインも含まれている。付録 III では、一般支援システムおよび主要なアプリケーションによって収集、処理、伝送、格納、配信されるあらゆる政府機関情報に対して、十分なセキュリティを用意することを要求している。同様にプライバシー法は、連邦政府機関の記録システムに保管される個人情報の収集、保管、使用、配信について規定する。

FISMA は、連邦政府機関に対して、自身の情報と情報システムを、正規の権限によらないアクセス、利用、開示、中断、変更、または破壊から保護することを求めている [HR2458]。規定された義務には、政府機関、政府機関からの受託者、または政府機関の代理となる他の組織によって使用または運用される情報システムの保護が含まれる。すなわち、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は、委託元の連邦政府機関と同等のセキュリティ要件を満たさなければならない。それらのセキュリティ要件は、連邦情報を格納、処理、伝送する外部サブシステムと、そのサブシステムが提供する、またはそのサブシステムに関連するあらゆるサービスにも適用される。

連邦記録法と NARA 規則は、連邦記録をライフサイクル全体を通して効果的に管理することは、政府機関の責任であると規定している。これには、電子情報システム内の記録、および請負業者の環境内の記録が含まれる。請負業者が連邦記録を保持する場合には、その記録に適用されるすべての記録管理法に従って、それらの記録を管理することが求められる。記録の管理には、その価値が恒久的である記録を所定のフォーマットで NARA に転送することを含む、記録のセキュアな保管、取り出し、適切な廃棄が含まれる [Fer10]。

政府および企業団体によるその他の要求には、医療保険の携行性と責任に関する法律 (Health Insurance Portability And Accountability Act (HIPAA))、クレジットカード業界のデータセキュリティ基準 (Payment Card Industry Data Security Standard (PCI DSS)) などがあるが、これらは特定の組織に適用される場合がある。たとえば、退役軍人健康局 (Veterans Health Administration) は、HIPAA 基準においては民間または公共の医療施設に分類され、職員だけでなく請負業者にも適用される [DVA]。HIPAA は、デ

ータへのアクセス管理のための技術面と物理面での保護対策の実施を求めるものであるが、クラウドプロバイダによってはコンプライアンス問題が生じる可能性がある。

クラウドプロバイダは、法規制に関わる問題について、より敏感になってきていて、データを特定の法管轄区域に保管し処理する保証や、セキュリティおよびプライバシーに関して求められる保護対策の実施に積極的であるかも知れない。しかしながら、自身が管理する内容の公開に対する責任をどの程度受け入れるかは定かでない。たとえても、クラウドプロバイダが組織に代わって保有するデータのセキュリティおよびプライバシーに関する責任は、最終的に組織に帰属する。

- **電子的な証拠開示 (Electronic Discovery)**。電子的な証拠開示には、訴訟の証拠開示段階における電子ドキュメントの特定、収集、処理、分析、作成が含まれる[Daw05]。組織が電子ドキュメントを保管し作成する他の動機と義務には、監査および規則に基づく情報の要求などがある。政府機関であれば、FOIA (Freedom of Information Act: 情報公開法) に基づく要求がそれに当たる。ドキュメントには、電子メール、添付ファイル、コンピュータシステムまたは記憶媒体に格納されているその他のデータオブジェクトに加えて、関連するメタデータ、例えば、オブジェクトの作成または修正日、非表示のファイルコンテンツ(すなわち、ユーザには明示的に見せないデータ)などがある。

クラウドプロバイダの機能と処理(データの保管形式や利用可能な電子的証拠開示ツールなど)は、クライアントである組織が、自身に与えられた義務を費用効果が高く、かつタイムリーで法規制に準拠した形で果たす能力に影響を与える[McD10]。例えば、クラウドプロバイダの記録保管機能では元のメタデータが期待通りに保管されず、書類の破棄または変更(すなわち、訴訟に関連する証拠の故意、重過失または過怠による破壊、紛失、大幅な変更、提出妨害)が行われ、訴訟に悪影響をもたらされることも考えられる。

4.3 トラスト

クラウドコンピュータのパラダイムでは、セキュリティの多くの面に対する直接的なコントロールを組織がプロバイダに委譲することになる。その結果、前例がないほどのレベルの信認をプロバイダに与えることになる。

- **内部関係者によるアクセス (Insider Access)**。組織の境界、組織のファイアウォール、およびその他のセキュリティ管理策の外側で処理または格納されるデータには、それに伴う一定のリスクが随伴する。内部関係者によるセキュリティ脅威は、多くの組織にとって既知の問題ではあるが、名前とはうらはらに、その脅威はアウトソーシングされたクラウドサービスにも及んでいる[Ash10, Cap09, Kow08]。内部関係者による脅威には、現職の職員または元職員のみならず、業務を遂行(あるいは支援)するために組織のネットワーク、システム、データにアクセスすることを許可された請負業者、関連会社、およびその他の関係者によってもたらされる脅威までが含まれる。インシデントには、各種の詐欺行為、情報リソースの破壊行為、機密情報の窃盗などがある。インシデントは過失によって発生することもある(例えば、ある銀行の職員が、顧客の機微な情報を誤って別の Google メールアカウントに送信してしまった場合など)[Zet09b]。

クラウドプロバイダが運営するクラウドコンピューティング環境にデータとアプリケーションを移行することによって、内部関係者によるセキュリティリスクがクラウドプロバイダのスタッフのみならず、そのサー

ビスを利用するユーザによってもたらされる可能性が生じる。例えば、悪意のある内部関係者が、名の知れた IaaS クラウドを対象にサービス妨害攻撃をしかけた事例がある[Sla09]。その攻撃では、一人のクラウドユーザが、はじめに 20 個のアカウントを作成し、アカウントごとに仮想マシンインスタンスを生成した後、それらの各アカウントをベースにして、さらに 20 個のアカウントとマシンインスタンスの生成を行うといった形でインスタンスを指数関数的に増やすことによって、制限を超えるリソースを消費した。

- **データの所有権 (Data Ownership)**。データに対する組織の所有権については、信頼の基盤を確立するためにも、サービス契約にきちんと盛り込むべきである。ソーシャルネットワーキングユーザのプライバシーとデータの所有権をめぐる果てしない議論は、曖昧な契約条件が関係者にもたらす影響を示すものである(例: [Goo10, Rap09])。理想的には、組織のすべてのデータに対して組織が所有権を保持すること、契約によってもクラウドプロバイダが自身の目的のためにデータを使用する権利(知的財産またはライセンスに関するものを含む)が与えられることはないこと、クラウドプロバイダがデータに関するセキュリティ上の利害関係を得たり主張することはないことが、契約によって明示されるべきである [Mcd10]。これらの規定が目的どおりに機能するためには、データ所有権に係る条項をクラウドプロバイダによる一方的な条項修正の対象としてはならない。
- **複合型のサービス (Composite Service)**。クラウドサービス自体は、他のクラウドサービスとの入れ子構造化や階層構造化によって実現することもできる。例えば、SaaS プロバイダが、PaaS や IaaS クラウドのサービスの上に自身のサービスを構築することができる。この場合、その SaaS クラウドの可用性のレベルは、ベースとなる PaaS または IaaS クラウドサービスの可用性に左右される。サードパーティのクラウドプロバイダにサービスの一部を委託またはアウトソースするクラウドサービスは、サードパーティに対するコントロールの範囲、サードパーティの責任の範囲、問題が発生した際の是正措置および償還 (recourse) などについて注意を払わなければならない。信認関係は遡及できない場合が多いので、クラウドプロバイダと契約を結ぶ前にサードパーティと交わした契約内容を開示すること、また、契約条件は契約期間中、または予期される変更についての十分な通知が行われるまでの間には変更しないことが必要である。

法的責任とパフォーマンスに関する保証は、複合型のクラウドサービスでは重大な課題となりうる。例えば、あるコンシューマ向けストレージサービスをベースにしたソーシャルネットワーキングサービスが、2 万人のユーザから集めたデータへのアクセスができなくなったまま廃止となる事例があった。当該サービスプロバイダが履歴データの管理を別のクラウドプロバイダに委託し、新規のアプリケーションとデータベースの管理をさらに別のクラウドプロバイダに委託していたために、障害に対する直接的な責任の所在を明らかにすることができず、問題が未解決に終わってしまった[Bro08]。

- **可視性 (Visibility)**。パブリッククラウドサービスに移行した場合、組織のデータおよびアプリケーションが稼働しているシステムのセキュリティの確保は、クラウドプロバイダに委ねられる。クラウドに使用されている管理、手順、技術面での管理策は、セキュリティ上のギャップが生じないようにするためにも、組織の内部システムに使用されているものと同様か、それ以上でなければならない。この二つのコンピュータシステムを比較するための評価手段はいまだに研究段階にあるため、そうした比較を行うことは容易でない[Jan09]。通常、クラウドプロバイダは、自身が提供するセキュリティおよびプライバシーの詳細を

示すことには消極的である。なぜなら、そうした情報は攻撃の手段を編み出すのに利用される可能性があるからである。また、クラウドユーザがプロバイダのネットワークおよびシステムを詳細にモニタリングすることは、サービス契約には含まれていないことが多く、プロバイダのオペレーションに対する可視性や、オペレーションを直接監査するための手段を制約している(例:[Bro09, Dig08, Met09])。

クラウドプロバイダのオペレーションに対する可視性は、システムセキュリティおよびプライバシーに対する効果的な監視を組織が行ううえで極めて重要である。ポリシーと手続がそのシステムのライフサイクル全体を通して確実に遵守されるようにするには、クラウドプロバイダが導入しているセキュリティ管理策およびプロセス、ならびに時間の経過に伴うパフォーマンスの変化に対する可視性を得るための手段をサービス契約に含めなければならない。理想的には、組織のニーズを満たすためには、警告および通知に関する閾値や、どの程度詳細な報告をどのようなスケジュールで行わせるかなど、可視性を得るための手段については、組織がコントロールできることが望ましい。

- **リスクマネジメント (Risk Management)**。クラウドベースのサービスでは、利用者組織が直接コントロールできないサブシステムまたはサブシステムコンポーネントが存在する。一方で、関連するプロセスと機器をより自由にコントロールできるのなら、リスクについてより安心できると考える人も多い。少なくともコントロールできる度合いが高ければ、インシデントに直面した場合に、代替対策との比較検討、優先順位の設定、組織の最優先事項に基づいて躊躇することなく行動する、といったことが可能になる。リスクマネジメントとは、リスクを特定し評価したうえで、そのリスクを受容可能なレベルまで軽減するために必要な手立てを講じることを意味する[Sto02]。パブリッククラウドベースのシステムにおいても、従来型の情報システムと同様に、そのシステムのライフサイクル全体を通してリスクを管理する必要がある。

クラウドサービスを利用するシステムにおけるリスクを評価し管理することは、困難な課題と言える。実務的に可能な限り、組織は、セキュリティ管理策が正しく導入されていること、意図したとおりに運用されていること、組織のセキュリティ要件を満たしていることを確実にしなければならない。クラウドサービスについて一定の信頼を確立するには、組織のデータとアプリケーションを保護するのに必要なセキュリティ管理策の配置に関して、組織がプロバイダをどの程度コントロールできるか、また、そのセキュリティ管理策の有効性について示された証拠によって左右される[Jff10]。しかしながら、サブシステムが正しく機能していることと、セキュリティ管理策が有効であることを自組織内のシステムに対する検証と同じように詳細に検証することができない場合がある。このような場合、第三者による監査など、他の手段によって信頼を確立することも必要である。最終的に、提供されるサービスの信頼の度合いが期待を下回る場合で、かつ、組織が補完的管理策を採用できない場合には、そのサービスを利用しない、または、より高いレベルのリスクを受容することになる。

4.4 アーキテクチャ

クラウドサービスを提供するためのソフトウェアシステムのアーキテクチャは、クラウド上に存在するハードウェアとソフトウェアによって構成される。クラウド基盤の物理的な所在地は、クラウドプロバイダが決定する。クラウドのベースとなる支援フレームワークの信頼性と拡張性を実現するためのロジックの実装も同様である。仮想マシンは、クラウドを展開するための抽象化の単位としての役割を果たすことが多く、クラウドのストレージアーキテクチャとは緩やかに結合される。アプリケーションは、インターネットを介して利用できるサービスのプログラミングインターフェース上に構築され、複数のクラウドコンポーネントがアプリケーションプログラミングインターフェースを介して互いにコミュニケーションをとるのが一般的である。簡易化されたインターフェースおよびサービスの抽象化の多くは、セキュリティに影響を与える内部の複雑さを覆い隠す。

- **攻撃の矢面 (Attack Surface)**。ハイパーバイザあるいは仮想マシンモニタは、OS とハードウェアプラットフォームの間にあるソフトウェアレイヤであり、マルチテナントの仮想マシン群を操作するのに使用される。通常、ハイパーバイザは、仮想化されたリソースに加えて、仮想マシンインスタンスの生成、移転、終了などの管理的なオペレーションを実施するためのアプリケーションプログラミングインターフェースもサポートする。仮想化されていない従来型の実装に比べて、ハイパーバイザが追加されることで、攻撃の矢面の増加をもたらす。

仮想マシン環境の複雑さは、セキュリティを危うくする条件が追加されるため、従来型のシステム環境よりも多くの困難を伴う[Gar05]。例えば、仮想マシンの呼び出し、検問、移転が機微なデータの実記憶へのリークを引き起こし、このような事態を未然に防ぐためにあるゲスト OS の保護メカニズムが、損なわれる可能性がある。また、ハイパーバイザ自体が侵害される可能性がある。例えば、広く使われている仮想ソフトウェア製品について、NAT (Network Address Translation: ネットワークアドレス変換) ルーチンの中で、特殊な仕掛けをした FTP (File Transfer Protocol: ファイル転送プロトコル) リクエストを通過させることによってハイパーバイザのヒープバッファを破壊し、ホスト側で任意のコードを実行することを可能にする脆弱性が発見された[Sec05, She05]。

- **仮想ネットワークの保護 (Virtual Network Protection)**。仮想プラットフォームの多くは、仮想環境の一部としてソフトウェアベースのスイッチおよびネットワーク環境を構築することができる。これにより、同一のホスト上の仮想マシンが、より直接的に、かつ効率的にコミュニケーションをとることができる。例えば、外部ネットワークアクセスを必要としない仮想マシン向けに、多くの仮想ソフトウェア製品の仮想ネットワークアーキテクチャが、同一ホスト上でのネットワーク構築、すなわち、プライベートサブネットを構築することによってホスト内通信を可能にする仕組みをサポートしている。仮想ネットワーク上のトラフィックは、物理ネットワーク用のセキュリティ保護装置、例えばネットワークベースの侵入検知防止装置 (IDPS) からは見えない[Vie09]。可視性とホスト内攻撃に対する防御の喪失を避けるためには、物理ネットワーク上の保護機能を仮想ネットワークにも実装することが必要であろう[Ref10, Vmw10]。
- **二次データ (Ancillary Data)**。保護の焦点は主にアプリケーションデータに置かれているが、クラウドプロバイダが保有するサービスユーザのアカウントについての膨大な詳細情報も侵害され攻撃に使用される可能性があるため、注意が必要である。1つの例として支払情報があるが、それ以外にも、より機微性の高い情報が含まれる可能性がある。例えば、ある SaaS クラウドプロバイダの職員の一人に対す

る標的型フィッシング攻撃により連絡先情報が格納されたデータベースが盗まれて、そのクラウドサービスの利用者に対する標的型電子メール攻撃が成功裏に行われた事例がある[Kre07, Mcm07]。この事例を通じて明らかになったのは、クラウドプロバイダは、ユーザのために保管している情報だけでなく、ユーザに関して自身が保有している情報についても、セキュリティ侵害が発生した場合には速やかに報告すべきであるということである。

IaaS クラウドプロバイダが保有する他の種類の二次データとして、仮想マシンイメージがある。仮想マシンイメージには、インストールと設定がなされたアプリケーションを含む、ソフトウェアのスタックが含まれる。このスタックは、仮想マシンを初期状態に立ち上げ、あるいは前もって設定された特定のチェックポイントの状態に設定するのに使用される。仮想マシンイメージの共有が一般的に行われるクラウドコンピューティング環境もある。イメージリポジトリは、問題を回避するためにも慎重な管理とコントロールが必要となる。

イメージには私有のコードやデータが含まれる可能性があり、それが脆弱性となるため、イメージの提供者はリスクに直面することになる。アタッカーがイメージを分析して、情報漏えいを行ったり、攻撃の手段として利用したりといった判断をすることも考えられる[Wei09]。特に、開発段階のモノのイメージがたまたま盗まれた場合は危険である。これとは逆に、マルウェアが仕込まれた仮想マシンイメージをアタッカーがクラウドコンピューティングシステムのユーザに送り付けることも考えられる[Jen09, Wei09]⁶。例えば、研究者たちは、名の知れたクラウドプロバイダのイメージリポジトリに自作の仮想マシンイメージを投稿し、登録プロセスを不正に操作してそれらのイメージが最初のページにリストアップされるようにすることによって、クラウドユーザを魅了しイメージを起動させることができることを示した[Mee09]。改ざんされたイメージを起動した場合のリスクには、データの盗難や破損がある。

- **クライアント側の保護 (Client-Side Protection)**。攻撃を首尾よく防ぐためには、クラウドコンピューティングのクライアント側とサーバー側の両方のセキュリティを確保することが必要となる。通常、サーバー側に重きが置かれるため、クライアント側はおろそかになりがちである。多くのクラウドコンピューティングサービスにとって重要な要素であるウェブブラウザに加えて、手に入れられる種々のプラグインや拡張機能も、セキュリティに問題があることで評判が悪い[Jen09, Ker10, Pro07, Pro09]。ブラウザのアドオンの多くはまた、自動的アップデート機能を持たないため、既存の脆弱性が解消されずに残っている可能性を高めている。

クライアント側の物理的および論理的セキュリティを維持することは、とりわけスマートフォンなどの組み込み携帯機器の場合には、困難を伴う。そうした機器のサイズと持ち運び可搬なことで、物理的なコントロールが不可能な場合がある。あらかじめ組み込まれているセキュリティ機能は使われないことが多く、知識の豊富な者によって容易に破られたり、すり抜けられ、装置のコントロールを奪われる可能性がある[Jan08]。スマートフォンは、汎用システムとしてよりも、特定機能に限定した装置として扱われている。

⁶ PaaS および SaaS 環境向けの悪質な実装モデルがすでに出回っている。

1種類のOSがほとんどを占めている訳ではなく、システムコンポーネントとアドオンのセキュリティパッチおよびアップデートもデスクトップクライアント程頻繁には行われぬ。このため、脆弱性が長期にわたって存続し、悪用される機会も増加する。

ソーシャルメディア、パーソナルウェブウェブメール、およびその他の一般に利用可能なサイトの提供と利用の増加は、関連するリスクがあり、1つの懸念材料である。なぜなら、ソーシャルエンジニアリング攻撃を受けた場合にブラウザだけでなく、そのベースとなるプラットフォームや利用対象のクラウドサービスにまで悪影響が及ぶ可能性があるからである。例えば、ある病院の職員のパーソナルウェブウェブメールアカウントを介して病院のシステムにスパイウェアがインストールされ、財務情報などの機密情報を含む1,000個以上のスクリーンイメージがアタッカーに送信されるといった事例があった[Mcm09b]。バックドアを仕込むトロイの木馬、キーロガー、その他の種類のマルウェアがクライアントデバイス上で動作しているといった状況は、クラウドまたはクラウドがアクセスするウェブベースのサービスのセキュリティにとって好ましくない状況である[Fre08, MRG10]。クラウドコンピューティングの全体的なセキュリティアーキテクチャの一環として、組織には、既存の対策の見直しを行い、必要であれば追加の対策を実施して、クライアント側のセキュリティを確保することが求められる。銀行は率先して、ネットワーク上で交換される情報の暗号化と、キーロガーからの保護を実現する、セキュリティが強化されたブラウザ環境の配布に取り組んでいる[Dun10a, Dun10b]。

- **サーバー側の保護 (Server-Side Protection)**。IaaS クラウドにおける仮想サーバーおよびアプリケーションは、仮想化されていないサーバーやアプリケーションと同様に、物理的にも論理的にもセキュリティの確保が必要となる。実装する仮想マシンイメージの作成にあたっては、組織のポリシーおよび手順への準拠、OS およびアプリケーションのセキュリティ強化が必要となる。イメージを実装する仮想環境にセキュリティを施す際には、注意が必要である[You07]。例えば、仮想ファイアウォールを使用して、あるグループの仮想マシンを他のグループから分離することができる(開発システムと本番システムの分離や、開発システムとクラウド上の他のシステムとの分離など)。仮想マシンイメージを慎重に管理することは、開発中の、または脆弱性を含むイメージを誤って実装してしまうといったことを回避するためにも重要である。

ハイブリッドクラウドは、複数の要素から成るクラウドであり、保護に関する同様の問題を抱えている。ハイブリッドクラウドでは、そのインフラが、パブリッククラウドとプライベートクラウドの組合せ、あるいは別の組織のプライベートクラウドとの組合せによって構成される。各クラウドは独立の存在であるが、標準の、あるいは固有の技術で結合されることで、統合されたサービスを実現している。その一方で、各クラウド間の相互依存関係も生じる。例えば、パブリッククラウドによって提供されるサービスを利用するユーザに対して、識別と認証を組織のプライベートクラウド基盤で行うといったことが考えられる。基盤の組み合わせにより生じるセキュリティホールや欠陥をいかに防ぐかは、ハイブリッドクラウドにとって大きな課題である。なぜならば、ハイブリッドクラウドは他のクラウドよりも複雑で、かつ責任も拡散するからである。ハイブリッドクラウドでは可用性も問題になる。ハイブリッドクラウドの可用性は、計算上はその構成要素である各クラウドの可用性の積であり、いずれかの構成要素の可用性が低下した場合に、全体的な可用性も比例して低下する。

4.5 アイデンティティとアクセスの管理

情報におけるデータの機微度 (sensitivity) とプライバシーに対する組織の関心度が高まってきており、クラウドにおいて情報資源への権限のないアクセスは重要な懸念事項となっている。繰り返し起こる問題として、組織の識別および認証フレームワークをクラウドにそのまま適用できない上に、クラウドサービスをサポートするために既存のフレームワークを拡張したり、変更を加えることは容易でないことが挙げられる[Cho09]。代替案として、二つの異なる認証システムを用意して、1つは組織の社内システムに、もう一つは外部のクラウドベースのシステムにあてるといった方法は、複雑さであり、時間の経過とともに役に立たなくなる可能性がある。解決策の一つに、サービス指向型アーキテクチャの登場により一般に普及したアイデンティティフェデレーションの導入がある。これは、SAML (Security Assertion Markup Language) 規格または OpenID 規格など、さまざまな方法で実現できる。

- **認証 (Authentication)**。SAML 規格をサポートするクラウドプロバイダは増えており、ユーザを管理し、アプリケーションやデータへのアクセスを許可するための認証に使用している。SAML は、協力関係にあるドメイン間で、アクセス主体に対する確認 (アサーション) や認証情報などの情報をやりとりするための手段を提供する。通常、SAML リクエスト/レスポンスメッセージは、フォーマットに XML (eXtensible Markup Language: 拡張マークアップ言語) を使用する SOAP (Simple Object Access Protocol) にマッピングされる。SOAP メッセージは電子的に署名される。例えば、ユーザがそのパブリッククラウドの公開鍵証明書を取得すれば、秘密鍵を使用して SOAP リクエストに署名することが可能である。

SOAP メッセージのセキュリティの検証は複雑であり、攻撃を受けないためにも慎重に実施しなければならない。例えば、あるパブリック IaaS クラウドに対して XML ラッピング攻撃が成功裏に行われた事例がある[Gaj09, Gru09]。XML ラッピングにより SOAP メッセージの不正操作ができる。追加の要素 (すなわち、ラッパー) が SOAP セキュリティヘッダに組み込まれると、ラッパーによってオリジナルのメッセージ部が取り除かれ、アタッカーが指定したオペレーションを要求する偽のものに置き換えられる[Gaj09, Gru09]。見た目はオリジナルのメッセージが参照されて署名の検証も行われるが、実際には、置き換えられたメッセージ部に記載されているオペレーションが実施される。

- **アクセスコントロール (Access Control)**。SAML 単体では、クラウドベースのアイデンティティおよびアクセス管理サービスを提供するには十分でない。クラウドユーザ権限を適用し、リソースに対するアクセスコントロールを維持する能力が必要となる。アイデンティティ管理の一環として、クラウドプロバイダは独自のインターフェースの代わりに XACML (eXtensible Access Control Markup Language) などの規格を使用して、クラウドリソースへのアクセスをコントロールできる。XACML は、認可 (Authorization) の判断を提供するためのメカニズムを受け持ち、協力関係にある組織の間で認証と認可の判断を伝達する部分を受け持つ SAML を補完する。XACML の利用により、大半のプロバイダの独自のサービスインターフェースをコントロールできるようになる。このため、すでに XACML を導入しているクラウドプロバイダもある。XACML を使用する組織間で伝送されるメッセージは、悪意のある第三者による攻撃に遭いやすい。そこで、不正な開示、再現、削除、改変など、考えられる攻撃から認可判断の依頼と判断結果を保護するための、保護対策を実施することが重要となる[Kel05]。

4.6 ソフトウェアの隔離

クラウドコンピューティングでは、多数のプラットフォームをベースにして高度のマルチテナント環境を実現することが必要となる。そうでないと、信頼できるサービスのオンデマンドでの提供という柔軟性への期待や、スケールメリットによるコストメリットや効率性を実現することができない。必要な利用規模に到達するには、サービスをダイナミックに、かつ柔軟に提供することと、ユーザのリソースを分離することの保証がクラウドプロバイダに求められる。通常、クラウドコンピューティングにおけるマルチテナントは、同一の物理サーバー上で複数のユーザが仮想マシンを多重に走らせることによって実現される[Ris09]。ゲスト仮想マシン上に実装されたアプリケーションは、仮想化されていないアプリケーションと同様に、攻撃や侵害を受けやすいことに留意すべきである。これは、IaaS クラウドコンピューティング環境で稼働するボットネットの発覚によって劇的に実証された[Mcm09a, Whi09]。

- **ハイパーバイザの複雑性 (Hypervisor Complexity)**。コンピュータシステムのセキュリティは、そのベースにあり、プロセスの制御や実行をつかさどるソフトウェアカーネルの品質に左右される。仮想マシンモニタもしくはハイパーバイザは、単一のホストコンピュータ上で、OS とアプリケーションを載せた仮想マシンを複数同時に走らせられる設計になっていて、異なるゲスト仮想マシン間の分離を実現する。

仮想マシンモニタは、論理上、OS よりも規模が小さく、より単純な構造になっている。この特性はセキュリティの品質の分析・改善を容易にするので、OS によるプロセス間の隔離よりも、ゲスト仮想マシン間の隔離を強かに維持するのに適している可能性が高い[Kar08]。ところが実際のところ、最新のハイパーバイザは、OS に匹敵する規模と複雑さを備えているものもあり、前述の利点を得ることはできない。例えば Xen や KVM などが、その典型例である。Xen は、オープンソースの x86 仮想マシンモニタであり、Linux カーネルを改良したものを使用して入出力操作のための特権パーティションを実装している。一方、別のオープンソース製品である KVM は、Linux カーネルを改造して仮想マシンモニタとして使用する[kar08, Sha08, Xen08]。クラウドプロバイダが仮想化技術をどのように使用しているかを理解することは、関連するセキュリティリスクを理解するうえで必須となる。

- **攻撃ベクトル (Attack Vectors)**。仮想マシンをベースにしたクラウド基盤におけるマルチテナント環境では、ゲスト仮想マシン間で物理リソースが共有されるという微妙さもあって、新たな脅威にさらされる可能性がある。最も深刻な脅威は、悪質なコードが仮想マシンの境界を越えてハイパーバイザまたはその他のゲスト仮想マシンに支障を来す可能性である。異なるホストコンピュータ上のハイパーバイザ間でゲスト OS を休止させることなく仮想マシンを移動することを可能にするライブマイグレーション、およびシステム管理を容易にするために仮想マシンモニタ環境によって提供されるその他の機能の実装は、ソフトウェアのサイズと複雑さの増加につながり、ひいては攻撃の対象となる分野も増加すると考えられる。

いくつかの例によって、考えられる攻撃ベクトルの種類が明らかになる。第一に、クラウド基盤のマッピングがある。研究者たちは、一見難しいと思えるが、名の知れた IaaS クラウドにおいて一つのアプローチを実演した[Ris09]。彼らは複数のクラウドユーザアカウントを使用して複数の仮想マシンインスタンスを生成した後に、ネットワークプローブを使用して、割り当てられている IP アドレスとドメイン名を分析し、サービスの提供元の所在地に関するパターンを特定した。そこで得た情報と一般的な技法を使用して、

攻撃の標的である特定の仮想マシンの所在地を特定することができ、新しい仮想マシンインスタンスを生成して、そのターゲットマシンと同じ場所に配置した。

ターゲットマシンの所在地を突きとめた後にゲスト仮想マシンがとる次の行動は、ハイパーバイザによる封じ込めをすり抜けもしくは回避する、またはハイパーバイザとシステム全体を停止させることである。提供されるプログラミングインターフェースおよび命令コードの処理の弱さは、アタッカーが利用できる脆弱性を発見するための標的となるのが普通である[Fer07]。例えば、ハイパーバイザの電源管理用のプログラムコード内に、エミュレートされたI/Oポートをごまかすことで、メモリー内の書き込み禁止領域への書き込みを可能する深刻な弱点が見つかった[Omm07]。⁷ よく使われている仮想化ソフトウェア製品の仮想デバイスドライバに、ゲスト仮想マシンを使って、ホストコンピュータをホスティングされているその他の仮想マシンもろともクラッシュさせて、サービス拒否を引き起こすことを可能にする脆弱性が発見された。[Vmw09]。

より間接的な攻撃手法も考えられる。例えば、研究者たちは中間割込み (man-in-the-middle) 攻撃によって認証用のプログラムコードを修正し、ライブマイグレーション中のゲスト仮想マシンの管理者権限を取得する方法を開発した[Obc08a]。マイグレーション中にメモリーの内容が変更されると、OSの下に仮想マシンベースのルートキット層を挿入される恐れなどの別の可能性が生じる[Kin06]。仮想プライベートサーバーを管理するためのオープンソースアプリケーションである HyperVM にゼロデイ攻撃が仕掛けられ、あるサービスプロバイダによってホスティングされていた約 100,000 個の仮想サーバーベースのウェブサイトが破壊されたという情報がある[Goo09b]。間接的な攻撃のもう一つの例は、共有サーバーのリソースの使用状況を監視することによって情報を得ていた事例で、これは、他のコンピュータ環境で行われるのと同様のサイドチャネル攻撃をしようとしていたと考えられる。[Ris09]。例えばアタッカーが利用が盛んな期間を特定し、通信量のピークを予測した上でキーストロークタイミング攻撃をしかけて、ターゲットサーバーからパスワードなどのデータを取得することが考えられる。

4.7 データの保護

通常、クラウドでは、データは、他の利用者のデータとともに、共有環境に置かれる。したがって、機微なデータおよび規制対照であるデータをクラウドに移行する組織は、データへのアクセスがどのように管理され、データの安全性がどのように確保されるかについて、確認しなければならない。

- **データの分離 (Data Isolation)**。データはさまざまな形態をとる。例えば、クラウドベースのアプリケーション開発中の場合、データにはアプリケーションプログラム、スクリプト、設定情報、および開発ツールが含まれる。一方、すでに実装されているアプリケーションの場合、データには、アプリケーションによって作成または使用されるレコードその他のコンテンツと、アプリケーションユーザのアカウント情報が含まれる。アクセスコントロールは、権限のないユーザがデータにアクセスするのを防ぐ一つの手段であり、他の方法として暗号化がある。通常、アクセスコントロールはアイデンティティに基づいて行われる。このためクラウドコンピューティングでは、ユーザのアイデンティティの認証が重要な事項となる。

⁷ ファジー化とは故障注入テクニックの一種であり、アタッカーは、特定のインターフェースに疑似ランダムデータを送信することによって欠陥の特定を試みる。

クラウドコンピューティングで使用されるデータベース環境は、大幅に異なる場合がある。例えば、マルチインスタンスモデルをサポートする環境もあれば、マルチテナントモデルをサポートする環境もある。マルチインスタンスモデルでは、クラウド利用者ごとに各仮想マシンインスタンス上で稼働する別々のデータベース管理システムが各ユーザに提供される。この場合、そのシステムに対する役割定義、ユーザに対する権限の認可、セキュリティに関連するその他の管理業務を各ユーザが完全にコントロールすることになる。マルチテナントモデルでは、全てのユーザがあらかじめ用意された環境を共有することになり、データには各ユーザの識別子がタグ付けされる。タグ付けはインスタンスの専用使用を提供するように見えるが、健全でセキュアなデータベース環境を確立し維持することを、クラウドプロバイダにゆだねることになる。

データベースのマルチテナントの実現方法にはいくつかのタイプがある。リソースの集積方法、隔離の程度およびリソースの効率性は、方法によって異なる[Jac07, Wai08]。他にも考慮すべき事項がある。例えば、データの暗号化など、機能によっては共有型データベースではなく分離型データベースを使用する方法でないと実現できない。この種のトレードオフに関しては、扱われるデータに対するデータマネジメントソリューションが適切であるか否かを慎重に評価することが求められる。医療など、いくつかの分野における要求事項がアプリケーションに使用するデータベースとデータ編成の選択に影響を与えることが予想される。一般的に、プライバシーにかかわる情報は、通常、深刻に考慮する必要がある[Pea09]。

データは保存中、伝送中、使用中を通じてセキュアでなくてはならず、アクセスはコントロールされなければならない。通信プロトコルおよび公開鍵証明書に関する標準により、伝送中のデータの暗号化による保護が可能になる。しかし、保存中のデータを保護する手順は、そのようには標準化されていない。独自のシステムが多く存在するため、相互運用性が問題となる。相互運用性の欠如は、データの可用性に影響を及ぼすと同時に、クラウドプロバイダ間のアプリケーションとデータの移行可能性の問題を厄介なものにする。

現在のところ、暗号鍵の管理についての責任は主にクラウドサービスユーザが負うことになる。通常、鍵の生成と保管はクラウドの外部でハードウェアベースのセキュリティモジュールを使って行われるので、クラウドの拡張性のパラダイムに対応できない。NISTの暗号鍵管理プロジェクト(Cryptographic Key Management Project)は、政府による利用のために、拡張性に富み使い勝手のよい暗号鍵管理・交換方式を模索している。この戦略によって一般向けも実質的に問題が緩和されると期待される。⁸ 暗号技術にとって使用中のデータを保護することは新たな課題であり、これといった成果を示すまでには至っていない。このため主な保護対策としては信頼(Trust)の仕組みに依存することになる[Gre09]。

- **データの無毒化＝サニタイズ＝(Data Sanitization)**。クラウドプロバイダが提供するデータのサニタイズ処理がセキュリティに明らかに影響を与える。サニタイズとは、例えば記憶装置がサービスから外された場合や、異なる場所に移して格納する場合など、さまざまな状況において機微なデータを記憶装置から消去することを意味する。データのサニタイズは、サービスのリカバリやリストアを可能にするために作成したバックアップコピーや、サービス終了時に残っている残存データにも適用される。クラウドコ

⁸ Cryptographic Key Management Project のウェブサイトは、http://csrc.nist.gov/groups/ST/key_mgmt/で閲覧できる。

ンピューティング環境では、あるユーザのデータが、他のユーザのデータと物理的に混在した状態になるため、問題がさらに複雑になる可能性がある。例えば、研究者たちがオンラインオークションその他の場を通じて使用済みデバイスを手入れし、それらのデバイスから大量の機微な情報を復元することに成功した例はたくさんある(例:[Val08])。適切なスキルと機器が備わっていれば、クラウドプロバイダが適切に廃棄処理しなかった故障したデバイスからデータを復元することも可能である。

4.8 可用性

可用性とは、簡単に言えば組織のコンピュータ関連のリソース一式がアクセス・使用可能である範囲を意味する。可用性は一時的に、あるいは恒久的に影響を受ける可能性があり、部分的に、あるいは完全に失われることも考えられる。サービス拒否攻撃、機器の停止、および自然災害は、すべて可用性にとって脅威である。問題は、ダウンタイム(システムが休止する期間)は突然訪れることと、組織の任務に影響が及ぶことである。

- **一時的な停止 (Temporary Outages)**。クラウドコンピューティングサービスでは、サービスの高い信頼性と可用性のために設計されたアーキテクチャが使用されるが、サービスの停止やパフォーマンスの低下が起きる可能性は十分にある[Lea09]。この点を明らかにした事例は多数ある。2008年2月には名の知れたストレージクラウドサービスが3時間にわたって停止し、Twitter やその他の新興企業を含む利用者が影響を受けた[Dig08, Kri08, Mil08]。2009年6月には雷雨により IaaS クラウドの一部が停止し、一部のユーザが4時間にわたって影響を受けた[Mil09]。同様に2008年2月には SaaS クラウドにおけるデータベースのクラスターが故障し、サービスが数時間にわたって停止した。また、2009年1月には、ネットワークデバイスが故障し、サービスが短時間停止した[Fer09, Goo09a, Mod08]。2009年3月には、アップグレードに伴うネットワークの問題が原因となり、PaaS クラウドのサービスが約22時間にわたって重篤な機能低下を起した[Clu09, Mic09]。

信頼性が99.95パーセントである場合、年間で4.38時間のダウンタイムが予想される。通常、定期保守に必要な期間については、SLAが規定するダウンタイムの対象から除外され、クラウドプロバイダは短い予告によって予定を組むことができる。クラウドサービスの信頼性のレベルとバックアップおよびリカバリの機能は、組織の異常対処計画によって手当てすべきである。それによって、クラウドサービスおよびオペレーションが中断された場合に、必要に応じ代替となるサービス、機器、場所を使用してリストア/リカバリを確実に行わなければならない。クラウドストレージサービスは、ホストされたアプリケーションにとって単一障害点 (single point of failure)となる。そうした状況下では、第二のクラウドプロバイダを、主たるプロバイダによって処理されるデータのバックアップとして利用することが考えられる。そうすることで、主たるプロバイダが提供するサービスが長期にわたって中断したり、深刻な災害が発生した場合にも、データの可用性を維持し、重要な業務を速やかに再開することが可能になる。

- **長期的および恒久的な停止 (Prolonged and Permanent Outages)**。クラウドプロバイダが倒産または施設の喪失など、重大な問題に遭遇し、その結果、長期にわたってサービスが影響を受ける、あるいは完全に停止する可能性がある。例えば、2009年4月には、FBIがTexasにあるコンピュータセンターに捜査に入り、センターを使って業務をしていた少数の企業に対するあいまいな不正容疑の捜査のために数百台のサーバーを押収した[Zet09a]。この押収によって、捜査と無関係の数百の企業に対するサービスが止まった。ターゲットとなったセンターにコンピュータ運用をコロケーションしていたことによる不

幸だった[Zet09a]。サービス停止の別の例としては、2009年にブックマークリポジトリサービスにおいて大量のデータが消失したと、2008年にオンラインストレージサービスプロバイダがユーザへの通知を行わずに突然サービスを終了したことが挙げられる[Cal09, Gun08]。経営環境の変化によってサービスを終了するということも、最近オンラインクラウドストレージサービスにおいて発生したように、起こりうる[Sto10]。組織の異常対処計画には、長期的および恒久的なシステムの中断に備えた事業継続案を盛り込み、業務継続をサポートすることで、重要な機能を他の場所で復旧することを可能にする。

- **サービス拒否 (Denial of Service)**。サービス拒否攻撃は、攻撃の対象を偽のリクエストで飽和状態にさせ、正規のリクエストにタイムリーに回答できなくなる仕組みである。通常、アタッカーは複数のコンピュータまたはボットネットを使用して攻撃をしかける。分散サービス拒否攻撃が失敗に終わっても、防御に必要な大量のリソースが短時間で消費されてしまい、使用料が跳ね上がることが考えられる。クラウドのダイナミックプロビジョニングのおかげで、危害を加えるためのアタッカーの作業が容易になる。クラウドのリソースは膨大だが、それでも十分な攻撃用コンピュータがあれば、クラウドを飽和させることが可能になる[Jen09]。例えば、IaaS クラウド上のコードをホスティングするサイトに対するサービス拒否攻撃により、19時間以上に及ぶダウンタイムが生じた事例がある[Bro09, Met09]。

一般にアクセス可能なサービス以外にも、クラウドマネジメントに使用されるサービスなど、内部からしかアクセスできないサービスに対してサービス拒否攻撃が行われることもある。[Sla09]。クラウドプロバイダのネットワーク内のリソースの管理に使用するための、内部で割り当てたルーティング対象でないアドレスもまた、攻撃ベクトルとして利用される可能性がある[Kre08]。最悪の可能性としてありうるのは、あるクラウドの元素が別のクラウドの元素を攻撃することや、自クラウド内の他の元素を攻撃することである[Jen09]。

- **価値の集中 (Value Concentration)**。「あなたはなぜ銀行を襲うのか？」という質問に対しては、歴史に名を残した凄腕の強盗である Willie Hutton[Coc97]の「そこに金があるからさ」という答えがよく引き合いに出される。いろいろな意味で、データレコードは 21 世紀の貨幣であり、クラウドベースのデータの保管庫は銀行の金庫室であり、そこに集中する価値の集積は、ますます格好の標的になっている[Row07]。個人よりも銀行を襲うことによって得られるスケールメリットと同様に、クラウドの侵害に成功した場合の稼ぎの率も大きい。

直接的なアプローチとは対照的に、Willie Hutton の特徴は、手際の上と、すり抜けのうまさにあった。そのスタイルは、クラウドコンピューティングのデジタル世界にも通用する。例えば、最近発生した悪用の事例では、ソーシャルネットワーキングサービスの管理者の電子メールアカウントが狙われた。アカウントにアクセスするためのセキュリティ上の質問への答えから情報を得て、PaaS クラウドに格納されている会社のファイルへのアクセスを得たとの報道がある。[Inf09, Sut09]。同様の弱点がパブリッククラウドでも発見された[Gar07]。クラウドプロバイダの管理用ダッシュボードから認証情報をダウンロードするには、登録済みの電子メールアドレスと、当該アカウントの有効なパスワードが手元があれば十分であり、それがあればそのアカウントの全てのリソースにアクセスできる。パスワードを紛失しても電子メールでリセットが可能のため、アタッカーはそのアカウントのメールシステムのコントロールを握るか、ある

いはパスワードリセットのための電子メールを受動的に盗聴することで、巧みにアカウントを乗っ取ることも可能である。

自組織のデータがサービス拒否攻撃の標的になりやすい組織のデータと同じ環境に置かれた場合、その組織を狙ったサービス拒否攻撃に巻き込まれる可能性がある[Row07]。同様に、攻撃の標的になりやすい組織のクラウドベースのリソースに対する物理的攻撃が行われた場合に、副次的な影響を受ける可能性もある。例えば、内国歳入庁 (Internal Revenue Service)の施設は、長年にわたってアタッカー予備軍の関心を引き魅了してきた[Kat10, Lab95, Lat96, Sch10]。

4.9 インシデント対応

その名が示すとおり、インシデント対応には、コンピュータシステムのセキュリティに対する攻撃の結果を取り扱うための体系だった方法を意味する。インシデントの検証、攻撃の分析、封じ込め、データの収集および保管、問題の緩和、サービスの復旧を含む、インシデント対応活動におけるクラウドプロバイダの役割は極めて重要である。アプリケーションとデータの移行に際して、組織内のコンピュータ環境とクラウドコンピューティング環境との違いを意識してインシデント対応計画を改定することは重要な必須条件であるが、つい見逃されがちである。

サービス利用者とプロバイダが協力してインシデントを検知し対応を取ることは、クラウドコンピューティングのセキュリティとプライバシーを確保するうえで重要である。サービスの複雑さがインシデントの検知と分析を妨げることもある。例えば、IaaS プロバイダが、サービス利用者からの通告を受けてから、自身のクラウド基盤に対する明白なサービス拒否攻撃への対応を開始するまでに約 8 時間かかったという事例がある[Bro09, Met09]。インシデント対応に関する役割分担や手順を正しく理解し、交渉することは、後知恵でなく、サービス契約を結ぶ前にやっておく必要がある。データの地理的な位置は、調査の妨げとなる要因になることもあるので、契約上の交渉の対象に含めるべきである。

インシデントの対応は、被害を最小限に抑え、リカバリにかかる時間と費用を削減できるような形で実施されるべきである。これには、クラウドプロバイダとサービスユーザの代表から成る混合チームを迅速に召集できることが重要となる。問題の改善には片方の関係者だけで済む場合と、双方の関係者の参加が必要な場合がある。一つの問題の解決が当該クラウドサービスを使用する他のユーザになんらかの影響を与えることがある。クラウドプロバイダが、インシデントの発生時および発生後にユーザと情報を共有するための透明な対応プロセスとメカニズムを備えることが、重要である。

4.10 推奨事項のまとめ

前サブセクションでは、セキュリティおよびプライバシーに関する重要な課題を示した。表 1 に、それらの課題と注意事項の要約を示す。これらは、パブリッククラウドサービスへのアウトソーシングのお膳立てを計画、レビュー、交渉または開始する際に、組織が従うべき推奨事項である。

表 1: セキュリティおよびプライバシーに関する課題と注意事項

分野	注意事項
ガバナンス	組織の実践規範を拡張して、クラウドにおけるアプリケーションの開発とサービスの提供に

(Governance)	<p>関するポリシー、手順、標準に適用すること、ならびに実装された、または稼働中のサービスの設計、実施、テスト、モニタリングにも適用すること。</p> <p>組織の実践規範がシステムのライフサイクル全体を通して順守されることを確実にするための監査メカニズムおよびツールを導入すること。</p>
コンプライアンス (Compliance)	<p>セキュリティおよびプライバシー関連の組織の義務を規定し、クラウドコンピューティングイニシアチブに影響を与える可能性のある様々な種類の法規制について理解すること。特に、データの所在地、プライバシーおよびセキュリティ管理策、電子的な証拠開示に関するものについて実施すること。</p> <p>充足される必要がある組織の要求条件についてクラウドプロバイダの提供条件をレビュー・評価し、契約条件がそれら要求事項と合致することを確実にすること。</p>
信用 (Trust)	<p>クラウドプロバイダが採用しているセキュリティおよびプライバシーに関する管理策とプロセスについて、その継続実施も含めて把握できるための仕組みを確保するための仕組みを契約に盛り込むこと。</p> <p>絶え間なく進化と変化を遂げるリスク状況に対応できるだけの柔軟なリスクマネジメントプログラムを制定すること。</p>
アーキテクチャ (Architecture)	<p>システムのライフサイクルの全過程とすべてのシステムコンポーネントについて、サービスを提供するためにクラウドプロバイダが使用するテクノロジーを理解すること。これには、システムのセキュリティとプライバシーに関わる技術的管理策に関わる部分の理解も含まれる。</p>
アイデンティティ・アクセス管理 (Identity and Access Management)	<p>認証、承認、その他のアイデンティティ・アクセス管理機能を確保するための適切な保護対策が実施されることを確実にすること。</p>
ソフトウェア間隔離 (Software Isolation)	<p>クラウドプロバイダが導入している仮想化およびその他のソフトウェア間の隔離技術を理解し、内在するリスクを評価すること。</p>
データの保護 (Data Protection)	<p>扱われる組織のデータに対するクラウドプロバイダのデータマネジメントソリューションが適切であるか否かを評価すること。</p>
可用性 (Availability)	<p>中期のもしくは長引いたサービスの中断または深刻な災害に遭遇した場合に、重要な業務を速やかに再開し、最終的にはすべての業務をタイムリーに、かつ系統的に復旧できることを確実にすること。</p>
インシデント対応 (Incident Response)	<p>組織にとって必要なインシデント対応に関する、契約上の条件および手順について、確認し確保すること。</p>

5. パブリッククラウドのアウトソーシング

クラウドコンピューティングは、新しいコンピュータパラダイムであるが、IT サービスのアウトソーシングはそうではない。組織が取る措置は、パブリッククラウドであれ、他のより従来型の IT サービスであれ、基本的に変わらない。また、アウトソーシングに関する既存のガイドラインも、一般的にはそのまま適用できる。異なる点としては、パブリッククラウドコンピューティングでは、実装されたアプリケーションとシステムに対する説明責任とコントロールを、ライフサイクル全体を通して維持するための適切な監視を十分に行うことがより複雑、かつ困難である可能性があることである。交渉の余地のない SLA ではこの問題が深刻化する。なぜなら、本来なら組織が担うべき責務をクラウドプロバイダに委ねることになり、問題が起きたときに満足いく対応をし、事態を解決するすべが組織にほとんど残らないからである。

パブリッククラウドサービスにおける交渉可能な SLA のサービス条項について合意に至ることは、技術と法律面での問題が満載の複雑なプロセスである。前章で述べたように、組織のデータと機能をクラウドに移行する際には、セキュリティおよびプライバシーに関する多くの問題に取り組まなければならない。それらの問題の多くは、クラウドプロバイダの技術面での管理策が組織のニーズを満たすか否かにかかわってくる。サービス条項によって規定するサービスの提供は、情報の保護、配信、開示に関する既存のプライバシーポリシーに適合するものでなければならない。関連する費用とリスクとは、プロバイダやサービスごとに異なる。一つの問題に対する意思決定は、組織の他の問題に大きな影響を与える可能性がある[Gra03]。

クラウドプロバイダの数が増え、サービスの範囲も広がることを踏まえると、組織が機能をクラウドに移行する際には、デューディリジェンス(詳細立入調査)を実施する必要がある。新しいサービスとサービス提供についての意思決定では、費用および生産性の面での利益と、リスクや法的責任による不利益とのバランスの問題に直面することになる。

クラウドへの移行の事例:ロサンゼルス市によるクラウドコンピューティングへの移行の取り組みは、関連する計画作成および起こりうる問題についての洞察を提供している[CSC10]。その取り組みは、市の電子メールおよびスケジュール管理システムをオンサイト環境から同じサービスを提供するパブリック SaaS クラウドに移行することで、生産性および協働作業を改善する力を獲得するというものである[CSC10, DPW10, SECS09]。本契約には、ユーザトレーニングとデータの移行も含まれる。

SECS (SaaS E-mail and Collaboration Solution)のレポートによると、同市は、セキュリティおよびプライバシー関連のいくつかの項目を話し合いを通じて契約に盛り込むことに成功した。これは、多くの政府機関にとって興味深い話であろう[CSC10, Ove10, Wil10]。例えば、警察署と消防署は、彼らが扱う逮捕歴やその他の機微な犯罪データを外部のサーバーに保存する場合のリスクについて、懸念を示した。その結果機微なデータはプライベートクラウド環境に置かれた。追加の対策としてカリフォルニア州司法省は、市のデータにアクセスするクラウドプロバイダの職員に対して検証を行う予定である。

この他にも重要な交渉事項として、データの強制的暗号化、データを保管する場所に関する制限、罰金を伴うサービスレベル要件、電子的な証拠開示機能、明確に定義されたデータの所有権とその停止の権利、下請業者に同等の義務を負わせることの義務化、特定の違反に対する無制限の賠償責任を含む広範な補償義務[Ove10, Wil10]を含む。データは暗号化された状態で保存され、恒久的に市の財産となる[Cra10]。クラウドプロバイダがどんなファイルであれ平文で開くにあたっては、書面による市の承認が必要となる。すべてのアクセスはログに記録され、市は、自ら監査するためのアクセス手段を有する[Cra10]。そのクラウドプロバイダは、ロサンゼルス市およびその他の公共部門の顧客が所有するデ

ータを保管するための、隔離されたクラウドを構築中であると伝えられている。

ほぼすべてのソフトウェアの変更と同様に、クラウドコンピューティングへの移行もトレーニング、インテグレーション、データの移行、その他関連問題を伴う。クラウドコンピューティングへの移行を計画する際には、それらの問題が生産性にもたらす影響を過小評価したり、軽視することがないようにすべきである[Mic10]。例えば、ロサンゼルス市の送信メールサービスと SaaS の送信メールサービスとの間に、機能面で大きく異なる点がある[DPW10]。クラウドプロバイダのメールサービスでは、送信メールの高、標準、低い機密ランク付けは行われない。また、受信者からの返信を追跡する機能もなく、メールを整理するためにラベリングに頼る代わりにフォルダを使用することへのサポートもない。市の職員には、移行に関わる重要な業務を実施することが求められる。これには、重要でない電子メールやキャンセルされたアポイントメントなどをすべて削除すること、すべてのメールを年ごとにアーカイブすること、新しいシステムに自動的に移行されない 25 メガバイトを超える添付ファイルを個別に保存することによって既存のメールアカウントをきれいにする事が含まれる[DPW10]。

警察署およびその他の市の機関の機微なデータのセキュリティの確保は、当初の想定ほど容易ではないことが明らかになり、実施に遅延を生じさせている[Sar10]。この遅延のため、問題が解決するまで現行のシステムを当初の予定よりも長い期間にわたって更新するシステムと併用することになり、費用も増大する。結局、新システムに移行した警察署職員数百人分のアカウントを現行のシステムにも暫定的に復元しなければならなかった。クラウドプロバイダの事業本部長は、「ロサンゼルス市のクラウドへの移行は初めての試みであり、市のユニークな要件をすべて明らかにして対応するのに多少予想以上の時間がかかるのは驚くに当たらない」と述べた[Din10]。仮にこの問題が会計年度末である 2011 年 6 月までに解決しない場合には、市の幹部は契約の解約を検討することになり、契約違反が発生していないか検証する可能性があることが報じられた。

5.1 一般的な懸念事項

従来型の IT アウトソーシング契約に含まれる条項、特に機微なデータに関するものは、クラウドコンピューティングについて検討する際のガイドラインにもなる。サービス契約における三つの主なセキュリティおよびプライバシー関連問題については前述したが、それらの問題はパブリッククラウドコンピューティングサービスのアウトソーシングにも当てはまる[All88, Len03]。

- **不適切なポリシーおよび実践手順 (Inadequate Policies and Practices)**。クラウドプロバイダのセキュリティポリシーおよび実践手順は、組織に対して適当でなく、適合しない可能性がある。プライバシーに関しても同じことが言える。その結果、クラウドプロバイダの監査と監視に関するポリシーが不十分であるが故に侵入や違反行為が検知されない、組織とクラウドプロバイダ間で職務の分離(すなわち、役割と責任の明確な割り当て)または二重化(すなわち、十分な相互確認によって業務の一貫性と正確さを保つこと)のポリシーに相違があるが故にデータと設定の完全性が確保されない、機微な情報が組織のポリシーが定める厳密さのレベルで扱われていないためプライバシーが損なわれる、といったことが起こりうる[All88]。
- **機密性と完全性の保証の不十分さ (Weak Confidentiality and Integrity Sureties)**。クラウドプロバイダのプラットフォームに十分なレベルのセキュリティ管理策が導入されていないと、システムの機密性とプライバシー、または完全性に悪い影響が生じる可能性がある。例えば、セキュリティが確保されていないリモートアクセス方式を使用している場合、システムに侵入され、組織の情報システムとリソースが不正にアクセス、改ざん、または破壊される可能性、またはセキュリティ上の脆弱性またはマルウェアが意

図的にシステムに導入される可能性、もしくは組織のネットワークから他のシステムへの攻撃が行われ
て損害賠償責任を負わされる可能性がある [All88]。

- **可用性の保証の弱さ (Weak Availability Sureties)**。クラウドプロバイダのプラットフォームに十分なレベルの保護対策が導入されていないと、システムの可用性に悪い影響が生じる可能性がある。システムの可用性の喪失は、直接影響を受けるアプリケーション以外にも、組織の重要な業務に必要なキーリソースに対する問題を招く可能性がある。例えば、組織のコンピュータ処理がピークに達している時に、クラウドプロバイダによって大掛かりな処理(例: サイトの故障または緊急な修理のための負荷の再バランシング)が行われた場合、組織のシステムのサービス拒否が起きる条件が整う可能性がある [All88]。クラウドプロバイダに対するサービス拒否攻撃は、組織のデータセンタまたはクラウドで稼働中の組織のアプリケーションやシステムにも影響を与える。

パブリッククラウドのアウトソーシングでは、セキュリティとプライバシーに直接関連しないもの知っておくべき問題がある。最も一般的で厄介な問題の一つに、本人対代理人関係の問題がある。これ以外にも、組織の技術的専門知識の衰退がある。

- **本人対代理人関係の問題 (Principal-Agent Problem)**。本人対代理人関係の問題は、代理人(クラウドプロバイダ)のインセンティブが、本人(組織)のインセンティブと一致しない場合に生じる[Row07]。クラウドプロバイダがセキュリティとプライバシーの管理と改善にどの程度注力すべきかを決定するのは困難なので、サービスレベルが低下したり、要求されるレベルを下回ったとしても、組織が認識できないといったことが懸念される。厄介なのは、セキュリティに対する取り組みが向上したからといって、セキュリティが著しく向上する(例: インシデントの数が減る)わけではないということである。その理由の一つには、マルウェアや新種の攻撃が増え続けていることが挙げられる [Row07]。
- **専門技術の衰退 (Attenuation of Expertise)**。コンピュータサービスのアウトソーシングは、組織の技術的な知識と専門技術を時間の経過とともに衰退させる。なぜならば、経営陣と職員が、技術的な問題を細部にわたって扱う必要がなくなるからである[Gon09]。クラウドコンピューティング環境は進化すると同時に改善がなされるため、そこで得られた知識と経験を直接享受するのは組織ではなくクラウドプロバイダである。油断していると組織は技術の進歩や関連するセキュリティおよびプライバシー問題についていく能力を失い、ひいては新たな IT プロジェクトを効果的に計画・統率することや、既存のクラウドベースのシステムに対する説明責任を果たすことができなくなる。

上述のセキュリティおよびプライバシー問題に対する説明責任を果たし、それらの問題を軽減するには、アウトソーシングのライフサイクルの三つの段階、すなわち、アウトソーシングされたサービスの開始、継続、終了の各段階において、いくつかの作業が必要となる[All88, Len03]。通常、交渉の余地のない SLA では、ライフサイクルにおいて組織が実施できる作業が限られている。一方、交渉可能な SLA では、より広範の作業が可能であり柔軟性も与えられるが、高い費用対効果を得るためには、サービス条項に含まれる要求事項を慎重に精査して優先順位付けを行うことが必要となる。組織は、交渉の余地のない SLA によるパブリッククラウドサービスでは不足することが判明した部分を補うために補完的管理策を採用してもよい。もう一つの代替案は、より適した実装モデル(例えば、プライベートクラウド)を選択することである。それにより、セキュリティとプライバシーをより厳密に監視・コントロールできるようになる。

5.2 事前の実施事項

組織は、アウトソーシングするパブリッククラウドサービスに対する契約書を発行する前に、種々の計画作業を行う必要がある。計画作成は、IT への支出の効用を最大限に引き出せるようにすることに役立つ。また、コンピューティング環境の安全性を最大限に確保し、組織の関連するすべてのポリシーへの準拠を確実にし、データプライバシーの維持を確実にすることに役立つ。計画作業には、以下に示すセキュリティ関連の項目が含まれる。

- **要件定義 (Specify Requirements)**。組織は、クラウドプロバイダの選択基準となる、クラウドサービスが満たすべきセキュリティ、プライバシーその他の要件を定義する必要がある。一般的なセキュリティ要件には、以下の項目が含まれる。
 - 職員に対する要件。これにはクリアランス(権限の分離)および責任が含まれる
 - アクセス制御
 - サービスの可用性
 - 問題の報告、レビュー、解決
 - 情報の取り扱いおよび開示に関する取り決めと手続き
 - 物理的／論理的アクセス制御
 - ネットワークの接続性およびフィルタリング
 - 構成およびパッチの管理
 - バックアップおよびリカバリ
 - インシデントの報告、ハンドリング、対応
 - 運転の継続
 - アカウントおよびリソースの管理
 - 証明と認証
 - 保証レベル
 - 第三者による、サービスの監査

上記以外にも、セキュリティに関連する要求事項として、プライバシー、データの所有権、レコードマネジメントコントロール、ユーザトレーニングが明らかにされるべきである。クラウドコンピューティングに関する

る既存の契約書に含まれている一般的なアウトソーシング規定(プライバシーおよびセキュリティ標準、規制およびコンプライアンス、サービスレベルに関する基準および罰則、変更管理プロセス、サービス継続規定、終了に関する権利など)を見直すことは、要件定義の一助となる[Ove10]。

- **セキュリティおよびプライバシーリスクを評価する (Assess Security and Privacy Risks)**。アウトソーシングによって組織は業務上の責任から解放されるが、クラウドプロバイダが提供するパブリッククラウドサービスの利用に伴うリスクについては、組織が自己防衛する必要がある。分析には、使用するサービスモデル、サービスの目的と範囲、プロバイダが必要とし、かつ、組織のコンピュータ環境とプロバイダのサービス間での使用が推奨されるアクセスの種類とレベル、サービスの期間と依存性、クラウドプロバイダが用意するセキュリティ管理策が提供する保護の強度も含める必要がある[Len03]。プライバシーコントロールに加えて、クラウドプロバイダの所在地に起因する運用上のリスクも評価すべきである。交渉の余地のない SLA の場合には、サービス条項がクラウドプロバイダによる一方的な改訂の対象になるか否かも考慮する必要がある。

リスクの分析では、データの機微度が重要かつ決定的な因子となる。組織が扱うデータの範囲は、初期段階では十分に考慮されないことがある。個人情報または機密情報が保管されているデータリポジトリは、容易に認識され配慮の対象となるが、それ以外にも扱い方のルールが異なる機微なデータが存在しうる。そのようなデータには、以下のものが含まれる。

- 法の執行と調査に関するユニットデータ
- アプリケーションの開発に使用される、使用許諾を受けたソースコードおよびライブラリ
- 機密保持契約または MOA(合意の覚書)の下で入手したデジタル文書および資料
- 収集、保管、共有が規制されている研究・調査データ
- インディアン部族の領土の管理と資源保護に関連する文化的に機微なデータ

リスクレベルが高すぎるものがリスク分析によって判明した場合、組織はリスクを受容できるレベルまで低減するために補完的管理策を導入することもできる。そうでない場合、パブリッククラウドサービスを利用しない、または、より高いレベルのリスクを受容することになる。あるいは、サービスを受け入れずに足踏みするよりも、機微度の低いデータに限定してアウトソーシングを行うように範囲を狭めるという選択肢もある。

- **クラウドプロバイダの能力を評価する (Assess the Competency of the Cloud Provider)**。組織は、サービスのアウトソーシング契約を発注する前に、予定期間中サービス提供を継続し、表示されたセキュリティおよびプライバシーのレベルを確保する能力と意思が、クラウドプロバイダに備わっているか否かを評価すべきである。クラウドプロバイダには、セキュリティおよびプライバシーの実施に関してその能力と取り組みを示すこと、または第三者による設備とシステムの評価を受けることが求められることがある[All98]。現在サービスを利用しているユーザに聞き取りを行って、ユーザの満足度を確かめることも、ク

クラウドプロバイダの能力についての洞察を与えてくれる。サービスのプライバシーおよびセキュリティレベルの評価は厳密に行う必要があり、以下に示す項目も考慮対象とすべきである[Len03]。

- 職員の経験と技術的な専門知識
- 職員が受ける信用度調査プロセス
- 職員に対するセキュリティおよび意識向上トレーニングの質と頻度
- 提供されるセキュリティサービスと、そのベースとなるメカニズムの種類と有効性
- 新しい技術の採用率
- クラウドプロバイダの実績記録と、クラウドプロバイダが組織のセキュリティおよびプライバシーに関するポリシー、手続き、法規制順守対応ニーズを満たすことができる能力

5.3 契約開始と契約期間中の実施事項

クラウドプロバイダに契約を発注する際および契約期間中に、組織が実施すべき事項はいくつかある。

- **契約上の義務を定める (Establish Contractual Obligations)**。組織は SLA に、プライバシーおよびセキュリティに関する規定を含む、契約上のすべての要求事項が明確に記述されているようにしなければならない [Gra03, Len03]。契約書には、組織とクラウドプロバイダの双方の役割と責任の定義に加えて、以下に示す項目も含めなければならない [Gra03]。
 - 施設の所在地と、適用されるセキュリティ要件を含む、サービス環境についての詳細な説明
 - 職員の信用度調査と管理を含む、ポリシー、手続き、および標準
 - あらかじめ定められたサービスレベルおよびそれに伴うコスト
 - SLA をクラウドプロバイダが順守しているか、についての評価プロセス、および、その第三者による監査とテスト
 - クラウドプロバイダの契約違反またはクラウドプロバイダによりもたらされた危害に対する具体的な補償
 - サービス提供の期間と提供物の納期
 - クラウドプロバイダの組織に対する窓口
 - 組織が関連情報とリソースをクラウドプロバイダに提供する義務

- 組織のデータを他のデータと混在させることと、機微なデータの取り扱いに関する手続き、保護対策、および制限
- 契約が終了した際のクラウドプロバイダが果たすべき義務(例:データの返却および消去)

契約を結ぶ前に、経験豊富な法律の専門家に契約条件のチェックをしてもらうことをお勧めする。通常、交渉の余地のない SLA はクラウドプロバイダの都合に合わせて作成されるため、組織にとっては受け入れ不可能の可能性がある。交渉可能な SLA が使用される場合、交渉時に法律上の複雑な問題が浮上する可能性が高いため、交渉には法律の専門家にも参加してもらうことが望ましい。

- **クラウドプロバイダのパフォーマンスを評価する (Assess Cloud Provider Performance)**。契約上のすべての義務が果たされることを確実にするには、パフォーマンスの継続的な評価が必要となる。この継続的な評価によって、検知した問題に対して速やかに是正措置または懲罰措置をとることができ、SLA のサービス条項を改善するための参照事項も得られる[All88, Gra03, Len03]。

5.4 終了のための実施事項

プロジェクトのライフサイクルの最後の段階、他のクラウドプロバイダに乗り換える場合、または他の理由により、組織はアウトソーシングしていたパブリッククラウドサービスの利用を中止して契約を終了することを決める場合がある。組織は、アウトソーシング契約を終了する際には、以下に示す事項を実施しなければならない。

- **契約上の義務を再確認させる (Reaffirm Contractual Obligations)**。組織は、契約条件の守秘義務や組織のデータの削除など、契約終了時に守られるべき契約上の要求事項について、クラウドプロバイダに再度認識させなければならない[Len03]。
- **物理的アクセスおよび電子アクセス権限を無効化する (Eliminate Physical and Electronic Access Rights)**。組織は、クラウドプロバイダに割り当てたすべてのアカウントとアクセス権限を適時に無効化しなければならない[All88, Len03]。セキュリティトークンやバッジに付された物理的アクセス権を無効化すると同時に、アクセスのために使用した個人支給のトークンやバッジも回収しなければならない[All88]。
- **組織のリソースとデータを回収する (Recover Organizational Resources and Data)**。組織は、SLA に基づいてクラウドプロバイダが利用できるようにしたソフトウェア、機器、ドキュメント、データなどのリソースが、規定に従って利用できる形で返還されることを確実にしなければならない。サービス条項によりクラウドプロバイダがデータプログラム、バックアップコピー、およびその他のクラウド利用者に帰属するコンテンツを自身の環境から消し去ることが規定されている場合には、組織はシステムレポートまたはログなどの証拠を入手して検証し、実際に情報が正しく消去されていることを確認しなければならない[Len03]。

5.5 推奨事項のまとめ

表 2 に、アウトソーシングの各段階における課題と注意事項の要約を示す。これらは先の表 1 に示した推奨事項を補足するものであり、パブリッククラウドサービスのアウトソーシング契約を締結するに際しての、組織のための一連の推奨事項となる。

表 2: アウトソーシング活動とアウトソーシングに関する注意事項

分野	注意事項
<p>事前の実施事項 (Preliminary Activities)</p>	<p>クラウドプロバイダの選択基準となる、クラウドサービスによって満たされるべき要件(セキュリティおよびプライバシーに関する要件を含む)を抽出すること。</p> <p>リスク評価を行うこと。すなわち、組織の管理目標に照らして、クラウドプロバイダの環境におけるセキュリティおよびプライバシー管理策を評価すること。</p> <p>予定期間中サービス提供を持続し、表示されたセキュリティおよびプライバシーのレベルを確保する能力と意思が、クラウドプロバイダに備わっているか否かを評価すること。</p>
<p>契約開始と契約期間中の実施事項 (Initiating and Coincident Activities)</p>	<p>SLA に、プライバシーおよびセキュリティに関する規定を含む、契約上のすべての要求事項が明示的に記載されていることと、クラウドプロバイダがそれらの要求事項を受諾していることを確実にすること。</p> <p>SLA のサービス条項についての交渉とレビューを行う際には、法律の専門家を参加させること。</p> <p>クラウドプロバイダのパフォーマンスを継続的に評価し、契約上のすべての義務が果たされていることを確実にすること。</p>
<p>終了に際しての実施事項 (Concluding Activities)</p>	<p>契約終了時に守るべき契約上のすべての要求事項をクラウドプロバイダに再認識させること。</p> <p>クラウドプロバイダに割り当てたすべての物理的アクセス権限および電子的アクセス権限を無効化し、物理的なトークンおよびバッジを適時に回収すること。</p> <p>SLA に基づいてクラウドプロバイダが利用できるようにしたリソースが利用できる形で返還されることを確認し、情報が正しく消去されていることを証拠によって確認すること。</p>

6. むすび

クラウドコンピューティングの出現によって、連邦政府機関およびその他の組織のシステムとネットワークに広範な影響をもたらされると期待される。パブリッククラウドコンピューティングにおけるコストとパフォーマンスの利点が強調されるため、そうしたコンピュータ環境に対して連邦政府の各省庁が抱くセキュリティおよびプライバシーに関する基本的な懸念事項が過小評価されがちである。クラウドコンピューティングを魅力的にする機能の多くは、従来のセキュリティモデルや管理策が適用できない可能性がある。信認連携 (federated trust) など、いくつかの重要な技術要素が未実現のままであり、クラウドコンピューティングが順調に広まることを妨げている。複数の要素から成る複雑なコンピュータシステムのセキュリティを定義することは、一般的な大規模コンピューティング、とりわけクラウドコンピューティングにとって悩ましい、中々解決しないセキュリティ上の課題である。実装において保証レベルの高い品質を実現することは、コンピュータセキュリティの研究者および実務家にとって達成が困難な到達目標であり、この報告書で取上げた例が示すように、クラウドコンピューティングにおいても取り組み途上の課題である。とはいえ、パブリッククラウドコンピューティングは、政府機関が自身の IT ソリューション設備の一部に取り入れられないわけに行かないコンピューティングパラダイムである。

パブリッククラウドのセキュリティおよびプライバシーに関する説明責任は組織にある。連邦政府機関は、選択されたパブリッククラウドコンピューティングのソリューションが、組織のセキュリティやプライバシーなどの要求事項を満たすように設定、実装、管理されていることを確実にしなければならない。組織のデータは、自組織のコンピュータセンターまたはクラウドのどちらかに保管されているかにかかわらず、組織のポリシーに従って保護されなければならない。組織は、セキュリティおよびプライバシー管理策が正しく導入されていて、意図したとおりに運用されていることを確実にしなければならない。

アウトソーシングされたパブリッククラウドコンピューティング環境への移行は、いろいろな形でリスクマネジメントの課題となる。リスクマネジメントとは、リスクを特定し評価したうえで、そのリスクを受容可能なレベルまで軽減するために必要な手立てを講じることを意味する。クラウドコンピューティングシステムにおけるリスクを評価し管理することは、困難な課題と言える。システムのライフサイクル全体を通して、特定されたリスクは、利用可能なセキュリティおよびプライバシーの管理策ならびにそれらの適用効果に対して、うまくバランスさせなければならない。効果がコストおよび関連リスクを上回る場合、管理策の数が多すぎて効率が悪くなり効果も弱められている可能性がある。政府機関および組織は、管理策の数および強度と、クラウドコンピューティングのソリューションに伴うリスクとの適切なバランスを確保するために取り組まなければならない。

7. 参考文献

- [All88] Julia Allen et al., Security for Information Technology Service Contracts, CMU/SEISIM-003, Software Engineering Institute, Carnegie Mellon University, 1988年1月, <URL: <http://www.sei.cmu.edu/reports/98sim003.pdf>>.
- [Arm10] Michael Armbrust et al., A View of Cloud Computing, Communications of the ACM, Association for Computing Machinery, Vol. 53, No. 4, 2010年4月
- [Ash10] Warwick Ashford, Google Confirms Dismissal of Engineer for Breaching Privacy Rules, Computer Weekly, 2010年9月16日, <URL: <http://www.computerweekly.com/Articles/2010/09/16/242877/Google-onfirm dismissal-of-engineer-for-breaching-privacy.htm>>.
- [Avo00] Frederick M. Avolio, Best Practices in Network Security, Network Computing, 2000年3月20日, <URL: <http://www.networkcomputing.com/1105/1105f2.html>>.
- [Bin09] David Binning, Top Five Cloud Computing Security Issues, Computer Weekly, 2009年4月24日, <URL: <http://www.computerweekly.com/Articles/2010/01/12/235782/Topfive-cloud-computing-security-issues.htm>>.
- [Bra10] Simon Bradshaw, Christopher Millard, Ian Walden, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, Queen Mary School of Law Legal Studies, Research Paper No. 63/2010, 2010年9月2日, <URL: http://papers.ssm.com/sol3/papers.cfm?abstract_id=1662374>.
- [Bro08] Jon Brodtkin, Loss of Customer Data Spurs Closure of Online Storage Service ‘The Linkup,’ Network World, 2008年8月11日, <URL: <http://www.networkworld.com/news/2008/081108-linkup-failure.html?page=1>>.
- [Bro09] Carl Brooks, Amazon EC2 Attack Prompts Customer Support Changes, Tech Target, 2009年10月12日, <URL: http://searchcloudcomputing.techtarget.com/news/article/0,289142,sid201_gci1371090,00.html>.
- [Cal09] Michael Calore, Magnolia Suffers Major Data Loss, Site Taken Offline, Wired Magazine, 2009年1月30日, <URL: <http://www.wired.com/epicenter/2009/01/magnolia-suffer/>>.
- [Cap09] Dawn Cappelli, Andrew Moore, Randall Trzeciak, Timothy J. Shimeall, Common Sense Guide to Prevention and Detection of Insider Threats, 3rd Edition, Version 3.1, CERT, 2009年1月, <URL: <http://www.cert.org/archive/pdf/CSG-V3.pdf>>.

-
- [CBC04] USA Patriot Act Comes under Fire in B.C. Report, CBC News, 2004年10月30日, <URL:
http://www.cbc.ca/canada/story/2004/10/29/patriotact_bc041029.html>.
- [Cho09] Richard Chow et al., Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control, ACM Workshop on Cloud Computing Security, Chicago, Illinois, 2009年11月, <URL:
<http://www2.parc.com/csl/members/eshi/docs/ccsw.pdf>>.
- [Cla09] Gavin Clarke, Microsoft's Azure Cloud Suffers First Crash, The Register, 2009年3月16日, <URL:
http://www.theregister.co.uk/2009/03/16/azure_cloud_crash/>.
- [Coc97] Steve Cocheo, The Bank Robber, the Quote, and the Final Irony, nFront, American Bankers Association (ABA) Banking Journal, 1997年, <URL:
http://www.banking.com/aba/profile_0397.htm>.
- [Cra10] Private phone conversation with Kevin K. Crawford, Assistant General Manager, Information Technology Agency, City of Los Angeles, 2010年12月15日
- [CSC10] LA SECS Overview: SaaS E-mail and Collaboration Solution (SECS) –Implementing Google for the Los Angeles, CSC, 2010年4月15日, <URL:
http://assets1.csc.com/lef/downloads/LEFBriefing_CSC_LA_Google_041510.pdf>.
- [Daw05] Alistair B. Dawson, Understanding Electronic Discovery and Solving Its Problems, 56th Annual Program on Oil and Gas Law, The Center for American and International Law, 2005年2月17日から18日まで, Houston, Texas, <URL: <http://www.brsfirm.com/publications/docs/00037W.pdf>>.
- [Dig08] Larry Dignam, Amazon Explains Its S3 Outage, ZDNET, 2008年2月16日, <URL:
<http://www.zdnet.com/blog/btl/amazon-explains-its-s3-outage/8010>>.
- [Din10] Jocelyn Ding, LA's Move to Google Apps Continues Apace, Official Google Enterprise Blog, 2010年8月4日, <URL:
<http://googleenterprise.blogspot.com/2010/08/las-move-to-google-apps-continuesapace.html>>.
- [DoC00] Safe Harbor Privacy Principles, U.S. Department of Commerce, 2000年7月21日, <URL:
http://www.export.gov/safeharbor/eg_main_018247.asp>.
- [DPW10] LA DPW Engineering Newsletter, No. 10-22, Los Angeles City, Department of Public Works (DPW), 2010年4月21日, <URL:
<http://eng.lacity.org/newsletters/2010/04-21-10.pdf>>.
- [Dun10a] John E. Dunn, Ultra-secure Firefox Offered to UK Bank Users, Techworld, 2010年2月26日, <URL:
<http://news.techworld.com/security/3213740/ultra-secure-firefoxoffered-to-uk-bank-users/>>.

-
- [Dun10b] John E. Dunn, Virtualised USB Key Beats Keyloggers, Techworld, 2010年2月22日, <URL:
<http://news.techworld.com/security/3213277/virtualised-usb-key-beatskeyloggers/>>.
- [DVA] What the VA Is Doing to Protect Your Privacy, VA Pamphlet 005-06-1, Department of Veteran
Affairs, <URL: http://www.privacy.va.gov/docs/VA005-06-1_privacy_brochure.pdf>.
- [Eis05] Margaret P. Eisenhauer, Privacy and Security Law Issues in Off-shore Outsourcing Transactions,
Hunton & Williams LLP, The Outsourcing Institute, Legal Corner, 2005年2月15日,
<URL:http://www.outsourcing.com/legal_corner/pdf/Outsourcing_Privacy.pdf>.
- [Fer07] Peter Ferrie, Attacks on Virtual Machine Emulators, White Paper, Symantec
Corporation, 2007年1月, <URL:http://www.symantec.com/avcenter/reference/Virtual_Machine_Threats.pdf>.
- [Fer09] Tim Ferguson, Salesforce.com Outage Hits Thousands of Businesses, CNET News, 2009年1月8日,
<URL: http://news.cnet.com/8301-1001_3-10136540-92.html>.
- [Fer10] David S. Ferreiro, Guidance on Managing Records in Cloud Computing
Environments, NARA Bulletin 2010-05, 2010年9月8日,
<URL:<http://www.archives.gov:80/records-mgmt/bulletins/2010/2010-05.html>>.
- [Fre08] Stefan Frei, Thomas Duebendorfer, Gunter Ollmann, Martin May, Understanding the Web Browser
Threat: Examination of vulnerable online Web browser populations and the "insecurity iceberg",
ETH Zurich, Tech Report Nr. 288, 2008, <URL:<http://e-collection.ethbib.ethz.ch/eserv/eth:30892/eth-30892-01.pdf>>.
That May Mean, The Wall Street Journal, 2009年3月26日,
<URL:<http://online.wsj.com/article/SB123802623665542725.html>>.
- [Fow09] Geoffrey Fowler, Ben Worthen, The Internet Industry Is on a Cloud – Whatever That May Mean,
The Wall Street Journal, 2009年3月26日,
<URL:<http://online.wsj.com/article/SB123802623665542725.html>>
- [Gaj09] Sebastian Gajek, Meiko Jensen, Lijun Liao, and Jörg Schwenk, Analysis of Signature Wrapping
Attacks and Countermeasures, IEEE International Conference on Web Services, Los Angeles,
California, 2009年7月
- [Gar05] Tal Garfinkel, Mendel Rosenblum, When Virtual Is Harder than Real: Security Challenges in Virtual
Machine Based Computing Environments, HotOS'05, Santa Fe, New Mexico, 2005年6月,
<URL:<http://www.stanford.edu/~talg/papers/HOTOS05/virtual-harder-hotos05.pdf>>.
- [Gar07] Simson Garfinkel, An Evaluation of Amazon's Grid Computing Services: EC2, S3 and SQS,
Technical Report TR-08-07, Center for Research on Computation and Society, School for
Engineering and Applied Sciences, Harvard University, 2007年7月, <URL:
<http://simson.net/clips/academic/2007.Harvard.S3.pdf>>.

-
- [Gee08] Daniel E. Geer, Complexity Is the Enemy, IEEE Security and Privacy, Vol. 6, No. 6, 2008年11月/12月
- [Gon09] Reyes Gonzalez, Jose Gasco, and Juan Llopis, Information Systems Outsourcing Reasons and Risks: An Empirical Study, International Journal of Human and Social Sciences, Vol. 4, No. 3, 2009年, <URL: <http://www.waset.org/journals/ijhss/v4/v4-3-24.pdf>>.
- [Goo09a] Dan Goodin, Salesforce.com Outage Exposes Cloud's Dark Linings, The Register, 2009年1月6日, <URL:http://www.theregister.co.uk/2009/01/06/salesforce_outage/>.
- [Goo09b] Dan Goodin, Webhost Hack Wipes Out Data for 100,000 Sites, The Register, 2009年6月8日, <URL: http://www.theregister.co.uk/2009/06/08/webhost_attack/>.
- [Goo10] Dan Goodin, Privacy Watchdog Pack Demands Facebook Close the 'App Gap', The Register, 2010年6月16日, <URL:http://www.theregister.co.uk/2010/06/16/facebook_privacy/>.
- [Gra03] Tim Grance et al., Guide to Information Technology Security Services, NIST Special Publication 800-35, 2003年10月, <URL:<http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf>>.
- [Gre09] Andy Greenberg, IBM's Blindfolded Calculator, Forbes Magazine, 2009年7月13日, <URL: <http://www.forbes.com/forbes/2009/0713/breakthroughs-privacy-supersecret-encryption.html>>.
- [Gru09] Nils Gruschka, Luigi Lo Iacono, Vulnerable Cloud: SOAP Message Security Validation Revisited, IEEE International Conference on Web Services, Los Angeles, California, 2009年7月
- [Gun08] Mike Gunderloy, Who Protects Your Cloud Data?, Web Worker Daily, 2008年1月13日, <URL: <http://webworkerdaily.com/2008/01/13/who-protects-your-clouddata/>>.
- [HR2458] Federal Information Security Management Act of 2002 (FISMA), H.R. 2458, Title III—Information Security, <URL: <http://csrc.nist.gov/drivers/documents/FISMAfinal.pdf>>.
- [Inf09] Twitter Email Account Hack Highlights Cloud Dangers, Infosecurity Magazine, 2009年7月23日, <URL: <http://www.infosecurity-magazine.com/view/2668/twitter-emailaccount-hack-highlights-cloud-dangers-/>>.

-
- [Jac07] Dean Jacobs, Stefan Aulbach, Ruminations on Multi-Tenant Databases, Fachtagung für Datenbanksysteme in Business, Technologie und Web, Aachen, Germany, 2007年3月5日から9日まで, <URL: <http://www.btw2007.de/paper/p514.pdf>>.
- [Jan08] Wayne Jansen, Karen Scarfone, Guidelines on Cell Phone and PDA Security, Special Publication (SP) 800-124, National Institute of Standards and Technology, 2008年10月, <URL: <http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf>>
- [Jan09] Wayne Jansen, Directions in Security Metrics Research, Interagency Report (IR)7564, National Institute of Standards and Technology, 2009年4月, <URL: http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf>.
- [Jen09] Meiko Jensen, Jörg Schwenk, Nils Gruschka, Luigi Lo Iacono, On Technical Security Issues in Cloud Computing, IEEE International Conference on Cloud Computing, Bangalore, India, 2009年9月21日から25日まで
- [Jtf10] Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Joint Task Force Transformation Initiative, NIST Special Publication 800-37, Revision 1, <URL: <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>>.
- [Kan09] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Atanu Rakshit, Cloud Security Issues, IEEE International Conference on Services Computing, Bangalore, India, 2009年9月21日から25日まで
- [Kar08] Paul A. Karger, I/O for Virtual Machine Monitors: Security and Performance Issues, IEEE Security and Privacy, 2008年9月/10月
- [Kat10] Neil Katz, Austin Plane Crash: Pilot Joseph Andrew Stack May Have Targeted IRS Offices, Says FBI, CBS News, 2010年2月18日, <URL: http://www.cbsnews.com/8301-504083_162-6220271-504083.html?tag=contentMain%3bcontentBody>.
- [Kel05] Yared Keleta, J.H.P. Eloff, H.S. Venter, Proposing a Secure XACML Architecture Ensuring Privacy and Trust, Research in Progress Paper, University of Pretoria, 2005年, <URL: http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/093_Article.pdf>.
- [Ker10] Sean Michael Kerner, Mozilla Confirms Security Threat from Malicious Firefox Add-ons, eSecurity Planet, 2010年2月5日, <URL: <http://www.esecurityplanet.com/news/article.php/3863331/Mozilla-Confirms-Security-Threat-From-Malicious-Firefox-Add-Ons.htm>>.
- [Kin06] Samuel King, Peter Chen, Yi-Min Wang, Chad Verbowski, Helen Wang, Jacob Lorch, SubVirt: Implementing Malware with Virtual Machines, IEEE Symposium on Security and Privacy, Berkeley, California, 2006年5月, <URL: <http://www.eecs.umich.edu/~pmchen/papers/king06.pdf>>.

-
- [Kre07] Brian Krebs, Salesforce.com Acknowledges Data Loss, Security Fix, The Washington Post, 2007年11月6日, <URL:http://blog.washingtonpost.com/securityfix/2007/11/salesforcecom_acknowledges_dat.html>.
- [Kre08] Brian Krebs, Amazon: Hey Spammers, Get Off My Cloud! The Washington Post, 2008年7月1日, <URL:http://voices.washingtonpost.com/securityfix/2008/07/amazon_hey_spammers_get_off_my.html>.
- [Kow08] Eileen Kowalski et al., Insider Threat Study: Illicit Cyber Activity in the Government Sector, U.S. Secret Service and Carnegie Mellon University, Software Engineering Institute, 2008年1月, <URL:http://www.cert.org/archive/pdf/insiderthreat_gov2008.pdf>.
- [Kri08] Michael Kringsma, Amazon S3 Web Services Down. Bad, Bad News for Customers, ZDNET, 2008年2月15日, <URL: <http://blogs.zdnet.com/projectfailures/?p=602>>.
- [Kum08] Sushil Kumar, Oracle Database Backup in the Cloud, White Paper, Oracle Corporation, 2008年9月
- [Lab95] Stephen Labaton, 2 Men Held in Attempt to Bomb I.R.S. Office, New York Times, 1995年12月29日, <URL: <http://www.nytimes.com/1995/12/29/us/2-men-held-inattempt-to-bomb-irs-office.html?pagewanted=1>>.
- [Lat96] 20-Year Term in Plot to Bomb IRS Offices, Nation In Brief, Los Angeles Times, 1996年8月10日, <URL: http://articles.latimes.com/1996-08-10/news/mn-32970_1_20-year-term>.
- [Lea09] Neal Leavitt. Is Cloud Computing Really Ready for Prime Time?, IEEE Computer, 1月 2009年
- [Len03] Bee Leng, A Security Guide for Acquiring Outsourced Service, GIAC GSEC Practical (v1.4b), SANS Institute, 2003年8月19日, <URL:http://www.sans.org/reading_room/whitepapers/services/a_security_guide_for_acquiring_outsourced_service_1241>.
- [Mag10] James Maguire, How Cloud Computing Security Resembles the Financial Meltdown, Datamation, internet.com, 2010年4月27日, <URL:<http://itmanagement.earthweb.com/netsys/article.php/3878811/How-Cloud-Computing-Security-Resembles-the-Financial-Meltdown.htm>>.
- [Mcd10] Steve McDonald, Legal and Quasi-Legal Issues in Cloud Computing Contracts, Workshop Document, EDUCAUSE and NACUBO Workshop on Cloud Computing

-
- and Shared Services, Tempe, Arizona, 2010年2月8日から10日まで ,
<URL:http://net.educause.edu/section_params/conf/CCW10/issues.pdf>.
- [Mcm07] Robert McMillan, Salesforce.com Warns Customers of Phishing Scam, PC Magazine, IDG News Network, 2007年11月6日 ,
<URL:http://www.pcworld.com/businesscenter/article/139353/salesforcecom_warns_customers_of_phishing_scam.html>.
- [Mcm09a] Robert McMillan, Hackers Find a Home in Amazon's EC2 Cloud, Infoworld, IDG News Network, 2009年12月10日 , <URL: <http://www.infoworld.com/d/cloudcomputing/hackers-find-home-in-amazons-ec2-cloud-742>>.
- [Mcm09b] Robert McMillan, Misdirected Spyware Infects Ohio Hospital, PC Magazine, IDG News Service 2009年9月17日 ,
<URL:http://www.pcworld.com/businesscenter/article/172185/misdirected_spyware_infects_ohio_hospital.html>.
- [Mee09] Haroon Meer, Nick Arvanitis, Marco Slaviero, Clobbering the Cloud, Part 4 of 5, Black Hat USA Talk Write-up, SensePost SDH Labs, 2009年 ,
<URL:http://www.sensepost.com/labs/conferences/clobbering_the_cloud/amazon>.
- [Mel09] Peter Mell, Tim Grance, The NIST Definition of Cloud Computing, Version 15, 2009年10月7日 ,
<URL: <http://csrc.nist.gov/groups/SNS/cloud-computing>>.
- [Met09] Cade Metz, DDoS Attack Rains Down on Amazon Cloud, The Register, 2009年10月5日 , <URL: http://www.theregister.co.uk/2009/10/05/amazon_bitbucket_outage>.
- [Mic09] The Windows Azure Malfunction This Weekend, Windows Azure <Team Blog>, Microsoft Corporation, 2009年3月18日 , <URL:<http://blogs.msdn.com/windowsazure/archive/2009/03/18/the-windows-zuremalfunction-this-weekend.aspx>>.
- [Mic10] Fact-Based Comparison of Hosted Services: Google vs. Microsoft, Microsoft Corporation, 2010年5月16日 , <URL: <http://download.microsoft.com/download/0/5/F/05FF69ED-6F8F-4357-863B-12E27D6F1115/Hosted%20Services%20Comparison%20Whitepaper%20-%20Google%20vs%20Microsoft.pdf>>.
- [Mil08] Rich Miller, Major Outage for Amazon S3 and EC2, Data Center Knowledge, 2008年2月15日 ,
<URL:<http://www.datacenterknowledge.com/archives/2008/02/15/major-outage-foramazon-s3-and-ec2/>>.
- [Mil09] Rich Miller, Lightning Strike Triggers Amazon EC2 Outage, Data Center Knowledge, 2009年6月11日 , <URL:

-
- <http://www.datacenterknowledge.com/archives/2009/06/11/lightning-strike-triggersamazon-ec2-outage/>>.
- [Mod08] Austin Modine, Downed Salesforce Systems Slow Europe and US, The Register, 2008年2月11日, <URL:http://www.theregister.co.uk/2008/02/11/salesforce_outages_feb_2008/>.
- [MRG10] Online Banking: Browser Security Project, Malware Research Group, Zorin Nexus Ltd., 2010年6月, <URL: <http://malwareresearchgroup.com/wpcontent/uploads/2009/01/Online-Banking-Browser-Security-Project-June-201013.zip>>.
- [Nav10] Eliminating the Data Security and Regulatory Concerns of Using SaaS Applications, White Paper, Navajo Systems, 2010年1月, <URL:http://www.navajosystems.com/media/Virtual_Private_SaaS_White_Paper.pdf>.
- [Obe08a] Jon Oberheide, Evan Cooke, Farnam Jahanian, Empirical Exploitation of Live Virtual Machine Migration, Black Hat Security Conference, Washington, DC, 2008年2月, <URL: <http://www.blackhat.com/presentations/bh-dc-08/Oberheide/Whitepaper/bh-dc-08-oberheide-WP.pdf>>.
- [Obe08b] Jon Oberheide, Evan Cooke, Farnam Jahanian, CloudAV: N-Version Antivirus in the Network Cloud, USENIX Security Symposium, Association, San Jose, CA, 2008年7月28日から8月1日まで, <URL: <http://www.eecs.umich.edu/fjgroup/pubs/usenix08-cloudav.pdf>>.
- [Orm07] Tavis Ormandy, An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments, 2007年, <URL: <http://taviso.decsystem.org/virtsec.pdf>>.
- [Ove10] Stephanie Overby, How to Negotiate a Better Cloud Computing Contract, CIO, 2010年4月21日, <URL:http://www.cio.com/article/591629/How_to_Negotiate_a_Better_Cloud_Computing_Contract>.
- [Pea09] Siani Pearson, Taking Account of Privacy When Designing Cloud Computing Services, International Conference on Software Engineering (ICSE) Workshop on Software Engineering Challenges of Cloud Computing, Vancouver, Canada, 2009年5月23日
- [Pon10] Larry Ponemon, Security of Cloud Computing Users, Ponemon Institute, 2010年5月12日, <URL: http://www.ca.com/files/IndustryResearch/security-cloud-computingusers_235659.pdf>.
- [Pro07] Niels Provos, Dean McNamee, Panayiotis Mavrommatis, Ke Wang, Nagendra Modadugu, The Ghost in the Browser: Analysis of Web-based Malware, Hot Topics

-
- in Understanding Botnets (HotBots), 2007年4月10日, Cambridge, Massachusetts, <URL:
http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf>.
- [Pro09] Niels Provos, Moheeb Abu Rajab, Panayiotis Mavrommatis, Cybercrime 2.0: When the Cloud Turns Dark, Communications of the ACM, 2009年4月
- [Rag09] Steve Ragan, New Service Offers Cloud Cracking for WPA, The Tech Herald, 2009年12月8日, <URL:<http://www.thetechherald.com/article.php/200950/4906/New-service-offers-cloudcracking-for-WPA>>.
- [Rap09] J.R. Raphael, Facebook Privacy Change Sparks Federal Complaint, PC World, 2009年2月17日, <URL:
http://www.pcworld.com/article/159703/facebook.html?tk=rel_news>.
- [Ref10] Security Within a Virtualized Environment: A New Layer in Layered Security, White Paper, Reflex Security, retrieved 2010年4月23日, <URL:<http://www.vmware.com/files/pdf/partners/security/security-virtualizedwhitepaper.pdf>>.
- [Ris09] Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage, Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds, ACM Conference on Computer and Communications Security, 2009年11月, <URL:<http://cseweb.ucsd.edu/~hovav/dist/cloudsec.pdf>>.
- [Row07] Brent R. Rowe, Will Outsourcing IT Security Lead to a Higher Social Level of Security?, Research Triangle Institute International, 2007年7月, <URL:<http://weis2007.econinfosec.org/papers/47.pdf>>.
- [Sar10] David Sarno, Los Angeles Police Department Switch to Google E-mail System Hits Federal Roadblock, Los Angeles Times, 2010年11月3日, <URL:<http://articles.latimes.com/2010/nov/03/business/la-fi-google-la-20101103>>.
- [Sch00] Bruce Schneier, Crypto-Gram Newsletter, Software Complexity and Security, 2000年3月15日, <URL: <http://www.schneier.com/crypto-gram-0003.html#8>>.
- [Sch10] Jeff Schnepper, Don't Like the Tax Law? Don't Shoot the IRS, MSN, 2010年3月10日, <URL:http://articles.moneycentral.msn.com/Taxes/blog/page.aspx?post=1692029&_blg=1,1619827>.
- [Sha02] Adi Shamir, Cryptography: State of the Science, 2002 ACM Turing Lecture, <URL:<http://awards.acm.org/citation.cfm?id=0028491&srt=year&year=2002&aw=140&ao=AMTURING&yr=2002>>.

-
- [Sha08] Amit Shah, Kernel-based Virtualization with KVM, Linux Magazine, issue 86, 2008年1月, <URL: http://www.linuxmagazine.com/w3/issue/86/Kernel_Based_Virtualization_With_KVM.pdf>.
- [Sec05] VMware Vulnerability in NAT Networking, BugTraq, SecurityFocus, 2005年12月21日, <URL: <http://www.securityfocus.com/archive/1/420017> and <http://www.securityfocus.com/bid/15998/>>.
- [SECS09] Professional Services Contract, SAAS E-Mail & Collaboration Solution (SECS), City of Los Angeles, 2009年11月10日, <URL:https://sites.google.com/a/lageecs.lacity.org/la-geecs-blog/home/faqs-1/C-116359_c_11-20-09.pdf?attredirects=0&d=1>
- [She05] Tim Shelton, Remote Heap Overflow, ACSSEC-2005-11-25 - 0x1, <URL: <http://packetstormsecurity.org/0512-advisories/ACSSEC-2005-11-25-0x1.txt>>.
- [Sla09] Marco Slaviero, BlackHat Presentation Demo Vids: Amazon, part 4 of 5, AMIBomb, 2009年8月8日, <URL: <http://www.sensepost.com/blog/3797.html>>.
- [Sob06] Charles H. Sobey, Laslo Orto, and Glenn Sakaguchi, Drive-Independent Data-Recovery: The Current State-of-the-Art, IEEE Transactions on Magnetics, 2006年2月, <URL: <http://www.actionfront.com/whitepaper/Drive%20Independent%20Data%20Recovery%20TMRC2005%20Preprint.pdf>>.
- [Sto02] Gary Stoneburner, Alice Goguen, and Alexis Feringa, Risk Management Guide for Information Technology Systems, SP 800-30, NIST, 2002年7月, <URL: <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>>.
- [Sto10] Jon Stokes, EMC's Atmos Shutdown Shows Why Cloud Lock-in Is Still Scary, Ars Technica, 2010年7月, <URL: <http://arstechnica.com/business/news/2010/07/emcsatmos-shutdown-shows-why-cloud-lock-in-is-still-scary.ars>>.
- [Sut09] John D. Sutter, Twitter Hack Raises Questions about 'Cloud Computing', CNN, 2009年7月16日, <URL: <http://edition.cnn.com/2009/TECH/07/16/twitter.hack/>>.
- [UCG10] Cloud Computing Use Cases White Paper, Version 4.0, Cloud Computing Use Case Discussion Group, 2010年7月2日, <URL:http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf>.
- [Val08] Craig Valli, Andrew Woodward, The 2008 Australian Study of Remnant Data Contained on 2nd Hand Hard Disks: The Saga Continues, The 6th Australian Digital Forensics Conference, Perth, Western Australia, 2008年12月1日から3日まで, <URL: <http://conferences.secau.org/proceedings/2008/forensics/Valli%20and%20Woodward%202008%20remnant%20Data%20saga%20continues.pdf>>.

-
- [Vaq09] Luis M. Vaquero¹, Luis Rodero-Merino¹, Juan Caceres, Maik Lindner, A Break in the Clouds: Towards a Cloud Definition, Computer Communication Review (CCR) Online, Short technical Notes, 2009年1月, <URL:<http://ccr.sigcomm.org/online/files/p50-v39n11-vaqueroA.pdf>>.
- [Vie09] Kleber Vieira, Alexandre Schuster, Carlos Westphall, Carla Westphall, Intrusion Detection Techniques in Grid and Cloud Computing Environment, IT Professional, IEEE Computer Society, 2009年8月26日
- [Vmw09] VMware Hosted Products and Patches for ESX and ESXi Resolve a Critical Security Vulnerability, VMware Security Advisory, VMSA-2009-0006, <URL:<http://www.vmware.com/security/advisories/VMSA-2009-0006.html>>.
- [Vmw10] VMware vShield: Virtualization-Aware Security for the Cloud, product brochure, 2010年, <URL:http://www.vmware.com/files/pdf/vmware-vshield_br-en.pdf>.
- [Wai08] Phil Wainwright. Many Degrees of Multi-tenancy, ZDNET News and Blogs, 2008年6月16日, <URL: <http://blogs.zdnet.com/SAAS/?p=533>>.
- [Wal10] Hannah Wald, Cloud Computing for the Federal Community, IANewsletter, Vol. 13, No. 2, Information Assurance Technology Analysis Center, 2010年春.
- [Wei09] Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, Vasanth Bala, Peng Ning, Managing Security of Virtual Machine Images in a Cloud Environment, ACM Cloud Computing Security Workshop (CCSW'09), Chicago, Illinois, 2009年11月13日
- [Whi09] Lance Whitney, Amazon EC2 Cloud Service Hit by Botnet, Outage, 2009年12月11日, CNET News, <URL: http://news.cnet.com/8301-1009_3-10413951-83.html>.
- [Wil10] Matt Williams, All Eyes are on Los Angeles as City Deploys Cloud-Based E-Mail, Government Technology, 2010年2月10日, <URL: http://www.govtech.com/gt/744804?id=744804&full=1&story_pg=1>.
- [Xen08] Xen Architecture Overview, Version 1.2, Xen Wiki Whitepaper, 2008年2月13日, <URL:http://wiki.xensource.com/xenwiki/XenArchitecture?action=AttachFile&do=get&target=Xen+Architecture_Q1+2008.pdf>.
- [You07] Greg Young, Neil MacDonald, John Pescatore, Limited Choices are Available for Network Firewalls in Virtualized Servers, Gartner, Inc., ID Number: G00154065, 2007年12月20日, <URL: <http://www.reflexsystems.com/Content/News/20071220-GartnerVirtualSecurityReport.pdf>>.
- [You08] Lamia Youseff, Maria Butrico, Dilma Da Silva, Toward a Unified Ontology of Cloud Computing, Grid Computing Environments Workshop (GCE08), held in conjunction

with SC08, 2008 年 11 月 , <URL:
<http://www.cs.ucsb.edu/~lyouseff/CCOntology/CloudOntology.pdf>>.

[Zet09a] Kim Zetter, FBI Defends Disruptive Raids on Texas Data Centers, Wired Magazine, 2009年4月7日,
<URL: <http://www.wired.com/threatlevel/2009/04/data-centers-ra/>>.

[Zet09b] Kim Zetter, Bank Sends Sensitive E-mail to Wrong Gmail Address, Sues Google, Wired Magazine,
2009年9月21日, <URL: <http://www.wired.com/threatlevel/2009/09/bank-sues-google/>>.

付録 A 一略語

CAPTCHA	キャプチャ (Completely Automated Public Turing test to tell Computers and Humans Apart)
CRM	顧客関係管理 (Customer Relationship Management)
FISMA	連邦情報セキュリティマネジメント法 (Federal Information Security Management Act)
FOIA	情報公開法 (Freedom of Information Act)
FTP	ファイル転送プロトコル (File Transfer Protocol)
HIPAA	医療保険の携行性と責任に関する法律 (Health Insurance Portability and Accountability Act)
HVAC	暖房、換気、および空調 (Heating, Ventilation, and Air Conditioning)
IA	情報保証 (Information Assurance)
IaaS	IaaS (Infrastructure as a Service)
MX	メールエクスチェンジ (Mail eXchange)
NARA	米国国立公文書館 (National Archives and Records Administration)
NAT	ネットワークアドレス変換 (Network Address Translation)
OMB	行政管理予算局 (Office of Management and Budget)
PaaS	PaaS (Platform as a Service)
PCI DSS	クレジットカード業界のデータセキュリティ基準 (Payment Card Industry Data Security Standard)
PII	個人情報 (Personally Identifiable Information)
SaaS	SaaS (Software as a Service)
SAS	監査基準書 (Statement on Auditing Standards)
SECS	SECS (SaaS E-mail and Collaboration Solution)
SAML	エスエーエムエル (Security Assertion Markup Language)
SLA	サービス内容合意 (Service Level Agreement)
SOAP	シンプルオブジェクトアクセスプロトコル (Simple Object Access Protocol)
WPA	ワイファイプロテクトドアクセス (WiFi Protected Access)
XACML	拡張アクセスコントロールマークアップ言語 (eXtensible Access Control Markup Language)
XML	拡張マークアップ言語 (eXtensible Markup Language)

付録 B – オンライン参考文献

下記の表は、セキュリティの専門家をはじめとする本文書の読者にとって、クラウドコンピューティングのセキュリティおよびプライバシー問題への理解を深めるために役立つであろう。

参考文献の内容	URL
Top Threats to Cloud Computing, V1.0, Cloud Security Alliance, 2010年3月	http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
<i>Security Guidance For Critical Areas of Focus in Cloud Computing</i> , V2.1, Cloud Security Alliance, 2009年12月	http://www.cloudsecurityalliance.org/csaguide.pdf
<i>Cloud Computing Risk Assessment</i> , European Network and Information Security Agency, 2009年11月	http://www.enisa.europa.eu/act/m/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport
<i>The Future of Cloud Computing</i> , Version 1.0, Commission of the European Communities, Expert Group on Cloud Computing, 2010年1月	http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-reportfinal.pdf