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

NIST 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

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 12 月

米国商務省　長官代理

Rebecca M. Blank

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。

米国国立標準技術研究所、Special Publication 800-144、80 頁
(2011 年 12 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。

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の解釈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、データとサービス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

謝辞

本文書の著者である Wayne Jansen（Booz Allen Hamilton）と Tim Grance（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れた同僚たちに、また、本文書の一般公開ドラフトをレビューし、レビュー期間内に意見を寄せてくれた方々に感謝の意を表する。とりわけ、Erika McCallister 氏（NIST）はプライバシーがクラウドコンピューティングに関連することから、プライバシーという問題についての知識を提供しくださり、Tom Karygiannis 氏と Ramaswamy Chandramouli 氏（両者とも NIST）は早期ドラフトにおいてクラウドセキュリティに関する情報を提供してくださった。また、我々の内部レビュー作業を支援してくれた Kevin Mills 氏と Lee Badger 氏にも感謝の意を表する。こうした方々の意見と貴重な提案がなかったなら、本文書に対する主な改善は成し得なかったであろう。

目次

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[Mel11]。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。これには、そのインフラとコンピューティングリソースの外部所有者と運営者が、それらのサービスを複数テナントのプラットフォームを介して一般向けに提供するときの、パブリッククラウドが直面するセキュリティ上の課題が含まれる。

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。本文書は、特定のクラウドコンピューティングサービス、サービスアレンジメント、サービス契約、サービスプロバイダ、または実装モデルの利用を規定または推奨するわけではない。むしろ、各組織には、組織の要求事項を分析する際に本文書が示すガイドラインを適用し、それらの要求事項を最もよく満たすパブリッククラウドサービスを評価、選択、採用、監視することが推奨される。

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

パブリッククラウドコンピューティングは、大きなパラダイムシフトを引き起こし、従来の規範である組織のデータセンタの枠を超えて組織のインフラの境界を組み替えるため、悪意のある者によって利用されやすいといえる。 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、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。組織は、利用できるセキュリティおよびプライバシーオプションの分析と、組織の機能をクラウド環境に移行すべきか否かの判断において、リスクに基づくアプローチを取るべきである。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、利用、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、初期の計画作成段階から始まり、そのシステムのライフサイクル全体を通してセキュリティとプライバシーが考慮されなければならない。システムの導入・展開後にセキュリティとプライバシーの問題に取り組むことは、はるかに困難であり費用も高くなるばかりか、組織を不必要なリスクに晒すことになる。

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すること

組織とクラウドプロバイダの双方の責任は、利用するサービスモデルによって異なる。クラウドサービスを利用する組織は、コンピューティング環境に対する責任の分担と、セキュリティおよびプライバシー関連の影響について理解しなければならない。セキュリティまたはプライバシー関連の主張をサポートするためにクラウドプロバイダによって提供される保証、あるいは、クラウドプロバイダから委託された認証・コンプライアンスレビュー機関によって提供される保証は、可能な場合には常に、組織による独立したアセスメントを通じて検証されるべきである。

クラウドプロバイダによって使用されるポリシー、手順、および技術的管理策について理解することは、関連するセキュリティおよびプライバシー関連リスクをアセスメントするうえで必要不可欠である。サービスを提供するために使用される技術と、そのシステムのセキュリティおよびプライバシー関連の影響を理解することも重要である。クラウドのシステム構成の詳細を分析し、その分析結果をセキュリティおよびプライバシー管理策によってもたらされる保護の全体像を得るために使用することができる。そうすることで、リスクを的確に評価し管理するための組織の能力（そのシステムのセキュリティ状態を継続的にモニタリングするための適切な技法と手順を採用することによるリスク軽減を含む）が向上する。

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求事項を満たすことを確認すること

パブリッククラウドプロバイダが提供する標準のサービスは、通常、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反映しない。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必要である。組織が要求する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が、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、違反についての通知、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、法規制の遵守、連邦政府または国家の標準（例：FIPS 140）を

満たす製品の利用などが含まれる。交渉による契約も、組織の要求条件が満たされていることを裏付けるためにクラウドプロバイダが提供しなければならない保証を記載することがある。

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、組織内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可能性があり、プラットフォームリソースを共有できるユーザの種類をより厳密に限定し、管理策に不備があったり、設定に誤りがあった場合にも露出を減らすことができる。

クラウドプロバイダの数が増え、選択可能なサービスの範囲も広がることを踏まえると、組織が機能を選択し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。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。政府機関によって扱われるデータの機微度と、現在の最先端技術を考慮すると、すべての IT サービスをパブリッククラウドにアウトソーシングする可能性は低いと考えられる。しかしながら、ほとんどの政府機関にとって、必要なすべてのリスク軽減対策が実施されるならば、IT サービスの一部をパブリッククラウドに実装する可能性は否定できないだろう。

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求事項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。異なるクラウドプロバイダが提供するサービス、および組織が開発するクラウドベースのアプリケーションが、より厳しい要求をクライアント側に課すことが考えられる。その場合、考慮されるべきセキュリティおよびプライバシー関連に影響するだろう。

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。一方、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。

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。また、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。さらに、クラウドアプリケーションはウェブブラウザではなく、特注のネイティブアプリケーション（すなわち、アプリ）を介して利用者に提供されることが多い。

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、1つの懸念材料である。なぜなら、それらはソーシャルエンジニアリング攻撃の手段として利用されることが多く、そのような場合には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、パブリッククラウドサービスだけでなく、インターネット経由で利用できるその他のパブリックサービスのセキュリティとプライバシー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、既存のセキュリティおよびプライバシー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果たすこと

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、管理策、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。

組織は、それぞれのレベル（すなわち、ガバナンスレベル、任務または業務プロセスレベル、および情報システムレベル）で、そのシステムの状態について得られるデータを定期的に、かつセキュリティおよびプライバシー関連リスクを管理するのに必要な頻度で収集・分析すべきである。[Dem10]。情報セキュリティの継続的なモニタリングでは、プライバシーおよびセキュリティ管理策、脆弱性、および脅威についての意識を持ち続けることによってリスク管理上の意思決定をサポートすることが求められる。その目的は、組織のネットワーク、情報、およびシステムのセキュリティの継続的なモニタリングを実施し、状況の変化に応じてリスクを受け入れる、または回避する、もしくは軽減することによって対処することにある。

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。なぜならば、コンピューティング環境のかなりの部分がクラウドプロバイダの管理下に置かれるため、組織の管理外となる可能性が高いからである。リスクの分析では、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ず、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[JTF10]。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。

クラウドコンピューティングは、その多くの構成要素の各々のセキュリティに依存する。一般的なコンピューティングのためのコンポーネントの他に、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、サービスレベルのモニタリング、作業負荷管理など）を構成するコンポーネントがある。クラウドコンピューティングが提供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根底にある複雑さを覆い隠す。組織は、実現可能な範囲で、クラウドコンピューティングの構成要素のすべてがセキュアであり、健全なコンピューティング実践規範（FIPS および NIST Special Publications に記載されているものを含む）に基づいてセキュリティとプライバシーが維持されていることを確実にしなければならない。以下の表に記載されている標準およびガイドは、クラウドコンピューティングに特に関連する資料であり、本文書と併せて使用することが推奨される。

刊行物	タイトル
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems
SP 800-18	Guide for Developing Security Plans for Federal Information Systems
SP 800-34, Revision 1	Contingency Planning Guide for Federal Information Systems
SP 800-37, Revision 1	Guide for Applying the Risk Management Framework to Federal Information Systems
SP 800-39	Managing Information Security Risk
SP 800-53, Revision 3	Recommended Security Controls for Federal Information Systems and Organizations
SP 800-53, Appendix J	Privacy Control Catalog
SP 800-53A, Revision 1	Guide for Assessing the Security Controls in Federal Information Systems
SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories
SP 800-61 Revision 1	Computer Security Incident Handling Guide
SP 800-64, Revision 2	Security Considerations in the System Development Life Cycle
SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
SP 800-88	Guidelines for Media Sanitization
SP 800-115	Technical Guide to Information Security Testing and Assessment
SP 800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
SP 800-137	Information Security Continuous Monitoring for Federal Information Systems and Organizations

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とデータ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。本文書は、特定のクラウドコンピューティングサービス、サービスアレンジメント、サービス契約、サービスプロバイダ、または実装モデルの利用を規定または推奨するわけではない。各組織は、組織のニーズの分析と、それらのニーズを最もよく満たすパブリッククラウドサービスの評価、選択、採用、監視を行わなければならない。

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基本的な専門知識と、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、結論を手短に述べる。
- **第 7 章**では、参考文献の一覧を示す。

本文書の主部全体を通して、主題に関連する補足資料を含む補足記事が灰色のテキストボックスに囲まれて記載されている。本文書の末尾には、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 にはインターネット上で入手可能な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[Mel11]。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、高い関心を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、まだ進化と標準化の段階にある。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実装と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る。

2.1 実装モデル

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[Mel11]。実装モデルは、サービスを利用者に提供するためのコンピューティングリソースの管理および廃棄について、また、異なるクラスの利用者間の差別化について大まかな特性を示すものである。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利用者に提供するクラウドプロバイダが所有者かつ運営者であり、その定義上必然的に、利用者の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単一の組織のためだけに運用される。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、およびクラウドの利用者に対するコントロールが組織に与えられる可能性がある。

他の2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、その対象となる利用者の観点から、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。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の専用となる。[1] 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）の組み合わせであるため、他の実装モデルよりも複雑で

[1] 本文書全体を通して「組織」という用語は、「クラウドユーザ」の同意語として使用されている。

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、それらのクラウド間のアプリケーションとデータの移動可能性を実現している。

選択される実装モデルによってそのシステムに対するセキュリティとプライバシー関連の影響が変わってくるが、実装モデル自身が特定のクラウドサービスのセキュリティとプライバシーのレベルを決定づけるわけではない。そのレベルは、例えばセキュリティおよびプライバシーに関するポリシーの健全性、セキュリティおよびプライバシー管理策の堅牢性、およびクラウド環境のパフォーマンスとマネジメントについての詳細を利用者がどの程度把握できるかといった、保証によるところが大きい。そうした保証は、クラウドプロバイダによって提供されるか、あるいは組織が例えば自主的な脆弱性テストまたは運用監査によって単独で取得する。

2.2 サービスモデル

実装モデルがクラウドコンピューティングにおいて重要な役割を担うように、サービスモデルも重要な考慮事項となる。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、および利用に際しての抽象化のレベルは、そのクラウドが提供するサービスモデルによって異なる。サービスモデルは、パブリッククラウドとして、あるいはその他の実装モデルのいずれかとして実現することができる。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, Mel11, 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、サービス提供モデルの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。クラウドユーザは、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、サービス提供モデルの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。クラウドユーザは、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、サービス提供モデルの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、クラウドユーザは 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、クラウドユーザ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ユーザ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、「ファシリティ」レイヤのすぐ上にある「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、仮想ネットワーク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、ミドルウェア、ならびにアプリケーションの実装と提供に必要なその他のソフトウェアツールおよび開発コンポーネント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。

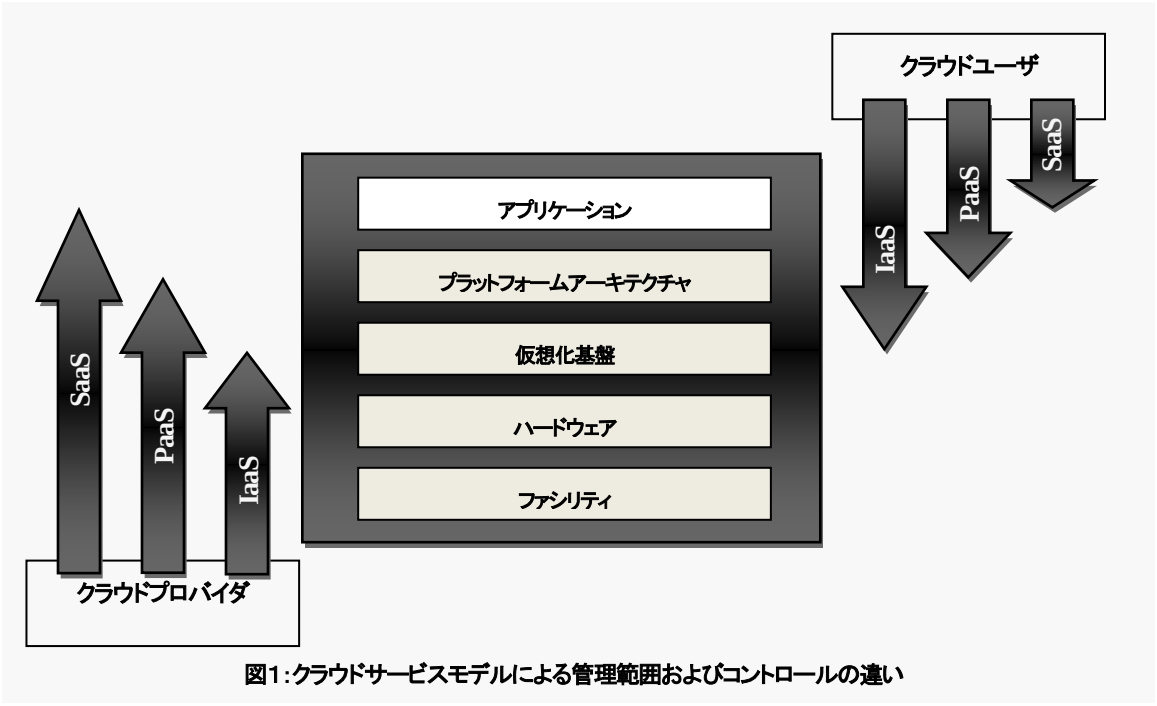

図1：クラウドサービスモデルによる管理範囲およびコントロールの違い

IaaS サービスモデルと PaaS サービスモデル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]。とはいうものの、「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 ではクラウドユーザ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。

2.3 アウトソーシングおよび説明責任

クラウドコンピューティングは特定の組織専用に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、本来の目的は組織のコンピュータ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し使用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は大きく 3 つのクラスに分類される。1 つ目のクラスは、利用者に無料で提供され、広告によって支えられるサービスである。よく知られている例としては、検索サービスや電子メールサービスがある。そうしたサービスは、個人的で、かつ営利を目的としない利用に限定されるだろう。サービスの登録時および使用中に収集された情報は、その他のソースから得た情報と結合され、個人向け広告を利用者に送るために使用される可能性がある。サービスとのやりとりを暗号化するなどの保護対策も実施されない可能性がある。2 つ目のクラスは、有料で広告などは送られてこないサービスである。このクラスのサービスは 1 つ目のクラスのサービスに似ているが、サービス提供に関する条項が交渉可能でないことと、それらの条項がクラウドプロバイダ側の自由裁量で一方的に変更されえるといった特徴があり、このため利用者には低価格でサービスが提供される。通常は、1 つ目のクラスのものよりも優れていて、利用者が設定できる保護メカニズムが提供される。3 つ目のクラスは、有料で、サービス条項が組織とクラウドプロバイダの間で交渉できるサービスである。こうしたサービスは組織のニーズに合わせて調整が可能であるが、コストは、通常はクラウドプロバイダによって提供される交渉の余地のない有料のサービスからどの程度逸れるかによって変わってくる。

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放棄するための移行であってはならない。最終的に、組織は、パブリッククラウドの選択と、アウトソーシングしたサービスのセキュリティとプライバシー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、パフォーマンスやデータのプライバシー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、組織の本来の目的、保有する資産、法律上の義務、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、プライバシーおよび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およびプライバシー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考える組織が多く、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)、機微度(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およびプライバシー目的を頭に入れ、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の分析に基づいて行われることになる。[2]

3.1 サービス契約

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、サービス契約と呼ばれる。サービス契約は、クラウドプロバイダによって提供されるサービスへのアクセスと利用に関する諸条件を定義する。サービス契約は、また、サービスの有効期間、終了のための条件、終了に伴うデータの廃棄(例:保存期間)も規定する。クラウドのサービス契約の諸条件一式は、通常、複数のドキュメントに明記されている。そうした文書には、通常、サービス内容合意書(SLA)、プライバシーポリシー、利用規定、および利用規約が含まれる[Bra10]。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。プライバシーポリシーは情報の取り扱いに関する実践規範と、利用者の情報がクラウドプロバイダによってどのように収集、利用、管理されるかを文書化したものであり、利用規定は利用者側の禁止されている行為を規定するものである。利用規約は、サービスの使用許可、責任制限、契約条項の変更規定など、他の重要な細目を取り扱う。プライバシーおよびセキュリティ関連のリスクは、サービス契約に規定されている諸条件に大きく左右される。

サービス契約には、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

[2] リスクの分析を実施し、リスクを管理するためのプロセスは、本文書では扱っていない。詳細な情報は、NIST SP 800-30『Risk Management Guide for Information Technology Systems』とSP 800-37 Revision 1『Guide for Applying the Risk Management Framework to Federal Information Systems』を参照のこと。これらは http://csrc.nist.gov/publications/PubsSPs.html から入手できる。

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方的に定められる。通常、サービス条項はプライバシーおよびセキュリティに関する連邦政府の要求事項を考慮して書かれていない[CIO10a]。さらに、サービスによっては、利用者に直接通知することなく、クラウドプロバイダが一方的にサービス条項を変更する場合がある（例：インターネット上に更新版が掲示されるだけ）[Bra10]。

交渉可能なサービス契約は、従来型の IT サービスアウトソーシング契約に近い。交渉可能なサービス契約では、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、違反についての通知、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、法規制の遵守（例：FISMA）、国家標準または国際標準（例： FIPS 140-2）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、交渉可能なサービス契約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、交渉の余地のないサービス契約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、交渉可能なサービス契約は交渉の余地のないサービス契約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。サービス契約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も推奨される。

3.2 セキュリティおよびプライバシーに関する利点

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の１つ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の提供に技術革新の機会をもたらし、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る小さな組織であるといえるだろう。そうした組織もパブリッククラウドに移行することによって、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ることができる。

セキュリティが向上すれば、プライバシーもその恩恵を受ける。すなわち、情報セキュリティのしっかりした土台がなければ、効果的なプライバシーはありえない。しかしながら、セキュリティ同様にプライバシーも、組織、運用、技術面で幅広い影響をもたらす。プライバシーには、セキュリティにおける機密性、完全性、可用性の目的に密接に関連している側面とそうでない側面がある。後者は、むしろ、法律、規制、および OMB のガイダンスで取り扱われている重要なプライバシー関連の原則と、考慮すべき事項に関連する。[CIO10b]

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およびプライバシー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他の組織と同様に、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およびプライバシー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、自身の経験と訓練を深め、是正措置を実施し、セキュリ

ティおよびプライバシーを向上させる機会を、より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。同様に、基盤の同一性は、プライバシーを保護するために採用されている管理面での管理策にも恩恵をもたらす。その一方で、同一性は、単一の欠陥がクラウド全体にわたる欠陥となり、すべての利用者とサービスが影響を受ける可能性があることを意味する。クラウドコンピューティング環境の多くが、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))、セキュリティ分野における、ISO 27001, 情報セキュリティマネジメントシステム - 要求事項 (Information Security Management Systems - Requirements)、会計監査における、監査証明契約に関する基準 No. 16 (Standards for Attestation Engagements (SSAE) No. 16) が挙げられる。また、（クラウドプロバイダが）一般に受け入れられ認められているなんらかの基準に沿ったレベルの保証を提供するために、独立した第三者から公式の保証書または証明書を取得している場合もある。

- **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、攻撃を阻止すると同時に、実稼働環境に影響を与えずにより詳細なイベント情報を即座に取得することが可能になる。可用性は、また、個人が記録にアクセスしたり、記録を訂正する機会を増加させ、記録収集時の目的を果たし必要な時にすぐに利用できるようにするため、プライバシーも向上させる[CIO10b]。しかしながら、場合によっては、そのような耐障害性と機能があだとなることがある。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、そうした状況で増加した使用に対する料金が課せられた場合、組織にとっては金銭上の損失となることが考えられる。大量の安価なストレージにアクセスする場合、情報が必要以上に収集されたり、必要以上に長く保持される可能性がある。

- **バックアップおよびリカバリ (Backup and Recovery)。**クラウドプロバイダ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、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、信頼性も高いうえに、オフサイトバックアップストレージの要求事項や地理的分散についての遵守要求も満たす。したがって、組織のデータセンタのためのオフサイトリポジトリとして、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は、汎用のウェブブラウザであったり、より特殊な用途のアプリケーションであったりする。クラウドベースのアプリケーションにとって必要なコンピューティングリソースの主なものは、通常はクラウドプロバイダが保有するため、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、スマートフォンやタブレットなど組み込みデバイスでも利用できる。このため、外勤職員が多い組織では、生産性が向上する。[3] この点に関して注意が必要なのは、携帯機器、とりわけ組み込みデバイスは、適切なセットアップと保護(そのデバイスに保管されるデータの種類に対する制限を含む)がなされなければ、全体的なメリットが得られないと点である[Jan08]。

- **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、データをパブリッククラウドで保管・処理する方が、同じデータをポータブルコンピューター、組み込みデバイス、または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、日常的に発生する盗難や紛失の可能性を排除できるからである。だからといって、データが集中管理される場合にリスクがまったくないというわけではない。[4] 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と、生産性の面での利益を得ることを目的として、自組織のデータに携帯機器からアクセスできる変更を実施している。慎重に構築されたアプリケーションは、ユーザが果たすべき責任に厳密に対応するデータとタスクにのみ、アクセスとサービスの利用を許可する。これにより、デバイスが侵害された場合のデータの露出を制限できる。

3.3 セキュリティおよびプライバシー上のデメリット

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、攻撃の矢面が広くなる。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、サービスレベルのモニタリング、作業負荷管理、およびクラウドバ

[3] 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。

[4] 次章で論じている関連するリスクを参照のこと。

ースト[5]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。クラウドプロバイダの専有であることが多いアプリケーションプログラミングインターフェースを理解しセキュリティを確保することは、困難を伴う。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も増す[Avo00, Gee08, Sch00]。セキュリティが低下すると、個人情報の喪失または正規の権限によらないアクセス、破壊、利用、変更、開示に関連するプライバシーリスクも高まる。

- **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。クラウドコンピューティングは、リソースの物理的な分離を管理策として用いるのではなく、アプリケーションスタックの複数のレイヤにおける論理的な分離に大きく依存する[Owa10]。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（例：[Bos11]）。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、分離メカニズムを回避し、不正アクセスを行う可能性もある。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、あるいは正規のユーザであっても遮断されることがある。

  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要となる。

- **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し管理することを可能にする管理インターフェースと、提供されるサービスにアクセスすることを可能にする非管理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。[6] 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

[5] 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。

[6] インターネットを利用した脅威を軽減するために推奨されるソリューションがある。これには、NIST SP 800-119『Guidelines for the Secure Deployment of IPv6』(http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf;)、SP 500-267『A Profile for IPv6 in the U.S. Government−Version 1.0』(http://www.antd.nist.gov/usgv6/usgv6-v1.pdf)、および SP 800-77『Guide to IPsec VPNs』(http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf)が含まれる。それらのソリューションの実施には、クラウドプロバイダのサポートが必要不可欠であり、これらの刊行物が指摘しているように、誤った実施や設定

とデータをパブリック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。インターネットを介して提供されるサービスのパフォーマンスと質も、未解決な問題であるだろう。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。そうした場合には、安全な利用のための追加の予防措置が必要となる。

クラウド内に保有される組織の資産を管理するための手段として、管理のためのリモートアクセスに依存することは、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（例：[Som11]）。同様に、クラウド基盤に対する管理のためのリモートアクセスがクラウドプロバイダによって実施される場合も 1 つの懸念事項となる。一般の人がインターネットを介して利用できるサービスを提供する、高度に複雑で利用者が複数であるコンピュータ環境では、前述の 2 つの項目が合わさった場合、ほぼ間違いなく格好の攻撃の矢面となり、慎重な保護が必要となるだろう。

- **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責任と管理下に置きかえることが必要となる。パブリッククラウドへの移行は、通常、運用の管理とコンピューティング環境についての決定事項に対する影響に関して、直の連絡先が設けられないまま進められてしまう。こうした状況では、継続的なモニタリングやインシデント対応など、利用者組織とプロバイダの双方の責任となる活動の実施に関して、利用者組織がプロバイダからの協力に依存することになる。データの保護に関する法規制の遵守は、共同責任におけるもう1つの重要な分野であり、クラウドプロバイダとの連携と、クラウドプロバイダによる協力を必要とする。

  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。情報が第三者のサービスプロバイダによって保管される場合、プライバシーの法的保護が影響を受ける可能性がある[Cou09, Han06]。このような状況では、説明責任を果たすことはより困難となり、前述したメリットの一部が相殺される可能性がある。

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。

他の種類のクラウドサービス。セキュリティおよびプライバシーに関連する他の種類のクラウドサービスがある。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あるいは自社所有のアプリケーションの代わりを提供するが、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のセキュリティを増強するために使用することができる。

が原因でシステムが悪用される可能性がある。

- **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。異なる組織からの多くの参加者から収集したオンライン活動についての情報は、より厳密な脅威モニタリングを可能にする。例えば、電子メールをメールエクスチェンジ(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[Obe08b]。

- **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管理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。

どんな技術でも同じことが言えるが、提供される機能が不適切または不正な行為に利用される可能性がある。クラウドコンピューティングも例外ではない。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[Mul10]。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[Mul10, 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 に、IaaS クラウド上で稼働中の司令塔(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[Cra08, 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テッドアクセス)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、暗号を解読し、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突き止める。このサービス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 分で終え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。過去に、あるオンラインゲームのネットワークに対してIaaSクラウドを利用した攻撃が行われ、1億人以上のユーザのアカウントが侵害されたという事例があった[Alp11]。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際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。[7]

[7] CAPTCHA (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、パブリッククラウドコンピューティング、そして多くの場合、他のクラウドコンピューティングサービスモデル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関連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。それらの事例は、包括的であるわけではなく、より一般的な課題の1つの側面のみ扱う場合がある。また、それらの課題の多くについて、論じられた具体的な問題はすでに解決されている。しかしながら、大抵の場合、より広範な課題が残っていて、さまざまなサービスモデルにおいて他の方法で再度述べられる可能性がある。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も存在する。そうした問題については、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、この新しい形において、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。パブリッククラウドコンピューティングは、従来の規範からオープンな、境界を組み替えた組織のインフラへと、思考力を刺激するパラダイムシフトを引き起こす。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も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、組織による、アプリケーションの開発と IT サービスの提供に関するポリシー、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、または稼働中のサービスの設計、実施、テスト、利用、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が容易であるが、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がもたらされる。

クラウドコンピューティングのメリットの一つに、コンピューティングリソースに対する資本投資を減らして運営経費に形を変えてコンピュータ処理関連のニーズを満たす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、投資に対する明白な利益を得るのに必要な時間を短縮するため（すなわち、価値実現までの時間短縮を促進する）、実際の利用に対応した支出にすることができる。[8] 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ために、組織が使用する正規のプロセスと手順を部署や個人が無視してしまい、リソースの調達を日常的な運営経費なみの扱いにかいくぐらせてしまう

[8] 多くの事業主は税金やその他の金銭上の考慮から、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。）。

可能性がある。[9] 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、使用、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、利用者組織とクラウドプロバイダ間の関連する役割と責任、とりわけリスクの管理と、組織の要求事項が満たされることを確実にすることに関して、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

コンプライアンスとは、定められた法律、規制、標準、仕様に従って運営するといった、組織側の責任のことをいう。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。例えば、2010 年の年末、全米州議会議員連盟は、46 の州が個人情報に対するセキュリティ違反の開示に関する法律を制定し、少なくとも 29 の州が事業者および／または政府によって保有される個人情報の廃棄に関する法律を制定したと報告した。[10]

- **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 年施行の電子政府法および添付のOMBガイダンス、ならびに 2002 年施行の連邦政府情報セキ

[9] 連邦政府における不適切かつ不正な購入を防ぐには、警戒を解かないことが求められる。例えば、米国政府説明責任局による『Government-wide Purchase Cards : Actions Needed to Strengthen Internal Controls to Reduce Fraudulent, Improper, and Abusive Purchases』に関するレポート（http://www.gao.gov/new.items/d08333.pdf）を参照のこと。

[10] 詳細については、『Issues & Research on Telecommunications & Information Technology（at http://www.ncsl.org/）』を参照のこと。

ュリティ管理法 (Federal Information Security Management Act (FISMA))が含まれる。[11]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。A-130 の付録 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。

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、個々に割り当てられた識別子(例:名前)によって取り出すことができる個人情報の収集、保管、使用、配信について規定する。プライバシー法は、それぞれの政府機関が、記録システムからの通知 (SORN)を連邦公報に公示することと、システム内の記録と情報に対するアクセスおよび訂正依頼を個人ができるようにすることを求めている。とりわけ、2002 年施行の電子政府法は、連邦政府機関に対して、個人情報の収集、保管、または配信のための技術が新たに登場したり、既存の技術に大きな変更があった場合に、プライバシー影響評価 (PIA)を実施し、アセスメント結果を一般の人が利用できるようにすることを求めている。2002 年施行の電子政府法の M-03-22『OMB Guidance for Implementing the Privacy Provisions』は、プライバシー影響評価の実施に関する指示を政府機関に与える。プライバシー影響評価は、情報システムを構造的にレビューすることであり、システムのライフサイクルのすべての段階において機密性に対するリスクを含む、プライバシー関連リスクを特定し軽減するために利用される。プライバシー影響評価は、プログラムに携わる個人またはシステムにアクセスする個人にとって、個人情報を取り扱う際にプライバシーの保護を組み入れるための最良の方法を知るための手段にもなる。

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求事項を満たさなければならない。それらのセキュリティ要求事項は、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

[11] FISMA は、2002 年施行の電子政府法の付録 III、公法 107-347 に相当する。

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令に従って、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 規定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、保護された医療情報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サービス契約によってどの程度受けいれるかは定かでない。だとしても、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。

- **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、データが複数の物理的な所在地に格納され、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。例えば、NARA 規則（すなわち、36 CFR 1234）は、連邦記録を保管する施設に対する要求事項を含み、洪水面を起点とした最低限必要な高さと距離を規定している。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、適用される法律、プライバシー、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ある（例: [CBC04, Wei11]）。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求事項が、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]。

  情報が国境を超えた場合のコンプライアンスに関する主な懸念事項としては、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]。 これらの問題は、クラウドプロバイダが、組織のデータの保管と処理が特定の管轄区域内でのみ行われるようにする信頼できる手段を備えている場合には、緩和される。

- **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的に保管された情報(ESI)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。ESI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、利用者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、訴訟に悪影響がもたらされることも考えられる。クラウドプロバイダの電子的証拠開示能力およびプロセスが、組織のデータおよびアプリケーションのプライバシーまたはセキュリティを侵害し、他のクラウドユーザによる証拠開示義務の履行を妨げることがあってはならない。逆の場合も同じである。

4.3 トラスト

クラウドコンピュータのパラダイムでは、セキュリティおよびプライバシー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、高レベルの信認をプロバイダに与えることになる。同時に、政府機関には、その情報の収集または管理が政府機関によってなされるか、あるいは政府機関の代理となる組織によってなされるかにかかわらず、また、その情報システムの利用または運用が政府機関、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いずれによってなされるかにかかわらず、正規の権限によらないアクセス、利用、開示、中断、変更、または破壊により生じるリスクおよび被害の規模に見合った保護をシステムと情報に施す責任がある[HR2458]。

- **内部関係者によるアクセス (Insider Access)。**組織の物理的境界、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、機微な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と報じられたことがある)[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、内部関係者の範囲がクラウドプロバイダのスタッフおよび請負業者のみならず、そのサービスを利用するユーザに広がり、リスクが増大する。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[Mee09, 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に、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、信頼とデータのプライバシー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独占的な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組織の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、パブリック 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。支援サービスの可用性が低下すると、全体的な可用性も比例して低下する。

  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（例：ポリシーおよびライセンス契約）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。相手方のアプリケーションまたはサービスをホストするパブリッククラウドプロバイダは、自身のコントロール領域以外に他の領域も受け持つ可能性があるが、透過的な認証メカニズムによって利用者には、あたかもクラウドプロバイダのコントロール領域であるように見える。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)。**情報セキュリティの継続的なモニタリングでは、セキュリティ管理策、脆弱性、および脅威についての意識を持ち続けることによってリスク管理上の意思決定をサポートすることが求められる。[Dem10]。システムの状態について得られるデータの収集と分析は、意思決定に関与する組織の各レベルに適合するように定期的に、かつセキュリティおよびプライバシー関連リスクを管理するのに必要な頻度で実施されるべきである。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一部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。継続的なモニタリングの義務を果たすために、組織はクラウドプロバイダに依存する。そのコンピューティング環境がクラウドプロバイダによって完全に管理されるため、クラウドプロバイダの協力は不可欠である。

  クラウドプロバイダのセキュリティ対策について知ることも、リスクマネジメントを行う上で必要である。例えば、脆弱性を特定するプロセスは、システムのセキュリティ機能と、クラウド環境の保護に使用されるセキュリティ管理策の分析を含む[Sto02]。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対策とステータスの詳細を示すことには消極的であると考えられる。なぜなら、そうした情報は専有であるとみなされることが多く、提供された場合に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]）。通常、利用者がステータスをモニタリングする手段として、通知用ツールやウェブベースのダッシュボードが用意されているが、それらは詳細さに欠けることもあり、システムの機能が停止した場合に利用できなくなる可能性がある[Goo09a, Ker11, Per11]。

  クラウドプロバイダのオペレーション（複合型のサービスの提供を含む）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。例えば、サービス契約には、管理の諸側面を評価する手段として、第三者を介して管理状況を監査する権利を含めることができる。このような手段がなければ、利用者はそうした情報にアクセスし、評価することはできない。理想的には、利用者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、利用者がコントロールできることが望ましい。

- **二次データ (Ancillary Data)。**クラウドコンピューティングでは、主にアプリケーションデータを保護することに焦点が置かれているが、クラウドプロバイダが保有するクラウド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、その情報がクラウド基盤内に保管されているか、あるいは別の場所に保管されているかにかかわらず、保護し、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。

他の種類の二次データとして、クラウドにおける利用者の活動についてクラウドプロバイダが収集または生成する情報がある。これには、リソースの使用量を計測し料金を請求するために収集した情報、ログと監査証跡、およびクラウド環境内で生成され蓄積されたメタデータなどが含まれる。組織のデータの場合と異なり、クラウドプロバイダが収集した組織のメタデータやその他の種類のメタデータに対して所有権を主張する傾向が強いと考えられる。しかしながら、そうした情報は、組織の取り組みの状況または展望（例：ある新興企業の活動レベルまたは成長計画）を推定するのに利用されることもあり、第三者に売り渡されたり、公開されたり、漏洩した場合には、組織のプライバシーにとって脅威となる可能性がある。サービス契約の中で明確にすべきいくつかのポイントは、クラウドプロバイダによって収集されるメタデータの種類、メタデータに対してどのような保護がなされるべきか、およびメタデータに対する組織の権利（所有権、収集と配信の停止を求めること、および公正使用を含む）である。

- **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組織も多い。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、情報システムの運用により生じる組織の業務、組織の資産、または個人に対する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]。このプロセスは、リスクアセスメントの実施、リスク緩和戦略の実施、および情報システムのセキュリティ状態を継続的にモニタリングするための技法と手順の使用を含む。[12]パブリッククラウドベースのシステムも、従来型の情報システムと同様に、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。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求事項を満たすことを要求している[JTF10]。実務的に可能な限り最大限に、組織は、プライバシーおよび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、組織の要求事項を満たしていることを確実にしなければならない。組織は、クラウドサービスが提供するプライバシーおよびセキュリティ管理策について理解し、サービス契約の中で十分な取り決めを確立し、必要な調整を行い、サービスコントロールが契約の条項に沿って実施されているか否かをモニタリングすべできある。

[12] リスクマネジメントについてのより詳細な情報は、NIST SP 800-37 Revision 1『Guide for Applying the Risk Management Framework to Federal Information Systems (http://csrc.nist.gov/groups/SMA/fisma/framework.html)』を参照のこと。

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[Jtf10]。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およびハードウェアのアーキテクチャは、特定のサービスモデルを提供するパブリッククラウドプロバイダ間で大きく異なる。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。その支援フレームワークの信頼性、リソースの集積化、拡張性を実現するためのロジックや、必要なその他のロジックの設計と実装も同様である。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。仮想マシンは、IaaS 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。クラウドプロバイダが、他のサービスモデル向けのサービスを提供するために、仮想マシン技術の代わりにその他の抽象化されたコンピューティング環境を使用することも考えられる。

サーバー側の均一化を補完するために、クラウドベースのアプリケーションはクライアント側に対してサービスの開始と取得を要求する。クライアントにはウェブブラウザが使用されることが多いが、ブラウザ以外が使用される可能性もある。さらに、適切かつセキュリティが確保されたネットワーク通信基盤が必要になる。クライアント、サーバー、およびネットワーク上の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、セキュリティとプライバシーに影響を与える内部の複雑さを覆い隠す。したがって、サービスを提供するためにクラウドプロバイダ使用する技術と、それらの技術的管理策がシステムのライフサイクル全体を通してシステムのセキュリティとプライバシーに与える影響を理解することが、重要である。そうした情報があれば、利用するクラウドのシステム構成を分解して、セキュリティおよびプライバシー管理策のフレームワークにマッピングし、リスクの評価と管理に使用できる

- **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、IaaS クラウドでよく使用される。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、攻撃の矢面が増加する。すなわち、追加となるメソッド（例：アプリケーションプログラミングインターフェース）、チャネル（例：ソケット）、データ項目（例：入力文字列）があり、これらもアタッカーがシステムに危害を加えるために利用できる。

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。ハイパーバイザが侵害されると、結果的に、そのハイパーバイザ上のすべてのシステムが侵害される可能性がある[Sca11]。例えば、広く使われている仮想ソフトウェア製品の 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に従って OS およびアプリケーションのセキュリティを強化することが必要となる。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。

- **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[Sca11, 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]。ハイパーバイザの中には、ネットワークのモニタリングが可能なものもあるが、それらの機能は物理ネットワークをモニタリングするためのツールに備わっている機能ほど堅固でないことが多い。組織は、トラフィックをハイパーバイザ内に遮蔽する場合と、物理ネットワークのモニタリングに晒す場合との、リスクとパフォーマンスのトレードオフについて考慮しなければならない[Sca11]。

仮想化された環境の副次的な影響は、組織内の既存の管理的役割に関して、責務の分離が失われる可能性があることである。例えば、従来型のコンピューティング環境では、通常、コンピュータアドミニストレータは侵入検知防止装置やファイアウォールなどのネットワークセキュリティコンポーネントの設定は行わない。一方、ネットワークセキュリティアドミニストレータは、そうしたデバイスの設定を行うことが許可されているが、ホスト上のシステムへのアクセスを許可する管理的権限は持たないことが多い。仮想環境では、コンピュータアドミニストレータとネットワークセキュリティアドミニストレータの異なる役割が、仮想インフラアドミニストレータという単一の役割に置き換えられる可能性がある。その他の異なる役割、

例えば、ストレージアドミニストレータの役割も、同様に影響を受ける可能性がある。仮想環境では、責務の分類を維持するために、技術的管理策の欠如を補う管理面と運用面での管理策が必要になるだろう。

仮想マシンイメージ(Virtual Machine Images)。IaaS クラウドプロバイダおよび仮想マシン製品のメーカーは、仮想マシンイメージのリポジトリを維持管理する。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の状態トに設定するのに使用される。いち早く立ち上げるための手段として、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。組織によって作成された仮想マシンイメージは、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。例えば、イメージは、最新のセキュリティパッチをもって最新に保つ必要がある。入念に検査されていないイメージを使用したり、やみくもにイメージを公開することがないよう、注意を払わなければならない。

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]。[13] 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, Sla09]。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。組織は、仮想マシンイメージの作成、保管、使用を管理するための正式なイメージ管理プロセスを実施することを検討すべきである。[Sca11]

- **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。異なるクラウドプロバイダが提供するサービス、および組織が開発するクラウドベースのアプリケーションが、より厳しい要求をクライアント側に課すことが考えられる。その場合、考慮されるべきセキュリティおよびプライバシー関連に影響するだろう。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、セキュリティが問題になっている[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

[13] 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。

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。さらに、クラウドアプリケーションは、ウェブブラウザではなく、特注のネイティブアプリケーション（すなわち、アプリ）を介して利用者に提供されることが多い。1 種類の OS がスマートフォンを占めている訳ではなく、システムコンポーネント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コンピュータ程頻繁には行われない。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。予防措置として、持ち運びが可能な機器および携帯機器からの個人情報やその他の機微な情報に対するアクセスを禁止または厳しく制限することによって、リスクを軽減するといった選択肢がある[Mcc10]。

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、それらはソーシャルエンジニアリング攻撃の手段として利用されることが多く、そのような場合には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上で動作しているといった状況は、パブリッククラウドサービスだけでなく、インターネット経由で利用できるその他のパブリックサービスのセキュリティとプライバシー保護に逆行する。[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]。セキュリティ意識向上トレーニングは組織が実施すべき重要な対策である。なぜならば、個々の職員の適切な行動は、多くの種類の攻撃に対する必要不可欠な予防措置であるからである。

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いる。アイデンティティマネジメントにおけるアイデンティの証明と認証の側面は、ユーザから収集した個人情報の使用、維持管理、保護を伴う。クラウド内の情報リソースに対する不正アクセスを防ぐのも、大きな課題である。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パブリック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。

アイデンティティフェデレーションは、利用者組織とクラウドプロバイダが、双方のドメインを跨いでデジタルアイデンティティと属性を信頼し共有することを可能にするため、シングルサインオンを実現するための手段となる。このフェデレーションがうまく機能するためには、アイデンティおよびアクセスマネジメントのトランザクションが慎重に、かつ明確に解釈され、攻撃に対して保護されなければならない。利用者のリソースをプロバイダによって認証されたエンティティから保護するためにも、また、その逆の場合も同じように保護するためにも、管理されたアイデンティティに関して、利用者のものとプロバイダのものを明確に分離する必要がある。アイデンティティフェデレーションは、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)。**認証は、ユーザの身元について信頼を確立するプロセスである。認証の保証レベルは、利用されるアプリケーションと情報資産の機微度と、関連するリスクに相応するレベルでなければならない[Bur06]。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情報をやりとりするための手段を提供する。例えば、ユーザがアイデンティプロバイダによって認証されたことに対するアサーションと、そのユーザの権限に関する情報を伝達するための SAML トランザクションが考えられる。この場合、トランザクションを受けとったサービスプロバイダは、ユーザに関して供給されたアイデンティと認証情報が正しく検証されたなら、前述の権限に関する情報を利用して、適切なレベルのアクセスをユーザに与える。

  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。[14] SOAPメッセージは電子的に署名される。パブリッククラウドの場合、例えば、ユーザがそのサービス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[Gru09]。XML ラッピングにより SOAP メッセージの不正操ができる。追加のエレメント（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方法の代わりに 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 規格はポリシーについて述べて、アクセスコントロールに関する判断を下すための XML ベースの言語を定義する。XACML は、認可 (Authorization)の

[14] もともとは、Simple Object Access Protocol の頭字語として命名された。

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 の基本的な使用例として、リソースに対するアクセスが試行された場合に、リソースに対するアクセスを保護する役割を担う PEP(Policy Enforcement Point:ポリシー実行点)から P DP(Policy Decision Point:ポリシー決定点)に対して、試行されたアクセスについての説明を含む、利用可能なポリシーと属性の評価を促すリクエストが送信される。PDP はこのリクエストを評価して、許可決定を PEP に返す。XACML は、プロトコルまたは伝送メカニズムを規定しない。また、ユーザの認証情報の検証方法について規定するわけでもない。XACML を使用する組織間で伝送されるメッセージは、トランザクションを保護するための十分な予防対策が実施されない限り、悪意のある第三者による攻撃(正規の権限によらない開示、再現、削除、変更を含む)に遭いやすい。[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、IaaS クラウドコンピューティング環境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]。

PaaS および SaaS クラウドコンピューティング環境におけるマルチテナントの扱い方は、IaaS とは異なる。例えば、SaaS プロバイダの多くは仮想マシンを伴わないインフラに依存する。彼らは、仮想マシンの代わりに、非常に大きな数の利用者を扱うことができ、必要に応じて内側または外側に拡張できるアプリケーションの単一の論理的なインスタンス(すなわち、ソフトウェアテクノロジースタック)を使用する[Arm10, Wai08]。使用されるサービスモデルとマルチテナントソフトウェアアーキテクチャにかかわらず、異なるユーザに対するコンピュータ処理は、主に、論理的な分離メカニズムの使用により、互いに独立した形で実施されなければならない。

- **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力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たす可能性である。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[Orm07]。[15] 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、研究者たちは中間者(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[Obe08a]。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

[15] 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。

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における暗号メカニズムの実装に対して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、パブリッククラウドでは、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パブリック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。クラウド内またはクラウド間で移行されるデータについても、同様の懸念が存在する。

- **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 Sutton[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。高い評価を得ていた警備会社による警備が破られたことにより、決意を秘めた相手には誰も太刀打ちできないことが明らかにされた（例：[And11], [Bra11], および[Pep11b]）。

  直接的なアプローチとは対照的に、Willie Hutton の特徴は、手際のよさと、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]。パスワードリセットにおける同様の弱点が IaaS 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にあれば十分であったため、アタッカーはそれらを入手し、アカウントの全てのリソースに対するアクセスを取得した。クラウドサービスのパスワードを紛失しても電子メールでリセットが可能であったため、アタッカーはそのアカウントに関連する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った。

  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]。

- **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(割り当てを解除されたオブジェクトを含む)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。保管される情報に対する物理的コントロールが欠如している場合、情報を確実に保護するには、暗号化が唯一の手段となる。

  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、クラウドユーザ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よりも分離型データベースを使用する方が実現しやすい。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、いくつかの分野または業種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、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り、通常は SaaS 環境であれ、PaaS 環境であれ、IaaS 環境であれ、実施にかかる手間は同じである[CSA11a, Pro10]。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。機能もサービスモデル間で大きく異なり、環境によっては、とりわけ PaaS や SaaS 環境では、暗号化による保護が可能でない場合がある[CSA11a, Pro10]。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。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, Pro10]。

暗号技術を採用しているシステムのセキュリティは、セントラル鍵と鍵管理構成要素の適切なコントロールに依存する。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。[16]

指針として、セントラル鍵の構成要素の管理とクラウドベースのアプリケーションの鍵管理構成要素の設定は、組織の職員が行うことが挙げられる[Bar05]。組織は、クラウドプロバイダが鍵管理用の設備を提供するクラウド環境に移行する前に、鍵管理ライフサイクルに関してクラウドプロバイダが定めたプロセスに関連するリスクを十分に理解し評価しなければならない[SCA11]。クラウドにおいて実施される暗号化操作は、鍵管理プロセスの一部となるため、組織による管理と監査が必要になる。

- **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、記憶媒体から情報を消去することであり、そうした情報の不正な開示を阻止するために行われ、その方法としては上書きや消磁、媒体の破壊などがある。[17] サニタイズは、例えば記憶装置がサービスから外された場合や、その用途が変更になった場合など、装置のリフレッシュまたはメンテナンスにかかわるさまざまな状況において実施される。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。

  パブリッククラウドコ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同じ場所に置かれる(例:IaaS 用データストア内に)、または混在した状態になる(例:SaaS 用データベース内に)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入手し、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[Sob06]。サービス契約は、データのサニタイズがそのシステムのライフサイクル全体を通して適切に行われることを保障するための、十分な対策について規定すべきである。

[16] 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。

[17] サニタイズについてのより詳細な情報は、Guidelines for Media Sanitization (http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.)を参照のこと。

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、2011 年 4 月には、ネットワークに対するアップグレードの試行が、サービスの 24 時間以上に及ぶ深刻な停止を引き起こした[Met11, Mil09, Pep11a]。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、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キング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[Cla09, Mic09]。

  可用性が 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が短い予告によって予定を組む可能性がある。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および災害復旧の機能は、組織の異常対処計画および事業継続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)となりうる。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、主たるプロバイダの施設に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]。つい最近、同様の強制捜査が行われ、その結果は前述とほぼ同じだった。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ことと、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]。

組織が、データの保管と処理に関してクラウドサービスに依存する場合には、クラウドが深刻な停止に遭遇し、サービスが利用できなくなっても、極めて重要な業務は継続できるよう準備が必要である。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。ポリシー、計画、および標準の運用手順を備えていれば、十分な償還が得られないクラウドサービスに過剰に依存することは避けられる。

- **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応答できなくする仕組みである。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]。

  インターネットを介して一般の人も利用できるサービス以外にも、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対してサービス拒否攻撃が行われることもある。[Mee09, 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。最悪の可能性としてありうるのは、あるクラウドのエレメントが別のクラウドのエレメントを攻撃することや、自クラウド内の他のエレメントを攻撃することである[Jen09]。

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。クラウドアプリケーションスタックの各レイヤ（アプリケーション、オペレーティングシステム、ネットワーク、およびデータベースを含む）は、ロードバランサや侵入検知装置などのその他のクラウドコンポーネントと同様に、イベントログを生成する。そうしたイベントソースの多くは、それらのソースにアクセスする手段と共に、クラウドプロバイダによって管理される。

クラウド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]。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。

- **データの可用性 (Data Availability)。** セキュリティインシデントをタイムリーに検知するためには、イベントのモニタリングから得られる関連データの可用性が極めて重要になる。パブリッククラウド環境では、極めて限られたインシデント検知機能しか提供されないことが多い[Gro10]。顕著な問題には、クラウドプロバイダの管理下にあるイベントソースおよび脆弱性情報に対して十分なアクセスが確保されない、イベントデータに自動的にアクセスしデータを処理するためのインターフェースに不備がある、クラウド基盤内に検知ポイントを追加できない、悪用やインシデントについての第三者からの報告を、そうした問題を処理するためにクラウドプロバイダまたは該当するユーザに効果的に伝達することが困難である、といったことが含まれる。こうした状況は、クラウドサービスモデルやクラウドプロバイダの間で異なる[Cro10]。例えば、PaaS プロバイダは、通常、イベントログをユーザに提供しないため、ユーザが得られるのは、主に、自身が実装したアプリケーションが生成するイベントデータ（例：アプリケーションによるロギングを介して）のみである。SaaS ユーザは、活動に関するログなどのイベントデータの提供に関して、クラウドプロバイダに完全に依存する。一方で、IaaS ユーザは、情報スタックをより広範囲にわたってコントロールでき、関連するイベントソースにアクセスできる。

- **インシデントの分析と解決 (Incident Analysis and Resolution.)。** インシデントの発生を確認し、どのように悪用されたかを特定するための分析は、十分な詳細さを備えたドキュメントと注意を払って迅速に行う必要がある。そうすることで、後続の使用（例：法的手続きのためにインシデントデータの法廷提出用のコピーを作成する）のための追跡可能性と完全性を確保しなければならない [Gro10]。発生したインシデントについて十分に理解するには、影響を受けたネットワーク、システム、アプリケーションの影響範囲を特定し、侵入の経路を明らかにして、実施された活動を再現する必要がある[Gro10]。インシデント分析を実施する際にクラウドユーザが直面する問題には、インシデントに関連するクラウドのアーキテクチャについて詳細な情報が得られないこと、クラウドプロバイダによって保有される当該イベント・データソースについての情報が得られないこと、クラウドプロバイダに対して規定されているインシデント対応に関する責任が明確に定義されていない、または曖昧である、ならびに関連するデータソースを証拠として収集し保管するための機能が限られていることが含まれる。

  インシデントの影響範囲と影響を受けた資産を特定した後は、インシデントを封じ込めて解決するための対策を実施して、システムをセキュアな運用状態に戻す[Gro10]。攻撃の封じ込めについてのクラウドプロバイダとクラウドユーザ間の責任と役割の区分けは、使用するサービスモデルとクラウドアーキテクチャによって変わる。例えば、SaaS および PaaS クラウド環境では、封じ込めは基本的には、アタッカーが無許可の活動を実施するために使用している機能を縮小または排除し（例：ウェブアプリケーションファイアウォールのフィルタリング機能を使って特定のユーザまたは機能を排除する）、必要に応じて、アプリケーション全体をオフラインにすることを意味する[Gro10]。IaaS クラウド環境では、クラウドユーザは、より大きな役割を担う。しかしながら、ベースとなるクラウド基盤において悪用された脆弱性を解消するためには、クラウドプロバイダによる支援が不可欠である。

インシデントの対応は、被害が最小限に抑えられ、リカバリにかかる時間と費用が最小となる形で実施されるべきである。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の確保には、クラウドのユーザとプロバイダが協力してインシデントを検知し対処することが不可欠である。連邦政府機関は、特定の種類のインシデントが発生した場合に、発見または検知した時点から1～2 時間以内にUS-CERT (U.S. Computer Emergency Readiness

Team)に報告する義務がある。[18] クラウドプロバイダに報告の義務があるインシデントの種類(例:データに対する侵害)と、報告する義務のないインシデントの種類(例:侵入検知装置による警告)について明確に理解することが必要である。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。効率的で費用効果的な対応には、クラウドのプロバイダと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。

インシデント対応チームが効果的に任務を遂行するには、自発的に、かつ決断力を持って行動する能力が求められる。一つの問題の解決が当該クラウドサービスを使用する多くのユーザになんらかの影響を与える可能性がある。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。インシデント対応に関する規定と手順について理解し交渉することは、後からの思い付きではなく、サービス契約を結ぶ前に行うべき行動である。例えば、インシデント対応計画は個人情報に対する侵害を取り扱うもので、報告と対処の対象になる侵害される個人情報の量を最小限に抑える方法について規定しなければならない[Mcc10]。データの地理上の所在地が調査を妨げる1つの要因になることもあるため、これもまた契約交渉時の議題の1つになる。

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、それらの課題の要約と、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の要約を示す。

表 1:セキュリティおよびプライバシーに関する課題と推奨事項

分野	注意事項
ガバナンス (Governance)	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、使用、モニタリングにも適用すること。 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遵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。
コンプライアンス (Compliance)	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、記録の管理、電子的な証拠開示に関するものについて実施すること。 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。 クラウドプロバイダの電子的な証拠開示に関する能力とプロセスが、データとアプリケーションのプライバシーまたはセキュリティを低下させることがないようにする。
信用 (Trust)	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

[18] 詳細については、http://www.us-cert.gov/federal/reportingRequirements.html を参照のこと。

	セスについて、その継続実施も含めて把握できるための十分な仕組みをサービス契約に盛り込むこと。 データに対する明確で独占的な所有権を確立すること。 絶え間なく進化と変化を遂げるリスク状況に、システムのライフサイクル全体を通して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。 現行のリスク管理上の意思決定をサポートするために、情報システムのセキュリティ状態を継続的にモニタリングすること。
アーキテクチャ (Architecture)	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対して、関連する技術的管理策がもたらす影響の理解も含まれる。
アイデンティティ・アクセス管理 (Identity and Access Management)	認証、認可、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と、それらの保護対策が組織に適することを確実にすること。
ソフトウェア間隔離 (Software Isolation)	クラウドプロバイダが自身のマルチテナントソフトウェアアーキテクチャに導入している仮想化およびその他の論理的隔離技術を理解し、内在するリスクを評価すること。
データの保護 (Data Protection)	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し、データに対するアクセスコントロール、保存中、伝送中、および使用中のデータのセキュリティの確保、ならびにデータのサニタイズにといった組織の能力を評価すること。 高い脅威プロフィールを持つ他の組織のデータ、または全体としての価値が著しく高いデータと同じ場所に、自組織のデータを置くことにより生じるリスクについて考慮すること。 そのクラウド環境で利用できる設備における暗号鍵管理と、クラウドプロバイダが定めたプロセスに関連するリスクを十分に理解し評価すること。
可用性 (Availability)	可用性、データのバックアップとリカバリ、および災害復旧に関する契約上の条件および手順について理解し、それらが組織の事業継続計画および異常対処計画の要求事項に適合することを確認し確保すること。 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。
インシデント対応 (Incident Response)	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理解し、それらが組織の要求事項に適合することを確認し確保すること。 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十分なメカニズムを備えていることを確認すること。 クラウドコンピューティング環境に対する利用者組織とプロバイダの各々の役割と責任に従って、プロバイダと協調する形でインシデントに対応する能力が、組織が備っていることを確認すること。

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、コンピュータの新しい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。この問題は、サービス契約のサービス条項が組織のニーズを完全に満たさない場合には、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、十分な取り決めがない場合には、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。要するに、サービス契約は組織にとって、コンピューティング環境に対するコントロールを実施し説明責任を果たすための主な手段になる。必要な要求事項または保証の内いずれかが欠落している場合、説明責任も脅かされることになる。

従来型の IT アウトソーシングの歴史を見ると、セキュリティとプライバシーへの懸念が随伴してきた。しかしながらこうした問題に、連邦政府機関が常に十分に取り組んできたわけではない（例：[GAO06, GAO10]）。前章で述べたように、組織のデータと機能をパブリック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、組織のプライバシーポリシーと、組織が遵守すべき情報の保護、配信、開示に関する現行の法規制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は、クラウド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]。

パブリッククラウドプロバイダの数が増え、提供されるサービスの範囲も広がることを踏まえると、組織が機能を選択しパブリック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。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。政府機関によって扱われるデータの機微度と、現在の最先端技術を考慮すると、すべての IT サービスをパブリッククラウドにアウトソーシングする可能性は低いと考えられる。しかしながら、ほとんどの政府機関にとって、必要なすべてのリスク軽減対策が実施されるならば、IT サービスの一部をパブリッククラウドに実装する可能性は否定できないだろう。

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電子メールの移行も含まれる。同市は 2009 年 11 月 20 日に本契約を締結した。

契約案を分析した結果[CAO09]、同市の行政官は、契約を進めることに関して、「市がこれらのサービスの利用を決定すると…、現在、市が所有し運営する構成に戻すには法外な費用がかかるだろう」という提言をした。**本分析は、また、以下のような警告を発した。**「提案されたシステムは現行のシステムよりも費用がかかること、Microsoft Office の使用を中断することにより生じうる運用上の影響、市の電子

メールとオフィスアプリケーションに対するコントロールが外部のベンダーに委譲されること、およびセキュリティ問題を取り巻く不確実性を含む、本報告書に示されたいくつかの分析結果から、本契約を承認することにより生じうるリスクが明らかになった」。

ロサンゼルス市は、セキュリティおよびプライバシー関連のいつくかの項目を話し合いを通じてSECS(SaaS E-mail and Collaboration Solution)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、市のデータを保護するために、データの暗号化、クラウドプロバイダによって保有されるその他のデータからの隔離、およびデータストレージの所在地に対する制約を義務づけることになった[LAPD10, Wil10]。追加の対策としてカリフォルニア州司法省が、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身元確認を行うことになった。

この他にも重要な交渉事項として、受託業者のセキュリティ計画をオンサイトで監査する権利、罰金を伴うサービスレベルに関する要求事項、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, SECS09, Wil10]を含む。データは恒久的に市の独占的な財産となる[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]。

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、ロサンゼルス市のレガシーな電子メールサービスとSaaSの電子メールサービスとの間に、機能面で大きく異なる点がいくつかあった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、低の機密ランク付けは行われない仕様になっていた。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かった。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た。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ことが含まれる[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た[CLA10, LAPD10, Sar10]。この遅延のため、問題が解決するまでレガシー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、費用も増大した。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レガシー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、市のユニークな要求事項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]。

2010年12月、ロサンゼルス市は、受託業者に対して、欠陥通知書を発行し、そのシステムがすべてのセキュリティ要求事項を満たしていないことと、そのことが同市の各部署にもたらす影響についての懸念を提起した[CWD10, Vij11]。2011年4月には、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と報じられた[Sar11a, Vij11]。

2011年8月22日の時点で、大多数のユーザが交換用のシステムに成功裏に移行されていた。ロサンゼルス警察署は、セキュリティ上の懸念からレガシーシステムに留まったが、彼らは、未解決の問題がすべて2012年の第1四半期までに解決し、同署がクラウドへの移行を完了することを望んだ[Cra11]。そのスケジュールによると、同市が契約の第1の選択年（すなわち、4年目）までサービスの利用を継続するか、あるいは別のソリューションを模索するかを決定するまでの期限は、約8ヶ月であろ

う。

2011 年 12 月 14 日、ロサンゼルス市議会は、SECS 契約の規模を縮小するか否かについて投票を行った。その結果、極めて重要な部署のセキュリティニーズがクラウドプロバイダによって満たされないと判断された[CLA11a, CLA11b, Gou11, Sar11b]。警察署、消防署、および市の検察局などは、契約の対象から外された。クラウドプロバイダは、また、契約期間中および契約の延長期間にレガシーシステムの運用にかかる費用を負担することに同意した。

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、以下のような面倒な事態になる可能性がある[All88]。
  - 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。
- **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発生した損害に対する賠償責任を組織が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。

セキュリティ関連の主張をサポートするためにクラウドプロバイダによって提供される保証、あるいは、クラウドプロバイダから委託された認証・コンプライアンスレビュー機関によって提供される保証は、可能な場合には常に、組織による独立したアセスメントを通じて検証されるべきである。また、第三者による認証またはクラウドプロバイダが提供するその他の保証が、利用者のアプリケーションまたはシステムに対して、必ずしも同レベルの認証またはコンプライアンスを提供するわけではない。それらの要素は、その特定のクラウド環境に対する独立した認証アセスメントを必要とするだろう。[19]

パブリッククラウドへ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間接的に関連する、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めるのは困難なので、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、通常は経営陣と職員が、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。

組織は、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なセキュリティおよびプライバシー管理策を採用してもよい。交渉の余地のないサービス契約では、通常、組織が実施できるリスク軽減活動が限られている。一方、交渉可能なサービス契約では、より広範の活動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

[19] 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（http://www.cio.gov/modules/fedramp/demo.cfm を参照）。

を行うことが必要となる。しかしながら、どちらの場合にも利用できるリスク軽減テクニックは、高価値のデータまたは機微度の高いデータ、もしくは極めて重要なアプリケーションをパブリッククラウドに移行しても対応できるほど十分ではないだろう。このような状況に対して組織は、より適した実装モデル（例えば、組織内プライベートクラウド）を採用することを考慮する可能性がある。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可能性があり、プラットフォームリソースを共有できるユーザの種類をより厳密に限定し、管理策に不備があったり、設定に誤りがあった場合にも露出を減らすことができる。

アウトソーシングにはいくつかの異なる段階があり、各段階において組織は、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ための所定の活動を実施する。すなわち、移行を計画する時（事前の実施事項）、サービス契約を開始し監視する時（契約開始と契約期間中の実施事項）、およびサービスと契約を終了する時（終了に際しての実施事項）である[All88, Len03]。本章の以降のセクションでは、これらの段階について詳しく説明する。

FIPSはアウトソーシングのすべての段階に関連する。とりわけFIPS 199とFIPS 200は、早い段階での計画作成に適用することができる。[20]

- **FIPS 199。** Standards for Security Categorization of Federal Information and Information Systems（連邦政府の情報および情報システムに対するセキュリティ分類規格）と題する本標準は、情報および情報システムの分類に関する共通のフレームワークとメソッドを提供する。本標準は、リスクレベルに見合った適切なレベルの情報セキュリティが提供されるのを確実にするために必要である。セキュリティ分類結果は、セキュリティ管理策の選択、プライバシー影響分析、重要インフラの分析など、その他の活動に対して情報を提供する。

- **FIPS 200。** Minimum Security Requirements for Federal Information and Information Systems（連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項）と題する本標準は、政府機関に対して、NIST SP 800-53 Revision 3に記載されているセキュリティ管理策と保証要求の中から適切なものを選択することによって、連邦政府の情報および情報システムに対して特定された最低限のセキュリティ要求事項を満たすことを命じている。

上述のSP 800-53以外にも、情報システムセキュリティの計画、実施、管理、および情報の保護に関する情報とガイダンスを提供するNISTガイドラインがあり、これらもアウトソーシングの取り組みに適用できる。そうしたガイドラインには、表2に記載されているNIST　SPが含まれる。これらのSPの原則は、クラウドコンピューティング環境全体に最も関連が深く、本文書と併せて使用することが推奨される。[21]

[20] FIPS Publicationsに関する情報は、NISTのFIPSのホームページ（http://itl.nist.gov/fipspubs/）を参照のこと。

[21] これらのNISTガイドラインと、その他のセキュリティ関連の刊行物に関する情報は、NISTのウェブページ（http://csrc.nist.gov/publications/index.html）を参照のこと。

表 2:選択された NIST Special Publications

Publication の番号	タイトル
SP 800-18	Guide for Developing Security Plans for Federal Information Systems
SP 800-34, Revision 1	Contingency Planning Guide for Federal Information Systems
SP 800-37, Revision 1	Guide for Applying the Risk Management Framework to Federal Information Systems
SP 800-39	Managing Information Security Risk
SP 800-53, Revision 3	Recommended Security Controls for Federal Information Systems and Organizations
SP 800-53, Appendix J	Privacy Control Catalog
SP 800-53A, Revision 1	Guide for Assessing the Security Controls in Federal Information Systems
SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories
SP 800-61 Revision 1	Computer Security Incident Handling Guide
SP 800-64, Revision 2	Security Considerations in the System Development Life Cycle
SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
SP 800-88	Guidelines for Media Sanitization
SP 800-115	Technical Guide to Information Security Testing and Assessment
SP 800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
SP 800-137	Information Security Continuous Monitoring for Federal Information Systems and Organizations

政府機関は OMB のポリシーに従って、特定の NIST Special Publications に従うことが義務付けられている。とはいうものの、どのようにガイダンスを適用するかについては、政府機関の裁量に任されている。連邦政府機関は、自身の任務、業務機能、および運用環境を考慮しそれらに適合するように、NIST Special Publications が規定するセキュリティ概念および原則を適用しなければならない。したがって連邦政府機関が NIST ガイダンスを適用した結果、異なるセキュリティソリューションとなることもあるが、それらのソリューションは同様に受け入れられ、その NIST ガイダンスに準拠し、OMB が定める連邦政府の情報システムに対する適切なセキュリティに適合しなければならない。

5.2 事前の実施事項

アウトソーシングの第 1 段階において、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、以下に示す項目が含まれる。

- **要求事項を定義する (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求事項を定義する必要がある。一般的なセキュリティ要求事項には、以下に示す分野が含まれる[CSA11b, Len03]。
  - 職員に対する要求事項。これにはクリアランス（権限の分離）、役割、および責任が含まれる
  - 法的な要求事項
  - 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／論理的アクセスコントロール
  - ネットワークのアクセスコントロール、接続性およびフィルタリング
  - データの保護
  - システムの構成およびパッチの管理
  - バックアップおよびリカバリ
  - データの保管と無毒化
  - セキュリティおよび脆弱性スキャン
  - リスクマネジメント
  - インシデントの報告、ハンドリング、対応
  - 業務の継続
  - 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

要求分析により、IaaS、PaaS および SaaS サービスモデルの中から組織の特定のニーズと目的に適したモデルを1つだけ選ぶことが可能になる。組織とクラウドプロバイダの双方の責任は、利用するサービスモデルによって異なる。例えば IaaS では、クラウドプロバイダの責任がハイパーバイザに留まるのが一般的である。クラウドサービスを利用する組織は、組織の実践規範がその環境にも適用されることと、組織の責任となる諸側面を管理するためのメカニズムとツールが提供されることを確実にするために、責任の分担とそれらの責任がクラウドプロバイダのプロセスにどのように結びつくべきかについて理解する必要がある。

停止に関する方策を立てることは、計画作成プロセスの重要な部分であり、要求分析の中で考慮されるべきである。これは組織の異常対処計画および事業継続計画の計画作業にも関連する。停止に関する方策は、例えばサービス契約が満期を迎えた場合などの正常な停止と、サービスプロバイダの倒産または業績不振などに起因する突然の停止の両方をカバーしなければならない[Gra03]。組織のすべてのデータを使用可能なフォーマットで安全に、かつ信頼できる効率的な方法でタイムリーにエクスポートする能力は、停止に関する方策の重要な側面である。そのほかの側面には、独自のプログラミングインターフェース、システムコール、データベース技術に対するアプリケーションの依存状態への取り組みと、クラウド環境内に蓄積された有用なメタデータのリカバリが含まれる。

さまざまな連邦 規格、OMBガイダンス、および公法に対する準拠は、要求分析で取り扱う必要があるさまざまな要求事項を課す。いくつかの主要な法規制がもたらす影響については、前の章で説明したが、他にもたくさんある。例えば、そのクラウドの実装に関して公表すべき側面(public-facing aspect)が存在する場合、OMBの覚書M-10-22『Guidance for Online Use of Web Measurement and Customization Technologies』、およびM-10-23『Guidance for Agency Use of Third-Party Websites and Applications』は、ブランド設定、プライバシー影響評価、ポリシー、および計画作成中に考慮すべきその他の問題に関するコンプライアンスガイダンスを提供する。個人情報の保護などのコンプライアンス関連の要求事項も、ある政府機関に特化する場合がある[Mcc10]。[22] 記録のマネジメントコントロール、アクセスのしやすさ、ユーザ教育など、 他にもアウトソーシングに関連する要求事項があり、これらもやはり、取り組みが必要になる。例えば、1973 年に施行のリハビリテーション法(29 合衆国法典 794d)の第 508 条は、障害を持つ人々（公務員や一般人を含む）による電子・情報技術へのアクセスを容易にするための要求事項を規定している。

クラウドコンピューティングに関す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、要求事項の定義の一助となる[Ove10]。組織が使用している IT アウトソーシングに関する既存の契約書も、有用である。

[22] 例えば、Veterans Affairs Information Security Enhancement Act の第 4 編、公法 109-461 は、復員軍人援護局に対して、機微な個人情報と情報システムを保護するために政府機関規模の情報セキュリティ手順を実施することを求めている。機微な個人情報は、個人にかかわる情報（学歴、金融取引、病歴、犯罪歴、職歴）や、個人の身元を識別または追跡するのに使用できる情報（氏名、社会保障番号、生年月日と出生地、母親の旧姓、生体に関する記録）を含む。

公正情報行動原則。プライバシー原則としても知られる公正情報行動原則は、世界中で最も現代的なプライバシー法を確立するためのフレームワークである[Mcc10]。米国もその一員である経済協力開発機構(OECD)は、1980 年に Guidelines on the Protection of Privacy and Transborder Flows of Personal Data を採用した[OECD80]。このガイドラインは米国連邦ガイダンスで参照されている、プライバシーを確保するためのフレームワークを提供し、国際的にも受け入れられていて、連邦政府が要求事項を定義し、計画作成中にプライバシー関連問題に取り組むために使用できる。このガイドラインは、以下に示す 8 つのプライバシー原則を規定する。

- 収集に対する制限。 個人情報の収集には制限を設けるべきであり、そうした情報は合法的に、かつ公正に、そして必要に応じて情報の主体の承認または同意を得たうえで、取得されるべきである。

- 情報の品質。 個人情報は、その使用目的に関連していなければならず、それらの目的を満たすのに必要なレベルの正確さと完全性を備え、最新に保たれていなければならない。

- 目的の明確化。 個人情報を収集する目的は、情報収集時より遅くならないように定義する必要があり、後続の使用はそれらの目的を果たすことに限定されなければならない。さもないと、情報が本来の目的に適合しなくなる。また、目的が変更になった場合には、その旨を示す必要がある。

- 使用に関する制限。 個人情報は、情報の主体からの同意を得た場合や、捜査当局から要請を受けた場合を除き、前述の原則に従って、規定されている以外の目的で開示、アクセス、または利用されないようにする必要がある。

- セキュリティ上の予防対策。 個人情報は、適切なセキュリティ上の予防対策をもって、情報の消失または正規の権限によらないアクセス、破壊、利用、変更、開示などのリスクから保護されなければならない。

- 開放性。 個人情報の開発、実践規範およびポリシーに関しては、それらの開放性についての一般的なポリシーが必要になるだろう。個人情報の存在と性質、およびそれらの情報の主な使用目的、ならびに情報管理者の身元と居住地を把握するための手段を用意する必要がある。

- 個人参加の原則。 個人は以下の権利を有するものとする。

  (ア) 自身に関連する情報を情報管理者が保有しているか否かを、管理者に直接確認するか、あるいは別の方法により確認する。

  (イ) 自身に関連する情報の保有について通知させること。通知は、妥当な時間内に、料金が発生する場合は度を越えないようにして、妥当な方法で、かつ、自分にとってすぐに理解できる形でなされるよう要求すること。

  (ウ) 副段落（ア）と(イ)をもとになされた要請が拒否された場合に、その理由を報告させること。また、そうした拒否に対して異議を申し立てることができること。

  (エ) 自身に関連する情報に関して、異議を申し立てることができること。また、申し立てが通った

場合に、情報を消去、修正、完全化または訂正させること。

■ 説明責任。情報管理者は、前述の原則を実行するための対策の遵守に説明責任を負う。

公正情報行動原則には、プライバシーの保護に関する 5 つの主な原則が含まれる[FTC07]。これらの原則は、OECD ガイドラインが規定する原則に似ているが、営利目的の組織を対象としている。しかしながら、これらの原則は、プライバシーの保護に関する有用で補足的な視点を提供する。

■ 通知／意識性。利用者は、個人情報の開示の範囲について十分な情報にもとづく意思決定を可能にするためにも、個人情報が収集される前に、その事業体の情報実践について通知を受けなければならない。以下の項目の一部または全てに関する通知は、利用者への通知が正しく行われるようにするうえで、極めて重要であると考えられる：情報を収集する事業体の識別情報; 情報の使用目的; 情報を受け取る可能性がある者の識別情報; 収集される情報の性質と（不明な場合には）情報の収集方法（例：電子監視によって受動的に、あるいは利用者に情報の提供を求めるといった能動的な方法で）; リクエストされた情報の提供が自発的であるか、あるいは義務づけられているか、そしてリクエストされた情報の提供が拒否された場合の結果; ならびに収集された情報の機密性、完全性、および品質を確保するために講じられた措置。

■ 選択／同意。選択とは、収集される個人情報の使用に関する選択肢を利用者に与えることを意味する。選択は、具体的に、予定されたトランザクションの実施に必要な用途ではなく、情報の二次的な用途に関連する。オプト・インとオプト・アウトは、選択／同意制度における 2 つの主な種類である。オプト・インは収集に対する利用者の同意を必要とし、オプト・アウトは収集を阻止することに対する利用者の同意を必要とする。選択は、2 つ以上の選択肢が用意される場合もあり、開示する情報の種類とその情報の許容できる用途を利用者が調整できるようにする。

■ アクセス／参加。ここでいうアクセスとは、自身に関して保有されている情報をレビューし、その情報の正確さと完全性について異議を唱える個人の能力を示す。このプロセスはシンプルかつタイムリーに、そして利用者にとって費用があまり掛からないように実施されるべきである。このプロセスにより、利用者が唱える 異議が組み入れられ、情報の受取人に送信される。

■ インテグリティ／セキュリティ。インテグリティは、情報が正確であり、セキュリティが確保されていることを必要とする。インテグリティを確保するには、合理的な対策（例えば、複数のソースからのデータを相互参照して正確さを確認する）の実施が必要になる。セキュリティは、情報の消失や、正規の権限によらないアクセス、破壊、利用、変更、開示に対する保護対策を含む。

■ 実施／救済策。効果的なプライバシーの保護には、収集された情報をもってコア原則を実施し、望ましくない状況または公正を欠いた状況を改善するための仕組みが必要である。情報の処理が行われることにより恩恵を受ける情報管理者は、コア原則を満たすことに責任を負う。業界自主規制による実施、利用者に対する個別の救済を可能にする法律、民事・刑事制裁によって強制執行できる規制スキームは、救済策の候補である。

■ **セキュリティおよびプライバシー関連リスクを評価する (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、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。前章では、システムのライフサイクル全体を通して柔軟で調整が可能なリスク管理計画を実施する重要性について述べた。この段階で実施されるリスクの分析

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]。交渉の余地のないサービス契約の場合には、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。もしそうなら、関連するセキュリティおよびプライバシー関連リスクが増加する。リスクの分析の一環として、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施設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。

組織には、新しい情報システムを開発または調達する前に、あるいは既存のシステムに大きな変更があった場合に、プライバシー閾値分析（PTA）の実施が必要になる可能性がある[Mcc10]。プライバシー閾値分析は、システムが個人情報を含むか、プライバシー影響評価または記録システムからの通知(SORN)が必要か否か、プライバシー関連のその他の要求事項がその情報システムに適用されるかを判断するために用いられる。先に述べたように、通常、プライバシー影響評価は、個人情報の収集、保管、または配信を行い、一般の人が利用できるようにするための技術が新たに登場したり、既存の技術に大きな変更があった場合に実施される。

個人情報は、そうした情報が不正にアクセス、利用、または開示された場合に、対象となる個人および／または組織にもたらされる可能性がある被害について判断するためにも、評価が必要になる（すなわち、機密性に対する影響レベル）[Mcc10]。組織は、個人情報の機密性に対する影響レベルを判断する際に使用する因子を決定し、情報を保護するための適切なポリシー、手順、管理策を策定し実施する。例えば、特定の種類の個人情報を保護するための法律上の義務を課している連邦政府機関もある。個人情報の機密性に対する影響レベルを判断し、適切な予防対策を選択する際には、そうした義務についても検討すべきである。[23]

リスクの分析では、組織が保有するその他の種類のデータの機微度も重要な因子となる。[24] 組織が扱うデータの範囲は、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、他に比べて、より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
- ネットワークの概略図、設定情報、脆弱性レポートなどの、システムセキュリティに関する情報
- 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

[23] 個人情報の機密性に対する影響レベルの判断に関する情報は、Guide to Protecting the Confidentiality of Personally Identifiable Information (http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf)を参照のこと。

[24] 自組織のデータと他組織のデータが同じ場所に置かれる場合には、他組織のデータの機微度も1つの因子となる可能性がある。

- 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

クラウドプロバイダがサービスを提供するために使用するベースとなる技術について理解することは、正確なリスク分析を行ううえで極めて重要である。前章で述べたセキュリティおよびプライバシー関連の問題は、以下に示すような、レビューが必要な重要な技術分野を明らかにした。

- クラウドのマルチテナントソフトウェアアーキテクチャに採用されている論理的な分離の技術
- データのバックアップとリカバリ、およびデータの無毒化のための施設
- 電子的証拠開示機能およびプロセス
- データに対するアクセスコントロール、保存中、伝送中、および使用中のデータの保護、不要になったデータの消去のための仕組み
- 暗号技術と暗号鍵管理のために利用できる施設
- セキュリティが確保された認証、権限付与、およびその他のアイデンティティ・アクセス管理機能のためのメカニズム
- インシデント対応と災害復旧用の施設

先に述べたように、リスクレベルが高すぎることがリスクの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。リスクの評価中に、分析中のサービスモデルとアプリケーションにとっては、パブリッククラウドではなく、別の実装モデルがより適していることが判明することも考えられる。

- **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]。現在クラウドプロバイダのサービスを利用しているユーザ（他の政府機関など、個別に特定されたユーザ、あるいはクラウドプロバイダによって用意された参考資料をもとに特定されたユーザ）に聞き取りを行って、組織の関心事であるセキュリティとプライバシーに関してユーザの満足度を確かめることも、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を厳密に行うことに加えて、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プライバシーの意識向上トレーニングの質と頻度
- アカウント管理の実践規範と説明責任
- 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
- 変更管理手順およびプロセス
- クラウドプロバイダの実績記録
- 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、法規制遵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

アウトソーシングの第 2 段階、すなわち、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全体を通して契約のサービス条項を監視する際に、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)。**組織はサービス契約に、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]。[25] 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を含めなければならない。組織は、リスクを受容可能なレベルまで軽減するために自身が必要とする補完的管理策が、契約のサービス条項の範囲内で実施されることを確認しなければならない。契約のサービス条項には、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求事項を含む、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、手順、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遵守しているか、についての評価プロセス（第三者による監査とテストを含む）
  - 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

[25] 連邦調達に使用されるセキュリティ契約の専門用語の例については、2009 年 11 月 6 日発行の『Security Language for IT Acquisition Efforts, CIO-IT Security-09-48, Revision 1 (http://www.gsa.gov/graphics/pbs/CIO_Policy.pdf)』を参照のこと。

- 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（または同じ場所に置く）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：組織のデータの返却および消去）

前章では、組織がサービスプロバイダに特に依存し、発生する可能性のある問題を回避するために非常に明確なサービス条項を必要とする、追加の分野について指摘した。それらの分野には以下が含まれる。

- データに対する所有権
- クラウド環境内の組織のデータの位置
- セキュリティおよびプライバシーの遂行に対する可視性
- サービスの可用性と選択可能な異常対処
- データのバックアップとリカバリ
- インシデント対応における調整と情報共有
- 災害復旧

プライバシー規制に対する解釈は、組織の法律およびプライバシー担当者とクラウドプロバイダとの間で異なる可能性がある。組織は、クラウドプロバイダのサービス契約に規定されている、または交渉によって盛り込まれた管理策をレビューする際に、組織のプライバシーポリシーとクラウドプロバイダのプライバシーポリシー間の一致しない部分を特定し解消するために相当な注意を払わなければならない。組織は、提供される管理策が、クラウド環境への実装を計画している種類の情報を保護するのに十分であることを確認しなければならない。OMB ガイダンス M-07-16『Safeguarding Against and Responding to the Breach of Personally Identifiable Information』は、プライバシー法が規定する要求事項について考察し、個人情報の保護に関する政府機関の義務に関する追加のガイダンスを提供する。

契約を結ぶ前に、経験豊富な法律の専門家に契約条件を詳細にチェックしてもらうことをお勧めする。通常、交渉の余地のないサービス契約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。パブリッククラウドサービスの交渉可能なサービス契約のサービス条項に関して合意に達することは、技術的な問題と法的な問題が伴う複雑なプロセスになる

可能性がある。交渉可能なサービス契約が使用される場合、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、交渉には始めから法律の専門家にも参加してもらうことが望ましい。

- **パフォーマンスを評価する (Assess Performance)。**契約上のすべての義務が果たされ、組織の要求事項が満たされることを確実にするには、クラウドプロバイダのパフォーマンスと提供されるサービスの質の継続的な評価が必要となる。この継続的な評価は、リスクマネジメントプロセスの必要不可欠な部分である。[26] 組織は、システムの状態の分析を定期的に、かつセキュリティおよびプライバシー関連リスクを適切に管理するのに必要な頻度で実施すべきである。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、サービス契約のサービス条項を改善するための参照事項またはベンチマークも得られる[All88, Gra03, Len03]。

5.4 終了に際しての実施事項

プロジェクトの最後の段階に、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の最終段階に入り、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に先立ち、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記憶媒体からの削除など、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、サービス契約の一部としてクラウドプロバイダに割り当てた、組織のコンピュータリソースに対する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]。同様に、クラウドプロバイダに発行した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、サービス契約のサービス条項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、ドキュメントなどのリソース、ならびにクラウドプロバイダが保有する組織のデータ、プログラム、スクリプトなどが、利用できる形で返還または回収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ユーザ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]。[27] これらの活動は、政府機関の記録管理ポリシーに沿って実施しなければならない。

---

[26] 継続的なモニタリングとリスクマネジメントに関するより詳細な情報は、SP 800-137『Information Security Continuous Monitoring for Federal Information Systems and Organizations』とSP 800-37 Revision 1『Guide for Applying the Risk Management Framework to Federal Information Systems』（両方とも http://csrc.nist.gov/publications/index.html）を参照のこと。

[27] 媒体の無毒化に関するより詳細な情報は、SP 800-88『Guidelines for Media Sanitization』(http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-

停止に関する方策を計画作成段階の初期に立てることと、その内容を定期的にレビューし更新することによって、サービス契約の終了時に遭遇する問題を最小限にし、アプリケーションを別のサービスプロバイダに移行する、あるいはアプリケーションを組織のデータセンタに戻す際の手間も最小にすることができる。

5.5 推奨事項のまとめ

表 3に、アウトソーシングの各段階における課題と推奨事項の要約を示す。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、セキュリティおよびプライバシー関連の特定の問題に由来する。

表 3:アウトソーシング活動と推奨事項

分野	注意事項
事前の実施事項 (Preliminary Activities)	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求事項（セキュリティおよびプライバシーに関する要求事項を含む）を抽出すること。 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し、関連するリスクのレベルを評価すること。 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。
契約開始と契約期間中の実施事項 (Initiating and Coincident Activities)	サービス契約に、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。 サービス契約のレビューと、サービス条項についての交渉を行う際には、法律の専門家を参加させること。 クラウドプロバイダのパフォーマンスと提供されるサービスの質を継続的に評価し、契約上のすべての義務が果たされていることを確実にし、リスクを管理・軽減すること。
終了に際しての実施事項 (Concluding Activities)	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。 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。 サービス契約のサービス条項に基づいてクラウドプロバイダが利用または保有できるようにした組織のリソースが利用できる形で返還または回収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確認すること。

88_rev1.pdf.)を参照のこと。

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が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ではコストとパフォーマンスの利点が強調されるが、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とのバランスを考慮する必要がある。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。システムの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に取り入れることを検討せざるをえ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実装におけるセキュリティおよびプライバシーに関する説明責任は、クラウドプロバイダに委譲することはできず、組織が果たすべき義務である。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、システムのライフサイクル全体を通して、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、そのシステムのセキュリティ状態の継続的なモニタリングを必要とし、コンピューティング環境のかなりの部分がクラウドプロバイダの管理下に置かれ、組織の管理外となる可能性が高いため、困難な課題になりうる。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。管理策の数が多すぎると効率が悪くなり、効果も弱められている可能性がある。政府機関および他の組織は、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維持するために熱心に取り組まなければならない。

クラウドコンピューティングはコンピュータの新しいパラダイムであり、いまだ発展途上にある。技術の進歩が、パブリッククラウドが提供するサービスのパフォーマンスやその他の品質（プライバシーとセキュリティを含む）を向上させることが期待される。政府機関のシステムの多くは長期にわたって使用され、パブリッククラウドに移行された場合、生涯にわたって技術面やその他の面での変化に遭遇するだろう。クラウドプロバイダが他の企業にサービスを販売する、あるいはマージすることを決断することも考えられる。自身が提供するサービスが別のクラウドプロバイダが提供するサービスに追い越されたり、人気を失う可能性もあるだろう。また、選択年をすべ

て使い果した後に、組織がクラウドサービスの既存の契約に再び立ち向かうことも考えられる。いつの日か一部のシステムを別のパブリッククラウドに移行せざるをえないといった状況も発生しうる。このような可能性について、政府機関やその他の組織は軽視してはならない。

7. 参考文献

[All88] Julia Allen et al., Security for Information Technology Service Contracts, CMU/SEI-SIM-003, Software Engineering Institute, Carnegie Mellon University, 1988年1月, <URL: http://www.sei.cmu.edu/reports/98sim003.pdf>.

[Alp11] Pavel Alpeyev, Joseph Galante, Mariko Yasu, Amazon.com Server Said to Have Been Used in Sony Attack Bloomberg, 2011年5月14日 , <URL: http://www.bloomberg.com/news/2011-05-13/sony-network-said-to-have-been-invaded-by-hackers-using-amazon-com-server.html>.

[And11] Nate Anderson, Anonymous vs. HBGary: the Aftermath, Ars Technica, 2011年2月24日, <URL: http://arstechnica.com/tech-policy/news/2011/02/anonymous-vs-hbgary-the-aftermath.ars>.

[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-confirms-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>.

[Bar05] Elaine B. Barker, William C. Barker, Annabelle Lee, Guideline for Implementing Cryptography In the Federal Government, NIST Special Publication 800-21, Second Edition, 2005 年 12 月 , <URL: http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf>.

[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>.

[Bos11] Bianca Bosker, Dropbox Bug Made Passwords Unnecessary, Left Data At Risk For Hours, The Huffington Post, 2011年6月21日, <URL: http://www.huffingtonpost.com/2011/06/21/dropbox-security-bug-passwords_n_881085.html>.

[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.ssrn.com/sol3/papers.cfm?abstract_id=1662374>.

[Bra11] Tony Bradley, Google, Skype, Yahoo Targeted by Rogue Comodo SSL Certificates, PCWorld, 2011年3月23日, <URL: http://www.pcworld.com/businesscenter/article/223147/google_skype_yahoo_targeted_by_rogue_comodo_ssl_certificates.html>.

[Bro08] Jon Brodkin, 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, Ma.gnolia 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/>.

[CAO09] Report from Office of the City Administrative Officer: Analysis of Proposed Contract, City of Los Angeles, CAO File No.:0150-00813-0001, 2009年7月9日, <URL: http://clkrep.lacity.org/onlinedocs/2009/09-1714_rpt_cao_7-9-09.pdf>.

[Cap09] Dawn Cappelli, Andrew Moore, Randall Trzeciak, Timothy J. Shimeall, Common Sense Guide to Prevention and Detection of Insider Threats, Third 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>.

[Cho010] Rajarshi Chakraborty, Srilakshmi Ramireddy, T.S. Raghu, H. Raghav Rao, The Information Assurance Practices of Cloud Computing Vendors, IEEE IT Pro, Vol. 12, Issue 4, 2010年7月／8月.

[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>.

[CIO10a] Privacy Recommendations for the Use of Cloud Computing by Federal Departments and Agencies, CIO Council, Privacy Committee, Web 2.0/Cloud Computing Subcommittee, 2010年8月, <URL: http://www.cio.gov/Documents/Privacy-Recommendations-Cloud-Computing-8-19-2010.docx>.

[CIO10b] Federal Enterprise Architecture Security and Privacy Profile, Version 3, 2010年9月30日, <URL: http://www.cio.gov/Documents/FEA-Security-Privacy-Profile-v3-09-30-2010.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/>.

[CLA10] Second Status Report on the Implementation of the Google E-Mail and Collaboration System, City Administrative Officer, City of Los Angeles, 2010年7月9日, <URL: http://clkrep.lacity.org/onlinedocs/2009/09-1714_rpt_cao_7-9-10.pdf>.

[CLA11a] Second Amendment to Contract Number C-116359 between the City and Computer Sciences Corporation for E-Mail and Collaboration Solution (Google), Inter-Departmental Correspondence, City of Los Angeles, 2011年12月9日, <URL: http://clkrep.lacity.org/onlinedocs/2009/09-1714-S2_RPT_CLA_12-09-11.pdf>.

[CLA11b] Record of Council Action Regarding Second Amendment to Contract Number C-116359, City of Los Angeles, 2011年12月20日, <URL: http://clkrep.lacity.org/onlinedocs/2009/09-1714-S2_CA_12-14-11.pdf>.

[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>.

[Cou09] David A. Couillard, Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing, Minnesota Law Review, Vol. 93, No. 6, 2009年6月

[Cra08] George Craciun, Amazon EC2 Spreads Malware, Softpedia, 2008年7月1日, <URL: http://news.softpedia.com/news/Amazon-EC2-Spreads-Malware-89014.shtml>.

[Cra10] Personal conversation with Kevin K. Crawford, Assistant General Manager, Information Technology Agency, City of Los Angeles, 2010年12月15日

[Cra11] Personal conversation with Kevin K. Crawford, Assistant General Manager, Information Technology Agency, City of Los Angeles, 2011年8月22日.

[CSA11a] Encryption and Key Management, Cloud Security Alliance, 2011年1月12日, <URL: https://wiki.cloudsecurityalliance.org/guidance/index.php/Encryption_and_Key_Management>.

[CSA11b] Cloud Controls Matrix, Version 1.2, Cloud Security Alliance, 2011年8月26日, <URL: https://cloudsecurityalliance.org/wp-content/uploads/2011/08/CSA_CCM_v1.2.xls>.

[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>.

[CWD10] Notice of Deficiencies-CSC Contract No. C-116359, City of Los Angeles, 2010年12月9日, <URL: http://www.consumerwatchdog.org/resources/googdeficiency.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>.

[Dem10] Kelley Dempsey et al., Information Security Continuous Monitoring for Federal Information Systems and Organizations, Initial Public Draft, SP 800-137, NIST, 2011年9月, <URL: http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.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>.

[Dij10] Marten van Dijk, Ari Juels, On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing, 5th USENIX Workshop on Hot Topics in Security (HotSec '10), 2010年8月10日, <URL: http://www.usenix.org/event/hotsec10/tech/full_papers/vanDijk.pdf>.

[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://export.gov/safeharbor/eu/eg_main_018475.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>.

[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>

[FTC07] Fair Information Practice Principles, Federal Trade Commission, 2007年6月25日, <URL: http://www.ftc.gov/reports/privacy3/fairinfo.shtm>.

[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>.

[GAO06] Privacy: Domestic and Offshore Outsourcing of Personal Information in Medicare, Medicaid, and TRICARE, United States Government Accountability Office, GAO-06-676, 2006年9月, <URL: http://www.gao.gov/new.items/d06676.pdf>.

[GAO10] Contractor Integrity: Stronger Safeguards Needed for Contractor Access to Sensitive Information, United States Government Accountability Office, GAO-10-693, 2010年9月, <URL: http://www.gao.gov/new.items/d10693.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/>.

[Goo11] Jeff Gould, Los Angeles Ends Google Apps for LAPD; Decision Bigger Than You Think, AOL Government, 2011年12月19日, URL: http://gov.aol.com/2011/12/19/los-angeles-ends-google-apps-for-lapd-decision-bigger-than-you/>

[Gra03] Tim Grance et al., Guide to Information Technology Security Services, 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>.

[Gro10] Bernd Grobauer, Thomas Schreck, Towards Incident Handling in the Cloud: Challenges and Approaches, ACM Cloud Computing Security Workshop, Chicago, Illinois, 2010年10月8日.

[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/>.

[Han06] Saul Hansell, Online Trail Can Lead To Court, The New York Times, 2006年2月4日, <URL: http://query.nytimes.com/gst/fullpage.html?res=9B03E5D7163EF937A35751C0A9609C8B63>.

[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>

[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>.

[Ker11] Justin Kern, Amazon Apologizes, Cites Human Error in Cloud Interruption, Information Management Online, 2011 年 4 月 29 日, <URL: http://www.information-management.com/news/cloud_SaaS_data_center_downtime_storage_Amazon-10020215-1.html>.

[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 Krigsma, 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>.

[LAPD10] Supplemental Report to the City Administrative Officer: Second Status Report on the Implementation of the Google E-Mail and Collaboration System (C.F. 09-1714), Los Angeles Police Department, City of Los Angeles, <URL: http://clkrep.lacity.org/onlinedocs/2009/09-1714_rpt_lapd_7-8-10.pdf>.

[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>.

[Mcc10] Erika McCallister, Tim Grance, Karen Scarfone, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), SP 800-122, National Institute of Standards and Technology, 2010年4月, <URL: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>.

[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>.

[Mel11] Peter Mell, Tim Grance, The NIST Definition of Cloud Computing, Special Publication 800-145, National Institute of Standards and Technology, 2011年8月, <URL: http://csrc.nist.gov/publications/nistpubs/800-145/sp800-145.pdf>.

[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/>.

[Met11] Cade Metz, Amazon Cloud Fell from Sky after Botched Network Upgrade, The Register, 2011年4月29日, <URL: http://www.theregister.co.uk/2011/04/29/amazon_ec2_outage_post_mortem/>.

[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-azure-malfunction-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>.

[Mul10] Robert Mullins, The Biggest Cloud on the Planet is Owned by the Crooks, Network World, 2010年3月22日, <URL: http://www.networkworld.com/community/node/58829>.

[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>.

[OECD80] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Organisation for Economic Co-operation and Development, 1980年9月23日, <URL: http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html>.

[Opp03] David Oppenheimer, Archana Ganapathi, David Patterson, Why Do Internet Services Fail, and What Can Be Done About It?, 4th USENIX Symposium on Internet Technologies and Systems, 2003年3月, <URL: http://roc.cs.berkeley.edu/papers/usits03.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>.

[Owa10] Cloud-10 Multi Tenancy and Physical Security, The Open Web Application Security Project, Cloud Top 10 Security Risks, August 30, 2010年8月30日, <URL: https://www.owasp.org/index.php/Cloud-10_Multi_Tenancy_and_Physical_Security>.

[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

[Pep11a] Julianne Pepitone, Amazon EC2 Outage Downs Reddit, Quora, CNN Money, 2011 年 4 月 22 日 , <URL: http://money.cnn.com/2011/04/21/technology/amazon_server_outage/index.htm>.

[Pep11b] Julianne Pepitone, RSA Offers to Replace All SecurID Tokens after Hack Attack, CNN Money Tech, 2011年6月8日, <URL: http://money.cnn.com/2011/06/08/technology/securid_hack/index.htm>.

[Per11] By Juan Carlos Perez, Microsoft's Cloud BPOS Suite Suffers Outage Again, InfoWorld Inc., 2011年6月22日, <URL: http://www.infoworld.com/d/applications/microsofts-cloud-bpos-suite-suffers-outage-again-050>.

[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

[Pro10] Cloud Security and Privacy: Data Security and Storage, 2010年11月18日, <URL: http://mscerts.programming4.us/programming/Cloud%20Security%20and%20Privacy%20%20%20Data%20Security%20and%20Storage.aspx>.

[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>.

[Sar11a] David Sarno, Google Facing Hurdles in Bid to Provide Email Service to Governments, Los Angeles Times, 2011年4月14日, <URL: http://articles.latimes.com/2011/apr/14/business/la-fi-google-email-20110414>.

[Sar11b] David Sarno, L.A. won't put LAPD on Google's cloud-based email system, Los Angeles Times, 2011年12月14日, <URL: http://articles.latimes.com/2011/dec/14/business/la-fi-google-email-20111215>.

[Sca11] Karen Scarfone, Murugiah Souppaya, Paul Hoffman, Guide to Security for Full Virtualization Technologies, Special Publication 800-125, National Institute of Standards and Technology, 2011年1月, <URL: http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf >.

[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>.

[Sch11] Mathew J. Schwartz, Are You Ready for an FBI Server Takedown?, Information Week, 2011年7月1日, <URL: http://www.informationweek.com/news/security/management/231000897>.

[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>.

[Som11] Juraj Somorovsky et al., All Your Clouds Belong to Us – Security Analysis of Cloud Management Interfaces, ACM Cloud Computing Security Workshop (CCSW), Chicago, 2011年10月21日.

[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/>.

[Swa06] Marianne Swanson, Joan Hash, Pauline Bowen, Guide for Developing Security Plans for Federal Information Systems, NIST, Special Publication 800-18, Revision 1, 2006 年 2 月 , <URL: http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf>.

[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-v39n1l-vaqueroA.pdf>.

[Vie09] Kleber Vieira, Alexandre Schulter, Carlos Westphall, Carla Westphall, Intrusion Detection Techniques in Grid and Cloud Computing Environment, IT Professional, IEEE Computer Society, 2009年8月26日

[Vij11] Jaikumar Vijayan, City of Los Angeles May Sue over Delays in Google Apps Project, Computer World, 2011年4月18日, <URL: http://computerworld.co.nz/news.nsf/management/city-of-los-angeles-may-sue-over-delays-in-google-apps-project-report>.

[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 Wainewright. 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

[Wei11] Thilo Weichert, Cloud Computing and Data Privacy, The Sedona Conference, Working Group on International Electronic Information Management, Discovery & Disclosure, 2011年2月, <URL: https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-and-data-privacy.pdf>.

[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 ー略語

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)
ESI	電子的に保管された情報 (Electronically Stored Information)
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)
OECD	経済協力開発機構 (Organization for Economic Co-operation and Development)
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)
PDP	ポリシー決定点 (Policy Decision Point)
PEP	ポリシー実行点 (Policy Enforcement Point)
PIA	プライバシー影響評価 (Privacy Impact Assessment)
PII	個人情報 (Personally Identifiable Information)
SaaS	SaaS (Software as a Service)

SSAE	監査証明契約に関する基準 (Standards for Attestation Engagements)
SORN	記録システムからの通知 (System of Records Notice)
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)
SPI	機微な個人情報 (Sensitive Personal Information)
US-CERT	US-CERT (United States Computer Emergency Readiness Team)
WPA	ワイファイプロテクテッドアクセス (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、考えられる軽減策について知るために役立つであろう。

参考文献の内容	URL
DRAFT Cloud Computing Synopsis and Recommendations, NIST, 2011 年 5 月	http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf
Challenging Security Requirements for US Government Cloud Computing Adoption (Draft), Cloud Security Working Group, NIST, 2011 年 11 月	http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Requirements_for_US_Government_Cloud.pdf
Top Threats to Cloud Computing, V1.0, Cloud Security Alliance, 2010 年 3 月	http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
Privacy Recommendations for the Use of Cloud Computing by Federal Departments and Agencies, CIO Council, Privacy Committee, 2010 年 8 月 19 日	http://www.cio.gov/documents/Privacy-Recommendations-Cloud-Computing-8-19-2010.docx
Security Guidance For Critical Areas of Focus in Cloud Computing, V2.1, Cloud Security Alliance, 2009 年 12 月	http://www.cloudsecurityalliance.org/csaguide.pdf
Cloud Computing Risk Assessment, European Network and Information Security Agency, 2009 年 11 月	http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport
The 10 Worst Cloud Outages (and what we can learn from them), J R Raphael, InfoWorld, 2011年6月27日	http://www.infoworld.com/d/cloud-computing/the-10-worst-cloud-outages-and-what-we-can-learn-them-902
The Future of Cloud Computing, 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-report-final.pdf