クラウドコンピューティングのためのセキュリティガイダンス　V3.0

日本語版の提供について

2013年5月8日

日本語版の提供について

「クラウドコンピューティングのためのセキュリティガイダンス　V3.0」（以下、ガイダンスと記述）は、Cloud Security Alliance よりリリースされている　“Security Guidance for Critical Areas of Focus in Cloud Computing V3.0”の日本語訳です。
このガイダンスは、原文をそのまま翻訳したものに一部脚注を付け加えたものとなっています。従って、日本独自の法令や基準に関する記述は含まれておりません。また、ガイダンス内で参照されている URL 等は、すべて英語版の記述のままとなっています。

なお、日本クラウドセキュリティアライアンスに関する情報は、以下の URL より参照可能ですのでご覧ください。
https://chapters.cloudsecurityalliance.org/japan/

このガイダンスは、以下の日本クラウドセキュリティアライアンスの有志により作成されています。
（敬称略、順不同）

島崎　眞波
小川　隆一
上村　竜也
山崎　英人
坂　恵理子
二木　真明
江曽　賢一
須崎　有康
前田　卓雄
高橋　郁夫
加藤　雅彦
諸角　昌宏

クラウドコンピューティングのためのセキュリティガイダンス　V3.0

2013年5月8日

はじめに

ここで提供しているガイダンスは、Cloud Security Alliance より 2009 年 4 月に初版をリリースした「**クラウドコンピューティングのためのセキュリティガイダンス**」の第 3 版である。これらのドキュメントは以下に保管されている:

http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf (本ガイダンス)

http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf (ガイダンス　バージョン 2)

http://www.cloudsecurityalliance.org/guidance/csaguide.v1.0.pdf (ガイダンス　バージョン 1)

ガイダンスの第 2 版とは異なって、各章はそれぞれの執筆者が担当し、業界の専門家のレビューを受けている。章の構成と番号付けは、業界標準およびベストプラクティスと揃えられている。このガイダンスの適用を推進することは、クラウドサービスの戦略的マネジメントにおける素晴らしい運用プラクティスになる。この白書とリリース計画は、以下に存在する:

http://www.cloudsecurityalliance.org/guidance/

第 2 版からのその他の変更点として、いくつかの章の名前が変更されている。変更を行ったのは: **第 3 章: 法律問題: 契約と電子的証拠開示**と**第 5 章: 情報管理とデータセキュリティ**である。また、別の章として、**第 14 章: Security as a Service** を追加している。

目次

序文

Cloud Security Alliance の「クラウドコンピューティングのためのセキュリティガイダンス」第 3 版へようこそ。クラウドコンピューティングの発展が続く中、新たなチャンスと新たなセキュリティ課題の両方が生じている。私たちは、新たなリスクを管理する皆様のビジネスニーズをサポートするために、ガイダンスと創造性を提供することを望んでいる。

Cloud Security Alliance は、今までのバージョンのガイダンスを元に、実用的でベストプラクティスな情報を提供している。リスクを軽減しながらビジネスをクラウドサービスに移行するためのツールを提供し続けていくために、本ガイダンスは将来の方向性を示す羅針盤の役割を果たす。V3.0 においては、全世界で 70 人の産業界の専門家からの事実と意見を集めている。私たちは、今後数カ月にわたり、国際支部、パートナーシップ、新たなリサーチおよびカンファレンス活動を含んだ私たちのミッション促進に関する幅広い活動をしていく。私たちの活動は、 www.cloudsecurityalliance.org に掲載されている。

クラウドコンピューティングの安全を確保するための道のりは、グローバルベースの幅広い利害関係者の参加を必要とする長いものである。しかし、私たちが目の当たりにしている進歩は喜んで評価すべきである。新たなクラウドセキュリティソリューションが定期的に現れ、企業は、クラウドサービスプロバイダと関与するために私たちのガイダンスを使用し、コンプライアンスと信頼性に関する健全で公開された議論が世界中で起こっている。私たちが得た最も重要な勝利は、セキュリティの専門家が、単に現状を守ることに関してだけではなく、未来を安全にすることに積極的に携わっているということである。

ぜひ本トピックに関与し続け、私たちと共にこの重要なミッションを完成していただきたい。

よろしくお願いします。

Jerry Archer　　Dave Cullinane　　Nils Puhlmann

Alan Boehme　　Paul Kurtz　　Jim Reavis

The Cloud Security Alliance Board of Directors

謝辞

各章の編集者/寄稿者

第 1 章: Chris Hoff, Paul Simmonds

第 2 章: Marlin Pohlman, Becky Swain, Laura Posey, Bhavesh Bhagat

第 3 章: Francoise Gilbert, Pamela Jones Harbour, David Kessler, Sue Ross, Thomas Trappler

第 4 章: Marlin Pohlman, Said Tabet

第 5 章: Rich Mogull, Jesus Luna

第 6 章: Aradhna Chetal, Balaji Ramamoorthy, Jim Peterson, Joe Wallace, Michele Drgon, Tushar Bhavsar

第 7 章: Randolph Barr, Ram Kumar, Michael Machado, Marlin Pohlman

第 8 章: Liam Lynch

第 9 章: Michael Panico, Bernd Grobauer, Carlo Espiritu, Kathleen Moriarty, Lee Newcombe, Dominik Birk, Jeff Reed

第 10 章: Aradhna Chetal, Balaji Ramamoorthy, John Kinsella, Josey V. George, Sundararajan N., Devesh Bhatt, Tushar Bhavsar

第 11 章: Liam Lynch

第 12 章: Paul Simmonds, Andrew Yeomans, Ian Dobson, John Arnold, Adrian Secombe, Peter Johnson, Shane Tully, Balaji Ramamorthy, Subra Kumaraswamy, Rajiv Mishra, Ulrich Lang, Jens Laundrup, Yvonne Wilson

第 13 章: Dave Asprey, Richard Zhao, Kanchanna Ramasamy Balraj, Abhik Chaudhuri, Melvin M. Rodriguez

第 14 章: Jens Laundrup, Marlin Pohlman, Kevin Fielder

評価者

Valmiki Mukherjee, Bernd Jaeger, Ulrich Lang, Hassan Takabi, Pw Carey, Xavier Guerin, Troy D. Casey, James Beadel, Anton Chuvakin, Tushar Jain, M S Prasad, Damir Savanovic, Eiji Sasahara, Chad Woolf, Stefan Pettersson, M S Prasad, Nrupak Shah, Kimberley Laris, Henry St. Andre, Jim Peterson, Ariel Litvin, Tatsuya Kamimura, George Ferguson, Andrew Hay, Danielito Vizcayno,

K.S. Abhiraj, Liam Lynch, Michael Marks, JP Morgenthal, Amol Godbole, Damu Kuttikrishnan, Rajiv Mishra, Dennis F. Poindexter, Neil Fryer, Andrea Bilobrk, Balaji Ramamoorthy, Damir Savanovic

編集部

Archie Reed: 3, 8, 9 章

Chris Rezek: 2, 4, 5, 7, 13, 14 章

Paul Simmonds: 1, 6, 10, 11, 12 章

CSA スタッフ

Technical Writer/Editor: Amy L. Van Antwerp

Graphic Designer: Kendall Scoboria

Research Director: J.R. Santos

編集者からのレター

過去 3 年間で、Cloud Security Alliance は、120 社の企業メンバーを誘致し、コンプライアンス、グローバルのセキュリティ関連の法律と規約、アイデンティティ管理、クラウドベースの IT サプライチェーンを通したセキュリティのモニタリングと監査を含んだすべてのクラウドセキュリティを扱う幅広い権限を持っている。CSA は、グローバルのセキュリティ標準に焦点を置き、クラウドセキュリティに対する複数の、また、異なった国のポリシーに適合し、国際標準 に批准するための標準化の推進を行っている。

CSA は、クラウドセキュリティ標準の推進役と見られている。そのため、その研究プロジェクトは、迅速に結果を出すために素早い開発技術を使用している。この目的を達成するために、CSA ガイダンス編集チームは、第 3 版となる 「クラウドコンピューティングのためのセキュリティガイダンス」を公開したことを誇りに思っている。この作業は、クラウドを所有し運用するための 14 のドメインを編集した CSA のベストセキュリティプラクティスの集まりである (クラウドアーキテクチャ、ガバナンスとエンタープライズリスクマネジメント、法律問題: 契約と電子的証拠開示、法律問題: 契約と電子的証拠開示、コンプライアンスと監査、情報管理とデータセキュリティ、移植性および相互運用性、従来のセキュリティ、事業継続性、災害復旧、データセンタ運用、インシデントレスポンス、通知および復旧、アプリケーションセキュリティ、暗号化と鍵管理、アイデンティティとアクセス管理、仮想化、Security as a Service).

CSA ガイダンス　第 3 版は、クラウド運用における安定して安全なベースラインを構築しようとしている。これは、管理者がクラウドパラダイムを安全でセキュアに保つための実践的で実行可能なロードマップを提供している。各ドメインは、セキュリティ、安定性、プライバシー、マルチテナント環境での企業ポリシーを強調するように書き直している。

過去 2 年間、ガイダンス 2.1 ではクラウドセキュリティの複数の領域における研究のための基礎を提供してきた。現在展開可能になっている GRC スタックのための TCI アーキテクチャは、前のバージョンのガイダンスで考案されたものである。また、このバージョンでも変更がないことを期待している。ガイダンスは、伝統的なインフラの代替あるいは追加としてクラウドサービスを利用したいと考えている経営者、利用者、実装者のための高いレベルの入門書である。しかしながら、ガイダンスは新しいアイデアを考慮して設計されている。企業家的な考え方を持っている人は、ドメインの作成に加わった執筆者のサービスやアプローチに対して目を向けてこの作品を読むべきである。投資家や会社の意思決定者は、世界中の企業がすでに新しいアイデアと開発のためのロードマップを提供しているように、この作品に興味を持つかもしれない。セキュリティを実践している人や教育者は、この本の要素として、権威と啓蒙の両面があることが分かるであろう。また、産業の進化として、参画している執筆者は影響力がありタイムリーであるという価値を見出している。

第 3 版においては、ガイダンスは構成と内容の両面において、複数の国のクラウド標準開発と並行して構造的な完成を目指している。バージョン 3.0 は、前のバージョンの測定可能で監査可能である実践的な推奨と要求の内容を拡張させている。文書全体を通して使用されている「要求」という用語は、その解釈の仕方が異なっているという点を付記しておく。ガイダンスは、法的義務は負っていないが、仮想的に私たちが描いているすべてのユースケースに対して、ガイダンスでは「要求事項」という用語を選択している。また、ガイダンスは、良く認められている文書と同じ立場にいる。CSA の業界専門編集員は、クラウドプロバイダとテナントの間で測定可能でバランスを保った作業成果物としていくように努めている。コントロールは、共有される物理的なインフラの概念を取り込みながら、テナントのデータ所有権の完全性を守ることにフォーカスしている。ガイダンス　バージョン 3.0 は、Cloud Controls Matrix, Consensus Assessments Initiative, Trusted Cloud Initiative, GRC Stack Initiative という研究プロジェクトとともに、クラウドコンピューティングのダイナミックな特性、業界の学習曲線、新しい開発と深く関わっており、また、包括的なC-レベルに対するベストプラクティスの中に様々な CSA の活動が結びついている。セキュリティガイダンス v3.0 は、世界の標準化団体が開発した新興標準を提供し、

クラウドにビジネス運用をホストしようとするための安全、安定した移行を求めている組織の経営者に提供している。

最後に、Cloud Security Alliance とその編集ワーキンググループを代表して、この新たなガイダンスの作成にあたり、ボランティアとして参加してくださった多くの方々に感謝する。私たちは、彼らが各自のエリアを広げ、かつ改善することに熱心であることに心を動かされ続けた。彼らの努力は、本ガイダンスの内容に大いに真の価値を加えたと信じている。彼らの貢献なくしては本ガイダンスを完成させることはできなかったであろう。私たちは、本ガイダンスについてのあなた方からのフィードバックを切望している。もし、本ガイダンスにおいてあなたの役に立った点、または改善すべき点があった場合は、ぜひ Cloud Security Alliance にメンバーとして、または寄稿者として参加していただきたい。

Paul Simmonds　　Chris Rezek　　Archie Reed

Security Guidance v3.0 Editors

リスクについての編集注記

本ガイダンスを通して、私たちは、クラウドコンピューティングを導入する際にリスクを減らすための幅広い提案を行っている。しかし、全ての提案が必ずしも全てのクラウド展開にとって必要なわけでも、現実的なわけでもない。編集にあたり異なるワーキンググループからの情報をまとめるにつれ、起こりうる全てのリスクシナリオに対する完全な提案を提供するのは無理であることが分かった。クリティカルなアプリケーションが、公共のクラウドサービスプロバイダに移行するには重要すぎるかもしれないのと同時に、低い価値のデータをクラウドベースのストレージに移行する際に、幅広いセキュリティコントロールを適用する必要性は低いか、または全くないかもしれない。

とても多くの異なるクラウド展開オプションが存在するため、１つのセキュリティコントロールのリストで全ての状況をカバーすることはできない。これらのオプションとは、SPI サービスモデル(SPI とは、**S**oftware as a Service, **P**latform as a Service, **I**nfrastructure as a Service のことであり、１章で説明されている)、パブリック対プライベートの展開、内部対外部のホスティング、および様々なハイブリッドへの置換である。他のセキュリティエリアと同様に、組織は、クラウドへの移行およびセキュリティオプションを選択する際に、リスクベースのアプローチを採用すべきである。以下は、初期のクラウドリスクを評価し、セキュリティ上の決定を通知するのに役立つ簡単なフレームワークである。

このプロセスは完全なリスク評価のフレームワークでもなければ、あなた方の全てのセキュリティ要件を決定する方法でもない。あなた方が資産を様々なクラウドコンピューティングモデルに移行する場合の許容範囲を評価するための簡素な方法に過ぎない。

クラウド展開する資産の特定

簡単に言うと、クラウドでサポートされる資産は一般的に以下の２つに分けられる:

1. データ
2. アプリケーション／機能／プロセス

私たちがクラウドに移行するのは、情報か、トランザクション／処理(機能の一部からアプリケーション全体まで)のどちらかである。

クラウドコンピューティングでは、データとアプリケーションが同じ場所に存在する必要はなく、機能の一部のみをクラウドに移行することさえ可能である。たとえば、Platform as a Service を通して機能の一部をクラウドにアウトソースする一方で、アプリケーションとデータを自分のデータセンタでホスティングすることができる。

クラウドのリスクを評価する第一歩は、どのデータまたは機能についてクラウドへの移行を検討するかを正確に特定することである。その際、仕様変更を防ぐため、クラウドに移行した資産の潜在的な利用法も含めるべきである。データおよびトランザクションの量は予想以上に多くなるものである。

資産の評価

次のステップは、移行を検討するデータまたは機能が、その組織にとってどれほど重要であるかを決定することである。あなたの組織に評価プロセスがある場合を除き、詳細な評価を実施する必要はないが、少なくとも

資産がどれほど機密であるか、およびアプリケーション／機能／プロセスがどれほど重要であるかの大体の評価を実施する必要はある。

各資産について、次の質問をしてみよう:

1. その資産が広く一般公開されたり配布されたりした場合、どれほどの被害を受けるか？
2. クラウドプロバイダの社員がその資産にアクセスした場合、どれほどの被害を受けるか？
3. プロセスまたは機能が外部の人間に操作された場合、どれほどの被害を受けるか？
4. プロセスまたは機能が期待した結果を出さない場合、どれほどの被害を受けるか？
5. 情報／データが予期せず変更された場合、どれほどの被害を受けるか？
6. 資産がある期間利用不可能となった場合、どれほどの被害を受けるか？

基本的に、私たちは、その資産に必要な機密性、完全性および可用性を評価しているのであり、資産の全てまたは一部がクラウドで扱われた場合にどのような影響を受けるかを評価しているのである。潜在的なアウトソーシングプロジェクトを評価するのにとてもよく似ており、異なるのは、クラウドコンピューティングでは内部モデルを含み、幅広い展開オプションがあるということである。

潜在的クラウド展開モデルへの資産のマッピング

ここまでで、私たちは既に資産の重要性を理解しているはずである。次のステップは、どの展開モデルが最適かを決定することである。潜在的なプロバイダを検討する前に、様々な展開モデル(プライベート、パブリック、コミュニティまたはハイブリッド)およびホスティングシナリオ(内部、外部、または組み合わせ)に潜んでいるリスクを受け入れることができるかどうかを知っておくべきである：

1. パブリック
2. プライベート　内部／社内(on-premise)
3. プライベート　外部(専用または共有のインフラを含む)
4. コミュニティ　ホスティング場所、潜在的なサービスプロバイダおよび他のコミュニティメンバーを考慮する
5. ハイブリッド　潜在的なハイブリッド展開を有効に評価するためには、コンポーネント、機能およびデータをどこに置くかについて少なくとも大まかなアーキテクチャを考慮しておく必要がある

この時点で、あなた方はクラウド移行にあたって安心できるレベル、およびどの展開モデルと場所があなたのセキュリティとリスク要件に合うかを把握できているはずである。

潜在的クラウドサービスモデルとプロバイダの評価

ここでは、要求されたリスク管理を実施するために、各 SPI レイヤにおいて有するコントロールの度合いに焦点を当てる。もし特定の提案を評価している場合は、この段階で完全なリスク評価に変更するかもしれない。

注目する点は、異なる SPI レイヤにおいてリスク対策を実施するために有するコントロールの度合いとなるだろう。既に具体的な要件(たとえば、規制されたデータの取り扱いなど)がある場合は、それを評価に含むこともできる。

潜在的データフローのスケッチ

具体的な展開オプションを評価する場合、あなたの組織、クラウドサービスおよび利用者／その他のノード間のデータフローを描くべきである。これらのステップの大半はハイレベルなものであっても、最終決断をする前に、データがどのようにクラウドに入ったり出たりするのかを理解することは絶対に不可欠である。

もしまだ特定の提案を検討していない場合は、受け入れ可能リストのどのオプションにおいても、大まかなデータフローを描くべきであろう。これにより、あなたは最終決定を行う際に、リスクのポイントを確認することができるようになる。

結論

この時点で、クラウドへの移行を検討しているデータまたは機能の重要性、リスク許容度(少なくともハイレベルでの)およびどの展開とサービスモデルの組み合わせを受け入れることができるかを理解できたであろう。また、機密情報と運用に関する潜在的な脅威のポイントについて大まかには把握できたであろう。

これらにより、本ガイダンスにある他のセキュリティコントロールを評価するために十分な背景をあなたは得ているであろう。低い価値を有した資産である場合、同じレベルのセキュリティコントロールは不要であり、オンサイト検査、開示可能性および複雑な暗号化スキームのような多くの忠告をスキップすることができる。高い価値を有し、管理された資産は、監査やデータの保有に関する要件を必要とするかもしれない。管理されていないが、高い価値を有した資産の場合は、技術的なセキュリティコントロールに焦点が当てられるかもしれない。

紙面は限られている中、カバーする題材が深く広いこともあり、本ガイダンスにはセキュリティ推奨の広範なリストが含まれている。すべてのクラウド展開において、それぞれのセキュリティとリスクコントロールが必要なわけではない。あなたのリスク許容度と潜在的な脅威を事前に評価することにより、あなたの組織における最善のオプションと展開を選択するための背景を得ることができるだろう。

セクション I //
クラウド
アーキテクチャ

第 1 章 //
クラウドコンピューティングのアーキテクチャフレームワーク

この章(クラウドコンピューティングのアーキテクチャフレームワーク)は、本ガイダンスの他の部分のための概念的なフレームワークを提供する。この章の内容は、特に IT ネットワークとセキュリティの専門家の視点に基づいてクラウドコンピューティングというものを記述することに焦点をあてている。

この章の最後のセクションで、他の章の簡潔な概要を述べている。

この章で記述されているアーキテクチャフレームワークを理解することは、本ガイダンスの他の部分を理解するための重要な第一歩である。このフレームワークは、他の章の中で使用される概念と用語の多くを定義している。

概要. 以下の 3 つのセクションは、このアーキテクチャ的な視点を定義している:

- 一貫した語彙を提供するためのガイダンスを通して使用される用語
- クラウドアプリケーションとサービスを安全に保つためのアーキテクチャ要件および課題
- クラウドサービスとアーキテクチャの分類を説明する参照モデル

1.1 クラウドコンピューティングとは何か?

クラウドコンピューティングは、ユビキタス、利便性、および、コンピュータ資源（たとえば、ネットワーク、サーバ、ストレージ、アプリケーション、サービス）を構成可能にするシェアードプールへのオンデマンドネットワークアクセスを実現するためのモデルである。クラウドコンピューティングは、潜在的に協調、迅速性、スケーリング、可用性を高める破壊的技術である。また、これは最適化され、効率的なコンピューティング環境を通して、コスト削減の機会を提供する。クラウドモデルは、コンポーネントが素早く組織化され、提供され、導入され、廃棄される世界を想像させる。また、オンデマンドのユーティリティ的なモデルにより、割り当て、利用のスケールアップ、スケールダウンができる世界を想像させる。

アーキテクチャの観点では、クラウドと既存のコンピューティングモデルとの類似点および相違点、また、これらの類似点と相違点がネットワークと情報セキュリティ対策への組織、運用、技術面におけるアプローチに与える影響について大きな混乱がある。伝統的なコンピューティングとクラウドコンピューティングの境界はほとんどない。しかしながら、クラウドコンピューティングは、データセキュリティ、ネットワークセキュリティ、情報セキュリティに対する優れた実践への組織的、運用的、技術的な取り組みに対して影響を与えている。

現在、学術的な観点、アーキテクトの観点、エンジニアの観点、開発者の観点、管理者の観点、さらに利用者の観点からクラウドを定義しようという試みがある。本ガイダンスでは、IT ネットワークとセキュリティの専門家に特有の観点からの定義に焦点を当てている。

1.2 クラウドコンピューティングの構成要素とは？

このクラウドセキュリティアライアンスのガイダンスでは、クラウドコンピューティングに対する米国標準技術局(**NIST**)[1]の科学者による公開に向けての作業と、クラウドコンピューティングの定義付けに対する努力に基づいた定義を用いている。

NIST の出版物は一般によく受け入れられている。 本ガイダンスの作成にあたっては、クラウドコンピューティングに対する NIST Working Definition of cloud computing (これを書いている時点では NIST 800-145)と合わせることにより、共通の言葉による一貫性とコンセンサスをもたらし、意味づけよりも使用事例に焦点を当てるようにした。

本ガイダンスが、グローバルな組織において幅広く使用可能で適用可能になるように試みていることは重要である。NIST は米国の政府組織であり、この参照モデルを選択するにあたっては、別の観点や地理的な要素にも配慮するべきである。

NIST は、クラウドコンピューティングを 5 つの基本特性、3 つのクラウドサービスモデルおよび 4 つのクラウド展開モデルにより定義している。それらは、図 1 に視覚化された形で要約され、その後で詳細に説明されている。

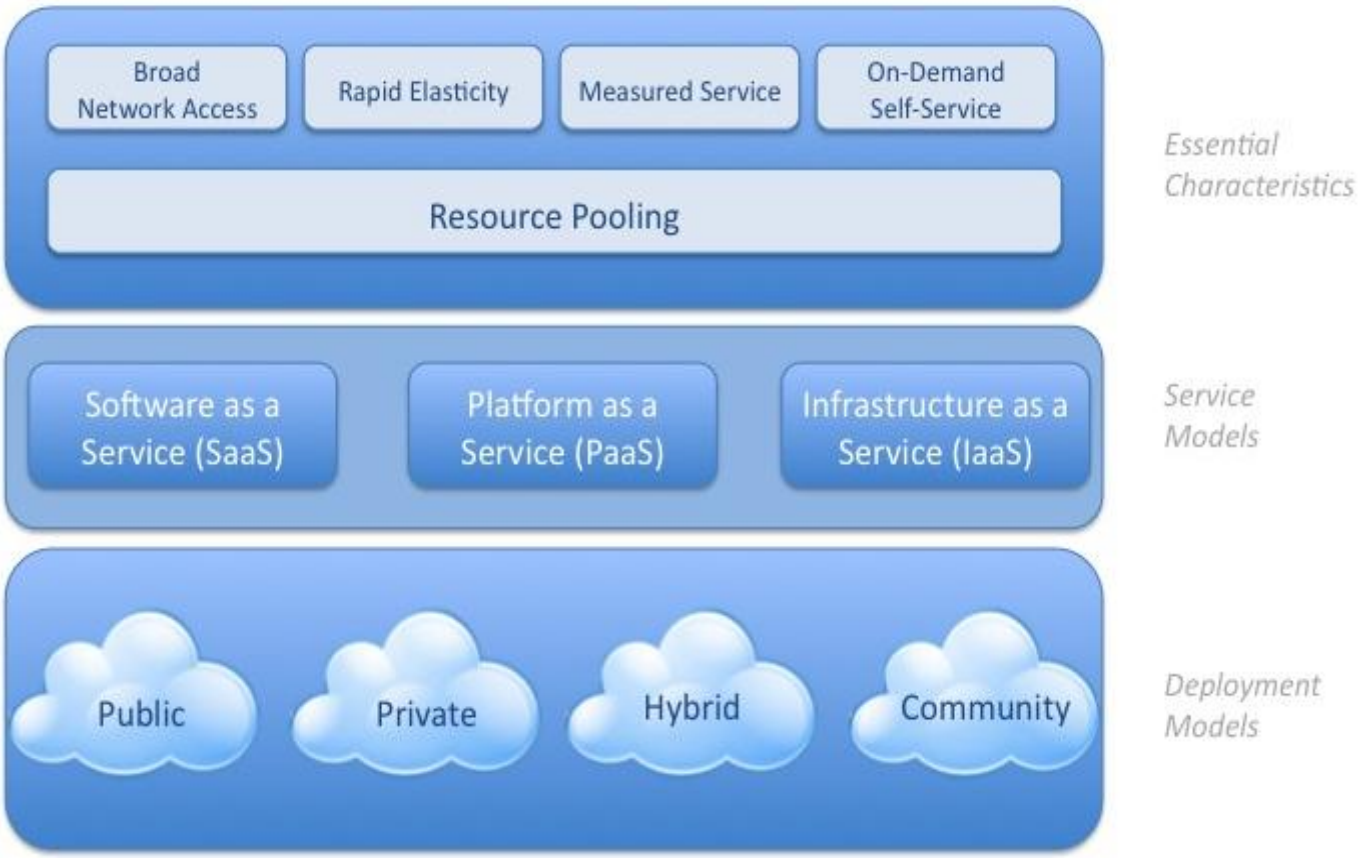


図 1—NIST Visual Model of Cloud Computing Definition[2]

1.3 クラウドコンピューティングの特性

[1] **NIST** - National Institute of Standards and Technology

クラウドサービスが、しばしば仮想化技術とともに、あるいは、仮想化技術により利用可能にされていることを理解することは重要である。しかし、リソースの抽象化と仮想化技術を結びつける必要はないし、多くの製品では、ハイパーバイザーやオペレーティングシステムコンテナによる仮想化は利用されていない。

さらに、マルチテナント性であることは、NIST におけるクラウドの基本特性として挙げられていないが、しばしばそうであると議論されているということに注意すべきである。NIST モデル におけるクラウドコンピューティングの基本特性として挙げられていないとしても、CSA はマルチテナント性をクラウドの重要な要素として認識している。

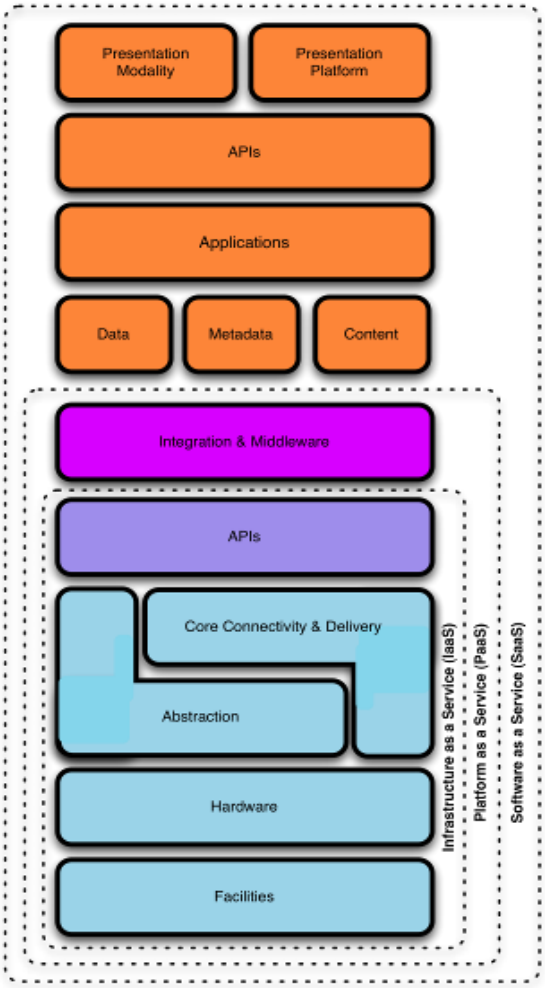


図 2—Multi-Tenancy

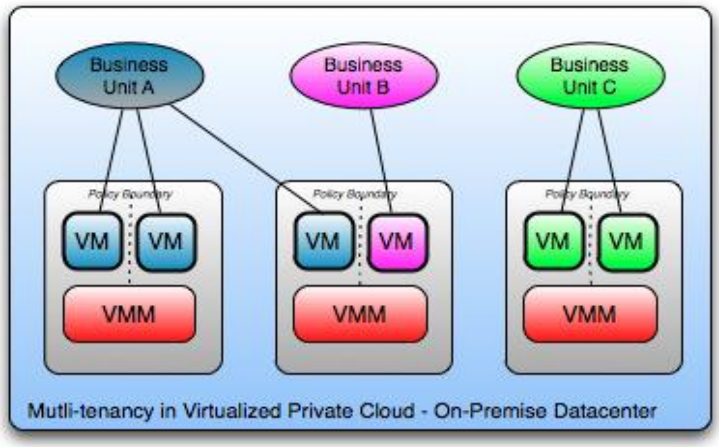
1.4 マルチテナント性

本ガイダンスでは、マルチテナントを重要な要素と考えている。以下のセクションでは、クラウドコンピューティングの重要な要素について、CSA の理解と定義の概要を記述している。

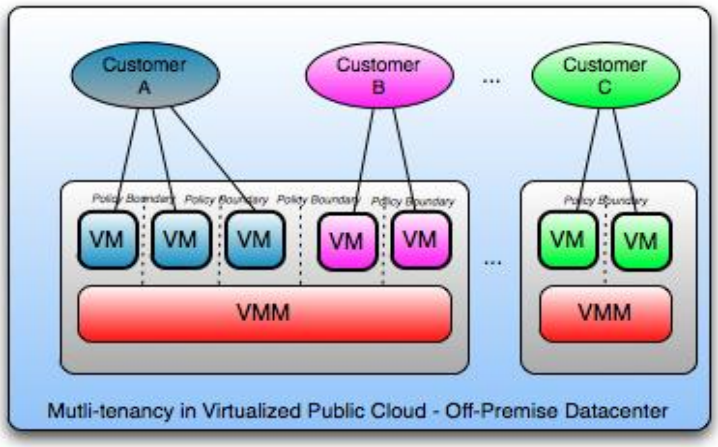
単純な形式のマルチテナント性は、同じリソースと同じアプリケーションを複数の利用者が使用するということである。ここで、利用者とは同じ組織の人かもしれないし異なった組織の人かもしれない。マルチテナント性のインパクトは、関わりのないデータや他の利用者すなわちテナントの運用履歴が見えてしまう可能性があることである。

クラウドサービスモデルにおけるマルチテナント性は、異なる利用者層のための、ポリシーに基づいた実施や、区分け、分離、ガバナンス、サービスレベル、支払取り消し／請求のモデルの必要性を含んでいる。

利用者は、個々のユーザごとに提供されるクラウドプロバイダのサービスを利用するか、プライベートクラウドとしてホスティングされたインスタンスを利用するかを選択するかもしれない。組織は、共通のインフラを



Private Cloud of Company XYZ with 3 business units, each with different security, SLA, governance and chargeback policies on shared infrastructure



Public Cloud Provider with 3 business customers, each with different security, SLA, governance and billing policies on shared infrastructure

共有している異なったビジネスユニットとしてユーザを区分するかもしれない。

プロバイダの観点では、マルチテナント性は、規模の経済性、可用性、管理、区分け、分離、および効率的な運用を可能にするためのアーキテクチャとデザインへのアプローチであり、多くの異なった利用者に対してインフラ、データ、メタデータ、サービスおよびアプリケーションの共有を促進している。

マルチテナント性には、プロバイダのクラウドサービスモデルごとに異なった定義が可能である。マルチテナントは、上記のインフラ、データベースまたはアプリケーションレベルで説明した機能を可能にするかもしれないからである。例としては、 Infrastructure-as-a-Service (**IaaS**)[2] , Software-as-a-Service (**SaaS**)[3], Platform as a Service (**PaaS**)[4] ではマルチテナントの実現方法に違いが見られる点がある。

クラウド展開モデルは、マルチテナント性に対して別の重要性を持っている。しかし、プライベートクラウドの場合でさえ、１つの組織には、サードパーティのコンサルタントや契約者が多数いるかもしれない。また、事業単位ごとに高度に論理的な分離を希望する可能性もある。したがって、マルチテナント性の懸念点を常に考慮するべきである。

1.5 クラウド参照モデル

クラウドコンピューティングのモデル間の関係と依存性を理解することは、クラウドコンピューティングのセキュリティリスクを理解する上で重要である。IaaS はすべてのクラウドサービスの基盤であり、PaaS は IaaS 上に作られており、SaaS はクラウド参照モデルの図で説明されているように PaaS 上に作られている。機能が継承されるのと同様に、情報セキュリティの問題とリスクも継承される。商業用クラウドプロバイダは、その階層化されたサービスモデルにきちんと収まらない可能性があることに注意する必要がある。それでもなお、実世界にあるサービスをアーキテクチャフレームワークに関連づけ、セキュリティ分析を必要とするリソースとサービスを理解するために、この参照モデルは重要である。

IaaS は、施設からそこに設置されているハードウェアプラットフォームまでを含んだ全体的なインフラのリソーススタックからできている。さらに、IaaS は、機能を抽象化する(あるいはしない)機能と、リソースに対する物理的あるいは論理的な接続性を提供する機能を包含する。つまり、IaaS は、サービスの利用者がインフラに対する管理やその他の相互のやり取りを行うための **API**[5]を提供する。

PaaS は IaaS の上に位置し、アプリケーション開発用フレームワーク、ミドルウェア機能およびデータベース、メッセージング、キューイングのような機能を統合するためのレイヤを提供している。これらのサービスにより、開発者は、プログラミング言語とツールがスタ

Infrastructure as a Service (IaaS), ストレージやネットワークとともに、プラットフォーム仮想化環境のようなコンピュータインフラをサービスとして提供する。サーバ、ソフトウェア、データセンタのスペース、ネットワーク機器、クライアントを購入する代わりに、これらのリソースをすべてアウトソースサービス化する。

Software as a service (SaaS), 「オンデマンドソフトウエア」と呼ばれることがあり、ソフトウエアと関連するデータを中央（一般的には（インターネット）クラウド上）にホストするソフトウエア提供モデルである。利用者はシンクライアントを使用し、ウェブブラウザを用いてインターネット越しに利用する。

Platform as a service (PaaS), コンピューティングプラットフォームやソリューションスタックをサービスとして提供する。PaaS は、下位のハードウエア、ソフトウエア、ホスティング機能の提供方法を購入あるいは管理するコストや複雑さ無しにアプリケーションを提供する機能を備えている。これは、インターネットから利用可能なすべてのウェブアプリケーションやサービスの構築や展開を行う完全なライフサイクルをサポートするために必要となるすべての機能を備えている。

[2] **IaaS** - Infrastructure as a Service
[3] **SaaS** - Software as a Service
[4] **PaaS** - Platform as a Service
[5] **API** - Application Programming Interface

ックとしてサポートされているアプリケーションをプラットフォーム上に構築することができる。

SaaS は、IaaS と PaaS スタックの上に作られ、内包した運用環境を提供している。これは、コンテンツ、プレゼンテーション、アプリケーションと管理機能を含んだ全体的なユーザ環境を提供している。

したがって、それぞれのモデルには統合機能、複雑性対公開性(拡張性)およびセキュリティにおいて重要なトレードオフがあることは明らかである。一般に、SaaS は製品に直接組み込まれた統合機能を最も多く提供し、利用者側の拡張性は最小であり、比較的高いレベルのセキュリティ(少なくともプロバイダ側がセキュリティに対する責任を負う) を提供する。

PaaS は、開発者にプラットフォーム上で開発者独自のアプリケーションを構築させることを意図している。結果として、利用者がすぐに利用できる機能を削減することで SaaS より拡張性が高い傾向にある。このトレードオフは、セキュリティ機能や能力にも及ぶ。PaaS では、作りこみの機能は完全ではないが、セキュリティのレイヤを追加することに対する柔軟性は高い。

IaaS は、アプリケーションのような機能をわずかしか提供しないが、拡張性が非常に高い。このことは、一般に、インフラ自身を守るセキュリティ機能や能力はほとんど持っていないということを意味する。このモデルでは、OS、アプリケーションおよびコンテンツがクラウド利用者によって管理され、安全に保たれている必要がある。

セキュリティアーキテクチャについての重要なポイントは、クラウドサービスプロバイダが提供するモデルのレイヤが下に行くほど、利用者が実装あるいは管理しなければならないセキュリティの機能と管理が増大するということである。

service level agreement (**SLA**)[6]が利用者に提示された時、サービスとプロバイダに対するサービスレベル、セキュリティ、ガバナンス、コンプライアンスおよび法的責任に対して期待される点が、契約上規定され、管理され、強制される。2 つのタイプの SLA、交渉可能と交渉不可能がある。SLA なしには、利用者は利用者の管理下においてクラウドのすべてを管理することになる。交渉不可の SLA が提示された時、プロバイダはこの部分を合意事項として扱う。PaaS あるいは IaaS の場合は、プロバイダには、基本サービスの可用性およびセキュリティを確保するため、プラットフォームおよびインフラのコンポーネントを安全にするための一部の埋め合わせが期待されるものの、SLA に記載されている残りのサービスを効果的に管理することは利用者側のシステム管理者の責任である。どちらの場合においても、実施責任は譲渡／移転できるが、必ずしも説明責任も譲渡／移転できるわけではないということは明確である。

それぞれのクラウド展開モデルについて、スコープや特定の機能を狭めていくか、あるいは各モデル間のサービスや能力をつなげていくと、派生した分類をもたらすかもしれない。たとえば、「Storage as a Service」は IaaS 系の中の一つの形態である。

成長し続けるクラウドコンピューティングソリューションをより広く検討することは、本ガイダンスの範囲外であるが、以下の図で示す OpenCrowd クラウドソリューションの定義・分類は素晴らしい出発点を提供している。OpenCrowd の定義・分類は、これまでに定義したそれぞれのモデルを超えて、さらに増え続ける今日のソリューションを示している。しかしながら、CSA は、以下に示されているソリューションや会社のいずれに対しても特別な支持をしておらず、今日利用可能な提供サービスの多様性を説明するためにこの図を提示している。

[6] **SLA** - Service Level Agreement

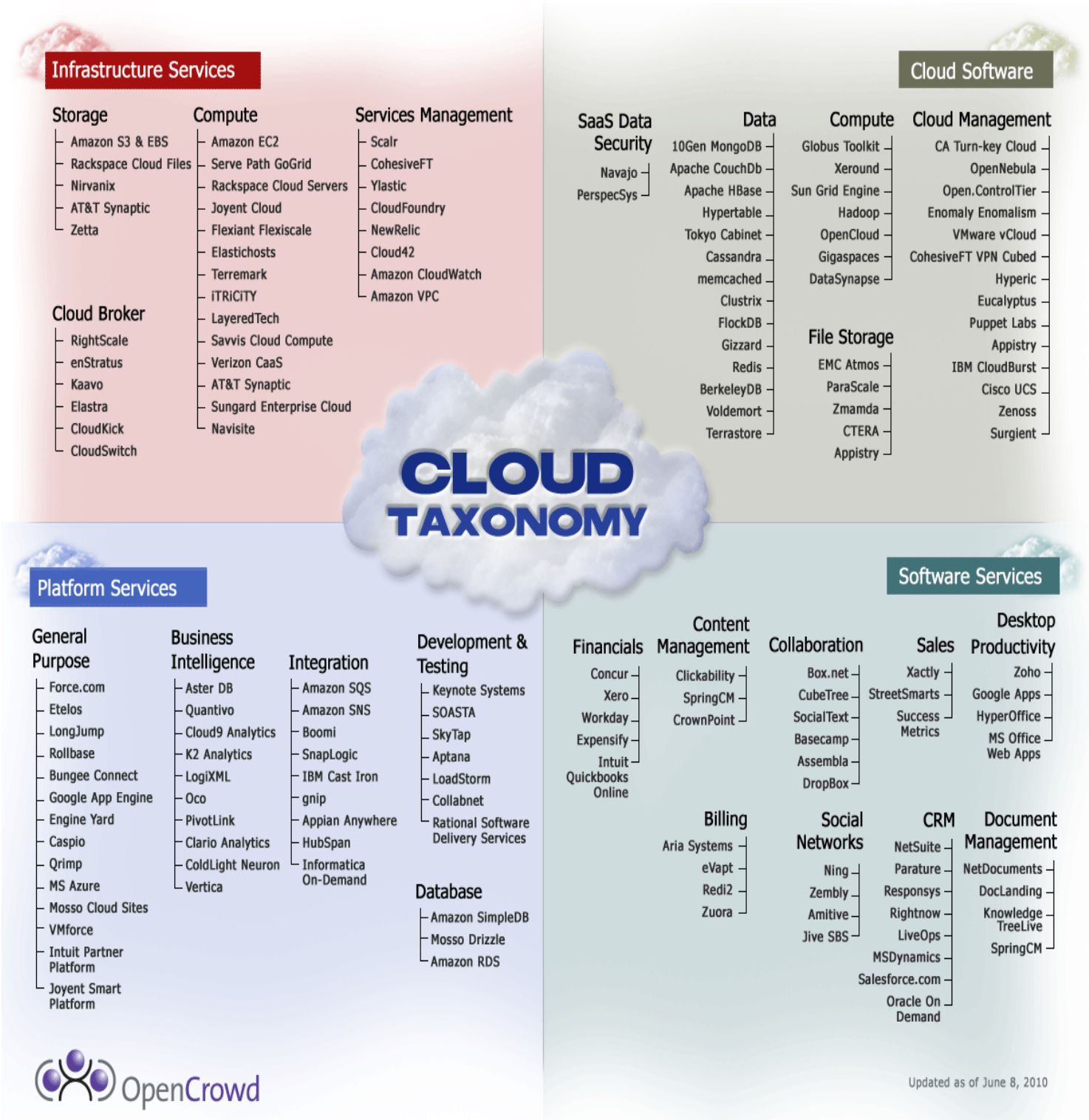


図 3 – OpenCrowd Taxonomy[7]

多くのクラウドコンピューティングのユースケースに関する優れた概要を作成するため、Cloud Computing Use Case Group は、「クラウド利用者およびクラウドベンダと共にクラウドコンピューティングの一般的な使用事例を定義し、相互作用性、統合の容易さ、および移植性を確保するために、クラウド環境で標準化される必要がある機能および要件を明らかにする」という目的のもと、一般的な事例を説明および定義し、クラウドの利点を説明するため、共同研究を行った。

[7] http://www.opencrowd.com/assets/images/views/views_cloud-tax-lrg.png

1.5.1 クラウドセキュリティ参照モデル

クラウドセキュリティ参照モデルは、クラス間の関係性を説明し、関連するセキュリティコントロールや懸念事項に応じてクラスを定義している。クラウドコンピューティングに初めて取り組む組織や個人は、以下の潜在的な落とし穴や混乱を避けることが重要である:

- クラウドサービスがどのように展開されるかという概念は、しばしば、それがどこに提供されるかという概念と混同して使われており、混乱を引き起こしている。たとえば、パブリックとプライベートのクラウドが、「外部」と「内部」のクラウドと呼ばれることがあるが、これは全ての状況において必ずしも正確ではない。

- クラウドサービスの利用形態は、しばしば組織の管理または境界セキュリティ(通常、良く知られた境界線の存在によって定義される)の位置に関連して説明されている。セキュリティ境界が、クラウドコンピューティングにおいてどこに位置しているかを理解することは重要である一方、明確な境界が存在するという考えは、ほとんどの組織において時代遅れの概念である。

- 企業において既に起こっている信頼境界の再境界化および侵害は、クラウドコンピューティングによって増幅され、加速される。ユビキタスな接続性、無定形な情報のやりとりおよび従来の静的なセキュリティコントロールの無効性は、動的な性質を持つクラウドサービスに対応できない。これらはすべて、クラウドコンピューティングに対する新しい考え方を必要としている。The Jericho Forum[8]は、多くのケーススタディを含む企業ネットワークの再境界化についての多くの資料を作り出した。

このように、クラウドの展開と利用方法は、資産、リソースおよび情報の物理的な場所に関する「内部」または「外部」か、の状況だけではなく、それらが誰によって利用されているか、そして、誰がポリシーと標準に対するガバナンス、セキュリティおよびコンプライアンスに責任を持つかということも合わせて考慮されるべきである。

このことは、資産、リソースおよび情報が存在する場所が社内(on-premise)であるか社外(off-premise)であるかどうかが、セキュリティおよび組織のリスク管理に影響を与えないということを示しているわけではなく(実際には影響は与える)、リスクは以下のことにも依存するということを強調しているのである：

- 管理される資産、リソースおよび情報のタイプ
- 誰がどのように管理するか
- どのコントロールが選択され、どのように統合されているか
- コンプライアンスの問題

たとえば、Amazon の AWS EC2 で展開される **LAMP**[9]スタックは、パブリック、社外(off-premise)、サードパーティによって管理される IaaS ソリューションとして分類されるであろう。それは、その中に含まれたインスタンスとアプリケーション／データが、利用者またはサードパーティによって管理される場合においても同様である。また、会社のコントロール、管理、および所有権のもとで Eucalyptus 上に展開された、複数の事業単位に提供されるカスタムアプリケーションスタックは、プライベート、社内(on-premise)、そして、自己が管理する SaaS ソリューションとして分類できる。この 2 つの例は、クラウドの弾力性によるスケーリングとセルフサービス機能を活用している。

[8] http://www.jerichoforum.org
[9] LAMP-Linux (operating system), Apache HTTP Server, MySQL (database software) and Perl/PHP/Python, the principal components to build a viable general purpose web server

以下の表はこれらのポイントをまとめている:

表1—クラウドコンピューティング展開モデル

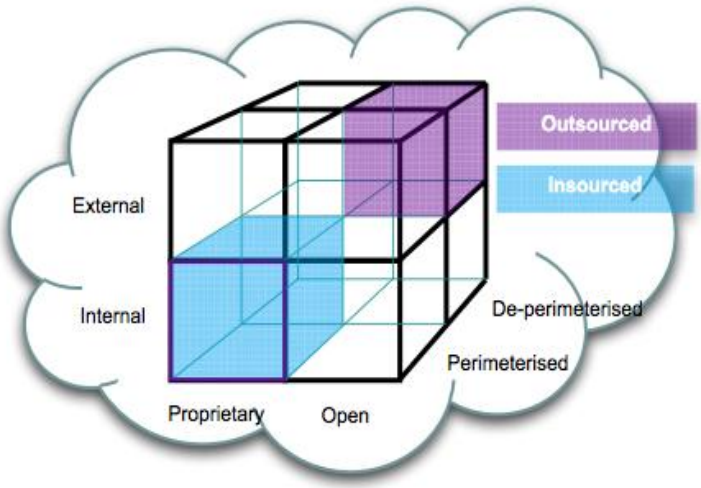
	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Or Organization / Third Party Provider	Organization / Third Party Provider	On-Premise / Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

[1] *Management includes: governance, operations, security, compliance, etc…*
[2] *Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment*
[3] *Infrastructure Location is both physical and relative to an Organization's management umbrella and speaks to ownership versus control*
[4] *Trusted consumers of service are those who are considered part of an organization's legal/contractual/ policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.*

クラウドサービスモデル、展開モデル、リソースの物理的な場所、管理と所有権の特性がどのように組み合わされているかを見える化するためのもう一つの方法として、以下の右側の図に示した Jericho Forum のクラウドキューブモデル[10]がある:

クラウドキューブモデルは、クラウドが今日提供している利用可能な組み合わせを示し、各クラウドの「構成」および提供方法を区別するための 4 つの評価基準／次元を提示している。これにより、クラウドコンピューティングがセキュリティへのアプローチ方法にどのように影響するかを理解することができる。

また、クラウドキューブモデルは、クラウドモデルを理解すること、また、これをコントロールフレームワークや ISO／IEC 27002 のような規格にマッピングすることの難しさを浮き彫りにし、「…組織におけるセキュリティ管理を開始し、導入し、維持し、改善するための一連のガイドラインや一般的な原理」を提供している。



The Cloud Cube Model

図 4—Jericho Cloud Cube Model

[10] http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

ISO／IEC27002 のセクション 6.2 「外部組織」のコントロール目標は、次のように記載されている。「…組織の情報と情報処理設備のセキュリティは、外部組織の製品やサービスの導入によって削減されるべきではない…」。

このように、3 つのクラウドサービスモデルを安全に保つための方法と責任の違いは、クラウドサービスの利用者が困難な試練に直面していることを意味する。クラウドプロバイダが、速やかにセキュリティコントロールおよびそれをどの程度利用者に対して実装しているかを公開し、また、利用者が情報セキュリティを維持するためにどのようなコントロールが必要であるかを理解しない限り、誤った意思決定や有害な結果をもたらす可能性が非常に多くなる。

重要な点としては、まず、クラウドサービスをクラウドアーキテクチャモデルに沿って分類する。そうすると、ギャップ分析の実践として、セキュリティアーキテクチャにマッピングすることができるようになる。同様に、ビジネス、規制、その他のコンプライアンス要件に対してもマッピングすることができる。結果として、そのサービスの全体的な「セキュリティ」に対する姿勢を特定したり、資産の保証と保護に関する要件にどのようにかかわっているかを特定したりすることできる。

以下の図では、クラウドサービスのマッピングが、どのように対象となるコントロールの一覧と比較することができるかについて例を示している。これは、利用者、クラウドサービスプロバイダあるいはサードパーティ機関のいずれかが提供するコントロールのうち、どのコントロールが存在し、どのコントロールが存在しないかを特定するためのものである。これは、以下の図が示すように、コンプライアンスのフレームワークあるいは PCI DSS のような一連の要件と比較することができる。

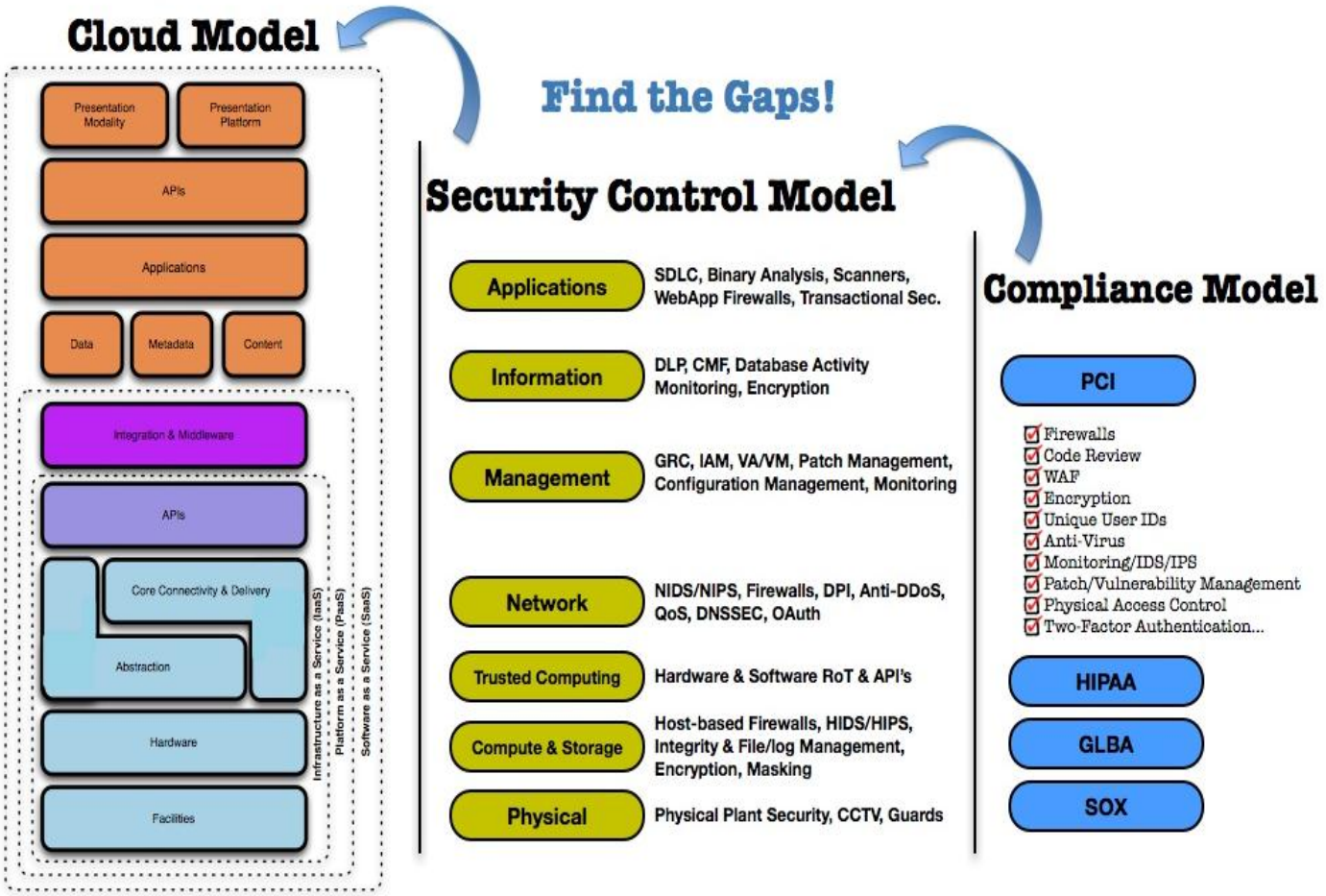


図5—クラウドモデルをセキュリティコントロールとコンプライアンスにマップ

一度、何らかの規制またはその他のコンプライアンス要件に対してこのギャップ分析を完成させると、リスク評価フレームワークにフィードバックするために行わなければならないことを特定することが容易になる。これは、今度はギャップに、そして最終的にはリスクに対してどのように対処: 受容、移転または緩和、するべきかの決定に役立つ。

クラウドコンピューティングを運用モデルとして使用することは、本質的にコンプライアンスを達成したり妨げたりすることはないということに注意するのは重要である。どのような要件に対しても準拠する能力は、サービス、使用されている展開モデルならびに対象範囲にあるリソースのデザイン、展開や管理によるものである。

上記で示した一般的なコントロールフレームワークの概要に関しては、Open Security Architecture Group[11]のセキュリティアーキテクチャパターン文書の「landscape」、あるいは、NIST800-53 revision3 で推薦されている Security Controls for Federal Information Systems and Organizations のセキュリティコントロールカタログに分かり易い説明がある。

1.5.2 クラウドコンピューティングのためのセキュリティとは何か?

クラウドコンピューティングにおけるセキュリティコントロールは、IT 環境におけるセキュリティコントロールとほとんど変わらない。しかし、使用されているクラウドサービスモデル、運用モデルおよびクラウドサービスの使用を可能にする技術により、クラウドコンピューティングは従来の IT ソリューションと異なったリスクをもたらす可能性がある。

組織のセキュリティに対する姿勢は、実装されているセキュリティコントロールの成熟度、有効性および完全性によって特徴付けられる。これらのコントロールは、施設(物理的なセキュリティ)からネットワークインフラ(ネットワークセキュリティ)、IT システム(システムセキュリティ)、情報とアプリケーション(アプリケーションセキュリティ)まで複数のレイヤに渡って実装される。さらに、コントロールは、職責の分離や変更管理など、人とプロセスのレベルにも実装される。

本ガイダンスで前述したように、プロバイダと利用者それぞれが負うセキュリティに関する責任の範囲は、クラウドサービスモデルごとに大きく異なる。例として、Amazon の AWS EC2 infrastructure as a Service は、ハイパーバイザーまでのセキュリティの責任をベンダが負っている。つまり、ベンダは物理的なセキュリティ、環境のセキュリティおよび仮想化のセキュリティのみを扱う。そして、利用者は、OS、アプリケーションおよびデータを含む IT システム(インスタンス)に関連したセキュリティコントロールに対して責任を負う。

Salesforce.com のカスタマリレーションシップマネジメント(CRM)SaaS では状況が逆になる。全体の「スタック」が Salesforce.com によって提供されるため、プロバイダは物理的および環境のセキュリティコントロールに対して責任を負うだけでなく、インフラ、アプリケーションおよびデータのセキュリティコントロールにも対応しなければならない。このことは、利用者の直接的な運用責任の多くを緩和している。

経験の少ないクラウドサービスの利用者にとって、このガイダンスを読むことが手助けになるけれども、責任範囲はどこまであるのかを理解することは簡単ではない。しかしながら、CSA や他の団体がクラウド監査の標準化を進めようとしている。

クラウドコンピューティングの魅力の 1 つは、規模の経済性、再利用および標準化による費用効率の良さである。これらの効率化を実現するため、クラウドプロバイダは可能な限り多くの利用者にサービスを提供するた

[11] www.opensecurityarchitecture.org

めの十分な柔軟性を保ち、対応可能なマーケットを最大化しようとする。残念ながら、セキュリティをこれらのソリューションに統合することは、しばしば柔軟性を低減させてしまうと認識されている。

この柔軟性の弱さにより、しばしばクラウド環境では従来の IT と同等のセキュリティコントロールを展開することができない。これは、多くの場合、インフラの抽象化や、特にネットワークレイヤにおいて、よく知られたセキュリティコントロールを統合するための可視性や能力が欠如していることに起因している。

以下の図は、これらの問題を表現している: SaaS 環境においては、セキュリティコントロールとそれらの範囲はサービス契約として取り決められる。サービスレベル、プライバシーおよびコンプライアンスは、すべて契約において法的に対処されるべき問題である。IaaS 提供においては、インフラと抽象化レイヤのセキュリティに対する責任はプロバイダ側にあるが、残りのスタックについては利用者の責任となる。PaaS は、それらの中間で、プラットフォームのセキュリティはプロバイダの責任であるが、プラットフォーム上に開発されたアプリケーションのセキュリティおよびやそれらのアプリケーションを安全に開発することは利用者側の責任である。

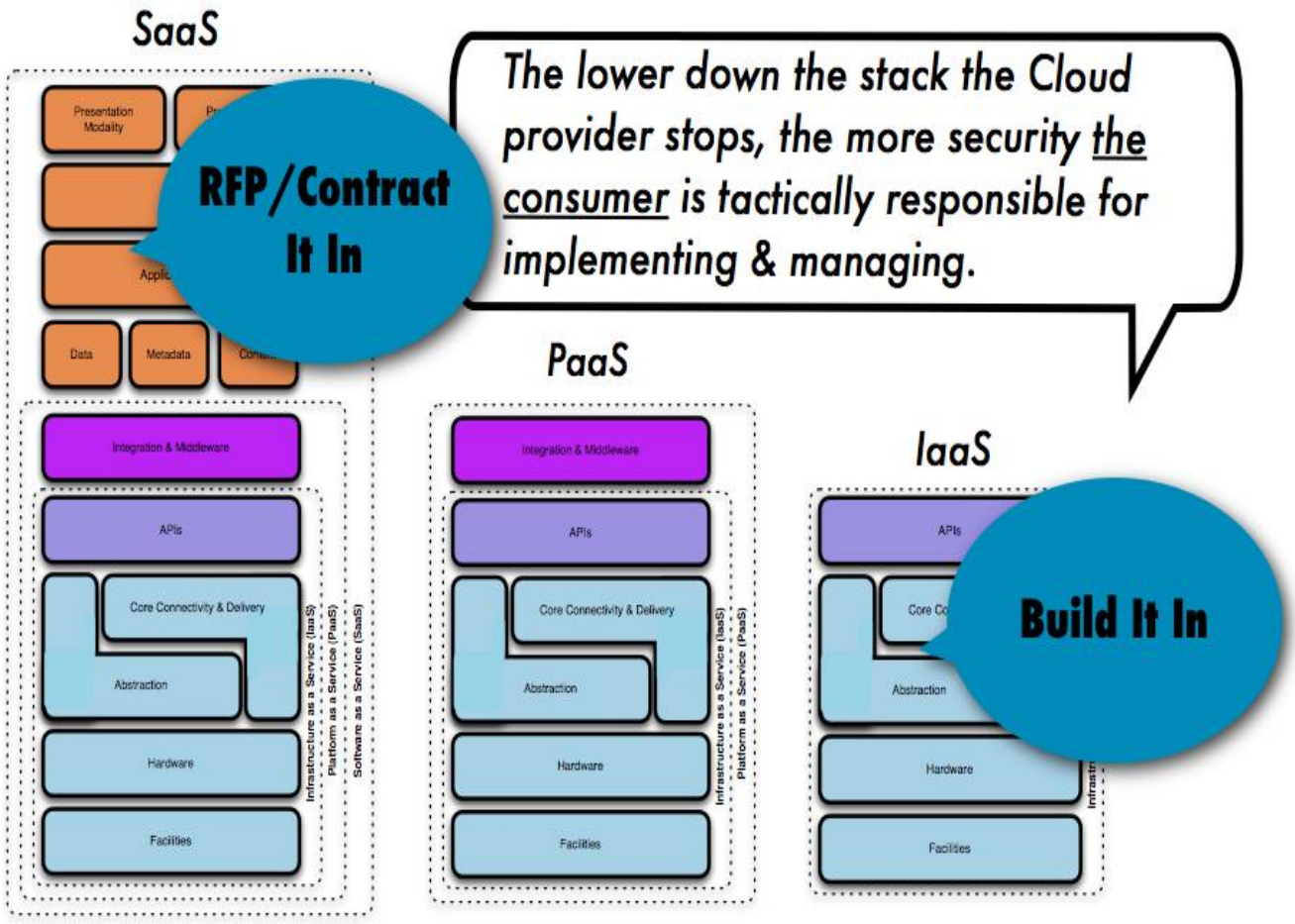


図6—セキュリティはどのように統合されるか

サービスモデルおよび展開方法の違いによるインパクトを理解することは、組織のリスクに対する姿勢を管理する上で重要である。

1.5.3 アーキテクチャを超えて: 重要なフォーカスエリア

CSA ガイダンスの残りの部分を構成している 13 の章は、クラウドコンピューティングにおける懸念点を浮き彫りにし、クラウド環境におけるセキュリティの「痛点」を戦略的、戦術的に扱い、クラウドサービスと展開モデルのどのような組み合わせにも適用できるようにしている。

各章は、ガバナンスと運用という 2 つの広義のカテゴリに分割されている。ガバナンスの章は幅広くクラウドコンピューティング環境における戦略的で政策的な問題を扱っている。一方、運用の章は、アーキテクチャにおけるより戦術的なセキュリティの問題と実現方法に焦点を当てている。

表 2a— ガバナンスの章

章	ガイダンスの取組み...
ガバナンスとエンタープライズリスクマネジメント	クラウドコンピューティングの導入によりエンタープライズリスクを統治し、測定する組織の能力。合意違反の際の法的な優先権、ユーザ組織によるクラウドサービスプロバイダのリスクを適切に評価できる能力、利用者とプロバイダの両者に過失がある場合の機密データ保護責任および国際的な境界がこれらの問題にどのように影響するか、などの項目を取り上げている。
法律問題: 契約と電子的証拠開示	クラウドコンピューティングを利用する際の潜在的な法的問題。このセクションで触れられている問題は、情報およびコンピュータシステムのための保護要件、セキュリティ違反の情報開示法、法的な要求事項、プライバシー要件、国際法などを含む。
コンプライアンスと監査	クラウドコンピューティングを使用する際のコンプライアンスの維持と証明。クラウドコンピューティングが、社内のセキュリティポリシーやその他さまざまなコンプライアンス要件(規制、立法、その他)へのコンプライアンスに与える影響の評価方法に関する問題がここでは議論されている。この章は、監査に際してコンプライアンスを証明するためのいくつかの方向性を含む。
情報管理とデータセキュリティ	クラウドに置かれているデータの管理。クラウド上のデータの認識とコントロールに関する項目や、クラウドにデータを移す際に失われる物理的なコントロールを補償するコントロールについて取り上げている。その他に、データの機密性、完全性および可用性に対する責任の所在についても言及している。
移植性および相互運用性	あるプロバイダから別のプロバイダへデータ／サービスを移行する、または社内に戻す能力。プロバイダ間の相互運用性に関わる問題についても論じている。

表 2b – 運用の章

章	ガイダンスの取組み...
従来のセキュリティ、事業継続性、災害復旧	セキュリティ、事業継続性および災害復旧を実装するために現在使用されている運用プロセスや手続きに対して、クラウドコンピューティングがどのように影響を与えるか。クラウドコンピューティングに起こりうるリスクについて論じ、分析することに焦点を当てている。これは、より優れたエンタープライズリスク管理モデルに対する需要についての話し合いや議論が増えることを期待してのことである。さらに、このセクションでは、クラウドコンピューティングをセキュリティリスクの低下に活用できる箇所や、クラウドコンピューティングによりセキュリティリスクが増加してしまう箇所を特定するために役立つ内容にも触れている。
データセンター運用	プロバイダのデータセンタのアーキテクチャや運用を評価する方法。主に、ユーザが、稼働中のサービスにとって有害である特性や、長期間の安定性の基本となる特性など、一般的なデータセンタの特性を認識することを助けることに焦点を当てている。
インシデントレスポンス、通知および復旧	正確で適切なインシデントの発見、対応、通知および復旧。これは、プロバイダとユーザの双方のレベルにおいて、正確なインシデントの処理と分析を行うために整備されるべき事項について扱っている。この章は、クラウドが、現在のインシデント処理プログラムにもたらす複雑性を理解する手助けとなる。
アプリケーションセキュリティ	クラウド上で稼働している、または開発されているアプリケーションソフトウェアの安全性の確保。これは、クラウド上に稼働するようにアプリケーションを移行または設計することが適当であるかについてや、適当である場合は、どのタイプのクラウドプラットフォーム(SaaS、PaaS または IaaS)が、最も適当であるか、などの項目を含む。
暗号化と鍵管理	適切な暗号化用法と拡張性のある鍵管理の特定。このセクションは、規範的ではないが、それらが必要である理由や、リソースへのアクセスやデータを保護するにあたって発生する問題などに関する、多くの情報を含む。
アイデンティティとアクセス管理	アイデンティティ管理およびアクセス制御を提供するためのディレクトリサービスの活用。組織のアイデンティティをクラウドに拡張する際に遭遇する問題にフォーカスしている。このセクションは、クラウドベースのアイデンティティ、権限付与、アクセス管理 (IdEA)を行う組織の準備状況を評価することについて、洞察を提供する。
仮想化	クラウドコンピューティングにおける仮想化の利用。この章では、マルチテナント性、VM による分離、VM 共存、ハイパーバイザーの脆弱性等に関連したリスク項目を扱っている。この章では、仮想化のあらゆる形に対する一般的なサーベイではなく、システム／ハードウェアの仮想化に関わ

	るセキュリティの問題にフォーカスしている。
Security as a Service	セキュリティ保証、インシデント管理、コンプライアンス認証、アイデンティティとアクセスの監視を用意したサードパーティの提供。Security as a service は、セキュリティインフラの検出、改善、ガバナンスを適切なツールや専門知識を用いて信頼できるサードパーティに委託している。このサービスの利用者は、独立した専門知識と先進技術の利益を得て、繊細なビジネス運用を安全で堅牢にすることができる。

1.6 クラウド展開モデル

利用するサービスモデル(SaaS、PaaS、IaaS)にかかわらず、クラウドサービスには 4 つの展開モデルと、特定の要求に対処するためにそれらから派生した変化形がある。

市場の製品と利用者要求の成熟化により、派生したクラウド展開モデルが出現してきていることに注意することは重要である。そのような例として、仮想化プライベートクラウドがある。これは、プライベートあるいは準プライベートな方法でパブリッククラウドインフラを利用して、利用者のデータセンタにある内部リソースを仮想プライベートネットワーク(VPN)を通して相互接続する方法である。

ソリューションを設計するときに用いられるアーキテクチャの考え方は、結果として得られるソリューションに対する将来の柔軟性、セキュリティおよび移行性に対して明確な意味を持っている。経験則からすると、境界のある(perimeterized)ソリューションは、それぞれの 4 つの領域において境界のない(de-perimeterized)ソリューションより有効性が低い。また、同様の理由で、独自のソリューションを用いるか、オープンなソリューションを用いるかの選択については慎重な検討を実施すべきである。

<u>展開モデル</u>

- *パブリッククラウド*: クラウドインフラは、一般社会や大企業グループに利用可能で、クラウドサービスを販売する組織によって所有される。
- *プライベートクラウド*: クラウドインフラは、1 つの組織のみのために運用される。組織あるいはサードパーティによって管理が行われ、組織内(on-premise)か、組織外(off-premise)に置かれる。
- *コミュニティクラウド*: クラウドインフラは、いくつかの組織によって共有され、関心事(たとえば、ミッション、セキュリティ要件、ポリシー、またはコンプライアンス問題)を共有した特定のコミュニティをサポートする。組織あるいはサードパーティによって管理が行われ、組織内(on-premise)か、組織外(off-premise)に置かれる。
- *ハイブリッドクラウド*: クラウドインフラは、2 つあるいはそれ以上のクラウド(プライベート、コミュニティ、パブリック)から構成され、それぞれが独自の実体が残るものの、データやアプリケーションの移植性(たとえば、クラウド間のロードバランスのためのクラウドバースティング)を可能にする標準ないしは独自の技術によって結び付けられている。

1.7 推奨事項

クラウドサービスの展開は、3 つの典型的なモデルと、様々な派生形の組み合わせに分けられる。3 つの基本的な分類は、しばしば「SPI モデル」と呼ばれる。ここで、「SPI」は、それぞれ、Software、Platform、Infrastructure (as a Service)と定義される。

- **Cloud Software as a Service (SaaS).** 利用者に提供される機能は、クラウドのインフラ上で動く、プロバイダが提供するアプリケーションを使用する機能である。アプリケーションは、ウェブブラウザ(例:ウェブベースの email)のようなシンクライアントインタフェースを通して、さまざまなクライアントデバイスからアクセス可能である。利用者は、限られたユーザ固有の設定を除き、ネットワーク、サーバ、OS、ストレージ、個々のアプリケーションの機能を含むクラウドインフラの管理およびコントロールを行わない。

- **Cloud Platform as a Service (PaaS).** 利用者に提供される機能は、プロバイダによってサポートされているプログラミング言語やツールを使用し、利用者が作成したアプリケーションをクラウドのインフラに展開する機能である。利用者は、基本的なクラウドのインフラ、ネットワーク、サーバ、OS およびストレージを管理およびコントロールしないが、展開しているアプリケーションと、場合によってはアプリケーションをホスティングしている環境の設定をコントロールする

- **Cloud Infrastructure as a Service (IaaS).** 利用者に提供される機能は、処理、ストレージ、ネットワークおよびその他の基本となるコンピューティング資源の割り当てであり、そこで利用者は OS とアプリケーションを含む任意のソフトウェアを展開して動かすことができる。利用者は、基盤となるクラウドのインフラを管理およびコントロールしないが、OS、ストレージ、展開されたアプリケーションおよび場合によっては選択されたネットワークコンポーネント(たとえば、ホストファイアウォール)をコントロールする。

NIST モデルおよび本ガイダンスでは、クラウドサービスブローカー、仲介や監視、移送・移植性、ガバナンス、プロビジョニングを提供するプロバイダ、およびインテグレーションサービスに関連した新たなサービスモデルの定義は直接行わない、また、さまざまなクラウドプロバイダと利用者の間の関係についての議論は直接行わない。

短期的には、イノベーションが迅速なソリューション開発を促すのに伴い、API やインタフェースの開発といった形態で、クラウドサービスのプロバイダと利用者がクラウドサービスと連携する方法は多様化している。これにより、クラウドサービスブローカーは、総合的なクラウドエコシステムにおいて重要な構成要素になる。

クラウドサービスブローカーは、利用者に代わって互換性のない機能やインタフェースを抽象化する。これは、一般的かつオープンで標準的な方法を用いて問題解決を行うという長期的な方法の前に、利用者独自のニーズに対して最も効果のあるモデルを活用することができるように、利用者に対して流動性や迅速性を得ることができるようなセマンティック機能を提供する。

また、クラウドの管理、セキュリティ、相互運用性などを可能にしようとするオープン API および独自の API の両方の開発に関する多くの取り組みにも注意する必要がある。これらの取り組みをいくつか挙げると、Open Cloud Computing Interface Working group、 Amazon EC2 API、VMware の DMTF によって提出された vCloud API、Sun の Open Cloud API、Rackspace API、GoGrid の API 等がある。オープンで標準的な API は、DMTF の Open Virtualization Format (OVF)のような共通のコンテナ形式と同様に、クラウドの移植性と相互運用性に重要な役割を果たすであろう。

現在、多くのワーキンググループやドラフトおよび公開済みの仕様があるが、利用者の要求や市場および経済の原理により、管理が容易で相互運用性のあるものだけに整理されていくだろう。

1.8 要求事項

クラウドサービスは、従来のコンピューティングのアプローチとの関係および違いを示す 5 つの基本特性を有している。

- ✓ **オンデマンドセルフサービス.** 利用者は、サーバタイムやネットワークストレージ等のコンピューティング機能を、サービスプロバイダとの人的なやり取りなしに、必要に応じて自動的に独自に供給することができる。
- ✓ **幅広いネットワークアクセス.** 機能はネットワークを通して利用でき、標準的なメカニズムでアクセスできる。これは、従来のサービスやクラウドベースのソフトウェアサービスと同様に、さまざまなシンクライアントあるいはシッククライアント(たとえば、モバイル携帯、ラップトップ、PDA[12])で使うことができる。
- ✓ **リソースプーリング.** プロバイダのコンピューティングリソースは、マルチテナントモデルを使用することで複数の利用者に提供されるようにプールされる。これは、異なった物理的リソースや仮想化リソースにダイナミックに割り当てられ、利用者の要求に従って再割り当てされる。ある程度の位置の独立性があり、利用者は、通常、プロバイダのリソースの正確な場所をコントロールすることや知ることはできない。しかし、より抽象度の高いレベル(たとえば、国、州またはデータセンター)では位置は指定できるかもしれない。リソースの例としては、ストレージ、プロセシング、メモリ、ネットワーク回線容量および仮想マシン(VM)が含まれる。プライベートクラウドでさえ、同じ組織の異なった部分のリソースをプールする傾向がある。
- ✓ **迅速な弾力性.** 機能は、素早くスケールアウトするために、迅速かつ弾力性をもって(場合によっては自動的に)プロビジョニングされ、また素早くスケールインするために迅速に解放することができる。利用者にとっては、プロビジョニング可能な機能は、しばしば無限にあるように見え、必要な時に必要な量だけ購入することができる。
- ✓ **度数性.** クラウドシステムは、サービスのタイプ(たとえば、ストレージ、プロセシング、帯域幅、アクティブなユーザアカウント)に適したレベルで抽象化された測定機能を活用することで、リソースの利用を自動的にコントロールし、最適化する。リソースの使用はモニタリング、コントロールおよびレポートが可能であり、これはプロバイダとサービス利用者の両方に透明性を提供する。

クラウドアーキテクチャがどのようにセキュリティアーキテクチャに影響を与えるかは、一貫性のある分類法に結びついた一般的で簡潔な用語を理解することが重要である。これは、クラウドサービスとアーキテクチャを分解し、セキュリティと業務管理のモデル、リスク評価と管理のフレームワーク、そしてコンプライアンス基準にマッピングすることである。

クラウドコンピューティングを展開する際、アーキテクチャ、技術、プロセスおよび人的資源がどのように変化するか、あるいは現状のままであるかを理解することが重要である。クラウドサービスにおける上位レベルのアーキテクチャの関係性を明確に理解しなくては、より詳細な問題に合理的に対処することは不可能である。このアーキテクチャ概要は、他の 13 のフォーカスエリアとともに、読者に対してクラウドコンピューティング環境のセキュリティを評価、運用、管理およびガバナンスの確固とした基礎を提供する。

参考文献

[12] **PDA** - Personal Digital Assistant

[1] NIST definition of Cloud.
NIST 500-292 “NIST Cloud Computing Reference Architecture”

[2] NIST definitions and API homepages.
www.cloud-standards.org

[3] Jericho Forum Cloud Cube Model.
www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

セクション II //
クラウドにおける
ガバナンス

第 2 章 //
ガバナンスとエンタープライズリスクマネジメント

クラウドコンピューティングにおけるガバナンスとエンタープライズリスクマネジメントの基本的な問題は、効果的な情報セキュリティガバナンス、リスクマネジメント、およびコンプライアンスを維持するための適切な組織構造、プロセス、およびコントロールの識別と実施に関係がある。また、組織は、どんなクラウド展開モデルの場合でも、クラウドコンピューティングサービスのプロバイダと利用者、それらをサポートするサードパーティベンダを取り巻く情報のサプライチェーン全体に渡る妥当な情報セキュリティを確保すべきである。

効果的なガバナンスとエンタープライズリスクマネジメントのクラウドコンピューティング計画は、組織の総合的なコーポレートガバナンスにおける注意義務の一部としての良く考えられた情報セキュリティガバナンスのプロセスから得られる。良く考えられた情報セキュリティガバナンスのプロセスは、(ビジネス上の拡張性があり、組織を超えて繰り返すことができ、測定でき、持続可能、正当と認められ、継続的に改善し、継続的に費用対効果に優れた)情報セキュリティ管理プログラムをもたらす。

多くのクラウド開発では、ガバナンスの大部分の要素はプロバイダと利用者との契約になる。カスタマイズされた環境では、各プロビジョニング毎に詳細な注意を払い、交渉する。大規模な利用者やプロバイダでは、必要事項と拡張性に対する考慮とをトレードオフするかどうかを決定する。こうした配慮は、重大な場面または特定のワークロードでのリスク値に基づき優先づけられることがある。(例えば、メールでは、稼働時間と可用性は人事システムよりも重要となるかも知れない)。成熟するにつれ、Cloud Audit や STAR のようなプロジェクトは、より標準化されたガバナンス方法、(よって、より大きな拡張性)を提供する。

概要. この章は以下を扱う:

- ガバナンス
- エンタープライズリスクマネジメント

この章は、Cloud Control Matrix Domains DG-01 と IS-02 および、GRC-XML の利用、ソルベンシーの確立のための CloudAudit にマップされる。

2.1 コーポレートガバナンス

コーポレートガバナンスは、企業が指示、管理、または統制される方法に影響を及ぼすプロセス、技術、習慣、ポリシー、法律、および制度の集合である。また、コーポレートガバナンスは、多くの利害関係者と会社の目標の間の関係を含む。良いガバナンスは、会社の真の所有者である株主の権利と、受託者としての経営幹部の役割の承認に基づいている。コーポレートガバナンスの多くのモデルがあるが、すべて 5 つの基本原理に従う:

- 監査のサプライチェーン
- 取締役会、経営組織、および手続き
- 企業の責任とコンプライアンス

- 財政的透明性と情報公開
- 統制権の所有構造と行使

ある会社に関わるという利用者の決定の重要なポイントは、期待に応えてもらえるだろうという信用である。クラウドサービスでは、複数のサービス間の相互依存性が、利用者が責任のある関係部署を仕分けることを、より難しくする。そのことが特定の業者の信頼性不足をもたらす場合、その業者と引き続き関係を持つことはないだろう。これが組織的特徴となる場合、ある業者の信用の喪失は他の業者に影響を及ぼし、また、マーケットでの失敗は外部の訴訟や別の関係者の登場の両方の可能性を増やすだろう。

利害関係者は会社の一貫した業績と成長に適切かつ必要な監視メカニズムを慎重に考えるべきである。

2.2 エンタープライズリスクマネジメント

エンタープライズリスクマネジメント(ERM)は利害関係者に価値を提供するあらゆる組織によるコミットメントに根づいている。全てのビジネスは不確実性に直面しており、経営層の課題の 1 つは、組織がどのようにその不確実性を測り、管理して、緩和できるかを決定することである。不確実性は、組織とその戦略の価値を増減する可能性を機会とリスクの両方に与える。

情報リスクマネジメントは、データ所有者のリスクをとる欲求と許容度合いに沿って、リスクに曝されることとそれを管理する能力を識別して理解するプロセスである。したがって、情報リスクマネジメントは情報資産の機密性、完全性、および可用性をもたらすための IT リソースの意志決定支援の第一の手段である。

この章は、Cloud Control Matrix Domains DG-08 および、ソルベンシーの確立のために ISO31000, ISF, ISACA の利用にマップされる。

ビジネスにおけるエンタープライズリスクマネジメントはリスクを管理し、組織の目的の達成に関連する好機をつかむために組織が用いる方法とプロセスを含む。クラウド環境では、経営者は、以下を含む識別・分析された特定のリスクのリスク対応戦略を選択する:

- 回避– リスクをもたらす活動を終了する
- 低減– リスクに関連する可能性や影響を低減する行動をとる
- 共有または保険 – 金銭的にリスクの一部を移転または共有する
- 受容 – コスト/利益判断により、何も行動をとらない

リスク管理は、必ずしも不確実性や変化を最小化するのではなく、どちらかと言うとリスク許容度と戦略に沿った価値最大化を目的に、自然とバランスをとるプロセスである。

いかなるクラウドの利用機会やクラウド計画にも、クラウドサービスがリスクまたはビジネス上の価値の見地から採用すべきかどうかという決定に影響する多くの変動要素、価値、およびリスクがある。各企業は、クラウドが適切な解決策であるかどうか決めるためにそれらの変動要素を熟慮しなければならない。

クラウドコンピューティングは多くの可能性のある利益を企業に提供するが、これらの利益のいくつかは以下を含む:

- 最適化されたリソース利用
- クラウドコンピューティングテナントでのコスト節減
- 資本支出の移行

- CAPEX[13]から営業支出(OPEX)へ
- クライアント用の IT パワーのダイナミックな拡張性
- 新しいアプリケーションや展開のライフサイクル開発短縮化
- 新しいビジネス実現のための時間的制約の短縮化

利用者はクラウドサービスとセキュリティをサプライチェーンのセキュリティ問題とみなすべきである。これは、可能な範囲で、プロバイダのサプライチェーン(サービスプロバイダの関係性と依存性)を調べて評価することを意味する。また、これは、プロバイダ自身のサードパーティの管理を調べることを意味する。サードパーティサービスプロバイダの評価は、プロバイダのインシデント管理、事業継続性、災害復旧ポリシー、プロセス、および手順を明確に対象とすべきであり、そして、コロケーション（ハウジング）とバックアップ施設の検討も含むべきである。これは、プロバイダ自身のポリシーや手順に対する準拠性のプロバイダの内部評価のレビュー、およびこれらの分野のコントロールのパフォーマンスと有効性の妥当な情報を提供するためのプロバイダの測定基準の評価を含むべきである。インシデント情報は、契約、SLA、または他の協定で指定でき、さらに自動的または定期的に直接リポーティングシステムら伝えられるか、あるいは主担当に届けられる。注意と精査のレベルはリスク値に関連づけられるべきである--第三者が直接企業データにアクセスしないなら、リスクのレベルはかなり低下する、そして、逆もまた同様である。

利用者は、それらのプロバイダのリスク管理のプロセスとガバナンスを調査し、その実施が一貫して揃っていることを確認すべきである。

2.3 許可

許可

- 企業のリスクを監視し測定するための確立済のリスクフレームワークを採用する
- リスク管理能力(例えば、セキュリティ設定共通化手順(**SCAP**)[14]、サイバーセキュリティ情報交換フレームワーク(**CYBEX**)[15]、または **GRC-XML**[16])を測定するための測定基準を採用する
- サプライチェーンの中で株主と利害関係者両方の受託者の役割を果たしている経営幹部と共に、コーポレートガバナンスのリスク中心の観点を採用する
- 法域間の違いを考慮するための法的な観点による枠組みを採用する

2.4 推奨事項

- 要件が継続的に充足されることを確実にするために、プロバイダのセキュリティ能力、セキュリティ管理のアプリケーション、及び継続中の詳細評価と監査、の精査に対し、クラウドコンピューティングサービスにより得られるコスト削減効果を再投資する。

[13] **CAPEX** -資本支出
[14] **SCAP** - Security Content Automation Protocol: セキュリティ設定共通化手順
[15] **CYBEX** - Cybersecurity Information Exchange Framework: サイバーセキュリティ情報交換フレームワーク
[16] **GRC-XML** - technology standards to enable and enhance the sharing of information between various technologies that support GRC efforts

- ユーザ組織は、採用見込みのプロバイダ組織に対するデューデリジェンス(正当な注意義務及び努力)の一部として、具体的なセキュリティ管理と同様に具体的な情報セキュリティガバナンス構造とプロセスの評価を含めるべきである。プロバイダのセキュリティガバナンスのプロセスと能力は、ユーザの情報セキュリティ管理プロセスで十分性、成熟性、および一貫性を評価すべきである。プロバイダの情報セキュリティ管理は、実証可能なリスクベースのものであり、これらの管理プロセスを明確にサポートすべきである。

- 利用者とプロバイダの間の協力的なガバナンス構造とプロセスは、サービスデリバリの設計・開発の一部や、サービスリスクアセスメントとリスク管理計画として、必要に応じて特定され、その後、サービス契約に組み入れられるべきである。

- セキュリティ要件が契約上実施可能であることを確実にするため、セキュリティ部門は、サービスレベルアグリーメント(SLA)[17]と契約上の義務が確立されるまでは、関与するべきである。

- 情報セキュリティ管理の能力と有効性を測定する測定基準と規格はクラウドに移行する前に、確立されるべきである。組織は、最低でも現在の測定基準と、異なる(潜在的に非互換の)測定基準を使用する可能性があるクラウドに運用を移行する際に、測定基準がどのように変化するかを理解し記録するべきである。

- 利用者によるインフラに対する物理的なコントロールが不足するため、多くのクラウドコンピューティングの展開では、SLA、契約要求事項、およびプロバイダによるドキュメンテーションはリスク管理において、従来の企業が所有しているインフラストラクチャよりも大きな役割を果たす。

- クラウドコンピューティングのオンデマンドプロビジョニングやマルチテナントの性質のため、従来の形式の監査や評価は、利用できないか、あるいは変更するかもしれない。例えば、いくつかのプロバイダは脆弱性評価とペネトレーションテストを制限するが、他のプロバイダは監査ログと活動モニタの利用を制限する。これらを社内ポリシーが求めるなら、代りの評価オプション、具体的な契約上の例外項、または、よりリスク管理要件に合う代りのプロバイダを探す必要があるかもしれない。

- クラウドで提供されるサービスが、企業運営に不可欠であるなら、リスク管理アプローチは資産の識別と評価、脅威と脆弱性の識別と分析、それらの資産への影響の見込み(リスクとインシデントシナリオ)、イベント／シナリオの可能性、経営層の承認済のリスク受容レベルと判断基準、複数の選択肢(コントロール、回避、移転、受容)を持つリスク対応計画を含めるべきである。リスク対応計画の結果はサービス契約に組み入れられるべきである。

- プロバイダとユーザ間のリスクアセスメントアプローチは、影響分析評価基準と発生する可能性の定義での一貫性と一致しているべきである。ユーザとプロバイダはクラウドサービスのリスクシナリオを共同で作り上げるべきである。これはプロバイダのユーザ向けサービスデザインと、ユーザのクラウドサービスのリスク評価に対し、固有のものであるべきである。

- クラウドとそのプロバイダが発展する性質を持つため、例えばプロバイダのビジネスの継続性、データとアプリケーションの移行性、およびサービスの相互運用性といった業者のリスクを、リスクシナリオに含めるように注意すべきである。

- 資産棚卸は、クラウドサービスを支え、かつプロバイダの統制下にある資産を説明する必要がある。資産分類と評価スキームはユーザとプロバイダ間で一貫しているべきである。

[17] **SLA** - Service Level Agreement

- 業者だけではなく、サービスがリスクアセスメントの対象であるべきである。クラウドサービスの利用、そして利用予定の特定のサービスや展開モデルは、組織のリスク管理目的、および経営目標と一致しているべきである。

- クラウドコンピューティングサービスの利用者とプロバイダは、サービスや展開モデルに関わらず堅牢な情報セキュリティガバナンスを作り上げるべきである。情報セキュリティガバナンスは、ビジネスのミッションと情報セキュリティプログラムをサポートする合意済の目標を達成するための、利用者とプロバイダ間の共同作業であるべきである。ガバナンスは定期的評価を含むべきであり、展開モデルは(リスクアセスメントに基づく)責任と期待値を定めるかもしれないが、サービスモデルは協力的な情報セキュリティガバナンスと(ユーザとプロバイダのコントロールのそれぞれの範囲に基づく)リスク管理において定義済の役割と責任を調整することがよくある。

- クラウドサービスの利用者は、自組織の経営者がクラウドサービスに関するリスク許容度を定義し、何らかのクラウドサービス利用の残存リスクを受容したかどうか尋ねるべきである。

- プロバイダが自社のサービスに関して包括的で有効なリスク管理プロセスを示すことができない場合、利用者は、潜在的なリスク管理のギャップを補うユーザ自身の能力と同様に、業者の利用を慎重に評価するべきである。

- 組織は、ビジネスと技術的影響に基づきプロバイダに関与させるためのリスク測定基準を定義するべきである。これらの測定基準は、対象データの種別、情報に関連するユーザ種別の多様性、そして業者とその他の関係先を含むことがある。

2.5 要求事項

- ✓ 財政的なソルベンシー(健全性)と組織的な透明性を明示して、利害関係者と株主に透明性を提供する。
- ✓ クラウドサプライチェーンに固有のリスクの相互依存性に注意し、企業としてのリスクに対する姿勢や準備状況を、利用者や依存関係者に伝える。
- ✓ クラウドサプライチェーンの他のプロバイダから引き継がれたリスクを検査して検討し、運用上の頑健性を通じてリスクを緩和、保有するための積極的対策を取る。

第 3 章 //
法律問題: 契約と電子的証拠開示

この章ではクラウドコンピューティングによる法的側面のいくつかをハイライトする。クラウドにデータを移行させることにより起こる法律問題、クラウドサービス契約での考慮すべき諸問題、および欧米の訴訟での電子的証拠開示で示される特別問題について一般的な背景を示す。

この章は選ばれた問題の概要を示し、法的助言に代わるものではない。

概要. この章は以下のトピックをとりあげる:

- クラウドにデータを移行させることによる固有の法律問題の概要
- クラウドサービス契約の問題
- 電子的証拠開示での特別な問題

3.1 法律問題

世界中の多くの国では、数多くの法、規則、その他の命令によって、公共団体や民間組織における個人情報のプライバシーと、情報とコンピュータシステムのセキュリティが保護されている。例えば、アジア太平洋地域では、日本、オーストラリア、ニュージーランド、および多くの他の国々が、消失、不正使用、または変更から個人情報を保護するため、データコントローラが経済協力開発機構(OECD)[18]の Privacy と Security Guidelines、およびアジア太平洋経済協力会議(APEC)[19]のプライバシーFramework に基づいて適切な技術的・物理的・管理方法の採用を求めるデータ保護法を採用した。

ヨーロッパでは、欧州経済地域(EEA)[20]加盟国が 1995 EU データ保護指令[21]と 2002 電子プライバシー指令[22] (2009 年に改正)に詳述された原則に従うデータ保護法を制定した。これらの法はセキュリティコンポーネント、そして下請事業者に負わせるべき十分なセキュリティを提供する義務も含む。アフリカのモロッコやチュニジア、中東のイスラエルやドバイなどの EEA と密な結びつきを持つその他の国が、同じ原則に従う同様の法を採用した。

また、北米、中米、および南米の国々は急速にデータ保護法を採用している。これらの法は各々セキュリティ要件を含み、データの保存場所にかかわらず、また特に第三者への移転について、個人情報の保護とセキュリティを確実にする負担をデータ管理者に課している。例えば、施行されて数年になるカナダ、アルゼンチン、およびコロンビアのデータ保護法に加え、メキシコ、ウルグアイ、およびペルーは、最近、主にヨーロッパのモデルの影響を受け、APEC Privacy Framework を参考にしたデータ保護法案を可決した。

[18] **OECD** - Organization for Economic Cooperation and Development - 経済協力開発機構
[19] **APEC** - Asia Pacific Economic Cooperation - アジア太平洋経済協力会議
[20] **EEA** - European Economic Area - 欧州経済地域
[21] **European Union (EU) Data Protection Directive** - EU データ保護指令
[22] **ePrivacy Directive** -電子プライバシー指令

日本では、個人情報保護法が、民間部門に安全に個人情報とデータを保護することを求めている。医療業界では、医師法[23]、保健師法[24]、そして薬剤師法[25]といった職域別法制[26]が、患者情報の機密性のため保健専門家の登録を求める。

合衆国でビジネスをする組織は、いくつかのデータ保護法の対象となりうるであろう。こうした法は組織に下請事業者の行為の責任を負わせる。例えば、1996 年のグラムリーチブライリー法(GLBA) [27]や米国医療保険の相互運用性及び説明責任に関する法律 (HIPAA)に基づくセキュリティとプライバシーのルールは、組織が契約書で、下請事業者に合理的なセキュリティ対策を用いてデータプライバシー条項に従わせることを求めている。 連邦取引委員会(FTC)や州検事総長などの政府機関は一貫して組織にその下請事業者の活動に対して責任を持たせている。Payment Card Industry (PCI) Data Security Standards (DSS) (下請事業者によって処理されたデータを含め、世界中のクレジットカード情報に適用される)には、同様の要件がある。

以下のセクションはクラウドへの個人情報の移転や、クラウドでの個人情報の処理に関して起こり得る法律問題の例を提示する。

表 1 -- 既知の義務

問題	説明
米国連邦法	GLBA や HIPAA 1998 年児童オンラインプライバシー保護法("COPPA")、などの多数の連邦法とそれらの関連する規則は、FTC が発する命令とともに会社がデータを処理する際、具体的なプライバシーと安全策を採用し、第三者サービスプロバイダとの契約に同様の注意を要求することを求めている。
米国州法	また、多数の州法は、企業に個人情報の十分な安全性を提供し、サービスプロバイダにも同じことを求める義務を負わせる。一般に、情報セキュリティ問題を扱う州法は、最低限、書面の契約書によって会社が、合理的なセキュリティ対策についてサービスプロバイダと定めることを求める。例としてマサチューセッツセキュリティ規制法での広範な要件を参照されたい。
基準	PCI DSS や ISO27001 などの基準も、連邦法や州法と同様にドミノ効果を引き起こす。PCI DSS や ISO27001 の影響を受ける会社は、自ら基準に従うのとともに、指定された基準を満たすために従うのと同じ義務を下請事業者に伝えなければならない。
国際規則	多くの国がヨーロッパ連合モデル、OECD モデルまたは APEC モデルに従うデータ保護法を採用した。これらの法の下では、データコントローラ(通常個人との最も重要な関係を持っている存在)は、第三者がデータを処理する場合であっても、個人情報の収集と処理に責任がある。データコントローラは、自らに代わって個人的なデータを処理する第三者に対して、データを保護するために適切な技術的組織的なセキュリティ対策を確実に執らせなければならない。
契約上の義務	特定の活動が規制されない場合であっても、会社は、利用者、連絡先または従業員

[23] **Medical Practitioners' Act** - 医師法
[24] **the Act on Public Health Nurses** - 保健師法（日本では「保健師助産師看護師法」）
[25] **the Pharmacist Act** - 薬剤師法
[26] **profession-specific laws** - 職域別法制
[27] **GLBA** - Gramm-Leach-Billey Act - グラムリーチブライリー法

	の個人情報を保護する契約上の義務がある場合があり、そのときは、データが二次用途に使用されず、また第三者に公開されないことを確実にしなければならない。この義務は例えば会社がウェブサイトで掲示する約款と個人情報の保護方針に起因する場合もある。 さもなければ、会社は、データ(個人情報か社内情報)を保護し、それらの使用を制限し、セキュリティを確実にして、暗号化を使用するなどの具体的なコミットメントを行なう利用者との(サービス契約のような)契約をしているかもしれない。 組織は、自らの管理下にあるデータがクラウドでホスティングされる際、プライバシー告知または他の契約でされた約束と責任を満たす継続的能力を確実に持たなくてはならない。 例えば、会社は、データの特定用途にのみ同意したかもしれない。その場合、そのクラウドのデータは、収集されたその用途にのみ使用されなければならない。 プライバシー告知で、個人のデータ主体が自らの個人情報へのアクセスができる場合、またこの情報の修正や消去ができる場合、クラウドサービスプロバイダは、これらのアクセス、変更、そして消去の権限を、クラウドでない関係と同程度に実施できるようにしなければならない。
国境を超える移転の禁止	世界中の多くの法は、情報の国外への移転を禁止または制限している。多くの場合、データを移転した国が個人情報とプライバシー権の適切な保護を提供する場合にだけ、移転が許される。この適切性要件の目的は、国境外に移転される個人のデータの主体者が、自身のデータが移転される新しい国で、少なくとも移転前に与えられたものと同様のプライバシー権とプライバシー保護を享受できることを確実にすることである。 従って、クラウドユーザが、外国のデータ保護法が課されるかもしれない特有の制限に対応できるよう、従業員、クライアント、およびその他の個人情報がどこに在るかを知ることは、重要である。 国によっては、この適切な保護を確実にするための要件は、複雑で、厳しいものかもしれない。いくつかのケースでは、自国のデータ保護コミッショナーの事前の許可を得ることが必要かもしれない。

3.2 契約問題

データをクラウドに移す際、データを保護し保証する責任は、とある状況のもと、責任が他者と共有されることがあったとしても、そのデータの収集者か管理者に通常残る。データのホスティングや処理を第三者に依存する場合、データ管理者はデータのいかなる紛失、破損、または不正使用にも依然として責任を負う。データ管理者とクラウドプロバイダが、役割、関係者の期待、データに付随する多くの責任を両者に割り当てることを明確に定義する書面(法的)契約を結ぶことは、賢明であり、法的に求められるかもしれない。

また、法律、規制、規格、およびこれまで論議したベストプラクティスは、データ管理者が、これらの義務を(契約の実行の前の)デューデリジェンスか(契約の履行の間)セキュリティ監査を行うことによって確実に実施することをも求める。

3.2.1 デューデリジェンス[28]

クラウドコンピューティングを導入する前に、会社は、提案されたクラウドコンピューティング取引に関連する法的な障害とコンプライアンス要件を識別するために社内の慣行、要件、および制約を評価すべきである。例えば、ビジネスモデルがクラウドコンピューティングサービスの使用を許容しているのか否か、どんな条件のもとそうなのかを判断すべきである。そのビジネスの特性は、社内データに対するコントロールの放棄が法律で制限されたり、重大なセキュリティ上の懸念を生じさせるといったものである可能性がある。

さらに、資産を保護する継続的な義務を果たすことを念頭に置いているかどうか判断するため、会社は、提案されたクラウドサービスプロバイダのデューデリジェンスを行うべきであるし、場合によっては、法的に求められることになる。

3.2.2 契約

関係者は書面で契約しなければならない。サービスの性質によって、契約は通常交渉をすることの無いクリッククラップ契約の形式かもしれないし; あるいは、関係者は特定の状況に適合する、より複雑な文書をめぐって交渉するかもしれない。クリッククラップ契約が利用可能な唯一の契約であれば、クラウドサービスクライアントは、クラウドサービスプロバイダが約束する実利、金銭的節約、および使いやすさと上記の交渉とのリスクのバランスをとるべきである。関係者が契約について交渉することができるなら、この契約の条件が、契約期間とその終了の際に関係者の要求と義務に対応できることを確実にするべきである。クラウド環境で運用する独特の要件とリスクに対応する詳細で包括的な条件を交渉すべきである。

問題が契約で対処されない場合、クラウドサービスの利用者は、代わりのプロバイダを用いたり、またはデータをクラウドに送らないといった目標達成のための代替手段を検討すべきである。例えば、クラウドサービスの利用者が HIPAA の対象となる情報をクラウドに送りたいなら、利用者は、HIPAA ビジネス関係協定にサインするクラウドサービスプロバイダを見つけるか、またはデータをクラウドに送ってはならないだろう。

以下は、いくつかのクラウド固有の問題の簡単な説明である。また、添付のチェックリストは、クラウドサービス契約を評価する際検討すべき問題の包括的(ただし網羅的でない)リストである。

3.2.3 モニタ、テスト、およびアップデート

クラウド環境は静的なものではない。クラウド環境は発展するので、関係者は順応しなければならない。必要なプライバシーとセキュリティの対策が用いられ、プロセスとポリシーに遵っていることを確実なものとするため、サービスの定期的なモニタ、テスト、および評価が推奨される。

さらに、法律的、規制的、そして技術的な状況は早いペースで変化しそうである。新しいセキュリティ上の脅威、新しい法律、新しいコンプライアンス要件に即座に対応しなければならない。関係者は、法律や他の要件に精通するよう保たなければならず、また、運用が適用される法律に適合するようにして、セキュリティ対策が新技術と新しい法が現れるのに応じて発展し続けるようにしなければならない。

「Cloud Audit」と「Cloud Trust Protocol」は、クラウドサプライチェーンのモニタとテストを自動化する 2 つのメカニズムである。さらに、ITU-T は CYBEX と呼ばれる X.1500Cloud Auditing 仕様に取り組んでいる。

3.3 電子的証拠開示での特別な問題点

[28] **デューデリジェンス** - しかるべき正当な注意義務及び努力

この節は合衆国での訴訟に特有な要件を記述する。訴訟で論争する際、米国の訴訟当事者はドキュメントに非常に頼る。他のほとんどの国と対照的に、アメリカの司法制度の特性の 1 つは、米国の訴訟当事者が訴訟に関係するすべてのドキュメントを相手に提供しなければならないということである。訴訟に有利なドキュメントだけではなく、もう片方の訴訟当事者にとり、有利なドキュメントも提供しなければならない。

近年、訴訟当事者が自発的に訴訟に不利だった重要証拠を削除、消失、または変更したと告発されたというたくさんのスキャンダルがあった。その結果、特に ESI[29]と呼ばれる電子形式で保存された情報の訴訟で、関係者の義務をはっきりさせるために手続きの規則が変った。

クラウドが訴訟や調査で必要となるほとんどの ESI の保管庫となるであろうから、連邦民事訴訟規則の電子的証拠開示やこれらの法律と同等の州法で課せられる厳格な要件を実現できるようにするため、クラウドサービスプロバイダとそのクライアントは、訴訟に関係するすべてのドキュメントを識別できるように慎重に計画しなければならない。

この点で、クラウドサービスクライアントとプロバイダは、クライアントが証拠開示要求を受け、関連していそうなデータがクラウドプロバイダに存在するとき、訴訟に関する以下の問題を考慮する必要がある。

3.3.1 所有、管理、およびコントロール

合衆国のほとんどの法域内では、関連情報を提出する関係者の義務は、所有、管理、またはコントロールするドキュメントとデータに限られる。一般に、第三者(クラウドプロバイダでも)が関連データをホスティングしている場合でも、法的なアクセス権を持っていたり、またはデータを入手することがあるので、情報を提出する関係者の義務はなくならない。しかし、クラウドプロバイダがホスティングするすべてのデータがクライアントのコントロール下にあるとは限らない(例えば災害復旧システム、環境を運用するためにクラウドプロバイダが作成し、維持する特定のメタデータ)。クライアントが得ることができる／あるいはできないデータを区別することは、クライアントとプロバイダの利益になるかもしれない。法的なプロセスに対応する情報の作成に関するクラウドデータ操作者としてのクラウドサービスプロバイダの義務は、各法域に残された問題である。

3.3.2 関連するクラウドアプリケーションと環境

特定の訴訟や調査では、実際のクラウド･アプリケーションや環境は、それ自体が訴訟や調査における紛争の解決に関連する可能性がある。こういう状況では、アプリケーションと環境は、おそらくクライアントの管理外にあり、直接プロバイダに対する提出命令か他の証拠開示のプロセスを必要とする。

3.3.3 検索能力と電子的証拠開示ツール

クラウド環境のため、クライアントは、自分の環境で使用する電子的証拠開示ツールを適用したり使用できないかもしれない。そのうえ、クライアントには、クラウドに保存されたすべてのデータを検索したり、アクセスするための能力も管理権限もないかもしれない。例えば、クライアントが自分のサーバでは複数の従業員のメールアカウントにアクセスできても、クラウドでホストされたメールアカウントではこの能力を持たないかもしれない。そのように、クライアントは、この限られたアクセスが引き起こす潜在的追加時間や追加費用を考慮に入れておく必要がある。

3.3.4 保全

[29] **ESI**- electronically stored information -電子形式で保存された情報

概して米国では、当事者が係争中または合理的に予想される訴訟や政府による取調べに関連している、所有、管理またはコントロールすることを知っている（ないしは、知りうべき）データや情報の、破壊や変更を防ぐために合理的な措置を実施する義務があることである。クライアントが利用しているクラウドサービスと展開モデルに依っては、クラウドにおける保全が他の IT インフラストラクチャにおける保存と非常に似ている場合があったり、あるいはかなり複雑である場合がある。

欧州連合では、情報の保全には 2006 年 3 月 15 日の欧州議会・協議会の Directive2006/24/EC が適用される。日本、韓国、およびシンガポールには、同様のデータ保護の取り組みがある。南米では、ブラジルとアルゼンチンはそれぞれ Azeredo 法、およびアルゼンチン Data Retention 法 2004、法 No.25.873、2004 年 2 月 6 日がある。

3.3.4.1 コストとストレージ

保全は、大量のデータを長期間保有することが必要とされることがある。サービスレベル協定(「SLA」)での影響は何か? 保全要請が SLA の期間より長かったなら、何が起こるか? クライアントが適所にデータを保存するなら、誰が拡張されたストレージの代価をどんな価格で支払うのか？クライアントは SLA 上、保存資格を持っているか? クライアントは、オフラインまたはオンラインに近い状態でデータを保存できるよう、「フォレンジック的に適正」な方法でデータをダウンロードできるか?

3.3.4.2 保全の範囲

正当な理由や特定の必要性なしには、要求当事者には、クラウドやアプリケーションにおけるすべてのデータではなく、関連情報を含むクラウドでホスティングされるデータの権利を与えられるだけである。しかし、クライアントに粒度の細かい方法で関連情報またはデータを保存する能力がないなら、訴訟や調査によっては、合理的な保全を有効にするため、過剰な保全が求められるかもしれない。

3.3.4.3 動的で共用されるストレージ

クライアントに適所にそれを保持するスペースがあり、データが比較的静的で、アクセスする人が制限されていて、保全するのを知っているなら、クラウドにデータを保存する負担は比較的小さいかもしれない。しかし、プログラムに基づいて、データを変更したり消滅させるクラウド環境や、保全する必要性に気づかない人々とデータが共有される場合は、保全がより難しくなる場合がある。そのようなデータが関連しており保全する必要があるとクライアントが判断した後、クライアントはそのようなデータを保存する合理的な方法を決定するためにプロバイダと連携する必要があるかもしれない。

3.3.5 収集

クライアントはクラウドにあるデータにたいして運営上のコントロールを潜在的に十分に有していないため、クラウドから収集するのは、クライアントのファイアウォール内からするよりも難しく、より手間がかかり、コストがかかる場合がある。具体的には、クライアントは、そのクラウド･データ全体の可視性と同じレベルを持っていない可能性があり、データ取り出しが合理的に完全で正確であったことを判断するために、集めたデータとクラウド内のデータを 比較するのにさらに苦労するかもしれない。

3.3.5.1 アクセスと帯域幅

多くの場合、クラウド内のデータへのクライアントのアクセスは SLA によって決定される。このことは、大量のデータをすぐに「フォレンジック的に適正」な方法で(すなわち、すべての合理的に関連しているメタデータが保全されている)集める能力を制限するかもしれない。クライアントとクラウドプロバイダは、早期にこの問題を検討し、訴訟と取調べの際に収集を可能にするための臨時のアクセスの手順（およびコスト）を確立する

ためによく尽くしている。そのような協定がなければ、要求当事者と裁判所に対応している際に、クライアントは、クラウド内での収集によって引き起こされる余分な時間とコストを考慮する必要があります。

3.3.5.2 機能性

アクセスと帯域幅に関連するが、それらとは異なる。クライアントのアクセス権は、データの最大範囲へのアクセスを提供するが、与えられた状況で最も支援できるような機能性の程度を提供しない場合もある。一例として、クライアントは、3 年間の小売の取引データへのアクセス権を持っていても、機能的制約のため一度に 2 週間のデータをダウンロードできるだけであるかもしれない。そのうえ、クライアントは実際に存在するすべてのメタデータへの参照権を持っているのではなく、むしろ限られた程度のメタデータしか持っていないかもしれない。

3.3.5.3 フォレンジック

クラウド･データ･ソースをビット単位で参照することは一般的に困難または不可能である。明白なセキュリティ上の理由で、特にクライアントが他のクライアントのデータへアクセスし得るマルチテナント環境では、プロバイダはハードウェアへのアクセスを許したがらない。プライベートクラウドでさえ、フォレンジックは非常に難しいかもしれず、また、クライアントはこれらの制限について相手側弁護士か法廷に通知する必要があるかもしれない。幸いなことに、フォレンジックはクラウドコンピューティングではめったに保証されていないが、これは、クラウドコンピューティングだからではなく、通常フォレンジック分析に適していない構造化データ階層あるいは仮想化であるためである。

3.3.5.4 合理的な完全性

特に情報を得るのに通常の業務手続きが利用できず、訴訟特有の対策が使われている場合は、証拠開示の対象となるクライアントは、クラウドプロバイダからの収集が完全で正確であることを正当化するための合理的手続きを執るべきである。このプロセスは、クラウドに保存されたデータが、正確で、真正であるもの、または許容されるといった検証とは別のものである。

3.3.5.5 合理的にアクセスできない

クライアントのデータがどう格納されるかや、クライアントのアクセス権、および特権が違うので、クラウドのクライアントのデータのすべてが等しくアクセス可能であるわけではない。クライアント(そして、プロバイダ)は関連性、重要性、比例性、およびアクセス可能性についての情報や関連データ構造についての要求を分析するべきである。

3.3.6 直接アクセス

クラウド環境外では、応答当事者の IT 環境へ要求当事者が直接アクセスすることは好まれない。クラウド環境では、さらに好まれず、フォレンジックと同じ理由で不可能かもしれない。重要なのは、ハードウェアとファシリティが所有、管理、またはコントロールの外にあるためクライアントは直接のアクセスを提供できないかもしれず、要求当事者が直接プロバイダに対して提出命令を取得したり、交渉する必要があることである。

3.3.7 ネイティブデータ提出

クラウドサービスプロバイダは、たいていクライアントが管理しないクラウドの中の非常に独自なシステムとアプリケーションにデータを保存している。このネイティブ形式でのデータが提出されたとしても、提出された情報を理解できないであろうから、要求当事者にとって役立たないかもしれない。こういう状況では、関係

者すべて-要求側、提出側とプロバイダ-にとり、標準的報告書またはクラウド環境内にあるデータ取り出しプロトコルを使用して関連情報が取り出されることが最も良いかもしれない。

3.3.8 真正性

ここでは、真正性とは、証拠と認められるデータのフォレンジック認証を意味している。これはアイデンティティ管理の構成要素であるユーザ認証と混同してはならない。クラウドにデータを格納することは、証拠と認められるべきかどうかを決定するためのデータの真正性の分析には影響しない。問題は、ドキュメントに意味があるかどうかということである。E メールは、会社のファイアウォールの後ろに格納されたり、またはクラウドに格納されるので、だいたい真正とされなくもない。問題は、完全な状態で保存されていて、法廷が送受信以来変更されていないと信じることができるかどうかということである。

3.3.9 許容性と信頼性

改変やハッキングなどの他の証拠がないからといって、単にクラウドで作成または格納されていたことで文書が認められたり信用できると考えるべきではない。

3.3.10 電子的証拠開示におけるプロバイダとクライアント間の協力

プロバイダとクライアントの関係の開始時に証拠開示で引き起こされる複雑さを考慮することや、SLA で検討しておくことは、双方にとって、非常に有益である。プロバイダがクライアントを引き付けるためにディスカバリー· サービスを含むようにクラウド製品の設計を検討するかもしれない(「ディスカバリーバイデザイン」)。どんな場合でも、クライアントとプロバイダは、双方に対する証拠開示要求の際に合理的にお互いに協力する契約を含めて検討するべきである。

3.3.11 提出命令または捜索令状への対応

クラウドサービスプロバイダは、第三者から、クライアントデータへのアクセスを要求する提出命令、捜索令状、または裁判所命令の形式で情報提供要求を受け取る可能性がある。求められたデータの機密性や秘密を保護するために、クライアントはアクセスを求める要求と争うことができるようにする必要がある。このため、クラウドサービス契約は、提出命令を受け取ったことを会社に通知し、会社に、アクセスを求める要求と争う時間を与えることをクラウドサービスプロバイダに求めるべきである。

クラウドサービスプロバイダは、施設を公開し、アクセス要求において特定されるすべての情報にたいして要請者に提供することによって要求に答えるようにしたくなるかもしれない。そうする前に、クラウドサービスプロバイダは、要求が整然としていて、適切な法的方法を用いていることを、確認すべきである。クラウドサービスプロバイダは管理する情報を開示する前に、慎重に要求を分析すべきである。

情報の特異性、場所などによって、複雑な法が適用される。例えば、メールが開かれているかどうかと、メールがどれくらい長い間格納されているかによって、メールのコンテンツへのアクセスを要求するのに異なった規則が適用される。要求された情報が、メールのコンテンツであったり、またはメールに関するトラフィックデータだけ(例えば、いつ、だれに送られたかなど)であれば異なる規則が適用される。

参考文献

International Treaties and Agreements

[1] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).

[2] OECD Guidelines for the Security of Information Systems and Networks (2002).

[3] OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy.

Publications

[4] GILBERT, Francoise. © 2009-2011. Global Privacy & Security. Aspen Publishing / Wolters Kluwer (2 volumes).

[5] GILBERT, Francoise. 2011. Cloud Service Providers Can Be Both Data Processors and Data Controllers (BNA Privacy & Security Law Report 10 PVLR 266 (2011). Journal of Internet Law, Volume 15, Number 2, page 3.

[6] POWER, Michael E. AND TROPE, Roland L. 2005. Sailing in Dangerous Waters: A Director's Guide to Data Governance. American Bar Association.

[7] SMEDINGHOFF, Thomas. 2008 Information Security Law: Emerging Standard for Corporate Compliance (ITGP).

Websites

[8] Cloud computing definitions and business models:
http://p2pfoundation.net/Cloud_ComputingDefinition (technical aspects, business models)

[9] Cloud Computing Incidents Database:
http://wiki.cloudcommunity.org/wiki/CloudComputing:Incidents_Database (Records and monitors verifiable, noteworthy events that affect cloud computing providers, such as outages, security issues, and breaches)

第 4 章 //
コンプライアンスと監査マネジメント

従来のデータセンタからクラウドに移行する際、組織は新しい課題に直面する。複数の法域に亘る多くの規制がある中のサービス提供、サービス測定とコミュニケーションのコンプライアンスは、最も大きい課題の 1 つである。利用者もプロバイダも、既存のコンプライアンス、監査基準、プロセス、および実務での違いと影響を理解して、正しく認識する必要がある。クラウドの分散仮想化された性質は、情報とプロセスの明確で物理的な具体例に基づく方法による重要な枠組みの調整を必要とする。

クラウドは、より集中、統合化された管理プラットフォームを通して、その運用・管理の透明性と保証を向上させられる可能性がある。さらに、クラウドプロバイダにアウトソースされたソリューションは、コンプライアンスの優劣における企業規模依存性を減らす。利用初日からコンプライアンスを持ったソリューションを提供できるプロバイダにより、新しい(営利、非営利の)会社はマーケットに参入し、クラウド以前の時代ではコスト的にできなかったであろう行動を取ることができるだろう。セキュリティとコンプライアンスの問題により、IT 運用を社外調達するのに以前は消極的だった政府やその他の組織も、コンプライアンスの一部を契約上の委任によって対処することができる場合には、クラウドモデルを採用する準備がより整うことになるかもしれない。

また、プロバイダと利用者に加えて、規制当局と監査人もまたクラウドコンピューティングの新世界に適応している。現状では、仮想化環境またはクラウド展開を説明する規制はわずかしか存在しない。クラウド利用者は監査人に、自らの組織にはコンプライアンスがあることを示す説明を要求される。クラウドコンピューティングと規制する環境との相互作用を理解することは、どんなクラウド戦略でも主要な要素である。クラウド利用者は、以下を考慮し、理解しなければならない:

- 国境超えまたは複数の法域の問題が該当する場合、具体的注意を払うべき特定のクラウドサービスまたはプロバイダを利用するための規制の影響
- 間接的なプロバイダ(すなわち、自分が利用しているクラウドプロバイダの（訳注:その基盤として使っている他の)クラウドプロバイダ)を含むプロバイダと利用者間のコンプライアンス責任の分担
- タイムリーな方法で、ドキュメント作成、証拠生成、およびプロセス上のものを含むコンプライアンスを示すためのプロバイダの能力
- 必要な(かつ適切に制限された)アクセスとガバナンス要件に沿っていることを確認するための、利用者、プロバイダ及び(利用者とプロバイダ双方の)監査人との関係

概要. この章は以下のテーマを記述する:

- コンプライアンス
- 監査

4.1 コンプライアンス

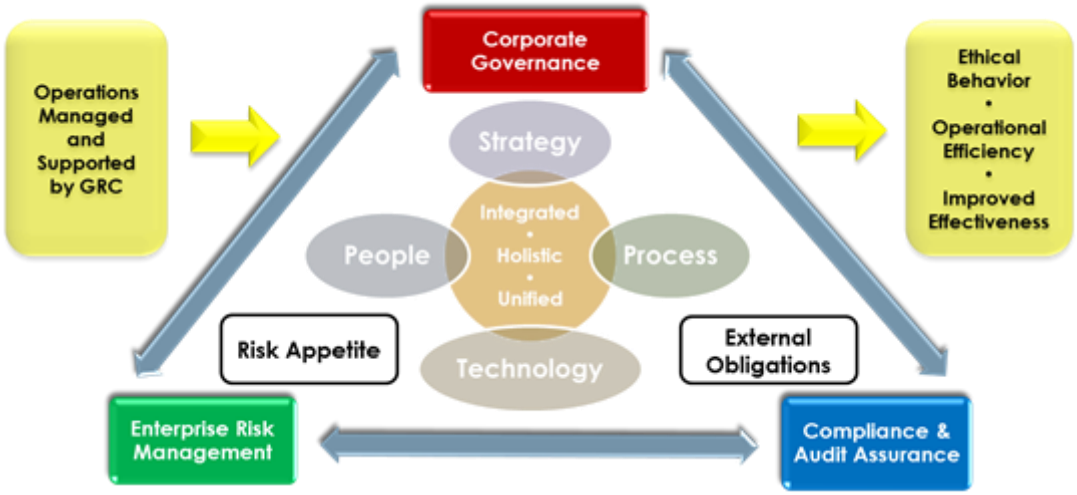


図 1-GRC　価値体系

- **コーポレートガバナンス:** 一貫した管理を提供し、ポリシー、ガイダンスやコントロールをまとめて適用し、有効な意思決定を可能にする組織の利害関係者[30]、ディレクターやマネージャ間の支配力バランス

- **エンタープライズリスクマネジメント:** 組織目標(リスクと機会)、それらの影響の可能性と大きさに関する評価、対応戦略の決定、及び利害関係者の価値の保護と創造のための進捗監視、これらに関連するイベントや状況の確認に基づき意思決定のバランスをとるために組織が用いる方法論とプロセス(フレームワーク)

- **コンプライアンスと監査保証:** 遵守状況の評価、遵守のためのコストに対する遵守しない場合のリスクと潜在的コストの評価による企業の責務(例えば、企業の社会的責任、倫理、適用法、規制、契約、戦略、およびポリシー)に対する認識と堅守、このために、優先順位付けをし、資金を出し、必要と考えられるすべての是正に着手しなさい

クラウドにおける情報技術はますます大量のポリシーや規則の対象になっていく。すべての利害関係者は、組織が複数の法域にまたがる規制ガイドラインと要件に事前に従うことを期待する。IT ガバナンスは、これらの要件に照らしてやり遂げる必要があり、また、すべての組織はやり遂げるための戦略が必要である。

ガバナンスは、外部環境の制約の中で組織の目標の円滑な実行を可能にするためのプロセスとポリシーが含まれる。ガバナンスには、事業がこれらのプロセスやポリシーに完全に沿ったものであることを確実にするためにコンプライアンス活動を必要とする。ガバナンスは、内部要件（たとえば、取締役会の決定、会社の方針など）に一致させることに焦点をあてているが、ここで言う意味でのコンプライアンスは外部要件(例えば、法、規制、業界基準)に一致させることに焦点をあてている。

コンプライアンスは、（たとえば、企業の社会的責任や、関連する法律、倫理規範など、企業の）義務に対する正しい認識と堅守と定義できる。この義務には、遵守状況の評価と、必要かつ適切な修正措置の優先順位付けが含まれている。一部の環境、特に規制の強い環境においては、コンプライアンスそのものよりも重視される報告要件で透明性の観点がむしろ重要になることがある。最も好ましい状況は、コンプライアンスが組織の有効性を阻害することなく、内部で決めたポリシーを補完することである。

[30]**利害関係者** - 出資者と役員

規制は通常、情報技術とそのガバナンス、特に監視、管理、保護そして情報開示の観点から強い影響力を持つ。IT ガバナンスは、コーポレートガバナンス、企業リスク管理、コンプライアンス、および監査/保証を支える要素である。

クラウドは、その管理基盤、とりわけ組織の内部で管理するクラウドである場合、その管理プラットフォームを通じてガバナンスおよびコンプライアンス、集中管理や透明性を可能にする技術となり得る。クラウドサービスを利用することによって、中小規模の組織であっても、はるかに大きく多くのリソースを持つ組織と同じレベルのコンプライアンスを達成できる。セキュリティと保証サービスは、サードパーティのプロバイダがコンプライアンスについて評価とコミュニケーションにおいて役割を果たすことができるひとつの方法である。

どんなコンプライアンスの取り組みも、IT を含めた組織全体での参画が必要である。外部のプロバイダが果たす役割は、慎重に考える必要があり、プロバイダを含むガバナンス上の責任は、クラウドの利用者の組織の中で間接的または直接的に明示的に割り当てるべきである。

加えて、以下に ISO/IEC と ITU-T で開発中の多くのクラウドセキュリティ基準を上げておく:

- ISO/IEC 27017: クラウドコンピューティングセキュリティとプライバシーマネジメントシステムーセキュリティコントロール
- ISO/IEC 27036-x: 複数のパートから構成される調達先管理に関する情報セキュリティ規格であり、クラウドにおけるサプライチェーンに関する事項も含まれる予定である[31]。
- ITU-T X.ccsec: 電気通信分野のクラウドコンピューティングのためのセキュリティガイドライン
- ITU-T X.srfcts: クラウドベースの電気通信サービス環境のセキュリティ要件とフレームワーク(X.srfcts)ITU-T X.sfcse
- ITU-T X.sfcse: Software as a Service (SaaS)アプリケーション環境のためのセキュリティ機能要件書

4.2 監査

適切な組織的ガバナンスには監査と保証が自然と含まれる。監査は独立して行わなければならず、また、ベストプラクティス、適切なリソース、検査済みの手順と基準を反映するよう、しっかりと設計されるべきである。

内部と外部の監査と統制のいずれも、利用者とプロバイダ両方にとって、クラウドに取り組むに当たっての合理的な役割を持つ。利害関係者の満足度を上げるには、クラウド導入の初期段階では透明性の向上が最も良いかもしれない。監査は、運用のリスクの管理活動が徹底的に検査され見直されているという保証を提供する 1 つの方法である。

監査計画は、組織の最も上位のガバナンス的な要素(例えば、取締役会と経営陣)により認可され、支持されるべきである。付随する監査証跡と文書を含む最も重要なシステムとコントロールの定期的な第三者による監査は効率性と信頼性の改善を支援するだろう。

多くの組織が、プロセスの有効性を分析するためのフレームワークとして成熟度モデル(例えば、CMM、PTQM)を使用する。一部のケースでは、リスク管理に対するより統計的なアプローチ(例えば、金融サービス業におけるバーゼルとソルベンシー規制など)を採用していると、その分野が成熟するにつれ、よりリスクに特化したモデルを業務機能や事業部門に対して適切に利用することができるようになる。

[31]訳注：クラウド関連は現在、Part4 として制定される方向で議論が進んでいる

クラウドでは、これらの手法は、改訂して精度を高める必要があるだろう。ちょうど情報技術の従来モデルの場合と同様に、監査はクラウドの潜在的な能力をそれ自身のために活用するだけでなく、クラウドがもたらす新たな切り口を取り扱えるように、そのスコープとスケールを広げていく必要がある。

4.3 推奨事項

プロバイダと契約する際は、利用者組織の中の適切な法務、調達、および契約チームに関わらせなさい。サービスの標準条項は、コンプライアンス要件に対応しないかも知れないため、交渉する必要があるだろう。

クラウドサービスを利用する際、非常に規制の強い業界(例えば、金融、医療など)に特化したコンプライアンス要件は考慮されるべきである。それらの現在の要件を理解している組織は、さまざまな地理的な位置と異なる法の適用下で運用するクラウドプロバイダの影響を含め、分散化された IT モデルのコンプライアンス要件に対する影響を考慮すべきである。

特に情報セキュリティに関連するので、各ワークロード(すなわち、アプリケーションとそれが処理するデータのセット)毎に、クラウドサービスの使用により既存のコンプライアンス要件にどのような影響があるかを見極めておく。任意のアウトソーシングソリューションと同様に、組織は、どのクラウドパートナーが、規制された情報を現在処理していて、また、本来そのプロバイダが処理すべきなのかを理解しておく必要がある。影響のあるポリシーや手順の例としては、活動レポート、ログ取得、データ保持の方法、期間、その後の処置などの原則、インシデントへの対応、統制状況の検査、およびプライバシーに関する方針が含まれる。

各当事者の契約上の責任を理解すること。契約上期待できる最低限の責任範囲は、IaaS モデルでより多くのコントロールと責任を持つ利用者と、SaaS ソリューションで支配的な役割を担っているプロバイダとで展開モデルごとに異なるだろう。特に重要なのは、要件と義務のサプライチェーンによる連鎖である。利用者が直接利用しているクラウドプロバイダに対してだけでなく、最終的な利用者とその利用者が直接契約しているプロバイダのそのサービス基盤もしくはサービスの一部として利用している下位のクラウドプロバイダとの要件と義務も重要である。

法律と業界規制への準拠とその準拠要件(すなわち、法律、技術要件、法的要件、準拠、リスク要件、およびセキュリティ要件)は重要であり、要求分析フェーズにおいて、必ず取り組まなくてはならない。個人識別可能情報（PII[32]）もしくはプライベートな情報と見なされる処理され、伝送され、保存され、閲覧されるすべての情報は、国や州ごとに異なる世界中の非常に多くの従うべき規制に直面する。クラウドは地理的に分散し、スケーラブルになるよう設計されているので、ソリューションのデータは、様々な場所やクラウドサービスプロバイダの複数のデータセンタで保存、処理、伝送、または検索されるかもしれない。いくつかの規制要件では、特定のクラウドサービスタイプでは達成するのが、難しいか不可能な統制を要求される。(例えば、地理的な要件は分散データ記憶システムでは満たせない可能性がある)　利用者とプロバイダは、どのように規則を遵守しているかの証拠（例えば、監査ログ、活動報告、システム構成情報）を集め、保存し、共有するかについて同意しておかなければならない。

- 仮想化とクラウドの保証の課題(と利点)に詳しい「クラウドに通じた」監査人を選択しなさい。
- クラウドプロバイダの SSAE16 SOC2 か ISAE3402Type2 レポートを要求しなさい。これらは監査人と査定者が承認可能な最初の参考資料となるだろう。
- 契約は、SLA の測定基準と遵守に関する第三者(例えば、互いが選択した仲介者による)のレビューに備える契約条文に入れておくべきである。

[32] PII Personal Identification Informaton （個人を識別可能な情報）

4.4 要求事項

- ✓ 監査する権利の条文は、クラウドコンピューティングと規則が頻繁に発展している環境においてトレーサビリティと透明性をサポートするクラウドプロバイダを監査する能力を利用者に与える。期待値の相互理解を確実にする監査権では標準仕様を使用しなさい。そのとき、第三者の認証(例えば、ISO/IEC27001/27017 による)でこの権利は取って代わられるべきである。
- ✓ 特定のアクセス権が持つ透明性についての条文に対する権利は、非常に規制された業界(コンプライアンスの無いことが刑事訴追の根拠となり得る場合を含む)の利用者に必須情報を提供できる。契約は、自動アクセスか直接の情報入手(例えば、ログ、レポート)と、作成された'情報(例えば、システムアーキテクチャ、監査レポート)を区別すべきである。
- ✓ プロバイダは、定期的(あるいは必要に応じて)にプロバイダ自身の情報セキュリティドキュメントと GRC のプロセスを再検討し、アップデートして、発表すべきである。これらは、脆弱性分析と、関連する修正判断と修正活動を含むべきである。
- ✓ 独立監査人は、プロバイダと利用者によってあらかじめ、相互で公開・選択されるべきである。
- ✓ すべての関係者は、IT ガバナンスとセキュリティ管理に、一般的な認証保証の枠組み(例えば、ISO や COBIT)を使用することに同意するべきである。

第 5 章 //
情報管理とデータセキュリティ

情報セキュリティの最も重要な目的は、私たちのシステムやアプリケーションを支える基盤データを守ることである。企業の IT 環境がクラウドに移行する場合、従来のデータ保護対策は、クラウド型アーキテクチャへの対応を迫られる。クラウドの持つ弾力性、マルチテナント性、新しい物理・論理アーキテクチャ、抽象化された制御などにより、新しいデータセキュリティ戦略が必要となる。多くのクラウドシステム配備において、ユーザは、たった数年前には考えられなかったやり方で、データを外部、場合によってはパブリックな環境に移行している。

クラウドコンピューティングの時代におけるデータ管理は、クラウドを利用したプロジェクトに積極的に関わらない組織を含め、あらゆる組織にとって、大変やっかいな課題である。それは内部データやクラウド移行の管理に始まり、組織を横断するように分散したアプリケーションやサービスの上での情報の安全確保に発展していく。幸い、クラウドユーザは必要なツールや技術を手に入れており、クラウドへの移行は、従来のインフラストラクチャにおけるデータ保護をより強化する機会をもたらしてくれる。

筆者らは、クラウドデータセキュリティ戦略の評価や定義のために、データセキュリティライフサイクル（以下で検討する）を用いることを推奨する。これを明確な情報統制ポリシーと重ね合わせ、暗号化や特殊な監視ツールなどのキーテクノロジーによって実施するべきである。

概要. 本章は以下の 3 節で構成される:

- 第 1 節はクラウド情報（格納）アーキテクチャに関する背景を述べる。
- 第 2 節はデータセキュリティライフサイクルを含む、クラウド情報管理のベストプラクティスを述べる。
- 第 3 節は具体的なデータセキュリティコントロールとその利用法について、詳細を述べる。

5.1 クラウド情報アーキテクチャ

クラウド情報アーキテクチャは、クラウドアーキテクチャそのものと同じように多様である。本節ですべての可能な形態をカバーすることはできないが、ほとんどのクラウドサービスが一貫して備えるアーキテクチャがある。

5.1.1 Infrastructure as a Service

IaaS は、パブリッククラウド、プライベートクラウドいずれについても、一般に以下のようなストレージのオプションを備えている:

- **ローストレージ。** データが格納される物理媒体をさす。プライベートクラウドを構成する一部からダイレクトアクセスを受けることもある。

- **ボリュームストレージ.** 典型的には仮想ハードドライブとして IaaS インスタンスにつながれるボリュームをさす。ボリュームでは、頑健性とセキュリティのために、データを分散格納することがしばしば行われる。

- **オブジェクトストレージ.** オブジェクトストレージは、ファイルストレージと紐づけられることがある。オブジェクトストレージは、仮想ハードドライブというより、**API**[33]や Web インタフェースを介してアクセスするファイル共有に近い。

- **コンテンツ配信ネットワーク.** コンテンツはオブジェクトストレージに格納され、その後、インターネットの応答速度を向上するため、地理的に分散したノードに配信される。

5.1.2 Platform as a Service

PaaS は非常に様々なストレージオプションを提供し、またそれらに支えられている。

PaaS は以下のようなサービスを提供できる:

- **Database as a Service.** 直接サービスとして提供されるマルチテナントデータベースである。ユーザはサービスが提供する API や直接的な **SQL**[34]呼び出しにより、データベースを利用する。各利用者のデータは、他のテナントから分離・隔離される。データベースはリレーショナル、フラット、あるいは他の共通な構造のいずれでもよい。

- **Hadoop/MapReduce/Big Data as a Service.** *ビッグデータ*とは、サイズの大きさ、広範囲な配信、内容の多様性、実時間性などの特性から、新しい技術アーキテクチャや分析手法を必要とするデータである。Hadoop や他のビッグデータアプリケーションはクラウドプラットフォームとして提供されることがある。データは通常オブジェクトストレージ、あるいは他の分散ファイルシステムに格納される。データは通常、処理環境に近接する必要があり、処理要求に応じて一時的に移動することもある。

- **アプリケーションストレージ.** アプリケーションストレージは、PaaS アプリケーションプラットフォーム中に構築され、API を介して利用でき、他のカテゴリに属さないオプションを総称する。

PaaS では以下のサービスを利用できる:

- **データベース.** 情報とコンテンツはデータベースに（テキストやバイナリオブジェクトとして）直接格納してもよいし、ファイルとしてデータベースから参照してもよい。

- **オブジェクト/ファイルストレージ.** ファイルや他のデータはオブジェクトストレージに格納されるが、PaaS API　を介してのみアクセスできる。

- **ボリュームストレージ.** データは PaaS サービスを提供するために IaaS インスタンスにつながれる IaaS ボリュームに格納してもよい。

- **その他.** 上記は最も一般的なストレージモデルであるが、PaaS はダイナミックな領域や他のオプションを利用することもできる。

5.1.3 Software as a Service

[33] **API** Application Program Interface アプリケーション　プログラム　インタフェース
[34] **SQL** Structural Query Language データ管理用に設計されたプログラム言語

PaaS と同様に、SaaS も幅広い種類の格納モデル、利用モデルを用いる。SaaS のストレージは常に Web ベースのユーザインタフェースか、あるいはクライアント/サーバアプリケーションを介してアクセスする。ストレージが API を介してアクセスできれば、それは PaaS とみなされる。多くの SaaS プロバイダは、そうした PaaS API も提供している。

SaaS は以下のサービスを提供できる:

- **情報ストレージと管理.** データは Web インタフェースを通じてシステムに入力され、SaaS アプリケーション（普通はバックエンドのデータベース）に格納される。SaaS サービスにはデータセットのアップロードオプションや、PaaS の API を提供するものもある。
- **コンテンツ/ファイルストレージ.** ファイル形式のコンテンツ（例えばレポート、画像ファイル、文書）は SaaS アプリケーションに格納され、Web ベースのユーザインターフェイスを通じてアクセスできる。

SaaS で以下のサービスを利用できる:

- **データベース.** たとえファイル格納のためだけであっても、PaaS と同様に、多数の SaaS サービスはバックエンドデータベースに支えられている。
- **オブジェクト/ファイルストレージ.** ファイルや他のデータはオブジェクトストレージに格納されるが、SaaS アプリケーションを介してのみアクセスできる。
- **ボリュームストレージ.** データは、SaaS サービスを提供するために仮想マシンにつながれた IaaS ボリュームに格納してもよい。

5.2 データ（情報）分散

データ（情報）分散は暗号化のメカニズムを用いずにデータセキュリティを強化するために普通に用いられる技術である。この種のアルゴリズム（**IDA**[35]と略す）は、データを断片化することでクラウドに格納されるデータの可用性と信頼性を高めることができ、多くのクラウプラットフォームで使われている。断片化方式においては、ファイル f は n 個の断片に分割され、それらがすべて署名をつけられ、n 個のリモートサーバに配信される。 その後ユーザは、任意のｍ個の断片にアクセスすることで f を再構築できる。断片化メカニズムは、クラウドでの長期間保存が必要なデータの信頼性保証に使うこともできる。

断片化と暗号化を併用すれば、データセキュリティは強化される： 攻撃者はファイル f の m 個の断片を検索するためにｍ個のクラウドノードに侵入し、さらに使われている暗号メカニズムを解読しなければならない。

5.3 情報管理

個別のデータセキュリティコントロールについて論じる前提として、私たちの守りたい情報を理解し、管理するためのモデルが必要である。情報管理には、情報がどのように使われるかを理解し、その使い方を統制するための手続きとポリシーが含まれる。データセキュリティの節では、そのような統制を監視あるいは実施するための、具体的な統制技術と推奨項目について検討する。

[35] **IDA** - Intrusion Detection Algorithm 侵入検知アルゴリズム

5.4 データセキュリティライフサイクル

*データセキュリティライフサイクル*は、かなり成熟した分野だが、セキュリティ専門家のニーズにうまく対応していない。データセキュリティライフサイクルは、情報管理とは異なり、セキュリティ分野の人々のニーズを反映している。以下に述べるのはこのライフサイクルの要約である。完全なバージョンは http://www.securosis.com/blog/data-security-lifecycle-2.0 を参照されたい。

ライフサイクルは生成から破棄まで六つのフェーズに分かれる。図では、フェーズが一方向に進むように描かれているが、データは一旦作られると、各フェーズの間を無制限に行き来する。また一方で、すべての段階を経由するとは限らない（例えば、すべてのデータが必ず破棄されるわけではない）。

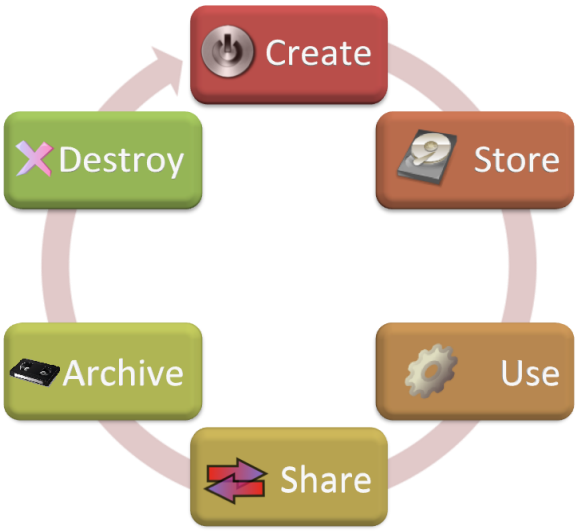


図 1—Data Lifecycle

1. **Create (作成).** 作成とは、新しいデジタルコンテンツの生成、あるいは既存コンテンツの変更/更新/修正をさす。
2. **Store (保存).** 保存は、デジタルデータを何らかの格納庫（データベース）に登録する作業で、通常は生成とほぼ同時に起こる。
3. **Use (利用).** データは閲覧、処理、あるいは他の何らかの作業に利用されるが、修正は含まれない。
4. **Share (共有).** 情報が他者、たとえばユーザ、利用者、パートナーなどからアクセス可能となる。
5. **Archive (アーカイブ).** データが高い頻度では使われなくなり、長期ストレージに移る。
6. **Destroy (破棄).** データは物理的またはデジタル手法（例えば暗号破砕法）により恒久的に破棄される。

5.4.1 位置とアクセス

このライフサイクルは、情報遷移のフェーズを表現しているが、情報の位置やアクセスの方法は示していない。

位置

これはライフサイクルを単一かつ一方向の操作と考えず、一連の小さなライフサイクルが、異なる操作環境でそれぞれ動いている、と考えることで表現される。ほとんどどのフェーズにおいても、データはその環境の間を出入りできる。

起こりうるあらゆる規則上、契約上、あるいは他の司法上の問題に備え、データの論理的、物理的な位置を把握することが非常に重要である。

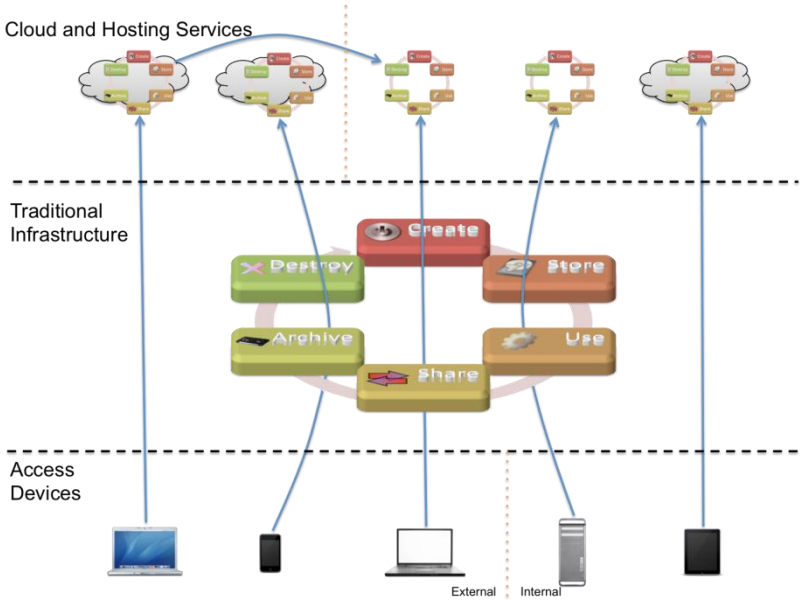


図 2—Cloud Access Devices

アクセス

ユーザは、データがどこにあってどう動くかを知るとき、誰がどのようにそのデータにアクセスするのか、を知る必要がある。ここで、以下の二つの要素がある:

1. 誰がそのデータにアクセスするのか？
2. 彼らはどのようにアクセスするのか（デバイス、チャネルは何か）？

今日、データは様々な異なるデバイスからアクセスされる。これらのデバイスは異なるセキュリティ特性を持ち、異なるアプリケーションや端末を利用することがある。

5.4.2 機能、アクター、統制

次のステップでは、アクター(人またはシステム）とデータの位置を特定して、データに対して行う機能を特定する。

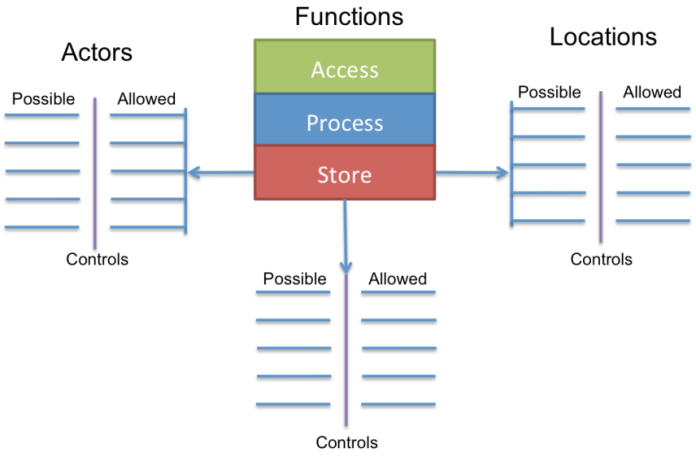


図3—Functions vs. Controls

機能

与えられたデータについて、以下の３つのことができる:

- **Access (アクセス).** データ閲覧/アクセス。生成、複製、ファイル転送、頒布、あるいは他の情報交換を含む。
- **Process (処理).** データのトランザクション処理実行、データ更新、業務処理トランザクションの中での利用、などを行う。
- **Store (保存).** ファイルやデータベースなどの中で）データを保持する。

以下の表は、どの機能がライフサイクルのどのフェーズに対応するかを示している:

表1—Information Lifecycle Phases

	Create	Store	Use	Share	Archive	Destroy
Access	X	X	X	X	X	X
Process	X		X			
Store		X			X	

アクター（アクセスデバイスに対応する人、アプリケーション、システム/プロセス）は、それぞれの位置でそれぞれの機能を実行する。

統制

*統制*は、可能な動作のリストを、許可される動作に絞りこむ。以下の表は、ユーザが可能な動作リストと統制項目とを対応づける一例を示す。

表2—Possible and Allowed Controls

Function		Actor		Location	
Possible	Allowed	Possible	Allowed	Possible	Allowed

5.5 情報ガバナンス

情報ガバナンスは、情報の利用の仕方を管理するポリシーと手続きを含む。それは以下の特徴を備えている:

- **情報分類.** 重要な情報カテゴリのハイレベルな記述。データ分類とは異なり、組織のすべてのデータをラベルづけするよりも、どのセキュリティコントロールを適用するかを決める「規制」や「企業秘密」のような、ハイレベルのカテゴリを定義することが目的である。
- **情報管理ポリシー.** 異なる情報タイプごとにどんな操作が許可されるかを定義するポリシー。
- **位置と司法ポリシー.** データが地理的にある場所に置かれると、その場所に特化した重要な法規や行政規則が適用される。
- **認可.** 社員、ユーザのどちらのタイプがどのタイプの情報にアクセスできるか、を定義する。
- **所有権.** 最終的に誰がその情報に責任を持つかを示す。
- **管理権.** オーナーの要請に基づき、誰がその情報の管理に責任を持つかを示す。

5.6 データセキュリティ

データセキュリティは、情報ガバナンスの実施に用いる特別の統制方法と技術を含む。これは、クラウドへ移行するデータの検出（と予防）、クラウドへの転送において、異なるプロバイダ/環境間で転送を行う場合のデータ保護、クラウド内部に入った後のデータ保護、という３つのセクションをカバーする。

5.6.1 クラウドへ移行するデータの検出と予防

組織がクラウド利用で直面する共通な課題はデータ管理である。多くの組織は、個人、あるいはビジネスユニットが IT 部門やセキュリティ部門の承認を得ないまま、ときには通知さえせずに機密データをクラウドサービスに移してしまうと報告している。

これまでの（アクセス制御や暗号のような）セキュリティ統制に加え、未承認データのクラウド移行を管理する支援として二つのステップがある:

1. データベース動作モニタ（**DAM**[36]）、ファイル動作モニタ（**FAM**[37]）によって大規模な内部のデータ移行を監視する。
2. URL フィルタや情報漏えい対策ツールによってクラウドへのデータ移動を監視する。

内部データ移行

データをクラウドに移動可能にする前に、現在格納されているデータベースからデータを引き出す必要がある。データベース動作モニタは、データのクラウドへの移行を示す予兆、すなわち管理者や他のユーザが大量のデータセットを抜き出したり、データベースを複製したりすることを検出する。

[36] **DAM** - Database Activity Monitoring ：データベース動作モニタ
[37] **FAM** - File Activity Monitoring ：ファイル動作モニタ

ファイル動作モニタはファイルシェアのようなファイル格納ツールについて、同様な保護機能を提供する。

クラウドへの移動

URL フィルタリング（Web コンテンツセキュリティゲートウェイ）と情報漏えい対策ツール（DLP）の組み合わせにより、企業からクラウドへ移されるデータを検知することができる。

URL フィルタリングは、ユーザがクラウドサービスに接続することの監視（そして予防）を可能にする。これらのサービスの管理インタフェースは、普通はエンドユーザと異なるアドレスを用いるので、管理コンソールに誰かがアクセスするのと、プロバイダがホストしているアプリケーションにユーザがアクセスすることは判別できる。

カスタムカテゴリの作成要求や、ユーザが宛先アドレスの管理をしなければならないツールではなく、クラウドサービスのリストを提供し、常に最新の状態に更新する（URL フィルタリングの）ツールを探すことが不可欠である。

より大きな粒度の対策として、情報漏えい対策（DLP: Data Loss Prevention）ツールを用いる。DLP ツールは、宛先だけでなく、転送されている実際のデータ/コンテンツも見ている。こうしてユーザはデータの分類に基づいて、警告を発したり（データをブロックしたり）できる。例えば、ユーザは企業の個人データを承認されたクラウドサービスに移すことを許可し、同じコンテンツが承認されていないサービスに移行するのはブロックできる。

DLP ソリューションをどこに配置するかによって、データ漏洩がどれだけ検知できるかが決まる。例えば、企業ネットワーク環境の外側にいる様々なユーザ（従業員、ベンダ、利用者）に向けた（社外の）クラウドソリューションを利用する場合、DLP ソリューションを企業の境界に設置してしまうと、その機能は回避され、無効になる。

5.6.2 クラウドへ（あるいはクラウド内部で）移動するデータの保護

パブリック、プライベートいずれのクラウド配備モデルにおいても、またすべてのクラウドサービスモデルを通じて、転送中のデータの保護は重要である。これは、以下の要素を含む:

- 従来型のインフラストラクチャから、パプッリック/プライベート、社内/社外、その他の組み合わせをまとめて含むクラウドプロバイダへのデータ移動。
- クラウドプロバイダ間のデータ移動。
- あるクラウド内の仮想サーバ間（あるいは他の資源要素間）のデータ移動。

以下の三つのオプション（あるいは優先順位）がある:

1. **クライアント/アプリケーション暗号化.** データは送信前にエンドポイントやサーバで暗号化されるか、または適切なフォーマットで暗号化して格納されている。これはローカル端末（エージェント型）暗号化（格納ファイル用など）や、アプリケーションと統合した暗号化を含む。
2. **リンク/ネットワーク暗号化.** SSL、VPN、SSH などを含む標準ネットワーク暗号技術。ハードウェア、ソフトウェアどちらの実装も利用できる。エンドツーエンドの暗号化が望ましいが、すべてのアーキテクチャに必須ではない。

3. **プロキシ型暗号化.** データはプロキシ型のアプライアンスか、サーバに転送され、そこで暗号化された後にネットワークに転送される。しばしば、既存アプリケーションとの統合がオプションとして好まれるが、一般的には推奨できない。

5.6.3 クラウド内のデータ保護

クラウドコンピューティングで利用できる機能のオプションや技術は非常に多岐に渡るため、可能なセキュリティのオプションをすべてカバーすることは困難である。以下では、様々なクラウドモデルにおいてデータを保護するためのより有効な技術、あるいはベストプラクティスのいくつかを示す。

5.6.3.1 コンテンツディスカバリー

コンテンツディスカバリーは、ストレージに格納された重要な情報を識別するツールと手続きである。これにより、組織は情報のタイプ、構造、分類などに基づくデータ保護ポリシーを定義し、先進のコンテンツ解析技術を用いて格納データを調べ、機密情報がどこにあるか、またポリシー違反があるか、を判定する。

コンテンツディスカバリーは、普通は DLP ツールの機能であり、例えばデータベースの場合、データベース動作モニタ（DAM）製品を使うことができる。データのスキャンは共有ファイルに直接アクセスしてもよいし、OS 上で動作するローカルエージェントソフトを使ってもよい。このツールは「クラウド対応」が必須であり、あなたのクラウド環境で動作できなければならない（例えばオブジェクトストレージをスキャンできる必要がある）コンテンツディスカバリーは、管理サービスとして利用することもできる。

5.6.3.2 IaaS 暗号化

5.6.3.2.1 ボリュームストレージ暗号化

ボリューム暗号化は、以下のリスクからデータを守る:

- ボリュームをスナップショットの複製/露出から守る
- ボリュームをクラウドプロバイダ（あるいはプライベートクラウド管理者）の無用な探索行為から守る
- ボリュームを物理ドライブの抜き取りによる情報露出から守る（現実のセキュリティ課題というよりもコンプライアンスが重要）

IaaS ボリュームは三種類の方法によって暗号化される:

- **仮想マシン管理暗号化.** 暗号化エンジンは仮想マシンインスタンスの中で動作し、暗号鍵はボリュームに格納されるが、パスワードや鍵のペアで保護される。
- **外部管理暗号化.** 暗号化エンジンは仮想マシンインスタンスの中で動作するが、鍵は外部で管理され、要求に応じて仮想マシンに発行される。
- **プロキシ暗号化.** このモデルでは、ユーザはボリュームを特別な仮想マシン、またはアプライアンス/フトウェアに接続し、その後そのインスタンスを暗号化インスタンスに接続する。プロキシはすべての暗号化操作を制御し、システム内部、外部のいずれかの方法で暗号鍵を保管する。

5.6.3.2.2 オブジェクトストレージ暗号化

オブジェクトストレージ暗号化は、ボリュームストレージと同じリスクについて、その多くを防ぐ。オブジェクトストレージは、よりしばしば公衆ネットワークにつながれるため、ユーザが仮想プライベートストレージ

を実装できるようにしている。VPN と同様に、**VPS**[38]はエンドユーザに共有されるインフラストラクチャを利用しながらデータを保護できる。たとえデータが他者に流れても、暗号鍵を持つ者しかそれを読めないからである。

- **ファイル/フォルダ暗号化と企業向けデジタル著作権管理.** ファイル/フォルダの標準暗号化ツールと、EDRM[39]を使い、オブジェクトストレージの格納前にデータを暗号化する。
- **クライアント/アプリケーション暗号化.** オブジェクトストレージをアプリケーション（モバイルアプリケーションを含む）のバックエンドとして使う場合、アプリケーションや端末にデータが埋め込まれる前に、暗号化エンジンでデータを暗号化する。
- **プロキシ暗号化.** データはオブジェクトストレージに送られる前に、暗号化プロキシで暗号化される。

5.6.3.3 PaaS 暗号化

PaaS は非常に広範囲であり、以下のリストはすべての想定しうるオプションをカバーするとは限らない:

- **クライアント/アプリケーション暗号化.** データは PaaS アプリケーション内部、あるいはプラットフォームにアクセスする端末内で暗号化される。
- **データベース暗号化.** データは暗号化機能がビルトインされたデータベース内で暗号化され、データベースプラットフォームでサポートを受ける。
- **プロキシ暗号化.** データは PaaS プラットフォームに送られる前に、暗号化プロキシで暗号化される。
- **その他.** 追加的なオプションとして、PaaS プラットフォームにビルトインされた API、外部暗号化サービス、そのバリエーションなどがある。

5.6.3.4 SaaS 暗号化

*SaaS プロバイダ*は上記で議論したオプションを利用することができる。マルチテナント間の独立性のためには、利用者ごとの暗号鍵を用いることを推奨する。以下に、SaaS ユーザのためのオプションを示す:

- **プロバイダ管理暗号化.** データは SaaS アプリケーション内部で暗号化され、一般にはプロバイダによって管理される。
- **プロキシ暗号化.** データが SaaS アプリケーションに送られる前に、暗号化プロキシで暗号化される。

暗号化操作では、共通鍵、公開鍵/秘密鍵のペア、**PKI/PKO**[40]（公開鍵基盤/操作）方式の拡張などから、最も適切な暗号化方式を用いるべきである。暗号化と鍵管理についての詳しい情報は、11 章を参照されたい。

[38] **VPS** - Virtual Private Storage 仮想プライベートストレージ

[39] EDRM - Enterprise Digital Rights Management 企業向けデジタル著作権管理

[40] **PKI/PKO** – Public Key Infrastructure/Operations - 公開鍵基盤/操作

5.6.4 情報漏えい防止

情報漏えい防止ツール（DLP）は、以下のように定義される:

集中管理されるポリシーに基づき、詳細なコンテンツ解析を行い、記録されているか、転送中か、利用中かによらず、データの識別、監視、保護を行う製品。

DLP はポリシー違反が検出されたデータの扱いについてオプション機能を提供する。データはブロック（作業を停止）することもできるし、DRM、ZIP、OpenPGP などの方式を用いた暗号化処理を行って作業を進めることもできる。

DLP は、通常コンテンツディスカバリーや、以下のオプションを用いた移動中のデータ監視に用いられる:

- **専用アプライアンス/サーバ.** クラウド環境と他のネットワーク/インターネットの境界や、異なるクラウドセグメントの境界にあるネットワークのボトルネック地点に置かれる標準ハードウェアである。
- **仮想アプライアンス**
- **エンドポイントエージェント**
- **ハイパーバイザーエージェント.** DLP のエージェントは、仮想マシン上で実行されず、ハイパーバイザー（仮想マシンモニタ）レベルに埋め込まれるか、アクセスされる。
- **DLP SaaS.** DLP はクラウドサービス（例えば E メールのホスティング）に統合されるか、またはスタンドアロンサービスとして提供される（典型的にはコンテンツディスカバリーツールとして）。

5.6.5 データベースとファイルの動作監視

データベース動作モニタ（DAM）は以下のように定義される:

データベース動作モニタは少なくとも、リアルタイム、またはそれに近い性能で、データベース問い合わせ言語（SQL）によるすべての操作を検出、記録する。これにより、複数データベースプラットフォームを横断するデータベース管理者の活動をとらえ、ポリシー違反に対して警告を発することができる。

DAM はデータベース動作の監視と、SQL インジェクション攻撃や管理者の無認可のデータベース複製など、ポリシー違反行為への警告をほぼリアルタイムで行う。クラウド環境の DAM ツールは、典型的にはエージェントが中央の情報収集サーバ（通常仮想化される）につながる構成をとる。これは利用者ごとに専用のデータベースを用いる場合を想定するが、将来的には PaaS で利用できるかもしれない。

ファイル動作モニタ（FAM)は以下のように定義される:

ユーザレベルにある専用のファイル格納領域に対するすべての操作を監視、記録し、ポリシー違反に対して警告を発する製品。

クラウド対応の FAM は、ユーザ端末側にエージェントを配備するか、ユーザとクラウドストレージの間に物理的な FAM アプライアンスを設置して利用する。

5.6.6 アプリケーションセキュリティ

データ流出事故のうち、アプリケーション層、特に Web アプリケーションへの攻撃によって引き起こされるものの割合は非常に大きい。アプリケーションセキュリティのより詳細な情報については 10 章を参照されたい。

5.6.7 プライバシー保護型ストレージ

ほとんどすべてのクラウドストレージシステムは、信頼関係構築のために、通信の一方の終端、あるいは両端において、通信参加者（クラウドユーザやクラウドサービスプロバイダ)になんらかの認証を要求する。暗号による証明書は多くの場合、十分な安全性を提供できるが、これは実際に利用する人（クラウドユーザ）が誰であるかを特定することが目的であり、プライバシーに対する配慮は十分ではない。こうした証明書を使うとき、認証を要求する側に対し、証明書の持ち主の ID 情報が常に開示される。証明書の利用により、持ち主の個人情報を不必要に開示してしまうケースがたくさんある（例えば電子健康記録の格納）。

過去 10-15 年の間、通常の暗号証明書のように信頼でき、かつ証明書の持ち主のプライバシーを守れる（持ち主の個人情報を秘匿する）システムを構築するため、多くの技術が開発されてきた。そうした技術のひとつである属性ベース証明書(ABC: attribute-based credential)は、デジタル（秘密）署名を用いた一般的な暗号化証明書（例えば X509 証明書）とまったく同じように発行される。しかし、属性ベース証明書は、オリジナルの属性情報の一部分だけを含む新しい証明書に変換することができる。しかも、変換された証明書は従来の暗号証明書（発行者の公開鍵を使う）と全く同様に検証され、同じセキュリティ強度を保つことができる。

5.6.8 デジタル著作権管理（DRM）

デジタル著作権管理の核心はコンテンツを暗号化し、複数の権益を保護することである。保護する権益は、例えばコピー禁止のような簡単なものだったり、カットアンドペースト、E メール、コンテンツ変更、などの動作に対しユーザやグループの制限ルールを指定するような複雑なものだったりする。DRM で保護されたデータと協調動作する任意のアプリケーションやシステムは、権益情報を翻訳し実装しなければならない。権益情報は一般に、鍵管理システムとの統合の手段でもある。

デジタル著作権管理には、以下の二つの大きなカテゴリがある:

- **コンシューマ向け DRM** は、膨大な数のユーザに向けた音声、動画、電子書籍など、広域に配信されるコンテンツを守るために用いられる。異なる様々な技術や標準があるが、一方向の配信、という点が重要である。
- **企業向け DRM** は、組織内のコンテンツ、あるいはビジネスパートナーと共有するコンテンツを守るために用いられる。より複雑な権利やポリシー、ビジネス環境との統合、特に企業ディレクトリサービスとの統合が重要である。

企業向け DRM は、クラウドに格納したコンテンツを安全に守ることができるが、インフラストラクチャとの密な統合が必要である。これは文書ベースのコンテンツ管理・配信に非常に有効である。コンシューマ向け DRM は、コンシューマへのコンテンツ配信を安全に守ることができるが、たいていの技術がいつかは破られるにもかかわらず、配信履歴をきちんと記録していない。

5.7 推奨事項

- 使われているクラウドストレージアーキテクチャを理解し、これをもとにセキュリティリスクや利用しうるコントロールを決定する。
- 可能なら、データ分散配置ができるストレージを選ぶ。
- データセキュリティライフサイクルを用いてセキュリティ要件を特定し、最も妥当なコントロールを決定する。
- 重要な内部データベースやファイル格納装置を DAM、FAM を用いて監視し、クラウドへのデータ流出を示唆する大規模データの移行を検出する。
- 従業員のインターネットアクセスを URL フィルタリングや DLP ツールで監視し、重要なデータのクラウドへの流出を検出する。クラウドサービスの定義カテゴリに合ったツールを選択する。未承認の動作をブロックするためフィルタリングを利用することを考える。
- クラウドへ、あるいはクラウド内で移動するあらゆる重要データをネットワーク層で暗号化するか、またはネットワーク転送の前のノードで暗号化する。これは、すべてのクラウドサービスモデル、デプロイメントモデルにあてはまる。
- データ暗号化を使う場合、鍵管理に特に注意する（11 章参照）。
- クラウドストレージをコンテンツディスカバリーツールで検査し、露出している重要データを検出する。
- スナップショット記録や未承認の管理者アクセスにおけるデータ露出を制限するため、IaaS の重要なボリュームを暗号化する。具体的な適用技術は運用上のニーズによって変わる。
- オブジェクトストレージの重要データを暗号化する。普通はファイル/フォルダ、あるいはクライアント/エージェント暗号化を用いる。
- PaaS アプリケーションやストレージの重要データを暗号化する。ほとんどのクラウドデータベースがネイティブ暗号化をサポートしないため、アプリケーションレベルの暗号化がしばしば好まれる。
- アプリケーション暗号化を使う場合、可能な限りアプリケーション外で鍵を格納する。
- 暗号化が SaaS で必要な場合、ネイティブ暗号化を提供するプロバイダを探してみる。プロバイダがみつからず、なおかつ信頼レベルを満たす必要がある場合は、信頼に足らないレベルである場合は、プロキシ暗号化を用いる
- 展開されたクラウド環境からのデータ流出を情報漏えい対策ツール（DLP)で検知する。通常これは IaaS 対応のみである。またパブリッククラウドプロバイダには利用できないかもしれない。
- データベース監視モニタ（DAM）により重要なデータベースを監視し、セキュリティポリシー違反アラームを発生させる。クラウド対応ツールを利用する。
- 通常のクラウドアクセスで、重要なユーザ情報が露出してしまうインフラストラクチャやアプリケーションを提供する場合、プライバシー保護型ストレージの利用を考える。
- 最も大きなセキュリティ違反は、貧弱なアプリケーションセキュリティの結果であることを覚えておく。
- クラウドプロバイダはこれらの施策を忠実に実施するだけでなく、データセキュリティツールとそのオプションを利用者に対して提供する。

- 契約終了、あるいは他の理由によるクラウドベンダからのデータの削除は、SLA を設定し、その一環として詳細にカバーされるべきである。これはユーザアカウントの削除や移行、あるいは主ストレージ/バックアップストレージからのデータ削除や鍵転送、などを含む。

5.8 要求事項

- ✓ データセキュリティライフサイクルを用いて、セキュリティ上の課題を識別し、もっとも妥当なコントロールを決定する。
- ✓ 起こりうるあらゆる規則上、契約上、あるいは他の司法上の問題に備え、データの論理的、物理的な位置を把握することが非常に重要である。
- ✓ URL フィルタリングや DLP ツールを用いて従業員のインターネットアクセスを監視し、クラウドへの重要データの移動を検知する。
- ✓ クラウドへ、あるいはクラウド内で移動する重要データについては、ネットワーク層の暗号化を行うか、ネットワーク転送前のノードで暗号化を行う。
- ✓ IaaS において、スナップショットや未承認の管理者アクセスによるデータ露出を制限するため、重要なボリュームを暗号化する。
- ✓ PaaS アプリケーションやストレージの重要なデータを暗号化する。

参考文献

[1] RABIN, M. O. 1989. Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance. J. ACM, 36(2), 335–348.

[2] SECUROSIS. 2011. The Data Security Lifecycle. http://www.securosis.com/blog/data-security-lifecycle-2.0

[3] SECUROSIS. 2011. Understanding and Selecting a Data Loss Prevention Solution. http://www.securosis.com/research/publication/report-data-loss-prevention-whitepaper

[4] SECUROSIS. 2008. Understanding and Selecting a Database Activity Monitoring solution. http://www.securosis.com/research/publication/report-selecting-a-database-activity-monitoring-solution/

[5] CHAUM, D. L. Feb. 1981. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM, 24 (2), 84-90.

第 6 章 //
相互運用性と移植容易性

クラウドコンピューティングの出現により、「昔ながらの」社内システムの能力を遙かに超える無尽蔵のコンピューティングパワーと管理能力を事業組織が得られるようになった。コンピューティングパワーはほぼ瞬時に追加でき、自由に移動できる一方で、事業上不要となった場合は容易に破棄することができる。新しいアプリケーションサポートシステムは週単位ではなく、時単位での増設要求に応えるように作られている。フォールバックの要求から、新規に追加したが余剰となったリソースは、ハードウェアが待機状態に入るか否かにかかわらず、即時にシャットダウンできる。環境に起因する相互運用性と移植容易性をより柔軟に利益として享受させることこそ、IaaS から SaaS までのあらゆるクラウドシステムにとっての目的である。

クラウドがもたらす相互運用性と移植容易性の 1 つの効果は、世界規模で展開する地理的にも離れた複数のサービスプロバイダやシステムオペレーションを行うプロバイダ間で、サービスをあたかも 1 つであるかのように提供することができることである。また、もう 1 つの効果として、プラットフォーム間やプロバイダ間でのデータやアプリケーションの移植を容易にすることがある。

相互運用性と移植容易性はクラウドコンピューティングにより改めて出てきた発想ではなく、また関連するセキュリティもクラウドにおける相互運用性と移植容易性に特化したものではない。しかし、オープンであり、時にはコンピューティング環境を共有するため、クラウドはより広範囲な事項を事前に注意する必要が今までのシステムに比べて求められる。マルチテナント性の環境では、ユーザが意識するしないにかかわらず、機密情報も含めて自社のデータやアプリケーションは他社のものと隣接し、プラットフォームやストレージ、ネットワークを共有することになる。

この章では相互運用性と移植容易性を検討するに当たり、重要な考慮事項について述べる。

概要. この章の各項では、相互運用性と移植容易性の下記の内容に関して定義する:

- 相互運用性の概要
- 相互運用性を実現するための要求事項
- 移植容易性の概要
- 移植容易性を実現するための要求事項

6.1 相互運用性の概要

相互運用性はエコシステム中にあるクラウド同士が協調動作することでユーザの求めるサービスを実現することである。

クラウドコンピューティングのエコシステムにおいて、構成するコンポーネントは異なるソース、クラウドやレガシーパッケージ、パブリックやプライベートクラウドを組み合わせるなど、異なる要素から構成されてい

る(ハイブリッドクラウドのこと)。相互運用性を構成するコンポーネントは、あえて言えばシステム間でのデータ交換が出来るとも言え、更新もしくは異なるプロバイダから提供されるものに変更できる。

事業面からのプロバイダの変更は、かなりの時間をかけて形成され、決断に至る。変更の要望は以下の理由を含んでいる:

- 契約更新時における受け入れがたい程のコストの増加
- 他プロバイダによる、より安価で同等のサービス提供
- プロバイダのサービス終了
- プロバイダが突然サービスを停止することによる受け入れがたいマイグレーションプランの発生
- 受け入れがたいサービス品質の低下、例えば要求する重要パフォーマンスや、実現するアーカイビングサービスレベル(**SLA's**)[41]
- クラウド利用者とプロバイダ間の事業契約に関する争議

相互運用性の欠如(移植容易性も含む)は特定のクラウドプロバイダへのロックオンを発生させる。

相互運用性がどの程度達成でき、維持されるかのレベルは、クラウド化のプロジェクトの用いるクラウドプロバイダがオープン、または実用済み、アーキテクチャ化とスタンダート化したプロトコルやスタンダードな**API's**[42]をどの程度用いるかにかかっている。とはいえ多くのベンダが「オープン」で「スタンダードベース」の対策をしたクラウド向け製品を提供しても、既存製品から持つ仕掛けや機能拡張(Eucalyptus[43])、機能強化により相互運用性や移植可能性は妨げられる。

6.2 移植容易性について

移植容易性はプロバイダやプラットフォーム、OS、インフラ、物理的な場所、ストレージの違い、データフォーマットや API の違いに関わらず、容易にアプリケーションコンポーネントを移動し、再利用できることを要件とする。

相互運用性と移植容易性はクラウド環境がパブリックやプライベート、ハイブリッドのいずれであろうと考慮されなければならない。たとえ SaaS、PaaS、IaaS いずれのサービスモデルのマイグレーション戦略でも考慮されるべき重要事項である。

移植容易性はクラウドプロバイダ選定における最重要課題である。その理由はベンダロックを避けると共に、事業からの恩恵を拡大するために、類似する他のクラウドベンダのソリューションを利用することにある。それにより、分散ソリューションによる災害復旧やグローバルへの展開を単一ソリューションで実現できる。

クラウドサービスにおける移植容易性を実現することは、アーキテクチャ的に同一のクラウドキューブ(1 章参照)内に両サービスが存在しているかどうかに依存する。異なるクラウドキューブに存在している場合、サービスをポーティングすることは、再度他のクラウドサービスにアウトソースする前に、一度「内部」にサービスを戻すことを意味する。

[41] **SLA** - Service Level Agreement
[42] **API** - Application Program Interface
[43] **Eucalyptus** - Amazon EC2 と API 護岸のあるクラウド基盤

クラウドのマイグレーションにおいて、移植容易性と相互運用性の適切な取り組みに失敗することは、クラウドの移植時に求められる恩恵を損ない、移植を実現するために費用面の問題やプロジェクトの遅延をもたらす。そのためには、下記に上げる要因を避けるべきである:

- アプリケーション、ベンダ、プロバイダによるロックイン　－　特殊なクラウドソリューションの選択は、他のクラウド環境や他のベンダへの移行が制約される。
- 互換性のない処理や処理の輻輳によるサービスの混乱　－　利用するプロバイダ、プラットフォーム、またはアプリケーションの違いが、アプリケーションの相互機能不全を異なるクラウドインフラ上に発生させ、相互利用性の喪失を発生させる。
- 予期しないアプリケーションの再設計や事業プロセスの変更　－　新しいクラウドプロバイダへの移行は、プロセス機能の再設計や本来の機能を維持するためのコード変更を要求することがある。
- データ移行やデータ変換に費用の発生　－　相互運用性や移植容易性を持たないデータフォーマットは新しいプロバイダへの移行の際に突発的なデータ構造の変更を発生させる。
- 新しいアプリケーションや管理ツールによる要員の再教育
- データまたはアプリケーションセキュリティの喪失　－　異なるセキュリティポリシーやセキュリティ管理、鍵管理やプロバイダ間のデータ保護は新しいプロバイダやプラットフォームへの移行の際に見えないセキュリティギャップを招くおそれがある。

クラウド上のサービスに移行するということはアウトソースすると言うことである。アウトソースにおける黄金律は「事前に理解したことを、いかに契約上に反映するか」である。それ故に移植容易性(と相互運用性の拡張)は、いかなる組織におけるクラウドサービスへの移行における重要な要因であり、開発を不要にするための実現可能な方法論である。

6.3 推奨事項

6.3.1 相互運用性に関する推奨事項

ハードウェア　－　物理的なコンピュータハードウェア

ハードウェアアーキテクチャやハードウェア自体は時代と共に変わり続け、ハードウェアへのダイレクトアクセスが必要な場合、プロバイダ間の相互運用性のギャップが不可避となる。

- 可能であれば仮想化技術を用い、可能な限りハードウェア依存を取り除く。ただし仮想化技術でも現在稼働中のシステムにおけるすべてのハードウェアに依存する影響を取り除くことはできない。
- ハードウェアを直接取り扱わなければならない場合、プロバイダの変更に備えて全く同じかそれ以上のハードウェアを、同レベルのセキュリティ管理で事前手配することが重要である。

物理ネットワークデバイス

セキュリティデバイスを含むネットワークデバイスはサービスプロバイダごとに異なる API と設定がなされている。

- 相互運用性を持った物理的ネットワークハードウェアやネットワークやセキュリティの装置は仮想ドメインに収容すべきである。できることなら API が同一の機能を持つことが好ましい。

仮想化

仮想化で物理的なハードウェアの制約を解消した場合、市場にあるハイパーバイザーソフト、たとえば Xen、VMWare やその他、の相違点が明らかになってくる。

- OVF のようなオープンバーチャライゼーションフォーマットを用いることは相互運用性の向上に寄与する。
- 特定の仮想化にフックした記録や理解は、他のハイパーバイザー上では用いることが出来ない。

フレームワーク

異なるプラットフォームのプロバイダが異なるクラウドのアプリケーションフレームワークと差分を持つことは相互運用性に影響を与える。

- 新しいプロバイダに移行する際に必要となる API の相違点の特定や、アプリケーション動作についていかなる変更が必要となるかを調査する。
- オープンかつ公開済みの API を用いることは、サービスプロバイダを変更せざるを得ないときのコンポーネント間の相互運用性や、サービスプロバイダ変更に際して発生するアプリケーションやデータの移行の支援における広範なサポートを実現する。
- クラウド中のアプリケーションでは、しばしばインターネットを介した相互運用や動作の切り替えの発生が予期される。あるコンポーネントの問題 (または反応の遅延)を究明することは、他のシステムへ与える悪影響やリモートコンポーネントが落ちた際にステートフルな従属関係にあるシステムデータの完全性へのリスクを避けることにつながる。

ストレージ

ストレージへの要求はデータの形式により変化する。構造化データはデータベースで最もよく使われ、もしくはアプリケーションの特定フォーマットにより必要とされる。非構造化データはワープロやスプレッドシート、プレゼンテーションソフトなど多くのエンドユーザアプリケーションで使われている。ここでは蓄積データをあるサービスから他のサービスに問題なく移行させるために考慮すべき事項を述べる。

- 非構造化データを移動可能な一般的フォーマットで保管する。
- 暗号化してのデータ転送の必要性を評価する。
    - 互換性のあるデータベースを確認し、もし必要があればデータ変換の必要性を評価する。

セキュリティ

システム内のクラウド中にあるデータとアプリケーションに対し、ユーザは制御権を全くまたはごく一部しか持つことができない。多くの重要アイテムは下記を含む相互運用で提供されるセキュリティを受けることとなる:

- SAML または WS-Security を用いることで、他にあるこれらを用いたシステムとの相互運用性を確保できる。詳細は第 12 章を参照のこと。
- クラウドの中に入る前の暗号化済みデータはクラウドの環境から不適切にアクセスをさせない手段を講じる。詳細な暗号化の詳細は第 11 章を参照のこと。

- 暗号鍵を使った場合、鍵の保管場所と暗号化済みデータ保管場所へのアクセス権を確保する。詳細な鍵管理については第 11 章を参照のこと。
- 使用しているサービスプロバイダからプロテクションの方法について、負っている責務と義務の間で妥協すべき事態が発生することを理解すること。
- クラウド環境へ移行する際、ログファイルの情報はすべての他のデータと同じセキュリティレベルで扱わなくてはならない。ログ管理システムが使われている状況であっても、移行前後で同等のログ分析を継続させる手段を講じ、ログファイルの相互運用性を確保する。
- 移行が完了後、オリジナルシステムにあるすべてのデータ、ログ、その他の情報を消去する手段を確保する。

6.3.2 移植容易性に対する推奨事項

多くの課題が、クラウドへの移行の際に発生する。移植容易性の判断と推奨事項は、以下のクラウド移行への影響に対応する;

- **サービスレベル** SLA はプロバイダにより異なるため、プロバイダを乗り換えた際にいかなる影響が発生するかを理解する必要がある。
- **異なるアーキテクチャ** クラウド内のシステムは全く異なるプラットフォームアーキテクチャ群が存在する。重要なのはこれらにより起きるサービスとプラットフォームの依存性、たとえば内包している API やハイパーバイザー、アプリケーションロジック、その他の制限により、移植容易性は制限を受ける。
- **セキュリティの変更** クラウドシステムは移植時のセキュリティのメンテナンスにおいて以下のような変わった考慮事項を発生させる:
- ユーザやプロセスからのシステムアクセスにおける認証と識別の機能は、クラウドシステム全体で絶対不可欠な機能である。SAML などのオープンスタンダードを用いた識別は移植容易性に寄与する。SAML アサーションを補助する内部的な IAM システムを開発し、内部システムが SAML で認証を行う構造は、将来的にシステムをクラウドへ移行することに寄与する。
    - 暗号鍵は内部的に第三者預託制度されなければならず、可能であれば定期的にメンテナンスされなければならない。
- デジタル情報の側面を持つにもかかわらず、直接ファイルやドキュメントで見ることができないため、(典型的な)メタデータはしばしば見落とされがちな側面を持つ。メタデータはファイルやドキュメントと共に動くため、クラウドにおいては重要な考慮対象である。ファイルやドキュメントがメタデータと共に新しいクラウド環境に移動する際には、コピーしたファイルやメタデータが後々まで残っていたり、情報漏洩の可能性にサラされることがないように、セキュアに消去されなければならない。

6.3.3 異なるクラウドモデルへの推奨事項

すべてのクラウドモデルには共通する根源的なリスクと考慮すべき推奨事項がある。

- クラウドプロバイダの変更に際し、通常これまで利用してきたクラウドプロバイダは難色を示す。3 章の契約内容の構成、7 章のビジネス継続プログラム、2 章のガバナンスの概要に基づいて計画されなければならない。
- クラウドプロバイダに預けるデータサイズを知っておくこと。莫大なサイズのデータはデータ移行の際にサービスの停止を引き起こしたり、予想以上の時間がかかることとなる。多くの利用者はデータの入ったハードドライブを配送する方が通信回線を用いた転送よりも大きなデータ移行を早くできることを知っている。
- セキュリティアーキテクチャや独立したコンポーネントのセキュリティコントロールの記録は内部監査に用いることができ、更に新しいプロバイダへの環境移行と新しい環境の妥当性確認に役立つ。

Infrastructure as a Service (IaaS)

クラウドプロバイダの果たす役割が、ストレージやコンピューティング能力等の提供に限定する場合、クラウドの利用者は相互運用性を持つアプリケーション設計作業を行う責任を持つ。クラウドプロバイダは標準化されたハードウェアやコンピューティングリソースで構成提供し、異種システムをごくわずかな労力で相互運用できるようにすべきである。クラウドプロバイダは相互運用性を保つために業界標準に厳しく準拠しなくてはならない。またクラウドブローカ、クラウドバースト、ハイブリッドクラウド、マルチクラウドフェデレーションなどの複雑なクラウドのシナリオに対応しなくてはならない。

- 仮想マシン のイメージをどうやって捕捉し、新しいクラウドプロバイダにポーティングするか、また誰が異なる仮想化技術を使うかを理解すること。例：Distributed Management Task Force (DMTF) Open Virtualization format (OVF)。
- 仮想マシンの環境にあるプロバイダ特有のあらゆる拡張機能を識別し、削除する(または最低限記録に残す)。
- アプリケーションをクラウドプロバイダに移行した際に、VM イメージがプロビジョニングできなくなる事例について理解する。
- ディスクやストレージデバイスの廃棄処理方法について理解する。
- アプリケーションやデータのマイグレーションの必要性を認識する前にハードウェアやプラットフォームベースの関係性を理解する。
- 以前のクラウドプロバイダから、システムログ、トレース、アクセスや課金情報へのアクセス方法を聞いておく。
- 新サービスが劣っていることが分かったときに備え、以前のクラウドプロバイダでの再起動やサービス拡張を一部または全体で行う方法を認識しておく。
- 新しいプロバイダにおいて互換性のない、または改変の余地がないマネジメントレベルの機能または API がないか特定する。
- クラウドプロバイダへの、又プロバイダ間でのデータ移動にかかる費用を確認する。
- たとえばデータ圧縮において、一般的にクラウドがどこまで処理できるか、データを移行する際のサポーを把握しておく。
- どのようなセキュリティが提供されていて、誰が暗号鍵を管理しているかを理解しておく。

Platform as a Service (PaaS)

この種のクラウドプロバイダはユーザがシステム上に自らのシステムを構築するためのプラットフォームを提供する。彼らはランタイム環境とアプリケーションスタックを用意する。開発側はインフラ整備の必要なく、カスタムアプリの迅速な開発と展開を容易にできる。一方クラウドプロバイダは彼らのインフラ全体を提供し、利用者のためにメンテナンスする。

- 可能なら標準的な構文で構成し、オープンな API とオープンスタンダードを採用する。たとえば Open Cloud Computing Interface (**OCCI**)[44]。
- セキュアにデータを転送、バックアップ、リストアするにはどのようなツールが有効かを理解する。
- PaaS 特有のアプリケーションコンポーネントやモジュールを理解および文書化し、抽象レイヤで既存のモジュールに直接アクセスすることを最小化する抽象化レイヤを持ったアプリケーションアーキテクチャを開発する。
- モニタリング、ロギング、監査など、どのサービスの内どれが新しいベンダに移行可能か理解する。
- クラウド中でどのようなセキュリティ防御策が提供され、どういったデータが作られているか、またそれらはどのようにメンテナンスされているかを理解する。
- 現在のクラウドプロバイダにおいて、どのような制御機能が動作しているかと新しいプロバイダへどうやって移行できるかを理解する。
- 新しい環境へマイグレーションする際に、アプリケーションのパフォーマンスと可用性にどれだけの影響を与えるかを測定する必要があることを理解する。
- サービスやアプリケーションが以前、以後のシステム間で移行が正確に成功したことをどのようなテストで確認するかを理解する。プロバイダもユーザも知名度のあるテストやその結果を確認する。

Software as a Service (SaaS)

この種のクラウドプロバイダは特定の実用アプリケーションをクラウド上で提供し、利用者は自身の情報を単に入出力する。利用者はブラウザを用いる必要があり、たいていの場合プロバイダに対する管理者権限を持つ。

- SaaS プロバイダを用いずに使用できるフォーマットで、通常のデータを抽出し、バックアップを行う。
- どのようなタイプのメタデータが保存され、移行されているかを理解する。
- 必要ならばデータのエスクローサービスを用いる。
- 将来利用者向けツールが更新される、新ベンダが同様のツールを提供する、または新しいベンダに置き換えられ入れ替えられてサポートする状況になる可能性があることを理解する。
- 新旧プロバイダ間で管理運用に関する一環性が保証されていることを確認、監査する。
- バックアップやその他のコピー動作に関するログや、アクセス記録、その他の関連記録を法的または他の理由により移管できるように手配する。
- マネジメント、モニタリング、インフラ運用の報告インタフェースと構造を理解する。

[44] **OCCI** - Open Cloud Computing Interface

- マイグレーション前にすべてのアプリケーションの評価テストを行い、新システム上でのカットオーバー前に同様のテストをできれば行っておく。

プライベートクラウド

プライベートクラウドは利用者がクラウド環境やサービスを自らの環境下に納めるか、クラウドプロバイダに委託するものである。(たいていの場合、社内ネットワークをサービスプロバイダのホスティングセンターまで拡張する)。

- 共通するハイパーバイザーを用い、相互運用性があることを確認する。たとえば KVM や VMWare や Xen などである。
- ユーザとユーザの持つ特権、VM イメージの管理、仮想マシン自体の管理、仮想ネットワークの管理、サービスマネジメント、ストレージマネジメント、インフラマネジメント、情報マネジメントなどにおいて、標準 API によってマネジメントが行われているかを確認する。

パブリッククラウド

パブリッククラウドにおいては公な相互運用性が最も重要な意味を持つ。ベンダ特有またはオープン性を特徴とし、インタフェースは OCCI や libcloud などとなる。

- クラウドプロバイダは共通またはオープンインタフェースをサービスからの要求があったときに公に提供できることを確認する。

ハイブリッドクラウド

このシナリオでは、ローカルなプライベートインフラは外部にあるクラウドプロバイダと協同することが求められる。「クラウドバースト」などのシナリオはローカルクラウドがピークに達したときに外部のクラウドに処理をロードするものである。

- クラウドプロバイダはサービス要求があったとき、すべてのクラウドに関する機能へのアクセスのための共通的かオープンインタフェースを公にしなくてはならないことを認識する。
- 異なるクラウドプロバイダとの同期は、より高いレベルの拡張性を実現することを認識する。

参考文献

[1] http://msdn.microsoft.com/en-us/library/cc836393.aspx

[2] http://blogs.msdn.com/b/eugeniop/archive/2010/01/12/adfs-wif-on-amazon-ec2.aspx

[3] http://download.microsoft.com/download/6/C/2/6C2DBA25-C4D3-474B-8977-E7D296FBFE71/EC2-Windows%20SSO%20v1%200--Chappell.pdf

[4] http://www.zimbio.com/SC+Magazine/articles/6P3njtcIjmR/Federation+2+0+identity+ecosystem

[5] http://www.datacenterknowledge.com/archives/2009/07/27/cloud-brokers-the-next-big-opportunity/

[6] http://blogs.oracle.com/identity/entry/cloud_computing_identity_and_access

[7] http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

[8] http://www.burtongroup.com

[9] http://www.pkware.com/appnote

[10] http://www.apps.ietf.org/rfc/rfc4880.html

セクション III //
クラウドにおける運用

第 7 章 //
従来からのセキュリティ対策、事業継続性、災害復旧

情報システムのアウトソースの方法としてクラウドコンピューティングが好まれるようになってから、ホスティングモデル特有のセキュリティの問題が非常に重要になってきた。クラウドコンピューティングというコンセプトには元々機密情報や機微情報を第三者または CSP[45]を信頼して預けるというリスクがある。

クラウドサービスの発展によって、企業は少ないリソースと予算で効率的な運用が可能になった。ビジネス上では目に見えるメリットが多くあるが、セキュリティのリスクは十分に評価し把握し解決しておくことで、IT サービスのアウトソース先としてクラウドサービスを利用する際に不安をなくすことができる。

この章は、Cloud Control Matrix Domains IS-01 と IS-02 および ISO/IEC 27002 Clause 9 にマップされる。

この章の目的はクラウドサービスのユーザに対して、クラウドサービスにおける従来のセキュリティ(物理セキュリティ)の基本的な考え方を共有することである。従来からのセキュリティは、盗難、スパイ活動、破壊、損害などから、従業員およびデータの物理的保管の安全性を守るための対策をすることである。 クラウドの情報セキュリティという意味では、これは、情報、製品、そして人が対象になる。

適切な情報セキュリティは、目的を達成するためにいろいろな階層で実施する。これは、「階層型セキュリティ」とか「多階層防御」などと言われる。セキュリティ対策に 100%安全というのはあり得ないということを責任者は認識して下さい。情報セキュリティは、階層の深さを使用し、その組み合わせによってセキュリティレベルを達成する。どこか 1 つの階層の弱点により、セキュリティが破られる。物理的保護は、クラウド情報セキュリティの階層化アプローチの最初のステップである。物理的保護がない、または間違った導入、弱い保護、一貫性のない実施、一時的な処理として扱われる（解雇になったら忘れろ)、または適切にレビューされず維持されていない場合は、最適な論理セキュリティ対策を講じても、物理セキュリティの弱みを補完することはできず、セキュリティ全体が失敗に終わることになる。

効率的な従来からのセキュリティの仕組みとは、リスク評価、脆弱性分析、BCP/DR 方針、プロセス、手順といったよく考えられた仕組みの上に成り立つ。すぐれた物理セキュリティの仕組みは、ビジネスと共に拡張可能で、全組織に導入が可能であり、運用状態が測定可能で、維持が可能であり、防衛力があり、改善が可能で、コスト効果があるものである。

概要: クラウドコンピューティングに関連するセキュリティリスクは独特であり 、クラウドサービスプロバイダの事業継続性、災害復旧、従来からのセキュリティ環境は、特定のセキュリティリスクとして網羅的に評価される必要がある(例えば、TOGAF[46], SABSA[47], ITIL[48], COSO[49], COBIT などの標準ガイドラインを用いるなど)。この章では、以下の内容を説明する:

[45] **CSP** - Cloud Service Provider
[46] **TOGAF** - The Open Group Architecture Framework
[47] **SABSA** - Sherwood Applied Business Security Architecture
[48] **ITIL** - Information Technology Infrastructure Library
[49] **COSO** - Committee of Sponsoring Organizations

- 物理セキュリティ機能の確立
- 人間系の物理セキュリティ
- 事業継続性
- 災害復旧

この章は、Cloud Control Matrix Domains FS-01, FS-02, FS-03,FS-04 および ISO/IEC 27002 Clause 9 にマップされる。

7.1 従来からのセキュリティ機能の構築

古くなった IT 設備、ネットワーク技術、通信などは、多くの組織で見落とされることが多くある。つまり、資産の安全性と可用性を維持するために適切な物理的な設備がない建物にコンピュータ、ネットワーク、ゲートウェイ等が設置されるケースがある。

クラウド環境で IT 設備、ネットワーク技術、通信設備のために適切な物理的セキュリティを確立するためには、クラウドプロバイダの組織内で適切な担当者が割り当てられていることが必要である。クラウドプロバイダ内で管理職の立場にいる者が、計画、導入、維持管理を担当する。物理セキュリティの担当者はトレーニングを受け、適切な業務評価が行われるべきである。クラウド環境で物理セキュリティを構築するには以下の項目を考慮する必要がある:

- 保護されるべき設備とサービスのためのセキュリティ
- 物理セキュリティ用の人員が割り当てられていること
- クラウドに移行する前に従来からの物理セキュリティ対策がどのように管理され、担当者が割り当てられているか
- これらの対策のための予算

物理セキュリティは、簡単なものではドアに鍵を追加することから、高度なものでは、武装した警備員の設置と複数レイヤの障害物を導入することがあげられる。適切な物理セキュリティは、適切な組み合わせによる多階層防御の考えを用いて、物理セキュリティの脅威を減少させたり、遅らせることでリスク管理を行う。インフラ、人員、システムに対する物理セキュリティの脅威は、侵入だけではない。これらのリスクを軽減するためには、アクティブおよびパッシブの両方の防備の方法を展開し、以下のような対策を取る必要がある:

- イベント、インシデント、攻撃を減少させたり、遅らせたりするための障害物
- セキュリティおよび環境条件を監視する検知システム
- 攻撃者を逮捕・撃退、諦めさせるようなセキュリティレスポンス

物理セキュリティは通常以下のいずれかの方法で設計および実行される:

- 環境設計
- 機械的、電気的、手順的コントロール
- 検出、レスポンス、回復手順
- 本人確認、認証、認可、アクセスコントロール
- スタッフのトレーニングを含んだ方針と手順

7.1.1　従来の物理セキュリティの評価

クラウドサービスプロバイダの従来のセキュリティの評価をする際、利用者はインフラを基本的なデータセンタープロバイダの infrastructure as a service あるいは物理的な状況の観点から検討を行う。これには、設備の物理的な所在地と重要なリスクおよび回復要因に関する文書も含まれる。

7.1.1.1　クラウドサービスプロバイダの設備の所在地

利用者は、データセンタの物理的所在地の評価をする必要がある。クラウドのサプライチェーンに依存している場合、依存しているクラウドのインフラを理解する必要がある。

設備の場所について以下の評価をすることを推奨する:

- 地震がよくおきるゾーンまたは地震のリスクを受けない場所であるか確認すること
- 洪水、土砂崩れなどの自然災害が発生する地域ではないこと
- 犯罪率が高い、政治的または社会的に不安定地域でないこと
- 設備の場所へのアクセスの便利しやすさ（また、アクセスできない頻度）

7.1.1.2　文書の確認

ホスティング企業が致命的なイベントが起こった際に、何をすべきかが判るようにした回復方法の文書は、評価をする上で非常に重要である。以下の文書は、データセンタープロバイダと契約する前に監査しておく必要がある:

- リスク分析
- リスク評価
- 脆弱性評価
- 事業継続性計画
- 災害復旧計画
- 物理および環境セキュリティポリシー
- ユーザアカウント停止手順
- 不測事態対応計画、テストプロトコルを含む
- 事故報告および対応計画、テストプロトコルを含む
- 緊急対応計画
- 設備レイアウト　—　非常口、CCTV カメラの位置、安全な入り口の確保
- 火災時非難経路図および火災時の命令系統
- 緊急避難計画と手順
- 緊急時の連絡手順

- 緊急時連絡先
- ユーザ設備へのアクセスの確認および監査記録
- セキュリティ意識向上のトレーニング、プレゼンテーション、資料、など。
- セキュリティ意識向上教育の参加者記録
- 主要役員の引き継ぎ計画
- 技術文書 – 電気配線図、BMS、UPS、AHU 詳細
- 電気、発電、CCTV の保守スケジュール
- 緊急時燃料サービスプロバイダとの契約
- 設備内に入室許可されている人員の一覧
- セキュリティ担当者の履歴書、経歴書
- セキュリティ担当者の身辺調査報告書（毎年実施）
- 主要設備と機器の定期保守契約書（障害時間と復旧作業の SLA に注意すること）

文書を検査する場合に、クラウドサービスの利用者のリスクが軽減されているかに焦点をおく。企業がクラウドへの移行を考えている場合に、クラウド環境で利用者にセキュアな環境を提供するためには、以下の推奨項目は重要である:

- 全ての文書が最新に更新されているか確認する。これらの文書は、最低一年に一回、CSP によってレビューされていること。更新履歴と内部でもレビューされている証明として管理職による承認が含まれており有効であること。
- 方針および手順書の文書（従業員用）は、イントラネットのサイトなどで閲覧可能になっており、CSP の社員はいつでもアクセス可能であること。セキュリティチームは、管理職が承認した最新バージョンがアップロードされていることを確認していること。
- 方針や手順書は、従業員が認識していて始めて効果がある。CSP が、セキュリティアウェアネスプログラムを行っているか確認する。最低限、CSP は一年に一度は、セキュリティア意識向上トレーニングを従業員に対して行っており、従業員の参加記録を必要とする。また、新しい従業員に対して、新入社員教育の一環としてセキュリティのオリエンテーションを行い、主要な方針および手順が説明されていることが必要である。本人の署名等出席が確認できるものを残し、いつでもレビューできるようにする。このプログラムの効果は、セキュリティチームのシニアスタッフがトレーニングを行う必要がある。

7.1.1.3 国際的または業界セキュリティ基準への準拠

CSP がグローバルセキュリティ基準 ISO 27001 ISMS や TOGAF、SABSA、ITIL、COSO、COBIT などの業界基準に準拠しているかを確認する。これらの基準に準拠する活動は、CSP のセキュリティレベルと成熟度を判断する基準になる。

- コンプライアンス証書と有効期限の確認

- リソース配分を確認できる証跡(コンプライアンスプログラムを維持するための予算、担当など)の受け入れ
- 内部監査レポート報告書と指摘事項に対する対応項目と状況を確認できる証跡

7.1.1.4 クラウドセキュリティプロバイダ設備の訪問検査

対象範囲

データセンタの境界セキュリティを評価することで、どのエリアが物理的にセキュアである必要があるかがわかる。以下はリスクが高いエリアであり、セキュアである必要がある:

- 総務エリア
- 受付エリア
- 駐車場
- 保管エリア
- 火災非常口
- CCTV 監視・指令センター
- 空調室(換気調整室)
- ロッカー室
- UPS 室
- 発電機室
- 燃料保管タンク

表示

以下の表示は非常に大切であり、適切な施設で適切に表示されているか確認して下さい:

- 火災時非難経路および非常口
- 火災時指示系統
- 火災案内標識
- セキュリティポスターと指示
- 共連れ禁止ポスター
- 温度/湿度に関する情報
- 警告と指示の標識
- 緊急時電話番号
- 報告経路チャート

7.1.2　インフラのセキュリティ

境界セキュリティは、侵入者、または不必要な訪問者の入室を最初に防止するラインであるため、重要である。境界セキュリティの基本は、技術変化にともない大きく変化する。境界セキュリティの４つの D とは、設備への侵入者に対して Deter, Detect, Delay and Deny(阻止、検出、遅延、拒否)を提供する。

以下の対策は、物理的なインフラプロバイダを選択する際に、あるとよいものである。クラウドサービスプロバイダの仕様および機能によっては、以下の項目は選定作業において考慮されるべきである。オペレーションの規模および性質によっては、物理的インフラの確保が重点的に考慮されるべきである。セキュリティコントロールは、戦略的に位置づけられており、一般的な規範およびベストプラクティスの基準を満たしている必要がある。

- セキュアエリアへの入り口-アクシスコントロールシステム（近接型カード、バイオメトリックアクセス）
- 緊急時に解放可能な火災制御パネルにリンクされたアクセスコントロールシステム(パニックオープン機能)
- モーションセンサーアラーム、温度変化追跡デバイス、ガラス破損検知器
- 防火設備　-　建物内消火栓、給水栓、ホース、煙探知機、スクリンクラー
- 消火器
- 火災非常口（ロックされていない、障害物がないこと）
- 火災非常口のパニックバー
- サイレンおよび警報灯
- CCTV カメラと DVR サーバ(バックアップスケジュールを含む)
- ドアの自動閉鎖器とドア解放警報装置
- データセンタ内のガスの火災抑制剤
- プリンタ近くのシュレッダ
- 消磁デバイスまたはデスクシュレッダ
- 緊急対応チームキット(ERT Kit)
- セキュリティ担当者用双方向トランシーバ
- セキュリティデスクまたは隠れた場所にある緊急事態警報器、隠ぺいされた監視カメラ
- ゲート型金属検出器または携帯金属検出器（必要であれば）
- 重要文書またはメディア保管用の防火保管場所

7.2　人に対する物理的セキュリティ

人に対する物理制御は、データに最も近い人員が運用を妨害またはクラウドを侵害するリスクを最低限にするものである。コンソールへのアクセス方法を知っている人物は、システムをリブートするだけ、または root や管理者権限で起動しているシステムにアクセスすることで、論理的な保護対策を回避することが可能である。ケーブルラックは、ネットワークへの隠れたアクセスや既存のネットワークを妨害する事に利用される。以下の対策を検討する必要がある：

この書は、Cloud Control Matrix Domains IS-15, FS-05, FS-06, FS-07, FS-08 および ISO/IEC 27002 Clause 9 にマップされる。

- 役割と責任(RACI スタイルの責任分担表)
- 身辺調査の確認とスクリーニング同意書
- 雇用契約書（例：秘密保持契約書など）
- 雇用修了書
- 企業方針の教育トレーニング（たとえば、ビジネス行動規範）

役割と責任はクラウド環境の一部です。クラウド環境では、人とプロセスが、技術と共に統合され、テナントのセキュリティを一貫して維持する。役割の分割は、一つの処理またはプロセスを完結するために、少なくとも 2 名を必要とする。クラウドの利用者を保護するためには、利害の不一致を避けることは非常に重要であり、リスクを回避するために、または監視するために対策を導入する。役割の分割は、元々会計および財務管理の考え方である。メリットとしては、物理セキュリティ、可用性、システム保護などのリスクも削減することが可能である。役割の分割は、リスクが高い役割を同一人物に割り当てることを止めることなどである。例えば、発注書の承認をする人物が支払も承認できる場合などである。この基本は、クラウド開発と運用で役割が分かれていることや、ソフトウェアのライフサイクルにも当てはまる。クラウドソフトウェア開発の共通点としては、アプリケーションの開発者と、システム運用者が分かれていることである。これによって、許可されていないバックドアが最終版に含まれていないことが確認できる。重要なインフラコンポーネントは異なる担当で運用されていることを確認して下さい。さらに、スタッフには業務遂行において最低限の権限を付与し、リスクを抹消せずともリスクを減らすことは可能である。役割の分割と最低限のアクセス権限付与の基本は、組織の情報資産を保護し利用するにあたり、CSP のゴールとなる。クラウドセキュリティ管理プログラムは、個人あるいはグループで行われる主要な役割と責任の割り当てを必要とする。これらの役割と責任は、組織内の情報セキュリティ方針のフレームワークの中で定義されており、上位管理者がレビューし承認し、受託者の GRC (Governance Risk and Compliance) の役割と責任と差異がないことを認識する必要がある。

さらに、有効な人的セキュリティを構築するためには、雇用契約、秘密保持契約、身辺調査（合法の範囲で）、合法的な雇用および解雇の実施を含む。また、組織全体に適用が可能な場合には、業務内容書、適切なトレーニング、セキュリティクリアランス(情報取扱資格管理)、業務変更、またセンシティブな情報を取扱うスタッフへの休暇強制などの仕組みを適用すべきである。

7.3 クラウドサービスプロバイダのセキュリティの評価

クラウドコンピューティングにおけるセキュリティリスクで、特異なものがある。それはデータ中心の工程管理であり、事業継続性、災害復旧、従来からのセキュリティ環境等によって CSP が評価されるべきで、業界基準を満たしている必要がある。

クラウドコンピューティングサービスプロバイダの設備における従来のセキュリティあるいは物理セキュリティは重要で、多くの方面から評価されるべきである。ここでは、クラウドまたは非クラウドのデータセンタでもセキュリティ要件はほぼ同じである。

クラウドサービスプロバイダの「人、プロセス、技術」モデルまたは考えは、CSP の成熟度を測る手立てになり、解決され、承認されるべきセキュリティの問題を明確にする。

組織的な成熟度や経験は、物理的セキュリティプログラムや緊急時への対応策を適切に導入するために重要である。物理的セキュリティプログラムを効果的に導入するには、人間に起因するところが非常に大きいのが事実である。マネジメント支援およびセキュリティのリーダーシップの手腕のレベルはマネジメント支援が重要である企業の資産を守るために非常に重要な要因になる。

物理的セキュリティは、組織内の物理資産に対して、許可されていないアクセスを不可能にする最初の防御ラインになり、記録、機密情報、産業スパイ、詐欺などの物理的な盗用に対する最初の防御ラインにもなる。

7.3.1 手順

クラウドサービスプロバイダは、クライアントの要求に応じて、検査があった場合に以下の文書を準備しておくこと:

- 外部による身辺調査（年に 1 度）
- 秘密保持契約
- 情報共有において「知る必要がある」また「持つ必要がある」方針を導入すること
- 職務の分離
- ユーザアクセス管理
- 業務内容の定義（役割と責任）
- ロールベースのアクセスコントロールシステム
- ユーザアクセスのレビュー

7.3.2 警備員

人間による監視および介在が必要な場合、物理的セキュリティの要員は警備員、スーパーバイザ、警備最高責任者から構成され、その体制図はクラウドサービスプロバイダ施設内に常に表示されているべきである。

とりわけ、サイトや掲載されている指示には、次のものが含まれている必要がある:

- ログインのログを使用して社員、契約社員、訪問者の資格情報を確認する事
- 訪問者用入館証の発行と回収
- 従業者の共連れの抑制
- 訪問者の対応と設備内の行動管理
- セキュリティに関係する電話対応
- 侵入監視、火災警報システム、要員の発報時に対応する分担分け
- 物資搬入搬出作業の監督と持ち出しルールの施行

- ビルの設備ルールおよび規則の施行
- 施設内の見廻り
- 監視カメラによる監視
- 鍵管理
- 緊急対応手順の実行
- セキュリティ問題の責任者への報告経路
- 郵便物の受領と配布
- オフィス内の訪問者への付き添いと案内

7.3.4 環境セキュリティ

クラウドサービスプロバイダの設備は、災害から、人員および資産を守るべきである。これらのコントロールは、温度、湿度、スモーク探知機、火災防止システムなどが含まれるが、これだけに限る物ではない。

7.3.4.1 環境制御

- データセンタは、社内基準、地域特定ルール、法令などに従い環境に対応する設備を整えること。自家発電などの仕組みを含む。
- 環境コントロールに対する設備および機器は、脅威や災害からのリスクと不正アクセスのリスクを共に軽減する事を目的として設置されるべきである。

7.3.4.2 機器の設置場所と保護

制限が掛けられたり機密情報と分類されたデータを含むシステムに対して、以下のコントロールが必要である:

- 設備は、不要にアクセスされないように物理的に安全な場所に設置されていること
- 湿度のようなコンピュータシステムのオペレーションに影響を与える可能性がある環境的条件は、監視されていること
- セキュリティスタッフは、境界の近くで発生する可能性がある災害（近所の火事、漏水、浸水、爆発など）の影響を考慮しておくこと
- ディスク装置等の破棄メディアの処理方法

7.3.4.3 機器のメンテナンス

可用性および完全性を確保するために、設備は適切にメンテナンスが行われていること。メンテナンスにおいては以下の項目が考慮されていること:

- サプライヤが推奨するサービス期間や使用に基づいて設備をメンテナンスすること
- 許可されているメンテナンス要員のみ修理の為の持出しや修理の実施ができること
- 障害と思われる、または実際の障害、防止または修理用のメンテナンスの記録をしておくこと

- 機器をメンテナンス目的で社外に運ぶ場合は、適切な処置を施すこと。例えば、適切な梱包方法、コンテナを密封する、安全な場所に保存する、搬送においては完全なトラッキングシステムがあること
- 資産コントロールにおける適切な方針と手順の維持は全ハードウェア、ファームウェア、ソフトウェアの記録と維持、追跡、責任部署、所有部署が明確であること

CSP 設備の完全なレビューをすることで、利用を検討しているクライアントはセキュリティプログラムの成熟度と経験レベルを理解することができる。通常、IT セキュリティに焦点をあてている場合は、物理セキュリティがおろそかになっている場合がある。しかしながら、脅威がさまざまな可能性を秘めている今日においては、物理セキュリティも十分に考慮する必要がでてくる。特に、環境的にクライアントのデータは他のクライアント（競合を含む）と同じ場所に存在するため、物理セキュリティは非常に重要になってくる。物理セキュリティは、侵入者や企業スパイを防止する最初の防御ラインになる。

7.4 事業継続性

従来より、情報セキュリティの 3 つの原則は、機密性、完全性、可用性である。事業継続性は、この中の継続性に関連する。CSP にとっては、契約上で約束されているのは提供時間である。しかし、利用者は SLA だけで満足しない。重大な機能停止が発生した際のことを考える。大手のサービス中断により、サードパーティが提供するサービスに影響したケースが近年発生しているため、サービスの提供継続は、業務を継続する上で非常に重要と考える。

サービスの継続を維持するために以下のガイドラインを参考にして下さい。これらの多くのガイドラインは、サードパーティが提供するサービス(例えば、クラウド)と共に内部サービスにも適用されると考えている。これらのガイドラインは、責任がサードパーティにかかっている名目で書かれている。

7.5 災害復旧

IT のクラウドストレージの重要な点は、バックアップと災害復旧(DR)時にどのように利用できるかである。インフラ、アプリケーション、ビジネスプロセスにおけるコスト削減は、クラウドのバックアップと DR サービスのゴールである。クラウドのバックアップと DR は信頼できるデータ保護を安価で、かつ容易に管理できる仕組みを提供する必要がある。クラウドストレージ、クラウドバックアップ、DR で難しいところは、モビリティ、クラウド間の情報送受信、可用性、最適な事業継続性、拡張性、および従量課金などが含まれることである。クラウドの DR ソリューションは 3 原則を元に構築されている。完全に仮想化されたストレージインフラ、拡張可能なファイルシステム、セルフサービス形式の DR アプリケーションにより、利用者の緊急要件に対応するものである。

DR からクラウドに移行している利用者は、以下の組織あるいはチームがサービスプロバイダの DR プログラムの中にあるかを確認する:

- 緊急対応チーム
- 危機管理チーム
- インシデントレスポンスチーム

危機連絡手順とあわせて、上記チームの存在を詳細にわたり確認して下さい。

7.5.1 復旧時の優先順位

プロバイダの復旧計画書をレビューしてください。この計画書は復旧順序の優先順位の詳細が記述されているもので、利用者が利用しているサービスとサービスの緊急度に関連して契約上義務がある SLA と直接関係するものである。復旧計画は、PRO[50]および RTO[51]が具体化され定量化されているものである。

復旧プロセスにおいて、詳細にわたる情報セキュリティコントロールが考慮され実装されているべきである。例えば、以下のような項目が含まれているべきである:

- 復旧作業に関わるスタッフへの許可
- 物理セキュリティ対策がバックアップサイトに導入されていること
- 普及作業における依存項目をリストしておくこと(サプライやおよびアウトソースパートナなど)
- 主要サイトが利用できなくなった場合のバックアップサイトのロケーションは適度に離れていること

7.6 許可

- 適切な設備設計がされていること
- 統合された物理および論理セキュリティシステムを採用し、相互に補完し合っている事
- サプライチェーンの末端における雇用セキュリティ義務および責任に基づく SLA を確立すること

7.7 推奨事項

7.7.1 ポリシーに関する推奨事項

- クラウドサービスプロバイダは、最も厳しい利用者のシステム、設備、手順書などに対する要件をセキュリティベースラインと考える事。これらのセキュリティを実施することは、利用者にとってネガティブに作用することはない。厳しいセキュリティの実施でも、人員、売り上げ、風評、株主へのリスクを軽減する意味で、コスト効率がよく、また定量化されるべきである。
- プロバイダは、セキュリティ要件が低いユーザにターゲットを絞る、またはベースラインセキュリティを全利用者に提供し、高いレベルが必要な利用者には付加サービスとして販売・実装することも可能である。高いレベルのセキュリティを求める利用者の中には、全体的に高いセキュリティを希望する利用者がいる場合がある。システム、設備、手順の文書化などに渡り、バランスをとることが必要である。
- プロバイダは、従業員に対して、業務担当を健全に仕分け、身辺調査を行い、秘密保持契約への署名を必須として下さい。利用者に関する知識を持つ従業員を限定し、必要に応じて権限を付与して下さい。

7.7.2 透明性に関する推奨事項

- クラウドサービスプロバイダのセキュリティに対する姿勢は対外的に明確である必要がある。クラウドサービスプロバイダの設備またはデータセンタのオンサイト訪問は、スポット的なアセスメントをするには有効で、どのようなセキュリティ対策が導入されているかが明確にわかる。しかしながら、必要に応じて

[50] **RPO** - Recovery Point Objective.　復旧時点目標
[51] **RTO** - Recovery Time Objective.　復旧時間目標

提供される環境や、マルチテナントで共有される環境であるため、従来からの監査やアセスメントの形式でない場合がある。(例えば、サードパーティの検査報告書に対するアクセスの他のクライアントと共有するなど)

- オンサイトアセスメントの効果を最大にするために、クラウドサービスプロバイダの設備またはデータセンタへの訪問は、抜き打ちでされるべきである(必要な場合には、特定の時間ではなく、ある程度の時間の幅があること)。これによってクラウドサービスプロバイダがクライアントまたはサードパーティが訪問中に「見かけ上保つ」状態ではなく、通常の営業日の本当のアセスメントが可能である。
  - 直接調査が可能な場合は、アセスメントチームには2名以上のIT、情報セキュリティ、事業継続性、物理セキュリティおよび経営的に詳しい担当者を含めてください。(例えば、部長、データ責任者など)
  - 訪問前に、利用者は関連する認証書、監査報告書、テスト方法を含む、事業継続性計画および災害復旧の文書を要求し、取得して下さい。

7.7.3 人的推奨事項

- 利用者は、クラウドサービスプロバイダが物理セキュリティに対して優秀なセキュリティ担当者を任命しているか確認すること。専任管理職が存在し、物理セキュリティプログラムに対するリーダーシップをとっていることが必要である。業界認証である、CISA[52]、CISSP[53]、CISM[54]、ITIL、CPP[55](ASIS[56])の取得者であることで、物理セキュリティに対する必要な知識とスキルを有している判断基準にすることも可能である。
- セキュリティマネージャの報告の仕組みを徹底的にレビューして下さい。このレビューで役職の重要性と責任が付与されているか確認できる。セキュリティマネージャは、業務上の上司とGRCコミッティ(存在する場合)に報告すべきである。総務や情報システム部門に報告すべきではない。セキュリティマネージャは、この役割の目的を考え独立性を保つためには、特別経路でCEOに報告するのが望ましいと考える。(例えば、CROまたは法務の上級弁護士)

7.7.4 事業継続性に関する推奨事項

- 利用者は、提供されるサービスが継続されるために、サードパーティとの契約内容をレビューすること。利用者は詳細にわたり分析をすること。通常、利用者は、個人情報が保存されている場合、個人情報データが適切に管理されているか具体的な法令要件があるため、データ所有者という認識を持っている。法令要件は、通常、サードパーティがデータ処理する場合にも適用される。
- 利用者は、サードパーティの事業計画プロセスおよび証書などをレビューして下さい。例えば、クラウドサービスプロバイダはBS25999(BCM)に準拠している可能性がある。利用者は証書のスコープを確認し、アセスメントの詳細を文書化することを期待する。
- 利用者は、クラウドサービスプロバイダの設備のオンサイト評価を行い、説明されている管理が実際にサービス提供維持に使用されているか確認すること。災害や事件が発生したときにのみに必要となる特

[52] **CISA** - Certified Information Security Auditor
[53] **CISSP** - Certified Information System Security Professional
[54] **CISM** - Certified Information Security Manager
[55] **CPP** - Certified Privacy Professional
[56] **ASIS** - American Society for Industrial Security

定の BCP 対策を確認するためにだけ、クラウドサービスプロバイダの設備に対して抜き打ち評価を行う必要はない。

- 利用者は、クラウドサービスプロバイダが行った BCP/DR テストの結果を受け取っていること。前述した多くの推奨項目は、サービスが継続して提供されることを文書化するということに重点を置いているが、一番重要なのは、重大なイベントが発生した時である。実際の災害や事件が発生する前に、利用者は公式な BCP/DR テストの結果を受け取ることが重要であることを強調し、契約上の SLA を満たすものであることを確認して下さい。

7.7.5 災害復旧に関する推奨事項

- クラウドの利用者は、単一のサービスプロバイダに依存することなく、サービスプロバイダー社がサービス停止した場合のフェールオーバの仕組みまたはリスクを軽減するような災害復旧計画を準備しておくこと。
- IaaS プロバイダは、マルチプラットフォームプロバイダと契約し、損失が発生した場合には迅速にシステムを復旧できるツールを所有すること。
- 利用者が自身のデータの完全性をいつでも確認できるよう、データ検証は自動的であるか、またはユーザから開始される検証手順であること。
- 差分バックアップは、保護されているシステム全ての複製の更新を頻繁に行うか、システム毎にユーザが設定した間隔でスナップショットを取るようにすること。そうすることで、顧客は復旧時点目標に従って設定することができる。
- サイト全体、システム、ディスク、ファイルリカバリは、ユーザ主導のセルフサービスポータルを通してアクセス可能にすべきである。これにより、ユーザはリカバリしたいファイルディスクやシステムの選択を柔軟に行うことができる。
- クラウドプロバイダは、迅速な SLA ベースのデータリカバリの仕組みを導入すること。
- SLA はきちんと交渉され、利用者は利害関係の衝突の起こらないことを保証するために SLA に代価を支払うべきである。データ、ファイル、システムディスクのリカバリは 30 分以内であること。
- 利用者と物理サイトの間の WAN は最適化され、クラウド環境において、帯域、ストレージ利用、コストが限定されている場合でもデータの遠隔操作が可能であること。

7.8 要求事項

- ✓ 全関連部署は、物理セキュリティの構造設計が適切であることを確認すること。
- ✓ サプライチェーンの関係者全員が、妨害物、探知、認証ソリューションが相互依存していることを認識すること。
- ✓ エンドユーザは、クラウドのサプライチェーンを取り巻く他者が持つ人的リスクを検証し、報告し、修正する必要がある。適切に責任分担がされており最低限のアクセス権限の割り当てをすることで、人的リスクに対して積極的な対策を設計し導入すること。

第 8 章 //
データセンタ運用

クラウドコンピューティングが進化するには、プロバイダは、仮想化技術を使用してサーバ資産を管理するだけでなく、エンタープライズデータセンターを進化させる必要がある。ビジネスの迅速性、グリーンテクノロジ、プロバイダの情報公開、さらに発電、データセンタ構築、運用の増え続ける斬新なアイデアなどに対応するためには、データセンタの変化が長期的なクラウドの成功につながる。

「次世代データセンタ」という言葉が使用されるようになってから数年になる。データセンタ運用にビジネスインテリジェンスへの適応を取り入れて成長をとげてきた。データセンタ内で稼動するアプリケーションを理解し、大規模ホスティングの分析クラスタへの要件も同様に進化してきた。データセンタは、単一で成り立つものではなく、アプリケーションと同様の変化に対応したり、他のデータセンタへの接続することが必要であり、それにより、セキュリティのみならず待機時間への対応が可能になる。

概要:このセクションでは以下のトピックを説明する。

- CCM に関連する物理セキュリティの注意点
- 自動化されたデータセンタのユースケースマッピング
- 新データセンタ? 家庭におけるクラウドコンピューティング
- クラウド基盤の分散とデータセンタ

CCM の考察と新しいクラウドデータセンターのアイデアがお互いに影響を及ぼすか

8.1 データセンター運用

このセクションの新しいコンセプト：

- **クラウドアプリケーションのミッション** データセンター内に収納されている業界およびアプリケーションにおけるミッション。例としては、医療または E コマースのアプリケーションのミッション
- **データセンタの分散** 物理的に離れた場所に存在するが、連携して動作するクラウド基盤

サービスベースの自動化や、サービスの自動化を可能にする予測的分析は、データセンタを発展させるための **ITIL**(Information Technology Infrastructure Library)[57]スタンダードを使用した **ITSM**(Information Technology Service Management)[58]によって長く提供されてきた。データセンタに収納されている様々なタイプのアプリケーションが、自動化を必要としている。データセンタの運用者は、データセンタ内で何がどのように稼動しているかを全体的に理解することで、様々な利用方法に対応をする上で大きな恩恵をうける。

[57] **ITIL** - Information Technology Infrastructure Library
[58] **ITSM** - Information Technology Service Management

Cloud Security Alliance の Cloud Controls Matrix は、複数のスタンダードおよび法令要件を基に、多数の物理要件が記載されている。このガイダンスおよび Cloud Controls Matrix の本バージョンの物理セキュリティの章では、データセンタの専門家がデータセンタの内部および外部要件を理解できるように書かれている。参考までに、以下の表では、データセンタ内に収納されているアプリケーションのミッションを基にデータセンタのコントロールを説明している。以下の表では、全てを網羅しているわけではないが、アプリケーションのタイプまたはミッションに対して、Cloud Control Matrix のコントロールおよび仕様を相互参照し、例を提供している。

表 1— Application Mission by Control

APPLICATION MISSION	CONTROL	SPECIFICATION
Health Care (HIPAA[59])	設備セキュリティ-セキュリティポリシー	オフィス、部屋、設備、および安全エリア内で、安心・安全な作業環境を維持するためにポリシーおよびプロシージャを制定する。
Card Processing/Payment (PCI[60])	設備セキュリティ-ユーザアクセス	ユーザおよびサポート要員から情報資産および機能への物理アクセスを制限する。
Power Generation (NERC CIP[61])	設備セキュリティ-コントロールされたアクセスポイント	機微データおよび情報システムを保護するために、物理的セキュリティ境界（フェンス、壁、バリア、ガードマン、出入り口、電子監視、物理認証メカニズム、受付、巡回員）を導入する。

上記のリストは、この章内で徹底的に説明するものではない。読者は、各組織が準拠すべき標準を基にマトリックスを参照していただきたい。

データセンタ内で稼動するアプリケーションは、規定されている情報（情報セキュリティまたはアプリケーションセキュリティスタンダードの規定対象）を含んでおり、監査の対象になる。データセンタ運用者により実施された物理監査の結果は、データセンタの利用者に対して公表されるか、または Cloud Audit が提供するアプリケーションに関する質問（基盤）に包括されるものである。

今までのバージョンのガイダンスでは、読者は自身で監査を実行するように指示されている。多くのデータセンタのオペレータまたはクラウドプロバイダにとって、これは現実的ではない。複数のテナントを抱える環境において、通常、運用者やプロバイダはそれぞれの顧客が監査のために来訪するといったことは受け入れることはできない。利用者は、オペレータまたはプロバイダに独自監査の結果を要求すべきである。

この考えは、サービスオートメーションの考え方である。レポート生成、ロギング、および監査結果発行を自動化することで、データセンタのオペレータは利用者に対して、アプリケーションのミッションに基づいて、データセンタが何をどのレベルで対策しているかの証跡を提供することができる。Cloud Audit、Cloud Trust Protocol、および、CYBEX (X.1500)は、共通にアクセス可能なインタフェース経由で監査結果の発行を自動化することが可能である。

[59] **HIPAA** - Healthcare Information Portability and Protection Act
[60] **PCI** - Payment Card Industry. Specifically PCI DSS, which is Data Security Standard
[61] **NERC CIP** - North American Electric Reliability Corporation Critical Infrastructure Protection

データセンタの自動化をさらに進めるには、データセンタ内に収納されている資産を含むライブラリ（一覧表）が必要となる。データセンタ内でライブラリ内の資産がどのようにリソースを使用しているかを理解することで、運用側はどのテナントがリソースを使用しているかを予測することが可能である。もし、データセンタが、PoD[62]および VMDC[63]などのコンセプトを使用している場合は、データセンタはクラウドおよび仮想化ビジネスを推進できるくらい、柔軟で迅速な対応が可能な状態といえるであろう。

8.1.1 新規あるいは最先端モデル

最近(2011 年夏)では、家庭ベースのクラウドプラットフォームに関するニュースが多く流れた。これらのタイプのインフラは、**SETI@home**[64]の後でひな形が作成されている。一般家庭またはオフィスのコンピュータが提供するボランティアの資産をベースに、その他さまざまなアプリケーションをサポートするクラウドが提供される。この場合、データセンタは各ボランティアの家庭である。このタイプのクラウドは、コミュニティベースのアプリケーションをホスティングする環境は問題ないが、特定の基準に対して監査が行われるように規定されている環境では適合しない。例としては、100,000 の家庭のコンピュータ上でクラウドが提供されている場合には、100,000 個に分割され広く地理的に分散しているデータセンタを監査することは現実的ではない。このタイプのインフラは、趣味（例: 読書クラブ）用のアプリケーションや地域住民用の Web サイトなどコミュニティベースのアプリケーションのホスティングが可能である。

クラウドは、徐々に一般的な基盤または便利なツールとして見なされるようになってきている。業界ではアイデンティティ, 相互運用性, および事業継続性などのために、Security as a Service もしくはブローカのインフラを提供する取組みがある。アプリケーションは、引き離され、特定の組織または組織が利用するアプリケーションの特別にニーズに注力した特別の物理環境に配置される。

データセンタの分散は、アプリケーションを他の特別なニーズを収納および管理できるデータセンタに配置する。アプリケーションを物理的な境界を越えて分散させることで、クラウド内のアプリケーションの負荷を減少させることができるが、コントロールおよび管理がより困難になる。

8.2 許可

- データセンタ連携の普及。データセンタ自動化には、複数の物理的に関係のないデータセンタを再編成するソフトウェアが、監査に必要なログ取得やレポートの生成に必要である。
- データセンタが個人的な家庭を基盤としたクラウド。家庭を基盤としたクラウドでは、基準またはコンプライアンスのための監査はほぼ不可能である。環境要件が定められていたり、標準的な環境を求めるコントロール要求では、家庭を基盤としたクラウドでは非常に困難である。アプリケーションの特定の部分をホームベースのインフラに分散してもよいアプリケーションでは、可能性があると思われる。

8.3 推奨事項

- クラウドのデータセンタを構築している組織は、データセンタ内で稼動している技術を理解および対応するために、管理プロセス、業務、およびソフトウェアを取り入れるべきである。

---

[62] **PoD** - Point of Delivery. A rack-able aggregated set of power, compute, storage access, and network components contained in a single unit

[63] **VMDC** - Virtual Multi-tenant Data Center. A concept using modular, easily rack-able components to quickly expand a data center such as PoD's

[64] **SETI@home** - http://setiathome.berkeley.edu/

- クラウドサービスを購入する組織は、プロバイダが、データセンタ運用に際して、サービス管理プロセスおよび業務を適用済みであり、データセンタ内で迅速かつ高度なリソースを確保できるラッキング技術を適用していることを確認する。
- データセンタ内で何が稼動しているか、ミッションを理解して下さい。Cloud Control Matrix 内のコントロールを基に構築または購入されたデータセンターは、物理および資産セキュリティ要件に適合する必要がある。
- データセンタの場所が重要である。もしテクノロジやアプリケーションコンポーネントがデータセンタをまたがって広がっている場合は、データセンタ間において待ち時間が発生する可能性がある。
- クラウドサービスを購入する組織は、コンプライアンス要件を満たす担当部署を明確にし、コンプライアンス評価時の担当部署およびクラウドプロバイダの役割を明確にして文書化する。

8.4 要求事項

Cloud Security Alliance には、クラウドのデータセンター構築および改築を支援するために、多くの情報を持っている。コントロールマトリックスは、非常に広範囲のセキュリティ要件および法令要件を強調している。CSA の Cloud Audit およびその他のプロジェクトでも、データセンターの構築および管理、ならびにデータセンター内で使われる技術に対する支援を行っている。

- ✓ データセンタ内で稼動しているものを基に Control Matrix 要件を完全に理解する。多くのアプリケーションのミッションを満足させる共通要素を使用する。
- ✓ 可用性、セキュリティおよび資産引き渡しおよび管理を確実にするために、IT サービス管理技術を使用する。
- ✓ プロバイダがデータセンタを所有している場合には、法令およびセキュリティ基準テンプレートに対して監査を行い、利用者に対して監査結果を公開する。

第 9 章 //
インシデントレスポンス

インシデントレスポンス（IR）は、セキュリティマネジメントにおける重要な分野のひとつである。どれだけ注意深く計画したとしても、防御的なセキュリティ対策では情報資産への攻撃を完全に排除することはできない。それゆえ、クラウド上に移行しようとする組織にとっての主要な疑問のひとつは、クラウド上のリソースが絡んだセキュリティインシデントを効率的かつ有効に取り扱うために何をすべきか、にある。

クラウドコンピューティングにおいてインシデントレスポンスについて新しい概念的なフレームワークを必要とするわけではなく、むしろ現存するインシデントレスポンスプログラムやそのプロセス、ツールなどを、確実にクラウドを取り巻く運用環境に適用させることが求められる。これは、このガイダンス文書全体に一貫していることだが、組織のインシデントレスポンスと関連するコントロールについてのギャップ分析が（他の章などと）同じ形で行われるべきである。

この章では、クラウドコンピューティング独特の特性がもたらす、インシデントレスポンス(IR)の根幹にかかわるようなギャップの特定を追求する。セキュリティ専門家は、この章の内容をインシデントレスポンス計画の策定や、関連するインシデントレスポンスライフサイクルにおける準備段階の活動へ活用できるだろう。クラウドコンピューティングがインシデントレスポンスにもたらす困難を理解するために、我々は、クラウドコンピューティング独特の特性や様々な配備モデル、サービスモデルのいずれがインシデントレスポンスに困難をもたらすかを検討しなくてはならない。

この章の構成は、一般に広く受け入れられている National Institute of Standards and Technologies（NIST）のコンピュータセキュリティインシデントハンドリングガイド（NIST SP800-61）[1]に記載されたインシデントレスポンスライフサイクルに沿って行われている。まず、インシデントレスポンスに最も影響を及ぼすクラウドコンピューティングの特性について述べた後、引き続く節では、ライフサイクルの各段階で対応者が直面するであろう問題について考察する。

概要. この章では、以下のトピックについて触れる:

- クラウドコンピューティングがインシデントレスポンスに与える影響
- インシデントレスポンスライフサイクル
- フォレンジックに関する責務

9.1 インシデントレスポンスを困難にするクラウドコンピューティングの特性

クラウドコンピューティングは様々なレベルで変化をもたらすが、中でもいくつかの特性[2]が他の特性[3]よりも直接的にインシデントレスポンスを困難にしている。

第一の問題は、「オンデマンドセルフサービス」というクラウドコンピューティングの性格上、クラウドサービスの利用者が、セキュリティインシデントへの対応にあたって、クラウドサービスプロバイダ (CSP)[65]から必要な協力を得ることが難しい、もしくは場合によってまったく不可能なことである。プロバイダがインシデントレスポンスにどの程度関与できるかは、サービスや使われている配備モデルによって様々である。インシデントの検知、分析、拡大の防止、復旧などがどの程度、サービスに対して技術的に検討されているのかということは、利用者がプロバイダに対してすべき、とりわけ重要な質問点の一つである。

第二の問題は、クラウドサービスによる、コンピュータリソースの集積・共有（resource pooling）と、さらにクラウド基盤が提供する、迅速な割り当てリソース量の変更（rapid elasticity）が、インシデントレスポンス、とりわけ、その中でもインシデント分析の一環として行われるフォレンジック作業を極度に複雑化する可能性である。フォレンジック作業は、きわめて動的に変化する環境上で行わなければならず、このことが、フォレンジックにおける基本的な要求事項[4]であるところの、インシデント範囲の特定や、データや属性の収集、データが持つ意味の完全性の保全、証拠全般の安定性の維持といったことを困難にするのである。これらの問題は利用者自身がフォレンジック作業を行おうとすれば、さらに悪化する。それは、彼らが不透明な環境（つまり、先に述べたように、こうした作業にプロバイダの協力が不可欠であるような環境）で作業しなければならないからだ。

第三の問題は、クラウドサービスによって行われるリソースの集積と共有によって、同じリソースを共有する利用者間でプライバシーに関する懸念、つまりテレメトリーや断片的なデータ（たとえば、ログ、ネットフローデータ[66]、メモリ、マシンイメージやストレージデータ）の収集や分析が、他の利用者のプライバシーを侵害せずにできるのかという懸念を生むことである。これは、主にプロバイダが解決すべき技術的課題である。またプロバイダが適切にこうしたデータの収集や分離を行っているかどうか、またインシデントレスポンスにおいて、必要とする支援ができるかどうかを確認することは、利用者側の責任である。

第四の問題は、クラウドの基本的な特性としては述べられていないが、クラウドコンピューティングでは、利用者が明示的に知らされないままに、データが地理的な、もしくは法制度的な境界を越えて移動してしまう可能性があることである。これにより引き起こされる法律や規則面での問題は、インシデントレスポンスライフサイクル[5]のすべての段階において、取りうる方法・手段に制限を課し、または、必ず行うべき事項や決して行ってはならない事項を想定するという意味での悪影響をもたらす。インシデントレスポンスチームには、法務部門から専門家を加えて、こうした面での指示を受けるのが賢明である。

一方で、クラウドコンピューティングは、インシデントレスポンスを行う者にとって恩恵ももたらしてくれる。クラウドを使った継続的なモニタリングシステムがあれば、インシデントレスポンスのための作業時間の短縮や、より高度な対応の実現につながる。仮想化技術やクラウドコンピューティング基盤によってもたらされる弾力性、拡張性は、既存のデータセンタ基盤で行われるよりもサービスへの影響が少ない形で、被害拡大の防止、復旧といった作業を可能にするだろう。同様にインシデントの調査も、いくつかの点で容易になる可能性がある。それは、仮想化されたイメージは、容易に実行状態での解析ができる検証環境に移動が可能であり、フォレンジックのためのイメージ取得や検査がしやすくなるからである。

9.2 クラウドアーキテクチャセキュリティの参照モデル

クラウドの配備モデルやサービスモデルはインシデントレスポンスのクラウドエコシステム内での作業分担に大きな影響を与える。第１章で説明したアーキテクチャのフレームワークとセキュリティコントロールのレビューを用いることは、どのような技術やプロセスの要素をどの組織がどの（クラウドサービスの）階層で受け持つべきかを明らかにする上で役立つ。

[65] **CSP** - クラウドサービスプロバイダ
[66] NetFlow　ネットワーク機器で、そのトラフィックデータをモニタリングする際の形式のひとつ

コンピューティング環境を提供するための情報システムやその基盤に対して利用者が可視性を持ちうる範囲やコントロール可能な範囲は、クラウドのサービスモデル（IaaS, PaaS, SaaS）の種類によって大きく異なる。このことは、インシデントレスポンスのすべての段階においても、このガイダンスの他の章で行われているのと同様のアプローチが必要であることを示唆している。

たとえば、SaaS ソリューションにおいては、インシデントレスポンスの作業のほとんどは、クラウドサービスプロバイダに頼らざるを得ないと考えられる。一方で、IaaS においては、セキュリティインシデントの検知と対応に関する多くの能力と責任は利用者の側に存在していると思われる。

しかし、IaaS であっても、その程度はクラウドサービスプロバイダのサービスに大きく依存している。物理的なサーバやネットワーク機器、共有デバイス、ファイアウォールなどのセキュリティ機器やその他の管理システムからのデータは、クラウドサービスプロバイダから提供されなければならない。一部のプロバイダは、すでにこうしたデータの利用者による遠隔監視機能を提供しており、また一部のセキュリティ監視サービスプロバイダ（MSSP[67]）はこれらのデータを受信するためのクラウドベースのソリューションを発表している。

第 1 章で書かれたセキュリティコントロールモデルの複雑さを考えれば、個別のクラウド配備モデルにマッピングする活動の作業はインシデントレスポンス計画に反映されるべきであり、逆もまたしかりである。従来、インシデントレスポンスのためのコントロールは、（他のコントロールに比べて）より狭い意味で、ハイレベルな組織的要求と関連づけられてきた。しかし、セキュリティ専門家は、これを真に有効なものとするために、より広い視点で考えていかねばならない。インシデントレスポンスに責任を負う者は、直接、あるいは間接にインシデントレスポンスと関係する技術的なセキュリティコントロールの選定、調達、導入のすべてに関わっていく必要がある。このプロセスは、少なくともインシデントレスポンスライフサイクルの各段階で、役割や責任を割り振る際に役立つだろう。

クラウドの配備モデル（パブリック、プライベート、ハイブリッド、コミュニティ）もまた、クラウドのインシデントレスポンス能力をレビューする際に考慮すべき点である。インシデントレスポンスに必要なデータへのアクセスの容易さは、モデルによって異なるからだ。ここでもまた、コントロールと責任の所在の間に同じようなモデルに応じた変化が存在することは明らかだ。この章での主な懸念は、よりパブリッククラウド側にあるこの同期した連続関係に存在する。このガイダンスの筆者たちは、よりプライベートな配備モデルであるほど、より多くのセキュリティコントロールが利用者側で作り込まれるか、もしくは、プロバイダから利用者の満足がいく形で提供される必要があると考えている。

9.3 インシデントレスポンスライフサイクルの検証

NIST SP800-61[1]では、準備、検知と分析、拡大防止、原因除去と復旧という、インシデントレスポンスの主要な段階について書かれている。この節では、これらの段階におけるクラウド固有の課題について検証し、いかにしてそれらを克服しうるかの推奨を行う。

9.3.1 準備の段階の考察

準備の段階は、情報資産をクラウドに配備する際におけるインシデントレスポンスライフサイクルの中で最も重要といえる。クラウド固有の課題及び利点を特定する作業は、クラウドの利用者である組織内のセキュリティ専門家による正式なプロジェクトとして、クラウドへの移行に先だって行われるべきである。もし、自組織

[67] MSSP：Managed Security Service Provider：セキュリティ監視などのセキュリティ管理サービスを提供するプロバイダ。

内のインシデントレスポンスに関する練度が不十分だと思われる場合は、外部の経験豊かな専門家（企業）に相談すべきである。これらの活動は、組織のインシデントレスポンス計画の更新ごとに実施されるべきである。

以下に引き続くインシデントレスポンスライフサイクルの各段階に関する議論で提起される疑問やそれに対する推奨は、クラウド利用者側のインシデントレスポンス計画プロセスにとっての参考として役立つものである。ここで議論される概念を、正式に文書化された計画に盛り込むことは、様々なクラウドへのギャップを埋めるための正しい活動の推進や、クラウドの利点を享受する上で役立つことになる。

準備段階は、まず利用者のデータが処理中や保存時に、どこにあるかについての完全な理解と説明から始まる。利用者の情報資産が、組織の境界やおそらくは地理的な境界を超えて移動する可能性があるため、脅威のモデリングを物理、論理の両面で行う必要が生じる。物理的な資産[68]、組織やネットワーク、そして法制度的な境界を意識してデータの流れをマッピングした「データフローダイアグラム」は、インシデントレスポンスの際に発生しうる様々な依存関係を明らかにするために役立つ。

（クラウドのサービスモデルを考えれば）複数の組織がインシデントレスポンスに関与することになるため、SLA や組織間の契約といったものが、インシデントレスポンスライフサイクルの各段階で期待される責任を果たすことやそのための情報交換にとって大きな意味を持つことになる。インシデントレスポンス計画を（関与する）他の組織と共有し、共通の用語や不明な用語は、正確に定義し不明点をなくしておくことが賢明である。そして、可能な限り、インシデントレスポンスが発生する前に、あらゆる「あいまいさ」を排除しておくべきである。

クラウドサービスプロバイダに、利用者ごとに個別のインシデントレスポンス計画を作ることを期待するのは無理である。しかし、以下に述べるような点のすべて、またはいくつかを契約書や SLA に記載することで、プロバイダがより発展的なインシデントレスポンス計画を立てているという安心感を利用者側組織に対して与えることにつながる:

- インシデントレスポンスチームへの連絡先、連絡手段、対応時間
- プロバイダと利用者、同様に他の関連する外部者間の双方向でのインシデントに関する定義と通報の基準
- クラウドサービスプロバイダが利用者に提供するインシデント検知の手段。（たとえば、利用可能なイベントデータ（ログ）、通知される不審なイベントの種類など）
- インシデントレスポンスにおける役割や責任の定義、クラウドサービスプロバイダから提供されるインシデントレスポンス作業の明示。（たとえば、インシデントデータやその断片の収集を通じたフォレンジックのサポート、インシデント分析への関与もしくはサポートなど）
- 契約にプロバイダと利用者双方で行われる定期的なインシデントレスポンステストの仕様や結果が共有されるかなどを盛り込むこと
- 事後対応の範囲（たとえば、根本原因解析、インシデントレスポンス報告、経験から学んだ内容のセキュリティ管理への反映など）
- SLA の一部として、インシデントレスポンスに関係するプロバイダと利用者の責任範囲を明示すること

一旦こうして役割と責任が明確になれば、利用者は、直接責任を持つべき部分について、彼らのインシデントレスポンスチームについて適切なリソース確保、訓練、装備などを行うことができる。たとえば、もし利用者が管理するアプリケーションが PaaS サービスモデル上で動作していて、クラウドプロバイダがその基盤固有の

[68] 訳注：たとえば、サーバやデータセンタなど、物理的な意味合いでの資産を意味する

ログを利用者に提供（もしくは利用者自身が取得することを許可）する場合、利用者側でその種のログを受け取って処理し、解析するためのツールや人員を用意する必要が生じることは明らかだ。IaaS と PaaS においては、仮想化の能力とフォレンジックスやその他の調査を仮想マシン上で行う手段は、あらゆるインシデントレスポンスの活動にとって必須のものとなるだろう。必要となる専門性を、利用者の組織自身が持つのか、それともサードパーティにアウトソースするのかという判断は、準備段階の間に行われるべきものだ。なお、アウトソースする場合は、さらにアウトソース先との間でも一連の契約や NDA[69]の管理が必要になることに注意してほしい。

関係するすべての組織の間で、連絡手段が確保されなければならない。また関係組織は、機微な情報をやりとりするために、通常の手段とは別枠の、暗号技術によって情報の完全性と真正性が保証される通信手段も検討すべきである。インシデントレスポンス中の通信手段については、被害の尺度を関係先間で共有したり、必要な時に第三者に調査を任せたりするための標準手法を利用できる。たとえば、**IODEF**[70i]や **RID**[71iiiii]などは、**IETF**[72]によって **ITU**[73]の **CYBEX**[74]プロジェクトの協力のもとで開発された。IODEF は、インシデントを記述するために使用される XML のスキーマを、RID は、インシデント情報を組織間（少なくとも、単一のクラウドプロバイダとその利用者間）で交換するための標準的な手順を記述したものである。

準備段階での最も重要な部分は、テスト計画である。テストは実際のインシデントに関係する可能性がある関係者を総動員して徹底的に行うことが望ましい。しかしながら、クラウドプロバイダが、すべての利用者のテストに対応できるリソースを持っているとは考えにくいので、それが困難な場合、利用者側でプロバイダに対して発生する可能性があるタスクや情報要求などを特定するためのロールプレイング[75]を行うことも検討すべきである。この情報は、その後、準備段階の間に行われるプロバイダとの議論を深めるために使われるべきである。他には、利用者がクラウドプロバイダ側で計画されるテストに協力する方法も考えられる。

9.3.2 検知と分析

インシデントを適時に検知することと、その後の（何が発生したか、どのように発生したか、どのリソースがその影響下にあるかなどの）分析がうまくいくかは、関連するデータが得られるかや、データを正確に解釈できる分析能力を持っているかに依存する。先にも述べた通り、クラウドコンピューティングは、その両方に課題を与える。まず、データの入手については、大半のデータはプロバイダが利用者に対して提供するかに依存しており、おそらくそれは、クラウドコンピューティングのきわめて動的な特性による制約を受けることになる。また、少なくとも、利用者自身が通常、限られた知識しか持たない、利用者に対して不透明なプロバイダ所有の環境が、データの分析を複雑なものにする。さらに何度も言うようだが、クラウドコンピューティングのきわめて動的な特性によって、データの解釈が困難になるか、場合によって不可能になる。

インシデントレスポンスの技術的な課題をとりあえず一旦棚上げにしたとしても、クラウドに対する電子的調査が、証拠の価値、（たとえば信頼性）を最大化するために、どのような形で行われるべきかという疑問の多くに対して、本稿の執筆時点では答えが出ていない。従って、今後、クラウドにからんだ判例などがより一般的になり、広く受け入れられるような、（インシデントレスポンスの）ベストプラクティスが出来るまでの間は、クラウドのセキュリティインシデント分析結果が、法廷において（証拠として）認められないというリスクを考慮しておく必要がある。

---

[69] NDA : Non Disclosure Agreement 秘密保持契約書
[70] IODEF ： Incident Object Description Exchange Format
[71] RID ： Real-time Inter-network Defence
[72] IETF ： Internet Engineering Task Force
[73] ITU : International Telecommunication Union
[74] CYBEX : Cybersecurity Exchange
[75] 訳注：つまり、利用者自身の誰かがプロバイダの役割を演じてテストを行うこと

標準的な方法や手順が定められ、クラウドコンピューティングによって技術が進歩して、インシデントの検知や解析のためのツールができるまでの間、クラウドの利用者は、(1)インシデントの検知、分析に必要なデータへのアクセス、(2)利用しているクラウド環境でのインシデント分析に対する（プロバイダによる）適切なフォレンジック面での支援への確証を得ることで、クラウド環境から発生するこれらの課題に立ち向かわなければならない。

9.3.3 調査に利用する情報源

なんらかの外部のサービスを統合するにあたって、インシデントレスポンスチームは、彼らの情報資産に対して影響しうる、異常な事象や不審な活動を適切に検知するためにふさわしいログ取得の方法を決める必要がある。利用者側にとって、どのようなログ（やその他のデータ）が取得可能で、それがどのように取得され、処理されるか、そして最終的にクラウドサービスプロバイダが、それをいつ、どのように提供するかという点に関するアセスメントを行うことは避けられない。

利用者側にとって、インシデントの検知とそれに引き続く分析のための主な情報源はログとして取得された情報である。ログ情報については、以下のような問題についての検討を行わなければならない:

- **どのような情報をログとして取得するか?** 適切なログ種別の例として、「監査ログ」（たとえば、ネットワーク、コンピュータシステム、アプリケーション、クラウドなどの管理者の役割とアクセス、バックアップと復元の操作、変更管理に関する活動など）、「エラーログ」（たとえばハイパーバイザーのカーネルメッセージ、オペレーティングシステム、アプリケーションなどのエラーについてのもの）「セキュリティログ」（たとえば IDS[76]やファイアウォールのログなど）、「パフォーマンスに関するログ」などがある。既存のログが（目的にてらして）不十分な場合は、追加のログ情報源を別途追加するか、もしくはプロバイダと交渉しなければならない。
- **ログ情報が完全かつ一貫しているか?** 不完全なログの例としてまず挙げられるのは、ログの取得元における時刻同期が不完全なものである。同様のものとして、記録された時刻についてのタイムゾーン情報が不明なものがある。これらは、ログを解析する際に、取得されたデータの正確な解釈を困難にする。
- **ログ情報に、クラウド特有の動的な特性が適切に反映されているか?** クラウド環境特有の動的な挙動は、しばしばログの不完全さや一貫性の欠如の原因となる。たとえば、サービスの必要から、新たにクラウド上のリソース（新しい仮想マシンインスタンスなど）が追加された場合、新しいリソースからのログも既存のリソースからのものと併せて取得されなければならない。類似の問題として、こうした動的な環境の変化が明示的にログに現れないことがある。たとえば、Web サービスが、ある PaaS アプリケーションのコンポーネントを呼び出したことがログに記録されていたとする。しかし、実際は、このサービスを構成する多数のインスタンスのいずれかに動的に割り当てられ処理されている可能性が高いが、それがどのインスタンスかまでは記録されないというような例だ。このように、どのリクエストをどのインスタンスが処理したのかがわからない不完全な記録では、たとえばインシデントの原因が、たったひとつの不正な侵害を受けたインスタンスであったような場合、分析を困難もしくは不可能にしてしまう。
- **法制度的な要求事項が、すべて満たされているか?** 同じサービスを利用しているテナントに関するプライバシー問題や、一般にログデータやとりわけ個人を識別可能な情報などに関する法令、規則などによって、ログの取得、保存および利用が制限される可能性がある。これらの法令や規則に依存する問題については、その会社のデータが処理、または保存されるいずれの地域の法制度についても理解、周知されなければならない。

[76] Intrusion Detection System（侵入検知システム）

- **どのようなログ保全条件を要求されるのか?** 法律、もしくはなんらかのルールが、具体的にログの保全条件を要求する場合がある。クラウドサービスの利用者は、分析やフォレンジック上の要求を満たすのに必要な保全の条件を理解、定義しておく必要がある。
- **ログ改ざんを防止できるか?** 改ざん防止できる形でのログ保存を保証することは、正確な法的、フォレンジック分析を行う上で不可欠である。一回書き込みのみ可能なメディアを使用することや、ストレージの分離、つまりアプリケーションサーバとログサーバを分離し、それらのアクセス権限も分離する、というような方法を考えることは、この要請を満たす上できわめて重要である。
- **ログデータをどのようなフォーマットで配信するか?** ログデータの正規化[77]は考慮すべき課題である。（最近出ている CEE[78][iv]のような）オープンフォーマットを使用することは、利用者側での処理を容易にする。

いくつかのインシデントは、クラウドプロバイダのみしか検知できない。それは、それらのインシデントが、プロバイダが保有するインフラの内部で発生するからである。クラウドプロバイダが、これらのインシデントの発生時に、利用者へ速やかに信頼できる形で通知し、あらかじめ合意されたインシデントレスポンスを実施することを SLA で言及することは重要である。それ以外のインシデント（おそらくは利用者側でも検知が可能なインシデント）であっても、プロバイダはより検知しやすい位置にいる。クラウドの利用者は、使えるログデータを相関分析[79]やフィルタ処理して、インシデント発見を最大限に支援してくれるプロバイダを選ぶべきである。

クラウドの導入によって発生する（ログ等の）データ量はかなり多くなる。ネットワークや利用者側での処理負荷を軽減するため、プロバイダがログデータを利用者側に送る前にフィルタリング処理するオプションが提供されるかどうかを調べておく必要があるかもしれない。さらに、クラウドサービスプロバイダ、テナント側双方での分析、相関（分析）のレベル等を含めた考察を行い、フォレンジックを行うにあたって特定可能なインシデントの種類などを明らかにしておくことも必要である。もし、分析が（最初に）クラウドサービスプロバイダ側で行われる場合、あらかじめ、どの時点でインシデントの調査をユーザ側にエスカレーションし、引き渡すかを決めておくことが必要になる。

9.3.4 インシデント分析のためのフォレンジックその他の調査サポート

途上ではあるが、フォレンジック関連コミュニティは、仮想環境でのフォレンジックのためのデータ断片を収集するツールやプロトコルについての検討を進めている。また、PaaS や SaaS 環境におけるフォレンジックサポートのための要求事項についても、研究が進んでいるテーマである。

利用者自身がフォレンジックのための要求事項を理解し、クラウドサービスプロバイダがどの程度それに適合するかを見極め、またそれに従ってクラウドサービスプロバイダを選んだものの、なおかつ要求事項とのギャップがあれば、それを明らかにすることが重要である。クラウドの利用者が得られる「証拠となり得る情報」[80]の量は、クラウドのサービスモデル、配備モデルの違いによって大幅に変わる。

IaaS サービスでは、利用者は自身が管理する仮想マシン環境について、自分自身でフォレンジック調査を実施できるが、クラウドサービスプロバイダが管理するネットワークコンポーネントについては、調査はできない。さらに、ネットワークトラフィック全般の調査、メモリのスナップショット取得、ハードディスクイメージの取得など標準的なフォレンジック調査の手順については、クラウドサービスプロバイダのサポートが必要とな

[77] Normalization: ベンダ固有の書式ではなく、標準的な書式に統一すること
[78] Common Event Expression
[79] Correlation : 相関分析
[80] Potential evidence : 証拠となり得る可能性を持つ（データ）

る。同様に、仮想化技術がもたらす高度な調査手法、たとえば仮想マシン状態のスナップショット[81]の取得やVMI[82]による動作中のシステム監視などについては、クラウドサービスプロバイダのフォレンジックサポートが必要だ。

PaaS や SaaS で、その根本原因がクラウドサービスプロバイダのインフラにあるようなインシデントについては、クラウド利用者は、ほぼ全面的にプロバイダの調査を信じるしかない。また前述のとおり、インシデントレスポンスにおける責任と役割は、SLA において、あらかじめ合意されていなければならない。PaaS においては、利用者側がクラウドに配備したすべてのアプリケーションレイヤのコードについて責任を持たなければならない。アプリケーション自体に根本的な原因があるようなインシデント（たとえば、アプリケーションコードのバグや脆弱性などによるもの）の調査に十分なだけのログはアプリケーション側で取得する（ように利用者側が実装する）必要がある。この場合、クラウドサービスプロバイダ側は、ログの生成機能を用意したり、安全なログストレージと読み出しのみ可能な API[83v]を使ったログへのアクセス機能を提供したりするような形でのサポートができることがある。SaaS プロバイダにおいても、利用者ごとに拡張されたログを出力したり、安全なログストレージや解析機能を提供したりすれば、利用者のインシデントレスポンス不可を軽減できる。それにより、アプリケーションレベルでのインシデントを大幅に減らすことにつながる。

プロバイダがその管理用バックプレーンやシステムを利用して、インシデントを監視し、攻撃を受けた、もしくは受けているシステムの部分を特定して、その情報をクラウドの利用者に提供できれば、すべてのサービスモデルにおいて、インシデントレスポンスは大幅に強化できる。

与えられたクラウド環境でのインシデント分析に備えて、利用者側のインシデントレスポンスチームはクラウドプロバイダが利用者の運用やインシデントレスポンスプロセスをサポートするために提供している情報ツールについて熟知しておく必要がある。（プロバイダが提供する）ナレッジベースや FAQ、インシデント分析マトリクス等は、クラウド基盤やその運用の一般事項についての利用者の経験不足を補うために役立てることができる。このような情報は、たとえばインシデントレスポンスチームが単なる運用上の問題と本当のセキュリティ上のイベントやインシデントとを切り分けるために役立つ。

9.3.5 拡大防止、原因の排除、そして復旧

インシデントレスポンスにおける他の段階と同じく、インシデントの拡大防止、原因排除、そして復旧のために立てられた方針が、有効かつ効率的で、法律やプライバシー面での懸念をすべて確実に考慮するためには、関係者の緊密な協力関係が不可欠となる。またこの方針は、ビジネスの目標と整合しており、サービスへの悪影響を最小限にとどめることを前提としたものでなければならない。クラウドコンピューティングのような複数の組織を巻き込むようなケースでは、さらに困難となるだろう。

この段階で取り得る選択肢は、クラウドの配備モデルやサービスモデルによって異なる。また、同様に、攻撃がクラウドのどの階層を標的にしているかによっても異なってくる。おそらく、状況に応じて異なる技術を持った異なる対応エンティティが、それぞれ複数の方針に基づいて対応することになるだろう。もし可能ならば、準備段階で、これらのシナリオを想定した机上演習を行い、（これらの複数の対応エンティティが）競合するような場合の対応も検討しておくべきだろう。また、利用者側は自分たちの組織が直接標的とされたインシデントだけでなく、プロバイダ自身への影響、もしくは同じ基盤を共有する他のテナントにも影響があるようなインシデントにプロバイダ自身がどう対応するかについても考慮しておかねばならない。

---

[81] 動作中の仮想マシンの、ある時点での状態をすべて取得、複製すること
[82] Virtual Machine Introspection : ハイパーバイザー側から動作中の仮想マシンやネットワークを監視するための技術の総称
[83] Application Program Interface : アプリケーションからプロバイダが提供する機能にアクセスするためのインターフェイス

IaaS の利用者は、インシデントの拡大防止、原因の排除、復旧に関して主たる責任を負うことになる。この場合、クラウドを利用することが利点となるかもしれない。たとえば、被害を受けた（仮想マシンの）イメージを、証拠を損なうことなく確保するようなことは、実行を一時停止した状態で（仮想マシンイメージを）アーカイブすれば可能である。また冒頭でも述べたが、修正されたコードを適用する際に、あるノードをシャットダウンする代わりに別のインスタンスを立ち上げることで、サービス中断時間を最小限に抑えるようなことも比較的容易になる。もし、特定の IaaS クラウドプロバイダに問題があるならば、利用者側は、他のクラウドプロバイダにサービスを移すこともできる。とりわけ、利用者側がメタクラウド管理ソリューション[84]を利用していれば簡単なことである。

SaaS や PaaS の利用では、もう少し話は複雑になる。利用者側で SaaS または PaaS におけるインシデントの拡大を防止するためには、ユーザアクセスを一旦遮断して、再度サービスを開始する前に、クラウド上のデータを検査し、修復する以外の技術的な選択肢はユーザにほとんど与えられていない。しかし、とりわけ SaaS においては、このような基本的な対応ですら、詳細なアクセス制御機能や（アプリケーション経由ではない）ユーザデータへの直接アクセス機能の提供などのような、クラウドサービスプロバイダ側のサポートがなければ困難、もしくは不可能となるかもしれない。

すべてのサービスモデルにおいて、プロバイダはサービス妨害（DoS[85]）のような、ある種のタイプの攻撃に対して支援ができるだろう。たとえば、小規模企業は、たとえば DDoS 対策のような高価な対策技術を自社のサイトにまで適用できるというような（クラウドサービスの）規模による経済的な利益を得ることができるかもしれない。この段階以前に検討が必要な項目としては、準備段階でプロバイダ側の施設において、利用者に対する攻撃対応支援が可能な範囲を明らかにすべきである。さらに、プロバイダが攻撃対応を支援する責任を負う条件については、契約上明記されるべきである。

SLA 及びインシデントレスポンス計画は、「経験のフィードバックと共有」[86]の活動を行えるように柔軟に作られるべきである。対応活動に基づいた詳細なインシデント報告を作成し、影響を受けた関係者（たとえば、クラウドの利用者、クラウドサービスプロバイダ及び対応に関与した他の関係先）間で共有すべきである。このような報告には、インシデントについての時系列の記述、主な原因もしくは脆弱性に関する分析、被害の低減、サービス復旧のために行った作業内容、そして長期的な再発防止策[87]についての推奨が含まれるべきだろう。

再発防止策については、利用者側に特化した部分と、プロバイダがサポートする部分の両方が含まれる可能性が高い。プロバイダ側のインシデントレスポンスチームは、インシデントに対する彼らの見解と、解決策に関する提案に関する部分を提供するべきである。利用者側とクラウドサービスプロバイダの双方で、まずインシデント報告の初期レビューを行った後、合同のミーティングを行って改善策の策定と承認を行うべきである。

9.4 推奨事項

- クラウドの利用者は、クラウドサービスプロバイダがどのような事象に着目して、それをセキュリティインシデントと定義しているかという点、また、どのようなイベントやインシデントを利用者側に、どのような方法で通報するかという点について理解しておかなければならない。オープンな標準形式を使用したイベント情報を使用することで、利用者側（のシステム）でも、容易に処理ができるようになる。

[84] 訳注：複数のクラウドプロバイダ間をまたいでサービスを複製、移動、管理できるようなクラウド管理のための製品のことをいう。
[85] Denial of Service (Attack)
[86] 原文では”Lessons Learned”だが、対応結果から学んだ経験をフィードバック、共有するための活動という意味で、このように訳した。
[87] 原文では、”Corrective Action”

- クラウドの利用者はインシデントに関連する事態の発生時に利用できる、クラウドサービスプロバイダとの間の確実な連絡手段をあらかじめ確保しておかなければならない。既存のオープンな標準方式を利用すれば、インシデントに関するコミュニケーションは容易になる[88]。

- クラウドの利用者は、クラウドサービスプロバイダのインシデント分析に関するサポート、とりわけ、クラウドサービスプロバイダがインシデント分析のための提供するデータの特性（内容やフォーマット）、クラウドサービスプロバイダ側のインシデントレスポンスチームが関与する内容や密度について理解しておかねばならない。特に、インシデント分析のために得られるデータが、利用者にとって重要になるだろうフォレンジック調査の要求事項を満たすかどうかについての評価は必須である。

- 特に IaaS において、利用者は仮想環境のスナップショットへのアクセスやロールバック、VMI など、フォレンジック分析や被害復旧に役立つ仮想化環境の利点を利用する機会を積極的に提供するようなクラウドサービスプロバイダを好んで利用すべきである。

- クラウドの利用者は、ハードウェアで支援された仮想化環境やフォレンジック分析機能を備えた堅固なハイパーバイザーの利用を推進するようなクラウドサービスプロバイダを好んで利用すべきである。

- それぞれのクラウドサービスごとに、利用者は最も重要なインシデントのクラスを特定し、インシデントの拡大防止、原因の排除、復旧などについての方針を定めると同時に、プロバイダがその方針の実行に必要なサポートを提供できることを確認しなければならない。

- クラウドの利用者は、クラウドサービスプロバイダのインシデントレスポンス履歴を入手し、レビューしておくべきである。また、クラウドサービスプロバイダは既存の利用者から得た情報をもとに、そのインシデントレスポンスプロセス(IRP)[89]に関する会社としての推奨事項を提供することもできる。

9.5 要求事項

- ✓ 利用しているクラウドサービスプロバイダそれぞれについて、そのプロバイダに預けられているリソースに影響するようなインシデントの検知と取り扱いについての計画を策定し、組織全体のインシデントレスポンス計画に記載すること。

- ✓ 利用されているクラウドサービスプロバイダそれぞれの SLA は、利用者企業のインシデントレスポンスプロセスにおける、検知、分析、拡大防止、原因の排除、復旧の各段階を効率的に行うためのサポートについて保証しなければならない。

- ✓ インシデントレスポンスの検証は、少なくとも毎年行うこと。利用者は、可能な限り多くの範囲で自身の検証手続きをプロバイダ（及びそのパートナー）のものと統合して実施すべきである。（利用者側とクラウドサービスプロバイダ側双方が参加した）チーム体制によって、インシデントレスポンス計画の様々な部分についての健全性チェックが実施され、それに基づいた推奨が、次のインシデントレスポンス計画に組み込まれることが理想である。

参考文献

[1] GRANCE, T., KENT, K., and KIM, B. Computer Security Incident Handling Guide. NIST Special Publication 800-61.

[88] 訳注：ここでは、単なる連絡手段のみならず、インシデント情報をプロバイダと利用者のシステム間で受け渡すことまでを想定して書かれている
[89] **IRP** - インシデントレスポンスプロセス。

[2] MELL, P. and GRANCE, T. The NIST Definition of Cloud Computing, NIST Special Publication 800-145.

[3] GROBAUER, B. and SCHRECK, T. October 2010. Towards Incident Handling in the Cloud: Challenges and Approaches. In Proceedings of the Third ACM Cloud Computing Security Workshop (CCSW), Chicago, Illinois.

[4] WOLTHUSEN, S. 2009. Overcast: Forensic Discovery in Cloud Environments. In Proceedings of the Fifth International Conference on IT Security Incident Management and IT Forensics.

[5] REED, J. 2011. Following Incidents into the Cloud. SANS Reading Room

[6] DANYLIW, R., et al. 2007. The Incident Object Description Exchange Format, IETF Internet Draft RFC 5070.

[7] MORIARTY, K. 2010. Real-time Inter-network Defense, IETF Internet Draft RFC 6045.

[8] MORIARTY, K., and TRAMMELL, B. 2010. Transport of Real-time Inter-network Defense (RID) Messages, IETF Internet Draft RFC 6046.

[9] FITZGERALD, E., et al. 2010. Common Event Expression (CEE) Overview. Report of the CEE Editorial Board.

[10] BIRK, D. and WEGENER, C. 2011. Technical Issues of Forensic Investigations in Cloud Computing Environments In Proceedings of 6th International Workshop on Systematic Approaches to Digital Forensic Engineering (IEEE/SADFE), Oakland, CA, USA.

第 10 章 //
アプリケーションセキュリティ

クラウド、特にパブリッククラウドの環境では、多大なフレキシビリティやオープン化の課題が、アプリケーションセキュリティの根本的な前提条件として発生する。いくつかの前提条件はよく知られているが、氷山の一角に過ぎず、ほとんどの前提条件は知られていない。この章ではデザイン、利用、最終的には廃棄に至るまでのアプリケーションライフサイクルについて徹底的に検証する。このガイダンスはいかにリスクを最小限化し、クラウドコンピューティングアプリケーションをデザインする際の前提条件を管理するかについて、すべてのステークホルダ(アプリケーションデザイナ、セキュリティプロフェッショナル、オペレータ、テクニカル管理者など)当てはまる。

クラウドコンピューティングは、Software as a Service (SaaS)、 Platform as a Service (PaaS)、Infrastructure as a Service (IaaS)の各レイヤにまたがるアプリケーション毎に課題が異なる。クラウド上で動作するアプリケーションは、生のインターネットと接続するアプリケーションと同等の設計の厳密さを要求する。つまり、そのセキュリティは外部環境を仮定しないでアプリケーション自体によって提供される。しかしアプリケーションへの脅威は、数多くの伝統的なデータセンタとは比べものにならないほど大量に、公のクラウド環境に侵入してくる。そのためアプリケーションをクラウド用に開発、あるいはマイグレーションする際なプラクティスが必要である。

概要. アプリケーションセキュリティの章では以下の分野に注目する:

- セキュア **SDLC**[90] (一般的なセキュアなソフトウェアの開発ライフサイクルの方法と、クラウドの特徴的な仕様について)
- アイデンティティ、承認、コンプライアンス ― クラウドでのアプリケーションセキュリティを構築するに不可欠なルール
- クラウドアプリケーションセキュリティに関連したアイデンティティの消費
- クラウドベースのアプリケーションによるクラウド暗号化に関連する資格付与の手続きとリスクベースのアクセス管理
- アプリケーション承認のマネジメント(ポリシー認証とアップデート、強制)
- クラウド環境下におけるアプリケーションの侵入テスト(一般的な方法と、クラウド上のアプリケーションの持つ特徴的な仕様について)
- クラウドでアプリケーションをモニタリングすること
- アプリケーションの承認、遵守すべき事項、リスクマネジメントと、マルチテナント性での利用や共有インフラのもたらす余波
- 悪意のあるソフトの回避とアプリケーションセキュリティを提供することの違い。

[90] **SDLC** - Software Development Life Cycle

10.1 セキュア SDLC (Software Development Life Cycle)

Secure Software Development Life Cycle (SSDLC) (もちろん一部は Secure Development Life Cycle を参照している (SDLC)) はクラウドへの移行とアプリケーションの開発においてその重要度を益々高めている。組織ではアイデンティティマネジメント、データマネジメント、プライバシーが開発したプログラムのラウンチからサービス終了までの期間を通して、アプリケーションセキュリティのベストプラクティスを定義しなくてはならない。

クラウド環境での開発は以下の点で伝統的なホスティング環境の開発と異なる:

- パブリッククラウドにとって、物理的なセキュリティの管理権はほとんど発生しない。
- サービス(たとえばストレージ)をあるベンダから他に移す際の潜在的な非互換性。
- ライフサイクル全般を通じたデータ保護を考慮しなくてはならない。これには、データの移動、処理、保管中も含む。
- クラウド環境下の Web サービスを組み合わせることは、将来的にセキュリティ脆弱性の温床につながる。
- 特に共用型のパブリッククラウドにおいて、ログへのアクセスは難しくし、且つ SLA に盛り込むべきである。
- クラウド中のデータの保全とデータセキュリティは伝統的な環境に比べてよりきめ細かく、階層構造をとらなくてはならない。
- クラウド環境内での関連業界や当局によるコンプライアンスの保証(と証拠としてのデモンストレーション)は、大抵困難を極める。

SSDLC の実施において、組織は開発のベストプラクティス、よく統制されたプロセス、ツール、彼ら固有の技術または成熟度モデルに適合するものを選択する。たとえば以下のようなものがある:

- Building Security In Maturity Model (BSIMM2)
- Software Assurance Maturity Model (SAMM)
- Systems Security Engineering Capability Maturity Model (SSE-CMM)

10.1.1 アプリケーションセキュリティ保証プログラム

アプリケーションのマイグレーションや、または下記のクラウド環境の開発やメンテナンスへの対応を実現するため、組織はアプリケーションセキュリティを保証するプログラムを持つ:

- 適切な幹部の管理下で、ゴールとメトリクスが決定され、導入、記録される。
- クラウド用のアプリケーションにおけるセキュリティとプライバシーのポリシーは、ビジネス上の理由や組織が規格に従う必要性から、当局や規格への遵守が求められる。

- 組織がセキュアなアプリケーションを設計し、デザインし、開発し、リリースした上で、実際に稼働し、教育を適切な要員に適切なタイミングで提供することで、適切な許容性やセキュリティの保証する許容範囲は可能になる。
- セキュリティとプライバシーリスクの評価はすべてのアプリケーションにおいて実施され、要求事項は適切に設定されなければならない。
- 開発やメンテナンスプロセスにおけるクラウドのセキュリティとプライバシーへの要求事項を定義し、導入する。
- 設定と変更の管理は監査されるべきであり、検証可能であるべきである。
- アプリケーションとデータ要件としての物理的セキュリティリスクの評価は実施されなければならず、すべてのクラウドインフラストラクチャコンポーネントへのアクセスはそれらを十分に満たす要件を持たなければならない。
- 規則に従ったコーディングのベストプラクティスや、使用する言語の強み、弱みの検討は、開発フェーズを通じて行われる必要がある。
- プライバシーとセキュリティの測定方法は監査可能であり、確認可能でなければならない。

10.1.2 確認と検証

10.1.2.1 デザインレビュー

いくつかの機能は他に比べてよりセキュリティに配慮が必要であり、クラウド内での実行可能権限が付与できないように、特定のアプリケーションのデザインや要求事項が示された際に検討しなければならない。

以下に挙げる理念はセキュアにデザインするアプリケーションを開発する際に従わなければならない。これらの理念がクラウドアーキテクチャと合わない場合、適切な技術や補完するコントロールに修正されるべきである。これらを行わないことは、クラウド能力の実行可能性に疑問をもたらすこととなる。

- **最低限の特権付与**. この理念は、業務を遂行するにあたり、処理上必要な最短期間だけ、必要最低限の特権とリソースを、個別またはプロセスや他のエンティティから与えられる。多くのケースでは、唯一セキュリティポリシーの自動化[91]メカニズムによる綿密で状況にあったアプリケーション認証マネジメントを用いることで、最低限の特権付与を効果的に実現できる。
- **権限分離**. これはコントロールポリシーと連動しており、2 つ以上の関連した機能に対する権限や、同時アクセスを認めてはいけない。
- **多階層防御**. これはアプリケーションを多層防御するものであり、前の層が破られても次の層で防御するものである。
- **フェイルセーフ**. もしクラウドシステムが落ちたらシステムのセキュリティ状態を把握できない状態になり、データの信用性を失う。例えば、システムがサービス不能な状態になったらユーザやプロセスからシステムへのアクセスを拒否する設定が必要である。
- **無駄のないメカニズム**. これは単純でわかりやすいデザインと防御メカニズムを実装するので、意図しないアクセスルートは存在しないか、してもたやすく検知して除外することができる。
- **完全な調停**. すべての構成要素[92]からコンピュータシステム内の全オブジェクトへのアクセスは承認を経なければならない。

[91] www.policyautomation.org
[92] An entity could be a user, code, a device, an organization or agent

- **オープンデザイン**. オープンアクセスクラウドシステムは、セキュアを高めるデザインをもたらすようにコミュニティのエキスパートに評価や査読をしてもらい、デザインする。
- **最小限の共通メカニズム**. 1 つのアプリケーションが他のアプリケーションを狂わせたり破壊する可能性を最小限にするため、(特に防御メカニズムは)最低限のメカニズムだけが複数のアプリケーションで共通して使われるようにしなければならない。
- **もっと弱い関連部分の認識**. セキュリティ機能のつながりや階層化した防壁において最も弱い部分を特定しておくことは重要である。これにより、システムへのリスクは許容できるレベルに抑えることができる。

10.1.3 構築

10.1.3.1 ソースコードのレビュー

セキュアソフトウェア開発の定義は組織レベルで実施し、遵守することが望ましい。セキュアソフト開発のガイドライは基礎事例として CERT (SEI)[93]から SAFECode[94]として、または ISO 基準に明確に記述されているものを使うことができる。

動的コード分析ではあたかもコードがクラウドアプリケーションとして動いているように動作し、テスターは外部インタフェースを用いてソースコードが正しいやりとりを実行中のコード中で行っているかを確認できるため、インタフェースの実行中に現れる脆弱性や異常はソースコード上で同時に起こり、その時点で修正することができる。

静的分析と異なり、動的分析はユーザとの対話を通じてソフトウェアの持つ脆弱性を引き出すことができ、ソフトウェアの設定の変更や環境コンポーネントの振る舞いを変更できる。

典型的なセキュアコードの作成とレビューのベストプラクティスは以下の通りである:

- クラウドサーバのコードには最低限の必要な情報しか入れない。コメントは実働コードから削除し、名前や他の個人的情報も取り除くべきである。
- バッファオーバフローや書式文字列アタック、競合等の典型的プログラミングエラーをチェックするため、ソースコード分析ツールを使う。
- 入力、ユーザ、コンピュータ、接続システムの「すべて」を検証し、正当であることを確認する。クラウド環境があらゆる入力を受け、受けたコンテンツを実行モジュールや SQL 命令に入れるような場合、コンテンツインジェクションなどの攻撃を受ける可能性がある。
- 例えばサードパーティ製ライブラリのオブジェクトコード(バイナリ)が使われる場合、静的な脆弱性チェックをオブジェクトコードに対して行うテストサービスを用いる。

10.1.3.2 セキュリティテスト

侵入テストは、悪意のあるソースからの攻撃に対するターゲットのネットワークセキュリティ耐性をシミュレーションで明らかにする方法である。このプロセスは、システム設定の練り込み不足や不適切さ、既知か未知のハードウェアやソフトウェアの欠陥、運用上の問題点または技術的な対策不足など、なにがしかの潜在的脅威を持つクラウドシステムの動作分析と関係している。この解析は潜在的な攻撃の特定や脆弱性の動的な検出に影響を与えることができる。

[93] https://www.cert.org/secure-coding/
[94] http://www.safecode.org/

クラウドモデルの形態は侵入テストの実施に大きな影響を与えるか、もし可能な場合でも選択に影響を与える。一般的に Platform as a Service (PaaS) と Infrastructure as a Service (IaaS) のクラウドは侵入テストを許諾する傾向がある。しかし Software as a Service (SaaS) プロバイダは、利用者が侵入テストを彼らのアプリケーションやインフラストラクチャに対して行うのを好まず、例外的にクラウドプロバイダのコンプライアンスに則るか、セキュリティのベストプラクティスとして、自主的な侵入テストをサードパーティに対して行う。

侵入テストは大抵「ブラックボックス」シナリオ、つまり事前に何もインフラに関する情報がない状態でテストを行う。最も単純なレベルで、ペネトレーションテストは 3 つのフェーズで構成される:

1. **準備(Preparation)**．この段階ではクライアントのデータの非公開とテスト実行者の法的な保護の条項を持つ形式的な契約の締結となる。また最低限、テスト対象の IP アドレスのリストを作成する。
2. **実行(Execution)**．このフェーズでは侵入テストが実施され、テスト実行者は潜在的な脅威を探す。
3. **提供(Delivery)**．結果の評価はテスト実行者から組織に伝えられ、修正手段が提案される。

ペネトレーションテストが明らかに知らされて (white box)行われたとしても、一部だけ知らされて(gray box)行われたとしても、全く知らされず(black box)行われたとしても、報告書と結果は渡され、脅威の軽減策の適用によりセキュリティ侵害のリスクは許容範囲内になるか許容可能なレベルになる。侵入テストは脅威とセキュリティ侵害のリスクをアプリケーション、リモートアクセスシステムや他の関連する IT も含む可能な限り幅広い視点をもって行われる。

10.1.3.3 相互運用性テスト

相互運用テストはクラウドアプリケーションがデータを他のコンポーネントやアプリケーションと交換できる(相互運用する)ことを評価する。相互運用性テストの活動はアプリケーションが共通のデータ交換フォーマットを用いてデータを交換し、同じファイルフォーマットを読み書きでき、同じプロトコルで通信できることを測定する。

相互運用性テストの大きな目的はクラウド中にあるアプリケーション同士の相互運用における問題点を、そのアプリケーションが使われる前に特定することである。相互運用性テストは主要なアプリケーションへのテストが、クラウド環境下で使用される前に終了している必要がある。

同様に相互運用性のテストは、これらのテストはすべてのデータの交換、プロトコルやインタフェースがセキュアな情報転送に用いられていることを確認する。

相互運用性テストは一般的に 3 つの中の 1 つの方法を用いる:

1. **全ペア同士のテスト**．このテストはしばしばサードパーティの独立したグループに属し、ソフトウェア製品間とソフトウェアベンダ間での相互運用の特性に深い造詣を持ったテスターによって実施される。
2. **いくつかの組み合わせでのテスト**．これはごく一部の組み合わせだけで行われ、テストしていない他の組み合わせでも同じように相互運用できていると推定する。
3. **参照実装に対するテスト**．これは、参照実装に基づいて、例えば許容される標準や、すべての製品を参照実装に対して使うことでテストされる。

10.1.4 定量的な改良

10.1.4.1 測定基準

いかなるアプリケーションセキュリティ保証プログラムも、分析されることができ、定期的なセキュア開発のステータスレポートで使われている測定基準で確認しなくてはならない。測定基準を用いた修正や報告を行うことは、いかなるアプリケーションセキュリティプログラムでもより高い成熟度へ増すことができる。

いくつかの推奨する測定基準は以下の通りである:

- クラウド中のアプリケーションとデータ資産は過去の 4 半期毎か、または年ごとのリスク度合い分類で測定できる。
- 4 半期か、または年内におけるアプリケーションセキュリティ保証プログラムのコストと、クラウドベースのアプリケーションのプロジェクトやプログラムの割合
- もし可能なら、アプリケーションが開発されるかまたはクラウド上で稼働してからセキュリティ不備による損失を試算する。

10.1.4.2 自動化した SDLC セキュリティテクノロジツールを使うこととその特性

人間中心の SDLC 行為(処理し、トレーニングし、テストする)は必要だが、時には不十分または実行可能な良いアプリケーションセキュリティの障害になる。可能であるならば、自動化ツールをセキュアアプリケーションの構築に使い、自動的にアプリケーション中にセキュリティを作り込んでいくべきである。

これらの自動的に技術的なセキュリティ特性を作り出すツールはしばしば開発と統合/組織化ツールをつなぎ合わせる。例えば、技術的な承認ポリシールールはアプリケーションとアプリケーション間のインタラクションを[95]分析するツールによるセキュリティ要件仕様から自動的に生成される(開発、導入、マッシュアップするとき)。

同様に、ある自動テストは開発、統合ステージで使われ、情報保証の証拠として扱われる。

クラウドにおいては、自動化ツールの使用は登録者の開発やマッシュアップ(特に IaaS)の終了と同時に終わるか、特に PaaS のクラウドアプリケーションプラットフォームでは、クラウドプロバイダから技術を提供する(登録者の設定がもしかしたら必要)。

ほとんどの SaaS では自動セキュリティはクラウドプロバイダにより作り込まれており、設定され、運用管理される。

10.2 認証、承認、コンプライアンス – クラウドにおけるアプリケーションセキュリティアーキテクチャ

10.2.1 クラウドサービス/アプリケーション開発とビジネス課題

重要なデータやシステムへのアクセスに関連して新しい潜在的リスクが発生する。明らかに分かっているアプリケーションやビジネス環境に関連したセキュリティリスクはセキュリティの全方位に渡って存在し、クラウドサービスやアプリケーションによる個人情報関連の参照によっても起こる:

- **統制権の喪失**. これはクラウド利用者がクラウドセキュリティポリシーやコントロール機能による統制権を喪失することが典型的である。
- **閲覧権の喪失**. これはクラウド利用者がクラウドセキュリティポリシーやコントロールの影響により閲覧権を喪失することが典型的である。
- **管理権の喪失**. これはクラウド利用者がしばしばクラウドアプリケーションのセキュリティ、特にアクセス権や監査ポリシーを管理できない状態である。

[95] This scientific field is called “model-driven security”, see www.modeldrivensecurity.org

- **ガバナンスの喪失**. 組織がインフラを直接管理する能力を失う可能性があり、そのときは適切な最高級のセキュリティを提供されていると、プロバイダを信頼する（もしくは常に信頼している）ことである。
- **コンプライアンスリスク**. データやシステムは管理者の直接管理下外にあるため、クラウドプロバイダは管理者の規制、プライバシーの保持、業界標準などの遵守に影響を与える。
- **独立性の喪失**. クラウドの特徴としてリソース共有やマルチテナント性がある。そのため競合企業が同じクラウドサービスで処理をしているのが実際である。その維持には、メモリやストレージ、ネットワークの独立が要点となる。
- **データ保護**. 組織が直接データを制御することを放棄したときに発生する。プロバイダがデータをセキュアに保ち、削除するときにはプロバイダがデータを完全に破壊する機能を持つ（または、破壊したことを検知できる）。
- **管理インフラとアクセス権の設定**. クラウドアプリケーションは、インターネット越しにアクセス、管理するために、複雑で制御の要求へ潜在的に関与する。セキュリティの落とし穴によるセキュリティリスクを拡大し続けるので、適したアクセス認証を慎重に考慮するべきである。

10.2.2 技術的リスクと解決方法

多くのサービスプロバイダは、クラウドサービスをデザインする際に、識別、権限付与とアクセス管理 (**IdEA**)[96] を作り込む。しばしばユーザの認証と認可システムは、フェデレーションクラウドで用いられる標準的な顧客管理システムに置き換えられる。

識別、権限付与とアクセス管理をサポートすることは、新任通過のメカニズムにより、導入に際して利用者に影響を及ぼす。課金や利用測定の基盤は識別管理に依存しており、導入や更新のリスクを発生させる。

識別、権限付与とアクセス管理のサポートは、利用者の統合に関連する。これらの関連付けにはセキュアを証明する認定証や属性、新しいユーザの追加などを含む。クラウドサービスプロバイダの事業オペレーションも課金やリソース利用の測定に影響を与える。結果として、識別、権限付与とアクセス管理統合を全体デザインの一部に組み入れるよう考慮することは重要である。

IdEA の能力を持つ（または持たない）アプリケーション、たとえば **SAML**[97]認証を受け付け可能なアプリケーションは、クラウドサービスのガバナンスや導入、ユーザへのサービス提供に影響を与える故に、IdEA に関する要求事項のあるクラウドアプリケーションは重大な定義を持っている必要がある。

典型的なクラウドアプリケーションにおける IdEA の要求事項は以下の通りである:

- 内部的な人事システムやクラウドベースの人事プラットフォームとの連動を引き金として、クラウドアプリケーションを一般ユーザや、パワーユーザ、管理者が使えるようにする構成になっているかを理解する。
- クラウドサービスにおけるサービス間のプロビジョニングを作り込む。たとえばクラウドベースサービスの内部アプリケーションなどである。
- 様々なソースからの要求や監査 (識別し、属性をつける)や、フェデレーション基準(例：SAML、WS FED など)に準ずる構成要素を受け入れる。

[96] **IdEA** - Identity, Entitlement, and Access Management
[97] **SAML** - Security Assertion Markup Language, an XML-based OASIS open standard for exchanging authentication and authorization data between security domains

- すべての関連する構成要素(ユーザ、デバイス、コード、組織、エージェント)を識別し、属性をつけることにより、リスクを基準とした　クラウド全体での(または内部への)資格付与の判断を実現する。
- 機能豊富なリスクベースの権限付与スクリプトは保護すべきリソース(つまりどのリソースを利用してよいか)へのアクセスマネジメント(認可、分配、更新など)を実現する
- たとえば要求ベースの認証や、最低限の役割ベースのアクセスコントロールのような統制を要求するポリシーを、内部セキュリティや規定によりサポートする。
- SOX、PCI、HIPPA など、内部ポリシーや法律上のコンプライアンスで規定されたユーザ稼働状況監視やログ、レポートを取ること。

様々な認証プロバイダやサービスプロバイダは、パススルーサインオンを実現するセッションキャッシュのため、 たとえば SAML, **OpenID**[98]、**OAuth**[99] トークンを作成する。クラウド中に展開されたアプリケーションはこれらの要求や判定を受け入れる機能を持つべきで、またアプリケーションやサーバはフェデレーションのために SAML、 OAuth、OpenID などのオープンスタンダードを受け入れるようデザインされるべきである。

権限付与の管理プロセスは、一元管理したインタフェースを通じてクラウドベースアプリケーションのアクセスコントロールルールを定義し、運用し、アクセスする能力を要求される。そうしたインタフェースやサービスは、それ自体がクラウド上にホスティングされているか内部化されており、**XACML**[100]のような標準を活用できる。ここでの主要な課題は管理可能性である。セキュリティポリシーやコンプライアンスの複雑性、IT の複雑性、そして IT の俊敏さの増加、セキュリティポリシーをセキュリティとして導入する変換作業はより時間がかかり、何度も繰り返し、高額がかかり、 間違いが起こりやすいと共に、簡単にエンドユーザ組織の負担するセキュリティコストが莫大になるため、従来のユーザはアクセスコントロールリストから役割ベースのアクセスコントロールで管理される一方、高額なエンジンは権限分離が侵害されないよう、これらのリストを処理する。

それどころか、権限付与レイヤへルールをセットすることは、要求、アサーション、トランザクション中にある要素の属性を供給することは著しい簡略化や組織の管理力を高め、最終利用組織（やクラウドプロバイダ）の支払うコストを減らす一方、ポリシー規定の持つ意味を高めることになる。

[98] **OpenID** - an open standard permitting users to be authenticated in a decentralized manner

[99] **OAuth** - Open Authorization, an open standard for authorization, allowing users to share their private resources with tokens instead of credentials

[100] **XACML**- eXtensible Access Control Markup Language, an OASIS standard

要求 / 属性	会社の人事マネジメントへのアクセス	ユーザ企業へのアクセス	企業人事マネージャによる自宅からのアクセス(会社のノート PC を用いて)	ユーザによる自宅からのアクセス(個人デバイス)
ID: 組織 ID	正当	正当	正当	不当
ID: ユーザ認証	正当	正当	正当	Valid
ID: デバイス	正当	正当	正当	不当
属性:機器はクリーン	正当	正当	正当	不明
属性: 機器にパッチ	正当	正当	正当	不明
属性: デバイスの IP アドレス (企業内ネットワークか?)	正当	正当	不当	不当
属性:ユーザは HR マネージャ	正当	不当	正当	不当
アクセス結果	Read/write access to all HR accounts	Read/write access to users HR account only	Read/write access to users HR account only	Read-only access to users HR account only

表1– クラウド人事アプリでの簡素な資格マトリクス

アプリケーションセキュリティコントロール、データセキュリティやプラバシー保護を導入するために、サービスは監査可能な業界標準、たとえば ISAE 3402/SSAE 16 (replaces SAS 70), PCI, HIPAA, ISO 27002 を用いるべきである。いずれもクラウドプロバイダのデータセンタの運用管理だけでなく、それらの環境下にホスティングしているアプリケーションに対しても、豊富な種類の規制手段を持っている。

クラウドにホスティングした環境下のアプリケーションとサービスに対し、どの基準をもって異なるセキュリティ要求と正しい判断を行ったかを測定することが重要である。要求ベースで分析をすることは、大きなコードの変更を避け、利用者はもとよりクラウドプロバイダの組織にとっても、アプリケーションや導入、サポートツールにとってサービスレベルの目的を向上させることにつながる。

10.2.3 コンプライアンス構成要素

いかなる基準を使うに関わりなく、クラウド中のアプルケーションのコンプライアンスを達成するには、それらがいくつかの基礎構成要素を持つと共に、すべての標準規格の基礎がクラウドプロバイダの物理インフラにより提供されていることが必要である。 インフラストラクチャの制御には、自然災害から設備を守る機能、電源喪失への対策、ハードウェア故障に対するデータバックなどが含まれる。これらには同時にシステムアドミニストレータの監査、データセンタへのアクセスや承認、アクセス内部的セキュリティのレビューの方式やそれの実施および報告の方法など、クラウドプロバイダのプロセスやポリシーのガバナンスをコントロールすることが含まれる。

インフラストラクチャ制御の上位レイヤは、アプリケーション制御の結果を収集する。複数レベルのセキュリティが求められ、たとえばトランスポート層はセキュアでなければならないなどがある。そこでは、データがデータセンタから出るとき、このレイヤは企業側の制御の元で、暗号鍵を使って暗号化が行われる。あるアプリケーションは、幾つかの基準にある保管方法やプライバシー要求を満たす強力な個別認識可能な情報転送のために、メッセージ層のセキュリティ、電子サインや他の付加的セキュリティ機能が必要な場合がある。すべてのこうしたサーバやアプリケーションに対するクラウド上で動くアプリケーションコントロールはデザイン段階から認識されている必要があるため、ふさわしい方法でアーキテクチャデザインに埋め込まれ、要求通りに開発される。特記する基準は PCI –DSS、 SOX、 ISAE 3402/SSAE 16、HIPAA や他のプライバシー基準である。

10.3 クラウドアプリケーションセキュリティのための ID, 資格とアクセスの管理

従来の自営型企業アプリケーションは、ファイアウォール、プロキシなどの従来からの境界型セキュリティ対策によって保護できた。このことにより、アプリケーションが、信頼できるハードウェアや信頼できるネットワーク上で動作するという意味で、企業が求めるリスクレベルやセキュリティ上の要求に非常に良く合致できた。また企業は、そのディレクトリ基盤を使って、アプリケーションに対してユーザを認証するとともに、アプリケーションにおける、すべてのアクセス（可否）判断を保持することができた。こうしたケースにおいては、企業（と外部との）境界が、きちんと定義されていたといえるだろう。

企業がこうしたアプリケーションをクラウドに移した時、それらのアプリケーションは、信頼できないネットワーク（境界のないネットワーク）で動作することになり、従来型の対策では、もはや十分に保護することができなくなる。アプリケーションは同じサービスプロバイダを利用している他の企業と共存する（リソースを共用する）可能性もあり、また様々なタイプのデバイスを使ってあらゆる場所からアクセスできるようになるかもしれない。このことは、クラウドアプリケーションに対するセキュリティ上の要求事項を根本から変えてしまう。このことを、www.rationalsurvivability.com による、「クラウド構造図」（cloud anatomy）にあてはめて見てみよう:

図 1—Cloud Anatomy

上の図の構造に、ユーザがアプリケーションにアクセスする手段を加えてみると、以下のようになる:

図 2—Cloud Delivery Components

上の構造図から、明らかにわかることは、アプリケーションはデータにアクセスするための窓であり、新しい境界はデータとそれにアクセスするための手段だということだ。このことにより、クラウドアプリケーションに対してセキュリティ対策を実施することが重要となる。データへのアクセス手段は極めて重要であり、様々な（利用者）識別情報や属性値の集まりによって、アクセス（許可）の判断を行う必要がある。IT の大衆化により、企業は現実の問題として私物デバイスの持ち込み（BYOD[101]）に直面している。故に、デバイスの識別情報や属性情報もまた、アクセス制御の判断を行うための重要な要素となる。

識別情報（ID)は単に認証のために参照されるだけではなく、そのユーザについてアクセスの判断を行うためのさらに多くの情報をたばねるためのものだと見なされるべきである。識別情報には同様に、アプリケーションが動作するデバイスに対するＩＤ（たとえば仮想マシンイメージにアクセスするためのＩＤ）や、仮想イメージに対して（利用企業側、サービスプロバイダ側のそれぞれにおいての）管理を行うための特権ユーザＩＤ、そのアプリケーションが連携する必要がある他のアプリケーションやサービスに対するＩＤ、アプリケーションの管理を行うための管理者ユーザＩＤ、そして、たとえばＢ２Ｂ，Ｂ２Ｃに類する企業外のサービスにアクセスするための外部ＩＤなどが含まれる。また、アクセスに関する判断は、ＩＤと紐付かない属性値によって行われる場合もあるので、（アクセス制御に関する）ポリシー作成・管理ツールは、こうした非ＩＤ属性も扱える必要がある。（以下の「承認管理とポリシーの自動化」を参照）

この節では、ＩＤ、資格の付与およびアクセスの管理（IdEA[102]）が、どのようにアプリケーションのセキュリティに影響するかについて見ていく。IdEA は、おおまかに以下の５つの部分に分けることができる:

1. 認証
2. アクセスの）承認[103]
3. （ＩＤや資格情報の）管理
4. 監査とコンプライアンス[104]の確認
5. ポリシー

10.3.1 認証

認証では、アプリケーションに対して（ユーザの）識別を行い、それを保証する。これは通常、二段階で行われる。最初の段階はユーザ（の ID)を正しく識別することであり、次に、そのユーザに対してあらかじめ発行されている認証情報[105]を検証することである。クラウドアプリケーションの認証にとって重要なことは、（アクセスに使用する）デバイスに依存しない共通かつシンプルなユーザインターフェイスと単一のすべてのデバイスで利用できるプロトコルなどである。同様に、多くのサービスプロバイダが、サービスを API[106]経由で公開し

[101] Bring Your Own Device : 私物デバイスを仕事にも使おうという考え方を意味する略語
[102] Identity, Entitlement,Access ：の頭文字
[103] 訳注：Authorization ： （アクセスなどに関する）承認、認可
[104] 訳注：Compliance：日本では法令遵守と狭い意味で使われるが、欧米では法令のみではなく、社内規則や、各種標準などとの「適合性」という意味で使われることも多い
[105] 訳注：Credentials ：パスワードなど、そのユーザの正当性を確認するための情報
[106] Application Program Interface : コンピュータプログラムから直接、サービスの機能を利用するための機能呼び出し用インターフェイス。これによって、ユーザ側のアプリケーションからその背後でサービスとして提供される機能を利用できる。

ているが、こうしたAPIはパスワードよりもアクセストークン[107]を利用してユーザを識別するように設計されていることが多い。

通常の企業用アプリケーションでは、認証は（Active DirectoryやLDAPのような）企業のユーザ情報ストア[108]に対して実行され、多くの場合、認証のための情報はユーザIDとパスワードである。クラウドベースのアプリケーションで、こうした企業内の識別情報を使用するには、ちょっと工夫が必要だ。いくつかの企業はプロバイダから企業のネットワークに対してVPN接続を行っており、それによって認証に企業のユーザディレクトリを使用できる。この方法は確かに使えるが、企業側は（ネットワーク）遅延や接続性の問題、BCP[109]やDR[110]に関する問題などを考慮しなければならないため、新たなクラウドアプリケーションの導入に際して、この方法は使わないほうがいいだろう。企業は（こうした方法にかえて）SAML[111]やWS-Federation[112]のような、オープン標準方式による連携を考えるべきである。

また、企業アプリケーションを、そのパートナーや利用者が利用するようなことも増えている。これは、同様にクラウドアプリケーションについても言えることだ。こうしたアクセスに対して異なる体系のIDを利用させるようなことを企業はあまりしたがらない。（しかし、今日においては、そうせざるを得ないこともよくある。）このため、企業は、パートナーが自分の（会社や他のプロバイダが発行した）IDを利用すること（BYOI[113]）を考えておくべきだ。そして、クラウドアプリケーションは、複数の組織が発行したIDや（そのユーザに付随する）属性値を受け入れられるように設計される必要がある。

クラウドアプリケーションは、広範囲から様々なデバイスを介してアクセスできるため、単純なユーザIDとパスワードによる認証方法はもはや安全とは言えない。（クラウドを利用する）企業は（クラウドに連携させるための認証システムに[114]）より強固な認証方式の利用を検討すべきである。（クラウドの）利用者は、オリジナル（のIDを提供するプロバイダ[115]）の認証方式として、自分のリスク（対策）要求にあった品証方式（たとえば、RSAトークン、SMSを使ったワンタイムパスワード、スマートカード／PKI、バイオメトリクスのような）強固な認証方式の利用を検討すべきである。これによって、強固な認証に基づく識別情報や属性値をクラウドアプリケーションに受け渡すことができるようになり、資格情報を確認してアクセス管理を行う際、より適切なリスク判断が行えるようになるだろう。

企業は彼らのクラウドアプリケーションに対して、「リスクベース認証[116]」の採用も検討すべきだ。この種の認証は、デバイスの識別情報や（アクセス元の）地域情報、インターネットプロバイダ、アクセスの傾向とい

[107] 訳注：APIによる利用の場合、毎回の認証によるオーバーヘッドを避けるため、最初に認証を行った際にアクセストークン（原文は単にtokenだが、意味がよくわかるように置き換えている）という証明データを発行し以後の利用ではそれを使用することが多い。Webベースアプリケーションにおけるクッキーやセッション IDに相当する。
[108] 訳注：ユーザ認証データベース、統合された企業ID管理システムのこと
[109] Business Continuity Plan : 事業継続性計画
[110] Disaster Recovery ：災害復旧（計画）
[111] Security Assertion Markup Language :（認証、承認などに関する）セキュリティ情報を交換するためのXMLベースの通信標準。主にWebベースアプリケーションの認証情報交換やシングルサインオンなどを実装するために使用される通信手順とデータ交換書式が定められている。
[112] 主に、XML Webサービスで実装されたサービス（API）に対する認証連携、シングルサインオンの構成に使用される通信手順とデータ書式の標準
[113] 訳注：Bring Your Own Identity : BYODになぞらえた造語
[114] 訳注：ここでは、クラウドの企業利用において企業が用意する認証システムもしくは、採用した認証サービスとクラウドを連携させる前提で書かれていると考えられる。
[115] 訳注：ここでは、一般利用者が、複数のクラウドサービスを利用する際に、たとえばOpenIDのような、特定のプロバイダが発行したIDを使用するような場合に、その発行元による認証について、（選択肢があれば）このような認証方式を選択すべきだということを述べていると考えられる。
[116] 最近、いくつかのサービスプロバイダがこうした認証方式を提供している。

った情報に基づいて（アクセスに関するリスクを算出して[117]）いる。クラウドのアプリケーションでは、最初に接続した段階の認証だけではなく、アプリケーション内で実行されるトランザクションの単位でも、このような「リスクベース認証」が行われてよい[118]。

また、クラウドアプリケーションにおいては、たとえば SAML や OAuth[119]のような適用が可能な標準仕様への準拠を推進すべきである。この節で先にも述べたように、クラウド（サービス）の API はパスワードではなく、アクセストークンを受け入れるように作られるので、モバイルデバイスを使ってクラウドサービスにアクセスしようとするユーザは、最初に自分の ID プロバイダ（現状では、おそらく自分の会社）によって認証を受け、それにより（企業の認証システムによって）生成された SAML アサーション[120]がクラウドサービスプロバイダに渡されなければならない。SAML アサーションの正当性が確認された後、OAuth のアクセストークンが生成され、モバイルデバイスに渡される。以降、モバイルデバイスは、このアクセストークンをクラウドサービスの REST[121]ベースの API にアクセスを行うために使用する。

10.3.2 承認とアクセス制御

承認（Authorization）という言葉を最も広い意味で考えるなら、それは、あるリソースに対するアクセス許可ルールの実行ということになるだろう。（アクセスのための）資格の付与というプロセスは、ビジネス上のポリシーを、企業リソースへのアクセスに適用するような形で実装するものだ。クラウドベースのアプリケーションに対しては、（アクセスの）承認は、単にその（対象の）内容だけを見て行うのではなく、一連の流れとしてとらえることが必要だ。

ユーザを中心に据えた承認モデルにおいては、ユーザがポリシーを決める主体（PDP[122]）である。ユーザが自分で管理するリソースに対するアクセスについて決定をし、サービスプロバイダ側が、それに沿った形での制御を行う主体（PEP[123])となるのである。OAuth は、このモデルの実装に広く利用されている。また、UMA[124]も、同様にこの領域での標準となりつつある。

企業を中心に据えた承認モデルでは、PDP もしくは、ポリシーを管理する主体（PAP[125]）となり、サービスプロバイダは、PEP となる。また場合によって、企業がクラウドセキュリティゲートウエイを導入し、これが PEP の役割をすることもある。（クラウドの）利用者企業は XACML[126]の採用とポリシーの集中管理を検討すべきだろう。

---

[117] リスクベース認証は、一般にそれのみで完結する認証ではなく、たとえばアクセスに付随する様々な情報をもとに、そのユーザのアクセス傾向を求め、通常とは異なるアクセス要素をもとに、なりすまし利用のリスクを計算するような機構を有している。

[118] この方式はそれのみで利用されることは少なく、他の認証方式と組み合わせて、たとえばリスク値がある値を超えたら、本人確認のため再認証や質問を行ったり、より強力な認証方式を要求したりというような使われ方が多い。

[119] OpenID で使用される、認証、許可情報を他のプロバイダと共有するための標準方式のひとつ

[120] SAML の仕様で定義された、認証済みユーザであることを証明するための書式

[121] REpresentational State Transfer の略、API の種類を意味する使われ方をする場合は、HTTP と XML を使用した形でデータ交換を行うような API で、SOAP（XML を使用して様々なオブジェクトを交換するために定義されたプロトコル）は使わない形のものを、おおまかに束ねるような意味で使用されることが多い

[122] Policy Decision Point：誰がポリシーを決めるか、という意味での主体を意味する

[123] Policy Enforcement Point：決められたポリシーに従ってアクセスなどの制御を行う主体を意味する

[124] User Managed Access：IETF で策定中の手順。OAuth の仕様を一部利用しているが、OAuth が、ユーザ自身でユーザ自身のアクセスポリシーを定める前提であるのに対し、ユーザ自身が、他のユーザに対し自分のリソースをアクセスさせるためのポリシーを決める状況も含めて拡張されている。

[125] Policy Administration Point：ポリシーを管理し、提供する主体を意味する

[126] eXtensible Access Control Markup Language：アクセス制御のための詳細なポリシーを記述するための XML 文書仕様。単純に誰がどのような権限でアクセスできるかのみならず、複雑な条件判断によるアクセス制御が記述できる。

クラウドアプリケーションによって、複数の形態でサービスを実現できる。それらは、従来のアプリケーションをミドルウェアを使用して Web サービス[127]として利用できるようにしたものかもしれないし、もともとクラウド用として作られた Web サービスかもしれない。しかし、たとえ Web サービスのインタフェースで抽象化されていたとしても、こうした（サービス）提供のためのサプライチェーンの広がりは、ガバナンスプロセスを複雑化させうるものだ。設計（開発[128]）時点でのガバナンスには、サービスの定義、開発、リリース、そしてこれらのサービスへのアクセスについてのポリシー要求事項の実装などが含まれる。実行時のガバナンスには、サービスの公開、サービス呼び出しへのセキュリティ制限の実装、サービスアクセス時のセキュリティ制限の実行、すべてのアクセスの監査などが含まれる。（こうしたガバナンスを行うために）セキュリティや管理のためのアサーションを生成するための W3C[129] WS[130]-Policy や、アクセス制限を実行するための WS-security. 各種トークンの発行と検証機能、交換のためのフォーマットを提供するセキュリティトークンサービス（STS[131]）を実装するための WS-trust などのオープンな標準方式を利用したい。

承認（とアクセス制御）の方式には、（認証情報をもとに都度、承認内容を確認する[132]）ロール（役割）ベース、ルールベース、属性（Attribute）ベース、クレーム（Claim）ベース[133]の承認モデル、そして（直接承認情報を受け渡して確認する）承認ベースのアクセス制御（ZBAC など）[134]のモデルがある。既に自身で Web アクセス管理（WAM[135]）ソリューションを保有している企業は、これを使ってクラウドアプリケーションも含めてシームレスに保護出来るように改良すべきだろう。多くの WAM では、ルールベースとロールベースのアクセス制御をサポートしている。

アプリケーションの設計者は、従来の（WAM）ソリューションを見直して、「（アクセスの）要求」と「（ユーザの）属性」を利用した、ルールに基づくアクセス制御への移行を検討すべきである。

属性ベースのアクセス制御を行う場合は、認証プロバイダ（IdP[136]）は、クラウドサービスプロバイダがアクセス制御を実行できるように、属性値を引き渡す。この場合、認証プロバイダは、以下の点に留意する必要がある:

- 認証情報[137]に付加される属性は、姓、名、メールアドレスのように、厳密ではないが、その利用者に紐付くものであることが必要。また、属性には IP アドレス、位置情報、所属するグループ情報、電話番号なども含まれることがある。
- 直接的に利用者を特定できるような属性を（サービスプロバイダなどと）共有する際には、それがプライバシー問題につながる可能性に注意が必要である。

---

[127] 訳注：この段落で言う Web サービスは、一般の Web サイトではなく、どちらかといえば、XML Web サービスのような、システム間のサービスインターフェイス（API）を意識していると考えられる
[128] 訳注：英文では Design time となっているが、明らかに開発も含まれる内容である
[129] World Wide Web Consortium : Web 関連の標準化団体
[130] WS：Web Service ：以下、WS-* シリーズは、それぞれの内容に沿った情報をシステム間で交換するための XML 標準書式の定義である
[131] Security Token Service : アクセストークンなどのセキュリティ情報を含むトークン発行、検証のためのサービス。WS-Trust の仕様に含まれている
[132] 訳注：こうした方式を総称して「認証」ベースのアクセス制御モデル（Authentication based access control）という。ここでは、後に出てくる「承認」ベースと暗に対比されている。
[133] 訳注：http://msdn.microsoft.com/ja-jp/library/ms729851.aspx
[134] 訳注：ZBAC は authoriZation Based Access Control（「承認」ベースのアクセス制御）の略で、HP によって提唱されたもの。認証情報としてではなく、直接、承認情報をセキュリティトークンで受け渡すような方式を言う。（http://www.hpl.hp.com/techreports/2009/HPL-2009-30.pdf）
[135] Web Access Management の略：（訳注）既存の企業向け、Web SSO 製品の多くがこれに該当する
[136] Identity Provider の略。（訳注）SAML などの実装において、一般に IdP は、SP（Service Provider）から、利用者の認証を請け負うので、ここでは「認証プロイバイダ」と訳した。
[137] Identity：厳密な意味での認証用 ID

- （IdP を設置・利用する）企業はアクセス制御の判断ができるような、属性の組み合わせを考えておかなくてはならない。また、（アクセスの）正当性を判断するための特定の属性を、どの属性プロバイダ[138]から得るべきかについても知っておく必要がある。これらの属性を（特定の利用者に関して）たばねて提供する属性アグリゲータ[139]も利用できるが、これは信頼関係の確立を単純にも複雑にもする。企業は、（アグリゲータを利用する際には）重複の解決や、不完全なデータの取り使いについて留意すべきである。

- 同様に、企業は属性値の拡張性、たとえば（電子署名のような）検証手段[140]、属性についての利用規約、日付などの付加、についても留意すべきだ。

- 企業はプライバシー、すなわち属性の提供ポリシー、同意の取得方法などについて検討するべきだ。この判断には、たとえば EU のプライバシー指令、国や地方の法令、認証サービス、クラウドサービスプロバイダおよび利用者の所在地における法律上の問題などが織り込まれるべきである。

- アクセス制御に必要な最小限の情報のみが（サービスプロバイダに）提供されるべきである。

- 企業は、利用者自身には常時紐付かないような属性[141]についてもサポートできるようにしておくべきである。

- 企業は、アクセスポリシーと権限付与ポリシー[142]の適切な管理に加え、それが技術的に実行（強制）可能であることを確認しておくべきである。（おそらくは PaaS アプリケーションをマッシュアップするためのツールに付随しているような）ポリシー自動化技術[143]などが、（技術的な）ソリューションの候補である。

クレームベースのアクセス制御が目指すものは、コントロールされた形での（ユーザ）情報共有である。「クレーム」はトランザクションの流れに沿って実行される。クレームベースのアクセス制御を使用しようと考える企業は、以下の点を検討すべきである:

- クレームとして意味があるものを使用する。（たとえば、単なるメールアドレスではなく、検証済みのメールアドレスなど）

- （クレームの）型、信頼度、新しさ、質など。（たとえば、もしクレームがその発行元以外でキャッシュされると、その新しさが失われる）

- クレームの内容に応じた、適切な発行・検証機関。（たとえば、電話会社は電話番号が正しいかどうか、メールプロバイダはメールアドレスが正しいかどうかを検証できる）

- クレームブローカー[144]を利用することで、必要な信頼度を持った複数クレームのパッケージを様々な発行元を持つクレームをもとに作るようなことができ、ユーザの許可情報へのアクセスを一元化できる。

---

[138] 訳注：Attribute Provider：ここでは、属性を取り出すべきディレクトリなどのシステムや、サービスとしての属性プロバイダ（SAML 仕様など）を含めた広い意味で解釈している。
[139] 訳注：Attribute Aggregator：これも、広い意味で、複数の格納場所にちらばった属性値を一元的にアクセスできるように統合するシステム、サービスを意味する言葉として解釈している。
[140] 訳注：Validation：例として電子署名をあげたが、たとえばより単純なチェックサムといったようなものも、その用途によっては考えられるだろう
[141] 訳注：not Identity-centric：たとえば、デバイス情報のような、同じ利用者に常には紐付かないような付加的属性。先に、アクセス制御におけるこうした属性の利用について触れた部分がある。
[142] 訳注：Entitlement Policy：承認を行うためのユーザ資格の付与に関するポリシー
[143] 訳注：10.3.5 以降に、より詳しい記述がある
[144] 訳注：Claim Broker：クレーム集中管理のためのシステム。信頼できるクレーム発行を代行し、様々なクレーム発行元からのクレームに対して、必要な確認を行った上で、パッケージとして保証するような役割をはたす。

- トランザクションが必要とする最小限のクレームのみの提供

クラウドアプリケーションは、それ自身と同じ、もしくは異なるプロバイダが提供するクラウドアプリケーションの機能を組み合わせて（マッシュアップして[145]）構成されることがある。このような場合、企業はいかにして、これらの（下位にある）アプリケーション全体にわたってシームレスにユーザ認証を行うのか、また、これらのアプリケーションが細部のアクセス制御を行うために、どのようにして、グループの構成や資格情報、役割のような属性を共有するのかを検討しておくべきれある。こうした企業においては、SAML、OAuth、XACML、などのオープンな標準方式を利用することが推奨される。

10.3.3 運用・管理

企業における ID 管理（IDM）は主にユーザ管理（アカウントの作成や変更、削除）[146]及び企業アプリケーションに対するアクセスポリシーの管理を主眼においている。ID 管理は IdEA（ID と権限付与、アクセス管理[147]）において、ユーザに対してタイムリーに必要なアクセスを許可するだけでなく、退職したユーザアカウントの無効化やユーザの役割が変わった際のアクセス管理などをタイムリーに行うなど、非常に重要なコンポーネントである。企業において、ID 管理は通常、ユーザ情報やポリシーが格納されたデータストアと直接的、かつ密接に統合されており、多くの実装において、それらは大きくカスタマイズされている。クラウドアプリケーションの分散的な性質を考えるならば、このやりかたを踏襲しようとしても、（たとえば、データストアがクラウドサービスに置かれていた場合）IDM が、うまくプロバイダのデータストアにアクセスできないといった問題から、うまくいかない可能性がある。さらに、ユーザアカウント操作に関する標準的な API が存在しないという問題がある。多くのサービスプロバイダは、いまだ SPML[148]を実装していないからだ。

クラウドコンピューティングという意味合いから IDM という言葉を捉えると、それは単なるユーザ ID の管理ではない。IDM の考え方は、（複数の）クラウドアプリケーションやサービスのユーザ ID（の統合管理）、これらに対するアクセス制御のポリシー、これらのサービスやアプリケーションについての特権 ID 管理なども含めて拡張される必要がある。

最近、脚光を浴びつつある標準が SCIM[149]である。この標準がまず目指すのは、ID 管理の安価かつ容易で高速な実装だ。次の目標はユーザ ID のクラウドへ、もしくはクラウドからの移行を容易にすることである。SCIM は、よく練られたシンプルなコアスキーマを持ち、多くのクラウドサービスプロバイダがサポートする RESTful[150]な API をサポートするため、クラウドとの親和性が高い上に、SAML や OpenID Connect[151]など既存のプロトコルとも連携できる。（執筆時点における）これらの事実から、今後 SCIM は、ID 管理における業界標準となり得るだろうと考える。

---

[145] ここでいうマッシュアップは、上位のアプリケーションが必要な機能を他のアプリケーションが提供する API を使用して実装するような形のことを言う。
[146] 訳注：原文は （provisioning）である。
[147] Identity, Entitlement, Access の略語（前出）
[148] Service Provisioning Markup Language の略：サービスやユーザアカウントの操作を自動化するための標準データ交換書式（XML）。こうした標準が実装されることで、異なるプロバイダのサービス管理を利用企業側のシステムで統一的に実装できる。
[149] 訳注：原文では Simple Cloud Identity Management の略とされているが、2012 年 6 月に IETF において、System for Cross-domain Identity Management という WG が立ち上がっており、翻訳時点ではより汎用的な意味でのこちらの頭文字とされている。
http://www.internetsociety.org/articles/introduction-simple-cloud-identity-management
http://www.simplecloud.info/

[150] 前出の REST に類する API をこのように表現することがある。
[151] OpenID 実装のために OAuth2.0 などをベースに定められた連携プロトコル仕様。
http://openid.net/connect/

ＩＤ管理に関して企業が考慮する必要がある問題を以下に列挙する:

- 企業システムとクラウド間の相互、もしくは複数のクラウド同士での、ＩＤやアクセス権限に関する変更をどのように同期させるかという問題。
- 企業システムとクラウドをまたいだＩＤやアクセス権の削除をどのように行うかという問題。
- いかに管理しやすく、かつ保守性がよくて低コストな方法で、アクセスポリシーを作成、更新、管理するかという問題。

多くの企業において、現状で考えられる解決策は、企業システムとクラウドの両方に対応出来るような、ハイブリッド IDM ソリューションの導入である。

アクセスポリシーの管理はアプリケーションセキュリティにおける主要な問題のひとつであり、その解決のため、しばしば最大限のセキュリティの自動化を要求される[152]。セキュリティポリシーの管理（の自動化）は、クラウド利用者が、法令遵守上の（要求事項に対する）支援をクラウドプロバイダに求めるであろうこと、しかし同時に、費用対効果の判断基準は、一般のクラウドコンピューティングに対してのものと同様に、それがどれだけ今後の支出や社内システムも保守コストを低減できるかという点である、ということを考えれば、とりわけ重要であると言える。

10.3.4 監査／コンプライアンス

企業が複数のクラウドサービスを利用するには 3 つの基本的な問題を解決しなくてはならない:

1. どのクラウドリソースにユーザはアクセスできるか?
2. どのクラウドリソースをユーザは具体的に利用しているか?
3. どのアクセスポリシールールに則って判断がなされているか?

現在のクラウドの展開手法では、企業利用者はクラウドサービスプロバイダの監査情報の閲覧をきわめて制限される。企業は事業運営上の遵守事項に合致しているかだけでなく、業界標準への適合と不正使用の疑念を持って監査情報にアクセスする必要がある。

現状の IDM 市場は識別アクセス統治(**IAG**)[153]に向かって市場全体が動いている。企業はクラウドアプリケーションのアクセスログデータや、ISAE 3402/SSAE 16, HIPPA, DSS PCI, ISO27002 等の監査標準に則ったポリシー遵守情報と相関性の高いものとして、SIEM (Security Incident & Event Management)ツールの利用も考慮すべきである。

一般的にクラウドアプリケーションセキュリティでの IdEA で考慮すべきことは以下の通りである:

[152] 訳注：ここでいう「自動化」は、管理者が管理画面から操作するというような管理ではなく、利用者側の管理システムが、API を介してすべての操作を自動的に実行できる、という意味で使われている。コンプライアンス等を考えると利用者の要求は多岐にわたるため、個別対応が困難なクラウドプロバイダは、管理機能を API として開放することで、利用者自身がそれを自分の管理システムから直接管理できるようにすることで、個別の要求事項を実装できるようにするのが一般化しつつある。

[153] **IAG** - Identity and Access Governance

- 認識、権限付与、アクセス管理は後付けの行為ではない。むしろアプリケーションが SDLC を開始するときに付加する要求事項である。
- デザイン段階では、可能である場合にアプリケーションに要求ベースでのアクセスをいかに管理するかを考慮する。
- SAPM (Shared Account Password Management)のようなツールを使い、アプリケーションでの特権アカウントの管理を行う。 これにより権限隔絶と最低限の特権付与を実現する。
- もし企業がすでに Web アクセス管理ツールを保有するなら、クラウド環境まで含むよう拡張する。つまり SAML を利用可能とする。
- クラウドアプリケーションはサービスプロバイダからの提供に合わせて、ロギング、データベース接続性などをうまく使う必要がある。多くのサービスプロバイダはこれらを Web サービスあるいは API を通じて提供している。OAuth トークンを利用することでこれらの Web サービスへの接続制御が出来る。つまりクラウドアプリケーションは OAuth、API 鍵等様々なトークンをサポート出来るよう考慮する必要がある。
- アジャイル開発プロセスに従うことと、アプリケーションがモジュール化したコンポーネントで構成していることを確認すべきである。これらはアプリケーションが新たに注目されている基準、例えば Mozilla's browserID、Microsoft's U-Prove、Kantara Initiative's UMA (User Managed Access)等を活用できるようにする。

クラウドアプリケーションは下記の脅威に注意しなくてはならない:

- **なりすまし.** 他人の身元情報を用いてシステムをごまかす
- **改ざん.** 通信データを変更する
- **否認.** 通信元からの通信を拒否する(要求またはレスポンス)
- **情報の開示.** 権限のない情報の開示する
- **サービス拒否.** 可用性に影響を与える
- **権限の昇格.** 役割と資格付を想定している

これらの脅威は IdEA の中で以下のように対応出来るとある:

- **なりすまし.** 認証(強力な認証)
- **改ざん.** 電子署名またはハッシュ(SAML アサーションの利用)
- **否認.** 電子署名(SAML アサーションの利用)、監査ログ
- **情報の開示.** SSL、暗号化(厳密に IdEA に特化しなくてもよい)
- **サービスの拒否.** セキュリティゲートウェイ(Web サービスでのセキュリティゲートウェイ)
- **権限の昇格.** 承認(OAuth)

10.3.5 ポリシー管理

アクセスポリシー管理(しばしば、資格付与の立場で「認証管理」と呼ばれる)とは、リソースとして保有するアクセスポリシーや、呼び出し者に関連した固有性や関連のある属性(例：呼び出し者の認証)、背景事情による属性(例：環境、ビジネス、IT に関連した)、目的に関連した属性(例：帯域制御や QoS アクセスポリシー)[154]等のアクセスポリシーを、特定し、メンテナンスする行為を指す。

権限付与の管理は、承認とアクセス管理で構成し、その中には識別には関連しないがアクセス判断には不可欠な属性(追加の識別とその属性)、オーサリングと属性管理のポリシーが自動的に盛り込まれている。

権限付与/承認は同時に個人識別に関連しない属性情報を考慮に入れる。例えば:

- IT の全体状態、ビジネスとビジネスプロセス、IT 同士の相互接続やビジネスプロセス、または環境など(例：危険レベル、緊急度合い)の一般的な状態
- 他のエンティティ(例：承認、先だっての判断)によるなされた他の判断
- 保護すべきリソースと関連がある属性(例：QoS または帯域制限ポリシー)

認証管理や判定、強制プロセスは、典型的に以下の 3 つの場所の 1 カ所で機能する:

1. 内在/または外部にあるポリシー強制ポイント/ポリシーサーバ/ Policy-as-a-Service の利用
2. クラウドアプリケーションの一部に組み込まれている
3. Identity-aaS か Persona-aaS (entities Persona は選択された属性を使った識別子である)を用いる

10.3.5.1 クラウドの問題 vs. ポリシー管理

クラウドにおける承認と権限付与管理はいくつかの課題を抱える[155]。

まずクラウドにおける権限付与の管理では、特徴的にクラウド利用者が技術的なアクセスポリシー決定および強制に十分なコントロールを持てないような問題がある。今日の多くのクラウドプロバイダでは、利用者が設定可能なポリシー適用ポイントを提供せず(例えば OASIS XACML Standard 等)、クラウドプロバイダは利用者のために利用者固有のポリシーを事前設定しないのが通例となっている(それらは加入者に特有のため)。

次に相互接続されたクラウド(マッシュアップされた)での権限付与管理の複雑性は、アクセスには相互接続されたクラウドマッシュアップ間での管理を要求し、各クラウドノードの判断で出来るものではない。このことは、ポリシーはサービスのつながりで承認される必要があり、相互接続したクラウドマッシュアップ間で権限委譲をしあうことを念頭に置かなければならないことを意味する。

10.3.5.2 承認管理のベストプラクティス

- 識別子または資格付与に基づく視点で規定を設けることは、組織へアクセスポリシーを付与し、メンテナンスする最もよい方法である。多くのケースにおいてリソース保護優先の視点は、ゴールをリソースの保護に設定し、自動的にエンドシステムに対しポリシーを適用されるため(例：権限付与/認証管理システム)、認証とメンテナンスを容易にする可能性がある。これらの事例では識別子はアクセスポリシーのわずか一要素であり、エンドシステムの保護を実施する目的のために書かれていることを忘れてはならない。

[154] Lang, U. “Access Policies for Middleware”, PhD thesis, University of Cambridge Computer Laboratory, 2003
[155] Details: Lang U, Schreiner R, Analysis of recommended cloud security controls to validate OpenPMF, Information Security Technical Report (2011), doi:10.1016/j.istr.2011.08.001

- ポリシーは必ず管理しやすい形態で特定されている必要がある。全般に関わるポリシーの特定、高レベル抽象化を満たす特定のポリシー、組織や事業、人の関連性がより理解しやすく表現されていることを含む。機構やツールは管理しやすい形態にし、詳細な技術的なアクセス接続ポリシーのルールを作れるようにする。(例:モデル駆動型のセキュリティポリシー自動化の利用)。

10.3.5.3 アクセス接続ポリシープロバイダのインタフェースアーキテクチャ

ポリシー決定店義/強制点(PEP's/PDP's)は標準的なプロトコル(例： XACML)または専用のプロトコル(例： Web サービスからの直接または他のミドルウェアからの要求)を用いてポリシーサーバにアクセスできる(相互接続したクラウドマッシュアップによるルールも含む)。ポリシーの適用先が単一の信頼できるドメイン（例：企業内インターネット）の場合、アーキテクチャは通常一対（サーバ）多(PDP/PEP's)となる。しかし、より大がかりな開発では、多くの異なる PDP/PEP's サービスを複数のポリシーサーバの連結により実現している。現在いくつかの承認管理製品では、承認管理ルールもサポートしており（例：XACML）、高速権限付与に使うこともできる。更にいくつかの認証管理製品は、より対象リソースに特化する観点から、認証ポリシーの生成にも使われている。

10.3.5.4 アクセスポリシーの提供

識別性と属性の提供を付加するために、アクセスポリシーはそれらの提供能力を持つ必要がある（「10.3.5.3 アクセスポリシープロバイダとのインタフェース接続アーキテクチャ」を参照）。更に言うならば、識別性のない属性は、提供可能でなければならない、例えば、ディレクトリサーバや他の属性を持つソースがある。両者とも PDP/PEP に対して設定可能である必要があり、適時性と正確さは重要な役割を果たす。

10.3.5.5 クラウドでのアクセスポリシー管理

アクセスポリシーの追加とメンテナンスにおける管理容易性の確保は主要な課題である。一般的に管理に関する管理者の理解と合致しない多数の技術的ルールや、システム変更(例：素早いクラウドマッシュアップ)のたびに頻繁に修正を施す必要のある技術的ルールの単純化、また秘匿性や監査レベルにおける技術的なポリシー適用と管理者の趣旨を合致させることは難しい。結果として、アクセスポリシーの追加と更新を自動化するツールとプロセスを注意深く設計することは重要である。

現在のソリューションは高レベルセキュリティポリシーを(低レベルの)アクセスルールに変換する下記を含む自動化機構を持っている:

- モデル駆動型セキュリティ[156]、ツール支援型のモデリングセキュリティプロセスは高レベルの抽象化を要求し、また他のシステム(他のステークホルダによって作られた)の情報の利用が可能であることを求める。ドメイン特定言語（DSL）で書かれているこれらの入力情報は、続いて強制可能なセキュリイティルールに人の手を極力介さずに変換される。同様にランタイムセキュリティマネジメント(例：権限付与、承認)、つまり IT システムデ守られたランタイムでのポリシーの強制、動的なポリシー更新、ポリシー侵害のモニタリングの機能も含む。
- 技術的アクセスルールを似たグループにまとめることは、複雑性を減らすことになる。
- 図解は技術的ポリシーの理解を容易にする。

10.3.5.6 クラウドでの承認のベストプラクティス

- 識別を中心とした視点に比べ、リソース保護の視点でアクセスポリシーを承認することが、よりクラウド環境に適しているかどうか、注意深く検討する。

[156] NIST IR 7628

- 特にクラウドマッシュアップを動的に行う環境では、アクセスポリシーの管理容易性を確保すること。このことはポリシー承認、ポリシー配布、強制、更新において一貫性を持つことを含む。技術的なアクセスルールを生成するにはポリシーの強制が必要であるため、自動化ツールやアプローチ(モデル駆動型セキュリティ)を検討する。
- ポリシー管理者とポリシー監査者に明確な権限を与え、指名する。
- クラウドプロバイダは利用者特有の承認ポリシーの設定を可能にし、ポリシーサーバが選択されたポリシーを正しく調停する PEP や PDP による承認管理を受け付けるよう手段を講じる。
- もしクラウドマッシュアップのための重要なポリシーサーバが必要ならば、「policy-as-a-service」をポリシーサーバとして利用することを考慮する。

現在選択出来る承認サービスのベストプラクティスは以下の通りである:

- 承認管理サービスの最も重要な特徴は、クラウド利用者ポリシーの管理性である。アクセスポリシーの管理は承認において最大の課題だからである。
- 人が直感的に理解でき、汎用なセキュリティポリシー要求から、サービスは可能な限り自動的に技術的ポリシー生成を認めるべきである。
- もし政治的に組織が存続可能で、自身も組織にいることが出来るのであれば、「policy-as-a-service」によりポリシー承認と更新をアウトソースすることを選択肢として考慮すべきである。クローズドコミュニティに提供される「policy-as-a-service」のように、コミュニティクラウドではよりふさわしく、受け入れられるだろう。
- サービスには OASIS XACML 等の入出力基準を確保する。
- サービスは、クラウドインフラにインストールされた PEP や PDP やインシデント管理と監査のためのポリシー監視ポイント連動できるようにする。

10.4 クラウド中のアプリケーションに対する侵入テスト

侵入テストは、悪意のある目的で内外のハッカーによる潜在脅威につながるアプリケーション中やシステムレイヤ中にある脆弱性の影響を測定することに関係している。テストは、「ブラックボックス」と見立てたアプリケーションやシステムなどの表層の動的分析によるものか、広く普及しているよくないプログラミングや固定的な経験則による典型的な脆弱性を特定する試みである。

Open Web Application Security Project (**OWASP**)[157]の中にある OWASP テストガイド V3.0 は動的セキュリティテストを 9 種類に分類している:

1. 構成管理テスト
2. ビジネスロジックテスト
3. 認証テスト
4. 承認テスト
5. セッション管理テスト

[157] OWASP - Open Web Application Security Project, www.owasp.org

6. データ検証テスト
7. サービス拒否テスト
8. ウェブサービステスト
9. Ajax テスト(RIA セキュリティテスト)

上記のセキュティテストのカテゴリは、アプリケーション脆弱性の性質はクラウド中に展開されても技術面では変化しないため、同様に適用できる。しかし、クラウド展開モデルのタイプによっては脅威ベクトルの追加(これは非クラウド環境での展開とは異なる)を盛り込む必要がある。

SaaS 展開において、同様の脅威ベクトルは、同じアプリケーションのランタイムが複数のテナントでサービスとして、あるいは異なるデータで使われる時、マルチテナントに起こりうる。

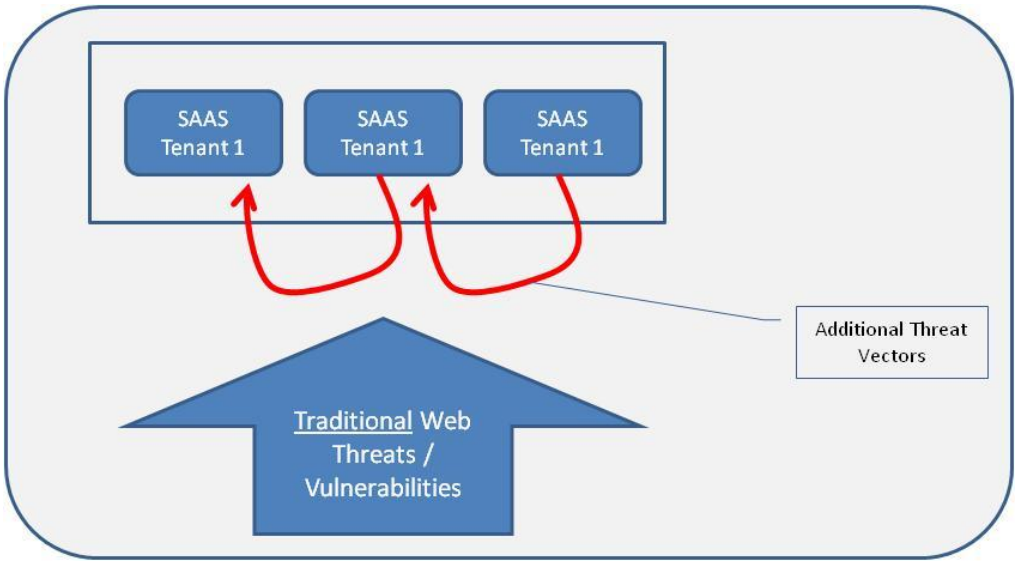


図3—脅威ベクトルの継承

テストの追加クラスは、クラウドのアプリケーション開発モデルの結果として脅威を表面化するために、開発及び収録される必要性がある。表で書くと以下のようになる。

表2—脅威ベクトルの継承

クラウドモデルアプリケーション	追加の脅威が内在する	脅威の例	未だに関係ある伝統的なセキュリティテスト	追加するテストの種類
SAAS	アプリケーションレベルでのマルチテナント性	異なるテナントが同じ SaaS 基盤を用いるので、他のテナントのデータに、Web レイヤの脆弱性を用いることでアクセスできる(昇格)	▪ 管理の設定テスト ▪ ビジネスロジックテスト ▪ 認証テスト ▪ 承認テスト ▪ セッション管理テスト ▪ データ正当性テスト ▪ サービス拒否テスト	マルチテナント性のテスト(特権増大の拡大)

			▪ Web サービステスト ▪ Ajax テスト(RIA Security Testing)	
PAAS	プラットフォームレベルでのマルチテナント性	同上	同上	同上
IAAS	インフラストラクチャレベルのマルチテナント性	仮想化セキュリティの不備(VM ゾーニングや分離のの不適切な実装が多重 IAAS テナントにわたり内部 VM 攻撃を引き起こす)	▪ 伝統的なインフラストラクチャの脆弱性評価(対象の「定義」が不可欠)	▪ 内部 VM セキュリティや脆弱性テスト

10.5 クラウド中のアプリケーションの監視

別の面でのクラウドセキュリティとして、異なるタイプのクラウドで構成されるクラウドベースシステムをどうやって、いかにして監視するかがある。クラウド中のアプリケーションを監視する意味は何か、どのように異なるタイプのクラウドアプリケーションを監視できるかを以下で詳細に述べる。

10.5.1 クラウド中のアプリケーションの監視: ギブアンドテイク

この文書では、我々は「監視」という言葉をアプリケーションセキュリティ監視に限定している。特に下記のカテゴリにおける評価基準は特定されるべきである:

1. **ログ監視.** コンプライアンスの目的のために、ログは単にためるだけはない。ログに出力された出力を理解し、対応可能なイベントを監視すべきである。アプリケーションが収集するログは、プロセスの存在が検出され、エラーに対して反応しなければ、全く用をなさない。

2. **パフォーマンス監視**. これは共有コンピューティング環境において大きな意味を持つ。アプリケーションパフォーマンスの劇的な変化は、他の利用者が与えられる制限以上のリソースを使用している(たとえば CPU、メモリ、SAN ストレージ等)、または悪意のある行為によりアプリケーションがモニタされているか、他のアプリケーションが共通基盤を共有している兆候と考えられる。

3. **悪意のある利用の監視**. これは成功するよう求められる監査と監視の混在である。企業側は悪意のあるユーザが攻撃によりアクセス権を得る、または彼らが持たなかった利用権を得ることが出来た時に何が起こるかを理解しなければならない。監査ログはログインの失敗または成功したことを記録しなければならない。データの妥当性検証ログは何を記録しているか。もしあるアプリケーションの通信量が明らかに増加するなら、誰が警報を鳴らすのか?

4. **セキュリティ侵害の監視**. ここでの鍵は、いかに早く、効果的に組織がセキュリティ侵害に対応するかにある。アプリケーションが複雑に関係し合っているなら、セキュリティ侵害の判別はおそらく比較的容易である(たとえば「ユーザ A は 2 回ログインしなくてはならない」)、さもなくばより努力を要する (たとえばデータの利用を監視するヒューリスティックアルゴリズムを開発する)。このことは SDLC が管理を容易にすることを示すよい事例である。

5. **ポリシー違反の監視(特にアクセス権).)** ポリシー判定点をどのように判断するかは、監視と監査は特に重要な 1 つである。つまり、どのポリシールールが特定のアクセス権につなげるかを決めるかである。これは一般的に一連の監査アプローチであり、典型的な監査の問題である誤認や記録の膨大化を避けることにつながる。

ログ監視の拝啓にはいくつかの重要なコンセプト、つまり「使う側」の公平さがある。公平性の重要さは、「提供側」にも言える。監視システムが効果的に動く機能を持たせるとき、アプリケーションは区切れのないロギングサブシステムを提供しなければならない:

1. **簡単に構文解析が可能**. ログは分離しているシステムで容易に構文解析できるフォーマットで書かれていなければならない。典型的なよく知られ、使われられている例としては XML がある。 悪い例としては領域が曖昧で、複数行にわたって出力しているのがある。

2. **容易な読解**. 考えられないことだが、ログをバイナリフォーマットで書いていると人間が直接読むことはあり得ない、ログエントリーはアプリケーションに精通した技術的バックグラウンドを持つひとが理解できるようにあるべきである。

3. **よくできたドキュメント**. ログをファイルに書き込んでいるのみでは十分でない。エラーコードは記録され、ユニークでなければならない。もし特定のログエントリーが解決の糸口となるなら、ドキュメントは確固としているかリファレンスとして扱うこととなる。

10.5.2 異なる型のクラウドでのアプリケーション監視

レガシーアプリケーションは共用環境にはないため、IaaS ベースのアプリケーションにおいて、アプリケーションを監視することは「当たり前」となっている。利用者は共用しているインフラに関しての監視情報や、悪意ある他のテナントからアプリケーションへのアクセスがあったかの情報を欲している。

プラットフォームとなるクラウドに監視アプリケーションを導入するには追加作業が必要となる。プラットフォームがアプリケーション監視を展開するソリューション機能を持たない場合、利用者は２つの選択肢を持つ。プラットフォーム上で監視を行う付加的なアプリケーションロジックを書くか、ログをリモートモニタリングシステム（顧客の内部モニタリングシステムかードパーティーのサービス）-に送るかである。

SaaS ベースのアプリケーションは最低限柔軟性を提供するため、これらのアプリケーションのセキュリティ監視を行うことは困難を極めることは驚くことではない。SaaS 製品を使う前に、利用者が考慮しなくてはならないことは:

- プロバイダはどうやってアプリケーションの監視を行うか?
- どういう種類の監査、ログ、または警報情報をプロバイダは利用者に提供するか。利用者は受け取る情報を選択する能力を持つか?
- いかなる手段でプロバイダは情報を利用者に送るか? (ツイッター? E-mail? 利用者の API 経由?)

クラウド中有でのアプリケーションセキュリティ監査における 1 つの終着点は、プロバイダ(またはサードーパーティーのクラウド監視サービス)が利用者のアプリケーション向けの監視システムを構築することである。もちろんこれらの監視システムは数百のアプリケーションをモニタリングする。プロバイダはこれらの監視リングシステムが事業上で「しっかり動く」ことを期待する。もし利用者が自らの監視システムを自らのアプリケーション上で稼働させる能力を持つならば、ほぼ間違いなくクラウドプロバイダの提供するシステムに比べて常に反応よく、より多くの情報を提供することになる。

10.6 推奨事項

10.6.1 セキュリティ保障のための推奨事項

- 機能面および規制面でのセキュリティと個人情報保護の要求は、クラウド開発と提供と一緒の、あるいは個別の要求事項と合致するよう設定する。
- クラウド環境中の攻撃ベクターとリスクの詳細な評価は理解されており、緩和戦略は要求事項の中に盛り込まれている。
- 全てのリスクや攻撃ベクターのインパクト評価は、各シナリオにおけるロスやダメージとともに請け負われ、文書化される。
- セキュリティやプライバシーへの要求、その影響は発生度合いと影響度合いにより順位付けされる。

10.6.2 リスク分析への推奨事項

- セキュリティやプライバシーのためのアプリケーションリスク分析　(秘匿性、完全性、可用性)は担保され、脅威モデルは設定され、保持されるべきである。
- クラウドにおける開発と運用の見込みから来るリスクは解析され、メンテナンスする脅威モデルに関連すべきである。
- クラウドアーキテクチャへの攻撃ベクターとインパクト解析仕様は分類され、メイテナンスされるべきである。
- セキュリティ保障の特徴とすべての認知されたリスクや脅威の追跡可能性は、メンテナンスされるべきである。

10.6.3 アーキテクチャへの推奨事項

- セキュアなソフトウェアアーキテクチャのフレームワークが開発され、メンテナンスされるべきである。
- 脅威を明確に軽減するクラウドコンピューティングのアーキテクチャパターン (たとえば“Open Security Architecture”[158]や TOGAF/SABSA[159])を使うべきである。
- アプリケーションアーキテクチャ内の再利用ブロックは、セキュリティ問題や欠陥発生の緩和に役立つ。

[158] www.opensecurityarchitecture.org
[159] www.opengroup.org

- クラウドに特化したセキュアデータアーキテクチャは選択されたセキュリティ構造上のフレームワークを拡張利用すべきであり、下記にあげるクラウドに特化した課題や脅威を考慮すべきである:
  - 動的データベースサービスの監視
  - データベースがいかなる時もどこに確実にホスティングされているかの確認
  - 離れている(全世界的かもしれない)システムから提供する総括的なアプリケーションの状況とイベントを予兆するフラグ等、すべての活動をログへ記録
  - どこに暗号化を使うべきかの判断(12 章参照)
  - システム内、データ、サードパーティによるすべての特権活動に対する適切な権限隔絶の付与、データを持つ組織のスタッフによる監視能力の付与

10.6.4 クラウド上のアプリケーションへの侵入テストへの推奨事項

- Web アプリケーションへの侵入テストを実施する際、OWASP のトップ 10 の脅威をチェックする
- 脅威を致命度や影響度によって脆弱性を分類し、改善プロセスを持つ
- 特権の昇格が行えないこと、またはセッションへの強制不能でもデータが独立していることを証明するため、マルチテナント性へのマニュアルテストを実行する
- アプリケーションを IaaS や PaaS 環境にマイグレーションするときに、VM ゾーニングや隔離、仮想化セキュリティなど下層のセキュリティコントロールへのセキュリティアセスメントを行い、見かけだけのアプリケーションエコシステムでなく、効果的に導入され、必ず実行されなければならない。

参照文献

[1] The Building Security In Maturity Model. http://bsimm.com/

[2] OpenSAMM – Software Assurance Maturity Model. http://www.opensamm.org/

[3] DAVIS, NOOPUR. Secure Software Development Life Cycle Processes. Software Engineering Institute

[4] SP-011: Cloud Computing Pattern. http://www.opensecurityarchitecture.org/cms/en/library/patternlandscape/251-pattern-cloud-computing

[5] KRUTZ, RONALD L. and VINES, RUSSEL DEAN. 2010. Cloud Security- A Comprehensive Guide to Secure Cloud Computing. Wiley Publishing, Inc., Indianapolis, IN.

[6] SARNA, DAVID E.Y. 2010. Implementing and Developing Cloud Computing Applications. Auerbach Publications.

[7] BELK, MARK, COLES, MATT, et al. 2011. Fundamental Practices for Secure Software Development: A Guide to the Most Effective Secure Development Practices in Use Today, 2nd EDITION. Software Assurance Forum for Excellence in Code. http://www.safecode.org/publications/SAFECode_Dev_Practices0211.pdf

[8] RITTINGHOUSE, JOHN W. and RANSOME, JAMES F. 2009. “Cloud Security Challenges” in Cloud Computing: Implementation, Management, and Security. Auerbach Publications.
http://www.infosectoday.com/Articles/Cloud_Security_Challenges.htm

[9] Guidelines on Security and Privacy in Public Cloud Computing. Computer Security Division Information Technology Laboratory. 2011. National Institute of Standards and Technology - Gaithersburg, MD 20899-8930
http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf

[10] Homomorphic Encryption. Making Cloud Computing More Secure.
http://www.technologyreview.in/computing/37197/

[11] Cloud Data Protection. Best Practices. http://www.ciphercloud.com/blog/?cat=10

第 11 章 //
暗号化と鍵管理

組織がデータの保存を必要とし、データにアクセスあるいは使用する人が信頼できない場合は、そのデータを暗号化しなければならないことはセキュリティ専門家にとって、言うまでもない。組織内で全設備を管理するオンプレミスのデータセンタ内でも、いくつかの規制（たとえば、PCI DSS）でデータは暗号化されなければならないと謳っているので、データは暗号化されている。

複数のテナントと、テナントのために作業する管理者がいるクラウドでは、より多くのデータを暗号化しなければならないのは明らかである。そうだとすると、それらのプロセスはどのように働き、組織は鍵をどのように管理するのだろうか？すべてを暗号化することは、複雑さを増すことになる。一方、それが他の問題に加えてビジネスプロセスの複雑さを引き起こしてしまう場合でも、これらの多量のデータを暗号化することが必要だろうか？データの暗号化と、後で鍵管理をする必要を減らす他の方法があるだろうか？本章ではこれらの課題を読み解く。

概要. このドメインでは、次のトピックを取り上げる:

- 暗号化概論
- 暗号化の代替方法
- クラウド展開における暗号
- クラウドデータベースにおける暗号
- クラウドにおける鍵管理
- 鍵の保存と安全確保

暗号化するか非暗号化を選ぶか？もし「はい」の場合、われわれはどのように鍵管理をするか？「いいえ」の場合、非常にリスクが高いのではないか？

11.1 暗号化概論

規制の順守または企業秘密という理由で機密に分類されるデータは、保護しなければならない。現在内部システムで管理されている秘密情報は、だんだんクラウドに移行していくので、同じく注意して保護しなければならない。クラウドへデータ移行させる事は、守秘義務とデータ保護の如何なる要件をも取り除かない。安全な企業の境界の外側（de-perimeterization）でデータのコントロールを失うことは、データ保護の複雑さと情報漏えいのリスクを増加させる。

クラウドにおけるデータ暗号化に関して、考慮すべき点が数多くある。それらは以下の通りである:

- クラウドに移行すると、暗号化を通してデータ保護することは、セキュア転送チャネル（例： TLS）を確実に使用すること以上のことを要求する。クラウドのデータ転送時の暗号化は、クラウドの中でデータ

が保護される事を保障していない。一度クラウドの中にデータが入った場合、使用中・未使用いずれでも、保護され続けるべきである。

- クラウドで保存や共有される際に保護されるべき非定型ファイルに関しては、ファイルへの直接保護を適用することが可能なときは、データ中心の暗号化、またはファイル形式に埋め込まれた暗号化を使用する。

- 暗号/復号キーを、全データライフサイクルに渡ってどのように管理するのか理解すること。重要情報を保護する鍵を保護し、適切に利用するため、可能な限りクラウドプロバイダへのあらゆる依存を避ける。

- 暗号化ファイルへの好ましくは無いが強制的なアクセスを規定する他国あるいは地域の法の従業員安全対策上の過失の機会を避ける。あなたが鍵を持っていれば、あなただけがファイルにアクセスできる。

- 見落とされがちだが、秘密情報を頻繁に含むファイルの保護を忘れてはならない。ログファイルとメタデータは、データ漏えいに至る途となり得る。

- 社内に保管されるファイルの暗号化に用いられる、同じ会社や規制の命令に準拠する十分な耐久性のある暗号強度(たとえば AES-256)を用いて暗号化すること。オープンで有効なフォーマットを使用し、可能な限り独自の暗号化は避けるべきである。

11.2 暗号化の代替方法

クラウドのデータの暗号化の代替方法を調べるのには、十分な理由がある。多くの組織にとっては、クラウドへデータを送ることは管理の関係を移行するのと同義である。

組織の外部に安全でないデータを送信することで問題がある組織においては、以下の代替策がある:

- **トークン化**. これは、パブリッククラウドとプライベートクラウドを統合/ペアにして極秘データの格納を実現することができる。パブリッククラウドに送られたデータは変更され、かつ プライベートクラウドに存在するデータへの参照を含むであろう。

- **データ匿名化**. これは（例として）、個人識別情報（Personally Identifiable Information (PII)[160]）や機密個人情報（Sensitive Personal Information (SPI)[161]）を処理する前に削除する。

- **クラウドデータベース制御の活用**. データベース内に構築したアクセスコントロールが、適切なレベルの分離を提供すると考えられる。

一般に、クラウドにデータを移動する前に、ほかの代替手法でデータのすべてまたは一部を暗号化し保護すべきか、あるいは、全く保護しないかを理解するために、良いデータ管理の実践が必要である。

他の代替手法の暗号化を通して何を保護するかを評価する際、以下に示す分野で、開示と悪用という 2 つのカテゴリに分割されるデータの共有リスクがある:

- **予期せぬ一般への開示**. Web での掲示あるいは投稿によって、情報またはデータを一般ユーザへ容易に利用可能とすること。

- **偶然または悪意のある開示**. 不適切なデータ保護の結果、第三者が情報またはデータを利用できるようにしてしまう行為。

[160] **PII** - Personally Identifiable Information
[161] **SPI** - Sensitive Personal Information

- **第三者に強いられた開示**. 訴訟における、データ開示を要求する召喚令状に応じなければならない義務。
- **政府への開示**. 政府機関、法律または裁判所命令（例：米国愛国者法）によるデータの公開。
- **ユーザまたはネットワークプロファイルの悪用**. 一見したところ安全なトラフィックデータから機密データを引き出してしまう分析やデータマイニングの能力、それによりユーザの行動、交友関係・嗜好・興味が暴露されてしまうこと。
- **推論の悪用**. 個人の行動や身元に関する推測をするために、1 次または 2 次の識別子を合成させることが可能なこと。
- **再識別と脱匿名性による悪用**. 元の内容を推測するのに十分な匿名情報へのアクセスが可能であること。

11.3 クラウド開発における暗号学

暗号化セクションの中で使用される 2 つの補足的な概念がある。それらは以下である:

- **コンテンツに応じた暗号化**. 情報漏えい防止(DLP)で用いられる content aware software は、データタイプやフォーマットを理解しポリシー設定を基に暗号化を行う。たとえば、クレジットカード番号は、法執行機関に送られる電子メールの中で暗号化される。
- **フォーマットを維持する暗号化.** フォーマットを維持する暗号化は、メッセージを暗号化し、それが入力メッセージであったような結果を生成するものである。例えば、16 桁のクレジットカード番号は暗号化の後にも 16 の桁数となり、電話番号も英単語も、電話番号や英単語のように見える。

ユーザの介在なしに企業～クラウド間を暗号化することは、データを安全にする望ましい方法である。もし、プロトコルも意識するよう構成され、パブリッククラウドアプリケーションへの REST http トランザクションの項目を暗号化できれば、Content aware software は、パブリッククラウド暗号化に活用できる。今日の情報漏洩防止(DLP)の使用事例は、通常電子メールによって企業を出るデータ保護を強化し、トランザクションが企業を出る前に、データを暗号化することができる製品に見られる。この原理は、クラウドデータ保護で使用することができるが、DLP 製品はアラートを発するかもしれない。content aware service　は、検知、暗号化、そして記録する必要があるが、アラートはする必要はない。

フォーマットを維持する暗号化は、暗号化データフォーマットやタイプを維持するデータに配慮することで、コンテンツを認識する手順をとる。例えば、従来の暗号化においては、暗号化されたクレジットカードはもはや 16 桁の数字ではない**暗号文**[162]**に変える**。フォーマットを維持する暗号化は、暗号化に加えて 16 桁の暗号テキスト値を生成する 。

さらにデータタイプとフォーマットを維持することで、暗号化を提供すれサービスは、多種多様なプロトコルの価値を容易に変えることができる。フォーマットを維持した暗号化の主要課題は、例えばクラウド内に格納された E-Mail 等の大きなクリアテキストの暗号化である。通常、大容量の暗号化は、ブロック**暗号**[163]を使用してテキスト値を暗号化する。フォーマットを維持する場合、それぞれの単語は同じ長さの文字列で暗号化され、時間がかかる。しかし結果は、オリジナルのプレーンテキストのように、同じデータタイプのフィールドに格納した暗号文データ値になる 。

クラウドアプリケーション内での暗号化は、アプリケーションのアーキテクチャが対応する必要があるビジネスアプリケーションにいくつかの課題を引き起こす:

[162] **Cipher text** - The result of an encryption operation. The input is known as clear text.
[163] **Ciphers** - Algorithm based software/hardware that perform encryption/decryption and signing/verifying

- もし、レコードまたはオブジェクトを検索するのにアプリケーションのデータが必要な時、暗号化された**主キー**[164]がそれを困難にする。

- もし、クラウドアプリケーションが機密データ特に PII や SPI データを扱うバッチジョブまたは他のタイプのプロセスを含む場合、さらにそれらのプロセスがクラウドに移行されたら、鍵管理が複雑となる。

データベースのレコードまたはオブジェクトを検索する必要のあるアプリケーションは、例えばトークン化などのユニーク値を格納するといった別の方法を選択することがある。アプリケーション内でクレジットカード番号へのアクセスを最少にすることを確実にするため、クレジットカード環境でトークンがよく使用される。ある値から生成されたユニークなトークンは、パブリッククラウド上の機密データを露出させることなくアプリケーションを使用することができる。

以下のセクション 11.4 で取り上げるように、可能ならば、鍵をクラウド内に格納すべきではなく、自社または信頼のおける鍵管理サービスプロバイダによって維持されなければならない。

クリアテキストデータ上で動作する必要があり他のビジネスアプリケーションやデータと一緒にクラウド上で実行されるプロセスは、機能するためには鍵あるいはサービスへのアクセスができなければならない。

11.3.1 クラウドデータベース内の暗号化

最初に考慮すべきことは、データを暗号化する必要があるのかどうかである。全てのデータベースは、データへのアクセス制限を行う機能を提供する。もし適切に実装されていれば、機密性を保護するのに十分かもしれない。

データベース内に格納されたデータを、保護するために暗号化を要する他の理由は次の通りである:

- データベースへの特権アクセスを持つ者から隠すため。（例：データベース管理者（**DBA**）[165]）

- 法的規制に応じるため。（例：カリフォルニアの SB1386）

- データ所有者が、データにアクセスするアカウント資格をコントロールできないために、アカウント資格をスキーマ内に保存するため。

クラウドデータベースや特にデータベースを用いる SaaS ソリューションを使用する場合、データベースまたはクラウドアプリケーションが鍵へのアクセスが必要な、暗号化されたデータで運用できる場合を除き、データベースの能力が損なわれるかもしれない。

データ暗号化は複雑さとパフォーマンスが犠牲となる。そしてこの暗号化には効果的な選択肢がある:

- **オブジェクトのセキュリティを使用する**. どのアカウントがデータにアクセスできるか制限するために、SQL の権限付与と取消しの命令文を使用する。あなたがアクセスを与えたアカウントは、認可されたユーザにのみアクセス権限を付与するようにコントロールしなければならない。

- **安全なハッシュを保存する**. データを直接格納するのではなく、データのハッシュ値を格納する。これは、あなたのプログラムが、所有者が実際に保存せずに、正しい値を持っていることを証明できるようにする。

11.4 鍵管理

[164] **Primary key** - A database column/field/attribute that is used to uniquely identify records in a database
[165] **DBA** - Database Administrator

パブリッククラウドコンピューティングにおける困難なプロセスの一つが、鍵管理である。パブリッククラウドソリューションのマルチテナント性は、そこで動作するプロセスの鍵管理の課題を引き起こす。

もっとも簡便なユースケースは、アプリケーションがパブリッククラウドのなかで実行され、企業からパブリッククラウドに移行するデータを暗号化する鍵が企業内でのみ使用されるものである。セクション 1 で述べられている通り、暗号化エンジンには出力時にデータを暗号化し、入力時にデータを復号化できるものがある。バッチ操作のような他のプロセスがデータを復号するため鍵へのアクセスを必要とし、それらのプロセスがパブリッククラウドに存在する場合、暗号鍵を使用するアプリケーションは複雑になる。

１つの共有鍵が会社全体で使用されることがないように、企業の暗号化ユーザは自身の鍵を持つ必要がある。そのような特定鍵を実現させる最も容易な方法は、それぞれのユーザあるいはエンティティのためのエンティティの識別を基に鍵をアサイン（また、管理する）する暗号化エンジンである。このように、エンティティのために暗号化されるものは、全てそのエンティティのために維持される。エンティティがグループ設定されているデータへのアクセス共有を必要とする場合、グループレベルの鍵がグループのアクセスを維持するアプリケーションに関係する。そして、そのグループのエンティティは鍵を共有することができる。このセクションの初めに議論されているような企業では、このような鍵を維持すべきである。

データがパブリッククラウド環境に保存される場合、その環境を終了する時にすべてのデータ（特に PII や SPI、または規定のある体制のデータ）がパブリッククラウドから削除されることを証明できるかどうかが問題である。これには、バックアップテープのようなすべてのメディアも対象となる。ローカル鍵管理の維持は、鍵管理システムで鍵を無効（あるいは削除/失効）にすることにより、パブリッククラウドに残るどんなデータも解読することができないことを保証する。

11.4.1 鍵の保存と保護

もし、プロバイダもクラウドサービスのユーザ同様、鍵管理にまつわるプロセスを強制的に実施しないのであれば、データ暗号化は価値がほとんどない。

プロバイダ側では、DBA が所有する個人鍵でのデータベースへのアクセス、又は単一鍵に依存しているデータベースサービスのアーキテクチャ同様、鍵サーバへのアクセスと暗号化データを持つサーバにまつわる SOD[166] の欠如は心配の種になる 。

KEK[167]やインメモリ上の暗号鍵生成を用いることで鍵自身を保護することにまつわるコントロールを行い、鍵サーバの暗号化された鍵のみを格納することは、あらゆる設計を行う場合に考慮に値する有効なアーキテクチャソリューションである。

デバイス自体が安全でないもの、あるいは、それ自身では暗号化システムと同等のコントロールレベルを持たないデバイス上の鍵を保護するようなクライアントサイドで管理される鍵は、心配の種となる。

11.5 推奨事項

一般的な推奨事項

- どのような暗号化/復号化製品を使用したとしても、鍵管理のベストプラクティスを実施する。
- 信頼できるソースからのベストプラクティスを得ることが可能な場合、既成の技術を使用する。

[166] **SOD** - Segregation of Duties - 責任の分離
[167] **KEK** - Key Encrypting Keys - 暗号鍵自身の鍵

- 信頼できるソースから暗号化、復号化、署名および検査の技術と製品を手に入れて、鍵管理のベストプラクティスの実践を行うこと。
- 最も推奨するのは、組織が自身で鍵を維持するか、あるいはそのようなサービスを維持している信頼できる暗号サービスを利用すること。
- もし組織が、解析または他のプロセスで、クラウド格納データを必要とする場合、組織は Hadoop のようなプラットフォーム上に構築し、データをクラウドから生成するべきである。このような Hadoop を含む開発プラットフォームでは、それ自身一連のセキュリティ課題を持っているが、本章の範囲外となる。
- 主要な範囲は、個人あるいはグループレベルで維持することができる。
- グループアクセスは、デジタル著作権管理(DRM)システムといった既製の技術やディスク、フォルダおよび E-Mail メッセージを暗号化するデスクトップ/ラップトップ上で動作するソフトウェアで管理される。

推奨事項 - データベース内の暗号化

- 標準のアルゴリズムを使用する。独自のスクランブル技術を考案/使用しない。独自の暗号化アルゴリズムは実証されておらず、簡単に破られる。
- Data Encryption Standard (**DES**)[168]のような、古く安全でない暗号化標準規格は避ける。
- オブジェクトセキュリティを使用する。基本的なオブジェクトセキュリティ（SQL ステートメントの権限許可と取り消し）を使用し、暗号化されたデータでさえもアクセスできないようにする。
- 主キーあるいは索引付きカラムを暗号化しない。もし主キーを暗号化すると、参照する外部キーもすべて暗号化しなければならない。索引付きカラムを暗号化すれば、その値を使用する問合せ処理が遅くなる。
- 縦欄式配列アプローチの暗号化（ビッグデータシステムがこの方式）を使用する。

11.6 要求事項

- ✓ 組織は、ベストプラクティスを維持し、監査をパスするために、自社の監督下で鍵を管理するか、または暗号サービスプロバイダの信用できるサービスを利用する。
- ✓ DRM やディスク暗号化製品のような既存の暗号化技術で使用される鍵は、集中化した企業の内部での鍵保管技術によって管理しなければならない。ハードウェアセキュリティモジュール （Hardware Security Modules (HSM)）は、鍵の格納や暗号化/復号化・署名・検査のような暗号処理の実行もしなければならない。
- ✓ 企業ユーザは、Content Aware systems または Format Preserving systems が必要に応じ暗号化/復号キーにアクセスできるといった、企業内の暗号化作業やその他のプロセスを有効にするために、登録手続を見直す必要がある。
- ✓ 権限付与の決定をするための処理の繋がりにおけるすべての構成要素の一体性に基づき、企業システムと統合された技術を展開する。

[168] **DES** - Data Encryption Standard

- ✓ 暗号化プロセスによって使用される鍵は、拘束力のある暗号オペレーションによって管理する。
- ✓ 可能であれば、**E-DRM**[169]または DLP のような既存の仕組みを使用する。
- ✓ 企業のアイデンティティ、システムへの拘束力のある暗号のオペレーションと鍵管理は、組織に最も柔軟な統合を提供し、組織が既知の監査や評価をした技術を用いる。

[169] **E-DRM** - Enterprise Digital Rights Management -企業向けデジタル著作権管理. A process that protects content such as internal corporate communications or copyrighted material.

第 12 章//
アイデンティティ、権限付与、アクセス管理

これまでのコンピュータ利用で用いられているアイデンティティ、権限付与、そしてアクセスの管理の背景にある考え方は、クラウド環境を導入する際の考え方、特に 3 つの別々の機能、アイデンティティ、権限付与、承認/アクセス管理(IdEA)に基本的な変化を求めている。

多くの組織にとって、従来型のアプリケーションを導入することは、サーバを場合によつては DMZ[170]に導入し、そして、多くの場合、ユーザ認証のためにディレクトリサービス(**DS**)[171]（例えば、マイクロソフト社の Active Directory、ノベル社の eDirectory、あるいは Open LDAP）と関連づけることである。場合によって、アプリケーションを導入したり、あるいは資格情報を思い出さなければならないユーザにとって非常に困ったことに、独自のスタンドアロン認証システムを使用して Web 配信サービスを使用することを意味する。（もっと悪い場合は、おそらくより信頼できる、他のドメインの資格情報を再利用する）。

これに比べ、うまく実装されているクラウドサービスあるいはアプリケーションのアイデンティティは、外部の多様な出所を、関連する属性と共に利用するべきである（アイデンティティが、ユーザ[172]だけでなく、すべてのアイデンティティと属性を持つデバイス、コード[173]、組織、そしてエージェントを利用することを忘れないよう注意する）。トランザクションに関わる複数のアイデンティティと属性をすべて活用することで、システム、プロセス、システム/アプリケーション内部のデータへの詳細なアクセスに関わる、全体的なリスクに基づいた優れた決定（この決定は権限付与プロセス[174]で定義され、承認とアクセス管理のコンポーネントによって実装される）をクラウドシステムが行えるようにする。

このアイデンティティとそれに関連する属性といつた複数のソースを使用するプロセスは、クラウドアプリケーションがインターネットに接続している可能性が高い場合に重要であり、また「本当の」クラウドサービスを使用したい組織や、代わりに内部の DS に接続された自組織の DMZ に仮想化技術を導入することを選択したい組織の主要なハードルの 1 つである可能性が高い。

アイデンティティ、権限付与、アクセス管理に対するこの境界のない方法[175]は、より柔軟で安全な方法を提供するだけでなく企業の境（すなわち、境界を仕切る線）の内部でも同様に実施することが可能である。

概要. 以下のセクションでは、クラウド環境のアイデンティティ、権限付与、アクセス管理の主要な側面を取り上げる:

- クラウド環境におけるアイデンティティの導入

[170] **DMZ** - DeMilitarized Zone

[171] **DS** or "Directory Service" is used through this section as an abbreviation for a generic corporate directory service, used for username and password login.

[172] Typically humans; for a wider definition and expansion refer to www.opengroup.org/jericho/Jericho%20Forum%20Identity%20Commandments%20v1.0.pdf

[173] Code includes all forms of code, up to including applications and self-protecting data.

[174] "Entitlement" is the process of mapping privileges (e.g., access to an application or its data) to identities and the related attributes.

[175] De-perimterization is a term coined by the Jericho Forum® (www.jerichoforum.org)

- クラウドにおけるアイデンティティアーキテクチャ
- アイデンティティ連携
- アイデンティティと属性のプロビジョニングとガバナンス
- 承認とアクセス管理
- アイデンティティと属性提供者とのインタフェースに必要なアーキテクチャ
- アイデンティティと属性の信頼レベル
- クラウドシステム上のアカウントのプロビジョニング
- アイデンティティに必要なアプリケーション設計
- アイデンティティとデータ保護

12.1 この文書で使用する用語

アイデンティティについて使用される言葉は混乱していて、ある用語は他の人にとってまったく反対の意味を持っている。この章を読む際の混乱を避けるため、この章で使用するアイデンティティ用語の一部を次のように定義する:

- **アイデンティティ**. *エンティティ*が一貫し、かつ包括的に唯一であると識別できる方法。
- **識別子**. 通常、公開鍵技術を用いて暗号学的に*アイデンティティ*を主張できる方法。
- **エンティティ**. *アイデンティティ*のある個別の種類。例えば、ユーザ、デバイス、コード、組織、エージェント。
- **権限付与**. *アイデンティティ*と関連する*属性*に権限（例えば、アプリケーションあるいはそのデータへのアクセス）を対応づけるプロセス。
- **リデュースドサインオン (RSO)**. ユーザが覚えていなければならない資格証明（通常、ユーザ名とパスワード）の数を最少にするためのアカウントそして/または資格証明同期ツールの使用；このための多くのソリューションはセキュリティ上何らかの妥協をしたものとなっている。
- **シングルサインオン(SSO)**. **SAML**[176]や **OAuth**[177]等の安全な規格を使用することで*アイデンティティ*と*属性*をクラウドサービスに安全に渡す能力。
- **連携**. ある*アイデンティティ*リポジトリと別なリポジトリとの結び付き。
- **ペルソナ**. *アイデンティティ*と、*エンティティ*が動作している環境にコンテキストを提供する特定の属性。*ペルソナ*は組織の*アイデンティティ*と組織の*属性*に伴う個々の*アイデンティティ*の集合である（例えば、企業の*ペルソナ*、ACME 社の CEO である Fred Smith 、ACME 社所有のパソコン）。
- **属性**. *アイデンティティ*の要素。

[176] **SAML**- Security Assertion Markup Language, an XML-based OASIS open standard for exchanging authentication and authorization data between security domains
[177] **OAuth** (Open Authorization)は、資格証明の代わりにユーザのプライベートなリソースを共有を可能にするオープンな標準である。

12.2 クラウド環境におけるアイデンティティ序論

アイデンティティのエコシステムは、拡張性の問題に直面している（誰もが互いを知っている小さな村から大きな町や都市に移住することを考えてみよう）。業界はアイデンティティシステムを単一のコンピュータからグローバル企業に、次いでクラウド展開モデルに拡大しているために、トランザクションに関わるあらゆるエンティティを識別する能力はさらに難しい深刻なものになっている。

しかし、クラウドでは、トランザクションのバリューチェーンでのすべてのエンティティのアイデンティティの使用、そしてリスクベースの決定への移行は、リスクを軽減することができないだけでなく、潜在的にセキュリティを改善することもできない。

以下の主要なポイントを考慮し、クラウドベースのソリューションを導入し、アイデンティティ情報を使用する必要がある:

- アイデンティティを主張できることでの強みは、そのアイデンティティと相互作用する場合にリスク計算に取り入れられる（匿名、自己主張、組織のアイデンティティを強く主張する知名度の高い信頼できる組織によって証明される、といったことが例に含まれる）。
- ペルソナの属性は、アイデンティティのように、そのペルソナと相互作用する際のリスク計算に取り入れられることを主張することが可能な強さを持つことになる。主張の強さは、自己主張から（組織のアイデンティティの強い主張をする）知名度の高い信頼できる組織による証明までの幅がある。
- アイデンティティと属性は、複数のソースにより利用される必要があり、その結果、クラウドソリューション/アーキテクチャがアイデンティティと属性という別個のソースを複数利用する能力を必要とする。
- 一時的なアイデンティティで十分（一意であると思えるエンティティに関する十分な情報）である場合がある。
- 見せかけの匿名が望まれる場合（例えば、投票）もある。

12.3 クラウド用のアイデンティティアーキテクチャ

内部のコンピュータセンターに在る従来型サーバベースのアプリケーションで境界のある組織の従来型アーキテクチャから移行しても、組織に柔軟さをもたらすことはほとんどない。クラウドベースのアーキテクチャへの移行は、組織の境界の内部に展開する（プライベートクラウド）か、パブリッククラウド（SaaS、PaaS、IaaS）で外部に展開するかに関わらず、組織に柔軟性を与える。

次ページの表に、実装されたクラウドアーキテクチャの種類によって、従来型への実装とクラウドへの実装とで、アイデンティティを如何に変える必要があるかを示す。

表 1—Identity Architecture Assertions

アーキテクチャの種類	従来型アーキテクチャ	クラウドアーキテクチャ
内部 / 境界内	内部の DS アイデンティティへの接続は、(おそらくリデゥースドサインオンのソリューションを使用する)アプリケーションで使用するために、DS 内で維持しなくてはならない。	複数のソースの*アイデンティティ*と*属性*を受け入れる能力。
内部 / 境界外	バックエンドで VPN のトンネルを使用して組織のサービスに対し密接なコントロールと接続をする必要がある。推奨しないアーキテクチャ。	アサーションを使用し、クラウドサービスにアクセスするための*アイデンティティ*と*属性*を提供する。
外部 / 境界内	外部のホスティングはサーバの提供者に境界を拡大することを意味する。*アイデンティティ*は利用者が管理しない環境に拡張され、多くは DS のレプリカをパフォーマンスのために外部の環境に設定することを意味する。	アサーションを使用し、クラウドサービスにアクセスするための*アイデンティティ*と*属性*を提供する。
外部 / 境界外	外部のホスティングは内部のアイデンティティを外部の境界(バックエンドのに繋がる回線あるいは VPN だけ)に拡大することを意味する。*アイデンティティ*は利用者が所有あるいは管理しない環境に拡張され、多くは DS のレプリカを処理のため外部の環境に置くことを意味する。	クラウドサービスにアクセスするための*アイデンティティ*と*属性*を提供するためにアサーションを使用する。

従来型の「**IAM**」[178]アーキテクチャでは、コンポーネントすべてが単一サーバの一部としてスタンドアロンであることが多いが、クラウドアーキテクチャでは多くのソースに基づいた*アイデンティティ*と*属性*を取り入れ、潜在的にもっと複雑であり、権限付与プロセスで定義した権限付与ルールによって承認/アクセス管理の決定をする。

図 1、*アイデンティティ*と*属性*は（潜在的に）複数の出所に由来し、権限付与ルールをアクセス権に変換する承認/アクセス管理レイヤに絡む。

[178] **IAM**-*Identity* and Access Management

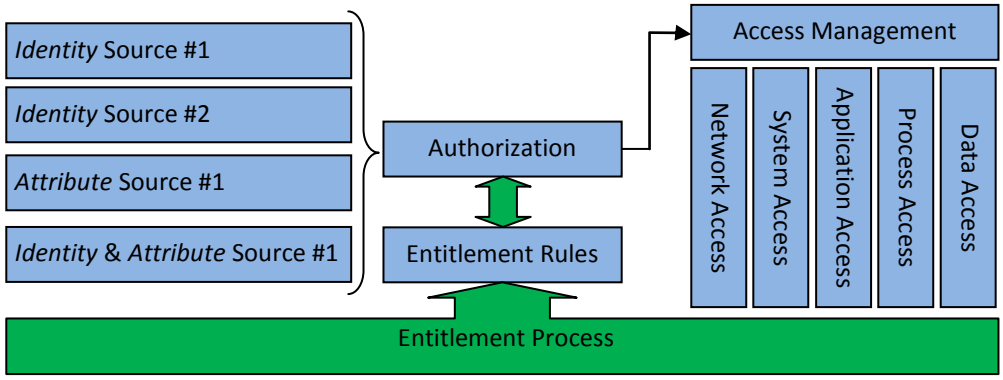


図 1: Generic Identity, Entitlement & Access Management System

アクセス管理は（ビジネス/セキュリティの要求事項、そして展開した IaaS、PaaS、SaaS のクラウドモデルによって）以下へのアクセスを決定しなければならない;

- **ネットワークレイヤ.** 権限付与ルールを満足させなければ、クラウドシステムを「見る」（例えば、Ping すなわち経路確認をする）ことさえも不可能であろう。権限付与ルールは、特定のインタフェースにアクセスを指示することもある。
- **システムレイヤ.** 権限付与ルールは、ターミナルサーバ対ウェブサーバのようにシステムにアクセスし変更を加えることが許されるプロトコルを定義する。
- **アプリケーションレイヤ.** 権限付与ルールは、例えばメニューや選択肢の限定された内容を表示するなど、*アイデンティティ*そして/あるいは*属性*を特定のアプリケーションが提供する機能に対応させることが可能である。
- **プロセスレイヤ.** 権限付与ルールは、アプリケーション内で実行可能なプロセス（すなわち、機能）を定義するために使用可能である。権限付与は、拡張機能（エコシステムからの送金等）が（バックグラウンドで直接取得あるいは導き出すことができる）追加の検証を必要とすることを定義することもある。
- **データレイヤ.** 権限付与ルールは、データ領域やファイル構造、さらに個々のファイルあるいはファイル内の（例えば、データベース内の）個々のフィールドへのアクセスを制限することがある。もっと高度なレベルでは、権限付与によって自動編集、例えば、まったく同じ文書にアクセスする 2 人のユーザが異なる中身（データベーステーブルの特定の動的ビュー等）を見るように使用することもできる。

権限付与プロセスは、利用者から解放しビジネス要求事項やセキュリティ要求事項を一連の権限付与ルールに変換する。このプロセスは、ルールの評価を可能にするために必要なアイデンティティと*属性*を定義する。そして、このルールは承認/アクセスシステムにも働く。

12.4 アイデンティティ連携

概念的に述べると、連携はばらばらなディレクトリサービスを相互に結合することである。組織の中には、連携の実装を外だしするため、このブリッジで他のパートナーに、アイデンティティ上定義された(パートナー自身が直接発行したのではない)信用のレベルを許すよう、アイデンティティがその「ブリッジ」の中で管理される連携とルール(通常法的契約)が一連の規則で決定される連携ゲートウェイ（「ブリッジ」あるいは「連携ハブ」）を選ぶものもある。

技術的に述べると、連携は、SAML のアサーションを扱えるゲートウェイ製品を介して DS 環境を拡張する組織に、本質的に異なる独立したセキュリティドメインへの移植可能性をもたらす SAML の利用である。他の組織はアイデンティティサービスからのネイティブの SAML アサーションを使うだろう。

この種の連携アーキテクチャの双方で、主張されている*アイデンティティ*と*属性*の出所を理解することは必須である。

連携の規格は、SaaS 展開モデルのアイデンティティ連携とアクセス制御に幅広く使用されている。類似の規格は PaaS と IaaS の展開モデルには存在しない。IaaS 展開モデルを活用するクラウド利用者は、アイデンティティのライフサイクル（共有アカウント、名前付きアカウント、特権アカウント等）をどのように管理するかを考慮に入れるべきである。スーパーユーザ管理（SUPM）と共有アカウント・パスワード管理（SAPM）用に特権*アイデンティティ*管理（PIM）を活用する企業は、クラウドの展開を支えるためこれらのツールを拡張して調査すべきである。企業すなわちクラウド利用者は、高度の特権を持つアクセス（HPA）用のポリシーを十分に定義しなければならない。

12.5 アイデンティティと属性のプロビジョニングとガバナンス

事前設定について述べる際に、通常、我々はユーザの事前設定について考えるが、リッチでリスクを考慮した決定をするには、クラウドシステム/アプリケーションは、トランザクションに関わるあらゆるエンティティの*アイデンティティ*と*属性*、そして潜在的に他のシステム/プロセスの別な*属性*を必要とする。

*アイデンティティ*と*属性*の一部の例（網羅したものではない）：

- ユーザアサーション：ユーザ*識別子*（ペアであるパブリック/プライベートキーのパブリックキー）
- ユーザ名（ユーザ名は*アイデンティティ*の別な*属性*でなければならない）
- 資格証明の強度/信頼
- 位置アサーション；IP アドレス、位置情報、GPS、携帯電話サービス位置情報
- 組織*識別子*（*識別子*ー暗号）と組織アサーション
- デバイス*アイデンティティ*（*識別子*ー暗号）とデバイスアサーション；必要機能、提示機能、サンドボックス機能、セキュアコンテナー、デバイスのクリーン度
- コード*アイデンティティ*（*識別子*ー暗号）とコードアサーション
- トレーニングの記録/コンプライアンス、等

*アイデンティティ*と*アイデンティティ*の*属性*の拠り所は（異なるソースに由来する場合もある）、権限付与プロセスの設計時に特定されている必要がある.。

原則として、クラウドサービスあるいはアプリケーション自体が*アイデンティティ*の拠り所となるソースであることを避けるべきである（例外として、クラウドベースの HR サービス、あるいはクラウド Identity as a Service の機能があり得る）。しかし、クラウドサービス（ベストプラクティスではない）への移行の間、クラウドサービス/アプリケーションは、アイデンティティを維持する、あるいは混用モードで運用する必要があり得る。

関連する*識別子*とその識別子の信頼のレベル無しには、*属性は根拠を持たないため*、あらゆる*属性*は*アイデンティティ*とリンクするべきである。これは直観に反するように最初見えるかもしれないが、権限付与プロセス

の強度は、ルールをビジネスが求めるやり方にするための必要*属性*を定義し、次いでその*属性*（関連する*エンティティ識別子*を伴う）を提供するために、信頼できる（あるいはできるだけ類似した）ソースを識別することにある。次のようないくつかの例がある:

- セキュリティ脅威レベル：組織、政府、あるいはアウトソーシング提供者の*アイデンティティ*
- 他のエンティティによってなされる承認あるいは事前の決定：*エンティティアイデンティティ*
- 保護対象のリソースに関わる QoS あるいは調整ポリシー：*システムアイデンティティ*

12.6 権限付与プロセス

権限付与プロセスは、利用者で始まりビジネス要求事項やセキュリティ要求事項を一連の権限付与ルールに変換し、クラウドシステムの様々な側面への承認とアクセスを決定する。次に、このプロセスは権限付与のルールを適正に評価するために必要なアイデンティティと*属性*を定義する。権限付与プロセスとその派生ルールは、クラウドシステムの承認とアクセス管理をするだけでなく、クラウド基盤のあらゆるレイヤの交渉/権限付与の程度、例えばネットワークそして/またはシステムレイヤのプロトコルやインタフェースを認めるといったことも、具体的に挙げることもできる。

権限付与プロセスは、あらゆるビジネス要求事項だけでなく技術的要求事項を記載した文書にも組込まれるべきである；そして、このプロセスはクラウドベンダのプロビジョニング/「利用者参加の」プロセスの不可欠な部分として特徴付けられるべきである。

権限付与プロセスは、いったんクラウドサービスが開始し提供されると停止しないが、権限付与ルールとそれに続くルールは承認とアクセスを導き、定常的レビューの主要なテーマでなければならない。そして、権限付与プロセスは、ビジネスの「システムオーナー」によってビジネスの要求事項に対し監査されなければならない。あらゆる監査には脅威とリスクの評価、そしてあらゆる規制要件が含まれていなければならない。

現在の解決策には、高いレベルのセキュリティポリシーを（低いレベルの）技術的アクセスルールに変換するための自動化したアプローチが含まれる。これには、以下の項目が含まれる:

- モデルドリブンのセキュリティ[179]，　これは、抽象度の高いレベルのセキュリティ要求事項をモデリングし、（別のステークホルダが作成する）システムで利用可能なその他の情報源を用いるツールが支援するプロセス。
- 複雑さを減らすため、技術的なアクセスルールを類似するグループにまとめること。
- 技術的なポリシーをもっと容易に理解できるようにする視覚的試み。

権限付与プロセスは、意味のある承認とアクセスの決定をするために要求されるエンティティ、アイデンティティ、そして*属性*を定義するべきである。また、プロセス内で固定する*属性*、一時的な（時間が経つと変わる）側面がある*属性*の定義をすべきで、このため再確認しなければならないインターバルと、プロセス内のトリガーのいずれも強制的に再確認しなければならない。

ビジネスのコントロールが及ばない外部のソースを必要とするアイデンティティと*属性*を権限付与プロセスで定義する場合、提供者（エンティティ）の組織的アイデンティティ（*識別子*）も同じく採用しなければならないが、しかし（時間を経たある時点で）採用を取り止めなければならない。

典型的な権限付与プロセスでは、次の 3 箇所のうちの 1 つで説明される:

[179] www.modeldrivensecurity.org

1. センター/外部のポリシー強制ポイント/ポリシーサーバ/Policy as a Service
2. クラウドアプリケーションの一部に組込まれる場合
3. Identity as a Service（IDaaS）を使用する場合

12.7 承認とアクセス管理

承認とアクセス管理は、権限付与ルールが（承認レイヤを介して）アクセス管理ルールに変換されるプロセスである。

ほとんどのクラウドベースのシステムでは、承認レイヤは、「ポリシー決定ポイント（PDP）[180]」、すなわち承認決定を評価して発行するポイント、そしてアクセス管理レイヤで「ポリシー強制ポイント（PEP）[181]」、すなわち PDP の決定を強制するポイントとなる可能性が高い。

PDP と PEP は、XML が実装されている宣言型アクセス制御ポリシー言語として XACML[182] (eXtensible Access Control Markup Language) を使用する、承認のエコシステムの一部である。

PEP は、クラウドアプリケーションの IF 文（条件文）と同じくシンプルであり、アプリケーションサーバ上で動いているエージェント、あるいは、アクセス要求に割り込み権限付与ルールの評価ができるよう必要なデータ（属性）を収集し、次いでその決定と実装を行う XML ゲートウェイのフィルターのように高度であったりする。

XACML、PDP、PEP の機能は、他の方法で実現する可能性もあるので（おそらく、閉鎖型か、独自のエコシステムの）クラウド環境で使用することは必須ではない。

PDP は、クラウド環境の外部の、おそらく利用者の環境で実装される。これには潜在的に幾つもの優位点があり、例えば、内部の DS とインタフェースすること、そして/または、判断がされたログを内部記録システムに直接統合することができること等である。

12.8 アイデンティティと属性の提供者とインタフェースするためのアーキテクチャ

*アイデンティティと属性*提供者とインタフェースするための 3 つの基本的なアーキテクチャは以下のとおり:

1. ハブが中心となつて*アイデンティティと属性*を管理（調整）し、次いでクラウドサービスあるいはクラウドアプリケーションと会話する「ハブ＆スポーク」モデル。
2. 複数のソースの*アイデンティティと属性*を受容するようクラウドサービスそして/またはアプリケーションが構成される自由形式モデル。
3. 複数のコンポーネントが分散し、潜在的に他のクラウドサービスを使用するハイブリッドソリューション。

いずれのモデルにも長所があり、以下を含むいくつかの要因に基づき選択される:

[180] **PDP** - Policy Decision Point
[181] **PEP** - Policy Enforcement Point
[182] **XACML** - eXtensible Access Control Markup Language

- サービスの利用者が自身のアイデンティティを持っている場合
- 選択するクラウドサービスの能力
- アサーションに基づく*アイデンティティ*と*属性*を提供する企業の能力

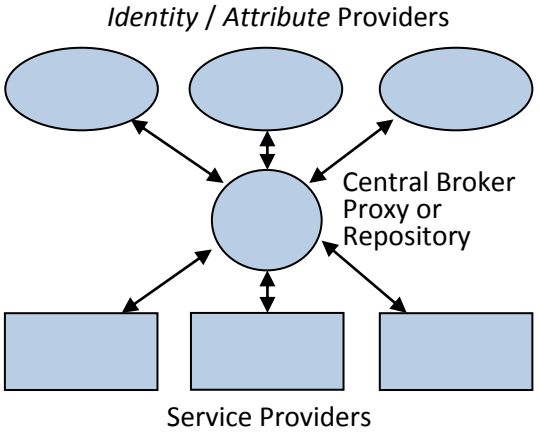


図 2— "Hub & Spoke" Model

12.8.1 ハブ＆スポークモデル

「ハブ＆スポーク」の手法では、一般的に、クラウドサービスが組織の*アイデンティティ*と*属性*情報用に組織と直接インタフェースすることが可能であり、理想的には基準に基づくアサーションのプロトコル形式、例えば OAuth や SAML が望ましい。

組織の内部システムは、ユーザ、その他のエンティティ、そして*属性の連鎖*を維持することに責任がある。これはたいてい従来型の IAM システムに似ていて、したがって組織が実装するクラウドソリューションにとり、DS あるいは LDAP システムの多くが SAML を「装着した」機能を持つことができるので、最も移行が容易である。

このモデルでは、権限付与プロセスでポリシー強制ポイントとポリシーサーバの使用を通じて組織内で処理し、XACML を介して（ただし、XACML はこのために広く使用されてはいない）通信することが多い。図 2 はハブ＆スポークの手法を図解したものである。

この手法の効果の 1 つは、組織内でのポリシー強制ポイントの維持で、必要な完全な全体像を得るために、組織内で維持される監査ログや、関連する他の（クラウド環境の外部、あるいは他のクラウド環境の）監査証跡の統合ができることである。これの例には、職務分掌の分析や、規制要件の充足が含まれる。

ハブ＆スポークの手法は、中央の登録プロセスですべての「ユーザ」全体に高度のコントロールが要求される場合に使用される可能性がある。これは、重い規制に従わなくてはならない組織ではいっそう可能性が高い。また、属性はたいてい中央のハブ内に保存（コピー）されるので、ハブ＆スポークは*アイデンティティ/属性の提供者*間の依存関係を教えるべきである。

また、組織がブリッジあるいは「アイデンティティハブ」に参加する場合に使用される。

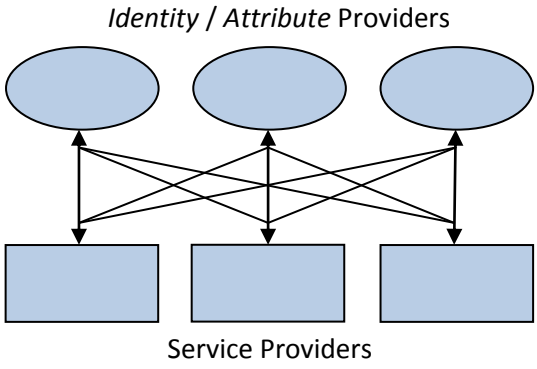


図 3—"Free Form" Model

12.8.2 自由形式モデル

「自由形式」モデルでは、クラウドサービス/アプリケーションは*アイデンティティ*と*属性*の出所を維持する責任がある。このモデルは、公衆向けのソリューション、あるいは多数の異なるパートナーとのソリューションにより適している。

自由形式の手法には、少なくとも現在の連携プロトコル（SAML 等）用には設定するのがより簡単であるという利点があるが、多数の「ユーザ」に拡張できる権限付与モデルが良好に実装されていることを当てにする。

手法の 1 つは、サービスと*属性/アイデンティティ*の提供者間に（SAML や OAuth 等のプロトコルを使用して）２点間の連携した信頼関係を確立することだが、この手法では提供者を採用するためとしないための効率的なプロセスが必要である。

自由形式モデルは、接続する新たなエンティティの環境がその場限りのものになりがちであるため、「ユーザ」プロビジョニングに課題がある。繰り返すが、権限付与プロセスを注意深く設計すれば、この問題を緩和することに役立つ。上の図 3 は 2 点間(訳注:「自由形式」)の手法を図解したものである。

12.8.3 ハイブリッドモデル

ハイブリッドモデルは、(定義上、)ハブ&スポークモデルと自由形式モデルの両方をミックスしたものである。例えば、権限付与ルールは組織内部に保持され、それ自身でクラウドサービスである PDP に押し出し、次いで、その決定が別なクラウドサービスの一部である複数の異なる.PEP に伝えられる。より大規模な展開では、多数の異なる PDP/PEP をサービスする複数の連携したポリシーサーバがあり得る。また、ハイブリッドモデルは、従来型、そして/またはレガシーなコンピュータと（パブリックそして/またはプライベート）クラウド環境を混ぜた構成で見受けることになる。

ハイブリッドモデルでは、分散したリソースの効率的利用を提供できるが、付随するものの範囲が複雑になるリスクがあり、セキュリティの抜け道が忍び込む。また、長期的維持をより不確実にする（実装したすべての人がとっくにいなくなった時に単純なルールの背景は、容易に理解できる）。

また、ハイブリッドモデルは、総合的な視点が取れるように共通フォーマットで一箇所にすべてのログを戻す潜在的な必要性のために取った意思決定と行動の、ログ収集上の課題を持つことになる。

ハイブリッドモデルの潜在的複雑さは、権限付与ルールの実際のアクセス制御への変換を開発、維持、そして監査するための可視化ツールを使用できる必要性を強調する。

12.9 アイデンティティと属性の信頼レベル

*アイデンティティ*と*属性*は、トランザクションで用いられる様々なアイデンティティ、そしてそれらのアイデンティティに付属する*属性の両者の*多くの信頼のレベルが付属する。これまで、この信頼の欠如は、システムにアクセスする必要のある全員の、それも（ある場合には）従業員でもなく、また直接管理していない何十万にもなる、アイデンティティの維持管理を組織にさせてきた。

あらかじめ合意した信頼レベルで協業する必要のある一部の組織（軍/航空業界、薬品、等）では、付随した信頼済みの*属性*も*持つ*信頼済みのアイデンティティがある場合、「ブリッジ」あるいは「連携ハブ」（12.4 節を参照）を使用する。

権限付与プロセスの中では、要求された*属性*だけでなく、それら*属性*の出所、それらを提供する組織、そして他から正当なものと主張され得る強度（信頼レベル）を理解することが必須である。

定義済みの信頼レベルをもつ外部の組織から*属性*を受け入れるためには、その組織の採用プロセス、そしてその*属性*を正当なものと主張する組織の*アイデンティティ*（*識別子*）が必要になる。

一般に、この目的は、正当性を主張する既知のアイデンティティをもつすべての属性で、主要な/信頼できる出所から来た*アイデンティティと属性の出所を明らかにすることであるべきで*、これは*属性*が示す信頼レベルは属性(訳補足:の正当性)を主張する*アイデンティティ*が示す信頼レベルを超えることができないからである。

*属性*がクラウドシステム自体の内部で独自に生成される場合、すべての*属性*が正確で、適切なライフサイクル管理をしていることを確実にするため、ガバナンスプロセスがなければならない。

12.10 クラウドシステム上のアカウントプロビジョニング

クラウドシステム上に（一般的に、ユーザ用であるが、あらゆるエンティティ用にも可能である）「アカウント」をプロビジョニングすることが必要な場合、これらのアカウントのプロビジョニング（そしてプロビジョニングの解除）に課題があるが、その理由は組織内で使用されている通常の「プッシュ」モデルは、たいていクラウド実装には実現可能なソリューションではないからである。

この文書を執筆している時点で、幅広く使用されている、あるいはデファクトなプロビジョニング標準は存在しない；SPML[183] (Service Provisioning Markup Language) はクラウド提供者には広く採用されておらず、SCIM[184] (Simple Cloud *Identity* Management)が唯一標準になる可能性をもって伸び始めている。

クラウドシステム上にエンティティをプロビジョニングするための鍵は、*アイデンティティ*と*属性*を提供し利用するシステムすべてに渡る、アカウント、アカウントの生成、管理、最終的に廃棄（削除、そして/または保管を含む）のライフサイクル管理全部を理解することである。

プロビジョニングする際には、*アイデンティティ*と*属性*の出所で対応の必要ないくつかの主要な課題がある:

- 人事部門が給与支払い名簿上の従業員の唯一の拠り所である場合が多いため、人事部門（あるいは人－ユーザ情報の信頼できる出所）との連係に問題が多い。
- 通常、パートナーの情報とパートナーのデバイスに信頼できる情報源はない。
- 他のエンティティ（特に、組織とデバイス）をプロビジョニングする能力のある組織はほとんど存在しない。
- パブリックなアイデンティティサービスは、一般的に自己主張した*アイデンティティ*と人についてのみ提供するだけである；その他のエンティティのタイプに拡張されることはない。
- プロビジョニングの解除はすべてのエンティティに拡げる必要があり、そのため契約終了時にほとんどの組織は他の組織の採用を取り止めたり、欠陥や陳腐化が分かった際にシステムで稼動中のコードを廃止する能力を持たない。

これらの課題や、標準のプロビジョニングの未成熟さは、良い計画策定や、開発中のクラウドエコシステムでアイデンティティ、属性、アカウント、そしてすべてのエンティティ種のライフサイクル管理を如何に運用するか包括的手法の必要性を強調する。

12.11 Identity-as-a-Service

クラウド Identity as a Service（**IDaaS**）[185]は幅広い意味の用語であり、クラウドサービスの*アイデンティティ*、権限付与、承認/アクセス管理のあらゆる部分の管理を対象とする。

これは、ソフトウェア、プラットフォーム、または基盤に対するサービス、そしてパブリックとプライベートの両方のクラウドに対するサービスを包含している。また、ハイブリッドソリューションも可能で、それによりアイデンティティは組織内で内部的になお管理可能であるが、一方で認証等の他の構成要素は SOA[186]を通して外部化する。これは、事実上クラウドベースの IAM ソリューションを促進する PaaS レイヤを生み出す。

さらに情報が必要であれば、14 章「Security as a Service」に記載した Identity as a Service を参照する。

[183] **SPML** - Service Provisioning Markup Language
[184] **SCIM** - Simple Cloud *Identity* Management
[185] **IDaaS** - Cloud *Identity* as a Service
[186] **SOA** - Service Oriented Architecture

12.12 コンプライアンスと監査

権限付与ルールの結果は、コンプライアンスまたはセキュリティ上の理由のため、権限付与ルール/承認プロセスでなされた決定と共に記録される必要があるだろう。コンプライアンスと監査は、*アイデンティティ*と一体のものとして結び付いている。*アイデンティティ*を適正に管理しなければ、規制に基づくコンプライアンスを確かめる方法は存在しない。また、監査も適正な*アイデンティティ*管理を要求し、またログファイルの利用は実用的な*アイデンティティ*システムがなければほとんど価値がない。

12.13 アイデンティティのためのアプリケーション設計

このセクションではアイデンティティに適用するのと同じくアプリケーション設計への適用を取り上げる。このセクションは 10 章ーアプリケーションセキュリティと合わせ読むことが必要である。

クラウドベースのシステムあるいはアプリケーションの設計は、アイデンティティのこととなれば、*アイデンティティ*と*属性*の情報が、少なくともトランザクションの間、そして恐らくある面ではもつと長くクラウドサービスやアプリケーションで利用するので、考え方を変える必要があるが、クラウド環境は恐らく一つの組織の物理的あるいは論理的な法域の一部とはならず、異なる法域にあることさえあり得るため、サービスとアプリケーションの設計は組織が所有し管理する DMZ 内の従来型のクライアントサーバシステムで用いられた設計手法と本質的に異なったものにする必要があるかも知れない。

この設計目標は、*アイデンティティ*と*属性*の必要性を最少にしなければならないことである。可能であれば、基本的な「on-the-fly(訳補足:その場で急いで作る)」アカウントのプロビジョニングから「アイデンティティ確認済み」のユーザアカウントに切り換える必要性がある敷居を把握している間は、アイデンティティの確認は必要ないという原則から始める。次のような例がある:

- 独自のセッションは、別な*属性*、例えば接続するデバイスの IP アドレス（IP アドレスがなりすましとして使用され得ることを理解し）あるいは独自のセッションクッキーを用いて確立できる。
- 多くの場合、ユーザ情報や実際の*アイデンティティ*を必要とせずに、*属性*に基づく権限付与だけで十分である；*ペルソナ*をセッション、さらにアカウントに結びつける必要があると仮定しない。
- 新たな*エンティティ*に初めて出くわした際（いわゆる SAML アサーションを伴う認証）、基本的なアカウントを on-the-fly で生成する。［この手法ではプロビジョニングの解除に関する考えが必要であることに注意する］
- 可能な場合は、いつも*属性*の派生物を使用する（例えば、誕生日を要求するのではなく「18 歳以上ですか」と質問する［誕生日＞（今日の日付ー18）］。

ユニークなアカウントを生成する場合、システムが*エンティティ*に基づく外部のユニークな識別子を利用するかどうか、あるいはシステムが自身で独自の*識別子*（利用者参照番号、等）を生成する必要があるかどうかを決定する。

ユーザアカウントを管理するクラウドシステムには、注意深い配慮を払う必要がある。クラウドのユーザアカウントが他のシステム（内部あるいは別のクラウドシステムいずれも）にある既存のユーザアカウントとどのように同期するか、特に「入会者と退会者（joiners and leavers）」のプロセスとの統合廻りや、ユーザが内部で異動する場合に必要なアクセス権の変更に注意深い設計上の考慮がなければならない。クラウドシステムを拡大させるための設計は（10 万ユーザもの関連性のないユーザ名、そして/または関連性のないパスワードを考えてみる）、すべての外部のアイデンティティの利用についての初期の設計上の考慮の欠如による手動あるいは

半自動の同期スクリプト、パスワード強度の確認プロセス、パスワードのリセットプロセス、漏洩後のパスワードのリセット等を含め、一般のヘルプデスクのプロセスに押し付けることを避ける必要がある。

内部の DS をクラウドサービスに拡げようとしたり、そして/または組織の DS をインターネット（一般に極めて安全性に欠ける）を通して、あるいは裏のチャネル（専用線あるいは VPN）を介して複製することは、組織全体の DS を組織のコントロールが及ばない環境に曝すので、避ける。また、RSO は on-log-in のセキュリティを内部で妥協して機能することが一般的であり、RSO をクラウドに拡張しようとするならなおさらそうなるため、RSO（リデュースドサインオン）製品を当てにすることに用心する。

概して、クラウドサービス、そしてクラウドアプリケーションは、SAML や OAuth（または、広く受け入れられてはいない WS-Federation）のような標準の SSO の連携フォーマットを受け入れる必要がある。

*アイデンティティと属性*を利用するアプリケーションを設計する場合、*アイデンティティ*があらゆるエンティティを含み、そしてアプリケーションのセキュリティが、可能な場合は、あらゆるレイヤ（ネットワークレイヤ、システムレイヤ、アプリケーションレイヤ、プロセスレイヤ、そしてデータレイヤ、詳細はセクション 12.3 を参照）を含む全体的なアプローチの一部であるべきであることを覚えておくこと。アプリケーションは、(例えば)Web/AJAX/Java を使用する完全で豊富な接続、あるいは（権限付与プロセスで定義された）権限付与ルールで判定された許可済み接続のタイプでの Citrix スタイルの「スクリーンスクレイプ」の接続の 2 つの接続方法がある。

12.14 アイデンティティとデータ保護

個人を識別可能な情報（PII）[187]や、特に機密個人情報（SPI）[188]に分類される情報から構成されている*アイデンティティ*の多様な態様を保持することは、あらゆる組織にとって問題である。組織の外部で管理されたり配置されるクラウドサービスは、あらゆる適用可能な法律と規制を順守していることを確実にするため、専門家のアドバイスを必要とすることになる。

どの法律や法域が適用されるかを考慮する際には、以下の項目（すべてを列挙したものではない）を検討するべきである:

- データ主体の国のすべて
- 組織が事業をしている国
- 組織が法人を持つ国々
- 組織が証券取引所に上場したり株式を発行している国々
- クラウドサービスが物理的に所在する国または国々
- 重要な法律、規制、そしてまた見せかけの規制（例えば、PCI-DSS）

12.15 利用者化とアイデンティティの挑戦

利用者そして/または利用者のデバイスとのやりとりは、クラウドベースのサービスとアプリケーションに多くの課題と機会をもたらす。インターネットに向かい合ったクラウドサービスに直接インタフェースする利用者と利用者のデバイスの能力は、ネットワークの複雑さのレイヤを剥ぎ取るが、*アイデンティティ*を使用して軽減可能な一連のセキュリティ上の難題も持ち込む。

しかし、利用者の場では、デバイスと、ユーザの*アイデンティティ*の規格はばらばらにされ、（定義上）企業社会で達成可能なのと同じレベルの準拠性と標準化を持つことはめったにない。

[187] **PII** - Personal Identifiable Information - 個人の識別可能な情報
[188] **SPI** - Sensitive Personal Information - 機密個人情報

残念ながら、ほとんどの利用者のデバイスと利用者自身は、強度の認証を行う認証システムに利用者とそのデバイスを登録する簡易で標準的な方法を持っておらず、その結果、強い*アイデンティティの無い認証*は難しい。ユーザが一つのアカウント用に既存の強力な認証方法を保有する場合（例えば、銀行）でも、このアカウントは、他のアカウント/提供者ではほとんど再利用されることはない。これは、利用者用の*アイデンティティ*が拡張性の限界を既に超えた状況をもたらした。61%以上の人がいつでも同じパスワードを使用している[189]；これは潜在的利用者の喪失を引き起こすあらゆる追加の規則や認証を生じさせる。

アプリケーションへのシームレスなアクセスに関するこの問題を解決することはビジネスを促進し、*アイデンティティ*と承認の明確な分離は更なる利用、例えば一人の個人が別な人の取引に代わり特定のクレジットカードに繋がる*ペルソナ*を使用する権限を与えること、を促進する。

12.16 アイデンティティサービス提供者

外部のサービスの*アイデンティティ*情報を利用すると、固有の問題が生じる。提供する組織での信頼レベルと*属性*確認は、まさにその 2 例である。包括的かつ一貫した*アイデンティティ*フレームワークのためのの提案や実際に提供されるものの多くは、他のコミュニティの要件の理解をほとんどあるいは全くすることなく、単独あるいはグループのプレーヤの要件を推定したものである。

ほとんどすべてのオープン/パブリックで使用可能な*アイデンティティ*サービスは、ユーザ検証を扱うだけである。これらの個人情報（*アイデンティティ同様属性*も）を提供するものは、自己主張、あるいは信頼できる出所からでない*属性*を使用しているかのいずれかである。

*アイデンティティ*と*属性*の出所の例は以下のとおりである:

- 政府
  - 米国の NSTIC (National Strategy for Trusted Identities in Cyberspace) ― 戦略と抱負
  - ドイツの“EID card”、オーストリアの“Citizen Card”、エストニアの “ID Card”、Finland の“Citizen Certificate”、香港の“Smart ID Card”、マレーシアの“MyKad”
- パブリック ― API を介した統合
  - Facebook
  - Amazon
  - Google
  - Microsoft Passport (Windows Live ID)
  - OpenID 提供者 (様々なもの)
  - Twitter
- ブリッジブリッジあるいはハブあるいはハブ

[189] http://www.guardian.co.uk/technology/2008/jan/17/security.banks

- REBCA[190] (Research and Education Bridge Certification Authority) －米国の高等教育セクターへサービスを提供
- 連邦政府 PKI アーキテクチャ（連邦政府ブリッジ）－連邦政府エージェンシすべてにサービスを提供
- CertiPath/Transglobal Secure Collaboration Program[191], 航空宇宙と防衛産業にサービスを提供
- SAFE-BioPharma Association[192], バイオ医薬品と保健医療産業にサービスを提供

- *アイデンティティ*サービスの提供物
  - 様々な郵便番号と住所の照合と有効性確認
  - Experian / Equifax
  - 3D カードの検証(Visa/MasterCard)
  - eBay / PayPal / X.Commerce

12.17 推奨事項

12.17.1 連携の推奨事項

- 利用者、実装者、そして提供者は、使用される連携の意味を定義し、同意すべきである。
- 実装者は、どのような信頼関係と推移的[193]信頼があるか、そして双方向の信頼関係の必要性を理解するべきである。
- 実装者は、可能な場合、オープンな標準、例えば SAML や OAuth に基づく連携を使用するべきである。
- 「ブリッジ」あるいは「連携ハブ」を使用する場合、実装者は参加メンバー間に存在する信頼の性質や関係を理解するべきである。クラウドに登録したり他のブリッジと連携する他のメンバーがいる場合、自分の権限付与ルールに対して何を意味するか理解する。
- 実装者は、Facebook、Yahoo あるいは Google 等のパブリックなアイデンティティ提供者が、（グレードの低い、通常は自身で主張する）アイデンティティの出所を他の提供者と将来連携する保証のないまま提供することを理解するべきである。
- 実装者は、クラウドソリューションのアクセス管理システムにリンクした DS から*アイデンティティ*を取得するという、未熟な設計ソリューション例を非難するべきである。このような例は、帯域内の VPN と帯域外専用線を含む。

12.17.2 プロビジョニングとガバナンスの推奨事項

- *属性*はすべて、できるだけ信頼のある/拠り所の近くから取得するべきである。

---

[190] www.hebca.org
[191] www.certipath.com / www.tscp.org/
[192] www.safe-biopharma.org/
[193]推移的：X=Y かつ Y=Z なら X=Z が成立する関係

- 原則として、クラウドサービスあるいはアプリケーション自体は、*アイデンティティ*の拠り所となることを避けるべきである。
- クラウドサービスあるいはアプリケーション自体は、自分が直接コントロールする*属性*の唯一の拠り所であるべきである。
- 利用される*属性*はすべて、既知の信頼レベルを持つべきである。
- 利用される*属性*はすべて、*アイデンティティ*とリンクするべきである。
- 定義済みの*エンティティ*の*識別子*は、利用されるすべての*属性*を署名するべきである。
- それぞれの*属性*は、目的に適合するライフサイクルを持つべきである。
- それぞれの*アイデンティティ*（そして関連する*識別子*）は、目的に適合するライフサイクルを保有するべきである。

12.17.3 権限付与の推奨事項

- 権限付与（定義）プロセスのすべての当事者は、明確に特定されるべきである。
- 権限付与ルールの承認とサインオフを明確に示す責任があるべきである。
- 権限付与ルールへの変更を管理するプロセスを明確に定義するべきである。
- 権限付与ルールを監査する頻度（あるいはきっかけ）を明確に定義するべきである。
- 権限付与プロセスは、分かり易く最低限の、さらに最小限の権限付与という原則を用いて設計した権限付与ルールを作成することに焦点をあてるべきである。
- 権限付与プロセスは*アイデンティティ*の露出を最少にする、あるいは*アイデンティティ*を全部利用する必要性を避ける権限付与ルールを作成することに焦点をあてるべきである。
- 一時的な*属性*（ユーザの位置情報等）は、トランザクションが存続する間、リアルタイムの*属性*確認をし、権限付与ルールを再確認する必要がある。
- 権限付与ルールは、プロセス（あるいはプロセス開始の試み、例えば外部からの送金等）を契機にするべきである。環境によっては、権限付与ルールでこのような機能を使用できなくすることがベストプラクティスとなる。別な環境では、実行時点で追加の*アイデンティティまたは属性*を要求することが、エンティティにプロセスを実行する資格を付与することを確実にするため、ベストプラクティスとなる。
- 実装者は、双方向の信頼確立を保証し、トランザクションに必要な最適で安全な関係を確実なものとするべきである。権限付与プロセスは、これを定義するべきである。
- 権限付与ルールの設計には、一次エンティティがアクセス可能な、一部の、ただし必ずしも全部ではない情報への二次*エンティティ*によるアクセス代行を含めるべきである。
- 権限付与ルールの設計者は、関係するシステム、組織、そしてエンティティの法域を考慮する必要があるが、権限付与の設計には、アクセス権の差し押さえ（法的な押収を含む）を含めるべきである。アクセス権の差し押さえを実装する前に、法的アドバイスに従わなくてはならない。

- 実践的な場合、管理用のインタフェース、ツール、その他の可視化技術は、権限付与の管理での支援に用い、その解釈がビジネスそして/または規制上の要求事項（例:SOX の職務分掌）を充足することを確実なものとするように用いるべきである。

12.17.4 承認とアクセスの推奨事項

- 実装者は、サービスが OASIS XACML 等の標準からインポートそして/または標準にエクスポートする機能を持つことを確実なものとするべきである。
- クラウド環境で PDP を使用する場合は、実装者は、どのように承認の決定の記録が抽出されるか、そして/またはアクセスの全体像の組織の記録と統合されるか理解するべきである。
- 実装者は、既存の（レガシーな）サービスが PEP/PDP とインタフェース可能なことを確実なものとするべきである。
- 実装者は、いかなる PDP も権限付与プロセスで定義された権限付与ルールを適正に解釈するに足ることを保証するべきである。
- 実装者は、中核となるポリシーサーバに対するニーズがある場合（例えば、クラウドマッシュアップ用）、”policy-as-a-service”の使用をポリシーサーバとして検討するべきである。

12.17.5 アーキテクチャの推奨事項

- 実装者は、あらゆるクラウド提供者が権限付与ルールで構成可能な承認管理 PEP/PDP を提供することを確実なものとするべきである。
- 実装者は、*アイデンティティ*、権限付与、そして承認/アクセス管理（IdEA）のあらゆるコンポーネントが共に正確に機能することを確実なものとするべきである。
- 実装者は、ポリシー決定/権限付与ポイント（PEP/PDP）が標準的プロトコル（XACML 等）を使用し、独自のプロトコル（ウェブサービスあるいは他のミドルウェアを直接コールする等）を避ける（あるいは減らす）ことを確実なものとするべきである。
- 実装者は、いかなる強い認証サービスも OATH 準拠であることを確実なものとするべきである。OATH[194] 準拠のソリューションでは、組織は特定ベンダの認証による資格証明にロックインすることを回避できる。
- クラウドサービスとアプリケーションは、SAML を用いる信用の置ける出所からの認証を利用する機能を支援するべきである。
- 実装者は、サービスに OASIS XACML 等の標準からインポート、そして/または標準にエクスポートする機能があることを確実なものとするべきである。
- 実装者は、クラウド基盤にインストールされている PEP/PDP と、そしてインシデントの監視/監査に必要なポリシー監視ポイントとインタフェース可能であることを保証するべきである。
- 実装者は、承認の決定と、実際のアクセス権の付与の承認が標準的で安全なプロトコルを用いて共通のフォーマットで記録可能であることを確実なものとするべきである。

[194] **OATH**- Open Authentication Reference Architecture, http://www.openauthentication.org/

12.17.6 権限付与の推奨事項

- 実装者は、権限付与プロセスで定義された*アイデンティティ*と*属性*がそれぞれ、*アイデンティティ*/*属性*の両方に必要とされる（あるいは受容可能な）信頼レベルに適合し、そしてそのレベルを提供する出所とも適合することを確実なものとするべきである。
- 実装者は、*アイデンティティ*/*属性*のすべての出所が組織の*アイデンティティ*を提供することを確実なものとするべきである。
- 実装者は、属性が可能な時はいつでも、あるいはできるだけ原本と確認していることを確実なものとするべきである。
- 実装者は、*属性の使用*が正しい結論に至ることを確実なものとするべきである（自分の解釈が*属性*の発信者と異なる可能性がある）。
- 実装者は、*アイデンティティ*/*属性*の出所に、自分の必要を満たすデータ品質とガバナンスの仕組みの両方の基準があることを確実なものとするべきである。
- 利用者は、評判が信頼の重要な出所であり得ることに気づくべきである。権限付与の定義を通じて、小さな価値のが変異が取引上の信頼を増すように誘導し、その後の高額取引で詐取される可能性があることに利用者は気づくべきである。

12.17.7 プロビジョニングの推奨事項

- 提供者は、SPML あるいは SCIM がプロビジョニングの実行可能な選択肢となるかどうかを理解するべきである。
- 実装者は、アカウントをプロビジョニングする際、最少特権の原理に従うべきである。コンピュータ装置等のエンティティの場合、組織の資産台帳にリンクしていることが望ましい。
- システムとアプリケーションの多くは、ユーザとアクセス権の 1 対 1 の関係を持ち、権限代行の考え方は持っていない。
- 実装者は、プロビジョニングとプロビジョニング解除がユーザのアイデンティティに制限されないことを確実なものとするべきである。アーキテクチャにはあらゆるエンティティタイプの承認が含まれていなければならない。
- 実装者は、プロビジョニングとプロビジョニング解除がリアルタイムで実行されることを確実なものとするべきである。
- 実装者は、権限付与を正確にするのに重要な*アイデンティティ*と*属性の両方の*維持を確実なものとするべきである。

12.17.8 アイデンティティのコンプライアンスと監査の推奨事項

- 実装者は、権限付与ルール/承認プロセスの正しいログを確実に利用できるようにすべきである。

- 実装者は、ログをもっと幅広い（おそらく遠隔の）システムに統合する必要がある場合（例えば、不正検出や職務分掌の分析）、可用性、適時性、フォーマット、そしてログの移送のセキュリティが適切であることを確実なものとするべきである。
- アクセス権の決定を記録する際、実装者は、*属性*を権限付与の決定時に使用されるロジックと一緒のグループにし、結果を記録することを確実なものとするべきである。
- クラウド関係者全員が、一時的な構成要素付きの*属性は、セッションの間*再度確認し、それにより再記録する必要があるかもしれないことを覚えておくべきである。
- PII あるいは SPI を記録する場合、可能な場合はいつも実装者はログ内の PII あるいは SPI の露出を最小限に留めるよう*属性*の派生物を使用するべきである。
- 利用者は、PII や SPI を含むログがデータ保護法令の対象となることに注意する必要がある。

12.17.9 アプリケーション設計の推奨事項

- 実装者は、隔離を確実にするためにユーザ、システム、およびマネジメント層の ITU X.805 /3 層の定義を使用すべきである。
- 実装者は、アプリケーション設計において*アイデンティティ*と*属性*の必要性を最小にするようにするべきである。
- 可能な場合、*アイデンティティ*と*属性*を外部の出所から利用するようにクラウドシステムを設計するべきである。
- 実装者は、クラウドシステムに標準の SSO 連携フォーマット、例えば SAML や OAuth を確実にサポートさせるべきである。
- 実装者は、システムのあらゆるレイヤにわたって*アイデンティティ*と*属性を用い*、セキュリティに対し全体的な取り組みを採用するべきである。
- まさにクラウド環境はエンティティと他のシステムが何者か認証する必要があり、代わりにクラウドシステムが認証できる必要があるので、実装者は、相互認証があらゆるレベルで重要であること、そしてクラウド環境ではさらに重要であることを覚えておくべきである。

12.17.10 データ保護の推奨事項

- 実装者は、PII あるいは SPI の使用と保存を最少にするべきである。プロセスに不可欠なアイデンティティと*属性*のみが使用されることを確実なものとするよう、権限付与の設計フェーズでこれをすべきである。
- 実装者は、PII あるいは SPI の露出を最少にするよう以下の技術を検討するべきである:
  - 暗号化
  - トークン化

- 準同型暗号[195]

詳細については 11 章 「暗号化と鍵管理」 を参照。

- 実装者は、SPI を保護するベストプラクティスである方法、例えば一方は対象者が持ち（ログイン時に入力する）、他方は処理に使用するためにシステムが持つ、デュアルキーアプローチの使用を検討するべきである。
- 実装者は、管理者が、制限されていたり停止しているかもしれない PII と SPI に、どのようにアクセスするか理解するべきである。
- 実装者は、　特に要求を受けた組織が所有・管理していないクラウドシステムにデータが保持されるかも知れない場合に、命令された法的時間枠内で「情報主体者のアクセス要求」[196]にどのように対処できるか、理解するべきである。
- PII あるいは SPI を共有する必要がある場合、利用者は PII/SPI の主体者の承認がどのように取得されるかを理解するべきである。
- 実装者は、特に信頼できる出所でない場合、PII/SPI を保存することを減らし、またそれらを保存（そして維持）するよりも信頼できる出所に由来する属性だけを参照するようにするべきである。
- 実装者は、（*アイデンティティ*であれ*属性*であれ）PII/SPI のメンテナンスが適時に処理されていることで、プロセスを理解するべきである。

12.17.11 アイデンティティ実装の推奨事項

- 実装者は、新しいユーザそして/あるいはデバイスの一意の登録よりも*アイデンティティ*再利用の原則から開始すべきである。
- 利用者は、どこで既存の*アイデンティティ*の出所が十分な信頼レベルを提供し再利用できるかを理解すべきである。
- 提供者は、開始されたトランザクションに必要な信頼レベルに対し、ユーザとデバイスに関してどんな属性を主張できるか理解すべきである。
- 適切であれば、利用者は、低いレベルの認証グレードを使用するリスクの低いトランザクションが生じることを容認すべきである。トランザクションの価値/リスクが増える場合にのみ、必要とされる*アイデンティティ*を拡大させよ。
- 提供者は、利用者とそのデバイスを考慮する際、権限付与プロセスの間に必要な*アイデンティティ*と*属性の批判的評価*を提供するべきである。
- 提供者は、保証レベルを向上させるためにどの技術が利用者のデバイスで使用することができるか、バックグラウンドで使えることができることよりも、特に技術を理解すべきである。
- 利用者は、利用者のデバイスの管理がどこで実施されないか理解すべきであり、保証のレベルは提供されるが；これには無保証から良い保証まで幅があり得る。

[195] At the time of release, Homomorphic Encryption is currently in the early stages of product implementation.
[196] A “Subject Access Request” is the legal right in some countries to request any PII or SPI held about yourself

- 利用者は、どこに保証のレベルと法的責任があるか、問題が利用者のデバイスからのトランザクションで生じることを理解すべきである。

12.18 要求事項

- ✓ 実装者は、既存の情報セキュリティのポリシーと手続きを犠牲にすることなくアプリケーションの自己中心的なやりかた(サイロ)を取り除けるよう、独立して活動するために共通のサービスレイヤを設計しなければならない。
- ✓ すべてのクラウド関係者はサプライチェーンの完全性を尊重し、既存の IAM の慣行を尊重しなければならない。プライバシー、完全性、監査能力等の要素は尊重されなければならない。*アイデンティティ*の完全性と監査は、データが外部に移動する場合に、そして/あるいはソリューションの柱を分離しウェブサービスに変える場合にも保持されなければならない。

第 13 章 //
仮想化

仮想化は Infrastructure as a Service (IaaS)クラウドおよびプライベートクラウドの主要要素の一つであり、Platform as a Service (PaaS)や SaaS (Software as a Service)プロバイダのバックエンドの一部としても使われている。仮想化は当然ながらプライベートおよびパブリッククラウドで提供される仮想デスクトップの主要技術でもある。

仮想化による恩恵には、マルチテナント性、より良いサーバ利用率、データセンタの統合がよく知られている。クラウドプロバイダは利益を生み出すための高密度化を達成することができ、利用企業はオペレーションの効率化ばかりでなくサーバハードウェアの設備投資を小さくするために仮想化を利用することができる。

しかしながら仮想化は、ゲストとして実行されている OS 自体のセキュリティ問題ばかりでなく、ハイパーバイザーレイヤの新しいセキュリティの問題、仮想化特有の新しい脅威としての VM(仮想マシン)間の攻撃や今まで気がつかなった盲点、セキュリティに使われる CPU やメモリから引き起こされるパフォーマンス問題、セキュリティを抑制する VM スプロール[197]の管理の困難さを持ち込むことになる。Instant-on gaps[198]、データ混合、仮想マシンイメージを暗号化する困難さ、未解決のデータ破棄などの新しい問題にフォーカスを当てる。

概要. 仮想化にはいくつかの形態があるが最も一般的なのはオペレーティングシステムの仮想化であり、本章ではそれにフォーカスを当てる。この章は下記の仮想化に関するセキュリティ問題を扱う。

- 仮想マシン上のゲストの強化
- ハイパーバイザーセキュリティ
- VM 間の攻撃や死角
- パフォーマンス問題
- VM スプロールに由来する管理の困難さ
- Instant-on gaps
- 仮想マシンの暗号化
- データの混合
- 仮想マシンのデータ廃棄
- 仮想マシンイメージの改ざん
- 移動 VM の問題

仮想化は、ゲスト OS によってもたらされるセキュリティの懸念と新しい仮想化特有の脅威を併せ持っている。

[197] VM スプロール - いつのまにか仮想マシンが増えてハードウェアのリソースを食いつぶしてしまう現象
[198] Instant-on gaps -古い仮想マシンイメージが復帰後に瞬時に危険にさらされる脅威

13.1 ハイバーバイザーアーキテクチャの問題

13.1.1 VM ゲストの強化

ファイアウォール、HIPS、ウェッブアプリケーションプロテクション、アンチウィルス、ファイルの完全性モニタリング、ログモニタリングによる仮想マシンインスタンスの適切な強化や保護は、各ゲストのソフトウェアを通して、あるいはハイバーバイザーベースの **API's**[199]によって統合されたインライン仮想マシンを使うことによって提供される。

13.1.2 ハイパーバイザーのセキュリティ

ハイバーバイザーはベストプラックティスに基づいて、ロックダウンあるいは強化される必要がある。利用企業や仮想化ユーザの主な懸念は、ハイパーバイザーをホスティングしているサーバの物理セキュリティだけでなく、構成管理やオペレーション管理が適切なことである。

13.1.3 VM 間の攻撃や盲点

仮想化はネットワークセキュリティに大きな影響を与える。仮想マシンはネットワークを通してではなくハードウェアバックプレーンを通して相互に通信するかもしれない。この結果として標準のネットワークベースセキュリティコントロールがトラフィックを監視することができず、モニタリングやインラインブロッキングを行うことが出来ない。この問題に対する一つのアプローチはハイパーバイザーと仮想化管理フレームワークの API レベル統合を要求するハードウェアアシストの仮想化を使うことであり、インライン仮想アプライアンスもこの問題の解決を助ける。仮想マシンのマイグレーションもまた問題を含む。攻撃者のシナリオとして悪意のある VM をトラストゾーンに送り込むことや、既存のネットワークベースセキュリティコントロールに対して不正行為を検出されないようにすることである。個々の仮想マシンにセキュリティツールフルセット一式をインストールすることはプロテクションレイヤを一つ加えるアプローチである。

13.1.4 パフォーマンス問題

物理サーバ用にデザインされたセキュリティソフトウェアを仮想化されたサーバにインストールすることは、幾つかのアンチウィルススキャナが CPU インセンティブであることから明らかなように、パフォーマンスの深刻な低下をもたらすことがある。つまり、仮想化されたサーバの共有環境はリソース競争を引き起こす。特に、仮想化デスクトップやサーバの高密度環境ではセキュリティソフトウェアが仮想化を認識する必要性、あるいは他の仮想マシンを維持するためにシングル仮想マシン上でセキュリティ機能を実行する必要性がある。

13.1.5 VM スプロールによる操作の困難性

VM のプロビジョンが簡単であることは、典型的な企業において VM のリクエストの増加を招く。これは攻撃面が拡大するばかりなく、セキュリティホールを作ってしまうオペレータエラーや設定間違いを増やすことになる。このため、ポリシーベース管理や仮想化管理フレームワークの利用が不可欠である。

[199] **API** - Application Program Interface

13.1.6 Instant-On Gaps

仮想マシンのストップとスタートが簡単にできることは、脅威の変化速度と密接な関係があり、仮想マシンが停止した時には仮想マシンは安全な構成であるかもしれないが、仮想マシンが再スタートした時には脅威が展開されて、仮想マシンは脆弱なまま残される状態を引き起こすこともある。ベストプラクティスは新規にプロビジョニングする前、あるいは新規にスタートする VM の前に既知の攻撃に対する調査を行うネットワークベースセキュリティあるいは「バーチャルパッチ」を当てることである。ルールファイルやパターンファイルが更新されるまで古くなった VM を隔離し、更新後にウィルススキャンを実行するような **NAC**[200] (ネットワークアクセスコントロール)的な機能を強制することも可能である。

13.1.7 仮想マシンの暗号化

仮想マシンが停止中や稼働中は、そのイメージが盗難や改ざんされることに対して脆弱である。この問題に対する解決策は常時仮想マシンイメージを暗号化することであるが、同時にパフォーマンス問題も引き起こす。ただし、高度なセキュリティを要求される場合や規制された環境では、パフォーマンスコストを掛けることに見合う価値がある。暗号化は、攻撃者が VM のスナップショットデータにアクセスを許すこと、つまり「野生に逃げる」“escaping into the wild,”ような走行中の VM スナップショットを禁止する運営管理、DLP、追跡記録と共に使われなければならない。

13.1.8 データの混合

異なるデータのクラス(あるいは異なるデータのクラスをホストする VM)が同じ物理マシンに混ざる問題がある。**PCI**[201]の用語ではこれを混合モード配置と呼ぶ。混合モード配置を使うためのメカニズムとしては、VM 隔離を確実にするために VLAN、ファイアウォール、**IDS/IPS**[202]の統合活用を推奨する。また、データのカテゴリ化およびポリシーベース管理(すなわち DLP)の活用を推奨する。クラウドコンピューティング環境においては、マルチテナント仮想環境上の全てのテナントが潜在的に最低限共通のセキュリティ基準を共有することなる。

13.1.9 仮想マシンのデータ廃棄

仮想マシンがある物理サーバから別の物理サーバに移動する場合、あるいはディスクがプロビジョニングを解除された場合、別のユーザがデータを回収してしまうかもしれないため、企業はデータがディスクに残っていないことの証明が必要となる。メモリやストレージをゼロクリアすること、あるいは全てのデータを暗号化することがこの問題への解決法である。暗号鍵は仮想環境から独立したポリシーベース鍵サーバに預けるべきである。加えて、VM が実行中にマイグレートする場合、暗号化や適切なデータ消去がなければマイグレーション中に危険にさらされる恐れがある。

13.1.10 仮想マシンイメージの改ざん

事前設定された仮想アプライアンスや仮想マシンイメージは設定間違いを含んでいるかもしれない、あるいは実行前に改ざんされているかもしれない。

---

[200] **NAC** - Network Access Control
[201] **PCI** - Payment Card Industry
[202] **IDS** - Intrusion Detection Systems; **IPS**- Intrusion Prevention Systems

13.1.11 移動 VM の問題

ある物理サーバから他の物理サーバに仮想マシンを移す機能は、管理やセキュリティモニタリングの困難さを発生させる。多くのケースでは、警告や追跡可能な記録を行わず仮想マシンを(地理的な場所に関わらず)別の物理サーバに移すことが可能になってしまう。

13.2 推奨事項

- 可能ならば利用者はクラウドプロバイダで使われている仮想化のタイプを識別すべきである。
- 実装者は製品環境をテスト/開発や重要なデータ/ワークロードから分離するゾーン化アプローチを考慮すべきである。
- 実装者は性能が大きく変わることがあるため、仮想マシンセキュリティツールのテストやインストール時にパフォーマンスを考慮すべきである。また、仮想化を認識したサーバやネットワークセキュリティツールも考慮する必要がある。
- 利用者は主要ベンダと仮想化された環境についてのライセンスアグリーメントの評価、交渉、改善をすべきである。
- 実装者はゲストインスタンス内の強化ソフトウェアを使って仮想化された OS をセキュアにするべきである。あるいはハイパーバイザーベース **API**[203]で統合されたインライン仮想マシンを使うべきである。
- 仮想化されたオペレーティングシステムは、階層化されたセキュリティコントロールを提供し、且つプラットフォームプロバイダの依存度を減少させるため、サードパーティのセキュリティ技術を活用したビルトイン可能なセキュリティ手段によって増補されるべきである。
- 実装者はデフォルトの設定のセキュリティが利用可能な業界基準に準拠する、あるいは上回ることを保証しなければならない。
- 仮想マシンイメージが使われない時には実装者は暗号化を施さなければならない。
- 実装者は利用タイプ(例えばデスクトップ 対サーバ)、生産の段階(例えば開発、本番、テスト)、サーバやストレージなど分離可能な物理ハードウェア上でのデータの重要度により、VM の分離とセキュリティゾーンの生成についてその有効性と実現可能性があること調査しなければならない。
- 実装者は脆弱性評価ツールやサービスが仮想化技術に適用できることを確認すべきである。
- 実装者は、仮想マシンと実行環境間におけるデータ分類とコントロールを増強するために、全組織的にデータの自動発見やラベリングによる解決手法(例えば DLP)を導入することを考慮すべきである。
- 実装者は、パッチが当てられていない仮想マシンがある場合、仮想マシンイメージを停止してパッチを当てることや新規の仮想マシンが実行されるのを取りやめることを考慮するべきである。
- 実装者は、管理者のインタフェース(Web ベース、API、など)がカスタマーに見えてしまうことを防ぐため、どのセキュリティコントロールが VM の外部に配置されているかを理解すべきである。

13.3 要求事項

[203] **API** - Application Program Interface

- ✓ VM バックプレーン間で粒度の細かいトラフィックモニタを提供するために、ハイパーバイザーの API に組み込まれている VM 特有のセキュリティメカニズムを活用すべきである。
- ✓ 仮想化に対する新しいセキュリティ課題に対応するために、実装者はセキュリティポリシーを更新しなければならない。
- ✓ 実装者は、暗号鍵を保存するポリシーベース鍵サーバを使って他の仮想マシンからアクセスされるかもしれないデータを暗号化しなければならない。
- ✓ 利用者は、規制当局により分離が要求される場合、自分の VM あるマルチテナント性の状態を理解しなければならない。
- ✓ 利用者は、サードパーティから提供される VM イメージやテンプレートの由来と完全性を確認しなければならない。よりよい手法としては自分の VM インスタンスは自分で作ることである。
- ✓ 仮想化されたオペレーティングシステムはファイアウォール(内向きと外向き)、ホストベース侵入防御システム(**HIPS**)[204]、ネットワークベース侵入防御システム(**NIPS**)[205]、Web アプリケーションプロテクション機構、アンチウィルス、ファイル完全性モニタ、ログモニタなどを含めなければならない。セキュリティの防御対策は各ゲスト仮想マシンインスタンスにソフトウェアとして配ること、あるいはハイパーバイザーベースの API を使ったインライン仮想マシンを通して配ることができる。
- ✓ プロバイダは VM イメージを削除、あるいは整理する際にバックアックや障害回避システムにおいても該当データを削除しなければならない。
- ✓ プロバイダは隔離されていることを示すエビデンスを提供し、分離違反があった場合にアラートを発行する報告メカニズムを持たなければならない。

[204] **HIPS** - Host Intrusion Prevention System
[205] **NIPS** - Network Intrusion Prevention System

第 14 章 //
Security as a Service

クラウドコンピューティングは、これまでに業界が経験してきた情報技術の最も重大な変革のひとつである。情報処理機能をユーティリティとして提供することを可能にしたことは、今後も発展するイノベーションを約束する大きな潜在的可能性がある。セキュリティ業界は、提供者と利用者の双方に標準化されたセキュリティフレームワークがもたらす効果をこれまで認識してきた。提供者と利用者の間のクラウドサービスレベルアグリーメントの置かれている状況は、標準化されたセキュリティフレームワークを文書という形で、セキュリティサービスを提供する方法と箇所を定義する方法を用いている。標準のフレームワークに基づいてセキュリティの提供を受けることが成熟するに従い、クラウド利用者はプロバイダと利用者のための情報処理資源を集中させる必要があることを認識してきた。ビジネス遂行の基盤としてのクラウドの成熟度のマイルストーンの 1 つは、SecaaS (Security as a Service)をグローバルな規模で採用し、どうすればセキュリティをさらに優れたものにできるかを認識することである。アウトソーシングの商品としてセキュリティを世界規模で導入することは、事実上、共通点のない部分とセキュリティが適用されていない部分をできるだけ少なくすることである。

SecaaS は、企業のセキュリティをクラウドの視点から対応することであり、この点がクラウドセキュリティに関わる他の作業や研究の多くと異なる点である。クラウドセキュリティに関わる議論の大部分は、いかにクラウドに移行するかの方法、そして、クラウドを利用した場合に機密性・完全性・可用性・位置をいかに確実に維持するかの方法を取り上げたものである。SecaaS は、クラウド基盤上のサービスを経由したハイブリッドと従来型の企業ネットワークだけでなく、クラウドのシステムとデータを安全なものとするかを別な視点からとらえている。これらのシステムはクラウドに設置されるか、あるいは利用者の施設内に古い従来のやり方で設置される。例えば、ホスト上のスパムと AV（アンチウィルス）のフィルタリング機能である。

概要. この章では、以下のトピックを取り上げている:

- 市場における Security as a Service の偏在性
- Security as a Service を導入した場合の懸念事項
- Security as a Service 導入の優位性
- Security as a Service のカテゴリに入る多様なサービス

この文書は CSA のクラウドコントロールマトリクスと同様、Security as a Service の発行物と対応している。

14.1 Security as a Service の偏在性

利用者にとって、クラウドコンピューティングの前途は関心が高いが不安なものでもある。関心が高い理由は、資本支出を抑え、インフラストラクチャの管理を不要にし、コアコンピテンシーに集中する機会をもたらしてくれるからである。とりわけ、オンデマンドのプロビジョニングでコンピュータ資源の提供を受けることからもたらされる敏速性と、情報技術を経営戦略と要求にすぐに整合させることが可能なことである。しかし、利用者が懸念することは、クラウドコンピューティングのセキュリティ上のリスクや、システムのセキュリティに対する直接的なコントロールをなくすことで責任を果たせなくなるのではないか、ということである。ベンダは、クラウドプラットフォーム上にセキュリティサービスを提供することによってセキュリティに対する要求を満足させようとしてきたが、そのサービスに様々な形があり、導入されたセキュリティコントロールが不透明なことによって市場に混乱をもたらし選択プロセスを複雑にしてきた。そして、これまでクラウドベース

のセキュリティサービスの採用を限られたものにしてきた。ガートナーによれば、Security as a Service は急激に増加すると予測されており、クラウドベースの Security as a Service は 2013 年までに多くのセグメントで 3 倍以上に伸びるとされている。

非常に多くのセキュリティベンダが、現在、クラウドベースのモデルを用いたセキュリティソリューションを提供している。この移行は複数の理由から生じたが、それには規模の経済の大規模化と効率的なサービス提供の仕組みが含まれている。利用者は、オンプレミス上ではないセキュリティソリューションを評価する状況にますます直面する。利用者は、クラウドが提供するセキュリティの中身の独自で多様で広範囲に広まる性質を理解することが必要であり、その結果、その中身を評価しそれが要求を満たしているかどうかを理解しなければならない立場になる。

14.2 Security as a Service を導入した場合の懸念事項

クラウドのセキュリティサービスからもたらされる素晴らしい数々の利点、例えば、動的な拡張性、事実上限界のないリソース、コストの安いあるいはコストのかからないより大きな規模の経済性があるにも関わらず、クラウド環境にはセキュリティに関わる懸念が存在している。セキュリティ上の懸念の一部は、コンプライアンス、マルチテナント性、ベンダロックインに関わるものである。これらは、セキュリティをクラウドに移すことへの阻害要因として取り上げられるが、同じ懸念はこれまでのデータセンタにも存在している。

クラウド環境のセキュリティは、導入されたセキュリティコントロールの可視性に欠けること、つまり、これまでのデータセンタと同じくシステムが守られていないのではないか、また、適格な資格の付与や身元の確認が不足しているのではないかという懸念に基づいている。Security as a Service プロバイダは、関係が希薄なことを認識し、可能な限り利用者の環境を守ることを極端に保証するようにしている。プロバイダは、個人の身元確認をよく実行し、最も頑強な政府の身元確認とさえ競争し、それを実行する。物理的なセキュリティと個人ベースのセキュリティは、Security as a Service プロバイダの最も高い優先度の 1 つである。

コンプライアンスは、グローバルな規制環境に提示された懸念として取り上げられてきた。Security as a Service プロバイダもこの懸念を認識し、大きな努力を払い、要求を満たせるだけでなく要求以上に持っている能力を示す、あるいはクライアントのネットワークと統合できることを保証してきた。Security as a Service プロバイダは、サービスと利用者に影響する広域的な規制や一部地域の規制も認識しなければならないだけでなく、提供物やサービスの導入に組み込むことも可能でなければならない。最も慎重な Security as a Service プロバイダは、仲介サービスや法的サービスの支援を受け、利用者に必要な司法機関の地域的な規制要求を優先的に解決している。非常に規制された業界や環境に Security as a Service を導入する場合、規制の目標を達成するために必要とされるサービスレベルを定義したメトリクスへの同意を、サービスを定義している SLA と並行し交渉するようにすべきである。

どんなクラウドサービスでもそうであるが、マルチテナント性は仮想インスタンス間にデータ漏えいがないかという懸念がある。利用者がこのことに懸念を懐く一方で、Security as a Service プロバイダも最新のビジネスが訴訟沙汰にならないか極度に心配している。結果的に、よく検討されたサービスでは意味のある予防措置を採用することで、データを互いにまったく影響しないように区画し、そして共有されるデータはすべて匿名にし、データの持ち主やデータそのものを保護する。つまり、このサービスを、SecaaS プロバイダにより継続して監視されるデータ、および、監視対象（クラウドと非クラウドの両方）の利用者システムのログや監査データのような保持しているデータの両方に適用する。

マルチテナント環境の訴訟問題に対し、セマンティック処理と結び付けた分析を増やす別な対応がある。リソース記述子や応用計量法学、すなわち、法的根拠を高水準の考え方としてとらえ、コンピュータで読めるファーマットで表現し、共有されているリソースに法的なあいまいさがないかを積極的に解決しようとしている。

Security as a Service のベンダを使用すると、企業はセキュリティログ、コンプライアンス、報告の一部あるいはすべてをプロバイダ固有の標準に留まる可能性がある管理のもとに置くことになる。結果的に、企業が新たなプロバイダを求めた場合、順序正しく移行できるかどうか、また、既存のデータやログファイルを適正に解釈できるかどうかに懸念を懐き、法的に立証可能な方法を見出さなければならない。

特筆すべき重要なことは、マルチテナント性でなくとも、これらの懸念事項の一つ一つは「クラウドに特有」なものではなく、自営のモデルやアウトソーシングモデルの両方が直面する問題であることである。このため、クラウドセキュリティアライアンスのクラウドコントロールマトリックスで提案されているような非独占的な統合されたセキュリティコントロールを提示することによって、Security as a Service の環境から企業やベンダが効果を得やすくすることを支援する必要がある。

14.3 Security as a Service を導入した場合の優位性

一元管理されたセキュリティサービスを利用することの潜在的な戦略的効果は、日常において効率性が生み出されていることを経験している専門家がよく理解している。クラウドコンピューティングが、プロバイダと利用者の双方に優れた効果を多数提示しているのと同じく、Security as a Service は極めて重要な多くの効果を提示しているが、その効果はいくつもの要因、例えば、知識の集積、行動に移せる専門的知識から構成され、そして、常時身近にいるが一部しか名前が知られていないセキュリティの専門家による全面的な支援を得られていることである。セキュリティのベストプラクティスを集中化し標準化することに積極的に関わっている企業は、通常、中長期の著しいコスト節約や市場で競合他社をしのぐ競争上の効果を獲得するが、これは効率性から得られるものである。サービスとして提供されるセキュリティは、そのサービスのユーザが唯一のセキュリティ標準によってベンダをそれぞれ測定することを可能にし、その結果、ユーザは提供されているサービスをよりよく理解することができる。

14.3.1 1 競争上の優位性

サードパーティのセキュリティサービスプロバイダを採用する企業は、同業他社を超える競争力を獲得できるが、それは、現行の IT 戦略のリスク上の問題を理解することに役立つ情報を早くから知ることができるからである。さらに、セキュリティ基盤を集中させることによって、利用者は不要なもの取り除くことができるようになる。サードパーティを使用して、法規制の順守について報告し、義務である条項、例えば、個人識別票やデータと結びついた法的義務や契約上の義務を継承した場合、競合他社が被りやすい高い訴訟費用や罰金を避けることができるかもしれない。いったん全体的なセキュリティサービスを採用し導入すると、提供者は競争上の効果を上げ、セキュリティのベストプラクティスを満たしていると利用者を安心させることができる。このようなサービスを使用する利用者が獲得する優位性は、自社のコンプライアンスのフレームワークの一部としてセキュリティプロバイダや、サービスレベルアグリーメントに基づく義務を達成していることを証明するサードパーティの保証のあるプロバイダを指名することができる。

14.3.2 ベンダと利用者との関係改善

Security as a Service には、多くの非常に明確な効果がある。サードパーティの保証するサービスによって提供される透明性によって、利用者は得ようとしているベンダのサービスを容易に比較することが可能になり、また、ベンダと明確で合意している標準に従っていることを理解することが可能になる。移行サービスでは、あるベンダから別のベンダへデータとサービスを移行させることができる。移行サービスを活用することによって、利用者とプロバイダは、第三のサプライヤに市場の圧力を及ぼし、サービスを消費する企業に役立つ価値を向上させ、サプライチェーンを安全なものにすることができるようになる。

14.4 既存の Security as a Service が提供する多様なサービス

Security as a Service は、セキュリティマネジメントのアウトソーシングモデル以上のものである。すなわち、ビジネスの弾力性や継続性を確保する上で欠かせない構成要素である。ビジネスの弾力性コントロールとして、Security as a Service は数多くの効果を提示している。クラウドを介して提供されるしなやかなモデルによって、利用者は要求される金額、例えば、保護しなければならない端末の数に対する金額を支払うだけでよく、基盤をサポートし多様なセキュリティサービスを支援する要員には支払う必要がない。セキュリティに特化したプロバイダは、組織で通常利用可能なサービスよりもっと優れた専門的セキュリティサービスを提示している。最後に、ログ管理のようなアウトソーシングの管理業務は、時間と費用を節約し、組織が経営資源をコアコンピテンシーにもっと集中することを可能にする。

ガートナーの予測によれば、2013 年までに、メッセージ処理アプリケーション、例えばアンチマルウェアやアンチスパム用プログラムによるクラウドベースのセキュリティコントロールによって、この業界の 60 パーセントの収入が稼ぎ出される。

クラウドの Security as a Service によって利用者とセキュリティ専門家の関心を最も引きつける可能性のある分野は、以下のとおりである:

- アイデンティティサービスとアクセス管理サービス
- 情報漏洩防止(DLP)
- ウェブセキュリティ
- 電子メールのセキュリティ
- セキュリティ評価
- 不正侵入の管理、検知、防止（不正侵入検知システム(IDS)/不正侵入防止システム(IPS)）
- Security Information and Event Management (SIEM)
- 暗号化
- 事業継続性と災害復旧
- ネットワークセキュリティ

14.4.1 アイデンティティ、権限付与、アクセス管理サービス

Identity-as-a-service は汎用的な用語であるが、１つあるいは多数のサービスがあり、例えば、ポリシー強制ポイント（PEP-as-a-service）[206]、ポリシー決定ポイント（PDP-as-a-service）[207]、ポリシーアクセスポイント（PAP-as-a-service）[208]等のアイデンティティを関連のサービス、アイデンティティのあるエンティティを特定するサービス、属性を付与するサービス、安心という評判を提供するサービスが含まれている。

[206] **PEP** - Policy Enforcement Points: ポリシー強制ポイント (XML 用語)
[207] **PDP** - Policy Decision Points: ポリシー決定ポイント(XML 用語)
[208] **PAP** - Policy Access Points: ポリシーアクセスポイント(XML 用語)

これらのアイデンティティサービスはすべて、スタンドアロンの単独なサービスとして、複数の提供者のサービスをミックスし適合させるサービスとして、あるいは今日では最も可能性の高いパブリックとプライベート、従来型の IAM[209]、そしてクラウドサービスのハイブリッドソリューションとして提供可能である。

これらのアイデンティティサービスは、アイデンティティ、アクセス、特権の管理に必要なコントロールを供給しなければならない。アイデンティティサービスには、人、プロセス、システムを含み、経営資源へのアクセスを管理することに使用するが、そのためエンティティのアイデンティティを確実に検証することを保証し、次いでその保証済みのアイデンティティに基づいて適正なアクセスレベルの権限を与えなければならない。認証やアクセスの試みがうまく行ったか行かなかったかの動きを記録した監査ログは、アプリケーション/ソリューション、あるいは Security Information and Event Management（SIEM）サービスによって管理されなければならない。アイデンティティ、権限付与、アクセス管理サービスは、防御と予防の技術的なコントロールである。

14.4.2 情報漏洩防止

クラウドおよびオンプレミスの両方で休眠中、更新中、使用中のデータを監視し、保護し、そして保護の状況を示す場合、情報漏洩防止（DLP）サービスではデスクトップ/サーバ上でクライアントとして動作し、特定のデータの中身に対する動作の承認に関わるポリシーを強制することよって、通常、データの保護を実行している。これらは「ftp 禁止」あるいは「ウェブサイトへのアップロード禁止」のような幅広いルールとは異なり、データのレベル、例えば、ユーザはクレジットカードと思われる数字の入った文書は電子メールで送れないように定義する、また USB メモリに保存したデータはすべて自動的に暗号化し別な拠点が所有するコンピュータ上で適正にインストールされた DLP クライアント上で平文に戻すことができる、さらに動いている DLP ソフトウェアを用いたクライアントだけがファイルサーバのファイルを開くことができることである。クラウドの内部では、DLP サービスは、クライアントのために組立てられたサーバすべてが一連の合意済みの展開ルールと共に DLP ソフトウェアを取得するように、ビルドの一部として提供される代物である。さらに、DLP は集中 ID、あるいはクラウドブローカを活用し使用プロファイルを強制することもできる。サービスを活用しクラウドサービスのサプライチェーン上のある企業から様々な層へのデータの流れを監視しコントロールする能力を、PII[210]のような規制されたデータの越境伝送、それに続く喪失を予防しコントロールするために使用することができる。この DLP は予防的な技術的コントロールである。

14.4.3 ウェブセキュリティ

ウェブセキュリティは、自営でソフトウェア/装置を備えるか、あるいはクラウドを介してウェブトラフィックをプロキシサーバあるいはクラウドプロバイダにリダイレクトすることによって提供されるリアルタイムの防御サービスである。このサービスは、他の防御、例えば、ウェブを閲覧することでマルウェアが企業に侵入することから防御するアンチマルウェアソフトウェアのように、他の防御の最上のレイヤに防御機能を追加して提供される。アプリケーションの承認管理を使用し、もっときめの細かな、そして状況に応じたウェブアプリケーションに対する特別なレベルのセキュリティの強制を行うことができる。ウェブセキュリティは、防御的、発見的、そして反応的な技術的コントロールである。

14.4.4 電子メールのセキュリティ

電子メールのセキュリティは、インバウンドとアウトバウンド双方の電子メールに関わるコントロール、フィッシング、悪意のある添付、企業のポリシーを強制すること、例えば許容可能な使用やスパム防止の変更、そ

[209] **IAM** - Identity and Access Management: 個人認証とアクセス管理
[210] **PII**-Personally Identifiable Information　個人を特定可能な情報

して事業継続性の選択肢を提供しなければならない。さらに、ソリューションとして様々な電子メールサーバだけでなく、電子メールのポリシーに基づいた暗号化も可能なソリューションでなければならない。識別と否認防止が可能なデジタル署名も、多数の電子メールのセキュリティソリューションの機能である。電子メールのセキュリティは、防御的、発見的、そして反応的な技術的コントロールである。

14.4.5 セキュリティ評価

セキュリティ評価は、サードパーティあるいは利用者が主導するクラウドサービスの監査、あるいはオンプレミスシステムをクラウドが業界標準に基づいて提供するソリューションを介して評価を提供することである。基盤、アプリケーション、そしてコンプライアンス監査の従来のセキュリティ評価は、NIST、ISO、**CIS**[211]のような複数の標準によって適切に定義され支援されている。かなり成熟したツールセットが存在し、多くのツールが SecaaS 提供モデルを使用し導入されてきている。SecaaS 提供モデルでは、購読者はクラウドコンピューティングの可変部分、例えば、弾力性、準備時間を無視可能なこと、管理に要する時間が少ないこと、初期投資の少ない従量制という典型的な効果を取得する。

この作業に集中しないが、これらのツールをクラウド環境を監査するために使用する場合、さらにチャレンジが必要となる。以下のような、この追加のチャレンジを企業が理解することを支援するために必要なガイドラインを、CSA を含む、複数の組織が作成を継続している:

- IaaS の基盤監査を実施する際によく必要になる、ツールの仮想化を認識すること
- PaaS アプリケーションでは共通のウェブフレームワークを支援すること
- IaaS、PaaS、SaaS の基盤に対するコンプライアンスコントロール
- クラウドのサプライチェーンの一貫性を維持するためのインシデントと違反の自動通知ツール
- 以下の質問を対象として支援する XaaS 環境に対する標準質問項目:
  - クラウド環境では何をテストしなければならないか？
  - マルチテナント環境でデータの分離がどのように保証されているか？
  - 基盤の脆弱性に関する通常の報告書には何を記載すべきか？
  - クラウドプロバイダから提供を受ける結果を使用することは受容可能か？

14.4.6 不正侵入の検知/防止（不正侵入検知(IDS)/防止システム(IPS)）

不正侵入検知/防止システムは、ルールベース、発見的、行動モデルを用いて企業にリスクを示す行動上の異常を検出するための行動パターンを監視する。ネットワークの不正侵入検知/防止システムは、これまで 10 年以上にわたって広く使用されてきたが、それは企業ネットワーク内で何が起きているかの細かな見方を提供してきたからである。不正侵入検知/防止システムは、ネットワークトラフィックを監視し、ルールベースのエンジンあるいは統計的分析から得られたベースラインと行動を比較する。不正侵入検知システムは、通常、パッシブモードで導入され、利用者のネットワークの重要なセグメントを受動的に監視するが、不正侵入防止システムは利用者ネットワークの防御に当たる能動的な役割を担って配置される。従来型の基盤では、このクラウドは非武装地帯(**DMZ**)[212]に含まれ、ファイアウォールあるいはルーターで分割された箇所に企業のウェブサーバが

[211] **CIS**-Center for Internet Security　インターネットセキュリティのためのセンター
[212] **DMZ**-De-Militarized Zone　非武装地帯

配置され内部のデータベースへの接続を監視している。クラウド内部では、不正侵入検知システムが仮想基盤とハイパーバイザーに共通の活動を集中し監視しているが、そこは連携した攻撃によってマルチテナントを破壊しシステムに混乱をもたらす箇所である。不正侵入検知システムは、検知型の技術的コントロールであり、不正侵入防止システムは、発見的、防御的、そして反応的な技術的コントロールである。

14.4.7 Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM)システムは、（プッシュとプルの仕組みを用いて）ログとイベントデータを仮想およびリアルのネットワーク、アプリケーション、システムから集めている。この情報は、その後、相互に関係づけて分析し、介入やその他の対応を必要とする可能性のある情報あるいはイベントの報告と警告をリアルタイムに提供する。このログは、通常、改ざんできないような方法で収集・保存し、あらゆる調査や過去の報告の証拠として使用可能にする。SIEM Security as a Service は、検知型の技術コントロールを提供しているが、防御的そして反応的な技術的コントロールとして構成することも可能である。

14.4.8 暗号化

暗号化は、暗号アルゴリズムを用いてデータをわかりにくく/符号化するプロセスであり、その結果が暗号化されたデータ（暗号文と呼ばれる）である。正しいキーを所有する限られた受け手かシステムのみが、暗号文を復号化（非暗号化）することができる。難読化するシステムの暗号化には、通常、1 つあるいはそれ以上のアルゴリズムが含まれ、1 つあるいはそれ以上のキー、そして暗号化、複合化、キーを管理するシステム、プロセス、手続きを破ることは、計算上困難（実行不可能）である。それぞれの構成部分は、他の構成部分がなければまったく無用であり、例えば、最良のアルゴリズムは、プロセスが弱いために攻撃側がアクセスできると簡単に「クラックする」ことである。

一方向の暗号化機能の場合、ダイジェスト、すなわちハッシュが代わりに生成される。一方向の暗号化機能には、ハッシング、デジタル署名、証明書の生成と書替、キーの交換が含まれる。これらのシステムには、通常、１つあるいはそれ以上のアルゴリズムが含まれ、容易に複製されるが、管理のためのプロセスと手続きが一緒になることによって、偽物に対しては強力な抵抗力がある。Security as a Service プロバイダに委託した場合の暗号化は、防御的で検知型の技術コントロールに分類される。

14.4.9 事業継続性と災害復旧

事業継続性と災害復旧は、サービスを中断するあらゆる事象に対して業務遂行上の回復力を保証するために設計し導入する処置である。この処置は柔軟で信頼できるフェールオーバと災害復旧のソリューションにより、自然と人為のいずれにせよ、サービス中断の事象に対し必要なサービスを提供する。例えば、拠点の 1 つで災害の筋書きが発生した場合、別な拠点のコンピュータが災害の発生した拠点のアプリケーションを保護することができる。この Security as a Service は、反応的、防御的、そして検知型の技術コントロールを提供する。

14.4.10 ネットワークセキュリティ

ネットワークセキュリティは、アクセスを制限あるいは割り当て、基盤を形成するリソースのサービスを提供、監視、記録、そして保護するセキュリティサービスから構成される。

アーキテクチャ上、ネットワークセキュリティは全体としてネットワークのセキュリティコントロールを対象としたサービス、基盤となるリソースそれぞれの個別のネットワークを特に対象としたコントロールを提供する。クラウド/仮想環境とハイブリッド環境で、ネットワークセキュリティは従来の物理的装置と共に、仮想装

置によって提供されることもある。ハイパーバイザーとの密接な結合によって仮想ネットワークレイヤ上のあらゆるトラフィックを完全に可視化することが、キーである。これらのネットワークセキュリティは、発見的、防御的、そして反応的な技術コントロールを提供する。

14.5 許可

- 実装者は、ユーザの行動のパターン認識を採用することができる。
- 実装者は、SLA[213]の期待管理で用いるセキュリティメトリクスを安心できる法的な橋渡しとして採用することができる。
- 実装者は、ペネトレーションテストに用いる信頼されたチャネルの提供を取り入れることができる。

14.6 推奨事項

- 実装者は、テナントと利用者の間の通信チャネルを安心できるものとして保証すべきである。
- 提供者は、知る必要があるとの基礎に基づいてサプライチェーン全体に保証のある継続した通知を自動で提供すべきである。
- 提供者は、サービスレベルアグリーメントのコンプライアンスに必要な内部操作の安全な記録を提供すべきである。
- 利用者は、サードパーティによる監査と SLA の仲介サービスを追加するように要求すべきである。
- すべての当事者は、SCAP (NIST)、CYBEX (ITU-T)、あるいは RID & IODEF (IETF) 等の標準的なセキュリティインタフェースを使用しあらゆるインタフェースの継続的な監視を可能にすべきである。

14.7 要求事項

14.7.1 Identity as a Service への要求事項

- ✓ IaaS プロバイダは、クラウド利用者にアカウントの（クラウドとオンプレミスのアプリケーションとリソースの両方の）プロビジョニング/プロビジョニング解除機能を供給しなければならない。
- ✓ IaaS プロバイダは、クラウド利用者に認証機能（複数のフォームと要素の）を供給しなければならない。
- ✓ IaaS プロバイダは、クラウド利用者にアイデンティティライフサイクル管理を供給しなければならない。
- ✓ IaaS プロバイダは、クラウド利用者にディレクトリサービスを供給しなければならない。
- ✓ IaaS プロバイダは、クラウド利用者に（要求に応じて、多面的な）ディレクトリの同期機能を供給しなければならない

[213] SLA-Service Level Agreement　サービスレベルアグリーメント

- ✓ IaaS プロバイダは、クラウド利用者に SSO の認証連携機能を供給しなければならない。
- ✓ IaaS プロバイダは、クラウド利用者にウェブ SSO 機能（より詳細なアクセス実行とセッション管理機能、これは SSO の認証連携と異なる）を供給しなければならない。
- ✓ IaaS プロバイダは、特権によるセッション監視機能を供給しなければならない。
- ✓ IaaS プロバイダは、詳細なアクセス管理機能を供給しなければならない。
- ✓ IaaS プロバイダは、監査記録（否認防止の選択肢を含む）の改ざん防止付きの記憶装置を供給しなければならない。
- ✓ IaaS プロバイダは、ポリシー管理機能（承認管理、役割管理、コンプライアンスポリシー管理を含む）を供給しなければならない。
- ✓ IaaS プロバイダは、クラウド利用者に承認権限（ユーザとアプリケーション/システムの両方）を供給しなければならない。
- ✓ IaaS プロバイダは、クラウド利用者に承認権限のトークン管理とプロビジョニング機能を供給しなければならない。
- ✓ IaaS プロバイダは、クラウド利用者にユーザプロファイルと権限付与管理機能（ユーザとアプリケーション/システムの両方）を供給しなければならない。
- ✓ IaaS プロバイダは、クラウド利用者に対し、ポリシーと規制に従ったコンプライアンスの監視および/あるいは報告を支援しなければならない。
- ✓ IaaS プロバイダは、クラウド利用者にクラウドアプリケーションの連携したプロビジョニング機能を供給しなければならない。
- ✓ IaaS プロバイダは、特権ユーザとパスワード管理機能（管理、共有のシステムとアプリケーションのアカウントを含む）を供給しなければならない。
- ✓ IaaS プロバイダは、クラウド利用者に（基盤であるシステム/サービスにより支援される箇所で）ロールベースのアクセス制御機能（RBAC）を供給しなければならない。
- ✓ IaaS プロバイダは、クラウド利用者に選択可能な DLP 統合機能を供給しなければならない。
- ✓ IaaS プロバイダは、クラウド利用者に選択可能な個人まで詳細化する行動監査機能を供給しなければならない。
- ✓ IaaS プロバイダは、クラウド利用者にアイデンティティの資格に基づいた任務の分離機能を供給しなければならない。

- ✓ IaaS プロバイダは、クラウド利用者にコンプライアンスに特化した報告機能を供給しなければならない。
- ✓ IaaS プロバイダは、クラウド利用者に集中したポリシー管理機能を供給しなければならない。
- ✓ IaaS プロバイダは、クラウド利用者が使用できる管理インタフェースを供給しなければならない。
- ✓ IaaS プロバイダは、クラウド利用者に統合したアクセス制御と監査機能を供給しなければならない。
- ✓ IaaS プロバイダは、クラウド利用者に様々な提供者間の相互運用性と異種混合を可能にしなければならない。
- ✓ IaaS プロバイダは、クラウド利用者に拡張性を供給しなければならない。

14.7.2 DLP の SecaaS 要求事項

- ✓ DLP プロバイダは、クラウド利用者にデータのラベリングと分類機能を供給しなければならない。
- ✓ DLP プロバイダは、クラウド利用者に重要データの識別機能を供給しなければならない。
- ✓ DLP プロバイダは、クラウド利用者に主要な法規制に対し、あらかじめ定義されたポリシーを供給しなければならない。
- ✓ DLP プロバイダは、クラウド利用者にコンテキストに沿って検出可能な方法を供給しなければならない。
- ✓ DLP プロバイダは、クラウド利用者に構造的にデータ（保存データ）を照合する機能を供給しなければならない。
- ✓ DLP プロバイダは、クラウド利用者に SQL の正規表現による検出機能を供給しなければならない。
- ✓ DLP プロバイダは、クラウド利用者にトラフィックスパニング（転送中データ）の検出機能を供給しなければならない。
- ✓ DLP プロバイダは、クラウド利用者にリアルタイムのユーザ認知機能を供給しなければならない。
- ✓ DLP プロバイダは、クラウド利用者にセキュリティレベルの設定機能を供給しなければならない。
- ✓ DLP プロバイダは、クラウド利用者に利用者属性の検索機能を供給しなければならない。
- ✓ DLP プロバイダは、クラウド利用者にインシデントに対する自動応答機能を供給しなければならない。
- ✓ DLP プロバイダは、クラウド利用者にデータへの署名機能を供給しなければならない。
- ✓ DLP プロバイダは、クラウド利用者に暗号データの保護とアクセス制御機能を供給しなければならない。
- ✓ DLP プロバイダは、クラウド利用者にコンピュータによる判読が可能なポリシー用言語を供給しなければならない。

14.7.3 ウェブサービスの SecaaS 要求事項

- ✓ ウェブサービス SecaaS プロバイダは、クラウド利用者にウェブ監視とフィルタリング機能を供給しなければならない。
- ✓ ウェブサービス SecaaS プロバイダは、クラウド利用者にマルウェア、スパイウェア、ボットネットワーク分析と遮断する機能を供給しなければならない。
- ✓ ウェブサービス SecaaS プロバイダは、クラウド利用者にフィッシングサイトの遮断機能を供給しなければならない。
- ✓ ウェブサービス SecaaS プロバイダは、クラウド利用者にインスタントメッセージをスキャンする機能を供給しなければならない。
- ✓ ウェブサービス SecaaS プロバイダは、クラウド利用者に電子メールのセキュリティ機能を供給しなければならない。
- ✓ ウェブサービス SecaaS プロバイダは、クラウド利用者に帯域管理とトラフィック制御機能を供給しなければならない。
- ✓ ウェブサービス SecaaS プロバイダは、クラウド利用者にデータ喪失防止機能を供給しなければならない。
- ✓ ウェブサービス SecaaS プロバイダは、クラウド利用者に詐欺防止機能を供給しなければならない。
- ✓ ウェブサービス SecaaS プロバイダは、クラウド利用者にウエブアクセス制御機能を供給しなければならない。
- ✓ ウェブサービス SecaaS プロバイダは、クラウド利用者にバックアップ機能を供給しなければならない。
- ✓ ウェブサービス SecaaS プロバイダは、クラウド利用者に SSL 暗号化（復号化/ハンドオフ）機能を供給しなければならない。
- ✓ ウェブサービス SecaaS プロバイダは、クラウド利用者に利用ポリシー強制機能を供給しなければならない。
- ✓ ウェブサービス SecaaS プロバイダは、クラウド利用者に脆弱性管理機能を供給しなければならない。
- ✓ ウェブサービス SecaaS プロバイダは、クラウド利用者にウェブ解析の報告機能を供給しなければならない。

14.7.4 電子メール SecaaS の要求事項

- ✓ 電子メールセキュリティ SecaaS プロバイダは、クラウド利用者に的確なフィルタリング機能を供給しスパムとフィッシングを遮断しなければならない。
- ✓ 電子メールセキュリティ SecaaS プロバイダは、クラウド利用者にウィルスとスパイウェアに対し高度の防御機能を供給し、それらが企業の領域に入ることを防止しなければならない。
- ✓ 電子メールセキュリティ SecaaS プロバイダは、クラウド利用者に詳細なメールフローと暗号化を定義する柔軟なポリシーを供給しなければならない。
- ✓ 電子メールセキュリティ SecaaS プロバイダは、クラウド利用者にリッチで会話型の報告書と相互に関連づけたリアルタイムの報告機能を供給しなければならない。

- ✓ 電子メールセキュリティ SecaaS プロバイダは、クラウド利用者にポリシーの実施を強制するため高度のコンテントスキャニング機能を供給しなければならない。
- ✓ 電子メールセキュリティ SecaaS プロバイダは、クラウド利用者にポリシーに基づいて電子メールの一部/すべてを暗号化する選択可能な機能を供給しなければならない。
- ✓ 電子メールセキュリティ SecaaS プロバイダは、クラウド利用者に様々な電子メールサーバソリューションを統合する機能を供給しなければならない。

14.7.5 セキュリティ評価 SecaaS の要求事項

- ✓ セキュリティ評価 SecaaS プロバイダは、クラウド利用者に詳細なガバナンスのプロセスとメトリクスを供給しなければならない（実装者はポリシーが設定され意思決定が行われるプロセスを定義し文書化しなければならない）。
- ✓ セキュリティ評価とガバナンスプロバイダは、自動化ソリューションを実装し、違反やセキュリティインシデントが発生した場合、サプライチェーン上の直接のメンバーに通知を出せるようにすべきである。
- ✓ セキュリティ評価 SecaaS プロバイダは、クラウド利用者に適切なリスク管理機能を供給しなければならない（実装者は、重要なビジネスプロセスと行動がポリシーと意思決定に基づいて許容されている状態を保証するプロセスを定義し文書化しなければならない）。
- ✓ セキュリティ評価 SecaaS プロバイダは、クラウド利用者に詳細なコンプライアンスを供給しなければならない（実装者は、ポリシーと意思決定に密接に関連するプロセスを定義し文書化しなければならない）。
- ✓ セキュリティ評価 SecaaS プロバイダは、クラウド利用者に内部の指示、手続き、要求、あるいは外部の法律、規則、標準、契約に基づくポリシーを供給しなければならない。
- ✓ セキュリティ評価 SecaaS プロバイダは、クラウド利用者に技術的なコンプライアンス監査機能（機器、オペレーティングシステム、データベース、アプリケーションの構成上の設定を自動で監査する）を供給しなければならない。
- ✓ セキュリティ評価 SecaaS プロバイダは、クラウド利用者にアプリケーションのセキュリティ評価機能（自社開発のアプリケーションの自動監査機能）を供給しなければならない。
- ✓ 評価とガバナンスサービスのプロバイダは、クラウド利用者に脆弱性評価機能、例えばネットワーク機器、コンピュータ、アプリケーションに既知の脆弱性や構成上の問題がないか自動調査する機能を供給しなければならない。
- ✓ セキュリティ評価 SecaaS プロバイダは、クラウド利用者にペネトレーションテスト機能（通常、手作業による支援が必要な場合も含め、環境、ネットワーク、あるいはコンピュータへアクセスし脆弱性と構成上の問題を探索する）を供給しなければならない。
- ✓ セキュリティ評価 SecaaS プロバイダは、クラウド利用者にセキュリティの格付けを供給しなければならない。

14.7.6 不正侵入検知 SecaaS の要求事項

- ✓ 不正侵入検知 SecaaS プロバイダは、クラウド利用者に不正侵入とポリシー違反の識別機能を供給しなければならない。
- ✓ 不正侵入検知 SecaaS プロバイダは、クラウド利用者に自動あるいは手動による修復処置を供給しなければならない。
- ✓ 不正侵入検知 SecaaS プロバイダは、クラウド利用者にワークロードのカバーレッジ、仮想化レイヤ（仮想マシン管理/ハイパーバイザー）管理機能を供給しなければならない。
- ✓ 不正侵入検知 SecaaS プロバイダは、クラウド利用者に 1 つあるいはそれ以上の統計的、ふるまい、署名、発見的な技法を用いた高度の検査機能を供給しなければならない。
- ✓ 不正侵入検知 SecaaS プロバイダは、クラウド利用者にシステムコールの監視機能を供給しなければならない。
- ✓ 不正侵入検知 SecaaS プロバイダは、クラウド利用者にシステム/アプリケーションのログ検査機能を供給しなければならない。
- ✓ 不正侵入検知 SecaaS プロバイダは、クラウド利用者に一貫した OS 監視機能（ファイル、レジストリー、ポート、プロセス、インストール済みソフトウェア等）を供給しなければならない。
- ✓ 不正侵入検知 SecaaS プロバイダは、クラウド利用者に一貫した仮想マシン管理/ハイパーバイザー監視機能を供給しなければならない。
- ✓ 不正侵入検知 SecaaS プロバイダは、クラウド利用者に仮想マシンのイメージリポジトリー監視機能を供給しなければならない。

14.7.7 SIEM SecaaS の要求事項

- ✓ SIEM SecaaS プロバイダは、クラウド利用者にリアルタイムのログ/イベント収集、重複の排除、正規化、集合、可視化の機能を供給しなければならない。
- ✓ SIEM SecaaS プロバイダは、クラウド利用者にフォレンジックサポートを供給しなければならない。
- ✓ SIEM SecaaS プロバイダは、クラウド利用者にコンプライアンスの報告とサポートを供給しなければならない。
- ✓ SIEM SecaaS プロバイダは、クラウド利用者に IR サポートを供給しなければならない。
- ✓ SIEM SecaaS プロバイダは、クラウド利用者に電子メールに制限されない異常検出機能を供給しなければならない。
- ✓ SIEM SecaaS プロバイダは、クラウド利用者に詳細な報告機能を供給しなければならない。
- ✓ SIEM SecaaS プロバイダは、クラウド利用者に柔軟なデータ維持期間と柔軟なポリシー管理機能を供給しなければならない。

14.7.8 暗号化 SecaaS の要求事項

- ✓ 暗号化 SecaaS プロバイダは、クラウド利用者に転送中のデータ保護機能を供給しなければならない。

- ✓ 暗号化 SecaaS プロバイダは、クラウド利用者に保存データの保護機能を供給しなければならない。
- ✓ 暗号化 SecaaS プロバイダは、クラウド利用者にキーとポリシーの管理機能を供給しなければならない。
- ✓ 暗号化 SecaaS プロバイダは、クラウド利用者にキャッシュデータの保護機能を供給しなければならない。

14.7.9 事業継続性と災害復旧の要求事項

- ✓ 事業継続性と災害復旧 SecaaS プロバイダは、クラウド利用者に柔軟な基盤を供給しなければならない。
- ✓ 事業継続性と災害復旧 SecaaS プロバイダは、クラウド利用者に安全なバックアップ機能を供給しなければならない。
- ✓ 事業継続性と災害復旧 SecaaS プロバイダは、クラウド利用者に運用の監視機能を供給しなければならない。
- ✓ 事業継続性と災害復旧 SecaaS プロバイダは、クラウド利用者にサードパーティのサービスと接続可能な機能を供給しなければならない。
- ✓ 事業継続性と災害復旧 SecaaS プロバイダは、クラウド利用者に複製した基盤構成要素を供給しなければならない。
- ✓ 事業継続性と災害復旧 SecaaS プロバイダは、クラウド利用者に複製データ（中核/基幹システム）を供給しなければならない。
- ✓ 事業継続性と災害復旧 SecaaS プロバイダは、クラウド利用者にデータおよび/あるいはアプリケーションのリカバリ機能を供給しなければならない。
- ✓ 事業継続性と災害復旧 SecaaS プロバイダは、クラウド利用者に運用の代替拠点を供給しなければならない。
- ✓ 事業継続性と災害復旧 SecaaS プロバイダは、クラウド利用者に運用上の弾力性を保証するため試験と計測が完了しているプロセスと運用機能を供給しなければならない。
- ✓ 事業継続性と災害復旧 SecaaS プロバイダは、クラウド利用者に地理的に分散したデータセンタ/基盤を供給しなければならない。
- ✓ 事業継続性と災害復旧 SecaaS プロバイダは、クラウド利用者にネットワークを供給しなければならない。

14.7.10 ネットワークセキュリティ SecaaS の要求事項

- ✓ ネットワークセキュリティ SecaaS プロバイダは、クラウド利用者にデータの脅威に関する詳細な情報を供給しなければならない。
- ✓ ネットワークセキュリティ SecaaS プロバイダは、クラウド利用者にアクセス制御の脅威に関する詳細な情報を供給しなければならない。
- ✓ ネットワークセキュリティ SecaaS プロバイダは、クラウド利用者にアクセスと認証制御機能を供給しなければならない。

- ✓ ネットワークセキュリティ SecaaS プロバイダは、クラウド利用者にセキュリティゲートウェイ（ファイアウォール、WAF、SOA/API）を供給しなければならない。
- ✓ ネットワークセキュリティ SecaaS プロバイダは、クラウド利用者にセキュリティ製品（IDS/IPS、サーバ層のファイアウォール、ファイルの完全性監視、DLP、アンチウィルス、アンチスパム）を供給しなければならない。
- ✓ ネットワークセキュリティ SecaaS プロバイダは、クラウド利用者にセキュリティ監視とインシデントレスポンス機能を供給しなければならない。
- ✓ ネットワークセキュリティ SecaaS プロバイダは、クラウド利用者に DoS（サービス拒否）保護/軽減機能を供給しなければならない。
- ✓ ネットワークセキュリティ SecaaS プロバイダは、クラウド利用者に DNSSEC、NTP、OAuth、SNMP、ネットワーク分割管理、セキュリティ等の安全な「基盤サービス」を供給しなければならない。
- ✓ ネットワークセキュリティ SecaaS プロバイダは、クラウド利用者にトラフィック/ネットフローの監視機能を供給しなければならない。
- ✓ ネットワークセキュリティ SecaaS プロバイダは、クラウド利用者にハイパーバイザーレイヤと一貫した機能を供給しなければならない。

参考文献

[1] Security and Economic Benefits of Standardization for Security as a Service. September 2011 Proceedings. United Nations ITU-T.

[2] Gartner. Gartner Says Security Delivered as a Cloud-Based Service Will More Than Triple in Many Segments by 2013. July 15, 2008. http://www.gartner.com/it/page.jsp?id=722307

[3] Cloud Security Alliance. Defined Categories of Service 2011. https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf

[i] DANYLIW, R., et al. 2007. The Incident Object Description Exchange Format, IETF Internet Draft RFC 5070.
[ii] MORIARTY, K. 2010. Real-time Inter-network Defense, IETF Internet Draft RFC 6045.
[iii] MORIARTY, K., and TRAMMELL, B. 2010. Transport of Real-time Inter-network Defense (RID) Messages, IETF Internet Draft RFC 6046.
[iv] FITZGERALD, E., et al. 2010. Common Event Expression (CEE) Overview. Report of the CEE Editorial Board.
[v] BIRK, D. and WEGENER, C. 2011. Technical Issues of Forensic Investigations in Cloud Computing Environments In Proceedings of 6th International Workshop on Systematic Approaches to Digital Forensic Engineering (IEEE/SADFE), Oakland, CA, USA.