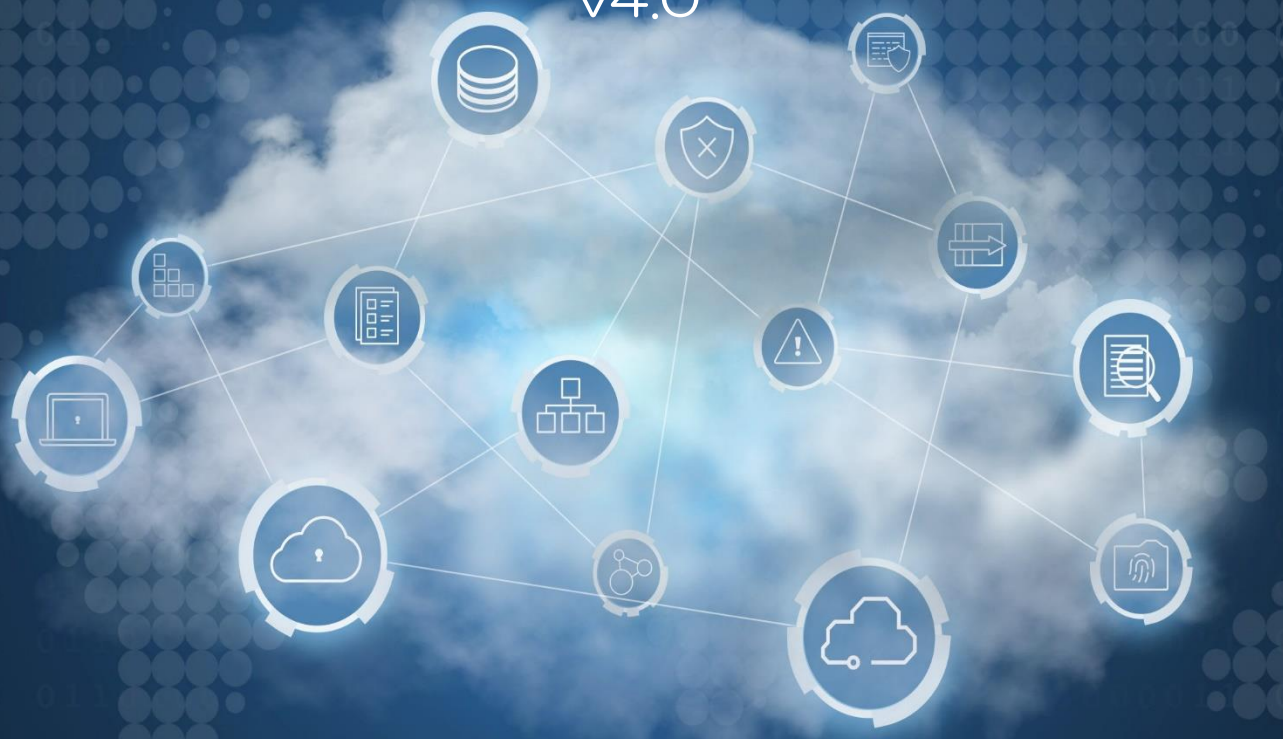
SECURITY GUIDANCE

For Critical Areas of Focus In Cloud Computing v4.0

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

v4.0



CSA JC Japan Chapter cloud security alliance℠

CSA cloud security alliance®

Cloud Security Alliance 著作になる
”Security Guidance for the Critical Areas of Focus in Cloud Computing v4.0” の正式の所在場所は
https://cloudsecurityallince.org/download/security-guidance-v4/ です。

本書は 

受験準備のための公式ガイドです。

日本語版提供に際しての告知、謝辞及び注意事項

本書「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 v4.0」は、Cloud Security Alliance (CSA)が公開している「Security Guidance for the Critical Areas of Focus in Cloud Computing v4.0」の日本語訳です。
本書は、一般社団法人日本クラウドセキュリティアライアンス（CSA ジャパン）が、CSA の許可を得て翻訳し、公開するものです。
本書は、原文をそのまま翻訳したものです。また、本書内で参照されている URL 等は、すべて英語版へのリンクとなっております。原文と日本語版の内容に相違があった場合には、原文が優先されます。

翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSA ジャパンは何らの保証をするものではありません。
技術用語等について、一般に定訳があると判断したものは、極力それを使用していますが、文脈上その他の理由で、一般に用いられる訳語が妥当でないと考えた場合は、他の語に置き換えている場合があります。また、同様の理由で、技術用語に対して訳語を 1 対 1 で充てているとは限りませんので、ご了解ください。確認が必要と思われた場合は、原典に当たられることをお勧めします。
本書の原文では、*斜体字(italic)*が、主として見出し語に多用されています。日本語ではフォントサポートおよび見易さの観点から、原則として**太字**に置き換えて表記しました。
翻訳に際して原文の誤りと推測されるものは原則として著作者に確認の上、最小限の修正を行った上で翻訳しています。また、翻訳に際して行った判断等については、脚注部（一部文中）に「訳注」として示しました。

この翻訳版は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。
変更履歴

日付	バージョン	変更内容
2017 年 11 月 27 日	CSA ガイダンス v4.0 日本語版 V1.0	初版発行
2018 年 7 月 24 日	CSA ガイダンス v4.0 日本語版 V1.1	初版更新版発行

日本語版作成に際しての謝辞

「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 v4.0」の日本語訳は、CSAジャパンの「ガイダンス・ワーキンググループ」に参加するメンバーを中心とした、CSAジャパン会員の有志により行われました。
作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。

以下に、翻訳に参加された方々の氏名および所属先（企業会員からの参加の場合のみ）を記します。
日本語版発刊に際して、謝意を表したいと思います。また、本日本語版の利用者にも、謝意を共有していただければ幸いです。

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 v4.0
日本語版作成作業参加者（氏名あいうえお順・敬称略）

有田　　仁
甲斐　　賢（株式会社日立製作所）
勝見　　勉
上村　竜也
最首　克也
新宮　　貢
鶴田　浩司
成田　和弘
羽田野尚登（株式会社日本環境認証機構）
諸角　昌宏
山崎　万丈

まえがき

Cloud Security Alliance (CSA)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 4 版へようこそ。クラウドコンピューティングの隆盛とその進化し続ける技術は、数多くの利点と同時に課題ももたらした。本書では、ビジネスの目指すところのために、ガイダンスと共に「啓示」もお届けしようと意図した。併せて、クラウドコンピューティング技術を採用することに伴うリスクについて、それを管理し緩和する術も示した。

CSA は、クラウドコンピューティングという世界の中でセキュリティを担保するための実践規範を定着させる活動を推進して、クラウドというパラダイムを取り入れようと模索する組織のために、実践的で実行可能なロードマップを提供してきた。「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」第 4 版は、今までの各版のガイダンスの上に、本書のために行った調査や、CSA 会員一般からの参加、ワーキンググループ、そしてこの世界の専門家の貢献が積み上げられたものである。今回の版は、クラウド、セキュリティ、関連技術の進化を取り入れ、クラウドセキュリティの実情を反映させ、CSA の研究プロジェクトの最新の成果を組み込んだ上に、関連技術に関するガイダンスも盛り込んでいる。

セキュアなクラウドコンピューティングへの到達には、世界にまたがる広範なステークホルダーからの積極的な関与が欠かせない。CSA ならでは、このような大きな広がりを持った仲間たち、業界団体、世界各地の支部、ワーキンググループ、そして個人のメンバーを結集することができる。この版の発行に貢献したこれらすべての人と組織に、深甚の謝意を表したい。

セキュアなクラウドコンピューティング環境の実現に向けた実践規範の開発と推進に向けて CSA と共に取り組むにはどうすればよいか、ぜひ cloudsecurityalliance.com のサイトを訪れて知っていただきたい。

よろしくお願いします。

Luciano (J.R.) Santos
Executive Vice President of Research
Cloud Security Alliance

謝辞

執筆主幹

Rich Mogull
James Arlen
Francoise Gilbert
Adrian Lane
David Mortman
Gunnar Peterson
Mike Rothman

編集担当

John Moltz
Dan Moren
Evan Scoboria

CSA からの従事者

Jim Reavis
Luciano (J.R.) Santos
Hillary Baron
Ryan Bergsma
Daniele Catteddu
Victor Chin
Frank Guanco
Stephen Lumpe (Design)
John Yeoh

謝辞

CSA 理事会および CSA 経営陣を代表して、今回のバージョンの”CAS Security Guidance for Critical Areas of Focus in Cloud Computing”のために時間を割き、またフィードバックを送ってくれた全ての人々に謝意を表します。皆様の貢献は価値あるものであり、皆様のようなボランティアの献身が、CSA の未来を切り開く原動力であり続けるものと信じています。

CEOからのメッセージ

2009 年 4 月に Cloud Security Alliance が初めてガイダンスを世に送り出した時に始まった事業である、クラウドセキュリティの世界における最善の対応策である「知恵」の集大成に向けての、新たな貢献ができることに、大きな興奮を覚えています。本書に記された課題と推奨事項をよく検討されることを期待しています。そして、ご自身の経験と照らし合わせて、ご意見を頂ければ幸いです。本書の作成に携わっていただいた全ての人に、満腔の感謝を捧げます。

最近、Cloud Security Alliance の設立に関わった業界の専門家と 1 日を共に過ごす機会がありました。彼は、CSA が、その当初の使命である、クラウドコンピューティングがセキュアでありうることを証明することと、そのために必要なツールを提供することのほとんどを成し遂げたね、と述懐してくれました。CSA は、クラウドコンピューティングが IT にとって信頼しうるセキュアな解となることに貢献して来ました。今やそれにとどまらず、クラウドコンピューティングは IT におけるデフォルトの選択肢となり、今日のビジネスの世界を根本から再構成するに至っています。

クラウドコンピューティングの高揚するような成功と、クラウドエコシステムへの信頼をリードする CSA の役割はしかし、さらに大きな課題をもたらし、新たな任務の重要性を示唆します。クラウドは、今日、全てのコンピューティングの基盤であり、Internet of Things のどこでもつながる世界を支えるものとなっています。クラウドコンピューティングは、情報セキュリティ分野の基盤でもあります。コンピューティングを実現する新たな手法であるコンテナや DevOps はクラウドと不可分であり、IT の進化を加速するものです。Cloud Security Alliance は、この急速に変化する IT の世界において、必要となるセキュリティの最重要の知識を提供し、次世代の安心と信頼への取組みの最前線に立つことを約束します。そして、皆さんが仲間として加わってくれることを、いつでも、お待ちしています。

心をこめて

Jim Reavis
Co-Founder & CEO
Cloud Security Alliance

TABLE OF **CONTENTS** ／ 目次

DOMAIN 1

クラウドコンピューティングのコンセプトとアーキテクチャ

1.0　はじめに

このドメインは、以下に展開する Cloud Security Alliance の「ガイダンス」がどのようなものであるかの大枠を示すものである。クラウドコンピューティングの説明と定義を行い、基本的な用語を定義し、本書で参照する論理的および構造的枠組みの全体像を示す。

クラウドコンピューティングの見方には様々なものがある。ざっと挙げただけでも、それは技術であり、技術の集成物であり、運用モデルであり、ビジネスモデルである。その本質は、**変革**をもたらし、**飛躍**をもたらす。また、極めて速いスピードで拡大しており、衰える兆しを見せない。この「ガイダンス」の初版で示したリファレンスモデルは現在でもある程度正しいが、今日完ぺきとは言えなくなっていることは間違いない。今回の改訂ですら、今後数年に起こりうる進化をカバーすることはできない。

クラウドコンピューティングが**機動性**、**耐障害性**、**経済性**の面でもたらすメリットは極めて大きい。利用組織はより早く事を起こすことができ（なぜなら購買もハードウェアの用意も不要で、全てはソフトウェアで定義可能だから）、停止時間を削減でき（クラウドにあらかじめ備わった拡張性やその他の特性のおかげで）、コストを削減できる（初期投資を抑えることができ、必要に応じた能力確保がよりうまくできるから）。**セキュリティ**面でのメリットもある。なぜならクラウド事業者には、顧客を守ることで収益面で莫大な利益が期待できるからである。

しかしながら、このようなメリットは、クラウド特有のモデルを理解した上で採用し、自社のシステム設計と管理をクラウドプットフォームの特性と機能に合うように調整した時に、初めて得られるものである。実際、既存の資産やアプリケーションを、何も変更を加えずに単純にクラウドプロバイダの下に移動しただけだと、往々にして、コストは上がる一方、迅速性や耐障害性は落ち、セキュリティまでも悪くしてしまう。

このドメインが目指す処は、本書のそれ以降の部分と、そこに書かれる推奨事項の基礎部分を構築することである。意図するところはセキュリティの専門家にクラウドコンピューティングに関する共通言語と理解を提供し、クラウドと従来型コンピューティングの違いを明らかにすることで、セキュリティの専門家が、リスクを増すのではなく、よりよいセキュリティ（および他のメリット）を実現できる、クラウドネイティブなアプローチが取れるよう導く一助となることである。

このドメインには 4 つのセクションがある。

- クラウドコンピューティングの定義
- クラウドの論理モデル
- クラウドの概念モデル、アーキテクチャモデル、リファレンスモデル
- クラウドのセキュリティと基準適合の視点、責任問題、そしてそれらのモデル

Cloud Security Alliance は、まったく新しい言語体系やリファレンスモデルを作ろうとしているのではない。狙いとするところは、すでにあるいくつかのモデルー特に注目すべきは NIST SP800-145、ISO/IEC17788 と ISO/IEC17789ーを抽出して調和させ、セキュリティの専門家に最も関係するものに焦点を当てることである。

1.1 概要

1.1.1 クラウドコンピューティングの定義

クラウドコンピューティングは新しい運用モデルであり、共有プールにあるコンピューティング資源をうまく動かすための技術の体系である。

それは過去の延長線上にはない技術で、協働作業、機動力、拡張能力および可用性を高めると共に、コンピューティングの最適化と効率化によってコスト削減の機会をもたらす可能性を秘めている。クラウドモデルは、コンポーネントが素早く組み立てられ、配置され、実装され、終了され、さらにスケールアップダウンが可能で、それにより、その手配と利用を、水や電気のように必要に応じて行える世界を構想するものである。

NIST はクラウドコンピューティングを以下のように定義している。

> クラウドコンピューティングは、共用の構成可能なコンピューティングリソース（ネットワーク、サーバ、ストレージ、アプリケーション、サービス）の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスすることを可能とするモデルであり、最小限の利用手続きまたはサービスプロバイダとのやりとりで速やかに割当てられ提供されるものである。 ＜訳注：IPA 提供の日本語版より引用＞

ISO/IEC の定義は非常によく似ている。

> セルフサービスの資源割当てと管理によって、物理または仮想のリソースの共同利用のための伸縮自在で拡張性のあるプールに、必要に応じてネットワーク経由でアクセスすることを可能にするパラダイムである。

もう少し簡単にクラウドを説明するとすれば、それはプロセッサやメモリといったリソースのセットを持ってきて、それを大きなプールの中に放り込む（この場合仮想化を用いて）ということである。利用者は自分が必要とするものを、例えば CPU8 個とメモリ 16GB を、プールから出すよう依頼し、クラウドはそのリソースを客に割り当て、客はネットワーク経由でそれに接続して利用する。利用が終了したらリソースを解放してプールに戻し、誰か他の人が利用できるようにする。

クラウドには殆ど全てのコンピューティングリソースを含むことができる。それは我々がコンピュータと考えるプロセッサ、メモリからネットワーク、ストレージ、そして上位のリソースつまりデータベースやアプリケーションまで多岐にわたる。例えば、他の何百もの組織と共同利用するサービスの中の CRM アプリケーションによる 500 人の社員の管理を利用することは、クラウド上のリモートにある 100 のサーバを起動することになり、まさにクラウドコンピューティングである。

用語の定義：**クラウド利用者(cloud user)**とはリソースを求めまたは使う人または組織であり、**クラウド事業者(cloud provider)**はそれを提供する人または組織である。また時にはクラウド利用者を指す言葉として **client** や **consumer** という用語を用い、事業者のことを**サービス**と言ったり単純に**クラウド**と言ったりする。NIST SP500-292 では、”cloud actor”という用語を用い、クラウドブローカー(cloud brokers)、通信事業者(carriers)、監査人(auditors)を加えている。ISO/IEC17788 ではクラウドサービス利用者(cloud service customer)、クラウドサービスパートナー(cloud service partner)、クラウドサービス事業者(cloud service provider)の用語を用いている。

[1]

クラウドを実現するカギとなる技術は抽象化(abstraction)と統合管理(orchestration)[2]である。下部にある物理的インフラストラクチャからリソースプールを作るのに抽象化を用い、そのプールから利用者にひとまとまりのリソースを切り出して提供する部分を取りまとめるのに統合管理（および自動化）を用いる。この二つの技術が、何かをクラウドと定義するのに使われる基本的な特性を生み出していることが、わかるだろう。

これが従来の仮想化とクラウドの違いである。仮想化はリソースの抽象化はするが、それらをまとめてプールして利用者にオンデマンドで提供する統合管理の機能は持たず、その部分は手作業のプロセスによっている。

クラウドは本来的に**マルチテナント**である。複数の相互に無関係の利用主体が一つのリソースプールを共用するが、お互いの間は**分離(segregate)**され**隔離(isolate)**されている。分離することで事業者は複数のグループにリソースを分配でき、隔離によってお互い相手の資産を覗き見たり変えたりできないことを確実にしている。マルチテナント性は複数の組織の間だけで実現するのではなく、一つの事業体または組織体の中の別の組織単位の間でリソースを分配する場合にも役に立つ。

1.1.2 定義に基づくモデル

Cloud Security Alliance (CSA)は、クラウドコンピューティングの定義に際して、NIST モデル(NIST model for cloud computing)をその標準としている。CSA はまた、ISO モデル(ISO/IEC model)も支持している。これは、より詳細で、リファレンスモデルとしても機能する。本ドメインではその両方を参照する。

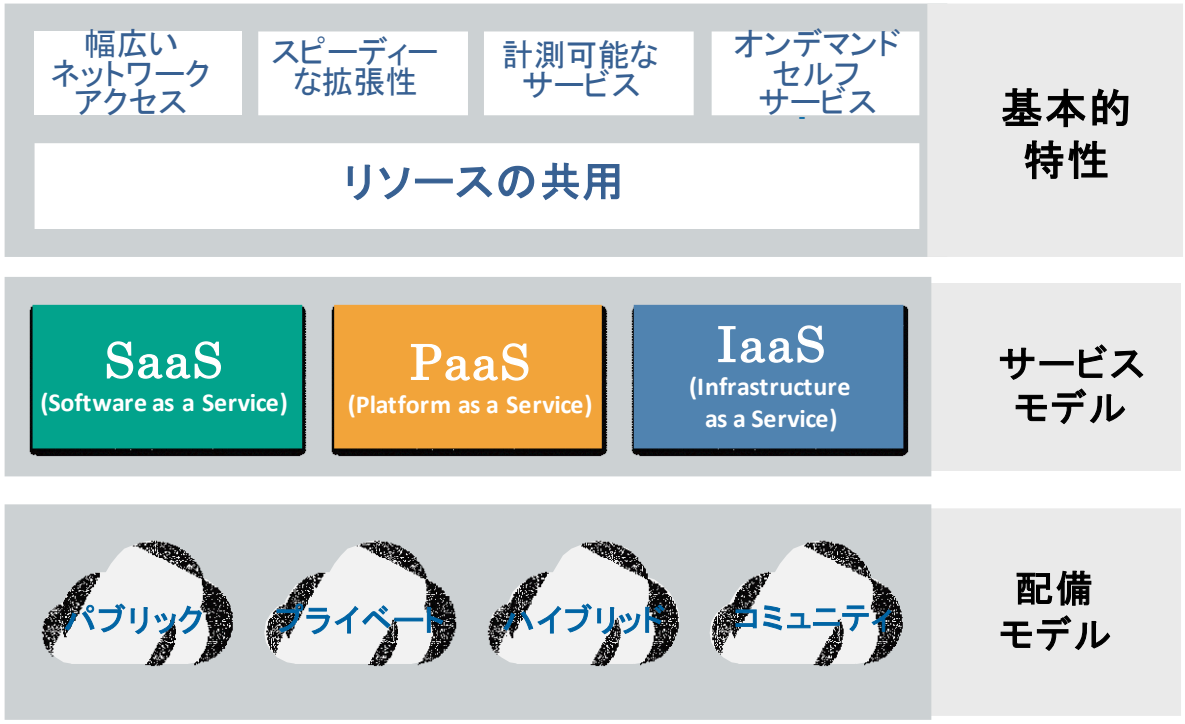
NIST の公表するものは一般に広く受け入れられており、「ガイダンス」も NIST の”Working Definition of Cloud Computing (NIST SP800-145)に準じることとする。それにより、意味論的な推敲より実事例に焦点を当てた共通言語を確立して、一貫性とコンセンサスを確保することを目指している。

この「ガイダンス」は広く活用され、世界中の組織に適用可能であることを意図していることに留意しなければならない。NIST は米国政府機関であるが、そのリファレンスモデルを選択することが他の見方や他国のものを排除するものでないことに留意が必要である。

訳注1　日本語訳に際しては、文脈上有意の差を認めなかったために、user, consumer, customer, client の語は基本的に「クラウド利用者」（例外的に単に「利用者」）とし、provider は「クラウド事業者」（例外的に単に「事業者」とした。また service, cloud については文脈によるが、基本的にはそのまま訳している。）

訳注2　“orchestration”は、原則として、文脈に応じて「統合管理」または「統合化」の訳語を当てる。

NIST はクラウドコンピューティングの定義に際して、5 つの基本的特性、3 つのサービスモデル、4 つの配備モデルを用いている。それらは図に要約されており、以下に詳述されている。



1.1.2.1 基本的特性

これらはクラウドをクラウドたらしめている特性である。もし何かがこれらの特性を備えているなら、それはクラウドコンピューティングであると考える。それがこれら特性のいずれかを欠いていたら、クラウドでない可能性が高い。

- 上述したように、**リソースの共用**は最も基本的な特性である。クラウド事業者はリソースを抽象化してプールの中に集合させ、その一部が（通常はポリシーに基づいて）複数の利用者に割り当てられる。
- 利用者はプールから割り当てられたリソースを、**オンデマンド・セルフサービス**によって割り付ける。利用者はリソースの管理を自分ででき、管理者と話す必要がない。
- **幅広いネットワークアクセス**が意味するところは、リソースがネットワークを介して利用可能であって、物理的に直接接触する必要がないことを意味するが、ネットワークはサービスの一部である必要はない。
- **スピーディな拡張性**によって、利用者はプールから取り出して使うリソースを拡張したり追加したり（割付けと割付けの解放）できる。しかも多くの場合完全自動で。これにより、利用者はリソースの利用をより精密に需要量に合わせられる。（例えば、需要が増えたら仮想サーバを追加し、需要が落ちたらそれらを立ち下げる。）
- **サービスが計測可能**であることにより、何が提供されているか測定でき、利用者が割り当てを受けたものだけを使用していることを確認できると同時に、必要に応じて課金できる。ここから、**ユーティリティ・コンピューティング**の用語が生れるわけだが、何故ならコンピューティングリソースはあたかも水道や電気のように使うことができ、利用者は使った分だけ払えばいいからである。

ISO/IEC17788 はカギとなる 6 つの特性を挙げているが、最初の 5 つは NIST の特性と同等である。唯一追加されているのはマルチテナント性であり、これはリソースをプールすることから自明である。

1.1.2.2 サービスモデル

NIST はクラウドサービスの基本的な分類について説明する 3 つのサービスモデルを定義している。

- **Software as a Service (SaaS)**は事業者がホストし管理する丸ごとのアプリケーションである。利用者は、Web ブラウザ、モバイルアプリまたは軽量のクライアントアプリからアクセスする。
- **Platform as a Service (PaaS)**は開発環境またはアプリケーションのプラットフォームを抽象化して提供する。例としては、データベース、アプリケーションプラットフォーム（つまり Python、PHP、その他のコードが走る場所）、ファイルの保存と共有、更には個別のアプリケーション処理（例えば機械学習、ビッグデータ処理、SaaS アプリへの直接アクセス API）まである。PaaS における特徴の鍵となるのは、利用者が下位層のサーバ、ネットワークその他のインフラを管理しないということである。
- **Infrastructure as a Service (IaaS)**は CPU、ネットワーク、ストレージのような基本的なコンピューティングインフラのリソースプールへのアクセスを提供する。

これらは"SPI"階層と呼ばれることがある。

ISO/IEC は**クラウド機能タイプ(cloud capability type)**としてより複雑な定義をしている。そのマッピングは SPI 階層（アプリケーション、インフラストラクチャ、プラットフォームの機能タイプ）に密接に対応している。そこからより細密な**クラウドサービスタイプ**を展開しており、Compute as a Service、Data Storage as a Service に加えて、IaaS/PaaS/SaaS も含めている。

これらのカテゴリ分けは幾分かの緩みを含んでいる。ある種のクラウドサービスはこれら階層をまたがっており、他のものはうまく単一のサービスモデルに収まらない。実際問題としては、全てをこれら 3 つの階層、あるいはさらに細かい ISO/IEC モデルの階層にはめ込もうとしなければならない理由はない。これは単に説明のために役立つツールであって、厳密なフレームワークというわけではない。

どちらのアプローチも同様に有効であるが、NIST のモデルが簡潔で現状広く使われているので、CSA の調査研究における主たる定義とする。

1.1.2.3 配備モデル

NIST と ISO/IEC は共に 4 つのクラウド配備モデルを用いている。これらは技術がどのように配備され使われるのかを示しており、全てのサービスモデルに適用可能である。

- **パブリッククラウド** クラウドのインフラストラクチャはクラウドサービスを売る組織の所有で、一般向けもしくは大規模産業グループ向けに利用可能にされる。
- **プライベートクラウド** クラウドのインフラストラクチャは単一の組織専用で運用される。管理はその組織が行う場合も第三者の場合もあり、設置場所は組織の所在場所内または別の場所となる。
- **コミュニティクラウド** クラウドのインフラストラクチャは複数の組織で共有され、共通の関心事（使命、セキュリティ上の必要、ポリシーまたは法令遵守の観点から）をもつ特定の共同体のために使われる。管理はその共有組織が行う場合も第三者の場合もあり、設置場所は組織の所在場所内または別の場所となる。
- **ハイブリッドクラウド** クラウドのインフラストラクチャは 2 つ以上のクラウド（プライベート、コミュニティまたはパブリック）から成り、各クラウドは独立した主体であるが、標準的もしくは専用の技術で相互に結合しており、データとアプリケーションの相互可搬性を確保している（例えば負荷分散のためのクラウドバースティング）。ハイブリッド構成はまた、非クラウド型データセンタがクラウド事業者に直結している姿を現すのにも広く用いられる。

配備モデルはクラウド利用者、すなわち「誰がクラウドを使うのか」ベースの定義となっている。下図が示すように、クラウドの所有者と管理者は、単一の配備モデルの中でも一律とは限らない。

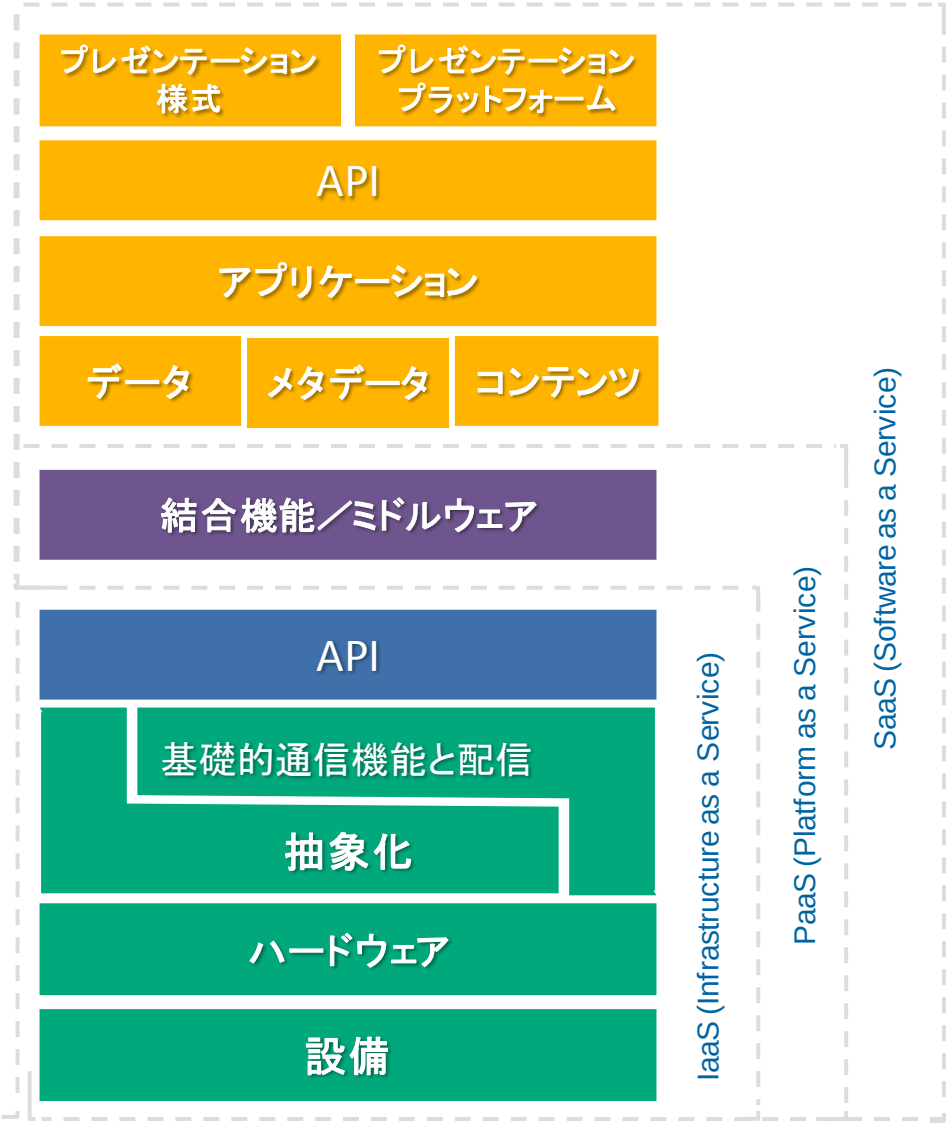
	インフラの管理者[1]	インフラの所有者[2]	インフラの所在場所[3]	アクセス者利用者[4]
パブリック	第三者の事業者	第三者の事業者	オフプレミス	トラストなし
プライベート/コミュニティ	組織 第三者の事業者	組織 第三者の事業者	オンプレミス オフプレミス	トラストあり
ハイブリッド	組織と第三者の事業者	組織と第三者の事業者	オンプレミスとオフプレミス	トラストありとトラストなし

1 管理には以下を含む：ガバナンス、運用、セキュリティ、コンプライアンス、その他
2 インフラストラクチャには設備など物理的インフラ、コンピュータ、ネットワーク、ストレージの装置を含む
3 インフラストラクチャの所在場所は物理的に組織の管轄下にあるかと、所管責任と管理の二つの意味がある
4 トラストのあるサービス利用者とは、組織の法的、契約上、または指揮命令関係の下に位置するもので、従業員、下請事業者、ビジネスパートナーが含まれる。トラストのない利用者とは、サービスの一部または全部の利用を認められているが、組織の支配の及ぶ範囲内にない者である。

1.1.3 クラウドのリファレンスモデルとアーキテクチャモデル

今日ではクラウドサービスを構築する技術的手法は多岐にわたり、絶えず進化を遂げている。その結果、単一のリファレンスモデルやアーキテクチャモデルを作ることは最初から時代遅れのものとなる。このセクションの目的は、セキュリティの専門家が情報に基づく意思決定を行うために役立つ基本的事項をいくつか提供することと、新しいより複雑なモデルを理解するための基礎知識を提供することである。より深い構造リファレンスモデルは、やはり ISO/IEC17789 と NIST SP500-292 がお薦めであり、これらが上記の NIST の定義モデルを補ってくれる。

クラウドコンピューティングの見方の一つはスタックモデルで、SaaS が PaaS の上に形成され、PaaS は IaaS の上に形成される形である。これは全て（あるいはほとんど）の実際の配備の姿を示すものではないが、説明を始めるのに役立つ参考図を提供してくれる。



1.1.3.1 Infrastructure as a Service

IaaS の基盤は、物理的設備とインフラストラクチャハードウェアで構成される。クラウドコンピューティングにおいて、これらのリソースは抽象化されるが、その構築は最も基礎的なレベルでは必ず物理的ハードウェア、ネットワーク、ストレージが必要となる。これらのリソースは抽象化と統合管理を用いてプールされる。ほとんどの場合仮想化によって行われる抽象化は、リソースのプールを実現するに際しての物理的制約から解放する。続いて、コアとなる相互接続と供給のツールのセット（つまり統合管理）が、抽象化されたこれらリソースを束ね、プールを形成し、更にそれを自動的に利用者に届ける機能を提供する。

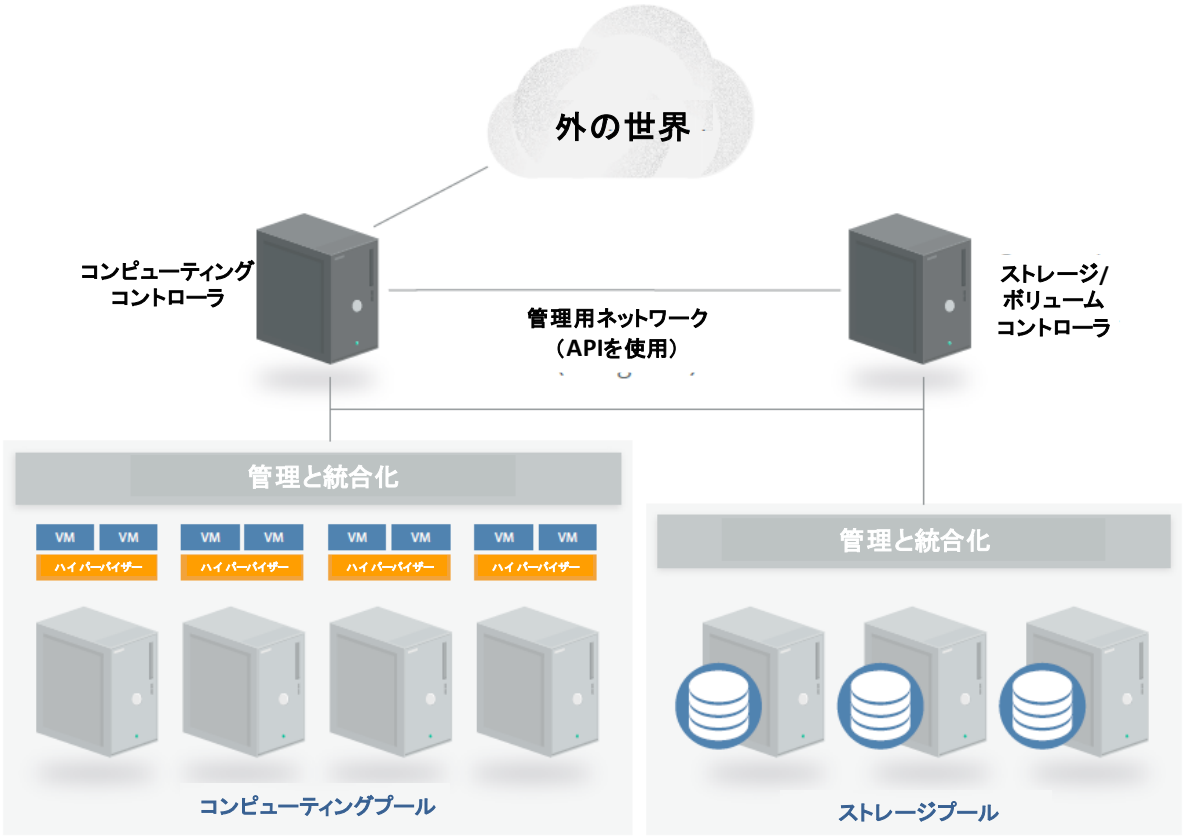
これら一連の流れは **API** によって簡単に使えるようになっている。API は通常、クラウド内部にあるコンポーネント間の通信手段で下に隠れているが、一部（または全く別のセット）はクラウド利用者に見えるようになっていて、利用者が使うリソースや設定の管理に使われる。今日、ほとんどのクラウドの API は REST(Representational State Transfer)を用いており、これは HTTP プロトコルの上で動作して、インターネットサービスに極めてうまく適合するものである。

ほとんどの場合、これらの API はリモートからアクセス可能で、Web ベースのユーザインタフェイスに組み込まれている。この組合せが**クラウド管理用ダッシュボード(cloud management plane)**である。なぜなら利用者は、仮想マシン（インスタンス）を走らせたり仮想ネットワークを設定したりといった、クラウドリソースの管理や設定にこれを使うからである。セキュリティの視点からは、これは物理的インフラストラクチャの防御と最も

大きく異なる点（なぜなら防御策として物理的アクセス制御を使えない）であり、またクウラドのセキュリティプログラムを考える上での最優先課題となる。もし攻撃者が管理画面に侵入できたならば、クラウド上の全ての資源に遠隔からあらゆるアクセスが可能になってしまう。

まとめると、IaaS は、設備、ハードウェア、抽象化レイヤ、抽象化されたリソースを束ねる統合管理（コアとなる相互接続と供給の機能）、および、遠隔からリソースを管理して利用者に届けるための API から成っている。

下図はコンピューティング IaaS プラットフォームの簡略化した構造の例である。



この図はたいへん簡略化したもので、統合管理のためのコンピューティングおよびストレージのコントローラ、抽象化のためのハイパーバイザ、CPU とストレージのプールの関係を示している。図ではネットワーク管理など多くのコンポーネントが省略されている。

いくつかの物理サーバがあり、各々がハイパーバイザ（抽象化用）と管理／統合管理ソフトウェアの二つのコンポーネントを走らせて、サーバを束ね、それらサーバをコンピューティングコントローラに接続している。利用者はあるサイズのインスタンス（仮想サーバ）を要求し、クラウドコントローラはどのサーバが余力を持っているかを判断して要求されたサイズのインスタンスを割り当てる。

続いて、コントローラはストレージコントローラにストレージのリクエストを出して仮想ハードドライブを形成する。ストレージコントローラはストレージプールからストレージを割り当て、ネットワーク（ストレージトラフィック専用のネットワーク）経由で該当するホストサーバとインスタンスに接続する。ネットワーク（仮想ネットワークとアドレスを含む）もまた割当てが行われ、必要な仮想ネットワークに接続される。

コントローラは続いて、仮想マシンにサーバイメージのコピーを送り込み、ブートし、設定を行う。これにより仮想マシン(VM)上で走るインスタンスが形成され、仮想ネットワークとストレージが割り当てられ、全体が適切にコンフィギュアされる。この一連のプロセスが完了すると、メタデータと接続情報がクラウドコントローラの仲立ちによって利用者に利用可能となり、利用者はインスタンスに接続してログインできるようになる。

1.1.3.2 Platform **as a Service**

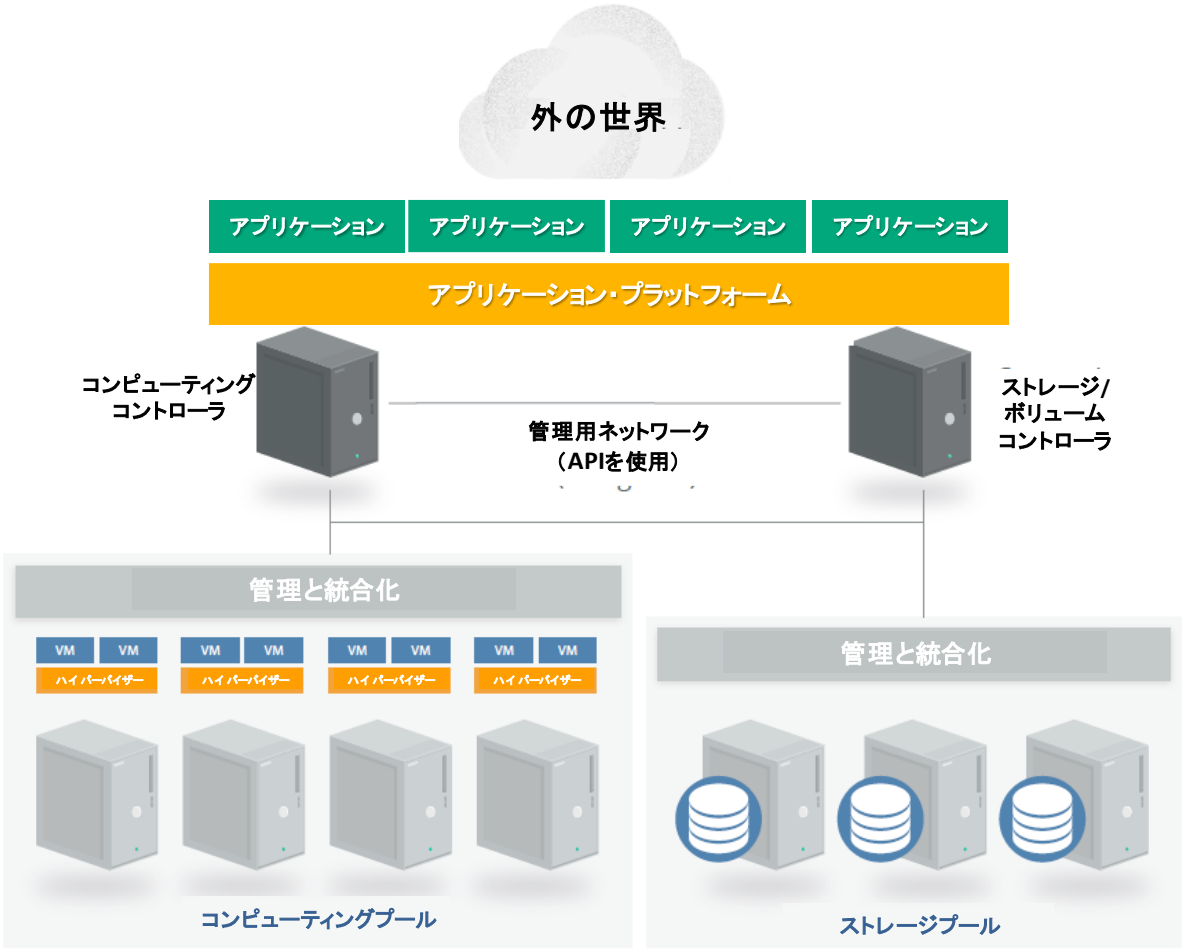
サービスモデルの中で、**PaaS** が最もその特性を定義するのが難しい。なぜならば、PaaS のサービスは多岐にわたるとともに PaaS のサービスを構成する手法もさまざまだからである。PaaS はアプリケーション開発用フレームワークとミドルウエア機能からなる付加レイヤと、データベースやメッセージングやキューなど様々な機能を提供する。これらのサービスにより、開発者は PaaS のスタックがサポートするツールやプログラミング言語を用いて、プラットフォーム上にアプリケーションを構築する。

実際にしばしば使われるオプションで本書のモデルにも示されているのは、IaaS の上にプラットフォームを構築する形である。インテグレーションとミドルウエアのレイヤは IaaS の上に形成され、しかる後にプールされ、統合され、API を通じて PaaS として利用者に示される。例えば、Database as a Service は、IaaS 上で走るインスタンスの上に、変更を加えたデータベースマネジメントソフトウェアを実装することで構築される。利用者はデータベースを API（および Web コンソール）を通じて管理し、通常のデータベースネットワークプロトコルか、再び API を通じてアクセスする。

PaaS では、クラウド利用者はプラットフォームだけが見え、その下層のインフラストラクチャは見えない。本書で示す例では、データベースは利用の度合いに応じて拡張（または追加契約）され、その際利用者は個別のサーバやネットワークやパッチなどを管理する必要がない。

他の例としては、アプリケーション開発プラットフォームがある。それは開発者が下層のリソースを管理することなくアプリケーションコードをロードして走らせることができる場所である。PaaS にはほとんどどんな種類のアプリケーションをどんな言語によってでも走らせられるサービスがあり、サーバの構築や設定、そのアップデート、クラスタリングやロードバランスなどの複雑な些事といった作業から開発者を解放する。

下図は模式化した構成図で、アプリケーションプラットフォームが本書で示す IaaS の上で走る形（PaaS）を示している。



PaaS は必ずしも IaaS の上に構築されるとは限らない。個別設計のスタンドアローンのアーキテクチャであっていけない理由は何もない。定義上の特性は、利用者はプラットフォームにアクセスしてそれを管理することであって、その下のインフラストラクチャ（クラウドインフラを含む）にアクセスしないということである。

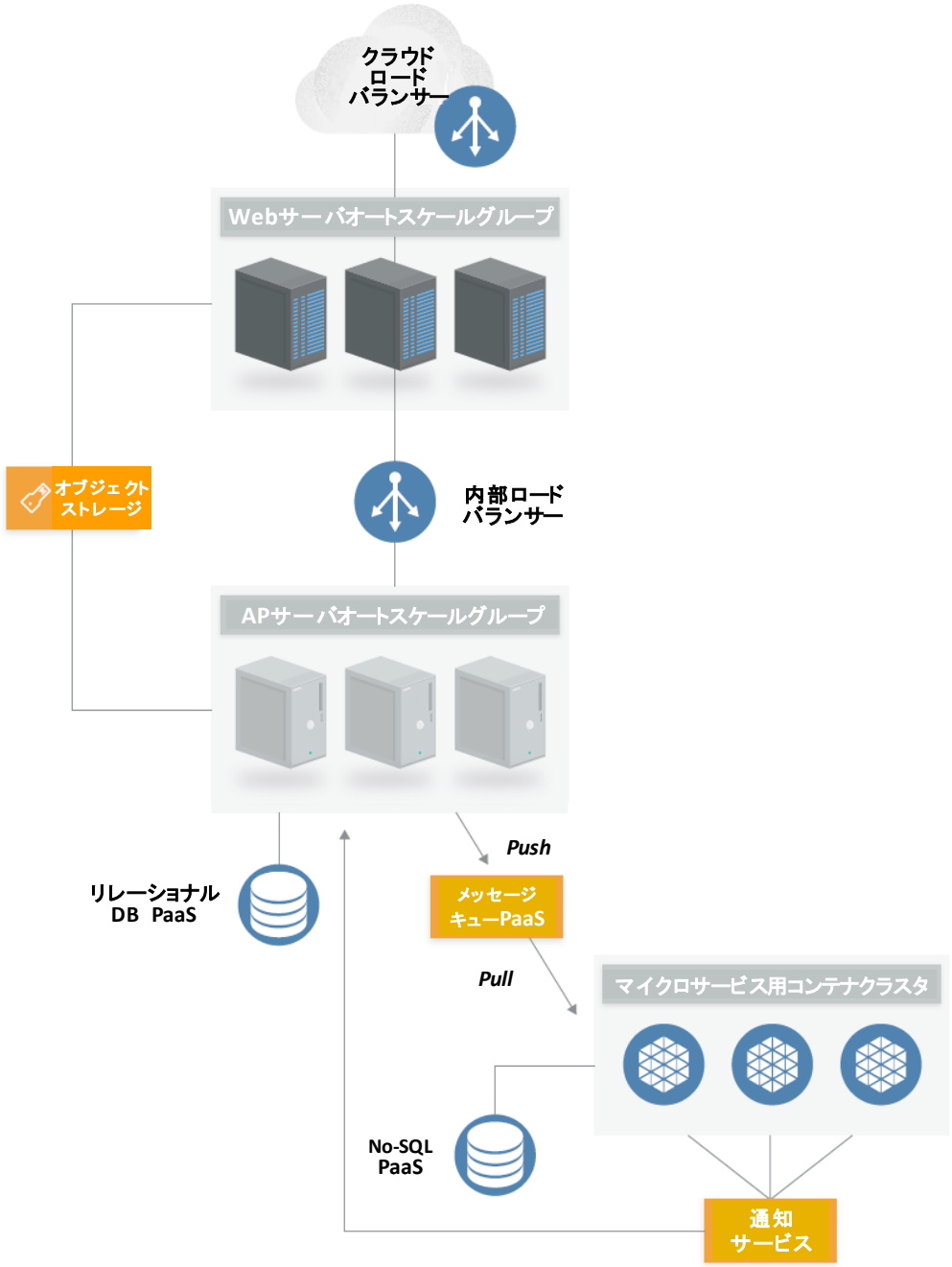
1.1.3.3 Software as a Service

SaaS サービスは、全て盛り込んだマルチテナントのアプリケーションで、どんなに大きなソフトウェアプラットフォームでも、そのアーキテクチャ的複雑さは全て取り込まれている。SaaS 事業者の多くは SaaS を IaaS および PaaS の上に構築する。それは機動性、耐障害性、そして（潜在的な）経済性のメリットのためである。

最新のクラウドアプリケーション（SaaS であれ何であれ）のほとんどは、IaaS と PaaS を組み合わせて使っており、それは場合によっては複数のクラウド事業者にまたがっている。同じく多くのものが機能の一部（または全部）に公開型 API を使う傾向にある。これは、様々な種類のクライアント、特に Web ブラウザやモバイルアプリケーションへのサポートが必要だからである。

従って、全ての SaaS が、API を最上位において、アプリケーション／ロジックレイヤーを備えることになる。そして、1 層または多層のプレゼンテーションレイヤーが置かれ、それはしばしば Web ブラウザやモバイルアプリケーションや公開 API を含んでいる。

下に示す単純化した構成図は実際の SaaS プラットフォームからとったもので、特定の製品名を省くための一般化を施してある。



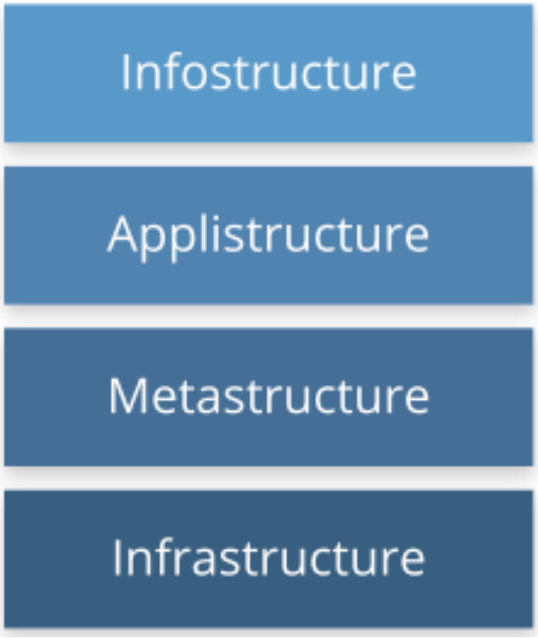
1.1.4 論理モデル

俯瞰的に見れば、クラウドも古典的コンピューティングも、階層分けを機能に基づいて行うという、一つの論理モデルに依拠している。これはいくつかのコンピューティングモデルの間の差を示すのに有効である。

- **インフラストラクチャ：**コンピューティングシステムの基本構成要素：CPU、ネットワーク、ストレージ。その他の全てがその上に形成される基盤。（物理的に）動作する部分である。
- **メタストラクチャ：**インフラストラクチャレイヤーと他のレイヤの間のインターフェイスを提供するプロトコルおよびメカニズム。各技術の間を結び付ける「のり」で、管理と設定を実現する。
- **インフォストラクチャ：**データと情報。データベース、ファイルストレージその他の中身。

- **アプリストラクチャ：**クラウド上に展開されたアプリケーションと、その構築のために使われる下層のアプリケーションサービス。例としてはメッセージキューのような PaaS の機能、人工知能分析、通知サービスなど。

セキュリティはその対象の違いにより、異なった論理レイヤにマップされる。アプリケーションセキュリティはアプリストラクチャに、データセキュリティはインフォストラクチャに、インフラセキュリティはインフラストラクチャに、といった具合である。



従来型コンピューティングとクラウドの根本的な違いはメタストラクチャにある。クラウドのメタストラクチャは管理画面のコンポーネントを含んでおり、それはネットワーク対応されていて、遠隔からアクセス可能である。ほかの基本的差異は、クラウドにおいては、各レイヤーで二重利用がなされることである。例えばインフラストラクチャは、クラウドを形成するのに使われるものと、クラウド利用者が使用し管理する仮想インフラストラクチャの両方がある。プライベートクラウドでは、同じ組織が両方の面倒を見なければならない。パブリッククラウドでは、クラウド事業者が物理インフラを管理し、利用者は自分の仮想インフラを管理する。

後に見るように、このことは誰がセキュリティを管理し責任を持つかについて意味深い示唆を含んでいる。

これらのレイヤは、IT 組織において一般に見られるチーム分け、規則区分、技術区分に対応づけることができる。セキュリティ管理に関する最も直接的ではっきりした違いはメタストラクチャにあるが、クラウドでは各レイヤごとに従来型コンピューティングとは大きく異なる。その差異の程度は、クラウドプラットフォームのみならず、まさに、クラウド利用者がどのようにプラットフォームを利用するのかによっている。

例えば、クラウド事業者の PaaS サービスを密度濃く活用するクラウドネイティブのアプリケーションは、既存のアプリケーションを最低限の変更で IaaS に移行した場合と比べて、アプリストラクチャにおいて大きな差が生じる。

1.2　クラウドセキュリティの範囲、責任およびモデル

1.2.1　クラウドにおけるセキュリティとコンプライアンスの範囲と責任

話は単純に聞こえるかもしれないが、クラウドのセキュリティとコンプライアンスは、セキュリティチームが今日責任を負うべき全てのものを含んでいる。それがクラウドにおいて、ということに過ぎない。全ての従来からあるセキュリティの要素はそのままある。しかし、**リスク、役割、責任の性質と対策の実装**は、従来型と異なっている。それも多くの場合、劇的に。

セキュリティとコンプライアンスの全体像は変わらないが、各部とクラウド関係者の責任は間違いなく変化する。こう考えてみるといい。クラウドコンピューティングは技術的共有のモデルであって、様々な組織が各々の責任

で、セキュリティの様々な要素について頻繁に実装と管理を行っている世界であると。結果として、セキュリティに関する責任は各要素に分散し、それはつまり全ての組織にまたがって存在することになる。

このことはしばしば、**責任共有モデル**と呼ばれる。つまり、あるクラウド事業者の機能や商品、そのサービスモデル、そして配備モデルの組合せ全般におよぶ責任のマトリクスである。

全体的に言って、セキュリティの責任は、あるクラウドの関係者がアーキテクチャの全階層に対して適用する管理策の程度に対応づけられる。

- **Software as a Service**：クラウド事業者はほとんど全てのセキュリティに対して責任を負う。なぜならクラウド利用者は自分の利用するアプリケーションにだけアクセスして管理するのであり、アプリケーションがどう機能するかについてはさわれないからである。例えば、SaaS 事業者はネットワーク境界のセキュリティ、ロギング／モニタリング／監査、アプリケーションセキュリティについて責任を負い、一方利用者は、せいぜい利用権とその付与の管理ができる程度に過ぎない。
- **Platform as a Service**：クラウド事業者がプラットフォームのセキュリティに責任を負う一方、利用者はクラウド上に実装した全てのものについて、提供されたセキュリティ機能をどのように設定したかも含めて、責任がある。従い、責任の分担はよりイーブンになる。例えば、Database as a Service を利用する場合、事業者は基本的セキュリティ、パッチ当て、基本的設定に責任があり、クラウド利用者はその他全て、例えばデータベースのどのセキュリティ機能を使うか、アカウントの管理、更には認証手段にまで、責任を負う。
- **Infrastructure as a Service**：PaaS と同様、事業者は基本的なセキュリティに責任を負う一方、クラウド利用者はインフラストラクチャの上に構築された全てに対して責任を負う。PaaS と異なり、このことは利用者に極めてより多くの責任を課す。例えば、IaaS の事業者はネットワーク境界で攻撃を見張りはするだろうが、利用者はその仮想ネットワークのセキュリティを、そのサービス上で利用可能なツールを使って、どう定義し実装するかの全責任を負っている。

これらの役割は、クラウドブローカーその他の仲介機能やパートナーを利用する場合はさらに一層複雑になる。

いかなるクラウドプロジェクトであれ、最も重要なセキュリティ上の注意点は、だれが何に責任を負うのかを的確に把握することである。あるクラウド事業者が特別なセキュリティ対策を提供するということは、何が提供されどのように機能するかを正確に知ってさえいれば、相対的に重要度は低い。自前の対策でギャップを埋めることも、対策ギャップを埋めきれない場合は別の事業者を選ぶこともできるのだから。このことは IaaS ではたいへんよく実現でき、SaaS ではそれほどでもない。

これがクラウドの事業者と利用者のセキュリティ責任の関係についての基本的ポイントである。事業者は何をするのか？利用者は何をする必要があるのか？クラウド事業者は利用者が必要なことをできるようにしてくれるのか？何が契約とサービスレベルアグリーメントで保証され、技術説明書と仕様で何が暗黙裡に示されているのか？

この責任共有モデルは、2 つの推奨事項に直結する。

- **クラウド事業者**は、内部のセキュリティ対策と利用者向けのセキュリティ機能をはっきりと文書で示し、クラウド利用者が情報に基づく意思決定をできるようにすること。事業者はまた、それらセキュリティ対策を適切に設計し実装しなければならない。
- **クラウド利用者**は、クラウドプロジェクトに際し、責任分担表を作成して誰がどの対策をどのように実装する必要があるのかを文書で示さなければならない。これは同時に、必要な準拠すべき基準に対応していなければならない。

CSA では、これらの要求事項に対応する 2 つのツールを提供している。

- Consensus Assessments Initiative Questionnaire (CAIQ)　標準的なテンプレートで、クラウド事業者が自社のセキュリティとコンプライアンスの対策を文書で示すことができる。
- Cloud Control Matrix (CCM)　クラウドセキュリティの管理策のリストであり、複数のセキュリティおよび遵守基準に対するマッピングを行っている。CCM はまた、セキュリティ責任を文書化するために利用することもできる。

これら文書はいずれも、特定の組織やプロジェクトの要件に沿ってチューニングが必要な場合はあるが、網羅的な、取っ掛かりとなるテンプレートで、特に法令・基準遵守義務を満たしているかを確認するために特に有用である。

1.2.2　クラウドセキュリティモデル

クラウドセキュリティモデルは、セキュリティの意思決定を支援するツールである。「モデル」という言葉は、やや漠然とした意味で使われるので、この場の目的としては、以下のタイプに分けることとする。

- **概念的モデルもしくは枠組み：**クラウドセキュリティの概念と原則を説明するために使われる可視化および記述で、本書における CSA 論理モデルなど。
- **管理策モデルもしくは枠組み：**個別のクラウドセキュリティ管理策もしくは管理策のカテゴリを詳述しまたはカテゴリ分けするもの。例えば CSA の CCM。
- **リファレンスアーキテクチャ：**クラウドセキュリティ実装のテンプレートで通常は一般化してある（例：IaaS セキュリティリファレンスアーキテクチャ）。高度に抽象的なもの、コンセプトに近いもの、あるいはかなり詳細なもの、更には個別具体的管理策や機能のリストまである。
- **デザインパターン：**特定の問題に対する再利用可能な解決策。セキュリティに関しての例としては IaaS のログ管理がある。リファレンスアーキテクチャと同様に、抽象的であったり具体的であったり、更には特定のクラウドプラットフォーム上の汎用実装パターンであったりする。

これらモデルの間の境は、モデルの作成者の目的次第で、あいまいであったり重なったりすることがよくある。これらを全てまとめて「モデル」という見出しの下にくくることすら、おそらく不正確である。しかし、登場する場所によって、使われる言葉が相互に入れ替え可能であるケースを見かけることから、グループ分けする意味はあると考えている。

CSA としては、以下のモデルを検証した。これらを推奨する。

- CSA Enterprise Architecture
- CSA Cloud Controls Matrix
- NIST Cloud Computing Security Reference Architecture (NIST SP500-299) <draft>　－概念モデル、リファレンスアーキテクチャ、管理策枠組を含む－

- ISO/IEC 27017[3] Information Technology – Security techniques – Code of practice for information security controls based on ISO/IEC27002 for cloud services.

本書においては、その他のドメインごとのモデルについても触れる。

1.2.2.1 単純化したクラウドセキュリティプロセスモデル

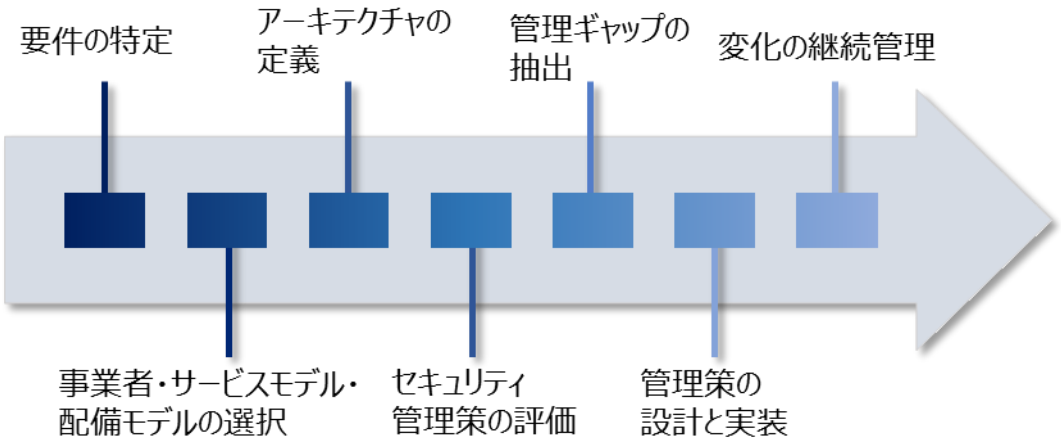
実装の詳細や、必要な管理策や、特定のプロセスや、更にはリファレンスアーキテクチャやデザインモデルは、個別のクラウドプロジェクトごとに大きく異なるが、クラウドセキュリティの管理に関して比較的簡単で概括的なプロセスをいくつか挙げることができる。

- 必要なセキュリティとコンプライアンスの要件を明確にし、実施済みの管理策を確認する。
- クラウド事業者、クラウドサービスの種類、クラウドの配備モデルを選択する。
- アーキテクチャを決定する。
- （実装済みの）セキュリティ管理策を評価する。
- 管理策に存在するギャップを明らかにする。
- ギャップを埋めるための管理策を設計し実装する。
- 変化に対応する管理を継続的に行う。

クラウドプロジェクトが異なると、たとえ同じクラウド事業者の上であっても、まったく異なる技術と設定の組合せを用いることになる可能性が高いので、各プロジェクトは各々の個別のメリットをもとに評価するべきである。例えば、ある事業者による純粋の IaaS 上に配備されたアプリケーションのためのセキュリティ管理策は、同じ事業者による PaaS をより多く用いた類似のプロジェクトと大きく違って見える可能性がある。

鍵となるのは、要求条件を特定し、アーキテクチャを設計し、その上で下層にあるクラウドプラットフォームの能力に応じてギャップを洗い出すことである。これが、セキュリティ要件を管理策に展開する前に、クラウド事業者とそのアーキテクチャを知らなければならない理由である。

訳注3　原文は FDIS と表記しているが、すでに国際規格として発行されているので外した。なお、リンク先は原文も発行済み IS のページの URL となっている。



1.3 焦点を当てるべき重要領域

本ガイダンスを構成する以下の 13 のドメインは、CSA ガイダンスがクラウドコンピューティングにおいて焦点を当てるその他の関心領域を扱っている。それらは、クラウド環境におけるセキュリティの「課題」について、戦略的および戦術的観点から焦点を当てるように作られており、その意味で全てのクラウドのサービスモデルと配備モデルに適用可能なものとなっている。

これらのドメインは、大別して 2 つのカテゴリに区分される。ガバナンスと運用である。ガバナンスのドメインは広範囲にわたり、クラウドコンピューティング環境における戦略的および政策的課題を取り扱い、運用関係のドメインはアーキテクチャにおけるより戦術的なセキュリティ課題とその実装に焦点を当てている。

1.3.1 クラウドにおけるガバナンス

ドメイン	ドメイン名	内容
2	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よってもたらされるエンタープライズリスクを定量化し統制する組織の能力。契約違反に際しての法務上の優位性、クラウド事業者にまつわるリスクを適切に評価する利用組織の能力、利用者と事業者が共に異常な場合の機密情報保護の責任、そして国の違いがこれらの問題に与える影響、などがある。
3	法的課題：契約と電子証拠開示	クラウドコンピューティングを利用する際に起こりうる法的問題。この章で取り上げる課題には、情報とコンピュータシステムの保護のための要求事項、セキュリティ侵害が起きた場合の開示に関する法務、公的規制、プライバシーに関する要求事項、および国際法務などがある。
4	コンプライアンスと監査マネジメント	クラウドコンピューティングを利用する際のコンプライアンスの実現と維持。課題としては、組織のセキュリティポリシーにクラウドコンピューティングがどのように影響するかの評価や、その他のコンプライアンス（公的、法的その他の規制）の要求事項を取り上げる。このドメインでは、監査におけるコンプライアンスの確保に関する方向づけにも触れる。
5	情報ガバナンス	クラウド上に置かれるデータのガバナンス。クラウド上のデータの特定と管理にまつわる事項、データをクラウド上に移行するに際して失われる物理的管理策を補完するのに利用可能な管理策について論じる。データの機密性・完全性・可用性に関する責任の帰属といった他の事項にも触れている。

1.3.2　クラウドにおける運用

ドメイン	ドメイン名	内容
6	管理画面と事業継続	クラウドにアクセスする際の管理画面と管理インターフェイス（Web コンソールも API も含む）のセキュリティ。クラウドの配備における事業継続の確保。
7	インフラストラクチャ・セキュリティ	クラウドの中核的なインフラストラクチャのセキュリティ。ネットワーク接続、ワークロードセキュリティおよびハイブリッドクラウドに関する留意事項を含む。このドメインでは、プライベートクラウドにおけるセキュリティの基礎も扱う。
8	仮想化とコンテナ技術	ハイパーバイザ、コンテナ、SDN(Software Defined Network)のセキュリティ
9	インシデント対応、通知および被害救済	インシデントに際しての適切かつ十分な検知、対応、通知および影響緩和措置。インシデント対応とフォレンジックスを適切に行うために事業者、利用者各々が行うべき事項の指摘を試みる。このドメインは、オンプレミスにおけるインシデント対応プログラムがクラウド環境でどれほど複雑になるか理解するのに役立つと期待される。
10	アプリケーションセキュリティ	クラウド上で実行中のまたはクラウド上で開発されるアプリケーションソフトウェアのセキュリティ。あるアプリケーションをクラウドで走るように移行または設計することが正しいかどうかに関する諸点や、そうする場合にどのプラットフォーム（SaaS、PaaS、IaaS）が適切かについて述べる。
11	データセキュリティと暗号化	データセキュリティと暗号化の導入および目的に見合った鍵管理
12	アイデンティティ、権限付与、アクセスの管理	アイデンティティ管理とアクセス制御を実施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管理をクラウド環境まで拡張する際に直面する課題に焦点を当てる。組織がクラウドベースの IdEA（Identity, Entitlement, and Access Management：アイデンティティ、権限付与、アクセス管理)を実施可能な状態にあるかを評価するための視点を提供する。
13	Security as a Service	第三者が用意し実施する、セキュリティ確保、インシデント対応、コンプライアンス検証、アイデンティティ・アクセス管理。
14	関連技術	クラウドコンピューティングに密接な関係がある既存のおよび新興の技術。Big Data, IoT, Mobile Computing など。

1.4　推奨事項

- クラウドコンピューティングと従来型のインフラストラクチャまたは仮想化との違いを理解すること。併せて抽象化と自動化がいかにセキュリティに影響を与えるか理解すること。
- NIST のクラウドコンピューティングモデルと CSA のリファレンスアーキテクチャに精通すること。
- クラウド事業者を比較評価するに際しては、CSA の CAIQ (Comsensus Assessments Initiative Questionnaire)などのツールを活用すること。
- クラウド事業者はそのセキュリティ管理策とセキュリティ機能を詳しく文書化し、CSA の CAIQ などのツールを活用して公表すること。

- CSA の CCM (Cloud Controls Matrix)のようなツールを用いて、クラウドプロジェクトのセキュリティ、コンプライアンス要件、管理策と、それら各々に関する責任の所在を評価し文書化すること。
- クラウドセキュリティプロセスモデルを用いて、事業者の選別、アーキテクチャの設計、対策ギャップの特定、セキュリティおよびコンプライアンス管理策の実装を行うこと。

1.5　出典の表記

- リファレンスアーキテクチャおよび論理モデルは Christofer Hoff の著作に依拠している。

DOMAIN 2
ガバナンスとエンタープライズリスクマネジメント

2.0　はじめに

ガバナンスとリスクマネジメントはとても広範囲にわたるトピックである。このガイダンスではそれがクラウドコンピューティングでどのように変わるかに焦点を当てる。つまり、クラウド外におけるこれらの課題に関して、初歩的あるいは包括的検討を行うものではないし、そのように解されるべきでない。

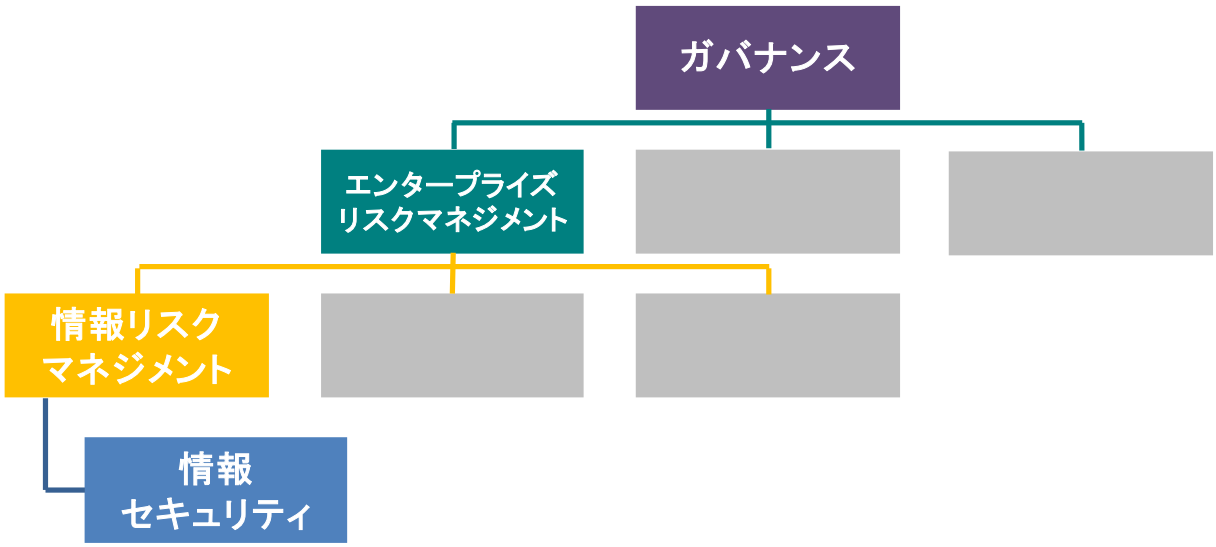
セキュリティの専門家にとって、クラウドコンピューティングは、ガバナンスとリスクマネジメントの 4 つの領域に影響を与える。

- **ガバナンス**は、組織がどのように運営されるかの枠組みである、ポリシー、プロセスおよび内部統制を含んでいる。組織構造およびポリシーからリーダーシップ、マネジメントのためのその他の仕組みまでのあらゆることを含んでいる。

ガバナンスについての更なる情報は下記参照。
* ISO/IEC 38500:2015 - 情報技術 - 組織の IT ガバナンス
* ISACA – COBIT - エンタープライズ IT のガバナンスおよびマネジメントのためのビジネスフレームワーク
* ISO/IEC 27014:2013 - 情報技術 - セキュリティ技術 - 情報セキュリティのガバナンス

- **エンタープライズリスクマネジメント**は、組織のガバナンスおよびリスク許容度との整合の下に、組織にとってのすべてのリスクを管理することである。エンタープライズリスクマネジメントの対象となるのは、ただ単にテクノロジに関係のあるものだけではなくリスクの領域のすべてである。
- **情報リスクマネジメント**は、情報（情報技術を含む）に対するリスクを管理することを対象にしている。組織は財務上のものから物理的なものまで、あらゆる種類のリスクに直面する。そして情報は、組織が管理する必要のある様々な資産のうちの 1 つに過ぎない。
- **情報セキュリティ**は、情報に対するリスクを管理するためのツールと実施事項である。情報セキュリティは、情報リスクを管理することの最重要事項ではない。ポリシー、契約、保険、その他の仕組みも同様に、(非デジタル情報の物理的セキュリティを含め)、一定の役割を果たす。とは言え、情報セキュリティの第一の（唯一ではないが）役割は、電子情報並びにそれへのアクセスに使用するシステムを保護するプロセスおよびコントロールを提供することにある。

単純化した階層構造で言えば、情報セキュリティは情報リスクマネジメントのツールであり、情報リスクマネジメントはエンタープライズリスクマネジメントのツールであり、エンタープライズリスクマネジメントはガバナンスのツールである。この 4 つは密接な関係にあるが、各々について対象、プロセス、ツールを必要とする。



2.1:リスクとガバナンスの単純化した階層構造

法的事項とコンプライアンスは各々ドメイン 3 と 4 でカバーされている。情報リスク管理とデータガバナンスはドメイン 5 でカバーされている。本ガイダンスのその他のドメインは基本的に情報セキュリティについて扱っている。

2.1 概要

2.1.1 ガバナンス

クラウドコンピューティングはガバナンスに影響を与える。パブリッククラウドやホストされたプライベートクラウドの場合には、ガバナンスのプロセスに第三者を組み入れることになるためであり、また社内でホストするプライベートクラウドの場合には内部のガバナンス構造を変化させる可能性があるためである。クラウドコンピューティングのガバナンスに際して留意すべき最重要の課題は、外部のクラウド事業者を使用する場合であっても、**組織はガバナンスの責任をアウトソーシングすることは絶対にできない**ということである。これは、クラウドであってもなくても常に真実であり、クラウドコンピューティングにおける責任共有モデルのコンセプトを適用していく場合に、頭に置いておくことが大事である。

クラウド事業者は、コストをコントロールし機能を実現するに際して規模の経済を活用しようとする。これは、すべてのクラウド利用者に適用可能な、極めて標準化されたサービス(契約およびサービスレベルアグリーメントを含む)を用意することを意味する。ガバナンスのモデルは、クラウド事業者と専任の外部サービス提供事業者とを同列に扱うことはできない。専任の外部サービス提供事業者の場合は通常そのサービスは、契約も含め、個別顧客ごとにカスタマイズされるからである。

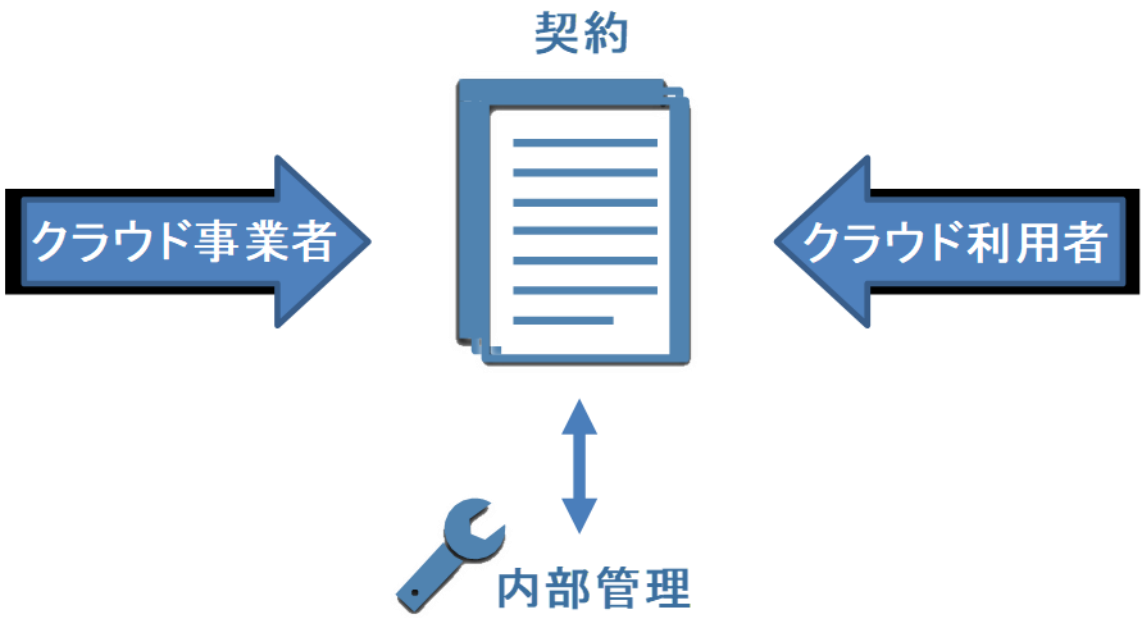
クラウドコンピューティングは、ガバナンスの実装および管理に対する**責任**と仕組みを変える。あらゆる取引関係と同様に、ガバナンスに対する責任および仕組みは契約の中で定義される。

重要な部分が契約にない場合、それを義務として守らせる仕組みはなく、そこにガバナンスギャップが生じる。ガバナンスギャップが必ずしもクラウドの利用を阻害するわけではないが、クラウド利用者は、ギャップを埋めるべく自身のプロセスを修正するか、あるいはギャップに伴うリスクを受容する必要がある。

2.1.1.1 クラウドガバナンスのツール

他の場合と同様に、ガバナンスのための固有の管理ツールがある。以下のリストは、外部のクラウド事業者に対するツールに重点を置いているが、これらのツールは、多くの場合組織内のプライベートクラウドの配備に対しても利用可能である。

- **契約：**ガバナンスの第一のツールは、クラウド事業者とクラウド利用者の間の契約である(パブリックでもプライベートクラウドでも)。契約は、全てのレベルのサービスや約束事に対する唯一の保障であり、契約違反がないことを想定するものであり、契約違反は全てを法的手続きに持ち込むことになる。契約は取引先企業やクラウド事業者へガバナンスを及ぼすための、第一のツールである。



> 契約は、クラウド事業者とクラウド利用者の関係を定義し、クラウド利用者がクラウド事業者に対してガバナンスを及ぼすための第一のツールである。

- **サプライヤ(クラウド事業者)に対する評価：** 評価は検討中のクラウド利用者が、利用可能な情報と承認されたプロセスや技術を使用して行うものである。評価は、第三者による評価証明(評価または監査の結果を表示するために一般に使用される法的な表明)についての契約ベースと手作業の調査と技術的な調査の組合せである。評価はサプライヤ評価に非常に似ており、財務の健全性、履歴、特色のアピール、第三者評価証明、同業者からのフィードバックなどのような要素を含むこともある。評価についての詳細は、以下このドメインと、ドメイン 4 でカバーされている。
- **コンプライアンス報告書：** コンプライアンス報告書には、クラウド事業者の内部(つまり自分による)および外部によるコンプライアンス評価についての全ての文書を含む。コンプライアンス評価は、組織が自身で実施するか、(クラウドでは通常行われないが)クラウド利用者がクラウド事業者に実施するか、あるいは信頼できる第三者によって実施される、コントロールの監査の報告書である。客観的な評価を提供するので、第三者による監査と評価アセスメントが望ましい(第三者を信頼すると仮定して)。

  コンプライアンス報告書は、一般的にはクラウドの利用を予定している者および（既存の）クラウド利用者が利用できるが、場合によっては、NDA の下で、もしくは契約を結んだクラウド利用者のみが利用可能である。そのようなことは一般に監査を実施した会社に要求されることが多いが、そのような報告書はクラウド事業者の完全な関与の下に作成されたものとは限らない。

評価や監査は、既存の基準(種類は多い)に基づくべきである。使用される基準だけでなく適用範囲を把握することは重要である。SSAE 16 のような基準には定義された適用範囲があり、そこには、**何が**評価されるか(クラウド事業者のサービスのうち何が)と、**どのコントロール**が評価されるかということが含まれる。その仕組み上、クラウド事業者は、セキュリティコントロールを全く含まない監査に「合格」することができるかもしれないが、

リスクマネジメントについての詳しい情報は以下を参照のこと。
* ISO 31000:2009 - リスクマネジメント---原則および指針
* ISO/IEC 31010:2009 - リスクマネジメント---リスクアセスメント技法
* [NIST SP800-37 Rev.1] (更新(2014 年 6 月 5 日)
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf)

それはセキュリティおよびリスクの管理者にとって全く役に立たない。同時に、第三者による評価を、自組織が自ら評価を行う場合に取る手続きと同等のものとして取り扱う場合には、他者に対する信頼が伴う必要があることに留意すること。すべての監査法人(あるいは監査人)が同じようなレベルにあるとは限らず、その法人の経験、経歴、および評価は、ガバナンスの判断に反映させることが望ましい。

Cloud Security Alliance の STAR 登録とは、CSA の Cloud Controls Matrix および Consensus Assessments Initiative Questionnaire(CAIQ) に基づくクラウド事業者評価のための保証プログラムと記録の登録制度である。クラウド事業者によっては、その他の認証や評価(自己評価を含む)についての記録も併せて開示している。

2.1.2 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、組織のリスクの総合的なマネジメントである。 契約においては、ガバナンスの場合と同様に、クラウド事業者とクラウド利用者の間のリスクマネジメントに対する役割と責任を定義する。そして、ガバナンスの場合と同様に、リスクマネジメントに対するすべての責任と説明責任を外部の提供事業者へアウトソーシングすることはできない。

クラウドにおけるリスクマネジメントは、**責任共有モデル**(セキュリティへの言及に際して最もよく語られる)に基づ

く。クラウド事業者は、一定のリスクに対する責任を負い、クラウド利用者はその先のすべてに責任を持つ。このことはサービスモデル間の違いを評価すれば明白で、SaaS においてはクラウド事業者が、IaaS においてはクラウド利用者がより多くのリスクを管理する。しかし、それでもなおクラウド利用者は、リスクを所管する最終的な責任を負っており、クラウド事業者には**リスクマネジメント**の一部を転嫁しているに過ぎない。これは自社ホスト型のプライベートクラウドにおいても該当する。その状況では、組織の中のある部署が、組織外の主体でなく内部のクラウド提供主体にリスクマネジメントの一部を転嫁しているのである。そして、内部の SLA および手順が外部との契約に代替する。

ERM においては、責任分界点がどこにあり、未対応のリスクの可能性がどこにあるかを示すためには、良い契約とドキュメンテーションが必要である。ガバナンスは、ほとんど契約の中でのみ取り扱われるが、リスクマネジメントでは、それらドキュメンテーションに基づいて、クラウド事業者の技術とプロセスの能力をより深く徹底的に調べることができる。例えば、契約に、ネットワークセキュリティを実際にどのように実装するかまで定義することはほとんどないであろう。クラウド事業者のドキュメンテーションのチェックによって、実効性のあるリスク判断をサポートする情報を非常に多く得ることができる。

リスク許容度は、組織の経営層および利害関係者が受け入れても良いと考えているリスクの量である。それは資産によって異なるので、特定のクラウド事業者に関して包括的なリスク判断を下すのではなく、リスク評価はむしろ、対象となる資産の価値と要求条件に整合させるべきである。 パブリッククラウド事業者が社外にあり、クラウド利用者が何かの資産について共有インフラであることに不安を感じるかもしれないということだけで、すべての資産についてリスク許容度内にないということを意味するわけではない。これが意味するものは、時間軸を加味して実務的に考えると、クラウドサービスと、そのサービスの利用を許容される資産のタイプの、マトリクスを形成していくことである。クラウドに移行することでリスク許容度が変わることはなく、リスクをどのように管理するかが変わるだけである。

2.1.3 サービスモデルおよび配備モデルの影響

クラウドサービス事業者においてだけでなく、クラウドサービスの基本的な提供において、利用可能な様々なオプションを考慮する際に、クラウドのサービスモデルと配備モデルによって、ガバナンスとリスクの管理機能が、どのような影響を受けるかに注意を払わなければならない。

2.1.3.1 サービスモデル

ソフトウェア アズ ァ サービス (SaaS)

大多数のケースでは、SaaS が交渉による契約が必要な最も重要な例である。交渉可能な契約によって、アプリケーションがデータを格納し、処理し、伝送することに関係のあるリスクをコントロールしたり確認したりする権利を確保できる。SaaS 事業者は、規模と能力において大小二極化する傾向にあり、小規模な SaaS 事業者を相手にする場合、交渉による契約を結べる可能性がとても高い。あいにく、小さな SaaS 事業者の多くは、クラウド利用者のガバナンスおよびリスクマネジメント能力と同等かそれ以上の高度な知識レベルで運用することはできない。実際問題として、SaaS アプリケーションを提供するインフラの運用の実態を可視化するレベルは、全体的に、そのクラウド事業者の開発によるユーザインタフェイスで見えるものだけに限られる。

プラットフォーム アズ ァ サービス (PaaS)

複数のサービスモデルを通じて連続的に、利用可能な詳細情報のレベル（それに伴ってガバナンスとリスクの課題を自ら管理できる能力)は増加する。完全に交渉による契約となるような可能性は、他のサービスモデルのいずれよりも低そうである。なぜならば、大部分の PaaS が目指す姿の主流は、高性能な単一の機能を提供するということだからである。

PaaS は、通常は多機能な API と共に提供され、また多くの PaaS クラウド事業者が、SLA が遵守されていることを証明するのに必要なデータのうちのいくつかの収集を可能にしている。これは、クラウド利用者が、大きな努力を払って、ガバナンスやリスクマナジメントの実行に必要なレベルのコントロールやサポートが、契約条項によって有効に提供されているかどうかを判断しなければならない立場にあることを意味する。

インフラストラクチャアズ ア サービス (IaaS)

インフラストラクチャアズアサービスは、クラウドが従来型のデータセンタ（あるいは、従来型の管理委託型データセンタ)に最も近い形を表しており、利点としては、組織が既に構築して利用している既存のガバナンスおよびリスクマネジメント活動の大部分が、直接移転可能であるということである。しかしながら、インフラストラクチャを機能させるために下位層にある統合化と管理の機能の複雑さの問題があり、それはしばしば見過ごされている。

多くの意味で、その統合化と管理の階層のガバナンスとリスクマネジメントは、従来型データセンタの下層にあるインフラ(ネットワーク、電力、冷暖房空調設備など)のそれと同じものである。同様のガバナンスおよびリスクマネジメントの課題が存在する、しかし、IaaS のシステムの外からの見え方は、既存のプロセスの変更を余儀なくさせるほど異なっている。例えば、誰がネットワークコンフィギュレーションに変更を加えることができるかのコントロールは、個々の装置上のアカウントからクラウドの管理画面に変わる。

2.1.3.2 配備モデル

パブリック

クラウド利用者では、パブリッククラウドの運用に関するガバナンスの権利は限定されている。なぜならば、クラウド事業者が、そのインフラ、従業員その他のもの全ての管理とガバナンスに責任を負うからである。 クラウド利用者は、契約に関する権限が限定され、その結果自身のガバナンス・モデルをクラウドに適用することに影響を受ける。柔軟性がない契約は、マルチテナントに伴う必然的な特質である。即ち、あらゆるものが、1 つのプロセスセットを使用し、1 つのリソースセット上で実行されるので、クラウド事業者は、必ずクラウド利用者ごとの契約や運用に合わせるという訳には行かない。クラウド利用者ごとに適合することは、コストを増加させ、トレードオフを引き起こす。多くの場合それは、パブリッククラウドとプライベートクラウドの使用の分界点になる。ホストされたプライベートクラウドは十分なカスタム化に対応可能だが、規模の経済性が犠牲になってコストは増加する。

これは、契約の交渉をすべきでないということを意味する訳ではなく、それが常に可能だとは限らないということを認識すべきである。代わりに、別のクラウド事業者(それは実際にそれほど安全でない可能性が高い)を選ぶか、要求条件を修正して、懸念を解消するために別のガバナンスメカニズムを適用するか、しなければならない。

類似の例として、発送サービスについて考える。定期便や通常の運送事業者を使用する場合、その運営を決めなければならないようなことはない。パッケージに機密文書を入れて、それを業者に預け、その業者が安全に、セキュアに、サービスレベルアグリーメントの想定値に収まる範囲で配達するという責任に対して信託している。

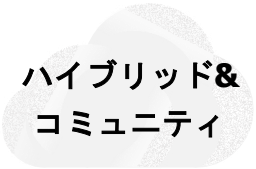
プライベート

パブリッククラウドだけが、ガバナンスに影響を与えるモデルではない。プライベートクラウドの場合にも影響があるだろう。組織が第三者にプライベートクラウドの所有または管理を委ねる(それは非常に一般的である)場合、委託先の事業者にどのようにガバナンスの影響があるかという問題に似ている。そこには共同責任が発生し、各々の責務は契約で定めることになる。

契約条項を左右することはより容易かも知れないが、必要なガバナンスの仕組みが確実に組み入れられるよ

うにすることは、依然として重要である。パブリッククラウド事業者の場合は様々な動機に基づいて、そのサービスが十分に文書化され、特定の基準レベルの性能で、機能性、および競争力を維持できるようにするが、それに反して、ホストされたプライベートクラウドでは、契約に規定されたものだけを提供し、その他のものにはすべて追加費用がかかるだろう。これは必ず考慮に入れて契約上反映させる**必要**があり、プラットフォーム自体を最新で競争力のあるものに維持することを保証する条項を入れるべきである。例えば、ベンダに対して、プライベートクラウドプラットフォームを、リリース後かつ**ユーザ**のサインオフ後の一定期間内に、最新バージョンに更新することを要求することである。

自社ホスト型のプライベートクラウドでは、クラウド利用者（事業部門その他の組織単位)に対する組織内のサービスレベルアグリーメントと、クラウドへのアクセス提供に対する、課金と請求のモデルが、ガバナンスの対象となる。



ハイブリッドクラウド環境を考える場合、ガバナンス戦略は、共通のコントロールの最小の組合せとして、クラウドサービス事業者との契約と、組織内部のガバナンスに関する合意の組合せを考える必要がある。クラウド利用者は 2 つのクラウド環境か、もしくは、クラウド環境とデータセンタの組合せのどちらかに接続する。いずれの場合も、全体に対するガバナンスはそれら 2 つのモデルを合わせたものである。例えば、専用のネットワークリンクを通して自らのクラウドに自社のデータセンタを接続するのであれば、両方の環境にまたがるガバナンスの課題に対応できなければならない。

コミュニティクラウドは複数の組織と共有するプラットフォームであるが、パブリックではない。故にガバナンスは、クラウド事業者とクラウド利用者の間だけでなく、そのコミュニティのメンバーとの関係にまで及ぶ。それは、パブリッククラウドとホストされたプライベートクラウドのガバナンスにどのようにアプローチするかの組合せとなる。そこでは、ガバナンスツールと契約の全体としては、パブリッククラウド事業者の規模の経済がある程度効くと同時に、ホストされたプライベートクラウドと同様にコミュニティの合意に基づいた調整も可能である。そこにはまた、コミュニティの参加者間の関係や、経済的関係や、メンバーの離脱の取扱いといった要素も含まれる。

2.1.3.3 クラウドにおけるリスクマネジメントのトレードオフ

クラウドの配備に対するエンタープライズリスクの管理には、有利な点と不利な点がある。これらの要素は、想定されるように、パブリッククラウドおよびホストされたプライベートクラウドについて、より顕著である。

- 資産およびそれらのコントロールおよびプロセスには、物的的コントロールがほとんどない。インフラストラクチャやクラウド事業者の内部プロセスに対する物理的コントロールは持てない。
- 日常の監視や管理ができないので、契約、監査およびアセスメントへの依存度が高まる。
- このことで、事業者利用者間の関係の先取り的な管理や契約の遵守の必要度が高まり、それは当初の契約締結内容や監査の範囲を超えて広がる。クラウド事業者もまた、競争に勝ち残るために絶えずその製品およびサービスを進化させるため、継続的に起こるイノベーションによって既存の合意事項や評価結果をはみ出したり、行き過ぎたり、超越したりする場合がある。
- クラウド利用者は、クラウド事業者が責任共有モデルの下で引き受けるリスクについて、管理の必要度が下がる（伴ってコストも削減する）。リスク管理の説明責任までアウトソーシングする訳ではないが、リスクの一部に対する管理は、確かにアウトソーシングすることができる。

2.1.3.4 クラウドのリスクマネジメントツール

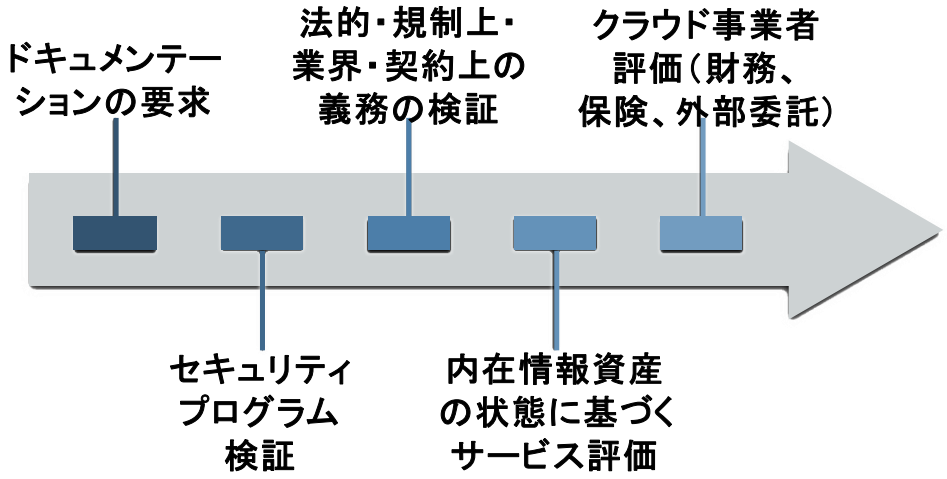
以下のプロセスは、クラウドコンピューティングの展開におけるリスクを管理するための基礎形成に役立つ。リスクマネジメントの重要な要素の 1 つは、リスクは**管理**したり、**移転**したり、**受け入れ**たり、**回避**したりすることがで

きるということである。しかし、すべては適切なアセスメントから始まる。

供給事業者に対するアセスメントは、クラウドのリスクマネジメントプログラムの土台となる。

- ドキュメンテーションを要求、入手する。
- 事業者のセキュリティプログラムおよびドキュメンテーションを調査する。
- 事業者および自組織の両方に対して、すべての法律上、規制上、契約上、そして司法上の要求事項を調査する。(詳細はドメイン３：法務を参照)
- 契約を締結したサービスを、自組織の情報資産の状態に照らして評価する。
- 別の角度から、クラウド事業者の全体像について評価する。財務状況、経営の安定性、世の中の評価、外部委託先等について。

サプライヤーアセスメントプロセス



定期的に監査と評価を見直し、最新であることを確認する。

- あるクラウド事業者からのすべてのサービスが同じ監査／評価基準を満たすとの予見を持たないこと。サービスごとに変化する場合がある。
- 定期的評価はスケジューリングし、自動化すべきである。

クラウド事業者がどれだけのリストを管理しているかチェックし把握した後に、取り残されているものが残存リスクである。残存リスクは、利用者が実装するコントロール(例えば暗号化)によって管理されることがよくある。リスクコントロールについて何が利用可能で何が具体的に実装されているかは、クラウド事業者、特定のサービスや機能、サービスモデルおよび配備モデルによって大幅に異なる。利用者側のリスク評価と実装したコントロールのすべてによってもなお、残存リスクがある場合、それは、移転するか、受容するか、回避するかしかない。

保険によって行われることが多いリスク移転は、特に情報リスク向けとしては、不完全な仕組みである。それは、一次損失事象に伴う財務損失のうちのいくらかを償うことができるが、(顧客の喪失のような)二次損失事象－特に無形資産や、風評被害のような計量困難な損失－には役立たない。保険会社の観点からは、サイバー保険はまた始まったばかりの分野であり、火事、洪水、などの他の形態の保険で利用する保険数理表並みの実績がないので、金銭的補填も、一次損失事象に伴うコストに見合わないかもしれない。限界を理

解すること。

2.2 推奨事項

- 選択したクラウド配備モデルとサービスモデルに基づいた、セキュリティおよびリスクマネジメントに関する共有責任を特定する。CSA CCM、COBIT 5、NIST RMF、ISO/IEC 27017、HIPAA、PCI DSS、EU GDPR などのような、適切な業界のベストプラクティス、世界標準および規制に沿って、クラウドのガバナンスフレームワーク／モデルを整備する。
- 契約がどのように自組織のガバナンスフレームワーク／モデルに影響するかを把握する。
    - 合意を結ぶ前に契約書（およびすべての参照付けられた文書）を手に入れて調査する。
    - クラウド事業者と効果的に契約を交渉することができることを前提とすべきではないが、そのクラウド事業者を使用するのを必ずしも止める必要はない。
    - もし、効果的に契約の交渉ができず、受容しがたいリスクを認識した場合は、そのリスクを管理するために代替の仕組み(例えば監視や暗号化)を検討すること。
- クラウド事業者評価のプロセスを整備する。
    - 評価プロセスには、以下の要素を含むこと。
        - 契約のレビュー。
        - コンプライアンスの自主評価結果の検査。
        - ドキュメンテーションおよびポリシー。
        - 利用可能な監査および評価結果。
        - クラウド利用者の要求事項へのサービスの適合性の確認。
        - クラウドサービスの自組織による利用の変化を監視するための強力な変更管理ポリシー。
    - クラウド事業者の再評価が定期的に行われ、できれば自動化されているべきである。
- クラウド事業者は、クラウドの潜在顧客がアセスメントのために必要とする資料と報告書に容易にアクセスできるようにするべきである。
    - 例えば CSA の STAR 登録。
- 対象となる特定の資産に対するリスク（に対処するための）要求条件とそれらの資産に対するリスク許容度を整合させること。
- ある範囲のすべてのソリューションのリスクを評価するために、リスクマネジメントおよびリスク受容／軽減のための特別な手法を開発すること。
- 残存リスクを管理するためにコントロールを使用すること。
    - 残存リスクが残る場合は、そのリスクを受容するか回避するかを決めること。
- 承認されたクラウド事業者を、資産タイプ(例えばデータ分類に紐づいたもの)、クラウドの利用方法およびマネジメントに基づいて継続調査するために、ツールを使用すること

DOMAIN 3

法的課題、契約および電子証拠開示

3.0　はじめに

このドメインでは、データのクラウドへの移送、クラウドサービス事業者との契約、訴訟における電子証拠開示により引き起こされる、法的課題のいくつかを取り上げる。ここに示す概観はすべての法的状況の可能性について述べることはできない。当事者の個別の問題については、その当事者が事業を行おうとしているまたは、その当事者の顧客が属する（単数または複数の）法管轄に所属する弁護士に相談する必要がある。さらに、法や規制は頻繁に変更される。従い、このドメインに盛り込まれた情報を利用するに際しては、それが該当しているか確認する必要がある。ドメイン 3 では、主にパブリッククラウドコンピューティングとホステッドプライベートクラウドに対する法の影響について取り扱う。このドメインでデータガバナンスや監査／コンプライアンスの一部側面について触れることもあるが、それらはドメイン 4 と 5 で詳しく扱っている。

このドメインで扱う対象は以下の範囲である。

- 法的問題
- クラウドサービス合意書（契約）
- クラウド上に保管された電子文書に対する第三者のアクセス

3.1　概要

3.1.1　データ保護とプライバシーを統制する法的枠組み

世界中で、多くの国が、個人データのプライバシーと情報およびコンピュータシステムのセキュリティ保護を公的および私的組織に義務付ける法的枠組みを整えている。これら法律のほとんどは、その一部を情報のプライバシーに関する公正原則に依拠している。同原則は 1960 年代後半から 1970 年代にかけて整えられ、のちに整理され拡張されて経済協力開発機構(OECD)のプライバシー・セキュリティ原則となった。

これらの法律において、データ管理者（data controller 代表的には個人と一次接点を持つ組織）は、一定の条件を満たさない限り、個人データの収集と処理を禁じられている。例えば、データ主体がそのデータに対する収集と利用に同意した場合には、データ管理者はその同意された範囲においてデータの収集と処理が可能となる。これらの法律は、個人データにアクセスする組織が守るべき多くの義務、守秘義務やセキュリティの義務などを定めている。データ管理者の代理として第三者（データ処理者（data processor））にデータ処理を委託する場合も、そのデータの収集と処理に関するデータ管理者の義務は存続する。データ管理者は、そのような第三者が、データの保護のためにしかるべき技術的および組織的セキュリティ対策を行うことを確実にするよう、求められる。

主題の共通性にも拘らず、世界の各国はデータ保護の体系を整えてきているが、往々にしてそれらは相互に矛盾をはらんでいる。その結果、複数の地域で事業を行うクラウド事業者とクラウド利用者は、法令遵守の要請に悩むことになる。

多くの場合、各国の法律は等しく以下の事項を適用していると考えられる：

- クラウド事業者の所在地
- クラウド利用者の所在地
- データ主体の所在地
- サーバの所在地
- 当事者間の契約の法管轄。これは関係当事者の所在地と異なる場合がある
- これら複数の所在地間での協定や法的枠組み

適用される法的義務は、関連する司法管轄、法の執行主体、法的枠組みによって大幅に変動する。

3.1.1.1 共通する主題

多くの国では、個人のプライバシー保護のために、一般もしくは包括法（個人データの全カテゴリに適用）または個別法（特定範囲のデータに適用）を制定してきた。

3.1.1.2 必要なセキュリティ対策

これらの法律の多くは、個人データのセキュリティを確保することは個人のプライバシー保護を確実にするために必須であることを認識した上でセキュリティ対策を施すよう定めた条項を盛り込んでいる。同時に企業は、適切な技術的、物理的、管理的対策を講じて広い範囲におよぶデータを喪失、誤用、改変から保護することが求められている。その対象には個人データ、財務データ、営業秘密その他の企業の機微なデータが含まれる。

3.1.1.3 国境を超えるデータ移転の制限

多くの国がその国境を越えて情報を移転することを禁止または制限している。多くの場合、移転が許可されるのは、移転先の国が、影響を受ける個人の個人情報とプライバシーの権利について（その国の関連法で定義される）「適正なレベルの保護」を提供している場合だけである。この適切性の要求の狙いは、その情報が国境を越えて移転される個人が、データ移転以前に提供されていたポリシーに基づく保護を、引き続き得られることを確実にすることにある。

他の方法として、データの受け入れ側と移転側が、データ主体のプライバシー権の保持の保証をする契約にサインする必要がある場合がある。国によっては、この適切な保護を保証する要件は複雑で厳しい場合がある。場合によっては、データを国外向けまたは国内向けに移転する前に、データ保護監督官から事前許可を得る必要かある。

更に、一部の国では、特定のデータがその国内に保存されることを義務付けるようになっている。この例として、例えば、ロシアと中国の新しいデータ国内処理保存法では、国内在住の個人にかかわる特定の個人データはその国内に保存することを義務付けている。

3.1.1.4 地域の事例

以下は、世界の各地域で現在適用されている、情報のプライバシーとセキュリティに関する法律と法的枠組みの例である。

オーストラリア

オーストラリアでは、2 つのカギとなる法律がクラウドサービスの利用者の保護を提供している。プライバシー法（1988）とオーストラリア消費者法(ACL)である。プライバシー法には 13 のオーストラリアプライバシー原則(APP)があり、適用対象は年間売上 3 百万豪ドル超の営利および非営利組織、医療サービス事業者、そして一部の中小企業である。

2017 年 2 月、オーストラリアは 1988 年プライバシー法を改正し、セキュリティ侵害が生じた場合に、企業が、影響を受けるオーストラリア在住者とオーストラリア情報コミッショナーに、報告することを義務付けた。セキュリティ侵害は、(a)重大な被害をもたらす可能性のある不正アクセスや個人情報の漏洩が発生した場合、(b)個人情報が不正アクセスもしくは漏洩の起こりうる状況で失われ、実際にそうなった場合にはその情報が関係する個人に深刻な被害をもたらす恐れがある場合には、報告しなければならない。

ACL は、過誤によるまたは誤解を与える契約や、情報漏洩の通告を怠るなどの事業者の怠慢から消費者を保護するものである。プライバシー法は、クラウド事業者が国外にある場合や、契約上の適用法が他の法律である場合でさえも、オーストラリアのクラウド利用者に適用される。

中国

ここ数年、中国は個人情報と企業情報のプライバシーとセキュリティを対象にした法的体系を形作るペースを加速してきている。2017 年サイバーセキュリティ法は、ネットワーク事業者と重要情報インフラ事業者の運営を統制するものである。2017 年 5 月、中国政府は個人情報および重要データの越境移転に関するセキュリティ対策案を公表した。同案は施行に向けて評価が行われている。

2017 年サイバーセキュリティ法は、ネットワーク事業者に一連のセキュリティ要件の遵守を義務付けるもので、情報セキュリティ対策の設計と実施、サイバーセキュリティ緊急対応計画、国家安全保障と犯罪捜査に必要な場合の捜査当局への協力と支援を盛り込んでいる。同法は、ネットワーク製品とサービスの供給元に、ユーザに既知のセキュリティ上の欠陥とバグを通知するとともに、所管当局にそれを報告することを義務付けている。

サイバーセキュリティ法は、重要情報インフラ事業者に対していくつかのセキュリティ上の義務を課している。それには、内部で組織を整え、教育を施し、データバックアップを行うこと、緊急対応義務、セキュリティ検査、サイバーセキュリティリスクの年次評価を行うこと、そして所管当局に報告すること、が含まれている。さらに、同法にはデータ国境規程が含まれており、個人情報その他の重要データは、中華人民共和国の域内に保存することを義務付けている。

2017 年第 2 四半期に、中国は、サイバーセキュリティ法を補完する越境データ移転規制法案を公表した。これらの規制はサイバーセキュリティ法の適用範囲を超え、対象を拡大するものとなると想定される。この法案は企業にとって海外へのデータ送信に適用される新たなセキュリティチェック義務を課すものとなりそうである。この規制はデータ国内処理・保管規程を拡張し、中国国内に保存が義務付けられる情報の類型を拡大するものと見られる。特に、ネットワーク事業者が収集する個人情報と重要情報が対象となる。サイバーセキュリティ法の下でのサイバーセキュリティとプライバシーとの適用範囲は変遷しており、収束は見えていない。

日本

日本では、個人情報保護法が民間部門に対して個人情報と個人データのセキュリティを義務付けている。ほかにいくつか一般法があり、うち一つは公的機関の保有する個人情報保護法であり、また医療分野を対象としたものなど特定分野対象の法がある。専門職法、例えば医師法、保健師助産師看護師法、薬剤師法は、医療従事免許者が患者の情報の秘密を保持する義務を課している。

2017 年 9 月以降、改正個人情報保護法により、個人データの第三者移転に制限を設け、第三者へのデータ移転にはデータ主体の事前同意を原則として必要とするようになる。移転への同意は、個人情報保護法が規定する標準に適合する個人情報保護の枠組みが確立している国向けの場合は不要となる。

ロシア

ロシアの情報保護法はデータ処理について厳重な規制を課している。ほとんどのデータ処理の形態には事前同意が必要とされる。しかし、ロシアの個人情報取り扱いに関する法体系で最も重要な要素はデータ国内処理保存法である。2015 年 9 月以降、企業はロシア国民の個人データをロシア国内に置くことが義務付けられた。ロシアのデータ保護監督官ロスコムナザールはすでに同法の適用を進めており、ある海外の SNS へのアクセスをブロックした。その SNS はロシア国内に物理的実体はなかったが、その Web サイトのロシア語版を提供していた。

欧州連合(EU)は 2016 年に一般データ保護規制(GDPR)を制定した。これは EU 加盟国すべてと欧州経済圏(EEA)参加メンバーに対して強制力を有する。GDPR は 2018 年 5 月 25 日に施行される。同日付で、EU および EEA 参加国すべての国ごとのデータ保護制度の法的基盤となっていたデータ保護指令 95/46/EC は廃止される。

EU/EEA で個人情報保護の諸側面を規制してきたもう一つの重要な文書は、プライバシーおよび電気通信指令 2002/58/EU である。この指令は段階的に廃止され、その代替となる E-プライバシー規制の第一次ドラフトが発表されている。このドラフトは 2018 年 5 月 25 日に施行されると思われるが遅れる可能性が強い。

セキュリティの観点からは、ネットワーク情報セキュリティ指令（NIS 指令）がセキュリティ遵守事項についてより厳密な要求をしている。2016 年に制定された NIS 指令は、EU/EEA 加盟国が 2018 年 5 月までに重要インフラと重要サービスの防御に関する情報セキュリティ法を制定するよう求めている。クラウド事業者とクラウド利用者は NIS 指令傘下で実施される各国法によって影響を受ける可能性が強い。

一般データ保護規制(GDPR)
新しい GDPR は EU 市民のデータを処理するすべての企業に適用される。そして加盟国の中で紛争の両当事者である個人または法人に最も関係のある国のデータ監督当局または裁判所において判断根拠となる。

適用範囲：GDPR は、EU/EEA 内で設立されたデータ管理者またはデータ処理者の活動に関連する個人データ処理に適用される。それはデータ処理が EU/EEA 域内であるか否かを問わない。GDPR はまた、EU/EEA 内のデータ主体の個人データの、EU/EEA 外で設立されたデータ管理者またはデータ処理者による処理に適用される。条件としてその処理が、(a)データ主体による対価の支払いの有無を問わず、商品またはサービスの提供に伴うものである場合、または(b)データ主体の行動が EU/EEA 内で行われる場合のその行動のモニタリングの場合に適用される。

合法性：データ処理が可能なのは、(a)データ主体がその個人データの処理について、自由意思に基づいて、個別の、告知に基づく、明白な同意の意志を示した場合、または(b)データ処理が法令の規定で認められている場合である。

説明責任：GDPR は企業に数多くの義務を課した。例えば、GDPR は企業にデータ処理作業の記録を保存することを義務付けている。データ処理の一部の分野では、「プライバシー影響評価」の事前実施を求められる。企業は、その製品やサービスの開発と運用において、「プライバシーバイデザイン」「初期設定されたプライバシー(Privacy by Default)」準拠が期待されている。

データ主体の権利：データ主体は自身のデータの処理に関する情報について権利を持つ。その権利は、自身の個人データのある種の用途に対する拒否権、自身のデータに対する修正または消去の権利、違法な処理の結果生じた損害を賠償される権利、忘れ去られる権利、データの移転に関する権利である。これらの権利があることで、クラウドサービスの関係者には多大な影響がある。

越境データ移転規制： EU/EEA 域外で、個人データおよびプライバシー権保護について同等の保護を提供しない国への、個人データの移転は禁止されている。

セキュリティ侵害：GDPR はセキュリティ侵害があった場合にそれを報告するよう企業に義務付けている。報告義務はリスクベースで、監督当局への報告とデータ主体への報告の異なる義務がある。セキュリティ侵害の報告は、企業がインシデントを知った時から 72 時間以内に行わなければならない。

加盟国間の不一致：各加盟国がその独自のルールを適用する事例は枚挙に暇がない。例えば、ドイツは 9 人超の従業員を有する場合にはデータ保護オフィサーの指定を義務付けている。

制裁：GDPR 違反は、企業に巨額の制裁をもたらす。最大の課徴金は、企業の全世界売上もしくは総収入の 4%か 2 千万ユーロの大きい方となる。

NIS 指令 (Network Information Security Directive)

NIS 指令は 2016 年 8 月に施行され、EU/EEA 参加各国に 2018 年 5 月までの国内法制定を求めている。NIS 指令は、ネットワークと情報システムが、一定の信頼できるレベルで、可用性・真正性・完全性・機密性を侵害する行為に対する耐性を備えるためのフレームワークである。その対象は、保存中・移送中・処理中のデータ、もしくは、そのデータに関連するサービスで、当該ネットワークおよび情報システムが提供しまたはそれ経由でアクセス可能なものである。

NIS 指令は加盟国の国内法が重要サービス事業者にネットワーク情報セキュリティ上の義務を課すよう求めている。重要サービス事業者とは、重要な社会活動または経済活動の維持に不可欠なサービスを営む法人で、そのサービスのネットワーク情報システムにインシデントが発生した場合、そのサービスの提供に甚大かつ致命的な障害をもたらす可能性のあるものを指す。国内法に組み入れるよう求められる項目は以下の通りである。

- その事業者の運営に用いられるネットワーク情報システムのセキュリティにかかわるリスクを管理するための技術的および組織的対策を講じること
- 重要サービスの提供と事業継続のために必要なネットワーク情報システムのセキュリティに影響を与えるインシデントによる打撃を予防し最小に抑えるための適切な対策を講じること
- 自社の重要サービスの継続的供給に重大な打撃をもたらすインシデントについて、所管当局または機関に遅滞なく通報すること
- 自社のネットワーク情報システムを検証するために必要な情報を提供すること
- セキュリティ監査結果など、セキュリティポリシーを有効に設定していることの証明を提供すること

NIS 指令はまた、デジタルサービスの提供事業者に対しても、ネットワーク情報システムのセキュリティに関する義務を課す法律を、加盟国が定めるよう求めている。対象はオンラインマーケット（つまり E コマースプラットフォーム）、クラウドコンピューティングサービス、そしてオンライン検索エンジンである。EU 域外の事業者で EU 域内でサービスを提供する事業者も NIS 指令の対象となる。

加盟国の国内法はまた、デジタルサービス事業者に、その使用するネットワーク情報システムのセキュリティに係るリスクを把握し適切かつ規模に相応した技術的および組織的対策を義務付ける必要がある。対策とはインシデント対応、事業継続管理、モニタリング、テストと監査、国際標準の遵守などである。

加盟国の国内法は、デジタルサービス事業者に、インシデントの打撃を防止し最小にするための対策を取るよう義務付ける必要がある。デジタルサービス事業者は、そのサービスの供給に重大な影響をもたらすインシデントについて、所管当局または機関に遅滞なく通報しなければならない。通報には所管当局または機関が国境を超える影響の度合いについて判断できるために十分な情報が含まれなければならない。重要サービス事業者が重要サービスについて第三者のデジタルサービス事業者に依存している場合は、当該事業者は、その第三者のデジタルサービス事業者に影響を与えるインシデントによって起こる重要サービスの継続性への重大な影響について通報しなければならない。

中南米地域

中南米諸国もまた急速にデータ保護法制を整えつつある。これらの法律の各々はセキュリティ上の義務を規定し、データ保管者に、データの所在場所の如何を問わず、また第三者移転の場合には特に、個人データのセキュリティと保護を確保する義務を課している。

例えば、アルゼンチン、チリ、コロンビア、メキシコ、ペルー、ウルグアイはデータ保護法制を制定しているが、これらは主として EU データ保護指令 95/46/EC を参考にしており、また APEC プライバシーフレームワークの参照を含んでいる場合もある。

北米：アメリカ合衆国

分野個別のアプローチの結果、米国は連邦レベル、州レベル、地方において数百の規制を行っており、文書化された詳細なセキュリティ計画からセキュリティ侵害の情報開示ルールまである。その結果、米国で事業をする組織や、米国所在の個人や企業の個人データその他のデータを収集したり処理したりする組織は、頻繁に、連邦・州・地方のプライバシー法や情報セキュリティ法の対象となる。これら諸規則の多様さと複雑さはクラウドサービスの提供者と利用者の双方にとって、またサービス提供事業者やサービスの提供に連なる下請け業者にとって、障害となりうる。

米国連邦法

数多くの連邦法とその関連する規制が個人情報のプライバシーとセキュリティに関係する条項を含んでいる。代表的なものは GLBA（Gramm-Leach-Bliley Act：金融サービス近代化法）、HIPAA（Health Insurance Portability and Accountability Act of 1996：健康保険の移転と責任に関する法律）、COPPA（Children's Online Privacy Protection Act of 1998：児童オンラインプライバシー法）がある。セキュリティに関する条項は企業に個人データの処理に際して適切なセキュリティ対策を施すよう求めている。

これらの法律のほとんどは、企業が下請事業者やサービス事業者を利用する際に予め注意することを義務付けている。その場合、下請事業者の行為の責任を組織が負うことになる場合がある。例えば、GLBA や HIPAA のセキュリティおよびプライバシー規則は、対象となる組織が、その下請事業者に対して、書面により、

適切なセキュリティ対策を施しデータプライバシー条項を遵守するよう義務付けることを要求している。

米国州法

連邦レベルの法と規制に加えて米国の多くの州では、データプライバシーやデータセキュリティに関する法律を定めている。それらの法の適用対象はその週に在住する個人に関する個人情報（確報により限定定義される）を収集または処理する法人すべてで、米国のどこにデータが保存されるかを問わない。

州法のいくつかは精妙に作られている。たとえばマサチューセッツ州法 201CMR17.00「コモンウェルス住民個人情報保護基準」による詳細な義務がある。他の州法はより一般的（例えばワシントン州法 RCW19.225.02(2)(b)は法令遵守基準で義務を指定している）であり、少数の例では他の特定の基準（例：上記 PCI DSS：決済カード業データセキュリティ基準）を参照している。情報セキュリティ問題を取り上げるほとんどの州法は企業がサービス事業者との契約で明文の適切なセキュリティ対策を規定するよう求めている。多くの州法がまた、企業が十分な個人データの保護とセキュリティを行い、その企業にサービスを提供する事業者も同様にする義務を課している。

セキュリティ侵害通報関連法制

例えば医療関係向けなどの数多くの連邦法と連邦規則、またほとんどの州法が、PHI（患者の健康情報）などの特定分野の情報が関わるセキュリティ侵害を受けた法人が、遅滞なく対象となる個人と、また多くの場合連邦・州の機関にそのセキュリティ侵害の発生を通知することを義務付けている。

これらの法律の知識と理解が、クラウド利用者とクラウド事業者の双方にとって重要である。なぜならば、セキュリティ侵害は多くの場合、集団訴訟への対応など、多大なコスト発生のトリガーとなるからである。最近のセキュリティ侵害の事例では影響を受ける人は何億人にも上り、その結果関係する企業の法務費用と賠償金の支払いは膨大な額に上っている。

連邦および州の機関

具体的な法令群に加えて、クラウド事業者とクラウド利用者はまた「プライバシーとセキュリティの慣習法」についても理解しておくべきである。これは同意審決の内容に対する通称で、連邦および州の行政機関が、セキュリティ事故と事案の調査の結果として公表するものである。

20 年近くにわたって、連邦政府機関、例えば FTC（公正取引委員会）や州の司法長官は、連邦または州レベルの「不公正取引慣行」関係法に基づく権限を行使して、プライバシーまたはセキュリティへの取り組みが、公表されている遵守要件を満たしていない企業に対して、その対応が不公正または欺瞞的であるとして行政命令を出している。FTC が FTC 法第 5 条「不公正または欺瞞的行為および慣行」に基づいて（または州の司法長官が州の同種の法律に基づいて）、これら多くのセキュリティ案件の調査結果として発行する命令による数多くの同意審決は、連邦および州政府が個人情報の収集、利用、保護に関してどう判断し何を目指しているかを知るための重要な指針となる。

3.1.2 契約とクラウド事業者の選定

例え法令で具体的措置が義務付けられていなくても、クラウド利用者は、その顧客、取引先、従業員の個人情報を保護し、それが二次的目的に使用されたり、第三者に開示されたり共有されたりすることのないよう担保する契約上の責任がある。この責任はまた、例えば企業がその Web サイトに掲げる契約約款やプライ

バシー方針、あるいは企業が第三者と交わす契約条項からも生じる。例えば、データ処理者はその掲げるサービス契約の条項により、個人データを特定の目的のためだけに処理する義務を負う。別の形としては、企業が顧客と契約（サービス契約等）を結び、その中で、データ（個人データまたは企業データ）を保護し、用途を限定し、セキュリティを担保し、暗号化を施し、等の特定の約束をする場合もある。組織は、その管理するデータがクラウド上にある場合は、自組織がそのプライバシー規程その他の契約でした約束や履行保証を遵守できる立場を維持することを保証しなければならない。クラウド上のデータはその収集目的のためだけに使用されなければならない。

プライバシー規定が、個人データの主体にその個人データへのアクセスや、情報の修正や削除を認めている場合は、クラウド事業者はそのようなアクセス、修正、削除の権利が、クラウド外の状況で可能なのと同等に実施できるようにしなければならない。

データまたはその処理がクラウドに移行した場合、そのデータの保護とセキュリティの責任は、たとえその責任が特定の状況下で第三者と共有されるとしても、そのデータの収集者または保管者に帰属する。データの扱いや処理を第三者に委託する場合でも、データの保管者は引き続きそのデータの喪失、毀損、誤用に対して責任を負う。従って、データ保管者とクラウド事業者は正式の書面による契約を交わし、各々の役割、相手先に期待されこと、対象となるデータに付随する多くの責任の帰属について明確に規定することが賢明であるし、あるいは法令や規制で義務付けられているかもしれない。そのような契約はまた、データの使用に対する許可と禁止ならびにデータの盗難もしくは侵害に際して取るべき対策について、明確に規定していなければならない。

上に見てきた法令、規制、標準、実践規範は、データ保管者がこれらの義務を満たすためにデューデリジェンス（契約締結前）やセキュリティ監査（契約期間中）を実施することを担保するよう求めている。

3.1.2.1 内部的デューデリジェンス

企業は寄託されたデータの保管者である。上述の通り、数多くの法令、規制および契約によって、データの第三者への開示や移転は禁止されている。例えば HIPAA の保護対象である医療情報は、第三者である「業務連携先」に対し、特段の義務を課した上でなければ移転することができない。さらに、データが海外由来のものである場合は、個人データとプライバシー権に「十全な保護」を施していない国への国境を超える移転に対してはおびただしい障害がある場合がある。

クラウドコンピューティングを取り入れる前に、クラウド事業者とクラウド利用者は、該当する法律上の問題点や遵守義務にはどんなものがあるか特定するために、相互の業務手法、ニーズ、制限事項について点検する必要がある。例えば、クラウド利用者は、その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利用を許容するのか、その場合どんな条件においてか、について判断しなければならない。そのビジネスの種類によっては、法令により、企業情報の管理権限を移管することが禁じられている場合がある。クラウド事業者は、なじみのない法的義務を伴う特定市場でビジネスをするコストを事前に評価するのが賢明であると悟るであろう。

クラウド利用者はデータの第三者への移転が、たとえその第三者がサービス事業者であっても、禁止されるような守秘義務契約もしくはデータ用途契約を交わしているか調べる必要がある。もしクラウド利用者となる可能性を有する或る企業が、個人情報や営業秘密を保護する守秘義務契約を交わしている場合には、その契約はデータ主体の事前同意なく下請を雇うことを禁止しているかもしれない。企業が交わしたデータ利用契約では、その企業が顧客のデータの処理を第三者に下請けさせる場合に顧客の事前同意を義務付けている場合がある。そのような制限は、多くの場合クラウド事業者へのデータ移転に適用される。そのような状況下では、顧客（データ主体）の事前許可なくクラウドにデータを移すことは、その顧客とのデータ利用契約違反となる可能性がある。

他の状況下では、その企業が処理するデータが極めて機微または機密で、クラウドサービスへの移転をするべきでなく、もしくは移転に際しては特別に細心の注意を払う必要があったりする。例えば、R&D ロードマップのような利害に大きく関わるプロジェクトに属するファイルの場合や、予定されている IPO や合併や買収計画の場合が該当する。

3.1.2.2 モニタリング、テスト、アップデート

クラウド環境は静的ではない。それは変化するものであり、関係者はそれに適応しなければならない。クラウドサービスの定期的なモニタリング、テスト、評価は、必要なプライバシーおよびセキュリティ対策が実施されていることを担保するために実施することが推奨される。クラウドサービスを定期的にテストしないと、見えないところで管理策の有効性が損なわれる恐れがある。

さらに、企業が事業を営む法令、規制、技術の背景は高速で変化している。新たなセキュリティ脅威、新しい法令、新規の遵守義務は早期に把握しなければならない。クラウド利用者とクラウド事業者は、関連する法令上、規制上、契約上、その他の義務について把握し、双方の営業が適用される法令や規制を遵守していることを担保し、実施されているセキュリティ対策が技術進化に合わせて進化し続けることを確実にしなければならない。

3.1.2.3 外部からのデューデリジェンス

どのような契約でも、デューデリジェンスの重要な要素は関係ある相手側の業務の要素－この場合クラウド事業者の運用－のすべてについて要求し評価することである。クラウドサービスを購入する者は、自分が購入しようとしている特定のアプリケーションまたはサービスについて、しっかり理解していることである。デューデリジェンスをどこまでやるかとどの程度時間をかけるかは状況次第である。作業は 1 日かも知れないし 1 週間かも知れないし 1 ヵ月かかるかも知れない。それは、利用者の特別なニーズ、処理対象のデータの特性、処理の機微性と深度、あるいは特定の処理を定常化したり特別に機微にしたりするその他の要素に応じて、変わる。

このように、対象となるプロジェクトの特性に応じて、デューデリジェンスの評価の対象は広がる：提供されるサービスの特性や完成度、サービスの品質や安定性に対する世評、一定のレベルのサポートやメンテナンスが提供されるか、カスタマーサービスの対応、ネットワークスピード、データセンタの立地などである。利用者へのインタビューは価値のある観察情報となる。クラウド事業者に対して提起された訴訟に関する報告書やクラウド事業者の評判をオンライン検索することも発見を与えてくれる。

ほとんどの場合、クラウド利用者は評価対象として最低限、適用されるサービスレベル、エンドユーザ契約と法的契約、プライバシーポリシー、セキュリティに関する情報開示、適用される法規制（登録義務）の適合証明を評価し、クラウド事業者の提示する条件が自組織に適合していることを確認する必要がある。デューデリジェンスに要求される深さと密度により、調査対象には以下の項目が必要となる。

- サービスが信頼でき、利用しやすいか？
- データ処理にどのようにサーバが利用されるか？
- サービスの運用と提供の仕方？
- データが他の利用者のデータとコロケーションされるか？
- 侵入や災害に対するデータの保護は？
- 時間経過に伴う価格の変化は？
- 利用組織のコンピューティングとアクセスのニーズにクラウド事業者が適合するか？
- クラウド事業者が向こう数年事業を続けるか？財務状況はどうか？
- サービスレベルはどうか？

- セキュリティ対策はどうなっているか？
- セキュリティ侵害が生じた場合の対応は？

クラウドのサービス契約（別紙、別表、付属書類を含む）の全条項をチェックすることはどんなプロジェクトでもデューデリジェンスの良い方法である。クラウドコンピューティングでは、一部の条項は交渉不可となっているので、このことは特に重要である。そのような場合、クラウド利用者は、そのクラウド事業者を利用するかしないかを、情報開示を受けた上で判断する必要がある。

3.1.2.4 契約交渉

クラウド契約は、すべての当事者の了解事項を正確に記述することを意図している。クラウドサービス利用に伴う法務上、商取引上および世情評価面でのリスクにさらされることを少なくするために、様々な予防措置や対策をとることができる。

提案された契約は、どんな場合も、たとえそれが交渉不可のものであっても、注意深くチェックする必要がある。一つには、実際に変更の交渉が可能な場合がある。例え交渉不可であっても、クラウドサービスを購入する場合は必ず、約束しようとしていることのもたらす結果や影響について理解しておく必要がある。交渉不可の契約は往々にして通常クラウド利用者が必要とする保護を欠いている可能性がある。その場合、クラウド利用者はそのような保護の外に置かれるリスクと期待されるメリットを比較衡量する必要がある。

3.1.2.5 第三者による監査や評価証明

監査とコンプライアンスはドメイン 4 で詳しく触れるが、2 つの事項が契約上および法令・規制上の義務に影響を与える可能性がある。クラウドコンピューティングでは、第三者監査や評価証明がクラウド事業者のインフォストラクチャに関するコンプライアンスの保証としてしばしば利用される。これによりクラウド利用者はそのクラウドプラットフォームの上に自社のコンプライアンスを満たしたサービスを構築できる。クラウド事業者は評価の対象範囲、評価対象となった機能とサービスを公表し、クラウド利用者はそれをチェックすることが重要である。

例えば、あるクラウド事業者の最新のストレージが HIPAA 適合でないかもしれない（従ってクラウド事業者はそのストレージを含む HIPAA の BAA(Business Associate Agreement)を結ぶことを躊躇するかもしれない）。例えその事業者の他のサービス機能は HIPAA 適合として使うことができたとしても。

3.1.3 電子証拠開示

「証拠開示」に関する米国のルール－相手側が未公開の書類を訴訟に利用することに関するプロセス－は広範な書類が対象となる可能性がある。特に、証拠開示は、法廷が証拠認定する対象として、開始時に既知であった書類に限定しない。証拠開示は認定証拠（関連性がありかつ証明性がある証拠）として合理的に判断できるすべての書類が対象となる。Federal Rules of Civil Procedure（FRCP：民事訴訟規則）第 26 号参照

ここ数年、多くの訴訟当事者が自分の訴訟に不利な証拠を削除したり無くしたり改変したりした。FRCP は、このようなケースでは、制裁の一つとして、証拠破壊に責任がない側に賠償金を認定することを認めており、一部の事例では、陪審員は、「不利な推定」の指示を受ける（陪審員が破壊された証拠は破壊した側にとって想定しうる最悪の情報を含んでいたと推定するよう指示される）。FRCP 第 37 号参照。この分野で進行中の訴訟の結果として、特に電子的に保存されている情報(ESI)が関係するケースでは、FRCP は訴訟当事者の責任を明確にする方向に変ってきている。

クラウドが訴訟や証拠調べに必要となる ESI の大半の保存場所となる可能性が高いので、クラウド事業者とクラウド利用者は、訴訟に関係するすべての書類を探し出すことができるように注意深く計画し、FRCP26 や州レベルの同様の規則がもたらす、ESI に関する厳しい義務を満たせる様にしなければならない。この関係で、クラウド利用者とクラウド事業者は、クラウド利用者が電子証拠開示の当事者となり、関連するデータがクラウド事業者の下に存在する可能性がある場合には、以下の課題について考えておく必要がある。

3.1.3.1 所持、保管、管理

米国のほとんどの法管轄において、当事者が関連する書類を用意する責任は、その所持・保管・管理の範囲の書類およびデータに限られる。第三者、例えばクラウド事業者を通じて関連データをホストしていることは、当事者の情報を用意する義務を免除するものではない。しかし、クラウド事業者にホストされたデータのすべてがクラウド利用者の管理下にある訳ではない（例えば災害復旧システム、クラウド事業者がその環境の運用のために生成し保持するある種のメタデータなど）。何のデータがクラウド利用者にとって入手可能で何がそうでないかは、クラウド利用者とクラウド事業者の双方にとって、その関係の初期から関心事であるだろう。クラウド事業者の、法的手続きに沿って情報を用意することに関する情報取扱者としての責任は、各法管轄において解を見出すべく与えられた課題である。

3.1.3.2 関連するクラウドアプリケーションとクラウド環境

場合によっては、実際のクラウドアプリケーションやクラウド環境はそれ自体が紛争解決に関係がある。そのような状況では、アプリケーションや環境はクラウド利用者のコントロール外である可能性が強く、召喚その他の証拠調べ手続きはクラウド事業者に直接行われる必要がある。

3.1.3.3 探査可能性と電子証拠開示のツール

クラウド環境では、クラウド利用者は自身の環境で使っている電子証拠開示のツールを適用したり使用したりできない場合がある。さらに、クラウド利用者はクラウド上にホストされたデータのすべてに対して検索やアクセスする能力や管理権限を持たない場合がある。例えば、クラウド利用者は自身のサーバにある何人もの従業員の e メールアカウントに瞬時にアクセス可能だが、クラウドにホストされた e メールアカウントにはできない可能性がある。そのため、クラウド利用者はアクセスが限定されることによって生ずる余計な時間と費用を負担しなければならない。クラウド利用者がクラウドサービス契約を交渉で変更したり追加したりできる場合には、この問題は第一に取り上げるべきである。そうでないと、クラウド利用者はその都度この問題に向き合わねばならず、その結果クラウド事業者から受ける追加サービスの対価を払わなければならなくなる可能性がある。

3.1.3.4 保全

クラウド利用者が利用するクラウドのサービスと配備モデル次第だが、クラウド上の保全は他の IT インフラにおける保全と類似であるか、あるいは大幅に複雑である可能性がある。米国では、訴訟当事者は、その所持・保管・管理するデータの破壊や改変を予防する適切な措置を講じる責任がある。対象となるデータは、その当事者が、進行中または当然に起こると推測できる訴訟もしくは政府による捜査に関連すると知っているか、または当然に知っているはずのものである。（これは一般的に書類の破壊に対する「訴訟ホールド＝訴訟に関連する資料・情報の保全義務」と呼ばれる。）このような問題は広く FRCP37 号の対象となっているが、訴訟当事者となる可能性のある者に適用されるルールは無数にある。EU では、情報保全は 2006 年 3 月 15 日付欧州議会および評議会指令 2006/24/EC で規定されている。日本、韓国、シンガポールは同様のデータ保護規則がある。南米では、ブラジルとアルゼンチンが各々Azeredo 法、2004 年アルゼンチンデータ保存法（法番号 25.873）を持っている。

3.1.3.5 データ保存法と記録保持責任

電子証拠開示に関連する米国法から生じたデータ保存義務に加えて、データ保存法は対象となる法人がデータを一定期間保存する義務を企業に課している。

コストとストレージ：保全は大量のデータを長期にわたって保存する必要を生じる。クラウド利用者は、クラウドへの移行の前に、以下の質問を検討し、リスクが許容できるか確認するべきである。

- SLA の中でデータの保存に関する条項は何か？
- 保全の要求が SLA の期限より長い場合はどうなるか？
- クラウド利用者がデータを所定の場所に置いたら、その追加費用はいくらで誰が払うのか？
- クラウド利用者はデータ保存用のストレージ容量を SLA の中で提供されているか？
- クラウド利用者は保存したデータを効率よく、フォレンジックに適う方法でダウンロードして、オフラインまたはニアラインで保持することができるか？

保存の範囲：要求側当事者は、当該法的争点に関連し、または証拠となる情報を含む、もしくは合理的にそうであると推測できるクラウド上のデータに対してのみ権利がある。クラウド上のすべてのデータまたはアプリケーション内のすべてのデータに対して権利がある訳ではない。（厳密にどこまでかは訴訟の中で判断される可能性が高い。）しかし、クラウド利用者が関連するデータを厳密に仕分けして保全する能力がない場合には、訴訟によっては、妥当な範囲の保全を担保するために過剰に保全するよう求められるかもしれない。過剰に保全された情報は、次に、何が必要で何が不要か判断するために精査され、証拠開示手続きのために提供される。このプロセスは、文書レビューまたは特権レビューと呼ばれ、弁護士のスタッフにより、または場合によっては新興のエキスパートシステムによって、クラウド利用者の費用で実施されることになる。証拠開示で生じる過去に類を見ないような膨大なデータをどのようにソートするかは、現在取り組まれている法的な、また技術的な研究領域である。

動的および共有ストレージ：データをクラウド上に保存する負荷は、次の場合には比較的緩くなる。すなわち、クラウド利用者が保存のための空間を持っている場合、データが比較的静的な場合、アクセスする人が限られてかつデータの保全について知っている場合、である。しかし、プログラムによってデータを変更したり排除したりするクラウド環境では、あるいはデータが保全の必要を認識していない人と共有されている場合は、保全の困難度は増す。クラウド利用者がデータを訴訟に関連するもので保全が必要だと判断したら、クラウド事業者と協働してそのデータを保全する適切な方法を見いだすことが必要だろう。

3.1.3.6 収集

クラウド利用者がクラウド上のデータに対する管理者レベルのコントロールを持てない場合があるので、クラウドからのデータ収集は、ファイアウォールの内側で収集するよりも、より困難で、より時間を食い、そしてよりコストがかかる。特に、クラウド利用者はクラウド上のデータに対して（オンプレミスと）同レベルの可視性を持たない。またクラウド利用者は自分が収集したデータをクラウド上のデータと比較してエクスポートが十分に完ぺきで正確であったことを検証するのがとても難しい。

アクセスと帯域幅：ほとんどの場合、クラウド利用者のクラウド上のデータへのアクセスは SLA の中で規定されている。このことは、クラウド利用者が定量のデータを迅速にかつフォレンジックに適う方法（つまり通常関連するメタデータを併せて保全）で収集することに対して制約となる。クラウド利用者とクラウド事業者はこの問題についてその取引の最初の段階で検討し、訴訟に際しての例外的アクセスのためのプロトコル（および費用）を決めておくべきである。このような事前合意がない場合で、訴訟相手と法廷に対して主張する際には、クラウド上でデータ収集する時間と費用を引き受けることになる。FRCP26 号(b)(2)(B)では、訴訟当事者が、要求された情報が合理的範囲でアクセスすることができないことを証明した場合には、認められることに留意すべきである。

しかし、要求側当事者がなぜその情報が必要かと、他の手段によっては入手できないことを立証した場合には、法廷は無条件にそのような情報源からの証拠開示を命ずる場合がある。

関連した問題として、クラウド利用者のアクセス権が全範囲のデータへのアクセスを可能にしたとしても、その状況の中で最もうまくアクセスできるようにする程度の機能までは提供していない。例えば、クラウド利用者が 3 年分の小売取引データにアクセスできたとしても、機能面の制約から一度にダウンロードできるのは 2 週間分であったりする。さらに、クラウド利用者はメタデータの一部しか見えないかも知れない。実際の訴訟に際して行使する必要が生じる前に、利用できるツールを使って何ができるのかを知っておくことが、クラウド利用者にとって賢明である。

フォレンジック：クラウド上のデータソースをビット単位でイメージすることは一般に困難または不可能である。明確なセキュリティ上の理由から、クラウド事業者はハードウェアへのアクセスを認めることに消極的である。特にマルチテナント環境で、そのクラウド利用者が他の利用者のデータにアクセスできる可能性がある場合は。プライベートクラウドでさえも、フォレンジックは極めて難しく、クラウド利用者はそのことを訴訟相手の弁護士か法廷に通告する必要があるかもしれない。（再度、FRCP26 号(b)(2)(B)はそのような未達の責務に救済を与える場合がある。） 幸いにも、この種のフォレンジック解析はクラウドコンピューティングでは滅多に認められない。なぜならばクラウド環境は一般に構造化データ体系や仮想化で構成されており、追加の関連情報をビット単位の解析に大量に提供することはできないからである。

妥当なレベルの完全性：証拠開示要求の当事者であるクラウド利用者は、そのクラウド事業者からのデータ収集が完璧で正確であることを検証する適切な手続きを踏まなければならない。特に、通常のビジネス上の処理で証拠開示要求に対応することが不可能で、情報を得るために訴訟特有の手段が用いられる場合には。このプロセスは、クラウド上に保存されたデータが正確で、認証されもしくは証拠能力があるかについての検証とは別のものである。

アクセス可能性への制限：データがどのように格納されているかの違いや、データオーナーに与えられたアクセス権または特権によっては、クラウド利用者がそのクラウド上に持つデータのすべてにアクセスできない可能性がある場合がある。クラウド利用者とクラウド事業者は、証拠開示の要求に際して、その要求された情報や対応するデータ構造を解析して、関連性、具体性、適合性、アクセス可能性を調べなければならない。

3.1.3.7 直接アクセス

クラウド環境の外では、原告側が被告側の IT 環境に直接アクセスすることは、一般には許されていない。（ただし、時として起こることがある。実際、いくつかの法廷は、労働紛争を含む民事係争では、証拠保全の目的で予告なしの IT 装置の停止を積極的に認めている。） クラウド環境では、それが許されるケースはより少なくて、フォレンジック分析がほとんど不可能なので、直接アクセスも不可能と考えられる。一部のクラウド事業者は、直接アクセスを提供することが無理であろう。なぜならばハードウェアと設備はその所持・保管・管理に属さないからであり、原告側はアクセスのためにその供給元に直接交渉しなければならないだろう。

3.1.3.8 元環境でのデータ生成

クラウド事業者は、通常データを独自性の高い、クラウド利用者の管理下にない、システムおよびアプリケーションに保存している。一般に、ESI（電子保存情報）は、変換に際して失われる情報（メタデータなど）が紛争に影響しない場合には、標準的フォーマット（電子文書用 PDF など）で作成されるものと考えられる。クラウド固有のフォーマットのデータは原告にとって役に立たない。このような状況では、すべての関係者 – 原告、データ生成側、クラウド事業者 – にとってベストと考えられる方法は、関係する情報を、クラウド環境の標準プロトコルにより、関係情報の保全に注意を払いつつエクスポートすることである。

3.1.3.9 認証

この場合の認証とはデータを証拠として認定するフォレンジック認証を指す。（アイデンティティ管理の一部であるユーザ認証と混同してはならない。）クラウド上にデータを保存することは、データを証拠として認定するかの判断であるデータ認証に影響しない。問題は文書が期待されるものであるかである。例えば、e メールは、それが企業内環境に保存されていたかクラウド上かによって認証可否は左右されず、問題はそれが完全性を維持して保存されているか、つまり法廷がそのデータが生成以降変更されていないと信用するかである。改ざんやハッキングなどの別の証拠がない限り、文書はそれがクラウド上で生成されまたは保存されたからという理由だけで、認定や信用ができるとかできないと考えるべきではない。

3.1.3.10 電子証拠開示におけるクラウド事業者とクラウド利用者の協力

クラウド事業者とクラウド利用者の双方にとって、その関係の始まる時点で、証拠開示によって生ずる煩雑さを考慮に入れ、SLA の中でそれについて対処しておくことは最も賢明である。クラウド事業者はクラウド利用者にとって魅力あるものにするために、そのクラウド商品に証拠開示サービスを含めること（Discovery by Design）を検討しようとするかもしれない。いかなる場合でも、クラウド利用者とクラウド事業者は、どちらに証拠開示請求が来た場合でも妥当な範囲で相互に協力することを契約に盛り込むことを検討すべきである。

3.1.3.11 召喚または捜査令状への対応

クラウド事業者が第三者から情報提供請求を受ける場合、それは差押え令状、召喚状または裁判所命令の形をとる場合があり、クラウド利用者のデータへのアクセスが命じられる。クラウド利用者は、そのデータの機密性確保のために、アクセス請求に対して争うことができるよう希望するであろう。このために、クラウドサービス契約では、クラウド事業者が差押え令状が届いたことをクラウド利用者に知らせ、クラウド利用者にアクセス請求に抗弁する時間的余裕を与えるようにしておくべきである。

クラウド事業者はそのような請求に対して、その設備を開扉し、請求者にその望むものを何でも提供する気になるかもしれない。そうする前に、クラウド事業者は弁護士と相談の上、請求が法的に有効で信用できるものであることを確認しなければならない。クラウド事業者はその保管する情報を開示する前に請求を慎重に検分し、情報を提供した場合に顧客への責任を果たすことができるか検討しなければならない。場合によっては、クラウド事業者は、曖昧であったり他の理由で問題のある情報提出命令に対して抗弁することで、顧客のニーズによりよく対応することができるかもしれない。

3.1.3.12 その他の情報

証拠開示と電子保存情報に関してさらに情報を求めるなら、多くの種類の文献がある。面白いと思われるのは Sedona Conference である。これは非営利の研究教育機関で、ここ数年、ESI の取り扱いについて影響力のある助言をしてきている。それらの推奨は徐々に法律問題のこの新しい分野を形成してきた。ただし、その推奨事項それ自体は法的効力を持っているわけではないことに留意すべきである。

3.2 推奨事項

- クラウド利用者は、システムとデータをクラウドに移行する前に、関係のある法令および規制の枠組みおよび、自社所有および自社管理のデータの取り扱いや自社の運用管理に適用される契約上の義務について理解しておくべきである。

- クラウド事業者は、明確にはっきりと、そのポリシー、要件、能力ならびにその提供するサービスに適用されるすべての条項・条件を開示すべきである。
- クラウド利用者は、契約にサインする前にクラウド事業者の提案を詳細に評価し、定期的にその評価を更新し、その利用するサービスの範囲、属性および一貫性を監視するべきである。
- クラウド事業者は、電子証拠開示などの法的責任に対応する自社のポリシー、要件、能力について情報公開し、顧客に提供すべきである。
- クラウド利用者は、特定のクラウド事業者を利用することの法的影響を理解し、自社の法的ニーズと照らし合わせるべきである。
- クラウド利用者は、クラウド事業者が情報を物理的に運用し保管していることの法的影響について理解すべきである。
- クラウド利用者は、自社の法管轄における対応要件の遵守のために、選択可能な場合には、自社のデータをどこにホストさせるかの選択を行うべきか判断すべきである。
- クラウド利用者とクラウド事業者は、電子証拠開示請求に対応するための法的および技術的要件について明確に理解しておくべきである。
- クラウド利用者は、クラウドサービス利用に際してのクリックで成立する契約は、デューデリジェンス実施のクラウド事業者への要求を否定することにならないことを理解すべきである。

DOMAIN 4
コンプライアンスと監査マネジメント

4.0　はじめに

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に対するコンプライアンスを実現し、測定し、伝えていくことは、これらの課題のうちの最も大きいものの一つである。利用者もクラウド事業者も同様に、法管轄上の違いと、既存のコンプライアンスと監査に関する基準、プロセス、および実務に対するその影響を理解し、認識する必要がある。クラウドコンピューティングの分散処理と仮想化という特性は、情報とプロセスが具体的かつ物理的インスタンスに基づくというアプローチに対して、大幅な変更を強いるものである。

また、クラウド事業者とクラウド利用者に加えて、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の配備に対応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、自らの組織が法令遵守していることを示す必要に迫られる。クラウドコンピューティングと規制環境の相互の関係を理解することは、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、監査人およびクラウド事業者は、以下の事項を考慮し、理解しなければならない:

- 特定のクラウドサービスまたはクラウド事業者を利用する場合の法規制の影響。国境をまたがる、あるいは複数の法管轄が関わる場合には、その問題に特に注意を要する。
- 間接的なクラウド事業者（すなわち、自分が利用しているクラウド事業者の（訳注:その基盤として使っている他の）クラウド事業者）を含むクラウド事業者とクラウド利用者間のコンプライアンス責任の分担。これには、コンプライアンス継承の概念（クラウド事業者が、そのサービスの一部について規制遵守の認証を受けている場合には、その部分はクラウド利用者の監査対象から除外される）が含まれる。しかし、クラウド利用者はそのクラウド事業者の上に構築されたあらゆるもののコンプライアンスに対して責任を持ち続ける。
- タイムリーな方法で、ドキュメント作成、証拠生成、および手続きの準拠性を含め、法規制に適合していることを示すクラウド事業者の能力。

これに加えて特別な注意が払われるべきクラウド特有の課題として、次のようなものがある：

- クラウド事業者の監査および認証の役割、ならびにこれらがクラウド利用者の監査（またはアセスメント）範囲へどのように影響するか。
- クラウド事業者のどの機能およびサービスが、監査およびアセスメントの範囲内になるのかの理解。
- コンプライアンスおよび監査を継続的にマネジメントすること。
- クラウドコンピューティング技術の経験が不足している可能性のある規制当局および監査人との連携。
- 監査や規制遵守の経験が不足している可能性のあるクラウド事業者との連携。

4.1 概要

過剰なまでの現代の規制および基準へのコンプライアンスを達成し維持することは、ほとんどの情報セキュリティチームにとって中核の活動であり、ガバナンスおよびリスクマネジメントの重要な手法である。そのため、この領域のツールおよびチームには、それ専用にガバナンス、リスク、コンプライアンスの頭字語：GRC がつくほどである。コンプライアンスをサポートし、保証し、実証するための重要なメカニズムである監査と密接に関係しているが、監査以上に重要なことがコンプライアンスにはあり、それらを規制に対するコンプライアンスの保証に利用することよりも重要なことが監査にはある。その目的は次のようなことである：

- コンプライアンスは、企業の義務（例えば、企業の社会的責任、倫理、適用法、規制、契約、戦略および方針）に対する認識と遵守を立証する。コンプライアンスプロセスは、認識と遵守の状態を評価し、さらにコンプライアンス達成のためのコストに対するコンプライス違反の場合のリスクおよび潜在的コストを評価し、優先順位付けをし、資金提供し、必要と考えられるすべての是正処置に着手する。
- 監査は、コンプライアンスを証明する（または反証する）ための重要なツールである。 同様に、コンプライアンス違反のリスク判断を支援するためにも監査とアセスメントを使用する。

このセクションでは、クラウドコンピューティングがそれぞれに及ぼす影響に焦点を当てるために、これらの相互に関連するドメインについて個別に説明する。

4.1.1 コンプライアンス

クラウドにおける（また、実際にはあらゆる）情報技術はますます、政府、業界団体、ビジネス関係者、およびその他の利害関係者からの過剰なまでの方針および規制の対象になっている。コンプライアンス管理はガバナンスの 1 つのツールであり、 組織が、どのように、これらの内部および外部の義務を満足しているかどうかを評価し、修正し、証明するものである。

特に規制は通常、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に対して強い影響力を持つ。多くの規制および義務は、一定のレベルのセキュリティを要求しており、そのために情報セキュリティはコンプライアンスと深く結びついている。従って、セキュリティコントロールはコンプライアンスを保証するための重要なツールであり、これらのコントロールの評価とテストはセキュリティ専門家の中核の活動である。これには、専任の内部監査人または外部監査人によって行われるアセスメントも含む。

4.1.1.1 クラウドはコンプライアンスをどのように変えるか

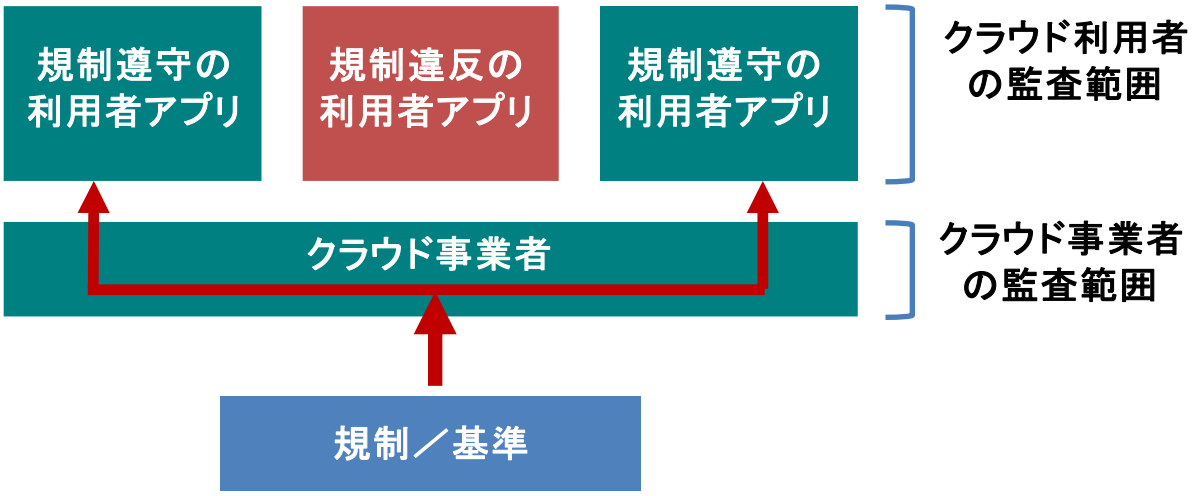
セキュリティと同様に、クラウドにおけるコンプライアンスは責任共有モデルである。クラウド事業者とクラウド利用者の両方に責任があるが、クラウド利用者が常に自己の最終的なコンプライアンス責任を負う。これらの責任は、契約、監査／アセスメントとコンプライアンス要件の仕様によって規定される。

クラウド利用者は、特にパブリッククラウドでは、自らのコンプライアンスとの整合性とギャップを把握するために、クラウド事業者の第三者評価証明に、より依存する必要がある。パブリッククラウド事業者はコストの管理を規模の経済性に頼っているため、多くの場合、クラウド利用者が独自の監査を実行することを認めていない。代わりに、公開企業の会計監査と同様に、彼らは第三者の事務所と監査を実施して評価証明を発行するための契約をする。従って、クラウド利用者は、通常、彼ら自身で監査範囲を定義したり、監査を実行したりすることはない。代わりに、そのサービスが彼らのコンプライアンス義務を満たしているかどうかを判断するために、これらのレポートおよび評価証明に頼る必要がある。

多くのクラウド事業者は、PCI DSS、SOC1、SOC2、HIPAA 等のさまざまな規制や業界の要求事項、

CSA CCM などのベストプラクティスやフレームワーク、および、EU GDPR などのグローバルあるいは地域の規制など、に対して認証を受けている。これらはパススルー監査と呼ばれることもある。パススルー監査はコンプライアンス継承の一形態である。このモデルでは、クラウド事業者のインフラストラクチャおよびサービスのすべてまたは一部は、コンプライアンス標準に対しての監査を受ける。クラウド事業者は、これらの認証のコストおよび維持に対して責任を持つ。パススルー監査を含むクラウド事業者に対する監査は、次のような制限内であることを理解する必要がある：

- クラウド事業者が基準に適合していることに対しての認証である。
- 基準に適合したアプリケーションおよびサービスをクラウド上に構築することは、引き続き、クラウド利用者の責任である。
- これは、クラウド事業者のインフラストラクチャやサービスは、クラウド利用者の監査やアセスメントの範囲内ではないことを意味する。しかし、クラウド利用者が構築するものはすべて、依然としてその範囲内である。
- クラウド利用者は、彼らが構築し管理するすべてのもののコンプライアンスを維持することに最終的に責任がある。例えば、IaaS クラウド事業者が、PCI DSS 認証を取得している場合、クラウド利用者はそのプラットフォームで独自の PCI 準拠サービスを構築でき、クラウド事業者のインフラストラクチャおよび運用は、クラウド利用者のアセスメントの範囲外となるだろう。しかしながら、クラウド利用者は、クラウド上で適切に動作するアプリケーションを設計しないと、容易に PCI に抵触してアセスメントに不合格になる。



> コンプライアンス継承により、クラウドプロバイダのインフラストラクチャはクラウド利用者のコンプライアンス監査の対象外となるが、クラウド利用者が認証されたサービスの上に構成し、構築するすべてのものは、引き続きその範囲内にある。

クラウドコンプライアンスの問題は、単にパススルー監査に限定されるものではない。クラウドの特性により、さらなる違いがもたらされる。

多くのクラウド事業者は、中央管理コンソール／プラットフォームの表示外の、グローバルに分散したデータセンタを提供している。 データおよびサービスをどこに配置するかを管理し、理解して、国内外の法域において法的コンプライアンスを維持することは依然として利用者の責任である。

組織は、伝統的なコンピューティングでも同じ責任を有しているが、クラウドは、このような国際的に配備するかもしれない時の面倒な手間を劇的に減少する。例えば、適切な統制で防ぐことができない場合には、開発者は、国際的なデータセンタを要求して複数の段階の契約を締結する必要に直面することなく、規制されているデータを非適合な国に配備してしまう可能性がある。

ある 1 つのクラウド事業者内のすべての機能およびサービスが、すべての規制および標準に準拠し、認証や監

査を受けているわけではない。クラウド事業者には、利用者が適用範囲および制限が理解できるよう、認証や評価証明について明確に伝達する義務がある。

4.1.2 監査マネジメント

適切な組織のガバナンスは、必然的に監査と保証を含む。監査は独立して行われなければならず、ベストプラクティス、適切な資源、並びに吟味された手続きおよび標準を反映するようしっかりと計画されるべきである。クラウドの影響を掘り下げる前に、情報セキュリティに関連する監査マネジメントの適用範囲を定義する必要がある。

監査およびアセスメントは、内部および外部の要求事項へのコンプライアンスを文書化する（または不備を特定する）ための仕組みである。報告には、発見された課題、リスク、および改善の推奨事項のリストと並んで、コンプライアンスの判断が含まれている必要がある。監査およびアセスメントは、情報セキュリティに限定されないが、情報セキュリティに関連するものは、通常、セキュリティマネジメントおよび統制の有効性を評価することに重点を置いている。ほとんどの組織は、内部と外部の要求事項へのコンプライアンスを保証するために、内部および外部の監査とアセスメントを組み合わせて実施する必要がある。

全ての監査には、都度設定可能な適用範囲と適用宣言書がある。これは、何を（例えば、財務データを持つ全てのシステム）、どのような統制（例えば、業界標準、特別の範囲、またはその両方）に対して評価するのかを定義する。評価証明は、第三者からの法的なステートメントであり、監査発見事項のステートメントとして使用することができる。クラウド利用者は、自分たち自身でのアセスメントを実施できるとは限らないため、評価証明は、クラウド事業者を評価して利用する際の重要なツールとなる。

監査マネジメントには、要求事項、範囲、スケジューリングおよび責任の決定など、監査およびアセスメントに関連するすべての活動の管理が含まれる。

4.1.2.1 クラウドは監査マネジメントをどのように変えるか

クラウド利用者の一部は、委託先の第三者を監査することに慣れているかもしれない。しかし、クラウドコンピューティングの特性およびクラウド事業者との契約のために、オンプレミスの監査のような事項が含まれないことが多い。クラウド利用者は、マルチテナントサービスを提供している場合には、クラウド事業者は、リスクに対するオンプレミスセキュリティ監査を検討できる（むしろすべき）ことを知っておくべきである。多くのクラウド利用者からの複数のオンプレミス監査の事例が、特にクラウド事業者が、リソースプールの作成を共有化された資産に依存している場合、明確なサービス構造上およびセキュリティ上の課題を指摘している。

これらのクラウド事業者を利用するクラウド利用者は、自身で行う監査よりむしろ、第三者の評価証明に、より頼らざるを得ないだろう。監査基準にもよるが、実際の結果は守秘義務契約（NDA）のもとでのみ開示される場合がある。そしてそれは、リスクアセスメントまたはその他の評価目的で評価証明にアクセスする前に、基本的な契約を締結する必要があることを意味する。これは、多くの場合、監査会社との法的または契約上の要求事項によるものであり、クラウド事業者が意図的に隠しているのではない。

クラウド事業者は、契約上および規制上の義務を満たしていることの保証を、クラウド利用者が依然として必要としていることを理解すべきであり、特にクラウド事業者がクラウド利用者の直接のアセスメントを認めていない場合、彼らが義務を果たしていること示すために、厳格な第三者の評価証明を提供すべきである。評価証明は業界標準に基づくもので、適用範囲をきちんと定義し、評価対象の管理策がリスト化されていなければならない。認証や評価証明の（法的に許可されている範囲での）公開は、クラウド利用者がクラウド事業者を評価する際に大いに役立つだろう。Cloud Security Alliance の STAR 登録は、クラウド事業者がこ

れらのドキュメントを一般向けに公開するための一元化したリポジトリを提供している。

SSAE 16 のようないくつかの基準は、文書化された管理策が、設計・要求されている通りに機能することを検証する。その基準は、必ずしも管理策の適用範囲を定義しているわけではないので、完全な評価を実施するためには、その両方が必要となる。 また、評価証明および認証は、クラウド事業者によって提供されるすべてのサービスに必ずしも等しく適用されるとは限らない。クラウド事業者は、どのサービスおよび機能に適用されているのかを明確にしておくべきであり、クラウド利用者は、クラウド事業者のそれらのサービスおよび機能を使用することが意味するところに注意を払い理解する責任がある。

ある種のクラウド利用者による技術アセスメントおよび監査（例えば脆弱性評価など）は、クラウド事業者のサービス利用規約で制限を受け、許可を必要とする場合がある。これは多くの場合、クラウド事業者が正当なアセスメントと攻撃を区別するためである。

評価証明および認証は、ある時点の活動であることを心にとめておくことは重要である。評価証明は、「ある期間の」アセスメントの結果報告であり、将来の時点では有効でない可能性がある。 クラウド事業者は、公表された結果を最新に保たなければならない。そうしないと、彼らはクラウド利用者をコンプライアンス違反のリスクにさらす危険性がある。契約によっては、これは、クラウド事業者にとっての法的な危険につながる可能性もある。同様にクラウド利用者は、最新の結果に依存していることを確認し、時間の経過とともにクラウド事業者の状態が変わるのを追跡する責任を負う。

事跡情報(artifacts)とはログ、ドキュメント、その他の資料であり、監査およびコンプライアンスに必要である。それらはコンプライアンス活動を裏付ける証拠である。クラウド事業者およびクラウド利用者の両者は、それぞれの事跡情報を作成し管理する責任がある。

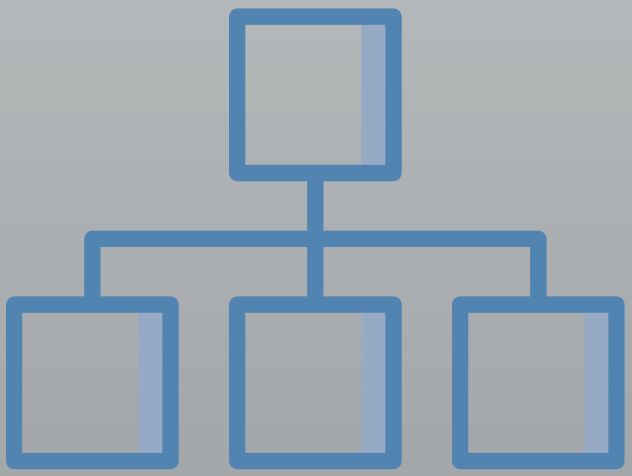
クラウドの事業者を利用している場合、コンプライアンスの事跡情報の収集と保存の態様は変化する

クラウド利用者は、自身の監査を裏付ける事跡情報に対する最終的な責任を負うため、クラウド事業者が何を提供するのかを知り、ギャップを埋めるために自前の事跡情報を作成する必要がある。例えば、PaaS 上のサーバーログが利用できない場合、アプリケーションにより強固なロギング機能を組み込む。

4.2　推奨事項

- コンプライアンス、監査および保証は継続的に行われるべきである。それは単なるある時点の活動であると見なすべきでなく、多くの標準と規制がこのモデルに向けて動いている。このことは、クラウド事業者およびクラウド利用者の両者が、常に変化し、固定的な状態になることがめったにないクラウドコンピューティングにおいては、特に当てはまる。
- クラウド事業者は、次のことをすべきである。
    - 次の事項に特に留意して、監査結果、認証、および評価証明を明確に伝達する。
        - アセスメントの適用範囲。
        - どのサービス／機能が、どの所在地や法管轄に帰属するのか。
        - クラウド利用者が、法令に適合しているアプリケーションおよびサービスをクラウドに展開する方法。
        - 追加されるクラウド利用者の責任と制約事項。
    - クラウド事業者は、認証／評価証明を継続的にメンテナンスし、いかなる状況の変化も前もって伝達しなければならない。
    - クラウド事業者は、コンプライアンスに継続的に取り組み、コンプライアンスからの乖離が生ずることを防止し、それによって顧客をリスクにさらさないようにするべきである。
    - クラウド利用者が他の方法では自ら収集できない管理者の行為のログのような、クラウド利用者が必要とするコンプライアンスに関する証拠および事跡情報を提供すること。
- クラウド利用者は、次のことをすることが望ましい。：
    - クラウドへの配備・移行、クラウドでの開発をする前に、すべてのコンプライアンス義務を理解すること。
    - クラウド事業者の第三者による評価証明および認証を検証し、コンプライアンスのニーズと整合させること。
    - 対象としている管理策および機能／サービスの両方を含め、アセスメントおよび認証の適用範囲を把握すること。
    - クラウドコンピューティングの経験を有する監査人を選定するよう努めること。特に、パススルー監査および認証を、クラウド利用者の監査範囲に対応するために使用する場合には。
    - クラウド事業者がどのようなコンプライアンスの事跡情報を提供するかを理解し、それらの事跡情報を効果的に収集し管理することを確実にすること。
        - クラウド事業者の事跡情報が十分でない場合、自身で事跡情報を作成し収集すること。
    - 使用するクラウド事業者の登録、関連するコンプライアンス要求事項、および現在の状況の情報を保存すること。 Cloud Security Alliance の Cloud Controls Matrix は、この取組みに役立つ。

DOMAIN 5
情報ガバナンス



5.0　はじめに

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礎となるデータを守ることである。企業のクラウドコンピューティングへの移行に際して、従来のデータ保護手法は、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の配備において、ユーザは、たった数年前には考えられなかったやり方で、データを外部環境（あるいはパブリック環境）に移転している。

クラウドコンピューティングの時代における情報管理は、あらゆる組織に影響する難題であり、単に新しい技術的保護だけでなく、基本的なガバナンスへの新しいアプローチを必要とする。クラウドコンピューティングは、情報ガバナンスのすべての分野に少なくとも何らかの影響を及ぼすが、第三者との作業や司法管轄上の境界（jurisdictional boundaries）への対応に関する複雑さを増加させる結果、特にコンプライアンス、プライバシーまたは企業ポリシーに影響を与える。

> データと情報の使用が、規制上、契約上および事業上の目的を含む、組織のポリシー、基準および戦略に準拠していることを確実にする

我々が扱うデータは、常にさまざまな要求事項の対象となる。それらは規制当局、顧客またはパートナー等によって課されるものもあれば、自社のリスク許容度や望ましい業務管理方法に基づいて自主的に定義されるものもある。情報ガバナンスには、目標や要求事項に従ってデータを確実に処理するために用いる企業の体制と統制が含まれる。

クラウドにデータを格納することには、情報とデータのガバナンス上の要求事項に影響する数多くの要素が存在する。

- **マルチテナンシー：**マルチテナンシーは、セキュリティへの複雑な影響をもたらす。パブリッククラウドに保管される場合、データは他の信頼していないテナントと共有されたインフラストラクチャに格納されることになる。プライベートクラウド環境に保管される場合も、ガバナンスの要件が異なるかも知れない他のビジネスユニットとの間で共有されるインフラストラクチャに格納され、管理されることになる。
- **セキュリティ責任の共有：**環境の共有度を高めることは、セキュリティ責任の共有度をも高める。データは今や、異なるチームや組織によって所有され、管理されるようになっている。よって、データを保管すること(custodianship)と所有すること(ownership)の違いを認識することが重要である。
    - **所有権(Ownership)**は、その名が示す通り「誰がデータを所有しているか」を指す。それは常に完全に明確になっているわけではない。法律、契約またはポリシーによっては、顧客がデータを

提供する場合、自社がデータを所有することになる場合もあれば、依然として法的に顧客がデータを所有している場合もある。パブリッククラウド事業者にデータを置く場合、自社がそのデータを所有しているべきであるが、それもまた契約次第である。

- **保管権（Custodianship）**とは、「誰がデータを管理しているか」を指す。顧客が貴組織に個人情報を提供し、貴組織がその情報を所有する権利を持たない場合、貴組織は単なる保管者（custodian）である。すなわち、あらかじめ承認された方法でのみ使用できる。貴組織がパブリッククラウド事業者を使用している場合、クラウド事業者がデータの保管者となるが、貴組織が自ら実装し、運営している管理内容によっては、貴組織も保管者としての責任を有するかもしれない。クラウド事業者を利用しても、貴組織の責任を回避できるわけではない。基本的に、データの所有者がルールを（時には規制を通して間接的に）定義し、保管者（custodian）がルールを実装する。所有者と保管者の間の境界線や役割分担は、特にパブリッククラウドの場合、クラウドインフラストラクチャの影響を受ける。

クラウドで顧客データを取り扱う場合、第三者であるクラウド事業者を、ガバナンス・モデルに組み込むことになる。

- **司法管轄上の境界（jurisdictional boundaries）とデータ主権（data sovereignty）：**クラウドはその定義上、幅広いネットワークアクセスを可能にするものであり、より多くの場所（司法管轄(jurisdictions)）でデータがホストされる可能性は増加し、一方データを移行する側の手間は低減される。クラウド事業者の中には、データの物理的な位置が明確でないものもあり、他の場合にはデータの特定の場所への移動を制限するために追加のコントロールが必要な場合もある。
- **コンプライアンス、規制、プライバシーポリシー：**これらの問題は、第三者のクラウド事業者と司法管轄が変わることが合わさることによって、クラウドの影響を受ける可能性がある。例えば、顧客との契約によって、クラウド事業者（の環境）上でデータを共有／使用することが認められていない場合や、（暗号化などの）特定のセキュリティ要件が含まれている場合などである。
- **データの破棄と削除：**この問題は、クラウドプラットフォームの技術的能力と関連する。ポリシーに従ったデータの破棄や削除を確実にできるかが問題である。

クラウドに移行する場合、情報アーキテクチャを再検討する機会とすべきである。現在の情報アーキテクチャの多くは、場合によっては数十年にわたって絶え間なく変化する技術の上に実装されてきているため、今日においては相当の不整合があると言える。クラウドへの移行は、情報の管理方法を再検討し、改善する方法を発見するためにゼロからスタートする機会を作り出す。既存の問題をそのまま持ち込むべきではない。

5.1　概要

データ／情報ガバナンスとは、データと情報の使用が、組織のポリシー、基準および戦略に準拠していることを確実にすることを意味する。これには規制上、契約上、ビジネス上の要件と目的などが含まれる。データと情報とは異なるものであるが、それらを区別しないで使用する傾向がある。情報は、価値のあるデータである。この章の目指すところに関しては、両方の用語を同じ意味で用いている。

5.1.1　クラウドにおける情報ガバナンスの項目

ここではデータガバナンスのすべてをカバーする積りはないが、クラウドにおけるデータの取り扱いがそのガバナンスに影響する項目に焦点を当てる。クラウドコンピューティングは、データガバナンスの多くの項目に影響する。：

- **情報の分類**　この項目は、コンプライアンスとの関係が強く、クラウドへの移行・移送と処理上の要件に影響する。データ分類のプログラムをあらゆる主体が有しているわけではないが、プログラムを有している場合は、クラウドコンピューティングに合わせた調整が必要となる。
- **情報管理ポリシー**　この項目は、情報の分類に関連し、情報管理ポリシーがある場合は、クラウドを追加する必要がある。また、SaaS 事業者へのデータ送信と自社用の IaaS アプリの構築では大きく異なってくるため、ポリシーは SPI の各々の層をカバーするものである必要がある。どのような情報がクラウド内のいかなる場所に行くことを許可されるか、どの製品とサービスによるか、そして、どのようなセキュリティ要件が必要か、といったことを判断する必要がある。
- **所在場所と司法管轄ポリシー**　これらは特に直接にクラウドに関連する。全ての外部へのホスティングは、所在場所および司法管轄上の要件を満たさなければならない。内部のポリシーはクラウドコンピューティングに対応して変更可能だが、法的要求は厳格なものである。（この点の詳細については、法的事項に関するドメインを参照。）条約や法律が（ポリシーとの）不一致を引き起こしうることを理解しておく必要がある。最善のコンプライアンスを確実にするために、規制されたデータを扱う際には法務部門と協力する必要がある。
- **認可（Authorizations）**　クラウドコンピューティングが認可（Authorizations）に与える影響は最小限であるが、クラウドによる影響の有無を判断するために、データセキュリティライフサイクルを確認する必要がある。
- **所有権**　組織は常にデータと情報についての責任を有しており、クラウドに移行することによって、それを転嫁することはできない。
- **保管権（Custodianship）**　クラウド事業者は保管者（Custodian）になりうる。適切に暗号化されていると言えども、（クラウドに）ホストされたデータは、依然として元の組織の保管権の下にある。
- **プライバシー**　プライバシーとは、規制上の要求事項、契約上の義務、顧客に対するコミットメント（例：公式声明（public statements））の総和である。すべての要求事項を理解し、情報管理ポリシーとセキュリティポリシーを、確実に整合させる必要がある。
- **契約によるコントロール**　この項目は、クラウドプロバイダのような第三者にガバナンス上の要求事項を拡張して適用するための法的ツールとなる。
- **セキュリティコントロール**　この項目は、データガバナンスを実装するためのツールである。クラウドコンピューティングにおいては、その態様が大きく変化する。データセキュリティと暗号化のドメインを参照のこと。

5.1.2　データセキュリティライフサイクル

情報ライフサイクル管理は、極めて成熟した分野ではあるが、セキュリティ専門家のニーズによく対応したものとは言えない。データセキュリティライフサイクルは、情報ライフサイクル管理とは異なり、セキュリティ関係者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 から入手できる。

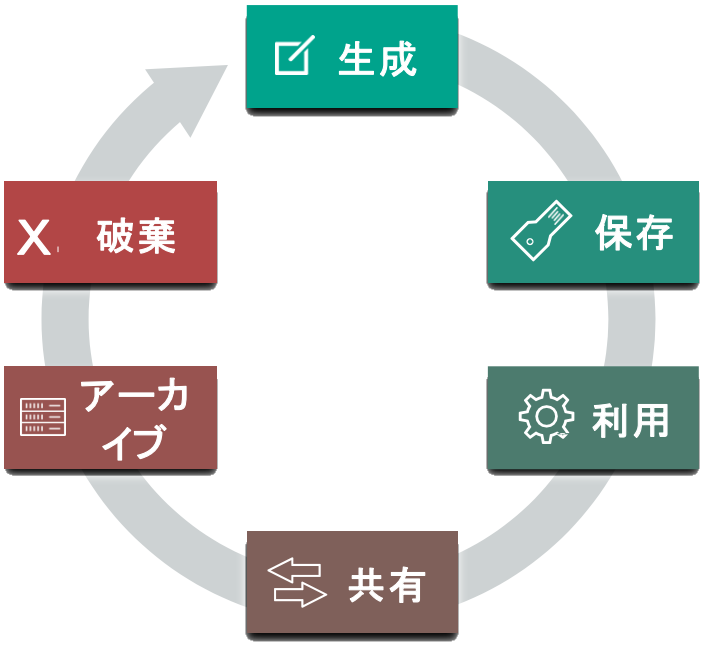
データセキュリティライフサイクルは、データに関するセキュリティ境界とコントロールを理解するのに役立つツールであるが、すべてのタイプのデータに対する厳密なツールとしての利用を想定したものではない。データセキュリティを大ぐくりのレベルで評価し、焦点を当てるべきポイントを発見することを支援するモデリングツールである。

ライフサイクルは生成から破棄まで６つのフェーズに分かれている。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ようにもなり、また、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）。

Create（生成） 生成とは、新しくデジタルコンテンツを作成すること、あるいは既存コンテンツを変更／更新／修正することを指す。

Store（保存） 保存とは、デジタルデータを何らかの保存格納場所に収納する作業で、通常はデータの生成とほぼ同時に起こる。

Use（利用） データが、閲覧、処理、その他の活動に利用される。ただし、修正はこれに含まれない。



データセキュリティライフサイクル

Share（共有） 情報を、ユーザ相互間、顧客向け、パートナー向けなどのように、第三者からアクセスできるようにする。

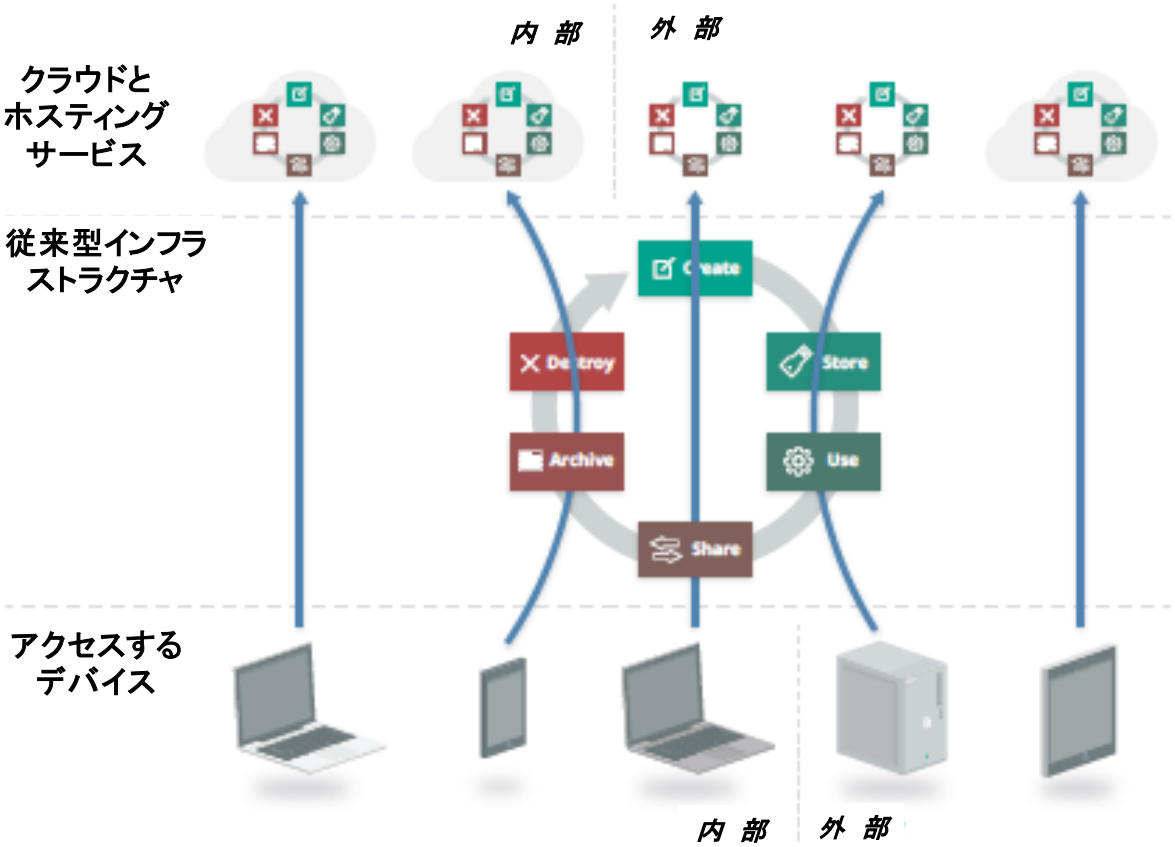
Archive（アーカイブ） データがアクティブには利用されなくなり、長期保存に回される。

Destroy（破棄） データが、物理的またはデジタルな手法（例えば cryptoshredding）によって恒久的に破棄される。

5.1.2.1 所在場所と権限付与

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、情報のロケーションやどのようなアクセスを受けるかは示していない。

所在場所　この図においてライフサイクルは、単一で一方向の動作ではなく、異なる動作環境で実行されるより小さなライフサイクルの連続として考えられている。データは、ほぼあらゆるフェーズにおいて、これらの環境に出入りし、その間を移動することができる。



データはアクセスされ、複数の場所に格納され、それぞれ独自にライフサイクルがある。

起こりうる全ての規制、契約、その他の司法上の問題に備え、データの論理的、物理的な所在場所を把握することは極めて重要である。

権限付与　データの所在や動作を把握するに際し、ユーザは、アクセスする人物とその方法を知る必要がある。以下の二つの要素がある:

- 誰がデータにアクセスするのか
- どのような方法（デバイスやチャネル）でアクセスするのか

今日、データは多種のデバイスから幅広くアクセスされる。デバイスはそれぞれ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クライアントを用いている。

5.1.2.2　機能、主体、コントロール

次のステップは、主体(人またはシステム）と所在場所によって、データに対して実行される機能を特定することである。

*機能。*あるデータに対して、３つのことが可能である:

- **Read (読込)**　データの閲覧／読込（生成、複製、ファイル転送、配布、その他の情報交換を含む）

- **Process (処理)** データに対する処理の実行（データ更新、業務実行処理での利用など）
- **Store (保存)** （ファイルやデータベースにおける）データの保持。
- 以下の表は、機能とライフサイクル上のフェーズとの対応関係を示している:

	作成	保存	利用	共有	アーカイブ	破棄
読込	×	×	×	×	×	×
処理	×		×			
保存		×			×	

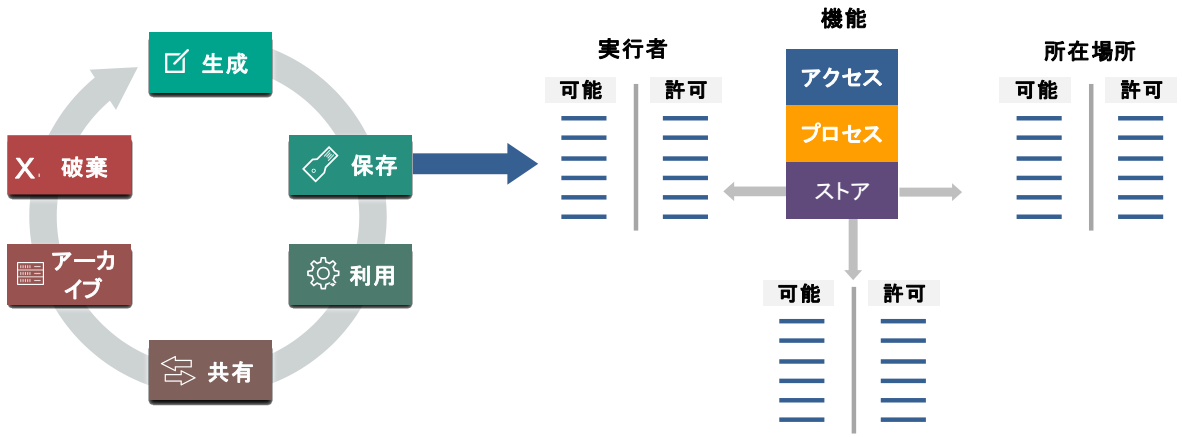
表 1 情報ライフサイクルのフェーズ

ある主体（アクセス用デバイスではなく、人、アプリケーション、またはシステム／プロセス）は、ある所在場所において、各機能を実行する。

コントロール:コントロールは、実行可能な動作のリストを制限して、許可されている動作に絞り込む。以下の表は、実行可能な動作のリストの一例を示しており、それをユーザがコントロールに対応づける。

機能		動作		所在場所	
可能	許可	可能	許可	可能	許可

機能とコントロールへのライフサイクルのマッピング

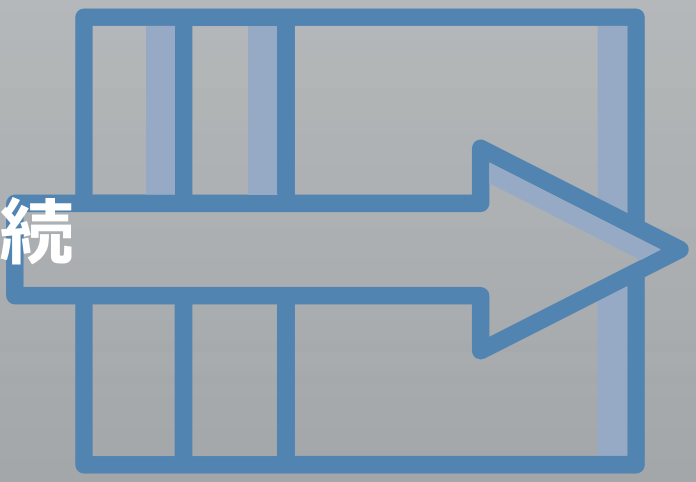


ライフサイクルの機能とコントロールへの対応付け

5.2　推奨事項

- クラウドへの移行を計画する前に、情報のガバナンス要件を決定すること。それには法的および規制上の要件、契約上の義務およびその他の企業ポリシーを含む。企業のポリシーと基準については、第三者がデータを取り扱うことができるように更新する必要があるかもしれない。
- 情報ガバナンスポリシーと実施規範のクラウドへの拡大適用を確実にすること。これらは契約およびセキュリティ上のコントロールを通じて実現できる。
- 必要に応じて、データ処理とコントロールのモデルを作る助けとして、データセキュリティライフサイクルを使用すること。
- 既存の情報アーキテクチャを当てはめる代わりに、クラウドへの移行の機会を利用して、既存のインフラストラクチャでしばしば使用されている不完全なやり方によるものを再検討し、再構築すること。 悪しき慣行を持ち込まないこと。

DOMAIN 6
管理画面と事業継続



6.0　はじめに

管理画面（管理用ダッシュボード）は、従来型インフラストラクチャとクラウドコンピューティングの間の違いとしては最も顕著な唯一のものである。これはメタストラクチャ（ドメイン 1 で定義）のすべてではないが、メタストラクチャとの接続やクラウドに関する多くの設定を行うためのインターフェイスである。

通常、インフラストラクチャやプラットフォーム、またアプリケーションを管理するために使用するツールおよびインターフェイスとして管理用ダッシュボードはある。しかしクラウドの場合、リソースの管理を抽象化し一点に集約する。筐体や配線を使ってデータセンタの構成を設定・変更するのでなく、クラウドは今や、API コールと Web コンソールを用いて管理されている。

誰が管理用ダッシュボードにアクセスできて何を行うことができるかを制限する適切なセキュリティ管理を施さない場合、管理用ダッシュボードへのアクセスを与えることはデータセンタへの無条件なアクセスを与えることになる。

セキュリティ面で考えると、従来は個別のシステムやツールを通じて管理してきた多くの事項について、管理用ダッシュボードに一まとめにされ、さらに単純な認証情報だけでインターネットからアクセスを可能にすることになる。このことは、セキュリティにとってマイナスばかりでなくプラスももたらすが、最も明らかに違う部分で、またセキュリティをどのように評価し管理する必要があるかということに影響を与えるものである。

集約することはまた、セキュリティ上のメリットももたらす。見えないリソースなどは存在せず、所管するすべてが常時どこにあるか、またどのような構成であるかを常に知ることができる。これは、広範囲のネットワークアクセスと従量制サービスによってもたらされる特性といえる。クラウド管理者は、プール内にあるリソースは何で、何が外に出されたか、そしてそれらはどこに割り当てられているか、を常に知る必要がある。

このことは、クラウド化するすべての資産が同じように管理されるということを意味しない。クラウドの管理者は稼働中のサーバを覗き見ることもロックされたファイルを開くこともできない。また特定のデータや情報の持つ意味について知ることもできない。

結局これは、ドメイン 1 で、また本ガイダンスを通じて語っている責任共有モデルの拡張である。クラウドの管理用ダッシュボードはリソースプールの中の資産の管理を引き受ける一方、クラウド利用者はそれら資産をどのように設定するかと、クラウド内に持ち込む資産に対して責任を負う。

- クラウド事業者は、管理用ダッシュボードがセキュアであり、必要なセキュリティの機能がクラウド利用者に示されていることに責任を負う。例えば、管理用ダッシュボードにアクセスできる者が何が可能かをコントロールする、細部にわたる権限付与の機能が該当する。

- クラウド利用者は、管理用ダッシュボードの利用に際して適切な設定を行うことと、認証情報をセキュアに管理することに対して責任を有する。

6.0.1 クラウドにおける事業継続と災害復旧

事業継続と災害復旧(BC/DR)は、他のあらゆる技術と同様にクラウドコンピューティングにおいても重要である。第三者の提供事業者（事業継続と災害復旧の場合しばしば関係する）が関係するかもしれないことによる変化は別として、共有資源を利用する際に必然的に起こる変化に対して留意が必要である。

クラウドにおける事業継続と災害復旧に関する主要な側面は以下の 3 つである

- 対象となるクラウド事業者の範囲内で事業継続と復旧ができるようにすること。これらは、クラウドに配備したものを最適に構成するためのツールであり技術であって、それにより、利用者資産の毀損やクラウド事業者側の一部の毀損が生じた場合でも、稼働を維持することができる。
- クラウド事業者のサービス停止に対する準備と管理。クラウド事業者のサービス停止は、その事業者の範囲で対応可能な限定的な障害から、組み込んであった災害復旧の能力を超えてクラウド事業者の全部または一部が停止するような、さらに広範な機能停止まである。
- クラウド事業者やプラットフォームを移行する必要がある場合に備えて、移植可能性の選択肢を検討しておく。そう言った場合とは、別の機能セットが必要な場合から、クラウド事業者が廃業したり、事業者と法的係争が生じた場合などに、事業者（の利用）が完全に失われる場合まであらゆるものがある。

6.0.1.1 障害に対する備え

クラウドプラットフォームは非常に耐障害性が高いが、クラウドの資産の一つひとつは従来型のインフラの場合よりも概して耐障害性が劣る。これは非常に複雑な環境で稼働する仮想化されたリソースに本来的に内在するもろさの故である。

このことはコンピュータ、ネットワーク、ストレージにほとんど当てはまる。なぜならばこれらのものはより多く直接アクセスを受けるからである。クラウド事業者は、そのプラットフォームやアプリケーションのために、IaaS 上で動作する耐障害性技術を追加して利用することができる。

しかし、このことが意味するところはクラウド事業者が、耐障害性を改善する選択肢を提示する場合が多いことを意味する。それは、多くの場合従来型のインフラにおいて（同等のコストで）達成できるレベル以上のものである。例えば、複数の「ゾーン」を機能させることにより、物理的に別個のデータセンタを包含する自動スケーリングのグループ内に仮想マシンを配備して、高い可用性を実現できる。アプリケーションをゾーン間でバランスをとって配置することで、あるゾーンが仮に完全に停止しても、アプリケーションは依然として動作する。これを従来型のデータセンタで実装することは実に困難である。相互隔離された複数の物理的ゾーンを設けて、系の自動切り替え機能付きでゾーン間のロードバランスがついたアプリケーションを配備できるようにすることは、通常費用対効果があるとはいえない。

しかしこのような特別な耐障害性は、これらの機能を活用すべく構造設計する場合のみ、実現できる。1 つのゾーンへすべてのアプリケーションを配備したり、あるいは単に単一ゾーン内の単一の仮想マシンへ配備した場合は、単一の良く整備された物理サーバへの配備と比較して、耐障害性が劣る可能性が高い。

このことがあるので、構造設計の変更なしに既存のアプリケーションをそのまま丸ごと移行させることで、耐障害性を低下させる可能性がある。既存アプリケーションが、これらの耐障害性のオプションの下で動作するように構造設計され配備されることはほとんどない。その上さらに、仮想化や変更のないそのままの移行で、個々に障害が発生する確率が高まる。

管理のために要求される能力の程度は、まさにセキュリティと同様に、IaaS の場合は高く、SaaS の場合ははるかに低い。SaaS においてはアプリケーションサービス全体の維持をクラウド事業者に依存することになる。IaaS では障害への対応を自ら構成できるが、その分自身の責任は重くなる。PaaS は、当然ながらその中間に位置する。PaaS の中には、構成可能な耐障害性オプションを有するものもあり、その他のプラットフォームはクラウド事業者の掌中にある。

全体として、リスクベースのアプローチが鍵となる。

- すべての資産が同レベルの継続性を要する訳ではないこと。
- コントロールを失うからと言って、クラウド事業者が完全にサービス停止に陥ることに備えようとして、混乱をきたさないこと。過去の実例を参照すること。
- 従来型のインフラと同等の RTO（目標復旧時間：Recovery Time Objective）および RPO（目標復旧地点：Recovery Point Objective）を設計するようにすること。

6.1 概要

6.1.1 管理用ダッシュボードのセキュリティ

管理用ダッシュボードはクラウドにおける資産管理のためのインターフェイスを指す。仮想ネットワーク上に仮想マシンを配備する場合、管理用ダッシュボードはマシンを起動しネットワークを設定するための手段である。SaaS では、管理用ダッシュボードの役割は往々にして利用者インターフェイスの「管理」タブであり、ユーザの設定や組織の構成の設定を行う場所である。

管理用ダッシュボードはメタストラクチャ（ドメイン 1 で定義）を管理し構成設定するものであり、またそれ自体がメタストラクチャの一部である。念のためにいえば、クラウドコンピューティングは（ネットワークやプロセッサのような）物理資産を取り入れ、それらを用いてリソースプールを構築する行為である。メタストラクチャはリソースプールの作成、提供、回収のための接着剤であり剥離剤である。管理用ダッシュボードにはクラウドそれ自体の構築や管理のためのインターフェイスが含まれ、またクラウド利用者が自身に割り当てられたクラウドリソースを管理するためのインターフェイスも含まれる。

管理用ダッシュボードは、マルチテナント状態における分離と隔離を実現し適用するための鍵となるツールである。管理用ダッシュボードの API によって誰が何をできるかを制限することは、クラウド利用者間、または一つのテナントの中のユーザ相互間の分離のための重要な手段である。リソースはプールに取り込まれ、プールから取り出され、ユーザに割り当てられる。

6.1.1.1 管理用ダッシュボードへのアクセス

API と Web コンソールは管理用ダッシュボードを提供する手段である。アプリケーションプログラミングインターフェース（API）はクラウドのプログラムによる管理を可能にする。それらはクラウドの構成要素を結合し、それらの統合化を可能にする接着剤となる。誰もがクラウド管理のためのプログラムを書くわけではないため、Web コンソールによって目で見るインターフェイスを提供している。多くの場合に Web コンソールはただ単に、直接アク

セス可能な同一の API を用いる。

クラウド事業者やクラウドプラットフォームはまた多くの場合、API との接続を容易にするための、ソフトウェア開発キット（SDKs）やコマンドラインインターフェース（CLIs）を提供している。

- **Web コンソール**はクラウド事業者によって管理される。それらは組織ごとに個別のものにすることができる（一般的には、アイデンティティ連携に紐づけた DNS リダイレクトを用いて）。例えばクラウドのファイル共有アプリケーションに接続する際、ログイン後にアプリケーションのユーザごとに専用の「バージョン」にリダイレクトされる。この「バージョン」は、それに紐づいたドメイン名を持ち、フェデレーションされた ID との接続を容易にする（例えばクラウド利用者内の全てのユーザが"application.com"にログインするのでなく"自組織名. application.com" にログインする）。

上述した様に、大抵の Web コンソールは、直接アクセスが可能な同一の API のためのユーザインタフェイスを提供する。しかしながら、プラットフォームもしくは事業者の開発プロセス次第で、Web フィーチャーあるいは API コールが互いに 1 つ前の画面に現れるといった不整合に直面することが時折あるかもしれない。

クラウドサービス向けの **API** は、インターネット経由で実行が容易との理由から、概して **REST** が用いられる。REST API は、HTTP/S 上で動作すること、またその結果多様な環境にわたって上手く機能することから、Web ベースのサービス向けの標準となった。

REST API は、認証の標準が単一に規定されていないために、多様な認証手段を用いることができる。HTTP リクエスト署名と OAuth が（認証手段として）最も一般的である。またこれらの両方が認証要求の検証のために暗号化技術を利用している。

リクエストの中にパスワードを埋め込むサービスを今でも多く見かける。これは認証情報が外から見えるという点でセキュアでなく、より高いリスクを伴う。そのことが最も頻繁に見られるのは、最初に Web インターフェイスを構築し、利用者 API を単に後付けする様な、古い、あるいは不十分な設計の Web プラットフォームにおいてである。こうしたことに直面した場合には、認証情報が外から見える可能性を減らすために、可能であれば API アクセスのための専用アカウントを用いる必要がある。

6.1.1.2 管理用ダッシュボードのセキュリティ

アイデンティティ／アクセス管理（IAM）には、本人確認(identification)、認証(authentication)、そして認可(authorizations アクセス管理を含む)が含まれる。このことは、利用するクラウドプラットフォームあるいはクラウド事業者の中で、誰が何をできるかをいかに決定するかを意味する。

事業者固有のオプション、構成設定、そして概念さえも、クラウド事業者やプラットフォームが違えば大きく異なる。クラウドごとに独自の実装があり、「グループ」や「ロール」といった言葉の定義でさえも、同じとは限らない。

それがプラットフォームであってもクラウド事業者であっても、全体の構成設定を管理するためのスーパーアドミン特権を有するアカウント所有者が常に存在する。この権限は、（個人ではなく）企業の所管に帰属し、厳重に格納され、ほぼ使用されることがないくらいであるべきである。

アカウント保持者とは別に、通常、個別のアドミンが使うための、スーパーアドミンアカウントを新設できる。このような特権は限定的に使うべきである。また使える範囲は少人数のグループとすべきである。なぜならば、これらのアカウントの一つが侵害されあるいは悪用されると、何者かが実質的にあらゆるすべてのことを変更できてしまうからである。

クラウドプラットフォームあるいはクラウド事業者は、サービス各部分の管理のみ可能な、より低いレベルの管理アカウントを提供する場合がある。これらは「サービス管理者」あるいは「日替わり管理者」と呼ばれたりする。これらのアカウントは仮に悪用され、あるいは侵害されても、必ずしも全体の配置を見せてしまうものではなく、従って日常の通常使用にとってはより望ましいものといえる。このようなアカウントはまた、個別のセッションを区分化することを容易にする。一人のアドミンの人間に複数のサービスアドミンアカウント（またはロール）へのアクセスを認めることは普通にあるが、その場合、アドミンは特定の作業に必要な権限に限定したログインとなり、より大きい範囲の権限を利用可能にすることにならずに済む。

基本的なクラウド管理プレーンにおけるユーザアカウントの例。スーパーアドミン、サービスアドミンを含む。

クラウド事業者とクラウド利用者は共に一貫して、エンドユーザごと、アプリケーションごと、またその他の管理用ダッシュボードの利用ごとに必要な、最小限の特権だけを許可するようにすべきである。

すべての特権ユーザーアカウントは多要素認証（MFA：Multi-Factor Authentication）を利用すべきである。可能であれば、（個別のユーザーアカウントをも含む）**すべての**クラウドアカウントは MFA を利用すべきである。それは様々な攻撃に対して防御するのに、単一手段による最も効率的なセキュリティ管理策の 1 つである。このことはまたサービスモデルにかかわらず当てはまる。すなわち、MFA はまさに、IaaS 用と同様に SaaS 用としても重要である。

（IAM とフェデレーションおよび強力な認証の役割については、IAM のドメインを参照されたい。その多くはクラウドの管理用ダッシュボードにも適用される。）

6.1.1.3 クラウドサービス構築／提供の際の管理用ダッシュボードのセキュリティ

例えばプライベートクラウドにおいて、管理用ダッシュボード自体の構築と保守に対して責任を負う立場であれば、その責任は大きい。クラウドを利用する立場であれば、クラウド事業者が提供する管理用ダッシュボードの一部の設定を行うだけだが、クラウド事業者の立場であれば、全てのことに責任がある。

実装作業の細部に深入りすることは本ガイダンスの範疇を超えることになるが、大まかに言って、管理用ダッシュボードをセキュアに構築し管理する上で、5 つの主要な要素がある。

- **境界セキュリティ：**Web サーバや API サーバなどの管理用ダッシュボードの構成要素自体に対する攻撃からの防御。下位レイヤにおけるネットワーク攻撃から上位レイヤでのアプリケーションへの攻撃までが対象となる。
- **利用者認証：**利用者が管理用ダッシュボードに対する認証を行う上での安全な仕組みの提供。これには、暗号的に有効で十分に文書化された（OAuth あるいは HTTP リクエスト署名の様な）既存の標準規格を利用すべきである。利用者認証は、一つの選択肢あるいは要件として MFA をサポートしているべきである。
- **内部認証と認証情報提供：**従業員が管理用ダッシュボードの顧客向け以外の部分に接続するのに利用する仕組み。これには、クラウド利用者の認証と内部の API リクエストとの間の情報変換も含む。クラウド事業者は、クラウド管理への認証には、常に MFA を義務付けるべきである。
- **認可と権限付与：**クラウド利用者が利用可能な権限付与と、組織内アドミンが行う権限付与。クラウド利用者が行う詳細な権限付与で、自組織内のエンドユーザとアドミンの安全な管理をよりやり易くする。組織内で行われるきめ細かい権限付与は、アドミンのアカウントが侵害されることや、従業員による悪用の被害を緩和する。
- **ログ記録、監視、および警報：**アドミンの活動をしっかりロギングしモニタすることは、実効あるセキュリティとコンプライアンスの管理にとって重要である。このことは、クラウド利用者がそのアカウント上で行うことと、自組織の従業員が日々のサービス管理において行うことの両方に当てはまる。異常な事象に対する警報は重要なセキュリティコントロールで、監視が有効に機能しており、単なる事後に眺めるだけのものでないことを保証するものである。クラウド利用者は理想的には、クラウドプラットフォーム上の自組織の動きのログに、API あるはその他の仕組みを通じてアクセスでき、自組織のロギングシステムに統合できるようにするべきである。

6.1.2 事業継続と災害復旧

セキュリティやコンプライアンスがそうである様に、事業継続と災害復旧（BC/DR）は共同責任である。クラウド事業者が管理するべき要素がいくつかあるが、クラウド利用者もまたクラウドサービスをいかに利用し管理するかということに最終的に責任を負う。このことはとりわけ、クラウド事業者（あるいはクラウド事業者のサービスの一部）の停止に対応する計画作りに当てはまる。

またセキュリティと同様、利用者は IaaS においてより多くの管理権限と責任を有し、それは SaaS では少なく、PaaS ではその中間である。

事業継続と災害復旧においてはリスクベースのアプローチをとらなければならない。事業継続に関する対策の多くはクラウドにおいてはコスト的に無理かもしれないが、同時に不要な場合もある。このことは従来型のデータセンタでも同様であるが、物理的なコントロールを失うことに対する過度の補償を求めることは稀ではない。例えば、大規模 IaaS 事業者の撤退やビジネスモデルの完全な転換の確率は低いが、より小規模なベンチャーによる SaaS 事業者においてはそれほど稀なものではない。

- リスク判断を形成する役に立つので、一定期間内のサービス停止に関する統計値をクラウド事業者に要求すること。
- クラウド事業者ごとに機能・能力が異なることに留意し、またそのことをベンダ選別過程（での判断要素）に含むべきこと。

6.1.2.1 クラウド事業者の側における事業継続

資産をクラウドに配備する際、クラウドが存続し続け、あるいは思った通りに機能するものと想定することはでき

ない。停止やトラブルは他の技術と何ら変わることなくある。ただし、クラウド事業者が耐障害性を持ったアプリケーションの構築を容易にする仕組みを組み入れた場合には、クラウドは全体としてより高い耐障害性を持つことができる。

このことは大事な点で、もう少し詳しく見る必要がある。すなわち、いくつかの箇所で述べてきた様に、資源を仮想化してプールすることの特性からして、仮想マシンなどの各個別の資産にとっては耐障害性が落ちることになる。一方で、リソースの抽象化とソフトウェアですべてを管理することは、柔軟性をもたらし、耐性のあるストレージや地域間で分散するロードバランシングの様に、耐障害性という機能をより容易に実現できるようになる。

選択肢の幅は非常に大きく、全てのクラウド事業者やクラウドプラットフォームが同様に作られている訳ではない。しかし、一般用語としての「クラウド」が従来型のインフラストラクチャより多少とも耐障害性を有すると想定するべきでない。よい場合もあるし悪い場合もある。その違いの全ては、リスクアセスメント次第であり、クラウドサービスをいかに使うか次第によっているのである。

このことが、クラウドへの移行に際して、（資産）配備の再構築をすることが一般的にベストである理由である。耐障害性自体は、そしてそれを実現するための基本的な仕組みは変化する。直接の「載せ替える」移行は障害対策の役に立ちそうもなく、また、プラットフォームやサービスの特定の機能を活かした改善の可能性を取り入れられるものでもない。

プラットフォームが持つ事業継続／災害復旧の機能の把握に注力することである。クラウドへの展開を意思決定した場合は、第三者ツールによる機能強化を行う前に、クラウドに含まれる事業継続／災害復旧の機能の最大限の活用を図るべきである。

事業継続／災害復旧（機能）はその全ての論理的構成要素に対応するものでなければならない。

- **メタストラクチャ：**クラウドの構成設定はソフトウェアにより管理されるため、リストア可能なフォーマットによりバックアップを取っておくべきである。このことはどこでも可能という訳ではなく、SaaS で可能なことは極めて稀であるが、**Software-Defined Infrastructure** を用いる IaaS プラットフォームの多くでは、それを実装するツール（第三者製のものを含む）がある。

- **Software-Defined Infrastructure** では、クラウド上の配備の全要素またはその一部を構成設定するためのインフラストラクチャのテンプレートを作成することが可能である。テンプレートは次に、クラウドプラットフォームの本来の構成の中に反映されるか、構成設定の統合管理をする API コールに転換される。この作成作業は IAM やログ記録の様な管理策を含むべきであり、単にアーキテクチャやネットワーク設計やサービスの構成設定だけであってはならない。

- **インフラストラクチャ：**前述した様に、どんなクラウド事業者も、従来型のデータセンタで同じコストで実現するものと比較して、高い可用性をサポートする機能を提供する。しかしそれは自組織のシステムのアーキテクチャをその機能に合わせる調整をして初めて利用可能になる。アーキテクチャの調整あるいは再設計を行うことなしにアプリケーションをクラウドへ「載せ替える」だけでは、通常、可用性はそれほど高くならない。

  この機能のコストモデルに留意し理解すること。とりわけ、クラウド事業者の地理的所在地や地域を跨る実装の場合には、コストは高くつく可能性がある。資産やデータの一部、例えばサーバを配備して起動するためのカスタムマシンイメージは、クラウドの所在地や地域を跨って機能するよう変換しなければならない。こういった資産は計画に組み入れなければならない。

- **インフォストラクチャ：**所在地をまたがったデータの同期化は、一般に管理が相当困難な課題の一つである。（実際のストレージコストの管理は容易だが。）その原因は、データセットのサイズによる（インフラストラクチャの構成設定に比べて）ことと、所在地やサービスをまたがってデータの同期を維持することにある。データの同期は一般に単一のストレージシステムや所在地であっても困難ではあるが。

- **アプリストラクチャ：**アプリストラクチャは上記のすべてを包含する。更にまた、コードやメッセージキューなどのアプリケーション資産をも含む。クラウド利用者がクラウドアプリケーションを構築する際、IaaS あるいは PaaS の上に構築することが一般的であり、そのため耐障害性や障害からの復旧はこれらのレイヤに必然的に依拠している。しかしアプリストラクチャはアプリケーションに関わるあらゆるものを全て包摂している。

  PaaS における制約およびロックインについて理解し、PaaS の構成要素の停止に備えること。PaaS のサービスは、アプリケーションに手作業で実装していた機能の一式、認証システムからメッセージキューや通知まで全てを備えている。今日ではアプリケーションは複数のクラウド事業者からさえこの種のサービスを組み入れることも珍しくなく、その結果たいへん込み入ったモヤモヤ状態を生み出す。

  利用しているクラウド事業者と、そのクラウドの構成要素やサービスの可用性について議論することは意味がある。例えば、利用しているインフラストラクチャ事業者のデータベースサービスは、その事業者の仮想マシンホスティングと同等の性能や可用性を提供しないかもしれない。

  リアルタイムのスイッチングができない場合、サービス停止に際しては問題が起きないように停止する様、アプリケーション設計を行うこと。これをサポートする多くの自動化技術がある。例えば仮に、キューサービスが落ちるとすると、それはフロントエンドを停止するトリガーを発し、メッセージが失われないようにする、といった具合に。

  サービス停止（を受け容れること）は常に選択肢としてある。完全な可用性は必ずしも必要ではないが、停止に備えて計画する場合には、緊急停止通知のページングと応急対応を受けて、問題を回避しつつ停止することを最低ラインとすべきである。これは DNS リダイレクションを利用した静的スタンバイを適用することで可能かもしれない。

  「カオスエンジニアリング」は、耐障害性を有するクラウド展開を構築するのにしばしば活用される。クラウドの全てが API ベースなので、カオスエンジニアリングは、クラウドの一部を選択的に機能不全にするツールを用いて、事業継続性を連続してテストする。（訳注：「カオス工学」については、マイクロソフトのブログがわかりやすい説明を提供している。）

  カオスエンジニアリングは、試験環境だけでなく本番環境でもしばしば行われ、エンジニアに対して、目にしていることだけが起こりうるすべてと考えるのでなく、障害に備えるようにさせる。機能停止に対処するシステム設計を行うことにより、個々の構成要素の故障についてより上手く対応できる。

6.1.2.2 クラウド事業者の停止に伴う事業継続

クラウド事業者の（サービスの）すべてが、あるいは少なくともそのインフラストラクチャの主たる部分（特定の地域）が停止することは、いつでも起こり得る。クラウド事業者の持つ能力を活用することの当然の帰結としてロックインが起こるので、クラウド事業者のサービス停止に備えた計画作りは困難である。当該クラウド事業

者の別のサービスに移行することができる場合もあるが、他のケースにおいては、（サービス）内部の移行は選択肢にならない。さもないとロックインに完全に陥るかもしれない。

クラウド事業者の過去の実績や、その内在する可用性提供能力次第では、サービス停止のリスクを受容するというのが適切な選択肢である場合も多い。

サービス停止（を受け容れること）はもう一つの選択肢かもしれないが、それは目標復旧時間（RTO）（がどの程度か）次第である。しかしながら、ある種の静的スタンバイは DNS リダイレクションによって実施可能の場合がある。衝撃抑制型停止（Graceful failure）には、API を提供している場合は、API コールに故障対応も含めるべきである。

予備のクラウド事業者やサービスを選ぶに際しては、そのサービスが同じ（メインの）事業者と同じ場所にあったり、その事業者に依存しているかもしれないので、慎重を期すこと。バックアップストレージの事業者が偶然にも（プライマリの事業者と）同一のインフラストラクチャ事業者の上にある場合、そのバックアップストレージの事業者を利用するのは何ら良いことではない。

クラウド事業者間でデータを移行することは容易ではないが、プラットフォーム同士の間で互換性がないかもしれない、メタストラクチャやセキュリティコントロールやロギングなどの移行に比べれば、容易かもしれない。

SaaS は通常、クラウド事業者に全面的に依存することから、クラウド事業者のサービス停止に関して最大の懸念点になるだろう。定期的にデータを取り出してアーカイブすることが、サービス停止を受容する以外では唯一の事業継続の手立てかも知れない。データを取り出して別のクラウドサービス、特に IaaS や PaaS にアーカイブする方が、ローカルのオンプレミスのストレージに移すよりはましだと言える。ここでも、クラウド事業者の個々の実績を織り込んだ、リスクベースのアプローチを採るべきである。

データを自身の手元に保持している場合も、データ移転できることを確認済みの代替のアプリケーションを持っておくべきである。データが利用できないなら、有効な復旧戦略はないに等しい。

一にテスト、二にテスト、三にもテストである。テストは一般に、従来型のデータセンタの場合よりも容易であるだろう。なぜならば、物理的資源による束縛を受けず、また使った資産のテスト期間中の使用料を払うだけですむためである。

6.1.2.3 プライベートクラウドとクラウド事業者における事業継続

事業継続は完全にクラウド事業者の肩にかかっており、事業継続／災害復旧は物理的設備に至るまでのすべてが対象となる。仮にクラウドが停止した場合はすべてが失われることになるため、RTO（目標復旧時間）および RPO（目標復旧地点）は極めて重要なものとなる。

他者にサービスを提供している場合、事業継続計画の立案に際しては、データの保存場所を含め、契約上の要件に留意すること。例えば、異なる司法管轄下にある遠隔の地域にフェイルオーバーすることは、契約や地元の法律に違反することになるかもしれない。

6.2 推奨事項

- 管理用ダッシュボード（メタストラクチャ）のセキュリティ

- API ゲートウェイと Web コンソールには強力な境界セキュリティを必ず設置すること。
- 強力な認証と MFA（多要素認証）を適用すること。
- 特権アカウント保持者やルートアカウントのための認証情報を厳密に管理すること。またそれらへのアクセスに関して二段階承認を検討すること。
  - 利用しているクラウド事業者に複数のアカウントを設定することは、アカウントの精度を上げることや（IaaS や PaaS の場合）不測事態の影響範囲を限定するのに役立つであろう。
- ルート／特権アカウント保持者の認証情報（で管理する）の代わりに、特権管理者と日替わり管理者のアカウントの分離を実施すること。
- メタストラクチャへのアクセスに対しては、最小特権アカウントを一貫して適用すること。
  - このことが、利用しているクラウド事業者における開発アカウントと試験アカウントを分離するべきである理由である。
- 可能な限り MFA（多要素認証）の利用を義務付けること。

- 事業継続
  - 障害に備えた設計をすること。
  - すべてに対してリスクベースのアプローチを採ること。最悪の事態を想定することは、最悪の事態に際してそれを乗り越えられるとか、完全な可用性を維持しなければならないということを意味する訳ではない。
  - 利用するクラウド事業者の可能な範疇で高い可用性に向け設計すること。IaaS や PaaS の場合は、従来型のインフラストラクチャで同様のことを行うよりも容易であり、費用対効果が高い場合が多い。
    - クラウド事業者が提供する機能を活用すること。
    - クラウド事業者の実績、機能、限界について把握すること。
    - 複数所在地の利用は常に検討対象とすべきであるが、可用性の要件次第でコストが変動することに留意すること。
      - また、イメージや資産の ID といったものを、異なる所在地においても必ず機能する様に変換するようにすること。
    - メタストラクチャに対する事業継続は資産に対するそれと同様に重要である。
  - クラウド事業者のサービス停止に際して、衝撃抑制型停止（graceful failure）ができるように準備すること。
    - このことには、他のクラウド事業者あるいは利用中のクラウド事業者の他のリージョンとの間で、相互運用や移植を行うことの計画も含まれる。
  - 極めて高い可用性を必要とするアプリケーションに対しては、クラウド事業者をまたがる事業継続を試みる前に、まず所在場所をまたがる事業継続から始めること。
  - クラウド事業者は、プライベートクラウドを含め、最高レベルの可用性を提供するとともに、クラウド利用者／エンドユーザが、自身の側の可用性を管理するための仕組みを提供しなければならない。

DOMAIN 7

インフラストラクチャ・セキュリティ

7.0　はじめに

インフラストラクチャ・セキュリティは、クラウドを安全に運用するための基礎となる。「インフラストラクチャ」とは、コンピュータとネットワークの結合体で、その上にあらゆるものを構築する。本ガイダンス向けの記述として、コンピュートとネットワークのセキュリティから始め、つぎにワークロードやハイブリッドクラウドも包含する。ストレージセキュリティもまたインフラにとって核ではあるが、それは「ドメイン 11：データセキュリティと暗号化」の中で詳しくカバーする。本ドメインはまた、プライベートクラウドコンピューティングの基本事項も含む。本ドメインは、既存の標準やガイダンスにてすでに十分にカバーされている、従来型のデータセンタセキュリティの全ての項目を含むわけではない。

インフラストラクチャ・セキュリティは、セキュリティの一番下のレイヤをカバーするもので、物理的な施設から、インフラストラクチャの構成要素をクラウド利用者が設定し実装することにまで及ぶ。インフラストラクチャの構成要素は最も基礎的なもので、クラウドのその他の要素の全てがそこから構築される。それにはコンピュート（ワークロード）、ネットワーキング、ストレージのセキュリティを含む。

CSA ガイダンスの趣旨に沿って、インフラセキュリティのクラウド特有の側面に焦点を当てる。データセンタセキュリティに関する知識体系や業界標準は、すでに信じられないくらい堅牢なものがあり、クラウドサービス事業者とプライベートクラウドの設置者は参照すべきである。本ガイダンスは、これら広範囲に入手可能な文献のさらに上に位置すると理解されたい。特に本ドメインは 2 つの側面を議論する：下位レイヤのインフラに関するクラウドにおける考慮事項と、仮想ネットワークとワークロードのセキュリティである。

7.1　概要

クラウドコンピューティングには、インフラストラクチャの 2 つのマクロな層がある。

- クラウドを構築するときに一括してプールされる基本的なリソース。このリソースは、クラウドのリソースプールを構築するのに使われる、基本の物理的あるいは論理的なコンピュート（プロセッサ、メモリなど）、ネットワーク、ストレージである。ここには、例えば、ネットワークリソースプールを作るのに使われるネットワーク用ハードウェアとソフトウェアのセキュリティが含まれる。
- クラウド利用者によって管理される仮想的な／抽象化されたインフラストラクチャ。このインフラストラクチャは、リソースプールから使用される、コンピュート、ネットワーク、ストレージのための資産である。例えば、仮想ネットワークのセキュリティは、クラウド利用者によって定義され管理される。

本ドメインの情報とアドバイスは、主に 2 番目のマクロな層、つまりクラウド利用者によって管理されるインフラ

のセキュリティに焦点を当てる。クラウド事業者やプライベートクラウドの管理者にとってより基礎的なインフラストラクチャのセキュリティは、データセンタに関する既存のセキュリティ標準との整合が十分できている。

7.2　クラウドのネットワーク仮想化

すべてのクラウドは、物理ネットワークを抽象化し、ネットワークのリソースプールを作成するために何らかの仮想的なネットワーキングを利用する。一般的にクラウド利用者は、このプールから望ましいネットワーキングリソースをプロビジョニングし、続いてそれを使用される仮想化技術の上限の範囲内で設定する。例えば、いくつかのクラウドプラットフォームは、特定のサブネットの中での IP アドレスの割り当てだけをサポートする。一方他のプラットフォームはクラウド利用者に、完全なクラス B の仮想ネットワークをプロビジョニングし、サブネットアーキテクチャを完全に定義できるようにする機能を提供する。

クラウド事業者（プライベートクラウドを管理する場合を含む）にとって、そのクラウドを構成するネットワークを物理的に分割することは、運用上の理由からもセキュリティ上の理由からも重要である。最も一般的には、機能的あるいはトラフィックの重複がないようにするために別々のハードウェアに分離した、少なくとも 3 つの異なるネットワークで構成する。

- 仮想マシンとインターネットの間の通信のためのサービスネットワーク。このネットワークは、クラウド利用者のためのネットワークリソースプールを構築する。
- 仮想ストレージと仮想マシンとを接続するためのストレージネットワーク。
- 管理と API トラフィックのためのマネジメントネットワーク。

IaaS の下層にある一般的なネットワーク構成

このようなネットワーク構成は、プライベートクラウドのネットワークアーキテクチャを構築するための唯一の方法ではないが、共通的なベースラインである。特にプライベートクラウドの場合は、パブリッククラウド事業者ほどの大きな規模を扱わないが、それでもなお、パフォーマンスとセキュリティとのバランスをとる必要がある。

今日のクラウドコンピューティングでよく見られるネットワーク仮想化には、2 つの主要なカテゴリがある：

- **仮想 LAN（VLAN）：**VLAN は、ほとんどのネットワークハードウェアで実装される既存のネットワーク技術を利用する。VLAN は、クラウドコンピューティングを使わない場合でも、企業ネットワークで極めて一般的に使われる。VLAN は単一組織のネットワーク（企業内データセンター）において、異なるビジネスユニットや機能など（ゲスト用ネットワークなど）を分離するために使うように設計されている。VLAN はクラウド規模の仮想化あるいはセキュリティ向けに設計されていないし、それだけでネットワークを分離するための効果的なセキュリティコントロールになると考えるべきではない。VLAN はまた物理的なネットワーク分離を置き換えるものでは決してない。

- **Software Defined Networking (SDN)：**ネットワーキングハードウェアの上に形成される、より完全な抽象的化された層である。SDN はネットワークコントロールプレーンとデータプレーンとを切り離す（もっと詳しく知りたい方は Wikipedia の SDN principles のページを参照）。SDN は LAN の従来の限界を超えてネットワーキングを抽象化することができる。

  SDN には複数の実装があり、標準に基づくものや、独自の実装もある。実装によっては、SDN はより高い柔軟性と隔離とを提供できる。例えば、複数の分離された重複 IP アドレスは、同じ物理ネットワークの上に仮想ネットワークとして配置できる。適切に実装すれば、また標準的な VLAN とは違って、SDN は効果的なセキュリティ隔離の境界区分を提供する。SDN はまた一般的に、ソフトウェア定義による任意の IP 範囲を提供し、クラウド利用者は既存のネットワークをクラウドに上手に拡張することができる。もしクラウド利用者が 10.0.0.0/16 の CIDR（Classless Inter-Domain Routing）ブロックを必要とするならば、下にあるネットワークアドレス体系が何であれ SDN は提供できる。SDN は通常、複数のクラウド利用者が同じ内部ネットワーク IP アドレスブロックを使うことさえサポートできる。

  表面的に SDN は、クラウド利用者にとって通常のネットワークのように見えるかもしれないが、もっと完全な抽象化によって、水面下では非常に様々な機能を発揮する。SDN を構成する技術と管理は、クラウド利用者がアクセスするものでないように見えるが、実のところもう少し複雑である。例えば SDN は、パケットのカプセル化を使って、仮想マシンと他の「標準的な」資産が、それらの下にあるネットワークスタックにいかなる変更も行わなくてよいようにするかもしれない。仮想化スタックは、仮想ネットワークインタフェースに接続した標準的な OS からパケットを受け取ると、パケットをカプセル化してそれらを実際のネットワークに流す。仮想マシンは、ハイパーバイザが提供する、互換性のある仮想ネットワークインタフェース以外に SDN のことを知る必要がない。

7.3 クラウドネットワーキングでセキュリティがどのように変わるか

ベースとなる物理ネットワークを直接的に管理できないことは、クラウド利用者にとってもクラウド事業者にとっても、一般的なネットワークの利用形態に変化をもたらす。もっとも一般的に使われるネットワークセキュリティのパターンは、物理的な通信経路の制御と、セキュリティアプライアンスの設置に依っている。このネットワークセキュリティは、仮想レベルでのみ運用するクラウド利用者にとっては、適用できない。

従来型のネットワーク侵入検知システムは、ホスト間の通信がミラーされ、仮想あるいは物理的な侵入検知システムによってその通信が検査されるものだが、クラウド環境ではサポートされないだろう。従って、クラウド利用者のセキュリティツールは、インライン型の仮想アプライアンス、あるいはインスタンスにインストールされるソフトウェアエージェントに依存しなければならない。このことは渋滞箇所を作るか、プロセッサの負荷を増やすかのいずれかにつながり、そのため実装の前に本当に必要な監視レベルを確認しなければならない。いくつかのクラウド事業者は、何らかのレベルのビルトイン型のネットワーク監視機能を提供するかもしれない（プライベートクラウドプラットフォームの場合にはもっと多くの選択肢がある）が、それは通常、物理ネットワークをスニファで見るのと同じ程度のものではない。

7.3.1 仮想アプライアンスの課題

物理アプライアンスは（クラウド事業者を除いて）設置することができないため、もしどうしても必要な場合には、仮想アプライアンスによって置き換える必要があるが、その場合はクラウドのネットワークが必要なルーティングをサポートしていなければならない。このことはネットワーク監視のために仮想アプライアンスを設置するときにも同じ問題をもたらす。

- 仮想アプライアンスはボトルネックになる。なぜなら、フェイルオープン（訳注：機械が故障したときには何もせずに通信を通すこと）ができず、全てのトラフィックを遮断しなければならないため。
- 仮想アプライアンスは、ネットワーク性能要件を満たすために、膨大なリソースを必要とし、コストを増加させるかもしれない。
- 仮想アプライアンスが使われるとき、守るべきリソースの拡張性に対応できるようにオートスケールをサポートすべきである。製品によるが、もしベンダがオートスケールに適合する拡張性のあるライセンス形態をサポートしないならば、オートスケールは問題を起こすかもしれない。
- 仮想アプライアンスはまた、クラウドでの運用に対応するとともに、異なる所在地やアベイラビリティゾーンの間でインスタンスを動かすことに対応するべきである。クラウドネットワークの変化の速さは物理ネットワークのそれよりも早く、ツールはこの重要な相異に対応できるように設計されなければならない。
- クラウドアプリケーションのコンポーネントは、耐障害性を向上するためにより分散配置される傾向にあり、さらにオートスケーリングのために仮想サーバはより短命でより頻繁に生成されるようになるかもしれない。このことは、セキュリティポリシーの設計に変化をもたらす。
    - この傾向は、セキュリティツールが（例えば、1 時間以内の寿命をもつサーバなど）対応しなければならない変化の頻度を非常に高める。
    - IP アドレスは従来型のネットワークの場合よりも格段に速く変化し、セキュリティツールはそれに対応しなければならない。理想的にはセキュリティツールは、ネットワーク上の資産を IP アドレスやネットワーク名ではなく、ユニークな ID によって識別すべきである。
    - 資産が静的な IP アドレスを保持する可能性は低い。異なる資産が短い期間に同じ IP アドレスを共有するかもしれない。アラートやインシデントレスポンスのライフサイクルは、そのような動的な環境の中でもアラートが確実に機能するように修正が必要かもしれない。一つのアプリケーション層の中の資産は、多くの場合、耐障害性のために複数のサブネットに位置し、IP アドレスベースのセキュリティポリシーをさらに複雑にするだろう。オートスケーリングのために、資産はまた短命で、数時間さらには数分のみ存在するかもしれない。利点としては、クラウドアーキテクチャはサーバ当たりのサービスの数が少なくなる方向に向かうので、ファイアウォールのルールを制限的に設定することを容易にする。一つの仮想マシン上に多くのサービスを動かす（ハードウェアの設備投資を最大化しなければならない物理サーバ上の場合のように）のではなく、一つの仮想マシンでより小さないくつかのサービスを稼動させたり、たった一つのサービスを動かしたりすることが一般的になる。

7.3.2　SDN のセキュリティ上の利点

良い点として、SDN は新しいタイプのセキュリティコントロールを可能にし、多くの場合、ネットワークセキュリティにとって総体としてプラスになる。

- 隔離がより簡単になる。物理的なハードウェアの制約なく、必要な数の隔離されたネットワークを構築することができるようになる。例えば、もし同じ CIDR アドレスブロックをもつ複数のネットワークを稼動させる場合には、アドレスの衝突のために、直接通信することが論理的にできない。SDN は、様々なセキュリティに対する条件を持ったアプリケーションとサービスを分離するための、優れた方法である。この微細分離機能(microsegregation)は、以下で詳細に述べる。
- SDN のファイアウォール（例えばセキュリティグループ）は、物理トポロジにもとづく制限がないため、ハードウェアベースのファイアウォールよりも柔軟な基準にもとづいて資産に適用できる。（これはソフトウェアファイアウォールの多くのタイプに当てはまるが、ハードウェアファイアウォールでは不可能）。SDN のファイア

ウォールは基本的に、入方向と出方向のルールを定義するポリシーの集合であり、ネットワーク所在場所によらず（特定の仮想ネットワークの中で）、一つの資産あるいは資産の集合に適用できる。例えば、特定のタグを持つ資産のすべてに適用するというファイアウォールルールの組みを作ることができる。これは検討することがいささか難しいことに注意が必要である。なぜなら、プラットフォームが違えば用語体系も違うので、この種の能力をサポートする機能も違ってくるためである。そのため概念レベルに留める積りである。

- クラウドプラットフォームの統合管理層と SDN の組合せは、従来型のハードウェアやホストベースの方法を使った管理よりも、非常に動的で細部にわたる組合せとポリシーを、より少ない管理負荷で実現できる。たとえば、もしオートスケールグループに属する仮想マシンが自動的に複数のサブネットに配備され、それらの間で負荷分散される場合には、IP アドレスやサブネットに関わらず、これらのインスタンスに適用するファイアウォールのルールセットを作成できる。これは、クラウドのセキュアなネットワークの重要な機能であり、従来型のコンピューティングとは全く異なる方法でアーキテクチャが使われている。
- デフォルトで禁止の設定をすることは多くの場合、出発点であり、そこから接続先を開けていくことになるが、ほとんどの物理ネットワークの場合はこの逆である。
    - SDN は、ネットワークアプライアンスの管理性を向上させて精度を高めたホスト型ファイアウォールと考えられる。ホスト型ファイアウォールには 2 つの問題がある：伸縮への対応が難しいことと、もしホストしているシステムが侵害されれば変更や停止が容易に行われること。一方、全ての内部トラフィックをネットワークファイアウォールに通すことは、たとえサブネット同士の間であっても、コスト的に難しい。セキュリティグループなどのソフトウェアファイアウォールは、システムの外側で管理され、追加的なハードウェアのコストや複雑なプロビジョニングを必要とせずに、それぞれのシステムに適用できる。従って、同じ仮想サブネットの上で仮想マシンを一つずつ隔離するようなことは無意味である。
    - 上記でも少し触れたが、ファイアウォールルールはタグなどの他の基準に基づいたものにできる。それは可能ではあるが、実際の能力はプラットフォームに依存することに注意が必要である。なぜならば、クラウドネットワークが SDN ベースというだけでは、実際にセキュリティの利点をもたらすことにはならないからである。
    - 単にスニフィングを排除するだけでなく、例えば ARP スプーフィングや他の低レベルの攻撃などの多くのネットワーク攻撃は、（プラットフォームによるが）デフォルトで排除される。これは SDN の本来の性質と、ソフトウェアベースのルールや、流れているパケットに対する分析を適用することによってである。
    - カプセル化することでパケットを暗号化することができる。
    - セキュリティグループと同じように、他のルーティングやネットワークの設計もダイナミックに実施でき、クラウドの統合管理層につなぐことができる。例えば、仮想ネットワークをブリッジすることや、内部の PaaS サービスと接続するなどが可能である。
    - 追加のセキュリティ機能を、ネイティブに追加することも可能である。

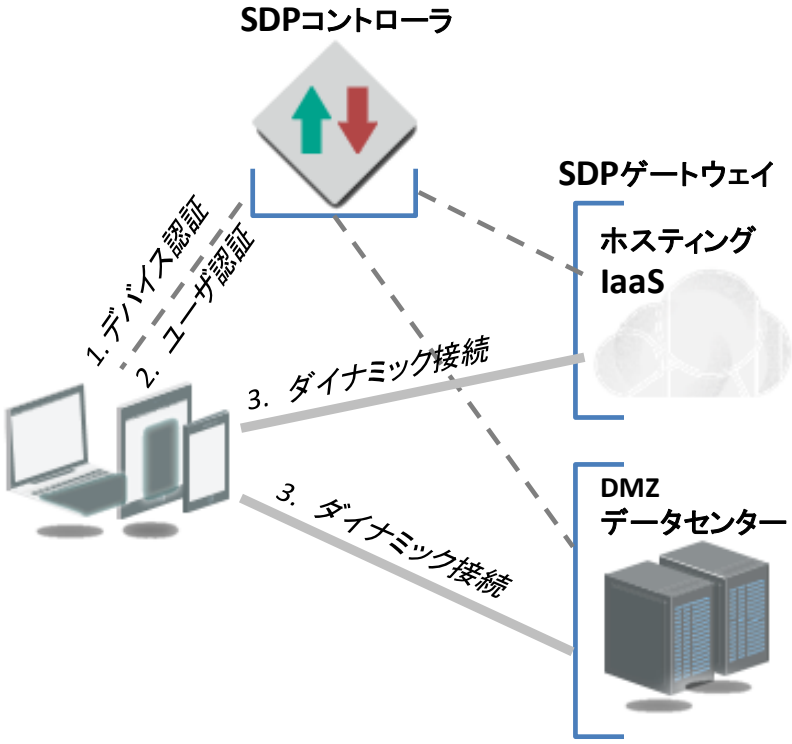
7.3.3　マイクロセグメンテーション（微細分割機能）と SDP（Software Defined Perimeter）

マイクロセグメンテーション（**ハイパー分割**と表現されることもある）は、仮想ネットワークのトポロジを活用して、ネットワークをより数多く、より小さく、より分割することができるようになる。これは過去にはそのようなモデルを不可能にしてきたハードウェアコストをかけることなく実現できる。全体のネットワークは従来のアドレス設定問題にほとんど影響されることなくソフトウェアで定義されるため、マイクロセグメンテーションというソフトウェアで定義される環境を、数多く稼動させることが極めて容易にできる。

このような機能を活かしている一般的で実践的な例は、自身の仮想ネットワーク上ですべてではないにせよほとんどのアプリケーションを稼動させ、必要な時だけそれらのネットワークをつなぐことである。これは、もし攻撃者がある一つのシステムを攻略しても、その影響する範囲を劇的に小さくする。攻撃者はその（侵略した）足場を活用してデータセンタ全体に出ていくことができない。

クラウドのマイクロセグメンテーションはソフトウェア設定にもとづくため資本支出は増えないけれども、複数の重複するネットワークと接続性を管理するための運用面のコストを増やす可能性がある。

CSA の Software Defined Perimeter（SDP）ワーキンググループは、デバイスとユーザの認証を結合し、リソースへのネットワークアクセスを動的にプロビジョンし、セキュリティを強化するという、モデルと仕様を開発した。SDP は 3 つのコンポーネントから成る：[4]



SDP通信ダイヤグラム

- 接続対象の資産（例えばラップトップ）上の SDP クライアント
- SDP クライアントを認証および認可し、SDP ゲートウェイへの接続を設定する SDP コントローラ
- SDP クライアントのネットワークトラフィックの到達先であり、SDP コントローラとの通信に関するポリシーを適用する SDP ゲートウェイ。

このことによって、ネットワークセキュリティは、単なる IP パケットを超えて幅広い基準に基づいて設定できる。特に SDN と組み合わせることで、SDP は、変化し続けるネットワークトポロジに対してより多くの柔軟性とセキュリティを提供することができる。

訳注4　図のタイトルは原文では”Common networks underlyng IaaS.”となっているが、前の図と同じであり、誤りと考えられるので、正しいと推測されるタイトルに変更した。

SDP に関するさらなる情報は、以下の CSA のサイトで入手できる。
https://cloudsecurityalliance.org/group/software-defined-perimeter/#_overview

7.3.4　クラウド事業者とプライベートクラウドのためのその他の留意事項

クラウド事業者は、プラットフォーム構築の基礎となる物理的／従来型ネットワークの核となるセキュリティを維持しなければならない。ルートネットワークのセキュリティ事故は、すべてのクラウド利用者のセキュリティを脅かすことになるだろう。物理ネットワークのセキュリティは、自由自在な通信やマルチテナントの環境に対して維持されなければならない。有害なものが混在すると想定しなければならないためである。

マルチテナント環境においては、分離と隔離を維持することは、絶対的に重要である。そのため、SDN のセキュリティコントロールを適切に実施し、設定し、維持するための負荷がかかるだろう。SDN はいったん立ち上げて走らせれば必要な隔離を提供することができる一方で、敵意のあるテナントの可能性に対応するために、すべてが適切にセットアップされていることを入念に確認することが重要である。クラウド利用者は必ずしも敵意があると言っているのではなく、ネットワーク上の何かがいつかの時点で侵害され、更なる攻撃のために使われることを想定しておくことが安全である。

クラウド事業者はまた、クラウド利用者が自身のネットワークセキュリティを適切に設定し管理することができるよう、クラウド利用者に対してセキュリティコントロールを開示しなければならない。

最後に、クラウド事業者は、環境を防御するための境界セキュリティを実装する責任をもつ。ただしそれはクラウド利用者のワークロードへの影響を最小に抑えなければならない。たとえば DDoS 対策とベースライン IPS によって、敵意のあるトラフィックがクラウド利用者に影響する前にフィルタで除去することである。他の留意事項は、仮想インスタンスがリリースされハイパーバイザに戻される時に機密の可能性のある情報を確実に取り除くことと、それによって、ハードディスク空間がプロビジョンされるときに他のクラウド利用者によってその情報が決して読まれないようにすることである。

7.3.5　ハイブリッドクラウドにおける留意事項

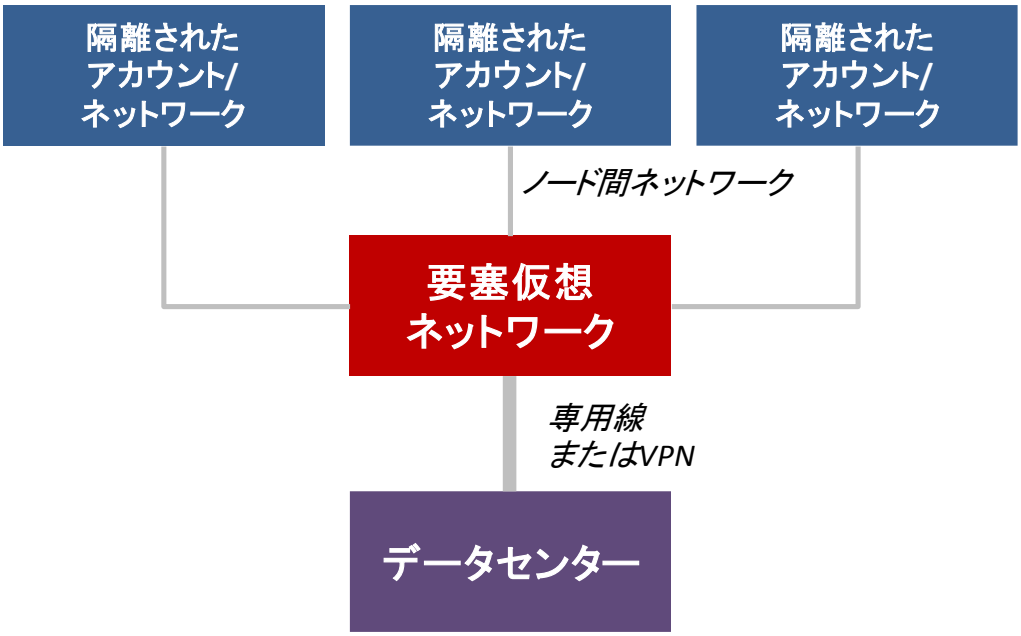
ドメイン 1 で述べたように、ハイブリッドクラウドは、企業のプライベートクラウドあるいはデータセンタと、パブリッククラウド事業者を接続する。典型的には、専用 WAN 回線あるいは VPN のいずれかを使う。理想的にはハイブリッドクラウドは、自由なアドレス設定をサポートして、クラウド利用者のネットワークをシームレスに拡張できるようにするのがよい。もしクラウドがクラウド利用者のオンプレミス資産と同じネットワークアドレス空間を使うとすれば、それは実際問題として使えない。

ハイブリッドクラウド間接続は、プライベートネットワークが同じレベルのセキュリティでない場合には、クラウドのネットワークのセキュリティを低下させるかもしれない。もし社内データセンタのネットワークがフラットで、従業員用システムとの分離が最低レベルの場合は、誰かが従業員のラップトップに侵入し、そこからハイブリッドクラウド間接続を通じてクラウドの設備全体をスキャンすることができる。ハイブリッドクラウド間接続は、両方のネットワークのセキュリティを同レベルにするような結果をもたらすべきではない。2 つのネットワークの間の分離を、ルーティング、アクセスコントロール、更にはファイアウォールその他のネットワークセキュリティツールの追加によって、実行するべきである。

管理とセキュリティのために、一般的には、ハイブリッドクラウド間接続を最小化することが望ましい。複数の個別のネットワークを接続することは複雑である。それらネットワークの一方がソフトウェア定義であり、もう一方にハードウェアによる制限がある場合には特にそうである。ハイブリッドクラウド間接続は多くの場合依然として必要であるが、それらが必要であると決めつけてはならない。それらはルーティングの複雑さを増し、複数のクラウドネットワークを重複した IP アドレス空間で走らせることを制限し、セキュリティコントロールを協調させる必要のために両方の側でのセキュリティを複雑にする。

ハイブリッドクラウド間接続向けの新しいアーキテクチャのひとつは、「要塞」あるいは「乗り継ぎ」（bastion）（訳注：「踏み台」とも言われる）仮想ネットワークである。

- このシナリオでは、単一のハイブリッドクラウド間接続を使って、複数の異なるクラウドネットワークをデータセンタへと接続することができる。クラウド利用者は、ハイブリッド接続のための専用仮想ネットワークを構築し、そのつぎに専用の要塞ネットワークを通じて他のネットワーク間を接続する。
- 第 2 レベルのネットワークは、要塞ネットワークを通じてデータセンタに接続するが、それらは互いに接続されていないために、互いに通信することができず結果的に分離される。さらに様々なセキュリティツール、ファイアウォールのルールセット、アクセスコントロールリストを要塞ネットワークに配備し、その上でハイブリッド接続に流入し流出するトラフィックを防御することができる。



「要塞」または「踏み台」ネットワーク。より柔軟なハイブリッドクラウドアーキテクチャ向け

7.4　クラウドにおけるコンピュートとワークロードのセキュリティ

ワークロードとは処理の一単位であり、仮想マシン、コンテナ、その他の抽象化したものの上に存在する。ワークロードは常に、プロセッサのどこかで稼動し、メモリを消費する。ワークロードは非常に広範囲な処理タスクから成り、標準的な OS 上で仮想マシンの中で稼動する従来型のアプリケーションから、GPU ベースあるいは FPGA ベースに特殊化されたタスクまでを含む。これらのタスクのほとんどすべては、クラウドコンピューティング上で何らかの形でサポートされる。

すべてのクラウドのワークロードはハードウェアスタック上で稼動することと、そのハードウェアの完全性を維持することはクラウド事業者にとって極めて重要であることを知っておくことが大事である。ハードウェアスタックが異なることによって、実行の隔離と信頼の連鎖（chain of trust）という諸機能が実現する。その内容としては、メインプロセッサ外で稼動するハードウェアベースの管理とモニタリングのプロセス、安全な実行環境、暗号化と鍵管理の分離などがある。これらの諸機能は広範囲に及ぶとともに変化が速いため、ここで規範的なガイダンスを提供することはできないが、一般的な意味で、これらの優れた機能をもつハードウェアを適切に選択し活用することによって、セキュリティに非常に大きな利点をもたらす可能性がある。

コンピュートの抽象化には複数のタイプがあり、それぞれ分離と隔離の程度が異なる。

- **仮想マシン：**仮想マシンはもっとも良く知られたコンピュートの抽象化方式であり、すべての IaaS 事業者が提供している。それらはベースイメージから作成される（あるいは複製される）ため、クラウドコンピューティングでは通常インスタンスと呼ばれる。仮想マシンマネージャ(VMM)（ハイパーバイザ）は、下にあるハードウェアから OS を抽象化する。最近のハイパーバイザは、今や標準的なサーバ（とワークステーション）では一般的となった、下層のハードウェアの機能と連携することで、高性能なオペレーションをサポートしつつ、隔離を強化することができる。

  仮想マシンは潜在的にある種のメモリ攻撃に対して無防備であるが、隔離を強化するために絶え間なく進むハードウェアとソフトウェアの強化の結果、こういった攻撃は次第に難しくなっている。最新のハイパーバイザ上に仮想マシンを形成することは一般的に効果的なセキュリティコントロールであり、仮想マシンのハードウェアベースの隔離の進化と、セキュアな実行環境の進化によって、このような能力の改善は続いている。

- **コンテナ：**コンテナは（現在では）OS のリソースを共有し活用する、OS の中で稼動するコード実行環境である。仮想マシンは OS を完全に抽象化したものである一方、コンテナは分離されたプロセスを稼動させるためのコンパクトな区画でありながら、ベースとなる OS のカーネルと他の機能を依然として利用する。複数のコンテナは、同じ仮想マシン上で稼動することができ、あるいは仮想マシンを全く利用せずにハードウェア上で直接稼動するよう実装できる。コンテナは制限された環境の中でのコード実行をサポートし、コンテナの設定で定義されたプロセスと機能のみにアクセスする。これによりコンテナを信じられないほど早く起動することができる。なぜならコンテナは OS の起動も、多くの（時には全く）新しいサービスの起動も必要がないためである。コンテナはホスト OS で既に実行中のサービスにアクセスする必要があるのみであり、そのためミリ秒単位で起動することができるものもある。

  コンテナは比較的新しく、隔離の機能はまちまちで、プラットフォームに大きく依存する。コンテナはまた、さまざまな管理システム、下層にある OS、コンテナの技術とともに、急速に進化している。コンテナについてはドメイン 8 でより詳しく説明する。

- **プラットフォームベースのワークロード：**これはより複雑なカテゴリであり、仮想マシンでもコンテナでもない共有プラットフォーム上で稼動するワークロードをカバーする。それは例えば共有データベースプラットフォーム上で稼動するロジック／プロシージャである。マルチテナントデータベースの中で稼動するストアドプロシージャ、あるいは機械学習の PaaS 上で稼動する機械学習ジョブを想像されたい。プラットフォームプロバイダが特定のセキュリティオプションとコントロールを公開する可能性があるかもしれないが、隔離とセキュリティは完全にプラットフォームプロバイダの責任である。

- **サーバレスコンピューティング：**サーバレスは幅広いカテゴリであり、クラウド利用者が下層のハードウェアあるいは仮想マシンを何も管理せず、単に外部に提示される機能にアクセスするという状況を指す。例

えば、アプリケーションコードを直接実行するための、サーバレスプラットフォームがある。この仕組みでは、サーバレスプラットフォームは依然として、コンテナ、仮想マシン、特殊なハードウェアプラットフォームを利用する。セキュリティの観点からすると、サーバレスは単に、コンテナとプラットフォームベースのワークロードをカバーする組合せ用語であり、クラウド事業者は基本的なセキュリティ機能とコントロールを含むすべての下位の層を管理する。

7.4.1　クラウドはワークロードのセキュリティをどのように変えるか

すべてのプロセッサとメモリは、通常様々なテナントから寄せられる、複数のワークロードをほぼ常時稼動させると考えられる。複数のテナントが同じ物理的なコンピューティングノードを共有する可能性があるが、ハードウェアスタックを分けることで分離を幅広く実現する機能がある。ワークロードの隔離を維持する責務は、クラウド事業者が負うものであり、その最優先事項のひとつとすべきである。

いくつかの環境では、専有／プライベートなテナントが可能であるが、一般的には高いコストがかかる。このモデルでは、指定されたワークロードだけが指定された物理サーバ上で稼動する。クラウド利用者が汎用のリソースプールからハードウェアを占有することは、内部リソースの利用効率が下がるために、パブリッククラウドではコストが増加する。プライベートクラウドでも同様である。

クラウド利用者は、クラウド利用モデルに関係なく、ワークロードが物理的にどこで稼動するかをコントロールすることはほとんどできない。ただしいくつかのプラットフォームは、可用性、コンプライアンス、他の要件をサポートするために、特定のハードウェアプールあるいは一般化した所在地名の指定をサポートしている。

7.4.2　変更無用(immutable)なワークロードはセキュリティに役立つ

オートスケーリングとコンテナはその性質上、イメージにもとづき動的に起動されたインスタンスを稼動させたときに、ベストに機能する。インスタンスは、不要になった時にはアプリケーションスタックを壊すことなくシャットダウンして容量を空けることができる。これはクラウドにおけるコンピュートの拡張性の中核機能である。そうすることで、稼動しているワークロードに対して、パッチを当てたりあるいは他の変更を加えたりはしないことになる。なぜならシャットダウンはイメージに変化を加えないから。その結果、新しいインスタンスは、稼動している何かに手動で何らかの変更を加えようとも、同期をとる対象外となる。このような仮想マシンを「変更無用」(immutable)と呼んでいる。

変更無用であるインスタンスを再設定あるいは変更するためには、下層のイメージを更新し、その後古いインスタンスをシャットダウンして同じ場所に新しいインスタンスを稼動させることで、新しいインスタンスへと入れ替える。

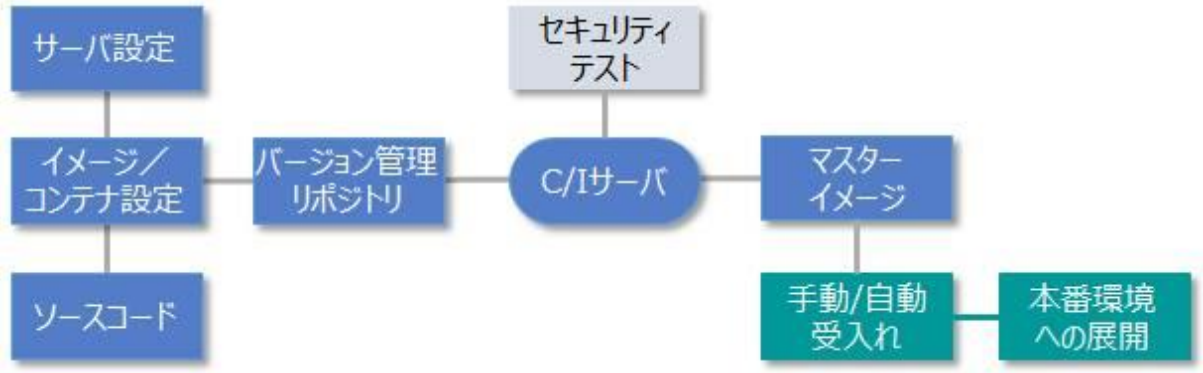
変更無用の属性には段階がある。純粋な定義は、新しいイメージで稼動しているインスタンスを完全に置き換えることである。しかしながら、いくつかの組織は、新しいイメージを OS 更新のためだけにプッシュし、他の配備技術を使って、稼動している仮想マシンにコードの更新をプッシュする。インスタンスが変更されるので技術的には完全に「変更無用」とは言えないが、このようなプッシュは現に自動化されて完全に実施されている。ローカルの変更を行うのに稼動しているシステム（インスタンス）に手動でログインするということは全く起きない。

変更無用のワークロードは、多大なセキュリティ上のメリットをもたらす。

- 稼動しているシステムにパッチを当てることや、依存性（訳注：パッチによりシステムに影響を与えること）やパッチプロセスの失敗を心配することなどは不要になる。稼動しているシステムを新しいマスターイメージに置き換えるだけである。
- 稼動しているワークロードにリモートからログインすることを禁止できるし、またそうすべきである（たとえログインがオプションであったとしても）。これはスタックをまたがって矛盾するような変更を防ぐための運用上の要件であり、また大きなセキュリティ上のメリットである。
- 更新版をロールアウトすることは非常に早くなる。なぜならアプリケーションは、個々のノードの操作で落とすように設計されなければならないためである（これはすべてのオートスケーリングにとって基本的であることを忘れてはならない）。稼動しているシステムにパッチをあてるという複雑さともろさに悩まされることは少なくなる。何かが故障したとしても、それをただ置き換えればよい。
- インスタンスは決して変化しないため、サービスの停止と、アプリケーション／プロセスのホワイトリスト化がさらに容易になる。
- イメージ生成の間にほとんどのセキュリティテストが行えるようになり、稼動しているワークロードに対する脆弱性診断の必要性を減らす。なぜならワークロードの振る舞いは生成時点で完全に把握されるはずであるからである。

変更無用には、追加の要件がいくつかある：

- 更新の配備をサポートするため、一貫性のあるイメージ生成プロセスと自動化が必要である。これらの新しいイメージは、パッチやマルウェアのシグネチャ更新に対応するために定期的に生成されなければならない。
- セキュリティテストは、イメージの生成と配備のプロセスの中に組み込まれなければならない。セキュリティテストにはソースコードテストを含み、もし仮想マシンあるいは標準的なコンテナを使うならば、脆弱性診断を含めること。
- イメージの設定には、イメージを配備しそれらを本番の仮想マシンに使う前に、ログインを無効化しサービスを制限する仕組みが必要である。
- いくつかのワークロードに対しては、トラブルシューティングのために、アプリケーションスタックの中で停止しているワークロードにログインできるようにするプロセスを必要とするかもしれない。これはグループからワークロードを引き出すことであるが、隔離下で稼動を続けられる必要がある。他の方法として（あるいは多くの場合望ましくは）、ログインする必要が決してないように、外部のコレクタに対して十分に詳細なログを送信すべきである。
- サービスカタログを管理するための複雑さが増すだろう。なぜならある 1 日のあいだに何十あるいは何百ものイメージを生成するかもしれないために。



変更無用な仮想マシンあるいはコンテナのイメージを生成するための、配備の流れ

7.4.3 標準的なワークロードセキュリティコントロールへのクラウドの影響

いくつかの標準的なワークロードのコントロールは、クラウドのワークロードの中では実行するべきものでない（たとえば、ある種のコンテナの中でアンチウイルスを稼動すること）。他のセキュリティコントロールは必ずしも必要ではなく、あるいはクラウドコンピューティングの中で効果を維持するために大幅に修正する必要がある。

- 非仮想マシンベースのワークロードに対してソフトウェアエージェントを稼動させることができないかもしれない。例えば、プロバイダ管理下の「サーバレス」コンテナの中でワークロードを稼動させることなど。
- 「古いタイプの」エージェントは、クラウドでは処理性能の低下がひどいかもしれない。少ないコンピューティングで済む軽量なエージェントは、より良いワークロードの配分と効率的なリソースの利用ができる。クラウドコンピューティング向けに設計されていないエージェントは、クラウドの配備設計を反映していない仮想のコンピュータを想定している場合がある。プロジェクトにかり出された開発者は、軽量で単一目的の仮想マシンの集合を走らせることを想定するかもしれない。このような環境に対応していないセキュリティエージェントは、負荷を著しく増加させ、より大きな仮想マシンのタイプを要求し、コストを増やすことになるだろう。
- クラウド環境で動作するエージェントはまた、動的なクラウドのワークロードとオートスケールのような配備パターンをサポートする必要がある。エージェントは、（エージェント側でも管理システム側でも）固定 IP アドレス体系に依存することはできない。クラウド上の資産のあるものは静的な IP アドレス上で稼動するかもしれないが、クラウドの場合、伸縮性のために、実行段階で IP アドレスを動的に割り当てることが一般的である。従って、エージェントは、管理／制御画面にアクセスし、そこからどの種のワークロードがどこで稼動しているかを知ることができる必要がある。
- エージェントの管理画面はまた、それ自身がオートスケーリングのスピードに対応し伸縮機能をサポートする必要がある（例えば、1 時間のあいだに複数のワークロードで同じアドレスが使われるなど、信じられないほど動的な IP アドレス割当に追随すること）。従来型のツールは通常、このレベルの速度向けに設計されておらず、ネットワークセキュリティやファイアウォールで見たのと同じ問題を引き起こす。
- エージェントは、通信／ネットワーキングによる攻撃対象面を増やすことや、攻撃対象面の増加につながる他の要件を増やすことをすべきではない。これは常にその通りである一方、エージェントがクラウドのセキュリティリスクになる可能性を高める理由がいくつかある：
    - 変更無用のシステムを稼動させることで能力は拡大しており、エージェントは、普通のソフトウェアのように、攻撃対象面を増やしている。特にエージェントが設定変更や署名を受け付ける場合、それが攻撃経路として使われうる。
    - クラウドではまた、物理サーバと比較して、仮想マシン（あるいはコンテナ）当たりのサービスの数は少なく、ネットワークポートの使用数も少ない傾向にある。エージェントによっては、ファイアウ

ォールポートの口を増やす要求を出すが、それはネットワークの攻撃対象面を増やすことになる。

    - これはエージェントが常に新しいセキュリティリスクを生み出すことを意味するのではなく、単にセキュリティリスクを多く引き受ける前にメリットとのバランスをとる必要があることを意味する。
- ファイルの完全性モニタリングは、稼動している変更無用なインスタンスに対する未承認の変更を検出するための効果的な手段となりうる。変更無用なワークロードはその堅牢化された性質のために、一般的にセキュリティツールの必要性は低い。それらは通常のサーバよりもきつく堅牢化され、稼動させるサービスの数は少ない場合が多い。ファイルの完全性モニタリングは、大変軽量であることが多く、変更されない性質上実質的に誤検出（false positive）がゼロであり、変更無用なワークロードのための良いセキュリティコントロールになりえる。
- 標準的なセキュリティコントロールを走らせている長期稼動中の仮想マシンは、ネットワークから隔離し、管理のやり方を変えるべきである。管理ツールをプライベートネットワークのサブネットで稼動する仮想マシンに接続することは難しい場合がある。管理ツールを同じサブネットで稼動させることは技術的には可能だが、それはコストを著しく増加させ、管理をより困難にする。
- 隔離して稼動するクラウドのワークロードは一般的に、抽象化の結果、物理インフラよりも障害耐性が弱い。そこに災害復旧の手当てをしておくことは、極めて重要である。

7.4.4　ワークロードのセキュリティモニタリングとロギングに起きる変化

セキュリティのロギング／モニタリングは、クラウドコンピューティングではより一層複雑である。

- ログの中の IP アドレスは必ずしも、特定のワークフローを反映しないだろう。なぜなら、複数の仮想マシンが一定期間同じ IP アドレスを共有するかもしれず、コンテナやサーバレスのようないくつかのワークロードは、認識可能な IP アドレスを全く持たないかもしれないからである。このため、ログの中身が実際に何を指しているかを確実に知るためには、ログの中の他のユニークな識別子を収集する必要がある。そのようなユニークな識別子は、短命なシステム（ワークロード）でのみ通用することになり、短い期間の間しか有効でない場合がある。
- クラウドでは変化が一層速いため、ログはオフロードで持つ必要があり、迅速にシステム外部に集積される必要がある。クラウドのコントローラが不必要なインスタンスをシャットダウンする前にログを集めなければ、オートスケールグループのログを失うことは容易に起きる。
    - ロギングのアーキテクチャは、クラウドのストレージとネットワーキングのコストに対応する必要がある。例えば、パブリッククラウドのインスタンスから全てのログをオンプレミスの SIEM (Security Information and Event Management)に送信することは、内部ストレージや外部のインターネット接続のコストが余計にかかるために、コスト面で現実的でないかもしれない。

7.4.5　脆弱性診断における変化

クラウドコンピューティングにおける脆弱性診断は、アーキテクチャと契約の両方の制約に対応しなければならない。

- クラウド（パブリックあるいはプライベート）のオーナー（所管者）は通常、脆弱性診断の通知を要求し、脆弱性診断の内容に制限を加えるだろう。これはなぜなら、事前の通告がない場合、実際の攻撃と、脆弱性診断とを区別することができない可能性があるためである。
- デフォルト設定を拒否としているネットワークはさらに、ファイアウォールと同様に、自動化されたネットワーク診断の本来の有効性を減殺する。脆弱性診断を実行するための穴をあけたり、脆弱性診断を実行す

るためにインスタンス上でエージェントを使ったりする必要がある。さもないと、数多くのテストがファイアウォールルールでブロックされたことを知るだけの診断になる。

- 脆弱性診断は、変更無用(immutable)なワークロードのイメージ生成プロセスの間に実行できる。これらは本番環境ではないために、またプロセスは自動化されているため、より少ないネットワーク上の制約のもとで実行でき、こうして脆弱性診断の対象面を拡大できる。
- ペネトレーションテストは、それが攻撃者と同じやり方を使うために、影響を受ける度合は少ない。ペネトレーションテストについては、ドメイン 10 で詳細に説明する。

7.4.6 クラウドストレージのセキュリティ

インフラの一部ではあるけれども、ストレージとデータセキュリティについてはドメイン 11 で深く詳しく説明する。

7.5 推奨事項

- 利用しているクラウド事業者またはプラットフォームのインフラセキュリティを知ること
  - セキュリティ共有モデルでは、クラウド事業者は（あるいはプライベートクラウドプラットフォームを擁する者は）、クラウドの下層にある物理、抽象化、統合管理の各層がセキュアであることを確実にする責務を負う。
  - コンプライアンスの認証（certification）と評価証明（attestation）を検証すること
    - クラウド事業者がクラウドインフラのベストプラクティスと規制に従っていることの担保を得るために、業界標準および業界固有のコンプライアンス要件に対する認証と評価証明を定期的に確認すること。
- ネットワーク
  - 利用可能であるなら SDN を利用すること。
  - 複数の仮想ネットワークと複数のクラウドのアカウント／セグメントに対し、SDN の機能を使って、ネットワーク間の隔離を強化すること。
    - 従来型のデータセンタに比べて、アカウントの分離と仮想ネットワークによって、劇的にインシデントの影響する範囲を小さくすることができる。
  - クラウドファイアウォールでデフォルト拒否を実装すること。
  - クラウドファイアウォールを、ネットワーク単位ではなく、ワークロード単位に適用すること。
  - 利用可能なかぎりクラウドファイアウォール（セキュリティグループ）ポリシーを使って、同じ仮想サブネット内のワークロード間のトラフィックを定常的に抑制すること。
  - 伸縮性を阻害したり性能のボトルネックを引き起こす仮想アプライアンスに依存することを最小にすること。
- コンピューティング／ワークロード
  - 可能なかぎり変更無用なワークロードを活用すること。
    - リモートアクセスを無効にすること。
    - イメージ生成の中にセキュリティテストを組み入れること。
    - ファイルの完全性モニタリングを使ってアラームを上げること。
    - 稼動しているインスタンスにパッチを当てるのではなく、イメージを更新することでパッチを適用すること。

    - もし必要なら、クラウドに対応していて、性能への影響を最小にできる、セキュリティエージェントを選択すること。
- クラウド対応のツールを利用した上で、長期間稼動するワークロードに対するセキュリティコントロールを維持すること。
- ログをワークロードの外部に保存すること。
- 脆弱性診断とペネトレーションテストに対してクラウド事業者が設定している制約を認識し、それに従うこと。

DOMAIN 8
仮想化とコンテナ技術

8.0　はじめに

仮想化は単に仮想マシンを作成するためのツールではなく、クラウドコンピューティングを実現するためのコアテクノロジーである。仮想化は、フル稼働の仮想マシンから Java 仮想マシンのような仮想実行環境まで、更にはストレージ、ネットワーキングなどのコンピューティング全体で使用されている。

クラウドコンピューティングは基本的にリソースをプールすることに基づいており、仮想化は固定のインフラをこれらのプールされたリソースに変換する技術である。仮想化は、リソースプールに必要な抽象化を提供し、リソースプールは統合管理を使用して管理される。

前述のとおり、仮想化は非常に幅広い技術をカバーしている。 基本的には抽象化を実施するたびに、仮想化を使用している。クラウドコンピューティングでは、リソースプールを構築するために使用される仮想化の特定の側面、特に以下の項目に注目する。

- Compute（コンピュート）
- Network（ネットワーク）
- Storage（ストレージ）
- Containers（コンテナ）

これらは仮想化に関連するカテゴリの全てではないが、クラウドコンピューティングに最も関連性の高いものである。

クラウドセキュリティを適切に設計し実装するためには、仮想化によるセキュリティへの影響を理解することが基本的に重要である。リソースプールから割り当てられた仮想資産は、置き換えられた物理資産のように見えるかもしれないが、その見た目や使い勝手は、我々が見ているものをよりよく理解して管理するのに正に役立つツールである。また、オペレーティングシステムなどの既存のテクノロジを、ゼロから完全に書き換えることなく、活用するのにも役立つ。その下では、これらの仮想資産は、それらが抽象化された元のリソースとはまったく異なる働きをする。

8.1　概要

最も基本的な処として、仮想化は基盤となる物理資産からリソースを抽象化する。 コンピュータそのものからネットワーク、プログラムコードに至るまで、テクノロジのほぼすべてを仮想化できる。冒頭で述べたように、クラウドコンピューティングは基本的に仮想化に基づいている。仮想化は、プールを構築するためにリソースを抽象化する方法である。 仮想化がなければ、クラウドはない。

多くのセキュリティプロセスは、基盤となるインフラの物理的な制御を想定して設計されている。これはクラウドコンピューティングでも必要である一方、仮想化ではさらにセキュリティ制御用の 2 つの新しいレイヤが追加される。

- **仮想化技術自体のセキュリティ。** 例えば、ハイパーバイザのセキュリティを確保する。
- **仮想資産のセキュリティ制御。** 多くの場合、物理層におけるセキュリティ制御とは異なる方法で実装しなければならない。例えば、ドメイン 7 で説明したように、仮想ファイアウォールは物理ファイアウォールと同じではなく、物理的なファイアウォールを仮想マシンに抽象化するだけでは、配備やセキュリティ上の要件を満たしていない可能性がある。

クラウドコンピューティングにおける仮想化セキュリティにおいても、共同責任モデルは変らない。クラウド事業者は、物理インフラと仮想化プラットフォーム自体のセキュリティに常に責任を負う。一方、クラウド利用者は、クラウド事業者によって実装され、管理されているものに基づいて、利用可能な仮想化セキュリティ制御を適切に実装し、根本にあるリスクを理解する責任がある。例えば、仮想化ストレージを暗号化するタイミングの決定、仮想ネットワークと仮想ファイアウォールの適切な設定、または専用ホストと共有ホストのどちらを使用するかを決定するなどである。

これらのコントロールの多くは、データセキュリティなどの他のクラウドセキュリティ分野にも関係するため、このドメインでは仮想化に固有の問題に集中しようとしている。ただし、その境界線は必ずしも明確ではない。また、クラウドセキュリティ制御の大部分については、このガイダンスの他のドメインでより詳しく説明している。 ドメイン 7：インフラセキュリティは、仮想ネットワークとワークロードに詳しく焦点を当てている。

8.1.1 クラウドコンピューティングに関連する仮想化の主なカテゴリ

8.1.1.1 コンピュート

コンピュートの仮想化は、コード（オペレーティングシステムを含む）の実行を、基盤となるハードウェアから分離して抽象化する。ハードウェア上で直接実行する代わりに、コードは抽象レイヤの上で実行され、そのことによって同じハードウェア上で複数のオペレーティングシステムを実行する（仮想マシン）など、より柔軟な使用を可能にする。これは単純化した説明であり、さらに知りたい場合は、仮想マシンマネージャとハイパーバイザについてさらに調べることをお勧めする。

コンピュートは最も一般的には仮想マシンで行われるものであるが、これは急速に変化している。その主な理由は、進化し続ける技術とコンテナの採用にある。

コンテナと特定の種類のサーバレスインフラもまた、コンピュートの抽象化を行う。これらは、コード実行環境を構築する別の種類の抽象化であるが、仮想マシンのように完全なオペレーティングシステムの抽象化を行う訳ではない。 （コンテナについては、後で詳しく説明する）。

クラウド事業者の責任

コンピュート仮想化におけるクラウド事業者の主要なセキュリティ上の責任は、隔離を実施し、安全な仮想化インフラを維持することである。

- **隔離**とは、1 つの仮想マシン／コンテナ内の計算プロセスまたはメモリが別の仮想マシン／コンテナから見えないことを確実にすることである。隔離により、同じ物理的なハードウェア上でプロセスを実行している場合でも、異なるテナントを切り離すことができる。

- クラウド事業者は、**基盤となるインフラと仮想化技術**を外部の攻撃や内部の誤用に対してセキュアに保つ責任も負っている。これは、適切に構成され、それらをいつでも最新の状態でセキュアに保つプロセスでサポートされている、パッチが適用された最新のハイパーバイザを使用することを意味する。クラウドの全体にわたってハイパーバイザにパッチを適用することができないと、その技術に新たな脆弱性が発見された場合、根本的にセキュアでないクラウドになる可能性がある。

クラウド事業者は、クラウド利用者のための仮想化のセキュアな使用もサポートする必要がある。その意味するところは、ブートプロセスから始まる一連のセキュアなプロセスを、仮想マシンが稼働するイメージ（または他の資源）に基づいて、セキュリティと完全性を確保しつつ、生成することである。これにより、テナントは、他のテナントに属しているイメージなど、アクセス権が無いイメージに基づいてマシンを起動することができず、実行中の仮想マシン（またはその他のプロセス）がまさに利用者が意図した通りのものであることが保証される。

さらに、クラウド事業者は、揮発性メモリが不正なモニタリングに対して安全であることをクラウド利用者に保証する必要がある。なぜならば、実行中のメモリに対し、他のテナント、悪意のある従業員、さらには攻撃者がアクセスできる場合には、重要なデータが見られる可能性があるためである。

クラウド利用者の責任

一方、クラウド利用者の主な責務は、仮想環境内に配備しているすべてのものに対しセキュリティを適切に実装することである。コンピューティング仮想化に関するセキュリティの責任はクラウド事業者にあるため、クラウド利用者にとって、ワークロードの仮想化に直接関係するセキュリティの選択肢はほとんどない。ワークロードをセキュアにする手段は他にも多くあり、それらはドメイン 7 で取り上げている。

とは言え、クラウド利用者がセキュリティ実装に際して押さえるべき、仮想化固有の相違点はいくつかある。まず、クラウド利用者は、仮想インフラを管理するためのセキュリティ制御を活用する必要があるが、セキュリティ制御手段は、クラウドプラットフォームに応じて異なる。一般に以下のようなものがある：

- **アイデンティティ管理などのセキュリティ設定の仮想リソースへの適用**　これは、オペレーティングシステムのログイン資格情報など、リソース内のアイデンティティ管理ではなく、例えば、仮想マシンの構成の停止や変更のようなクラウドリソースの管理を誰に許可するかという、アイデンティティ管理である。 管理用ダッシュボードのセキュリティの詳細については、ドメイン 6 を参照すること。
- **監視とロギング**　ドメイン 7 はコンテナや仮想マシンからのシステムログの取得方法を含め、ワークロードの監視とロギングを取り扱うが、それに加えて、クラウドプラットフォームは仮想化レベルでのロギングと監視を提供する。これには、仮想マシンのステータス、管理イベント、パフォーマンスなどが含まれる。
- **イメージ資産の管理**　クラウドにおけるコンピューティングの配備は、仮想マシン、コンテナ、またはその他のコードなど、クラウドで実行されるマスターイメージを基にしている。この仕組みは通常、高度に自動化されており、従来型コンピューティングにおけるマスターイメージと比較して、元となるイメージの数が多くなる結果をもたらす。それらイメージを管理すること、何がセキュリティ要件を満たしているか、どこに配備してよいか、アクセスできるのは誰か、などの管理は、重要なセキュリティ上の責任である。
- **専用ホスティングの使用**（リソースのセキュリティ環境に基づいて利用可能な場合）　場合によっては、マルチテナントクラウド上であっても、専用のハードウェアで資産を実行する（高いコストで）ように指定することができる。これは、他のテナントとのハードウェアの共有がリスクとみなされる特殊なケースでは、コンプライアンスの要件を満たしたり、セキュリティのニーズを満たすのに役立つ。

第 2 に、クラウド利用者は仮想化されたリソース内のセキュリティ制御に対しても責任を負う：

- これには、ワークロード、すなわち仮想マシン、コンテナ、アプリケーションコードなどの、全ての標準的セキュリティが含まれる。 これらのセキュリティは、標準的なセキュリティのベストプラクティスと、ドメイン 7 にある補足的なガイダンスによって十分カバーされている。
- 特に重要なのは、安全な構成設定（例えばパッチが適用された最新の仮想マシンイメージ）だけを配備することを確実にすることである。クラウドコンピューティングの自動化機能のおかげで、パッチが適用されていないかセキュリティが適切でない、古い構成設定が簡単に配備されてしまう。

他の一般的なコンピューティングのセキュリティに関する懸念事項は次のとおりである：

- 仮想化されたリソースは、より短命であり、より急速なペースで変化する傾向がある。監視などの、これに対応するいかなるセキュリティも、こうしたペースに追いついていなければならない。 これについても、詳細はドメイン 7 で詳しく説明する。
- 特にサーバレス型の配備の場合、ホストレベルの監視／ロギングを使用できないことがある。代替のログ方法を実装する必要があるかもしれない。例えば、サーバレス型の配備では、基盤となるプラットフォームのシステムログが提供されない可能性があり、より堅牢なアプリケーションログをコードに書き込むことで補完しなければならない。

8.1.2 ネットワーク

基本的な VLAN から完全なソフトウェア定義ネットワークまで、複数の種類の仮想ネットワークがある。クラウドインフラのセキュリティの根幹として、これらは本ドメインとドメイン 7 の両方で取り上げられている。

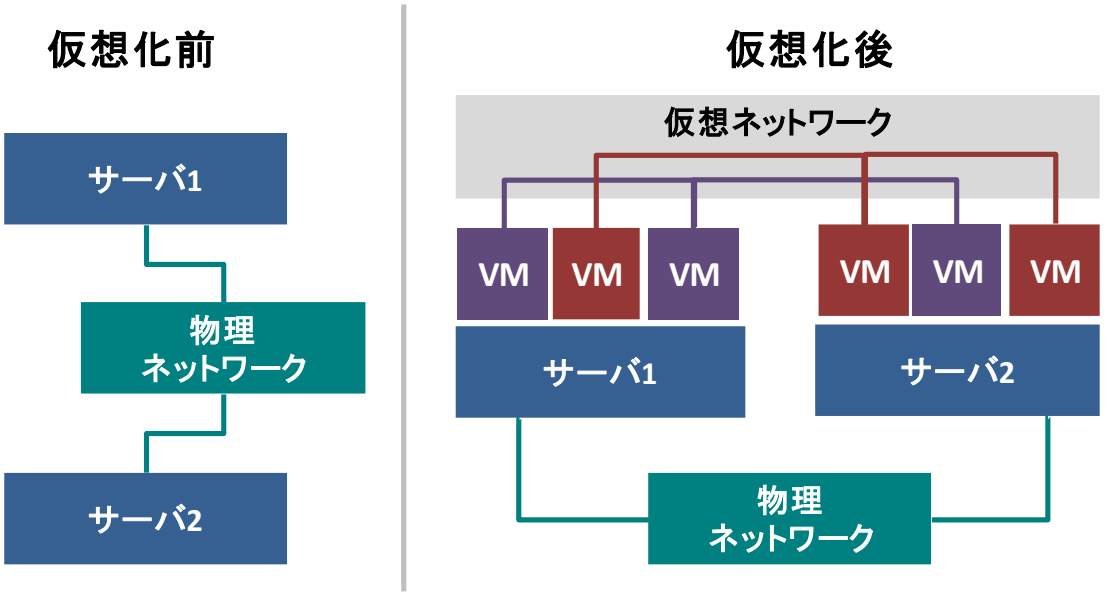
振り返ってみると、今日の多くのクラウドコンピューティングでは、SDN を使用してネットワークを仮想化している。（VLAN は、マルチテナントのために重要な隔離機能がないため、クラウドでの配備には適していない。）

SDN は、下層にある物理インフラからネットワーク管理プレーンを抽象化し、多くの典型的なネットワーク上の制約を取り除く。例えば、すべてのトラフィックが適切に分離され隔離されることで、同じ物理ハードウェア上で、複数の仮想ネットワークを、そのアドレス範囲と完全に重複するものでもオーバーレイすることができる。SDN はまた、統合管理と機動性をサポートする、ソフトウェア設定と API 呼び出しによっても、定義される。

仮想ネットワークは物理ネットワークとはまったく異なる。物理ネットワーク上で動作するが、抽象化によって、ネットワークの挙動を大きく変えることが可能になり、その結果、多くのセキュリティのプロセスや技術に影響を及ぼす。

8.1.2.1 監視とフィルタリング

（セキュリティへの影響として）特に、パケットが仮想ネットワークをどのように移動するかの違いによって、監視とフィルタリング（ファイアウォールを含む）が大幅に変化する。リソースは、トラフィックが物理ネットワークを通過することなく、物理サーバ上で通信することができる。例えば、2 台の仮想マシンが同じ物理マシン上にある場合、ネットワークトラフィックを外に出してネットワークにルーティングする必要はない。このようにしてリソースは直接通信することができ、ネットワーク上に組み込まれた（またはルーティング／スイッチングハードウェアに接続された）監視とフィルタリングのツールは全くトラフィックを検知できない。



仮想ネットワークではソフトウェアによりパケットが移動し、物理ネットワーク接続でのスニッフィングによる監視は不可能である。

5

これを補うために、同じハードウェア上の仮想ネットワーク監視またはフィルタリングツール（ネットワークセキュリティ製品の仮想マシンバージョンを含む）にトラフィックをルーティングできる。すべてのネットワークトラフィックを中継し、元の（物理）ネットワークに戻すか、同じ仮想ネットワーク上の仮想アプライアンスにルーティングすることもできる。これらのアプローチのそれぞれには、ボトルネックと効率の悪いルーティングが発生するという欠点がある。

クラウドプラットフォームやクラウド事業者は、ネットワークの直接監視のためのアクセスをサポートしていない可能性がある。パブリッククラウド事業者は、複雑さ（およびコスト）のために、完全なパケットネットワーク監視を利用者に許可することはめったにない。従って、ホスト上で自分で収集するか、仮想アプライアンスを使用しない限り、生のパケットデータにアクセスすることはできない。

特にパブリッククラウドの場合、クラウドサービス間の通信はクラウド事業者のネットワーク上で発生する。つまり、そのトラフィックのクラウド利用者による監視およびフィルタリングは不可能である（また、クラウド事業者のセキュリティリスクを引き起こす）。例えば、サーバレスアプリケーションをクラウド事業者のオブジェクトストレージ、データベースプラットフォーム、メッセージキュー、またはその他の PaaS 製品に接続すると、そのトラフィックはそのままでクラウド事業者のネットワーク上を通り、必ずしもクラウド利用者管理下の仮想ネットワークに行く訳ではない。単純なインフラストラクチャ仮想化から踏み出すにつれ、利用者管理によるネットワークという考え方は次第に希薄になっていく。

しかし、最新のすべてのクラウドプラットフォームにはファイアウォールが組み込まれており、これに相当する物理的なファイアウォールに比べて利点がある。それらは、SDN またはハイパーバイザ内で動作するソフトウェアファイアウォールである。それらは、通常、最新の専用の次世代ファイアウォールよりも提供する機能は少ないが、クラウド事業者が提供するその他の組込みセキュリティがあるために、そのような高度な機能は必ずしも必要ではない。

訳注5　図中の VLAN の接続線は、訳者の判断で、解りやすくするために若干変更を加えた。

8.1.2.2 管理インフラストラクチャ

クラウドコンピューティングの仮想ネットワークは常にリモート管理をサポートしているため、管理用ダッシュボードやメタストラクチャのセキュリティは重要である。場合によっては、複雑なネットワーク全体を、少数の API 呼び出しや Web コンソール上の数回のクリックにより、構築したり、また破壊したりすることも可能である。

クラウド事業者の責任

クラウド事業者は本来、セキュアなネットワークインフラを構築し、適切に設定する責任がある。セキュリティの絶対的な最優先事項は、テナントが他のテナントのトラフィックを参照できないようにするための、ネットワークトラフィックの分離と隔離である。これは、全てのマルチテナントネットワークで最も基本的なセキュリティ制御である。

クラウド事業者は、テナント間でデータや設定を見えるようにしてしまう可能性のあるパケットスニッフィングやその他のメタデータの「漏洩」を無効にする必要がある。またテナント独自の仮想ネットワーク内であっても、パケットスニッフィングを無効にする必要がある。それにより、非仮想ネットワーク上では一般的である、攻撃者がある（スニッフィング）ノードに侵入してネットワークをモニタする可能性を減らすべきである。タギングやその他の SDN レベルのメタデータもまた、管理用ダッシュボードの外部に曝されないようにすべきであり、さもないと、侵入されたホストが SDN 自体の中に入り込むために用いられる可能性がある。

すべての仮想ネットワークでは、ホストファイアウォールや外部製品を必要としないで済むように、クラウド利用者用に組込みのファイアウォール機能を利用可能とすべきである。クラウド事業者はまた、基盤となる物理ネットワークと仮想化プラットフォームに対する攻撃を検出して防御する責任がある。その責任には、クラウド自体の境界セキュリティも含まれる。

クラウド利用者の責任

クラウドの利用者は第一に、仮想ネットワーク、特に全ての仮想ファイアウォールの配備を適切に設定する責任がある。

物理的な接続やルーティングに制約されないため、ネットワークアーキテクチャは仮想ネットワークのセキュリティにおいてより大きな役割を担っている。仮想ネットワークはソフトウェア構造であるため、複数の別々の仮想ネットワークを使用すると、従来の物理ネットワークでは不可能な、微細な区画化の利点がもたらされる可能性がある。すべてのアプリケーションスタックを各々の仮想ネットワークで実行でき、これにより、悪意を持った者が攻撃の足場を得た場合の攻撃にさらされる口が劇的に減少する。 物理ネットワーク上で同等のアーキテクチャを築くことはコスト面で不可能である。

変更無用なネットワークは、ソフトウェアテンプレートを使用して、一部のクラウドプラットフォームで設定することができ、有効性が確認されている設定を適用するのに役立つ。有効性が確認されているネットワーク設定は、全ての設定を手動で設定するのではなく、テンプレートの中で全て定義できる。このことにより、セキュアなベースラインを備えたネットワークを数多く構築する能力がなくても、有効性が確認されている設定からの逸脱を検出し、場合によってはそれを元に戻すこともできる。

クラウド利用者は、さらに、管理用ダッシュボード内に表示されるコントロールの適切な権限管理と構成設定に責任がある。仮想ファイアウォールまたは監視機能がセキュリティニーズを満たしていない場合、クラウド利用者は仮想セキュリティアプライアンスまたはホストセキュリティエージェントにより補う必要がある。これはクラウドのインフラストラクチャ・セキュリティの領域で、ドメイン 7 で詳しく説明されている。

8.1.2.3 クラウドのオーバーレイ・ネットワーク

クラウドのオーバーレイ・ネットワークは、複数の「ベース」ネットワークをまとめて構成するネットワークのための特別な種類の WAN 仮想化技術である。例えば、オーバーレイ・ネットワークはクラウドの物理的所在場所または複数のクラウドネットワークにまたがる可能性があり、おそらく別のクラウド事業者間である場合もある。詳細な議論はこのガイダンスの範囲を超えているが、中核的なセキュリティ推奨事項は同様に適用される。

8.1.3 ストレージ

ストレージ仮想化は、ほとんどの組織で既に一般的である。SAN (Storage Area Network)と NAS (Network Attached Storage)はともにストレージ仮想化の一般的な形式である。ストレージのセキュリティについては、ドメイン 11 で詳しく説明している。

ほとんどの仮想化ストレージは耐久性があり、異なる所在地に複数のデータコピーを保持するため、ハードディスクドライブの障害によってデータが失われる可能性は低くなる。これらのドライブを暗号化すると、非常に頻繁に行われるハードディスクドライブのスワップアウトによって、データが外から見られる懸念が、軽減される。

ただし、この暗号化は仮想化レイヤ内のデータを保護しない。すなわち物理ストレージのデータのみを保護する。ストレージの種類によっては、クラウド事業者が仮想化レイヤでの暗号化を（場合によっては物理ストレージの代わりに）提供することもあるが、利用者のデータをクラウド事業者に見られないよう保護することはできない。従って、ドメイン 11 のアドバイスを使用して、何らかの追加的な保護を用意する必要がある。

8.1.4 コンテナ

コンテナは、移植性の高いコード実行環境である。簡単に言うと、仮想マシンはカーネルまですべてを含む完全なオペレーティングシステムである。一方、コンテナは、隔離されたユーザ空間を提供するが、共有のカーネルを使用する仮想実行環境である。詳細な議論はこのガイダンスの範囲を超えており、ソフトウェアコンテナに関する詳細は Wikipedia の記述を参照されたい。

このようなコンテナは、物理サーバ上に直接構築することも、仮想マシン上で実行することもできる。現在見られる実装は、既存のカーネル／オペレーティングシステムに依拠しているため、ネストされた仮想化がハイパーバイザによってサポートされていない場合でも仮想マシン内で実行できる。（ソフトウェアコンテナは、ハイパーバイザとは全く異なる技術によっている）。

ソフトウェアコンテナシステムには、常に 3 つの主要コンポーネントが含まれる：

- 実行環境（コンテナ）
- 統合管理とスケジューリングのコントローラ（複数のツールの組合せでもよい）
- コンテナイメージまたは実行するコードのリポジトリ
- これらをまとめて言うと、実行場所、実行対象、そしてそれらを結びつける管理システムである。

技術的プラットフォームが何であれ、コンテナのセキュリティには以下が必要である：

- **基盤となる物理インフラ（コンピュート、ネットワーク、ストレージ）のセキュリティを確保する。**これは他の形式の仮想化と変わりはないが、コンテナの実行環境が動作する基盤となるオペレーティングシステムにも対象範囲が拡張される。
- 管理用ダッシュボードのセキュリティを確保する。この場合は統合管理機能とスケジューラ。
- **イメージリポジトリを適切に保護する。**イメージリポジトリは、適切なアクセスコントロールが設定された安全な場所に置く必要がある。これは、コンテナイメージと定義ファイルの喪失または未承認の変更を防止するとともに、承認されていないファイルアクセスによる機微データの漏洩を未然に防止するためである。コンテナは実に簡単に実行できるので、イメージの配備が適切なセキュリティ環境でのみ行われることも重要である。
- **コンテナ内で実行されているタスク／コードにセキュリティを組み込む。** コンテナ内で脆弱なソフトウェアを実行することは実際に可能であり、場合によっては、共有オペレーティングシステムや、あるいは他のコンテナからのデータが外部にさらされる可能性がある。例えば、ファイルシステム上のコンテナのデータへのアクセスだけでなく、ルートファイルシステムへのアクセスを許可するようにいくつかのコンテナを設定することも可能である。あまりにも多くのネットワークアクセスを許可することもまた危険である。これらはすべて特定のコンテナプラットフォームに当てはまるため、コンテナ環境とイメージやコンテナの構成設定の両方をセキュアに設定する必要がある。

コンテナは急速に進化しており、セキュリティのいくつかの面を複雑なものにしているが、それらが本質的に安全でないという意味ではない。

コンテナは必ずしも完全なセキュリティ隔離を提供するわけではないが、タスク分離については間違いなく提供される。一方で、仮想マシンは通常、セキュリティ隔離を提供する。従って、同等のセキュリティ環境のタスクを同一設定の物理ホストまたは仮想ホストに置くことで、より高度なセキュリティ分離を実現できる。

コンテナの管理システムとイメージリポジトリには、使用する製品によって異なるセキュリティ機能がある。セキュリティ担当者は、サポート対象の製品の機能を勉強し、理解する必要がある。コンテナ製品は、最低限、ロールベースのアクセス制御と強力な認証をサポートする必要がある。また、ファイルシステム、プロセス、ネットワークアクセスを隔離するなど、設定をセキュアにすることもサポートする必要がある。

コンテナのセキュリティを深く理解するには、名前空間、ネットワークポートマッピング、メモリ、ストレージアクセスなど、オペレーティングシステムの内部構造の深い理解が必要である。

ホストオペレーティングシステムとコンテナ技術が異なれば、セキュリティ機能も異なる。セキュリティに関する評価は、コンテナプラットフォームの選定プロセスに必ず含める必要がある。

セキュリティを確保するための 1 つの重要な要素は、特定の実行環境にどのイメージ／タスク／コードが許可されるかという管理である。適切なコンテナ管理とスケジューリングを備えたセキュアなリポジトリがこれを可能にする。

8.2 推奨事項

- クラウド事業者がするべきこと
    - 仮想化に使われる基盤となるインフラの全てをそれ自体でセキュアにすること
    - テナント間のセキュリティ面の隔離を保証することに注力すること。

- 仮想化レイヤにおいて十分なセキュリティ機能を提供し、クラウド利用者がその資産のセキュリティを適切に確保できるようにすること。
- 物理インフォストラクチャと仮想化プラットフォームを攻撃者と内部不正に対してしっかりと防御すること。
- クラウド利用者が管理する全ての仮想化機能に対し、デフォルトでセキュアな設定を実装すること。
- 特に重要な事項：
  - コンピューティング
    - セキュアなハイパーバイザを使用し、パッチ管理手段を実装して最新に保つこと。
    - ハイパーバイザを仮想マシンが相互に隔離されるように設定すること。
    - 内部の手続きを定めて技術的セキュリティコントロールを実装し、管理者やテナントでない者による実行中の仮想マシンや揮発性メモリへのアクセスを防止すること。
  - ネットワーク
    - 優れた境界セキュリティ防御を実装し、基盤にあるネットワークを攻撃から守ると共に、可能な限り、物理レベルでのクラウド利用者への攻撃や、利用者が自分では直接守れない全ての仮想ネットワークへの攻撃を、検知して阻止すること。
    - たとえ全て同じクラウド利用者がコントロールしていたとしても、利用者が故意に別の仮想ネットワークを接続しているのでない限り、仮想ネットワーク間の隔離を確実に行うこと。
    - 内部のセキュリティコントロールとセキュリティポリシーを導入し、クラウド利用者のネットワークに変更を加えることと、別途の契約上の合意なくトラフィックのモニタリングすることの両方を防止すること。
  - ストレージ
    - 他のレベルですでに暗号化されていない場合は、基盤にある全てのストレージを暗号化し、ハードディスクドライブ交換に際してデータが外部から見られることを防ぐこと。
    - 暗号化機能をデータ管理機能から隔離し、クラウド利用者のデータへの承認を得ないアクセスを防止すること。
- クラウド利用者がするべきこと：
  - 利用しているクラウド事業者の提供する機能とセキュリティ上のギャップを確実に認識すること。
  - 仮想化サービスを、クラウド事業者のガイダンスと業界の実践規範に沿って適切に設定すること。
    - 仮想化のセキュリティの基本的部分はすべてクラウド事業者に依存する。そのため、このガイダンスでは、クラウド利用者向けのセキュリティの推奨事項は他のドメインで扱われている。
  - コンテナに関して：
    - 利用するコンテナプラットフォームとその下の OS のセキュリティのための隔離機能を把握し、適切な設定を選択すること。
    - コンテナ間の隔離の実施には物理マシンまたは仮想マシンを用い、同一の物理／仮想ホスト上の同一のセキュリティ要件のコンテナはグループ化すること。
    - 配備対象となるのは、確実に、承認済みで認知済みでセキュアなコンテナのイメージかコードだけとなるようにすること。
    - コンテナの統合化・管理およびスケジューラのソフトウェアのセキュリティを適切に設定すること。
    - 全てのコンテナとリポジトリ管理に対して、適切なロールベースのアクセス管理と、強度の高い認証を実装すること。

DOMAIN 9
インシデントレスポンス

9.0　はじめに

インシデントレスポンス（IR）は、全ての情報セキュリティプログラムの重要な一面である。予防的セキュリティコントロールでは、重要なデータが侵害される可能性を完全に排除することができないことが確認されている。大方の組織は、攻撃に対する調査プロセスを統括する何らかの IR 計画を備えているが、クラウドではフォレンジックデータへのアクセスと統制に大幅な違いが生じるため、組織は IR プロセスの変更について検討しなければならない。

このドメインでは、クラウドコンピューティング固有の特性がもたらす、IR に関するギャップを明らかにすることを目的としている。セキュリティ専門家は、このドメインの内容を IR ライフサイクルの準備段階で、レスポンスプラン（対応計画）を作成し、その他の活動を行う際に参考にすることができるだろう。 このドメインの構成は、米国国立標準技術研究所（NIST）のコンピュータセキュリティインシデント対応ガイド（NIST SP800-61,2012 年 8 月改訂第 2 版）[1]に記載されている、一般に受け入れられたインシデントレスポンスライフサイクルに沿って構成している。 インシデントレスポンスに関するその他の国際標準フレームワークとしては、ISO / IEC 27035 や ENISA の「インシデントレスポンスとサイバー危機における協力に関する戦略」が存在する。

このドメインでは、NIST SP800-61 Rev2 の記載に沿ってインシデントレスポンスライフサイクルについて述べた後、引き続く各節でライフサイクルの各段階について述べ、クラウド環境においてインシデントへの対応者が直面するであろう問題について明らかにする。

9.1　概要

9.1.1　インシデントレスポンスライフサイクル

インシデントレスポンスライフサイクルは、NIST SP800-61rev2 の文書で定義されており、そこには、以下のフェーズと主要な実施事項が含まれている。

インシデントレスポンスライフサイクル

- 準備：「組織がインシデントに対応する準備が整うようにインシデント対応機能を確立する」

- インシデントの処理プロセス。
- インシデント対応者のコミュニケーションとそのための設備。
- インシデント分析用ハードウェアとソフトウェア。
- 内部文書（ポート一覧、資産リスト、ネットワーク図、ネットワークトラフィックの現状のベースライン）。
- インシデントを発見するための訓練。
- スキャンとネットワーク監視、脆弱性評価およびリスクアセスメントの実施によるインフラストラクチャの事前評価。
- 外部機関による脅威情報サービスの提供契約。

- 検知と分析
  - アラート（エンドポイント保護、ネットワークセキュリティ監視、ホスト監視、アカウント作成、権限昇格、侵害に関するその他の兆候、SIEM、セキュリティ分析（ベースラインと異常検知）、ユーザ行動分析）。
  - アラートの検証（誤検知（false positives）の低減）とエスカレーション。
  - インシデントの範囲の推測。
  - それ以降の対応を調整するインシデントマネージャの任命。
  - インシデントの封じ込めと復旧の状況について上級管理層に報告する役割の者の任命。
  - 攻撃のタイムラインの構成。
  - データ損失が起きた場合の範囲の特定。
  - 通知および調整活動。

- 封じ込め、根絶と復旧[6]
  - 封じ込め：システムのオフライン化。データ損失とサービスの可用性のどちらを優先するかの検討。 検知時におけるシステムの損傷防止の確保。
  - 根絶と復旧：侵害されたデバイスのクリーンアップと通常運用へのシステムの復旧。システムが適正に機能していることの確認。類似インシデント防止のためのコントロールの展開。
  - インシデントの記録と証拠の収集（証拠保全の連続性）。

- 事後分析
  - 対応プロセスの改善点、攻撃の早期発見の余地、早期の攻撃隔離のために有用なその他のデータの特定、IR プロセス変更の必要性とその方法等

9.1.2 クラウドの IR への影響

IR のライフサイクルの各フェーズは、クラウドの配備によって、それぞれ程度の異なる影響を受ける。ある点は、アウトソースされた環境の中で行われる、第三者との連携が必要なインシデント対応に類似している。その他の違いは、抽象化され自動化されるクラウドの性質によって、より独特なものとなっている。

訳注[6] ：原文では、この項および以下の 3 項が「検知と分析」の下位項目と同列になっているが、明らかにライフサイクルの 1 フェーズであり、タブレベルのミスと判断されるので、正しい位置に修正して表記する。

9.1.2.1 準備段階

クラウドにおけるインシデント対応の準備には、いくつかの重要な考慮事項がある：

- **SLA およびガバナンス：**パブリッククラウドまたはホスト型サービスプロバイダを利用している際のインシデントへの対応には、サービスレベルアグリーメント（SLA）の理解と、場合によってはクラウド事業者との調整が必要である。クラウド事業者との取引内容によっては、直接の対応窓口が存在せず、標準のサポートによる対応しか得られない可能性も認識しておくこと。外部のデータセンタによるカスタム化されたプライベートクラウドの場合は、新しい SaaS アプリケーションについて Web サイト上で契約したり、ライセンス契約にクリックするような場合とは、大きく異なった取引内容になってくるだろう。

主な課題としては次のようなものがある： 自組織が行う作業は何か？ クラウドサービス事業者（CSP）の任務は何か？ 連絡窓口となるのは誰か？ 対応までの想定時間はどれくらいか？ エスカレーション手順はどのようなものか？ （ネットワークトラブルの場合の）ネットワーク外部を経由した連絡方法があるか？ 事業者との連携はどのように機能するか？ どのようなデータにアクセスできるのか？

可能であれば CSP との間の手順のテストを確実に実施すること。エスカレーションおよび各々の役割／責任が明確であることを検証すること。CSP が検知したインシデントについて通知する窓口が設定され、通知が自社のプロセスに組み込まれていることを確実にすること。クリックして利用するサービスの場合は、通知は登録されたメールアドレスに送信される場合がある。それらは企業側で管理し、継続して監視すること。CSP への連絡窓口を、ネットワーク外の手段も含めて確実に持ち、そのテストを確実に行うこと。

- **IaaS/Paas 対 SaaS：**マルチテナント環境では、自社のクラウドに固有のデータの、調査のための提供を、どのように受けられるか？ 主要なサービスごとに、インシデントが発生した場合に利用できるデータおよびログを把握し、文書化する必要がある。インシデント発生後にクラウド事業者に連絡することが可能で、通常は利用できないデータを収集できると考えてはならない。
- **「クラウドジャンプキット(cloud jump kit)」：**遠隔地（クラウドベースのリソースも）に対して調査するために必要なツールである。たとえば、クラウドプラットフォームからログとメタデータを収集するツールを用意しているか？情報を解釈する機能を備えているか？どのようにして実行中の仮想マシンのイメージを取得し、ディスクストレージや揮発性メモリなどから、どのような種類のデータを利用できるか？
- **迅速な検知、調査、および対応（封じ込めと回復）を実現できるように、クラウド環境を設計すること。**これは、インシデント対応をサポートするための適切な設定とアーキテクチャを確実に備えることを意味する。
    - クラウド API ログなどの情報入手手段を機能するようにし、インシデントが発生した場合に、調査担当者が利用できる安全な場所にデータが確実に送られるようにすること。
    - 攻撃が広がりアプリケーション全体を侵害しないよう、隔離技術を利用すること
    - 可能であれば、設定変更が不可能なサーバを使用すること。 問題が検知された場合、ワークロードを、侵害されたデバイスから、既知の正常な状態のインスタンスへと移動させること。ファイルの完全性の監視と構成管理に一層の重点を置くこと。
    - アプリケーションスタックのマップを実装し、監視とデータキャプチャの位置的な違いを分析して、データが存在する場所を把握する。
    - クラウドスタック内のさまざまなコンポーネントに対する各種の攻撃に対する最も効果的な封じ込め手段を確認するために、脅威をモデル化し机上演習を実行することは非常に役に立つ。
    - このような準備においては、IaaS/PaaS/SaaS の応答の違いが考慮されている必要がある。

9.1.2.2 検知と分析

クラウド環境での検知と分析は、ほぼ同様に（IaaS の場合）、または相当に異なって（SaaS の場合）、見える場合がある。どのような場合でも、監視範囲は配備された資産だけでなく、クラウドの管理画面をもカバーしていなければならない。

クラウドに装備された監視とアラートの機能を使って自動化された IR のワークフローを起動し、レスポンスプロセスを速めることができる。一部のクラウド事業者は、こういった機能を自社のプラットフォームで提供しており、一部では第三者による監視のオプションも利用できる。多くのクラウドプラットフォーム（IaaS、場合により PaaS）は、パフォーマンスおよび運用上の目的のために、多種のリアルタイムまたは準リアルタイムの監視指標データを公開している。それらはセキュリティ特化型のものではないが、セキュリティチームは、セキュリティニーズのためにこれらの機能を活用できる場合がある。

クラウドプラットフォームは、さまざまなログも提供している。これらのログは、既存のセキュリティ運用／監視に組み込むこともできる。ログは、操作ログから、API 呼び出しまたは管理アクティビティの完全なログにまで及ぶ。ただし、全てのプロバイダで利用できるわけではなく、SaaS よりも IaaS や PaaS の場合に多く得られる可能性が高い。ログが提供されない場合には、環境および構成の変更を認識する手段として、クラウドのコンソールを利用することができる。

クラウドのインシデントにおけるデータソースは、従来型のコンピューティングにおけるインシデント対応で使用されているものとはかなり異なる場合がある。システムログなどはかなりの範囲で重複することがあるが、クラウドの管理画面からのフィードなど、データを収集する方法や新しい情報源の点で違いがある。

前述したように、クラウドプラットフォームのログは利用対象になりうるが、常に利用できるわけではない。理想的にはすべての管理画面の動作を示すべきではある。何がログに記録され、どんなギャップがあってインシデント分析に影響を及ぼすかを把握することは重要である。すべての管理活動は記録されているだろうか？自動化されたシステムの動作（例えば、自動スケーリング等）や、クラウド事業者の管理動作は含まれているだろうか？深刻なインシデントの場合、クラウド事業者は通常クラウド利用者が利用することができない、他のログを保有している場合もある。

情報を収集する際の 1 つの課題は、ネットワークの可視性が制限されることである。クラウド事業者からのネットワークログは、フローの記録であって、全てのパケットのキャプチャではない場合が多い。

（取得できるログと必要なログに）ギャップがある場合には、独自のログ収集を技術スタックに装備することができる。これは、インスタンス、コンテナ、およびアプリケーションコード内で、調査のための重要なデータを遠隔で得るために機能する。PaaS とサーバレスアプリケーションのアーキテクチャには特に注意が必要で、アプリケーションレベルでの独自のロギングが必要になるだろう。

侵入の兆候を把握し、攻撃に関する情報を入手するためには、オンプレミスのインシデントレスポンスの場合と同様に、脅威インテリジェンスもまた役に立つ。

CSP によって提供される情報に証拠保全の連続性(chain of custody)上の疑義がある場合、問題が起きる可能性があることに注意しなければならない。現時点で信頼できる前例は確立されていない。

フォレンジックと司法捜査に対するサポートにおいても、データソースの変更を理解すること以上の対応が必要である。

CSP は何が提供可能で、それが証拠保全の連続性(chain of custody)の要件を満たすかにつき、常に分析すること。すべてのインシデントが法的アクションにつながるわけではないが、自社の法務部門と協業して、その線引きがどこかと、証拠保全の連続性(chain of custody)の問題にどこで終止符を打てるかを把握す

ることは重要である。

クラウド環境は変動が大きくそのスピードも速いので、フォレンジック／調査プロセスの多くを自動化する必要性が高まっている。例えば、通常の自動スケーリングの動作によってや、管理者が調査の対象となる仮想マシンを消滅させる判断をした場合に、証拠が失われる可能性がある。自動化できるタスクの例を次に示す。

- 仮想マシンのストレージのスナップショット。
- アラート発生時にメタデータをキャプチャして、その時点でのインフラストラクチャの状態に基づいて分析が行われるようにすること。
- クラウド事業者がサポートしている場合には、仮想マシンを一時停止し、揮発性メモリの状態を保存すること。

また、クラウドプラットフォームの機能を活用して、侵害がどこまで及んでいるかを判断することもできる。

- ネットワーク上のデータフローを分析して、ネットワークの隔離の維持を確認する。 また、API 呼び出しを使用して、ネットワークと仮想ファイアウォールルールの状態のスナップショットを取ることもできる。これにより、インシデント発生時にスタック全体を正確に把握できる。
- 設定データを調べて、他の類似するインスタンスが、同じ攻撃に対する危険にさらされていないか確認する。
- （可能であれば、クラウドベースのストレージの）データアクセスログと管理画面のログを検査して、そのインシデントがクラウドプラットフォームに侵入しまたは影響を及ぼしたかどうかを確認する。
- サーバレスと PaaS ベースのアーキテクチャでは、クラウドプラットフォーム全体にわたる相関分析と、アプリケーションが自ら生成した何らかのログとが必要になる。

9.1.2.3 封じ込め、根絶と回復

常に、クラウドの管理画面／メタストラクチャに攻撃者が侵入していないことの確認から始めること。これは、クラウドのアカウントのルートまたはマスター証明書にアクセスするために、他の動作をすべて停止させる手続きの起動を伴うことがしばしばある。なぜならば、攻撃者の活動がマスキングされたり、下位レイヤにある管理者のアカウントから隠ぺいされていないことを確認するためである。攻撃者がまだ管理画面に留まっている場合、攻撃を封じ込めることはできないことを忘れてはならない。仮想マシンなどのクラウド資産に対する攻撃は、管理画面の証明書情報を暴き出し、それを利用して、より広範で深刻な攻撃を仕掛ける場合がある。

クラウドは、特に IaaS の場合、インシデントレスポンスのこの段階で大きな柔軟性を示す。ソフトウェアディファインドインフラストラクチャは、クリーンな環境での迅速なゼロからの再構築を可能にする。さらに分離された攻撃に対しては、自動でスケーリングするグループや、仮想ネットワークやマシンの設定変更を行う API コール、スナップショットなどのクラウド本来の特性によって、隔離、根絶、回復プロセスを加速することができる。たとえば、多くのプラットフォームでは、インスタンスを自動スケーリンググループから移動し、仮想ファイアウォールで隔離し、置き換えることで、仮想マシンを即座に隔離することができる。

これは、攻撃者の攻撃メカニズムと侵害の範囲を特定する前に、攻撃者を即座に「根絶する」必要がないことを意味する。なぜならば、新たなインフラストラクチャ／インスタンスがクリーンであるためであり、代わりに攻撃者を簡単に隔離することができる。ただし、エクスプロイトパスが閉じていて、他の本番用資産への侵入のために使用することができないことを確認する必要がある。管理画面への侵入が懸念される場合は、新しいインフラストラクチャ/アプリケーションのテンプレートや設定が侵害されていないことを確認すること。

とは言うものの、これらの機能は常に誰でも使えるというわけではない。SaaS や一部の PaaS では、非常に限定される可能性があり、結果としてクラウド事業者への依存度を高めざるを得ない。

9.1.2.4 事後分析

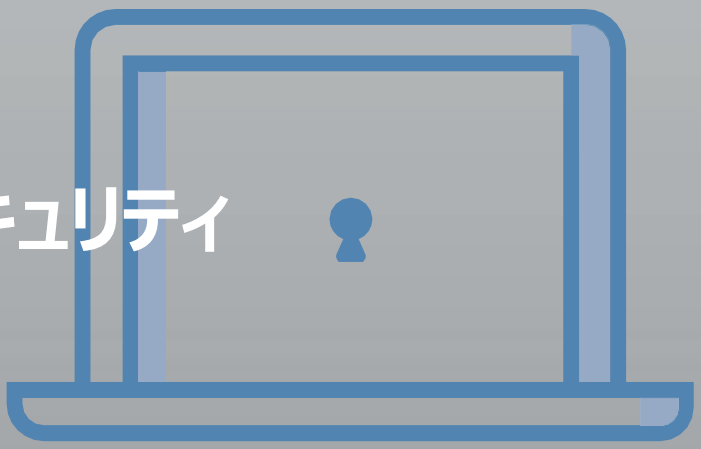
攻撃に対してと同様に、内部の対応チームおよびクラウド事業者と協力して、成功と失敗を把握し、改善すべき具体的な点を特定すること。収集されるデータに限界があることに特に注意を払い、今後に向けた課題への対処の方法を見つけ出すこと。

SLA を変更することは困難だが、合意した対応時間やデータ、あるいはその他のサポートでは十分でなければ、SLA に立ち返って再交渉を試みることが必要である。

9.2 推奨事項

- SLA および、クラウド利用者とクラウド事業者の所管範囲について期待値の調整をすることは、クラウドベースのリソースに対するインシデント対応の最も重要な要素である。役割や責任の明確な相互理解と、対応や連携の演習は非常に重要である。
- クラウド利用者は、インシデント発生時に利用できるクラウド事業者との適切なコミュニケーションラインを設定しておく必要がある。既存のオープンスタンダードを活用すれば、インシデント時のコミュニケーションを容易にすることができる。
- クラウド利用者は、クラウド事業者が分析目的で提供するデータの内容とフォーマットを理解し、利用可能なフォレンジックデータが法的な証拠保全の連続性の要件を満たすかどうかを評価する必要がある。
- クラウド利用者は、従来のデータセンタよりも早期に潜在的な問題を検知するために、クラウドベースのリソースを、継続的かつサーバレスで監視する必要がある。
    - データソースは、インシデント時に可用性を維持できる場所に格納し、またはコピーすること。
    - 必要かつ可能であれば、データソースはまた、適切な証拠保全の連続性を維持できるように取り扱うこと。
- クラウドベースのアプリケーションは、自動化と統合管理を活用して、封じ込めと復旧を含むインシデントレスポンスを効率化し、高速化する必要がある。
- 利用するクラウドサービス事業者ごとに、その事業者でホストされているリソースに関して、インシデントの検知および処理の方法を計画し、企業全体のインシデント対応計画に記述する必要がある。
- 各クラウドサービス事業者の SLA は、企業全体のインシデント対応計画の効果的な実行に必要な、インシデント処理のサポートを保証する必要がある。 これは、インシデント処理プロセスの各段階（検知、分析、封じ込め、根絶、および復旧）をカバーする必要がある。
- テストは、少なくとも年に 1 回、またはアプリケーションアーキテクチャに大きな変更があるたびに実行すること。クラウド利用者は、クラウド事業者（および他のパートナー）のテスト手順を可能な限り最大限、自社のテスト手順に統合するよう努めること。

DOMAIN 10
アプリケーションセキュリティ



10.0　はじめに

アプリケーションセキュリティは、信じられないくらい複雑で広範な知識体系を必要とする：初期段階の設計と脅威モデリングから、実利用アプリケーションの保守と防衛までのすべてを包含する。アプリケーションセキュリティはまた、アプリケーション開発手法が進化し続け、新しいプロセス、パターン、技術を取り込み続けるために、信じがたいほど速いペースで進化する。クラウドコンピューティングはこれらの進化を促進する最大の要因の 1 つであり、その結果、アプリケーションセキュリティのレベルを進化させるという圧力として表れる。その目指すところはそのような進化が可能な限り安全であることである。

このガイダンスにおけるこのドメインは、特に PaaS と IaaS のクラウドコンピューティング環境において、アプリケーションをセキュアに開発し配備しようと考えているソフトウェア開発と IT のチームを対象としている。(このドメインで取り上げる多くの手法はセキュアな SaaS アプリケーションを支えることにも利用できる。) このドメインでは特に以下のことに焦点を当てる。

- クラウドコンピューティングにおけるアプリケーションセキュリティにはどのような違いがあるか。
- セキュアなソフトウェア開発の基礎の見直しとそれがクラウドにおいてはどう変化するのか。
- よりセキュアなクラウドアプリケーションのためにクラウドの機能をどう活用するか。

ありうる全ての開発と配備の方法を盛り込むことはできない－直接クラウドコンピューティングに関連するものに限ったとしても。従って、開発と配備の状況の主なものに関するセキュリティを指南するのに役立つ主たる領域に焦点をあてることとする。このドメインではまた、DevOps におけるセキュリティの基礎についても述べる。DevOps はクラウドベースのアプリケーション開発における主流の手法として急速に広まっている。

アプリケーションに対し、クラウドコンピューティングは多くの場合セキュリティ上の恩恵をもたらす。一方で、クラウド技術の多くの領域と同様に、クラウド内で利用するように設計されていない既存の手法、プロセス、技術に対しても、それに見合う変化を要求する。このような利点と課題の主なものは以下のようになる：

利点

- **より高いレベルのベースラインセキュリティ**　クラウド事業者、特に主要な IaaS および PaaS の事業者には、他のほとんどの組織に比べ、より高いレベルのベースラインセキュリティを維持する大きな経済的インセンティブがある。クラウド環境では、ベースラインセキュリティで深刻な違反が生じると、パブリッククラウド事業者がその顧客ベースとの関係を維持する上で必須の信頼を根本から覆してしまう。
  クラウド事業者はまた、より広い範囲のセキュリティ要件にも対応して、法規制や産業ごとの基本遵守

事項を満たすことで、それら業界の顧客の満足を得る必要がある。これらの事柄はクラウド事業者にとって強い原動力となり、極めて高いレベルのセキュリティを維持している。

- **高い適応性**　API と自動化により、これまでのインフラストラクチャに比べ、高い柔軟性をもって、適応力の高いセキュティプログラムを低コストで構築できる。例えば、Firewall でのルールの変更や、更新されたコードを搭載した新しいサーバの配備を、少数の API コールや自動化機能によって実施することができる。
- **環境間の分離**　クラウドアプリケーションはまた、仮想ネットワークその他のインフラストラクチャ（PaaS も含む）を活用して、高度に相互分離された環境を提供する。例えば、複数のアプリケーションスタックを完全に別々の仮想ネットワークに配備することで、攻撃者が乗っ取ったアプリケーションを利用して境界防御ファイアウォールの内側にある他のアプリケーションを攻撃する可能性を、追加コストをかけずに排除できる。
- **独立した仮想マシン**　セキュリティはマイクロサービスアーキテクチャを用いることにより格段に強化される。クラウドは利用者が物理サーバの利用を最適化するよう求めたりしない。複数のアプリケーションコンポーネントやサービスを一つのシステム上に配備しようとすることはしばしば起こるが、開発者はそのようなことをせずに、多くの小さな仮想マシンを配備して各々に機能やサービスを割り当てることができる。このことは各々の仮想マシンにおける攻撃対象面を小さくし、より精細なセキュリティ対策を可能にする。
- **拡張性**　拡張性(elasticity)は固定した規模のインフラストラクチャをより拡大して使うことを可能にする。オートスケール(auto-scale)グループのような拡張性ツールを使うと、各本番システムはベースラインのイメージに基づいて動的に起動され、人の手を介さずに自動的に資源の再割り当てが行われる。その結果、運用の中心となる要件は、アドミニストレータがシステムにログインして変更を加えることを絶対に許可してはいけないということである。なぜならばそのような変更は通常の自動スケーリング作業過程で失われるからである。このことにより、リモート管理が完全に遮断された状態での変更無用な(immutable)サーバの利用を可能にしている。変更無用なサーバとインフラストラクチャについてはドメイン 7 で詳述している。
- **DevOps**　DevOps は、アプリケーションの開発と配備を自動化することにフォーカスした、アプリケーション開発の新しい方法論であり考え方である。DevOps はセキュリティにとって多くの利点をもたらしており、コード堅牢化、変更管理、本番アプリケーションのセキュリティを改善するだけでなくセキュリティ運用全般をも強化してくれる。
- **ユニファイドインターフェイス**　インフラストラクチャとアプリケーションサービス(PaaS 利用の場合)向けのユニファイドインターフェイス（管理インターフェイスと API）は、別々のグループに管理されることが多い従来式の個別のシステムやデバイス（ロードバランサ、サーバ、ネットワーク機器、ファイアウォール、ACL 等々）に比べると、より包括的な可視化情報とより優れた管理を可能とする。その結果、意思疎通の不備や全体像を見渡すことができないことに起因するセキュリティ上の問題を少なくする可能性をもたらす。

課題

- **細部の可視化の限界**　（クラウドにおいては）モニタリングとロギングが可視化できるかと入手可能かについては影響があり、セキュリティに関するデータを収集するには別のアプローチが必要となる。このことは特に PaaS に当てはまり、一般的に入手可能なログ、例えばネットワークログは、クラウド利用者にはアクセスできないことが多い。
- **アプリケーション情報への接点の拡大**　管理用ダッシュボードやメタストラクチャのセキュリティは、そのクラウドアカウントに紐づいているアプリケーションのセキュリティに直接影響を与える。開発者と運用側は、常に別々のチームとしてアクセスするのでなく、両方とも同じ管理用ダッシュボードにアクセスすることになる可能性が高い。管理用ダッシュボードではデータや機微な情報がオープンになる可能性がある。更に、特に PaaS に関連するところでは、最近のクラウドアプリケーションは、様々な自動化された機能を発動するのに、管理用ダッシュボードに接続することが多い。これらの理由から、管理用ダッシュボードのセキュ

リティは今日ではアプリケーションセキュリティの一部となっており、いずれかの破綻が他の破綻におよぶ可能性がある。

- **脅威モデルの変化**　クラウド事業者を利用することやセキュリティ共有モデルは脅威モデルや運用計画、インシデント対応計画に取り入れることが必要である。脅威モデルはまた、クラウド事業者もしくは利用するプラットフォームの技術的相違点を反映するように適合させなければならない。
- **透明性の制約**　アプリケーションの中で何が起きているかについては、特にそれが外部サービスと組み合わされている場合は、透明性が落ちる可能性が強い。例えば、自組織のアプリケーションに組み込まれた外部の PaaS サービスについてセキュリティコントロールを完全に把握することはめったに起こらない。

総じて言うと、セキュリティを共有するモデルの結果、アプリケーションセキュリティは変更を余儀なくされるだろう。一部はガバナンスと運用に直接結びついたものであるが、アプリケーションのセキュリティについて構想し計画するに際して、さらに多くの変更が必要となる。

10.1　概要

アプリケーションセキュリティは広範なものであり、効果的なアプリケーションセキュリティプログラムに必要な様々なスキルセットや役割に鑑みて、このドメインは以下の主要な領域に分けて記述する。

- **セキュアソフトウェア開発ライフサイクル:** 設計から開発に至るまで、クラウドコンピューティングがアプリケーションセキュリティにどのように影響を与えるか。
- **設計とアーキテクチャ:** セキュリティに影響を及ぼし、更には改善をもたらす、クラウドコンピューティング向けアプリケーション開発のトレンド
- **DevOps と Continuous Integration/Continuous Deployment (CI/CD)**: DevOps と CI/CD はクラウドアプリケーションの開発と配備の両方においてたいへんよく使われ、急速に主流のモデルになりつつある。これらの方式はセキュリティに関する新しい視点をもたらすとともに、ここでも、ウォーターフォールのようなより人手に頼る開発・配備パターンに比べてセキュリティを改善する機会ももたらす。

10.1.1　セキュアソフトウェア開発ライフサイクルとクラウドコンピューティング

セキュアソフトウェア開発ライフサイクル(SSDLC)は、アプリケーションの開発から配備、運用に至る全ての過程を通じた一連のセキュリティに関する取組みについて記述している。ソフトウェア業界ではいくつかのフレームワークが使われており、以下のようなものがある。

- マイクロソフト社の Security Development Lifecycle
- NIST 800-64
- ISO/IEC 27034
- OWASP や様々なアプリケーションセキュリティベンダを含む他の組織の出している独自のライフサイクルやセキュリティに関する取組みガイダンス

フレームワークの広がりや用語の違いがあるので、クラウドセキュリティアライアンスではそれらをより大きな「メタフェーズ」に分解し、フレームワークごとの取組みをより標準化された組合せとして記述できるようにする。これは公式の手法に取って代わることを意図する訳ではなく、組織が標準化に用いるライフサイクルとは無関係に、

主たるアクティビティを定義するのに利用できる記述モデルを提供するにすぎない。

- **セキュアな設計と開発:**組織全体にまたがる標準の教育と開発から実際にコードを書き、テストするまでの範囲
- **セキュアな配備:**コードを隔離された開発環境から本番環境に移す際のセキュリティと試験のための作業
- **セキュアな運用:** 本番アプリケーションのセキュリティの維持と保守。WAF(Web Application Firewall)などの対外防御と、継続的脆弱性評価を含む。

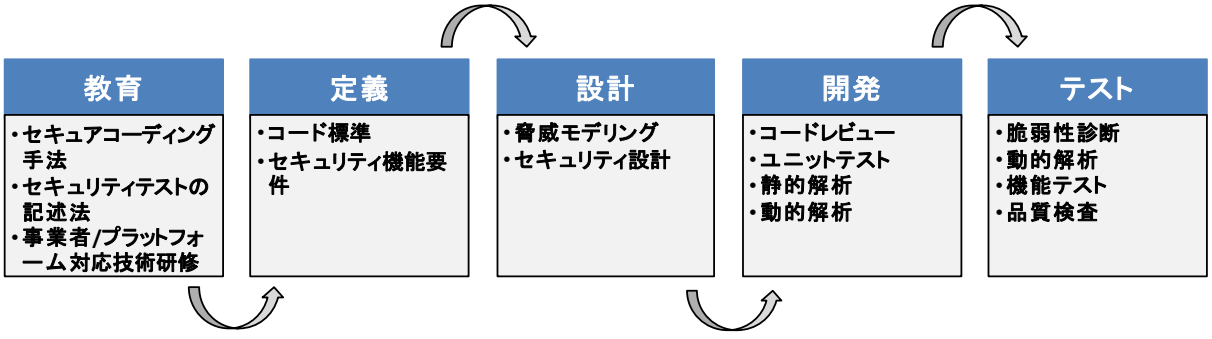
クラウドコンピューティングは、SSDLC の種類とは関係なく、SSDLC の全ての過程に影響する。これは、(パブリッククラウドにおける)外部の事業者により多く依存することと相まって、クラウドコンピューティングにおける抽象化と自動化の直接の結果である。特に以下のようなことがあげられる。

- 責任共有モデルが意味するところは、セキュリティのある面について常にクラウド事業者に依存しているということであり、それは IaaS ベースのむき出しのアプリケーションにおいてもである。PaaS や事業者固有の機能を用いる度合いが強いほど、セキュリティ責任の分散は大きくなる。このことはロードバランサの利用の場合最も単純明快であろう。クラウド事業者はロードバランサをセキュアに維持する責任を全面的に負うが、それを適切に設定し使用するのはクラウド利用者の責任である。
- このガイダンスのほぼ全てのドメインで述べられている通り、可視性やコントロールに関して大きな変化が生じる。IaaS 上でほとんどのものを走らせている場合はネットワークログが手に入らないだけだが、PaaS に移行したときにはサーバやサービスのログを失うことを意味する。このようなことはクラウド事業者や技術によってすべて異なる。
- クラウド事業者が違えば、その機能、サービス、セキュリティに関する能力は異なり、このことは全体のアプリケーションセキュリティの計画に際して考慮に入れなければならない。
- 管理用ダッシュボードとメタストラクチャは今やアプリケーションセキュリティの視点でとらえるべきかも知れず、特にアプリケーションのコンポーネントが直接クラウドサービスとやり取りする場合にはそうである。
- 新しい様々なアーキテクチャのオプションがある。特にやはり PaaS サービスを利用する場合には。
- DevOps の隆盛とその影響。本ドメインで以下に触れる。

10.1.2 セキュアな設計と開発

セキュアなアプリケーションの設計と開発には 5 つのステップがあり、その全てにクラウドコンピューティングが影響する。

教育： 3 つの別々の役割が 2 種類の教育を必要とする。開発、運用、セキュリティの各役割はすべて、クラ



セキュアアプリケーション設計開発ステップ

ウドセキュリティ基礎（事業者固有のものでない）についての追加教育と、プロジェクトで使われる特定のクラウド事業者とプラットフォームに対応した適切なセキュリティ教育を受けなければならない。クラウドインフラストラクチャのアーキテクチャ構築と運用には、一般的に開発と運用の関与はより大きくなる。従って、利用予定のツールに固有のベースラインセキュリティの教育は重要である。

定義： クラウド利用者はクラウド事業者、セキュリティ基準、他の要求条件に対応したアーキテクチャまたは機能・ツールを承認し決定する。これらはコンプライアンス要件や、例えば何処のクラウドサービスでどのデータが使えるかのリスト(規模の大きな事業者の場合はどのサービスかを含む)と密接に繋がっている。時にプロジェクトのより後の段階で決まることもあるが、配備プロセスもこの段階で定義するべきである。セキュリティ基準には、クラウド事業者内の誰がどのサービスを管理できるかについての初期の権限付与を含んでいなくてはならない。これは多くの場合、実際のアプリケーションアーキテクチャとは無関係に決められる。そこには事前に使用の許されているツール類、技術、設定や更には設計パターンも含まれているべきである。

設計： アプリケーションの設計過程では、PaaS が関係する場合は特に、クラウド内のセキュティについては、アーキテクチャ、クラウド事業者の持つベースラインの機能、クラウド事業者の特性、配備や運用におけるセキュリティの自動化や管理機能に焦点を置く。アプリケーションアーキテクチャにセキュリティを組み込むに際して、クラウド事業者自身のセキュリティ機能を活用できる可能性があることから、際だったセキュリティ上のメリットが得られることがあることが確認されている。例えばサーバレスのロードバランサやメッセージキューの機能を付加することで、特定のネットワーク攻撃のルートを完全に封じることができる。この場合には脅威モデリングをする必要がある。なぜならばそれはクラウド事業者とプラットフォームごとに個別だからである。

開発： ネットワークやサービスその他の設定を可能とするために、開発者は開発環境にクラウド管理用ダッシュボードへの管理者権限でのアクセス権を設定する必要がある。これは絶対に本番環境であってはならないし本番データを扱ってはならない。開発者はまた CI/CD パイプラインを活用する場合があるが、そのセキュリティを、特にコードのリポジトリに関しては確保しなければならない。もし PaaS を利用するならば、開発者はネットワークやシステム、サービスログの如何なる欠落に対しても可能な限りカバーできるように、アプリケーションにロギング機能を組み込まなければならない。

テスト：セキュリティのテストは配備プロセスやパイプラインに組み込まれていなくてはならない。テスト段階は配備プロセス・パイプラインと「セキュア配備」段階にまたがって行われる傾向にあるが、セキュリティのユニットテスト、セキュリティ機能テスト、静的アプリケーションセキュリティテスト(SAST) 、動的アプリケーションセキュリティテスト(DAST)などの手法が好んで用いられる。この重複（訳注：テストと配備）の関係で、クラウドに関する考慮事項は次の節でより詳しく取り扱う。

組織はクラウド内での自動診断もより活用するべきである。インフラストラクチャは、それ自身がテンプレートや自動化を通じて定義され実装されている関係上、コード化されたインフラ（infrastructure as code）となっており、アプリケーションテストの領域でとらえられている。セキュリティテストの一環として、より深いセキュリティ検証が必要な、認証や暗号化コードのようなセキュリティに深く関わる機能のために、セキュリティフラギングの機能を要求することを検討すべきである。

10.1.3　セキュアな配備

配備の自動化はクラウド環境で特に顕著な機能であることから、「設計開発」段階でも組み込まれるような、セキュリティに関するいくつかの作業を含むことがしばしばある。セキュリティテストの自動化は非常にしばしば配備パイプラインに組み込まれ開発者の管理外で実行される。これは本質的に、また自然に、オンプレミスの開発努力に別れを告げるものであるが、テスト自体はまた、クラウドコンピューティングに適合したものになる必要がある。

アプリケーションセキュリティのテストには数多くの種類があり、（クラウド上の）開発と配備に組み込める可能性がある。

コードのレビュー： 必ずしも自動診断に組み込む必要のない、手動の作業であるが、CI/CD パイプラインでは手作業のゲートとして実施させられるかもしれない。（コードの）レビュー自体は必ずしもクラウド向けに変更する必要はないが、追加で注意すべきいくつかの領域がある。アプリケーションの管理用ダッシュボードとの通信（例えばクラウドサービスへの API コール。一部はインフラストラクチャの変更を伴うことがある）はすべて、特にプロジェクトの早い段階で精査されるべきである。コード自体の検証の他に、セキュリティチームはアプリケーションの管理用ダッシュボードとの通信に対して最小特権の付与にとどめるように注意し、さらにそれを管理用ダッシュボードの設定で確認するという方法も可能だ。認証や暗号化に関連するあらゆることは追加レビューにおける重要事項である。しかる後に配備プロセスは自動化され、これらのコードに変更があればセキュリティ担当者に通知が行くようにする。その変更は人手による承認か、変更後のレビューの対象となる。

ユニットテスト、回帰テスト、機能テスト： これらは開発者が通常のプロセスで用いる標準的なテストである。セキュリティテストはこれらのテストに組み込むことができ、またそうすべきであり、それにより、アプリケーション内のセキュリティ機能が想定通りに動作し続けることを確認できる。これらのテストそれ自体は、すべての API コールを含め、クラウド上で走ることを確実にするためにアップデートする必要があるだろう。

静的アプリケーションセキュリティテスト(SAST: Static Application Security Testing)： 一般の一通りのテストに加え、SAST はクラウドサービスへの API コールに対するチェックも組み込むべきである。SAST はまた、API コールの中にハードコードされた認証情報のチェックも行うべきである。これは深刻化しつつある問題である。

動的アプリケーションセキュリティ診断(DAST: Dynamic Application Security Testing)： DAST はアプリケーションを動作状態で診断すると共に、Web の脆弱性診断やファジング診断のような診断も包含している。クラウド事業者とのサービス条項により、DAST は実施に制約があったり、クラウド事業者から事前の許可を得なければならない場合があったりする。クラウドや自動配備パイプラインを利用することで、“infrastructure as code”を用いて完璧に機能する診断環境を立ち上げることができ、本番環境への変更を承認する前に詳細な分析を実行することができる。

10.1.3.1 脆弱性診断への影響

脆弱性診断は CI/CD パイプラインに組み込んでクラウド上に極めて容易に実装できるが、ほとんど全ての場合、クラウド事業者のサービス条項の遵守が求められる。

よく目にする 2 つのパターンがある。第一は、顧客がそのために設定するクラウド内の特設テスト領域(仮想ネットワークで区切られたセグメント)内で、パイプラインの一部であるイメージやコンテナに対してフルの診断を行うことである。このイメージはテストに合格した場合のみ本番環境に配備することが許可される。似たようなパターンでは、”infrastructure as code”を用いてテスト環境を構築し、インフラストラクチャの全体をテストしている。

どちらの場合も本番環境のテストはわずかであるか全く行われない。なぜなら本番環境は不可変(immutable)でありテスト環境と完全に一致していなければならない（両方とも同一の定義ファイルに基づいている）からである。組織はまた、ホストベースの脆弱性診断ツールを利用することができる。このツールは仮想マシン上でローカルに動作し、従ってクラウド事業者と協調したりその許可を取ったりする必要がない。

10.1.3.2 侵入検査への影響

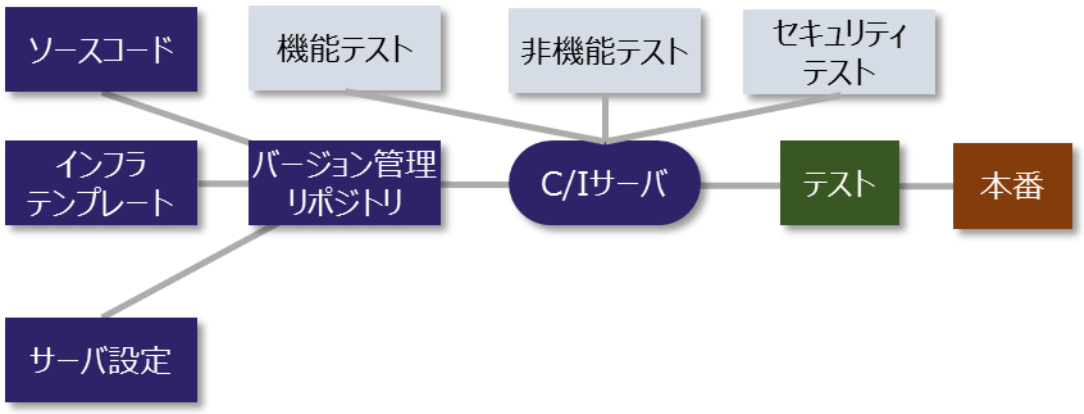
脆弱性診断の場合と同じく、侵入検査もクラウドサービス事業者の許可なしに実施するにはほぼ間違いなく制約がある。CSA では以下のガイドラインに沿って侵入検査を実施するよう推奨している。

- アプリケーションが配備されているクラウド事業者に対して実績のあるテスト業者を利用する。
- 開発者とクラウドサービス管理者を検査に関与させる。クラウドへの侵入の多くはクラウドを管理する側を攻撃しており、クラウド上のアプリケーションそのものに対してではない。攻撃対象にはクラウドの管理用ダッシュボードも含まれる。
- アプリケーションがマルチテナント向けの場合、侵入検査業者にはテナントとしてのアクセスを許可し、テナント間の隔離を破って、そのアクセスを他のテナントの環境やデータに侵入するのに利用できるか確かめること。

10.1.3.3 配備パイプラインのセキュリティ

CI/CD パイプラインは、(希に手作業での本番環境への変更があるが)変更無用型(immutable)インフラストラクチャのサポートや、自動化されたセキュリティテスト、さらにはパイプライン経由のアプリケーションやインフラの変更に関する、広範なログ取得のサポートにより、セキュリティを強化している。正しく設定されていれば、ログは、全てのコード、インフラストラクチャ、設定の変更をトレースし、誰が変更を申請し、誰が許可したかの情報と結び付け、さらにテストの結果も残すことができる。

パイプライン自体は厳密にセキュリティを確保されなければならない。アクセスが極めて限定された専用のクラウド環境、またはパイプラインのコンポーネントをホストしているインフラストラクチャで、パイプラインをホストすることを検討すべきである。



Continuous Deployment パイプライン

10.1.3.4 ”Infrastructure as Code”と不可変性(immutable)による影響

様々なところで”Infrastructure as Code”について述べている。仮想化とソフトウェアでの定義がクラウドの特性のため、環境全体をテンプレートを使って定義することが容易にでき、テンプレートはツール(プロバイダによるものも第三者によるものも)によりAPIコールに変換可能で、APIコールは自動的に環境を構築する。身近な例はテンプレートからサーバ設定を構築することである。より複雑な実装ではクラウドアプリケーションのスタックを丸々構築することができ、更にネットワークの設定や認証管理まで生み出せる

これらの環境はソースファイルの組合せから自動的に構築でき、従ってそれは不可変(immutable)である。

システムまたは環境がテンプレート（可能性としては CI/CD パイプライン）から自動的に構築できるとしたら、すべての本番環境に対する変更はその次のコードもしくはテンプレートの変更により上書きされる。本番環境はかくして非クラウドにおけるアプリケーション配備（インフラストラクチャの多くは仕様に従って主導で設定される）で通常できるよりずっと堅固に固定できる。セキュリティチームが適切に関与している場合には、“Infrastructure as Code”と不可変(immutable)の配備を利用することで、セキュリティは格段に改善される。

10.1.4 セキュアな運用

アプリケーションが本番環境に配備された後も、セキュリティチームの活動は継続する。この活動の多くは本ガイダンスの他のドメイン、特にドメイン 7(インフォストラクチャ)、ドメイン 8(コンテナ)、ドメイン 11(データ)、ドメイン 12(アイデンティティ・アクセス管理)で取り扱っている。この節ではより直接アプリケーションに適用される、その他のガイダンスを提供する。それは以下の通り：

- 本番環境の管理用ダッシュボードは、開発環境用に比べ、格段に堅固に固定されるべきである。先に言及したとおり、ホスティングされている環境の管理用ダッシュボードに直接アプリケーションがアクセスする場合は、それに与えられる特権は必要最小限に絞り込まれるべきである。アプリケーションサービスごとに複数の資格情報のセットを用意して、権限付与の細分化を行うべきである。
- 不可変(immutable)のインフラストラクチャを利用する場合でも、本番環境は許可されたベースラインからの変更や逸脱に対して能動的に監視すべきである。これは、コードまたはツールにより自動化が可能でありまたそうすべきである。そのコードやツールはクラウドへの API コールを発行して設定状態を常時チェックする。

幾つかのクラウドプラットフォーム上では、ビルトインされた評価機能および設定管理機能を利用できる場合がある。そのような機能はまた、プラットフォームまたは変更の属性次第で、許可を得ていない変更を自動的に修復することができる場合がある。例えば、セキュリティチームに承認されていないファイアウォールのルールの変更に対してはコードは自動的に元に戻される。

- 配備後であっても、また不可変(immutable)なインフラストラクチャであっても、アプリケーションのテストや評価の継続的実施を怠ってはならない。パブリッククラウドの場合には、サービス条項違反を回避するためにクラウド事業者と調整しまたはその許可を取る必要があるであろう。それはその他のあらゆる脆弱性検査と同様である。
- 変更管理はアプリケーションだけではなく、すべてのインフラストラクチャとクラウドの管理用ダッシュボードも対象となる。

インシデントレスポンスに関する情報はドメイン 9 を参照のこと。事業継続と管理用ダッシュボードのセキュリティについてはドメイン 6 を参照のこと。

10.1.5 クラウドのアプリケーション設計とアーキテクチャへの影響

クラウドの持つ性質そのものが、すでにして、アプリケーションの設計やアーキテクチャ、パターンの選好に変化をもたらしている。そのような変化の中には、セキュリティに直接作用しないものもあるが、以下のようなトレンドは一般的なセキュリティ上の問題を減らす契機になっている。

- **隔離が最初から備わっていること：** アプリケーションをそれ用の隔離されたクラウド環境で走らせることは簡単である。クラウド事業者如何で異なるが、その仕組みは専用の仮想ネットワークであるか、またはアカウントもしくはサブアカウントである場合がある。アカウントやサブアカウントの構造は、管理用ダッシュボードを分離できるというメリットをもたらす。利用組織は開発用のアカウントでは権限を広く設定する一方で、本番用アカウントでは厳しく制限された実行ができる。
- **不可変(immutable)なインフラストラクチャ：** 既に述べた通り、不可変(immutable)なインフラストラクチャは、クラウドの運用上の理由から、どんどん一般的になりつつある。セキュリティチームはこういったメリットを活用して、不可変(immutable)のサーバ／コンテナへのリモートログインを不能とすること、ファイルの完全性のモニタリング、インシデント復旧計画に不可変(immutable)技術を取り入れること、ができる。
- **マイクロサービス利用の拡大：** クラウドコンピューティングでは、異なるサービスを各々異なるサーバ（あるいはコンテナ）に分離することは容易である。なぜならば、一つには、物理サーバの利用率を最大化する必要が無いからであり、また一つには、伸縮自動化（オートスケール）チームが、たとえワークロード処理に小型コンピュータノードを連結して使っている場合でも、アプリケーションの拡張性を担保してくれるからである。各ノードの処理能力は限られているので、ノードをロックしてその上で走るサービスを最小化することは簡単にできる。このことは、各ワークロードのセキュリティを（適切に利用されている限り）改善する一方で、全マイクロサービス間の通信をセキュアにすることや、サービスの認知、スケジューリング、ルーティングの設定がセキュアにできていることを確実にする上で、多少負荷がかかる。
- **PaaS と「サーバレス」アーキテクチャ：** PaaS や(下位のサービスや OS の管理不要なクラウド事業者のプラットフォーム上で直接ワークロードを動かす)「サーバレス」のセットアップは、攻撃される要素(attack surface)を劇的に削減する大きな可能性を秘めている。ただしこれは、クラウド事業者がプラットフォームとサーバレスのセットアップに責任を持ち、利用者の要件を満たす場合のみである。

サーバレスは幾つかの利点をもたらす。第一に、クラウド事業者にとって、極めて高いセキュリティレベルを維持し、それを最新のものに保つことに対する経済的誘因である。これにより、クラウド利用者は環境のセキュリティを日々維持する責務から解き放たれる。ただし、クラウド利用者の最終的説明責任を取り除くものでは決してない。信頼できるクラウド事業者と付き合い、確たる証跡を確保することが大事である。

次に、サーバレスのプラットフォームはクラウド事業者のネットワーク上で走る場合があり、クラウド利用者のコンポーネントとは API または HTTPS プロトコルで通信する。このことにより、たとえ攻撃者がサーバやコンテナを乗っ取ったとしても直接ネットワーク攻撃するパスを除去する。攻撃者にできることは API コールや HTTPS 通信を試みることに限られ、ポートスキャンも、他のサーバの発見も、その他の一般的手法を使うこともできない。

- **Software-defined security：** セキュリティチームは同じツールと技術を様々なセキュリティ対策作業の自動化に活用することができる。それら（訳注：自動化されたセキュリティ対策作業）をアプリケーションスタックに組み入れることさえも可能である。例としては、インシデント対応の自動化、権限付与の動的な変更、承認されていないインフラストラクチャの変更の修復があげられる。
- **イベント駆動型セキュリティ(Event driven security)：** 一部のクラウド事業者はイベント駆動型のコード実行をサポートしている。その場合、管理用ダッシュボードが様々な動きを検知する。例えば、特定のオブジェクトストレージの所在場所にファイルがアップロードされることや、ネットワーク管理またはアイデンティティ管理の設定変更がある。これらは同時に通知メッセージングまたはサーバレス環境にホストされたコード経由で、コード実行にトリガーをかける。セキュリティチームはセキュリティ対策作業対象となるイベントを定義し、自動化された通知、評価、修復、その他のセキュリティ処理を発動するのに、イベント駆動型の機能を利用することができる。

10.1.6　クラウド事業者が考慮すべきその他の事項

クラウド事業者は、いかなるサービスモデルであれ、セキュリティ問題があった場合にクラウド利用者に著しい障害をもたらす可能性のある、アプリケーションサービスのいくつかの面について、特別な注意を払う必要がある。例えば：

- API と Web サービスは特に入念に堅牢化し、認証を受けたのと受けないのと両方の攻撃者からの攻撃を想定しておくこと。それには API 向けに特別に設計された業界標準の認証手段を利用することも含まれる。
- API の不正利用や異常な動作を監視すること。
- API と Web サービスは特に入念に設計とテストを行い、攻撃やテナント間の不正なまたは偶発的なアクセスを防ぐようにしなければならない。

10.1.7 DevOps の隆盛とその役割

DevOps とは、開発チームと運用チームの間の協力とコミュニケーションを改善してより深く結びつけることを意味し、特にアプリケーション配備とインフラストラクチャ運用の自動化に焦点を当てている。幾つかの定義があるものの、全体的にその概念は文化、考え方、プロセス、ツールから成り立っている。

その核となるのは、CI/CD を配備自動化パイプラインによって組み合わせることと、インフラストラクチャ管理をうまく行うためのプログラム式自動化ツールを利用することである。DevOps はクラウドに限定的な手法ではないが、上述のようにクラウドに非常に適合しており、クラウドアプリケーションの配備モデルとして支配的位置に就きつつある。

10.1.7.1 セキュティへの波及効果とその長所

- **標準化：** DevOps では、本番に組み込まれるものはすべて、承認済みのコードと設定用テンプレートに基づき、CI/CD パイプラインによって生み出される。開発、テスト、本番（のコード）はすべて完全に同一のソースファイルから派生しており、周知となっている優れた標準からの逸脱を防いでいる。
- **自動化されたテスト： 上**述の通り、広範な種類のセキュリティテストは、必要に応じて補助的に手動テストを加えることで、CI/CD パイプラインに組み込むことが可能である。
- **不可変性(immutable)：** CI/CD パイプラインは、素早く確実に、仮想マシンやコンテナ、インフラストラクチャスタックのマスターイメージを生成する。これにより配備の自動化と不可変(immutable)なインフラストラクチャを実現する。
- **監査と変更管理の改善：** CI/CD パイプラインはソースファイルにある 1 文字の変更に至るまでの全てを追跡調査できる。その変更は変更を行った人物と紐づけられる。バージョン管理リポジトリに格納されたアプリケーションスタック（インフラストラクチャを含む）の全履歴と共に。このことは監査と変更管理に著しいメリットをもたらす。
- **SecDevOps/DevSecOps と Rugged DevOps：** これら 2 つの用語は新たに登場してきた言葉で、DevOps へのセキュリティ作業の組入れのことを指している。 SecDevOps/DevSecOps はセキュリティ運用を改善するために DevOps の自動化技術を使うということを意味する場合がある。Rugged DevOps はアプリケーション開発過程にセキュリティテスティングを組み入れることを意味し、より強固で、よりセキュアで、より障害耐性の高いアプリケーションを生み出すものである。

10.2　推奨事項

- 利用しているクラウド事業者の持つセキュリティに関する能力を把握すること。ベースラインのセキュリティだけでなく、複数のプラットフォームとサービスの全般にわたって把握すること。
- 初期設計のプロセスにセキュリティを組み込むこと。クラウド上の配備は多くの場合未経験の領域であり、早い段階でセキュリティチームを関わらせる場は広がっている。
- 形式の整った SDLC を導入できていないときは、CD に移行して配備パイプラインにセキュリティの自動化を組み入れることを検討すること。
- 脅威モデリング、SAST、DAST(ファジングを含む)は全て取り入れるべきである。テストはクラウド環境で機能するように設定しなければならない。しかし同時に、クラウドプラットフォームに固有の懸念事項、例えば API 資格情報の保存状態などをテストできる設定もしなければならない。
- 新しくクラウド内で遭遇するアーキテクチャの選択肢や要求条件を理解すること。それらをサポートするべく、自組織のセキュリティポリシーとセキュリティ基準を改定すること。決して単純に従来の基準を全く新しいコンピューティングモデルに強制的にはめ込むようなことはしないこと。
- 配備プロセスにセキュリティテストを組み込むこと。
- セキュリティコントロールを自動化するために、Software Defined Security を活用すること。
- 可能なら、イベント駆動型セキュリティを活用し、セキュリティ事案に対する検知と修復の自動化を実現すること。
- 複数の異なるクラウド環境を利用し、管理用ダッシュボードへのアクセスの分離を改善すること。同時に、本番環境は固定しつつ、開発チームには必要な開発環境の設定を自由にさせること。

DOMAIN 11

データセキュリティと暗号化

11.0　はじめに

データセキュリティは情報およびデータのガバナンスを実現するための鍵となるツールである。クラウドセキュリティの他のすべての領域と同様に、その適用はリスクベースであるべきである。なぜならば、全てのものを同等にセキュアにするという考え方は適当でないから。

このことは、クラウドが関係するかしないかに関わらず、データセキュリティ一般に当てはまる。しかしながら、多くの組織では、その膨大な量の機微なデータを－たとえ全部ではないにせよ－第三者に預託する、あるいは共有のリソースの中に自組織のデータを混在させる、ということに慣れていない。その結果、「クラウドにあるすべて」に対して本能的に一律的なセキュリティポリシーを適用しがちであり、セキュリティ度が著しく高く、コスト効率もよいリスクベースアプローチは取られないことになる。

例えば、プロバイダを信用できないので SaaS の中をすべて暗号化する。それは結局、最初からそのプロバイダを使うべきでないということだ。しかし、全てを暗号化することは、全てを満たすことにはならず、却ってセキュリティに対して誤った理解につながりかねない。例えば、デバイスのセキュリティの確認を怠ったままトラフィックを暗号化するといったように。

ある意味で、情報セキュリティはデータセキュリティである。しかしこのドメインの目指す処としては、データそのもののセキュリティに関わる管理策に焦点を当てる。そのために最も重要なのが暗号化である。

11.1　概要

11.1.1　データセキュリティのための管理策

データセキュリティの管理策は概ね 3 つの領域に分類できる。このセクションではそのすべてについて見る。

- クラウドに持って行くデータ（およびその所在場所）に対する管理
- クラウド上にあるデータの保護と管理。鍵となるコントロールと手順は：
    - アクセスコントロール
    - 暗号化
    - アーキテクチャ
    - 監視と警報（対象は利用、設定、ライフサイクル上のステージなど）

- 追加的コントロール。利用するプロバイダの特定の製品／サービス／プラットフォームに対応したもの。DLP、ERM(Enterprise Rights Management)などを含む。
- 情報ライフサイクル管理に対応したセキュリティの適用
  - データの存在場所／収容場所の管理
  - コンプライアンスの確保。監査のための事跡情報（ログ、設定）を含む。
  - バックアップと事業継続（ドメイン 6 参照）

11.1.2 クラウドにおけるデータストレージのタイプ

クラウドのストレージは仮想化されているので、従来型ストレージ技術で使われる以外の異なったストレージタイプがサポートされる傾向にある。仮想化のレイヤより下層では既知のデータストレージ機構が使われるであろうが、クラウド利用者がアクセスする対象であるクラウドストレージ仮想化技術は別のものである。ごく一般的にそれらは：

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システムに似ている。「オブジェクト」は典型的にはファイルであり、クラウドプラットフォームに特有のメカニズムを使って格納される。アクセスの殆どは API 経由で、標準的ファイル共有プロトコルではない。ただし、クラウド事業者はそういったプロトコルをサポートするためのフロントエンドインターフェイスを提供することがある。

ボリュームストレージ：これは本質としてはインスタンスまたはバーチャルマシン用の仮想ハードドライブである。

データベース：クラウドプラットフォーム、あるいはクラウド事業者は、異なる種類の様々なデータベースをサポートしている場合がある。既存の商用データベースやオープンソースのものから、事業者独自のシステムのものまである。独自仕様のデータベースは一般にその固有の API を用いる。それらはリレーショナルであったり、ノンリレーショナルであったりする。後者には NoSQL、その他のキーバリューストアシステム、あるいはファイルシステムベースのもの（例：HDFS）がある。

アプリケーション／プラットフォーム：この例としてはコンテントデリバリネットワーク(CDN)、SaaS に格納されたファイル、キャッシングや、その他の新しいタイプの選択肢がある。

ほとんどのクラウドプラットフォームはまた、冗長化した、耐久性のあるストレージメカニズムを持っている。それは多くの場合、データ分散（data dispersion）（あるいは data fragmentation または bit splitting とも呼ばれる）を利用している。このプロセスはデータの塊を取り出し、それを分解し、複数のコピーを別々の物理ストレージに格納することで高い耐久性を実現するものである。この方式でストアされたデータは、従って、物理的に分散している。ある一つのファイルが、単一のハードドライブに収まっているとは限らない。

11.1.3 クラウドへのデータの移行の管理

クラウド上にデータを保存する前に、ほとんどの組織は何らかの手段でどのデータがプライベート／パブリッククラウド事業者の中に収納されるのか管理する方法を模索する。このことは多くの場合、セキュリティのためよりコンプライアンス要件に不可欠なためである。

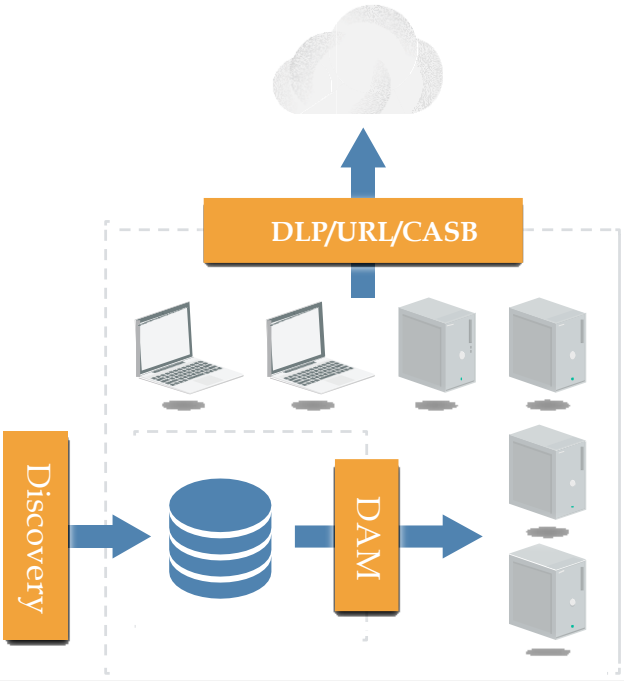
まずもって、どんなデータタイプをどの場所に置いてよいかのポリシーを定める。次にそれを自組織のベースラインとなるセキュリティ要件と紐づける。例えば、「PII (Personally Identifiable Information)は『y』暗号化

を施しアクセス制御要件を満たした上で『x』サービスに置くことができる」といったように。

次に自組織の主たるデータリポジトリを定める。大規模な移動や操作を、Database Activity Monitoring(DAM)や File Activity Monitoring(FAM)といったツールを用いて監視する。これは本質的には大規模なデータ移送に対する「早期警戒システム」を構築することを意味する。しかし同時に、あらゆる種類の深刻な違反や誤用の発生を検知するセキュリティコントロールとして重要な役割を果たす。

実際の移動を検知するにはクラウドの利用状況とあらゆるデータ移送をモニタする必要がある。これは以下のツールにより実現可能である：

CASB：Cloud Access and Security Brokers（またの名を Cloud Security Gateways）は様々な仕組みで内部のクラウド利用を検出する。例えばネットワークモニタリングを既存のネットワークゲートウェイやモニタリングツールと組み合わせたり、更にはDNSクエリをモニタリングすることによって。組織内のユーザがどのサービスに接続しているかを検知すると、この種の製品（サービス）の多くは、認定済みのサービスに対する操作を、API 接続（利用できる場合）やインライン割り込み（中間者モニタリング）によって監視する。サービスの多くはDLPその他のセキュリティ警告機能をサポートしており、更に機微なデータをクラウドサービス（SaaS/PaaS/IaaS）で利用する場合の高度な管理も提供している。



クラウドへのデータの移行の管理

URL Filtering：CASBほどしっかりした仕組みではないが、URL Filtering または Web gateway も組織内のユーザがどのサービスを利用している（もしくは利用しようとしている）か知らせてくれるのに役立つ。

DLP：Web へのトラフィック（および SSL 接続の中身）の監視には、DLP (Data Loss Prevention)ツールもデータのクラウドサービスへの移行を検出するのに役立つ。しかしクラウドの SDK や API の一部は、データやトラフィックの一部に DLP が解析できない暗号化を施すので、DLP はペイロードの中身を知ることができなくなる。

11.1.3.1 クラウドへのデータ転送のセキュリティ

クラウドにデータが移動するに際しては管理下のデータが保護されることを確実にしなければならない。そのためには、利用するクラウド事業者が提供するデータ移行メカニズムを理解する必要がある。なぜならば、事業者の仕組みを利用すると、多くの場合、SFTP (Secure File Transfer Protocol)のような「手動の」データ転送法式より安全でコスト効率が良いからである。例えば、API を通じて事業者のオブジェクトストレージにデータ送信すれば、同じ事業者内の仮想マシン上に自前の SFTP サーバを立てるより、はるかに信頼でき安全である。

クラウドプラットフォームが何をサポートしているか次第だが、転送中の暗号化にはいくつかの選択肢がある。一

つの方法はクラウドに送る前に暗号化（クライアントサイド暗号化）することである。ネットワーク暗号化（TLS/SFTP/その他）は別の選択肢である。ほとんどのクラウド事業者の API はデフォルトで TLS (Transport Layer Security)をサポートしている。そうでない場合は他の事業者を選ぶべきである。なぜならばこれは欠くべからざるセキュリティ機能であるから。プロキシベース暗号化は第三の選択肢で、その場合、暗号化プロキシをクラウド利用者とクラウド事業者の間の安全な領域に置き、プロキシがデータを事業者に送る前に暗号化することができる必要がある。

公開の、あるいは信頼できないデータを受け入れなければならない場合がある。取引相手や一般の相手から送られるデータを受け取る場合には、セキュリティの仕組みを機能させて受け取ったデータを既存のデータと混在させて処理する前に確実にサニタイズするようにしなければならない。そのような（外部）データは、常に、組み入れる前に隔離してスキャンしなければならない。

11.1.4　クラウド上のデータのセキュリティ

数ある技術の中で、アクセス制御と暗号化がデータセキュリティの中核的対策である。

11.1.4.1　クラウド上のデータに対するアクセス制御

アクセス制御は最低限 3 つのレイヤにおいて実装されなければならない。

- **管理用ダッシュボード：**クラウドプラットフォームの管理用ダッシュボードに直接アクセスできるユーザのアクセスに対する管理を組織として行う。例えば、IaaS の Web コンソールへのログインは、そのユーザにオブジェクトストレージ上のデータへのアクセス権を与える。幸いにも、クラウドプラットフォームとクラウド事業者のほとんどは、初期設定では、デフォルトで拒否に設定したアクセス管理ポリシーを適用している。
- **外部向けと内部向けの共有の制御：**データが外部と共有するもので、外部利用者またはパートナーがクラウドプラットフォームへの直接のアクセス権を持たない場合には、アクセス用に二次レイヤのコントロールを設けるべきである。
- **アプリケーションレベルコントロール：**クラウドプラットフォーム上に独自のアプリケーションを構築する場合は、アクセスを管理するために独自のコントロールを設計して実装するべきである。

アクセス制御のための選択肢は、クラウドのサービスモデルならびにクラウド事業者ごとの特性によって異なる。プラットフォームごとの機能に基づいて、権限付与リストを作成すること。権限付与リストとは、どのユーザ、グループまたは役割の人がどのリソースとどの機能にアクセスを許されるかの文書である。

権限	スーパーアドミン	サービスアドミン	ストレージアドミン	開発	セキュリティ監査	セキュリティアドミン
ボリューム記述	X	X		X	X	X
オブジェクト記述	X		X	X	X	X
ボリューム更新	X	X		X		X
ログ読み取り	X				X	X

適用しているコントロールが自組織の要求条件を満たしているか、特にすべての外部向け共有に特段の注意

を払いつつ、高い頻度で（理想的には継続的に）確認すること。すべての外部向けの新しい共有、または外部からのアクセスの許可に対する変更に際して警報を発することを検討すること。

きめ細かなアクセス制御と権限付与マッピング

将来権限付与がどの程度の深さになるかは、技術ごとに大きく異なる。一部のデータベースは低レベルのセキュリティをサポートするかも知れないが、他のものは全面的アクセスより少しましな程度かも知れない。あるものはクラウドプラットフォーム備え付けのアイデンティティに権限付与を紐づけて強制する仕組みを提供するかも知れない。しかし他のものは仮想マシンで単純に走るストレージプラットフォームに完全に依存するものである可能性もある。

自組織がどんな選択肢を持っているか把握し、マッピングして自組織のためのマトリクスを作ることが大事である。このことは、当然、単にファイルアクセスにだけ当てはまるものではない。データベースやすべてのクラウド上のデータストレージにも当てはまる。

11.1.4.2 ストレージ（格納状態）暗号化とトークナイゼーション

暗号化の選択肢は、サービスモデル、クラウド事業者およびアプリケーション／配備の状態により、著しく変化する。鍵管理は暗号化と全く同等に大事なので、この後のセクションで取り扱う。

暗号化とトークナイゼーションは二つの別々の技術である。暗号化はデータを守るのに、データを「かき混ぜる」数学的アルゴリズムを用い、データの復元はそれに見合った鍵を用いたかき混ぜを元に戻すプロセスを走らせることによってのみ実現できる。暗号化の結果は暗号文の塊となる。一方、トークナイゼーションはデータをランダムな値と置き換える。しかる後にオリジナルのデータとランダム化したものを、後で復元できるように安全なデータベースに格納する。

トークナイゼーションはデータのフォーマットが大事である場合にはよく使われる（例えば、同じフォーマットのテキストストリングが必要な既存のシステム内でクレジットカード番号を置き換える場合）。フォーマット保持暗号化は暗号鍵によるデータ暗号化を行うが、同時にトークナイゼーションと同じように構造的フォーマットを維持する。しかしこの方式は無理があるので暗号化並みに安全とは言えないかもしれない。

暗号化システムの仕組みには 3 つの構成要素がある。データ、暗号化エンジン、鍵管理である。データとはもちろん、暗号化対象の情報である。エンジンとは暗号化の数学的プロセスを実行するものである。最後に鍵管理が暗号のための鍵を取り扱う。システム全体の設計の焦点はこれらの構成要素をどこに配置するかである。

暗号化システムの設計に際しては、脅威モデルからスタートすべきである。例えば、鍵管理に関してクラウド事業者は信頼できるか？鍵が露出する可能性は？懸念対象である脅威に対抗するには暗号化エンジンをどこに配置すべきか・

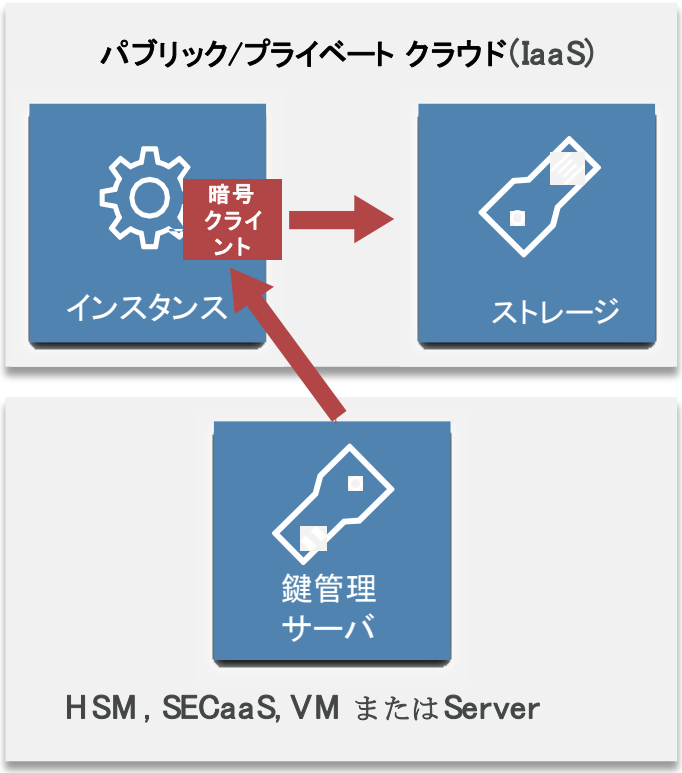
IaaS 環境における暗号化

IaaS 環境にあるボリュームは、データの種類によりいくつかの方法により暗号化することができる。

ボリュームストレージ暗号化

- **インスタンス管理下の暗号化：**暗号化エンジンはインスタンス内で走る。鍵は同一ボリューム内に保存されるが、パスワードまたは鍵ペアにより保護される。

- **外部管理式暗号化：**暗号化エンジンはインスタンス内で走る。鍵は外部で管理され、必要に応じてインスタンスに対して発行される。



外部管理ボリューム暗号化

オブジェクトとファイルのストレージ

- **クライアントサイド暗号化：**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オブジェクトストレージを用いる場合は、アプリケーションまたはクライアントに組み込まれた暗号化エンジンを使ってデータを暗号化すること。
- **サーバサイド暗号化：**データは転送後にサーバ（クラウド）サイドで暗号化される。クラウド事業者が暗号化エンジンを走らせ、暗号鍵へのアクセスも持つ。
- **プロキシ暗号化：**このモデルでは、まずボリュームを特殊なインスタンスまたはアプライアンス／ソフトウェア（訳注：即ちプロキシ）に接続し、しかる後にインスタンスを暗号化インスタンスに接続する。プロキシがすべての暗号化処理を取り扱い、場合によって暗号鍵を内部または外部に保存する。

PaaS 環境における暗号化

PaaS 環境における暗号化は PaaS プラットフォーム**環境における暗号化**が多様であるために極めて大きなバリエーションがある。

- **アプリケーションレイヤー暗号化：**データは PaaS アプリケーション内部またはプラットフォームにアクセスするクライアントによって暗号化される。
- **データベース暗号化：**データは、データベースプラットフォームに組み込まれサポートされている暗号化機能、例えば Transparent Database Encryption (TDE)を用いて暗号化される。もしくはフィールドレベルで暗号化される。
- **その他：**アプリケーションの中に、メッセージキューのようにクラウド事業者が管理するレイヤがある。下層のストレージに暗号化を利用する場合には、IaaS 環境での選択肢も得られる。

SaaS 環境における暗号化

SaaS 事業者は上記の選択肢のいずれかを用いる。可能な限り顧客別暗号鍵を使用して、マルチテナント間の分離を実行することをお薦めする。SaaS 利用者には、以下の選択肢が用意されている。

- **事業者管理下の暗号化：**データは SaaS アプリケーションの中で暗号化される。一般的にはその管理は事業者が行う。
- **プロキシ暗号化：**データは、SaaS アプリケーションに送られる前に、暗号化プロキシを通過する。

11.1.4.3　鍵管理（利用者が管理できる鍵を含む）

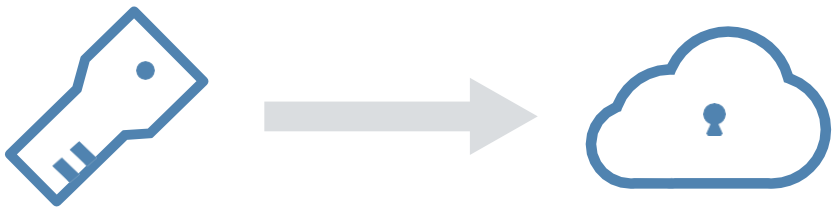
鍵管理において考慮すべき主な要素はパフォーマンス、アクセシビリティ、遅延、セキュリティである。セキュリティとコンプライアンスの要件を満たしつつ、同時に正しい鍵を正しい場所に正しい時間内に置くことは可能か？

鍵管理を実施するために、4 つの選択可能な方法がある。

- **HSM／アプライアンス：**伝統ある HSM(Hardware Security Module)またはアプライアンスベースのキーマネージャを用いる。それは通常オンプレミスに置く必要がある。そして鍵のクラウドへの搬送には専用の接続を用いること。
- **仮想アプライアンス／ソフトウェア：**クラウド上に仮想アプライアンスまたはソフトウェアベースのキーマネージャを配備する。
- **クラウド事業者のサービス：**これは、クラウド事業者による鍵管理サービスである。このオプションを選ぶ前に、鍵が外部にさらされる可能性について、事業者のセキュリティモデルと SLA を確認するようにする必要がある。
- **ハイブリッド：**組合せ利用もある。例えば鍵の安全の根本のところに HSM を用いつつ、（そこから）クラウド上の、特定の用途においてのみ鍵管理を行う仮想アプライアンスに、アプリケーション専用の鍵を配送する。

利用者が管理できる鍵

利用者が管理できる鍵は、クラウド事業者が暗号化エンジンを管理するのに対して、クラウド利用者が自身の暗号鍵を管理できるようにする。例えば、SaaS プラットフォームの中で SaaS データを暗号化するのに利用者自身の鍵を使う。クラウド事業者の多くは、デフォルトでデータを暗号化するが、事業者自らの完全な管理下にある鍵を使う。一部の事業者では、利用者が自分の鍵に差し替えて事業者の暗号化システムに組み入れることを許している。利用する事業者のやり方が利用者自身の要求条件と合致するか確認する必要がある。



利用者が管理できる鍵

あるクラウド事業者は、鍵管理に事業者が提供するサービスを使うように求めるかもしれない。この場合、鍵の管理は利用者側にあっても、それは潜在的には事業者が利用可能なものである。このことは必ずしも、それがセキュアでないことを意味するわけではない。鍵管理とデータストレージシステムは分離することができ、データを侵害しようとするならば、クラウド事業者の側で複数の従業員が共謀しなければならないからである。一方で、国の法律によっては、政府の要求に基づいて、暗号鍵とデータはアクセスされる可能性がある。暗号鍵をクラウド事業者の外部に保管し、必要な時にだけ渡すこともできる。

11.1.5　データセキュリティアーキテクチャ

アプリケーションのアーキテクチャはデータセキュリティに影響を及ぼす。利用するクラウド事業者が提供する機能は、攻撃にさらされる面を減らすかもしれないが、メタストラクチャのセキュリティを強固にするよう求めることを

忘れてはならない。例えばネットワークを分離すること。クラウドストレージやキューイングサービスを使う場合、それらはクラウド事業者のネットワークを通じて通信するべきで、利用者の仮想ネットワーク経由でではない。その結果ネットワーク攻撃のパスは閉ざされるので、攻撃者はクラウド事業者のネットワークを根本のところから破るか、アプリケーションレベルのアタックにとどめるか迫られることになる。

例として、静的インスタンスに SFTP するよりは、データ転送とバッチ処理にオブジェクトストレージを用いるケースがあげられる。ほかの例はメッセージキューによる隔離である。アプリケーションのコンポーネントを別々の仮想ネットワーク上で走らせ、それらの間をつなぐのには、クラウド事業者のキューイングサービスを通じてデータ転送することだけを利用するというやり方である。これによって、アプリケーションの一部から他の部分へネットワーク攻撃することを防止できる。

11.1.6 モニタリング、監査、警報発信

これら（モニタリング、監査、警報発信）は、クラウド監視の全体と結びついていなければならない。（ドメイン 3、6、7 参照）機微な情報に関する権限付与の変更や外部からのアクセスをすべて把握（および警報発信）しなければならない。可能であれば、警報発信のサポートとしてタグを使うこと。

API とストレージアクセスの両方を監視する必要がある。なぜならば、データはそのいずれかを通じて漏洩する可能性があるからである。別の言い方をすれば、オブジェクトストレージにあるデータへのアクセスは、API コール経由または公開の共用 URL 経由で行われるからである。データベース操作監視(Database Access Monitoring)を含む操作監視は別の選択肢となる。ログを、専用ログアカウントのような安全な場所に保存するようにすること。

11.1.7 その他のデータセキュリティコントロール

11.1.7.1 クラウドプラットフォームまたはクラウド事業者独自のコントロール

クラウドプラットフォームまたはクラウド事業者は、このドメインで取り上げている以外のセキュリティコントロールを用意している場合がある。それらは何らかの形のアクセス制御または暗号化である可能性が高いが、このガイダンスで可能性のあるすべての選択肢をカバーすることはできない。

11.1.7.2 DLP (Data Loss Prevention) ＜データ流出防止対策＞

DLP (Data Loss Prevention)は、従業員がモニタリング端末装置、Web、電子メールその他の手段を通じてアクセスするデータを、監視し保護する方法の総称である。DLP は一般にデータセンタでは使用されていない。従って、PaaS や IaaS より、通常は DLP が配備されていない SaaS においてより適用されるべきものである。

- **CASB :** CASB のいくつかは、保護対象のサービスのために DLP の機能を提供している。例えば、特定のクラウドサービスにはクレジットカード番号を絶対に保存しないというポリシーを設定することができる。どの程度効果があるかは、どんなツールであるか、どのクラウドサービスか、そして CASB がモニタリング用途でどのように組み込まれているかによって大きく異なる。ある種の CASB ツールは通信を専用の DLP プラットフォームに振り向けて、CASB が一般に機能として提供する分析に比べて、より精緻な分析を行う。

- **クラウド事業者による機能：**クラウド事業者自体も DLP 機能を提供する場合がある。例えば、クラウドのファイルストレージ兼コラボレーションプラットフォームでは、アップロードされたファイルの内容をスキャンして、その内容に見合うセキュリティポリシーを適用する。

11.1.7.3 ERM (Enterprise Rights Management)

DLP と同様に、ERM は一般に従業員に対するセキュリティコントロールの一つで、クラウドで必ず利用可能とは限らないものである。すべての DRM (Digital Rights Management)/ERM (Enterprise Rights Management)は暗号化をベースとしているため、既存の ERM ツールは、特に SaaS の場合、クラウドの機能を損なう可能性がある。

- **全面的 DRM：**これは従来型の、既存のツールを使った、全面的 Digital Rights Management である。例えば、クラウドサービス上に保存される前に、ファイルに権利（制限）を適用する。上記のように、これはクラウド事業者が提供する、ブラウザによるプレビューや共同作業といった機能を制限する可能性がある。これを避けるには何らかの機能の組込みが必要だが、本書の執筆時点ではその例はまれである。
- **クラウド事業者が提供するコントロール：**クラウドプラットフォームはもとからある機能を用いて全面的 DRM に似た機能を適用することができる場合がある。例えば、「user/device/view versus edit」というポリシーは、特定のユーザに対して Web ブラウザを介してファイルを閲覧することだけを許可する一方で、他のユーザに対してダウンロードや内容の編集を許可する。一部のクラウドプラットフォームはこのようなポリシーを、ユーザレベルだけでなくて、特定のデバイスに対応付けることができる。

11.1.7.4 データのマスキングとテストデータの生成

これら（データのマスキングとテストデータの生成）は開発およびテスト環境におけるデータを守るため、もしくはアプリケーションにおいてデータへのリアルタイムアクセスを制限するための技術である。

- **テストデータの生成：**実際のデータベースに即した、重要性のないテストデータでデータベースを生成することである。スクランブルとランダム化の手法を用いて、元のデータにサイズと構造を似せた上で機微性を排除したデータセットを生成する。
- **ダイナミックマスキング：**ダイナミックマスキングは処理過程でリアルタイムにデータを書き換えるもので、一般にプロキシメカニズムを用い、ユーザに配送されるデータの全部または一部をマスキングする。これは通常、アプリケーションの中のある機微なデータを保護するのに用いられる。例えば、クレジットカード番号の全部でなく最後のいくつかの数字を、ユーザに提示する際にマスクする。

11.1.8 ライフサイクル管理のセキュリティの適用

- **データの保存場所／所在の管理：**生成段階において、不要な保存場所を使用不可にする必要がある。コンテナまたはオブジェクトレベルにおけるアクセス制御には暗号化を用いること。そうすれば、万が一データが許可されていない保存場所に移送されても、暗号鍵が一緒に移動しない限り、データは保護される。
- **法令遵守の確保：**法令遵守を維持するのに、単にコントロールを実装するだけではなく、そのようなコントロールを文書に記し、テストする必要がある。これらは"artifacts of compliance"（法令遵守の事跡情報）と呼ばれるもので、全ての「監査の事跡情報」を含むものである。
- **バックアップと事業継続性：**ドメイン 6 を参照のこと。

11.1　推奨事項

- 自組織が使用しているクラウドプラットフォームに固有の機能を理解すること。
- クラウド事業者のデータセキュリティをオフにしないこと。ほとんどの場合それは自組織独自のデータセキュリティより安全で、しかも低コストで手に入る。
- アクセス管理の設定のために権限付与の表を作ること。それをどこまで実施できるかは、クラウド事業者の機能によって異なる。
- SaaS へのデータ流入を監視するために CASB の利用を検討すること。CASB は PaaS や IaaS にも有効な場合があるが、大規模なマイグレーションの場合は、既存のポリシーやデータリポジトリのセキュリティに左右される。
- 自組織のデータや事業や技術要件にとっての脅威モデルに基づいて、利用しうる暗号化手段の中で適切なものを活用すること。
- クラウド事業者が管理する暗号化とストレージの選択肢の利用を検討すること。できれば、利用者管理型の暗号鍵を用いること。
- アーキテクチャを活用してデータセキュリティを改善すること。アクセス管理と暗号化に全面的に依存してはならない。
- API とデータレベルの監視が行われていることと、そのログがコンプライアンスとライフサイクルのポリシーの要件を満たすことを確認すること。
- 様々な標準があり、適切なセキュリティと暗号および鍵管理の技術とプロセスの利用を実現するのに役立つ。特に NIST SP800-57、ANSI X9.69、ANSI X9.73 が役立つ。

DOMAIN 12

アイデンティティ管理、権限付与管理、アクセス管理（IAM）

12.0　はじめに

アイデンティティ管理、権限付与管理、アクセス管理（IAM）は、クラウドコンピューティングによって深く影響を受ける。

パブリッククラウドとプライベートクラウドの両方において、クラウド事業者とクラウド利用者はセキュリティを犠牲にすることなく IAM を管理する必要がある。このドメインは、クラウドのアイデンティティ管理で何を変更する必要があるかに焦点を当てる。 いくつかの基本的な概念を見直しながら、クラウドがアイデンティティ管理をどのように変え、どのように対処するかについて焦点を当てる。

クラウドコンピューティングは、内部システムの IAM を今までどのように管理してきたかについて、複数の変更をもたらした。これらは必ずしも新しい問題ではないが、クラウドを扱う際により大きな問題になる。

主な違いは、クラウド事業者とクラウド利用者の関係で、これはプライベートクラウドにおいても関係する。IAM は、クラウド事業者だけでもクラウド利用者だけでも単独では管理できないため、信頼関係、責任の明示、それを可能にする技術的な仕組みが必要である。

多くの場合、これは ID 連携に帰着する。このことは、ほとんどの組織がクラウド事業者を数多く（時には何百も）持っているという事実によって悪化し、自組織の IAM を拡張してそれらを取り込むことが必要である。

クラウドはまた、より変化が速く、より分散（法域の境界を超えることを含めて）していて、管理プレーンの複雑さを増し、全てにおいて広範なネットワーク通信により一層（しばしば全面的に）依存する。このことは、ネットワーク攻撃に対して、コアのインフラ管理を新規に開発することになる。さらに、クラウド事業者によって、またサービスモデルと配備モデルの違いによって、大きな違いがある。

> このドメインでは、主に、組織とクラウド事業者間、あるいはクラウド事業者とサービス間の IAM にフォーカスする。IaaS 上で動作するエンタープライズアプリケーション用の内部 IAM のような、クラウドアプリケーション内で IAM を管理する面については説明しない。これらの問題は、従来のインフラで同様のアプリケーションやサービスを構築する場合とほとんど同じである。

12.0.1　クラウドにおける IAM の違いは何か

アイデンティティ管理とアクセス管理は常に複雑である。その中心は、ある形式のエンティティ（人、システム、コードの一部など）を、様々な属性（その時の環境によって変り得る）に関連した検証可能なアイデンティティにマッピングすることである。そして、権限付与に基づいて何を行うことができるかどうかを決定する。そのプロセスのチェーン全体を制御する時にも、異種のシステムやテクノロジ間で、特に大規模で安全かつ検証可能な方法で管理することは難しい。

クラウドコンピューティングでは、複数の組織がリソースに対するアイデンティティ管理とアクセス管理を行うため、プロセスを非常に複雑にする可能性があるという根本的な問題がある。たとえば、同じユーザを数十～数百の異なるクラウドにプロビジョニングする必要がある。ID 連携は、組織間の信頼関係を構築し、標準ベースのテクノロジによって組織に適用することで、この問題の管理に使用される主要なツールである。

初期のコンピュータ（銀行や政府に利用）以前から、ID 連携やその他の IAM 技術とテクノロジが存在していた。また、多くの組織では、IAM のパッチワークとサイロを IT の進化に合わせて構築してきた。クラウドを採用するということは、組織が IAM という仕組みに対応し、またクラウドの違いに対処するためにそれらを更新することを非常に迅速に推し進めるため、クラウドコンピューティングは多少強制力のある機能となる。これは機会と問題の両方をもたらす。

大まかに言って、クラウドへの移行は、近代的なアーキテクチャと標準を用いて新しいインフラとプロセスを構築する機会になる。何年にもわたって、IAM には大きな進歩があったが、予算や既存のインフラの制約のために限られたユースケースの中でしか実装できなかった多くの組織があった。クラウドコンピューティングの採用は、小規模なプロジェクトでもデータセンタ全体の移行においても、一般的に最新の IAM の仕組みを採用して設計された新しいインフラ上に新しいシステムを構築することを意味する。

こういった移行は課題をもたらす。複数の内部および外部の存在を取り込んでフェデレーションに移行することは、関係するすべての変数が膨大な数になるために複雑化し、管理することが難しくなる。異種のシステムおよびテクノロジ間で、属性および権限を決定して実施することは、プロセスおよび技術上の両方の問題をもたらす。基本的なアーキテクチャ上の決定でさえ、クラウド事業者やプラットフォームによりサポート対象が多様であることによって妨げられる可能性がある。

IAM は、基本的にこの文書のすべてのドメインにまたがる。このセクションでは、すべての読者が慣れ親しんでいるとは限らない基本的な用語を簡単に見直してから、まずクラウドのアイデンティティ管理、そしてアクセス管理と権限付与管理に与える影響について掘り下げる。

12.1　概要

IAM は、独自の語彙を使用した広範な実践領域である。従って、この領域の専門家ではない人にとっては混乱を招く恐れがある。それは特に、ある用語が異なるコンテキストにおいて異なる意味を持つ（かつ IAM 外の領域で使用される）ためである。「IAM」という用語でさえ普遍的ではなく、しばしばアイデンティティ管理（IdM）と呼ばれる。

ガートナーは、IAM を「適切な人物が、適切な理由のために適切なタイミングで適切なリソースにアクセスできるようにするセキュリティ原理」と定義している。詳細を説明する前に、クラウドコンピューティングにおける IAM について、ここでの議論に関連した主要な用語を以下に示す：

- **エンティティ(Entity)：** アイデンティティを持っている人物または「物」。個人、システム、デバイス、アプリケーションコードになる。
- **アイデンティティ(Identity)：** エンティティに対する与えられた名前空間内のただ一つの表現。 エンティティは、ある個人が作業アイデンティティ（またはシステムによっては複数のアイデンティティ）、ソーシャルメディアアイデンティティ、個人アイデンティティを持つように、複数のデジタルアイデンティティを有することができる。たとえば、単一のディレクトリサーバ内の単一のエントリであれば、それがあなたのアイデンティティになる。
- **識別子(Identifier)：** アイデンティティをアサーションできる手段。デジタルアイデンティティの場合、これはしばしば暗号学的なトークンになる。現実の世界では、それはあなたのパスポートかもしれない。
- **属性(Attribute)：** アイデンティティの一つの面。属性は、比較的静的（組織単位のように）あるいは高度に動的（IP アドレス、使用されているデバイス、多要素認証（MFA）で認証されたユーザ、場所など）になる。
- **ペルソナ(Persona)：** コンテキストを示す属性を持つアイデンティティの表現。たとえば、ログインして特定のプロジェクトの開発者としてクラウド環境に接続する開発者。 アイデンティティは依然として個人であり、ペルソナはそのプロジェクトのコンテキストにおけるその個人である。
- **役割（ロール）(Role)：** アイデンティティは、コンテキストを示す複数の役割を持つことができる。「役割」は、多くの異なる方法で使用される紛らわしくて濫用される用語である。 本書の目的のために、それはペルソナと同等と考えるか、ペルソナのサブセットと考える。たとえば、特定のプロジェクトの特定の開発者は、”super-admin”や”dev”などの異なる役割を持つことがあり、それはアクセスの決定を行うために使用される。
- **認証(Authentication)：** アイデンティティを確認するプロセス。システムにログインするときに、ユーザ名（識別子）とパスワード（認証要素と呼ばれる属性）を提示する。Authn とも呼ばれる。
- **多要素認証(Multifactor Authentication)（MFA）：** 認証に複数の要素を使用すること。一般的なオプションには、物理デバイスまたは仮想デバイス／トークンによって生成されたワンタイムパスワード（OTP）、テキストメッセージを使用して送信された OTP による帯域外検証[7]、モバイルデバイス、バイオメトリクス、プラグイントークンによる確認が含まれる。
- **アクセス制御(Access Control)：** リソースへのアクセスを制御すること。アクセス管理は、リソースへのアクセスを管理するプロセスである。
- **認可(Authorization)：** アイデンティティが何か（例えば、データや機能）にアクセスできるようにすること。Authz とも呼ばれる。
- **権限付与(Entitlement)：** ID（ロール、ペルソナ、属性を含む）を認可にマッピングすること。 権限付与は、何が許可されているかであり、文書化する場合にはこれらを権限付与マトリクスに格納する。
- **アイデンティティ連携管理(Federated Identity Management)：** 異なるシステムまたは組織間でアイデンティティをアサーションするプロセス。これは、シングルサインオンの重要な実現要素で、クラウドコンピューティングにおける IAM の管理にも役立つ。
- **権威あるルートソース(Authorative Source)：** 従業員のアイデンティティを管理するディレクトリサーバのようなアイデンティティの「ルート」(“root”)ソース。
- **アイデンティティプロバイダ(Identity Provider)：** ID 連携(federation)におけるアイデンティティソース。アイデンティティプロバイダは、常に権威あるルートソースであるとは限らず、特にプロセスのブローカである場合は、権威あるルートソースに依存することがある。
- **リライングパーティ(Relying Party)**：アイデンティティプロバイダからのアイデンティティのアサーションに依存するシステム。

訳注[7]：2 要素認証のひとつで、別の通信チャネルでの認証を通して第 2 認証とする方法。電話による確認等。

主な IAM 標準を含め、以降のセクションでカバーされる関連用語がさらにいくつかある。また、このドメインはパブリッククラウドに集中しすぎているように見えるが、プライベートクラウドにも同じ原則が適用される。しかし、プライベートクラウドでは、組織が全般にわたりより多くのコントロールを持つ可能性があるため、範囲は小さくなる。

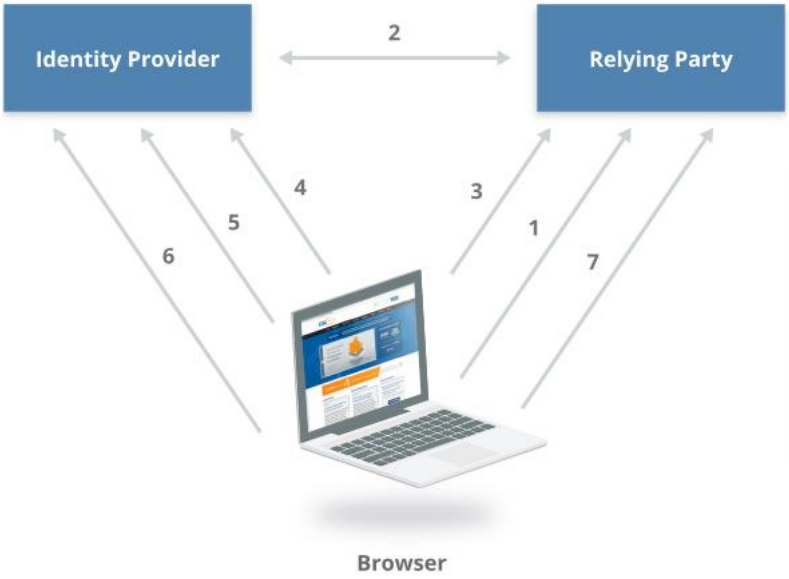
12.1.1　クラウドコンピューティングにおける IAM 標準

かなりの数のアイデンティティ管理とアクセス管理の標準があり、それらの多くはクラウドコンピューティングで使用できる。幅広いオプションにもかかわらず、業界ではさまざまに配備されているものの中で最も一般的であり、ほとんどのクラウド事業者によってサポートされるコアセットを選択している。有望であってもまだ広く使われていない標準もいくつか存在する。以下のリストは、特定の推奨を反映するものではなく、またすべてのオプションを含んでいるわけでもない。幅広いクラウド事業者によって最も一般的にサポートされているものを表す：

- **Security Assertion Markup Language（SAML）2.0** は、認証と認可の両方をサポートするアイデンティティ連携管理の OASIS 標準である。これは、XML を使用して、アイデンティティプロバイダとリライングパーティの間でアサーションを作成する。アサーションには、認証ステートメント、属性ステートメント、認可決定ステートメントを含めることができる。SAML は、企業向けツールとクラウド事業者の両方で非常に幅広くサポートされているが、最初は設定が複雑になる。
- **OAuth** は、Web サービス（個人向けサービスを含む）に非常に広く使用されている認可のための IETF 標準である。OAuth は、HTTP 上で動作するように設計されている。現在のバージョン 2.0 は、バージョン 1.0 と互換性がない。混在に少し混乱をもたらしているのは、OAuth 2.0 はむしろフレームワークであり、OAuth 1.0 よりもあまり厳格ではない。それは、実装に互換性がない場合があることを意味する。サービス間のアクセス制御／許可を橋渡し(delegate)するために最もよく使用される。
- **OpenID** は、Web サービスで非常に広くサポートされている認証連携の標準の一つである。これは HTTP ベースで、アイデンティティプロバイダおよびユーザ／アイデンティティ（例えば、identity.identityprovider.com）を特定するために URL を使用する。現在のバージョンは OpenID Connect 1.0 で、個人向けサービスでよく見られる。

他に以下の 2 つの標準があり、これらは、一般的にはあまり見かけないがクラウドコンピューティングには有用である：

- **eXtensible Access Control Markup Language（XACML）** は、属性ベースのアクセス制御／許可を定義するための標準である。ポリシー決定ポイント（PDP）でアクセス制御を定義し、それをポリシー強制ポイント（PEP）に渡すためのポリシー言語である。SAML と OAuth のどちらとも併用できる。なぜなら、問題の別な部分を解決できるからである。つまり、ログインや権限の橋渡し(delegate)の処理ではなく、エンティティがある属性の組合せによって何を許可されているかを決定する。
- **System for Cross-domain Identity Management（SCIM）** は、ドメイン間でアイデンティティ情報を**交換**するための標準である。外部システムのアカウントのプロビジョニングとプロビジョニング解除、属性情報の交換に使用できる。



1. ユーザが *OpenID URL* を送る
2. *IP* と *RP* は、共有シークレットを設定する
3. ブラウザは、クラウド事業者からトークンを得るためにリダイレクトされる
4. *IP* にサイトのためのトークンを要求する
5. 必要に応じてログインする
6. トークンがブラウザに返される
7. トークンが要求されたサイトに渡される

> アイデンティティ連携管理の仕組み：ID 連携は、信頼関係を構築した後に、リライングパーティにアサーションを行うアイデンティティプロバイダを必要とする。その中心は、信頼関係を構築し資格情報を交換する一連の暗号操作にある。実際的な例は、ユーザがアカウントのためのディレクトリサーバをホストしている職場ネットワークにログインする場合である。ユーザは、SaaS アプリケーションへブラウザから接続する。ログインする代わりに、アイデンティティプロバイダ（内部のディレクトリサーバ）がユーザのアイデンティティ、ユーザに対する認証、その全ての属性をアサーションする一連の内部の操作を行う。リライングパーティは、これらのアサーションを信頼し、ユーザは資格情報を入力することなしにログインする。実際に、リライングパーティはユーザのユーザ名やパスワードを持っていない。成功した認証をアサートするために、アイデンティティプロバイダを信頼する。ユーザは、SaaS アプリケーションの Web サイトにアクセスするだけで、内部ディレクトリで正常に認証されたものと想定してログインを許される。

これは、アイデンティティ、認証、認可のために、クラウドコンピューティングで使用される他の技術や標準がないことを意味するものではない。ほとんどのクラウド事業者、特に IaaS では、これらの標準を使用しない、またはこれらの標準を使用して組織に接続できる独自の内部 IAM システムがある。たとえば、HTTP リクエストへの署名は REST API の認証によく使用され、認可の決定はクラウド事業者側の内部ポリシーによって管理される。リクエストへの署名は、SAML を介した SSO をサポートしているか、API が完全に OAuth ベースであるか、独自のトークンメカニズムを使用している可能性がある。これらすべては一般的に使われるが、ほとんどのエンタープライズクラスのクラウド事業者は、何らかの ID 連携を提供している。

> アイデンティティ関係のプロトコルと標準は、それ自身では完全な解決策ではないが、目的を達成するための手段になる。

アイデンティティプロトコルを選択する際の基本的な概念は以下のとおりである:

- プロトコルは、すべてのアイデンティティおよびアクセス制御の問題を解決する銀の弾丸（訳注：どんなに困難な課題 も一気に解決できるような幻の手法や理論のこと）ではない。
- アイデンティティプロトコルは、ユースケースのコンテキストで分析する必要がある。たとえば、ブラウザベースのシングルサインオン、API キー、モバイルからクラウドへの認証など。これらは、それぞれ異なるアプローチに企業を導く可能性がある。

- 主な運用上の前提は、アイデンティティは DMZ と同様にそれ自体が境界であることである。従って、危険な領域を横断し悪意に耐えられるという立場から、アイデンティティプロトコルを選択して設計する必要がある。

12.1.2 クラウドコンピューティングのためのユーザ、アイデンティティ管理

アイデンティティ管理における「アイデンティティ」は、アイデンティティの登録、プロビジョニング、配布、管理、プロビジョニング解除のプロセスとテクノロジに重点を置いている。システムとしてのアイデンティティ管理とプロビジョニングは、情報セキュリティが何十年にもわたって取り組んできた問題である。 IT 管理者は、さまざまな内部システムごとにユーザを個別にプロビジョニングする必要があった。今日においてさえも、集中型ディレクトリサーバとさまざまな標準によっても、すべての場合に真のシングルサインオンを行うことはまれである。 ユーザは過去のものよりはるかに小さいセットであるにもかかわらず、依然一連の資格情報を管理している。

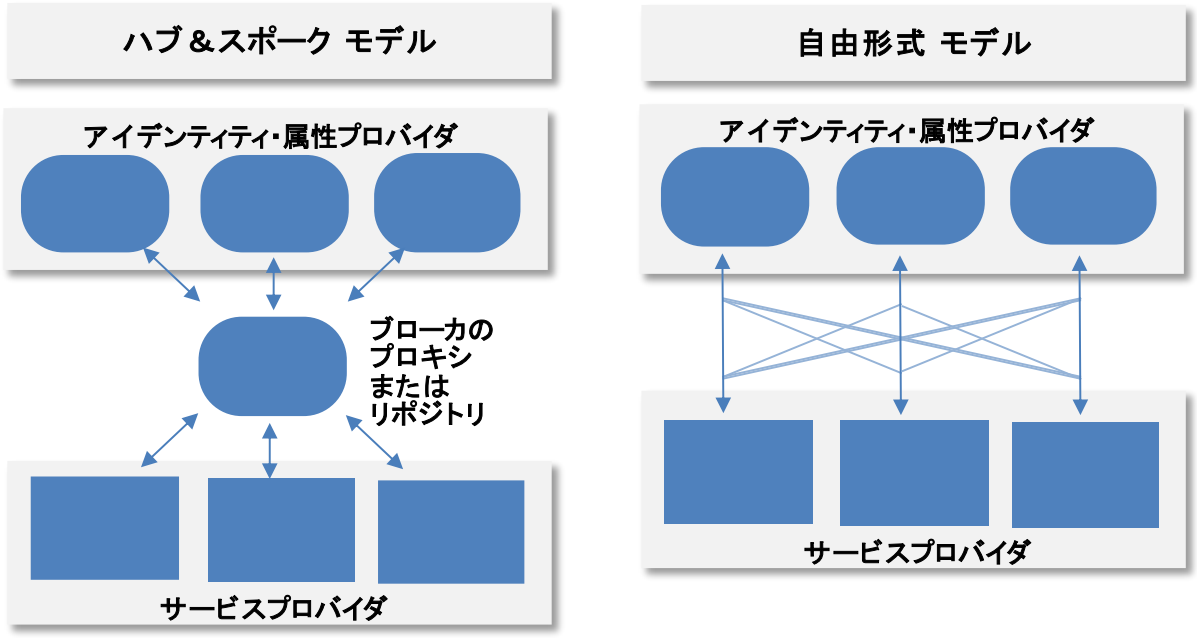
> 範囲に関する注記：このセクションの説明は一般的であるが、ユーザ管理に偏っている。サービス、デバイス、サーバ、コード、その他のエンティティのアイデンティティにも同じ原則が適用されるが、それらのプロセスと内容は複雑であり、アプリケーションのセキュリティとアーキテクチャに密接に関連している。このドメインには、同様に、クラウド事業者の内部アイデンティティ管理の問題に関しては限られた議論しか含まれていない。これらの領域は重要でないということではない。多くの場合重要であるが、このガイダンスの制約内で完全にカバーし切れないほどの複雑さをもたらす。

クラウド事業者とクラウド利用者は、アイデンティティの管理方法に関する基本的な決定から始める必要がある：

- クラウド事業者は、サービスに直接アクセスするユーザの内部アイデンティティ、識別子、属性を常にサポートする必要がある。また、クラウド事業者のシステム内のすべてのユーザを手動でプロビジョニングして管理したり、全てのユーザを個別に認証したりする必要がないように、ID 連携をサポートする。
- クラウド利用者は、アイデンティティを管理する場所と、クラウド事業者との統合をサポートするアーキテクチャモデルとテクノロジを決定する必要がある。

クラウド利用者は、クラウド事業者にログインして、システム内にすべてのアイデンティティを作成することができる。これは、ほとんどの組織にとってスケーラブルではないため、ほとんどが ID 連携に向かう。アイデンティティ連携の接続問題をデバッグするのに役立つバックアップ管理者アカウントなど、クラウド事業者におけるアイデンティティのすべてまたは一部を分離しておくことが理にかなっている場合は例外となりうることに留意すること。

ID 連携を使用する場合、クラウド利用者は、ID 連携する一意のアイデンティティを保持する権威あるルートソースを決定する必要がある。これは、しばしば内部ディレクトリサーバになる。次の決定は、権威あるルートソースをアイデンティティプロバイダとして直接使用するか、権威あるルートソース（人事システムから供給されるディレクトリなど）からフィードする別の ID ソースを使用するか、**アイデンティティブローカ**を組み入れるかどうかである。
２つのアーキテクチャがある。



Free-form vs. hub and spoke 自由形式モデル 対 ハブ＆スポークモデル

- **自由形式モデル:** 内部アイデンティティプロバイダ／ソース（多くの場合、ディレクトリサーバ）はクラウド事業者に直接接続する。
- **ハブ&スポークモデル：**内部アイデンティティプロバイダ／ソースは、中央のブローカまたはリポジトリと通信し、その後、クラウド事業者と ID 連携するためにアイデンティティプロバイダとして機能する。

自由形式モデルで内部ディレクトリサーバを直接連携すると、いくつかの問題が発生する：

- ディレクトリはインターネットアクセスが必要である。これは、既存のトポロジ次第で問題になる可能性がある。あるいは、セキュリティポリシーに違反する可能性がある。
- クラウドサービスにアクセスする前に、ユーザは企業ネットワークに一旦 VPN 接続する必要が生じる場合がある。
- 既存のディレクトリサーバによっては、特に組織のサイロ毎に複数のディレクトリサーバがある場合、外部のクラウド事業者との連携が複雑で技術的に困難な場合がある。

アイデンティティブローカは、アイデンティティプロバイダとリライングパーティ（必ずしもクラウドサービスとは限らない）間の連携を処理する。アイデンティティブローカは、Web-SSO（シングルサインオン）を有効にするために、ネットワークエッジまたはクラウドに配置することができる。

アイデンティティプロバイダは社内のみに配置する必要はない。多くのクラウド事業者は、内部的に、ID 連携と他のクラウドサービスをサポートするクラウドベースのディレクトリサーバをサポートする。たとえば、より複雑なアーキテクチャでは、内部ディレクトリの組織のアイデンティティの一部をアイデンティティブローカとクラウドでホストされたディレクトリに同期または連携させることができる。このディレクトリは、他の ID 連携接続のためのアイデンティティプロバイダとして機能する。

大規模なモデルを決定した後は、どんな実装においてもプロセスとアーキテクチャに関する判断が、依然として必要である:

- アプリケーションコード、システム、デバイス、その他のサービスのアイデンティティをどのように管理するか。同じモデルや標準を活用したり、クラウド展開やアプリケーションで異なるアプローチをとることもできる。たとえば、上記の説明はユーザがサービスにアクセスするときには該当するが、サービスが（他の）サービス、システム、デバイスと通信する場合には同じように当てはまらないかもしれない、あるいは IaaS に配備されているアプリケーションコンポーネントには該当しない場合がある。
- アイデンティティのプロビジョニングプロセスの定義、および、それをクラウド展開に統合する方法。さまざまなユースケースに対して複数のプロビジョニングプロセスが存在することもあるが、可能な限り統一されたプロセスを持つことを目標とすべきである。
    - 組織が従来のインフラのために効果的なプロビジョニングプロセスを実施している場合、理想的にはこれをクラウド展開に拡張する必要がある。しかしながら、既存の内部プロセスに問題がある場合、組織は代わりに新しいより効果的なプロセスを構築する機会としてクラウドへの移行を利用すべきである。
- 個々のクラウド事業者およびクラウド配備のプロビジョニングとサポート。新しいクラウド事業者を IAM インフラに追加するための正式なプロセスが必要である。これには、必要な ID 連携接続を確立するプロセスだけでなく以下を含む：
    - アイデンティティプロバイダとリライングパーティの間の属性（ロールを含む）のマッピング。
    - ふるまい分析などのアイデンティティにひもづけたセキュリティ監視を含む、必要な監視／ログの有効化。
    - 権限付与マトリクスの構築（次のセクションで詳しく説明する）。
    - ID 連携接続（またはその他の手法）の技術的な障害がある場合に備えて、中断／修正のシナリオを文書化する。
    - 特権アカウントの乗っ取りを含む、アカウント乗っ取りが起きた場合に対するインシデント対応計画を確認する。
- アイデンティティおよびクラウド事業者のためのプロビジョニング解除または権限付与変更プロセスを実装する。ID 連携では、接続の両側で作業が必要である。

最後に、クラウド事業者は、サポートしたいアイデンティティ管理標準を決定する必要がある。あるクラウド事業者は ID 連携のみをサポートし、他のクラウド事業者は複数の IAM 標準と独自の内部ユーザ／アカウント管理をサポートする。企業向け市場にサービスを提供するクラウド事業者は、アイデンティティ連携と、ほとんどの場合 SAML を、サポートする必要がある。

12.1.3 認証と資格情報

認証とは、アイデンティティを証明または確認するプロセスである。情報セキュリティでは、認証は最も一般的にはユーザログインの行為を指すが、同時にどんな場合でも、自分が誰であるかを明らかにして、アイデンティティを付与される主体（entity）のことを指す。認証はアイデンティティプロバイダの責任である。

クラウドコンピューティングが認証に及ぼす最大の影響は、**多要素**を使用した**強力な認証**の必要性が高まることである。これには 2 つの理由がある：

- 幅広いネットワークアクセスとは、クラウドサービスが常にネットワーク経由でアクセスされること、多くの場合インターネット経由でアクセスされることを意味する。攻撃がローカルネットワークに限定されていないため、資格情報が失われると、攻撃者によるアカウントの乗っ取りがより簡単になる可能性がある。
- ID 連携をシングルサインオン（SSO）でより多く使用することは、ひとつの資格情報が潜在的に多数のクラウドサービスを危険にさらす可能性があることを意味する。

多要素認証（MFA）は、アカウントの乗っ取りを減らすための最も強力な選択肢のひとつである。それは万能薬ではないが、クラウドサービスにおいて一要素認証（パスワード）に依存することは非常に危険である。ID 連携で MFA を使用する場合、アイデンティティプロバイダは MFA ステータスを属性としてリライングパーティに渡すことができるしそうすべきである。

MFA には以下の複数の選択肢がある：

- **ハードウェアトークン**は、手動入力用のワンタイムパスワードを生成するか、あるいは読み取り機に接続する必要がある物理デバイスである。これらは、最高レベルのセキュリティが必要な場合に最適な選択肢になる。
- **ソフトウェアトークン**は、ハードウェアトークンと同様に機能する、電話やコンピュータで実行されるソフトウェアアプリケーションである。ソフトウェアトークンは、優れた選択肢だが、ユーザのデバイスが侵害された場合に侵害される可能性があり、このリスクをあらゆる脅威モデルで考慮する必要がある。
- **帯域外（アウトオブバンド）パスワード**は、ユーザの電話（通常は）に送信されたテキストやその他のメッセージで、トークンによって生成された他のワンタイムパスワードのように入力される。良い選択肢ではあるが、メッセージの傍受（特に SMS の場合）をどんな脅威モデルでも考慮に入れなければならない。
- **生体認証（バイオメトリクス）**は、携帯電話で一般的に利用できる生体情報リーダのおかげで、選択肢として成長している。クラウドサービスの場合、バイオメトリクスはローカルな手段であり、バイオメトリクス情報をクラウド事業者には送信しない。その代わりに、クラウド事業者に送信することができるのは属性情報である。 従って、ローカルデバイスのセキュリティと所有責任を考慮する必要がある。

クラウド利用者にとって、FIDO はひとつの標準であり、余計な手間を最小限に抑えながらクラウド利用者を強力に認証することを容易にする。

12.1.4 権限付与管理とアクセス管理

権限付与、認可、アクセス制御という用語は、すべて部分的に重複し、コンテキストによって異なる定義がされる。このセクションの前半で定義したが、ここでは簡単に振り返る。

認可とは、何かをすることの許可である。何かとは、ファイルやネットワークにアクセスしたり、特定のリソース上で API 呼び出しのような特定の機能を実行したりすることである。

アクセス制御は、その認可の表明に対して許可または拒否する。従いそれは、アクセスを許可する前にユーザが認証されることを保証するような側面を含む。

権限付与は、アイデンティティを認可および任意の必要となる属性にマッピングする（例えば、属性 Z が指定された値を持つとき、ユーザ X はリソース Y へのアクセスを許可される）。通常、これらの権限付与のマップを権限付与マトリクスと呼ぶ。権限付与は、配布および適用のために技術的ポリシーとしてエンコードされることがよくある。

これは、これらの用語のひとつの定義に過ぎず、他のドキュメントでそれらの用語が異なって使用されることがある。また、アクセス管理という用語も IAM の「A」部分として使用し、認可の定義、伝達、適用のプロセス全体を指している。

ここで、実際のクラウドの例を挙げる。クラウド事業者には、新しい仮想マシンを起動するための API がある。この API には、新しいマシンの起動を許可する権限があり、ユーザが VM を起動できる仮想ネットワークの追加の認可オプションがある。クラウド管理者は、開発者グループのユーザが MFA で認証された場合のみプロジェクトネットワーク限定で仮想マシンを起動できるという権限付与を作成する。グループと MFA の使用は、ユーザのアイデンティティの属性である。この権限付与は、クラウド事業者のシステムに適用のためにロードされるポリシーとして記述される。

クラウドは、権限付与、認可、アクセス管理に複数の方法で影響を与える。

- クラウド事業者とプラットフォームは、他のテクノロジと同様に、独自の認可のセットを持つ場合がある。クラウド事業者が XACML をサポートしていない（現在では稀）限り、クラウド利用者は通常、クラウドプラットフォーム内で権限を直接設定する必要がある。

権限付与マトリクスの例

権限	スーパーアドミン	サービス1アドミン	サービス2アドミン	開発	セキュリティ監査	セキュリティアドミン
サービス1のリスト	X	X		X	X	X
サービス2のリスト	X		X	X	X	X
サービス1 ネットワークの変更	X	X		X		X
サービス2セキュリティルールの変更	X	X				X
監査ログの読み取り	X				X	X

- クラウド事業者は、認証とアクセス制御の適用に責任を持つ。
- クラウド利用者は、権限付与を定義し、クラウドプラットフォーム内でその権限付与を適切に設定する責任がある。
- クラウドプラットフォームは、IAM として、**ロールベースのアクセス制御（RBAC）**モデルよりも優れた柔軟性とセキュリティを提供する**属性ベースのアクセス制御（ABAC）**モデルをより大きくサポートする傾向がある。RBAC は、認可を適用する従来のモデルであり、しばしば単一の属性であるもの（定義された役割）に依っている。ABAC は、役割、場所、認証方法、その他などの複数の属性を組み込むことにより、より精緻な、コンテキストに応じた決定を可能にする。
    - ABAC は、クラウドベースのアクセス管理に適したモデルである。
- ID 連携を使用する場合、クラウド利用者はロールやグループなどを含む属性をクラウド事業者にマッピングし、認証時にこれらの属性が適切に伝達されるようにする責任がある。
- クラウド事業者は、クラウド利用者のために、ABAC と効果的なセキュリティを実現するための、粒度の高い属性と認可をサポートする責任がある。

12.1.5　特権ユーザ管理

リスクを管理する上で、特権ユーザ管理ほど重要なものはほとんどない。強力な認証のための上記の要件は、特権ユーザに関して入念に検討すべきである。さらに、特権ユーザに関する説明責任と可視性を高めるために、アカウントとセッションの記録を実装する必要がある。

場合によっては、特権ユーザのサインインを専用の厳密に管理されたシステムで行うことが有益である。そのシステムは、資格情報制御、デジタル証明書、物理的および論理的に分離したアクセスポイント、ジャンプホスト（訳注：分離したネットワークゾーンでデバイスを管理すること）による高いレベルの保証を使用するものである。

12.2　推奨事項

- 組織は、クラウドサービスでアイデンティティと認可を管理するための包括的かつ公式な計画とプロセスを開発する必要がある。
- 外部のクラウド事業者に接続する場合は、可能であれば ID 連携を使用して、既存のアイデンティティ管理を拡張する。内部のアイデンティティに結びついていないクラウドプロバイダ固有のアイデンティティ管理を最小限に抑えるようにする。
- 適切であれば、アイデンティティブローカの使用を検討する。
- クラウド利用者は、アイデンティティプロバイダを管理しアイデンティティと属性を定義する責任を負う。
    - これらは権威のあるルートソースに基づくべきである。
    - オンプレミスのディレクトリサーバが利用できないあるいは要件を満たしていない場合、分散した組織ではクラウドホスト型のディレクトリサーバの使用を検討する必要がある。
- クラウド利用者は、すべての外部のクラウドアカウントに対して MFA を選択し、認証連携を使用する場合には MFA ステータスを属性として送信するべきである。
- 特権を持つアイデンティティは、常に MFA を使用することが望ましい。
- クラウド事業者とプロジェクト毎に、メタ構造や管理プレーンへのアクセスに重点をおいた権限付与マトリクスを開発すること。
- クラウド事業者またはプラットフォームでサポートされている場合は、権限付与マトリクスを技術ポリシーに組み入れること。
- クラウドコンピューティングでは RBAC よりも ABAC を優先すること。
- クラウド事業者は、オープンな標準に基づく内部アイデンティティと ID 連携の両方を提供する必要がある。
- 魔法のプロトコルはない。まず、ユースケースを取り上げて制約条件を洗い出し、次に適切なプロトコルを見つけること。

DOMAIN 13

Security as a Service

13.0 はじめに

このガイダンスの大部分はクラウドプラットフォームとクラウドの配備に関するセキュリティに焦点を当てているが、本ドメインでは、方向を変えて、クラウドから提供されるセキュリティサービスを取り上げる。それらのサービスは、一般的に SaaS または PaaS であるが、必ずしもクラウドの配備への保護に特化して利用されるわけではなく、同時に従来からあるオンプレミスのインフラストラクチャの防衛にも役立つ。

Security as a Service (SecaaS) 事業者は、セキュリティの機能をクラウドサービスとして提供する。ここには、SecaaS に特化した事業者もいると同時に、一般的なクラウドコンピューティングの提供事業者によるセキュリティ機能のパッケージもある。Security as a Service は非常に広い範囲の技術を包含するが、以下の基準を満たしている必要がある。

- SecaaS には、クラウドサービスとして提供されるセキュリティ製品またはサービスを含むこと。
- SecaaS と認められるためには、そのサービスがドメイン 1 で定義した NIST によるクラウドコンピューティングの基本特性を満たしていること。

このセクションでは、市場にみられる比較的一般的な形態に光を当てる。しかし、SecaaS は常に進化しており、ここに示す記述内容や以下に示すリストが確定的なものであると考えるべきでない。この文書で取り上げない例やサービスもあるし、新たな市場への参入も常態化している。

13.1 概要

13.1.1 SecaaS に潜在するメリットと懸念事項

SecaaS の主要なカテゴリの詳細に分け入る前に、SecaaS がオンプレミスのセキュリティや、自力で管理するセキュリティとどう違うのかを押さえておくことは大事である。そのためには、どんなメリットの可能性があるのかと、それがもたらすものが何かを考えてみよう。

13.1.1.1 期待されるメリット

- **クラウドコンピューティングにおけるメリット** クラウドコンピューティングにおいて通常期待されるメリット－投下資本の節約、即応性、冗長性、高い可用性、障害耐性－のすべてが SecaaS に当てはまる。

一般のクラウド事業者の場合と同様に、セキュリティ提供事業者の場合にも、こういったメリットがどの程度効くかは、その価格、実運用、能力の如何にかかっている。

- **スタッフと専門能力**　多くの組織で、様々な専門能力に関して、セキュリティのプロフェッショナルの雇用、教育、繋ぎ留めの課題と格闘している。この問題をさらに深刻にする要素として、地域の労働市場の限界、専門家の高いコスト、そして攻撃側の高速な進化に日々対応しなければいけないという問題がある。それに対して、セキュリティだけ、あるいは特定のセキュリティ領域だけですら注力することができない一般の組織においては実現不可能な、広範な専門知識とその分野での研鑽というメリットを、SecaaS 事業者は提供してくれる。
- **情報共有**　SecaaS 事業者は複数の顧客を同時に守っており、それらの間での情報分析やデータの共有が可能である。例えば、ある顧客でマルウェアのサンプルを入手したら、SecaaS 事業者は直ちにそれを防御用プラットフォームに追加することができ、他の顧客全部を守ることができる。カテゴリによってその効果は異なるので、実際のところこれは魔法の杖という訳には行かないが、情報共有の仕組みはサービスの中に組み込まれているので、うまく機能する可能性は高い。
- **配備の臨機応変さ**　SecaaS は、それ自体広範囲のネットワークアクセスと伸縮性を備えたクラウドネイティブなモデルなので、拡大する職域やクラウドへの移行をサポートする点でよい位置にいると言えるであろう。サービスは通常、よりフレキシブルな配備形態に対応可能である。例えば、複数の場所に対して、ハードウェアを個々に設置するという煩雑さを伴うことなくサポートできる。
- **顧客の隔離**　場合によっては、SecaaS は組織に対して攻撃が直接加えられる前に阻止できる。例えば、スパムフィルタリングとクラウドベースの WAF が、攻撃者と組織の**間**に配置されている。そのため、ある種の攻撃はそれが顧客の資産に到達する前に取り除くことができる。
- **スケーラビリティとコスト**　このクラウドモデルは、利用者に「成長に応じて支払う」モデルを提供する。それによって利用組織はそのコアの事業に集中でき、セキュリティに関する懸念事項を専門家に委ねることができる。

13.1.1.2　懸念事項

- **可視性の不足**　サービスが顧客と離れた形で行われるため、自前での運用に比べて可視性の点やデータ提供の面で劣る。SecaaS 事業者は、自社のセキュリティをどう実装し、その環境をどう管理しているかの詳細を明かさない可能性がある。どんなサービスか、どんな事業者かによるが、監視やインシデントの発生に際してデータソースの差やどの程度の詳細情報が得られるかに影響する。顧客が従来手に入れていた情報の一部は、見え方が違ったり、ギャップが生じたり、あるいは全く得られなかったりする。実物証拠やコンプライアンスの事跡情報、さらにはその他の証拠となるデータが顧客の目的とするところに適合しないかもしれない。これらのことはすべて、契約を結ぶ前に確認できることであり、そうすべきである。
- **法規制の違い**　グローバルな法規制に準拠する結果、SecaaS 事業者は場合によっては顧客の組織の事業に対する管轄法に対するコンプライアンスを保証できない可能性がある。
- **規制対象データの取扱い**　顧客は、規制対象のデータが通常のセキュリティスキャンの一環として収集されるかも知れないことや、セキュリティインシデントが遵守すべき要求事項に従って処理されることに対する保証を必要とする。このことにより、上記の国際間の法管轄の差の遵守が必要になる。例えば、従業員に対する監視は米国以上に欧州では制限されており、欧州では通常の基本的セキュリティ監視活動でさえ労働者の権利の侵害となる可能性がある。同様に、SecaaS 事業者がデータセンタの移転やロードバランスのためにその業務を移転させた場合、データの地理的所在場所に関する制限を定めた規制に抵触する場合がある。
- **データ漏洩**　クラウドコンピューティングサービスまたは製品と同様に、あるクラウド利用者から他のクラウド利用者にデータが漏れることに関する懸念が常にある。このリスクは SecaaS に特有というものではないが、セキュリティのデータは特に機微性が高いという性質があり（またその他の規制対象のデータがセキュリティスキャンの時やセキュリティインシデントに際して漏洩する恐れから）、SecaaS 事業者はマルチテナント間の隔離と分離に関する最高度の基準に準拠すべきである。セキュリティに関するデータはまた、

訴訟、司法当局による捜査、その他の証拠開示の場に関わる可能性がある。SecaaS の利用者は、このような状況において他のサービス利用者が関わっている場合には、自組織のデータが開示されないことの保証を求める。

- **SecaaS 事業者の変更**　オンプレミスのハードウェアやソフトウェアを入れ替えるよりは、単に SecaaS 事業者を入れ替えるほうが表面的には簡単に見える。しかし、ロックインのリスクがある。なぜならば、コンプライアンスや法的調査への対応のために必要な時系列データを含むデータへのアクセスが失われる恐れがあるからである。
- **SecaaS への移行**　既存のセキュリティオペレーションやオンプレミスの従来型セキュリティ管理ソリューションを持っている組織では、SecaaS への移行、さらには内部の IT 部門と SecaaS 事業者の間の責任分界点やインターフェイスは細心に計画し、実施し、保守するようにしなければならない。

13.1.2　SecaaS サービスの主たるカテゴリ

数多くの商品やサービスが Security as a Service という呼称に該当する。以下に示すものが正規なリストというわけではないが、本書執筆時点で一般的に見られるカテゴリについて記している。

13.1.2.1　アイデンティティ・権限付与・アクセス管理サービス

アイデンティティ・アズ・ア・サービスは、アイデンティティに関するエコシステムを構成する様々なサービスのうち一つ以上を含む、一般的な呼称である。様々なサービスとは、Policy Enforcement Points (PEP-as-a-service)、Policy Decision Points (PDP-as-a-service)、Policy Access Points (PAP-as-a-service)、組織にアイデンティティを提供するサービス、識別情報（例：MFA(Multi-Factor Authentication)を提供するサービス、信用評価を提供するサービスなどである。

クラウドセキュリティで多く利用されている、更によく知られているサービスの一つに Federated Identity Brokers（アイデンティティ連携仲介事業者）がある。このサービスは、組織がすでに持っている複数のアイデンティティプロバイダ（内部管理またはクラウド上でホストされたディレクトリ）と組織が利用する多種類のクラウドサービスの間で IAM を仲介する。このサービスは Web ベースのシングルサインオン(SSO)の提供が可能で、各々別々の ID 連携の設定を使う外部の多様なサービス接続する、という複雑な処理の一部を容易にするのに役立つ。

その他に二つのカテゴリが、クラウドで一般的に配備されている。強固な認証サービスでは、複数の強固な認証方式の統合を単純化するのにアプリとインフラを用いる（例としてモバイルデバイスにおける MFA のためのアプリとトークン）。もう一つのカテゴリはクラウド上でディレクトリサービスをホストして、組織のためにアイデンティティプロバイダとして機能する。

13.1.2.2　クラウドアクセス・セキュリティ・ブローカ（CASB。別名 Cloud Security Gateway）

この商品は、クラウドサービスに向けた通信に割り込みをかけたり、直接 API を介してクラウドサービスに接続したりして、挙動の監視、ポリシーの適用、セキュリティ問題の検知や予防を行う。このサービスが最もよく使われるのは、組織が認定したものや未認定の SaaS サービスの管理である。CASB はオンプレミスの形態もあるが、多くの場合、クラウド上でホストされたサービスとして提供される。

CASB はまた、オンプレミスのツールと接続してクラウドの利用や承認されていないサービスについて検知し、評価し、場合によってはブロックする。多くの場合このようなツールはリスクのランク付け機能を持っていて、顧客が何百何千というクラウドサービスを理解しカテゴライズする手助けをする。ランク付けはその CASB 事業者によるいくつか

の評価を組み合わせたものをベースにしており、組織の優先度に応じて重みづけをしたり組み合わせたりすることができる。

ほとんどの CASB 事業者はまた、そのカバーするクラウドサービスに向けて基本的な DLP(Data Loss Prevention)機能を提供しており、それは内在型であったり他のサービスと連携する複合型であったりする。

CASB について語る組織にもよるが、CASB は時として、Federated Identity Brokers（アイデンティティ連携仲介事業者）を含む言葉として使われることがある。これは混乱を招く。「セキュリティゲートウェイ」と「アイデンティティブローカ」の機能の組合せは可能だし現に存在しているが、市場では依然として、この二つのカテゴリが独立したサービスである状態が一般的である。

13.1.2.3 Web セキュリティ（Web Security Gateway）

Web セキュリティはリアルタイム保護を行うもので、ソフトウェアまたはアプライアンスを設置してオンプレミスで提供する形や、クラウド上で、クラウド事業者向けのトラフィックをプロキシ経由にしたりリダイレクトしたりする形（あるいはその両者のハイブリッド）で提供される。これは他の防御の上に防御を重ねるもので、他の防御とは例えば、Web 閲覧などの企業の活動を通じてマルウェアが侵入するのを防止するアンチマルウェアソフトである。更に、このサービスは、Web アクセスのタイプや Web アクセスが認められる時間帯に関するポリシーに基づくルールを、遵守させることができる。アプリケーションについての許可の管理は、Web アプリケーションに関してさらに上位の、精緻で状態遷移ベースのセキュリティ規制を実現できる。

13.1.2.4 e メールセキュリティ

e メールセキュリティは着信と発信双方の e メールに対する管理を提供し、フィッシングや悪意ある添付ファイルのリスクから組織を保護し、更に企業ポリシーに基づく適正利用やスパム防止を適用し、事業継続に関する機能も提供する。

それに加え、e メールをポリシーに基づいて暗号化することや、各種の e メールサーバによるソリューションとの組合せもサポートする。e メールセキュリティソリューションの多くは、発信者確認や否認防止のためのデジタル署名といった機能も提供する。このカテゴリには、アンチスパム機能といった単純なものから、最も高度なところでは高機能なマルウェアおよびフィッシングに対する防御を備える e メールセキュリティゲートウェイまで、あらゆる種類のサービスが含まれる。

13.1.2.5 セキュリティアセスメント

セキュリティアセスメントとは、第三者もしくは利用者によるクラウドサービスの監査、またはクラウドベースのソリューションを用いたオンプレミスシステムの評価である。従来からのインフラ、アプリケーションおよびコンプライアンス監査のためのセキュリティアセスメントは、複数の標準、NIST、ISO、CIS などにより十分に定義づけられサポートされている。比較的成熟度の高いツールセットがあり、数多くのツールが SecaaS のサービスモデルを使って実装されている。このモデルを使うことで、クラウド利用者はクラウドコンピューティングによる代表的な利点、すなわち柔軟な拡張性、無視できるほどのセットアップ時間、低い管理コスト、低い初期投資と利用料課金、などを得ることができる。

セキュリティアセスメントには主として 3 つのカテゴリがある：

- クラウド上またはオンプレミスに配備されている資産に対する伝統的なセキュリティ／脆弱性評価（つまり仮想マシン／インスタンスへのパッチ・脆弱性検査）。

- SAST、DAST および RASP 管理といった、アプリケーションに対するセキュリティ評価。
- API を介して直接クラウドサービスに接続するクラウドプラットフォーム評価ツールによる、クラウド上に配備された資産のみならずクラウドの設定にまで及ぶアセスメント。

13.1.2.6 Web アプリケーションファイアウォール

クラウドベースの WAF(Web Application Firewall)では、クラウド利用者は Web トラフィックを（DNS を使って）(WAF)サービスにリダイレクトし、対象の Web アプリケーションにそれが渡される前に分析しフィルタする。クラウドベースの WAF の多くはまた、DDoS 攻撃対策の機能も持っている。

13.1.2.7 侵入検知／防止（IDS/IPS: Intrusion Detection/Prevention）

侵入検知／防止システムはルールベース、自律解析または挙動解析モデルにより行動パターンをモニタリングし、企業にリスクをもたらす可能性のある挙動における不正を検出する。IDS/IPS as a Service では、（オンプレミスでは）利用者自身がイベントの解析を引き受けるのに対して、情報はサービス事業者の管理用プラットフォームに入力される。クラウド用の IDS/IPS は、オンプレミスのセキュリティシステムの中のハードウェアや、クラウド上では仮想アプライアンス（制約についてはドメイン 7 参照）またはホストベースのエージェント上で稼働することができる。

13.1.2.8 セキュリティ情報・イベント管理（SIEM: Security Information & Event Management）

セキュリティ情報・イベント管理（SIEM: Security Information & Event Management）システムは、仮想／実ネットワーク、アプリケーション、システムから（プッシュまたはプルの仕組みで）ログおよびイベントデータを収集蓄積する。この情報は次に相関付けられ、分析されて、攻撃の阻止やその他の対応が必要な情報もしくはイベントについて、リアルタイムで報告と警報が上げられる。オンプレミスの利用者が管理するシステムと異なり、クラウド上の SIEM はこのような情報をクラウドサービスについて収集する。

13.1.2.9 暗号化と鍵管理

このサービスはデータの暗号化と、暗号鍵の管理のどちらかまたは両方を行う。クラウドサービスでも、クラウド利用者の管理下で行う暗号化とデータセキュリティをサポートするために、このサービスは提供されている。その場合はその特定のクラウド事業者内の資産の保護に限定されることもあるが、このサービスは複数のクラウド事業者にまたがって（さらには API 経由でオンプレミスにも）アクセス可能で、より広範な暗号化の管理ができる場合もある。このカテゴリにはまた、SaaS 向けの暗号化プロキシもあり、むき出しのデータを暗号化するために SaaS の通信をインターセプト（途中介入）する。

ただし、SaaS プラットフォームの外で暗号化を行うと、プラットフォームが対象となるデータを処理する機能に影響を及ぼす可能性がある。

13.1.2.10 事業継続と災害復旧（BC/DR: Business Continuity / Disaster Recovery)

クラウドベースの BC/DR サービス事業者は、ローカルのストレージやテープを運び出すことに頼る代わりに、個別のシステム、データセンタ、またはクラウドサービスからのデータバックアップを、クラウドプラットフォーム上に行う。このサービスは、データ転送とローカルへのリカバリを高速化するために、ローカルのゲートウェイを使う場合があり、クラウドサービスの側は、最悪のシナリオへの備えやアーカイブのために最終のリポジトリとして機能する。

13.1.2.11 セキュリティ管理

このサービスは、従来からあるセキュリティ対策機能、例えばエンドポイント防御(EPP)、エージェント管理、ネットワークセキュリティ、モバイルデバイス管理その他諸々をまとめて、単一のクラウドサービスに取り込む。そうすることで、ローカルの管理用サーバを減らしたりなくしたりできるし、また複数地点に分散している組織にとって特にうまく適合する。

13.1.2.12 DDoS 対策（Distributed Denial of Service Protection）

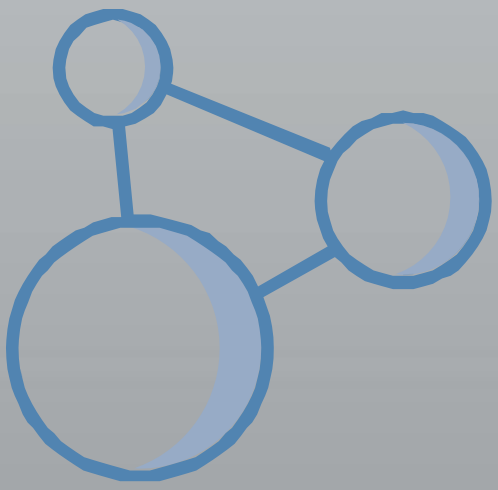
ほとんどの DDoS 対策はその性格上、クラウドベースである。このサービスは DDoS 対策サービスの中でトラフィックを経路変更し、攻撃が顧客自身のインフラストラクチャに影響を与える前にその攻撃を吸収する。

13.2 推奨事項

- SecaaS 事業者と契約する前に、データ管理（可用性を含む）、調査対応、コンプライアンスへのサポートに関するセキュリティに固有の要求条件を把握するようにすること。
- 規制対象のデータ、例えば PII の取り扱いについては特段の注意を払うこと。
- 自組織のデータ保存の要求度合を把握し、ロックインを招かないデータ取り扱いをサポートできる事業者を選ぶこと。
- SecaaS サービスが自組織の現状と将来の計画と適合することを確認すること。例えばそのサービスがサポートするクラウド（およびオンプレミス）プラットフォームや、そのサービスが対応しているワークステーションとモバイルの OS の種類や、その他のことについて。

DOMAIN 14

関連技術



14.0　はじめに

このガイダンスは、全体に渡ってクラウドコンピューティングを直接的にセキュアにするバックグラウンド情報およびベストプラクティスを提供することに重点をおいている。そのような基盤技術として、各々特定のセキュリティ上の関心事項を扱う様々な関連技術がある。

クラウドの用途をすべてカバーすることは、この文書の範囲を超えるが、CSA は、クラウドと相互に関連する重要な技術のバックグラウンドおよび推奨事項にも触れることが重要だと感じている。コンテナや SDN などの技術は、非常に密接に関連しているので、本ガイダンスの各ドメインでカバーしている。 このドメインでは、これまでのドメインに収まりきらない追加の技術について、より詳しい情報を提供する。

これらの技術を、個別にセクションとして取り扱うことで、内容を更新し、使い道の変化や新しい機能の登場に合わせて技術の追加や削除を柔軟に行うことができる。

14.1　概要

関連技術は、次の 2 つの大きなカテゴリに分けられる。

- 専ら、クラウドコンピューティングの範囲で使われる技術。
- 必ずしもクラウドに限定されないが、クラウド展開でよく使われる技術。

クラウドなしでは、これらの技術が機能しないわけではないが、クラウドの展開と重なったり、依存したりすることが多く、クラウドセキュリティ専門家の大多数にとって意味があると考えられている。

現在の一覧には次のようなものがある。

- ビッグデータ
- モノのインターネット（IoT）
- モバイルデバイス
- サーバレスコンピューティング

これらの各技術は、現在、CSA の研究ワーキンググループによって、多くの進行中のプロジェクトや出版物の中でカバーされている。

- ビッグデータワーキンググループ

- IoT ワーキンググループ
- モバイルワーキンググループ

14.1.1 ビッグデータ

ビッグデータには、従来のデータ処理ツールでは管理できない非常に大きなデータセットを扱うための一連の技術が含まれている。 これは単一の技術ではなく、広く、分散型の収集、保管、およびデータ処理のフレームワークを意味している。

ガートナーは次のように定義している。「ビッグデータは、大量、高速、多様な情報資産であり、意思決定の高度化、洞察による解明、並びにプロセスの最適化のために新しい形の処理を必要とする。」

他にも多くの解釈があるが、 "3 V"は、ビッグデータの中核の定義として一般に受け入れられている。

- **大量（High volume）：**件数および属性の種類の点で大規模なデータ。
- **高速（High velocity）：**高速生成および高速処理されるデータ、すなわちリアルタイムまたはストリームデータ。
- **多様（High variety）：**構造化、半構造化、または非構造化データ。

クラウドコンピューティングでは、その伸縮性と巨大なストレージ能力のために、ビッグデータのプロジェクトが展開されることが頻繁にある。ビッグデータは、必ずしもクラウドだけのものではないが、ビッグデータ技術は、一般的にクラウドコンピューティングアプリケーションに組み込まれ、クラウド事業者によって IaaS または PaaS として提供されることが多い。

ビッグデータには、使用される特定のツールセットに関係なく、次の 3 つの共通的な構成要素がある。

- **分散データ収集：**大量のデータ（ストリーミング型が多い）を取り込む仕組み。 これには、Web クリックのストリーミング分析のような簡単なものから、高度に分散された科学的イメージングやセンサーデータのような複雑なものまである。 すべてのビッグデータが分散型またはストリーミング型のデータ収集によっているわけではないが、分散データ収集は中核となるビッグデータ技術である。
- **分散ストレージ：**分散ファイルシステム（Google File System、Hadoop Distributed File System など）やデータベース（多くの場合 NoSQL）に大量のデータセットを格納する機能で、非分散ストレージ技術には制限があるため、しばしば必要とされる。
- **分散処理：**単一処理では効率的に処理できないほど、大量で変化の激しいデータセットの、効率的な分析を行うジョブのための、分散処理ツール（MapReduce、Spark など）。

14.1.1.1 セキュリティおよびプライバシーへの考慮

ビッグデータアプリケーション（多様なノードに分散されたデータの収集、蓄積、処理を伴う）の高度に分散型の特性と、情報が大量であることと機微である可能性のために、セキュリティとプライバシーの重要性が一般的に高い。しかしそれは、ツールやプラットフォームの組合せが多様であるために容易ではない。

14.1.1.2 データ収集

データ収集メカニズムでは、中間ストレージを使用する場合があるが、それには適切なセキュリティが必要である。中間ストレージは、収集から蓄積へのデータ転送の一部として使用される。プライマリストレージのセキュリティが確保されている場合でも、処理ノード上のスワップスペースのような単純な中間ストレージをチェックすることも重要で

ある。例えば、収集がコンテナまたは仮想マシンで実行されている場合は、基になるストレージが適切に保護されていることを確実にすること。また、分散型の分析／処理ノードは、追加のセキュリティが必要な中間ストレージを使用する可能性がある。例えば、処理ジョブを実行しているインスタンスのボリューム記憶域などである。

14.1.1.3 鍵管理

ストレージに対する鍵管理は、ノードが分散する特性のために、厳密にどのメカニズムが使われるか次第で複雑になる場合がある。今日、ビッグデータストレージ層の大部分を適切に暗号化する技術があり、これらはドメイン 11（データセキュリティと暗号化）に書かれている。複雑化する要因は、鍵管理が複数のストレージや分析ノードへの鍵の分配を処理する必要があることにある。

14.1.1.4 セキュリティ機能

すべてのビッグデータ技術が、強力なセキュリティ機能を備えているわけではない。いくつかのケースでは、クラウド事業者のセキュリティ機能は、ビッグデータ技術の限界を補うのに役立つ。どちらの機能もセキュリティアーキテクチャに含めるべきであり、その内容は選択した技術の組合せごとに個別のものになる。

14.1.1.5 アイデンティティ・アクセス管理

アイデンティティ・アクセス管理は、クラウドおよびビッグデータツールの両方のレベルで生じることが多く、権限付与マトリクスを複雑にする場合がある。

14.1.1.6 PaaS

クラウド事業者の多くは、ビッグデータのサポートを拡大し、機械学習およびエンタープライズデータへのアクセスを伴う PaaS のオプションを提供している。これらのサービスは、データ漏洩、コンプライアンス、およびプライバシーへの影響の可能性を十分に理解した上で使用すべきである。例えば、機械学習がクラウド事業者のインフラストラクチャ内の PaaS で実行される場合、クラウド事業者の従業員が技術的にアクセスできる可能性があり、コンプライアンスを損なう恐れを生じるのではないか。

これは、そのサービスを使用すべきではないということではなく、単にその影響を理解し、適切なリスク判断を行う必要があることを意味する。機械学習およびその他の分析サービスは、必ずしも安全でないというわけではなく、必ずしもプライバシーやコンプライアンスに関する責務を侵害するものでもない。

14.1.2 IoT（モノのインターネット）

IoT は、物理的世界で使用されインターネット接続を利用する、非従来型のコンピューティングデバイスの総称である。 それには、インターネットを活用した（電源や水道などの公共サービスで使用される）運用技術から、フィットネスのモニタ装置、スマート照明、医療機器、その他のものが含まれる。これらの技術は、企業環境にますます導入されており、次のような例がある。

- サプライチェーンのデジタルトラッキング
- 物流のデジタルトラッキング
- マーケティング管理、小売り管理、および顧客管理
- 従業員向け、または消費者向けの、オンラインヘルスケア管理やオンラインライフスタイル管理

これらのデバイスの大部分は、バックエンド処理とデータストレージのためにクラウドコンピューティングのインフラストラクチャに接続される。 IoT に関連する主要なクラウドセキュリティの課題には次のようなものがある。

- セキュアなデータ収集とサニタイズ
- デバイスの登録、認証、および認可。今日、直面している共通的な課題の 1 つは、バックエンドのクラウド事業者へ直接 API コールを行うために、格納された資格情報を使用することである。 攻撃者がアプリケーションやデバイスソフトウェアを逆コンパイルし、悪意のある目的のためにこれらの資格情報を使用することはよく知られている
- デバイスからクラウドインフラストラクチャへの接続のための API のセキュリティ。 前述の格納された資格情報の問題だけでなく、API 自体をデコードして、クラウドインフラストラクチャに対する攻撃に使用することもできる。
- 通信の暗号化。 現在のデバイスの多くは、データやデバイスを危険にさらしてしまう、弱い、古い、または使用されなくなった暗号化を使用している。
- デバイスがセキュリティ侵害の穴にならないようにパッチとアップデートができること。 今日、デバイスは、製造された状態のまま出荷され、オペレーティングシステムまたはアプリケーションのセキュリティアップデートが行われないのが一般的である。 このことは既に、セキュリティを侵害された IoT デバイスによる大規模なボットネット攻撃など、大規模で頻繁に取り上げられる複数のセキュリティ事件を生じさせている。

14.1.3 モバイル

モバイルコンピューティングは、新しいものでもクラウドだけのものでもないが、モバイルアプリケーションの大部分は、バックエンド処理のためにクラウドコンピューティングに接続している。クラウド事業者は地理的に分散しており、モバイルアプリケーションでよく利用する非常に動的なワークロードという特性向きに設計されているため、クラウドはモバイルをサポートする理想的なプラットフォームになり得る。このセクションでは、モバイルセキュリティ全般ではなく、クラウドセキュリティに影響を与える部分だけを取り上げる。

モバイルコンピューティングの（クラウドの文脈における）基本的なセキュリティの問題は、携帯電話やタブレットも一般のコンピュータと同じであることを除けば、IoT と非常に似ている。

- デバイスの登録、認証および認可は、問題の共通原因である。 特に（ここでも）、格納された資格情報の使用は問題であり、モバイルデバイスが、クラウド事業者のインフラストラクチャ／ API に直接接続する場合には一層問題となる。攻撃者は、モバイルアプリケーションを逆コンパイルして、格納された資格情報を解読し、クラウドインフラストラクチャを直接操作し、または攻撃するために使用することが知られている。デバイスに保存されているデータは、デバイスの利用者が、悪意を持った攻撃者であるかもしれないという想定も含めて保護されるべきである。
- アプリケーション API も不正アクセスの原因となる可能性がある。 攻撃者は API 接続を盗聴することが知られており、時にはローカルプロキシを使用して自分のデバイスをリダイレクトし、（暗号解読されている可能性が高い）API コールを逆コンパイルしてセキュリティの弱点を探ることが知られている。デバイスアプリケーション内部での証明書のピン留め／検証は、このリスクを軽減するのに役立つ。

モバイルおよびクラウドコンピューティングのセキュリティに関するその他の推奨事項については、CSA のモバイルワーキンググループの最新の調査を参照すること。

14.1.4　サーバレスコンピューティング

サーバレスコンピューティングとは、ある種の PaaS 機能をさらに進めて使う手法で、アプリケーションスタックのすべてまたは一部が、利用者が管理するオペレーティングシステムや、さらにはコンテナすらなくても、クラウド事業者の環境で動作するようになる。

ワークロードを実行しているサーバが常にどこかには存在するので、「サーバレスコンピューティング」という呼称は少し間違っているが、サーバおよびそれらの構成とセキュリティは、完全にクラウド利用者から隠されている。 利用者は、サービスの設定のみを管理し、基盤となるハードウェアやソフトウェアスタックは一切管理しない。

サーバレスには、次のようなサービスがある：

- オブジェクトストレージ
- クラウドロードバランサ
- クラウドデータベース
- 機械学習
- メッセージキュー
- 通知サービス
- コード実行環境（一般的には、クラウド利用者がアップロードしたアプリケーションコードを実行させる特定のコンテナである）
- API ゲートウェイ
- Web サービス

サーバレス機能は、クラウド事業者によって深いところに組み込まれ、イベント駆動型システムや組込み型 IAM およびメッセージングと結合されたもので、利用者によるサーバ、コンテナ、その他のインフラストラクチャの管理なしで、複雑なアプリケーションの構築に利用される場合がある。

セキュリティの観点からは、次のような重要課題がある。

- サーバレスは、クラウド事業者に、非常に高いセキュリティの重い責任を負わせる。事業者を選択することと、そのセキュリティ SLA およびセキュリティ能力を確認することは、極めて重要である。
- サーバレスでは、クラウド利用者は、サーバまたはネットワークログなど、よく使用されるレベルのモニタリングやロギングには、アクセスすることができないだろう。アプリケーションはより多くのロギングを組み込む必要があり、クラウド事業者は主要なセキュリティとコンプライアンスの要求事項を満たすために必要なロギングを、提供する必要がある。
- クラウド事業者のサービスは、さまざまなコンプライアンス要求事項に対して認証または評価証明を受けているかもしれないが、必ずしも、あらゆるサービスがすべての適用される規制に対応しているとは限らない。クラウド事業者は基準適合のマッピングを最新の状態に保つ必要があり、クラウド利用者は自らのコンプライアンス要件の範囲内でサービスを使用することを確実にする必要がある。
- クラウド事業者の管理用ダッシュボードへのアクセスは、サーバレス機能を統合し、使用する唯一の方法であるため、高い頻度のアクセスが行われる。
- サーバレスは、攻撃対象や攻撃経路を大幅に減らすことができ、サーバレスコンポーネントを組み込むことは、アプリケーションスタック全体がサーバレスでない場合でも、攻撃チェーンのリンクを遮断する優れた方法となる。

- 全ての脆弱性検査やその他のセキュリティテストは、クラウド事業者の利用規約を遵守しなければならない。クラウド事業者のインフラストラクチャには、すべてのものがホストされており、正当なテストと攻撃を区別できないため、クラウド利用者はアプリケーションを直接テストする権利がなかったり、範囲を狭めたテストをする必要がある。
- インシデント対応も複雑になる可能性があり、サーバレスベースのインシデントを管理するために、プロセスおよびツールの変更が、間違いなく必要になる。

14.2 推奨事項

- ビッグデータ
  - ビッグデータのツールのセキュリティ機能と重複した場合でも、クラウド事業者の機能を可能な限り（優先して）活用すること。 これにより、クラウドのメタストラクチャと特定のアプリケーションスタックで適切な保護が確実に受けられるようになる。
  - データの収集とデータストレージの両方について、一次ストレージ、中間ストレージ、およびバックアップストレージのそれぞれに暗号化を使用すること。
  - プロジェクトの権限付与マトリクスには、ビッグデータのツールとクラウドプラットフォームのアイデンティティ・アクセス管理の両方を取り入れること。
  - クラウドの機械学習および分析サービスを利用することによるメリットとリスクを十分に理解すること。 プライバシーとコンプライアンスへの影響に特に注意すること。
    - クラウド事業者は、技術的コントロールおよびプロセスコントロールを使用して、利用者データが従業員や他の管理者から見える状態とならないことを確実にする必要がある。
    - クラウド事業者は、分析サービスおよび機械学習サービスが、（利用者のために）準拠しているコンプライアンス標準を明確に公表すべきである。
    - クラウド利用者は、セキュリティ、プライバシー、またはコンプライアンスの要求事項を満たしていないサービスを検討する場合、データマスキングまたは難読化の使用を検討すべきである。
  - ツールベンダ（またはオープンソースプロジェクト）および Cloud Security Alliance によって提供されるもの等の、本書以外のビッグデータセキュリティの実践規範に従うこと。
- IoT(モノのインターネット)
  - デバイスが、パッチが当てられたり、アップデートができることを確認すること。
  - クラウドアプリケーションやインフラストラクチャのセキュリティ侵害につながる可能性があるので、デバイスに資格情報を静的に格納しないこと。
  - クラウド側アプリケーションに対しデバイスの登録および認証をセキュアに実行するための実践規範、典型的にはアイデンティティ連携の標準の利用を遵守すること。
  - 通信を暗号化すること。
  - セキュアなデータ収集パイプラインを使用し、データをサニタイズして、データ収集パイプラインへの攻撃によるクラウドアプリケーションまたはインフラストラクチャの悪用を防ぐこと。
  - 全ての API 要求に悪意があると想定すること。
  - CSA の IoT ワーキンググループによって発行された、より詳細なガイダンスに従うこと。
- モバイル
  - クラウドインフラストラクチャに直接接続するアプリケーションを設計する際に、モバイルデバイスの適切な認証および認可に関するクラウド事業者のガイダンスに従うこと。

- モバイルデバイスアプリケーションをクラウド上のアプリケーションに接続するには、業界標準（通常はアイデンティティ連携）を使用すること。
- 暗号化されていない鍵または資格情報をインターネット経由で送信しないこと。
- 悪意のある攻撃者が、認証された暗号化されていないアクセスをすることを想定して、すべての API をテストすること。
  - モバイルアプリケーション内での証明書のピン留めおよび検証を検討すること。
  - セキュリティの視点ですべての API データを検証しサニタイズすること。
  - API における悪意のある活動に対する、サーバ／クラウド側のセキュリティ監視を実装すること。
- デバイスに保管されているすべてのデータのセキュリティを確保し、確実に暗号化すること。
  - アプリケーションスタックへの侵入を許す元となり得る秘匿されたデータは、悪意のあるユーザがアクセスする可能性のあるデバイス上にローカルに格納すべきではない。
- CSA の Mobile ワーキンググループにより発行されたより詳しい推奨事項および研究に従うこと。

- サーバレスコンピューティング
  - クラウド事業者は、どの PaaS サービスがどのコンプライアンス要件または基準に対して評価を受けているかを明確にしなければならない。
  - クラウド利用者は、法令遵守およびガバナンス上の義務の要件を満たすサーバレスサービスのみを使用しなければならない。
  - 攻撃対象またはネットワークからの攻撃経路を縮小または除去するアーキテクチャを使用して、サーバレスコンポーネントをアプリケーションスタックに組み込むことを検討すること。
  - セキュリティアセスメントおよび監視へのサーバレスの影響を理解すること。
  - クラウド利用者は、サーバおよびネットワークのログよりも、アプリケーションコードのスキャンとログを活用する必要がある。
  - クラウド利用者は、サーバレスの配備に向けて、インシデント対応プロセスを更新する必要がある。
  - クラウド事業者は、サーバレスプラットフォームのレベルより下層のセキュリティに責任があるが、クラウド利用者は依然として、サーバレス製品を適切に構成設定して使用することに対する責任がある。

以上