クラウド時代の ITAM の考え方

平成 28 年 2 月

一般財団法人日本情報経済社会推進協会

はじめに

近年、クラウドの利用がビジネスの世界にとって必要不可欠な時代となってきた。しかしながらセキュリティやライセンスのコンプライアンス、TCO の問題、ICT ガバナンス等、クラウドサービス提供者及び利用者がどのように実現するかはビジネス上の重要な課題となっている。

クラウドコンピューティングもソフトウェアの利用方法の一形態と考えられるため、クラウドコンピューティングという新しい形態で何をどう管理すればよいのか、どのような点に留意する必要があるのかを IT 資産管理（IT Asset Management：ITAM）の側面から調査研究することとした。

本書は、「クラウド時代の ITAM の考え方」について解説するとともに、ITAM の観点からクラウド利用の留意点を取りまとめたものである。本書が企業・団体における IT 資産管理に携わる方々のお役に立てば幸いであり、IT 資産管理の普及促進に資することが期待される。

平成 28 年 2 月

一般財団法人日本情報経済社会推進協会
IT 資産マネジメント評価検討委員会

目次

1. 序文

今日のクラウドコンピューティングでは、複雑な ICT の運用をすることなく、コストを最小限に抑え、直ちにビジネスを立ち上げることができると言われている。利用者にとってはバラ色の世界であるが、本当にそうなのであろうか？確かに個人で利用しているとき、いわゆる B to C では、Web ブラウザーさえ動作すれば、大量のドキュメントや写真を保管してくれるし、メールや知り合いとのコミュニケーションも可能だ。簡単なワープロや表計算、プレゼンテーション資料までできてしまう。移動先でも簡単に利用でき、移動中のスマートフォンからもアクセスできる。更に個人の PC よりは信頼がおける管理をしてくれる。このようにクラウドコンピューティングという非常に有効な仕組みがビジネスの世界に入ってきた。セキュリティやライセンスのコンプライアンスや TCO（Total Cast of Ownership）の問題、企業における ICT のガバナンスをどうするかを適切に考え対応しておかなければ、これまで以上に大変なことになることが予想される。

クラウドコンピューティングは、どの層までのサービスを受けるかで、SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）、DaaS（Desktop as a Service）などと分類して説明されることが多い。ビジネスに使われるということから、セキュリティや品質面の安心感を求めて、雲の向こうのサービスを自分の組織だけで利用する形態も提唱されている。これを通常のクラウドコンピューティングと区別して「プライベートなクラウドコンピューティング」と呼んでいる。因みに従来のものは「パブリックなクラウドコンピューティング」という。分類は様々だが、クラウドコンピューティングでは、ICT リソースの物理的な構成にとらわれず（仮想化）、ユーザーの要求に応じて迅速に割り当て提供される（プロビジョニング）という共通の特徴がある。クラウドコンピューティングを導入すれば ICT の運用管理がなくなるとか、IT 資産管理が楽になるとよく言われるが、ビジネスの分野では ICT を会社の経営資源として管理しなければならない範囲が広がることで、サービスを提供するソフトウェアや関連する資産の管理が発生し、これまでより管理が一層困難になる場合も多い。そこで我々は、一般的な企業や団体に適用され始めたクラウドコンピューティングで何をどう管理してゆけば良いのかを、改めて考察することは非常に有意義であると考えた。

本書では、「クラウド時代の ITAM の考え方」をまとめている。即ち ICT を利用する企業や団体がクラウドコンピューティングや仮想化技術を利用する際にどのようなマネジメントが必要になるのかを ITAM の延長として捉える。この序文に続く第 2 章では本書に掲載した主な用語について解説する。第 3 章では仮想化とクラウドコンピューティングの定義と分類について解説する。第 4 章ではクラウド時代の ITAM の目的とリスク、クラウド環境における課題と留意点について解説する。最後の第 5 章ではクラウドにおける今後の課題と留意点についてまとめた。

2. 用語の解説

本章では本書に掲載した主な用語について、仮想化に関連する用語、クラウドコンピューティングに関連する用語、ITAM に関連する用語の三つに分類して、それらの用語の意味や使われ方について解説する。

2.1. 仮想化技術関連用語

2.1.1. 仮想化（Virtualization）

サーバー、ストレージ並びにネットワークなどの様々な IT リソースの物理的特性を、そのリソースと相互作用するシステム、アプリケーション並びにエンドユーザーから隠蔽する技法。

2.1.2. プロビジョニング（Provisioning）

ネットワークやシステムリソースなどをユーザーの要求に応じて迅速に割り当てサービスを提供すること。

2.1.3. ハイパーバイザー（Hypervisor）

仮想化を実現するための制御プログラムで仮想化 OS とも呼ばれ、ハードウェア上で直接動作し、その上で複数の OS が動作する。

2.1.4. クライアント仮想化 OS（Client virtualization OS）

クライアント自身で動作する仮想化 OS であり、通常はクライアント OS（ホスト OS と呼ぶ）上で動作し、他の複数の OS（ゲスト OS と呼ばれる）を動作させる。VMware Workstation、Microsoft Virtual PC などが代表的な製品である。

2.1.5. シンクライアントシステム（Thin client system）

クライアント端末に最低限の機能しか持たせず、サーバー側でアプリケーションソフトやファイルなどの資源を管理するシステムアーキテクチャである。一般的には以下の 4 つの実装方式がある。

- ネットワークブート方式
- サーバーベース方式
- ブレード PC 方式
- 仮想 PC 方式

本書の DaaS でのシンクライアントは、仮想 PC 方式を想定している。

2.1.6. ネットワークブート方式（Network boot）
シンクライアントの実装方式の一つで、サーバー側に OS やアプリケーションを置き、実行時にサーバーから端末に転送し実行する方式。

2.1.7. サーバーベース方式（Server base）
シンクライアントの実装方式の一つで、アプリケーション実行など全ての処理をサーバー上で行い、端末側は遠隔操作端末としての役割のみを担う方式。

2.1.8. ブレード PC 方式（Blade PC）
シンクライアントの実装方式の一つで、デスクトップ環境 1 台毎に用意したブレードをネットワーク越しに操作する方式。

2.1.9. 仮想 PC 方式（Virtual PC）
シンクライアントの実装方式の一つで、 サーバーOS で仮想 OS を実行させ、複数のブレード PC のように見せてネットワーク越しに操作するものである。

2.1.10. VDI（Virtual Desktop Infrastructure）
デスクトップ OS 環境をサーバー側の仮想マシン上に実装・集約するための基盤システム。

2.2. クラウドコンピューティング関連用語

2.2.1. クラウドコンピューティング（Cloud computing）
ネットワークを介してサーバー・ストレージなどのハードウェア、OS・ミドルウェア･アプリケーションなどのソフトウェアを利用する IT サービスの利用形態の一つ。IT リソースの仮想化とプロビジョニング技術を活用し、高可用性を得ていることが多い。IT の「購入から利用へ」という流れの中で急速に普及しつつある。

2.2.2. クラウド（Cloud）
クラウドコンピューティングの略称。

2.2.3. クラウドサービス（Cloud service）
クラウドコンピューティングにより提供される IT サービス。

2.2.4. オンプレミス（On-premises）
サーバー等を「(ユーザー企業の）自社施設内」に設置し運用する IT サービスの利用形態の一つ。これに対しサーバーを自社施設外に設置し運用することを「オフプ

レミス（Off-premises)」と呼ぶ。「オンプレミス」は本来「クラウド」の反対語ではないが、世の中の IT サービスの利用形態が「オンプレミス」から「クラウド」に急速に移行しているためしばしば「オンプレミス」は「クラウド」と対比して用いられる。

2.2.5. プライベートクラウド（Private cloud）

単一組織によって独占的に利用されるクラウドサービス（NIST 定義)。一般的には企業のファイヤーウォールの内側に存在する個別企業ないしはグループ企業向けのクラウドサービスを指す。

2.2.6. コミュニティクラウド（Community cloud）

特定のコミュニティの利用者を対象に提供されるクラウドサービス（NIST 定義)。プライベートクラウドとパブリッククラウドの中間的な形態と位置付けられるが、我が国では一般的でないため本書では採り上げない。

2.2.7. パブリッククラウド（Public cloud）

多種多様な企業や組織、個人といった不特定多数の利用者を対象に広く提供されるクラウドサービス（NIST 定義)。一般的には企業や組織、個人がインターネットを介して自由に利用できるオープンなクラウドサービス。

2.2.8. ハイブリッドクラウド（Hybrid cloud）

本来の意味は、「パブリッククラウド、プライベートクラウド並びにコミュニティクラウドのうち２つ乃至それ以上の形態を併用するクラウドサービス」（NIST 定義)。我が国ではユーザー企業の自社施設内（オンプレミス）の IT リソースを残存させつつ、部分的に「パブリッククラウド」、「プライベートクラウド」を併用して、目的とするサービスを実現する IT サービスの複合的利用形態を指す場合がある。

2.2.9. クラウドサービスモデル（Cloud service model）

クラウドサービスの階層別モデル。SaaS、PaaS、IaaS などの形態があり、各モデルの定義は後述の通りである。各モデルの提供事業者に注目すると、SaaS 事業者ではハードウェアからアプリケーションソフトまで一貫して自社で提供するケース（垂直モデル）と、OS・ミドルウェア以下のサービスは専門の PaaS 事業者（又は IaaS 事業者）に委託するケース（水平モデル）がある。近年特に PaaS/IaaS 事業者の寡占化傾向が強まっており、多くの SaaS 事業者がこれら PaaS/IaaS 事業者の提供する IT 基盤を利用して自社のアプリケーションサービスを展開している。

2.2.10. SaaS（サース：Software as a Service）

アプリケーションソフトウェアをネットワーク経由でクラウドサービスとして提供する形態。自社でデータセンターを保有していなくても、アプリケーションさえ保有していれば、他の PaaS 事業者/IaaS 事業者の顧客となることで、SaaS 事業者となることができる。

2.2.11. PaaS（パース：Platform as a Service）

OS・ミドルウェアなど、アプリケーションソフトウェアのプラットフォームとなる階層の IT リソースをクラウドサービスとして提供する形態。後述の IaaS 事業者がサーバー・ストレージの提供に加えて、OS・ミドルウェアまで提供することで PaaS 事業者に転ずるケースが多い。

2.2.12. IaaS（イアース：Infrastructure as a Service）

サーバー・ストレージなど、OS・ミドルウェアのインフラストラクチャとなる階層の IT リソースをクラウドサービスとして提供する形態。基本的にデータセンターを保有していないと、IaaS 事業者にはなれない。また多くの IaaS 事業者がサービスメニューに OS・ミドルウェアを加えて PaaS 事業者を兼ねることが多い。

2.2.13. DaaS（ダース：Desktop as a Service）

本書では、サーバーの仮想化 OS 上に複数のデスクトップ環境をクラウドコンピューティングのサービスとして提供する形態を言う。技術的には、仮想 PC 方式のシンクライアントシステムのサービスに相当する。尚、データベース機能をクラウドで提供する Database as a Service や、データストレージ機能をクラウドで提供する Data Storage as a Service を DaaS と呼ぶこともある。

2.3. ITAM 関連用語

2.3.1. SAM（Software Asset Management）

ソフトウェア資産からの価値を実現するための組織の協調的な活動。

注：組織内のソフトウェア資産の有効な管理、制御及び保護並びに、ソフトウェア資産管理に必要な関連資産に関する情報の有効な管理、制御及び保護などを含む。

2.3.2. IT 資産（Information Technology Asset）

デジタル情報を取得し、処置し、保存し、拡散できるとともに組織の潜在的な又は実際的な価値を持つ品目、物あるいは、実体。

注：ソフトウェア、メディア（物理的/デジタル）、ハードウェア、ドキュメント（契

約書類を含む物理的又はデジタル媒体のドキュメント)、ライセンス（権利書（entitlement）ともいう)、ライセンスの証拠、及びこれらの資産を管理するために必要なメタデータなどを含む。

2.3.3. ITAM（Information Technology Asset Management）

IT 資産からの価値を実現するための組織の協調的な活動。

2.3.4. SLA（Service Level Agreement）

サービス品質に対する利用者側の要求水準と提供者側の運営ルールについて明文化したものである。

2.3.5. SLM（Service Level Management）

サービスに関わるルール、プロセス、体制などの改善により高品質なサービスを維持し、サービスレベルの要求水準とサービス内容を利用者の事業上の要求の変化に対応させるための継続的な運営・管理手法である。

2.3.6. EULA（End User License Agreement）

ソフトウェア利用許諾契約またはソフトウェア使用許諾契約が書かれた契約書のこと。ソフトウェアの著作権者が、そのソフトウェアを利用するユーザーに示す利用条件を表している。

2.3.7. ISMS（Information Security Management System）

個別の問題ごとの技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用するための仕組み。組織が保護すべき情報資産について機密性、完全性、可用性をバランス良く維持し改善することを基本コンセプトとする。

2.3.8. マッシュアップ（Mash up）

複数の Web サービスの API を組み合わせ、あたかも一つの Web サービスのようにすること。音楽用語に由来する。

2.3.9. XML（Extensible Markup Language）

文書やデータの意味や構造を記述するためのマークアップ言語であり、マークアップ言語作成にも使われる汎用的な仕様。

2.3.10. プロプライエタリ・ソフトウェア（proprietary software）

ソフトウェアの使用、改変、複製を法的・技術的な手法を用いて制限しているソフトウェアを指す。法的制限手法としては、著作権や特許権及びそれに基づくソフトウェアライセンス許諾といった方法がある。技術的制限手法としては、バイナリ実行コードのみをユーザーに提供し、ソースコードは公開しないというソフトウェア流通の方法がある。

2.3.11. コピーレフト（copy left）

著作権（copyright）に対する考え方で、著作権を保持したまま、二次的著作物も含めて、すべての者が著作物を利用・再配布・改変できなければならないという考え方である。

3. 仮想化とクラウドコンピューティング

本章では、ITAM における仮想化、クラウド利用時の留意点について検討するに当たり、第２章で定めた「仮想化、クラウド」の定義に従い、それぞれの現状説明とサービス事例について解説する。

表 3-1　仮想化、クラウドの用語定義（第２章より）

#	用語	本書における定義
1	仮想化	サーバー、ストレージ並びにネットワークなどの様々な IT リソースの物理的特性を、そのリソースと相互作用するシステム、アプリケーション並びにエンドユーザーから隠蔽する技法。
2	クラウド	ネットワークを介して、サーバー・ストレージなどのハードウェア、OS 及びミドルウェア、アプリケーションソフトウェアなどの IT リソースを即時に迅速かつ効率的に利用できる、IT サービスの利用形態。

3.1. 仮想化

3.1.1. 仮想化の定義

仮想化（Virtualization）とは、（サーバー、ストレージ並びにネットワークなどの）様々な IT リソースの物理的特性を、そのリソースと相互作用するシステム、アプリケーション並びにエンドユーザーから隠蔽する技法である。この技法により単一の物理リソースを複数の論理リソースに見せかけたり、逆に複数の物理リソースを単一の論理リソースに見せかけたりすることができる。前者の具体例として、１台の大型サーバーをあたかも複数台のサーバーであるかのように論理的に分割し、それぞれに別の基本ソフトウェアやアプリケーションソフトを動作させて複数の顧客が利用する「サーバー仮想化」がある。また後

者の具体例として、複数のディスクをあたかも 1 台のディスクであるかのように扱い大容量のデータを一括保存したり耐障害性を高めたりする「ストレージ仮想化」が実用化されている。更に近年では、世界各地に分散する複数のサーバー群に跨るシステムをあたかも一つのシステムのように運用する、地球規模でのグローバル仮想化システムも実用化されつつある。

仮想化という用語自体の歴史は古く、1960 年代から広く用いられている。初期のコンピュータはメモリー上に 1 つのプログラムしか呼び出せなかった。そのため 1 つのプログラムがリソースをすべて占有していた。これでは高価なコンピュータの利用効率が上がらないので、1 台のコンピュータを複数のユーザーで同時利用するための研究・開発が始まり、TSS（Time Sharing System）や仮想記憶などの技術が登場した。これらはコンピュータの限られた物理リソースを論理的に分割して、ユーザーごとに割り当てる（多重化）と共に、ユーザープログラムから物理リソースを隠蔽して、より使いやすい論理的な利用環境を提供することを目的としていた。これらの技術はその後、オペレーティングシステム（OS : Operating System）へと発展し、現在では OS の標準機能となっている。

このように、コンピュータ発展の歴史は仮想化の積み重ねともいえる。その後も様々な仮想化技術が登場しているが、いずれの場合も共通する目的は「カプセル化によって実装技術の詳細を隠蔽すること」である。近年ハードウェアの性能向上と共に新たな仮想化技術が登場し、この歴史ある用語・概念が再び注目されている。

なお、仮想化＝隠蔽という意味から、本項には「クラウド」と共通する項目が多く見られるが、ここでは「仮想化」の技術的側面を中心に記述し、ビジネス的側面としての「クラウド」に関する課題は後述する。

3.1.2. 仮想化の分類

「仮想化」という用語は、現在コンピュータ以外の分野においても様々な文脈で用いられている。そのため仮想化を「複雑な実装を隠蔽し、単純化されたユーザーインタフェースを提供するもの」と定義するだけでは議論が混乱する恐れがある。そこで本書ではまず IT プラットフォームの仮想化について解説する。続いて仮想化技術の代表的な実用例として、サーバー仮想化、ストレージ仮想化、ネットワーク仮想化、デスクトップ仮想化（クライアント仮想化）の 4 つを解説する。

表 3-2　仮想化の分類

#	分類
1	IT プラットフォームの仮想化
2	IT リソースの仮想化 (1)　サーバー仮想化

	(2)　ストレージ仮想化 (3)　ネットワーク仮想化 (4)　デスクトップ仮想化

3.1.2.1. IT プラットフォームの仮想化

IT プラットフォームの仮想化とは、あるコンピュータのハードウェア上で制御プログラムが擬似的なコンピューティング環境を生成し、その環境上で稼働するゲストソフトウェアに対して「仮想機械（Virtual Machine)」を提供するものである。単一の物理マシン上で複数の仮想機械を動かすことができるため、様々なソフトウェアの開発、テスト、シミュレーションなどに用いられる。プラットフォーム仮想化には、エミュレータまたはシミュレータなどのソフトウェアを使用する方法、同一プラットフォーム上でネイティブに仮想化を実現する方法、ハードウェア自体が隔離された状態で動作できるハードウェア仮想化と呼ばれる方法などがある。

3.1.2.2. IT リソースの仮想化

上記のプラットフォーム仮想化の概念から発展し、演算装置、補助記憶装置、回線終端装置、端末装置など特定の IT リソースを仮想化するシステムが実用化されている。ここではそれらの代表例を 4 つ解説する。

(1)　サーバー仮想化

サーバーの仮想化とは単一の物理サーバーをあたかも複数のサーバーであるかのように論理的に分割し、それぞれに別の基本ソフトウェアやアプリケーションソフトウェアを動作させる技術である。具体的には、単一サーバー内に OS からアプリケーションまで含めた分割領域を複数設定し、それぞれの領域が独立して動作するものである。この分割領域をそれぞれ「仮想サーバー」と呼ぶ。仮想サーバーは単一のサーバー上で動作しながら、お互いに悪影響を及ぼすことがないように設計・設定されているので、仮にある仮想サーバーの OS やアプリケーションソフトウェアがダウンしても、他の仮想サーバーは稼動し続けることができる。サーバー仮想化を一言で表現すると「複数の物理サーバーをそのまま単一の物理サーバーに移行・集約する技術」である（図 3-1)。

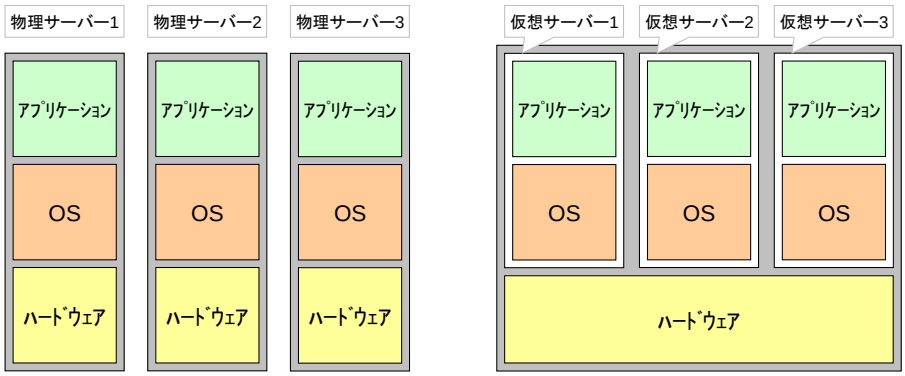


図 3-1　サーバー仮想化の基本概念

サーバー仮想化には、ホスト OS の上にゲスト OS を稼働させる方法、ハイパーバイザーと呼ばれるファームウェアの上に複数 OS を稼働させる方法、ハードウェア自体にシステムを分割／統合する機能を装備する方法などがある。またグリッドコンピューティング関連技術も、サーバーを統合化して取り扱う仮想化技術の応用といえる。サーバー仮想化技術はこれまでは独立したソフトウェアとして提供されることが多かったが、OS や CPU 製品でサポートするものも登場しつつある。サーバー仮想化のメリットは、前述のように「これまで複数の物理サーバーで行ってきたことを単一の物理サーバー上で実現できる」ということである。サーバー仮想化の導入による代表的なメリットは以下の３点である。

①　サーバー統合によるコスト削減効果

多数の物理サーバーを保持・運用している組織では、各サーバーはそれぞれの処理能力は余裕を持ってキャパシティ設計されているため、全てのサーバーが常時フル稼働している訳ではなく、極端に利用率が低いサーバーも存在する。これを一台の大型サーバーに移行・集約することで、管理対象となるサーバーの台数を減らすことができる。統合先となる大型サーバーは従来の小型サーバーよりも堅牢な上位機種が必要となる。しかしサーバーの利用に関するコストでは運用管理のための人件費が大きな割合を占めている。そして人件費はサーバーの台数に比例して増加するとも言われている。従って大型サーバーへの買い替え費用を考慮しても、多数の小型サーバーを個別に購入、維持運用するコスト（特に人件費）を削減できる効果は大きいと考えられる。更にサーバーを多数稼動させることは大量のサーバー電力消費と発熱（空調電力消費）につながる。このような環境負荷を軽減し、グリーンコンピューティングを実現することも、サーバー統合すなわちサーバー仮想化の副次的効果と考えることができる。

②　プロビジョニングによる安定稼動効果

サーバー仮想化技術によって仮想サーバー同士がリソースを共有できるようになれば、

異なるアプリケーション間でリソースを融通し合ったり、予備のリソースをプール（集約管理）したりできる。特定の仮想サーバーの処理負荷が高まった時、この予備のリソースを追加で割り当てることで、サーバーの稼動を止めずに特定の仮想サーバーの性能をアップさせることができる。このような処理負荷の増減に応じたITリソースの動的再配置による最適化はプロビジョニングを呼ばれ、システムの安定稼働やディザスタリカバリのソリューションとして有効である。

③　コンピューティング環境整備の短工期化

あるアプリケーションソフトウェアを新規に導入したり、開発環境や検証環境を整備したりする際に、サーバーの調達に時間を要することがある。仮想化サーバーを利用することにより、必要なときに必要なサーバー環境を即座に設定し、役割が終われば即座に撤収することもできるので、新規アプリケーションソフトウェアの導入コストの削減や、開発や検証に係る作業効率の向上策として大変有効である。

(2)　ストレージ仮想化

ストレージ仮想化とは、複数のストレージ装置を論理的に集約する技術である。基本的にはサーバー仮想化の一領域とも考えられるが、ストレージの構成要素はサーバーほど複雑ではないため、むしろサーバー仮想化（サーバー統合）よりも先行して普及している。近年特に企業のインターネットサービスの拡充、動画サービスの増加、ビッグデータの本格的導入等に伴い、ストレージ装置の台数や容量も急速に増大している。近年このデータやストレージ装置の増加がシステム構成を複雑化し、コストを押し上げる大きな一因となりつつある。

ところで、サーバー仮想化が基本的には「複数の物理サーバーで行ってきたことを単一のサーバー上で実現する」こと、すなわち「サーバー統合」とほぼ同義であるのに対し、ストレージ仮想化には、統合と分割という二つの意味があるので、注意しなければならない。現在主流となっているストレージ仮想化は、複数の物理ストレージ装置を仮想的に単一の論理ストレージ装置（ストレージプール）に見せるという考え方である（図3-2左）。もうひとつの考え方は単一の大型物理ストレージ装置を仮想的に複数のストレージ装置に見せるというものである（図3-2右）。これはサーバー仮想化（サーバー統合）と同じ狙いであり、多数のストレージ装置を管理・運用する負荷を削減するために既存の小型ストレージ群を1台の大型ストレージ装置に統合することを目的としている。両者はあたかも正反対の行動に見えるが、「物理的な実装を隠ぺいして仮想的なユーザーインタフェースを提供する」という点では仮想化の定義に合致している。それぞれのユーザーの目的が「小型ストレージをあたかも大型ストレージのように利用したいか」あるいは「大型ストレージをあたかも小型ストレージのように利用したいか」という点が異なるだけである。

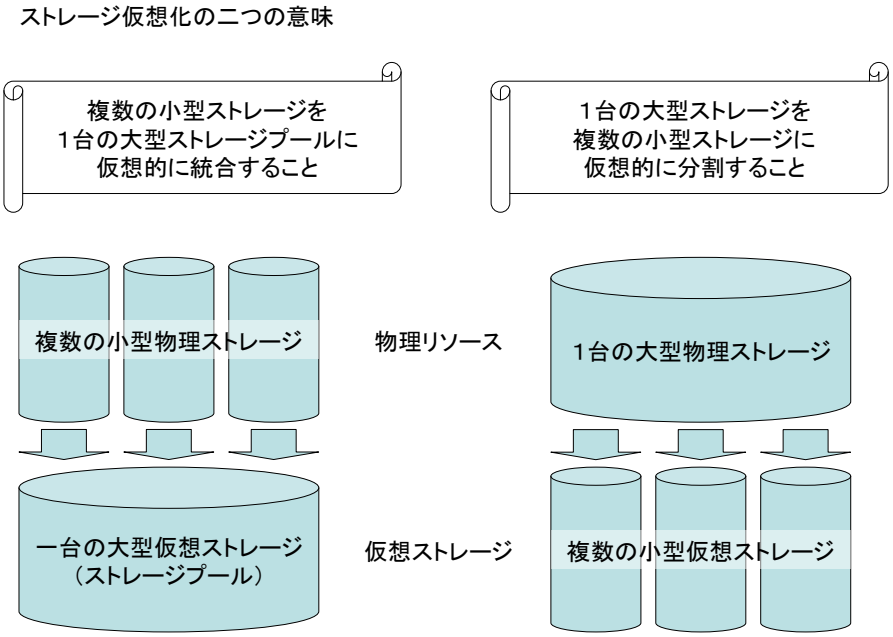


図 3-2　ストレージ仮想化の基本概念

(3)　ネットワーク仮想化

ネットワーク仮想化とは、ネットワーク機器を個別に用意するのではなく大型サーバーの内部に仮想的にルーター／スイッチ、セキュリティ・アプライアンスといったネットワーク機器を準備し、柔軟に組み合わせて使うものである（図 3-3)。サーバー仮想化のネットワーク機器版とも考えられる。システム変更の効率化が最大のメリットである。

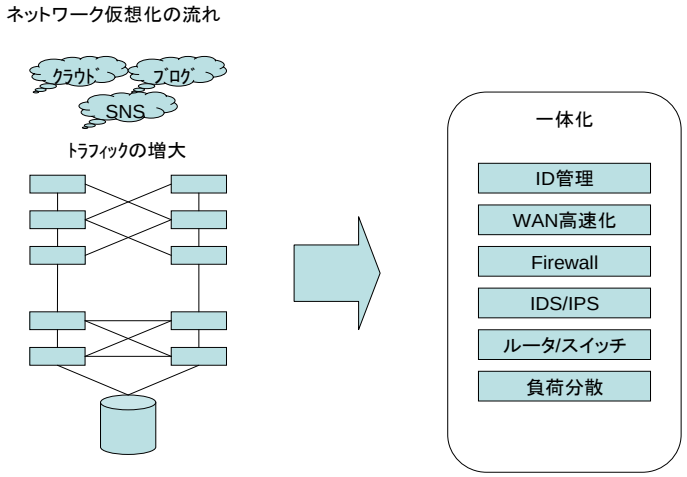


図 3-3　ネットワーク仮想化の基本概念

(4)　デスクトップ仮想化（クライアント仮想化）

デスクトップ仮想化（またはクライアント仮想化）とは、仮想化技術を利用して PC の運用管理を効率化するための技術の総称である。PC の運用管理の負荷は PC 台数の増加に比例して増大する。そこで PC 用ソフトウェアの実行をサーバー側で行ない、PC はユーザーインタフェースとしての役割のみに徹するという考え方が生まれた。これにより PC の OS やアプリケーションソフトウェアをサーバー側で一元管理できるようになる（図 3-4）。仮想化の対象をアプリケーションソフトウェアまでとして PC 側の OS を利用するものをアプリケーション仮想化と呼び、OS まで含めて全てサーバー側で実行するものを OS 仮想化と呼ぶ。デスクトップ仮想化の主なメリットは以下の通りである。

①　アプリケーションやデータを集中管理できる。

②　サーバー側でポリシー設定を行うことでユーザー別にアクセス制御ができる。

適用例として、正社員と派遣社員で利用可能なアプリケーションを区別することができる。最近では外注業者を社内に常駐させてシステム開発を委託する場合に、アプリケーション仮想化を利用する例が増えている。あるいは旧式のアプリケーションソフトウェアと最新のアプリケーションソフトウェアを同じ PC 上で動作させることもできる。

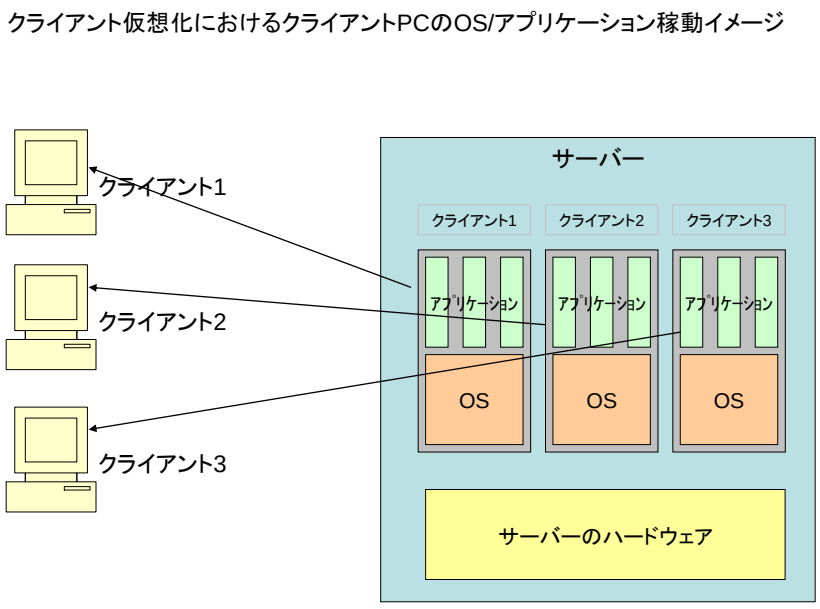


図 3-4　クライアント仮想化の基本概念

3.1.3. 仮想化と ITAM

以上で代表的な「仮想化」概念について解説した。仮想化技術を基盤とする「クライド時代の ITAM」の留意点については第 4 章以下で詳説するが、ここで若干の課題提示を行う。

(1)　一般的な注意点

仮想サーバーのソフトウェアのライセンス料は一般的に仮想サーバー単位で発生するものが多い。即ち仮想サーバーの設定毎にそれぞれライセンス料が必要になる。

(2)　仮想サーバーの追加・削除時の注意点

仮想サーバーは容易に追加・削除が可能なのでライセンス管理が甘くなりがちである。仮想サーバーの追加・削除時にライセンス変更も連動するような、変更管理のルール作りが求められる。

(3)　ソフトウェアベンダーの対応

サーバー仮想化が定着しつつある中でソフトウェアベンダー各社も柔軟なライセンス体系を導入しつつある。CPU 課金体系を大別すれば、物理サーバーの CPU 数、仮想サーバーに割り当てられた CPU 数のいずれかをカウントすることになる。仮想サーバーに割り当てられた CPU 数によって課金される場合、仮想サーバーの特徴である CPU 数の動的配置への対応が課題となる。

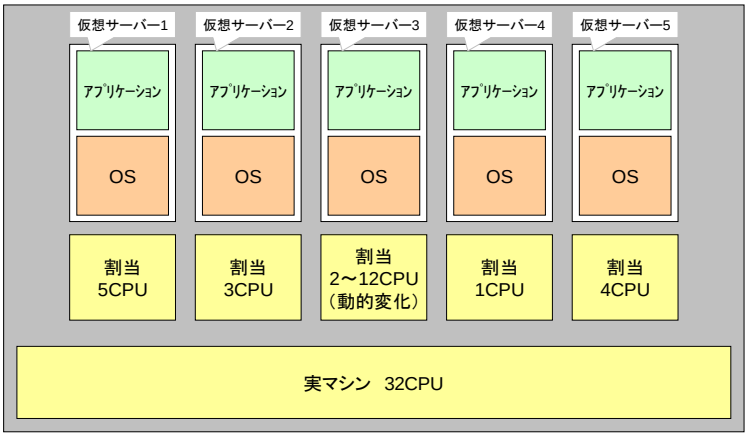


図 3-5　サーバー仮想化におけるライセンス課金問題

3.2. クラウドコンピューティング

3.2.1. 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（Cloud computing）とは、ネットワークを介してサーバー・ストレージなどのハードウェア、OS・ミドルウェア・アプリケーションなどのソフトウェアを利用できる IT サービスの利用形態の一つであり、構成可能な共有プール化された IT

リソースを必要時に迅速かつ効率的に利用できる点が特徴である。クラウドとは「雲」という意味であるが、これは情報システムのネットワーク構成図を描く際に、インターネット全体という意味で「雲」の絵を慣習的に使用することに由来するとされている。利用者がインターネット（雲）の先に用意されている IT リソースの実装の詳細を知らないまま（あるいは気にせずに）それらのリソースを利用することから、「クラウドコンピューティング」と呼ばれるようになった。（以下「クラウド」と略称する。）

クラウドは５つの基本特性を有する。まず①オンデマンド性、すなわちインターネット回線とブラウザーがあればユーザーは必要なリソースを必要な時に利用できる。次に②ネットワークアクセス性、すなわち必要な全ての IT リソースがネットワーク経由で提供される。そして③IT リソースプール、すなわちハードウェア、OS 及びミドルウェア、アプリケーションソフトウェアなどの IT リソースは共有プールとして蓄積され、必要時に（契約に基づき）必要な量を呼び出し、必要な形態に構成することができる。更に④システムの迅速性、すなわちシステム構築や運用管理の専門知識がなくても、業務に必要な情報システムを短期間に構築し、従来とは比較にならない早さで利用に供することができる。最後に⑤サービスの計測可能性、すなわちすべてのサービス品質がネットワーク経由で計測可能であり、それ故 SLA（サービスレベルアグリーメント）がクラウド運用の鍵となる。

クラウドで提供されるリソースの所有権並びに一次使用権は一般的にサービス提供者（サービスプロバイダ）側にあり、費用もサービス単位の期間課金制あるいは従量課金制を採用するものが多い。顧客企業側から見ると「IT の所有から利用へ」というパラダイムシフトが起きており、社会的にも大きな注目を集めている。

本書ではアメリカ国立標準技術研究所（National Institute of Standards and Technology、NIST）によるクラウドコンピューティングの定義を幅広く引用する。以下の文書は IPA のサイトから入手可能である。[1]

> クラウドコンピューティングは、共用の構成可能なコンピューティングリソース（ネットワーク、サーバー、ストレージ、アプリケーション、サービス）の集積に、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り当てられ提供されるものである。このクラウドモデルは５つの基本的な特徴と３つのサービスモデル、および４つの実装モデルによって構成される。
>
> アメリカ国立標準技術研究所（National Institute of Standards and Technology、 NIST）

[1] https://www.ipa.go.jp/files/000025366.pdf

【５つの基本特性（Essential Characteristics)】

① オンデマンドセルフサービス（On-demand self-service）
② 幅広いネットワークアクセス（Broad network access）
③ リソースの共用（Resource pooling）
④ スピーディーな拡張性（Rapid elasticity）
⑤ サービスが計測可能であること（Measured service）

【３つのサービスモデル（Service Models)】

① SaaS (サービスの形で提供されるソフトウェア:利用者に提供される機能はクラウドのインフラストラクチャ上で稼働しているプロバイダ由来のアプリケーションである。)
② PaaS (サービスの形で提供されるプラットフォーム:利用者に提供される機能はクラウドのインフラストラクチャ上にユーザーが開発したまたは購入したアプリケーションを実装することである。)
③ IaaS (サービスの形で提供されるインフラストラクチャ : 利用者に提供される機能は演算機能、ストレージ、ネットワークその他の基礎的コンピュータリソースを配置することである。そこでユーザーはオペレーティングシステムやアプリケーションを含む任意のソフトウェアを実装し走らせることができる。)

【４つの実装モデル（Deployment Models)】

① プライベートクラウド（Private cloud）: クラウドのインフラストラクチャは、複数の利用者から成る単一の組織の専用使用のために提供される。存在場所はその組織の施設内または外部となる。
② コミュニティクラウド（Community cloud）: クラウドのインフラストラクチャは、共通の関心事を持つ複数の組織から成る特定の利用者の共同体の専用使用のために提供される。
③ パブリッククラウド（Public cloud）: クラウドのインフラストラクチャは広く一般の自由な利用に向けて提供される。
④ ハイブリッドクラウド（Hybrid cloud）: クラウドのインフラストラクチャは二つ以上の異なるクラウドインフラストラクチャ（プライベート、コミュニティ又はパブリック）の組み合わせである。

3.2.2. クラウドコンピューティングの分類（用途別分類）

クラウドは用途別と階層別に分類される。本書ではまず用途別分類に従って解説し、続けて階層別分類（サービスモデル）に従って解説する。

表 3-3　クラウドの用途別分類

(1)　パブリッククラウド
(2)　プライベードクラウド
(3)　ハイブリッドクラウド

(1)　パブリッククラウド

パブリッククラウドとはインターネットを経由して不特定多数の利用者に向けて提供される IT サービスであり、一般的に「クラウド」という場合はこのパブリッククラウドを指すことが多い。パブリッククラウドとは、次項のプライベートクラウドの対義語と考えることもできる。パブリッククラウドを提供する事業者は自社で大規模なデータセンターを保有し、サーバー仮想化技術によってクラウド環境を構築している。また提供される IT 基盤にオープンソースのソフトウェアを積極的に活用して、コスト削減を図っている点も特徴である。

パブリッククラウドの IT リソースは、クラウド事業者の自社施設内（オンプレミス）に設置されているケースと、クラウド事業者が契約しているアウトソーシング事業者の施設（オフプレミス）に設置されているケースがある。この点からも「クラウド」と「オンプレミス」は対義語ではなく、別の概念に基づく用語であることがわかる。

表 3-4　代表的なパブリッククラウドサービス

階層別分類	サービス名	事業者名
SaaS	Salesforce.com	セールスフォース・ドットコム（米国）
	Google Apps for Works	グーグル（米国）
	Microsoft Office 365	マイクロソフト（米国）
PaaS	Force.com	セールスフォース・ドットコム（米国）
	Google App Engine	グーグル（米国）
	Microsoft Azure	マイクロソフト（米国）
IaaS	Amazon Web Services (EC2)	アマゾン（米国）
	Rackspace Cloud Server	ラックスペース（米国）
	Google Compute Engine	グーグル（米国）

(2)　プライベートクラウド

プライベートクラウドは、インターネットやイントラネット等を経由して特定の利用者（顧客企業等）に向けて提供される IT サービスである。顧客企業等はデータセンターのサーバー上で Web アプリケーションソフトウェアを稼働させ、企業内の利用者がイントラネット等を通じて IT サービスを利用する。プライベートクラウドは、クラウド技術を活用しつつ、あくまで IT リソースは顧客企業等が自社の管理下に置いている点が特徴である。パ

ブリッククラウドと比較して、自社のポリシーに基づいたセキュリティマネジメントや IT サービスマネジメント（サービスレベル管理を含む）を反映しやすいことから、大企業や官公庁などで利用が拡大している。

プライベートクラウドは、クラウド技術を活用した新時代のアウトソーシングサービスと考えることもできる。一方、IT リソースが自社保有あるいは自社管理下に置かれるため、そもそもプライベートクラウドはクラウドか否か、というような議論がなされる場合もある。いずれにせよ、（顧客企業等の）利用者が IT の設計・構築・設定・運用・保守などの作業から解放され、ネットワーク経由で IT をサービスとして必要な時に必要なだけ利用できるという点から、クラウド的なアウトソーシング形態であると考えられる。

尚、サーバー等がユーザー企業の自社施設内に設置されていればオンプレミス（自社施設内）のプライベートクラウドであり、アウトソーシング事業者が保有する外部のデータセンターに設置されていればオフプレミス（自社施設外）のプライベートクラウドとなる。従って繰り返しになるが、オンプレミスとクラウドは対義語ではなく、別の概念に基づく分類である。

近年、ハードウェアベンダーによる顧客囲い込み戦略の一環として、ベンダーの用意したクラウド基盤上に顧客企業の社内サーバー群を移行・集約・再構築する動きが急速に進んでいる。顧客企業にとっては全ての IT リソースを仮想化することでより柔軟な IT サービスの提供を受けることが可能となる一方、他社のハードウェア製品への乗り換えは事実上困難となる。この場合も、顧客企業の自社施設内に仮想化サーバー群を構築するケースと、ハードウェアベンダーの保有するデータセンターに顧客企業専用の領域を設けて仮想サーバー群を構成するケースがある。

(3) ハイブリッドクラウド

現在のようなクラウドへの移行期においては、前述のパブリッククラウドとプライベートクラウドの混合型が採用される場合も多い。パブリッククラウドはコスト面では優位だが、機能面では自社のニーズに 100%適合している訳ではなく、またセキュリティ面の不安も払拭できない。その点、自社専用環境に仮想化技術を駆使して構築されたプライベートクラウドは、コスト面では多少割高であっても、様々な安心感を得ることができる。そのため、大企業を中心に、セキュリティ要件の厳しい IT サービスはプライベートクラウドで提供を受け、コスト優先の IT サービスはパブリッククラウドを活用する、という、混合型の IT サービス形態が選択される場合が増えている。

用語定義でも述べたように、ハイブリッドクラウドとは本来の意味は、「パブリッククラウド、プライベートクラウド並びにコミュニティクラウドのうち 2 つ乃至それ以上の形態を併用するクラウドサービス」（NIST 定義）であるが、我が国ではユーザー企業の自社施設内（オンプレミス）の IT リソースを残存させつつ、部分的に「パブリッククラウド」、「プ

ライベートクラウド」を併用して、目的とするサービスを実現する IT サービスの複合的利用形態を指す場合がある。とはいえ、このオンプレミスの IT リソースも大企業を中心にプライベードクラウド形態に移行・集約・再構築されるケースが増加しており、結果的には本来の意味の「複数のクラウド形態を併用するクラウドサービス」に落ち着くことになると思われる。

3.2.3. クラウドコンピューティングの階層（サービスモデル分類）

一方、クラウドは提供するリソースの階層により分類することもできる。これをサービスモデル分類と呼ぶ。それぞれのサービスモデルは、提供するリソースにより「XaaS: Xxxxx as a Service」（サービス型○○：○○はアプリケーション、プラットフォーム、インフラストラクチャなど）という名称で呼ばれる。

表 3-5　クラウドの階層別分類

(1)　SaaS（サース）: Software as a Service（サービス型アプリケーション）
(2)　PaaS（パース）: Platform as a Service（サービス型プラットフォーム）
(3)　IaaS（イアース）: Infrastructure as a Service（サービス型インフラストラクチャ）
(4)　DaaS（ダース）: Desktop as a Service（サービス型デスクトップ）

(1)　SaaS（サービス型アプリケーション）

クラウドコンピューティングのサービスの中でアプリケーションソフトウェアを提供するものであり、かつての ASP（Application Service Provider）とほぼ同義語と考えられる。SaaS という名称は、2004 年頃に米国 Salesforce.com（セールスフォース・ドットコム社）が営業支援用ソフトウェアをインターネットサービスとして提供した頃から広まり始めたとされる。従来型の ASP 事業者によるサービスとは異なり、同社の Salesforce サービスはカスタマイズ性に優れており、自社のアプリケーションとのデータ連携等も自由にできたため、急速に普及していった。

現在米国では、営業支援分野に限らず、グループウェア、セキュリティ管理、財務会計、HR（人事・人材管理）などの各方面で SaaS が急速に普及し始めている。SaaS で提供されるアプリケーションソフトウェアはパッケージソフトウェアと同様、自社でコントロールできる部分は少ない。従って、提供されるサービス内容、サービスレベルが自社の業務に適合していることを確認することが前提となる。

表 3-6　代表的な SaaS

サービス名	事業者名
Salesforce.com	セールスフォース・ドットコム（米国）
Google Apps for Works	グーグル（米国）
Microsoft Office 365	マイクロソフト（米国）

(2)　PaaS（サービス型プラットフォーム）

クラウドコンピューティングのサービスの中で、アプリケーションソフトウェアが稼動する IT プラットフォームを提供するものである。データセンターにあらかじめ用意されたハードウェア、OS、ミドルウェア、フレームワークなどのリソースが、インターネットを経由して期間課金制あるいは従量課金制の IT サービス形態で提供される。

PaaS を利用することで、顧客は必要な IT インフラストラクチャを即座に、必要な期間だけ利用することができる。例えば、アプリケーションソフトウェアの開発業務に PaaS を利用すると、開発用機器の調達が不要となるため、開発プロジェクトの工期（特に立ち上げ準備期間）を短縮することができる。自社データセンターを保有しない SaaS 事業者が、サービス提供基盤として他社の PaaS を利用する例も多い。

表 3-7　代表的な PaaS

サービス名	事業者名
Force.com	セールスフォース・ドットコム（米国）
Google App Engine	グーグル（米国）
Microsoft Azure	マイクロソフト（米国）

(3)　IaaS（サービス型インフラストラクチャ）

クラウドコンピューティングのサービスの中で、ハードウェアやネットワーク回線等の IT インフラストラクチャを提供するものである。顧客はインターネット経由で IT インフラにアクセスし、その上に自ら購入した OS やアプリケーションソフトウェアをインストールして利用する。以前は HaaS（Hardware as a Service）と呼ばれていたが、近年はハードウェアのみならずネットワーク等を含む IT インフラ全体が提供されることが多くなったため、IaaS（Infrastructure as a Service）という用語が広く使用されるようになった。

従来型のホスティングサービスと異なる点は、仮想化技術を活用して仮想インフラを提供する点である。仮想化技術によりユーザーはサーバーやストレージの実装の詳細を気にせずに、IT インフラのサービスを利用できるようになった。

IaaS と PaaS は概ね同じ事業者が提供していることもあり、サービス内容の拡充に伴い、実質的な境界線は近年急速に曖昧になりつつある。

表 3-8　代表的な IaaS

サービス名	事業者名
Amazon Web Services (EC2)	アマゾン（米国）
Rackspace Cloud Server	ラックスペース（米国）
Google Compute Engine	グーグル（米国）

(4)　DaaS（サービス型デスクトップ）

クラウドコンピューティングのサービスの中で、デスクトップ機能を提供するものである。シンクライアント、VDI（Virtual Desktop Infrastructure）などの仮想デスクトップを IT サービスとして提供する。ユーザーは Web ブラウザーがあれば、インターネット経由でどこでも自分の仮想デスクトップを操作できる。仮想デスクトップでは、管理者がサーバー上に複数の仮想マシンを稼働させており、これらの仮想マシンの処理結果画面のみを端末に転送するという仕組みである。端末側はキーボードやマウスなど入力装置の操作情報のみをサーバーに転送する。

DaaS がもたらすメリットは、端末にデータを保存しないためセキュリティや事業継続性の確保が容易である、端末のセキュリティパッチやソフトウェア資産管理などについてサーバー側で一括管理ができる、などの点が挙げられる。

尚、同じ"DaaS"という略称を用いるものに、クラウド形態でデータベース機能を提供する DataBase as a Service、データストレージ機能を提供する Data Storage as a Service などがあり、混同しないようにしなければならない。

表 3-9　代表的な DaaS（Desktop as a Service）

サービス名	事業者名
Microsoft SQL Azure Database	マイクロソフト（米国）
VMware Hrizon DaaS	ヴイエムウェア（米国）
Citrix XenDesktop	シトリックス（米国）

4. クラウド時代の ITAM

4.1. ITAM の目的

クラウドコンピューティング時代における ITAM (IT 資産管理) のあり方を考える上で、我々は ITAM の目的に沿ってこれらを検討してみることが有効であると考えた。一般に ITAM の目的は以下のように整理される（表 4-1)。

表 4-1　ITAM の目的

#	目的
(1)	リスク管理 a) 説明責任 b) 資産保全 c) 法的リスクの回避 d) セキュリティ上の問題への対処 e) 可用性の確保
(2)	コスト管理（TCO 削減等）
(3)	競争上の優位性確保（IT 資産の有効活用）

4.1.1. リスク管理

4.1.1.1. 説明責任

【仮想化技術】

(1)　仮想化に伴う管理範囲の拡大：

仮想化技術を利用することで、これまで物理的な単位に縛られてきた IT リソースを論理的に再配分することが可能となる。IT リソースをフレキシブルに組み合わせることで、効率的かつ安定的に運用することができる一方、組み合わせの最適化に関する説明責任が増加することになる。具体的には IT リソースの構成管理・変更管理、キャパシティ管理の範囲が拡大かつ複雑化することが想定される。

①　構成管理・変更管理：仮想化環境下では、IT リソースの物理的な構成に加えて論理的な構成も管理しなければならない。一般に論理構成は物理構成と比較して変更が容易なため、変更管理の機会が飛躍的に増加する。また論理構成は目に見えないため現状及び変更の視認が難しいという問題がある。

②　キャパシティ管理：仮想化環境下では IT リソースを論理的に構成するため、その組み合わせが飛躍的に増加する。従来はハードウェア機器など物理構成単位での CPU やメモリー利用率などを管理しておけばよかったが、仮想化環境下では論理構成単位でのパフォーマンス管理、キャパシティ管理が求められる。

(2)　仮想化に伴うライセンス管理体制の再検討の必要性：

仮想化環境でのソフトウェアの利用に伴い、これを前提としたライセンス管理体制が必要となる。尚、仮想化環境で利用されるソフトウェアは以下のように分類される。

①　仮想環境を構成あるいは管理するための OS、ミドルウェア

②　仮想マシン上で個別に利用されるアプリケーションソフトウェア

③　仮想マシン上で共通に利用されるアプリケーションソフトウェア

(3)　仮想化環境に合わせたソフトウェアの最適化の必要性：

仮想化環境下では従来型のアプリケーションが十分なパフォーマンスが発揮できない場合がある。例えば従来型の PC アプリケーションを仮想化環境に載せ替えただけでは、多数の PC が特定のリソースに一気に集中し、想定外の負荷が発生し十分なパフォーマンスを得られないことがある。そのため仮想化環境での負荷分散の仕組みを備えた専用アプリケーションの調達、追加機器の導入、機器構成の変更等が必要となる。

(4)　仮想化環境に合わせた監査体制の整備：

仮想化環境下では物理環境と論理環境が切り離されるため、一般にデータの物理的な所在、即ちハードウェア筐体とデータの紐つけが難しくなる。特に IT リソースが動的に再配分される仕組みを導入している場合は紐付けが一層難しくなる。特定の法律の適用、公的監査への対応、情報資産管理の観点で所在を特定しておく必要が在る場合には、所在を特定可能とする方法を検討する必要がある。

(5)　仮想化環境に合わせた障害発生時の対応体制の整備：

仮想化環境は一般に障害発生時の耐性が高いとされており、それが仮想化の大きなメリットの一つであると認識されているが、一方で多様なハードウェアとソフトウェアを同時且つ多角的に組み合わせて使用しているため、障害発生時の原因究明に時間がかかることがある。そのためには以下のような取り組みが必要と考えられる。

①　仮想化レイヤーでの障害発生時の原因を解析できる仕組みの構築
②　ライセンス適合性を測定し証明できる仕組みの構築
③　仮想化・クラウドサービスを利用している場合は、プロバイダとの SLA の締結等

【クラウドコンピューティング】

(1)　社内システム環境が提供されるアプリケーションに対応していない可能性：

Web ブラウザーとの相性等によるシステムの不具合や、VB、VBA 等のバージョンの違いにより、プログラムが正常に機能しなくなる可能性が生じること。

(2)　サーバー・リージョンによる外為法などへの違反リスク：

クラウドコンピューティングの利用に際しては、外国為替及び外国貿易法の規定に基づき許可を要する取引又は行為については違反リスクを認識する必要がある。

【オンプレミス】

(1)　自社資産として管理し、説明責任を負う：

オンプレミスの IT サービス基盤は基本的に顧客企業が自社で購入（リース・レンタルを含む）した資産により構成されるため、不具合発生時の説明責任は資産保有者（または実

質的な管理者）である顧客企業が負うことになる。

(2)　セキュリティ、コンプライアンスを自社による管理：
　オンプレミスの IT サービス基盤のセキュリティ対策の維持、運用は自社で行わなければならない。そのため常に新たなセキュリティリスクにキャッチアップし、それに対応するためのリソースの投入が必要となる。ハードウェア、ソフトウェア、ネットワーク等のすべてについてリスク管理の計画、実施、及び改善活動を行う必要がある

(3)　クラウドサービスとの比較において：
但し、クラウドサービスを利用する場合もサービスプロバイダ（自社から見た業務委託先）の選定責任は顧客企業側（委託元）にある。従ってクラウドサービスを利用すること自体は説明責任のリスク移転にはならない点に注意しなければならない。

4.1.1.2. 資産保全

【クラウドコンピューティング】
(1)　事業部門での直接契約による管理対象外の IT 資産の発生：
　クラウドサービスは利用部門の主導で容易に導入できるため、全社的な IT サービスの利用状況、IT 資産の保有状況を把握できないリスクがある。対策としては、システム関連のサービス調達における承認フローの中に情報システム部門の承認権限を組み込むことで、情報システム部門が全社的な IT サービスの導入状況を決裁・契約前に把握する仕組みを導入する必要がある。

(2)　利用サービスの台帳管理が必要：
　クラウドサービスを利用する場合には、当該サービスを適切に利用し、管理するための「サービス管理台帳」を作成し、更新する必要がある。これにより定期的にサービスの棚卸し、サービスの内容・条件・利用環境の確認を行うことができ、また条件変更の有無を確認できる。

【オンプレミス】
(1)　自社資産として資産を管理し保全する：
　オンプレミスの IT サービス基盤は基本的に顧客企業が自社で購入（リース・レンタルを含む）した IT 資産により構成されるため、資産保全の責任は資産保有者（または実質的な管理者）である顧客企業が負うことになる。

4.1.1.3. 法的リスクの回避

【仮想化技術】

仮想化環境下では様々な理由によりライセンス契約違反を犯し易い。例えば物理サーバーから仮想サーバーへ移行する、あるいは物理サーバー上で仮想サーバーを複製するようなケースでは従来のオンプレミス環境とは異なるソフトウェアライセンス上の様々な制約があり、ライセンス違反を犯さないためには仮想化環境向けの適切なライセンスの調達と適用が必須である。そこで具体的には以下のような対応が求められる。

(1) 仮想化環境向けソフトウェアの使用許諾契約条件の特殊性の理解：

仮想化環境向けのソフトウェアライセンスは、CPU のコア数やシステム構成によってカウント方法が異なり、従来のオンプレミスのライセンスとは大幅に条件が異なっているという基本認識の下で、正しいライセンス条件を理解することが最重要である。

(2) ベンダー毎の仮想化ライセンス条件の違いに関する理解：

仮想化環境向け使用許諾条件がオンプレミス環境と異なっていることは理解しても、その条件がソフトウェアベンダー毎に千差万別であることまで思いが至らない場合がある。仮想化環境下での業務向けソフトウェアの利用が本格的に開始されてから日が浅いため、各ベンダーのライセンス許諾条件は現状では大きく異なっている。特に EULA（エンドユーザ向け契約条件）の仮想化環境向け特別条件はベンダー毎の差が大きいので注意が必要である。これらはいずれある条件に収斂することが予想されるが、それまではベンダー間の条件の違いに配慮した利用方法の選択が必要となる。

(3) 自動的構成変更に伴う「意図しない使用許諾契約違反」の可能性：

仮想化環境下では、ハードウェアのスペック変更、CPU の割当変更等が自動的に発生するため、ソフトウェアの使用許諾条件が変更後のハードウェア構成と合致していない場合などにおいて、意図しない使用許諾契約違反を犯す可能性がある。ダイナミックな仮想化環境を構築する場合には特にライセンス管理が難しくなることに留意する必要がある。

【クラウドコンピューティング】

基本的には、仮想化環境下におけるライセンス契約違反の状況に準ずるリスクを認識する必要がある。

(1) アプリケーションをインストールする環境の理解不足：

クラウドサービス事業者のうち、特に基盤部分を提供するサービス（PaaS、IaaS）においては、アプリケーションのインストールを顧客企業自身で行う必要がある。自ら購入したハードウェアはスペックに対する意識も高くなるが、借り物であるクラウド基盤の場合そ

こまで意識が行き渡らない場合がある。そのため、ユーザーがあるソフトウェアを複数の仮想化サーバーで同時に起動している、あるいはユーザーがソフトウェアを定められた以外の仮想化サーバーにインストールしている等の使用許諾契約違反の可能性がある。

(2)　クラウドサービス事業者による提供スペック変更への未対応：
上記同様、特に基盤部分を提供するサービス（PaaS、IaaS）において懸念されるリスクとして、プラットフォームないしインフラストラクチャの提供スペックが変更された場合、顧客企業自身の責任で、インストールしているアプリケーションのライセンスを新たなスペックに適合したものに変更ないし再調達する必要が生ずる。このような変更は通常一定の周知期間を経て実施されるケースが多いが、事業者の基本契約書（約款）の中には「事業者側の単独の判断により、いつでも任意のタイミングで提供サービスの内容の全部または一部を変更することができる」という条件で双方が同意・契約しているケースもある。

(3)　クラウドサービス事業者によるライセンス条件解釈誤り：
これは顧客企業自身の責任ではないのだが、サービス事業者自身が仮想化環境への移行に伴い、無知ないし無意識で基盤ソフトウェアのライセンス違反を犯しており、それを是正する過程で顧客企業がこれまで利用してきたサービスが利用できなくなったり、価格改定されるケースがある。

【オンプレミス】
(1)　従来通りの IT 保有形態なので、特に「クラウド時代における」と特筆するほどの内容ではないが、特に近年の傾向として、ソフトウェアの提供パッケージが簡略化・小型化される中で、インストール媒体やライセンスキーの紛失が急増している点を指摘しておきたい。インストール媒体やライセンスキー等を適切に保管しておらず紛失した場合、ライセンス保有が認められず、コンプライアンス違反を指摘される可能性があることに留意しなければならない。

4.1.1.4. セキュリティ上の問題への対処

【仮想化技術】
(1)　仮想環境では、物理的環境に加え、論理的環境を前提としたセキュリティリスクにも対応しておく必要がある。また物理環境と論理環境は別のものとしてセキュリティ管理を行なう必要がある。

(2)　複数の物理的環境に跨る論理的環境についても同様の問題が起こりうる。仮想化技術と広帯域ネットワークの普及により、複数の物理的環境に跨る一つの論理的コンピューティング環境が既に多く実現している（グリッドコンピューティング、ストレージエリアネ

ットワーク等)。このような環境でも、物理環境と論理環境は別のものとしてセキュリティ管理を行なう必要がある。

【クラウドコンピューティング】

(1) クラウド形態ごとの事業者と顧客企業の責任分担：(別紙２参照)

SaaS は事業者がハードウェア、OS、アプリケーションの全てを用意し、顧客企業は利用規約に従ってこれを利用する。SaaS の場合、顧客企業ないしエンドユーザーはアプリケーション以外操作できないようになっており、そのため利用規約のセキュリティ条項に定められた顧客企業の責任範囲はもっぱらアプリケーションの利用に関する部分であり、その内容は顧客企業自身の故意または重大な過失によるアプリケーションの誤操作と、エンドユーザ（顧客企業の従業員又は社外利用者）に規約を遵守させることの責任を謳った内容が多い。

PaaS は事業者がハードウェアと OS を用意し、顧客企業がアプリケーションを調達し、ハードウェアと OS の利用規約に従って自らの責任でインストールする。セキュリティに関する責任も、ハードウェアと OS に起因するインシデント・アクシデントは事業者の責任であり、アプリケーションに起因するものは顧客企業の責任となる。PaaS の場合、顧客企業が与えられた OS 上に自ら調達したアプリケーションをインストールするため、SaaS の利用と比べて責任範囲が広くなり、また要求される技術も高度化する。

IaaS は事業者がハードウェアのみ用意し、顧客企業が OS とアプリケーションを用意する。PaaS と似ているが、顧客企業がハードウェアにダイレクトに触れることになるため、より一層の広い範囲の責任と高度な技術が求められる。

(2) シャドーIT への対応：

会社として承認していない（パブリックな）クラウドサービスを業務目的で利用することを「シャドーIT」と呼ぶ。この利用法はセキュリティ、ガバナンスの観点から見ても大きなリスクが存在する。例えば、情報共有ツールの利用などによる情報漏えいのリスクなどが頻発している。但し、顧客企業として承認していない利用法なので、実態の把握が難しく、有効な根絶対策が取れないのが実情である。

(3) 事業者による従業員の管理

これはあってはならないことだが、サービス事業者の従業員（多くは退職した従業員）によって事業上の秘密が盗まれるという事故が発生している。特に退職した従業員による元の職場、元の業務サーバーへのアクセスは即時遮断されるべきであるが、退職時点に於いて適切なアカウント抹消処理がなされているかどうかは顧客企業側からは中々判りにくい点が難点である。また現役で就労中の従業員・委託先従業員の故意または重大な過失による事故は教育訓練の繰り返し以外に有効な管理策がなく、保険によるリスクの一部移転

を図る以外に手段がないのが実情と言える。

【オンプレミス】
(1)　データ消去の不備によりデータが漏えいする可能性：
　ハードウェアの廃棄時に、適切にデータ消去を行っておらず、その結果、データが漏えいする可能性が生じること。

(2)　バックアップの不備によりデータが消失する可能性：
　適切なバックアップスケジュール並びにバックアップデータの定期的な確認を行うプロセスに不備があるなどして、データが消失する可能性が生じること

(3)　マルウェア等による情報セキュリティ事故発生の可能性：
　利用しようとするソフトウェアの素性や使用許諾条件を確認するプロセスに不備があるなどして生じるマルウェアのインストールと、それによりデータが漏えいする可能性が生じること

4.1.1.5. 可用性の確保
【仮想化技術】
(1)　ハードウェアリソースを仮想化することで、障害発生時における代替リソースの手配が容易になるため、復旧が早まり、結果的に可用性の確保に資する。仮想化技術の一つの成果として、ユーザーの需要を予測し、IT リソースを予め計画的に用意し、ユーザーの必要に応じて提供すること（プロビジョニング）が容易になった。

(2)　障害発生時においても、予め構成可能なリソースがプール化されていれば、代替リソースの手配が一層迅速になり、IT サービスの復旧が早まり、ビジネスの停止を回避することができる。

【クラウドコンピューティング】
(1)　サービス継続性リスク：サービスの運用面は基本的にクラウド事業者任せになるため、事業者がサービスを停止してしまった場合は他の類似サービスを提供する事業者に乗り換える必要がある。

(2)　サービス内容の変更リスク：クラウドサービス事業者のサービス内容や条件が変更される可能性がある。利用時にはそのような点も十分考慮して利用する必要がある。

【オンプレミス】
(1)　オンプレミスの IT サービスにおいても可用性の確保は可能であるが、高可用性を確保するためにはシステムを完全に二重化した冗長構成が必要となり、製品の仕様・価格に直接跳ね返ることになる。

4.1.2. コスト管理（TCO 削減等）

【仮想化技術】
(1)　仮想化技術を導入した場合、機器の統合と集約により物理的なラック数の削減、電源容量の低減等によるコスト削減が期待できる。また標準インスタンスを展開することにより構成管理を簡素化することができる。需要変動時におけるリソース運用の柔軟性が高まるため無駄な買い物が減り、結果的に TCO 削減に資する。

(2)　一方、これと相反する可能性も指摘しておきたい。仮想化技術を導入する目的の一つに、組織の成長に合わせたスケーラビリティの確保や耐障害性の向上がある。この期待に応えようとすると、常にオーバースペックなハードウェアを調達しなければならない。そのため要求仕様の策定のタイミングが大雑把だと、TCO 削減に効かないという可能性もある。

【クラウドコンピューティング】
(1)　一般にクラウドコンピューティングを導入した場合、スケールメリットにより自社運用と比べて低コスト、高サービスレベルになると考えられている。クラウドサービス事業者は複数の顧客に同一サービスを幅広く提供するため、共通サービス部分についてコストダウンが可能となるとともに、当該分野での知識や経験の蓄積による習熟度のアップが期待できるからである。顧客企業はこうした事業者から IT サービス提供を受けることで、自社で IT システムを構築した場合に比べ、低コストで質の高いサービスを受けることが可能となる。

(2)　但し、ある IT サービスを長期間継続利用した場合、自社で購入・構築した場合よりも割高になる可能性がある。これは IT サービスの利用料金の設定次第であるが、概ね３～５年程度で自社購入・構築した場合と等価となるように設定されている場合が多いためである。従って顧客企業は３～５年間の利用料金総額、運用要員を含めた TCO 全体、そのための専門要員を自社で抱える意味などを総合的に考えて、IT サービスの採否を判断しなければならない。

【オンプレミス】
(1)　ソフトウェアライセンスの保有状況を把握せず、あるいは部門間の利用調整等を行わ

ないことによる、無駄にライセンスを調達する可能性。

⑵　ハードウェアの保有状況を把握せず、あるいは部門間の利用調整等を行わないことによる、無駄にパソコン等ハードウェアを調達する可能性。あるいは他部門で利用可能なハードウェアを廃棄してしまう可能性。

4.1.3. 競争上の優位性確保（IT 資産の有効活用）

【仮想化技術】

⑴　IT の導入が早くなる：

仮想化技術の導入により、IT リソース構成の変更が容易に行えるようになる。業務の拡大や縮小など組織の要求に合わせて IT リソースをいち早く弾力的に提供することが可能となる。

⑵　運用管理の標準化・自動化：

仮想化技術の導入により、属人性が排除されて運用の見える化が進み、運用の効率化が容易になる。

⑶　リリース・展開管理が失敗する可能性：

仮想化技術を導入した場合、それが環境に組み込まれていることを認識せず、通常のリストア等を実行してしまい、環境を壊してしまう可能性が生じる。

【クラウドコンピューティング】

⑴　過去の IT 投資の残存資産に縛られず、企業の成長に合わせて常にその時点でのベストサービスを選択できる。

【オンプレミス】

⑴　業務の拡大など組織の要求に合わせて IT リソースを増強する場合、意思決定の都度、ハードウェア、ソフトウェアを購入しなければならず、仮想化されたシステム環境に比べ、組織の成長スピードに対して適時環境を提供することが難しい。

4.1.4. その他の目的・課題

【仮想化技術】

⑴　構成管理の難度が高い

説明責任の項でも述べたが、仮想サーバーの構築においてプロビジョニングを可能にするためには正確な構成情報の把握が必要となる。仮想化することでリソースの共有と有効

活用が可能になるが、反面、動的な構成変更に対応できる構成管理 DB と構成管理プロセスが重要になる。また、仮想化環境では構成情報を自動収集する仕組みも必要となる。

【クラウドコンピューティング】

(1) データ移転制限リスク（欧州対米国、対テロ支援国）

国内のクラウド事業者のサービスを利用しているような企業が EU 等、データ保護が厳しい国で事業を展開する場合に、「EU データ保護指令」の制約を受け展開に障害が生じる場合がある。

(2) 複数のクラウド事業者をベースとしたサービスを利用する場合の留意点

サービス契約はフロント事業者との間で締結されるとしても、サービス自体が複数事業者による混成サービスとして提供されるため、サービス品質や継続性等について十分な留意が必要となる。

(3) 監査の留意点

クラウド事業者が外部監査に必要な証跡を提供できず、監査証明が受けられないリスクがある。クラウド事業者との契約において監査対応等の条件を入れておかなければ、クラウド事業者に監査対応を拒否され監査証明が受けられない場合が考えられる。

4.2. クラウド環境におけるライセンス管理の課題と留意点

Salesforce.com や Google Apps などに加え、最近では Office365 や Creative Cloud など、クラウド環境においてソフトウェアの利用を許諾するケースも増えてきている。このようなクラウド環境に移行するとソフトウェアライセンスの管理が楽になると考えている人は少なくない。

具体的にはソフトウェアの利用者と利用ハードウェアをパブリッシャー（ソフトウェアベンダー）のサイトに登録すれば、ユーザーID が発行され、クラウド環境下で当該ソフトウェアの利用を開始することができる。当該ソフトウェアは登録したハードウェア以外にはインストールできない、あるいはインストールしても利用できない仕組みとなっている。一見すると顧客企業側には特別な管理体制は不要のように見えるが、果たしてその通りであろうか？

前述のとおり、クラウド環境には４つのタイプが存在する。

・パブリッククラウド
・コミュニティクラウド
・プライベートクラウド
・ハイブリッドクラウド

タイプ毎にソフトウェアライセンス管理の課題は異なってくる。ここではクラウド環境

におけるライセンス管理の留意事項についてまとめる。尚、コミュニティクラウドは日本では馴染みがないため解説を省略した。

4.2.1. パブリッククラウド環境における留意事項

一般的には、利用するソフトウェアやサービスのライセンスはクラウドサービス事業者がソフトウェアベンダーと契約をしてユーザーに提供するケースと、Office365 や Creative Cloud のようにソフトウェアベンダーが自らサービス事業者として自社製品を提供するケースの２通りがある。いずれの場合も以下の項目は顧客企業側で管理すべきである。

(1) 使用許諾条件について：

クラウド環境下におけるソフトウェアの利用について、オンプレミスと同様、使用許諾条件が定められているケースが多い。例えば利用条件として、ソフトウェア管理履歴を過去３年間にわたって保持しなければならないとか、内部監査の要求、ならびにソフトウェアベンダーによる第二者監査の権限などが明記されているケースもある。顧客企業が業務目的で自社の従業員に当該ソフトウェアを利用させる場合、そこに記載されている内容について顧客企業とその従業員に遵守させる義務が生ずる。

ライセンスの保有を証明するために必要な文書類等も記載されているケースもある。これらの使用条件を遵守するためには、ID やパスワードの管理状況や、登録ユーザー以外のハードウェアが登録されていないとか、頻繁に登録されているハードウェアが変更されるなど不自然な動きがないかなど、当該ソフトウェアの適切な利用状況についても把握できる仕組みを持っておくことが望まれる。

(2) サービスレベルについて：

サービスレベルの検証も重要なポイントである。後記に詳述しているのでここでは割愛するが、少なくとも当該サービスの提供レベル（利用可能時間や保証される可用性の割合（%））とセキュリティレベル、またシステムの所在やデータがどこに保持され、どのようにバックアップがとられているか、あるいは当該システムやデータが存在する国の法規に合致した運用となっているかについては十分に確認をし、その変更の有無についてもチェックできるようにしておくことが大切である。

4.2.2. プライベートクラウドとハイブリッドクラウド環境における課題

プライベートクラウドやハイブリッドクラウドにおいては、使用許諾条件についても自社内での利用と同じように考えてしまうケースが少なくない。しかし多くの場合、クラウド環境で利用できるライセンスとオンプレミスで利用できるライセンスでは使用許諾範囲が異なるため、利用環境に合致したライセンスを調達する必要がある。またプライベート

クラウドについては、ソフトウェアをクラウド事業者が保有しサービスで提供するのか、エンドユーザーが保有しているものをインストールして利用するのかによっても条件が異なるためこの点についても留意が必要である。

(1) クラウド環境で利用可能なライセンスの確認

プライベートクラウドやハイブリッドクラウドにおいては、自分が既に保有しているライセンスをそのままクラウド環境で利用しようとするケースがある。しかしながら、オンプレミスのライセンスを単純にクラウド環境に移行できるものは少なく、一般的にはクラウド用に別途ライセンスを調達しなければならないケースが多い。クラウド事業者の提供するハードウェアをエンドユーザーが専有的に利用する場合であっても、エンドユーザーが保有しているライセンスは当該ハードウェアでは利用できず、別途クラウド事業者用のライセンスを調達しなければならないとされるソフトウェアも少なくない。

(2) オンプレミスの環境をクラウドに移行する場合の留意点

オンプレミス環境をクラウド環境へ移行する際に留意すべきことは、移行するクラウド環境の検証も含めた必要ライセンスの把握である。例えば、現状オンプレミスで利用している OS のバージョンが、クラウド環境に適応可能な OS のバージョンとは異なる（古いバージョンの OS を利用している）ケースもある。この場合は、事前にオンプレミスで利用している OS バージョンをアップグレードしておくことが必要となるが、当然に新しい OS のライセンスを新たに取得する必要が生じる。またオンプレミスのクラウド環境への移行については事前に検証作業を実施することが必要だが、ここでも別の環境を構築することによるライセンスも事前に必要となる場合がある。したがってクラウド環境への移行を検討する際には必要なライセンスと保有しているライセンスを事前に確認し、場合によっては個別にソフトウェアベンダーに相談するなどの対応が望まれる。

これらの詳細については、一般社団法人ソフトウェア資産管理評価認定協会の仮想化・クラウド WG が資料（http://www.samac.or.jp/docs/150612-SAMAC-wg-cloud-report.pdf）にまとめており、誰でもダウンロードできるので、別途参照されたい。

4.3. クラウド環境における IT サービス管理の課題と留意点

4.3.1. クラウドサービス(SaaS)の導入

クラウドが誕生して 10 年、多くの企業ではビジネスへの IT 利活用のためにクラウドサービスの本格的な活用が始まっている。背景には、経営層からの絶え間ないコスト削減の圧力と事業に資する IT 部門となることへの要求がある。一方クラウドの利用者（エンドユーザー）にとっては、SaaS のクラウドサービスと、オンプレミスで利用する IT サービスとの間に本質的な相違は無い。

IT サービスの提供にどのようなサーバーやストレージを採用しようと、そのことは利用者にとってはさほど重要ではなく、提供されるサービスの内容こそが重要である。

例として業務アプリケーションを SaaS の形態で利用する場合を考えてみよう。SaaS を利用する事で、システムは「所有」するものから「利用」するものへと変化する。情報システムのスタイルが変化することには多くのメリットがあるが、最大の価値は「俊敏性の向上」である。SaaS を採用すれば、契約したその日から業務アプリケーションを使い始めることができる場合もある。自社で企画・購入・構築した場合、サービスインまでの期間を考えると、SaaS のスピード感はとても魅力的に映るであろう。しかしその一方では様々な課題を内包していることも事実である。システムを「所有」せずに「利用」しているからといって、顧客企業は一定の法的責任から開放されるわけではない。場合によっては果たすべき法的責任を不透明にしてしまうケースもある。

クラウドサービスの場合、情報システム部門が関与することなく、利用部門がクラウドサービス事業者と直接契約して IT サービスの利用を開始することができる。しかしながら、そこにはサービス利用に伴うコンプライアンスリスクやコスト問題など様々な課題が潜んでいることを忘れてはならない。例えば、以下のような課題が存在している。

(1) クラウドサービス事業者に、個人情報を始めとする秘密情報の管理を実質的に委ねている場合、情報セキュリティのレベルはクラウドサービス事業者の水準に左右されること。

(2) クラウドサービス事業者の問題によりコンプライアンスリスクが発生する可能性があること。

(3) クラウドサービス事業者のサービス品質により顧客企業のビジネスの成否が左右される可能性があること。

特にセキュリティとサービス品質の問題は重要である。例えば高いサービス品質を提供するクラウドサービス事業者であればインシデント管理プロセスも周到な準備がなされているだろうが、そうでない場合サービスが長期間にわたって停止する、あるいは情報セキュリティ事故が発生することも考えられる。データアクセスに対する適切なプロセスが欠落していることにより、個人情報や取引情報などの重要データへのバックドアが開放されてしまうことにもなりかねない。クラウドサービスの導入のメリットは大きいが、ソフトウェアを所有せずサービスとして利用するからといって運用管理業務から完全に開放されるというわけではない。

本章では SaaS の導入プロセスを例に、以下の観点から留意点をまとめた。

・ 組織
・ 契約（コンプライアンス、SLA、EULA）
・ セキュリティ
・ 運用管理（SLA／SLM の運用）

4.3.1.1. 組織

業務アプリケーションが SaaS で提供されている場合、サービスを利用する利用部門（契約部門）は、「業務アプリケーションを SaaS で利用する場合の規程」に則ってサービスを利用し、管理者はその運用状態が規程に則って利用されているかどうかを管理しなければならない。

以下の図に組織と役割の例を示す。

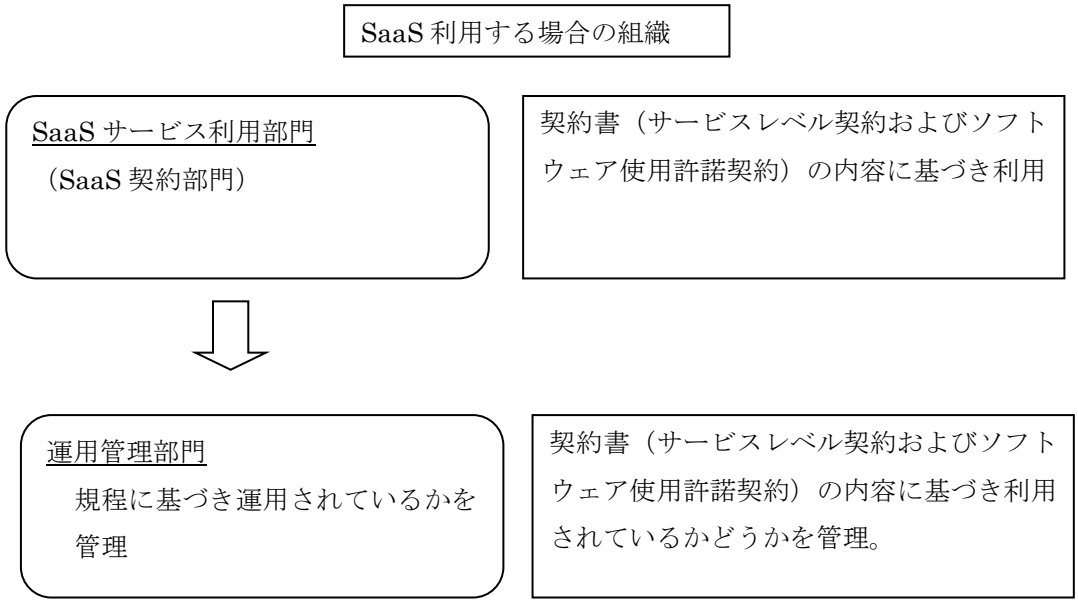


図 4-1 SaaS 利用する場合の組織

(1) サービス利用部門：

スピード、コスト、利便性などのバランスを考慮し、規程に則り利用サービスを決定することが望ましい。「利用」するサービスとして提供される SaaS の性質から、サービス利用部門が利用可能なサービスの範囲、サービス提供者としての適格性の基準、SLA（Service Level Agreement：サービスレベル合意）で網羅すべき項目および課題、SLM（Service Level Management：サービスレベル管理）などが定義されていることが望ましい。

またサービス利用部門が個別に契約できる IT サービスの範囲と、企業による包括契約を必須とする IT サービスの範囲について規定されていることが望ましい。サービスの利用によるメリットを最大化するためにはデータ連携などが必要に応じて行われるシステム連携

を考慮しなければ、サービスがあちこちで「孤立」するシステムの乱立という結果を招くことになる。「孤立」するシステム利用は、結局は無駄なコストの上昇を招き、スピードだけを求めてコスト削減のメリットを享受することが不可能となる。SLA／SLM の成功には、早期に関係各部門との共通認識を形成することが肝要である。

(2) 運用管理部門：

SaaS の実行環境となるクライアント環境を提供し、SLA／SLM の運用管理の実働部門として、規程に則りサービス利用部門の利便性を損ねることなく、サービスインのスピード、コストなど SaaS のメリットを利用部門が享受すべく、支援する体制とプロセスを形成することが肝要である。

SaaS を利用する場合、サービス利用部門は「うちの部門がサービス契約をするのだし、コスト負担しているし、契約も部門契約だから他部門に干渉されずに進められる。運用管理も SaaS 事業者が行うわけだし、情報システム部門にお世話になることもない」と考えてしまうことが多い。この考えが企業内に蔓延するとサーバー統合以前のサイロ型システムが乱立し、孤立したシステムにデータが重複して散在し、結果としてデータ整合性の取れない、全体最適化が不可能な、情報統制がとれないコスト高な情報システムの利用を推進することになる。

例えば、企業の顧客管理システムを各部門において自部門で使い勝手が良いと考える SaaS の利用を進めていくと、結果としてデータ整合性の取れない顧客データが部門毎に存在することになる。また、SaaS 事業者との契約を全社的な内部統制ポリシーやセキュリティ、法令順守などコンプライアンスに対応を考慮せずに進めた場合、結果として企業として法的責務を果たせずに市場における信頼の失墜などの原因となることも考えられる。

以上の点から、SaaS 事業者との契約は社内の規程に則り、全体最適化を前提とした内部統制ポリシーやセキュリティ、法令順守など、業務影響分析（BIA：Business Impact Analysis)、リスクアセスメントなど考慮されたかたちでサービス契約、SLA（Service Level Agreement：サービスレベル合意または契約）が行われ、システム利用の効果測定を SLM（Service Level Management）により実施し、SLA の改善を行うライフサイクル管理が実施されることが望まれる。

4.3.1.2. 契約

SaaS 事業者との契約時には留意すべき点は多い。SaaS 事業者が提示するサービス契約や SLA では利用者の利益や法的責務への考慮が不足している場合も考えられるので、十分な検討や、網羅すべきポイントを規程にまとめ、利用部門や関係各部門の合意と共通認識の上、契約交渉を行うことが望ましい。また、ソフトウェアがサービスとして提供されているとしても、ソフトウェアコンポーネント（フォント、常駐プログラム、アプリケーシ

ョンの一部機能を担うソフトウェアコンポーネント）などがクライアント PC へインストールされ、提供される場合がある。この場合は、コンポーネントの使用許諾契約が、サービス契約とは別途提供されることも考慮したほうがよい。ソフトウェアコンポーネント毎に使用許諾契約がある場合は、それらの契約内容に基づく運用が必要となるので運用管理部門の関与は不可欠となる。これらを怠った場合、SaaS というサービス提供の形態であってもソフトウェア使用許諾契約違反として損害賠償請求されることも考えられる。少なくとも以下の点に留意し契約することが望まれる。

- SaaS 事業者の選定（提供者に依存するセキュリティ対策とサービスの継続性）
- システム間連携
- カスタマイズの可否
- サービス終了時のデータ移行
- ソフトウェアコンポーネントの使用許諾契約
- 財務情報、営業機密情報の取り扱い
- SLA：サービスレベル合意（契約）
- サービスサポート

(1) SaaS 事業者の選定（提供者に依存するセキュリティ対策と継続性）

SaaS の利用は、自社データを外部に預けるということであり、SaaS 事業者のセキュリティレベルにデータの安全性を完全に依存することである。また、サービス利用の継続性が、SaaS 事業者の存続性と等しいので、提供者の選択は慎重に行わなければならない。

SaaS 事業者を選定する際の留意点としては SLA（Service Level Agreement）や企業の財務諸表、セキュリティポリシー、データセンターの堅牢性、インターネット接続回線、ハードウェア、ソフトウェアなど基盤、アプリケーションや Web システムとしてのセキュリティ、脆弱性診断の報告書など加味し慎重に問題がないことを確認し、契約しなければならない。もちろん、重要な業務や機密性の高い情報を処理するサービスと、比較的機密性の低い情報を処理するサービスでは選定条件を分けて検討する。

以下に継続性における選定条件の一つとして、SaaS 事業者の提供基盤の構成例をあげる。

① 建物施設を所有し、インフラストラクチャのハードウェア、ソフトウェアを所有し、アプリケーションを所有。全ての構成要素を所有した状態でサービス化を行い、ユーザー企業へサービスを提供している。

② 建物施設を利用し（ハウジングの状態）、インフラストラクチャを所有、アプリケーションを所有、これらを組み合わせてサービス化を行い、ユーザー企業へサービスを提供している。

③ 建物施設を利用し、インフラストラクチャを利用し（PaaS 利用の状態）、アプリケーションを所有し、これらを組み合わせてサービス化を行い、ユーザー企業へサービスを提

供している。
④　建物施設を利用し、インフラストラクチャを利用し、アプリケーションを利用し、これらを組み合わせてサービス化を行い、ユーザー企業へサービスを提供している。

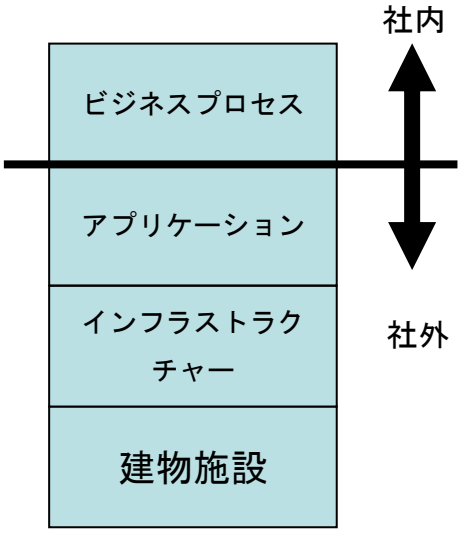


図 4-2 基盤のレイヤー

①から④の順に SaaS 事業者の制御範囲が制限される。また、建物施設やインフラストラクチャ自体が海外にある場合は、何らかの問題が発生した際に、その対応に時間を要し、かえって運用コストが高くなるという可能性も考慮する必要がある。

①の提供者の例としては、電力系、通信系などそもそも IDC 事業を経営の主軸とし、インフラを所有している事業者があげられる。

②の提供者の例としては、大手 IDC 事業者の施設をハウジングしきた準大手のサービス事業者があげられる。PaaS や IaaS などのサービスを提供している場合もあるだろう。

③の提供者の例としては、現在増加している PaaS などを利用して自社開発したアプリケーションの SaaS 展開を図るアプリケーション開発事業者があげられる。

④の提供者の例としては、今後増加すると考えられる PaaS 上にアプリケーション開発事業者から OEM 提供を受けサービスを提供するサービス事業者があげられる。

SaaS で提供されるアプリケーションを分類すると以下のようにまとめられる。

（ア）基幹系、情報系、顧客管理系
（イ）セキュリティ系、運用管理系、データ保存系
（ウ）業務支援系

独自カスタマイズやシステム間連携が必要で、高いデータの機密性や継続性が求められ

るシステムであれば SaaS 事業者の制御範囲に制限が少ないほうが最終的なコストや SLA の柔軟性が高いと考えられる。一方で、中小企業や（イ）の分類のような、独自カスタマイズやシステム間連携が限られた範囲で足りるシステムであれば、SaaS 事業者の制御範囲が制限されていても問題とならない範囲が存在するだろう。

ユーザー企業独自のカスタマイズへの対応やシステム間連携を高いデータ機密性と同時に求める場合は、アプリケーションを所有していなければカスタマイズや機能対応はコスト高となる。具体的には、アプリケーションを OEM 提供で受けてサービスを提供している事業者であれば、カスタマイズはアプリケーションを製造しているソフトウェアメーカとの交渉となり、実際の開発もユーザー企業とソフトウェアメーカの間にプロジェクトマネジメントとして関与することとなり、複雑でコスト高な対応となることが考えられる。

技術情報などもアプリケーション開発元であれば、独自カスタマイズやシステム間連携に必要となるソースコードレベルでの理解のある技術者が対応することもあり得るが、開発元でなければユーザー企業の要件を反映させるための技術的要件定義に時間を要することも考えられる。また、著作物にたいする著作権や使用権などの交渉も開発元と直接交渉できるか、そうでないかでは大きく工数に影響することが考えられる。具体的には、例えば交渉相手が開発元ではなく、開発元が海外の企業であった場合などは、著作物に対するカスタマイズ部分の著作権や使用権の交渉には海外にある開発元の許可や、適法もその開発元企業が存在する国の知的財産法に則って契約書を英語にて取り交わさなければならないなど工数を増加させることも考えられる。

(2)　システム間連携

システム間連携を行うには、連携部分の作りこみが発生するため、自社でシステム開発者を用意するか、開発を外部委託する必要がある。

簡単なカスタマイズであれば SaaS 事業者が API（Application Programming Interface）を提供し、連携が可能な場合もあるが、既存システムや他社 SaaS アプリケーションとの連携が可能かどうかは技術要件を確認しなければならない。

SaaS アプリケーションの API は、各サービス提供者が独自に定義しているが、連携を意識した共通の API やデータ構造を持たない限り異なる SaaS 事業者のシステム連携を行うことは困難である。システム間連携が必要となるシステムを SaaS で利用する場合は、十分に連携の実現可能性、費用対効果、開発コストなどを考慮して判断するべきである。今後はデータを XML 化し、Web Service 連携によるシステム連携の可能性を提供する SaaS 事業者も現れると考えられることから、SaaS 事業者との契約時に提供者がどこまでシステム間連携をサポートするか、技術情報の提供範囲、今後の対応予定なども事前に確認するべきである。

(3)　カスタマイズ

今日の SaaS は、パラメータ化などにより、プログラムの改修を行わず設定変更レベルの作業でカスタマイズが可能である（但し、カスタマイズの定義は SaaS 事業者毎に異なるため注意が必要である）。

しかし、設定変更レベルでユーザー企業が期待する全ての機能を実現できるわけではない。したがって、将来的な利用用途や業務拡大で必要となる機能が事前にわかっている場合は、提供されるカスタマイズ機能で実現可能かどうかを検討しておく必要がある。ユーザー企業独自のカスタマイズが発生する場合は、実現性やコスト、著作権、サービス移行時の再利用性など SaaS 事業者と事前に協議して合意しておかなければならない。

カスタマイズは結果的に多額のカスタマイズ費用や特別に保守費用やメンテナンス費用が必要となることが考えられる。加えて、レスポンスの低下、SaaS 事業者の通常保守や機能拡張の際に問題が発生する場合もあり注意が必要である。

また、カスタマイズの内容はしっかりと文書化しておく必要がある。サードパーティのコンサルティング会社を利用する場合は、プロジェクトのオーナーシップや、責任の所在など明確にしなければならない。SaaS 事業者の乗り換えに伴うコストや、開発作業のリスクを共有することにコンサルティング会社が同意するかを事前に確認する必要もある。選択肢としては、SaaS 事業者のソフトウェアのカスタムフロントエンドを作成することで、自社でカスタマイズを行い、その成果を保持することができる。

この場合、自社でカスタマイズする部分に自社のノウハウが含まれて、市場における差別化や企業優位性となるプロセスが実装されたりする。SaaS はサービスインのスピードやコスト面でのメリットがあるが、実装されたノウハウが SaaS 事業者のノウハウとして吸収され、将来のバージョンアップに利用され競合他社へも一般的なサービスとして提供されてしまうという危険性を含んでいる。ユーザー企業内での使用者数が少ない場合は、オンプレミスのシステムより SaaS のメリットが勝ることになるが、それでもノウハウの流出が企業優位性を損なう可能性を秘めている場合は、あえて SaaS を選択しないということも考慮する必要があるだろう。もちろん、ある程度の流出を想定しながらも SaaS 事業者に対して、SaaS システムに実装するカスタマイズ部分の著作権に関する契約により保護し、必要であれば損害賠償訴訟により一般公開を妨げるという選択肢も考えられる。

(4)　サービス終了時のデータ移行

SaaS の利用を終了する際に、SaaS 事業者のシステムに蓄積されているデータから新たなシステムまたは異なる SaaS 事業者のシステムにデータ移行を行う必要がある。SaaS の導入検討の際に次期システムへの移行を具体的に計画することは困難であるため、移行に必要と考えられるデータの権利（利用期間中に入力したデータや、入力データから得られる集計結果、加工されたデータなどを契約解除時に再利用する権利、SaaS 事業者のデータ消去処理のプロセス）、機能面での出力可否（CSV、XML）などデータ出力の対応状況など

事前に確認する必要がある。

(5) ソフトウェアコンポーネントの使用許諾契約

SaaS を利用する場合でも全てのソフトウェアがブラウザーで提供されるとは限らない。アプリケーションによってはネットワークの負荷やクライアントにおける処理パフォーマンスを考慮して一部機能をソフトウェアコンポーネントとしてクライアント PC の環境にインストールするものや、適宜ダウンロードされメモリー上で利用されるもの、テンプレートやフォントなど利用頻度が高いのでローカルハードディスクに保存されるものなどが考えられる。これらのソフトウェアコンポーネントは、各コンポーネントが SaaS 事業者の著作物として EULA（End User License Agreement：使用許諾契約）がインストール時に結ばれることが多い。これら契約も、サービスの利用者の利用形態を考慮して SaaS 事業者と合意できるかの可否も含め検討する必要がある。

(6) 財務情報、営業機密情報

SaaS を利用して財務情報や営業機密情報を扱う場合は、SaaS 事業者が国内法規（商法、会社法、税法、労働法など）に則っているかなど事前に確認しなければならない。また、上場企業が SaaS 型の財務関連のシステムを導入する場合は、金融商品取引法の適用を受けるため、以下の要求事項が考えられる。

① 提供する財務関連のシステムが会計規則の要件を満たしていること
② IT 全般統制や財務関連システムの IT 業務処理統制に対する経営者評価や監査人監査への協力を提供者が受け入れること
③ 日本公認会計士協会の監査基準委員会報告書第 18 号に準拠した監査報告書の提供

これら国内法令対応は必須であり、SaaS 事業者が国内法令対応を疎かにしていると、業務を複雑にするばかりでなく、データ保全、説明責任という観点からも事故を発生させやすいということを認識しなければならない。法令改正に対する対応のスピードや、今後の対応予定など契約時に確認しなければならない。

(7) SLA（契約）

SLA（Service Level Agreement）は、提供されるサービスの範囲・内容・前提事項を踏まえた上で「サービス品質に対する利用者側の要求水準と提供者側の運営ルールについて明文化したのも」である。SaaS によるメリットへの期待値が膨らむ一方、SaaS は様々な課題を抱えているのも事実である。

「SaaS を利用すればソフトウェアの管理や、運用管理の責任を一切免れることができる」、「コストを削減し、短期で導入可能で、レスポンスなどパフォーマンスの高いシステムを

利用できる」など過度な期待は、トラブルへと発展する恐れがある。

SaaS 事業者と利用者双方にとっては、適切な SLA の締結が重要であり、定めたサービスレベルを定期的に測定、分析、評価することにより継続的にサービス改善を実現することが必要である。

SaaS を利用している際に発生したトラブルがすべて提供者の責任であるとは限らない。自社所有システムであればインシデント管理などにより原因分析に必要な情報を管理しているが、SaaS として提供されている場合、提供者がどこまでを管理対象の範囲としているのか、利用者への報告対象としているのかにより、利用者が知りえる範囲が決定されてしまう。

何がトラブルなのか、セキュリティ事故なのかの判断基準は企業によって異なり、ポリシーや事業影響度分析（BIA）やリスクアセスメントにより判断される。SaaS 事業者の基準と利用者の基準は、利用者が基準としているポリシー、事業影響度分析、リスクアセスメントの基準に則った合意が SLA に明示されていなければ期待する報告が SaaS 事業者からは提供されないことも考慮しなければならない。

また、利用者がもとめているすべてについて SaaS 事業者が対応できるわけではないので、それを前提に利用者の責任と提供者の責任を明確にし、SLA に反映させておかなければならない。

しかし、SLA を交渉・管理できる能力を有する情報システム部門を持たない中小企業においては、SaaS 事業者があらかじめ用意している標準的な SLA を締結する際に、本章の確認事項や留意点を十分に確認するとともに、信頼できる SaaS 事業者の選定を行うことが肝要である。

(8) サービスサポート

SaaS 事業者のサービスはアプリケーションの機能だけの提供にとどまらず、アプリケーションを利用するためのサポートも重要なサービスの一つである。この観点から、SaaS 事業者が IT サービスマネジメントのプロセスを正しく運用できるのか、というサービス運用能力も契約時に見極める必要がある。ヘルプデスクの設置、迅速なトラブル対応などの体制やプロセスについては ITIL に取り組んでいるか、また JIS Q 20000:2007 認証を取得しているかなどについても確認を行う必要がある。

4.3.1.3. セキュリティ

SaaS 事業者の選定には、安全性の観点から JIS Q 27001 : 2006（ISO/IEC27001:2005）の要求事項を基本としたセキュリティ対策の実施状況を確認することが重要である。更に、Web 脆弱性検査など、第三者による安全性検証試験／セキュリティ診断を定期的に実施し、その結果をユーザー企業に対して公開していることを前提条件と考えるべきである。サービスの継続性、信頼性の高さを判断する基準としても、これらの対応を含む、プライバシ

ーマーク付与認定、ISMS 認証取得、情報セキュリティ監査制度の利用などを行っているユーザー企業においては、必要に応じて利用者の基準に応じた監査を行うことができるかどうかも重要な判断要素となる。以下の点について留意点を記述する。

- 機密性
- 完全性
- 可用性
- データ保護
- アカウント管理

(1) 機密性

SaaS ではデータは外部に委託され、他社のデータと同じデータベース上で管理されている。したがって、データベースのセキュリティ上の懸念事項については自社のデータベースセキュリティ以上にデータ機密性の高さに応じた SaaS 事業者のセキュリティ管理能力の考慮が必要である。

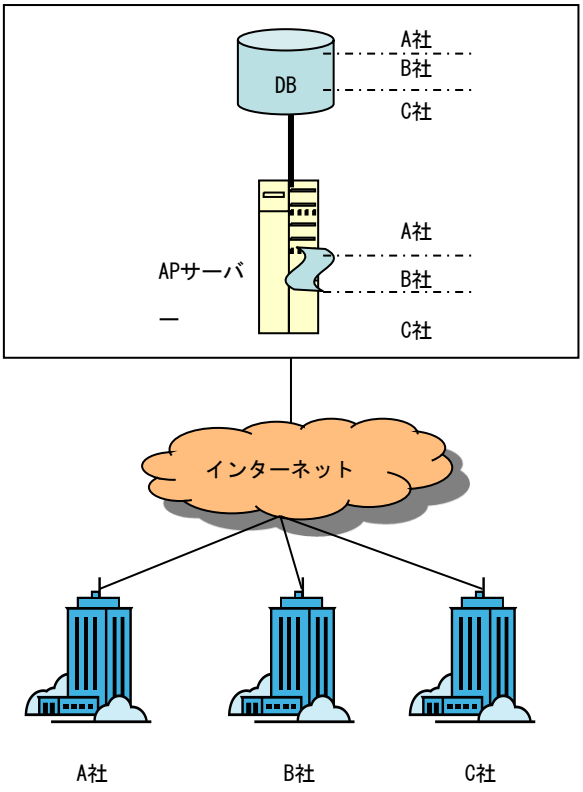


図 4-3 SaaS 型サービス：マルチテナントにおけるデータベース

例えば、SaaS に使用されているデータベースの製品、バージョン、セキュリティパッチの適用ポリシー、システム構成など、必要なセキュリティ対策が行われているかどうか自

社システムのセキュリティポリシーとの比較など行い機密性に問題がないかどうか確認しなければならない。

また、データベースに蓄積されているデータの種類や特性、蓄積される情報の種別、情報管理に関するアクセス制御の内容なども明確にしておく必要がある。SaaS で提供されているユーザー権限だけでは、今まで自社で運用してきたアクセス制御や情報の閲覧権限の制御など厳格な情報管理ができなくなる可能性がある。社内ポリシーに則った情報統制など、内部統制にかかわるコンプライアンス構築の一環として社内ポリシーの運用にそぐわない SaaS であれば実運用に耐えることができない。

Web アプリケーションである SaaS は、機密性の確保のため通信として HTTPS を用いることが要求される。しかし、通信路の保護だけでは十分ではなく、預託したデータを記録したハードディスク、光学メディア、USB メモリーなどの記憶媒体の管理状態やデータベースへの直接アクセスによる情報漏えいを防ぐための適切なアカウント管理など、データ保護の管理策についても確認する必要がある。

(2) 完全性

データが漏えいしなくても改ざんされることで信頼性が損なわれる。また、消去されれば業務の継続ができなくなるなど、重大な問題が発生するため、預託データの完全性、整合性検証について対策が施されていることを確認する必要がある。

情報システムの効率的利用にはデータの再利用が不可欠であるため、データをダウンロードして加工できるなどの手段が提供されていなければならない。

ダウンロードしたデータは独自のデータフォーマットではなく、標準的な CSV、TSV、XML などで提供され、再利用性の高いデータでなくてはならない。

(3) 可用性

SaaS の特徴として柔軟なカスタマイズ機能や、マッシュアップによる機能の融合などがある。この際に的確な処理が行われているか、データの受け渡しの正確性についても確認する必要がある。また、マッシュアップなどで複数の SaaS 連携を行うサービスを利用する場合は、それぞれの役割と責任範囲を明確にしておかなければならない。

SaaS のサービスの利便性としてネットワークさえ繋がっていれば利用できるという点があるが、低コストを追求しすぎるとサービス継続性の低いサービスであったり、サービスの停止だけでなく、復旧に要する時間も特定できないという問題が発生する可能性もある。国外の SaaS 事業者で国内拠点ではないサポート窓口の場合、時差によりコミュニケーションに時間を要し、問題の詳細説明を外国語で行わなければならないなど、大きな負担としてかえってコスト高になることも考慮する必要がある。

(4) データ保護

重要な業務や機密性の高い情報を扱うサービスの場合、インターネットを経由することから暗号化通信が必須となる。サービス提供されるシステムがユーザー認証時だけでなく、HTTPS 通信や VPN に対応していることや、データの格納形態（分散化、暗号化の有無）の確認、障害時の復旧範囲（復旧できるデータとできないデータの種類）、復旧に要する時間、データに関わるサービス提供者のプロセスや要員の数の最小化、アクセスできるデータの範囲などに関して SaaS 事業者に確認し、事前に SLA などで定義しておく必要がある。SSL が使用される場合は SSL3.0 および TLS1.0 に限定し、脆弱性のある SSL2.0 は使用しないなどのポリシーを定めることが望ましい。

(5) アカウント管理

SaaS はインターネットで提供されているサービスであるため、ユーザー企業が利用するログインページへ誰でもアクセスすることができる。なりすましなどにより攻撃者が不正ログインを試みるリスクが存在する。このような脅威に対して、連続したログイン失敗時の処理方法（一定期間ログインできなくなる制限処理や、証跡（ログ）の保存、ユーザーの運用管理者への通知、回復手順など）や、パスワードの桁数、使用可能文字種類、有効期限、履歴管理などユーザー企業の規程やセキュリティポリシーに適用可能かどうかを確認し、SLA などで定義しておくことが望ましい。

4.3.1.4. 運用管理

SaaS 型サービスであれば運用管理は SaaS 事業者が基本的には提供する。しかし、だからといって運用管理の責任がまったく無くなるわけではない。システムの運用面では工数は大幅に削減されるが、SaaS 型だから増える管理の項目も存在する。ここでは SaaS 形式と自社所有のオンプレミス型とを比較して情報システム部門が調達・導入・運用管理において留意すべき点を検討する。

(1) 導入のための事前検討

SaaS 型サービスであっても、業務分析、業務設計／見直しなどはオンプレミス型同様必要である。上流工程の設計を外部に委託する場合は、コンサルティング費用などもオンプレミスと変わらないコストが発生する。

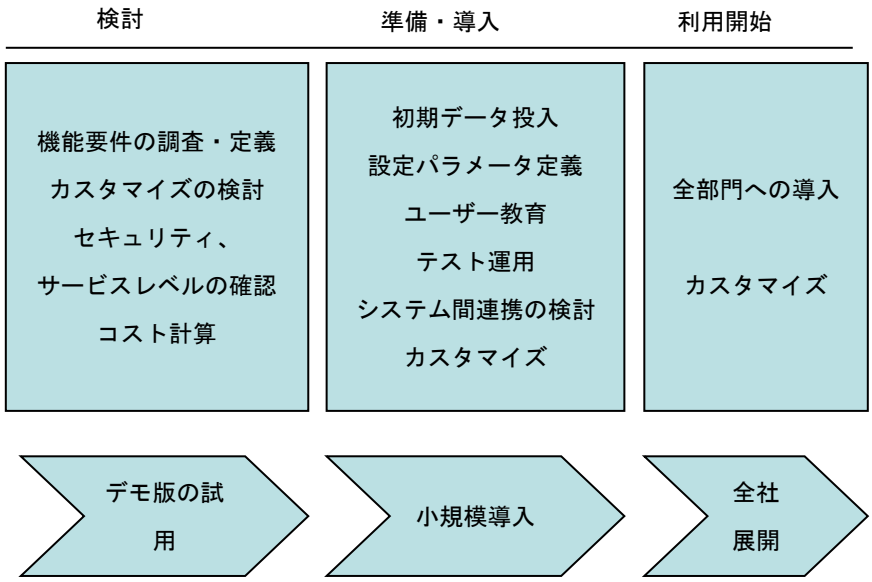


図 4-4　SaaS 型サービス導入フロー

(2)　アプリケーションのカスタマイズ

利用部門の要望により利用にあった仕様を要件定義書にまとめ、SaaS 事業者が提供する汎用カスタマイズなどパラメータの設定で対応可能か否かを検討する。表示項目、表示項目名や参照データのレベル、参照アクセス権の設定など自社の情報統制のポリシーに則って運用可能かを確認する。

また、パラメータ設定では対応不可能である独自のカスタマイズが必要と判断される場合は、SaaS 事業者が提供する API を利用する範囲でカスタマイズの開発が自社情報システム部門の開発リソースで対応可能かどうかを調査する。この場合、カスタマイズ部分に自社ノウハウや差別化、企業優位性などが含まれるプロセスを実装する場合、これらカスタマイズ部分が実装される SaaS 事業者のシステムにおいて、SaaS 事業者のスタッフがどのレベルまでの情報アクセスができるのか、あるいは実装することで SaaS 事業者のスタッフによりノウハウが吸収される恐れがある場合は、その防止策を技術的に実現できるのかなどを検討することが望ましい。規程作成部門と SaaS 事業者とのサービス契約の内容に自社ノウハウを含むカスタマイズのコンポーネント部分の著作権保護など盛り込むなどを検討することが望ましい。

また、独自カスタマイズを実装した場合の SaaS 事業者から提供されるサービス（例えば保守、機能バージョンアップなど）が通常通り提供可能か、独自カスタマイズにより別途、機能バージョンアップ時にも同様の独自カスタマイズ部分の差異を吸収するための作業が発生するのかなども考慮することが望ましい。

(3)　システム初期導入

ネットワーク環境やクライアント環境が SaaS 型サービスの仕様要求に対応しているかなどを確認し、準備する。対応 OS や、ブラウザーの種類、バージョン、クライアントのローカルにインストールしなければならないコンポーネントの有無、実行に必要となるメモリー、適宜ダウンロードされ実行されるオンメモリのコンポーネントの有無や Java Runtime Edition、.NET フレームワークのバージョンなどが考えられる。

ローカルにインストールされるコンポーネントがある場合は、それらの使用許諾契約書に則った運用ポリシーを策定する。例えばフォントやテンプレートなど、インストールされたクライアントからコピーされて当該 SaaS サービスの利用者ではないクライアント PC 上で実行された場合は使用許諾契約違反となり損害賠償請求の対象となることから、使用範囲と利用者管理を行うことが望ましい。

また、ネットワーク負荷を考慮して SaaS サービスのソフトウェアコンポーネントの一部がクライアントに常駐する形式でインストールされる場合、そのダウンロードのサイズや常駐のサイズなど管理し、多数のユーザーが同時にダウンロードしてネットワーク負荷が突然ピークに達しないような計画を立てることも考える必要がある。同時に常駐コンポーネントなどは、常駐するクライアントのメモリーを圧迫する可能性があるので利用者のメモリーの空き容量や CPU の処理能力なども考慮することが望ましい。

ネットワークおよびクライアントのセキュリティ対策の実施はオンプレミス型同様の対応が必要となる。システム間連携が必要となる場合は、連携部分の作りこみや、連携データの整合性の設計や計画なども必要となる。

(4)　ユーザー教育

利用者の操作および情報モラルの教育はオンプレミス型同様の教育が必要となる。SaaS 型サービスはどこからでもアクセスできることから、部外者の誰でもユーザーカウントの情報さえ入手できれば、なりすましでデータへのアクセスが可能となってしまう。アクセス権限が高いユーザーほど高いモラルやセキュリティの意識を持たなければ、データの消失、漏えい、改ざんなどオンプレミス型以上にセキュリティリスクは高くなる。

(5)　クライアント管理

セキュリティの観点から、一般的には OS はもちろん、クライアントにインストールされているソフトウェアを最新のパッチが当たっている状態に維持することが望ましい。クライアントの管理はオンプレミス型同様の管理が求められる。見落とせないのは SaaS サービスによっては提供されるクライアント常駐コンポーネントの実行環境のサポートと、常駐コンポーネントのイメージ管理やバージョン管理、展開などインストールの管理などである。具体的には、例えばクライアントシステムのセキュリティ管理を行うためのクライアント常駐コンポーネントを、クライアント PC にインストールする場合などは、常駐コンポ

ーネントとなるソフトウェアのシステム要件にみあった実行環境（例えばシステム要件に.NET Framework のバージョンや、JRE のバージョンの指定がある場合など）のサポートを情報システム部門が対応しなければならなくなる。さらに、常駐コンポーネントとしてソフトウェアが提供される場合は、これらの在庫管理プロセスも、通常の SAM 同様、情報システム部門が対応しなければならない。

また、当該 SaaS サービス利用者ではないユーザーによる不法なコンポーネントの利用管理も必要となる。例えば、フォントなどが提供されるソフトウェアを SaaS 型で利用しているユーザーが、フォントのファイルをコピーして利用権のないユーザーへ提供して、それが使用された場合に、ソフトウェア使用権を持たないユーザーの不正な使用として検知し管理する仕組みなどが望まれる。

(6) データメンテナンス

SaaS 事業者のサービス内容にもよるが、システムによっては、サービス管理のプロセスを ITIL に則ってポリシーにあったデータのベースラインを保存しておく必要がある。
具体的には、例えば IT 管理の一部のシステム（IT 資産管理システム、セキュリティ管理システムなど）を、SaaS 事業者によるサービスとして利用し、そのデータを社内にある IT 統合管理システムと連携させているような場合は、SaaS で提供されている IT 管理システムのデータベースが、直接（SOAP などプロトコルを利用した Web サービスによる直接連携により）、社内の IT 統合管理システムの構成管理データベースと連携してベースラインを保存している場合を除いては、別途、変更管理に必要となるベースラインを適宜、バッチ処理などによりデータとして保存し、標準的なデータフォーマット（例えば、CSV、TSV、XML など）でエキスポートしたデータを社内の IT 統合管理システムの必要なデータベースへインポートしたりする必要がある。

またシステムのデータにも依存するが、データの整合性や鮮度、正確性を維持するためのデータメンテナンスなどが必要な場合も考えられる。
具体的な例としては、顧客管理システムのマスターデータの管理や、人事管理システムや人事情報を利用する資産管理システムや、職務や職責に紐付けられるセキュリティポリシー管理などリアルタイムのデータ連携が行われない場合はバッチ処理でのデータの洗い替えなどが挙げられる。

(7) ヘルプデスク

SaaS サービスとして提供されるアプリケーションの基本操作に関するヘルプ対応要員の要否も検討することが望まれる。データの再利用のためのダウンロードや、再利用の際の制限や規制などに対応する担当者も必要に応じて定めることも望まれる。

(8) セキュリティ

アプリケーションが SaaS サービスとして提供されている場合には、SaaS 事業者がアプリケーションの稼働環境となるプラットフォームのレイヤーからアプリケーションのレイヤーまでのセキュリティを確保しなければならない。だからと言って、SaaS 事業者のセキュリティが完全なものであるという保証はないため、SaaS 事業者との SLA により、SLM（本項（９）参照）を実施し、利用部門やユーザー企業が要求するセキュリティレベルが維持されているかどうかを定期的に評価する仕組みを持つことが望ましい。セキュリティ事故などが発生した場合には、どこに責任があるのかを明確に切り分けることが可能なレベルの情報が収集でき、改善に必要な要件やプロセスの提案ができることが望ましい。
一般的には、クライアントの管理はオンプレミス型と同様に必要となる。

(9) SLM（Service Level Management：サービスレベル管理）

また、SLM についてはサービス管理の（ITSM）のベストプラクティスである ITIL や、その国際標準である ISO/IEC 20000、国内標準である JIS Q 20000-2 では、SLM を「サービスレベル管理とは、“サービスレベルを定義、合意、記録及び管理するため”の継続的なプロセス活動である」と定義している。SLM においては、利用者と SaaS 事業者が協力して問題を確認し、根本原因の分析やプロセスの変更などを通じて問題の再発を防ぐ継続的な問題解決が重要となる。

SaaS サービスの運用管理において重要なことは SLA に基づいた SLM（Service Level Management：サービスレベル管理）の実施である。SLA では契約時にサービスレベルの定義が行われ、サービスレベル測定のための項目が設定される。SLA で定められた条件を SLM によって管理できるようにする。万一トラブルが発生した場合には、業務に与える影響を考慮した上で、優先順位を定め、優先順位が高いものを中心に定義する。あまり多くの項目を管理しようとすると、管理負荷の増加やコストの上昇を招くことにもなるため、システムの重要度に則って、必要最小限に抑えた効率的な運用を行うことが望ましい。重要なことは、サービスの内容が決まり、サービスレベルが設定され、利用者にサービスが提供されてからそのサービス契約が終了するまでの間、SLM は継続的なプロセス監視活動として利用者（ユーザー／事業部門）と運用者（情報システム部門）およびサービス提供者（SaaS サービス提供業者）のすべての関係者によって参画、実施されなければならない活動であるということである。SLM の一般的な目標としては以下の項目が挙げあれる。

① 提供されるサービスのレベルを定義、文書化、合意、モニタ、測定、報告およびレビューすること
② サービスに対して具体的で測定可能な目標値が策定されるようにすること。
③ 提供されるサービスの品質に対する利用者の満足度をモニタし改善すること
④ サービス提供者と利用者が、提供されるサービスのレベルに対して、双方に解釈の

差異が生じないような定量的な目標を持つこと

SLM の成功には、計画段階からの利用部門の参画が必須である。SLM 運営組織を立ち上げる際には利用部門の主要関係者を配置し、SLA／SLM の重要性について早期に共通認識を形成することが望ましい。

4.3.2. クラウド環境での IT サービス管理の課題と留意点

企業の IT 部門にとって、クラウドコンピューティングの出現は運用管理のパラダイムシフトを引き起こす要因となっている。

クラウドサービスの最大の特徴は、その俊敏性にある。必要とするサービスの構築から利用者への展開までがオンデマンドの仕組みにより短期間で利用可能となる。サービスを利用する側にとってはビジネスの変化に即座に対応できるソリューションとなる。さらに、プライベートクラウドとパブリッククラウドを併用したハイブリッドクラウドが今後のトレンドになるとの見方もある。

最近では、クラウドの活用方法がさまざまに進化するに伴い、IT 部門がクラウド環境を利用者に提供することが要求され、クラウドサービスブローカーとしての役割を担う可能性も出てきている。IT 部門が外部のクラウド事業者と契約し、企業内へクラウドサービスとして展開する形態である。

ハイブリッドクラウドでは、IT 部門がクラウドサービス提供者としての機能を持つことを意味している。クラウド環境における IT サービス管理への対応は IT 部門にとって避けて通れない重要なテーマとなりつつある。

IT 部門は従来のオンプレミスでの IT サービス運用管理に加えて、クラウド提供者としての視点で、クラウド環境の運用管理に留意しなければならない。従前のオンプレミスで物理サーバーを対象にしていた運用管理では対応しきれないからだ。

オンプレミスの運用管理ではサーバー単位あるいはシステム単位で対応する形が多く、IT サービス単位での運用管理の必要性は認識されていても、実装されているケースは少ないのが実情であろう。クラウドとオンプレミスの混在する環境での運用管理では、システム毎の運用管理ではなく、オンプレミス/クラウドで提供する IT サービスを対象とした運用管理を目指す必要がある。

クラウドのサービスの種類（SaaS、PaaS、IaaS）により、IT 部門が説明責任を負うべき運用管理の対象は差異を生じる。例えばパブリッククラウドで SaaS を利用している場合は、IT 部門はクラウド上の仮想システムへの運用管理に注意を払う必要はないだろう。SaaS のサービス契約を締結するときに、SLA が自社の要件を満たしているかを検証する事が中心となる。仮想サーバーの運用管理はクラウド事業者の責任範囲となるからだ。IaaS の場合は、インフラのハ―ドウェア部分がクラウドサービスで提供されるが、OS、ミドル

ウェア、アプリケーションといったソフトウェアの管理はIT部門で行う必要がある。

このようにクラウドサービスの種類によって運用管理の対象が異なるにしても、オンプレミス/クラウドの混在したサービスを運用管理するには、従来以上のサービスマネジメントシステムの構築が重要となることは言うまでも無い。

4.3.3. 仮想化とITサービス管理

クラウド環境では仮想化技術が前提であり、物理リソースは論理リソースにマッピングされる。クラウドの特徴として、リソースの置き換えがダイナミックに発生する可能性が高い。オンプレミスのように物理的なシステム上に構築されたITサービスを運用管理するよりも、更に複雑さが増している。従来のITサービス管理に必要なプロセスの重要さはオンプレミス/クラウド混在環境でも変わりはないが、クラウド環境下のITサービス管理を考えた場合、クラウドの持つ「俊敏性」を生かすための運用管理には、運用の「見える化」、「自動化」が必須になってくる。

クラウドコンピューティングを支える仮想化技術は、オンプレミス、クラウドの形態を問わず利用可能である。オンプレミスでは物理サーバーの基盤統合という形で、すでに一般的なソリューションとして定着している。反面、仮想化は運用管理における複雑さを増す原因となっている。仮想化は物理リソースを仮想リソースとして再構築することで、ITサービスの提供に必要な物理的なリソースの制限を取り払った。IT部門では、複雑化したリソースの状態をダイナミックに把握する必要がある。仮想化ではリソースの追加、仮想リソースの移動等により、物理リソースと論理リソースの対応付けが変わるからである。

仮想化環境の障害では、迅速な対応と復旧には、仮想化サーバーがどの物理サーバーで稼働しているかを把握しておく必要がある。仮想化環境であっても、問題発生時には障害内容を切り分け、原因を特定する作業は変わらない。そこで、どの仮想サーバーがどの物理サーバーで稼働中であるかが不明なようでは、仮想化していることの意味がなくなってしまう。仮想化サーバーと物理サーバーのクラウドサービス提供者は、構成管理の一元化と構成管理情報の自動収集と見える化は必須と言って良いだろう。

物理サーバーの上に多くの仮想サーバーを構築した場合、パフォ―マンスの低下を招くことがある。仮想サーバー上のアプリケーションの負荷の組み合わせにより、物理サーバーでのリソース競合を起こすケースだ。こういった事態をプロアクティブに処理するには、リソースの監視とキャパシティ管理が必要となる。リソースの監視や、キャパシティ管理といった非機能要件を運用管理プロセスとして備える必要も出てくる。

IT部門にとってクラウドを採用し、企業内外の利用者にサービスを提供するには、従来からのオンプレミスでの運用管理体制の見直しが必要であることに留意すべきでる。

4.3.3.1. 仮想化環境での構成管理

今までの「システム」と呼ばれる単位が「サーバーハードウェア上に存在する一つの OS に紐づくアプリケーション」というハードウェア、OS、アプリケーションが 1 対 1 対 1 のサイロ型のシステムであったのに対し、クラウド環境においては、サーバーは統合され、仮想化される。

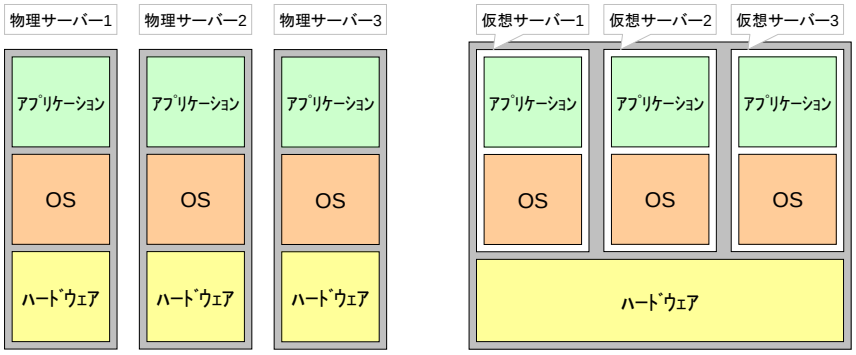


図 4-5 サーバー仮想化の基本概念

統合され仮想化されたサーバー環境は、例えば 4 つのコアを持つ CPU が複数個、一つのサーバー筐体の中に存在し、仮想化層のハイパーバイザー上に複数個の OS が存在し、OS 上には例えば JavaEE などのミドルウェア、そしてそれぞれのミドルウェア上に個別のアプリケーションが存在する環境が考えられる。

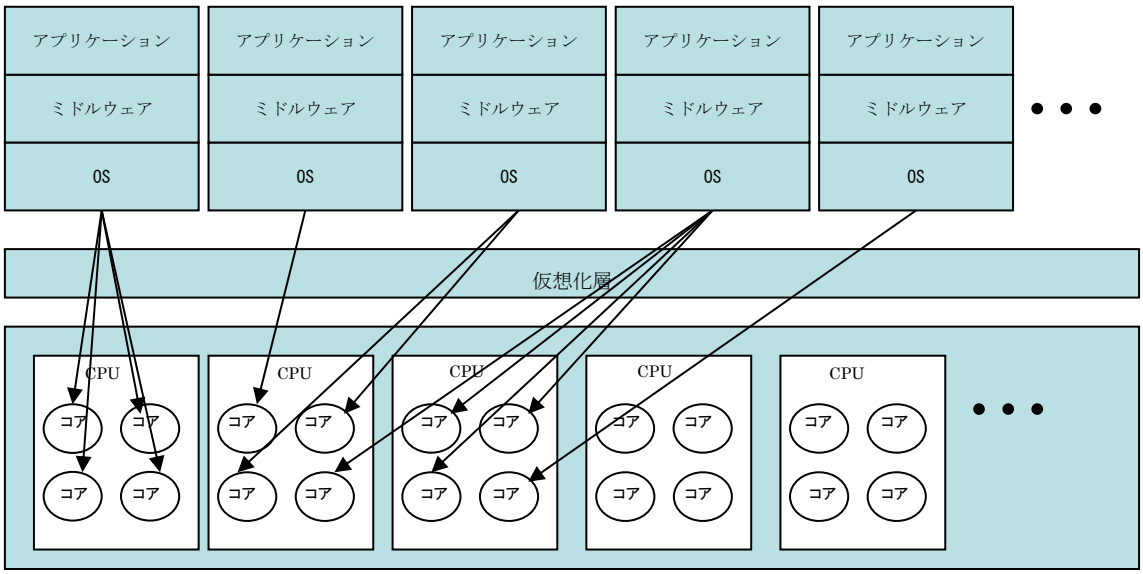


図 4-6　サーバー仮想化環境における OS と CPU コアの関係

このような環境でのソフトウェアは、

① 仮想化層を構成するソフトウェア（例：ハイパーバイザー）

② OS

③ ミドルウェア

④ アプリケーション

これら全てのソフトウェアにおいての使用許諾契約（EULA：End User License Agreement ）やライセンス契約の内容に基づいて利用されているかどうかを常に管理しなければならない。具体的には、ハイパーバイザーや OS、ミドルウェア、アプリケーションのそれぞれの使用許諾条件において、その条件に物理的な CPU 数やコア数、サーバー数での制限などへの考慮が考えられる。

また、クラウド環境では柔軟なプラットフォームが求められるため、OS が使用する CPU コア数をポリシーベースの運用により動的に変化させることが考えられる。その場合、OS に紐づくミドルウェアのライセンス契約が CPU コア数による制限があった場合は、契約しているコア数を考慮にポリシーを設計しなければならないし、使用するコア数を常に監視し、管理しなければコンプライアンス違反を犯してしまうことも考えられる。

クラウド環境は、SOA 化（Service Oriented Architecture：サービス指向アーキテクチャ）により俊敏性やスケーラビリティなど、特にミッションクリティカルな基幹システムの運用では優先度に応じて優先的に CPU リソースが割り当てられる。その場合、IT アーキテクトは基幹システムの可用性を重視するあまり、そのシステムを構成しているインフラストラクチャのソフトウェアライセンス契約の内容までの順守に運用設計の考慮を怠ることもある。あるいは、設計者は「後は運用チームがなんとかしてくれるだろう」と運用者にゆだねてしまうことも考えられる。

柔軟な環境を構築すれば、当然、システムの優先度に応じた CPU リソースの再配置がどこかのタイミングで発生する。全くスケールアウトや動的なプロビジョニングを行わないシステムであればクラウドとは言えないのだから、当初は予定になくとも、いずれは CPU リソースの再配置が行われるという前提で、ライセンス契約の内容を加味したポリシーを設計し管理しなければならない。

具体的には、例えば「アプリケーション A」 と「アプリケーション B」という異なるアプリケーションが稼動しているのは、「ミドルウェア C」という同じミドルウェア上だった場合、当初「ミドルウェア C」が使用する CPU コア数の契約が 6 個と仮定する。「アプリケーション A」はミッションクリティカルな基幹システムで優先度が高いので、必要に応じて優先度の低い「アプリケーション B」に割り当てられている CPU コアを一つだけ「アプリケーション A」に動的に再配置できるポリシーを設計したとする。この場合は、動的なリソース再配置の結果、「ミドルウェア C」が使用する CPU コア数の合計が 6 個と再配置前と変わらないので、「ミドルウェア C」のライセンス契約である「CPU コア数 6 個までの使用許諾ライセンス」の条件に違反がないので問題はない。(図 4-7)

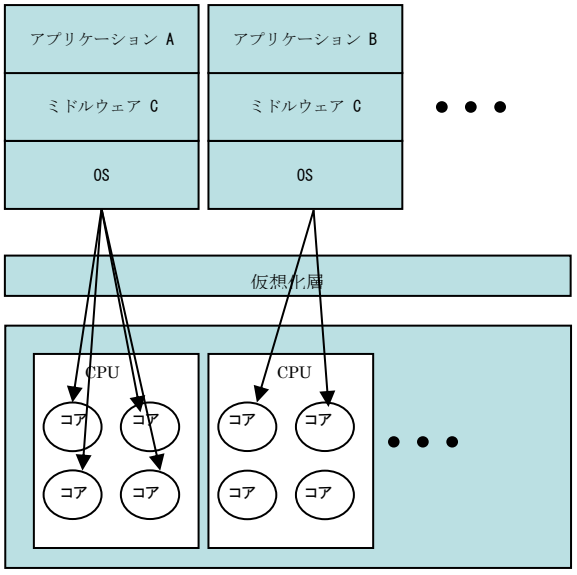


図 4-7 仮想環境におけるアプリケーションと CPU コアの関係

ところが、「アプリケーション A」の CPU コアを「アプリケーション B」ではない「アプリケーション X」に割り当てられた CPU コアを 2 個、再配置したとすると。(図 4-8)

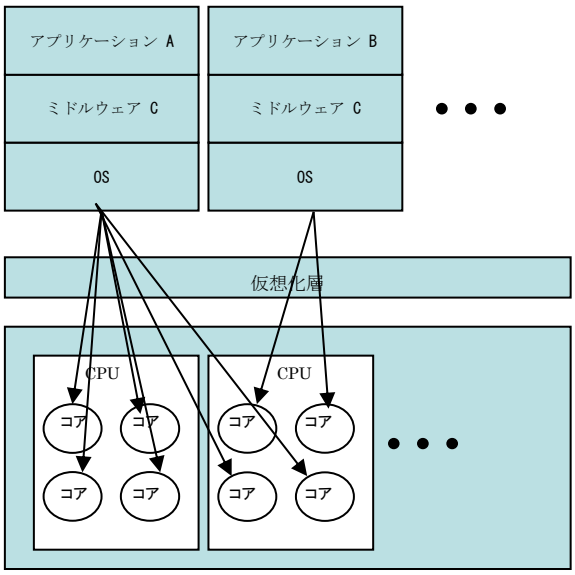


図 4-8 アプリケーションに対する CPU コアの再配置

この場合、「ミドルウェア C」が使用する CPU コア数の合計が 8 個となり、ライセンス契約において「CPU コア数 6 個までの使用許諾ライセンス」となっているので、2 個の CPU コアライセンスをオーバーして使用していることとなる。これは、ライセンス契約違反となりコンプライアンス違反が発生することになる。

ビジネス環境はめまぐるしく変化する。気が付けば「アプリケーション B」の優先度が「アプリケーション X」の優先度に勝るようになり、「アプリケーション A」は、さらに優先度が増したので追加可能な CPU コア数を増加させた、などという状況は発生するだろう。運用ポリシーを再検討するなど、何らかの変更が発生する場合は、物理的な影響分析だけではなく、その変化にともなうソフトウェアライセンス契約も考慮しなければならない。

このようにサーバー仮想化環境では今までのサイロ型のシステムでは無かった新たな考慮点が出現するのである。特に複雑さを隠蔽し自動化のシステムを提供するハイパーバイザーなどを使用する場合は、自動化され動的に変化する運用環境のソフトウェア資産管理を今までのサイロ型システムの管理同様に人手だけに頼って管理することは不可能なのは明らかである。

もちろんそのような事は織り込み済みで、それらを考慮した運用管理の手法が IT サービス管理では既に提唱されている。例えば、IT サービス管理（ITSM）のベストプラクティスである ITIL（IT Infrastructure Library）や、その国際標準である ISO/IEC20000、国内標準である JIS Q 20000 では、構成管理データベースにより管理対象となる構成品目（Configuration Item：CI）の関係を管理するとしている。

2.5 構成管理データベース、CMDB（configuration management database）
各構成品目に関連するすべての詳細、及びそれら構成品目間の重要な関係の詳細を含むデータベース。
（JIS Q20000-1:2007 2.5 構成管理データベース、CMDB（configuration management database）より引用）

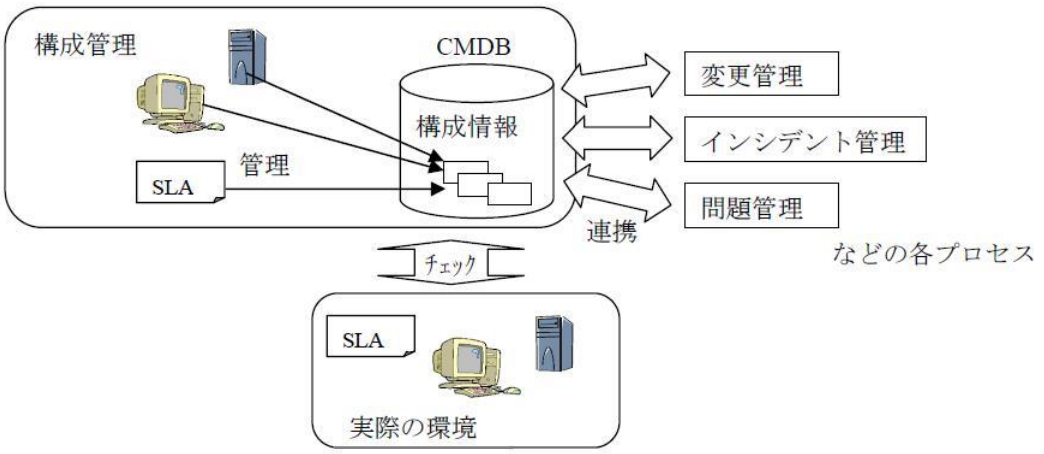


図 4-9 CMDB：構成管理の概要[2]

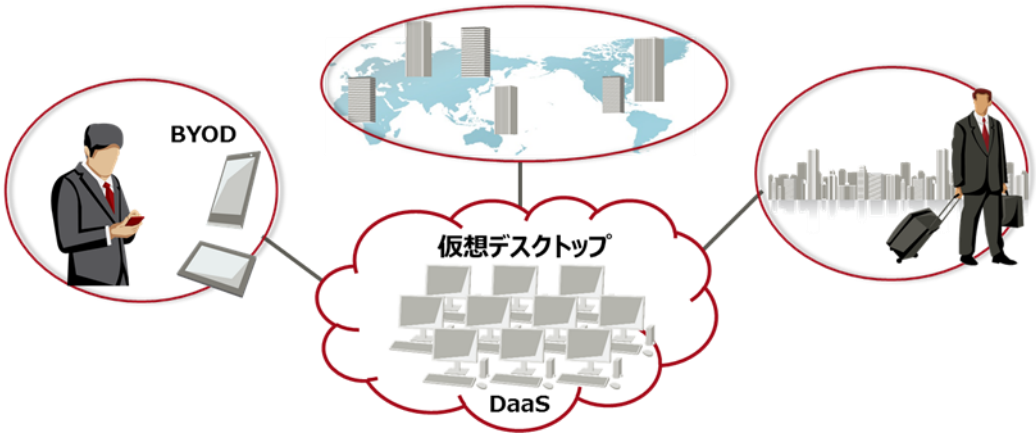
統合運用管理のソフトウェア製品などでは Application Dependency（アプリケーション依存関係）の検出やマッピングのソフトウェアが存在するが、ソフトウェア資産管理においてはアプリケーションの依存関係を可視化するだけでは管理不足であり、アプリケーションやミドルウェアなど、システムを構成する全てのソフトウェアのライセンス契約を当該ソフトウェアと紐付け、そのシステムに割り当てられた CPU リソースを含む全ての構成品目を紐付けた構成管理データベースによりライセンス契約に基づいてコンプライアンス

[2] JIPDEC　ITSMS ユーザーズガイドーJIS Q 20000(ISO/IEC 20000)対応ー 平成 19 年 4 月 20 日出版 より抜粋。詳しくは、www.isms.jipdec.jp/itsms/doc/JIP-ITSMS111-10.pdf

違反が発生していないかどうかを実際の環境との突合などにより、常に監視し、管理することが肝要となる。

5. クラウドにおける今後の課題と留意点

活用される機会が増えてくるクラウドであるが、特に普及が予想されるクラウド型の VDI（Virtual Desktop Infrastructure）である DaaS（Desktop as a Service）とその普及に伴い増えてくると予想される BYOD（Bring Your Own Device）について説明する。最初に、そもそも DaaS に対して世間はどのような期待を持っているのか列記する。



DaaS への期待

1. オフィス環境の柔軟性（組織改革、事業所移転、海外展開）
2. ワークスタイル変革（どこでもオフィス、BYOD）
3. スモールスタートとスピード（ニーズ優先、アジャイル）
4. 標準化と共通化（ツール乱立防止、情報共有）
5. 運用負荷軽減（新入社員や人事異動時キッティング作業自動化）
6. セキュリティ強化（情報漏えい対策、ウイルス/パッチ適用の徹底）
7. アプリと端末 OS の分離（ライフサイクルの適正化でアプリ開発/維持コストの削減
8. 標準化と共通化（ツール乱立防止、情報共有）

図 5-1　DaaS への期待

メリットのみであるように思われるが、現実は、この良い点のみに着目し、現実の技術レベル、環境整備が追い付いていないことに伴う落とし穴がついて回る。企業における ITAM の観点から課題と留意点を考える。

5.1. VDI（DaaS）の展開について

DaaS はクラウド上で展開される VDI であるが、その基本である VDI の構成要素は以下の通りである。

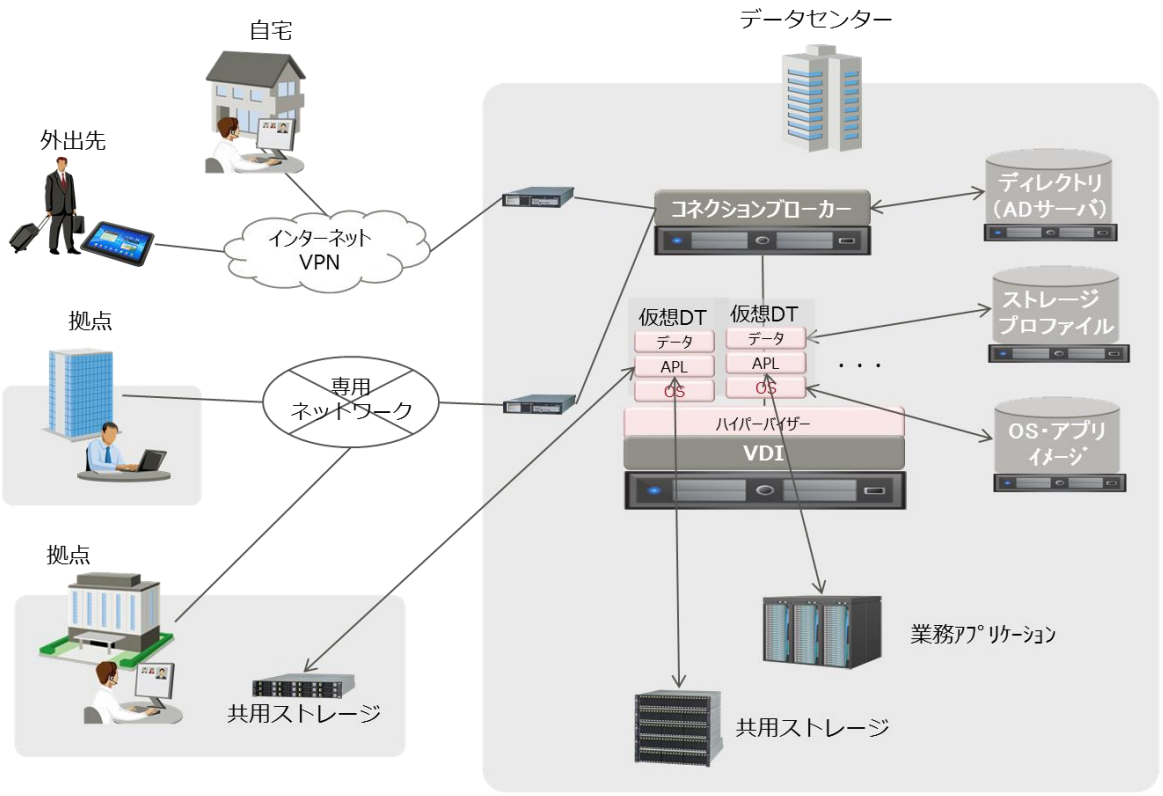


図 5-2　VDI の基本構成要素

- クライアントデバイス
  仮想マシンにリモート接続する。専用端末としてシンクライアントを使う場合や既存のパソコン、タブレットやスマートフォンなどのスマートデバイスが使われる。
- コネクションブローカー
  クライアントデバイスから接続要求を出したときに、ディレクトリーサーバーと連携し、仮想マシンを割当る。
- ディレクトリーサーバー
  コネクションブローカーから認証の要求を受け正しいユーザーかどうかを確認する。
- VDI（仮想インフラストラクチャ）
  仮想マシンを動かすインフラストラクチャである。仮想化製品で仮想化されたサーバー、ストレージによって構築される。

・ 仮想デスクトップ
仮想インフラストラクチャ上で動作する仮想マシンを指す。Windows、Linux などのクライアント OS が使われる。

DaaS(Desktop as a Service)とは、この VDI をクラウドのインフラを使用し、サービスとして利用者に提供するものである。DaaS 業者により、サービスの考え方が微妙に違っており、それに伴う課題、留意点も多く現れてくる。以下では、DaaS に対する ITAM の基本機能を以下の視点で記述する。

・ データ管理
・ ライセンス管理
・ 関係及び契約管理
・ 財務管理
・ サービスレベル管理
・ セキュリティ管理

5.1.1. データ管理

ITAM においては基礎となるデータが正しく収集されていることが要件である。DaaS としては以下のものが要求される。

- DaaS で提供される VDI のスペック情報
- VDI で動作するアプリケーションソフトウェアの情報

エンドユーザーにソフトウェアのインストール権限を与えるかどうかで必要とするレベルが変わってくるが、配付で与えた環境以外のインストールを許している場合、実体情報の収集が必要である。

- 改竄される可能性のあるソフトウェアのファイル情報

IPA 等の脆弱性報告を検知できるデータであることが要求される。

- 利用者の情報

契約しているアカウントの情報と利用者が対応付けて管理されていることが必要である。例えば、契約しているアカウントの数と利用数だけの情報だと現実問題として利用者に改善の情報を通知できない。

- 利用状況

VDI の利用状況を把握することは、サービスが妥当かどうかについてモニタリングするために必要とする。

上記のデータが正しく記録されているかどうかについて定期的に検査し、間違いがあれば、原因を究明し、対策を講じなければならない。

5.1.2. ライセンス管理

DaaS で VDI を提供している場合、DaaS 業者や契約の内容の違いによってライセンス管理の内容が変わってくる。DaaS 自身の契約に含まれるもの、VDI 上で動作するために必要となるもの、及び、既保有のソフトウェアライセンスが利用できるもの、など色々なケースがあり、間違えることが多くなる。しかし ITAM ではライセンス購入時及び資産変更時に権利の理解と権利を説明する方法（説明責任）をライセンサーが正しく確認することを要求している。これを正確に履行するなら、ライセンス管理は正しく行える。以下では、ライセンス管理が ITAM の要求事項に沿って正しく行われるとして、特に注意を要する事項について説明する。

(1) VDI ソフトウェアのライセンス：
ヴィエムウェアの「VMware Horizon」、シトリックスの「Citrix XenDesktop」、マイクロソフトの「Microsoft VDI」などがある。通常ライセンスは、DaaS の契約に含まれているが確認しておく。

(2) VDA（Windows Virtual Desktop Access）ライセンス：
Windows Server OS ライセンス (SPLA)は、通常 DaaS 事業者が DaaS の契約の中で持っているが、VDI の Windows の OS がクライアント OS の場合、VDA ライセンスが必要となる。但し、Microsoft 社のボリュームライセンスにある、ソフトウェアアシュアランス（SA）契約を結ぶことで、VDI 上でクライアント OS を利用できるようになる。ここで注意しなければならないのは、クライアント OS の Professional Edition、Windows Embedded を使用したシンクライアントはこの SA の対象にはならないこと、iOS や Android などももちろん対象にならない。従って、VDA ライセンスが必要となる。また、VDA ライセンスにもデバイスライセンスとユーザーライセンスがあり、VDI の利用形態によってどちらかを選ぶことになる。

(3) サーバーVDI：
VDI に Windows のサーバーOS を持ってくることで VDA のライセンスを不要とすることもできる。サーバーOS はクライアント OS より割高であるが、Windows Server 2012 R2 Datacenter のような 1 つのプロセッサライセンスで無制限に仮想インスタンスを実行できるようなライセンスを使えば、クライアントはサーバーCAL のライセンンスだけで VDI にアクセスできる。DaaS 業者によっては、アカウント単位に CAL のライセンスを含めることにより、利用者が CAL を意識することが無く契約ができるようにしているところもある。ただ、サーバーOS は完全にクライアント OS と互換があるわけではないので VDI 上で利用するアプリケーションは事前に動作テストを行っておくことが必要である。

(4) VDI 上のアプリケーション：

VDI 上の動作可能なライセンスであるかどうかをライセンサーに確認しておく。また、ユーザーライセンス、VDI 単位のライセンス、VDI の能力が関連するライセンス、ユーザーデバイスが関連するライセンス、CPU ライセンス、アカウントライセンスなどの可能性も調査し、また、DaaS の管理機能でこれらの情報が取得できるかどうかも確認し、方式を変更することでコストが削減できないかも十分調査する。購入ライセンスと DaaS 上で動作しているアプリケーションにライセンス違反がないか定期的にチェックし、違反がある場合には早急に対応する。

5.1.3. 関係及び契約管理

DaaS 業者との契約、及び、VDI 関連ソフトウェアベンダーとの契約を管理する。VDI では、どこにユーザーのデータを記録させるかということが問題になる。VDI の使われ方次第ではあるが、通常このストレージについては、データの共有範囲が国内のみなのか海外拠点を含めるのかによって各種の法規制を考慮し、調整が必要となる場合がある。また、DaaS 業者との契約では、デスクトップインフラを任せるのであるから、BCM（BCM: Business continuity management）の視点から業者の分析を定期的に行い、評価すべきである。

以下は、経済産業省がクラウドサービスを利用する上で留意すべき法規制をまとめているので紹介する。

http://www.meti.go.jp/committee/sankoushin/jouhoukeizai/jinzai/002_02_03d.pdf

表 5-1　クラウドサービスを利用する上で留意すべき事項

データの物理的保存場所がわからない場合がある 海外の大規模クラウド事業者が提供するサービスの場合、自分のデータがどの国に設置されたサーバーに保存されているかを特定できない場合がある 法規制上の制約（後述）や、司法の実効性を考えた場合、国内のサーバーに保存することを確約する事業者を選択することも必要
隣接利用者の影響を受ける場合がある 低価格のクラウドサービスの場合、１台のサーバー上に複数の仮想マシンを設定し、多くの利用者の共用として運用するのが一般的 結果的に、同じサーバーを用いる利用者が負荷の高い処理を行うと、自分の処理速度が低下することがある こうした影響を回避するには、１台のサーバーを占有できる「物理的アイソレーション」の付加サービスを利用する
クラウド事業者の都合でサービスが中止される場合がある 多くのクラウドサービスの契約条項には、事業者の都合でサービスを中止する可能性があることが示され、それに合意することが利用の条件となっていることが多い 特定のクラウドサービスの仕様に特化した運用をしていると、こうしたサービスの中止時の移行コストが高くなる

表 5-2　クラウドを利用するにあたって考慮すべき法規制等

米国愛国者法（USA Patriot Act）

1. 2001年9月11日に発生した同時多発テロ事件を受け、捜査機関の権限の拡大や国際マネーロンダリングの防止、国境警備、出入国管理、テロ被害者への救済などについて規定
2. テロリズムやコンピュータ詐欺及びコンピュータ濫用罪に関連する有線通信や電子的通信を傍受する権限を明記するとともに、捜査機関は金融機関やプロバイダの同意を得れば、裁判所の関与を求めることなく操作を行うことができることを規定
3. 米国サーバーにデータを保存する場合は、政府機関の捜査権限が大きいことに留意が必要
4. クラウドサービスを利用する場合、仮想的に分離された環境であっても、他ユーザーと物理的に同一のサーバー機器などを共有している場合があるため、他ユーザーが捜査を受けることで、自社もシステム停止などの影響を受けるリスクがある

EUデータ保護指令（Data Protection Directive）

1. EU内の住民の個人情報に関して十分なデータ保護レベルを確保していない第三国へのデータの移動を禁止
2. 十分な保護水準を確保している国・地域は、スイス、カナダ、アルゼンチン、ガンジー島、マン島、ジャージー島の６つのみ
3. 米国はEUとの間でセーフハーバー協定を締結することで、その認証を受けた企業・組織へのデータ移転が可能となっているが、ドイツは2010年に同協定のみでは不十分であると表明
4. クラウドサービスでEU内の住民の個人情報を扱う場合は、同指令に準拠した保存ができるよう立地等を考慮してサービスを選定する必要がある

外国為替及び外国貿易法（外為法）

1. 国際的な平和及び安全の維持を妨げることがないよう、特定の技術を特定の外国において提供する際や特定の外国人・外国企業に提供する際には、経済産業大臣の許可が必要と規定
2. 日本国内から海外の外部サーバーに情報を送信する際や、当初から外国の利用者に情報を提供することを目的に自社の海外サーバーに情報を送信する際、国内サーバーのリソースを演算処理等のために提供してその結果を送信する際等も、許可の対象となる場合がある
3. 対象となる情報は核兵器等の大量破壊兵器や通常兵器に関連した技術であるが、この技術の中には暗号技術などの汎用的な技術も多く含まれるため、これらの情報を取り扱う際には留意が必要

米国輸出管理規則

1. 自国で開発されたソフトウェアの輸出を規制
2. 日本国内のクラウド事業者が他国のソフトウェアをクラウドサービスの中で提供する場合には、各国の輸出規制に準拠しているかどうかに留意する必要がある

不正競争防止法

1. 「営業秘密管理指針」において、営業秘密としての保護を受けるためには、「当該情報を他情報と区別して、より高度な管理を行うことが望ましい」旨を定めている
2. 社外サーバーへの情報の保管は、管理状況によっては、営業秘密としての保護を受けられない場合もありうることに留意が必要
   逆に、安全管理が徹底されている社外サーバーの場合には、社内サーバーよりも安全性が高い場合もあり得る

e-文書法（民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律）
1. 記録を外部のサーバーへ保管することに関しては必ずしも考慮されていないため、個別の法令によっては、データの外部保存に関して一部制約が残っている
例：割賦販売法施行規則：帳簿を主たる営業所に備えることを規定
法人税法施行規則：帳簿を納税地に保存することを規定
医療情報システムの安全管理に関するガイドライン（第４．１版）
以下の条件を満たす場合は、目的に関係なく外部に保存することが可能
①病院、診療所、医療法人等が適切に管理する場所
②行政機関等が開設したデータセンタ等
③医療機関等が民間事業者等との契約に基づいて確保した安全な場所

5.1.4. 財務管理

DaaS 業者との契約情報、及び DaaS 関連ソフトウェアから費用を計上し、データとして関連部署（特に財務部門と利用部門）に定期的に報告する。DaaS に関係するクライアントのハードウェア情報、ソフトウェア情報などの費用も全体の IT 資産の財務データとして一緒に報告する。

5.1.5. サービスレベルの管理

DaaS 業者との SLA（Service Level Agreement）の内容について、社内のエンドユーザーの要求（何のために DaaS を導入するのか）にあっていることを確認する。そして、この SLA を記録として残し、定期的に遵守状況を評価することが必要である。また、このことは、DaaS 業者だけでなく、WAN の提供業者、インターネットとの接続についても言えることである。

注意したいのは、エンドユーザーの要求事項によっては基幹業務用端末と同レベルでの性能と安定性を求められることがあり、代替手段等の準備状況を含めて、DaaS に期待するサービスレベルを決めなければならない。

5.1.6. セキュリティ管理

DaaS 導入に関する IT 資産へのセキュリティ管理については、ネットワークに関するもの、端末デバイスに関するもの、VDI に関するものに特に注意が必要である。

(1) ネットワーク

クラウド型の VDI に踏み切るうえで一番のネックになるのはネットワークの問題である。VDI から企業内に構築した業務システムをアクセスすることは、利用者のデバイス→コネクションブローカー⇒AD サーバー⇒コネクションブローカー→クラウド内の VDI⇒企業内の業務サーバー⇒クラウド内の VDI→利用者のデバイスの通信を行うことであるが、

→で示した通信は、デスクトップの画像データであり、セキュリティよりもむしろ、安定性、スピードといった品質面の要請が強い。逆に、⇒の部分はデータ通信であり、通信の品質よりもむしろ、セキュリティ面から要請が強い。従って、→の部分はインターネットでも良いが、⇒の部分は、セキュアな通信、インターネット VPN や専用ネットワーク接続が推奨される。

以下は、Amazon の場合のインターネット網と専用ネットワーク接続の例（図 5-3 専用ネットワーク接続（Direct Connect））とインターネット網とインターネット VPN 接続の例（図 5-4 Amazon の VPN 接続（VPN Connection））である。

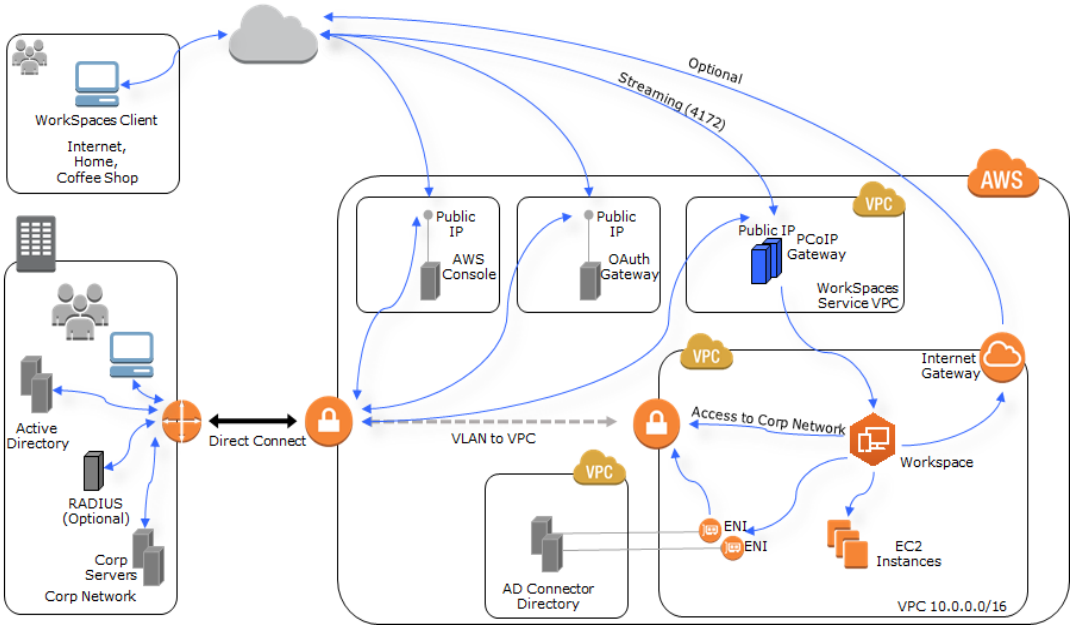


図 5-3　専用ネットワーク接続（Direct Connect）　※Amazon HP より

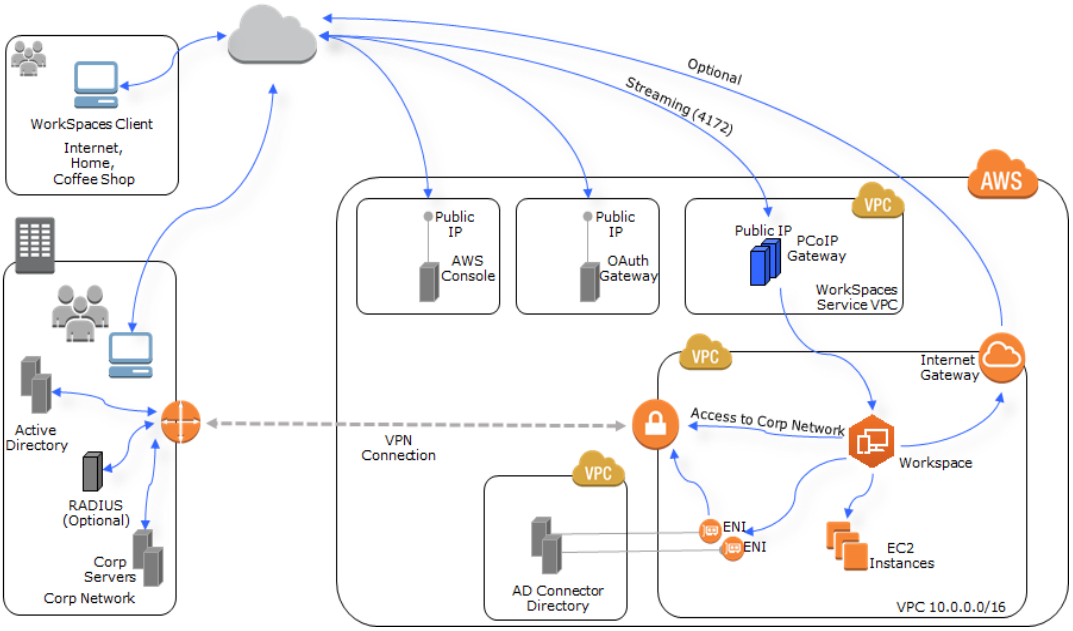


図 5-4　Amazon の VPN 接続（VPN Connection）　※Amazon HP より

(2)　端末デバイス

BYOD については後の章で記述するので、ここでは、企業の端末デバイスについて ITAM のセキュリティ要件について考える。

VDI への期待で情報漏洩対策を上げたが、VDI の端末ソフトウェアには USB などの外部記憶装置の接続を許可するポリシーを設定できる。また、持ち運び等で盗難に合う場合もある。いずれにしても企業におけるどの端末に VDI へのアクセスを許しているのかとそのポリシーについて記録し、定期的に検証する必要がある。

(3)　VDI

VDI に対する要求事項は、導入する部門によって異なる。VDI に割り当てるマスターを変更することで対応するが、マスターが増えると運用が大変になるので標準化とのバランスで決めるべきである。OS のスペック、インストールするアプリケーション、USB への記録の有無、印刷機能の有無など、DaaS の導入目的に設定する。また、アクセスを許可している社内システムやストレージなども明確にする。セキュリティ要件と設定内容を確認するとともに記録し、定期的に検証する必要がある。

DaaS 業者は、ウィルス対策をオプションとして提供している場合が多いので利用することをお勧めする。独自に導入する場合、ディスク I/O やネットワークに思わぬ負荷をかけることになるので注意を要する。

5.2. BYOD の展開について

BYOD (Bring your own device)は、従業員が個人保有の携帯用機器（スマートフォン、タブレット、パソコンなど）を職場に持ち込み、業務に使用することであるが、現状、リスク管理の観点で、セキュリティが確保されているとは言い難い。インターネット VPN で認証している場合でも、個人のデバイスに情報を記憶させないようにしたり、セキュリティ条件にあったデバイスかどうかチェックしたり、認証方式のセキュリティが十分かなど多くの配慮や運用の手間が必要になる。ましてや、BYOD の PC を企業の LAN に Wifi などで直接接続させたいなどの要求事項がある場合、セキュリティ条件の設定、そのための検討作業、様々な防御策を運用する工数など膨大なものとなる。

また、ここで設定するセキュリティ条件もユーザーの要件で骨抜きにされることが多々ある。例えば、外出先でメールとかスケジュールを見られるようにしたいが、このアプリケーションではユーザーのデバイスに情報がダウンロードできてしまうなどだ。しかし、これら BYOD の問題も VDI（DaaS）と組み合わせることで解決可能となってきた。以下では、VDI(DaaS)を前提にした BYOD で ITAM における課題と留意点を記述する。

- データ管理
- ライセンス管理
- 関係及び契約管理
- 財務管理
- サービスレベル管理
- セキュリティ管理

5.2.1. データ管理

BYOD で DaaS の仮想デスクトップのみにアクセスさせることにすれば、BYOD のデータ管理は、アクセスを許可する BYOD 情報を記録するだけで、データ管理における課題・留意点は VDI（DaaS）の展開で記述した事項のみだ。BYOD としては、申請者と端末識別情報を申請システムなどで記録し、インターネット VPN や VDI へのアクセスログを記録しておくことで十分と言える。

また BYOD は、使用しなくなるときが把握しにくいので、一定期間利用が無ければ自動的に許可を取り消しにすることも必要である。

5.2.2. ライセンス管理

BYOD は私物であるが、VDI（DaaS）やインターネット VPN にアクセスするソフトウェアは、企業がセキュリティ要件に従った設定にして提供することが望ましい。申請ルールや登録情報を利用して、ライセンス管理が可能となる。また、前にも記述したが、BYOD

は使用されなくなる時が把握しにくいので、先のデータ管理の情報をもとに、一定期間利用されない場合、自動的にライセンスも返却する仕組みを入れておくことが必要と思われる。

(1) VDI クライアントソフトウェア

ヴィエムウェアの「VMware Horizon View Client」、シトリックスの「Citrix Reciever」などが相当するが、DaaS によって、VDI にアクセスするライセンスが DaaS の料金に含まれている場合もある。仮想化デスクトップの OS が windows クライアント場合、VDA ライセンスが必要になる。VDA ライセンスには、ユーザー単位のライセンスとデバイス単位のライセンスがあるので、ユーザー単位のライセンスにして、DaaS のアカウント発行時に DaaS の料金に含めるようなサービスにすれば、ユーザーは、VDA を意識しなくて済みそうだが、現状の DaaS 事業者は、VDA をユーザーに準備させる場合が多いようだ。

(2) インターネット VPN クライアントソフトウェア

Cisco の AnyConnect Secure Mobility Client などでは、AnyConnect Plus ライセンスまたは AnyConnect Apex ライセンスを購入する必要があるので、期間とかユーザー数でなどライセンスを購入するようになっている。

5.2.3. 関係及び契約管理

BYOD の導入に際しては、個人への費用負担（福利厚生費）や安全性、責任分担などを取り決め、記録して置く。

5.2.4. 財務管理

BYOD 導入で IT 投資と運用のコストがどう変化しているのかモニターし、定期的に評価する。

5.2.5. サービスレベル管理

エンドユーザーとの間で BYOD の利用に対する要件をセキュリティ要件と合わせて確認して置く。また、実施状況をモニターし、サービスレベルの評価を定期的に行う。

5.2.6. セキュリティ管理

今回の前提である「BYOD には、DaaS（VDI）のみの利用を許可する」とすれば、セキュリティ管理の大半は 5.1.6 で記述されている。しかし、BYOD そのもののセキュリティ管理について考慮しなければならない課題と留意点は残る。以下にその要点を述べる。

- BYOD で社内 LAN への接続を許可するなら、BYOD の記憶装置には企業の情報を保存できないようにして置く
- 社内 LAN に直接接続できる BYOD は、企業が設定しているセキュリティ要件を事前にチェックし、満たしていない場合には LAN を使用できないものとする。
- インターネットで DaaS に接続する BYOD の認証は ID/PWD 方式が多いが十分セキュリティが保証されるような運用にする。

付属資料１

クラウドにおけるライセンス契約等の当事者（IaaS、PaaS、SaaS の違い）

<table>
<tr><th></th><th>IaaS
Infrastructure as a Service</th><th>PaaS
Platform as a Service</th><th>SaaS
Software as a Service</th></tr>
<tr><td>Client</td><td>エンドユーザー</td><td>エンドユーザー</td><td>エンドユーザー</td></tr>
<tr><td>Application software</td><td rowspan="2">エンドユーザーがソフトウェアベンダーとアプリケーションソフト及び OS の使用許諾契約を直接締結する。これらのソフトはクラウド事業者の指定するハードウェア領域にインストールする。</td><td>エンドユーザーがソフトウェアベンダーとアプリケーションソフトの使用許諾契約を直接締結する。</td><td rowspan="3">クラウド事業者はハードウェア＋OS に加えて、アプリケーションソフトの機能まで完全にサービス化して提供する。</td></tr>
<tr><td>Platform (Middleware: OS 、 DBMS 、 etc.)</td><td rowspan="2">クラウド事業者はハードウェア＋OS（及びミドルウェア層）までをサービス化して提供する。</td></tr>
<tr><td>Infrastructure (Hardware: Server 、 Network、 etc.)</td><td>クラウド事業者はハードウェア（演算装置、ストレージ、ネットワーク機器）までをサービス化して提供する。（本来の NIST の定義では IaaS には OS は含まれない。）</td></tr>
</table>

付属資料２

クラウド時代の ITAM の課題（ITAM の目的と、仮想化技術・クラウド・オンプレミスにおける課題）

		仮想化技術	クラウドコンピューティング	オンプレミス（自社施設内）
(1)リスク管理	a)説明責任	● 説明責任範囲が拡大し、説明の難易度がアップする ● 仮想化ライセンスの適合性証明のために特別な環境を要する ● 仮想化レイヤーにおける障害発生時の原因解析負荷が大きい ● データの所在が特定できないためデータベース監査対応が困難	● 提供アプリケーションに社内システムが対応していない可能性 ● サーバー・リージョンによる外為法等違反 ● 利用者が用意した範囲に関する説明責任	● 自社資産として説明責任を負う ● セキュリティ・コンプライアンスについて自社で管理 ● 全て利用者に責任があり、ハード、ソフト、ネットワーク等全てについてリスク管理の計画、実施、および改善活動を行う必要がある
	b)資産保全	● 仮想化を前提とした全社 IT 資産管理体制が必要となる	5.2.1全社的な IT 資産把握が困難 6.2.1全社的な契約状況把握が困難	● 自社資産として資産管理する
	c)法的リスクの回避	● 自動構成変更に伴う意図しないライセンス違反の可能性 ● 仮想化ライセンス条件の理解不足によるライセンス違反リスク	● ライセンス利用状況の把握不足による意図しないライセンス違反 ● CSP のライセンス条件解釈誤りによる間接的ライセンス違反 ● CSP のインスタンススペック	● 自社資産としての法的リスク ● ライセンス管理不徹底により保有ライセンス証明ができなくなる ● カジュアルコピーによるライセンスコンプライアンス

			変更に気づかずBYOLソフトを利用したことによるライセンス違反	違反
	d)セキュリティ上の問題への対処	● ホストOS障害による複数インスタンスでの業務停止 ● 物理的環境に複数の論理的環境が並存することに伴うセキュリティリスク、アクセス権、トラブル対応 ● 仮想化デスクトップのリスクの理解度の低さ	● CSP従業員による情報漏洩 ● 不適切な設定による踏み台化 ● シャドーITへの対応リスク	● 自社資産のセキュリティ問題として対処する ● データ消去の不備によりデータが漏洩する可能性 ● バックアップの不備によりデータが消失する可能性 ● マルウェア等のインストールによる情報セキュリティ事故発生の可能性
	e)可用性の確保	● ハードウェアの仮想化による対障害性の向上	● 経営不振による事業停止リスク ● サービス継続性リスク	● 自社資産として冗長性を備える

	仮想化技術	クラウドコンピューティング	オンプレミス（自社施設内）
(2)コスト管理（TCO 削減等）	● ハードウェア台数削減による使用電力、フロア、運用管理工数の削減 ● 標準インスタンスの展開による構成管理の簡素化 ● トライアルによる撤退費用低減 ● 需要変動時に対するリソース運用の柔軟性	● 一般にはスケールメリットがあるため自社運用と比べて低コスト、高サービスレベルになる ● 同じサービスを長期間継続利用すると購入した場合より割高になる可能性がある	● システム構築の初期費用、維持管理費用がクラウドより高くなる ● 過剰ライセンスを調達する可能性 ● 過剰ハードウェアを調達する可能性 ● 他部門で利用可能なハードウェアを廃棄してしまう可能性
(3)競争上の優位性（IT 資産の有効活用）	● 運用管理の標準化・自動化 ● ビジネス要求への迅速な IT 対応	● 過去の投資資産に縛られず、企業の成長に合わせて常にその時点でのベストサービスを選択できる	● スケーラビリティが硬直化するため、組織の成長に合わせて最適な環境を提供できないリスク
(4)その他事項	● 仮想化を前提とした最適化の必要性	● データ移転制限リスク（欧州） ● 複数 CSP をベースにしたサービスを利用する場合契約条件に留意する必要がある ● 外部監査を受ける場合 CSP が外部監査に必要な証跡を提供できず、監査証明が受けられないリスク	

IT 資産マネジメント評価検討委員会
「クラウド時代の ITAM の考え方」
作成メンバー

（敬称略）

氏名	会社/機関名
篠田　仁太郎 （委員長）	㈱クロスビート
今田　英顕	日本電気㈱
塩田　貞夫	洛 IT サービスマネジメント ㈱
高橋　快昇	富士通㈱
田村　仁一	有限責任監査法人トーマツ
中村　究	タレンタ㈱
野間　恭介	新日本有限責任監査法人

氏名	会社/機関名
高取　敏夫	一般財団法人日本情報経済社会推進協会
諸橋　智江	