The Software Alliance

BSA

NAVIGATING THE CLOUD

ソフトウェア資産管理が以前に増して重要課題となる理由

目次

エグゼクティブサマリー

クラウドコンピューティングの登場によって、ライセンスコンプライアンスに対する懸念は解消されるとかつて考えられていました。サービスプロバイダーが、単純にリモートサーバーから必要なコンピューティングリソースを提供し、その利用に応じて課金するだけ — だから、問題も混乱もなく、不注意による著作権侵害もなくなり、法的リスクもない、と考えられていたのです。

今日まで、クラウド環境においてソフトウェア資産管理（SAM）を行う理由およびその方法について、実用的な指針はほとんどありませんでした。本レポートはこれらの指針を網羅するものであり、組織がクラウドコンピューティング環境で SAM を構築し、運用するにあたって直面する課題を解決するための指針となるものです。

クラウドコンピューティングには、市場の多様なニーズに応えるために様々な形態があり、ライセンスコンプライアンス上のある問題が解決される場合もあれば、新たな課題が生まれる場合もあります。そのため、SAM が必要となります。

ソフトウェア資産管理はすでにビジネス環境において広く採用されていますが、その利点（コストおよびリスクの削減、運用効率の向上など）を考えれば、これは驚くことではありません。SAM はビジネスを順調に遂行するためのフレームワークに不可欠な要素となっています。

組織がクラウドへ移行した場合でも SAM は必要なのでしょうか？答えは、当然「はい」です。クラウドサービスは、従来の配布型ソフトウェアと重要な点で異なる部分もありますが、ソフトウェア資産のライフサイクルを効果的に管理する必要性が切実なのは、クラウド環境でも同じです。

SAM とクラウドコンピューティングはともに、今もなお進化を続けている複雑な概念です。そのため、様々なクラウドアプローチが SAM に与える特有の影響を検討すると、クラウドへ移行することで、組織は SAM プログラムの重点が変わる可能性があることに気付くでしょう。組織は、クラウド戦略が SAM プログラム全般へ与える影響、特に組織のソフトウェアライセンスに与える影響について、慎重かつ積極的に検討する必要があります。

組織は、どのソフトウェア資産に利用権があるか、そのうち実際に利用しているラインセンスの数、またクラウドへ移行した場合、その資産にどのような影響があるのかを把握しておく必要があります。SAM に関して熟慮をせずにクラウドアーキテクチャを採用すると、コストとリスク分析に関連する重大な過ちにつながる可能性があります。

クラウドコンピューティング

クラウドコンピューティングは、物理的なハードウェアの要素を抽出したコンピューティングリソースを使うモデルです。このような仮想化されたサービスは、通常インターネット経由でアクセスされるコンピューティングリソースへのスケーラブルなオンデマンドアクセスを提供します。クラウド・コンピューティング・サービスとして、仮想化されたコンピューティングリソースの多様な組み合わせが提供されていますが、一般的には以下の 3 つのモデルに分類することができます。即ち、Software as a Service（SaaS）、Platform as a Service（PaaS）、Infrastructure as a Service（IaaS）です。SaaS は、ウェブ・クライアント経由で配信されるオンデマンド・ソフトウェア・アプリケーションを提供します。PaaS は通常、組織がソフトウェア・アプリケーションを構築・稼働できるオペレーティングシステム、ミドルウェアおよび・またはデータベースを含むコンピューティング・プラットフォームを提供します。IaaS は、一般的に、組織がプラットフォームやソフトウェア・アプリケーションを構築できるハイパーバイザー、ストレージ、ネットワーキングなどのリソースを含むユーティリティコンピューティングインフラストラクチャーを提供するものです。クラウドコンピューティングの各モデルが、問題なく提供されて導入されれば、組織にとって、スケーラビリティ、俊敏性、スピーディーな市場展開、コスト管理といった多くのメリットがあります。

ソフトウェア資産管理

ソフトウェア資産管理（SAM）とは、組織内で利用するソフトウェア資産のライフサイクルを管理することです。SAM の目的の一つは、組織におけるソフトウェアライセンス契約の遵守です。国際標準化機構（ISO）は、効果的な SAM を実現するために必要なプロセスおよび成果を定義した SAM 国際標準規格（19770-1）を発行しています。

SAM は、ソフトウェアを利用するすべての組織に該当するものであり、すべての組織に必要なものです。そして、クラウドアーキテクチャを採用しようとする組織においては、その重要性はより一層高まっています。SAM を効果的に実施することでクラウドイネーブラーとなる一方、SAM を効果的にしない場合はクラウドコンピューティングによるコストベネフィットを得られない、またはその他の点においてもベネフィットを得ることができないことになります。

クラウドにおける SAM

組織がクラウドに移行する場合、クラウドアーキテクチャによって顕在化する多様かつ新たな課題に、SAM プログラムを対応させる必要があります。SAM の原則は変わりませんが、クラウド上でのライセンスリスクと SAM の効果的な適用は、従来の IT 環境のものとは根本的に異なります。SAM プログラムは、新しいアーキテクチャで、そのすべての複雑さとニュアンスを含めて、ハードウェアとソフトウェアが完全かつ正確に測定可能である必要があります。

クラウドにおいて SAM は資産の管理だけでなく、サービスの管理にも対処する必要があります。サービスが数分で提供、構成、再構成、リリースされるというように、クラウド環境では急速なペースで変化が起こるため、SAM は以前よりもリアルタイムなものになります。プロビジョニングの容易さとスピードにより、従来の IT、調達および SAM の手続きをバイパスしてしまい、部署あるいは個人がクラウド利用において、組織内不正利用を行うリスクは、絶えず存在することになります。クラウドにおける SAM は、この新たなリスクに対処する必要があります。組織は、総所有コスト（TCO）の計算の際、隠れたクラウドサービス費用、クラウドでのソフトウェア導入により発生する追加ソフトウェアライセンス費用やその他の新たな多くの要素を検討する必要があります。その他にも、私物端末を持ち込む BYOD（Bring Your Own Device）のような技術動向が、クラウドと相まって独自のリスクをもたらすため、SAM ではこのリスクにも対処しなければなりません。

SaaS 環境は、SAM に多くのライセンスに関係する課題をもたらします。クラウドサービスプロバイダー（CSP）がソリューションを提供する際に第三者の知的財産権を侵害した場合、組織はリスクにさらされる恐れがあります。SaaS アカウントの不正利用は、別のコンプライアンスリスクを引き起こす恐れがあります。例えば、禁止地域からのサービスへのアクセス、ユーザーアカウントの共有、システムによるユーザーの成りすまし、あるいはアクセスが禁止されている従業員以外の者（請負業者、ベンダー、または顧客など）へのアクセス権の提供などが考えられます。また、SaaS ソリューションの中には、プラグインや他のユーザー側ソフトウェアにつき、適切なライセンスと管理を必要とするものがあります。一般的に誤解されている点は、シェルフウェア（購入済みだが利用されていないソフトウェア）が SaaS ではなくなると思われていることです。実際は、効果的でない SAM により管理が行き届いていない SaaS 環境では、使われていないあるいは不要なサービスへの過剰な支出によって、コスト面で重大な影響が出る可能性があります。

PaaS および IaaS クラウドのデリバリーモデルは、他のライセンス上の問題を SAM にもたらします。これらのクラウドモデルのベースとなる仮想化が、ソフトウェアのライセンス契約で許可されていない場合があります。さらに別の事例では、ソフトウェアがインストールされている特定の仮想マシンに割り当てられた仮想プロセッサに対するライセンスではなく、基盤となるハードウェアのすべての物理プロセッサに対してライセンスを取得する必要があるなど、仮想化がコスト面に大きく影響する可能性があります。仮想環境におけるハードウェアメトリクスの測定は、ソフトウェアとハードウェアとのさらなる分離のため、より複雑になります。組織は、ソフトウェア発行者が満足するだけのハードウェアメトリクスへのアクセスと、それを測定する能力を失う可能性があります。また、クラウドへのライセンスの移行は禁止されたり、制限されたり、ソフトウェア発行者による事前承認が必要となったり、または追加のコストを伴う場合があります。さらに、クラウドから組織のライセンスを取り戻すことが許可されない可能性もあります。

組織がソフトウェア発行者との間で、オンプレミス利用について従来型のソフトウェアライセンス契約を締結している場合、このオンプレミスライセンスをクラウドでの利用へ移行することで、ソフトウェア発行者へのエンドユーザー組織のコミットメントが軽減されたり、コンプライアンス違反に対する責任を免除されたりするものでもありません。同様に、CSP が適切なライセンスを受けないまま組織に対してソフトウェア利用を可能にした場合、知的財産権侵害のリスクは権利侵害による受益者である組織に及ぶ可能性があります。責任が立証されると、契約条件によって、組織が CSP に対し償還請求が可能な場合と、そうでない場合があります。ただし償還請求が可能な場合でも、これは事後のことでしかなく、組織が責任に対処する負担を負うことは変わりありません。

SAM プログラムは、クラウドに関する戦略、設計、導入、運用、モニタリングのすべての面に十分に関わる必要があります。クラウドは、組織に様々な利益をもたらすものですが、SAM は、クラウド利用に伴うリスクを軽減しつつ、クラウドから利益を享受できるよう、組織を支援するものなのです。

クラウドにおける SAM — 何から始めるのか

SAM プログラムは、クラウドに適合したものである必要があります。その性質と取り組みの優先順位は、組織により異なりますが、以下の項目は、着手の際に推奨レベルが高い事項です。

- SAM は、初期計画およびアーキテクチャの設計から契約と交渉、CSP のサービス品質保証契約（SLA）の遵守、ソフトウェア資産管理の設計と導入、CSP からの請求の確認に至るまで、クラウド管理プロセスに十分に組み込まれる必要があります。
- SAM 担当部署は、現行の従来型ソフトウェアライセンス契約を見直し、またクラウドにおけるソフトウェア利用の規則を理解するため、ソフトウェア発行者との協議を行うべきです。クラウドが組織戦略および将来の方向性に含まれる場合は、一部のソフトウェアライセンス契約に関する再交渉が必要になる可能性があります。
- SAM 担当部署は、数ある問題の中でも、クラウドサービスのプロビジョニングとリリースのプロセス、必要とされる承認や通知、必要な制御、必要な契約条件が、利用するクラウドサービスに含まれるようにするため、クラウドに関する組織全体のポリシーを定める必要があります。
- SAM 担当部署は、現在組織が利用するすべてのクラウド（IaaS、PaaS、または SaaS）を可視化し、実際の契約を見直し、どのソフトウェア資産がクラウドで利用され、ライセンスまたは SAM 関連のリスクが他に存在するかどうかを理解しておく必要があります。

本報告書は、BSA の委託により Anglepoint Group が作成したものです。Anglepoint はソフトウェア資産管理、契約遵守などのライセンス関連サービスをフォーチュン グローバル 500 の顧客に提供する世界的なプロフェッショナルサービス会社です。本報告書で扱う内容は、いまもなお進化を続け、新たな脅威と新たなソリューションをもたらし続けていることから、本報告書は全ての内容を網羅したものではなく、または専門家のアドバイスとしてみなされるべきものではありません。

重要ポイント

- クラウドコンピューティングは、ライセンスコンプライアンスの懸念を払拭するものではなく、むしろ新たな懸念を生み出します。これらの課題はソフトウェア資産管理（SAM）を効果的にすることによって対処できるものです。
- ソフトウェア資産管理（SAM）は、従来のオンプレミスの IT 環境の組織と同様に、クラウドへ移行する組織にとっても極めて重要なものです。効果的な SAM は、クラウド イネーブラーです。
- クラウドであっても SAM の目標は変わりませんが、SAM の「手法」はクラウド環境に適合したものでなければなりません。
- SAM は、組織のクラウド戦略および導入計画において不可欠な要素であり、クラウド管理プロセスのあらゆる段階で十分に組み込まれるべきです。
- SAM は、基盤となる資産だけでなく、クラウドサービス全体を管理するために適用されるべきです。クラウドにおける SAM は、動的かつリアルタイムであるクラウド プロビジョニングの性質に対処するため、ポリシーと自動制御をより重要視すべきです。
- クラウドへの移行を検討する際には、従来型のソフトウェアライセンス契約によりライセンス コンプライアンスが保証されるという考え方に対して、特に注意する必要があります。この場合、組織はソフトウェア発行者と緊密に連携し確認する必要があります。
- BYOD は、特にクラウドサービスと併用された場合に、組織にさらなるリスクをもたらす可能性があります。
- サービスとして提供されるソフトウェアは、不正利用やシェルフウェアに関連する潜在的な課題をもたらします。

クラウド テクノロジー入門

クラウドコンピューティングの基本となる定義と関連する概念は以下のとおりです。但し、クラウドに関する技術、プラットフォームおよびアプローチは、今日も急速に進化し続けている点に留意する必要があります。

米国国立標準技術研究所（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ます[1]。

> **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、サービスなど）の集積に、オンデマンドでどこからでも簡単にネットワーク経由でのアクセスを可能にするモデルであり、最小限の管理手続とサービス プロバイダーとの連携で、素早くプロビジョニングおよびリリースされるもの。**

クラウドコンピューティングは、中でも以下の多様なトレンドとの融合によって、急速に浸透してきています。

仮想化および仮想化管理技術の成熟

ビッグデータ（非常に大規模なデータセットの収集、保存、管理、分析）

手頃な価格の大容量ブロードバンド ネットワークの普及

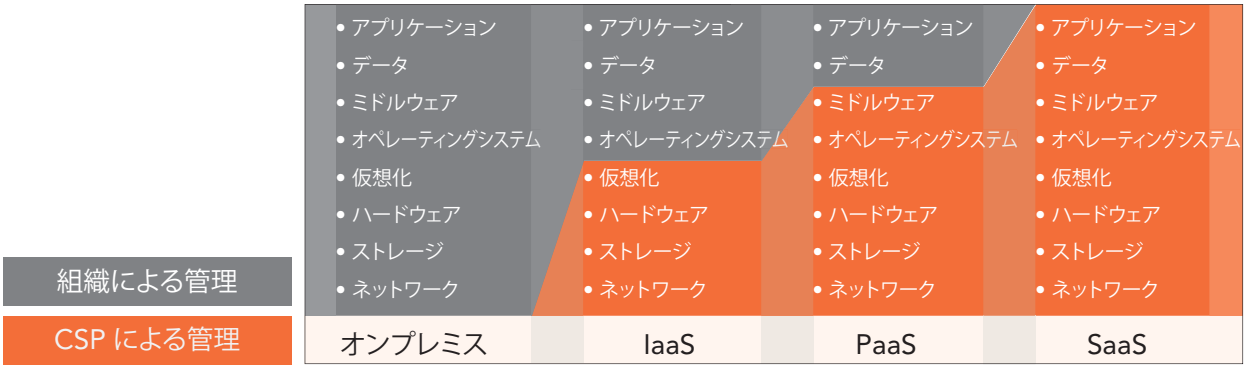
モバイル端末の普及

クラウド サービス モデル

クラウドコンピューティングプロバイダーは、様々なサービスモデルを利用します。実際のクラウド ソリューションは、複数のアプローチの組み合わせとなる場合があります。NIST が定義している最も一般的な 3 つのサービスモデルの詳細は以下のとおりです。

Software as a Service（SaaS）：	顧客は、クラウド インフラストラクチャ上で稼働しているプロバイダーのアプリケーションを利用できます。これらのアプリケーションは、ウェブブラウザのようなシンクライアントのインターフェイス（例：ウェブメール）またはプログラムインターフェイスにより、様々なクライアントデバイスからアクセスすることが可能です。顧客は、ネットワーク、サーバー、オペレーティングシステム、ストレージ、個別のアプリケーションなどの基盤となるインフラストラクチャを管理しませんが、ユーザー固有のアプリケーション構成の設定という限定的な範囲では例外となる場合があります。
Platform as a Service（PaaS）：	顧客は、クラウドインフラストラクチャ上でプロバイダーがサポートするプログラミング言語、ライブラリ、サービスおよびツールを利用して、顧客が作成または取得したアプリケーションを展開できます。顧客は、ここでも基盤となるクラウド インフラストラクチャを管理しませんが、展開したアプリケーションおよび場合によってはそのアプリケーションのホスト環境の構成について管理します。
Infrastructure as a Service（IaaS）：	顧客は、プロセシング、ストレージ、ネットワークなどの基本的なコンピューティングリソースをプロビジョニングできます。顧客は、オペレーティングシステムおよびアプリケーションを含む任意のソフトウェアを展開し、稼働させることができます。顧客は、基盤となるクラウド インフラストラクチャについては管理しませんが、オペレーティング システム、ストレージおよび展開したアプリケーションを管理するほか、選択したネットワークコンポーネント（ホストのファイアウォールなど）を限定的に管理する場合もあります。

従来の IT アーキテクチャは、8 つのキーコンポーネントを含むものとして説明されることがあります。次の表は、3 つのクラウド サービス モデルにおいて、組織と CSP 間で各コンポーネントに対する責任がどのようにシフトされているかを示しています。



クラウド展開モデル

クラウド技術は、様々な展開モデルによって提供が可能です。NIST が定義する最も一般的な展開モデルは以下のとおりです。

プライベートクラウド	クラウド インフラストラクチャは、複数の内部顧客（事業部など）からなる一つの組織（顧客）の独占的利用のために提供され、顧客、第三者、またはこれらの組み合わせによって所有、管理、運用され、組織の施設内又は施設外の両者で存在することがあります。
コミュニティクラウド	クラウド インフラストラクチャは、共通の関心事（ミッション、セキュリティ要件、ポリシー、コンプライアンス上の考慮事項など）を共有する組織からなる特定コミュニティの顧客による独占的利用のために提供され、コミュニティ内の 1 つまたは複数の組織、第三者、またはこれらの組み合わせによって所有、管理、運用され、施設内又は施設外で存在することがあります。
パブリッククラウド	クラウド インフラストラクチャは、公衆により利用されるために提供され、企業、学術機関、政府組織、またはこれらの組み合わせによって所有、管理、運用され、クラウドプロバイダーの施設内に存在します。
ハイブリッドクラウド	クラウド インフラストラクチャは、それぞれ独自の存在を保っている 2 つ以上の異なるクラウド インフラストラクチャ（プライベートクラウド、コミュニティクラウドまたはパブリッククラウド）から構成されるものの、データやアプリケーションの可搬性を実現する、標準または独自の技術で結び付けられたもの（クラウド間のロードバランシングのためのクラウド バーストなど）をいいます。

パーソナルクラウドとして知られ急成長を遂げている一般向けのパブリッククラウドは、個人の顧客にサービスを提供するものです。パーソナルクラウドサービスにはソーシャルメディア、個人用電子メール、文書の作成と編集、音楽、写真、動画、ファイルの保存など多く分野のサービスが含まれています。

ソフトウェア資産管理入門

The Information Technology Infrastructure Library（ITIL）は、ソフトウェア資産管理を以下のように定義しています[2]。

> **ソフトウェアのライフサイクルの全段階を通じた組織内ソフトウェア資産の効果的な管理、統制、保護に必要なすべてのインフラストラクチャおよびプロセス**

上記の標準的な定義に加え、機能上の定義として、詳細を次のように説明しています。

> **SAM は組織がソフトウェアで行うこと、行わないことを効果的に管理することです。SAM はソフトウェアの 5 段階のライフサイクル（計画、要件定義、導入、保守、廃棄）を通じて、ソフトウェア資産を管理するための一連の管理プロセスおよび機能**

ソフトウェアライセンス管理（SLM）は、SAM をライセンスに適用したものです（保有ライセンスおよび使用ライセンスの測定および管理）。

ソフトウェア ライセンス コンプライアンス（SLC）は、SAM および SLM の一部であり、ソフトウェアのライセンス付与と利用について規定する契約条件の遵守を確実にするものです。ソフトウェア ライセンス コンプライアンスは、SAM の重要な目的です。当該ソフトウェアライセンス契約を確実に遵守するため、組織は定期的に割当済みライセンスと保有ライセンスの調整を行わなければなりません。割当済みライセンスの情報は、ライセンス メトリクス（製品によって異なります）の計数、ライセンス規則の適用、製品利用権、その他の情報（製品バンドルに関する規則など）を含む、完全かつ正確なソフトウェア展開情報を分析することによって得られるものです。保有ライセンス情報は、完全かつ正確な購買履歴、ソフトウェアライセンス契約、および製品名の変更や関連するライセンス規則といった情報を分析することによって得られるものです。

前述のとおり、SAM には以下の特徴があります。

- SAM は、人、プロセス、テクノロジーに関わるビジネス・プラクティスです。
- SAM は、一連の管理プロセスおよび機能を意味するものです。ツールは、これらのプロセスおよび機能を促進するものであり、自動化することも可能ですが、ツールを導入することによってのみでは、効果的なソフトウェア資産管理を保証するものではありません。
- SAM は、組織が管理ポリシーを設定する必要があると考えるソフトウェアすべてに関わるものです。つまり、デスクトップ上のソフトウェアだけに限定されるものではありません。実際に SAM は、ソフトウェア資産の費用およびその運用の影響が最も集中するサーバー上のソフトウェアに関わるものであるということが最も重要です。さらに興味深いことに、クラウドもまたサーバー上のソフトウェアに関するものだということです。電話、ストレージアレイ、スイッチ、プリンター、ストレージメディア、その他のデバイス上のソフトウェアにも、SAM は対処します。
- SAM は、部門横断的なプラクティスであるため、単独の部署内だけで機能させても効果的ではありません。IT、財務、購買、法務、人事その他の複数の部署間における連携が必要になります。

効果的な SAM により、保有するソフトウェア資産および展開するソフトウェア資産を把握し、何処でどのようにそれらの資産が利用されているのかを、合理的な完全性と正確性をもって、一貫して、繰り返し把握することが可能になります。これは、SLM、SLC、情報セキュリティ、事業継続性、変更および構成管理、ライセンス コンプライアンスなどの様々な目的に役立ちます。

情報セキュリティが有効であるためには、組織全体にわたるすべてのハードウェアおよびソフトウェア資産を識別できる必要があります。その結果、これらの資産が許諾を受けて展開され、正規のものであり（つまり、改ざんされていない）、セキュリティの脆弱性から保護するために、ソフトウェア発行者による最新のセキュリティ パッチで構成されていることを確実なものとすることができます。効果的な**事業継続性**を実現するには、どの資産がどのビジネスプロセスをサポートするのかを理解するとともに、複数の資産の相互依存性を識別する必要があります。また、あらゆるサーバーにつき、すべてのソフトウェア コンポーネントに関して必要なバージョンやパッチのレベルまで、再構築が可能な状況である必要があります。効果的な**変更および構成の管理**のためには、マシンの構成に不正な変更が一切加えられていないことを確認しておく必要があり、そのためには、組織が所有するマシンと、その場所および構成を知っておく必要があります。

SAM 標準規格

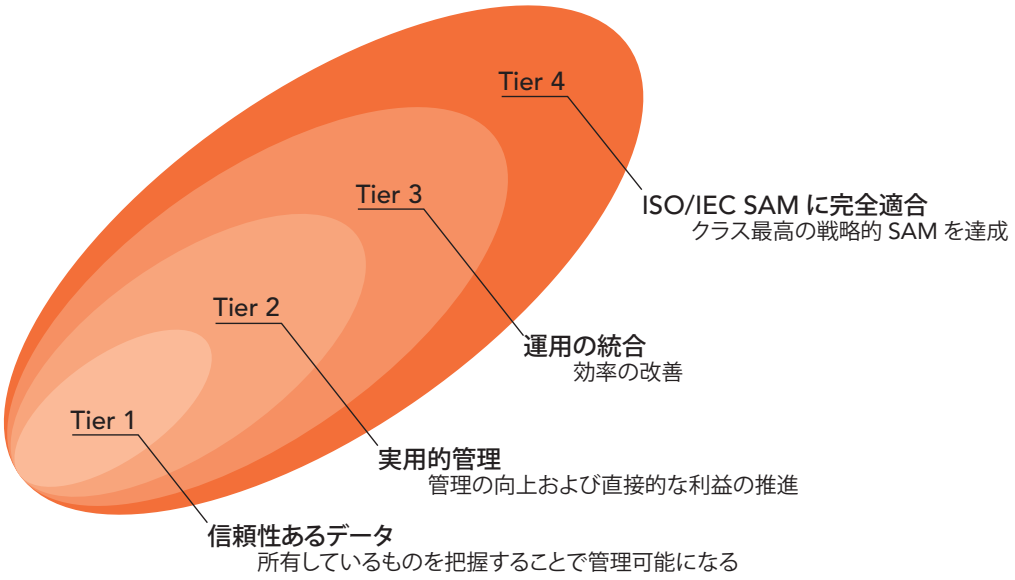
国際標準化機構（ISO）は、最大かつ最も一般に認知されている世界的な標準化機構です。SAM 標準の ISO 19770[3] シリーズは、SAM の唯一の世界標準です。

19770-1 SAM プロセス

2006 年に初めて発行され 2012 年に改定されたこの規格は、SAM プロセスと適合性の段階的な評価に焦点を当てています。本規格は、SAM の導入を 4 段階に分けており、どれも効果を中心に据えています。

BSA の SAM Advantage コース[4] は、ISO/IEC 19770-1:2012 標準に対応した初めての業界策定の SAM コースです。

ISO 19770-1 段階的評価の枠組み



ISO/IEC 19770-1 は、SAM における一連の統合プロセスおよびそのインプリメンテーションに焦点を当てた段階的アプローチを特定します。特定された 27 のプロセスは、3 つの主要カテゴリと 6 つのサブグループに分類されます。4 段階のインプリメンテーション アプローチは、そのプロセスに起因する適合性の達成度に基づいています。

ISO/IEC 19770-1 は、すべてのソフトウェアおよびすべての技術的アーキテクチャに適用されます。この規格はノートパソコンにインストールされている職場の生産性を上げるアプリケーションにも、クラウドコンピューティング環境での SaaS として提供されるアプリケーションにも関連するものです。

ISO 19770-1 SAM プロセスの枠組み

SAM の組織管理プロセス

4.2 SAM の制御環境

SAM のコーポレート ガバナンス プロセス 4.2.2	SAM の役割および責任 4.2.3	SAM のポリシー、プロセスおよび手順 4.2.4	SAM の能力 4.2.5

4.3 SAM のプランニングおよびインプリメンテーション プロセス

SAM のプランニング 4.3.2	SAM のインプリメンテーション 4.3.3	SAM のモニタリングおよびレビュー 4.3.4	SAM の継続的改善 4.3.5

SAM のコア・プロセス

4.4 SAM のインベントリ・プロセス

ソフトウェア資産の識別 4.4.2	ソフトウェア資産のインベントリ管理 4.4.3	ソフトウェア資産の管理 4.4.4

4.5 SAM の検証およびコンプライアンス プロセス

ソフトウェア資産記録の検証 4.5.2	ソフトウェア ライセンス コンプライアンス 4.5.3	ソフトウェア資産セキュリティ コンプライアンス 4.5.4	SAM の適合性検証 4.5.5

4.6 SAM の運用管理プロセスおよびインターフェイス

SAM の関係および契約管理 4.6.2	SAM の財務管理 4.6.3	SAM のサービス レベル管理 4.6.4	SAM のセキュリティ管理 4.6.5

SAM の主要なプロセス インターフェイス

4.7 SAM のライフサイクル・プロセス・インターフェイス

変更管理プロセス 4.7.2	ソフトウェア開発プロセス 4.7.4	ソフトウェア デプロイ プロセス 4.7.6	問題管理プロセス 4.7.8
取得プロセス 4.7.3	ソフトウェア リリース管理プロセス 4.7.5	インシデント管理プロセス 4.7.7	廃棄プロセス 4.7.9

19770-2 ソフトウェア識別タグ

ISO/IEC 19770-2 は、ソフトウェア識別タグ（SWID）に焦点を当て 2009 年に発行されました。その主な目的は、インストールされたソフトウェアを完全かつ正確に識別する枠組みを確立することです。これは、ソフトウェア発行者およびエンドユーザー組織の双方に利益をもたらします。

19770-2 は、SWID タグ内の必須の要素とオプション要素の両方を定義しています。SWID タグは、対応するソフトウェアがインストールされると、デバイス上のあらかじめ決められた場所に保存された標準 XML を利用します。

TagVault[5]（tagvault.org）は、中央タグ リポジトリをホストすることで、19770-2 のインプリメンテーションを促進するために設立された非営利組織です。

多くのソフトウェア発行者が標準規格を取り入れ、今では新しいソフトウェアに SWID タグを付けて出荷しています。まだ SWID に対応していないソフトウェア発行者については、レガシー ソフトウェア製品と同様、組織が独自に作成した SWID タグ、あるいは第三者の SWID タグを利用することもできます。

SWID タグを利用することで、組織はその環境内で展開されているソフトウェアを迅速かつより正確に識別できるようになります。IaaS/PaaS 環境では、独自に作成した SWID の利用により、組織は CSP から提供されたソフトウェアまたは他の顧客のソフトウェアと、自社のソフトウェアを区別することができます。したがって、すべての環境において益々 SAM の一部となりつつある SWID タグは、クラウド環境での SAM を促進する上で、大変重要なものとなる可能性があります。

将来の ISO SAM 標準規格：ISO は現在、ソフトウェア ライセンス権利タグに焦点を当てた 19770-3 並びに 19770-2 および 19770-3 のタグ管理に対処する 19770-7 など、将来的な標準規格に取り組んでいます。

クラウドにおける SAM の一般的な検討事項

クラウド サービス モデルは、ソフトウェア ライセンスに関連しているため、各クラウド サービスはそれぞれのリスクがあり、後述する項目で議論されている事項を検討する必要があります。本項では高いレベルから、すべてのクラウドサービスおよび展開モデルに共通する SAM に関する一般的な検討事項について詳しく説明します。

クラウドに SAM を適合させる

クラウドコンピューティングは、組織が SAM を行う必要性をなくすものではありません。クラウド環境は、単に SAM のプロセスが効果的に実施されるインフラストラクチャが異なるというだけのことです。組織は、クラウド環境内でのソフトウェアおよびアーキテクチャの微細な違いを考慮に入れて、組織に合うように ISO 19770-1 で定義されている 27 のプロセスに調整をして実施する必要があります。組織は、従来の物理的環境と仮想環境の違いに対処するため、アプローチを変更しなければならないのと同様に、クラウド環境に対処するためにアプローチを適応させなければなりません。

組織は、19770-1 の条件を満たすための組織のポリシーおよび手順において、クラウドコンピューティングを具体的に対応させる必要があります。クラウドに SAM をインプリメンテーションする際に対処すべき主な留意事項は以下のとおりです。

- **ソフトウェア資産の性質を変更する：**（クラウド以前の）従来の SAM は、基礎となるソフトウェア資産のライフサイクル管理のみに焦点を当てています。クラウドにより、SAM プログラムは、ソフトウェア資産管理に追加する、またはそれにとって代わるものとして、クラウドサービスを管理する必要があります。つまり、クラウドサービス自体が管理を必要とする資産になっています。SAM の一部が現在 CSP 経由で提供されていて、顧客が保有していないことから、SAM プログラムは CSP がサービス品質保証契約（SLA）およびその他の適用要件に準拠しているかどうかをモニタリングする必要があります。このようなモニタリングを効果的に行う能力とは、SAM プログラムにおいて開発する必要のある新たな考え方、新たなスキル セットおよび新たなツールセットからなるものです。

- **リアルタイム SAM：**クラウドのビジネス上の利点の 1 つは、俊敏性と市場化までの期間を短縮できることです。クラウドサービスは、マウスを数回クリックするだけでプロビジョニングおよびリリースが可能です。（クラウド以前の）従来の多くの SAM プロセスでは、長期ライフサイクルを前提とした計画、契約、定期的な確認と調整、その他の SAM の統制活動により多くの時間を当てるものとされています。クラウドでの SAM プログラムは、より迅速な対応が可能となるようプロセスを設計し、組織全体でのクラウドの契約、インプリメンテーション、管理に関する詳細なポリシーおよびプロセスをさらに重視することによって、よりリアルタイムの環境に適応しなければなりません。

- **分散化：**クラウドサービス、特に SaaS は一般的に実装が容易で、IT に関する知識やリソースを多くは必要としない場合もあります。したがって、多くの組織は、従業員がクラウドサービスの展開にあたり、通常の IT 調達プロセスに則っていないことに気づきます。SaaS プロバイダーは、従来の IT 購買担当を通すのではなく、直接ビジネス部門の購買者（営業または人事部など）に営業を行う可能性があります。クラウドサービスは通常、運用コストとして考えられるため、設備投資の際の厳格な承認プロセスが行われません。事実、クラウドサービスについては、法人クレジットカードを利用して支払われ、通常の調達／財務承認という手続きが行われないことがよくあります。これらの事実から、IT および SAM 部門は、クラウドのインプリメンテーションについて、事後になって初めて知ることになり（もしくは全く知らずに）、契約段階に関わらない場合もあります。これらの結果、以下の問題が起こる可能性があります。

  - **契約手続の脆弱さ：**SAM、IT および調達担当部門が契約段階に十分に関わらない可能性があります。
  - **増加するライセンス コンプライアンス リスク：**SAM 担当部門がライセンス リスクの観点で、クラウド ソリューションの設計、契約、モニタリングに関わらない可能性があります。
  - **組織がデータ保存場所の統制喪失：**組織が管理できないことにより、プライバシー、情報セキュリティ、および事業継続性のリスクをもたらす可能性があります。
  - **運用面に依存し組織としての統制を喪失：**特に組織が事業運営のために不正なクラウド ソリューションに依存するようになると、問題が深刻化する可能性があります。
  - **クラウドへの支出や最終的なコストの上限に関する知識の欠如：**ユーザーの行為によって、組織がクラウドサービスに関し金銭的な責任を負う場合もあります。例えば、ユーザーが追加機能を有効化または利用したり、基準として設定されたデータストレージ制限を超えたりする場合などです。これは、部署またはユーザーが有効化したクラウドサービスに対する IT 統制の欠如によって発生する課題であり、そもそも不正な行為です。
  - **財務上の可視性の低減：**部署または従業員個人が直接クラウドサービスを調達できることから、費用の一部が不正確に分類される可能性があり、組織は IT およびクラウドの支出全体に対して財務上の可視性を失う可能性があります。

- **クラウドの総所有コスト（TCO）の把握：**SAM プログラムの一面として、ライフサイクルの全段階に通じた SAM に関連する総費用および予算を把握することが重要です。SAM プログラムでは、従来のソフトウェアライセンス契約関連の費用を把握し、予算に組み込まなければなりません。しかし、クラウドは従来のソフトウェアとは異なるタイプの契約による異なる環境であるため、SAM プログラムのための新たなスキルセットや機能の開発が必要となります。クラウド契約は単純に見えますが、計上および把握しなければならない複数の直接費用、間接費用、隠れた費用が含まれる場合があります。これらの費用には、クラウドへの移行費用、他の IT システムとの統合、クラウドサービスのオーバーサブスクリプション、プレミアム サポートサービスの必要性、追加ストレージ条件、データ抽出費用、サービス範囲変更の費用、および増加するサービス更新費用などが含まれます。従来付与されたライセンスの範囲には必ずしも含まれないクラウドの高度に仮想化された性質によって、追加費用が発生する場合があります。

Bring Your Own Device（BYOD）

クラウドモデルの主な長所の 1 つに、インターネットを通じた利用があげられます。この特徴は、IT におけるもう 1 つのトレンドである BYOD とともにあります。BYOD は、従業員が個人所有のデバイス（ノートパソコン、タブレット、スマートフォン）を利用して、組織の情報およびアプリケーションにアクセスすることを、組織が許可することです。クラウドは通常どこからでもアクセスできるため、BYOD に最適です。多くの SaaS プロバイダーは、BYOD 型デバイス向けに特別に設計したアプリケーションを提供し、ユーザーがそのサービスを十分に活用できるようにしています。SAM の観点から見ると、BYOD はクラウドに関連して、新たなリスクをもたらします。

- **モバイルデバイスからアクセスするためのライセンス：**組織は、すべてのデバイスからクラウド ソフトウェアにアクセスするために適切なライセンスを取得する必要があります。ソフトウェア ライセンスの契約条件によっては、BYOD アクセスが禁止されている、あるいは追加ライセンス料金が発生する場合があります。

- **セキュリティの問題：**組織が BYOD のセキュリティ設定または BYOD とクラウド間の接続（個人の携帯電話／Wi-Fi 経由で可能）のセキュリティ設定を制御しないため、さらなる情報セキュリティ リスクが発生する可能性があります。

- **ビジネス利用における BYOD 経由でのパーソナル クラウドとパーソナル アプリの利用：**BYOD の本質は、パーソナルクラウドサービスに基づく個人アプリ（メモ帳や to-do リスト管理などの生産性向上のためのアプリ）へ簡単にアクセスできるということです。これらの個人アプリが、組織のアプリやデータへのアクセスに利用されるのと同じデバイス上で利用が可能であることから、ユーザーが個人アプリをビジネス目的にも利用する可能性は非常に高いと言えます。しかし、これらの個人アプリのライセンス条件は、ビジネス／商用目的での利用を禁じている場合があり、従業員および組織の双方をさらなるライセンスリスクにさらすことになります。そのため、組織の情報が、組織が知らないまたは管理の届かないパーソナルクラウド上に存在する可能性があり、さらなる情報セキュリティやプライバシーのリスクにつながる可能性があります。

- **BYOD に伴う偽造および海賊版ソフトウェアのリスク：**組織は、従業員がどのソフトウェアを個人のデバイスにダウンロードし、インストールしているのか、そのソフトウェアの出所がどこで、従業員が適切なライセンス契約に基づきインストールし、利用しているか、ほとんど管理できません。これらの管理されていないソフトウェアが正規のものではないため、デバイスおよびこのデバイスを通じてアクセスされる組織のデータ全体をリスクにさらす可能性があり、組織に対して多様なリスクをもたらします（当該ソフトウェアそのものが組織データへのアクセスに利用されない場合であっても、同じデバイス上でインストールまたは実行されているソフトウェアによりリスクが発生する可能性があります）。また、従業員が実際に海賊版ソフトウェアをビジネス目的で利用している場合、組織をライセンス コンプライアンスおよび情報セキュリティのリスクにさらすことになる可能性があります。

規制およびデータセキュリティに関するコンプライアンスの促進

多くの組織では、データプライバシーおよび情報セキュリティに関連して、規制およびその他のビジネス上の要求事項があります。データを確実に保護することは、すべての組織にとって共通の優先事項です。その中には、データを保護するだけでなく、データが実際に保護されていることを示す証明書またはその他の保証書を提供するという規制およびビジネス要求を有する組織もあります。

このようなビジネスコンプライアンスの 1 つに PCI DSS があります。PCI DSS は、主要なクレジットカード、デビットカード、プリペイドカード、ATM カードなどのカード所有者情報を扱う組織向けの独自情報セキュリティ基準です。PCI DSS 認定を取得し維持するために、組織は毎年検証を行う必要があり、毎年この検証を完了するには、組織はインフラストラクチャ（ハードウェア、ソフトウェア、ネットワーキング、ファイアウォールなど）の詳細について把握していなければなりません。大容量データを処理する組織は、コンプライアンスを検証するために現地を訪問する必要があります。クラウド環境のインプリメンテーションが適切に計画されていない場合、規制遵守を維持できるかについて説明を求められる可能性が高くなります。

次に示す法規制は、組織がデータの所在、アクセス、セキュリティなどについて従うべき多くの要件を規定しています。

- 米国関連：
  - Sarbanes-Oxley（SOX：サーベンス オクスリー法）
  - Health Insurance Portability and Accountability Act（HIPAA：医療保険の携行性と責任に関する法律）
  - Electronic Records and Electronic Submissions CFR 21 part 11（電子記録および電子申請 CFR 21 part 11）
  - Financial Modernization Act of 1999（1999 年金融サービス近代化法）
  - Federal Desktop Core Configuration（FDCC：連邦政府共通デスクトップ基準）
  - USA PATRIOT Act and US Presidential Executive Order 13103（米国愛国者法および米国大統領令 13103）
- 米国以外関連：
  - 欧州連合 — EU 加盟国における Data Protection Directive（データ保護指令）およびその他の特定の法律
  - オーストラリア — Corporate Law Economic Reform Program Act 2004（CLERP9、2004 年会社法経済改革プログラム法）
  - マレーシア — Personal Data Protection Act 2010（2010 年パーソナルデータ保護法）
  - インド — The Institutes of Technology（Amendment）Act（工科大学（改正）法）および Clause 49 of the Listing Agreement to the Indian Stock Exchange（インド証券取引所への上場契約 49 節）
  - 南アフリカ — コーポレートガバナンスに関するキング委員会の報告

データプライバシーはクラウドに伴って大きな懸念が持たれている分野です。具体的には、欧州連合の Data Protection Directive（データ保護指令）が、プライバシー保護に関して欧州連合（EU）が「適切」とする基準を満たしていない非 EU 加盟国との個人データの転送を禁止しています。米国はプライバシーに関して異なるアプローチをとっているため、これらの違いを埋め、米国内の組織が EU の指令を遵守するための合理化された手段を提供する仕組みが導入されています。そして、米国商務省は、欧州委員会と協議の上、「セーフハーバー」というフレームワークをつくりました。一連のプライバシー原則に基づく基準を満たしている場合、組織はセーフハーバープログラムに加入することができます。これらの原則には、パーソナルデータの収集に関する通知、対象データの利用方法についての選択、収集されたデータを保護するためのセキュリティと予防措置が含まれています。しかし、セーフハーバーは合法的なデータ転送を保証するためのひとつのオプションに過ぎないという点に留意する必要があります。したがって組織は、クラウド上での個人情報のガバナンスやデータの適法性を確実にするために、その他のオプションを検討する必要がある場合もあります。

クラウドアーキテクチャによってもたらされた複雑さは、組織が SAM プログラムをどのように管理する必要があるかという点に、根本から影響するものです。クラウドサービスの形態に関わらず、SAM プログラムは、規制およびデータセキュリティに関するコンプライアンスを管理している組織（グループ）と、自身のチームの延長のように、連携しなければなりません。SAM を軽視したり、クラウドに関する SAM の権限を縮小することは、さらなるリスクとコストが発生することにもなりかねず、クラウドに移行することによって得られた他の利益を台無しにしてしまう可能性をはらんでいます。

クラウドイネーブラーとしての SAM

SAM プログラムの長所としてしばしば見過ごされるのが、組織の将来的な戦略形成を支援することです。組織内のハードウェア、ソフトウェア、インフラストラクチャに関する詳細な知識は、成長、買収、その他重要な戦略的決定において、確かな情報に基づいた強力なものとなります。

クラウドコンピューティングは、SAM が重要な見識を提供することができる戦略のひとつです。組織の現在の環境（ハードウェアおよびソフトウェア）を把握することは、クラウドコンピューティングがビジネスとして意味を成すかどうかを決定づけるための重要事項です。

組織は、知らないものを最適化することはできません。目的がオンプレミスの仮想化であれ、プライベートクラウドへの移行であれ、またはパブリッククラウド（IaaS、PaaS または SaaS）への移行であれ、組織は所有するハードウェアおよびソフトウェア資産、その所在、設定、ユーザーを把握し、それらがどのように利用され、どのようなライセンスを有するのか（それらのライセンスがクラウド環境への費用効率の良い移行をサポートするかを含む）、それらの資産に関連した総費用について把握する必要があります。完璧で正確な資産情報を有することによってのみ、組織は仮想化またはクラウドコンピューティングを利益に変えるために必要な真の投資回収率を把握することができます。したがって、SAM はクラウドへの移行を可能にする中核となるものなのです。

Software as a Service（SaaS）に関する SAM の検討事項

Software as a Service（SaaS）は、ウェブブラウザ経由で最も一般的にアクセスされるサブスクリプションサービスです。主な SaaS には Salesforce.com、Microsoft Office 365、Google Apps、NetSuite 等があります。

SaaS は、通常次の 4 つのビジネスモデルの 1 つ、またはそのいずれかの組み合わせによって提供されます。

- **期間に応じたサブスクリプション：**最も一般的なモデルであり、ユーザーは一定期間（通常 1 年）、システムへアクセスするためのユーザー 1 人当たりの料金を支払います。料金は、ユーザーがアクセスできるサービスまたはモジュールによって異なる場合があります。
- **実際の利用量：**今日ではあまり見られないモデルであり、料金はシステムへのログイン回数、利用時間、データ保存量、処理数、または、それらのバリエーションの測定結果に基づき計算されます。
- **業績：**今日ではあまり見られないモデルであり、SaaS プロバイダーがサービスの利用（処理された各取引からの一定割合の収益など）によって得られた実際の結果、または顧客の業績全般（収益など）をもとに請求します。
- **広告支援：**顧客が料金を支払うのでなく、CSP がユーザーに表示される広告収入に基づきサービスを提供しています。本モデルは、パーソナルクラウドでより一般的です。

一般的な誤解として、SaaS はライセンスリスクがないため、SAM の範疇から除外できるというものです。SaaS に関連するライセンスリスクは、SaaS の CSP および契約の仕様によって異なります。以下は、一般的なリスクの一部です。

- **知的財産侵害：**SaaS プロバイダーは、故意であるか否かに関わらず、第三者の知的財産を侵害している場合があります。CSP があらゆる知的財産侵害に対して顧客を保護し、免責し、補償することを契約上要求されない限り、その利用者が当該侵害の最終受益者として、法的リスクにさらされる可能性があります。CSP は、利用者とは異なる国で運営する場合もあるため、CSP は知的財産侵害に関して保護が弱い法律の対象となる可能性があります。さらに、このような侵害が発生した場合、現行の機能または料金のままでサービスを提供する CSP の能力に関して、リスクとなる可能性があります。これは、サービスに依存する利用者にとっては、さらなる運用リスクを意味しています。

- **クライアント側のソフトウェア コンポーネント：**一般的な認識と異なり、SaaS ソリューションでは、クライアント側でのコードのインストールを要求する場合があります。これは、ブラウザ プラグイン、アプレット、エージェント、クライアント ソフトウェア、または本格的なソフトウェアスイート（Microsoft Office 365 サブスクリプションの場合はMS Office Professional スイート）といった形式で提供されます。利用者は、(a) このようなクライアント側ソフトウェアの利用に適切なライセンスを得ている、監査またはライセンス確認の際にライセンスの十分な証明書を保有する、(b) これらのソフトウェア資産を他のソフトウェア資産と同様に管理し、これらの資産を計上でき、範囲外の展開はせず、該当製品の利用権および制限に従って利用する必要があります。

  例：ある組織が SaaS サービスのクライアント側コンポーネントを標準 PC 画像の一部として含めていた。当該組織は、大幅に範囲を超えて展開をしていたため、許諾済ユーザー数および SaaS 契約条件について違反していた。

- **不正利用：**SaaS は通常、利用上の制限を伴います。多くの場合、この制限は SaaS の契約の性質上、交渉できるものではありません。利用者は、契約上のすべての条件および制限を確実に遵守するために、適切な管理体制を整備する必要があります。このような条件には、次のようなものがあります（これらに限定されるものではありません）。

  - 地理上の制限：例えば、契約では米国を拠点とする従業員のみ、サービスへのアクセスを許可する場合があります（SaaS プロバイダーが、米国以外のユーザーに対して、もしくはその他の理由によって、異なる料金を請求するサービスの場合）

  - 複数の従業員間でユーザーアカウントを共有することに対する制限

    例：ある部署のマネージャーが、あるソフトウェアトレーニングサイトの個人ユーザーアクセス ログイン情報を、自身のチーム 10 名に提供することで、チームメンバー全員がトレーニングを受講することができる。

  - システム アカウントで当該サービスにアクセスを制限する（ここでの「ユーザー」は他のシステムであり、個人エンドユーザーではない）。

  - 非従業員の利用者（請負業者、外部プロバイダー、ベンダー、ビジネスパートナー、顧客）または利用者の関係会社へのユーザーアクセス提供を制限する。このような制限は、利用者による SaaS ソリューションの利用を完全に阻み得ます。

  - サブスクリプション料金を支払わず、ライセンスを持たない個人に対する SaaS で生成されたレポートや情報提供に関する制限をする。例えば、1 つのユーザー アカウントを持ち、SaaS からのレポートをチーム全体にメールで送信することは制限されます。

SaaS プロバイダーには、不正利用を検知するアナリティクスを実装しているものもあります。これらのアナリティクスには、次の検査が含まれます。

- 同一ユーザー・同一アカウントの同時接続
- 接続元が示されている接続中の IP アドレス
- ユーザーアカウントがアクセスされた時間
- ユーザーアカウントの処理／データ量
- 公的に入手可能な情報と、利用組織のプロファイルとの比較（利用組織の総従業員数など）
- 異常な利用パターンを検知するために、利用組織プロファイルと、同業他社の顧客との比較

- **シェルフウェア：**一般的な誤解に反して、シェルフウェア（支払はされているが未利用のソフトウェア）は、SaaSでさえも発生する可能性があります。これは、主として現在の全 SaaS モデルでは利用に応じて支払うのではなく、一定期間の先払い契約（一定数のユーザーに 12 カ月間など）が求められるためです。したがって、ほとんどのSaaS 導入の費用は、通常、実際の利用とは合致しません。エンドユーザーの組織は、必要以上の支払いをしていることに気づくかもしれません。これは多くの場合、新たに SaaS を導入する際（支払いはすぐに発生するが、ユーザーがそのサービスへ移行するのに数ヶ月かかる場合がある）、または支払われたサブスクリプションを実際に利用しているユーザーが僅かしかいない場合、もしくはSaaS プロバイダーへの支払いは最初の契約に従って継続が必要な一方、利用組織の従業員数とその構成に大幅な削減が生じた結果として発生します。

- **規模の経済：**ハードウェア メトリックに基づくモデルなど、従来のエンタープライズソフトウェア ライセンスモデルでは、規模の経済概念を有し、エンドユーザーは、ソフトウェアの費用を追加せずに、その需要を増大させることができるものがあります。組織はソフトウェアモデルをユーザーベースの SaaS モデルに移行する際、この利点を失う場合があります。これにより、ソフトウェア費用に影響する複数のコンピューティング技術を活用する組織の能力が制限される可能性があります。例えば、組織はソフトウェアの需要の増加に対し、もはやソフトウェアのライセンスモデルに合った方法でハードウェアをアップグレード（プロセッサ スピード、メモリ、ネットワークスピード）することでは対処することは不可能です。その代わりに、追加された各ソフトウェアユーザーは、一定の契約期間、直接のコスト増となり、これが組織にとって実際に必要な利用期間と一致する場合もしない場合もあります。

- **SaaS の外注：**SaaS 契約にさらなる複雑さを加えているのは、多くの SaaS プロバイダーがサービスの提供において他のプロバイダー（例：IaaS/PaaS）を利用している点にあります。例えば、ウェブの SaaS サービスは、Amazon のクラウドベースインフラストラクチャ経由でサービスを運営している場合があります。前述した問題の一部は、これらのプロバイダーに関連し、プロバイダーによって異なります。組織は、SaaS のエコシステム全体について、どのような保証を受けているのかを把握する必要があります。

SAM と仮想化／プライベートクラウド

非 SaaS 型クラウドの技術および展開は、主に仮想化技術によって実現されます。

仮想化には、ハードウェアまたはストレージといった IT リソースの仮想バージョン（物理的バージョンではない）の展開を伴います。メインフレーム コンピュータと伴に始まった仮想化は、技術としては、数十年利用されてきました。近年では仮想化は充分に浸透した IT テクノロジーとなっています。本編では仮想化技術の詳細に触れませんが、クラウドにおける SAM 管理上の課題を理解するためには、仮想化の基本的な概念を理解する必要があります。

仮想化は、ソフトウェアとハードウェア間の分離の程度に関係します。仮想化されていない従来の IT では、ハードウェアとソフトウェアの 1 対 1 の関係を持っていました。つまり、1 つのオペレーティングシステム（OS）（または、ソフトウェア製品の 1 インスタンス）が、1 台のハードウェアに紐付けられていました。ソフトウェア業界において今日最も一般的なライセンス メトリックは、未だにハードウェア測定に紐付けられたものです（プロセッサ／コア毎のライセンスなど）。なぜなら、ハードウェアは、今も昔も変わらず、最も簡単かつ客観的に測定ができる要素だからです。

その反対となる仮想化は、ハードウェアとソフトウェアの関係は 1 対多の関係になり、各々が独自のオペレーティングシステムおよびアプリケーションを持つ複数の仮想化マシンを、一台のハードウェアで構成することができます。ハードウェアリソース（CPU またはメモリなど）は多くの場合、仮想化マシンがピーク利用量に対応できるように、様々なオペレーティングシステム間で動的に割り当てられます。

現在有効なライセンス契約の多くは、これらが書かれた当時は仮想化が想定されていなかったため、仮想化は、ハードウェアメトリックに基づくソフトウェアライセンスにとって根本的な問題となっています。各々のソフトウェア発行者が、仮想化環境において、ハードウェアメトリックの測定に関して、それぞれの異なったポリシーを採用しています。仮想化環境におけるリソース割り当ての動的な性質により、多くの発行者は利用者が考え得る最大限のハードウェア構成（実際の基盤になるハードウェアのすべての CPU など）に対してライセンスを持つべきだと主張しています。ソフトウェア発行者には、利用する仮想化技術（またはクラウドサービス）が自身のものか、第三者のものかによって、または承認された追跡ツールが実装されているかによって異なるポリシーを採用しているところもあります。利用者は、ソフトウェアライセンス契約を再確認し、その契約に適用される特定の規則について把握するために、ソフトウェア発行者に確認する必要があります。

ハードウェアとソフトウェアの間で複数の関係を可能にする新たな仮想化管理技術の開発は、SAM の課題をさらに複雑なものにする可能性があります。あるシナリオでは、一方にある複数のハードウェア、およびもう一方にある複数の仮想マシン（オペレーティングシステム）の間で仮想レイヤーがバッファとなり、特定の仮想マシンを特定のハードウェアに紐付けることができなくなります。

仮想化は、IT コストや二酸化炭素排出量（消費電力）の削減、事業継続性の向上および俊敏性と市場化までの時間短縮など、利用者に多くの利益をもたらします。しかし、ライセンス関連事項だけをとっても、適切に検討、計画されなければ、コスト面から仮想化が非現実的なものとなる可能性があります。

仮想化は、主に検出と管理によって、SAM に特有の課題を提示します。仮想マシンはマウスを数回クリックするだけで作成または削除することができ、その構成は頻繁かつ自動的に変更されます。仮想マシンが、SAM 部門の関与もなく、または必要な追加ライセンスを取得することなく、一時的な需要（事業体の作業負荷の急増、または R & D グループのテストおよび開発ニーズなど）のサポートのために作成され、後に削除されることは珍しいことではありません。この仮想化の動的な性質は、ライセンス規則に関する不確実性と課題（特に過去のライセンス契約に関するもの）と相まって、今日では仮想化の効果的な SAM にとっての最大の課題の 1 つになっています。

仮想化に関連したライセンスの課題、および仮想化そのものの存在の高まりによって、ソフトウェア発行者には、2 つの方向性が考えられます。 1 つ目のアプローチは、ハードウェアベースのライセンス メトリックへの依存度を減らし、その代わりにユーザーベースのメトリック、スループットベースのメトリック（処理数など）、または結果ベースのメトリック（収益など）を推進するものです。もう 1 つのアプローチは、利用者に仮想化環境でハードウェアメトリックを収集するための特定のツールを提供する方法です（IBM License Metrics Tool、ILMT など）。前述のアプローチにより、ソフトウェア発行者に対して、組織はより効果的に、仮想化環境下で SAM を実装できるようになります。しかし、組織は仮想化に関連する SAM の課題のすべて、もしくはその多くの解決をソフトウェア発行者だけに依存することはできません。

エンドユーザー組織にとって、SAM に対する仮想化の影響は重大です。SAM プログラムは、SAM の対象の範囲内のすべての仮想化された資産に対処し、仮想化の影響を受けるソフトウェアライセンスについての総合的なデータを持っている必要があります。ソフトウェア発行者がポリシーを更新し続けるため、SAM プログラムは、定期的にライセンス規則の理解を新たにする必要があります。仮想化によって影響を受けるソフトウェア資産はすべて、仮想化の展開によって潜在的な負の財政的影響を引き起こさないように、慎重に管理しなければなりません。さらに、SAM プログラムは、既存の管理プログラムの範囲外である可能性のある仮想化技術のあらゆる不正利用に関して、IT インフラストラクチャを定期的に見直す必要があります。

仮想化に関するもう 1 つの SAM 特有の課題は、プロビジョニング解除に関係するものです。仮想マシンは、一時的なニーズに対応するために迅速かつ容易に作成することができます。しかし、ビジネスニーズが無くなれば、誰かがこの仮想マシンを削除する必要があり、そうしなければ組織は不要な追加ライセンスを消費し続けることになります。多くの組織は、何のために作成されたのかを知る人がいない「孤児の」仮想マシンを多数所有しています。SAM プログラムは、不要となった仮想マシンのタイムリーなプロビジョニング解除に関する管理機能を実装すべきです。

ソフトウェア発行者は、様々なレベルで、仮想化の影響に関する公式なガイダンスとポリシーを開発しています。SAM プログラムは、ソフトウェアライセンス契約で「言及されていない」場合でも、ソフトウェアライセンスへの仮想化の影響を「想定」することはできません。組織は、常に聞きたい答えを得られないかもしれませんが、発行者がライセンス付与に関して仮想化をどのように位置づけているのかについて十分に明確にしておくことは、SAM プログラムを成功させるために必要なことです。

さらに、SAM を複雑にするのは、仮想化環境で見られる複合メトリックという現実です。組織は、おそらく仮想化前と仮想化後の両方でソフトウェアを購入します。つまり、同じソフトウェアに対して異なるタイプのライセンスを持ち、これらのライセンスは、仮想化によって異なる影響を受けることになります。組織は、発行者のポリシーに明確に沿った方法で、仮想化環境内でライセンスを展開するために、ソフトウェア発行者と連携しなければなりません。そうしなければ、予定外の監査関連費用のリスクを負うことになります。

SAM と Infrastructure as a Service / Platform as a Service

SaaS 以外のクラウド実装モデル（IaaS や PaaS）においては、CSP によって提供されるソフトウェアもあれば、組織が提供するソフトウェアもあります。IaaS/PaaS には、Amazon EC2、Microsoft Azure、IBM SmartCloud 等があります。

SaaS の場合と同様に、**CSP が提供するソフトウェア**（オペレーティングシステムまたはミドルウェアソフトウェアなど）に関して、利用者は CSP がソフトウェアを提供するために適切なライセンスを取得しており、予定している利用方法が CSP 保有のライセンスでカバーされるという保証を得る必要があります。CSP が利用者に対し自社製品以外のソフトウェアを利用させる場合（その可能性は大いにあります）、CSP は、サービスプロバイダーライセンス契約、またはそれと同等の形で、CSP が第三者にサービスを提供するために、CSP によるソフトウェアの利用を許可するソフトウェア発行者からのライセンスが必要となります。利用者は、CSP がサービスを提供する法的権利を有するという保証を、CSP から受け取りたいと思うかもしれません。また、利用者は、そのサービスが知的財産権を侵害しているという第三者による申し立てから自身を保護するクラウド契約上の補償条項を要求すべきです。

CSP が提供するソフトウェアに関するもう 1 つのリスクは、CSP が正規のソフトウェアを利用していないというリスクです。CSP が偽造ソフトウェアを利用している場合、コードに対し不正な変更（トロイの木馬ウイルスを含めるなど）が行われている可能性があり、これは組織にとっての情報セキュリティ リスクとなります。組織は、CSP が提供するソフトウェアに対して如何なる制御も持たないことから、CSP が正規のソフトウェアだけを利用していることを契約条項に含めたり、または評判の高いもしくは認定されている CSP のみを利用するといった方法で、CSP の正規ソフト利用を確実にする必要があります。

利用者が用意するソフトウェアに関しては、利用者はソフトウェア発行者との契約および CSP との契約という、2 つの異なる契約書の下での管理に直面することに留意しなければなりません。

組織とソフトウェア発行者の関係、組織と CSP の関係の間に溝ができると、クラウドでの効果的な SAM を達成する上で、次の課題および留意事項が生じる可能性があります。

ライセンス契約から抜粋した以下の条項は、内部利用ソフトウェアを第三者に対して利用させることについての制限（適切なライセンスを取得していない場合には、CSP が負う制限）の一例です。「ライセンシーは、ソフトウェアをリース、貸借またはレンタルせず、サービスビューロー、タイムシェアリング、アプリケーションサービスプロバイダー、ホスティングまたはその他第三者へのコンピュータサービスに提供するためにソフトウェアを利用せず、また、ソフトウェアの機能を第三者が利用できるようなことは行いません」。

CSP がソフトウェア発行者でもあり、同一のソフトウェアを 2 つの方法（従来型／オンプレミスとクラウド型）で提供している場合もあります。

- **クラウドへのライセンス移行：**ライセンス条件に基づき、ソフトウェアライセンスのクラウドへの移行は、ソフトウェア発行者の同意を必要とすることがあります（例えば、ソフトウェアライセンス契約の中には、原則的に施設外での利用または組織が保有していないハードウェア上での展開を禁じているものもあります）。主要な発行者の中には、クラウドでのライセンスの利用を禁止するポリシーを持つところもありますが、その一方で独自のクラウドを作成し、クラウドにおけるソフトウェアの利用を計測する仕組みを作成し、一部の CSP（他は除く）をソフトウェアが安全に利用できる場と認定している発行者もあります。しかし、他の多くのソフトウェア発行者は、明確なポリシーを持っていません。クラウドへ許可なくソフトウェアライセンスを移行すると、組織または場合によっては CSP が責任を負うリスクにさらされる可能性があります。

- **不正利用：**ライセンス条件は、クラウドにライセンスを移行する能力に影響を与えかねない様々な制限を規定することがあります。そのような制限の例には次のものが含まれます。

  - 地理的制限 — 一部のクラウドサービスでは、利用者が、サーバーの物理的な場所（または国）を把握していない場合があるため、管理が特に困難な可能性があります。

  - ライセンス付与によってカバーされる法人の制限 — 特定の条件があるため、クラウドを利用できない場合があります。

  - デバイスおよびプラットフォームに対する制限 — 特定のクラウド環境で利用できない場合があり、一部のクラウド環境においては、利用者はクラウドアーキテクチャについて技術的詳細を知らないことから、管理が特に難しい場合があります。

- **クラウドでのハードウェア関連ライセンスメトリックの測定：**完全、正確、かつ再現可能な方法でハードウェア関連のライセンスメトリックを測定することは、対象となるハードウェアが利用者のデータセンターに存在するという従来型の状況下であっても、SAM の重大な課題であることに変わりはありません。IaaS/PaaS の複雑さが追加されることで、タスクがより困難になります。CSP が保有／提供するソフトウェアを、利用者が保有／提供しているものと区別し、それぞれを正しく計上するのが困難になるため、ライセンス料金の過剰支払いまたは過小支払いのいずれかのリスクが発生する場合があります。

- **ソフトウェアベンダー監査：**ほとんどのソフトウェアライセンス契約には監査条項が含まれており、ソフトウェア発行者が通知をもって、利用者がライセンス契約の条件を遵守しているかを確認するために、利用者の環境へアクセスすることが認められています。他方、利用者がクラウド内における物理サーバーの場所を知る方法があるとしても、ソフトウェア発行者に現地へのアクセスを許可することを CSP と合意できる可能性はほとんどありません。そのため利用者は、ソフトウェアベンダーとの間で結んだソフトウェアライセンス契約に違反する可能性があります。また、場合によっては、利用者がクラウド上の仮想マシンへのリモートアクセスを監査人に提供できる場合があります。もっとも、基盤となるハードウェアの全メトリックに対するライセンスを求めるソフトウェア発行者にとって、このようなアクセスだけでは十分ではない場合があります。利用者がマルチテナントの環境で、CSP の他の利用者とこのような基盤となるハードウェアを共有している可能性が高いことからすれば、利用者が CSP から基盤となるハードウェアにアクセスできる可能性はほとんどありません。さらに、ライセンス契約によって、組織が指定された時間内に特定のデータを提供する必要がある場合、SAM プログラムはそのような要件が確実に遵守されるよう CSP と連携しなければなりません。

- **クラウドからのライセンスの回収：**利用者は、クラウドサービス契約、ソフトウェアライセンス契約およびソフトウェア発行者のポリシーに基づいて、クラウドの利用が終了した際に、ライセンスを再利用するかどうかを判断しなければなりません。ライセンスを元に戻すには、ソフトウェア発行者または CSP の同意が必要な場合があります。

BSA | ザ・ソフトウェア・アライアンスについて

BSA | The Software Alliance（BSA | ザ・ソフトウェア・アライアンス）は、政府や国際市場に先駆けて、世界のソフトウェア産業を代表する業界団体です。BSA 加盟企業は、経済の活性化とより良い現代社会を築くためのソフトウェアソリューションの創造に年間数十億もの投資を行っています。

BSA は著作権をはじめとする知的財産権の保護およびテクノロジーの革新や経済活性化のための政策提言を世界において率先して行っています。

BSA は知的財産権の保護、イノベーションの促進、市場の開放、公正な競争の取り組みとして、世界中の政府とコミュニケーションを取り、知的財産権の啓発、教育活動を実施し、情報テクノロジーに対する消費者、組織、政府の信用と信頼の構築に努めています。

BSA は著作権をはじめとする知的財産権の保護や、テクノロジーの革新や経済活性化のための公共政策提言を世界で率先して行っています。

知的財産の保護とイノベーションの促進

著作権、特許権、商標権等の知的財産権は、創造的企業や組織に対し、法的な枠組を提供し、経済成長の基礎をなすものです。著作権に関連する産業で大きな割合を占めているビジネスソフトウェアの開発においても、知的財産権は必要不可欠なものです。

BSA は政策立案者と連携し、ビジネスソフトウェアをめぐる啓発・教育活動を行うことで、知的財産権がグローバル経済と社会の全体で尊重されるよう取り組んでいます。

- **知的財産権の保護：**BSA は世界中の政府と協力し、知的財産の保護が、クラウドコンピューティングなどの新しいイノベーションに迅速に対応するよう尽力しています。
- **ソフトウェア不正利用の撲滅：**BSA は、ソフトウェア不正使用を撲滅するため、ソフトウェアの組織内不正使用、海賊版、インターネット上での不正に対する加盟企業による権利保護活動の支援を行っています。
- **先進的なリサーチ：**BSA は、著作権侵害およびそれに関わる経済的影響についてグローバルな研究成果を発表し、問題を浮き彫りにするとともに、解決するための国内および国際的な政策を提言しています。
- **パブリック エデュケーション：**BSA は、消費者にソフトウェアの不正コピーに関連したリスクに関する教育を提供すると同時に、組織がより効果的なソフトウェア資産管理（SAM）を実現するためのツールおよびトレーニングプログラムを提供しています。

市場開放および公正競争の確保

- 開かれた市場は、経済の成長と繁栄に不可欠です。BSA は、貿易障壁の撤廃と競争を妨げイノベーションを停滞させる差別的な調達優遇の排除に向けて政府に働きかけ、ソフトウェア業界の市場機会を拡大します。

- **成長の障壁の撤廃：**BSA は市場開放を促進するため、政策立案者に対し情報提供、専門家による分析や業界の見識の共有をしています。このような取り組みは、テクノロジー分野の市場が急速かつ最も成長している一方で、不正利用がおびただしい BRIC 諸国に対して特に注力しています。

- **テクノロジーの中立性の促進：**BSA は、国際的に認知された基準と公平な IT 政府調達ポリシーを促進することで、テクノロジーに関する公正競争を奨励します。

- **新たなイノベーションのサポート：**BSA は世界中の政策立案者とともに、クラウドコンピューティング等の新しいテクノロジーが広く利用される環境づくりに努めています。これは、技術標準に携わるだけでなく、知的財産保護の向上、国際的な法的原則の協調、一組織や一政府の枠を越えた取組みを含みます。

テクノロジーへの信用と信頼の構築

セキュリティおよびプライバシーといった項目は、消費者や組織、政府にとって情報テクノロジーの根底にあるものです。BSA では責任あるデータ管理に加え、テクノロジー市場を変容させ、社会に価値を創造するイノベーションの浸透を支援しています。

- **官民連携の推進：**BSA 加盟企業の専門知識を活かして、政府関係者と生産的な活動をするため、BSA はナレッジセンターとして機能する他、業界と政府間の協力とコンセンサスの構築を促す役割を果たしています。

- **消費者の保護：**クラウドコンピューティングなどの新しいテクノロジーが生まれる際、BSA および加盟企業は、プライバシーとセキュリティの適切な基準を策定し、政策立案者や規制当局とその見識を共有します。

- **政策ソリューションの提案：**BSA は、サイバー犯罪の効果的な阻止と処罰、脅威の軽減、消費者への情報提供と保護、サイバー事件への対応に向けた政策を策定する際に、政府の指針となるグローバル サイバーセキュリティについての枠組みを策定しました。

巻末注

[1] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2] ITIL V3 Guide to Software Asset Management
（ITIL V3 ソフトウェア資産管理ガイド）

[3] http://www.19770.org

[4] https://samadvantage.bsa.org

[5] http://www.tagvault.org

www.bsa.co.jp

BSA Worldwide Headquarters

20 F Street, NW
Suite 800
Washington, DC 20001

T: +1.202.872.5500
F: +1.202.872.5501

BSA Asia-Pacific

300 Beach Road
#25-08 The Concourse
Singapore 199555

T: +65.6292.2072
F: +65.6292.6369

BSA Europe, Middle East & Africa

2 Queen Anne's Gate Buildings
Dartmouth Street
London, SW1H 9BP
United Kingdom

T: +44.207.340.6080
F: +44.207.340.6090

Argentina Australia Belgium Brazil Canada Chile China Colombia Czech Republic Denmark France Germany Greece India Indonesia Israel Italy Japan Malaysia Mexico Netherlands Panama Peru Poland Russia South Africa South Korea Spain Taiwan Thailand Turkey Vietnam