COSO

トレッドウェイ委員会支援組織委員会

全社的リスクマネジメント

クラウドコンピューティングのための全社的リスクマネジメント

Crowe

マイク・グローブ | ヴィクトリア・チェン

2021 年 7 月

著　者

Ｃｒｏｗｅ社シカゴ、コンサルティング部門
プリンシパル・パートナー
マイク・グローブ

Ｃｒｏｗｅ社シカゴ、コンサルティング部門
マネージング・ディレクター
ヴィクトリア・チェン

トレッドウェイ委員会支援組織委員会（ＣＯＳＯ）理事

序　文

本プロジェクトは、トレッドウェイ委員会支援組織委員会（ＣＯＳＯ）から委嘱されたものである。ＣＯＳＯは、組織のパフォーマンスや監督を改善するとともに、組織における不正を減らすために立案された内部統制、全社的リスクマネジメントおよび不正抑止に関する包括的なフレームワークとガイダンスの開発を通じて先進的な考え方を提供することに取り組んでいる。ＣＯＳＯは、次の団体の協賛と資金提供によって運営されている民間部門主導の団体である。

米国会計学会（American Accounting Association）

米国公認会計士協会（American Institute of Certified Public Accountants）

国際財務担当経営者協会（Financial Executives International）

管理会計士協会（Institute of Management Accountants）

内部監査人協会（Institute of Internal Auditors）

COSO
トレッドウェイ委員会
支援組織委員会

coso.org

全社的リスクマネジメント

クラウドコンピューティングのための全社的リスクマネジメント

調査委嘱者

COSO

トレッドウェイ委員会支援組織委員会

2021 年 7 月

Design and production: Sergio Analco.

coso.org

目　次

はじめに

クラウドコンピューティングが初めて導入されて以来、クラウドは成長し拡大してきた。2020 年の新型コロナウイルス感染症のパンデミックに先立ち、2019 年 4 月にガートナー社は、2019 年の市場規模を 2,140 億ドルと評価し、2020 年は 16.5%増の 2,500 億ドル、2021 年には 15.7%増の 2,890 億ドルに成長すると予測した[4]。パンデミックとリモートワークの必要性を踏まえ、クラウドコンピューティングの拡大はより早くなり、多くの組織で導入時期が前倒しされた。１年半後の 2020 年 11 月、ガートナー社は世界のパブリッククラウドサービスの 2019 年の収益が 2,430 億ドルであったと報告し、2020 年は６%増の 2,580 億ドル、2021 年には 18%増の 3,050 億ドルになると予測した[5]。これらは、2020 年予測で３%増、１年半後の 2021 年予測で 5.5%増となる。

一部の業種では、クラウドコンピューティングを活用することが、ある時点では戦略的な優位性であったかもしれない。パンデミックによって浮き彫りになったのは、よりリモートで柔軟な労働環境の必要性と、そのために組織を支援するＩＴインフラの必要性であった。クラウドコンピューティングの活用は、市場で競争するために必要不可欠な要素となっている。

クラウドコンピューティングは、調達から導入までのスピードが速いことが大きな特徴である。しかし、クラウドベースへのアクセスを加速することに慣れてしまい、クラウド環境におけるリスクを軽減するために設計された適切な統制を実施する能力がない組織があるかもしれない。

クラウドコンピューティングには、いくつかの定義がある

「クラウドコンピューティングは、共用の構成可能なコンピューティングリソース（ネットワーク、サーバー、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当てられ提供されるものである[1]。」

ー米国国立標準技術研究所（ＮＩＳＴ）

・・・

「セルフサービスのプロビジョニング及びオンデマンド管理を備える、スケーラブルで伸縮自在な共有できる物理的又は仮想的なリソース共用へのネットワークアクセスを可能にするパラダイム[2]。」

ー国際標準化機構（ＩＳＯ）

・・・

「インターネットを介してアクセスできる複数のサーバに、定期的に使用するコンピュータのデータを保存する方法[3]。」

メリアム・ウェブスター

・・・

最も簡単に言えば、**クラウドコンピューティングとは、インターネット上にプールされたリソースを利用するコンピューティングモデルである。**基盤となるサーバやプロセスの管理は、他の組織に委託する場合がある。

1 The NIST Definition of Cloud Computing Special Publication 800-145 – September 2011 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf（訳注：邦訳は、独立行政法人情報処理推進機構「NIST によるクラウドコンピューティングの定義　米国国立標準技術 研究所による推奨」によるもの。https://www.ipa.go.jp/files/000025366.pdf）

2 ISO/IEC 17788:2014 In formation technology — Cloud computing — Overview and vocabulary – October 2014 https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en（訳注：邦訳は、「日本工業規格 JIS X 9401：2016（ISO/IEC 17788：2014）情報技術ークラウドコンピューティングー概要及び用語」によるもの。https://kikakurui.com/x9/X9401-2016-01.html）

3 Merriam-Webster

4 https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g

5 https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021

トレッドウェイ委員会支援組織委員会（ＣＯＳＯ）の『内部統制の統合的フレームワーク』（2013 年）[i] と、『全社的リスクマネジメント－戦略およびパフォーマンスとの統合』（2017 年）[ii] は、クラウドコンピューティングとクラウドセキュリティのガバナンスと統制のための包括的な基盤を提供している。ＣＯＳＯの全社的リスクマネジメント（ＥＲＭ）フレームワークは、組織がガバナンスを確立し、リスクを識別して対応し、パフォーマンスをモニタリングし、コミュニケーションを維持し、組織やその事業目標、または業界やその環境に変化があった場合に調整するための仕組みを提供している。また、ＣＯＳＯの内部統制フレームワークは、リスクとリスク対応を評価するために、ＣＯＳＯ ＥＲＭフレームワークのパフォーマンスという構成要素で通常使用するツールも提供している。

本稿の目的は、ＣＯＳＯのフレームワークを活用して、クラウドコンピューティングのガバナンスを確立するためのガイドを提供することである。また、クラウドコンピューティングを導入するための行程（付録Ａ．クラウドコンピューティングへの行程）も提供し、適切な役割と責任（付録Ｂ．役割と責任）も説明する。本稿は、多くの組織がハイブリッドなＩＴ環境（インハウス・オンプレミスのＩＴリソースとクラウドコンピューティングリソースの両方を使用）であることを認識している。本稿では、クラウドコンピューティングの検討事項のみに焦点を当てている。

クラウドコンピューティングの採用と導入においては、組織はさまざまな成熟段階にある。初期段階にある組織には、このガイダンスが役に立つ。また、導入が完了した組織は本ガイドを利用して評価し、必要に応じてガバナンスと統制の強化を遡及的に実施できる。クラウドガバナンスを強化することで、組織のリスクを低減し、また、より効率的かつ効果的なクラウドコンピューティングの利用とマルチクラウド環境でのモニタリングが可能になる。

i 訳注：邦訳は、八田進二・箱田順哉監訳、日本内部統制研究学会・新ＣＯＳＯ研究会訳『内部統制の統合的フレームワーク』日本公認会計士協会出版局、2013 年。
ii 訳注：邦訳は、一般社団法人日本内部監査協会・八田進二・橋本 尚・堀江正之・神林比洋雄監訳、日本内部統制研究学会ＣＯＳＯ - ＥＲＭ研究会訳『COSO 全社的リスクマネジメント－戦略およびパフォーマンスとの統合』同文舘出版、2018 年。

クラウドコンピューティング環境での全社的リスクマネジメント

クラウドコンピューティング環境は、パブリッククラウド、プライベートクラウドまたはハイブリッドクラウドのいずれに配置されるかにかかわらず複雑である。さまざまな第三者のサービスプロバイダと多くの業務機能を統合する必要があるため、その管理は同じく複雑である。同様に複雑なのは、組織が使用する総体的なＥＲＭプロセスとフレームワークの中にクラウドガバナンスを統合することである。

2004 年版のＣＯＳＯ『全社的リスクマネジメントーフレームワーク篇』[iii]は、戦略の設定や組織のパフォーマンスを推進する上でリスクを識別して対処することの重要性に着目して、2017 年版『ＣＯＳＯ 全社的リスクマネジメントー戦略およびパフォーマンスとの統合』へと改訂された。この改訂により、組織には、クラウドコンピューティング環境のガバナンスと管理に適用する強固なフレームワークが提供された。

図１.『ＣＯＳＯ 全社的リスクマネジメント―戦略およびパフォーマンスとの統合』

出典：2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*（邦訳は、『COSO 全社的リスクマネジメントー戦略およびパフォーマンスとの統合』）

組織の経営者には、組織に対するリスクを管理する責任がある。経営者はリスクマネジメントが組織の戦略や事業目標と統合されるように、取締役会や主要な利害関係者をＥＲＭプログラムに組み込まなければならない。効果的なＥＲＭは複数の部門や機能が関与するものであり、組織の戦略に統合され、カルチャーに組み込まれるべきである。ＥＲＭの成功は内部統制にとどまらず、ガバナンス、カルチャー、戦略およびパフォーマンスにまで及ぶ。効果的なクラウドコンピューティングとクラウドＥＲＭは、組織の戦略と目標を支え、カルチャーと調和し、価値を高め、組織内で統合される。

iii 訳注：邦訳は、八田進二監訳、中央青山監査法人訳『全社的リスクマネジメント フレームワーク篇』東洋経済新報社、2006 年。

ＣＯＳＯの全社的リスクマネジメントのフレームワーク自体は、相互に関連する５つの構成要素に整理された一連の原則である。

ガバナンスとカルチャー：ガバナンスは、全社的リスクマネジメントの重要性を重視し、それに対する監督責任を確立する組織の気風を醸成する。カルチャーは、事業体の倫理観、望ましい行動およびリスクの理解に関係している。

戦略と目標設定：戦略計画立案プロセスにおいて、全社的リスクマネジメント、戦略および目標設定は、一体となって機能する。リスク選好が設定され、戦略との整合性が図られる。事業目標は、戦略を実践するとともに、リスクの識別、評価および対応の基礎となる。

パフォーマンス：戦略と事業目標の達成に影響を及ぼす可能性のあるリスクは、識別し、評価する必要がある。リスクは、リスク選好に基づいて、その重大度により優先順位づけられる。組織は、リスクへの対応を選択し、想定したリスク量のポートフォリオの視点を得る。このプロセスの結果は、主要なリスクのステークホルダーに報告される。

レビューと修正：事業体のパフォーマンスをレビューすることにより、組織は、全社的リスクマネジメントの構成要素が、長期的かつ大きな変化を踏まえた上で、どの程度有効に機能しているか、そして、どのような修正が必要かを検討できる。

情報、伝達および報告：全社的リスクマネジメントには、必要な情報を入手し、共有する継続的なプロセスが必要である。情報は、内部および外部から入手され、組織内を下から上へ、上から下へ、そして、横断的に流れる[6]。

図２．『ＣＯＳＯ 全社的リスクマネジメント－戦略およびパフォーマンスとの統合』－５つの構成要素と結びついた 20 の原則

ガバナンスとカルチャー	戦略と目標設定	パフォーマンス	レビューと修正	情報、伝達および報告
1．取締役会によるリスク監視を行う	6．事業環境を分析する	10．リスクを識別する	15．重大な変化を評価する	18．情報とテクノロジーを有効活用する
2．業務構造を確立する	7．リスク選好を定義する	11．リスクの重大度を価する	16．リスクとパフォーマンスをレビューする	19．リスク情報を伝達する
3．望ましいカルチャーを定義づける	8．代替戦略を評価する	12．リスクの優先順位けをする	17．全社的リスクマネジメントの改善を追求する	20．リスク、カルチャーおよびパフォーマンスについて報告する
4．コアバリューに対するコミットメントを表明する	9．事業目標を組み立てる	13．リスク対応を実施する		
5．有能な人材を惹きつけ、育成し、保持する		14．ポートフォリオの視点を策定する		

出典：2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*（邦訳は、『COSO 全社的リスクマネジメント－戦略およびパフォーマンスとの統合』）

以下の章では、『ＣＯＳＯ 全社的リスクマネジメント－戦略およびパフォーマンスとの統合』のフレームワークの適用方法として、各構成要素の評価に加えて、20 の原則をクラウドコンピューティングガバナンスに適用する方法を説明し、その後、原則をクラウドコンピューティングに適用する方法についてのガイダンスを示している。本ガイドは、クラウドコンピューティングのリスクを考える上で、ＣＯＳＯ ＥＲＭフレームワークを活用するための仕組みを提供している。クラウドコンピューティングは、組織が事業戦略を達成し、価値を創造するためのもう１つのツールであるため、クラウドコンピューティングの戦略、リスクおよびＥＲＭは、組織内のＥＲＭプログラム全体に組み込まれるべきである。

6 2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*（邦訳は、『COSO 全社的リスクマネジメント－戦略およびパフォーマンスとの統合』）

ガバナンスとカルチャー 

表１．１ 『ＣＯＳＯ 全社的リスクマネジメント－戦略およびパフォーマンスとの統合』－ガバナンスとカルチャーの原則[7]

原則	説明
１．取締役会によるリスク監視を行う	取締役会は、戦略を監視し、ガバナンスの責任を果たすことにより、経営者が戦略と事業目標を達成できるよう支援する。
２．業務構造を確立する	組織は、戦略と事業目標を達成するために、業務構造を確立する。
３．望ましいカルチャーを定義づける	組織は、事業体の望ましいカルチャーを特徴づける望ましい行動を定義づける。
４．コアバリューに対するコミットメントを表明する	組織は、事業体のコアバリューに対するコミットメントを表明する。
５．有能な人材を惹きつけ、育成し、保持する	組織は、戦略と事業目標にふさわしい人的資本の形成にコミットメントする。

❶ 取締役会によるリスク監視を行う

組織のガバナンスとカルチャーは、取締役会と経営者から始まる。経営者が事業目標とカルチャーを定義する一方で、取締役会はその戦略と目標を監督すべきである。組織の事業目標を実現するための経営者の活動をモニタリングするのに必要な専門知識を提供するためには、業界、組織、テクノロジー、ガバナンスとコンプライアンスおよび財務に関する幅広い知識を持つ者を集めた多様な取締役会が必要である。

取締役会はその監督の役割を利用して、以下のような質問を組織に投げかけるべきである。

- テクノロジーは組織の目標達成にどのように役立つか。
- テクノロジーは（第三者のリスクを含む）組織のリスクをどのように増加または減少させるか。
- 現在および将来のクラウドのトレンドと業界のテクノロジーの変化は何か。
- （オンプレミス・インフラの廃棄を含め）クラウドコンピューティングが組織に与える影響は何か。
- 組織の戦略とクラウドサービスプロバイダ（ＣＳＰ）の戦略はどのように整合しているか。
- 組織は同業他社やベンチマークと比較してどうか。

7 2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*（邦訳は、『COSO 全社的リスクマネジメント－戦略およびパフォーマンスとの統合』）

❷ 業務構造を確立する

組織はクラウドコンピューティングに移行する前に、フレームワークとガバナンスを定義する必要がある。組織は事業目標を支えるための組織構造を整備する必要がある。これらの組織構造が、クラウドコンピューティングをどのように支援できるかを検討すべきである（すなわち、追加の役割は定義されるか、追加の報告は行われるか、責任はどこにあるかなど）。

必要なガバナンス構造を構築するために、組織はクラウドコンピューティング運営委員会の設置を決定し、どのようなプロセス、アプリケーションおよびデータがクラウドコンピューティングに移行されるかについて適切な監督が行われるようにすることができる。このクラウドコンピューティング運営委員会は、方針、手続、シャドーＩＴ（ＩＴ部門の承認を受けていないＩＴリソース）を回避するための監督およびクラウドコンピューティングのパフォーマンスをモニタリングするための組織構造など、適切なクラウドガバナンス構造を確保すべきである。クラウドコンピューティング運営委員会は得られた教訓を再確認して、継続的にリスクカルチャーを強化できる。

クラウドコンピューティングのアクティビティは、組織内の複数の領域に影響を及ぼす。例えば、法務、財務、情報テクノロジー、リスク、ベンダー管理、コンプライアンス、内部監査および影響を受けるすべての業務部門は、クラウドコンピューティングの採用とモニタリングのプロセスについて透明性を保ちながら協力的に取り組むべきである。

さらに、組織はＣＳＰと協力して、組織、ＣＳＰおよび該当する場合はＣＳＰにとってのＣＳＰの運用体制と責任を定義する必要がある。例えば、サービスとしてのソフトウェア（ＳａａＳ）のＣＳＰが、サービスとしてのインフラストラクチャ（ＩａａＳ）プロバイダのオペレーティングシステムとデータベースサービスを使用する場合、組織のＣＳＰであるＳａａＳ企業には、ＩａａＳ企業というＣＳＰも存在することになる。ベンダー間の役割分担とパフォーマンス指標を明確にすることが、優れたガバナンスには不可欠である。

ＲＡＣＩ（responsible（実行責任者）－ accountable（説明責任者）－ consulted（相談先）－ informed（報告先））マトリクスなどの明確な責任分担マトリクスを担当者に割り当てれば、説明責任とコミュニケーション、そして組織がクラウドコンピューティングで達成しようとするオープンで前向きな思考と協力的なカルチャーが生み出せる。オープンなコミュニケーション経路と各ＲＡＣＩレベルにおける個人の適切な関与は、リスクの考え方を理解させ、組織のカルチャーに根付かせるのに効果的である。クラウドコンピューティングに必要な主な役割は、付録Ｂ．役割と責任を参照されたい。

❸ 望ましいカルチャーを定義づける
❹ コアバリューに対するコミットメントを表明する

組織全体で一貫したガバナンスを実施するためには、組織全体でクラウドを意識したカルチャーを作ることが必要である。経営者は、クラウドのカルチャー、使用方法、データプライバシー、データセキュリティおよびサイバーセキュリティの方向性を決定する。クラウドコンピューティングは組織内のどの部署でも利用する可能性があるため、全員が自身の役割とクラウドコンピューティングに関連する全社的なリスクを理解する必要がある。透明性を確保するためには、クラウドコンピューティングを部門横断的な計画プロセスに統合する必要がある。クラウドコンピューティングを総体的な戦略の一部として捉えることは、各部門が業務上のニーズを満たすために独立したソリューションを見つけることとは異なり、優れたクラウドガバナンスモデルに不可欠である。説明責任者を定めることで、組織のコアバリューに対するコミットメントが表明できる。

また、ＣＳＰパートナーのカルチャーや価値観を理解することも重要な要素である。ＣＳＰを活用すると、ＣＳＰは組織の延長線上の存在となる。この関係を理解して適切なパートナーを選択すれば、組織のカルチャーやコアバリューが反映され強化される。

❺ 有能な人材を惹きつけ、育成し、保持する

人的資本管理の一環として、組織はクラウドガバナンスを管理するために必要な社内リソースを特定すべきである。従業員がクラウドコンピューティング環境でしっかり業務ができるように、適切な研修を開発して提供すべきである。クラウドコンピューティングのタスクの中には、クラウドコンピューティングにおける相違に対していくつかの追加研修や微調整をすることによって、既存の機能に組み込めるものがある。エンドユーザの役割は、クラウドベンダーの管理やユーザの管理の担当者の役割とは異なる。役割にかかわらず、クラウドコンピューティングのガバナンスフレームワークの確立においては、組織のカルチャーと価値観が反映されるべきである。

ＣＳＰを利用する場合、テクノロジーに対する一定の責任がＣＳＰの組織に移ることになるが、同様に、人的資本管理もＣＳＰに移ることになる。ＣＳＰの人的資本管理のアプローチと、それが組織の能力をどのように補完するかを理解することは、クラウドコンピューティングの人的資本管理を総合的なＥＲＭプロセスの一部として見るための方法である。

表1．2　**クラウドコンピューティングのための主要な活動―ガバナンスとカルチャーの原則**

原則	説明	クラウドコンピューティングＥＲＭの主要な活動
1．取締役会によるリスク監視を行う	取締役会は、戦略を監視し、ガバナンスの責任を果たすことにより、経営者が戦略と事業目標を達成できるよう支援する。	取締役会は、クラウドコンピューティング、トレンドおよび組織や業界への潜在的な影響を理解する。
2．業務構造を確立する	組織は、戦略と事業目標を達成するために、業務構造を確立する。	組織は、クラウドコンピューティングの移行と導入を監督するために、クラウドコンピューティング運営委員会を設置する。
3．望ましいカルチャーを定義づける	組織は、事業体の望ましいカルチャーを特徴づける望ましい行動を定義づける。	経営幹部は、クラウド利用カルチャーを定義し、また、組織のミッション、ビジョン、コアバリュー、戦略および事業目標を支えるために、クラウドコンピューティングをどのように活用できるかを定義する。
4．コアバリューに対するコミットメントを表明する	組織は、事業体のコアバリューに対するコミットメントを表明する。	クラウドコンピューティング運営委員会は、コミュニケーションとフォローアップを通じて、クラウドガバナンスの説明責任を向上させる。
5．有能な人材を惹きつけ、育成し、保持する	組織は、戦略と事業目標にふさわしい人的資本の形成にコミットメントする。	組織は必要な人材を定義し、組織全体でクラウドガバナンス活動を実施して管理する包括的な環境を構築できる多様な人材を特定し、惹きつけ、育成し、管理し、報酬を与え、保持する。

戦略と目標設定

表２．１ 『ＣＯＳＯ 全社的リスクマネジメント―戦略およびパフォーマンスとの統合』―戦略と目標設定の原則[8]

原則	説明
６．事業環境を分析する	組織は、リスクプロファイルに対する事業環境の潜在的影響を検討する。
７．リスク選好を定義する	組織は、価値の創造、維持、実現の観点からリスク選好を定義する。
８．代替戦略を評価する	組織は、代替戦略とリスクプロファイルに対する潜在的影響を評価する。
９．事業目標を組み立てる	組織は、戦略と結びつき、かつ、戦略を支える事業目標をさまざまな階層において設定する際にリスクを検討する。

❻ 事業環境を分析する

クラウドコンピューティングは参入が容易で迅速な変化をもたらすが、クラウドに移行する前に、組織はクラウドコンピューティング全体の戦略とクラウドに移行する目標を正式に定義すべきである。ＩＴ環境の一部または全部をクラウドに移行する理由は数多くあるが、恩恵と価値を得るためには、ＩＴ組織は事業部門と協力して目標と戦略を理解し、事業を支えるクラウドコンピューティング戦略の策定を支援しなければならない。このクラウド戦略は、経営者だけでなく取締役などの他の利害関係者とともに吟味し、他の影響や方向性を評価すべきである。

2017 年版のＥＲＭフレームワークによると、事業環境には「事業体に影響を及ぼしたり、より明確にしたり、または変更をもたらすかもしれない傾向、事象、関連性およびその他の要素」が含まれる[9]。新型コロナウイルス感染症のパンデミックは、多くの組織の事業環境を変化させた。その結果、多くの企業は従業員がシステムやデータにリモートでアクセスできるようにするために、クラウドコンピューティング戦略を迅速に変更する必要があった。マイクロソフト社のサティア・ナデラ最高経営責任者は、2020 年４月、「この２か月で ２年分に匹敵するほどのデジタルトランスフォーメーションが起こった」と述べた[10]。

また、クラウド戦略では、感覚的に操作できるユーザインターフェイスによる使いやすさ、カスタマイズの少なさ、導入スピードの速さ、拡張性の容易さなど、クラウドコンピューティングに関連する機会にも焦点を当てることになる。これらはすべて組織が迅速に方向転換し、新たな事業目標を支えることを可能にするイノベーションとデジタルトランスフォーメーションを実現するものである。

事業目標に大きな変更がない、より確立された組織のクラウド戦略は、ＩＴ部門にとって保守が容易なことや、ピーク時の容量を維持する代わりに必要なストレージとコンピューティングだけを使用することによるコスト削減など、効率性が重視できる。

クラウド戦略には、組織とその目標、そして組織の成長を支えるために必要なものが含まれる。組織の基盤となるミッション、ビジョンおよび価値観、そしてその「理由」は、クラウド戦略に反映される。クラウド戦略は、インフラやアプリケーションの移行や取得のためのガイダンスを提供する。

8 2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*（邦訳は、『COSO 全社的リスクマネジメント－戦略およびパフォーマンスとの統合』）
9 同上。
10 https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/30/2-years-digital-transformation-2-months/

クラウド戦略には、マルチクラウド戦略、マルチクラウド配置モデルおよびマルチクラウドサービスモデル[iv]が含まれる場合がある（付録C．用語集と定義参照）。さらに、クラウド戦略は複数年にわたる行程の場合もあるため、当面の戦略やアプローチと最終結果は異なって見え、その過程でのリスクや使用するベンダーも異なる可能性がある。

クラウド戦略とＣＳＰの利用は組織のリスクプロファイルに影響を与えるため、分析が必要である。ＣＳＰが異なると、ＣＳＰのＥＲＭガバナンス、ＣＳＰのベンダーのＥＲＭガバナンスおよびＣＳＰの顧客のＥＲＭガバナンスによっては、組織のリスクプロファイルに異なる影響を与える可能性がある。

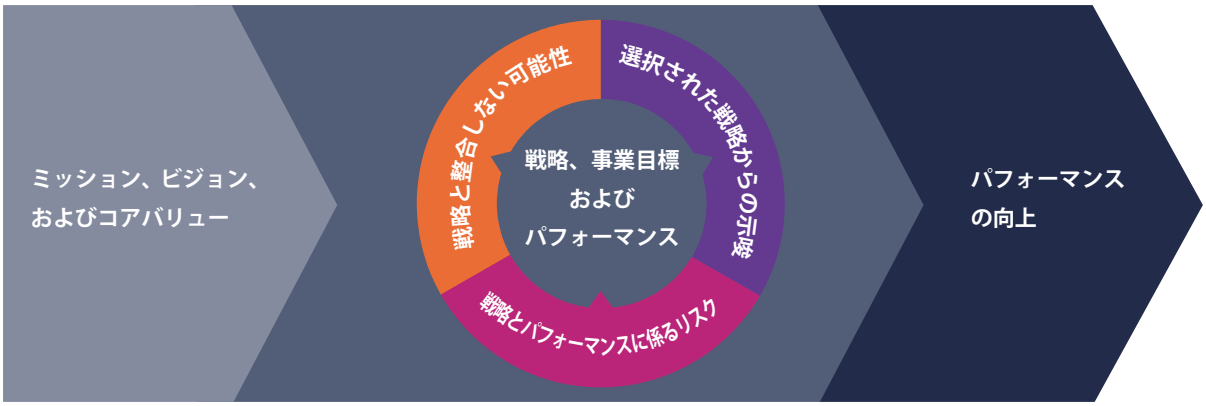
⑦ リスク選好を定義する

一旦クラウド戦略が決定されると、組織はその戦略に対するリスクを評価し、リスク選好に影響があるかを見極めなければならない。この理解は、ＥＲＭのパフォーマンスという構成要素において、異なるクラウド配置モデル、クラウドサービスモデルまたは特定のＣＳＰに基づいて、固有リスクと残余リスクおよび可能性と影響の評価に対する詳細なクラウドコンピューティング・シナリオ評価の結果を組織が適切に判断するのに役立つ。例えば、ハイブリッドなＩＴ環境の一部には、機密データのデータアナリティクスのためには社内管理のアプリケーションを使用し、企業資源計画（ＥＲＰ）アプリケーションはクラウドＳａａＳ上にあり、プライベートＰａａＳ（サービスとしてのプラットフォーム）にはデブオプス（ＩＴの開発（Development）と運用（Operations）を組み合わせた造語）があるといったことが考えられる。経営者が固有リスクと残余リスクを分析することで、組織に適したＩＴ環境を選択することが可能になる。

以下の図３のリングで示されるように、クラウド戦略は組織にリスクをもたらす可能性がある。クラウド戦略が事業戦略と整合していない可能性もあるし、クラウドコンピューティングの利用によって事業戦略の遂行に新たなリスクが生じる可能性もある。例えば、クラウド戦略やクラウドアプリケーションが、組織の製品やサービスラインの一部しかサポートしていない可能性がある。また、クラウド戦略によって１つのＣＳＰに集中し、潜在的な脆弱性や高いリスクプロファイルをもたらすなどの影響もあり得る。これらを適切に管理して対処した場合、組織のパフォーマンスは向上する。

組織はクラウド戦略に関するリスク選好を定義する必要がある。例えば、従業員個人を特定できる情報（ＰＩＩ）と、他の事業組織を顧客とする場合の顧客データでは、リスク選好が異なると判断できる。同様に、組織はアプリケーションごとに異なる可用性要件と復旧時間目標を持つ場合がある。例えば、発注システムは研修システムよりも要件が厳しい可能性がある。このような知識と理解により、組織は何がクラウドコンピューティング戦略に適しているかが評価でき、そのクラウド戦略は、それらのプロセスに関連するリスク選好に応じて、組織の異なる部分（例えば、事業部門や部署）ごとに異なる場合がある。

図３．ミッション、ビジョンおよびコアバリューの観点からの、また、事業体の全体的な方向性とパフォーマンスの原動力としての、ＣＯＳＯ全社的リスクマネジメント



出典：2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*（邦訳は、『COSO 全社的リスクマネジメント－戦略およびパフォーマンスとの統合』）

iv 訳注：原文では、クラウドのサービスモデルのことを「cloud service delivery model」または「cloud delivery model」と表記しているが、いずれも「クラウドサービスモデル」と訳した。

❽ 代替戦略を評価する

当初のクラウド戦略を定義することで、組織は代替案を客観的にレビューして「価値の創造、維持、実現」という観点から評価することができるようになる[11]。さまざまなクラウド戦略、クラウドサービスモデルおよびクラウド配置モデルを検討する際には、組織のリスクプロファイルと事業目標の達成能力、そしてそれらの目標が最終的にどのように成長、生産性、効率および価値を促進するかを検討すべきである。

組織が代替戦略を考えて評価する際に考慮すべきことは、その戦略がイノベーションの機会にどのような影響を与えるかである。従来のオンプレミス型システムは、テクノロジー負債と呼ばれるものを蓄積することが知られている。テクノロジー負債は、既存のシステムを維持するためのコストと、最新のシステムを優先させなかったことによる機会費用として要約できる。

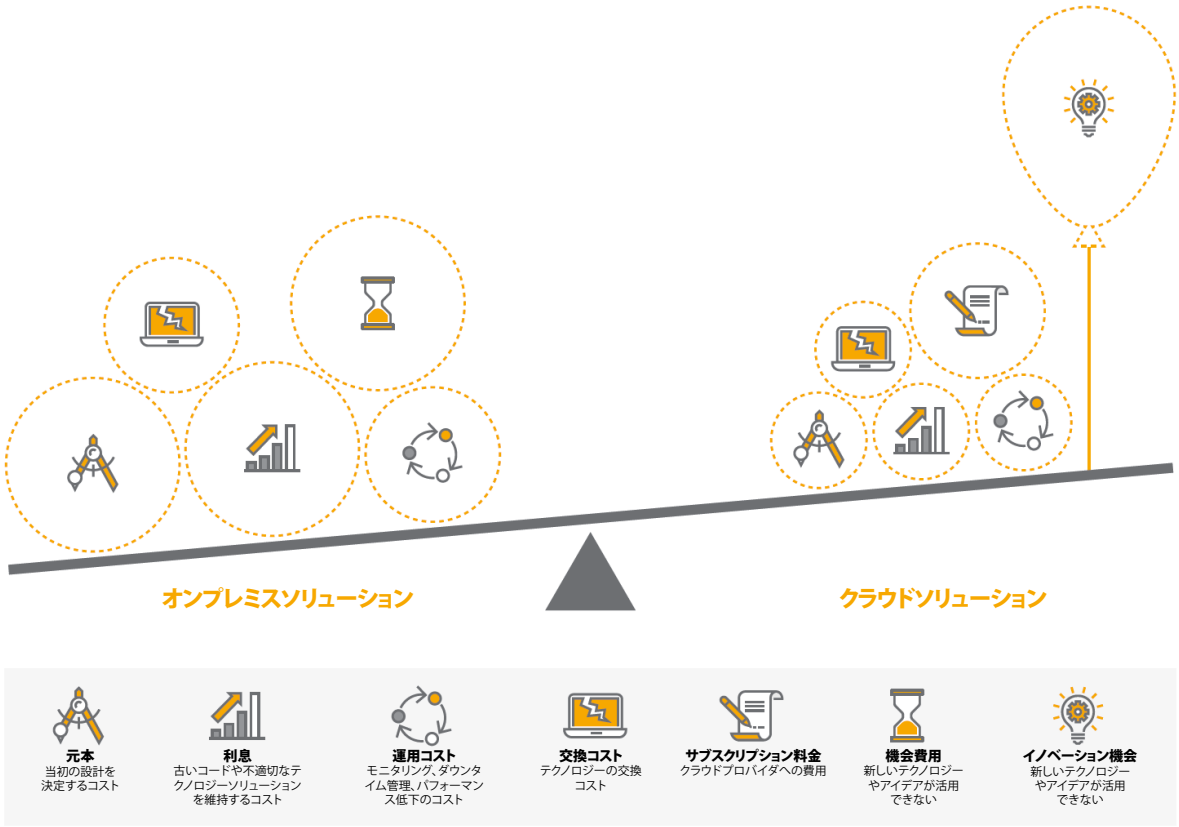
テクノロジー負債の一般的な原因には、以下のようなものがある。

- **過度にカスタマイズされたパッケージソフトウェア**ー大幅にカスタマイズされたＥＲＰシステムを導入すると、ソフトウェアベンダーからの更新を受ける組織の機能を阻害するおそれがある。
- **不適切な技術的ソリューション**ービジネス要件に対処するために、より戦略的な長期的選択肢があるにもかかわらず、短期的またはより慣れ親しんだアプローチを選択すること。
- **時代遅れのテクノロジー**ー時代遅れのオペレーティングシステム、ソフトウェアパッケージおよびインフラ。

テクノロジー負債が多い組織は、通常、リスクが高まり、（負債の維持と解消の両方に）高いコストがかかる。適切な行動を決定するために、組織はテクノロジー負債を増加させる原因となるコスト（図４に表示）と、負債を解消するための代替策を比較検討しなければならない。同様に、テクノロジーに効果的な投資をしてこなかった組織は、テクノロジーの導入や関連事項に関する効率性や有効性が失われるため、リスクが高まりコストが増加する可能性がある。

組織はクラウドの代替案を評価してテクノロジー負債を見直す際に、特定のアプリケーションの機能に合わせてプロセスを変更するコスト、代替ソリューションを導入する時間、マルチテナンシーによる追加のサイバーセキュリティリスクのバランスを取るべきである。

図４．**テクノロジー負債と代替コストの一因となる要素**



11 2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*（邦訳は、『COSO 全社的リスクマネジメント－戦略およびパフォーマンスとの統合』）

❾ 事業目標を組み立てる

一旦クラウド戦略が定まれば、事業目標を支えるためのクラウド目標を定めるべきである。クラウド目標には、クラウドガバナンスの一環として、クラウドセキュリティモデルを含めるべきである。

事業戦略や事業目標は、組織が成長するにつれて、あるいは外部の事象に対応するために更新される。これらの更新は、ＥＲＭフレームワークの観点からクラウド戦略の継続的な評価を促進する。さらに、リスク選好は時間の経過とともに変化する可能性があるため、同様に定期的に更新すべきである。

表２．２　**クラウドコンピューティングのための主要な活動―戦略と目標設定の原則**

原則	説明	クラウドコンピューティングＥＲＭの主要な活動
６．事業環境を分析する	組織は、リスクプロファイルに対する事業環境の潜在的影響を検討する。	組織は、さまざまなクラウド戦略（クラウド配置モデル、クラウドサービスモデルなど）が、戦略や事業目標の達成に与える影響を評価する。
７．リスク選好を定義する	組織は、価値の創造、維持、実現の観点からリスク選好を定義する。	組織は、データプライバシー、アクセス、信頼性、コンプライアンスおよびサイバーセキュリティなどのクラウドリスクに対応するための、クラウドガバナンスのリスク選好を定義する。
８．代替戦略を評価する	組織は、代替戦略とリスクプロファイルに対する潜在的影響を評価する。	組織は、代替クラウド戦略と事業目標への影響を検討する。
９．事業目標を組み立てる	組織は、戦略と結びつき、かつ、戦略を支える事業目標をさまざまな階層において設定する際にリスクを検討する。	組織は、事業目標を支えるために、クラウド目標を定義する。

パフォーマンス

表３．１ 『ＣＯＳＯ全社的リスクマネジメント―戦略およびパフォーマンスとの統合』―パフォーマンスの原則[12]

原則	説明
10. リスクを識別する	組織は、戦略および事業目標のパフォーマンスに影響を及ぼすリスクを識別する。
11. リスクの重大度を評価する	組織は、リスクの重大度を評価する。
12. リスクの優先順位づけをする	組織は、リスク対応選択の基礎として、リスクの優先順位づけを行う。
13. リスク対応を実施する	組織は、リスク対応を識別し、選択する。
14. ポートフォリオの視点を策定する	組織は、リスクのポートフォリオの視点を策定し、評価する。

⑩ リスクを識別する

クラウドコンピューティングのリスクは内部環境や外部環境から生じ、戦略、財務、業務、コンプライアンスおよび／または報告の目標に影響を与える可能性がある。クラウドコンピューティング戦略のパフォーマンスと達成に影響を与え、それによって事業目標の達成と価値の創造に影響を与えるリスクを識別することは非常に重要である。

組織がクラウドコンピューティングを採用する場合、１つ以上のＩＴの責任を外部に移管することになる。大部分の組織はこれらの責任を自社の中核業務として遂行する戦略的パートナーを見つけることができるため、このアプローチには大きな利点がある。しかし、これらの責任を委ねることは責任の所在を移すことではあるが、リスクを取り除くことにはならない。リスク（およびそのようなリスクを軽減するための責任）は、配置モデルによって異なる。組織が犯し得る最も一般的なリスクは、あるリスクに対する統制をどの組織が所有しているかを誤解することであると言える。統制に責任を持つ組織は、組織に対するリスクの影響度に作用する。

ガートナー社は、2025 年までにクラウドのセキュリティ障害の 99%は顧客の責任になると予測している[13]。組織はもはや、クラウドが自らにとって十分に安全かどうかを問うべきではない。より適切な質問は、「組織はクラウドを安全に利用しているか」である。

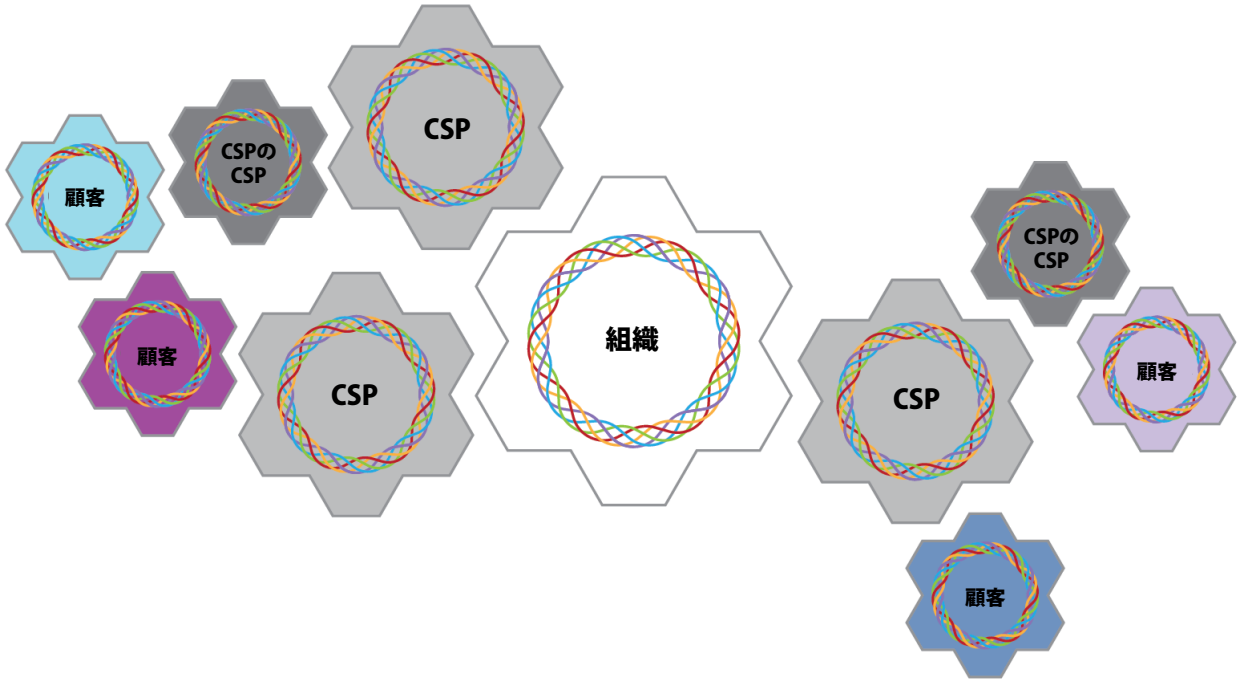
組織は一部の作業をＣＳＰに移管することはできるが、すべてのリスクを移管することはできない。例えば、ＣＳＰがパッチ適用などの合意した作業を行わず、その脆弱性が組織のデータ漏洩に悪用された場合、組織には直接落ち度がなかったとしても、顧客からの信頼失墜やデータの消失に対処する必要がある。

ＣＳＰを利用する場合、組織のリスクプロファイルは、組織のクラウドベンダーのリスクプロファイルと繋がることになる。マルチクラウド環境では、図５に示すように、複数のクラウドベンダーの利用により、ＥＲＭフレームワークが他の多くのベンダーのものと複雑に絡み合ってしまう。さらに、一部のＣＳＰはサポート用に別のＣＳＰを利用するため、さらに多くのベンダーを巻き込むことになる。多くの組織は、マルチクラウド環境を導入して複数のＣＳＰを利用している。ある組織で起きたことが、別の組織に影響を与える可能性がある。例えば、ＰａａＳでクラウドが停止すると、その基盤となるインフラにＰａａＳを利用しているＳａａＳのＣＳＰに影響が及ぶ。

12 2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*（邦訳は、『COSO 全社的リスクマネジメント―戦略およびパフォーマンスとの統合』）

13 https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

図５．戦略およびパフォーマンスと統合したＣＯＳＯ全社的リスクマネジメントのフレームワーク－組織とＣＳＰの表示付き



責任の所在の誤解

すべてのクラウド環境では、何らかの形で権限委譲が行われることが想定されている。図６に示すように、多くのクラウドサービスモデルやクラウド配置モデルでは責任が共有される。しかし、多くの組織は、自らが負う責任やＣＳＰと共有する責任を過小評価している。これは、ＩａａＳやＰａａＳのモデルを扱う場合に特に重要であるが、ＳａａＳにも当てはまる。組織は責任を移転することはできても、リスクを外部に委託することはできないことを覚えておくことが重要である。ここでは、よくある誤解の領域を浮き彫りにするための質問をいくつか紹介する。

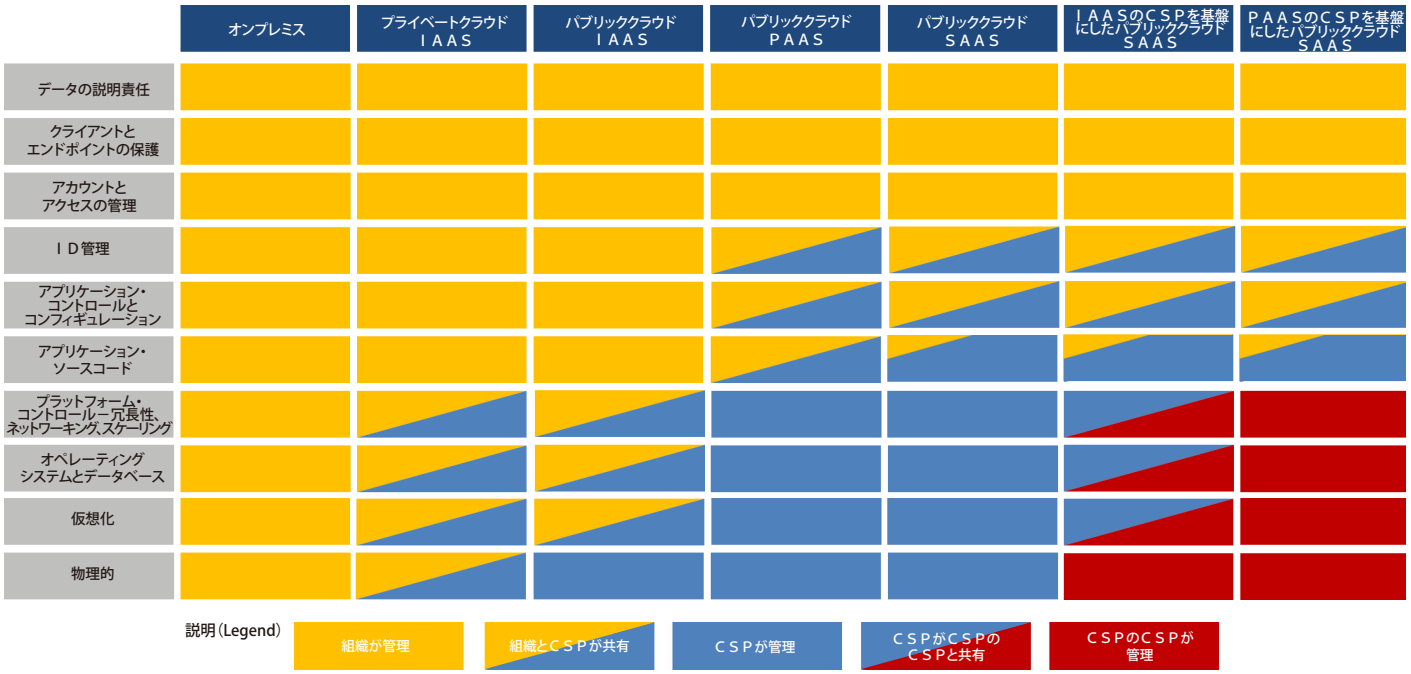
- どの部分が**マルチテナント**環境なのか。
  ある程度は、すべてのクラウド環境で共有が成り立つ。重要なのは、何が共有され、誰がその境界をコントロールするのかを理解することである。マルチテナンシーには、さまざまな意味がある。

- どのような**アクセス制御**を組織が管理するのか。
  すべてのクラウド配置モデルでは、利用する組織がある程度のアクセス制御を管理することが求められる。ファイアウォール、ＶＰＮ（仮想プライベートネットワーク）、多要素認証などの分野では、（組織とＣＳＰの間で）責任を共有することが多い。これらの機能を提供するＣＳＰは、コンフィギュレーションや実行を利用する組織に任せることが多い。

- インフラの**冗長性**は、どの程度までクラウドプロバイダによって管理されるのか。
  組織は、クラウドのあらゆる要素が予め冗長化[v]されていると過度に思い込むべきではない。ＣＳＰは確かに責任の大部分を担っているが、配置モデルによっては、その責任が別の当事者にある場合もある。

v 訳注：機器やシステムの構成要素について、同じ機能や役割の要素をあらかじめ複数用意しておき、異状が発生した時に肩代わりできるよう待機させておくこと。

図６．クラウド配置モデルとクラウドサービスモデルの責任分担



⑪ リスクの重大度を評価する
⑫ リスクの優先順位づけをする

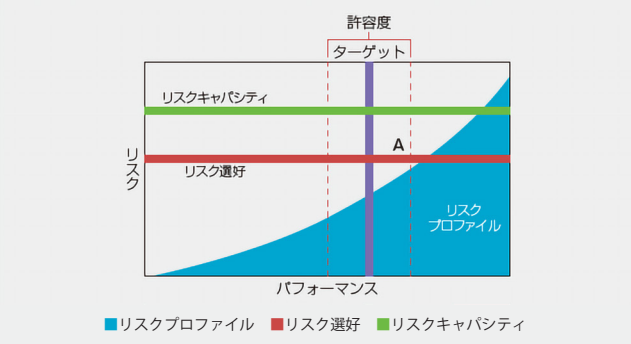
クラウドコンピューティングのリスクは、一旦識別されたら優先順位づけされ重大度が評価されるべきである。評価は定性的にも定量的にも可能であり、リスクの影響度と発生可能性を考慮すべきである。さらに、さまざまな種類のデータについて、複数の時点や組織全体にわたって評価すべきである。例えば、同じユーザアクセスというリスクでも、クラウドアプリケーションの種類や、クラウドの配置モデルやサービスモデルによって、重大度が異なる可能性がある。例えば、プライベートＩａａＳクラウドで管理するカスタム・アプリケーションの場合と、ＣＳＰによって管理され基盤となるＰａａＳのＣＳＰがそれをサポートするパブリックＳａａＳアプリケーションの場合の違いである。

特定のＣＳＰ、クラウド配置モデルおよびクラウドサービスモデルを評価する場合、組織はアプローチとベンダーを選択する前に、リスクを定義し、リスクを評価し、リスクに優先順位をつける。一旦ＣＳＰが決定されると、ＣＳＰが提示する特定のリスクとシナリオに対処するために、適切なリスク対応が策定される。リスク対応には、受容、回避、活用、低減および共有などがある。

⑬ リスク対応を実施する

リスク対応は、残余リスクを評価し、組織がリスク選好とリスクキャパシティー内のどこに位置するかを判断するために実施され評価される。図７に示すように、ゴールはリスクの許容度の範囲内に収まることである。

図７．COSO ERM－リスクプロファイル



出典：2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*（邦訳は、『COSO 全社的リスクマネジメント－戦略およびパフォーマンスとの統合』）

主なリスク対応は５つあるが、クラウドコンピューティングの場合は低減が中心となる。

- **受容**ークラウドコンピューティングのリスクを受容することは、他のクラウド利用者のリスクプロファイルを受容するなど、組織が制約を感じるような特定のシナリオでは可能である。組織はこれを自らのリスク許容度の閾値に照らして評価しなければならない。

- **回避**ー一般に、回避が有効なのは、特定のデータプライバシー要件に対応するために国際的なＰａａＳではなく国内のＰａａＳを選択する場合、知的財産など特定の種類のデータをパブリッククラウドに置けないと判断する場合、完全なプライベートクラウドソリューションを導入する場合など、特定の状況においてのみである。このようなシナリオの場合でも、さらなるリスクが発生する可能性があり、低減と緩和に取り組む必要がある。

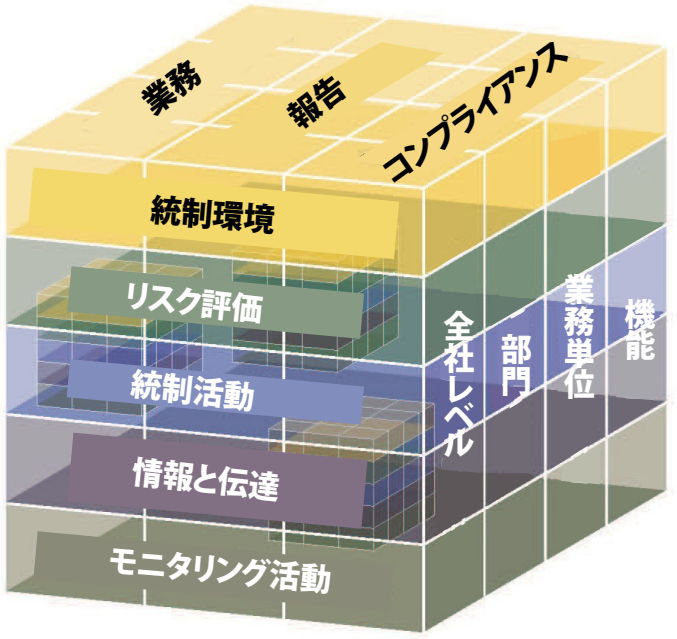
- **活用**ークラウドに移行する場合、組織がイノベーションとデジタルトランスフォーメーションをさらに進め、効率性を高めることが可能になるため、組織の価値を創造、維持および実現する新たな機会が頻繁に生じる。

- **低減**ークラウドガバナンスとモニタリングの統制を追加することで、リスクを低減することができる。これは、テクノロジーの固有リスクと、クラウドコンピューティングやＣＳＰへの外部委託によって組織にもたらされる追加リスクを軽減するための、クラウドコンピューティングに対する最も一般的なリスク対応である。

- **共有**ー共有がクラウドコンピューティングに適した対応となるには限界がある。サイバー侵害のように、サイバー保険に加入してリスクを共有することである程度対応できるリスクも少しはある。しかし、クラウドコンピューティングの主なリスクは共有することができない。

2013 年版ＣＯＳＯ『内部統制の統合的フレームワーク』の活用は、クラウドコンピューティングのリスク低減対応を構築して展開するための１つのアプローチである。また、図８に示すように、組織の内部統制フレームワークとＣＳＰの内部統制フレームワークの統合を認識することが重要である。（より大きいキューブ内のキューブで表されている）ＣＳＰの内部統制は、（より大きいキューブで表されている）組織の内部統制の一部となる。すべてのクラウドサービスモデルにおいて、プロセスと統制の一部がＣＳＰに委託される。組織はそれらの内部統制の実施をＣＳＰに委ねる。組織はＣＳＰの統制の設計がリスクに適切に対処していることを理解してレビューする必要があり、また、統制の効果的な実施をモニタリングする必要がある。

図８．2013 年版ＣＯＳＯ『内部統制の統合的フレームワーク』[14] ー組織とＣＳＰを結びつけた視点



『ＣＯＳＯ 全社的リスクマネジメントー戦略およびパフォーマンスとの統合』のパフォーマンスの構成要素は、リスク対応に焦点を当てている。以下は、典型的なクラウドコンピューティングのリスクに対して推奨されるいくつかの対応を詳しく説明したものである。

14 2013 *COSO Internal Control – Integrated Framework*（邦訳は、『内部統制の統合的フレームワーク』）（訳注：原文では「18」となっているが、前の注の番号に続けて「14」とした。以後の番号もこれに合わせた。）

リスク－信頼性と脆弱性

対応

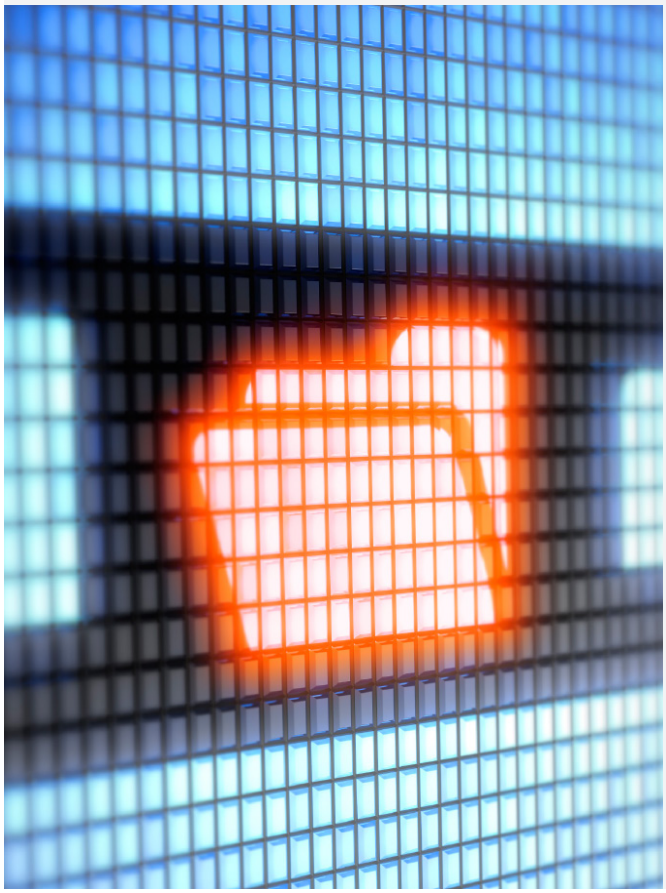
パフォーマンスのモニタリング、セキュリティのモニタリングおよびインシデント対応

組織はまず、信頼性の高いＣＳＰとの提携を模索すべきである。次に、組織はＣＳＰのパフォーマンスと稼働時間をモニタリングする必要がある。

大部分のクラウドサービスモデルでは、ＣＳＰがインフラの管理を行い、セキュリティ評価と脆弱性評価を実施するはずである。これらの評価結果やＣＳＰがどのように問題に対応して修復するかは、組織に共有され、組織がモニタリングすべきである。

ＣＳＰは、自社で発生したインシデントを特定するための適切なインシデント対応を整備すべきである。さらに、ＣＳＰは、組織がＣＳＰにインシデントを報告するためのプロセスと、組織がインシデントの進捗を追跡するためのプロセスを整備すべきである。アプリケーションとサービスの管理は連動しているため、インシデント対応も連動すべきである。

リスク－マルチテナンシー、データ漏洩およびデータ盗難



対応

データの分類、データの破棄およびセキュリティ

パブリッククラウドやマルチテナンシーの場合、データの盗難や漏えいのリスクがより高くなる。組織は、クラウド上に置いた場合にどのようなデータが適切に保護されるかを徹底的に評価すべきである。データのリスクを分類して評価するデータ分類の作業を行うことで、（どのようなアプリケーションとともに）どのようなデータをどのような種類のクラウド配置モデルやクラウドサービスモデルに置くべきかというパラメータが定義できる。組織はデータをどの程度管理したいかを評価すべきである。

組織はデータの分類方針だけでなく、データの破棄方針も実施すべきである。こうすることで、組織は過剰なデータや古くなった可能性のあるデータをクラウドに残さなくなる。分析のために個人データをクラウドに保管すると、データが通知要件から外されてしまい、組織が個人データを明示された許可の範囲外で使用できるようになり、プライバシー規則に違反する可能性がある。

データ周りのセキュリティは、セキュアアクセスサービスエッジ（ＳＡＳＥ）ソリューションの導入により得ることができる。ＳＡＳＥには、セキュアウェブゲートウェイ、ＣＡＳＢ（クラウドアクセスセキュリティブローカー）、高度な脅威防御、ゼロトラストネットワークアクセスなどのネットワークとセキュリティの要素が含まれている。ＳＡＳＥには、オンプレミスやリモートのユーザとデバイスがクラウドに接続する際に、組織のセキュリティ方針を適用するための、接続性とセキュリティの層を提供するネットワークセキュリティの仕組みが含まれている。

リスク－単一障害点

対応

冗長性、事業継続計画およびインシデント対応

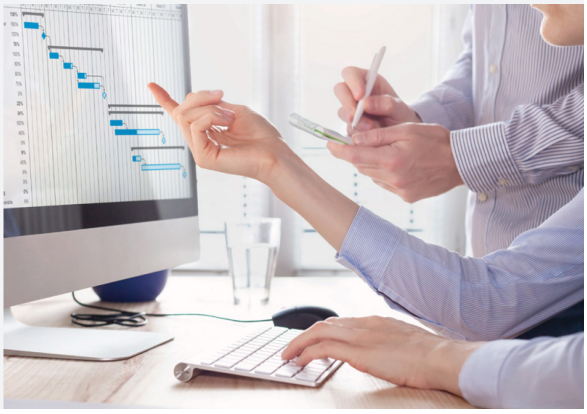
クラウドコンピューティング環境では、すべてのデータとトランザクションがインターネットを経由する必要があるため、接続に単一障害点が存在することになる。組織は必要に応じてトラフィックを迂回できるように、クラウドコンピューティング環境でどのような冗長性オプションが利用可能かを検討すべきである。クラウドツールを導入する場合、組織は障害を想定した設計を行うべきである。さらに、組織は短期的および中期的な回避策を含む事業継続計画を策定すべきである。

一般的なシステム信頼性のリスクと同様に、インシデント対応プロセスはオンライン復旧に不可欠である。

リスク－コンプライアンス

対応

内部環境、外部環境およびベンダーのモニタリング



規制は進化し、組織は時とともに変化する。したがって、組織のコンプライアンスのニーズも変化する。組織は内部環境をモニタリングし、組織が行った変更とコンプライアンス要件への影響を理解する必要がある。同様に、組織は外部環境をモニタリングし、追加または変化するコンプライアンス要件を評価する必要がある。

さらに、組織はＣＳＰベンダーをモニタリングして、ＣＳＰのコンプライアンス能力を評価し、コンプライアンスに対応するために組織が行わなければならない追加の手順がある場合には、それを評価する必要がある。

リスク－サイバー攻撃

対応

インシデント管理

クラウドコンピューティングに対するサイバーセキュリティの脅威には、多くの種類がある。最も一般的なものは、マルウェアの侵入、サービス妨害（ＤｏＳ）、ＡＰＩvi攻撃および不正アクセスによる乗っ取りなどである。また、オープンソーステクノロジーを使用することで、脆弱性が一般に知られるようになり、サイバー攻撃へのリスクが高まる可能性がある。サイバーセキュリティはオンプレミスとクラウドの両方に存在するリスクであるが、マルチテナンシーによる更なるリスクも存在する。マルチテナントモデルは、組織をより価値の高いターゲットにする可能性がある。

組織はＣＳＰが潜在的な脅威をモニタリングして検知し、どのように対策を講じるかについて、そのプロセスを理解する必要がある。さらに、組織はインシデントをＣＳＰに通知し、ＣＳＰと共にインシデントを管理する仕組みが必要である。

vi 訳注：「Application Programming Interface」の略で、あるソフトウェアが持つ機能を共有するための仕組み。

リスクーシャドーＩＴ

対応

方針と手続およびセキュリティ対策ツール

クラウドコンピューティングのサービスやベンダーはどのようなものが許されるのか、誰がサービスを調達できるのか、どのようなデータをクラウドに移行できるのかについて、従業員への期待を定める方針と手続によって、未承認のクラウドアクティビティを減らすためのフレームワークが提供できる。

さらに、ファイアウォール、プロキシサーバおよびウェブフィルタを使用することで、組織内で使用されるシャドーＩＴの量がさらに減らせる。これらの設定は、新しいソフトウェアやウェブサイトがリリースされたときにも有効であるように、常に維持して適用する必要がある。また、組織はデータ損失防止ツールを使用して、データが組織の外に出ないようにモニタリングと制限も行える。

表３．２は、一般的なクラウドコンピューティングのリスクと、考えられるリスク対応をまとめたものである。この表は一般的なリスクと対応を示しているものの、すべてのクラウドコンピューティングリスクを完全に網羅しているわけではない。

表３．２　**一般的なクラウドコンピューティングのリスクとリスク対応**

クラウドコンピューティングのリスク	クラウドコンピューティングのリスク対応
信頼性と脆弱性	• ベンダーデューデリジェンスプロセス • パフォーマンスモニタリングプロセス • セキュリティモニタリングプロセス • インシデント対応プロセス
マルチテナンシー、データ漏洩、データ盗難	• データ分類方針 • データ破棄方針 • セキュリティプロセス
単一障害点	• データの冗長性 • 事業継続方針 • インシデント対応プロセス
コンプライアンス	• 外部環境モニタリングプロセス • 内部環境モニタリングプロセス • ベンダーモニタリングプロセス
サイバー攻撃	• インシデント管理プロセス
シャドーＩＴ	• クラウドコンピューティング方針 • データ損失防止プロセス • セキュリティモニタリングプロセス

14 ポートフォリオの視点を策定する

クラウドコンピューティングは事業戦略を支える全体的なＩＴ戦略の一部であるため、リスクに対するポートフォリオの視点を策定する必要がある。これには、パブリック、プライベートおよびハイブリッドのクラウドモデルにおけるリスクと、さまざまなＣＳＰベンダーの利用が、組織を支えるＩＴ環境全体の一部であるクラウド戦略全体にどのように影響するかを評価することが含まれる。また、ビジネスプロセス内のクラウドコンピューティングをレビューし、その利用が事業部門にどのような影響を与えるかを確認することも含まれ、これはさまざまな可能性がある。例えば、ＥＲＰの事業継続性に関するリスクが財務部門に与える影響（報告や支払いが遅れる可能性）は、製造現場に与える影響（製造が中断する可能性）とは大きく異なる。

クラウドコンピューティングのリスクを考える際には、サイバーセキュリティのリスクを考慮すべきである。サイバー脅威は、他のＥＲＭリスクと総合的に検討すべきである。例えば、財務計画・分析部門が使用している予測ツールへのサイバー侵害と、同部門が使用している財務データウェアハウスへのサイバー侵害では、サイバーリスクの影響が異なる可能性があることも留意すべき点である。サイバーセキュリティリスクに対するポートフォリオの視点を評価する際には、組織のクラウドコンピューティングの利用状況をデータ分類方針と照らし合わせて検討すべきである。

組織がクラウドコンピューティングのリスクを検討する際には、さまざまな視点や部門および関連するすべてのクラウドシステムから総合的に検討すべきである。これらの全体的なリスクは、戦略、財務、業務、コンプライアンスおよび報告の目標の観点から検討すべきであり、ＥＲＭリスクポートフォリオ全体の中に組み込むべきである。

表３．３　**クラウドコンピューティングのための主要な活動―パフォーマンスの原則**

原則	説明	クラウドコンピューティングＥＲＭの主要な活動
10. リスクを識別する	組織は、戦略および事業目標のパフォーマンスに影響を及ぼすリスクを識別する。	組織は、クラウドコンピューティングのリスクを識別するために、内部環境と（業界、ＣＳＰおよびＣＳＰのベンダーを含む）外部環境を評価する。
11. リスクの重大度を評価する	組織は、リスクの重大度を評価する。	組織は、組織全体のクラウドコンピューティングのリスクを評価する際に、リスクの影響度とリスクの発生可能性を考慮する。
12. リスクの優先順位づけをする	組織は、リスク対応選択の基礎として、リスクの優先順位づけを行う。	組織は、クラウドコンピューティングのリスクに対応するために、リスクとリスク対応の優先順位づけを行う。
13. リスク対応を実施する	組織は、リスク対応を識別し、選択する。	組織は、リスク対応を実施するためのプロセスと統制を設計する。
14. ポートフォリオの視点を策定する	組織は、リスクのポートフォリオの視点を策定し、評価する。	組織は、クラウドコンピューティングのリスクを、戦略、財務、業務、コンプライアンスおよび報告の目標に対するリスクとして総合的に捉える。

レビューと修正

表４．１ 『ＣＯＳＯ 全社的リスクマネジメント―戦略およびパフォーマンスとの統合』―レビューと修正の原則[15]

原則	説明
15. 重大な変化を評価する	組織は、戦略や事業目標に重大な影響を与え得る変化を認識し、評価する。
16. リスクとパフォーマンスをレビューする	組織は、事業体のパフォーマンスの結果をレビューし、リスクを考慮する。
17. 全社的リスクマネジメントの改善を追求する	組織は、全社的リスクマネジメントの改善を追求する。

15 重大な変化を評価する

ＥＲＭは継続的で反復的なプロセスである。ＥＲＭは孤立して実施され棚上げされるものではなく、同様に、毎年取り出して更新し、更新時以外は無視されるものでもない。ＥＲＭは組織の業務方法に組み込まれるべきものである。

ＥＲＭは環境、組織またはＣＳＰに重大な変化がある場合は常に更新されるべきであり、また、クラウドベースのサービスの導入と統合に関する決定は、重大な変更に該当するか、それを促す可能性がある。経営者は日常的にリスクを評価し、リスクが組織のリスク選好を超える可能性がある状況を特定する責任がある。2020 年は、新型コロナウイルス感染症のパンデミックによる変化もこれに含まれていた。多くの組織が、リモートワークの推進を急いだ。多くの場合、これには従業員がテクノロジーに接して事務所以外の場所で効率的に業務を遂行できるようにするための、クラウドコンピューティングアプリケーションの拡張が含まれていた。また、組織が事業を展開する地理的な場所の追加も、実質的な変化として考えられる。組織が提携するＣＳＰは、遅延への対応や災害復旧に適切な対応をするために変更が必要になるかもしれないし、取り組みを支援するＣＳＰを追加する必要があるかもしれない。

前章で述べたように、規制やコンプライアンス環境における外部の変化もクラウドコンピューティングに影響を与える可能性があり、モニタリングすべきである。例えば、シンガポールでは 2021 年２月から改正個人情報保護法が施行される予定で、データ侵害の通知に関する要件が盛り込まれている。

クラウドコンピューティングのテクノロジーは絶えず進歩している。これらの進歩により、クラウドのセキュリティと移行に新たな選択肢が加わり、組織はこれらが事業目標や組織の付加価値を生み出す能力にどのような影響を及ぼすか、日常的に評価する必要がある。

その他にも、合併、買収および事業売却など、社内の大きな変化があり得る。組織は売却の際に移行サービス契約を結ぶことがよくあるが、クラウドの契約やアクセスなどの管理に、また別の複雑さが加わる可能性がある。

経営者は自社のカルチャーについても評価して判断すべきである。新型コロナウイルス感染症のパンデミックで見られたように、リモートワークは多くの組織のカルチャーを変えた。

15 2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*（邦訳は、『COSO 全社的リスクマネジメント－戦略およびパフォーマンスとの統合』）

16 リスクとパフォーマンスをレビューする

クラウドコンピューティングのガバナンスプロセスは、改善点を特定するためにレビューしなければならない。クラウドコンピューティングのガバナンスプロセス強化には、バランススコアカードの利用が考えられる。クラウドベンダーは、通常、可用性を含むサービスレベル合意書に照らして評価しなければならない。クラウド契約は継続や自動更新の前に常にレビューすべきである。ベンダーは監査すべきであり、そうでなければＳＯＣ（システムおよび組織統制）報告書を取得してレビューすべきである。組織はＣＳＰに変化があるかも評価すべきである。侵害などの重大な項目は、たとえそれが組織に影響を及ぼさなかったとしても、当面の事業目標を達成する組織の能力に影響を及ぼす可能性がある。ベンダーを評価した結果、組織のリスク選好よりも高いリスクが生じる状況が発生することがある。そのような場合、組織はリスクをレビューし、リスクに対処するために適切な措置を講じる必要がある。さらに、組織が維持し実施する統制についても、その遵守状況をレビューすべきである。統制のパフォーマンスのレビューは、経営者、コンプライアンスまたは内部監査が行う場合がある。

クラウドコンピューティングとクラウドガバナンスのプロセスは、組織の全階層に組み込まれ、明確な役割分担のもとで運用されるべきである。クラウドコンピューティングガバナンスは組織の一部だけで行うべきではなく、組織全体が一体となって取り組むべきである。リスクは、統制実施後の実際の残余リスクがリスク許容度内にあることを確認するためにレビューされるべきである。その結果はＥＲＭプロセス全体に組み込むべきである。

17 全社的リスクマネジメントの改善を追求する

クラウドガバナンスとサプライヤー管理の一環としてクラウドベンダーのパフォーマンスをレビューするだけでなく、クラウドコンピューティングのプロセスについてもパフォーマンスをレビューしなければならない。組織はリスクとパフォーマンスのレビューを利用して、クラウドガバナンスのプログラム、プロセスおよび統制を更新すべきである。さらに、組織はクラウドガバナンスとクラウドプロセスが、組織のＥＲＭプロセス全体にどのように反映されているかを確認すべきである。組織はクラウドガバナンスプログラムにおける部門間の協力のレベルを評価し、更新を伴うＥＲＭプロセスの改善を図るべきである。また、組織はＥＲＭプロセスのアウトプットを活用し、更新とアウトプットをクラウドガバナンスプログラムに適用すべきである。

表４．２　**クラウドコンピューティングのための主要な活動―レビューと修正の原則**

原則	説明	クラウドコンピューティングＥＲＭの主要な活動
15. 重大な変化を評価する	組織は、戦略や事業目標に重大な影響を与え得る変化を認識し、評価する。	組織は、内部および外部の変化と事業戦略や事業目標への影響、それらがクラウドコンピューティング戦略に与える影響、あるいは、クラウドコンピューティングがその変化を実現するための効果的なインフラをどのように提供できるかを評価する。
16. リスクとパフォーマンスをレビューする	組織は、事業体のパフォーマンスの結果をレビューし、リスクを考慮する。	組織は、クラウドガバナンスプログラムをレビューする。また、ＣＳＰやクラウドリスクをレビューするために、クラウドガバナンス活動を行う。
17. 全社的リスクマネジメントの改善を追求する	組織は、全社的リスクマネジメントの改善を追求する。	クラウドプログラムを評価し、組織のＥＲＭプログラム全体に適用すべき改善点を追求する。

情報、伝達および報告

表５．１　『ＣＯＳＯ全社的リスクマネジメント―戦略およびパフォーマンスとの統合』―情報、伝達および報告の原則[16]

原則	説明
18. 情報とテクノロジーを有効活用する	組織は、全社的リスクマネジメントをサポートするために、事業体の情報とテクノロジーシステムを有効活用する。
19. リスク情報を伝達する	組織は、全社的リスクマネジメントをサポートするために、コミュニケーション経路を利用する。
20. リスク、カルチャーおよびパフォーマンスについて報告する	組織は、リスク、カルチャーおよびパフォーマンスを複数の階層に、また、全社にわたって報告する。

18 情報とテクノロジーを有効活用する

組織はクラウドコンピューティングのリスクを識別し、伝達し、対応し、管理するＥＲＭ機能を支援するために、テクノロジーを活用すべきである。クラウドガバナンスをモニタリングするための情報は、モニタリングアプリケーション、内部監査のテストと評価、ベンダー管理システムおよびガバナンスとコンプライアンスのツールなど、さまざまなソースから得ることができる。

組織の財務的健全性を評価する金融格付け機関に加え、データを収集し、ウェブサイト、ベンダーまたはＣＳＰのセキュリティー・スコアを提供するＩＴセキュリティ組織も複数存在する。これらのセキュリティ格付けは、ＣＳＰのセキュリティに対する姿勢に関する洞察を提供する。また、ベンダーの評価に含まれる評判リスクを評価する組織もある。これらのツールは、クラウドインフラとサービスの状態（パフォーマンスや可用性など）を評価する他のクラウドモニタリングツールとともに、クラウドコンピューティングの管理に利用できる。これらの外部ツールは、クラウドコンピューティングのガバナンスプログラムに影響を与え得る新たな情報を取得するために使用すべきである。

一部のテクノロジーは、組織が利用するためにＣＳＰから提供される場合がある。また、ＣＳＰは組織に対する責任の遂行に関する情報を収集し共有するために、テクノロジーツールを活用する場合もある。

19 リスク情報を伝達する

優れたガバナンスの重要な要素は、明確な伝達と報告である。適切な者に最新の情報が提供されなければ、適切な意思決定は行えない。情報はクラウドコンピューティングのガバナンスプログラムのすべての関連する役割間で報告され、透明であるべきである。オープンなコミュニケーションとデータの共有により、全関係者がリスクへの最新の影響とリスクへの対応を認識できる。また、全部門が参加して説明責任を果たすことで、組織内で共有された総体的なリスクマネジメントのカルチャーが促進される。

クラウドコンピューティングが組織内で採用されるにつれて、個人の役割と責任は変化する。アプリケーションやプロセスによる責任の変更は、従業員に伝達すべきである。組織は複数のコミュニケーション経路を通じて、リスクを認識するカルチャーを継続的に強化すべきである。組織はクラウドガバナンスプログラムがＥＲＭプログラム全体の一部であることを伝え、各従業員の役割を確実に理解させるべきである。

クラウドコンピューティング運営委員会は、クラウドへの移行や継続的なクラウドコンピューティングのパフォーマンスについて最新情報を入手すべきである。

16 2017 *COSO Enterprise Risk Management – Integrating with Strategy and Performance*（邦訳は、『COSO 全社的リスクマネジメント－戦略およびパフォーマンスとの統合』）

組織とＣＳＰの間には、明確なコミュニケーション経路が存在すべきである。これらは、問題の上申や、定期的な情報更新およびベンダーとその関係管理に必要である。

20 リスク、カルチャーおよびパフォーマンスについて報告する

取締役会は、クラウド戦略とそれが事業目標に与える影響について、最新情報を入手すべきである。また、組織はクラウドコンピューティングのパフォーマンスについて報告するとともに、カルチャーの変革管理とリスクカルチャーに関する進捗を組織全体に伝えるべきである。組織内のカルチャーを変えるには時間がかかる。オープンで透明性の高いコミュニケーションは、組織に必要な協力的なカルチャーを生み出すのに役立つ。一貫したメッセージが提供され、進捗と変化が組織全体で理解されるためには、組織の全階層で報告が入手できるようにすべきである。

各部門の異なる階層は、異なる最新情報を取締役会に伝達する必要がある。例えば、第１ラインである経営者は、クラウド戦略や事業目標の変更を伝えるべきである。第２ラインの一部であるコンプライアンスは、ＣＳＰのモニタリングとリスクを報告すべきである。内部監査は第３ラインとして、第１ラインと第２ラインで対応されなかったリスクに関する問題の伝達を含め、組織のクラウドコンピューティングと活動について、独立的かつ客観的に報告すべきである。

表５．２ **クラウドコンピューティングのための主要な活動―情報、伝達および報告の原則**

原則	説明	クラウドコンピューティングＥＲＭの主要な活動
18. 情報とテクノロジーを有効活用する	組織は、全社的リスクマネジメントをサポートするために、事業体の情報とテクノロジーシステムを有効活用する。	組織は、全社的リスクマネジメントをサポートするために、クラウドコンピューティングの情報とテクノロジーデータを活用し、統合するための利用可能なプラットフォームを追加し、適宜導入する。
19. リスク情報を伝達する	組織は、全社的リスクマネジメントをサポートするために、コミュニケーション経路を利用する。	組織は、全社的リスクマネジメントをサポートするために、クラウドコンピューティングに関わるあらゆる人とのコミュニケーション経路を利用する。
20. リスク、カルチャーおよびパフォーマンスについて報告する	組織は、リスク、カルチャーおよびパフォーマンスを複数の階層に、また、全社にわたって報告する。	組織は、クラウドコンピューティングのリスクとパフォーマンスを、複数の階層と組織全体にわたって報告する。

結論

クラウドコンピューティングは、組織が利用できる多くのテクノロジーの選択肢の１つである。関連するリスクに対処し、ＥＲＭプログラムに組み込まれた、総体的なクラウドコンピューティングガバナンスプログラムを含むクラウドコンピューティングを体系的に導入すると、組織は最も価値を引き出し、その戦略目標の達成を可能にする。

組織が競争力を維持するためには、ＩＴ戦略を駆使して事業を強化する必要がある。クラウドコンピューティングをＩＴ戦略に統合し、ＩＴ組織を戦略的パートナーにすることで、組織の成功に必要な多くのツールやフレームワークが提供できる。

クラウドコンピューティングのリスクは、組織の広範なＥＲＭプログラムとの関連で識別して管理しなければならない。タスク、プロセスおよび保守は外部委託できるが、リスクに対する説明責任は委託できない。リスクの所有権は組織にとどまるので、組織は組織内とＣＳＰの内部統制をモニタリングする必要がある。

クラウドを安全に利用するために、組織はさまざまなセキュリティツールに投資して導入すべきである。組織は利用可能なテクノロジーを活用して、クラウドコンピューティングのテクノロジー、ベンダーおよびＥＲＭプログラムをモニタリングし、報告し、評価の更新を継続的に行う必要がある。また、上級経営者と統治機関は内部監査部門が独立したアシュアランスと助言を提供するために、リスクベースの計画プロセスにクラウドベースのサービスを組み込んでいることも確認すべきである。

ＥＲＭフレームワークを導入せずにクラウドコンピューティングへの道を既に歩んでいる組織でも、クラウドガバナンスをプロセスに追加することは可能であり、また、そうすべきである。クラウドガバナンスのプロセスは、事業戦略、ＩＴ戦略およびクラウドコンピューティングに関連する継続的な活動に組み込まれるべきであるため、クラウドガバナンスは継続的に更新して新たな情報に基づいて改訂すべきである。組織がクラウドガバナンスプログラムを作成していない場合は、いつでも作成することができ、変更が生じた場合は継続的に更新できる。組織のクラウドコンピューティングプロセスにクラウドガバナンスを組み込むことで、組織は組織の戦略と目標を脅かすリスクを管理しやすくなる。

『ＣＯＳＯ 全社的リスクマネジメント－戦略およびパフォーマンスとの統合』のフレームワークを使用することで、クラウドコンピューティングを組織のＥＲＭ機能に統合できる。クラウドコンピューティングのガバナンスアプローチでは、組織全体を通したクラウドコンピューティングの全体像が把握できる。ガバナンスと伝達および報告は、クラウド戦略、パフォーマンスおよびモニタリングと修正に密接に結びついている。これは、クラウドコンピューティングの導入により、ＣＳＰのクラウドコンピューティングガバナンスプロセスと組織のガバナンスプロセスを融合させることを目的として実施される。

付録A.
クラウドコンピューティングへの行程

クラウドの導入戦略を計画することは、方法論的なプロセスである。この付録Aでは、従来のオンプレミスのワークロードをクラウドコンピューティングに移行するための検討事項を説明する。主にＩａａＳとＰａａＳに焦点を当てる。

この行程は、組織がクラウドの旅を始めるにあたって、ガバナンスと戦略が十分に考慮されている理想的な状態を表している。しかし、状況や組織の焦点は変化するため、クラウド戦略も同様に変化させる必要があり得る。クラウドコンピューティングガバナンスは、必要に応じて再評価し、取り組みを方向転換するためのチェックポイントとして、プロセスのさまざまな段階で遡及的に追加することができる。

段階的アプローチ

クラウド移行を成功させるための４つの基本的な段階を以下に示す。段階的なクラウド移行アプローチには、ＣＯＳＯＥＲＭフレームワークの構成要素をいつ組み込むかが織り込まれている。

クラウド移行を開始する際は、ＩＴ環境の詳細な評価に先立ち、組織はクラウドの**ガバナンスとカルチャー**を定義すべきである。クラウドコンピューティング運営委員会は、監督を行い、責任マトリクスを構築することができる。一旦監督体制が確立されると、組織はＥＲＭの**戦略と目標設定**の際に、組織全体のミッションと戦略目標に関連したクラウド戦略が定義できる。

評価

この段階では、組織はＩＴポートフォリオを評価し、インフラの発見とアプリケーションの合理化を行う。インフラの発見を評価する間、「現状の」インフラ状況を分析し、サーバ構成、使用率パラメータ、ネットワークセグメンテーション、ストレージ割り当ておよび依存関係などの詳細を収集する。

アプリケーションの合理化プロセスでは、アプリケーションは、アプリケーションの複雑性、（将来のビジネストレンドを含む）重要性および依存関係などの要因によってグループ化される。各アプリケーションには、移行段階で従うべき移行経路が割り当てられる。総所有コスト（ＴＣＯ）分析が行われ、「現状」のコストとクラウドで「実現すべき」コストが比較される。通常、この段階では、組織はクラウドへの行程を成功させるためのチームを特定して移行計画を作成する。一般に、クラウドは使用量に応じたストレージとコンピューティングパワーのみを支払い、コストを（資産化された費用ではなく）業務費用に振り向けることでコスト削減を実現する。

移行経路が確定した時点は、ＥＲＭフレームワークのパフォーマンスの構成要素を使用して、クラウドの**パフォーマンス**をレビューする良い機会である。クラウドに対するリスクを識別して軽減策を講じるべきである。

構築

この段階では、組織はスケール、セキュリティ、ガバナンス、ネットワーキングおよびアイデンティティを考慮したクラウド環境を整備するための基盤が構築できる。これはランディングゾーンと呼ばれている。基盤の計画が不十分であると、組織は遅延、混乱およびダウンタイムに直面し、クラウド移行の成功が危ぶまれる。クラウドランディングゾーンを設定する目的は、開発、テスト、配置、モニタリングおよび保守のための基盤を構築することである。ランディングゾーンを定義する際には、ガバナンス、管理およびサブスクリプションが確立される。ネットワーク、計算、ストレージ、データベース、管理、モニタリング、セキュリティ、継続的統合と継続的開発（ＣＩＣＤ）、アプリケーション移行およびアナリティクス機能が確立される。変革の推進、ガバナンスの確立、クラウドの中核的研究拠点の設立、あらゆるレベルのセキュリティの定義、コンプライアンスの履行、方針の設計、アーキテクチャの定義および変革のための詳細計画（人、プロセス、テクノロジー）のためのリソースにアクティビティが割り当てられる。

移行

この段階では、アプリケーションとワークロードは評価段階で定義された移行経路に従って、クラウドのランディングゾーンに移行される。組織のアプリケーションポートフォリオの規模にもよるが、クラウドへの移行はワークロードを移行するための反復プロセスである。これらの反復は基本的に、評価段階で移行計画に定義された依存関係マトリクスとビジネスの優先順位に基づいて、異なる波や移動グループとなる。

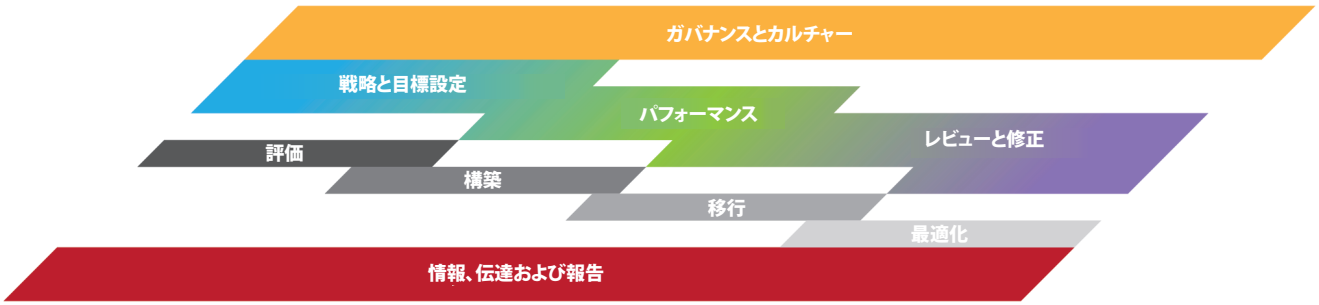
クラウドの設定と拡張に伴い、環境や組織の変化を評価するために、クラウドガバナンスの**継続的なレビューと修正**をすべきである。

最適化

組織の成熟度に応じて、クラウド環境の基盤を確立するためのランディングゾーンの設定は、小規模から始めて拡張することができる。成熟した組織は通常、全社的な規模で開始する。最適化の段階では、クラウド環境をより効率的にするための改良が行われる。これは環境の進化に伴う継続的かつ連続的なプロセスである。

クラウドの業務が開始されたら、組織はクラウドをＥＲＭの**情報、伝達および報告**に活用すべきである。これにより、組織はクラウドとＣＳＰについて報告できるようになる。

図９[vii]．クラウドへの行程にはＣＯＳＯ ＥＲＭフレームワークを含めるべきである



戦術的な移行戦略

ワークロードをクラウドに移行するためには、６つの異なる移行経路があり、それぞれにリスクが伴う。これは６Ｒ手法とも呼ばれている。これらの移行経路は、クラウド移行の評価段階で決められる。クラウド移行は、主に後述する「Ｒ」のいずれかのアプローチを採用して行われる。

保持（Retain）

このアプローチは、組織がワークロード全体をクラウドに移行する準備ができていないハイブリッドのＩＴ環境に適用される傾向がある。これは通常、組織が完全な移行に臨む準備が整うまで、オンプレミスのワークロードの一部を「保持」する一時的なアプローチである。クラウドへの移行は長期にわたるプロジェクトになる可能性があり、オンプレミスのサービスを一時的に（または永久に）保持することが含まれる場合がある。

リホスト（Rehost）

これは、クラウドへの移行で最も簡単な方法である。このアプローチでは、組織の現在のサーバとワークロードを、ソフトウェアやプラットフォームに一切変更を加えることなく、目的のクラウド環境に移行することができる。多くの移行では、ワークロードを単純にリホストできるものもあれば、より複雑なアプローチを必要とするものもある。これは、リフト＆シフトと呼ばれることがよくある。

リプラットフォーム（Replatform）

ワークロードによっては、それが動作するプラットフォームの変更が必要になる場合がある。これには、ソフトウェアが動作するオペレーティングシステムの変更や、新しいデータベースエンジンへのデータ転送が必要になる場合がある。ワークロードによっては、クラウドプラットフォームに直接移行できるものもあるが、リプラットフォームが必要なものもある。

vii 訳注：原文では「Diagram 10」となっているが、原文には「Diagram 9」に相当する図がないため、この図を「図９」とした。

再購入（Repurchase）

このアプローチは、製品を完全に切り替える選択肢であり、通常はＳａａＳアプリケーションに切り替える。このアプローチは通常、オンプレミスで稼働しているサードパーティ製品で、同じ製品のクラウド版にライセンスを移植できないもの（例えば、商用オフザシェルフ（ＣＯＴＳ）[viii]アプリケーションなど）に適用される。

リファクタリング（Refactor）

クラウドネイティブ[ix]のサービスを十分に活用するためには、ワークロードのアーキテクチャを変更する必要がある場合が多い。リファクタリングには、組織がクラウドのリソースを最大限に活用できるように、コンテナ化するためにソフトウェアを再構築して、組織のソリューションを変更することが含まれる場合がある。古いモノリシック[x]なソフトウェアソリューションは、クラウドにうまく対応できない可能性があり、リファクタリングが有効な場合がある。ソフトウェアのリファクタリングには、最終的なソリューションのリプラットフォームもある程度必要な場合がある。

廃止（Retire）

このアプローチは、クラウド移行の評価段階において移行計画の中で廃止することが確認された資産やアプリケーションに対して行われる。これには既にクラウドへの移行が完了したワークロードや、クラウド環境では不要となったソリューションが含まれる場合がある。

以下の表で、主な移行アプローチのリスクと利点を紹介する。

表６．１　**戦術的なクラウド移行アプローチのリスクと利点**

アプローチ	利点	リスク
リホスト	• 移行速度の向上 • 移行に伴うリスクの低減 • この移行アプローチをネイティブにサポートするツールのＣＳＰとパートナーのエコシステム • 自動化やツールによる支援も可能	• ＰａａＳサービスを使用しない可能性 • 同じ性能特性を受け継ぐ可能性 • テクノロジー負債の解消は限定的
リプラットフォーム	• コード変更なしでクラウドサービスを利用 • 物理的なハードウェアプラットフォームへの依存がない • 新しいプラットフォームへの移行 • テクノロジースタック[xi]を最新化する機会 • 場合によっては自動化ツールの利用が可能	• 移行に時間とコストがかかる可能性 • 追加の計画や調整が必要
再購入	• カスタム・ハードウェアや独自のテクノロジー・プラットフォームへの依存を排除 • ＳａａＳソリューションの直接導入により、アプリケーションやインフラの維持にかかる間接費の削減が可能	• パートナーやベンダーの慎重な評価が必要 • 一部のユースケースは時間と労力が増大する可能性 • データの移行が必要
リファクタリング	• クラウドネイティブの機能を活用 • 効率性と迅速性を向上させ、コストを改善 • 最新の顧客ニーズへ対応 • 顧客のハードウェアや独自のテクノロジー・プラットフォームへの依存を排除 • ユーザエクスペリエンスの向上	• 複雑でコストがかかり、移行スケジュールにも影響する可能性 • アプリケーションのあらゆる側面、コンプライアンス、規制要件、セキュリティ、コード、デザインなどを十分に理解する必要性 • 一部のユースケースは時間と労力が増大する可能性

viii 訳注：「Commercial Off-The Shelf（COTS）」とは、既製品で販売やリースが可能となっているソフトウェア製品やハードウェア製品、または一般向けにライセンス提供されるもの。
ix 訳注：最初からクラウド上で動くことを前提にクラウドならではの特性を活かせるよう設計されたシステムやサービス。
x 訳注：組織や機器、システムなどの構造について、要素に分割されておらず全体が一体になっている様子。
xi 訳注：１つのアプリケーションを構築および実行するのに使用される一連のテクノロジーサービス。

付録Ｂ.
役割と責任

クラウドのアクティビティを管理するための強力なＥＲＭプログラムでは、経営者がさらなる責任を負うことが必要である。以下では、クラウドの主要な責任の割り当てを説明する。

組織の規模や複雑性によっては、これらの役職が直接一致しない場合があるため、これらをガイドとして組織内の適切な人と調整や統合をしていただきたい。また、可能な限り、組織はクラウドガバナンスの責任を既存のＥＲＭの責任と一致させるべきである。

表７.１　**クラウドにおける役割と責任**

職位	職位の責任
取締役会	• クラウドコンピューティングの動向を把握し、クラウドが業界やビジネスモデルに与える影響について経営者の視点を理解する • クラウドサービスなどの変革的なＩＴプロジェクトを認識して監督する • 経営者が事業戦略やテクノロジー戦略の一環として、クラウドの利点とリスクのバランスをどのようにとっているかを理解する • 内部監査のリソースを活用し、クラウド構想が組織のリスク選好や統制の考え方と整合しているかについてアシュアランスを得る • ＥＲＭプロセスに参加する
最高経営責任者	• 組織の事業戦略と、クラウドコンピューティングによるその実現方法を定める • 外部委託に関する組織の見解と方針を定める • クラウドコンピューティングが組織の属する業界に与える影響を理解する • 組織がクラウドコンピューティングをどこで、どのように使用しているかを認識する • ＥＲＭプロセスに参加する
最高財務責任者	• 財務報告においてクラウド利用に関する新たな開示を行う • クラウドコンピューティングと社内ＩＴサービスの総所有コストと投資対効果の評価とモニタリングを行う • クラウドコンピューティングの税務・会計上の利点と代替案を評価する • クラウドサービスの調達に関する方針と統制を導入する • 各ＣＳＰの財務の健全性をモニタリングする • クラウドのガバナンスプロセスに参加する • ＥＲＭプロセスに参加する
最高法務責任者	• 組織のクラウドアクティビティが法令を遵守していることを確認する • コンプライアンスの必要性が増すような組織内の変化をモニタリングする • 組織のクラウドソリューションやＣＳＰに影響を及ぼす可能性のある新しい法律や規制をモニタリングする • クラウドサービス調達方針をレビューして承認する • データ分類方針とプロセスに関する情報を提供する • ＣＳＰとの契約をレビューして組織の利益と権利の保護を確実にする • さまざまな国で運営されているクラウドサービスを使用することに関連する、組織の業務に関する法的側面を理解する • クラウドのガバナンスプロセスに参加する • ＥＲＭプロセスに参加する

表7.1 **クラウドにおける役割と責任**

職位	職位の責任
最高リスク管理責任者	• クラウドコンピューティングの導入を含む、組織全体のＥＲＭの取り組みを管理する • 組織と環境全般の変化をモニタリングする • ＣＳＰのコンプライアンスに関して最高コンプライアンス責任者と連携する • カルチャーの変化をモニタリングして評価する
最高コンプライアンス責任者	• コンプライアンスの必要性が増すような組織内の変化をモニタリングする • クラウドアクティビティに影響を与える新たな規制に対するコンプライアンス計画を策定する • コンプライアンス要件に照らした組織のクラウドアクティビティをモニタリングする • ＳＯＣ２、ＰＣＩ－ＤＳＳまたは規制コンプライアンスなどの外部レビューに参加する • 適用されるコンプライアンスについてＣＳＰをモニタリングする • クラウドのガバナンスプロセスに参加する • ＥＲＭプロセスに参加する
最高情報責任者または最高テクノロジー責任者	• 現在の事業戦略や新規事業の機会を支援するためのクラウドコンピューティングの可能性を理解してモニタリングする • 新製品や新サービスのためのクラウドソリューションの活用と連携について、全般的な戦略を確立する • クラウドソリューションの業務、組織および現行のＩＴインフラへの統合を促進する • クラウドにおける組織の変化と成功を可能にする • 組織のＥＲＭプログラムへのクラウドガバナンスの組み込みを支援する • データ所有者と連携して、データ分類スキームを導入する • リソースプロビジョニング[xii]、ユーザアクセス管理および変更管理のためのクラウドプロセスを確立する • 組織内のクラウドインシデント管理プログラムを確立する • インシデント管理のためのＣＳＰとのプロセスとプロトコルを確立する • ＥＲＭプロセスに参加する
最高情報セキュリティ責任者	• クラウド上の情報とテクノロジー資産を保護するための戦略と監督を確立する • クラウドにおける組織の変化と成功を可能にする • 侵入評価などのサイバーセキュリティ評価を実施する、またはクラウドベンダーからの結果をレビューする • クラウドベースのサービスに対して適切なセキュリティ管理が確立されていることを確認する • クラウドベースのサービスに対してサイバー攻撃やリソースの内部不正使用の指標となるものをモニタリングする • クラウドのガバナンスプロセスに参加する • ＥＲＭプロセスに参加する
内部監査部門長	• リスクベースの監査を実施して統制とプロセスがＣＳＰと共有される混合型統制環境の設計と有効性を評価する • ＣＳＰを監査する、あるいは、ＳＯＣ、ＰＣＩ－ＤＳＳまたはその他の規制コンプライアンスレポートをレビューして、組織が依拠するＣＳＰの統制手段の有効性を検証する • 外部のクラウド上に存在するデータについて定期的なコンプライアンス監査を実施してデータ分類方針の遵守状況を検証する • ＣＳＰに対する支出と契約の遵守状況を監査する • クラウドガバナンスを評価する • クラウドのガバナンスプロセスに参加する • ＥＲＭプロセスに参加する
プライバシー責任者	• 組織のプライバシー保護プログラムを維持する • データ分類方針とクラウドに移行する可能性のあるデータをレビューする • ＣＳＰが組織のプライバシー要件をどのように遵守しているかをモニタリングする • ＥＲＭプロセスに参加する
クラウドコンピューティング運営委員会	• クラウド移行プロセスに対して監督を行う • クラウドガバナンス全体がプロセスに組み込まれるように組織をモニタリングする • ＥＲＭプロセスに参加する

xii 訳注：必要に応じてネットワークやコンピュータの設備などのリソースを提供できるよう予測して準備しておくこと。

表７．１　**クラウドにおける役割と責任**

職位	職位の責任
戦略的ソーシングまたは調達	• ビジネスプロセスオーナーと連携してクラウドベンダーの要件を定義する • 承認されたクラウドベンダーのリストを維持する • ＣＳＰ候補の適性を評価する • ＥＲＭプロセスに参加する
ベンダーリスクマネジメント	• ＣＳＰ用のベンダー管理方針を定める • ＣＳＰのサービスレベル合意書をモニタリングする • ＣＳＰとクラウドテナント顧客のアクティビティをモニタリングする • ＥＲＭプロセスに参加する
テクノロジー設計者	• クラウド戦略およびシステムやソフトウェアなどの環境を含む、組織全体のテクノロジー戦略を設計する • ＩＴ環境全般を実装して維持する
ネットワークエンジニア	• クラウド内外のシステムとアプリケーションの可用性を実現するためのネットワークアーキテクチャを設計して実装する • クラウドインフラストラクチャ（ＩａａＳとＰａａＳ）を維持する • ネットワークソフトウェアを最適化する • クラウド内外の通信とハードウェア接続を実装して維持する
セキュリティエンジニア	• クラウド環境のセキュリティ、機密性、完全性およびプライバシーを保護するための戦略を策定してツールを実装する • 潜在的な脅威に対してクラウド環境をモニタリングする • 組織のためのインシデント対応を管理する • インシデント対応のためにＣＳＰと連携する
デブオプスエンジニア	• クラウドの開発と運用のためのプロセスを維持する • 機能性、拡張性、耐障害性に優れたクラウド向けアプリケーションを作成する
品質評価エンジニア	• クラウドに対応したシステムとアプリケーションの変更点をテストする • クラウドの事業継続計画のためのデータを準備する
システム・アプリケーション管理者	• クラウドシステムとアプリケーションに対してアプリケーションユーザ管理とセキュリティを維持する • システム構成を管理する • クラウドプロセスのマネージドサービス[x iii]をモニタリングする • 必要に応じて、クラウドシステムの保守を管理する
ＣＳＰリレーションシップマネージャー	• 部署によって複数存在することに注意する • ＣＳＰとの関係や連絡を維持する • 必要に応じてＣＳＰとの間でインシデントを上申する • ＣＳＰとのサービスレベル合意書をモニタリングして執行する
エンドユーザ	• クラウドアプリケーションとツールを安全かつ適切に使用する • データのプライバシーとセキュリティの実務を理解する

x iii 訳注：通信サービスやＩＴサービスなどのうち、サービスの利用に必要な機器やソフトウェアの導入や管理、運用などの業務も一体的に請け負うサービス。

付録C.
用語集と定義

「はじめに」では、クラウドコンピューティングの３つの定義を説明した。繰り返しになるが、最も簡単に言えば、クラウドコンピューティングとは、インターネット上にプールされたリソースを利用するコンピューティングモデルである。基盤となるサーバやプロセスの管理は、他の組織に委託する場合がある。以下では，本稿で使用する主なクラウド用語の概要を説明する。

クラウドコンピューティングの用語

一般的なクラウドコンピューティングの用語を以下に説明する。

- **クラウドサービスプロバイダ（ＣＳＰ）**ークラウドコンピューティングサービスを提供するベンダーで、インフラ、ネットワークまたはビジネスアプリケーションを含む場合がある。

- **マネージドシステムプロバイダ（ＭＳＰ）**ー組織のＩＴニーズを管理するベンダー。ＣＳＰはＭＳＰであるが、ＭＳＰはＣＳＰである必要はなく、ＭＳＰはクラウド以外のプロセスも管理する場合がある。

- **マネージドクラウドサービス**ー組織のＣＳＰが提供するマネージドサービス。これらはサービス提供方法と契約によって異なる。

- **マルチクラウド**ー複数の配置モデル、サービスモデルおよび／または異なるプラットフォームを異なるパブリックＣＳＰと利用している組織は、マルチクラウド環境にある。マルチクラウドは、戦略的な決定の場合もあれば、異なる部門の協調的でない取り組みから発生する場合もある。

- **マルチテナント**ーほとんどのＣＳＰテクノロジーソリューションでは、顧客は共通のリソースとテクノロジーを共有する多数のテナントの中の１つのテナントになる。マルチテナントのコンセプトは、ＣＳＰが顧客に提供するリソースの構成や提供方法に影響する。例えば、あるクラウド利用者のデータは、同じクラウドソリューションの複数のテナントのデータと共有される単一の大規模データストレージ・プラットフォームに格納される場合がある。

- **クラウドアクセス・セキュリティブローカー（ＣＡＳＢ）**ークラウドユーザとクラウドアプリケーションの間に存在し、組織のセキュリティ方針をクラウドリソースに適用するセキュリティアプリケーションである。ＣＡＳＢは、データの保護とセキュリティ方針の適用に使用される。

- **セキュアアクセスサービスエッジ（ＳＡＳＥ）**ークラウドベースの方針を適用し、安全なクラウドアクセスを提供する。ＳＡＳＥは、ネットワーキングとセキュリティに重点を置いている。

- **コンテナ化**ーワークロードやサービスを管理するための手法で、自動化を容易にする。

クラウド配置モデル

最も一般的なクラウドコンピューティングの配置モデルには、次のようなものがある。

- **プライベートクラウド**ープライベートクラウドは、１つの組織のためだけに構築され、その組織またはＣＳＰによって管理される。

- **コミュニティクラウド／パートナークラウド**ーコミュニティクラウドやパートナークラウドは、共通の関心事（例えば、ミッションや業界協業など）を持つ組織によって共有される。コミュニティ組織またはＣＳＰによって管理される場合がある。

- **パブリッククラウド**ーパブリッククラウドは、ＣＳＰによって管理され、サービスを利用または購入したい人々や組織が利用できるようにする。

- **ハイブリッドクラウド**ーハイブリッドクラウドは、プライベートクラウドを含む２つ以上のクラウド（プライベート、コミュニティまたはパブリック）環境で構成されており、各クラウドエンティティ間の通信を伴う固有のエンティティを維持しなければならない。ハイブリッドクラウドは、ワークロードに柔軟性を持たせるために使用される。

- **ガバメントクラウド**ーガバメントクラウドは、政府のセキュリティ要件を満たすために、政府組織や政府機関向けに設計されたものである。これらは政府またはＣＳＰによって管理される場合がある。

クラウドサービスモデル

最も一般的なクラウドコンピューティングのサービスモデルには、次のようなものがある。

- **サービスとしてのインフラ（ＩａａＳ）**－ＣＳＰは、リソース（例えば、コンピューティングリソースやストレージリソース）の仮想データセンター全体を提供する。
- **サービスとしてのプラットフォーム（ＰａａＳ）**－ＣＳＰは、ＣＳＰが提供するホストインフラ上で動作するアプリケーションシステムやプログラムの作成を容易にする独自のツールを提供する。
- **サービスとしてのソフトウェア（ＳａａＳ）**－ＣＳＰは、組織が特定の機能やプロセスを実行するために使用できるビジネスアプリケーションを提供する（例えば、電子メール、顧客管理システム、エンタープライズリソースプランニングシステム）。

クラウド料金モデル

最も一般的なクラウドコンピューティングの料金モデルには、次のようなものがある。

- **サブスクリプション**－通常、ライセンスまたはシートに基づいて料金を支払う。これはＳａａＳでよく使われ、通常、月単位で設定される。
- **使用量**－使用量に基づくもので、使用するストレージ、計算能力、時間、帯域幅、バックアップおよび／またはサポートが含まれる場合がある。
- **階層**－使用量や機能に応じた料金体系。サブスクリプションや使用量のモデルに連動することもある。
- **複合**－使用量、階層および／またはサブスクリプションの側面を併せ持つ料金モデル。
- **ダイナミック**－需要と供給に基づいて調整される料金モデル。ユーザは現在の需要料金を支払うか、予約料金を支払って設定された時間にリソースを取得することができる。
- **マーケット**－料金は、組織がオンデマンド時間を使用する場合と、制限料金を設定する場合とで異なることがある。料金設定はサービス提供時の需要と供給に基づいて変化する。組織がリバースオークションのように制限料金を設定し、組織の設定した料金まで下がれば組織のワークロードが実行される。
- **広告**－料金は通常、低料金か無料であるが、システムを利用するために広告を表示することが条件となる。

著者について

Ｃｒｏｗｅ社プリンシパル・パートナー　マイク・グローブ

マイク・グローブは、Ｃｒｏｗｅ社のコンサルティング部門のプリンシパルである。クラウドトランスフォーメーションサービスを主導しており、顧客のＩＴサービスの近代化を支援する役割を担っている。ＡｚｕｒｅとＤｙｎａｍｉｃｓのマイクロソフト認定プロフェッショナルである。

ミシガン州立大学でメディアコミュニケーション戦略の理学士号を取得している。

Ｃｒｏｗｅ社マネージング・ディレクター　ヴィクトリア・チェン

ヴィッキーは、Ｃｒｏｗｅ社のコンサルティング部門のマネージング・ディレクターである。ＩＴリスクマネジメントとクラウドガバナンスを専門としている。

イリノイ大学を卒業。イリノイ州公認会計士であり公認情報システム監査人でもある。米国公認会計士協会、イリノイ州公認会計士協会、内部監査人協会およびＩＳＡＣＡの会員である。

ＣＯＳＯについて

1985 年に設立されたＣＯＳＯは、5 つの民間団体の共同イニシアチブであり、全社的リスクマネジメント（ＥＲＭ）、内部統制および不正抑止に関するフレームワークとガイダンスの開発を通じて、先進的な考え方を提供することに取り組んでいる。ＣＯＳＯの支援団体は、内部監査人協会（ＩＩＡ）、米国会計学会（ＡＡＡ）、米国公認会計士協会（ＡＩＣＰＡ）、国際財務担当経営者協会（ＦＥＩ）、管理会計士協会（ＩＭＡ）である。

ＣＲＯＷＥについて

Ｃｒｏｗｅ社は世界各地に拠点を持つ、会計、コンサルティングおよびテクノロジーの事務所である。同社の熱心な専門家は、業界や専門分野の深い知識と革新的なテクノロジーを融合させ、誠実さと客観性をもって顧客のために価値を創造している。また、顧客の声に耳を傾けることで、顧客のビジネスと顧客が直面する独特な課題について学んでいる。さらに、コアバリューと専門職基準を守りながら、卓越した顧客サービスを提供することを意図してそれぞれの関係を構築している。同社が将来に投資するのは、賢明な決断が顧客、人々および専門職のために永続的な価値を築くことを知っているからである。

一般社団法人日本内部監査協会

内部監査および関連する諸分野についての理論および実務の研究、ならびに内部監査の品質および内部監査人の専門的能力の向上を推進するとともに、内部監査に関する知識を広く一般に普及することにより、わが国の産業、経済の健全な発展に資することを目的に活動。

また、国際的な内部監査の専門団体である内部監査人協会（The Institute of Internal Auditors：ＩＩＡ）の日本代表機関として世界的な交流活動を行うとともに、内部監査人の国際資格である“公認内部監査人（Certified Internal Auditor：ＣＩＡ）”等の認定試験を実施している。1957（昭和 32）年創立。

公益財団法人日本内部監査研究所

内部監査に関する研究調査を推進するとともに、わが国の内部監査の普及発展に貢献することにより、わが国経済、社会の健全な発展に資することを目的として、2020 年 7 月に設立。2021 年 6 月に公益財団法人としての認定を受け「公益財団法人日本内部監査研究所」となった。

監訳者

八田　進二　（大原大学院大学　会計研究科　教授　／　青山学院大学　名誉教授）

橋本　　尚　（青山学院大学大学院　会計プロフェッション研究科　教授）

訳　者

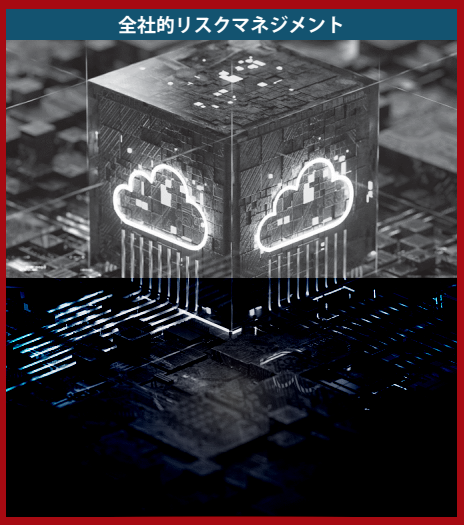
堺　　咲子　（内部監査人協会（ＩＩＡ）国際本部　北米外地域筆頭理事　／　インフィニティコンサルティング　代表　／　プレミアアンチエイジング株式会社　社外取締役　／　ＣＩＡ，ＣＲＭＡ，ＣＣＳＡ，ＣＦＳＡ）

全社的リスクマネジメント

COSO

トレッドウェイ委員会
支援組織委員会

coso.org



クラウドコンピューティング のための 全社的リスクマネジメント

COSO

トレッドウェイ委員会支援組織委員会

coso.org