The bridge to possible

2023 年グローバル ネットワーキング トレンド レポート

分散化したワークフォースのための
セキュアなマルチクラウド接続の簡素化

The bridge to possible

2023 年グローバル ネットワーキング トレンド レポート

分散化したワークフォースのための
セキュアなマルチクラウド接続の簡素化

目次

ようこそ

この『グローバル ネットワーキング トレンド レポート』では、エンタープライズ ネットワーキングおよびクラウド業界における最新の戦略とテクノロジーに焦点を当てています。一次調査と業界の調査をエグゼクティブの視点およびインサイトと組み合わせることで、最新のテクノロジートレンドを明らかにしました。このレポートをガイダンスとして利用すると、ネットワーキングモデルを発展させ、変化し続けるビジネスニーズに対応することができます。

2023 年のレポートでは、分散化したアプリケーション、従業員、勤務場所、モノを考慮して、組織がどのようにネットワークを展開し進化させ、セキュアな接続環境を実現しているかを説明しています。この調査は、北米、中南米、アジア太平洋、西ヨーロッパ 13 ヵ国の IT リーダー 2,500 人以上を対象に実施されました。

The bridge to possible

重要な調査結果：複数のクラウドを接続するネットワーキングの現状

ハイブリッドワークにはセキュアな接続という課題が今も存在しています。

ハイブリッドワークが浸透する今日では、企業のデータや資産が複数のマルチクラウド環境に分散して保存されており、リモートワーカーがそれらに安全に接続できるようにするための新たなアプローチが求められています。

- 従業員にはオフィス勤務の再開が奨励されていますが、今でも 40% 以上がフルタイムまたは週に数日リモートで仕事をしています。
- アプリケーションが複数のクラウドに展開され、以前よりもはるかにさまざまな場所で働けるようになったことで、従来のセキュリティモデルが時代遅れになっています。これが IT プロフェッショナルを悩ませており、半数以上 (51%) がクラウドのセキュリティリスクを特定しています。また、39% がリモートワーカーの増加を大きな課題として挙げています。

クラウドとマルチクラウドへの移行が加速しています。

ビジネスの俊敏性が課題となった場合、クラウドが解決策とされることが今でも少なくありません。

- クラウドプラットフォームの導入が現在も進んでおり、今回の調査の 78% が 2025 年までにワークロードの 40% 以上をクラウドでホストすると回答しており、現在の 63% からその割合に上昇することになります。
- マルチクラウドの導入も増加しており、クラウドおよびネットワーキング プロフェッショナルの 42% が、俊敏でスケーラブルなアプリケーション開発が複数のクラウドを利用する主な要因と回答しています。

クラウドアプリケーションへのユーザーアクセスの保護は、2023 年におけるネットワーキングの最も大きな課題です。

その他に企業の IT プロフェッショナルにとって大きな関心事となっているのは、デジタル サービス デリバリ チェーン (例：ユーザーとクラウド間) 全体でエンドツーエンドの可視性を維持し、一貫したアプリケーション体験を確実に提供することです。

- ネットワーキング プロフェッショナルの 41% が、複数のクラウドをまたいで稼働するアプリケーションに安全にアクセスできるようにすることが最大の課題と回答しています。
- 2 番目に大きな課題となったのは、ネットワークのパフォーマンスおよびセキュリティをエンドツーエンドで可視化することでした (37% が回答)。以前よりも多くのトラフィックが企業ネットワークの境界を越えて行き来するようになったことがその理由に挙げられています。

The bridge to possible

重要なガイダンス：クラウドベースのアプリケーションに安全にアクセスするためのネットワーキング成功戦略

ネットワーキングおよびセキュリティ統合の追求

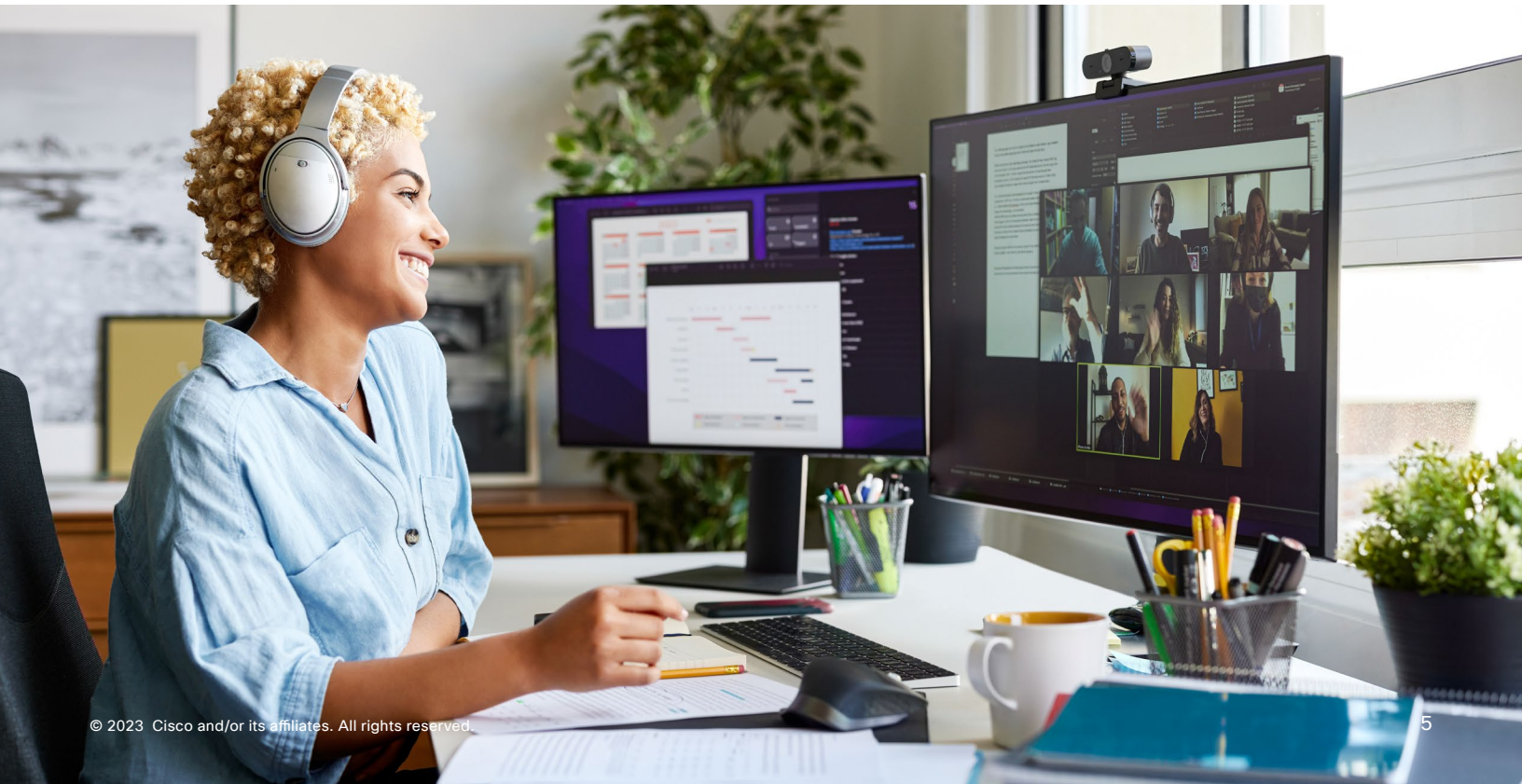
IT チーム間の連携を強化し、アクセスから、ネットワーキング、クラウドに至るまでの運用を簡素化する。

分散化したアプリケーション、従業員、勤務場所、モノのセキュリティニーズは常に変化しています。組織がサイロ化し、接続環境の提供に従来のモデルが使用されていると、こうしたニーズにはもはや対応できません。

- 標準ポリシーや共有テレメトリを実装し、ワークフローをセキュリティ、ネットワーキング、クラウド運用全体で合理化できれば、技術がサイロ化した状態で環境を運用する場合よりも、優れた IT およびビジネス成果を短期間で得ることができます。
- さまざまな勤務場所からクラウドベースの複数のアプリケーションに安全にアクセスできるようにする場合の主な課題として、回答者の 40% が運用のサイロ化を挙げています。
- クラウドプロフェッショナルはネットワーク運用とクラウド運用チーム間の連携強化が必要と考えており、38% がネットワークチームとの協力を深めるべき、また、34% が運用上の一貫性の確保を主な目標にしていると回答しています。

SASE アーキテクチャを使用した統合ネットワーキングおよびセキュリティモデルに移行する。

セキュア アクセス サービスエッジ (SASE) を導入すると、運用を簡素化し、常にセキュリティおよびパフォーマンスを確保して、マルチクラウドアクセスとハイブリッドワークフォースの要件に対応できます。



- SASE アーキテクチャを実現すべく、ソフトウェア定義型 WAN (SD-WAN) とクラウドセキュリティの統合が進められています。
- 回答者の 47% が、2 年以内に SD-WAN 環境を完全な SASE アーキテクチャに拡張してブランチとリモートクライアントに接続環境を提供すると予測しています。

クラウドファーストのネットワーキングおよびセキュリティの導入

SD-WAN 接続を複数のクラウドに一貫して拡張することで、IT 管理の簡素化とアプリケーション体験の向上を実現する。

すべてのクラウドに常にポリシーを適用することで、クラウドに依存しない接続を自動化すると同時に、アプリケーション体験の最適化およびセキュリティ確保を行います。

- クラウド、SaaS、ミドルマイルプロバイダー全体に可視化、制御、ゼロトラストアクセスを拡張することで、安全で優れたユーザー体験を提供できます。
- 回答者の半数以上 (53%) が、クラウド サービス プロバイダー環境との統合を優先し、今後 2 年にわたって、すべての勤務場所からクラウドベース アプリケーションに接続できるよう改善を進めるとしています。

クラウド中心のセキュリティに発展させ、一貫した運用とポリシーを実現する。

クラウドプラットフォームでセキュリティ機能を統合することで、可視化、ポリシー管理、制御を以前よりもさまざまな環境で簡単かつ効果的に行えるようになります。

- 回答者の 59% が、勤務場所に関係なくユーザーやデバイスにポリシーを常に適用することが重要な要件と認めたうえで、クラウドでのセキュリティ一元化を、クラウド アクセス ネットワーキングにおける今後 2 年間の最優先事項としています。

プロアクティブな運用への移行

エンドツーエンドでネットワークを可視化し、ますます複雑になるデジタル サービス デリバリ チェーン全体で一貫性のあるユーザー体験を追求する。

自社のネットワークを越え、インターネットやクラウドの環境まで可視化できなければ、クラウドベースのアプリケーションとサービスで高品質のユーザー体験を常に提供することはできません。

- 回答者の 51% が、エンドツーエンドのネットワークテレメトリ利用と可視化を優先的に行い、問題をプロアクティブに検出し修復しています。
- インターネットとクラウドのトラフィックの可視化がとりわけ重要となるのは、ユーザーとデバイスによるトランザクションデータの大部分が企業の境界を越えて転送される場合です。

リアクティブ運用からプロアクティブ運用に移行して、アップタイムとパフォーマンスを向上させる。

Artificial Intelligence for IT Operations (AIOps) の一連のツールでは、IT 運用全体の簡素化、迅速化、効果向上という点で、予測分析が重要視されつつあります。

- 回答者の 47% が、予防的な対処によってネットワーク品質の低下を未然に防げるよう、今後 2 年間、予測ネットワーク分析を優先的に導入するとしています。

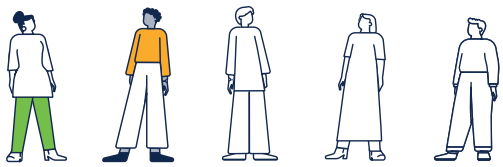
はじめに：マルチクラウドアクセスにおける傾向

「電話のシステムが公共インフラであるように、コンピューティングもいつの日か公共インフラとして整備されるかもしれません。どの利用者も、実際に使用した分の料金のみ支払えばよいことになるでしょう」[1]。1961 年、John McCarthy 教授は、MIT の式典でそのように述べ、未来を予見しました。

それから 60 年以上がたった今日、オンデマンド コンピューティングを公共インフラとして共有するという McCarthy 教授のビジョンは、実現しただけでなく、グローバルなデジタル革命実現に不可欠な要素の 1 つとなっています。

マルチクラウドへの移行は続く

今日では、ほとんどの組織で複数のクラウドが導入されています。このシスコの『2023 年グローバル ネットワーキング トレンド』の調査によると、組織の 2/3 がワークロードの 40% 以上を複数のクラウドで処理していました。さらに、ほとんどの組織が 2 社以上 (大多数が 5 社以上の SaaS プロバイダー) のクラウドプロバイダーを使用しています (図 1 を参照)。



5 人に 2 人が、少なくとも週何日かはリモートで働いています。

ハイブリッドワークが定着

分散化がきわめて進んだのは、アプリケーションだけではありません。ハイブリッドワークが浸透したことで、従業員やモノも、かつてないほど分散化が進んでいます。

最近の調査によると、59% がフルタイムでのオフィス勤務を再開しています。その一方で、28% がハイブリッドワークで、それら以外 (13%) が完全なリモートワークといったように、多くの従業員が今でもリモートで働いています[2]。これらの割合は、業界や職務によって大きく異なります。

同時に、IoT 技術とエッジコンピューティングが急速に導入されたことで、接続数が増加し続け、データフロー数も数兆にまで及んでおり、これらの管理と保護が日々必要となっています。

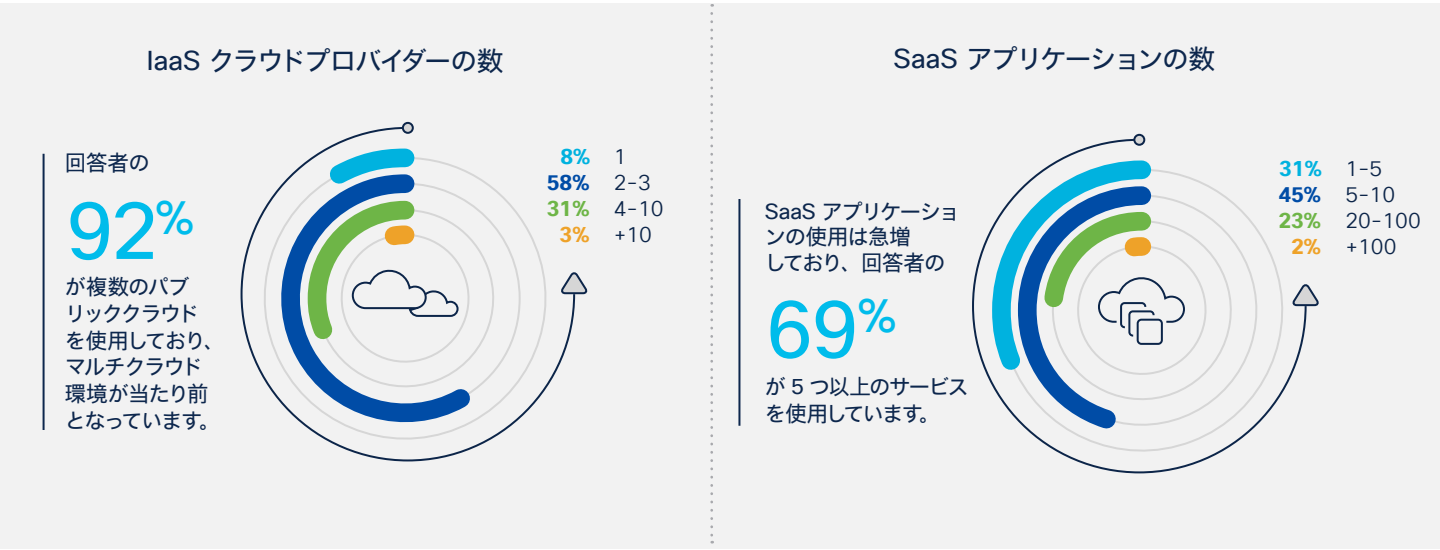


図 1. 複数クラウドと SaaS プロバイダーの利用が当たり前

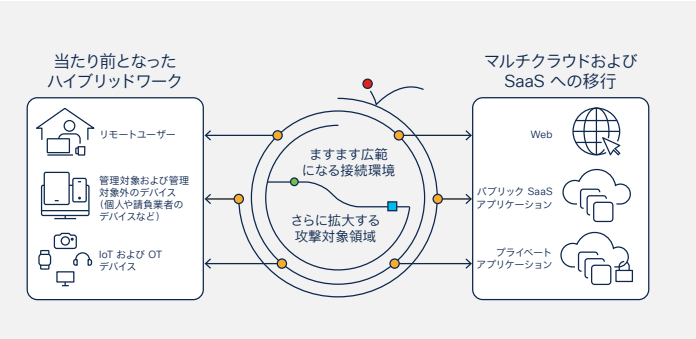


図 2. ハイブリッドワークの普及と SaaS への移行が進み、人間の能力ではネットワークセキュリティの課題解決が困難に

従業員の分散化が進み、IoT とエッジコンピューティングが急増したことで、マルチクラウド アプリケーションや、さまざまなネットワークでグローバルに稼働するサービスに大規模かつ安全に接続およびアクセスできる環境がますます必要となっています (図 2 を参照)。ネットワーキング プロフェッショナルは、これを 2023 年の最大の課題と捉えています。

そうした課題を複雑にする要因となっているのが、インターネットを介した接続です。その理由は、ネットワーキングおよびセキュリティ プロフェッショナルにとって、それらのインフラストラクチャの可視化と管理が不可能な点にあります。それにもかかわらず、こうしたプロフェッショナルは、従業員、顧客、パートナーにデジタル体験を提供しセキュリティを確保する任務を背負っています。

ますます重要になる迅速さと俊敏性

今日では、ほとんどの組織が、成功には俊敏性が不可欠と考えています。調査結果によると、マルチクラウドへの移行の最大要因は、McCarthy 教授が最初に予測したように、コスト削減ではなく、ビジネス俊敏性の確保およびイノベーションに加え、高品質の新規アプリケーションおよびサービスの迅速な展開が必要なことです。破壊的なパンデミック、地政学的および経済的な混乱、サプライチェーンの課題に続き、迅速に方向転換し市場動向を活用する能力確保への対応が最優先されるようになりました。

現在の環境で使用されているサイロ化した技術と運用モデルは、多くの制約を抱え十分に機能していないため、新たなツールとプロセスが求められています。接続とセキュリティの課題解決に必要なのは包括的なアプローチであり、これによって、以前よりも簡素化され安全で柔軟なネットワーク インフラストラクチャと運用モデルを実現しなければなりません。

「ビジネス上の優先事項に、数週間、数ヵ月かけるわけにはいかないのです。ビジネス上の取り組みが何であれ、これまで生じていたボトルネックがなく、すぐに成果を得られることが求められています」

- 小売業、IT 責任者

この後のページでは、こうした課題への対策を取り上げ、柔軟でありながらセキュアな接続を実現するためのベスト プラクティス ガイダンスを提示します。また、信頼性の高い安全かつ堅牢なクラウド体験をあらゆる勤務場所の従業員、パートナー、顧客に提供するには、ネットワークチームとセキュリティチームがどのような理由でどのように連携すべきかについても説明します。

1 https://www.technologyreview.com/2011/10/03/190237/the-cloud-imperative

2 https://wfhresearch.com/wp-content/uploads/2023/02/WFHResearch_updates_February2023.pdf

重要なガイダンス：複数のクラウドへのセキュアなアクセスを実現する 6 つのベストプラクティス

重要なガイダンス 1：IT チーム間の連携を強化して、アクセスからクラウドに至るまで IT 運用を簡素化する。

分散化したアプリケーション、従業員、勤務場所、モノのセキュリティニーズは常に変化しています。組織がサイロ化し、接続環境の提供に従来のモデルが使用されていると、こうしたニーズにはもはや対応できません。

複雑さの増大と脅威対象領域の拡大という課題を抱える IT リーダーには、チーム間の連携を強化し、急速に変化するビジネスニーズにこれまでよりも迅速、効率的、かつ安全に対応することが求められています。

分散化した勤務場所から複数のクラウドベース アプリケーション (Infrastructure as a Service (IaaS) や Software as a Service (SaaS) など) にアクセスできるようにする際の課題は、上位 5 つのうち 4 つがセキュリティに関連していました。回答者の 40% が、分散化した勤務場所から複数のクラウドベース アプリケーションに安全にアクセスできるようにする際の最大課題として、サイロ化したクラウド、ネットワーク、セキュリティ運用を挙げています。

IT 組織の多くでは、ネットワークチームとセキュリティチームが個別に計画と運用を行っています。しかし、今日のセキュリティ課題に対処するには、技術と運用のサイロ化を解消し、個別の統合システムの数を減らすしかありません。

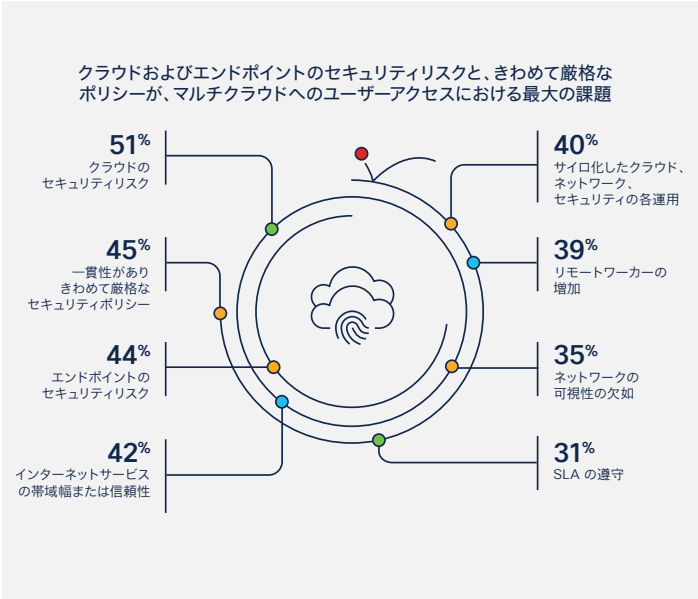


図 3. リモートから、複数のクラウドベース アプリケーションに安全にアクセスできるようにする際の課題

また、チーム、ツール、プロセスを調整し運用を合理化するには、運用モデルの一貫性を高める必要があります。シスコの調査によると、CIO と IT リーダーの 86% が、一貫性のある運用モデルを開発して、オンプレミス、プライベートクラウド、パブリッククラウド、SaaS システム全体に適用する必要があると考えています。[3] クラウド運用モデルの原則に従う DevOps チームと CloudOps チームは、運用の簡素化と俊敏性の確保という点で確実に成果を上げています。IT チームでも、クラウド運用モデルの原則を導入することで、同様の利点を享受できます。こうした考え方は、調査データによって

クラウドプロフェッショナルの 38% が、ネットワークチームとの連携改善を運用上の大きな課題と捉えている。

も裏付けられています。クラウドプロフェッショナルの 38% が、運用の最大課題として、ネットワークチームとの連携改善を挙げ、それ以外の 34% が、クラウドとネットワーク間における運用の一貫性維持を挙げています。

クラウド運用モデルの原則をネットワーク全体、さらにはクラウド / ネットワークの IT スタック全体に適用することで、イノベーションの推進、セキュリティの向上、クラウド運用からのリスク排除が可能になります。また、ネットワーク、セキュリティ、クラウド間の運用連携を妨げかねない複雑さや断片化が軽減され、ひいては、変化し続ける、組織のニーズに対応できるようになります。

要点

クラウド中心のモデルに基づいて、ネットワーキングとセキュリティのポリシー、技術、ツール、運用ワークフローを統合することで、共通した一連のツールでの作業が可能になります。さらには、常にセキュアな接続環境の提供、効率の改善、リスクの軽減も実現します。

3 https://ebooks.cisco.com/story/accelerating-digital-agility-2021/page/7/1

エキスパートの見解

チーム間の連携を深めることで、簡素化された運用と一貫性のあるセキュリティおよびパフォーマンスを実現する。

「ずいぶん前の運用チームでは、ケーブルの配線からアプリケーションに至るまで、レイヤやシステムをすべて把握したうえで、それらをまとめて管理していました。そのモデルに戻る必要があります。

オンプレミスからクラウドに移行したことでネットワーキングが様変わりし、エコシステムのデバイスやソフトウェアの管理が一部不要になったとしても、セキュリティ対策が必要なことに変わりはありません。重要なのは、クラウドアプリケーションに従業員が安全にアクセスできるようにする際に、勤務場所やデバイスを問わず、一連のポリシーが必要となることです。こうしたポリシーは、設計、運用、アーキテクチャを連携させるための指針となる可能性があります。

今後さらに多くのネットワーキングチームとセキュリティチームが、運用パフォーマンスの原則だけでなく、セキュリティ確保と簡素化の原則に基づいて、インフラストラクチャ運用での連携を深めるでしょう。こうした原則はすべて、両チームに共通する目標の達成につながるからです」

シスコ
アドバイザリ CISO 責任者
Wendy Nather

The bridge to possible

重要なガイダンス 2：SASE アーキテクチャを使用した統合ネットワーキングおよびセキュリティモデルに移行する。

SASE を実装することで、マルチクラウドアクセスとハイブリッドワークフォースに必要な運用の簡素化と一貫したセキュリティおよびパフォーマンスの確保を実現します。

これを実現するには、ネットワークドメインとセキュリティドメインを統合し、高度に分散化した複雑な環境でユーザーがアプリケーションに安全かつシームレスに接続するのに必要なフレームワークを確立します。

SASE は、セキュアなマルチクラウドアクセスに最適な統合アーキテクチャになりつつあり、回答者の 47% が、主に SASE モデルを使用して、ブランチとリモートクライアント向けの接続環境を 2 年以内に構築すると予想しています。

しかし、組織の多くが、SASE の可能性の最大化に困難を抱えています。ソリューションに特定の機能を備えられなかったり、ネットワークとセキュリティが完全に統合されたソリューションを実現できなかったりするためです。

SASE 統合には、充実したクラウドセキュリティ機能または Security Service Edge (SSE) ソリューションと連携する堅牢な SD-WAN 基盤が必要です (図 4)。これらのアーキテクチャを完全に統合して初めて、IT 部門では、SASE の利点をすべて享受できます。こうした利点の 1 つに合理化された運用モデルがあり、これによって、可視化、管理、制御が可能となり、ユーザーがどこにいても常に安全かつ簡単に接続できるようになります。

統合 SASE ソリューションを導入した NetOps および SecOps チームでは、標準ポリシーや共有テレメトリを実装すると同時に、セキュリティおよびネットワーク要素全体でアラートを連携できるため、IT の効率、パフォーマンス、保護機能が向上します。また、これら 2 つのチーム全体で、以前よりも効率的で一貫した運用モデルとワークフローが確立すれば、優れたユーザー体験を常に提供できます。

SASE の機能を完全に実装すると、運用のさらなる効率化、ユーザー体験の向上、セキュリティの強化が可能になります。こうした利点の例をいくつか紹介しましょう。

「セキュア アクセス サービスエッジ（SASE）を実装すると、ネットワークとセキュリティの機能をサービスとして統合し、SD-WAN、SWG、CASB、NGFW、ゼロトラスト ネットワーク アクセス（ZTNA）などの機能を提供できます。また、ブランチオフィス、リモートワーカー、オンプレミス向けに構築するセキュアなアクセス環境のユースケースにも対応可能です。SASE は主にサービスとして提供します。SASE により、デバイスまたはエンティティの ID に加え、リアルタイムのコンテキストや、セキュリティおよびコンプライアンスポリシーに基づいて、ゼロトラストアクセスを実現できます」

– Gartner『IT 用語集 (Information Technology Glossary)』[英語]、セキュア アクセス サービスエッジ (SASE)、2023 年 5 月 2 日。

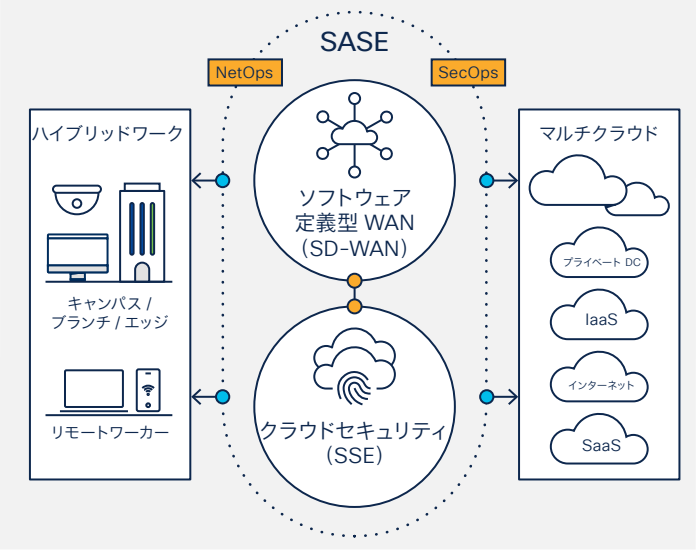


図 4. ネットワークおよびセキュリティの技術と運用を統合することで、安全性の高い新たな接続モデルであるセキュア アクセス サービスエッジを実現

Gartner® によると、2025 年には、SD-WAN 製品の 50% が SASE 製品を提供する 1 社のベンダーから購入されるようになり、2021 年の 10% 未満からこの割合にまで上昇します。[4]

- シスコの社内 IT チームでは、SASE を使用したことで OpEx を 40% 削減できました。
- 独立系テスト会社が実施した厳格なパフォーマンス評価によると、セキュリティポリシーが設定された Umbrella（Cisco SASE のコアコンポーネント）は、セキュリティ対策なしにインターネット経由で SaaS アプリケーションにアクセスするのと同様のパフォーマンスを示し、多くの場合、それ以上の効果を発揮しました。
- TechValidate の顧客調査によると、シスコの顧客の 85% が、SASE アーキテクチャ導入によって、マルウェアの感染を 50% 削減しています。

こうした望ましい結果を得るには、2 つの基本的なアプローチを取ります。

1 つ目は、個別のネットワーキング製品とセキュリティ /SSE 製品を組み合わせることです。こうした製品は、通常、1 ～ 2 社のベンダーから提供され、完全な SASE ソリューションに統合することができます。このアプローチは、SSE または SD-WAN を展開済みで、カスタマイズ機能と柔軟性の向上を必要とする組織に適しています。

2 つ目は、統合アプローチです。この場合、ネットワーキングおよびセキュリティの要素が、単一のターンキー方式のクラウドサービスとして提供され、それらを統合的に管理することになります。適切に設計された統合 SASE ソリューションであれば、迅速化、簡素化、短期間での価値実現が可能になります。

4 Gartner 社『SASE コンバージェンスのための 2022 年戦略ロードマップ』[英語]、Neil MacDonald、Andrew Lerner、John Watts、2022 年 6 月。Gartner は、Gartner, Inc. とその関係会社の米国およびその他の国における登録商標およびサービスマークであり、許可を得てここで使用しています。All rights reserved.

エキスパートの見解

SASE ソリューションが機能しない場合とは？

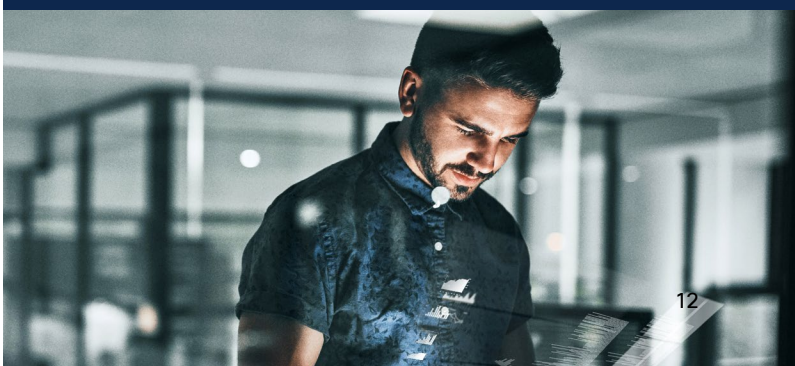
「どのような組織にも導入済みの技術基盤があるため、既存環境では補えない SASE 機能を単純に追加したい誘惑に駆られるかもしれません。しかし、SASE は長期的な戦略として選択されるものである点に注意すべきです。高度な統合を行わずに SASE モデルの要素をすべて展開しても、完全に機能する SASE ソリューションは実現しません。望ましい結果を得られないことになるのです。

ネットワーキングとセキュリティのリーダーには、優先順位に応じて、適切に統合された SASE ソリューションまたはターンキー方式の統合サービスのいずれかを選択することを強くお勧めします。

統合されたターンキー方式のクラウドサービスを選択した NetOps および SecOps チームでは、さまざまな利点を享受できます。たとえば、インテリジェントな分散型セキュリティ適用、制御、可視化をエンドポイント、エンタープライズエッジ、クラウドエッジ全体で行い、それらを一元的に管理できます。これにより、よりセキュアなエンドツーエンドのソリューションが実現し、エンドユーザー体験が向上します。

「ニーズを満たす技術やアーキテクチャの選択では、それが何であれ、重要な確認ポイントがあります。すべての要素を適切に統合し 1 つのシステムに統一する意欲が、常にベンダーにあるかどうかです」

Cisco Meraki
NaaS/SASE 製品管理担当
VP Omri Guelfan



The bridge to possible

要点

従来のセキュリティソリューションの導入とは対照的に、クラウド中心の SASE 統合アーキテクチャを実装すると、セキュリティポリシーを一元管理し、エンドユーザーとアプリケーションの近くにそれらを適用すると同時に、柔軟かつシームレスでセキュアな接続環境を提供できます。

SASE の詳細

重要なガイダンス 3：SD-WAN 接続を複数のクラウドに一貫して拡張することで、IT 管理の簡素化とアプリケーション体験の向上を実現する。

すべてのクラウドに常にポリシーを適用することで、クラウドに依存しない接続を自動化すると同時に、アプリケーション体験の最適化およびセキュリティ確保を行います。

今日、クラウドは、エンタープライズ ネットワークの拡張環境として機能しており、多くの企業にとって、SD-WAN 導入は、SASE を完全実装するための足がかりになっています。主要な IaaS、SaaS、ミドルマイルプロバイダー環境などの導入による SD-WAN 拡張を自動化すると、運用上の制御が強化され、ユーザー体験が向上します。

ネットワーキングチームでは、ユーザー体験の適切な管理が明らかに最優先されています。回答者の 53% が、クラウド サービス プロバイダー環境との統合を優先することで、分散化した勤務場所からクラウドベースのアプリケーションに快適に接続できるようにしています。また、こうしたチームは対策も立てており、回答者の 49% が、今後 24 ヵ月の間、SD-WAN とマルチクラウドの統合を最優先で行うとしています。

SD-WAN とマルチクラウドを統合したネットワーキングチームとクラウドチームでは、インターネット、相互接続、コロケーション環境およびクラウド プロバイダー ネットワークを介して、企業拠点から、さまざまなクラウドプロバイダー環境および他の企業拠点への拡張を推進し、自動化することができます (図 5)。また、こうした統合によって、アプリケーション体験を最適化し、すべてのクラウドとオンプレミス環境で運用体験の一貫性を向上させることも可能です。さらに、Equinix や Megaport などのグローバルネットワーク相互接続プロバイダーと連携すると、クラウドアプリケーションやプロバイダーのアクセスポイントに安全かつスケーラブルにアクセスできる環境が実現します。こうした統合では、グローバルネットワークの構築を簡素化および完全自動化し、数分以内で完了することもできます。

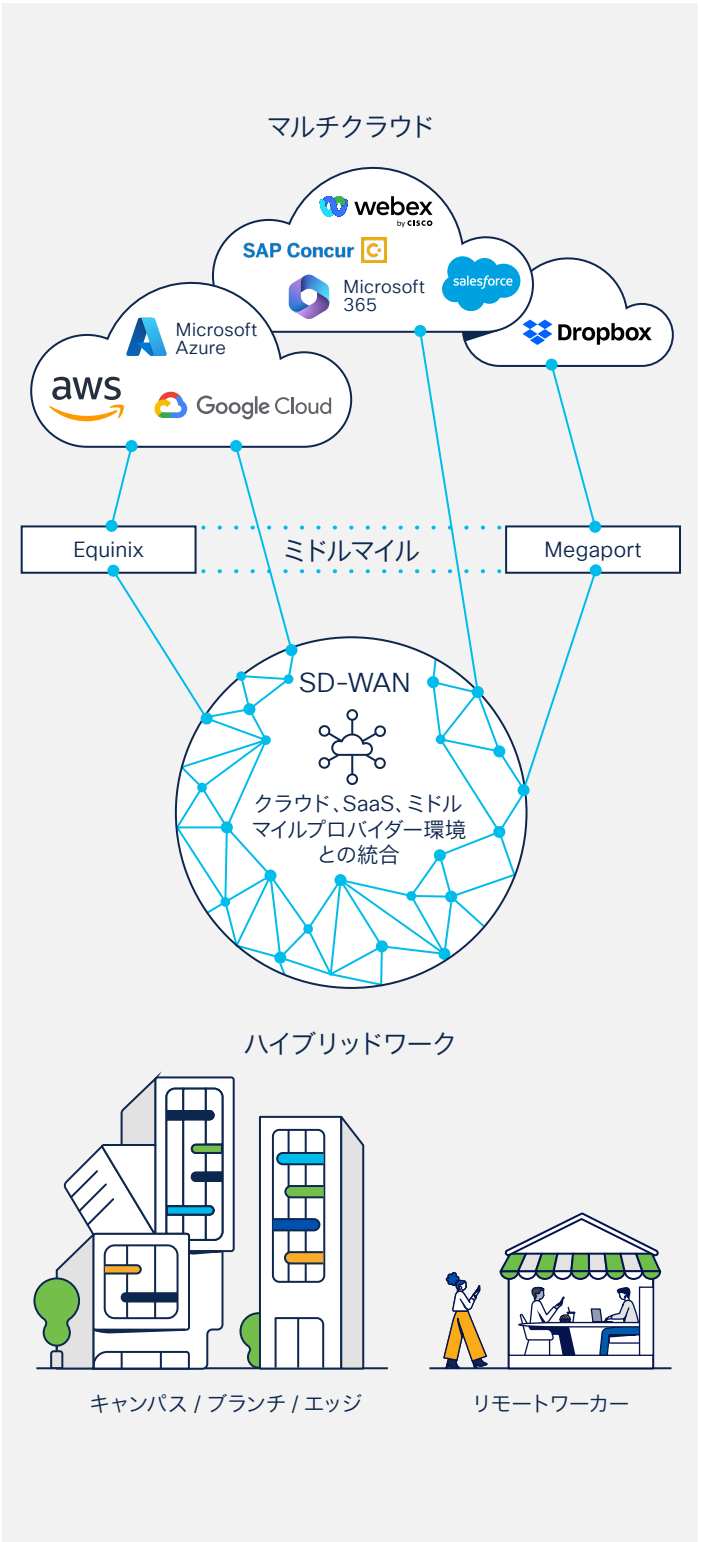


図 5. IaaS、SaaS、ミドルマイルプロバイダー環境との SD-WAN 統合は、IT 担当者およびユーザーの体験向上に不可欠です。

The bridge to possible

要点

SD-WAN とマルチクラウドの統合は、「社内ネットワークからマルチクラウドへの拡張を迅速に簡素化する」、「ユーザーアプリケーション体験を最適化する」、「ゼロトラストアクセスによってクラウドアプリケーションのセキュリティを高める」、といったニーズを満たす必要がある IT チームにとっては不可欠です。

SD-WAN の詳細はこちら

エキスパートの見解

マルチクラウド接続の複雑さとリスクを無視することはできません。

クラウド中心となった今日の世界において、主要なクラウド、SaaS、ミドルマイルプロバイダー環境と緊密に統合されていない SD-WAN ソリューションの提供は、想像し難いものです。グローバル拠点やクラウドワークロードに対応可能な SD-WAN ファブリックの拡張を自動化すれば、クラウド運用の取り組みを推進できます。また、ネットワーク運用の簡素化、エンドツーエンドの暗号化によるアシュアランス、柔軟性を活用した迅速なビジネスイノベーションを実現し、それらの利点を享受することも可能です。

さらに、脅威が増大し進化し続け、分散型クラウドや SaaS アプリケーションが利用される中で必要不可欠なのは、「ゼロトラスト」アプローチとそのコア原則「信頼できることを前提にせず、常に検証し最小限の権限を適用」の概念をネットワークに取り入れることです。SD-WAN をゼロトラストアプローチと統合すると、アクセス先のクラウドサービスとそれらにアクセスするユーザーを制御可能なセキュリティ態勢を確立できます。また、許可したトラフィックへの自動セキュリティ制御、セキュリティ対策の継続的な適用、セキュリティ態勢変更への素早い適応が可能になります」

シスコ 製品管理
エンタープライズ ルーティング
SD-WAN およびクラウドネットワーキング担当 VP
JL Valente

重要なガイダンス 4 : クラウド中心のセキュリティに発展させ、一貫した運用とポリシーを実現する。

クラウドプラットフォームでセキュリティ機能を統合することで、可視化、ポリシー管理、制御を以前よりもさまざまな環境で簡単かつ効果的に行えるようになります。

ハイブリッドワークが普及している今日、従業員は、会社のデバイスと自分のデバイスの両方を使用して、さまざまなアプリケーションにアクセスしています。こうしたアプリケーションは、管理対象または管理対象外のネットワークで稼働しており、それらのネットワークは、企業ネットワークの内外に存在しています。これまでのような境界防御では、もはや十分ではないのです。そのため、IT 部門では、すべてのエンドポイント、アプリケーション、データのセキュリティ確保が最優先で行われています。

これまで、リモートワーカーとオンプレミス環境には異なるセキュリティポリシーが使用されていました。リモート セキュリティ ポリシーにはさまざまな信頼レベルがあり、個別のセキュリティツールで管理されています。異なるポリシーに対応するとなると、IT のオーバーヘッドが増加するうえ、エンドユーザーに不満が生じる可能性があります。この調査でセキュリティポリシーについて尋ねたところ、回答者の 45% が、分散化した勤務場所からマルチクラウドに安全にアクセスできるようにする際の最大課題は、一貫性があり、きわめて厳格なセキュリティポリシーの確立と考えていました。

セキュリティチームには、絶え間ないサイバー攻撃への対応に加え、セキュリティポリシーの定期的な更新も求められています。分散化した従業員全員を対象にしてアプリケーションポリシーを常に更新しなければならないことが、セキュリティ対策一元化の大きな推進要因となっており、回答者の 59% が、今後 24 ヵ月、最も重要なクラウド アクセス ネットワーク イニシアチブとして、クラウドセキュリティの一元化を最優先するとしています (図 6)。

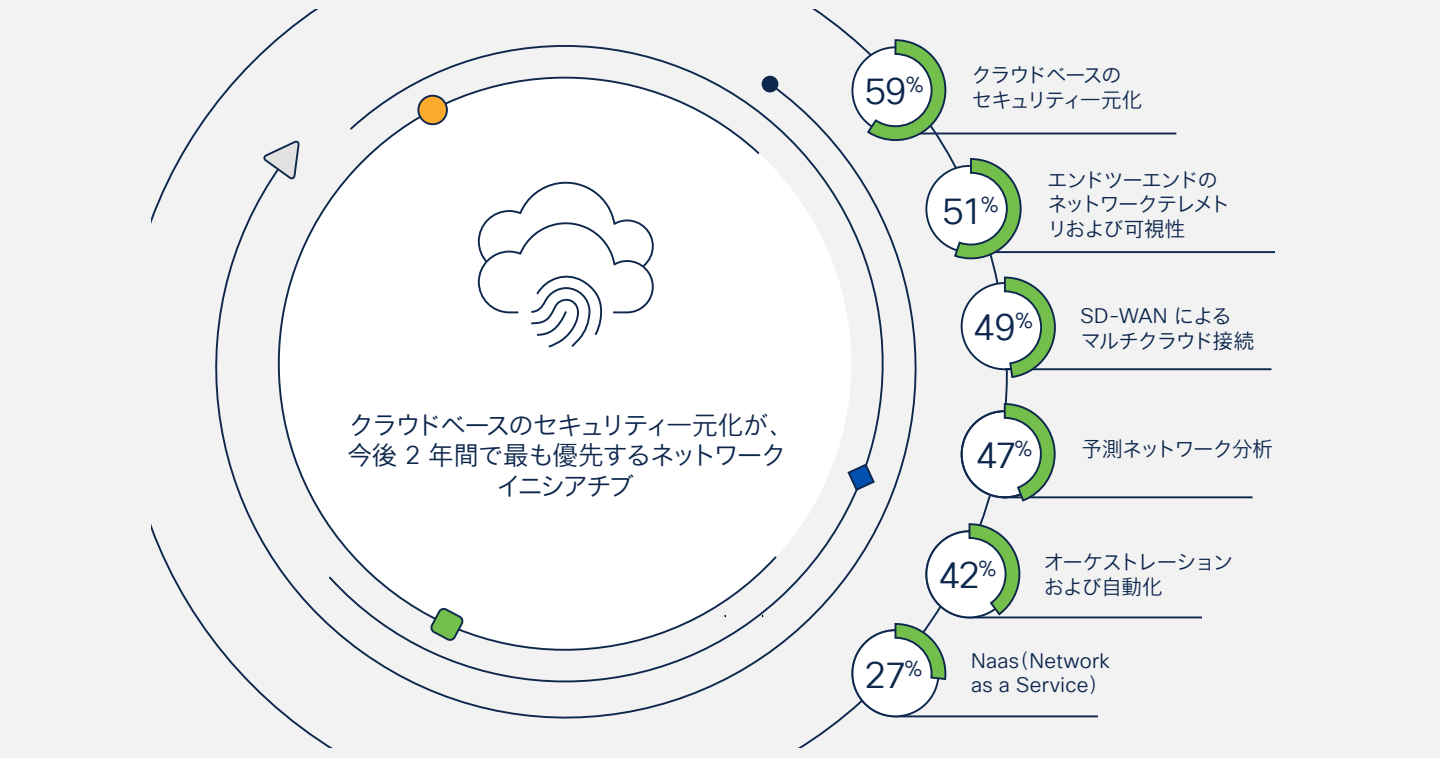


図 6. 今後 24 ヵ月間における最も重要なクラウド アクセス ネットワーク イニシアチブ

これまでのような境界防御だけでは、もはや成果は得られません。今日必要なのは、広範囲にわたるアプリケーションやワークロードに安全にアクセスするためのインテリジェントな方法であり、それを、一元化したクラウド セキュリティ ソリューションに取り入れることです。そこで有用なのが、SASE の中心的役割を担う SSE です。

要点

勤務場所を問わない働き方、BYOD、クラウドサービスの普及などにより、かつて明確に定義されていたセキュリティ境界の効力は失われてしまいました。日常的に使用するアプリケーションの多くがクラウドに存在する場合、包括的な SSE 戦略を設計して、複数のセキュリティ機能を統合し、クラウドからそれらを効果的に提供するのが賢明でしょう。

エキスパートの見解

一元化した統合モデルを確立するための鍵は、クラウドセキュリティの統合。

「この数年間、個別のセキュリティ製品を追加することで、拡大し続ける脅威への対処が行われてきました。これによりセキュリティは向上しましたが、運用の複雑さが大幅に増大したため、そのような利点が弱まっています。SSE ソリューションに移行すると、スケーラブルでクラウドネイティブの各種セキュリティ機能 (セキュア Web ゲートウェイ、クラウド アクセス セキュリティ ブローカ、ゼロトラスト ネットワーク アクセス、Firewall as a Service) を統合でき、これによって、エンドユーザー体験の向上、セキュリティ対策の成果改善、IT チームの負担軽減が可能となります。

そうした統合および一元化のアプローチを取ることで、管理タスクの確実な簡素化、パフォーマンスの容易な拡張、詳細な可視化が可能になるほか、組織全体で堅牢なセキュリティを実現できます。完全な SASE アーキテクチャには、統合 SSE ソリューションが不可欠です」

シスコ
セキュリティ /SSE 製品管理担当 VP
Jeff Scheaffer

重要なガイダンス 5：エンドツーエンドでネットワークを可視化し、ますます複雑になるデジタル サービス デリバリ チェーン全体で一貫性のあるユーザー体験を追求する。

自社のネットワークを越え、インターネットやクラウドの環境まで可視化できなければ、クラウドベースのアプリケーションとサービスで高品質のユーザー体験を常に提供することはできません。

IT 部門にとって、ユーザー体験の向上は重要な目標です。ネットワーキングチームでは、優れた体験を提供しようと、従来のツール以外にも目を向け、自社ネットワーク内外での現状をリアルタイムかつ詳細に可視化するソリューションを導入しています。こうした拡張メトリックをアプリケーション パフォーマンスと関連付けてインサイトを取得しそれらを活用すると、すべての従業員と顧客のデジタル体験を最適化できます。

組織では、SaaS やクラウドソリューションの導入が加速し、インターネットなどのパブリックネットワークの使用を増やすことで、そうしたアプリケーションへのアクセスを提供しています。そうしたマルチホップネットワークが、ますます複雑になる中、不可欠とされているのが、高度な可視性ソリューションへの投資です。実際に、回答者の半数以上 (51%) がそれを最優先事項と考えており、主要なネットワークイニシアチブとして、エンドツーエンドのネットワークテレメトリと可視性に注目しています。

アプリケーション トランザクションは、複数のネットワーク、ネットワークセグメント、サービスにわたって実行されており (図 7)、これが、特定のアプリケーションにおけるパフォーマンスと可用性の追跡を困難にしています。実際に、回答者のほぼ半数(48%) が、接続環境を向上させるにはインターネットの可視化とインサイト取得を優先すべきと考えています。この点からはさらに、トランザクションのパスをすべて把握し可視化するためのツールが求められていることもわかります。こうしたツールでは、所有や管理を行えない外部のネットワークや環境も確認できなければなりません。

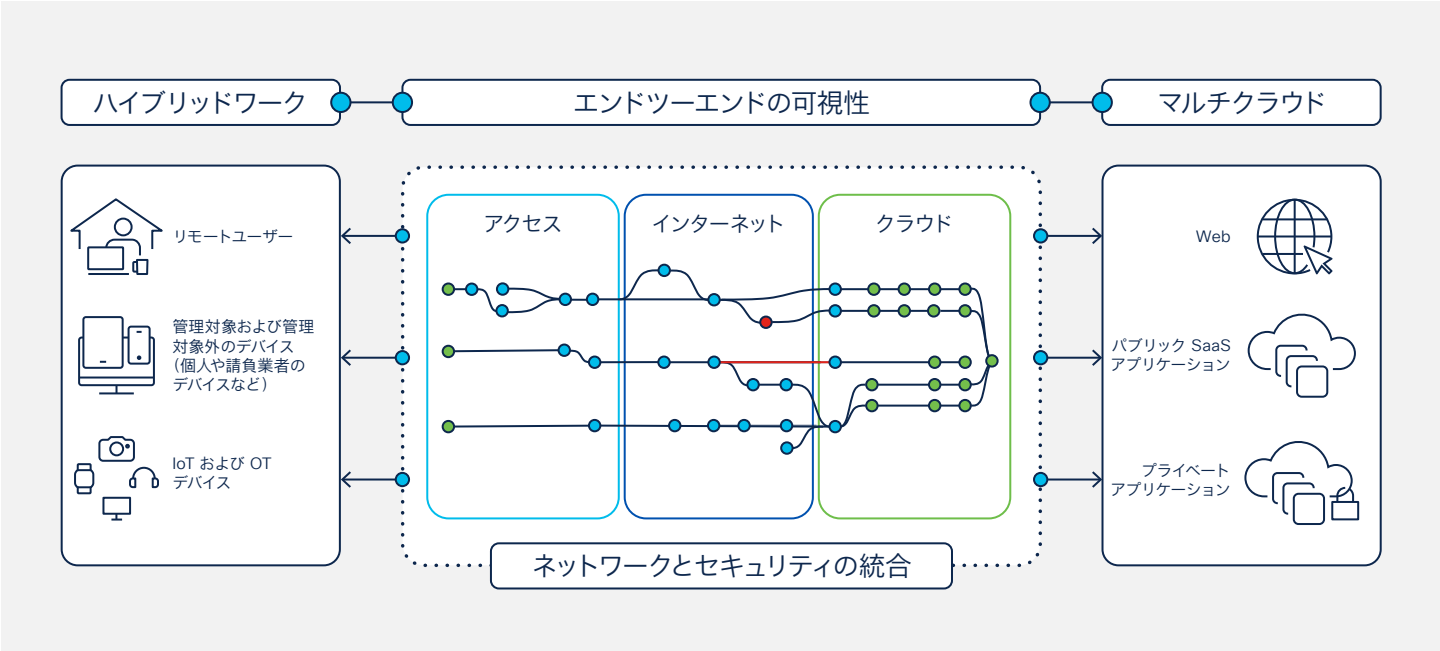


図 7. 分散環境は、インターネットを介して接続される。こうした複雑さの増大に対処するには、エンドツーエンドの詳細な可視化が必要

The bridge to possible

要点

クラウドは新たなデータセンターとして、そして、インターネットは新たなネットワークとして機能しており、クラウドサービスがアプリケーションの多くを占めるようになりました。そうした中でも**グローバルなインターネットの正常性**と上位の SaaS アプリケーションのパフォーマンスを把握できれば、ユーザーに影響の及ぶ重大なネットワークやアプリケーションの問題が予期せず発生した際に、それらを事前に検出し修正できます。

エキスパートの見解

インターネットを新たなインフラストラクチャ バックボーンと捉える。

「デジタル体験のサプライチェーンは、1 つのドメインから、マルチベンダーの連携システムおよびネットワークへと姿を変えました。ユーザーはどこにでも存在しています。アプリケーションは、俊敏性重視で設計され、API と分散型マイクロサービスが基盤となっています。そうした中、求められているのは、多数のアプリケーション、サービス、クラウド、ネットワークで、シームレスな体験を実現することです。しかし、これらすべてを簡単には制御できなくなりました。

そのため、デジタル体験をモダナイズするには、可視化とアシュアランスにこれまでとは異なるアプローチが必要です。そうしたアプローチを取ることで、ドメイン（家庭、オフィス、クラウド、インターネット）に関係なく、サービス中断を素早く検出して診断し、その結果をインフラストラクチャおよびネットワークの問題に関連付けることができます。このためには、適切なデータに適切なタイミングで容易にアクセスできる必要があります。また、そうしたデータの収集および関連付けを、内部のアプリケーション、ネットワーク、インフラストラクチャの各運用に対し、また、接続されているエコシステム内のサードパーティプロバイダー環境に対しても行えなければなりません」

シスコ ThousandEyes
製品管理担当 VP
Joe Vaccaro

The bridge to possible

重要なガイダンス 6：リアクティブ運用からプロアクティブ運用に移行して、アップタイムとパフォーマンスを向上させる。

予測分析は、Intelligence for IT Operations（AIOps）のさまざまなツールの 1 つとして、ますます注目されるようになりました。これにより、IT 運用全体の簡素化、迅速化、効率化が可能になります。

ビジネス運営上、拡張ネットワークが不可欠だとしても、サービスの品質低下やダウンタイムはユーザーにとって耐え難いものです。そのため IT 部門では、問題をプロアクティブに特定し修正できる仕組みが検討されています。この仕組みがあれば、ユーザー体験に影響が及ぶ前に問題に対処できます。

クラウドベースの管理プラットフォームが登場したことで、これまで以上に多くのソースからリアルタイムまたは過去のテレメトリを利用できるようになりました。人工知能と機械学習（AI/ML）技術を使用した予測分析モデルがさらに進歩していますが、これを活用すると、そうしたリアルタイムまたは過去のデータに基づいて実用的なインテリジェンスを導き出すことができます。これにより、データのパターンを把握して、問題の正確な予測と修正を行い、ネットワークへの影響を未然に防ぐことができます。こうしたモデルの能力は、継続的なフィードバックループを通じて受け取ったデータを学習することで、徐々に高めることが可能です。

プロアクティブな IT 運用がとりわけ重要となるのは、分散型クラウドアプリケーションにアクセスする分散型ユーザーに一貫した高品質サービスを提供する場合です。調査回答者は、これが将来における重要な方向性を示していると考えており、47% が今後 2 年間、予測ネットワーク分析を優先的に導入してクラウド接続を改善するとしています。

回答者の 47% が今後 2 年間、予測ネットワーク分析を優先的に導入してクラウド接続を改善するとしています。

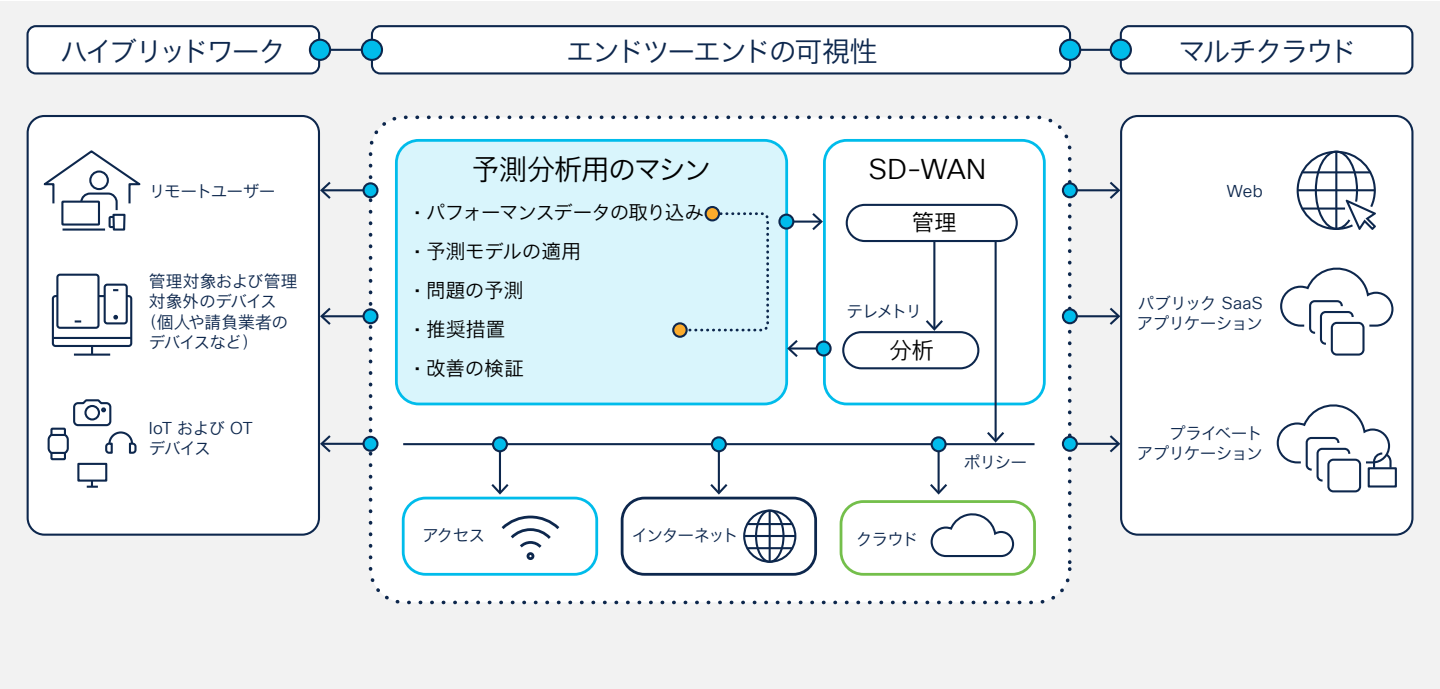


図 8. 予測分析を SD-WAN 管理と統合すると、ネットワーク品質の低下を特定および防止し、ユーザー体験への影響を未然に防ぐことが可能

The bridge to possible

要点

インターネットの変化や発展が進むと、デジタル体験の速度、コスト、品質のバランスが悪くなります。そのため、予測モードとプロアクティブな運用ワークフローを導入し、継続的なデータフィードバックループによってそれらを徐々に最適化する必要があります。同時に、インフラストラクチャの柔軟性とレジリエンスも高めなければなりません。

エキスパートの見解

予測分析の登場は、IT の現場でニーズが生じ、実現する技術が整ったことによる。

「従来のリアクティブな運用モードでは、トラフィックを代替パスに再ルーティングできますが、これは、問題（多くは、接続の問題やサービスの低下が原因）を検出した後でのみ可能です。予測分析がきわめて有用な理由は、テレメトリ、統計データ、AI/ML ベースのコンピューティングモデルを使用して、潜在的な問題を発生前に予測できる点にあります。クラウド中心の環境での問題予測は本質的に不可能です。そのため、いかに推奨アクションを自動的に提示したり、トラフィックをプロアクティブにリダイレクトしたりできるかが、パフォーマンスの最適化と、システムのダウンタイムによるリスクの軽減を行うための鍵となります。そうした能力が組織に利益をもたらします。ユーザー体験が向上し、IT 担当者がリアクティブなトリアージではなく戦略的イニシアチブに集中して取り組めるようになるからです」

シスコ ThousandEyes
エンジニアリング担当 VP
Murtaza Doctor

The bridge to possible

まとめ

リモートワークとハイブリッドワークの両方がすでに定着しており、マルチクラウドの導入も加速しています。しかし、広範囲に分散化した従業員、デバイス、アプリケーション向けにセキュアな接続環境を常に提供することが、いまだに課題となっています。その要因は、脅威の影響範囲が拡大し、ネットワーキング、クラウド、セキュリティの各チームで使用されるツールや技術が複雑になっていることです。

こうしたチーム単独では、そのような接続やセキュリティの課題に対処したり、自社の競争力維持に必要なデジタル体験と俊敏性を確保したりすることはできません。非常に多くの IT リーダーがそれを理解しており、ネットワーキング、クラウド、セキュリティ技術を積極的に統合すると同時に、革新的な運用モデルをテストし、変化し続けるこうしたニーズに対応しようとしています。

そのための明確なアプローチの 1 つが SASE への移行であり、実際に、調査回答者のほぼ半数が、今後 2 年にわたって、適切に統合された SASE アーキテクチャを展開し、ブランチとリモートクライアント向けに接続環境を提供するとしています。SASE を導入すると、IT 部門での体験がこれまで以上に簡素化され、セキュリティも向上します。なぜなら、分散化した従業員と顧客がクラウドアプリケーションに安全に接続できる大規模な環境を簡単かつ柔軟に提供できるからです。クラウド主導の自動化とネットワークインサイトの取得が可能なネットワーキング プラットフォームとセキュリティ プラットフォームを組み合わせることで、緊密に統合されたワークフローが実現し、NetOps チームと SecOps チーム間の連携も向上します。

クラウド中心の SASE モデルを導入すると、データの力を活用し、一貫したユーザー体験提供に不可欠なエンドツーエンドの可視化や予測分析といった機能を得ることができます。

自社のビジネスおよび技術の優先順位に基づいて、SASE 導入に着手するさまざまな方法をご検討いただけます。

SASE の詳細のほか、SASE 実現の取り組みに役立つシスコのソリューションについてご説明します。

このレポートの内容

『グローバル ネットワーキング トレンド レポート』は 2023 年 2 月にまとめられ、北米、中南米、アジア太平洋、西ヨーロッパの 13 ヵ国で実施された調査に基づいています。

2023 年のレポートでは、クラウドサービスを使用している組織でネットワーク運用を専門とする方々からの調査データを紹介しており、そうしたデータを使用して、マルチクラウド環境がネットワークの技術および運用の優先順位、志向、選択にどのように影響しているかについて、インサイトを提示しています。

このレポートで参照している調査データは、シスコが S&P Global Market Intelligence 傘下の 451 Research 社に委託して収集したものであり、分析はシスコが行っています。

このレポートでは、独立した Web 調査の一部を紹介しており、この調査は、クラウドコンピューティング、DevOps、エンタープライズ ネットワーキングに携わる世界中の意思決定者およびプロフェッショナル 2,500 人を対象に実施されました。

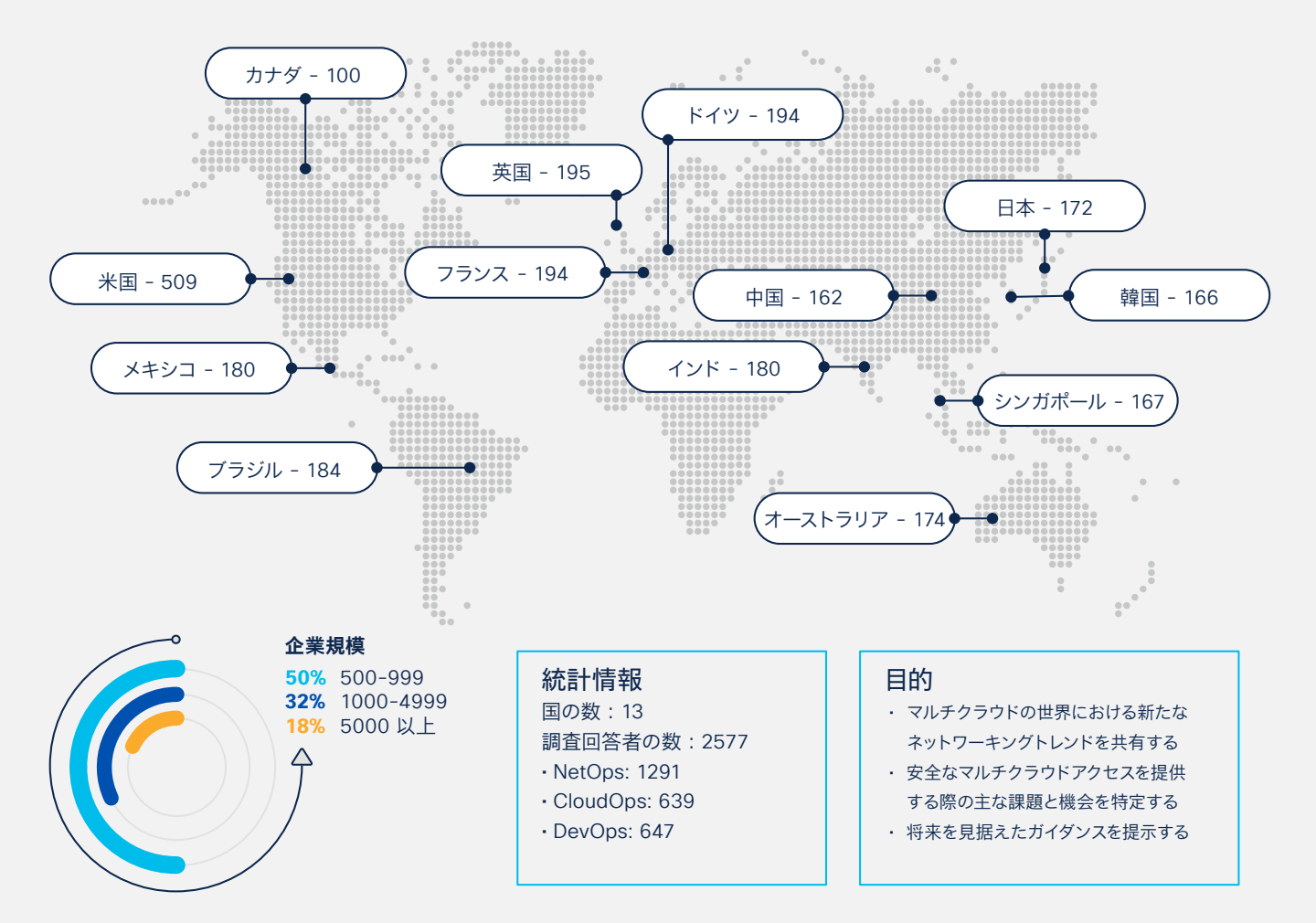


図 9. シスコ『グローバル ネットワーキング トレンド』（2023 年版）の調査における調査方法と目的