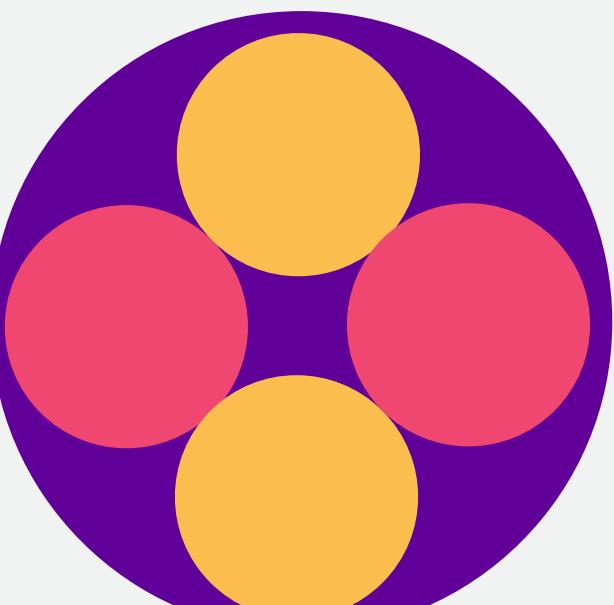
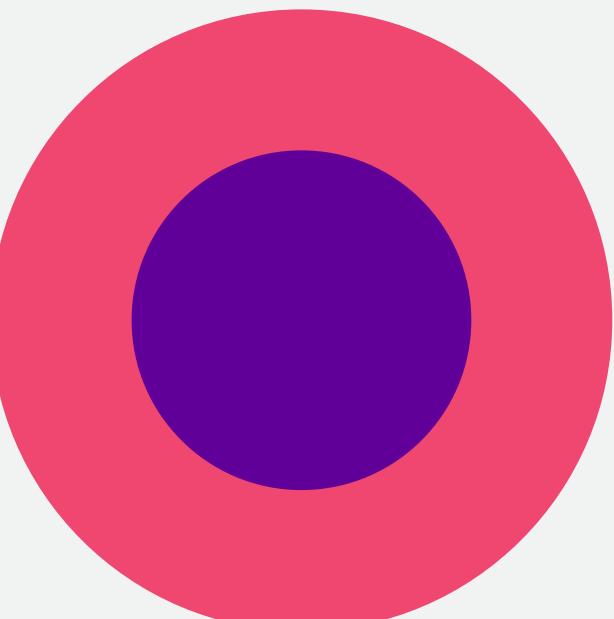


colt

# 境界線の無い セキュリティ対策

## SASE

構築を成功に導くガイドライン





今や、ネットワークに垣根はありません。リモートワークが可能となり、重要なシステムはクラウド化するなど、ネットワークには従来の境界線が存在しなくなりました。企業アーキテクチャにとって、このような柔軟なアプローチは着実にニューノーマルになりつつあります。クラウドベースで境界線が曖昧となった企業アーキテクチャの将来を見据えるにあたり、ビジネスリーダーには向き合わなくてはならない多くの課題があります。

広く分散化されたデジタル資産は、サイバー攻撃の脅威にさらされたり、サイロ化によるサポートの限界に直面する恐れがあります。リモートで働く従業員が基幹業務システムにアクセスできなかったり、ハッカーがネットワークにアクセスを試みたり、分散化された資産の問題を解決することは、CIOにとって頭痛の種となります。堅牢なセキュリティガバナンスやコンプライアンスと、日々の業務遂行のためのアプリケーションや効率的なデータ活用とのバランスをとりながら、広く分散化されたデジタル資産のリスクを管理するには、どうすればよいでしょうか。

CIO、IT戦略決定者、および経営者にとって、会社の資産を保護することが最優先事項でありながら、各アーキテクチャに付随するリスクや管理がそれぞれ異なることを考えると、あらゆるビジネスリソースへのアクセスを一つに集約したネットワークやセキュリティで管理することが最適と言えます。すべてを解決する方法は存在しませんが、SD WANとSASEを組み合わせたデジタルインフラストラクチャの構築によって、信頼性の高いアクセス、堅牢なセキュリティ、リモートサポートを実現し、さらにビジネス 資産へのアクセスを保護しながら、境界線なくビジネスに携わるすべてのユーザーに必要なパフォーマンスを提供できます。

## SD WANとSASEの概要

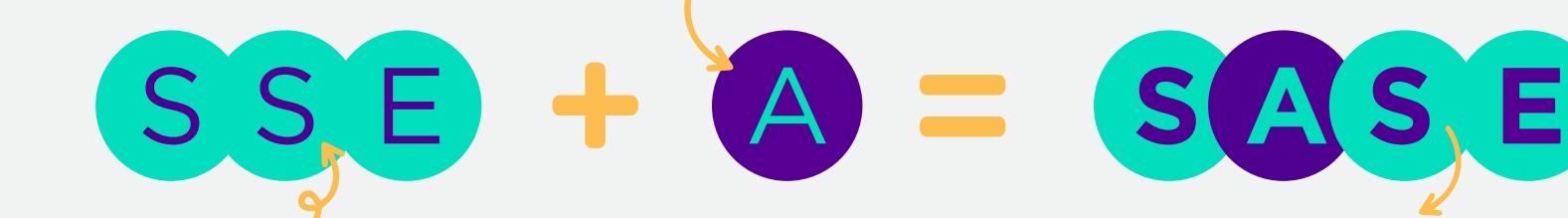
業界調査企業のGartner社が提唱した概念では、SASE（Secure Access Service Edge / セキュア アクセス サービス エッジの略）とは、柔軟なプログラムを可能とする広域ネットワーク（WAN）とクラウドベースのセキュリティ管理の両方を同じシステム内で提供するアーキテクチャを提唱しています。従来の構成では、組織のさまざまな部分に個別のセキュリティシステムを「後付け」していましたが、この新しいモデルでは、クラウドベースのコンピューティングでデータや通信を制御できるメリットを活かしつつ、システム自体に包括的な保護機能が組み込まれています。

SD WAN(Software Defined Wide Area Networkの略)は、地理的に離れた場所に分散している企業にとって最適なアプローチと認識されています。この技術は、従来ネットワークをホストしていたハードウェアからネットワーク管理を切り離し、クラウドベースのプラットフォームを通じてエンドツーエンドのセキュリティパフォーマンスを最大限に提供し、企業のコスト削減を可能とします。

次に、SASEモデルの完全化のためにクラウドセキュリティが追加され、「SSE」とも呼ばれるようになりました。このSSE（セキュリティサービスエッジ）もまた、Gartner社が提唱した用語で、ゼロトラストなどの包括的な現代のセキュリティポリシーを提供するセキュリティ技術および機能を指します。これにより、Webサイト、アプリ、APIなど、企業のリソースとサードパーティシステム両方のアクセスを統制し、セキュリティを管理します。



A (アクセス) = ネットワーク



セキュリティサービスエッジ

SASE=同一システム内でクラウドベースのセキュリティ機能を備えた広域ネットワーク (WAN)

このように、デジタル・トランスフォーメーションを加速させる選択肢が広がると、セキュリティ、法規制、ハイブリッドワーク環境など考慮すべき事項も増えてきます。

[こちらの動画（約7分）](#)では、ColtのセキュリティプロダクトマネージャーであるMark Balesが、これらの課題とどう向き合っていくべきか解説しています。

## SASE& SSEはどのような価値があるでしょうか？

こうしたあらゆるテクノロジーは、ファイアウォールのような従来のシステムに比べ、ネットワーク保護を進化させています。ネットワークがオンサイトでホストされていた時代には、堀で守るようなセキュリティ戦略でビジネスを効果的に保護できましたが、今日での境界線のないビジネスにはそれ以上のものが求められます。

デジタルインフラストラクチャの分野において、各ベンダーが専門とする領域は異なります。セキュリティソリューションに受賞歴のあるベンダーや、ネットワークスペシャリストを自称するベンダー、さらにはオールインワンのSASEパッケージを提供し、完全な「Ground to Cloud」を実現するベンダーも存在します。

ネットワークとビジネスが共に成長するにつれ、ITマネージャーがデジタルインフラストラクチャを進化させる上での選択肢も増えてきます。シングルベンダーのSASEソリューションを選び、スタック構成全体を一社のサプライヤーに統一するか、ベンダー各社の最高の技術を集めて、自社のビジネスに適した、真の「ベスト・イン・ブリード」のソリューションを構築するか、十分に検討することが重要です。

#Cybersecurity

Learn about  
**SASE & SSE**



2023年は、AIの話題から逃れることは不可能であり、Colt発行の2023年最新版レポート：[【デジタルインフラストラクチャへのインテリジェンス導入】](#)では、IT戦略決定者の47%がすでに何らかの形でAIを採用していることが報告されています。SASEは、ビジネスにAI人工知能を導入する上で完璧な基盤となるものです。AIという業界を変革しつつある技術を導入する場合、自社の将来のデジタルインフラストラクチャ計画がAIの導入にどう対応できるか検討する必要があります。



## SASEの方向性

市場調査企業のGartner社によると、SASE市場は、2022年の70億ドル規模から、2027年までに250億ドル規模（年平均成長率29.4%）へと成長する見込みです。つまり、企業が一社もしくは複数のベンダーからSASEソリューションを導入する規模は、増加の一途を辿っているといえます。どちらが理想的なソリューションを提供してくれるかについて、経験・実績豊富なデジタルインフラストラクチャ企業にアドバイスを求めるのもよいでしょう。

最善の対策を決定する際の参考として、以下ではシングルベンダーとマルチベンダーのそれぞれのSASEに関する特徴や検討事項について解説します。

## オプション1：シングルベンダーからの導入による合理化 メリット

シングルベンダーからSASEソリューションを導入すると、必要な機能のすべてがひとつに合理化されたパッケージで提供されます。予算やシステムの規模が限られている企業の選択肢となり、詳細な構成の仕組みを深く掘り下げる手間を省き、SASEが提供する更新プログラムをそのまま利用することができます。

シングルベンダーからのSASEでまとめることで、必要な投資額を引き下げることができます。ネットワークの各レイヤーのソースが一つのため、通常よりコスト効果の高いソリューションが期待できます。同じベンダーから提供されるスタッフは、すべてがシームレスに連携するよう構成されているため、マルチベンダーソリューションにありがちな非互換性の問題も回避できます。

また、SASEネットワークに関する担当窓口が一つとなり、専任チームがすべての問い合わせや懸念事項に対応するので、請求処理、トラブルシューティング、メンテナンスプロセスがシンプルになります。すべての問題をシングルベンダーに委ねるので、ITチームは解決までの時間を取られる心配がありません。

シングルベンダーのソリューションは、ネットワークの複雑さの軽減、帯域の効率化を実現します。また、インフラストラクチャを一つのベンダーが管理することで、ベンダーの担当者が一か所に配置され、移動にかかるコストも削減されます。ネットワーク接続距離が短いことは、セキュリティの向上、

信頼性の強化、遅延の短縮にもつながり、すべてがネットワーク機能にメリットをもたらします。

### 考慮すべき事項

シンプルさは魅力的ですが、シングルベンダーの場合、市場における「ベスト・イン・ブリード」な選択肢を放棄することになります。シングルベンダーの場合、特定の分野に弱点がある可能性や、ビジネスのニーズが変化した場合にアップグレードが必要になる可能性があります。その結果、長期的に見て継続的な投資が必要となります。

シングルベンダーに一本化した契約はプロセスを簡素化しますが、通常は長期契約となるため、実質的な拘束となります。サプライヤーの変更も複雑なプロセスとなるため、契約に署名をする前に、企業が、日々進化し柔軟性のあるSLA（サービスレベルアグリーメント）がもたらすメリットを必要としていないか考慮する必要があります。

シングルベンダーの場合、何らかの理由で障害が発生すると企業のビジネスにダウンタイムが生じる恐れがあります。そのような場合に企業はどう対処するか、事前に検討しておく必要があります。

### シングルベンダーの活用戦略

デジタル・トランスフォーメーションへの一番の近道と言えるシングルベンダーSASEは、以下の場合に適しています。



## オプション2：マルチベンダーの活用で柔軟なSASEの構築 メリット

マルチベンダーによるSASEインフラストラクチャは、ベスト・イン・ブリードのアプローチにふさわしい最も包括的で機能豊かなソリューションとなります。予算が潤沢な企業の場合、最上位の製品やソリューションを選択できるということは、スタックのポテンシャルを最大化できることを意味します。あるベンダーのSSEと、別のベンダーのネットワークを選択することで、「テーラードフィット」して長く使える構成を実現できます。

SASEを導入する場合、ネットワークチームとセキュリティチームが自分たちの責任領域で利用可能な機能について合意する必要があります。複数のベンダーから導入することで、どちらかのチームが導入に関して妥協をする必要性が低減します。このことは、当初から完成形に近いシングルベンダーのパッケージと比較して優位な点です。

マルチベンダーソリューションは、時間の経過とともに再構成することが非常に容易です。ネットワークの一部のポテンシャルが十分に発揮できていなかつたり、あるベンダーのセキュリティ製品では新しいセキュリティ態勢の展開が難しい場合、新しいサプライヤーや製品に入れ替えるという選択がしやすくなります。

ネットワーク構成の中の一つのレイヤーにダウンタイムが発生しても、インフラストラクチャ全体がダウンすることはありません。マルチベンダーSASEは冗長性の確保や生産性の向上につながります。問題が他と切り離されているため、

ビジネス全体に影響が及ぶことはありません。たとえばネットワークに障害が発生しても、セキュリティ態勢が危うくなることはありません。

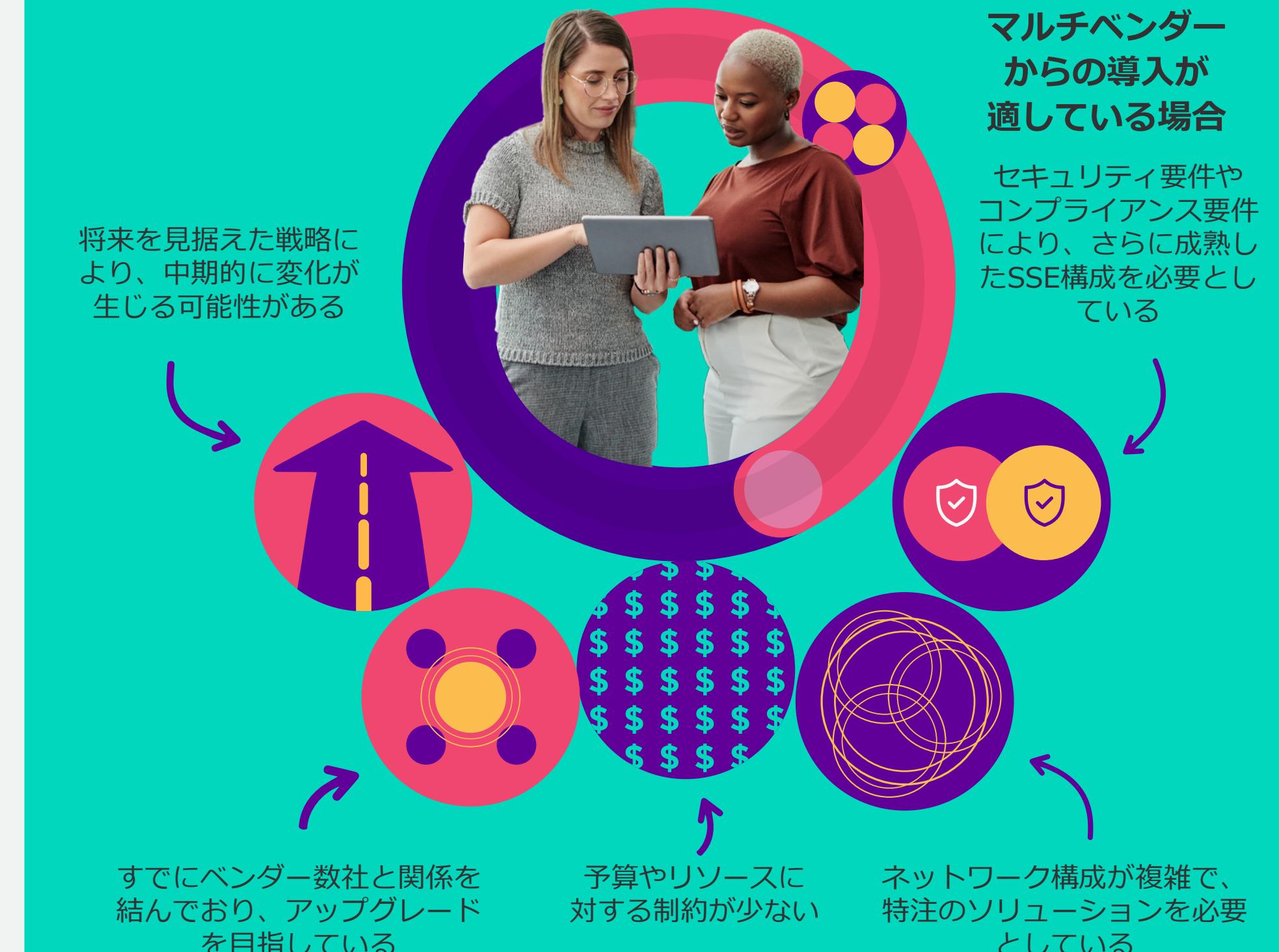
### 考慮すべき事項

マルチベンダーSASEは、デジタルインフラストラクチャの頂点ですが、複雑になりがちな個々の製品の連携にうまく対処するために、企業のITチームや選択したサプライヤーの知識と専門技術が必要です。通常、各製品はサードパーティを想定して設計されていないため、ベンダー間の互換性については、注意深く計画する必要があります。インフラストラクチャを確実に管理できるよう、エンジニアに必要なスキルを身に着けさせることが必須要件となります。

同様に、複数のベンダーの製品を相互運用することは、テクノロジーのアップデートや進歩の足並みを揃える必要があります。SASEの構成要素の一部が他に悪影響を及ぼさないよう、すべてのベンダーの製品アップデートについて、最新情報を漏れなく確認する必要があります。

市場屈指のネットワークテクノロジーを運用するということは、求められる管理水準も高くなります。ベンダーが複数になるため、ポータル、SLA、請求処理要件も複数となります。その場合、Coltのような企業に代わってベンダーとの関係や統合の管理を専門とするサービスプロバイダーが存在するため、運用タスクをこれらのサービスプロバイダーに任せることで、企業は本来の事業に集中できます。

### マルチベンダーの活用戦略





## 境界線の無いセキュリティ対策

どのソリューションが最適かは、企業のニーズやデジタル・トランスフォーメーションの進行具合に応じて異なります。企業がデジタルインフラストラクチャの進化に向けて最初の一歩を踏み出したばかりなのか、あるいはすでに高パフォーマンスなネットワークを運用しており、新たな課題に対応するために追加のセキュリティを必要としているのか、というように状況によって異なります。

成長を始めたばかりのビジネスを支える効率的なソリューションを求めている場合、シングルベンダーからの導入手法が最適です。この方法では、ソリューションを一つのソースから入手するため、導入するコンポーネントは相互運用可能に設計されています。また、コスト削減も可能となり、将来のビジネス成長にメリットをもたらします。

トランスフォーメーションの道筋を進んでおり、費用上の制約があまりない場合は、インフラストラクチャのスタックごとにサプライヤーを選ぶ「ベスト・イン・ブリード」のアプローチをとるマルチベンダー活用戦略が理想的です。

どんな道筋であろうと、企業がSASEを導入する際、その旅路を案内するサービスプロバイダーが一社いるだけで、導入のハードルを乗り越えやすくなります。企業は現在、規制遵守の厳しさなど、さまざまな要素を考慮する必要があります。しかし、サービスプロバイダーがSASEプロジェクトを専任でサポートすることで、企業は成功に向けて初日から万全の態勢で臨むことができるでしょう。

## Coltが選ばれる理由：境界線の無いネットワークへ

Coltはネットワークのポテンシャルを最大限に引き出すため、厳選された最高クラスのソリューションを提供するベンダーを選定しています。Coltの30年に及ぶ経験とベンダーの専門技術との相乗効果により、デジタルユニバースの力をいつでも、どこでも、あらゆる手段を駆使してお客様にお届けします。つまり、トランスフォーメーションに向けたお客様の計画がどのようなものであれ、Coltがお客様をサポートします。

また、Coltのエキスパートチームは、ソリューションエンジニア、サイバーセキュリティ専門家、およびネットワークスペシャリストから構成されています。このチームは、お客様が適切な選択ができるよう案内し、デジタル・トランスフォーメーションの旅路で進むべき方向を決めるサポートをします。ビジネスにはそれぞれ固有の要件があります。お客様の選択を支援することは、Coltのエキスパートが最も得意とするところです。

Coltは、企業のITチームが新しいネットワーク構成について最適な選択ができるようサポートし、インフラストラクチャを効果的に社内管理できるよう導きます。パフォーマンスが最適化されていないネットワークでは、そのポテンシャルを完全に発揮することはできません。Coltは、お客様のビジネスが業界で最も効果的なテクノロジーを導入し、最大限に活用できるよう後押しします。

本レポートやColtサービスに関する詳細は以下よりお問合せください。

<https://www.colt.net/ja/contact-us/>

営業代表：03-4560-7100

メール：[asia-sales-online@colt.net](mailto:asia-sales-online@colt.net)

詳細は以下へお問い合わせください。

WEBフォーム：<https://www.colt.net/ja/>

