2023年版

アプリケーション戦略状況レポート

目次

はじめに

「And」の力を取り入れる

今日のグローバル文化における成功とは、地理的な境界やその他の境界を越え、衝突を克服し、多様性の溝を埋め、人、アイデア、機会、資源を集結させることです。これは個人レベルにも当てはまり、私たちの多くはさまざまな役割をこなしています。私たちは職業人であり、家族であり、隣人であり、趣味人であり、国家市民であり、そして多文化なグローバルコミュニティの一員でもあります。同様に、企業組織でも、広範囲に広がる資源や人材を結びつけ、相補的な目的を果たしています。あらゆる役割を取り入れながら成長するために、個人や企業組織は、アプリケーションやAPIによって提供される迅速かつ効率的なデジタル体験によってますます支えられる行動の流暢さ、つまりアジリティを必要としています。

ハイブリッドITは困難だが持続可能

現在、このようなアプリケーションの40%は最新のアプリケーションであるか、または最新のコンポーネントを使用していますし、10社に9社の企業組織が、さらなる最新化、ITスタックの効果的な統合、エッジで可能なパフォーマンスとエンゲージメントの活用のためにデジタルトランスフォーメーションに取り組んでいることはニュースにもなりません。第9回目となる「F5アプリケーション戦略現状」調査におけるその他の結果には、これより驚くものがあり、ビジネス戦略の指針となるインサイトや議論を引き起こす可能性があります。

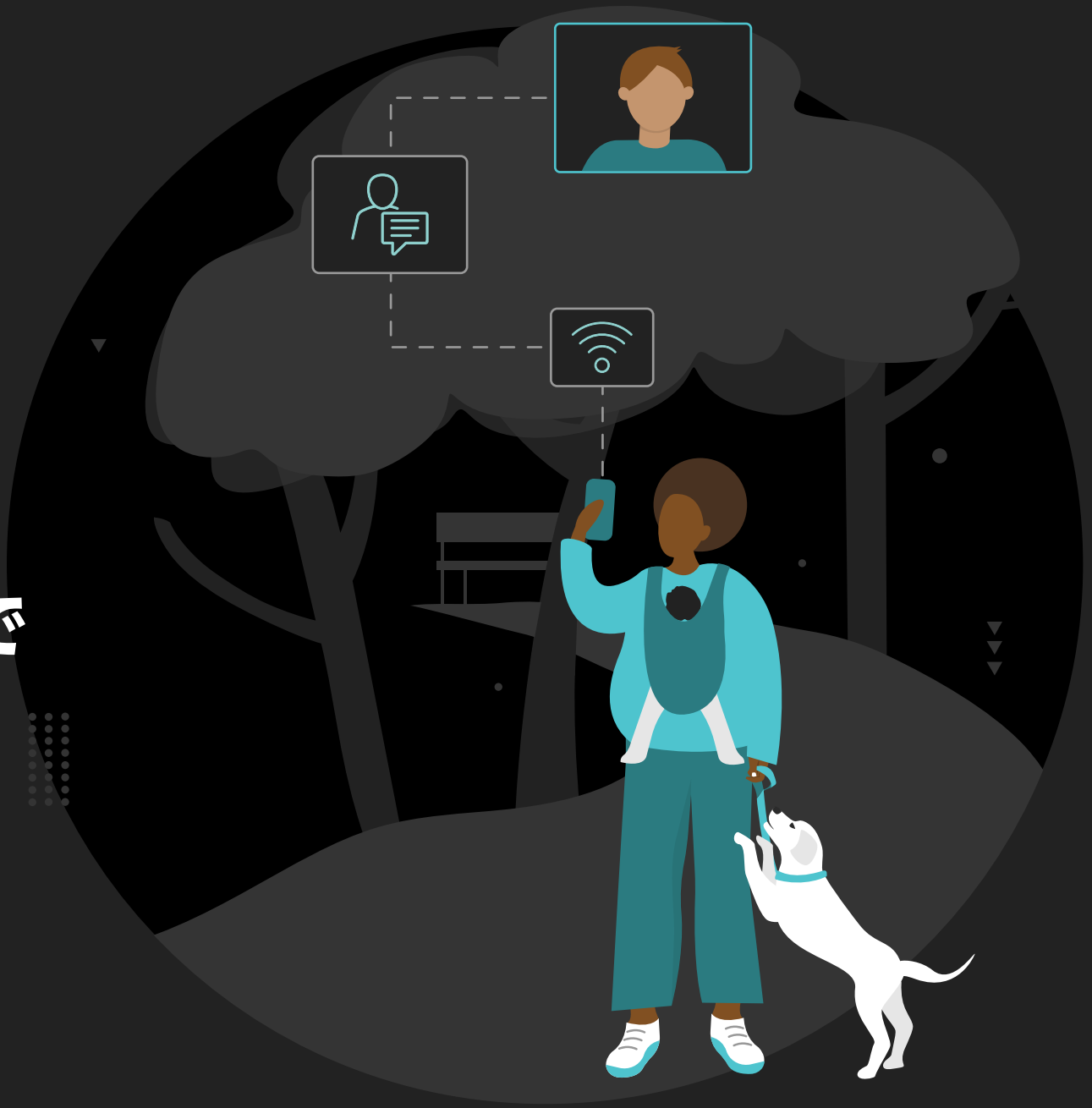
今年、特に新たにわかったことは、コンピュート、ネットワーク、ストレージ、アプリケーションなどの機能がコア、クラウドおよびエッジの環境全体に広く分散され、平均的なITスタックがハイブリッドであり続けるということです。「ハイブリッド」はクラウドに限ったことではありません。企業組織は今後も、複数の異なる技術スタックを管理し、異なる世代のインフラストラクチャやアプリケーションをサポートすることになります（身近な例では、電子メール、テキスト、アプリの時代でも、数十億ドル規模のファックス市場が存在し続けています）。

エンタープライズアーキテクチャを担当するCIOの多くは、このバランスの難しさを認識しています。このようなCIOは、デジタルビジネスの実現と、顧客の期待に応える新しい技術の導入を同時に実現しながら、リソースの制約、技術的負債の課題、そして安定性、レジリエンシー、効果的な変更管理に対する企業組織のニーズにうまく対応しなければなりません。その結果、ITプロフェッショナルは、異なる動的なシステムや技術にこれまで以上に精通していなければなりません。

しかし良い面もあり、ハイブリッドITは、持続可能であることが証明されています。私たちの生活の他の多くの側面には、「どちらか」ではなく「どちらも」という語が重要であるハイブリッドな役割や関心が存在します。ビジネスの速さと長期的な成長は、複雑なハイブリッド環境の管理を簡素化しながら、場所を越えてアプリケーションとAPIを接続および保護する方法を見つけることに依存することになります。このような現実は、アプリケーションのセキュリティと提供の形を変えています。IT意思決定者を対象としたF5の最新の年次調査では、成長しつつあるアプローチ、特に、私たちが共有するハイブリッドな未来をリードする他の企業組織の状況を常に把握しなければならない理由とそのために必要なことが明らかになりました。

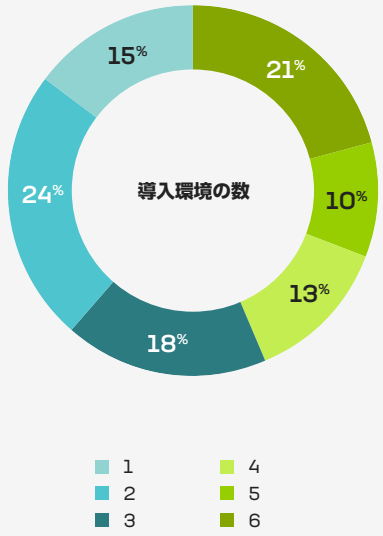
01

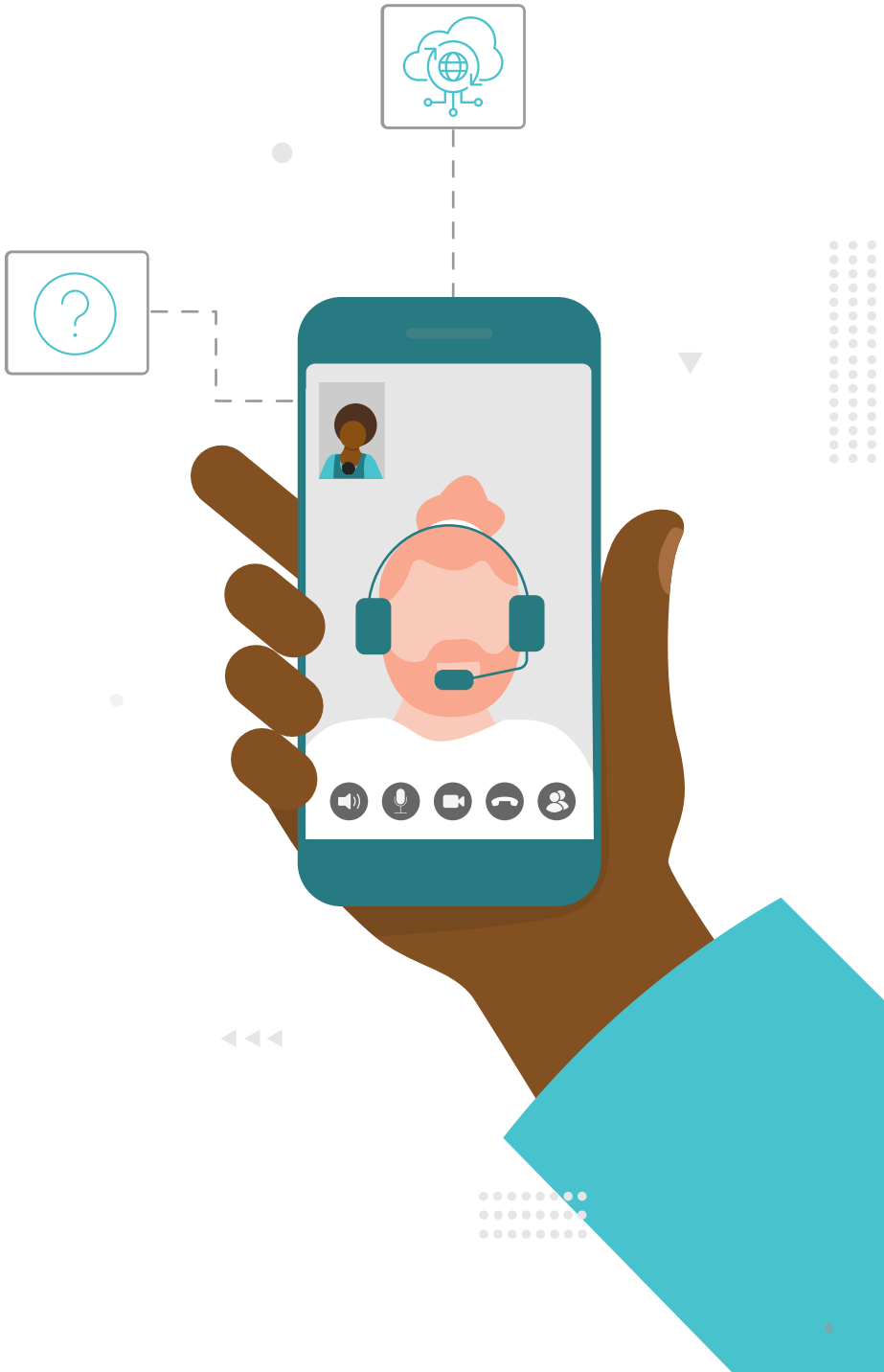
IT は無期限にハイブリッドであり続ける



本年度のデータは納得がいくもので、ハイブリッドITは今後もあり続けます。調査回答者によると、アプリケーションのうち、単一環境に導入されているのはわずか15%でした。大多数のアプリケーションはより広く分散していて、5分の1以上は6つの異なる環境でホストされています。一般的に、アプリケーションのホスティングに関する意思決定は、アプリケーション固有の目標を達成するためにアプリケーションごとに行うため、企業組織は、すべてのアプリケーションに最適な単一の環境は存在しないと認識しています。オンプレミスのデータセンターが必要なこともあれば、1つ以上のクラウドのスピード、スケーラビリティ、効率性が必要なこともあります。

アプリケーションは広範囲に分散





パブリッククラウドの導入はユビキタスから懸け離れています。
また、パブリッククラウドへの憧れ（と誇大広告）が落ち着きつつあることも判明しました。5年前の2018年では、74%の調査回答者が、自社アプリケーションの「半分まで」を「クラウド」に導入する予定だと答えていました。その2年後の2020年、その計画を実行に移した企業組織は約4分の1程度でしたが、クラウドコンピューティングは依然として、最も注目の技術トレンドで断トツの1位に挙げられていました。
さらにその3年後、現在クラウドに導入しているアプリケーションがあると答えた回答者は、全体の半数弱（48%）であり、平均的な企業組織では、アプリケーションポートフォリオのうち15%しかクラウドに導入していません。パブリッククラウドの導入が制限される背景には、大規模なデータ管理、セキュリティ、コストに関する懸念があると考えられます。

パブリッククラウド ユースケースのトップは事業継続

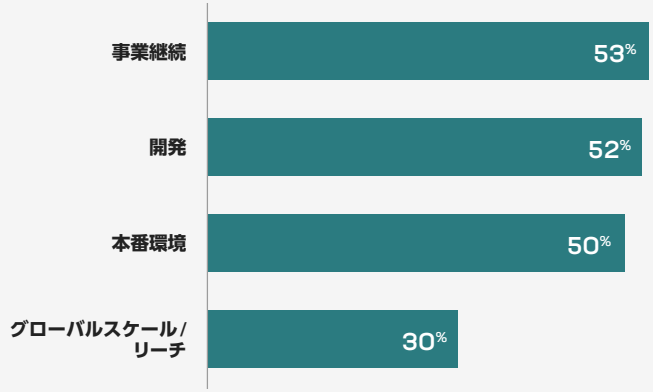
パブリッククラウドは、特にバックアップやビジネスレジリエンスの目的で、多くの企業にとっての選択肢の1つであり続けていますが、必ずしもアプリケーションホスティングにおける最初の選択肢になっているわけではありません。この点ではオンプレミス導入が優位にあり、統合の期間を経て、振り子が戻り、オンプレミスの導入が再び増加しています。

オンプレミスの導入は、今日のアプリケーションアーキテクチャの基盤であり続けています。
従来のオンプレミスデータセンターでホストされるアプリケーションの割合は、何年も減少が続いていましたが、今回は2022年と比較して2ポイント増加し、37%になりました。オンプレミス導入の比率は全体の半分を超えていて、これは、多くの人がオンプレミスデータセンターをモノリシックな環境だと考えている一方で、現実には従来型とクラウド型の両方の環境がオンプレミスに存在するためです。パブリッククラウドやSaaSなど、その他の導入モデルは近年増加傾向にありますが、2023年にはそれぞれ横ばいまたは微減となっています。.

パブリッククラウドが実現するレジリエンスファースト

質問：
パブリッククラウド（IaaS）をどのように活用していますか？該当するものをすべて選んでください。

結果：
パブリッククラウドを利用している回答者の約半数において、トップのユースケースはバックアップと災害復旧でした。



オンプレミス回帰は、この傾向の1つの要因です。オンプレミス回帰は2年連続で高い割合で続いていて、3分の1以上（43%）の回答者が、アプリケーションを最近オンプレミスに戻した、または近々戻す予定であると答えています。アプリケーションをオンプレミスに戻したと答えた回答者の54%が挙げた最大の動機は、マルチクラウドの世界でのアプリケーションの乱立を抑制する必要があるということでした。

オンプレミス回帰の熱意は特に、金融サービス、電気通信、テクノロジー業界で高まっています。これらの業界は、複数のクラウドを運用している可能性が高く、さらに、オンプレミスでアプリケーションを効率的に自己管理できるスキルを備えている可能性も高いと考えられています。

導入モデルとして最も利用されるオンプレミス導入とその次の導入モデルには落差があります。プライベートクラウドは、平均的な企業ポートフォリオの17%しかホストしておらず、オンプレミスデータセンターの半分に過ぎません。

その後に僅差の16%でSaaSが続いています（ただし、これは技術的には消費モデルであり、導入モデルではありません）。全体像としては、オンプレミスデータセンターを中心としたハイブリッドな多様性を示しています。

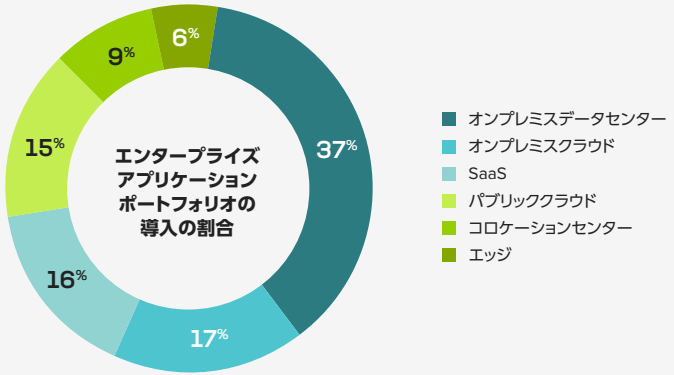
最新のアプリケーションアーキテクチャはどこにでもあります。

アプリケーションのアーキテクチャも混在しています。調査回答者の全員が、最新のアプリケーションの運用、SaaSの利用、またはその両方を行なっています。回答者によると、アプリケーションの導入場所に関係なく、平均してアプリケーションポートフォリオ（SaaSを除く）の3分の1以上（40%）が、モバイルアプリやマイクロサービスの利用を含む最新と表現できるようです。この割合は予想通り着実に増えていて、2025年には50%（おそらく60%）を超えると予想されます。しかし、現在ほぼ全員（95%の企業組織）がまだ、従来のアプリケーションも運用しています。その結果、企業組織の大部分（85%）が、多くの場合はさまざまなホスティング環境において、最新のアプリケーションと従来のアプリケーションの両方を管理および保護するという課題に直面しています。

マルチクラウド環境はあり続ける

質問：
現在導入されている（ご自身の）アプリケーションのうち、以下の導入モデルを利用している割合は約何パーセントですか？合計が100%になるように数字を入力してください。

結果：
アプリケーションのロケーションが多様的なことが標準的な状況です。



アプリケーションポートフォリオは時間とともに最新になる傾向があるため、最新のアプリケーションと従来のアプリケーションの両方を管理する企業組織の割合は減少すると予想されています。この割合は、2022年の88%がピークとなるかもしれません。しかし、最新化に慎重な方法で取り組むCIOは、ビジネスに付加価値を与え、ビジネスの優先順位と一致し続ける従来のアプリケーションをそのまま残しているため、すぐにゼロになることはありません。

従来のアプリケーションの廃止に関して、59%の回答者は、最新版を構築することで置き換えています。製造業や政府機関の企業組織は、アプリケーションを自社で構築する傾向が最も強いようです。一方、ヘルスケアを中心とする約46%の企業組織は、従来のアプリケーションをベンダーが提供するSaaSに置き換えています。事実、これらの企業組織は、最新化をアウトソーシングし、アプリケーションの構築を少なくして、導入を多くすることで、より早く価値を獲得しています。5社に1社の企業組織は、不要になったアプリケーションは廃止すると答えています。

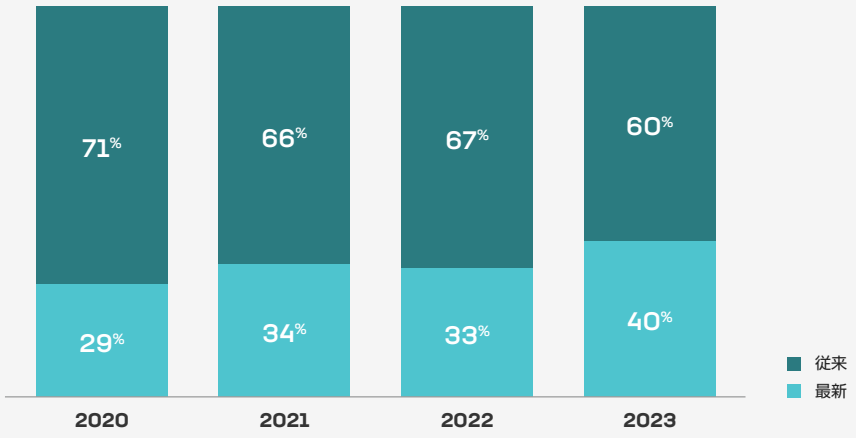
しかし、回答者の16%は、従来のアプリケーションを廃止する予定はないと答えています。このようなアプリケーションは、銀行や保険会社のアプリケーションのように、コアビジネスの機能を維持している可能性があります。エネルギー、ヘルスケア、電気通信などの業界では、規制要件の変化が少なく、技術が固定化しやすいため、最大33%の回答者が従来のアプリケーションを維持すると答えています。その結果、業界全体の平均的なポートフォリオに占める最新のアプリケーションの割合は、この10年で最高で85%近くとなる可能性があります。さらに、それらのかなりの部分は、従来のアプリケーションとのインターフェイスとしてのみ連携するマイクロサービスである可能性があります。

つまり、大多数のCIOは、これからもしばらく、ハイブリッドアプリケーションアーキテクチャと、ハイブリッド環境に分散した多世代アプリケーションを監視することになります。

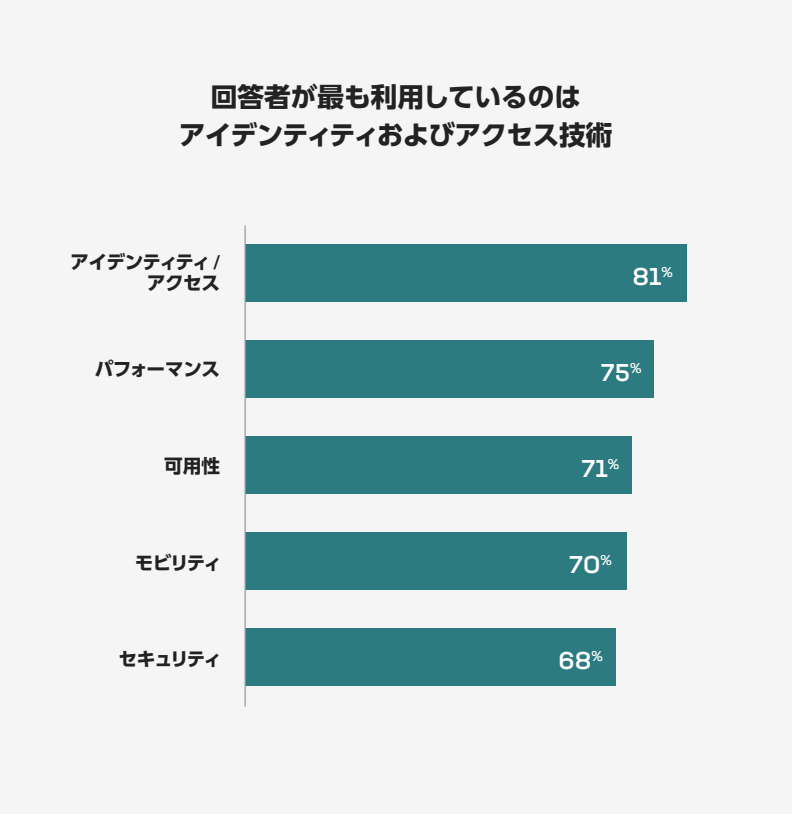
成長を続ける最新のアプリケーションアーキテクチャ

質問：
現在導入しているアプリケーションのうち、以下のカテゴリーに当てはまる割合は約何パーセントですか？合計が100%になるように数字を入力してください。

結果：
最新のアプリケーションアーキテクチャは、平均的なポートフォリオの半数に近づきつつあります。



アプリケーションのセキュリティと配信の技術も分散しています。
アプリケーションのセキュリティと配信をサポートする技術は、アプリケーションそのものと同様に、環境全体に分散しています。多くの場合、特定の技術（アプリケーションサービスと呼ばれることもあります）をどこに導入するかは、その目的によって決まります。さらに、環境自体が、理想的な技術やフォームファクターに影響を与えることもあります。たとえば、Webアプリケーションファイアウォール（WAF）ハードウェアは、オンプレミスデータセンターに最適かもしれませんが、クラウドに導入されるアプリケーションはSecurity as a Service（SECaaS）の方がより効率的に保護できるかもしれません。また、セキュリティサービスは、攻撃をすぐに止めればリソースの過剰供給を防ぐことができるため、できるだけユーザーの近くに導入することが最適です。しかし、レイヤー7ルーティングサービスは、アプリケーション自体のできるだけ近くに置くことが最適な場合があります。そのため、ハイブリッド環境では、多くの場合、重要なアプリケーションのセキュリティと配信の技術を複数導入することが理にかなっています。



アプリケーションセキュリティ技術は、クラウドに導入される可能性が特に高い

その結果、過半数（59%）の回答者が、このようなサービスをオンプレミスに導入していると答えていて、また同数の回答者が少なくとも1つをクラウドに導入していると答えています。クラウド導入は、特にセキュリティ技術で一般的です。しかし、アプリケーションのセキュリティと配信の技術をサードパーティのSaaS経由で提供することが増加していて、次に多い方法となっています。この方法は、約3分の1（30%）の回答者が使用していると答えていて、複雑化することも、制御性を低下させることもなく、クラウドやその他の環境でアプリケーションを成長および拡張できます。

アプリケーションがどこでホストされているかに関係なく、アプリケーションのセキュリティと配信の技術を使用することは、企業組織がデジタルトランスフォーメーションを進め、デジタルの速度と安全性や安定した運用とのバランスを図る中で、増加傾向にあります。SSL VPN、シングルサインオン（SSO）、IDフェデレーションなどのアイデンティティおよびアクセス管理（IAM）技術は、現在最もよく導入されているアプリケーションサービスですが、全体で導入されているさまざまなアプリケーションサービスの数は、2017年から2倍以上に増加しています。これは、提供するデジタルサービスが単にビジネスの顔ではなく、その心臓部（より正確には財源）であるアプリケーションがどれだけ重要であるかを示しています。

マルチクラウドの課題は残ります。しかし解決策はあります。
このようなハイブリッドで分散したアプリケーションのランドスケープにおいて、複数のクラウドで運用する回答者の10人中9人近くの方が、マルチクラウドのセキュリティ、パフォーマンス、コストに関する課題を挙げ続けているのは驚くべきことではありません。2023年におけるこれらの課題のトップは、ツールとAPIの複雑さであり、これは、異なる導入モデルに使用されるツールの標準化または相互運用性の欠如に起因します。一貫したセキュリティポリシーの適用は、2年連続で次点の課題であり、パフォーマンスの最適化がほぼ同数でこれに続きます。

APIの攻撃対象が増えることで、マルチクラウドの課題がさらに深刻化している

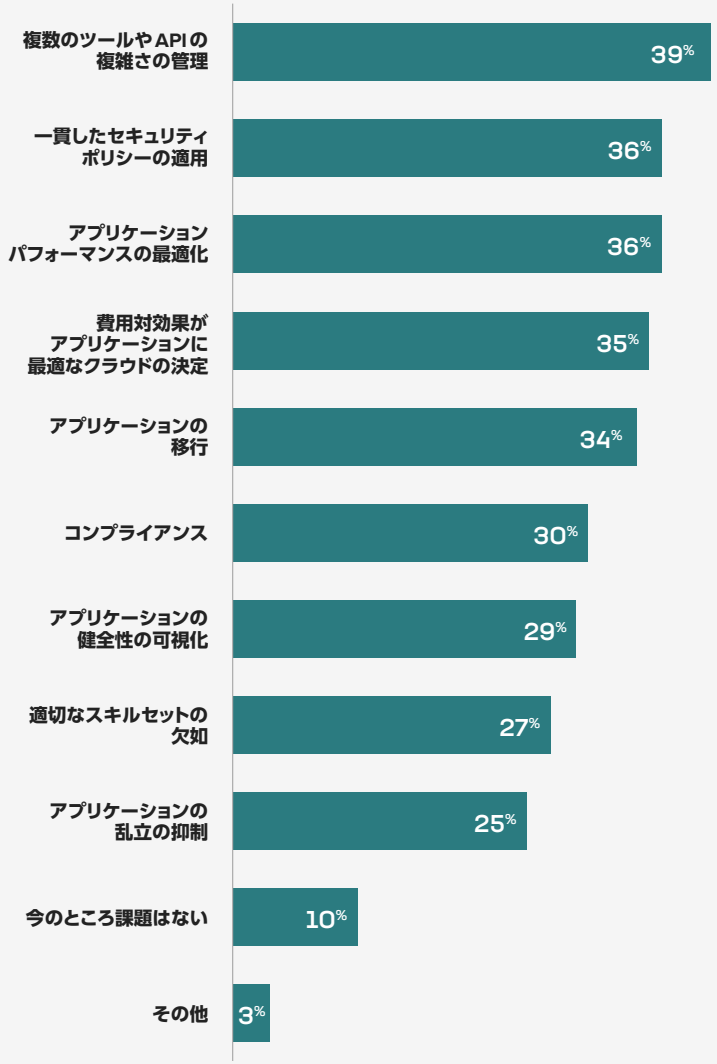
アメリカ大陸とヨーロッパ、中東、アフリカ（EMEA）の企業組織が、マルチクラウドネットワーキングを今後数年間で最も注目のトレンドとしたのは、間違いなく、こうした課題があるからです。しかし、他の地域や世界全体では、他のトレンドがこれよりやや上にランクしています。特に、アジア太平洋、中国、日本（APCJ）の回答者は、ITと運用技術の融合（IT/OT）により熱意を示しています。これは、グローバルな製造業の中心としてのこの地域の役割だと思われますが、効率性を高めるために機械制御と他のビジネスシステムをよりよく統合する必要があることも示しています。

マルチクラウドの現実を接続、保護、管理するために現在利用可能なその他のソリューションには、自動化の拡張、エコシステムのアプローチ、および環境に分散したアプリケーションのツールやポリシー実施を統合して簡素化を支援するパートナーなどがあります。一貫したセキュリティを提供する宣言型導入ポリシーは、保護をグローバルに拡大し、機能サイロ間の摩擦を取り除く上で役に立ちます。また、ハイブリッドITがなくなることはないため、マルチクラウドの管理を簡単にする同じソリューションが、ほとんどの企業組織にとって役立つことが証明されていきます。

マルチクラウドの課題トップは複雑さ

質問：
現在、複数のクラウドにアプリケーションを導入する上で、どのような課題を抱えていますか？該当するものをすべて選んでください。

結果：
複雑さがトップで、次にセキュリティの問題が続き、2022年に1位だった可視化は7位に落ちました。



F5のインサイト

現在、ほとんどの企業組織は、インフラストラクチャの複雑さの緩和、選択したインフラストラクチャのライフサイクルの延長、導入環境の統合、および複数のポイントソリューションの必要性の軽減を望んでいます。しかし、アプリケーションを最新化し、アプリケーションをオンプレミスに戻して、そして多くの場合はアプリケーションポートフォリオを拡大していますが、アーキテクチャやアプリケーションの分散がなくなるわけではなく、新旧アプリケーションの割合、各環境の目的、生じる課題の性質が変化しているだけです。さらに、平均的なポートフォリオに占める最新のアプリケーションアーキテクチャの割合は、2030年までに約85%に達すると予想されています。その頃には、より新しいアーキテクチャが登場し、「ハイブリッド」の意味が進化して、これらのアーキテクチャの成長は減速または停止すると考えられます。コスト、制御、遅延、事業継続性、拡張可能性などは永遠の課題であるため、複数の導入オプションを保持することは常に理にかなっています。1つの環境があらゆる目的に適合したり、複数の目標を同じように満たしたりすることはありません。

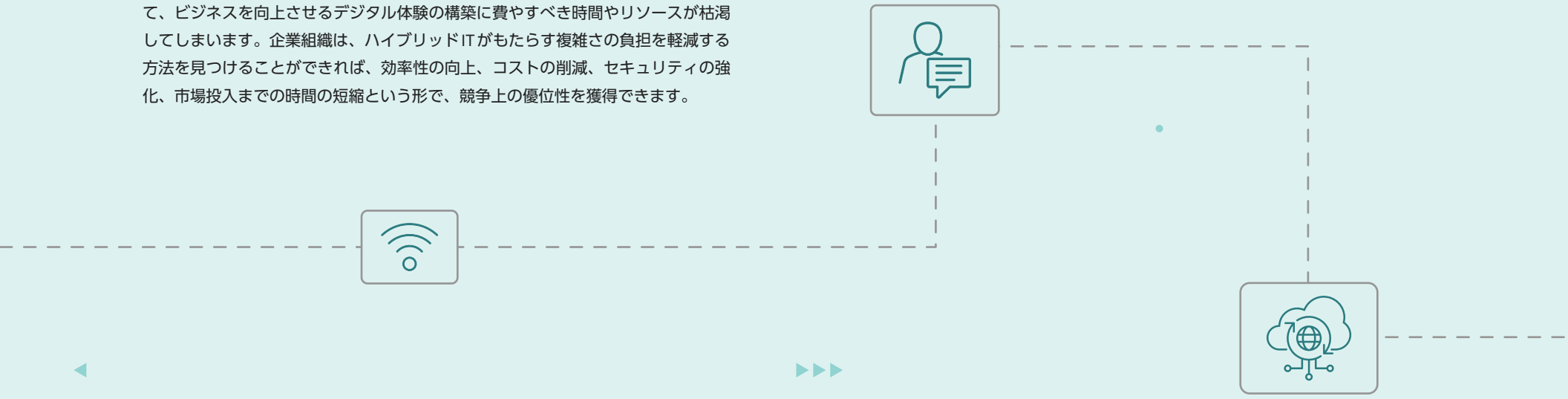
これが意味すること

デジタルビジネスには、適応力のあるITインフラストラクチャが必要です。その目標を達成するために、企業組織は、ハイブリッドクラウド、そしてマルチクラウドとなることが多いランドスケープで運用する上での課題を軽減するソリューションを必要としています。このようなソリューションがなければ、管理の複雑さによって、ビジネスを向上させるデジタル体験の構築に費やすべき時間やリソースが枯渇してしまいます。企業組織は、ハイブリッドITがもたらす複雑さの負担を軽減する方法を見つけることができれば、効率性の向上、コストの削減、セキュリティの強化、市場投入までの時間の短縮という形で、競争上の優位性を獲得できます。

さらに、以下のような補完的なアプローチを組み合わせることができます。

- 限定的な専門知識にとらわれず、システムや技術に全体的に精通しているIT専門家
- サイト信頼性エンジニアリング（SRE）などのプロセス方法論
- 宣言型導入ポリシーなどのツール
- 導入モデル全体に及び、サービスとして提供され、企業組織のすべての分散アプリケーションとアーキテクチャ（SaaSとして入手したものも含む）で一貫して機能し、現在のアーキテクチャに対応しながらアーキテクチャの変更に適応できる、アプリケーションのセキュリティと配信の技術

多くの企業組織にとって、これらの目標のほとんどを簡単に達成するために必要なことは、マルチクラウドネットワーキングの接続性を拡張し、さまざまなクラウド、データセンター、エッジロケーションに分散するあらゆる種類のアプリケーションやAPIを保護および配信するソリューションを持つパートナーと連携することです。



02

デジタルトランスフォーメーションはIT as a Businessを超越

2023年、業界全体の調査回答者のうち約10人中9人が、過去3年と同様に、デジタルトランスフォーメーションプロジェクトの進行中であると答えています。ハイブリッドな世界におけるデジタルトランスフォーメーションは、もはや新しいものではありませんが、2つの理由からニュースとして残っています。

個人レベルでは、食料品店の顧客から政治的な抗議者、世界的な慈善団体が支援する子供たちまで、ほぼすべての人に影響を与えています。ビジネスレベルでは、効率性の向上、新たな機会の創出、顧客体験と関係の改善、迅速な拡張能力といった価値をもたらしています。このようなメリットから、デジタルトランスフォーメーションは、ITのためだけではなく、トップレベルのビジネス戦略となっています。

最新化は今日のデジタルトランスフォーメーションの力になります。
これらのメリットをどのように実現するかに関して、現在、最新化がその中心になっています。

以前から述べているように、私たちはデジタルトランスフォーメーションを3つのフェーズに分けています。つまり、タスクの自動化、デジタル拡張（自動化の拡張と統合を含む）、およびテレメトリ、人工知能（AI）、機械学習（ML）を活用した意思決定です。フェーズ2には、既存のシステムやアプリケーションの最新化が含まれます。2023年には、このような活動が中心となります。

実際、10社中8社以上が現在、最新化とデジタル拡張に取り組んでいます。このような取り組みは、3分の1強（37%）の企業組織しか取り組んでいなかった新型コロナウイルス感染症のパンデミック以前に比べて、2倍以上多くなっています。パンデミックは、デジタルトランスフォーメーションを数年分推進しました。

現在の最新化活動には、最新のアプリケーションを開発することや、コアビジネス機能を提供する従来のアプリケーションに最新のコンポーネントを追加して、アプリケーションへのアクセスや体験を変えることが含まれます。たとえば、銀行や保険などの業界を支える基本的なロジックと連動するモバイルアプリ、または注文入力や、製造装置の制御のためのトラッキング統合などがあります。

ほぼ全員が最新化に取り組んでいる

27%
フェーズ1
タスクの自動化：
アプリケーション

81%
フェーズ2
デジタル拡張：
最新化

54%
フェーズ3
AIを活用したビジネス：
データとアナリティクス

半数以上の企業組織がデジタルトランスフォーメーションのフェーズ3であるAIを活用したビジネスにも取り組んではいますが、その割合は2021年の割合よりも下がっています。その理由は次の2つが考えられます。AIやMLを本番環境に導入することが難しいため、フェーズ3への移行に水を差しています。より一般的に、デジタルトランスフォーメーションは反復的なプロセスです。企業組織は、3つのフェーズすべてを同時に行うか、1つのフェーズを進展させた後に前のフェーズに戻り自動化を拡張することが一般的です。特にAIの活用に関しては、後退したように見えたことが、前進するための基礎となることがあります。フェーズ1であるタスクの自動化が2020年の46%から低下していることは、このためでもありますが、企業組織がバックオフィス業務をより自動化するために、しばらくは続くと可能性があります。

IT運用は、デジタルトランスフォーメーションの最重要課題であることに変わりはありません。
回答者の3分の2近く（64%）が現在IT運用の最新化を進めています。これはこれまで以上に増えています。企業組織全体に及ぶトランスフォーメーションは、限られたITリソースへの需要を高めるため、最新化はAI活用を可能にするだけでなく、ITチームの負担を管理しやすくするためにも必要です。また、ボトルネックが生じないように、関連するITプロセスも最新化する必要があります。

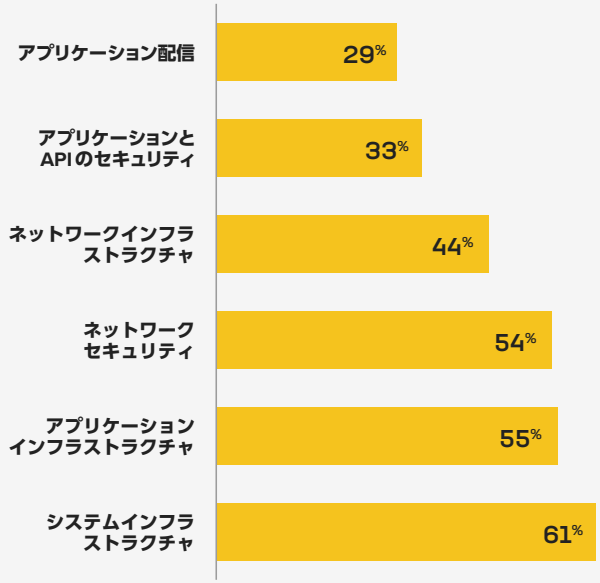
一般的に、自動化が進むと、IT効率性が向上する

このようなニーズは、半数以上（59%）の回答者がデジタルツールや自動化を利用して業務を拡張および拡大するサイト信頼性エンジニアリング（SRE）を採用する予定であることにも表れています。

自動化はIT機能によって異なる

質問：
どのようなIT機能を自動化しましたか？
該当するものをすべて選んでください。

結果：
アプリケーションのセキュリティと配信には自動化の機会が残されているようです。



しかし、最新化ではなく、自動化こそが、ITの効率化の最重要経路です。自動化は、システムインフラストラクチャ、ネットワークインフラストラクチャ、アプリケーションインフラストラクチャ、ネットワークセキュリティ、アプリケーション配信、アプリケーションセキュリティという6つのコアIT機能で実現できます。これまでの自動化の多くは、システムインフラストラクチャ、ネットワークセキュリティ、アプリケーションインフラストラクチャを対象としてきました。

- 仮想マシンやKubernetesの使用など、システムインフラストラクチャの自動化は、仮想化の成熟とコンテナエコシステムに対する業界の強固なサポートから恩恵を受けています。
- サービスモデルへのオフロードが進むネットワークセキュリティの自動化は、AIと、それに沿った定義済みのシナリオの存在に支えられています。
- アプリケーションインフラストラクチャの自動化は、アプリケーションの保護と導入の迅速化に役立ち、セキュリティの脅威と、新しい機能やアプリケーションの市場投入までの時間短縮を求める必要性によって推進されています。

3分の2の企業組織は、2018年にデジタルトランスフォーメーションの潜在的な利益の上位にランクされていたITの効率化をすでに実現していると答えています。それから5年、その価値は実現されつつあります。

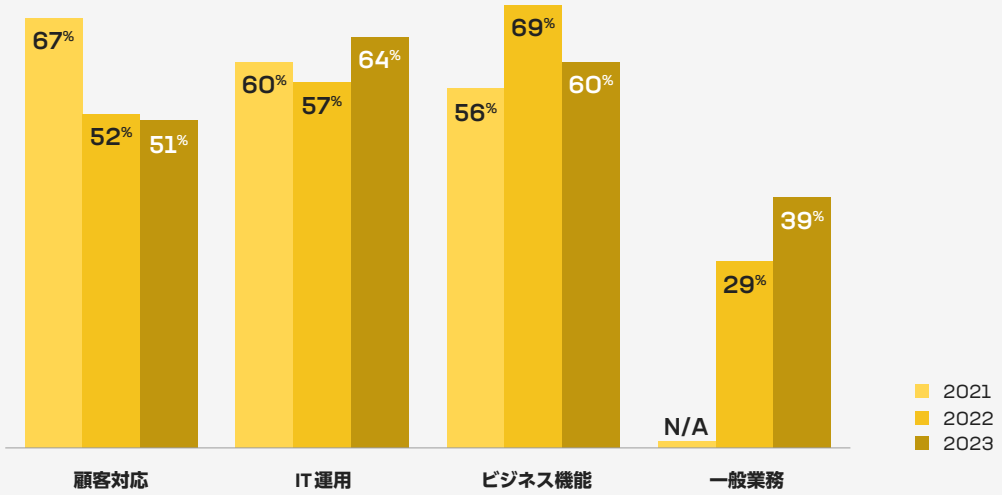
ITの効率化を報告した調査回答者は、6つの分野のうち平均して少なくとも3つの分野で自動化を実施しています。当然ながら、活動と自動化の成熟度が最も高い3つの分野、つまりシステムインフラストラクチャ、アプリケーションインフラストラクチャ、ネットワークセキュリティにおいて、最も強い効率化の効果が報告されています。しかし、一般的に、自動化が進むと、IT効率性が向上するため、競争上の優位性を求める企業組織は、6つの分野すべてで自動化を進めるのが良いようです。

これらのメリットは、主にデジタルで運用する企業にとって、特に大きな意味を持ちます。従来の製造業では、設備投資や倉庫スペースなど、さまざまな固定費がかかっていました。実店舗を持つ小売業も同様の固定費がかかります。

変化するデジタルトランスフォーメーションの優先順位

質問：
デジタルトランスフォーメーションの取り組みで優先されるビジネス機能は何ですか？該当するものをすべて選んでください。

結果：
2021年以降、ビジネス機能および一般業務のデジタルトランスフォーメーションが増加しています。



対照的に、デジタルビジネス（オンライン販売を主とする小売業）の場合、変動する人件費やIT費用が、ほとんどの場合サービスである「製品」の大部分のコスト、あるいは主要なコストであることが一般的です。このような場合、ITの効率化は収益に直結します。

デジタルトランスフォーメーションは、ビジネスのあらゆる側面にメリットをもたらします。

もちろん、ITの効率化だけが自動化のメリットではなく、最新化の利点は他のビジネスプロセスにも適用されます。顧客サービスは依然として最新化の重要な優先事項ですが、顧客対応アプリケーションとプロセス全体（営業とマーケティングを含む）は、過去2年間で優先事項としてはかなり縮小しています。その理由の1つとして、これらの分野ではすでに大きな取り組みが行われていることも考えられますが、今日の不透明な経済状況下で業績悪化につながらないように、非効率な社内プロセスやサイロ化したレガシーアプリケーションに対するリーダーからの注目がますます強くなっていることも明らかです。

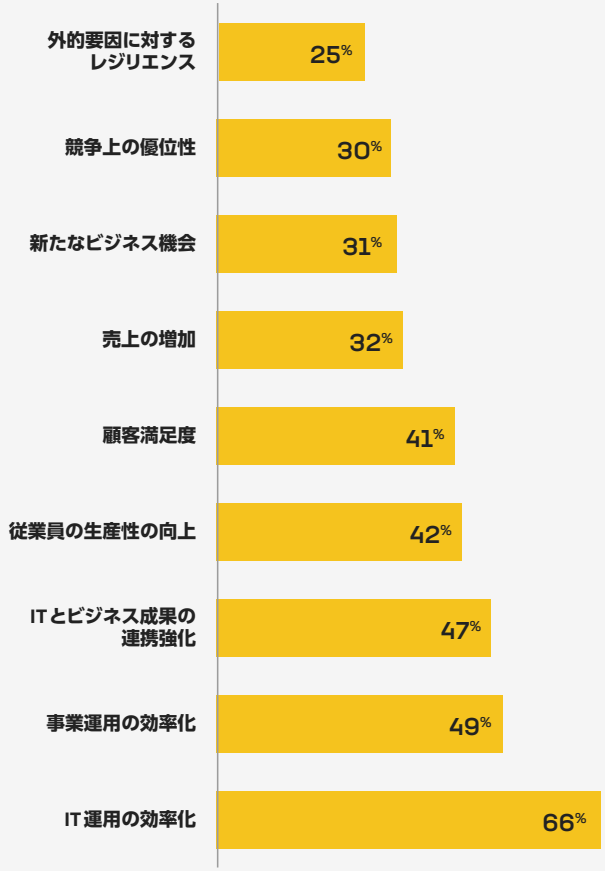
その結果、デジタルトランスフォーメーションは、顧客とのやり取りや顧客関係管理、製品の設計や開発、製造などの事業活動、リスクを管理する人事および法務部門、全従業員の生産性など、ビジネスのあらゆる側面との関係がますます強くなり、さらにこれらを強化しています。このような包括的な影響があるため、急速にデジタル化が進む世界で競争力を維持するには、ビジネス全体での最新化が必要です。

幸い、デジタルトランスフォーメーションに取り組んでいる回答者の約半数は、ITだけでなく、ビジネス全体の運用効率性が向上したと答えています。従業員全体の生産性と顧客満足度の向上も、近いうちに実現しそうです。同様に、3分の1近くが、売上と新たなビジネスチャンスが増加したと報告しています。

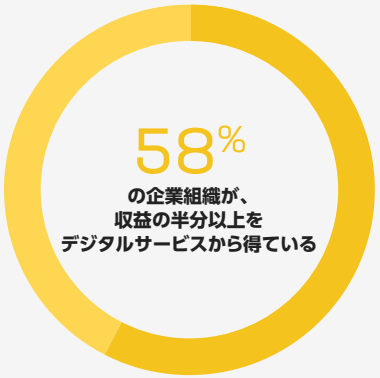
運用効率化がデジタルトランスフォーメーションに続く

質問：
デジタルトランスフォーメーションへの取り組みから、どのようなメリットを実感していますか？該当するものをすべて選んでください。

結果：
3分の2でIT運用が効率化されていますが、それ以外にも大きなメリットがあります。



すべてに当てはまるトランスフォーメーションジャーニーはありません。
企業組織がデジタルトランスフォーメーションのメリットを享受しているかどうかは、そのビジネスモデルがどの程度デジタルであるかで決まる場合があります。現在、4分の3以上（79%）の回答者は、デジタルサービスを消費者または他の企業組織、あるいはその両方に提供していると答えています。デジタルサービスを自社の従業員に対してのみ提供しているのは、5人に1人（21%）程度です。



私たちは、デジタルサービスとは、アプリケーション、API、アプリケーションの配信とセキュリティの技術、データなどのリソースをシームレスにつなぎ合わせて、サービスを提供する企業組織に成果をもたらすデジタル体験を提供するものと定義しています。たとえば、ギグワーカーのアプリケーションや従業員の時間報告から、デジタルメディアの購読、モバイル空港チェックイン、モバイル決済まで、さまざまなものがあります。これらのサービスは、ユーザーに無償（別料金）で提供されることもあれば、オンデマンド、従量課金、サブスクリプションなど、さまざまな収益モデルに依存することもあります。

しかし、ほぼすべての回答者がデジタルサービスを提供している一方で、半数強（58%）がデジタルサービスを利用して、実質的にビジネスを推進し、そのサービスが会社の年間収益の半分以上を占めています。

さらに、このような収益になるデジタルサービスを優先する企業組織と、アナログなやり取りで主に収益を上げる企業組織に分かれています。具体的には、デジタルで収益を上げる企業組織は、他の企業組織よりも以下のような傾向があります。

- 最新のアプリケーションポートフォリオを運用している
- アプリケーションのセキュリティや配信のさまざまな技術を導入している
- パブリッククラウドをあらゆる目的で使用し、特に本番環境では、インフラストラクチャやアプリケーションをグローバルに迅速に拡張し、事業継続性を確保するために使用している
- SaaSとSECaaSを購入している
- エッジを目的に応じて使用していて、より効果的に顧客にアプローチするために使う可能性が3倍ある

つまり、半数以上の企業組織は、多かれ少なかれ最新のIT技術に対応しているデジタルダイナモであると言えます。しかし、残りの半数は、他のニーズを優先し、限られたリソースを地理的な拡大や製品開発、セキュリティの問題など、他の場所で利用している可能性があります。うまくバランスが取れています。さらに、2つの企業組織が、同じ業界であっても、同時に同じ優先順位に集中することはありませんし、集中したとしても同じように進展することはありません。

とはいえ、現代生活のデジタル化が元に戻りそうにはありません。CIOやその他の企業リーダーは、それぞれの目的に応じて、最先端技術から大きく遅れたり、アナログ中心の収益モデルに固執し過ぎたりすると、後で追いつくのが難しくなることを忘れないでください。最新化は、企業組織によってそれぞれ異なる、長い旅になる可能性がありますが、賢明なCIOであれば、大きく遅れないように、何らかの方法で前進し続けることを考えます。

F5のインサイト

デジタルサービスがもたらす収益の程度に関係なく、アプリケーションやAPIを活用した未来の経済で成功を望む企業組織は、デジタルサービスを最も効果的に収益化している企業の活動、技術、戦略を常に把握しておく必要があります。

競合他社に後れを取っている暇など誰にもありません。最も伝統的な業界でも、将来的にデジタルサービスを追加する可能性があります。これは、教育向けの新しいバーチャルサービスから、高齢者ケアのロボット工学、ドローンを活用した資源採取まで、あらゆる業界に言えることです。

また、デジタル体験を主な拠り所としているかどうかに関係なく、セキュリティまたは運用の目立った失敗によって評判が落ちたり、規制の影響を受けたりするリスクは依然として存在します。他の企業が現状に満足しているときに、自動化と最新化、そして効率化に投資するリーダーは、イノベーションにおいて有利な立場に立つことができ、変化に直面したときに競合他社に差をつけることができるかもしれません。

これが意味すること

IT運用チームがシステムインフラストラクチャ、アプリケーションインフラストラクチャ、ネットワークセキュリティの自動化をまだ始めていない企業でも、大きなメリットを得ることができますが、これらはすでに多くの競合会社が恩恵を受けている可能性もあります。先行している企業であれば、ネットワークインフラストラクチャ、アプリケーション配信、アプリケーションセキュリティという3つのコアIT機能の自動化も検討すべきです。これらの分野であまり一般的でない効率化が、最終的に優位性をもたらす可能性があります。

特に、アプリケーション配信およびアプリケーションとAPIのセキュリティの自動化は、ほとんどの企業組織にとって大きな機会となります。もちろん、個々のアプリケーションが既存のリソースやツールを簡単に活用できない止むを得ない状況にあることが多いため、これらの分野で自動化を行うことは難しいかもしれません。しかし、これらの領域における自動化は、他のコアIT領域における自動化よりも、顧客満足度の向上、収益の増加、新しいビジネス機会の獲得とより強く関連しています。ITの効率化を超えてビジネス全体に影響を与えるこれらのメリットは、困難なだけに、それだけの価値もあります。

最後に、企業組織がこの自動化と最新化の一環として、長期的な成功を追求する場合、コアからエッジに分散するアプリケーションを接続するための高度で適応性のある保護を含む、アプリケーションのセキュリティと配信の統合技術が必要であることがますます明らかになっています。SaaSベースのソリューションで利用できる迅速な対応と簡単な管理は、WebアプリケーションとAPI、およびこれらのアプリケーションをホストするインフラストラクチャを保護し、企業がデジタルの速さと制御およびパフォーマンスとのバランスを取る上で役立ちます。

03

時間的な制約がセキュリティ戦略を左右する

このハイブリッドで急速に最新化するデジタルの世界におけるセキュリティは、ますます難しくなっています。アプリケーションやAPIの活用が進む経済では、リスクと報酬のバランスを取りながら、顧客の意欲をそぐ摩擦を増やすことなく、新たな脅威をうまく検知および緩和することが、長距離的な戦略です。しかし、サイバーセキュリティの運用は、急速に進化する攻撃の先を行くために、短距離的な速さも必要です。

このような迅速な対応へのニーズは、セキュリティ戦略に影響します。たとえば、新たな攻撃や脆弱性を迅速に修正する手段として実績のあるSECaaSに移行する企業組織は、最大の要因としてスピードを挙げています。特に、セキュリティ担当者やSRE、DevOps担当者は、スピードを動機として挙げる傾向が強くありました。

もちろん、SECaaSには他にもメリットがあり、専門的なセキュリティを提供しながら、運用と管理を簡素化する可能性もあります。そのため、十分なスキルを持つ人材の不足も、SECaaS採用の後押しとなっています。その結果、より多くの企業組織が、俊敏にセキュリティを提供できるSaaSプロバイダを信頼し、自社で管理するよりも迅速かつ専門的に新たな脅威に対応し、阻止しています。

しかし、自社でセキュリティを管理している企業組織も、じっとしているわけではありません。これは、新型コロナウイルス感染症のパンデミックが始まってから今日までのアプリケーションセキュリティ技術の導入状況に表れています。

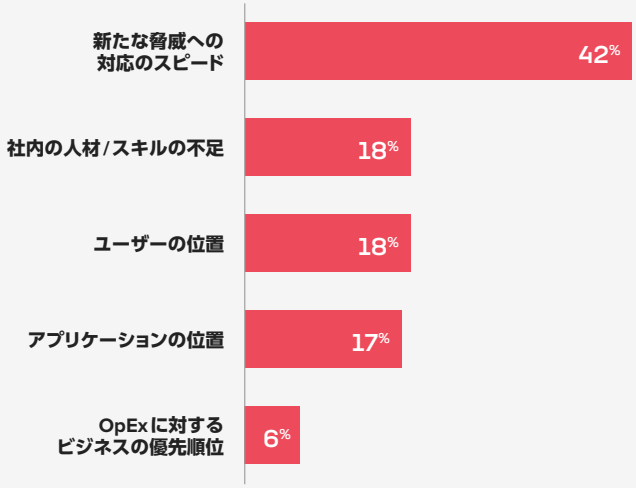
- APIゲートウェイの利用が、回答者の35%から78%へと2倍以上に増加
- IDフェデレーションの導入率が52%から75%に増加
- エンドポイントセキュリティが65%から86%に増加
- セキュアウェブゲートウェイ (SWG) サービスが61%から85%へと急増
- WAFの利用率が66%から82%に増加

アプリケーションセキュリティ技術の導入が増加していることは、変化する脅威のランドスケープでリスクを迅速に修正するために、この技術が重要であるという認識が高まっていることを反映しています。

SECaaSのスピードは魅力

質問：
Security as a Service (WAAP、WAF、DDoS、API保護など) を利用している主な理由は何ですか?1つ選んでください。

結果：
主な動機は脅威緩和のスピードです。



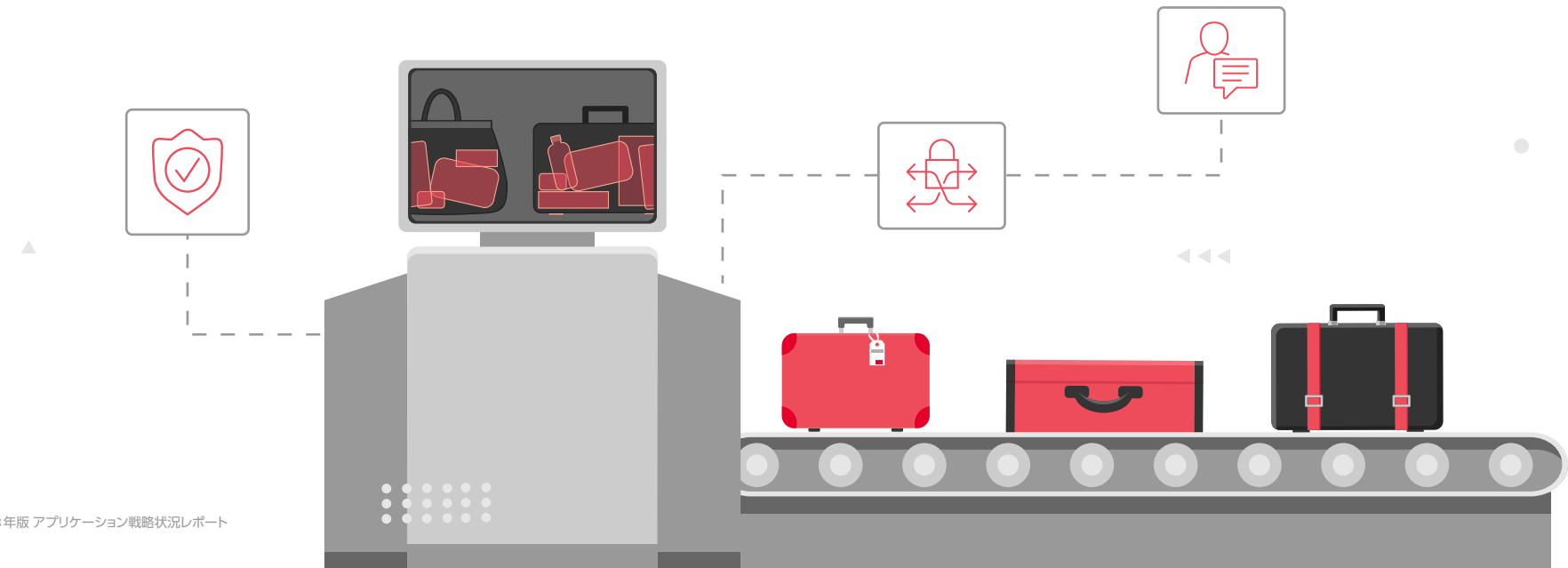
ビジネスはゼロトラストに向かって疾走しています。
速さは、ゼロトラストセキュリティモデルの台頭の要因でもあります。このモデルは、さまざまなアーキテクチャやハイブリッド導入を越えて、開発および導入プロセスのセキュリティ面を簡素化できます。回答者の80%以上は、ゼロトラストを採用している、または採用する予定だと答えています。実際、ゼロトラストは、ITと運用技術の融合（IT/OT）と並んで、今後数年間での最も注目のグローバルトレンドになりました。これは2022年の3位から上昇しました。

80%以上の企業組織がゼロトラストを採用

特に、ゼロトラストモデルの継続的な検証は、セッション途中でのセキュリティ侵害や、許可されたアクセスを強制的に使用することによる未許可のリソースへの到達を防ぐことができます。このアイデンティティ中心のアプローチでセキュリティを確保することで、新しい機能やアプリケーションの市場投入までの時間を短縮できるだけでなく、手動での攻撃緩和やパッチ適用が必要になる侵害を防ぐことができます。これは、IAM技術の導入が増加している理由の1つでもあります。

反応スピードが確実に向上することも、セキュリティでのAI/MLの使用を後押ししています。3分の2近くの企業組織が、AIの活用を計画している（41%）、またはすでに導入しています（23%）。すでにAIやMLを使用している企業組織は、セキュリティを最大のユースケースに挙げていて、現在計画中の企業組織は、セキュリティを主な要因に挙げています（AI運用は2位でした）。

同様に、スピードは、自動化への取り組みの動機にもなっています。その必要性は明らかです。アプリケーション開発は、自動化によって変化し、ますます高速化している一方、セキュリティとリスク管理は、一般的に、手作業による労力、監視、介入が必要です。しかし、企業組織は前進しています。2023年、6つのコアIT機能における自動化の進捗に関して、ネットワークセキュリティは、システムインフラストラクチャに僅差で続く3番目でした、サービスモデルへのオフロードが進むネットワークセキュリティは、AIの活用によるメリットもあります。



プラットフォームとゼロトラストは密接に関係していることがよくあります。
10人に9人近く（88%）の回答者が、企業組織でセキュリティプラットフォームを採用していると答えていて、これはゼロトラストモデルに取り組んでいる企業組織とほぼ同じ割合です。これらの傾向は重なっています。どちらも、ハイブリッドでマルチクラウドの世界を保護することの複雑さを反映しています。しかし、プラットフォームセキュリティは、ハイブリッドインフラストラクチャ、従来のアプリケーションと最新のアプリケーション、分散APIに対して一貫したセキュリティを提供しながら、ソリューションやベンダーの乱立を抑えたいという要望にも応えています。

特に、外部ユーザーにデジタルサービスを提供する企業組織は、アメリカ大陸の企業やハイテク産業の企業と同様に、プラットフォームアプローチを採用する傾向があります。これは、これらの調査回答者がグローバルな展開と拡張を必要とする傾向が強いためだと思われます。

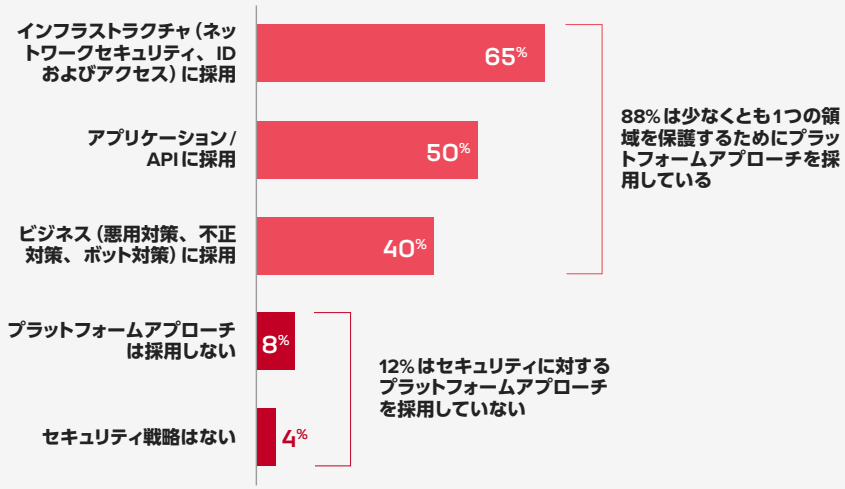
適用方法については、プラットフォームアプローチは、インフラストラクチャの保護が最も一般的です。ほぼ3分の2（65%）が、ネットワークセキュリティ、またはIDおよびアクセス管理にプラットフォームを使用することを想定しています。この傾向は、インフラストラクチャを保護するために設計されたプラットフォームが以前から利用可能であったことも後押しとなっているようです。しかし、半数（50%）の回答者は、データセンターからエッジまでのWebアプリケーションやAPIを保護するためのプラットフォームへの移行を進めています。さらに40%は、ボット対策や不正対策ソリューションなど、ビジネスセキュリティのニーズに対応したプラットフォームを求めています。

何を保護するかに関係なく、新しい脅威への対応のスピードは、エコシステムアプローチを使用してセキュリティプラットフォームを選択している40%の回答者にとって特に重要です。エコシステムアプローチ（パブリッククラウドプロバイダのパートナーマーケットプレイスへの依存など）には、2つの利点があります。1つは、複数のベンダーの中から選択することで、企業はそのエコシステムに適合する最高効率のソリューションを選択できることです。もう1つは、パブリッククラウドプロバイダが、エコシステム内のサードパーティに基本的な統合を要求していることがわかっているので、セキュリティソリューションの価値実現までの時間が短縮されることです。

セキュリティプラットフォームの最大のターゲットはインフラストラクチャ

質問：
セキュリティ戦略を考えるとき、プラットフォームアプローチを採用していますか？該当するものをすべて選んでください。

結果：
約90%がプラットフォームアプローチを採用していて、多くの人がプラットフォームを使って複数の領域を保護する予定です。



興味深いことに、シニアIT管理者は特にエコシステムアプローチに関心があります。しかし、SecOpsチームは、シングルベンダーのセキュリティプラットフォームを好みます。このような意見の相違は、企業組織の上位にいるほど、IT機能間の分断によるコストをより強く認識していることが原因だと思われます。

セキュリティサービスは、最も一般的なエッジワークロードだが、監視が最も急速に成長している

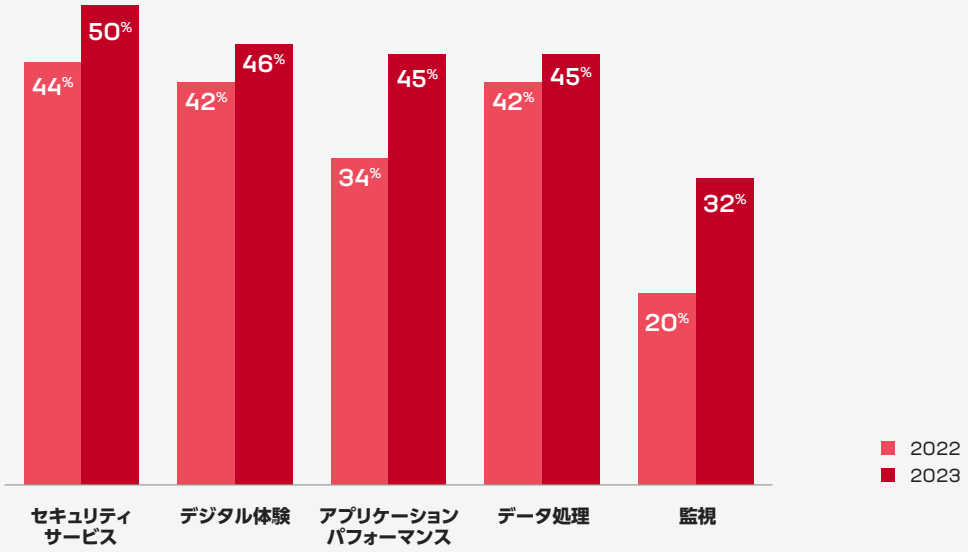
セキュリティはエッジワークロードのトップです。
ワークロードをエッジに移行することを計画している企業の半数は、セキュリティのワークロードを想定しています。しかし、現在ゼロトラスト戦略を採用している回答者の約3分の2は、ゼロトラストを完全に実行し、そのメリットを最大限に得るには、エッジを使用してすべてのエンドポイントを保護する必要があるという認識から、エッジにセキュリティワークロードを導入する予定です。

しかし、エッジのユースケースのトップは、セキュリティサービスですが、2022年以降最も急成長しているエッジワークロードは監視です。これは、リモートワークの爆発的増加、IoTアプリケーション、アプリケーションの普及傾向、今日の市場の世界的展開、リアルタイムデータに依存してプロセス調整を導くIT/OTコンバージェンスに対する強い関心など、複数の要因が反映されていると思われます。

セキュリティがエッジワークロードのトップ

質問：
エッジに導入する予定のワークロードの種類は何ですか？該当するものをすべて選んでください。

結果：
エッジワークロードのトップはセキュリティですが、監視が最も急速に増加しています。



より多くの企業組織が、安全なソフトウェア開発ライフサイクルを採用する必要があります。

しかし、強力なセキュリティは、ワークロードがどこでホストされるかに関係なく、導入の前から始まります。その結果、4分の3（75%）の回答者は、安全なソフトウェア開発ライフサイクル（SDLC）を採用しているか、採用する予定があります。これは、セキュリティとリスク管理は、たとえば、インフラストラクチャやアプリケーションの導入レベルだけで行えるような「1回で完了」の活動ではないことを認識した結果です。しかし、包括的で一貫した保護には、ITとビジネスの役割を超え、時間をかけ、複数の取り組みを協調する必要があります。アプリケーションの開発時にセキュリティに対処することで、成功してしまった攻撃を緩和するときはもちろん、後から改良するときの時間的損失を防ぐことができます。

SDLCについてまだ考えていない企業組織は少数ながらまだいますが、ソフトウェアについてもビジネスについても、セキュリティ戦略がまったくないと答えた4%の調査回答者よりはましなようです。

幸いなことに、ほとんどの企業組織は、より積極的に、より前向きにすべてのリスクを軽減しようとしています。たとえば、ソフトウェアのサプライチェーンのセキュリティに関する懸念は、さまざまな方法で対処されています。

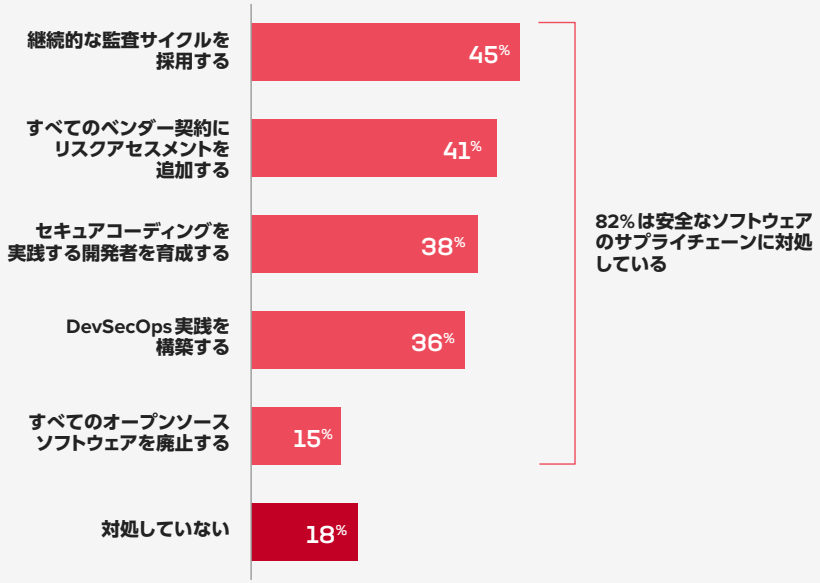
最も人気のあるアプローチは、継続的な監査サイクルの採用です。3分の1以上（36%）の企業は、DevSecOps実践を構築しています。また、約3分の1（38%）は、セキュアコーディングを実践する開発者を育成しています。

意外ではないかもしれませんが、金融サービス業界とヘルスケア業界の企業組織は、ソフトウェアのサプライチェーンのセキュリティに何らかの形で取り組んでいる可能性が最も高い企業組織です。一方、5社に1社近く（18%）は、ソフトウェアのサプライチェーンのセキュリティに関心がなく、対応する計画も立てていないようです。

ソフトウェアがセキュリティリスクとして残る

質問：
組織では、安全なソフトウェアのサプライチェーンにどのように取り組んでいますか？該当するものをすべて選んでください。

結果：
ほとんどの回答者は少なくとも1つのアプローチを採用していますが、約5分の1はソフトウェアのサプライチェーンを未対処のリスクとしています。



F5のインサイト

今日のハイブリッドな世界では、ビジネスの保護はこれまで以上に難しく、一貫したセキュリティポリシーの導入は特に困難ですが、速さ、アジリティ、レジリエンスを向上させる上で重要です。ゼロトラスト戦略がネットワークやインフラストラクチャのセキュリティとますます強く関連するようになっていますが、APIセキュリティのための認証と認可の使用を含むアイデンティティ管理技術は引き続き、アプリケーションを保護するための最も価値のあるアプローチであると考えられています。

これらのアプリケーションをサポートするために、セキュリティとアイデンティティの技術は、すでにオンプレミスとクラウドの両方に最も導入されているアプリケーションサービスとなっています。また、これらは、企業組織がその潜在的なパフォーマンスとエンゲージメントを活用するために、エッジに配置されることも増えています。アプリケーション技術、特にセキュリティ技術は、アプリケーションやAPIが導入されるあらゆる場所で必要とされるため、セキュリティワークロードに占めるエッジの割合が増えても、環境全体での導入率の差は縮小し続けると私たちは考えています。

これが意味すること

セキュリティは、デジタルの差別化要因になることができ、これにより、アプリケーション開発チームは、リスクを高めず、IT機能間の摩擦を増やすことなく、革新のスピードを上げることができます。ゼロトラストモデル、アイデンティティ管理、安全なソフトウェア開発、その他のセキュリティ戦略や方法は、共存できますし、共存すべきです。企業組織は、ゼロトラストの概念を、コードリポジトリを含むソフトウェア開発パイプラインのツールに拡大することを検討する必要があります。意欲的な攻撃者に打ち勝つためには、企業は、ドアや窓だけでなく、郵便物入れ、煙突、ストーブの吹き出し口も保護する必要があります。そのため、SDLCのようなソフトウェアセキュリティプロセスを開発し、それに従う必要があります。あらゆる脆弱性に対処することで、初めてITリーダーはデータ、顧客、ビジネスを守ることができます。

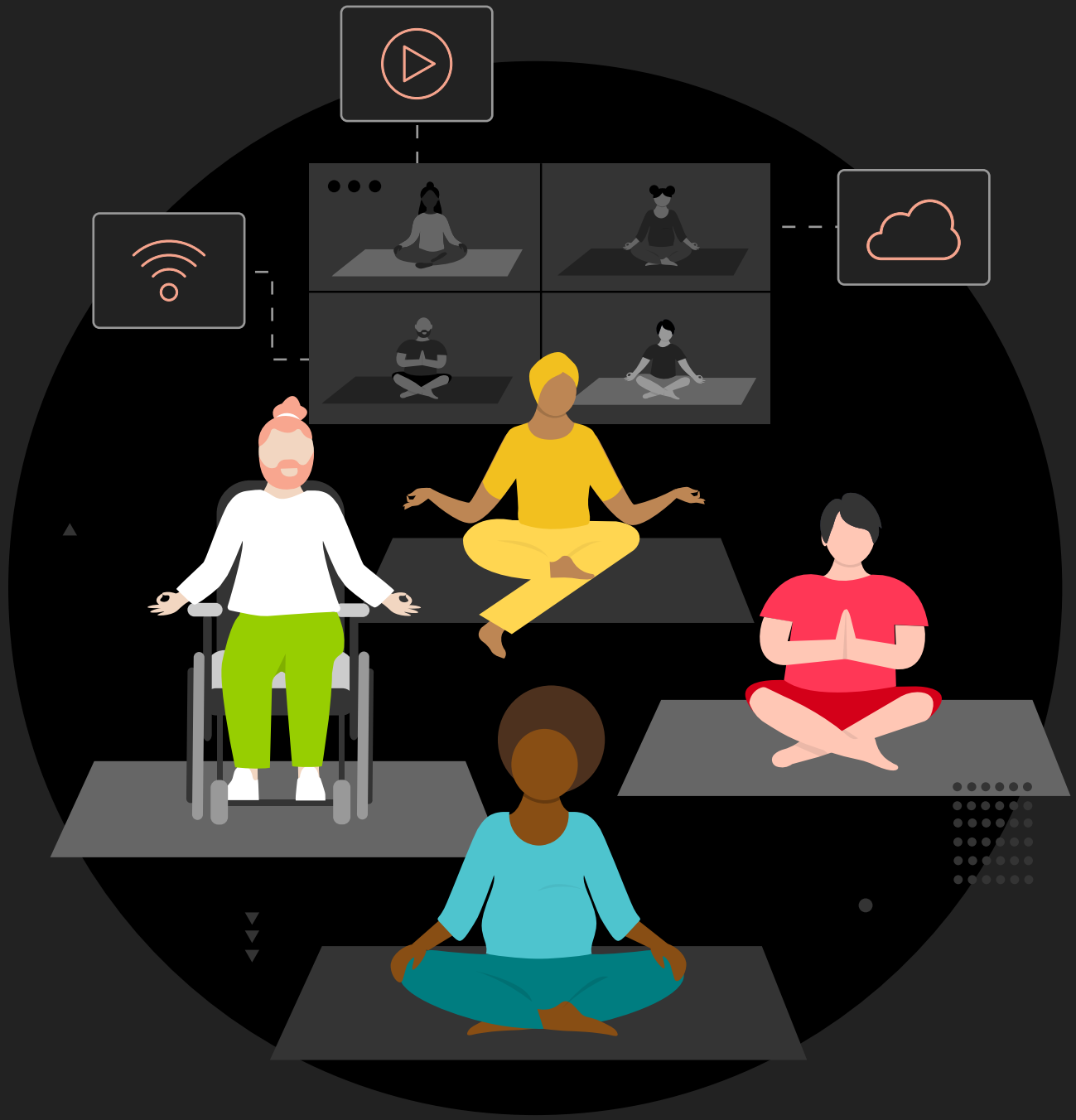
このような考え方の一例として、APIセキュリティが従来のデータパスでの使用から拡大されていることがあります。最近登場したより興味深いAPIセキュリティソリューションは、POSTエージェントを介したような東西の通信に対応しています。このような創造的な考え方により、企業組織は、攻撃者の先を行くことができ、ITリソースを手作業による攻撃緩和から解放し、ビジネスの加速に利用できます。

さらに、アプリケーションとその基盤となるAPIファブリックは、それらが構築、導入、運用されるインフラストラクチャと同程度の安全性しかありません。レジリエンスとアジリティを提供する包括的な保護を得る最も簡単な方法は、あらゆる場所でアプリケーションとインフラストラクチャの両方を保護する、環境に依存しないソリューション、消費モデルおよびベンダーを使用することです。SECaaSは、たとえば、緊急の攻撃緩和ニーズがある、社内でのセキュリティ専門知識が不十分、あるいは資本コストよりも運用コストを優先したい、といった企業組織にとって特に有用な選択肢の1つになる可能性があります。

場所に関係なく、あらゆるアプリケーションとあらゆるAPIに対して、統一されたセキュリティポリシーを実装できることが重要です。SaaSベースのサービスを含むセキュリティプラットフォームは、ポリシーの一貫性、幅広い可視化、簡単な管理により、コアからエッジまで、すべてのホスト環境全体でハイブリッドアプリとAPIを保護できます。このようなアプローチは、セキュリティスタック全体の行動ベースの侵入防御や攻撃緩和と統合されたWAF、DDoS防御、ボット防御によって、最新と従来の両方のアーキテクチャとハイブリッドアプリを防御できます。このような効果的なセキュリティは、ビジネスのスピードで実行され、最も重要なものを保護すると同時に、企業組織の成長の可能性を解放します。

まとめ

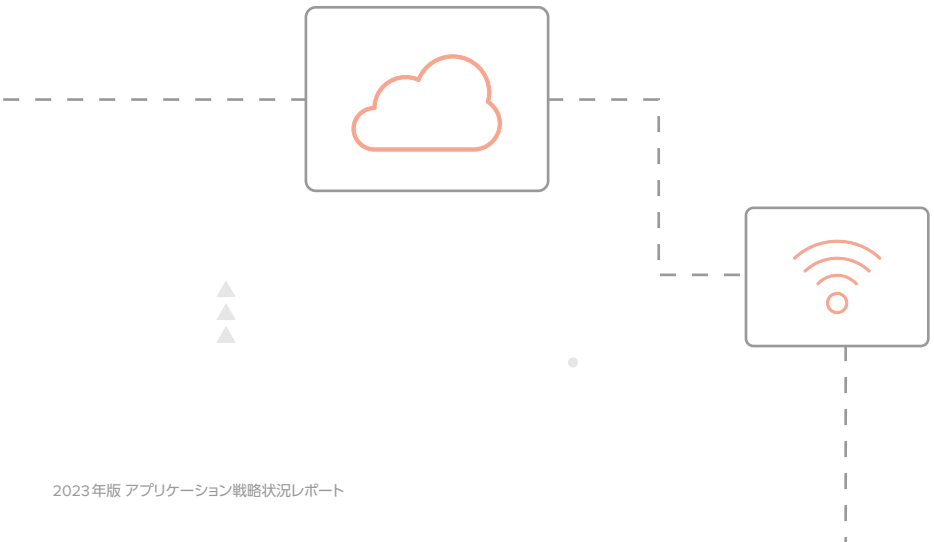
働きすぎのITチームにも希望はある



アプリケーションポートフォリオの最新化が進む中で、企業組織は、導入アーキテクチャを調整し続け、運用上の需要と市場の需要のバランスを取りながら、オンプレミス、クラウド（プライベート、パブリック、またはその両方）、エッジ環境間の適切な配分や、SAASとして利用するアプリケーションを見つけていくことになります。統合できるところは統合していくと思いますが、大半の企業はハイブリッドクラウドやマルチクラウドモデルを無期限に使用すると私たちは考えています。

この見解の裏付けとなるのは、技術革新のペース、技術的負債のトレードオフ、そして結果として、ほとんどの企業組織が2世代、3世代の技術でやりくりしなければならないという事実です。これらの技術は互いを追い越すこともあるかもしれませんが、携帯電話が固定電話のほとんど、またはまったくなかった市場を征服したように、複数のパラダイムが共存することになります。

ハイブリッドモデルは、一般的にアプリケーション固有のニーズ、メリット、目的に基づいてアプリケーションごとに行われる導入意思決定において、最大の柔軟性を提供します。市場投入までの時間短縮を迫られ、顧客満足度を重要視する中で、ほとんどの企業組織は、アジリティ、スピード、デジタル体験を最適化する能力を選択し続けます。最新のアプリケーションとマイクロサービスは、ビジネスの核となる従来のモノリシックなアプリケーションとモバイルインターフェイスの間など、必要な接続を可能にします。



その結果、複数のクラウド、分散導入、ハイブリッドITスタックといった課題は、何らかの形で続いています。しかし、働きすぎのITチームにも希望はあります。自動化の拡張、宣言型導入ポリシーによる一貫したセキュリティ強化、IT運用におけるAI/ML、SREなどの標準化された手法、さらに適切なテクノロジー、ソリューション、パートナーによって、企業組織は、複雑さを乗り越えてビジネスの速度を向上させることができます。エッジでのリアルタイム監視の継続的な成長と、そのテレメトリを実用化するソリューションにより、手作業による管理を減らすAIOpsを促進できます。ゼロトラストセキュリティのアプローチと環境間プラットフォームは、導入場所に関係なく、あらゆるアプリケーションやAPIと、それらをサポートするインフラストラクチャを接続および保護できます。アプリケーションのセキュリティや配信技術で利用されるような抽象化レイヤーは、境界を越えて、より集中的、つまり簡素化された接続と制御のための接続点を提供できます。

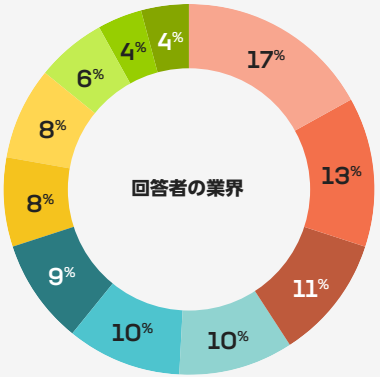
大半の企業組織はハイブリッドモデルを無期限で使用する

すべてに万能な専門知識を有する企業組織はないので、ハイブリッドの世界を理解し、そこで活躍するビジネスパートナーは、大きな価値を提供できます。特に、F5のような技術プロバイダは、包括的な保護と一貫したパフォーマンスを提供するために、複雑さを簡素化する力となることができます。このような適切なパートナーは、SaaSを含むさまざまな消費モデルにより、ハイブリッドITスタックに分散する最新と従来のアプリケーションを提供および保護できるように支援できます。私たちが協力することで、今生きているハイブリッドライフを、より簡単かつ安全、そしてやりがいのあるものにすることができます。

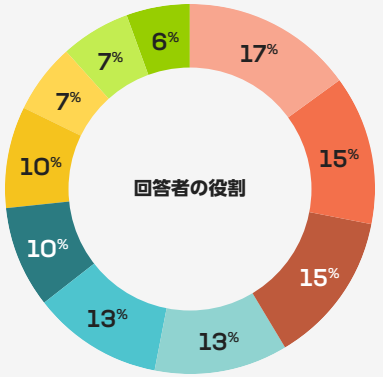
レポートについて

F5の今年の調査では、世界中の1,000人以上のIT意思決定者にそれぞれの優先事項や懸念事項を共有していただきました。今年は特にAPCJ地域の方々にご協力いただきました。これまで同様、さまざまな業種の方々からご回答いただきましたが、政府関係者が例年より多く、テクノロジー企業はやや少なめでした。

データは、C-Suiteからアプリケーション開発の現場まで、幅広いITおよび管理職の役割の人々から提供され、例年よりも多くのビジネスアプリケーション所有者にご参加いただきました。F5は、皆様がデジタルトランスフォーメーションに関する活動、興味、インサイトを共有するために時間を割いてご協力いただいたことに大いに感謝しております。



- テクノロジー
- 金融サービス
- 製造および資源
- 小売、卸売、運輸、メディアなどの流通およびサービス業
- 政府/公共部門
- クラウドサービスプロバイダ
- 電気通信
- 教育
- その他
- ヘルスケア
- エネルギー/公共事業



- ITリーダー
- ネットワーク
- データサイエンス
- 運用
- その他
- セキュリティ
- ビジネスリーダー
- ビジネスまたは技術アプリケーションオーナー
- クラウドアーキテクトまたはエンタープライズアーキテクト
- サイト信頼性エンジニア（SRE）、開発者、DevOpsまたはDevOps管理者

F5について

F5は、マルチクラウド アプリケーション サービスおよびセキュリティ企業であり、より良いデジタル世界の実現に取り組んでいます。F5は、世界最大かつ最先端の企業組織と提携し、オンプレミス、クラウド、エッジなど、あらゆる場所のすべてのアプリケーションとAPIを保護し、最適化しています。F5のソリューションをご利用いただくことで、みなさまの顧客に優れた安全なデジタル体験を提供し、常に脅威に先んじることができます。詳細については、f5.comをご覧ください（NASDAQ：FFIV）。