サイバーセキュリティ動向調査

デジタル時代のアイデンティティ／アクセス管理

kpmg.com/jp

目次

本冊子は、2016年5月にPAC, a CXP Group CompanyがKuppingerColeの協力を得て発行した“Identity and Access Management in the Digital Age”（スポンサー：KPMG, CYBERARK, SailPoint）を翻訳したものです。翻訳と英語原文間に齟齬がある場合には、当該英語原文が優先するものとします。

まえがき

多くの企業が、新しいデジタル経済の波に乗り遅れまいとして、先を争うようにビジネストランスフォーメーションを進めています。しかし、往々にして、この変革の途上ではさまざまなリスクが生じます。そして、それらのリスクを注意深く管理しなければ、企業のサイバーセキュリティの脆弱性が露呈してしまう恐れがあります。

しかも、さらに問題を複雑化しかねない事情があります。それは、既存のプラットフォームとテクノロジーが、デジタル経済の本質的な要素、たとえば、モノのインターネット（IoT）、ハイブリッドクラウド、個人の社会的属性、個人が特定される／されないことを隔てる境界線設定の難解化などに対応するように設計されていないことです。これは、今や主要なビジネスプロセスを担うようになったアイデンティティ／アクセス管理（IAM）ソリューションについても言えることです。

サイバーセキュリティとIAMの専門家にとって、今は刺激的な時代です。なぜなら、専門家たちがインサイダーリスクを引き起こす多くの脅威ベクター（攻撃発動者が使用する経路やツール）を必死に理解しようと努めている間にも、デジタルトランスフォーメーションの機会は待ったなしで押し寄せてくるからです。

この変化の渦に巻き込まれた企業や組織は、回答を見出す暇もなく、次々と新しい疑問に直面しています。

- アイデンティティが特定されるべき境界線はどこまで広がっているのか？
- 企業と顧客のアイデンティティの管理原則は（実際のところ）どのくらい隔たりがあるのか？
- 組織の内部と外部のアイデンティティを単一の視点で統合的に見渡すことは可能なのか？
- デジタルトランスフォーメーションに欠かせないサービスとなったIAM — それは、変革の実現、トレーニング、そして導入にどのように影響するのか？

PACおよびKuppingerColeとの連携によって、KPMGは、本調査を通じて、デジタルトランスフォーメーションにおけるIAMの役割を図式的に明らかにしようと試みました。本レポートが、デジタルトランスフォーメーションにおけるIAMの役割に対する認識を広め、最終的に、ビジネストランスフォーメーションの主役への道を歩みつつあるIAMの重要性を理解する助けとなることを願っています。

Manoj Kumar
KPMG英国
サイバーセキュリティ
主席アドバイザー

John Hermans
KPMGオランダ
欧州・中東・アジア
サイバーセキュリティ
責任者

本調査の英語原文のエグゼクティブサマリーとインフォグラフィックは、以下のウェブページでご覧いただけます。
https://www.pac-online.com/trend-study-identity-and-access-management-digital-age

デジタル時代のアイデンティティ／アクセス管理

Paul Fisher
PAC英国、リサーチディレクター
2016年5月

はじめに

欧州では、数万のアイデンティティ／アクセス管理（IAM）システムが、適切な人員だけにデータとシステムへのアクセスを許可するという方法で、長年にわたり企業のセキュリティ維持に使われてきました。

従来、そのようなソリューションは、従業員個人のアイデンティティを管理する目的で設計されたものですが、時代の変化に伴い、モバイルワークという働き方へのシフトによるエンドポイントの多様化まで、カバーするべき役割が広がってきました。

しかし、今日、あらゆる業界がデジタルトランスフォーメーションを推進することで、競争力の強化、効率性の向上、そして顧客やサプライチェーンとの接近を図ろうと試み、新しい課題が出現しつつあります。

今、デジタルトランスフォーメーションは、単なる業界の流行語という域を超えて、欧州全域に広がる現実となっています。これは、本調査の結果が示すとおりです。

とはいえ、デジタルトランスフォーメーションは、既存のテクノロジーとプロセスにも影響を及ぼすことが予想されます。組織変革の途上においてそのセキュリティを維持していく前提となるのは、アイデンティティが安全に保たれているということです。

デジタル世界のアイデンティティの数は急激に増加することが予想され、より多様かつ制御困難な形式で広まっていく可能性が高いでしょう。企業が消費者のアイデンティティを持つことの意義とは何か、どうすれば消費者のアイデンティティを適切に管理できるのか、そしてどうすれば安全に保護できるのかについて、企業は真剣に考え始めています。また公的機関も、どのようにデジタルアイデンティティを利用すれば公共サービスを改革できるのか検討し始めています。

セキュリティおよび情報担当の上級管理責任者は、もしこの課題に取り組み始めていないなら、可能な限り早急に対策に乗り出す必要があるでしょう。そして、デジタルビジネスの中でのアイデンティティに対するニーズの解決に、IAMソリューションがどのように役立つかを検討することも必要となるでしょう。

本調査は、IT意思決定者が、変化するビジネス環境の中でアイデンティティ／アクセス管理（IAM）システムにおける新たなサイバーセキュリティの課題にどう立ち向かうべきかについて、有意義な洞察を提供するものと私たちは考えています。

> 企業が消費者のアイデンティティを持つことの意義について検討し始めています。

主な調査結果

今回の調査結果からは、デジタル時代の課題と新たな機会に応えると同時に、安全に機能するIAMソリューションの必要性に関する認識が、ITの上級意思決定者の間で高まっている様子が見て取れます。

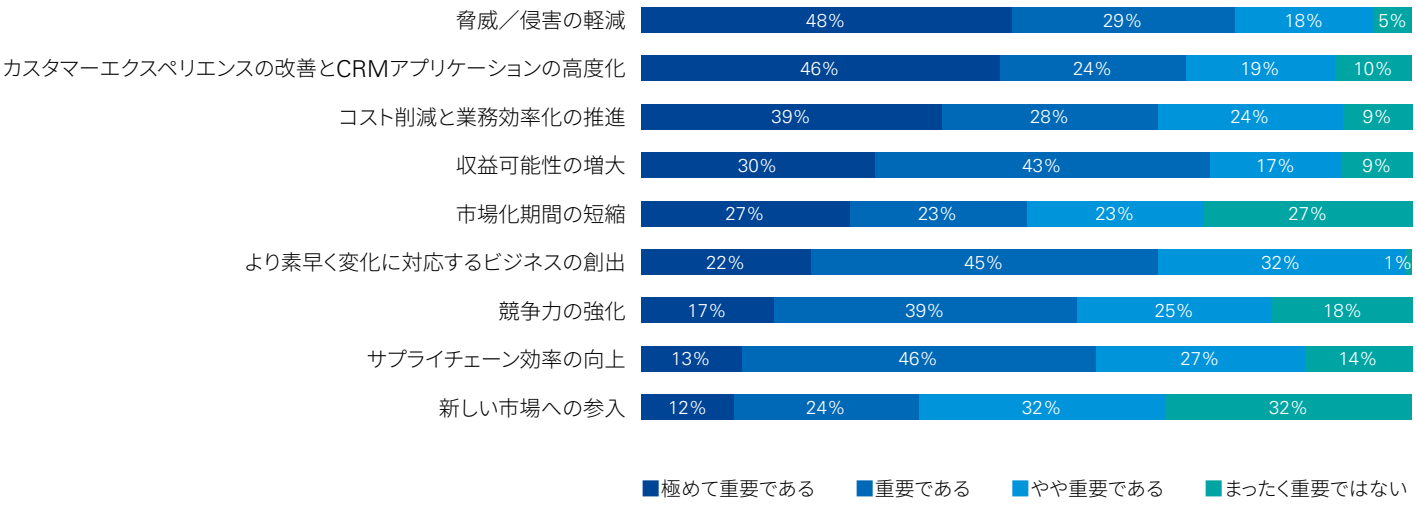
欧州の主だった地域の銀行、保険、製造、小売、サービス、通信、運輸および公的機関で活動するセキュリティ／情報担当の上級管理責任者は、セキュリティが確実に組み込まれない限り、デジタルトランスフォーメーションの到来による恩恵は得られないであろうと懸念しています。

デジタルトランスフォーメーション戦略の主要な目標は何かという質問を受けて、回答者の48%が、脅威や侵害の軽減が極めて重要であると回答しています。

カスタマーエクスペリエンスの改善やコスト削減と効率化の推進は、調査対象企業の優先課題であることが予想されていましたが、「脅威／侵害の軽減」は、この2つの項目より上位となりました。

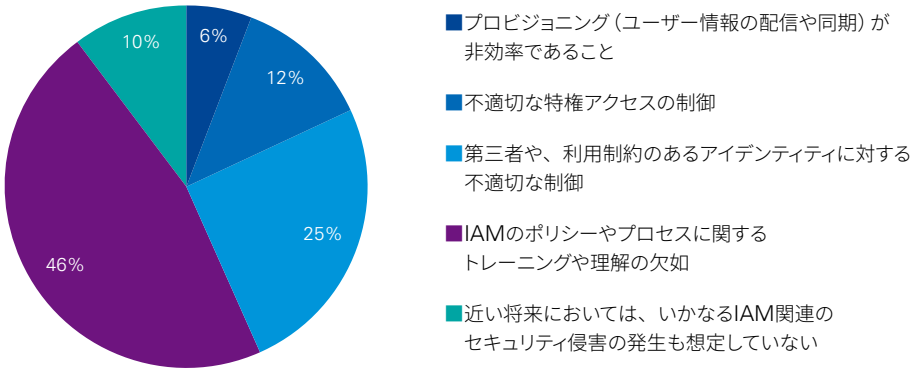
シャドーIT（正式に許可されていないアプリケーション、ハードウェア、クラウドサービスの購入）が、デジタル時代の安全なIAMソリューションに対する重大な脅威として浮かび上がっています。

図1：デジタルトランスフォーメーション戦略における各課題に対する重要性の認識



注記：小数点以下四捨五入のため合計値は100%にならないことがある

図2：今後発生すると考えられる、IAM関連のセキュリティ侵害の主な原因



注記：小数点以下四捨五入のため合計値は100%にならないことがある

回答者のうち46%が「IAMのポリシーやプロセスに関するトレーニングや理解の欠如が、今後発生すると考えられるIAM関連のセキュリティ侵害の主な原因になる」と予想しています。

他方で、企業がデジタルトランスフォーメーションを進めるにつれて、シャドー ITが、安全なIAMソリューションの開発を危うくする重大な脅威として浮かび上がっており、43%がシャドー ITを困難な課題であると回答し、22%が極めて困難な課題であると回答しています。

本調査のその他の要点：

- 92%の回答者が、今後3年間、IAMへの投資を維持または増額することを予定しています。
- 65%の回答者が、消費者向けのアイデンティティ管理とアプリケーションの提供を、次期のIAM投資の検討事項であるとみなしています。
- 57%の回答者が、次期のIAM投資として、（少なくとも部分的には）マネージドセキュリティサービスプロバイダー（MSSP）によって管理されるソリューションの採用を検討しています。

欧州では92%の組織が、今後3年間、IAMへの投資を維持または増額することを予定しています。

IAMとデジタル時代

デジタルトランスフォーメーションは、ビジネスモデル、テクノロジー戦略、そしてパートナー関係を変化させつつあります。なぜなら企業は、デジタル経済がもたらす新たな機会と課題に向き合う準備を進める必要があるからです。

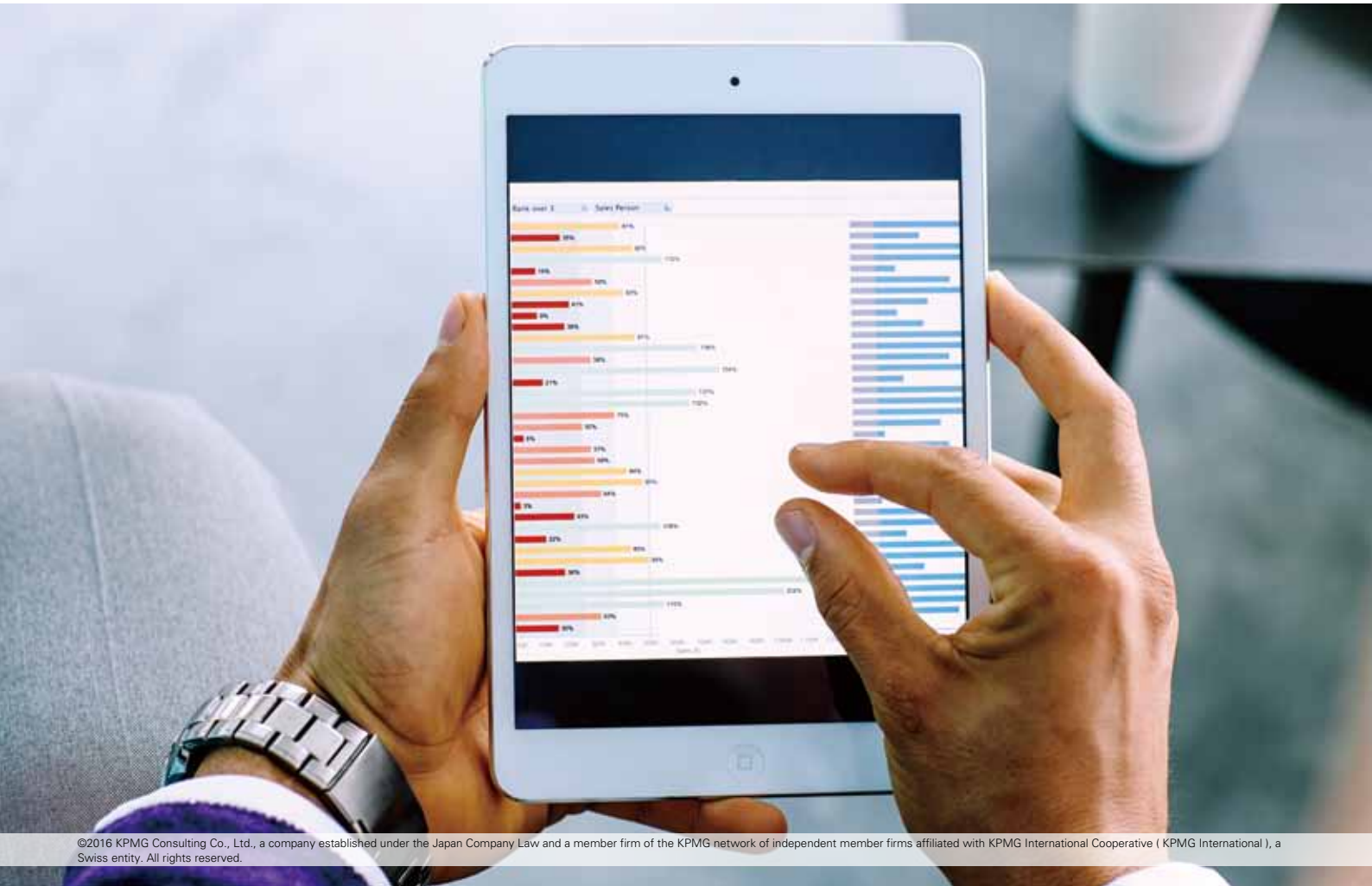
これは欧州全域で本格的に進展しているプロセスであり、約77%の回答者が「すでに企業全体でのトランスフォーメーション戦略を導入しているか、または一部の業務活動をすでに変更済みである」と回答しています。

これは大きな割合ですが、今後3年間のうちに、この数字はさらに増加する可能性が高いでしょう。なぜなら、ますます多くの企業が「デジタル市場で競争力を維持するには自社の組織自体がデジタル化する必要がある」と認識することが予想されるからです。

本調査は、かつてはデジタルへの変化に対する抵抗勢力とみなされていた保険や製造業などの業界でさえ、今では変革の取組みを加速させていることを示しています。

この調査結果は、従来のビジネス境界の外部でのデジタル化や、ソーシャルメディアを通じた消費者への接近、特に小売業界におけるオムニチャネル型の取引モデル活用の推進が加速していることを意味しているとも考えられます。

欧州企業の77%が、すでにデジタルトランスフォーメーションを進展させています。



また、一部の業界（例：公共、サービス、製造）におけるIoTテクノロジーの統合や、インターネットに接続された「モノ」（人の行動を記録するデバイスからコネクテッドカーまで）の利用全般も、デジタルトランスフォーメーションに含まれている可能性があります。さらにテクノロジーの面では、ハイブリッドデータセンター、DevOps（開発と運用の担当者同士が連携して協力する開発手法）、そしてアジャイルコンピューティングのような最新の開発動向にも、デジタルトランスフォーメーションの成果が取り込まれている可能性があります。

しかしいずれの場合でも、デジタルトランスフォーメーションの進展に伴ってアイデンティティの管理は、業務活動のセキュリティを実現するうえで主役を演じるようになり、IAMはセキュリティ／情報管理責任者だけでなく、他のチーフオフィサーレベルの意思決定者にとってもますます重要になるでしょう。

IAMの守備範囲拡大に伴う課題の1つは、デジタルトランスフォーメーションがもたらすリスクの増加について、あらゆるビジネスリーダーに理解させることです。

これが必要な理由は2つあります。1つは、コネクテッドデバイスの供給によって生じる攻撃対象の拡大。そして2つ目は、脆弱性の拡大が顧客情報や知的財産（IP）にまで対象を広げることです。

リスクを低減するために、情報担当のリーダーは、最初の設計段階から「モノ」をセキュリティプロセスと結び付ける必要性について、またセキュリティ侵害とそれに続くブランドへのダメージや投資家からの信頼喪失を避けるためにデータ保護を拡大強化する必要性について、取締役会を説得する必要があります。

銀行業界の41%は、すでに全社的なデジタルトランスフォーメーション戦略を導入しています。

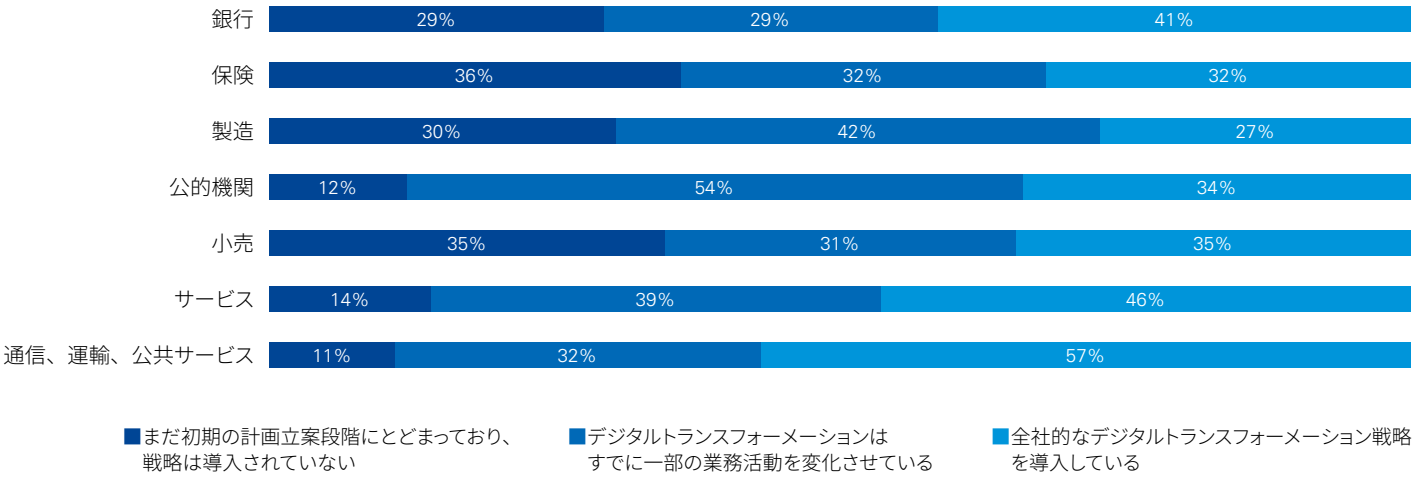
業界別のデジタルトランスフォーメーションの動向

デジタルトランスフォーメーションがIAMの計画立案にどのように影響しているかを判断するためには、各業界がどこまでデジタル化の道を進んでいるのか見定めることが重要です。デジタルトランスフォーメーションを強力に推進すると期待されていた一部の業界では、予想を裏切って進捗が遅れており、他方で遅れを取り戻す途上にある業界も見られます。

加えて、一部の業務活動に変化が見られるという回答も、その変化が包括的かつ全社的なデジタルトランスフォーメーション戦略を基盤としていることを指すとは限りません。

私たちの分析はこのことを考慮に入れていますが、それでもやはり基本的な動向は変革を目指す動きであり、それが真の牽引力を獲得していることは間違いありません。

図3：業務遂行全般におけるデジタルトランスフォーメーションの影響（業界別）



注記：小数点以下四捨五入のため合計値は100%にならないことがある

銀行業界では、41%の回答者が「すでに全社的なデジタルトランスフォーメーション戦略を導入している」と回答しています。

しかし小売業では、デジタル化の動きを先取りしている業界というイメージとは裏腹に、組織全体にデジタルを導入していると回答した企業は35%であり、31%は「デジタル化によって一部の業務が変化している」と回答しています。

製造業は相対的に遅れており、全社的なデジタルトランスフォーメーション戦略をすでに導入している企業は27%でした。

変革の鍵を握る業界の1つである公的機関は、今回の調査対象全体の中で最も多くの割合を占めており、欧州全域で変革を積極的に推進しています。

回答者のうち、34%は「組織全体でデジタル戦略を導入している」と回答していますが、おそらくより重要なことは、54%が「デジタルはすでに組織活動を変化させている」と回答していることでしょう。これは、本調査において他のどの業界よりも高い数字です。

これは2つの面で重要です。すなわち欧州全域の公的機関がコスト削減の圧力を受けていること、そして政府と地方自治体は顧客重視の姿勢をさらに強めるように要求されていることです。これはサービスのデジタル化という形で表われています。

英国政府は行政のためのデジタルプラットフォームの開発を言明しており、ドイツ連邦政府は2014年の白書、“The Digital Agenda”で全国規模のデジタルトランスフォーメーション政策を発表し、推進しています。この白書では“Digital Administration 2020”という表題のもとに、公共サービスの変革に対する連邦政府の公約も掲げられています。

両国、そして他の欧州諸国も、デジタル技術と高速ブロードバンド網は将来の経済成長にとって極めて重要であると考えており、

欧州全域で、公的機関はコスト削減の圧力を受けており、政府と地方自治体は顧客重視の姿勢をさらに強めるように要求されています。

そのために政府のデジタル化は必要不可欠であるとみなしています。EUは、デジタルトランスフォーメーション担当の委員長を任命しており、政府機関と企業の両方のデジタルトランスフォーメーションを推進するさまざまなプログラムを実施しています。

この変革プロセスの一部として考えられるのは、市民のデジタル空間でのアイデンティティを証明する仕組みを創設し、さまざまな省庁や政府機関のウェブサイトへのシームレスなアクセスを可能にすることです。

そして、その際に極めて重要なのは、アクセス権限とアイデンティティ管理に高いセキュリティを設けることです。これは単独企業のIAM要件を超えた課題であり、全市民が利用できるように、十分なセキュリティを備えたシステムの構築が要求されます。

この取組みで最も先行しているのが、公的機関とサービス業界（46%が組織全体でのデジタル戦略を導入済み）であることは、意外ではありません。両者とも、デジタルの課題に容易に適合できる無形の製品（ソフトプロダクト）を提供しているからです。

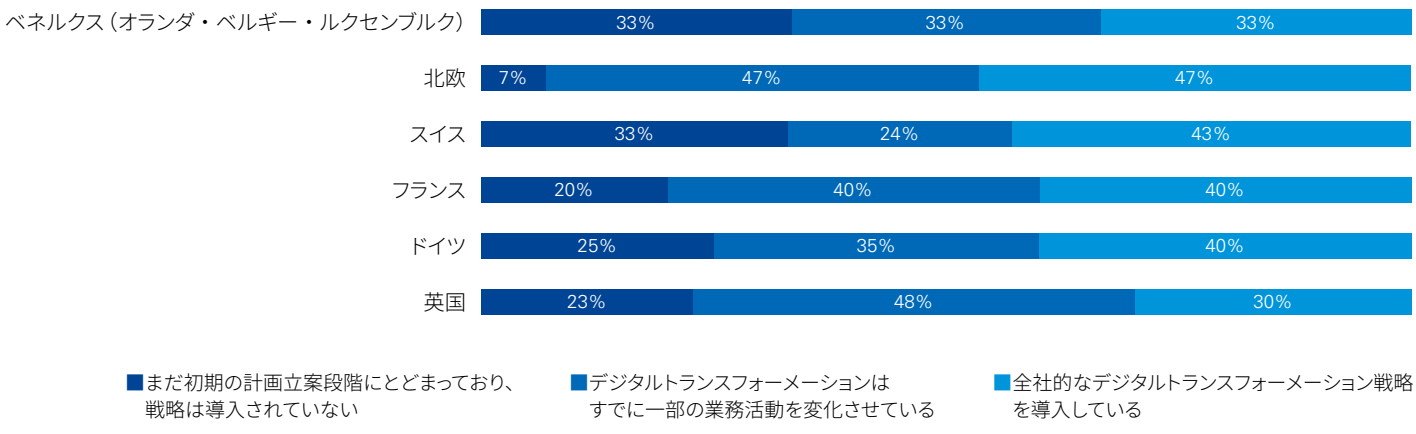
通信業界は、回答者の64%という最も高い割合で、全社的なデジタルトランスフォーメーション戦略を導入しています。

製造業と小売業は、いずれもまだ進むべき行程を残しています。保険会社と銀行の大部分は「まだ戦略を導入していない」と回答していますが、そうした既存企業は、フィンテック（FinTech）の新興企業から破壊的な影響をこうむる恐れがあります（特に、英国、フランス、ドイツの企業が考えられます）。

実際、金融と保険は極めて競争の激しい市場であり、競争力を維持できるかどうかは、顧客との緊密な関係と付加価値サービス次第です。

デジタル化は国によって多様なペースで進んでいますが、現在のところ集団から抜け出して独走態勢に入っている国は存在しません。

図4：業務遂行全般におけるデジタルトランスフォーメーションの影響（地域別）



注記：小数点以下四捨五入のため合計値は100%にならないことがある

デジタルビジネスのセキュリティをIAMによって保護する

組織におけるデジタルトランスフォーメーションの主な目標は何かと質問したところ、意外な結果とほぼ予想どおりの回答が混在していました。

回答者の48%が「脅威や侵害の軽減はデジタルトランスフォーメーションの実現において、特に必要な前提条件である」と考えていた点には着目する必要があります。

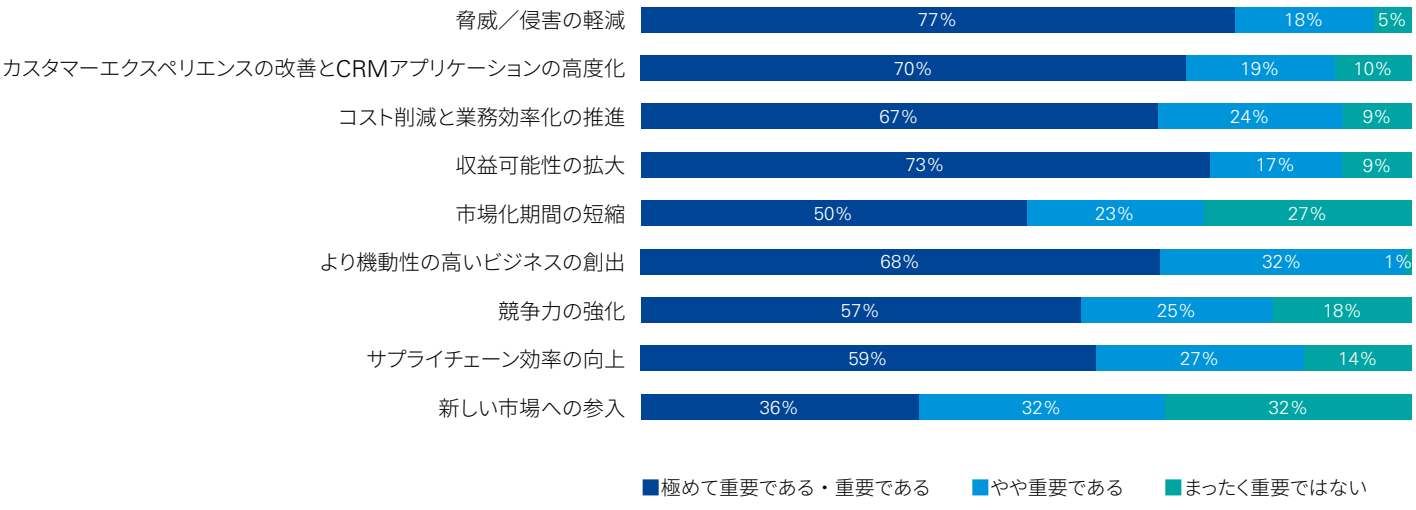
それは、回答者がそれぞれの組織の中で十分な影響力を保持しているならば、最初の段階からセキュリティが考慮された形でトランスフォーメーションが推進される可能性が高まるからです。

今回の調査回答者がセキュリティを大きな課題として認識していたことは事前の予想どおりでしたが、そうした回答者はセキュリティだけではなく、ビジネスニーズにも目を向けています。その証拠に、回答の中には、セキュリティの枠を超えて、ビジネストランスフォーメーションにおける戦略的な目標についても高い数字が見られます。

それには、カスタマーエクスペリエンスの改善、業務効率化の推進、収益可能性の拡大などが含まれています。

欧州のシニアITリーダーの48%は、脅威や侵害の軽減を、デジタルトランスフォーメーションの推進において極めて重要な要素であると考えています。

図5：デジタルトランスフォーメーション戦略の個別目標に対する重要性の認識



注記：小数点以下四捨五入のため合計値は100%にならないことがある

ほぼすべての組織が、ビジネスにおける機動力を高める必要性を理解しています。実際、組織のデジタルトランスフォーメーション戦略には、必ずビジネスの機動力の向上が組み込まれています。

興味深いのは「新しい市場への参入」を「極めて重要」と回答した割合が最低の数字になっていることです。なぜならデジタルトランスフォーメーションは、新たな市場参入ルートを切り開いてくれる見込みがあるからです。Apple Payがその一例です。

EU一般データ保護規則の影響

アイデンティティ／アクセス管理は、基本的に、組織におけるセキュリティ侵害の防止に役立つように設計されています。また侵害防止は、今では基本的なビジネス目標の1つでもあります。

セキュリティ侵害が業務や社会的評価にもたらすダメージや信用の失墜は別としても、まもなくEU域内では、侵害から生じる規制上のコストが急激に増加することになるでしょう。

EU一般データ保護規則（GDPR）が新たに施行されると、サイバー攻撃やその他の原因でデータを消失した企業は、厳しい状況に陥ることになるでしょう。2018年4月から、EU住民に関するデータを保持している事業体は、その漏えいによって最高で売上の4%または2,000万ユーロ（どちらか多い方）の罰金を科される可能性があり、いかなるセキュリティ侵害も72時間以内に報告することが義務付けられます。

GDPRは、計画段階で極めて長い間、足踏み状態にあったので、情報セキュリティの専門家のほか、多くの経営者からも見過ごされていた可能性があります。しかし、こうして規制の施行が現実となった以上、今からGDPR対策をリスク管理戦略の中に組み込んでおくべきです。そしてその一環として、デジタルトランスフォーメーションに起因する侵害リスクの増加に対処するための将来的なアイデンティティ／アクセス管理（IAM）ソリューションに関する意思決定も行う必要があります。

2,000万ユーロまたは年間売上の4% — GDPRを遵守しない事業体は、この金額を罰金として支払う必要があります。

IAMに関する脅威ベクター

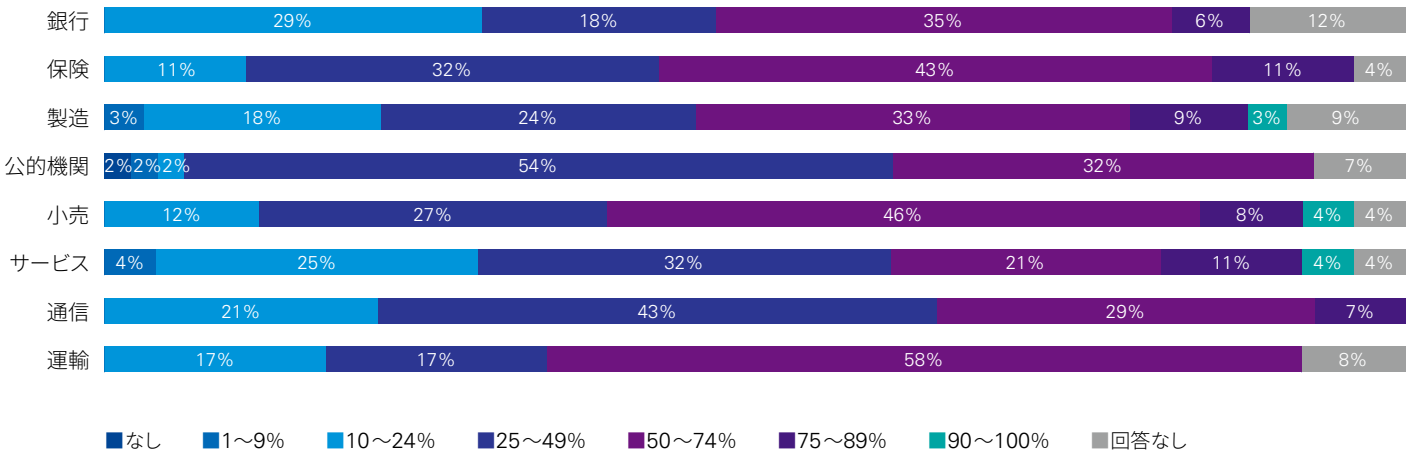
デジタルは、モバイル、クラウド、シャドー ITなどを含む多数のベクターにわたって、脅威を増大させるでしょう。

モバイルコンピューティング

モバイルコンピューティングは、事業変革が進むにつれてアイデンティティのセキュリティに影響を及ぼすことが予想され、しかもあらゆる業界で発展しています。

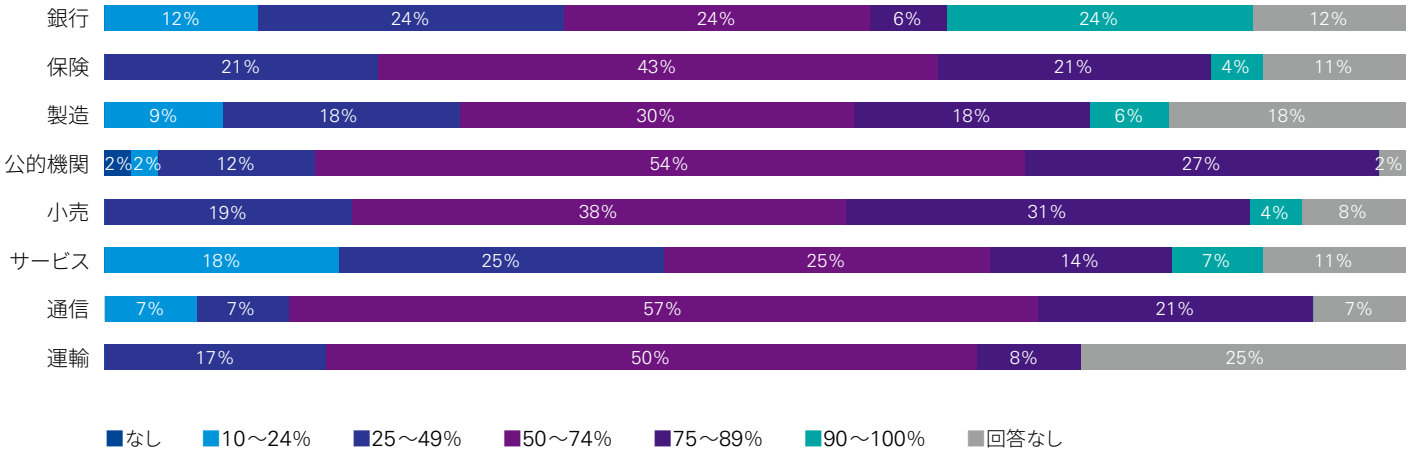
銀行は保守的な業界の1つであり、インフラを従来の境界領域外に拡大することに消極的なため、モバイル利用は依然として他の業界の後塵を拝しています。(混合型の産業である) サービス業は別として、銀行は今後もモバイル機器を使用していない従業員の割合が最も高い業界 (図7の10～24%および25～49%の割合) であり続けると予想されています。

図6：現在、企業サービスへのアクセスにモバイル機器を使用している従業員の割合



注記：小数点以下四捨五入のため合計値は100%にならないことがある

図7：3年後、企業サービスへのアクセスにモバイル機器を使用していると予想される従業員の割合



注記：小数点以下四捨五入のため合計値は100%にならないことがある

これは特に従来型の職場（例：支店など）に基づいた結果ですが、自分の机のみで仕事をしているバックオフィスにも部分的に当てはまります。

他方で、3年後に90～100%域が占める割合の増加は著しく、一部の銀行は従来の職場の慣行から脱却して、モバイルビジネスの実現を目指す業務の抜本的な変革を（おそらく対抗勢力の異論を払いのけつつ）進めている様子が見て取れます。

通信は、予想に違わずモバイル化しつつあります。これはセキュリティ分析の複雑さを増大させます。なぜなら、システムはどのユーザーがどのような機器や「モノ」を使用しているかという関係性を理解する必要が生じ、さらにはアクセスの前後関係も理解しなければならなくなるからです。今後ますます増大する複雑さに対処するためには、高度なセキュリティ分析が必要不可欠になるでしょう。

全体として、モバイルの利用率の増加は、あらゆる業界にわたる私たちの予測と整合しており、その数字はさらに大きくなる可能性もあるでしょう。

セキュリティ部門は、クラウドとオンプレミスシステムの両方を取り扱う能力が必要となるでしょう。

クラウド

クラウドへの移行については、すべての業界が「3年後にはクラウドに移行された企業システムが増加している」と回答しています。

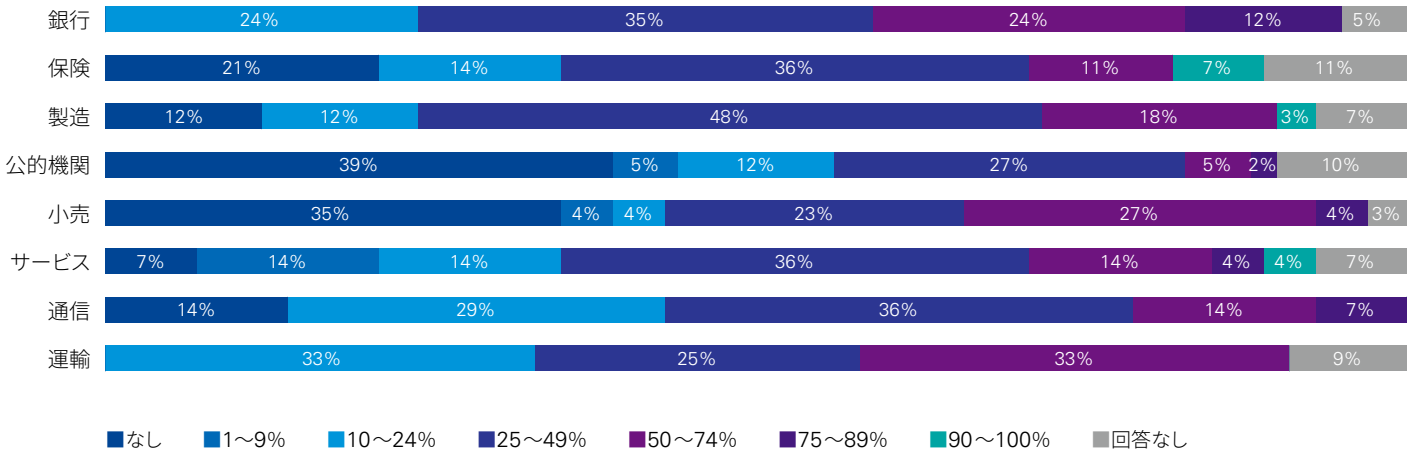
ここでの興味深い特徴は、以前はクラウドを忌避していた業界すべて（銀行、保険、公的機関など）がクラウドへの移行を見込んでいることです。

これは、特に公的機関ではコスト面での判断が作用していると考えられます。しかしセキュリティの懸念は残るでしょう。特に

トランスフォーメーション計画によって、従来なら部外者だった人々や組織（たとえば消費者やサプライチェーン先）にも企業システムへのアクセスが許可されるようになる場合は、その懸念は大きくなります。

すべての組織がますます多くの業務をクラウドに移行させています。セキュリティ部門は、クラウド（パブリック、プライベート、ハイブリッド）とオンプレミスシステムの両方を取り扱う能力が必要となるでしょう。

図8：3年後にクラウドに置かれていると予想される企業システムの割合



シャドー IT

さらに、このデジタル時代においてすでに「大問題」に陥りつつある1つの分野があります。それは、現在も依然としてIT関係者の中で論争のテーマとなっているシャドーITの拡大です。

シャドーITは、企業主導の戦略が存在しない状況において、従業員が自ら、ほとんど組織的にデジタルトランスフォーメーションを遂行しようとする意思の表明であるとも言えます。

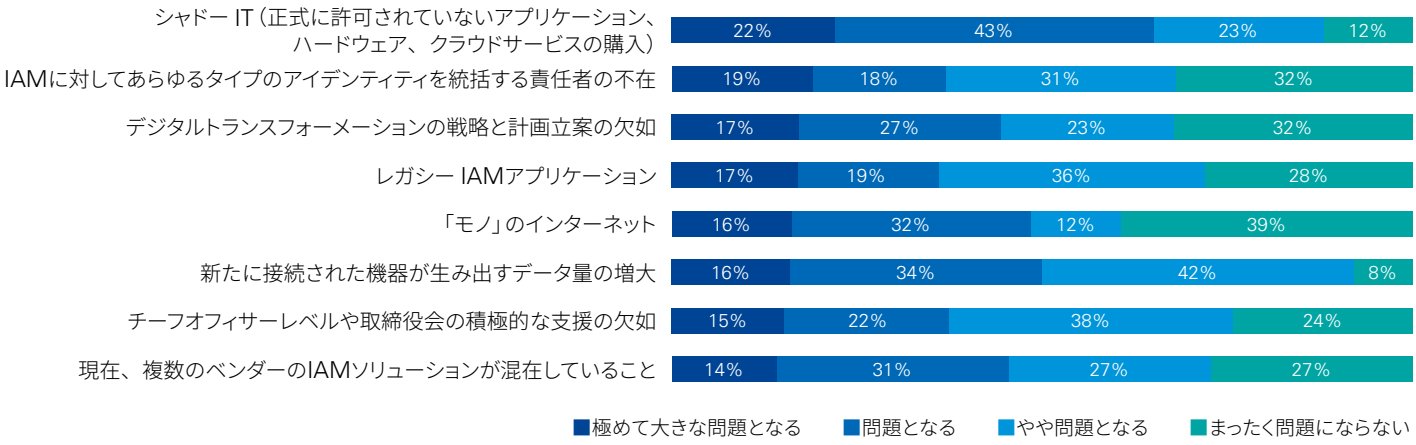
ウェブベースのアプリケーション、クラウドリソース、モバイル機器、そして仮想ツールの導入の容易さと低コストは、IT部門の調達先を新しい領域へと拡大させてきました。

AWS、Dropbox、BoxおよびSalesforceなどのアプリケーションを従業員は熟考せずに使用しているのですが、同時に、従業員はそうしたアプリケーションを極めて生産的に、良い意図を持って使用することで、プロジェクトを成し遂げようとしていることも事実です。この動きは今後さらに加速し続けるでしょう。

また、普段からさまざまなメッセージングやソーシャルアプリケーションを個人所有機器にインストールし、その使いやすさから業務用として使用する従業員もいますが、そうした機器が正式に許可または安全化されていないことも少なくありません。

欧州の情報セキュリティ担当の上級意思決定者の65％が、シャドーITを安全なIAMソリューションの展開を阻害する課題であるとみなしています。

図9：今後2～3年間で、自社のデジタルトランスフォーメーションを後押しすることに役立つ安全なIAMソリューションの展開に対して阻害要因となり得る課題



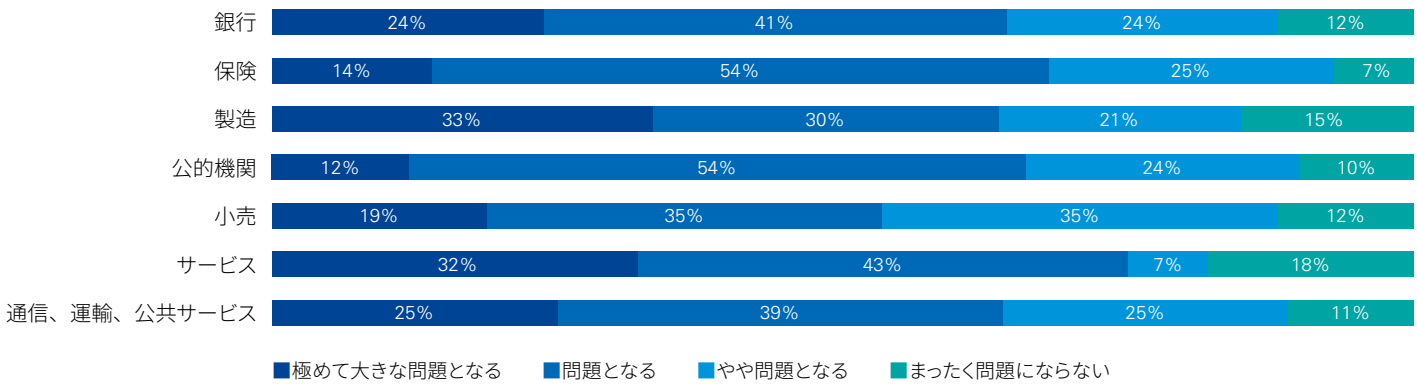
注記：小数点以下四捨五入のため合計値は100%にならないことがある

最高情報責任者（CIO）、最高情報セキュリティ責任者（CISO）およびITセキュリティ部門にとっての課題は、たとえビジネス上のメリットが明らかでも、そのようなアプリケーションが新たな脆弱性を招き寄せ、潜在的にセキュリティに問題があるアクセスポイントを生み出すことです。

こうした懸念が回答者の念頭にあることは明らかです。その証拠に、22%がシャドー ITを安全なIAMソリューションの導入を危うくする「極めて大きな問題となる」とみなし、43%が「問題となる」とみなしています。

ここで重要となるのは、IAMサプライヤーとIAMに注力するMSSPが、シャドー ITを十分に考慮した形でそれぞれのソリューションを開発することです。これはユーザーとベンダーの双方にとって今後ますます重要となります。

図10：今後2～3年間で、シャドー ITはデジタルトランスフォーメーションに役立つ安全なIAMソリューションの開発に、どの程度問題となるか？

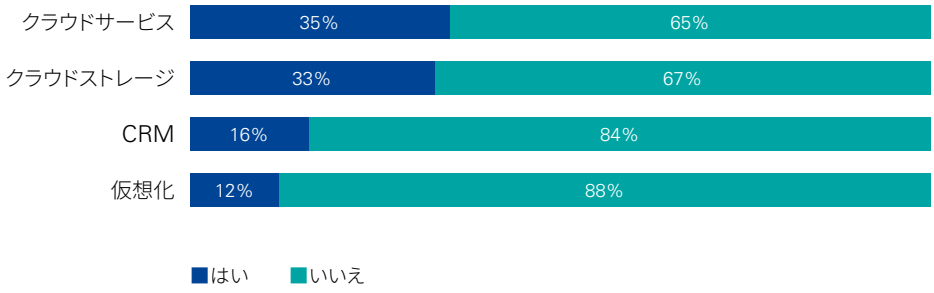


注記：小数点以下四捨五入のため合計値は100%にならないことがある

クラウドも影響を及ぼしています。組織はクラウドへの移行を管理するための適切なリソースを必要としています。たとえば、周到に考案されたクラウドリスク評価を、IT部門だけでなく調達部門でも実施するように義務付けることなどです。

複数ベンダーの製品が混在する古いIAMソリューションを一掃したいという要望とその機会が存在しています。

図11：自社の従業員が、これらのアプリケーションのいずれかをIT部門に相談せずに使用しているか？



従業員が許可なしでクラウドサービスにアクセスしていると回答したのは35%であり、続いてクラウドストレージが33%、CRMツールが16%、仮想化が12%でした。

この場合、数字が小さいから望ましい結果であるとは言い切れません。たとえ少数でも、許可されていないリソースへのアクセスや使用を行う従業員がいるということは、セキュリティリスクなのです。クラウドストレージの無許可利用が多いことは、IT部門の統制が及ばない場所に相当な量の機密情報が保存されていることを意味します。

複雑かつ予測困難にならざるを得ない変革のプロセスを企業が辿る途上では、そのようなシャドー ITの使用はさらに多くのリスクを引き起こす恐れがあります。

シャドー ITは、特権アカウント管理（PAM）の効果的な導入を危うくする脅威の2番目に挙げられており、回答者の26%が懸念を表明しています。無許可のアプリケーションやクラウドが増加するにつれて、何が本物の特権アカウントなのか、そしてどれがサポート対象外または規制対象であり、そのうちのどれが本当の従業員に属するものなのかを判断することがますます困難になっています。

また別の問題として、複数ベンダーの製品が混在する古いIAMソリューションを一掃したいという願望とその機会も、明らかに存在しています。

約31%が、シャドー ITが安全なIAMソリューションを実現する障害になると考えています。シャドー ITとクラウドがすでに引き起こしているセキュリティの懸念と課題を踏まえると、機能の寄せ集めから成り立つ古いIAMシステムがもたらす脆弱性が懸念材料になることは間違いありません。

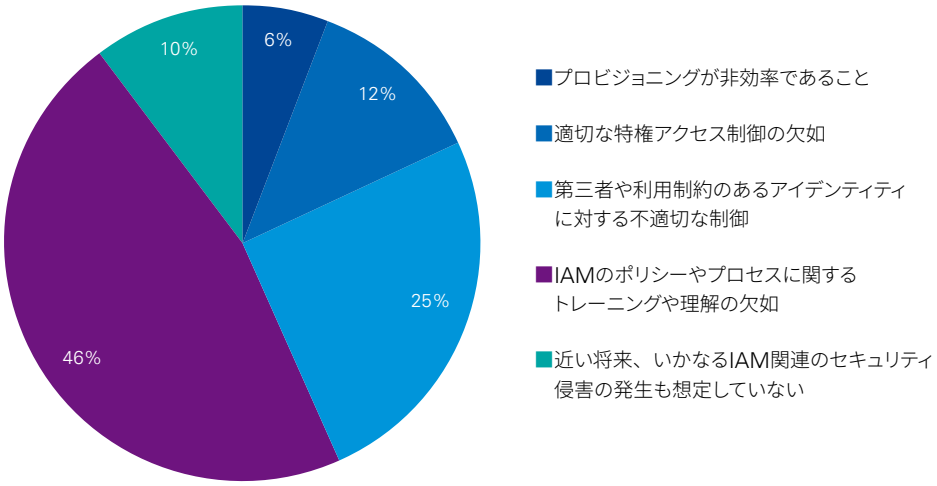
IAMがもたらすものとリスク

私たちはサイバー攻撃が絶えず続く時代に生きており、いかなる企業や組織もセキュリティ侵害から無関係ではいられません。そして、規則が破られたり、IT部門が許可していない業務の変更が行われたりすれば、優れたIAMソリューションでさえ侵害を受ける可能性があります。欧州企業のセキュリティは、シャドーITの拡大によってますます大きな脅威に晒されています。

私たちは今回の調査で、企業が次に発生するIAM関連の侵害の主な原因は何であると捉えているかを知りたいと考えました。セキュリティ意識向上トレーニングの有効性を認めていない企業の回答者にとって、この調査結果は警鐘の役割を果たすかもしれません。

あらゆる業界の全回答者の46%が「IAMのポリシーやプロセスに関するトレーニングや理解の欠如がIAM関連のセキュリティ侵害を引き起こす可能性がある」と考えていました。そうした状況は、デジタルトランスフォーメーションの複雑さが影響力を増すにつれて、さらに悪化する恐れがあります。

図12：今後発生すると考えられる、IAM関連のセキュリティ侵害の主な原因



注記：小数点以下四捨五入のため合計値は100%にならないことがある

企業は自社の同僚の認識不足を非難しているのでしょうか？ それとも、遅きに失する前に、特にアイデンティティの数の増加に関連して、内部の関係者に起因する脅威のリスクを警告しているのでしょうか？

業界別にみると、サービス業、通信業および運輸業は、IAMに関するトレーニングと理解の欠如を最も懸念しています。

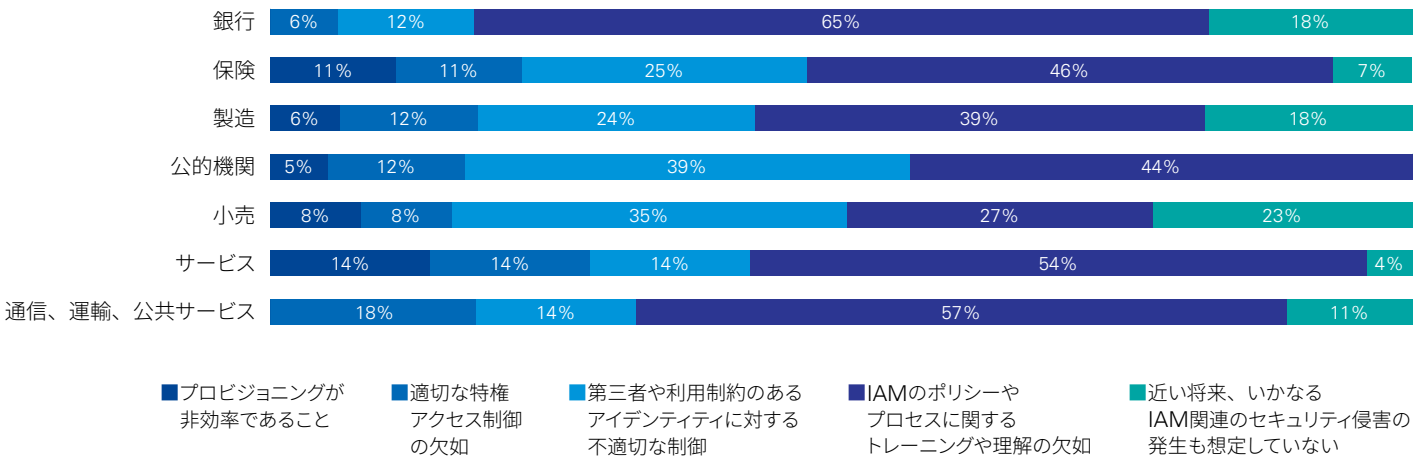
逆説的なのは近い将来、IAM関連の侵害は発生しないと確信している割合が全業界にわたって驚くほど高いことであり、10%がそのような見方を表明しています。この結果はあまりにも楽観的であると言えます。

すべての技術的な統制手段と並んで、情報セキュリティに関する従業員の教育とトレーニングは必要不可欠な要素です。

たとえテクノロジーが完璧でも、人間が失敗すれば物事は悪い方向に進みます。その端的な例は、リソースへの過剰なアクセスを許可することです。

全業界を通じて、ITの上級意思決定者の46%が「IAMのポリシー、プロセスに関するトレーニングや理解の欠如がIAM関連のセキュリティ侵害を引き起こす可能性がある」と考えています。

図13：自社で次に発生すると考えられるIAM関連のセキュリティ侵害の主な原因

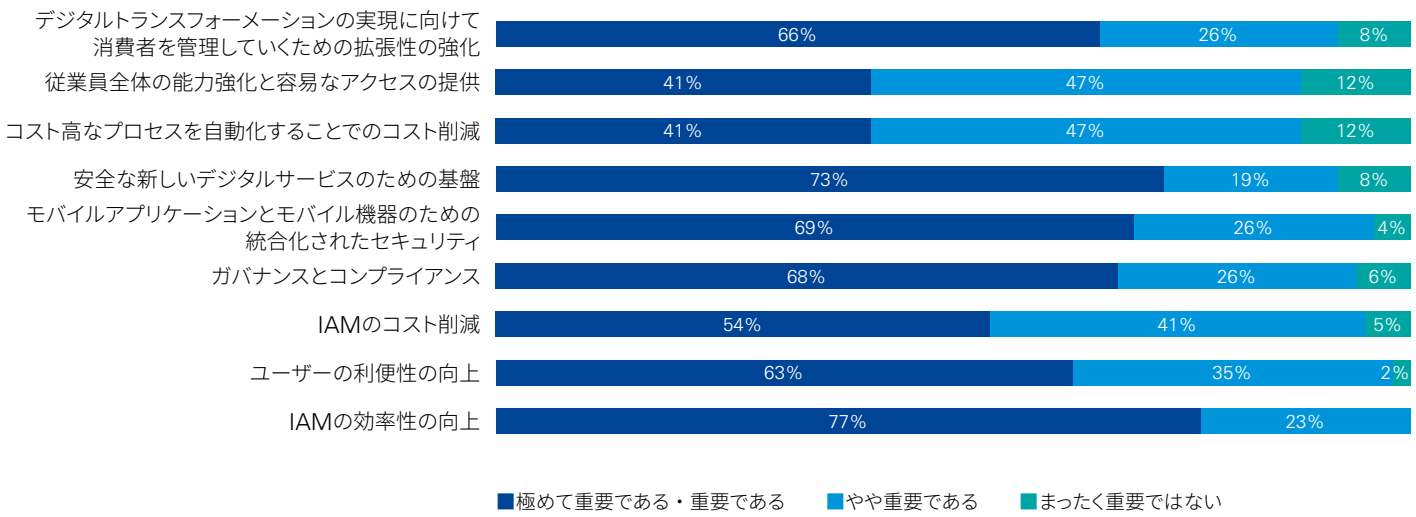


注記：小数点以下四捨五入のため合計値は100%にならないことがある

IAMに関するデジタル世界で果たすべき目標は明らかになっている

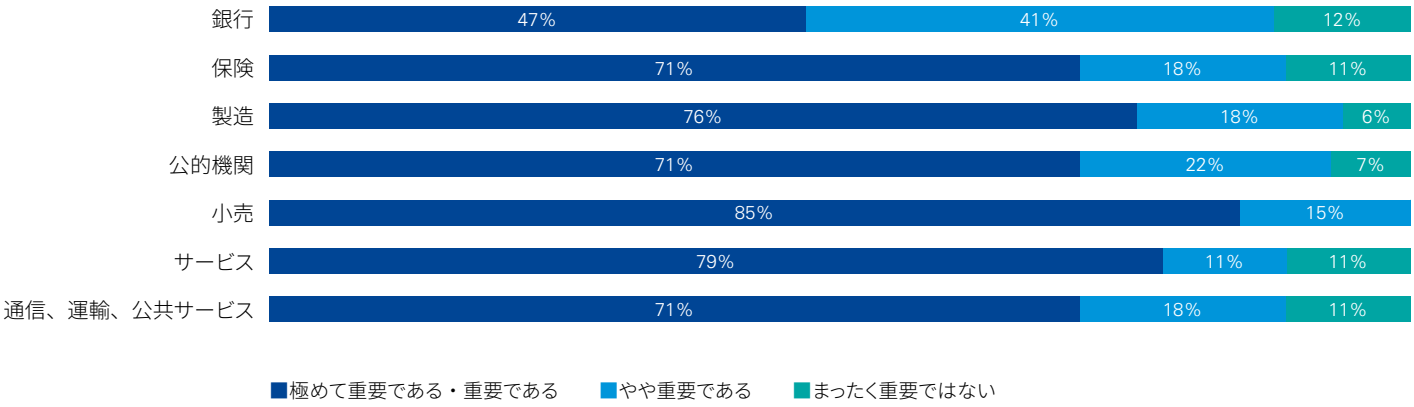
回答者は、セキュリティの枠を超えて、既存のIAMソリューションの目標として何を目指しているかという点についても明確にしていました。「デジタルトランスフォーメーションの実現に向けて消費者を管理していくための拡張性の強化」について、21%が「極めて重要である」、45%が「重要である」とみなしているという結果に、デジタルに対する認識の深まりが表れていました。

図14：企業のセキュリティという範囲を超えて考えた場合、現在のアイデンティティ／アクセス管理（IAM）アプリケーションが担っている各役割はどのくらい重要か？



注記：小数点以下四捨五入のため合計値は100%にならないことがある

図15：IAMを安全な新しいデジタルサービスの基盤にすることの重要性に対する認識



注記：小数点以下四捨五入のため合計値は100%にならないことがある

さらに望ましいことに、IAMを安全な新しいデジタルサービスの基盤にすることについて、24%が「極めて重要である」、47%が「重要である」とみなしていたことです。

これはすべての業界と国で見られ、意思決定者がデジタルを重視していることを示しています。

ただし、効率性の向上は依然として最上位の目標であり、40%がこれを「極めて重要」と評価していました。

同時に、リスク軽減はあらゆるIAMソリューションの重要な要因であり続けています。全業界を通じて、かなり高い割合の回答者が「全社的リスクマネジメント（ERM）との統合と連携レベルの向上をあらゆるIAM投資の必要不可欠な要素である」とみなしています。

デジタルトランスフォーメーションがERMに影響を及ぼすかどうかに関する質問に対して、35%が影響の存在に全面的に同意し、46%が「IAMはそれに対処すべきである」と回答しています。

欧州組織の41%が2016年にIAMへの投資を増額する見通しです。

IAMへの投資のパターン

PACによる市場分析では、IAM市場の取引高は2016年から2019年の間に成長し続けると予想されています。代表的な見通しとして、図16に英国市場の予想数値を示します。

このような成長は、すでに課題が山積しているセキュリティの状況に対するIAMの重要性を浮き彫りにしています。

本調査の結果は、デジタルトランスフォーメーションに伴って新たに生じる課題に対処するために、堅牢なIAMソリューションが必要であることを一層強く裏付けています。

IAM投資の意向に関する質問からは興味深い回答が得られており、消費者のアイデンティティが表れています。

ほとんどのIAM専門家は「デジタルトランスフォーメーションに対処するように設計された堅牢なIAMシステムは、消費者のアイデンティティを処理する能力を必ず備えなければならない」と考えています。

さらに、今回の調査に回答した欧州のセキュリティ／情報管理責任者の意見も、これを裏付けているように思われます。

73%の回答者は、エンドポイントのセキュリティをIAM投資の計画立案における主要な要因として含めていましたが、続いて65%の回答者が、消費者アイデンティティを扱うアプリケーションと消費者アイデンティティ管理を挙げています。

図16：IAMへの投資予算は2016年に増額と減額のどちらになると予想するか？

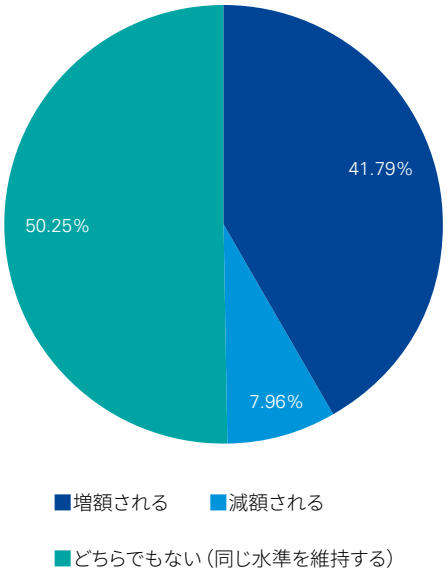
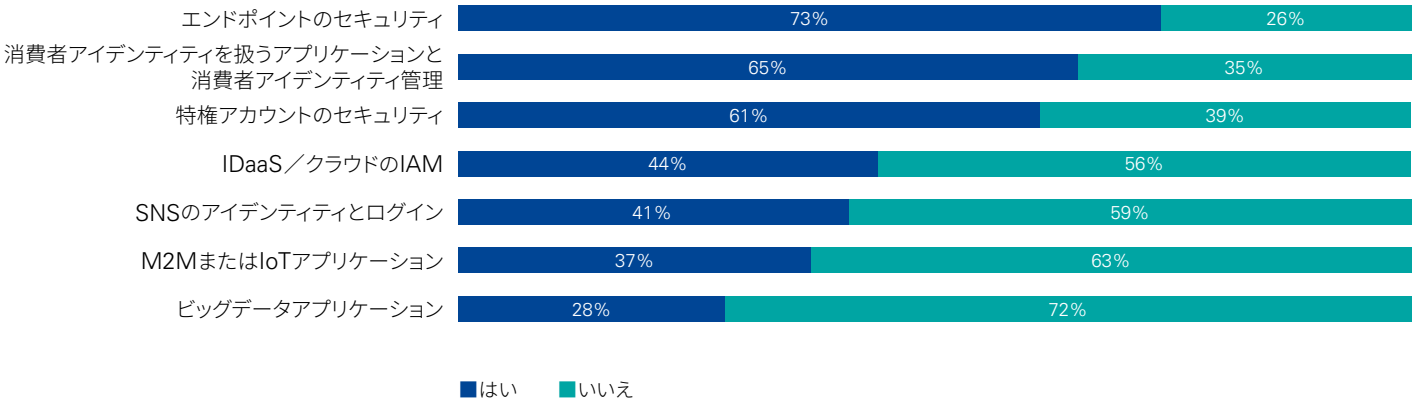
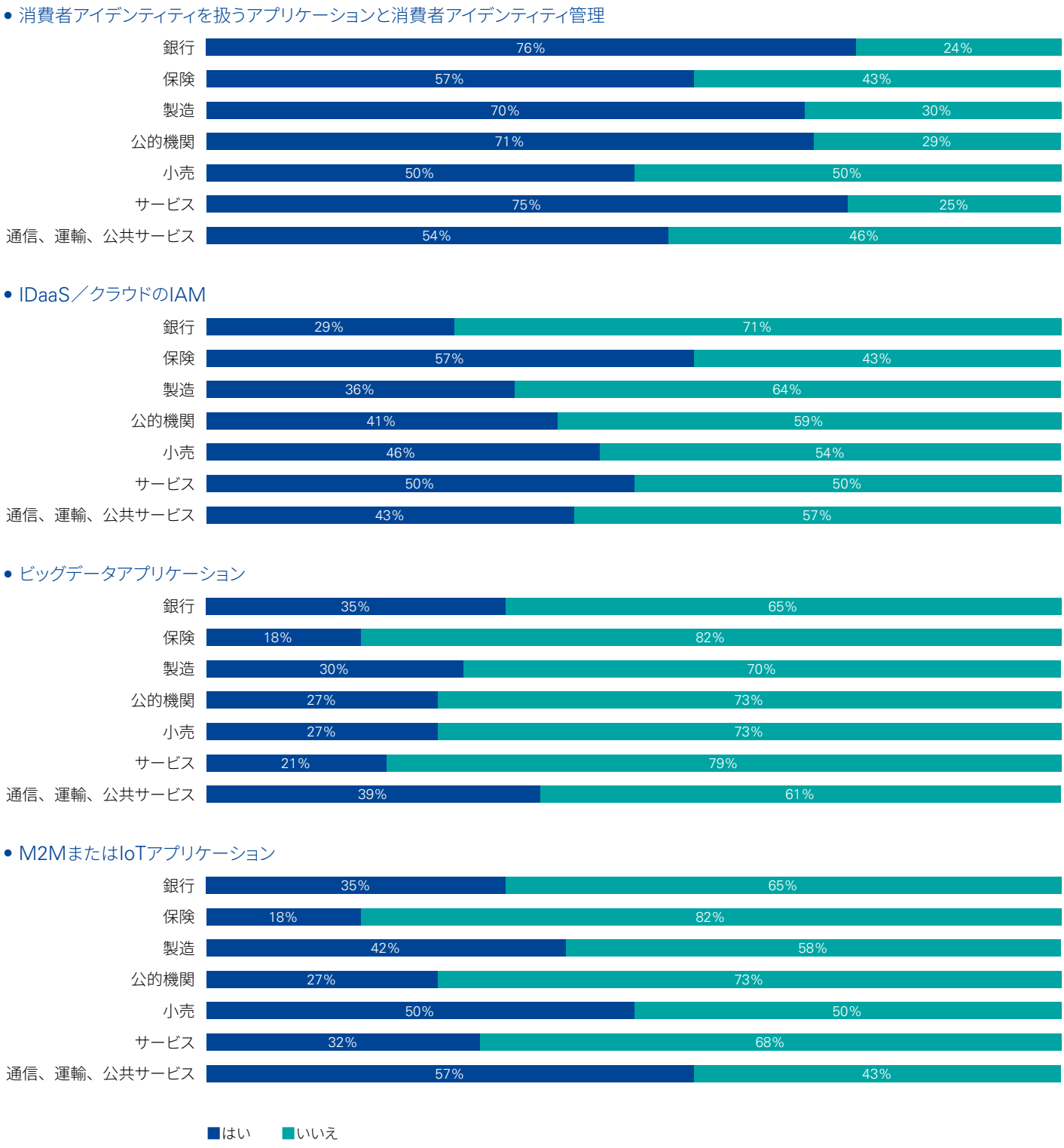


図17：IAMへの投資計画には、これらの要素が盛り込まれているか？（全業界）

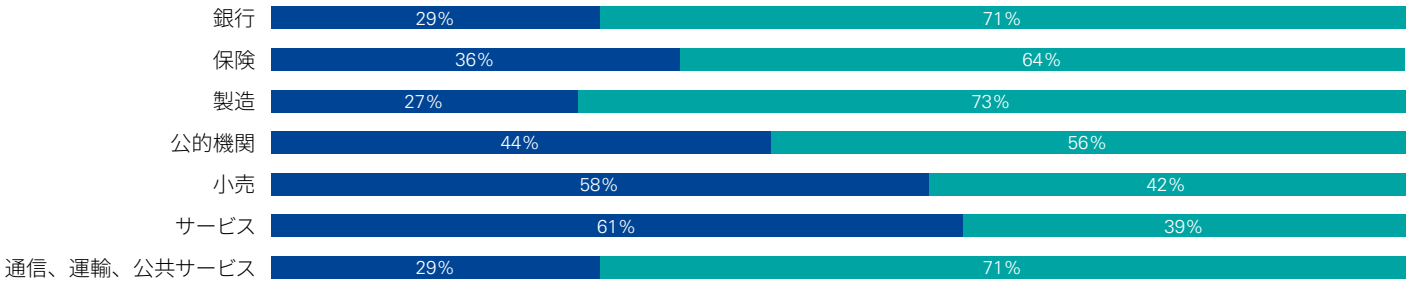


注記：小数点以下四捨五入のため合計値は100%にならないことがある

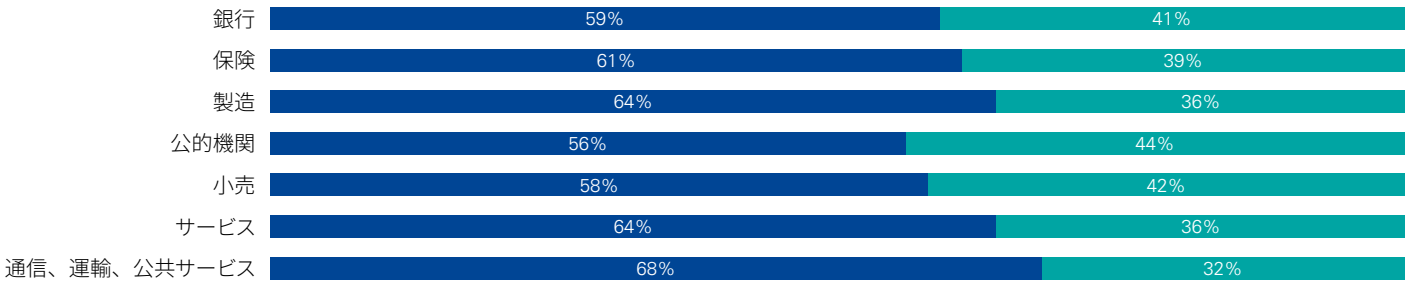
図18：IAMへの投資計画には、これらの要素が盛り込まれているか？（業界別）



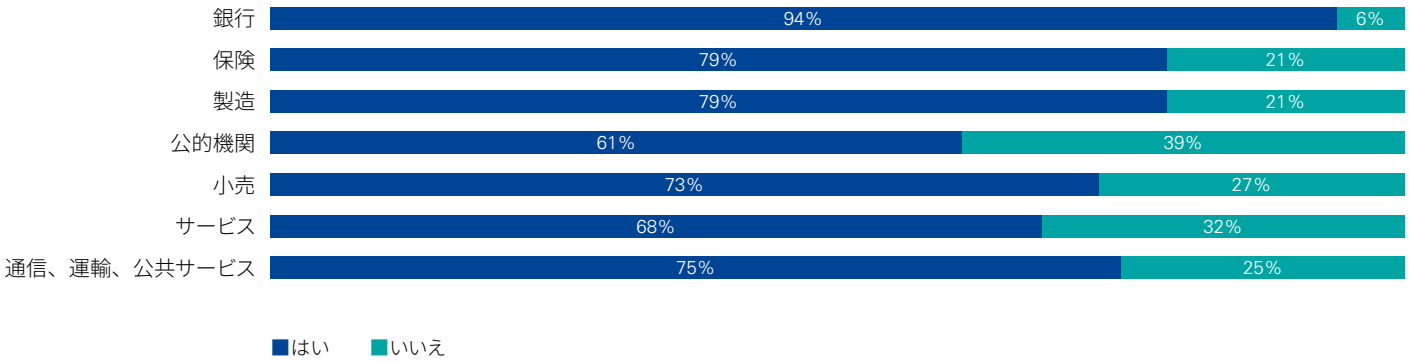
• SNSのアイデンティティとログイン



• 特権アカウントのセキュリティ

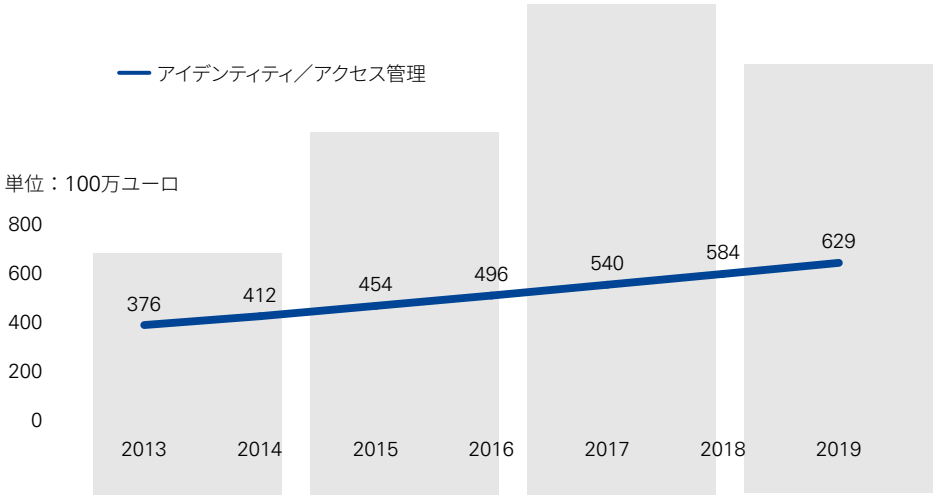


• エンドポイントのセキュリティ



さらに興味深いことは、SNSのアイデンティティとそのログインであり、これは今回の調査サンプルの41%によって選ばれていました。明らかに、今回の回答者は、将来のIAM投資計画を策定する際に、従来のセキュリティの守備範囲であると解されている領域から大きく外れたところまで考慮しています。

図19：英国のセキュリティ市場の規模



デジタルトランスフォーメーションが完全に実現されたステージにまだ達していない企業でも、さらには、まだ初期段階にとどまっている企業でさえも、従業員や特権アカウントという従来の領域のアイデンティティをはるかに超えた領域のアイデンティティまで考慮に入れることの重要性を認識しているのです。

全体として、今回の調査では、M2MとIoTも含めてすべてのデジタル化の契機に対して健全かつ有望な反応が返ってきました。このことは、デジタルへの理解が高まっていることを示唆しています。

セキュリティ計画の立案者が、将来のIAMソリューションに関するこうした新しいデジタルの課題をセキュリティ計画の立案者がどのように管理する意向であるかに目を向けると、興味深い構図が見えてきます。

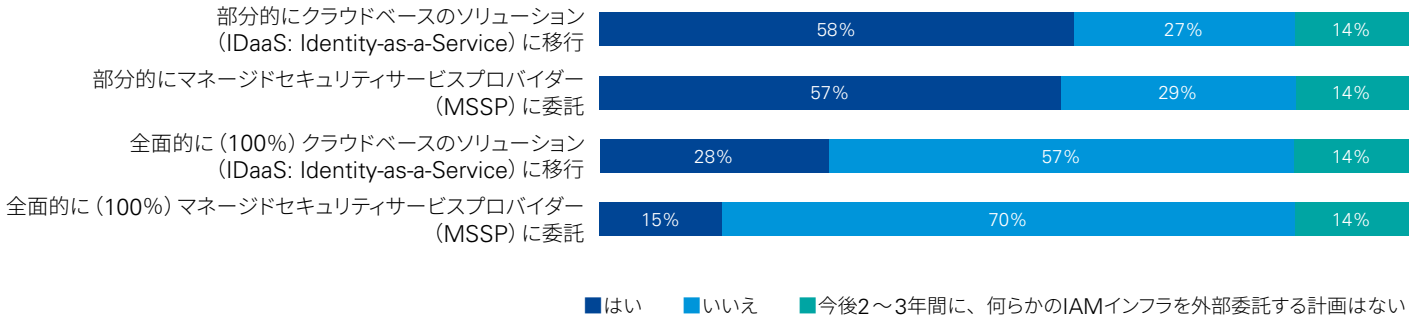
サイバーセキュリティの他の領域では、長年にわたってマネージドセキュリティサービスプロバイダー（MSSP）がウェブや電子メールのフィルタリングなど、アプリケーションの日常的な実行の管理を委託されてきました。

しかし、もし今回の調査におけるすべての業界と国の回答を信じるならば、IAMソリューションについては、MSSPへの信頼はまだ十分なレベルに到達していません。

IAMをMSSPに全面的に外部委託（アウトソース）することを計画しているのは回答者のわずか15%に過ぎず、部分的な外部委託を計画しているのは57%でした。MSSPはこうした動向を真剣に受け止める必要があるでしょう。IAMをMSSPの手に委ねても安全であることを納得させるために、MSSPができることは何でしょうか？

それに比べれば、クラウドベースのIDaaS（identity as a service）ソリューションは、リスクが少ないとみなされており、28%がその外部委託に積極的であり、58%は部分的にアイデンティティ機能の一部を外部委託する意向を示しています。

図20：今後2～3年間に、IAMインフラの何らかの部分を外部委託する計画はあるか？



注記：小数点以下四捨五入のため合計値は100%にならないことがある

ここで指摘しておくべきことは、MSSPに依存することで、クライアントはより多くの統制権をMSSPに委ねることになり、それはリスクが大きいということです。一方で、IDaaSはプラットフォームを外部委託先の管理下に置きます。

さらにMSSPへの外注の数字が低いことは、クラウドやMSSPではあらゆるものを管理することは難しい、という事実に起因すると考えてほぼ間違いないでしょう。たとえば、旧型のアプリケーションのためのIAMを考えてみればわかります。

ほとんどの組織は、IAMの一部をクラウドで実行することを計画していますが、その大半は、何らかのIAM機能をオンプレミスに残しておくでしょう。その理由は、おそらく既存のオンプレミスアプリケーションをサポートする必要性があるからです。またマルチベンダーの古いIAMソリューションの存在もその1つの要因でしょう。

さらに、IDaaSは、クラウドアプリケーションへのアクセスを管理することや、新しいタイプのユーザー集団（例：顧客）によるアクセスを管理することに最も適しているのに対して、既存のオンプレミスIAMはより複雑な要件を満たすように最適化されています。

以前と比べると、コスト削減は目標として選ばれなくなっています。組織は次第にビジネス能力の強化に目を向けるようになっており、その手段としてモバイルワーカーの支援（69%がこの項目を「極めて重要」または「重要」と評価）、新しいデジタルサービスの実現（72%）、消費者のアイデンティティ情報へのアクセスの管理（66%）などに注目しています。

欧州企業の15%がIAMを全面的にMSSPに外部委託することを計画しています。

結論

本調査における欧州全域の情報／セキュリティ担当シニアエグゼクティブの回答から、企業のデジタルトランスフォーメーションの必要性が適切に認識されているという心強い結果が明らかになりました。

また、デジタルトランスフォーメーションへの抵抗勢力と目されてきた業界（例：保険）が、市場情勢の変化と課題の出現に呼応して方向転換を開始していることも確認されています。これは全業界を通じて、セキュリティをデジタルトランスフォーメーションに適応させることがある時点で必要になり、その適応はできるだけ早い方が望ましいということを意味しているでしょう。

今回の調査に回答した情報担当エグゼクティブは、現在のセキュリティの考え方の枠組みにとどまって以前のように単にすべてをロックダウンして封じ込める道は選んでいません。むしろデジタルトランスフォーメーションがもたらすビジネスメリットに気づいており、組織の競争優位を維持したいならばそのような変革を受け入れる必要がある、という認識に至っていることを、本調査は示しています。

これはデジタル時代のセキュリティに懸念を抱いていない、という意味ではありません。懸念していることは確かです。しかも、消費者に由来する新しいアイデンティティや、さらにはモノやセンサーのアイデンティティまで安全に管理しようとするならば、アイデンティティ／アクセス管理（IAM）ソリューションが主役となって新たな課題を解決する必要があることも強く認識しています。

今日のセキュリティ侵害の大半は、従業員のありふれたミスによるものです。たとえば、電子メールの不正リンクをクリックした、悪意の添付ファイルをダウンロードした、あるいは単にセキュリティポリシーやトレーニングの教えに従わなかった、などです。

デジタル時代でも人間が不完全であることに変わりはありませんが、アイデンティティとモノの急激な増加に呼応して脅威ベクターが拡大するにつれ、そうしたミスがもたらす結果とリスクはますます増大していきます。デジタル時代には、インサイダーに起因する脅威を一層安全に管理する必要が生じるでしょう。

消費者、モノやセンサーなどの新しいアイデンティティからのアクセスがデジタルトランスフォーメーションの重要な一角を担うことを考えれば、安全で高度化されたIAMソリューションの必要性は、最初の段階から考慮に入れておかなければなりません。

CIOとCISOはこれを成し遂げることができるでしょうか？ そして、IDaaSを提供するIAMベンダーやMSSPはそれにどこまで対応できるでしょうか？

欧州全域ですでに大きく広がっている新しい動きが、情報管理責任者の尽力も、最高クラスのIAMシステムも無力化してしまう恐れがあります。それは、シャドーITの拡大です。

今や、IT部門の統制が及ばない事業部門でも、デジタル主導のサービスやソフトウェアが容易かつ安価に入手可能になっています。

本調査では、シャドーITが旧型IAMの実効性にどのように影響を及ぼすか、そしてシャドーITをどのような形で将来の投資における検討事項として考慮しなければならないかに関して、大きな懸念が生じていることがわかりました。

これはユーザーとサプライヤーの双方にとっての課題です。出発点としては、双方での対話のほか、関係組織による現実に即したシャドーIT監査も適切でしょう。

規制当局、データプライバシーを懸念する一般市民、そしてセキュリティ侵害が事業に及ぼすダメージを懸念する株主が産業界に対する監視を強化する中では、リスクとコンプライアンスについても、デジタル時代のIAMの意思決定の検討事項として考慮しなければなりません。

デジタルトランスフォーメーションを急ぐあまり、他の事業部門がセキュリティへの投資を見過ごしたり、軽視したりする懸念も存在します。今後は、多種のアイデンティティや機器を対象とした新しいIAMソリューションを選択する際に、そうした拙速が生じるのを防ぐことをITやセキュリティの責任者に要求する圧力もさらに高まっていくでしょう。

近い将来に計画されているIAMへの投資に関して、ITとセキュリティの責任者は、何に重点を置いて投資する必要があるのかを、明確に伝えなければなりません。つまり、どのような要件に対処するために新しいソリューションとIAMポリシーが必要とされる

のかを明確にする、ということであり、それが要するに、デジタル時代のためのIAMなのです。

アイデンティティ／アクセス管理（IAM）は、デジタル時代のサイバー攻撃に対する主な防御手段として、ますます中心的な役割を担うようになるでしょう。企業は、サイバーセキュリティに対しても、他の脆弱性に対する脅威の管理に対しても、よりインテリジェンスベース（情報の収集と分析を重視する）のアプローチに移行していますが、それでもIAMの中核的な重要性に変わりはありません。

しかし、もし欧州企業の事業責任者がデータとインフラにアクセスするヒトやモノのアイデンティティを統制することができなければ、その企業の将来のセキュリティと成長、ひいては企業そのものも破綻に追いやられることになるでしょう。

付属資料

調査方法

PACは、2016年3月に本調査を実施しました。一定の審査の後、欧州全域から選ばれた202人の上級情報セキュリティリーダーが調査に回答しました。回答者は、銀行、保険、製造、小売、サービス、通信、運輸の企業および公的機関に属しており、ベネルクス、北欧、スイス、フランス、ドイツおよび英国に拠点を置いています。

図21：回答企業の従業員数

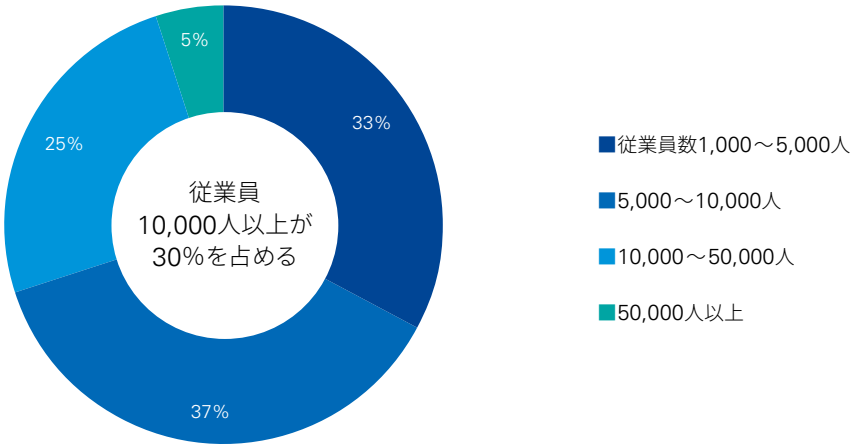
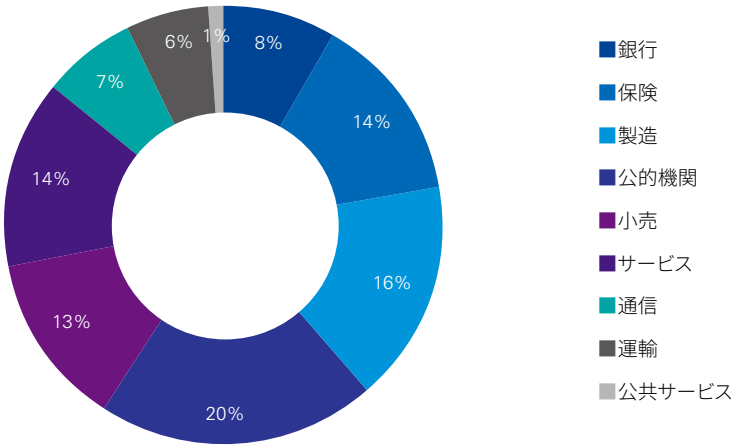


図22：回答企業の業種



注記：小数点以下四捨五入のため合計値は100%にならないことがある

図一覧

KPMGについて

今日、サイバー攻撃はビジネスの現実の脅威となっています。技術の進歩と業務慣行の変化が、サイバー犯罪者やハクティビストが暗躍する機会を拡大しています。組織は、彼らによって、今や「コントロールを失う」状況にまで達してしまっているのです。

パスワードの共有が広まっています。ソリューションがアプリケーションやプラットフォームごとに乱立し、数え切れないほど多くの認証手法とパスワード管理方法を生み出しています。権限付与は多層化し、職務分掌はもはや明確さを失っています。管理者によって付与される権限を見通す能力も欠如しています。パスワードの変更、アクセス統制へのコンプライアンスの実証、特権アカウントの保護、プロビジョニングなどを受け持つヘルプデスクのコストは高騰しています。

弱点のリストは際限なく増加する

多くの組織はこうした問題に対処するために、ユーザーの管理、アクセスの統制、特権アクセス管理、アイデンティティ連携（フェデレーションサービス）、ロールベースのアクセス制御、プロビジョニングの効率性などを向上させるためのプロジェクトを始動させています。こうした機能はアイデンティティ／アクセス管理（IAM）の構成要素です。

KPMGのグローバルサイバーセキュリティアドバイザリーは、長年の経験と広範な専門知識をIAMのあらゆる側面について提供します。

- 多数の業界でビジネスに影響を及ぼす現在および将来のIAM動向に関する深い**理解**
- 遵守すべき法令、ビジネス、プライバシーおよび規制リスクに関する**専門知識**
- **IAM戦略の評価、アドバイザリー、プロジェクト管理および導入支援**を幅広いIAMツールを用いて提供する傑出した能力
- セキュリティ評価／認証、セキュリティアーキテクチャ開発／導入、セキュリティ／テクノロジー統制、ITインフラストラクチャ／コントロールおよびオペレーション／プロジェクトリスクマネジメントを包括する**広範な能力**

KPMGのグローバルサイバーセキュリティアドバイザリーについて

KPMGの2,200人を超えるサイバーセキュリティ専門家のネットワークが、世界中の企業と連携して、組織全体を安全に保護するための支援を企業に提供しています。人、プライバシー、情報ガバナンスおよびビジネスレジリエンス（回復力）の問題の解決を図ることで、顧客企業がデジタルの世界において、企業グループ全体での経営アプローチを導入できるように支援することがKPMGの務めです。経営幹部に新たな展望を提供することによって、サイバーリスクを独創的かつ建設的な方法でコントロールできるように支援するとともに、ビジネスの成長、変革、そしてイノベーションを実現する顧客企業自身の能力も高めています。

詳細については、KPMG Cyber Securityウェブサイトをご覧ください。

www.kpmg.com/jp/cyber-security

連絡先：

John Hermans
KPMGオランダ
欧州・中東・アジア
サイバーセキュリティ責任者
hermans. john@kpmg.nl

Prasad Jayaraman
KPMG米国
アイデンティティ／アクセス管理
グローバル責任者
prasadjayaraman@kpmg.com

Manoj Kumar
KPMG英国
サイバーセキュリティ
主席アドバイザー
manoj .kumar@kpmg.co.uk

www.kpmg.com

免責、使用権、独立性およびデータ保護

本調査の作成と配布は、KPMG、CyberArkおよびSailPointをはじめとする各社の支援を得て実施されました。

詳細については、www.pac-online.comをご覧ください。

免責

本調査の内容は、最大限の注意を払って編集されています。しかし、その正確性については一切の責任を負いません。分析と評価は、2016年4月の時点における知見を反映しており、任意の時点で変更される可能性があります。これは特に将来に関する記載に該当します（ただし、それだけに限定されません）。本調査の中に記載された名称や記号は登録商標である場合があります。

使用権

独立性とデータ保護

本調査は、Pierre Audoin Consultants（PAC）が、KuppingerColeの協力を得て作成されました。スポンサーは、データの分析と調査の作成に対していかなる影響力も及ぼしていません。

本調査の参加者は、提供した情報が機密として扱われる確約を受けています。いかなる記述からも、個々の企業に関する結論を引き出すことはできません。また、いかなる個々の調査データもスポンサーや他の第三者に引き渡されていません。本調査のすべての参加者は無作為に選ばれました。たとえ本調査の回答者とスポンサーの間に商業的関係が存在する場合でも、その関係と本調査の作成との間にはいかなる関連性も存在しません。

お問合せ先

KPMGコンサルティング株式会社

〒100-0004
東京都千代田区大手町1丁目9番5号
大手町フィナンシャルシティ ノースタワー
TEL : 03-3548-5111

kpmg.com/jp

twitter.com/KPMG_JP
www.facebook.com/KPMG.JP

Publication Number: JAPAN:16-1562