オラクルとKPMGによる クラウドの脅威レポート 2018年

クラウド利用促進による サイバーセキュリティ戦略への影響

クラウド・サービスの幅広い採用から生まれるサイバーセキュリティの課題と解決策に関する独自調査ベースの概論

目次

序文

Oracle Corporation、CSO、Mary Ann Davidson

"歴史は繰り返す"という表現があり、情報技術（IT）にもそれが当てはまります。私の大学でのITの経験として、大学のコンピュータ学科では、学生向けに"サービスとして"プログラム（パンチ・カードのデッキ）を実行していました（個人の"サブスクリプション"は学期ごとに厳しく制限されていました）。コンピュータは後に"個人的"になり、多くの人がアクセスできるだけでなく、ほぼすべての企業の中核的な存在になりました。これにはITに焦点を絞っていない企業（農業など）も含まれます。

今日、ITの人材確保を含む、重要なIT資産を多く管理する企業の取り組みによって、クラウド・サービスは爆発的に増加しました。これには、Infrastructure-as-a-Service（IaaS）からPlatform-as-a-Service（PaaS）、Software-as-a-Service（SaaS）に至る、企業が利用するすべての重要なアプリケーションが含まれます。我々は、このサービス提供の価値を直感的に理解できます。例えば、自分で家を建てたり、車の整備を自分でしたり、歯科治療を自分で行ったりしません。その代わりに、自分で行うよりも少ないリソースで、より迅速に、よりよい価格で、より多くのことを行うことができる各分野の専門家を探します。ITは、サービス提供手段の一つにすぎません。

クラウド・サービスを利用することで、古いままで投資されていない設備機器（その一部は寿命が過ぎている可能性があります）をメンテナンスし使い続けて行き詰るのではなく、最新かつ最高の技術を取り入れることができます。さらに、ITはイノベーションに利用することができます。イノベーションは、多くの場合、柔軟でスケーラブル（必要な分だけリソースを借りることができます）、高度に熟練したデータ分析の活用、マシンの能力によって人間ができない推論を導くことを実現します。クラウド・サービスの採用は、実験的な試みから、クラウド内でミッション・クリティカルなデータを管理することに移行しました。多くのクラウド利用者は、クラウドにこのようなデータを置くと信じるようになったため、容易に保護でき、究極的にはより安全な組織となります。結局のところ、5,000人のお客様が個別にテストを行い、重大なセキュリティ脆弱性に対するパッチを適用することと、5,000人のお客様が使用するサービスにクラウド・プロバイダーがパッチを適用することの、どちらが簡単でしょうか。これらのトピックを掘り下げるために、オラクルとKPMGはEnterprise Strategy Groupと提携し、このレポートの基礎となる調査研究を実施しました。

『*オラクルとKPMGによるクラウドの脅威レポート 2018年*』の優れた考察は、プロフェッショナルな専門家によるものではなく、組織のセキュリティ上の課題に取り組んできたセキュリティ専門家と意思決定者、および重要なアプリケーションのクラウドへの移行を進めているセキュリティ専門家と意思決定者によるものです。回答者は、製造、保健医療、メディア、小売、政府（連邦、州、地方）を含むさまざまな業種から、地理的にさまざまな場所の人を対象としています。回答者の大半は、機密データをクラウドに格納していると回答し、多くの回答者はクラウドのセキュリティがオンプレミスのセキュリティと同等かそれ以上のものだと考えていました。回答者はまた、組織のサイバーセキュリティ・リーダーシップの役割が、組織の領域を保護するために、数多くの優れたソリューションとツールを組み合わせて管理していると回答しました。回答者のほぼ3分の1が、限定的であっても、すでに機械学習を使用しています（クラウドのもう1つの利点は、"よりよく迅速に実行するだけでなく、継続的かつシステム的に向上する"ことです）。

企業は、パッチの適用されていないアプリケーションの既知の脆弱性を標的にした攻撃を経験しています。これは、ハッカーのリバース・エンジニアリング技術が向上し、自動配信メカニズムを使用して悪用コードを共有する能力を高めたときにのみ増加する可能性があります。現実的には、週に1回リリースされるパッチの範囲を考えると、ほとんどの組織は必要なものすべてをパッチ適用することはできず、十分な速さで対応することはできません。より高度な自動化とDevOpsの新しいコンポーネント/改良されたコンポーネントを迅速に統合する機能を備えたクラウド・プロバイダーは、脆弱性の検出、パッチの作成、パッチの適用のギャップをより迅速に解消できます。

規制の圧力が強まると、クラウドを望む声が高まります。ほとんどの回答者は、1つ以上の規制のフレームワークが組織に適用されると指摘しました。すべてではないですが、多くの組織がセキュリティ要件を強化しています。その中には、クレジット・カード業界（PCI）のデータ・セキュリティ標準（DSS）、グラム・リーチ・ブライリー法、サーベンス・オクスリー（SOX）法、医療保険の相互運用性と説明責任に関する法律（HIPAA）などの長年にわたる規制があります。これらには、欧州連合（EU）の一般データ保護規則（GDPR）も含まれてきます。多くの組織は、これに影響を受けていると述べました。

ソーシャル・メディアの時代には、何が"トレンド"かを語るのが一般的です。私たちが注視しているのはトレンドではなく、戦略的な変化、つまり、セキュリティを可能にするクラウドです。

エグゼクティブサマリー

クラウド・コンピューティングは、確立された市場を混乱させ、既存ブランドの動きを速くするよう働きかけて、競争優位性を実現するための抜本的なパラダイム・シフトです。クラウド・サービスの幅広い採用とナレッジ・ワーカーのモビリティの導入により、新たなサイバーセキュリティの課題が生まれました。クラウドの俊敏性は、大規模な変化に対応するための戦略的原則を生み出しました。組織がインフラストラクチャ、アプリケーション、およびユーザーの規模を拡大すると、セキュリティ要件への対応が遅れ、同じ速度で今後も拡張することがさらに困難になっています。クラウド対応の職場がサイバーセキュリティの優先事項に及ぼす影響について、『*オラクルとKPMGによるクラウドの脅威レポート 2018年*』の主な調査結果を確認しながら説明します。

- **クラウドの利用は継続的に拡大しています。**クラウドファーストのイニシアチブとパブリック・クラウド環境のセキュリティ態勢への自信の高まりは、クラウド・サービスの幅広い採用を促し、組織の機密データのかなりの部分がクラウドに常駐するようになりました。
- **セキュリティ専門家は、事業運営に対する攻撃の影響を心配しています。**サイバーセキュリティ攻撃は財務上の損失をもたらしますが、もっとも言及されている影響は事業運営に対するものです（コアサービスを提供する能力など）。
- **テクノロジーだけでは不十分です。**組織は、人、プロセスおよびテクノロジーに焦点を当てた一連のベスト・プラクティスで、クラウド・アプリケーションとインフラストラクチャの使用を保護するために、再編成の取り組みに資金を提供しています。
- **クラウド・サービス・プロバイダーの評価が必要です。**クラウド・サービスを利用するにあたり、セキュリティが担保されているか評価する必要があります。
- **サイバーセキュリティの再構築が求められています。**クラウド・サービスの利用において、サイバーセキュリティに求められる要件が変わってきていますので、専任のクラウド・アーキテクト設置を検討する必要があります。
- **検出と対応は非常に重要ですが、クラウドでは必ずしも容易ではありません。**利用者は、クラウド内の脅威を検出し、その脅威に対応することが、サイバーセキュリティの最重要課題であると指摘しています。これにより、利用者が対応しなければならないクラウドの"可視性ギャップ"が作成されます。
- **クラウドとモバイル中心の従業員には、新しいIDとアクセスの管理戦略が必要になります。**ナレッジ・ワーカーのモビリティとクラウド配信アプリケーションの使用により、ロールと権限を戦略的に調整することで、大規模なID管理が課題となりました。
- **機械学習と自動化が役立ちます。**機械学習やセキュリティ自動化などの新興テクノロジーは、脅威の検出と防止の効果を向上させるとともに、クラウド対応の職場の安全を確保する運用効率を約束します。

主な調査結果

90 %
の企業が、クラウド・データの少なくとも半分が機密情報であると回答しました

41 %
の企業が、専用のクラウド・セキュリティ・アーキテクトを備えていると回答しました

66 %
の企業が、過去24か月間に大きな事業運営の中断を経験しました

38 %
が、クラウドのセキュリティ・インシデントを検出して対応する問題を報告しました。これが、この調査でもっとも言及されたサイバーセキュリティの課題になります

82 %
のサイバー・リーダーが、従業員がクラウドのセキュリティ・ポリシーに従わないことを懸念しています

36 %
が、モバイル機器とアプリケーションの利用拡大によりアイデンティティ／アクセス管理（IAM）の統制と監視が困難になると回答しました。

47 %
の組織が、クラウド・サービス・プロバイダーを自身で評価しています。

84 %
の企業が、セキュリティ自動化のレベルアップに取り組んでいます

“多くの企業はクラウド活用が進む中、安全にクラウドを利用するための課題への対策を行う必要性に直面しています"

クラウドに関するセキュリティ上の懸念がクラウド・サービスの使用を妨げていない事が本調査から明らかになりましたが、多くの課題があります。事業部門では、アジリティ（俊敏性）の向上のためにクラウド利用を要求するだけでなく、企業のITおよびサイバーセキュリティ・チームの承認なくクラウド・サービスを使用することがよくあります。この、サイバーセキュリティのポリシーとプロセスを迂回するシャドウITは、企業のサイバーセキュリティ戦略を脅かしています。このため、多くの企業は、クラウド利用が進む中、安全にクラウドを利用するための課題への対策を行う必要性に直面しています。そのため、人、プロセスおよびテクノロジーの再編成が必要です。本調査では、クラウドのセキュリティのギャップを埋めるための投資が必要であるという回答が得られています。89 %は、組織が次の会計年度でサイバーセキュリティの予算を増やすと見込んでおり、その中の44 %は7 %以上の増加を予想しています。ESGの調査によると、企業の43 %[1]が2018年にもっとも重要なサイバーセキュリティの投資を行うと見込む分野として、クラウド・インフラストラクチャのセキュリティとクラウド・アプリケーションのセキュリティの2つをあげています。

本レポートでは、ますますクラウド中心になる中でのデータセンターを保護するため重要な考慮事項に焦点を当てていますが、オンプレミスのクライアント・サーバー型のアプリケーションなどが利用されるITシステムが、引き続きビジネス・クリティカルな機能を担うという事実にも考慮することが重要です。現代のテクノロジーは、さまざまな世代のコンピューティング技術とプラクティスを利用したインフラストラクチャで構成されているため、セキュリティに対する全体的なアプローチが必要です。

[1] 出典：ESG Master Survey Results, *2018 IT Spending Intentions Survey*（2017年12月）

目次に戻る

KPMGの視点：
クラウド・セキュリティの実施要請

クラウドをセキュリティで保護しても、ベンダーに任せているだけでは不十分です。あなたは、ビジネス・リーダーとしての責任とリスクを知っていますか。

Laeeq Ahmed、KPMG LLP、Cyber Security Services U.S. Leader
Tony Buffomante、KPMG LLP、Oracle Security & Controls Leader

かつてないペースで企業のクラウド活用が進みつつありますが、その多くでは、関連するリスクを適切に管理できていません。有事の際の被害額を見積もっている企業もわずかです。

クラウドによって、リスクとコンプライアンスの新しい要件が発生し、業種を問わず、世界中の組織に影響が生じました。クラウドへ移行する組織では、クラウド・サービス・ポートフォリオは絶えず追加され、重要な情報資産を効果的に保護する最高のセキュリティが求められています。

多くの企業がクラウド・セキュリティの標準化とスキルの確立に苦労しています。さまざまなクラウド・プラットフォームとベンダーが独自のサイバーセキュリティの基準と要件を持っているため、戦略上や運用上で直面するリスクは、複合的なものです。サイバーセキュリティのノウハウが不足していると、クラウドへの移行を進める中で、ベンダーが提供するサイバーセキュリティ対策がビジネスを保護するのに充分なものであると誤解してしまい、重要な制御の実装を欠いてしまうおそれがあります。

KPMGとオラクルの共同調査では、サイバー脅威の多様性と攻撃の規則性が事業運営を妨げていることが示されており、この問題の深刻さを強調しています。

Call to Action 行動喚起

経営層や、財務、人事、リスクマネジメント、ITおよびセキュリティの各リーダーは、クラウドに固有のリスクに対処するためのサイバーセキュリティ・プログラムを組織に確実に提供する責任があります。

リーダーは、リスクが軽減され、コンプライアンスの要件が確実に満たされることを保証することに加え、ビジネスを保護する責任があります。重要な第一歩は、クラウド・セキュリティと制御の"共有責任"の原則を理解することです。ベンダーが提供するセキュリティ制御を知ることで、企業は独自のクラウド環境を保護するための対策を講じることができます。

組織を守るためには、組織のリーダーだけでなく、すべての従業員が、クラウド固有のリスクとそのリスクを防ぐために設計されたポリシーについて教育を受けることが重要です。これには、クラウドの使用に関する従業員への明確なコミュニケーションと啓発が必要です。KPMGとオラクルの調査によると、組織内の個人、部門および事業部門は、多くの場合、クラウド・サービスのポリシーに違反しており、この面では改善の余地がかなりあると思われます。

クラウド・セキュリティの責任について

クラウド・ベンダーはセキュリティに関する一部の責任を負いますが、サービスを利用する企業こそが、サイバーセキュリティを維持し、リスクとコンプライアンスを管理する責任を負っています。

クラウド・サービスの使用は、新たな脅威をもたらす可能性があり、企業はファイアウォール、アクセス制御、イベント・ログ、構成などの主要な制御を含む従来のセキュリティ保護をどのように実装したかを再評価し、セキュリティを維持する必要があります。

組織の各リーダーはこの新しい現実に対し、迅速にチームで取り組み、クラウド・セキュリティの共有責任を理解し、フレームワークを活用して、サイバー脅威から組織を守らなければなりません。

多くの企業では、そのための予算や知識、フレームワークが欠けています。企業はオンプレミスのセキュリティ・レイヤーを構築している場合がありますが、新しいクラウドベースを支えるために強化されたセキュリティ・プログラムに投資する必要があります。

クラウド・セキュリティの課題は、単一のテクノロジー・ツールやパッチを寄せ集めても解決できません。クラウドに焦点を当てたセキュリティとリスク機能の全体的な進歩によって解決されます。クラウドへの適切な移行とその効果的な運用には、情報を保護し、リスクを管理し、コンプライアンスを満たすための戦略的で柔軟なアプローチが必要です。ハイブリッド・クラウド環境、脅威の状況およびナレッジ・ワーカーのモビリティのすべてにより、クラウド・プラットフォーム、ユースケース、採用のフェーズに関係なく、数多くのサイバーセキュリティの課題が生まれます。

クラウド対応の職場を保護するには、人、プロセスおよびビジネス・クリティカルな資産に焦点を当てます。成功させるためには、企業は、（オンプレミス・システムに対して実施したのと同じように）クラウドベースの環境を保護するための具体的な機能を開発する必要があります。また、リスクとコンプライアンスに一貫して対応しなければなりません。

KPMGによるサポート

KPMGは、可用性、整合性、機密性に関する基本的なセキュリティの考慮事項、および実装のロードマップを備え、オラクルのテクノロジー・ソリューションに基づいた、幅広いクラウド・セキュリティ・アーキテクチャのフレームワークを開発しました。

KPMGクラウド・セキュリティ・フレームワークは、企業がクラウド・セキュリティのためのターゲット・オペレーティング・モデル（TOM）の定義に役立ちます。KPMGのフレームワークは、組織が（1）ビジネスを保護し、（2）クラウド・サービスに関連するプロセスを進め、（3）競合他社よりも優れた立場に立つように、人、プロセス、テクノロジーおよびポリシーをまとめることを支援します。

KPMGとオラクルの調査結果は、企業のクラウド環境におけるセキュリティ・リスク状況の確認に役立ちます。

オラクルの視点：クラウド・セキュリティ・アーキテクト

Oracle Corporation、 Senior Principal Director - Security、 Greg Jensen

企業は多くの場合、自社のセキュリティ対策を改善するためにもっとも大きな効果が見込める領域を探します。クラウド中心の戦略で取り組みの優先順位を決めるようになるにつれて、セキュリティ対策とコンプライアンス対応を達成する上でもっとも重要かつ戦略的な役職の1つとしてクラウド・セキュリティ・アーキテクト（CSA）が注目をあびるようになっています。

では、CSAがどのような役割をになうのか、またセキュリティ・アーキテクトとはどのように異なるのでしょうか。多くの場合セキュリティ・アーキテクトは、オンプレミス、モバイル、さらにはクラウドを含めた広範なセキュリティ領域を対応していますため、この数年でこの役職はいわば"何でも屋"のようになってしまいました。CSAは、事業部門（LoB）やインフラストラクチャ、またはアプリケーション・チームが、新しいクラウド・サービスを展開する際に直面することが見込まれる、セキュリティやコンプライアンス関連のあらゆる課題を理解している、"クラウド・セキュリティ・マスター"となるように設けられました。そのため『*オラクルとKPMGによるクラウドの脅威レポート 2018年*』によると、CSAの役職がセキュリティ・アーキテクトより人気が出ていることが明らかになっています。

一般的に、*アーキテクト*は計画、設計・体制の構築をします。IT視点でクラウド・セキュリティにあてはめて考えても非常に似ています。CSAは以下の責任を負います。

- 業界のベスト・プラクティスのためにSaaS、PaaS、IaaSのすべてのプロジェクトのセキュリティ態勢を見直す
- プロジェクトの期間内にセキュリティ要件を完全に満たすことができないリスクを特定する
- セキュリティ対策の最適化と強化する機会を探す
- クラウド全体でコンプライアンス要件を満たせるようにポリシーとメカニズムを万全に準備する

CSAには、企業のセキュリティ・ガイドラインとLoB側の要件のバランスを取るよう強く迫られており、これらの目標を達成するのには時間の制約、リソースや予算の問題がしばしばぶつかります。企業は、多くのアプリケーションとワークロードをクラウドに展開することが急務ですが、複数のクラウド・サービス・プロバイダーがそれぞれ独自のSLAを持つことがよくあります。また、すべてのクラウド・サービス・プロバイダーは、異なった脆弱性対策とインシデント対応を行っています。CSAは、各ベンダーの課題を特定してリスクを把握する上で重要な役割を果たし、サービス・プロバイダーや社内のメンバーとともにそれらに対処する計画を立てることができます。

ORACLE

クラウド・セキュリティ・アーキテクト・ツールキット

CSAは、企業が認可しているクラウド組織が利用していることに対して、一定の可視性と評価基準を持つこと、また認可されていないアプリケーションを使用するユーザーの行動を可視性することを強く求められます。

昨今、暗号通貨のマルウェアに感染している企業が増えています。アプリケーション・サーバーやクラウド・アプリケーションを、暗号通貨マイニング攻撃のためのホストされたプラットフォームに変えています。企業が、セキュリティ・オペレーション・センターに情報を提供しているネットワーク・パフォーマンス監視（NPM）ツールまたはアプリケーション・パフォーマンス監視（APM）ツールへのトラフィックの影響を確認していない限り、ほとんど把握することが出来ません。『*オラクルとKPMGによるクラウドの脅威レポート 2018年*』の回答者の48 %は、現在はAPM/NPMイベント・フィードを使用して脅威を特定していると述べています。

また、CSAは、Cloud Access Security Broker（CASB）などのツールを使用して、使用中のすべてのクラウド・アプリケーションを識別し、ユーザーにリスク・スコアをつけ、疑わしいアクティビティが特定されたときに対処することを推奨します。

オラクルがお客様のCSAまたはITセキュリティ戦略を実現する方法の詳細については、
www.oracle.com/jp/securityをご覧ください。

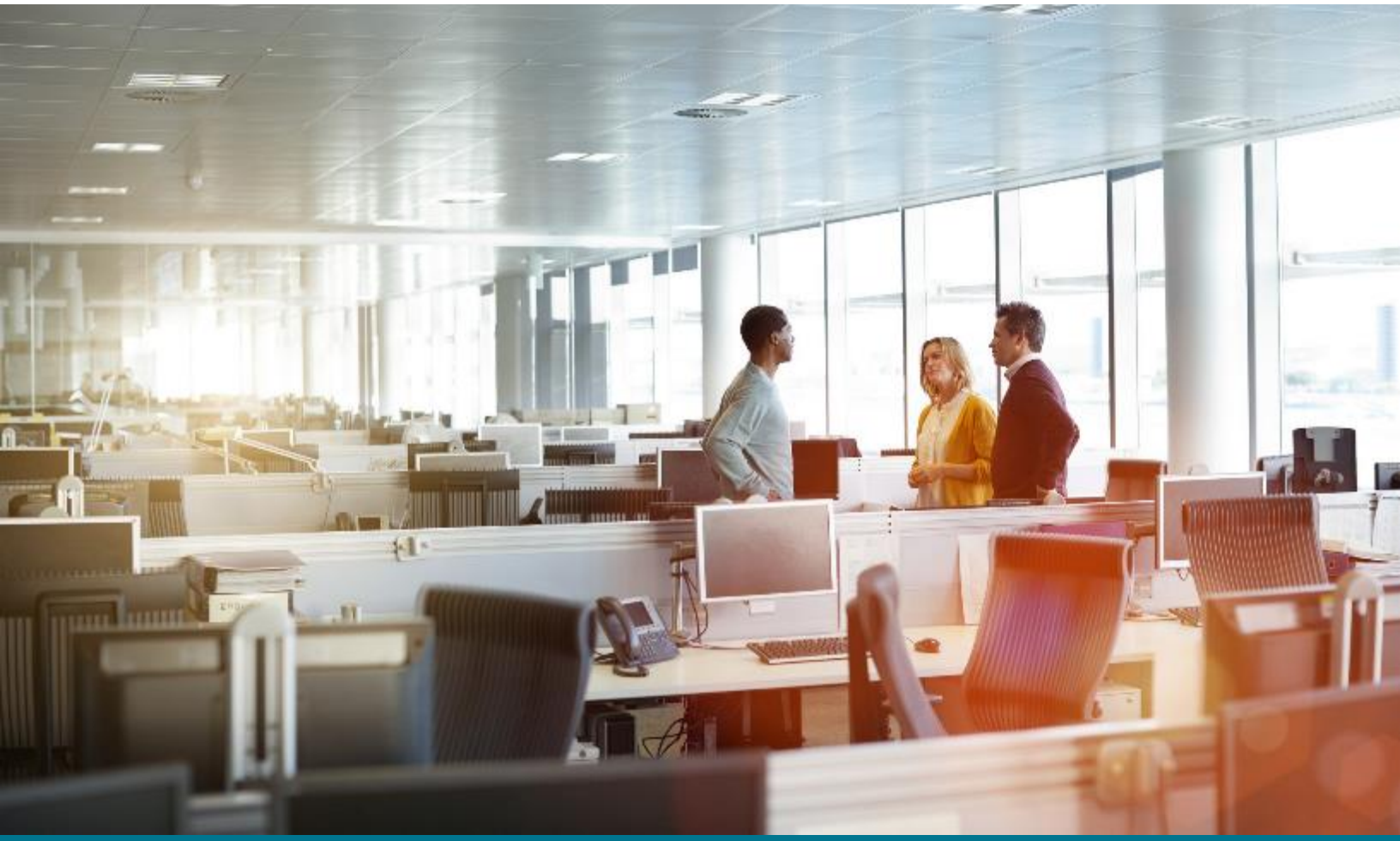
目次に戻る

重要な課題の1つは、ハイブリッドとマルチ・クラウド環境間でセキュリティ対策とコンプライアンス対応のバランスを取ることです。一部の企業では、クラウド・サービス（DaaS、SaaS、PaaS、IaaS）全体で緊密に統合したフレームワークを使用する単一ベンダーのモデルを採用しています。これは、リスクと露出点を減らすために多くの議論が行われたアプローチです。単一のベンダーのアプローチは、企業を保護し、必要に応じて拡張できるようにするという課題に役立つことが多いです。クラウド・サービス・プロバイダーでCSAが確認する主な基準は、次のとおりです。

- **包括的** - 完全なクラウド・スタック（DaaS、SaaS、PaaS、およびIaaS）でユーザー、アプリケーション、データ、およびインフラストラクチャを保護します。
- **自動化** - AIや機械学習により最新のセキュリティ脅威を検出、防止、予測、対応します。
- **データ中心** - 暗号化、マスキング、ユーザー・アクセス制御を使用して、機密性の高いデータへのアクセスを制御します。
- **統一** - サイバー脅威を相関分析するために、セキュリティと運用データの両方のデータで収集します。
- **統合** - 開発、設計、展開、および保守を行い、セキュアに連携します。

CSAの役割は、クラウド・アーキテクチャを支え、企業を保護するために選んだクラウド・ベンダーと同じくらい戦略的です。オラクルとKPMGは、今日のCSAに直面している非常に大きな課題を解決するソリューションでお客様をサポートしてきた長い歴史を持っています。

オラクルのセキュリティ・ソリューションの詳細については、www.oracle.com/jp/securityをご覧ください。



1

幅広いクラウドの採用により注目されるサイバーセキュリティ対策

クラウド・ソリューションに対する企業のニーズが高まっています。セキュリティがクラウドの採用の障害となっているという従来の考え方は、当てはまらなくなってきています。パブリック・クラウド・サービスは現在、セキュリティの問題にかかわらず、ほとんどの企業で利用されています。CISOは、クラウドの採用を無視したままでいることは、セキュリティの障害となることを理解しなければなりません。この変化は、従来のサイバーセキュリティへのアプローチを変えました。

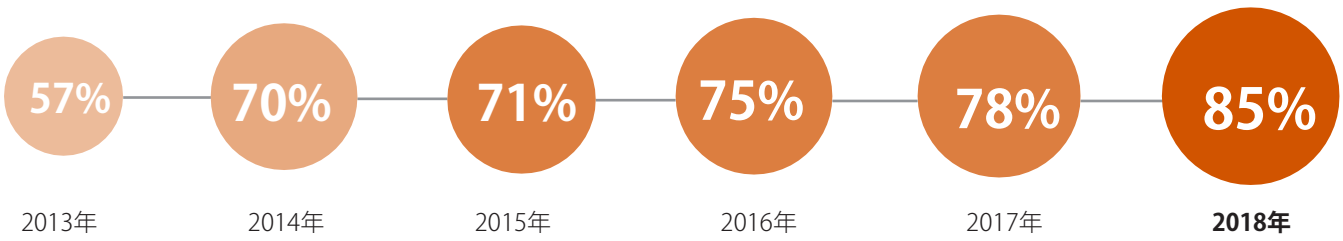
クラウドファーストのイニシアチブが採用を推進

米国連邦政府が実施している"クラウドファースト"は、現在、クラウド・サービスを使用してITプロジェクトを提供する多くの民間および公共組織にとっての戦略的原則となっています。今回の調査では、回答者の87 %が、その組織がクラウドファーストの方向性を持っていると報告されており、このことからクラウドファーストの広がりがわかります。

この調査結果と同様に、ESGの調査においても、85 %の企業が現在何らかのパブリック・クラウド・サービスを利用しています。[2] クラウド採用の速度は加速しています。2013年の調査では、組織の21 %がInfrastructure-as-a-Service（IaaS）を使用していると回答しました。当該調査研究によると、この年に、IaaSを利用している組織の割合は51 %に上昇し、143 %の増加となりました。さらに、IaaSプラットフォーム・サービスを利用する大多数の企業（81 %）は、複数のクラウド・サービス・プロバイダーのサービスを使用していると述べました。[3] SaaSの採用はIaaSの採用率を上回り続けています。現在74 %の組織がSaaSアプリケーションを使用していると述べたのに対して、現在IaaSを使用している組織は51 %です。

図1：パブリック・クラウドの採用、2013-2018

パブリック・クラウド・サービスの全体的な使用率、5年間の傾向（回答者の割合）



総務省の調査では日本企業の56.9%†がクラウドを利用しており、海外と比べると利用割合は若干低い傾向にあります。しかし、日本企業の利用割合は前年より10%ポイント上昇しており、今後の急拡大が予想されます。日本企業においてもクラウド利用を前提としたサイバーセキュリティ対策を講じることが求められます。（† 総務省「平成２９年通信利用動向調査」）

[2] 出典：ESG Master Survey Results, 2018 IT Spending Intentions Survey（2017年12月）
[3] ibid.

目次に戻る

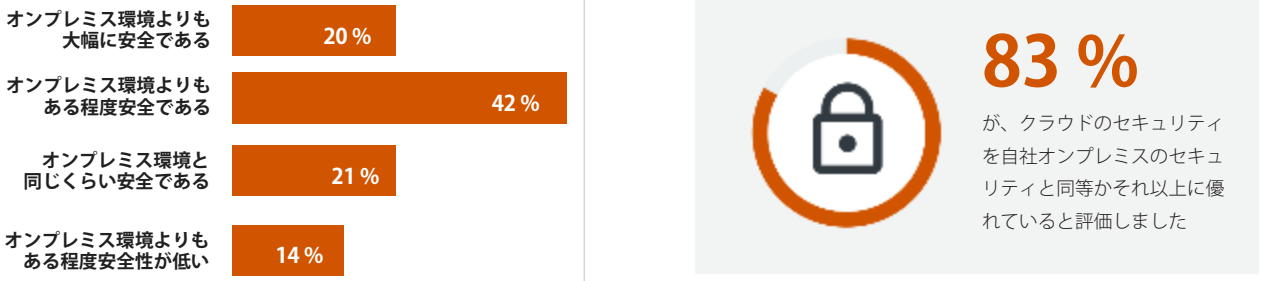
クラウド・サービスの利用が広がった結果、さまざまなテクノロジーを活用した複数のデータセンターを利用するという分散された環境が発生しました。クラウド環境は複雑であるため、調査回答者の26 %が、上位の課題として、異なるインフラストラクチャ間で統一されたポリシーが欠如していると述べたことは、不思議ではありません。クラウド・サービスが統合されていないため、IT部門とサイバーセキュリティ・チームはクラウド・サービスごとに独立したポリシーを定義して適用することになります。

クラウド・サービス利用者は使用しているクラウド・サービス・プロバイダーのセキュリティを信頼しているが、慎重な査定が必要

パブリック・クラウド環境のセキュリティの重要性が高まっていることに関して、調査参加者が自社のオンプレミス環境とクラウド・サービス・プロバイダー（CSP）のセキュリティを評価しています。調査回答者の83 %がCSPのセキュリティが自社のものと同等かそれ以上に優れていると考えています。

図2：利用者のセキュリティに関するCSPの評価

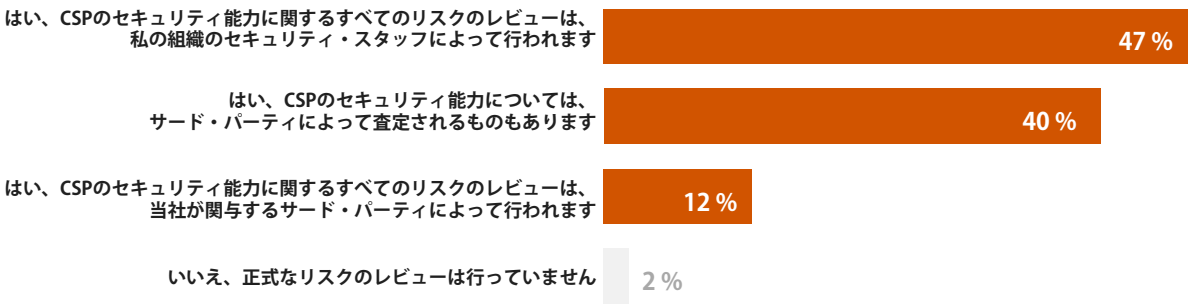
組織は、ビジネス・アプリケーションとデータ資産をホストして提供するパブリック・クラウド環境のセキュリティをどのように認識しているでしょうか。（回答者の割合、N=450）



調査対象の組織の98 %が、パブリック・クラウド・サービス・プロバイダーとビジネスを行う前に、プロバイダーに関するサイバーセキュリティ評価を実施していると述べました（図3を参照）。これらの回答者の47 %だけがCSPのセキュリティを自ら評価したと回答し、52 %の組織が第三者に評価の一部または全部を依頼していると述べています。CSPのセキュリティ評価に関しては、CSPのサイバーセキュリティをベンチマークする業界標準が存在しません。そのため、クラウド・サービス利用者がCSPのサイバーセキュリティ・プログラムを評価するための独自のサイバーセキュリティ要件を確立する必要があります

図3：CSPを積極的に査定する利用者

あなたの組織は、CSPのサービスを利用する前にCSPの正式なサイバーセキュリティのリスクレビューを実施していますか。（回答者の割合、N=447）



日本企業では、全社的にクラウドを利用している割合が29%†と低く、一部部門での限定的な活用に留まっている企業が多く見られます。全社的にクラウドを利用する場合には、セキュリティ・リスクが拡大するため、クラウド・サービス・プロバイダーを適正に評価するためのプロセスを整備する必要があります。（† 総務省 「平成２９年通信利用動向調査」）

クラウド・サービス・プロバイダーのサイバーセキュリティ能力をクラウド利用者が評価する場合、第三者が保有する経験の幅広さと奥深さを活用することは、明確によい方法です。たとえば、参加組織の51 %が回答しているとおり、第三者を活用していない利用者がCSPを評価するために実施したことは、CSPのサイバーセキュリティ・ポリシーの簡単なレビューでした。また、侵入テストの結果のレビュー、プライバシー・ポリシーのレビュー、業界の規制とデータセンターの認定の両方の準拠レベルの把握なども評価しています。

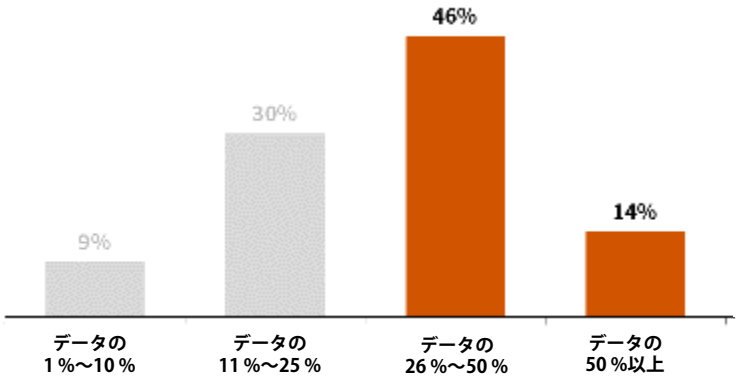
しかし、これらはCSPを評価するチェックリストですが、信頼できる第三社と協力してCSPのセキュリティ態勢の包括的な評価を実施するなど、チェックリストを詳細化する必要があります。評価を行うことは、カスタマ・リレーションシップ・マネジメント（CRM）、ヒューマン・キャピタル・マネジメント（HCM）、エンタープライズ・リソース・プランニング（ERP）、サプライ・チェーン管理（SCM）ソリューションなど、組織のもっとも機密性の高い、ビジネス・クリティカルなクラウド・アプリケーションにとって、特に重要となります。これらのアプリケーションは、日々の事業運営の中心であり、企業のもっとも重要なデータ資産を含むことが多く、その整合性を損なうことはビジネスにとって重大なリスクになります。

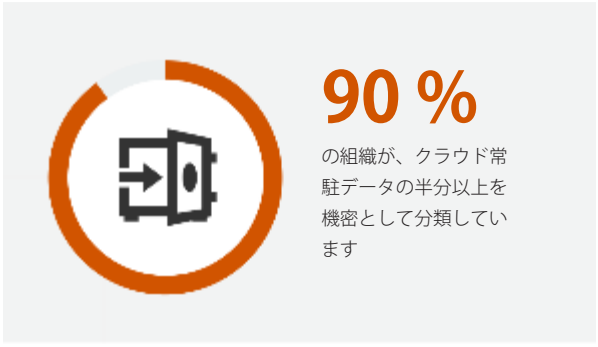
機密データがクラウドに移行

現在、多くの組織ではクラウドのセキュリティに問題はないと感じており、データ資産のかなりの部分がクラウドに格納されています。組織の60 %が、現在データの4分の1以上がクラウドに常駐していると回答しました。

図4：クラウド常駐データの範囲

あなたの知識の範囲内で、オンプレミスに対比して、パブリック・クラウドにあなたの組織のデータのおよそ何パーセントが存在していますか。（回答者の割合、N=450）





しかし、特筆すべきは、クラウドに常駐されている機密データの量です。組織にとって機密であると思われる情報は企業ごとに異なるため、CRMデータ、個人情報（PII）、支払いカードデータ、法的文書、デザイン、ソース・コード、その他の種類の知的財産などを含む幅広い種類のデータ・タイプが含まれる可能性があります。私たちの調査参加者の90 %は、クラウド常駐データの半分以上は機密性の高い情報であると回答しました。組織は、最も重要な資産でさえもクラウドを活用するようになっています。

日本企業では、重要情報を暗号化してクラウドに保存している企業の割合は30.6%に留まっています†。クラウド上で安全に機密データを取り扱うには、機密データの取り扱いポリシーを定め、ポリシーに準じた取り扱いがなされるよう対策を講じる必要があります。（† 「KPMG サイバーセキュリティサーベイ2017」）

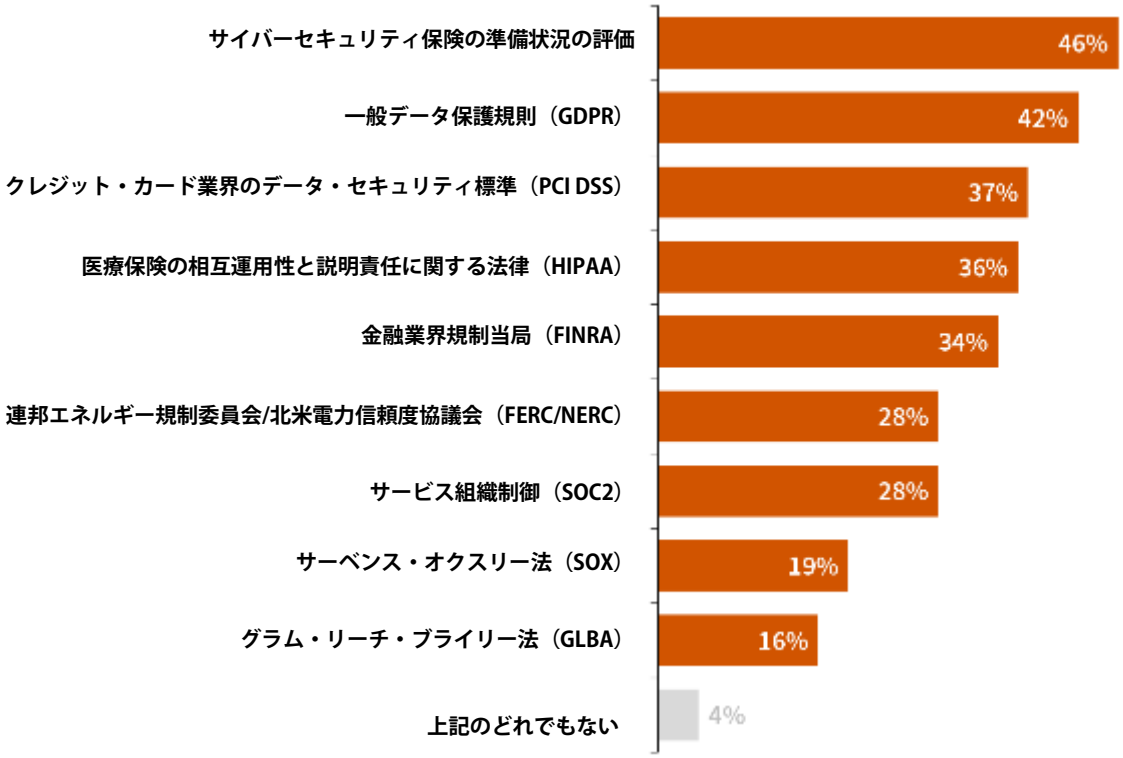
“GDPRは、EU市民の個人データを扱うための新しい規制とプロセスです。"

スポットライト：GDPRがクラウド戦略に与える影響

2018年5月25日 発効の欧州連合（EU）の一般データ保護規則（GDPR）は、28の加盟国にわたるEU市民の個人データの保護を管理し、企業がEU市民の個人情報を保護するための新しい義務を遵守することを求めています。違反の範囲、要件、違約金などの点から、加盟国のいずれかでビジネスを行っている大部分の企業にとって、GDPRは最重要視すべき問題となっています。調査の回答組織の42 %がGDPRを遵守しなければならないと述べています（図5を参照）。

図5：調査回答者ベースの遵守義務

組織が準拠する必要があるのは、次の業界規制のうちのどれですか。（回答者の割合、N=450、複数回答可）

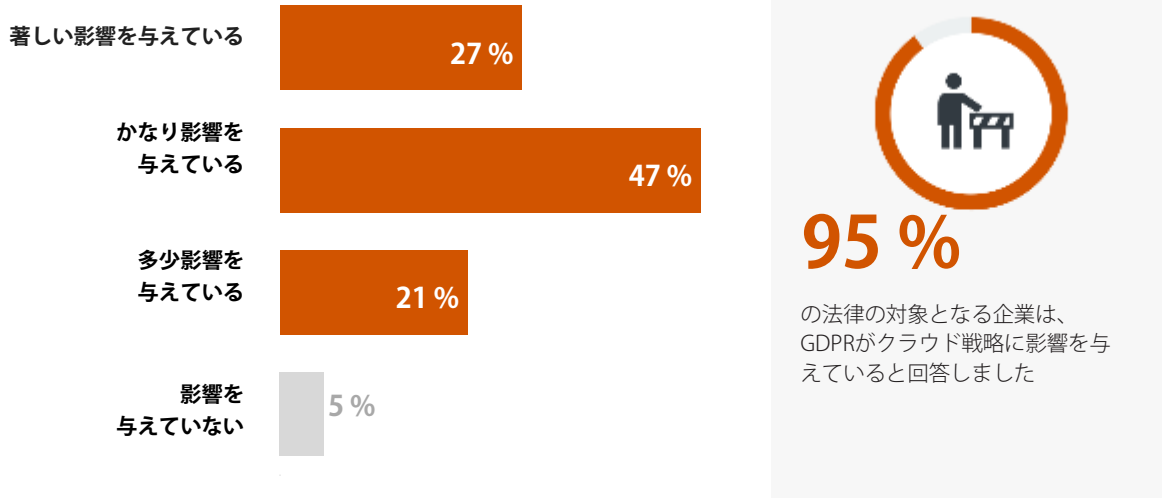


サイバー攻撃の高度化に合わせて、国内の各種法令・ガイドラインが頻繁に公開・更新されています。日本企業は業界や取り扱うデータに合わせて、法令・ガイドラインの更新を遅滞なく把握し、対応することが望まれます。また、GDPRのように、域外に適用される法令についても留意が必要です。

GDPRは、EU市民の個人データを扱うための新しい規制とプロセスです。複雑なデータの棚卸、必須の違反通知、データポータビリティの権利などのプロセスの実装を規定する、広範囲で複雑な法律です。調査の回答者は、GDPRの影響を感じています。回答組織の42 %は自身の組織がGDPRを遵守する必要があると述べ、法律の対象となる企業の95 %は、GDPRがクラウド戦略に影響を与えていると回答しました（図6を参照）。

図6：GDPRがクラウド・セキュリティ戦略に影響を与えている

あなたの組織のGDPRへの準拠を維持するための要件は、あなたのクラウド戦略とCSP評価プロセスにどの程度影響を及ぼしますか。（回答者の割合、N=190）



GDPRがクラウド・サービスの採用にどのように影響するかについての主な考慮事項の1つとして、クラウド・サービス・プロバイダー（CSP）のデータセンター間でのデータ移転があります。組織は、CSPが以下に限らず、データ・セキュリティのベスト・プラクティスを採用しているかどうかを理解する必要があります。

- **職務分掌：**クラウド・サービスの加入者が暗号化鍵の管理する責務を負います。多くのCSPは、現在、Bring-Your-Own-Key（BYOK：利用者管理する鍵）およびシングルテナントのハードウェア・セキュリティ・モジュール（HSM）の実装オプションをサポートしており、加入者は職務分掌を確実にすることができます。

- **データの検出と分類：**ポリシーの適用対象として、組織が義務を履行することができます。これには忘れられる権利を含みます（EU市民による行使があった場合、その個人データを消去する必要があります）。組織は、忘れられる権利を満たすためには、すべての個人情報を識別、タグ付け、追跡する必要があります。

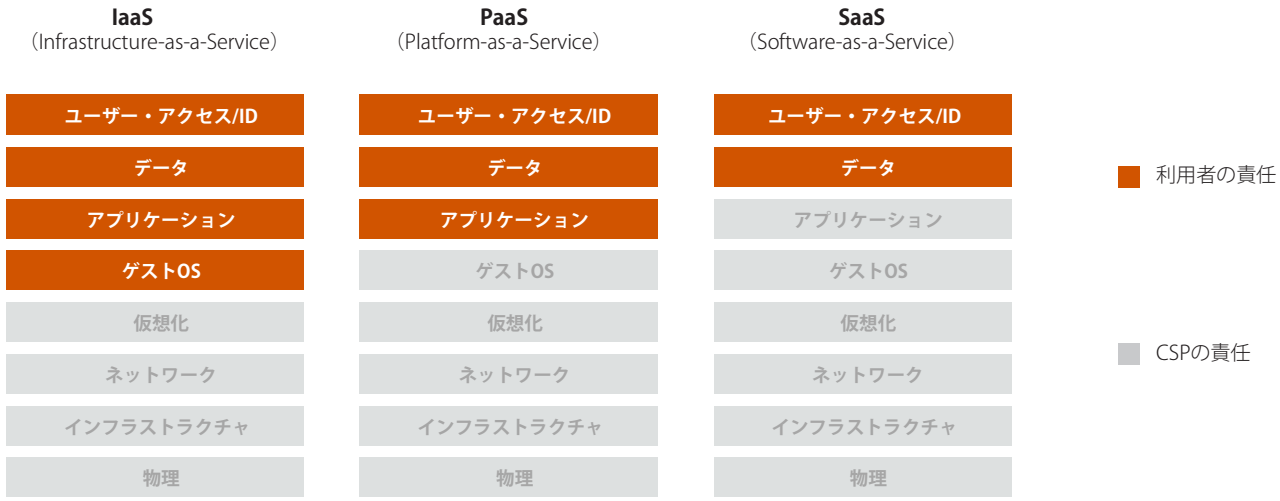
さらに、GDPRだけでなく、他の法令に準拠するために上記を含めた手順を実施するために第三者のサービスが必要となる場合があります。これには、サイバーセキュリティ保険引受監査、PCI DSS、HIPAAなどの準備が含まれます。

誤解されているクラウド・セキュリティの共有責任

共有責任のセキュリティ・モデルでは、クラウド・プロバイダーとクラウド利用者のそれぞれが、クラウド上のインフラストラクチャとクラウド・アプリケーションを保護する役割を担います。各当事者がどの部分を保護する責任を持つかについての境界線は、SaaS、IaaS、PaaSのサービスによって異なります。たとえば、IaaSは一般に、CSPが仮想化レイヤーまでの物理インフラストラクチャの保護に責任を持ち、利用者がサーバー・ワークロードを保護する責任を持ちます。ただし、使用モデル（IaaS、PaaS、SaaS）にかかわらず、利用者は一般的にデータ・セキュリティと、ユーザーのアクセスおよびID管理に対する責任を持ちます（図7を参照）。

"もっとも一般的なIaaSの共有責任のセキュリティ・モデルを正しく特定できたのは回答者の半分以下（43 %）にとどまりました"

図7：クラウド・セキュリティの共有責任モデル



この3つのタイプの共有責任のセキュリティ・モデルは一般に受け入れられていますが、責任範囲はプロバイダーによって異なるため注意が必要です。たとえば、CSPの中には、差異化の魅力的なポイントとして、データベース・サーバーなどの重要なシステムを悪意ある攻撃者から保護するために自動パッチ管理機能を提供するものがあります。利用者は通常、第三者のクラウド・セキュリティ・ツールと連携してホストベースのファイアウォールなどのCSP提供のネイティブ制御の組み合わせを活用します。

共有責任は比較的簡単なようですが、現実には多くの問題を抱えています。今回の調査では、もっとも一般的なIaaSの共有責任のセキュリティ・モデルを正しく理解できたのは回答者の半分以下（43 %）にとどまりした。共有責任でどの程度安全が保障されるかについての課題は、コンプライアンスにも及んでいます。たとえば、SOC 2などの規制へのCSPの準拠は特定のセキュリティ・プラクティスの指標ですが、クレジット・カード取引を処理する利用者は、CSPのPCI DSSへの準拠が必要となります。同様に、HIPAAビジネス・アソシエート契約（HIPAA BAA）を締結している医療組織は、HIPAA準拠のクラウド・サービスで患者の健康情報（PHI）を保護する責任があることを理解する必要があります。どのような場合でも、利用者はCSPと協力して、プロバイダーの特定の共有責任のセキュリティ・モデルを理解する必要があります。

共有責任に関して、物理的なネットワーク・セキュリティもあいまいになっています。組織は、物理およびVMベースのファイアウォール、侵入検知と防止システム、ゲートウェイなどのネットワーク・セキュリティ制御の使用について、目的のワークロードとクラウド・アプリケーションを使用して強化する必要があります。たとえば、オンプレミス・ユーザーおよびアプリケーションからのクラウド・サービスへのアクセスを制御する物理およびVMベースのファイアウォールについては、クラウド上にてホストされたファイアウォールでアクセス制御を強化する必要があります。目的に沿ったクラウド・セキュリティ制御を実現する例として、クラウド上のデータ資産を保護するためのデータ損失防止（DLP）ポリシーを含む、クラウド・アプリケーションの使用を保護するために不可欠な機能を提供するクラウド・アクセス・セキュリティ・ブローカー（CASB）があります。

2

今日の脅威の状況は多様で継続的

サイバー犯罪者はもっとも重要なサイバーの敵対者

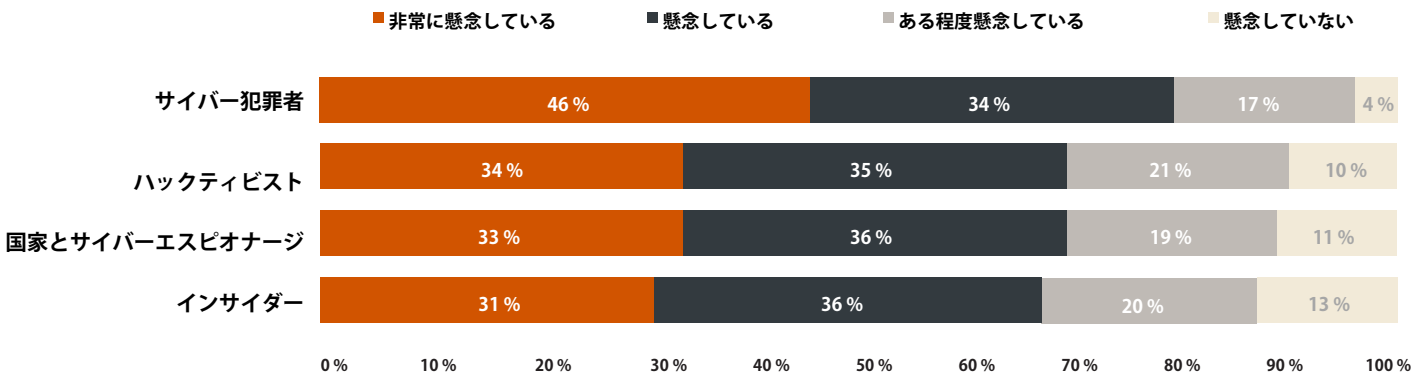
今日のサイバーセキュリティの脅威はますます多様化しており、技術的にも悪質なものになっており、多くの場合組織のもっとも価値のある資産を標的としています。これらは、サイバー犯罪者、ハックティビスト、国家、さまざまな動機のある内部従業員など、さまざまな悪意ある攻撃者によって設計され、配信されています。

しかし、過去数年にわたっておこなわれた脅威を1つ挙げるとするならば、それはランサムウェアです。ESGの調査研究の回答者の約2/3（62 %）は、過去12か月間以上ランサムウェア攻撃を受けたと答えています。[4] 100以上の国々で数十万台のコンピュータに感染しているパッチがあてられていないオペレーティング・システムを悪用したNotPetyaなどのランサムウェア攻撃や、世界中で30万以上の組織に侵入したWannaCryが注目を浴び、サイバー犯罪者によって実行される攻撃やその変異体によって大きな被害がもたらされました。

過去数年にわたってランサムウェアの大きな流行があったことを考えると、すべての種類の攻撃者が企業にとって心配の種となっています。調査回答者の80 %が、サイバー犯罪者が自分のデータやネットワークに与える脅威を懸念している、または非常に懸念していると回答したことは、驚くことではありません（図8を参照）。

図8：さまざまな種類の"悪意のある攻撃"に対する懸念

あなたの組織をサイバーセキュリティの脅威から守ることに関して、次の種類の"悪意のある攻撃"のそれぞれが与える脅威に対する懸念のレベルはどのくらいですか。（回答者の割合、N=450）



[4] 出典：ESG Master Survey Results, *2018 IT Spending Intentions Survey*（2017年12月）

目次に戻る

ランサムウェアはシステムや人間の脆弱性を悪用しやすいため、これらのすべての攻撃は非常に一般的な攻撃となっています。そして、今や攻撃方法によらず、サイバー犯罪者の動機は、金銭的な要求であることは明らかになっています。暗号通貨のマイニングを実行するために処理能力を奪うようシステムの脆弱性を悪用する暗号通貨ハイジャックは、金銭的利益を実現するためのますます普及した手段になっています。

スポットライト：内部従業員による脅威

調査回答者はサイバー犯罪者をもっとも懸念していますが、今回の調査で、サイバーセキュリティの担当者が内部従業員に関連するリスクについても懸念していることが明らかになりました。内部従業員による脅威には、証明書を盗まれた従業員が外部の攻撃者に対して意図せず代理人になっている状況などがありますが、真に悪意のある従業員を見つけることは、非常に困難です。これらの個人は、その目的に応じて、企業のIT環境の知識と与えられた権限を活用して内密にデータを盗み、事業運営を混乱させる可能性があります。

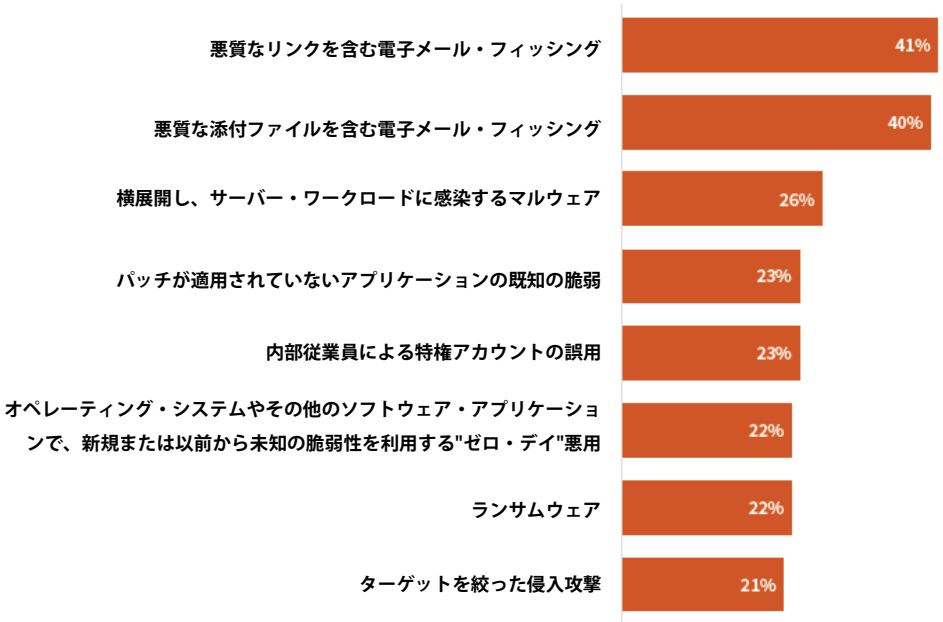
内部従業員の脅威を緩和するための重要なベスト・プラクティスには、コンテキストに基づいた2番目の認証要素を利用したリスクベース認証の使用と、悪意のある意図を示す可能性のあるアクティビティについてサイバーセキュリティの専門家に警告するための、異常なエンドユーザー・アクティビティの監視が含まれます。

フィッシングはもっとも多い攻撃

一方、ランサムウェアなどの脅威をもたらすものの主な攻撃手段は、フィッシングや悪意のある攻撃といった古い手法です。回答者の55 %は、昨年2種類のフィッシング・メールのうち1つ（または両方）に被害を受けたと回答しました。2種類とは悪質なリンクを持つメッセージまたはマルウェアを含む添付ファイルがあるメッセージです（図9を参照）。

図9：上位10件の一般的なサイバー攻撃の手段

次の中で、過去2年間にあなたの組織で経験したサイバーセキュリティ攻撃を選択してください。（回答者の割合、N=450、複数回答可、上位10件の回答のみを下に表示）



55 %

が、2種類のフィッシング手法のうちの少なくとも1つを経験しています

IPAが公開した「情報セキュリティ10大脅威 2018」では、ビジネスメール詐欺が昨年のランク外から2018年では３位に急上昇しました。海外では数年前からビジネスメール詐欺の注意喚起がされており、日本では遅れて急上昇しています。海外で広がっているセキュリティ脅威は日本でも遅れて広がるため、日本企業は海外のセキュリティ脅威にも注意する必要があります。

電子メール・フィッシングの対象は、幅広い攻撃の一部である大勢のユーザーを対象とした電子メールから、個人をターゲットにしたスピア・フィッシング、企業の経営陣を攻撃することに焦点を当てたホエール・フィッシング（すなわち、"ホエーリング"）まで、高範囲に及びます。どのような場合でも、成功したフィッシング攻撃は人間の脆弱性を利用しています。つまり、うまく設計された電子メールはユーザーをだますことで不適切な行動をとるようにユーザーを誘導します。このように、ユーザーが虚偽の電子メールを特定できるよう継続的にセキュリティ意識を啓発し、クロスチャネル攻撃（たとえば、悪意のある電子メールへのリンクを含む電子メールなど）を検出して防止するセキュリティ制御の強化することが不可欠です。

組織は、攻撃者が現在次のような他のフィッシング手段を使用していることにも気付かなければなりません。

- **ビッシング (Vishing)** - ユーザーが個人情報を共有するよう説得される折り返し電話を求めるボイスメール。
- **スミッシング (Smishing)** - 資格証明を盗むように設計されたWebページにつながるリンクをクリックするよう受信者に促すSMSテキスト・メッセージ。

これらの新しいタイプのフィッシング攻撃は、エンドユーザーを直接ターゲットにしているだけでなく、ほとんどはその個人のデバイスもターゲットにしているため、これらの脅威を軽減するにはセキュリティ意識啓発がもっとも効果的であることが証明されています。組織は、そのパスワードがどれほど強力であっても、資格証明を盗もうとするフィッシング攻撃のリスクが完全に解消されることはないことを理解する必要があります。

悪用された脆弱性の拡大

悪用については、45 %が、パッチがあてられていないアプリケーションの既知の脆弱性、パッチがあてられていないオペレーティング・システムの既知の脆弱性、新規および未知のゼロ・デイ脆弱性の悪用による攻撃を1回以上体験していると回答しました。

多様な脅威、手段、方法が今後の懸念

今回の調査によると、企業は、今後発生する脅威の種類や脅威をもたらすために攻撃者が使用する方法に関して、さまざまな種類の攻撃を懸念しています（図10を参照）。調査参加者の懸念事項は次のとおりです。

- **脅威の種類：**ランサムウェア、マルウェア、悪用など。
- **方法：**ターゲットを絞った侵入攻撃、企業の電子メールの攻撃、資格証明の盗難や誤用など。
- **手段：**電子メール・フィッシングと誤った構成のサーバー・ワークロード、クラウド・サービス、ネットワーク制御など。

この調査では、これらの手段とサイバー攻撃者がさまざまな脅威をもたらすために採用する方法の組み合わせの頻度と量が、課題であることが明らかになりました。

“注目すべきは、サーバー・ワークロードを感染させるために増殖するマルウェアについての懸念..."

図10：今後12か月間の上位の懸念事項

組織のインフラストラクチャ、データ資産、事業運営のリスク・レベルに関して、（経験した過去の攻撃に関係なく）今後12か月間に次のそれぞれの脅威の種類にどの程度の懸念がありますか。（回答者の割合、N=450）

注目すべきは、サーバー・ワークロードを感染させるために属職するマルウェアについての懸念です。このことは、組織のもっとも重要なビジネス・アプリケーションを保護することを重視すべきであることを示しています。クラウド上のワークロードは、増殖するマルウェアの影響を受けます。侵入されたエンドポイントを介してマルウェアを感染させる攻撃チェーンは、オブジェクト・ストアなどのクラウド・サービスや、その他のオンプレミスまたはクラウド上のサーバー・ワークロードからも同様に機能するためです。

増殖するマルウェア以外では、攻撃の種類ごとに調査回答者の懸念のレベルの差があまりないことは、攻撃者がさまざまな方法で攻撃に来ていることを組織が理解しているという事実を示しています。このレポートの後半では、組織がそのような攻撃から身を守るために採用しているいくつかの多層防御の方法を紹介します。

サイバー攻撃が及ぼす運用上および財務上の影響

サイバーセキュリティ・インシデントの報告では、攻撃の主要な影響として財務的損失が強調されています。しかし、通常、財務的損失だけでなく、事業運営の混乱がより頻繁に起こることがわかりました。たとえば、回答者の2／3（66％）が過去2年間に事業運営に影響を与えたサイバーセキュリティ・インシデントを経験しています。これらの影響には、事業運営の混乱、サービス提供能力の低下、従業員の生産性の低下、ITプロジェクトの遅延などがあります。サイバー攻撃による運用上の影響は、非常に混乱した状況で明らかになる可能性があります。たとえばランサムウェアが感染した医療機関では患者のケアの提供能力を阻害することが明らかになります。

ただし、財務的損害も確かに発生します。回答者の半数以上（51 %）が、財務的損失、資本支出の増加、株主価値の低下などの財務的影響について述べています。財務的損害と事業運営の混乱は相互に排他的ではないことに注意してください。サービスの中断や従業員の生産性が低下すると、多くの場合、組織のビジネス機会が直接失われてしまいます。

注目すべき財務的影響の1つは、新しいテクノロジーに対する資本支出の必要性です。一部の組織では、古いシステムを使用して業務を遂行しており、ハードウェアをアップグレードしてソフトウェアを更新するためのコストを払っていません。これらの古いシステムは、新しいバージョンのオペレーティング・システムをサポートしていない可能性があり、攻撃に対して脆弱なままになっています。また、基礎となるオペレーティング・システムの新しいバージョンをサポートしていないレガシー・アプリケーションのサポートを維持するために、オペレーティング・システムにパッチが適用されないままになっています。一部の企業にとって、サイバーセキュリティ・インシデントは、将来の攻撃から身を守るために必要な手段として、古いシステムをアップグレードしたり、クラウドに移行したりするための資本投資を促します。しかし、クラウド・サービスをさらに導入することで、そのような資本投資の必要性を取り除くことができます。

3

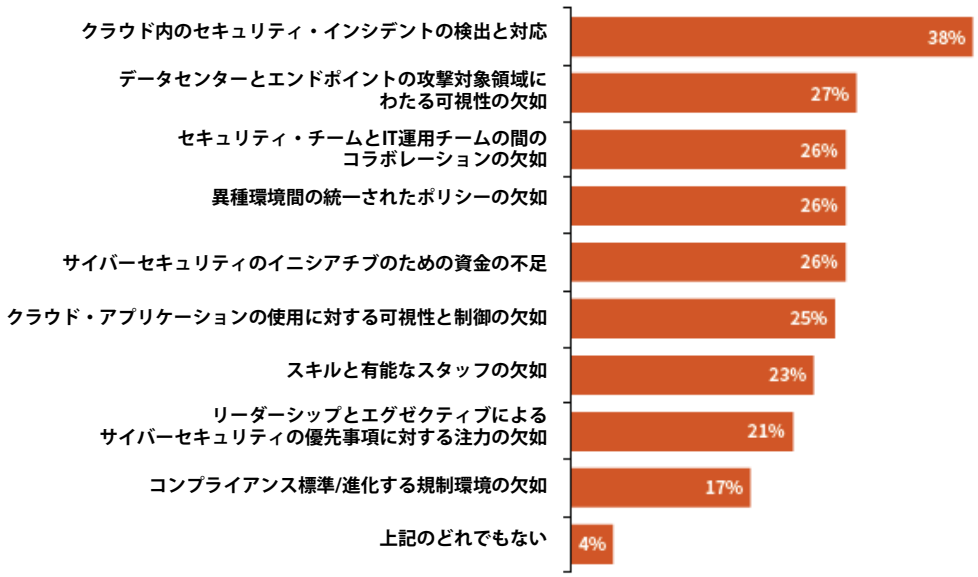
クラウドの採用による新しいサイバーセキュリティの課題

クラウドの採用によって可視性のギャップが発生

今日のもっとも重要なサイバーセキュリティの課題について、群を抜いてもっとも頻繁に言及される懸念事項（回答者の38 %が言及）は、クラウド環境でセキュリティ・インシデントを検出して対応する能力です（図11を参照）。

図11：企業が報告するサイバーセキュリティの最大の課題

あなたの組織においてのサイバーセキュリティの最大の課題は何ですか。
（回答者の割合、N=450、複数回答３つ可能）



> **"可視性の欠如は一般的な繰り返される話です。これは、利用者が物理的なネットワーク・レイヤーにアクセスできないことと、クラウド・サービスのセルフサービスの性質が原因です。"**

可視性の欠如は、クラウド・サービス使用におけるセキュリティの観点では、一般的に言及されている話です。これは、利用者が物理的なネットワーク・レイヤーにアクセスできないことや、クラウド・サービスのセルフサービスの性質など、オンプレミスのインフラストラクチャとは根本的に異なるクラウド・サービスを保護するいくつかの特性が原因です。

海外ではサイバーセキュリティ・インシデントのモニタリングに関わる課題が大きくなっていますが、日本企業は未だ限定的なクラウド利用に留まっており、モニタリングまで議論が及んでいない状況です。今後、オンプレミスのシステムとクラウドを併用していく中で、インシデントをどのようにモニタリングしていくか、態勢の検討が望まれます。

ESGの調査研究では、IaaSのセキュリティの可視性を向上させるためにもっとも重要な領域を評価することにより、クラウドの可視性の欠如を定義しました。[5]この調査結果では、何よりもまず、クラウド上のワークロードにソフトウェアや設定に関わる脆弱性が存在するかどうかを把握し、システムの振る舞い、異常、特権アカウントの使用を監査し警告する必要性を示しています。この一連の可視性要件は、ワークロード中心のアプローチを示しています。

図12：クラウドがホストするワークロードへのセキュリティ可視性を向上させるための分野

組織のIaaS/PaaSがホストするワークロードのセキュリティ可視性を向上させるためにもっとも重要であると思われる分野はどれですか。（回答者の割合、N=450、複数回答３つ可能）

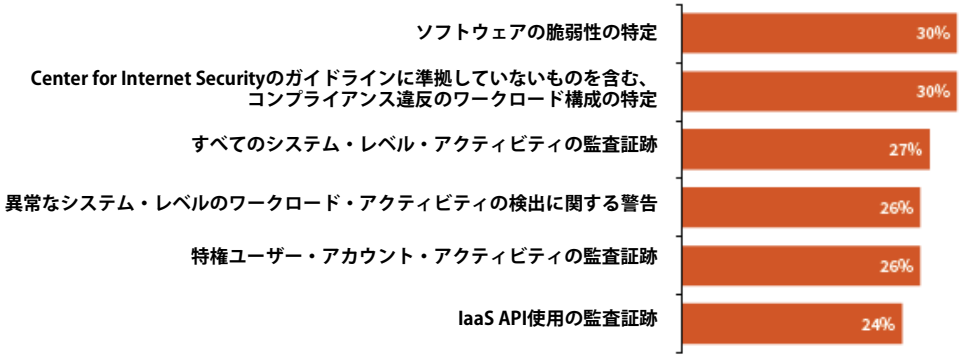


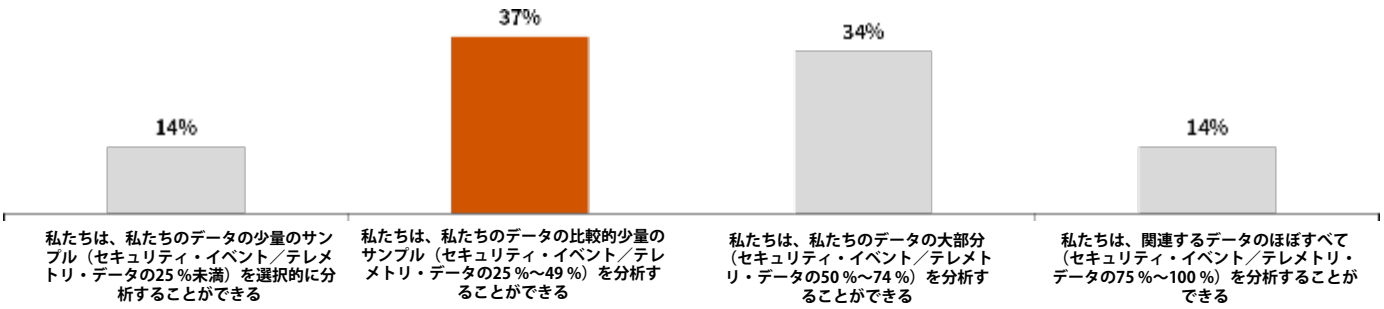
図11で示した通り、私たちの調査によると、サイバーセキュリティの専門家は、データセンターとエンドポイントの攻撃対象領域にわたる可視性の欠如にも懸念を示していますが、これには正当な理由があります。サイバーセキュリティ攻撃の段階を描いたモデルでは、いくつかの攻撃がデータセンター全体でターゲットまで到達するためのエンドポイントに基盤を築く方法を示しています。たとえば、特権アカウントの資格情報（ID／パスワード等）を盗み出すフィッシング攻撃は、オンプレミスでもクラウドでも、重要なシステムを危険にさらします。異常なエンドポイント・アクティビティを検出して評価する機能によって、リモート・コマンドおよび制御サーバーへの接続の作成など、攻撃チェーンの動作が可視化されます。そのようなエンド・ツー・エンドの可視性により、組織はサイバーセキュリティ防御の弱点を特定し、必要な変更を加えることができます。

イベント・データの分析は規模の課題

大量のセキュリティ・イベントとテレメトリ・データを企業全体で収集して分析する能力は、重要な問題です。本調査の回答者の37 %のみが比較的少量のサンプルデータ（すべてのデータの25 %～49 %として定義）のみを分析可能であり、別の14 %が少量のサンプルデータ（イベント・データの25 %未満）のみを分析可能であると回答しました。図13を参照してください。

図13：セキュリティ・イベント・データの分析機能

セキュリティ・イベント／テレメトリ・データを大規模に（つまり企業全体で）収集し分析する組織の能力を表しているものはどれですか。（回答者の割合、N=450）



[5] 出典：ESGの調査『*Trends in Hybrid Cloud Security:Minding the Gap*』（2017年11月）

目次に戻る

イベントを分析できないことは、今回の調査により判明した大きな課題の1つです。多くの組織が、イベントを収集して分析することに苦慮している理由には、クラウド・サービスの利用によりイベント・データが生成される攻撃対象領域が拡大されたことを含む、複数の要因があります。

量が膨大であることに加えて、分析の優先順位付けを行うためにイベントを分類するためには、イベント・データの関連付けをもとにしたコンテキストが必要です。機械学習の適用を含む高度な分析ソリューションを使用しなければ、時間のかかる手作業が必要になります。組織は利用可能なコンテキストを設定するため、コンテキストの設定と修復の手順を自動化する機能はクラウド上の大量のデータを処理するのに役立ちます。

確立したクラウド・セキュリティ・ポリシー遵守の課題：がシャドウITの阻止

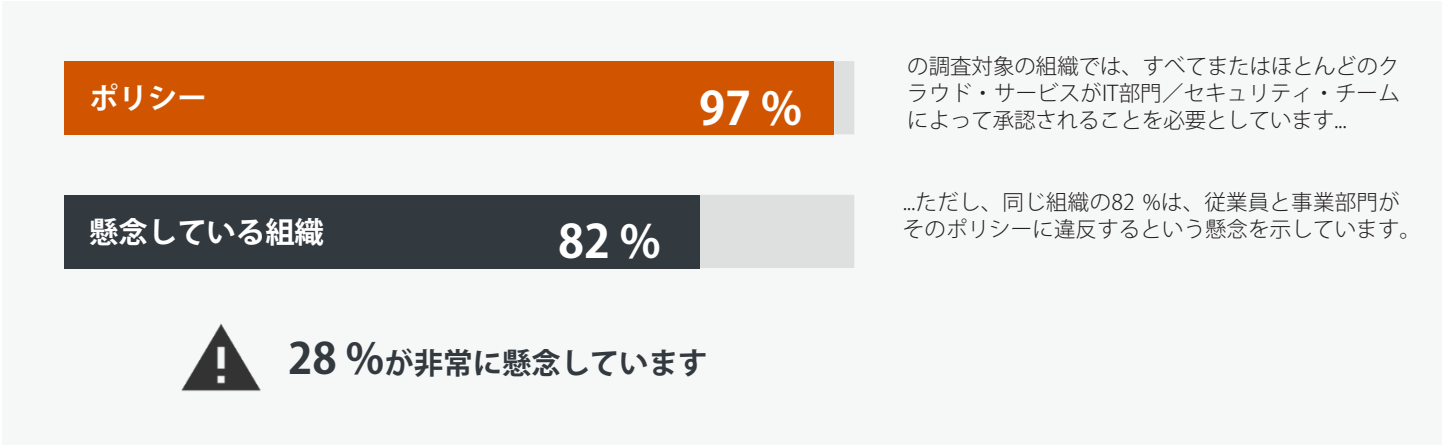
競争の圧力によって、企業は製品やサービスをより迅速に提供する必要があるため、事業部門（LOB）長がクラウド・サービスを利用できるようにする必要があります。しかし、IT部門とサイバーセキュリティ・チームは、ポリシーによりセキュアにクラウド・サービスを使用できるようにしようとしましたが、ほとんど成功しませんでした。

調査によると、組織の50 %は、*すべて*のクラウド・サービスはIT部門／セキュリティ・チームによって承認される必要があると述べ、別の47 %は、大多数のクラウド・サービスはIT/セキュリティによって承認される必要があると指摘しました。しかし、現実には、これらのポリシーは守られていません。合計で97 %がクラウド承認ポリシーを定義していますが、驚くべきことに回答者の82 %はこれらのポリシーが守られていることを懸念しています（図14を参照）。

図14：確立されたポリシーにもかかわらず、クラウドの使用に関する懸念が残っている

あなたの組織でクラウド・サービスを使用するための組織のポリシーをもっともよく表しているのはどれですか。
（回答者の割合、N=450）

組織内の個人、部門、事業部門がクラウド・サービスのポリシーに違反していることをどの程度懸念していますか。
（回答者の割合、N=450）



クラウド使用ポリシーにもとづいていないシャドウITが個人や事業部門にて蔓延している状況は、すぐにクラウド・サービスを利用しなければならない必要性、個人的な好み、外部コラボレーションの増加を含む多くの要因によって引き起こされています。高いレベルのコラボレーション（多くの場合、エンタープライズ・ファイル共有および同期（EFSS）アプリケーションを介した外部パーティとのコラボレーション）を伴う一連の作業は、未承認のクラウド・アプリケーションの使用を増加させます。特定のクラウド・アプリケーションをよく利用しているエンドユーザーは、職場でそのサービスを使用し、そのサービスを介して企業データを共有する傾向があります。

シャドウITを利用する主な原因は、個々の従業員による幅広いSaaSアプリケーションの不正使用と、IaaSおよびPaaSプラットフォームを活用して迅速なアプリケーション開発を行う分散開発チームの2つです。IT部門とセキュリティ・チームの関与は業務の俊敏性を妨げているとみられており、クラウド・サービスの安全な使用を受け入れて有効にする新しいアプローチが必要になります。

サイバーセキュリティ・スキルの深刻な不足

多くの企業は、クラウド・セキュリティに対応できるようITとサイバーセキュリティの運用を変えていません。大部分は、彼らがまだ必要なスキルを身に付けておらず、特定の運用上の問題を解決していないからです。

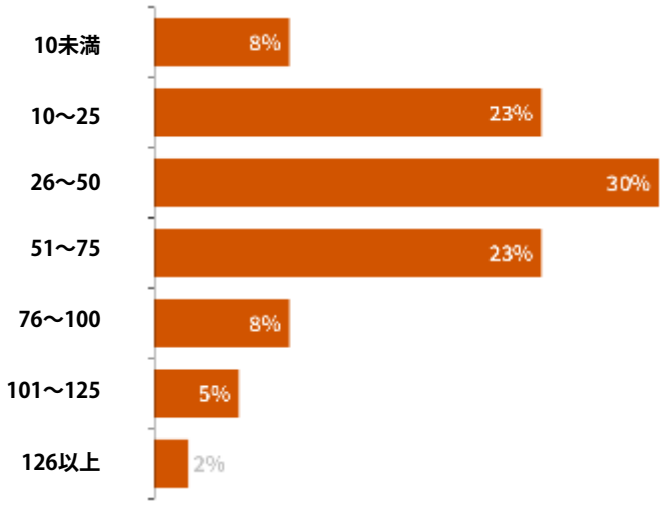
私たちの調査で言及されている最大のサイバーセキュリティの課題の1つは、スキルと有能なスタッフの欠如です。回答者の23 %が組織の最大のサイバーセキュリティの課題の1つとして、スキルを持つ有能なスタッフの欠如であると回答しました（前の図11を参照）。ESGの調査研究では、51 %の回答者が組織のサイバーセキュリティ・スキルの欠如が問題になっていると答えています。[6]

スポットライト：ポイント・ツールによる疲弊

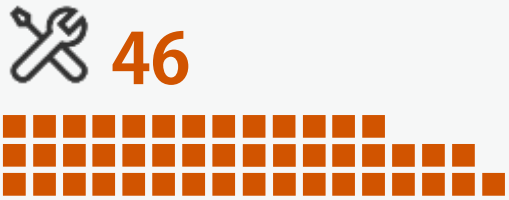
企業のサイバーセキュリティの担当者が多忙を極めていることは明らかです。サイバーセキュリティの担当者は平均46個のセキュリティ製品を管理しており（図15を参照）、新しいクラウド・テクノロジー、ツール、最新のベスト・プラクティスを習得する時間はほとんどない状況となっています。このような深刻な疲弊の結果、運用上の非効率性が生じています。その一例として、この調査では、サイバーセキュリティ・チームがイベント・テレメトリを大規模に処理しようと苦労していることが明らかになりました。

図15：サイバーセキュリティの担当者が管理するポイント・ツールの平均数

あなたが自ら担当しているサイバーセキュリティのディスクリート製品またはポイント製品のおおよその数を教えてください。
（回答者の割合、N=450）



リーダーシップの役割（CISO、VP、セキュリティなど）によって管理されるさまざまなサイバーセキュリティ製品の数（平均）：



[6] 出典：ESG Master Survey Results, *2018 IT Spending Intentions Survey*（2017年12月）

4

IDとアクセス管理の重要性

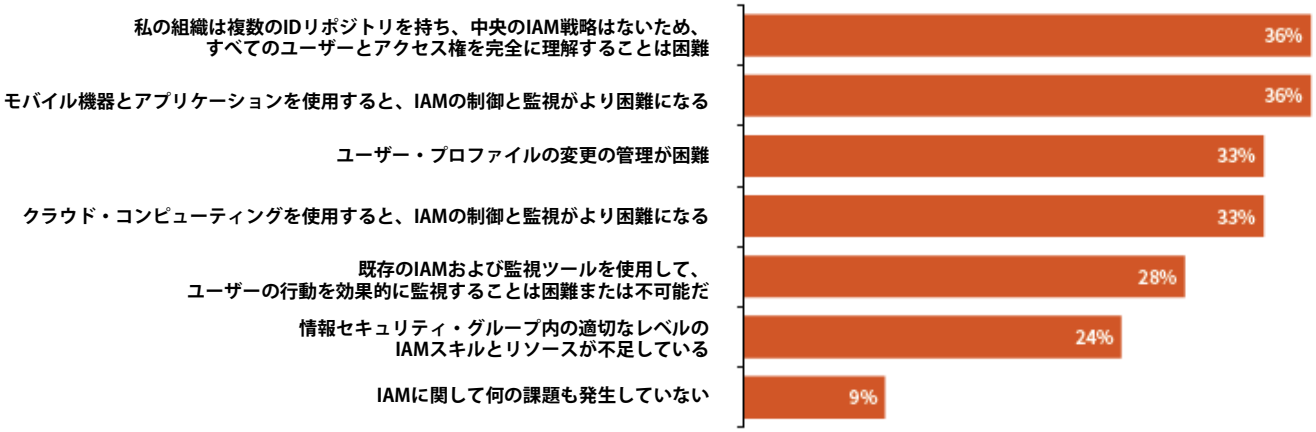
"いつでもどこでも、誰でも、どんなデバイスからでも"により大規模環境のIDの課題が発生

現在、さまざまなナレッジ・ワーカーがモバイル機器を使用して、CRM、ERP、HCMなどのクラウド配信の企業向けビジネス・アプリケーションや機密情報を含むドキュメントにアクセスしています。そして、彼らのその行動は、時間と場所を問いません。同時に、請負業者、ビジネス・パートナー、パートタイム労働者、顧客、サプライヤなどの従業員よりも広い範囲の個人が、アプリケーションやデータにアクセスしているため、ID管理は課題ですが、クラウド対応の職場を保護するうえでも重要になっています。

実際に、クラウド・サービスの使用は、ナレッジ・ワーカーのモビリティの向上とともに、IDとアクセス管理（ID and Access Management : IAM）のシステムとその業務にとって課題となっています。私たちの調査でもっとも頻繁に言及されているIAMの課題は、モビリティの問題（モバイルユーザー、機器、アプリケーションの増加）と、組織が複数のIDリポジトリを管理する必要性であることは驚くべきことではありません（図16を参照）。その結果、統合IAM戦略が欠如しているため、ユーザーを認証しアクセス権を管理するための信頼できる情報源を構築することが困難になっています。

図16：IDとアクセス管理の課題

あなたの組織でもっとも重要なIDとアクセス管理（IAM）の課題は次のうちどれですか。
（回答者の割合、N=450、複数回答３つ可能）



日本企業ではクラウド利用の全社展開はこれから本格化していく状況であり、クラウド利用におけるアクセス権限管理に関わる課題が今後顕在化することが考えられます。そのため、クラウド利用を全社展開する前に、まずは現在利用しているクラウドにおいて、ID・アクセス権限管理を高度化し、今後の本格展開に備えることをお勧めします。

企業は、既存のIAMと監視ツールを使用してユーザーの行動を監視することは、不可能ではないにしても、困難であると述べました。調査の回答者は、特に監視については、モバイル機器とクラウド・アプリケーションの使用がIAMの制御と監視の使用を複雑にしていると述べました。しかし、調査の回答に基づくと、企業は従業員に付与した権限のレビューをより頻繁に行うことでセキュリティ上のメリットを享受することができます。現在、45 %が四半期に1回権限をレビューし、28 %が毎月レビューしていると答えています。

権限のレビューは、退職した従業員がオンプレミス・アプリケーションへアクセスする権限を削除するプロセスと、クラウド配信アプリケーションへのアクセス権を削除プロセスにおいて重要となります。元従業員のオンプレミス・アプリケーションへのアクセスを排除する場合、IT部門は、通常、従業員のラップトップを回収したり、VPNアクセスを無効にしたり、ドメインからユーザーを削除したりするなどの手順を含む退職手順に従います。しかし、元従業員は企業のSaaSアプリケーションにアクセスするためのVPN接続を必要とせずに、自分の認証情報を使用して別のデバイスからアクセスすることができます。そのため、クラウド・アプリケーションを使用するための元従業員のアクセス権限の削除により、クラウド・アプリケーションの認証情報の無効化が従業員退職プロセスの重要な手順になると同時に、ERPやCRMシステムなどのビジネス・クリティカルなアプリケーションにとって特に重要なものになります。

クラウド対応の職場でIDを管理することは、任意の場所および時間にすべてのユーザー、デバイス、アプリケーションに対応する、大きな課題となっています。そのため、IDはクラウド対応の職場のサイバーセキュリティ戦略の中心になければなりません。IAMは大規模に運用されていますが、今日の複雑なITインフラストラクチャではさらに重要となり、企業が完全な最新のID戦略を実装することを必要とします。結局のところ、IDは、エンタープライズ・アプリケーションおよびシステムのすべての扉を開く合鍵です。

> **IDとアクセス管理のポリシーは、最小権限のベスト・プラクティスに従い、ビジネス・プロセス、ロールおよび権限を個人のHRプロファイルと整合させることに基づいている必要があります"**

IAMポリシーで業務と権限の整合が必要

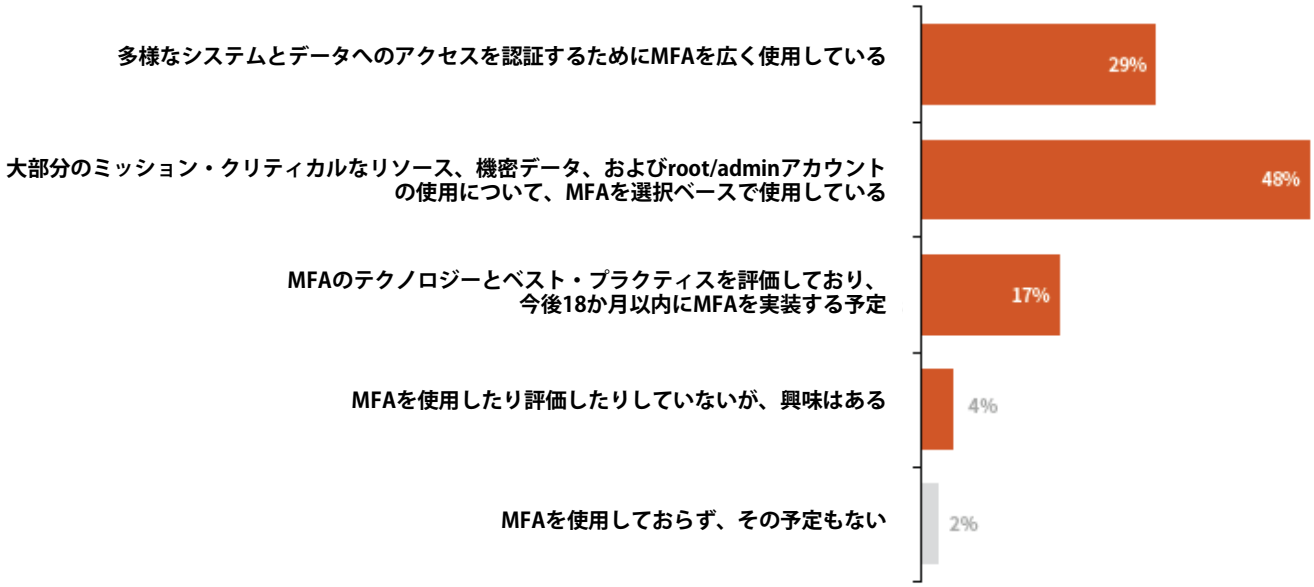
IDを正確に管理するために、企業は、これまで管理していたIDやデバイスではなく、今後は個人（個人ユーザー）をもとにしてIDを管理する、という考え方を持つ必要があります。これは特に、個人がアクセスできる対象と、持っている権限のレベルについての信頼できる唯一の情報源がないため、IAMに複数のリポジトリを使用しているという図16の36 %の企業に対する課題です。

また、IAMの機能が進化すると、職場における従業員の流動性が高くなります。従業員の離職率が非常に低い組織であっても、今日の従業員は以前に比べてより多くの業務を担う傾向があります。効果的にIDやアクセス権限を管理するには、従業員の権限が業務に応じて設定必要があります。つまり、IDとアクセス管理のポリシーは、最小権限のベスト・プラクティスに従い、ビジネス・プロセス、業務および権限を個人のHRプロファイルと整合させることに基づいている必要があります。これにより、最小限の個人に、効果的に業務を遂行するために必要な最低限の権限を設定し、最低限のシステムへのアクセス権が付与されます。ただし、この調査で示されているように、一元化されたIAMリポジトリを持たないクラウド対応の職場では、最小権限のユーザー・アカウント（Least-privileged user Account: LUA）管理を実装するのは難しい作業です。一元化されたポリシーに基づいて複数のクラウド・サービスへのアクセスを統合する手段としてSecurity Assertion Markup Language（SAML）を採用したシングル・サインオン（SSO）ソリューションは、LUAの目的に向けた手段を提供します。

機密資産および重要資産へのアクセスにMFAを採用

幸いにも、多くの企業では、もっとも機密性の高いミッション・クリティカルな資産へのアクセスを許可するために、多要素認証（MFA）を採用しています。実際に、回答者の約半数（48 %）は、MFAを使用して、機密データやミッション・クリティカルなデータと資産へのアクセスを制限し、別の29 %がMFAを使用して、より多様なシステムやデータ資産へのアクセスを認証しています（図17を参照）。MFAの使用は、PCI DSSなどの業界規制への準拠要件となることもあります。

図17：多要素認証の現在の使用



スポットライト：リスクベース認証

基本的なMFA以外に、多くの組織は二次的な要素を要求する、より洗練されたリスクベースのアプローチを採用しています。"リスクベース認証"は、ユーザーのリスク・プロファイルや行動など、認証リクエストのコンテキストを評価します。たとえば、米国のある場所から通常ログインしている従業員が、他の国から企業ネットワークまたはクラウド・サービスにアクセスしようとしていて、その履歴レコードがない場合、リスクベース認証を使用するMFAソリューションは、この異常を認識して、別の認証方式によるユーザー認証を要求します。このソリューションは、クリティカルかつ機密と判断するアプリケーションおよびデータ資産へアクセスする際に、上記コンテキストを利用したリスクベース認証を実施するといった構成にすることもできます。つまり、このアプローチでは、不必要にユーザーを遮断することなく、コンテキストに基づいてリスク・レベルを判定し、認証のレベルを設定することができます。

リスクベース認証は、フィッシング対策の制御としても機能し、盗難された資格証明を使用して企業資産にアクセスするような攻撃を防止します。調査の回答者の66 %が、企業資産へのアクセスを保護するためのリスクベース認証について興味があることを示しており、このような認証方式は本調査結果と強く関連しています。

また、リスクベース認証は、ユーザーの行動を監視して二次要素による認証を促すだけでなく、通常のアクセスと使用を識別し、潜在的な悪意のある内部従業員を特定することに対しても効果的です。この種類の継続的な監視は、どの従業員がどの資産にアクセスしているかを企業が判断するのに役立ちます。これにより、最小権限のアクセスやリスクベース認証などのIAMベスト・プラクティスを実装することで、組織がこれらの資産のリスクをより適切に管理するのに役立ちます。

66 %

が、異常を検出したときに二次的な要素をトリガーすることに非常に興味があるか、ある程度興味があります

5

最新のIT環境におけるサイバーセキュリティのベスト・プラクティス

この調査結果では、次の内容で構成された最新のIT環境が示されています。

- 境界の定義の再定義が必要となるさまざまな世代のアプリケーション・スタック
- SaaS、PaaS、IaaSのスタック全体にわたる複数のクラウド・プロバイダーの使用
- クラウド・アプリケーションの使用を保護にするための実用的なアプローチ
- 意識啓発の継続的な重視
- テクニカル・サイバーセキュリティのスキルとロールを再定義する必要性
- 構成管理のベスト・プラクティスとしてのパッチ適用
- ミッション・クリティカルなアプリケーションを保護するための多層防御アプローチの実装

この最新のIT環境に類似しているか、その環境に移行している組織が今日から実装を開始できるいくつかのベスト・プラクティスを紹介します。

既存の境界防御にとどまらない思考

ネットワーク境界は、現在、モビリティとクラウド・サービスの普及により、形を持たない広い境界の一部となっています。ITとサイバーセキュリティのリーダーは、サイバーセキュリティ・プログラムを、今日のIDベースの境界防御に向けて、戦略、スキル、プロセスの面において、ネットワーク・セキュリティ制御を強化する必要があります。

クラウド・セキュリティ実用主義を採用

クラウド・アプリケーションとサービスが採用される速度と程度は、より慎重なアプローチを必要とする企業のサイバーセキュリティ・プログラムとは異なる可能性があります。クラウド・サービスの使用はしばしばユーザー主導であり、ビジネスの緊急性から生まれているため、ITとサイバーセキュリティのリーダーはクラウドの安全な使用を可能にし、関連するリスクを緩和する必要が生じます。

このようなバランスをとるためには、事業部門のリーダーと連携するという実用的なアプローチをとり、クラウド・アプリケーションの使用を推進するための要件を理解することが必要です。このようなビジネス上の議論は、事業部門のリーダーが、クラウドの安全な使用を確実にするために不可欠なサイバーセキュリティ・ポリシー、プロセス、およびコントロールを理解するのに役立ちます。このような実用的なアプローチを実施するには、以下を含む一連のベスト・プラクティスを採用する必要があります。

クラウド・セキュリティのベスト・プラクティス：

クラウド・サービス全体のカバー：SaaSのプロパティやIaaSサービスなどを含む、使用されている幅広いサービス全体に可視性と制御ポリシーを適用できます。

コンテキストによる可視性：シャドウITアプリケーションの検出以上のことを対象として、組織は、使用中の各アプリケーションおよびサービスに関連するリスクを評価することができます。

データの検出と分類：可視性の別の側面として、クラウド・サービスの使用と連携してどのような種類のデータ資産が格納されているかについてのインサイトを提供します。

システムの整合性の維持：構成のずれを監視し、不適合ワークロードやクラウド・サービス（オブジェクト・ストアのACLなど）の修復を自動化することで行います。

脅威の防止：クラウド・サービスが攻撃手段として使用されないように、悪意のあるペイロードの転送中のトラフィックと保存中のコンテンツを検査することで行います。

データ損失防止（DLP）ポリシー：どのユーザーがクラウド常駐データのクラスにアクセスできるかを制御します。

ユーザーの行動の監視：非標準のログインの時間や場所、不規則なデータ・アクセス操作など、異常なアクティビティを監視します。

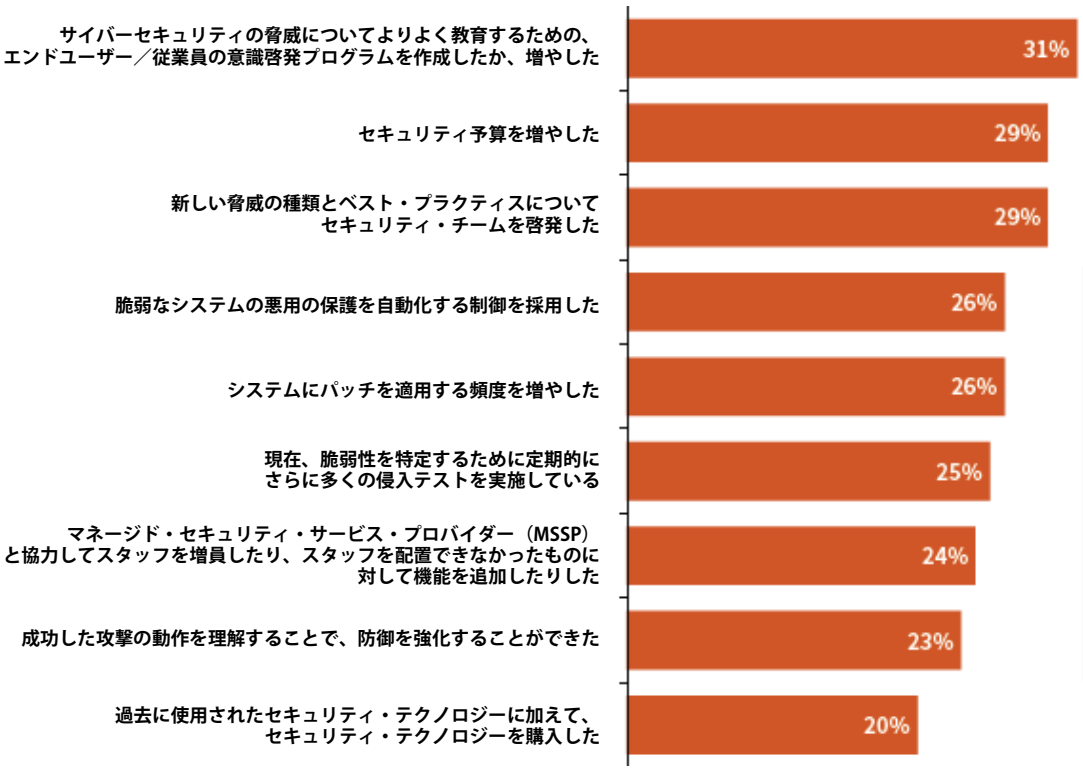
これらのベスト・プラクティスは、完全に許可されたクラウド・アプリケーションおよびサービスと、許可されていないクラウド・アプリケーションおよびサービスの両方に適用できます。しかし、許可されていないクラウド・アプリケーションおよびサービスは、現在、クラウド・サービスの使用を保護するための実用的なアプローチとして利用を許容されています。

エンドユーザーの意識啓発トレーニングの重視

私たちの調査によれば、人とプロセスに焦点を当てたアプローチは、もっとも影響力のある結果をもたらす傾向があります。過去2年間にどのような行動がセキュリティにもっともプラスの影響を及ぼしているのかを尋ねたところ、回答者は、新しい脅威についての従業員向けの啓発プログラムであると回答しています（図18を参照）。特に、過去1年間のフィッシング攻撃の増加により、従業員がフィッシング攻撃を識別できるようになるために、個別に啓発する必要があります。この調査では、人への投資には、サイバー攻撃者が使用する手法、戦術、ツールについて、セキュリティの専門的な知識を深めることが含まれる必要があることも示されています。

図18：サイバーセキュリティ態勢を改善するための措置

組織のサイバーセキュリティ態勢を向上させるのにもっとも効果的だった組織のアクションは次のうちどれですか。（回答者の割合、N=403、複数回答３つ可能）



サイバーセキュリティ予算を増やす優先順位がもっとも高い分野：

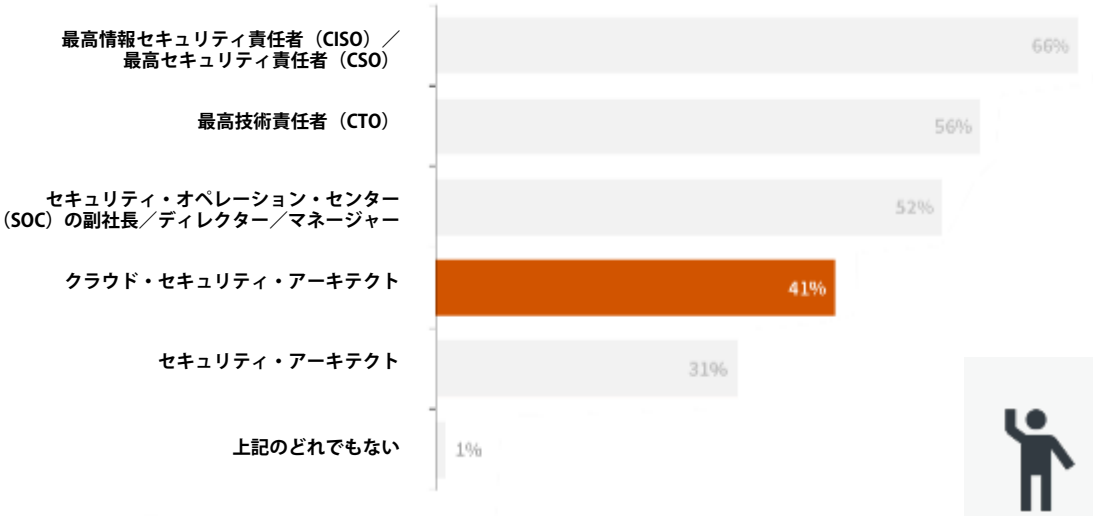
トレーニングの増加

スポットライト：サイバーセキュリティの役割の再設定

人に焦点を当てたサイバーセキュリティの役割を再設定する必要性は、この調査の注目すべき発見の1つ、すなわちクラウド・セキュリティ・アーキテクトの出現によって明らかになっています。回答者の31 %が、現在組織にセキュリティ・アーキテクトの役職を設定していると回答したのに対し、41 %が、クラウド・セキュリティ・アーキテクトを設定していると回答しており、すでに新しい考え方が導入されていることを示しています（図19を参照）。多くの企業は、新しいクラウド・セキュリティ・チームの中核的メンバーとしてのクラウド・セキュリティ・アーキテクトの重要性が増していることを認識しています。クラウド・セキュリティ・アーキテクトには、技術スキルのギャップを埋めることができるだけでなく、クラウドのスピードに合わせてサイバーセキュリティ戦略を戦略的に設計できることが求められます。

図19：一般的なサイバーセキュリティ・リーダーシップの役割

あなたの組織に存在するセキュリティ・リーダーシップの役割は次のうちどれですか。（回答者の割合、N=450、複数回答可）



従来のセキュリティ・アーキテクトではなく、専任の職務である**クラウド・セキュリティ・アーキテクト**が存在する組織が増えました。

日本においてはクラウド・セキュリティ・アーキテクトを設置している企業は今のところ限定的な状況です。クラウド・サービス向けに考慮すべきセキュリティは、オンプレミス環境向けとは異なるため、今後、クラウド利用のさらなる拡大によって、クラウド・セキュリティ・アーキテクトの設置を含めたクラウド・セキュリティの管理体制を明確にする必要があります。

“効果的なサーバー・セキュリティには、調整されたパッチ適用と構成管理プログラムが不可欠です。"

パッチ適用は通常IT運用で処理されますが、一部の組織では、IT部門とセキュリティ・チームの間でパッチ適用の責任者が誰か曖昧になることがあります。あいまいな状況であったとしても、パッチ適用プログラムはリスク削減の観点から設計する必要があります。たとえば、新しい脆弱性が判明すると、企業はまず、特定の脆弱性がよりミッション・クリティカルなシステムに影響を与えるかどうか、出回っている悪意ある攻撃がこれらの脆弱性を利用しているかどうかを調べ、それに応じて優先順位を決める必要があります。

このような常識的なガイドラインが存在していたとしても、パッチと構成の管理は依然として曖昧なルールです。多くの組織では、標準的な構成の基準に基づいてサーバーを構成しています。しかし、基準は変わりうるため、組織は本番システムの構成を継続的に評価し、強化する必要があります。構成とソフトウェアの脆弱性を定期的に評価した結果、パッチを適用する可能性があります。この目的は、全体的な構成管理の規律の一環としてパッチ管理を運用可能にすることであり、これによりリスク評価に基づいて脆弱性のパッチ適用を迅速に行うことができます。このプロセスにより、企業は組織の資産に悪意をもたらすリスクを軽減するパッチ適用アプローチを合理化することができます。

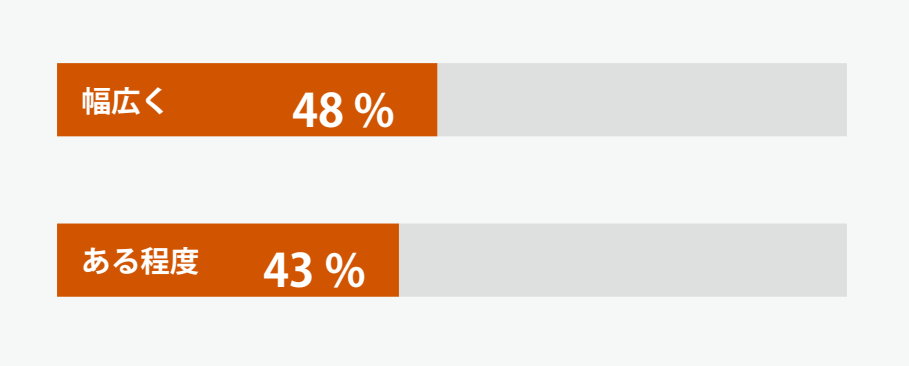
クラウド・コンピューティングの規模によって攻撃対象領域が急速に拡大し、より多くの資産を危険にさらす可能性があるため、パッチ適用は重要になります。マルチ・クラウド環境の組織では、システムの整合性の一貫性を確保するために、クロスクラウドのパッチ適用戦略を検討する必要があります。

多層防御によるアプリケーション・スタックの保護

企業は、ネットワークベースのセキュリティ制御や監視などの検出および検査のテクノロジーを長年にわたって使用してきました。現在、企業は、異常な振る舞いを検出するユーザーおよびエンティティ行動分析（User and Entity Behavior Analytics: UEBA）、エンドポイントでの検出と対応（Endpoint Detection and Response: EDR）、およびサイバー攻撃者を撃退するのに役立つテクノロジーを含む新しい"多層防御"ツールを採用しています。私たちの調査によると、多層防御アプローチには、幅広い水平攻撃対象領域にわたるネットワークのパフォーマンス監視（Network Performance Monitoring: NPM）アクティビティと、アプリケーション・スタックへの垂直可視性のためのアプリケーションのパフォーマンス監視（Application Performance Monitoring: APM）の活用も含まれています。実際には、多くの企業がNPMとAPMのソリューションを利用しており、潜在的なセキュリティの脅威と攻撃を特定して分析するために48 %が幅広く使用しています（図20を参照）。

図20：サイバーセキュリティのためのNPMとAPMのツールの使用

潜在的なセキュリティ上の脅威や攻撃を特定して分析するために、あなたの組織はネットワークのパフォーマンス監視（NPM）/アプリケーションのパフォーマンス監視（APM）ツールとデータをどの程度使用していますか。（回答者の割合、N=450）



私たちの調査によると、多層防御アプローチには、NPMとAPMのツールの活用も含まれています"...

サイバーセキュリティにNPMとAPMを使用するユースケースでは、ネットワークとアプリケーションのパフォーマンスを監視するIT運用管理/ネットワーク・オペレーション・センター（NOC）チームと、セキュリティ・オペレーション・センター（SOC）のサイバーセキュリティ・アナリストとのコラボレーションも促進されます。

図21：NOCチームとSOCチームのコラボレーション

あなたの組織のネットワーク・オペレーション・センター（NOC）チームとセキュリティ・オペレーション・センター（SOC）チームは、サイバーセキュリティの問題に関してどの程度協力していますか。（回答者の割合、N=450）

37 %

NOCチームとSOCチームは、脅威を検出するためのネットワーク監視ポリシーの定義と、脅威に対する調査と対応について積極的に協力している

24 %

SOCチームは、ネットワーク監視ポリシーについてNOCチームに提案し、受動的に協力してサイバーセキュリティ・インシデントに対処している

17 %

NOCとSOCの両方として機能する1つのチームを持っている

NOCからの通知をSOCに活用する組織は、リモート・サイトへの外部接続を含め、ネットワーク全体の利用率の急上昇に関連するセキュリティ・イベントのアクティビティに対するモニタリングが可能となります。このようなエンド・ツー・エンドのネットワーク・レベルの可視性により、NOCチームおよびSOCチームは、分散サービス拒否（DDOS）またはボーダー・ゲートウェイ・プロトコル（BGP）攻撃を示す可能性のあるアクティビティを識別できます。

APMソリューションを活用して、異常な基盤システムの振る舞いを追跡することにより、より広範で包括的な監視が可能となります。たとえば、異常なCPU使用率の検出、特に新規および未知のプロセスによる異常なCPU使用率の検出は、暗号マイニング操作に含まれるシステムのハイジャックを検出するのに役立ちます。

これらのユースケースでは、NOCチームおよびSOCチームがネットワーク、アプリケーション、およびデータを危険にさらしているこれらの攻撃や他の種類の攻撃から組織を保護することを可能にする、NPMとAPMのソリューションが果たす魅力的な脅威検出の役割を強調しています。

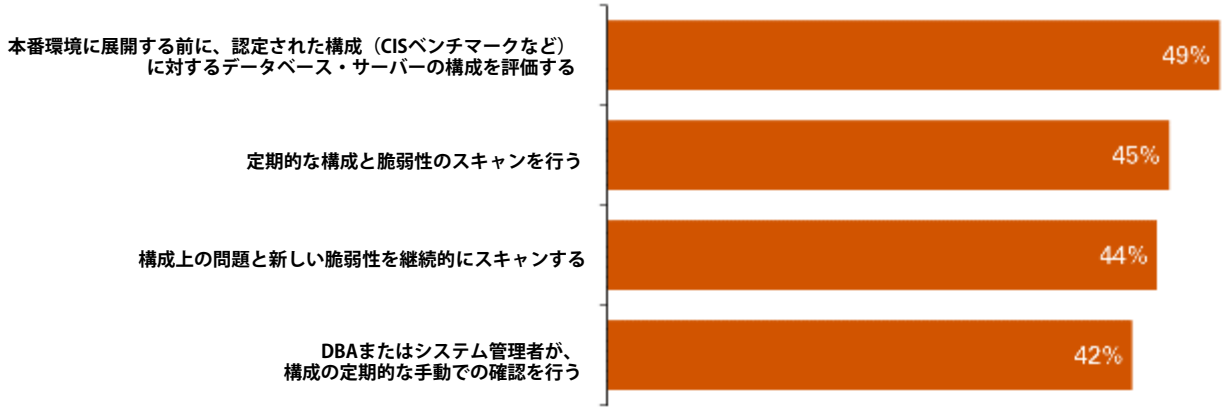
多層防御アプローチによるデータベース層の保護

データベースは、ビジネス・クリティカルなアプリケーションの基盤となります。そのため、攻撃対象領域を限定し、アクセス制御ポリシーを適用し、異常な行動をあらゆる角度から監視するのに役立つ包括的なデータベース・セキュリティ戦略が不可欠です。

データベースのセキュリティは、構成管理のベスト・プラクティスから開始され、攻撃対象領域を限定します。私たちの調査では、これを実現するために、企業は保証された構成に対してデータベース・サーバーを評価し、定期的な構成と脆弱性のスキャンを行い、構成を手動で確認しています（図22を参照）。

図22：適切なデータベース・サーバー構成を保証するための措置

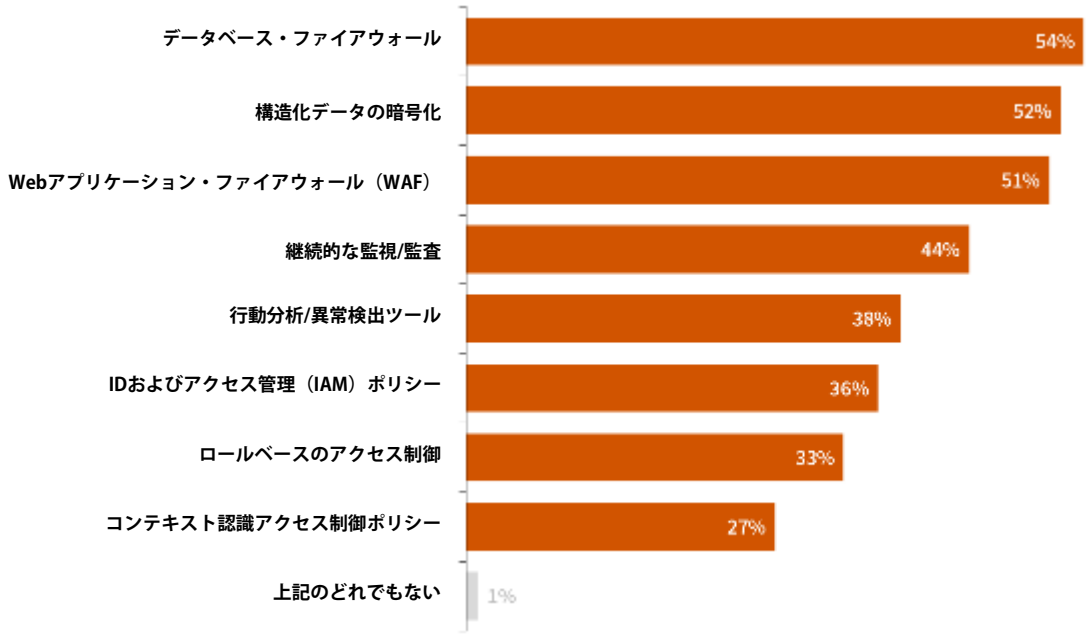
あなたの組織は、本番データベース・サーバーが適切に構成されていることをどのように確認しますか。
（回答者の割合、N=450、複数回答可）



また、組織は、人とデータベースにアクセスするアプリケーションに対してアクセス制御を行い、ミッション・クリティカル・データベースを保護しています。これらの保護を行うために、データベース・ファイアウォールの使用、構造化データの暗号化、アプリケーション・ファイアウォール、およびその他の制御を使用しています（図23を参照）。

図23：データベース・サーバーのセキュリティ・テクノロジーと方法

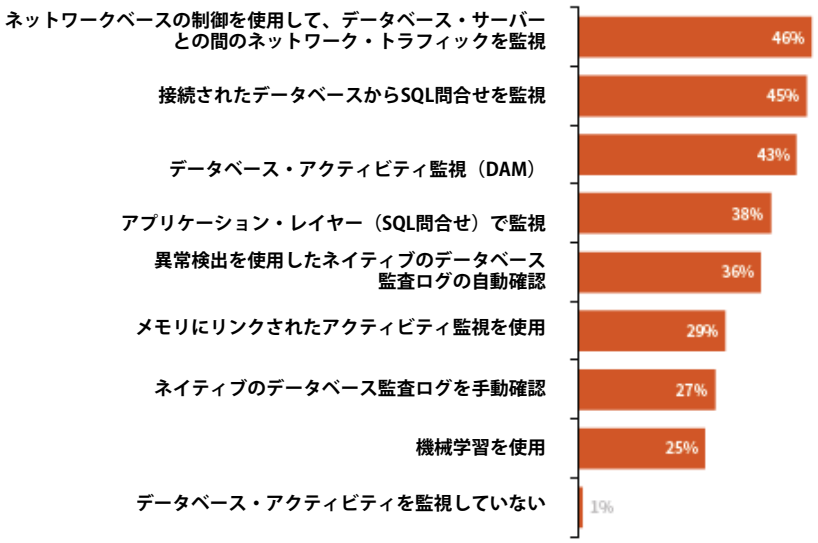
組織の機密性の高い重要なデータベース・サーバーへの不正アクセスを防止するために、あなたの組織で使用しているテクノロジーと方法は次のうちどれですか。（回答者の割合、N=450、複数回答可）



今日のデータベース・セキュリティの目的は、データの損失からの保護だけでなく、システムの操作による詐欺やデータの破損から保護することにまで及んでいます。このような脅威を軽減するために、複数の監視方法を使用しています。調査回答者の中でもっとも一般的なアプローチとしては、ネットワーク・ツールを使用してデータベース・サーバーとの間のトラフィックを監視する方法、接続されたデータベースからSQL問合せを監視する方法、データベース・アクティビティ監視を使用する方法です（図24を参照）。

図24：データベース・サーバーの監視方法

あなたの組織は、疑わしいアクティビティを検出するために本番データベース・サーバーをどのように監視していますか。（回答者の割合、N=450、複数回答可）



データベース・サーバーの保護は重要であり、このセクションで説明する重要なサイバーセキュリティのベスト・プラクティスの1つです。上記手法では、セキュリティ・チームとデータベース管理者が協力して、データベース常駐アセットが不正アクセス、不正行為、破損などの脅威から保護されることを保証するための方法のフレームワークを利用しています。今後も、常に進化するサイバーセキュリティのベスト・プラクティスは、いくつかの非常に影響力のある新しいテクノロジーによって変わる可能性があります。私たちは、現在、それらに注意を向けています。

6

新しいテクノロジーにより期待されるサイバーセキュリティの向上

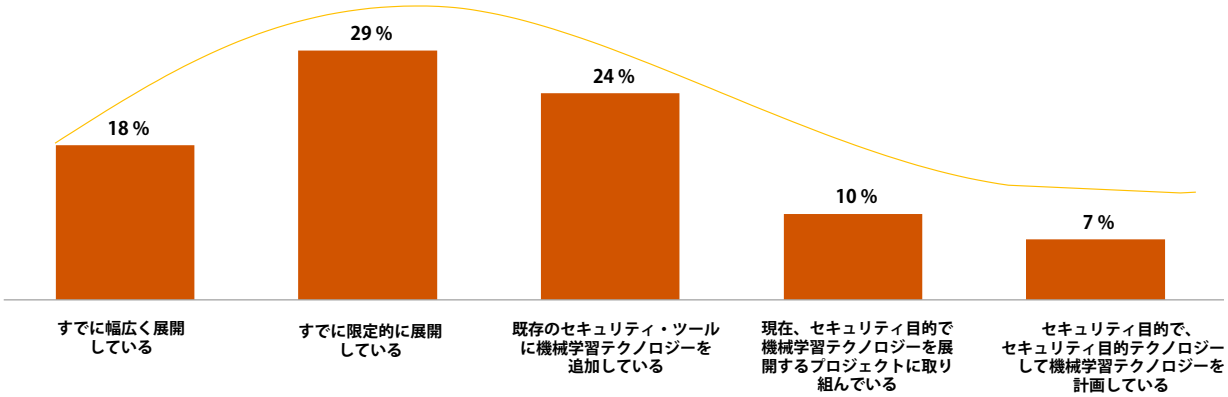
本のレポートで取り上げたセキュリティ・プロセスとテクノロジーを企業が導入を進める一方で、多くの新しいテクノロジーが登場しています。歴史的に、脅威の検出とセキュリティの向上と運用効率の向上は、しばしば互いに排他的に行われていました。機械学習とセキュリティの自動化は、これらを同時に改善する可能性を提供する2つのテクノロジーです。

機械学習は脅威からの保護の有効性向上を約束

機械学習は、ゼロ・デイの脅威を特定するのに役立つサイバーセキュリティ・テクノロジーになりつつあります。機械学習では、新規または以前から未知であった脅威を識別するための予測を行うため、行動と属性をモデル化します。調査回答者の29 %が限定的に機械学習を使用し、18 %が幅広く使用していると答え、24 %が、現在、既存のセキュリティ・ツールに機械学習を追加しています。さらに、組織の27 %が、機械学習を現在展開しているか、使用を計画しているか、活用に興味を持っています（図25を参照）。このことは、脅威の検出と保護の効果を向上させるためのサイバーセキュリティ・テクノロジーとして、機械学習が利用されていることを表しています。

図25：サイバーセキュリティのための機械学習の利用

あなたの組織は、サイバーセキュリティの目的で機械学習テクノロジーを展開した、または展開する予定ですか。
（回答者の割合、N=449）



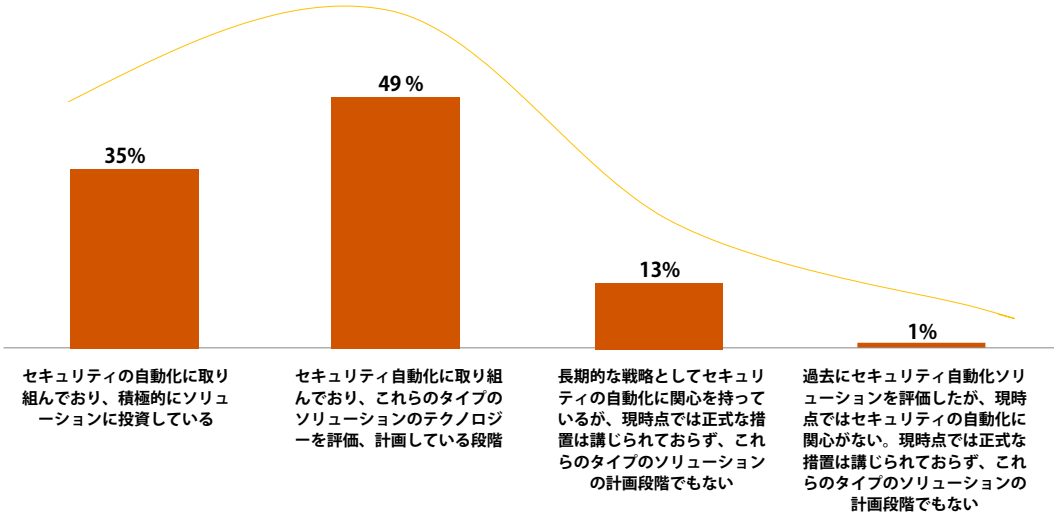
機械学習は、ゼロ・デイ・マルウェアなどの脅威を緩和するだけでなく、多くの組織が手作業で分析するために苦労している大規模なセキュリティ・イベント・データセットの分析を自動化するために、さまざまなサイバーセキュリティ制御に組み込まれています。

セキュリティの自動化により、より高い運用効率を実現

これまで、ITとサイバーセキュリティの担当者は、SOCが検知したアラートに対応し、ファイアウォール・ルールを更新するなど、サイバーセキュリティのアクションの自動化を不便に感じていました。今日、セキュリティの自動化は、効率的にアラートに対応し、脆弱性を改善するための基本的なテクノロジーとみなされています。実際に、回答者の半数近く（49 %）が現在、セキュリティの自動化を評価および計画していると答えています。また、35 %が、積極的にソリューションに投資していると回答しています（図26を参照）。

図26：企業はセキュリティの自動化に取り組んでいる

修正措置を自動化するセキュリティ自動化ソリューション（ファイアウォール・ルールの更新、影響を受けるシステムの隔離など）のあなたの組織の計画／導入について表しているものはどれですか。（回答者の割合、N=450）



日本企業では、リソースの不足により、SOCが報告するアラートの一部しか調査できていない状況です。セキュリティ自動化ソリューションを導入することで、アラート対応への負荷が軽減できるため、より多くのアラートに対応できるようになります。リソース不足によりアラート対応を制限している企業は、自動化ソリューションの導入が望まれます。

レーダー・スクリーン：IoT

モノのインターネット（IoT）の出現によって、プラットフォームや地域間でデータを保存し共有する接続デバイスの数が増大しているため、IDの課題は急速に増加しています。ESGの調査によると、回答者の25 %がすでにIoTに対応しており、43 %が今後1～2年にIoTプロジェクトを開始する計画があると述べています。[7] これらの接続されたデバイスの増加により、小売店や輸送用ハブとなる拠点など、現場のセンサー・デバイスが提供する自動化およびテレメトリを使用して、製品、サービス、およびビジネス・モデルを拡張することができます。

クラウド・サービスの普及と同様に、IoTによって、サイバーセキュリティを考慮して設計されていない何百万ものデバイスがネットワークに接続され、サイバー攻撃の対象領域が拡大し、リスクが増大しています。これらのデバイスが生成するイベント・テレメトリは、本レポートで述べてきたセキュリティ・イベントの処理の課題にさらに影響を及ぼします。

[7] 出典：ESG Master Survey Results, *2018 IT Spending Intentions Survey*（2017年12月）
目次に戻る

IoTセキュリティは、IT部門とオペレーション・テクノロジー（OT）チームが協力して、IoTデバイスの保護に関する一連のベスト・プラクティスの実装に取り組む必要があります。IoTセキュリティのベスト・プラクティスには、以下のものがあります。

- 組織のオンボーディング・プロセスの一環としてデバイスを評価して、不正なデバイスにネットワーク・アクセスが許可されていないこと、またはシャドウ・ネットワークの設定が許可されていないことを保証します。
- 承認された構成のデバイスのみがネットワークに接続できることを保証します。
- 可能であればデバイスを分類し、そのアウトバウンド・トラフィックを監視してボットネットからのハイジャックを検出する必要があります。
- 新しいIoTデバイスは、ハードコードされたパスワードを含まないか、サポートされていない（さらにパッチを適用できない）オペレーティング・システムに付属していないなどを保証するために、メーカーによるセキュリティ対策を遵守していることを査定する必要があります。

まとめ

『オラクルとKPMGによるクラウドの脅威レポート 2018年』の調査では、クラウド対応のセキュリティに関する多くの真実が明らかになりました。セキュリティは、大規模な変化に対応するうえでの課題です。クラウド利用者は、セキュリティおよびコンプライアンスの課題に目を向け、クラウドを活用する職場を保護するために、本レポートにあるベスト・プラクティスの適用方法に関する戦略的な議論を行う必要があります。

この調査の結果は、クラウド・サービスが採用されている速度、脅威の状況の多様性、攻撃対象領域が拡大したことで生成されるセキュリティ・イベント・データの膨大な量など、複数の要因の兆候として規模を定義するのにも役立ちます。また、ITとサイバーセキュリティのリーダーは、サイバーセキュリティのイニシアチブに資金を提供するだけでなく、今日のITモデルのダイナミクスに関するスキルとアプローチを再編成することによって、課題に対応していることも明らかになりました。

クラウド・セキュリティの準備状況のギャップを埋めるために行われる施策は、ビジネスの俊敏性を実現する重要なアプリケーション（CRM、ERP、HCM）を保護することに重点を置き、人、プロセス、テクノロジーをカバーしています。データの盗用、暗号通貨をマイニングするためのCPUサイクルのハイジャック、人質を取ることでの金銭の要求、事業運営の混乱を望むサイバー攻撃者に対して、サイバーセキュリティの担当者はこれまで以上に警戒しなければなりません。これらの脅威を防止するための実証済みのベスト・プラクティスの多くは、現在では物理的な境界と同程度の量のユーザーとデータの境界を保護するために適応させる必要があります。

また、サイバーセキュリティのアプローチは、ポリシーを遵守しないユーザーがクラウド・サービスを使用する方法に合わせる必要があります。したがって、資産を攻撃から保護するというサイバーセキュリティの目的は、クラウドのスピードに対応する必要があります。このレポートで取り上げられている最新のテクノロジーである機械学習とセキュリティの自動化は、サイバーセキュリティ・チームが事業部門と同様に機敏であるように支援することを約束し、そのチームも大規模な変化に対応できるようになります。

日本企業も業務の効率化・働き方改革の実現に向けてクラウドの利用が拡大し、本リポートで報告されているサイバーセキュリティの課題が顕在化することが想定されます。本格的にクラウドを利用する前に、今後、どのような体制、プロセス、テクノロジーでクラウド・セキュリティを確保すべきか、早急に議論を進めることが望まれます。

[7] 出典：ESG Master Survey Results, *2018 IT Spending Intentions Survey*（2017年12月）

目次に戻る

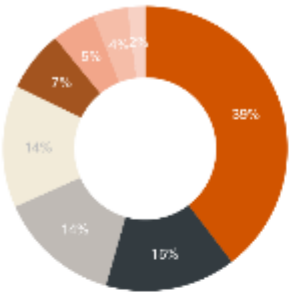
付録：調査方法とデモグラフィックス

本レポートに記載されているデータは、北米（米国およびカナダ）、ヨーロッパ（英国）、アジア・太平洋（オーストラリア、シンガポール）の民間および公共組織からの450人のサイバーセキュリティおよびITの専門家による、Enterprise Strategy Groupが実施した2017年12月4日から2018年1月10日までの包括的なオンライン調査によって収集されました。調査の対象者は、組織のパブリック・クラウドの利用状況をよく理解している、サイバーセキュリティ・テクノロジーの製品とサービスの評価、購入、管理の担当者です。

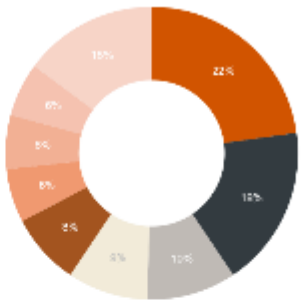
注：このレポートの図と表の合計は、四捨五入のため、100 %にならない場合があります。

次の図は、回答組織のデモグラフィックスを示しています。

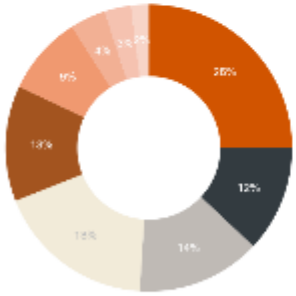
従業員数別の回答組織の割合



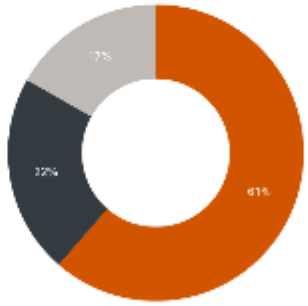
業界別の回答組織の割合



年間収益別の回答組織の割合（USドル）



地域別の回答組織の割合



主な貢献者

Mary Ann Davidson
Chief Security Officer – Oracle Corporation

Greg Jensen
Sr Principal Director Cloud Security Business – Oracle Corporation

Tony Buffomante
Principal – KPMG LLP

Laeeq Ahmed
Oracle Security & Controls Leader – KPMG LLP

Brian Jensen
Oracle Risk Consulting Sales Leader – KPMG LLP

Doug Cahill氏
Group Director and Senior Analyst – Enterprise Strategy Group

特別な感謝：

Akshay Bhargava、Suzanne Blackstock、Adam DeMattia、Troy Kitch、Mary Beth McCombs、John Hodson、James Finlaw、Peter Sinanian、Jennifer Gahm、Dan Koloski、Darren Calmen、Russ Lowenthal、Brendan Keane、Tim Stahl、Matt Flynn、Doug Madory、Sebastian Rovira、Josh McKibben、Rajan Behal、Eric Maurice、Sridar Karnam、Vidhi Desai

お問合せ先

KPMGコンサルティング株式会社
Mail：cybersecurity@jp.kpmg.com
Tel：03-3548-5111

日本オラクル株式会社 Oracle Digital
URL：oracle.com/jp/contact-us
Tel：0120-155-096