



クラウド環境の 信頼性の向上

クラウド サービスはITオペレーションに浸透し、世界の90%以上の企業で利用されています。多くの企業はクラウドファーストで、クラウドサービスが不都合な場合に限りオンプレミスのサービスを利用しています。ITアーキテクチャは急速にハイブリッドなプライベート/パブリッククラウド モデルに移行しています。今後15か月間で、IT予算の80%はクラウド関連に費やされると見られています。

93%



の組織が何らかの形式でクラウドサービスを利用している。

2016年9月、Intel Securityでは、2,000人を超えるIT担当者を対象に今年のクラウドの採用状況を調査しました。調査対象の業種、国、企業の規模は多岐に渡っていますが、スキルのあるセキュリティ担当者の不足は依然として解消されていません。今年の調査結果を見ると、この人材不足がクラウドの採用に大きな影響を及ぼしています。この調査では、クラウドの利用形態やシャドウITの影響を調査し、プライベート/パブリッククラウドサービスの主な問題点を把握することも目的としました。

今回の調査は、オーストラリア、ブラジル、カナダ、フランス、湾岸諸国（サウジアラビア、UAE）、ドイツ、日本、メキシコ、シンガポール、英国、米国にある中小企業（社員数500～1,000名）、中堅企業（社員数1,000～5,000名）、大企業（社員数5,000名以上）で技術的な意思決定を行う上級担当者を対象に実施しました。



49%

の回答者が、サイバーセキュリティのスキルがないため、クラウドの採用を躊躇している。

重要な調査結果

- クラウド サービスは広く利用されています。回答者の93%は、SaaS、IaaS、PaaSのいずれかの形態でサービスを利用しています。
- 組織内で使用しているクラウド サービスの平均数を見ると、2015年は43でしたが2016年は29に減少しています。これは、クラウド プロバイダーやソリューションの統合が影響しているものと思われます。クラウド アーキテクチャも大きく変化しています。2015年はプライベートクラウドが主流でしたが、その後、パブリッククラウドの採用が増加し、2016年はプライベートとパブリックを組み合わせたハイブリッド インフラが主流となっています。
- 回答者の約半数（49%）は、サイバーセキュリティのスキル不足でクラウドの採用が進んでいないと回答しています。このような回答が最も多かった国は日本、メキシコ、湾岸諸国です。
- パブリッククラウドサービスに対する信頼と認知度は年々向上しています。多くの組織は、クラウドサービスがプライベートクラウドと同等以上の安全性を備えていると考えています。また、所有コストを抑え、データ全体の可視性を実現できると見えています。パブリッククラウドを信頼しているユーザーと信用していないユーザーの割合は2対1になっています。

62%



の組織がパブリッククラウドに顧客の個人情報を保存している。

エグゼクティブ サマリー

52%



の回答者がSaaSアプリケーションに対するマルウェア感染を経験している。

- 信頼性が高まり、普及が進むにつれ、リスクに対する理解も深まり、パブリッククラウドに重要なデータを保存する組織が増えています。パブリッククラウドに最も多く保存されているのが顧客の個人情報で、62%の回答者がこのような保存を行っていると考えています。
- サイバー犯罪者もクラウドアプリケーションを見逃しません。回答者の半数以上(52%)がSaaSアプリケーションに対するマルウェアの感染を確認しています。
- IT部門にとってシャドウITの普及は頭の痛い問題です。IT部門やメインストリームでのクラウドの導入が進まないため、クラウドサービスの約40%はIT部門の承認なく利用されています。回答者の65%は、この状況でクラウドの安全性を維持することは難しいと考えています。
- プライベートデータセンターでアーキテクチャの仮想化が進んでいます。平均で約52%の企業のデータセンターでサーバーが仮想化されています。また、多くの回答者は、今後2年以内に完全なソフトウェア定義のデータセンターに移行すると予測しています。

40%



のクラウドサービスはIT部門の承認なしで利用されている。

まとめと推奨事項

クラウドサービスの信頼度が増し、様々なアプリケーションやデータが利用されています。ビジネスにかかせない重要なデータが扱われることも少なくありません。データは必要とされる場所で迅速かつ効率的に処理されています。脅威を迅速に検出してデータ侵害を未然に防ぐには適切なセキュリティ対策を実施する必要があります。クラウドサービスを利用することで、コストを削減し、必要なリソースを抑えることが可能になりました。また、様々なサービスが提供され、最適なサービスを選択できるようになりました。セキュリティベンダーもセキュリティの基本的な問題(移動中のデータの保護、ユーザーアクセスの管理、複数のサービスに対する一貫したポリシー)を解決するツールを提供しています。

65%



のIT担当者は、シャドウクラウドがクラウドの安全性を阻害していると考えている。

パブリッククラウド上に存在する重要なデータはサイバー犯罪者にとって格好の標的となります。攻撃者は、場所に関係なく、最も狙いやすい対象を攻撃します。このような攻撃に対して統合されたセキュリティソリューションは強力な防御策となります。また、このようなソリューションにより、組織が使用しているサービスやデータセットをセキュリティオペレーションですぐに把握できるようになります。

管理者が特に注意しなければならないのはユーザーの認証情報です。攻撃者に最も狙われるのが認証情報です。認証のベストプラクティス(まったく異なるパスワード、二要素認証または生体認証などの使用)を実施する必要があります。

シャドウITが組織のリスクとなることが分かっているにも関わらず、データ損失防止(DLP)、クラウドアクセスセキュリティブローカー(CASB)などのセキュリティ技術が十分に活用されていません。これらのツールを既存のセキュリティに統合するだけで、可視性を強化し、シャドウサービスを検出することができます。また、環境の種類に関わらず、保存または転送中のデータを自動的に保護することもできます。

2年



完全なソフトウェア定義のデータセンターの実現までにかかる時間

作業を外部に委託しても、リスクまで委託することはできません。どの企業も情報セキュリティに対するリスク管理と回避策を強化しなければなりません。クラウドファーストの指針に基づき、クラウドサービスでコストの削減と柔軟性の強化を行うだけでなく、セキュリティオペレーションも事後対応型からプロアクティブなものに変える必要があります。

レポートの完全版は、[こちら](#)からダウンロードしてください。



McAfee. Part of Intel Security.

マカフィー株式会社

東京本社 〒150-0043 東京都渋谷区道玄坂1-12-1
渋谷マークシティ5F 20F
TEL 03-5428-1100 (代) FAX 03-5428-1490
西日本支店 〒530-0003 大阪府大阪市北区堂島2-2-2
近鉄堂島ビル18F
TEL 06-6344-1511 (代) FAX 06-6344-1517
名古屋営業所 〒450-0002 愛知県名古屋市中村区名駅4-6-17
名古屋ビルディング13F
TEL 052-551-6233 (代) FAX 052-551-6236
福岡営業所 〒810-0801 福岡県福岡市博多区中洲5-3-8
アーク博多5F
TEL 092-287-9674 (代)

www.intelsecurity.com

Intel、Intelのロゴ、McAfeeのロゴは、米国法人Intel Corporation、McAfee、Inc.もしくは米国またはその他の国の関係会社における登録商標です。その他すべての登録商標および商標はそれぞれの所有者に帰属します。Copyright © 2017 Intel Corporation.1955_0117 2017年1月