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。

詳細情報

レポートの完全版については、**こちらからダウンロード**してご覧ください。

エグゼクティブ サマリー

2016 年 9 月、Intel Security（現 McAfee）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。

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。
- 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答えています。
- 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 の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。

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。**

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。**

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。**

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。

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。

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。

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。

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。

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。

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

〒 150-0043
東京都渋谷区道玄坂 1-12-1
渋谷マークシティ ウエスト 20F
Tel. 03-5428-1100（代表）
www.mcafee.com/jp