クラウド環境の信頼性の向上

医療機関の現状

医療業界のクラウド サービスの利用率は他の業界の平均値よりも若干高くなっています。医療情報のデジタル化が急速に進み、経費削減にもつながるためでしょうか。全体的な平均は93%ですが、医療機関の使用率は96%です。他の業界と同様に81%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。医療機関のITアーキテクチャでは、プライベートなクラウド データセンターからハイブリッドなプライベート/パブリック クラウド モデルへの移行が段階的に進んでいます。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。

医療機関でのクラウド サービスの利用率、課題、今後の計画に関するこの分析は、**Intel Securityが2016年に実施したクラウドの調査結果**を基にしています。この調査は、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、米国の技術的な意思決定を行う上級管理者を対象に実施しました。

96%

クラウドの採用率。医療機関は採用率が高い**業界のトップ3**に入っている。

主な調査結果 – 医療機関

今回の調査で、クラウドの採用率が最も高い業界のトップ3に医療業界が入りました。何らかのクラウド サービスを利用している割合は、金融サービスが99%、テクノロジ企業が99%、医療機関が96%です。医療機関で利用されているクラウド サービスの平均数は、2015年の41から減少し、2016年は33となっています。全体平均は43から29に減少していますので、医療機関の減少率はやや少なく見えますが、クラウド プロバイダーやサービスの統合が続いていることは間違いないようです。

24%

パブリック クラウド サービス（SaaS、IaaS、PaaS）のみを使用している医療機関の割合

クラウド アーキテクチャは大きく変化し、2015年はプライベート クラウドが主流でしたが、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型が主流となっています。しかし、医療機関でハイブリッド アーキテクチャの普及は進んでいません。パブリックのみのクラウド サービス（SaaS、IaaS、PaaS）を利用している医療機関が多く、その利用率は24%です（全体平均は19%）。医療機関のIT管理者に聞くと、IaaSやPaaSよりもSaaSサービスを利用するという回答が多く、67%はこれらのサービスに対する増資を計画していると答えています。今後もSaaSが中心となることは間違いありません。

intel Security

エグゼクティブ サマリー

46%

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**回答者

医療機関のIT管理者の約半数（46%）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。IaaSに関する質問では特にこの傾向が強くなります。全体的に見ると、IaaS導入の不安材料として最も多かった回答は、一貫した統合セキュリティ統制でしたが、医療機関ではITセキュリティ担当者のスキルが最も多い回答となりました。

スキル不足で採用が遅れている面もありますが、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増加しています。多くの組織は、パブリック 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、パブリック クラウドのほうがプライベート クラウドよりも所有コストを抑え、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医療機関が増えています。プライベート クラウド上の重要データに対する不正アクセスを懸念する回答は全体的な平均を上回っています（医療機関は37%、全体平均は30%）。医療記録の電子化や医療システムの相互接続が進み、医療機関でも重要データのパブリック クラウドへの移行が進む可能性があります。たとえば、60%の回答者は顧客データ（患者の情報）を保管すると答え、54%の回答者はスタッフのデータを保管すると答えています。

60%

パブリック クラウドに**顧客データ（患者の情報）を保管**している医療機関

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。医療機関の回答者の半数以上（52%）がSaaSアプリケーションに対するマルウェアの感染を懸念しています。クラウド サービス プロバイダーの利用について、回答者の25%はデータの漏えいを懸念（全体平均は22%）し、13%はマルウェア インシデントを懸念しています（全体平均は10%）。

52%

SaaSアプリケーションに対するマルウェア感染を懸念している回答者

他の業界と同様に、医療機関のIT部門でもシャドウITは問題となっています。医療機関で利用されているSaaSサービスがすべてIT部門の承認を得ているわけではありません。医療機関の担当者の回答を見ると、利用されているクラウド サービスの38%はIT部門の承認を得ずに利用されています。また、このようなアプリの約半数はIT部門で認識されていません。未承認のシャドウITアプリを見つけた場合の対応については、大半の回答者がアプリに対するアクセスをすべてブロックすると答えています。全体的に、医療機関のIT担当者はシャドウITを重大な問題と認識しています。回答者の63%は、クラウドの安全と安定を阻害する要因としてシャドウITの問題を挙げています。

多くの医療機関はSaaSサービスを導入し、パブリックのみのクラウド サービスを利用していますが、26%はプライベートのみのサービスを利用し、50%はパブリックとプライベートのハイブリッド型を利用しています。プライベート クラウドの場合、仮想データセンター サーバーの利用率（51%）は全体平均（52%）よりも若干低くなっていますが、医療機関の担当者の回答を見ると、コンテナーの利用率が最も高くなっています。76%の回答者が、2年以内を目途に完全なソフトウェア定義データセンターへの移行を計画していると回答しています。

38%

医療機関で使用されているクラウド サービスの中で**IT部門の承認を得ていないサービスの割合。**IT部門が存在を確認しているのはその半数に過ぎない。

まとめと推奨事項

医療業界は、他の業界と比べてSaaSアプリの利用率が高く、アプリに対する信頼度も高いようです。この業界の回答を見ると、プライベート クラウドの利用率は平均的ですが、ハイブリッド クラウドは最も低い結果となっています。パブリック クラウドの使用率の高さ、データの価値向上、あるいはその両方が原因で、他の業界と比べてサイバー攻撃、マルウェア インシデント、データ漏えいが増える可能性があります。

クラウドが定着した現在、医療機関はクラウドの普及に遅れずに、セキュリティの強化を急がなければなりません。様々なクラウド サービスの中から、経費削減とセキュリティ要件の両方を満たす最適なサービスを選択する必要があります。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。

医療記録を狙うサイバー犯罪者も増えています。『**McAfee Labs 脅威レポート: 2016年12月**』で報告したように、医療機関の医療データを狙ったランサムウェア攻撃が発生しています。医療機関では、治療の品質と効果を向上させるため、新しい技術を積極的に導入していかなければなりません。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。

『**McAfee Labs 2017年の脅威予測**』で報告したように、攻撃で最も狙われるのがユーザーの認証情報（特に、管理者の情報）です。タブレット、スマートフォンを含むすべてのエンドポイントを適切なセキュリティ対策で保護しなければなりません。感染や侵害のリスクを排除するには、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。

詳細については、『**クラウド環境の信頼性の向上**』の完全版をご覧ください。

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 渋谷マークシティウエスト 20F
TEL 03-5428-1100（代）FAX 03-5428-1480
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 アクア博多 5F
TEL 092-287-9674（代）
www.intelsecurity.com