【プレスリリース】

マカフィー株式会社
2018 年 12 月 5 日

※当資料は、2018 年 10 月 29 日に米国で発表されたプレスリリースの抄訳に、日本独自の内容を追加しています。

マカフィーレポート：クラウド上のデータは予想以上に危険に晒されている

クラウド上の機密情報、SaaS でのコラボレーション（協働）、IaaS/PaaS における設定ミスが増加するにつれ、クラウド上の脅威も増大

主な調査結果：

- クラウド上の全ファイル中、機密データは 21%。年々着実に増加
- オープン且つ、一般からアクセス可能なリンク経由での機密データの共有は前年比で 23%増
- パブリッククラウドを使用する企業では、IaaS、PaaS などのインスタンスで毎月あたり 2,200 件以上の設定ミスによるインシデントが発生
- クラウドでの脅威インシデント、たとえばアカウント侵害、特権ユーザーなどの内部脅威は前年比で 27.7%増

デバイスからクラウドまでを保護するサイバーセキュリティ企業である米国マカフィー（McAfee LLC、本社：米国カリフォルニア州）は、「Cloud Adoption and Risk Report（クラウドの採用とリスクに関するレポート）」を発表しました。本レポートは、クラウドの採用とリスクを明らかにするため、匿名化されたクラウド上の数十億単位のイベントを分析し、その結果をまとめたものです。今回の調査により、クラウド上に格納されている全データのうち 21%が機密データに該当し、盗難や漏洩が生じれば企業が危機に直面することが明らかになりました。クラウド上での機密データの共有が対前年比で 53%増加していることも相まって、データ保護、システム構成の監査、そしてコラボレーションの制御など、クラウドベースのセキュリティ戦略がない企業は、最も重要な資産、すなわちデータを危険に晒し、また内外の規制違反を引きおこす危険が一層高まります。

この調査では、企業は積極的にパブリッククラウドを利用し、顧客向けの新たなデジタル体験の創造を図る一方で、IaaS や PaaS インスタンスで月平均約 2,200 件以上もの設定ミスを発生させていることが明らかになりました。クラウドサービス事業者はクラウドそのもののセキュリティについては責任を負いますが、顧客のデータや顧客のインフラ、プラットフォームは事業者側の責任範疇ではありません。自社のデータを護るのは、どこに格納されているにせよ、その企業の責任です。そのためには、SaaS から IaaS や PaaS までをカバーする、クラウド全般のセキュリティソリューションが必要となります。

米国マカフィーのクラウドセキュリティ事業部 上席バイスプレジデントであるラジブ・グプタ（Rajiv Gupta）は、次のように述べています。「クラウドを利用した業務遂行はもはや標準となり、社員は躊躇なく機密データをクラウドに格納、共有するようになっています。意図しない共有や SaaS 上のコラボレーションでのエラー、IaaS や PaaS クラウドサービス上での設定ミスや脅威は増加しています。ビジネスを加速するために、企業はクラウドネイティブでスムーズな方法で自社のデータを保護し、SaaS、IaaS および PaaS 全般にわたって脅威から護る必要があります。」

クラウド上でのコラボレーションの長所と短所：

クラウドサービスはその優れた拡張性からビジネスを加速して好機をもたらし、迅速なリソースの活用やコラボレーションを可能にします。Box や Office 365 などのクラウドサービスは、コラボレーションの迅

速性と効果を増大するために利用されています。しかし、コラボレーションとは共有することであり、無制御な共有は機密データを危険に晒す可能性があります。
今回の調査では、以下のような実態が明らかになりました。

- 外部とファイルを共有するクラウドユーザーは全体の 22%、前年比 21%増
- 機密データをオープンで一般からアクセス可能なリンク経由で共有するケースが前年比で 23%増
- 機密データの個人メールへの送付は前年比 12%増

クラウド上で機密データの安全な保管、ファイル共有、コラボレーションを行うには、企業はまず自社が使用しているクラウドサービスを把握し、どこに機密データが格納されているのか、どのように、そして誰とその機密データを共有しているのかを確認しなければなりません。それらを把握しないと、適切なセキュリティポリシーの強化を図ることはできないのです。実態を把握することで、重要な機密データの未許可のクラウドサービスへの格納を禁じ、許可されたクラウドサービスにおける機密データの不適切な共有、例えば個人的なメールアドレスへの転送やオープンで一般からアクセス可能なリンクを経由した共有などを防止するための、いわば「ガードレール」を設置することが可能になります。

使用しているクラウドサービスの認識と現実：
2018 年 4 月に、マカフィーは「クラウド環境の現状レポートと今後: クラウドの安全性の状況と実用的ガイダンス」というレポートを発行しました。これは 11 か国 1,400 名の IT 専門家に対する、組織のクラウド利用に関する 100 問以上の質問を含む調査をもとにしています。今回のレポートでは、この調査の回答と、今回のマカフィーの分析からわかった現実を比較した内容も収めています。

4 月の調査では、自社組織内で使用されているクラウド サービス数を推測するよう尋ねました。平均的な回答は 31 で、80 以上あると考えている回答者がわずか 2% 、日本の場合は 37 という結果でした。一方で、今回の分析でわかった実際企業で使用されているクラウドサービスの平均は 、1,935 という結果でした。非常に驚くべき認識のギャップがあることがわかります。つまり IT 部門は 98% のクラウド サービスを認識していないということを意味しています。これは明らかにクラウドのリスクにつながります。

IaaS の設定ミスのリスク：

SaaS ではデータ保護、ユーザーID の管理、データへのアクセス管理は利用者側の責任です。一方、IaaS では、データ、ID、アクセスに加え、さらにアプリケーション、ネットワーク制御、ホストインフラ等についても、利用者側が責任を負います。これは自社のクラウドインフラに対してより大きな制御を施せる反面、セキュリティーリスクに晒される範囲とそれに対する責任が増大します。アマゾン ウェブ サービス（AWS）などの IaaS 型サービスは複数のインフラ プラットフォーム サービスを提供していますが、それぞれに複雑なセキュリティ設定が必要になります。IaaS や PaaS 等のセキュリティ問題が増大しているのは、企業が複数の IaaS、PaaS ベンダーを利用し、それぞれのベンダーの複数のインスタンスを運用しているからです。
今回の調査では、以下のような実態が明らかになりました。

- IaaS、PaaS の利用では AWS の割合が 94%と最も多いものの、78%は AWS と Azure を併用
- 企業の IaaS、PaaS の設定ミス関連のインシデントは一度の運用で平均して 14 件、その結果、設定ミスの件数は月ベースで 2,200 件超
- AWS S3 バケットの 5.5%は、ワールドリード許可設定がされ、一般公開の状態に

マカフィーでは標準的なセキュリティ対策の一環として、導入した AWS、Azure、Google Cloud Platform や他の IaaS、PaaS の設定に対して常に監査、監視を行い、IaaS や PaaS プラットフォームに格納された情報を保護することを推奨しています。オンプレミス型のデータセンターの代替として、IaaS、PaaS の利用は急速に拡大しています。企業は、SaaS クラウドサービスにおける自社のデータ保護と脅威からの防御、

IaaS、PaaS クラウドサービスにおける適切な設定、ワークロードの安全の確保などのセキュリティ対策の責任を果たし、セキュリティ インシデントを未然に防止することが重要です。

アカウント侵害と内部脅威：

クラウド上のデータに対する脅威の大半は、アカウント侵害と内部脅威に起因します。クラウドを利用するエンタープライズ企業では、クラウド上に生成される平均イベント数は月間 32 億件を超え、その内異常イベントが 3,217 件、実質的な脅威イベントは 31.3 件となっています。アカウント侵害と内部脅威について、今回の調査結果では、以下のような実態も明らかになりました。

- アカウント侵害、特権ユーザーまたは内部脅威などのクラウド上の脅威は、前年比で 27.7%増
- 調査対象の全組織の内 80%は、少なくとも 1 件／月のアカウント侵害が発生
- 調査対象の全組織の内 92%ではクラウド認証情報が盗まれ、ダーク・ウェブ上で販売されている
- Office365 での脅威は、前年比で 63%増

アカウント侵害や内部脅威に備えるためには、企業はクラウドサービスがどのように利用されているかを把握する必要があります。また、同じユーザーが同時に複数の異なった場所からアクセスするなど、アカウントの不正利用の恐れがある異常なイベントの特定も必要です。

以上のような実態を改善するためにクラウド上のデータ保護に向けてまず取り組むべきことは、CASB（Cloud Access Security Brokers）（英語）の導入です。CASB はクラウドネイティブのセキュリティサービスで、クラウドサービスのセキュリティ、コンプライアンス、そしてガバナンスポリシーを強化します。CASB は既存のセキュリティ対策を活用し、新たなクラウドネイティブなセキュリティと組み合わせることで、SaaS、IaaS、および PaaS 全般にわたって企業のデータの保護と脅威からの防御を可能にします。

参考資料：

·McAfee MVISION Cloud
https://www.mcafee.com/enterprise/ja-jp/products/mvision-cloud.html

·クラウド環境の現状レポートと今後: クラウドの安全性の状況と実用的ガイダンス
https://www.mcafee.com/enterprise/ja-jp/solutions/lp/cloud-security-report.html

·2016 Office365 Adoption & Risk Report（英語）
https://info.skyhighnetworks.com/WPOffice365CARRQ22016_BannerCloud-MFE.html

調査方法：

当社では、McAfee MVISION Cloud ユーザーのクラウドサービス利用状況を 25,000 以上のクラウドサービスで用いられるデジタルシグネチャを分析し、追跡しています。今回の「Cloud Adoption and Risk Report（クラウドの採用とリスクに関するレポート）」の作成にあたり、そのうち 3,000 万人超相当の利用状況に関する匿名化されたデータを分析・集計しました。また、調査を補足する関連データとして、パブリックまたはプライベートクラウドサービスのユーザーである 11 ヵ国のセキュリティ専門家 1,400 人を対象とした調査（2018 年）も引用しています。

マカフィーについて

マカフィーはデバイスからクラウドまでを保護するサイバーセキュリティ企業です。業界、製品、組織、そして個人の垣根を越えて共に力を合わせることで実現するより安全な世界を目指し、マカフィーは企業、そして個人向けのセキュリティ ソリューションを提供しています。詳細は http://www.mcafee.com/jp/ をご覧ください。

＜本情報のお問い合わせ＞

マカフィー株式会社（ http://www.mcafee.com/jp/ ）
広報担当 戸田
東京都渋谷区道玄坂 1-12-1 渋谷マークシティウエスト 20 階
Tel: 03-5428-1226 Fax: 03-5428-1480
hiromi_toda@mcafee.com

マカフィー広報担当
ウィタンアソシエイツ
担当：住川／中根
Tel: 03-4570-3169
mcafee-pr@witan.co.jp