クラウドセキュリティについて Salesforce システム管理者が 知っておくべき **４つの隠れた真実**

WITH secure

目次

クラウドセキュリティとは何か?

クラウドを活用したインフラ、プラットフォーム、アプリケーション、サービス等の利用が拡大するに従い、悪意のある攻撃者によってシステムに侵入される事例も増えています。効果的な防御策を講じることができなければ、標的型サイバー攻撃やランサムウェアなどのサイバー攻撃により業務に深刻な支障をきたし、企業の評価を落とし、コンプライアンスやデータ保護の規制に違反してしまう可能性が高まります。クラウドセキュリティとは、クラウドベースの攻撃から企業を守るために導入する技術、プロセス、リソースを指していますが、多くの企業ではそれらが正しく運用されていません。

クラウド利用が拡大しても、安全を確保

企業がクラウドに移行する背景には、運用コストの削減、運用上の柔軟性の確保、遠隔地での業務やコラボレーションの必要性など多くの理由があり、それらは皆納得できるものです。新型コロナウイルスの感染拡大によってソーシャルディスタンスを確保することの重要性が指摘されたため、この2年間でクラウドを使って業務を行うことが常識となり、その中でもSalesforceは最もよく使われているクラウドサービスの1つになりました。

この傾向は今後も続くと思われます。米Gartner社が2020年4月に、CFOを対象に行った調査では、74%の企業が従業員の一定数が常にオフィス外で働いていると考えており、そのうち17%は、リモートで働く従業員は全体の少なくとも20%を占めるようになるだろうと予測していることがわかりました。[1]

そしてクラウドプラットフォームは、機密資料の共有や顧客およびパートナーとのコラボレーションなどのビジネス上重要な業務に利用されることが多くなっています。

クラウドが生産性や利便性を高めることに疑いの余地はありませんが、このような新しい働き方によって生じるセキュリティリスクを理解し、効果的に対応できている企業はあまりに少ないのが現状で、サイバー犯罪者は巧みにこれらの防御の隙を突いてきます。
Salesforce、Microsoft 365、Google WorkspaceなどのSaaS型サービスの利用が増加するにつれ、これらのサービスは攻撃者にとってこれまで以上に魅力的なターゲットになりつつあります。

たとえ攻撃者がクラウド上のデータを盗むことに関心がなかったとしても、クラウドサービスを「踏み台」にして社内外の他のシステムに侵入しようとすることは十分に考えられます。実際に、クラウドサービスを経由してフィッシングやランサムウェアによる攻撃が行われた例が確認されているのです。

本ドキュメントでは、Salesforceをはじめとするクラウドサービスを安全に利用するための4つの隠れた真実をウィズセキュアの専門家がご紹介します。

1. https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2

1. 制御のために可視性を高める

Salesforce のようなクラウドサービスにデータを移行する場合、完全な可視性と制御を維持する必要があります。保存しているデータの種類と、それらがどのように分類されているか、データの出所、アクセス可能なユーザー、データの行き先などを把握しておかなければなりません。データがEメールのような外部の未知または信頼できないソースから提供される場合は、有害なコンテンツや許可されないコンテンツが社内外のユーザーに届く前にブロックする機能が必要です。

また、EUのデータ保護規制であるGDPRや、支払いカードのセキュリティ基準であるPCI-DSSなど、事業を展開する地域や業界あるいはマーケットに適用される規制やコンプライアンス要件に違反していないことを確認しなければなりません。つまり機密データへのアクセスを監視して制御し、完全な監査証跡を保持しなければならないのです。また悪意のある内部関係者やデータへの不正アクセスを検知する能力も必要です。これは既知の脅威を探すだけでなく、活動や行動を監視することを意味します。

2. 自社の責任を理解し、セキュリティギャップを埋める

クラウドにおいてセキュリティギャップが生じる主な原因の1つは、サードパーティのクラウド上で、誰が、何を保護する責任があるのかについて、広く誤解があることです。クラウド事業者は認定書や証明書を表示して安全性を誇示していますが、通常クラウド事業者が保証するのは自社のプラットフォームのセキュリティだけです。それを知らないクラウド利用者の中には、クラウドのセキュリティについては何も心配する必要がないという間違った理解をしている人もいます。

Salesforceなどのクラウドサービスを利用する場合、セキュリティの「責任共有」という原則に同意することになります。クラウド事業者は、インフラとプラットフォームのレベルでシステムの安全性を確保する責任を負いますが、日常のセキュリティハイジーン（衛生状態）の維持、クラウド事業者が提供するクラウドセキュリティ制御の適切な設定と管理、そしてシステム上のデータの保護については、利用する企業の側が責任を負うのです。具体的な責任分担は契約によって異なる場合がありますが、ほとんどの場合はこれとほぼ同じです。

3. 複雑化するクラウドを適切に設定する

クラウドサービスやアプリケーションは複雑になりやすいため、設定ミスが起きたりアクセス制御に不備があったりした場合には、それがデータ侵害につながることがあります。またAPIと呼ばれるソフトウェアインターフェースを使うと、クラウドプラットフォームに接続された他のアプリケーションやサービスからもデータにアクセスすることができるため、これらのAPIが誤って設定されたり、必要以上の権限を付与されたりした場合にも、データ侵害のリスクがあります。

Salesforceのシステム管理者は、新機能の追加やプラットフォームの高度な機能の利用、そしてSalesforce AppExchange からのサードパーティ製アプリケーション・サービスやアドオンの導入などの要望が絶え間なく寄せられるため、このような問題に直面することが特に多くなります。クラウドでの脅威検出やCSPM（Cloud Security Posture Management：クラウドセキュリティ体制管理）などのツールを導入して、危険な設定やコンプライアンス違反の可能性がある設定を自動的に識別することで、複雑さを軽減することができます。

4. サプライチェーン攻撃の緩和

クラウドプラットフォームやサービスの設定が適切に行われている場合でも、サードパーティーとの統合やAPI経由で接続されるアプリケーションにはリスクが存在することがあります。そのため、ソフトウェアに潜む脆弱性や設定ミスによって自社のクラウドに接続されたシステムが危険にさらされる可能性を想定しておく必要があります。また、攻撃者はサードパーティシステムを運用している組織を侵害し、横展開の手法で侵入することもあります。これは「サプライチェーン攻撃」と呼ばれます。

例えば2019年から20年にかけて、広く使われているネットワーク管理システム「SolarWinds」のバックドアが侵害され、攻撃者が複数の米国政府機関のシステムに侵入する事件がありました。
さらに最近では、Javaのロギングフレームワークであるlog4jの脆弱性により、企業のクラウド環境の93%が攻撃のリスクにさらされたと考えられています（出典：Wiz/EY）。多くのシステムにパッチが適用されましたが、Log4jは非常に広く使われており、特定のJavaコンポーネントを必要とする（「依存関係」にある）他のパッケージによって知らぬ間にインストールされていることも多いため、もうしばらくの間、この脆弱性がもたらす影響に注意する必要があると思われます。

自社のSalesforceクラウド環境と、パートナーや顧客またはサードパーティのシステムが統合されており、それら外部のシステムがLog4jのような脆弱性によって知らないうちに侵害された場合、攻撃者はその統合を使って企業内に侵入する可能性があります。企業は、既知のマルウェアによる脅威と、未知の脅威を示す異常なアクティビティの両方を監視することが非常に重要です。

Salesforce のセキュリティを強化する必要があるのは、どのような企業なのか?

WithSecure™ Cloud Protection for Salesforce[2] は、Salesforce環境にアップロードされるすべてのコンテンツをスキャンし、ウイルスやトロイの木馬、あるいはランサムウェアなどから企業をリアルタイムに保護します。Salesforceプラットフォームに組み込まれたセキュリティ制御を補完し、Salesforceを介して保存または共有されるあらゆるデータを保護することで、クラウドセキュリティにおける責任を確実に果たすことができます。

このソリューションにより、悪意のあるファイルやフィッシングリンクを介した攻撃を阻止または中断させる機能が提供されます。また、社内外のユーザーがアクセスしたすべてのコンテンツの詳細などの完全な可視性と分析も提供します。

Salesforceを利用している企業では、WithSecure™ Cloud Protection for Salesforceのような追加の防御機能をSalesforceプラットフォームに導入する必要性が高まっています。次頁以降では、3つの典型的なユースケースをご紹介します。

2. https://www.withsecure.com/jp-ja/solutions/software-and-services/cloud-protection-for-salesforce

ユースケース 1:
意識の高い管理者

クラウドシステムやサービスの利用が増えるにつれ、Salesforce プラットフォームを完全に保護する必要があると考えるシステム管理者が増えています。彼らはランサムウェアやデータ漏洩などのクラウドにおける脅威が拡大していることを認識しており、セキュリティに対する責任共有モデルについても理解しています。しかし、その責任を果たすためにどのようなサードパーティツールが利用できるのかについては、十分には認識できていない場合はどうしたら良いでしょうか?
セキュリティ意識の高いシステム管理者は、セキュリティや Salesforce[3] 環境をサイバー攻撃から保護するための方策について調査するでしょう。AppExchangeでどのようなセキュリティ アプリケーションが利用可能かを検索すれば、すぐに WithSecure™ Cloud Protection for Salesforceのようなソリューションを見つけることができます。そうすれば、ウィズセキュアのソリューションがSalesforceのセキュリティのギャップをどのように埋めることができるのかもわかります。そしてその投資に関する堅実なビジネスケースを構築した上で、調達の準備を行い導入を申請するのです。

3. https://help.salesforce.com/s/articleView?id=000318378&type=1

ユースケース 2:
ポータルサイト管理者

多くの企業が、Salesforceの利用を拡大してパートナーや顧客と連携するために、Experience Cloud（旧Community Cloud）を使っています。しかし、その企業のポータルサイトに接続しているサードパーティのシステムやデバイスなどのエンドポイントで、十分なセキュリティが確保されているとは限りません。外部のユーザーがドキュメントやフォーム、あるいはリンクなどのコンテンツをSalesforceにアップロードすることを許可している場合には、これらの潜在的に危険なエンドポイントがマルウェアやフィッシングリンクなどの脅威を持ち込んでいないことを確認しなければなりません。また、システムだけでなく企業の評判が損なわれる可能性があることにも注意が必要です。さらには、パートナーや顧客がダウンロードした「何か」が通り抜けてくるような事態も避けなければなりません。金融機関、人材紹介会社、旅行代理店、その他の専門的なサービス業では、ポータルサイトがビジネスの中核となる場合が多いため、システムを停止させるわけには行きません。

ユースケース 3:
コンプライアンス責任者

大企業、あるいは医療、金融、政府機関などの規制の厳しい分野の企業には、準拠すべき厳格なコンプライアンス規制が存在することがあります。これにはデータ保護やプライバシーに関する法律や規制が含まれる場合もあれば、ISO 27001セキュリティ規格などの、ベストプラクティスに従った単なる内部コンプライアンスのための手順である場合もあります。CISOやCIO、あるいはCEOといった上級管理職は、明確な目標を定めてクラウドプラットフォームやアプリケーション、およびサービスが企業の包括的なデータセキュリティポリシーに完全に準拠していることを確認しなければなりません。
そのため管理者は、Salesforce環境を適切に保護するためには追加のツールが必要なことを認識することになります。これには、ウィズセキュアのCloud Protectionなどのソリューションによるコンテンツセキュリティの実装も含まれますが、ビジネス全体のコンプライアンスを確保するためのCSPM（Cloud Security Posture Management）ソリューションが必要になる場合もあります。

WithSecure™ について

WithSecure™は、ITサービスプロバイダー、MSSP、ユーザー企業、大手金融機関、メーカー、通信テクノロジープロバイダー数千社から、業務を保護し成果を出すサイバーセキュリティパートナーとして大きな信頼を勝ち取っています。私たちはAIを活用した保護機能によりエンドポイントやクラウドコラボレーションを保護し、インテリジェントな検知と対応によりプロアクティブに脅威を探し出し、当社のセキュリティエキスパートが現実世界のサイバー攻撃に立ち向かっています。当社のコンサルタントは、テクノロジーに挑戦する企業とパートナーシップを結び、経験と実績に基づくセキュリティアドバイスを通じてレジリエンスを構築します。当社は30年以上に渡ってビジネス目標を達成するためのテクノロジーを構築してきた経験を活かし、柔軟な商業モデルを通じてパートナーとともに成長するポートフォリオを構築しています。

1988年に設立されたWithSecure™は本社をフィンランド・ヘルシンキに、日本法人であるウィズセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。

ウィズセキュア株式会社
〒105-0004 東京都港区新橋2丁目2番9号 KDX新橋ビル2階
Tel: 03-4578-7710 / E-mail : japan@f-secure.co.jp
https://www.withsecure.com/
2022/04

WITH secure