2023年のSalesforce セキュリティ保護

その脅威と課題を解明する

WITH secure

はじめに

2022年もサイバーセキュリティにとって激動の年になっています。

Lapsus$やContiなどの狡猾な脅威グループが大手企業や国家のインフラに大規模な攻撃を仕掛け混乱を招きました。また、知名度の低い犯罪集団でさえ、標的型ランサムウェアなどの手口で深刻な脅威をもたらしています。

ほとんどのサイバー攻撃は、従来のITシステムとエンドポイントを経由して実行されます。しかし、多くの企業がインフラと運用をクラウドに移行していくと、サイバー犯罪者はすぐに応じてSalesforceのようなクラウドベースの環境に狙いを定めるようになりました。

15万社以上の企業が重要な顧客関係管理（CRM）業務をSalesforceプラットフォームに依存しており、そこには貴重で機密性の高い顧客データが大量に保存されています。また、Salesforceは高度なコラボレーションとカスタマイズが可能で、膨大な数のサードパーティ製プラグインと接続オプションをサポートしています。

これらの要素が相まって、Salesforceは脅威アクターにとって魅力的な標的になっているのです。まだ重大な事件は報告されていませんが、それは可能性の問題ではなく時間の問題だと考えられます。

Salesforceは極めてセキュアなプラットフォームで、お客様のデータを安全に保存できるように設計された非常に多くのセキュリティ制御機能を備えています。しかし、データを安全に保つためには、これらの機能の多くをお客様自身が適切に設定する必要があります。これが責任共有モデルの本質です。

このレポートでは、Salesforceを熟知したセキュリティエキスパート3名が、今後1年間でSalesforceのセキュリティで着目すべき点について知見を共有します。彼らの経験は、2022年のクラウドとSalesforceのセキュリティに関するWithSecure™市場調査*による最新データによって裏付けられています。

本稿では、この調査結果と共に、2023年にSalesforceのセキュリティで最優先される事項と、それらを先取りしてリスクを軽減するためにできることを解説します。

2022年の主なセキュリティトピック

- ITプロフェッショナルとSalesforceの管理者が抱えるセキュリティ上の最大の懸念
- 設定ミスや監視外の資産によりもたらされる脅威
- Salesforceにおける悪意のあるファイルやURLの増加
- 適切なセキュリティ制御機能の特定
- 2023年にSalesforceを保護するための推奨事項トップ8

*** WithSecure™市場調査：2022年4月から5月にかけて実施された12か国のIT意思決定者およびインフルエンサー3,072人に対するB2B市場調査。調査の対象国は、英国、フランス、ドイツ、ベルギー、オランダ、フィンランド、ノルウェー、スウェーデン、デンマーク、米国、カナダ、および日本。**

エキスパートの紹介

Dmitriy Viktorov

製品・技術責任者、クラウドプロテクション、WithSecure™

Dmitriyは、経験豊富な製品とセキュリティのプロです。お客様を支援して複雑な問題を解決し、クラウドとデジタルサービスを安全に保護することに情熱を注いでいます。これまでに研究開発、製品管理、および技術部門でさまざまな職務を歴任し、現在はCloud Protection for Salesforceの製品開発を主導しています。

Pankaj Paryani

Salesforceテクニカルリード、WithSecure™

Pankajは熟練したSalesforce開発者兼コンサルタントで、米国、英国、およびアジア太平洋地域の顧客向けに複数の開発プロジェクトに携わってきました。最近は、WithSecure™のCRM開発チームを統率して、お客様のニーズに合わせてSalesとServicesを安全に稼働させることに注力しています。

Doug Merrett

Salesforceセキュリティ、コンプライアンス、プライバシーおよびレジリエンス担当スペシャリスト、Platinum7

Dougは熱心なセキュリティ提唱者であり、プラットフォームとセキュリティのスペシャリストとしてSalesforce社で13年間勤務しました。その間、多くのお客様にSalesforceのセキュリティとインフラストラクチャに対するアプローチを理解していただき、Salesforceプラットフォームに保存されたデータのセキュリティを最大化する助言をしてきました。Dougは、2021年6月にSalesforceのセキュリティ、コンプライアンス、レジリエンスに特化したコンサルティング企業Platinum7を創設しました。

ITプロフェッショナルと Salesforceの管理者が抱える セキュリティ上の最大の懸念

セキュリティの課題トップ5

1. データ侵害の防止
2. マルウェアやウイルスからの確実な防御
3. フィッシングやビジネスメールの侵害など、高度なEメールベースの脅威の防止
4. *Office 365やSalesforceなどのクラウドベースのコラボレーションアプリケーションのセキュリティ確保
5. さらに多様化するデバイス、サービス、ソフトウェアプールのセキュリティ確保

*クラウドとコラボレーション

Salesforceなどのクラウドプラットフォームは、コロナ禍によって加速したリモートワークやハイブリッドワーク戦略を維持し、効率性やアジリティの向上、コストやリソースの削減といったメリットをもたらすために不可欠な存在となっています。しかし、クラウド環境では、ギャップや未確定要素が数多く発生し、その多くは直接制御することができません。

「何十年もの間、すべてがオンプレミスで直接制御されており、懸念すべき外部接続の数は限られていました。しかし、今ではすべてがクラウド上にあり、重要なシステムの多くが直接制御できなくなっています。」

Pankaj Paryani、Salesforceテクニカルリード、WithSecure™

過去18か月の間で、データセキュリティの管理で苦労した課題トップ3は何ですか？

(2020年Salesforceトップセキュリティトレンド報告書より)

*59%	サードパーティのセキュリティ管理
**53%	コンプライアンス/法令の遵守
49%	モバイルデバイスのセキュリティ
38%	リソースの制約
37%	脆弱性管理
28%	プロアクティブなハッキング対策
15%	監査
5%	ユーザーの行動

*サードパーティのセキュリティ管理

Salesforceは高度なカスタマイズが可能で、必要に応じて新機能を簡単に見つけて実装できるように設計されています。Salesforce AppExchangeだけでも 3,400を超えるアプリケーションがあり、数え切れないほどのサードパーティAPIやプラグインがオンラインで簡単に利用することができます。これは統合したり利用したりする点では優れていますが、サードパーティのサプライチェーンが広範囲に及ぶため、すぐに制御不能になる危険性があります。アドオンを実装するたびにサプライチェーン攻撃にさらされるリスクが高まります。ここ数年来、サイバーセキュリティの環境では、サプライチェーン攻撃が支配的になっており、Salesforceのセキュリティにとっても重大な懸念事項であることは驚くには当たりません。詳細はSalesforceのサードパーティ管理に関する当社の最新レポートをご覧ください。

**規制とコンプライアンス

規制の状況は進化し続けており、デジタル化とクラウド移行が加速する中で、セキュリティとプライバシーの規制に準拠する取り組みは一段と複雑化しています。さまざまな地域に特有の法律や規制当局があるため、企業はデータの転送先、保存先、そして処理される地域を正確に把握する必要があります。また、医療や金融などの業界固有の規制にも留意しなければなりません。

新しい規制が公布されたり、現行の規制が改正されるなど、今後も状況はさらに変化していきます。欧州委員会は、新しいNIS2指令（ネットワークおよび情報システム指令）を制定し、18か月以内に施行する予定です。

ITセキュリティに関する懸念事項トップ3は何ですか?

ランサムウェアとフィッシング

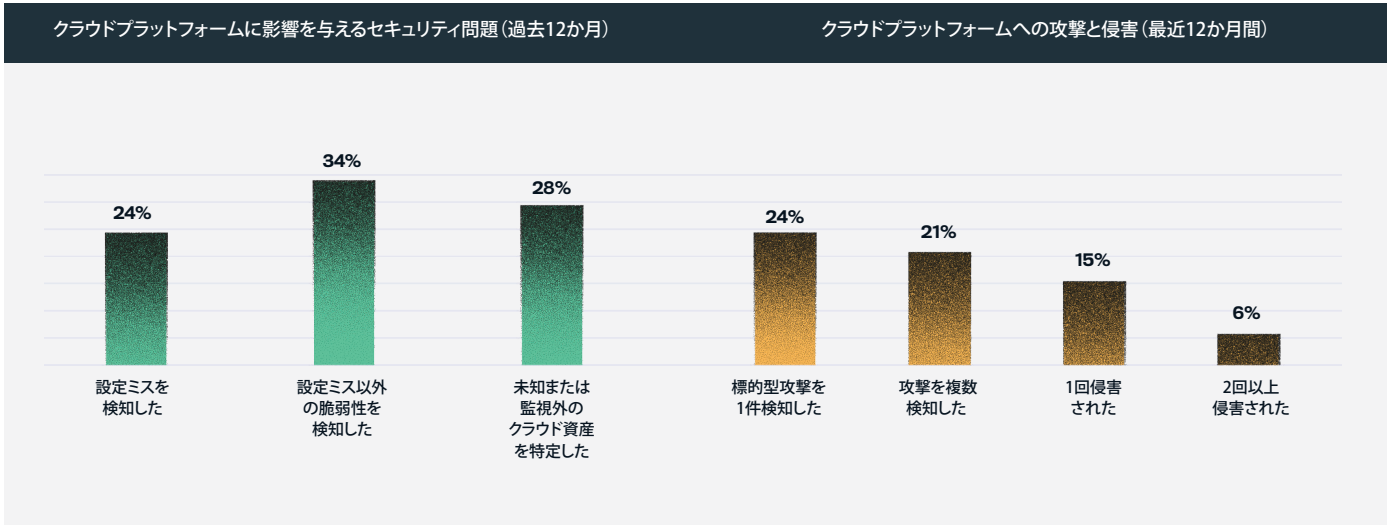
フィッシングは、従来からEメールを媒介とした脅威と考えられており、攻撃者はフィッシング攻撃にEメールを悪用し続けています。残念ながら、Salesforceはメールから案件、メールからChatter（チャター）など、さまざまなEメールベースのフローを提供しているため、当然ながらフィッシング攻撃と無縁ではありません。さらに、SalesforceはSlackやChatterといったサードパーティのオプションにより、コミュニケーションやコラボレーションチャネルを数多く提供しています。これらもフィッシング攻撃に悪用される可能性があります。

同様に、Salesforceの環境自体は、標準的なランサムウェアにとってかなりアクセスが困難になっていますが、悪意のあるファイルやリンクを標的のシステムへ送り込むために悪用される可能性があります。また、ランサムウェアやその他の悪意のあるプログラムは急速に進化していることにも留意すべきです。Salesforceの柔軟性の高いコミュニケーション機能は、こうした次世代型脅威に対してチャンスを与えてしまうことにもなります。

アクセスの可視性と制御

3名のエキスパートは、自らの経験に基づいて、ネットワーク接続の可視性と制御についても大きな懸念事項だと強調しています。社内外のユーザーが機密データやシステムにどのようにアクセスできるのか、またSalesforceプラットフォームが他のシステムとどのように接続し、連携しているのかをしっかりと把握していなければならないのです。

設定ミスや監視外の資産により もたらされる脅威



回答者の1/4が過去12か月間に標的型攻撃の被害に遭ったと考えているという事実は、攻撃者がより巧妙になり、組織化されてきたことを実証しています。しかし、多くの組織がクラウド環境の適切な設定と監視を怠っており、簡単な攻撃を許していることも確かです。

平均的なクラウド環境には膨大な選択肢が用意されているため、特に設定ミスが頻繁に発生します。私たちが遭遇するSalesforceの設定に関する問題で最も一般的なのは、アクセスに関するものです。ユーザーとアプリケーションの両方で、プラットフォームへの高度な特権アクセスを許可するデフォルトの権限が放置されていることがよくあります。これにより、外部のサイバー犯罪者と悪意のある内部関係者の両方によるリスクが大幅に増加するだけでなく、ヒューマンエラーの可能性も高まります。

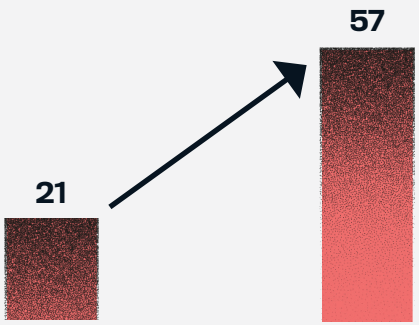
これに加えて、組織はシステムの追跡に苦慮していることが多々あります。SaaS（Software-as-a-Service）モデルでは、従業員が新しいアドオンやアプリケーションを簡単に購入して実装できてしまうため、IT部門は何も知らされない状態に陥ります。その結果、Salesforceは適切に検証されていない要素で溢れ返り、脆弱性や不審な行動を監視することが不可能になるのです。

「複雑化はセキュリティの敵です。環境が複雑になるほど何かが見落とされ、正しく設定されない可能性が高まります。高度にカスタマイズ可能なプラットフォームであるSalesforceには、設定ミスの機会が数多く存在しているのです。」

Dmitriy Viktorov、製品・技術責任者、クラウドプロテクション、WithSecure™

Salesforceに悪意のあるファイルやURLが増加中

1顧客の月当たりファイル/URL検知数



過去6か月間で悪意のあるファイルとURLの検知数が250%増加

検知した悪意のあるファイルタイプトップ5

1. HTMLファイル 49%
2. アーカイブRAR/ZIPファイル 23%
3. Microsoft Officeファイル 10%
4. Exe/comファイル 4%
5. PDFファイル 3%

*過去6か月間

マルウェアの種類 トップ5

1. トロイの木馬 54%
2. アドウェア 15%
3. エクスプロイト 12%
4. その他 12%
5. ダウンローダー 2%

*過去6か月間

攻撃の試行回数が着実に増加していることは広く認められており、この傾向は、Salesforce環境を監視して得られたWithSecure独自のデータによっても確かに裏付けられています。この6か月間に検知された悪意のあるファイルまたはURLは、1顧客あたり月平均57件になりました。これは、その前の6か月平均と比べて274%も増加しています。

悪意のあるHTMLファイルは、最も一般的な攻撃方法で、私たちが検知したファイルの半分以上を占めています。また、特定したマルウェアベースの攻撃の大部分は、トロイの木馬型マルウェアでした。

私たちは、サイバー犯罪者が特にSalesforceの資産を監視して攻撃していることを示していると思われるいくつかの傾向にも気付きました。たとえば、お客様がSalesforce Experience Cloudを実装し、コンテンツのアップロード用のポータルを作成すると、その直後に検知されるファイルやURLの数が急増します。

また、URLの数がファイルの数よりも多いことも注目すべきです。攻撃者は、ファイルスキャンを中心とした強力な防御戦略を持つ企業が増えていることを認識しています。そこで、より汎用性が高く検知が困難なURLの手口に乗り換えているのです。

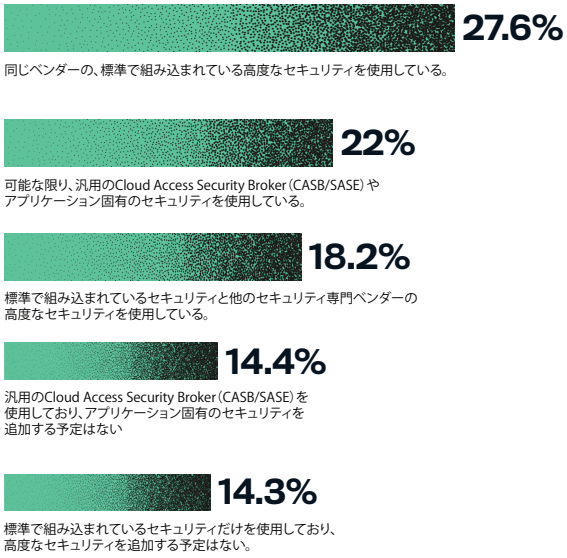
「悪意のあるファイルをスキャンすることは誰もが知っています。しかしURLのスキャンは、特にEメール以外ではまだ標準的に実施しているわけではありません。」

Doug Merrett、Salesforceセキュリティ、コンプライアンス、プライバシー、およびレジリエンス担当スペシャリスト、Platinum7

適切なセキュリティ制御機能を見つける

クラウドアプリケーションのセキュリティに関する以下の記述のうち、あなたの会社/組織に最も当てはまるものはどれですか?

(例:Office 365、Google Workspace、Salesforce)



調査の結果、クラウドのセキュリティ機能にはさまざまな形態があることがわかりました。ほとんどの回答者は、専門ベンダーのセキュリティアプリケーションを組み合わせて使用していますが、アプリケーションやプラットフォームに備わっているネイティブなセキュリティ機能だけに依存している回答者も多数いました。

これらの組み込みツールは出発点としては優れた選択と言えます。多くの場合、アプリケーションのベンダーによって構築されていることのメリットがあります。しかし、これらのツールを使うと、いくつかの重大なギャップが生じることも事実です。たとえば、Salesforceは非構造化データのセキュリティを提供しておらず、コンテンツのアップロード/ダウンロードをスキャンするためのネイティブ機能もありません。

したがって、利用しているSalesforceサービスのネイティブなセキュリティ機能に、専門ベンダーのセキュリティツールを少なくとも1つ組み合わせることでギャップを埋めるのが理想的です。また、企業は可能な限り単一ベンダーのソリューションで自社のすべての基盤をカバーするよう努めるべきです。複数のベンダーのソリューションを使用すると、複数の分断されたデータストリームや脅威アラートに対処しなければならず、管理が大変になる可能性があります。

プロキシとして機能するCloud Access Security Broker(CASB/SASE)を選択する場合は、各SaaS製品固有の設定をすることになるため実装が困難になります。さらに非常に脆弱になる可能性もあります。APIベースのCASBやネイティブに統合されたソリューションは、より汎用的で使用しやすいことがわかります。

「組込みのベンダーツールは、すべてをカバーできるわけではありませんが、その開発者がシステムを熟知しているため非常に効果的に機能します。その上に別の専門ツールを組み合わせると、バランスが取れてギャップを埋めることができます。」

Pankaj Paryani、Salesforceテクニカルリード、WithSecure™

2023年にSalesforceを保護するための推奨事項トップ8

2022年の重要な調査データを見直すことで、今後1年間におけるセキュリティの最優先事項が明らかになります。3名のエキスパートが推奨する、2023年以降に注力すべき事項は以下のとおりです。

1. IDとアクセスを管理する

システムアクセスの管理に注力すれば、最も確実で手っ取り早く成功が得られます。多要素認証（MFA）は、侵害リスクを直ちに大きく削減することができます。今ではSalesforceに標準搭載されたことで、追加コストなしで迅速に導入できるようになりました。

これに加えて、ユーザーとAPI統合の両方のシステムアクセスに最小特権アプローチを実装すると、攻撃対象領域が大幅に縮小します。これは時間のかかるプロセスですが極めて重要です。

2. Salesforceを襲う脅威を監視する

脅威アクターは、攻撃のツールボックスをEメール以外にも拡張しています。Salesforceのコンテンツアップロード機能や、Chatterなどの組み込みコミュニケーションチャネルは、マルウェアやフィッシング攻撃に悪用される可能性があります。しかし、このプラットフォームには、ネイティブのコンテンツ監視機能がありません。WithSecure™ Cloud Protection for Salesforceは、Salesforceと連携して、送受信されるすべてのコンテンツをリアルタイムでスキャンして、悪意のあるファイルやURLを特定してブロックするように設計されています。

3. プライバシーとコンプライアンス規制を遵守する

規制の状況は変化し続けており、Salesforceの環境には非常に多くの不確定要素があることから、コンプライアンス遵守の追跡は複雑な作業になります。デフォルトで最小限のアクセスしかできないようにする厳密な最小特権アプローチを取れば、コンプライアンスを確保するのに大いに役立ちます。サードパーティにまで及ぶ規制については、関係と責任をカバーするために厳格な審査を実施すべきです。

4. 組み込みツールを無駄にしない

Salesforceには、非常に便利なツールが標準で多数組み込まれているので、サードパーティのソリューションに投資する前に、それらを最大限に活用しましょう。Health CheckとOptimizerは、設定ミスやアクセス制御不能の状況を迅速に明らかにできるツールです。

「Salesforceは、自社のインフラストラクチャの安全性確保に努めていますが、ユーザーは、自らのインスタンスを安全に保つ責任を認識しなければなりません。Salesforceが標的にされない日は限りなくゼロに近いので、無駄にする時間はありません。」

Doug Merrett、Salesforceセキュリティ、コンプライアンス、プライバシー、およびレジリエンス担当スペシャリスト、Platinum7

「効果的なユーザー監視が必須になります。脅威アクターや悪意のある内部関係者だけでなく、事故や設定ミスの発見にも役立ちます。」

Doug Merrett、Salesforceセキュリティ、コンプライアンス、プライバシー、およびレジリエンス担当スペシャリスト、Platinum7

5. バックアップをさらにバックアップする

信頼性の高いバックアップは、レジリエンスを向上させるための最も貴重なリソースの1つです。Salesforceインスタンスを復旧できれば、CRMデータを損傷したり破壊しようとしたりするランサムウェアなどの攻撃による被害が大幅に軽減されます。またバックアップは、ヒューマンエラーから保護するためのもう1つのレイヤーを提供し、設定ミスやアプリケーションの統合失敗によって問題が発生したときにリセットすることができます。

6. デューデリジェンス（企業調査）を実施する

Salesforce環境が拡大し続ける中、デューデリジェンスを徹底することの重要性がこれまでになく高まっています。新しいサードパーティ製アプリケーションまたはプラグインを実装する場合は、必ずベンダーを調査し、信頼できるかどうかを確認してください。コミュニティはAppExchangeストアに正確なレビューを残すことに長けているので、それらを確認することから始めるのが良いでしょう。レビューは更新されるので時折確認するようにしましょう。

7. イベント監視を有効にする

イベント監視は、Salesforce環境内で何が起こっているかを把握するために不可欠です。これにより、ユーザーやアプリケーションが重要データにどのようにアクセスし、やり取りしているかを確認することができます。この可視性は、悪意のあるものや偶発的なものを問わず、外部からの攻撃と社内からのリスクの両方からSalesforceプラットフォームを保護するために欠かすことができません。

こういったフォレンジックデータは、適切に取り込まれ、理解されて初めて役立つため、SplunkやImprivata FairWarningなどのツールは、状況を確実に把握するために有効な手段になります。

8. 機密データを保護する

ビジネスデータは貴重であり、すべてのビットとバイトは保護する価値があります。しかし、特に顧客データと機密データには細心の注意を払う必要が有ります。Salesforce Shieldまたはその他のサードパーティのソリューションを使用して、機密データの検索、暗号化、監視、保持を実行してください。

出典

WithSecure™ 2022年B2B市場調査は、2022年5月に12か国3,072人の回答者を対象にオンライン調査を実施しました。調査対象国は、英国、フランス、ドイツ、ベルギー、オランダ、デンマーク、フィンランド、ノルウェー、スウェーデンの欧州9か国と、北米（米国、カナダ）、および日本の計12か国です。回答者は全員、IT/ネットワーク/クラウドセキュリティの意思決定者であり、組織におけるIT/ネットワーク/クラウドセキュリティ製品とサービスの購入に影響力を持つ方々です。

WithSecure™は、保護されたSalesforce環境から受け取った脅威分析リクエストの匿名化された社内データから、悪意のあるファイルとURLの検出数と傾向を収集しました。

2022年におけるSalesforceのトップデータトレンド - SalesforceとPulseが実施した300人のInfoSecおよびITエグゼクティブを対象とした調査に基づく。

「Salesforceは、新たな機能を組み込むことで、フィッシングなどの脅威への対応を継続的に改善しています。しかし、これらのツールを適切に導入し、活用するのはユーザー自身の役割です。」

Pankaj Paryani、Salesforceテクニカルリード、WithSecure™

「過去2年間で、サプライチェーンへの攻撃は深刻な問題になりました。そして今後1年間も継続することは間違いないでしょう。組織は、拡張されたデジタル環境を理解し、その安全確保を最優先する必要があります。」

Dmitriy Viktorov、製品・技術責任者、クラウドプロテクション、WithSecure™

WithSecure™ Cloud Protection for Salesforceは、アップロードされたファイルやURLのリスクを軽減することで、Salesforceのネイティブなセキュリティ機能を補完します。

ご連絡ください

salesforce PARTNER SINCE 2016

WithSecure™について

WithSecure™（旧名称：F-Secure）は信頼できるサイバーセキュリティパートナーです。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の業務を、成果ベースのソリューションによって保護し、大きな信頼を勝ち取っています。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、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、伝統的な企業からスタートアップ企業に至る幅広い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。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生かし、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™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@withsecure.com
https://www.withsecure.com/jp-ja/home

WITH secure