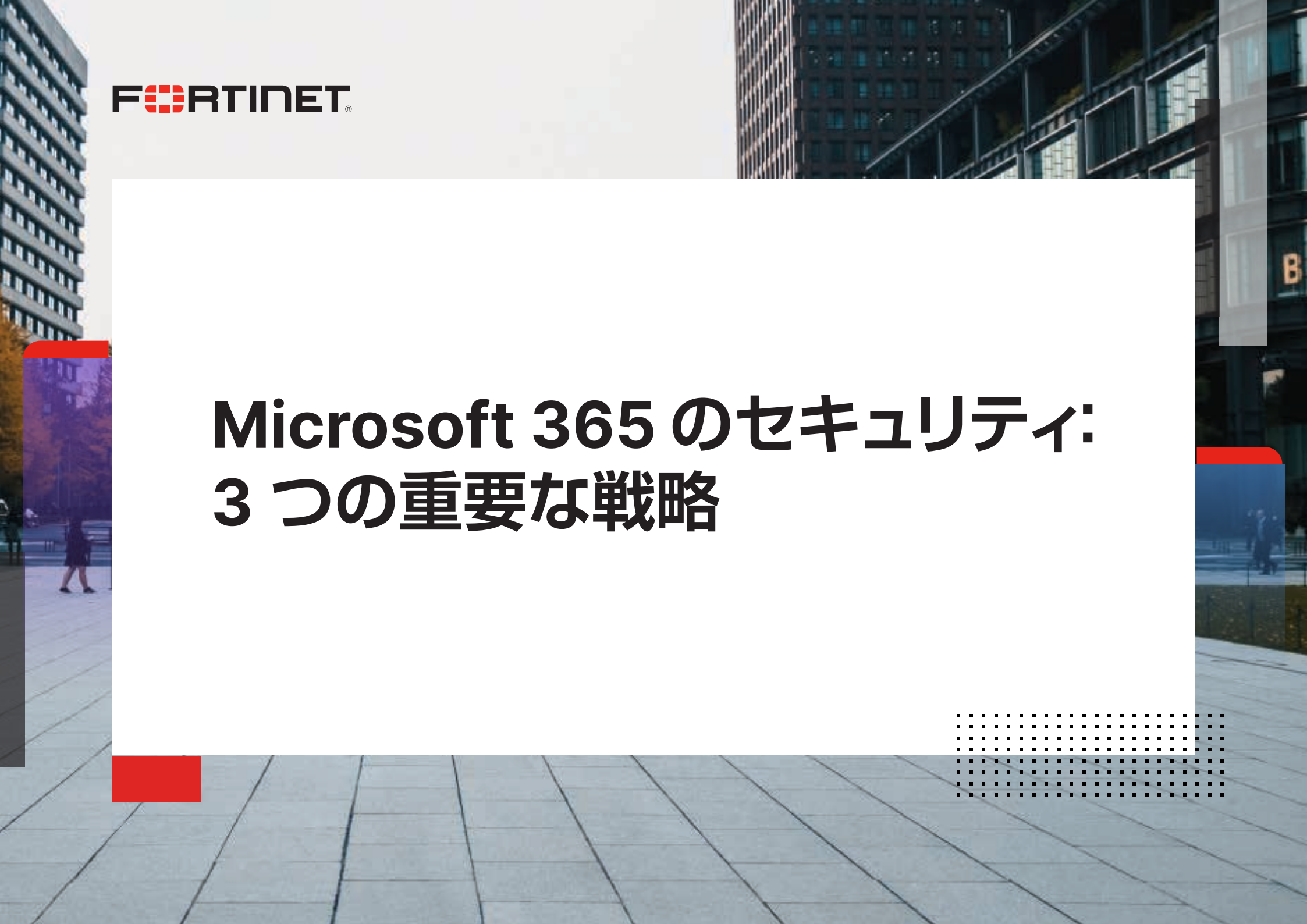

Microsoft 365 のセキュリティ: 3 つの重要な戦略

目次

概要

2 億 5,800 万人以上の有料ユーザーが利用する Microsoft 365 は、顧客とユーザーのサブスクリプション数で Google Workspace を大きくリードし、市場シェアを拡大しています [1]。クラウドベースのオフィススイートでは、E メール、OneDrive ストレージ、スプレッドシート、プレゼンテーションファイルなど、膨大な量の企業データが送受信されています。そのため、ビルトインのセキュリティツールだけでは十分に保護することはできません。Microsoft 365 を導入する場合、以下の点に注意してください。

Microsoft 365 でフィッシング、マルウェア、なりすまし、ビジネスメール詐欺（BEC）などの E メールを悪用した脅威から組織を効果的に保護できますか？

SE Labs によると、Microsoft 365 は Defender を有効にしても、E メールによるスパムやフィッシング、マルウェアの検出精度の総合評価は 30% 未満です。E メールは現在でも攻撃ベクトルの上位を占めているため、マイクロソフトの E メールセキュリティだけで組織のニーズに十分対応できるか検討する必要があります [2]。

Microsoft 365 へのアクセスを管理していますか？また、セキュリティポリシーに準拠したデバイスを使用していますか？

Microsoft 365 を導入する場合、アクセス制御とエンドポイント保護は不可欠です。これまで特権ユーザーはログインするとネットワーク全体で信頼されてきましたが、現在では認証情報の窃取はデータ損失の主な原因となっています。単純なユーザー名とパスワードによる認証だけでは不十分です。

Microsoft 365 で機密データを使用しますか？また、どのようなユーザーがその情報にアクセスしていますか？

データ損失防止は Microsoft 365 を保護する上で重要な機能です。他の多くのクラウドソリューションと同様に、Microsoft 365 のデフォルト設定ではファイルやその他のデータを内部と外部で無制限に共有できます。そのため、データの損失を防ぐには戦略的なアプローチが必要です。

この eBook はこれらの疑問に答え、Microsoft 365 を利用する組織を保護するための重要な戦略について説明しています。

クラウドベースのオフィススイートがもたらす新たなリスク

Microsoft 365 はクラウドベースの強力なオフィスソリューションです。ただし、Microsoft 365 とクラウドベースのオフィスツールやコラボレーションツール、E メールインフラストラクチャなどのコンポーネントは組織にセキュリティリスクをもたらす可能性があります。

一般的なクラウドサービスと同様、Microsoft 365 の多くの顧客でもコストと容量を節約し、日常的なインフラストラクチャ管理にかかる時間を短縮するためにワークロードをクラウドに移行しています。そうすることにより、コストを大幅に削減し、コアビジネスの優先事項により多くの労力を費やすことができます。ただし、Microsoft 365 とクラウドベースのオフィスツール、E メールインフラストラクチャ、データストレージを使用することで、以下のようなサイバーリスクが発生する可能性があります。

- 特権ユーザーになりすましたサイバー犯罪者によるデータの窃取
- Microsoft 365 を使用した企業の内外での情報共有
- コンテンツ、マルウェア、リンクなどの E メールを悪用した脅威

Microsoft 365 の最も一般的な E3 ライセンスと機能を拡張した E5 ライセンスには多くの基本的なセキュリティ機能が組み込まれていますが、これらのセキュリティ機能を評価して、リスクを効果的に緩和し、組織全体のセキュリティとコンプライアンスのニーズに適合できるか判断する必要があります。

戦略 I：E メールセキュリティ

Microsoft 365 でフィッシング、マルウェア、なりすまし、ビジネスメール詐欺（BEC）などの E メールを悪用した脅威から組織を効果的に保護できますか？

ガートナー社によると、2020 年には 71% もの企業がクラウドまたはハイブリッドクラウドの E メールサービスを利用しています [3、4]。その一方で、E メールは現在も攻撃者にとって主要な攻撃ベクトルであり、組織に大きなリスクをもたらしています。ベライゾン社の『2021 年度データ漏洩 / 侵害調査報告書』によると、データ漏洩 / 侵害に占めるフィッシングの割合は前年の 25% から 36% へと大幅に増加しています。ソーシャルエンジニアリングのインシデントでは「詐称」やなりすましが急増し、前年の 15 倍になっています。ランサムウェアを使用した攻撃も 2 倍以上増加し、10% を占めています [5]。IT チームと IT セキュリティチームは既存の E メールセキュリティソリューションを見直し、その効果を検証する必要があります。

マイクロソフトは Microsoft 365 を強化するためにさまざまなセキュリティオプションを提供していますが、第三者機関によるテストでは、Microsoft 365 Exchange Online Protection（EOP）と Advanced Threat Protection（現在の Microsoft 365 Defender）のパフォーマンスは他のベンダーのソリューションより劣る結果となっています。実際、SE Labs のテストでは、Microsoft 365 のネイティブセキュリティツールの検出精度の総合評価は 29%（EOP）と 28%（Defender）で、Microsoft 365 は「C」と評価されています。それに対して、フォーティネットの検出精度の総合評価は 90% でした [6]。

概要				
製品	保護の検出精度	合法性の検出精度	検出精度の総合評価	検出精度の総合評価（%）
Fortinet FortiMail	2,525	640	3,165	90%
Google G Suite Business	825	535	1,360	39%
Microsoft Office 365	463	550	1,013	29%
Microsoft Office 365 Advanced Threat Protection	426	550	976	28%

図 1：Microsoft EOP と Defender の脅威検出の精度が他のすべてのベンダーより劣っていることを示す SE Labs のテスト

フォーティネットの推奨事項

Microsoft 365 ネイティブの E メールセキュリティツールをテストし、ツールで対応できない脆弱性、パフォーマンスの問題、潜在的なリスクを特定します。フォーティネットは企業の代わりに比較分析を行い、無料で E メールのリスク評価を提供しています。

戦略 II：アイデンティティ / アクセス管理

Microsoft 365 へのアクセスを管理していますか？また、セキュリティポリシーに準拠したデバイスを使用していますか？

サイバー犯罪者が正規ユーザーを装って環境にアクセスできるため、認証情報の窃取は現在も攻撃目的の上位になっています。実際、ベライゾン社の「2021 年度データ漏洩 / 侵害調査報告書』で調査した侵害の 58% は認証情報の窃取でした [7]。ソーシャルエンジニアリングの場合、この数値は 85% に上昇します [8]。そのため、ユーザー名とパスワードを使用したアイデンティティ / アクセス管理では、これらのリスクに十分に対応することはできず、多面的なアプローチが必要です。

プロセスとして、まず外部のクラウドと組織のディレクトリサービスを統合して、アクセスするユーザーに関する情報源を一元化する必要があります。また、可能であれば、強力な多要素認証（MFA）とアクティビティログの両方でユーザーの本人確認を行います。MFA では二要素（ソフトトークンやハードトークンなど）で確認します。アクティビティログでは機械学習を使用してユーザーの過去のログインを分析し、時刻やデータの種類などが通常とは異なるアクセスを検出します。

少なくとも、Microsoft 365 に含まれる基本的な二要素認証は使用してください。ただし、ネットワークと各クラウドでアイデンティティとアクセスを管理するには、さまざまな環境で機能する高度なアイデンティティ / アクセス管理ソリューションを使用し、MFA を強化（およびその操作を簡略化）する必要があります。IDaaS（サービスとしてのアイデンティティ / アクセス管理）を利用する組織が増えており、認証は最も重要な機能になっています。デバイス管理はアクセス管理のもうひとつの重要な機能です。機密データへのアクセスに使用するデバイスは最新かつ安全な状態を維持し、ポリシーに準拠している必要があります。

オンプレミス環境とクラウド環境の両方ですべてのシステムとアプリケーションのアイデンティティの認証と承認を安全かつ効果的に管理することは、セキュリティ侵害を最小化する上で不可欠です。

フォーティネットの推奨事項

強力な多要素認証とトークンのベストプラクティスに基づいて、適切なアイデンティティとアクセスの保護を導入します。

戦略 III：アプリケーションとデータのセキュリティ

Microsoft 365 で機密データを使用しますか？また、どのようなユーザーがその情報にアクセスしていますか？

Blissfully によると、中規模企業は平均 185 の SaaS（サービスとしてのソフトウェア）を利用し、過去 2 年間で SaaS に移行した組織は 58% に上ります。企業全体では平均 288 の SaaS アプリケーションを使用し、過去 2 年間で 60% の組織が SaaS に移行しています [9]。組織における SaaS アプリケーションの利用は動的であるため、単一のメカニズムによって複数のクラウドアプリケーションのデータを特定して保護することが重要です。そうすることにより、オンプレミスのデータ制御と統合して、ポリシーの一貫した適用とレポートの統合も可能になります。

最初は Microsoft 365 の Information Rights Management をセキュリティ / コンプライアンスセンターのデータ損失防止（DLP）ポリシーテンプレートやレポートと組み合わせて使用するとよいでしょう。そうすれば Microsoft 365 環境を保護できます。ただし、データは Microsoft スイートだけでなく、オンプレミスネットワークと他のクラウドにも存在します。すべてのデータを保護するには、データの場所とタイプを特定する必要があります。これは、データが対象となる標準や規制に準拠するためにも必要です。

そこで、CASB（クラウドアクセスセキュリティブローカー）を使用します。ガートナー社によると、「CASB では複数のクラウドサービスのポリシーとガバナンスを一元管理し、クラウドからクラウドへのアクセスを含め、企業の境界の内外のユーザーのアクティビティと機密データの詳細な可視化と制御が可能になります [10]」と述べています。

CASB（クラウドアクセスセキュリティブローカー）製品では SaaS アプリケーションを使用する社員、企業環境、およびデータに対する保護が提供されます。この保護は COVID-19 のパンデミック以降、ますます重要になっています。

さらに、効果的な CASB ソリューションには以下のような利点があります。

- **可視化：**SaaS アプリケーションの正規使用と不正使用を識別できます。
- **データセキュリティ：**データ中心のセキュリティポリシーをクラウドにまで拡張し、重要なデータと知的財産を保護できます。
- **脅威保護：**リスクのある活動とデータを特定して対応できます。
- **コンプライアンス：**企業のコンプライアンスポリシーに準拠して SaaS を使用できます。

CASB ソリューションを導入した企業にはそのほかにも、コラボレーションの改善、社員の生産性の向上、製品開発の加速、ビジネスの成長促進など、さまざまな利点があります [11]。これらの利点を得るためにも、Microsoft 365 を利用している組織は SaaS の使用とアプリケーションセキュリティの戦略の一環として、CASB ソリューションの導入を検討する必要があります。

フォーティネットの推奨事項

Microsoft 365 をはじめとする SaaS の使用を拡大している組織の重要なアプリケーションとデータのセキュリティリスクに対応するため、CASB サービスを導入します。

終わりに

Microsoft 365 の有料ユーザーは 2 億 5,800 万人を超え、いまや組織にとって Microsoft 365 ネイティブのセキュリティ機能の潜在的なリスクと制限を理解することは不可欠です [12]。標準の E3 ライセンスには多くの基本的なセキュリティ機能が、E5 ライセンスには拡張機能がそれぞれ含まれますが、フォーティネットなどのサードパーティの専門家による実績あるセキュリティコンポーネントの導入も検討する必要があります。

[1] 「Microsoft FY20 Third Quarter Earnings Conference Call - Michael Spencer, Satya Nadella, Amy Hood」、Microsoft、2020 年 4 月 29 日（英語）：https://www.microsoft.com/en-us/Investor/events/FY-2020/earnings-fy-2020-q3.aspx

[2] 「Email Security Services Protection」、SE Labs、2020 年 1 月～ 3 月（英語）：https://selabs.uk/reports/email-security-services-protection/

[3] 「Market Guide for Email Security」、Mark Harris、Peter Firstbrook、Ravisha Chugh 共著、Gartner、2020 年 9 月 8 日（英語）：https://www.gartner.com/en/documents/3989940/market-guide-for-email-security

[4] 「2020 Businesses@Work Report」、Okta、2020 年（英語）：https://www.okta.com/businesses-at-work/2020/

[5] 「2021 Data Breach Investigations Report」、Verizon、2021 年 5 月（英語）：https://www.verizon.com/business/resources/reports/dbir/

[6] 「Email Security Services Protection」、SE Labs、2020 年 1 月～ 3 月（英語）：https://selabs.uk/reports/email-security-services-protection/

[7] 「2021 Data Breach Investigations Report」、Verizon、2021 年 5 月（英語）：https://www.verizon.com/business/resources/reports/dbir/

[8] 同上

[9] 「The 3 Biggest SaaS Trends in 2020」、Blissfully、The Blissfully Report、2020 年 3 月 10 日（英語）：https://www.blissfully.com/saas-trends/2020-annual-report/

[10] 「Magic Quadrant for Cloud Access Security Brokers」、Craig Lawson、Steve Riley 共著、Gartner、2020 年 10 月 28 日（英語）：https://www.gartner.com/en/documents/3992205/magic-quadrant-for-cloud-access-security-brokers

[11] 「Cloud Adoption and Risk Report」、McAfee、2019 年 6 月（英語）：https://www.mcafee.com/enterprise/en-us/solutions/lp/cloud-adoption-risk.html

[12] 「Microsoft FY20 Third Quarter Earnings Conference Call - Michael Spencer, Satya Nadella, Amy Hood」、Microsoft、2020 年 4 月 29 日（英語）：https://www.microsoft.com/en-us/Investor/events/FY-2020/earnings-fy-2020-q3.aspx

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

EB-Microsoft-365-202108-R1