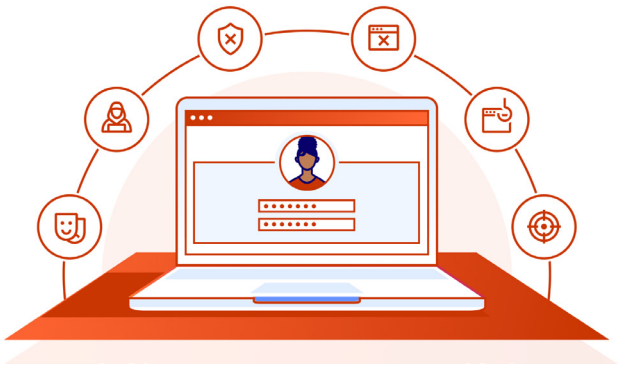
CLOUDFLARE

ソリューション概説

マルチチャネルフィッシングから従業員を守る

受信トレイを超えて機能する多層式保護



概要

もはやメールだけにとどまらなくなったフィッシング攻撃

フィッシングキャンペーンにとってメールが最もよく見られ被害につながりやすい方法であり続ける一方、攻撃者は、日常的に利用される複数のチャネル（コミュニケーションやコラボレーション用のアプリなど）を通じてユーザーを侵害する巧妙な戦略をますます使うようになっています。これらの攻撃ではしばしば、巧妙で判別しにくいリンクを用いてユーザーをだまし、悪意のあるコンテンツおよび安全ではない環境へと誘導させてきます。

チャネルの増加 = 従業員を侵害する危険性の高まり

標的とする従業員にメールおよびその他コラボレーションに用いるアプリで偽リンクを仕込むことで、攻撃者は従来の検出方法を回避しながら、より信頼性が高いと感じさせる方法でユーザーを誘導することができます。これにより、従業員による悪意あるWebコンテンツのクリック、認証情報の曝露、機密情報の漏えいリスクが高まります。メールセキュリティは、攻撃が受信トレイ経由で行われた場合にのみ役立つものであり、他のアプリにこうした攻撃が広がるのを防ぐには、より広範なセキュリティソリューションが必要になります。

課題

従来式のメールフィルタリングを通過し得るマルチチャネルの脅威

マルチチャネル攻撃では、リンクの複雑な難読化技術や各種コラボレーションアプリを悪用し、ユーザーに悪意のあるコンテンツをクリックさせたり機密情報を漏えいさせようとし向けてきます。この種の攻撃は、以下の理由から対処が困難な場合があります。

- **リンクの難読化**（URLリダイレクト/短縮化）
- **画像ベースのURL**（QRコード）
- **遅効性攻撃**（仕込まれた後に発動）
- **分散性のある挙動**が職務用アプリに渡って発動

89%

セキュリティ意思決定者のうち、マルチチャネルの脅威に懸念を持つ割合[1]

No. 1

悪意のあるリンクは、検出量ベースで最も顕著なフィッシング脅威[2]

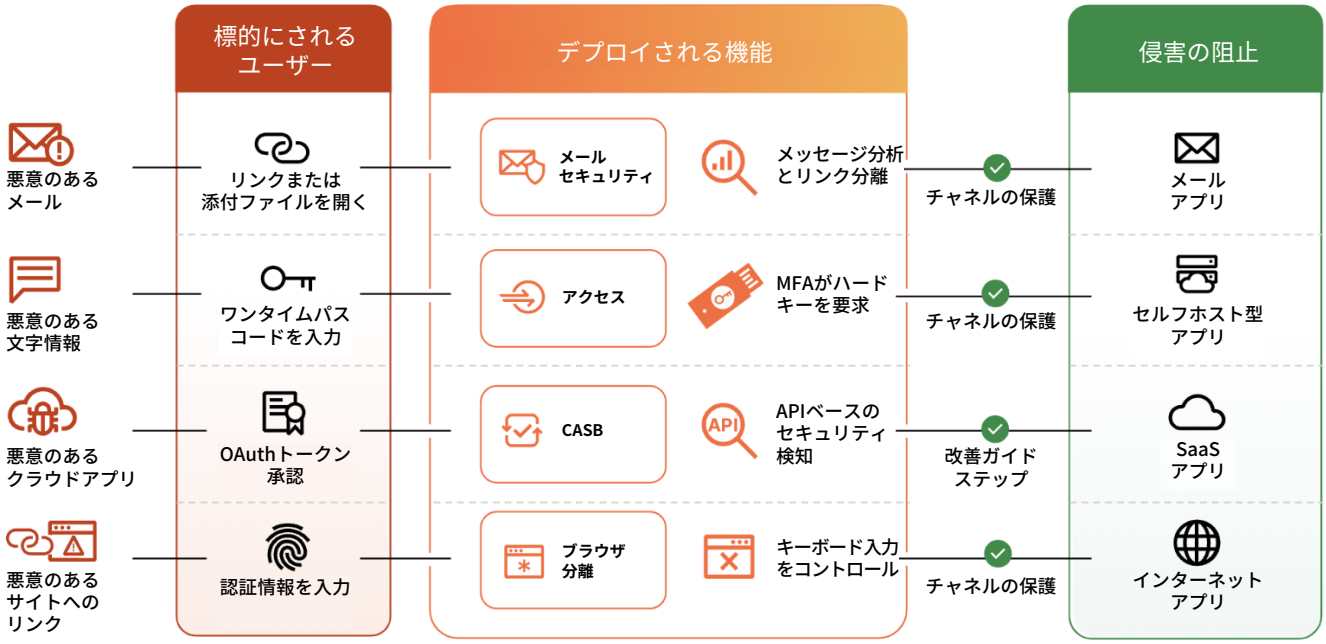
81%

過去12か月にマルチチャネル攻撃を経験した組織の割合[1]

ソリューション

フィッシングの脅威にさらされるあらゆるポイントでの統合型セキュリティ

マルチチャネル攻撃の阻止には、従業員の作業フローやアプリ内でのやり取りに存在する脆弱性の全容に対処できるプラットフォームが必要になります。このことから、Cloudflareでは、従業員とアプリケーション全体にわたるシームレスな保護を実現するための最も包括的なフィッシング対策を提供しています。Cloudflare Oneプラットフォームを活用することで、メール、自己ホスト型アプリ、SaaSアプリ、インターネットアプリのためのレイヤー型保護をデプロイできる、統合したメールセキュリティ（ES）およびZero Trustサービスのメリットを活用でき、不正決済やデータ漏洩などを食い止める多層防御を実現できます。



メールを媒介とする脅威を先制的に阻止

ビジネスメール詐欺（BEC）、マルウェア、その他メール由来の脅威をAI/ML搭載コンテンツ分析により検出し、自動保護します。

認証情報の盗難から発生する漏洩を防ぐ

認証情報が盗難または侵害された際の最終防衛ラインとしての、条件付きアクセスとハードキー要求で漏洩を阻止します。

侵害的リンクベースの攻撃をブロック・隔離

一般的に用いられるメッセージアプリを使った、判断しづらい巧妙に難読化したリンクを用いた標的型攻撃から従業員を保護します。

メール起因の脅威の防止（ES）

ビジネスアプリケーションの中で最も使用頻度が高い一方、悪用される頻度も最も多いのがメールです。メールを通してユーザーの信頼感につけ込み、隙を狙って繰り出されるフィッシング攻撃からユーザーを守ることは、これまで以上に重要になっています。現状のメール防御をCloudflareで強化または置き換えることにで、埋め込みメールリンク、添付ファイル、なりすまし、または侵害されたアカウントを使用して機密情報を盗み金銭詐欺を働く巧妙化したフィッシング攻撃を自動的に軽減することができます。

Cloudflareの軽量なクラウドネイティブなソリューションは数分でデプロイでき、MicrosoftおよびGoogleが提供するメール機能を補完することができます。Cloudflareでは、最適な結果を得るために必要な自動化を進め、設定を最小限にすることで、続行中のメールセキュリティ管理にかかる時間と手間を大幅に削減します。

ビジネスメール詐欺（BEC）
AI/MLを活用したコンテンツ分析があらゆるメッセージを分析し、会話履歴、文章のパターン、感情などの要素を分析して、送信者の正当性を判断します。

ランサムウェアおよび悪意のある添付ファイル
ペイロードに対する機械学習（ML）検出モデル、非署名の検出、コンピュータビジョン、リモート抽出、その他の分析手法を用いて、暗号化された悪意のあるペイロードと暗号化されていないものを特定します。

悪意のあるメールリンク
複雑なURLを分解し詳細に分析する高度な技術と、適応型リンク隔離を組み合わせることで、従業員にとって安全でストレスのないWeb体験を提供します。

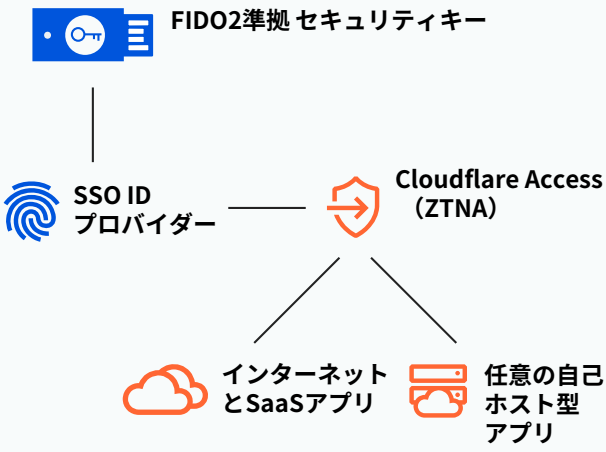
OAuthフィッシング攻撃を軽減（CASB）

OAuthフィッシングは、正規のIDプロバイダーと認証ワークフローを悪用し、ユーザーに悪意のあるアプリに許可を与えるよう仕向けます。Cloudflare Oneプラットフォームは、このようなアプリを検出する機能を提供すると同時に、これらの脅威を迅速に軽減するための改善ガイダンスを提供します。

認証情報の侵害を回避（ZTNA）

多くの組織が従業員の認証情報を悪意ある者の手に渡さないよう拡張的な防御策を講じていますが、予防措置が100%確実ということはありません。認証情報が盗まれてしまうまたは知らぬ間に漏洩してしまった場合、侵害を防ぐための最終防衛ラインが必要です。

Cloudflare Accessは、自己ホスト型または非Webリソースなどのあらゆるリソースにおける集約層として機能し、フィッシングに対抗するための二要素認証（MFA）のためにFIDO2準拠型認証を一貫して適用することができます。そのため、従業員の資格情報が侵害された場合でも、組織はデータを確実に保護することができます。



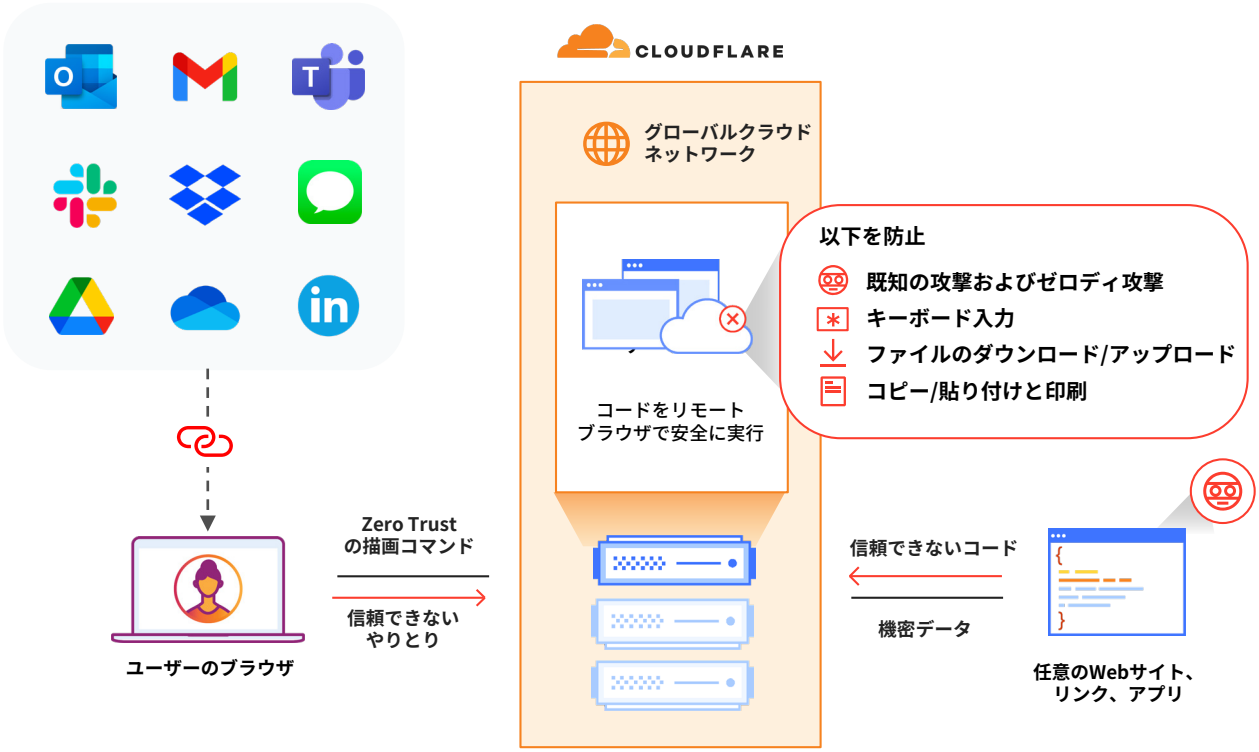
リンクベースの攻撃を隔離（ES + リモートブラウザ分離 + SWG）

リンク攻撃が、資格情報窃取、マルウェアやランサムウェアの仕込み、機密情報抽出の常套手段になっています。メール、チャット、SMS、ソーシャルアプリ、クラウドドライブを組み合わせてリンクを送る手口であるため、従業員とデータの両方を標的型フィッシング攻撃から保護するプロセスが一層複雑になっています。

Cloudflareのブラウザ分離は、すべてのWebコードをユーザーのローカルデバイスではなく弊社のグローバルクラウドネットワーク上でリモートでレンダリングすることにより、リンクを使ったフィッシング攻撃の問題を解決します。それによって、マルウェアやブラウザのゼロデー脆弱性の影響を軽減すると同時に、ユーザーアクションをきめ細かく制御（キーボード入力の無効化など）してクレデンシャルハーベスティングやデータ漏洩を防止します。

業務のスピードを落とさずフィッシングのリスクを排除

Cloudflareは、独自のネットワークベクトルレンダリング（NVR）技術を使った次世代のブラウザ分離機能を統合することにより、潜在的悪性リンクを分離するシームレスでセキュア、かつスケーラブルなソリューションを提供することができます。帯域幅を大量使用する手法と違い、NVRは安全な描画コマンドをデバイスにストリーミングします。それにより、エンドユーザーエクスペリエンスに影響を及ぼすことなく、悪性Webコンテンツのリスクを排除できます。NVRとCloudflareの低遅延ネットワークによって、マルチチャネルの脅威を分離し、支障のない業務遂行を可能にして従業員の生産性を維持することができます。



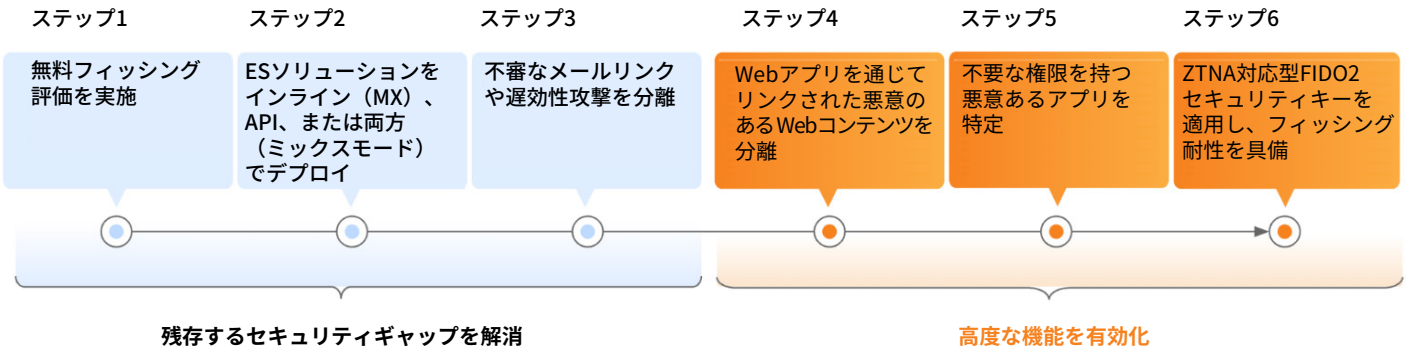
メリット

完全なマルチチャネル保護

フィッシング攻撃はメールだけでなく他にも急拡大しており、十分なマルチチャネル保護を迅速に、簡単に提供するフィッシング対策ソリューションの実装が急務となっています。

Cloudflare Oneプラットフォームでは、まず業界最先端のメールセキュリティをデプロイしてフィッシングの最重要チャネルを保護し、その後Zero Trustサービスを簡単に有効化して保護を全チャネルに拡大でき、既知や新規のフィッシング脅威を効果的に阻止できます。

- **少ない手間で高効率の保護：**
  最低限のチューニングで業界屈指の検出効果を発揮し、フィッシングのリスクを最小化します。
- **幅広い統合、低コスト：**
  あらゆるフィッシングのユースケースを解決する、完全統合型単一プラットフォームにより、費用を削減することができます。
- **すばやくデプロイ、簡単に管理：**
  継続的管理に必要な時間と労力を削減しつつ、即時の保護を確保します。



評価と比較

現在のメール防御を評価し、見逃されている脅威を確認しましょう

無料レトロスキャン（O365受信トレイ）を数分で実行し、過去14日間にすり抜けたフィッシングの脅威をご確認ください。また、あらゆる受信トレイに配信されたフィッシングを監視するためのフィッシングリスク評価（PRA）をご依頼いただくこともできます。設定不要を掲げるプロバイダー他社と比較し、どのメールセキュリティソリューションの保護が最も速く、最も簡単かご覧いただけます。

貴社の防御態勢をすり抜けている
フィッシングの脅威をご覧ください

レトロスキャンを実行　PRAをリクエスト

CLOUDFLARE

1. 2023年 Forrester Opportunity Snapshot: 出典
2. 2023年フィッシング脅威レポート出典