CLOUDFLARE

製品概要

Cloudflare Email Security

セキュアなワークスペースコミュニケーションを
実現する自律的なマルチチャネル保護

標的型フィッシング攻撃から保護

他のソリューションが見逃す脅威を楽々とブロックして分離

ビジネスアプリケーションの中で最も使用頻度が高く、悪用される頻度も高いのがメールです。ユーザーの信頼に付け込もうとするフィッシング攻撃からユーザーを守ることが、これまで以上に重要になっています。ハイブリッド環境で働く従業員のサポートを強化するためにMicrosoft 365やGoogle Workspaceといったクラウド型メールサービスを導入する企業が増えるに従って、脅威アクターは、ProofpointやMimecastなどの従来型のセキュアメールゲートウェイ（SEG）を回避できる、より対象を絞った低ボリューム攻撃を仕掛けるようになってきました。

そこで、Cloudflareが提供するクラウドネイティブのメールセキュリティソリューションは、先制型の攻撃インテリジェンス、MLベースのコンテキスト分析、統合型のゼロトラストプラットフォームによってフィッシングの脅威が従業員に達する前に阻止するユニークな設計になっています。

91%

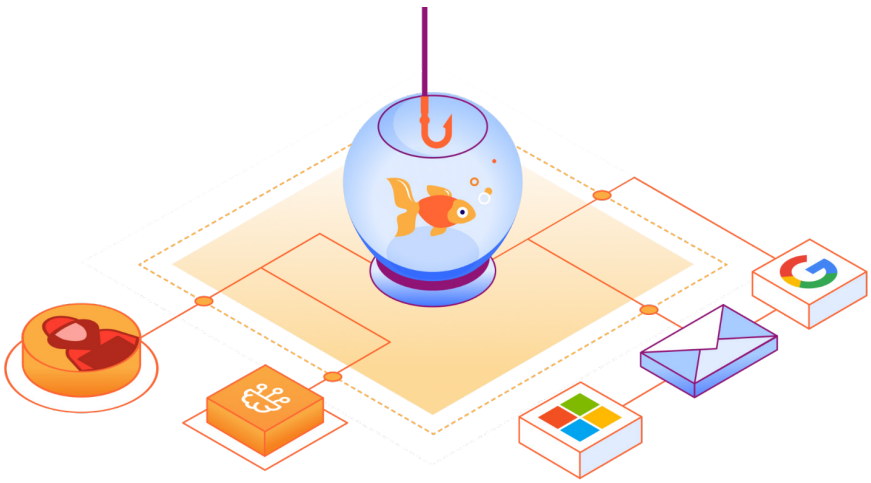
フィッシングメールを発端とするサイバー攻撃の割合[1]

500億ドル

ビジネスメール詐欺による過去10年の損失額[2]

81%

過去12か月でマルチチャネル攻撃を受けた組織の割合[3]



ビジネスメール詐欺（BEC）を阻止

MLを活用した階層的コンテキスト分析により、なりすましアカウントや侵害されたアカウントを検出。

遅効性のマルチチャネル攻撃を分離

未知のリンクや難読化されたリンクを通して配信される悪性Webコンテンツからユーザーを隔離。

ランサムウェアと悪意のある添付ファイルをブロック

企業を危険にさらす脅迫行為や悪意のあるコードから企業を保護。

保護強化と簡素化

わずかな費用で優れた保護が可能な階層型セキュリティを実装

フィッシング攻撃は増え続け、MicrosoftとGoogleでは、重要メールとデータの保護を可能にするネイティブ機能の拡張（認証、アーカイブ、クライアントサイド暗号化など）を続けてきました。しかし、攻撃者の手口も、ネイティブのセキュリティ対策をバイパスして成功率を上げる標的型回避攻撃へと進化しています。

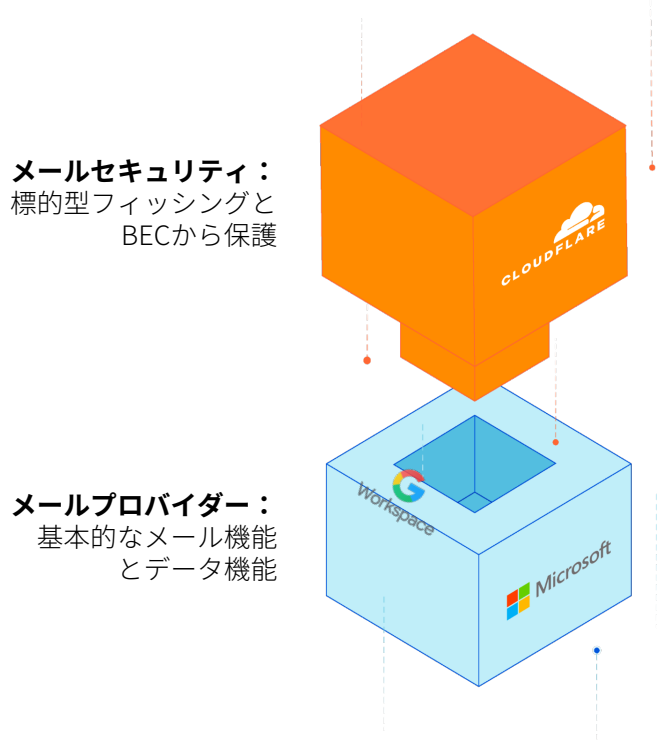
Cloudflareを重ねることにより、悪性リンク、添付ファイル、侵害されたアカウントを利用して機密情報を盗んだり金融詐欺を働いたりする標的型フィッシング攻撃を、自動的にブロックまたは分離することができます。

既存のメールセキュリティコントロールを強化

Cloudflareのクラウドネイティブなメールセキュリティソリューションは数分でデプロイでき、既存のSEG環境の強化や、MicrosoftやGoogleが提供する内蔵型メール機能の補強が可能です。チューニングはほぼ不要で、継続的セキュリティ管理の時間と労力を減らしつつ、フィッシング対策を強化できます。

「（Microsoft 365を導入し）Cloudflareを実装して以来、ユーザーが日々受信する悪性メールや不審メールの数が50%減少しました。それにより多くの時間が解放され、他の目的に振り向けられるようになりました。」

Werner Enterprises
（フォーチュン1000）



自動化により節約した時間を再投入

Cloudflareの自動化された軽量ソリューションは、MicrosoftやGoogleのワークフローとシームレスに統合し、単一の直感的UIで分析も行えます。

99.997%の検出効率を達成

Cloudflareのフィッシング・BEC対策機能をメールプロバイダーのネイティブ機能と統合することで包括的なカバーを実現し、リスクを最小化します。

低コストでより大きな価値を実現

旧式で高コストの複雑なデプロイ環境をCloudflareのロータッチソリューションに置き換えることにより、運用のオーバーヘッドを削減し、機能の重複や過剰なチューニングを抑えられます。

最新のBEC攻撃を阻止

報告された損失は500億ドルに上り、依然増加中

過去10年にわたりBEC攻撃で膨大な損失が出ていることを考えると、この効果的な金融詐欺の手口に対する対策を最優先しない組織が未だにあることに驚かされます。BEC攻撃は、フィッシングの脅威全体に占める割合は小さいものの、SEGやクラウドメールプロバイダーで検出されずに大きな財務損失につながるケースが多く見られます。これらの標的型攻撃は、なりすましアカウントや侵害されたアカウント、会話のコンテキストを利用して従業員や信頼されたベンダーを装うため、検出が困難です。

ゼロトラストの原則をメールに適用

侵害された従業員やベンダーのメールアカウントを使った攻撃は、送信者アカウントの正当性のみを確認しようとする従来のセキュリティコントロールを掻い潜ります。Cloudflareはさらに一歩踏み込んで、書き方のパターン、感情インジケーター、会話履歴などさまざまな行動属性を分析して送信者の真正性を判別します。CloudflareのMLを活用した脅威モデルと広範なネットワークインテリジェンスが、侵害されたアカウントを利用した金銭詐取に対する最強の武器になります。

図1： メッセージ分析

MLベースのコンテキスト分析でBECを検出

ビジネスメール詐欺の正確な識別は、メッセージの構造分析だけではできません。検出精度を上げるには、会話スタイルや意図のバリエーションを詳細に理解することも必要です。Cloudflareでは、広範なネットワークテレメトリ（1日に3テラバイト強のDNSリクエスト）と進化するMLモデルを小規模パターン分析エンジンに活用し、メールメッセージのあらゆる側面を分解して、書き方のパターン、感情、時系列コンテキストなど、送信者の真正性を探るのに役立つ変数を幅広く評価します。

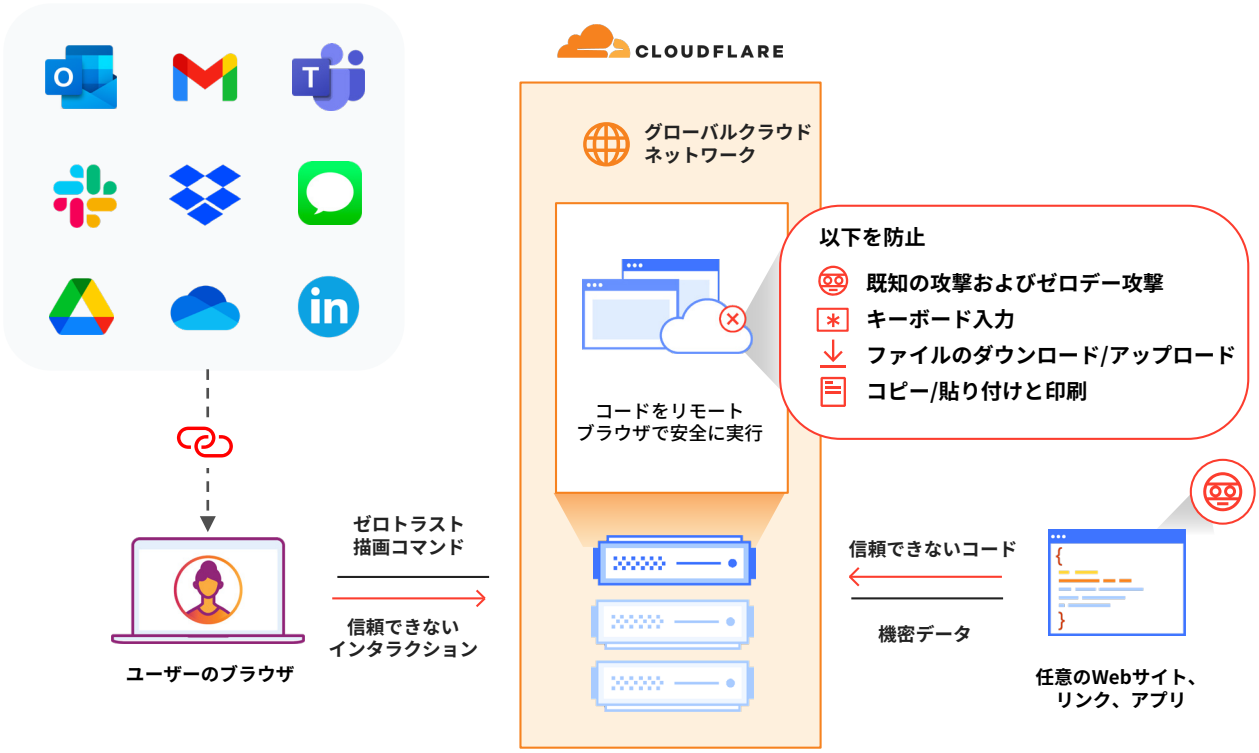
リンク攻撃を分離

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、ソーシャルアプリその他のアプリ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当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（キーボード入力の無効化など）をきめ細かく制御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。



迅速な調査と解決

直感的でロータッチのセキュリティ管理

Cloudflareは自動化を進め、最適な結果を得るのに必要な設定を最小限にすることにより、継続的なメールセキュリティ管理に要する時間と手間を大幅に削減します。セキュリティチームは、ダッシュボードで最上位のメトリクスとトレンドを一望できます。フラグの立ったメッセージに関しては、クリックして詳細情報を表示する機能も備わっています。トレンドを掘り下げることにより、頻度の高い攻撃タイプ、標的にされたエグゼクティブ、軽減された遅効性攻撃、その他の重要なデータポイントをすばやく検出できます。

アナリティクス、テレメトリ、脅威観測事象、侵害インジケーター（IOC）はすべて拡張API経由で取得でき、既存のアナリストワークフローやオーケストレーションツールに簡単に統合できるようになっています。

「CloudflareがクラウドベースのSaaSソリューションとしていかにシンプルで使いやすいか、その精度の高さにどれほど満足しているかということを同僚によく話しています」

日本航空

マネージド検出対応サービス（PhishGuard）

CloudflareのマネージドメールセキュリティサービスPhishGuardは、お客様の既存SOCチームを補完してセキュリティ調査のサイクルを解放し、貴重な脅威インテリジェンスを提供します。PhishGuardは、調査、内部脅威評価、アクティブな詐欺サイトのテイクダウン、複雑な修復ニーズの充足をアシストして、フィッシングキャンペーンの無害化に役立ちます。PhishGuardは、セキュリティリソースと専門知識を活かして潜在的な詐欺や内部脅威を通知する他、メールベースの脅威のハンティングも行います。

PhishGuardの機能とメリット：

- マネージド型のフィッシング報告とインシデント対応で解決を促進。
- BECや不正行為について予防的な通知を行い、攻撃ライフサイクル早期のすばやい対応を支援。
- リアルタイムモニタリング、定期的なアカウントレビュー、継続的な脅威評価のための専用リソース。
- マネージド環境の脅威分析をもとに、署名をカスタムブロック。

1100+

手動トリアージの自動化による年間節約時間

Cloudflareの自動化されたソリューションは時間のかかる手作業を排除して応答時間を短縮し、サイクルの解放を促進します。

50%減

悪性・不審メールの到達率（M365使用）

Microsoft 365にCloudflareを重ねることにより、標的型攻撃を検出し、悪意あるメールの総数を減らすことができます。。

40時間

7年間でメールセキュリティの設定に費やされた時間

Cloudflareのロータッチメールセキュリティは事前設定や継続的チューニングの必要がほとんどなく、導入後すぐに高検出率を実現します。

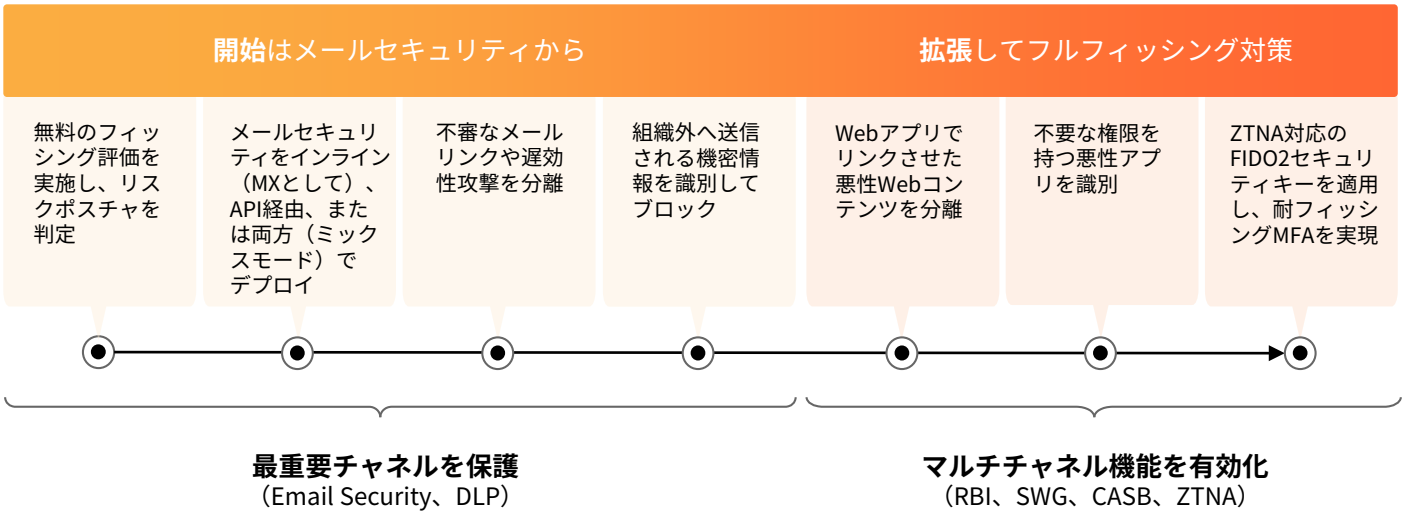
メリット

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かつ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の統合セキュリティ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、その後ゼロトラスト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することが可能です。

- **ロータッチで効果の高い保護：**
  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：**
  単一の完全統合プラットフォームですべてのフィッシング対策ユースケースに対応でき、支出を削減します。
- **すばやくデプロイ、簡単に管理：**
  即時保護を提供し、継続管理に必要な時間と労力を減らします。



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。受信トレイへのフィッシング配信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。チューニング不要を掲げるプロバイダー他社と比較して、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、最も簡単かをご確認ください。

レトロスキャンを実行　PRAをリクエスト

1. 2020年 Deloitte調査：出典
2. 2023年 FBI IC3 PSA：出典
3. 2023年 Forrester Opportunity Snapshot: 出典