CLOUDFLARE

ソリューション概説

Cloudflare + Microsoft 365 フィッシング対策

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

レガシーゲートウェイの使用を中止し、フィッシング対策をアップグレード

2000年代初頭、メールのルーティングとフィルタリングに関するニーズの高まりに対処するため、セキュアメールゲートウェイ（SEG）が導入されました。SEGは長年その使命を果たしてきましたが、その基本的設計では、範囲と高度を急速に増すフィッシングの脅威に対してペースを維持することがもはやできなくなりました。

オンプレミスのサーバー用に構築された手動のルールセットやポリシーを更新し続けることは、SEGの維持にかかる時間と労力を増大させるだけです。これにより、ビジネスメール詐欺（BEC）攻撃のような最も危険な脅威を捕捉するには至らないまま、コストと複雑さが増大する結果となりました。諸経費の増大と効果の低下の主な理由は次の通りです。

- **新たなフィッシングの手口とzero-dayの脅威** - 現代のフィッシング攻撃は、静的フィルタや従来の制御を回避するために設計され、ますます欺瞞的な手口を採用しています。そのため、SEGが侵害の既知の指標がまだない新しい脅威をブロックすることは困難です。
- **複雑なデプロイ** - SEGは、新たな脅威に適応するために広範な構成と継続的なチューニングを必要とする一方で、その機能を十分に活用するために複数のアドオンモジュールを必要とします。
- **時間のかかるインシデント対応** - 疑わしい、または悪意のあるアクティビティがデプロイされたSEG制御を迂回する場合、調査と対応のプロセスは、多くの場合、インターフェイスとワークフローのパッチワークを含む、長くて面倒なものになります。

高効率、ロータッチ保護をデプロイ

ハイブリッドワークフォースのコミュニケーションとコラボレーションを企業が強化するためにMicrosoft 365を採用し続ける中、Microsoftのネイティブセキュリティ機能を活用しつつ、最も危険な脅威を自動的にブロックし隔離するための補完的な機械学習ベースのソリューションを統合することが極めて重要です。この戦略は、フィッシングリスクの大幅な低減に加え、ワークフローの簡素化、継続的セキュリティ管理に必要な時間と労力を最小限に抑えるものです。

91%

のサイバー攻撃はフィッシングメールから始まります[1]

No. 1

の不正行為や不正アクセスへの攻撃ベクトル[2]

500億ドル

過去10年におけるBEC攻撃による損失[3]

488万ドル

2024年におけるデータ漏洩の平均コスト[4]

1. 2020年Deloitte調査
2. Microsoft SIRレポート
3. 2023年FBI IC3 PSA
4. 2024年IBMデータ侵害のコストに関する調査

Microsoftのメールセキュリティ機能

SEGの重複を排除してリスクとコストを削減

分析者たちは、重複する機能を最小限にするために機能を統合することが、企業のコストと複雑さの削減に役立っているという点で一致しています。とはいえ、すべてのユースケースを満足させるために、ネイティブの機能を慎重に評価するよう企業に助言しています。

Microsoftがメールセキュリティの必須機能を強化し続ける中、SEGとの重複が増加しているため、企業はE3ライセンスまたはE5ライセンスに既に含まれている機能を活用することで、セキュリティ運用を合理化する機会を得ています。このシフトにより、企業は複雑でコストのかかるSEGの導入を排除し、その予算の一部を最も危険なフィッシングの脅威に効果的に対処する軽量なソリューションの統合に振り向けることができます。

Cloudflare Email Securityは、機械学習による脅威分析を用いてMicrosoft 365を拡張し、BECやマルチチャネル攻撃の検知を自動化する、ロータッチ統合ソリューションを提供します。

SEGの機能が重複している領域：

- **メール衛生**
  既知のマルウェアをシグネチャベースで検出する、スパムおよびバルクメッセージ用のルールベースのポリシー。
- **URLと添付ファイルの保護**
  すべてのメールリンクの基本的な書き換えと、添付ファイルのサンドボックス機能。
- **調査と脅威ハンティング**
  メール検索、インシデント調査と相関関係、調査、修復。
- **情報保護**
  メール、ファイル、エンドポイントの暗号化、アーカイブ、DLPポリシー。
- **意識向上とトレーニング**
  フィッシング攻撃のシミュレーションとエンドユーザー向けのトレーニング。

オンライン保護を変更

すべてのプランに含まれており、バルク、スパム、マルウェアをフィルタリングするために不可欠なメール衛生を提供。

- アンチスパム
- シグネチャベースのマルウェア対策

Microsoft Purview (DLP)

設定可能なデータ損失防止ルールと実施。Microsoft Information Protectionと統合されています。

- メールとファイル用DLP
- Teams用DLP
- エンドポイント用DLP

Defender for O365 プラン1

悪意のあるリンクや添付ファイルに対する基本的な保護のための追加的セキュリティ制御。

- セーフリンク機能（URLリライト）
- Safe Attachments（サンドボックス）
- 社内メール 保護

Defender for O365 プラン2

プラン1の内容に加え、脅威ハンティング、調査、訓練、対応に関する追加機能が含まれます。

- 脅威ハンティング
- ドメイン横断的なインシデント相関
- サイバー攻撃シミュレーショントレーニング

E3ライセンス

E3ライセンス + コンプライアンス

E3ライセンス + コンプライアンス + セキュリティ

E5ライセンス

● 完了　● 制限付き　● なし

		SEG	M365	Cloudflare
脅威 からの保護	許可リスト／ブロックリスト	●	●	●
	既知の悪意のある送信者	●	●	●
	既知の悪意のあるURL／添付ファイル	●	●	●
	スパム／バルクフィルタリング	●	●	●
	機械学習（コンテンツ分析）	●	●	●
	Zero-Dayマルウェア／ランサムウェア	●	●	●
	悪意のあるリンク	●	●	●
	URLリライト（クリックタイム分析）	●	●	●
	適応型リンク分離	●	●	●
	ビジネスメール詐欺（BEC）	●	●	●
	従業員偽装	●	●	●
	ベンダー偽装	●	●	●
	従業員の侵害（ATO）	●	●	●
	ベンダー侵害	●	●	●
	DMARC管理	●	●	●
	悪意のあるアプリ検出（OAuthフィッシング）	●	●	●
	Webコンテンツセキュリティ	●	●	●
	セキュリティ意識向上とトレーニング	●	●	●
脅威 レスポンス	単一の直感的インターフェイス	●	●	●
	脅威の自動トリアージ	●	●	●
	迅速な検索と調査	●	●	●
	自動取消	●	●	●
	オンデマンドレポート	●	●	●
	マネージド検出とレスポンスサービス	●	●	●
データ 保護	暗号化	●	●	●
	アーカイブ	●	●	●
	メールDLP	●	●	●
	クラウドDLP（コラボレーションアプリ）	●	●	●
	ネットワークDLP	●	●	●

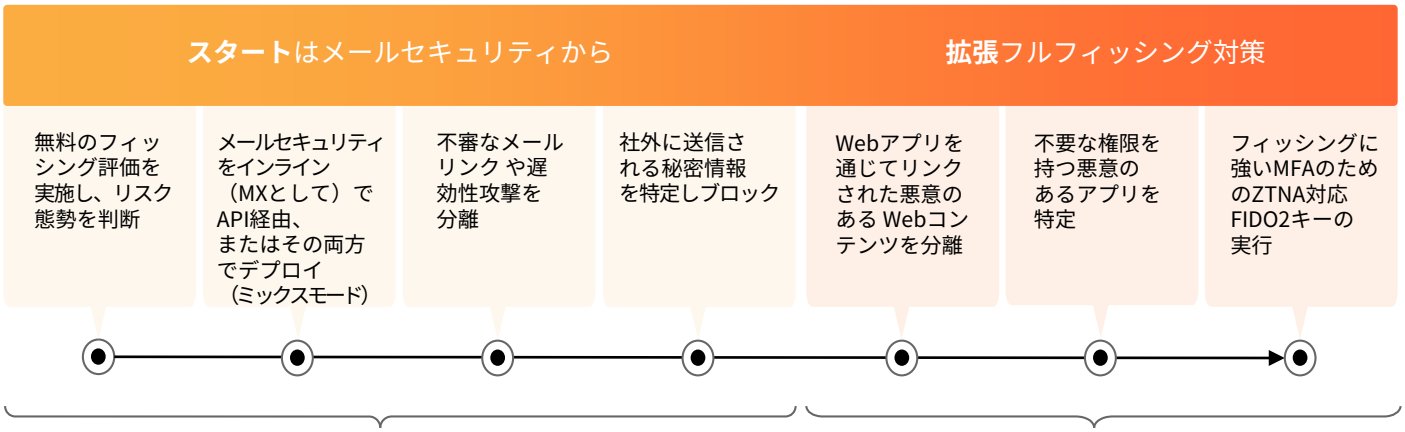
メリット

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。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。

レトロスキャンを実行　PRAをリクエスト