Email Link Isolation

メールリンクの分離によって攻撃対象領域を縮小し、運用を簡素化

ブラウザ分離による保護と制御を適用し、フィッシングのリスクを低減

問題：高度なマルチチャンネルフィッシング

マルチチャンネルフィッシングは、フィルタリングのルールを巧みにすり抜ける方法でメールやWeb配信を攻撃してきます。よくあるマルチチャンネルフィッシングのタイプは：

- **遅延フィッシング：**メール内の当初は良性のリンクが受信後に悪性リンクに変わって有害化します。
- **クラウドサービスフィッシング：**危険なHTTPSリンクは、普及しているクラウドサービス（Google Drive、Boxなど）とよく似ています。

これらの脅威を阻止するために、最新のメール保護はZero Trustの「決して信頼せず、常に検証する」精査を全リンクに適用できるものでなくてはなりません。

ソリューション：メールリンク分離

リモートブラウザ分離（RBI）機能とクラウドメールセキュリティ（CES）を統合してZero Trustの精査を適用し、フィッシングに対する保護を強化します。Cloudflare Area 1をご利用のお客様は、Cloudflare Browser Isolationをオンにして、そうしたマルチチャンネルの脅威を 無害化することができます。

管理者は、分離したWebページ上のユーザーインタラクションを制御し（キーボード入力やファイルアップロードの制限など）、クレデンシャルハーベスティングや機密データ窃盗といったフィッシング被害を防止することができます。

しかも、分離されたブラウザでメールリンクを開け、クラウド内の全コードをローカルデバイスから遠く離れたところで実行することによって、マルウェアを無害化します。

アナリストのコメント：

「外部参照を解決するメールベースのURLが、従業員を狙ったフィッシングによく使われます。それらのURLを分離すれば、フィッシング攻撃の成功率を下げることができます。」

「攻撃の多くはパブリックインターネット経由で、ユーザーを騙して悪性サイトを訪問させるWebブラウジングまたはメールリンクによるものです。エンドユーザーのデスクトップからブラウザを除去（はっきり言えば分離）するだけで、ランサムウェア攻撃からの保護を含め、企業のセキュリティポスチャを大幅に強化することができます。」

「特定の高リスクユーザー（財務チームなど）またはユースケース（メールベースのURLのレンダリングなど）用に、ブラウザ分離ソリューションを評価し、パイロット導入してみましょう。特に、リスク回避的な企業にお勧めします。」[1]

Gartner

続きを読む

CESとRBIを統合することのビジネス上のメリット

フィッシングに対する保護を強化

メール分離は、フィッシングリンクに含まれる有害なコードがローカルで実行されることを阻止するだけでなく、データ保護の制御を適用して機密情報が良からぬ輩の手に渡ることも防止します。

ITとセキュリティの生産性を解放

どのWebサイトについても、数クリックでメール分離をオンにします。

ITとセキュリティの担当チームは、フィルタリングポリシーを設定する面倒と、設定による「オーバーブロッキング」（とユーザーの生産性低下）や「アンダーブロッキング」（と脅威の侵入）のリスクを回避することができます。

サンプルユースケース：遅延フィッシングの阻止

問題：遅延フィッシングは検出を回避

遅延フィッシングキャンペーンは、強い動機と巧みな戦術を以て従来の保護策をバイパスする可能性があります。

キャンペーンセットアップ：攻撃者はまず、新たに作成したドメインから、適正なメール認証（SPF、DKIM、DMAR）と良性Webページを使って、正統に見えるメールを送信します。

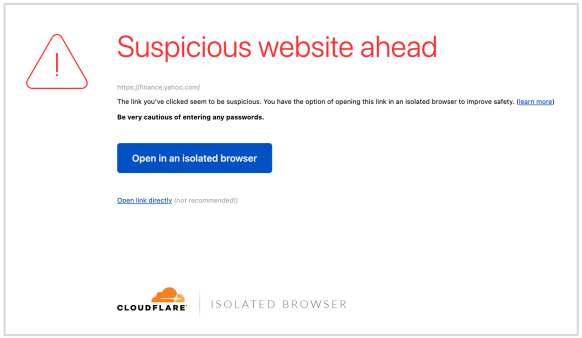
受信箱への配達に成功：それらのメールは、セキュアメールゲートウェイ、認証ベースのフィルター、あるいは評判ベースの兆候などの判定手法を用いた他のサービスによる検出を回避することができます。

悪性リンクに切り替え：メールの配達に成功すると、攻撃者は自分が管理するWebページを変更することによってリンク先を悪性のものに切り替えることができます。たとえば、よくあるのは資格情報を収集するための偽ログインページへの切り替えです。

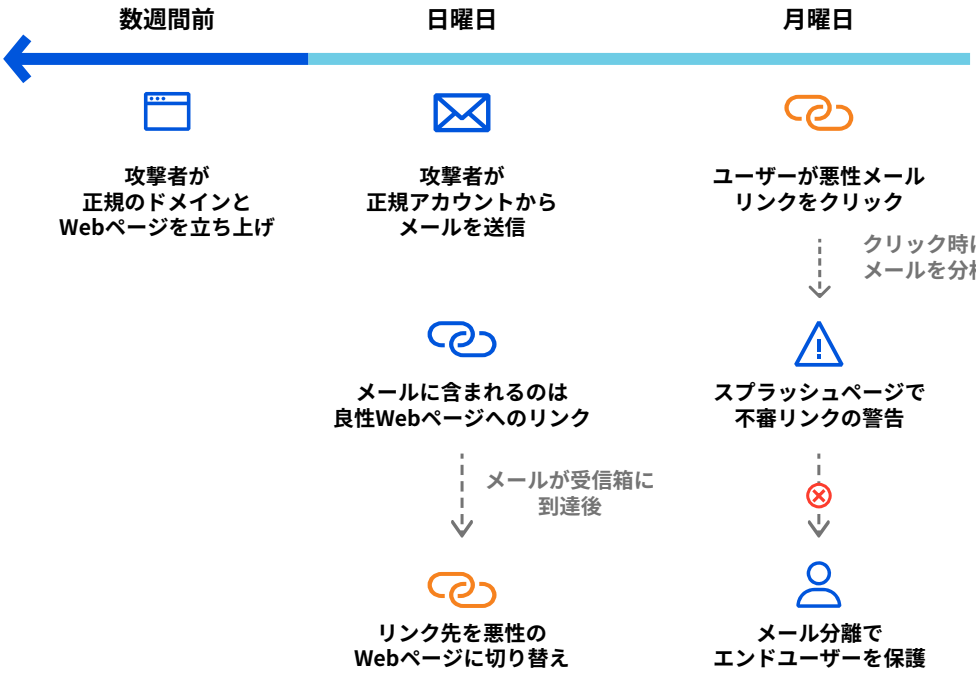
ソリューション：不審なリンクを受信箱到達後に分離

メールリンク分離によって、重要な受信箱到達後の保護層ができます。Cloudflareは、ユーザーがクリックするメール内リンクをすべて分析します。リンクが不審または危険と判断されるとCloudflareが警告スプラッシュページ*（下図）*を表示し、ユーザーがナビゲートする場合はそのWebページを分離します。

管理者は悪性コードがローカルデバイスで実行されるのを阻止し、ファイルのアップロードやダウンロードを制限する、ユーザーキーボードでの入力を阻止する、ページを読み取り専用モードで開くなどのデータ保護制御を適用することができます。



遅延フィッシングキャンペーンのタイムライン



クリック時に各リンクをCloudflareが分析

安全なリンク：ユーザーはこのサイトへ透過的にリダイレクトされます。

悪性リンク：ユーザーはナビゲートを阻止されます。

不審なリンク：ユーザーはナビゲートしないよう強く促され、分離されたブラウザでリンク先を見るよう勧める警告スプラッシュページが表示されます。

クラウドメールセキュリティとCloudflare Zero Trustの統合

Zero Trustを使った最新セキュリティ

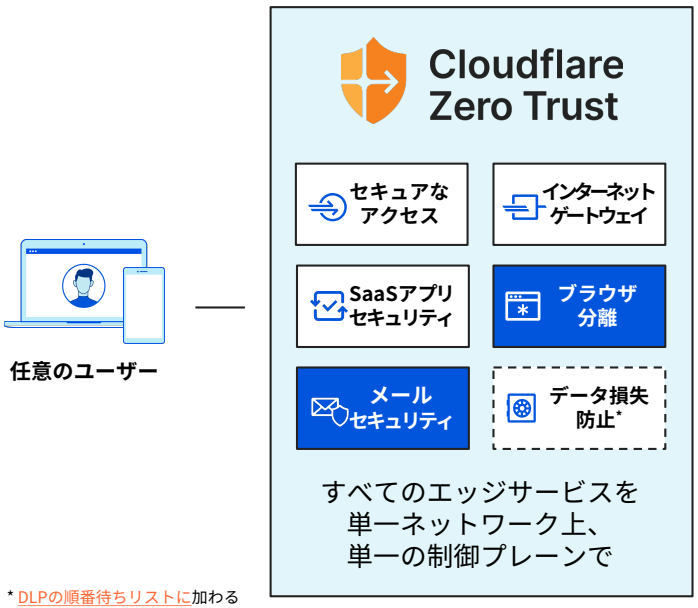
Cloudflare Zero Trustは可視性を高め、簡素化して、リモートユーザーとオフィスユーザーが企業アプリケーションやパブリックインターネットに接続する際のリスクを低減します。

Cloudflareは、当社のZero Trustプラットフォームの強化によってメール、Web、ネットワーク環境でのフィッシング攻撃からユーザーを守るというビジョンのもと、2022年4月1日にArea 1 Securityの買収を完了しました。詳しくはこちら。

メールセキュリティ：Zero Trustの中核

Cloudflare Area 1メールセキュリティは、メールから暗黙の信頼を排除することでZero Trustを強化し、フィッシングやビジネスメール詐欺（BEC）を先制的に阻止します。

どんな送信者も信頼しません。社内の送信者であろうと同じです。メールを含むすべてのユーザートラフィックを検証、フィルタリング、検査し、インターネット上の脅威から分離します。メールセキュリティはCloudflareのZero Trustサービス全体と統合し、RBI、CASBなどと組み合わさって強力なものとなります。



* DLPの順番待ちリストに加わる

VPNの代替
あらゆるユーザーをあらゆるリソースへ簡単かつ安全に接続します。

インターネットの保護
あらゆるポートとプロトコルにわたり、脅威からデータを安全に保護します。

SaaSセキュリティの効率化
メールを含むアプリケーションを可視化し、制御します。

セキュリティの最新化
生産性を向上、運用を簡素化、攻撃領域を縮小します

クラウド型メールセキュリティ（CES）

- フィッシングインシデントへの対応時間を90%短縮します。
- 攻撃サイクルの初期段階でフィッシングを止めるため、早期に攻撃者のインフラストラクチャと攻撃メカニズムを特定します。
- コンテンツ、コンテキスト、通信のソーシャルグラフを分析し、メールから暗黙の信頼を排除します。
- Microsoft、Googleその他の環境との統合によって、ビルトインセキュリティを強化します。

リモートブラウザ分離（RBI）

- ユーザーインタラクション（たとえばキーボード入力、コピー＆貼り付け、アップロード/ダウンロード）を制御し、危険なサイトを「読み取り専用モード」で開くことによって、資格情報侵害を阻止します。
- ブラウザコードをすべてCloudflareのネットワークで実行し、ローカルデバイスを悪性コードから分離します。
- 摩擦のない高速のエンドユーザーエクスペリエンスを提供します。通常のピクセルストリーミングではなく、世界のインターネットユーザーの95%から50ミリ秒以内のリモートブラウザから、ページを正確に複製します。

フィッシングのリスク評価を今すぐ依頼

お問い合わせ

03-4510-1893 | enterprise@cloudflare.com | www.cloudflare.com

REV: PMM-2022JUN