

## ソリューション概要

# Proofpoint Collab Protection

チャットツールやコラボアプリケーションより  
侵入する脅威から人を守る



## 主なメリット

- メールの枠を超えてフィッシング保護を提供
- リアルタイムで悪意のあるURLをブロック
- すべてのデジタルチャネルにおいてフィッシング脅威を可視化
- 広範なフィッシング保護によりデータ侵害のリスクを低減

今日のダイナミックな業務環境において、コミュニケーションや共同作業に用いられているものはメールだけでなく、チャットツール、コラボレーション アプリ、ソーシャル メディア プラットフォームなど、その他の多くのデジタルチャネルも利用されています。攻撃者はこのように移行している状況を把握しており、こうしたチャネルを悪用して攻撃を仕掛けるようになっています。

## 包囲されるチャットツールおよび コラボレーション プラットフォーム

攻撃者は、チャットツールやコラボレーションのプラットフォームを、フィッシング攻撃の新たな起点としています。この目的のために、ソーシャル エンジニアリング 戦術や悪意のあるURLを使用しています。悪意のあるURLは、攻撃者がペイロードを配布するために最も用いられている方法となっています。Proofpoint Threat Research

チームによると、ここ3年で、SMSベースのフィッシング（スミッシング）によって配信されたURL脅威は2,524%もの上昇が確認されています。攻撃者は、チャットツールやコラボレーション アプリを使用して、偽のアカウントをセットアップし、見せかけの関係を築き、相手を偽のログインページに誘導します。こうしたページは、個人情報を取得したり、ユーザーを騙して送金させたり、企業の機密情報を提供させたりすることを目的としています。

## チャットツールおよび コラボレーション アプリにおいて 攻撃が発生する仕組み

Microsoft Teams、Slack、Zoomなど、チャットツールおよびコラボレーションアプリを標的にしたフィッシング攻撃は、以下の手順で行われます。



図1：チャットツールやコラボレーション アプリへの攻撃は一般的に複数の段階に分けて行われる

## チャットツールおよび コラボレーション アプリの セキュリティを強化する

チャットツールおよびコラボレーション アプリは、人と組織をフィッシング攻撃から保護するためのネイティブセキュリティ機能を備えていません。そこでプルーフポイントが役立ちます。

Proofpoint Collab Protectionは、チャットツール、コラボレーション アプリ、ソーシャルメディアのアプリケーションで配布された悪意のあるURLから保護します。URLのレビュー調査と分析をリアルタイムで実行し、悪意のあるURLにユーザーがアクセスしようとなればブロックします。Proofpoint Collab Protectionにより、プルーフポイントは、ユーザーを高度なフィッシング攻撃からいつでもどこでも保護します。

## 従業員を 悪意のあるメッセージから保護

Proofpoint Collab Protectionは、プルーフポイントの業界有数の脅威インテリジェンスを活用しています。従業員がデスクトップPCまたはモバイルデバイスから、チャットツールおよびコラボレーションアプリ内の不審なリンクにアクセスしようとすれば、Proofpoint Collab ProtectionはURLをリアルタイムで分析します。URLのレビュー調査と分析を行い、ブラウザで入力されたURLを分析します。Proofpoint Collab Protectionが悪意のあるURLを検知した場合、これをブロックします。このようにしてユーザーは、悪意のあるWebサイトやコンテンツから保護されます。

The screenshot shows the Proofpoint TAP Dashboard interface. The main header bar includes the 'proofpoint' logo, a dropdown menu, and various navigation icons. Below the header, a search bar displays the URL 'i.qleap.share....'. The main content area is titled 'Threats via ZenWeb' and shows a single threat entry for 'i.qleap.sharepoint.com/X8enGZ'. This entry includes a preview icon, a link to 'Open in Proofpoint Browser Isolation', and a status indicator. To the right of the threat entry are two progress bars: 'Threat Severity' at 50 and 'Proofpoint Customers' at 100+. Below the threat entry, there are sections for 'Attributes' (Family: Credential Phishing, Technique: Social engineering, Threat Objectives: Credential Harvesting) and 'Evidence'. The 'Affected Users' section indicates 2 clicks attempted by Bobby Williams and John Smith, which were successfully blocked. The 'Click Details' section provides a table of 4 Clicks, listing timestamp, full name, email, URL, status, platform, browser, and extension ID for each event.

Timestamp	Full Name	Email	URL	Status	Platform	Browser	Extension ID
2024/09/05 01:20	Bobby Williams	bobby.williams@fort...	i.qleap.sharepoint.com...	Blocked	Windows 10	Chrome 5.0	ext-hy7835dfg6sh76e
2024/09/05 01:20	John Smith	john.smith@fortress...	i.qleap.sharepoint.com...	Blocked	Windows 10	Chrome 5.0	ext-hy7835dfg6sh76e

図2: Proofpoint Collab ProtectionはユーザーがアクセスしたURLをリアルタイムで分析

## マルチチャネルのフィッシング脅威の可視化

攻撃者は、さまざまなデジタルチャネルで従業員を標的にするようになっています。これらのチャネルには、メール、コラボレーション プラットフォーム (Microsoft Teams、Slack、Zoom)、そしてテキストメッセージさえも含まれます。セキュリティチームやITチームは、これらすべてのチャネルにおいて脅威を監視しなければなりません。Proofpoint Collab Protectionはこのようなマルチチャネルの可視性を提供します。従業員がチャットツールまたはコ

ラボレーション アプリ内の不審なリンクにアクセスした場合、Proofpoint Collab Protectionはリンクにアクセスしたユーザーと、リンクを送信したデバイス (デスクトップPCまたはモバイルデバイス) を表示します。また、該当するURLがブロックされたかどうかも示します。Proofpoint Collab Protectionは、すべてのチャネルにおける脅威に関する統一されたビューを提供するため、フィッシング脅威を迅速に追跡し、軽減できます。セキュリティチームやITチームは、組織に害を及ぼす前に攻撃を検知し、阻止できます。

The screenshot shows the Proofpoint Collab Protection interface. On the left is a sidebar with icons for Mail, Chat, People, Cloud, Metrics, Search, and Settings. The main area has a header 'Threats via ZenWeb' and a dropdown for 'Last 24 hours'. Below is a table titled 'Threats' with columns for Threats, Latest Activity, and Users Affected. The table lists several threat entries:

Threats	Latest Activity	Users Affected
<a href="https://acusconsulting.com">https://acusconsulting.com</a>	09/22/2023	1
<a href="http://www.conchtech.com">www.conchtech.com</a>	09/22/2023	1
<a href="http://speedtrainingonline.com/">speedtrainingonline.com/</a>	09/22/2023	3
<a href="http://93.127.168.184.host.secureserver.net">http://93.127.168.184.host.secureserver.net</a>	09/22/2023	1
<a href="https://myll.s3.us-east-2.amazonaws.com/van.html">https://myll.s3.us-east-2.amazonaws.com/van.html</a>	09/22/2023	1
<a href="https://saapartmentguide.com/Mobile.aspx">https://saapartmentguide.com/Mobile.aspx</a>	09/22/2023	1
<a href="http://arinhiyapi.com/">arinhiyapi.com/</a>	09/22/2023	1
<a href="https://i.qleap.sharepoint.com/X8enGZ">i.qleap.sharepoint.com/X8enGZ</a>	09/22/2023	2

図3: Proofpoint Collab Protectionは複数チャネルでの脅威に関する統一されたビューを提供

## 次の進化： Human-Centric Security

近年、企業業務におけるコミュニケーションや共同作業に、ますますメール以外のチャネルが利用されるようになっています。攻撃者はこの変化に目を付け、サイバー攻撃のための新たな侵入経路を見出しています。そういうたたかいで攻撃には、フィッシング、マルウェア、アカウント乗っ取りが含まれます。こうした新たな脅威に先手を打つためには、メール保護と同等の検知精度をチャットツールやコラボレーション アプリにも拡大するソリューションが必要です。

Proofpoint Collab Protectionなら、メールの枠を超えてフィッシング保護を拡大することができます。Proofpoint Collab Protectionは、チャットツールまたはコラボレーション アプリにおいて悪意のあるフィッシング メッセージを阻止できます。URLのレビューション調査と分析により、これらの脅威がリアルタイムで検知され、阻止されます。これにより、従業員を高度なフィッシング攻撃からいつでもどこでも保護できます。



Proofpoint, Inc. は、サイバーセキュリティのグローバル リーディング カンパニーです。組織の最大の資産でもあり、同時に最大のリスクともなりえる「人」を守ることに焦点を当てています。プルーフポイントは、クラウドベースの統合ソリューションによって、世界中の企業が標的型攻撃などのサイバー攻撃からデータを守り、そしてそれぞれのユーザーがサイバー攻撃に対してさらに強力な対処能力を持つよう支援しています。また、Fortune 100 の 85% の企業などさまざまな規模の企業が、プルーフポイントのソリューションを利用しており、メールやクラウド、ソーシャルメディア、Web 関連のセキュリティのリスクおよびコンプライアンスのリスクを低減するよう支援しています。詳細は [www.proofpoint.com/jp](http://www.proofpoint.com/jp) にてご確認ください。

プルーフポイントとつながる : [X](#) | [LinkedIn](#) | [Facebook](#) | [YouTube](#)

Proofpoint は、米国および / またはその他の国における Proofpoint, Inc. の登録商標または商標名です。記載されているその他すべての商標は、それぞれの所有者に帰属します。

プルーフポイント プラットフォームをご覧ください →