

人中心のセキュリティで リスクを低減：

サイバー攻撃の一步先を行く 戦略の立案

主なメリット

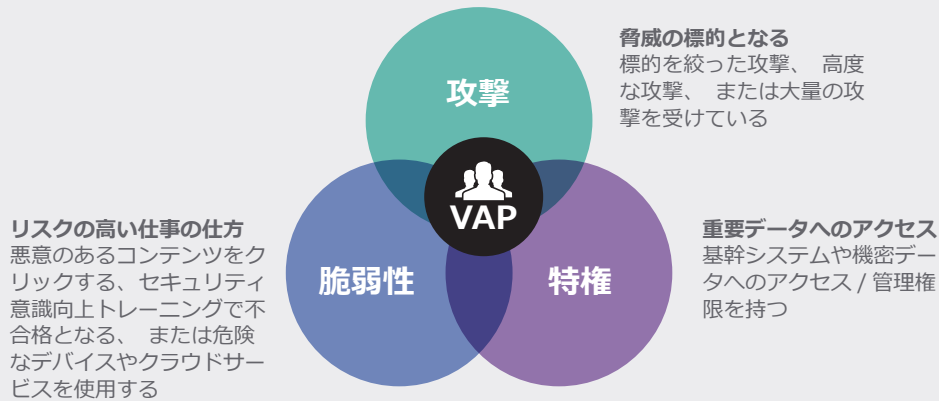
以下を明らかにすることによって、 ビジビリティの向上とコントロールを可能にします：

- 人がどのように脅威の標的とされているか
- 人がどれだけリスクの高い方法で仕事をしているか
- 人が重要なデータにどのようにアクセスしているか

現代の脅威ランドスケープの基本的な特徴は、 ソーシャルエンジニアリングの利用です。 攻撃はテクノロジーやインフラではなく、 人を標的にするようになっていました。 そしてクラウドへのシフトがこの傾向をさらに強めています。 Proofpoint は、 ビジビリティの向上やインサイトの収集をサポートし、 また最大のセキュリティリスクである「人」をベースにしたアダプティブ（適応型）な制御を可能にします。 重要視しているのは「人」だけではありません。 人がアクセスする「データ」、 そして彼らが最新のソーシャルエンジニアリング攻撃に騙される可能性、 またはすでに騙されていることを示唆する「行動」にも注目しています。

攻撃者は人にフォーカス

攻撃者は組織を狙ったキャンペーンの準備として、 Google や LinkedIn などを使ってインターネット上で偵察活動を行います。 彼らの攻撃手法はさらに高度に、 かつ大規模になってきています。 ほとんどの IT/ サイバーセキュリティプロフェッショナルはいまだにネットワークや IP アドレスを世界の中心に据えて考えていますが、 攻撃者は世界をネットワーク構成図の視点では見ていません。 さらに、 Microsoft Office 365 や Google G Suite のようなクラウドアプリやプラットフォームの利用が増えるにつれ、 ネットワークをベースにした防御アプローチは限界を迎えつつあります。 クラウドアプリには重要な企業情報が含まれていますが、 これらはファイアウォールやその他のネットワーク制御を通さずにインターネット上のトラフィックに乗っています。 そのため、 人に影響を及ぼすあらゆる脅威を可視化することは非常に困難であり、 組織に関係するリスクを基にアラートやインシデントを優先順位付けすることも困難です。



攻撃対象になる人を特定する

Proofpoint は、人を標的にして利用しようとする脅威にフォーカスしてセキュリティリスク管理を行います。そのため、まずは Very Attacked People (VAP) を特定することから始めます。Proofpoint はこれを戦略的に行い、以下のインサイトを提供します。

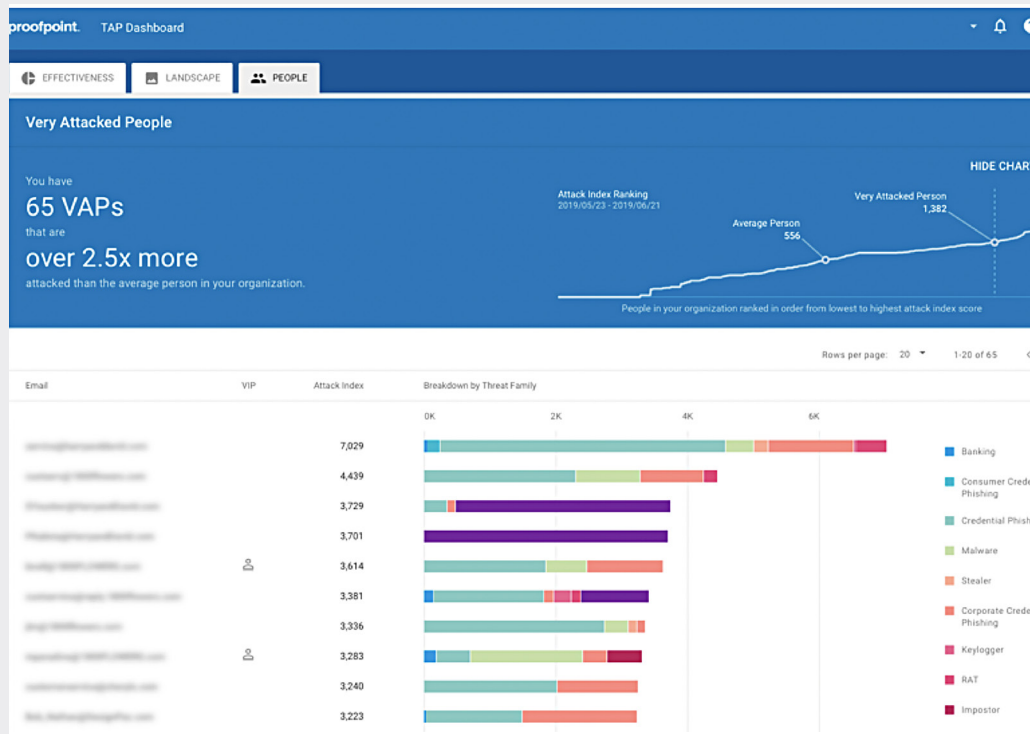
- 人がどれだけリスクの高い方法で仕事をしているか：意図的かどうかにかかわらず、悪意のあるリンクや添付ファイルをクリックしたり、脆弱なアプリを使用したりしたことがあるか。
- 人がどのように脅威の標的とされているか：受けているのは、標的を絞った攻撃なのか、高度な攻撃なのか、または無差別型の大量攻撃なのか。
- 人が重要データにどのようにアクセスしているか：重要なシステムやデータにアクセスしたり、それを管理したりしている場合、ビジネスシステムまたはサードパーティアプリを通じたデータの悪用、損失、漏洩のリスクが高い。

Proofpoint Attack Index でリスクを数値化

人を中心としたリスクを数値化する方法の一つに、Proofpoint の Attack Index があります。Proofpoint は標的になっている人を識別し、毎日の脅威アクティビティからノイズを取り除いて本当に心配すべき脅威を表面化させるために、Attack Index を考えだしました。Attack Index は人を狙うすべての脅威の加重複合スコアで、4つの要因に基づいて点数付けされています。

- **攻撃のボリューム**：脅威の総数
- **攻撃のタイプ**：例えば、クレデンシャルフィッシングはリモートアクセス型トロイの木馬よりもリスクは低いと考えられます
- **標的の絞り込み度合い**：脅威の標的が世界全体か、地域か、業界か、組織か
- **アクターの洗練度**：有名で高度な脅威アクターによる脅威かどうか

Attack Index を用いると、ユーザーが直面する個々のリスクと全体リスクを評価・報告でき、脅威への最も効果的な対応策を優先順位付けできます。



人を中心としたセキュリティアプローチ

Proofpoint は人を中心としたセキュリティ強化を支援するソリューションを提供しています。

人を標的にした脅威からの保護

人を攻撃対象とするあらゆる脅威に対して、検出からレスポンスまで対応します。誰が攻撃されているか、どのように攻撃されているか、そして実際に侵害されているかを可視化できます。すべての攻撃経路（社外メール、社内メール、個人 Web メール、クラウドアカウント）からの人を狙う攻撃を防御します。ビジネスエコシステムをより幅広く保護し、取引先からリスクがもたらされないようにしましょう。

高度な最新型脅威へのユーザーの耐性強化

ユーザーが最後の砦となるよう、教育を徹底します。どのユーザーがフィッシング攻撃をクリックしたかを識別して、そのユーザーに攻撃を見分ける方法とそれを報告する方法を理解させます。ユーザーが自分の ID、クレデンシャル、そしてデータを保護できるよう、ベストプラクティスを共有しましょう。

ユーザーが作成しアクセスするデータの保護

分離可能でアダプティブな統合制御で VAP を保護しましょう。ユーザーが作業を行うデジタルチャネル（メール及びクラウドを含む）の機密データを守ります。これまでに行った投資を最大限活用し、人中心のセキュリティを強化して、Microsoft Office 365 や Google G Suite などのクラウドアプリのアカウント侵害の問題を解決します。

詳細は [proofpoint.com](https://www.proofpoint.com) でご確認ください。

proofpoint について

Proofpoint, Inc. (NASDAQ:PFPT) は、サイバーセキュリティの主導的企業であり、組織の最大の資産であり同時に最大のリスクでもある「人」を守ります。Proofpoint 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脅威を阻止し、データを守り、ユーザーがサイバー攻撃に対してより大きな耐性を持てるように支援します。また、Fortune 1000 の過半数を超える企業を含むあらゆる規模のトップ企業が、メールやクラウド、ソーシャルメディア、Web 関連の最も重要なセキュリティリスクおよびコンプライアンスリスクを低減させるために、Proofpoint を利用しています。詳細は www.proofpoint.com でご確認ください。

©Proofpoint, Inc. Proofpoint は、米国およびその他の国における Proofpoint, Inc. の商標です。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。