

Proofpoint Web Security

Webトラフィックのアクセスポリシー制御

主な機能

- 監視と可視性**— SSLトラフィックの復号および検査、ドメインベース、URLベース、およびIPベースのフィルタリング、コンテンツや脅威に対するカテゴリベースのフィルタリング、カスタマイズ可能なブロックページとWeb分離による対策強化、インラインSaaSディスカバリー（シャドーIT）とアプリケーションコントロール
- 高度な脅威対策**— インラインでのファイルダウンロードの保護、カスタマイズ可能なブロックページとブラウザのWeb分離による対策強化、プルーフポイントの脅威インテリジェンスに基づくレピュテーションベースの検出と防止、サンドボックス、ゼロデイ保護
- データ漏えい対策**— インラインでのダウンロードとアップロードの保護、選択的なブラウザのWeb分離による対策強化、何百もの定義済みの検出機能、ディクショナリ、スマートID、カスタマイズ可能なデータ型
- 管理**— クラウドネイティブ、グローバル分散型プロキシ、クラウドベース管理、Proofpoint ZTNA および Proofpoint CASB との共通クライアント、インフォメーションクラウドセキュリティプラットフォームのモジュールコンポーネント、Windows および macOS のサポート、SSO 認証、IdP (SCIM, SAML, JIT) によるユーザープロビジョニング、SIEM の統合

Proofpoint Web Security は、Web を閲覧するユーザーを高度な脅威から守ります。境界の内外を問わず、すべての従業員が安全にインターネットにアクセスできるようにすることで、分散して働く従業員をサポートします。監視と可視性、高度な脅威対策、データ漏えい対策 (DLP) ポリシーを、「人」を中心としてセキュリティを構築するPeople-Centricアプローチに適用します。

監視と可視性

監視と可視性は、Proofpoint Web Security のアプローチの中心をなすものです。このソリューションでは、すべての SSL トラフィックを即座に検査します。これにより、脅威を発見し、従業員がコンプライアンスに反するコンテンツを閲覧した場合、検知することができます。また、SaaS (Software as a Service) アプリを検出し、セキュリティを確保するためのコントロールを適用することができます。これらのコントロールは、以下の防止に役立ちます。

- 認証情報の窃取
- 制限付きコンテンツの閲覧
- コンプライアンスに反する Web サイトの訪問
- ボットネットの挙動やコマンド アンド コントロール通信
- 未承認の SaaS アプリ (シャドー IT) の使用

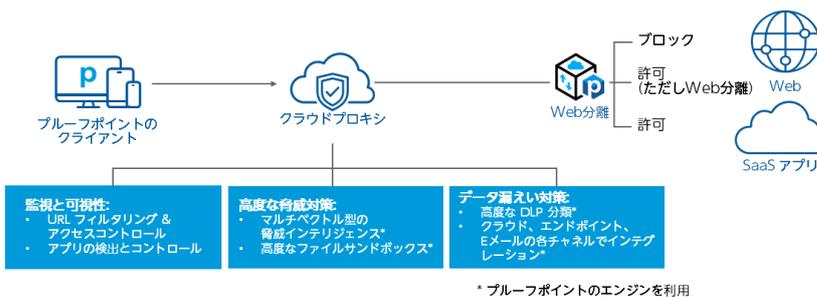


図 1: Proofpoint Web Security の仕組み

Proofpoint Web Security は脅威をリアルタイムで特定します。ドメイン、URL、および IP レベルで危険を監視し、オーバーヘッドを削減する包括的な防御を提供します。また、Proofpoint Web Security はサイトをブロックすることもできます。さらに、ユーザーが不審な URL を閲覧した場合、その Web セッションを自動的に分離することもできます。これらのコントロールは、組織全体に適用することができます。また、特定のユーザーグループやリスクの高いユーザーにのみ適用することも可能です。

高度な脅威対策

Proofpoint Web Security の高度な脅威対策により、エンドポイントを保護します。シグネチャベースの検出により、既知の脅威を阻止します。未知のゼロデイファイルについては、クラウド上のサンドボックスでリアルタイムに検査します。また、Proofpoint Web Security は透過的に動作します。不正なファイルをダウンロードしたり、不審なサイトを訪れたりしても、ユーザーのエクスペリエンスに著しい影響を与えることはありません。この対策では、Nexus Threat Graph を搭載したプルーフポイントの脅威インテリジェンスを採用しています。

データ漏えい対策

Proofpoint Enterprise DLP と統合された Proofpoint Web Security は、すべての Web アプリに対してビルトイン DLP を提供します。また、データ分類を共有し、アラート管理と調査を単一のポータルから行うことができます。カテゴリ、URL、リスクのレベルごとにアップロードやダウンロードを制限することができます。また、ユーザーが不審な URL にアクセスしたときに、読取り専用モードを強制することも可能です。

Proofpoint Web Security は、さまざまなデータタイプに対応した 240 以上のデータ分類検出機能、ディクショナリ、スマート ID を備えています。また、ビルトインテンプレートによるシンプルで統一された分類ポリシー定義も含まれています。多くの組織がカスタマイズされたデータセットを必要とするため、EDM (Exact Data Match) を行うことができます。すべてのルールを、組織全体、特定のユーザーグループ、または主要な個人に適用することができます。

マネージメント

Proofpoint Web Security はクラウドネイティブです。あらゆるニーズに対応する拡張性を備えています。また、グローバルに配信されるため、ユーザーの所在地に関わりなく低遅延を実現します。また、管理はすべてクラウドベースのコンソールで行われます。API ベースのソリューションであるため、リモートで管理することができます。また、セキュリティ情報およびイベント管理 (SIEM) システムとの統合も容易です。Proofpoint Web Security は、Proofpoint ZTNA (ZeroTrust Network Access) および Proofpoint CASB (Cloud App Security Broker) と同じエンドポイントクライアントを使用します。

インフォメーション クラウド セキュリティ プラットフォーム

Proofpoint Web Security は、インフォメーション クラウド セキュリティ プラットフォームのコンポーネントです。このプラットフォームは、セキュリティサービスエッジ (SSE) 戦略の一環として、お客様の組織全体に一貫したセキュリティを提供します。また、管理と対応が統合されたコンソールを提供します。

このプラットフォームで使用する製品は次のとおりです。

- Proofpoint CASB (Cloud App Security Broker)
- Proofpoint ZTNA (Zero Trust Network Access)
- Proofpoint Web Security と Proofpoint Browser Isolation
- Proofpoint Email DLP (Data Loss Prevention) と Proofpoint Email Encryption
- Proofpoint Endpoint DLP (Data Loss Prevention) を使用する Proofpoint ITM (Insider Threat Management)

また、インテリジェント リスク モデリング、ワールドクラスの脅威、コンテンツ、行動検知、および包括的な可視性とコントロールを提供します。

詳細はこちら

詳細は proofpoint.com/jp でご確認ください。

プルーフポイントについて

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あてています。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応能力を持てるよう支援しています。また、Fortune 1000 の過半数を超える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 にてご確認ください。

©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。