Advanced URL Filtering

最高峰の Web 保護

リアルタイム Web 保護

アプリケーションのクラウド移行と場所を選ばない働き方が普及し、Web セキュリティの重要性は高まり、同時に困難にもなります。これはフィッシングやファイルレス攻撃などの Web ベース攻撃が高速かつ大規模に行われる上、手口が巧妙化しているためです。こうした状況でも、Web セキュリティ ソリューションの多くは、既知の有害 Web ページのデータベースのみに依存していますが、日々発生する数十万件の脅威によりデータベースは短期間で効果を失います。

パロアルトネットワークスの Advanced URL Filtering は、近代企業のための最高峰の保護をする製品です。有害 URL のデータベース機能と、ディープラーニングを活用した業界初のリアルタイム Web 保護エンジンという、トップクラスの機能を組み合わせています。これにより、悪意ある新しい Web ベースの標的型脅威を自動的に検知して即座に阻止できます。リアルタイム保護の世界へ。

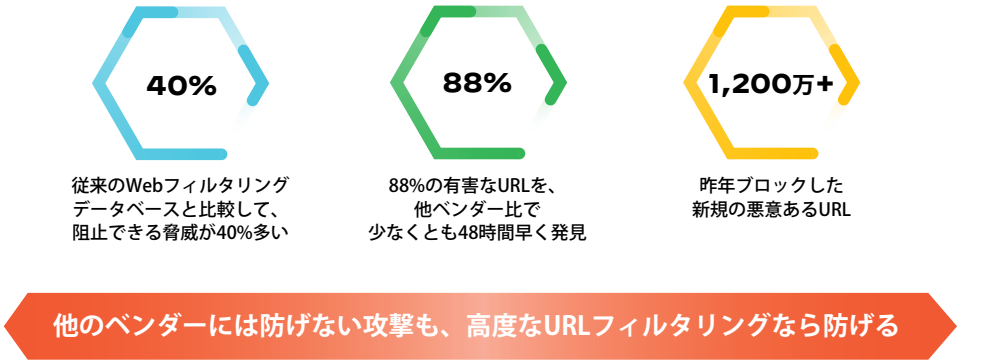

図 1: Advanced URL Filtering は現代の企業ネットワークを標的とした、最も被害の大きい Web ベース攻撃を検出

Advanced URL Filtering の利点

Advanced URL Filtering はクラウド上に構築されるサブスクリプション サービスであり、パロアルトネットワークスの次世代ファイアウォール (NGFW) とネイティブに連携して、フィッシング、マルウェア、ランサムウェア、コマンド アンド コントロール (C2) などの Web ベースの脅威からネットワークを保護します。

さらに、特許出願中の技術であるインライン ディープ ラーニングを使用して URL をリアルタイムに分析し、無害または有害のカテゴリに分類します。この分類を NGFW のポリシーに組み込むことで、Web トラフィックの完全な制御を容易にできます。また、分類を利用して NGFW プラットフォームの補完機能を起動することで、的を絞った SSL 復号や高度なロギングなど保護の層が厚くなります。Advanced URL Filtering は自身の分析機能に加えて、弊社の業界トップクラスのマルウェア防御サービス「Advanced WildFire」などの情報源から取得した共有の脅威情報を使用して、悪意のあるサイトに対する防御を自動更新します。Advanced URL Filtering の主なメリットは以下の通りです。

- **Web ベースの攻撃に対する優れた保護**：既知の脅威を阻止する URL データベースと、機械学習を活用したクラウド提供型 Web セキュリティ エンジンを組み合わせて使用しています。機械学習を利用することで、コンテンツがクローラーから隠された場合も、新しい有害 URL をリアルタイムに分類してブロックできます。Advanced URL Filtering は、従来の Web フィルタリング データベースよりも脅威を 40% 多く阻止できます。
- **業界トップクラスのフィッシング防御**：最も一般的な侵害の原因に対処します。
- **Web トラフィックの完全な制御**：きめ細かい制御およびポリシー設定を通して、ユーザー、リスク評価、およびコンテンツ カテゴリに基づくセキュリティ アクションの自動化を可能にします。
- **運用効率を最大化**：パロアルトネットワークスのプラットフォームを通じた Web 保護によって実現。

ビジネス上の利点

- **インライン保護 :** 100 ミリ秒未満で新たな未知の Web ベースの攻撃を阻止して、最初の被害を防ぎます。
- **回避技術を用いる標的型攻撃を検出 :** Web クローラーのデータではなく、実際の Web トラフィックを検出することで、回避技術を用いる標的型攻撃の検出率を向上させます。
- **クラウド ネイティブ サービス :** 時間とともに機能を拡張できるように設計されています。
- **一貫したセキュリティ ポリシーと機能を活用 :** Advanced URL Filtering をハードウェア アプライアンス、仮想環境、またはクラウドのいずれに導入する場合でも、同じポリシーのセットとセキュリティを一貫して適用できます。
- **セキュリティ サイロを解消してユーザーの安全を確保 :** ポイント ソリューションよりも 30% 早く適切なセキュリティ体制を実現できます。
- **運用コストの最小化 :** パロアルトネットワークスのクラウド提供型セキュリティ サービスを使用すれば、スタンドアロン ソリューションが不要になるため、3 年間で 990 万米ドルを節約できます [1]。
- **フィッシングに対する防御。**何層もの防御により、認証情報のフィッシングをリアルタイムに阻止し、既知 / 新規フィッシングサイトからお客様の組織を守ります。
- **法規制の順守と利用規定への対応。**お客様の組織が社内、業界、政府の規制ポリシーを順守し続けられるようにします。

主な機能

悪意のある新たな Web ページに対するインライン保護

パロアルトネットワークスは悪意のある Web ページが 2019 年から 2021 年の間に 127% 増加したことを確認しています [2]。新たな脅威が大量に発生しているため、前例のあるネットワーク攻撃はまず発生しません。

さらに、攻撃者は一般に信頼できると見なされている Web サイトに脅威を埋め込もうとするため、有害な URL の 40% は合法的なドメインに存在します [3]。つまり、無害な URL が有害な URL に変化することは珍しくないため、ソリューションが URL を絶えず分析しなければ、リスクは解消されません。静的なデータベースや更新の遅いデータベースだけに依存することはできません。新しいアプローチが必要なのです。

Advanced URL Filtering では、新たな脅威をリアルタイムに検出してブロックし、最初の被害を防止することで、Web 保護を次のレベルに引き上げます。クラウドベースのインライン ML は、Web クローラーのデータではなく、実際の Web トラフィックをリアルタイムに分析することで、有害な URL を数ミリ秒で分類してブロックし、感染の機会を失わせます。新たな Web ベースの脅威に対する最新の検出インテリジェンスを取り込むため、弊社は ML モデルを頻繁に再訓練しています。また、拡張可能なクラウドベースのアーキテクチャのおかげで、手間のかかる更新プロセスを実行することなく、即座に最新の画期的な検出モジュールの利用を開始できます。

今こそ、更新に時間がかかりすぎるオフライン クローリングとデータベースへの過度の依存から脱却しましょう。そしてその鍵を握るのが、未知の Web ベースの脅威を検出してリアルタイムに阻止する、業界初のインライン Web 保護エンジンを備えた Advanced URL Filtering なのです。

回避技術の無力化

最近の攻撃者はセキュリティ対策を回避するように進化しており、現在ダーク Web で販売されているフィッシング キットの 90% は 1 種類の回避手法があります [4]。クローキングと呼ばれる最も一般的な手法は、Web ページ コンテンツのオフライン クローリングだけで脅威の有無を判断する Web セキュリティ ソリューションが多数存在する状況を利用したものです。攻撃者はセキュリティ企業と判明している特定の IP アドレスやホストからの接続を能動的にブロックすることや、無害なコンテンツに再ルーティングすることがあります。

Advanced URL Filtering は、Web ページのクローリングにとどまらず、実際の Web コンテンツを分析することで、攻撃を阻止するとともに、回避技術で隠された悪意ある Web サイトの正体を暴きます。

1. *The Total Economic Impact™ of Palo Alto Networks for Network Security and SD-WAN*、Forrester、2021 年 1 月、https://start.paloaltonetworks.jp/2021-forrester-tei-report-network-security.html。
2. パロアルトネットワークスのシステムでの観察結果、2019-2021。
3. *2019 Webroot Threat Report*、Webroot、2019 年 2 月 22 日、https://www-cdn.webroot.com/9315/5113/6179/2019_Webroot_Threat_Report_US_Online.pdf。
4. 「6 Phishing Techniques Driven by the Phishing-as-a-Service Industry」、Cyren Security Blog、2019 年 7 月 1 日、https://www.cyren.com/blog/articles/evasive-phishing-driven-by-phishing-as-a-service。

フィッシング防御

フィッシングは記録にある最古のサイバー攻撃の手口ですが、依然として組織を悩ませます。20 秒に 1 件のペースで新たなフィッシング サイトが公開されており [5]、フィッシングは報告されているセキュリティ インシデントの 80% 以上 [6]、また成功した侵害の 22%[7] を占めています。

フィッシング攻撃が無くならない原因は、新しいフィッシング サイトを数秒で作成・削除できるためです。Advanced URL Filtering を利用することで、数百万件の既知のフィッシング ページから保護され、新たなフィッシング ページを即座に正確に検出して、最初の被害者にならないようにすることも重要です。パロアルトネットワークスでは、最も包括的なフィッシング防御を提供するために、以下のような何層もの画期的な検出機能を組み込んでいます。

- 高度な検出回避能力を備えた未知のフィッシング攻撃をリアルタイムに検出する、ML を利用したインラインの Web コンテンツ分析
- 業界唯一、認証情報の盗難をリアルタイムに阻止
- ML ベースのイメージ分析
- 静的分析と動的分析
- 詳細な再帰分析
- ディープラーニングの畳み込みニューラル ネットワーク (CNN) モデル
- アペンド攻撃の検出
- ML を活用したドメイン分析
- JavaScript エンジンの難読化解除
- フィッシング リダイレクション チェーン分析
- 偽の CAPTCHA のやり取り分析

運用上の利点

Advanced URL Filtering のメリットを以下にご紹介します。

- **共有インテリジェンスを活用 :** アプリケーションとユーザーに基づく扱いやすいポリシーに加えて、Advanced Threat Prevention と Advanced WildFire との緊密な統合を利用した最高峰の Web セキュリティの恩恵を受けられます。
- **Web トラフィックの完全な制御を維持 :** 疑わしいサイトに対する選択的な TLS/SSL 復号などの高度なセキュリティ アクションを、URL カテゴリを使用して自動的に起動できます。
- **セキュリティを自動化 :** アナリストの介入がなくとも、URL カテゴリにポリシーが自動適用されるため、時間を節約できます。
- **ユーザーと URL アクティビティを把握。**事前定義済みのレポートまたは完全にカスタマイズされたレポートを使用して、IT 部門が URL フィルタリングと関連する Web アクティビティを可視化できます。

Web トラフィックの完全な制御

Web ポリシーはファイアウォール ポリシーを拡張したものです。パロアルトネットワークスの NGFW では Advanced URL Filtering を使用して URL カテゴリを識別し、リスク評価を割り当て、一貫したポリシーを適用します。複数の URL カテゴリおよびリスク評価を組み合わせて微妙な違いのある複数のポリシーを作成することで、単一のポリシー セットを通じた例外に基づく正確なポリシーの適用、簡素な管理、Web トラフィックのきめ細かい制御を実現します。フィッシング攻撃、エクスプロイト キットの配布、C2 に使用される可能性がある危険なサイトをブロックしつつ、業務に必要なリソースへの自由なアクセスを従業員に許可できるのです。

運用効率

パロアルトネットワークスのプラットフォームを通して Web 保護を実施することにより、セキュリティ スタックの総コストを削減し、運用効率を最大限に引き出せます。Advanced URL Filtering はクラウド アーキテクチャを採用しているため、Web 保護のために追加のアプライアンスを導入して管理する必要はありません。NGFW で有効にするだけです。弊社のクラウド提供型セキュリティ サービスを使用すればスタンドアロン ソリューションが不要になるため、3 年間で 990 万米ドルを節約し、リスクを 45% 減らせます [8]。また、各セキュリティ機能が互いを強化するプラットフォームを使用することで、ポイント ソリューションと比べて 30% 早く適切なセキュリティ体制を実現できます [9]。

パロアルトネットワークスのセキュリティ サブスクリプションの力

今日のサイバー攻撃は、量も質も向上し続けており、ネットワーク セキュリティ デバイスおよびツールを回避するために高度な手法が使われています。企業各社は、なるべくセキュリティ チームの負荷を増やさず、またビジネスの生産性を損なわずに、ネットワークを保護しなければいけません。弊社のクラウド提供型のセキュリティ サブスクリプションは、業界屈指の NGFW プラットフォームとシームレスに統合されており、インテリジェンスをコーディネートし、あらゆる攻撃経路を防御します。これにより、クラス最高の機能を提供する一方で、バラバラのネットワーク セキュリティ ツールを使うことによって生じる隙間を埋めることができます。市場をリードする各種の機能と 1 つのプラットフォームによる一貫したエクスペリエンスを利用することによって、最先端の検出回避型の脅威からもお客様の組織を保護することができます。Advanced URL Filtering と弊社のセキュリティ サブスクリプションを導入するメリットは以下の通りです。

5. *Mobile Threat Landscape Report 2020*、Wandera、2021 年 5 月 6 日にアクセス 、https://www.wandera.com/mobile-threat-landscape。
6. 「Top cybersecurity facts, figures and statistics」、IDG 社 CSO、2020 年 3 月 9 日、https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html。
7. *2020 Data Breach Investigations Report*、Verizon、2021 年 3 月 3 日にアクセス 、https://enterprise.verizon.com/resources/reports/dbir。
8. Forrester による *Total Economic Impact* 調査。
9. Andy Elder、「Managing Risks and Resources to Lower Your Cybersecurity TCO」、2022 年 1 月 26 日にアクセス、https://www.paloaltonetworks.com/cxo-perspectives/managing-cybersecurity-TCO。

表 1: パロアルトネットワークスのクラウド提供型セキュリティ サービス	
サービス	**説明**
Advanced Threat Prevention	既知のエクスプロイト、マルウェア、スパイウェア、およびコマンド アンド コントロール (C2) を阻止するほか、業界初のゼロデイ攻撃に対する防御機能を搭載しています。これにより、従来の IPS ソリューションと比べて未知のインジェクション攻撃を 60%、高度な回避技術を用いるコマンド アンド コントロール トラフィックを 48% 多く阻止します。
Advanced WildFire	業界最大の脅威インテリジェンスとマルウェア防御エンジンを利用して、高度な回避技術を用いるマルウェアを既知・未知問わず 60 分の 1 の時間で自動的に阻止し、ファイルの安全を確保します。
Advanced URL Filtering	既知と未知の脅威をリアルタイムに防御する業界初の機能によって、悪意のある URL の 88% を他社より 48 時間早く阻止。安全なインターネットアクセスを実現するとともに Web ベースの攻撃を 40% 多く防ぎます。
DNS Security	脅威のカバー範囲を 40% 拡大し、コマンド アンド コントロールとデータ窃盗を目的とした DNS 悪用の 85% を阻止します。インフラストラクチャの変更は不要です。
Enterprise DLP	どのクラウド提供型エンタープライズ DLP と比べても 2 倍以上のカバー範囲により、データ侵害リスクの最小化、ポリシーに違反するデータ転送の阻止、エンタープライズ環境全体で一貫したコンプライアンスを実現します。
SaaS Security	パロアルトネットワークスの SASE にネイティブ統合された業界唯一の次世代 CASB。SaaS の予防的な可視化、設定ミスに対する包括的な保護、リアルタイムのデータ保護、業界最高峰のセキュリティを実現します。
IoT Security	業界で最もスマートなセキュリティをスマート デバイスに導入してあらゆる「モノ」を保護することで 20 倍高速なゼロ トラスト デバイス セキュリティを実現します。
AIOps	AIOps for NGFW は予防的なセキュリティ体制の強化とファイアウォール障害の解決を実現し、セキュリティ チームによるファイアウォール運用のエクスペリエンスを再定義します。

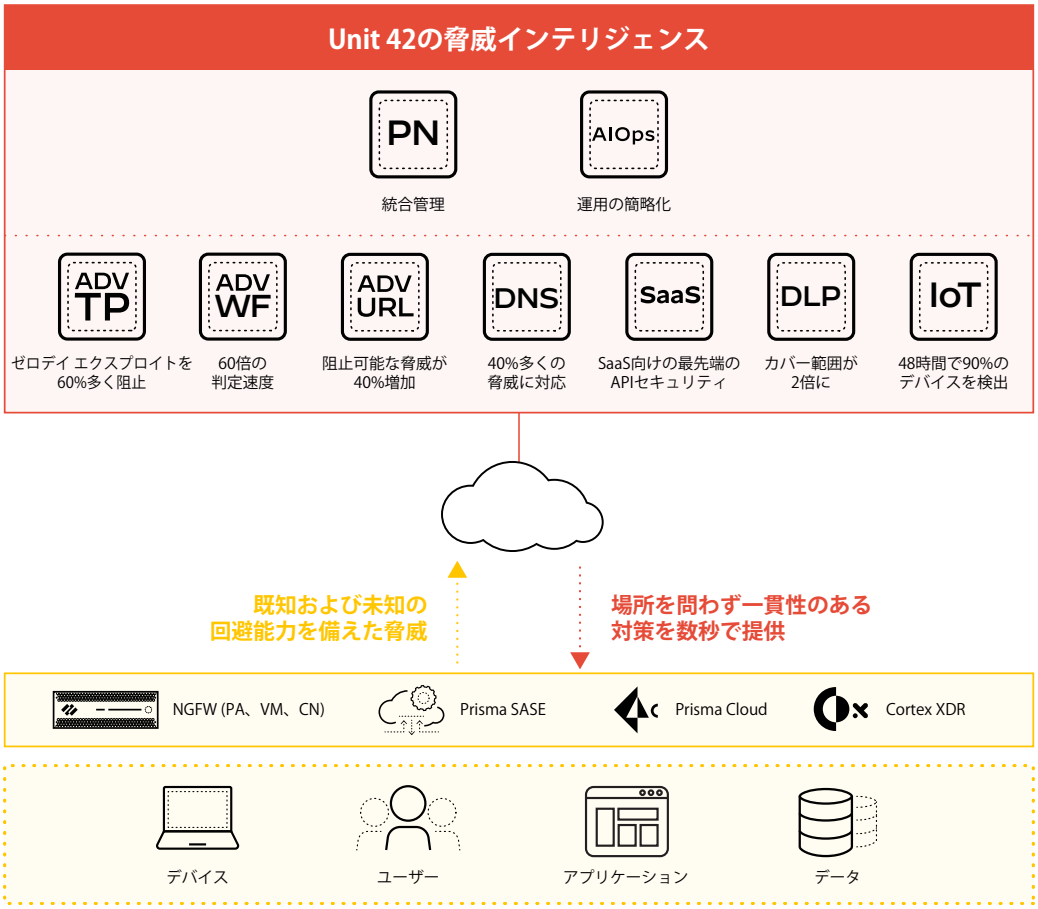

図 2: パロアルトネットワークスのクラウド提供型セキュリティ サービス

表 2: Advanced URL Filtering の機能	
機能	**説明**
インラインのリアルタイム Web 脅威防御	クラウドベースのインライン ML を使用して、実際の Web トラフィックを分析し、有害な URL をリアルタイムに分類してブロックします。新たな脅威および進化する未知の脅威 (フィッシング、エクスプロイト、詐欺、C2 など) を防御できるように、ML モデルを頻繁に再訓練しています。
回避技術への対策	クローキング、偽の CAPTCHA、HTML 文字エンコーディングなどの回避手法に対処できます。
URL データベース	静的分析、動的分析、機械学習による分析、および人間による分析を組み合わせて分類した数億件の既知の有害 URL/ 無害 URL のデータベースを維持しています。
コンテンツ カテゴリ	サイトのコンテンツ、機能、および安全性に基づいて Web サイトを分類。70 以上の無害および有害なコンテンツ カテゴリが含まれます。
リスク評価	リスクを判断するため、さまざまな要因に基づいて URL を評価します。セキュリティに重点を置いた URL カテゴリを利用してさまざまなレベルのリスクをもたらすが、有害サイトと断定されていないサイトに的を絞った復号とポリシーの適用を行うことにより、攻撃対象領域を削減できます。
マルチカテゴリのサポート	最大 4 つのカテゴリに URL を分類することで柔軟なポリシーの適用と、カスタム カテゴリの作成が可能になります。
カスタム カテゴリ	組織のニーズに合わせて、カテゴリやポリシーをカスタマイズできます。Advanced URL Filtering では定義されたカテゴリのセットを使用しますが、リスク許容度、コンプライアンス、規制、および利用規定に関するニーズは組織ごとに異なる場合があります。自社の要件を満たし、ポリシーを微調整するため、管理者は複数の既存のカテゴリを組み合わせて新しいカスタム カテゴリを作成できます。
認証情報の盗難をリアルタイムに阻止	サイトの URL カテゴリに基づいて、ユーザーが自社の認証情報を送信できるサイトを管理することで、認証情報の盗難を検出して防止します。誤検出を発生させることなく、信頼されていないサイトへの認証情報の送信をリアルタイムにブロックしながら、会社サイトや承認済みサイトへの認証情報の送信を許可できます。
フィッシング画像の検出	ML モデルを使用して Web ページの画像を分析し、フィッシング攻撃で一般的に使用されているブランドを模倣したものかどうかを判断します。
基準一致	URL カテゴリまたは基準に基づいて、複数のポリシー アクション タイプを指定できます。単にサイトをブロック / 許可するだけでなく、選択的な SSL 復号、高度なロギング、ダウンロードのブロック、認証情報の送信防止などのポリシーを実行できます。
選択的な SSL 復号	的を絞った復号によりさらにリスクを軽減できます。TLS/SSL で暗号化された Web トラフィックを選択的に復号することで、潜在的な脅威に対する可視性を最大化しながら、データ プライバシー規制を順守し続けるためのポリシーを設定することができます。特定の URL カテゴリ (ソーシャル ネットワーキング、Web ベース メール、コンテンツ デリバリー ネットワークなど) は復号し、その他の種類のサイト (政府、金融機関、医療機関など) については暗号化したままにすることを選択可能です。また、リスク評価が高または中に該当するコンテンツ カテゴリの復号を有効にする、単純なポリシーも導入できます。選択的な復号により、最適なセキュリティ体制を維持しながら、社内ポリシーまたは外部の規制により設定された機密トラフィックのパラメータを順守することが可能です。
翻訳サイト フィルタリング	ポリシーを回避する目的で翻訳サイト (Google 翻訳など) に入力された URL に Advanced URL Filtering のポリシーを適用します。
検索エンジンがキャッシュした検索結果の使用防止	Web 検索のキャッシュされた検索結果やインターネット アーカイブをエンド ユーザーが表示しようとした場合に、Advanced URL Filtering のポリシーを適用します。
セーフ サーチの適用	ユーザーの検索結果に不適切なコンテンツが表示されないようにします。この機能を有効にすると、最も厳格なセーフ サーチ オプションが設定されている Google、Yandex、Yahoo、または Bing 検索のみが許可され、その他の検索はすべてブロックされます。
カスタマイズ可能なエンドユーザー通知	管理者はカスタム ブロック ページを使用して、ユーザーに違反を通知できます。ページでは、警告を表示した上でユーザーに続行を許可することや、ポリシーの例外を許可するパスワード (変更可能) を要求することが可能です。
多言語サポート	41 言語でのクローリングと分析をサポートします。
レポート	事前定義済みまたは完全にカスタマイズされた Advanced URL Filtering レポートにより、Advanced URL Filtering と関連する Web アクティビティを可視化できます。

表 3: プライバシーとライセンスの概要	
Advanced URL Filtering サブスクリプションでのプライバシー	
信用とプライバシー	パロアルトネットワークスは、機密情報または個人を特定できる情報への不正アクセスを防止するために、厳格なプライバシーおよびセキュリティ管理を実施しています。セキュリティと機密性については、業界標準のベストプラクティスを適用しています。詳細は、プライバシー データシートを参照してください。
ライセンスおよび要件	
要件	パロアルトネットワークスの Advanced URL Filtering サブスクリプションを使用するには、PAN-OS 9.0 以降を実行するパロアルトネットワークスの次世代ファイアウォールが必要です。リアルタイム Web 分析は、PAN-OS 10.2 Nebula 以降でのみサポートされます。
推奨環境	Advanced URL Filtering は、インターネットの接続点に導入されたパロアルトネットワークスの次世代ファイアウォールとともに使用します。これは、ランサムウェア、マルウェア、グレイウェア、フィッシング、認証情報の窃盗、および C2 が外部との接続を必要とするためです。
Advanced URL Filtering のライセンス	Advanced URL Filtering はスタンドアロンのライセンスを必要とし、パロアルトネットワークスの次世代ファイアウォール向けの、クラウドベースの統合サブスクリプションとして提供されます。エンタープライズ ライセンス契約または Software NGFW Credits の一部として提供される場合もあります。

〒 100-0011
東京都千代田区内幸町 2 丁目 1 番 6 号
日比谷パークフロント 15 階
電話番号 : 03-6205-8061
www.paloaltonetworks.jp

parent_ds_advanced-url-filtering_110922