DNS セキュリティ

他のソリューションより、40% 多くの DNS 脅威をカバー

DNS (ドメイン ネーム システム) は攻撃に対して無防備です。散在しトラフィック量が非常に多いため、攻撃者は活動を簡単に隠すことができます。パロアルトネットワークスの Unit 42 脅威調査チームの調査によると、マルウェアの 85% が DNS を使用してコマンドアンドコントロール (C2) の手順を開始します。さらに攻撃者は、多様な技術を用いて DNS を悪用し、マルウェアの配信やデータを盗みます。残念ながら、セキュリティチームには DNS を悪用する手口に関する基本的な理解が不十分で、効果的な対処の妨げになります。現在のアプローチでは、自動化が不足、またはツールから連携の取れない膨大なデータが出力されています。回避可能で継続的な保守が求められる DNS インフラの変更が必要です。今こそ、DNS トラフィックのコントロールを取り戻しましょう。

ビジネス上の利点

- **最新の DNS ベースの脅威から組織を保護。**インライン機械学習によって、DNS を悪用する最新の攻撃を識別し、阻止します。
- **DNS セキュリティ ツールによって、コストを削減しベンダーを集約。**アラート、ポリシー、ルール違反、IDPS、Web セキュリティ、マルウェア分析、DNS をすべてカバーする連携のとれた単一のネットワーク セキュリティ スタックにより、NGFW への投資を有効活用し、作業時間を削減します。
- **ユーザーに影響を与えることなく、最新のセキュリティ イノベーションのメリットを享受。**モジュール式のクラウドベース アーキテクチャ上に構築される DNS セキュリティが、最新の検出・防御・分析機能をシームレスに追加。他の製品と異なり、再設定は不要です。
- **セキュリティ体制を最適化。**DNS セキュリティ分析ダッシュボードを使用して、重要な DNS トラフィックを NGFW で確実に保護できます。

DNS セキュリティはリアルタイム保護を実現し、業界初のセキュリティ保護対策を実施することで DNS を悪用した攻撃を阻止します。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) との緊密な統合によって、保護を自動化し、セキュリティ対策の回避を阻止し、多様なツールの導入や DNS ルーティングの変更が不要です。DNS セキュリティは、組織に重要な制御ポイントを新設し、攻撃を阻止します。

DNS セキュリティの特徴

DNS セキュリティは、クラウド上に構築されるサブスクリプション サービスです。NGFW とネイティブに連携して、DNS トラフィックのセキュリティ対策を行います。

共有の脅威インテリジェンスと機械学習 (ML) によって、DNS トラフィックに隠れた脅威を迅速に識別します。クラウドベースのセキュリティ対策の特徴は、即座に導入可能で、利用者数を自在に調整でき、常にアップデートされる点です。また、専用の分析ダッシュボードを使用すれば、DNS トラフィックを完全に可視化できるうえ、DNS セキュリティ サービスが検出した攻撃のコンテキストをワンクリックで表示できます。DNS セキュリティの機能は次のとおりです。

- 革新的なインライン機械学習アルゴリズムを使用。高度な新種の脅威を予測して攻撃を阻止。
- DNS 設定を変更してセキュリティ対策を回避しようとする攻撃を阻止。
- NGFW からサブスクリプションを有効化して管理するだけ。DNS トラフィックの再ルーティングや、手間のかかる変更管理プロセスは不要。
- パロアルトネットワークスのプラットフォームを通じて、DNS トラフィックのセキュリティ対策を実施することで実現。

主な機能

きわめて高度な最新の DNS ベース攻撃へのセキュリティ対策

脅威はマルウェアやフィッシングといった従来の手法にとどまりません。攻撃者は、DNS の脆弱性を利用して強固な C2 を確立する手法を生み出しました。これにより、インターネット上から、企業ネットワーク内部のホストに対する攻撃や DDoS (分散型サービス妨害) 攻撃を行います。さらに、ドメインを奪うことで企業の評判までも傷つけます。現代の DNS レイヤーのセキュリティ対策には、こうした攻撃を識別して阻止する能力が必要です。

巧妙な DNS レイヤーのネットワーク攻撃とデータ盗み出しの手口を検出して阻止するには、機械学習アルゴリズムが不可欠です。使用するアルゴリズムは、DNS トラフィックを迅速に分析して脅威に先回りできるこ

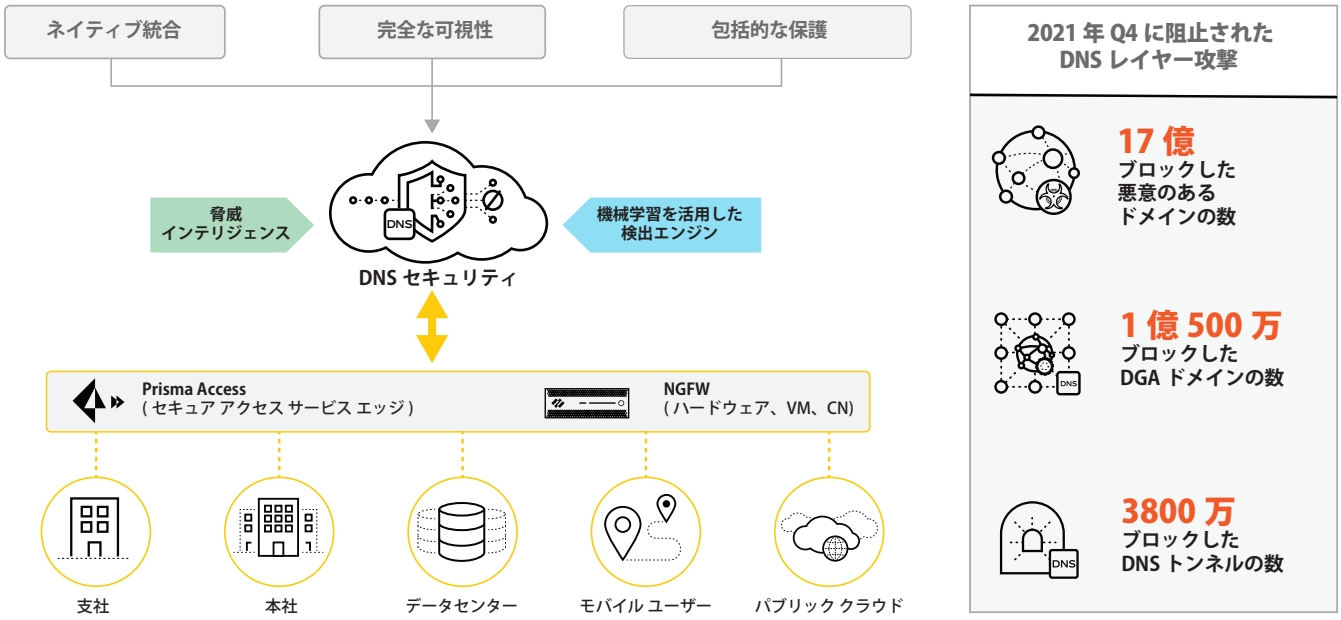

図 1: 業界トップクラスの保護機能で DNS トラフィックのセキュリティを確保

とが必要です。さらに、機械学習アルゴリズムの情報源となる強固な脅威インテリジェンスと、特定の攻撃の手口を阻止できるように設計された対策も必要となります。そのうえ、識別した悪意のある DNS アクティビティをブロックまたはシンクホール化するための、適用ポイントが必要です。

DNS セキュリティ サービス製品は、NGFW を通じた即時適用によって悪意のあるドメインを予測・阻止することで、自動化された攻撃へのセキュリティ対策を実施します。弊社が機械学習によって実現した検出エンジン (表2) は、増加している主要な DNS ベース攻撃を解決します (超低速 DNS トンネリング、ダングリング DNS、DNS リバインディングなど)。DNS セキュリティは、登録されたばかりの悪意あるドメインを、攻撃に使用される前に予測することも可能です。DNS セキュリティの包括的な業界最先端のセキュリティ対策を導入することで、DNS の設定・構成・導入モデルに関係なく、最も効果的なセキュリティを実現できます。

既知の脅威を阻止

DNS セキュリティ サブスクリプションは、数千万もの悪意のあるドメインに対する無制限のセキュリティ対策を実施します。リアルタイム分析と、常に拡充される国際的な脅威インテリジェンスを用いて、こうしたドメインを特定します。拡大を続ける巨大な脅威インテリジェンス共有コミュニティから提供されるデータを用いて、弊社はクラウド データベースを拡張しています。また、次のようなパロアルトネットワークスの情報源も使用します。

- 新しい C2 ドメイン、ファイルのダウンロード元ドメイン、悪意ある電子メールのリンクに使われるドメインなどを発見します。
- 新発見または未分類のサイトを常にクローリングして脅威インジケータをチェックします。
- 導入済みの数千の NGFW から見たドメイン解決履歴を把握し、1 日にペタバイト単位のデータを生成します。
- 攻撃者の追跡とマルウェアのリバース エンジニアリングを人の手で行います。世界中に展開されたハニーポットからの知見も提供します。
- 脅威インテリジェンスのサードパーティ ソースによってデータを補足することで、漏れのない対策を行います。

カテゴリベースのアクションを活用

DNS トラフィック タイプに特化したポリシーを作成します。すべての DNS クエリは、リアルタイムで弊社のスケーラブルなクラウド データベースと照合され、適切な対策が決定されます。DNS セキュリティは、DNS を悪用した脅威を機械学習によって迅速に検出・分類します。この分類を元に、きめ細かいポリシーベースのアクションを使用して、最も効果的なレスポンスを自動で実行します。ポリシーは、マルウェア、DGA、DNS

表 1: DNS セキュリティのカテゴリ

コマンドアンドコントロール (C2)	このカテゴリには、マルウェアや侵害されたシステムが攻撃者のリモート サーバーと密かに通信するために使用する URL とドメインが含まれます。攻撃者の目的は、悪意のあるコマンドの受信やデータの盗み出しです (ここには、DNS トンネリング検出や DGA 検出が含まれます)。
ダイナミック DNS (DDNS)	DNS セキュリティは、さまざまな情報源から取得した DNS データのフィルタリングと相互参照によって、悪用されている可能性がある DDNS サービスを検出し、候補リストを作成します。その後、候補リストを元に追加検証を行って精度を最大限高めます。
マルウェア	悪意のあるドメインは、マルウェアのホストと配布を行います。さまざまな脅威 (実行ファイル、スクリプト、ウイルス、ドライブ バイ ダウンロードなど) をインストールしようとする Web サイトを含むこともあります。
新規登録ドメイン (NRD)	新規登録ドメインとは、TLD のオペレータやエンティティによって最近追加された、今まで登録されたことのない新規ドメインを指します。新規ドメインは合法的な目的で作成される場合もありますが、大多数は、C2 サーバーの運用や、マルウェア、スパム、PUP/アドウェアの配布といった悪意のある活動を進めるためにしばしば使用されます。
フィッシング	フィッシング ドメインは、ユーザーを騙して個人情報やユーザー資格情報などの機密情報を送信させようとします。その手段として、合法的な Web サイトになりすまし、フィッシングやファーミングを通じてサイトにアクセスさせます。
グレイウェア	グレイウェア ドメインが直接的なセキュリティ上の脅威となることは通常ありません。しかし、攻撃の経路として利用される場合や、さまざまな望ましくない動作を引き起こす場合があります。あるいは、疑わしい/不快なコンテンツを含むだけということもあります。
パーク ドメイン	パーク ドメインとは一般的に活動していない Web サイトを指し、コンテンツはクリックスルー広告などに限定されます。ホストに収入を生むこともありますが、エンドユーザーの役に立つコンテンツは含まれないことが普通です。
プロキシ回避 & 匿名プロキシ	プロキシ回避と匿名プロキシは、コンテンツ フィルタリング ポリシーの回避に使われるサービスです。

トンネリング、C2、ダイナミック DNS、新規登録ドメインなどのカテゴリを元に、ブロック、アラート、またはシンクホールに設定します。管理者は、DNS トラフィックの詳細な分類 (表1) を使用してカスタム ポリシーを作成し、無害なドメイン、悪意のあるドメイン、疑わしいドメインを個別に扱うことができます。

感染したシステムを識別して検疫

自動化によって感染の拡大を阻止します。自動化された動的なレスポンスによって感染マシンを発見し、ポリシーに従って迅速に対処します。DNS を使用した攻撃を識別した場合、セキュリティ管理者は NGFW で悪意のあるドメインをシンクホール化するプロセスを自動化できます。これにより、C2 を遮断してネットワーク上の感染ユーザーを迅速に特定し、さらには隔離することが可能です。また、悪意のあるドメインのシンクホール化、ダイナミック アドレス グループ (DAG)、ロギング アクションを組み合わせることで、検出とレスポンスのワークフローを自動化できます。そのため、他のソリューションで必要とされる手作業にアナリストが時間を取られることはありません。

DNS 分析から知見を取得

セキュリティ対策の実行に必要なコンテキストを、セキュリティ担当者に提供します。脅威レポート機能により、脅威に関するより深い知見が得られます。さらに、次の機能によって、DNS トラフィックを完全に可視化できます。

- 使いやすいダッシュボードにあらゆるドメインの完全な履歴が表示されます。発信元ドメインの特定、悪意あるドメインの確認、インシデントのトリアージとレスポンスのサポートに役立ちます。
- DNS イベントに関するコンテキスト。クエリされているドメインの種類とその頻度、タイムスタンプ、各ドメインのパッシブ DNS 情報、WHOIS 情報、関連するマルウェアのタグを表示します。
- セキュリティ衛生。事業所全体で NGFW によってどのようなセキュリティ機能が有効化されているかを継続的に追跡し、盲点を迅速に除去できます。

あらゆるタイプの DNS トラフィックの検査

プレーンテキストの DNS、DNS over TLS (DoT)、DNS over HTTPs (DoH) など、あらゆるタイプの DNS トラフィックを可視化して保護します。未知のリゾルバに向かっているものも含まれます。

- ファイアウォールでの復号を利用して、暗号化 DNS トラフィック (DoH や DoT など) を検査します。
- ネットワーク内の感染ユーザーのシンクホールと検疫を行います。
- AIOps を活用してすべての DNS トラフィックを完全に可視化します。傾向に関する知見も含まれ、すべてが 1 つのダッシュボードに表示されます。
- 未知の DNS リゾルバに向かうものも含め、すべてのタイプの DNS トラフィックのセキュリティを確保します。

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

クラウド配信型セキュリティ サービスによって、高度な脅威を検出・阻止

近年、サイバー攻撃の数と質が向上しています。30 分あたり 45,000 種に相当する亜種が出現しているうえ、複数の攻撃経路や高度な技術を用いて悪意のあるペイロードが企業に送られるようになっているのです。従来の連携が取れないセキュリティ対策のままでは、組織がユーザー、デバイス、アプリケーションを保護するのが困難です。セキュリティ ギャップが生まれ、セキュリティ チームの管理オーバーヘッドが増加し、一貫性のないアクセスと可視性によりビジネスの生産性が低下します。弊社のクラウド提供型セキュリティ サービスは、業界最先端の次世代ファイアウォール プラットフォームをシームレスに統合しています。80,000 社のお客様がもたらすネットワーク効果を利用して、即座にインテリジェンスを連携させ、あらゆる攻撃経路からのあらゆる脅威にセキュリティ対策を実施します。すべての事業拠点を漏れなくカバーできることに加え、業界最高クラスのセキュリティ対策が常にプラットフォームに配信されます。これにより、きわめて高度で捉え難い脅威にも対応したセキュリティ対策を実施できます。

運用上の利点

DNS セキュリティ サブスクリプションにより、次のことが可能です。

- **導入が容易**。NGFW プラットフォームと緊密に統合されているため、サービスを有効化するだけで導入できます。DNS トラフィックを外部のリゾルバに再ルーティングする必要はありません。そもそも、攻撃者はこのようなリゾルバを簡単に回避できます。
- **パフォーマンスに影響を与えないセキュリティ対策**。高度なセキュリティ対策を、DNS クエリに対してシームレスかつリアルタイムに実施するため、ビジネスに影響がありません。
- **DNS トラフィックに対する完全な可視性を維持**。ネットワーク セキュリティ エンジニアや SOC アナリストはダッシュボードを使用し、組織の DNS 利用状況を迅速に確認して評価できます。
- **DNS カテゴリによってカスタマイズされたレスポンス**。DNS トラフィック タイプに応じたレスポンスを自動化することで、リスク プロファイルに沿ったポリシーを容易にセットアップできます。

表2: クラウド提供型セキュリティ サービス	
Advanced Threat Prevention	業界初のゼロデイ攻撃阻止を活用しながら、既知のエクスプロイト、マルウェア、スパイウェア、コマンドアンドコントロール (C2) の脅威も阻止します。従来の IPS ソリューションよりも、未知のインジェクション攻撃を 60% 多く阻止し、高度な回避能力を備えた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、60 分の 1 の時間で既知および未知の、高度な回避能力を備えたマルウェアを自動的に防御することで、ファイルの安全を確保します。
Advanced URL Filtering	業界初の既知および未知の脅威のリアルタイム防御によって、インターネットへの安全なアクセスを確保し、Web ベースの攻撃を 40% 多く阻止します。悪意のある URL の 88% を、他社より少なくとも 48 時間早く阻止します。
DNS セキュリティ	脅威に対する保護範囲を 40% 拡大し、コマンドアンドコントロールとデータ窃盗のために DNS を悪用するマルウェアの 85% を阻止します。インフラストラクチャを変更する必要はありません。
Enterprise DLP	クラウド提供型エンタープライズ DLP の 2 倍のカバー範囲で、データ侵害リスクを最小化し、ポリシー違反のデータ転送を阻止し、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可能にします。
SaaS セキュリティ	パロアルトネットワークスの SASE に統合された業界唯一の次世代 CASB で、プロアクティブな SaaS 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、業界最高のセキュリティを提供します。
IoT セキュリティ	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、セキュリティ チームがプロアクティブにセキュリティ体制を強化し、ファイアウォール障害を未然に解決可能にすることで、ファイアウォールの運用エクスペリエンスを再定義します。

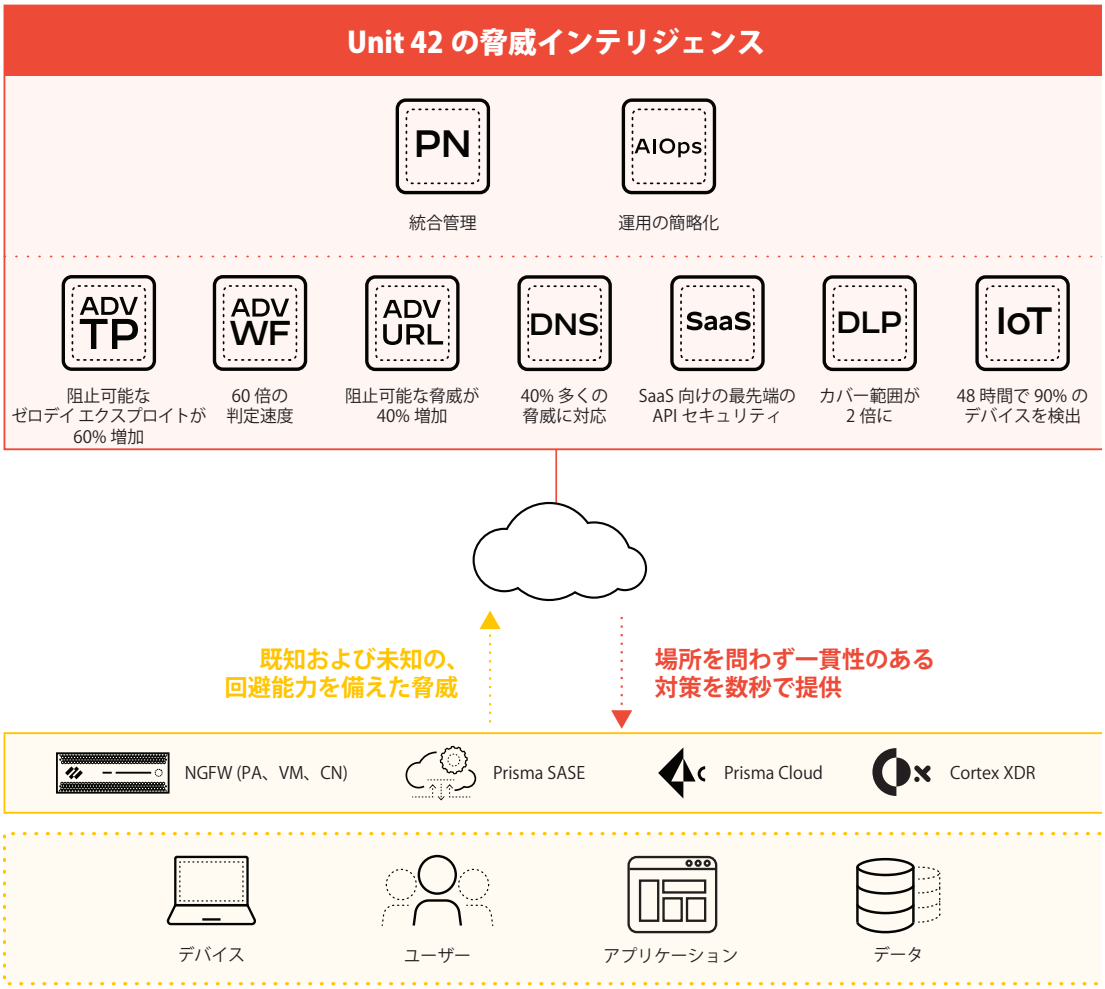

図 2: クラウド提供型セキュリティ サービスによって、高度な脅威を検出して阻止

表 3: DNS セキュリティ機能	
機能	**説明**
機械学習ベースのインライン保護	機械学習ベースの分析により、高度な DNS ベース脅威を特定 (DNS セキュリティ検出機能の下にリスト化)。
クラウド データベース	何千万もの既知の悪意のあるドメインが記録されており、フィッシングやマルウェアをはじめとする高リスク カテゴリのブロックに利用できます。
DNS セキュリティ分析	脅威レポート機能を提供。DNS トラフィックだけでなく、セキュリティ イベントや経時的なトラフィックの傾向に関する完全な DNS コンテキストも確認できます。
DNS シンクホール	既知の悪意あるドメインへの DNS クエリに対するレスポンスを変更することで、悪意のあるドメイン名を、指定可能な IP アドレスに解決してクライアントに与えることを可能にします。クライアントがシンクホール アドレスにアクセスしようとすると、その活動を記録し、自動化されたアクション (検疫など) を起動します。この技術は、ネットワーク上の感染ホストの特定に利用できます。
DNS セキュリティのカテゴリ	個別のポリシー アクションを定義できるうえ、特定のシグネチャ タイプに対する重大度レベルを記録できます。使用するネットワーク セキュリティ プロトコルと脅威の性質に応じて、個別のセキュリティ ポリシーを作成可能です (例: C2、ダイナミック DNS、マルウェア、新規登録ドメイン、フィッシング、グレイウェア、パーク ドメイン、プロキシ回避、匿名プロキシ)。
DNS セキュリティ検出機能	
ドメイン生成アルゴリズム (DGA)	DGA の使用を識別します。DGA とは、マルウェアが C2 サーバーへのコールバックに用いる、ランダムなドメインをその場で生成する技術です。
辞書に基づく DGA	ディクショナリに基づく DGA ドメインを特定します。
DNS トンネリング	DNS トンネリングの利用を阻止します。DNS トンネリングとは、DNS プロトコルを悪用し、クライアント サーバ モデルでマルウェアなどのデータのトンネリングを行う技術です。
超低速 DNS トンネリング	超少量/低速の DNS トンネリングを阻止します。この攻撃手法は、複数のドメインにトンネル化されたデータとエクスプロイトを拡散し、通信速度を大幅に抑えることで検出を回避します。データを盗み出す目的や、ネットワークに悪意のあるペイロードを追加送信する目的で使われます。
戦略的熟成ドメイン	予約され、数か月の休眠後に攻撃者が使用するようなドメインに、ユーザーが接続しないように保護する予測分析です。
ファスト フラックス ドメイン	ファスト フラックスを阻止します。これは、サイバー犯罪者が使用する、ボットと DNS レコードを次々に切り替える手法です。ファスト フラックス ネットワークは、フィッシング、マルウェアの拡散、詐欺、ボットネットの運用に使われます。
侵害ドメイン ゾーン	評判の良いドメインのハッキングされた DNS ゾーンに密かに追加されたドメインから保護します。
DNS リバインディング攻撃	DNS リバインディング攻撃を阻止します。この手口は、インターネット上の攻撃者が企業ネットワーク内部で横方向に移動して、社内サービスを攻撃する際に使用される可能性があります。
ダングリング DNS 攻撃	ダングリング DNS 攻撃を阻止します。これは、古くなった DNS ゾーン データを悪用してドメインを乗っ取る攻撃です。企業の評判を傷つけたり、フィッシング攻撃を展開したりする用途に使われます。
ワイルドカード DNS	ワイルドカード DNS レコードの使用によって攻撃者が悪意のあるドメインにユーザーを誘導することを阻止します。
DNS 侵入	悪意のあるペイロードをネットワークにトンネリングするための DNS プロトコルの悪用を阻止します。
NXNS DoS ドメイン	DDoS 攻撃の展開に使用されるおそれがあるドメインに、ユーザーが接続することを防ぎます。
悪意のある新規登録ドメイン (NRD)	予測分析によって、攻撃者が登録したドメインを登録時点で識別します。

表 4: プライバシーおよびライセンスの概要	
DNS セキュリティ サブスクリプションとプライバシー	
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。詳細については、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 DNS セキュリティ サブスクリプションを利用するには、次の要件を満たす必要があります。 • PAN-OS 9.0 以降を実行する Palo Alto Networks Next-Generation Firewall • パロアルトネットワークスの脅威防御ライセンス
推奨環境	DNS セキュリティを、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合わせて使用すること。悪意のあるドメインやトンネリングなど DNS を悪用する脅威は、外部との接続を必要とするためです。
DNS セキュリティのライセンス	DNS セキュリティ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。また、パロアルトネットワークスのサブスクリプション ELA、VM-Series ELA、Prisma Access の一部としても利用可能です。

〒 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