netskope

SOLUTION BRIEF

次世代 Secure Web Gateway

ユーザー、地域またはデバイスに関わらず、マルウェア防御、高度な脅威検知、カテゴリ別のWebサイト フィルタリング、データ保護、アプリ／クラウド サービスの管理をサポートする次世代Secure Web Gateway（次世代SWG）です。他の製品にはないシングルパスのインラインプロキシによって、クラウドや Webの暗号化トラフィックを復号し、インスタンスやアクティビティを可視化・制御します

概要

- インスタンス、アクティビティ、データを分析する、Webやクラウドのための粒度の高いポリシー制御
- 異常検知を伴うシングルパスでの高度な脅威防御とデータ保護
- SaaSなどのクラウドやSWGに対し、DLPなどの共通のポリシー制御を適用できる一元的で統一されたコンソール
- 8年以上に渡り、フォーチュン100選出企業を保護してきた成熟したインライン プロキシ
- あらゆるユーザー、デバイスまたは場所からの通信を保護する、クラウド型で提供される高いパフォーマンスとグローバルな拡張性

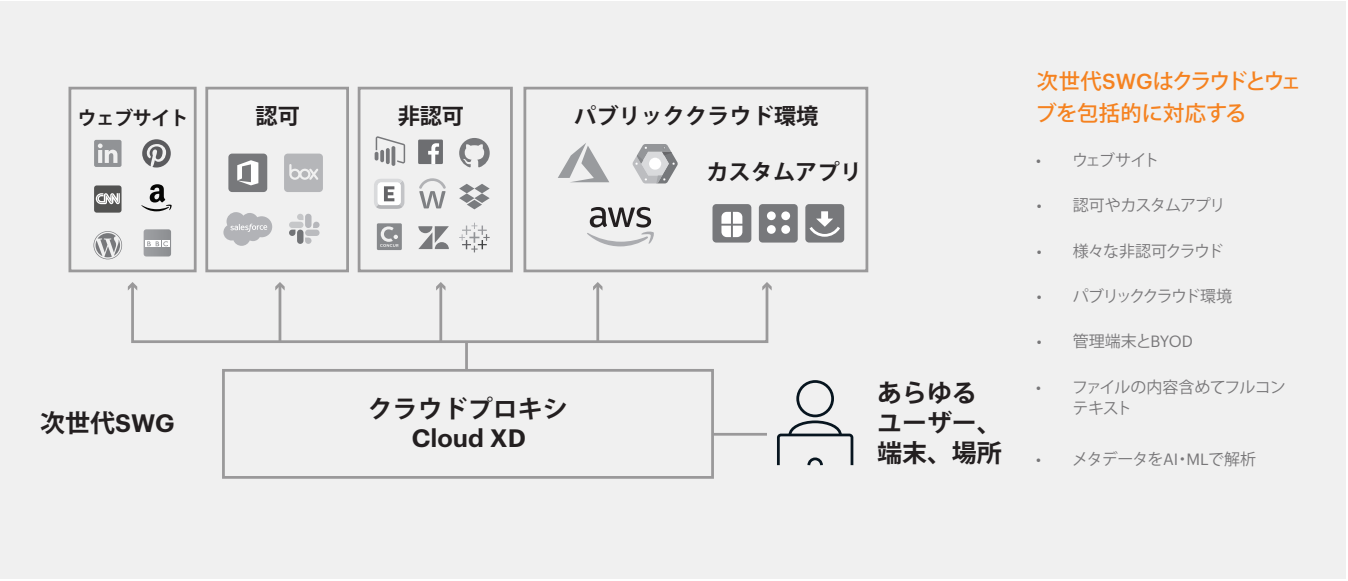
企業において、平均して89%のユーザーがクラウドを活用し、2,415種類のクラウド アプリを使用しています。そのうち98%がアンマネージド クラウド アプリです。

変化するWEBセキュリティの情勢

現代の企業は平均して89%のユーザーがクラウドを活用し、2,415種類のクラウド アプリを使用しています[1]。そのうち、98%以上がアンマネージド クラウド アプリです。従来型のAPI保護はマネージド アプリしか保護できませんが、Netskopeの次世代SWGはインライン(クラウドプロキシ型) で、数千種類のクラウド アプリを復号します。クラウドでの脅威は、2019年に検知された脅威全体の44%を占め、1,609種類以上のアプリにおいてすべてのキルチェーン ステージに及んでいます[2]。さらに悪いことにSaaSは、ホワイトリストなどで守る従来型の防御を、信頼の置けるドメインや有効な認証情報を悪用して回避する攻撃の主な標的となっています。

クラウドの普及と共に、可視性の欠如や、コンテキストを把握しない粒度の低い許可／ブロック制御が原因で従来型のWeb防御が、今までのセキュリティの境界の外にあるデータの流れを見逃す問題が発生しています。データは、クラウド アプリの企業インスタンスから個人インスタンスへ、マネージド クラウド アプリからアンマネージド クラウド アプリへ、また低リスクのクラウド アプリから使用すべきでない高リスクのクラウドアプリへも自由に移動できます。アクティビティやその異常な振る舞いに限らず、コンテンツそのものや全体的なコンテキストも理解するには、インスタンスを認識するだけでは十分ではありません。次世代SWGは、セキュア アクセス サービス エッジ（SASE）アーキテクチャの中心として、クラウドやWebに対してデータに基づく粒度の高いポリシー制御を提供します。

[1] 2020 Netskope Cloud and Threat Report
[2] Ibid



Cloud XDによる粒度の高いポリシー制御

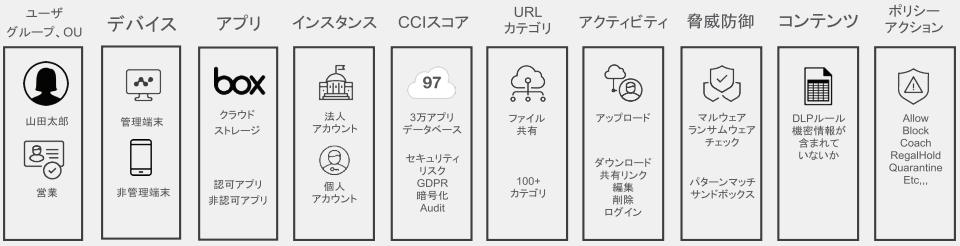
現代の動的なWebサイトは、クラウド アプリやサービスと同じ言語を使用しています。クラウドの脅威と機密データの移動を可視化させるためには、次世代SWGソリューションにこの言語のデコード機能を搭載することが極めて重要です。アンマネージド アプリにデータが移動するようになれば、使用するデバイスや場所に関わらず、ユーザーのセキュリティを確保できるクラウド ベースのSWGが普及します。その結果、SWG、クラウド／インライン型SaaS、DLP機能の収束化が進み、クラウドやWebトラフィックに対して高度な脅威防御とデータ保護を適用することできるようになります。

従来型のWeb防御における「許可」または「ブロック」しかできない粒度の低いポリシー制御は、今、ユーザー、アプリ、インスタンス、リスク評価、データ、そしてアクティビティのコンテンツとコンテキストも理解する粒度の高いポリシー制御に置き換えられています。アプリの、企業インスタンスで機密データのアップロードなどのアクティビティが発生していても問題はないかもしれませんが、個人インスタンスで同様のアクティビティが行われている場合は、データ漏洩や退職間際の従業員によるデータの窃盗を意味しているのかもしれません。

次世代SWGを定義する

従来型の防御でセキュリティ問題を解決しようとしても、多くの問題が残ります。マネージド クラウド アプリのAPI保護を利用してWebトラフィックをCASBに繋げることに注目した従来型のSWGと言えば完璧なソリューションに聞こえますが、各事業部門やユーザーがデジタルトランスフォーメーションの一環として自由に取り入れた、シャドーITを含む数千種類のアンマネージド クラウド アプリの存在を見逃しています。これらのクラウド アプリを許可／ブロックする制御を従来型のSWGに追加するか、次世代ファイアウォール（NGFW）やクラウドアプリを使用することは、データフロー、クラウドの脅威やコンテキストの把握しかできません。クラウド アプリのセキュリティ面でのリスク評価に基づき、リスクの高いアプリをブロックし、ユーザーに安全な代替手段について指導する場合でも、やはり一部のクラウド アプリでは、アクティビティ、コンテンツ、コンテキストの見逃しを「誘発」することになります。実際には、クラウドの普及やデータの可動性が原因で、従来型のSWG、NGFW、さらにはエンドポイント保護ですらコンテキストを可視化することができず、以前ほどの効果を失っています。

さまざまな理由から、データやコンテキストが次世代SWGの中心に、そしてSASEアーキテクチャの中心的原理になっています。データセンターの持つセキュリティ境界の外に移動するユーザーが増えたため、クラウドDLPは必要不可欠なソリューションになりました。ユーザーは日常の業務で、Web、マネージド アプリ、アンマネージド アプリ、パブリック クラウド、クラウドベースのプライベート アプリにアクセスしています。これら5つのアクセス先のすべてにデータが移動していますが、インラインのクラウドDLPルールやポリシーであれば保護することが可能です。キルチェーンのすべてのステージの全域にクラウドの脅威が存在し、クラウド フィッシング詐欺などの手法を使ってアクセス権を侵害し、エンドポイント保護などの従来型の防御を回避しています。次世代SWGは従来のWebログに留まらず、豊富なメタデータを提供し、機械学習を使って、クラウドやWebトラフィックに潜む脅威や異常な振る舞いを検知します。



Cloud XDエンジンできめ細かなポリシー制御

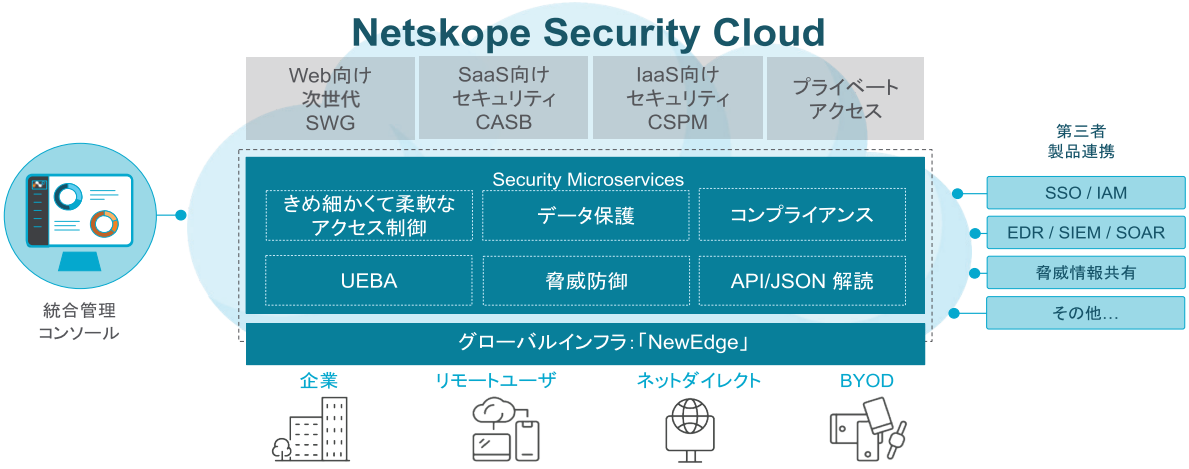
- ユーザー、グループ、OU
- 管理端末、個人端末（BYOD）
- URL、アプリ、カテゴリー、リスク度
- 会社と個人アカウント
- アクティビティとファイル内容
- 高度な脅威防御
- 情報漏洩対策(DLP)
- 内部不正対策と異常な行動の検知

粒度の高い制御、メタデータ、異常な行動をするユーザーの検知

防御ですべての問題を解決できれば理想的です。しかし現実は、セキュリティ チームが検知、調査、対応を行い、遡及的に新たな脅威インテリジェンスを適用しなければなりません。そのためには、次世代SWGを介して、アプリ、インスタンス、データ、アクティビティが存在するWebやクラウドのトラフィックに関する豊富なメタデータを提供する必要があります。メタデータは、内部関係者による脅威やアカウントの侵害など、高度な脅威やユーザーの異常な行動・振る舞いを検知する機械学習モデルの原動力です。許可／ブロックによる制御はもう通用しません。粒度の高い制御が可能な「許可」を実現し、豊富なメタデータを収集し、調査や対応、機械学習ベースでのユーザーの異常行動検知機能などにそのメタデータを活かすことが必要です。次世代SWGは、Webおよびクラウドのトラフィック全体について、必要なデータやコンテキストを可視化させます。これは従来型のSWGでは不可能なことです。

独自のSASEアーキテクチャを構築できる柔軟性

変更には時間がかかります。優れたアーキテクチャ計画はコアから始まります。Netskopeの次世代SWGは、クラウドネイティブなコアに拡張性のあるマイクロサービスを利用し、セキュリティ トランスフォーメーションの進行に合わせて、セキュリティ機能を追加します。次世代SWGにNetskope Private Accessを組み合わせれば、先ほどの5つのアクセス先に加え、ゼロトラスト ネットワーク アクセス（ZTNA）のための完璧なソリューションを提供し、データセンターとパブリック クラウド内のプライベート アプリへ安全にアクセスすることが可能になります。脅威保護は、標準分析、高度分析（振る舞い分析を含む）から選択でき、DLP（情報漏洩対策）も、標準的なものと高度なものの 2 つから選択できます。これらの共通のプラットフォーム保護やポリシーは、パブリック クラウド環境内のマネージド クラウド アプリやクラウド セキュリティ ポスチャ管理（CSPM）に対するCASB APIベースの制御についても、共通の管理コンソールから適用することができます。



NetskopeはSASEのアーキテクチャに基づき、多くの機能をもつマイクロサービスをクラウドネイティブなプラットフォームにより提供します。また、データのコンテキストを分析し、ポリシーによるきめ細かい通信の制御を実現します。

NETSKOPEの次世代SECURE WEBGATEWAY（次世代SWG）パッケージ内容	PROFESSIONAL	ENTERPRISE
クラウド セキュリティ プラットフォーム		
グローバルなNewEdge Network – 大手クラウド プロバイダと幅広く結合され、ハイパースケール、キャリア向けプライベート ネットワーク、グローバル データセンター、最短RTT（往復遅延時間）での高速パフォーマンスを実現	Y	Y
トラフィック フォワーディング – Web、クラウド、デスクトップ アプリ、モバイル アプリ、同期クライアント操作のためのクライアント、またはオフィス向けGREおよびIPsecトンネル	Y	Y
フォワード／リバース プロキシ – クライアントありのマネージド デバイスからクラウドやWeb、およびクライアントなしのアンマネージド デバイス（BYODなど）からマネージド クラウド アプリに対応	Y	Y
Cloud XD – 数千種類のクラウド アプリをデコードし、アクティビティやインスタンスの認識を含め、コンテンツやコンテキストを提供することで、粒度の高いポリシー制御を実現	Y	Y
認証 – 各種SSO／MFA／IAM、SAML、AD、LDAP	Y	Y
TLSインスペクション – TLS v1.3のネイティブサポート、ポリシー制御による除外	Y	Y
アナリティクスとレポーティング – Webやクラウドのあらゆる使用データについて、90日間のデータ保持要件を基準に、契約ごとに延長可能な標準レポートやアドホック クエリに対応。データのエクスポートやオープンAPIによる第三者ソリューションとの統合も可能	Y	Y
Cloud Threat Exchange – エンドポイント保護プラットフォーム（EPP）、セキュリティ情報・イベント管理（SIEM）、インシデントレスポンス（IR）などのソリューションに対する設定不要で使える統合機能の活用、また、独自のIOCを追加することで、セキュリティ スタックやエンドポイント保護とIOC情報を共有可能	Y	Y
クラウド セキュリティ サービス		
Cloud Confidence Index (CCI) – クラウド アプリやサービスのリスク評価、3万3,000件以上のエントリが含まれるデータベース、ポリシー制御によりユーザーに安全な代替手段を指導(コーチング)	Y	Y
URLフィルタリング – カテゴリ 120種類以上、言語200か国以上、カスタム カテゴリ、YouTubeカテゴリ、翻訳サービス、安全な検索、サイレント広告ブロック、未評価Webページの動的評価、サイト検索ツール、再分類サービス、カテゴリまたはドメイン別のトラフィック検査に対応	Y	Y
標準的な脅威対策 – マルウェア対策エンジン、クライアント トラフィック悪用対策、ファイルタイプの識別、40種類以上の脅威インテリジェント フィード、PE（Portable Executable）ファイルのベアメタル サンドボックス分析、UEBAの異常パターン ルール	Y	Y
高度な脅威対策 – 350種類以上のインストーラ、パッカー(自己解凍型圧縮ファイル)、圧縮ファイルの難読化の解除と再帰的な解凍。3,500種類以上のファイル形式に対応し3,000種類以上の静的バイナリ脅威インジケータの実行前分析とヒューリスティック分析。30種類以上のファイルタイプ（実行可能ファイル、スクリプト、文書を含む）のベアメタル サンドボックス分析。Netskopeが管理する複数の機械学習モデルとエンジンに加え、第三者製サンドボックスとリスクベース検査（RBI）を統合		Y
UEBA（ユーザーおよびエンティティの行動分析） – インサイダーの脅威、アカウントの侵害、およびデータ抽出に関するUEBA機械学習モデルと、カスタムUEBA異常パターン ルール、ユーザー信頼性スコアリング、時間軸に沿ったイベント相関分析、ユーザースコアに基づくポリシー対策		Y
標準的な情報漏洩対策（DLP） – クラウド アプリ／サービス、Webトラフィック、ファイルおよびフォームのための移動データ分析。GDPR、PCI、PHI、PII、ソースコードなど、40種類以上の規制コンプライアンス関連テンプレートを含む。3,000種類以上のデータ識別子を利用し、1,400種類以上のファイルタイプと、カスタム正規表現、パターン、辞書に対応。また、AI・機械学習ベースの標準文書分類も追加	Y	Y
高度な情報漏洩対策（DLP） – 類似ベースおよび完全一致ベースのインライン型データ マッチングによるファイル フィンガープリンティングを含む。また、AI・機械学習ベースのインライン型文書（特許、ソースコード、納税書など）および画像（スクリーンショット、運転免許証、身分証明書、パスポート）分類も追加		Y

netskope

Netskopeはクラウドセキュリティのリーディングカンパニーです。企業や組織がセキュリティを犠牲にすることなく、最大限クラウドやWebを利用できるように するためのソリューションを提供いたします。特許取得済みのCloud XD テクノロジを使用し、あらゆるクラウドサービスやWebサイトでのユーザーのアクテ ィビティを可視化・制御します。それによりお客様は、360°のデータ保護および脅威防御である「スマートクラウドセキュリティ」を手に入れることができます。ご興味をお持ちの方はぜひ弊社のWebサイト(www.netskope.com/jp)にお越しいただくか、japan@netskope.com へご連絡ください。