提供：

netskope

SASE アーキテクチャの設計

for dummies®
A Wiley Brand

クラウドセキュリティを知り尽くす

アプリ、データ、セキュリティ、ネットワークの大きな変化に適応する

ユーザーエクスペリエンスの改善と維持

Jason Clark
Lamont Orange
Steve Riley

Netskope 特別版

Netskope の概要

SASE の大手企業 Netskope は、ネットワークの内外にかかわらず、あらゆるデバイスからユーザーをインターネット、アプリケーション、インフラに安全かつ迅速に直接接続します。Netskope には CASE、SWG、ZTNA が単一のプラットフォームにネイティブに備わっており、どこでも高速で、データ中心で、クラウド対応に優れています。さらに、デジタルシチズンシップの採用により総所有コストが削減できます。詳しい情報は、www.netskope.com をご覧ください。

本書の出版にあたり、ご協力いただいた数多くの皆様に感謝申し上げます。

Netskope より：Amanda Anderson, Mike Anderson, Chad Berndtson, James Christiansen, Tom Clare, Mark Day, David Fairman, Maxwell Havey, Scott Hogrefe, Kathy Jacobsen, Greg Mayfield, Mariesa Milan, Sasi Murthy, Krishna Narayanaswamy, Lauren Polito, Kate Reid, Zoe Revis, Brian Tokuyoshi

Evolved Media より：Karen Queen, Evan Sirof, Lauren Wagner, Dan Woods

SASE アーキテクチャの設計

Netskope 特別版

Jason Clark, Lamont Orange, Steve Riley 共著

SASE アーキテクチャの設計 For Dummies®, Netskope 特別版

出版元：
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-85535-4 (ペーパーバック); ISBN 978-1-119-85513-2 (電子書籍)

製作：アメリカ合衆国

10 9 8 7 6 5 4 3 2 1

謝辞

本書の出版にあたりご協力いただきました皆様に心より御礼申し上げます。

プロジェクト編集者：Elizabeth Kuball
アキジションエディター：Ashley Coffey
編集責任者：Rev Mengle
事業開発担当：William Hull
プロダクション編集者：Vivek Lakshmikanth
特別協力：Nicole Sholly

はじめに

皆様の会社の従業員、提携先企業、そして顧客も、プライベートネットワークやデータセンターの使用からクラウドへと移行しています。セキュリティ上の課題は移行を阻害できません。一方で、従来のセキュリティツールを依然として使用している企業の経営者は、自社の管理の及ばない環境に対してセキュリティを再編することに苦心しています。セキュリティとユーザーエクスペリエンスの間でバランスをとるのは「平時」には困難なことですが、新型コロナウイルスのパンデミックという未曾有の危機が、数多くの従業員に在宅勤務を強いることになりました。

セキュリティをめぐる環境が複雑化して、最高のセキュリティチームでさえ課題に直面し、設定ミスや脅威侵入の可能性を増大させています。また、矛盾する製品やサービス、つじつまの合わない業界のメッセージなどが、ニーズに合わせてセキュリティを再構成しながらビジネスチャンスを掴みたいセキュリティ部門の意思決定者の悩みの種となっています。

今後の解決の方向性を示してくれるのは、SASE（Secure Access Service Edge）と呼ばれる新しいネットワーキングとセキュリティのアーキテクチャです。SASE アーキテクチャの重要な構成要素は NG-SWG（次世代セキュアウェブゲートウェイ）、CASB（Cloud Access Security Broker）、ゼロトラストの原則です。これらが主要なネットワーク サービスとネットワーク セキュリティサービスを統合してシステムを一元化し、クラウドによるビジネス上の利益と利便性の向上を実現します。これを然るべき方法で、正しい順序で構築するにはどうすればよいのか？その疑問にお答えするのが本書です。

本書の概要

本書は、ネットワーキングとセキュリティのプロジェクトを実施するためのロードマップ作りに役立ち、短期的には段階的なプラスの効果をもたらしながら、クラウドファーストで耐障害性に優れた安全な将来への道を切り拓きます。いわゆる SASE ベンダーのマーケティング戦略にはまることなく、SASE とは何かを実践的な面から理解することができます。また、セキュリティとネットワークへの投資を将来を見据えたものにすることで、不可避な変化への対応を可能な限り容易に、かつ費用対効果の高いものにすることができます。

対象読者

インターネットについてはよくご存知でしょう。仕事とプライベートの両方で使用する幅広いクラウドベースのデジタルツールが存在しますが、その多くはセキュリティや IT 部門が承認どころか関与すらしていません。また、クラウドは、個人と企業の両方の認証情報やデータが攻撃対象となってきた、危険をともなう場所であることもご存知と思います。そして、あなたは会社、従業員、株主、顧客、ビジネスパートナーを守るため、この課題を解決したいと考えています。

本書で使用するアイコン

注目していただきたい重要情報の左側に、次のようなアイコンを表示しています。それぞれの意味をご紹介します。

ヒントのアイコンは、特定の作業を容易にするショートカットとお考えください。

ポイントとして、特に重要な、覚えておいてほしい内容を記載しています。

このアイコンが出てきたら、読み飛ばしても特に問題はないような、専門的な技術情報を提供しています。

後々、皆さんの頭痛の種にならないよう、注意を促す内容を記載しています。

本書を読み終えた後で

本書には豊富な情報を盛り込んでいますが、読み終えた後で「もっと知りたい」と思われたら、www.netskope.com をご覧ください。

本章の内容

- クラウド時代にセキュリティの本質はどう変化してきたか
- クラウド以前のセキュリティ対策によって起こる新たな問題とは
- SASE がビジネス向けクラウドを実現する方法
- SASE アーキテクチャを構築して持続性あるビジネス価値を創造する
- マーケティング戦略による SASE の誤解を解く

第1章 クラウドファーストな企業に向けたセキュリティ対策、SASE のビジョン

クラウドという言葉が頻繁に使われるようになりましたが、その意味を正確に理解するのは実は簡単なことではありません。アプリケーションという観点から端的に言うなら、クラウドには次のような意味があります。

- **プライベートクラウド：**データセンター内のアプリケーション。
- **パブリッククラウド：**IaaS（Infrastructure as a Service）やPaaS（Platform as a Service）など、さまざまな要素が含まれる場合がありますが、ここではシンプルに、公衆インターネット上で利用可能なアプリケーションをパブリッククラウドとします。

» **仮想プライベートクラウド：**パブリッククラウドからアクセス可能なプライベートアプリケーション。

» **SaaS（Software as a Service）：**サードパーティベンダーにホストされ、インターネットを介してアクセスされるアプリケーション。

このように気軽にクラウドという言葉を使ってしまうと、それが皆様の持つニーズに対応するかどうか、選択肢としてふさわしいのかなどを見極めるのが難しくなります。そのため、問題を明確化し、セキュリティにどんな機能を求めるのかを理解するところから始める必要があります。これはクラウドを利用する上で、常に念頭においておくべきことです。

本章では、クラウドはセキュリティをどう変化させてきたか、クラウド以前のセキュリティがクラウド時代に通用しなくなる理由、ヘアピニングなどの従来型のネットワーク形態が役に立たない理由、クラウド環境に SASE（Secure Access Service Edge）を活用してセキュアで生産性の高い働き方を実現する方法、そして最高レベルの SASE の定義要素について解説します。

NO MORE「ニッチ」

クラウドの中心に潜む脆弱性は、もはや「ニッチ」な問題とはみなされません。2021 年の現状：

- 組織で使用されているクラウドアプリケーションの数は、1 社当たり前年比で 20%増加した。Netspoke は 2021 年 2 月のレポートで、従業員数が 500 人から 2,000 人の組織が 1 カ月間に使用しているクラウドアプリ数は平均で 664 と発表。
- この Netspoke のレポートによると、2020 年 12 月時点でマルウエアダウンロードのうち 61%がクラウドストレージやコラボレーションアプリへの侵入を原因とし、2020 年 1 月の 48%から増加している。
- ウェブトラフィックで、セッションの 55%はアプリやクラウドサービスに関連するものだったと、同レポートは述べている。
- また、このレポートによると、83%のユーザーが会社所有のデバイスから個人のアプリにアクセスしている。ビジネスユーザー、顧客、データ、その他の大切な資産の安全を常に確保しながらも、クラウドが提供する柔軟性、コスト管理、ビジネスチャンスへの新しい手法などを最大限に活用すること、これこそが喫緊のセキュリティ課題である。

クラウドはセキュリティとネットワークをどう変えてきたか

その昔、ビジネス界の要塞として守りを固めていたのは企業のデータセンターでした。企業はデータセンターという城を築き、その城壁の中でビジネスアプリケーションを構築、展開していました。城の内部に張り巡らされたプライベートネットワークにより、本部の従業員、離れた支社の社員、世界中を駆け巡る出張している社員などがデータにアクセスしていました。

大きな城には明瞭な境界線がつきものです。この要塞も門を備えた城壁で守られていました。門の先にある、危険がつきまとうインターネットからの出入りは厳しく規制され、数少ない保護されたネットワークの通路を流れるトラフィックを門番が常に見張り、信頼できるものを入れ、不審なものを排除し、問題の兆候があれば直ちに行動をおこすことで安全を確保していたのです。外界とのすべてのやり取りは、プライベートネットワークの狭い空間を行き来することを余儀なくされていました。

クラウドベースのアプリに惹きつけられるビジネスユーザーの数は当初は少数でしたが、しだいに増加し、激流となりました。ソーシャルメディアで繋がったりコラボレーションするためだけでなく、売上や財務、マーケティング、顧客関係などのデータを高速処理するためにも、クラウドベースのアプリケーションは単に、会社が提供するものよりも優れていたのです。その後、多くの企業をはじめ、動きの遅い政府機関もクラウドベースのアプリを採用し始めました。今日、企業は SaaS アプリケーションを好んで使用しているだけでなく、ビジネス上の課題をクラウドソリューションで解決し、重要なシステムをクラウドに移行することを義務付けるクラウドファースト方針を全面的に採用しつつあります。

新しい、パワフルなアプリケーションがクラウドで使用可能になったことで、変化が起きたのです。ネットワークの内外を問わず、人、デバイス、アプリケーションはモバイル化しています。長期にわたる開発に加えて、ハードウェアとソフトウエアの調達も必要になる従来の手法に比べて迅速かつ質の高い、素晴らしい機能を企業に提供できるのが SaaS 製品です。

Synergy Research Group の調査によると、過去 10 年間の変化で、クラウド展開のための支出が顕著に増大して、IT 予算での他の支出項目を大きく上回るようになりました。2024 年までに、システムインフラ、インフラソフトウェア、アプリケーションソフトウェア、ビジネス プロセス アウトソーシングにかかる IT 関連支出の 45%以上が従来のソリューションからクラウドに移行し、クラウドコンピューティングはデジタル

時代の黎明期以来、IT 市場に持続的かつ破壊的影響を与えるテクノロジーの１つになるとガートナー社は予測しています。

しかも、こうしたクラウドベースのツールの多くは可視化されず、依然として IT 部門の管理外にあります。セキュリティの観点からするとこれは非常に大きな問題です。ですが、セキュリティは単にクラウドベースのアプリを保護するだけではありません。

セキュリティとは、従業員全員がリモートで働くようになった時にも、必要なすべての保護を提供することでもあるのです。どこにいようとも、ユーザーを攻撃から守り、データやアプリケーションの安全を確保するための防御策を講じる必要があります。一方で、ネットワークの観点からは、安全を担保するだけでなく機能性も求められます。ユーザーがクラウドを使用して、場所を問わずに、より多くの仕事をより速くこなせるようになった時、セキュリティがボトルネックとなって生産性を損なうようなことがあってはならないのです。

次に検討するのは情報です。データ（知的財産から売上高、顧客のクレジットカード番号までのあらゆる情報）は、企業が保有する貴重な資産であり、おそらくは、取扱い製品そのものよりも価値が高いものでしょう。事実、IT セキュリティがトップニュース扱いになるのは驚くことでもなく、それは多くの場合、よいニュースではありません。データ、アプリケーションがクラウドに存在し、それを従業員がクラウドを利用して運用している現在、オンプレミスのデータセンターや従来型インフラストラクチャ向けに開発された古いセキュリティ技術で追いつくことはもはや至難の業です。世界では、さまざまなハッカーが洗練された技術を駆使して、クラウドアプリケーションやそのアクセス方法の脆弱性を突いて、大混乱を引き起こす攻撃が急増しています。

クラウドへの移行は、今のところ容易でもシームレスでもありません。データセンターネットワークを走る古い通路に散在しているのは、生産性を低下させ、ユーザーを疲弊させ、セキュリティを危険にさらす障害物、頭痛の種、非効率性の山。データセンターに導入されたアプリケーションは、生産性、ユーザーエクスペリエンス、利便性の点で SaaS アプリケーションよりも見劣りします。SaaS によって待望の改善が実現したことで、営業担当者の売上は増加し、マーケティング担当者は最良の広告を打ち、人事部は最適な人材を見つけることができ、製品開発者は迅速に仕事を進めることができるようになりました。SaaS を導入しないのは、前例のない高い生産性を手放すことと同じです。そんなことを望む企業はありません。

ここで問題となるのは、SaaS アプリケーションの利用には城壁の中にあるデータが必要になること。ただし、アプリケーションは城壁の外側にあり、セキュリティで管理も保護もされていないことです。企業のセキュリティ部門には、クラウド上、つまり「外」に存在するものはほとんど制御できないことを前提に、ノーと言うか、見て見ぬふりをするかという 2 つの選択肢があります。これが現在、シャドー IT と呼ばれているもの。つまり、ユーザーや部門全体が IT やセキュリティを迂回して、便利ではあっても企業として業務での使用は認められていない Salesforce や Google Docs などの SaaS ツールや Dropbox などの大容量ファイル共有ツールを使用する慣習です。シャドー IT は何年も前からありましたが、クラウドの普及に伴ってその使用（そして危険性）が加速してきています。従来の企業のデータセンター向けのツールキットを使用して、古い手法でアプリケーションの追跡とコントロールをしてきたセキュリティ担当者が窮地に陥るのも当然です。

従来のセキュリティでは常に妥協を強いられます。スピードや柔軟性などの基準を上げる選択をすると、セキュリティの基準を犠牲にすることになりますが、SASE は、適正に機能すれば、これらを*可能*にします。問題に最も近いところにいる人々が、安全で管理された方法でテクノロジーを使ってイノベーションを起こし、問題を解決することを可能にするのが SASE です。

クラウド以前の時代に普及したセキュリティに潜む問題

クラウド時代以前のセキュリティツール、テクニック、テクノロジーは今でもあらゆる場所で使用されています。本書の読者が勤務する企業の IT インフラにも使用されている可能性は高いのです。このような状況で、多くのセキュリティ「対策グッズ」が出回っても、その結果はセキュアでも効率的でもないというのが現実です。この根深い問題の原因は通常は 2 つ、間違ったアプローチか戦略が全くないアプローチかのどちらかです。

間違ったアプローチ

企業のデータセンターのメリットとセキュリティの有効性とは、会社のデジタル資産を単一の安全な場所に置いておくことができることでした。そして、企業は独自にプライベートネットワークを構築し、本社や支社の従業員をつなぎ、データセンター内の必要な情報へのアクセスをコントロールすることができました。

企業がデータセンターを必要とすることに変わりはありません。ただし今ではデータセンターはユーザーやデータが行き交う数多くの場所の 1 つにすぎません。ビジネスの必要性という点からも、単一のセキュリティ管理ポイントとしても、データセンターはもはや中心的な存在ではありません。

データセンターのセキュリティシステムは、特定の限られた機能を果たすアプライアンスと呼ばれる物理的なボックスをデータセンターに接続するのが普通です。長年にわたり、企業がセキュリティシステムを調達してきたベンダーの数は数百にも上ると言われています。2021 年時点では、平均的な企業では数十種類のセキュリティ製品を購入し導入しています。ほとんどの場合、こうした製品は連携して動作するよう設計されていないため、セキュリティ担当者がこれらすべてのシステムを統合して、クラウドアプリケーションやテレワーカーをサポートするポリシーを適用できる、組織化された適応型のセキュリティソリューションにするのは不可能です。

多くの場合、多様なシステムはコンソールの乱立につながります（そして、誰がどのコンソールを担当するかという議論が起こります）。セキュリティ担当者やネットワーク管理者が直面する混沌とは、それぞれ独自の優先順位を持ち、一斉に注意を促してくる数十の異なる管理画面との闘いです。問題の診断に追われているときに、全体像や単発の状況を早急に理解することは非常に困難です。このようなセキュリティ管理手法は受身的で、発生した事象の再現や診断にはログが頼りという場合が多いのです。さらに悪いことには、スパゲッティのように絡み合ったシステムでは、全体の安全を確保するための秩序を確立することはできません。システムに秩序と安全性を実現するには、実に多種多様なデジタル情報のやり取りにおいて、自動的にセキュリティを維持するための機能を組み込むきめ細かいルールを構築する必要があります。

セキュリティの役割は単に「No」を突きつけることではありません。ビジネスをより迅速かつ効果的に進めることに対して、特に分散して働く従業員に対しては、「Yes」と返したいのです。セキュリティにとってユーザーとデータの保護は最優先事項ですが、一方では、目まぐるしく変化する要件にリアルタイムに対応しなければなりません。これは言い換えれば、高い生産性と成果を上げることのできるツールを利用して必要なデータにアクセスできる環境を用意し、場所を問わずにスムーズで生産的なワークエクスペリエンスをユーザーに提供することです。

アプローチの欠如

ユーザーはあらゆる場所にいる。ネットワークの設計で念頭に置くべきなのは、この点です。ユーザーがどこにいたとしても、のすべてのトラフィックをデータセンターの多数のセキュリティサービスに繰り返し通

す行為は生産性を低下させます。（セキュリティやネットワークの専門家は、このような処置を「ヘアピン」と呼ぶことがあります。ユーザーは目的地に直接向かうことはできず、常に速度を落としながら進路を変更させられます。）ヘアピンすることでビジネスシステムの使い勝手は悪くなり、パフォーマンスは大幅に低下し、ユーザーの不満は募るばかりになります。

こうした新しい環境をコントロールするのはどれほど大変なことなのでしょうか？事例を示しましょう。米国国立標準技術研究所（NIST）は、組織にサイバーセキュリティに関する指導をするよう米国議会から義務づけられています。NIST が発表した「サイバーセキュリティ・フレームワーク」では、組織内のアプリケーションのセキュリティを確保するにあたって考慮すべき 400 の管理ポイントが特定されています。これは、多い数ではありません。ユーザー、データ、アプリケーション、ネットワークなどのすべてがオンプレミスに設置されていると想定しているので、少ないのでしょう。そして、その想定は、もはや通用しません。

SaaS アプリケーションの場合、ネットワーク内に存在するユーザーやサービスに対する広範なコントロール機能は、セキュリティシステムとして機能しません。従来より遥かに広い視野でリアルタイムに機能するセキュリティ戦略を立てて、そのすべてを 3 つの管理ポイントで実行してください。

- SaaS アプリケーションに出入りする、自社が保有するデータ
- これらのアプリにアクセスしている各ユーザーの ID
- 自社のビジネスが外部のエンティティと取引しているかどうかに基づく承認


ポイント

クラウドセキュリティの成功を左右するのは、最重要項目の再調整です。従来のセキュリティシステムでは主にアクセス制御に主眼が置かれていました。前述した、城の城壁と門番のようにです。しかし、城と城壁のアプローチはもはや通用しません。クラウドセキュリティを成功に導くには、アクセスではなくアクティビティに焦点を移すべきです。つまり、誰が何をして、どのようにアプリケーションが使用され、データがどこに転送されているのか。城のたとえに飽きたなら、バスケットボールで考えてみてください。境界ベースのゾーンディフェンスから、動きを基本としたマンツーマンディフェンスに切り替える時が来ています。


技術情報

従来のセキュリティシステムは、インターネット上でのユーザーの動きを把握していました。しかし、SaaS アプリケーションの場合、ユーザーが見たい Web ページを表示させるのに何十、何百、時には何千もの追加リソースに依存している可能性があります。クラウドを保護するには、こうした詳細な点まで把握する必要があります。従来のツールにはトラ

ンスポート レイヤー セキュリティ（TLS）の復号化のような機能がないため、ユーザーがアプリケーションと通信する際にトラフィック内で何が起こっているかを把握できません。こうしたツールには、ユーザーが他のリソースとデータを交換するために SaaS アプリケーションが用意している、アプリケーション プログラミング インターフェース（API）での情報に焦点をあてることができません。こうした詳細情報なしに、データが安全かどうか、ユーザーが閲覧している内容の情報ソースが適正かどうかを確かめる術はありません。

SASE の定義

程度の差はありますが、SASE の定義は、ネットワークセキュリティの境界管理をクラウドに移行すると同時に、その管理をより高速に、さらにアプリケーションやユーザーの違いを認識し、何よりも、データを中心に考えるということです。

別のレベルから見ると、セキュリティとネットワークのための新しいアーキテクチャ戦略を意味し、今後組織は SASE の実現に向けて努力することになります。クラウドを中心とした世界ではセキュリティとネットワークに最新のモデルが求められている事実があり、一方では、セキュリティ、ネットワーク、アプリケーション、データ保護のすべてが変化する環境への基本的な対策が必要です。これらに対応するのが SASE というわけです。

機能的には統合され、連携して機能する複数のセキュリティとネットワークのサービス一式が SASE です。ユーザーにクラウドへのアクセスを許可するだけでなく、ユーザーの活動、デバイス、使用するアプリケーションを継続的に監視し、ユーザーエクスペリエンスを損なうことなく、データを常時どの場所からでもセキュアに扱えるよう構築・提供されています。嬉しいことに、SASE のセキュリティアーキテクチャの基盤は、今日からでも、計画的かつ段階的に導入することができます（第 5 章を参照）。


注意

SASE のセキュリティアーキテクチャのあらゆる側面が、クラウド上あるいはクラウドでの使用を目的として構築されているのが大きな特徴の１つです。データセンター向けのデバイスやコードは、SASE の用途では使用されません。その理由についてはもうご存知でしょう。データセンター向けのセキュリティサービスはアクセスの制御を主な目的としているため、クラウドの言語ともいえる、エンド間のトラフィックフローに内包される細かいニュアンスや詳細情報を豊富に含む情報（コンテキスト）を処理することはできません。今後のセキュリティやネットワークについて検討する際は、これを念頭に置いてください。

コンテキストは非常に重要で、この新しいセキュリティアーキテクチャがどれほど深く、優れているかを知る情報源として有用です。SASE のコンテキスト情報には次の要素が含まれます。

- ユーザーの ID
- アクセス要求に使用されているデバイス
- アクセスが試みられている位置の情報
- クラウドでアクセスしているアプリケーションの ID
- 要求されているデータ（その内容および保存場所）
- ユーザーの行動パターン
- アプリケーションインタラクション（ユーザーが具体的に何をしようとしているか）

そして、SASE のセキュリティシステムはこの動的な情報ストリームを常に評価しながらも、以下を決定するポリシーに基づいてセキュリティを適用します。

- 適用するネットワークサービスのサービスレベルとタイプ
- 適切な種類のデータ暗号化
- データの悪用防止のために適用されるデータ保護のレベル
- 適用する認証のレベル
- CASB（Cloud Access Security Broker）など、特定の専門セキュリティサービスを使用して、さらに対象活動の監視を強化する必要があるかどうか

ご覧のように、SASE のアーキテクチャにはさまざまな要素が含まれています。真に機能する SASE が正しく実装されれば、セキュリティとネットワーク接続の品質は大幅に簡素化され、劇的な改善を見せるでしょう。継続的なリスク管理を含め、すべてのことをリアルタイムで実行するには SASE を適切に実行しなければなりません。セキュリティサービスをデータセンターからクラウドに移行し、ユーザーの近くに配置することで、誰に、そしてどこで何が起こっているかを常に可視化し、コントロールを強化することができます。SASE は、新しいアプリケーションやビジネスモデルへの移行に取り組むネットワークやセキュリティ担当チームを支援しながら、同時に、従来のオンプレミス型アプリケーションへのアクセスも保護します。

SASE のビジネス上のメリットを理解する

セキュリティに SASE モデルをなぜ採用するかは、ビジネスにおいてクラウド使用の有益性が広く認識されるようになったことと深く関係しています。クラウドの使用によって、人々や企業はより効率的に、より協力しつつ、より迅速かつ柔軟に、よりコスト効果の高い仕事ができるようになります。こうした進歩を安全に実現するのが SASE です。

デジタルトランスフォーメーションを実行する企業の成長を促す

セキュリティの役割は、高速走行中の車のブレーキに例えることができます。高速走行が可能なのは必要に応じてブレーキをかけることができるからで、それによってリスクをより素早く管理できます。ビジネスを減速させたり、スピードを制限したり、スピードを上げさせないためにブレーキが存在するわけではありません。

セキュリティ管理を変革することなく、安全な方法でデジタルトランスフォーメーションを行うことはできません。あらゆる企業が成長を加速させたり、顧客にアプローチするために新しいテクノロジーを採用しているなかで、IT 組織は、ユーザーやデータを追跡できるセキュリティ管理に移行すること、プロセスから多くの摩擦を取り除くことで、企業を力強く支援することができます。ユーザーが求めるアプリやアクセスを提供するとともに、それらを安全に使用する方法をタイミングよく指導するとよいでしょう。

変化に対応する

ビジネスのあらゆる側面を網羅して重要なサービスを提供するクラウドですが、日々新たなユースケースが登場しています。読者の企業でも、ユーザー向けのクラウドサービスをいくつか承認しているはずです。また、個人や組織全体にとって、仕事の質、スピード、コストの面でより優れた未承認のクラウドサービスがあれば、組織内の誰かがもう利用している可能性は高いでしょう。この場合、ユーザーは企業のセキュリティスタックを回避し、利用料を支払い、アプリをダウンロードして日々の仕事で使っています。

コストの削減

セキュリティに関する決まり文句に、「セキュリティは高くつくと思っているなら、セキュリティ侵害を試しにやってみるといい」というのがあります。IBM と Ponemon が実施した調査によると、データ侵害でかかる総費用の平均は 386 万ドルです。ほとんどの企業はセキュリティの必要性を認識していますが、被害を受けるまで、どれほど重要なことかほぼ理解していません。

セキュリティはコストセンターと認識されることが多く、最適に機能している限り目立たない存在です。実際にはセキュリティが備わっているからこそビジネスが可能になるのですが、この本質的な役割を脇に置いても、セキュリティ予算は潤沢であるかどうかにかかわらず賢明に使用する必要があります。セキュリティに対して賢く、効率的な支出をする。このことに多くの企業は依然として頭を悩ませております。

SASE が可能にするのは、費用対効果の面での大きなメリットです。セキュリティサービスを高度に統合した SASE のアプローチでは、データセンターに設置された多くのセキュリティアプライアンスの機能が統合されるため、設備投資を削減することができます。監視とメンテナンスにかかるシステムの数も減るため、運用コストも低減できます。さらに、ベンダーの統合、ネットワーク設計の改善、およびクラウドプロバイダーとの効率的な連携などからの費用削減効果も期待できます。

SASE は、世界中で課題となっている熟練したサイバーセキュリティ人材不足の解決にも役立ちます。検知と応答の動作の多くを自動化することで、スキルの高い人材をより高い価値を生む活動に再配置できます。例えば、新たなビジネス活動を加速させるセキュリティポリシーの開発や、セキュリティインフラの自動化と柔軟性を向上させる人工知能（AI）モデルの構築などが挙げられます。SASE アーキテクチャは、他のどんな企業セキュリティフレームワークと比べても、チームの構成員をよりよく、生産性を向上させることに寄与できます。

維持すべきなのはシンプルさ

セキュリティ上の脅威となるインシデントが頻発してきていますが、その主な原因の 1 つはヒューマンエラーです。その背景には、従来のセキュリティやネットワークシステムが本来意図されない目的のために使用され、セキュリティアナリストが手に負えないほど複雑な問題に直面してしまう、という状況もあるのです。こうしたシステムが日々格闘しているのは、互いに共通言語を持たず、管理者もその言語を使用しない、何十もの監視アプリケーションという形で存在する現代のフランケンシュタイン級の怪物です。このような状況に対して明確なプランを提供し、多くのセキュリティサービスが理解し合い連携して機能できるようにするのが SASE です。

SASE の通説を暴く


注意

たぶん、本書はあなたが SASE に関して初めて読んだ For Dummies 本ではないでしょうし、最後でもないと思いますが、本書を最高の内容にするのが私の仕事です！冗談はさておき、数ある新テクノロジーやトレンドと同様に、SASE についても誤った情報は溢れるほどあります。製品名の

頭に「*i*」をつけただけで自動的にデザインが洗練されるわけはないですし、「*e*」をつけたところでパワーや効率性が向上するわけではありません。同じように、SASE はすでに多くの人々に選ばれ、過剰なほど販売され、誤解されています。ここで、よくある通説をいくつか検討してみます。

通説：SASE はレガシーテクノロジーでも対応可能

今日のネットワーク セキュリティ インフラは、長年（場合によっては数十年）にわたる開発と販売の努力により培われたものです。しかし、いくらパッチをあてたり、微調整したり、ライセンスを上げたりしても、従来のアプライアンスが魔法のようにクラウドネイティブなセキュリティソリューションに生まれ変わることはありません。クラウドには新しいアプローチが必要なのです。

通説：SASE は標準の SWG を基盤にして構築できる

従来の SWG（Secure Web Gateway）はアクセス制御と Web の脅威に対する防御に特化していましたが、SASE の守備範囲は、アプリケーション、クラウドサービス、データ保護、データ損失防止などの広範に及ぶものです。（第 2 章では、次世代 SWG [NG-SWG] サービスが幅広いニーズにどう対応しているかを詳しく解説します。）

通説：SASE を導入しても既存のネットワークアーキテクチャは維持できる

SASE は、ポリシーを適用する制御ポイントがエッジに設けられ、ユーザー、デバイス、アプリケーションがやり取りする場所の近くに存在し、その効果を発揮します。この近接性こそが、SASE に動的なセキュリティ機能を与え、ユーザーが最高の生産性をあげる（しかもストレスなく）ためのパフォーマンスと信頼性を提供しています。

通説：SASE はすべてのネットワークトラフィックを可視化する必要はない

SASE が効果的なのは、まさにセキュリティ対策のためのオール・イン・ワンのアプローチだからです。ユーザー、データ、アプリケーションに関するコンテキストを開発する能力（基礎となる API も含む）が SASE のパワー、シンプルさ、インパクトの源泉です。SASE が機能するには可視性が必要です。それによって得られる豊富なコンテキストこそが、従来のデータセンターに比べてコントロールポイントがはるかに少ない環境においても SASE が効果的に機能する理由です。

通説：SASE は複雑化を増長させる

複雑さはセキュリティやネットワーク担当者にとって悩みの種であり、ニュースで報じられるセキュリティ上の失敗例の大半に共通する課題です。SASE では、ネットワークセキュリティに関わるすべての要素が調和して機能することが必要です。バラバラに寄せ集められた従来のネットワークセキュリティでは、ポリシーとその適用場所が完璧に調和し、急速に変化しつづける要件に適応できる、単一で統合されたクラウド セキュリティ アーキテクチャという SASE のビジョンを実現することはできません。

通説：SASE は SD-WAN を使ってネットワークから始める必要がある

ネットワーク技術が進歩した結果、SD-WAN（Software-Defined Wide Area Networking）は、WAN（Wide-Area Network）の管理・運用を大幅に簡素化し、MPLS（Multiprotocol Label Switching）などの従来ある接続技術に対抗する有用な（そして、より費用対効果の高い）選択肢になりえます。SD-WAN の有用性を否定することはできませんし、SASE を構築する重要な要素として決して無視できるものではありません。一方で、SD-WAN に注力している多くのベンダーは、「SD-WAN は SASE を実現するための正しい選択肢」という飛躍した販売戦略をとっていますが、これはひいき目に言っても不誠実です。SD-WAN や、さらに言えばファイアウォールも、SASE に到達するための唯一の道ではありませんし、最も重要な構成要素でもありません。

通説：SASE にはベンダーの新しいエコシステムは必要ない

企業が過去からの古い遺産（旧来の製品、偏見、思考、投資など）を完全に捨て去ることは事実上不可能です。他の企業や技術を買収してきた歴史を持つ企業や、深い井戸に組織としての知識の源泉を蓄積し、それを重要資産とみなしている企業は、それらの重荷から解放されるのに苦労しています。SASE はネットワークとセキュリティに対する新しいアプローチです。昨日のソリューションを明日のニーズに合わせようとすると、将来よりよい一歩を踏み出すことができません。

本章の内容

- クラウドネイティブなセキュリティ実現への要件
- クラウドに適したセキュリティを SASE が構築する方法
- NG-SWG が真の SASE の重要な構成要素である理由
- NG-SWG の実際を概観する

第2章 次世代セキュアウェブゲートウェイの重要性

最近まで、セキュリティ戦略の多くは Web の脅威に焦点を当てていました。これは、当然のなりゆきです。クラウドサービスが普及する以前、Web トラフィックや E メール内の Web リンクがデジタル空間での脅威の主要因だったからです。セキュリティ部門の戦術は、従来のセキュアウェブゲートウェイ（SWG）、ウェブ フィルタ、企業ネットワークに広く普及しているプロキシ設定などを駆使しながら、Web の性質に合わせてきめ細かく調整されていました。

このような方法は、ほとんどの従業員が会社のビル内で勤務し、企業ネットワークを介してリソースやインターネットに接続していた時代には理にかなっていました。しかし、今日、ユーザーが「作業中」という時、多くの場合はリモート、モバイル、ネットワーク間の移動中、さらに、クラウドで作業中という状態にあります。自宅で仕事をしたり、作業が捗るカフェで仕事をするユーザー、客先に行ったり、出張する社員、彼らはさまざまなデバイスを使っており、ネットワーク、アプリ、データが常時あらゆる場所に分散する、動的なユーザー集団を作り出しているのです。

クラウド時代にセキュリティ強化が必要なのは明らかです。ですが、空港でチェックインの行列に並んだことがあるなら、セキュリティの強化が必ずしもその向上を意味しないことも、よいユーザーエクスペリエンスを保証しないことも承知されているはず。空港では、TSA 事前審査や旅客信頼性プログラムを通して、搭乗客をより速くゲートに案内することができるようになりました。保安手続の主要な側面は、空港での警備員による検査などから、乗客が空港に到着する前に始まる審査のプロセスへと移行しました。こうした手続きによって乗客のエクスペリエンスを向上させるとともに、システム全体の安全性を確保し、効率性を高めることが目的です。

NG-SWG（次世代セキュアウェブゲートウェイ）は SASE（Secure Access Service Edge）への重要な一歩であり、SASE への道のりの大部分を短期間で完成に近いレベルまで到達できる、最初のステップとして採用する企業が増えています。

従来の手法からの脱却

旅行業界がフリークエントトラベラーに提供した優遇プログラムと同様のパターンで、セキュリティ業界も、高いセキュリティを提供する方法と場所を検討する必要に迫られました。従来世代のセキュリティハードウェア製品は、ネットワークやデータセンターを保護するように設計されており、クラウドアプリケーションは範疇外です。また、ユーザーがクラウドに期待する柔軟性や即応性を提供する設計にもなっていません。

新しい成果を求めて従来のアプライアンスを使用しようとする様なこのミスマッチでは、耐えられないほど複雑なセキュリティ設定が必要となり、ユーザーの不満や生産性の低下、エラーの頻発、セキュリティ侵害への対応の遅れなどの問題が発生します。旧世代のツールでは、クラウドでの仕事の質の変化についていけないのです。

このミスマッチがセキュリティにどう影響するかの事例、そして SASE が今日の環境になくてはならない理由をご説明しましょう。従来のアプローチでは、ユーザーのブラウザが Web サーバーに接続した時点でセキュリティシステムのチェックが入っていました。セキュリティ分析は、URL の安全性を判断するためのリストのチェック以上のことはしません。（第 1 章で、ゾーンディフェンスについて解説しています。）

企業でクラウドを保護する責任者にとって、これは大きな問題です。現在急増しているセキュリティ課題の 1 つに、許可された接続の*内部*で発生する侵害があります（つまり、ある URL を許可した後で起こるもの）。SaaS（Software as a Service）アプリやクラウドサービス内で情報を収集するため、攻撃者は一見すると正しい形態をとりつつ、ユーザーを騙して貴重なデータやログイン認証情報を提供させます。また、従業員が迅速に物事を進めようとするあまり、機密データをカット、コピー、ペースト、シェアしたり、会社が不適切とみなす場所に移動させたりすることもあります。こうした環境では、ゾーンディフェンスはもはや適切な保護ではありえません。

企業にとってクラウドサービスの重要性が急速に高まり、テレワークが急増する現在、SASE を含めた新しいアプローチの開発、導入は急務となっています。クラウドに依存する企業では、場所、デバイス、ユーザー ID の限りない組み合わせに対応できるセキュリティが必要です。ユーザーが業務に使用するアプリケーションとの生産性の高いやり取りを、安全かつ高速でできるようにすることがその目的です。

広範囲の可視性に対するニーズ

空港を出て、高速道路に合流すると想定してください。Web が介在するアプローチは、ネットワークが外界と接する交差点を監視する警備員に例えると理解しやすいかもしれません。この警備員が車の流れを注意深く見守り、道を間違えようとするドライバーを制止したり、不審な車を見張ったりしています。

ただ、クラウドが普及した世界では、警備員は 2 つの大きな問題にぶつかります。

- 特定の車両を監視するよう指示されたり、ドライバーが目立った行動をしない限り、警備員は行動を起こせません。
- クラウド以前のサイバーセキュリティシステムは、Web トラフィックという 1 つの車線のトラフィックしか監視しません。こうした従来のシステムでは、SaaS、クラウドベースのサービス、カスタムアプリといった新しい車線を点検できません。その車線がおそらく監視されていないことを、サイバー犯罪者に知られてしまっているにも関わらずです。こうした新しい車線を走る乗用車やトラックを警備員が監視できないなかで、車には盗んだダイヤモンドの山、つまり、企業にとって貴重なデータが隠されている可能性があるのです。

真の可視性とは、ユーザー、データ、アプリケーション間で起こる活動ややり取りをきめ細かい層まで見通せることです。アプリケーション内でユーザーの行為を継続的に把握する必要があります。例えば、機密データを SaaS アプリケーションにペーストしようとしているユーザーはいないか？給与明細ファイルをオープンなクラウドサービスに晒そうとしていないか？そのような振る舞いをセキュリティシステムは検知する必要があるのです。

可視性を超えて：膨大なデータ収集がコンテンツを充実させる

クラウドの時代には、可視性だけでは不十分です。最高の解像度で撮影された写真でも、何をどのように見たらよいのか、さらには、実際に何を見ているのかが理解できてなければ、写真の中の細かい部分を見落とすことになります。セキュリティチームは、次のような質問に答えるために、写真の細部まで見通す必要があります。

- ユーザーは誰か？
- ユーザーの使用デバイスは何か？
- ユーザーが利用しているネットワークは？
- どのようなアプリケーションにアクセスしているか？
- 各アプリケーションとその動作について何がわかるか？
- ユーザーはどんなデータにアクセスしているか？
- ユーザーの現在と過去の行動には一貫性があるか？

写真の細部として説明しましたが、これはクラウドアクセスで最も重要な概念の 1 つ、*コンテキスト*と呼ばれるものです。このコンテキストがあるからこそ、動作やアプリケーション内で起こることを必要に応じて制限できるセキュリティポリシーをリアルタイムに定義、実施することが可能になります。((コンテキストおよびポリシーについての詳細は、第 4 章をご参照ください。)

クラウド時代の効果的なセキュリティの要件を以下に挙げます。

- セキュリティアーキテクチャの複雑さを最小限に抑え、ユーザーとセキュリティ部門の両方が作業しやすいようにする
- ユーザーの場所にかかわらず、アプリケーションとの高速かつ応答性の高いインタラクションを提供し、クラウドのメリットを最大限に活用できるようにする

- 企業のデータやユーザーに関わる潜在的なリスクを容易に把握、迅速に対処することで、ビジネスへのリスクを継続的に管理する

SASE アーキテクチャが適切に実装されていれば、このすべてが可能です。

SASE：クラウド向けに構築されたセキュリティ

従来の技術の呼び方を変えて再編するだけでは現代のクラウドセキュリティには使用できませんし、ましてや将来に対応できません。従来のアプライアンスをデータセンターの中に維持しながら、その弱点は隠しておこうとしても行き詰ります。クラウドは、まったく異なるスケールとスピードで機能するので、セキュリティサービスも同じスピードやスケールで動作するよう設計されている必要があります。

SASE がセキュリティフレームワークとして魅力的なのは、クラウドと同じように、仕事を楽にし、もっとフレキシブルに働けるようにしてくれるからです。

クラウド向けに構築されたセキュリティの意味、それは重要な SASE 要件がすべてアーキテクチャの設計に組み込まれている必要があるということです。迅速かつ大規模に仕事をするため、真の SASE に必要なのは、セキュリティに関するあらゆるサービスが、1 つの継続した迅速なアクションとして協調しながら動作すること。そして、検証や検査を行うのは、それの場所がどこであろうとも、「外で」実行されなければなりません。ユーザーのトラフィックを、インタラクションのたびにセキュリティボトルネック（データセンターのことです）に戻す必要はありません。ユーザーやアクセスポイントの近くにセキュリティを移動させれば、あらゆるインタラクションをより安全に効率よくできます。これが、セキュリティをクラウドのあるべき姿に合わせるということです。高速道路のたとえに戻ると、SASE が設置されていれば、警備員は全ての車線を走る車を監視できるようになるのです。

真のクラウドセキュリティを実現

SASE は適切に導入された場合、2 つの重要な役割を担います。

- **ユーザーがどこにいても、クラウドサービスへのアクセスを可能にするグローバルエッジネットワークを提供する：**グローバルエッジネットワークはユーザーを認証し、SaaS アプリケーション、企業のデータセンター、その他のサービスへの接続を最適化します。

» **セキュリティサービスをグローバルエッジネットワーク全体で提供し、ユーザーの近くで利用可能にする：**これにより、ユーザーと企業はこのセキュリティネットワークを頼りに、いつでも安全に仕事ができるようになります。このような構成により、ユーザーが誰かや、どこにいるかに基づいてセキュリティポリシーを適用したり、ユーザーのオンラインでの活動に指示を送ったりすることも可能になるうえ、活動のセキュリティ、信頼性、パフォーマンスを最適化することも可能になります。

適切に実装された SASE が優れている理由は、アプリケーションやワークロードがクラウドに移行したことの認識、そして、それに従ったセキュリティサービスの機能が備わっているからです。ユーザーは、アプリケーションを利用するために面倒なプロセスを経る必要はなくなります。カフェに移動し、必要な情報にアクセスするのもコーヒーを注文するのと同じぐらい簡単です。セキュリティのプロである読者の皆さんにとっては、コンテキストと共有された統合セキュリティサービスがあれば、アクセスが必要なユーザー、アクセスしようとしている対象、インタラクションのすべての要素がどこに存在するかに基づいて、自動的かつ適切に適用される高度なポリシーを作成することが可能になります。制約の多いデータセンターから開放的で可能性あるクラウドへと移行したデジタルの世界で機能するセキュリティとネットワークのアーキテクチャといえるのは SASE だけです。

データセンターについての考察

データセンターは、今後も企業の IT として一定の役割を維持すると思われます。ERP（Enterprise Resource Planning）などの大規模なアプリケーションは何十年も使用できるよう設計されているため、プライベートクラウド内のこうしたアプリは、SaaS やパブリッククラウドと長い間共存することになるでしょう。さらに言うと、企業は長期間にわたり、企業データセンターの構築と拡大に莫大な投資をしてきました。この勢いをすぐに断つのは困難というものです。忍耐強く、対処する必要があるでしょう。

データセンターを、ユーザーが仕事をするために利用する数多くの場所の 1 つと捉えると、クラウドに向かうトラフィックをすべてデータセンター経由でルーティングしてもあまり意味はありません。ユーザーのトラフィックを常に企業のプライベートネットワークを経由して迂回させ、分散したセキュリティのブラックボックスでわざわざ処理する。こうしたプロセスは、セキュリティ担当者の間でヘアピニングやバックホーリングと呼ばれる処理で、煩雑かつ非効率的です。例えると、よほどの余暇（と船）がない限り、ロサンゼルスからサンフランシスコのドライブで、カイロを経由して行くなんてことはしないでしょう。ユーザーと SaaS アプリケーションの連携にもこれと同じことが当てはまります。


ヒント

SASE は、SaaS アプリケーションのためだけにあるのではありません。ユーザーがオンプレミスかオフプレミスかにかかわらず、データセンター内のアプリケーションも含めたあらゆるアプリケーションへのアクセスを提供し、保護するためのセキュリティとして使用可能ですし、またそうすべきです。

あらゆるシナリオを網羅するサービス

クラウドサービスのメリットの 1 つは高い柔軟性です。ただ、*クラウド*や *SASE* などの名前を製品に付けるだけでは SASE になりません。真の SASE を実現するためには、柔軟性が意図的に設計に組み込まれていなければなりません。クラウドではコンテキストが常に変化するため、さまざまなテクノロジーやサービスがアドホックに連携し、シナリオの変化に合わせて適用されることが求められるのです。真の SASE は、あらゆる接続に対してセキュリティポリシーを実行するため、必要なすべてのセキュリティサービスを適用する一方で、以下の目的を常に優先します。

- 分散した従業員とユーザーに対応する
- 変化を続けるコンテキストに基づいてサービスレベルを最適化する
- セキュリティサービスを常にユーザーの近くに配置する
- ハイパースケール環境での運用が求められるセキュリティサービスを、最新のビジネスワークフローに必要なパフォーマンスで提供する

ここで出る質問は、どうすれば、会社で効果的な SASE 導入を実現できるか？でしょう。この後に続くセクションでは、NG-SWG という大きな要素を含め、いくつかの重要な要件を見ていきます。

グローバルエッジネットワークの必要性

従来のセキュリティアーキテクチャというレンズを通すと、ビジネスのためにクラウドを保護するという考え自体が矛盾をはらんでいるように見えます。一方では、ユーザーは、セキュリティによる障壁を最小限にしながら、どこからでもアプリケーションやデータに素早くアクセスできることを期待しています。その一方で、最高のセキュリティやデータ保護をユーザーやビジネスに提供するという、相反する 2 つのことを期待されているのです。

データセンター経由のヘアピニングは、ユーザーの 85%が企業のオフィスで仕事をしていた頃は大きな問題ではありませんでした。新型コロナウイルスによる世界的なパンデミックのなかで在宅勤務の良さを多くの人が実感し、今では 74%の人が少なくとも週に 2 日は在宅勤務を希望していることが PwC の調査で明らかになりました。リモートユーザーにとって、ヘアピニングは遅延を招き、生産性の高いユーザーエクスペリエンスの妨げとなるものです。テレワークがニューノーマルとして定着しつつある今、セキュリティをクラウドに移行し、ユーザーエクスペリエンスを低下させることなく、ユーザーに最適なサービスを提供し、データ保護を実現することが必要不可欠です。

このユーザーエクスペリエンスが重要な理由は、高速アクセスを求めるユーザーが不満をつのらせると、仮想プライベートネットワーク（VPN）への接続を避けるようになるからです。これは、すでに何年も前からやっていることです。そうなると、ユーザーやデータはまったく保護されることなく、セキュリティ部門の視界にもまったく入りません。グローバルエッジネットワークでは、保護やデータセキュリティを確保するためデータセンターにユーザーをヘアピンする必要はなく、どこからでもクラウドへの安全な接続を可能にします。


ポイント

テレワーク従業員などのモバイルユーザーにとって、グローバルエッジネットワークへのアクセスは大きなメリットです。Netskope が提供するグローバルエッジネットワークは、セキュリティ機能がホストされ実行されるアクセスポイントを世界の 40 以上の地域に展開しています。これにより、セキュリティを常にユーザーの近くに置くことができ、シングルパスでのトラフィック検査を実現しています（詳しくは、本章で後述する「シングルパス検査」を参照。ここでは、「速い」という点だけを考えてみてください）。セキュリティとグローバルエッジネットワークの組み合わせで、円滑で高速かつセキュアなユーザーエクスペリエンスの提供が実現します。

SASE と従来のセキュリティの基本的な違いの 1 つは、セキュリティの適用方法と適用される場所です。SASE のセキュリティアーキテクチャでは、ユーザーがインターネットに接続しようとすると、SaaS アプリケーションの利用、ウェブの閲覧、ソーシャルメディアへの投稿などの目的にかかわらず、まずグローバルエッジネットワーク上のアクセスポイントに接続します。各アクセスポイントには、セキュリティサービスを実行するのに必要な計算能力が備わっています。アクセスポイントは分散して存在するため、ユーザーは、パフォーマンスのトレードオフや、企業データセンターを経由する際に遭遇していたような複雑で多段階のセキュリティ対策に悩まされることはありません。

NG-SWG と SASE はどう連携しているか

理想的な SASE の完成形は、すべてのセキュリティサービスが完璧に連携して動作する、まったく新しいセキュリティアーキテクチャといえます。大事業のように聞こえるかもしれませんが、その通りです。ですが、直ちに実現する必要はありません。あるべき最初のステップを踏めば、後に続くすべてを支える強固な基盤を作れるでしょう。この最初の重要な一歩とは、NG-SWG の実装です。「SASE もどき」とあるべき姿の SASE とを決定的に分けるのはこの部分で、SASE を実現するセキュリティクラウドを構成するための足がかりとなるのが NG-SWG なのです。

SASE はマイクロサービスアーキテクチャを使って実装するのが最適です。端的に言えば、マイクロサービスは、小さな個別のサービスモジュールを多数組み合わせて構築する方法で、適切に導入されれば、こうしたモジュールは共通のコードベースを共有し、連携して動作してクラウドのネイティブ言語を理解します。

これらすべてのサービスは、コンテンツやコンテキストに基づいたセキュリティポリシーの適用を連携して行えるよう、組織化する必要があります。NG-SWG は、SASE 実装を管理する航空管制官のような役割を果たします。ユーザーがデータにアクセスする時と場所にかかわらず、NG-SWG は各サービスを調整し、サービス同士が連携して動作し IT 環境全体にセキュリティポリシーを適用できるようにします。

ポリシーベースでセキュリティを適用するために必要なすべての共有セキュリティ サービスをネットワーク上のユーザー、データ、アプリケーション、トラフィックに関する豊富な情報に基づいて、各接続に対して 1 回の高速シーケンスで適用できます。

さらに、NG-SWG の導入で機能の低いアプライアンスを排除できるため、最高かつ最も有用なサービスの機能を手放すことなく、セキュリティインフラの複雑さを軽減できます。NG-SWG の構成要素であるこうしたサービスは、多くの新しいサービスと連携して適用され、SaaS や Web トラフィックの深部まで検査し、豊富な情報を獲得して、コンテキストベースのセキュリティポリシーを実行します。

注意

AWS（Amazon Web Services）や Google Cloud などの一般的なパブリッククラウド プラットフォームは、それだけでは SASE として機能せず、SASE に対応しているとも言えません。パブリッククラウド ソリューションはアプリケーションの配信に最適化されており、パブリッククラウドのアーキテクチャは、トラフィックがどこかに向かう時に経由するセキュリティサービスの中継地ではなく、目的地として設計されています。一方で、SASE には、セキュリティワークロード向けに設計されたマイクロサービス型のアーキテクチャをサポートする、独自のコンピューティングとパフォーマンス要件が備わっています。

SWG と NG-SWG の比較

SWG は、セキュアインターネット ゲートウェイ、ウェブプロキシ、ウェブ フィルターなどと呼ばれることもあります（これ以外にもいくつかの名称があります）。少なくとも 1990 年代から何らかの形で存在していて、現在とはまったく異なる時代に誕生した技術です。

NG-SWG は、従来の SWG やその他の一般的に知られた類似製品とどこが違うのでしょうか？簡単に言うと、従来の SWG は、Web トラフィックのみに対応し、許可 / 拒否のみで制御していました。これは、インターネットが Web サイトと HTTP/S（Hypertext Transfer Protocol/Secure）通信に特化していた時代に作られた技術で、「その Web サイトへのアクセスを許可します」、あるいは「*あの* Web サイトへの接続は禁止されています」のどちらかで制御が行われました。

一方で、NG-SWG では、あらゆる Web サービスなどがその傘下に収まっていると同時に、ユーザーの近くにコントロールポイントを置いた（グローバルエッジネットワークで前述したとおりです）広大なセキュリティクラウドを構築し、そこで多様なセキュリティサービスが編成されています。従来の SWG や同様のアプライアンスに搭載されていた基本的な Web トラフィック機能をすべて実行、強化するとともに、数多くの新しいセキュリティ機能が追加されたのが NG-SWG です。特に、NG-SWG では、クラウドや Web のトラフィックを詳細に検査し、インタラクションの内部で何が起こっているかを調べ、データや脅威の保護を適用し、コンテンツやコンテキストを理解して、きめ細かいポリシー制御を実行します。

SASE に NG-SWG が備わっていれば、交通警備員やコントローラーは全ての車線を流れる車両を監視し、車内で何が起きているかまで把握して、ルールを適用できるのです（表 2-1 を参照）。

表 2-1 **Netskope が SASE 要件を満たす方法**

SASE 要件	Netskope NG-SWG
暗号化されたトラフィックを検査するシングルパスアーキテクチャを持つクラウドネイティブなシステム	アプリやクラウドサービスをデコードして理解し、データのコンテキストを把握する機能を持つクラウドネイティブアーキテクチャで、完全にクラウド内に構築される。Netskope のシングルパスアーキテクチャは、すべてのサービス（SWG、クラウド アクセス セキュリティ ブローカー（CASB）、高度なデータ漏洩防止（DLP）、サンドボックス、機械学習（ML）分析、FWaaS（Firewall as a Service）、リモートブラウザアイソレーション（RBI）など）に向けて、NewEdge のすべてのデータセンターで、暗号化トラフィックの高度なデータ・脅威の検査をラインスピードで提供する（接続プロトコルのダウンネゴシエーション（TLS1.2 に強制など）なしに TLS1.3 に対応）。
SLA（サービスレベルアグリーメント）で低遅延・高可用性を実現したポイント オブ プレゼンス	高性能なセキュリティプライベートクラウドである Netskope NewEdge Network は、セキュリティサービスをホストし、世界中に豊富なアクセスポイントを提供している。1 桁ミリ秒の低遅延で最高のエクスペリエンスを提供する NewEdge は、ファイブナイン（99.999%）の可用性インラインサービス SLA に加えて、リアルタイムのサービス / データセンターステータスを公開している Trust Portal（`https://trust.netskope.com`）により支えられている。
単一のポリシーコントロールプレーンによるサービスとしてのセキュリティ	シングルクラウドプラットフォームとポリシーエンジンは、トラフィックを処理するデータプレーンとは別のマネジメントプレーン上で動作する。管理が容易な単一のコンソールから、SASE セキュリティサービスの管理と追加が可能。これらのサービスは、単一のエージェントを介してデプロイされ、すべての場所でのアクセスとユーザーエクスペリエンスを容易に実現される。
NG-SWG フォワードプロキシによる 5 種類のユーザー トラフィックの検査	Web トラフィックのみを解析する従来の SWG とは異なり、パブリッククラウドやデータセンター内の Web、認可 SaaS、シャドー IT アプリ、パブリッククラウド サービス、カスタム アプリなど、あらゆるレーンのユーザートラフィックを解析できる。すべてのアクセス方法に一貫したセキュリティ検査ポリシーが適用される。
機密データの可視化と制御、およびクラウド DLP	Web、SaaS、シャドー IT、パブリッククラウド サービス、パブリッククラウド内のカスタムアプリなどでの機密データの動きを比類のないレベルで可視化する。これらの 5 種類のユーザー トラフィックに加え、Microsoft Office 365（M365）および Gmail の Simple Mail Transfer Protocol（SMTP）のアウトバウンドトラフィックに対する E メール DLP により、転送中のデータを保護する。この機能が鍵となるのは、企業と個人のアプリやアプリインスタンス間のデータ転送、およびデータ転送時の異常の分析である。

(continued)

表 2-1 ***(continued)***

SASE 要件	Netskope NG-SWG
高度な脅威対策（ATP、Advanced Threat Protection）と、ユーザおよびエンティティの行動分析（UEBA、User and Entity Behavior Analytics）	インラインのアンチマルウェア、実行前分析、サンドボックス、機械学習分析、行動異常やユーザーリスクスコアリングのための UEBA により、Web やクラウド上に侵入したマルウェア、クラウドフィッシング、悪意のあるドキュメントからユーザーを保護し、データ、脅威、活動に関するすべてのユーザーやアプリケーションのリアルタイム分析とダッシュボードによる可視化を実現している。
クラウドファイアウォール	すべてのポートとプロトコルにわたって制御するアウトバウンドクラウドファイアウォールにより、リモートユーザーや拠点を保護する。
RBI	ターゲット RBI は、未分類の危険な Web サイトをピクセルレンダリングして安全なアクセスをユーザーに提供するほか、ファイルのダウンロードやアップロード、フィッシング攻撃で見られるフォーム入力、クリップボードのコピー / ペーストなどもブロックする。
ゼロトラストネットワークセキュリティ	ゼロトラストセキュリティコントロールの適用はユーザーアクセスの始まりから（ゼロトラストネットワークアクセス（ZTNA）、アイデンティティアクセスマネジメント（IAM））リスクとコンテキスト情報を取得し、ユーザー、デバイスタイプ、アプリ、アプリのインスタンス、アプリのリスク評価、カテゴリー、行動、コンテンツ、アクションなどのリスクに基づいた条件付きかつコンテキストベースのポリシー制御を適用する。ユーザーの行動や異常を監視することで、適応型のポリシーがゼロトラストの原則に従って動的に実施される。これには、ステップアップ認証、アクティビティへのアクセスやデータ移動の制限、ユーザーのアプリケーションへのアクセスの完全停止などが含まれる。
適応性あるコンテキスト重視型のポリシー作成と一貫した適用	アプリのリスク、ユーザのリスク、データのコンテキストに基づいて、リアルタイム コーチング、ステップアップ認証、適応性のあるポリシーを提供。リアルタイムのポリシー適用は、すべてのユーザー、支社、その他のエッジに対して一貫して実施される。
IAM	ユーザーやグループのデジタル ID を管理・検証する IAM システムや ID プロバイダシステムと連携する。
エンドポイント保護	自動化された IOC（Indicator of Compromise、セキュリティ侵害インジケーター）の双方向での共有に加えて、エンドポイント保護機能による条件付きアクセス、調査のための豊富なメタデータの共有が可能。

SASE 要件	Netskope NG-SWG
セキュリティ情報イベント管理（SIEM）およびセキュリティオペレーション センター（SOC）	セキュリティ担当者がアラートやインシデント調査に使用する管理ポイントやダッシュボードとシームレスに連携できるように、IOC の共有と豊富なメタデータの提供を実現。
リアルタイム分析・可視化	データの移動、脅威、ユーザー、アプリケーションに関するリアルタイムの可視化と分析のためのクラウドメタデータを、経営幹部職、役員レベル、セキュリティおよびリスク対策チーム向けに、動的でカスタマイズ可能なダッシュボードで提供する。

SASE 実装の完成度による比較

NG-SWG を導入すると、データセンター内のトラフィックのごく一部を処理するセキュリティソリューションやアプライアンスごとに、何百、何千もの細かく複雑なルールを個別に設定する必要がなくなります。NG-SWG を使用した最高レベルの SASE ソリューションでは、すべてのトラフィックに対して求める結果を記述したハイレベル ポリシー作成に注力します。その後、NG-SWG は、ウェブ トラフィック、認可 SaaS アプリ、非認可 SaaS アプリ（シャドー IT）、パブリッククラウド サービス、パブリッククラウドでホストされているカスタム アプリの全体で、こうした結果を出すためにすべき事をさまざまなセキュリティサービスに指示します。このエンフォースメントには、きめ細かい適切な応答を可能にするユーザーコーチングやリスクベースの動作などの豊富な機能を盛り込むことができます。アーキテクチャ全体にわたって実現したいことをあなたが定義したら、それを実現するよう各サービスを調整するのは NG-SWG の仕事です。


技術情報

NG-SWG は、SASE を適切に実装するためのコンテキストベースの基盤をどのようにして構築するのでしょうか？表 2-1（本章で前半）で、NG-SWG が提供する SASE アーキテクチャのサービスと機能を示しています。また、Netskope NG-SWG に接続して SASE を完成させるのに役立つ他のサービスについても記載しています。

NG-SWG の仕組みを検証する

ここまでは、より広範な SASE アーキテクチャの中で NG-SWG が提供する機能について解説しました。ここからは、NG-SWG がそれをどのように実行しているかを見ていきます。

この後の説明はセクションごとの構成になっていますが、NG-SWG によるセキュリティは、一連の個々のアプライアンスやデータセンターのような直線的につながったシーケンスではないことを覚えておいてください。

シングルパス インスペクション

ユーザーのデバイスがグローバルエッジネットワーク上のアクセスポイントに接続されると、そのユーザーのすべてのトラフィックはシングルパスインスペクションを受けます。シングルパスとは、まさに読んで字のごとしで、ポリシーの適用に必要なすべてのセキュリティサービスが 1 つの連続したファネル（じょうご）を形作り、そこにトラフィックが流れます。ユーザーと目的地の間を移動するトラフィックは、この 1 つのファネルを一度だけ、リアルタイムで通過します。このプロセスは、別々の独立したファネルが連続して設置され、すべてがそこを通過しなければならなかった従来のウェブ専用の SWG アプライアンスやインラインのクラウドトラフィックソリューションとはまったく異なるものです。

NG-SWG のシングルパスインスペクションは、Web コンテンツ、認可 SaaS アプリ、ユーザーが使用するシャドー IT や非認可 SaaS アプリ、パブリッククラウドサービス、組織が展開するパブリッククラウド内のカスタムアプリに適用されます。Web とクラウドのトラフィックはこの単一のシステムを通過します。このシステムがすべてのセキュリティサービスを単一の一貫したプラットフォームとして集約、調整し、さらにそれらを改良して、適切に実装された SASE を実現します。

トラフィックはここを 1 回通過する間に段階的にフィルタリングされます。最も明確に分かる問題が最初に排除され、ふるいにかけられ次第に量を減らしたトラフィックはさらに詳細な分析を受けます（これらの段階については第 4 章を参照してください）。

コンテキスト量に対応したセキュリティ強化

適切に実装された SASE が持つアクティブで深い洞察力や軽快なセキュリティの鍵となるのがコンテキストです。ユーザーがアクセスポイントに接続するとすぐに、セキュリティクラウド内の NG-SWG サービスが、すべてのサービスで利用可能なコンテキストの全体像を作成します。ポリシーの実施方法を決めるのに使用されるこのコンテキストは、メタデータ（他のデータを説明したり、コンテキストを追加したりするデータ）の巨大な集合体であり、以下を識別・認識する豊富な情報が含まれています。

- ユーザーまたはユーザーが所属する組織部門
- ユーザーのデバイス、その場所、そのデバイスが組織に管理されているかどうか
- ユーザーが使用中の Web サイト、アプリ、アプリスイート
- Netskope の Cloud Confidence Index（複数の独立したセキュリティ評価サービスから得られたリスク評価で、アクセスしている特定の Web サイト、アプリ、アプリスイートに割り当てられている）
- ユーザーおよびアプリケーションが要求、生成、および / または使用しているデータ

これらに加えて、このコンテキストは多くの新しく多様な情報で拡張され、NG-SWG はこれを活用して、次のプロセスに基づいてさらに詳細な情報を追加します。

- ユーザーの行動とその行動の異常性の認識
- トラフィックに含まれるコンテンツとデータの検査
- アクセスしたアプリケーション、ウェブコンテンツ、サービスで実行された活動内容と、その活動の性質
- アプリケーション環境内のデータに関する知識
- 過去のインタラクションから収集され保存された情報

コンテキストはユーザーがアクセスしている間、常に変化しています。詳細なコンテキストがさまざまに組み合わさって生じるリスクの微妙な変化に迅速に対応し、適切に対処できるシステムが必要です。ポリシーにはセキュリティに求める結果が記述されていますが、その時々の状況に応じて、結果をもたらすサービスとセキュリティアクションの最適な組み合わせを決定するのはコンテキストです。例えば、突然挙動がおかしくなり、アクセスしてはいけないファイルにアクセスしたユーザーは、*ステップアップ認証*の対象となり、ユーザー ID 確認のために詳細な情報を要求されます。膨大かつ動的なコンテキストは、きめ細かなセキュリティポリシーの適用や、コンテキストの変化に応じたリアルタイムのポリシー実行を可能にします。こうした微妙で詳細なコンテキストを使ったセキュリティ強化に大役を果たすのは、人工知能（AI）と機械学習（ML）です（第 4 章を参照）。

従来の Web セキュリティは基本的に、「Yes」か「No」を判断することでした。NG-SWG では、動的で継続的なセキュリティ確保の方法で、すべての Web やクラウドのトラフィックの内部で起きていることや動作を継続的に監視します。このアプローチにより、NG-SWG はセキュリティに関する決定をその場で調整することができます。これは、アプリや Web サイトを利用するユーザーを保護する重要な機能です。

表 2-2 に、NG-SWG によって拡張・強化され、本格的な SASE アーキテクチャの基盤となるセキュリティ機能の一部を示しています。

表 2-2 NG-SWG が提供する主要なセキュリティ サービス

セキュリティ サービス	従来の設定でのサービスの役割	NG-SWG で強化されるサービス内容
SWG	Web の脅威や不適切なコンテンツからユーザーを保護する。	アプリやデータのコンテキストを追加する（アプリやデータの使用者、その使用場所、使用理由）。 データ保護を追加する（改ざんや盗用の防止）。 不適切なデータ使用を防止する（意図しない場所でのデータの使用や送信を防ぐ）。
DLP	データセンターに保存され、Web 経由でデータセンターのファイアウォールの外へ転送されるデータのみを保護する。	Web、SaaS アプリ、クラウド、クラウド サービス、パブリック クラウド上のカスタムアプリなどに散在するデータなど、移動中のすべてのデータを保護する。
CASB	API（Application Programming Interface）による可視化を提供する認可アプリケーションの監視と保護。これは API を介してやインラインでも監視、保護することは可能だった。アプリ環境またはデータセンターに保存されているデータ、および両者の間を行き来するデータなど、静止中および移動中のデータを対象としていたが、すべてのソリューションがすべてのモードをサポートしているわけではなかった。	確実な管理 API を提供していないアンマネージド アプリを監視することで、多数のアンマネージド アプリの監視と保護を可能にする。 移動中のデータ、つまり、アプリや Web サイトで活発に使用されていたり、それらに転送されているデータを監視する。 アプリのリスクに関する強力なインサイトを提供し、SaaS の選択や導入を支援する。

セキュリティサービス	従来の設定でのサービスの役割	NG-SWG で強化されるサービス内容
高度な脅威からの保護（ATP、Advanced Threat Protection）	サンドボックス（実行ファイルを安全に開き、悪意のある意図やハイパーリンクを検出する）や脅威インテリジェンス（公開および有料のソースからの IOC を共有する）などの高度な手法を用いて、Web ベースの脅威から保護する。	Microsoft Office 365 や Google Docs などのアプリやクラウドサービスを利用したマルウェア送信やフィッシング攻撃など、クラウドを利用した脅威から保護する。 未知のアプリや Web サイトを隔離して安全なインタラクションを確立し、潜在的脅威から保護する。

シングルパスでのポリシー実施

どれほど詳細なコンテキストが与えられても、ユーザーとセキュリティサービスの両方が何をすべきで、何をすべきでないかを分かっていなければ、あまり役に立たないのは当然のことです。コンテキストを比較できる基本的ルールは必要です。

これまでに、ユーザーが入力した URL とブロック対象の Web サイトとの照合に基づいて、ファイアウォールの動作を決定する一連のルールを記述されている場合もあると思います。しかし、従来のセキュリティでは常に、速度と柔軟性を求めればセキュリティで妥協を強いられることの繰り返しです。絶え間なく増える新規ウェブサイトと、担当者の時折の人事異動によって、ルールに記述したリストは膨大にふくれあがり、危険レベルに達します。知らず知らずのうちに新たな脆弱性を生んでしまうことを恐れて、便利な営業ツールへのアクセス許可のためのルール変更を躊躇してしまうかもしれません。

適切に導入された SASE では、超一流のセキュリティを提供できる新たなパラダイムがこうしたジレンマを解消します。すべてのアプリ、カテゴリ、Web サービス全体に対してデータポリシーやアクティビティコントロールを実施する SASE のスーパーパワーは、シングルパスポリシーエンフォースメントという強力な機能そのものです。これを、実践的なコンテキストのパワーと捉えてみるとよいでしょう。例えば、シングルパス検査で、Web フォーム、ファイル、アプリ内のフィールド、Slack チャンネルに機密データが含まれていることがわかった場合、シングルパスポリシーの適用により、Web 上のコンテンツをブロックしたり、閲覧を許可しながらもアプリ内のアクティビティ（アップロード）を制御したりすることができます。

一貫した、きめの細かい、一元化されたポリシーフレームワークがセキュリティサービス全体に適用されることで、特定のポリシーをどのように実装するかという詳細を気にすることなく、自らコントロールし、意図を明確に示すことができます。こうすることで、複雑さを大幅に軽減できます。

SASE と NG-SWG の組み合わせで、セキュリティ部門の仕事は大きく変わります。個別のアプライアンスをひとつひとつ管理するため別のコードを書くという非効率な作業はいりません。セキュリティチームは、ビジネスにとって意義のあるサービスを提供する、効果的でハイレベルなルールに集中できます。

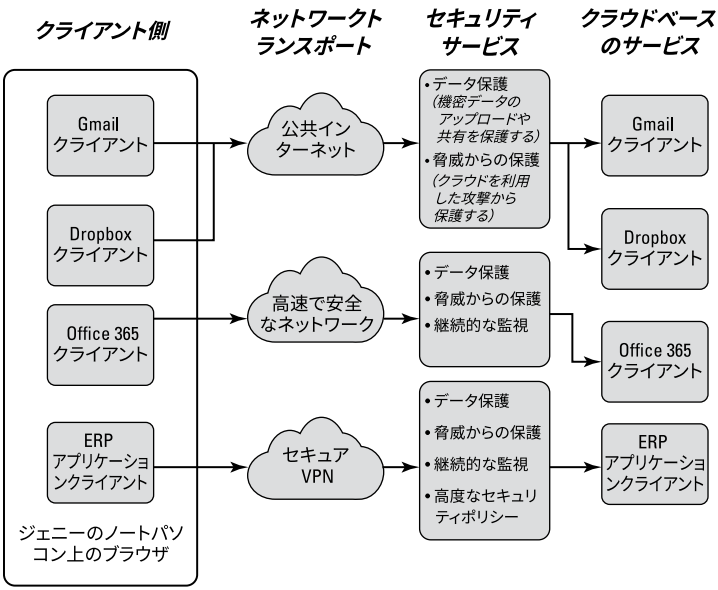

図 2-1: ジェニーというユーザーの NG-SWG の実際の構成

NG-SWG の実際

図 2-1 は、1 人のユーザーの視点から見た実際の NG-SWG を示しています。

図 2-1 でわかるとおり、在宅勤務中のジェニーは、次の 4 つの接続を開始しようとしています。

- 個人の Gmail アカウント
- 会社の Microsoft Office 365 の Email
- Dropbox のようなクラウド ストレージ アプリ
- Salesforce、ServiceNow、Workday などの、企業が管理する重要アプリ

このケースでは、NG-SWG はこれらの個別のインタラクションを次のように処理します。

- **ジェニーの個人の Gmail アプリは、パブリック インターネットにルーティングされる。**NG-SWG はこの接続を保護・分析し、脅威対策とデータ保護を提供し、ハイパフォーマンスなユーザー エクスペリエンスを実現します。
- **ジェニーの会社の Microsoft Office 365 Email は、高速で安全なネットワークを経由する。**この接続のトラフィックは常に監視され、重要なデータが共有されないようになっています。
- **管理されていない Dropbox クラウド ストレージ アプリへは、パブリック インターネット経由で接続する。**NG-SWG はこの接続を常に保護・分析し、セキュリティ・ポリシーを適用することで、ジェニーはサードパーティ由来の共有ファイルを閲覧することができます。ただし、NG-SWG はアップロードをブロックし、ジェニーが正当な理由を示してファイルのダウンロードをする場合は、ファイルのダウンロードに脅威防御を適用します。
- **ミッションクリティカルな企業アプリへの接続は、特別に暗号化された VPN でルーティングされる。**この接続は複数の異なるセキュリティサービスによって監視されており、データが不正に共有や使用されないように何重にも保護されています。また、アプリが適切に使用されることを確認するポリシーも適用されます。

このケースでは、1 人の従業員が 4 つの異なる接続をする場合にどのように保護するかを見ていただきました。それぞれの接続には、特定のポリシーを適用するための明確なコンテキストが示されています。結果、このユーザーのエクスペリエンスは素晴らしく、セキュリティは高い水準で確保されています。ジェニーは会社のデータを危険にさらすことなく個人の Gmail をチェックし、仕事ができるのです。これが NG-SWG が生み出す違いです。

ここで重要なのは、適切に実装された SASE アーキテクチャについて言えば、NG-SWG だけが違いを生むわけではないということです。NG-SWG は魔法の杖ではありません。CASB 機能（SWG にはなく、真の NG-SWG に備わる）、ゼロトラスト原則を正しく適用すること、これら 2 つがパズルの重要なピースです。

それでもなお、NG-SWG の存在感は大きく、SASE 達成までの時間を劇的に短縮させ、SASE アーキテクチャの実現の妨げにしかならない、従来の SWG のような古い技術からの脱却に役立ちます。

本章の内容

- 従業員をよく知ることでセキュリティを向上させる
- 強固なセキュリティを実現するサービスの組み合わせ
- 管理された従来のネットワーク外で従業員が働くようになった今、信頼はどう変化したか
- クラウドでユーザーを保護するためのセキュリティ強化

第3章
従業員を攻撃から保護する

セキュリティの多くの要素は人に関係しています。あなたにとって大切な人を守り、あなたが大切にするものを悪意ある人々から守るのがセキュリティの使命です。企業のセキュリティやネットワーク担当部門にとって明確かつ現実的なシナリオとは、従業員や顧客に安心できる信頼性の高い環境や操作性を提供しつつ、従業員やデジタル資産を悪意のある攻撃者から守りぬくことです。

その一方で、従業員を自分自身のリスクから保護することもセキュリティの役割です。つまり、ミスや気のゆるみ、怠慢、判断ミスなどにより、従業員やひいては企業に取り返しのつかない損害を与える可能性があるのです。（サイバーセキュリティ侵害の 90%以上がヒューマンエラーに起因しているという Kaspersky Lab の調査結果には驚かれることでしょう。）

適切に設計された SASE（Secure Access Service Edge）は、セキュリティ担当者が効果的かつ正しくこの大きな課題に取り組める見識とツールを提供し、次の 2 つの側面から組織を支援します。

- **企業システムへのアクセスを許可されていない人々からシステムを保護する。**システムがデータセンターにあっても、クラウドにあっても、常に同じ基準が適用されます。

- **システムへのアクセスを許可された人々が意図的または無意識に危険な行動をとるのを防ぐ。**

SASE は、セキュリティをエッジベースのクラウド環境に移行し、充実したセキュリティサービス、完全な可視化と制御、どこにでもアクセスできる機能を備えた体制を実現します。

本章では、次世代 SWG（Next-Generation Secure Web Gateway）、CASB（Cloud Access Security Broker）機能、ゼロトラスト原則が導入されたあるべき姿の SASE が、いかにしてクラウドを使用するユーザーの日常を安全かつ楽にするかをご覧いただきます。

コンテキスト：セキュリティのゲームチェンジャー

SASE はコンテキストによってその効果を発揮しますが、この豊富な背景情報が生成されるのは Netskope プラットフォーム内です。Netskope が提供する Cloud XD（*Extreme Definition* の略）は、Web トラフィック、クラウドサービス、SaaS アプリのアクティビティを、分かりやすく実用的なインサイトに変えてお届けするコンテキスト サービスです。トラフィック内部の詳細までキャプチャしてデコードする Cloud XD は、ユーザー、ユーザーの使用デバイス、使用中のアプリケーション、さらにこうしたアプリケーション内の特定の操作まで識別します。デコードされた情報はすべてのセキュリティサービスと共有されるため、Cloud XD が提供した情報を手がかりとして、詳細なセキュリティ ポリシーを適用することが可能になります。

基本的な質問への回答

Cloud XD が提供する情報は詳細かつ多岐にわたり、進行中の特定の操作に依存しています。具体的には次のような情報が含まれます。

- ユーザーは何かをアップロードまたはダウンロードしているか？
- その「何か」には、機密データは含まれているか？
- アップロード / ダウンロードしているデータは何バイトあるか？
- 使用されているアプリケーションは何か？

- そのユーザーが使っているのは、アプリケーションの企業インスタンスまたは個人インスタンスか？

こうした情報の収集は簡単そうに見えますが、セキュリティ担当者はこのような基本的でハイレベルなデータをつい最近まで事実上使用できず、ましてや、セキュリティ全体に集約的に一貫して適用できる状態からは程遠かったという事実には驚かれるかもしれません。

このような新たに利用可能になった詳細情報で、ユーザーの行動を次のように説明することができます。

> ローレンは Gmail の企業インスタンスを使用しています。会社のログイン認証情報（ユーザー名、パスワード、2 要素認証（2FA）コード）を使用したアクセスを許可されています。ローレンは個人用の Gmail アカウントを持っている可能性もあります。Gmail では使用しているブラウザのウィンドウ内で簡単にアカウントを切り替えることができるので、ローレンがどのインスタンスで仕事をしているかを追跡できることになります。


注意

今日の高度なセキュリティという観点でコンテキストを知るには、使用しているセキュリティサービスが、*常に*変化や異常に目を光らせている必要があります。最近では、攻撃者は SaaS アプリを利用したフィッシングやクラウド関連の攻撃を仕掛けて認証情報を取得することに長けてきており、従来の Web 防御は簡単に破られています。ユーザーにアクセスを許可した時点からセキュリティの仕事は始まると言えます。

行動の検証

ユーザーがアクセスした後にとる行動パターンを検知・評価することで、基本的な質問（前のセクションを参照してください）よりもさらに貴重なコンテキスト情報を得ることができます。Cloud XD では、高度な分析を適用してアカウントが侵害された手がかりを探し、「許可されたユーザー」（またはそう見えるユーザー）が通常の行動や与えられた役割を超えたふるまいをした場合にそれを提示します。Cloud XD は疑わしい行動の兆候を探し、次のような質問の答えを提供します。

- ユーザーは、データの移動など、通常とらない行動をとっていないか？
- 通常とは異なるアプリケーションやコンテンツにアクセスしていないか？

- ユーザーがアップロードまたはダウンロードしているデータ量はどれくらいか、また、その活動やデータ量は通常と異なっていないか？
- ユーザーは、通常と違う方法でデバイスを操作していないか？

人の行動は予測不可能に見えても、いつもとる行動やパターンが違っていると分かるものです。次世代 SWG は時間をかけてユーザープロファイルを作成し、通常と異なるデータの移動、認証情報の悪用、その他のさまざまな異常な行動をとろうとするなど、通常とは異なる行動の検知にプロファイルを利用します。

豊富な外部コンテキストの掘り下げ

このような全体的なコンテキスト重視のアプローチにより、クラウドに対するセキュリティはスマートなものに進化します。企業ネットワークの内部のコンテキスト（ユーザー、デバイス、ネットワーク、アプリケーションなど企業ネットワークの「内側に」あるもの）だけでなく、その外側にあるものについても詳しく知る必要があります。Netskope は、アプリケーション同士が通信するための API（Application Programming Interface）や、データを柔軟な構造にするための JSON（JavaScript Object Notation）など、クラウドを支えるすべての要素を SASE アーキテクチャを使ってより深く理解することを可能にします。これに加えて、特定の Web サイト、クラウドサービス、データリポジトリに関するコンテキスト情報を提供し、ユーザーが使用しているクラウド環境の全体像を把握することができるサービスもあります。

このように、コンテキストによってセキュリティーサービスをより効果的に使えますが、それはセキュリティサービスの持つ情報が増えたから。より多くのことを知ることで、より洗練された行動がとれるようになるというわけです。各サービスに関しては、非常に具体的かつ詳細にわたり、刻々と変化するコンテキストに至るまで、何が許可され、何が禁止されるのかを明確に定義したポリシーでサービスを制御することができます。

個別サービスの合計よりも、サービスがどのように優れているか見る

従来のセキュリティ製品は、それぞれが独立して機能していることが多く、個々のジョブはシークエンスで独立して実行されていました。それに対して、Netskope が提供する、効果的な SASE に必要なアーキテクチャは必要に応じてサービス同士が助け合い、アーキテクチャ全体をよりスマートにします。DLP（データ損失防止）サービスと UEBA（ユーザー

およびエンティティの行動分析）サービスが連携して機能し、ユーザーの行動にリスクがあることが示されると、データ保護のレベルを上げて対応します。また、高度な DLP サービスである光学式文字認識（OCR）を使用して、ユーザーがアップロードしているドキュメントに何が含まれているかを検出し、そのドキュメントが共有しても安全かどうかを判断するのもその一例です。チームワークで勝利を収めるというアプローチです。

そして、最高財務責任者（CFO）が会社の経理担当者と情報を共有することを許可する一方で、アクセス権を持つラインマネージャーがこの情報の一部を株式仲買人と共有することを禁止するなど、ユーザー プロファイルがプロセスにさらなる情報を与えます。

ユーザーが境界になった時にセキュリティをどう確保するか

SASE が登場する以前、セキュリティとは「ユーザーは誰か」を見極めることでした。ユーザーを特定できたら、境界を越えて、いわゆる*城*（使用を許可されたデータ、アプリケーション、サービスの総体）へのアクセスが許可されます。それ以外にも、ユーザーが何を扱うことができるかを規定する特定の権限や制限があったかもしれませんが、それより詳しいことは識別されず、許可された境界内でユーザーがとる危険行動に対する保護はありませんでした。


注意

SASE による保護は、ID とアクセスの管理から始まります。つまり、私たちがデジタルライフで毎日遭遇する、通常のユーザー名、パスワード、多要素認証を使ったプロセスですが、SASE のアーキテクチャでは、これらはユーザーの身元を確認するための始まりに過ぎません。セキュリティサービスには、豊富で詳細、そして常に更新を繰り返すユーザープロファイルがあります。ユーザーが使用しているデバイス、時間帯、場所、使用中のアプリケーション、文字入力の速さなど、その他のすべての「情報」は、ユーザーが本人であることを確認するためのより多くの情報を提供してくれます。たとえユーザーの基本認証情報が盗まれたとしても、SASE セキュリティサービスは企業やそのデータを保護するために機能し続けます。（Netskope のアーキテクチャでは、こうした漏洩情報もユーザーの危険度スコアに記録されます。詳しくは、第 4 章をご覧ください。）

セキュリティ業界で広く支持されている考え方に*ゼロトラスト*があります。企業システム内のアプリケーションやデータにユーザーやデバイス

がアクセスしようとする時、そのユーザーが自分の身元、つまり誰であるかを証明できるまで、まったく信頼できないという前提に立っています。その場合でも、ユーザーはアクセスを許可されたリソースの使用だけに留まります。何か他の行動をとろうとすると、再度認証を受けなければなりません。

ゼロトラストの原則は、SASE のアーキテクチャ全体にさらに強力に適用することができ、SASE を適切に実装するもう 1 つの鍵となります。言いかえると、あらゆるネットワークトラフィックで、ユーザーやその使用デバイスなどの識別の有無にかかわらず、ユーザーは悪事を働くものという前提に立つのがゼロトラストの原則です。

ZTNA（Zero Trust Network Acdess）と呼ばれている実装の方が広く知られており、企業向けセキュリティ業界では目新しいものではありませんが、SASE によってゼロトラストの適用範囲は広がります。ゼロトラスト以前を振り返ると、ユーザーがデータセンターのサービスへのアクセスを許可された後、特定の活動だけしか許可されない場合がありましたが、その範囲内では基本的に何をしても自由でした。

SASE は、ゼロトラストの原則をより強固なものにするとともに、全世界のすべてのユーザーに対してより柔軟かつ寛容な環境を提供します。（ポイント：今ではユーザーが境界になりました。もっと分かりやすく言うと、「境界線」に近いものを形成しています。）SASE のアーキテクチャは、ユーザーが持つすべてのトラフィックのコンテキストを使用して、ユーザーができること、許可されるべきことについて、より多くの情報に基づいたきめ細かな決定をします。ユーザーのトラフィックに問題がないと仮定することは*決して*ありません。例えば、あなたがよく知る社員が、あなたが使ってほしいと頼んだ SaaS アプリケーションを使って、その役職に適切なデータセットを利用している場合であっても、この 2 つのことを根拠に、それは問題ないと想定することはできないのです。


ポイント

トラフィック内で何が起こっているか、つまり、許可された接続の内部のインタラクションやトランザクションを知ることができなければ、セキュリティは脆弱になります。ユーザーがデータにアクセスしている場所の*近く*にセキュリティ機能を移動させ、エッジアクセスポイントにサービスを分散させることで、ユーザーをデータセンターにヘアピニングさせて戻すことなく、トラフィック内を見ることができます。こうすれば従業員はどこでも仕事ができ、あらゆる場所でセキュリティポリシーを適用できます。

高度な脅威対策はクラウドの方が優れている理由

既存のセキュリティ対策の 1 つである高度な脅威対策（ATP、Advanced Threat Protection）は、適切に実装された SASE でその範囲と効果が飛躍的に向上します。最近まで ATP は、特に悪意のあるファイル形式で外部から侵入してくる脅威からユーザーを保護するアプローチのことだけを意味していました。

ですが、クラウドのワークフローで効果を発揮するには、クラウドベースの脅威にも焦点を合わせる必要があり、そこには悪意のあるファイルだけでなくリスクとなる可能性のあるアプリケーションやシステムも含まれます。クラウドでは新しいタイプの攻撃を考慮に入れる必要があり、これには以下のものが挙げられます。

- ノートパソコン、タブレット、電話、IoT (Internet of Things) センサーやデバイスなどのエンドポイントやエッジ。これらは、クラウド接続を介して外部から社内システムに情報を送信する。
- クラウド。そこには SaaS アプリケーションや Web サイトなど、適正なもの、悪質なもの、その中間にあるものすべて（正規のサービスが悪質な行動をとる者に利用されている場合など）が含まれる。
- ユーザー。主に、企業名を使って行動する人々は評価や検証を受ける。

クラウドで効果的な ATP を実現するために必要なのは、能動的なアプローチです。脅威の発生を可能な限り防止し、発生した脅威をできるだけ迅速に検知しなければなりません。（Netskope では、さらに AI（人工知能）および ML（機械学習）分析サービスを導入して問題を認識する能力を高めています。）

次世代 SWG は、この大きな課題を解決する最前線を担うものとして Netskope Cloud Threat Exchange を提供しており、SASE プラットフォームに貢献するすべてのベンダーが結集して開発した最新の脅威インテリジェンスを SASE サービスに供給し続けています。次世代 SWG から得られる情報に加えて、ID 管理、エンドポイント保護、セキュリティ情報、イベント管理、その他の統合サービスからの特定の専門的な情報も提供されています。

ヒント

クラウドにはさまざまな脅威ベクターが存在し、その数は膨大です。1 つの組織だけでは到底対応できないため、セキュリティサービスプロバイダーが協力して、効果的な SASE を作り上げます。

SWG をクラウド向けに進化させる

基本的な Web の脅威だけを防御していた時代のセキュリティインフラには、ユーザーが悪質な Web サイトにアクセスするのをブロックしたり、Web からマルウェアなどのファイルをダウンロードしたりするのを防止するアプライアンスが存在していました。一般的には SWG と呼ばれるこうしたシステムは、*Web プロキシ*や*コンテンツフィルタリング*などとも呼ばれ、ユーザーがリクエストした URL を事前に読取り、通信アプリの使用状況を監視し、受信トラフィックに既知のマルウェアやウイルスが含まれていないかを監視します。

もちろん、こうした機能は依然として必要です。次世代 SWG（第 2 章を参照）には、これらの基本的な SWG 機能が備わっています。さらに、次世代 SWG にはより充実したインスペクションのサービスや豊富なコンテキスト情報へのアクセスがあるため、クラウドによって出現した新たな脅威に対してより強力な防御で対抗することができます。例えば、次世代 SWG にはマルウェアのダウンロード防止機能が依然として備わっていながらも、Dropbox、Google Workspace、Microsoft Office 365 などの SaaS やクラウドベースのサービスを利用する際のトラフィックを内部から監視することができます。これにより、ユーザーの作業環境が完全にクラウド上にあり、企業のローカルシステムにダウンロードされていない時でも、ユーザーの環境を保護することが可能になります。

これらすべてを適切な方法で実現した場合、ユーザーはより安全な環境でより多くの仕事ができるので、生産性は向上します。従業員が貴重な資産を侵害したり、コンプライアンスやガバナンスに違反する心配をしたりすることなく自由に能力を発揮できたら、企業は、脅威から従業員を保護しながら利益を上げることが可能になるでしょう。

本章の内容

- セキュリティの潮流を変えるハイレベルのポリシー設定
- 次世代 SWG のスーパーパワーでアクセス場所を問わずデータをコントロール
- 管理されていないクラウドアプリやサービスの課題を克服
- シングルパスインスペクションの実例
- 効果的なデータ保護にゼロトラストが不可欠な理由

第4章 データとアプリケーションの保護

従来は、データ保護と言えば、データセンターを取り囲む境界の内部ですべてデータを安全に保管することでした。今日、データやアプリケーションはデータセンターという要塞の外部やクラウドにあり、データ保護についての古い概念からは脱却すべきです。

本章では、データ保護を成功に導くために取るべき方法、企業の機密データの悪用や脆弱化の防止に役立つ Netskope SASE テクノロジーについて検討していきます。

ポリシーの力で複雑さを解消

これまで、セキュリティチームにはスキル面だけでなく管理できる範囲にも限界がありました。彼らの主な防御策は、ファイアウォール、SWG（セキュア Web ゲートウェイ）、CASB（クラウドアクセスセキュリティブローカー）など、さまざまなセキュリティアプライアンスをスタックするこ

とでした。一貫性のないセキュリティ環境にさまざまな専用アプライアンス、そこには本質的な限界があります。最悪なのは、これらの専用機器をどのように動作させるかの調整を終えても、こうしたシステムにはクラウドを適切に保護したり、協調して脅威を防止したり対応するための可視性、適用範囲、能力もないことです。唯一の選択肢はアクセスをブロックすることですが（図 4-1 参照）、ユーザーコンテキストが利用可能なためにポリシーが意味をなさないことがあります。

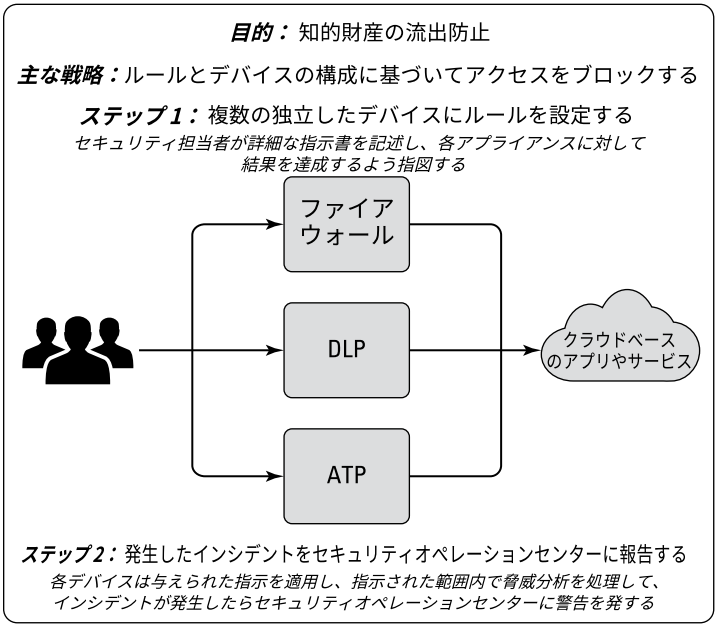

図 4-1： コンテキストに関係なくアクセスをブロックする。

Netskope はこのバラバラに分散する問題を一掃します（図 4-2 を参照）。セキュリティチームは幅広いマクロレベルのポリシーを設定できます。つまり、求める結果を記述することで一貫した一連の指示を作成するということです。次世代 SWG（NG-SWG）は、こうした指示を実行に移すことを支援し、お客様が求める結果を達成するために、セキュリティ サービスを調整したり指示を与えたりします。

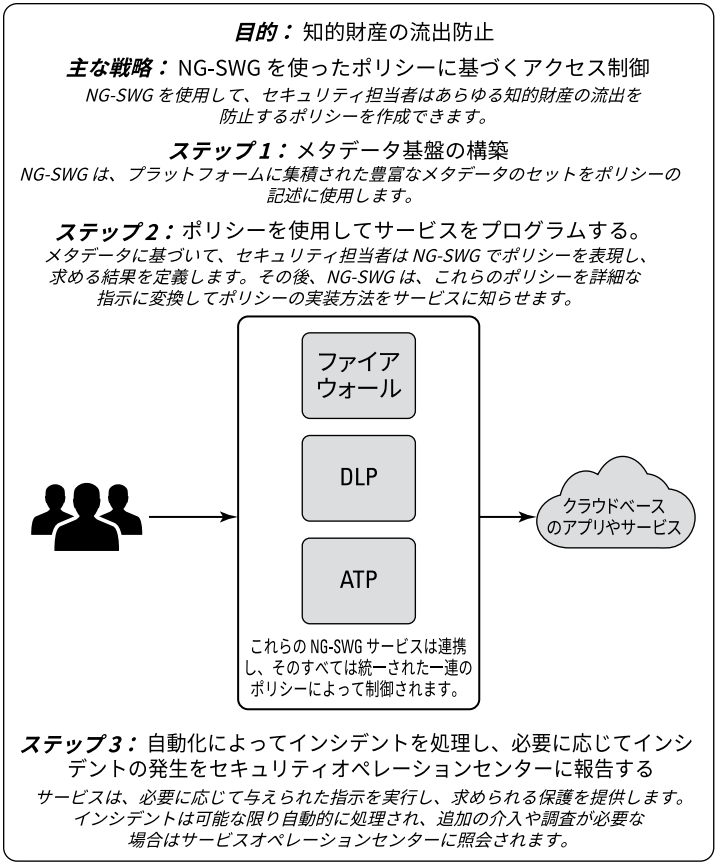

図 4-2: 広範なポリシーがセキュリティサービスに指示を与え、求める結果を達成する。

許可かブロックかだけで制御する初歩的なアプローチとは異なり、コンテキストやニュアンスまでを考慮する特定のポリシーで制御すれば、管理に要するデバイスやルールを減らせるだけでなく、より多くのユーザーがアプリやサービスを利用できるようになることで生産性は向上するでしょう。企業のセキュリティチームにとっても、仕事を簡素化できるアプローチと言えます。管理すべきデバイスや記述すべきルールが減れば、エラーが発生する可能性も低下します。ニーズの変化に伴ってシステムを維持、変更することも容易になります。基盤となるシステムに更新・改善があっても、ポリシーは変わりません。変更によってセキュリティフレームワークが破壊されることがないため、新たな脅威に対応しなければならない時でもサービスを迅速に進化させることができます。

データの保護

SASE（Secure Access Service Edge）が登場する以前は、DLP（Data Loss Prevention、データ損失防止）システムが企業ネットワークの外へ出ていくデータを追跡し、不正使用や共有を防ぎ、コンプライアンス要件を遵守するために使用されていました。現在では、企業のデータはクラウドサービスやアプリケーションなど外部に存在するようになるとともに、クラウド上のアプリケーション内やアプリケーション間を移動し、エンドポイントを通過することすらない場合もあります。

Netskope は Web トラフィックとクラウド上のアクティビティ両方を監視して、すべてのデータを保護します。次世代 SWG が学習した内容を記憶し、セキュリティサービスを継続的に強化します。特別な制御を行うことで、使用されているクラウドサービスがマネージドでもアンマネージドでも、ユーザーがオフィスにいてもリモートでも、次世代 SWG はユーザーの行動を認識することができます。そして、ユーザーが各サービス内で何をしているか、サービス間で何が起こっているかを認識します（例えば、従業員がマネージドサービス内で機密データをダウンロードした後、そのデータを個人の Gmail アカウントにアップロードしようとした場合など）。

次世代 SWG はセキュリティポリシーを自動で実施してしてデータを保護します。例えば、機密情報の共有を禁止するポリシーを設定すると、次世代 SWG は、DLP サービスと画像分類を使用してユーザーが機密テキストを含む Microsoft PowerPoint のスライドやホワイトボード画像のスクリーンショットをキャプチャしたことを検知します。これにより、スクリーンショットを E メールで送信したり、管理されていない共有ドライブや個人の共有ドライブにアップロードしたり、Web フォームでデータを共有したりすることを防止します。


ポイント

人工知能 (AI) と機械学習 (ML) はデータ保護の水準を押し上げます。Netskope 次世代 SWG では AI と ML を使用して、より正確に、細かいニュアンスまでコンテキストを検知するための後押しをしています。こうしたテクノロジーによって、以下のような特殊な機能を実現しています。

- **パターンと画像の検出：**情報の分類を支援するアルゴリズムを使用して、動的な Web ページのリスク評価を提供したり、悪意のある文書や機密情報の画像を検出する
- **アノマリー検知：**データや行動において、稀であったり、異常であったり、逸脱のある状態を認識する

AI や ML による特殊な分類を行い、パスポート、ホワイトボード画像、運転免許証、スクリーンショットなどの機密データを認識して、どのような種類の画像がやりとりされているかを判断します。また、文書の種類を分析して、ソースコードや履歴書などの保護されたデータソースを検出する分類もあります。この機能は、膨大なデータ量を保護する重要性が増した今日、データセキュリティの正確性と効率性を大幅に向上させています。

アプリケーションの保護

今日の組織が依存しているアプリケーションは、マネージドアプリケーション、アンマネージドアプリアプリケーション（*シャドー IT* と呼ばれる）、パブリッククラウドサービス、パブリッククラウドにホストされたカスタムアプリなど、いくつかに分類されます。

従来、セキュリティチームはファイアウォールの更新さえ行えば、外部の脅威からアプリケーションを守ることができました。その後、Web アプリケーションファイアウォールによってさらにセキュリティ機能が追加されましたが、データセンター内部で実行される Web アプリケーションの保護に限られていました。

クラウド アプリケーションが登場した時、クラウド アプリケーションベンダーは、管理用の API（Application Programming Interface）を提供するよう求められました。API によって、IT 部門はユーザーのアプリケーション内での動作を可視化し、いくぶんかのコントロールが可能になりました。こうしたクラウド アプリケーションには、Salesforce、ServiceNow、Workday などがあり、*マネージドアプリケーションまたは承認アプリケーション*と呼ばれるようになりました（第 2 章を参照）。

Netskope は CASB としてこれらのアプリを管理する最初のツールの一つを提供しました。このツールは、Google、Microsoft、Salesforce などが提供する API を利用して、これらのアプリ開発者が組み込んだ監視機能や制御機能へアクセスすることができました。


注意

セキュリティチームにとって頭が痛いのは、多くの重要なアプリケーションが管理用 API を公開していないことです。こうしたアンマネージドアプリは、IT スタッフが信頼性、セキュリティ、安全性を評価できる場合もあります。ただ、これまでの章で述べてきたとおり、従業員は好きなアプリを使用することが多く、未承認で監視されないシャドー IT になってしまいます。

一方で、次世代 SWG は従来の SWG とは異なり、CASB の機能が大幅に拡張されています。Netskope Security Cloud 全体に分散して搭載されているディープインスペクション機能は、従業員が使用するすべての Web アプリやクラウドベースのアプリの HTTP/S（Hypertext Transfer Protocol/Secure）や API トラフィックを監視します。これには、以前は CASB では見えなかったマネージドアプリ / サービスやアンマネージドアプリ / サービスも含まれます。ついに、シャドー IT が表に出てきます。

Netskope は、何千、何万というクラウドアプリやサービスを見つけ、それぞれにリスク評価レベルを付与します。このリスク評価は、Netskope の持つリソースや業界のさまざまな脅威検出サービスからの情報源を使ってクラウドサービスのリスク対策を客観的に測定する指標である、Netskope Cloud Confidence Index（Netskope クラウド信頼性指標）に基づきます。次世代 SWG はこの評価をユーザーやセキュリティ部門に通知したり、評価に基づいてセキュリティ ポリシーを実施できます。ユーザーが Microsoft Office 365 などの組織で利用するクラウドサービスにログインするとその活動が監視され、そのインスタンスでダウンロードしたデータを、管理されていない危険なクラウドアプリにアップロードしたりすることができなくなります。

Netskope の実際

第 2 章で、Netskope 次世代 SWG シングルパスインスペクションのアプローチについて説明しました。ここでは、次世代 SWG がこのアプローチでデータとアプリケーションを保護する仕組みを詳しく見ていきます。

- **ステージ 1：**次世代 SWG は、クラウドサービスやアプリケーションの複数のインスタンスを識別し、電子メールや生産性アプリケーションの個人、サードパーティ、企業の各インスタンスを区別します。使用するのは Netskope Cloud Confidence Index 評価システムで、悪意のある Web サイト、リスクのある SaaS（Software as a Service）アプリケーション、安全でないクラウドサービスなどへのアクセスをブロックします。また、マルウェアや高度な Web からの脅威が拡散するのを積極的に防止します。
- **ステージ 2：**ユーザーの ID、ロケーション、デバイス、ネットワークと言ったメタデータを使用して、そのコンテキストに基づいて各セッションでのアクセスレベルを調整します。例えば、完全に認証された従業員であっても、パブリック WiFi に接続して個人のタブレットを使用していると次世代

SWG が判断した場合、重要なマネージドクラウドアプリケーションへのアクセスを阻止することができます。

- **ステージ 3：**データ漏洩のリスクを減らすため、ユーザーの特定の活動に対して制御を実施します。文書のアップロードやダウンロード、スクリーンショットの共有、ウェブフォームへの入力、ソーシャル メディアなどのサービスへの作成・投稿・公開などに関するルールが、各アプリケーションやインスタンスに適用されます。
- **ステージ 4：**これまでのステージで許可されたすべての活動を継続的に監視するとともに、異常や脅威を監視します。やり取りされる機密データを認識し、そのデータの機密性、操作の種類、他の関連パラメータに基づいて、即時に対応します。ML で強化された画像分類やパターン検出技術がここで駆使されます。次世代 SWG は、特定の操作をブロックしたり、アラートを作動させたり、ユーザーに目的を尋ねたり、ステップアップ認証を求めたり、セキュリティチームがさらに検査すべきデータを隔離することができます。次世代 SWG が提供するコンテキストは非常に詳細なため、誤検知はほとんどありません。

適切に実装された SASE の原則を 次世代 SWG が広範囲に適用しているため、データやアプリケーションの場所を問わず、どこから、どのようにアクセスされても保護されます。

データ保護におけるゼロトラスト原則の重要性

ゼロトラスト原則の適用は、過去 10 年間のセキュリティにおける最も重要な開発の 1 つであり（第 3 章を参照）、データ保護に関するいかなる率直な議論もこの原則なしでは成立しません。この原則は、データにアクセスするユーザーは基本的に信頼すべきではなく、アプリケーションやデータへのアクセスは可能な限り最小限に止めるという考え方に基づいています。ZTNA（Zero Trust Network Access）などのゼロトラストの実装は、セキュリティおよびネットワーク業界ではよく知られています。では、データ保護にとってゼロトラストはどのような意味を持つのでしょうか？

クラウド以前の他のフレームワークと同様に、DLP（Data Loss Prevention）は、重要なものはすべてデータセンターの中にあり、ネットワーク境界で保護されているという考えに基づいて構築されました。当時のデータ保護の役割は、データが不適切な方法で外部に漏れるのを防止することと、許可されていない個人が境界の内部に侵入してデータにアクセスするのを阻止することでした。

現在のクラウド時代には、このようなアプローチは通用しません。確かに、一部の重要なデータはデータセンター内（従来の境界の内部）にありますが、少なくとも同じ量のデータが（そしてその量は増加の一途にある）、SaaS アプリケーションやパブリッククラウド上のアプリケーションに移行しています。より広く、より動的に進化した攻撃対象を保護するため、企業は、最近のユーザーの新しい働き方に対応してデータ保護を再検討しなければなりません。必要なのは、ユーザーが必要な時に、必要なデータだけにアクセスを許可する方法です。

2021 年に Netskope が最初に説明した言葉、*Zero Trust Data Protection* は、リスクとコンテキストに基づいて、継続的かつリアルタイムにアクセス制御とポリシー制御を提供するセキュリティのアプローチです。コンテキストはユーザーとアプリ間で何が起こっているかの理解を助けるとともに、ユーザーは誰か、何をしようとしているか、その理由は何かを深く理解した上で、データアクセスをどのように許可・却下すべきかを示唆してくれます。これにより、セキュリティチームは、データの機密性、アプリケーションのリスク、ユーザーの行動によるリスク、その他の要因に基づいた条件付きの制御をすべてリアルタイムで定義し、実施することができます。継続的なリスク管理によって、より効果的なセキュリティ体制を実現できます。

この継続的なリスク管理アプローチは、生産性を維持するためにクラウド アプリやデータへの常時アクセスが必要なリモートワーク主体の従業員がいる場合に、サードパーティ アプリの組み合わせでリスクを動的に管理することのできる、唯一の効果的な方法です（第 2 章を参照）。

ゼロトラストデータ保護は、DLP を単に新しくした概念でも、*ゼロトラスト*という言葉の人気を利用して生み出した新しいマーケティング手法でもありません。それは、クラス最高の SASE とは何かという核心に迫り、どこからでもアクセス可能なクラウド時代に向けたセキュリティやネットワークの変革を促し、あらゆる場所でデータ保護を可能にするアプローチです。SASE とゼロトラストデータ保護への統合的かつ包括的なアプローチは、真の SASE 技術を提供するプロバイダーと模倣するだけの亜流プロバイダーとの一線を画します。

本章の内容

- 自社のクラウドセキュリティ体制を完全に把握する
- データセンターの外での行動を観察することでリスク評価の精度を上げる
- 誰が、どこで、どんなデータを移動させようとしているかを制御する
- 大規模なテレワークの実現とテレワーカーの保護
- クラウドと安全に連携させるためのデータセンターの再構築

第5章 SASEを実現するための7つのステップ

本章では、SASE（Secure Access Service Edge）を導入する際に、どこから開始してどこへ到達すれば最適化できるのか、また、その間に存在するステップなど、段階的なアプローチをご紹介します。

一連の7つのステップでSASEの導入をいかに成功させるかを簡潔にご覧いただけます。各段階で、組織のセキュリティ体制を大幅に改善してリスクを管理し、従業員や顧客が求めるエクスペリエンスを提供するという目標に向けて大きく歩みを進めていけることでしょう。

ステップ1：目的地の決定

新しいプロジェクトを担当したら、CIO（最高情報責任者）、CISO（最高情報セキュリティ責任者）、または企業のネットワークとセキュリティに経営レベルで責任を負う人々が直面している重要な課題に、今日中に（あ

るいは、少なくとも非常に迅速に）数値で結果を見せることが非常に重要になります。長期の開発サイクルが許容されていることもある一般的な IT プロジェクトとは違って、セキュリティはすぐに価値を提供し、迅速に成果を上げなければなりません。脆弱性や不正行為などは、可能中桐早急に対応すべき敵なのです。

SASE は、セキュリティを現在において提供すべき方法や、セキュリティとネットワークのさらなる（好都合な）融合を考慮に入れたアーキテクチャを用いて、この脆弱性や不正行為などに対処します。ただし、真の SASE は長期的な進化のプロセスを経て実現させるもので、組織は SASE の実現に向けて成長していくのです。成功への鍵を握るのは、目に見える勝利、つまり計画的な達成を重ねていくことで、実証ができて意義のある方法で組織のセキュリティを持続的に拡大、強化していくことです。

ですが、そのためには、出発地点と目的地を知らなければなりません。

SASE 実現への道筋を情報に基づいた投資と実装として捉え、そのプロセスこそが事業に大きな変革をもたらすと信じて進めば、データセンターを中心とした狭い世界観から脱却し、クラウドがもたらす多くのメリットを完全かつ安全に享受できる企業へと導きながら、継続的かつ劇的な成果を得ることができます。

ステップ 2：課題の認識と可視化の重要性

問題を解決する最初の一歩は、問題の存在を認めることです。本書では企業のセキュリティ対策が、現代のセキュリティやアクセスニーズに追いつけなくなってきた現状があるにも関わらず、従来のままデータセンターに依存してしまっていることの問題点を解説しています。

企業のアプリケーショントラフィックとユーザーの半数以上は、組織の管理下にないネットワーク上で活動しています。これは、新型コロナウイルスの流行によって在宅勤務が新しい常識になる前の話です（第 1 章を参照）。

企業もその従業員も、「管理できないものがある」ということの深刻さやその量の多さを理解し、管理できないものが多くあるという状態が企業のビジネスにおいて普通の状態となってしまっている現実を受け止める必要があります。次世代 SWG を導入することで、たった 1 つのサービスであっても、そこに対して何が起こり、何が保護されていないかを把握できるようになります。

ヒント

どのようなソリューションでも自信を持って導入するためには、少なくとも、クラウドでのユーザーの行動を完全に可視化する必要があります。また、組織の意思決定者の同意も必要です。意思決定者が、リスクにさらされていることに気付いていない重要な資産を SASE が保護してくれると認識すれば、賛同を得ることができるでしょう。何百万ドル、さらには何十億ドルもの価値が、「会社の外」で起こっているものから生まれているのです。

ステップ 3：ユーザーとアプリの間に検査ポイントを配置

次世代 SWG（セキュア Web ゲートウェイ）を適切に導入し、すべてのトラフィックへの可視性が飛躍的に向上したところで確かなことが 1 つあるとすればそれは、見えたことにより、色々なものが気になってしまうだろうということです。

従業員は Microsoft Office 365 を使っているか？ Salesforce は？ Workday はどうだろうか？ Box は？その答えがイエスであることはほぼ間違いありません。ですが、セキュリティの境界を越え、目に見える環境の外にあるクラウド環境は、どのくらいの規模で、どのくらい成熟しているのでしょうか。あなたの組織のデータのうちどれくらいが、外部の環境で誰にもチェックされずに動き回っているのでしょうか。

可視化により組織のデータがどれほどリスクにさらされてきたか、初めて気付くことになります。多くのデータが行き来し、その一部は機密性が高いものである可能性があるにもかかわらず、セキュリティが確保されていないサイト、サービス、アプリを出入りしています。

そして今、クラウド環境への依存度に関して組織が置かれている状況が明確に分かってきました。内容は、非常に懸念点の多いものでした。非常に多くのアプリやサービスが使用されており、しかし効果的なセキュリティ管理はほとんどされていないという状況が現在に至るまで続いてきました。

次世代 SWG は、クラウドおよびデータセンター内を行き来するあらゆるトラフィックに対して、シングルパスで、ファネル（じょうご）状の主要検査ポイントを設置します（第 2 章を参照）。この主要検査ポイントは、従来の境界よりも遥かに優れています。

ポイント

見て見ぬふりをされてきたシャドー IT の結果であれ、意図的に進められてきたビジネスのデジタル化のせいであれ、時代遅れになった古いセキュリティシステムでは詳細までは視認できませんでした。従来の SWG やそれに類するアプライアンスを置き換えることで、エンタープライズグレー

ドのアプリケーションやサービスを使っていないのは誰か、組織の管理が及ばない「外部」にどのような企業データが送信されているかをようやく完全に可視化できるようになります。表 5-1 に示すとおり、次世代 SWG というクラウド上の新しい検査ポイントを介して、Web、管理された SaaS（Software as a Service）、シャドー IT アプリ、パブリッククラウドサービス、パブリッククラウド内のカスタムアプリなど、すべてのトラフィックの内部で何が起こっているかを確認することができます。

表 5-1　検査ポイントを使ったトラフィックの監視

置き換えるべき従来機能	Netskope が提供する機能	Netskope と統合するシステム
従来の SWG - Web トラフィックにイエス / ノーだけで対処する。	すべてのトラフィックを詳細に検査する。その対象には、Web、管理された SaaS、シャドー IT アプリ、パブリッククラウドサービス、パブリッククラウド上のカスタムアプリが含まれる。	シングルサインオン（SSO）ソリューション
SSL（Secure Sockets Layer）アプライアンス。	SSL / TLS の復号化を、アプライアンスを必要とせず、クラウド上でクラウド規模で実行する。	
従来の CASB（Cloud Access Security Broker）- API（Application Programming Interface）を提供する管理されたアプリのみを監視する。	管理されたアプリに加えて、API を提供しない管理されていないアプリも監視する。また、アプリ、サービス、Web サイトで使用されているデータも監視する。	

ステップ 4：Web、クラウドへのアクセスやアクティビティにゼロトラストの原則を導入

この段階は、SASE の基盤を構築しながらテクノロジーの有効活用を始める時期です。幸いなことに、Netskope のプラットフォームには、これを適切に進めるのに必要な機能が組み込まれています。企業ネットワークだけでなく、最終的にはクラウド上のあらゆる場所で、企業データの管理を再構築するのに必要なすべての機能が備わっています。

表 5-2 に示すとおり、ステップ 3 では、従来のアプライアンスで使用されていた「イエス」か「ノー」かだけで判断する機能ではなく、拡張されたセキュリティ制御を活用してコンテキストを確認します。また、次世代 SWG は、Web トラフィックとクラウドトラフィックの両方を詳細に検査します。新たな検査ポイントを設置したことで、データの移動やアクセスを細かく制御できる機能が備わり、ビジネスに適したポリシーに基づいたリスク管理が可能になります。

表 5-2　リスク管理のためのポリシー設定

置き換えるべき従来機能	Netskope が提供する機能	Netskope と統合するシステム
データセンター内だけを保護する、従来の DLP（Data Loss Prevention）。	あらゆる場所を移動するすべてのデータを保護する、高度な DLP。	セキュリティ情報・イベント管理システム、エンドポイント保護システム
ユーザーおよびエンティティの行動分析（UEBA）	拡張された異常行動検知機能と、ユーザーリスクスコアリング機能。	
さまざまなサンドボックスソリューション。	サンドボックスや機械学習に基づく、異常検知などの高度な脅威防御（ATP）。	

ステップ 5：ゼロトラストの原則をデータ保護とプライベートアクセスにまで拡張して適用する

トラフィックへの理解が深まり、何が起こっているかを把握し、データ保護のポリシーを実施できるようになった組織は、従業員の勤務形態をリモートファーストにするという目標を実現することができます。従業員はどこからでも仕事ができるようになり、データ、アプリケーション、従業員を高いレベルで保護しながら柔軟性と生産性を保つという素晴らしい体験を提供することができるようになります。

最も顕著な変化は、従来の VPN（Virtual Private Network）からの脱却です。そこには、インターネットに向かうすべてのリモートユーザーのトラフィックにデータセンターを経由することを強いていた、長く、

非効率なヘアピニングはもうありません。Netskope NewEdge を活用することで、セキュリティポリシーを適用してデータを保護しながら、こうしたトラフィックを効率的に目的地まで導くことができます。

*ゼロトラスト*とは、ユーザーが何かを企んでいる可能性があるという前提を常に適用し、データがどこにあっても常に保護されるように徹底することです。Netskope プラットフォームは、ユーザー、デバイス、ネットワーク、行動、その他の何百もの詳細に関する深いコンテクスト情報を使用して、ポリシーで許可されたものだけに活動を制限し、ユーザーが本人であることを識別します。

このプラットフォーム導入後、組織のセキュリティとネットワークは、クラウドを使用する従業員やデータセキュリティのニーズを満たすものに進化します（表 5-3 を参照）。

表 5-3　テレワーカーのニーズを満たすセキュリティとネットワーク

置き換えるべき従来機能	Netskope が提供する機能	Netskope と統合するシステム
従来の VPN	ポリシーに基づいてトラフィックをルーティングし保護するセキュリティクラウド	SD-WAN（Software-defined Wide Area Network）プロバイダー
	ZTNA（Zero Trust Network Access）	ユーザーやグループの ID を管理・検証する ID 管理システム
	Zero Trust Data Protection - ゼロトラストに基づくデータ保護	

ステップ 6 ：データセンターに置くアプリや、アクセス方法を見直す

データセンターは、人とデータが行き来する場所の 1 つにすぎず、もはや関心の的ではありません。SASE アーキテクチャの構築が進んできたら、データセンターの見直しを図る時期だと思ってください。

データセンターには、移行に手間のかかりすぎるアプリケーションや、監視下に置いておきたい重要なアプリケーションが残っているかもしれません。こうしたアプリケーションへのアクセスには、VPN を使用せずに世界中から安全にアクセスできる Netskope Private Access の機能が役立ちます。

SASE アーキテクチャで Netskope プラットフォームサービスに代替された、その他の一連の製品についてはどうでしょうか？これはまさに、複雑化したネットワークやその維持費を大幅に削減するチャンスです。従来のシステムが徐々に価値を失って過去のものとなる中で、企業とその担当者は前を向き踏み出しましょう。

表 5-4 に、Netskope のプラットフォームで置き換えることのできる従来のシステムやテクノロジーをまとめました。

表 5-4　データセンターへの安全なアクセスの提供

置き換えるべき従来機能	Netskope が提供する機能	Netskope と統合するシステム
ファイアウォール、IPS（Intrusion Prevention System）、DNS（Domain Name System）	多数のサービスの 1 つとして、ファイアウォールによる保護を提供	従来のデータセンターでの侵入制御

真の SASE は継続的な運用コストの削減を可能にします。適切に導入された SASE アーキテクチャでの成功事例を表 5-5 に示してあります。財務部の方をはじめとして、数多くの利害関係者から感謝状が届くかもしれません！

表 5-5　継続的な運用コストの削減

領域	何が起こるか	推定削減額
マルチクラウドへのアクセス	マルチクラウド戦略を実現 ユーザーエクスペリエンスの向上 調達と導入作業の合理化 ビジネスユニット主導のアプリケーションを実現	接続およびインフラストラクチャで 30% 将来のクラウドコストで 20%
VPN 置き換え	VPN アプライアンスの廃止 帯域幅の使用が多いアプリに対する Direct-to-Net 通信 VLAN（Virtual Local Area Network）やファイアウォールポリシーの変更の低減	ハードウェアコストの 80% セキュリティ変更や管理費用の 50%

(continued)

表 5-5 *(continued)*

領域	何が起こるか	推定削減額
ビジネスパートナー	サードパーティのアクセスを管理 公開アプリケーションへの直接アクセス アクティビティに対するきめ細かい制御を適用 ラテラルムーブメントの余地を排除	ハードウェアコストの 80% サポート時間の 20%
企業の合併買収（M&A）	オンボーディングと統合の効率化 現在と将来のネットワークおよびセキュリティ費用を統合 ポリシーを同期させる	ハードウェアコストの 40% オンボーディングが 5 倍効率的に

ステップ 7：監視、評価、そして最適化

SASE への道のりには時間がかかりますが、そのすべての段階において、セキュリティチームと組織に大きな変革をもたらす機会を提供してくれます。その道のりを経て、セキュリティは確かに向上しますが、効果はそれだけにとどまりません。従来のセキュリティ機器のメンテナンスやアップグレード、交換が不要になるので、コスト削減効果をすぐに実感できるでしょう。さらに素晴らしいのは、クラウドに完全に最適化されるため、今までのように容量が過剰かつ、高額な設備投資が必要なセキュリティアプライアンスを購入する必要もありません。

一方で、SASE を支える原理は一貫していても、SASE の仕組みはそれぞれの企業によって異なるでしょう。SASE を活用し、健全性を維持するためには、SASE がどの程度適切に機能しているかを監視し、改善が必要な箇所を評価し、導入後も最適化するためのステップを実行しなければなりません。

時間をかけて継続的に改善していくことで、利益を守ることができるでしょう。次世代 SWG がプラットフォームの一部として企業のセキュリティにもたらすメリットは、いくら強調してもし過ぎることはありません。従来セキュリティ部門は、何十もの複雑で独立したセキュリティ用

アプリケーションがアラートを出すと短時間のうちに様々なログを確認し、それらを関連付けることに追われていましたが、今や、統合され自動化されたプラットフォームがリアルタイムで機能しています。すべてのセキュリティサービスがメッセージを共有し、その内容に一貫性が保たれることでエラーを減らし、ブレのない行動を迅速に取ることが可能になります。そして、チームの皆さんはより多く行動に移せることで、セキュリティをさらに向上させ、ビジネスを円滑に運営できるようになるでしょう。

ですが、最も重要なのは、次世代 SWG を備え適切に導入された SASE によって、ビジネスの運営、従業員とテクノロジーの関係、ネットワークチームとセキュリティチームの関係に変化が起きることです。シャドー IT が表に出て来ることで真のデジタルトランスフォーメーションが可能になり、必要なアプリケーションやツールを迅速かつ安全に導入して、効率性を高め、ビジネスチャンスを活かすことができます。ユーザーエクスペリエンスが適切に維持されてユーザーの満足度は上がり、生産性が高まります。このようなことは、セキュリティがデジタルイノベーションやクラウドサービスの普及を確実にサポートし、デジタルトランスフォーメーションの優先事項の実現に向けてネットワークやビジネスのあらゆる部分と連携させることで初めて可能になります。そして、それこそが、真の SASE で得られる成果です。

データを保護し、持続的なビジネス価値を生み出す SASE アーキテクチャの構築

制約の多いデータセンターから広く開かれた可能性のあるクラウドへと移行したデジタルの世界で機能するアーキテクチャといえるのは SASE だけです。CASB（Cloud Access Security Broker）、次世代 SWG（次世代セキュア Web ゲートウェイ）ゼロトラスト原則といった成功への要素を組み合わせた優れた設計の SASE で、ユーザーの満足度向上、データの保護、ビジネスの成長を実現できます。

本書の内容...

- データ、アプリケーション、ネットワーク、セキュリティの進化について学ぶ
- SASE アーキテクチャにおける CASB、次世代セキュア Web ゲートウェイ、ゼロトラスト原則の役割を理解する
- テレワーカーを大規模に保護し、ユーザーのエクスペリエンスを総合的に改善する
- 企業のセキュリティとネットワークの将来に向けて、確実な計画を策定する

Netskope を率いるリーダーの **Jason Clark**（CSO）、**Lamont Orange**（CISO）、そして **Steve Riley**（フィールド CTO）は、クラウド、セキュリティ、ネットワークの権威として広く知られており、Ernst & Young、Gartner、Optiv、Riverbed、Websense などのグローバル企業で数十年の経験を積んできたエキスパートです。

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-85535-4

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.