MENLO SECURITY

ネットワークセキュリティアプライアンスからクラウドベースのセキュアWebゲートウェイ（SWG）への移行

ユーザーおよびアプリケーションのワークロードがクラウドに移行するのに伴い、セキュリティアーキテクチャもそれに対応して完全かつシームレスな保護を提供しなければなりません。
アイソレーション機能を活用したセキュアWebゲートウェイ（SWG）を採用することで、完全に統合されたSecure Access Service Edge（SASE）へのアプローチを確実に進めることができます。

Solution Brief

かつてはエンタープライズセキュリティの定番と考えられていたオンプレミスのWebプロキシは、現代の業務環境を保護するために最適ではありません

この技術が最初に導入された頃に比べると、今では技術が変化しただけでなく、世界中の知識労働者の働き方が劇的に変化しています。最新の業務環境においてはユーザー、データ、アプリ、およびサービスは高度に分散化されており、オフィスや家庭、データセンター、およびクラウドなどのサービスを利用してコラボレーションしながら業務を行っています。インターネットのトラフィック量は急増しており、毎月200エクサバイトを超えるトラフィックがインターネットのバックボーンを通過しています。従来のオンプレミス型のWebプロキシを使用してこれらの急速に増加するトラフィックを保護するためには、企業は追加のハードウェアを導入展開する必要があり、その結果としてIT部門の管理および設定の負荷が増大します。さらに、これらの物理アプライアンスは高価であり、分散化しモバイル化する業務に合わせて拡張することは簡単ではありません。

現代の分散した労働力は、高速で安全かつ信頼性の高いインターネットアクセスを必要としています

COVID-19のパンデミック以前は、「たまに自宅で働く」ユーザーの割合は約20%で、「常に自宅で働く」ユーザーの割合はこれよりもさらに少ないものでした。しかしパンデミック後に多くの組織がユーザーを分散させ、急速に在宅勤務に移行しなければならなくなったことで、この割合は大幅に変化しました。

パンデミック後、自宅で働くユーザーは全体の70%以上に達しました [1]

1. Pew Research Center

ユーザーがどこにいても業務を行えるようになったことで、生産性の観点からは組織に多大なメリットがもたらされました。しかし大多数の企業は、このような急速な移行に備えていませんでした。パンデミックが発生する以前は、在宅勤務を推進するということは、VPNのスイッチを入れ、セキュリティアクセスポリシーを適用できる本社または中央のデータセンターにインターネットトラフィックをバックホールすることを意味していました。しかし、急速な在宅勤務への移行が要求されたとき、VPNコンセントレータはトラフィックに追いつくことができなかったのです。組織はこれに対応するための緊急避難的なソリューションとして、トラフィックをオフロードするためのスプリットトンネルVPNの導入展開を急ぎましたが、そのためには多くのハードウェアを取得しなければならず、分散したユーザーのために安全なローカルインターネットブレイクアウトを構築するプロセスには高額なコストと大きな負担がかかりました。また、今はユーザーがセキュリティ制御なしにインターネットに直接接続することを多くの組織が容認していますが、ブラウザーが「新しいオフィス」と考えられている現代においては、これは組織のリスクを劇的に高める結果となっています。

ユーザーがWebブラウザーを使う時間は、勤務時間の75%に達しています [2]

ブラウザー上でさまざまな業務が行われるようになったことに加えて、クラウドおよびSaaSアプリの利用も急速に拡大しています。平均的な企業は現在651個のSaaSアプリを使用しており、大規模な組織の場合、その数は指数関数的に増加します。[3]

パンデミックはサイバーリスクの「パーフェクト・ストーム」を生み出しました。これは、分散したユーザーと膨大なインターネットトラフィックに対応するために導入された新しい技術によって、攻撃可能な領域が拡大したためです。そしてこの問題への対処において、組織はレガシーなアプローチに依存せざるを得ませんでした。

ファイアウォールおよびウイルス対策エンジンからSIEMへのレポートとログ送信のためのデータ漏洩防止（DLP）ソリューションまで、これらのレガシーな技術では、アクセスと制御を管理するオンプレミスのWebプロキシと統合するために複数のベンダーのツールをインストールする必要があります。企業はこれらの断片をすべて取り纏めなければならず、ITの観点からは非常に複雑となり、管理負荷もかかります。そして複雑さの増大はセキュリティギャップに繋がり、それを攻撃者が狙います。

2. Google, "The future of enterprise: Your business, in the browser"
3. Zylo, "Zylo's 2020 SaaS Management Benchmarks Report"

FBIのIC3ユニットに報告されたオンライン犯罪は、COVID-19パンデミックが始まってから400%も増加しました [4]

最新のビジネス環境およびリモートユーザーがクラウドに移行したことで、インターネットおよびミッションクリティカルなSaaSアプリケーションへの高速で安全なアクセスがビジネスを継続するために必須の条件となりました。そして、従来のオンプレミス型のプロキシには、インターネットやSaaSアプリケーションを保護したり、DLP機能を提供したりする機能が備わっていないことも明らかになったのです。

Isolation Core™ を活用したメンロ・セキュリティのセキュア Web ゲートウェイ（SWG）が、生産性を保護します

メンロ・セキュリティのセキュアWebゲートウェイ（SWG）は、Isolation Core™ を活用し、これまでとは根本的に異なるアプローチによって企業が業務を保護するために必要とする機能を提供します。メンロ・セキュリティはすべてのSWG機能を単一のクラウドネイティブなプラットフォーム（CASB、DLP、RBI、プロキシ、FWaaS、プライベートアクセスなど）に統合し、拡張可能なAPIとポリシー管理、レポート、脅威分析のための単一のインターフェイスを提供します。そしてこれは、悪意のある攻撃を防ぐために最も安全なゼロトラストアプローチを提供し、エンドユーザーがオンラインで業務を行っている間はセキュリティを気にする必要を無くし、セキュリティチームの運用負担を軽減することでSecure Access Service Edge（SASE）の目標を実現する、唯一のソリューションです。

メリット

- **エージェントやエンドポイントを管理する必要無しに生産性を維持**
- **デスクトップ、ラップトップ、およびモバイルデバイスをサポート**
- **ネイティブのエンドユーザーエクスペリエンスを維持**
- **CPU/メモリを有効活用**

4. FBI, "2020 Internet Crime Report"

Isolation Core™を活用したメンロ・セキュリティのSWGはグローバルな柔軟性を備えたCloud-as-a-Serviceによって提供されており、ユーザーはどこからでもインターネットに安全に接続できます。企業はWebベースのサイバー脅威から保護され、すべてのデバイスとロケーションでのきめ細かいアクセス制御とコンプライアンスを保証します。メンロ・セキュリティのSWGは、他に例の無いパフォーマンスと規模でこれを実現するため、組織は既知および既存の脅威だけでなく将来の脅威にも対応することができます。

メンロ・セキュリティのIsolation Core™ は、すべてのWebコンテンツが危険であり、組織に危険をもたらす可能性があることを前提としています

ゼロトラストアプローチにより、曖昧な分類やフィルタリング、および説明できないポリシーに基づいて許可かブロックかを決定する必要がなくなります。メンロ・セキュリティのSWGを使用すれば、企業はアイソレーションかブロックかというポリシーを採用できるため、検知と対応による受け身の対応ではなく、セキュリティに対する真の予防的アプローチが可能です。

コンテンツが許可されると、Adaptive Clientless Rendering（ACR）技術がコンテンツをエンドユーザーのブラウザーに効率的に配信します。その際ユーザーエクスペリエンスや生産性に影響を与えることはなく、また特別なクライアントソフトウェアやプラグインも必要ありません。その結果セキュリティチームはセキュリティ体制に100%の信頼を持つことができ、エンドユーザーは安心してクリック、ダウンロード、ブラウジングを行うことができ、生産性を落とすことはありません。

レガシーなオンプレミスのWebプロキシからIsolation Core™を活用したSWGに移行するための方法については、menlosecurity.com/ja-jp/にアクセスするか、japan@menlosecurity.comまでお問い合わせください。

お問い合わせ：
www.menlosecurity.jp
japan@menlosecurity.com

Menlo Securityについて

メンロ・セキュリティは、他に類を見ないアイソレーションを活用したクラウドセキュリティプラットフォームにより、企業が脅威を排除し、生産性を完全に維持することを可能にします。メンロ・セキュリティは、悪意のある攻撃を防ぐために最も安全なゼロトラストアプローチを提供し、エンドユーザーはセキュリティの存在を気にせずにオンラインで仕事をすることができ、さらにセキュリティチームの運用負担を軽減することで、クラウドセキュリティの目標を実現できる唯一のソリューションとなっています。これにより企業は安全なオンライン体験を提供することができ、ユーザーは安心して業務を行いビジネスを進めることができます。