

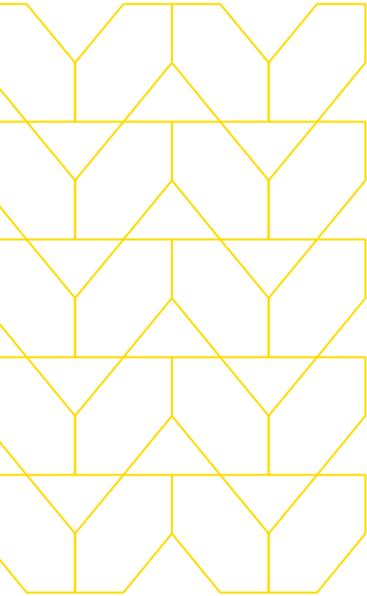


White Paper

# ゼロトラストで マルウェアの脅威を 排除

アイソレーションを活用したセキュリティで  
メールおよびWebベースの脅威に対する  
完全な保護を提供

## それは「起きるかどうか」ではなく、 「いつ起きるか」という問題です



残念ながら、多くの企業では、サイバーセキュリティの防御が限界を迎えるのは避けられないという見方をしています。インターネットの誕生以来ほとんど変わっていない現在のセキュリティ技術には根本的な欠陥があるため、部分的な保護に甘んじるしかありません。

これらは脅威を見つけ出し、それらがネットワークに到達するのを防ぐように設計されていますが、現在市場に出回っている製品では、ファイル、画像、ドキュメントなど、インターネットの何が安全かを100%正確に評価することはできないのです。

### 脅威を発見し、慌ててそれに対応するのではなく、 以下を目指すべきです：



組織にリスクを与えることのない、安全なクラウド  
アクセスを従業員のために確保する



フィッシング攻撃に遭ったときに、速やかに従業員  
に警告する



マルウェア、ウイルス、またはランサムウェアについて  
二度と心配しなくても良いようにする

メンロ・セキュリティは、これまでとは根本的に異なるアプローチを使用して、マルウェアからの脅威を完全に排除し、独自のアイソレーション機能を備えたクラウドセキュリティプラットフォームで生産性を完全に保護します。これは、悪意のある攻撃を防ぐための最も安全なゼロトラストアプローチを提供し、セキュリティから推測に基づく対応を取り除くことでクラウドセキュリティの目標を実現する、唯一のソリューションです。

ゼロトラストは、従来のサイバーセキュリティとは根本的に異なる、「デフォルトで拒否」のアプローチを採用しています。

## 検知と防止は誤った戦略です

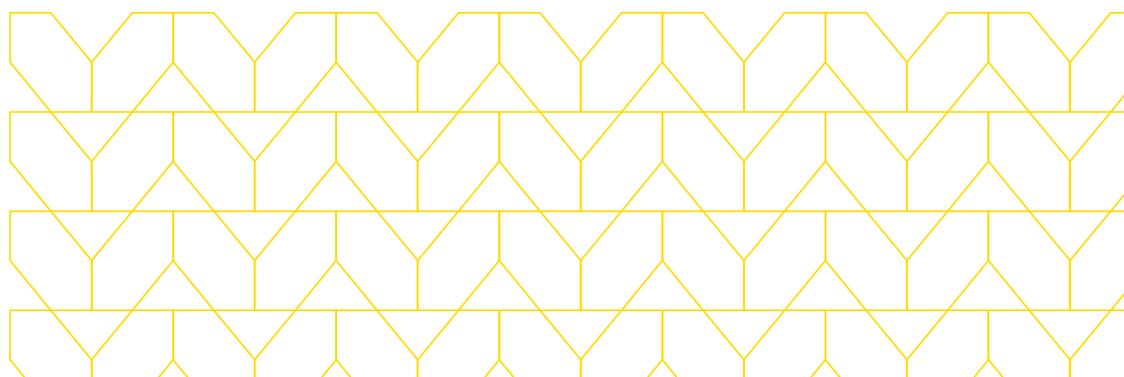
サイバー攻撃はますます巧妙化しており、メールの形で標的を絞ったフィッシング詐欺が増えています。技術に精通した従業員でさえ、最も重要な情報を漏らしてしまう可能性があります。Gartnerによると、クラウドアプリケーションの採用が進み、従業員は常に移動しているため、ブラウザが組織の生産性を上げるための最も重要なツールになっています。同時に、サイバー攻撃の大部分はメールまたはブラウザから始まり、偽のメールや感染した添付ファイル、Webサイト、ダウンロード可能なドキュメントを持つエンドユーザーを標的としています。組織、従業員、および顧客が晒されるリスクは増大し続けています。しかし、セキュリティ業界はこれまでと同じ古いアプローチ、つまり検知と防止に拘っています。

検知と防止はその可能性の限界に達しており、攻撃者はすでにそれを回避する方法を学んでいます。Verizonによると、2018年には41,686件のセキュリティインシデントが報告され、2,013件のサイバーセキュリティ侵害が確認されました。さらに悪いことに、侵害の68%は検知するまでに数か月以上かかりました。これは、攻撃をブロックし、侵害が発生したらそれを検知するという2つの主要な防御方法が無残にも失敗していることを意味します。

68%

侵害の68%は、検知までに数か月以上かかっています

Verizon, 2018 Data Breach Investigation Report



## 問題は悪化しています

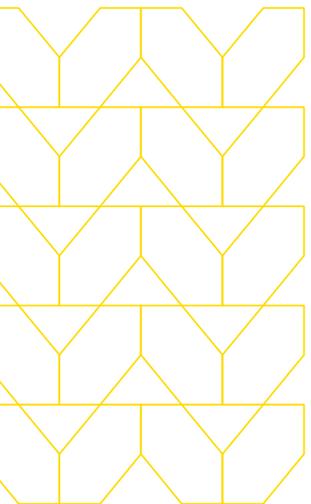
すでに数百万、さらには数十億ものマルウェア攻撃が作成されています。企業がクラウドに移行してSaaSの採用が進むと、ユーザーが安全な企業ネットワークの範囲外で攻撃に遭遇する可能性があります。クラウドやSaaSは、企業ネットワークのハブ&スポーク構造を破壊してしまいました。ユーザーが直接インターネットに接続するようになったことで、ネットワークセキュリティを回避することが可能になり、サイバーセキュリティが破られることで企業は数百万ドルの損害を被る可能性があります。

---

ある世界的な保険会社がWebマルウェアとフィッシング攻撃に晒された際、これらの問題の80%が、従業員が未知のセキュリティリスクを持つWebサイトにアクセスしたときに発生したことがわかりました。

感染したデバイスには、費用と時間のかかる再イメージ処理が必要になりました。従業員向けのフィッシング対策トレーニングは攻撃への対処にいくらか役立ちましたが、多くの従業員が感染したリンクをクリックし続け、認証情報の盗難やマルウェアの感染につながりました。

---

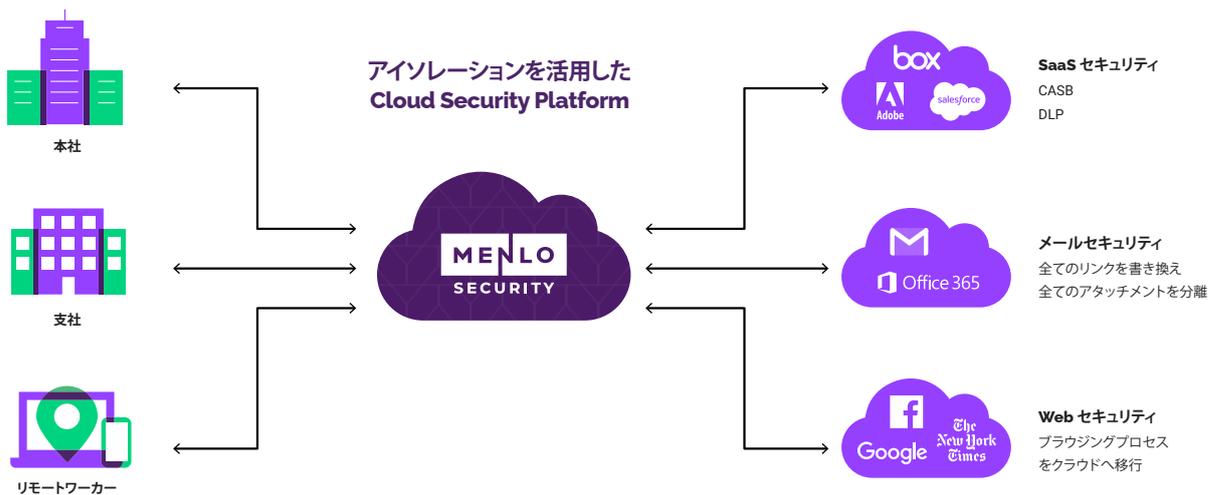


業界は脅威の検知能力を改善しようとしています。人工知能 (AI) に大きな期待が寄せられており、実際それは有望に見えます。膨大な量のデータ処理が必要なため、必要な計算規模を達成できるのは機械ですが、機械が人間の知能に劣らない真のAIを実現するのは、まだ何年も先でしょう。今現在増大し続けている危険な問題に対処するためには、セキュリティパラダイムを根本的に考え直す必要があるのです。

**アイソレーションによって実現するゼロトラストは、メールやWebからのすべてのマルウェアの脅威を100%防止します。**

## ゼロトラスト:メールおよびWebセキュリティを再考する

多くのサイバーセキュリティの専門家が、欠陥を持つパラダイムをなんとか完全にしようとする日々を過ごす中、これまで考えられなかったことを実現するための最良の方法として登場したのが、ゼロトラストです:これは、100%安全なメールとWebへのアクセスを可能にします。メンロ・セキュリティでは、アイソレーションを活用したCloud Security Platformでゼロトラストを実現しています。このプラットフォームは、ブラウジングプロセスの処理をデスクトップからクラウドに移動して、インターネットとエンタープライズネットワークの間に効果的な「エアギャップ」を作成します。コンテンツから不要なものが排除され、クラウドブラウザからデスクトップ上のブラウザに安全にレンダリングされるため、ユーザーはデスクトップと同じエクスペリエンスを得ることができます。侵害や攻撃は、エンドポイントとユーザーから完全に切り離されます。



アイソレーションはセキュリティについてのまったく新しい考え方で、組織のネットワークをインターネットから分離してしまうため、攻撃者が業務環境に足場を築くことは決してありません。マルウェアは文字通りエンドポイントから遮断されるのです。すべてのメールおよびWebトラフィックは、コンテンツは表示されるがエンドポイントにはダウンロードされないこのアイソレーションレイヤーを通過します。その結果、メンロ・セキュリティのアイソレーションを活用したCloud Security Platformにより、企業はセキュリティの制御を維持し、すべてのユーザーに一貫したグローバルなポリシーを適用することができます。

## アイソレーションの進化

アイソレーション技術が最初に登場したのは約10年前で、サイバー攻撃に対して効果的であることが証明されましたが、インターネットのブラウジングが遅く使いにくかったため、ユーザーエクスペリエンスも台無しになりました。

しかし他の優れたアイデアと同様に、イノベーターはそれを改善し、最も要求の厳しい企業でも受け入れられるレベルに達しました。現代の従業員はクラウドベースのアプリケーションへの依存をますます高めており、メンロ・セキュリティはアイソレーションテクノロジーが快適でシームレスなブラウジング体験を提供できるよう長年取り組んできました。

**Isolation Core™ は、ネットワークとインターネットを分離し、攻撃者がお客様の環境に侵入できないようにするという、全く新しい考え方のセキュリティです。**

現在、Adaptive Clientless Rendering™ (ACR) と呼ばれるメンロ・セキュリティのコンテンツレンダリング技術は、デスクトップでのネイティブブラウジングと同じユーザーエクスペリエンスを提供できるまで完成されています。ユーザーが自分のコンピューターからローカルのブラウザーにコマンドを送信すると、アイソレーションを活用したCloud Security Platformがコマンドを受信し、クラウド上のリモートテナ内のブラウザーでそのサイトを開きます。次に、コンテンツはACRを介してローカルブラウザーに複製されます。そして、3つの異なるレンダリング方法を使用してユーザーエクスペリエンスを最適化します。

ユーザーは、自身のコンピューター上にアクティブなコンテンツをロードしなくてもWebサイトを利用できます。これは、Webサイト上の悪意のあるコンテンツがラップトップやその他のデバイスに感染することが無いことを意味します。さらに、フィッシングサイトでは警告が表示され、認証情報の入力やファイルのアップロードがブロックされます。その結果、従業員はサイバー攻撃を恐れることなく、メールを安全に開き、クラウドベースのアプリケーションを利用することができます。

## マルウェアを完全に取り除きます

メンロ・セキュリティの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はゼロトラストを可能にし、メールやWeb攻撃によるすべてのマルウェアの脅威を100%排除し、生産性を完全に保護します。これで、組織は安全なオンラインエクスペリエンスを提供できるようになり、ユーザーはビジネスを前進させながら心配することなく作業できるようになります。

メンロ・セキュリティは、あるグローバルな金融企業のマルウェア防止対策を6か月間で変革しました。このフォーチュン100企業は、世界で最も高度なセキュリティ運用を行っている企業のひとつであり、最も高度なサイバーセキュリティ製品のいくつかを備えています。彼らがサイバーセキュリティに何百万ドルも費やしていたにもかかわらず、フィッシング攻撃とマルウェア攻撃は、メンロセキュリティに移行するまで発生していました。

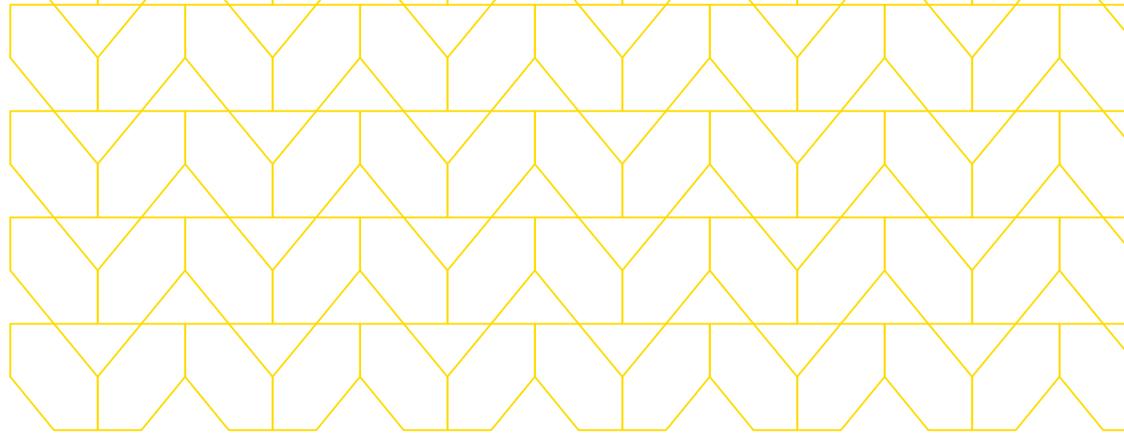
メンロ・セキュリティのアイソレーションを活用したクラウドプラットフォームは、以下に対して100%の保護を提供しました：

1,089

防御システムを回避したフィッシングマルウェアとマルウェアリンクがメンロ・セキュリティによって阻止されました

8,541

既存のセキュリティソリューションでは見逃されていた既知のマルウェアサイトが、メンロ・セキュリティによってブロックされました



メンロ・セキュリティのIsolation Core™には、メールやマルウェアの脅威からの保護の他にも多くのメリットがあります。たとえば、メールとWebの脅威が排除されるため、アラートが最大90%も減少することがあります。これによりただでさえ採用、トレーニング、確保が困難なサイバーセキュリティ担当者のリソースを節約することができます。ゼロデイ脅威も排除されますし、パッチが適用されていないシステムも安全に運用できるため、MicrosoftやGoogleが新しいパッチをリリースするたびに演習を行う必要はありません。

セキュリティへの取り組みを再考すべき時です。メンロ・セキュリティは、いかなる脅威も逃しません。メンロ独自のアイソレーションコア上に構築された拡張可能なセキュリティプラットフォームは、組織とその人々が心配することなく作業できるように、すべてのオンラインの脅威を排除することでクラウドセキュリティの約束を実現できる、唯一のソリューションです。



お問い合わせ:  
[www.menlosecurity.jp](http://www.menlosecurity.jp)  
[japan@menlosecurity.com](mailto: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。