

注目すべき特徴

- アイソレーション（分離）により安全な Web アクセス環境を提供 – リスクのあるコンテンツの検出に終始するのはもう不要です
- シームレスなエンドユーザーの操作性 – ユーザーの操作性を変えないで、デジタルデータを安心して業務に利用できます
- クラウドによるシンプルな構成と拡張性 – エンドポイントソフトや従来型のアプリケーションを使用しないため、セキュリティの複雑さがなくコストも抑えられます



Web コンテンツやドキュメントからマルウェアを排除

現代の IT 環境では、Web サイトにアクセスしたり、ドキュメントをダウンロードしたりするだけで、デバイスがマルウェアに感染する恐れがあります。定評あるニュース サイトや有名なエンターテイメント サイトなど、「安全」だと思われている Web サイトにさえ、マルウェアが潜んでいる可能性があります。

従来の脅威防御製品は、「安全なコンテンツ」と「危険なコンテンツ」の検査を試み、安全なコンテンツを許可し、危険なコンテンツをブロックするポリシーを作成しなければなりません。そのため、マルウェアを作成する攻撃者には悪意のアクティビティを検知され、ブロックされるポリシーが作成されるまでには十分な時間がありましたので、このような手法による脅威防御は成功しませんでした。

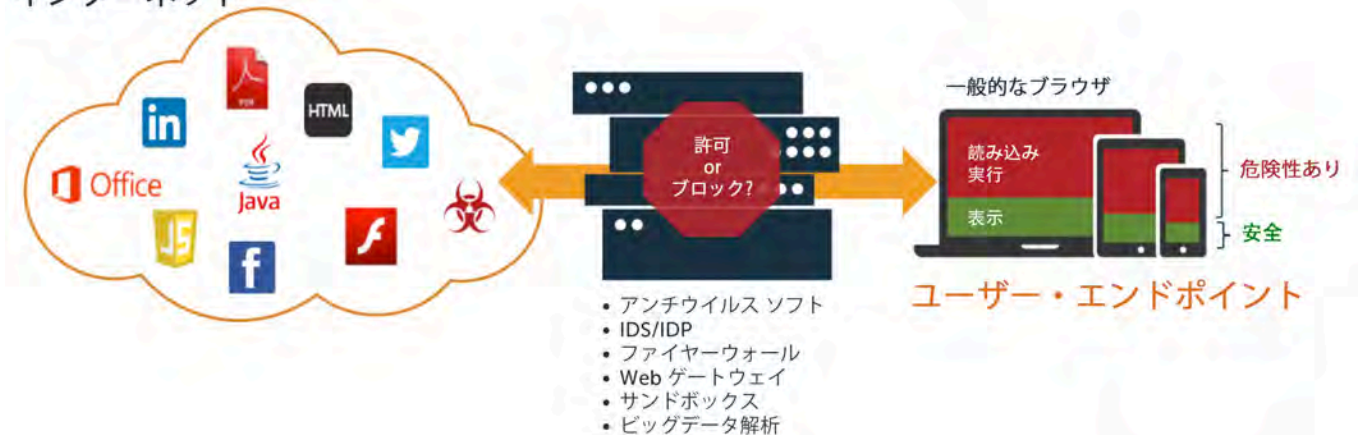
今や、新たなソリューションが求められています。

新たなソリューション: アイソレーション（分離）

アイソレーション（分離）テクノロジーを基盤とする新たなセキュリティモデルでは、正当なコンテンツとマルウェアを区別せずに、ユーザーと潜在的な攻撃元との間に、安全で信頼できる実行環境（アイソレーション（分離）プラットフォーム）を提供します。そしてエンドポイントから離れた場所でユーザー セッションを実行し、安全なレンダリング情報のみをユーザーのデバイスに提供することで、マルウェアや悪意のあるアクティビティからユーザーを保護します。

従来の脅威防御モデル

インターネット



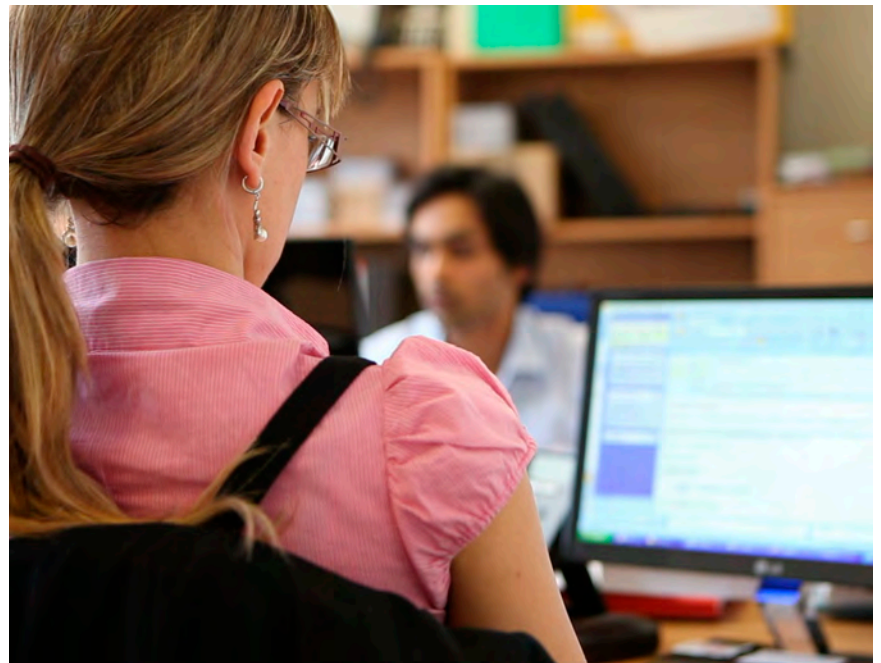
エンタープライズ クラスのアイソレーション (分離) プラットフォームの特性

最先端のエンタープライズ クラスのアイソレーション (分離) ソリューションとは、次のような特性を備えたものです。

- 悪意のある Web コンテンツやドキュメント、フィッシングによる攻撃を防止
- アプライアンスやエンドポイント ソフトが不要で、導入が迅速かつ容易
- 元の操作性が維持され、ユーザーが認識できるような遅延がない
- 主要なデバイス、OS、ブラウザに対応 (カスタム ブラウザは不要)
- パブリック クラウド サービスとしても、仮想アプライアンス経由でも利用可能
- 既存のセキュリティ システムと統合 (Web セキュリティ ゲートウェイなど)
- ポリシーに例外を設定する面倒な管理作業を排除
- 誤検知によって危険なサイトを見逃したり、安全なサイトをブロックしたりすることは皆無
- プライバシー・ポリシー設定機能、広範囲の可視化、フォレンジック機能の提供

Menlo Security Isolation Platform (MSIP)

Menlo Security は、ユーザーの操作性を損なわず、IT スタッフに大きな負担をかけないようなアイソレーション (分離) セキュリティを提供することで、さまざまな企業のお客様に貢献しています。MSIP は、仮想化テクノロジーと Adaptive Clientless Rendering (ACR) テクノロジー (特許取得済み) を活用しています。エンドポイントの導入や管理をしなくても企業全体にわたってアイソレーション (分離) セキュリティを導入でき、インターネットを幅広く利用しながら、リスクを大幅に抑えることができます。



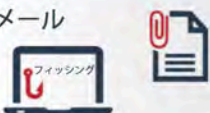
ウェブ



ドキュメント



Eメール



ユーザー・エンドポイント

Adaptive Clientless Rendering™ (ACR)

表示



- ユーザー操作性変更なし
- 機器、OS、ブラウザの制限なし
- エンドポイントへのエージェントなし
- SaaS での利用 (アプライアンス必要なし)
- 高可用性、高スケーラビリティ

セッション終了時に破棄される

主な機能とメリット

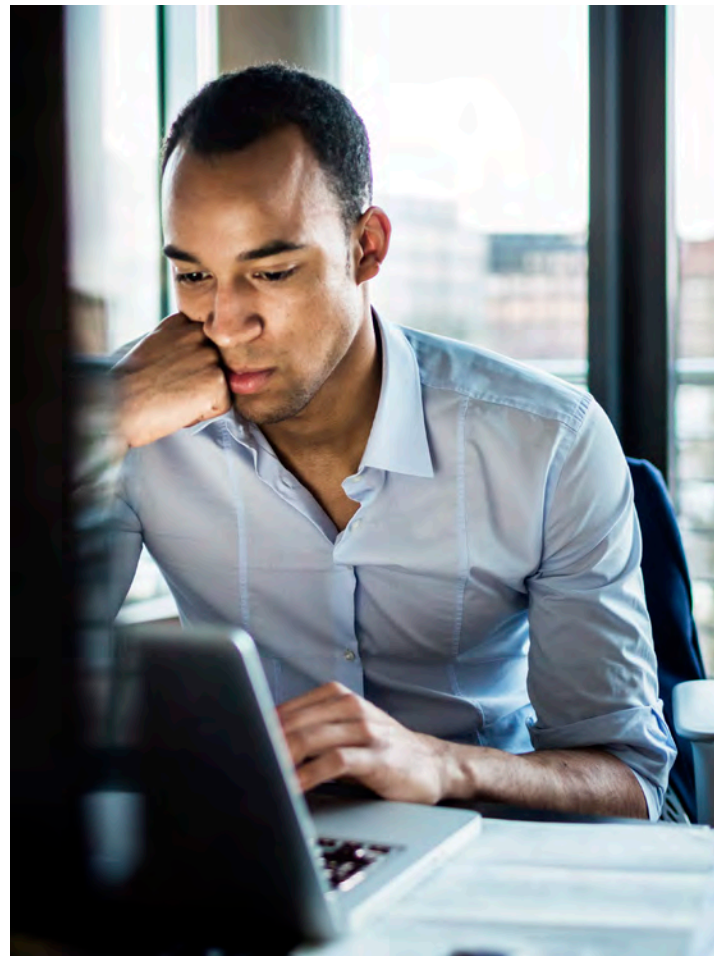
アイソレーション（分離）により安全な Web アクセス環境を提供

- **アイソレーション（分離）によってマルウェアを排除** – ユーザーセッションは MSIP 内のディスポーザブル ヴァーチャル コンテナ（DVC）で実行されます。プラットフォームは、ユーザーがセッションを完了するたびに、マルウェアを含むすべてのコンテンツをコンテナごと破棄します。脆弱性をつく攻撃がプラットフォームをすり抜けてユーザーのエンドポイントに到達する恐れは一切ありません。そのため、誤検知によって正当なコンテンツをブロックして警告を発したり、見逃したマルウェアがターゲットに到達したりすることはなくなります。
- **ドキュメントから脅威を排除** – MSIP は、ドキュメント（PDF および Microsoft Office 形式（Word、Excel、PowerPoint））をプラットフォーム内に分離することで、ドキュメントに潜むリスクを排除できます。アクティブ コンテンツを削除してレンダリング（表示）したドキュメントを「安全な」PDF ファイルとしてダウンロードできます。また、指定ユーザーが元のドキュメントをダウンロードできるように設定することも可能です。
- **エンドポイントを Flash から保護** – Flash など潜在的に有害なコンテンツはプラットフォーム内で実行されるため、感染する恐れのあるアクティブ コンテンツをエンドポイントに配信することなく、オリジナルに忠実なユーザー エクスペリエンスを実現します。管理者は、ユーザーのブラウザから Flash を削除しながら、マルウェアのリスクのない Flash コンテンツへのアクセスを許可できます。

シームレスなエンドユーザーの操作性

- **ユーザーの操作性を保持** – Adaptive Clientless Rendering™（ACR）テクノロジーにより、Web サイトに直接アクセスした場合とほぼ区別の付かない操作性をユーザーに提供します。ユーザーが認識できるような遅延は発生せず、カット & ペーストや印刷などのブラウザ機能への影響もありません。画面がコマ送り表示される、スクロールがギクシャクするなど、VDI のような「表示データを抽出する」テクノロジーにありがちな視覚的問題は発生しません。ACR では、コンテンツ タイプごとに最適なエンコーディング メカニズムを活用し、あらゆる端末やブラウザ、OS に対応する業界標準のレンダリング要素を使用して、コンテンツを安全にユーザーの端末に提供します。

- **利用頻度の高いドキュメント タイプをサポート** – ドキュメント アイソレーション サービスでは、PDF および Microsoft Office 形式（Word、Excel、PowerPoint）など、業務に欠かせない利用頻度の高いドキュメント タイプのほとんどをサポートしています。
- **Web サイトの再分類リクエスト数を削減** – デジタル データを利用する今日のビジネスは、Web コンテンツとアプリケーションに大きく依存しています。マルウェアのリスクを抑えようとして IT 部門が Web アクセスを制限すると、ビジネスに欠かせない正当なサイトが悪意のあるサイトとして分類され、社員が利用できなくなる場合があります。その結果、社員がヘルプ デスクに分類のやり直しを求め、それを処理するためのコストが増加します。MSIP なら、社員は業務に必要なあらゆる Web アプリやコンテンツに自由にアクセスできるので、サイトを再分類する必要がありません。



メンローセキュリティについて

Menlo Security は、アイソレーション（分離）技術によってユーザー PC の安全を確保し、Web や E メールによるマルウェアの脅威を取り除くことで、組織をサイバー攻撃から守っています。Menlo Security Isolation Platform (MSIP) は、アクティブコンテンツをすべてクラウド内に分離し、セキュリティを損なうことなく、Web サイトやリンク、オンラインドキュメントなどをユーザーが安全に操作できるようにするプラットフォームです。

Menlo Security は、Fortune 500 企業や金融サービス機関をはじめ、世界のさまざまな大企業からの信頼を集めています。カリフォルニア大学バークレー校の著名な研究者の協力のもと、セキュリティ業界のベテランたちが Menlo Security を創業しました。Menlo Security は、General Catalyst、Sutter Hill Ventures、Osage University Partners の支援を受け、カリフォルニア州メンローパーク市に本社を構えています。

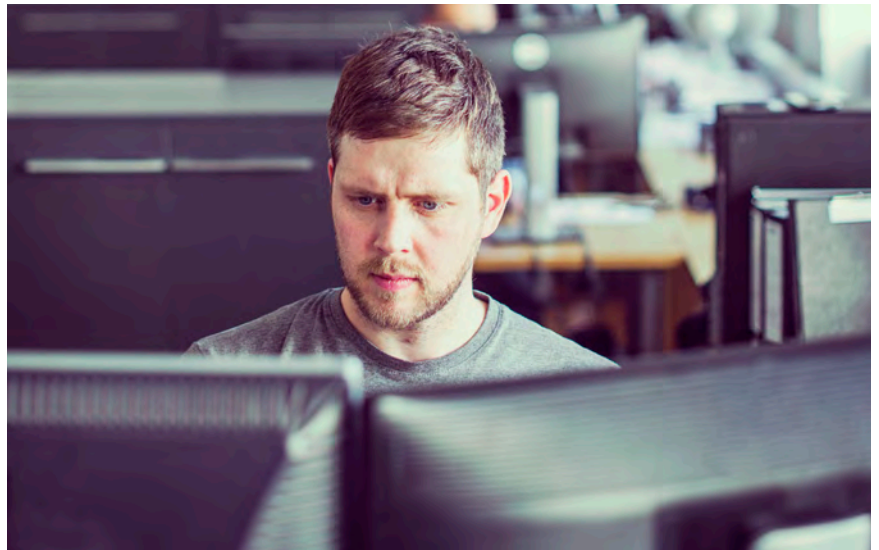


ホームページ：
www.menlosecurity.com

お問い合わせ：
japan@menlosecurity.com

クラウドによるシンプルな構成と拡張性

- **導入が迅速かつ簡単（アプライアンスやエンドポイント ソフトは不要）** – MSIP はクラウドベースのソリューションで、エンドポイント ソフトや旧式のアプライアンスを使用しないため、セキュリティの複雑さがなくコストも抑えられます。導入は数分で完了し、インシデント対応に追われることも、許可やブロックの判別を誤ることもなく、簡単に運用できるようになります。また、クラウドベースなので、小規模企業からグローバル エンタープライズまで、ニーズに合わせて拡張できます。



- **既存のセキュリティ システム（Web セキュリティ ゲートウェイなど）やメール システム、シングル サインオンと統合** – ユーザーのブラウザにプロキシの自動構成（PAC）を設定し、Microsoft Active Directory (AD) や他の端末管理システムを通じて自動的にプロビジョニングすることで、ユーザーのトラフィックを MSIP 経由で転送できます。または、既存の Web プロキシ システムとの統合機能を利用してトラフィックをルーティングすることもできます。MSIP は AD との統合によってシングル サインオンを実現します。また、SAML をサポートしているので、Centrify、Okta、OneLogin、PingIdentity など、よく利用されるクラウド ID プロバイダと統合できます。
- **強力なフォレンジック機能とレポート作成機能を搭載** – 管理者は、ログデータやレポートを MSIP 管理ポータルから直接参照できるだけでなく、自社の SIEM や運用管理システムにデータをエクスポートできます。このポータルには、ユーザー別や Web カテゴリ別のアクティビティ、既知の脆弱性を備えたサイトへのブラウジング、回避した脅威など、さまざまなレポートを作成できる機能が豊富に用意されています。