モバイルデバイスからのセキュアなクラウドアプリケーションの利用

MobileIron と A10 の連携によるセキュアな Office 365/G Suite 利用環境の実現

課題：

社内外でノート PC やタブレット、スマートフォンなどのモバイルデバイスから、Office 365 や G Suite などのクラウドアプリケーションを利用する際のセキュリティの確保

解決策：

- MobileIron の提供する統合エンドポイント管理（UEM）とセキュアゲートウェイ（SENTRY）により、許可されたデバイスからのみ企業内の社内リソースとクラウドアプリケーションを利用可能とし、不正なデバイスからの利用を阻止
- モバイルデバイスからの通信に対して A10 Thunder® CFW を用いた SSL/TLS 通信の可視化とヘッダ挿入機能を用いることで Office 365 や G Suite などクラウドアプリケーションのログインアカウントの利用制限を行い、企業で利用が許可されてない個人アカウントなどからのログインを制限

メリット：

- 不正なデバイスからの社内リソースやクラウドアプリケーションへのアクセスのブロック
- SSL/TLS 通信可視化とヘッダ挿入により、利用が許可されていないアカウントでの Office 365 や G Suite などの利用をブロック
- SSL/TLS 通信可視化のために必要な証明書を、容易に多様なモバイルデバイスへ配布することが可能
- Office 365 や G Suite などにより既存のプロキシサーバーやファイアウォールにかかる通信負荷のオフロードや、SSL/TLS 通信可視化を用いたセキュリティ強化が可能

モバイルデバイスでクラウドアプリケーションを利用する際のセキュリティリスク

社内外で利用するノート PC やタブレット、スマートフォンから Office 365 や G Suite などのクラウドアプリケーションを利用することで、いつでもどこでもオフィスワークを行うことができ、生産性を大幅に向上できます。その一方で、多様なデバイスでクラウドアプリケーションを利用することで、機密情報の漏洩などのセキュリティリスクが懸念されます。

どこからでもサービスを利用でき、いつでも保存されたデータにアクセスできることがクラウドサービスの利点ですが、一方で、企業が許可していない PC やモバイルデバイスからクラウドサービスにログインされてしまったり、クラウド内のデータを持ち出されて企業情報が漏洩してしまったりといったリスクがあります。

これらのセキュリティリスクに加え、企業内からクラウドアプリケーションにアクセスすることで大量の通信セッションが生じ、既存のプロキシサーバーやファイアウォールなどの通信負荷が高まるリスクもあります。これにより、クラウドアプリケーションが快適に利用できなくなります。

モバイルデバイスからセキュアにアプリケーションを利用

MobileIron の提供する統合エンドポイント管理（UEM）と、企業内に配置するセキュアゲートウェイ（SENTRY）により、許可されたモバイルデバイスからのみクラウドアプリケーションにログインさせることができるようになります。MobileIron UEM は単なるデバイス管理にとどまらず、デバイスの通信を制御することができ、デバイスからの通信を SENTRY に集約し、許可されたデバイスのみが企業の認証基盤にアクセスできるようにします。iOS や Android だけでなく Windows 10 や macOS など、企業で利用されている多様なデバイスを一元管理できます。MobileIron SENTRY はエンドポイントとバックエンドの企業システムの間で、トラフィックの暗号化と制御、セキュリティ保護を行うインラインのゲートウェイです。多様なモバイルデバイスに企業内システムへのセキュアなアクセスを提供します。

また、A10 ネットワークスの提供する Thunder CFW をプロキシサーバーとして利用すると、企業が許可していない個人アカウントなどの利用制限が可能になります。A10 Thunder CFW が SSL/TLS 通信可視化機能を用いて HTTPS 通信を一旦復号し、アカウント識別情報を含むヘッダを挿入して再暗号化した通信をクラウドアプリケーションに送信することで、許可されていないアカウントでのログインを拒否します。

上記の MobileIron UEM と SENTRY、A10 Thunder CFW を併せて利用することで、モバイルデバイスからのセキュアなクラウドアプリケーション利用を実現できます。この構成を図 1 に示します。

この連携ソリューションでは、MobileIron UEM で管理されているデバイスがクラウドアプリケーションを利用する際に、企業ネットワークに配置された MobileIron SENTRY と接続します。許可されていないデバイスは接続できません。A10 Thunder CFW は MobileIron SENTRY の後段に設置され、Office 365 などのクラウドアプリケーションに向かうトラフィックの HTTPS 通信を復号してアカウント識別情報を付加し、再暗号化してクラウドアプリケーションに送信します。クラウドアプリケーションはアカウント識別情報に基づき許可されていないアカウントでのログインを拒否します。これにより、不正なデバイスの企業内への接続を防ぐと共に、不正アカウントでのクラウドアプリケーションの利用とそれに伴う情報漏洩を防ぐことができます。

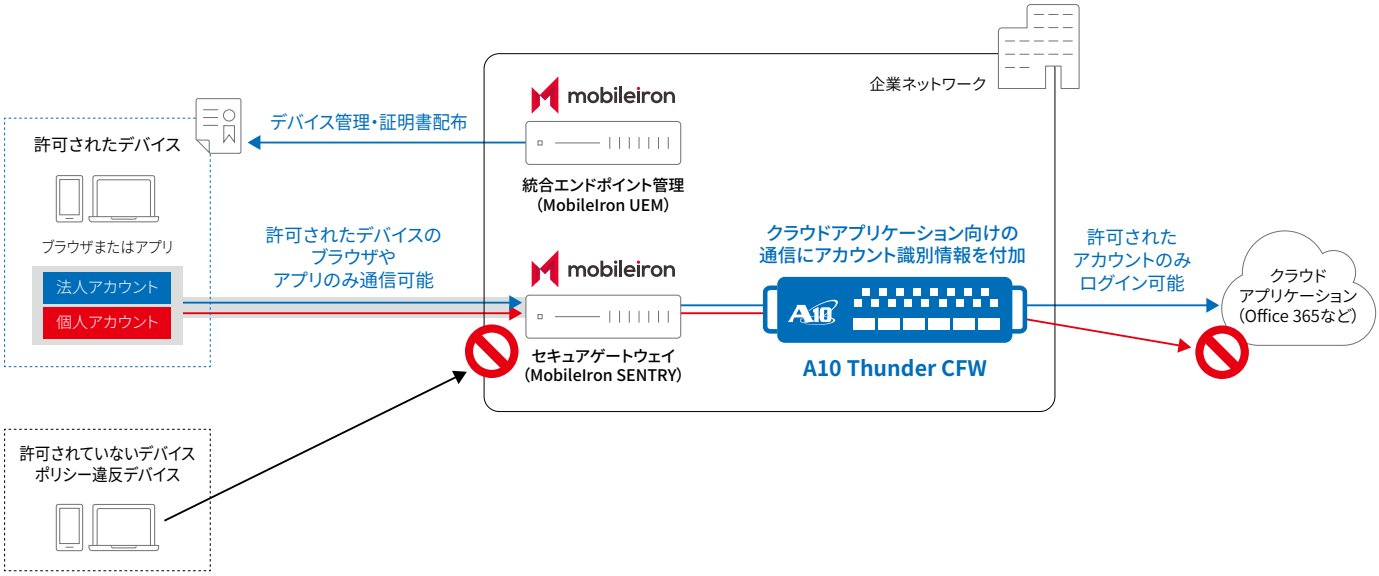

図1：MobileIronとA10によるセキュアなクラウドアプリケーション利用の実現

A10 Thunder CFWでSSL/TLS通信可視化に必要な証明書についても、MobileIron UEMを通じて一元的に各デバイスに自動で配布しインストールすることが可能です。SSL/TLS通信可視化を用いたアカウント制御は、Office 365やG Suiteの他、BoxやLINE WORKSなどのクラウドアプリケーションでも利用することができます。

通信負荷のオフロードとセキュリティの強化

A10 Thunder CFWを導入することで、クラウドアプリケーションへのログインアカウントを制御するだけでなく、クラウドアプリケーション利用で生じる通信機器への負荷の軽減や、SSL/TLS通信に対するセキュリティ強化も実現できます。

Office 365などのクラウドアプリケーションを利用すると、各クライアントが膨大な通信セッションを利用することから、既存のプロキシサーバーやファイアウォールに大きな通信負荷がかかります。膨大な通信セッションを処理できる独自のアーキテクチャを持つA10 Thunder CFWを用いることで、ドメイン名に基づいてクラウドアプリケーション向けのトラフィックを振り分け、プロキシサーバーやファイアウォールをバイパスすることができ、快適なクラウドアプリケーションの利用を実現できます。

また、SSL/TLS可視化を用いることにより、A10 Thunder CFWが復号した通信を既存のセキュリティ機器（ファイアウォール、サンドボックス、UTM、IPS/IDS、URLフィルターなど）で検査することができます。HTTPS通信をはじめとするSSL/TLS通信を検査できなかった機器での検査や、A10 Thunder CFWの高速なSSL/TLS通信処理能力により高いパフォーマンスでの検査が可能になり、SSL/TLSに隠れた脅威を防御できます。

MobileIronについて

MobileIronは、モバイルデバイスやクラウドサービスの普及で変容するゼロ・トラスト環境に最適な、モバイルを中心に据えた企業セキュリティを提供しています。2007年の創立以来、世界で19,000社以上のお客さまに採用され、80件以上の特許を取得し、主要な市場アナリストから統合エンドポイント分野でのリーダとの評価を得ています。

https://www.mobileiron.com/ja

A10 Networks / A10 ネットワークス株式会社について

A10 Networks（NYSE: ATEN）はセキュアアプリケーションサービスにおけるリーディングカンパニーとして、高性能なアプリケーションネットワーキングソリューション群を提供しています。お客様のデータセンターにおいて、アプリケーションとネットワークを高速化し可用性と安全性を確保しています。A10Networksは2004年に設立されました。米国カリフォルニア州サンノゼに本拠地を置き、世界各国の拠点からお客様をサポートしています。

A10ネットワークス株式会社はA10 Networksの日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワーキングソリューションを提供することを使命としています。

詳しくはホームページをご覧ください。
www.a10networks.co.jp
Facebook：http://www.facebook.com/A10networksjapan

A10ネットワークス株式会社
www.a10networks.co.jp
a10networks.co.jp/contact

お問い合わせ：

Part Number: SB_MobileIron_and_A10 Nov 2019