IceWall技術レポート:

モバイルアクセスの認証強化
– VMware AirWatchとIceWall SSOとの連携

1. はじめに　～働き方改革とモバイルアクセス～

ダイバーシティマネジメントへの取り組みや、生産性向上、優秀な人材確保のため「働き方改革」に取り組む企業が増えています。そのため社員の働く場所や環境、時間などで多様化が進み、自宅やリモートオフィスなど社外からスマートフォンやタブレット端末を使って社内システムを利用する「モバイルアクセス」が急速に進んでいます。

社外からのアクセスでは、特にセキュリティの担保が重要です。モバイルアクセスでは通常のパスワードなどによるユーザー認証に加えて、特定のデバイスからのアクセスのみを許可する「デバイス認証」の仕組みが求められています。デバイス認証によって、例えば会社から支給されるデバイスや会社から承認を受けたBYOD(Bring Your Own Device)からのアクセスのみを許可し、社外からのなりすましによる不正アクセスを防止します。

本技術レポートでは、代表的なモビリティ管理製品の「VMware AirWatch」と「IceWall SSO」との連携ソリューションをご紹介します。VMware AirWatchによるデバイス認証と、IceWall SSOによるシングルサインオンを組み合わせることで、モバイルアクセスのセキュリティと利便性の双方を向上させることができます。

2. モビリティ管理製品VMware AirWatchについて

AirWatchはVMwareのエンタープライズモビリティ管理製品です。会社の業務専用のワークスペースをモバイルデバイス内に構成し、個人利用のアプリケーションやメール等から切り離すことで、BYOD環境においても高いセキュリティを保った状態で業務アプリケーションやデーターを利用することができます。

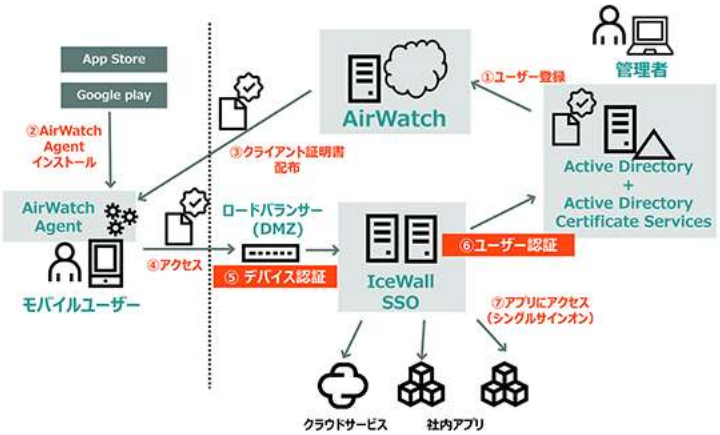
AirWatchにはモバイルデバイスマネジメント(MDM)、モバイルアプリケーションマネジメント(MAM)、モバイルコンテンツマネジメント(MCM)、モバイルEmailマネジメント(MEM)の4つの主要機能があり、それぞれモバイル環境に求められる、デバイス管理、アプリケーション管理、コンテンツ共有、企業メール送受信等の機能を提供しています。

vmware®
airwatch®

3. 連携ソリューション概要

今回の連携ソリューションでは、AirWatchのデバイス管理機能(MDM)で提供されるクライアント証明書配布を利用し、IceWall SSOの前段でデバイス認証を行います。

連携ソリューションの概要を以下の図に示します。



AirWatch / IceWall SSO 連携ソリューション

1. 管理者がモバイルデバイスのユーザーをActive DirectoryからAirWatchに登録し、ユーザーにEメールを送付します。
2. ユーザーがストアからAirWatch Agentをモバイルデバイスにインストールします。

3. ユーザーが管理者から送付されたEメールに従ってAirWatchにアクセスすると、AirWatch AgentがVMware Browserとクライアント証明書をモバイルデバイスにインストールします。
4. ユーザーがVMware Browserで社内システムにアクセスします。
5. ロードバランサーが、登録されたデバイスからのアクセスかどうかクライアント証明書で認証を行います。
6. IceWall SSOがActive Directoryへアクセスし、ユーザー認証を行います。
7. ユーザー認証が完了すると、社内アプリケーションや社外のクラウドサービスへシングルサインオンでアクセスが可能になります。

4. 検証

実際にAirWatchを使用してモバイルデバイスにクライアント証明書を配布し、IceWall SSOとの連携ができることを確認しました。

AirWatchの設定は以下の手順で行いました。

1)「エンタープライズ統合」から、ディレクトリ サービスとMicrosoft 証明書サービスを有効化したクラウドコネクタをダウンロードし、ディレクトリサービスに使用するActive Directoryを指定。

2)「エンタープライズ統合」から「認証局」にて、使用するActive Directory Certificate Servicesを指定し、証明書の要求テンプレートを構成。

3)「セキュリティポリシー」から、統合認証を「有効」に設定し、「証明書を使用」を選択して、上記で構成した認証局及び証明書の要求テンプレートを指定し、VMware Browser アプリを配信アプリのリストに追加。

IceWall SSOでは以下のように設定しました。

1) 認証DBとして使用するActive Directoryを設定。
2) IceWallサーバーを社外からアクセスできるDMZに配置し、前段のロードバランサーでクライアント証明書による認証を行うように設定。

各設定が完了後、モバイルデバイスからアクセスを行い、AirWatchによって配布されたクライアント証明書によるデバイス認証と、IceWall SSOによるユーザー認証が行われ、社内アプリケーションへシングルサインオンによって正常にアクセスできることを確認しました。

5. まとめ

この連携ソリューションによって、強固なセキュリティと高い利便性を確保しながら、モバイルデバイスの利用をより促進させることが可能です。

2017/5/16　新規掲載

執筆者　株式会社　ネットワールド
SI技術本部　統合基盤技術部　プラットフォームソリューション課
服部 卓

日本ヒューレット・パッカード株式会社
テクノロジーコンサルティング事業統括　IceWallソフトウェア本部
情報セキュリティスペシャリスト　並木 岳夫