EMMを活用したセキュアなモバイルワークソリューション

及川 剛　吉田 かずみ

要 旨

「働き方改革」の推進にあたり、いつでもどこでもさまざまなデバイスでフレキシブルに働けるICT環境の提供が求められていますが、サイバー攻撃からのリスクは増えるため、その対策が不可欠となります。スマートデバイスを使って安全・安心なモバイルワークを実現するEMM（Enterprise Mobility Management）ソリューションについて、NECの社内導入事例も交え紹介します。

KeyWords

モバイルセキュリティ／モバイルワーク／働き方改革／EMM／MDM／暗号化

1. はじめに

昨今、一億総活躍社会の実現に向け、日本政府が進めている「働き方改革」。多くの企業がこの働き方改革に向けた取り組みを開始しており、そのなかでもモバイルデバイスやクラウドサービスを活用した「モバイルワーク」は多くの注目を集めています。

モバイルワークを導入することで、企業は従業員に対し多様なワークスタイルを提供できます。例えば、どこからでも仕事ができるようになることで、育児や介護などで安定した勤務時間が取れない従業員や、外出先からも社内リソースにアクセスしたい営業担当者などの働き方の幅を広げることができます。

しかし、モバイルワークの導入は従業員の利便性向上と引き換えに、ウイルス感染やデバイス盗難・紛失などに起因する、セキュリティ面でのリスクが懸念されており、多くの企業の情報システム担当者の頭を悩ませる課題となっています。

本稿で紹介する「ActSecureモバイル基盤サービス Powered by VMware AirWatch」（以下、モバイル基盤サービス）は、利便性とセキュリティを兼ね備え、モバイルワークに不可欠となる多様なデバイスやアプリケーションを包括的に管理することができるサービスです。

2. サービスの概要

モバイル基盤サービスは、デバイスの状態やシステム設定などを管理するモバイルデバイス管理（MDM：Mobile Device Management）、デバイス内で利用するアプリケーションを管理するモバイルアプリケーション管理（MAM：Mobile Application Management）、そして、ローカルデータやコンテンツなどを保護するモバイルコンテンツ管理（MCM：Mobile Contents Management）の機能を統合した、EMM（Enterprise Mobility Management）のサービスです。

対応OSも幅広く（Android、iOS、Windows、MacOS、BlackBerryなど）、管理者は多様なデバイスを統一のプラットフォームで一括管理することができます。

一方、利用者は専用のアプリケーションを利用することで、オフィスで利用している電子メールやアドレス帳、スケジュールなどに安全にアクセスすることができるため、業務効率を上げることができます。

第5章にて後述しますが、NEC社内においても、働き方改革のためのデバイス管理基盤として本サービスの機能

図1　NEC社内向けにリリースされた機能概要

を利用することが決定し、2017年6月19日にリリースされています（**図1**）。

市場におけるEMMの需要は年々高まっており、今後も成長が見込まれるなか、NECとして外販を行う本サービスについて、次章以降でその詳細と特長を説明します。

3. サービスの特長

本章では、サービスの特長について以下で説明します。

(1)豊富な対応デバイス

業務において個人のデバイスを利用するBYOD（Bring Your Own Device）の普及により、企業で業務利用されるデバイスの種類は膨大な数となっています。これにより、企業管理者はデバイスの種別に応じて管理方法を変えなければならず、大きく工数を奪われるとともに、デバイスごとにセキュリティのレベルが疎らになってしまう傾向があります。

モバイル基盤サービスは数多くのデバイス、OSに対応しており、BYODを含む多数のデバイスについて統一の基盤上で、セキュリティレベルを合わせて管理することができます。OSのバージョンアップ時にも、基本的にはリリース日に即日対応となるため、管理から外れることはありません。

(2)オフライン環境でのセキュアなモバイル活用

モバイル基盤サービスが提供する専用アプリケーションを利用する際、基本的にメールやファイルなどのデータはモバイルデバイスのローカル記憶領域（以下、ローカル）に保存されます。これにより、ユーザーは電波の弱い環境や飛行機などでの移動の際にも、データにアクセスすることができるようになります。

一方で、システム管理者としては情報漏えいのリスクを高める危険性を鑑み、モバイルデバイスのローカルにデータを残すことを良しとしない傾向がありますが、モバイル基盤サービスで提供される専用アプリケーションはすべてFIPS140-2に準拠しており、ローカルに保存されるデータは、AES256bit暗号化方式によって保護されるため、安全性の高い仕組みとなっています。

また、各専用アプリケーションを利用する際のパスコード入力を義務化することができ、暗号化されたデータは、専用アプリケーション以外のアプリケーションから閲覧することができないため、万一データが漏えいしてしまった際も安全です（**図2**）。

(3)汎用的に設定可能なデバイス運用ポリシー

モバイルワークにより、いつでもどこでも業務遂行可能な環境が提供されることで、従業員（担当者）が業務時間外にも仕事をしてしまい、過労につながってしまうという問題があります。

第4章で後述しますが、モバイル基盤サービスは時間や位置情報を条件として、特定の機能やアプリケーションに対し制限を掛けることができます。これにより、前述の問題を解決することができます。

図2　コンテンツ閲覧時のポイントについて

また、もう1つのモバイルワークの問題として、従業員がモバイルデバイスを自由に使うことで脆弱性が生まれ、セキュリティ事故につながってしまう、というものがあります。

これについても、モバイル基盤サービスであれば、デバイスが準拠すべきポリシーについてあらかじめ詳細に設定することができるため安心です。例えば、デバイスロックのためのパスワードは必須、かつ、8文字以上での設定を義務化したり、ユーザー権限の制限を取り除いて開発者の意図しない方法でソフトウェアなどを動作させるAndroidOSのroot化やiOSのJailbreakを禁止するなど、細かく設定することができます。

4. サービス内容

以上、前章でサービスの特長について紹介しましたが、本章ではモバイル基盤サービスが提供する機能の詳細について、以下で説明します。

(1) モバイルデバイス管理機能（MDM）

MDMの機能としては、一般的なデバイス紛失時のリモートワイプ、リモートロックに加え、時間や位置情報によって利用できる機能を制限するなど、ポリシーに合わせてデバイス側の動作を細かく設定することができます。例えば、特定の敷地内での写真撮影（カメラ機能）の禁止や、業務時間外のメールを禁止することができます。

また、モバイル基盤サービスにはSelf Service Portal（以下、SSP）という、ユーザー自身がリモートワイプ、リモートロックを実施できるポータルサイトが存在します。

これにより、ユーザーがモバイルデバイスを紛失した際の管理者の工数を下げつつ、対応が遅れがちなデバイスのデータ消去対応までの時間を短縮し、情報漏えいのリスクを下げることができます。

(2) モバイルアプリケーション管理機能（MAM）

次にMAMの機能としては、App Catalogという専用のユーザー向けアプリケーションを利用することで、管理者は業務に必要なアプリケーションや自社内で開発した業務アプリケーションを統一の基盤上に掲載し、インストール状況やバージョン情報など、詳細に管理することができます。また、社有のデバイスであれば、端末機種によってはアプリケーションを自動でインストールさせることもできるため、ユーザーの工数を短縮させることも可能です。

情報漏えい対策としては、インストール禁止アプリケーションの指定や、業務アプリケーションと個人利用アプリケーション間でのデータの受け渡し制限を掛けることができ、セキュリティの向上につながります。

(3) モバイルコンテンツ管理機能（MCM）

MCMの機能としては、専用のアプリケーションを利用することで社内ファイルサーバ上に格納されているファイルの閲覧や、イントラネット上のサイトを閲覧できます。前者は、Content Lockerという専用のビューアアプリケーションを利用することで、前述の暗号化方式によってオフラインでもセキュアにローカルのファイル閲覧が可能となるもので、後者はVMware BrowserというWebブラウジングアプリケーションを利用して、イントラネット上のサイトへの安全な通信を実現します。

モバイルデバイスにデータを残さないことで、セキュリティを向上させるという考え方もある一方、モバイル基盤サービスではデータを残して暗号化でセキュリティを担保することにより、オフラインでの利用を可能とするなど、利便性を高めています。

5. NEC社内導入について

第2章で記載したとおり、2017年6月19日よりNEC社内においても、本サービスの機能が展開・利用されています。本サービス導入のポイントは以下のとおりです。

(1)導入のきっかけ

近年、NEC社内において海外出張時など、ネットワーク環境が不安定な場所でのスマートデバイス活用ニーズが高まっていること、また、グローバルを含めたグループ会社で共通の基盤として展開したいことから、オフラインでも利便性を高めることができ、グローバルに利用可能な本サービスの導入を決定しました。

(2)利用範囲・端末

NECグループ会社含め、全社員が利用可能です。端末としては、社有、BYODでの利用をサポート対象としています。特にBYODは、社有レベルのセキュリティを徹底しつつ、プライバシー情報の収集はしないなどの工夫をし、展開しています。

(3)適用されるNEC社内ポリシー

デバイスパスワードの設定やストレージ暗号化の強制などのセキュリティポリシーに加え、オフィス内無線LAN用プロファイルを自動配布し、オフィスに入ると社内無線LANに自動で切り替わるポリシーを適用し、利便性の向上も図っています。

NECの周囲からも「オフラインでの利用ができることで効率が上がった」「操作性が高く、非常に使いやすい」「BYOD利用で1台持ち歩くだけで良いのが嬉しい」など、ユーザーからの声が聞こえてきており、本サービスが利便性の向上に貢献していることを実感しています。

今後、旧サービスの2万ユーザーに加え、グローバルに導入を進めることで、3万ユーザーまで規模を拡大していく予定です。

6. 今後について

(1)他プロダクトとの連携

本サービスを利用することで、モバイルデバイスをセキュアに利用可能とここまで紹介しましたが、今後は「現在モバイルデバイスにおけるセキュリティがネックとなり、利用シーンが限られている」などの課題をお持ちのお客様に対し、モバイル基盤サービスと連携することで提供価値を広げることができるプロダクトやソリューションと連携することで、より多くの課題を解決できるよう取り組んでいきたいと考えています。

(2)NECをリファレンスとしたモデル展開

本サービスは提供できる機能が多く、お客様によっては、自社においてどこまで機能を利用すべきか、またどの範囲までポリシーとして展開するか、という点で迷われることが予想されます。その際、NEC社内での展開をリファレンスモデルとして提供できるよう、導入コンサルを含めたサービスを検討しています。

(3)海外向けサービスリリース

現在、本サービスは日本国内でのみ提供可能となっていますが、今後海外での販売も予定しています。

実際、NEC社内としてもグローバル含め、統一のデバイス管理基盤として利用していく予定ですが、「海外のお客様に対して提供したい」というニーズにもいち早くお応えできるよう、準備を進めてまいります。

7. おわりに

企業において、モバイルデバイスはもはや欠かせないツールの1つとなっています。更に、BYODでのデバイス利用も広がってきているなか、業務に関係するさまざまなデバイスを管理することは、企業の情報セキュリティを守るための必要事項となってきています。

本稿にて紹介したモバイル基盤サービスは、利用者が利便性を損なうことなく、管理者がデバイスを細かく柔軟に管理することができるため、NECとしてこれからのモバイルワークの基盤として位置付け、社内利用のリファレンス活用、他プロダクト、サービスとの組み合わせを通して、さまざまなお客様ニーズに応えていきます。

執筆者プロフィール

及川 剛
スマートネットワーク事業部

吉田 かずみ
スマートネットワーク事業部
マネージャー

関連URL

ActSecure モバイル基盤サービス Powered by VMware AirWatch
http://jpn.nec.com/act/acts_airwatch.html

NEC 技報のご案内

NEC 技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報（日本語）　NEC Technical Journal（英語）

Vol.70 No.2　ビジネスの安全・安心を支えるサイバーセキュリティ特集
～Futureproof Security　安心の先へ。～

ビジネスの安全・安心を支えるサイバーセキュリティ特集によせて
増大するサイバー犯罪の根源的な解決へ～“産学官”のオールジャパンで立ち向かう第三者機関の姿とは？～
サイバーセキュリティを取り巻く社会動向とNECの取り組み

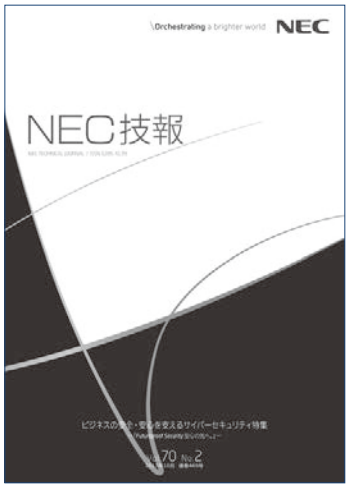
◇ 特集論文

社会の動向とNECの取り組み
重要インフラに対するサイバー攻撃の実態と分析
2017 サイバー攻撃最新動向 NEC Cyber Threat Intelligence活用モデル
サイバーセキュリティ対策の社内事例

サイバーセキュリティソリューション
複雑化 / 高度化するサイバー脅威に対抗するSOCとセキュリティ監視サービス
攻撃被害を極小化するためのインシデント対応支援ソリューション
サイバー演習によるインシデントハンドリング能力の強化
セキュリティ統合管理・対処ソリューション「NEC Cyber Security Platform」
クラウド型ファイル暗号化サービス －ActSecureクラウドセキュアファイルサービス－
セキュリティLCMサービス
EMMを活用したセキュアなモバイルワークソリューション
IoT 時代の経営を支援するサイバーセキュリティコンサルティング

サイバーセキュリティへのAI技術の活用
AI（人工知能）を活用した未知のサイバー攻撃対策
採るべき対策の「なぜ？」に答えるAIの可能性
オープンソースインテリジェンスを活用したサイバー脅威の検出と自動分析
犯罪捜査支援のためのサイバー・フィジカル統合分析技術

お客様に安全・安心を届けるための社内の取り組み
安全・安心な製品・サービスをご提供するための取り組み ～セキュア開発・運用～
サイバーセキュリティ人材のタレントマネジメント



Vol.70 No.2
（2017年10月）

特集TOP