

McAfee Enterprise Mobility Managementと Microsoft Exchange ActiveSync

安全で、扱いやすい、スケーラブルなモバイルデバイス管理

目次

Exchange ActiveSyncで実行できること	3
企業に広まりつつあるスマートフォン革命	3
企業は安全で、扱いやすく、スケーラブルな方法で増大しつつある、 モバイルデバイスの拡大を管理できるか？	3
ActiveSyncが十分でない理由	3
容易なセットアップとプロビジョニング	4
幅広い機能	4
強力な認証	4
コンプライアンスの徹底	4
詳細なレポート	4
運用上の留意点	4
アプリケーションのモバイル化	4
モバイルオペレーティングシステム(OS)の向上	5
デバイス管理	5
企業のIT活性化支援	5
ポリシーコンプライアンス	5
アプリケーション利用による生産性のアップ	6
企業のIT部門の責務	6
まとめ	6
ご利用にあたって	6
マカフィーについて	6

Microsoft Exchange ActiveSync(EAS)は、ActiveSync対応サーバーとデバイス間で連絡先、カレンダー、タスク、メールのプッシュ同期を提供するモバイル同期テクノロジーおよびプロトコルです。ただしEASは限定されたセキュリティポリシー管理しかサポートしていません。一方、McAfee® Enterprise Mobility Management(McAfee EMM®)は、デバイスのライフサイクル全体、セルフサービスのプロビジョニング、構成およびポリシー管理、コンプライアンス管理、およびレポート機能を提供することによりEASを補完します。McAfee EMMは、安全で、扱いやすく、スケーラブルな方法で拡大するモバイルを管理しようとしている企業に最適なソリューションです。

Exchange ActiveSyncで実行できること

ActiveSyncは、元々1996年にリリースされたMicrosoftが開発したモバイルデータの同期テクノロジーおよびプロトコルです。このテクノロジーの主要なポイントは次のとおりです。ひとつは、ハンドヘルドデバイスのデータおよび情報を特定のデスクトップコンピューター(元々ハンドヘルドPC Explorerとして知られる)と同期するテクノロジーで、もうひとつは、ActiveSync対応のサーバーとデバイス間で連絡先、カレンダー、タスク、メールのプッシュ同期を提供する、一般的にExchange ActiveSync(EAS)として知られるテクノロジーです。

Exchange ActiveSync(EAS)は独自のプロトコルで、Apple iPhoneのApple、webOSデバイスのHP、特定のAndroidスマートフォンのGoogleなど、多数のモバイルデバイス企業にライセンス供与されています。また、Exchange ActiveSyncテクノロジーは、Novell GroupWiseやLotus Dominoなどの他のメッセージングおよびコラボレーティブソフトウェアサーバーでも使用されています。

最初にEASを導入してすでに満足を得られているにもかかわらず、McAfee EMMソリューションを購入し、導入して活用するのはなぜでしょうか？

企業に広まりつつあるスマートフォン革命

2007年1月9日のiPhone 1.0の最初のリリースから、モバイル市場は大幅なパラダイムシフトを経験しています。スマートフォンは現在、使用されているモバイルデバイスの大半になりつつあり、優れた製品を開発できる賢明なベンダーはこの急速に成長する市場で優位に立っています。革新的で新しいスマートフォンは、従来のモバイルフォンを排除しつつあり、その波は今や企業にまで押し寄せています。最近まで、BlackBerryがモバイルビジネスユーザーにとって望ましい選択肢でしたが、今日ではその状況は急速に変化しています。BlackBerryとは異なり、McAfee EMMでは、企業がメールを端から端まで制御でき、スマートフォンやApple iPadがノートPCと同様にデータセンターの一部である真のエンドポイントになっています。企業ではますます、iPhoneやAndroidなど、他のスマートフォンプラットフォームをテストするようになってきました。さらに、iPadの発売によるタブレットの再出現により、モバイルデバイスの機会と要件の新しいセットを切り拓いています。

企業は安全で、扱いやすく、スケーラブルな方法で増大しつつある、モバイルデバイスの拡大を管理できるか？

エンタープライズレベルのモバイルデバイス管理(MDM)ソリューションに対するニーズは、多くのCIO、CSO、およびそれらのチームにとって重要な問題になっています。最初は、多数がMicrosoft EASなどの既に社内にあるツールを使用してこの問題に取り組もうとしました。しかしながら、ますます多くの企業内のITリーダーがEASなどのツールではこれ以上引き出せないことを認識するようになりました。安全で、容易で、スケーラブルなエンタープライズモバイルティ管理ソリューションはこのようにして企業にとってミッションクリティカルになっています。

ActiveSyncが十分ではない理由

ActiveSyncは、デバイスとMicrosoft Exchangeを同期させるために、主にMicrosoftによって開発された高度にスケーラブルなプロトコルです。Microsoftは、デバイスメーカーおよび多くのメールサーバーベンダーに対してこのプロトコルをライセンス供与しています。たとえば、IBM Lotus Notesは、Apple iPhoneへメールをプッシュするためにActiveSyncを使用します。また、ActiveSyncにはプロトコルの一部として限定されたポリシー管理機能も含まれていて、Microsoft Exchangeは基本的なポリシー管理にActiveSyncを活用しています。

一方で、McAfee EMMは、以下を含むデバイスのライフサイクル全体に対応することが重要であると考えています。

- セルフサービスのプロビジョニング
- 構成とポリシー管理

- コンプライアンス管理
- 詳細なモバイルデバイスレポート

EASではこのライフサイクルの限定されたサブセットのみに対応し、一部のポリシー管理とコンプライアンスの要素に焦点を当てています。

容易なセットアップとプロビジョニング

McAfee EMMのセルフサービスプロビジョニングは、Wi-FiおよびVPNとともに、電子メールに対してもデバイスを完全に構成します。ExchangeのActiveSyncポリシーは、Exchangeの構成が一度完了すれば、デバイスに対して部分的にコントロールを施すことができるようになります。実はこの最初のデバイス構成が複雑なのですが、McAfee EMMではこれを簡単に実行できるようにしています。

幅広い機能

ActiveSyncは、McAfee EMMとの比較ポイントにおいて、実行できる内容が限定されています。たとえば、ActiveSyncはデバイス全体を消去できますが、McAfee EMMはデバイス全体のほか、デバイスの一部(Exchangeで同期したメール、連絡先、カレンダー)を選択して消去できます。これは、企業のメール、連絡先、カレンダーだけを同期している個人所有のデバイスの場合に有効です。

強力な認証

McAfee EMMは、デバイス上にクライアント証明書を置いて、ネットワークからのメールアクセスに対して強力な認証を実行します。多くの大企業では、強力な認証または2要素認証を要求し、プッシュメールを許可するようにポリシーを変更しています。また、待ち時間、バッテリーの影響、および複雑さから、VPNを使用しない選択をしています。McAfee EMMでは、パフォーマンスまたはバッテリー寿命に影響を及ぼすことなく、強力な認証を使用したプッシュメールを提供し、モバイルVPNの複雑な要素を隠して、扱いを容易にします。

コンプライアンスの徹底

企業では、セキュリティ設定を満たすデバイスのみがネットワークに接続できるようにする必要があります。Exchangeだけでコンプライアンスを実施する機能は限られています。McAfee EMMでは、認証、管理、およびセキュリティ保護されているデバイスのみが接続できるように設定できます。たとえば、“ジェイルブレイク”された iPhone を接続ブロックすることも可能です。

詳細なレポート

McAfee EMMは、デバイスに関するリアルタイム情報とともに多数のデバイスデータやメタデータを収集し、これらの情報に関するレポートを提供します。デバイスに関するExchangeのレポートは極めて限定されています。McAfee EMMレポートはデバイスのコンプライアンス状況を追跡し、非準拠のデバイスについての状況をレポートできます。このレポートを使用して、ITサービスとしてユーザーにデバイスの修正を求めてコンプライアンス状態に戻すことができます。

運用上の留意点

デバイスの管理にExchangeを使用したくないと考える企業はいくつかあり、そうした企業ではノートPCの管理にもExchangeは使用しておらず、メールの利用度を高めてまでリスクを負いたくないと考えます。EMMにおいてiPhoneデバイスはメールを確認するための補助的な端末としてではなく、エンドポイントグループによって適切に管理される小型のコンピューターとして表示されるため、デバイスと情報を適切に管理することができます。

アプリケーションのモバイル化

企業では、ビジネスインテリジェンス、セールスフォースオートメーション、POS、文書作成などのメール以外のビジネスアプリケーションをモバイル化しようとしています。現在、McAfee EMMは、Windowsモバイルデバイス向けのアプリケーションを配信することもできます。またAppleによるiOS 4.0のリリースにより、iOSプラットフォームはiPhoneやiPadなどのAppleモバイルデバイス向けに企業のカスタムアプリケーションを配信するためのエンタープライズ・アプリケーションストアにもなり得ます。

モバイルオペレーティングシステム(OS)の向上

モバイルOSベンダーは、ActiveSyncを超えるデバイスのセキュリティとその管理の必要性を認識しています。Apple iOS 4.0には、成熟したMDM機能、そしてセキュリティ管理用にMcAfee EMMと同様なサーバーを必要とするデバイス補助ツールがあります。Google Android 2.2には、同様なMDM機能が導入されています。これはいずれもエンタープライズモバイルデバイスのセキュリティ管理には、スケール、セキュリティ、コンプライアンス、レポートに対応する完全な管理サーバーが必要と考えていることを示しています。

デバイス管理

McAfee EMMはActiveSyncポリシーおよびiPhone構成プロファイルの使用を通して、完全なiPhoneセキュリティと構成管理を行います。反対に、ExchangeはiPhoneの機能のサブセットを管理するActiveSyncポリシーのみを管理するにとどまります。

現在、ActiveSyncポリシーは、iPhoneやiPod Touch機能のサブセットを管理するもので、ActiveSyncはデバイスのパスワード設定の強制やデバイスカメラの利用を制限するといった機能を定義するためのポリシーセットを提供しています。ActiveSyncプロトコルはデバイスのリモートワイプをサポートしています。

Appleは、企業のIT部門が一斉にデバイスを構成できるようにするための優れた方法を提供することによって、iPhoneを他のスマートフォンと差別化しています。構成プロファイルは、デバイス構成(たとえば、VPNやWi-Fi設定)および認証情報をすばやくロードするXMLファイルとして提供され、構成プロファイルの作成および安全な配布に使用されるプロファイルサービスは、Appleブループリントの中核をなしていて、iPhoneやiPod Touchをサポートする企業のIT部門のリファレンスモデルとして機能しています。

McAfee EMMは、Apple構成プロファイルとActiveSyncポリシー管理という二つの管理アプローチを一つのデバイス管理ソリューションに統合しており、グループに関連付けられたユーザーをさらにデバイスに関連付けるというグループベースのポリシー管理を適用しています。これにより、一対多数のポリシー管理が可能になり、iPhoneの大規模展開を簡素化します。一方、Exchangeは各デバイスを個別に管理する方法をとっています。

企業のIT活性化支援

企業では今後、社員がビジネスに個人のiPhone使用を許可するようになっていくと考えられます。企業のIT部門は従業員が個人用デバイスを職場に接続できるアクティブ化プロセスを自動化したいと考えています。自動化には通常、メールやアクセス(Wi-FiまたはVPN)などの基本的なサービスの構成が含まれます。iPhoneの場合、これらの機能はExchangeの機能範囲以上を含んだ設定ファイルの配布を通じて構成されます。

McAfee EMMは、iPhoneユーザーが接続する企業のデータセンターを意識することなく自動的にiPhoneをモバイル用アプリケーションやサービスが管理されているシステムのエンドポイントに設定することができます。Exchangeは、ExchangeがサポートしているActiveSyncポリシーの設定を介してiPhone側でActiveSyncメールクライアント設定を手動で有効にする必要があります。

また、McAfee EMMは、デジタル証明書をiPhoneに導入するためにSimple Certificate Enrollment Protocol (SCEP)の使用を含むApple iPhone登録プロセスも実装しています。この機能により、ITサービスおよびアプリケーションの構成に使用される今後のiPhone構成プロファイルの安全な導入が可能になります。このプロセスはExchangeポリシー管理の範囲外です。

ポリシーコンプライアンス

McAfee EMM Access Managerは、企業ネットワークに接続される前にActiveSyncポリシーと構成プロファイルが有効状態にあるかを確認するための機能で、これによりすべてのiPhoneデバイス上でコンプライアンスチェックが実行されます。McAfee EMM Access ManagerはDMZ内で操作されるため、IT部門はActiveSyncをインターネットに直接公開して、セキュリティの追加レイヤーを提供する必要がありません。

McAfee EMMプラットフォームによるポリシーコンプライアンス適用は、iPhoneに関するすべてのデバイス情報をカバーしています。これにはハードウェアのバージョン(たとえばiPhone 3GSであればデータが確実に暗号化されていることがわかるため)、ソフトウェアのバージョン、コンフィグレーション設定、ActiveSyncポリシーおよびユーザーとそのiPhoneの認証が含まれます。

アプリケーション利用による生産性のアップ

McAfee EMMは、メッセージングサーバー非依存で、Exchange、Lotus Notes、IMAP、Google Appsを含む環境をサポートしています。McAfee EMMでは電子メールをあたかも一つのアプリケーションのように取り扱いますが、さらに個人設定を可能にして、VPNおよびWi-Fi構成を使用してiPhoneをアプリケーションに接続することで電子メールに加えてさらに生産性を発揮することができます。

企業のIT部門の責務

概して、多くのIT組織はExchangeからBlackBerryデバイスの管理およびコントロールは考えないでしょう。企業のIT部門はメッセージングインフラを高度に保ちますが、それをノートPCまたはPCのエンドポイントマネージャーとして使用してきていないため、iPhoneのデバイス管理にExchangeを使って企業のメッセージングサーバーの利用幅を広げるというリスクを負いたくはありません。同様に、メッセージンググループはデバイス管理グループにExchangeへの管理アクセス権を付与したいとは考えていません。

まとめ

企業におけるモバイル環境は急速に変化しています。スマートフォン革命は世界中に広まりつつあり、その影響はITおよびセキュリティ組織全体に及んでいます。将来のモバイルビジネスユーザーによって、スマートフォンやタブレットを含む多くのモバイルコンピューティングプラットフォームの有効化が求められるため、そのすべてが安全で、扱いやすく、スケーラブルな方法でサポートされる必要があります。

Exchange ActiveSync (EAS)をエンタープライズモバイル管理ツールとして拡張しようというMicrosoftの試みは幅広さにおいて十分ではありません。一見してEASは組織のMDMニーズのすべてを提供できるように思われますが、これが事実でないことは明白になってきています。

McAfee EMMは、安全で、容易で、スケーラブルなエンタープライズモバイル管理ソリューションを提供します。EASはMcAfee EMMの実行可能な代替にはなり得ません。

ご利用にあたって

McAfee EMMは、現時点でエンタープライズモバイル管理に最適なソリューションです。マカフィーの営業担当者にお問い合わせください。私たちは、iPhones、iPad、およびAndroidデバイスを組織内にシームレスに統合すれば、確実に生産性が増すことを確信しています。

マカフィーについて

マカフィーは、インテル・コーポレーション (NASDAQ:INTC) の完全子会社であり、セキュリティ・テクノロジー専門のリーディングカンパニーです。世界中で使用されているシステム、ネットワーク、モバイルデバイスの安全な接続、webの閲覧およびオンライン取引の安全を確実に支えています。マカフィーは、他の追従を許さないクラウドベースのセキュリティ技術基盤Global Threat Intelligence™ (グローバル スレット インテリジェンス) を活用して、革新的な製品を送り出しています。個人ユーザーをはじめ、企業、官公庁・自治体、ISPなど様々なユーザーは、コンプライアンスの確保、データの保全、破壊活動の阻止、脆弱性の把握を実現し、またセキュリティレベルを絶えず管理し、改善することができます。詳しくは、<http://www.mcafee.com/jp/>をご覧ください。