≪コラム 1 ≫

モバイル環境におけるエンドポイント管理

― PC、サーバーからスマートフォンまで、ネットワーク接続端末（エンドポイント）を全部まとめて統合管理 ―

日本アイ・ビー・エム株式会社
ソフトウェア事業 Tivoli 事業部
クライアント・テクニカル・プロフェッショナルズ
主任ITアーキテクト

南郷 理恵子 Rieko Nangoh

【プロフィール】
1999年、日本IBM入社。金融機関のインフラ管理システム構築プロジェクトへの参画、システム管理製品テクニカル・セールスを経て、2004年よりセキュリティ管理製品テクニカル・セールスを担当。2011年よりエンドポイント管理製品テクニカル・セールスを担当し、現在に至る。

■ モバイル・デバイスのビジネス利用が本格化

世界のスマートフォン出荷台数が、2011年、初めてPCとタブレットの合計を上回ったというニュースをご存知でしょうか。スマートフォンの市場規模は急激に拡大しており、2015年にはPCなどエンタープライズ・デバイス市場の約40%を占め、その市場規模は12億ドルを超すと予測されています。

日本でも、2011年度のスマートフォン法人加入者数は2010年比で約2倍となる134万人に拡大し、2015年には8倍増の554万人に達するだろうといわれています［1］。

これは、必要な情報に瞬時にアクセスできる「機動力の高さ」と軽量デバイスであるための「持ち運びやすさ」というスマートフォンの特性が、場所にとらわれずに仕事ができる環境を整備し、事業継続性と生産性を向上したいという企業ニーズに合致した結果です。

それでは、どのようなビジネス・シーンでモバイル・デバイスは活用されているのでしょうか。現状では、スケジュールの確認、メールの送受信、Webサイトを活用した移動経路や訪問先の確認などが利用目的の多数を占めています。これだけでも外出時の業務の迅速化やモバイル社員とのコミュニケーション向上を図ることができ、ビジネスへの貢献度は高いといえます。

しかし、モバイル・デバイスのビジネス・ユースはこれだけではありません。営業日報の作成、e-ラーニングの実施、顧客先での説明資料提示など、さまざまな業務アプリケーションでの活用が、今後は増えていくと予想されます。

このように、飛躍的な成長を遂げるスマートフォン市場ですが、ビジネスへの利用には慎重な企業も数多くあります。

その理由としてよく挙げられるのが、盗難・紛失による情報漏えいやウイルス感染といった「セキュリティー面での不安」と、管理が煩雑になる、新たなスキルと人員を維持することは難しいといった「運用面での不安」です。

■ モバイル・デバイスのセキュリティー

米国のセキュリティー調査会社の昨年のレポート［2］によると、4人に1人が過去に携帯電話を紛失した経験があり、67%のユーザーがパスワード保護を実施していないと回答しています。このことから、個人に依存したセキュリティー対策だけでは不十分で、企業レベルでの管理が必要な現状がうかがえます。

またIBMのセキュリティー・リサーチ機関「X-Force」のレポート［3］によると、スマートフォンの出荷台数と比例してモバイル・デバイスを対象とした脆弱（ぜいじゃく）性が急増しており、2009～2011年の2年間で3倍を超える脆弱性が確認されています（図1）。同様に、モバイル・デバイスの脆弱性を利用した攻撃もこの2年間で10倍近くに増加しています（図2）。では、どうすれば「ビジネスの効率化」と「他社との差別化」を図る画期的なツールであるモバイル・デバイスを安心して利用できるのでしょうか。

モバイル・デバイス使用時のセキュリティー・リスクの中でも、企業への影響度が大きいのが「機密情報の漏えい」です。図3のようなセキュリティー対策を取ることでリスクを軽減できますが、AndroidやiOSのセキュリティー機能は発展途上であり、モバイル・デバイス単体でセキュリティー対策を講じることは難しいのが現状です。また、コスト削減のため、個人所有デバイスのビジネス・ユースを許可する企業も多く、使用アプリケーションを規制しきれないという事情もあります。

■ モバイル・デバイス管理システムの登場

こうした背景から、近年、脚光を浴びているのがMobile

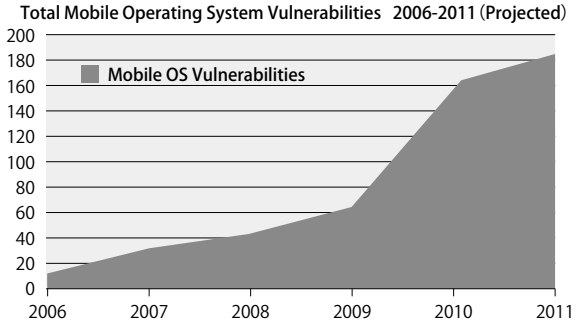

図1. モバイル・デバイスの脆弱性

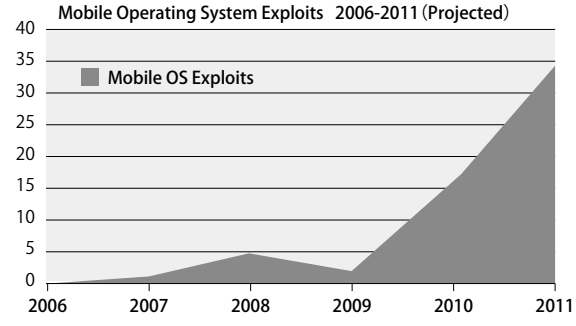

図2. モバイル・デバイスの脆弱性を突いた攻撃

Device Management（以下、MDM）です。

MDMとは、スマートフォンやタブレットPCなどのモバイル・デバイスに特化したセキュリティー強化機能や端末管理機能を提供するツールやサービスを指します。一般的にMDMは下記のような機能を提供しています。

《MDMの提供機能》

- デバイス情報の取得
- セキュリティー・ポリシーの作成・適用
- アプリケーションの利用制御
- パスワードのリセット
- 位置情報の取得
- リモート・ロック
- リモート・ワイプ（盗難・紛失時のデータ削除）
- Jailbreak/Root化の検出
  （制限を非正規に解除し、特権ユーザーへの昇格を検出）

MDMを導入することで、モバイル・デバイス単体では実現できないセキュリティー対策を実施することができ、企業がスマートフォン採用に慎重な理由の1つである「セキュリティー面での不安」を低減することができます。しかし、依然として管理の煩雑さに代表される「運用面での不安」は残ります。

再度、図3を見てみましょう。「端末情報の把握」「社内共通セキュリティー・ポリシーの整備／適用」「必須アプリケーションの適用状況管理」など、見覚えのある項目が並んでいませんか？実は、モバイル・デバイスとPCのセキュリティー対策には共通項が多くあります。そこで、ご紹介したいのが、「エンドポイントの統合管理」です（図4）。

IBM Endpoint Manager for Mobile Devices［4］をはじめとするエンドポイントの統合管理製品は、既存デバイスとモバイル・デバイスを同一のインフラで管理することで、MDM特有の管理機能に加え、共通コンソールでのデバイス状況の可視化、レポートの共通化など、管理ポイントを集約したシンプルな運用を実現します。

また、情報を集約し状況を的確に把握することは、セキュリティー・リスクの早期発見、早期対応につながります。

エンドポイント統合管理の特長としては以下が挙げられます。

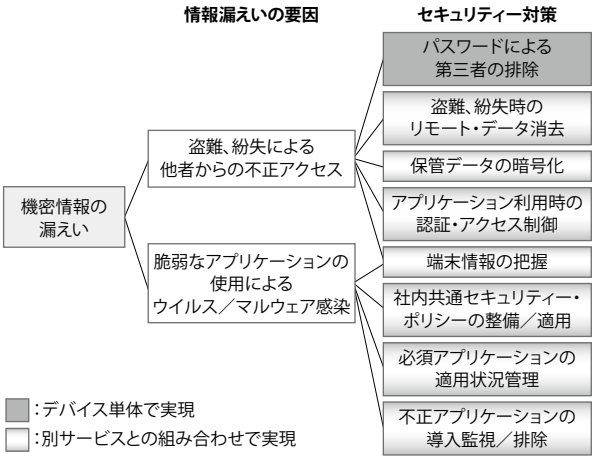

図3. 情報漏えいの要因とセキュリティー対策

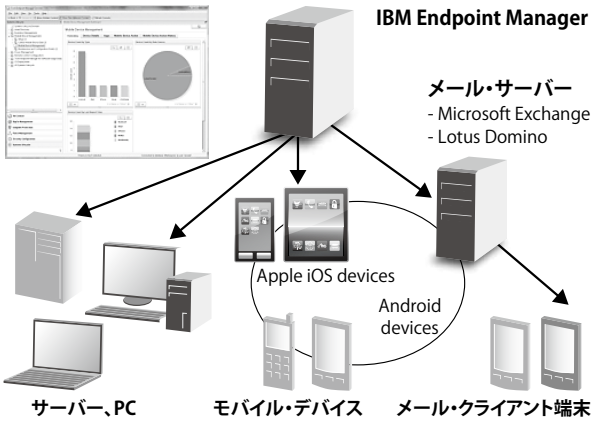

図4. 既存デバイスとモバイル・デバイスの統合管理

《エンドポイント統合管理の特長》

- 既存担当者による管理体制の確立
- 既存管理基盤の再利用によるコスト削減
- 管理項目の共通化による効率的な運用
- 単一レポートによる資産管理工数の削減
- 全端末状況の可視化による脆弱性の早期発見／早期対応
- 共通管理基盤利用によるセキュリティー・レベルの底上げ
- モバイル利用者、社内業務担当者など業務に応じた柔軟なセキュリティー・ポリシーの適用

このように、エンドポイントの統合管理は、シンプルで効率的な運用と、エンタープライズ・レベルのセキュリティー強化をモバイル・デバイスにもたらします。

自社でエンタープライズ・レベルの管理システムを構築・維持することが難しい場合には、クラウド・コンピューティングのサービスであるSaaS（Software as a Service）やMSP（Management Service Provider）を利用してエンドポイント管理サービスを外部に委託してもよいでしょう。

■ 最後に

ビジネスを取り巻く環境は日々進化しています。個人向けのデバイスであったスマートフォンがビジネスで当たり前に使用されるなど、モバイル・デバイスの積極的な活用が進んでいます。どこからでも業務情報にアクセスできるモバイル・デバイスの特性を考えると、企業のMDMには、エンタープライズ・レベルの管理が必須といえます。

ビジネスの変革をもたらすスマートフォン。この画期的なビジネス・ツールの採用をきっかけに、シンプルで効率的なエンドポイント統合管理を目指してみませんか。

［参考文献］

［1］ IDC Japan, 国内ビジネスモビリティ市場予測, http://www.idcjapan.co.jp/Press/Current/20110602Apr.html
［2］ Sophos Press Releases, TNSによる調査結果, http://www.sophos.com/en-us/press-office/press-releases/2011/08/67-percent-of-consumers-do-not-have-password-protection-on-their-mobile-phones.aspx
［3］ IBM X-Force 2011 Mid-year Trend and Risk Report, http://www.ibm.com/services/us/iss/xforce/trendreports/
［4］ IBM Tivoli Endpoint Manager, http://www.ibm.com/software/jp/tivoli/products/endpoint/