NIKKEI BUSINESS DAILY FORUM
日経産業新聞
フォーラム2013

マルチデバイス時代のセキュリティを考える

～効率と安全を両立させる スマートデバイス活用法とは～

個人端末を仕事で使う「BYOD（Bring Your Own Device）」は企業の情報管理コストを削減し、利用者の利便性が高いことから最近注目を集めている。一方、紛失時のデータ流出や、ウイルスの感染リスクなど、普及に向けてセキュリティ面での課題がある。先ごろ開催した日経産業新聞フォーラム2013「マルチデバイス時代のセキュリティを考える」（主催＝日本経済新聞社、協賛＝ソリトンシステムズ、日商エレクトロニクス、AirWatch/データコントロール）では、 業務効率化とセキュリティの確保を両立させるスマートデバイス活用の可能性を、事例を交えて紹介した。

基調講演

マルチデバイス時代のネットワークセキュリティ

東京大学大学院情報理工学系研究科教授　江崎　浩氏

BYOD利用に安心不可欠

マルチデバイス、マルチスクリーンの時代のセキュリティをどのように考えるかがテーマだが、そもそもセキュリティとはどうあるべきかを問い直す必要がある。「安全」とあるがゼロのインシデントを目指すのは間違いであり、ある程度の安全性を保証しながら「安心」してモバイルデバイスを使える環境を構築すべきである。極端に言えば「デバイスを飲み屋で落としても大丈夫」という安心感があれば、モバイルワークの効率も高まるはずだ。

クラウド化の進展は著しく、マルチデバイス時代のモバイル型ビジネスの台頭をバックエンドクラウド化が支援・実現しているのが現状である。日本は高速の無線通信環境が整備されており、モバイル端末が使いやすい。つまりセキュアなバックエンド環境と非常に高いコンピューティング性能を持ったスマートデバイスを使うことで高いセキュリティが高い効率性とともに実現されている。

その環境を生かしたビジネススタイルがBYODである。もともとBYODは米政府の予算削減から出てきた話題とされている。つまり企業にとってもコスト削減の可能性がある。しかしセキュリティは確保しなければならないので、バックエンドでしっかり管理しようというのがもともとの発想だった。

最近ではスマートフォンやタブレットで複数のOS、しかもそれぞれ異なるバージョンが混在するようになった。またユーザーはプライベートでも業務でも、様々なクラウドにアクセスするようになっている。複数のID・パスワードを保有するのは面倒なので、シングルサインオンの環境も実現しなければならない。しかも複数の運用ポリシーが1つのデバイスに適用されなければならなくなる。

従来はファイアウオールで防げると考えていたものが、もはや通用しなくなっている。データセンターの中でも仮想マシンが増えていることで、1カ所から侵入できれば、どこでも侵入できるようになる。ファイアウオールで防御できなければ、全てのデバイスがしっかりとしたセキュリティ機能を備えていなければならない。モバイルデバイスを誰がアクセスするのか、何をできるのかを管理できなければならない。

BYODを実現するためには、スマートデバイス側にもバックエンドのシステムにも、セキュリティとプライバシーを初めから意識してデザインできるようなシステム、アクセスのログをしっかりと管理して、どういうリアクションをするかという機能を備えたシステムを構築しなければならない。セキュリティで活動をがんじがらめにすれば、スマートデバイスを使っての業務効率向上は不可能となる。セキュリティは本来、「安心」を保証するものであり、それが保証されていれば使い慣れたオウンデバイスを使用して、のびのびと仕事ができる環境を提供することが可能になる。

プレゼンテーション1

機密情報を持ち歩かないＢＹＯＤモバイルワーク ～セキュアブラウザでマルチデバイス時代を乗りこなす～

ソリトンシステムズ
プロダクトマーケティング部プロダクトマネージャ　宮崎　洋二氏

証明書でシャドーIT排除

スマートフォンやタブレットなどスマートデバイスは、モバイルワークと相性がいい。スマートデバイスは軽量かつ高機能で安価、しかも通信機能が強力。ユーザーからみれば非常に使いやすいデバイスだが、情報システム部門から見ると危険な要素も多い。頻繁に持ち運ぶと落とす危険性が高まる。盗まれやすいという面もある。企業ネットワークに侵入され、重要な情報が盗まれるのではないかなど。便利さの裏返しが危険な部分と映る。

その相反する事実をどう捉えるかで、便利なのか、それとも危険なのかという見方も変わる。BYODを検討する際には「リスクは確かにある。しかしそれよりも使うメリットが大きい」ということを認識する必要がある。スマートデバイスを活用するためには、まず情報漏洩リスクを排除する。ゼロにできないならば、許容できる範囲までレベルを落とす。そのために必要な対策を、パズルのピースのように順序良く当てはめていく。アクセスできる人、端末をふるいにかけることが第1ステップ。次にその人が端末を紛失したケースでもリカバリーできる仕組みを考える。

まず、認証・識別。以前から社員なのかそうではないのかをID・パスワードで区別してきた。会社支給のパソコンが使用されていたので端末を識別する必要性は低かった。しかしモバイルワークでBYODを導入する場合、端末の識別は必須だ。「つないでいい社員」による「つないでいいデバイス」利用のみを許可するのが目的。社員はプライベートで専有するデバイスだけでなく、「家族と共有するデバイス」も所有しているかもしれない。企業の方針によっては「つないでいい社員」が持つ「つないでほしくないデバイス」が出てくるわけだ。これを〝シャドーIT〟と言う。

こうしたデバイスの多様化の中で、セキュリティをどのように確保するかが最重要課題となる。この対策には、デジタル証明書による認証が最適だと考えている。証明書はID・パスワードによる認証では対応できない〝シャドーIT〟を排除できる。買い替えの激しい個人用スマートデバイスにも投入でき、端末を紛失した場合でもすぐに失効や再発行ができる。そうしたニーズに向けて、ソリトンシステムズではネットワーク認証サーバーとして「NetAttest EPS」を提供している。証明書の発行や認証機能を搭載し、すぐに活用できるアプライアンス製品である。管理・運用機能も充実している。

企業のネットワークは水道や電気と同じインフラである。止まれば業務が停止してしまう。BYODで生産性向上を図るためには、使う側が不安や不便を感じない仕組み、つまり「安心」なシステムを構築し提供することが重要だと考えている。

プレゼンテーション2

Going Mobile!モバイルワークスタイルを追い求めて ～モバイルアプリケーション活用でＢＹＯＤが進化する～

日商エレクトロニクス
マーケティング本部第二マーケティング部部長　榎本　瑞樹氏

クライアント環境の全体最適化

近年、コンシューマー市場でのスマートデバイスの普及やデジタルネーティブの社会進出により、スマートデバイスをビジネスに活用したいという要求が強まっている。

それは、スマートデバイスからメール・スケジュールが確認できるという限定的な活用ではなく、慣れ親しんだユーザーデバイスやアプリケーションを利用し、自宅、喫茶店などオフィス以外の環境で働きたいという要求である。

つまり、いつでも・どこでも・どんなデバイスからでも業務ができる「モバイルワークスタイル」という働き方だ。

それを実現するためには、スマートデバイスをどのように活用するかだけでなく、PCを含めたクライアント環境全体を最適化する必要がある。最適化方法の一つとして、Citrix XenDesktopで実現するVDI（デスクトップ仮想化）だ。マルチデバイスから個人に割り当てられたデスクトップ環境にアクセスし、異なるOSでアプリケーションを稼働することができる。iPad上で、Windows8を動かすことも可能だ。

しかし、モバイルワークスタイルを実現するためには、VDI導入を行うだけではなく、スマートデバイスへのセキュリティも十分注意しなければならない。スマートデバイスのセキュリティといえばMDM（モバイルデバイス管理）が一般的だが、ユーザーデバイスの業務利用を考慮するとMDMだけでは十分ではない。なぜなら、ユーザー所有のスマートデバイスにはプライベートと業務利用のアプリやデータが混在し、情報漏洩などのセキュリティリスクが高まるからだ。しかしながら、ユーザーはプライベートの環境を会社のIT部門に監視されたくない。

そこで、プライベートと業務を両立するソリューションの一つが、Citrix XenMobileだ。業務領域とプライベート領域を分離し、業務アプリやデータは隔離された領域のみで利用できる。そのため、プライベート領域から業務データへのアクセスやダウンロードはできない。

XenDesktopとXenMobileを組み合わせることで、ユーザーへ高い利便性を提供しながら、すべてのアプリケーション、データを一括で管理することができ、どんなデバイスを利用しても、会社として守るべきものを守る。真のモバイルワークスタイルを実現できる。

プレゼンテーション3

ＡｉｒＷａｔｃｈが実現する、シンプルでセキュアな スマートフォン・タブレットの活用

ＡｉｒＷａｔｃｈアジア・パシフィック担当取締役　ジェフ・バウム氏

様々なデバイスを統一的に管理

スマートデバイスの活用は、ビジネスにとっては不可欠な要素になっている。ビジネスパーソンの多くは、スマートフォンなど自分の所有する端末を仕事にも活用したいと考えており、それも電子メールだけではなく業務のアプリケーションや企業の保有する情報にもアクセスすることを求めている。しかも個人所有のスマートデバイスは、流行や好き嫌いで買い替えることも多く、BYODの場合、そうした変化にも対応する必要がある。

BYODで鍵となるのは、まずセキュリティ。様々なデバイスを統一的にセキュリティ管理することが必要だ。また、企業の業務アプリケーションをラッピングしMDMと連携させていくことも重要になる。しかも個人所有の端末に備わるMDMと企業が支給する端末のMDMを識別することも必要である。

当社が提供する「Workspace」は、アプリケーションレベルでミッションクリティカルな業務用アプリを、完全にその他のアプリと遮断しシングルコンテナ化する。それによりデバイスの暗号化を確実に行うとともに、シングルサインオンの機能も統合。そして各端末に備わる固有のMDMや電子メール管理、アプリケーション管理、コンテンツ管理などに対応できる管理システムを提供している。しかも複数の部署や遠隔地のオフィス、社内の各層に応じたマルチテナント型管理に加え将来的な端末の拡張にも対応した管理手法を構築することができる。BYOD用に「Workspace」を適用することでBYODをサポートし、支給された標準デバイスでは端末固有のMDMを適用することで、企業内のシステムから末端にある個人のモバイル端末までシステム統合することが可能になる。

一般的にスマートデバイスなどモバイル端末に対する管理は、デバイスのロック機能や位置情報の取得、情報を消すワイプ機能などが現在の主流になっている。しかしビジネスでBYODに対する要求が拡大し、多種多様なデバイスが導入され、しかも急速に変化している状況では、既存の管理手法ではセキュリティ対策が追いつかないのが実情だ。そうした変化に対応しながら投資に対するリターンを確保し、同時に社員にとって利用しやすいシステム環境を提供することが、今後のビジネスの拡大には不可欠になっている。

当社の提供するシステムは、日本の大手メーカーを含めグローバルな大企業や米政府、警察機関などでも採用実績がある。日本語を含め、世界の主要地域の言語をサポートしており、毎月500以上の新規顧客を獲得している。それだけ世界のビジネス環境でスマートデバイスを活用したモビリティーが重視されるとともにBYODが注目され、実際に導入が進んでいるということである。

協賛：ソリトンシステムズ
日商エレクトロニクス
Air Watch／データコントロール

広　告　企画・制作＝日本経済新聞社クロスメディア営業局