煩雑化する管理：
モバイルデバイスの管理方法

ある従業員が週末に iPhone を購入し、それで業務の E メールを受信できるようにしたいので方法を教えてほしいと言ってきたとします。そのような場合のポリシーは用意されていますか？

もしなければ、すぐに用意することになるでしょう。

これは業務環境でモバイルデバイスが急増し、それによって IT の新たな課題がもたらされることを示すほんの一例にすぎません。しかもこのような状況がなくなることはなく、しばらく続きます。世界のモバイルワーカー人口は 2013 年までに 12 億人に達すると予測されています。

ある市場調査会社は、世界中で使用される携帯電話台数が 2011 年までに 50 億台になると予測しています。この台数には、人々が使用するタブレット、ネットブック、およびノートパソコンは含まれていません。

過去数年間におけるこうしたモバイルデバイスの急増は、IT 責任者にとって、まったく新たな管理とセキュリティの課題を生み出しています。従業員が業務環境に自分のモバイルデバイスを持ち込み、それを企業のネットワークに接続することを求めるようになっているからです。

デバイスが企業の所有、または個人の所有いずれの場合でも、IT 部門には企業データが保存された PDA、タブレットコンピュータ、スマートフォン、ノートパソコン、その他のモバイルデバイスをどのように管理するかという戦略が必要です。

このエグゼクティブソリューションテクノロジーガイドでは、企業が大量のモバイルデバイスを管理する最適な方法について、専門家や同様の環境にある企業のアドバイスを紹介します。また、モバイルデバイスに保存されたデータのセキュリティ維持に利用できるテクノロジーソリューションもいくつか考察します（3 ページ、「モバイル環境のセキュリティ強化」）。最後に、10 ページには「モバイルデバイスの管理とセキュリティをマスターする方法」という役立つチェックリストがあります。

目次

モバイル化がもたらす IT の新たな課題

モバイルデバイスの急増は、戦略的および戦術的な数多くの問題に対応している IT 部門にとって課題となっています。戦略的な問題としては、モバイル環境に IT 組織内のどこが対応するかという課題があり、戦術的な問題としては、デバイスを管理し、企業のデータ資産を保護するという視点からの課題があります。

さらに、スマートフォンは現在、仕事と私用との両方で使用されているため、プライバシーおよびセキュリティに関する懸念事項も増えています。何年にも渡って企業は、従業員に BlackBerry（ビジネス向けスマートフォン市場で優位に立ち続けているスマートフォン）を貸与してきました。しかし、企業側の経費削減に加え、自分のスマートフォンを使用したいという従業員の希望により、多くの従業員がそれぞれのデバイスを所有して、業務上の連絡も個人的な連絡もすべてそのデバイスで処理するようになりました。

「これまで多くの企業が RIM または Windows Mobile デバイスを標準的な端末として選んでいましたが、最近はアップルの iOS やグーグルの Android などが搭載された別のタイプのデバイスが普及し始めています」と、IDC のモバイルエンタープライズ担当シニアリサーチアナリストの Stacy Crook 氏は述べています。

利用端末の混在

どの通信業者を選択するかはユーザーが使用しているスマートフォンによって決まることが多く、さまざまなスマートフォンが使用されている今の状況から考えると、企業が通信業者を 1 社に絞る可能性は低くなります。その一方で通信業者は企業顧客と協力し、個人のスマートフォンにあるエンタープライズアプリケーションへのアクセスだけでなく、IT 部門が企業の情報資産を保護するために必要なツールも提供しています。

「個人が自分のスマートフォンを企業に持ち込むことを希望するようになったことで、セキュリティの問題が今まで以上に表面化しています」と、Crook 氏は述べています。「IT 部門は、新しいデバイスの急増について考え始めています」。

デスクトップの場合と同様、モバイルワーカーを管理する IT 責任者は、正確で効率的なインベントリ管理システムを確実に導入する必要があります。つまり、自社が所有しているもの、デバイスの所在場所、およびそのデバイスが使用されているかどうかを把握する必要があります。次にソフトウェアの配布の問題に対応する必要があります。またデバイスの紛失、盗難、または破損が生じた場合にそのデバイスを特定して使用できないようにし、データを消去する仕組みも必要になります。ノートパソコンで行われている管理は、既に標準となっていますが、スマートフォンでも同様の管理が不可欠になってきています。

戦略面では、IT 部門は、例えばサーバの専門的な技術者と同様に「モバイル環境に対応するための専門的な技術者」が他の技術者と協力して、IT 業務の中核的なタスクに今まで以上に取り組むことができるようにする必要があると、一部の専門家は指摘しています。またモバイル環境への対応は、企業のエンタープライズアーキテクチャにも組み込む必要があります。

外部の調査機関である Forrester Research の最新レポート『Insight for CIOs: Make Mobility Standard Business Practice（CIO 向けレポート : モバイル環境への対応をビジネスの標準的な手法にする）』では、「現在、IT 部門にはモバイル環境に対応するための専門的な技術者がいます。この技術者が BlackBerry Enterprise Server を管理し、また iPhone や Windows Mobile などのスマートフォンの設定と管理を担当しています。多くの場合、彼らはアプリケーションのモバイル化において重要な戦力になっています」と述べられています。

しかし同レポートは、このような役割が必要であるとする一方で、IT 部門が行っているモバイル環境を十分に活用するための取り組み方は、その大半が「常識やこれまでの経験に反するもの」であると述べています。

モバイル環境のための再構築

IT 部門は、日々の業務やさまざまな業務でのモバイルテクノロジーの利用に対応するために、組織を再構築する必要があります。モバイル環境に対応するための専門的な技術を備えた技術者の才能は、インフラストラクチャに関する業務に専念させる以外にも活用できます。Forrester によると、この技術者たちをアプリケーション開発チームに参加させることも、IT で実現する主要な機能としてモバイル環境を提供するための 1 つの方法です。

また、どのような場所にいても利用できるアプリケーションを提供することも役に立ちます。これはモバイルテクノロジーによって、作業場所が選べるようになったことが主な理由です。このような再構築により、モバイル環境への対応の機会に合わせて、事業の見通しを行う必要があります。

「個人が自分のスマートフォンを企業に持ち込むことを希望するようになったことで、セキュリティの問題が今まで以上に表面化しています。**IT 部門は、新しいデバイスの急増について考え始めています」。** - Stacy Crook 氏

モバイル環境のセキュリティ強化

企業のモバイルワーカーの生産性が高いことにあまり疑問の余地はありませんが、IT 責任者にとっては、モバイルコンピューティングによってセキュリティレイヤがもう 1 つ増えることになります。John Dodge 著

デバイスがさまざまな用途に使用される状況などへの対応、主要な IT 機能のモバイル化、および管理ツールとセキュリティツールの導入によって、企業はモバイル環境への投資に対して最大の成果を得ることができます。

この 20 年間で、モバイルコンピューティングはほとんどのプロフェッショナルにとって不可欠なものとなっています。

しかし広範囲に分散した従業員によって、情報資産の保護という業務を担当する IT 管理者にとっては問題が生じています。実際、モバイル環境への対応によって、こうした資産は企業のオフィスやデータセンター内にのみ保存されている場合と比べ、漏洩や攻撃に対する脆弱性が大きくなっています。

オフィスにいる場合と同様の情報資産とツールを使って、時間や場所を問わずに仕事ができることのメリットは極めて明らかです。それ故、モバイル環境への対応は競争力を得るために不可欠であり、企業にとっても従業員にとってもメリットがあります。

モバイルコンピューティングは従業員とお客様の距離を縮めます。従業員がリモートで業務を行う、つまりお客様と直接面談して仕事を進めれば、双方が同じ情報にアクセスしやすくなります。在宅勤務の従業員であれば、オフィススペースが共有できるようになります（あるいはオフィススペースがまったく不要になるかもしれません）。モバイルコンピューティングによって通勤時間を短縮でき、消費電力も削減できます。このようにモバイルコンピューティングにはさまざまなメリットがあります。

では、従業員がいるあらゆる場所に存在するこの情報資産を、どのように保護すればよいのでしょうか？これは皆さんが考えているほど難しいことではありません。

モバイルデータには 2 種類あります。1 つは保存データです。ノートパソコンなどのモバイルデバイスに保存されているデータです。もう 1 つは転送データです。例えば、ノートパソコンとクラウド間で転送されるデータです。この記事では、これらの保存データについて説明します。

「要は、（セキュリティに）どれだけコストをかけようと思うかです。組織は、専門家や博士のチームでなければ破れないような、最高水準のセキュリティを必要としているのでしょうか？それとも、その組織の環境には Microsoft BitLocker Drive Encryption の無料バージョンで十分なのでしょうか？」デルのビジネスクライアント製品グループ、ソフトウェアソリューション企画担当シニアマネージャである John Holstrom はそう尋ねます。「100 % 安全なシステムというものは世界にありません」。

保存データを保護する方法は、企業に適したデータセキュリティのレベルに応じて主に 3 つあります。
1 つ目は、デバイスへの不正アクセスの防止です。これには、チップレベルの防止を始め、

いくつかの方法があります。チップレベルの防止では、侵入者はデバイスの電源を入れた直後に何もできなくなります。

指紋認証や自己完結型のスマートカードは、認証の最初の関門となるものです。セットアップ時に設定されるパターンやプロファイル情報がチップに保存されます。ユーザーの親指の指紋やスマートカード情報がノートパソコンのチップに保存されているものと照合され、情報が一致しない場合はそのノートパソコンにアクセスすることはできません。しかもその照合は、ユーザーが使い慣れた Microsoft Windows のパスワードを入力する前に行われます。

データを保護する 2 つ目の方法は、データの暗号化です。これにより、デバイスの紛失や盗難が発生しても誰もそのデバイスを使用することができなくなります。データの暗号化で重要なのは、それが法律的な見地から見て暗号化されているという証明です。

「暗号化をしました、と言う人に対して、弁護士は『それを証明してください』と言います」。IDC のリサーチ担当バイスプレジデント、Charles Kolodgy 氏はそう語ります。暗号化ベンダーは、デバイスのシステム構成を検証して暗号化がどの時点で有効になっているかを示す管理システムの開発に取り組んでいる、と同氏は述べています。

企業は、暗号化が例えば連邦処理標準（FIPS）などに準拠していることを証明できれば、コストや手間を大幅に削減できます。例えば、企業がノートパソコンのハードディスクが暗号化されていることを示すことができれば、侵害が生じたときも、個人情報がリスクにさらされる可能性のある人全員にそのことを通知する必要がありません。そのディスク上のデータは使用できないからです。

「企業はしばしば、データそのものよりも、データが暗号化されていると証明できることに、より関心を持っています」と Holstrom 氏は指摘します。「多くの場合、データそのものはさほど重要ではないのです」。

ノートパソコン上のデータを暗号化する一般的な方法は 2 つあります。ハードディスク上のデータのみを暗号化する方法と、ノートパソコンに接触するすべてのデータを暗号化する方法です。例えば、デルは Wave Systems Corp. と提携し、高速で低コストのさまざまなハードディスク暗号化テクノロジーに取り組んでいます。いわゆる「エンドポイント」デバイスが、デバイスごとにセキュリティを確保するという考え方です。
しかし、誰かがサムドライブをそのノートパソコンに差し込んで、持ち主をリスクにさらす可能性のある情報をダウンロードしたらどうなるでしょうか。それを防ぐためには、モバイルデバイスと接触するすべてのものを暗号化する必要があります。デルは CREDANT Technologies との提携により、サムドライブと、その他モバイルデバイスに接触するすべてのものをハードドライブと同様に効率的に暗号化することに取り組んでいます。

「サムドライブは非常に心配です。ユーザーによっては、サムドライブに転送するデータをすべて暗号化する必要があります」と IDC の Kolodgy 氏は述べています。

暗号化自体は優れた対策ですが、その暗号化機能があると証明できることが必要です。そのため、特にミッドマーケットの企業を対象とするデルのシステム管理アプライアンスである KACE シリーズのようなツールには、モバイルデバイス管理機能が搭載されています。これは重要なテーマであるため、別の機会に取り上げます。
*John Dodge 氏はマサチューセッツを中心*に活動するテクノロジーおよびビジネス

デルが提供する支援

デルは、ハードディスク、およびノートパソコンと通信するあらゆるデータデバイスを暗号化する新しいテクノロジーを2つ用意しています。

デルは CREDANT Technologies との提携により、保護対象のノートパソコンと通信するすべてのデータデバイスを暗号化する機能を提供します。企業はノートパソコン 1 台あたり約 60 ドルで、ソフトウェア暗号化ツールである CREDANT Mobile Guardian Dell Edition を入手できます。
さらに 50 ドルを追加すると、Mobile Guardian Dell Edition にハードウェアアクセラレーターが付属します。

モバイル市場を革新し続けるインテル

インテルがモバイル市場向けに提供するプロセッサーには、以下のような機能があります。

インテル ® Core ™ vPro ™プロセッサー には、高度なセキュリティ、管理、仮想化、およびエネルギー効率を実現するハードウェア支援型の機能が搭載されています。このテクノロジーにより、すべての PC の電源を入れてウイルス対策用パッチをアップデートしたり、OS が機能していない場合でも帯域外（OOB）PC のリモート診断と修復を行うことができます。

インテル ® AES New Instructions（インテル ® AES-NI） は、インテル ® Xeon® プロセッサー 5600 番台、およびインテル ® Core ™ i5 プロセッサー 600 番台に保存されたデータを暗号化します。高速な暗号化と復号化、鍵の生成とマトリックス操作性の向上、およびキャリーなし乗算支援のための 7 つの新しい命令で構成されています。また、暗号化処理につきもののパフォーマンスの課題を緩和することもできます。

インテル ® アンチセフト（AT） テクノロジーは、ノートパソコンのセキュリティを保護します。このセキュリティテクノロジーはノートパソコンのプロセッサーに組み込まれ、マシンの電源が入るとすぐに、起動前でもアクティブになります。ノートパソコンの紛失や盗難が発生した場合は、ローカルまたはリモートの「ポイズンピル」を有効にしてその PC の起動プロセスをブロックし、PC を動作不能の状態にできます。これにより、窃盗犯はシステムの起動時からそのシステムへの不正侵入が不可能になります。インテル AT は、インターネットにアクセスしなくても機能します。また、他の多くのソリューションとは異なりハードウェアベースであるため、改ざんされることがありません。IT 管理者に最大限の柔軟性を提供し、ネットワーク資産の安全なコントロールを可能にします。このテクノロジーはプロセッサーレベルで組み込まれているため、IT 管理者はモバイル資産のセキュリティ保護に役立つ、以下のように多彩なオプションを利用できます。

インテル ® ターボ・ブースト・テクノロジー 2.0 処理性能が向上し、負荷の高い動的なワークロードにも対応できるパフォーマンスの向上を達成できます。ターボ周波数は命令のタイプに応じて調整されるため、消費電力を節約でき、その消費電力と平均アルゴリズムによって電力余剰と耐熱余剰を管理し、最適なパフォーマンスを実現します。

インテル ® ハイパースレッディング（HT）テクノロジー このテクノロジーによって、各プロセッサーコアで同時に 2 つのタスクを実行できます。そのため、より多くのスレッドで効率的なマルチタスク処理が可能になり、パフォーマンスが向上すると共に、応答時間も短縮されるというメリットがあります。

モバイル化を検討する CIO たち

CIO、Lauren Brouseli 著

分野のベテランライターです。連絡先は、jdodge349@gmail.com です。

IT 責任者の 3 分の 2 以上が、モバイルテクノロジーは自社のビジネス革新を促進すると考えています。一方、ビジネス戦略がモバイル関連の投資を推進すると考える人は半数以下です。

CIO が先ごろ 276 人の IT プロフェッショナルを対象にモバイル関連の IT 計画について行った調査では、そのような結果となっています。また、モバイル環境への対応が IT の課題のトップとなり、66 % の企業が、来年の IT 予算でモバイルソリューションへの投資を増やす予定であることを示しています。

何がモバイルテクノロジーへの投資を推進しているのでしょうか。ほとんどの IT 担当者が、生産性の向上（87 %）と顧客に対するサービスとサポートの向上（86 %）を挙げています。リアルタイムの情報の必要性（84 %）も上位に挙がっています。CrossCom National の CIO、Tim Walter 氏はそれを重要と答えた一人です。同社では従業員のモバイル化が進み、従業員は複数のリモートサイトで業務を行うようになっています。「モバイルデバイスから当社のシステムへ接続する機能がますます重要になっています」。

法律事務所、Dechert の CIO である Michael Shannon 氏も、より効率的なビジネス手法を実現する必要があるため、モバイル関連の投資は促進されると述べています。「（モバイルによって）基本的に、より多くのことをより適切でより早く、より強力に行うことができます」と同氏は言います。「モバイルによって弁護士が法律業務を行う方法が変わるわけではありませんが、業務を行うための新しい便利な入口となります」。

IT 担当者が注目しているモバイルソリューションのトップに挙がっているのはデバイス（71 %）、続いてセキュリティおよびデータ管理ソフトウェア（70 %）、アプリケーション（63 %）、ワイヤレスサービス（62 %）となっています。購入の決定要因については、IT 担当者はほぼ全員一致で使いやすさをトップに挙げ、サポート、サービス、信頼性、およびセキュリティがそれに続きます。

一方、懸念事項のトップとなったのは、ROI が測定しにくいこと、およびモバイルネットワークが攻撃に対して脆弱であるという点です。FragranceNet.com の CTO、Barbara Porter 氏は様子見の構えです。

「モバイル分野はまだ形成段階にあり、いずれ、何らかの戦略が他よりも確実であることがはっきりしてくるでしょう」と同氏は述べ

エンドポイントのセキュリティおよび管理ソフトウェアを強化する McAfee

Network World、Ellen Messmer 著

ています。
McAfee は、モバイル化が進んだことで従業員が特定の場所に縛られずにスマートフォンを使用できる環境の中でユーザーを保護することを念頭に開発された、新しいエンドポイントセキュリティおよび管理製品の提供を開始しました。

「仕事とはもはや場所ではなく、行動」であり、その結果、IT インフラストラクチャは「もはや 1 ヶ所ではなくなっている」と McAfee のリスクおよびコンプライアンス担当シニアディレクター、Martin Ward 氏は述べています。

McAfee は、Windows と Apple Macintosh に加えて、Android 搭載のハンドヘルドデバイス、iPhone、Symbian、および Windows Mobile の各種スマートフォンなど、さまざまなプラットフォームをサポートする Endpoint Security 9.0 を発表しました。

「仕事とはもはや場所ではなく、行動です。」

Endpoint Security 9.0 は、マルウェア対策とデータロスからの保護をモバイルデバイス管理と組み合わせたものです。このソフトウェアは McAfee の一元管理コンソールである ePolicy Orchestrator（ePO）を介して管理できます。

また、McAfee では今年 Trust Digital の買収によって取得したエンタープライズモビリティ管理ソフトウェアの統合も第 1 段階を完了し、この管理ソフトウェアは McAfee ePO と連携してデバイスのステータスを記録できるようになっています。
例えば、現在このエンタープライズモビリティ管理ソフトウェアでは、Apple iPhone 4.0 が「脱獄」状態にある場合にそれを通知し、リモートでその iPhone からユーザーの個人情報を残して企業データを消去するという選択的なデータ消去が可能です。

McAfee は来年後半にはさらに ePO との統合を進める計画であり、それによって ePO をエンタープライズモビリティ管理ソフトウェアの主要管理コンソールにする、としています。現時点では、ePO は今年初めの Trust Digital 買収の一環として取得した管理コンソールとの連携で機能しているためです。

さらに McAfee は、仮想デスクトップおよびサーバ環境向けに最適化されたウイルス対策製品を、McAfee for Management of Optimized Virtualized Environments という製品名で提供することも発表しています。

MOVE A/V の略称で呼ばれるこのソフトウェアはハイパーバイザに常駐し、McAfee が開発したテクノロジーを使用して仮想マシンベースのオペレーティングシステムとアプリケーションをスキャンします。MOVE A/V は、Citrix および VMWare をベースとする仮想化ソフトウェアの最新バージョンで動作します。

また、McAfee は今週ラスベガスで顧客とベンダーパートナーを対象とした FOCUS カンファレンスを開催しますが、今年 12 月に Security Management 5.0 という名称で Web サービス API を追加することによって、ePO 管理コンソールの用途を広げていくという取り組みも発表しています。

Security Management 5.0 と新しい Web サービス API の目標は、ベンダーパートナーが「ePO から Security Management 5.0 に情報を取り込めるようにする」ことだと McAfee のエンドポイントセキュリティ向け製品マーケティング担当シニアディレクター、Kevin LeBlanc 氏は述べています。これにより、他社製の管理プラットフォームでも ePO から情報を取得して、そうした環境で情報を活用できるようになります。
モバイル環境の管理に収拾がつかなくなる企業について述べた私の最近のコラムを読んだ方は、おそらく、ワイヤレスおよびモバイル環境に対する自社の取り組みで最大限の成功を収めるにはどうすればよいのだろう、と思っていることでしょう。幸い、Nemertes

モバイル環境管理のための 5 つのヒント

Johna Till Johnson **著**

Research が先ごろ、200 以上の組織の詳細なベンチマークを基に、ワイヤレスおよびモバイル環境への対応で何が機能し、何が機能しないかを詳しく調査しました。相関分析を行って、ワイヤレスおよびモバイル環境に取り組むための明確なベストプラクティスを導き出しました。

その結果は、予想外のものもあれば比較的予想通りのものもあります。ワイヤレスへの成功する取り組みは、以下の点と大きな相関関係があります。

エンタープライズアプリケーションの選択にあたっては、モバイル環境をサポートしていることを重要な選択基準にします。半数以上の企業が、エンタープライズアプリケーションの選択にあたってはモバイル環境のサポートが重要な選択基準であると報告しています。そして、そのような選択をした企業は、成功したと報告することが多いようです。この点を覚えておいてください。後で述べるように、アプリケーションのサポート状況がデバイスの選択も左右するからです。

モバイル環境への取り組みに着手する前に、モバイル環境のリスク評価を行います。これには、データ漏洩の防止（モバイルデバイスの紛失や盗難が生じたら企業データはどうなるか）、デバイス管理、さらにはデバイスの追跡などの人事上の課題（デバイスによって IT 部門が従業員の行動に関する詳しい位置情報を入手できる場合、勤務時間外にもデバイスの携帯を従業員に義務付けることは合法か）などの問題についての検討も含まれます。

モバイル環境に対応するための戦略を策定します。これはいたって明白です。IT 部門は、デバイス、ユーザー、サービス、およびアプリケーションがどのように進化するかを考え、変化するそのニーズに合わせて組織と運用の構造を変えていけるように備える必要があります。前述したリスク評価の実施が、そのような戦略の一部であることは確かです。

企業が支給する iPhone のサポート強化を計画します。これは間違いではありません。モバイル環境への成功する取り組みと、企業が支給する iPhone のサポート強化には、大きな相関関係があります。正確な理由は不明ですが、1 つ考えられることは、アプリケーションフレームワークにモバイルデバイスを統合しようと考える企業は、当然、iPhone の観点から考えるのかもしれない、ということです。

企業が支給する BlackBerry のサポート削減を計画します。これはさらに意外なことですが、BlackBerry のサポート削減を計画することと、モバイル環境への成功する取り組みには相関関係があります。この点についてもはっきりした理由は分かりませんが、BlackBerry のサポートを削減しようとする企業は、それをアプリケーションサポートの強化という目的の一環として行っているのではないかと思われます。

以上の対応すべてに加え、IT 部門は、企業内におけるモバイル環境の役割をどのように考えるか、という明確なビジョンを持つことが重要です。モバイル関連のコストは IT 予算の中で、他の項目が 20 % 以上削減されているにもかかわらず、過去 3 年に渡って一定額が維持されている、または増えています。その理由は、1 つには日常生活の中にモバイルデバイスがますます浸透しつつあり、従業員が自分の生活にそのデバイスを使うことが非常に増えているということがあります。

しかし、もう 1 つの重要な理由は、モバイル環境は適切に管理すれば多くの企業にとって真の市場活性化要因となり、競争上の堅固で持続可能な優位性を企業にもたらすということです。

つまり、 モバイル環境への対応は IT の重要な取り組みであり、そのような取り組みをするだけの価値があるということです。
最近デルが手掛けるコンサルティング契約の大半は、その内容が 1 つのことのみに集中しています。それは、モバイル環境への対応です。これは iPhone/iPad/Android 効果とでも呼ぶべき現象ですが、以下の 2 つの重要な疑問について検討する IT 責任者や経営者が増えています。

モバイル環境に関する批判的思考

• 従業員が所有するデバイスを活用することで、コストを削減する機会はあるのか？

• 新たに登場するモバイルデバイスおよびプラットフォームを活用して、ビジネスプロセスの改善、新しいサービスの提供、あるいは企業の変革を行う方法は？もちろん、単に「私の新しいデバイスをネットワークに接続するのを手伝ってほしい」という問い合わせに対処する方法を見つけることが最大の懸念事項だ、という責任者が多いことは確かです。しかし、より大局的な見方をしている人々は、モバイル環境は混乱をもたらすテクノロジーであると考えています。

こうした 2 つの疑問に加え、可用性 / パフォーマンス / セキュリティ / コンプライアンス / ガバナンス要件にどう対処するか、といった一般的な懸念事項もあります。その結果、企業のモバイルプラットフォームを少数のデバイスやプラットフォームに制限するという長年のポリシーが撤回されることはよくあります。IT 責任者は、業務環境により多くのデバイスを導入するための計画を作成した途端に、モバイル環境の管理とモバイルエンタープライズアプリケーション開発プラットフォーム（MEAP）のスピードに対応する必要性を認識することになります。

効果的なモバイル環境戦略を考案するには、以下の質問に答える必要があります。

• デバイスの所有者は誰ですか？

• 従業員が個人所有のデバイスを持ち込んだ場合、どの機能を許可しますか？

• どのタイプのデバイスを許可しますか？

• どのタイプのデバイスに対応する必要がありますか（例えば、タブレットなど）？

• どのモバイルオペレーティングシステムをサポートする必要がありますか（例えば RIM、Apple、Microsoft、Android など）？

• エンタープライズアプリケーションへのサポートをどのようにサポートしますか？（この場合、通常は HTML5、デスクトップ仮想化、フラッシュについて検討）

• どのようなセキュリティ / ガバナンス要件がありますか？

• モバイルデバイスおよびアプリケーションをどのように管理しますか？

• モバイルデバイスの調達を、自社の全体的な通信戦略にどのように組み込みますか？

多くの場合、最良のアプローチはまず、役割とプロファイル、つまり誰が何を必要としているかを定義することから始めることです。企業が提供「すべき」ものと提供することが「望ましい」ものとを明確にします。ユーザープロファイルを確立してセキュリティ / ガバナンスのニーズを考慮することによって制約が生まれ、それがさらに意思決定を促進します。そして、過去ではなく将来に目を向けることが大切です。「現在」の市場にあるデバイスを網羅した戦略の作成に 6 ヶ月を費やしても、今後数年間に新たに登場する新しいデバイスに対応できる柔軟性が得られることにはなりません。iPad と、現在それに競合するタブレットがもたらす影響を予測していた人はほとんどいませんでした。今後数年の間に、同様の変革をもたらすテクノロジーやデバイスが出現し、企業がリスクと機会を簡単で迅速に評価するための戦略が必要であることは確かです。

つまり、モバイル環境に対する取り組みを成功させるためには、モバイル環境に対する戦略が不可欠であるということです。さらに重要なのは、IT プロフェッショナルたちが、各社の戦略をじっくり考える時間を取るべきだということです。なぜなら、明確で簡単だと思える決断が、実はそうではないことがよくあるからです。

個人所有のモバイルデバイスが増えるにつれて、画一的な指示を撤回する企業が多くなっています。従業員に標準のスマートフォンを使用することを求めるのではなく、従業員が所有する（または「従業員負担の」）デバイスをある程度コントロールすることによって、それらのデバイスを管理しセキュリティを維持するという方法を検討する IT 部門が増えているのです。

可用性、パフォーマンス、セキュリティ、コンプライアンス、ガバナンスの要件に対応するにはどうすればよいですか？

企業ネットワークに接続する従業員の個人所有モバイルデバイスのセキュリティ保護と管理の方法

従業員に iPhone や他のデバイスの使用を認める企業が増えていますが、それは条件付きの許可です。Network World、John Cox 著

ガートナーのバイスプレジデント、Phillip Redman 氏は次のように語ります。「Android や iPhone などのプラットフォームが企業内に浸透してきたことで、社内標準という抑制手段は崩れつつあります。ほとんどの企業はこれらのデバイスを受け入れ、それを管理してセキュリティを維持するためのガイドラインとプロセスを用意することになるでしょう」。

そのためのベストプラクティスとして、「ユーザーをモバイル環境とアプリケーションの要件別に複数のワークスタイルに分類し、それに合わせたデバイスの選択肢を設定する、といった方法があります」と Redmond 氏は述べています。もう 1 つの重要な点は、モバイルデバイス管理プラットフォームまたはサービスを利用して、それらのデバイスの使用、設定、およびセキュリティの管理に役立てることです。

このアプローチは体系的で包括的なものであることが必要だと、シマンテックのモバイルセキュリティグループでグループ製品マネージャを務める Khoi Nguyen 氏は言います。そのときに極めて重要な要素となるのが、全体的なデバイスおよびアプリケーション管理、ポリシーを確実に導入、実施、更新できるセキュリティ機能、および不正アクセスの警告とレポート作成機能です。

詳細はともかく、全体的なプロセスは、「要約すれば、スマートフォンとその他のモバイルデバイスも、他の IT 資産と同様に重要になっているのだから同様に扱う必要があるということを認識した、組織的でポリシーに基づくアプローチです」と、ExtremeLabs の最高経営責任者、Tom Henderson 氏は語ります。

「技術的には、それを妨げるものは何もありません」と述べるのは、Enterprise Mobility Foundation の理事長、Philippe Winthrop 氏です。それよりも、真に問題となるのは企業文化だと同氏は言います。「E メールは企業の知的財産であるという認識を（従業員）一人ひとりが持つ必要があるのです」と同氏は述べています。「そして E メール以外のものについても目を向けてみると、企業にはその情報のセキュリティを維持するすべての権利があります」。
モバイルポリシーを文書で作成し、従業員が自分のデバイスで企業の E メールやその他のデータにアクセスする前に、それを読み、理解して署名することを従業員に求める企業がますます増えています。Winthrop 氏のある隣人が新しい iPhone 4 を購入したところ、勤務先の企業の IT 部門が、同社で義務付けられている安全なメッセージングプラットフォームを App Store からそのデバイスにインストールしたということです。

こうした方法は今後ますます一般的になるだろう、と Winthrop 氏は言います。「従業員と雇用主との間の合意、企業が所有するエージェントを従業員のハンドセットにインストールすること、といった法律上の課題をめぐっては、大いに疑問があります」と、モバイルコンサルタント会社 Farpoint Group の Craig Mathias 氏は述べています。

個人の消費者と従業員という 2 つの役割を持つモバイルデバイスユーザーと、そのユーザーが勤務する企業とのまったく新しい関係は、まだ始まったばかりです。
デルは KACE システム管理製品のアップデートを続け、IT 部門が自社の企業ネットワークに浸透する大量のスマートフォンとタブレットを管理できるよう支援していると、Michael Dell は語っています。

モバイル対応が進むデルの KACE 管理ツール

KACE 製品は将来のバージョンで iPhone、iPad、および Android デバイスに対応

サンフランシスコで行われた KACE カスタマカンファレンスで、Dell は同社が今後も KACE 製品を拡充し、Apple iPhone および iPad に加え、グーグルの Android OS を搭載するタブレットとスマートフォンもサポートしていくと述べました。

「クライアントデバイスやモバイルデバイスにかかわらず、すべてのデバイスを管理できることが非常に重要であり、それはまさに、デルが対応したいと考えている課題です」と Dell は言います。スマートフォンは「基本的に小型のコンピュータ」であり、「多少セキュリティに欠ける」ところがあるため、IT 部門がその管理を支援する必要があるのだと Dell は述べています。

デルは PC を超えて自社のビジネスを拡大するための広範な取り組みの一環として、2 月に KACE を買収しました。以来、KACE に多額の投資をしていると Dell は言います。顧客ベースは 900 ほど増えて約 2,500 になり、アジアと日本に新しいサポートセンターができてサポートスタッフは 3 倍になりました。

「システム管理はデルにとって多額の投資対象となる分野であり、大いに力を入れていく分野です」と Michael Dell は語ります。

KACE は現在、PC とサーバの管理用に 2 つのアプライアンスを提供しています。インベントリおよびパッチ管理用の K1000 と、アプリケーションおよび OS のイメージを展開できる K2000 です。

しかし、現在このアプライアンスではスマートフォンのサポートが限定され、iPhone の基本的な管理機能のみとなっています。今後は KACE 製品で、Android、Windows 7、および Apple の iOS を搭載するスマートフォンとタブレットを管理できるようになる、とデル KACE 部門の製品管理担当バイスプレジデント、Lubos Parobek は述べています。

お客様は、基本的なインベントリ管理の他、デバイスへのソフトウェア展開や、デバイスが盗難にあった場合のデータの消去とロックが可能になると Parobek は言います。また、発表の時期については言及しませんでしたが、K1000 アプライアンスの機能が拡張される予定であると語っています。

デルは多くの企業と競合することになります。Fiberlink、サイベース、LogMeIn はいずれも、コンピュータ向けだけでなく携帯電話向けの管理ツールを提供しています。グーグルは基本的な携帯電話管理サービスを提供し、Good Technology は企業がほとんどのメーカーの携帯電話を管理できるソフトウェアを販売しています。デルはそうした問題を解決しようとする一方で、ある意味ではさらに問題を大きくしているとも言えます。デル自身、スマートフォンを販売しているからです。デルは既に Streak と Venture Pro を発売していますが、さらに先ごろ Michael Dell は自分のポケットからもう 1 つの Android 搭載デバイスを取り出し、これが間もなく正式に発表される製品だと述べました。 このデバイスは 3.5 インチ画面で、インドおよびその他の新興市場で販売するということですが、それ以上の詳細には言及しませんでした。

iPad の同等製品も提供する、と Dell は言います。これは Android の Honeycomb リリースを搭載する 10 インチのデバイスで、来春に発表が予定されています。

Dell は今後発表予定の小規模組織向け「ミニ」KACE アプライアンスも簡単に紹介しました。アプライアンスサーバというより、ミニデスクトップ PC のように見えるこの製品は、管理対象サーバが約 150 台以下の企業向けとなります。

「これは、来年になればもう少し詳しくご紹介できる製品です」。Dell はステージ上で銀色のボックスを示して簡単にそう述べました。「これには非常に使いやすいインターフェイスが搭載されており、小規模な組織でもインベントリおよび資産管理が可能になります」。

Dell は「スーパーディスク」という新しい KACE テクノロジーも簡単に紹介しました。このテクノロジーによって、組織全体の使用されていないディスクスペースをすべて活用できるようになる、と Dell は説明します。しかしそれ以上の詳細や、このテクノロジーが利用可能になる時期については言及しませんでした。

チェックリスト：モバイルデバイスの管理とセキュリティをマスターする方法

IT 責任者たちが、自社内に急増するデスクトップ PC に対処しようとして直面する課題について不満を口にしていたのは、わずか 10 ～ 15 年前のことだったのでしょうか？その責任者たちがもし今、愚かにも当時のことを振り返っているのだとしたら、彼らを許してあげてもよいでしょう。

なぜなら、 そのデスクトップ PC の急増に続き、すぐにモバイルデバイスが浸透するようになったからです。それはノートパソコンに始まり、間もなく、PDA、スマートフォン、タブレット PC、その他のワイヤレス対応製品が雪崩のように世間に浸透して増えました。今や、固定された PC を管理するという課題は、モバイルデバイス、データ、およびネットワークを管理し、セキュリティを維持することの難しさに比べれば、ごく些細なことのように思われます。

そうした企業のモバイル環境に対する戦略と取り組みを調査すると、IT 責任者や経営者は常に、管理とセキュリティの課題が最優先事項であり最大の懸念事項であると考えています （最近 CIO Magazine がモバイル環境への対応について行った調査では、モバイルデバイスがアクセスするネットワークの保護という課題より上位となった課題は、測定が難しい ROI のみでした）。こうした課題をさらに深刻なものにしているのが、従業員が個人のモバイルデバイスを使用して企業のデータとアプリケーションにアクセスするときに生じる、時として無秩序でリスクの高い相互作用です。

プラス面としては、モバイルソリューションによって、売上高の増加、従業員の生産性向上、顧客満足度の向上など、ビジネス上の真のメリットが得られるということがあります。しかしそうしたメリットは、企業がモバイルデバイスと、モバイルワーカーがアクセスできる企業リソースを、十分に管理してセキュリティを維持することができなければ、すぐに価値のないものになってしまいます。

IT 責任者と経営者は、モバイル管理およびセキュリティ戦略を考えるときに、以下の点に対処することによって成功の確率を高めることができます。

可能な場合には、許可されたモバイルデバイスの一覧を作成する前に、また、従業員にモバイルデータおよびモバイルアプリケーションへのアクセスを許可する前に（それがたとえ E メールであっても）、管理とセキュリティのニーズおよび対象を綿密に決めておきます。

早い時期に従業員の教育とトレーニングを行うことをおろそかにしないようにします。モバイル環境のセキュリティの成否は、従業員がユーザー認証、デバイスの紛失や盗難の報告などの適切な手順を知っているかどうか、そしてそれに従うかどうかに大きく左右されるからです。

一部のモバイルデバイスおよびソフトウェアベンダーは、自社独自仕様の管理ソリューションを提供していますが、多くのサードパーティベンダーは、より包括的な管理およびセキュリティソフトウェアおよびサービスを提供しています。導入するモバイル環境管理システムは、企業の既存のシステム管理およびセキュリティアーキテクチャとシームレスに統合できるものであれば理想的です。

従業員のモバイルデバイスとモバイルオペレーティングシステムを 1 種類に制限できない場合、または制限が望ましくない場合であっても、サポート対象システムの種類をできるかぎり抑えるように努めます。現在、市場には主要なモバイルオペレーティングシステムとして BlackBerry、iPhone、Android、Palm、Windows Mobile/7、Symbian の 6 種類があり、それぞれ異なる管理特性と管理機能を提供します。

どのモバイル管理ソリューションも、IT 管理者が、モバイルデバイスへのソフトウェア、アップデート、およびパッチの一元的な展開、そのデバイスに搭載されているソフトウェアのインベントリ、およびユーザー認証とネットワークアクセスアクティビティの追跡を行えるものであることが必要です。ほとんどの企業は、デバイスをリモートでロックまたは無効化する機能、および必要に応じてデバイスのメモリ上のデータを消去する機能が必要です。

最後に、データの自動暗号化などのデバイス固有のセキュリティ方法や、指紋認証リーダーやスマートカードなどの高度なユーザー認証テクノロジーを検討します。