

TRENDS IN ENTERPRISE MOBILITY

SECTION 3: MOBILITY DRIVERS AND STRATEGIES



SECOND ANNUAL • APRIL 2013

セクション3：モビリティのドライバー（推進力）と戦略

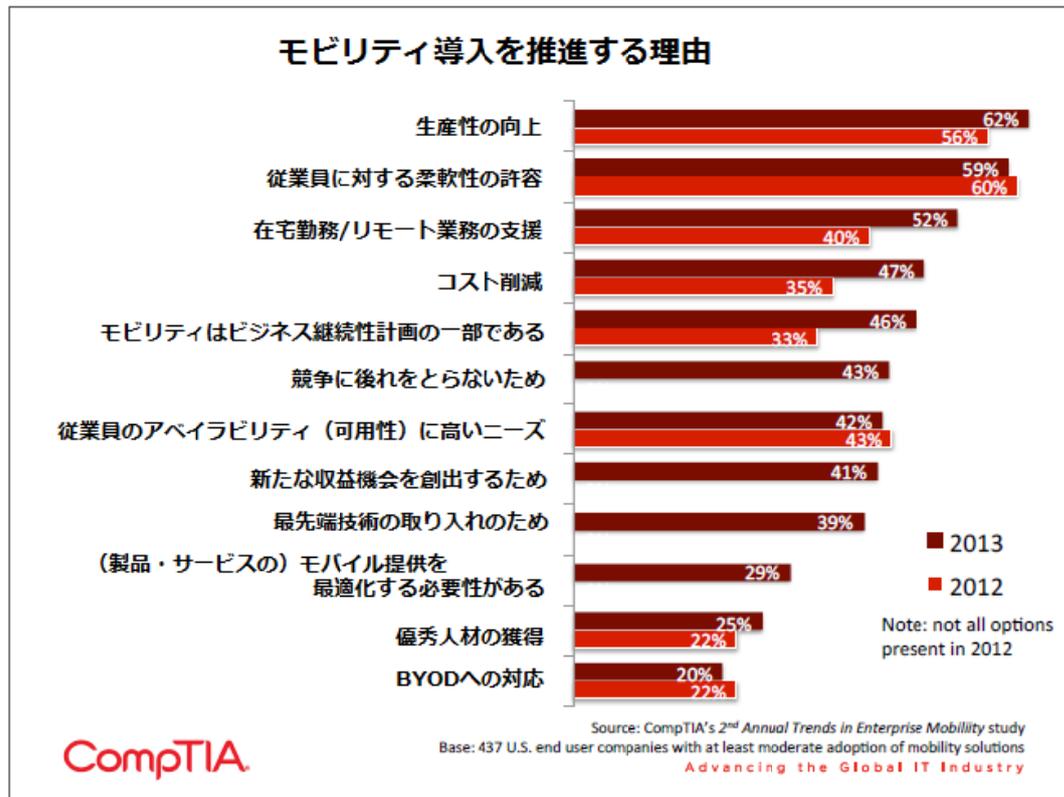
主要所見

- モビリティ導入を推進する理由の上位二つは、エンタープライズでのモビリティが持つ二面性を反映しています。62%が「生産性の向上」、59%が「従業員に対する柔軟性の許容」をドライバーとしてあげています。
- 企業の24%は、正式なモビリティポリシーを所有。これは昨年比わずか2%の上昇です。しかし、ポリシー策定を予定している企業は20%から40%と倍に増加しています。また、ポリシー策定に携わる部門に広がりが見られることから、モバイルプラクティスを全体的視野でみていることがわかります。
- 仮想デスクトップは、モバイル従業員と企業システムをつなぐテクノロジーの代表です。数あるモビリティ問題に対応するための手段として有効とされています。その他にはVPN、ビデオカンファレンス、VoIP等テクノロジーが含まれます。

モビリティのドライバー（推進力）と利点

モバイルソリューションを大きく推進させたのは消費者と言われていますが、ビジネス上の利点がなければ今日のようなエンタープライズでの浸透は困難であったかもしれません。従業員は柔軟な業務形態が可能となり、企業は生産性の向上の一助となることから、見方によればモビリティはWin-winの関係が可能となるのです。

こうした二面性が、モビリティ導入のドライバーとなる理由の上位二つに反映されています。最多理由となった「生産性の向上」は、エンドユーザーのモバイルデバイスやアプリケーションの精通度の高さから、理にかなった結果といえます。また、現時点において、従業員のリモート作業を可能にする積極的なデバイス展開よりも、従業員個人のデバイス使用の対応に徹する企業が多いことから、2番目にあがった理由「従業員に対する柔軟性の許諾」は、便宜的回答であるかもしれません。



「コスト削減」も理由にあがっていますが、セクション 2 にあったように、モビリティもこの分野においてはクラウドコンピューティングと同様の道を行くことでしょう。初期計画では潜在利益を示しますが、見えない費用や予期しないコストが最終的に発生する可能性があります。意図しないコストの例としては、ネットワークのアップグレード、インテグレーションのためのコスト、IT 部門のテクサポートの必要性などがあります。これはモバイルソリューションに利点がないといっているのではなく、クラウドコンピューティング同様、コスト削減という目的外で導入が進められる可能性があることを表します。

「コスト削減」「ビジネス継続性計画として」「リモート業務の支援」といった理由は昨年比より大幅に上がっていることから、企業のモビリティソリューションを導入する理由に多様化がみられます。こうした様々なモビリティオプションがあるからこそ、企業は様々な状況を見据えることが可能となり、最も有効となるシナリオを描くことができるのです。

モバイル人材の創出に関連のない項目は、優先順位が低くなります。また、顧客との直接的なつながりや、モバイルコマースのニーズがある小規模・中規模企業の間では、「新たな収益機会の創出」が推進理由として最多でした。これら企業は、ジオロケーション（地理位置情報）やオムニチャンネルマーケティングのようなモバイルテクノロジーの進んだ利用に期待を寄せています。しかし、こうしたテクノロジーを駆使するためのノウハウを持たない可能性があることから、サードパーティにとってはビジネス機会の一つになり得るでしょう。

モバイル提供の最適化に対するニーズが、新たな収益機会の創出よりも低い位置にあるのが興味深い点です。こうした傾向は、CompTIA が実施したビッグデータに関する調査でもみられ、多くの企業がビッグデータのビジネス機会に期待をしているものの、最大限の活用はできていないという結果に類似しています。収益源として新たなモバイルアプリケーションの活用方法を模索している一方で、第一段階は現在提供している製品やサービスのモバイル化の構築であることがわかります。

実際のところ、彼らの目標は、モビリティ戦略を立てる際にその多くが達成されていることがわかっています。調査参加企業の 68%が「モビリティは生産性向上につながっている」、63%が「モビリティが従業員間のつながり（連絡）を円滑にし、柔軟性を提供している」と回答しています。また半数が、「モバイルソリューションは、顧客エンゲージメントの向上につながっている」とし、34%が「モバイル製品・サービスにより新たな市場セグメントでの機会がうまれた」と報告しています。

モビリティ導入を実施していないと回答した企業はわずか 2%であったように、モビリティは驚くべき普及率をみせています。モビリティの定義は多岐にわたり、多くのモビリティ議論からはそれるものの、ノート PC のみを配置する企業であればモビリティアダプター（導入者）として分類されてしまいます。モビリティを低いレベルで導入していると評価する企業は 11%ですが、彼らが導入の障害として捉えているものはすべて対処可能なものといえます。モビリティに精通する IT 企業の増加により、そうした懸念事項が取り組まれる体制も整えられることでしょう。

モビリティに注力されない要因とは

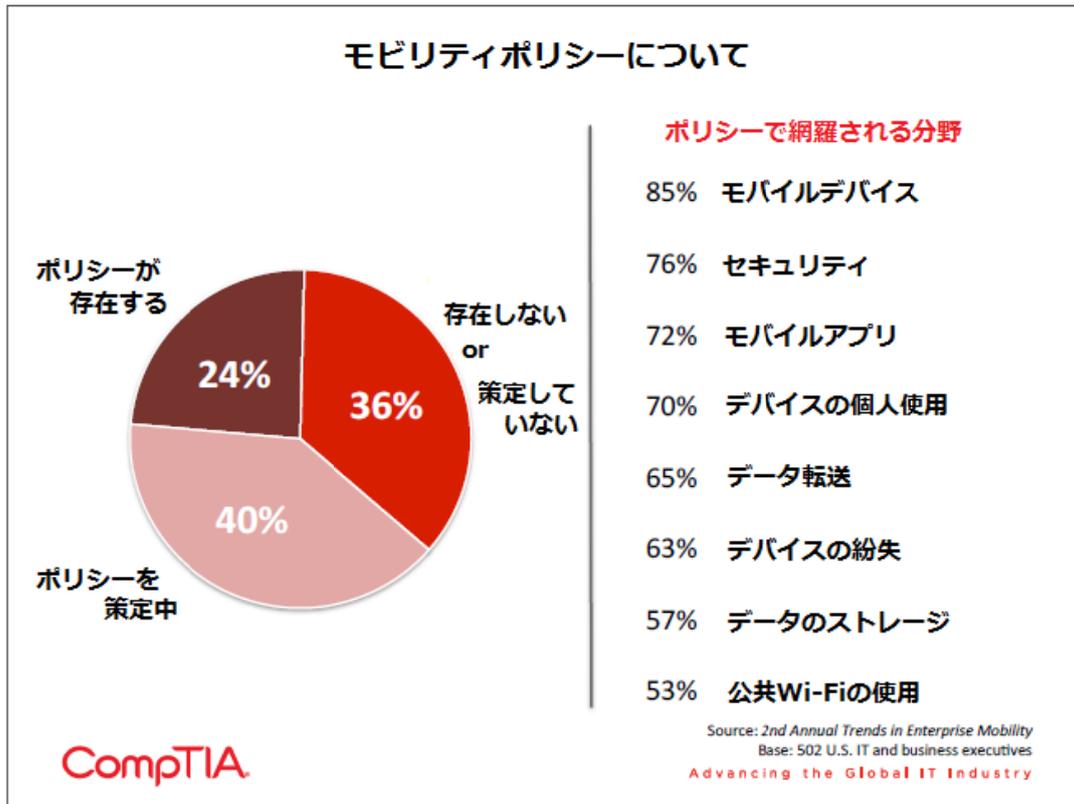
- 43% IT ニーズにおいて最優先事項ではない
- 29% 全従業員がオフィス勤務である
- 23% モビリティイニシアチブをサポートできる十分な IT スタッフが確保できない
- 26% モバイルテクノロジーのセキュリティを懸念している
- 22% モビリティの利点が不透明
- 14% 従業員は個人デバイスを利用しているため、企業が投資する必要性がない

モビリティの基礎を構築する

CompTIA 実施の「第 1 回エンタープライズモビリティのトレンド」調査では、正式なモビリティポリシーを持つ企業は 22%に留まりました。モビリティポリシーは、企業戦略やセキュリティにおいて重要な役割を担うことからこれは意外な結果でした。同調査では、「ポリシーを策定中」と回答した企業が 20%であったことから、上昇の可能性が見えた結果に終わりました。

しかし一年後に実を結ぶことはなく、この度の調査では、正式なモビリティポリシーを持つと回答したのは 24%に留まります。大きな増加をみせたのは、小規模の企業で 7%から 16%のアップです。

モビリティポリシーの策定へ向けた動きは引き続き上向きようです。「ポリシーを策定中」とする企業は、第 1 回目の調査から 2 倍の 40%になります。モビリティ成長が勢いを増し、企業はより積極的なアプローチを実施することから、多くの企業がポリシー策定を遂行することが考えられます。



モビリティポリシーを持つ企業、またポリシー策定中である企業にとっても、注目すべき分野は多く存在します。当然、デバイス、セキュリティ、アプリはその上位に入りますし、それらに関連するポリシーは、企業の知識度合いにより変化して行くものでしょう。例えば、初期のアプリケーションポリシーには、いかなるダウンロードはIT部門からの事前承認が必要という内容の記載があったかもしれませんが、しかし、承認済みアプリを置いたアプリストアが検討されるのであれば一変して、アプリを申請するための新たなプロセスが必要となります。

セキュリティは強い懸念事項ですが、これは多くの場合パスワードの必須化やジェイルブレイキングの禁止などデバイス上のセキュリティを指している可能性があります。企業データの使用や保管といったトピックもセキュリティ議論にあがりますが、データはデバイス固有ではないため異なるアプローチが必要とされます。データは組織のファイアウォールを超え急速に広がることから、IT部門はデータ損失防止（DLP）や他技術を用いてデータを監視し保護するよう努めなければなりません。そしてユーザーには、適切な使用ができるようポリシーに準拠したガイドラインが必要となります。

モビリティポリシー策定に携わるグループに関するデータで、興味深い点があります。昨年と比較したところ、全般的に組織全体での関わりが増加しているという点です。これは企業がモビリティに対し、全体的なアプローチを行っているという表れで、テクノロジーがビジネスのあらゆる側面に深く浸透していることが要因といえるでしょう。ポリシー策定の主な当事者は、ITスタッフ（74%）とITエグゼクティブ（69%）ですが、ビジネスエグゼクティブ（48%）、ビジネススタッフ（43%）、CEO/オーナー（39%）のエンゲージメントも多く見受けられます。

モビリティ戦略における基本ステップの二番目は、ツールの提供です。ツールを通してモバイルワーカーは、企業システムの接続、従業員同士の連絡が可能となります。調査対象となった全てのテクノロジーにおいて、昨年度からの採用増加がみられました。これは、企業から提供される

オフィシャルアプリケーション、また、従業員自身がダウンロード使用しているアドホックアプリケーションの両方にみられた結果です。

モバイル生産性テクノロジー	オフィシャルアプリケーション	アドホックアプリケーション
仮想デスクトップ	47%	22%
VPN	44%	23%
ビデオカンファレンス（会議）	43%	25%
VoIP	40%	24%
コラボレーションプラットフォーム	36%	20%
公共のソーシャルネットワーキングサイト	27%	35%
企業のソーシャルネットワーキングツール	16%	23%

仮想デスクトップが最大の採用増加をみせ、ランクの上位に入

っています。この結果は、仮想デスクトップの採用は依然多くないとされる事例証拠に相違するものですが、様々なデバイス環境下での業務遂行という点において、仮想デスクトップは大いに期待されるものでもあります。今回の調査で示された採用の高さは、モビリティソリューションのアーリーアダプター（初期導入者）とする企業で仮想デスクトップの使用率が非常に高かったことが要因としてあげられます。また、回答者は仮想デスクトップに対してゆるい定義を持っているという点、同カテゴリにおいて仮想サーバーで実行されるフルデスクトップよりもブラウザベースアプリケーションを捉えているという点が考えられます。

ビデオカンファレンス（会議）利用にも大幅な増加が見られます。コミュニケーション改善のため着実に進歩をみせるテクノロジーであり、無料の消費者ツールから、高額なテレプレゼンス導入など、ビデオカンファレンシングは様々な形で存在するテクノロジーです。投資や使い易さを評価するには導入が不十分であったりと、これまでも多くのハードルを経験してきましたが、徐々にそうした障害を解消できるほどテクノロジーは改善しています。今注目されているWebRTCプロトコルが導入の後押しとなるかもしれません。

リスト下部に入るのは、大きなグループ間での情報共有を容易にするためのテクノロジーです。コラボレーションプラットフォームやソーシャルネットワーキングツールの需要は、現在のところ他オプションと比べ低いようですが、これらは企業で利用されるなかで最も若いテクノロジーといえます。企業がこれらテクノロジーのベストプラクティスを確立した際、従業員をつなぐ有効なオプションと成り得るでしょう。

インテグレーションテクノロジーとモビリティが作り出すニーズに大差はありません。企業は常にコミュニケーション向上の必要性に言及していますし、モビリティが提供できるサービスは混在するテクノロジーに重要な要素を付け加えます。すでに企業で使用されているテクノロジーに焦点を置き、新たなモバイルソリューションのテクノロジーに統合することで、IT企業はクライアントのモビリティ戦略にさらなる価値を付加することができます。

TRENDS IN ENTERPRISE MOBILITY

SECTION 4: CHALLENGES IN BUILDING MOBILITY SOLUTIONS



SECOND ANNUAL • APRIL 2013

セクション4：モビリティソリューション実施の課題

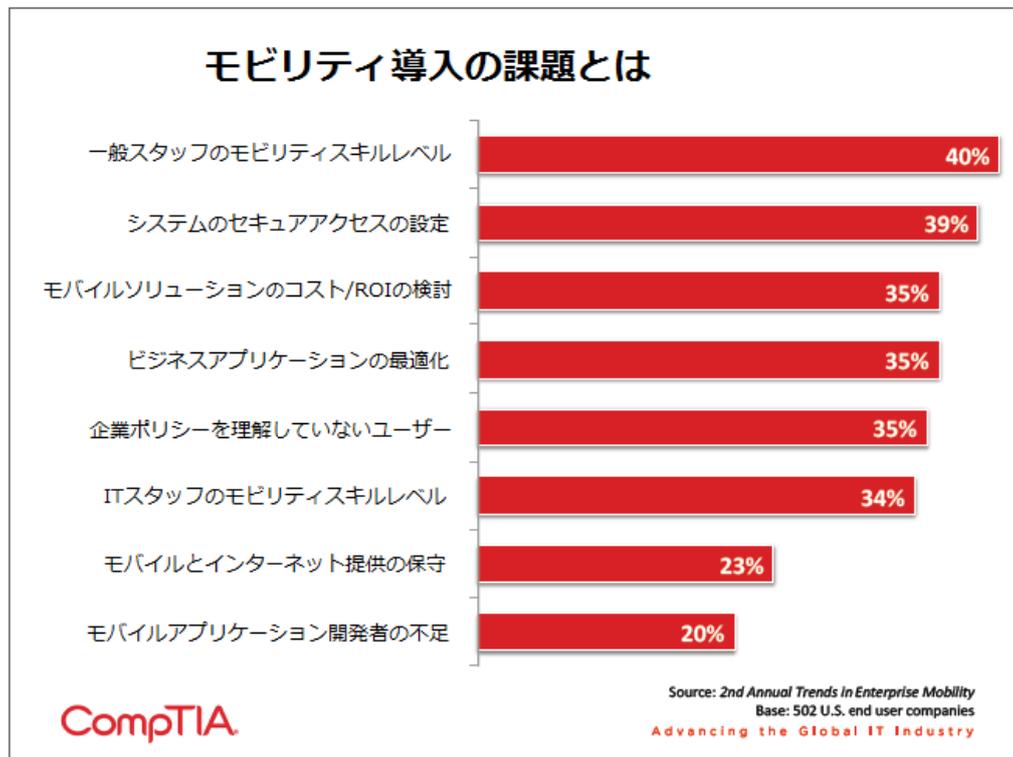
主要所見

- モビリティソリューションを実装する上で、第一の課題事項は、「スタッフのモビリティスキル」であると 40%の企業が報告しています。従業員はプライベートでシステムを使用しているにもかかわらず、全ての機能、特にセキュリティ機能に精通していないと考えられます。次にあがる課題事項は、「システムのセキュアアクセスの設定」と 39%の企業が報告していました。
- 62%の企業が、エンタープライズモビリティをサポートする際の最大リスクを、「モバイルデバイスセキュリティ全般」としています。デバイスの紛失は、最も一般的なモバイルセキュリティインシデントですが、アンドロイドエコシステムにおいては特に、モバイルマルウェアが考慮すべき脅威として上昇しています。
- 企業はモバイルワーカーのサポート体制を確立するも、社内サポートの程度や、技術サポートで使われるツールも考慮される必要があります。最も効率の良いツールは、リモートアクセスですが、これは低いレベルでモバイル導入を実施した際使用されるツールとなります。

モビリティ実装の課題

いかなるテクノロジーであっても、期待された効果が証明されるまで困難が立ちはだかります。インテグレーション、セキュリティ、エンドユーザー教育支援の全ては、新しいテクノロジーが導入された際に直面する共通課題です。

インテグレーションやセキュア化が必要とされるモビリティデバイスは、IT 部門によって調達されるとは限りません。そのため、IT スタッフやソリューションプロバイダーはあらゆるデバイスに精通してなければならず、対応を進める上で最良の方法を見極める必要があります。



しかしながら、エンドユーザーが自身のデバイスを持ちこむことで問題を引き起こしているにもかかわらず、デバイス性能（キャパビリティ）に十分な理解を持たないことが問題を悪化させているという見方もあります。多くのエンドユーザーは、デバイス性能のサブセットを熟知しているものの、それにはセキュリティやデータ暗号化は含まれていないのかもしれませんが。IT 部門がこうした機能を有効にすると、ラーニングカーブは高まる一方で、生産面でのオペレーションに支障も生じることでしょう。Samsung の KNOX テクノロジーや General Dynamics の GD Protected のような BYOD を扱うアドバステクニックは、エンドユーザーの精通といった課題に直面する可能性があります。

二番目の課題「企業システムのセキュアアクセス設定」は、いかなるデバイスやウェブブラウザであってもアクセスできるセキュアなバックエンドを提供するという IT チームの取り組みを示しています。CompTIA の調査「第 10 回情報セキュリティの傾向」では、モビリティは、クラウドコンピューティングやソーシャルネットワーキングと並んで、新しいセキュリティアプローチが必要とされる分野として認識されていました。その課題の一つが、必要となる予算の調達であり、ウイルス対策やファイアウォールに必要な支出を担当するエグゼクティブは、構造的な見直しが必要となります。

こうした見直しは、他の課題にも必要とされます。ビジネスアプリケーションをモバイル用に最適化したり、多様なインターネットサービスに一貫性を維持するという作業は、レガシーアプリケーションを保守するスキルスタッフに容易に対応できることではありません。適切なスキルの投資は、新規雇用であれ、既存スタッフのトレーニングであれ、強固なモバイル戦略を立てる上で重要なステップとなります。

企業が、自社タフのスキルが最も高いと評価する分野は「Wi-Fi ネットワーキング」です。Wi-Fi は、モビリティ以外にも広く導入されていることから納得の結果といえます。モバイルデバイスマネジメント (29%)、モバイルセキュリティ (27%)、モバイルアプリケーション開発 (21%) といった主要分野におけるスキルレベルの高さを感じている企業は 3 分の 1 以下に留まりました。IT ワーカーはスキルレベルに肯定的な見方をしている傾向があることから、企業との間にギャップが存在することがうかがえます。

提供されているモビリティトレーニングの種類

- 45% ポリシーの見直しや、新しいトピックを扱う継続的なトレーニングセッション
- 32% オンライントレーニングモジュール
- 28% モビリティポリシーやプラクティスを扱うワンタイムトレーニングセッション
- 19% イントラ上でモビリティポリシーに関する指示書
- 25% 公式トレーニングは提供していない

モバイルセキュリティ

多くの組織は、セキュリティを IT の最優先事項として捉えています。IT 予算やプロジェクトがセキュリティに多く投資されるというわけではありません。セキュア環境構築のため、過去に取られた措置を適用している企業も少なくないでしょう。モビリティは、そうした思い込みに対し根本的な疑問を投げかけます。IT チームは、デバイス選択とアプリケーション使用に関してわずかながら制御を失っているようですが、企業資産をセキュアに保つことという任務において責任を持つ当事者として見なされています。

企業の 62% が、エンタープライズモビリティをサポートする際の最大リスクはセキュリティであると回答しています。そして回答者の半数近くが、セキュリティ分野に入る「モバイルデバイスの紛失」をリスクとしてあげています。その次に、38% の企業がコンプライアンス問題をあげています。

企業にとって重大な問題となるモバイルセキュリティ

モバイルセキュリティを「重大なリスク」とすると回答

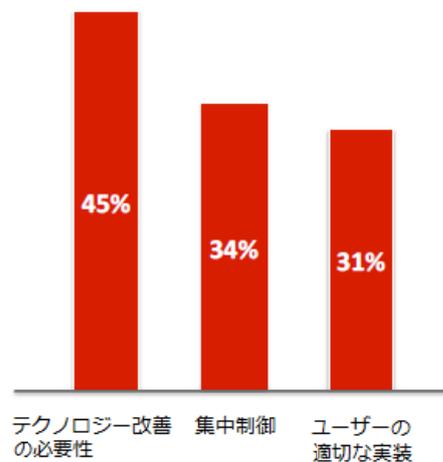
職務ファンクション別

- 65% 業務機能 (ビジネスファンクション)
- 64% IT 機能 (IT ファンクション)
- 54% エグゼクティブ

企業サイズ別

- 71% 大規模企業
- 62% 中規模企業
- 55% 小規模企業

モバイルセキュリティ問題の上位



業務機能（ビジネスファンクション）にいる回答者が、モバイルセキュリティを高いリスクとしていることは好ましいサインといえるでしょう。彼らは、IT 機能（IT ファンクション）によるセキュリティ管理を期待しているかもしれませんが、特定のセキュリティ対策を容認する準備がある表れでしょう。企業サイズ別のデータに関しては、企業規模に応じ多くの資産を持つ傾向があることから、当然の結果といえるでしょう。しかし、最近のセキュリティ調査によると、サイバー攻撃は、防御が弱いとみなされる小規模の企業も標的としていることが分かっています。サイバー犯罪者は、いかなる種類の情報を収益化する方法を見つけるため、すべての企業は自社のデジタルセキュリティについて真剣に取り組む必要があります。

CompTIA の第 1 回のモビリティ調査では、「テクノロジー改善の必要性」がモビリティセキュリティを実装する際の課題として上位にあがりました。第 1 回目目の数字（33%）からさらに上昇していることから、利用できるテクノロジーは市場ニーズを満たしていないことがわかります。従業員のモバイルソリューションのスキルレベルを考慮しても、テクノロジーは複雑であるため運営が難航するでしょう。セキュリティプロフェッショナルは、生産性を妨げることなく集中制御やデバイスマネジメントが与えられるようなオプションを必要としています。

現時点においてモバイルセキュリティに対する注力は、セキュリティ領域においてさほど高くはありません。モバイルデバイスを巻き込む大規模な企業セキュリティインシデントは発生していないことが分かっています。本調査がこれを反映しています。最も一般的なモバイルセキュリティインシデントはデバイスの紛失（49%）で、次に企業ポリシーの違反（28%）が続きます。モバイルマルウェアを経験しているのは 24%に留まりました。また、31%の企業がいかなる種類のモバイルセキュリティインシデントを経験していないと回答しています。

モバイルデバイスに関わるセキュリティインシデントが発生した場合に取られるアクションは二つあります。一つは、パスワード設定の要請です。ユーザーには不便とされるも、作業目的でデバイスにログインするという慣習は確立されている上に、セキュリティレイヤーを追加する簡単な方法といえます。二つ目は、デバイス紛失に関する手順の確立です。これは、モビリティポリシーには至らないものの、まん延する多種インシデントが取り扱われている必要があります。その他のアクションには、モバイルデバイスの暗号化、追跡/ワイピングができるソフトウェアのインストール、モバイルポリシーに関するトレーニングの実施などがあります。

アンドロイド/iOS マルウェア

現時点でモバイルマルウェアを経験している企業は多くないものの、モバイルプラットフォームが攻撃対象となることから、消費者市場において深刻な問題となりつつあります。f-Secure の 2012 年 Q4 モバイル脅威報告書によると、モバイル脅威とされる数は変異したものもあわせ、2010 年の 80 から 2012 年には 301 に増加しています。

問題はアンドロイド市場で広くまん延しています。f-Secure では、アンドロイド市場シェアを 69%としていて、アンドロイドアプリのオープンなエコシステムが攻撃を招く要因としています。アンドロイドプラットフォームは、2012 年の脅威件数の 79%を占め、Q4 だけを見ても、変異したものも含め脅威数は 96 であったと報告しています。

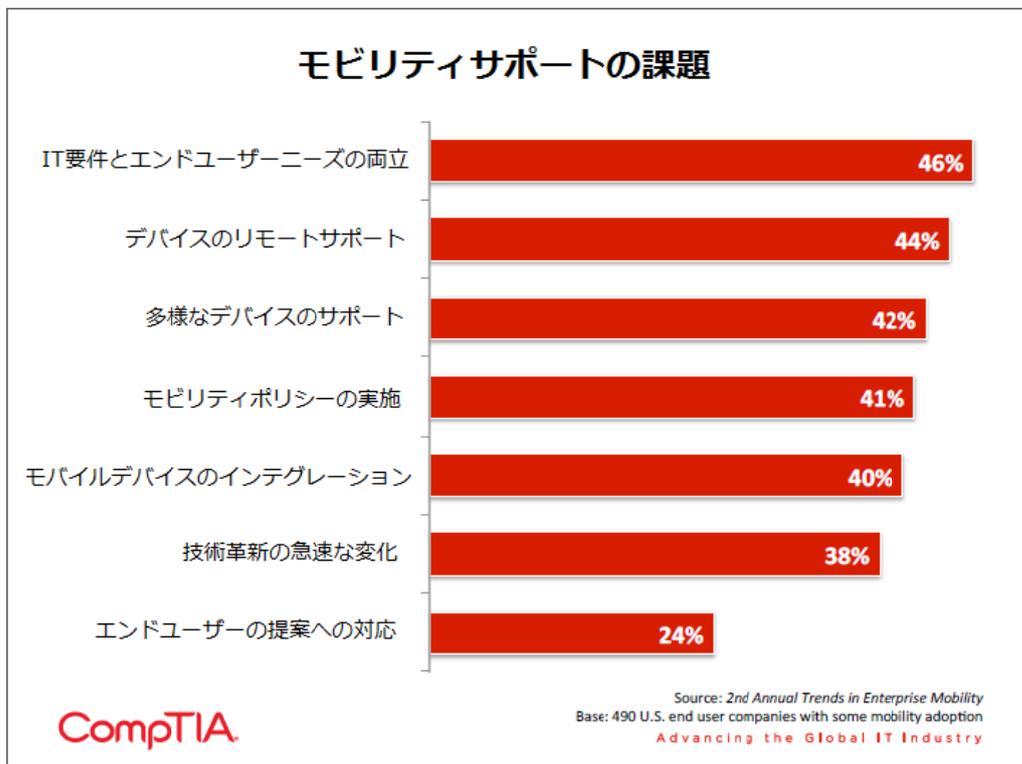
一方で iOS マルウェアは、閉鎖されたエコシステムであることから数が少なく、2012 年の脅威数で占める割合はわずか 0.7%でした。iOS に見られる脅威の大半は、特定の OS を標的にしたのではなく、複数のプラットフォームを標的にしたものであることが分かっています。

モバイルマルウェアは、SMS メッセージを送信するもの、個人情報を盗むためトロージャンとなるものなど様々な形式をとります。セキュリティプロフェッショナルの課題は、これら脅威からの保護を行うと同時に、エンドユーザーの教育です。エンドユーザーは私用のシステムに高いレベルで信頼を置く傾向がある上に、必ずしも脅威を認識しているとは限りません。

モビリティサポート

IT サポートは、企業でモビリティについて議論される際に中心となるトピックのひとつです。BYOD 戦略を検討している多くの企業は、決定プロセスを盛り込むケースがあります。ユーザーは、自身のデバイスにおける選択肢を得ると同時に、メンテナンスやサポートにおいて責任を担うことから、IT チームは他業務に専念することが可能となります。しかし、このようなプロセスは、社内 IT サポートからユーザーを切り離すことから、組織によっては困難かつ非生産的と捉えるかもしれません。

このセッションで述べてきたように、エンドユーザーのニーズと IT 要件の両立は、重要な業務です。これはエンドユーザーにサポート責任を移行するのは賢明でないとされる理由の一つです。



デバイスのリモートサポートは常にある課題ですが、今日の環境下でさらに拡大している問題となっています。ラップトップの登場からリモートサポートが必須となりましたが、デバイスに許可されたオプションは制限されたものであったため、企業イメージを保持することが容易でした。しかし多種多様なモバイルデバイスでは、使用される OS やアプリケーションの制御には制限があることから、リモートで問題解決にあたり解決策を提供することはより困難となりました。

昨年の調査結果と同様に、「リモートアクセスの使用」がサポートを提供する上で最も有効なツールとして考えられていますが、導入率は高くはありません。多くの企業はいまだ電話、email、オンラインヘルプデスクといった従来のサポート体制に依存しています。スマートホンやタブレットへのリモートアクセスを可能にするソリューションなどは、モバイルデバイスの使用による生産性向上を目指す企業が投資を検討する分野の一つといえるでしょう。