2013.1.4

情報セキュリティニュース ＜2012 No.4＞

2012 年に登場したスマートデバイスに伴う情報セキュリティのあり方の変化について

1. はじめに

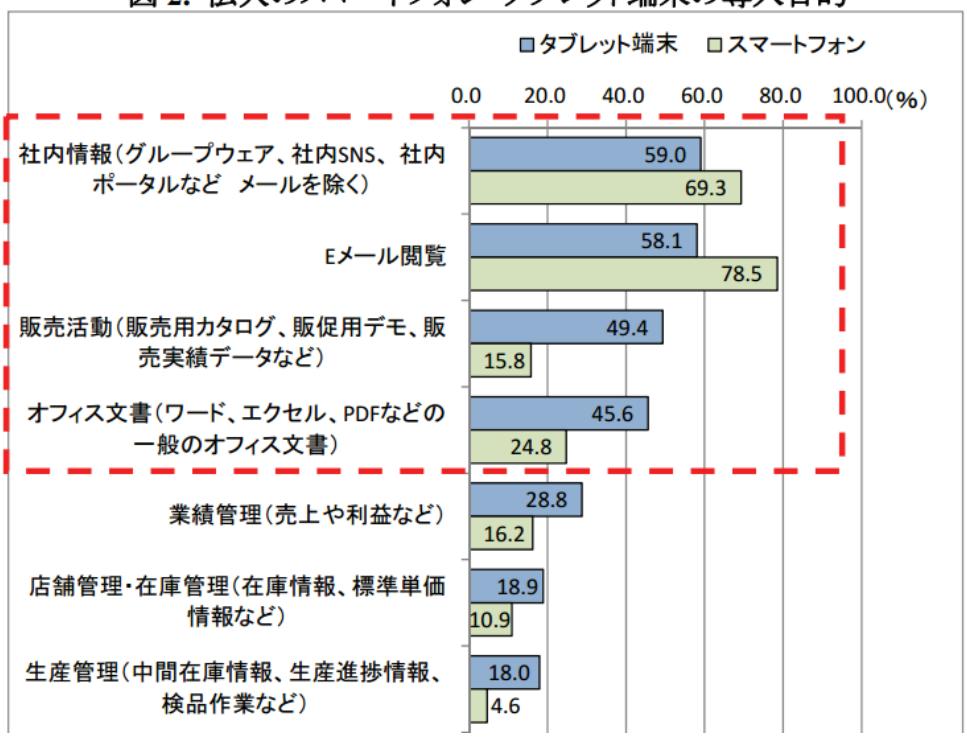
2012 年、これまで 10 インチ前後が主流であったタブレット市場に、Nexus 7、iPad mini、Kindle Fire と、7 インチ前後の小型軽量タブレットが立て続けに投入され、タブレット市場が急速に広がり始めた。一方、スマートフォンでは Android 端末の多くが 4 インチを超える画面サイズで展開されて、iPhone も iPhone 5 でいよいよ 4 インチへと画面を拡大、スマートフォンの画面サイズはおおむね 4 インチ以上がトレンドとなり、こちらは大画面化が進んできた。タブレットは 7 インチ台、スマートフォンは 4 インチ台がボリュームゾーンとして定着しつつある。

本稿では 2012 年に見られたこのようなスマートデバイス(スマートフォン・タブレットの総称)の変化により個人が持つ端末がスマートデバイスへ急速に変わっていく中で、企業はどのように振る舞い、取り扱うべきかを考察する。

2. 従来のスマートデバイスの利用用途

矢野経済研究所の調査によれば、スマートデバイスを導入した企業の導入目的のほとんどが「閲覧用途」であった。

図 2. 法人のスマートフォン・タブレット端末の導入目的



出典: スマートデバイスに関する法人アンケート調査結果 2012 (矢野経済研究所)

この調査結果からみると、スマートデバイスの導入企業においても、現状では、文書作成や業務管理、生産管理などの業務上の主要なツールとしては、依然としてパソコンが主力であり、スマートデバイスは主として情報の閲覧に利用している状況であると推察される。

3. 2013 年に予想される、スマートデバイス活用方法の変化

では、2012 年にみられたスマートデバイスの急速な進展に伴って、今後の企業におけるスマートデバイスの活用方法はどのように変化していくであろうか。

3.1. 主要業務上での活用

2012 年のスマートデバイス端末の急速な進展に伴って、既に店舗管理などで活用を始めている企業や、外出の多い社員向けの業務用端末として活用を始める企業もみられるようになってきている。また、災害時や停電等の際に、建物内の社内 LAN 回線などが使用できなくなった場合のバックアップのツールとして、緊急対策本部要員や優先復旧業務要員などに配布している企業もある。こうした閲覧目的にとどまらないスマートデバイスの業務上の活用は、今後、スマートデバイスが更に一般化し、普及するにつれて、急速に広がっていくものと予想される。

他方で、既に導入済みのパソコンに加えて、こうしたスマートデバイスを新たに導入し、配布していくには、相当のコストが必要となる。また、次々に登場する新たな商品の変化に企業全体として統一的な導入に踏み切ることができないという企業も多い。こうした場合に注目されるキーワードが BYOD である。

3.2. BYOD

BYOD とは、社員が個人所有の端末を持ち込み業務に活用することを指す、”Bring Your Own Device”の頭文字を取ったものである。BYOD はスマートフォン、クラウドサービスの普及や端末の高性能化等を契機として海外から広がり、昨年の東日本大震災以降、日本でも注目されつつある。

現在、多くの企業では業務端末を自社で用意し社員に貸与することを基本としているが、そうした企業でも、携帯電話については一部を除き私物の携帯電話を利用させていることも多い。この場合、私物の携帯電話を業務利用させているわけであるから、既に BYOD を導入しているということもできる。

スマートデバイスの普及に伴い、従業員が利用する端末もスマートフォンに置き換わる。スマートフォンは画面が大きく、端末の性能や処理能力が高い。言わば「電話アプリが搭載された小型パソコン」である。つまり「社員所有の携帯電話の業務利用」が、「社員所有の小型パソコンの業務利用」に変化したと言える。

スマートデバイスはクラウドサービスと連携でき、通信機能搭載のものであれば場所の制約も大幅に緩和されることから、スケジュール管理や、簡単な文書作成などの業務効率向上のために、個人所有のスマートデバイスを紙の手帳やノートの代わりに業務利用するようになる。すなわち、従前組織が想定していた個人携帯電話の用途と、実際の現場でのその用途とが乖離する状況がある。

こうした流れに対し、組織は従来、規制して対応しようとすることが多かった。しかし実際の運用ニーズを考慮せずに厳しいセキュリティルールを導入している組織ほど、ルールを逸脱した利用欲求が高まり、かえってリスクが隠されてしまう傾向にある。むしろ個人のスマート

デバイス利用は一定程度行われるものだと認識し、あるいは、一歩進んで、会社から貸与しなくとも活用できるリソースの 1 つと認識して、BYOD を前提とした情報セキュリティ環境を作ることをお勧めしたい。

3.3. BYOD のリスクとその対応

BYOD のリスクは多種多様に及ぶが、最も大きなものとしては、社員のプライベート情報と業務情報が 1 台の端末に混在することであり、これへの対応が急務となる。

BYOD におけるリスクに対し、携帯電話事業者や機器メーカー、IT ベンダーなど 100 社以上が参加する「日本スマートフォンセキュリティフォーラム」が 2011 年 12 月に「スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン」を公表した。この中でスマートフォン等の利用シーンごとに脅威とその対策を示している。この主なポイントは下表の通りである。

利用シーン	脅威	リスク	対策例
アドレス帳の利用	プライベートデータの消去	漏洩事故発生時の強制消去対象にプライベートデータが含まれる	・誓約書で了解を取る ・プライベートデータと業務データとの保存場所を分けるなど、データを区分する
メール	プライベートメールの混在	漏洩事故発生時の強制消去対象にプライベートデータが含まれる	・誓約書で了解を取る ・プライベートデータと業務データとの保存場所を分けるなど、データを区分する
スケジュール	誤操作・知識不足	情報の公開範囲を誤って指定した結果、クラウドのスケジュールと同期されるなどにより、意図せず情報が広く公開されてしまう	・手順書の作成 ・教育などにより、アプリケーションの動作を理解させる
アプリケーションの利用	マルウェア	悪意のあるアプリケーションにより、不正に利用される。	・信頼できるマーケットを組織が提示し、そこからのみアプリケーションを入手する。 ・組織で許可するアプリケーションを決める。
カメラ		利用を制限されたエリアでの利用、持ち込みによって、取引先等のセキュリティルールの如何、不正な情報の漏洩に繋がる。	・手順書の作成 ・教育による啓発
マイク	知識不足	利用を制限されたエリアでの利用、持ち込みによって、取引先等のセキュリティルールの如何、不正な情報の漏洩に繋がる。	・手順書の作成 ・教育による啓発

利用シーン	脅威	リスク	対策例
位置情報	マルウェア	アプリケーションがスマートフォンの位置情報を収集し、意図しないタイミングで利用される	・アプリケーションのインストール時、利用時に不用意に位置情報の利用に関するアクセス許可をしないよう教育する
データ可搬媒体として利用	盗難・紛失	盗難や紛失により、持ち出し字に保存されたデータの消失及び情報漏洩が発生する(PC等と比較して携帯性が高いため頻度が高くなる)	・スマートフォンのデータ可搬媒体利用を禁止する ・データ領域を暗号化する
PC やクラウドサービスへのバックアップ	バックアップデータにおける業務データの混在	バックアップ先の私物 PC から業務データを含むバックアップデータが流出する恐れがある	・バックアップデータを暗号化する ・私的な保存場所でのバックアップデータのアクセス権限を絞り込む

4. おわりに

BYOD は普段使い慣れたデバイスを業務に利用できることから、従業員満足や生産性の向上などに繋がることが期待されている。

また、企業としても運用面の工夫は必要なもののコスト面でのメリットも決して小さくない。企業は適切なリスクマネジメントを通じて BYOD を上手に取り入れ、企業価値の向上に繋げていくことが今後は大事になっていくであろう。

参考文献

1. スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン
   （日本スマートフォンセキュリティフォーラム）
   http://www.jssec.org/dl/guidelines2011_v1.0.pdf
2. スマートデバイスに関する法人アンケート調査結果 2012 (矢野経済研究所)
   http://www.yano.co.jp/press/press.php/001029

以上

インターリスク総研 コンサルティング第二部　BCM 第一グループ
主任コンサルタント 頼永　忍

株式会社インターリスク総研は、ＭＳ＆ＡＤインシュアランスグループに属する、リスクマネジメントについての調査研究およびコンサルティングに関する専門会社です。
弊社では情報セキュリティに関するコンサルティング・セミナー等を実施しております。
コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問い合わせ先、または、 あいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
㈱インターリスク総研 コンサルティング第二部
TEL.03-5296-8918　　http://www.irric.co.jp/

本誌は、マスコミ報道など公開されている情報に基づいて作成しております。
また、本誌は、読者の方々が企業の情報セキュリティへの取り組みを推進する際に、役立てていただくことを目的としたものであり、事案そのものに対する批評その他を意図しているものではありません。