気になる！技術・サービス

広がるBYOD（Bring Your Own Device）の課題とは

1．BYODの語源

BYODとは、従業員が個人所有のスマートフォンやタブレットPCなどの携帯用機器を職場に持ち込み、それらを業務に使用することを言います。

その語源は、もともとは海外のレストランで酒の持ち込みを許可するという意味の“Bring Your Own”から来ています。レストランで酒類を提供するにはライセンス料（酒類販売許可）が必要ですが、中小のレストランにとってはこのライセンス料が高額なためこれを取得せず、客が自分のワインやビールを勝手に持ち込むことを許可する場合があり、これを、BYOB（Bring Your Own Bottle）と言う場合があります。

2．BYODの普及状況

BYODは世界的に見て普及が進んでいますが、米VMware社の調査によると、その普及率は日本では22%（2012年１～２月の調査結果）となっています。一方、トレンドマイクロ社の調査（2012年６月）によると、日本では約50%の従業員がBYODを利用しているが、BYODを認めている企業が13%に対し、BYODを禁止している企業が29%となっており、会社が禁止しているのにも関わらず従業員が個人機器を勝手に業務に利用している場合が多数あることが推測されています。

また、諸外国では、米VMware社の調査によると、韓国が96%、中国が94%と日本と比べて極めて高い。また、アルバネットワーク社の調査によると、ヨーロッパでは約５～７割の企業がBYODを容認しています。

3．BYODの課題

管理されていないスマートフォンやタブレットPCなどの携帯用機器を会社のネットワークに接続した後に、これらの携帯用機器を紛失した場合、会社の機密情報や個人情報の漏えいにつながる恐れがあります。企業はこのようなことを防止するため、従業員が個人機器を業務に使う場合は、事前に会社が指定する、遠隔操作可能な情報漏えい防止用のMDM（Mobile Device Management）ソフトウェアを個人機器にインストールする必要があります。

個人機器との接続は、有線接続の可能性もありますが、基本的には無線接続と考えられ、無線アクセス部分からの情報漏えいを防止するため、WPA2-Enterprise相当のセキュリティを確保する必要があります。

企業内においては、BYOD実施時のセキュリティ確保のため、無線LANを中心に企業内ネットワークを見直す必要があります。

無線LANアクセスポイント（以下AP）は、AP単体で動作する自立型APと、複数のAPを一元管理するコントローラ型APの２種類があります。BYODに移行する場合は、最終的には全拠点、全フロアにAPを設置することになるため、コントローラ型APにより集中管理することが望ましいといえます。

4．BYODの導入プロセス

BYODの導入は、次の４つのプロセスにより移行すると考えられます。

（1） BYOD禁止（現状）
（2） BYOD一部許可（社内システムを限定し、特定の機器に対して解禁）
（3） BYOD許可（閲覧制限付であるが、全ロケーション、全社員への解禁）
（4） BYOD化（フルアクセス）

日本では、多くの企業が（１）BYOD禁止または（２）BYOD一部許可の状況と考えられますが、個人へのスマートフォンの急激な普及、従業員の労働生産性向上、会社貸与端末のコスト削減等の観点から、（３）BYOD許可を経て、いずれは（４）BYOD化に至ると考えられています。

5．IBMにおける導入事例

米IBMは、2010年からBYODを導入していますが、MIT Technology Review誌（2012年５月21日）は、「IBMがBYODの危機に直面」と題して、IBMの最高情報責任者（CIO）ジャネット・ホランへのインタビュー記事を掲載しています。彼女は、Brian Bergstein記者のインタビューに対して次のように述べています。

「IBMは、従業員に個人の電話やタブレットPCを業務に利用することを推進しているが、その結果、オープンなWeb環境からの安全でないアプリケーションの洪水に直面した。IBMにおいては、2010年にBYODポリシーを採択し、オフィス外で働く従業員がIBMから貸与したスマートフォン以外を利用しても良いことにした。結果的に、全世界40万人の従業員のうち４万人がIBMの貸与したブラックベリーを未だに利用しているが、一方、８万人の従業員が自身で購入したスマートフォンやタブレットPCを利用してIBMの内部ネットワークに接続している。このような状況下において、従業員はどのアプリケーションを利用して良いのか、また、どのアプリケーションは利用していけないかのガイドラインを策定した。利用してはいけないものの一つは、Dropboxのような公衆ファイル転送サービスである。このようなサービスの利用は、会社の機密情報を失うこととなる。また、アップル社のiCloudも同様の危険がある。さらに、音声認識サービスのSiriは、質問内容がアップル社のサーバに蓄積され、重要情報の漏えいにつながる。」

6．最後に

BYODの導入にあたっては、どの企業もIBMがとおって来た課題を経験した後、最終的にはBYODを使いこなして行くものと考えられます。IBMのように利用制限するアプリケーションを指定する場合と、それとは逆に利用すべきアプリケーションを会社が指定する方法が考えられます。いずれにせよ、BYODのメリット、デメリットを十分に理解したうえ、セキュリティの確保やガイドラインの策定が必要となります。