「BYOD」による業務効率化に落とし穴、企業が考えるべきセキュリティー対策とは

～業務を踏まえたセキュリティーポリシー、それを実現するための技術を選定～

今やビジネスツールとして市民権を得たスマートフォン。従業員が個人で所有するスマートフォンをビジネスで使う「BYOD」も珍しくはありません。しかし適切に管理せず、重要な機密情報や顧客情報などを、各々が勝手に個人所有のスマートフォンに保存していたのではいつ事故が起こるかわかりません。スマートフォンをビジネスに活用するのに、企業が検討するべきセキュリティー対策とは、どのようなものでしょうか。

半数を超える企業はスマートフォンをビジネスに活用

スマートフォンやタブレット型端末などモバイルデバイスの普及にともない、個人所有の端末を業務でも使用するいわゆる「BYOD（Bring Your Own Device）」が注目されるようになりました。業務用の端末を従業員に配布するやり方に比べ、端末導入のコストや通信費などを抑えられるという大きなメリットがあります。

では、実際に、BYOD を許可している企業はどのくらいの割合でしょうか。

日本スマートフォンセキュリティ協会（JSSEC）では、2014 年 1 月に企業のスマートフォン利用実態調査を実施しました。企業に勤務し、一般従業員としてスマートフォンを利用する 220 人にアンケートを行ったところ、BYOD が許可されていると答えたのは半数を超える 57.8%。また 54.7%が、端末に業務情報を「保存している」と回答しています。これらは 2 年前の調査結果ですから、現在はさらに進んでいると推測されます。

BYOD には業務の効率化やコスト抑制という利点がある一方、やはり懸念されるのはセキュリティーリスクです。JSSEC の調査でも、BYOD において懸念される点として、約 6 割が「機密情報漏えい」「個人情報流出」を挙げています。

また個人所有の端末は、セキュリティー対策も個人に委ねられるため、甘くなる傾向があります。情報処理推進機構（IPA）による「2015 年度セキュリティーに対する意識調査」では、所有するスマートデバイスのセキュリティー対策について聞いていますが、「画面ロック機能を設定している」「セキュリティーソフトを導入している」はいずれも 2 割前後に過ぎません。

BYOD の抱えるリスク

このように、情報資産の徹底管理が求められる企業にとって、BYOD は諸刃の剣ともいえます。ではコストメリットをあきらめ、単純に「持ち込み端末を禁止」すれば安全といえるのでしょうか。

勝手に従業員がBYODを始めたら、セキュリティーは従業員任せに

実は、BYOD を完全に禁止すれば安心かというと、そうともいえないのです。禁止したとしても、管理者の目の届かないところで勝手に私物の端末を業務利用する「シャドウ IT」が行われてしまうかもしれません。

なかには、会社から業務用端末としてスマートフォンを支給されていても、従業員が「会社の端末よりも、自分用に購入した端末のほうが性能もよく、使いやすい」と勝手に個人端末を持ち込んでいるケースもあります。

企業側のコントロールが利かないところで BYOD が進めば、端末のセキュリティー対策は、従業員任せになり、セキュリティーのリスクも高まります。いざ問題が判明したら一大事です。

「BYOD」で求められる、業務の利便性を損ねないセキュリティーポリシー

「シャドウ IT」などを含め、BYOD のリスクについて取り上げてきました。こうした問題へ企業はどのように対応すべきでしょうか。

それは企業が主導しつつ、BYOD 環境を導入することです。企業側、従業員側が納得し、持ち込んだ私用端末を積極的に活用していくのであれば、双方にメリットがあります。

「BYOD」による業務効率化に落とし穴、企業が考えるべきセキュリティー対策とは

まず考えねばならないのが、セキュリティーポリシーです。企業にとって効果的で統制や管理がしやすく、なおかつ従業員にとって業務上の利便性を損なわないポリシーを策定するには、工夫が必要です。ここでは、チェックすべき主な項目について簡単に紹介します。

業務データの保存を私物の端末に保存を許可する BYOD ともなれば、紛失や盗難による内部データの流出が懸念されます。これを防ぐには、リモートワイプ機能（リモートで端末内のデータを削除する機能）の導入をポリシーに定めておきます。

とはいえ、端末全体のデータを削除するとなると、従業員から不満が出る可能性もあります。その場合、同一端末上で業務領域とプライベートな領域を分離し、業務データのみリモートから削除できるソリューションなどを活用すれば、従業員の不満も取り除くことができます。

その他、SD メモリーカードなどの外部ストレージやカメラ機能の制限、社内へのアクセス時は通信の暗号化を義務付ける、公衆 Wi-Fi は利用しない、セキュリティー対策ソフトを導入するなど、端末の所有者である従業員の事情も踏まえた上で、ポリシーを策定します。

なお JSSEC では、BYOD 導入時に留意すべき点について解説した「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」を公開しています。またコンピュータソフトウェア協会（CSAJ）では、「『BYOD』導入検討企業向けに私有スマートデバイス取扱規程及びスマートデバイス・セキュリティポリシーサンプル」を公開しています。現場の意見に耳を傾けつつ、自社の環境に合ったポリシーを策定するには、これらのサンプルが参考になります。

セキュリティーポリシーで検討するべきポイント

- ☐ セキュリティーソフトの使用
- ☐ リモートロック、ワイプ
- ☐ SD カードなど外部ストレージの利用
- ☐ カメラ機能の利用
- ☐ 通信の暗号化の利用
- ☐ 公衆 Wi-Fi の使用
- ☐ SNS の利用
- ☐ セキュリティーパッチの定期的な適用
- ☐ 端末に対するパスワードの設定やパスワード強度の設定
- ☐ 端末内データの暗号化
- ☐ 利用、インストールするアプリケーションの制限
- ☐ ウェブサイトへのアクセス制限
- ☐ ジェイルブレイク・root 化の禁止

ポリシーを徹底する技術的な対策を考える

検討を重ね、隅々まで配慮の行き届いたセキュリティーポリシーを策定しても、それが従業員に遵守されなければ宝の持ち腐れです。

そこで重要なのが、MDM や MAM、MCM といった技術的な対策です。MDM（モバイルデバイス管理）とは、業務で使われる複数の端末を、統一したポリシーで一元管理する機能を提供します。機能は各社で差がありますが、主なものを挙げるとリモートロックやワイプ機能、デバイス制御、端末情報の収集、ポリシーの一括配布などです。

また、アプリケーションの管理に特化した MAM（モバイルアプリケーション管理）では、アプリケーションの一括配布のほか、情報漏えいリスクの高いアプリケーションを強制的にアンインストールするなど、アプリケーション単位の制御を可能にします。先に説明したように、業務用アプリケーションと個人使用のアプリケーションを分けて管理し、業務アプリケーションを暗号化して保護したり、業務アプリケーションの領域だけ強制的に初期化できる製品もあります。

業務データを保護する MCM（モバイルコンテンツ管理）も、最近注目されています。顧客情報や業務データなど社内コンテンツへモバイルからアクセスする際のユーザー認証を行ったり、コンテンツの閲覧や編集、保存などの操作をユーザーごとに制御できる機能などが特徴です。業務で使う書類や写真のデータに関して、オンラインストレージへのアップロードを禁止するような機能を設定できる製品もあります。コンテンツ管理のポリシーを技術的に徹底することができます。

さらに最近は、MDM、MAM、MCM の機能を網羅した EMM（エンタープライズモビリティ管理）の製品も登場してきました。

このように用途、利用形態に応じて、適切なモバイルデバイスの管理ツールを選択できるようになっています。

MDM、MAM、MCM、EMM の違い

	MDM	MAM	MCM	EMM
概要	モバイルデバイス全体を管理する	モバイルデバイスに導入したアプリケーションを管理する	業務コンテンツを、暗号化したり、閲覧、編集、印刷などを制御する	MDM、MAM、MCM の機能を統合して、モバイルデバイスを管理する
制御対象	モバイルデバイス	業務アプリ	業務コンテンツ	モバイルデバイス 業務アプリ 業務コンテンツ
主な機能	・デバイスの一元管理 ・リモートワイプ ・リモートロック ・ストレージの暗号化 ・アプリケーションの制御 ・root 化の制御 ・遠隔監視 ・バックアップ	・業務アプリのリモートインストール ・業務アプリのリモート削除 ・業務アプリの暗号化 ・業務アプリの管理	・業務コンテンツの配信 ・業務コンテンツの閲覧制御 ・業務コンテンツの削除 ・業務コンテンツのコピー&ペーストなどの制御	・MDM の機能 ・MAM の機能 ・MCM の機能

※製品によっては搭載機能が異なったり、機能の名称が異なっている場合がある

また端末やアプリケーションの管理以外にも、端末上にデータが残らないブラウザーとリモートアクセス製品を組み合わせ、社内のデータをスマートフォンから参照できるソリューションなども登場しています。

このように守るべき対策を踏まえた「現実的なセキュリティーポリシー」と、それを強制的に実施する「技術的な対策」の二本柱が、安全な BYOD 体制を支える礎です。利便性とセキュリティーのバランスを考えることで、システム管理者と従業員の双方にストレスのない環境が構築できます。