

今、企業として知っておきたい

## BYOD 導入のメリット・デメリット



新年度を迎えました。フレッシュな顔ぶれが増えて、気持ちが新たに引きしめる、そんな時期ではないでしょうか。さて、インターネット、そしてクラウド型サービスの普及により、パソコン、スマートフォンを使って、職場以外でもメールや業務ができるということで、とても便利になっています。会社から業務用でノートパソコンやスマートフォンを支給している場合も多くありますが、近年では個人の私物の端末を業務で利用することを認めたり、推奨したりする企業が増えてきているそうです。そこで今回はそういった「BYOD」を導入する際の、メリット・デメリットをみていきたいと思います。

### BYODとは？

BYOD(ビー・ワイ・オー・ディー)とは「Bring Your Own Device」(自分のデバイスを持ち込む)の略であり、会社が従業員に対して、個人所有のスマートフォンやタブレット等の社内への持ち込み、社内ネットワークへの参加、ならびに業務使用を認めることをいいます。



### BYODのメリット

#### 1. 業務効率の向上

使い慣れた端末を使えるので、同じ業務を行うにしても生産性の向上が見込めます。また、空いた時間や移動中などにも端末を扱えるので、業務に充てられる実質的な時間が延びることにつながります。

#### 2. 端末の複数台持ちが不要になる

個人用と別で会社用の端末が支給されている場合がありますが、BYODを導入すれば1台で済みます。また紛失リスクも減少します。

#### 3. コストが削減できる

従業員が所有する端末を利用するため、初期費用や維持費などのコストが削減できます。

#### 4. 「シャドーBYOD」を防止できる

これは、企業側でBYODを許可していないのに従業員自身の判断でBYODをしてしまうことを指します。たとえば、個人のスマートフォンで会社内のクラウドサービスを利用した際に、もしそのスマートフォンをなくしたり、ウイルスの入ったアプリによって攻撃されるなど、情報流出の危険性は大いに高まります。

きちんと明示的にBYODを企業に導入することで、こうしたケースを防止できると言われています。

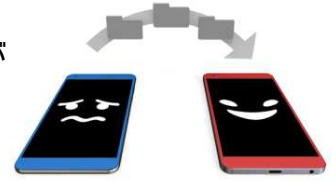


## BYOD のデメリット

### 1. 情報セキュリティリスクの増加

プライベートでも同じ端末を使用しているため、業務に関する情報漏えいのリスクが高まる可能性があります。

(ロックの設定やアプリのセキュリティ更新を必ずしも行っているとは限らないため)



### 2. 従業員の公私の切り替えが難しくなる

個人の端末を使用するため、従業員はプライベートと仕事の区切りが曖昧になってしまい、休憩時間や休日も気が休まらずストレスが増加する恐れがあります。また企業側も勤怠の管理が難しくなります。

### 3. 従業員のプライバシー保護の問題

企業情報のセキュリティや安全性を高めるために個人端末を企業側で管理するようになると、個人のプライバシーが守られないのではないか、という不安が残る場合があります。

## 導入時のポイント

BYOD を導入するには、システム的対策と運用面での対策が必要となります。

### 1. システム的な対策

個人端末と業務端末が一緒になるわけですので、情報漏えいやウイルス感染等を防ぐためにしっかりと管理システムを使用する必要があります。最も一般的な対策は、BYOD を導入する多くの企業で活用されているモバイル端末管理システム(MDM)の利用です。MDM は、企業のシステム上から各個人端末をリモート制御することができます。例えば、紛失などの際には端末をロックしたりデータ削除したりすることができます。また、端末のセキュリティポリシーの設定や使用するアプリケーションの管理(利用許可、機能制限、配布など)が可能で、企業のセキュリティポリシーに沿ったモバイル端末の管理・運用ができるようになるため、情報セキュリティ対策に有効です。

### 2. 運用面での対策

システム面での対策は非常に強力なものですが、それを有効に働かせるには運用ルールをきちんと定めておく必要があります。具体的には、個人端末で行ってよい業務の範囲を定め、情報の保管や持ち出しルールを決めます。また、社員に就業時間と認められる時間以外に業務を行わないよう周知したり、MDM システム上で個人情報を取得したり閲覧したりしない、といった方針を定めることも必要です。また、こうして決定した運用ルールを使用する従業員側もよく理解して使用することもとても大事になります。

## まとめ



BYOD を導入するにあたり、上記でみてきたとおり業務効率向上やコスト削減などメリットも多くありますが、やはりなんといっても情報セキュリティのリスクが高まる、と言った不安な一面があります。そういったリスクが起こりうる可能性があることを認識した上で、システム面、及び運用のルール策定と周知を徹底して行うことが、BYOD の導入を成功させるための重要なポイントのようです。

また、個人端末を業務で使用することや会社の情報資産を扱うため、ルールだけでなく、何らかの規約でその利用を定義する必要があります。会社の管理者が端末の遠隔消去の実行権を持つなど、規約の中で会社の就業規則と紐づけたり、その遵守を誓約してもらうことも導入する際には考慮する必要がありそうです。