

## 「対応は必須、未導入でも安心できない BYOD 対応とは」：出典(GlobalSign)を一部、編集

文責：河東岩夫、作成日：平成 29 年 01 月 20 日

日本の企業や組織において BYOD(「Bring Your Own Device」(自分のデバイスを持ち込む)の略)の積極的な推進は進んでいません。それは企業が十分安心だと思えるセキュリティに対する規定やソリューションが確定されていないからです。しかし BYOD を導入していない又は BYOD を認めていない企業や組織においても BYOD の規定をしっかりとしないとセキュリティリスクが高まります。なぜ、BYOD を認めていない場合でも BYOD に対する規定を定めなければならないのか、BYOD のメリットとセキュリティのリスクについて考えます。

**BYOD とは？BYOD のメリットとデメリット：**BYOD とは一般的に個人所有のデバイスを業務に持ち込んで使用することをいいます。企業にとって最先端技術を取り入れ常に新しい技術を利用したサービスを展開する必要に迫られています。常に新しいデバイスを完備して配布するにはコストがかかりすぎる。そんな中で BYOD は大きなメリットがあると考えられます。

**BYOD のメリット：**BYOD のメリットは従業員が所有するデバイスを業務に利用することにより常にデバイスを企業が購入して従業員に貸与する必要がなくなるという点にあります。最新のデバイスは以前のように PC やノート PC のみならずスマートフォンやタブレットなど、現在ではさまざまな最新デバイスが存在します。それを企業が準備して常に最新の状態を保つにはかなりのコストになりますが BYOD を導入すれば従業員の個人所有の最新機器を業務に利用することができるのです。又、個人所有のデバイスを業務に利用することによって業務時間や社内にいる時間以外でも業務を行う事ができるので企業にとっては生産性の向上が見込めるというメリットがあります。

**BYOD のデメリット：**メリットばかりのように見える BYOD にもやはりデメリットは存在します。それは主としてセキュリティ上のリスクになります。リスクとして一番大きなものは情報の漏洩リスクです。個人端末を業務に利用している状況の場合においてその端末を紛失してしまうと情報漏洩リスクが一気に高まります。又、同時に BYOD にインストールされているソフトも情報漏洩のリスクとなります。企業や組織によっては特定のアプリの利用を禁止しているケースもあります。これは BYOD のソフトウェア利用によるインターネット経由の情報漏洩を危惧したための措置です。

**BYOD と MDM の関係、新しい認証方法としての BYOD：**最近のスマートフォンやタブレットの普及には目を見張ります。個人が所有しているデバイスを業務に利用するためにはできる限りセキュリティのリスクを低減させておきたいです。又、スマートフォンなどのデバイスは PC と比べて持ち運びが容易で常時携帯できるために常に紛失の恐れがあります。紛失した場合、その端末の所在地を確認する、端末をロックする、端末を消去するなどの対応ができる事が望ましいです。又、個人利用端末の業務利用においては従業員が不正な行為をしていないかについての管理も必要になってきます。企業の業務における BYOD のリスク管理を解決してくれる仕組みが MDM で MDM と BYOD で使用する個人利用端末と一定周期で通信を行い、以下のような機能を提供してくれます。

1. 遠隔操作：紛失した端末のロックやスワイプ(端末情報の削除)
2. 情報収集：端末の OS 情報やインストールされているアプリの情報、設定の収集
3. 設定配信：セキュリティーポリシーの配信や業務利用アプリの配信など

MDM を利用することによって BYOD を運用する上でのセキュリティリスクを低減し、業務効率の改善を図ることができます。MDM を利用するためには従業員の個人端末を常に企業が監視状態、管理状態におくことになります。個人端末管理のサーバが従業員の個人端末の自由を制限する形になるためにあまりにも厳しいセキュリティーポリシーを導入すると逆に BYOD が進まないという事態も発生しかねません。セキュリティの担保と個人端末の自由やプライバシーの保護については十分検討する必要があります。BYOD を進めるに当たって一番の懸念は情報漏洩のリスクです。例えば外部からのアクセスを許可する場合には通常の ID とパスワードの管理だけではのぞき見などによるハッキングによる違法アクセスを防ぐことができません。それを回避するために接続可能な端末情報と ID、パスワードが揃わなければ社内システムに接続できなくすればセキュリティは高まります。又、昨今増えているリモートワークや災害時におけ

る遠隔アクセスの認証条件に許可された端末情報を必須とすれば安全にリモート接続が可能になります。又、BYOD の新しい活用方法として、個人端末を認証の要素として利用する事例もあります。これまではセキュリティカードなどで運用していた二要素(多要素)認証の要素の1つを個人の持っているスマートフォンに置き換えるという活用方法です。セキュリティカードなどを導入するコスト面の負担を回避することができるというコスト面でのメリットがあります。いずれにせよ、BYOD を推進するためには企業は個人の端末の登録と管理が必要となるでしょう。

**BYOD を導入していなくても考慮が必要なリスクとは：**BYOD を積極的に導入していない、又、はBYOD を禁止している場合にはセキュリティのリスクがないと思われがちです。しかし実際のところはBYOD を積極的に禁止している企業において無許可の私物端末の業務利用がはびこっている事が多くあります。上記のBYOD はBYOD 自体が禁止されている企業において無許可で個人端末を利用されている状態のことを言います。つまり利用自体禁止されているが業務効率のために隠れて個人端末を利用するという状況のことをいいます。無許可で持ち込んでいるBYOD の利用形態は、年々増加しています。ある調査によると2011年と2016年の調査においてスマートフォンの無許可での持ち込み利用者は約53万台から約447万台に増加し、タブレットは約34万台から350万台に増加するなど5年で9倍から10倍の伸びを示しています。このように隠れた利用が進むBYOD において利用規定を定めず、ただ単に禁止するという方針だけではリスクの回避ができないことを示しています。このような無許可での持ち込みのBYOD 利用を無くすためにもBYOD を受け入れる姿勢が必要です。社内システムを外部に開放する際にID、パスワードの管理だけでなく、接続する端末を端末固有の情報と合わせて認証する二要素認証を取り入れれば無許可での持ち込みのBYOD を無くした上でセキュリティの向上を見込むことが可能です。企業のインフラ、セキュリティ担当者は、個人端末を業務に利用するBYOD はすでに避けられないという事態となっている事を認識する必要がある、組織としてBYOD を積極的に運用するための規定を策定する必要があります。

**セキュリティ以外のBYOD を導入する際の検討事項：**セキュリティの観点からはBYOD の運用のための規定を設ける事は避けて通れないということはこれまでにご説明しました。しかしBYOD を導入するためにはセキュリティの規定以外にも決めなければならない問題が複数あります。

**労働時間の管理の問題：**BYOD を積極的に利用し始めると労働時間以外の時間においても業務を行う事が可能となります。そのため、業務時間が際限なく拡大する可能性があり、又、逆に業務中に私用利用しているかどうかの判別も難しくなります。

**費用負担の考え方：**BYOD を導入するに当たっては端末の費用負担の問題や通信費用の負担の問題が発生します。私物といえども業務に使うからには端末の購入費用は別としても通信費用については対応が必要です。端末の購入費用についても企業が従業員に対して端末の選定を規制する場合には、相応の負担の必要があるでしょう。

**端末内のプライバシーの保護：**BYOD はその性質上、利用するデバイスの中に利用者のプライベートな情報と業務に必要な情報が同居する形になります。そのため、利用区分をはっきりさせておく必要があります。業務利用のデータは企業の所有です。しかし同じ端末に同居する個人データは所有者の物です。又、GPS の位置データのような情報は業務利用を考えた場合には紛失時の端末の搜索に必要ですがプライベートにおける従業員の行動履歴を常に把握しているのは問題となります。BYOD には業務利用情報とプライベート情報が重なる問題が存在するので解決のためには利用者と企業や組織の間で個人端末をどのように利用するか、データの所有者は誰なのかについての合意が必要です。

**BYOD 未導入リスクはある。今すぐBYOD の利用規定作成を！：**日本ではまだまだBYOD を積極的に推進している組織や企業は多くありません。しかしスマートフォンやタブレット、モバイルPCなどのスマートデバイスの普及は加速度的に進んでいます。自分の組織ではBYOD を禁止しているから安心と思っていると隠れた個人端末利用による情報漏洩被害に遭うかもしれません。認証を強化するなどして重要な情報へのアクセスを制限するなどの措置は必要です。BYOD は遠い物ではなく、積極的に利用のための規定を設けて従業員と利用についての合意を形成することが重要です。