IBM Security
Thought Leadership White Paper

BYOD の 10 のルール

ユーザーが仕事で個人デバイスを使用する場合に企業データを保護する方法

IBM

BYOD を許すべきか?

職場に入ってきたモバイル機器の急増は、多くの IT リーダーにとって、天からの介入のようなものです。モバイル・デバイスとそのアプリによって、私たちの生活様式、コミュニケーション方法、移動や買い物の方法、仕事の仕方、その他多くのことが変わりました。このモビリティの変革は非常に急進的、革命的だったため、これらのデバイスのない生活は想像がつかないほどです。BYOD (個人所有機器の持ち込み可) が生まれ、従業員は熱心に従いました。

BYOD など起こっていないふりしても、「当社では従業員にそのようなことを許可しない」と言っても、何にもなりはしません。実のところ、従業員はすでに個人用デバイスを持ち込んでおり、会社の許可があろうとなかろうと、非準拠デバイスをネットワーク内にこっそりもぐりこませ続けるでしょう。2016 年には、企業の従業員の大半が自分のスマートフォンとタブレットを仕事で使うことを許可される見込みです。

そのため、避けようのない疑問が起こります。個人用アプリとデバイスを使用したいと言う従業員の希望をサポートしながら、企業データを保護する安全な環境で生産性を発揮できるようにするにはどうしたらいいのでしょうか? *BYOD の 10 のルール* では、平和で安全、生産的なモバイル環境を構築する方法をご紹介します。

BYOD の 10 のルール

1. テクノロジーを調達する前にポリシーを作成する
2. 企業リソースにアクセスしているデバイスを見つける
3. 登録はシンプルにする
4. 無線を使ってデバイスを構成する
5. ユーザーに自分で問題を解決させる
6. 個人情報を保護し続ける
7. 個人情報を企業データから分離する
8. データ使用状況を管理する
9. デバイスが非準拠になっていないか継続的に監視する
10. BYOD からの投資回収率 (ROI) を享受する

1. テクノロジーを調達する前にポリシーを作成する

他の IT プロジェクトと同様に、テクノロジーよりもポリシーを優先させなければなりません。それはクラウドであっても同じことです。モバイル機器管理 (MDM) テクノロジーを従業員所有のデバイスに対して効果的に使うには、やはり、ポリシーを決める必要があります。これらのポリシーが影響するのは IT だけではありません。人事、法務、セキュリティーなど、生産性の名のもとにモバイル機器を使用するあらゆる部署に影響します。

すべての事業部門が BYOD ポリシーの影響を受けるので、IT 単独でポリシーを作るわけにはいきません。ユーザーの様々なニーズを汲んで、全員をポリシー作成に関わらせる必要があります。

唯一正しい BYOD ポリシーというのはありませんが、考えるべき問いがいくつかあります。

- **デバイス:** どのモバイル機器をサポートするのか?特定のデバイスだけか、それとも従業員が求めるデバイスすべてか?
- **データ・プラン:** 会社がデータ・プランを支払うべきなのか?自分たちが利用料金を出すのか、それとも従業員が経費報告書を提出するのか?
- **コンプライアンス:** 会社で保護する必要のあるデータにはどのような規制があるのか?たとえば、HIPAA (医療保険の携行性［相互運用性］と責任に関する法律) によって、対象となるデータが保存されたデバイスをネイティブ/暗号化することが求められます。
- **セキュリティー:** どのようなセキュリティー対策が必要か (パスコード保護、脱獄/ルート化されたデバイス、アンチマルウェア・アプリ、暗号化、デバイスの制限、iCloud バックアップ)?
- **アプリケーション:** どのアプリを禁止するのか?IP スキャニング、データ共有、Dropbox?
- **契約書:** 企業データを扱う従業員のデバイスを規定する AUA (許容される使用方法に関する同意書) はあるか?
- **サービス:** 従業員はどのような種類のリソースにアクセスできるのか - 電子メール?特定の無線ネットワークや VPN?CRM?
- **プライバシー:** 従業員のデバイスからどのデータを収集するのか?収集できない個人データはどれか?

BYOD の場合、質問に聖域はありません。デバイスをどのように使うのか、IT はそれらのニーズを現実にどう満たすことができるのか、率直かつ正直に話す必要があります。

2. 企業リソースにアクセスしているデバイスを見つける

次のことを想像してみてください。会社で 100 台以上のデバイスをサポートすることを前提に、MDM ソリューションを使い始めました。デバイスのタイプとユーザーについて細かくスプレッドシートに記録しています。想定外のことが起こらないようにするためです。しかし、レポートを初めて表示したとき、200 台以上のデバイスがありました。このシナリオは実際にあったことで、フィクションではありません。このようなことは想像よりもはるかに多く起こります。

現実を否定しないでください。知らないことは害になり得ます。戦略を確定する前に、モバイル・デバイス利用者の現在の環境を理解してください。それには、電子メール環境と継続的に通信でき、企業ネットワークに接続された全デバイスを検出できるツールが必要です。受信箱で ActiveSync をオンにすれば、通常、IT が知らない間に、何の障害もなく複数のデバイスが同期されることに留意してください。

すべてのモバイル機器をモバイル・イニシアチブに組み込む必要があり、新しいセキュリティー・ポリシーが動き始めたら、モバイル機器の所有者に通知する必要があります。

3. 登録はシンプルにする

複雑さは非準拠を生みだす傾向にあります。登録するデバイスを特定したら、ユーザーがシンプルにたやすく登録を行えるテクノロジーを BYOD プログラムで利用する必要があります。プロセスは、セキュリティーで保護されたシンプルなものにする必要があり、それと同時にデバイスを構成します。

完璧なシナリオでは、ユーザーは電子メールのリンクまたはテキストをたどって、自身のデバイスで作成されている MDM プロファイル (重要さを増している AUA の同意を含む) にアクセスできる必要があります。

BYOD を結婚として、AUA を調和のとれた結合をサポートする婚前同意書として考えてください。

既存のユーザーに BYOD プログラムへの登録方法を指示してください。デバイスで企業データを隔離、管理できるように、既存のユーザーの ActiveSync アカウントを消去することをお勧めします。新しいデバイスは、新しいプロファイルでスタートすべきです。

IT の観点から、皆さんは既存のデバイスをまとめて登録する機能を求めているか、ユーザーに自分でデバイスの登録を行ってほしいとお考えでしょう。　また、ワンタイム・パスコードなどの基本的な認証プロセスで従業員を認証するか、Active Directory/LDAP など、既存の企業ディレクトリを使用する必要もあります。企業リソースにアクセスしようとする新しいデバイスは隔離し、IT はそのようなデバイスの通知を受け取る必要があります。これにより、IT は、適切な登録ワークフローが承認されたら、それを柔軟にブロックまたは開始して、企業ポリシーとのコンプライアンスに準拠することができます。

4. 無線を使ってデバイスを構成する

BYOD ポリシーと MDM ソリューションで 1 つ避けた方がいいことがあるとすれば、それは、より多くのユーザーをヘルプ・デスクに送ることです。IT とビジネス・ユーザーの双方にとって等しく効率性を最適化するには、デバイスを無線で構成すべきです。

ユーザーが AUA に同意したら、従業員がアクセスする上で必要な、以下のようなプロファイル、認証情報、設定すべてを提供します。

- 電子メール、連絡先、カレンダー
- VPN および Wi-Fi
- 会社のドキュメントとコンテンツ
- 内部アプリとパブリック・アプリ

この時点になったら、特定のアプリケーションへのアクセスを制限するポリシー、ユーザーがその月のデータ使用量または利用料金の制限を超過した場合に警告を生成するポリシーを作成する必要もあります。

5. ユーザーに自分で問題を解決させる

また、皆さんは自分のしたことに感謝することになります。ユーザーは機能するデバイスを求めており、皆さんはヘルプ・デスクの時間を最適化したいと思っています。強固なセルフサービス・プラットフォームを使用すると、ユーザーは直接次のことを実行できます。

- 従業員が現在の PIN またはパスワードを忘れた場合はリセット可能
- マッピング統合を使って、紛失したデバイスの位置情報を Web ポータルから特定
- デバイスをリモートでワイプして、機密企業データを削除

セキュリティー、企業データの保護、コンプライアンスは、皆で共有する責任です。これは従業員にとって苦い薬になるかもしれませんが、彼らの協力なしでリスクを軽減できる見込みはありません。セルフサービス・ポータルにより、従業員はコンプライアンスに違反している理由を理解できます。

6. 個人情報を保護し続ける

もちろん、BYOD ポリシーは企業データを保護するだけではありません。優れた BYOD プログラムは従業員の個人的なデータを IT など他のデータから分離します。個人を特定できる情報 (PII) を使用すると、人物の識別、連絡、発見が可能です。一部の個人保護法は、企業がこのデータを閲覧することすら禁じています。個人情報保護方針を従業員に伝え、彼らのモバイル機器から収集できないデータがどれかを明確に説明してください。たとえば、MDM ソリューションは次のように、アクセス可能な情報とアクセスできない情報を解析できる必要があります。

- 個人の電子メール、連絡先、カレンダー
- アプリケーション・データとテキスト・メッセージ
- 通話履歴と音声メール

その一方で、何を収集しているのか、どのように使用するのか、それがなぜユーザーにとって有益なのかをユーザーに伝えます。

先進的な MDM ソリューションは、個人情報保護方針をプライバシー設定に変換して、デバイス上で位置情報とソフトウェア情報を非表示にすることができます。これにより、企業は PII 規制を満たし、スマートフォンやタブレットでの個人情報の閲覧を防止することで、従業員の安心感を高めることができます。

- アプリ在庫報告を無効にすることで、管理者による個人用アプリケーションの閲覧を制限
- 位置情報サービスを非アクティブ化することで、物理的な住所、地理的座標、IP アドレス、Wi-Fi SSID など、ロケーション・インジケーターへのアクセスを阻止
- 透明性と明確性は重要な合言葉です。各自がルールを知っていれば、BYOD ポリシーへの抵抗がはるかに和らぎます。

7. 個人情報を企業データから分離する

IT とユーザーの双方が BYOD について折り合いをつけられるようにするには、誕生パーティーの写真のような個人情報や小説などを生産性アプリから分離する必要があります。

簡単に言うと、従業員が退職を決めた場合、企業のアプリ、ドキュメント、その他の資料は IT が保護する必要がありますが、個人の電子メール、アプリ、写真は会社の IT が手を付けるべきではありません。

このアプローチがもたらす自由に感謝するのはユーザーだけではありません。IT も同様に感謝するでしょう。その方が人生がはるかに楽になる可能性が高いからです。このアプローチの場合、従業員が会社を退職する際、IT は企業データを選択的にワイプできます。状況によっては、従業員がデバイスを紛失した場合、デバイス全体をワイプできます。真の MDM ソリューションは皆さんに選択肢を与えてくれます。

デバイス・ワイプの 86 パーセントくらいは選択的に行われていると見込まれています (企業データのみをワイプ)。

8. データ使用状況を管理する

BYOD ポリシーにより、通信に関する IT の作業負荷は大幅に減りますが、多くの企業は余分な料金を避けるために、従業員がデータ使用を管理できるように支援しなければなりません。

企業がデータ・プランの料金を支払う場合、このデータを追跡する方法が必要な場合があります。支払わない場合は、ユーザーが現在のデータ使用量を追跡できるように支援しなければならないかもしれません。デバイス上のネットワーク内およびローミング・データを追跡でき、ユーザーがデータ使用量のしきい値を超えた場合は、アラートを出せるようにする必要があります。

ローミングおよびネットワーク内のメガビット制限を設定し、使用されたパーセントに基づいて通知を作成する課金日をカスタマイズすることができます。Wi-Fi (利用可能な場合) を使用することのメリットをユーザーに教えることをお勧めします。自動 Wi-Fi 構成を使用すると、会社の拠点にいるときに、デバイスを自動的に Wi-Fi に接続させることができます。

利用料金プランが毎月、50 ドルまたは 200 MB のデータ使用量しかカバーしない場合、超過料金が発生する寸前であることを伝える警告が従業員に表示されます。

9. デバイスが非準拠になっていないか継続的に監視する

デバイスを登録したら、肝心なのはコンテキストです。特定のシナリオが発生していないかデバイスを継続的に監視し、自動ポリシーを設ける必要があります。ユーザーが管理を無効にしようとしていないだろうか?デバイスはセキュリティー・ポリシーに準拠しているか?表示しているデータに基づいて調整を行う必要があるか?ここから、追加のポリシーまたはルールを作成する必要があるか判断し始めることができます。次に、一般的な例をいくつか挙げます。

- **脱獄の「根本的原因」を理解する:** 従業員は時々、有料アプリを無料で手に入れるために電話を「脱獄」または「ルート化」して、情報を盗むことができるマルウェアを招き入れることがあります。デバイスが脱獄されると、MDM ソリューションは、デバイスから即座に企業データを選択的にワイプするといった措置を講じることができなくてはなりません。
- **ワイプを実行せずに、SMS を送る:** Angry Birds のような時間つぶしのゲームが企業ポリシーに抵触しても悪意はない場合、自動ワイプは手厳しすぎます。MDM ソリューションは攻撃に基づいてポリシーを実施できます。MDM はユーザーにメッセージを送って、IT がワイプ・ブタンを押す前にアプリケーションを削除するための猶予を提供します。
- **新しいオペレーティング・システムが利用可能:** BYOD の効果を継続するには、新しい OS のインストールが可能になったらユーザーに知らせるシンプルな方法が必要です。適切な MDM ソリューションを使用すれば、OS アップグレードはセルフサービス機能になります。古い OS バージョンを制限することで、コンプライアンスを確実に守り、デバイスの操作性を最適化できます。

10. BYOD からの投資回収率 (ROI) を享受する

BYOD によって、デバイスを購入する責任は従業員にシフトしますが、全体像と会社の長期的なコストについて考えてみることをお勧めします。

ポリシーを作成する際、それが ROI にどのように影響するのかを考えてください。それには、以下に示すように、アプローチの比較が含まれます。

企業所有のモデル

- 各デバイスにいくら使うのか
- 全額補助のデータ・プランのコスト
- 数年ごとのデバイスのリサイクルにかかるコスト
- 保証プラン
- プログラムの管理に要する IT の時間と労力

BYOD

- 部分補助のデータ・プランのコスト
- 排除されたデバイス購入コスト
- モバイル管理プラットフォームのコスト

BYOD ポリシーは万能ではありませんが、注意深く作成すれば、モバイル機器を効果的、効率的に管理する上で必要な方向性を定めることができます。

もちろん、従業員が常時モバイルを使用し、接続されていれば、生産性の向上が見られることがほとんどです。企業デバイスの使用権限が付与されたことがなかった新しいユーザーの生産性にこうした進歩をもたらす上で、BYOD は優れた手段になります。

BYOD:自由のセキュリティー

BYOD は、従業員に自分のデバイスで仕事をする自由を与える一方で、IT の財務面、管理面の負担を大幅に軽減する新しいベスト・プラクティスです。ただし、BYOD は、綿密に作成したポリシーと強固な管理プラットフォームがなくては、効率的な管理とコスト節約のこれらの約束を果たすことはできません。

まだモバイル戦略の初期段階にある場合は、IBM® MaaS360® の豊富な教育リソースをご利用ください。

BYOD がビジネスに最適だと判断したら、ここをクリックして、30 日間無料の MaaS360 評価版をお試しください。MaaS360 はクラウドベースなので、データを一切失うことなく、テスト環境が自動的に本番環境になります。

IBM MaaS360 について

IBM MaaS360 は、業務のあり方に合わせて生産性とデータ保護を実現するエンタープライズ・モビリティ管理プラットフォームです。モバイル・イニシアチブの基盤として多数の組織から信頼されています。MaaS360 は包括的な管理機能を提供し、ユーザー、デバイス、アプリ、コンテンツへのセキュリティーを強力に制御することで、どのようなモバイル導入もサポートします。IBM MaaS360 の詳細と 30 日間の無料トライアルのご利用については、次の Web サイトをご覧ください。www.ibm.com/maas360

IBM Security について

IBM のセキュリティー・プラットフォームはセキュリティー・インテリジェンスを提供して、組織が人々、データ、アプリケーション、インフラストラクチャーを包括的に保護できるように支援します。IBM は、ID およびアクセス管理、セキュリティー情報およびイベントの管理、データベース・セキュリティー、アプリケーション開発、リスク管理、エンドポイント管理、次世代侵入保護などのためのソリューションを提供しています。IBM は、世界で最も幅広くセキュリティー研究開発を行い、セキュリティーを提供している組織の一つです。詳細は、以下をご覧ください。www.ibm.com/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in Japan
March 2016

WGW03112-JPJA-01