シンプルかつセキュアなデバイス管理を実現するためのベストプラクティス

ビジネスの生産性を高めるモバイル環境の実現
ユーザーが自由にデバイスを選択できるソリューション
IT 部門による万全のセキュリティとシステムの完全な管理

企業における現代の IT 戦略において、その基盤の 1 つとなるのは、従業員が自身のニーズに最適なデバイスを自由に選択できる環境です。このような環境が実現すれば、企業の生産性と柔軟性は高まり、従業員の満足度も向上します。適切な戦略を採用している IT 部門では、最適なポリシーやテクノロジーを導入できるようになっており、これにより、コストを削減しユーザーエクスペリエンスを大幅に向上させながら、ビジネス情報のセキュリティも確保していけます。

策定する戦略は、次のようなことが実現できるものでなければなりません。

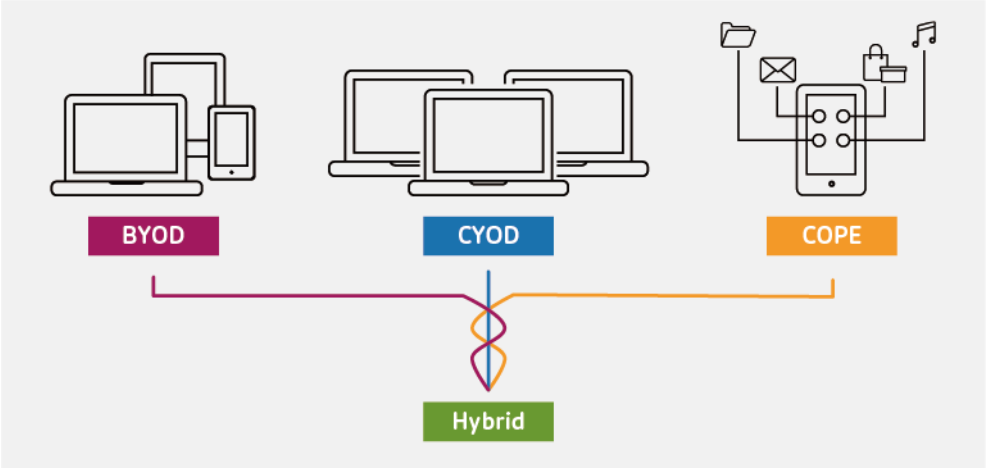
- **ユーザー自身によるデバイスの選択：**ユーザーが自身の生産性や、コラボレーションの能力、モビリティの能力を高められるよう、使用するデバイスを自ら選択できるようにする。
- **機密情報の保護：**プライバシーやコンプライアンス、リスク管理の要件を満たしながら、機密性の高い情報を紛失や盗難のリスクから保護する。
- **コストの削減と管理の簡素化：**セルフサービスプロビジョングの導入と、管理および監視の自動化を通じて、コストを削減し管理を簡素化する。
- **IT 部門の業務負荷の軽減：**包括的な単一のソリューションにより、データ、アプリケーション、デバイスの管理と、これらのセキュリティを確保し IT 部門の業務負荷を軽減する。

以下に説明する 8 つのベストプラクティスに従い、戦略を策定すれば、エンドユーザーにとってはシンプルである一方、IT 部門がセキュリティと管理性を効果的に確保できる環境が実現します。

1. ポリシーの選択

モビリティとコンシューマライゼーションによって、IT の変革が進展しています。これを受けて新たに登場したいくつかのポリシーでは、従業員によるデバイス選択の自由度を確保しながら、IT 部門の管理性を高めることが可能になっています。

- BYOD（Bring-Your-Own-Device）：個人所有のデバイスを業務で利用できるようにします。
- CYOD（Choose-Your-Own-Device）：企業が所有するデバイスの中から、業務に使用するデバイスを従業員が自分で選択します。
- COPE（Corporate-Owned, Personally Enabled）：企業が所有するデバイスに一定の条件や制限を施し、このデバイスで個人所有のアプリケーションや企業所有のアプリケーションを使用します。
- ハイブリッドアプローチ：複数のポリシーを組み合わせて使用し、個々のユーザーやグループに最適なかたちでモビリティを強化します。たとえば、COPE は、CYOD や BYOD と組み合わせて使用することができます。



ポリシーごとに微妙な違いがあるのは事実ですが、セキュリティ面を含め、ユニファイドエンドポイント管理（UEM）に関する最も基本的な考え方は、どのポリシーも同じであり、大きな違いがあるのは、コストの扱いです。

BYOD では、デバイスとデータプランのコストは、ユーザーが負担します。場合によっては、一部の額または全額分の手当が企業から支給されることもあります。一方、COPE と CYOD の場合は、デバイスの費用とデータの使用料は企業が負担します。また、BYOD のポリシーの場合、COPE や CYOD では考慮する必要ない事柄にも注意を向けねばなりません。たとえば、就業後や週末の業務時間外に従業員がメールをチェックしたようなときに時間外手当を支払う必要があるかどうかといったようなことを検討しておく必要があります。

2. 適格性の判断

個人所有のデバイスの業務利用をどのユーザーに許可するのかを明確にします。また、それが、企業所有のエンドポイントの利用を補完する一時的な措置であるのか、あるいは、企業デバイスの利用と完全に置き換えるものであるのか、それともその中間に位置するものであるのかも明らかにしなければなりません。個人所有のデバイスの業務利用を許可する場合、ある種の権限として許可が与えられることもあれば、従業員の要求に応えるかたちで行われることもあります。特定のタイプの職務では必須条件となるケースもあります。また、一部のユースケースにおいては過度のリスク要因ともなり得ます。そして多くの場合、これらの状況が混在しています。

BYOD を適用する適格性があるか否かを判断する際、業務のタイプや出張の頻度、パフォーマンス、機密性の高いデータをオフラインで使用する必要性などの点を基準に判断する方法があります。ただし、適格性は広範なレベルで規定されるものであり、プログラムの適用に伴いチームメンバーに手当を支給する場合は、その対象者決定の最終承認を常にマネージャーが行う必要があります。また、マネージャーは、ほかの部署で適用されているインセンティブや権限、ほかの部署で発生した懲戒処分も念頭において、BYOD や COPE、CYOD を利用するようお勧めします。

一般に契約社員は、BYOD の候補としては理想的です。すでに多くの組織が、個人所有のデバイスを持ち込むよう、契約社員に求めています。そしてこれを要求するかわりに、個々の契約社員独自のコンプライアンス条件を認めています。

3. 利用を許可するデバイス

デバイスの種類が増えすぎて管理不能にならないよう、社内で許可するモバイルデバイスのタイプを制限します。このポリシーをどの程度まできめ細かくするのかは、ユーザーの要件やセキュリティリスク、サポートリソースなどの要因に応じて異なります。一般に、デバイスのタイプや OS のバージョン、モデルの番号などの面でポリシーをきめ細かく規定すればするほど、デバイスのテストやサポートを適切に行うためのリソースが多く必要になります。

デバイスの所有者を明確にできるよう、BYOD のプログラムに参加する従業員は、社内の購買部門は利用せず、一般のコンシューマーチャネルを通じてデバイスを購入したほうがよいでしょう。また、デバイスのベンダーとの契約上、従業員割引が可能である場合は、これを適用することも企業は検討すべきでしょう。

ユーザーによっては、モニターやキーボードなどの周辺機器を必要としている場合もあります。いずれにせよ、個々のアイテムを個人で調達し所有しているユーザーを明確にしなければなりません。

4. 実際の展開

実際の展開を問題なく完了するためには、コミュニケーションが不可欠です。そこで、ユーザーがプログラムに参加するかしないかを判断する場合や自身のニーズに適したデバイスを選択する場合にユーザーをサポートできるよう、ガイダンスを提供する必要があります。また、データのアクセス方法やデータの利用方法、データを保存する方法もユーザーに理解してもらう必要があります。IT 部門の管理下にないコンシューマーアプリケーションやサービスを使用するために業務用のアカウントをセットアップし利用する適切な方法についても伝えねばなりません。

さらには、業務用データやビジネスデータは厳密に分離して、e-Discovery の要件やデータ保存のポリシーに対応できるようにします。同様に、業務メールが私用のアカウントから送信されるようなことがないようにします。そして、BYOD で利用するデバイスには、社内のデバイスと同じように、組織の要件に適った利用ポリシーを適用します。

さらにほかにも重要なことがあります。従業員がシステムの利用を開始するのを支援する導入プログラムの準備です。プログラムの開始を知らせる E メールにセルフサービスポータルのリンクを記載して対象の従業員に送れば、従業員は速やかにかつ効率的にサービスの利用を始められます。

5. コストのシェア

BYOD の導入によって得られる主要なメリットの 1 つに、コストの削減があります。BYOD では、業務に使用するさまざまな個人所有のデバイスのコストは、その一部、または全部を従業員が負担します。BYOD について手当を支給している企業では一般に、手当の額はデバイスのコストの 18%から 20%になっています。なお、BYOD のプログラムに参加する従業員は、この手当が所得税の課税対象になる点を意識しておく必要があります。そして、企業の側では、所得税の税率が高い地域のユーザーにはそれに応じて手当の金額を積み増しし、プログラムの参加者全員で税引き後の手当の金額が均一になるようにしなければなりません。

手当を支給する場合には、プログラムの参加者の参加期間全体に対応した金額の支払いが必要です。また、個人所有のデバイスのスペックが古くなって業務用の端末として必要な要件を満たすことができなくなるのを回避するために、手当の内容は定期的に更新する必要があります。さらに、BYOD プログラムの参加途中で従業員が退職する場合には、手当の一部の返金を従業員に求める必要があります。

BYOD プログラムの導入に際しては、それがコストのシェアという意味合いを持つ点を意識しなければなりません。導入を一度に行った場合、コストが増加する可能性がありますが、これは、エンドポイントの更新時にすべてのエンドポイントで一斉にサインアップが行われ、手当の請求が発生するためです。デバイスのライフサイクルを間近に迎えているユーザーを対象に BYOD プログラムを適用した場合は、コスト増加の影響がさらに拡大します。一方、手当を支給しない場合には、最初から一斉に運用を開始する方法を進められます。

これらに加え、BYOD のポリシーでは、コストのシェアをするかしないかにかかわらず明確にしておくべきことがあります。企業のファイアウォールの外側で行われる通信のコストを誰が負担するのか、また、この通信には、モバイルネットワーク、公衆 Wi-Fi、ホームブロードバンドのいずれを使用するのかといったことです。

6. セキュリティとコンプライアンス

個人所有のデバイス、企業所有のデバイスのいずれを利用する場合でも不可欠となる要件の 1 つに、データの保護があります。しかも、ユーザーエクスペリエンスに影響を与えることなく保護ができなければなりません。業務に使用するデバイス上に個人のアプリケーションやデータを置くことを許可しているプログラムの場合、モバイルアプリケーション管理（MAM）の手法が役に立ちます。この手法を活用すれば、個人のアプリケーションやデータを企業のコンテンツと分離することが可能です。

個人所有のデバイスに業務アプリケーションをインストールすれば、リスクの増大を招きます。しかし、統合エンドポイント管理、アプリケーションとデスクトップの仮想化、セキュアなファイル共有を統合する戦略を採用すれば、そのようなインストールをしなくてすみます。企業のデータはデータセンターやクラウドでセキュリティが維持されます。そして、これらのデータをどうしてもモバイルデバイス上に置く必要のあるときには、コンテナ化や暗号化、リモートワイプといったメカニズムにより、データの保護が行われます。また、ローカルドライブや USB ストレージなど、クライアント側にあるストレージへのアクセスをできなくしたり、印刷の機能を無効にしたりすることも可能です。

MAM では、デバイスの所有者、ステータス、ロケーションにもとづくポリシーを用いて、アプリケーションやデータへのアクセスを制御したり、アクセスのセキュリティを確保したりすることもできます。さらには、デバイスの登録と管理、パスコード要件の設定、脱獄デバイスの検知が可能であるほか、コンプライアンスを満たしていないデバイスや、紛失したデバイス、盗難にあったデバイス、退職した従業員や契約の切れた契約社員が使用していたデバイスについて、部分的なワイプや完全なワイプの処理ができます。アプリケーションのトンネリングやブラックリスト登録、ホワイトリスト登録、コンテキスト対応の動的なポリシーの機能を通じてセキュアなアクセスも実現しており、これにより、アプリケーションのセキュリティが維持されます。

ネットワークを保護する場合は、ネットワークアクセス制御（NAC）テクノロジーを使用します。このテクノロジーでは、ネットワークに接続してくるユーザーの認証を行い、ユーザーのデバイスのアンチウイルスソフトウェアやセキュリティパッチが最新の状態になっているかどうかをチェックします。

また、ファイアウォールの外側においては、暗号化や仮想化を行うことで、Wi-Fi や WEP 暗号化、オープンワイヤレス、3G/4G など、コンシューマーグレードのアクセス方式に存在するセキュリティ脆弱性のほとんどを緩和することができます。さらに、ネットワークのセキュリティ機能では、組織の内部、外部に存在するモバイル上の脅威について、その詳細な把握と攻撃の防御が可能であり、問題のあるデバイスやコンプライアンス違反のアプリケーションが利用されないようにしたり、権限のないユーザーのアクセスをブロックしたりします。加えて、SIEM（Security Information and Event Management）システムとも連携します。

BYOD プログラムの参加者が退職したり、重要なポリシーで侵害が発生したり、個人所有のデバイスの紛失や盗難が発生したりしたときに、これに対処するための仕組みも用意されており、対象となるデバイスにおけるアプリケーションやデータへのアクセス機能をすぐに停止できます。具体的な機能としては、業務で使用する SaaS アカウントを自動で無効化する機能や、紛失したデバイスの内容を部分的にワイプする機能などがあります。このメカニズムは、COPE や CYOD のプログラムでデバイスを使用するにあたっても不可欠となるものです。過去に誰かが使っていたデバイスを新しいユーザーに再度割り当てる場合、デバイスにデータが残っていると、これにアクセスする権限のないユーザーがデータにアクセスしてしまう危険がありますが、前述のメカニズムがあれば、このようなリスクを回避できます。

従業員が持ち込むどのようなデバイスでも業務アプリケーションや業務データを利用できるようにするオープンな BYOD は許可せず、一部の組織では、管理を徹底するアプローチを採用しています。このシナリオでは、登録の処理や、評価、認証、リソースへのデバイスのアクセスなどについて、IT 部門が直接、個人所有のデバイスを管理します。

7. 監視と管理

ポリシーのコンプライアンスを確保し、投資収益率を明確にするうえで、継続的な監視と管理が欠かせません。

一部の UEM ソリューションでは、各種違反への対応におけるアクションの指示など、監視と管理のいくつかの側面を自動化することで、IT 部門の生産性と業務効率を高めます。また、自動化の対象項目としては、デバイスの内容の部分的なワイプや完全なワイプ、「コンプライアンス違反」のステータスにデバイスを設定する処理、デバイスの無効化などがあります。あるいは、ブラックリストに登録されているアプリケーションを削除するなど、問題修正の措置を一定の期限内に行わないとさらに厳しいアクションを行う旨をユーザーに通知するといったことも自動化できます。

8. デバイスの保守サポートおよびメンテナンス

BYOD プログラムでは多くの場合、各デバイスで必要とされるメンテナンスについて、IT 部門の作業が減ります。これは、ユーザーもデバイスのオーナーであるためです。それゆえ、各種サポートタスクやメンテナンスタスクにおける処理やコスト負担の方法をポリシーで明確にし、IT 部門の行う作業が煩雑になったり、IT 部門の負荷が増えたりしないようにしなければなりません。CYOD や COPE のプログラムではほとんどの場合、デバイスの保守サポートとメンテナンスは、IT 部門が全面的に担う業務になります。

Citrix Workspace で実現するセキュアなデバイス管理

どのようなデバイス管理プログラムであっても、個人所有のデバイス上で業務アプリケーションや業務ファイルをセキュアに利用できるようにするためのテクノロジーが必須です。Citrix Workspace には、組織がシンプルかつセキュアで効果の高い BYOD、CYOD、COPE を実現するうえで必要となる主要な機能がすべて揃っています。統合エンドポイント管理、Windows のデスクトップとアプリケーションの仮想化、セキュアなファイル共有、アプリケーションの配信といった機能を組み合わせ、これにより、従業員が業務で利用するあらゆるデバイス上で業務アプリケーションと業務データを利用できるようにしながら、セキュリティと管理性も維持します。

ユニファイドエンドポイント管理

アイデンティティベースでの、アプリケーション、データ、デバイスのプロビジョニングと管理を可能にするほか、退職した従業員のアカウントを自動で削除したり、デバイスを紛失した場合にそのデバイスの内容を部分的にワイプしたりできます。Citrix Workspace では、IoT を含むデバイスを管理することができます。さらには、アプリケーションレベルでのセキュリティと制御の機能により、BYOD や CYOD、COPE プログラムのデバイスにおいて、プラベートコンテンツの利用になんら支障を与えることなく企業のデータを保護することも可能です。また、Citrix Workspace のエンドポイント管理では、個々の組織にとって最適な MAM 戦略を選択できます。Samsung KNOX や Appconfig、Citrix MDX などのプラットフォーム MAM（デバイスを登録せずに、よりレベルの高いアプリケーションの暗号化を実現）、Intune MAM のいずれもが利用可能です。

Windows のデスクトップとアプリケーションの仮想化

Windows のデスクトップとアプリケーションを個々のデバイスにインストールして管理するのではなく、必要に応じてその都度、デバイスを問わずこれらを利用できるようにします。アプリケーションやデータはデータセンターやクラウド内で管理されるため、個人所有のデバイス、企業所有のデバイスのいずれについても、データの保護やコンプライアンスの順守、アクセス制御、ユーザーの管理を、IT 部門は共通の統合環境で容易かつ一元的に行えます。

アプリケーションストア

統合アプリケーションストアでは、ワンクリックで、モバイル、Web、SaaS、企業、および Windows のアプリケーションにアクセスできます。Windows、Mac のどちらのコンピューターでも、また、iOS、Android、Windows ベースのいずれのモバイル製品、あるいは、Google Chromebook であっても、ユーザーの選択したデバイスにかかわらず、ネットワークや利用場所を問わずに、同じユーザーエクスペリエンスを実現します。

セキュアなアクセス

統合管理のフレームワークでは、あらゆるデバイス上での、アプリケーション、デスクトップ、サービスへのアクセスについて、セキュリティの確保、制御、最適化ができるほか、監査やレポーティングの機能を通じ、コンプライアンスの順守とデータの保護も可能です。また、シトリックスのみが提供している機能もあり、この機能では、ファイアウォールの内側でモバイルデバイスが社内リソースとアプリケーションデータをやり取りする際に、独自のマイクロ VPN でデータをさらに保護します。

セキュアなファイル共有

従業員は組織の内部、外部のほかのユーザーとセキュアにファイルを共有しコラボレーションに活用できるほか、複数のデバイス間でファイルを同期することも可能です。ポリシーベースのアクセス制御、監査、レポーティング、リモートでのデバイスワイプの機能により、ビジネスコンテンツのセキュリティが確保されます。

適切なポリシーとテクノロジーを導入すれば、従業員のデバイス選択の自由度を確保しながら、IT 部門がセキュリティと管理性を確保できる環境が実現します。こちら、www.citrix.co.jp/workspace に、Citrix Workspace についての詳しい情報をご用意しておりますので是非ご覧ください。Citrix Workspace が実現するシンプルかつセキュアなデバイス管理の詳細をご理解いただけます。