ISF NET

テレワーク時代の情報システム部門の方に読んで欲しい

現代的な
デバイス管理とは？

1. こんな悩みありませんか？

テレワークが増えて、きちんと
端末の管理ができていない…

業務で利用するアプリケーションが
増えすぎてて、**バージョン情報**が
しっかりと管理できないよ …

PCにタブレットにスマホ…
管理するべき**端末が増えすぎ**…

情報システム担当

上層部から**BYODの検討**をしろ
と言われたけど…
何をすればよいか分からないよ …

2. それらの悩み…EMM製品の導入で解決！

EMM製品とは？？

Enterprise Mobility Management の頭文字を取った略称で、
「業務で利用するデバイスを統合的に管理する」サービスです。

社員に貸与しているPCやタブレットスマートフォンや、会社が業務利用を許可している個人の端末（BYOD＝Bring Your Own Deviceの略称）について、社内のセキュリティポリシーに基づいた適切な管理が“遠隔で”できるサービスとなります。
例えば、業務に必要な機能やシステムへの有効化や逆に業務に関係ない機能の制限などをリモートから端末ごとに設定することができます。

EMM製品のメリット

リモートワーク環境下にある端末は以下のようなセキュリティリスクを抱えておりますがこのリスク低減を行うことができるのがEMM製品の最大のメリットとも言えるでしょう。

リモートワーク環境下における端末のセキュリティリスク

- 盗難や紛失
- 端末の不正利用
- 情報漏洩
- OSアップデート未実施によるウィルス感染

※EMM製品の導入が全てのセキュリティを担保する訳ではありません

EMMの3つの管理機能

MDM（モバイルデバイス管理）	• リモート制御・管理 • アプリケーション配布・利用制限 • アップデート管理
MAM（モバイルアプリケーション管理）	• 業務用アプリケーションの管理 • 不正アクセス禁止の認証機能
MCM（モバイルコンテンツ管理）	• 業務用コンテンツの制限 • アクセスログの解析

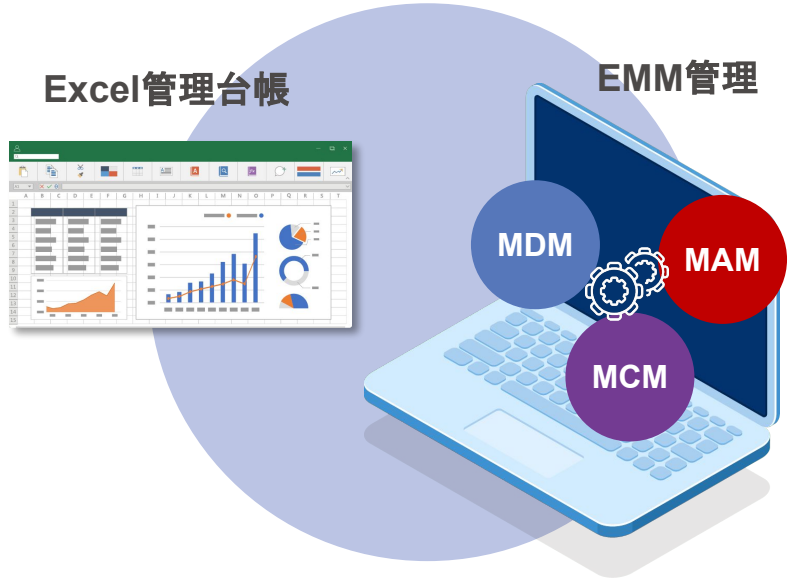
3. Excelでの管理で十分じゃない？じゃないんです！！

Excelでの管理は、最も手軽に始められる手法であり、緊急での対応時にはおすすめです。
ですが事業を長期で展開していく中で、デバイス数の増減・利用者の入れ替えに伴い、**ハードウェア・ソフトウェア・OS・ライセンスの運用業務**が発生します。さらにテレワークや働く場所の増加に伴う、**デバイスの紛失リスクや情報漏洩リスク**、OSやライセンスのアップデート管理ができないことによる**ウイルス感染リスク**を回避するためには、Excelでの管理は十分とは言えません。

Excelでの管理と、EMMでの管理を導入した場合で、利便性・メリットを表にまとめました。

ユーザーにとって、各デバイスを適切な状態に維持し、必要があれば最適化を図ることにより、仕事の生産性に寄与します。さらに情シス部員本人の時間を確保することにもつながり、ITによる事業の付加価値の創出にもつながるでしょう。
もし、従業員がスマートフォンを紛失してしまったら？セキュリティ面のこのような課題についても、EMMは解決します。
次のページから詳しく説明していきます。

	Excel 管理台帳を利用した場合	EMM を利用した場合
ハードウェア管理	△	◎
ソフトウェア管理	△	◎
ライセンス管理	△	◎
セキュリティ対策	✕	◎
手軽さ	◎	○



4. MicrosoftのEMM Intune導入で、デバイスを管理

Microsoft Intuneとは？

安心安全なMicrosoft社製クラウド型EMM製品

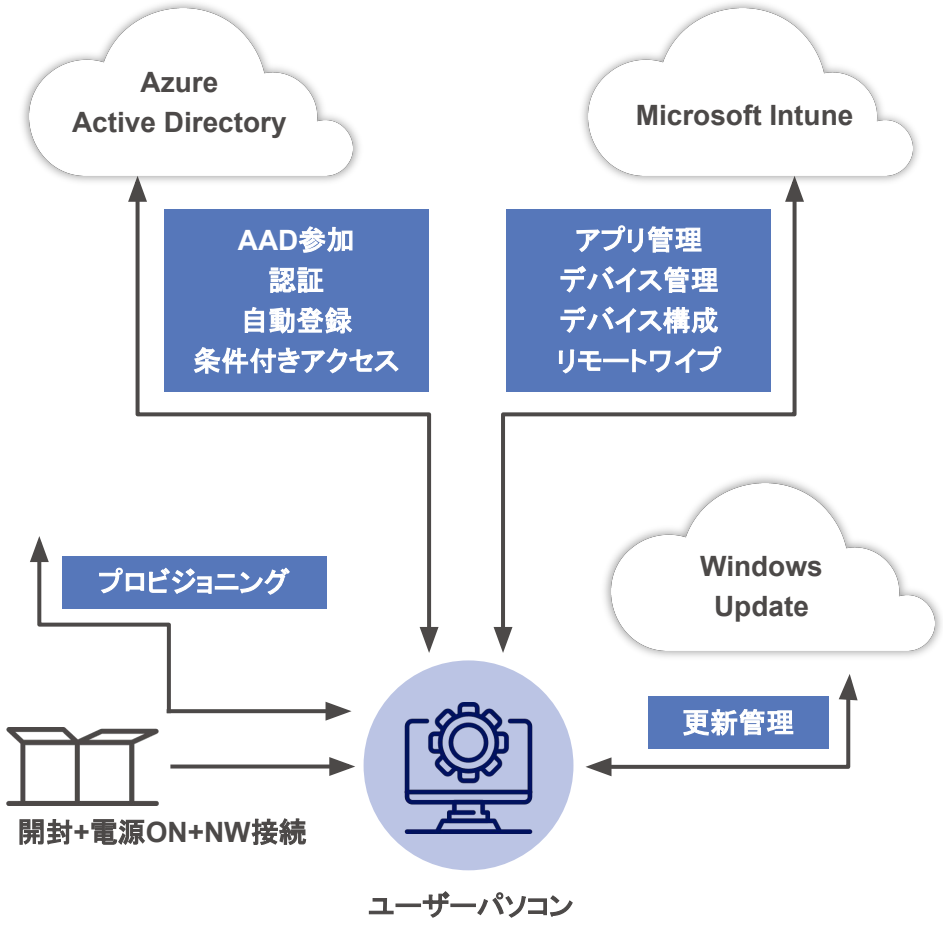
- クラウド製品のため専用サーバが不要！！
- マルウェア対策機能搭載でよりセキュアなデバイス管理が可能！！
- WindowsはもちろんMacやAndroidなど多様なOSをサポート！！

Microsoft Intune導入で実現できること！

- ✔ 年々増えていくハードウェアやソフトウェアの管理
- ✔ それらの増加に伴うOSやライセンス、ハードウェア運用の管理
- ✔ 働く場所を選ばないリモートでのハードウェアやソフトウェアの管理
- ✔ BYOD環境でのデバイス/アプリケーションの管理
- ✔ リモートでの端末ロックによるセキュリティリスクの軽減
- ✔ 個人ごとのアプリケーションの権限付与によるセキュリティの強化

など

モダンなデバイス管理環境イメージ



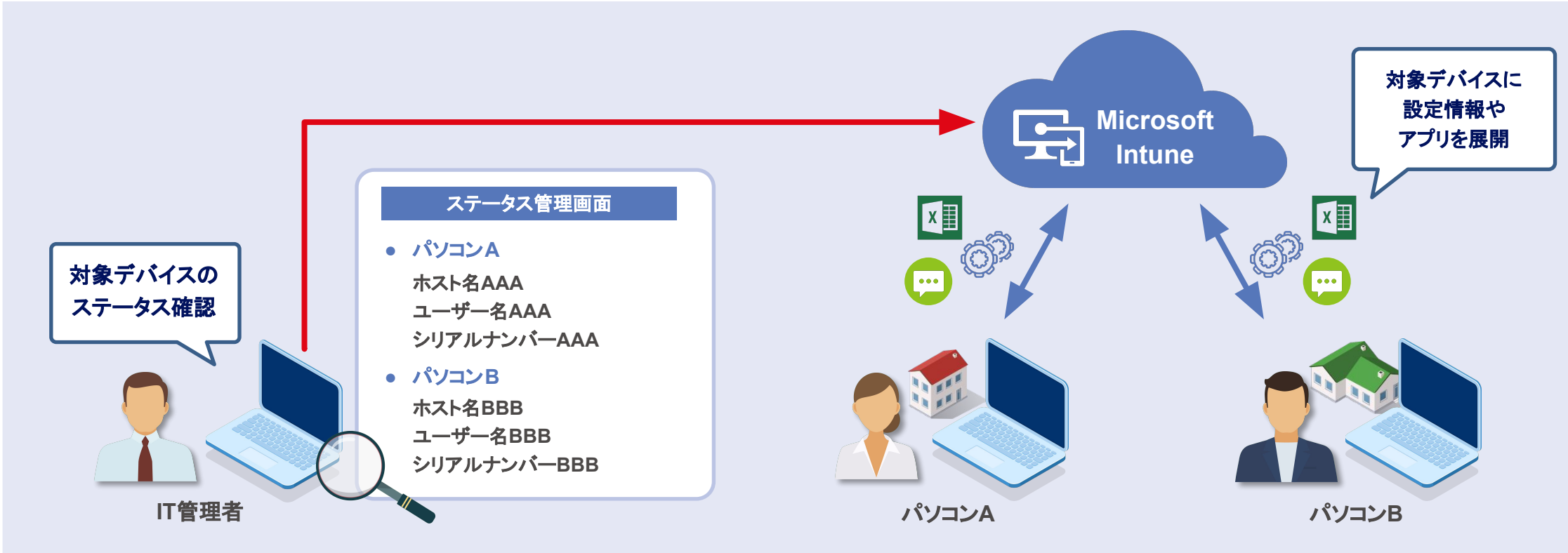
1. 現代的なデバイス管理とは？　～リモート管理～

リモート管理の主な機能

- ステータス確認
- OS設定変更
- アプリ配信

メリット

- 対象デバイスに一括設定が可能
- Active Directoryのようにポリシー制御が可能
- アプリ配信が可能
- デバイスのステータス確認が可能



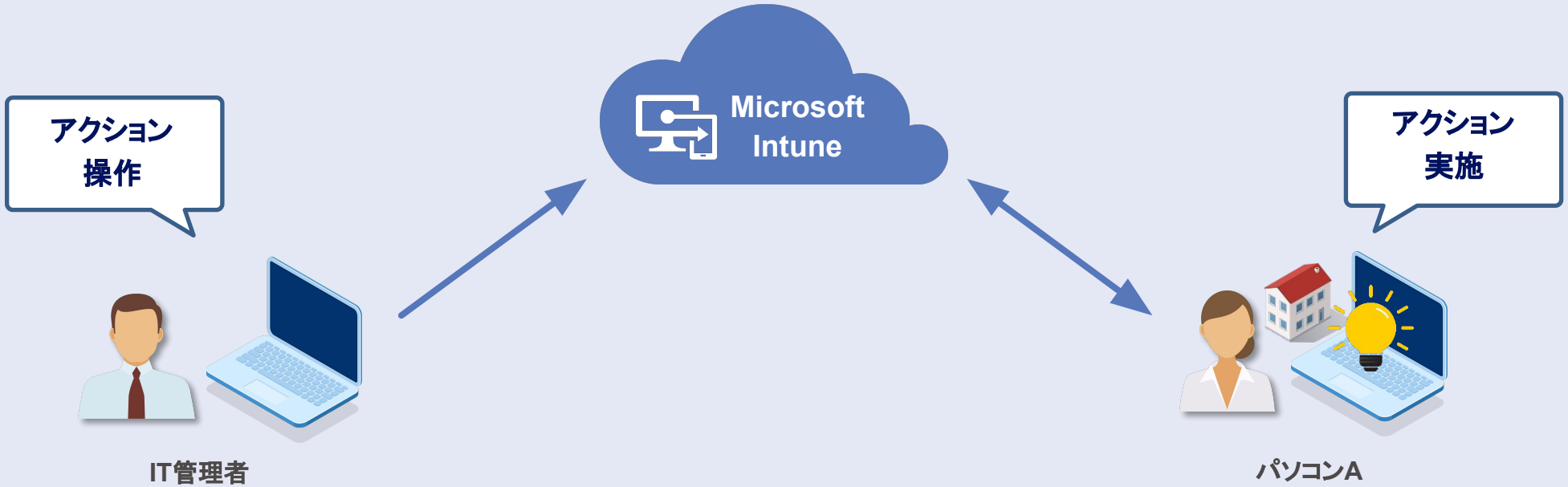
2. 現代的なデバイス管理とは？　～リモート操作～

リモート操作の主な機能

- リモートワイプ
- パスワードリセット

メリット

- どこからでもリモート操作が可能
- ワイプはデバイス紛失時にデータ漏洩を防ぐのに効果的



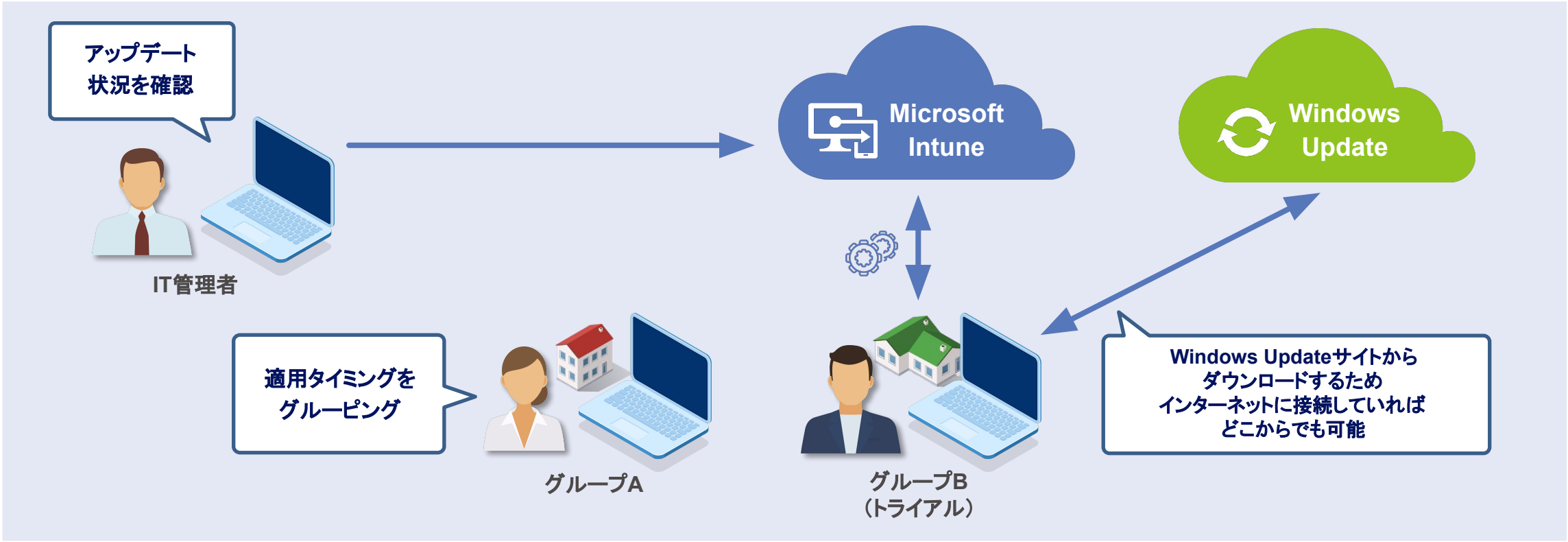
3. 現代的なデバイス管理とは？　～パッチ処理～

パッチ処理の主な機能

- WinUpdateからダウンロード
- アップデート適用タイミングをグループごとに設定
- 適用状況をリモートから確認

メリット

- サポート切れのOSバージョンの状態を防ぐセキュリティリスクの回避
- 動作検証前の更新プログラムはダウンロードさせないことでトラブル回避



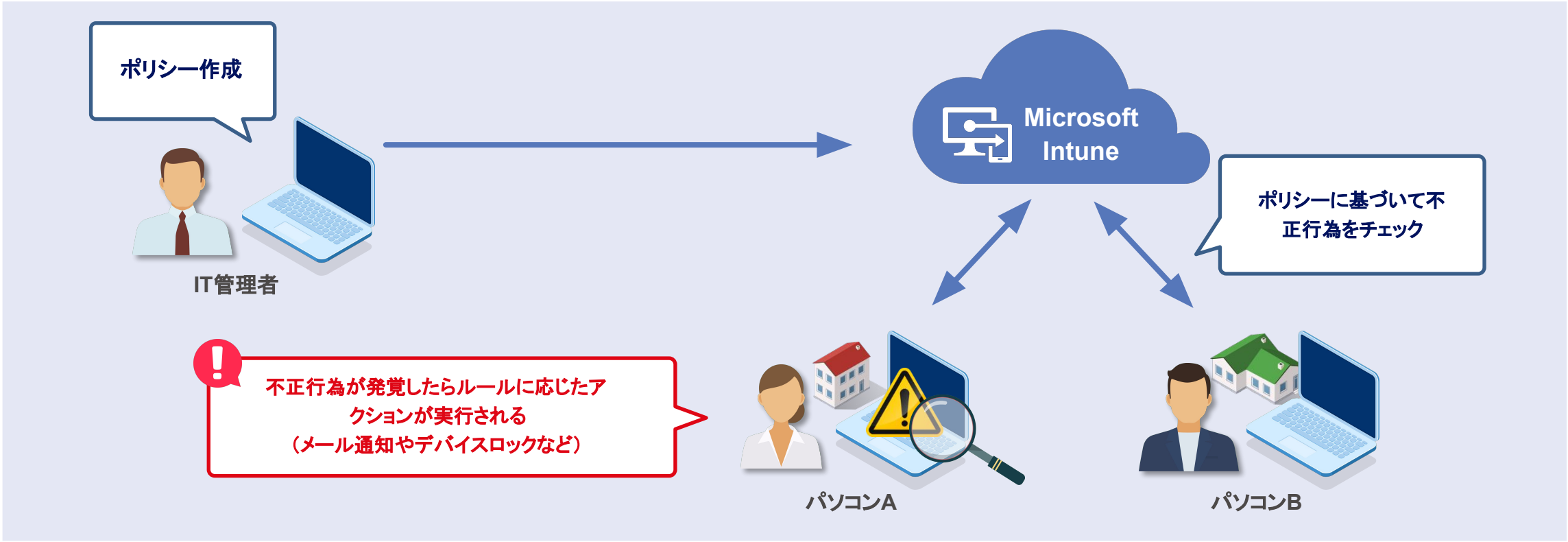
4-1. 現代的なデバイス管理とは？　～セキュリティ強化①～

コンプライアンスチェック機能

- 利用デバイスのチェック機能
  （OSバージョン、ディスク暗号化など）
- 違反時にアクション設定
  （メール通知、デバイスロックなど）

メリット

- デバイスの不正行為を管理してセキュリティ対策
- 不正行為を確認したデバイスにはペナルティで再不正を抑止



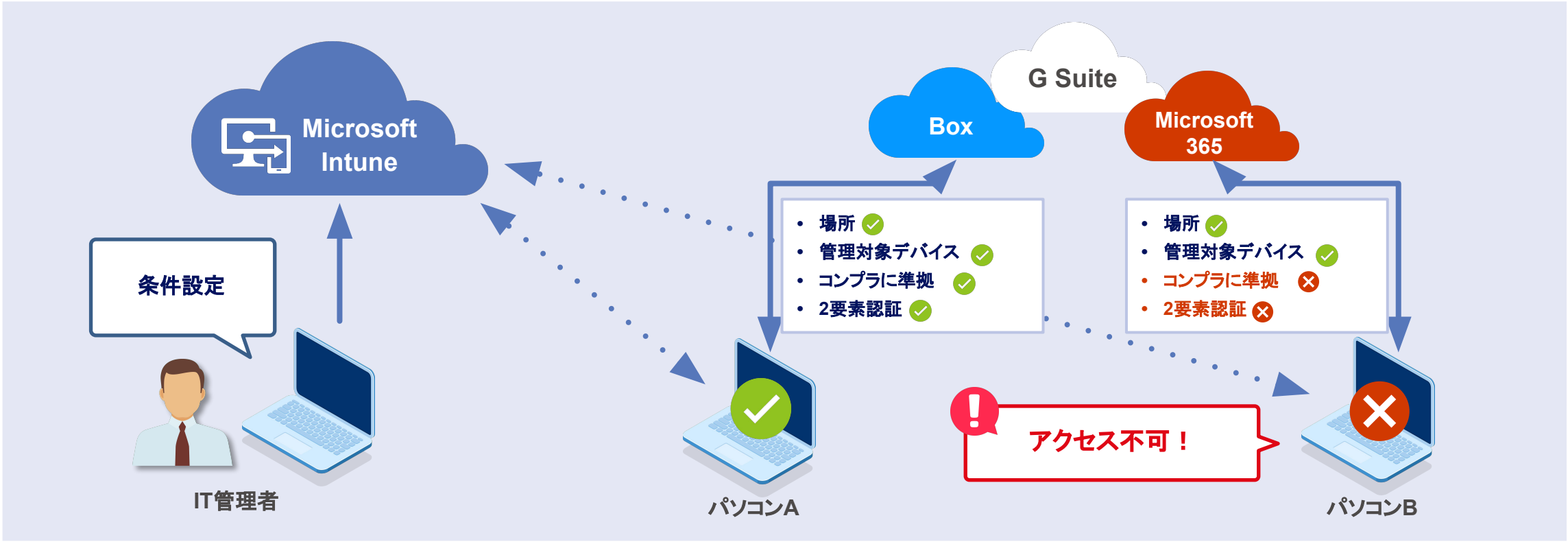
4-2. 現代的なデバイス管理とは？　～セキュリティ強化②～

アクセス制御の機能

- ID/場所/デバイス/リソースを条件にアクセス制御が可能
- 多要素認証の設定が可能

メリット

- IDパスの不正利用から守る
- 安全なデバイス（条件をクリアしたデバイス）のみアクセスさせ、セキュリティを向上



アイエスエフネットは、

さまざまな課題にこたえるための、ITソリューションを提供しています。

貴社の経営課題を抽出し、解決策となるITソリューションの

導入、運用、保守に至るまで一気通貫で全力サポート。

ITに関するお困りごとは、弊社担当にご相談いただくか、

下記のURLやQRコードよりお問い合わせください！

弊社サービスサイトはこちら　»»　https://www.isfnet-services.com/

当資料に掲載されている内容、お問い合わせ先、サービス・製品の価格、仕様、その他の情報は、発表時点の情報です。
その後変更となった際、ダウンロードのタイミングによっては旧情報が含まれる場合があります。あらかじめご了承ください。