【Microsoft Intune】サービス概要

2025年9月30日

改訂履歴

版数	発行日	改訂内容
第1版	2025年5月31日	初版発行
第2版	2025年9月30日	スライド26:価格表記を削除

本資料の内容は 2025/9/30 時点のものです。製品のアップデートにより変更となる場合がございます旨ご了承ください。

Agenda

1. 前提情報
    1. 用語集
2. Microsoft Intuneとは
    1. Intuneが必要とされている背景
    2. Microsoft Intuneとは
3. Microsoft Intuneの基本機能
    1. 基本機能① MDM
    2. 基本機能② MAM
    3. 基本機能③ セキュリティポリシー
    4. 基本機能④ 条件付きアクセス
4. 導入メリットとポイント
    1. 導入メリット
    2. 導入時の注意点
5. ライセンスのプラン比較
    1. ライセンスのプラン比較/選定方法
6. シナリオ別の活用方法
    1. ①会社支給PCの一元管理とセキュリティ強化
    2. ②BYOD端末（スマートフォン）からの安全な業務アクセス

1. 前提情報

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
1	境界型セキュリティ	PCやサーバーを社内で結んでいるネットワークと、外部ネットワークとの「境界線（ペリメータ）」にファイアウォールやIPSなどのセキュリティ措置などの、「社内と社外の接点で侵入を防ぐことで、“社内”の安全性を保つ」という発想に基づいて行われるセキュリティ対策のことを指します。
2	ゼロトラスト	社内外のネットワーク環境における、従来の「境界」の概念を捨て去り、守るべき情報資産にアクセスするものはすべて信用せずにその安全性を検証することで、情報資産への脅威を防ぐというセキュリティの新しい考え方です。
3	エンドポイント	コンピューター ネットワークに接続してそのネットワークとの間で情報を交換する物理的なデバイスのことです。エンドポイントの例としては、モバイル デバイス、デスクトップ コンピューター、仮想マシン、組み込みデバイス、サーバーなどがあります。 本資料で記載がある「クラウドベースのエンドポイント管理ソリューション」とはクラウド環境を利用して様々なデバイスやプラットフォームのデバイスを管理・保護するサービスであることを指しています。
4	インベントリ	資産の台帳や目録のことで、情報システム分野ではパソコン、サーバー、ネットワーク機器、プリンターやソフトウェア等、情報システムに関連するすべての項目をまとめた、IT情報資産の台帳・目録のことを意味します。
5	ABM（Apple Business Manager）	Apple Business Manager（以下、ABM）は、企業のIT管理者がApple製デバイス、アカウント、そしてコンテンツを統合管理できるWEBポータルサイトです。費用は無料で利用できます。

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
6	ADE（Automated Device Enrollment）	自動デバイス登録機能です。ABMの機能の一つであり、Appleが提供する企業向けのiOS端末導入支援サービスです。 ADEを利用すれば、一台一台行うべきキッティングを一括で行え、端末導入時の作業を簡略化できます。 また、自動的にMDMの管理下に置けます。ADEを活用することで、端末の導入コストを大幅に削減できます。
7	BYOD（Bring Your Own Device）	個人が所有しているPCやスマートフォンなどのデバイスを業務に利用する形態のことを指します。 近年リモートワーク化が進み、BYODの需要は高まっています。
8	Windows Auto pilot	企業が新しいWindowsデバイスを導入・初期設定する際に、手作業を減らして効率的に自動構成を行うためのMicrosoftのクラウドベースの機能です。従業員が新しいPCを初めて起動したときに、自動で企業のポリシーや設定、アプリケーションが適用され、すぐに業務利用できる状態にすることを目指します。
9	アプリ保護ポリシー（App Protection Policy：APP）	Intuneで管理された（または管理されていない）デバイス上のアプリケーションに対して、 データの保護ルールを適用するためのポリシーです。 BYODにモバイルアプリだけ保護をかけたい場合や、デバイス全体のMDM登録は避けつつ、業務アプリのデータ流出を防止したい場合に活用されます。
10	MFA（多要素認証）	システムやサービスのログイン時に、下記の3つの認証要素の中から2つ以上の認証要素を活用して、認証を行うセキュリティ方法を指します。 知識情報…パスワードやPIN、秘密の答えなど「本人が知っている情報」 所持情報…スマートフォンやセキュリティトークンなど、ユーザーだけが物理的に所持している物の情報。 生体情報…指紋認証や顔認証・音声認証など、ユーザーの身体的特徴に基づく情報。

2. Microsoft Intune とは

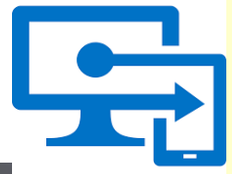
2.1. Microsoft Intuneが必要とされている背景

近年、リモートワークの普及、クラウドサービスの一般化により、企業のIT環境は急速に進化しています。
社員が社内外の多様な場所から、PC・スマートフォン・タブレットなど複数のデバイスを使って業務を行うようになったことで、従来の境界型セキュリティや手動によるデバイス管理では対応しきれない課題が顕在化しています。

現代のIT管理における主な課題

働き方の多様化	デバイス管理の複雑化	セキュリティリスクの増加	従来の管理手法の限界
• リモートワークやハイブリッドワークの普及 • 社外からの業務システムアクセスが常態化	• 従業員の所有する端末（BYOD）対応 • WindowsPCだけでなく、iOS、Androidなどマルチ OS環境への対応	• 不正アクセス、情報漏洩、マルウェア感染のリスクが拡大 • 物理的に管理できないデバイスの増加	• Active Directoryやオンプレミス中心の管理・運用では、クラウド時代のスピード・柔軟性に対応できない

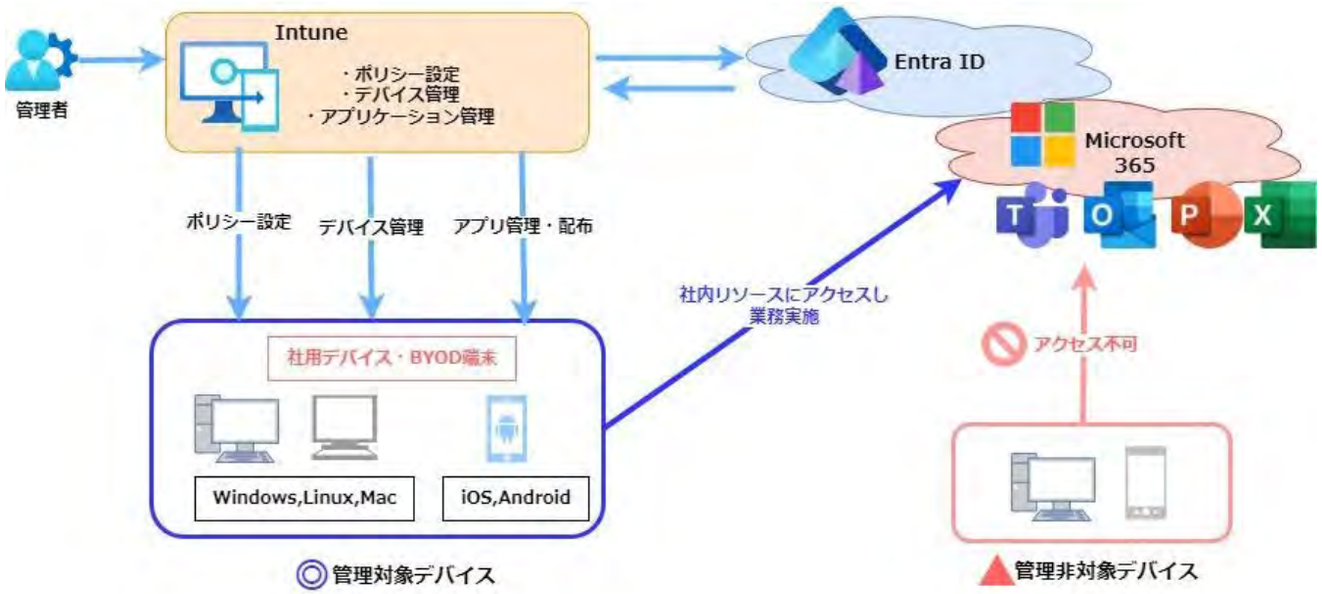
これらの課題に対処するためには、**「すべてを信頼せず、常に検証する」ゼロトラスト セキュリティモデル**に基づいた対策が必要です。
企業は、あらゆる場所・端末からのアクセスを前提とした、柔軟かつ強固なIT管理基盤を求められています。



Microsoft Intune は、こうした背景の中で登場した**クラウドベースの統合エンドポイント管理プラットフォーム**です。
ゼロトラストを支える仕組みとして、従業員の多様な働き方を支援しながら、企業資産の保護と運用効率の向上を実現します。

2.2. Microsoft Intune とは

Microsoft Intune（以下、Intune）は、クラウドベースの統合エンドポイント管理ソリューションです。
従業員が**どこからでも、どのデバイスからでも、安全に業務を行えるように**、デバイス・アプリ・セキュリティの一元管理を可能にします。
Intuneは、ユーザーやデバイスの状態をリアルタイムに検証し、必要に応じてアクセス制御やポリシー適用を自動で実施します



主な特徴

クラウド管理
インターネット経由で、社内外問わずデバイスを一元管理
マルチデバイス対応
Windows、macOS、 iOS、 Android をサポート
セキュリティポリシーの配布
パスワード設定や暗号化、ウイルス対策などをリモートで設定
業務アプリの配布と更新
Microsoft 365 や業務用アプリを自動配信・管理
条件付きアクセス（Entra IDと連携）
準拠していないデバイスからのアクセスを制御

これは、「常に検証し、最小権限でアクセスを許可する」ゼロトラストのアプローチそのものであり、
従来の境界型モデルでは実現できなかった柔軟かつ強固なセキュリティ体制を提供します。

このようにIntuneは、働く場所や端末の種類を問わず、ゼロトラスト セキュリティを支える中核的な仕組みとして、
企業のセキュリティと業務効率の両立を実現します。

3. Microsoft Intuneの基本機能

3.1. 基本機能① MDM

機能概要

MDM（Mobile Device Management/モバイルデバイス管理）機能は、企業や組織が**スマートフォンやPCなどのデバイス自体を一元管理・制御するための機能です。**対象のデバイス（Windows, macOS, iOS, Androidなど）に対して、情報漏洩対策（紛失時の遠隔ワイプ）、セキュリティポリシーの適用（パスコードや暗号化の強制）、管理者の運用負荷軽減（一括管理、リモート操作）等の設定・管理を行うことが可能となります。

MDMでできる主なこと

デバイス登録	Windows / iOS / Android / macOS 等の従業員のデバイスをIntuneに登録し管理対象とします。 自動登録（Auto-enrollment）機能を使えば、Azure AD参加時に自動で登録されることも可能です。
アプリ配布	管理対象アプリを定義し、業務に必要な対象ユーザーに業務アプリ（Outlook,Teams等）を配布
デバイス構成プロファイル	Wi-Fi設定やVPN設定、証明書などの設定を自動で一括で配布
セキュリティポリシーの適用	パスワードの必須化、OSのバージョンの制限など
遠隔操作	遠隔から以下のような操作が可能です。 ロック、会社のデータのみ削除、パスワードリセット
コンプライアンスポリシーの設定・評価	デバイスが組織のルールに合っているかを自動でチェックします。 （OSバージョンやパスワード設定、暗号化状態など）ルールに違反した端末を自動分離・通知します
OSアップデート管理	OSのアップデートスケジュールや適用範囲をコントロールします。特定のパッチだけ適用したり、延期させたりすることも可能です。
インベントリ管理	デバイス情報（OSやバージョン）を一覧で管理

3.1. 基本機能① MDM

メリット

✓ **端末の一元管理が可能**

社内にあるすべてのスマートフォン・タブレット・PCをクラウド上から一元管理することができ、管理台帳が不要になります。これにより 管理者の作業負荷を大幅に削減できます。

✓ **情報漏洩リスクを低減**

・紛失・盗難時に遠隔でロック／初期化（ワイプ）が可能です。
・BYOD(個人端末)でも会社データのみ削除できる仕組み（ワイプ）
・パスコード強制、スクリーンショット禁止、保存先制御などで社内データを防御

✓ **業務アプリ・設定の自動配布**

・必要なアプリや構成（Wi-Fi設定、証明書、VPNなど）を自動で配布
・キッティングの工数削減、IT部門の省力化
・入社・異動時の対応が迅速かつミスが減る

✓ **OSアップデートや資産情報の見える化**

・各端末のバージョン状況や利用状況を可視化し、セキュリティホールの把握が容易になります。
・アップデートの延期や強制も可能で、企業

✓ **セキュリティポリシーの徹底適用**

・利用者が勝手に設定を変えることを防止
・デバイスの状態（OSのバージョン、ロックの有無など）に応じて業務利用の許可/ブロックを自動制御（コンプライアンス管理

✓ **BYOD対応も可能（MAM併用）**

・個人端末に業務アプリのみを配布し、業務データだけを制御（プライバシー配慮）
・社用端末と私用端末を柔軟に混在管理することができます

ポイント

MDMは「企業の情報資産を守りながら、働き方の自由度を高める」ための基盤です。主に情報漏洩リスクの最小化、管理者の管理工数削減、安定したモバイル運用の実現を行うことができ、テレワークやBYODが進む今、導入を検討すべきソリューションと言えます。

3.1. 基本機能① MDM

Microsoft製品との連携

Microsoft Intuneは、単体でのデバイス管理にとどまらず、他のMicrosoft 365製品やセキュリティサービスと連携することで、より強力で一貫性のあるエンドポイント管理・セキュリティ対策が可能です。以下は主要な連携例とその効果です。

内容	説明
Microsoft Entra IDとの連携	Intuneと連携することで、**条件付きアクセスを活用することが可能。** 例：コンプライアンスに準拠していないデバイスからは、Microsoft 365や業務アプリへのアクセスを自動でブロックするなど、セキュリティポリシーを一貫して適用。
Microsoft Defender for Endpoint との連携	• Intuneが管理するデバイスと、Defenderが検出した脅威情報を統合。 • 脅威レベルが高い端末は、自動的に「非準拠デバイス」として判定し、アプリやデータへのアクセスを制限。 • エンドポイントのセキュリティ対策とアクセス制御を連動させることで、ゼロトラストセキュリティを実現。
MAM（モバイルアプリケーション管理）との併用	• 個人所有デバイス（BYOD）に対しては、MDMではなくMAM（アプリ単位の制御）を適用。 • 業務アプリ（Outlook, Teamsなど）内のデータは保護され、**ローカル保存やコピー&ペーストを制限**。 • デバイス登録不要で業務利用が可能になり、プライバシーとセキュリティを両立。

このようにIntuneは、**Microsoftの他のセキュリティ・ID管理ソリューションと密接に連携**することで、企業の多様なデバイス環境に対し、安全性と運用効率を両立する強力な統合管理基盤を提供します。

3.2. 基本機能② MAM

機能概要

MAM（Mobile Application Management /モバイルアプリケーション管理） とは、**デバイス全体ではなく、「業務アプリ単位」でセキュリティ制御を行う仕組み**です。 Intuneを使用して、スマートフォン、タブレット、ノート PC などの会社のデバイスとユーザーの個人デバイスの両方で、アプリ レベルで組織のデータを保護することができます。デバイスを管理対象にしなくても、業務用アプリだけにポリシーを適用したり、個人データと会社データを分離して管理できるため、特にBYOD（私用端末）のように、社員の個人スマホやタブレットで業務アプリを安全に使いたいケースに有効です。

MAMでできる主なこと

管理者は以下のような操作をIntune管理センターから実施することが可能です。

機能カテゴリ	内容
アプリの構成	業務アプリに対してサインイン方法、起動時のパスコード、保存先などを自動で適用させます。
アプリの保護ポリシー（APP）適用	Intuneのアプリ保護ポリシーにより、業務用アプリ内のデータに対し、コピー＆ペースト、保存、スクリーンショットなどの操作を制限できます。 個人のスマートフォンでも業務データの情報漏洩リスクを大幅に低減します。
アプリの監視と更新	アプリの利用状況の可視化、監視と更新が可能。必要に応じ最新版へのアップデートも可能
業務データ分離	業務データと個人データをアプリ内で分離して管理が可能。BYOD利用時にもセキュリティを担保できる。
選択的ワイプ	デバイス単位でなく、特定の業務アプリのみ削除が可能

3.2. 基本機能② MAM

メリット

✓ **BYODに最適**
・端末全体ではなくアプリ単位で業務データのみを保護できます
（アプリ保護ポリシー：APP）
・従業員のプライバシーを保護しつつ、セキュアな業務環境を提供します

✓ **情報漏洩リスクを低減**
・業務データのコピー／ペースト、保存、スクリーンショットなどの操作を制御可能
・業務データの自動暗号化やアプリコンテナ化で、個人データと厳格に分離

✓ **柔軟なセキュリティポリシー適用**
・組織のセキュリティポリシーに応じて、アプリごとに制御ポリシー(APP)を細かく設定可能
・利用状況に応じて制御を動的に変更可能
（例：ネットワーク状況により制限強化

✓ **選択ワイプ可能**
・退職や紛失時に、端末全体を初期化しなくても、業務データ（アプリ）だけ遠隔で削除することが可能であるため、**従業員に対する影響が最小限**に抑えられ、BYODでも運用しやすいのが大きなメリットです

ポイント

MAMは、個人端末にも配慮しながら業務データを安全に保護できる柔軟な管理手法です。
「端末ではなくアプリを守る」ことで、BYOD環境でもセキュリティと利便性を両立することができます。

3.2. 基本機能② MAM

Intuneの利用パターン

Intune MAM は、2 つの構成をサポートします。
以下の2つ構成は「どこまで企業が制御したいか」「利用者の端末がどのような所有形態か」によって選び分けます。
特にBYODが普及している現代では、MAMのみの構成でセキュリティと柔軟性を両立させる提案が増えています。

利用構成	説明・適したケース	メリット	注意点
① Intune MDM + MAM	デバイスが Intune に MDM登録済みの状態で、アプリにもMAMを併用。 →会社からの貸与端末や社内で配布するモバイルデバイスを利用する企業向け。業務に特化した端末管理が必要なケースに適しています	デバイス制御（リモートワイプ、パスコードポリシーなど）とアプリ制御を併用可能。セキュリティ面で最も強固	MDM登録が前提なので、従業員の私物端末への適用はプライバシーの観点から慎重に検討が必要。
② MAMのみ（デバイス未登録）	デバイスがIntuneに登録されていない（私物端末など）場合でも、アプリ内データは保護可能。 → BYOD環境、業務委託先や短期契約者などの外部利用者に適しています。	個人の端末を企業が直接管理する必要がなく、プライバシーの懸念が少ない。 導入も比較的容易で、利用者の負担も軽い。	デバイスのネットワーク制御やOSレベルの制御は行えない（例：VPN自動接続やWi-Fi構成など）。必要に応じて条件付きアクセスと併用推奨。

3.2. 基本機能② MAM

対応アプリ

■Microsoft社製アプリ

Microsoft 365（Office）系の主要アプリに対応しています。
以下対応アプリの一部となります

アプリ名	
Outlook	OneDrive
Teams	Office（Word / Excel / PowerPoint）
SharePoint	Microsoft Edge
OneNote	Power BI
Copilot	Planner
Loop	Lens - PDF スキャナー

■Microsoft社以外のサードパーティ製アプリ

一部の企業アプリも、Intune App SDK もしくは Intune App Wrapping Tool を使って MAM に対応しています。

アプリ名	
Zoom for Intune	Acronis Access
Slack for Intune	Akumina EXP
Box for EMM	Board Papers
Adobe Acrobat Reader	Cisco Jabber for Intune
Asana: Work in one place	Citrix Secure Mail
Webex for Intune	DealCloud
Lemur Pro for Intune	Dooray! for Intune
Goodnotes 6	LumApps for Intune

※一部抜粋

（詳細は公式のMAM対応アプリ一覧を参照）

3.3. 基本機能③ セキュリティポリシー

機能概要

セキュリティポリシーとは、**組織内のデバイスに対して統一されたセキュリティ設定を遠隔で適用・管理できるIntuneの機能**です。
管理者は、情報漏洩やウイルス感染、不正アクセスなどのリスクを低減するためのルールを定め、一括で適用・強制することができます。

これにより、**社内外に分散するデバイスのセキュリティ水準を一定に保つことが可能**になります。

主な機能と活用例

セキュリティポリシーでは、次のようなセキュリティ設定やルールを、対象のデバイスやユーザーに対して適用することができます。

機能	内容	活用例
デバイス構成ポリシー	デバイスの基本設定を一括適用	パスワードの強制、画面ロック時間の制御
コンプライアンスポリシー	準拠状況の確認と制限	OSのバージョン制限、ウイルス対策の有無チェック
条件付きアクセス	安全な状態のデバイスだけアクセス許可	非準拠デバイスはTeamsやOutlookへのアクセスを遮断
セキュリティベースライン	Microsoft推奨の設定を簡単に反映（テンプレート設定）	推奨レベルのセキュリティ構成を簡単に反映
エンドポイントセキュリティ	詳細なセキュリティ制御	BitLocker（暗号化）、ウイルス対策、ファイアウォール制御など

ポイント

このように、Intuneのセキュリティポリシー機能を活用することで、管理者は全デバイスのセキュリティ状態を常に把握・維持することが可能となり、人手不足による管理ミスや設定盛れを防ぎつつ、IT運用を効率化することができます。

3.3. 基本機能③ セキュリティポリシー

メリット

Intuneのセキュリティポリシーは、管理の自動化とリスク低減の両立が可能です。セキュリティポリシーの設定を行うメリットは、企業の情報セキュリティ対策・業務効率・管理の観点から非常に大きいです。

導入メリット	内容
情報漏洩リスクの大幅な低減	**紛失・盗難時も業務データを守れる** • 不正アクセスや紛失・盗難時にも、業務データへのアクセスを制限 • アプリ単位・デバイス単位でセキュリティ制御（MAM／MDM） • 条件付きアクセスと連携することで、未承認端末の利用を防止
IT部門による運用効率化	**社用デバイスに統一ポリシーを自動適用** • 個々の手作業をなくし、運用効率が向上 • 違反端末を自動で検出・対応可能（例：準拠していない端末にアラート）
コンプライアンスの強化	**法令・社内規定への確実な準拠** • セキュリティやプライバシー保護に関する社内・法的要件に対応 • 脆弱なデバイス・古いOSの排除が可能（例：OSバージョン制限） • ログを自動で取得し、内部監査対応にも有効
柔軟な働き方とセキュリティの両立	**BYODやリモートワークに対応** • 個人データと業務データを分離管理（業務データだけ遠隔削除） • 場所やデバイスを問わず、安全に業務継続が可能
Microsoft 365との高い親和性	**Teams、Outlook、SharePointなどの利用を安全に制御** • 条件付きアクセスと組み合わせて「安全な状態」でのみ利用を許可 • エコシステム全体で統一されたセキュリティ管理が可能

3.4. 基本機能④ 条件付きアクセス

機能概要

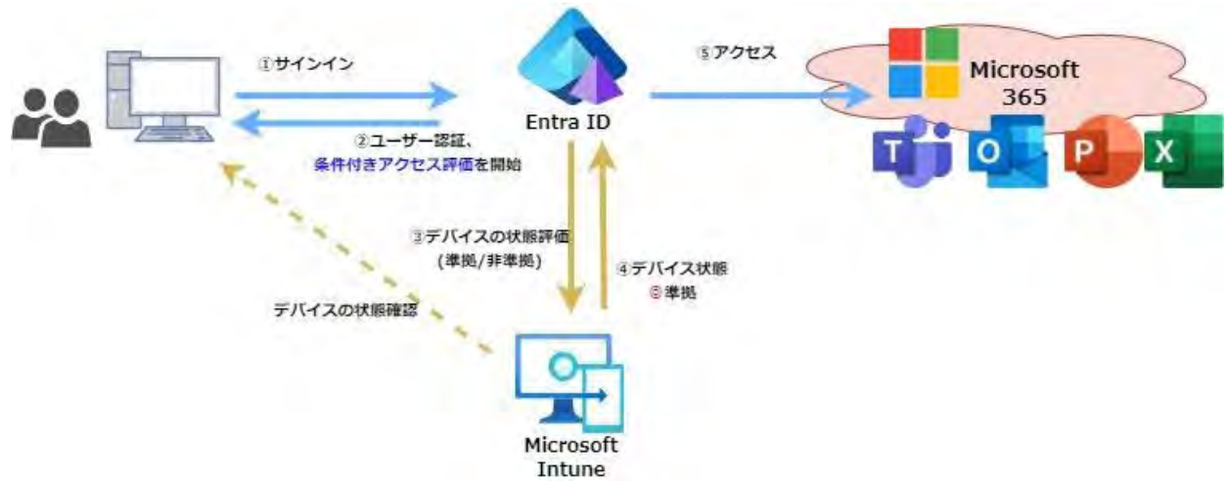
「条件付きアクセス」は**Microsoft Entra IDの機能**であり、**Intuneと連携することで、ユーザーのサインイン時に多角的な条件を評価し、アクセス可否を制御する仕組み**です。
従来の「IDとパスワードが合っていればOK」というアクセス制御に代わり、以下のような条件を柔軟に組み合わせて適用できます。

- **誰が（ユーザー）**
- **どの端末から（デバイス）**
- **どこから（IPアドレス/国）**
- **端末がIntune管理下であり、ポリシーに準拠しているか**
- **MFA（多要素認証）の有無**

これにより、テレワーク・モバイルワークなど多様な働き方に対応しながらも、社内リソースへの安全なアクセスを実現できます。

Entra IDとの連携と制御の流れ

- ユーザーが TeamsやSharePointなどクラウドサービスへアクセスを試みる
- Microsoft Entra ID がユーザー認証を実施
- Entra IDは、設定された「条件付きアクセスポリシー」を評価
- Intuneに対しデバイスの準拠状況を問い合わせ（コンプライアンス違反の有無など）
- 条件をすべて満たしていればアクセス許可、それ以外はブロック・MFA要求など



3.4. 基本機能④ 条件付きアクセス

メリット

条件付きアクセスのメリットは以下となります

導入メリット	内容
セキュリティ強化	**不正アクセスを遮断（ブロック）** ・Intuneと連携し、準拠していないデバイスや不審なIPアドレスからのアクセスを自動で遮断できます。 **→情報漏洩やマルウェア感染のリスクを低減させます。**
柔軟な働き方を支援	**リモートワークでも安全にアクセス◎** ・自宅・外出先・海外など、場所に関係なくポリシーに準拠した端末であれば安全に業務システムへアクセス可能です **→働き方改革の推進に貢献できます。**
管理者の負担軽減	**ポリシーの一括適用が可能** ・ユーザーやデバイスごとに設定をそれぞれに適用する必要がなく、ポリシーの集中管理が可能です。 **→管理ミスの削減と運用効率向上に繋がります。**
ユーザー体験向上	**MFA（多要素認証）などを必要時のみ要求** ・通常のアクセスではMFA不要、リスクの高いアクセス時のみ追加認証を要求するなどができます。 **→ユーザーへの負荷を最小限にできます。**

ポイント

Intuneはデバイスの準拠状況（例：パスワード設定・暗号化・セキュリティ更新の有無など）を評価し、**Entra IDがその情報をもとに条件付きアクセスの可否をリアルタイムに判断します。**

→ セキュリティ要件を満たした端末のみを業務環境に許可することで、組織全体の安全性と生産性を両立できます。

4.導入メリットとポイント

4.1. 導入メリット

改めて、Intuneを導入することによるメリット/導入効果についてまとめました。

セキュリティ強化

・**デバイス・アプリの統合管理**により、不正利用や紛失時の情報漏洩リスクを低減
・**条件付きアクセスで**「安全なユーザー、デバイス」だけに業務アプリへのアクセスを許可
・**アプリ保護ポリシー**により、**個人領域と業務領域を明確に分離し**BYODにも対応

運用効率の向上

・**クラウドベースの管理**で、物理サーバーやVPN不要の運用が可能
・**Windows Autopilot**により、新規デバイスの初期設定・キッティングを自動化
OSやアプリの更新を一元管理し、常に最新・安全な状態を保てる

多様な働き方の支援

・BYODでも業務利用が可能、業務データは分離して保護できる
・場所・時間を問わずアクセス可能な環境を提供し、リモートワークに最適
・iOS、Android、Windows、macOSなど、マルチOSに対応し社内外の端末を一括管理

Microsoft365との親和性

・Microsoft Entra IDと連携し、シングルサインオンや多要素認証を強化
・**Teams、OneDrive、Outlookとの統合運用**により、シームレスな業務環境を実現可能
・Microsoft Defender / Entra / Purview等と連携し、包括的なセキュリティ体制を構築可能

4.2. 導入時の注意点

導入時の注意点については以下の内容を想定しています。

ライセンス要件の確認

・**Microsoft 365 Business Premium や EMS 等のライセンスが必要**
・利用予定の機能に応じたライセンスの精査が重要

ポリシー設計の準備

・**自社のセキュリティ方針に基づいた設定が必要**
・**ポリシーの誤設定により業務停止のリスク**もあるため、段階的適用を推奨

段階的な導入推奨

・全社一斉導入はリスクが高いため、**パイロット導入が望ましい**
・問題点を事前に洗い出し、本番展開へ反映

従業員の説明・同意

・BYOD利用時は特に**プライバシーへの配慮が必須**
・管理範囲、アクセス制限、情報の扱いについての**明文化と周知が必要**

Apple / Google 側の変更影響

・iOS やAndroidの仕様変更により一部設定が非推奨になることもあるため、**継続的な情報収集が必要**

5. ライセンスのプラン比較

5.1. ライセンスのプラン比較/選定ポイント

プランの種類

Intuneには主に3つのプランが用意されています。Intune Plan1が一般的なもので、E3,E5ライセンスにIntuneが含まれています。Plan2とPlan3はアドオンとなり、より高度な管理を希望する場合などに検討を行います。

プラン	機能・内容	含まれるサブスクリプション
Intune Plan1	基本的なデバイス・アプリ管理。MAM/MDM、ポリシー適用、条件付きアクセス、OS/アプリ更新制御など	**Microsoft 365 E3、E5、F1、F3 や※ Enterprise Mobility + Security E3、E5、Business Premium**
Intune Plan2	Plan1に加えて、特殊なデバイス管理・VPNプロファイルの構成、デバイス制限の自動設定など	**Microsoft Intune Plan1 へのアドオン Intune Suite に含まれています。**
Intune Suite	Plan2に加え、リモートヘルプ、特権管理（EPM）、エンドポイント分析、脅威対策強化機能などを含む完全版	**Microsoft Intune Plan1 へのアドオン** 単体購入またはアドオン

※補足　Enterprise Mobility + Security E3/E5 について

「**Enterprise Mobility + Security（EMS）**」は、Microsoft が提供する**セキュリティとデバイス管理に特化したライセンス製品群**です。Microsoft Entra ID P1 または P2、Azure Information Protection、および Microsoft Intune で構成されるスイートです。 フロントワーカーでOfficeはアプリ不要、しかし管理・セキュリティは必要な場合などに適しています。EMSに含まれる主な機能は以下となります。

Microsoft Intune ：MAM,MDM等
Microsoft Entra ID ：ID管理とSSO,MFAによる安全な認証を実現
Azure Information Protection：機密情報を暗号化・制御
Defender for Identity（※E5のみ）：不審なログインや内部不正をリアルタイム検知
Defender for Cloud Apps（※E5のみ）：クラウドアプリの利用状況を可視化し、不正利用（シャドーIT）を検出・制御

5.1. ライセンスのプラン比較/選定ポイント

こちらは各プランごとの機能の比較表となります。

機能 / プラン	説明	Intune	ntune Plan 2	Intune Suite
・基本的なデバイス・アプリ管理 ・クロスプラットフォーム対応 ・エンドポイント分析 ・Microsoft Configuration Manager との連携	企業のエンドポイント管理を効率化し、セキュリティを高めるための基盤を提供します	◎	◎	◎
Intune Tunnel（モバイル向け VPN）	スマホやタブレットなどのモバイルデバイスで、セキュリティを保ちつつ社内システムにアクセスする	✕	◎	◎
特殊デバイスの管理（AR/VR 等）	AR/VRデバイス（HoloLensなど）、通常のモバイル端末やPC以外の特定用途・業種向けの特殊なエンドポイント機器の管理が可能	✕	◎	◎
リモートヘルプ	ヘルプデスク担当者が、社員のPC画面を遠隔で見ながらトラブル対応が可能	アドオン購入可	✕	◎
エンドポイント特権管理	社員に常時管理者権限を与えず、必要なときだけ一時的に付与できる	アドオン購入可	✕	◎
高度なエンドポイント分析	PCやデバイスの状態（遅い・古いなど）をスコアで見える化	アドオン購入可	✕	◎
今後追加される高度な機能	-	アドオン購入可	✕	◎

5.1. ライセンスのプラン比較/選定ポイント

以上のプラン比較をもとに、選定時のポイントを以下に示します。

プラン選定ポイント

Intune Plan 1： 基本的なデバイスとアプリの管理を必要とする企業向け
例：BYODを含む従業員のスマホ・ノートPCを対象に、パスコードの強制やアプリ配布、条件付きアクセスを行いたい企業等

Intune Plan 2： 特殊な業務端末や制限が必要なモバイル環境を運用している企業向け
例：物流業で使用される専用Android端末に対して、VPN自動構成や詳細なOS制限が必要なケース

Intune Suite ： ITサポートやセキュリティ体制が厳格な企業向け。
例：一部の従業員にのみ特定アプリの管理者権限を一時付与、サイバー攻撃リスクが高く脅威検出やログ分析を強化したい等

6.シナリオ別の活用方法

6.1. ①会社支給PCの一元管理とセキュリティ強化

課題

- 新入社員用PCのセットアップに毎回時間と手間がかかる
- 社員が勝手にパスワードを設定しないなど、セキュリティ設定が徹底されない

活用/設定

• Windows Autopilot	工場出荷状態のPCを開封後、インターネット接続だけで自動構成（部署ごとのポリシー適用）
• コンプライアンスポリシー	BitLocker有効化・パスコード必須・OS最新版などを強制
• 条件付きアクセス	準拠デバイスでなければMicrosoft 365へのアクセスをブロックし情報漏洩を防止
• アプリの自動配布	Teamsや業務アプリを自動インストールし、セットアップ工数を削減
• リモートワイプ・ロック	紛失・盗難時に遠隔操作でPCの初期化 or ロックが可能

導入効果

✓ 新入社員のPC準備時間を大幅に削減（管理者が「触らずに構成」可能）
✓ セキュリティポリシーを強制適用できるため、社員の誤設定やルール違反を防止
✓ 紛失・盗難時にも迅速に対応でき、リスクを最小限に抑制

6.2. ②BYOD端末（スマートフォン）からの安全な業務アクセス

課題

- 社員の私物端末（スマホ・タブレット）からメールやTeamsにアクセスしており、情報漏洩の不安がある
- 会社の機密情報が個人の端末に残るリスクを懸念

活用/設定

• 登録方式	BYOD端末は「アプリ保護ポリシー（APP）」を利用し、端末の完全登録は不要
• MAM/ アプリ保護ポリシー(APP)	・デバイスをIntuneに登録せずに、業務アプリ単体で保護することが可能 ・OutlookやTeamsなどM365アプリに対し「コピー・貼り付け・保存」などの操作制御
• 条件付きアクセス	「アプリ保護ポリシーが適用されている場合のみアクセス許可」などのポリシーを設定
• MFA必須	社外ネットワークからのアクセス時には多要素認証を要求し、不正アクセス防止
• リモートワイプ・ロック	紛失・退職時などに、業務アプリ内の会社データのみを遠隔で削除（端末本体や個人データは保持）

導入効果

- ✓ 私用端末でも安全に業務が可能になり、リモートワークを促進
- ✓ 会社の機密情報が端末本体に残らず、持ち出し・流出リスクを大幅に低減
- ✓ 端末登録が不要なため、管理者の負担を軽減しスムーズな導入が可能
- ✓ 管理もデバイス単位の管理でなくアプリ単位での管理となる