【SharePoint Online】IP 制御について

2026年6月30日

改訂履歴

版数	発行日	改訂内容
第1版	2026年6月30日	初版発行

本資料の内容は 2026/6/30 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のでご了承ください。

Agenda

1. 前提情報
    1. 本資料の目的
    2. 用語集
2. 背景
    1. SharePoint Online が外部から狙われやすい理由
    2. SharePoint Online が「単体で完結しない」理由
3. SharePoint Online の IP 制御
    1. SharePoint Online IP 制限の仕組み
    2. 注意点/制限事項/落とし穴
4. Intune によるアプリ制御（APP）
    1. Intune アプリ保護ポリシーとは
    2. SharePoint Online × APP の関係
    3. モバイル / Windows の違い
    4. (補足)Windows 端末の保護（Purview）
5. IP 制御 × APP を組み合わせた設計パターン
    1. 設計判断の軸
    2. ユースケース
6. ライセンスおよび運用ベストプラクティス
    1. 必要ライセンス
    2. 運用ベストプラクティス
7. 設定手順
    1. SharePoint 管理センターでの IP 制御設定手順
    2. Intune 管理センターでの APP 設定手順
    3. 条件付きアクセスの設定手順
    4. 本資料のまとめ

1. 前提情報

1.1. 本資料の目的

目的

本資料は、SharePoint の IP 制御を軸に、アクセス元のネットワークに応じた制御の考え方を整理し、実環境における利用シナリオを想定したセキュリティ設計を理解することを目的としています。

1.2. 用語集

本資料で利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	ID 管理	ユーザーのアカウントや認証情報を一元的に管理し、誰がどのサービスにアクセスできるかを制御する仕組み。
2	条件付きアクセス	ユーザーの状態やアクセス元（ IP /端末など）に応じて、アクセス可否や追加認証を自動的に制御する仕組み。 ※Entra ID P1 以上のライセンス必須
3	Microsoft Intune	企業のモバイル端末やPCをクラウド上で一元管理し、セキュリティポリシーやアプリ配布を行うサービス。
4	Microsoft Entra ID	クラウドサービスへの認証とアクセス管理を行う ID プラットフォーム。
5	フィッシング	偽のサイトやメールでユーザーをだまし、ID やパスワードなどの機密情報を盗み取る攻撃手法。
6	クラウドサービス	インターネット経由でシステムやデータを利用できるサービス形態。
7	IP アドレス	ネットワーク上の機器を識別するための番号であり、通信の送受信先を特定するために使われる情報。
8	Exchange Online	Microsoft が提供するクラウド型メールサービスであり、メール送受信や予定管理を行う基盤。
9	テナント	クラウドサービス上で企業ごとに分離された利用環境の単位。

1.2. 用語集

本資料で利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
10	アクセス回線	ユーザーがインターネットや社内ネットワークに接続するための通信経路。
11	暗号化	データの内容を第三者に読み取られないように変換し、安全に通信・保存するための技術。
12	ローカル	インターネットではなく、端末自身や社内ネットワーク内に限定された環境を指す用語。
13	PIN	端末やアプリの認証に利用される短い数字コードであり、本人確認の簡易手段。
14	サードパーティ	サービス提供元とは別の外部企業や開発者が提供するソフトウェアやサービスを指す用語。
15	Intune SDK	アプリに企業向けのセキュリティ制御（データ保護やアクセス制限）を組み込むための開発用ツール。
16	管理ブラウザ	企業ポリシーに従って制御されたブラウザであり、安全なアクセスを実現するために管理下に置かれるアプリ。
17	モバイル端末	スマートフォンやタブレットなど、持ち運び可能なコンピュータ機器の総称。
18	Windows	Microsoft が提供するパソコン向けのオペレーティングシステムであり、アプリやデバイスを動作させる基盤。

1.2. 用語集

本資料で利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
19	BYOD	従業員が自分の私物端末を業務に利用する運用形態。
20	ISP	自宅や会社の回線をインターネットに接続し、通信サービスを提供する事業者。
21	DLP	機密情報の外部流出を防ぐために、データのコピー・送信・共有などの操作を制御する仕組み。
22	秘密度ラベル	データの機密レベルに応じたラベルを付与し、そのラベルに基づいて暗号化やアクセス制御などを行う仕組み。
23		
24		
25		
26		
27		

2. 背景

2.1. SharePoint Online が外部から狙われやすい理由

SharePoint は業務で広く利用され、機密情報を含むデータが集約されるサービスです。
本ページでは、こうした特性を踏まえて、外部からの攻撃対象となりやすい理由について解説します。

用途と扱うデータ

■用途

- 社内ファイル共有（部門/全社）
- プロジェクト資料の管理
- 契約書/設計書/報告書の保存
- 外部との共同作業（ゲスト共有）

■含まれる可能性のある情報

- 個人情報（顧客/社員）
- 機密資料（契約/価格/設計）
- 経営情報（予算/戦略）

・業務データの集約場所
・日常的に更新・共有される

発生リスク

■漏洩リスク

- アカウント侵害（フィッシング）
- 誤共有（外部公開）
- URL の拡散

■漏洩した場合の影響

- 信用失墜
- 損害賠償
- 競争力低下

外部から狙われやすい理由（まとめ）

SharePoint はインターネット経由でアクセス可能なクラウドサービスであり、社内外から広く利用される一方で、
機密情報を含む業務データが集約される場所でもあります。
そのため、アカウント侵害や誤共有が発生した場合の影響が大きく、攻撃者にとって価値の高い標的となりやすいという特徴があります。

3章以降ではこうしたリスクを踏まえ、SharePoint の IP 制御の具体的な仕組みについて解説します。

2.2. SharePoint Onlineが「単体で完結しない」理由

SharePoint Online (以下：SharePoint)は単体でセキュリティを完結するサービスではなく、
Microsoft 365 の共通機能と組み合わせて利用する前提の設計となっています。本ページではその背景や前提を解説します。

SharePoint の役割

SharePoint は、主に以下の機能を提供するサービスです。

データの保存
社内の重要なファイルを安全に保存します。

ファイル共有
組織内外のユーザーとスムーズにデータを共有します。

権限管理
ユーザーやグループごとに適切なアクセス権限を設定します。

担っていない役割

一方で、以下のセキュリティ制御は SharePoint 単体では提供されていません。

ユーザー認証
本人確認や ID 管理は提供されていません。

端末の安全性評価
端末のコンプライアンスや脅威状態の評価は提供されていません。

アクセス可否の最終判断
条件に基づくアクセス許可/ブロックの判定は提供されていません。

なぜ分離されているか

すべての Microsoft 365 サービスで統一されたセキュリティと利便性を実現するため、必要な機能を共通基盤が担います。

認証
→ Microsoft Entra ID（以下： Entra ID）
ユーザーの本人確認と ID の管理を行います。

端末管理
→ Microsoft Intune（以下：Intune）
端末の安全性や準拠状態の評価を行います。

アクセス制御
→条件付きアクセス
条件に基づきアクセスの可否を判断します。

3. SharePoint Online の IP 制御

3.1. SharePoint Online IP 制御の仕組み

本ページでは、SharePoint の IP 制限がどのように動作し、どの単位で適用されるかについて、左の解説カードと右の処理フローで解説します。

IP 制御とは

- アクセス元の IP アドレスをもとにアクセスを制御します。
- 許可されたネットワークからのみ接続可能です。
- 社外/未許可の回線からのアクセスは遮断されます。

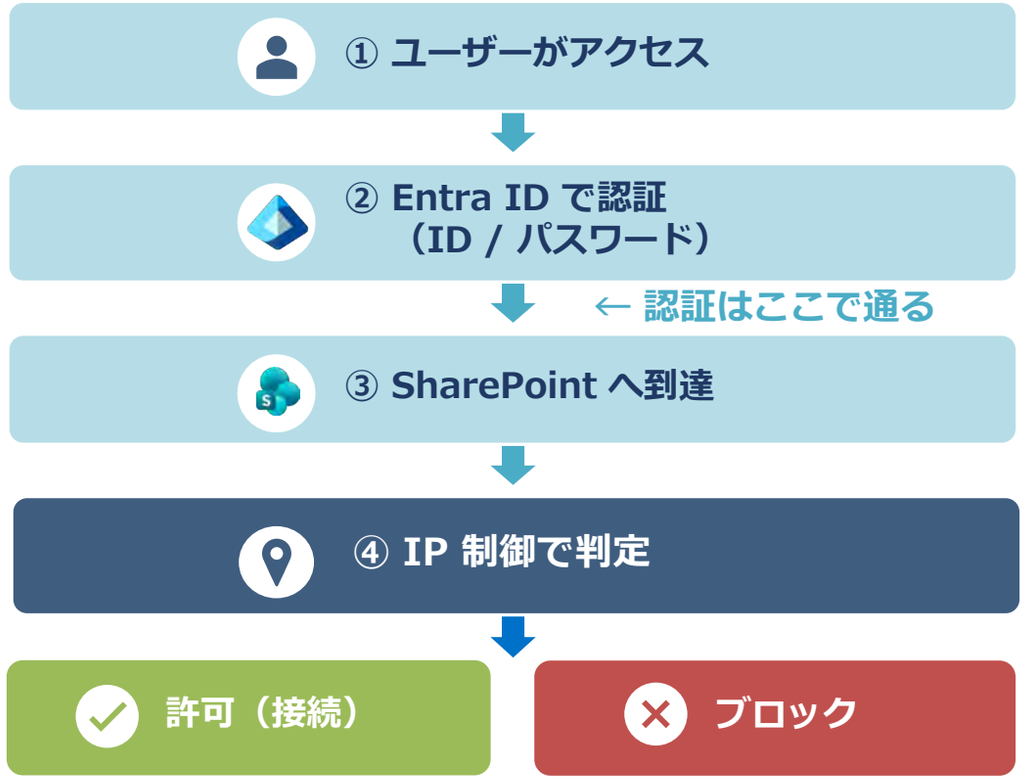
どの単位で制御されるか　重要

- **テナント単位（SharePoint 全体）で一律に適用されます。**
- **個別ユーザー単位での制御はできません。**
- OneDrive / Teams など SharePoint に関連がある
  サービスのファイルにも横断的に適用されます。

ポイント（認証と IP 制御の関係）

IP 制御は、Entra ID による認証が成功した**「後」**に
アクセス元の IP を評価して通信の可否を判定します。
正しい ID とパスワードでも、接続元 IP が違うと接続できません。

アクセスから判定までの流れ



3.1. SharePoint Online IP 制御の仕組み　～どのサービスに影響するか～

IP 制御は、データの実体が SharePoint 上にあるサービスへ横断的に適用されます。判定は「ネットワークの場所」を基準に、認証の後で行われます。

影響を受けるサービス（IP 制御の対象）

SharePoint サイト

チーム/コミュニケーションサイト本体。IP 制御が直接適用されます。

OneDrive for Business

個人用ストレージの実体は SharePoint のため、ポリシーが適用されます。

Teams のファイル

共有ファイルは SharePoint / OneDrive に保存し参照時に適用されます。

その他の参照アプリ

Office on the web や Power Platform など、SharePoint 参照経路にも波及します。

影響を受けにくいサービス（直接の対象外）

Exchange Online（メール）

メールは別基盤のため Exchange 側の制御で管理されます。

Teams チャット/通話

SharePoint を経由しないため対象外です。

「実体が SharePoint 上にあるか」
これらは SharePoint の IP 制御ではなく、各サービス側のアクセス制御（条件付きアクセス等）で個別に管理します。

ポイント

1. **「ネットワークの場所」で判断**
   社内/社外などアクセス回線で可否を決定
2. **認証の“後”に適用**
   正しい ID でも未許可の回線はブロック
3. **テナント単位で横断**
   SharePoint に関連のあるサービス全体へ一律に適用

3.2. 注意点/制限事項/落とし穴

IP 制御は有効なセキュリティ対策のひとつですが、単独ではすべてのリスクを防げるわけではありません。
本ページでは、その注意点/制限事項/落とし穴を整理します。

注意点

ユーザーの安全性は判断できない

IP だけでは、利用者が正当なユーザーかどうかは判断できません。

端末の安全性は判断できない

PC が安全な状態かは分かりません。
マルウェア感染も検知できません。

接続元のIPアドレスが変動するケース

モバイル端末からのアクセス

キャリア回線を利用するケースが多いため、**IP アドレスでの制御が困難**です。

IP アドレスが固定されていないネットワーク環境

会社にて固定のグローバルIPアドレスを所有していない場合、設定が困難です。

社外から VPN を利用しない場合

接続元の IP アドレスを指定できる仕組みがないと社外からは利用できません。

設計上の落とし穴

IP 制御だけでは不十分

ID 侵害（資格情報の盗難）は防げません。
正規 IP からの内部不正も防げません。

多様な働き方とミスマッチ

在宅/ BYOD /モバイル利用などさまざまな働き方が前提の場合、不正利用を防ぐことができません。

対策

1. **多要素認証（MFA）**
   本人確認を追加し「誰か」を担保
2. **条件付きアクセス**
   端末状態や条件で動的に許可
3. **ゼロトラスト**
   場所に依存せず継続的に検証

4. Intune によるアプリ制御（APP）

4.1. Intune アプリ保護ポリシーとは

本ページでは、Intune のアプリ保護ポリシー（APP）の基本的な仕組みと、どのような対象に対してデータ保護を行うのかを解説します。

APP とは

業務アプリ内のデータに対して認証や暗号化を行い、
コピー/保存/共有を制御して情報漏洩を防ぐ仕組みです。

端末管理との違い

従来は端末全体を管理するMDMが使われていましたが、BYOD 環境では適用が難しいため、アプリ単位でデータを守る MAM としての APP が利用されます。

項目	MDM（端末管理）	APP（アプリ管理）
管理対象	端末	アプリ内のデータ
BYOD 対応	✕ 難しい	○ 可能

注意

APP は「データの持ち出しを制限する仕組み」であり、
完全な流出防止ではありません。

制御できる内容

- コピー＆ペースト制御
- アプリ間データ共有制限
- 保存先制限（ローカル NG）
- スクリーンショット制御（※一部）
- PIN 要求

対象となるアプリ

- **Microsoft 製**
  Outlook / Teams / OneDrive / SharePoint
- **サードパーティ製**
  Intune SDK / APP 対応アプリのみ
- **ブラウザ**
  通常ブラウザ → **対象外**
  管理ブラウザ（Edge など）→ 一部対応

4.2. SharePoint × APP の関係

本ページでは、SharePoint と APP のアクセス制御の考え方について解説します。

基本的な考え方

SharePoint のデータは、**APP が適用された安全なアプリ経由でのみアクセスさせる**よう制御することが重要です。
これにより、業務データを安全な領域内に閉じ込めることができます。

SharePoint 、条件付きアクセス単体では不十分な理由

SharePoint のデータは複数のアプリケーションから利用されるため、SharePoint 単体ではなく**関連するアプリ全体に対して制御を適用する必要**があります。

また、条件付きアクセスは柔軟な制御が可能である一方、条件を満たしたアクセスは許可されるため、**ネットワーク（場所）観点での制限が弱くなる場合**があります。

どのように実現するか

この制御は、条件付きアクセスと組み合わせ、**入口と内部の両方を制御する構成**で実現します。

条件付きアクセス（入口の制御）
APP 適用アプリのみを許可

＋

APP（データの制御）
アプリ内データの取り扱いを制御

＋

IP 制御（場所の制御）
許可されたネットワークのみアクセス

具体的な挙動

APP が適用されている場合、SharePoint データへのアクセスは以下のように制御されます。

許可

APP 適用アプリからのアクセスのみを許可

Outlook　Teams　OneDrive　…

ブロック

個人アプリ/非管理ブラウザからのアクセスをブロック

Chrome　Edge　Gmail　…

4.3. モバイル / Windows の違い

APP は、利用するデバイスの種類によって適用できる範囲や効果に違いがあります。
本ページでは、モバイルと Windows の違いを整理します。

大きな違い

APP は、モバイルにおいて高い効果を発揮する一方で、Windows では適用範囲に制限があります。

モバイルの場合

- iOS や Android では、アプリごとにデータ領域を分離する仕組みがあるため、APP による制御が効果的に機能します。
- そのため、コピー制御やデータ共有制限などの機能を厳格に適用することが可能です。

制御操作例


コピー&ペースト


保存先制限


他アプリへの共有


PINコード要求

Windows の場合

- Windows では、ファイルシステムやアプリ間の自由度が高く、完全にアプリ単位でデータを隔離することが難しいため、 APP の制御には制限が生じます。
- また、**ブラウザ経由の利用が多い点**も制御を難しくしている要因です。

制限のある操作例


コピー制御


ローカル保存の完全制御


ブラウザ経由の操作


同期/外部連携の制限

設計への影響

この違いにより、デバイスごとに適切なセキュリティ対策を検討する必要があります。

モバイル：APP 中心の制御が有効
Windows：条件付きアクセスやデバイス管理との併用が必要

APP はすべての環境で同じように機能するわけではなく、デバイス特性を考慮した設計が重要である。

4.4. （補足）Windows 端末の保護（Purview）

APP では Windows は適用範囲に制限がありました。
そのため本ページでは Microsoft Purview（以下、Purview） による Windows 端末の保護について整理します。 Purview についての詳細はこちら

SharePoint / クラウド上のデータ

管理方法：情報保護（秘密度ラベル）

- データを検出/分類し、秘密度ラベルを付与
- ラベルに応じて暗号化・アクセス権を自動制御
- SharePoint / OneDrive / Exchange を一貫保護

Windows 端末（エンドポイント）

管理方法：エンドポイント DLP

- 端末上のファイル操作（コピー/印刷等）を監視
- USB /クラウドアップロード/印刷を制御
- Windows 端末からのローカル漏洩を防止

APP との違い（補完関係）

	APP（Intune）	Purview（Windows）
保護の対象	アプリ内のデータ	端末上の全データ （ファイル・メール等）
管理単位	アプリ単位	ファイル／ラベル単位
主な役割	アプリ間の持ち出し制御	秘密度ラベル＋エンドポイント DLP で保護
適用端末	iOS / Android / Windows（一部）	Windows 端末全体（主に Windows）

設計・運用のポイント

- SharePoint は秘密度ラベル、端末はエンドポイント DLP で住み分ける
- 機密情報の分類（ラベル設計）を適切に行う
- APP と合わせて多層で制御する
- テストモードで影響を確認してから本番適用する

5. IP 制御 × APP を
組み合わせた設計パターン

5.1. 設計判断の軸

IP 制御および APP は、それぞれ異なる観点でアクセス制御を行う仕組みです。
本ページでは、利用環境や要求されるセキュリティレベルに応じた適切な組み合わせ方について整理します。

IP 制御と APP での役割分担

IP 制御は**「どこからアクセスするか（場所）」**を制御し、
APP は**「データをどう扱うか」**を制御します。

社内（信頼できるネットワーク）

IP 制御により
フルアクセス

・社内 IP からはブラウザ含め
フルアクセスを許可

社外（インターネット経由）

APP 適用アプリ
のみを許可

・APP でデータを保護
・ブラウザからはブロック

条件付きアクセスと IP 制御を併用する理由

条件付きアクセスは柔軟な制御が可能ですが、条件を満たしたアクセスは許可されます。
そのため、安全ではないネットワークからのアクセスが許可されるケースがあります。
IP 制御を併用することで、**アクセス元（場所）を強制的に制限することができます。**

アクセス制御の基本観点（Microsoft 365）

アクセス制御の設計では、以下の観点を考慮する必要があります。

利用場所（社内/社外）→IP 制御
どこからアクセスするかを考慮し、適切な制御方法を選択します。

デバイス（管理端末/ BYOD ）→条件付きアクセス
端末の管理状態に応じて、適用可能な制御を検討します。

データの重要度（一般/高機密）→ APP / Purview
扱うデータの重要度に応じて、セキュリティレベルを決定します。

認証コンテキストの活用

→詳しくは公開記事へ

特定の SharePoint サイトに対して、より厳しい条件付きアクセスを適用する仕組みです。

■効果

- サイト単位で **厳格化が可能**
- 条件付きアクセスを **詳細に設定**
- 機密データの **保護を強化**

IP 制御は「場所」、APP は「データ」を制御する仕組みであり、それぞれ条件付きアクセスを組み合わせることで、より実践的なセキュリティ対策が実現できます。

5.2. ユースケース

本ページでは、実際の利用シーンを想定し、 IP 制御と APP を組み合わせたアクセス制御の具体例を解説します。
なお、データ保護については、Microsoft Purview DLP（SharePoint / OneDrive など）がダウンロードまでを制御し、端末上の操作は Endpoint DLPで補完することで、より強固に実現します。

シナリオ①：IP 制御で SharePoint アクセスのみ制御＋条件付きアクセスで全体アクセスを制御（BYOD 許可）

■ 概要

SharePoint は社外から遮断しつつ、BYOD 端末では Teams や Outlook などの業務利用を可能とする構成。

■アクセスイメージ

社内
SharePoint：フルアクセス
その他：条件付きアクセスの制御

社外
SharePoint（OneDrive含む）：アクセス制御
その他：登録済 BYOD のみ許可
Outlook　Teams　SharePoint（OneDrive含む）

■ ポイント

- IP 制御で SharePoint へのアクセスを制限し、社外アクセスを防止
- SharePoint のデータ漏洩リスクを低減しつつ、利便性を確保
- 条件付きアクセスで Microsoft 365 全体を制御し、登録済み BYOD は社外からも利用可能

■ 実現構成

IP 制御 → SharePoint（社内 IP のみ） ＋ 条件付きアクセス → Entra ID（Microsoft 365 全体制御） ＋ 登録済み BYOD → Intune（データ保護）

シナリオ②：認証コンテキスト＋条件付きアクセスにより重要サイトのみ厳格制御（BYOD モバイル端末利用を想定）

■ 概要

特定の高機密サイトに対してより厳格な条件を適用。通常サイトは標準的な制御で、利便性とセキュリティのバランスを取る。

■アクセスイメージ

通常サイト
標準的な制御
（通常のアクセス条件）

高機密サイト（認証コンテキスト適用）
厳格な制御
（ APP 必須＋追加条件）
Outlook　Teams　OneDrive　ブラウザ

■ ポイント

- 重要サイトにだけ厳格な制御を適用し、リスクを最小化
- 認証コンテキストにより、サイト単位での制御が可能
- 業務への影響を抑えながら、機密データを重点的に保護

■ 実現構成

認証コンテキスト → Entra ID（重要サイトのみ） ＋ 条件付きアクセス → Entra ID（ APP ＋強化） ＋ APP 必須 → Intune（データ保護）

6. ライセンスおよび
運用ベストプラクティス

6.1. 必要ライセンス

SharePoint の IP 制御および Intune の APP を利用するためには、それぞれ対応したライセンスが必要となります。
本ページでは、機能ごとに必要なライセンスと、それが含まれる主な Microsoft 365 プランを表で整理します。

機能	必要ライセンス	含まれる主な Microsoft 365 プラン	役割/備考
条件付きアクセス	Microsoft Entra ID P1 以上	Microsoft 365 E3・E5/EMS E3・E5/Business Premium	アクセス可否を判定する中核機能。APP 適用の前提（4.2参照）
APP	Microsoft Intune（Plan1）	Microsoft 365 E3・E5/EMS E3・E5/Business Premium	アプリ内データの制御（コピー制限・保存制御）を実現。
SharePoint IP制御（SharePoint/OneDrive/Teams）	Microsoft 365 ライセンス	Microsoft 365 Business/E3・E5 など	場所による強制的なアクセス制御。

※SharePoint の IP 制御機能は、SharePoint の利用が可能なライセンスを保有していれば、追加ライセンスなしで利用することができます。

6.2. 運用ベストプラクティス

本ページでは、IP 制御および APP を実際に運用する際のポイントと注意点について解説します。

IP 制御の考え方

IP 制御は最小限にする

適用範囲を広げすぎると利便性を損なうため、「本当に必要な範囲」に限定して適用します。

補助的な対策と位置づける

「場所」による制御であり、端末や利用者の安全性は判断しません。他の制御と組み合わせて使います。

APP 運用のポイント

条件付きアクセスとセットで使う

APP 単体では適用を強制できないため、条件付きアクセスと組み合わせて「 APP 必須」の状態を作ります。

対象アプリを正しく設計する

SharePoint だけでなく、Teams や OneDrive など関連するアプリすべてにポリシーを適用します。

導入・運用のコツ

レポートモードで事前検証

「レポート専用モード」でブロックせず影響を確認し、本番適用前の検証で業務影響を最小化します。

ユーザー影響を考慮する

強化しすぎると利便性が低下します。利用シーンに応じてバランスを取ることが重要です。

まとめ

セキュリティ対策は「強さ」だけでなく、「使いやすさ」とのバランスを考慮して設計・運用することが重要です。

IP 制御（場所の制御） ＋ **APP**（データの制御） ＋ **条件付きアクセス**（アクセスの制御） → **組み合わせることで、より実践的なセキュリティを実現します。**

7. 設定手順

7.1. SharePoint 管理センターでの IP 制御設定手順

本ページでは、SharePoint 管理センターでの IP 制御設定手順について解説します。

手順(1)

1. SharePoint 管理センターへ
   テナントの管理者権限を持つアカウントでサインインします。
2. [ポリシー]>[アクセスの制御]へ移動します。
3. [ネットワーク上の場所]を選択します。

次のページへ

7.1. SharePoint 管理センターでの IP 制御設定手順

手順(2)

4. [特定の IP アドレス範囲のアクセスのみを許可する]をオンにします。
5. IP アドレスを入力します。
6. [保存]を選択し完了です。

7.2. Intune 管理センターでの APP 設定手順

本ページでは、 Intune 管理センターでの APP 設定手順について解説します。

手順(1)

1. Intune 管理センターへ
   テナントの管理者権限を持つアカウントでサインインします。

2. 画面左側より[アプリ]を選択します。

3. 画面中央のメニューより[保護]を選択します。

4. [＋作成]を選択します。

次のページへ

7.2. Intune 管理センターでの APP 設定手順

手順(2)

5. [iOS/iPadOS] または [Android] を選択すると、
   [ポリシーの作成] ウィンドウが表示されます。

6. [基本] ページにて APP の
   名前と説明を入力し、[次へ] を選択します。

7. [アプリ]ページにてポリシーの対象となるアプリを選択します。

8. [データ保護] から [条件付き起動] まで
   希望のポリシーを設定します。

9. [割り当て] にてユーザーのグループに
   ポリシーを割り当てます。

10. [作成]を選択し完了です。

詳しくはMicrosoft社公開記事参照

7.3. 条件付きアクセスの設定手順

本ページでは、 APP を利用した条件付きアクセスの設定手順について解説します。

手順(1)

1. Entra 管理センター へ
   テナントの管理者権限を持つアカウントでサインインします。
2. 画面左部より [条件付きアクセス] を選択します。
3. 画面中央より [ポリシー] を選択します。
4. [＋新しいポリシー] を選択します。

次のページへ

7.3. 条件付きアクセスの設定手順

手順(2)

5. [名前] から [条件] まで希望の設定をします。

6. [アクセス制御]の[許可] より [アプリ保護ポリシーが必要] を選択します。

7. [セッション] より希望の設定をします。

8. ポリシーの有効化をオンにし [作成] を選択し完了です。

7.4. 本資料のまとめ

SharePoint の IP 制御や Intune の APP を活用したアクセス制御についてまとめています。
なお、データ保護についてはMicrosoft Purview DLPで補完されます。

おすすめの人・使い方

社内（固定拠点）中心の組織
- 社内ネットワークからのみ許可
- シンプルな構成で運用が可能

社外・BYOD モバイル利用の組織
- APP でアプリ内データを保護
- 利便性とデータ保護を両立

高機密データを扱う組織
- 認証コンテキストで重要サイトを厳格化
- メリハリのある制御が可能

セキュリティ・IT 部門がある組織
- IP 制御と APP を組み合わせ運用
- 効率と安全性のバランスを確保

向いていない人・使い方

社外からフルアクセスしたい組織
- IP 制限で柔軟なアクセスが困難
- 社外利用は別の仕組みが必要

ブラウザ中心で利用する人
- APP の保護はアプリ内が中心
- ブラウザ経由は制御の対象外になりやすい

Windows 端末だけで利用する人
- Windows は APP の制限が多い
- Purview の併用が必要になる場合がある

IP が頻繁に変わる環境の組織
- 固定設定の維持で運用負荷が増大
- モバイル回線や可変 IP に不向き