【Microsoft Entra ID Protection】サービス概要

2026年2月27日

改訂履歴

版数	発行日	改訂内容
第1版	2026年2月27日	初版発行

本資料の内容は 2026/2/27 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 Entra ID Protectionとは
    1. 現代における ID セキュリティの課題
    2. Microsoft Entra ID Protectionとは
    3. Microsoft Entra ID Protectionの全体像
3. Microsoft Entra ID Protectionの機能詳細
    1. 脅威シグナルの収集
    2. リスクの検出
    3. リスクレベルの判定
    4. リスクの調査
    5. リスクベースの条件付きアクセスによる自動対応
    6. ワークロードIDのリスク検出
    7. リスク情報の活用（通知・外部連携）
4. リスクベースの条件付きアクセスにおける設計概要
    1. 設計の全体概要
    2. 設計の構造
5. 利用メリットと注意点
6. 活用シナリオ
    1. シナリオ①：リスクベースMFAによる不正サインイン対策
    2. シナリオ②：ユーザーリスクに基づくアカウント侵害への自動対応
7. ライセンス要件

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	脅威シグナル	不審なサインインや異常挙動、攻撃に関連するイベントなど、リスク判定の材料となる観測データ全般を指す。
2	MFA	パスワードに加えて別の要素（スマホ認証、SMS、アプリ通知など）を用いて認証を行う仕組み。
3	条件付きアクセス	ユーザーの状態、デバイス、場所、リスクレベルなどの条件に基づいてアクセス可否や MFA 要求を制御するポリシー機能。
4	Log Analytics ワークスペース	ログデータを収集・保存・分析するための基盤で、Microsoft DefenderやEntra のログを横断的に可視化・クエリ実行できる。
5	Microsoft Sentinel	クラウドネイティブの SIEM/SOAR プラットフォームで、大量のログから脅威検知・自動対応・ハンティングを行う。
6	SIEM	各種システムログを統合収集し、脅威検知・分析・アラート管理を行うプラットフォーム。
7	Microsoft Entra脅威インテリジェンス	Microsoft が収集・分析するグローバルな攻撃データを基に、不正なIP、サインイン挙動、攻撃手法を評価し、Entra の条件付きアクセスやリスク判定に活用される脅威情報。
8	VPN	インターネット上に仮想的な専用通信経路を構築し、拠点外からでも安全に社内ネットワークへ接続する技術。
9	認証トークン（セッション トークン／更新トークン）	ユーザー認証後に発行される情報で、セッショントークンは短時間のアクセス認可に使用され、更新トークンは新しいセッショントークンの再発行に用いられる。
10	Microsoft Defender for Cloud Apps	クラウドサービスの利用状況を可視化し、シャドーITの検出やデータ保護、脅威検知を行う。
11	匿名IP	送信元の実IPアドレスを隠蔽しているIPアドレスで、不正アクセスのリスク指標として扱われる。
12	Microsoft Defender for Office 365	Exchange Online、SharePoint、OneDrive、Teams を対象に、メールやコラボレーション経路を通じたフィッシング、マルウェア、ゼロデイ攻撃を検知・防御するセキュリティサービス。

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
13	Microsoft Defender for Endpoint	エンドポイント端末を対象に、マルウェア、ランサムウェア、侵入後の不審な挙動を検知・防御し、インシデント対応までを提供するEDR／XDRソリューション。
14	リバース プロキシ	クライアントとサーバーの間に配置され、通信を中継することで、アクセス制御や負荷分散、セキュリティ強化を行う仕組み。
15	中間攻撃者	通信の途中に介入し、データの盗聴、改ざん、なりすましを行う攻撃者。
16	フィッシングサイト	正規サイトを装い、IDやパスワード、クレジット情報などの機密情報を不正に取得することを目的とした偽のWebサイト。
17	ダークウェブ	通常の検索エンジンではアクセスできない匿名性の高いネットワーク領域で、不正取引や攻撃ツールの流通に利用されることがある。
18	プライマリ更新トークン（PRT）	Microsoft Entra 環境で使用される長期間有効な認証トークンで、シングルサインオンや再認証なしのアクセス継続に利用される。
19	API	アプリケーション同士が機能やデータをやり取りするためのインターフェースで、外部連携や自動化の基盤となる。
20	Microsoft Graph API	Microsoft 365 や Entra、Intune などのデータや機能に統一的にアクセスできるREST APIで、管理や連携の自動化に利用される。
21	匿名プロキシ	通信元のIPアドレスを隠蔽するプロキシサーバーで、不正アクセスや検知回避に悪用される場合がある。
22	Torブラウザー	Torネットワークを利用して通信経路を多段暗号化し、送信元の匿名性を高めるためのWebブラウザー。
23	脅威アクター IP	サイバー攻撃に関与したと特定または疑われる攻撃者が使用するIPアドレスで、検知やブロックの判断材料として利用される。
24	機械学習アルゴリズム	データから特徴やパターンを学習し、予測や分類を行う手法で、セキュリティ分野では異常検知や脅威判定に活用される。

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
25	セッション	ユーザーが認証してからログアウトや有効期限切れまでの一連の操作状態を指し、アクセス制御やトークン管理の単位として扱われる。
26	診断設定	Azure や Microsoft 365 のログやメトリックを Log Analytics ワークスペースや Event Hubs などに送信するための構成設定。
27	Intune	デバイスやアプリをクラウドから管理するエンドポイント管理サービスで、ポリシー適用やコンプライアンス制御を提供。
28	Azure ストレージ アカウント	データを格納する Azure のストレージ基盤で、ログ保存やバックアップにも利用される。
29	Azure Event Hubs	大量のイベントデータをリアルタイムで受信・処理するためのイベントストリーミングサービスで、ログ連携や分析基盤に用いられる。
30	SOAR	セキュリティ運用における検知、分析、対応を自動化・オーケストレーションする仕組みで、インシデント対応の効率化を目的とする。
31	Entra Internet Access	インターネット上のWebサービスやSaaSに対する通信を指し、アクセス制御や監視の対象となる。
32	Entra ID Governance	ユーザーIDのライフサイクル管理やアクセス権の適正化を行う仕組みで、過剰権限や不正利用の防止を目的とする。
33	Entra Verified ID	分散型IDを用いて、組織や個人の属性情報を検証可能な形で提示するデジタルIDソリューション。
34	Entra Private Access	社内アプリケーションへのアクセスをインターネット経由で安全に提供する仕組みで、VPNを使わずにゼロトラスト型の接続を実現する。
35	シークレット	アプリケーションやサービスが認証時に自身を証明するために使用する機密情報で、主にクライアント シークレットや API キーなどの形で管理される。

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
36	Microsoft Entra 管理センター	Microsoft Entraに関するユーザー、グループ、認証、条件付きアクセス、セキュリティ設定などを一元管理するための Web ベースの管理ポータル。
37	攻撃キャンペーン	特定の目的を持ち、同一または関連する手法・インフラを用いて、一定期間継続的に実行されるサイバー攻撃の集合体。
38	貼り付けサイト	テキスト情報を貼り付けて URL で公開・共有できるサービス。 不正に取得された ID やパスワードの一覧が掲載される事例があり、資格情報の流通経路として利用されることがある。
39	Workload Identities Premium ライセンス	Microsoft Entra ID においてワークロードIDを対象に、リスクの詳細可視化やリスクベースの条件付きアクセスなどセキュリティおよびガバナンス機能を提供するスタンドアロン（単体型）の有償ライセンス。 Premium 機能を利用するワークロード ID の数に応じてライセンスを保有する形態をとる。
40	サービス プリンシパル	Microsoft Entra ID に登録されたアプリケーションが、特定のテナント内で動作する際に使用される ID。 ユーザーを介さずに認証・認可を行い、Microsoft Graph や各種 API へのアクセスを実現する。

2. Microsoft Entra ID Protectionとは

2.1. 現代における ID セキュリティの課題

クラウド利用やリモートアクセスが一般化した現在、ユーザー ID はビジネスを支える資産であると同時に、主要な攻撃対象となっています。
攻撃者は認証プロセスの弱点を突くため手法を自動化・巧妙化しており、従来のパスワード依存型対策では防御が困難です。
こうした環境変化を受け、組織には**「常にユーザーとサインインの正当性を検証する」ゼロトラストの考え方と、動的なリスク評価にもとづく高度な ID 保護**が求められています。

現代における ID セキュリティの課題

■ユーザーをだます攻撃が巧妙に
メールや偽サイトを使って、ユーザーのログイン情報を盗み取る手口が、より自然で見分けにくくなっています。
その結果、本人も気づかないうちにアカウントが奪われるケースが増えています。

■パスワードに依存した仕組みが限界に
パスワードを使い回しているユーザーはいまだに多く、漏洩した認証情報を悪用したログイン試行が日常的に発生しています。
これらの攻撃は自動化ツールにより大量かつ継続的に実行されるため、パスワードのみの対策では十分な安全性を確保することが困難になっています。

■どこからでもアクセスできる時代のリスク
リモートワークやクラウド利用が当たり前となり、国内外のさまざまな場所からログインされるようになりました。
その結果、「そのアクセスが正しいか」を判断することが難しくなり、誤った判断が不正アクセスにつながる可能性があります。

補足：ゼロトラストとは

ゼロトラストとは、「**あらゆるアクセスを最初から信用せず、毎回安全性を確認する**」という考え方にもとづくセキュリティモデルです。
社内外の区別に頼らず、ユーザーの行動やアクセス状況を踏まえて常に正当性を検証することで、不正アクセスを未然に防ぐ仕組みです。

2.2. Microsoft Entra ID Protectionとは

現代の ID セキュリティでは、利用者の行動やアクセス状況を正確に把握し、危険な兆候を早期に見つけることが求められています。
Microsoft Entra ID Protection は、ユーザーやサインインのリスクを自動で評価し、安全なアクセス運用を支援します。

Microsoft Entra ID Protection とは

Microsoft Entra ID Protection は、組織のユーザーアカウントやサインイン、認証イベントなど ID 全体を対象に、**AI と機械学習を活用して Microsoft が収集する膨大な脅威インテリジェンスおよび認証データを分析し、リスクを自動的に評価**します。
さらに、**不審なログインやアカウント侵害の兆候をリアルタイムで検出し、必要に応じて追加認証やブロックなどの対策を自動適用**します。
これにより、組織は複雑化・高度化する ID 脅威に対して、AI を活用した継続的かつ自動化された防御を実現できます。

特徴

■Microsoftの脅威インテリジェンスを活用したリスク検知
- 兆単位の脅威シグナルから不審な挙動を自動識別
- パスワード漏洩、異常アクセス、攻撃パターンなど を継続的に監視

■条件付きアクセスと連携した自動防御
- リスクの高さに応じて MFA 要求やパスワード変更 を自動適用
- ゼロトラスト運用を“仕組み”として実現

■ユーザーリスクとサインインリスクの可視化
- アカウントそのものが危険か（ユーザーリスク）
- そのサインインが危険か（サインインリスク） を一元的に把握できるレポートを提供

■IT 管理者の負荷軽減
- 異常検知～対応までの自動化により、 手動判断の依存を低減
- 組織全体の ID セキュリティ運用を効率化

2.3. Microsoft Entra ID Protection の全体像

Entra ID Protection は、**収集したシグナルの中から不審な挙動を抽出してリスクとして検出**し、その内容を分析して**リスクレベルを判定**します。
さらに、条件付きアクセスやMicrosoft Sentinelなどの監視サービスとの連携により、**検出されたリスクに対して適切な対応**を実施します。
本図は、脅威シグナルの収集からリスク検出・判定・対応までの一連の流れを示しており、各機能の詳細は次章で解説します。

脅威シグナルの収集・リスクの検出

自動生成シグナル

- 既知の攻撃パターンや異常挙動を基にした自動検知
- Defenderなど他のMicrosoft製品から集まる脅威情報

専門家による分析

- Microsoftのセキュリティ専門チームが、攻撃調査や検証を通じて、自動検知だけでは判断しづらい攻撃パターンや傾向を補完

エンドユーザーからのフィードバック

- ユーザーや管理者がサインインの正当性を確認し、その結果をフィードバックとして検知精度の向上に活用

リスクレベルの判定

リスクの高いユーザー

リスクの高いサインイン

リスクのあるアプリ

ポリシー適用と統合調査

レポート機能による監視・可視化

リスクベースの条件付きアクセスによる自動対応

Log AnalyticsやMicrosoft Sentinelとの統合

外部SIEM製品へのリスク転送

3. Microsoft Entra ID Protectionの機能詳細

3.1. 脅威シグナルの収集

Microsoft Entra ID Protection は、**ユーザーやサインインに関する多様な挙動データを「脅威シグナル」として継続的に収集**しています。
脅威シグナルは、この時点では「危険かどうか」を判断したものではなく、あくまで **後続のリスク検出に利用される観測データ**です。
Microsoft では、脅威シグナルを生成元の異なる3つのカテゴリ（①自動生成シグナル ②専門家による分析 ③エンドユーザーからのフィードバック）に分類し、相互に補完しながら活用しています。

①自動生成シグナル

Microsoft クラウド上で発生する認証・アクセス挙動を対象に、自動的に生成・収集されるシグナルです。

- **サインイン時の接続情報**
  IP アドレスやアクセス元の地理的位置、VPN などの接続元ネットワークの特性
- **利用されているデバイス・クライアントの情報**
  OS の種類やバージョン、使用されているブラウザーやアプリ、PC・モバイルといった端末種別
- **認証プロセスの挙動に関する情報**
  利用された認証方式、認証の試行回数や失敗の頻度、トークンの発行・利用状況
- **人の操作とは異なる不自然なアクセス挙動**
  自動化された認証試行や、短時間に繰り返される多数のアクセス

他の Microsoft セキュリティ製品で観測された情報を、脅威シグナルの判定材料として利用する場合があります。

- **Microsoft Defender for Cloud Apps**
  クラウドアプリ利用時のアクセス挙動に関する情報
  （匿名 IP からのアクセス、機密ファイルへの大量アクセスなど）
- **Microsoft Defender for Office 365**
  メール環境における不審なメール挙動に関する情報
  （アカウント侵害を示唆する疑わしいメール送信）
- **Microsoft Defender for Endpoint**
  端末上での認証情報利用の挙動に関する情報
  （端末上で認証トークンの不正利用が疑われる挙動）

3.1. 脅威シグナルの収集

②専門家による分析

Microsoft のセキュリティ専門チームが、1日約100兆件にのぼるシグナルを処理する大規模な自動分析基盤によって収集・相関分析された情報や、実際の侵害事例の調査結果をもとに、新たな攻撃手法や脅威の傾向を整理・検証し、脅威シグナルとして継続的に反映・更新しています。
なお、この分析には 34,000人以上のセキュリティ専門家から成る Microsoft のグローバルセキュリティ体制が関与しており、これらの知見は、Microsoft Entra ID Protection を含む各セキュリティ製品の検知ロジックへ継続的に反映されます。

- **実際の攻撃事例に基づく分析情報**
  過去に確認された不正アクセスや侵害事例の調査結果
- **新たに確認された攻撃手法や傾向に関する情報**
  既存の自動検知では捉えにくい、新規・高度な攻撃の特徴
- **グローバルで観測された攻撃情報**
  複数の組織で共通して確認された攻撃の動きやパターン

③エンドユーザーからのフィードバック

エンドユーザーや管理者が、自身の利用状況をもとに確認した結果を、検知精度の向上に役立てるためのフィードバックとして取り込む仕組みです。
これらのフィードバックは、他のシグナルと組み合わせて分析され、検知精度の向上や誤検知の抑制に長期的に活用されます。

- **ユーザーによるサインイン確認結果**
  自身が行ったものではないサインインとして報告された情報
- **正当な利用として確認されたサインインの情報**
  問題がなかったとユーザーや管理者が判断した結果
- **管理者による確認・対応結果**
  管理者が実施した調査や対応の結果に基づく情報

ここまでが、Microsoft Entra ID Protection におけるリスク判定の前提となる情報収集のフェーズです。
次に、これらのシグナルを単体ではなく全体で評価し、ユーザーやサインインに不審な兆候があるかを判断する「リスク検出」について説明します。

3.2. リスクの検出

Microsoft Entra ID Protection のリスク検出は、**収集された脅威シグナルを基に、疑わしい/異常なアクティビティを検出イベントとして識別する仕組み**です。 個々のユーザーまたはサインイン イベントにリンクして記録され、後続のリスク評価に利用されます。

リスク検出の対象

「どのアカウントが危険な状態か」と「どのサインインが不正の可能性を持つか」を切り分けて判断するため、リスク検出を2つの観点で整理しています。

ユーザーリスク

ユーザーアカウント自体が侵害されている可能性を示すリスク

- ✓ ユーザーリスクは、ユーザーアカウント単位で評価される。
- ✓ 単一のサインインに限定されず、**複数のリスク検出結果や過去の挙動を含めた総合的な評価**に基づいて判定される。
- ✓ 資格情報の漏洩や継続的な異常なアクティビティなど、**アカウントの信頼性そのものに影響する兆候**が評価対象となる。

サインインリスク

特定のサインイン試行が、正当なユーザーによるものではない可能性を示すリスク

- ✓ **1回の認証イベント（サインイン）単位**で評価される。
- ✓ 認証が成功している場合でも、アクセス元、デバイス、認証方式、挙動などの**文脈情報**を基に不正利用の可能性が評価される。
- ✓ サインイン時点の状況に依存するため、**同一ユーザーであってもサインインごとに評価結果が異なる場合がある。**

※ 本項では、ユーザーおよびサインインを対象としたリスク管理について説明しています。
アプリケーションに対するリスク管理は、別の機能として後述します。

3.2. リスクの検出

ユーザーリスク検出は、**ユーザーアカウント全体の状態を対象**に、アカウントが侵害されている可能性を識別する検出です。
これらのリスク検出は Microsoft Entra 管理センターのレポートから確認することができ、本スライドでは代表的な検出を抜粋して紹介します。

ユーザーリスク検出	検出の概要	検出の例
異常なトークン	通常とは異なる特性を持つ認証トークン（セッション トークン／更新トークン）が使用されていることを示す検出。	見慣れない場所や IP アドレスから、既存のトークンが再利用された。
異常なユーザー アクティビティ	管理者の通常の操作パターンを基に、ディレクトリに対する不審な変更などの異常な挙動を検出。	普段はユーザー管理のみ行う管理者が、突然セキュリティ設定や権限構成を変更した。
中間攻撃者	認証セッションが悪意のあるリバース プロキシを経由している可能性を示す高精度な検出。Microsoft Defender for Cloud Apps などの情報を基に判定される。	フィッシングサイト経由でサインインし、認証トークンが第三者に中継された。
漏洩した資格情報	ユーザーの有効な ID やパスワードが、ダークウェブや貼り付けサイト等で流通していることを示す検出。	外部リークサイトで確認された資格情報が、実在するユーザーのものと一致した。
Microsoft Entra 脅威インテリジェンス（ユーザー）	Microsoft 内外の脅威インテリジェンスを基に、既知の攻撃パターンと一致するユーザー活動を検出。	他組織で観測されている攻撃キャンペーンと類似した操作が確認された。
プライマリ更新トークン（PRT）へのアクセス試行の可能性	Microsoft Defender for Endpoint が検出した情報を基に、端末上で使用される PRT への不正なアクセス試行を示す検出。	侵害された Windows 端末から、トークンの取得が試みられた。
不審な API トラフィック	ユーザーの資格情報を用いた API 利用に、通常とは異なる挙動が確認された場合の検出。	Microsoft Graph API が呼び出され、短時間に大量のディレクトリ情報が取得された。

3.2. リスクの検出

サインインリスク検出は、**1回の認証イベント（サインイン）を対象**に、正当なユーザーによるサインインかどうかを評価する検出です。
これらのリスク検出は Microsoft Entra 管理センターのレポートから確認することができ、本スライドでは代表的な検出を抜粋して紹介します。

サインインリスク検出	検出の概要	検出の例
匿名 IP アドレス	匿名プロキシや Tor、VPN など、接続元を隠蔽する IP アドレスからのサインインを示す検出。	Tor ブラウザーや匿名 VPN 経由でサインインが行われた。
悪意のある IP アドレス	過去の攻撃や不正な挙動と関連付けられている IP アドレスからのサインインを示す検出。	攻撃に使用された実績のある IP アドレスからサインインが行われた。
パスワード スプレー	一般的なパスワードを用いて複数アカウントへのサインインが試行され、正しい資格情報が特定されたことを示す検出。	多数のユーザーに対するログイン試行の中で、特定ユーザーの認証が成功した。
見慣れないサインイン プロパティ	過去のサインイン履歴と比較して、通常とは異なる特性で行われたサインインを示す検出。	これまで使用実績のない国やデバイス、ブラウザーからサインインが行われた。
通常とは異なる移動	地理的に離れた場所で、短時間のうちに行われた複数のサインインを基に検出されるリスク。	日本でのサインイン直後に、短時間で海外からサインインが行われた。
Microsoft Entra 脅威インテリジェンス（サインイン）	既知の攻撃パターンや脅威インテリジェンスと一致するサインイン アクティビティを示す検出。	他組織で観測されている攻撃と類似したサインインが検出された。
検証済み脅威アクター IP	国家レベルやサイバー犯罪グループに関連付けられた IP アドレスからのサインインを示す検出。	攻撃者として知られているIP アドレスから、サインインが試みられた。
機密ファイルへの大量アクセス	機密情報を含む可能性のあるファイルへの大量アクセスが確認された場合の検出。Microsoft Defender for Cloud Apps などの情報を基に判定される。	機密情報を含む、SharePoint や OneDrive 上のファイルが短時間に大量に閲覧・取得された。

※全てのユーザーリスク検出およびサインインリスク検出については、Microsoft 公式サイトをご確認ください。

3.2. リスクの検出

これまでに紹介した各リスク検出は、検出が行われるタイミングによって「**リアルタイム検出**」と「**オフライン検出**」に分類されます。
ここでは、両者の違いと、それぞれの役割について説明します。

リアルタイム検出

- ✓ **サインイン時点で即座に評価されるリスク検出**
- ✓ 条件付きアクセスと連携し、**MFA 要求やブロックを即時適用**
- ✓ 不正なアクセスを**リソース到達前に防止**することを目的とする

例）
- 匿名 IP アドレス（サインインリスク）
- 見慣れないサインイン プロパティ（サインインリスク）
- 検証済み脅威アクター IP （サインインリスク）

オフライン検出

- ✓ **サインイン後に追加分析を行い、評価されるリスク検出**
- ✓ より多くのシグナルを用いて、**侵害の兆候や背景を分析**
- ✓ オフライン検出の結果は、**次回以降のサインイン時**のリスク判定に利用される

例）
- 異常なユーザー アクティビティ（ユーザーリスク）
- 漏洩した資格情報（ユーザーリスク）
- 通常とは異なる移動（サインインリスク）

※ 同一のリスク検出が、リアルタイムとオフラインの両方で評価される場合もあります。

これらのリスク検出の結果は、検出された事象そのものを最終判断とするのではなく、後続の「リスクの評価」において
重要度（深刻度）を判定するための材料として利用されます。次に、検出結果を基に リスクレベルをどのように評価・判定するのか を説明します。

3.3. リスクレベルの判定

前のスライドで紹介したリスク検出は、検出された事象の内容および信頼度に基づいて、リスクレベルを判定します。

リスクレベルとは

- リスクレベルは、検出されたリスクが**実際にアカウント侵害である可能性がどの程度高いかを示す指標**です。
- Microsoft Entra ID Protection では、**機械学習アルゴリズム**を用いてリスクレベルが算出されます。
- 評価結果は、調査や対応の**優先順位付け**や条件付きアクセスによる**自動対応**に利用されます。

リスクレベルの分類

低（Low）

- **通常と異なる挙動はあるが、侵害の可能性は低い状態**
- 一時的な環境変化や新しい利用パターンが原因の場合がある
- **監視を継続し、必要に応じて対応**

中（Medium）

- **不審な兆候はあるが、確証には至っていない状態**
- 複数の異常が確認されているものの、**追加確認が必要**
- 追加認証などにより**正当性を判断**

高（High）

- **アカウント侵害の可能性が非常に高い状態**
- 漏洩した資格情報や、検証済み脅威アクターに関連する検出など、**強い根拠**が確認されている
- **即時の対応が必要**

補足：保持期間

低リスクの検出は、6か月間保持された後、自動的に期限切れとなり、レポートや評価対象から除外されます。
一方、中・高リスクは修復または、誤検知として却下されるまで保持されるため、運用上は定期的にリスク検出をレビューし、対応状況を整理することが推奨されます。

3.4. リスクの調査

Microsoft Entra ID Protection では、検出・判定されたリスクを **「調査」するためのレポート機能**が提供されます。
調査フェーズは、「**本当に侵害なのか**」「**自動対応で十分か**」を見極めるための段階です。
ここで得られる情報は、**●管理者による手動対応** または **●条件付きアクセスによる自動対応** を選択するための判断材料として利用されます。

主な調査レポート

ここでは、検出・判定されたリスクを可視化し、対応方針を決定するために用いられる調査レポートを3つ紹介します。
各調査レポートには、検出されたリスクの内容に加えて、各リスクの**リスクレベル（低・中・高）**が表示されます。

危険なユーザー

アカウントの「状態」を判断する

- ユーザーアカウントが、**現在どの程度危険な状態にあるか**を示す。
- 単一のサインインではなく、**複数の検出結果や履歴を踏まえた総合的な評価**が反映。
- 調査の起点として、「どのユーザーに対応が必要か」を判断するために用いられる。

危険なサインイン

問題となった「事象」を確認する

- 不正の可能性がある **特定のサインイン試行**を示す。
- サインイン時の状況（場所・IP・デバイス・認証方式など）が確認できる。
- 管理者がリスクのあるサインインを確認し、対応を検討するために利用される。

リスク検出

判断の「根拠」を把握する

- 匿名IP、漏洩した資格情報など、**リスクと判断された具体的な検出内容**を示す。
- 危険なユーザーやサインインが**なぜ危険と評価されたのか**を理解するための情報。
- 誤検知の確認や、ポリシー・運用改善の検討時に利用される。

調査では、アカウントの状態・発生した事象・判断の根拠という異なる視点のレポートを組み合わせてリスクを判断します。
これらのレポートは、Microsoft Entra 管理センターから各レポートを確認できます。

3.4. リスクの調査

Microsoft Entra ID Protection では、レポートによる調査結果を基に、自動対応と管理者対応を適切に使い分けることでリスク対応を行います。

■調査

- 危険なユーザー、危険なサインイン、リスク検出の各レポートを確認（環境・リスク状況に応じて週次/月次で確認）
- アカウントの状態、発生した事象、判断の根拠を把握
- 検出されたリスクの内容を整理し、対応判断の材料とする

■対応判断

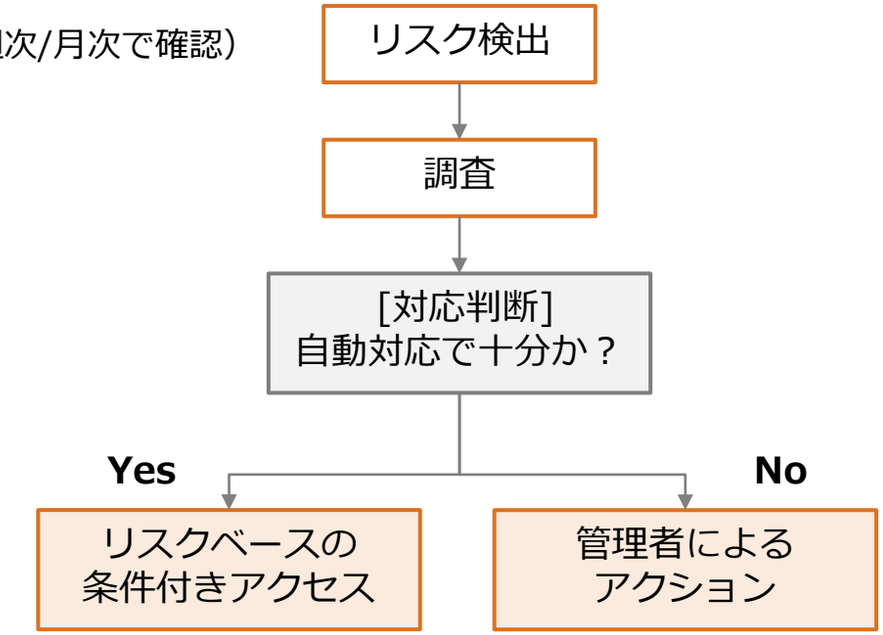
- 調査結果を基に、「自動対応で十分か」を基準に対応方針を判断
- 自動対応で不十分な場合とは、自動的な認証制御だけではリスクを確定できず、管理者の判断が必要なケースを指す。

■自動対応

- **リスクベースの条件付きアクセス**により自動対応
- MFA 要求やパスワード変更などを通じて、ユーザー自身による自己修復を促す

■管理者対応

- 自動対応では不十分な場合は、管理者が調査結果を基に明示的なアクションを行う
  例）パスワード変更の依頼/ユーザー侵害の確認・リスク解除/ユーザーのブロック/MFA の再登録依頼 など



調査のポイント

自動対応や一次対応の後も、管理者はリスク検出などのレポートを確認し、不審な挙動が実際の侵害かどうかを調査したうえで、リスクの状態を最終的に確定します。その結果は、今後の 条件付きアクセス ポリシーの見直し・改善やリスク検知精度向上のための判断材料として活用されます。

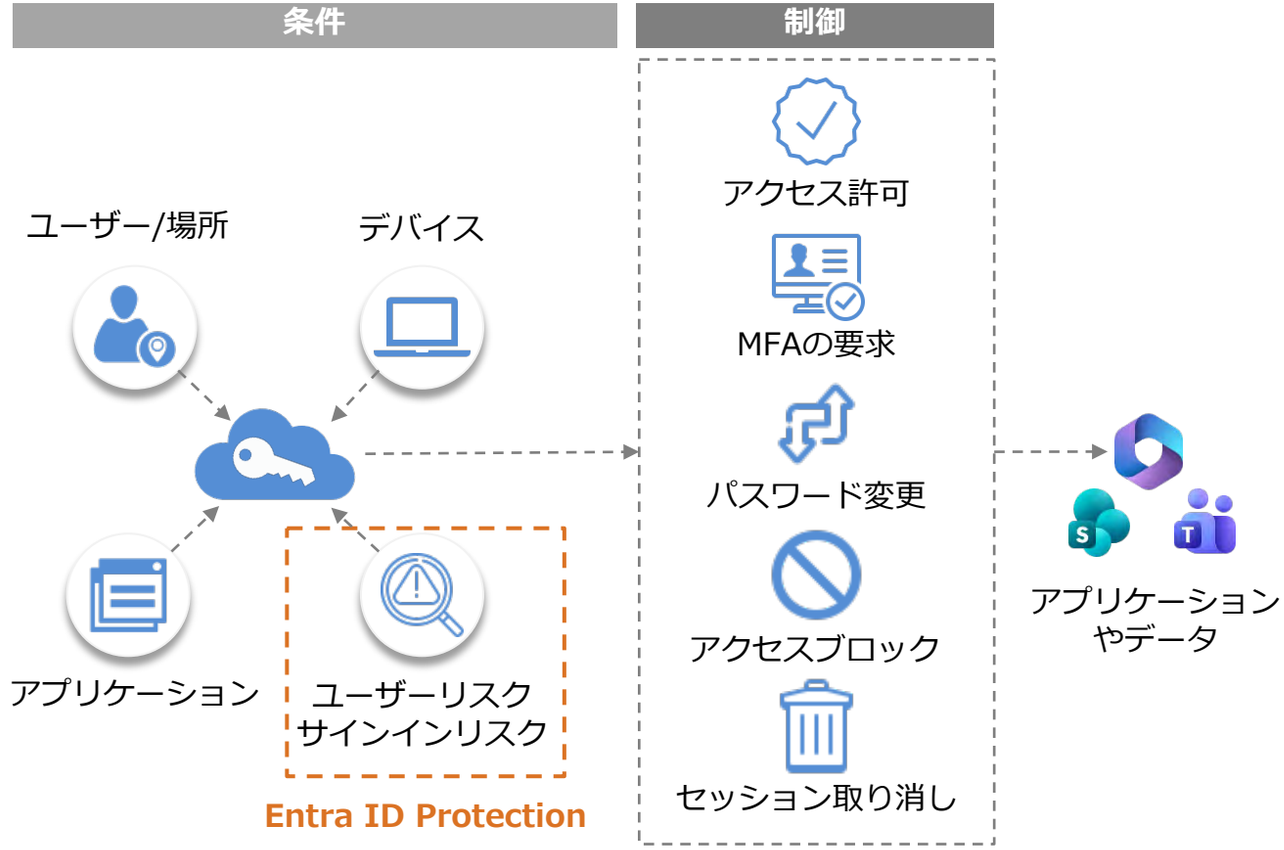
3.5. リスクベースの条件付きアクセスによる自動対応

前項では、検出・判定されたリスクを調査し、「自動対応で十分か」「管理者対応が必要か」を判断する流れを説明しました。
リスク対応をすべて管理者の判断に委ねた場合、対応の遅れにより **不正アクセスや被害が拡大する可能性**があります。
そのため Entra ID Protection では、一定条件を満たすリスクに対しては、即座に自動対応を実行できる仕組みを提供しています。

リスクベースの条件付きアクセスとは

Microsoft Entra ID Protection によって判定された**ユーザーリスクおよびサインインリスクを、条件付きアクセスの「条件」として利用し、**リスクの高さに応じて **認証要件やアクセス可否を自動的に制御する仕組み**です。

条件付きアクセスでは
ユーザー・場所・デバイス・アプリケーション
といった複数の条件を組み合わせてアクセス制御を行います。
その中で Entra ID Protection は、
リスクレベルの判定（低・中・高）を「リスク条件」として提供し、
MFA の要求、アクセスブロックなどの**制御を実行**します。
これにより、**調査 → 判断 → 自動対応** という一連の対応を
管理者の操作を介さずに実現できます。



次章では、リスクベース条件付きアクセスを設計する際の考え方や構造について説明します。

3.5. リスクベースの条件付きアクセスによる自動対応

本スライドでは、リスク判定から条件付きアクセスによる制御、そして自己修復に至るまでの一連の流れを説明します。

条件付きアクセスの流れ

1. ユーザーのサインインが発生
2. サインインリスク/ユーザーリスクを基にリスクレベル（低・中・高）を判定
3. 判定されたリスクレベルが条件付きアクセスの **リスク条件** として評価される
4. 他の条件（ユーザー、場所、デバイス、アプリケーション等）と合わせてポリシーの適用可否が判断される
5. 条件に一致した場合、**アクセス制御が自動的に適用**される

条件付きアクセスでは、リスクレベルを含む複数の条件に基づいて、アクセス制御が適用されます。
このとき適用される制御の内容によっては、**正当なユーザーが要求された操作を完了することで、リスク状態が解消される**場合があります。（自己修復）

自己修復の考え方

自己修復とは、**条件付きアクセスによって要求された操作**（例：MFAの要求、パスワード変更など）を正当なユーザーが完了することで、**リスク状態が解消される仕組み**です。なお、自己修復は、条件付きアクセスで自己修復につながる制御が適用された場合に成立します。

ポイント

- ✓ 不正なアクセスを抑止しつつ、正当なユーザーは自ら状態を回復可能
- ✓ **管理者の手動対応に依存しない**自動的なリスク収束を実現
- ✓ 制御内容によっては、自己修復が成立しない場合がある
  （例：MFA 要求は自己修復可／アクセスブロックは管理者対応が必要）

自己修復の例

海外からのサインインにより「サインインリスク：中」と判定
→ 条件付きアクセスにより **MFA を要求**
→ 正当なユーザーが MFA を完了
→ **サインインを許可し、リスク状態は自動的に解消**

3.6. ワークロードIDのリスク検出

これまでのスライドでは、ユーザーやサインインに対するリスク検出と対応を説明してきました。
Microsoft Entra ID Protection では、同様の仕組みを **アプリケーションやサービス プリンシパル（ワークロード ID）** に対しても提供します。

ワークロード ID とは

- 社内 Web アプリや自動化処理、システム連携用アプリなどの人以外のワークロードが、Microsoft Entra ID 上で IDを持ち、認証・認可を受けて、Microsoft Graph や独自 API などの Entra ID で保護されたリソースへアクセスするための仕組みを指します。
- ユーザー ID と異なり MFA を実行できず、シークレットや証明書を保持する必要があるため、**侵害に気づきにくく悪用されやすい**特性を持ちます。

ワークロード ID のリスク検出

サインイン挙動などを基に、ワークロード ID のリスクを検出します。

- **Microsoft Entra 脅威インテリジェンス**
  既知の攻撃パターンと一致するアクティビティを検出
- **不審なサインイン**
  通常と異なる IP、資格情報の使用など
- **漏洩した資格情報**
  ダークウェブなどで確認された有効な資格情報
- **悪意のある／疑わしいアプリケーション**
  Microsoft Defender for Cloud Appsと連携して判定

リスクの可視化と調査

- Microsoft Entra 管理センターから、ワークロードID用のレポートを確認可能
- ユーザーリスク／サインインリスクと同様に、いつどのアプリがなぜ危険と判断されたかを調査できる

リスクへの対応

- リスクベースの条件付きアクセスと連携することで、高リスクのワークロード ID に対するアクセス制御が可能
  ※リスク検出は標準機能だが、リスクの詳細確認やリスクベースの条件付きアクセスを利用する場合は、専用のWorkload Identities Premium ライセンスが必要
  ※適用可否は、アプリの種類によって異なる

3.7. リスク情報の活用（通知・外部連携）

Microsoft Entra ID Protection の通知機能や外部ツールとの連携を活用することで、検出されたリスク情報を調査・可視化し、迅速な運用対応につなげることができます。

Microsoft Entra ID Protectionの通知機能によるリスク検知の即時把握

- **リスク検知時に管理者へ自動通知メールを送信**し、週間ダイジェスト通知によって一定期間のリスク状況をまとめて確認できます。
- 通知対象のリスク レベルや受信者を指定することで、管理者が早期にリスクを把握し、調査や対応を開始できます。

診断設定によるデータの保存・エクスポート

- Microsoft Entra ID の診断設定を構成することで、リスクデータを用途に応じた宛先へエクスポートすることが可能です。
- Log Analytics ワークスペース、Azure ストレージ アカウント、Azure Event Hubs などへエクスポートすることで、**リアルタイムでの分析や可視化、長期的なデータ保管が可能**となります。

Microsoft Sentinel との連携

- リスクデータを Sentinel に取り込み他のセキュリティログと 相関分析することが可能です。
- Sentinelの機能である、**ダッシュボード表示や自動対応（SOAR）に活用**することが可能です。

Microsoft Graph API によるデータ活用

- リスクデータをMicrosoft Graph APIで取得することができます。
- 取得したデータは **SIEM や独自分析基盤で加工・分析**が可能です。

4. リスクベースの条件付きアクセスにおける設計概要

4.1. 設計の全体概要

本章では、Microsoft Entra ID Protection を活用したリスクベースの条件付きアクセス設計の全体像を説明します。
リスクベースの条件付きアクセスは、単に強い制御を適用する仕組みではなく、検知されたリスクに応じて適切な対応を自動的に選択することを目的としています。
そのため、何を守るのか、どのリスクを対象とするのか、どこまでを自動対応とするのかを整理したうえで、段階的かつ一貫性のある設計を行うことが重要です。以下に、設計時の基本的な検討フローを示します。

0. 設計目的の整理	1. 対象ユーザー・アクセスの整理	2. 対象とするリスクの選定	3. リスクレベルごとの対応方針決定	4. 適用する制御の選択	5. 例外・影響範囲の検討	6. 段階的な適用と改善
リスクベース制御を導入する目的を明確にします。	一般ユーザー/特権ユーザー、業務アプリ/管理センターなど、ポリシーの適用対象を整理します。	ユーザーリスクとサインインリスクを切り分け、どのリスクを制御対象とするかを決定します。	リスクレベルの「低・中・高」それぞれに対して、監視/追加認証/遮断などの基本方針を定めます。	MFA 要求、パスワード変更、アクセスブロックなど、自己修復可否を考慮して制御内容を選択します。	管理者アカウント、緊急対応用アカウント、業務影響が大きいシナリオへの配慮を行います。	レポートやユーザー影響を確認しながら、ポリシーを段階的に本番適用・改善していきます。

設計のポイント

目的を明確にする：どのリスクにどの強さで対応するかを定義します。整理せずに強化すると、過剰な制御や業務影響につながります。
リスク＝即ブロックにしない：正当なユーザーには自己修復の機会を与えることが重要です。MFA要求など、段階的な制御を基本とします。
段階的に強化する：最初から完成形を目指さず、影響を確認しながら徐々に強化していきます。

4.2. 設計の構造

0. 設計目的の整理 → 1. 対象ユーザー・アクセスの整理 → 2. 対象とするリスクの選定 → 3. リスクレベルごとの対応方針決定 → 4. 適用する制御の選択 → 5. 例外・影響範囲の検討 → 6. 段階的な適用と改善

0. 設計目的の整理

リスクベース条件付きアクセスの設計は、「何を守るのか」「なぜ自動制御が必要なのか」を明確にすることから始まります。

■設計目的の例

- 不正なサインインを早期に遮断したい
- 正当なユーザーには自己修復の機会を与えたい
- 管理者アカウントの侵害を最優先で防ぎたい

■設計上の考え方

- 目的が曖昧なまま設計すると、MFA 多発や業務停止といった副作用が発生しやすい
- 「何を守るための制御か」を先に定義することで、後続のリスク条件や制御内容の判断が一貫する

1. 対象ユーザー・アクセスの整理

次に、どのユーザー・どのアクセスに制御を適用するかを整理します。条件付きアクセスは強力な仕組みであるため、適用範囲の設計が不適切だと影響が全体に波及します。

■主な検討対象

- 一般ユーザーか、特権ユーザーか
- 全クラウドアプリか、特定アプリか
- 管理センターや組織の設定変更など、環境全体に影響する操作を対象に含めるか

■設計上の考え方

- 業務影響が読みにくい場合は、まず一般ユーザーを対象とし、影響範囲が限定的なアプリケーションから段階的に適用
- 挙動や誤検知の傾向を確認したうえで、主要サービスへ適用範囲を拡大
- 特権ユーザーは、一般ユーザーとは別ポリシーで設計するのが前提

4.2. 設計の構造

0. 設計目的の整理 | 1. 対象ユーザー・アクセスの整理 | 2. 対象とするリスクの選定 | 3. リスクレベルごとの対応方針決定 | 4. 適用する制御の選択 | 5. 例外・影響範囲の検討 | 6. 段階的な適用と改善

2. 対象とするリスクの選定

Entra ID Protection では、2種類のリスク（ユーザーリスク/サインインリスク）が明確に区別されて提供されます。
これらは意味も対応も異なるため、設計段階で切り分ける必要があります。

■リスクの位置づけ

ユーザーリスク：「このアカウントは侵害されていないか？」
※ 資格情報の漏洩や継続的な不審挙動など、アカウントの状態を基に評価されるリスク
サインインリスク：「今回のアクセスは正当か？」
※ アクセス元や挙動など、サインイン時点の文脈を基に評価されるリスク

■設計上の考え方

- 両者を同一ポリシーで扱うと、制御の意図が不明瞭になる
- リスクの性質ごとに、別ポリシーとして設計することが前提

3. リスクレベルごとの対応方針決定

次に、リスクレベルごとにどこまで対応するかを決定します。
組織としてのリスク対応方針を定義する工程です。

■代表的な整理例（Microsoft 推奨構成）

ユーザーリスク
低：監視対象とし、状況の変化を確認する
中：侵害の兆候はあるが、直ちに強制対応は行わず、段階的な対応を検討する
高：アカウント侵害の可能性が高いため、リスクの解消（修復）を必須とする

サインインリスク
低：正当な利用の可能性が高いため、直ちに制御は行わない
中・高：正当性確認を行い、正当な利用であればアクセスを継続させる

■設計上の考え方

- すべてを一律にアクセスブロックする設計は、リスク対応として過剰
- 「確認」「修復」「遮断」を、リスクの種類とレベルに応じて使い分けることが重要

4.2. 設計の構造

4. 適用する制御の選択

3で定義した制御方針を踏まえ、条件付きアクセスでどの制御を適用するかを選択します。
この工程では、**自己修復が可能かどうかを意識して制御を選ぶ**ことが重要です。（例：MFAの要求やパスワード変更など）

■ユーザーリスクに対する制御
「アカウント自体が侵害されている可能性」を示すリスクであり、アカウントの信頼性を回復するための制御を選択します。

高リスクの場合：アカウント侵害の可能性が高いため、**パスワード変更を要求**

- MFA のみではアカウント侵害が解消されたとは判断できない
- リスク状態は、修復が完了するまで継続する
- ユーザーリスク対応のポリシーは重複させず、1ユーザー1方針で設計

■サインインリスクに対する制御
「今回のアクセスが正当か」を確認するためのリスクであり、その場での正当性確認を目的とした制御を選択します。

中・高リスクの場合：正当性確認を目的として、**MFAを要求**

- 正当なユーザーが操作を完了することでリスクが解消される（自己修復）制御を基本とする

■制御選択における考え方

- 可能な限り、正当なユーザーが自らリスクを解消できる制御（自己修復）を優先する
- アクセスブロックは、高リスク時や影響の大きい操作に限定（自己修復が成立しない制御であり、管理者による介入が前提となるため）
- リスクの種類ごとに、目的に合った制御を明確に使い分ける
- ユーザーリスクとサインインリスクは独立して評価され、両方に該当した場合は各ポリシーの制御が同時に適用される。
  その結果、アクセスは各制御条件をすべて満たす必要があり、ブロックが含まれる場合は他の制御に関わらずアクセスは拒否される。

4.2. 設計の構造

0. 設計目的の整理 → 1. 対象ユーザー・アクセスの整理 → 2. 対象とするリスクの選定 → 3. リスクレベルごとの対応方針決定 → 4. 適用する制御の選択 → 5. 例外・影響範囲の検討 → 6. 段階的な適用と改善

5. 例外・影響範囲の検討

条件付きアクセスは強力な制御であるため、例外設定や運用時の影響を事前に整理しておく必要があります。設計が不十分な場合、業務停止や管理者ロックアウトにつながる可能性があります。

■主な検討ポイント

- **緊急用アカウント**をポリシーから除外するか
  ※条件付きアクセス誤設定や障害発生時に、管理者が緊急復旧を行うためのアカウント
- 管理者アカウントによるアクセスや設定変更など、高権限操作をどのように制御するか
- アクセス ブロック適用時の復旧手段が確保されているか

■ 設計上の考え方

- 例外設定は 必要最小限 とし、理由を明確にする
- セキュリティ強度だけでなく、運用・復旧まで含めて成立する設計を行う

6. 段階的な適用と改善

リスクベースの条件付きアクセスは、一度で完成形を作るものではなく、段階的に成熟させることが前提です。実際の影響を確認しながら、継続的に見直しを行います。

■主な検討ポイント

- ポリシーを **レポート専用モード**（条件付きアクセスの検証機能）で適用し、実際に有効化した場合の対象ユーザー・影響範囲を事前に把握する
- 想定外の対象ユーザーや業務影響の有無を確認
- 問い合わせや誤検知の発生状況を確認

■ 設計上の考え方

- 初期は 自己修復が可能な制御から適用する
- 強い制御（アクセスブロック等）は、対象や条件を限定して段階的に適用
- 運用結果を踏まえ、ポリシーを定期的に見直し・改善する

5. 利用メリットと注意点

5.1. 利用メリットと注意点

メリット

- **ユーザーリスク／サインインリスクを分けて可視化できる**
  「アカウント自体が危険か」「今回のサインインが危険か」を分離して把握でき、状況に応じた対応判断がしやすい。
- **リスクに応じた柔軟なアクセス制御ができる**
  すべてのユーザーに一律制御をかけるのではなく、「怪しいときだけ MFA」「危険なときだけブロック」といった運用ができる。
  また、ユーザー、デバイス、場所、アプリケーションなどの条件と組み合わせた制御が可能。
- **ゼロトラストを“仕組み”として実装できる**
  すべてのサインインを前提に疑い、都度リスク評価と制御を行うゼロトラスト運用を実現できる。
- **自動検知・自動対応により運用負荷を下げられる**
  管理者がログを常時監視しなくても、リスク検知から初動対応までを自動化できる。
- **セキュリティ成熟度を段階的に高められる**
  まずは可視化だけ → MFA 要求 → 自動ブロック、というように段階的な適用が可能。

注意点

- **MFAの事前登録**
  MFAを制御として利用する場合は、あらかじめユーザーがMFA実行に必要な認証方法を登録しておく必要がある。
- **“入れただけ”では効果が出ない**
  条件付きアクセスや MFA、パスワード変更機能と組み合わせて初めて価値が出る。
- **誤検知・ユーザー影響を考慮した設計が必要**
  出張・VPN・新端末利用など、正当な行動でもリスク判定される可能性がある。
- **すべての攻撃を防げるわけではない**
  Entra ID Protection は ID 観点の防御であり、端末侵害や内部不正などは別対策が必要。
- **ポリシー設計を誤ると業務影響が大きい**
  高リスク時の「即ブロック」などは、管理者への影響を特に考慮する必要がある。
- **ユーザーが自己修復できない場合の管理者対応**
  MFA 端末紛失やパスワード忘れなど自己修復できない場合、管理者対応（リスク却下等）を前提としたヘルプデスク運用が必要となる。

6. 活用シナリオ

6.1. シナリオ①：リスクベースMFAによる不正サインイン対策

本章では、Microsoft Entra ID Protectionのリスク判定から自動対応までを含め、IDセキュリティ運用の仕組みとして活用するための
シナリオを2つ紹介します。

背景・課題

- フィッシング等により **不正サインインのリスクが高まっている**
- 常時 MFA は **ユーザー負荷・業務影響が大きい**

条件付きアクセスの設計

- 対象ユーザー：一般ユーザー
  （管理者・緊急用アカウントは除外設定）
- 対象アプリ：Microsoft 365
  （Exchange / SharePoint / Teams など）
- 主な条件：
  ・サインインリスク：中・高
  ・場所：信頼済みネットワーク以外
  （社外ネットワーク、不明なIP など）
  ・デバイス：非準拠デバイス
- 制御：MFA を要求（自己修復）

運用イメージ・効果

✓ 怪しいサインイン時のみ MFA を要求し、正当ユーザーは MFA 完了で利用継続、**不正アクセスは リソース到達前に抑止**

✓ 正当な利用は阻害せず、リスクに応じた**段階的制御**を実現

✓ 検出されたリスクや制御結果は、**危険なサインイン レポート**として可視化され、運用改善に活用

✓ **検知から初動対応までを自動化**し、管理者は結果の**調査と例外・ポリシーの見直し**に集中できる

6.2. シナリオ②：ユーザーリスクに基づくアカウント侵害への自動対応

背景・課題

- フィッシングや情報漏洩により、**アカウントが侵害されている可能性を事前に把握しにくい**
- ユーザー種別（一般ユーザー／管理者）に応じて影響範囲を考慮した制御を行いたい
- 管理者による個別調査・手動対応に依存した運用は、初動の遅れや運用負荷増大につながりやすい

条件付きアクセスの設計

一般ユーザー向けポリシー

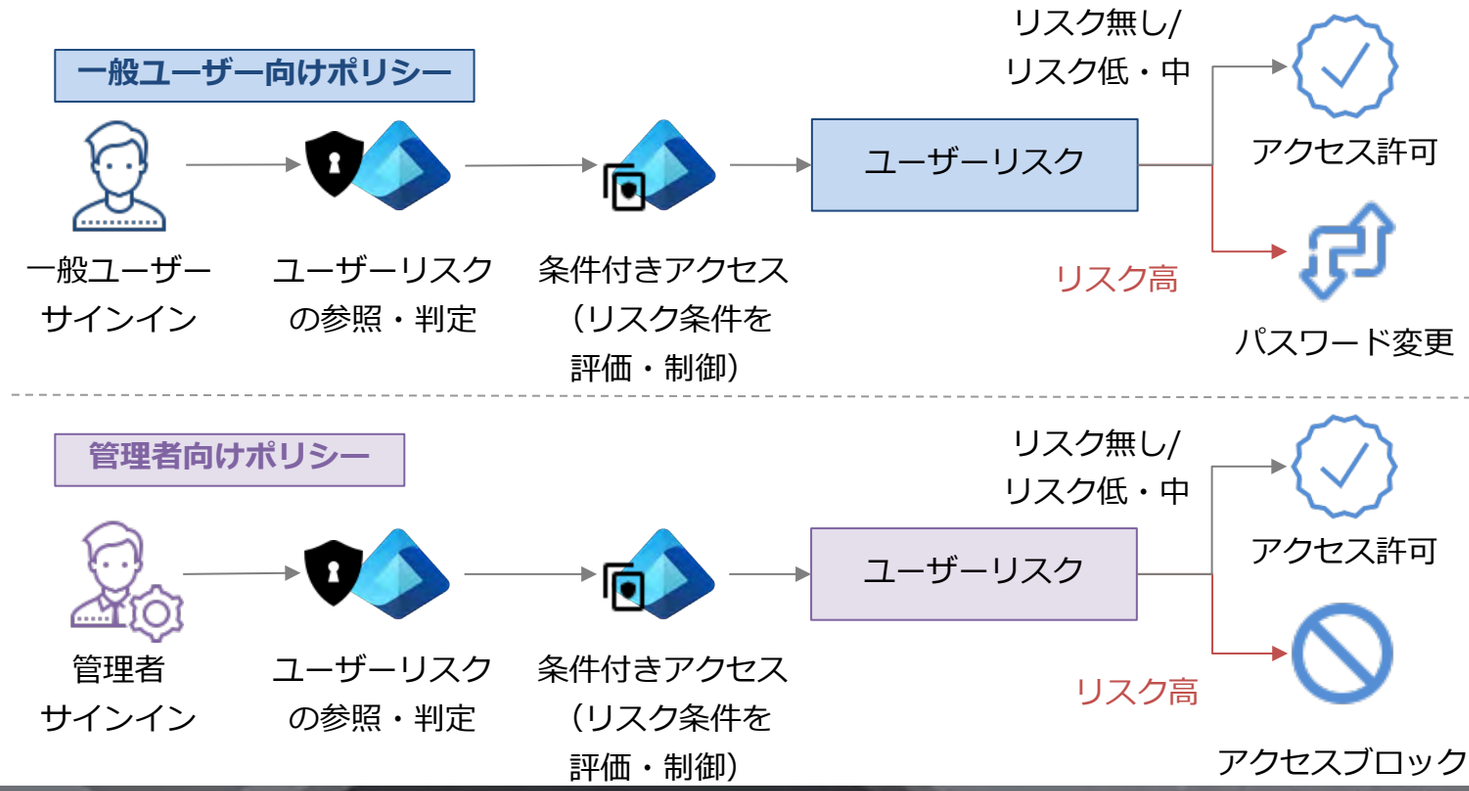
- 対象ユーザー：一般ユーザー
- 主な条件：**ユーザーリスク：高**
- 制御：パスワード変更を必須（自己修復）

管理者向けポリシー

- 対象ユーザー：管理者ロール付与アカウント
- 主な条件：**ユーザーリスク：高**
- 制御：アクセスブロック
- 管理者アカウントのログイン不可を防ぐため、緊急用管理アカウントを除外設定する

運用イメージ・効果

- ✓ アカウント侵害の兆候を**ユーザーリスクとして検知・評価**
- ✓ **一般ユーザーは自己修復**によりアカウントの信頼性を回復
- ✓ **管理者は高リスク判定時点で管理操作を即時遮断**
- ✓ リスク対応を自動化し、影響拡大を防止



7. ライセンス要件

7.1. ライセンス要件

Microsoft Entra ID Protection を利用するには、リスク検出・制御の対象となるユーザーごとに、対応するライセンスが必要となります。

必要ライセンス

Microsoft Entra ID Protection は単体ライセンスとしては提供されておらず、利用するには、**Microsoft Entra ID P2** を含むライセンスが必要です。※ Entra ID Free / P1 のみでは利用不可
以下のライセンスを保有している場合、Entra ID Protection が利用可能です。

ライセンス名	説明
Microsoft Entra ID P2	Entra ID の高度なセキュリティ機能を提供する単体ライセンス
Microsoft 365 E5	Entra ID P2、高度なセキュリティ・コンプライアンス機能を含む最上位プラン
Enterprise Mobility + Security（EMS）E5	Entra ID P2、Intuneなどを含む、ID・デバイス・情報保護に特化したセキュリティアドオン
Microsoft Defender Suite	Entra ID P2 を含み、ID・エンドポイント・メール・クラウドアプリを横断的に保護する統合セキュリティアドオン
Microsoft Entra Suite	ID Protection、Internet Access、Private Access、ID Governance、Verified IDを統合した Entra 製品群のアドオン

補足

Microsoft Defender for Cloud Apps、Defender for Office 365、Defender for Endpoint などのDefender 製品から提供されるシグナルを Entra ID Protection で活用する場合、Entra ID P2 に加えて、各 Defender 製品のライセンスが必要となります。
※上記の機能・ライセンス要件は、Microsoft 365 E5 および Microsoft Defender Suite に含まれています。