# 参考. ABAC の実装例-Microsoft Azure Active Directory 編



Microsoft Azure Active Directory（以下、「AAD」という。）は Identity as a Service（IDaaS）や Identity Governance Administration（IGA）等のデジタル・アイデンティティ管理における Microsoft 社製のサービスであり、アクセス制御機能もその一部として実装している。本文書では、AAD で管理可能なリソースに対して適用できる属性を用いたABAC実装例を紹介する。なお、本ドキュメントは2023年3月段階の仕様である。

## 1. グループにユーザーを追加する ABAC（サブジェクト側での制御）

この例（図 1）では、ユーザーグループにおけるメンバーの管理におけるABACを例にしている。AAD のグループは AAD に登録された特定のサービスに対するアクセスを制御するために一般的に利用されている。従来グループにおけるメンバーシップ管理は管理者による静的な作業であった。つまり、グループ管理に対するアクセス制御が適用されており、管理者であれば許可される図式であった（図 1 左）。しかし、AAD では動的なグループ管理が実装可能である。これは、ユーザーの属性を入力値としてメンバーシップ対象とするか判定するルールによって実現される（図 1 右）。つまりリソースの属性に着目して、グループに対する処理を制御できる。

図 1

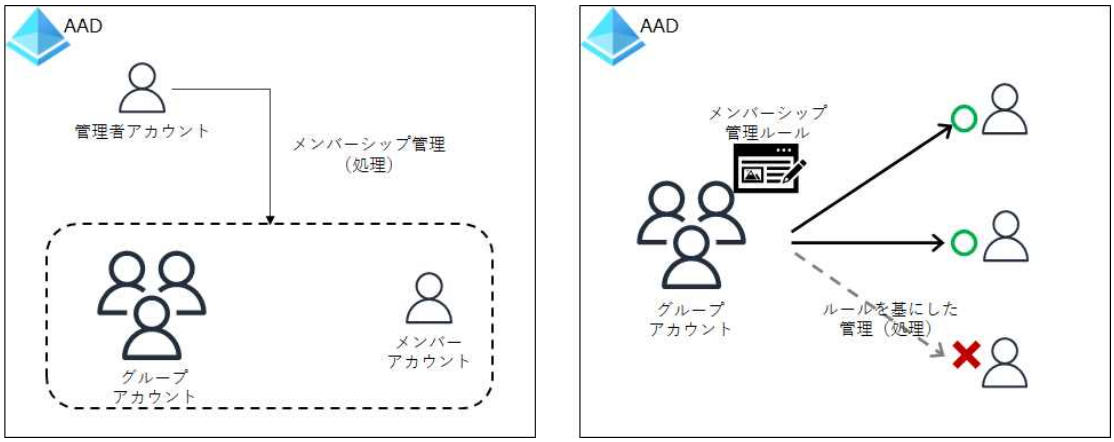


表 1

| アクセス制御のコンポーネント | 例で該当する機能 |
|---|---|
| ユースケース | グループオブジェクトのメンバーシップの管理 |
| サブジェクト | AAD グループ |
| オブジェクト | AAD グループメンバーシップ |
| 属性 | AAD ユーザーにつけられた属性及びその値 |
| PDP | AAD グループのルール |
| PEP | AAD グループ |

具体的には、AAD グループを動的グループとして作成し、その中にある「動的メンバーシップルール」を定義する（図2）。このルールに利用可能な属性（表2）を使い、特定の属性条件に合致するユーザーを抽出し、自動的にメンバーとして追加および削除する。このようにグループのメンバーシップ管理（処理）を管理者による作業から ABAC を基にして自動化できる。更に、このグループを SaaS アプリケーションに割り当てることで、SaaS アプリケーションへのアクセスも ABAC にできる。

図 2


表 2: AAD で設定できる属性一覧（一部）

| 属性名 | 説明 | 型 |
|---|---|---|
| accountEnabled | 検出ソースでのアカウントの状態 | Boolean |
| dirSyncEnabled | オンプレミスの Active Directory 同期 | Boolean |
| country | 国/リージョン | 文字列 |
| companyName | 会社 | 文字列 |
| department | 部署 | 文字列 |
| employeeId | 社員 ID | 文字列 |
| givenName | 名 | 文字列 |
| jobTitle | 役職 | 文字列 |
| mail | E メールアドレス | 文字列 |
| mailNickName | E メールユーザー名(@以下除く) | 文字列 |
| memberOf | 動的グループ | 文字列 |
| objectId | オブジェクト ID | 文字列 |
| passwordPolicies | パスワードポリシー | 文字列 |
| physicalDeliveryOfficeName | 勤務先オフィス | 文字列 |
| preferredLanguage | 言語(ISO 639-1 コード) | 文字列 |
| surname | 姓 | 文字列 |
| usageLocation | 国または地域コード | 2 文字の国または地域コード |
| userPrincipalName | ユーザー名 | 文字列 |

| | | |
|---|---|---|
| userType | ユーザータイプ | 文字列 |
| otherMails | その他 E メールアドレス | 文字列コレクション |
| proxyAddresses | E メールアドレス(プライマリ、セカンダリ等) | 文字列コレクション |

## 2. クラウドサービスへのデバイス属性によるアクセス制御（サブジェクト側での制御）

オンプレミス環境又はクラウド環境にかかわらず、管理外の端末の業務利用は、様々なリスクがある。ネットワークによるアクセス制限が困難なクラウド環境では、そのリスクをコントロールするために個々の端末を認証する重要性が高くなる。本 ABAC 例では、AAD によるデバイス属性をベースにした SaaS アプリケーションへのアクセス制御を条件付きアクセスによって実装する。具体的には、最新パッチの適用をしていない等、特定の構成ルールに準拠していないデバイスからの処理が拒否される。なお、SaaS アプリケーションが AAD と信頼関係を結び、認証連携を強制されている前提となる。パスワード等で、SaaS アプリケーションへのログインが AAD を迂回できるのであればバイパス可能である。

図 3

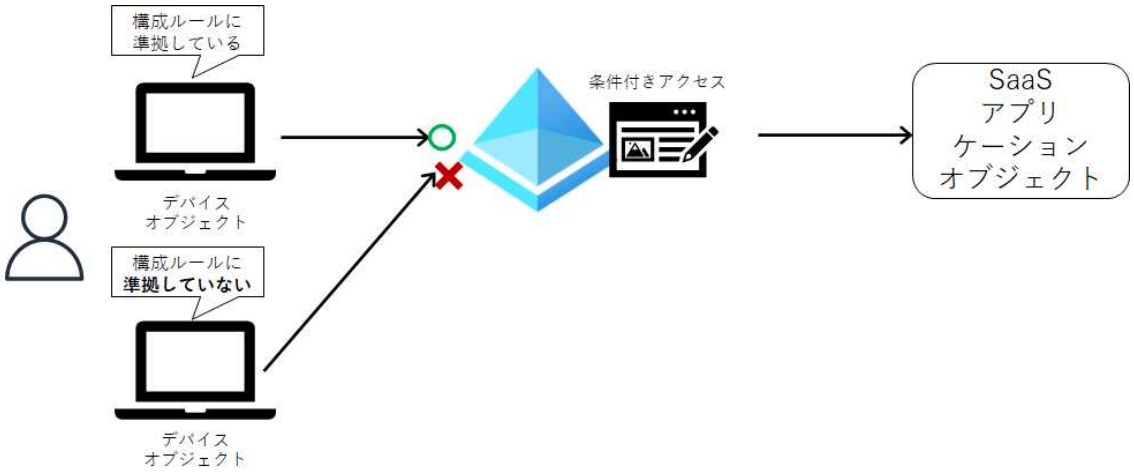



表 3

| アクセス制御のコンポーネント | 例で該当する機能 |
|---|---|
| ユースケース | SaaS アプリケーションへのアクセス元が構成ルールに準拠していない場合、ブロックする |
| サブジェクト | AAD に登録されたデバイスオブジェクトおよびその利用者 |
| オブジェクト | AAD と認証連携した SaaS アプリケーション |
| 属性 | デバイスオブジェクトの構成ルールへの準拠状態 を示す属性 |

| | |
|---|---|
| PDP | AAD – 条件付きアクセス |
| PEP | AAD – 条件付きアクセス |

Microsoft Intune（以降、Intune）というデバイス管理サービスに、登録されたデバイスオブジェクトが特定の構成ルールに準拠しているか自動で判定し、IsCompliant としてマークする機能がある[1]。Intune と連携すると AAD は、マークされたデバイスオブジェクトを識別可能となる。

図4は Intune から連携されたデバイスオブジェクトの IsCompliant で値が True ではない、つまり準拠状態にない端末からのアクセスを拒否するような設定である。これにより構成ルールに準拠していない端末だけでなく、AAD に登録されていない端末から SaaS アプリケーションへのアクセスをブロックすることが可能となる。今回は、IsCompliant に着目したが、他の属性も当該機能に利用できる。その一部を表4に記載する。

図 4


表 4

| 属性名 | 説明 | 型 |
|---|---|---|
| deviceId | デバイス ID | GUID である有効な deviceId |
| displayName | 名前 | 文字列 |
| deviceOwnership | デバイス所有者 | "Personal"（個人所有デバイス）と"Company"（企業所有 device の場合） |

[1] これ自体も構成情報を属性と見立てた ABAC とも言える

| | | |
|---|---|---|
| manufacturer | 製造メーカー | 文字列 |
| operatingSystem | OS | 有効な OS（Windows、iOS、Android など） |
| operatingSystemVersion | OS バージョン | OS ごとの有効なバージョン |
| trustType | 結合の種類 | デバイスの有効な登録済み状態。 サポートされている値は、AD (AAD 参加デバイスに使用)、ServerAD (Hybrid AAD 参加済みデバイスに使用)、Workplace (AAD 登録済みデバイスに使用) |
| department | 部署 | 文字列 |

## 3. クラウドサービスに付与した独自定義の属性によるアクセス制御（サブジェクト側での制御）

図5は、特定のクラウドサービスへのアクセスに、特定の追加条件を要求する ABAC の例である[2i]。具体的には、重要な業務を処理する SaaS アプリケーションに対するアクセスにのみ、より厳格なポリシーを適用する。これにより必要に応じた柔軟なセキュリティを実現できる。まず、AAD 管理者が、事前に定義したカスタムセキュリティ属性を、AAD に登録された SaaS アプリケーションに付与する。更に、AAD 管理者が、その属性を持つ SaaS アプリケーションに対するアクセスポリシーを条件付きアクセスとして構成する。

図 5

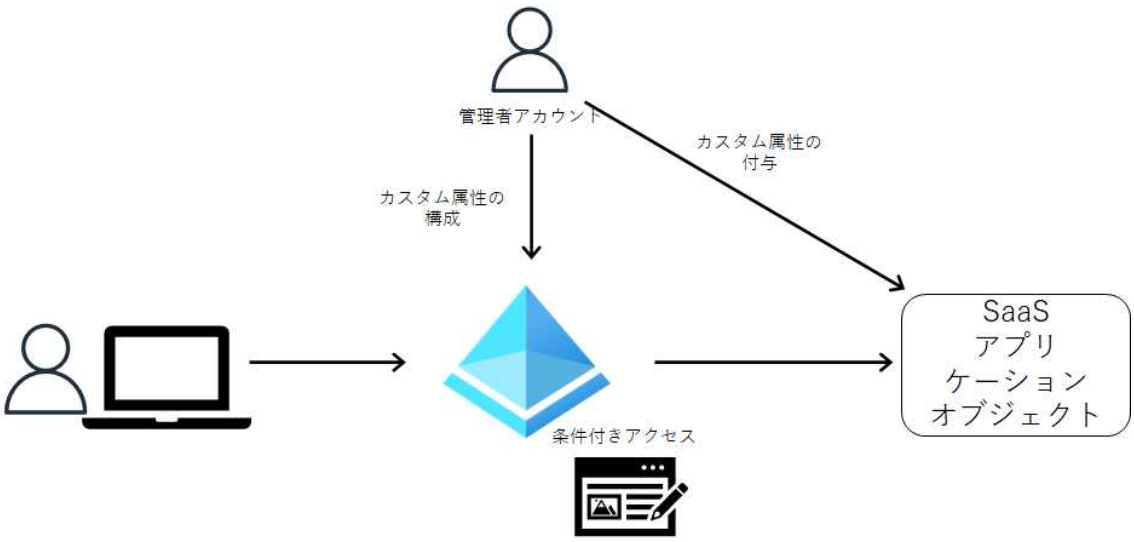



表 5

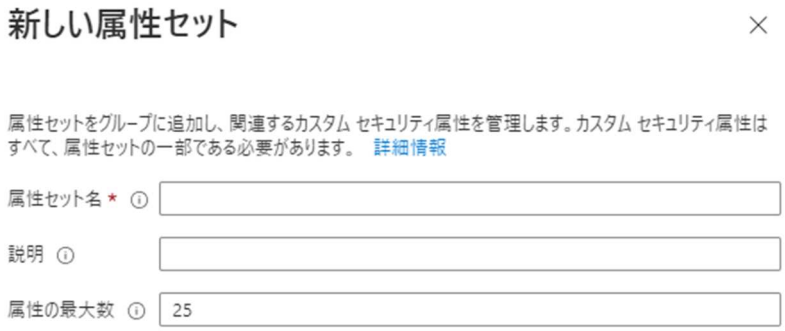
| アクセス制御のコンポーネント | 例で該当する機能 |
|---|---|
| ユースケース | 重要業務を処理する SaaS アプリケーションに通常より厳格なポリシーを適用する |
| サブジェクト | AAD に登録されたデバイスオブジェクトおよびその利用者 |
| オブジェクト | AAD と認証連携した SaaS アプリケーションオブジェクト |
| 属性 | SaaS アプリケーションオブジェクトに設定したカスタムセキュリティ属性と、デバイスオ |

[2] 基本的に全てのユーザーは多要素認証を設定すべきである

| | ブジェクトの構成ルールへの準拠状態を示す属性 |
|---|---|
| PDP | AAD – 条件付きアクセス |
| PEP | AAD – 条件付きアクセス |

カスタムセキュリティ属性の定義には、AAD の管理画面から[Custom Security Attributes(Preview)]を開き、[+属性セットを追加する]をクリックする。“属性セット名” を指定し、任意で説明や属性の最大数を決定する（図６）。

図 6

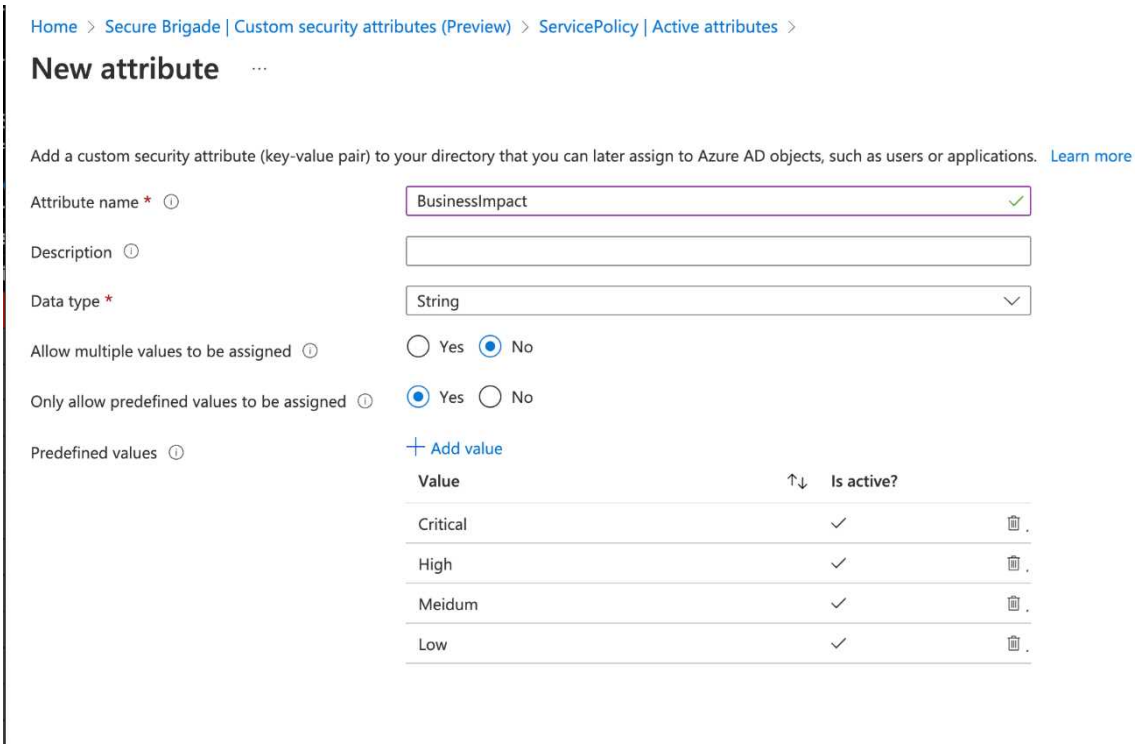



新しい属性セットを作成後に、作成した属性セットを選択すると以下の画面が表示されるので、[属性の追加]を選択すると、属性を定義できる（図７）。なお、条件付きアクセスで使用可能なデータ型は String(文字列)のみである。

図 7

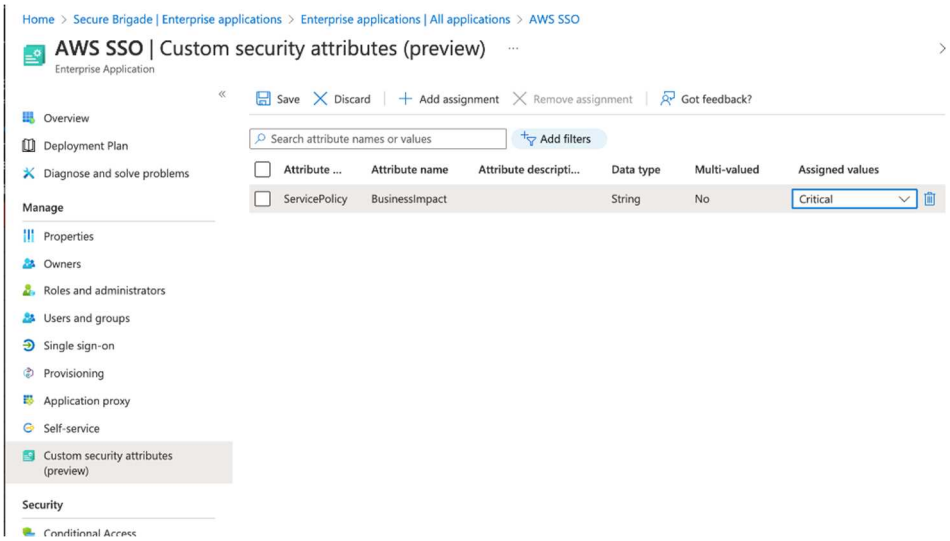

定義したカスタムセキュリティ属性と値を、[エンタープライズアプリケーション]として登録された SaaS アプリケーションに割り当てる。図８では業務上の影響度を表す「BusinessImpact」という属性を生成し、その値を Critical, High, Medium, Low に限定するよう定義した。

図 8




次に定義された属性が SaaS アプリケーションに付与される。図 9 では、侵害された際の影響が非常に大きい IaaS である AWS に、「BusinessImpact」属性名とその値を「Critical」とした属性を設定している。[3]

図 9

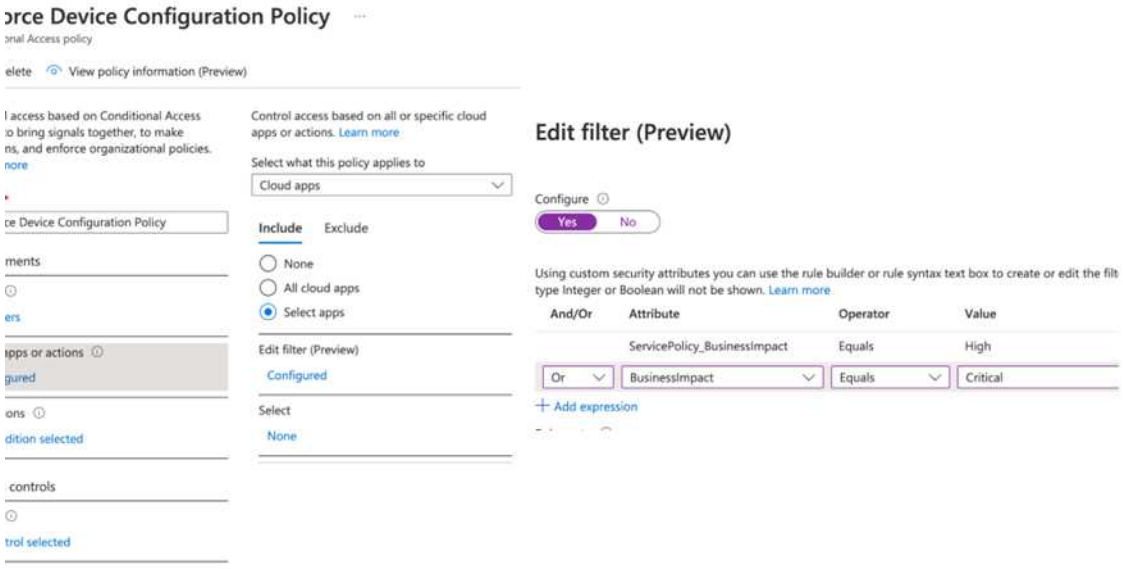



次に PDP・PEP となる条件付きアクセスを構成する。条件付きアクセスは対象の SaaS アプリケーションを選択する際に、カスタムセキュリティ属性を基にすることがで

[3] 資産管理の観点では、全ての資産を重要度に応じて分類すべきである。

きる。具体的には、[Azure AD 条件付きアクセス]を選択し、[+新しいポリシー]から作成したポリシーの[クラウドアプリまたは操作]をクリックし、[アプリを選択]-[フィルター編集(プレビュー)]から設定が可能だ。図 10 では、先に設定した「BusinessImpact」属性の値が「Critical」または「High」を指定することで、重要な業務を処理する SaaS アプリケーション全体を対象にしたポリシーが構成されている。

図 10




特定の条件に合わせポリシーの強度を変えるニーズは多くあるが、その対象を静的なリストで管理するのではなく、属性に応じた条件・ルールにする ABAC 例を示した。

## 4.参考文献

Azure Active Directory の動的グループ メンバーシップ ルール:
https://learn.microsoft.com/ja-jp/azure/active-directory/enterprise-users/groups-dynamic-membership
条件付きアクセス: デバイスのフィルター:
https://learn.microsoft.com/ja-jp/azure/active-directory/conditional-access/concept-condition-filters-for-devices
Azure AD のカスタム セキュリティ属性とは (プレビュー):
https://learn.microsoft.com/ja-jp/azure/active-directory/fundamentals/custom-security-attributes-overview