2019

ManageEngine

AD360

Required Privileges and Permissions

AD360 にて管理・監査を行う上で必要となる権限・アクセス許可の設定についてご紹介

■注意事項
本ガイドの内容は、改良のため、予告なく変更することがあります。
ゾーホージャパン株式会社は本ガイドに関しての一切の責任を負いかねます。 当社はこのガイドを
使用することにより引き起こされた偶発的もしくは間接的な損害についても責任を負いかねます。

目次

1. はじめに

1-1 本ガイドについて

AD360 を使用して各種操作を実行するためには、Administrator 権限をもつアカウントを登録する必要があります。本ガイドでは、Administrator アカウントの登録が難しいという方向けに、最低限必要な権限・アクセス許可についてご案内します。

NOTE

本製品ではすべての操作を確実に実行できるように、Domain Admins あるいは Administrator アカウントの登録を推奨しています。やむを得ない場合を除き、基本的には推奨アカウントをご利用いただきますようお願いいたします。

1-2 対象読者

本ガイドは、導入に関するシステム管理者を対象としています。

1-3 必要な権限について

次章では、AD360 に統合されている製品ごとに必要となる権限についてご案内しています。特定の製品について参照される場合は、以下のリンクをクリックしてください。

- ADManager Plus
- ADSelfService Plus
- ADAudit Plus
- O365 Manager Plus

2. 製品ごとに必要な権限について

2-1 ADManager Plus の場合

操作	必要な権限
ユーザー管理	
ユーザーの作成	• Administrators グループ/Account Operators グループに所属 (あるいは) • 該当 OU/コンテナーを対象に、オブジェクト制御の委任ウィザードで「ユーザーアカウントの作成、削除、および変更」の制御を委任
ユーザーの変更	• Administrators グループ/Account Operators グループに所属 (あるいは) • 該当 OU/コンテナーを対象に、オブジェクト制御の委任ウィザードで「ユーザーアカウントの作成、削除、および変更」の制御を委任
ユーザーの削除	• Administrators グループ/Account Operators グループに所属 (あるいは) • 該当 OU/コンテナーを対象に、オブジェクト制御の委任ウィザードで「ユーザーアカウントの作成、削除、および変更」の制御を委任
コンピューター管理	
コンピューターの作成	• Administrators グループ/Account Operators グループに所属 (あるいは) • 該当 OU/コンテナーを対象に、オブジェクト制御の委任ウィザードで「コンピューターオブジェクト」にチェックし、「選択されたオブジェクトをこのフォルダーに作成する」オプションにチェックを入れる
コンピューターの変更	• Administrators グループ/Account Operators グループに所属 (あるいは) • 該当 OU/コンテナーを対象に、オブジェクト制御の委任ウィザードで「コンピューターオブジェクト」にチェックし、「選択されたオブジェクトをこのフォルダーに作成する」オプションにチェックを入れる
コンピューターの削除	• Administrators グループ/Account Operators グループに所属 (あるいは) • 該当 OU/コンテナーを対象に、オブジェクト制御の委任ウィザードで「コンピューターオブジェクト」にチェックし、「選択されたオブジェクトをこのフォルダーに作成する」オプションにチェックを入れる
グループ管理	
グループの作成	• Administrators グループ/Account Operators グループに所属 (あるいは) • 該当OU/コンテナーを対象に、オブジェクト制御の委任ウィザードで「グループの作成、削除、および変更」の制御を委任
グループの変更	• Administrators グループ/Account Operators グループに所属 (あるいは) • 該当OU/コンテナーを対象に、オブジェクト制御の委任ウィザードで「グループの作成、削除、および変更」の制御を委任
グループの削除	• Administrators グループ/Account Operators グループに所属 (あるいは) • 該当OU/コンテナーを対象に、オブジェクト制御の委任ウィザードで「グループの作成、削除、および変更」の制御を委任
連絡先管理	
連絡先の作成	• Administrators グループ/Account Operators グループに所属 (あるいは) • 該当OU/コンテナーを対象に、オブジェクト制御の委任ウィザードで「連絡先オブジェクト」にチェックし、「選択されたオブジェクトをこのフォルダーに作成する」オプションにチェックを入れる

連絡席の変更	• Administrators グループ/Account Operators グループに所属 (あるいは) • 該当 OU/コンテナーを対象に、オブジェクト制御の委任ウィザードで「連絡先オブジェクト」にチェックし、「選択されたオブジェクトをこのフォルダーに作成する」オプションにチェックを入れる
連絡先の削除	• Administrators グループ/Account Operators グループに所属 (あるいは) • 該当 OU/コンテナーを対象に、オブジェクト制御の委任ウィザードで「連絡先オブジェクト」にチェックし、「選択されたオブジェクトをこのフォルダーに作成する」オプションにチェックを入れる
GPO 管理	
GPO の作成	• Group Policy Creator Owners グループに所属
GPO の無効化/有効化	• 管理する GPO オブジェクトの ’flags’ 属性に対する書き込み権限を所有
ユーザーの構成の無効化/有効化	• 管理する GPO オブジェクトの ’flags’ 属性に対する書き込み権限を所有
コンピューターの構成の無効化/有効化	• Group Policy Creator Owners グループに所属
GPO リンクの無効化/有効化/削除	• リンクの変更や削除を行うドメイン/OU/サイトの ’gPLink’ 属性に対する書き込み権限を所有 • リンクの継承を行うドメイン/OU の ’gPOptions’ 属性に対する書き込み権限を所有
GPO 設定	• Group Policy Creator Owners グループに所属
GPO リンクの強制	• リンクの変更や削除を行うドメイン/OU/サイトの ’gPLink’ 属性に対する書き込み権限を所有
レポート	• ドメイン/OU/サイトの ’gPLink’ 属性に対する読み取り権限を所有 • ドメイン/OU の ’gPOptions’ 属性に対する読み取り権限を所有 • GPO オブジェクトの “flags, versionNumber, modifyTimeStamp, createTimeStamp” 属性に対する読み取り権限を所有
ファイルサーバー管理	
アクセス許可の変更	• 対象のファイル/フォルダーに対する、読み取り/書き込み権限を所有
Active Directory レポート	
レポートの生成	• ドメイン/OU に対する「内容の一覧表示」の権限を所有
NTFS レポートの生成	• 対象のファイル/フォルダーに対する読み取り権限を所有
Exchange サーバー管理	
Exchange 2010 ～	• Organization Management グループに所属
Microsoft 365 管理	
Microsoft 365 管理	• 「ユーザー管理の管理者」の役割を所有
Exchange Online 管理	• 「Exchange の管理者」の役割を所有
Microsoft 365 レポート	
Microsoft 365 レポート	• 「レポート閲覧者」の役割を所有
Exchange Online レポート	• 「ユーザー管理の管理者」の役割を所有
G Suite (Google Apps) の管理とレポート	
G Suite 管理	• 以下の API Scope をご参照ください： https://www.googleapis.com/auth/admin.directory.user https://www.googleapis.com/auth/admin.directory.group https://www.googleapis.com/auth/admin.directory.orgunit
G Suite レポート	• 以下の API Scope をご参照ください： https://www.googleapis.com/auth/admin.directory.user

2-2 ADSelfService Plus の場合

操作	必要な権限
パスワードリセットのセルフサービス	• オブジェクト制御の委任ウィザードで「ユーザーオブジェクト」にチェックし、「パスワードのリセット」・「pwdLastSet の書き込み」・「pwdLastSet の読み込み」のアクセス許可を付与する
アカウントロック解除のセルフサービス	• オブジェクト制御の委任ウィザードで「ユーザーオブジェクト」にチェックし、「lockoutTime の書き込み」・「lockoutTime の読み込み」のアクセス許可を付与する
ユーザーによる AD 属性の更新	• オブジェクト制御の委任ウィザードで「ユーザーオブジェクト」にチェックし、「読み取り」・「書き込み」のアクセス許可を付与する
パスワードポリシーの表示	• オブジェクト制御の委任ウィザードで「msDS-PasswordSettings オブジェクト」・「msDS-PasswordSettingsContainer オブジェクト」を選択し、「読み取り」のアクセス許可を付与する
メールグループ管理のセルフサービス	• オブジェクト制御の委任ウィザードで「グループオブジェクト」にチェックし、「読み取り」・「書き込み」のアクセス許可を付与する
NTLM 認証によるシングルサインオン	• オブジェクト制御の委任ウィザードで「コンピューターオブジェクト」にチェックし、「読み取り」・「書き込み」のアクセス許可を付与する
ログオンスクリプトを使用した強制登録	• オブジェクト制御の委任ウィザードで「ユーザーオブジェクト」にチェックし、「scriptPath の読み取り」・「scriptPath の書き込み」のアクセス許可を付与する
削除されたユーザーのレポート表示	• Domain Admins グループに所属
GINA/CP のインストール	• Domain Admins グループに所属

NOTE

設定の詳細は以下の URL をご参照ください。
https://www.manageengine.jp/download/products/ADSSP/ADSelfService_Plus_permissions-requirement-guide.pdf

2-3 ADAudit Plus の場合

操作	必要な権限
セキュリティログ監査	• Event Log Readers グループに所属 • Group Policy Creator Owners グループに所属 • ローカルの Administrators グループに所属 • グループポリシー管理エディターより、「ユーザー権利の割り当て」→「監査とセキュリティログの管理」のプロパティ画面からユーザーを追加する • DCOM・WMI アクセス許可を付与する

NOTE

設定の詳細は以下の URL をご参照ください。
https://www.manageengine.jp/support/kb/ADAudit_Plus/?p=1265

2-4 O365 Manager Plus の場合

操作	必要な権限
Exchange Online レポートと監査	• 「View-Only Audit Logs」の役割を付与 • 「View-Only Configuration」の役割を付与 • 「View-Only Recipient」の役割を付与
Microsoft 365 レポートと管理	• 「レポート閲覧者」の役割を付与 • 「ユーザー管理の管理者」の役割を付与 • 「Exchange の管理者」の役割を付与
コンテンツ検索	• 以下の REST API へのアクセス権を所有 ▶ Windows Azure Active Directory ▶ Microsoft Graph API

本製品に関するお問い合わせ

ゾーホージャパン株式会社 ManageEngine 事業部

〒222-0012 神奈川県横浜市西区みなとみらい三丁目 6 番 1 号 みなとみらいセンタービル 13 階

ホームページ：https://www.manageengine.jp/

AD360 製品ページ： https://www.manageengine.jp/products/AD360/