

第4章：グループポリシーによるデスクトップとアプリケーション設定の管理

演習 A：グループポリシー オブジェクトと設定の構成

練習 1：グループポリシーによる Windows 10 の管理

▶ 作業 1：組織単位 (OU) の構造を作成する

1. LON-DC1 のサーバー マネージャーで、[ツール]、[Active Directory 管理センター] の順にクリックします。
2. Active Directory 管理センターの左側のウィンドウで、[Adatum (ローカル)] をクリックします。
3. [Adatum (ローカル)] を右クリックし、[新規]、[組織単位] の順にクリックします。
4. [組織単位の作成] ダイアログ ボックスで、[名前] ボックスに「MachineFloor」と入力し、[OK] をクリックします。
5. [Adatum (ローカル)] を右クリックし、[新規]、[組織単位] の順にクリックします。
6. [組織単位の作成] ダイアログ ボックスで、[名前] ボックスに「CorpComputers」と入力し、[OK] をクリックします。
7. 詳細ウィンドウで、[Computers] コンテナをダブルクリックします。
8. [LON-CL1] を右クリックし、[移動] をクリックします。
9. [移動] ダイアログ ボックスで、[MachineFloor]、[OK] の順にクリックします。
10. [LON-CL2] を右クリックし、[移動] をクリックします。
11. [移動] ダイアログ ボックスで、[CorpComputers]、[OK] の順にクリックします。
12. Active Directory 管理センターを閉じます。
13. ホスト コンピューターで、Hyper-V マネージャーに切り替えます。
14. Hyper-V マネージャーで [23697-2B-LON-CL1] をクリックし、操作ウィンドウで、[起動] をクリックします。
15. Hyper-V マネージャーで [23697-2B-LON-CL2] をクリックし、操作ウィンドウで、[起動] をクリックします。

▶ 作業 2：管理用テンプレートのセントラル ストアを作成する

1. LON-DC1 のタスク バーで、[エクスプローラー] アイコンをクリックします。
2. エクスプローラーのアドレス バーに「E:\Labfiles」と入力し、Enter キーを押します。
3. 詳細ウィンドウで、[PolicyDefinitions] を右クリックし、[コピー] をクリックします。
4. アドレス バーに「¥¥LON-DC1¥sysvol¥Adatum.com¥Policies」と入力し、Enter キーを押します。
5. 詳細ウィンドウの何も表示されていない場所を右クリックし、[貼り付け] をクリックします。

▶ 作業 3：MachineFloor のコンピューターのグループポリシーを構成する

1. LON-DC1 のサーバー マネージャーで、[ツール]、[グループポリシーの管理] の順にクリックします。
2. 必要に応じて、グループポリシーの管理に切り替えます。

3. グループポリシーの管理で、[フォレスト : Adatum.com]、[ドメイン]、[Adatum.com] の順に展開し、[グループポリシーオブジェクト] を右クリックして、[新規] をクリックします。
4. [新しい GPO] ダイアログボックスで「MachineFloor GPO」と入力し、[OK] をクリックします。
5. [グループポリシーオブジェクト] ノードをクリックし、[MachineFloor GPO] を右クリックして、[編集] をクリックします。
6. グループポリシー管理エディターで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[システム] の順に展開します。
7. [インターネット通信の管理] を展開し、[インターネット通信の設定] をクリックします。
8. 詳細ウィンドウで、[Windows Update のすべての機能へのアクセスをオフにする] をダブルクリックします。
9. [有効] を選択し、[OK] をクリックします。
10. グループポリシー管理エディターで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント] の順に展開し、[データの収集とプレビュービルド] ノードをクリックします。
11. 詳細ウィンドウで、[Insider ビルドに関するユーザーコントロールの切り替え] をダブルクリックします。
12. [無効] を選択し、[OK] をクリックします。
13. グループポリシー管理エディターで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[Windows リモート管理 (WinRM)] の順に展開し、[WinRM サービス] をクリックします。
14. 詳細ウィンドウで、[WinRM によるリモートサーバー管理を許可する] をダブルクリックします。
15. [無効] を選択し、[OK] をクリックします。
16. グループポリシー管理エディターで、[コンピューターの構成]、[ポリシー]、[Windows の設定]、[セキュリティの設定] の順に展開し、[システムサービス] をクリックして、[Windows Remote Management (WS-Management)] をダブルクリックします。
17. [このポリシーの設定を定義する] チェックボックスをオンにします。
18. 必要に応じて、[無効] をクリックし、[OK] をクリックします。
19. グループポリシー管理エディターで、[コンピューターの構成]、[ポリシー]、[Windows の設定]、[セキュリティの設定]、[セキュリティが強化された Windows ファイアウォール]、[セキュリティが強化された Windows ファイアウォール - LDAP://CN=<GUID>] の順に展開し、[受信の規則] をクリックします。
20. [受信の規則] を右クリックして、[新しい規則] をクリックします。
21. 新規の受信の規則ウィザードで、[事前定義] を選択し、ドロップダウンリストで、[Windows リモート管理] を選択して、[次へ] をクリックします。
22. [事前定義された規則] ページで、[次へ] をクリックします。
23. [操作] ページで、[接続をブロックする] を選択し、[完了] をクリックします。
24. グループポリシー管理エディターで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント] の順に展開し、[Microsoft Edge] をクリックします。
25. 詳細ウィンドウで、[Web サイトでオートフィルを使用できるようにする] をダブルクリックします。
26. [無効] を選択し、[OK] をクリックします。
27. 詳細ウィンドウで、[パスワードマネージャーの構成を許可する] をダブルクリックします。

28. [無効] を選択し、[OK] をクリックします。
29. 詳細ウィンドウで、[ポップアップの実行を許可する] をダブルクリックします。
30. [無効] を選択し、[OK] をクリックします。
31. 詳細ウィンドウで、[Configure how Microsoft Edge treats cookies] をダブルクリックします。
32. [有効] を選択し、[OK] をクリックします。
33. グループ ポリシー管理エディターを閉じます。

▶ 作業 4: CorpComputers のグループ ポリシー設定を構成する


1. LON-DC1 のグループ ポリシーの管理で、[ドメイン]、[Adatum.com] の順に展開し、[グループ ポリシー オブジェクト] を右クリックして、[新規] をクリックします。
2. [新しい GPO] ダイアログ ボックスで、[名前] ボックスに「CorpComputers GPO」と入力し、[OK] をクリックします。
3. [グループ ポリシー オブジェクト] ノードをクリックし、[CorpComputers GPO] を右クリックして、[編集] をクリックします。
4. グループ ポリシー管理エディターで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[Windows リモート管理 (WinRM)] の順に展開し、[WinRM サービス] をクリックします。
5. 詳細ウィンドウで、[WinRM によるリモート サーバー管理を許可する] をダブルクリックします。
6. [有効] を選択し、[IPv4 フィルター] ボックスに「アスタリスク (*)」を入力し、[OK] をクリックします。
7. グループ ポリシー管理エディターで、[コンピューターの構成]、[ポリシー]、[Windows の設定]、[セキュリティの設定] の順に展開し、[システム サービス] をクリックして、[Windows Remote Management (WS-Management)] をダブルクリックします。
8. [このポリシーの設定を定義する] チェック ボックスをオンにします。
9. [自動]、[OK] の順にクリックします。
10. グループ ポリシー管理エディターで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[リモート デスクトップ サービス]、[リモート デスクトップ セッション ホスト] の順に展開し、[接続] をクリックします。
11. 詳細ウィンドウで、[ユーザーがリモート デスクトップ サービスを使ってリモート接続することを許可する] をダブルクリックします。
12. [有効] を選択し、[OK] をクリックします。
13. グループ ポリシー管理エディターで、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント] の順に展開し、[Delivery Optimization] をクリックします。
14. 詳細ウィンドウで、[Download Mode] をダブルクリックし、[有効] を選択します。
15. [Download Mode] ドロップダウン リストで [LAN] を選択して、[OK] をクリックします。
16. グループ ポリシー管理エディターを閉じます。

▶ 作業 5: グループ ポリシー設定を検証する


グループ ポリシー オブジェクト (GPO) を適用する前に設定を確認する

1. LON-DC1 のタスク バーで、[Windows PowerShell] アイコンをクリックします。
2. Windows PowerShell ウィンドウで、次のコマンドレットを入力し、Enter キーを押します。


```
Invoke-Command -Computername LON-CL2 -ScriptBlock {hostname}
```

 **注:** LON-CL2 上でコマンドレットを実行できないことを確認します。


3. [スタート] をクリックし「mstsc」と入力して、Enter キーを押します。
4. リモート デスクトップ接続ウィンドウで「LON-CL2」と入力し、Enter キーを押します。

 **注:** リモート デスクトップ接続クライアントが接続を作成しようとすると、一定期間経過後にエラー メッセージが表示されることを確認します。


5. エラー メッセージで、[OK] をクリックします。
6. リモート デスクトップ接続ウィンドウを閉じます。
7. LON-CL1 に切り替えます。
8. ユーザー名「Adatum¥Administrator」、パスワード「Pa\$\$w0rd」を使用してサインインします。
9. [スタート]、[設定] の順にクリックします。
10. 設定ウィンドウで、[更新とセキュリティ] をクリックします。
11. [更新プログラムのチェック] をクリックします (「更新プログラムのインストール中に問題が発生しました」というエラー メッセージが表示されたら、[再試行] をクリックします)。

 **注:** エラー メッセージが表示されるまでにしばらく時間がかかることに注意してください。また「オンラインにして更新プログラムをダウンロードすることができませんでした。インターネットに接続していることを確認してください」というメッセージが表示される場合もあります。

12. [詳細オプション] をクリックします。

 **注:** [開始する] をクリックすることができることを確認します。

13. サインアウトし、ユーザー名「Adatum¥Allie」、パスワード「Pa\$\$w0rd」を使用して再度サインインします。
14. タスク バーで、[Microsoft Edge] アイコンをクリックします。
15. Microsoft Edge で、[他の操作 (...)] をクリックし、[設定]、[詳細設定を表示] の順にクリックします。

 **注:** [パスワードを保存する] が [オン] に設定され、クッキーがブロックされていないことを確認します。

16. LON-CL1 からサインアウトします。

GPO をリンクする

1. LON-DC1 に切り替えます。
2. グループ ポリシーの管理に切り替えます。
3. コンソール ツリーで、[CorpComputers] OU を右クリックし、[既存の GPO のリンク] をクリックします。

4. [GPO の選択] ダイアログ ボックスで、[CorpComputers GPO]、[OK] の順にクリックします。
5. コンソール ツリーで、[CorpComputers] OU を右クリックし、[既存の GPO のリンク] をクリックします。
6. [GPO の選択] ダイアログ ボックスで、[CorpComputers Firewall policy]、[OK] の順にクリックします。
7. コンソール ツリーで [MachineFloor] OU を右クリックし、[既存の GPO のリンク] をクリックします。
8. [GPO の選択] ダイアログ ボックスで、[MachineFloor GPO]、[OK] の順にクリックします。


GPO を適用し設定を確認する

1. LON-CL1 に切り替え、必要に応じて、ユーザー名「Adatum¥Administrator」、パスワード「Pa\$sw0rd」を使用してサインインします。
2. [スタート] をクリックし「cmd」と入力し、Enter キーを押します。
3. コマンド プロンプトで、次のコマンドを入力し、Enter キーを押します。


```
gpupdate
```

4. [スタート] を右クリックし、[シャットダウンまたはサインアウト] をポイントして、[再起動] をクリックします。
5. LON-CL2 に切り替え、手順 1 ～ 4 を繰り返します。
6. コンピューターが再起動されるまで待ち、次に進みます。
7. LON-DC1 に切り替えます。
8. [スタート] を右クリックし、[シャットダウンまたはサインアウト] をポイントして、[再起動] をクリックします。
9. ユーザー名「Adatum¥Administrator」、パスワード「Pa\$sw0rd」を使用してサインインします。
10. [スタート] をクリックし、「powershell」と入力して、Enter キーを押します。
11. Windows PowerShell ウィンドウで、次のコマンドレットを入力し、Enter キーを押します。

```
Invoke-Command -Computername LON-CL2 -ScriptBlock {hostname}
```

 **注:** LON-CL2 でコマンドレットを実行できることを確認します。

12. [スタート] をクリックし「mstsc」と入力して、Enter キーを押します。
13. リモート デスクトップ接続ウィンドウで「LON-CL2」と入力し、Enter キーを押します。

 **注:** サインインのプロンプトが表示されることを確認します。

14. [キャンセル] をクリックします。
15. LON-CL1 コンピューターに切り替え、ユーザー名「Adatum¥Administrator」、パスワード「Pa\$sw0rd」を使用してサインインします。
16. [スタート]、[設定] の順にクリックします。
17. 設定ウィンドウで、[更新とセキュリティ] をクリックします。
18. [更新プログラムのチェック] をクリックします。(「更新プログラムのインストール中に問題が発生しました」というエラー メッセージが表示されたら、[再試行] を 1 回クリックします。)



注：エラーメッセージが即座に表示されることを確認します。

19. [詳細オプション] をクリックします。



注：[開始する] をクリックできないことを確認します。

20. LON-CL1 からサインアウトします。

21. ユーザー名「Adatum¥Allie」、パスワード「Pa\$\$w0rd」を使用して再度サインインします。

22. タスク バーで、[Microsoft Edge] アイコンをクリックします。

23. Microsoft Edge で、[他の操作 (...)] をクリックし、[設定] をクリックします。

24. [詳細設定を表示] をクリックします。



注：いくつかの設定は、グループポリシー経由で構成されているため、グレースアウトされていることを確認します。

25. 「Adatum¥Allie」を LON-CL1 からサインアウトします。

結果：この練習により、GPO とセントラルストアを作成し、いくつかのグループポリシー設定を構成して、それらが適用されていることを確認することができました。

▶ 次の演習の準備をする

次の演習のために、仮想マシンを起動したままにします。

演習 B：グループ ポリシーの基本設定によるデスクトップ設定の管理

練習 1：ドライブおよびプリンターのマッピングを適用するためのグループポリシーの基本設定の構成

▶ 作業 1：グループ ポリシーの基本設定を構成してドライブ マッピングを構成する

ファイル共有を作成する

1. LON-DC1 のタスク バーで、[エクスプローラー] アイコンをクリックします。
2. エクスプローラーで、[AllFiles (E:)] ドライブをダブル クリックします。
3. 何も表示されていない場所を右クリックし、[新規作成]、[フォルダー] の順にクリックします。
4. 「Research」と入力し、Enter キーを押します。
5. [Research] フォルダーを右クリックし、[共有]、[特定のユーザー] の順にクリックします。
6. [ファイルの共有] ダイアログ ボックスに「Research」と入力し、[追加] をクリックします。
7. [読み取り] ドロップダウン リストで、[読み取り/書き込み] をクリックします。
8. [共有] をクリックし、[終了] をクリックします。
9. Research を Sales に置き換えて、手順 3 ～ 8 を繰り返し、Sales 共有フォルダーを作成します。

GPO を作成する

1. グループ ポリシーの管理に切り替えます。
2. グループ ポリシーの管理で、[ドメイン]、[Adatum.com] の順に展開し、[グループ ポリシー オブジェクト] を右クリックして、[新規] をクリックします。
3. [新しい GPO] ダイアログ ボックスで「Adatum Mapped Drives GPO」と入力し、[OK] をクリックします。
4. [グループ ポリシー オブジェクト] ノードをクリックし、[Adatum Mapped Drives GPO] を右クリックして、[編集] をクリックします。
5. グループ ポリシー管理エディターで、[ユーザーの構成]、[基本設定]、[Windows の設定] の順に展開し、[ドライブ マップ] をクリックします。
6. [ドライブ マップ] を右クリックし、[新規作成]、[マップされたドライブ] の順にクリックします。
7. [新しいドライブのプロパティ] ダイアログ ボックスの [全般] タブで、次の値を使用します。
 - 場所：¥¥LON-DC1¥¥Research
 - 再接続：オン
 - ラベル：Research Data
 - 次の文字を使用：R
8. [共通] タブで、次の値を使用します。
 - ログオンしているユーザーのセキュリティ コンテキストで実行する (ユーザー ポリシー オプション)：オン
 - 項目レベルで対象化する：オン
9. [対象化] をクリックします。

10. [ターゲット エディター] ダイアログ ボックスの [新しい項目] ドロップダウン リストで、[セキュリティグループ] をクリックし、[省略 (...)] をクリックします。
11. [グループの選択] ダイアログ ボックスで「Research」と入力し、[OK] をクリックします。
12. [ターゲット エディター] ダイアログ ボックスで、[OK] をクリックします。
13. [新しいドライブのプロパティ] ダイアログ ボックスで、[OK] をクリックします。
14. Research を Sales に置き換えて、手順 6 ~ 13 を繰り返し、Sales に割り当てられたドライブを作成します。
15. グループ ポリシー管理エディターを閉じます。

▶ 作業 2: グループ ポリシーの基本設定を構成してプリンターを構成する

プリンターを作成する

1. LON-DC1 で、[スタート] をクリックし「デバイスとプリンター」と入力して、[デバイスとプリンター] をクリックします。
2. [デバイスとプリンター] で、[プリンターの追加] をクリックします。
3. [探しているプリンターはこの一覧にはありません] をクリックします。
4. [その他のオプションでプリンターを検索] ページで、[ローカル プリンターまたはネットワーク プリンターを手動設定で追加する] を選択し、[次へ] をクリックします。
5. [プリンター ポートの選択] ページで、[次へ] をクリックします。
6. [プリンター ドライバーのインストール] ページで、[次へ] をクリックします。
7. [プリンター名を入力してください] ページで「ResearchPRT」と入力し、[次へ] をクリックします。
8. [プリンター共有] ページで、[次へ] をクリックします。
9. [ResearchPRT が正しく追加されました] ページで、[完了] をクリックします。

GPO を作成する

1. グループ ポリシーの管理に切り替えます。
2. グループ ポリシーの管理で、[ドメイン]、[Adatum.com] の順に展開し、[グループ ポリシー オブジェクト] を右クリックして、[新規] をクリックします。
3. [新しい GPO] ダイアログ ボックスで「Adatum Network Printers GPO」と入力し、[OK] をクリックします。
4. [グループ ポリシー オブジェクト] ノードをクリックし、[Adatum Network Printers GPO] を右クリックして、[編集] をクリックします。
5. グループ ポリシー管理エディターで、[ユーザーの構成]、[基本設定]、[コントロール パネルの設定] の順に展開し、[プリンター] をクリックします。
6. [プリンター] を右クリックし、[新規作成]、[共有プリンター] の順にクリックします。
7. [新しい共有プリンターのプロパティ] ダイアログ ボックスの [全般] タブで、次の値を使用します。
 - 共有パス : \\LON-DC1\\ResearchPRT
 - このプリンターを通常使うプリンターとして設定する : オン
8. [共通] タブで、次の値を使用します。
 - ログオンしているユーザーのセキュリティ コンテキストで実行する (ユーザー ポリシー オプション) : オン


- 項目レベルで対象化する: オン

9. [対象化] をクリックします。
10. [ターゲット エディター] ダイアログ ボックスの [新しい項目] ドロップダウン リストで、[セキュリティ グループ] をクリックし、[省略 (...)] をクリックします。
11. [グループの選択] ダイアログ ボックスで「Research」と入力し、[OK] をクリックします。
12. [ターゲット エディター] ダイアログ ボックスで、[OK] をクリックします。
13. [新しい共有プリンターのプロパティ] ダイアログ ボックスで、[OK] をクリックします。
14. グループ ポリシー管理エディターを閉じます。


▶ 作業 3: 基本設定が適用されていることを検証する

GPO を適用する前に設定を確認する


1. LON-CL1 で、ユーザー名「Adatum¥Allie」、パスワード「Pa\$\$w0rd」を使用してサインインします。
2. タスク バーで、[エクスプローラー] アイコンをクリックします。
3. エクスプローラーで、[PC] をクリックします。

 **注:** ネットワーク ドライブが表示されないことを確認します。

4. [スタート]、[設定]、[デバイス] の順にクリックします。

 **注:** ResearchPRT プリンターがないことを確認します。

5. LON-CL2 に切り替えます。
6. LON-CL2 で、ユーザー名「Adatum¥Dan」、パスワード「Pa\$\$w0rd」を使用してサインインします。
7. タスク バーで、[エクスプローラー] アイコンをクリックします。
8. エクスプローラーで、[PC] をクリックします。

 **注:** ネットワーク ドライブが表示されないことを確認します。

GPO をリンクする

1. LON-DC1 に切り替えます。
2. LON-DC1 で、サーバー マネージャーに切り替えます。
3. サーバー マネージャーで、[ツール]、[グループ ポリシーの管理] の順にクリックします。
4. グループ ポリシーの管理のコンソール ツリーで、[Adatum.com] ドメインを右クリックし、[既存の GPO のリンク] をクリックします。
5. [GPO の選択] ダイアログ ボックスで、[Adatum Mapped Drives GPO]、[OK] の順にクリックします。
6. ツリーで [Adatum.com] ドメインを右クリックし、[既存の GPO のリンク] をクリックします。
7. [GPO の選択] ダイアログ ボックスで、[Adatum Network Printers GPO]、[OK] の順にクリックします。

GPO を適用し設定を確認する

1. LON-CL1 に切り替えます。
2. LON-CL1 で、[スタート] をクリックし「cmd」と入力して、Enter キーを押します。

3. コマンド プロンプトで、次のコマンドを入力し、Enter キーを押します。

```
GPUdate
```

4. エクスプローラーに切り替え、ネットワーク ドライブが表示されていることを確認します。
5. デバイス ウィンドウに切り替え、[ResearchPRT (LON-DC1 上)] プリンターが表示されていることを確認します。
6. LON-CL2 に切り替えます。
7. LON-DC2 で、[スタート] をクリックし「cmd」と入力して、Enter キーを押します。
8. コマンド プロンプトで、次のコマンドを入力し、Enter キーを押します。

```
GPUdate
```

9. エクスプローラーに切り替え、ネットワーク ドライブが表示されていることを確認します。

結果：この練習により、ドライブ マップとネットワーク プリンターの基本設定を作成し、GPO を使用してそれらを割り当てることができました。

▶ 次の章の準備をする

演習が完了したら、仮想マシンを初期状態に戻します。

1. ホスト コンピューターで、Hyper-V マネージャーを起動します。
2. [仮想マシン] リストで、[23697-2B-LON-DC1] を右クリックし、[戻す] をクリックします。
3. [仮想マシンを戻す] ダイアログ ボックスで、[戻す] をクリックします。
4. 23697-2B-LON-CL1 と 23697-2B-LON-CL2 に対して、手順 2 ～ 3 を繰り返します。