

# PowerShell Constrained Language Mode 導入手順書

## WDAC（Windows Defender Application Control）を使用した実装

文書バージョン: 1.0

作成日: 2025年10月6日

対象者: IT初心者・システム管理者

所要時間: 約2-3時間（テスト含む）

### 目次

- [1. 事前準備](#)
- [2. 環境要件の確認](#)
- [3. テスト環境の準備](#)
- [4. WDACポリシーの作成](#)
- [5. ポリシーの適用とテスト](#)
- [6. 本番環境への展開](#)
- [7. トラブルシューティング](#)
- [8. ロールバック手順](#)

### 事前準備

#### 必要なもの

- ☐ Windows 10 Pro/Enterprise（バージョン1903以降）またはWindows 11
- ☐ 管理者権限を持つアカウント
- ☐ バックアップ済みのシステム（推奨）
- ☐ テスト用のPCまたは仮想マシン（強く推奨）
- ☐ 約2GB以上の空きディスク容量

#### ⚠ 重要な注意事項

必ずお読みください：

- 本番環境で直接作業しないでください**
  - 設定ミスで業務システムが動かなくなる可能性があります
  - 必ずテスト環境で動作確認してから本番適用してください
- バックアップを取得してください**
  - システムの復元ポイントを作成

- 重要なデータをバックアップ

### 3. 作業時間の確保

- 業務時間外での作業を推奨
- ロールバックの時間も考慮（+1時間）

---

## 環境要件の確認

### 手順1: Windowsバージョンの確認

1. キーボードで `Windows キー + R` を押す
2. 「ファイル名を指定して実行」ウィンドウが開きます
3. `winver` と入力して「OK」をクリック

#### 確認ポイント：

- Windows 10の場合：バージョン1903以降であることを確認
- Windows 11の場合：すべてのバージョンで対応

✅ OK: Windows 10 バージョン 2004（例）

❌ NG: Windows 10 バージョン 1809以前

### 手順2: PowerShellバージョンの確認

1. スタートメニューを開く
2. 「PowerShell」と検索
3. 「Windows PowerShell」を右クリック
4. 「管理者として実行」を選択
5. 以下のコマンドを入力してEnterキーを押す

#### コマンド：

```
$PSVersionTable.PSVersion
```

#### 確認ポイント：

- Major（メジャーバージョン）が5以上であることを確認

✅ 期待される表示例：


### 手順3: 管理者権限の確認

PowerShellウィンドウのタイトルバーに「管理者」と表示されていることを確認してください。

表示されていない場合は、手順2に戻り、必ず「管理者として実行」で起動してください。

---

## テスト環境の準備

 **本番環境では絶対に作業しないでください**

### オプションA: 仮想マシンを使用する場合（推奨）

Hyper-Vを使用する場合：

1. コントロールパネルを開く
2. 「プログラム」→「Windowsの機能の有効化または無効化」
3. 「Hyper-V」にチェックを入れる
4. PCを再起動
5. 「Hyper-V マネージャー」を開く
6. テスト用のWindows仮想マシンを作成

VMware/VirtualBoxを使用する場合：

- 各ソフトウェアのマニュアルに従ってテストVMを作成

### オプションB: テスト用PCを使用する場合

業務に影響しない独立したPCを用意してください。

---

## WDACポリシーの作成

### 手順1: 作業フォルダの作成

1. 管理者PowerShellを開く（前述の手順参照）
2. 以下のコマンドを**1行ずつ**実行：

コマンド1（作業フォルダを作成）：

```
New-Item -Path "C:\WDACPolicy" -ItemType Directory
-Force
```

コマンド2（作業フォルダに移動）：

```
Set-Location -Path "C:\WDACPolicy"
```

確認：

- エラーが表示されないことを確認
- `C:\WDACPolicy` フォルダが作成されたことをエクスプローラーで確認

## 手順2: ベースポリシーの作成

以下のコマンドを実行します：

```
Copy-Item -Path "C:\Windows\schemas\CodeIntegrity
\ExamplePolicies\AllowMicrosoft.xml" -Destination
"C:\WDACPolicy\InitialPolicy.xml"
```

確認：

- `C:\WDACPolicy\InitialPolicy.xml` ファイルが作成されたことを確認

## 手順3: ポリシーの編集（PowerShell CLM有効化）

以下のコマンドを実行して、PowerShell CLMを有効化するルールを追加します：

```
Set-RuleOption -FilePath "C:\WDACPolicy
\InitialPolicy.xml" -Option 3
```

オプション3の意味：

- PowerShellのConstrained Language Modeを有効化する設定

## 手順4: 監査モードの設定（重要）

本番適用前に、まず「監査モード」で動作確認を行います。

コマンド1（オプション3を一旦削除）：

```
Set-RuleOption -FilePath "C:\WDACPolicy
\InitialPolicy.xml" -Option 3 -Delete
```

コマンド2（監査モードを有効化）：

```
Set-RuleOption -FilePath "C:\WDACPolicy  
\InitialPolicy.xml" -Option 0
```

### 監査モードとは：

- ポリシー違反があっても実行をブロックしない
- 違反をイベントログに記録するだけ
- 安全にテストできる

## 手順5: ポリシーのバイナリ変換

XMLポリシーをWindowsが読み込める形式に変換します：

```
ConvertFrom-CIPolicy -XmlFilePath "C:\WDACPolicy  
\InitialPolicy.xml" -BinaryFilePath "C:\WDACPolicy  
\InitialPolicy.bin"
```

### 確認：

- `C:\WDACPolicy\InitialPolicy.bin` ファイルが作成されたことを確認
- ファイルサイズが 0KB でないことを確認

## 手順6: ポリシーファイルの配置

```
Copy-Item -Path "C:\WDACPolicy\InitialPolicy.bin"  
-Destination "C:\Windows\System32\CodeIntegrity  
\SIPolicy.p7b" -Force
```

---

## ポリシーの適用とテスト

### 手順1: ポリシーの有効化

コマンド1（ポリシーの更新）：

```
Invoke-CimMethod -Namespace root\Microsoft\Windows  
\CI -ClassName PS_UpdateAndCompareCIPolicy  
-MethodName Update -Arguments @{FilePath =  
"C:\Windows\System32\CodeIntegrity\SIPolicy.p7b"}
```

または、より簡単な方法（PCを再起動）：

Restart-Computer -Confirm

⚠️ 再起動の確認プロンプトで「はい」を選択してください

## 手順2: CLMの動作確認

PCが再起動したら、以下の手順でCLMが有効になっているか確認します：

1. 通常の（管理者権限でない）PowerShellを開く
2. 以下のコマンドを実行：

コマンド：

```
$ExecutionContext.SessionState.LanguageMode
```

期待される結果：

```
ConstrainedLanguage
```

✅ 成功: `ConstrainedLanguage` と表示される

❌ 失敗: `FullLanguage` と表示される → トラブルシューティングへ

## 手順3: 制限の動作テスト

CLMが正しく機能しているか、以下のテストを実行します：

### テスト1: 危険なコマンドの制限確認

以下のコマンドはCLMでエラーになるはずです：

```
Add-Type -TypeDefinition "public class Test {}"
```

期待される結果：

```
エラー: ConstrainedLanguage モードではこの操作は  
サポートされていません
```

### テスト2: 基本的なコマンドの動作確認

以下のコマンドは正常に動作するはずです：

```
Get-Process | Select-Object -First 5  
Get-Date
```

これらが正常に動作すればOKです。

## 手順4: イベントログの確認

監査モードでの違反を確認します：

1. スタートメニューから「イベントビューアー」を検索して開く
2. 左側のツリーで以下を展開：
  - 「アプリケーションとサービス ログ」
  - 「Microsoft」
  - 「Windows」
  - 「CodeIntegrity」
  - 「Operational」
3. ログを確認：
  - イベントID 3076: ブロックされたファイル情報
  - イベントID 3077: 監査モードでの違反

確認すべき項目：

- 業務アプリケーションが違反ログに記録されていないか
  - 予期しないブロックが発生していないか
- 

## 本番環境への展開

 監査モードで1週間以上問題がないことを確認してから実施

### 手順1: 強制モードへの変更

テスト環境で問題がなければ、強制モードに変更します：

コマンド1（監査モードを無効化）：

```
Set-RuleOption -FilePath "C:\WDACPolicy  
\InitialPolicy.xml" -Option 0 -Delete
```

コマンド2（バイナリに再変換）：

```
ConvertFrom-CIPolicy -XmlFilePath "C:\WDACPolicy  
\InitialPolicy.xml" -BinaryFilePath "C:\WDACPolicy  
\InitialPolicy.bin"
```

コマンド3（システムに再配置）：

```
Copy-Item -Path "C:\WDACPolicy\InitialPolicy.bin"  
-Destination "C:\Windows\System32\CodeIntegrity  
\SIPolicy.p7b" -Force
```

コマンド4（再起動）：

```
Restart-Computer -Confirm
```

## 手順2: 本番環境での展開方法

小規模環境（10台未満）の場合：

- 上記手順を各PCで手動実行

中規模以上の環境の場合：

- グループポリシー経由での展開を推奨
- または、IntuneなどのMDMツールを使用

グループポリシーでの展開手順：

1. ドメインコントローラーで「グループポリシー管理」を開く
2. 新しいGPOを作成（例: "WDAC-PowerShell-CLM"）
3. GPOを編集：
  - 「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」
  - 「アプリケーション制御ポリシー」
  - 「Windows Defender Application Control」
4. ポリシーファイル（SIPolicy.p7b）を配置
5. 対象のOUにリンク

## 手順3: 段階的な展開計画

1. フェーズ1（第1週）：テスト部門の5-10台に展開
2. フェーズ2（第2週）：問題なければ50%のPCに展開
3. フェーズ3（第3週）：残りすべてのPCに展開

---

## トラブルシューティング



## 問題1: CLMが有効にならない

症状： `$ExecutionContext.SessionState.LanguageMode` が `FullLanguage` のまま

原因と対処：

### 1. ポリシーが正しく配置されていない 確認コマンド：

```
Test-Path "C:\Windows\System32\CodeIntegrity\SIPolicy.p7b"
```

- False の場合：手順6を再実行

### 2. 再起動していない

- PCを再起動してください

### 3. PowerShellを管理者権限で実行している

- 管理者権限のPowerShellはCLMの対象外です
- 通常のPowerShellで確認してください

## 問題2: 業務アプリケーションが動かない

症状： 特定のアプリケーションやスクリプトが実行できない

対処法：

### 1. イベントログを確認

- CodeIntegrity ログでブロックされたファイルを特定

### 2. 許可ルールを追加 コマンド1（ブロックされたアプリのルールを追加）：

```
New-CIPolicy -ScanPath "C:\Program Files\YourApp"
-UserPEs -FilePath "C:\WDACPolicy\AppPolicy.xml"
-Level Publisher -Fallback Hash
```

コマンド2（既存ポリシーとマージ）：

```
Merge-CIPolicy -PolicyPaths "C:\WDACPolicy\InitialPolicy.xml", "C:\WDACPolicy\AppPolicy.xml"
-OutputFilePath "C:\WDACPolicy\MergedPolicy.xml"
```

### 3. ポリシーを再適用

- 手順5-6を再度実行

## 問題3: PowerShellスクリプトがエラーになる

症状： 既存のPowerShellスクリプトが動作しない

原因： CLMでは以下の機能が制限されます：

- Add-Type コマンド
- 動的なコード実行 (Invoke-Expression)
- .NETクラスの直接呼び出し

対処法：

#### 1. スクリプトの書き換え

- CLM対応の代替コマンドを使用
- 例: `Invoke-Expression` → `&{ }` ブロック

#### 2. 信頼されたスクリプトとして署名

- コード署名証明書でスクリプトに署名
- 署名されたスクリプトはCLMでも制限が緩和されます

### 問題4: システムが起動しない

症状：ポリシー適用後、Windowsが正常に起動しない

緊急対処（セーフモード起動）：

1. PC起動時にF8キーを連打
2. 「セーフモード」を選択
3. 管理者PowerShellでポリシーを削除：

```
Remove-Item "C:\Windows\System32\CodeIntegrity  
\SIPolicy.p7b" -Force
```

4. 通常モードで再起動

---

## ロールバック手順

### 緊急時のポリシー無効化

コマンド1（ポリシーファイルを削除）：

```
Remove-Item -Path "C:\Windows\System32\CodeIntegrity  
\SIPolicy.p7b" -Force
```

コマンド2（PCを再起動）：

```
Restart-Computer -Force
```

再起動後、CLMは無効になり、PowerShellは通常モード（FullLanguage）に戻ります。

## 確認

\$ExecutionContext.SessionState.LanguageMode

結果: FullLanguage

---

## 運用管理

### 定期的な確認項目

#### 月次チェックリスト：

- ☐ イベントログでブロックされたアプリケーションを確認
- ☐ ユーザーからの問い合わせ記録を確認
- ☐ ポリシーの更新が必要か検討

#### 四半期チェックリスト：

- ☐ 新規導入アプリケーションのホワイトリスト追加
- ☐ Windowsアップデート後の動作確認
- ☐ ポリシー設定の見直し

### ポリシーの更新手順

1. 変更内容をXMLファイルに反映
2. バイナリに変換
3. テスト環境で動作確認
4. 本番環境に展開

### ドキュメント管理

以下を記録・保管してください：

- ポリシーXMLファイルのバックアップ
  - 変更履歴
  - トラブル対応記録
  - ユーザーからの問い合わせ記録
- 

## 付録A: よくある質問

Q1: 管理者権限のPowerShellはCLMになりますか？

A1: いいえ、管理者権限で実行されているPowerShellはCLMの対象外です。これは意図的な設計です。

Q2: 既存のPowerShellスクリプトは動かなくなりますか？

A2: 基本的なスクリプトは問題ありませんが、Add-TypeやInvoke-Expressionを使用しているスクリプトは修正が必要です。

Q3: ユーザーへの影響は？

A3: 一般ユーザーが通常業務でPowerShellを直接使用することは少ないため、影響は限定的です。

Q4: CLMは無効化できますか？

A4: はい、ポリシーファイルを削除して再起動すれば無効化できます。

Q5: 署名されたスクリプトはCLMでも動きますか？

A5: コード署名証明書で署名されたスクリプトは、CLMでも一部の制限が緩和されます。

付録B: 用語集

用語	説明
WDAC	Windows Defender Application Control。Windowsのアプリケーション実行制御機能
CLM	Constrained Language Mode。PowerShellの制限モード
ポリシー	アプリケーション実行の許可/禁止ルール
監査モード	ブロックせずにログのみ記録するモード
強制モード	ポリシー違反を実際にブロックするモード
バイナリ	コンピューターが読み込める形式のファイル

付録C: チェックリスト

導入前チェックリスト

- ☐ Windows 10 バージョン1903以降、またはWindows 11
- ☐ 管理者権限アカウントの準備
- ☐ テスト環境の準備完了
- ☐ システムバックアップ取得済み
- ☐ 関係部署への事前通知完了

導入中チェックリスト

- ☐ 作業フォルダ作成完了

- ☐ ベースポリシー作成完了
- ☐ CLMオプション設定完了
- ☐ 監査モード設定完了
- ☐ バイナリ変換完了
- ☐ ポリシーファイル配置完了
- ☐ テスト実施完了

導入後チェックリスト

- ☐ CLM有効化確認完了
- ☐ 制限動作テスト完了
- ☐ イベントログ確認完了
- ☐ ユーザー動作確認完了
- ☐ 問題なく1週間経過
- ☐ 本番展開計画策定完了

改訂履歴

バージョン	日付	変更内容	作成者
1.0	2025/10/06	初版作成	-

問い合わせ先

本手順書に関する質問や問題が発生した場合：

社内連絡先：

- 情報システム部門
- DX推進課

外部サポート：

- Microsoft サポート: <https://support.microsoft.com/>

本書の使用にあたって：

この手順書は一般的な環境を想定して作成されています。お使いの環境によっては追加の設定や調整が必要になる場合があります。不明な点がある場合は、必ず情報システム部門に相談してください。