

## Blue Prism Data Protectorツール


Blue Prism Data Protectorツールを使用して、appsettings.jsonファイルに格納されている接続文字列を復号および暗号化します。セキュリティ上の理由から、接続文字列は暗号化されますが、Blue Prism Data Protectorツールでは文字列を復号できるため、必要に応じて変更して再度暗号化できます。

BluePrismDataProtector.Consoleツールはコマンドラインツールで、管理者として実行しているWindows PowerShellで使用する必要があります。

### 接続文字列を復号する

ツールを使用して接続文字列を復号するには:

1. Blue PrismポータルからBluePrismDataProtector.Console.exeファイルをダウンロードし、デバイスの任意の場所に保存します。
2. BluePrismDataProtector.Console.exeがあるフォルダーで、管理者としてPowerShellを開きます。  
管理者: Windows PowerShell] ウィンドウが表示されます。

 コマンドラインに「.\BluePrismDataProtector.Console.exe」と入力してEnterを押すと、使用可能なコマンドのリストが表示されます。

3. Windowsエクスプローラーから、復号する文字列を含むappsettings.jsonファイルを開き、コピーします。  
例:

```
"HubServiceBus": {  
  "Connection": "CfDj8LadX9spUNhMhvbXtcsxZYTHFA3m8Ty1-Z_EZ0Zn16mYfv_23Q2D2waPDTBxaz4-viN02Akk-S5C73dNjOdGHifGCxSIftwExJ304FuDXHpbNo0be-xyQt1D1-j7rosuYw",  
  "Topic": "thttopic",  
  "Subscription": "Hub",
```

4. PowerShellで、次のように入力します。

```
.\BluePrismDataProtector.Console.exe unprotect -v "[string]" -p "[path]"
```

ここでは、

[string] = ファイルからコピーされた文字列

[path] = DataProtectionKeysへのパス。通常は、C:\Program Files (x86)\Blue Prism\DataProtectionKeys

例:


```
.\BluePrismDataProtector.Console.exe unprotect -v "CfDj8LadX9spUNhMhvbXtcsxZYTHFA3m8Ty1-Z_EZ0Zn16mYfv_23Q2D2waPDTBxaz4-viN02Akk-S5C73dNjOdGHifGCxSIftwExJ304FuDXHpbNo0be-xyQt1D1-j7rosuYw" -p "C:\Program Files (x86)\Blue Prism\DataProtectionKeys"
```

5. Enterキーを押します。  
文字列が復号され、暗号化されていない値がPowerShellに表示されます。

## 接続文字列を暗号化する

ツールを使用して接続文字列を暗号化するには:

1. BluePrismDataProtector.Console.exeがあるフォルダーで、管理者としてPowerShellを開きます。  
管理者: Windows PowerShell] ウィンドウが表示されます。

 コマンドラインに「.\BluePrismDataProtector.Console.exe」と入力してEnterを押すと、使用可能なコマンドのリストが表示されます。

2. PowerShellで、次のように入力します。

```
.\BluePrismDataProtector.Console.exe protect -v "[string]" -p "[path]"
```

ここでは、


[string] = 暗号化する文字列

[path] = DataProtectionKeysへのパス。通常は、C:\Program Files (x86)\Blue Prism\DataProtectionKeys

例:

```
.\BluePrismDataProtector.Console.exe unprotect -v "Str0ngP@S$w0rd" -p "C:\Program Files (x86)\Blue Prism\DataProtectionKeys"
```

3. Enterキーを押します。  
文字列が暗号化され、PowerShellに値が表示されます。例:  
CfDJ8LadX9spUNhMhvbXtcsxZYTHFA3m8Tyl-Z\_EZ0Znl6mYfv\_23Q2D2waPDTBXaz4-viNO2Akk-S5C73dnJodGHifGCxSiftwExJ3O4FuDXHpbNo0be-xyQt1D1-j7rosuYw
4. 暗号化された文字列をappsettings.jsonファイルの適切な場所にコピーし、ファイルを保存します。
5. IISマネージャーを開き、適切なアプリケーションプールを再起動して、新しい接続文字列を使用していることを確認します。

 PowerShell自体のコマンドに関連付けられている文字列に文字がある場合、意図したとおりにPowerShellが文字列を受け入れるように、文字列にエスケープ文字を追加する必要があります。以下のような例:

- 「`」と「\$」は、文字の前に「`」(バックティック)が必要です。たとえば「Str0ng`P@\$SW0rD」は、コマンドラインで「Str0ng`P@`\$`\$W0rD」と入力する必要があります。
- 「"」は、文字の前に「\"」が必要です。たとえば、「P@\$"W0rD」は、コマンドラインで「P@`\$`"W0rD」と入力する必要があります。

これらの追加エスケープ文字により、文字列の整合性が維持されます。結果の暗号化値が再び復号された場合、値はコマンドラインバージョンではなく元の文字列と一致します。