


# Windowsの運用管理を快適にする
# 10の裏ワザ／表ワザ

## セキュリティ編

山市 良 著

更新管理に役立つバージョン、ビルド情報の取得
- 製品名、バージョン情報、詳細なビルド番号の情報を取得するさまざまな方法
  - Windows標準のバージョン情報
  - その他のコマンドライン
  - レジストリから取得
  - リモートマシン、仮想マシンから情報を取得する方法

Windows Updateはお任せではなく、戦略的に
- 長く変わらず、信頼できるWindows Update Agent（WUA） API
  - SconfigユーティリティとWindows Admin CenterはWUA APIで動く
- 不足しているセキュリティ更新をレポートする（オンラインスキャン）
- 不足しているセキュリティ更新をレポートする（オフラインスキャン）
- 更新履歴を表示する
- ディスク領域節約と更新時間の改善に効く、Windows Updateのクリーンアップ
  - %WINDIR%¥SoftwareDistributionのリセット

現在のセキュリティ設定を推奨基準と比較する
  - Microsoft Security Compliance Toolkit（SCT）の入手と準備
  - SCTによる現在のローカル設定の評価
  - SCTによるグループポリシー設定の評価
  - ベースラインからのGPOの作成
  - ベースラインのローカルインストール（非推奨）

セイ・テクノロジーズからのお知らせ
- 自立分散型サーバー監視ソフト『BOM for Windows』
  - システム安定運用-セキュリティテンプレート
    - Windows バージョン取得監視
    - Windows Update 成否リスト取得監視
    - Windows Update未適用リスト取得監視
  - 参考情報
- サーバー設定仕様書自動生成サービス『SSD-assistance』
- お問い合わせ

## 免責事項

本書に記載された情報は、予告無しに変更される場合があります。セイ・テクノロジーズ株式会社は、本書に関していかなる種類の保証 (商用性および特定の目的への適合性の黙示の保証を含みますが、これに限定されません) もいたしません。
セイ・テクノロジーズ株式会社は、本書に含まれた誤謬に関しての責任や、本書の提供、履行および使用に関して偶発的または間接的に起こる損害に対して、責任を負わないものとします。

## 著作権

本書のいかなる部分も、セイ・テクノロジーズ株式会社からの文書による事前の許可なしには、形態または手段を問わず、決して複製・配布してはなりません。

## 商標

文中の社名、製品名、サービス名等は各社の商標または登録商標である場合があります。
なお、本文および図表中では「™ (Trademark)」、「® (Registered Trademark)」を明記しておりません。

## 注記

本文にある下記は、コマンドラインを示し、コピーして利用する際は ↲ を削除してください。

> Get-ComputerInfo | Select WindowsProductName,WindowsVersion, OsBuildNumber ↲
>
> WMIC OS Get Caption, Version ↲

# 更新管理に役立つバージョン、ビルド情報の取得

Windows 10およびWindows Server 2016以降は、半期チャネル（Semi-Annual Channel、SAC）と長期サービスチャネル（LTSC、旧称LTSB）の2つのサービスチャネルで提供されています（Windows ServerのSACはバージョン1709から）。SACは年に2回、LTSCは数年に1回に新バージョン（Windows 10では機能更新プログラムと呼びます）がリリースされ、SACのサービス期間は現在、原則18か月、下半期リリースのEnterpriseおよびEducationエディションについては30か月、LTSCは10年（メインストリーム5年＋延長サポート5年）となっており、サービス期間中、セキュリティ更新やバグ修正を含む品質更新プログラムが提供されます。

Windows 10およびWindows Server 2016以降のバージョン番号は、OSビルド番号（10.0.は省略する場合があります）と1対1で対応します（表1）。

**表1　Windows 10およびWindows Server 2016以降のバージョンとOSビルド、サービス期間**

| サービスチャネル | バージョン | OSビルド | サービス期間 |
|---|---|---|---|
| SAC | なし<br>（便宜上1507） | 10.0.10240.x | 既に終了 |
| LTSC（LTSB） | 2015 | 10.0.10240.x | Enterprise LTSB 10年 |
| SAC | 1511 | 10.0.10586.x | 既に終了 |
| SAC | 1607 | 10.0.14393.x | 既に終了 |
| LTSC（LTSB） | 2016（1607） | 10.0.14393.x | Enterprise LTSB 10年<br>Server 10年 |
| SAC | 1703 | 10.0.15063.x | 既に終了 |
| SAC | 1709 | 10.0.16299.x | 既に終了 |
| SAC | 1803 | 10.0.17134.x | 既に終了*1 |
| SAC | 1809 | 10.0.17763.x | 既に終了*2 |
| LTSC | 2019（1809） | 10.0.17763.x | Enterprise LTSC 10年<br>Server 10年 |
| SAC | 1903 | 10.0.18362.x | 全エディション 18か月 |
| SAC | 1909 | 10.0.18363.x | Home/Pro/Server 18か月*1<br>Enterprise/Education 30か月 |
| SAC | 2004 | 10.0.19041.x | 全エディション 18か月 |
| SAC | 20H2 | 10.0.19042.x | Home/Pro/Server 18か月<br>Enterprise/Education 30か月 |
| SAC | 21H1 | 10.0.19043.x | 全エディション 18か月 |
| SAC | 21H2 | 10.0.19044.x | Home/Pro 18か月<br>Enterprise/Education 30か月 |

| サービスチャネル | バージョン | OSビルド | サービス期間 |
| --- | --- | --- | --- |
| LTSC | 2022（21H2） | 10.0.19044.x | Enterprise LTSC 5年*3<br>Server 10年 |

*1　2021年5月11日ですべてのサービス期間が終了しました。
*2　2020年11月10日ですべてのサービス期間が終了しました。
*3　Windows 10 Enterprise LTSC 2022はサービス期間が5年に短縮されることが発表されています（IoT Enterprise LTSC 2022は10年のまま）。

WindowsおよびWindows Serverの毎月の品質更新プログラムは、前月までの更新内容を累積した累積更新プログラムとして提供されます。OSビルド番号の最も左に位置するリビジョン番号（表1の.xの部分）は、Windowsの累積更新プログラムによってインクルメントされます。つまり、リビジョン番号を参照すれば、OSの更新状態を判断できるということです。最新の累積更新プログラムがインストールされたWindows 10およびWindows Server 2016以降のOSビルド番号は、以下のWindows 10 release informationのページで確認することができます。また、最新状態にするための累積更新プログラムのKB番号を確認することもできます。

Windows 10 release information

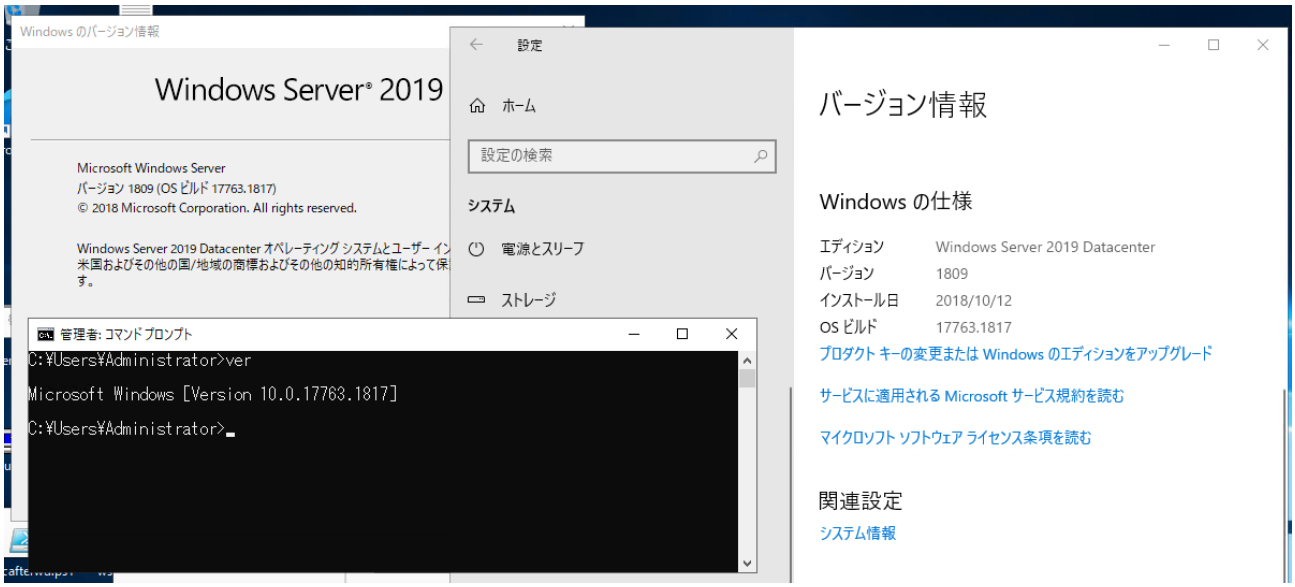
https://docs.microsoft.com/en-us/windows/release-health/release-information

## 製品名、バージョン情報、詳細なビルド番号の情報を取得するさまざまな方法

GUIツールやコマンドラインを使用して、Windowsの製品名、バージョン情報、ビルド番号を取得するいくつかの方法を紹介します。

### Windows標準のバージョン情報

Windows 10およびWindows Server 2016以降のデスクトップエクスペリエンス（LTSCのみ）では、［設定］アプリの［システム］の［詳細情報］（バージョン1909以前は［バージョン情報］）やwinverコマンドで開く［Windowsのバージョン情報］から、OSの製品名、バージョン、およびリビジョン番号を含むOSビルド番号を確認することができます。Windows 10およびWindows Serverのバージョン1709からは、コマンドプロンプトのcmdコマンド（またはcmd /c "ver"）の実行結果にもリビジョン番号を含むOSビルド番号を確認できるようになりました（それ以前はリビジョン番号を含まないOSビルド番号）。



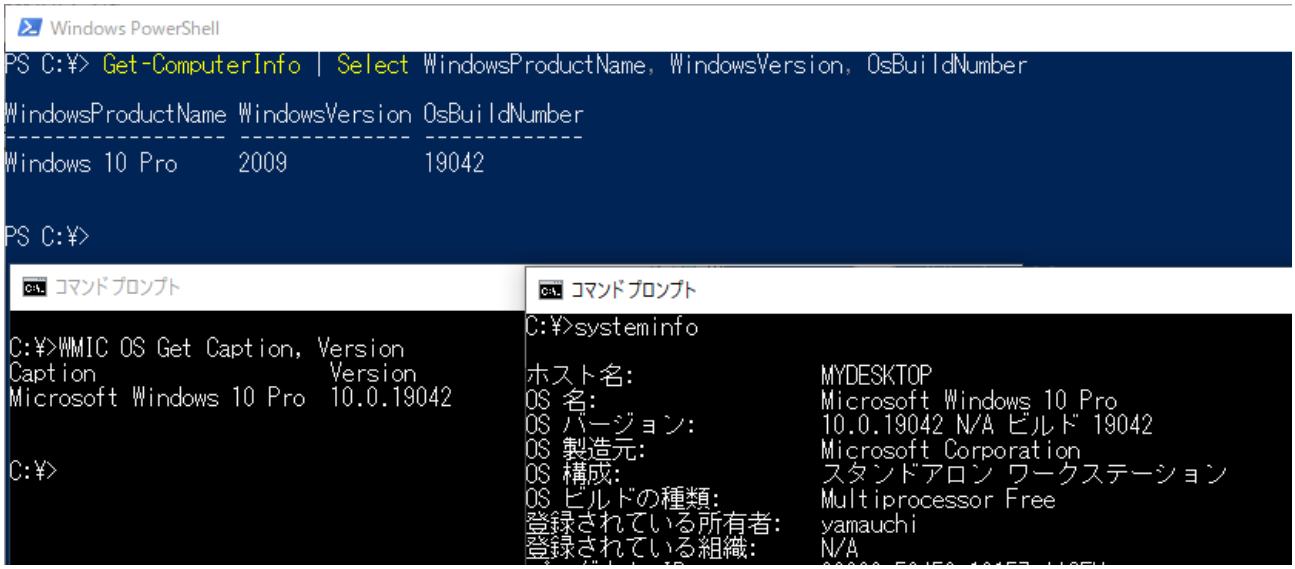

**画面1　Windows標準のバージョン情報**

### その他のコマンドライン

コマンドラインで製品名やOSビルド番号を確認する他の方法としては、Get-ComputerInfoコマンドレット、WMICコマンド、およびSysteminfoコマンドを利用できます。次のコマンドラインを実行すると同等の情報を取得できます（↲ は Enter キーまたは改行位置、以下同じ*1）。ただし、これらのコマンドでリビジョン番号までは知ることはできません。

```
Get-ComputerInfo | Select WindowsProductName,WindowsVersion, OsBuildNumber ↲

WMIC OS Get Caption, Version ↲
```




**画面2　Get-ComputerInfo、WMIC、Systeminfo コマンドによる製品名、バージョン情報、ビルド番号の取得**

## レジストリから取得

Windowsの製品名、バージョン番号、ビルド番号、リビジョン番号は、レジストリキーHKEY_LOCAL_MACHINE（HKLM）¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersionにある表2に示すレジストリ値に格納されています。参考として、表2にはGet-ComputerInfo、Systeminfo、WMICコマンドとの対応を含めています。

**表2　HKLM¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersionキー内のバージョン情報関連のレジストリ**

| | レジストリ値 | Get-ComputerInfo | Systeminfo | WMIC |
|---|---|---|---|---|
| 製品名 | ProductName | WindowsProductName | OS名 | Caption |
| バージョン番号（2004以前） | ReleaseId | WindowsVersion | なし | なし |
| バージョン番号（20H2以降） | DisplayVersion | なし | なし | なし |
| OSビルド | CurrentBuild | OsBuildNumber | OSバージョン | Version |
| リビジョン番号 | UBR | なし | なし | なし |

例えば、次の1行のコマンドラインを実行すると、リビジョン番号を含む詳細なビルド番号（例：19042.867）を取得することができます。

```
(Get-ItemProperty "HKLM:¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion").CurrentBuild +
"." +(Get-ItemProperty "HKLM:¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion").UBR ↲
```

なお、レジストリ値DisplayVersionは、YYH1/YYH2（YYは西暦下2桁）形式が採用されたWindows 10バージョン20H2から追加されたものであり、以前のバージョンには存在しません。次のコマンドラインを実行すると、DisplayVersionまたはReleaseIdの適切な方からバージョン番号（例：2004、20H2）を取得します。

```
$winver = (Get-ItemProperty "HKLM:¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion" -
ErrorAction SilentlyContinue).DisplayVersion ↲

if($winver -eq $null){ ↲
```

```
$winver = (Get-ItemProperty "HKLM:¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion").ReleaseId ↲

} ↲

Write-Host $winver ↲
```

### リモートマシン、仮想マシンから情報を取得する方法

リモートのWindowsやWindows Serverに対話的にログオンすることなしに、ネットワーク経由で情報を取得するには、PowerShell RemotingのInvoke-Commandコマンドレットが便利です。

Invoke-Commandコマンドレットは次のように実行します。1行目のコマンドラインで資格情報の入力が要求されるので、リモートコンピューターの管理者ユーザーの資格情報を指定してください。なお、PowerShell Remotingを利用するには、リモート接続される側で事前にEnable-PSRemotingを実行し、PowerShell Remotingを許可しておく必要があります。

```
$cred = Get-Credential ↲

Invoke-Command -ComputerName <コンピューター名> -ScriptBlock {<リモートコンピューターで実行するコマンドライン>} -Credential $cred ↲
```

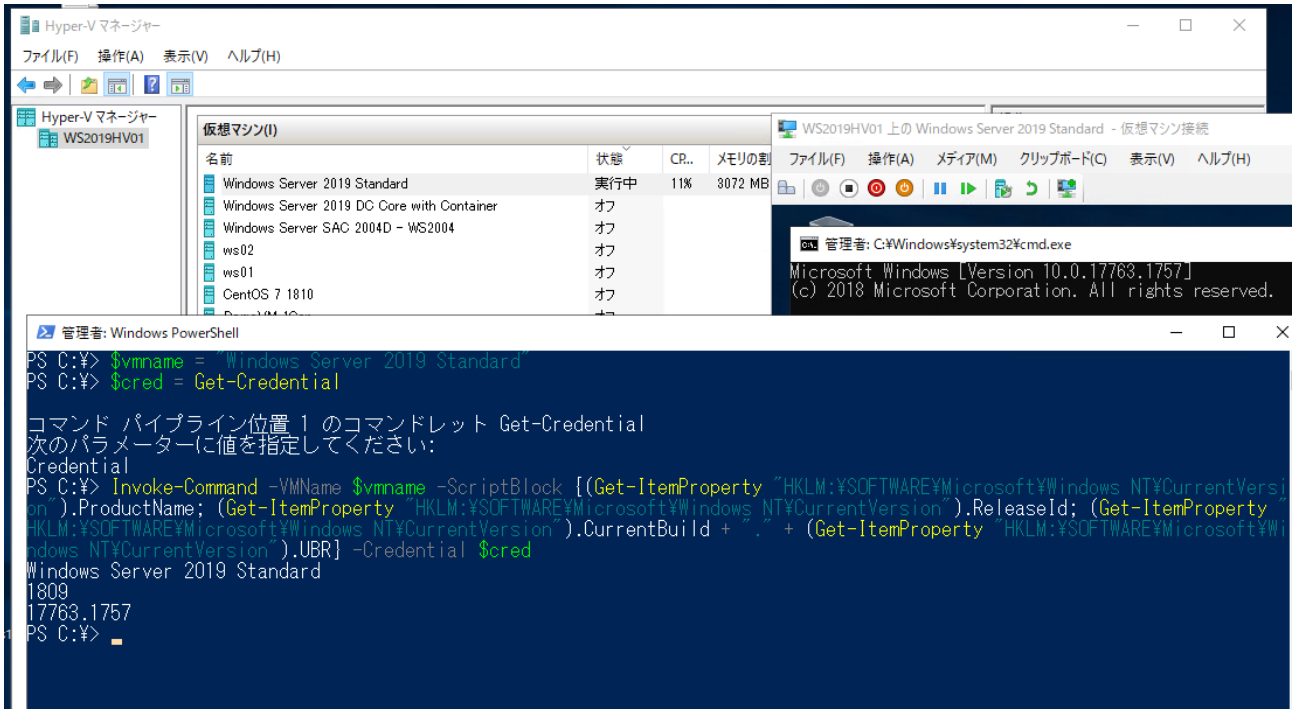
Windows 10またはWindows Server 2016以降のHyper-Vホストでは、Hyper-VホストからWindows 10またはWindows Server 2016以降を実行するWindows仮想マシンのゲストに対してリモート実行できるPowerShell Directを利用できます。PowerShell Remotingによく似ていますが、仮想マシンのネットワーク接続は使用しません。また、ゲスト側でPowerShell Remotingを許可する必要もありません。使い方もPowerShell Remotingによく似ており、-ComputerNameの代わりに-VMNameパラメーターに仮想マシン名を指定します（画面3）。

```
$cred = Get-Credential ↲

Invoke-Command -VMName <仮想マシン名> -ScriptBlock {<リモートコンピューターで実行するコマンドライン>} -Credential $cred ↲
```

次の画面3の実行例では、スクリプトブロックとして以下のコマンドラインを実行するように指定しています。実行結果として、Windowsの製品名、バージョン番号、およびリビジョン番号を含む詳細なビルド番号の3つの情報を取得できます。

```
(Get-ItemProperty "HKLM:¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion").ProductName;
(Get-ItemProperty "HKLM:¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion").ReleaseId;
(Get-ItemProperty "HKLM:¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion").CurrentBuild +
"." + (Get-ItemProperty "HKLM:¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion").UBR ↲
```




**画面3　Hyper-VホストからWindows仮想マシンのゲストに対するPowerShell Directを利用して、バージョン情報を取得しているところ**

PowerShell DirectはWindows 10およびWindows Server 2016以降のHyper-Vゲスト用の統合コンポーネント（Hyper-V PowerShell Direct Service）とやり取りして結果を取得します。そのため、Windows 8.1やWindows Server 2012 R2以前を実行するWindows仮想マシンでは利用できません。また、Linux仮想マシンにクロスプラットフォーム対応のPowerShell 7.0をインストールしても、PowerShell Directで接続できることはありません。

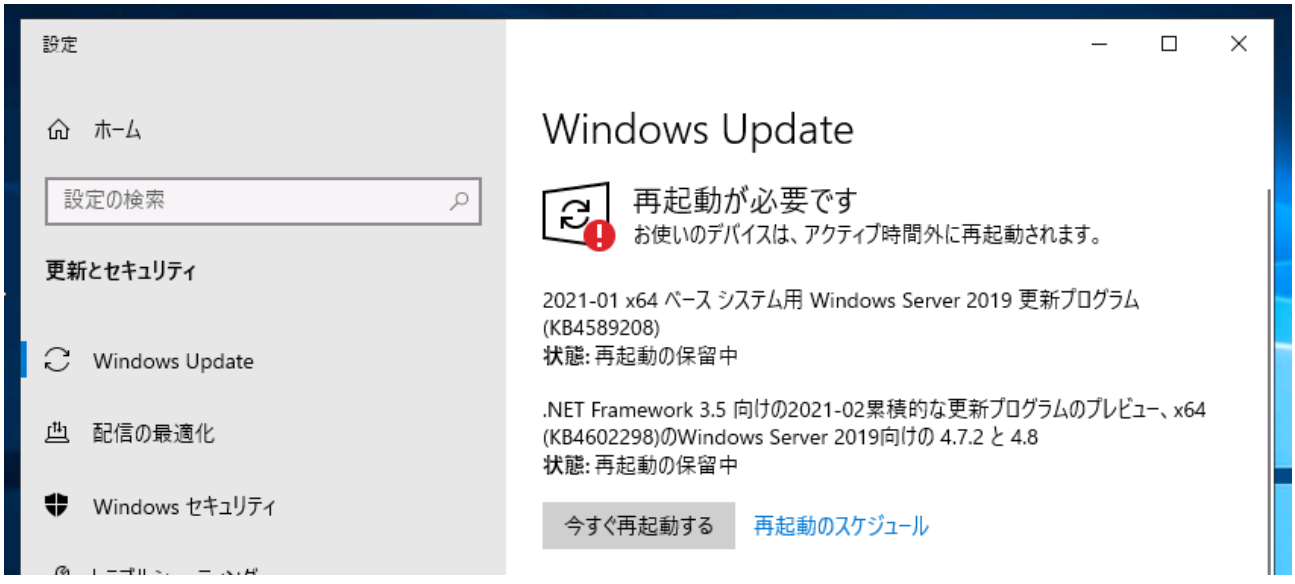
# Windows Updateはお任せではなく、戦略的に

Windows 10になって、Windows Updateの仕組みは大幅に再設計され、Windows 8.1以前のようなユーザー側でコントロールできる部分が少なくなりました。Windows 10になってからも、新しいバージョンで次々に変更が加えられてきています。

Windows 10のWindows Updateの仕組みは、Windows Server 2016以降のデスクトップエクスペリエンスにも共通のものが搭載されています。中には、長期運用が前提のWindows Serverには余計とも思える機能もあります。例えば、再起動が必要な品質更新プログラムのインストールで再起動待ちになり、そのまま放置すると、アクティブ時間外に自動的に再起動が始まってしまう仕様がWindows Serverにも組み込まれています。また、［更新プログラムのチェック］をクリックすると、インストールが必須ではないオプションの更新プログラムのダウンロードとインストールが始まってしまうのも同じOSビルドのWindows 10と同じです。

WindowsおよびWindows Serverの品質更新プログラムは米国時間で毎月第2火曜日にセキュリティ更新を含む累積更新プログラムがリリースされ（Bリリースと呼ぶことがあります）、自動更新が有効な場合は自動配布されます。2021年4月時点では、Windows 10バージョン1809およびWindows Server 2019以降を対象に、その翌週、または翌々週にWindowsと.NET Frameworkのそれぞれに対してオプションの更新プログラムがリリースされます（Cリリース、累積更新プログラムのプレビューと呼ぶことがあります）。.NET FrameworkのBリリース、Cリリースについては、リリースされない月もあります。

オプションの更新プログラムは新たなセキュリティ更新を含まないため、インストールは任意です。オプションの更新プログラムで修正される問題を抱えていて、できるだけすぐに問題を解消したい、重要な変更点をテストしたいといった場合にのみインストールすればよいのです。しかし、［更新プログラムのチェック］をクリックしてしまうと、意図せず、オプションの更新プログラムを受け取ってしまいます（画面4）。




画面4　［更新プログラムのチェック］をクリックしてしまうと、意図せず、オプションの更新プログラムのダウンロードとインストールが始まってしまうことがある。アクティブ時間外の自動再起動もサーバーの安定運用を妨げる余計な機能

## 長く変わらず、信頼できるWindows Update Agent（WUA） API

古いバージョンのWindowsから引き継いだ、変更されていない更新機能の1つに、Windows Update Agent（WUA）APIを利用する方法があります。

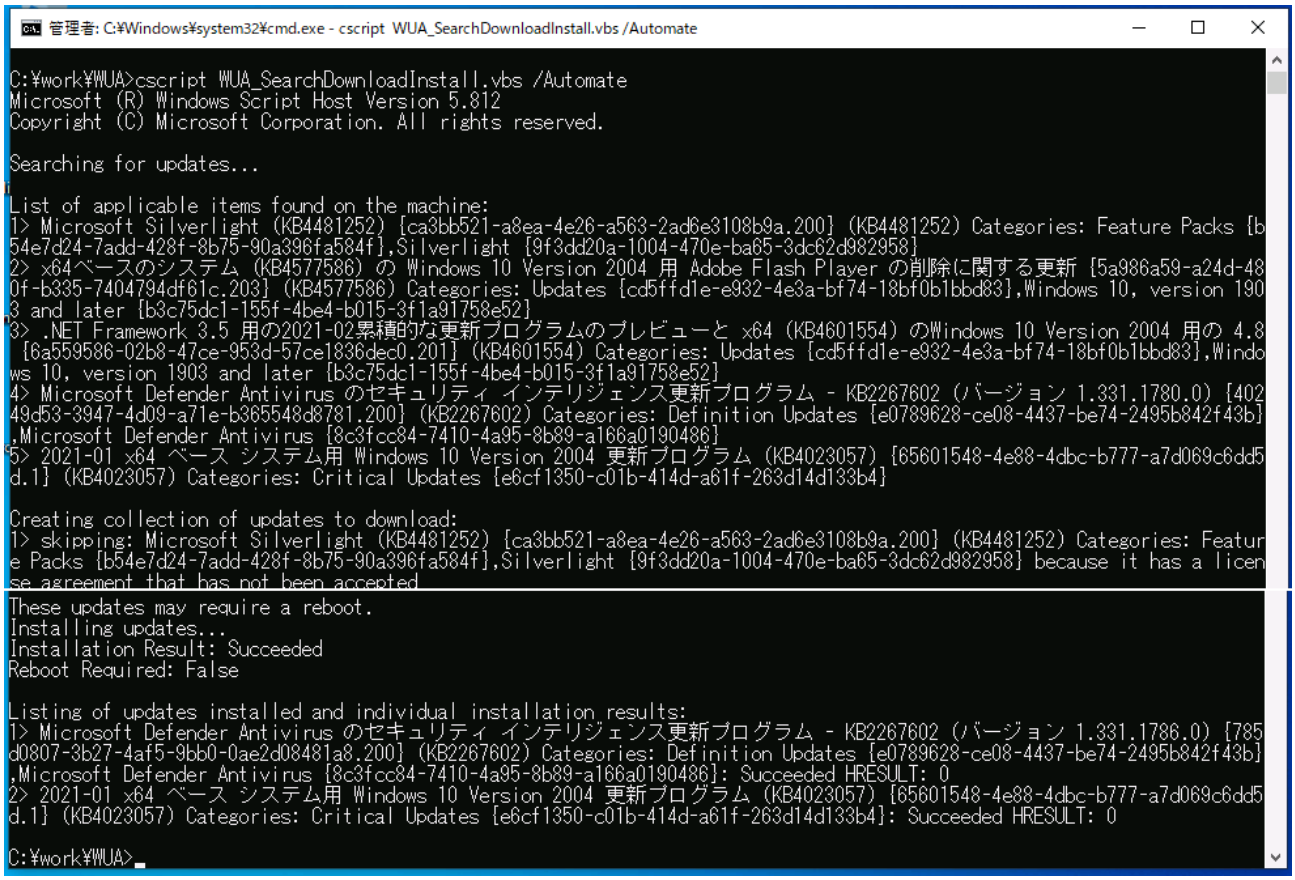
以下のサイトにWUA APIを利用して更新プログラムの確認、ダウンロード、インストールを行うサンプルスクリプトWUA_SearchDownloadInstall.vbsが公開されています。

Searching, Downloading, and Installing Updates
https://docs.microsoft.com/ja-jp/windows/win32/wua_sdk/searching--downloading--and-installing-updates

以前は更新の各ステップをY/Nの入力で対話的に実行するシンプルなスクリプトでしたが、最近、いくつかの新しいパラメーターをサポートする高機能版に差し替えられました（古いスクリプトは別のURLのページにアーカイブされています*1）。新しいスクリプトをパラメーター無しで実行すると、以前のスクリプトと同様に対話的に更新の確認、インストールの選択、ダウンロード、およびインストールを行うことができます。このスクリプトを利用して更新プログラムをインストールするには、管理者権限で実行する必要があります。

次のように/Automateパラメーターを追加して実行すると、利用可能な更新プログラムを確認し、検出されたすべてをインストールできます（画面7）。ただし、EULA（ライセンス条項）に同意する必要がある更新プログラムについてはスキップされます。

> Cscript  WUA_SearchDownloadInstall.vbs /Automate ↲




画面5　WUA_SearchDownloadInstall.vbsによる更新プログラムのインストールの自動化

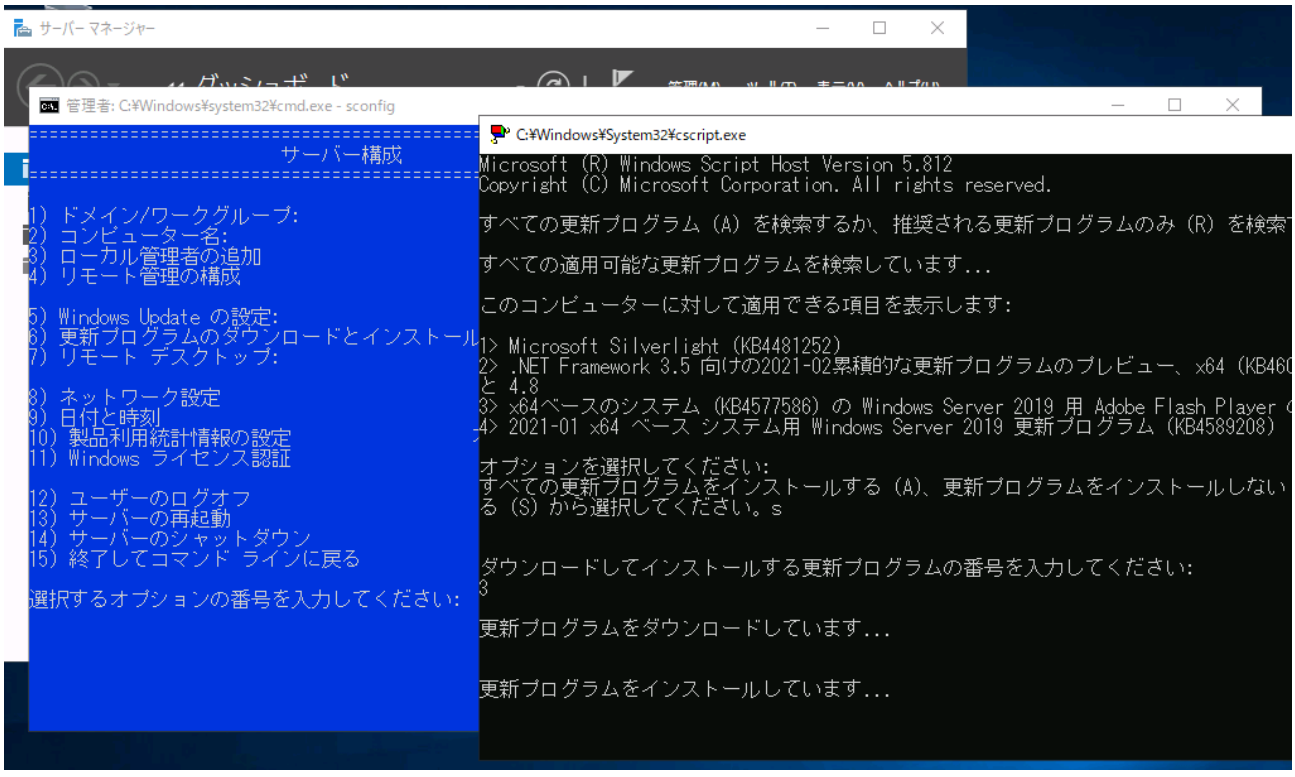
*1　旧サンプルスクリプトのアーカイブ先 https://docs.microsoft.com/en-us/previous-versions/windows/desktop/aa387102(v%3dvs.85)

現在のWindows 10およびWindows Server 2019以降は、Windowsの累積更新プログラムのプレビューはWindows 10で新たに追加されたUpdateOrchestratorサービスによって検出されます。WUA APIは、Windowsの累積更新プログラムのプレビュー（Cリリース）や定例外のオプションの更新プログラム（Out-of-bandリリース）は検出しません。.NET Frameworkの累積更新プログラムのプレビュー（Cリリース）はWUA APIの検索対象に入ります。

---

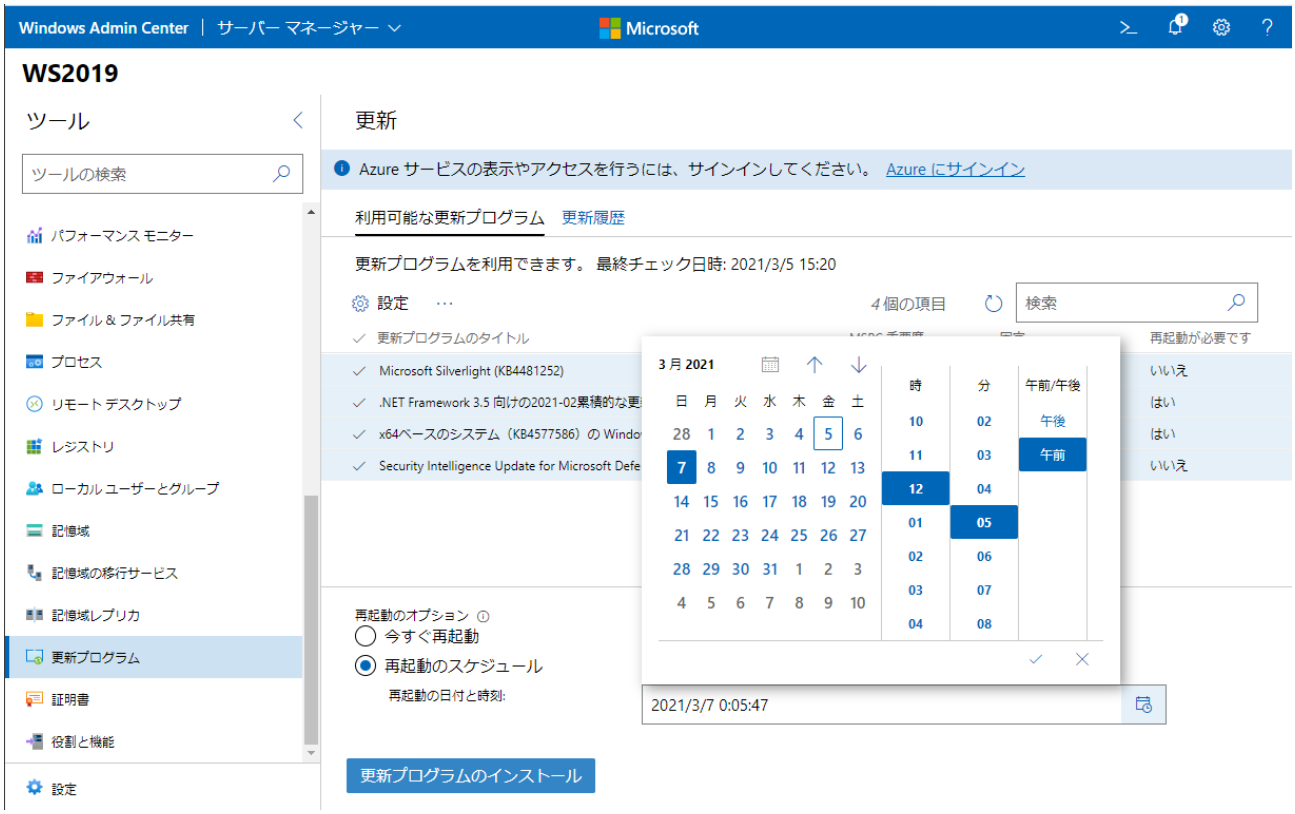
## SconfigユーティリティとWindows Admin CenterはWUA APIで動く

Windows ServerはSconfigというテキストベースのユーティリティを搭載しています。Windows Server 2012以降のSconfigユーティリティはWindows Serverのインストールの種類（GUI使用サーバー/デスクトップエクスペリエンスとServer Core）に関係なく、どちらでも利用できます。Sconfigユーティリティの［6 更新プログラムのダウンロードとインストール］は、WUA APIを利用するWSHスクリプト（C:¥Windows¥System32¥ja-jp¥WUA_SearchDownloadInstall.vbs）として実装されており、利用可能な更新プログラムの検索、インストールする更新プログラムの選択、およびダウンロードとインストールを実行できます（画面6）。本書で紹介したサンプルスクリプトと同じファイル名ですが、内容は異なります。現在の高機能版に差し替えられる前の古いバージョンのWUA_SearchDownloadInstall.vbsをベースとしています。 前述したように、WUA APIはWindowsの累積更新プログラムのプレビューを検出しません。そのため、Sconfigを利用すればデスクトップエクスペリエンス環境で意図せずWindowsの累積更新プログラムのプレビューがインストールされるのを防止できます。なお、「推奨される更新プログラムのみ（R）」の検索は現在、期待どおりに機能しなくなりました。これは検索条件（Criteria）としての「AutoSelectOnWebSites=1」が推奨される更新プログラムに設定されない場合があるためです。




画面6　Windows Serverはインストールの種類に関わらず、Sconfigユーティリティを使用可能。［6 更新プログラムのダウンロードとインストール］はWUA APIを利用したスクリプトで実装されている マイクロソフトは2018年4月、HTML5ベースのサーバー管理アプリWindows Admin Centerをリリースし、概ね半期に一度、更新バージョンをリリースしています。Windows Admin Centerは、Windows Server 2012 R2以降のWindows Server、フェールオーバークラスター、Azure Stack HCIクラスター、およびWindows 10のリモート管理に対応しています。Windows Admin Centerの［更新プログラム］ツールはWUA APIを利用して不足している更新プログラムの確認とインストールの選択、ダウンロードとインストールを行います。再起動が必要な更新プログラムがある場合は、再起動の日時をスケ

ジューリングして実施することができるので、更新プログラムのインストールに起因する再起動が業務時間内に行われるのを回避できます（画面7）。

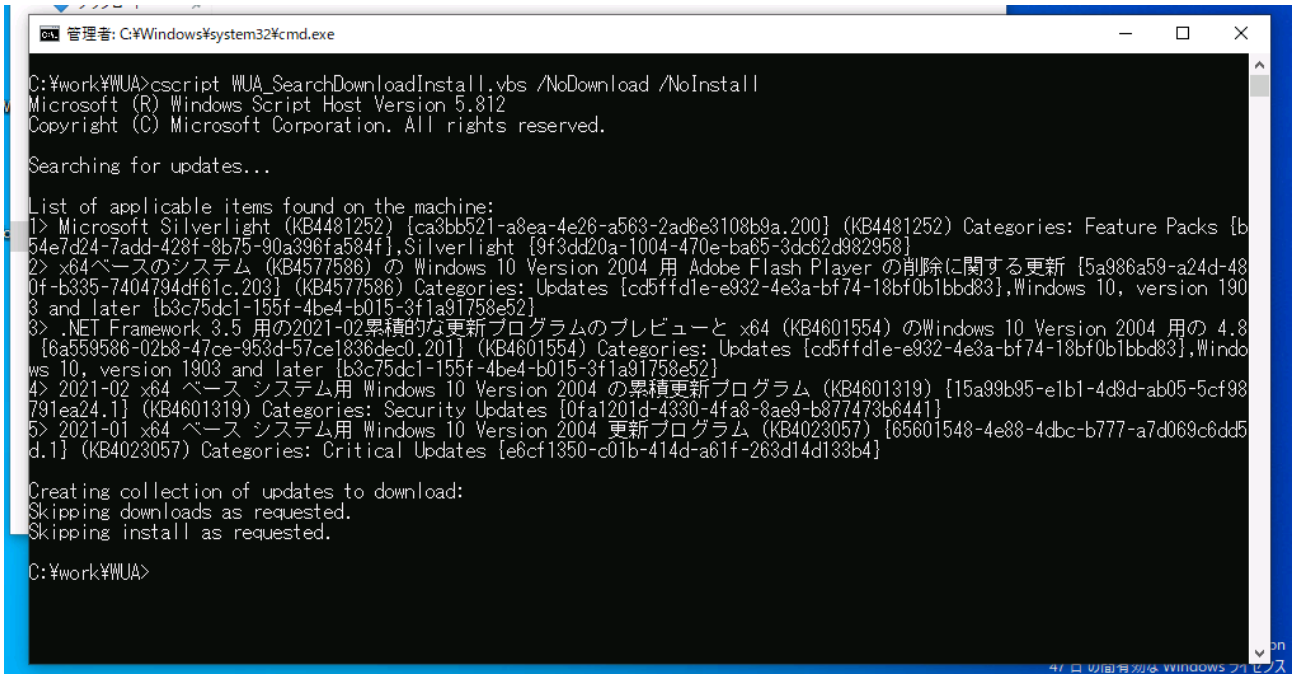



画面7　Windows Admin Centerを利用すると、更新のための再起動を計画的に実施できる

## 不足しているセキュリティ更新をレポートする（オンラインスキャン）

WUA_SearchDownloadInstall.vbsに/NoDownloadおよび/NoInstallパラメーターを指定して実行すると、ダウンロードとインストールは行わずに、スキャン結果だけをレポートしてくれます。この機能は稼働中のサーバーの更新状態を調査するのに便利です（画面8）。なお、スキャンの実行のみであれば、管理者権限は不要です。

```
Cscript  WUA_SearchDownloadInstall.vbs /NoDownload /NoInstall ↲
```




画面8　WUA_SearchDownloadInstall.vbsでスキャンだけを実施し、不足している更新プログラムを調査する

## 不足しているセキュリティ更新をレポートする（オフラインスキャン）

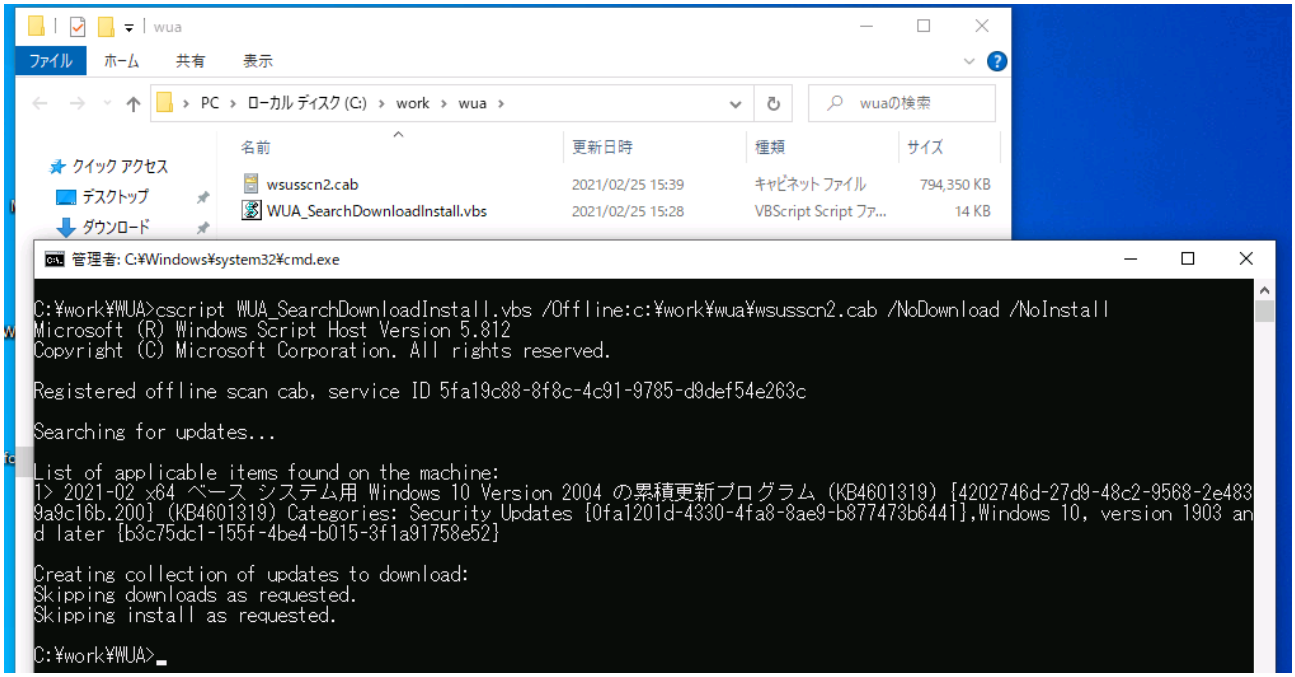
WUA_SearchDownloadInstall.vbsはオフラインスキャンにも対応しています。最新のオフラインスキャンファイルであるWSUSSCN2.cabを入手し、/OfflineパラメーターにWSUSSCN2.cabのパスを指定すると（C:¥work¥WSUSSCN2.cabのように、絶対パスで指定する必要があります）、インターネット接続の制限されたコンピューターに対してスキャンを実行することができます。オフラインスキャンもスキャンの実行のみであれば、管理者権限は不要です。

> Cscript　WUA_SearchDownloadInstall.vbs /Offline:<絶対パス>¥WSUSSCN2.cab　/NoDownload /NoInstall ↲

最新のWSUSSCN2.cabのダウンロード（米国時間毎月第2火曜日に更新）
http://download.windowsupdate.com/microsoftupdate/v6/wsusscan/wsusscn2.cab

オンラインスキャンは、オプションの更新プログラムをインストールが必要な更新プログラムとして検出しますが、オフラインスキャンは自動配布対象のセキュリティ更新および重要な更新のみを対象としています。次のようにオフラインスキャンと/Automateオプションを組み合わせることで、オフラインスキャンに基づいて本当に必要な更新プログラムだけを自動的にインストールすることができ便利です（画面9）。更新プログラムのダウンロードとインストールまで行う場合、管理者権限で実行する必要があります。

> Cscript　WUA_SearchDownloadInstall.vbs /Offline:<絶対パス>¥wsusscn2.cab　/Automate




画面9　最新のWSUSSCN2.cabを使用してオフラインスキャンを実施する。/NoDownload /NoInstallパラメーターの代わりに/Automateパラメーターを指定すると、オフラインスキャンに基づいてインストールを行うことも可能

## 更新履歴を表示する

WindowsおよびWindows Serverのデスクトップエクスペリエンスには、インストールの成功と失敗を含む更新の履歴を表示する機能があります。Windows ServerのServer Coreには更新の履歴を表示する機能はありません。

WUA APIを利用した次のサンプルスクリプトGet-WUHistory.vbsを使用すると、Windows標準の更新の履歴と同等の履歴情報を取得することができます（画面10）。Windows ServerのServer Coreでも利用できます。履歴情報を取得するために、管理者権限は必要ありません。

**Get-WUHistory.vbsのスクリプト**
**注：UTF-8ではなくANSIコード（シフトJIS）で保存すること**

```
Set objSession = CreateObject("Microsoft.Update.Session") ↲
Set objSearcher = objSession.CreateUpdateSearcher ↲
intCount = objSearcher.GetTotalHistoryCount ↲
Set colHistory = objSearcher.QueryHistory(0, intCount) ↲
For Each objHistory In colHistory ↲
If objHistory.HResult = 0 then ↲
WScript.Echo DateAdd("h",9,objHistory.Date) & ", " & objHistory.Title & ", 成功" ↲
ElseIf objHistory.HResult = -2145116140 then ↲
WScript.Echo DateAdd("h",9,objHistory.Date) & ", " & objHistory.Title & ", 成功（再起動が必要な更新）" ↲
Else ↲
WScript.Echo DateAdd("h",9,objHistory.Date) & ", " & objHistory.Title & ", 失敗(エラーコード：0x" &
Hex(objHistory.HResult) & ")" ↲
End If ↲
Next ↲
```

このスクリプトはインストールの結果コードに基づいて、成功（0）と失敗（0以外）を判断し、失敗の場合はエラーコードを出力します。エラーコードの一覧は以下のサイトで確認することができます。2つ目のIf文で評価している-2145116140（0x80242014）は再起動の保留状態を示しており、再起動されると結果コードに0がセットされます。しかし、筆者が確認した限り、Windows 10バージョン2004および20H2では再起動後も結果コードが0にセットされない不具合があるようです。そのため、「成功（再起動が必要な更新）」として出力するようにしました。

Windows Update の一般的なエラーと軽減策
https://docs.microsoft.com/ja-jp/windows/deployment/update/windows-update-errors



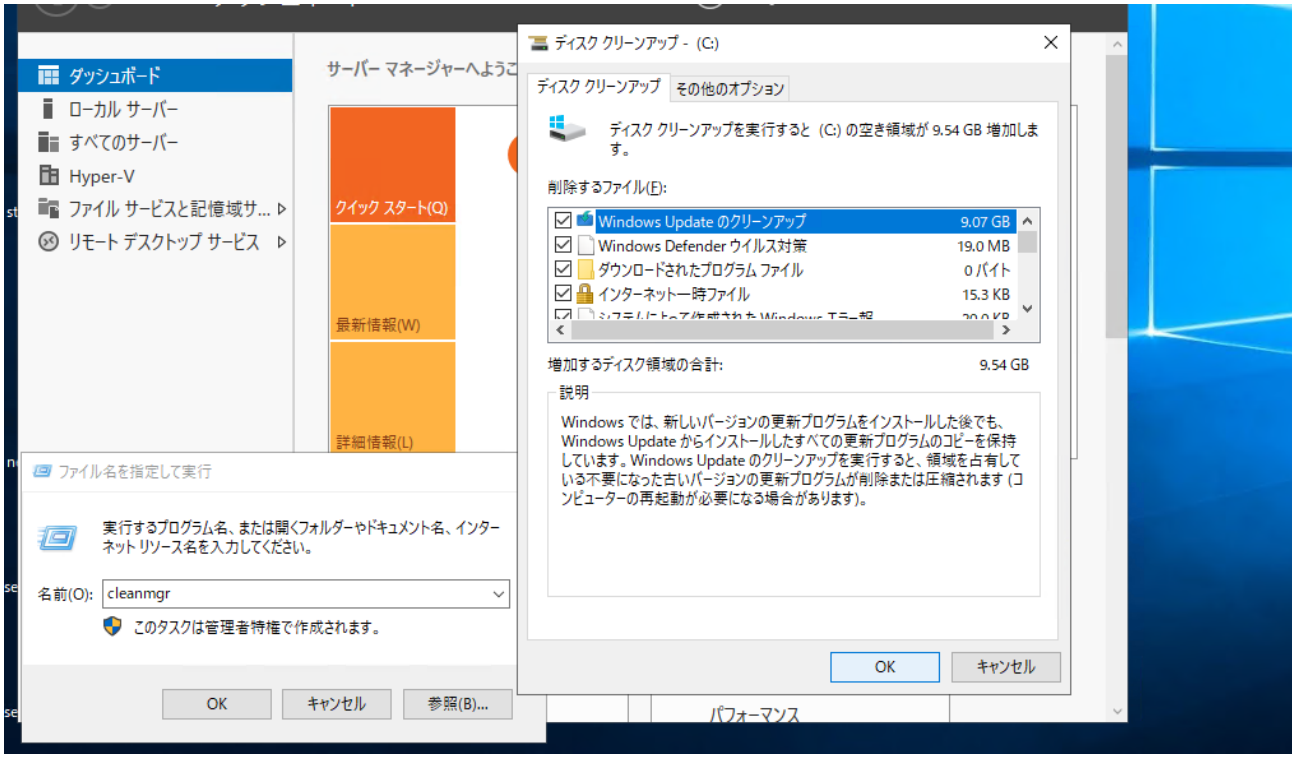

画面10　WUA APIを利用して成功／失敗を含む更新プログラムのインストール履歴を取得する

## ディスク領域節約と更新時間の改善に効く、Windows Updateのクリーンアップ

Windows Updateを実施して、安定運用の状態を確認できている場合は、定期的に、例えば数か月に一度にWindows Updateのクリーンアップを実施することをお勧めします。Windows Updateのクリーンアップを実施すると、古いファイルの削除や圧縮が行われ、ディスクの使用領域を数GB単位で解放できる場合があります。また、次回のWindows Updateのパフォーマンス改善を期待できます。ただし、クリーンアップ後は古い更新プログラムをアンインストールできなくなるため、必ず安定運用の状態にあることを確認してから実施してください。

Windows Updateのクリーンアップを実施するには、［ディスククリーンアップ］（cleanmgr.exe）を管理者権限で実行し、［Windows Updateのクリーンアップ］を選択します（画面11）。クリーンアップで増加するディスク領域のサイズは不正確な場合があります（例：1MBや3.66 TBといったありえないサイズを報告）が、クリーンアップの実施には影響はありません。Windows 10の場合、［ディスククリーンアップ］ではなく、［設定］アプリの［システム｜記憶域｜一時ファイル］から［Windows Updateのクリーンアップ］を選択して削除することもできます。

コンピューターのスペックやインストールされている更新プログラムの数にもよりますが、通常、数時間かかかります。100%に近くなっても、それから数時間かかることもあるので、根気よく待ってください。



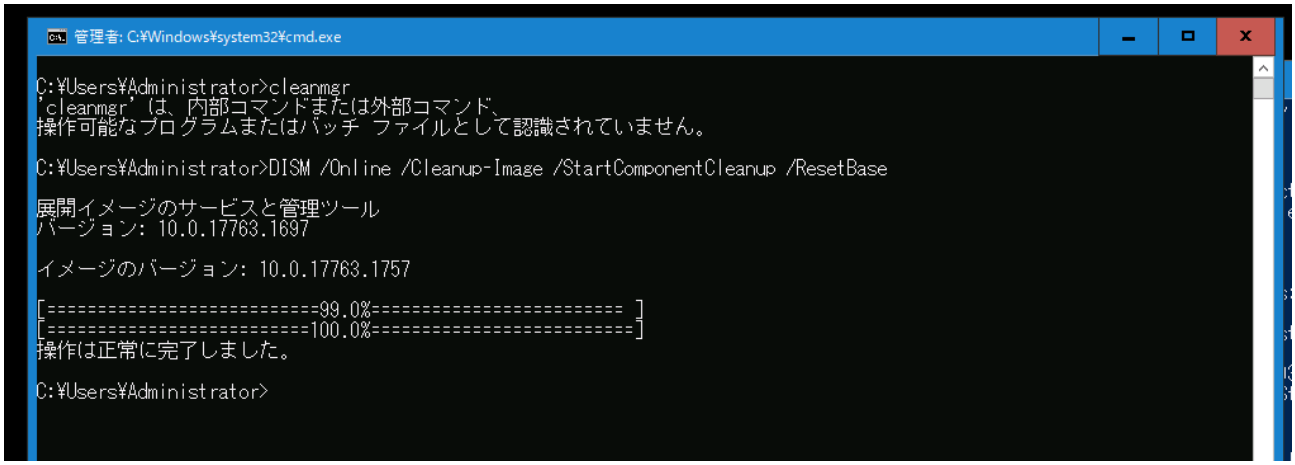

画面11　［ディスククリーンアップ］（cleanmgr.exe）を実行してWindows Updateのクリーンアップを選択

［ディスククリーンアップ］（cleanmgr.exe）は、WindowsおよびWindows Server 2016以降のデスクトップエクスペリエンスに標準で含まれます。Windows Server 2012 R2以前の場合は、サーバーの機能［デスクトップエクスペリエンス］を有効化することでインストールされます。Server Coreでは使用できません。また、理由は不明ですが、Windows Serverの場合は［Windows Updateのクリーンアップ］の項目が表示される場合とされない場合があるようです。

Windows Serverでのディスククリーンアップの使用について
https://docs.microsoft.com/ja-jp/windows-server/storage/file-server/disk-cleanup

Server Coreの場合、および［Windows Updateのクリーンアップ］の項目が表示されない場合は、次のコマンドラインを管理者権限で実行することで、同様の効果が期待できます。/ResetBaseパラメーターは省略できますが、指定することでより多くの領域を解放できます（画面12）。ただし、アンインストール用に保持されていた、更新で置き換えられたバイナリがすべて削除されることに注意してください。/ResetBaseパラメーターを指定しない場合、不要なコンポーネントだけがクリーンアップされ、コンポーネントストア（C:¥Windows¥WinSxS）のサイズが最適化されます。

```
DISM  /Online /Cleanup-Image /StartComponentCleanup /ResetBase ↲
```




画面12　Server CoreでWindows Updateの不要なコンポーネントと更新で置き換えられた古いバイナリをクリーンアップする

---

### %WINDIR%¥SoftwareDistributionのリセット

Windows 10およびWindows Server 2016以降のWindows Updateが原因不明のエラーで失敗を繰り返す場合、更新プログラムのダウンロード先（¥Download）やデータベース（¥DataStore¥Datastore.edbなど）を含む%Windir%¥SoftwareDistributionディレクトリをリセットする（削除して再作成させる）ことで解消する場合があります。　SoftwareDistributionディレクトリの再作成を含むWindows Updateのコンポーネントのリセットの完全な手順については、以下のドキュメントで説明されています。

Windows Update - 追加リソース | Windows Update のコンポーネントをリセットする方法

https://docs.microsoft.com/ja-jp/windows/deployment/update/windows-update-resources#how-do-i-reset-windows-update-components

上記の手順は複雑ですが、SoftwareDistributionのリセットだけで多くの問題が解消します。それには、コマンドプロンプトを管理者として開き、次の一連のコマンドラインを実行してWindows Update関連のサービスを停止し（ほとんどの場合、wuauservの停止のみでよい）、%WINDIR%¥SoftwareDistributionディレクトリをリネーム後に削除します。

```
NET　STOP wuauserv
NET　STOP bits
NET　STOP cryptsvc
NET　STOP msiserver
NET　STOP usosvc
NET　STOP dosvc
REN　%WINDIR%¥SoftwareDistribution SoftwareDistibution.old
RD　%WINDIR%¥SoftwareDistibution.old /S
```

Windows Update（wuauserv）サービスが自動開始されてしまうとSoftwareDistributionディレクトリのリネームに失敗するので、その場合は再度停止後にすばやくリネームしてください。もしくは、Windows Updateサービスのスタートアップを“無効”に変更してコンピューターを再起動し、SoftwareDistributionディレクトリをリネーム後に“手動”に戻します。

# 現在のセキュリティ設定を推奨基準と比較する

WindowsおよびWindows Serverのシステム設定は、パフォーマンスやネットワークスループットを最適化するため、セキュリティを強化するため、効率化するためなど、さまざまにカスタマイズすることができます。しかし、不適切なシステム設定や、意図せず設定が重複してしまい上書きされてしまったりすることがあります。特にセキュリティに関連する設定が不適切であると、たとえOSやアプリが最新状態に更新されていたとしても、自ら作り出してしまった脆弱性を突かれセキュリティ侵害されてしまうリスクもあります。ここでは、マイクロソフトが無料提供するMicrosoft Security Compliance Toolkit（SCT）1.0を利用したセキュリティ設定の評価と実装について紹介します。

## Microsoft Security Compliance Toolkit（SCT）の入手と準備

Microsoft Security Compliance Toolkit（SCT）1.0は、企業のセキュリティ管理者がWindows、Windows Server、およびその他のマイクロソフト製品用の、マイクロソフト推奨のセキュリティ設定のベースラインをダウンロードし、現在の設定との比較評価、および実装するのに役立つ一連のツールです。

SCTを使用すると、Active Directoryドメインで展開している現在のグループポリシーとマイクロソフト推奨のベースラインを効率的に比較したり、マイクロソフト推奨のベースラインからグループポリシーオブジェクト（GPO）を作成して展開したりできます。また、ローカルコンピューターの現在のシステム設定とベースラインを比較したり、現在のシステム設定にベースラインの設定を上書きしたりすることもできます。

Microsoft Security Compliance Toolkit 1.0のダウンロード
https://www.microsoft.com/en-us/download/details.aspx?id=55319

Microsoft Security Compliance Toolkit 1.0のドキュメント
https://docs.microsoft.com/ja-jp/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10

SCTのダウンロードサイトからは以下の表3のツールをダウンロードすることができます。SCTのバージョンは1.0のまま変わらなくても、ダウンロードコンテンツは不定期に更新されます。必ず最新版を入手して使用するようにしてください。なぜなら、マイクロソフト推奨のセキュリティ設定は変更される場合があります。以前の推奨設定が、現在では推奨されない設定になっていることもあるからです。

表3　SCT 1.0として提供されているツール群（2021年3月16日公開版）

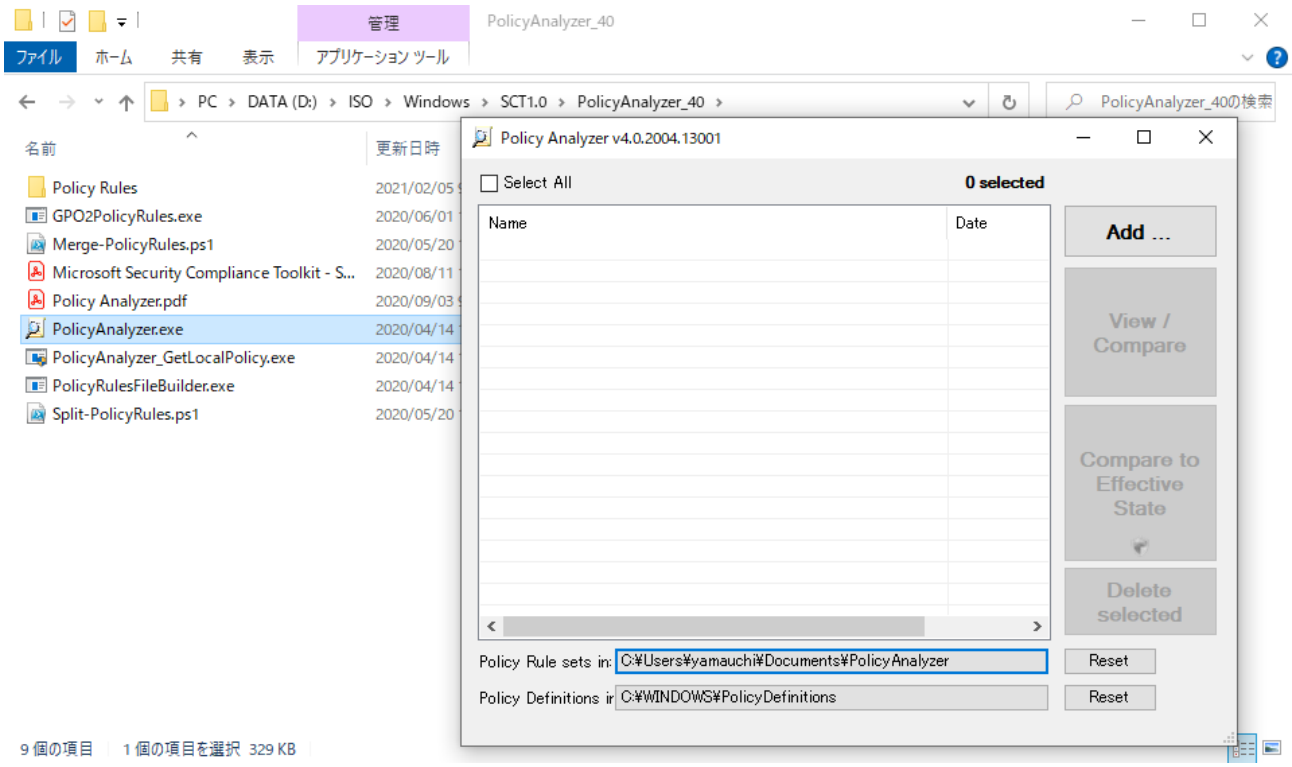
| ダウンロードファイル名 | 説明 |
|---|---|
| PolicyAnalyzer.zip | Policy Analyzer v4.0（PolicyAnalyzer.exe） |
| LGPO.zip | LGPO v3.0（LGPO.exe） |
| SetObjectSecurity.zip | SetObjectSecurity v1.0（SetObjectSecurity.exe） |
| Windows Server 2012 R2 Security Baseline.zip | WindowsおよびWindows Serverの各バージョンに対応したセキュリティベースライン |
| Windows 10 Version 1507 Security Baseline.zip | |
| Windows 10 Version 1607 and Windows Server 2016 Security Baseline.zip | |

| ダウンロードファイル名 | 説明 |
| --- | --- |
| Windows 10 Version 1803 Security Baseline.zip | |
| Windows 10 Version 1809 and Windows Server 2019 Security Baseline.zip | |
| Windows 10 Version 1903 and Windows Server Version 1903 Security Baseline - Sept2019Update.zip | |
| Windows 10 Version 1909 and Windows Server Version 1909 Security Baseline.zip | |
| Windows 10 Version 2004 and Windows Server Version 2004 Security Baseline.zip | |
| Windows 10 Version 20H2 and Windows Server Version 20H2 Security Baseline.zip | |
| Windows 10 Update Baseline.zip | Windows 10のWindows Updateのベースライン |
| Microsoft Edge v88 Security Baseline.zip | Chromium版Microsoft Edge Stableバージョン88のセキュリティベースライン |
| Office365-ProPlus-Sept2019-FINAL.zip | Microsoft 365 Apps（旧称、Office 365 ProPlus）のセキュリティベースライン |

各ツールの機能については以下の公式ブログを参照してください。

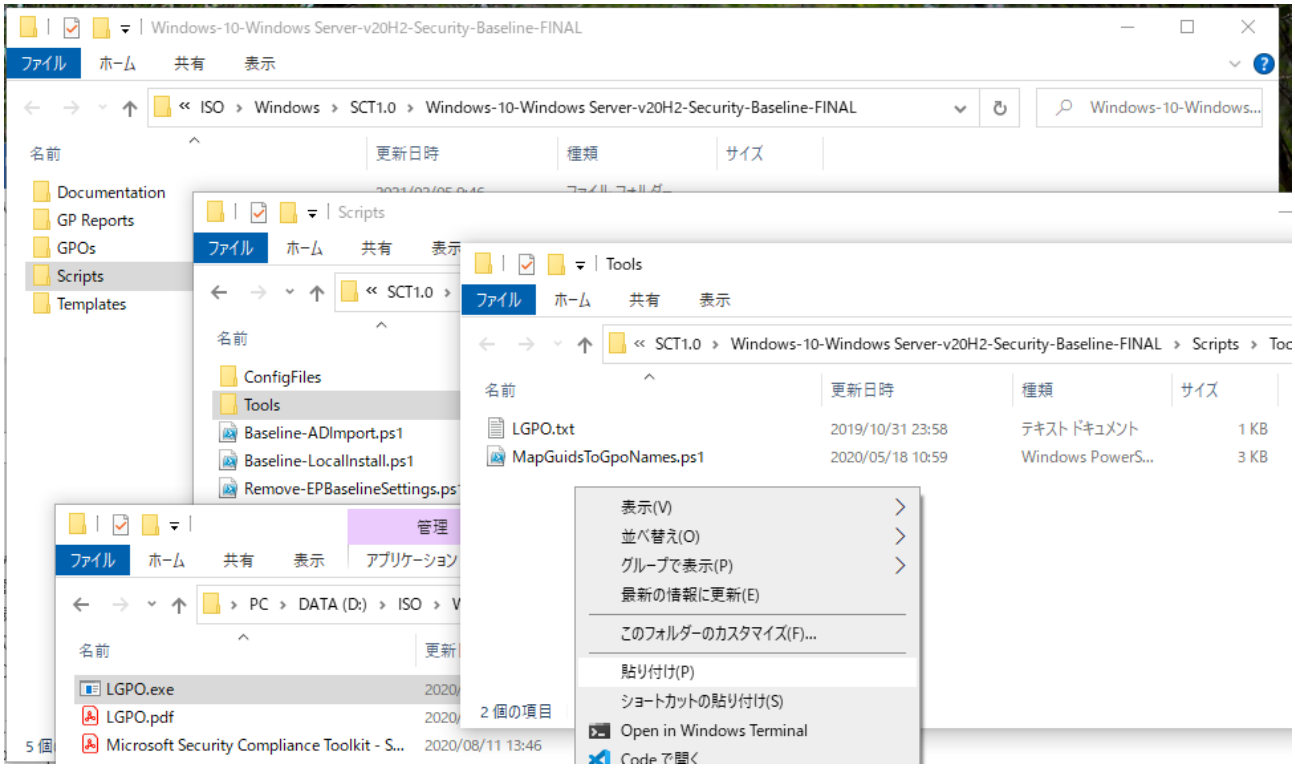
New & Update Security Tools
https://techcommunity.microsoft.com/t5/microsoft-security-baselines/new-amp-updated-security-tools/ba-p/1631613

セキュリティベースラインとの比較を行う場合は、Policy Analyzer.zipと、評価したいWindowsやWindows Server、その他のマイクロソフト製品のベースラインの.zipファイルをダウンロードして任意の場所に展開します。Policy Analyzer（PolicyAnalyzer.exe）は、1つ以上のセキュリティベースラインとGPO、またはローカルコンピューターの現在の設定を比較するための分析ツールです（画面18）。



画面18　SCT 1.0の分析ツールであるPolicy Analyzer（PolicyAnalyzer.exe）

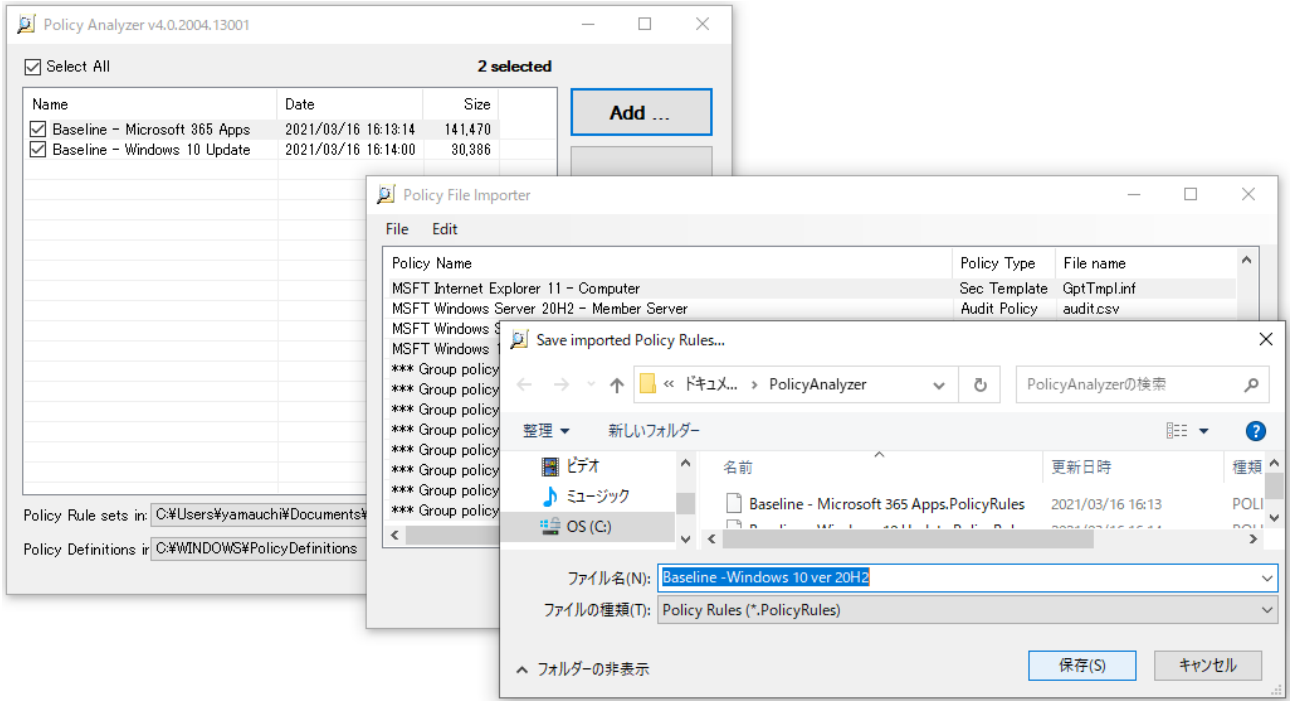
推奨のベースラインからGPOを作成したり、ローカルコンピューターを設定する場合はLGPO.zipをダウンロードして展開し、LGPO.exeを各セキュリティベースラインのスクリプト用ディレクトリのToolsに格納しておきます（Scripts¥ToolsまたはLocal_Scripts¥Toolsディレクトリが存在する場合、画面19）。GPOの作成や設定のインストールには、スクリプト用ディレクトリにあるスクリプト（.ps1）またはバッチ（.cmd）を使用します。ベースラインの評価目的だけであれば、この準備作業は不要です。



画面19　ベースラインのScripts¥ToolsディレクトリにLGPO.exeをコピーしておく

### SCTによる現在のローカル設定の評価

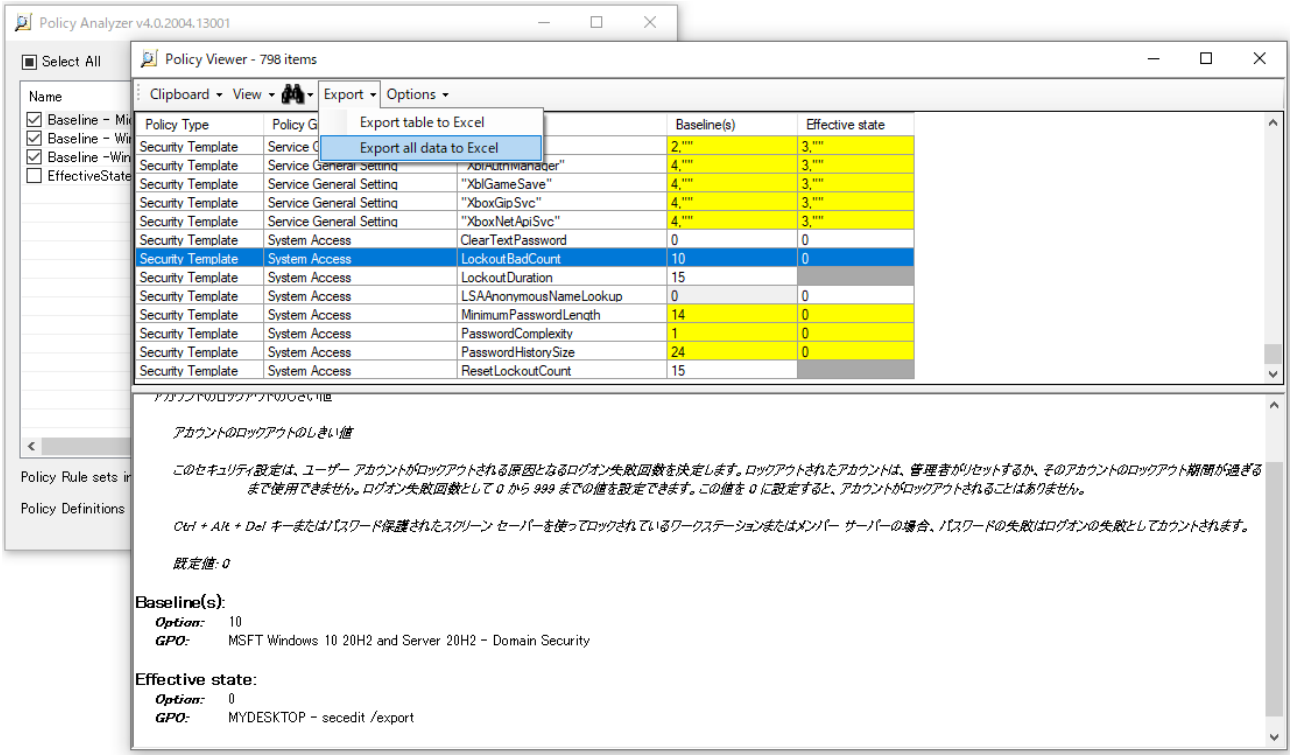
SCT を使用してローカルコンピューターのシステム設定をセキュリティベースラインと比較します。Policy Analyzer（PolicyAnalyzer.exe）を開き、［Add］ボタンをクリックし、さらに［File］から［Add Files from GPO(s)］を選択して、調査したいセキュリティベースラインの展開先ディレクトリにあるGPOsサブディレクトリを選択してポリシーをインポートします。インポートする際、［Save imported policy Rules］の場所と名前を要求されるので、ベースラインであることが分かるように分かりやすい名前を入力してインポートします（画面20）。




画面20　ベースラインのGPOsサブディレクトリからポリシー設定をインポートする

1つ以上のベースラインをインポートしたら、調査したいベースラインを選択した状態で［Compare to Effective State］ボタンをクリックします。すると、［Policy Viewer］が開き、ローカルコンピューターのレジストリ設定とベースラインのポリシー設定が比較され、違いをハイライト表示されます。

［Policy Viewer］で1つの行を選択すると、設定の意味やどのベースラインに設定されている推奨設定なのか、および現在ローカルコンピューターで有効になっている設定を確認できます（画面21）。［Export］メニューを使用すると、表形式のレポート、またはすべてのデータをExcelワークシートにエクスポートすることができます。



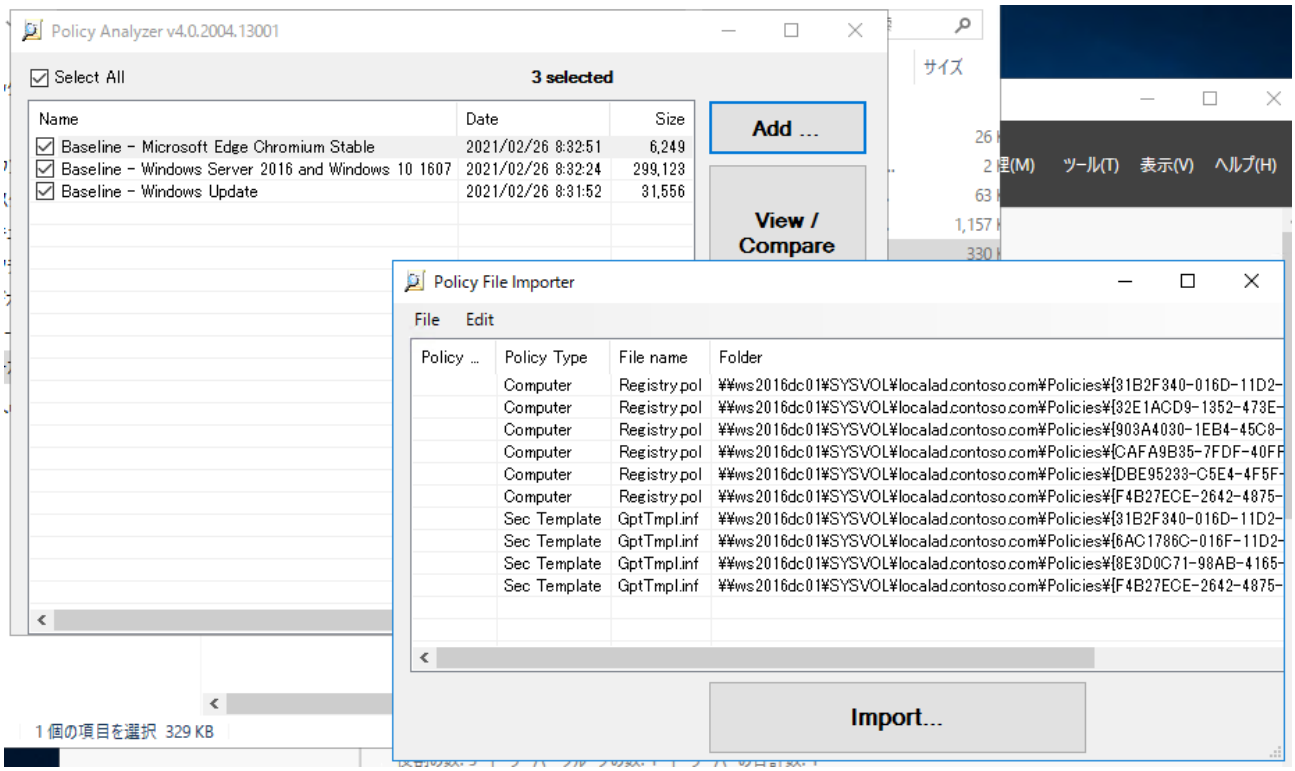

画面21　［Policy Viewer］で現在のシステム設定と推奨のベースライン設定を比較する

## SCTによるグループポリシー設定の評価

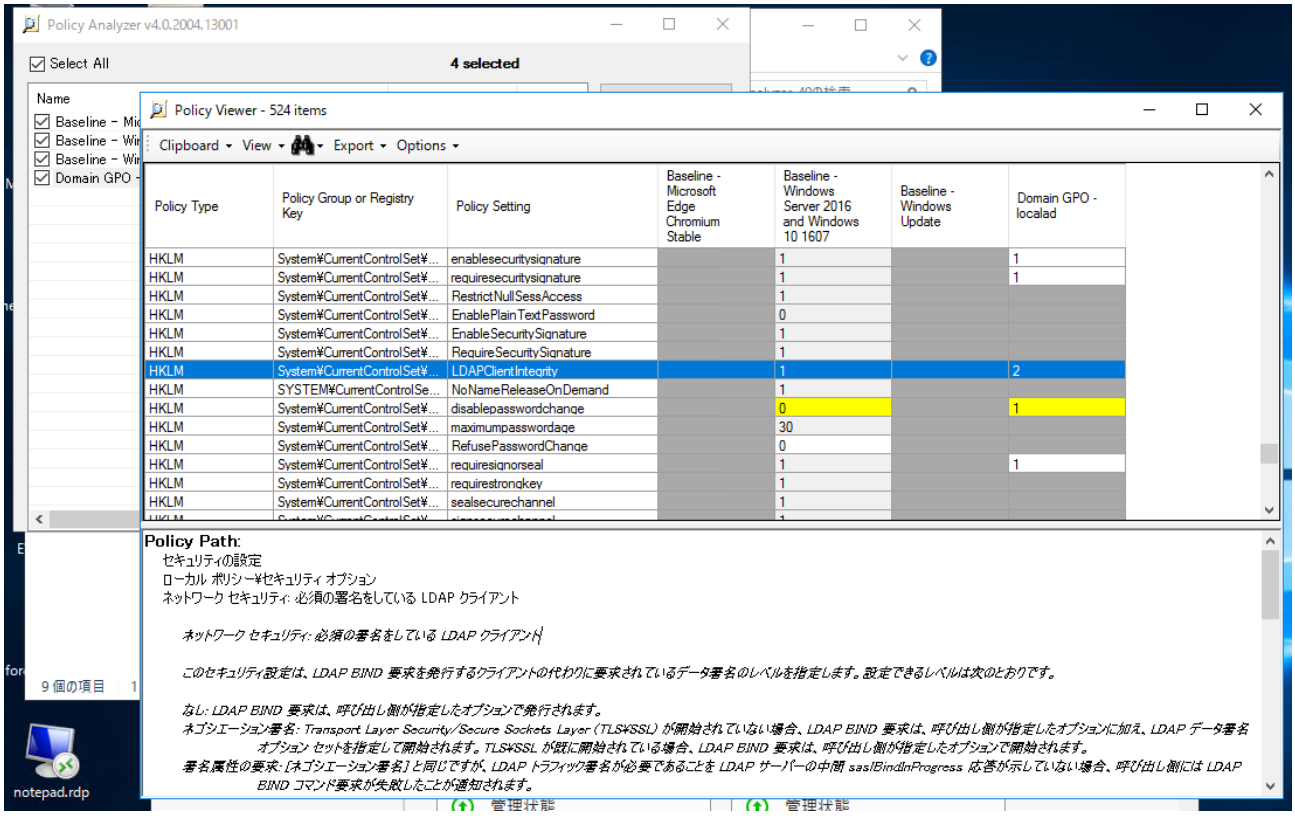
SCTを使用してActive Directoryドメインの現在のグループポリシー設定を調査したい場合は、ドメインコントローラーまたはActive Directoryの管理ツールを利用できるメンバーコンピューターでPolicy Analyzer（PolicyAnalyzer.exe）を実行します。

［Add］ボタンをクリックし、ベースラインをインポートしたら、さらに続けてドメインのSYSVOL共有パス内のGPO（¥<ドメインコントローラー名>¥SYSVOL<DNSドメイン名>¥Policies）からポリシー設定をインポートします（画面22）。SYSVOL共有のGPOをインポートする代わりに、［グループポリシーの管理］スナップインを使用してバックアップしたGPOを、バックアップ先（またはそのコピー）からインポートすることもできます。

調査したいベースラインとドメインのGPOからのインポートしたポリシー設定のすべてを選択し、［View/Compare］ボタンをクリックします。すると、［Policy Viewer］が開き、現在のドメインで有効なGPOとベースラインとの違いをハイライト表示で調査することができます（画面23）。ローカル設定の評価の場合と同様に、［Export］メニューを使用すると、表形式のレポート、またはすべてのデータをExcelワークシートにエクスポートすることができます。



画面22　ドメインのSYSVOL共有からGPOをインポートする



画面23　ドメインで有効なGPOとベースラインのポリシー設定を比較する

### ベースラインからのGPOの作成

各セキュリティベースラインはActive DirectoryドメインのGPOとして簡単にインポートできます。例えば、Windows 10 Update Baselineの場合はScriptsディレクトリにあるbaseline-ADImport.ps1をドメインコントローラー上のPowerShellウィンドウで実行するだけです。

```
.¥baseline-ADImport.ps1 ↲
```

インポートされたGPOは、［グループポリシーの管理］の［グループ ポリシー オブジェクト］の下で確認できます。GPOをドメインのコンテナーや組織単位（OU）に関連付ければ、推奨セキュリティ設定をドメイン内に展開できます。

なお、スクリプトのファイル名や使用方法はベースラインにより異なる場合があります。パラメーターの指定が必要なものもありますし、バッチファイル（例：Domain_Controller_Install.cmd）として提供されている場合もあります。スクリプト用ディレクトリ（ScriptsやLocal_Scripts）内にあるスクリプトやバッチの内容を確認して適切に使用してください。

### ベースラインのローカルインストール（非推奨）

推奨セキュリティ設定のベースラインをローカルコンピューターのローカル設定（レジストリ設定）として直接的に上書きするローカルインストール用スクリプトやバッチ、パラメーターが利用可能な場合もあります（例：Baseline_LocalInstall.ps1、Client_Install.cmd）。しかし、ベースラインのローカルインストールはお勧めしません。アンインストール用のスクリプトやバッチが用意されて場合もありますが（例：Remove-EPBaselineSettings.ps1）、設定を完全に元の状態に戻すことができないからです。

もしローカルインストール機能を利用したいのであれば、簡単にロールバックできる仮想マシン環境などで十分にテストした上で実施してください。

| | |
|---|---|
| 変更前 | $status = SQLCMD -S ¥¥.¥pipe¥Microsoft##WID¥tsql¥query -i $SQLPath -I ↲ |
| 変更後 | if ( $script:SqlServer -match "microsoft##" ){ ↲<br>  $status = SQLCMD -S ¥¥.¥pipe¥Microsoft##WID¥tsql¥query -i $SQLPath -I ↲<br>} else { ↲<br>  $status = SQLCMD -S $script:SqlServer -i $SQLPath -I ↲<br>} ↲ |

# セイ・テクノロジーズからのお知らせ

## 自立分散型サーバー監視ソフト『BOM for Windows』

運用管理を快適にする自立分散型サーバー監視ソフト『BOM for Windows』を簡単にはじめられる監視テンプレートのご案内です。

### システム安定運用-セキュリティテンプレート

本監視テンプレートは、本書に沿って作成された、監視・アクション設定およびバッチファイルからなる BOM for Windows Ver.8.0 (BOM 8.0)向けのテンプレートです。

本テンプレートに含まれている内容は以下の内容になります。

- Windows バージョン取得監視
- Windows Update 成否リスト取得監視
- Windows Update 未適用リスト取得監視

それぞれの監視項目とアクションについてご説明します。

環境条件

本監視テンプレートは、以下の条件を満たしている環境で使用できます。
・BOM 8.0 の動作要件を満たし、インストールおよび動作が正常であること。
・以下の OS が動作する環境であること。

Windows 10 (64-bit)

Windows Server 2016 (デスクトップ エクスペリエンス)

Windows Server 2019 (デスクトップ エクスペリエンス)

詳細なエディション名、アップデートの適用については、BOM 8.0 の動作要件に準じます。

・ローカル (自立) 監視であること。（代理監視では使用できません）

### Windows バージョン取得監視

この監視設定は、対象の監視インスタンスで動作する Windows OS のバージョン情報やビルド番号を定期的 (30日ごと) に csv 形式で取得し、メール送信します。

(1)Windows バージョン情報取得

バージョン情報取得バッチファイル "get_winver.bat" を実行するためのカスタム監視です。

既定値で "get_winver.bat" は "C:¥Program Files¥SAY Technologies¥BOMW8¥Bin¥Support" 以下に保存されている設定となっており、バージョン情報を書き出す csv ファイル (バージョン情報ファイル) も同じフォルダー内に出力されます。テンプレートを使用する際、必要に応じて設定を変更してください。

・"get_winver.bat" の格納先を変更する場合は、「設定」タブ「プログラム名」欄の内容を更新してください。

・バージョン情報ファイルの保存先を変更する場合は、「設定」タブ「引数」欄の内容を以下に沿って更新してください。

- 保存先のフォルダーをフルパスで入力してください。

- パスにスペースが入る場合は、ダブルクォーテーションで囲んでください。

・バージョン情報ファイルは以下の名称になります。

[コンピューター名]_osver.csv

(2)Windows バージョン情報ファイル送信

(1) で更新された Windows バージョン情報ファイルをメールに添付して送信するためのアクションです。
このアクションを使用する際は、事前に SMTP サーバー設定が完了している必要があります。

設定方法は、製品同梱の以下のマニュアルを参照してください。

BOM for Windows Ver.8.0 ユーザーズ マニュアル
(BOM8-ユーザーズマニュアル.pdf)

SMTP サーバーの設定後、「設定」タブの「宛先アドレス」欄に、送信先のメールアドレスを入力してください。

## Windows Update 成否リスト取得監視

この監視設定は対象の監視インスタンスで動作する Windows OS の不足しているセキュリティ更新 (Windows Update 成否リスト) を定期的 (7 日ごと) にメール送信します。

(1)Windows Update成否リスト取得

Windows Update成否リスト取得バッチファイル "get_update_result.bat" を実行するためのカスタム監視です。

既定値でこれらのバッチファイルは "C:¥ProgramData¥SAY Technologies¥BOMW8¥support_script" 以下に保存されている設定となっており、Update成否リストを書き出すテキストファイルも同じフォルダー内に出力されます。

テンプレートを使用する際、必要に応じて設定を変更してください。

・"get_update_result.bat"の格納先を変更する場合は、「設定」タブの「プログラム名」欄の内容を更新してください。

・未適用リストファイルの保存先を変更する場合は、「設定」タブで「引数」欄の内容を以下に沿って更新してください。

- 保存先のフォルダーをフルパスで入力してください。

- パスにスペースが入る場合は、ダブルクォーテーションで囲んでください。

・Update成否リストは以下の名称になります。

WinUpdateYesNo.txt

(2)WinUpdateYesNo.txtファイルのチェック

Update成否リストの更新状況を監視します。

テンプレートを使用する際は、「設定」タブの「ファイル名」欄に入力された文字列について、バージョン情報ファイルの保存先、ファイル名を修正する必要があります。

既定値は "C:¥ProgramData¥SAY Technologies¥BOMW8¥support_script¥WinUpdateYesNo.txt" と入力されており、必要に応じて修正してください。

・インストールが失敗した時のみ検知したい場合は「テキスト検索」タブの検索テキストを「失敗」に更新ください。

(1)でUpdate成否リストの保存先を変更した場合はパスから変更してください。

(3)Update成否メール送信

(2)で更新されたことを検知した際に、Update成否リストをメールに添付して送信するためのアクションです。
このアクションを使用する際は、事前に SMTP サーバー設定が完了している必要があります。

設定方法は、製品同梱の以下のマニュアルを参照してください。

BOM for Windows Ver.8.0 ユーザーズ マニュアル
(BOM8-ユーザーズマニュアル.pdf)

SMTP サーバーの設定後、「設定」タブの「宛先アドレス」欄に、送信先のメールアドレスを入力してください。

## Windows Update未適用リスト取得監視

この監視設定は、対象の監視インスタンスで動作する Windows OS の不足しているセキュリティ更新（Windows Update 未適用リスト) を定期的 (7日ごと) にメール送信します。

(1)未適用リスト取得実行トリガー

本サービス監視は、7日に一度不足しているセキュリティ更新のリスト(未適用リスト)取得を実行するためのトリガーとして設定された監視で、監視対象となるサービスやその監視結果は問いません。既定値は "LanmanWorkstation" サービスが設定されています。特別な理由がない限り、本項目の設定を変更する必要はありません。

(2)(オンライン)Windows Update未適用リスト取得

Windows Update未適用リスト取得バッチファイル "online_KBcheck.bat" (オンライン時) "offline_KBcheck.bat" (オフライン時) を実行するためのカスタムアクションです。インターネットに接続可能であれば「(オンライン) Windows Update未適用リスト取得」を、接続不可の場合には、「(オフライン)Windows Update未適用リスト取得」を「有効」にしてください。また、「(オフライン)Windows Update未適用リスト取得」の場合は、あらかじめ以下のサイトから WSUSSCN2.cab を入手する必要があります。入手したWSUSSCN2.cabはoffline_KBchek.batファイルと同一フォルダーに保存ください。

WSUSSCN2.cab

http://download.windowsupdate.com/microsoftupdate/v6/wsusscan/wsusscn2.cab

WSUSSCN2 とは

https://support.microsoft.com/ja-jp/topic/上級ユーザー向けの新しいバージョンの-windows-update-オフライン-スキャン-ファイル-wsusscn2-cab-について-fe433f4d-44f4-28e3-88c5-5b22329c0a08

既定値でこれらのバッチファイルは "C:¥ProgramData¥SAY Technologies¥BOMW8¥support_script" 以下に保存されている設定となっており、未適用リストを書き出すテキストファイルも同じフォルダー内に出力されます。

テンプレートを使用する際、必要に応じて設定を変更してください。

・"online_KBcheck.bat","offline_KBcheck.bat"の格納先を変更する場合は、「設定」タブの「プログラム名」欄の内容を更新してください。

・未適用リストファイルの保存先を変更する場合は、「設定」タブで「引数」欄の内容を以下に沿って更新してください。

- 保存先のフォルダーをフルパスで入力してください。

- パスにスペースが入る場合は、ダブルクォーテーションで囲んでください。

・未適用リストは以下の名称になります。

WinUpdateList.txt

※なお、本リストは過去取得した未適用リストについても参照できるよう、取得結果を追記しています。本リストの容量が肥大化した場合には、退避するか、不要な場合は削除してください。

※未適用リストを追記するのではなく、上書きする場合には、以下のバッチファイルの内容を変更ください。

online_KBcheck.bat

offline_KBcheck.bat

上記バッチファイルの内容を以下に変更してください。

```
cscript C:¥ProgramData¥SAY Technologies¥BOMW8¥support_script¥WUA_SearchDownloadInstall.vbs /NoDownload /NoInstall >> %1

cscript C:¥ProgramData¥SAY Technologies¥BOMW8¥support_script¥WUA_SearchDownloadInstall.vbs /NoDownload /NoInstall /Offline:C:¥ProgramData¥SAY Technologies¥BOMW8¥support_script¥wsusscn2.cab >> %1
```

「 /NoInstall >> %1 」→ 「 /NoInstall > %1 」

(3)WinUpdateList.txtファイルのチェック

Windows Update未適用リストの更新状況を監視します。

既定値は "C:¥ProgramData¥SAY Technologies¥BOMW8¥support_script¥WinUpdateList.txt" と設定されており、必要に応じて修正してください。

(2)で未適用リストの保存先を変更した場合はパスから変更してください。

(4)未適用リストメール送信

(3)で更新されたことを検知した際に、未適用リストをメールに添付して送信するためのアクションです。
このアクションを使用する際は、事前に SMTP サーバー設定が完了している必要があります。設定方法は、製品同梱の以下のマニュアルを参照してください。

BOM for Windows Ver.8.0 ユーザーズ マニュアル
(BOM8-ユーザーズマニュアル.pdf)

SMTP サーバーの設定後、「設定」タブの「宛先アドレス」欄に、送信先のメールアドレスを入力してください。

**参考情報**

(1)メール送信アクションについて
本テンプレートでは取得したバージョン情報ファイルを「メール送信アクション」で送信していますが、その他にも「AWS S3 ファイル送信アクション」や、「HTTPS 送信アクション」の「ファイル送信」などで送ることも可能です。各アクションの詳細は、製品同梱の以下のマニュアルを参照してください。

BOM for Windows Ver.8.0 ユーザーズ マニュアル
(BOM8-ユーザーズマニュアル.pdf)

BOM for Windows Ver.8.0 HTTPS 送受信マニュアル
(BOMW8.0-HTTPS送受信マニュアル.pdf)

(2)Windows Update 適用状況の監視について

本テンプレートとは別に、BOM 8.0 では適用済みの Windows Update の情報 (KB) を取得して csv 形式で出力できる、「Windows Update 監視」を用意しています。適用された KB を把握する場合は、この「Windows Update 監視」が便利です。「Windows Update 監視」については、上記の「BOM for Windows Ver.8.0 ユーザーズ マニュアル」を参照してください。

- 自立分散型サーバー監視ソフト『BOM for Windows』の製品詳細はこちら
  https://www.say-tech.co.jp/product/bomwin80
- 『BOM for Windows』の評価版ダウンロードはこちら
  https://www2.say-tech.co.jp/bom-eval
- 『BOM for Windows』の監視テンプレートダウンロードサイトはこちら
  https://www.say-tech.co.jp/support/download?hsLang=ja-jp

## サーバー設定仕様書自動生成サービス『SSD-assistance』

OSのさまざまな設定情報を簡単にドキュメント化する　サーバー設定仕様書自動生成サービス『SSD-assistance』のご案内です。

- サーバー設定仕様書自動生成サービス『SSD-assistance』の詳細はこちら

  https://www.say-tech.co.jp/product/ssda

- サーバー設定仕様書自動生成サービス『SSD-assistance』の無償評価利用お申し込みはこちら

  https://www.say-tech.co.jp/eval2

## お問い合わせ

本書に関するお問い合わせは、以下のフォームをご利用ください。

https://www.say-tech.co.jp/contact

---

**Windowsの運用管理を快適にする10の裏ワザ／表ワザ**　- セキュリティ編 -

2022年 5月 9日 初版

著作・発行者・発行

セイ・テクノロジーズ株式会社

© 2022 SAY Technologies, Inc.