WSUS 正常性監視のポイント

Windows 10 時代の重要インフラ WSUS、安定運用の勘所

山市 良 著

WSUS 正常性監視のポイント

Windows 10 時代の重要インフラ WSUS、安定運用の勘所

Windows 10 は、半年に 1 回（年に 2 回）、新バージョンがリリースされます。企業はこの新しいサービスモデルをしっかりコントロールしなければ、Windows Update に起因する互換性問題やネットワーク使用帯域の圧迫が大きな課題となってしまうでしょう。企業の標準クライアントとして Windows 10 の導入が進む中、その更新管理のための Windows Server Update Services（WSUS）の重要性がこれまで以上に高まっており、多くの企業が WSUS を効果的かつ安定的に運用する方法を模索しています。

ライター 山市良

Windows 10 の登場で再注目される WSUS

Windows Server が提供する「Windows Server Update Services（WSUS）」は、Windows Server や Windows クライアントで構成される Windows ネットワークにおいて、Windows やその他のマイクロソフト製品の更新プログラムを効率的に配布する、あるいはインターネット接続が制限されたクライアントに更新ポイントを提供するといった、重要な役割を果たしてきました。Windows 10 が登場するまで、WSUS は低コストで中・小規模から導入できるパッチ管理ツールという位置付けでした。多くの企業は、大規模対応、インベントリ収集、ソフトウェアの配布、OS のアップグレードの展開などを含む高度な更新管理のために、System Center Configuration Manager（SCCM）やサードベンダーの電子ソフトウェア配布（Electric Software Delivery、ESD）システムを導入することを選択しました。一方で、Windows Server の標準機能だけで構築できる WSUS は、中小規模環境には導入がしやすく、階層構造でダウンストリームサーバーやレプリカサーバーを設置できるため、リモート拠点にも柔軟に対応できるという利点があります。

WSUS は、マイクロソフトの製品サポート期間中のすべてのバージョンの Windows、マイクロソフト製品、およびサードベンダーのドライバーの、完全にコントロールされた、集中的な更新管理環境を企業内に構築することができます。Windows 10 の登場により、WSUS はさらに、Windows 10 の新しいサービスモデルに対応した新たな役割を担うことになります（図 1）。

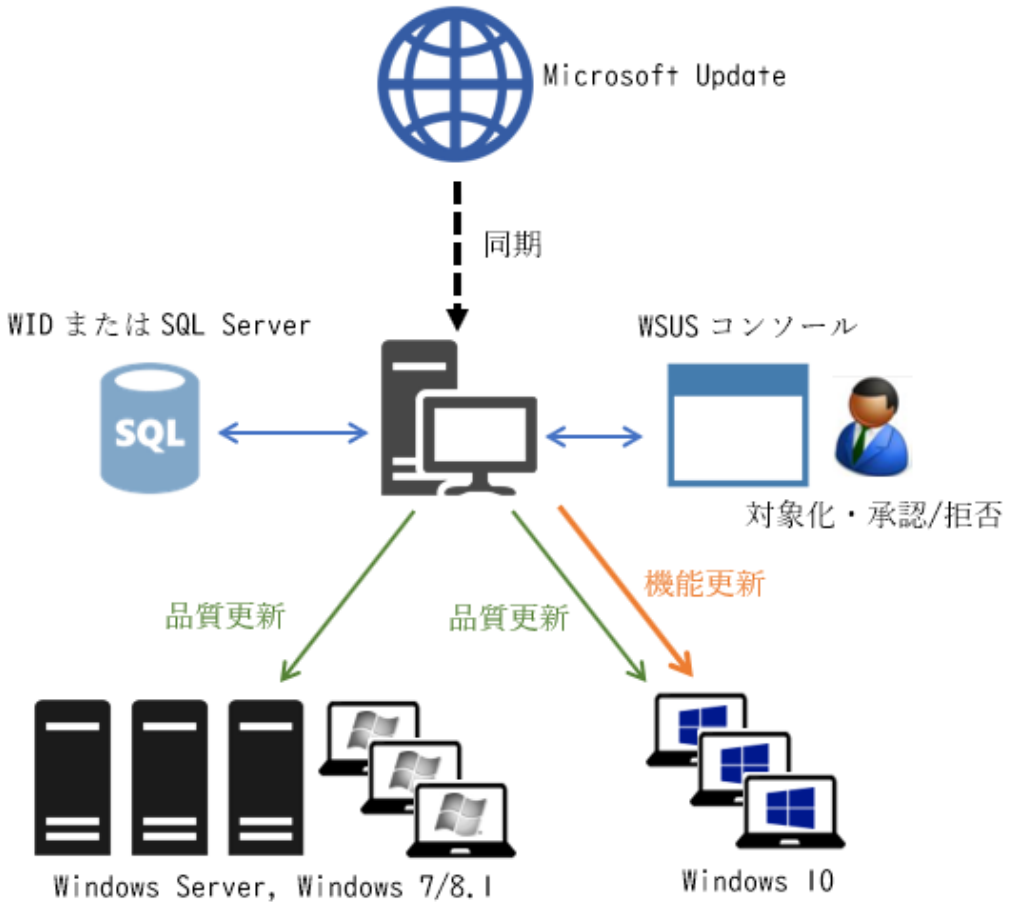
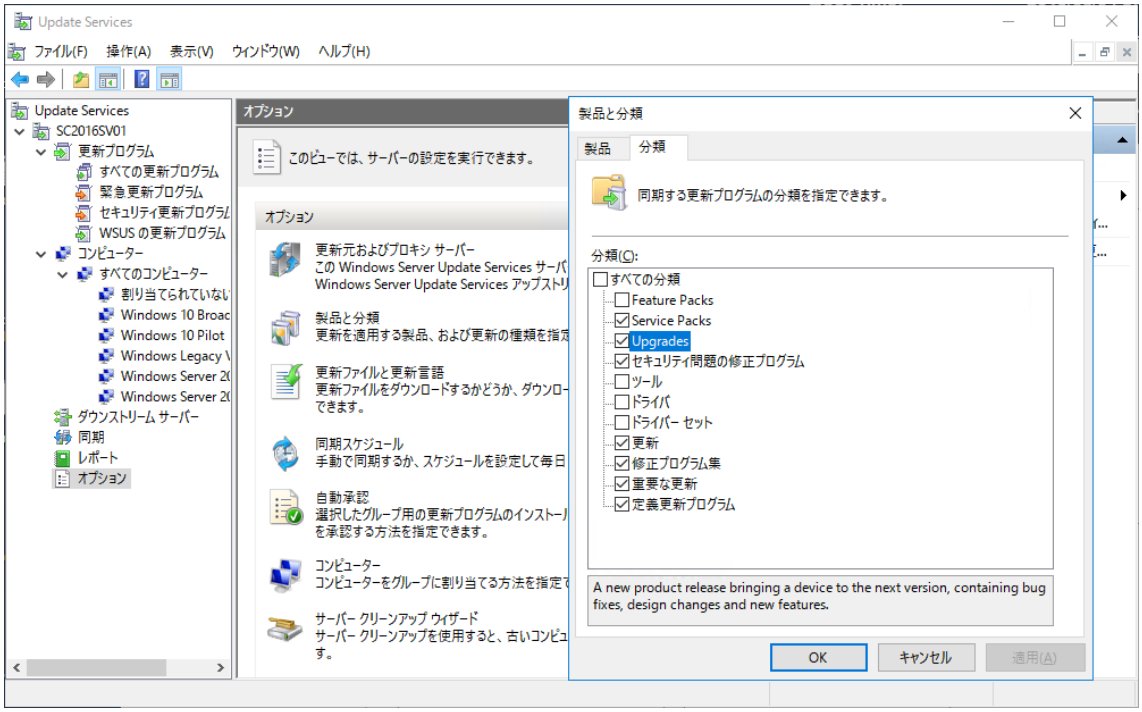


図 1　WSUS の導入イメージ。企業内の集中的なパッチ管理ツールだった WSUS は、Windows 10 に対しては機能更新プログラム（アップグレード）を提供するようにもなった

Windows 10 では、「サービスとしての Windows（Windows as a Service）」のコンセプトのもと、半期チャネル（Semi-Annual Channel、SAC）という新しいサービスモデルが導入されています。半期チャネルのサービスモデルでは、半年に 1 回の短いサイクルで「機能更新プログラム」という名前で Windows 10 の新しいリリース（新しいビルド）が提供され、各リリースには最大 18 か月または 30 か月（リリース時期とエディションに依存）、セキュリティ更新や不具合の修正、定義ファイルの更新などが「品質更新プログラム」として提供されます。一般ユーザーは、機能更新プログラムと品質更新プログラムの両方を Windows Update を通じて、両者をほとんど変わらないエクスペリエンスで受け取ることができます。

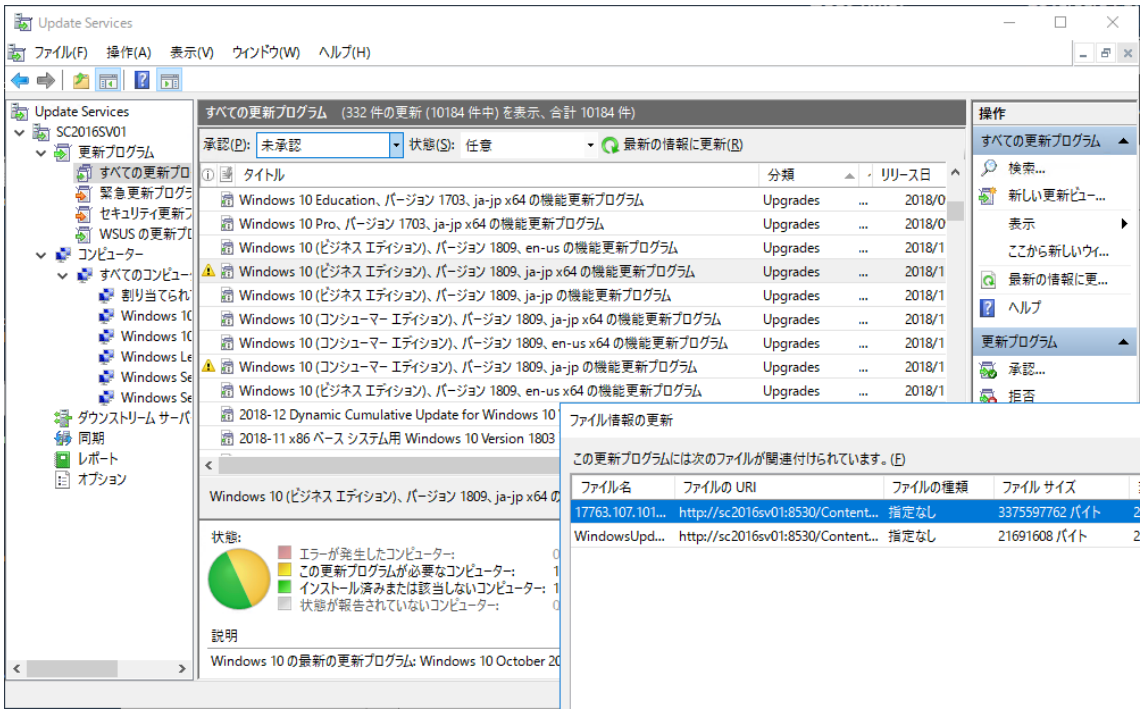
WSUS はこれまで OS のアップグレード展開の機能は提供してきませんでしたが、Windows 10 に対しては機能更新プログラムと品質更新プログラムの両方を提供するようになりました（画面 1）。つまり、SCCM（SCCM も WSUS を利用しています）やその他の ESD システムを使用しなくても、WSUS だけで Windows 7/8.1 から Windows 10 へのクライアント OS のアップグレード、および Windows 10 の新しい機能更新プログラムへのアッ

プグレードが行えるようになったのです。Windows 10 の Windows Update の改良は、従来のようにアップグレード展開のために配布用イメージをカスタマイズしたり、応答ファイルで自動化したりする必要性を省きました（従来の方法も引き続き利用できます）。



画面 1　「Upgrades」は Windows 10 で追加された WSUS の新しい分類であり、Windows 10 の機能更新プログラムの配布に対応する

Windows 10 の機能更新プログラムは、更新プログラムという名前ですが、実質は Windows の新バージョンのアップグレードであり、クライアントのダウンロードサイズは数 GB になります（画面 2）。また、Windows 10 の品質更新プログラムは累積的であり、機能更新プログラムのリリースから時間が経つと次第に品質更新プログラムのサイズが大きくなっていきます（1GB を超えることもあります）。機能更新プログラムと品質更新プログラムのダウンロードサイズや配信方法など、技術的な改善の努力は継続して行われていますが、企業内のクライアントが個別に、同時期に Windows Update で更新されてしまうと、企業のインターネット接続回線をあっという間に逼迫してしまい、通常の業務の遂行に支障をきたしてしまうでしょう。ネットワークの使用を効率化するために、WSUS はこれまで以上に重要なインフラストラクチャになったのです。



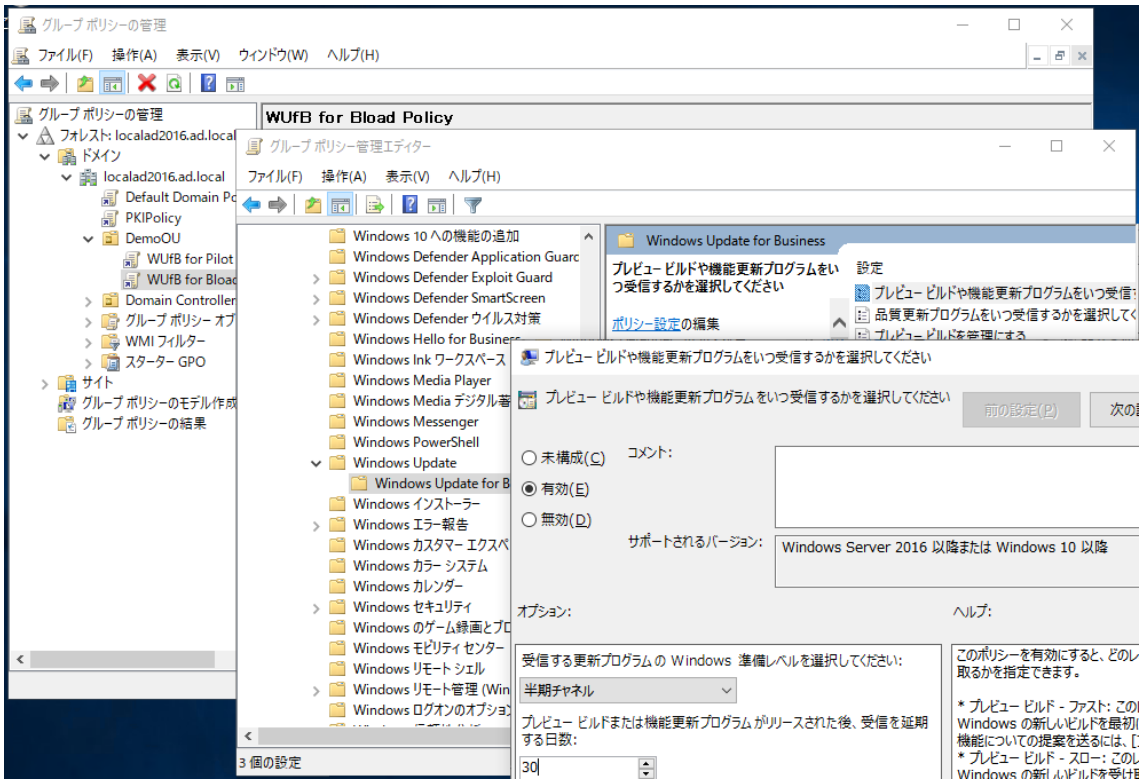
画面 2　例えば、64 ビット版 Windows 10 October 2019 Update（バージョン 1809）の機能更新プログラムのダウンロードサイズは約 3.14GB。x64 が付かない機能更新プログラムは 32 ビット版と 64 ビット版の両方を含むパッケージ

なお、Windows Server 2008/2008 R2 上の WSUS 3.0 SP2 は、Windows 8.1 および Windows Server 2012 R2 以前を想定したもので、Windows 10 の機能更新プログラムの配布をサポートしていません（Windows 10 の品質更新プログラムの配布は可能です）。Windows 10 の機能更新プログラムに対応するためには、Windows Server 2012 以降の WSUS（WSUS 4.0 とも呼ばれます）が必要です。

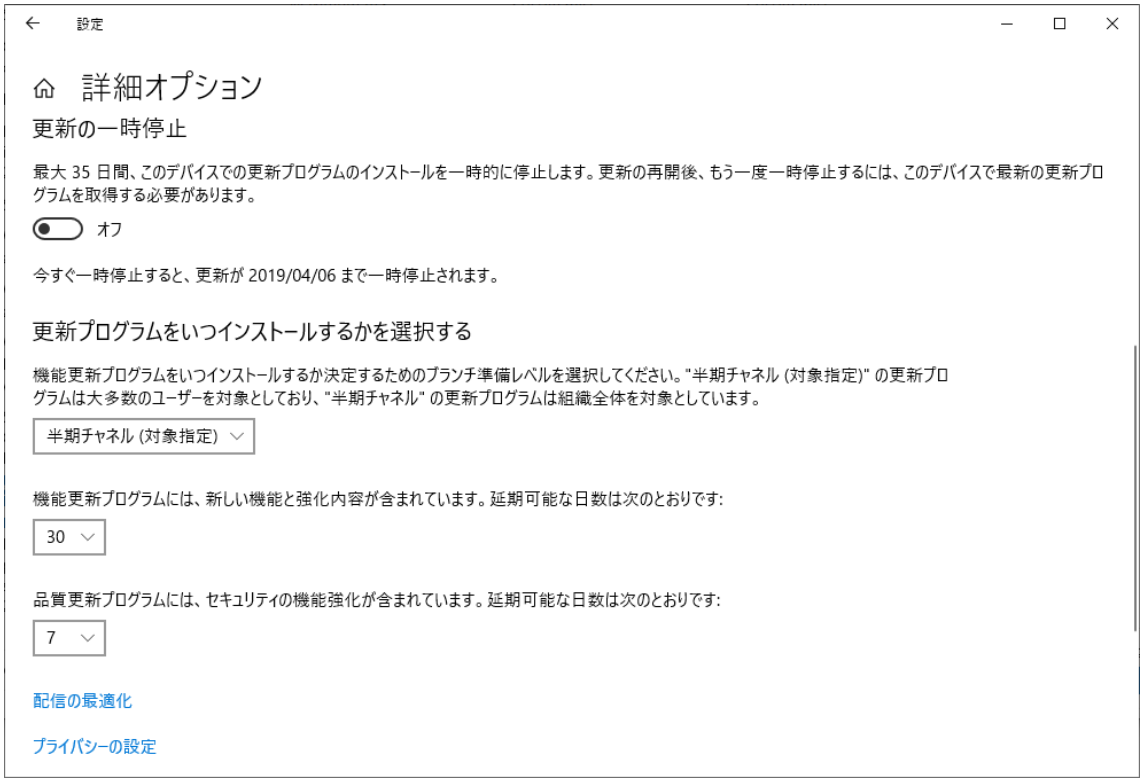
Windows Update for Business と WSUS の違い

Windows 10 の機能更新プログラムおよび品質更新プログラムは、WSUS で完全にコントロールできます。WSUS とは別に、「Windows Update for Business（WUfB）」を利用して受け取る時期をコントロールすることも可能です（画面 3）。WUfB はもともとグループポリシーの機能として登場した機能更新プログラムおよび品質更新プログラムの延期設定として登場しましたが、Windows 10 バージョン 1703 以降はクライアント側の「設定」アプリでユーザー自身が構成できるようにもなりました（画面 4）。Windows 10 バージョン 1809 までは機能更新プログラムの一般向けリリースと同日の「半期チャネル（対象指定）」とその 2～3 か月後の「半期チャネル」から選択でき、さらに日数（最大 365 日）による延期を

行うことができます。Windows 10 バージョン 1903 からは「半期チャネル（対象指定）」が廃止され、機能更新プログラムの一般向けリリース日からの日数で延期（最大 365 日）のみとなります。品質更新プログラムについては、リリースされてから最大 30 日延期することができます。



画面 3　「Windows Update for Business」ポリシーを使用した機能更新プログラムの延期設定（Windows 10 バージョン 1607 までは「Windows Update の延期」ポリシー）

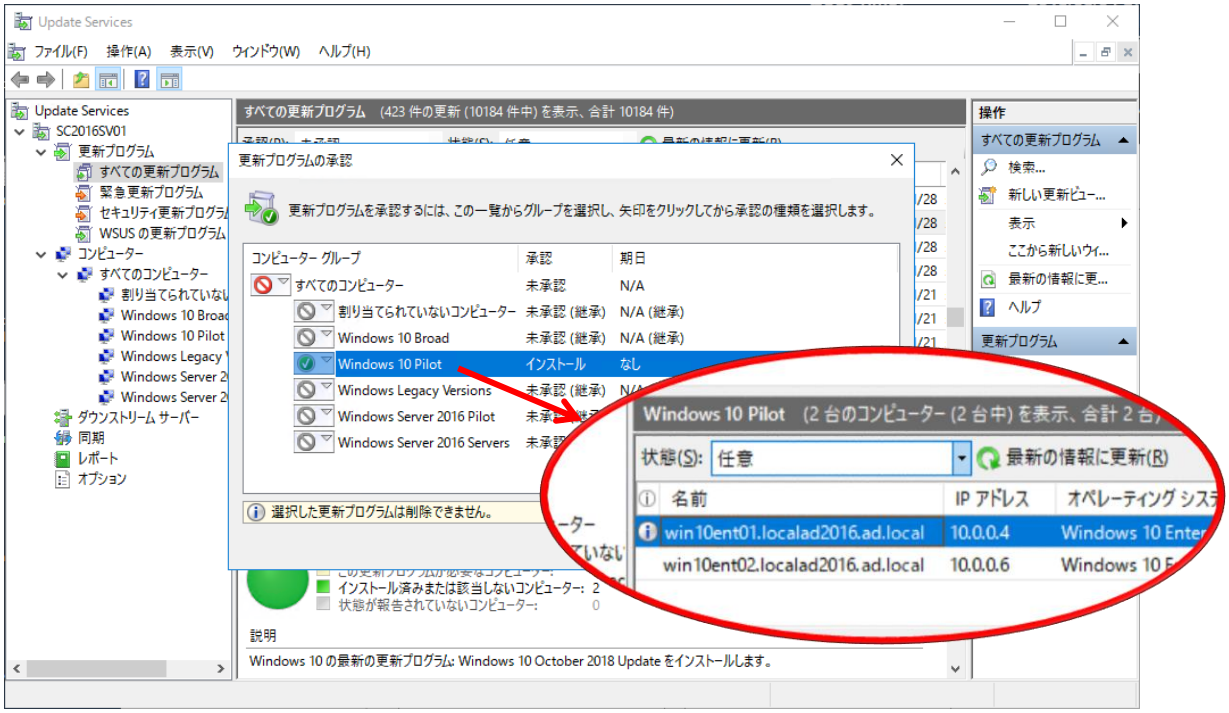


画面 4　Windows 10 バージョン 1703 以降は WUfB をクライアント側の「設定」アプリで構成することも可能に（画面はバージョン 1809）。なお、バージョン 1903 でブランチ準備レベルのオプションは廃止される（SAC に一本化）

WUfB と WSUS を併用することは可能ですが、その利用シナリオは限定されたものであり、それを十分に理解していないと適切に運用することはできないでしょう。WSUS クライアントは、WSUS サーバー側で管理者が承認した、利用可能なすべての更新プログラムを受け取ります。一方、WUfB クライアントは、常に Microsoft Update で利用可能な更新プログラムを検索します。WUfB クライアントがその延期設定に基づいて、WSUS から機能更新プログラムや品質更新プログラムを受け取るような動作はしません。WUfB と WSUS を併用する利用シナリオとしては、Windows 10 の機能更新プログラムと品質更新プログラムを WUfB で受け取り、Windows 10 以外の更新プログラムは WSUS の承認に基づいて受け取るというものに限定されます。Windows 10 以外の更新プログラムには、Windows 以外のマイクロソフト製品（MSI 版 Microsoft Office など）の更新プログラムやサードベンダーのドライバーがあります。

一方、WSUS を導入している場合は、管理者による承認に基づいて、機能更新プログラムや品質更新プログラムの配布を詳細にコントロールできます。また、WSUS のコンピューターグループを利用して配布対象の対象化を行うことが可能です。Windows の更新プログラムは、しばしば不具合が含まれていたり、アプリケーションの互換性に影響することがあ

ります。先行展開用のコンピューターグループに対して先に更新プログラムを配布し、その結果を評価した上で、全社展開用のコンピューターグループに展開するという、計画的、段階的な展開が可能です（画面 5）。



画面 5　WSUS を導入済みであれば、コンピューターグループを利用して先行展開、評価、全社展開のように、段階的に機能更新プログラムや品質更新プログラムを配布できる

つまり、「半期チャネル（対象指定）」と「半期チャネル」の区別は WUfB だけのものであり、WSUS にはまったく関係しません。そして、WSUS を導入する場合は、通常、WUfB と併用することはありません。

WSUS を安定的に運用するための考慮点

Windows 10 の WSUS クライアントが存在するかどうかにかかわりなく、WSUS の導入やセットアップは比較的簡単です。しかし、更新対象の規模やネットワークトポロジによってはネットワークトラフィックを最適化するための調整が必要ですし、Windows 10 を含む広範囲の Windows バージョンおよびマイクロソフト製品の更新のため、適切にメンテナンスしなければデータベースや WsusContent（<コンテンツの場所のパス>¥WsusContent）フォルダー内のコンテンツが肥大化してしまい、WSUS のパフォーマンスが劣化したりディスクを圧迫したりする一因になります。

WSUS を安定的に運用していく上で、以下に示す 5 点は、特に重要な考慮点になります。

- エンドユーザーによる Microsoft Update の検索をブロック
- ネットワーク使用帯域の制御
- WSUS サービスの正常性の監視
- WSUS のディスク使用率の監視
- WSUS のクリーンアップタスクの定期的な実施

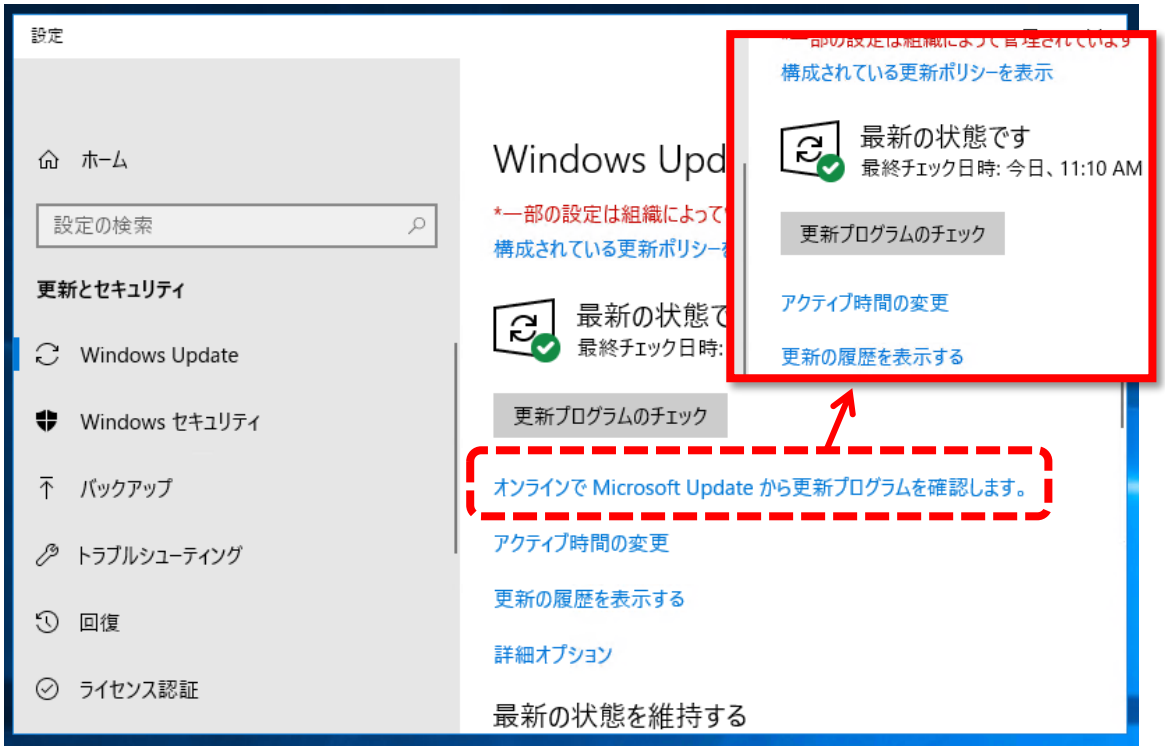
考慮点① ― エンドユーザーによる Microsoft Update の検索をブロック

WSUS クライアントの Windows を利用するエンドユーザーが、不用意に Microsoft Update をチェックして WSUS で承認していない更新プログラムがインストールしてしまうと、せっかくの WSUS での詳細なコントロールが失われてしまいます。WSUS クライアントとして構成されていても、クライアント側の Windows Update の UI には Microsoft Update カタログを検索するためのオプションが存在し、エンドユーザーは WSUS の代わりに Microsoft Update を検索して更新プログラムを取得できます。例えば Windows 10 の場合、「設定」アプリの「Windows Update」に表示される「オンラインで Microsoft Update から更新プログラムを確認します。」がそのオプションです。この Microsoft Update をチェックするオプションは、グループポリシー（またはローカルコンピューターポリシー）で以下のいずれかのポリシーを有効にすることで非表示にできます。

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¥インターネット通信の管理¥インターネット通信の設定¥Windows Update のすべての機能へのアクセスをオフにする（Windows 8.1 以降はこちらを推奨）

または

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 Update¥インターネット上の Windows Update に接続しない（Windows 8.1 以降は Microsoft ストアとの通信にも影響することに注意が必要）



画面 6　ポリシー設定を利用して「オンラインで Microsoft Update から更新プログラムを確認します。」を非表示にすることで、ユーザーが Microsoft Update をチェックして、WSUS で承認されていない更新プログラムを取得するのを防止できる

考慮点② ― ネットワーク使用帯域の制御

多くの企業にとって WSUS を導入する目的の 1 つは、クライアントが個別に Microsoft Update に接続して更新プログラムをダウンロードしてしまうことによる、インターネット接続回線の使用帯域の改善でしょう。社内に WSUS サーバーを 1 台設置することで、WSUS サーバーと Microsoft Update との同期およびコンテンツのダウンロードを一本化することができます。しかし、一本化したダウンロードトラフィック自体が回線の帯域を占有する可能性は残っています。WSUS はコンテンツのダウンロードに「バックグラウンドインテリジェント転送サービス（BITS）」を使用するため、以下のポリシーを使用して BITS が使用する帯域の上限値（Kbps）を設定することで、帯域の占有を回避することができます。

コンピューターの構成（¥ポリシー）¥管理用テンプレート¥ネットワーク¥バックグラウンドインテリジェント転送サービス（BITS）¥BITS バックグラウンド転送の最大ネットワーク帯域幅を制限する

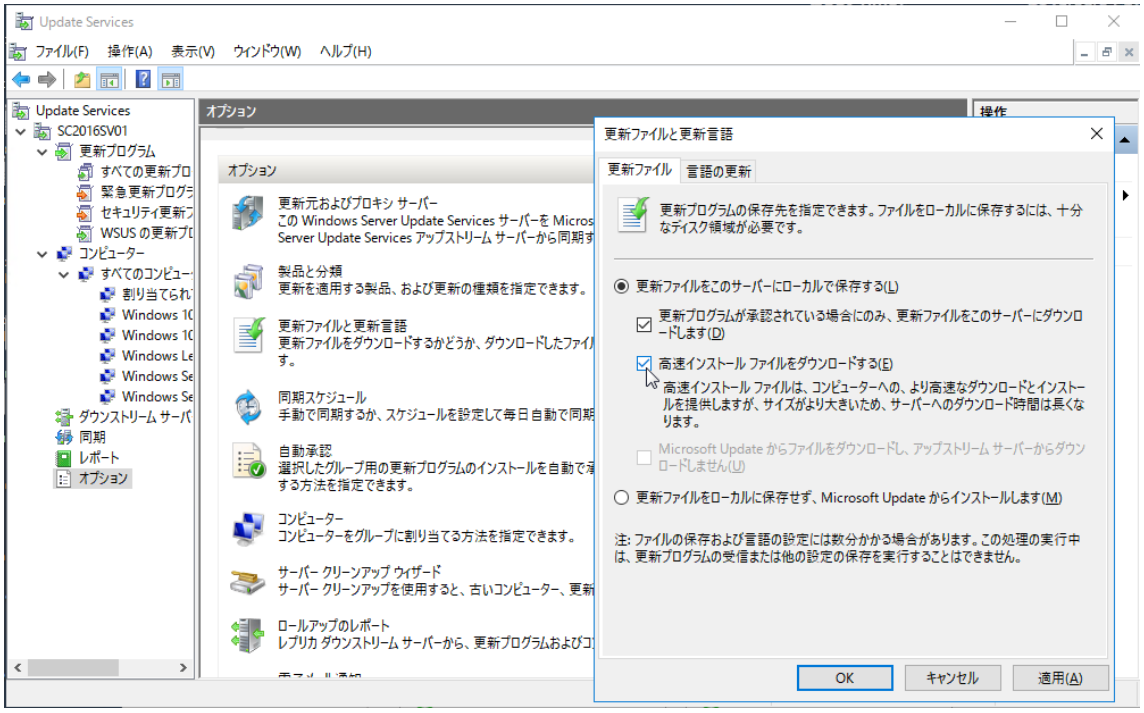
社内に WAN で接続されたリモート拠点がある場合は、WSUS のダウンストリームサー

バー（WSUS の管理は各拠点で）やレプリカサーバー（WSUS の管理は中央で）を設置し、同じように BITS の使用帯域を制限することで、WAN のトラフィックを最適化できます。

社内の LAN のトラフィックを最適化、つまり WSUS サーバーと WSUS クライアントの間のダウンロードを高速化したい、あるいは LAN のトラフィックを削減したいなら、「高速インストールファイル」の使用を検討してください。WSUS で「高速インストールファイル」のサポートを有効化すると、Microsoft Update からダウンロードされるコンテンツや WsusContent フォルダー内のコンテンツは増加しますが、WSUS サーバーから WSUS クライアントへのダウンロードサイズは大幅に小さくなります（画面 7）。

このほか、LAN のトラフィックの最適化のためには、Windows Server および Windows クライアントが備える「BranchCache」のキャッシュ機能や、Windows 10 の「配信の最適化」によるピアツーピア配信機能を利用できます。

WSUS に関連するネットワークトラフィックの影響や最適化の効果を測るには、WSUS サーバーの同期のタイミングや WSUS クライアントの更新プログラムのダウンロードのタイミングで、インターネット接続回線や WAN 回線に接続するネットワークデバイスのトラフィック量や LAN のトラフィック量を監視するとよいでしょう。



画面 7　WSUS で「高速インストールファイル」のサポートを有効化すると、WSUS クライアントは更新プログラム全体ではなく、更新が必要なファイルのみのをダウンロードするため、LAN のトラフィックを削減できる

【2021 年 6 月 3 日 追記】

高速インストールファイルの対象は、Windows 10 バージョン 1803 までです。Windows 10 バージョン 1809 および Windows Server 2019 以降は、累積更新プログラムについては高速インストールファイルが使用されなくなりました。

考慮点③ ― WSUS サービスの正常性の監視

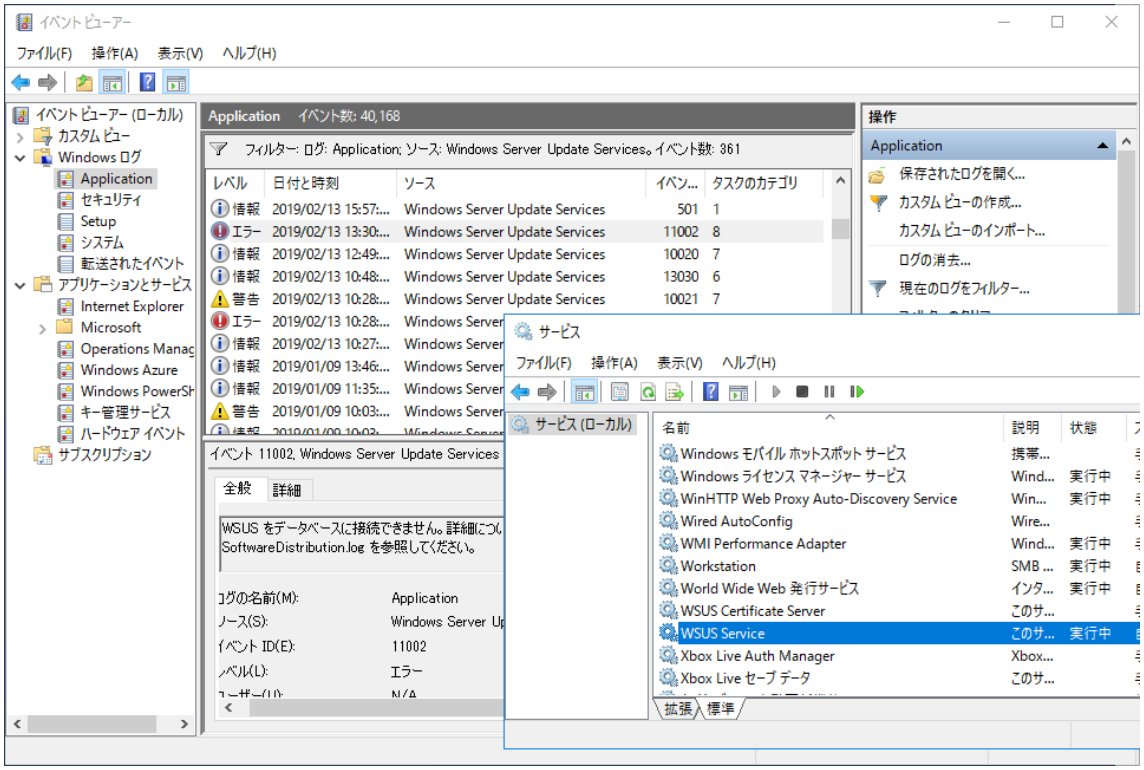
WSUS サーバーでは、Windows の以下のサービスが WSUS の更新管理環境を提供します（この他にも BITS など、オンデマンドで WSUS が使用するサービスがあります）。以下のサービスのいずれかが停止している場合、WSUS サーバーの同期処理や管理コンソールの機能、WSUS クライアントへのサービス提供に影響する場合があります。

- WSUS Service（サービス名：WSUSService）
- World Wide Web 発行サービスまたは World Wide Web Publishing Service（サービス名：W3SVC）
- SQL Server（MSSQLSERVER）（サービス名：MSSQLSERVER）または Windows Internal Base（サービス名：MSSQL$MICROSOFT##WID）

WSUS の正常性を監視するためには、これらのサービスの動作状況を確認します。なお、後述するクリーンアップタスクの実行中、WSUS Service が一時的に停止状態になるのは想定された挙動であることに留意してください。

IIS（W3SVC）については、「WSUS の管理」サイトにバインドされた TCP ポート 8530（http）や 8531（https）の監視や、「WsusPool」アプリケーションプールの状態も監視することをお勧めします。

また、イベントログの Application ログには、イベントソース「Windows Server Update Services」のイベントとして、WSUS の正常性に関する重要なイベントが記録されます（画面 8）。表 1 は、WSUS の正常性に関係するエラーおよび警告イベントで、筆者が把握しているものをまとめたものです。



画面 8　WSUS 関連の Windows サービスの稼働状況と WSUS の重要なイベントを監視する

レベル	イベント ID	メッセージ
エラー	1102	WSUS をデータベースに接続できません。詳細については、SoftwareDistribution.log を参照してください。
警告	7032	WSUS 管理コンソールは、リモート API 経由で WSUS サーバーに接続できませんでした。...
エラー	7053	WSUS 管理コンソールで予期しないエラーが発生しました。これは一時的なエラーの可能性があります。管理コンソールを再起動してみてください。このエラーが続く場合は、%appdata%¥Microsoft¥MMC¥ の下にある wsus ファイルを削除することにより、コンソールの保存される設定を削除してください。...
警告	10021	カタログが正しく同期されたのは、1 日以上前です。
エラー	10022	最後のカタログ同期の試みは正しく行われませんでした。
エラー	11002	WSUS をデータベースに接続できません。詳細については、SoftwareDistribution.log を参照してください。
エラー	12002	レポート Web サービスは動作していません。

エラー	12012	API リモート Web サービスは動作していません。
エラー	12022	クライアント Web サービスは動作していません。
エラー	12032	サーバー同期 Web サービスは動作していません。
エラー	12042	単純な認証 Web サービスは動作していません。
エラー	12052	DSS 認証 Web サービスは動作していません。
エラー	12072	WSUS コンテンツ ディレクトリにアクセスできません。...
エラー	13002	クライアント コンピューターは 25% を超える失敗率で更新プログラムをインストールしています。これは正常ではありません。
エラー	13032	多くのクライアント コンピューターは、ここ 30 日間サーバーにレポートを戻していません。これまでに X 台が検出されました

表 1　WSUS の正常性に関するエラーおよび警告イベント（イベントソースはすべて Windows Server Update Services）

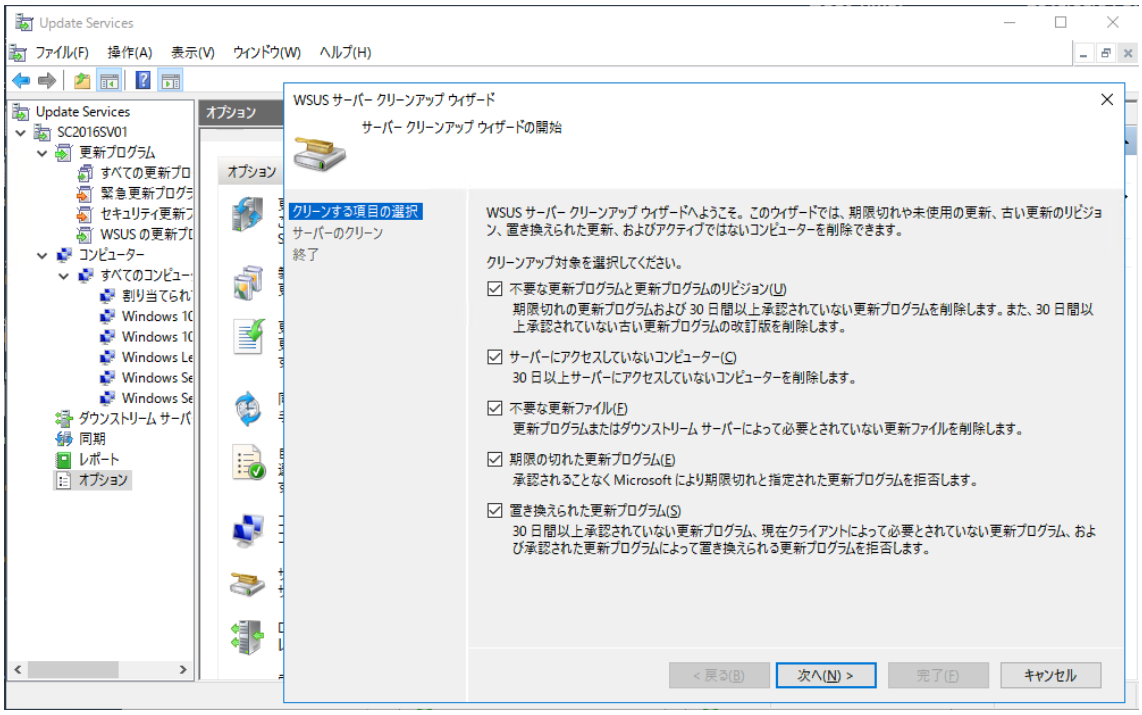
考慮点④ ― WSUS のディスク使用率の監視

WSUS サーバーは Microsoft Update と更新カタログを同期して、更新プログラムのメタデータをデータベースに、管理者が承認（自動承認を含む）した更新プログラムの本体を WsusContent フォルダーに格納します。WSUS を導入して、運用していくにつれ、これらのデータは蓄積され、増大していきます。一方、WSUS には不要なデータを自動削除するような、自己管理機能は搭載していません。データベースの肥大化は WSUS のパフォーマンスを低下させる一因になります。WsusContent フォルダーは、ディスク領域を圧迫する可能性があります。不要なデータは、後述するクリーンアップタスクを実施することにより、整理することができます。

Windows 10 の品質更新プログラムは累積更新プログラムとして提供され、新しい品質更新プログラムは、これまでリリースされている品質更新プログラムの内容に、新しいセキュリティ更新や不具合の修正を加えたものになっています（現在は Windows 8.1 以前や Windows Server 2012 以前の更新プログラムも累積更新プログラムのタイプになっています）。そのため、WSUS サーバー上で古い品質更新プログラムをいつまでも利用可能な状態にしておくことはディスク領域の無駄になります。また、「高速インストールファイル」のサポートを有効化すると、WsusContent フォルダーのコンテンツサイズが数倍に肥大化するので特に注意が必要です。WSUS サーバーのコンテンツ格納用ディスクの使用率または空き領域の監視と警告は、継続的に行うべきであり、自動化したいところです。

考慮点⑤ ― WSUS のクリーンアップタスクの定期的な実施

WSUS には不要なデータを自己管理する機能はありませんが、WSUS の管理コンソールである「Update Services」スナップインの「オプション」から「WSUS サーバークリーンアップウィザード」を実行することで、手動で不要なデータの削除や圧縮を行うクリーンアップタスクを実行させることができます（画面 9）。



画面 9　不要なデータを削除して、データベースを健全化し、ディスク領域を解放するには、「WSUS サーバークリーンアップウィザード」を定期的（1 か月に 1 回など）に実行する

このウィザードは、毎月 1 回など定期的に実行することが望ましいもので、実行せずに長期間放置した WSUS サーバーでは「WSUS サーバークリーンアップウィザード」の実行に長い時間がかかったり、タイムアウトで失敗したりする場合があります。その場合、時間はかかりますがオプションを 1 つずつ選択実行することでタスクを完了できる場合があります。なお、レプリカサーバーを設置している場合は（ダウンストリームサーバーには影響しません）、承認/拒否状態の不整合が発生しないように、下位層のレプリカサーバーで先にウィザードを実行し、その後、上位の WSUS サーバーで実行する必要があることに留意してください。

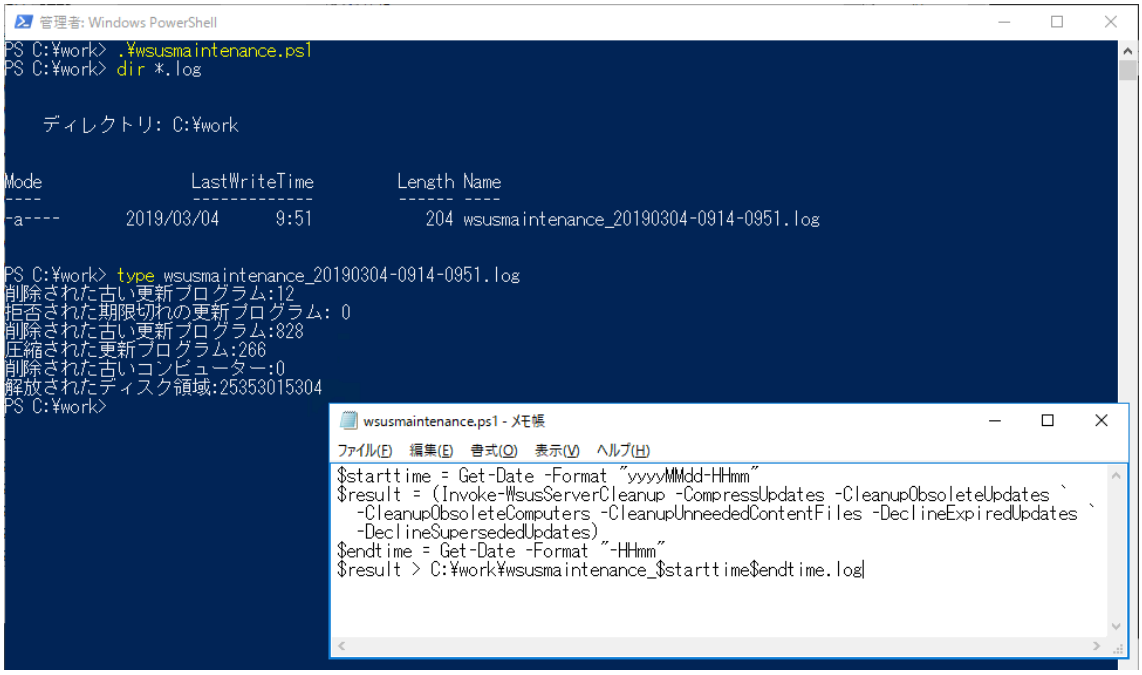
「WSUS サーバークリーンアップウィザード」を開始すると、クリーンアップタスクが完了するまで WSUS のサービスが一時的に停止します。そのため、このウィザードは WSUS

の同期タスクの実行中や、WSUS クライアントの更新時間帯を避けて実行する必要があります。影響のない夜間などに「WSUS サーバークリーンアップウィザード」の実行を自動化したい場合は、Windows PowerShell の Invoke-WsusServerCleanup コマンドレットを利用する方法があります。このコマンドレットは、「WSUS サーバークリーンアップウィザード」と同じクリーンアップタスクを個別または一括で実行するものです。

例えば、次に示す PowerShell スクリプトのサンプル「WsusMaintenance.ps1」を、定期実行タスクとしてタスクスケジューラに登録します（プログラム：powershell.exe、引数：スクリプトのパス）。このサンプルでは、「WSUS サーバークリーンアップウィザード」ですべてのオプションを有効（既定）にして実行したのと同じクリーンアップタスクを実行し、その実行結果を「C:¥Work¥WsusMaintenance_年月日-開始時刻-終了時刻.log」というテキストファイルに出力します（画面 10）。

WsusMaintenance.ps1

```
$starttime = Get-Date -Format "yyyyMMdd-HHmm"
$result = (Invoke-WsusServerCleanup -CompressUpdates `
  -CleanupObsoleteUpdates `
  -CleanupObsoleteComputers `
  -CleanupUnneededContentFiles `
  -DeclineExpiredUpdates `
  -DeclineSupersededUpdates)
$endtime = Get-Date -Format "-HHmm"
$result > C:¥work¥wsusmaintenance_$starttime$endtime.log
```



画面 10　「WSUS サーバークリーンアップウィザード」の既定のオプションと同じすべてのクリーンアップタスクを実行する PowerShell スクリプト「WsusMaintenance.ps1」の実行例

「WSUS サーバークリーンアップウィザード」や Invoke-WsusServerCleanup コマンドレットの実行結果やエラーは、Windows のイベントログには記録されません。上記のようなサンプルを使用して独自に取得しない限り、クリーンアップされた項目を調査するには、ログファイル「%ProgramFiles%¥Update Services¥LogFiles¥SoftwareDistribution.log」を調査する必要があります。このログファイルには、エラー情報も記録されます。

実行結果やエラー発生を含めて効率的に監視できるようにするため、先ほどサンプルにさらに改良を加えました。

次の PowerShell スクリプトのサンプル「WsusMaintenanceLogEvent.ps1」は、Invoke-WsusServerCleanup コマンドレットを実行し、開始とその実行結果をイベントログの Application ログに情報または警告のカスタムイベント（イベント ID 65000～65002）として記録します。また、Invoke-WsusServerCleanup コマンドレットで発生した例外エラーを補足して、エラーのカスタムイベント（イベント ID 65003）として記録します（画面 11）。データベースのサービスを停止してから実行することで、エラー発生時のイベントをテストすることができます。タスクの実行にかかった時間は、イベントの「日付と時刻」から判断してください。なお、このサンプルを初めて使用する際には、WSUS サーバー上でコメント欄にある New-EventLog コマンドレットを一度だけ実行し、イベントソースを作成しておく必要があります。また、サンプルで使用しているイベントソースの名前は、既存のものと重複しない限り任意の名前に変更できますし、カスタムイベントのイベント ID は 0～

65535 の範囲に任意の番号に変更できます。

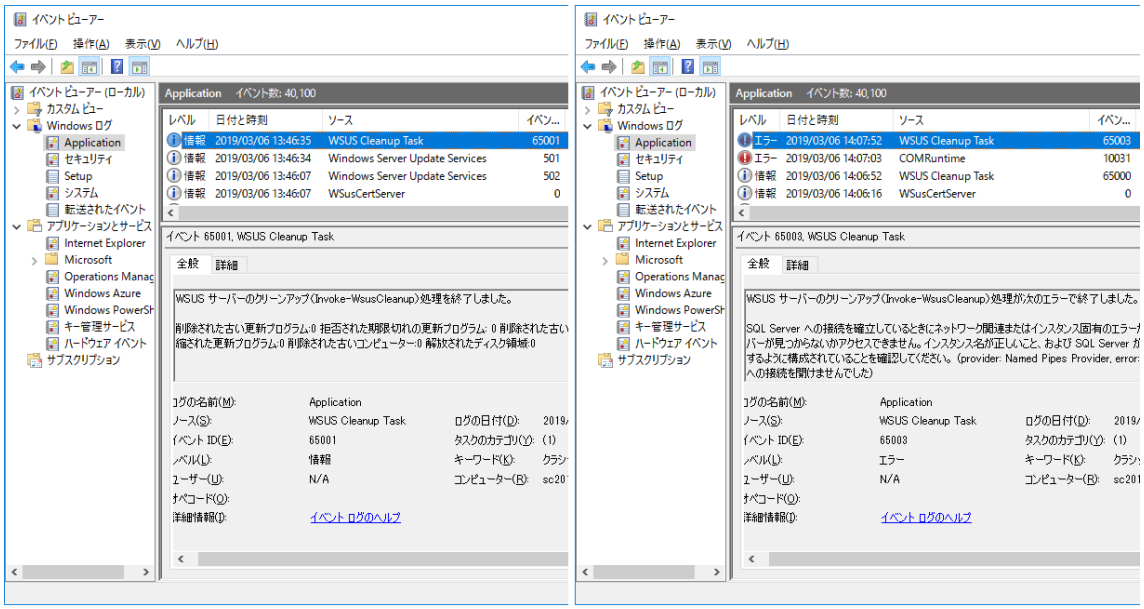
紹介した 2 つのサンプルのいずれかを利用することで、ログファイルやイベントログを使用してクリーンアップタスクの実行状態を監視することができるでしょう。

WsusMaintenanceAndLogEvent.ps1

```
# このスクリプトを初めて実行する場合は、事前に PowerShell を開いて以下のコマンドラインを一度だけ実行する必要があります。
# New-EventLog -LogName Application -Source "WSUS Cleanup Task"
#

$message = "WSUS サーバーのクリーンアップ（Invoke-WsusCleanup）処理を開始します。"
Write-EventLog -LogName Application -Source "WSUS Cleanup Task" -EventID 65000 -EntryType INFORMATION -Message $message
try {
  $result = (Invoke-WsusServerCleanup -CompressUpdates `
    -CleanupObsoleteUpdates `
    -CleanupObsoleteComputers `
    -CleanupUnneededContentFiles `
    -DeclineExpiredUpdates `
    -DeclineSupersededUpdates)
  if ($result -ne $null) {
    $message = "WSUS サーバーのクリーンアップ（Invoke-WsusCleanup）処理を終了しました。`r`n`r`n"+$result
    Write-EventLog -LogName Application -Source "WSUS Cleanup Task" -EventID 65001 -EntryType INFORMATION -Message $message
  } else {
    $message = "WSUS サーバーのクリーンアップ（Invoke-WsusCleanup）処理を終了しましたが、結果がありません。"
    Write-EventLog -LogName Application -Source "WSUS Cleanup Task" -EventID 65002 -EntryType WARNING -Message $message
  }
}
catch {
    $message = $error[0].Exception.Message
    $message = "WSUS サーバーのクリーンアップ（Invoke-WsusCleanup）処理が
```

```
次のエラーで終了しました。`r`n`r`n"+$message
    Write-EventLog -LogName Application -Source "WSUS Cleanup Task"
-EventID 65003 -EntryType ERROR -Message $message
}
```



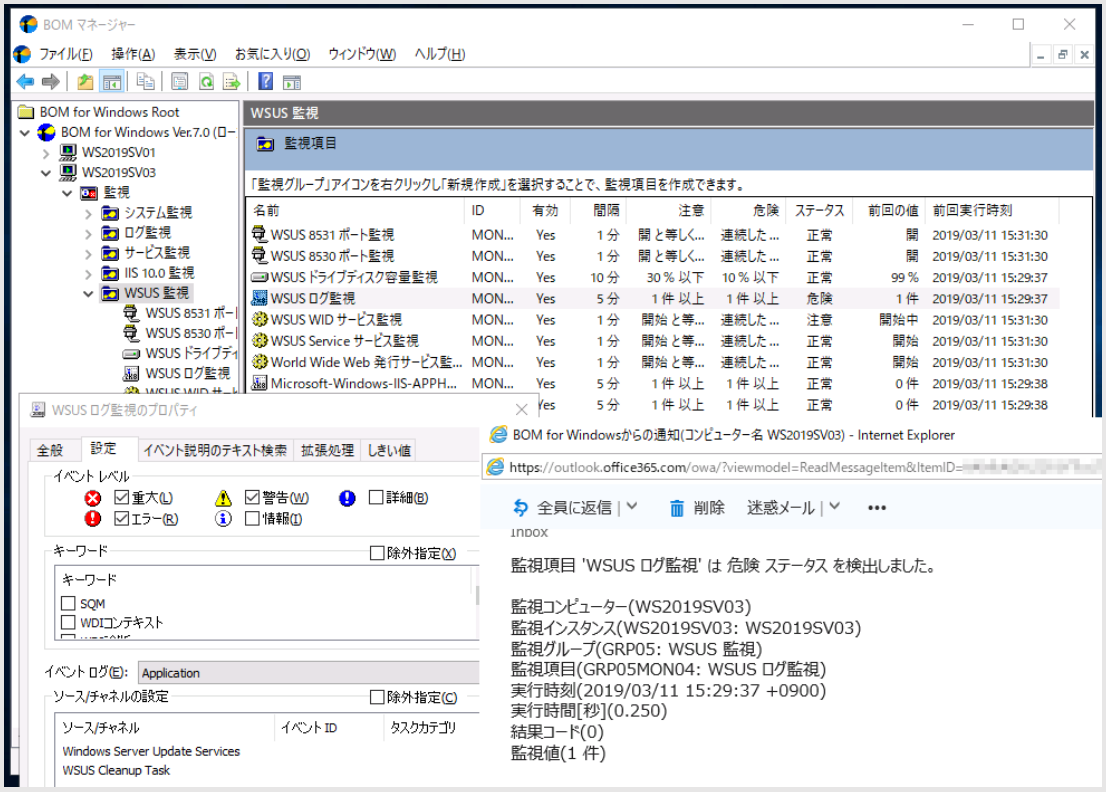
画面 11　PowerShell スクリプト「WsusMaintenanceAndLogEvent.ps1」で記録されたカスタムイベントの例

コラム

BOM for Windows Ver.7.0 SR2 を使用した WSUS 監視のヒント

2019 年 4 月に BOM for Windows Ver.7.0 の最新アップデート、SR2 がリリースされました。SR2 では SR1 までの機能に加えて、①Windows Server 2019 への対応、②Amazon S3 互換ストレージへの対応（ストレージ容量監視、ファイル送信アクション）、③HPE Integrated Lights-Out（iLO）ログ監視への対応、④Microsoft Office 365 を使用したメール通知への対応の、新機能および機能改善が行われています。

BOM には豊富な監視テンプレートが付属しており、テンプレートをインポートすることで簡単に監視項目をセットアップできるという利点があります。現状、WSUS に特化した監視用テンプレートはありませんが、今回の WSUS の記事で紹介した監視のポイントを参考にすれば、「ディスク容量監視」「サービス監視」「イベントログ監視」「ポート監視」「ネットワークインターフェイス監視」を適切に構成して WSUS の監視設定を比較的簡単に実装できるはずです（画面 12）。



画面 12　WSUS サーバーのクリーンアップタスクのエラーも、サンプル「WsusMaintenanceAndLogEvent.ps1」を利用すれば監視することが可能

2019 年 4 月 1 日 初版
2021 年 6 月 3 日 改訂

著者　　山市 良
発行者　セイ・テクノロジーズ株式会社
発行　　セイ・テクノロジーズ株式会社