

Windowsの運用管理を快適にする
10の裏ワザ／表ワザ

パフォーマンス改善編

山市 良 著

メンテナンスタスクは確実に完了させること
- 自動ディスククリーンアップタスク
- NGENタスク

タスクスケジューラの使いこなし
- 週末に再起動をスケジューリングする
- PowerShellコマンドのスケジューリング
- PowerShellスクリプト（.ps1）のスケジューリング

Windowsファイアウォールの健全性チェック
- ネットワークの場所とファイアウォールプロファイルの関係
- コマンドラインによるプロファイルの確認と変更
- ファイアウォールのルールが肥大化していないか
  - ・事例1
  - ・事例2
  - ・事例3
  - ・事例4

重大障害につながるイベントログを見逃さない
- 過去24時間に発生した重大／エラー／警告イベントをすばやく確認する
- 構造化（XPath）クエリ式の簡単な作り方
- システムやアプリケーションの重大／エラー／警告イベントをリアルタイムに監視する
- Sysmonで詳細なアクティビティを徹底的にログに記録し、調査する

突然調子がおかしくなった!? そんなとき頼りになる信頼性モニター
- 信頼性モニターを起動するには
- トラブルシューティング事例

WSUSが遅くなった？ 長期運用WSUSのメンテナンス
- SUSDB用WID/SQL Serverの最小／最大メモリの調整
- 高速インストールオプションの必要性の検討
- WSUSサーバークリーンアップウィザードの定期的な実行
- その他のクリーンアップスクリプト

マルウェア対策の最適化
- Microsoft Defenderの自動除外
- Microsoft Defenderの自動除外＋カスタム設定
  - カスタム除外設定の追加
  - Hyper-Vホストのためのカスタム設定
  - Windowsコンテナーのためのカスタム設定
  - SQL Serverのためのカスタム設定
- 他社マルウェア対策製品を利用する場合の考慮事項

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-パフォーマンス改善テンプレート
    - ディスククリーンアップタスク実行
    - NGEN監視
    - FireWall監視
    - Microsoft Defender の除外設定監視
  - 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 ↲

メンテナンスタスクは確実に完了させること

通常、再起動が必要な更新プログラムをインストールする場合、コンピューターが再起動されることでその処理は完了します。しかし、次の更新プログラムがインストールされる前に、実行されていることが推奨されるメンテナンスタスクが残っています。

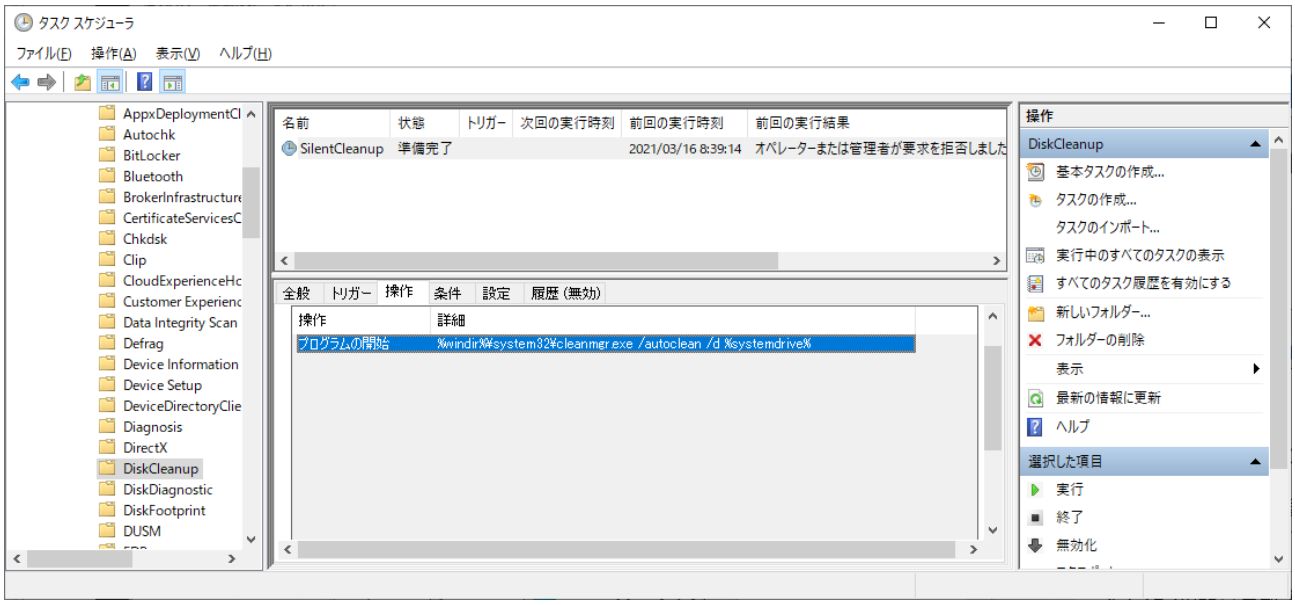
自動ディスククリーンアップタスク

Windows 8.1、Windows 10、デスクトップエクスペリエンス機能を追加したWindows Server 2012/2012 R2、およびWindows Server 2016以降のデスクトップエクスペリエンスでは、［タスクスケジューラ］（Taskschd.msc）の以下の場所にあるSilentCleanupタスクが定期的に実行されるようになっています（画面13）。

¥Microsoft¥Windows¥DiskCleanup¥SilentCleanup

SilentCleanupタスクは、コンピューターのアイドル時間にのみ実行され、アイドル状態でなくなると停止します。サーバーアプリケーションやインフラストラクチャサービスを実行するサーバーの場合、十分なアイドル時間が取れずにSlientCleanupタスクが完全に完了しない状態が続く可能性があります。

特に、更新プログラムのインストール後のSlientCleanupタスクは、Windows Updateの不要なコンポーネントの削除やコンポーネントストア（C:¥Windows¥WinSxS）の最適化（ファイルの圧縮など）が行われるため、完全に完了するためには余計に多くの時間がかかります。



画面13　SilentCleanupタスクは、Windows Update直後の実行には時間がかかるため、非アイドル状態になって途中で中止されることもある

更新プログラムのインストールのために業務時間外に集中して作業を行える場合は、SlientCleanupが実行するのと同じ以下のコマンドラインを、管理者として開いたコマンドプロンプトで実行します。コマンドプロンプトはすぐに帰ってきますが、cleanmgr.exeプロセスは実行中になります。［タスクマネージャー］（Taskmgr.msc）でcleamgr.exeプロセスが終了するまで待つとよいでしょう。

```
cleanmgr  /autoclean /d C: ↲
```

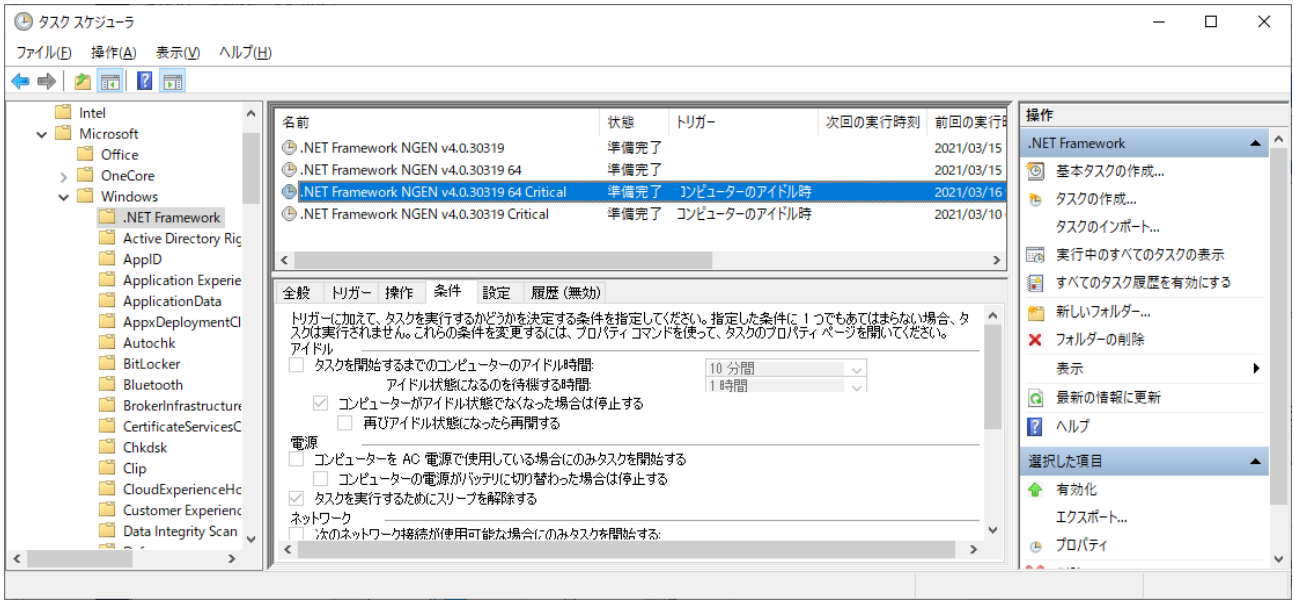
［ディスククリーンアップ］（cleanmgr.exe）を搭載しないServer Coreには、SlientCleanupタスクは存在しません。次のコマンドライン（/Resetbaseパラメーターは付けない）を実行することで、同様の効果を期待できます。

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

NGENタスク

.NET Frameworkの累積的な更新プログラム（注：Windows 10バージョン1803以前に標準搭載される.NET Frameworkバージョンの更新プログラムはWindowsの累積更新プログラムに含まれます）がインストールされると、以下の場所にある2つのタスク（32ビットOSの場合は2つ目のみ）が“準備完了”状態にセットされ、コンピューターのアイドル時間に自動実行されます（画面14）。

¥Microsoft¥Windows.NET Framework.NET Framework NGEN v4.0.30319 64 Critical
¥Microsoft¥Windows.NET Framework.NET Framework NGEN v4.0.30319 Critical



画面14　.NET Framework NGEN v4.0.30319 64 Critical（64ビット用）と.NET Framework NGEN v4.0.30319 Critical（32ビット用）は、.NET Frameworkの累積更新プログラムがインストールされると“準備完了”状態となり、実行が完了すると“無効”になる

これらのタスクは、.NET Frameworkのマネージドアプリケーションのパフォーマンスを向上するために、ネイティブイメージを生成して、ローカルコンピューターのネイティブイメージキャッシュに格納します。キャッシュが作成されることで、ランタイム時にJust-In-Time（JIT）コンパイラを使用してイメージをコンパイルする代わりに、キャッシュ内のイメージを使用できるようになります。

イメージキャッシュが存在しなければその時点でコンパイルされるため、これらのタスクが完了することは必須ではありません。しかし、これらのタスクの実行が次回のWindows Updateと重なると、システムの負荷が高まり、Windows Updateのインストール時間にも影響します。

更新プログラムのインストールのために業務時間外に集中して作業を行える場合は、タスクの状態を確認し、“準備完了”状態の場合は手動で集中的に実行するとよいでしょう。管理者として開いたコマンドプロンプトで次の4行のコマンドラインを実行します。なお、32ビットOSの場合は、3、4行目の実行は不要です。バッチファイルを作成しておくと（ngen.cmdなど）、コマンドラインを連続実行できて便利です。

```
C:¥Windows¥Microsoft.NET¥Framework¥v4.0.30319¥ngen.exe  executeQueuedItems ↲
C:¥Windows¥Microsoft.NET¥Framework¥v4.0.30319¥ngen.exe  update ↲
C:¥Windows¥Microsoft.NET¥Framework64¥v4.0.30319¥ngen.exe  executeQueuedItems ↲
C:¥Windows¥Microsoft.NET¥Framework64¥v4.0.30319¥ngen.exe  update ↲
```

タスクスケジューラの使いこなし

Windows標準のタスク機能を利用すると、さまざまなタイミング、条件に基づいて、管理操作を自動化することができます。タスクは［タスクスケジューラ］（Taskschd.msc）、Schtasks.exeコマンド、およびPowerShellのScheduledTasksモジュールのコマンドレット（Get-Command -module ScheduledTasksで確認可能）を使用して作成および管理できます。ここでは［タスクスケジューラ］（Taskschd.msc）と一部コマンドラインを利用した活用例を紹介します。

週末に再起動をスケジューリングする

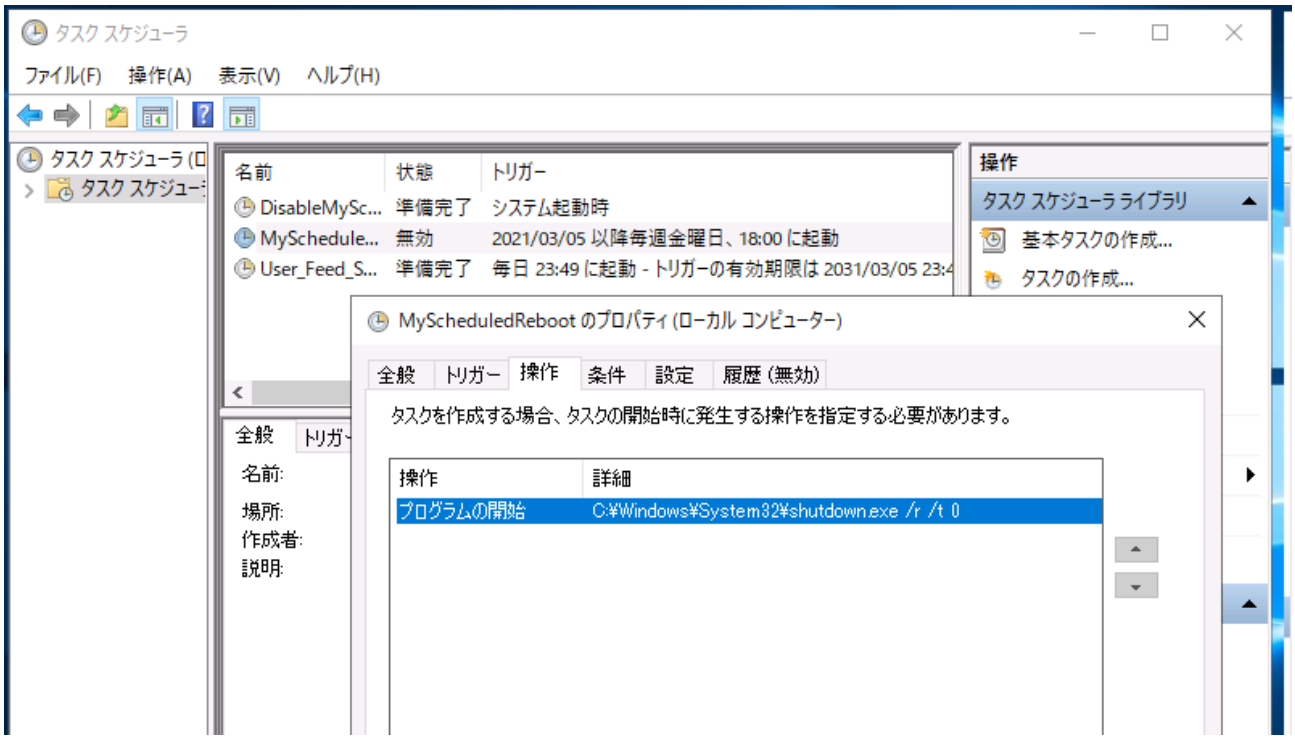
再起動保留状態の更新プログラムのインストールを完了させるため、サーバーで週末に再起動を実施するというシナリオを考えてみましょう。再起動は毎週必要なわけではなく、必要時にのみ簡単に再起動をスケジューリングすることにします。

［タスクスケジューラ］（Taskschd.msc）を起動し、次の2つのタスクを作成します（画面15、画面16）。MyScheduledRebootタスクは毎週土曜日の23:59にshutdown.exe /r /t 0コマンドを実行して再起動するタスクです。もう1つのDisableMyScheduledRebootタスクは、システム起動時にMyScheduledRebootタスクの状態を“無効”にセットするタスクです。

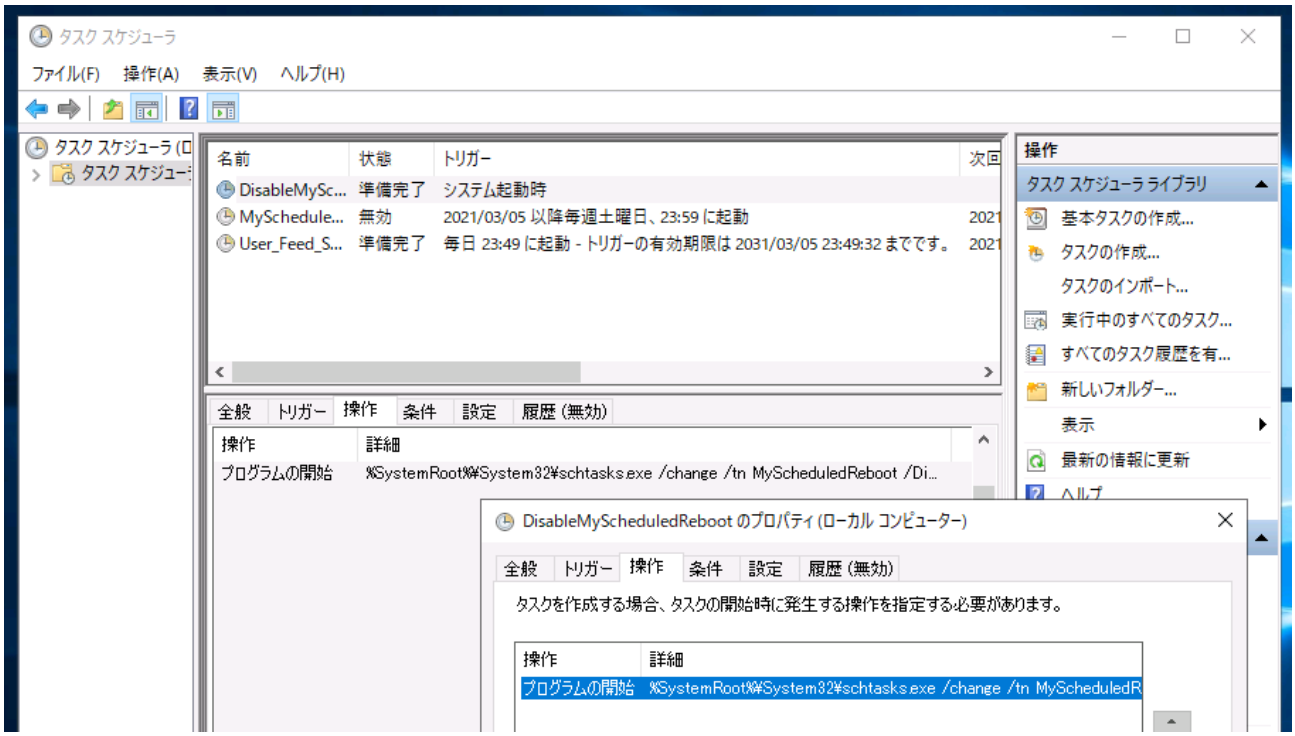
全般	名前	MyScheduledReboot
	セキュリティオプション	☑ユーザーがログオンしているかどうかにかかわらず実行する ☑最上位の特権で実行する
トリガー	タスクの開始	スケジュールに従う、毎週、土曜日、23:59
操作	操作	プログラムの開始
	プログラム/スクリプト	%SystemRoot%¥System32¥shutdown.exe または C:¥Windows¥System32¥shutdown.exe
	引数の追加	/r /t 0

全般	名前	DisableMyScheduledReboot
	セキュリティオプション	☑ユーザーがログオンしているかどうかにかかわらず実行する ☑最上位の特権で実行する
トリガー	タスクの開始	スタートアップ時（システム起動時）
操作	操作	プログラムの開始
	プログラム/スクリプト	%SystemRoot%¥System32¥schtasks.exe または C:¥Windows¥System32¥schtasks.exe
	引数の追加	/change /tn MyScheduledReboot /Disable

2つのタスクを作成したら、“準備完了”状態になっているMyScheduledTaskタスクを右クリックして［無効］を選択し、タスクを“無効”の状態に切り替えます。または、DisableMyScheduledRebootタスクを手動で一度実行します。



画面15　毎週末に再起動を実施するMyScheduledRebootタスクを作成し、“無効”状態にしておく



画面16　システム起動時にMyScheduledRebootタスクの状態を“無効”にセットするためのタスク

2つのタスクをこのように準備しておくことで、週末に再起動が必要な際に簡単かつすばやく再起動をスケジューリングできるようになります。PowerShellのEnable-ScheduledTaskコマンドレットまたはSchtasks.exeコマンドを次のように実行することで、MyScheduledRebootタスクが“準備完了”の状態にセットされます。すると、その週の週末に再起動が自動実行されます。そして、再起動後はDisableMyScheduledRebootタスクによって再びMyScheduledRebootタスクは“無効”の状態に戻ります。

> Enable-ScheduledTask -TaskName MyScheduledReboot ↲

または

> Schtasks.exe /change /tn MyScheduledReboot /Enable ↲

PowerShellコマンドのスケジューリング

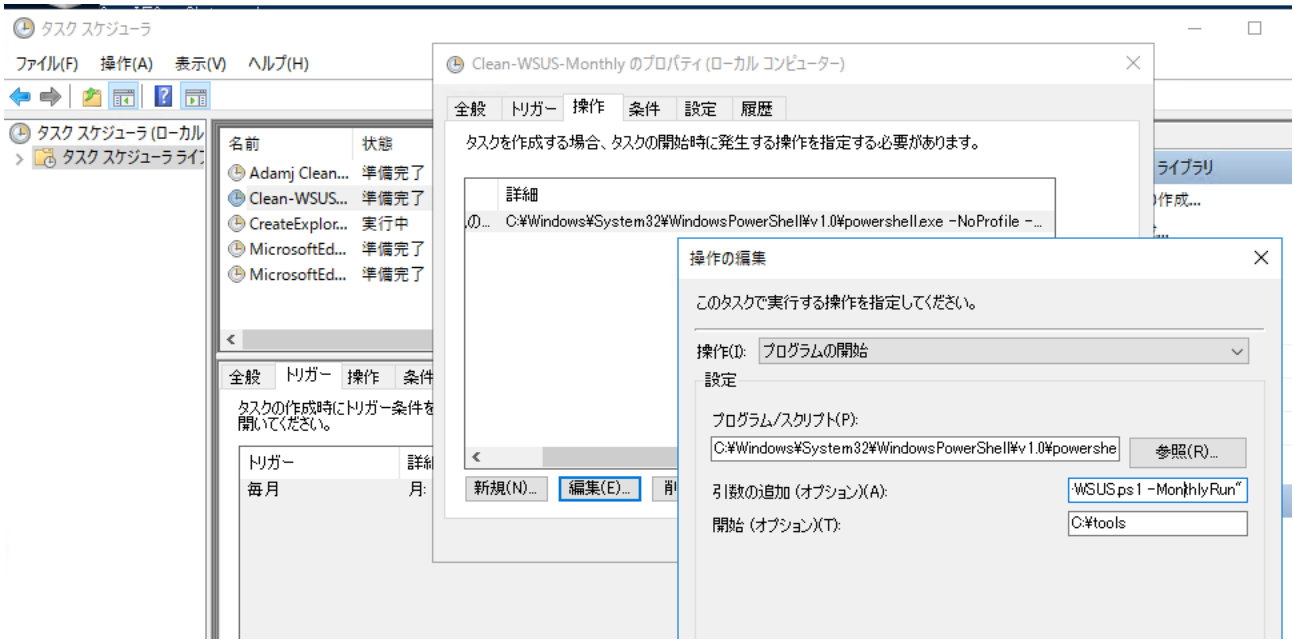
タスクの［プログラムの開始］操作にPowerShellコマンドレットのコマンドラインを指定したい場合は、次のように設定します。先ほどのDisableMyScheduledRebootタスクの［プログラムの開始］操作は、この方法で**<PowerShellのコマンドライン>**の部分に**Disable-ScheduledTask -TaskName MyScheduledReboot**と指定することで構成することもできます。

操作	操作	プログラムの開始
	プログラム/スクリプト	%SystemRoot%¥System32¥WindowsPowerShell¥v1.0¥powershell.exe または C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe
	引数の追加	-Command "<PowerShellのコマンドライン>" または -Command "& {<PowerShellのコマンドライン>}"
	開始	コマンドラインの実行を開始するカレントディレクトリ、省略すると%SystemRoot%¥System32

PowerShellスクリプト（.ps1）のスケジューリング

タスクの［プログラムの開始］操作にPowerShellのスクリプト（.ps1）をパラメーター付きで指定したい場合は、次のように設定します。スクリプトの実行ポリシーの現在の設定に関係なく、確実にスクリプトを実行させることが可能です（画面17）。スクリプトのパスには、［開始］に指定した場所からの相対パス（例： .¥script.ps1）で記述することもできます。

操作	操作	プログラムの開始
	プログラム/スクリプト	%SystemRoot%¥System32¥WindowsPowerShell¥v1.0¥powershell.exe または C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe
	引数の追加	-NoProfile -ExecutionPolicy unrestricted -Command "<.ps1ファイルのパス> <スクリプトに渡すパラメーター>" または -NoProfile -ExecutionPolicy unrestricted -Command "& {<.ps1ファイルのパス> <スクリプトに渡すパラメーター>}"
	開始	スクリプトの実行を開始するパス、省略すると%SystemRoot%¥System32



画面17　PowerShellスクリプト（.ps1）をタスクで実行させる場合の設定

Windowsファイアウォールの健全性チェック

WindowsおよびWindows Serverでは、エンドポイントのファイアウォール機能として［Windows Defenderファイアウォール］（旧称、Windowsファイアウォール）が既定で有効になっており、送受信トラフィックの許可／禁止を制御しています。Windows Defenderファイアウォールは不要な、あるいは許可されていないネットワークトラフィックをブロックすることで攻撃面を縮小することが主な目的です。Windows Defenderファイアウォールが適切に構成されていないと、セキュリティを低下につながるばかりか、パフォーマンスに影響することもあります。

ネットワークの場所とファイアウォールプロファイルの関係

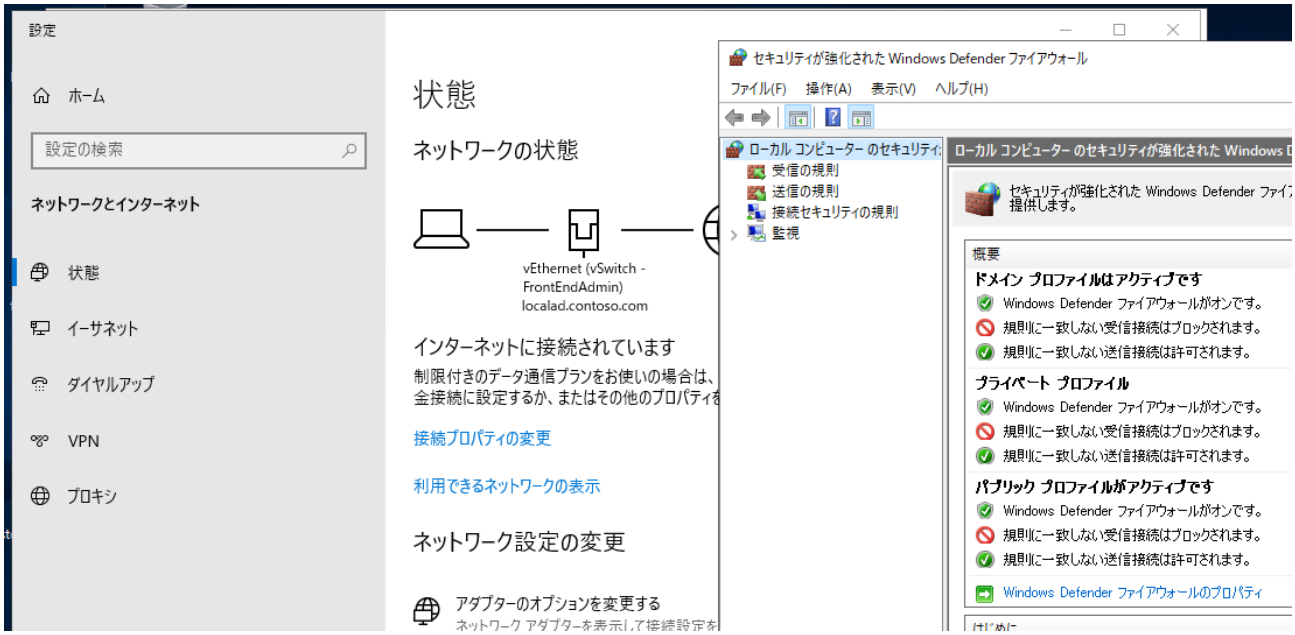
コンピューターにインストールされている物理ネットワークアダプターには、アダプターごとに**ネットワークプロファイル（ネットワーク接続プロファイル）**が関連付けられます。

Windowsは新しいネットワーク接続を検出すると、それを識別し、ネットワークの場所（Network Category）を**パブリックネットワーク（Public）**または**プライベートネットワーク（Private）**に設定します。既定ではパブリックに設定しようとしますが、ユーザーに対してプライベートネットワークに切り替えるか問い合わせますし、後から［設定］アプリの［ネットワークとインターネット］のGUIで変更することもできます。プライベートに設定されたネットワークがActive Directoryドメインとして認証されると（コンピューターがドメインメンバーである場合）、ネットワークの場所を**ドメインネットワーク（DomainAuthenticated）**に設定します。デフォルトゲートウェイが存在せず、インターネット接続を確認できない接続については、**識別されていないネットワーク**として**パブリックネットワーク（Public）**が設定されます。

一方、Windows Defenderファイアウォールには、**パブリック（Public）**、**プライベート（Private）**、**ドメイン（Domain）**の3つの**ファイアウォールプロファイル**が存在します。**パブリック（Public）**は信頼できないネットワーク接続に対して最小限の通信を許可するファイアウォールルールが、**プライベート（Private）**にはLAN（ローカルエリアネットワーク）上でさまざまなネットワーク機能（ファイルとプリンター共有など）を可能にする緩和されたファイアウォールルールが、**ドメイン（Domain）**にはActive Directoryドメインのネットワーク機能に不可欠なファイアウォールルールが定義されています。

そして、**ネットワークプロファイル**の**パブリックネットワーク（Public）**、**プライベートネットワーク（Private）**、**ドメインネットワーク（DomainAUthenticated）**の設定には、**パブリック（Public）**、**プライベート（Private）**、**ドメイン（Domain）**の**ファイアウォールプロファイル**が適用され、それぞれにファイアウォールのルールが適用されることになります。

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の場合、現在のネットワークの識別状態は、［設定］アプリの［ネットワークとインターネット］、およびコントロールパネルの［ネットワークと共有センター］で確認することができます。また、Windows Defenderファイアウォールの状態は［セキュリティが強化されたWindows Defenderファイアウォール］（WF.msc）スナップインで確認することができます。ネットワークを安全な状態を維持するためには、最低限、ネットワークの場所が適切に識別されており、対応するファイアウォールプロファイルが有効になっていることが重要です。



画面1　ネットワークの識別と対応するファイアウォールプロファイルが有効になっていることを確認する

コマンドラインによるプロファイルの確認と変更

物理ネットワークアダプターが共有タイプのHyper-V仮想スイッチとして使用されている場合や、ドメインネットワークとして識別されている場合など、Windows標準のGUIでは**ネットワークプロファイル**の**パブリック（Public）**と**プライベート（Private）**を切り替える場所がなくなります（画面2、注：**ドメインネットワーク（DomainAUthenticated）**として識別されているのであればネットワークの識別は適切です）。Windows ServerのServer Coreはもともと GUIを提供しません。*1

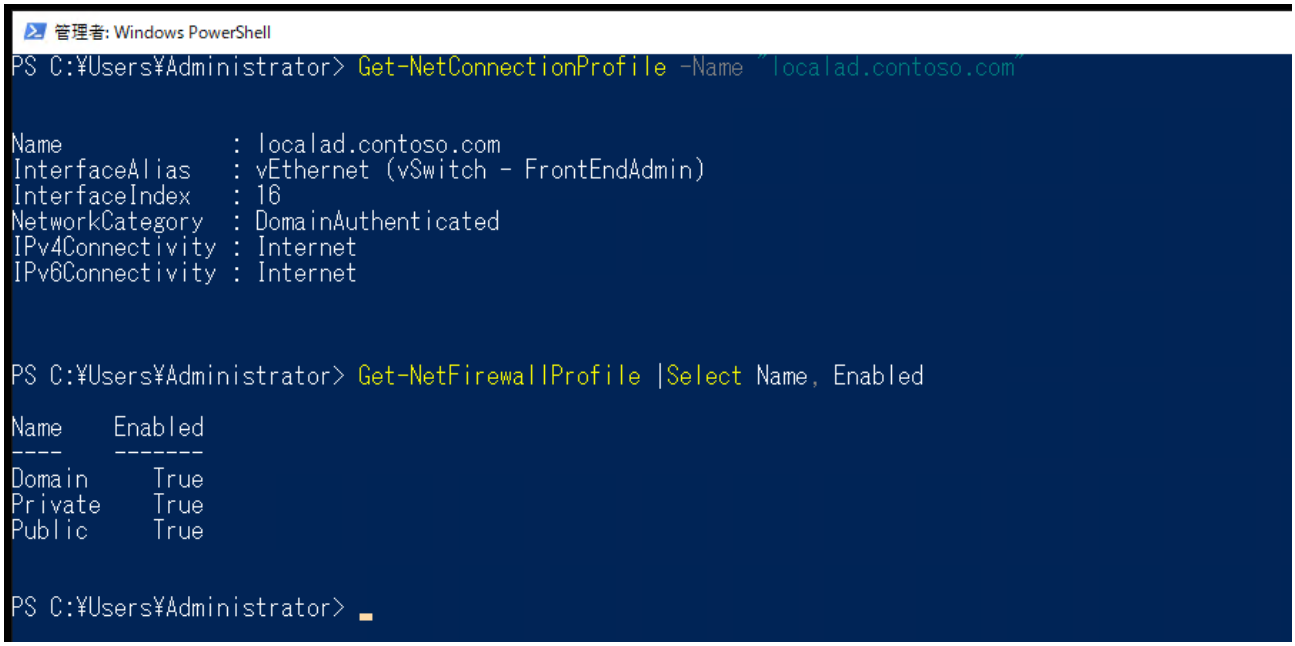


画面2　同じコンピューターでHyper-V仮想スイッチを作成する前（画面左）と作成した後（画面右）

*1　Windows Server 2019/2018以降はServer Coreアプリ互換性FoDをインストールすることで、［セキュリティが強化されたWindows Defenderファイアウォール］（WF.msc）スナップインを含む一部の管理ツールを利用可能ですが、ネットワークプロファイルの確認や切り替えのためのGUIはありません。

現在の**ネットワークプロファイル**における**ネットワークの場所（Network Category）**の識別と、**ファイアウォールプロファイル**の状態をコマンドラインで確認には、PowerShellのGet-NetConnectionProfileおよびGet-NetFirwewallProfileコマンドレット（↲ は Enter キーまたは改行位置、以下同じ*2）を利用できます（画面3）。

> Get-NetConnectionProfile ↲
>
> Get-NetFirewallProfile ↲



画面3　Get-NetConnectionProfileとGet-NetFirewallProfileで現在の状態を確認する

ネットワークの場所（NeworkCategory）が適切でない場合は、Set-NetConnectionProfileコマンドレットを次のように実行することで適切なものに切り替えることが可能です（画面4）。-Nameパラメーターの他、-InterfaceAliasや-InterfaceIndexパラメーターでネットワーク接続を指定することもできます。

> Set-NetConnectionProfile -Network "<ネットワーク名>" -NetworkCategory PublicまたはPrivateまたはDomainAuthenticated ↲



画面4　Set-NetConnectionProfileでネットワークの場所をパブリックからプライベートに切り替える

ファイアウォールのルールが肥大化していないか

Windows Defenderファイアウォールには既定のファイアウォールルールが定義済みとなっており、既定で有効になっているもの、Windows Serverのサーバーの役割や機能の有効化、WindowsやWindows Serverのリモート管理の設定やリモートデスクトップ接続の設定によって自動で有効化されるもの、サーバーアプリケーションやデスクトップアプリケーション、ストアアプリ（ユニバーサルWindowsプラットフォームアプリ、UWPアプリ）のインストールや使用によって自動またはユーザーの許可により追加されるものがあります。

Windows Server 2019のインストール直後の状態で確認すると、デスクトップエクスペリエンスで104、Server Coreで55のファイアウォールルールが有効でした。Windows 10 Enterpriseバージョン20H2のインストール直後の状態で確認すると、202のファイアウォールルールが有効でした。

ファイアウォールルールはレジストリに格納されるため、ルールが肥大化すると、レジストリハイブも肥大化します。大きすぎるレジストリハイブは、システムの応答停止やエラー、パフォーマンスの低下など、さまざまな問題を引き起こす可能性があります。*3

*3　レジストリ64ビット版Windows XP SP2およびWindows Server 2003 SP2からレジストリハイブの最大サイズは2GBになりました。しかし、2GBを超えた場合に再起動できなくなる問題があり、Windows 8およびWindows Server 2012以降については更新プログラムによって最大4GBまで拡張されました（Computer cannot be restarted if the registry hives are larger than 2 GB https://support.microsoft.com/help/2978366）。Windows 10およびWindows Server 2016以降については最初から4GB（4095MB）です。現在のロードされているレジストリハイブのサイズと最大サイズは、PowerShellでGet-WmiObject Win32_registryを実行して確認できます。32ビット版Windowsにはより小さな上限が設定されます。

ルールの数に特に上限はなく、明確な基準を示すことはできませんが、異常な数のルール、あるいは同じ名称や似た名称のルールが大量に存在する場合は、早めに対処したほうがよいでしょう。ただし、Windowsに既定で用意されている定義済みのルールについては削除しないでください。

PowerShellで以下のコマンドラインを実行すると、現在、有効になっているファイアウォールルールの数を確認することができます。

```
(Get-NetFirewallRule | where {$_.Enabled -eq $true}).Count ↲
```

同じ名称のルールが重複して登録されている状況は、PowerShellで次のコマンドラインを実行することで、ルールの表示名でグループ化し、降順にソートして調査することができます。

```
Get-NetFirewallRule | Group-Object -Property DisplayName | Sort-Object -Property Count -Descending ↲
```

次に実際のルールの肥大化の例と対処方法を示します。肥大化したルールを安易に削除することはせず、ルールの詳細な設定を確認し、削除による影響をよく検討してください。また、できるだけ現在のルールをバックアップしてから対処しましょう。次のコマンドラインを実行すると、現在のルール設定をファイル（.wfw）にエクスポートしてバックアップ、およびインポートして復元することができます。［セキュリティが強化されたWindows Defenderファイアウォール］（WF.msc）スナップインでの［ポリシーのエクスポート］と［ポリシーのエクスポート］の操作と同じことをコマンドラインからすばやく実行する方法です。

```
Netsh advfirewall export <エクスポート先パス>¥ファイル名.wfw" ↲

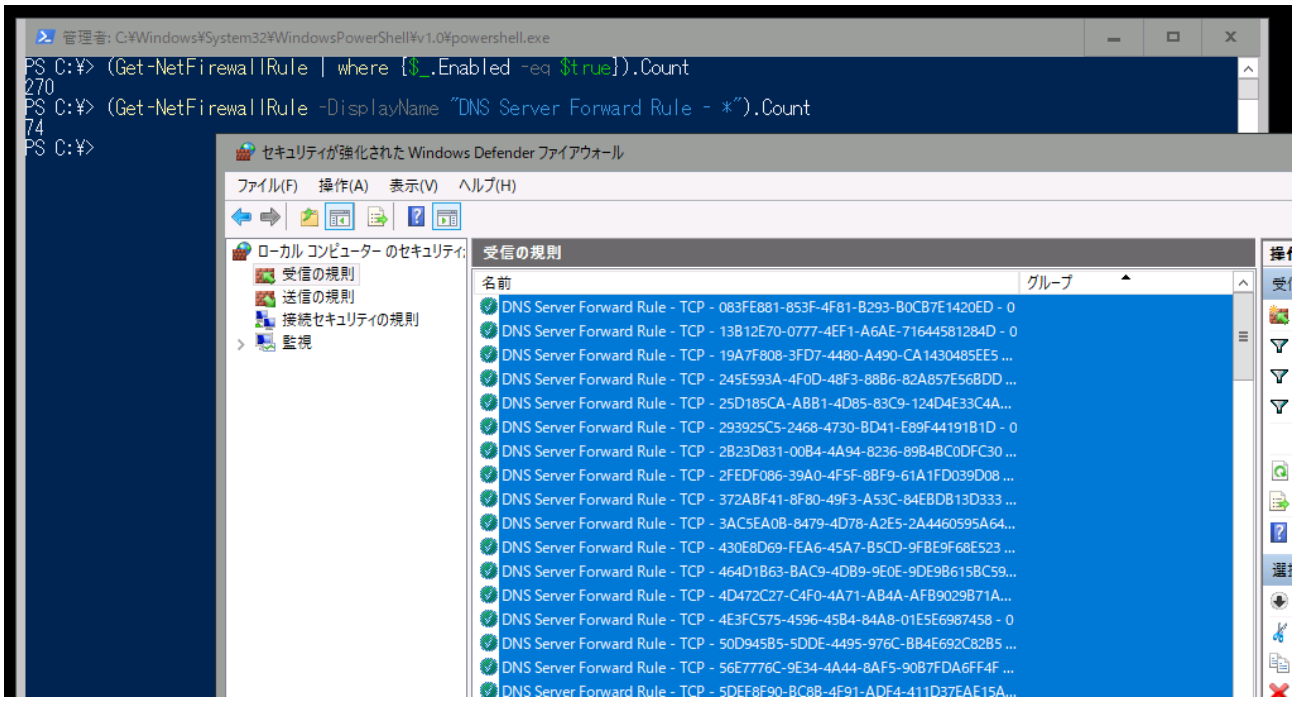
Netsh advfirewall import <エクスポート先パス>¥ファイル名.wfw" ↲
```

・事例1

Windows 10バージョン1809およびWindows Server 2019のHyper-Vホストやコンテナーホストでは、受信の規則に次のルールのペアが大量に登録されることを確認しています（画面5）。ルールの名前は完全に同一ではなく、GUID（XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX）の部分はペアごとに異なります。

DNS Server Forward Rule - TCP - GUID - 0

DNS Server Forward Rule - UDP - GUID - 0



画面5　Windows 10バージョン1809やWindows Server 2019のHyper-Vホストに大量に登録されるDNS Server Forward Rule。削除しても次回起動時に再登録されるので問題ない

この問題は、既定で作成されるDefault Switchという名前のHyper-V仮想スイッチが、ホストの起動のたびにリセットされることが原因と思われます。ルールの数が多くなっている場合は、以下のコマンドラインを実行して既に作成されているルールを削除し、コンピューターを再起動すると、新たなペアが自動的に登録されます。

```
Remove-NetFirewallRule -Displayname "DNS Server  Forward Rule -*" ↲

Restart-Computer ↲
```

なお、重複して登録される問題が解決されるわけではないので、定期的にルールをクリーンアップするとよいでしょう。Windows 10およびWindows Serverのより新しいバージョンでは、次のルール名が次のペアに変更され、極端に重複登録されることはなくなったようです。Windows 10の機能更新プログラムによるアップグレードを繰り返していると、過去に自動登録され、現在は利用されていないルールとして旧名称のルールが残っていることがあるかもしれません。

HNS Container Networking - ICS DNS (TCP-In) - GUID - 0

HNS Container Networking - DNS (UDP-In) - GUID - 0

・事例2

Mirantis Container Runtime（旧称、Docker Enterprise）のコンテナーホストでは受信の規則と送信の規則に、次の名前のルール（XXXXは数字）が大量に登録される場合があることを確認しています。これらのルールが存在しなくても、コンテナーのネットワーク機能に影響がないようなので、大量に登録されている場合は削除してもよいでしょう。

```
Get-NetFirewallRule -Displayname "docker*in" ↲

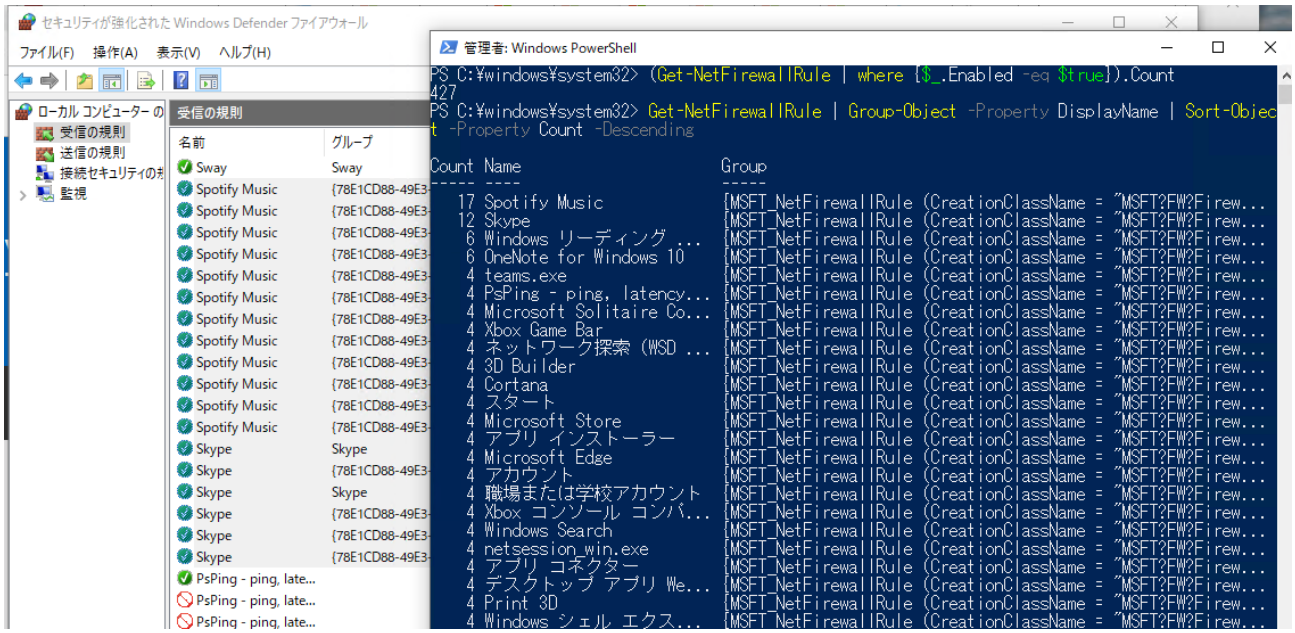
Get-NetFirewallRule -Displayname "docker*out" ↲

Remove-NetFirewallRule -Displayname "docker*in" ↲

Remove-NetFirewallRule -Displayname "docker*out" ↲
```

・事例3

Windows 10ではストアアプリ（UWPアプリ）のインストールや使用により、同じ名前のルールが重複して登録される場合があります。次の例は、Spotify MusicアプリとSkypeアプリのルールが重複して登録されている様子です。



画面6　重複登録されたSpotify MusicアプリとSkypeアプリのルール

実は、このコンピューターではこれらのアプリを使用したことがありません。使用しないアプリの登録を削除しても何の問題もないでしょう。また、削除したとしても必要時に自動的に再登録されるはずです。

Windows 10の機能更新プログラムによるアップグレードを繰り返していると、廃止やアンインストールなどで既に存在しないストアアプリのためのルールが残っている場合もあります。不要なストアアプリ用のルールは削除して問題ないでしょう。

・事例4

リモートデスクトップセッションホストであるWindows Server 2016、Windows Server 2019、および仮想デスクトップインフラストラクチャ（VDI）のWindows 10仮想デスクトップでは、移動ユーザープロファイルやユーザープロファイルディスクの問題で、ファイアウォールルールが肥大化し、デスクトップの機能不全（スタートメニューが開かないなど）、パフォーマンスの劣化、サーバーのハングアップなどの症状を引き起こすことが知られています。該当する場合は、以下の対処方法に従ってください。

Windows Server 2016 および 2019 における Windows ファイアウォール規則の肥大化について
https://jpwinsup.github.io/blog/2020/10/08/RemoteDesktopService/wnf-leak-issue-on-windows-server-2016-and-windows-server-2019/

重大障害につながるイベントログを見逃さない

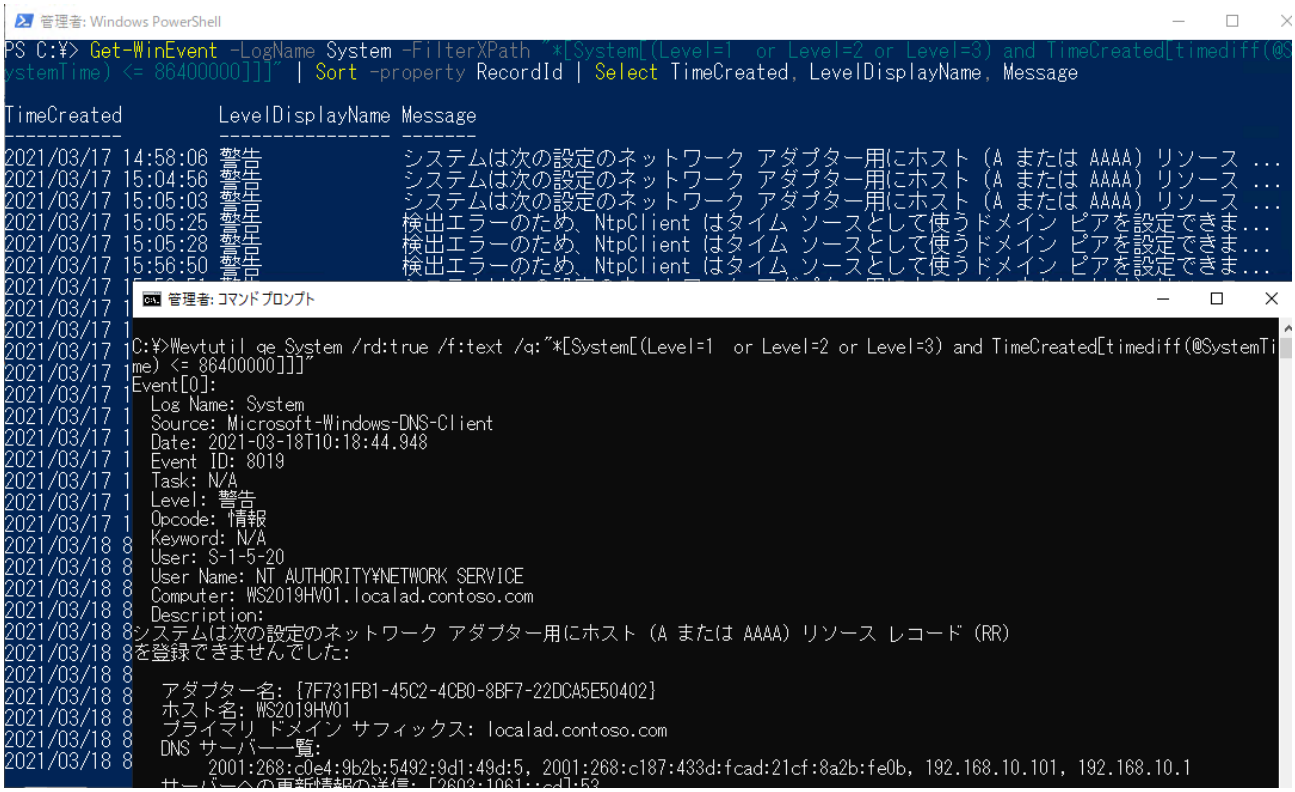
Windowsイベントログは、システムで発生するシステム、アプリケーション、セキュリティに関する膨大なイベントを記録し、提供するサービスです。Windowsイベントログを使用すると、ハードウェアの障害の予兆、容量不足、システムやアプリケーションの重大なエラー、セキュリティ侵害の痕跡などを調査することができます。Windowsに標準搭載されている［イベントビューアー］（Eventvwr.msc）スナップインを使用すると、イベントログを参照したり、フィルター条件を設定して効率的に調査したりできます。しかしながら、［イベントビューアー］（Eventvwr.msc）スナップインは現在進行中の問題を調査するのに快適なパフォーマンスを提供できるとは言えません。また、膨大なイベントに埋もれて、重大なイベントの発生を見逃してしまうこともあるでしょう。

過去24時間に発生した重大／エラー／警告イベントをすばやく確認する

WindowsはWindowsイベントログにコマンドラインからアクセスする複数の方法を用意しています。その中で共通のフィルター条件で利用できるPowerShellのGet-WinEventコマンドレットとWevtutilコマンドの2つを紹介します。

次のコマンドラインの例はいずれも、過去24時間（86400000ミリ秒）にシステム（System）ログに記録された、警告レベル以上のイベント、すなわち警告（レベル3）、エラー（レベル2）、重大（レベル1）イベントをフィルターし、記録された順番に出力するものです（画面9）。

> Get-WinEvent -LogName System -FilterXPath "*[System[(Level=1 or Level=2 or Level=3) and TimeCreated[timediff(@SystemTime) <= 86400000]]]" | Sort -property RecordId | Select TimeCreated, LevelDisplayName, Message ↲
>
> または
>
> Wevtutil qe System /rd:true /f:text /q:"*[System[(Level=1 or Level=2 or Level=3) and TimeCreated[timediff(@SystemTime) <= 86400000]]]" ↲

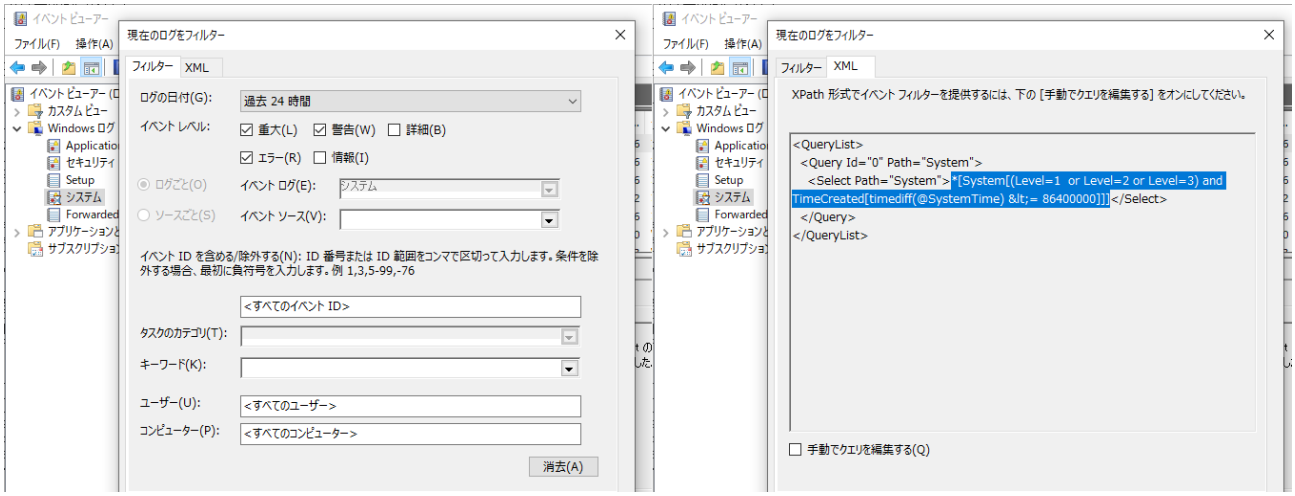


画面9　過去24時間に発生した警告レベル以上のイベントを確認する

構造化（XPath）クエリ式の簡単な作り方

Get-WinEventコマンドレットとWevtutilコマンドはどちらも、構造化（XPath）クエリ式でフィルター条件を設定します。クエリ式を作成するのが難しそうと思うかもしれませんが、実は非常に簡単です。

［イベントビューアー］（Eventvwr.msc）スナップインを開いて、目的のログを選択し、［現在のログをフィルター…］をクリックします。［フィルター］タブのGUIでフィルター条件を設定したら、［XML］タブに切り替えます。すると、<Select>セクション内に目的のクエリ式が見つかります。なお、クエリの中にXMLの中でエスケープされている>と<が含まれる場合は、それぞれ>と<に置き換えて使用してください。目的のクエリ式を取り出したら、フィルター設定は破棄してかまいません。



画面10　GUIでフィルター条件を設定すると、XPathクエリが完成する

システムやアプリケーションの重大／エラー／警告イベントをリアルタイムに監視する

現在進行中の問題をリアルタイムに追跡したい、あるいは再現テストをしながらのイベント発生をリアルタイムに監視したいという場合は、PowerShellで簡単なスクリプトを書くことで対応できます。例えば、次のコードは、過去1時間（3600000ミリ秒）にシステムログに記録された警告以上のイベントがあればそれを出力し、その後、10秒間隔で新たに記録される警告以上のイベントを出力し続けます。-LogNameパラメーターのSystemをApplicationに書き換えることで、アプリケーションログに対応させることができます（画面10）。

```
$lastRecordId = 0 ↲

while ($true) { ↲

$events = Get-WinEvent -LogName System -FilterXpath "*[System[(Level=1 or Level=2 or
Level=3) and TimeCreated[timediff(@SystemTime) <= 3600000]]]" -ErrorAction
SilentlyContinue | Sort -property RecordId ↲

if ($events.Count -ne 0) { ↲

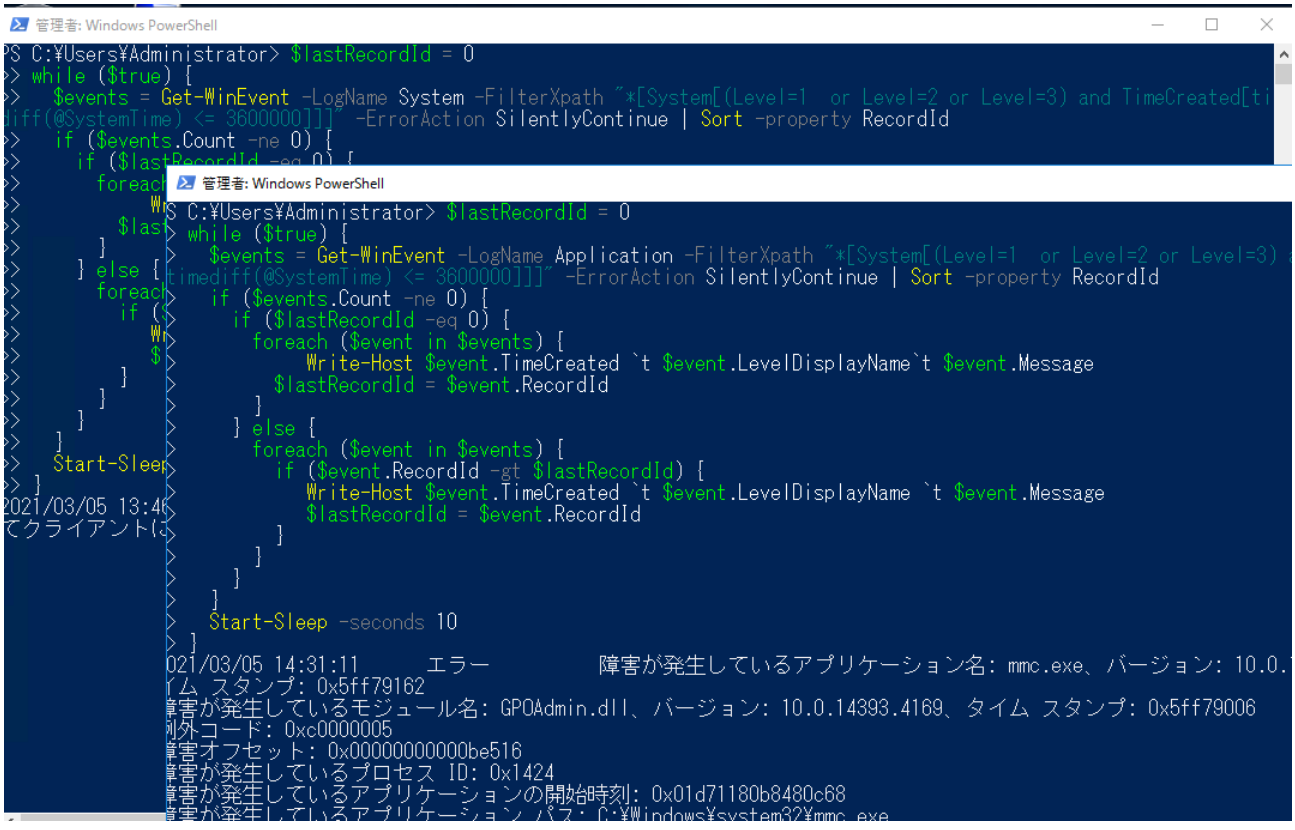
    if ($lastRecordId -eq 0) { ↲

        foreach ($event in $events) { ↲

            Write-Host $event.TimeCreated t $event.LevelDisplayNamet $event.Message ↲

            $lastRecordId = $event.RecordId ↲
```

```
    } ↲
} else { ↲
    foreach ($event in $events) { ↲
        if ($event.RecordId -gt $lastRecordId) { ↲
            Write-Host $event.TimeCreated t $event.LevelDisplayNamet $event.Message ↲
            $lastRecordId = $event.RecordId ↲
        } ↲
    } ↲
} ↲
Start-Sleep -seconds 10 ↲
} ↲
```



画面11　システムとアプリケーションログの警告以上のイベント発生をリアルタイムに監視する

Sysmonで詳細なアクティビティを徹底的にログに記録し、調査する

マイクロソフトが無料提供しているWindows Sysinternalsは、WindowsおよびWindows Serverのシステムを高度に監視、診断、およびトラブルシューティングするのに役立つユーティリティ群です。Windowsイベントログ関連のユーティリティとしては、System Monitor（Sysmon）があります。

Sysmonは、個々のコンピューターやネットワーク上の、潜在的で悪質なアクティビティを追跡するために作成されたものですが、悪質なアクティビティだけでなく、トラブルシューティングの目的にも使用できます。

SysmonはWindows SysinternalsのサイトからZIP（sysmon.ziip）としてダウンロードできるほか、Live Sysinternalsのサイトから実行可能ファイル（sysmon.exe）を直接ダウンロードすることもできます。

Windows Sysinternals | Sysmon
https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Live Sysinternals
https://live.sysinternals.com/sysmon.exe

Sysmonは多数のルールを用いて、表2に示すイベントを検出します。Sysmonが検出したアクティビティはイベントログ（Microsoft-Windows-Sysmon/Operations）に記録され、［イベントビューアー］（Eventvwr.msc）スナップインやその他の標準的なコマンドラインツールから参照できます。

表2　Sysmonのルールと検出可能なイベント（Sysmon v13.02、SchemaVersion 4.50の場合）

ルール名	イベント	イベントID	既定	説明
ProcessCreate	Process Create	1	include	プロセスの作成
FileCreateTime	File creation time changed	2		ファイル作成日時の変更
NetworkConnect	Network connection detected	3		ネットワーク接続の検出
ProcessTerminate	Process terminated	5	include	プロセス終了
DriverLoad	Driver loaded	6		ドライバーの読み込み
ImageLoad	Image loaded	7		実行可能イメージの読み込み
CreateRemoteThread	CreateRemoteThread detected	8		リモートスレッド作成の検出
RawAccessRead	RawAccessRead detected	9		RAWリードアクセスの検出
ProcessAccess	Process accessed	10		別のプロセスからアクセスの検出
FileCreate	File created	11	exclude	ファイルの作成、上書き検出
RegistryEvent	Registry object added or deleted	12	exclude	レジストリの作成、削除の検出

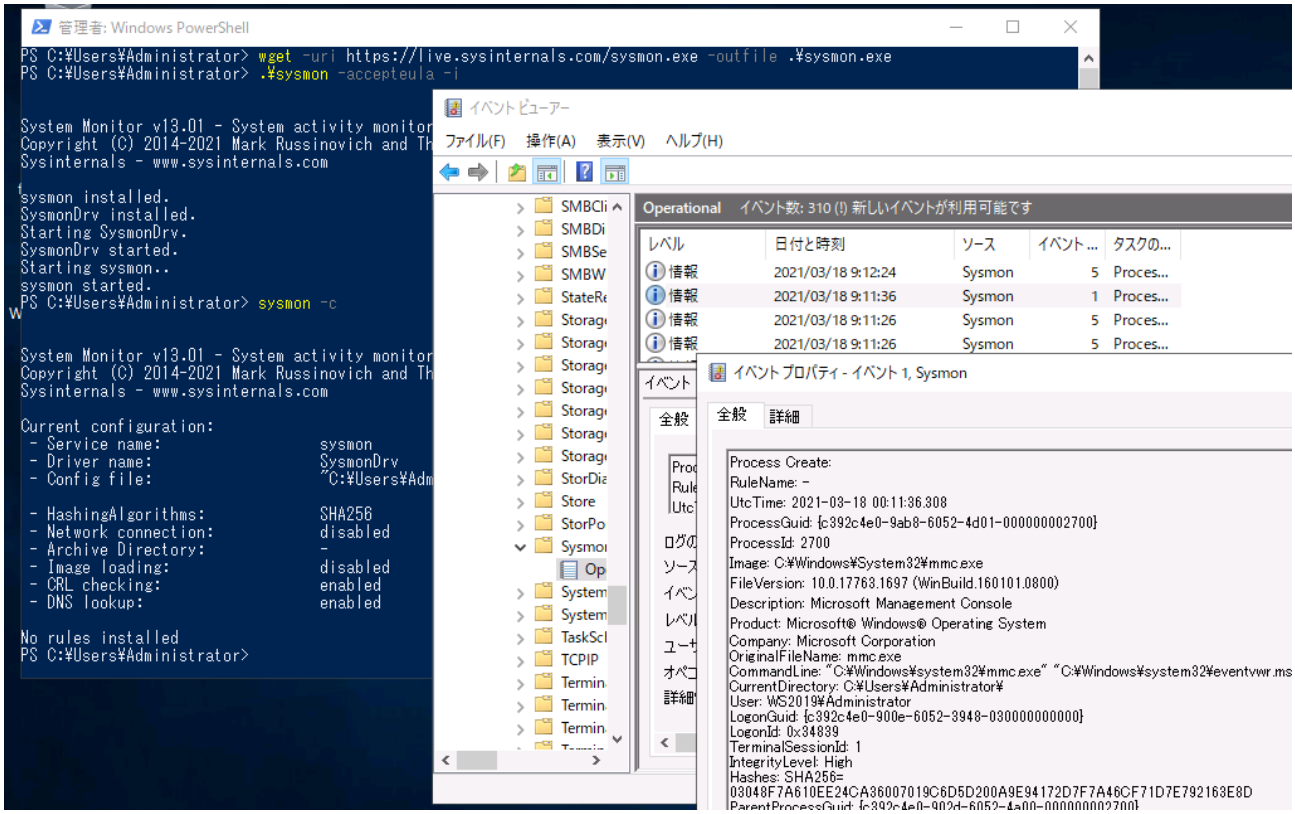
ルール名	イベント	イベントID	既定	説明
	Registry value set	13	exclude	レジストリ値の設定の検出
	Registry object renamed	14	exclude	レジストリのリネーム検出
FileCreateStreamHash	File stream created	15	exclude	ファイルストリームの作成検出
PipeEvent	Pipe Created	17	exclude	名前付きパイプの作成検出
	Pipe Connected	18	exclude	名前付きパイプへの接続検出
WmiEvent	WmiEventFilter activity detected	19	exclude	WMIイベントフィルター登録の検出、マルウェアの挙動の可能性あり
	WmiEventConsumer activity detected	20	exclude	WMIコンシューマーの登録検出
	WmiEventConsumerToFilter activity detected	21	exclude	WMIコンシューマーのフィルターバンドの検出
DnsQuery	Dns query	22	exclude	DNSクエリの検出
FileDelete	File Delete	23		ファイルの削除検出
ClipboardChange	Clipboard changed	24		RDP接続でクリップボード共有を検出
ProcessTampering	Process Tampering	25		プロセスのイメージの外部からの変更の検出
–	Sysmon service state changed	4	–	Sysmonサービスの状態変更（開始、停止）の検出
–	Sysmon config state changed	16	–	Sysmon構成の変更の検出、フィルタールールの更新など
–	Error report	255	–	Sysmonのエラーの検出

インストールなしで利用できるWindows Sysinternalsの大多数のユーティリティとは異なり、Sysmonはシステムにインストールすることでサービスとして動作し、システムの起動直後からシャットダウンまで、長期にわたって（Sysmonをアンインストールするまで）監視を継続します。Sysmonは構成によっては膨大なイベントを記録し続けるため、フィルター条件を設定して、短期間に集中的に監視することをお勧めします。

Sysmonをインストールするには-iパラメーターを指定して管理者として実行します。すると既定の構成でインストールされ、監視がスタートします。既定の構成では、表2のincludeとなっているプロセスの作成と終了イベント、およびSysmon関連のイベントです。また、ネットワーク接続の検出とイメージの読み込みイベントの監視機能は無効化されます。Sysmonのインストール後、-cパラメーターを指定して実行すると、現在の構成をダンプ出力できます（画面12）。

```
sysmon.exe -acceteula -i ↲

sysmon -c
```



画面12　Sysmonを既定の構成でインストールし監視をスタート。既定の構成では、すべてのプロセスの作成と終了がログに記録される

Sysmonによる監視を停止するには-uパラメーターを指定して実行してSysmonをアンインストールします。アンインストールすると記録済みのイベントログを解釈できなくなります。アンインストール後もイベントログを参照するためには-mパラメーターを指定して実行し、ログの解釈に必要なイベントマニュフェストのみをインストールします。

```
sysmon -u ↲

sysmon -m ↲
```

特定のプロセスに対象を絞って、イメージの読み込みイベント、およびネットワーク接続（TCP/UDPポートへの接続）イベントを含めて監視するには、次のようなコマンドラインでインストールします。既にSysmonをインストールしてある場合は、いったんアンインストールしてから、再インストールしてください。次の例は、app.exeというプロセスに関連するイベントのみをログに記録します。複数のプロセスを指定する場合は、app.exe, app2.exeのようにカンマで区切って指定してください。

```
sysmon.exe -accepteula -i -l -n app.exe ↲
```

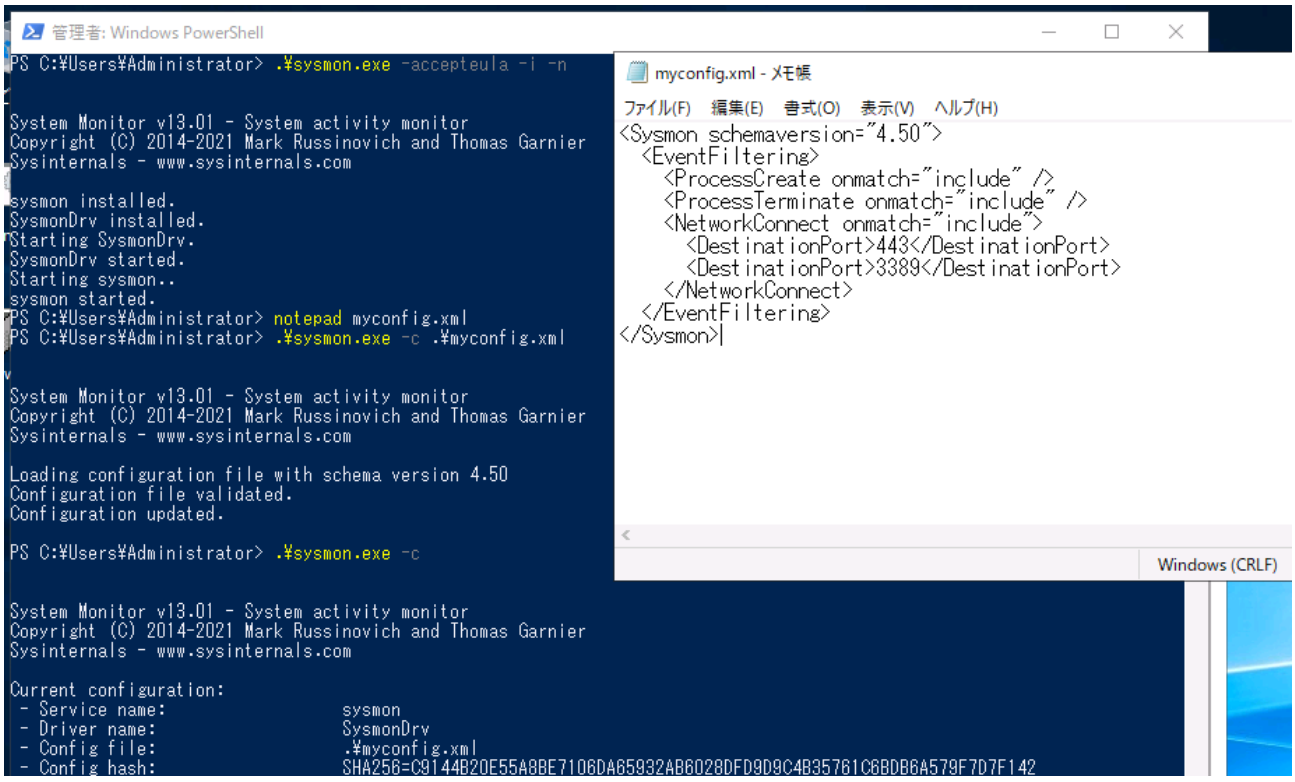
SysmonはXML構成ファイルを使用して複雑なフィルター条件を設定できます。例えば、HTTPS（443）およびRDP（3389）へのネットワーク接続のみを検出させたい場合は、次のようなmyconfig.xmlファイルを記述し、Sysmonをネットワーク接続イベントの検出を有効（-nパラメーター）にしてインストールしたあと、-cパラメーターを付けてXML構成ファイルを読み込ませます（画面13、画面14）。

```
sysmon.exe -accepteula -i -n ↲

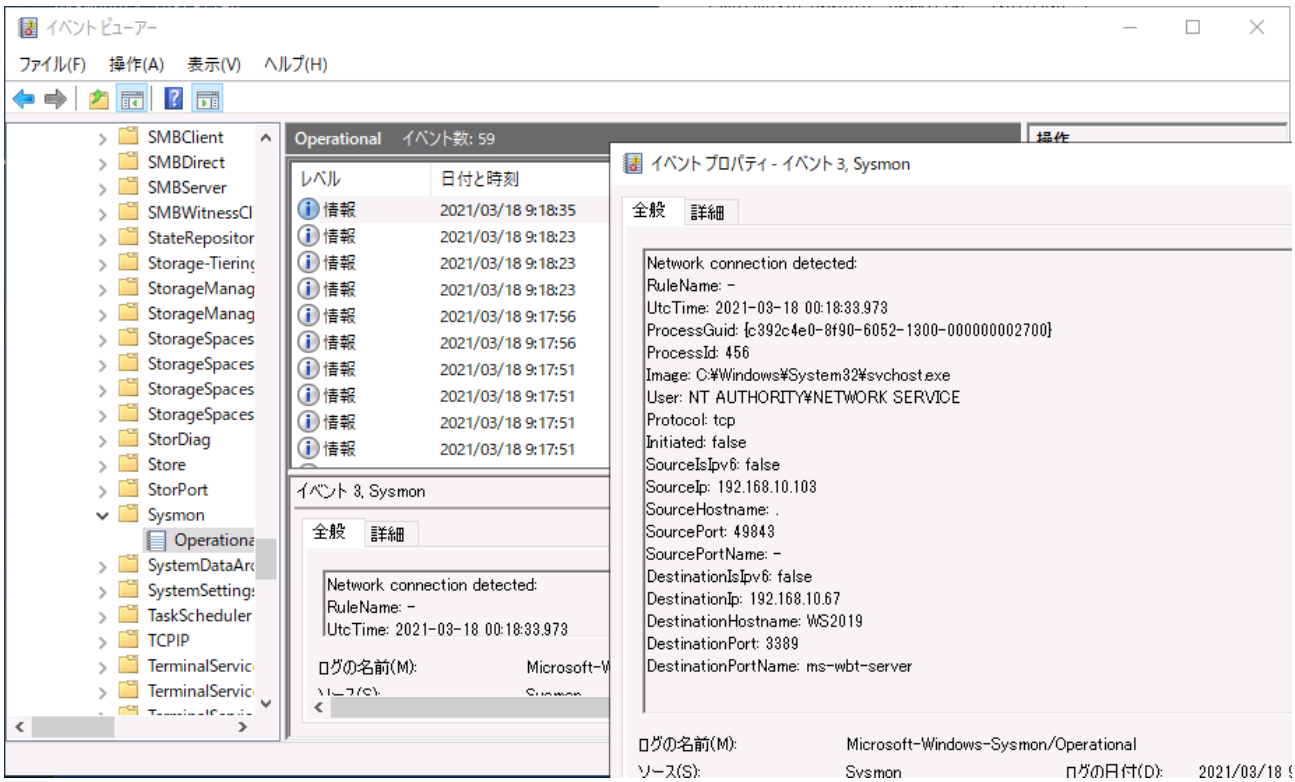
sysmon -c myconfig.xml
```

myconfig.xml
※SchemaVersionはSysmonのバージョンによって更新されることがあります。適切なSchemaVersionはSysmon -sを実行して確認、変更してください。

```
<Sysmon schemaversion="4.50"> ↲
<EventFiltering> ↲
<ProcessCreate onmatch="include" /> ↲
<ProcessTerminate onmatch="include" /> ↲
<NetworkConnect onmatch="include"> ↲
<DestinationPort>443</DestinationPort> ↲
<DestinationPort>3389</DestinationPort> ↲
</NetworkConnect> ↲
</EventFiltering> ↲
</Sysmon> ↲
```



画面13　XML構成ファイルを使用してSysmonをインストール、構成する



画面14　Sysmonを使用してHTTPS（443）およびRDP（3389）ポートへの着信を監視する

Sysmonをうまく使いこなすことで、知りたい情報に絞って効率よく監視することができます。しかし、複雑な条件を設定するのは難しいかもしれません。Sysmonのダウンロードサイトにある使用例や、以下の書籍の解説が参考になるでしょう。ただし、現在利用できるバージョンは、さらに機能が拡充されており、使用方法のすべてが説明されているわけではないことに留意してください。

Windows Sysinternals徹底解説 改訂新版（日経BP社）
https://www.nikkeibp.co.jp/atclpubmkt/book/17/P98960/

突然調子がおかしくなった!? そんなとき頼りになる信頼性モニター

Windowsの標準ツールである信頼性モニターは、システムのパフォーマンスと信頼性に影響する可能性があるエラーや警告イベント、およびアプリケーションのインストールなどの情報イベントの発生状況に基づいて、システムの安定性を日別（過去20日）または週別（過去20週）に1～10の安定性インデックス（インデックス10が最も安定）で評価します。最近、システムの調子が悪い、あるいはあるタイミングで突然、エラーが多発するようになったという場合、信頼性モニターを利用することでトラブルの予兆や原因に迫ることができます。

信頼性モニターを起動するには

信頼性モニターはWindows 10以降レガシな扱いとなったコントロールパネルの深い場所にあるため、信頼性モニターの存在すら知らず、利用したことがないというユーザーも多いようです。

信頼性モニターにアクセスするには、コントロールパネル（Control.exe）の［システムとセキュリティ¥セキュリティとメンテナンス］（Windows Server 2012 R2以前は［システムとセキュリティ¥アクションセンター］）を開き、［メンテナンス］の項目に含まれる［信頼性履歴の表示］をクリックします（画面15）。



画面15　WindowsやWindows Serverで利用できる信頼性モニターの安定性のレポート

信頼性モニターが初めて搭載されたWindows VistaおよびWindows Server 2008（フルインストール）ではパフォーマンスモニター（信頼性とパフォーマンスモニター）の機能の一部として提供され、コントロールパネルには含まれていませんでした。その名残というわけではありませんが、パフォーマンスモニターのコマンド（Perfmon.exe）に/rel（信頼性を示す**Rel**iavilityの略）パラメーターを指定して実行すると、すばやく信頼性モニターを開くことができます。また、［パフォーマンスモニター］（Perfmon.msc）スナップインを開き［モニターツール］を右クリックして［システム信頼性の表示］をクリックすることで開くこともできます。

> Perfmon /rel ↵

Windows Server 2012 R2以前のレガシなWindows Serverバージョンでは、信頼性モニターに何も記録されない場合があります。以下のサポート情報の解決策に従って対処することで、信頼性モニターによる評価を開始することができます（過去に発生したイベントや安定性インデックスは作成されません）。

Reliability Monitor displays no information in Windows Server
https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/reliability-monitor-shows-no-information

トラブルシューティング事例

信頼性モニターを使用したトラブルシューティング事例を紹介します。

先日、私はWindows 10にインストールしたWindows Admin Centerを利用して、複数台のWindows Serverをリモート管理していました。ふと、ローカルのWindows 10の管理画面はどうなっているのだろうと接続先を切り替えようとしたところ、ローカルのWindows 10にだけ応答なしになったり、エラーで接続できなくなっていることに気付きました（画面16）。数時間前までは確かに問題なく接続できていました。



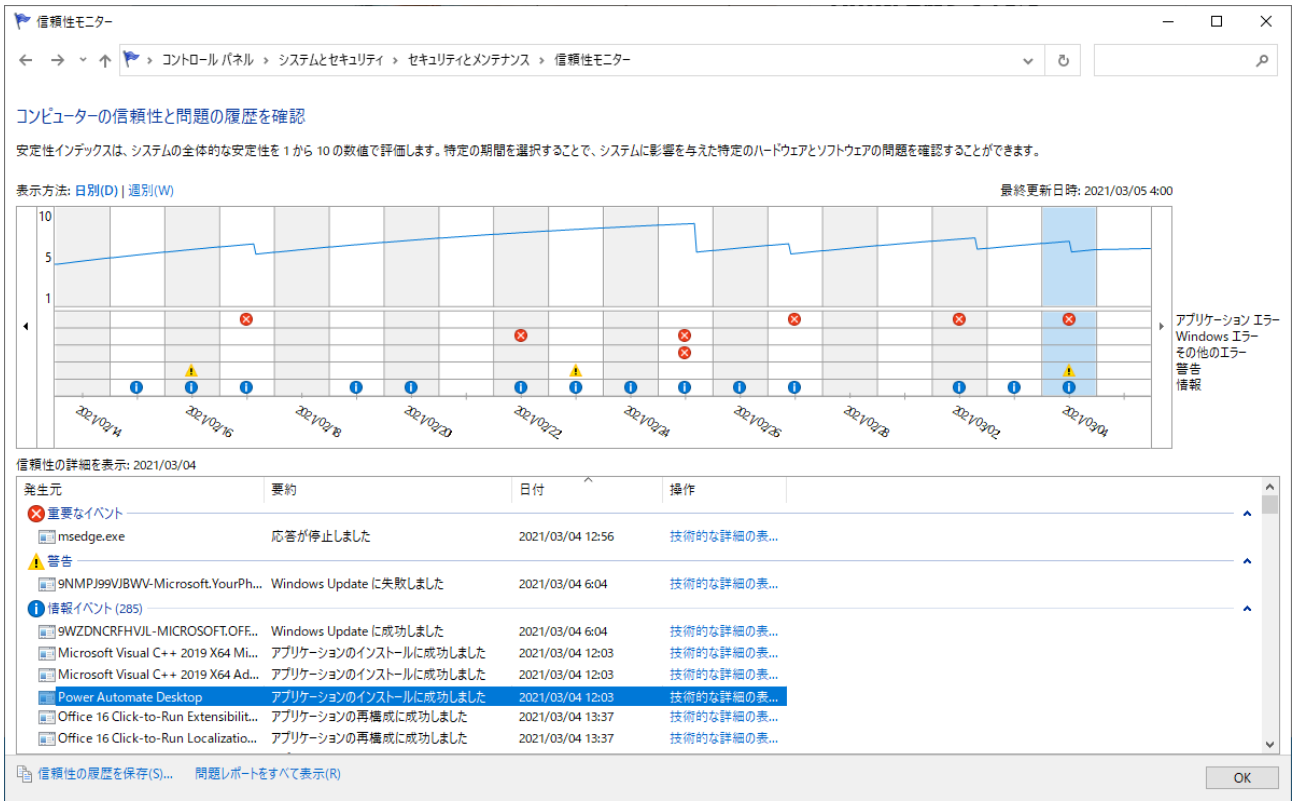
画面16　Windows 10にインストールしたWindows Admin Centerで、ある日、どこかのタイミングで突然、ローカルのWindows 10にだけ接続できなくなった

思い当たることがあるとすれば、このエラーが発生する少し前、マイクロソフトが無料公開したばかりの、あるデスクトップアプリケーションをインストールしたことです。しかし、それが直接的な原因かどうかは定かではありませんし、インストールした時間まで正確には覚えていません。

そこで、信頼性モニターを開いてここ数時間のイベントを確認してみました。すると、Windows Admin Centerを開いていたMicrosoft Edgeで応答なしのエラーが発生するまでの1時間の間に、疑っていたアプリケーション（Power Automate Desktop）とその関連コンポーネント（Microsoft Visual C++ 2019 Runtime）インストールが情報イベントとして記録されていました（画面17）。

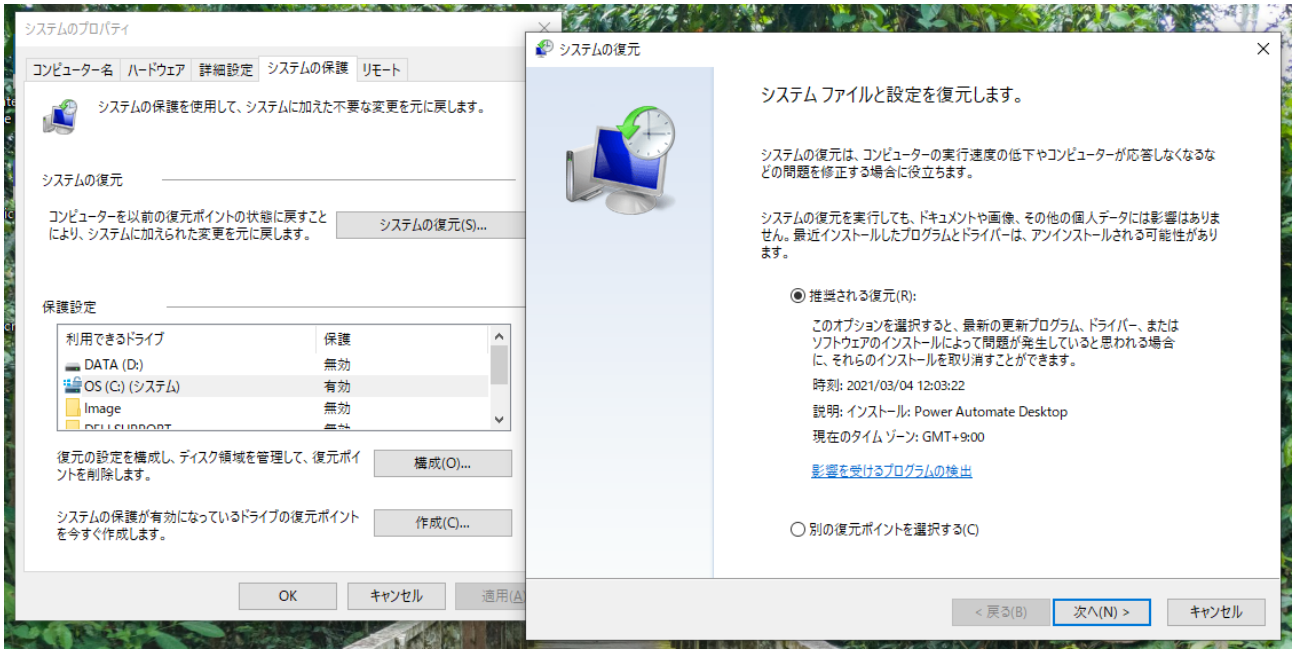
別のWindows 10の仮想マシン環境にWindows Admin Centerをインストールし、ローカルのWindows 10に接続できることを確認した上で、問題のアプリケーションをインストールしてみると、同じ問題が再現されました。問題の原因は特定できたので、問題のアプリケーションと関連コンポーネントをアンインストールし、コンピューターを再起動してみましたが、問題は解消されませんでした。Windows Admin Centerのアンインストールと再インストールも実施しましたが、それでも問題は解消されませんでした。**（注：この問題は Power Automate Desktop の当時のバージョ**

ンで確認しましたが、現在のバージョンでは再現しません。バージョン固有の問題あるいは筆者の環境固有の問題の可能性もあります。）

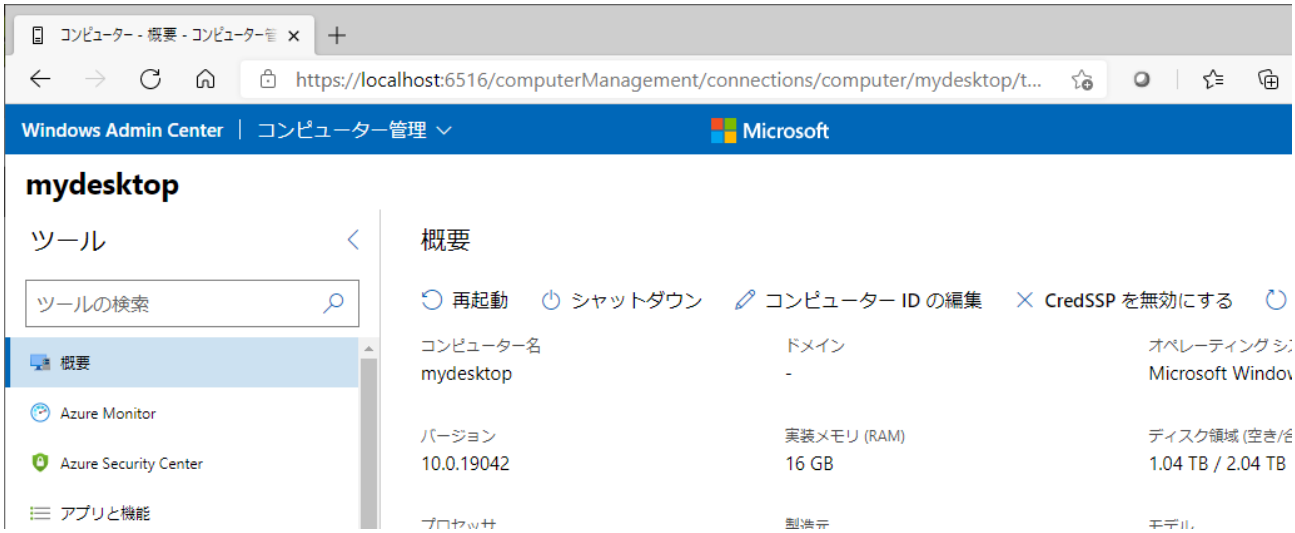


画面17　Microsoft Edgeのエラーが発生する少し前に、疑っていたアプリケーションをインストールしていたことを確認

Windowsは更新プログラムのインストール、ドライバーのインストール、アプリケーションのインストールといったタイミングでシステムの保護の復元ポイントを自動作成します（仮想マシンの場合は保護設定が既定で無効になっている場合があります）。問題のアプリケーションのインストール直前に作成された復元ポイントを復元することで、Windows Admin Centerの問題は完全に解消しました（画面18、画面19）。



画面18　問題のアプリケーションのインストール直前に自動作成された復元ポイントを使ってシステムを復元する



画面19　システムの復元によりWindows Admin Centerのローカル接続問題は解消

なお、オンラインの状態からシステムの復元を実行できない（OSが起動しない、あるいは復元が失敗する）場合は、Windows回復環境（WinRE）からシステムの復元を開始（トラブルシューティング｜詳細オプション｜システムの復元）できる場合があります（画面20）。また、システムの復元が無効になっており、利用可能な復元ポイントがない場合は、過去に取得済みのシステムのフルバックアップからシステム全体またはシステム状態を復元することができます。



画面20　Windowsからシステムの復元ができない場合は、Windows回復環境から実行する

問題を解決しようと、関係のないシステム設定を変更したりすると、別の問題を引き起こす、原因の特定が困難になるなど、問題が悪化することがあります。システム設定を意図的に変更していない限り、突然の問題発生の原因はシステム設定ではありません。オンラインのサービス関連の問題であれば、ローカル側のシステム設定は全く関係なく、サービス提供者側の障害や一時的な問題かもしれません。

それ以外の問題、WindowsのシステムエラーやSTOPエラー（ブルースクリーン、BSoD）、アプリケーションのエラーは、Windows Updateの更新プログラムのインストール、ドライバーのインストールや更新、アプリケーションのインストールや更新、アンインストールのタイミングで発生することがあります。信頼性モニターを使用すると、これらの履歴が情報イベントとして記録され、その前後のエラーの発生状況から関連性を調査することができます。

WSUSが遅くなった？ 長期運用WSUSのメンテナンス

Windows Serverのサーバーの役割の1つであるWindows Server Update Services（WSUS）は、企業内ネットワークでWindows、Windows Server、およびその他のマイクロソフト製品の更新プログラムの管理の一元化と配布の自動化を可能にする、Windowsネットワークにおける重要なインフラストラクチャサービスです。

しかし、WSUSサーバーを長期に運用していると、WSUSの管理コンソールでエラーが発生して管理画面にアクセスできなくなったり、パフォーマンスが低下したり、WSUSのコンテンツの格納先のディスク領域が不足したりといった、さまざまなトラブルを発症することがあります。

特に、WSUS管理コンソールのエラーに関する問題については、マイクロソフトの公式ドキュメントおよびWSUSサポートチームの情報が役に立つでしょう。また、WSUSの安定運用に関するホワイトペーパー『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』も参考にしてください。

WSUSメンテナンスガイド
https://docs.microsoft.com/ja-jp/troubleshoot/mem/configmgr/wsus-maintenance-guide

「WSUS 管理コンソールにつながらない！」を解消するための 7 つのワザ（JAPAN SCCM & WSUS Support Team）
https://social.msdn.microsoft.com/Forums/ja-JP/0dc69153-1d4e-4e91-bf91-df311424a8be/wsus-7-?forum=jpsccmwsus

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
https://www.say-tech.co.jp/yamaichi/key_point_of_wsus_monitoring

ここでは、WSUSを長期的に安定運用するのに役立つ、一般的な考慮点やメンテナンスタスクの定期実行について説明します。既にパフォーマンスの低下や容量不足に陥っているWSUSサーバーについても、これらの手順を実施することで劇的に改善する可能性があります。

SUSDB用WID/SQL Serverの最小／最大メモリの調整

WSUSデータベース（SUSDB）をホストするWindows Internal Database（WID、Windows Server付属のサーバーの機能の1つ）またはSQL Serverのサーバーメモリオプションは、WSUSサーバー全体のパフォーマンスを最適化できる重要な調整ポイントです。

WIDおよびSQL Serverのサーバーメモリオプションは、最小サーバーメモリと最大サーバーメモリがあり、既定値は最小0MB、最大2,147,483,647MB（約2ペタバイト）で、SQL Serverがメモリを動的に自動管理します。最大サーバーメモリを既定から変更していない場合、SQL Serverは最大で、システムやSQL Server以外のアプリケーションに必要なメモリ容量を物理メモリ全体量から差し引いた容量を割り当てます。SQL Serverの負荷が高く、既に利用可能な最大容量を使用している場合、新たに起動するサービスやアプリケーションや、既存のプロセスが追加で要求するリソースを確保できないという状況が発生します。

動的メモリを使用する仮想マシン仮想環境では、最小サーバーメモリをメモリを予約しておく目的で重要です。SUSDBをホストするSQL Serverでは、最小サーバーメモリを1024MBに設定することで安定したという実績があるそうです。

物理サーバーメモリを指定すると、サーバーの物理メモリ容量に余裕がない場合に、システムやSQL Server以外のアプリケーションのためにメモリを予約できます。

最小サーバーメモリおよび最大サーバーメモリは、SQL Server用の管理ツールであるSQL Server Management Studio（SSMS）を使用して簡単に変更できます。SUSDBのホストにWIDを使用している場合は、以下のURLから最新のSSMSをダウンロードしてWSUSサーバーにインストールしてください。

SQL Server Management Studio (SSMS) のダウンロード
https://docs.microsoft.com/ja-jp/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver15

SSMSを起動したらSQL Serverのインスタンスまたは WIDをホストするサーバーのデータベースエンジンに接続します。WIDを使用している場合はサーバー名として以下の名前を入力して接続してください。

¥.¥pipe¥MICROSOFT##WID¥tsql¥query

サーバーに接続したらサーバー名を右クリックして［プロパティ］を選択し、［メモリ］を選択し、［最小サーバーメモリ］および必要に応じて［最大サーバーメモリ］を変更し、［OK］をクリックします（画面24）。設定の変更は即座に反映されます。



画面24　SQL Serverのサーバーのプロパティを開き、［最小サーバーメモリ］および必要に応じて［最大サーバーメモリ］を変更する

WIDを使用している場合、SSMSでデータベースサーバーのプロパティを開くとエラーが発生する場合があります。その場合は［新しいクエリ（New Query）］を開き、次のようなクエリを入力して実行（Execute）し、設定値の変更を確認します（画面25）。次の例は最小サーバーメモリを1024MB（1GB）に変更します。

```
sp_configure 'show advanced options', 1 ↵

GO ↵

RECONFIGURE ↵

GO ↵

sp_configure 'min server memory', 1024 ↵

GO ↵

RECONFIGURE ↵
```

```
GO ↲

EXEC sp_configure 'min server memory' ↲

GO ↲
```

次の例は最大サーバーメモリを4096MB（4GB）に変更します。

```
sp_configure 'show advanced options', 1 ↲

GO ↲

RECONFIGURE ↲

GO ↲

sp_configure 'max server memory', 4096 ↲

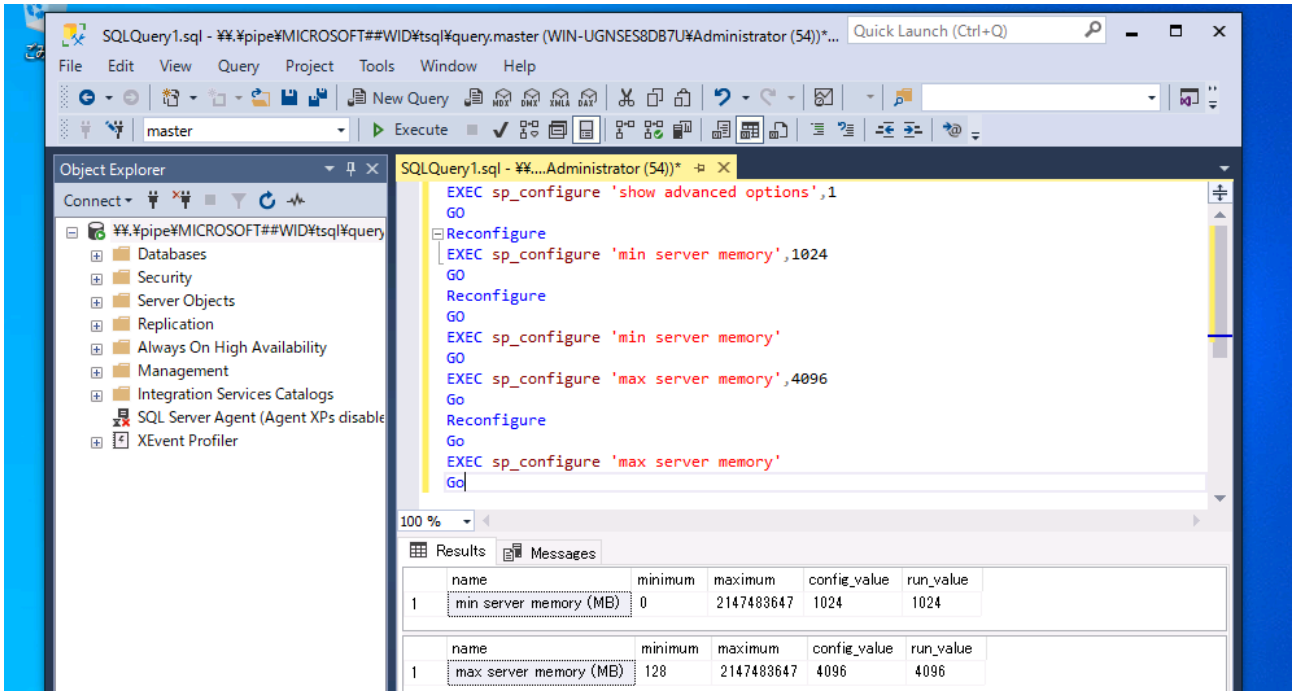
GO ↲

RECONFIGURE ↲

GO ↲

EXEC sp_configure 'max server memory' ↲

GO ↲
```



画面25　WIDの最小サーバーメモリと最大サーバーメモリをTransactSQLクエリで変更する

高速インストールオプションの必要性の検討

Windows 10バージョン1809およびWindows Server 2019では、累積更新プログラム（Cumulative Updates）と呼ばれる毎月の品質更新プログラムのWindows Updateでの配布方法とパッケージ形式に大きな変更が加えられました。

Windows 10バージョン1803以前の従来の累積更新プログラムは、以前にリリースされたすべての修正プログラムが含まれています。半期チャネル（SAC）ではあまり問題になることはありませんが、複数年にわたって品質更新プログラムが提供される長期サービスチャネル（LTSC）の場合、毎月の累積更新プログラムに累積される以前の修正プログラムが増える影響で、更新プログラムのパッケージサイズが肥大化し続け、ダウンロードのためのネットワーク帯域幅に直接的な影響を与えてしまうことがあります。例えば、Windows Server 2016用の累積更新プログラムは半年ほどで1GBを超え、リリースから4年以上経過した2021年春には1.6GBを超えるまでになっています。

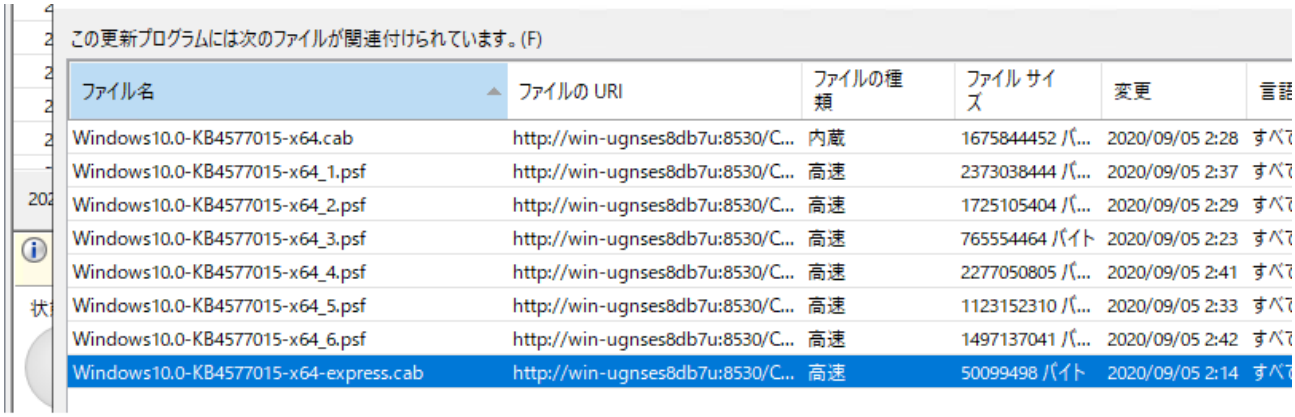
累積更新プログラムのサイズの肥大化に対して、Windows Updateにおけるダウンロード時間とネットワーク帯域幅の圧迫を改善するため、高速インストール（Express Install）または高速ダウンロード（Express Download）という仕組みが利用されてきました。高速インストール／高速ダウンロードでは、フルパッケージ（例：Windows10.0-KBXXXXXXX-x64.cab）をダウンロードする代わりに、カタログを含むExpressパッケージ（例：Windows10.0-KBXXXXXXX-x64_express.cab）がまずダウンロードされ、Expressパッケージの内容に基づいて、更新が必要なものだけを差分でダウンロードするようになっています。

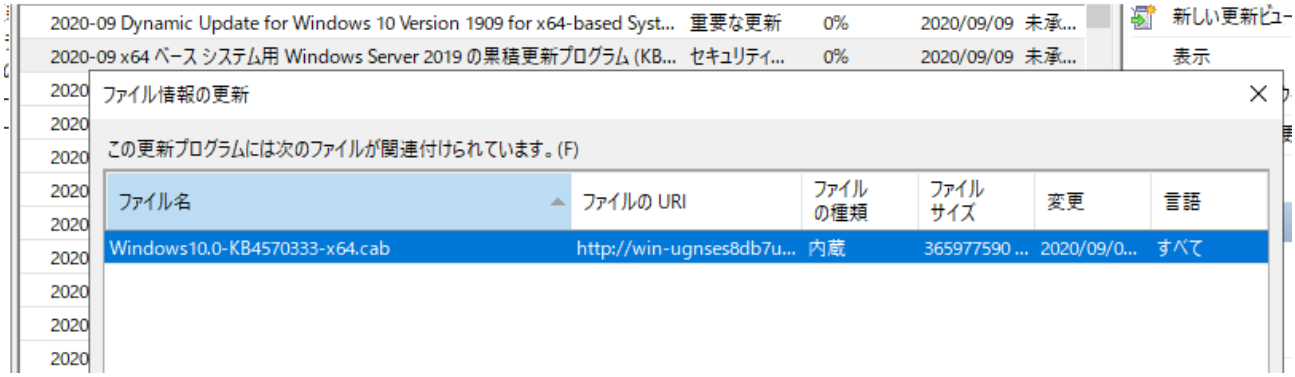
Windows 10バージョン1809およびWindows Server 2019では、Windows Updateでの累積更新プログラムのダウンロードに高速インストール／高速ダウンロードは原則として使用しなくなり、フルパッケージをダウンロードするようになりました（サービススタックの更新プログラムなど一部の更新プログラムについては引き続きExpressパッケージが使用されます）。新しい累積更新プログラムは以前にリリースされたすべての修正プログラムを含むのではなく、前方差分と後方差分を含む形で更新履歴を追跡可能にしています。これにより、フルパッケージのサイズは小さく抑えられ、年月とともに肥大化するということはなくなりました。詳しくは、以下のホワイトペーパーで説明されています。

前方差分と後方差分を使用したWindowsの更新プログラム（Windows Updates using forward and reverse differentials）
https://docs.microsoft.com/ja-jp/windows/deployment/update/psfxwhitepaper

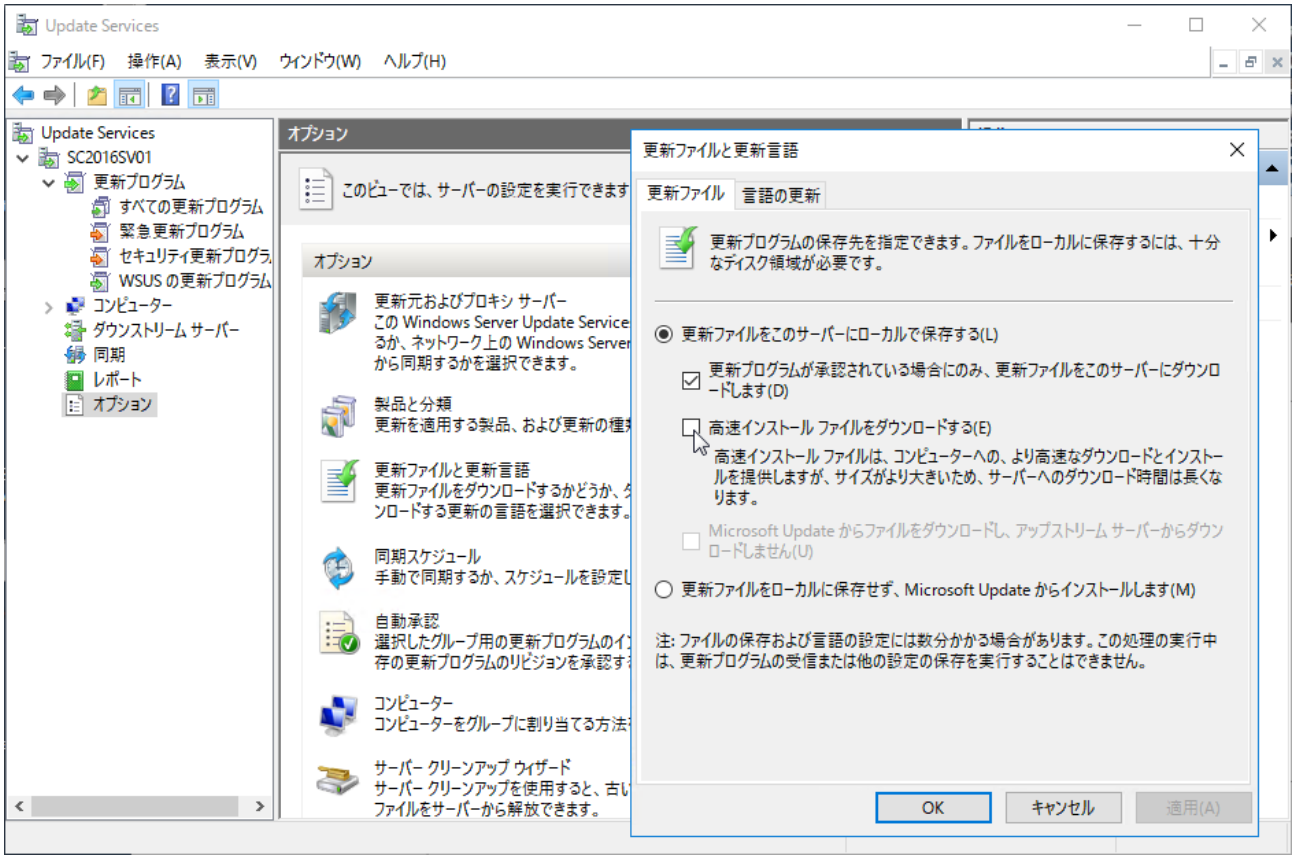
Windows 10バージョン1803以前（Windows Server 2016を含む）のWindows Updateで利用される高速インストール／高速ダウンロードの仕組みは、WSUSでも［高速インストールファイルをダウンロードする］というオプションを有効化することで対応できます。このオプションを有効化した場合、企業内ネットワーク内での高速インストール／高速ダウンロードを提供できますが、WSUSサーバーにMicrosoft Updateからダウンロードされるコンテンツは大幅に増加します。そのため、サーバーへのダウンロード時間が長くなり、WSUSコンテンツのディスク領域をより多く消費するようになります。

もし現在、WSUSで［高速インストールファイルをダウンロードする］オプションを有効にして運用している場合、その必要性を検討してください。企業内ネットワークで稼働中のクライアントやサーバーの、Windows 10バージョン1809およびWindows Server 2019以降への移行が完了し、以前のバージョンのWindows 10やWindows Server 2016が存在しなくなったのであれば、［高速インストールファイルをダウンロードする］オプションを有効にしているメリットはもうありません（画面26、画面27）。





画面26　WSUSに同期された累積更新プログラムのファイル情報の比較。Windows 10バージョン1803以前向けはフルパッケージ（.cab）と高速インストール用（_express.cabおよび.psf）の両方が用意されているが（画面上）、Windows 10バージョン1809以降はフルパッケージ（.cab）の提供のみ



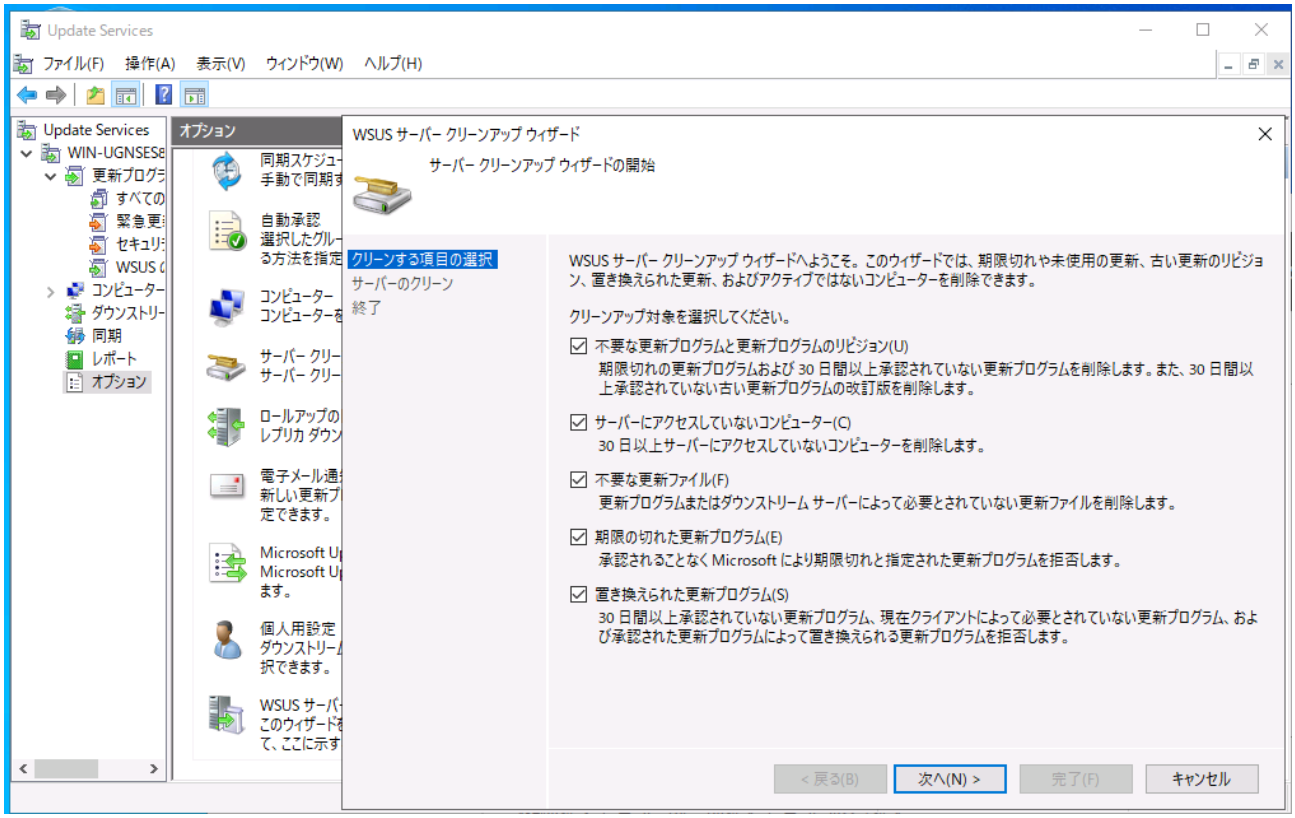
画面27　企業内のWindowsバージョンによっては［高速インストールファイルをダウンロードする］オプションを有効化するメリットはほとんどない

WSUSサーバークリーンアップウィザードの定期的な実行

毎月リリースされる更新プログラムおよび数か月ごとにリリースまたは改訂される機能更新プログラムの情報はWSUSデータベース（SUSDB）に蓄積され、承認に基づいてダウンロードされたWSUSコンテンツ（WSUSContent）ディレクトリに格納される更新プログラムの本体はドライブのディスク領域を使用し続けます。

WSUSはデータベースのデータとコンテンツディレクトリからのファイルの削除に関しては自動管理を行いません。そのため、数か月に1回、あるいは毎月（同期完了後）など定期的にメンテナンスを実施することが重要です。それには、［Update Services］（wsus.msc）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］を開始して、すべてのクリーンアップ対象を選択して実行します（画面28）。

なお、WSUSをダウンストリームサーバーとアップストリームサーバーの多階層構成で展開している場合は、階層の下部から順番にクリーンアップを実施するようにしてください。同じ階層の場合は複数のサーバーで同時にクリーンアップを実行できます。



画面28　WSUSサーバーを安定的に運用するためには、［WSUSサーバークリーンアップウィザード］を定期的に実行してデータベースとコンテンツディレクトリを最適化する

クリーンアップを定期的に実施していれば短時間で終了しますが、そうでない場合はすべての対象をクリーンアップするのに数時間単位の時間を要する場合があります。また、クリーンアップの実行中に複数回、WSUS Serviceサービスが再起動されます。長時間かかる場合、管理コンソールへのアクセスやパフォーマンス、クライアントアクセスに影響する可能性があります。影響を最小限にするためには、クライアントに影響しない業務時間外の日時に、クライアントの更新スケジュールと重複しない形で実施することをお勧めします。

PowerShellのInvoke-WsusServerCleanupコマンドレット（Windows Server 2012以降のWSUSで利用可能）を使用すると、パラメーターで1つ以上のクリーンアップ対象を指定することでコマンドラインからクリーンアップを実施することができます。クリーンアップ対象とパラメーターの対応を表3にまとめました。コマンドラインを記述したPowerShellスクリプト（.ps1）をタスクとして登録（**Windowsの運用管理を快適にする10の裏ワザ／表ワザ**　『パフォーマンス編 - タスクスケジューラの使いこなし』を参照してください）することで、毎月1回、あるいは数か月に1回といったサイクルで自動実行することができます。

表3　クリーンアップ対象とInvoke-WsusServerCleanupコマンドレットのパラメーターの対応

WSUSサーバークリーンアップウィザードでのクリーンアップ対象	Invoke-WsusServerCleanupのパラメーター
不要な更新プログラムと更新プログラムのリビジョン	-CompressUpdate -CleanupObsoleteUpdates
サーバーにアクセスしていないコンピューター	-CleanupObsoleteComputers
不要な更新ファイル	-CleanupUnneededContentFiles
期限の切れた更新プログラム	-DeclineExpiredUpdates
置き換えられた更新プログラム	-DeclineSupersededUpdates

次のWsusmaintenance.ps1は、ホワイトペーパー『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』で紹介したサンプルスクリプトです。すべてのクリーンアップ対象にクリーンアップを実行し、実行結果をログファイルにリダイレクトします。

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.logs ↲
```

その他のクリーンアップスクリプト

［WSUSサーバークリーンアップウィザード］と同等、あるいはそれ以上の機能を持つメンテナンスタスクをタスクスケジューラで自動実行することを目的とした有償／無償のツールや製品*4がいくつか存在します。その中で、Samer Sultan氏がGitHubで無償で公開しているWSUS Cleanup PowerShell Scriptを紹介します。

WSUS Cleanup PowerShell Script（GitHub samersultan/wsus-cleanup）
https://github.com/samersultan/wsus-cleanup

*4　筆者は以前、Adam Marshall氏（https://www.adamj.org/）が作成し、無料公開していたClean_WSUS.ps1スクリプト（通称、Adamj Clean-WSUS）をWSUSのメンテナンスに優れたツールとして利用および紹介していましたが、現在、数年前にこのスクリプトの提供は終了しています。Adamj Clean-WSUSは後継のWSUS Automated Mantenanceという有償ツールに置き換えられました。その早期のバージョンであるAdamj Clean-WSUSは使用しないことが推奨されています。

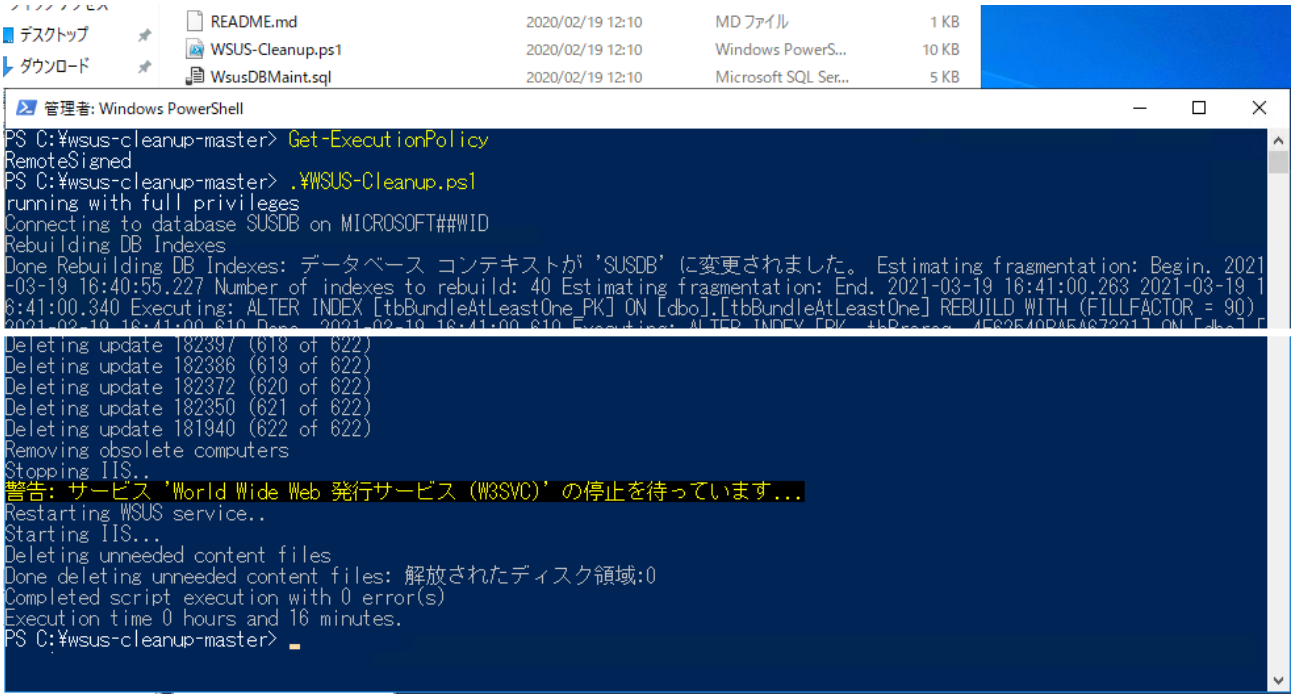
WSUS Cleanup PowerShell Scriptは、［WSUSサーバークリーンアップウィザード］やInvoke-WsusServerCleanupコマンドレットが行うのと同じメンテナンスタスクを、SQL Serverのストアドプロシージャを直接的に実行することで、タイムアウトエラーなどを回避しながらメンテナンスタスクを確実に実行するように作られています。さらに、データベースのインデックスの再構築という追加のデータベースメンテナンスタスクも実施してくれます。しかも、最後にIISとWSUSサービスの再起動は発生するものの、実行中にWSUSへのクライアントアクセスや管理アクセスが制限されることはありません。

このスクリプトはマイクロソフトが提供するものではなく、コミュニティベースのものですが、通常の［WSUSサーバークリーンアップウィザード］がエラーで失敗する場合は、試してみる価値はあります。

使い方は非常に簡単で、ダウンロードしたWSUS-Cleanup.ps1およびWsusDBMaint.sqlを格納したディレクトリから、WSUS-Cleanup.ps1を管理者として実行するだけです（画面29）。タスクスケジューラに登録して（**Windowsの運用管理を快適にする10の裏ワザ／表ワザ**　『パフォーマンス編 - タスクスケジューラの使いこなし』を参照してください）、毎月1回、あるいは数か月に1回といったサイクルで自動実行すればよいでしょう。スクリプトの作成者によると、週次または月次での実行を薦めています。

> .¥WSUS-Cleanup.ps1 ↲

なお、リモートのSQL Serverインスタンスを使用している場合はWSUS-Clean.ps1の$SqlServerにコンピューター名を設定する必要があります。



画面29　WSUS-Cleanup.ps1を利用したWSUSサーバーのメンテナンス

データベースのインデックスの再構築のためには、SQLCMDユーティリティが利用可能であることが必要です。WIDを使用している場合は、以下のURLからSQLCMDユーティリティ（本稿執筆時点のバージョンはMicrosoft Comman d Utilites 15 for SQL Server）をダウンロードしてWSUSサーバーにインストールしてから実行してください。

sqlcmd ユーティリティ
https://docs.microsoft.com/ja-jp/sql/tools/sqlcmd-utility

SQL Serverを使用している場合、スクリプトの問題によりインデックスの再構築でエラーが発生し、スキップされるかもしれません。筆者が使用したスクリプトのバージョン（Last updated 11-26-2019、Version 4）の場合は、WSUS-Cleanup.ps1のfunction RebuildDBIndexes{} 内のコードを以下のように変更することでローカルのWIDとSQL Serverの両方に対応させることができます。なお、WIDを使用している場合は変更の必要はありません。

変更前	$status = SQLCMD -S ¥¥.¥pipe¥Microsoft##WID¥tsql¥query -i $SQLPath -I ↲

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

マルウェア対策の最適化

Windows 10およびWindows Server 2016以降には、Microsoft Defenderウイルス対策（旧称、Windows Defender）が標準搭載されており、サードベンダーのウイルス対策製品がインストールされていない限り既定で有効です。サードベンダーのウイルス対策製品がインストールされている場合は、自動的に無効化されます。

マルウェア対策としてMicrosoft Defenderウイルス対策を利用している場合、リアルタイムスキャンが有効であること、エンジンと定義ファイル（セキュリティインテリジェンス更新プログラム）が最新版に更新されていること、および定期的にスキャンが実行されていることが高いセキュリティを維持する上で重要です。

その上で、特にサーバーのパフォーマンスを最適化するためには、適切な除外設定を行うことが重要です。除外設定なしで運用する場合、パフォーマンスが劣化したり、サービスやアプリケーションでエラーが発生して正常に動作しなくなったりすることがあります。ここではMicrosoft Defenderウイルス対策の除外設定の具体的な方法、およびHyper-Vの役割とWindowsコンテナー用コンテナーホストのための除外設定について説明します。

Microsoft Defenderの自動除外

Windows Server 2016以降のMicrosoft Defenderウイルス対策では、自動除外（Automatic Exclusions）という機能を備えており、既定で有効になっています。この機能はWindows 10にもあり既定で有効ですが、特にさまざまな役割やサーバーアプリケーションを実行するWindows Serverでこの機能が有効になっていることが重要です。

Microsoft Defenderウイルス対策の自動除外が有効になっているかどうかは、PowerShellの以下のコマンドラインの実行結果がFalseになっているかどうかで分かります。

> (Get-MpPreference).DisableAutoExclusions ↲
>
> False ･･･ 自動除外が有効

Windows Serverで自動除外が有効になっている場合、有効になっているサーバーの役割に応じて定義済みの除外設定が適用されます。

具体的にはWindows Updateのデータベースやログファイル、Windowsのセキュリティデータベース、グループポリシー関連ファイル、WINSデータベース、ファイルレプリケーションサービス（FRS）データベース、分散ファイルシステムレプリケーション（DFSR）のデータベースとプロセス、Hyper-V関連のファイルの種類、ディレクトリ、およびプロセス、Active DirectoryのNTDSデータベース、SYSVOL共有、DHCPサーバーのデータベース、DNSサーバーのデータベース、クラスター共有ストレージ、プリンタースプーラーのディレクトリおよびプロセス、IIS Webサーバーのディレクトリとプロセス、Windows Server Update Services（WSUS）のコンテンツとデータベースなどが除外されます。

詳しくは、以下のドキュメントで説明されています。

Windows Server で Microsoft Defender ウイルス対策の除外を構成する
https://docs.microsoft.com/ja-jp/windows/security/threat-protection/microsoft-defender-antivirus/configure-server-exclusions-microsoft-defender-antivirus

例えば、Hyper-Vの役割が有効になっている場合、表1に示す除外設定が適用されます。

表1　Hyper-Vの役割の自動除外設定

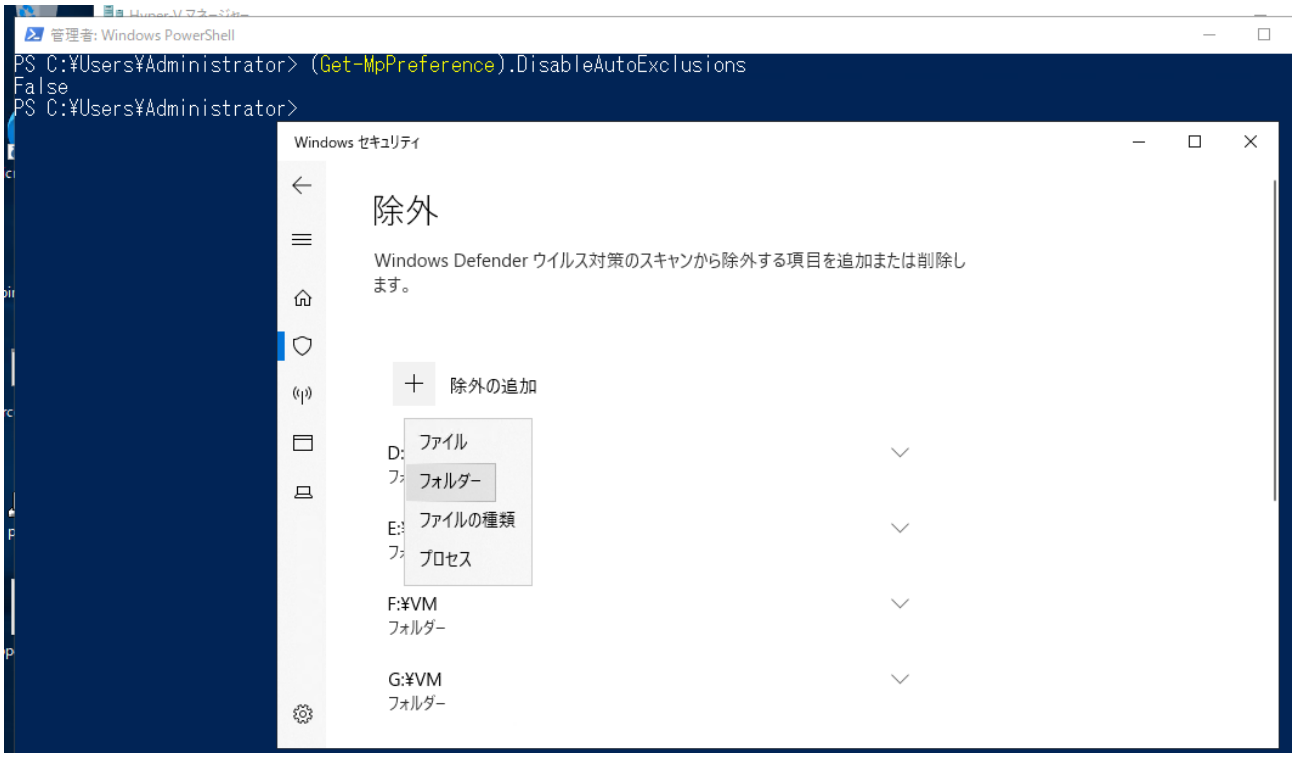
ファイルの種類の除外	.vhd、.vhdx、.avhd、.avhdx、.iso、.rct、.vsv、.vmcx、.vmrs
ディレクトリの除外	%ProgramData%¥Microsoft¥Windows¥Hyper-V %ProgramFiles%¥Hyper-V %Public%¥Documents¥Hyper-V¥Virtual Hard Disks %SystemDrive%¥ProgramData¥Microsoft¥Windows¥Hyper-V¥Snapshots
プロセスの除外	%systemroot%¥System32¥Vmms.exe（Virtual Machine Management Service） %systemroot%¥System32¥Vmwp.exe（Virtual Machine Worker Process）

Microsoft Defenderの自動除外＋カスタム設定

自動除外設定でカバーされない場所に除外するべきデータベースやファイルを配置している場合は、自動除外に加えて、カスタム設定を追加することを推奨します。また、自動除外設定の対象外の役割やアプリケーションを利用している場合もカスタム設定を検討してください。除外設定によりパフォーマンスを改善できる場合があります。一方で、除外対象からはマルウェアが検出されなくなるというデメリットにも留意してください。

カスタム除外設定の追加

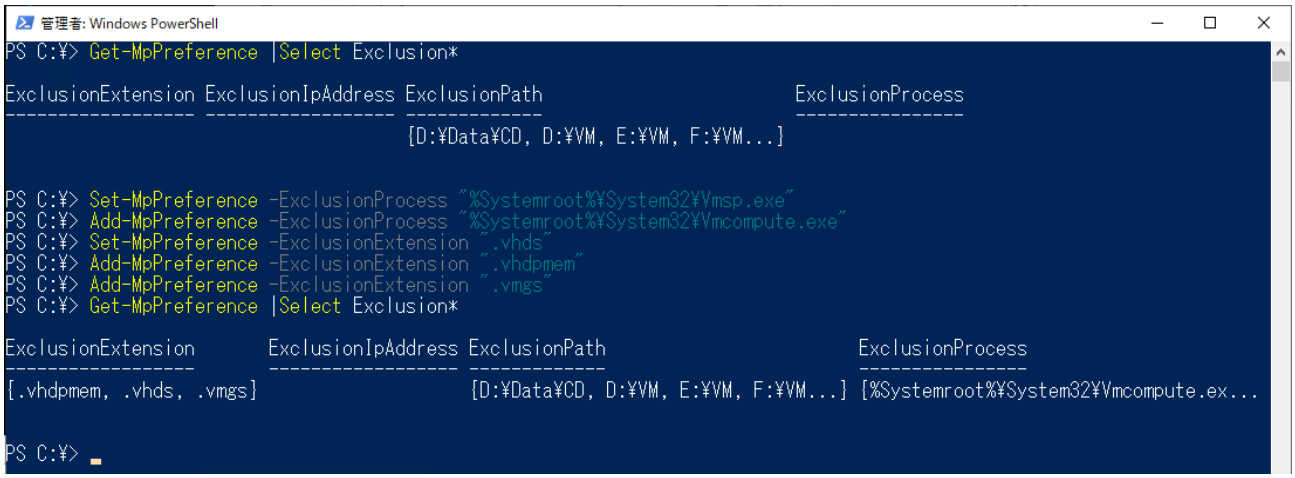
Microsoft Defenderウイルス対策の除外設定は、Windows 10やWindows Server 2016以降のバージョンによって異なります。Windows Server 2016デスクトップエクスペリエンスの場合、［設定］アプリの［更新とセキュリティ］－［Windows Defender］－［除外］から除外を編集します。Windows Server 2019デスクトップエクスペリエンスの場合は、［Windowsセキュリティ］の［ウイルスと脅威の防止］－［ウイルスと脅威の防止の設定］の［設定の管理］から除外設定を編集します（画面7）。



画面7　Windows Server 2019デスクトップエクスペリエンスでのカスタム除外設定

PowerShellのDefenderモジュールのコマンドレットを使用すると、Windowsのバージョンによる設定の場所の違いや、インストールの種類（デスクトップエクスペリエンスとServer Core）に関係なく、一貫性のある方法で除外設定が行えます（画面8）。

> Get-MpPreference |Select Exclusion* ↲
>
> Set-MpPreference -ExclusionExtension ".拡張子" ↲（新たに設定）
>
> Add-MpPreference -ExclusionExtension ".拡張子" ↲（設定を追加）
>
> Remove-MpPreference -ExclusionExtension ".拡張子" ↲（設定を削除）
>
> Set-MpPreference -ExclusionPath "ディレクトリパス" ↲（新たに設定）
>
> Add-MpPreference -ExclusionPath "ディレクトリパス" ↲（設定を追加）
>
> Remove-MpPreference -ExclusionPath "ディレクトリパス" ↲（設定を削除）
>
> Set-MpPreference -ExclusionProcess "実行可能ファイルのパス" ↲（新たに設定）
>
> Add-MpPreference -ExclusionProcess "実行可能ファイルのパス" ↲（設定を追加）
>
> Remove-MpPreference -ExclusionProcess "実行可能ファイルのパス" ↲（設定を削除）



画面8　PowerShellのDefenderモジュールのコマンドレットを使用したカスタム除外設定。なお、自動除外の設定内容は表示されない

Hyper-Vホストのためのカスタム設定

以下の「Hyper-V ホストに推奨されるウイルス対策の除外」のドキュメントの説明によると、自動除外に含まれない以下のファイルの種類、ディレクトリ、およびプロセスを除外することが推奨されています。Hyper-V環境ではホストとゲストの両方でMicrosoft Defenderウイルス対策またはサードベンダーのマルウェア対策製品の保護が働きます。スキャンが重複しないようにホスト側での除外設定は重要です。

- VHDセット（.vhds）（Windows Server 2016以降）
- VMゲスト状態ファイル（.vmgs）（Windows Serverバージョン1709以降の仮想マシン構成バージョン8.2以降）
- メモリ状態ファイル（.bin）（Windows Server 2012 R2の古い仮想マシン構成バージョン5.0）
- 仮想マシン構成ファイルが配置されているカスタムディレクトリ
- 仮想ハードディスクファイルが配置されているカスタムディレクトリ
- Hyper-Vレプリカを使用している場合はレプリケーションデータのディレクトリ

- SMB 3.0共有に仮想マシンを配置している場合は、共有しているディレクトリ（ファイルサーバー側のウイルス対策で除外）
- %SystemRoot%¥System32¥Vmsp.exe（Virtual Machine Security Process、Windows Server 2016以降）
- %SystemRoot%¥System32¥Vmcompute.exe（Hyper-V Host Compute Service、Windows Server 2019以降）

Hyper-V ホストに推奨されるウイルス対策の除外
https://docs.microsoft.com/ja-jp/troubleshoot/windows-server/virtualization/antivirus-exclusions-for-hyper-v-hosts

Windowsコンテナーのためのカスタム設定

Windows Server 2016以降の新しい機能である、Mirantis Container Runtime（旧称、Docker Engterprise）対応のWindowsコンテナーに関しては自動除外の対象として明記されていません。

Microsoft Defenderウイルス対策は、Windows Serverベースのコンテナーホストの保護をサポートしますが、Windowsコンテナー内ではMicrosoft Defenderウイルス対策はサポートされません。WindowsコンテナーのベースOSイメージであるservercoreおよびnanoserverにはMicrosoft Defenderウイルス対策のバイナリ（C:¥Program Files¥Windows Defender）やサービス（WinDefend）は含まれません。言い換えると、Windowsコンテナー内の実行環境でMicrosoft Defenderによる保護は提供できないため、コンテナーのイメージやプロセスをコンテナーホスト側で保護することが重要です。

Microsoft Defenderを対象としたものではありませんが、コンテナーホストにおけるマルウェア対策の最適化については、マイクロソフトおよびDockerのドキュメントで説明されています。

Windows コンテナー用のウイルス対策最適化
https://docs.microsoft.com/ja-jp/windows-hardware/drivers/ifs/anti-virus-optimization-for-windows-containers

Antivirus software and Docker
https://docs.docker.com/engine/security/antivirus/

Dockerドキュメントによると、Dockerが使用中のファイルをマルウェア対策ソフトウェアがスキャンすると、対象のファイルがロックされることにより、dockerコマンドのハングが発生する可能性があるそうです。この問題を緩和するには、Dockerのデータディレクトリ（Windows Serverベースのコンテナーホストの場合の既定はC:¥ProgramData¥docker）を保護の対象から除外します。しかし、除外により、イメージ内にウイルスやマルウェアが含まれる場合やコンテナーボリュームに書き込まれた場合、それを検出できません。なお、除外設定なしでも通常は問題なく機能しますが、スキャンの負荷がコンテナーの開始と実行に影響する可能性はあります。

Dockerのデータディレクトリ（既定のパスまたはdaemon.jsonのgraphパスで指定されたカスタムパス）を保護から除外する場合は、Dockerサービスの停止、除外の解除、データディレクトリのスキャン、除外の再設定、Dockerサービスの起動を定期的なタスクをスケジューリングするとよいでしょう。Microsoft Defenderの場合は、PowerShellの次の一連のコマンドラインをタスクとして実行することで実現できます。PowerShellコマンドやPowerShellスクリプト（.ps1）のタスク登録については、本編の『タスクスケジューラの使いこなし』を参照してください。

```
Stop-Service -Name Docker ↲

Remove-MpPreference -ExclusionPath "C:¥ProgramData¥docker" ↲

Start-MpScan -ScanPath "C:¥ProgramData¥docker" -ScanType CustomScan ↲
```

```
Add-MpPreference -ExclusionPath "C:¥ProgramData¥docker" ↲

Start-Service -Name Docker ↲
```

SQL Serverのためのカスタム設定

SQL Serverを実行しているコンピューターのマルウェア対策の一般的なガイドラインは以下のドキュメントに記されています。

How to choose antivirus software to run on computers that are running SQL Server
https://support.microsoft.com/en-us/topic/feda079b-3e24-186b-945a-3051f6f3a95b

ガイドラインでは、SQL Serverのパフォーマンスの改善に寄与するディレクトリ、拡張子、プロセスの除外設定が詳細に記されています。適切な除外設定を行うことで、SQL Serverのサービスが関連ファイルを使用する際にスキャンツールがロックするのを回避できます。ただし、除外設定したファイルがマルウェアに感染した場合、マルウェア対策ソフトウェアはそれを検出できないというデメリットがあります。

SQL Server用に除外設定を行う場合は、Windowsコンテナーの場合と同様に、業務時間外などにSQL Serverのサービスを停止した上で、除外設定を解除してカスタムスキャンを実施することをお勧めします。

他社マルウェア対策製品を利用する場合の考慮事項

Windows Serverでサードベンダーのマルウェア対策製品を利用する場合は、Microsoft Defenderウイルス対策の除外設定、およびHyper-Vホストに推奨されるウイルス対策の除外のドキュメントを参考に、サーバーの役割に適切なすべての除外設定をカスタム設定で実装してください。

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-パフォーマンス改善テンプレート

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。

- ディスククリーンアップタスク実行
- NGEN監視
- FireWall監視
- Microsoft Defender の除外設定監視

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)

ディスククリーンアップタスク実行

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Windows Updateの不要なコンポートネントの削除やコンポーネントストアの最適化を定期的 (7日ごと) に実施し、終了するとメール送信します

(1) ディスククリーンアップ実行トリガー

本サービス監視は、ディスククリーンアップを実施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。

なお、本トリガーの実行はサービス直後に一度実行し、それ以降は7日毎の午前3時に実行します。実行時間間隔や

実行時刻については、お客様の環境に応じて変更ください。

(2) SilentCleanupタスク実行

ディスククリーンアップ実行バッチファイル"silentcleanup.bat" を実行するためのカスタムアクションです。

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、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。

(3) cleanmgrプロセス終了確認開始

(2)の実行後に起動されるcleanmgr.exeのチェックを実施するため(4)の監視を有効にします。

※監視有効無効の設定については、「ディスククリーンタスク実行」グループの「終了確認」項目を指定してください。既に別の監視項目が設定されているインスタンスに監視項目をインポートした場合やグループID、監視IDが変更された場合は監視有効無効の指定位置が変更になりますので、必ず実施し、確認してください。

(4) 終了確認

(2)で起動された"cleanmgr.exe"が終了したかを監視する監視項目です。

(5) 終了メール送信

ディスククリーンアップの終了時にメール送信するアクションです。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。

(6) 現ID無効

(4)の終了確認の監視項目を無効にします。

※監視有効無効の設定については、「ディスククリーンタスク実行」グループの「終了確認」項目を指定してください。既に別の監視項目が設定されているインスタンスに監視項目をインポートした場合やグループID、監視IDが変更された場合は監視有効無効の指定位置が変更になりますので、必ず実施し、確認してください。

NGEN監視

この監視設定は7日ごとに対象の監視インスタンスで動作するWindows OS の.NET Frameworkの累積的な更新プログラムがインストールされているかをチェックして、実行し、実行開始と実行終了をメール送信します。

(1) 準備完了ステータスチェック

"ngen_ready.bat"を実行するための監視項目です。

タスクスケジューラに登録されているNGENタスクの状態をテキストログ"tasksch_check.txt"に出力します。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

いる設定となっています。最初の1回目は、サービス開始直後に実行し、2回目以降は、7日毎の午前3時に実行します。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。

(2) NGEN開始チェック有効

(1)で出力した"tasksch_check.txt"のログをチェックする監視項目を有効にするアクションです。

※監視有効無効の設定については、「NGEN監視」グループの「NGEN開始」項目を指定してください。既に別の監視項目が設定されているインスタンスに監視項目をインポートした場合やグループID、監視IDが変更された場合は監視有効無効の指定位置が変更になりますので、必ず実施し、確認してください。

(3) NGEN開始

(1)で出力した"tasksch_check.txt"ファイルの中の文字列を検索する監視項目です。NGENを開始する条件を検知します。既定値での対象ファイルは "C:¥ProgramData¥SAY Technologies¥BOMW8¥support_script" 以下に保存されている設定となっています。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。

(4) NGEN実行

NGENタスクを実行する"ngen.bat"ファイルを実行するアクションです。

既定値での対象ファイルは "C:¥ProgramData¥SAY Technologies¥BOMW8¥support_script" 以下に保存されている設定となっています。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。

・"ngent.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。

(5) NGEN開始メール送信

NGENタスクの実行開始時にメール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。

(6) 現監視無効

「NGEN開始」監視項目を無効にするためのアクションです。

※監視有効無効の設定については、「NGEN監視」グループの「NGEN開始」項目を指定してください。

既に別の監視項目が設定されているインスタンスに監視項目をインポートした場合やグループID、監視IDが変更された場合は監視有効無効の指定位置が変更になりますので、必ず実施し、確認してください。

(7) 無効ステータスチェック有効

「無効ステータスチェック」監視項目を有効にするためのアクションです。

※監視有効無効の設定については、「NGEN監視」グループの「無効ステータスチェック」項目を指定してくださ

い。既に別の監視項目が設定されているインスタンスに監視項目をインポートした場合やグループID、監視IDが

変更された場合は監視有効無効の指定位置が変更になりますので、必ず実施し、確認してください。

(8) 無効ステータスチェック

(1)と同様に"ngen_ready.bat"を実行するための監視項目です。

タスクスケジューラにNGENタスクが登録されているかをテキストログ"tasksch_check.txt"に出力します。

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います。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。

(9) NGEN終了有効

「NGEN終了」監視項目を有効にするためのアクションです。

※監視有効無効の設定については、「NGEN監視」グループの「NGEN終了」項目を指定してください。既に別の

監視項目が設定されているインスタンスに監視項目をインポートした場合やグループID、監視IDが変更された

場合は監視有効無効の指定位置が変更になりますので、必ず実施し、確認してください。

(10) NGEN終了

(1)で出力した"tasksch_check.txt"ファイルの中の文字列を検索するテキストログ監視です。NGENを終了する条件

を検知します。既定値での対象ファイルは "C:¥ProgramData¥SAY Technologies¥BOMW8¥support_script" 以下

に保存されている設定となっています。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。

(11) NGEN終了メール送信

NGENタスクの終了時にメール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。

(12) 現監視無効

「NGEN終了」監視項目を無効にするためのアクションです。

※監視有効無効の設定については、「NGEN監視」グループの「NGEN終了」項目を指定してください。既に別の

監視項目が設定されているインスタンスに監視項目をインポートした場合やグループID、監視IDが変更された

場合は監視有効無効の指定位置が変更になりますので、必ず実施し、確認してください。

(13) 無効ステータスチェック無効

「無効ステータスチェック」監視項目を無効にするためのアクションです。

※監視有効無効の設定については、「NGEN監視」グループの「無効ステータスチェック」項目を指定してくださ

い。既に別の監視項目が設定されているインスタンスに監視項目をインポートした場合やグループID、監視IDが

変更された場合は監視有効無効の指定位置が変更になりますので、必ず実施し、確認してください。

FireWall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 Defender ファイアウォールのルール数とルールリストを、7日ごとにチェックしてメール送信します。

(1) FireWallルール数監視

"count_fwrures.bat"を実行し、ファイアウォールのルール数を取得します。

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います。最初の1回目は、サービス開始直後に実行し、2回目以降は、7日毎の午前1時に

実行します。また、既定値でルールが1つでもあればメールが送信される設定となっています。

テンプレートを使用する際、必要に応じて各設定を変更してください。

(2) FireWallルール数メール送信

(1)で取得したファイアウォールのルール数をメール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。

(3) FireWallリスト監視

ファイアウォールに設定されているルールをリスト化し、テキストファイルに出力する監視項目です。

出力ファイルは "C:¥ProgramData¥SAY Technologies¥BOMW8¥support_script¥fwlist.txt" 以下に保存されてい

る設定となっています。最初の1回目は、サービス開始直後に実行し、2回目以降は、7日毎の午前2時に実行します。

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。出力ファイルを変更する際は、"fwlist.ps1"

ファイルの該当ファイルのパスをフルパスで指定ください。

(4) FireWallListメール送信

(3)で取得したファイアウォールのルールリストをメール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。

既定値でのルールリストは"C:¥ProgramData¥SAY Technologies¥BOMW8¥support_script¥flist.txt"となっています。(3)で変更された際は「設定」タブの「添付/埋め込みファイル」のファイル内容を更新してください。

Microsoft Defender の除外設定監視

この監視設定は、監視対象のWindowsOSで動作するMicrosoft Defender(以下Devender)での自動除外設定の有無を1日ごとにチェックすることと、カスタム除外リストを7日ごとにメール送信します。

(1) Defenderの自動除外チェック監視

"defender_exclusive.bat"を実行し、Microsoft Defenderの自動除外設定がされているかどうかを チェックします。

自動除外設定がされていれば、取得値が0となり、ステータスは正常で、それ以外の数値は設定されていないことを示し、危険ステータスになります。最初の1回目は、サービス開始直後に実行し、24時間毎に実行します。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。

(2) 自動除外チェックメール送信

(1)で取得したステータスに応じてメール送信するためのアクションです。
自動除外が設定されていない場合に、メール送信されます。

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。

(3) Defenderカスタム除外リスト取得監視

Defenderに設定されているカスタム除外リストをテキストファイルに出力する監視項目です。

出力ファイルは "C:¥ProgramData¥SAY Technologies¥BOMW8¥support_script¥exclusivelist.txt" に保存される設定となっています。最初の1回目は、サービス開始直後に実行し、2回目以降は、7日毎の午前1時に実行します。

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。出力ファイルを変更する際は、

"defender_exclusivlist.bat"ファイルの該当ファイルのパスをフルパスで指定ください。

(4) カスタム除外リストメール送信

(3)で取得したDefenderカスタム除外リストをメール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。

既定値でのDefenderカスタム除外リストは

"C:¥ProgramData¥SAY Technologies¥BOMW8¥support_script¥exclusivelist.txt"となっています。(3)で変更された際は「設定」タブの「添付/埋め込みファイル」のファイル内容を更新してください。

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
(BOM8.0-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　- パフォーマンス改善編 -

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.