別添資料

Windows Sandboxを悪用した手口及び痕跡・検知策

2025年1月8日

警察庁

1-1 はじめに

(1) 背景

遅くとも2023年6月頃からMicrosoft社が提供するWindows Sandboxの機能を悪用した手口が見られています。

Windows Sandboxは、Windows 10 Pro等に標準で搭載され、アプリケーションを単独で安全に実行するための軽量のデスクトップ環境（サンドボックス）を提供し[1]、以下のような特徴があります[2][3]。

- Windows Sandboxは、ホストコンピュータ（実機）と分離された一時的な仮想的なデスクトップ環境です。
- Windows Sandboxは実行される度に新しいクリーンな環境を提供し、使用された環境はWindows Sandboxの終了時にすべて破棄されます。
- ホストコンピュータにインストールされているアプリケーションは、サンドボックスから直接使用できません。

1-2 はじめに

（2）目的

本資料には、類似手口を用いたサイバー攻撃の被害拡大防止及び被害の未然防止のための適切なセキュリティ対策を講じていただくことを目的として、Windows Sandboxを悪用した手口及びWindows Sandboxの動作を検証した結果を紹介いたします。当該手口に対する検知策を検討する際の参考としてください。

ただし、本資料で紹介するものは、以下表1の環境でWindows Sandboxの動作を確認した結果を示したものになります。

Windows OSのバージョン	Windows Sandboxのバージョン
Windows 11 Enterprise（24H2）	10.0.26100.2454
Windows 11 Pro（23H2）	10.0.22621.3527
Windows 10 Pro（22H2）	10.0.19041.3636

表1：検証環境におけるWindows OS及びWindows Sandbox

2-1 攻撃手口

（1）特徴

標的型メール等により、コンピュータをLODEINFO等のマルウェアに感染させた後、Windows Sandboxを悪用した手口により、サンドボックス内でマルウェアを実行していたとみられます。

当該手口では、ホストコンピュータにおけるウイルス対策ソフト、EDR（Endpoint Detection and Response）等の検知を逃れてマルウェアを実行します。

また、ホストコンピュータをシャットダウン又は再起動することにより、サンドボックスの痕跡が消去されることから、マルウェアが実行した動作について事後調査することが困難になります。

2-2 攻撃手口

（2） 手口事例

① Windows Sandbox構成ファイル(wsbファイル)には、ホストコンピュータとサンドボックス間の共有フォルダ設定、サンドボックスにおける実行コマンド設定、サンドボックスからのネットワーク接続許可設定が記載されています。

ホストコンピュータのタスクスケジューラにより、wsbファイルを読み込み、Windows Sandboxを起動します。

② ホストコンピュータとサンドボックス間の共有フォルダとして、「C:¥Users」フォルダを、書き込みを許可する設定でサンドボックスにマウントします。

③ サンドボックス内で、マウントされた共有フォルダに保存されていたバッチファイルを実行します。

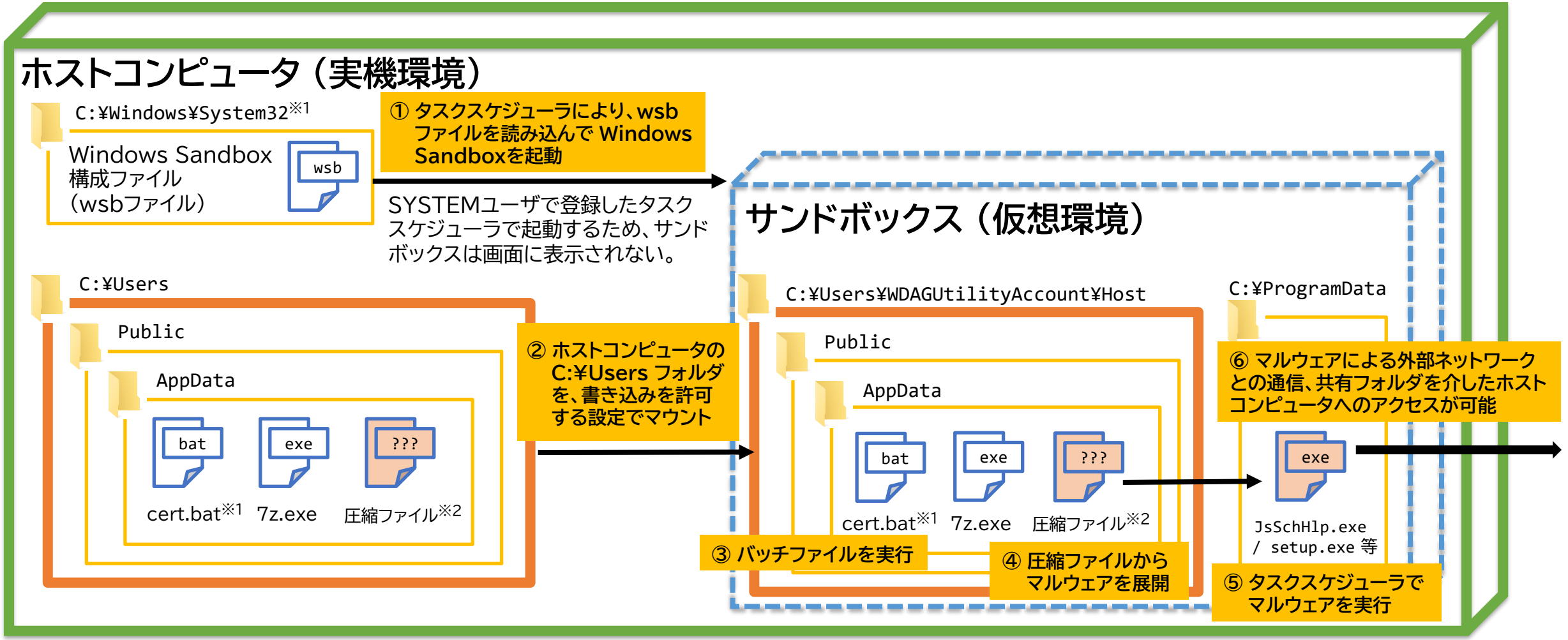
④ 暗号化された圧縮ファイルが展開され、マルウェアをサンドボックス内のフォルダに保存します。

⑤ サンドボックス内のタスクスケジューラにより、マルウェアを実行します。

⑥ マルウェアによるC2サーバを含む外部ネットワークとの通信及び共有フォルダを介したホストコンピュータへのアクセスが可能となります。

2-3 攻撃手口

概略図



※1　wsbファイルの保存場所、自動実行するファイル名は任意指定が可能
※2　圧縮ファイルはパスワード保護されており、拡張子は .dat / .db などに偽装

3-1 痕跡・検知策

Windows Sandboxを悪用した手口の痕跡・検知策を検討するために、Windows Sandboxのの機能が有効か否かを確認する手法及びWindows Sandboxの実行痕跡を確認する手法について検証しました。

これらの検証結果における例などを以降のページに記載しますので、検知策を検討する際に参考としてください。

3-2 痕跡・検知策

（1）Windows Sandboxの機能が有効か否かを確認

① 「Windowsの機能」による確認方法: コントロール パネル → プログラムと機能 → Windowsの機能の有効化または無効化

以下の図1のように「Windows サンドボックス」のチェックボックスがオンになっている場合は、機能が有効となっています。

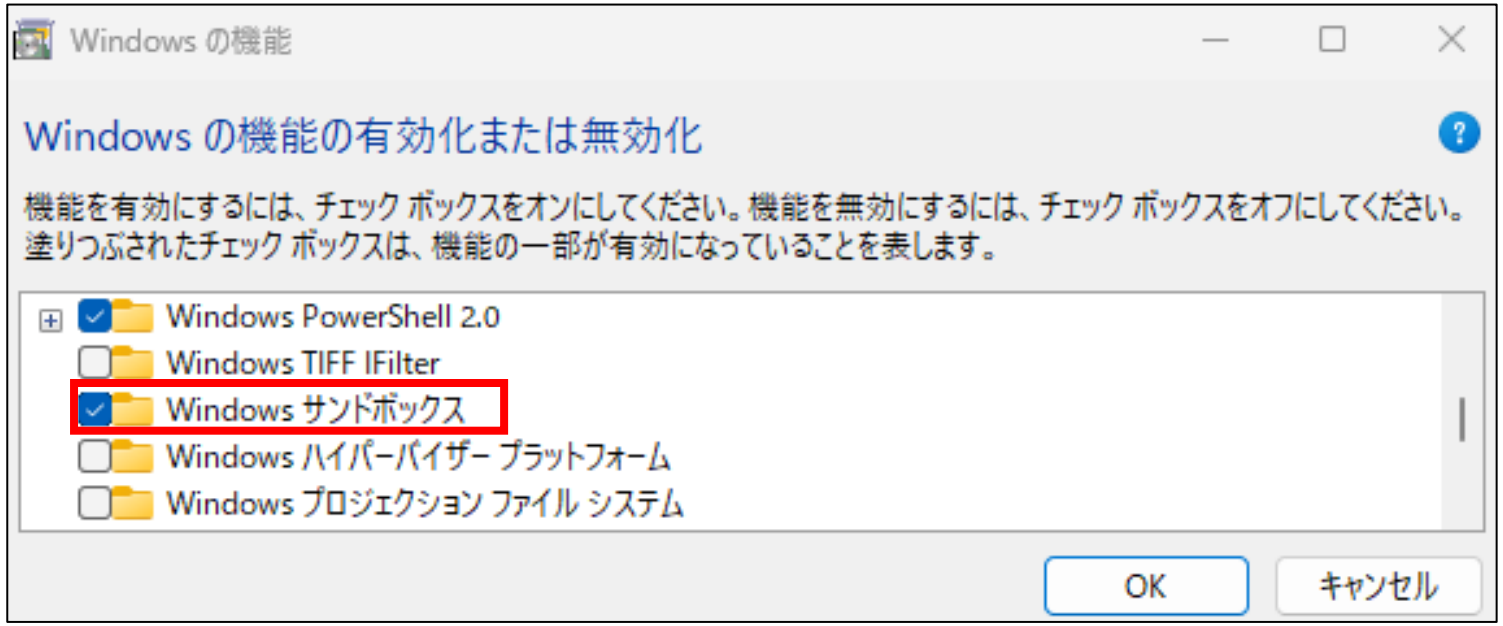


図1：Windows Sandboxが有効の場合

利用する予定がなければ、オフ(無効)にすることを検討してください。

3-3 痕跡・検知策

② コマンドプロンプト又はPowerShellによる確認方法: 以下のコマンドを実行することにより、項目「状態」がWindows Sandboxの機能が有効か否かで変化することを確認しました[4]。ただし、図2及び図3の確認には管理者権限が必要になる場合があります。

コマンド:

```
dism /online /Get-Featureinfo /FeatureName:Containers-DisposableClientVM
```

図2：Windows Sandboxが有効の場合

図3：Windows Sandboxが無効の場合

3-4 痕跡・検知策

③ PowerShellによる確認方法：以下のコマンドを実行することにより、項目「state」がWindows Sandboxの機能が有効か否かで変化することを確認しました。ただし、図4及び図5の確認には管理者権限が必要になる場合があります。

コマンド：

```
Get-WindowsOptionalFeature -online -FeatureName "Containers-DisposableClientVM"
```

```
PS C:\Users\user > Get-WindowsOptionalFeature -online -FeatureName
 "Containers-DisposableClientVM“


FeatureName      : Containers-DisposableClientVM
DisplayName      : Windows サンドボックス
Description      : Windows サンドボックスのシナリオ実行に必要な依
                   存関係を有効にします。
RestartRequired  : Possible
State            : Enabled
CustomProperties :
```

図4：Windows Sandboxが有効の場合

```
PS C:\Users\user > Get-WindowsOptionalFeature -online -FeatureName
 "Containers-DisposableClientVM"


FeatureName      : Containers-DisposableClientVM
DisplayName      : Windows サンドボックス
Description      : Windows サンドボックスのシナリオ実行に必要な依
存関係を有効にします。
RestartRequired  : Possible
State            : Disabled
CustomProperties :
```

図5：Windows Sandboxが無効の場合

3-5 痕跡・検知策

（2）Windows Sandboxの実行痕跡確認

ア． イベントログ

Windows Sandboxの実行痕跡を確認するにあたり、以下のイベントログが有用な場合があります。例えば、イベントログを確認することで、Windows Sandboxの実行日時、サンドボックスとの共有フォルダ及びサンドボックスで実行されたコマンドの記録を見つけることができました。

他方、サンドボックス内でのファイルの実行及び作成、レジストリ及びタスクスケジューラの設定変更等、サンドボックスにのみ影響し、ホストコンピュータに影響がない動作については、ホストコンピュータのイベントログでは確認できませんでした。

イベントログ		主な記録内容
Windowsログ	セキュリティ	サンドボックスのログオンの記録
	システム	サンドボックスがネットワークに接続する時の記録
アプリケーションとサービスログ	Microsoft-Windows-Hyper-V-Compute/Operational	ホスト側からサンドボックスに対して実行したコマンドの記録
	Microsoft-Windows-Hyper-V-Worker/Admin	サンドボックスの起動や終了、仮想ネットワーク接続等の記録
	Microsoft-Windows-Hyper-V-Worker/Operational	サンドボックスとホスト側の共有フォルダ設定

表2：有用な場合があるイベントログ

3-6 痕跡・検知策

イ．実行痕跡確認例

○ イベントログ「セキュリティ」

イベントID: 4648

（確認情報）

① アカウント名：[実行の都度変化]

② アカウントドメイン：NT VIRTUAL MACHINE

③ プロセス名：
C:¥Windows¥System32¥vmcompute.exe

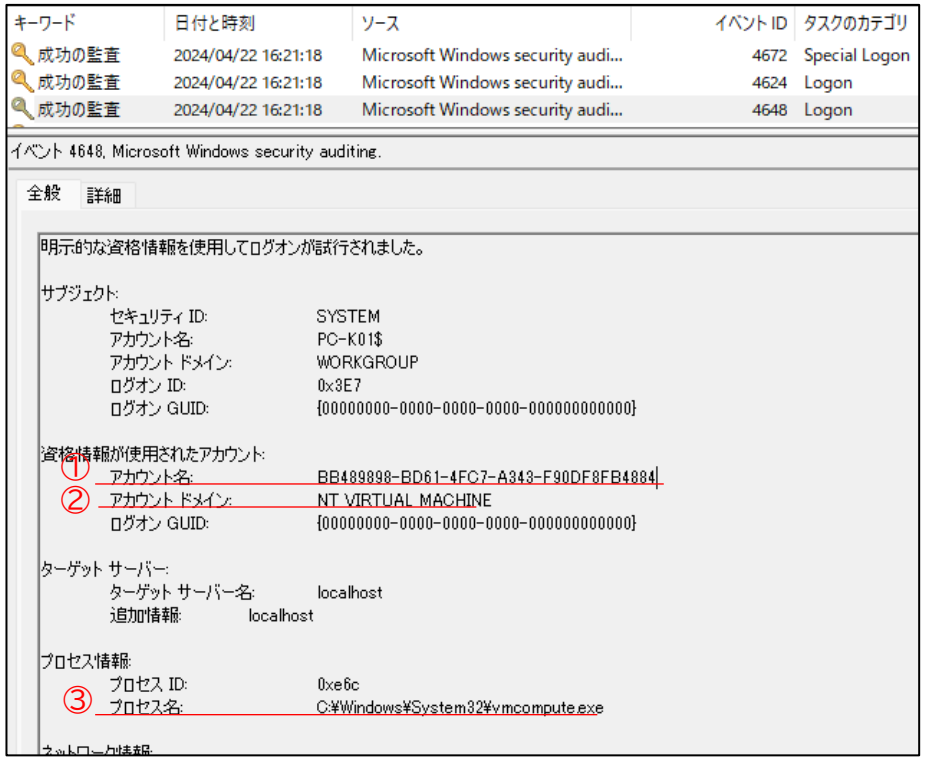


図6：イベントログ「セキュリティ」

3-7 痕跡・検知策

○ イベントログ
「Microsoft-Windows-Hyper-V-Compute/Operational」
イベントID: 2500

（確認情報）

① Windows Sandboxで実行されたコマンド

② コマンドを実行したユーザ：
WDAGUtilityAccount
（サンドボックスにデフォルトで存在するユーザ）

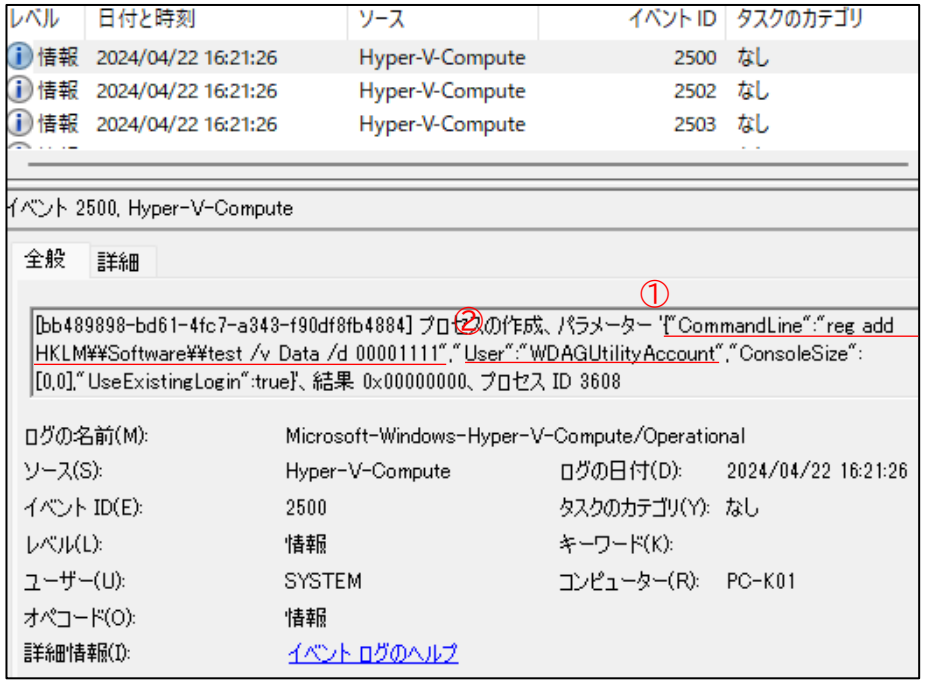


図7：イベントログ「 Microsoft-Windows-Hyper-V-Compute/Operational 」

3-8 痕跡・検知策

○ イベントログ
「Microsoft-Windows-Hyper-V-Worker/Operational」
イベントID: 301

（確認情報）

サンドボックスと共有したフォルダ名：

（例）C:¥Users

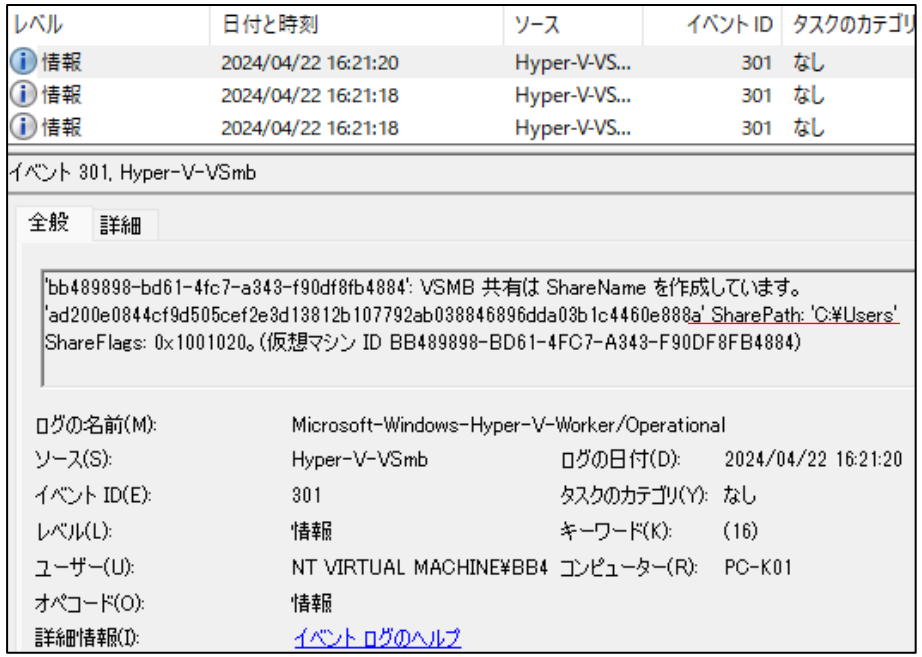


図8：イベントログ「 Microsoft-Windows-Hyper-V-Worker/Operational 」

3-9 痕跡・検知策

ウ. プロセス作成に関するイベントログ

デフォルトでは設定されていませんが、プロセス作成をイベントログに記録するように設定すると、Windows Sandboxの実行や使用したWindows Sandbox構成ファイルを把握することができます。

プロセス作成をイベントログに記録するにはグループポリシーを編集する必要があります。Windowsの検索ボックスに「gpedit.msc」と入力すると、グループポリシーの設定画面が表示されます。

※ グループポリシーの編集には管理者権限が必要です。慎重に設定を行ってください。

3-10 痕跡・検知策

○ プロセス作成を記録するためのグループポリシーの設定①

コンピューターの構成 → Windowsの設定 → セキュリティの設定 → 監査ポリシーの詳細な構成 → システム監査ポリシー - ローカル グループ ポリシー オブジェクト→ 詳細追跡

プロセス作成の監査を「成功および失敗」に変更

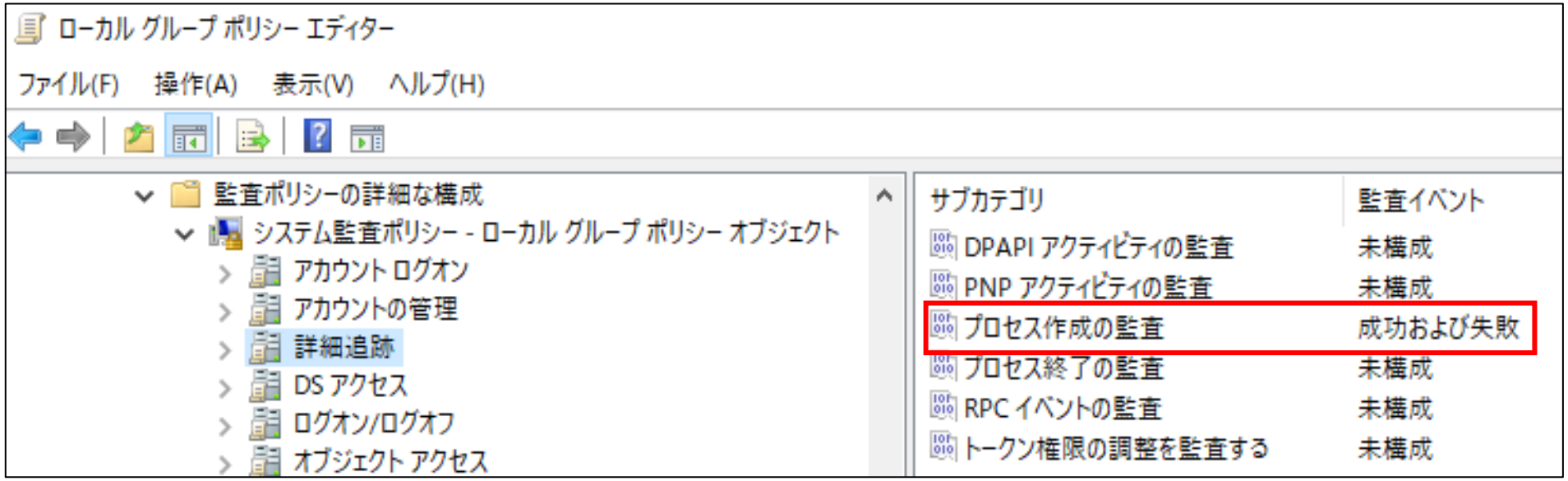


図9 :プロセス作成を記録するためのグループポリシーの設定①

3-11 痕跡・検知策

○ プロセス作成を記録するためのグループポリシーの設定②

コンピューターの構成 → 管理用テンプレート → システム → プロセス作成の監査

プロセス作成イベントにコマンドラインを含めるを「有効」に変更

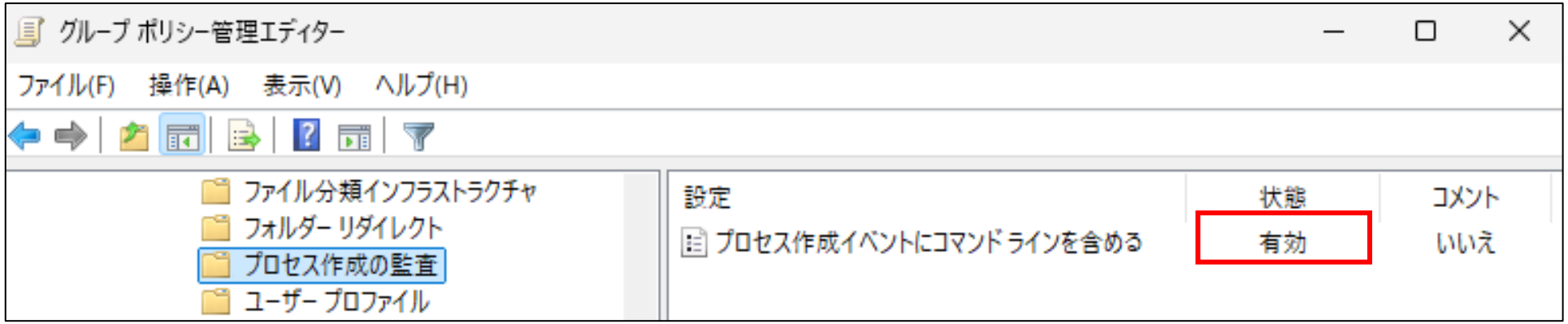


図10 :プロセス作成を記録するためのグループポリシーの設定②

3-12 痕跡・検知策

○ イベントログ「セキュリティ」
イベントID：4688

（確認情報）

プロセス作成を記録するよう設定したイベントログ「セキュリティ」において、Windows Sandboxのプロセス名及びWindows Sandbox構成ファイル（wsbファイル）のパス

① 新しいプロセス名
C:¥Windows¥System32¥WindowsSandbox.exe

② プロセスのコマンドライン：
Windows Sandbox構成ファイルのパス
（例）C:¥Windows¥System32¥{wsbファイル名}

図11：イベントログ「セキュリティ」

3-13 痕跡・検知策

エ. その他

サンドボックス内でのプログラム及びコマンドの実行は、サンドボックスのみに影響し、ホストコンピュータへの影響はありませんが、Windows Sandbox構成ファイル（wsbファイル）の設定によっては、ホストコンピュータへの影響が確認されました。

○ サンドボックスとの共有フォルダを、書き込みを許可する設定でマウントしている場合、ホストコンピュータへのファイル保存等の影響を受ける場合があります。

○ サンドボックスにおいてネットワーク利用を許可している場合、ホストコンピュータ側のネットワーク設定（プロキシ設定を含む）を利用して、サンドボックスから外部へ通信することができます。

○ 共有フォルダの設定及びサンドボックス内で実行するファイルを設定している場合、ホストコンピュータに保存されているプログラムをサンドボックス内で自動実行することができます。

参考文献

[1] https://learn.Microsoft.com/ja-jp/windows/security/application-security/application-isolation/windows-sandbox/windows-sandbox-overview

[2] https://learn.microsoft.com/ja-jp/windows/security/application-security/application-isolation/windows-sandbox/windows-sandbox-architecture

[3] https://learn.microsoft.com/ja-jp/shows/it-ops-talk/how-to-configure-windows-sandbox

[4] https://learn.microsoft.com/ja-jp/windows-hardware/manufacture/desktop/enable-or-disable-windows-features-using-dism