Microsoft

Windows Defender Advanced Threat Protection

攻撃シミュレーション

シナリオ 2: ファイルレス マルウェア攻撃の PowerShell スクリプト

Copyright

マイクロソフトの攻撃検出の指針

シンプルです。

高度で持続的な攻撃 (APT) の兆候や攻撃手法がテレメトリによって可視化されます。このため、迅速に攻撃の予兆を検知し関連するアラートを発行することができます。

アラートはほぼリアルタイムで発行されます。そのとき、攻撃者の属性、被害に関する情報、地理的な親和性、主な攻撃手法を含むコンテキストも提供します。このようなコンテキスト情報を提供できるのは、以前に実際のマシンで見つかった脅威コンポーネント、感染したサイトや悪意のあるサイトの IP、URL、そこで見つかったスクリプトまたは Web ページの一部、攻撃者のドメインなど、既知の攻撃のサインを集めたリッチでダイナミックなライブラリがあるからです。マイクロソフトでは、このライブラリを新しい脅威インテリジェンスで常に更新しています。脅威インテリジェンスは、独自の APT ハンティング & リサーチ チームが作成しているものですが、パートナーの協力や共有フィードを通じて内容が強化されています。

常に新しい脅威が生み出され、既存の脅威にも変更が加えられています。マイクロソフトでは、新しい未知の攻撃者の活動を特定するため、膨大な量の疑わしい動作や通常と異なる動作を監視しています。そして、疑わしい動作や通常と異なる動作が見つかると、アラートを発行し、セキュリティ オペレーション センター (SOC) のアナリストに問題の検証と対応を依頼します。SOC のアナリストは、同じマシンやその他の関連するマシンで発生している類似したイベントの情報に基づいて、実際のデータ侵害アクティビティの検証、リスクの判断、データ侵害範囲の特定、攻撃を封じ込めるアクティビティの定義を行います。その後、実際に攻撃を封じ込め、脅威を軽減することで、攻撃に対応します。

はじめに: ファイルレス マルウェア攻撃の PowerShell スクリプト

このシナリオでは、高度なテクニックを駆使して検出を逃れようとする、より洗練された攻撃を取り上げます。この種の攻撃は、通常、攻撃したマシンにファイルをドロップすることはなく、メモリ上で実行されます。既存のシステムと管理ツールだけを使用し、システム プロセス内にコードを注入することにより、セキュリティ対策の検知の目をくぐろうとするのです。

ここでは、この種のファイルレス マルウェア攻撃のシミュレーションを行い、Windows 10 の Exploit Protection 機能を利用して、攻撃者が悪意のあるアクティビティを実行するのを阻止する方法を紹介します。

このシミュレーションのシナリオは、PowerShell スクリプトからスタートします。ユーザーが騙されてスクリプトを実行してしまうこともあれば、横移動をねらう攻撃者が、以前に感染させた組織内の別のマシンからリモート操作でスクリプトを実行することもあります。このようなスクリプトの検出は困難です。なぜなら、正規の管理者も、リモート操作でスクリプトを実行してさまざまな管理タスクを実行するからです。

このシミュレーションでは、攻撃者は一見無害なプロセス (ここでは notepad.exe) にシェルコードを注入します。ただし、実際の攻撃者は、svchost.exe のような常駐型のシステム プロセスをターゲットにする場合が多いでしょう。注入されたシェルコードは、攻撃者のコマンド アンド コントロール (C&C) サーバーを通じて、攻撃の指示を受け取ります。

このシミュレーションで使用するマシンの条件は、次のとおりです。

- Windows Defender ATP のオンボーディングが完了している
- Windows 10 Fall Creators Update (バージョン 1709 以上) を実行している
- PowerShell が有効になっている
- Windows Defender ウイルス対策が有効になっている

オンボーディングの方法については、製品ガイドをお読みください。テスト マシンのオンボーディングを行うには、ローカルのオンボーディング スクリプトを実行することをお勧めします。

攻撃シミュレーション シナリオ 2: ファイルレス マルウェア攻撃の PowerShell スクリプト

シミュレーションの実行

この攻撃シナリオを実行するには、次の手順に従います。

1. 指定されたテスト マシンで Windows Defender ATP ポータルにログインし、**[Help (?)] > [Simulations & tutorials]** を選択します。

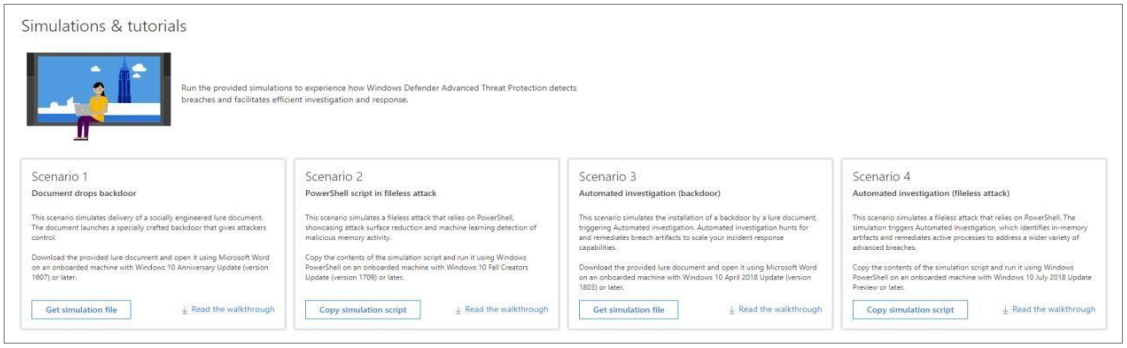

図 1: ポータル内のシミュレーション シナリオ

2. **[Scenario 2: PowerShell script in fileless attack]** の下の **[Copy simulation script]** ボタンをクリックして PowerShell スクリプトをコピーします。

3. テストマシンで、管理者権限を使用し Windows PowerShell ウィンドウを開きます。

4. プロンプトが表示されたら、スクリプトを貼り付けて実行します。

   数秒後、notepad.exe が起動し、シミュレーションの攻撃コードが注入されます。この攻撃コードは、シミュレーションで使用する C&C サーバーを示す外部 IP アドレスへの通信を試みます。

攻撃とエクスプロイト対策のシミュレーション

Windows 10 Fall Creators Update (バージョン 1709) の Exploit Protection を使用すると、ポリシーを適用して、マシン上のコードの実行を制限することができます。これにより、多くのエクスプロイト攻撃を軽減することができます。エクスプロイトが検出されると、Windows Defender ATP からアラートが発行され、SOC の担当者にイベントが通知されます。

このセクションでは、所定のプロセスで notepad.exe 内の動的なコード実行を却下するように Exploit Protection を設定してから、シミュレーションの攻撃を再度実行します。

攻撃とエクスプロイト対策のシミュレーションを行うには、次の手順に従います。

1. 管理者権限で Windows PowerShell ウィンドウを開きます。

2. プロンプトが表示されたら、次のコマンドを実行してエクスプロイト対策の設定を行います。

```
$path = “HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options\runtimebroker.exe”;
$value =
([byte[]](0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x11,0x11,0x01
,0x01,0x00,0x00));
New-Item -Path $path -Force;
New-ItemProperty -Path $path -Name “MitigationOptions” -Value $value
-PropertyType
Binary -Force
```

   注: この設定は、関連する機能について説明する目的で提供されています。どのような影響があるか適切な分析を行わずに、実稼働環境内の他のマシンに適用しないでください。

3. **[Simulations & tutorials]** ページから入手した PowerShell スクリプトを再度実行します。

   前回と同様に、notepad.exe が実行され、悪意のあるシェルコードが注入さ

れ、その実行が試みられますが、今回はエクスプロイト対策の設定のおかげで、シェルコードの実行が阻止され、notepad.exe は終了します。

4. [オプション] テスト マシン上のエクスプロイト対策の設定を元に戻すには、PowerShell ウィンドウで次のコマンドを実行します。

```
Remove-ItemProperty -Path $path -Name “MitigationOptions” -Force
```

お疲れ様です。シミュレーションが完了しました。

これで攻撃シミュレーションは終わりです。実際の攻撃者は、多くの場合、情報のスキャンを続け、収集した偵察情報をコマンド アンド コントロール (C&C) サーバーに送信し、この情報を利用して他の魅力的なターゲットに横移動します。

次に、シミュレーションの攻撃を知らせる Windows Defender ATP アラートについて見ていきましょう。

✎ **注**: アラートは、バックドア型マルウェアのシミュレーションの実行後 15 ～ 30 分で発行され始めます。

ポータル内の攻撃の調査

ここからは、防御者の役割に切り替えて、Windows Defender ATP ポータルから SOC の視点で攻撃を分析していきましょう。

1. 任意のマシンから https://securitycenter.windows.com にアクセスし、Windows Defender ATP ポータルを開きます。

2. Windows Defender ATP の資格情報を使ってログインします。サインアップ時のメールでは、既定のグローバル管理者の資格情報が提供されます。

3. シミュレーションの攻撃から 15 ～ 30 分経つと、ダッシュボードに複数の新しいアラートが表示されます。

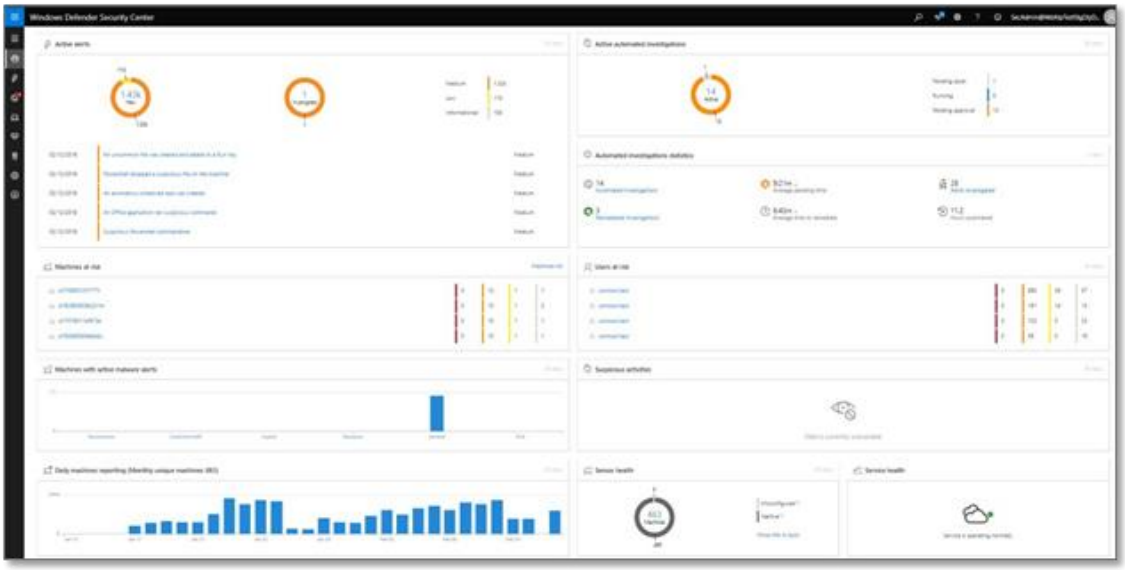

図 2: ダッシュボード上のアラート

攻撃シミュレーション シナリオ 2: ファイルレス マルウェア攻撃の PowerShell スクリプト

4. **[Machines at risk]** ウィジェットで、テスト マシンをクリックしてマシンとすべての関連アラートの詳細を表示します。

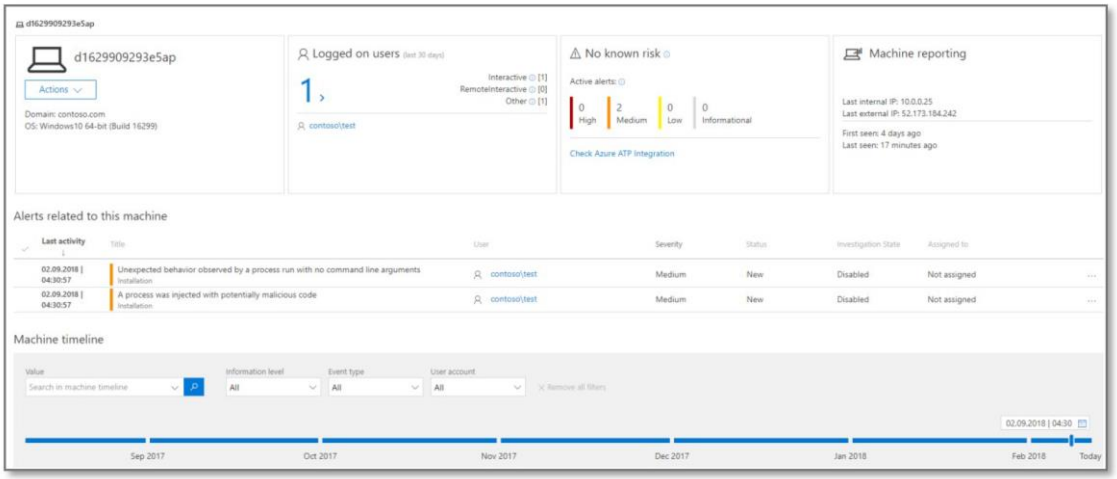

図 3: 被害を受けたマシンとアラート

攻撃シミュレーション シナリオ 2: ファイルレス マルウェア攻撃の PowerShell スクリプト

生成されたアラートの確認

シミュレーションの攻撃で生成されたいくつかのアラートを見ていきましょう。

アラート: Suspicious process injection observed

高度な攻撃者は、より洗練された巧妙な手口でメモリ内にとどまり、検出ツールから身を隠そうとします。彼らがよく使用するテクニックは、悪意のある実行可能ファイルではなく信頼されたシステム プロセスから攻撃を仕掛けることです。そうすることで、悪意のあるコードが検出ツールやセキュリティ オペレーションに特定されにくくなります。

SOC の担当者がこうした高度な攻撃を捕捉できるようにするには、Windows Defender ATP を使用します。Windows Defender ATP のディープ メモリ センサーを使用すれば、クラウド サービスで、各種クロスプロセス インジェクション技術を特定できるようになります。その精度はかつてないほど高くなっています。以下に示すように、Windows Defender ATP は notepad.exe にコードを注入する試みを検出し、アラートを発行します。

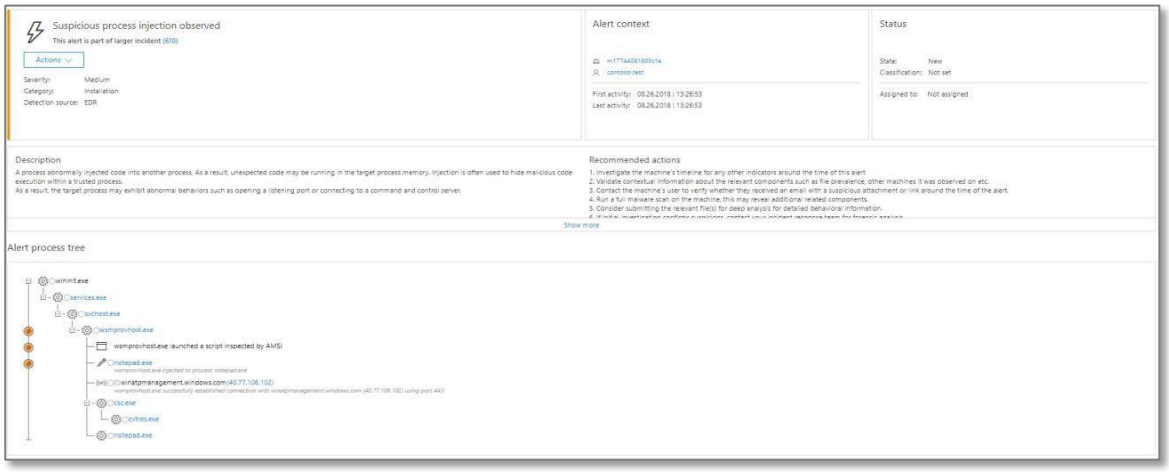

図 4: 悪意のあるコードの注入を警告するアラート

攻撃シミュレーション シナリオ 2: ファイルレス マルウェア攻撃の PowerShell スクリプト

アラート: Unexpected behavior observed by a process run with no command line arguments

Windows Defender ATP はしばしば、攻撃テクニックの最も不変的な部分をターゲットにします。そうすることで、耐久性が増し、攻撃者が新しい戦術に切り替えるのが難しくなります。

マイクロソフトでは、大規模な学習アルゴリズムを利用して、組織内または世界的に一般的なプロセスの標準動作を定義しています。この標準動作に照らあわせて、プロセスの動作に異常がないかを監視します。ここでは異常な動作は、信頼されたプロセス内で不正な外部コードが実行されていることを示します。

この例では、よく知られたプロセスの notepad.exe が外部と通信しています。これは異常な動作とみなされます。これは、悪意のあるコードを導入、実行するために使用された特定の方法とは関係がありません。

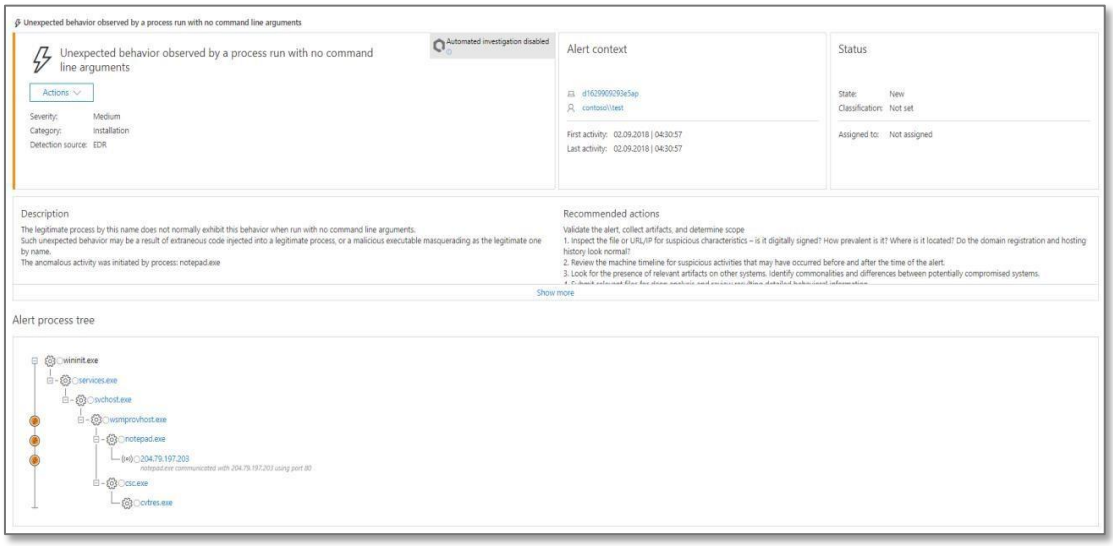

図 5: プロセス実行による予期せぬ動作が発生した際のアラート

✎ **注**: このアラートは、バックエンド プロセスを必要とする機械学習モデルに基づいて発行されています。このため、ポータル上でアラートが生成されるのに少し時間がかかることがあります。

アラートの詳細ページには、外部 IP アドレスも含まれています。この IP アドレスをピボット ポイントとして利用して、調査を拡張することができます。**アラート プロセス ツリー**内で IP アドレスをクリックすると、その IP アドレスの詳細ページが開きま

す。

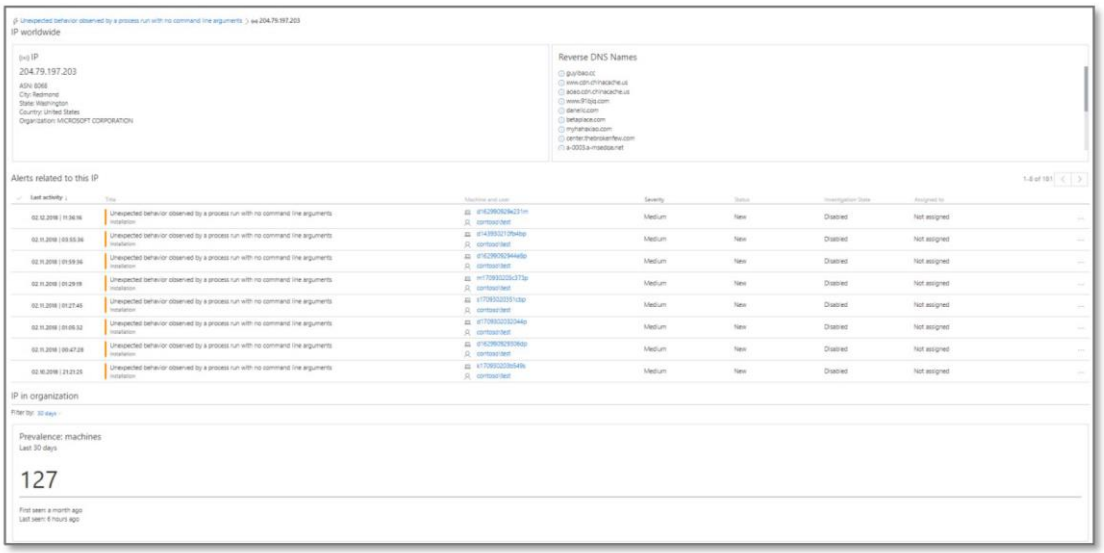

図 6: IP アドレスの詳細ページ

アラート: EAF violation blocked by exploit protection

Exploit Protection 機能を有効にして、予期しないコードの実行の被害を受けたマシンのセキュリティを高めています。特に、notepad.exe における予期しないコード実行を検出、阻止するエクスプロイト対策ルールを有効化しています。その結果、注入されたシェルコード実行の試みが検出、ブロックされ、攻撃の進行が停止します。

Exploit Protection 機能が攻撃を検出すると、Windows Defender ATP ポータルで [EAF violation blocked by exploit protection] アラートも発行されます。アラートの重要度のレベルは [Informational] になっています。これは攻撃が停止したからです。ただし、セキュリティ チームには、エクスプロイトの試みがあったという通知が送信されます。セキュリティ チームは、この通知に基づいて事前に予防策を講じ、しつこい攻撃者のアラートを警戒することができます。

攻撃シミュレーション シナリオ 2: ファイルレス マルウェア攻撃の PowerShell スクリプト

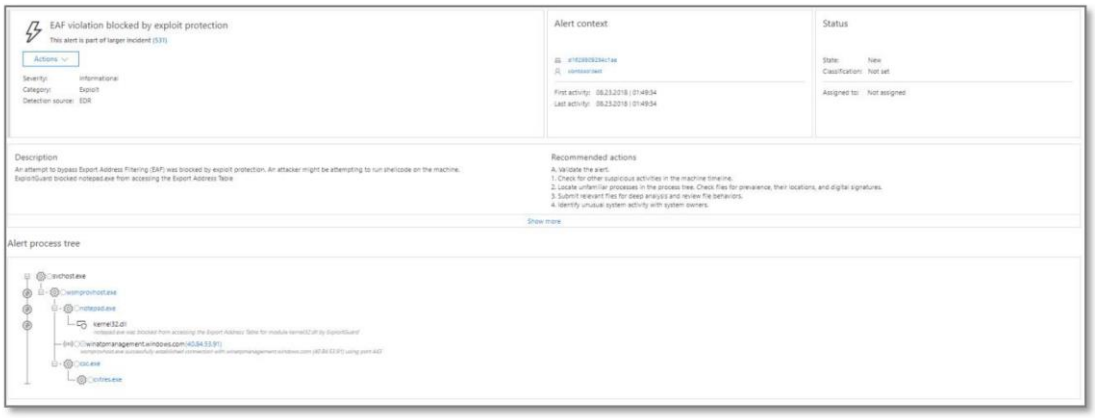

図 7: Exploit Protection 機能によって検出された EAF 違反のアラート

攻撃シミュレーション シナリオ 2: ファイルレス マルウェア攻撃の PowerShell スクリプト

まとめ

ここでは、メモリを用いた高度な攻撃をシミュレーションし、Windows Defender ATP がディープ OS センサーを利用して、ステルス性の高い悪意のあるアクティビティを検出し、アラートを発行ことを確認しました。また、Exploit Protection 機能を使って、高度な攻撃を阻止し、ポータルにアラート情報を表示する方法についても確認しました。さらに、他のコンテキスト情報と一緒にアラートが配信される方法も確認しました。SOC 担当者は、アラートに基づいて調査を行い、必要な措置を取ることができます。

シミュレーションを楽しんでいただけましたら幸いです。他の機能もぜひ利用してみてください。詳細については、製品ガイド (docs.microsoft.com) をご覧ください。

また、Windows Defender ATP ポータルのフィードバック アイコンから、このシミュレーションや製品に関するご意見、ご感想をお寄せください。お寄せいただいたご意見やアイデアは、今後のシミュレーションやチュートリアルのために利用させていただきます。ご協力よろしくお願いいたします。