セキュアエンドポイントの除外の設定と特定

内容

はじめに
免責事項
概要
除外の概要
- シスコが維持する除外
- カスタム除外

除外のタイプ
- プロセスの除外
  - MacOSおよびLinux
  - Windows
- 脅威の除外
- パスの除外
  - 部分的なパスの一致（Windowsのみ）
- ファイル拡張子の除外
- ワイルドカード除外
  - Windows
- 実行可能ファイルの除外（Windowsのみ）
- IOCの除外（Windowsのみ）

CSIDLおよびKNOWNFOLDERID（Windowsのみ）
除外チューニング用のコネクタの準備
除外の識別
- MacOSおよびLinux
  - プロセスの除外の作成
  - パス、ファイル拡張子、およびワイルドカードの除外の作成
  - 動作保護エンジン
- Windows

セキュアエンドポイントコンソールでの除外ルールの作成
ベスト プラクティス
- 推奨されない除外

関連情報

はじめに

このドキュメントでは、Cisco Secure Endpointで除外される項目、除外される項目の識別方法、および除外される項目を作成する際のベストプラクティスについて説明します。

免責事項

このドキュメントの情報は、Windows、Linux、およびmacOSオペレーティングシステムに基づ

くものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

このドキュメントを読み終えたら、次の項目について理解する必要があります。

- 除外の概要と、Cisco Secure Endpointで使用できるさまざまな除外タイプ
- 除外チューニング用にコネクタを準備する方法
- 強力な可能性がある除外を特定する方法
- Cisco Secure Endpoint Consoleで新しい除外を作成する方法
- 除外を作成する際のベストプラクティス

除外の概要

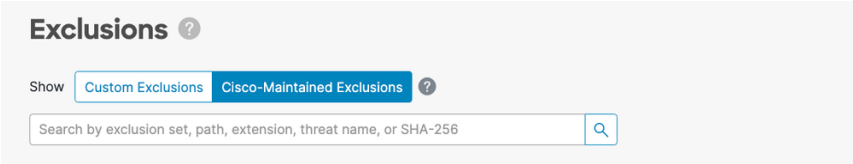
除外セットとは、コネクタによるスキャンや処罰の対象から除外するディレクトリ、ファイル拡張子、ファイルパス、プロセス、脅威名、アプリケーション、または侵入の痕跡のリストです。Secure Endpointなどのエンドポイント保護が有効な場合、マシンのパフォーマンスとセキュリティのバランスを保つために、除外は慎重に作成する必要があります。この記事では、Secure Endpoint Cloud、TETRA、SPP、およびMAPの除外について説明します。

あらゆる環境は、その環境を制御するエンティティと同様に、厳格なポリシーからオープンなポリシーまで異なります。したがって、除外は状況に応じて個別に調整する必要があります。

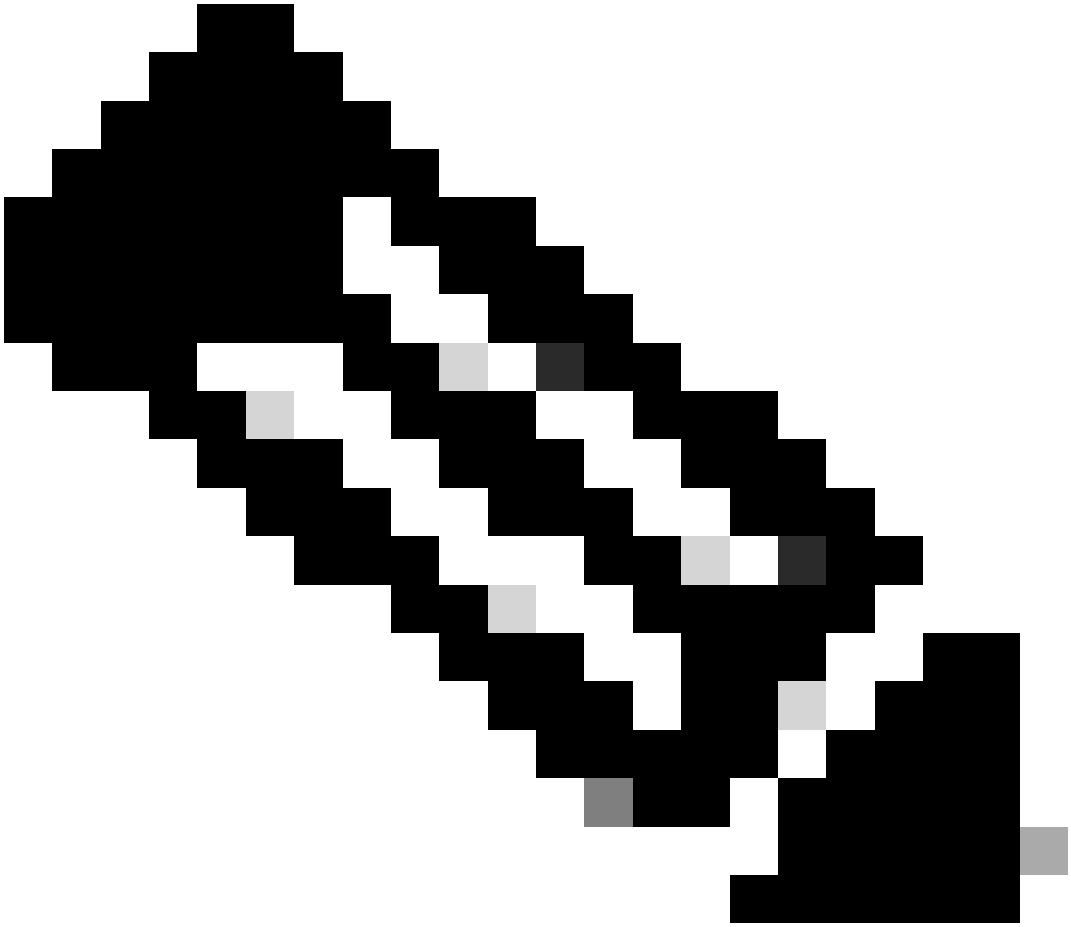
除外は、Cisco-Maintained除外とカスタム除外の2つの方法で分類できます。

シスコが維持する除外

シスコが管理する除外は、調査に基づいて作成され、一般的に使用されるオペレーティングシステム、プログラム、およびその他のセキュリティソフトウェアについて厳格なテストを受けた除外です。これらの除外を表示するには、Secure Endpoint ConsoleのExclusionsページでCisco-Maintained Exclusionsを選択します。



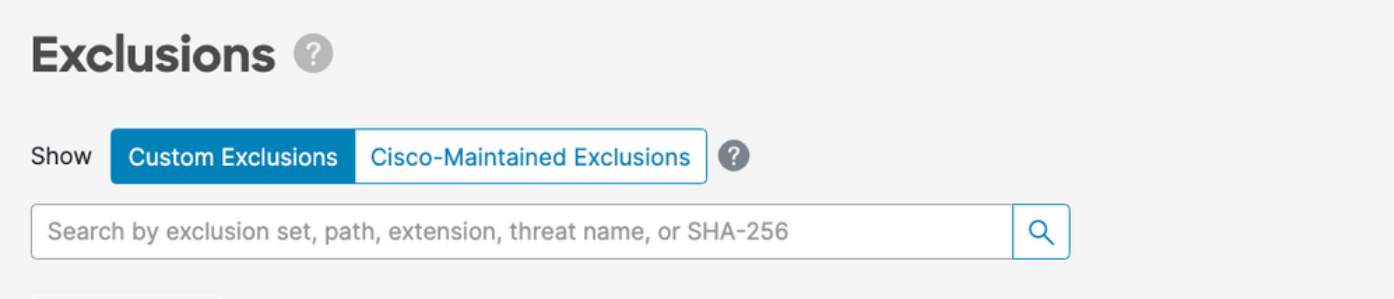
シスコは、アンチウイルス(AV)ベンダーによって公開された推奨される除外リストを監視し、推奨される除外を含むようにシスコが維持する除外を更新します。



注：一部のAVベンダーは、推奨される除外を公開していません。この場合は、AVベンダーに問い合わせて推奨される除外リストを要求し、サポートケースをオープンしてCisco-Maintained除外リストを更新する必要があります。

カスタム除外

カスタム除外は、エンドポイントのカスタムのユースケースのためにユーザーによって作成された除外です。これらの除外は、Secure Endpoint ConsoleのExclusions ページでCustom Exclusions を選択することで表示できます。



除外のタイプ

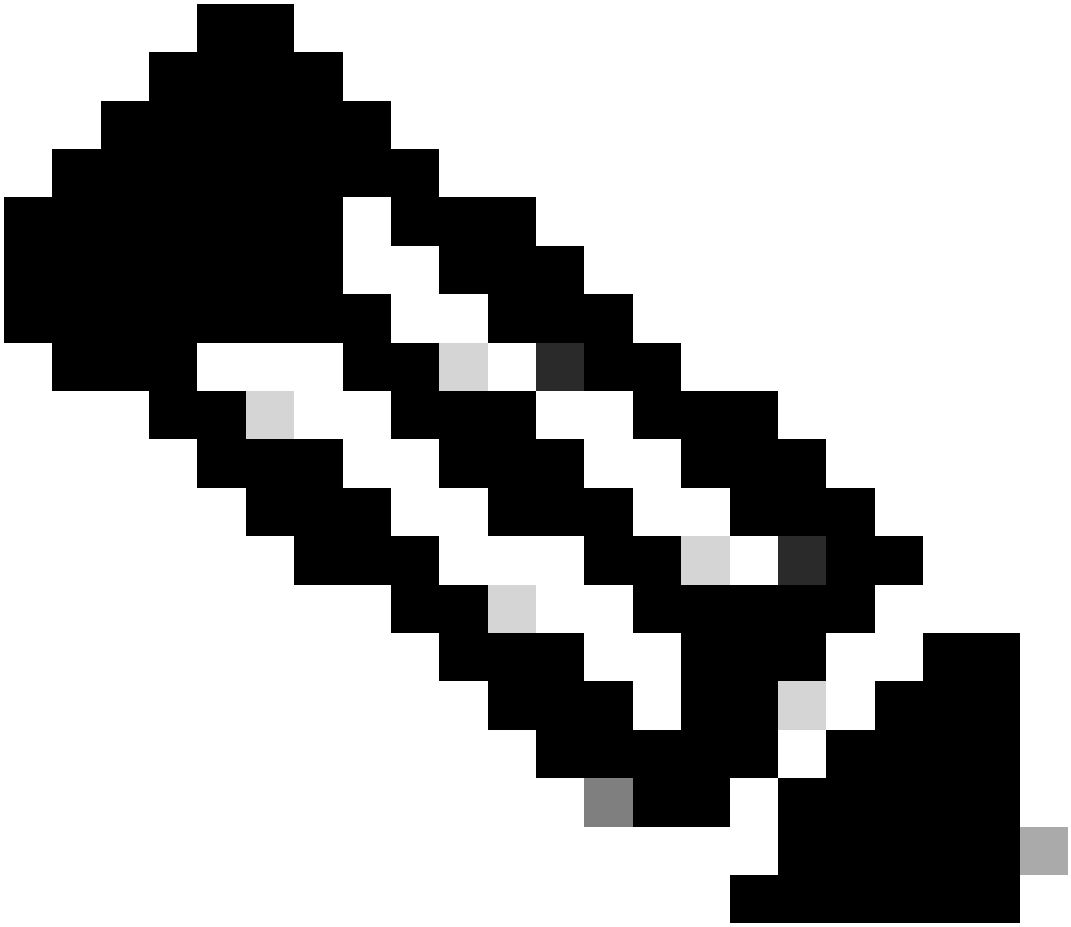
プロセスの除外

プロセスの除外により、管理者はサポートされているエンジンからプロセスを除外できます。次の表に、各プラットフォームでプロセス除外をサポートするエンジンを示します。

オペレーティング システム	[Engine]			
	ファイルスキャン	システムプロセスの保護	悪意のあるアクティビティの保護	動作保護
Windows	✓	✓	✓	✓
Linux	✓	✗	✗	✓
MacOS	✓	✗	✗	✓

MacOSおよびLinux

プロセス除外を作成するときは、絶対パスを指定する必要があります。オプションのユーザーを指定することもできます。パスとユーザーの両方を指定した場合、プロセスを除外するには両方の条件を満たす必要があります。ユーザーを指定しない場合、プロセスの除外はすべてのユーザーに適用されます。



注:macOSおよびLinuxでは、プロセスの除外はすべてのエンジンに適用されます。

プロセスワイルドカード：

セキュアエンドポイントLinuxおよびmacOSコネクタは、プロセスの除外内でワイルドカードを使用してサポートします。これにより、除外される項目が少ない広範なカバレッジが可能になりますが、定義されていない項目が多すぎる場合は危険です。必要な除外を指定するために必要な最小限の文字数をカバーするには、ワイルドカードのみを使用する必要があります。

macOSおよびLinuxでのプロセスワイルドカードの使用：

- ワイルドカードは、1つのアスタリスク(*)を使用して表されます
- ワイルドカードは、単一文字またはディレクトリ全体の代わりに使用できます。
- パスの先頭にワイルドカードを配置することは無効と見なされます。
- ワイルドカードは、スラッシュまたは英数字の2つの定義済み文字の間で機能します。

例:

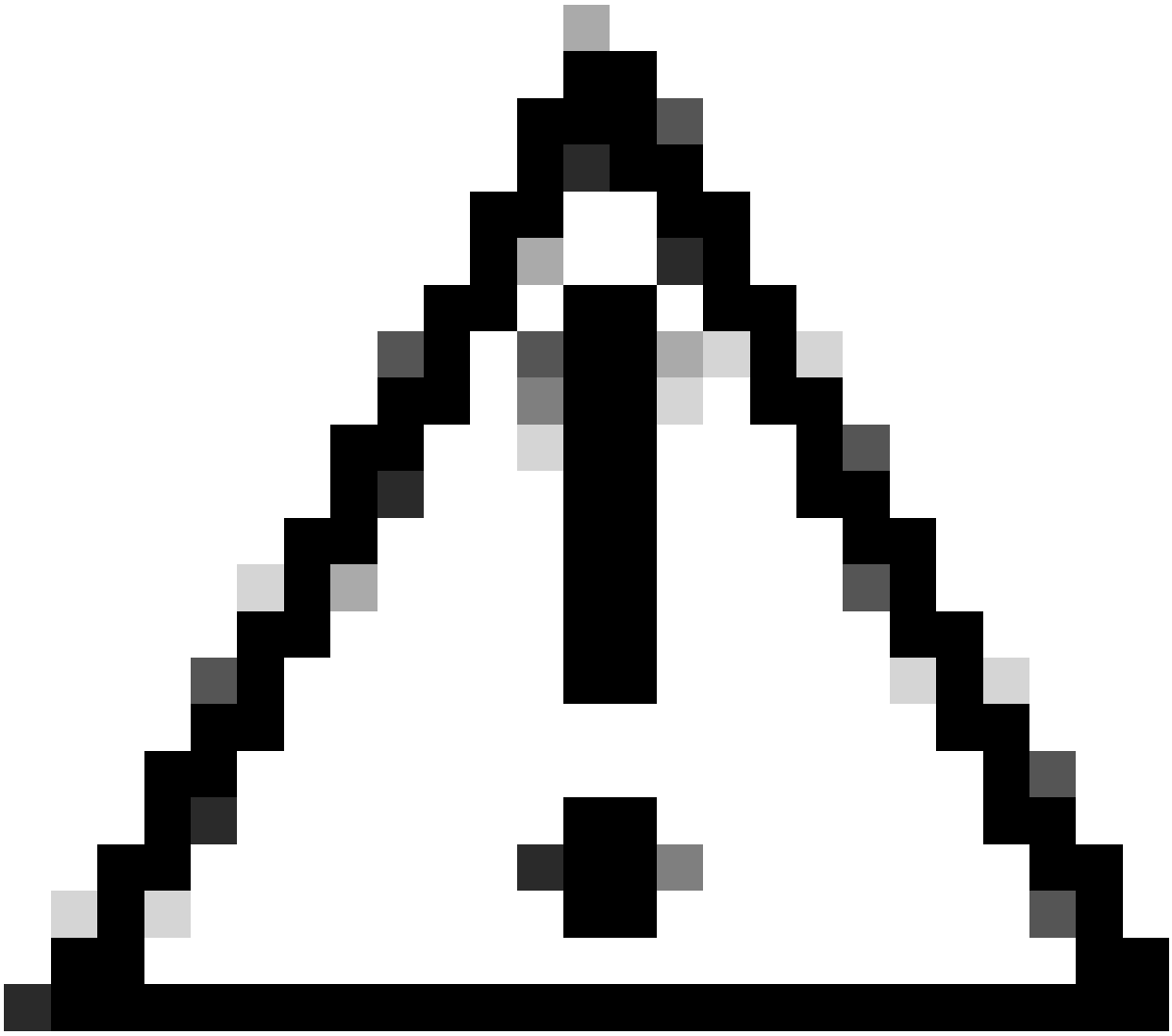
除外	予想される結果

/Library/Java/Java仮想マシン/*/java	JavaVirtualMachinesのすべてのサブフォルダ内のjavaを除外
/Library/Jibber/j*bber	jabber、jibber、jobberなどのプロセスを除外

Windows

プロセスの除外を作成する際に、プロセス実行可能ファイルの絶対パスまたはSHA-256を指定できます。パスとSHA-256の両方を指定した場合、プロセスを除外するには両方の条件を満たす必要があります。

Windowsでは、パス内でCSIDLまたはKNOWNFOLDERIDを使用して、プロセス除外を作成することもできます。

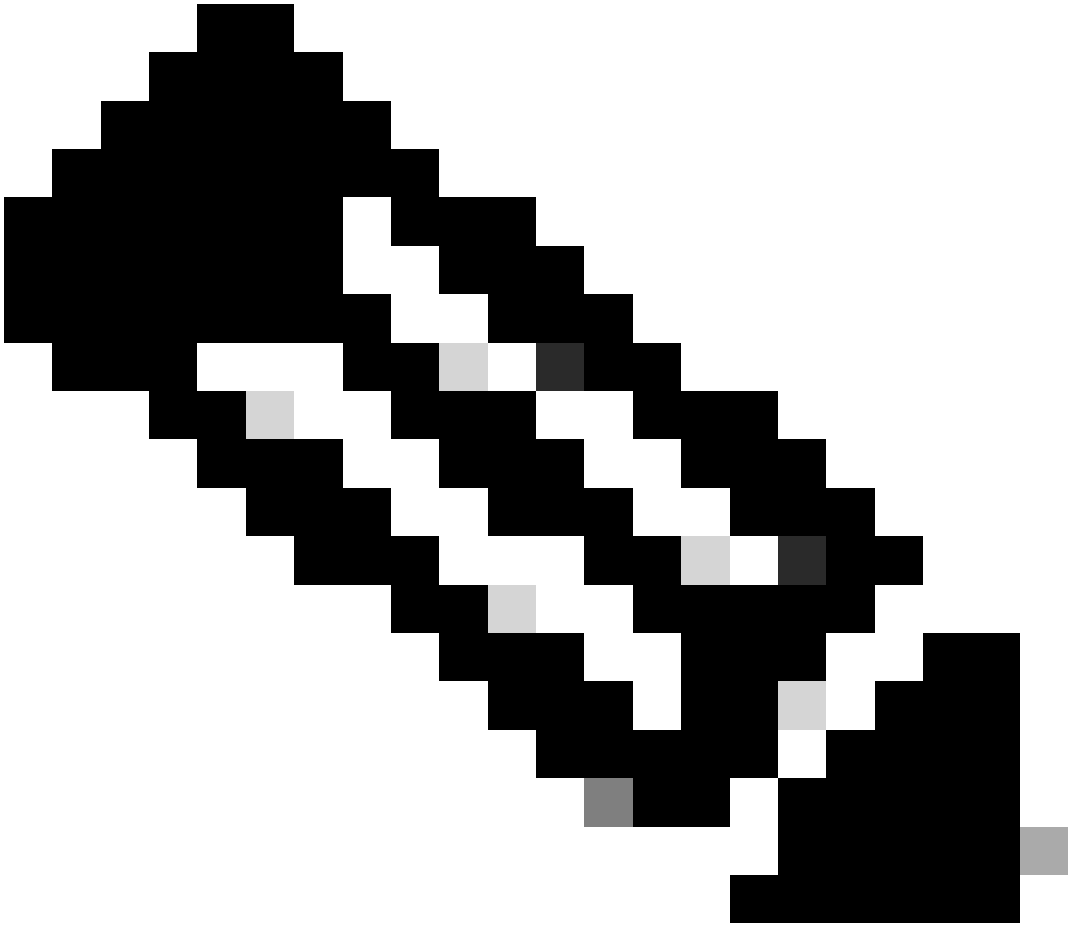


注意：除外されたプロセスによって作成された子プロセスは、デフォルトでは除外されません。プロセスの除外を作成するときに追加のプロセスを除外するには、Apply to Child Processesを選択します。

制限：

- プロセスのファイルサイズ（バイト）がポリシーで設定されているスキャンファイルの最大サイズよりも大きい場合、プロセスのSHA-256は計算されず、除外は機能しません。最大スキャンファイルサイズよりも大きいファイルには、パスベースのプロセス除外を使用します。
- Windowsコネクタでは、すべてのプロセス除外タイプに対して500件のプロセス除外の制限が課されています。
  - プロセスの除外は、policy.xmlのプロセス除外リストの先頭から、上限まで有効です。
  - すべてのWindowsポリシーにはsfc.exeのプロセス除外があり、プロセス除外の制限にカウントされます。

```
3|0||CSIDL_Secure Endpoint_VERSION\sfc.exe|48|
```



注:Windowsでは、プロセスの除外はエンジンごとに適用されます。同じ除外を複数のエンジンに適用する必要がある場合は、該当するエンジンごとにプロセスの除外を複製する必要があります。

プロセスワイルドカード：

Secure Endpoint Windowsコネクタは、プロセスの除外内のワイルドカードを使用してサポートします。これにより、除外される項目が少ない広範なカバレッジが可能になりますが、定義されていない項目が多すぎる場合は危険です。必要な除外を指定するために必要な最小限の文字数をカバーするには、ワイルドカードのみを使用する必要があります。

Windowsのプロセスワイルドカードの使用：

- ワイルドカードは、単一のアスタリスク(*)または二重のアスタリスク(**)を使用して表されます
- アスタリスクのワイルドカード(*):
  - ワイルドカードは、単一文字またはディレクトリ全体の代わりに使用できます。

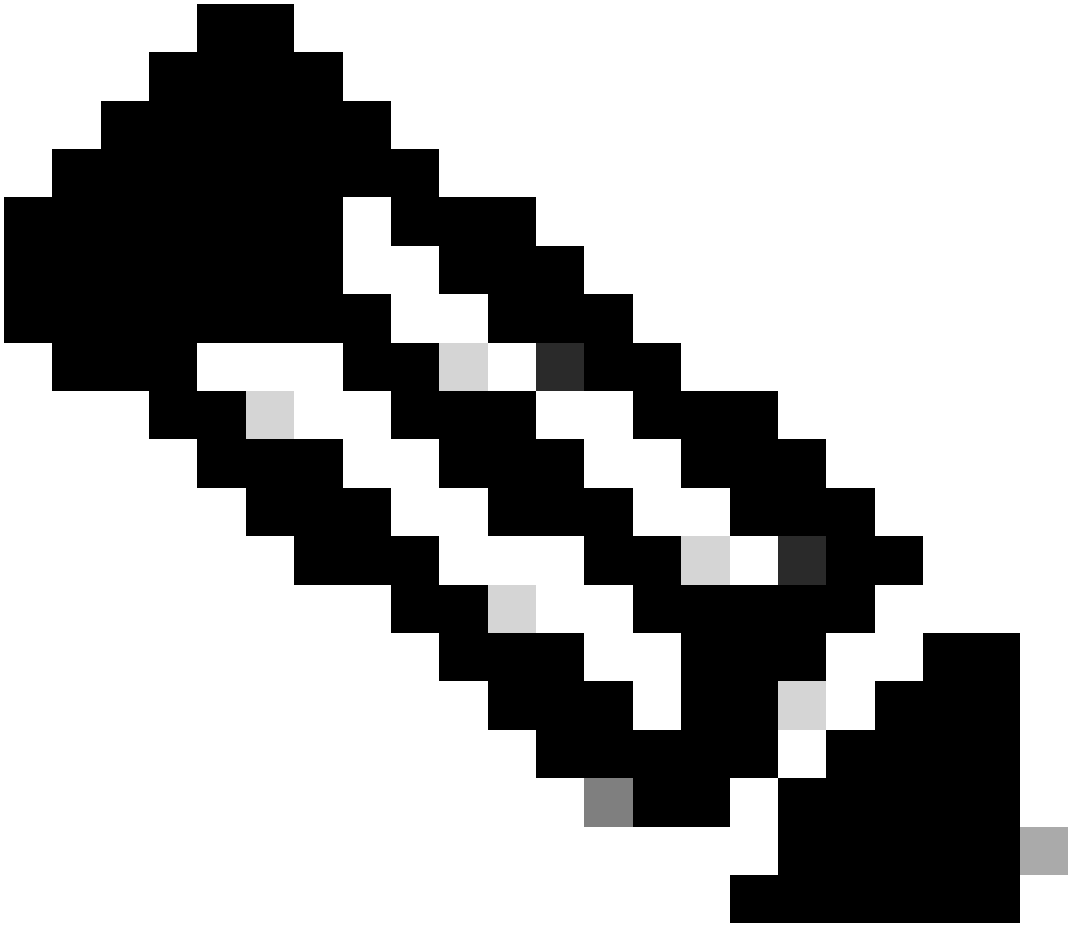
    - パスの先頭にワイルドカードを配置することは無効と見なされます。
    - ワイルドカードは、スラッシュまたは英数字の2つの定義済み文字の間で機能します。
    - パスの最後にワイルドカードを置くと、そのディレクトリ内のすべてのプロセスが除外され、サブディレクトリは除外されません。
- ダブルアスタリスクのワイルドカード(**):
    - パスの終端にのみ配置できます。
    - パスの最後にワイルドカードを置くと、そのディレクトリ内のすべてのプロセスとサブディレクトリ内のすべてのプロセスが除外されます。
    - これにより、最小限の入力で非常に大きな除外セットが可能になりますが、可視性のために非常に大きなセキュリティホールが残ります。この機能は、細心の注意を払って使用してください。

例:

除外	予想される結果
C:\Windows*\Tiworker.exe	Windowsのサブディレクトリにあるすべての Tiworker.exeプロセスを除外します
C:\Windows\P*t.exe（登録ユーザ専用）	Pot.exe、Pat.exe、P1t.exeなどを除く
C:\Windows*chickens.exe	chickens.exeで終わるWindowsディレクトリのすべてのプロセスを除外します
C:*	C：ドライブ内のすべてのプロセスを除外しますが、サブディレクトリ内のプロセスは除外しません
C:**	C：ドライブ上のすべてのプロセスを除外

脅威の除外

脅威の除外では、特定の脅威名をトリガーイベントから除外できます。脅威の除外は、イベントが誤検出の結果であることが確実な場合にのみ使用する必要があります。この場合、脅威の除外としてイベントからの正確な脅威名を使用します。このタイプの除外を使用する場合は、脅威名の真正検出も検出されず、隔離されず、イベントも生成されないことに注意してください。



注：脅威の除外では、大文字と小文字は区別されません。例：W32.Zombies.NotAVirusとw32.zombies.notavirusは両方とも同じ脅威名に一致します。

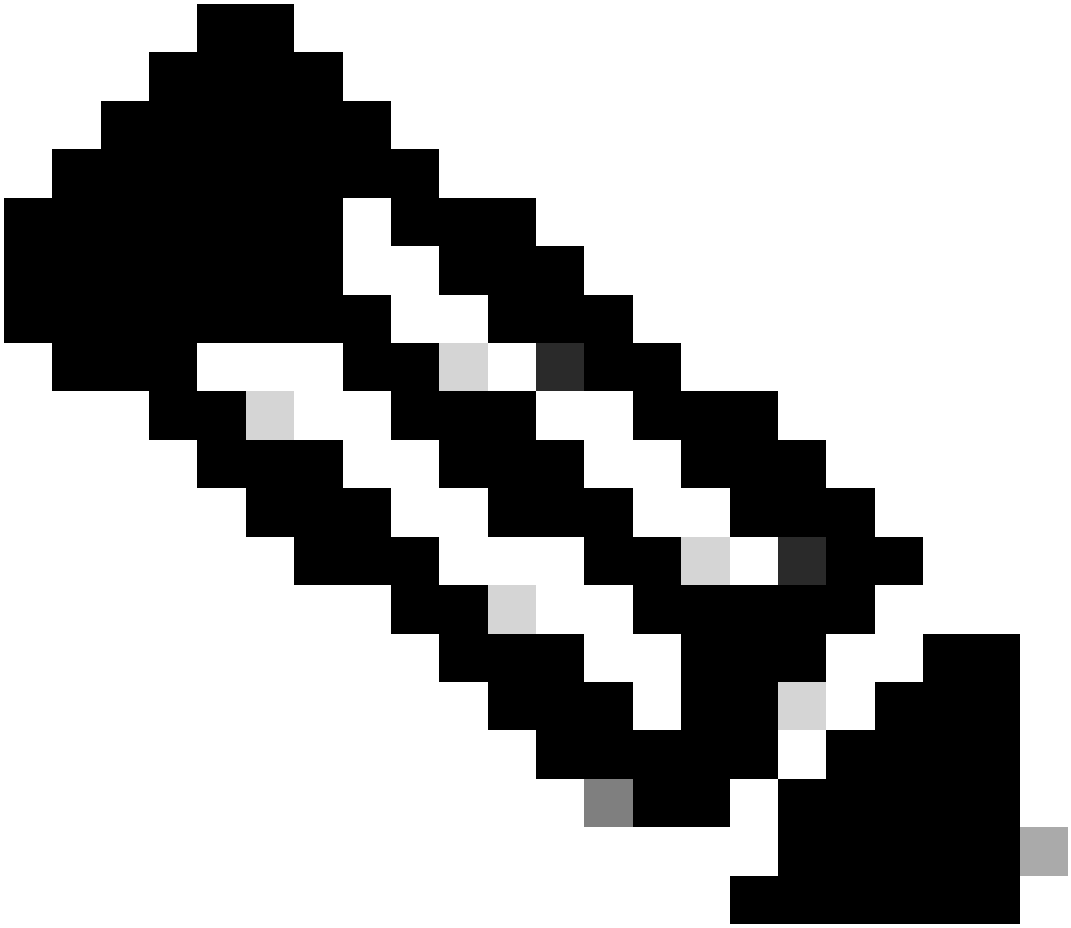
警告：徹底的な調査により脅威名が誤検出されていることが確認された場合を除き、脅威を除外しないでください。除外された脅威は、レビューと監査のイベントタブに表示されなくなりました。

パスの除外

アプリケーションの競合は通常、ディレクトリの除外を伴うため、パスの除外が最もよく使用されます。絶対パスを使用してパス除外を作成できます。Windowsでは、CSIDILまたはKNOWNFOLDERIDを使用してパスの除外を作成することもできます。

たとえば、WindowsのProgram Filesディレクトリ内のAVアプリケーションを除外するには、除外パスとして次のいずれかのパスを指定します。

```
C:\Program Files\MyAntivirusAppDirectory
CSIDL_PROGRAM_FILES\MyAntivirusAppDirectory
FOLDERID_ProgramFiles\MyAntivirusAppDirectory
```



注：パスの除外は再帰であり、すべてのサブディレクトリも除外されます。

部分的なパスの一致（Windowsのみ）

パスの除外に末尾のスラッシュが指定されていない場合、Windowsコネクタはパスの部分一致を行います。MacおよびLinuxでは、部分的なパス一致はサポートされていません。

たとえば、Windowsで次のパス除外を適用する場合は、次の手順を実行します。

```
C:\Program Files
C:\test
```

次に、これらすべてのパスが除外されます。

```
C:\Program Files
C:\Program Files (x86)
C:\test
C:\test123
```

C:\testからの除外をC:\test\に変更すると、C:\test123は除外されなくなります。

ファイル拡張子の除外

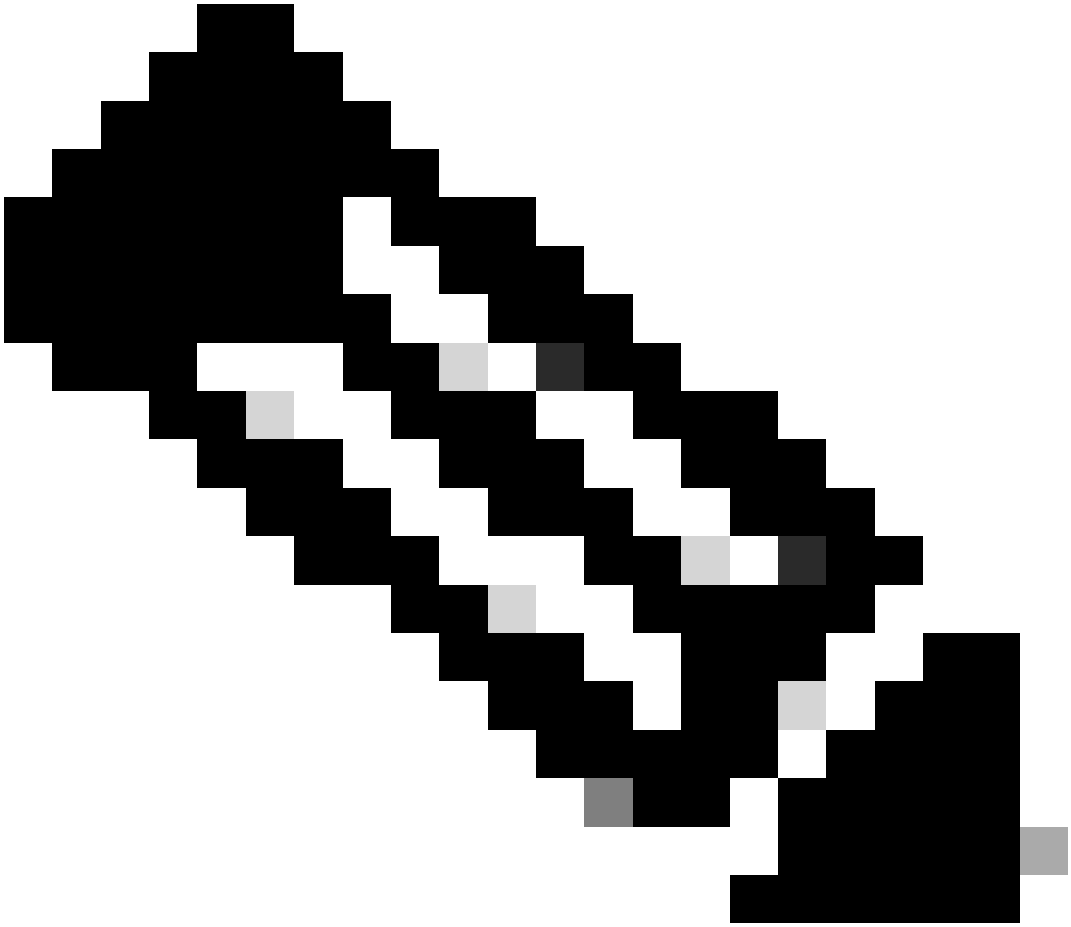
ファイル拡張子の除外では、特定の拡張子を持つすべてのファイルを除外できます。

キー ポイント：

- セキュアエンドポイントコンソールに必要な入力は.extensionです。
- ファイル拡張子が追加されていない場合は、Secure Endpoint Consoleによって自動的にピリオドがファイル拡張子の先頭に付加されます。
- 拡張子では大文字と小文字が区別されません。

たとえば、すべてのMicrosoft Accessデータベースファイルを除外するには、次の除外を作成します。

```
.MDB
```



注：標準のファイル拡張子による除外がデフォルトリストで使用可能です。これらの除外を削除することは推奨されません。削除すると、エンドポイントのパフォーマンスが変更される可能性があります。

ワイルドカード除外

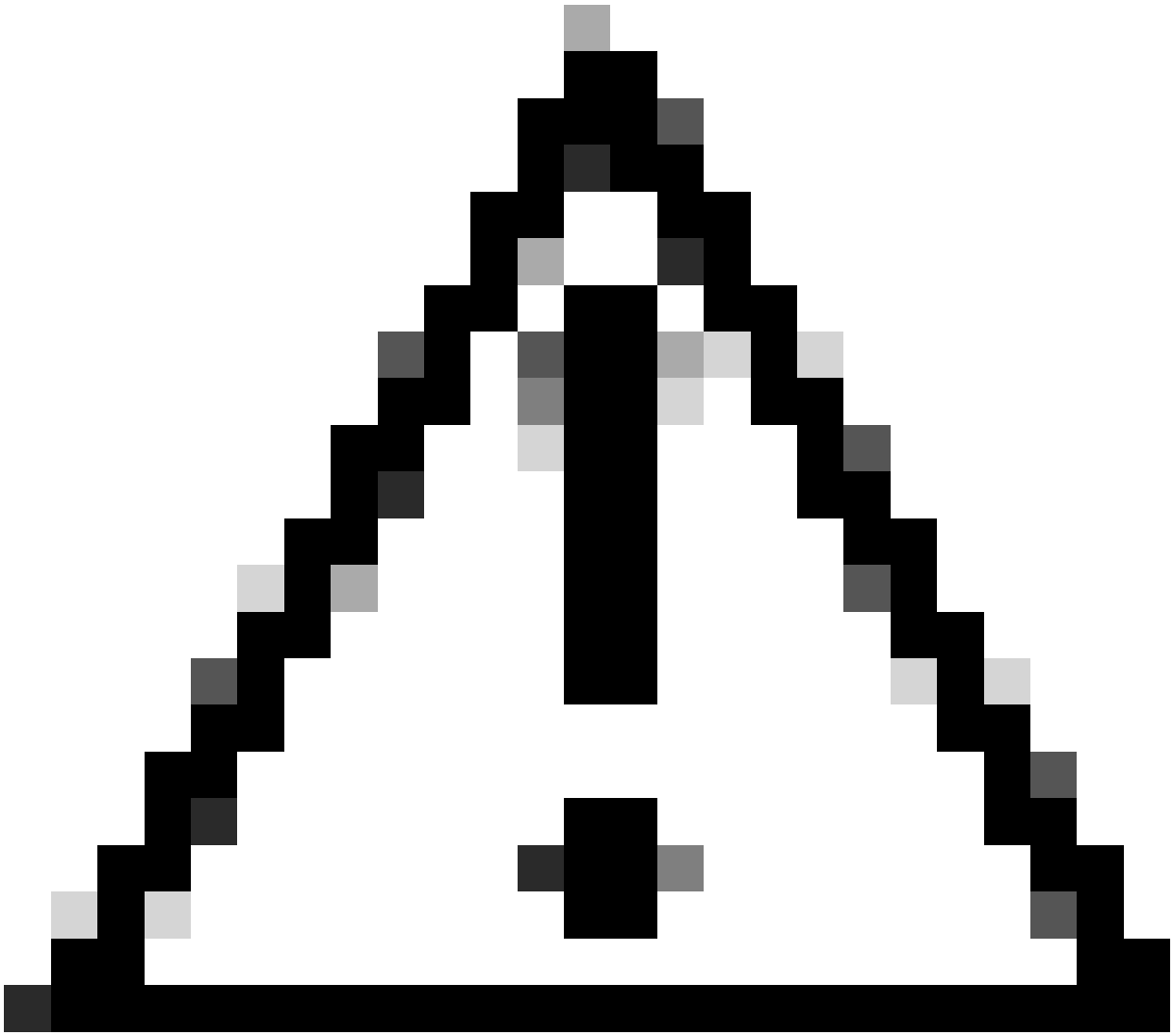
ワイルドカードの除外は、パスまたはファイル拡張子の除外と同じですが、パスまたは拡張子の中にワイルドカードを表すためにアスタリスク(*)を使用できる点が異なります。

たとえば、macOS上の仮想マシンをスキャンから除外する場合は、次のパス除外を入力できます。

```
/Users/johndoe/Documents/Virtual Machines/
```

ただし、この除外は1人のユーザに対してのみ機能します。パス内のユーザ名をアスタリスクに置き換え、ワイルドカード除外を作成して、このディレクトリをすべてのユーザに対して除外します。

```
/Users/*/Documents/Virtual Machines/
```



注意：ワイルドカードによる除外は、パスの区切り文字で終わるものではありません。このため、意図しない除外が行われる可能性があります。たとえば、C:*\test excludesC:\sample\testおよびC:\1\test**またはC:\sample\test123などです。

警告：除外をアスタリスクで始めると、重大なパフォーマンスの問題が発生する可能性があります。CPUへの影響を軽減するために、アスタリスクで始まるすべての除外を削除または変更します。

Windows

Windowsでワイルドカードの除外を作成する場合は、すべてのドライブ文字に適用するオプションがあります。このオプションを選択すると、ワイルドカードの除外がマウントされたすべてのドライブに適用されます。

同じ除外を手動で作成する場合は、^[A-Za-z]を先頭に付加する必要があります。次に例を示します。

```
^[A-Za-z]\testpath
```

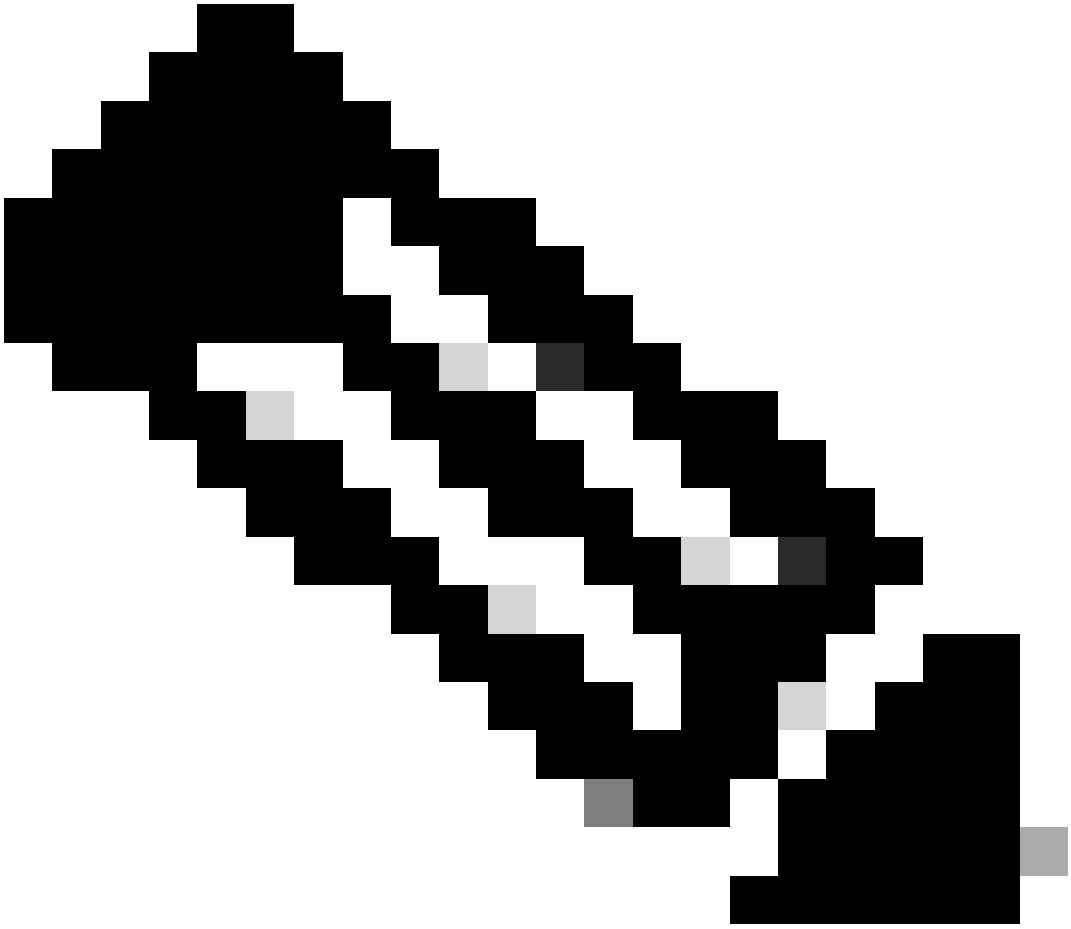
どちらの例でも、C:\testpathとD:\testpathは除外されます。

Secure Endpoint Consoleでは、ワイルドカードの除外に対してApply to all drive lettersが選択されている場合、^[A-Za-z]が自動的に生成されます。

実行可能ファイルの除外（Windowsのみ）

実行可能ファイルの除外は、Exploit Preventionが有効になっているWindowsコネクタにのみ適用されます。実行可能ファイルを除外すると、特定の実行可能ファイルがエクスプロイト防止による保護の対象から除外されます。問題やパフォーマンスの問題が発生した場合にのみ、実行可能ファイルをエクスプロイト防止から除外する必要があります。

保護されたプロセスの一覧を確認し、アプリケーションの除外フィールドに実行可能ファイル名を指定することで、保護から除外できます。実行可能ファイルの除外は、name.exe形式の実行可能ファイル名と正確に一致する必要があります。ワイルドカードはサポートされていません。



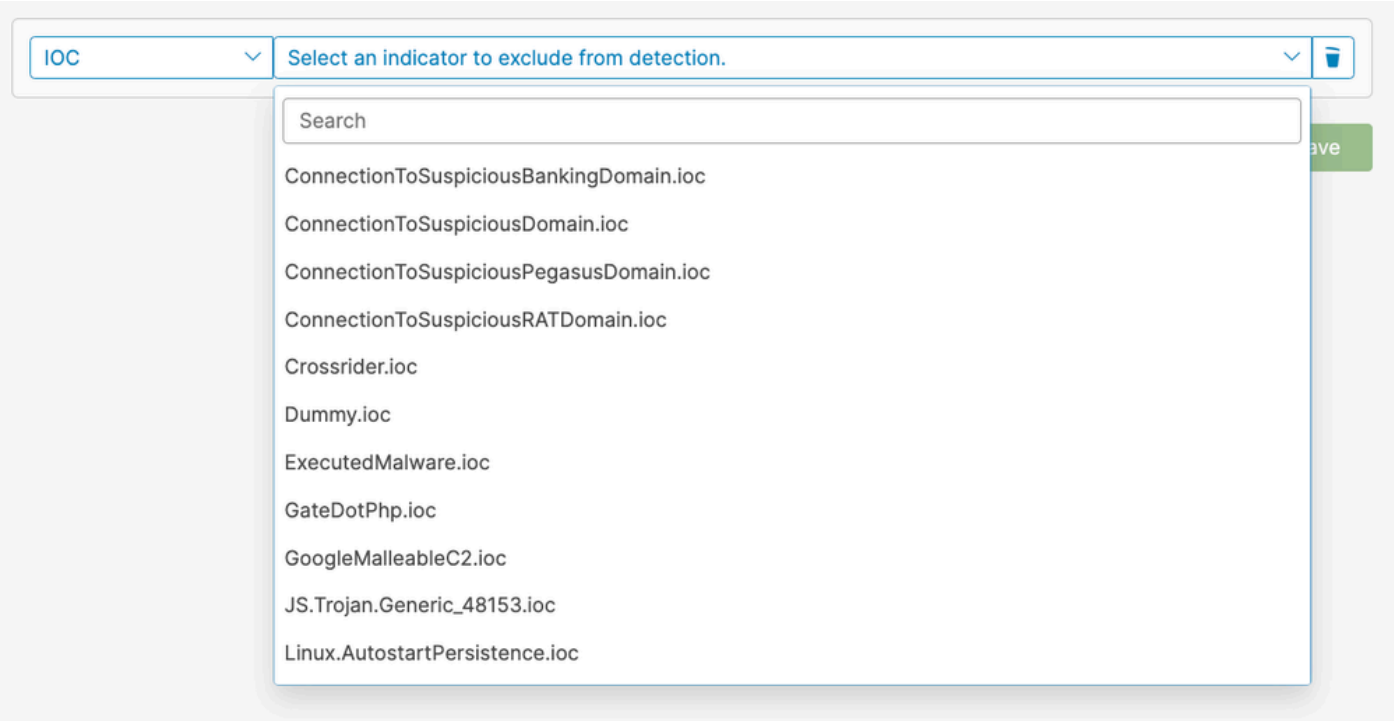
注:Secure Endpoint Consoleで実行可能ファイルの除外を使用して除外できるのは、アプリケーションだけです。DLLに関連する除外を作成するには、サポートケースを開く必要があります。

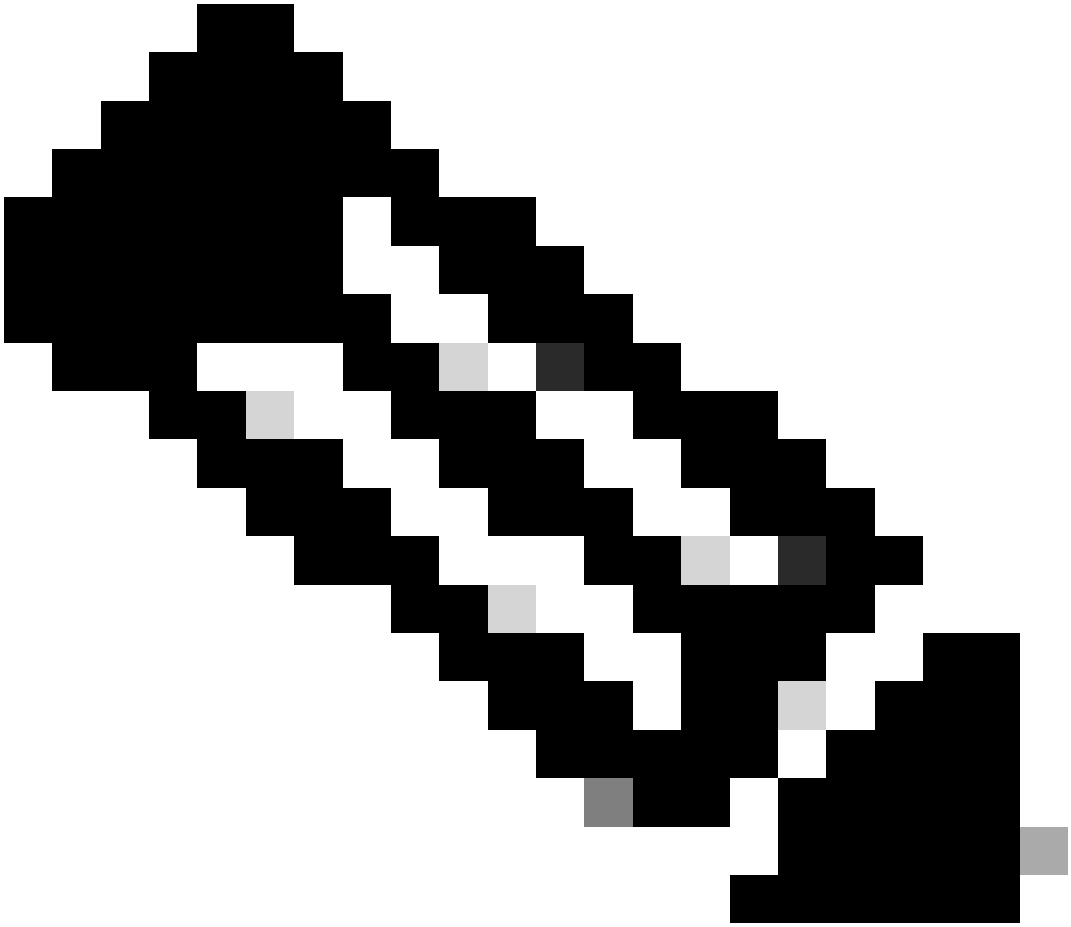
Exploit Preventionの正しい除外を見つけることは、他の除外タイプよりもはるかに集中的なプロセスであり、有害なセキュリティホールを最小限に抑えるために広範なテストが必要です。

IOCの除外（Windowsのみ）

IOCの除外により、クラウドの侵入の痕跡を除外できます。これは、署名できないカスタムアプリケーションや内部アプリケーションがあり、特定のIOCが頻繁にトリガーされる場合に便利です。Secure Endpoint Consoleには、IOCの除外に関して選択できるインジケータのリストが表示されます。

除外するインジケータをドロップダウンから選択できます。





注：重大度が高い、または重大なIOCを除外すると、IOCへの可視性が失われ、組織がリスクにさらされる可能性があります。これらのIOCを除外する必要があるのは、誤検出が多数発生している場合だけです。

CSIDLおよびKNOWNFOLDERID（Windowsのみ）

Windowsのパスとプロセスの除外を記述する場合は、CSIDLとKNOWNFOLDERIDの値を受け入れ、推奨します。CSIDL/KNOWNFOLDERID値は、代替ドライブ文字を使用する環境のプロセスおよびパスの除外を作成する場合に便利です。

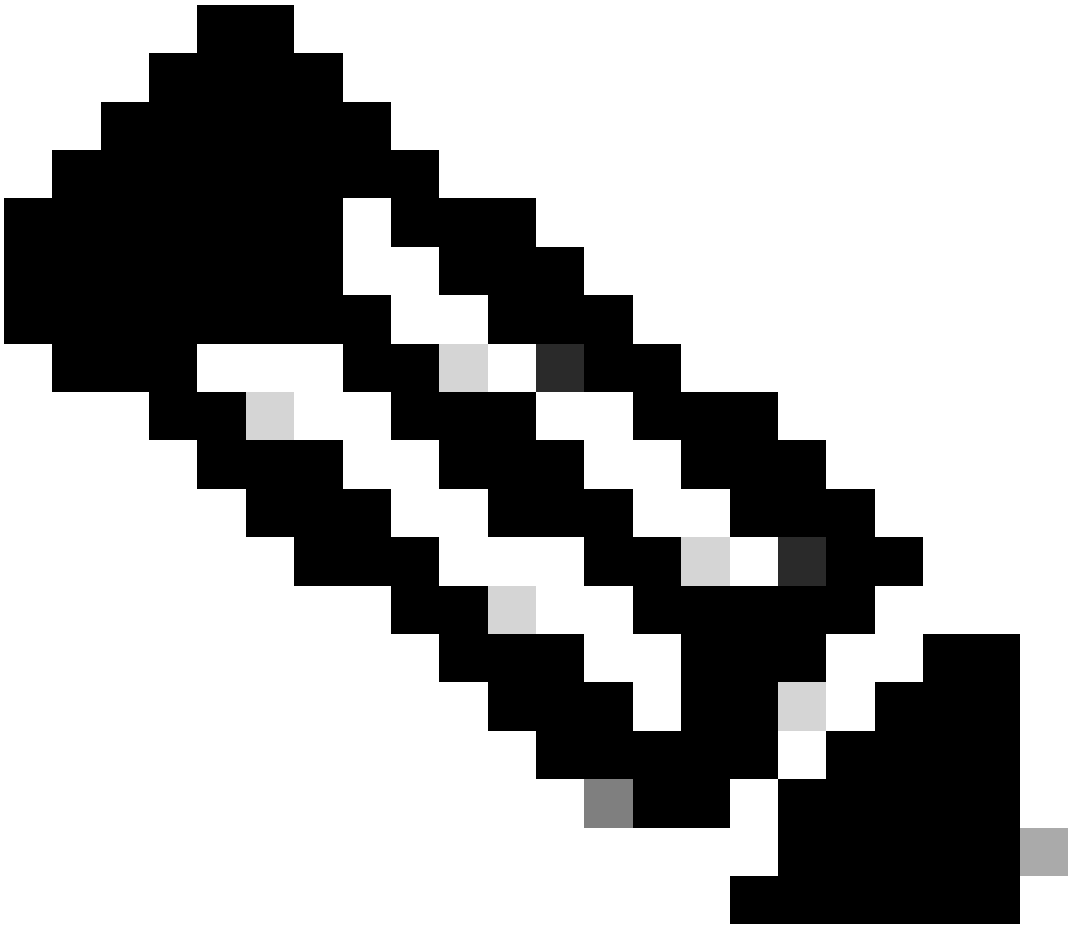
CSIDL/KNOWNFOLDERIDを使用する際には、考慮する必要のある制限事項があります。複数のドライブ文字にプログラムをインストールする場合、CSIDL/KNOWNFOLDERIDの値は、既定のインストール場所または既知のインストール場所としてマークされたドライブのみを参照します。

たとえば、OSがC:\にインストールされていても、Microsoft SQLのインストールパスが手動で`D:\`に変更されている場合、維持されている除外リストのCSIDL/KNOWNFOLDERIDに基づく除外

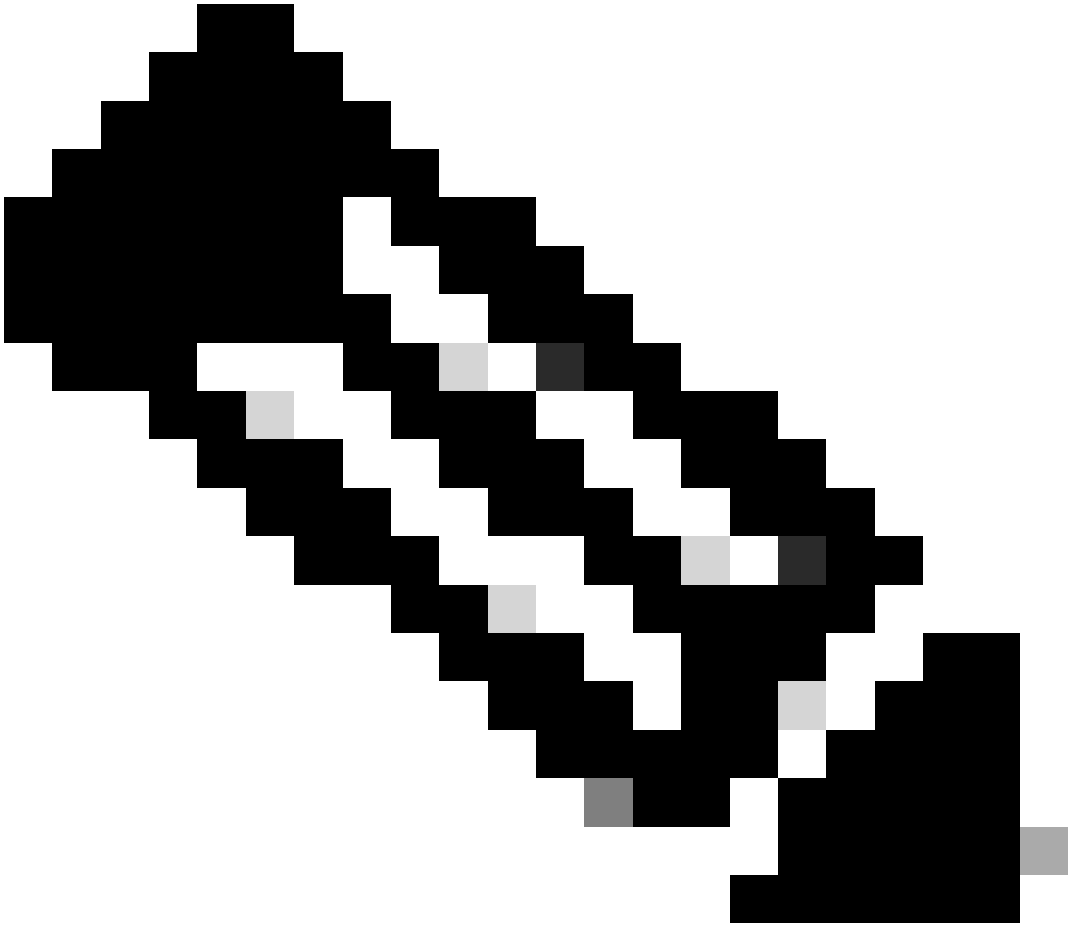
は、そのパスには適用されません。つまり、CSIDL/KNOWNFOLDERIDを使用するとパスがマッピングされないため、C:\ドライブに存在しないパスまたはプロセスの除外ごとに1つの除外を入力する必要があります。

詳細については、次のWindowsのドキュメントを参照してください。

- CSIDL
- KNOWNFOLDERID



注: KNOWNFOLDERIDは、Windowsコネクタ8.1.7以降でのみサポートされています。以前のバージョンのWindowsコネクタでは、CSIDL値を使用します。



注意: KNOWNFOLDERID値では、大文字と小文字が区別されます。たとえば、無効なvalueFolderID_programfilesではなく、値FOLDERID_ProgramFilesを使用する必要があります。

除外チューニング用のコネクタの準備

除外を調整するためにコネクタを準備するには、次の操作を行う必要があります。

1. デバッグモードで実行するポリシーとグループを設定します。
2. 通常の業務操作に従って、新しいデバッググループのコンピュータを実行し、十分なコネクタログデータを取得する時間を確保します。
3. 除外の識別に使用するコネクタの診断データを生成します。

デバッグモードを有効にし、異なるオペレーティングシステムで診断データを収集する手順については、次のドキュメントを参照してください。

- Cisco Secure Endpoint Connector for Mac診断データ収集

- Linux診断データ収集用Cisco Secure Endpoint Connector
- 高CPU用AMP診断バンドルの分析(Windows)

除外の識別

MacOSおよびLinux

デバッグモードで生成された診断データには、除外の作成に役立つ2つのファイルfileops.txtとexecs.txtが用意されています。fileops.txtファイルはパス/ファイル拡張子/ワイルドカード除外の作成に役立ち、execs.txtファイルはプロセス除外の作成に役立ちます。

プロセスの除外の作成

execs.txtファイルには、セキュアエンドポイントがファイルスキャンを実行するトリガーとなった実行可能パスが一覧表示されます。各パスには、スキャンされた回数を示すカウントが関連付けられ、リストは降順で並べ替えられます。このリストを使用して、大量の実行イベントが発生しているプロセスを特定し、プロセスパスを使用して除外を作成できます。ただし、一般的なユーティリティプログラム（/usr/bin/grepなど）やインタプリタ（/usr/bin/rubyなど）を除外することは推奨されません。

一般的なユーティリティプログラムやインタプリタが大量のファイルスキャンを生成している場合は、さらに調査を行って、対象を絞った除外を試みることができます。

1. 親プロセスの除外：プロセスを実行しているアプリケーションを特定し（grepを実行している親プロセスを検索するなど）、この親プロセスを除外します。これは、親プロセスがプロセスの除外に安全に設定できる場合にのみ行う必要があります。親プロセスの除外が子プロセスに適用される場合、親プロセスからの子プロセスへの呼び出しも除外されます。
2. 特定のユーザのプロセスを除外する：プロセスを実行しているユーザを特定します。特定のユーザによってプロセスが大量に実行されている場合、その特定のユーザのプロセスだけを除外できます(たとえば、ユーザrootによってプロセスが大量に呼び出されている場合、そのプロセスを除外できますが、指定されたユーザrootに対してのみ、セキュアエンドポイントでroot以外のユーザによる特定のプロセスの実行をモニタできます)。

execs.txtの出力例：

```
33 /usr/bin/bash
23 /usr/bin/gawk
21 /usr/bin/wc
21 /usr/bin/sleep
21 /usr/bin/ls
19 /usr/bin/pidof
17 /usr/bin/sed
14 /usr/bin/date
13 /usr/libexec/gdb
13 /usr/bin/iconv
11 /usr/bin/cat
10 /usr/bin/systemctl
 9 /usr/bin/pgrep
 9 /usr/bin/kmod
```

```
 7 /usr/bin/rm
 6 /usr/lib/systemd/systemd-cgroups-agent
 6 /usr/bin/rpm
 4 /usr/bin/tr
 4 /usr/bin/sort
 4 /usr/bin/find
```

パス、ファイル拡張子、およびワイルドカードの除外の作成

fileops.txtファイルには、ファイルの作成、変更、および名前の変更アクティビティによってSecure Endpointがファイルスキャンを実行する際にトリガーされるパスがリストされています。各パスには、スキャンされた回数を示すカウントが関連付けられ、リストは降順で並べ替えられます。パスの除外を開始する方法の1つは、最も頻繁にスキャンされるファイルおよびフォルダパスをfileops.txtから検索し、それらのパスのルールを作成することを検討することです。カウントが高い場合は、パスを除外する必要があるとは限りません（たとえば、メールを保存しているディレクトリは頻繁にスキャンできますが、除外する必要はありません）。除外する候補を特定するための開始点となります。

fileops.txtの出力例：

```
31 /Users/eugene/Library/Cookies/Cookies.binarycookies
24 /Users/eugene/.zhistory
9 /Users/eugene/.vim/.temp/viminfo
9 /Library/Application Support/Apple/ParentalControls/Users/eugene/2018/05/10-usage.data
5 /Users/eugene/Library/Cookies/HSTS.plist
5 /Users/eugene/.vim/.temp/viminfo.tmp
4 /Users/eugene/Library/Metadata/CoreSpotlight/index.spotlightV3/tmp.spotlight.state
3 /Users/eugene/Library/WebKit/com.apple.Safari/WebsiteData/ResourceLoadStatistics/full_browsing_sessio
3 /Library/Logs/Cisco/supporttool.log
2 /private/var/db/locationd/clients.plist
2 /Users/eugene/Desktop/.DS_Store
2 /Users/eugene/.dropbox/instance1/config.dbx
2 /Users/eugene/.DS_Store
2 /Library/Catacomb/DD94912/biolockout.cat
2 /.fseventsd/000000000029d66b
1 /private/var/db/locationd/.dat.nosync0063.arg4tq
```

経験則として、ログファイルまたはジャーナルファイルの拡張子を持つものは、適切な除外候補と見なす必要があります。

動作保護エンジン

動作保護エンジンは、Linuxコネクタバージョン1.22.0とmacOSコネクタバージョン1.24.0で導入されました。これらのバージョン以降では、コネクタによって過剰に高いシステムアクティビティが検出され、障害18が発生します。

プロセスの除外は、すべてのエンジンとファイルスキャンに適用されます。この障害を修復するには、プロセス除外を非常にアクティブな良性プロセスに適用します。デバッグモードの診断デ

ータによって生成されたtop.txtファイルを使用して、システム上で最もアクティブなプロセスを判別できます。詳細な修復手順については、『セキュアエンドポイントMac/Linuxコネクタ障害18』のガイダンスを参照してください。

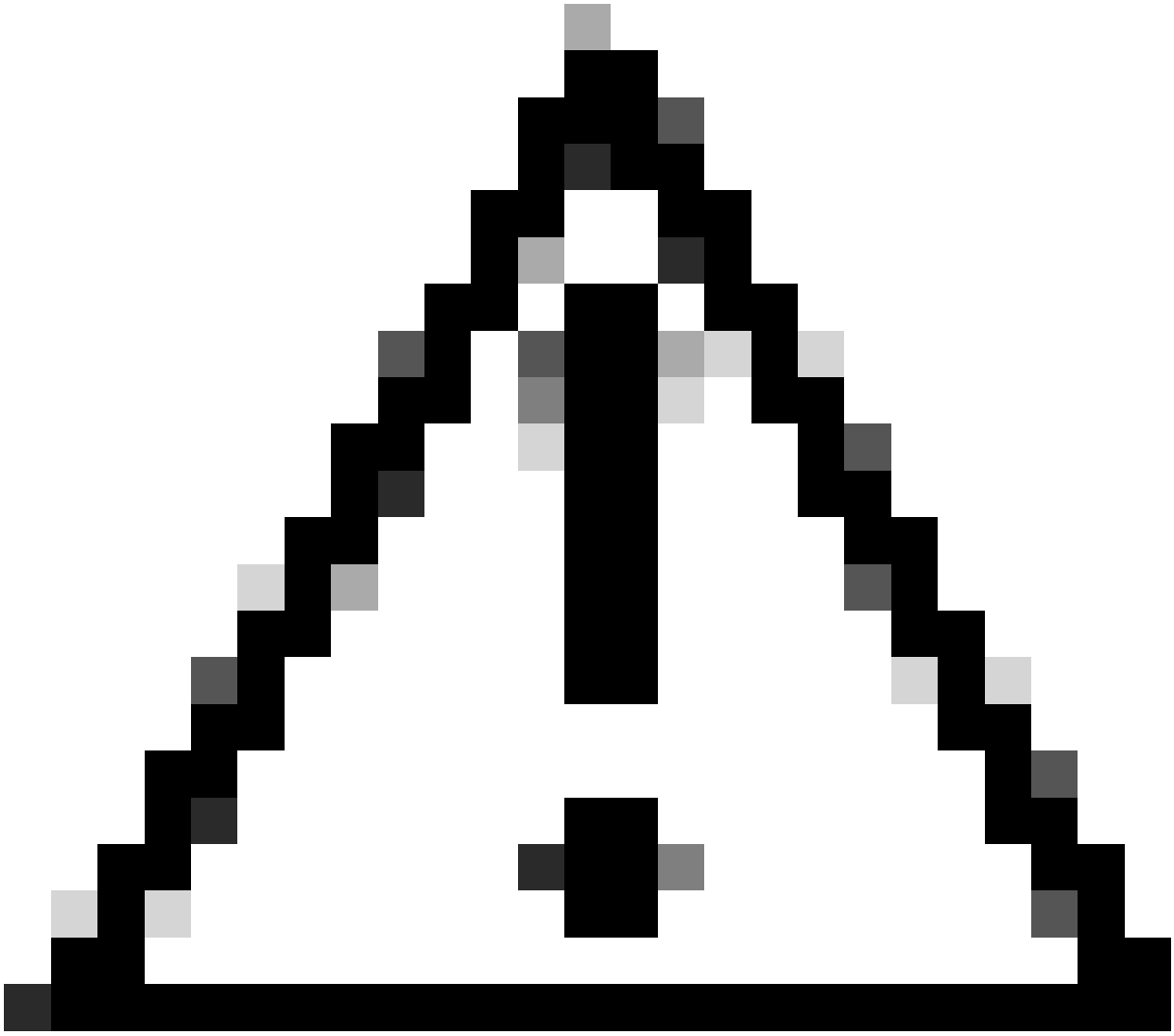
さらに、プロセスの除外により、良性ソフトウェアからの誤検出の動作保護を抑制できます。Secure Endpoint Consoleで誤検出が検出された場合は、このプロセスを除外してレポートを改善できます。

Windows

Windowsオペレーティングシステムはより複雑で、親プロセスと子プロセスのために、より多くの除外オプションが利用可能です。これは、アクセスされたファイルだけでなく、それらを生成したプログラムを特定するためにより深いレビューが必要であることを示しています。

セキュアエンドポイントでWindowsのパフォーマンスを分析して最適化する方法の詳細については、Cisco SecurityのGitHubページにある、このWindowsチューニングツールを参照してください。

セキュアエンドポイントコンソールでの除外ルールの作成



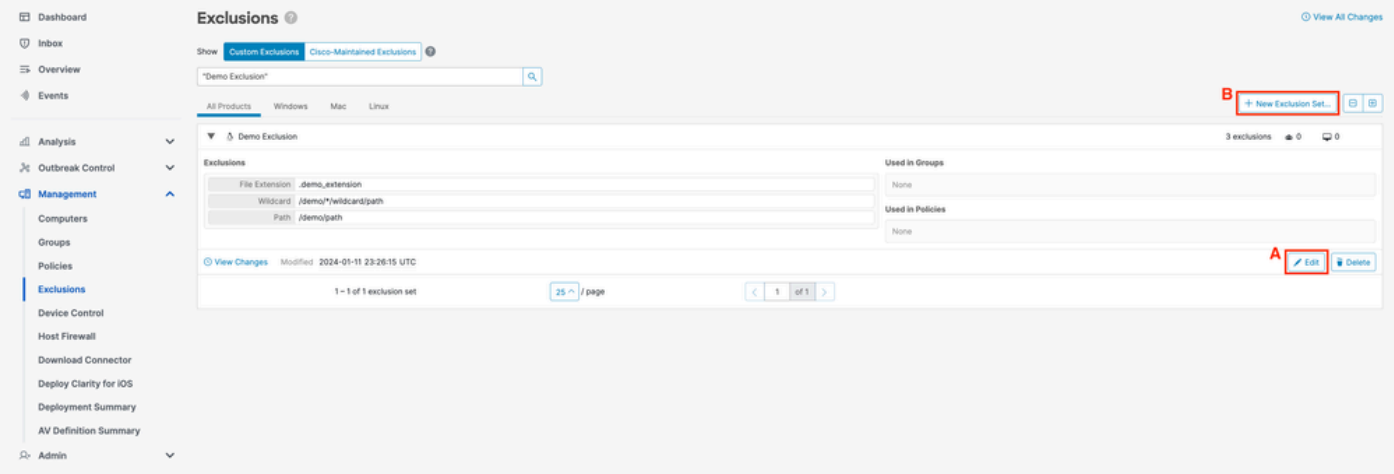
注意：除外を書き込む前に必ずファイルとプロセスを理解して、エンドポイントのセキュリティの脆弱性を回避してください。

セキュアエンドポイントコンソールを使用して新しい除外ルールを作成するには、次の手順を実行します。

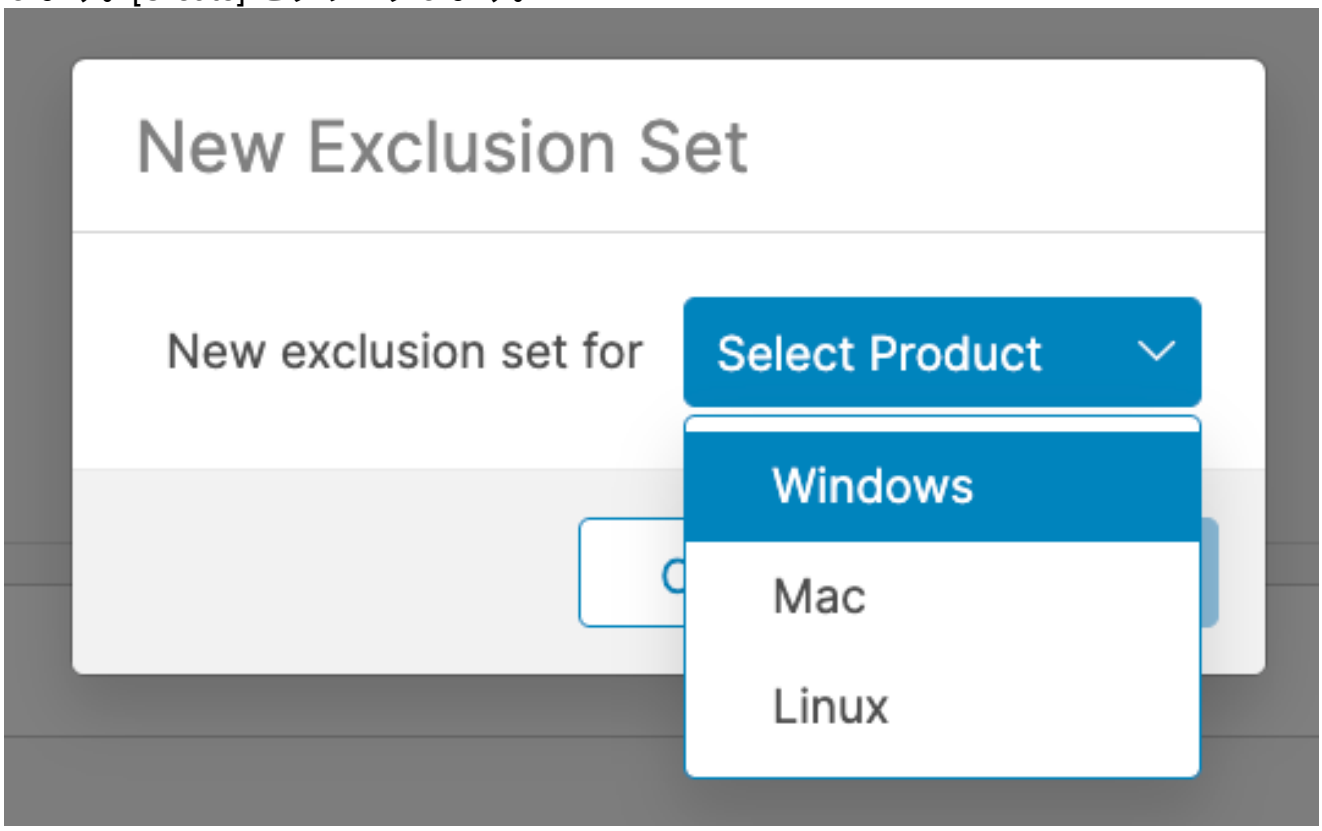
1. Secure Endpoint Consoleで、Management -> Exclusionsの順に選択して、Policiesページに移動します。どちらでも:

(A)変更する除外セットを探して、Editをクリックします。または、

(B) +新規除外セット...をクリックします。

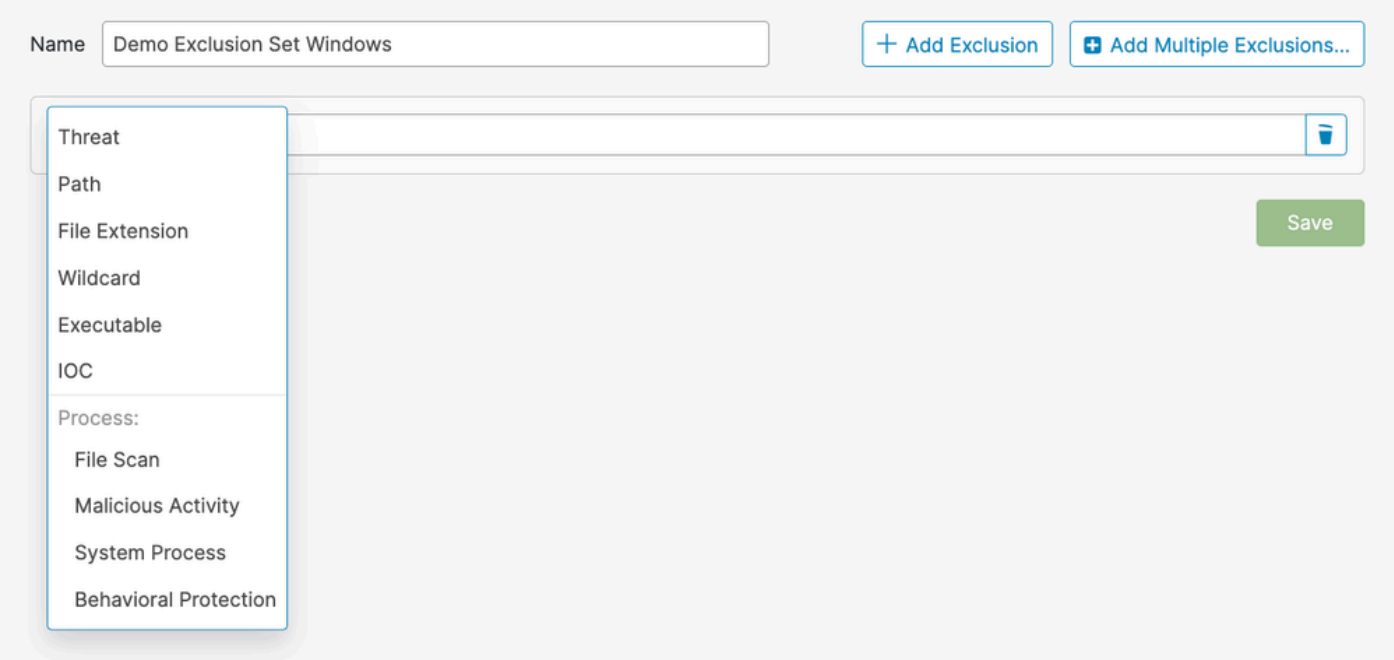


1. 新しい除外セットポップアップで、除外セットを作成するオペレーティングシステムを選択します。[Create] をクリックします。

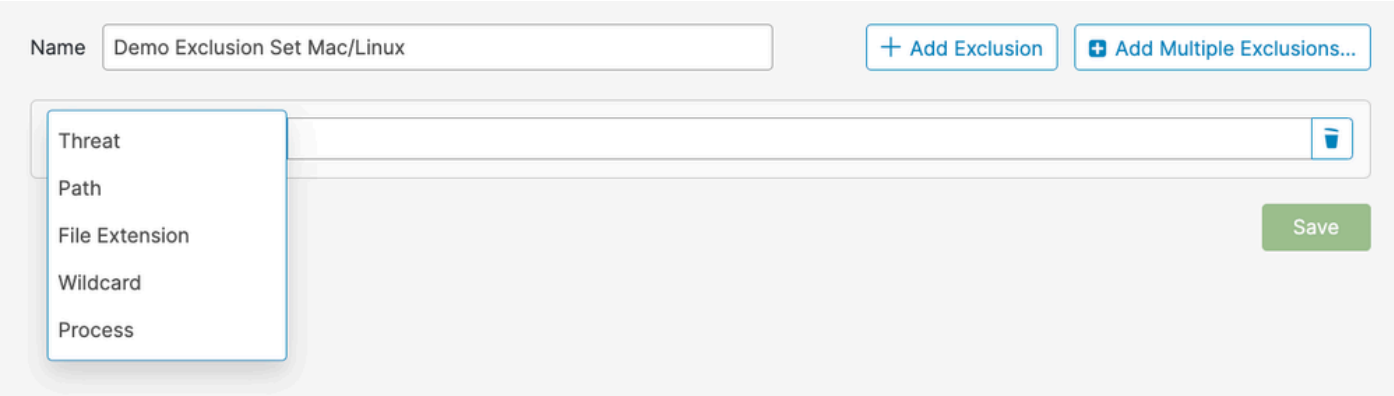


2. 新規除外セットのページにリダイレクトされます。+除外の追加をクリックし、タイプの選択ドロップダウンから除外タイプを選択します。

Windows：

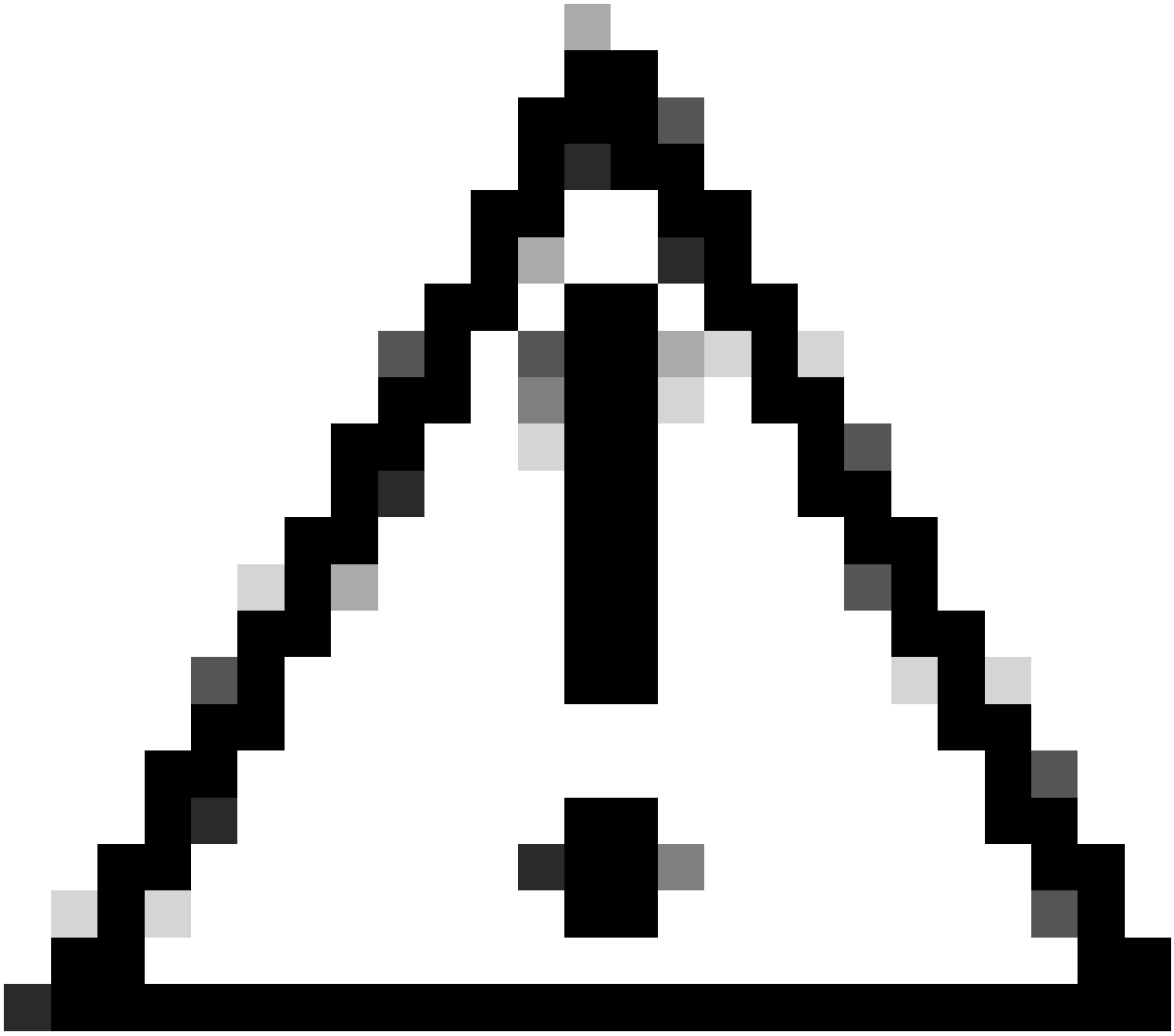


Mac/Linux:



1. 選択した除外タイプの必須フィールドに入力します。
2. さらにルールを追加するにはステップ2と3を繰り返します。除外セットを保存するにはSaveをクリックします。

ベスト プラクティス



注意：除外を作成すると、Cisco Secure Endpointで提供される保護のレベルが低下するため、注意が必要です。除外されたファイルは、キャッシュまたはクラウドでハッシュ、スキャン、または利用できず、アクティビティは監視されず、バックエンドエンジン、デバイストラジェクトリー、および高度な分析から情報が欠落しています。

除外は、特定のアプリケーションとの互換性の問題や、他の方法では改善できないパフォーマンスの問題など、対象を絞ったインスタンスでのみ使用する必要があります。

除外を作成する際に従うべきベストプラクティスは次のとおりです。

- 実証済みの問題に対してのみ除外を作成します。
  - 除外が他の方法では対処できない問題であることが証明されない限り、除外が必要であると仮定しないでください。
  - 除外を適用する前に、パフォーマンスの問題、誤検出、またはアプリケーションの互換性の問題を徹底的に調査し、軽減する必要があります。
- パス/ファイル拡張子/ワイルドカードの除外よりもプロセスの除外が優先されます。
  - プロセスの除外は、パス、ファイル拡張子、およびワイルドカードの除外を組み合わ

せて同じ結果を得るよりも、良性ソフトウェアのアクティビティを除外する直接的な方法です。
    - 可能な場合は、プログラム実行可能ファイルを対象とするパス、ファイル拡張子、およびワイルドカードの除外を、対応するプロセスの除外に置き換えることをお勧めします。
- 広範な除外は避けてください。
    - Cドライブ全体など、エンドポイントの大きな部分を除外しないでください。
    - ファイル名だけでなく、ファイルへの完全修飾パスを使用します。
    - デバイストラジェクトリー、Secure Endpoint Diagnostics Data、およびWindowsチューニングツールを使用して、特定の除外を調査および決定します。
- ワイルドカードの除外を使いすぎないようにします。
    - ワイルドカードを使用して除外を作成する場合は注意してください。可能な場合は、より具体的な除外を使用してください。
    - ワイルドカードの最小数を除外に使用します。ワイルドカードを使用する必要があるのは、真に可変なフォルダのみです。
- 一般的なユーティリティプログラムやインタプリタを除外しないでください。
    - 一般的なユーティリティプログラムやインタプリタを除外することは推奨されません。
    - 除外する汎用ユーティリティプログラムまたはインタプリタを除外する必要がある場合は、プロセスユーザを指定します（macOS/Linuxのみ）。
    - たとえば、python、java、ruby、bash、およびshを含む除外を記述することは避けてください。
- 除外の重複を避ける。
    - 除外を作成する前に、カスタム除外またはCisco-Maintained除外のいずれかに除外がすでに存在するかどうかを確認してください。
    - 重複する除外を削除すると、パフォーマンスが向上し、除外の運用管理が軽減されます。
    - プロセスの除外で指定されたパスが、パス/ファイル拡張子/ワイルドカードの除外の対象となっていないことを確認してください。
- マルウェア攻撃でよく使用されるプロセスを除外することは避けてください。
    - 詳細は、『推奨されない除外』を参照してください。
- 古い除外の削除
    - 除外リストを定期的に確認および監査し、特定の除外が追加された理由を記録します。
- セキュリティ侵害の除外を削除
    - 最適なセキュリティと可視性を取り戻すには、除外を削除する必要があります（コネクタが侵害されている場合）。
    - 自動化されたアクションを使用して、感染後にコネクタにより安全なポリシーを適用できます。コネクタが侵害された場合、最高レベルの保護が適用されるように、除外されていないポリシーを含むグループにコネクタを移動する必要があります。
    - 「Move Computer to Group Upon Compromise」自動処理を事前に設定する方法の詳細については、「Identify Conditions to Trigger Automated Actions in Secure Endpoint」を参照してください。
- 除外された項目の保護を強化する
    - 除外が絶対に必要な場合は、除外された項目に対して書き込み保護を有効にして保護のレイヤを追加するなど、どのような緩和策を講じることができるか検討してくださ

い。

- 除外をインテリジェントに作成
  - ルールを最適化するには、除外するアプリケーションを一意に識別する最上位レベルの親プロセスを選択し、「子プロセスに適用」オプションを使用してルールの数を最小限にします。
- スタートアッププロセスを除外しない
  - 起動プロセス(macOSではlaunchd、Linuxではinitまたはsystemd)は、システム上の他のすべてのプロセスを起動する役割を担い、プロセス階層の最上位にあります。
  - 起動プロセスとそのすべての子プロセスを除外すると、セキュアエンドポイントのモニタリングが実質的に無効になります。
- 可能な場合は、プロセスユーザを指定します（macOS/Linuxのみ）。
  - ユーザーフィールドを空白のままにすると、指定したプログラムを実行するすべてのプロセスに除外が適用されます。
  - 任意のユーザに適用される除外はより柔軟ですが、この広範な範囲では、意図せずにモニタする必要のあるアクティビティが除外される可能性があります。
  - ランタイムエンジン（javaなど）やスクリプトインタープリタ（bash、pythonなど）などの共有プログラムに適用されるルールでは、ユーザの指定が特に重要です。
  - ユーザーを指定すると、スコープが制限され、Secure Endpointが他のインスタンスを監視している間に特定のインスタンスを無視するように指示されます。

推奨されない除外

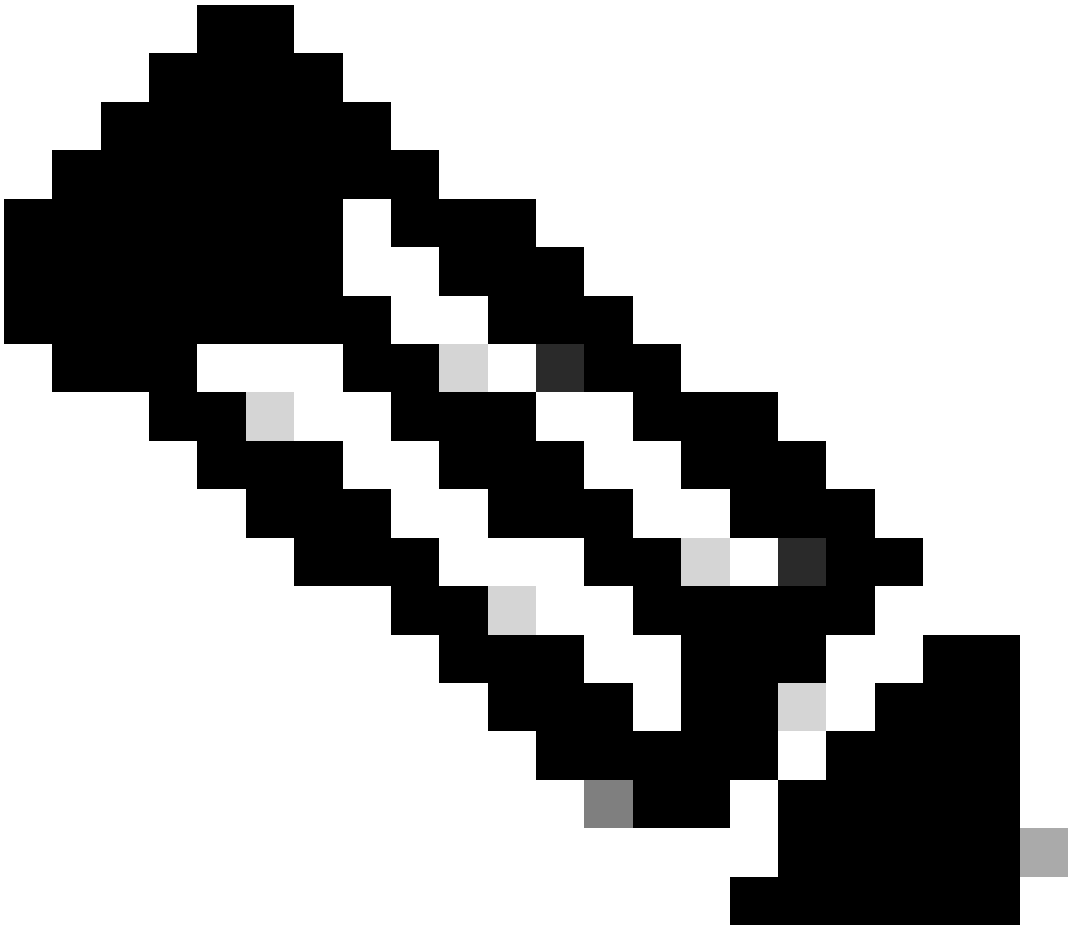
攻撃者が使用できるすべての攻撃ベクトルを知ることは不可能ですが、監視する必要のあるコア攻撃ベクトルがいくつかあります。良好なセキュリティポスチャと可視性を維持するために、次の除外は推奨されません。

AcroRd32.exe（ベータ版）
addinprocess.exe
addinprocess32.exe
addinutil.exe
bash.exe（ファイル名）
bginfo.exe（ダウンロード）
bitsadmin.exe
cdb.exe（ダウンロード）
csi.exe
dbghost.exe
dbgsvc.exe
dnx.exe
dotnet.exe（登録ユーザ専用）
excel.exe（ダウンロード）
FSI.EXEファイル
fsiAnyCpu.exeファイル
iexplore.exe
java.exe（ダウンロード）

kd.exe
lxssmanager.dll
msbuild.exe（ビルドのセットアップ）
mshta.exe
ntkd.exe
ntsd.exe
outlook.exe
psexec.exe
powerpnt.exe（登録ユーザ専用）
powershell.exe
rcsi.exe
svchost.exe
schtasks.exe
system.management.automation.dll（自動）
windbg.exe（ベータ版）
winword.exe
wmic.exe（登録ユーザ専用）
wuauclt.exe
0.7z
.bat
.bin
.cab
.cmd(cmd)
.com
.cpl
.dll
.exe
.fla
.gif
.gz
.hta
.inf
.java
.jar
ジョブ
.jpeg
.jpg
.js
.ko
.ko.gz
.msi
.ocx

.png
.ps1
.py
.rar
.reg
.scr
.sys
.tar
.tmp
.url
.vbe
.vbs
.wsf
.zip
バッシュ
java
Pythonの
python3
sh
ZSH
/
/bin
/sbin
/usr/lib
C:
C:\
C:*
D:\
D:*
C:\Program Files\Java
C:\Temp\
C:\Temp*
C:\Users\
C:\Users*
C:\Windows\Prefetch
C:\Windows\Prefetch\
C:\Windows\Prefetch*
C:\Windows\System32\Spool
C:\Windows\System32\CatRoot2
C:\Windows\Temp
C:\Windows\Temp\

C:\Windows\Temp*
C:\Program Files\<会社名>\
C:\Programファイル(x86)\<会社名>\
C:\Users\<UserProfileName>\AppData\Local\Temp\
C:\Users\<UserProfileName>\AppData\LocalLow\Temp\



注：これは除外する対象の完全なリストではありませんが、コア攻撃ベクトルに関する詳細な情報を提供します。これらのパス、ファイル拡張子、プロセスの可視性を維持することが重要です。

関連情報

- テクニカル サポートとドキュメント - Cisco Systems
- Cisco Secure Endpoint – テクニカルノート
- Cisco Secure Endpoint – ユーザガイド
- セキュアエンドポイントにおける不正利用防止のトラブルシューティング

- セキュアエンドポイントで自動アクションをトリガーする条件の特定

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。