セキュリティ タスク マネージャ

for Windows XP, Vista, 2003, 2000, ME, 98

プログラムとプロセスに関する詳細な情報でセキュリティの大幅な向上を

© A. & M. Neuber Software GmbH / P.& A. International, Inc.

目次

セキュリティ タスク マネージャの機能 3

セキュリティ タスク マネージャを使う 3

プロセスの種類 4

プロセスのリスク レート 5

プロセスの詳細を表示する 8

プロセスを詳しく調べる 8

プロセスを終了する 9

隔離フォルダを使う 9

プロセス リストをエクスポートする 9

プロセス リストを印刷する 9

コメントを入力する 10

コンピュータを スパイ プロテクタで保護する 10

セキュリティ タスク マネージャのテクニカル サポート 11

セキュリティ タスク マネージャをアンインストールする 11

試用版について 12

試用版から製品版に切り替える 12

セキュリティ タスク マネージャの機能

セキュリティ タスク マネージャは、コンピュータ上で動作しているプログラム やプロセスに関する詳細な情報を提供します。プロセスごとに、Windows のタスク マネージャでは 確認できない次の情報を表示します :

- ファイル名とフォルダ パス
- セキュリティのリスク レート
- 説明、開始時間、プログラムのアイコン 、プロセスの 種類
- CPU 使用率のグラフ
- 隠れた 機能
  (キーボードの監視、ブラウザの監視、操作)

スパイ プロテクタは、インターネット履歴の 削除、レジストリ変更の 警告、キーボードやマウスの 監視の 無効化を行うことができます。

セキュリティ タスク マネージャを使う

セキュリティ タスク マネージャは、コンピュータ上で実行中のプロセスをすべて表示します。レートはプロセスが 含むセキュリティに関する機能をすべて表示します。

一覧表示されるプロセスは、次のプロパティで並べ替えることができます。**[表示]** メニューをクリックして、どのプロパティが 表示するか 選びます。

- 名前
  ソフトウェアの 名前、または ドライバの 名前を表示します。
- レート
  プロセスのセキュリティに関する客観的なレートを表示します。レートの 赤いバーが 長ければ長いほど、より危険性の 高い機能をプロセスが 含んでいることになります。ただし、レートの 高いプログラム が 必ずしも危険というわけではなく、スパイウェアとして 認識され やすい性質を持っているということです 。プロセスをクリックすると、詳細を表示します。その後で、ソフトウェアの 信頼性を評価することができます。
- CPU
  CPU (プロセッサ) の 使用率を表示します。アクティブ なプログラム は、非アクティブのプロセス よりも 多くプロセッサを占有し続けます。
- メモリ
  メモリの 使用量を表示します。
- ファイル
  ファイル のフォルダ パスと名前を表示します。
- 種類
  ファイル の 種類を表示します。ファイル の 種類は、プログラム、システム トレー アイコン プログラム、ブラウザ ヘルパー オブジェクト、ドライバ、サービスのいずれかになります。
- タイトル、説明
  ファイル に 含まれている タイトルとファイル の 説明を表示します。タイトルは、可視ウィンドウのタイトル バーに表示される文字列に 相当します。
- 製造者、製品
  ファイル 内にある 会社の 名前と製品の 説明を表示します。

プロセスをクリックすると、そのプロセスに 関する詳細情報が 表示されます。次の 作業を行うことができます :

プロパティを表示する

プロセスを終了する

プロセスを隔離する

注意

- **[Windows プロセス]** ボタンをクリックすると、すべての 内部 Windows プロセスも表示されます。これらのプロセスは、Windows オペレーティング システム に属しています。Windows のシステム プロセスは 既定では 表示されません。

- プロセスは、プログラム、ドライバ、サービス、プラグインのいずれかになります – コンピュータのメモリ内でアクティブになるすべての実行コードです。

プロセスの種類

セキュリティ タスク マネージャは、次の種類のプロセスを識別します。メイン画面で [種類] フィールドの表示/非表示を切り替えるには、**[表示]** メニューの **[種類]** をクリックします。

ソフトウェア

- プログラム
  可視ウィンドウでプログラムを表示します。あるいは、ウィンドウのない不可視のプログラムもあります。
- タスクバー アイコン
  システム トレー (時計の左側) にアイコンを表示するプログラムです。タスク バーのアイコンを右クリックすると、ショートカット メニューを開いて詳細情報を表示します。

DLL ファイル

- DLL
  ダイナミック リンク ライブラリ (DLL) は、プログラムと同じようにプログラム コードを実行します。DLL ファイルには、メイン プログラムではあまり使われない機能が含まれています。
- ShellExecute
  このファイルは、Windows レジストリ内の ShellExecute コマンドを使うフックを使って開始されます。ShellExecute は、Windows プログラムが開始されるときにプロセス (ほとんどの場合 DLL) を実行します。このプロセスは注意深く調べる必要があります。

インターネット プラグイン

ブラウザ ヘルパー オブジェクト
ブラウザ ヘルパー オブジェクト (BHO) は、開発者によって Internet Explorer をカスタマイズ/制御することが可能な DLL です。PimpFish、Alexa、GetRight、Go!Zilla などのダウンロード マネージャは、BHO を使用しています。BHO は、インターネットでのすべての活動を監視することが可能です。BHO を無効にするには、Internet Explorer の **[インターネット オプション]** から **[詳細設定]** タブをクリックします。[設定] リスト ボックスにある **[サードパーティ製のブラウザ拡張を有効にする]** チェック ボックスのチェックを外します。

ドライバとサービス (製品版でのみ参照できます)
ドライバやサービスは、ハードウェアの低いレベルでシステム機能を実行します。

デバイス ドライバ
ハードウェア コンポーネント (グラフィック アダプタやスキャナなど) を制御する Windows デバイス ドライバを示すサービス タイプ フラグです。一部のソフトウェア モジュール (ファイアウォールやアンチウィルスなど) はデバイス ドライバですので、このようなプロセスは終了しないでください。

ファイル ドライバ
Windows NT のファイル システム ドライバを示すサービス タイプ フラグです。

サービス (独自プロセス)
独自のプロセスとして動作する Win32 サービスを示すサービス タイプ フラグです。Windows 起動時に自動的に開始する Win32 サービスは、常に動作していて、ユーザーに依存しません。

サービス (デスクトップと統合する独自プロセス)
独自のプロセスとして動作し、デスクトップと連動することが可能な Win32 サービス (ファイアウォールやアンチウィルスなど) を示すサービス タイプ フラグです。Windows 起動時に自動的に開始する Win32 サービスは、常に動作していて、ユーザーに依存しません。

サービス (共有プロセス)
他のサービスとプロセスを共有する Win32 サービスを示すサービス タイプ フラグです。Windows 起動時に自動的に開始する Win32 サービスは、常に動作していて、ユーザーに依存しません。

サービス (デスクトップと統合する共有プロセス)
他のサービスとプロセスを共有し、デスクトップと連動することが可能な Win32 サービスを示すサービス タイプ フラグ です。Windows 起動時に自動的に開始する Win32 サービスは、常に動作していて、ユーザーに依存しません。

プロセスのリスク レート

セキュリティ タスク マネージャは、プロセスのセキュリティ リスクを判断するのに客観的な基準を使います。セキュリティ タスク マネージャは、プロセスを検査して、危険性のあるファンクション コールや疑わしいプロパティを含んでいないかどうか判断します。レートのポイントは、これらのファンクションやプロパティの潜在的な危険性に応じて割り当てられています。ポイントの合計が、セキュリティ タスク マネージャでのリスク レート (0 – 100 ポイント) になります。

セキュリティ タスク マネージャは、次の機能性に関して、プロセスを検査します (危険性の高い順):

- キーボード入力の記録可能
  プロセスがキーボードのすべての入力を監視します。これは Hook ファンクションによって実現されています。通常、プログラムはこの Hook ファンクションを使用しません。
- ファイルが不可視
  ファイルが Windows エクスプローラから隠れています。特に害のないファイル属性の「隠しファイル」とは区別して考えるべきです。
- キーボード ドライバ、入力の記録可能
  キーボード ドライバで、キーボードの全入力を読み取ることができます。
- 他のプログラムの操作可能
  プロセスが、Windows 上で動作しているプログラムや、Windows オペレーティング システムの一部分となるプログラムを操作することが可能です。Hook は、この機能のために設定されています。Hook は、たとえば dir コマンドを操作することによって、ハードディスク上のファイル一覧を作り出すことのできる Windows の内部ファンクションです。プロセスを開始するプログラムは、アンチウィルス ソフトウェアなどの他のプログラムには見えません。
- インターネット ブラウザの監視可能
  ブラウザ ヘルパー オブジェクト (BHO) は、開発者によって Internet Explorer をカスタマイズ/制御することが可能な DLL です。PimpFish、Alexa、GetRight、Go!Zilla などのダウンロード マネージャが BHO を使用しています。BHO は、インターネットのすべての活動を監視することができます。BHO を無効にするには、Internet Explorer の **[インターネット オプション]** から **[詳細設定]** タブをクリックします。[設定] リスト ボックスにある **[サードパーティ製のブラウザ拡張を有効にする]** チェック ボックスのチェックを外します。
- 他のプログラム起動時に開始
  このファイルは、Windows レジストリの ShellExecute コマンドを使って Hook によって開始されました。ShellExecute は、何らかの Windows プログラムが開始されたときに、プロセス (主に DLL) を実行します。このプロセスは注意深く調べる必要があります。
- リッスン – ポート *<No.>*
  プロセスはインターネットから情報を受け取ることができます。ハッカーはこのような情報を使って、コンピュータから制御を奪います。良質なファイアウォールでこのような攻撃を防ぐことができます。
- 送信先 *<computer name>* ポート *<No.>*
  プロセスは名前の付いたコンピュータ、または IP アドレスに接続して、情報を送信することができます。

良質なファイアウォールでこのような攻撃を防ぐことができます。

- 不明なプログラムのリッスンまたは送信
  ポートがネットワークまたはインターネットを通して情報を送受信するために開かれていました。どのプログラムか見つけ出すべきです。良質なファイアウォールでは、このような接続を防ぐことができます。
- プログラム起動の監視
  プロセスは、いつどのプログラムが開始され、閉じられるかを監視します。
- ウィンドウが不可視
  プログラムに、表示されるウィンドウが一切なく、バックグラウンドで動作します。もっとも無害なケースでは、たとえばデバイス ドライバ ソフトウェアなどです。
- Windows 起動時に開始
  プログラムが、レジストリの autostart キーに書き込んでいるため、Windows が起動するたびに開始されます。
- 詳細情報なし
  ファイル内に重要な標準の説明が見つかりませんでした。既定では、各ファイルの内部に説明のためのフィールドがあります。
- 非 Windows システムファイル
  ファイルは Windows オペレーティング システムの一部ではありません。Windows のシステム ファイルは Windows によって特殊なチェックと保護を受けています。
- プログラムの説明なし
  ファイル内に説明が見つかりませんでした。既定では、各ファイルの内部に説明のためのフィールドがあります。
- ファンクション: インターネット、モニタ、入力記録、隠し、操作
  ファイルに名前の付いたプロパティのあるファンクション コールが含まれています。このファンクションが利用されているという形跡がないので、レートにはあまり影響しません。
- ファンクション: 特定できず
  ファイル内に危険性のあるファンクション コールが見つかりませんでした。ただし、このようなコールはファイル内に隠すことができます。
- 不明の製造者
  ソフトウェアの製造者をファイルの説明フィールドからは識別できません。既定では、各ファイルの内部にソフトウェアの製造者を識別するためのフィールドがあります。

信頼できるプロパティ (リスクを減らす要因):

- Microsoft 署名済みファイル
  このファイルは、Microsoft によって署名されています。このファイルを Microsoft と同じように信頼することができます。
- Verisign 署名済みファイル
  このファイルは、VeriSign によって署名されています。このファイルを VeriSign と同じように信頼することができます。
- *<software product>* に属する (*<manufacturer>*)
  ファイルを信頼することができます。表記のインストール済みソフトウェアの一部分です。このソフトウェアをアンインストールすると、ファイルが削除されます。
- *<registrar>* による会社 *<manufacturer>* の証明済み
  このファイルはレジストラー (審査登録機関) によって署名されています。このファイルをこのレジストラーやソフトウェア製造者と同じように信頼することができます。
- コメント
  リスク レートに反映させるために、自分のコメントを書き込むことができます。

注意

- レートの高いプログラムが必ずしも危険だとは限りません。特定のスパイウェア プログラムと同様のプロパティを持っている可能性があるというだけです。
- **[Windows プロセス]** ボタンをクリックすると、すべての内部 Windows プロセスも表示されます。これらのプロセスは Windows オペレーティング システムに属しています。Windows のシステム プロセスは既定では表示されません。

プロセスの詳細を表示する

プロセスをクリックすると、そのプロセスに関する詳細情報を表示します。次のプロパティが表示されます:

- 名前
  ソフトウェア、またはドライバの名前を表示します。
- レート
  プロセスのセキュリティに関する客観的なレートを表示します。レートの赤いバーが長ければ長いほど、より危険性の高い機能をプロセスが含んでいることになります。ただし、レートの高いプログラムが必ずしも危険というわけではなく、スパイウェアとして認識されやすい性質を持っているということです。プロセスをクリックすると、詳細を表示して、ソフトウェアの信頼性を評価することができます。
- ファイル
  フォルダ パスとファイルの名前を表示します。
- 種類
  ファイルの種類を表示します。ファイルの種類は、プログラム、システム トレー アイコン プログラム、ブラウザ ヘルパー オブジェクト、ドライバ、サービスのいずれかになります。
- タイトルと説明
  ファイルに含まれているタイトルとファイルの説明を表示します。タイトルは、可視ウィンドウのタイトルバーに表示される文字列に相当します。
- 製造者と製品
  ファイル内にある会社の名前と製品の説明を表示します。

メモ

- **[Windows プロセス]** ボタンをクリックすると、すべての内部 Windows プロセスも表示されます。これらのプロセスは Windows オペレーティング システムに属しています。Windows のシステム プロセスは既定では表示されません。
- メイン画面にフィールドとして表示されるプロパティを選択するには、**[表示]** メニューをクリックします。

プロセスを詳しく調べる

1 調査するプロセスをクリックします。

2 ツールバーの **[オンライン検索]** ボタンをクリックします。

このソフトウェア/ドライバに関する意見を投稿したり、他のユーザーのコメントを参照することのできる www.neuber.com/taskmanager 上の情報ページが表示されます。この Web ページから Google.com でこのプロセスに関する詳細情報を検索することもできます。

メモ

- インターネットブラウザが情報(オペレーティング システム、言語設定など)を転送します。セキュリティ タスク マネージャやそのコンポーネントがインターネットに接続することはありません。
- Google.com は、もっとも使われている検索エンジンの一つで関連する結果を提供しています。

プロセスを終了する

1 終了するプロセスをクリックします。
2 **[削除]** ボタンをクリックします。
3 次のいずれかのオプションを選択します:
   - プロセス終了
     プロセスがメモリから除外されます。そのプロセスがレジストリ(Windows 設定データベース)に自動スタートエントリを書き込んでいれば、Windows の次回起動時に再びアクティブになります。
   - ファイルを隔離する
     この場合も、プロセスがメモリから除外されます。さらに、セキュリティ タスク マネージャが該当するファイルを隔離フォルダに置いて、レジストリの該当する自動スタートエントリを削除します。ファイルとレジストリ エントリは保存されるので、いつでもプロセスを復元することができます。

注意

- プロセスを終了すると、クラッシュを含むシステムの不安定を引き起こすことがあります。アドウェア プログラムを必要とするソフトウェアは動作しなくなる可能性があります。開いている文書は保存してください。

隔離フォルダを使用する

隔離フォルダは、Windows のごみ箱と同じように動作します。ファイルを隔離フォルダに入れると、そのファイルは名前が変更されて分離したフォルダに移されます。Windows レジストリの該当する自動スタート キーは削除されます。したがって、そのプロセスは開始させることができなくなります。ただし、いつでもプロセス全体を復元することが可能です:

プロセスを復元する

1 ツールバーの **[隔離]** ボタンをクリックします。
2 隔離フォルダ内で、復元するプロセスをクリックします。
3 **[復元]** ボタンをクリックします。

プロセス リストをエクスポートする

1 [ファイル] メニューの **[エクスポート]** をクリックします。
2 ファイルの種類を選びます:
   - テキストファイル (*.txt)
   - HTML 文書 (*.html)

プロセス リストを印刷する

1 [ファイル] メニューの **[印刷]** をクリックします。
2 プリンタと必要となるプロパティ(部数など)を選びます。

メモ

- **[Windows プロセス]** ボタンをクリックすると、すべての内部 Windows プロセスも表示されます。これらのプロセスは Windows オペレーティング システムに属しています。Windows のシステム プロセスは既定では表示されません。
- 定期的にプロセス リストを保存することをお勧めします。保存したプロセス リストが将来的に新しいプロセスを見つけるのに役立たせることができます。

コメントを入力する

プロセスごとにコメントを入力することができます。このコメントはプロセスのプロパティに表示されます。独自のリスク評価を設定して、セキュリティ タスク マネージャのレート付けに影響を与えることもできます。

コメントを入力するには

1 関連するプロセスを右クリックします。

2 ショートカットメニューの **[コメント]** をクリックします。

3 コメントを入力して、プロセスに関する見解がある場合は設定します。

コンピュータをスパイ プロテクタで保護する

スパイ プロテクタを実行するには、タスク バーのシステム トレーにあるアイコンをクリックします。

スパイ プロテクタは、コンピュータをキーロガー、スパイウェア、トロイの木馬から保護するために、次の機能を用意しています:

履歴の削除
Internet Explorer でのインターネット活動 (cookies、キャッシュ、履歴、入力した URL) の履歴を削除することができます。最近使ったプログラム (ACDSee、Adobe Reader、WinZip、Windows Media Player など) や Windows の [スタート] メニューの最近開いたファイルの一覧を削除することもできます。

キーボードの監視をブロック
現在の Windows セッションでのほとんどのキーロガーをブロックすることができます。キーボード入力の他のプログラムへの転送がすべてブロックされます。このようなキーボード入力の転送は、Hook ファンクションをプログラムに組み込むことによって実現されます。マクロや自動テキスト入力プログラムなどのキーボード ユーティリティでさえ、このような Hook は利用しません。

その他の監視をブロック
現在の Windows セッションのデータのログを記録するプログラムをブロックするには、次のオプションをチェックします:

キーボード入力 (間接)
他のプログラムによる内部 Windows メッセージ (キーボード入力など) の監視を防ぎます。

マウスの活動
マウスの動きやクリックの監視を防ぎます。

マクロ
ユーザー活動の記録を防ぎます。この方式はマクロ プログラムによってよく使われていますが、一般的にキーロガーには使われません。

プログラムの起動と終了
プログラムの開始と終了がログに記録されます。この機能はチュートリアル プログラム (CBT) によって対象となるソフトウェアとの連携目的でよく使われます。

注意: 一部の安全で正当なプログラム (一部のマクロ プログラムなど) でも、これらの Hook ファンクションを使うことがあります。このようなプログラムが適切に動作しなくなった場合は、該当するオプションを無効にしてコンピュータを再起動してください。

レジストリが変更されたときに警告する
プログラムが Windows レジストリにオートスタート キーを入力しようとすると、メッセージ ボックスを表示します。この種のエントリで、可視/不可視のいずれも可能となり、ソフトウェアは Windows が起動するたび

に隠れて 開始します。 危険性のあるプログラムはすべてコンピュータの 再起動時にアクティブになるためのこのようなレジストリ キーを必要とします。

セキュリティ タスク マネージャのテクニカル サポート

テクニカル サポートの 連絡先:

住所: 株式会社ピーアンドエー・インターナショナル
〒190-0012
東京都立川市曙町2-22-5 立川青色申告会館ビル 2F
FAX: 042-525-9502
ホームページ: http://www.panda.co.jp/support/

※ テクニカル サポートは、製品版をご 購入いただき、ユーザー登録された方に限らせていただきます。

セキュリティ タスク マネージャをアンインストールする

1 [スタート] メニューから [コントロール パネル] をクリックします。
2 **[プログラムの追加と削除]** をクリックします。
3 **[削除]** ボタンをクリックすると、コンピュータからセキュリティ タスク マネージャを削除します。

メモ

- セキュリティ タスク マネージャのインストールされているフォルダにある uninstal.exe を実行して削除することもできます。

試用版について

30 日間の試用期間の間、無料で試用版を使用することができます。試用期間以降もセキュリティ タスク マネージャを使い続けるには、製品版を購入する必要があります。試用版のロックを解除する登録コードをお知らせします。登録コードは、すべての試用版画面や試用版の制限を取り払い、アップデート サービスを受けることができます。

登録ユーザーになると、次の特典を受けられます:

- ソフトウェアの使用ライセンス
- 試用版のロックを解除する専用の登録コード
- 無償のマイナー アップデート
- アンチスパイ ソフトウェア: スパイ プロテクタ
  スパイ プロテクタは、インターネット履歴の抹消、レジストリの Autostart キーが変更されたときに警告、キーボードやマウスの監視の無効化などを行います。
- 無償のテクニカル サポート

ご使用のプログラムが製品版かどうかを確認するには、**[ヘルプ]** メニューの **[バージョン情報...]** をクリックします。

試用版から製品版に切り替える

1 **[登録]** メニューの **[ロック解除]** をクリックします。

2 [登録] ダイアログ ボックスに、送られた情報に表示されている通り正確に名前をコードを入力します。

3 **[ロック解除]** をクリックします。