(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2020-522808
(P2020-522808A)
(43)公表日　令和2年7月30日(2020.7.30)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/56	(2013.01)	G06F	21/56	360	
		G06F	21/56	380	

審査請求 未請求　予備審査請求 未請求　（全 50 頁）

(21)出願番号　特願2019-566622 (P2019-566622)
(86)(22)出願日　平成30年5月30日 (2018.5.30)
(85)翻訳文提出日　令和2年1月30日 (2020.1.30)
(86)国際出願番号　PCT/US2018/035205
(87)国際公開番号　WO2018/222766
(87)国際公開日　平成30年12月6日 (2018.12.6)
(31)優先権主張番号　62/512,659
(32)優先日　平成29年5月30日 (2017.5.30)
(33)優先権主張国・地域又は機関
米国 (US)

(71)出願人　517255773
サイエンプティブ　テクノロジーズ　インコーポレイテッド
アメリカ合衆国　９８２９０　ワシントン州　スノホミッシュ　シダー　アベニュー　１１０　スイート　１０３
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所
(72)発明者　スチュワート　ピー．マクロード
アメリカ合衆国　９８２９０　ワシントン州　スノホミッシュ　シダー　アベニュー　１１０　スイート　１０３　サイエンプティブ　テクノロジーズ　インコーポレイテッド内

最終頁に続く

(54)【発明の名称】カーネルモードにおけるマルウェアおよびステガノグラフィのリアルタイム検出ならびにマルウェアおよびステガノグラフィからの保護

(57)【要約】
カーネルモードにおけるマルウェアのリアルタイム検出のための方法が、ユーザモードにおいて実行されているプロセスによって開始されたファイル操作要求を検出することを含む。検出されたファイル操作要求に関連付けられたファイルバッファに関してマルウェア検出分析が行われて、マルウェアの存在を示す挙動を検出する。マルウェアの存在を示す挙動を検出することに応答して、検出されたファイル操作要求を開始することを担当するプロセスが識別される。プログラムのブラックリストおよびプログラムのホワイトリストのうちの１つまたは複数において、識別されたプロセスの検索が行われて、識別されたプロセスが信頼されたプロセスであるかどうかを決定する。識別されたプロセスが信頼されたプロセスではないと決定することに応答して、識別されたプロセスに対してマルウェア修正アクションが実行される。マルウェアを記述する情報がクライアントデバイスに送信される。

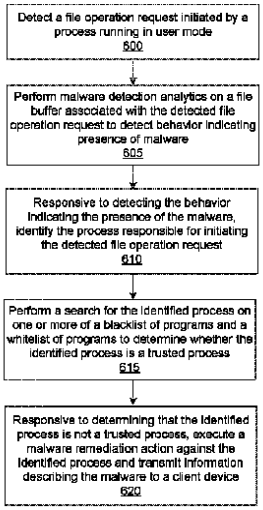

FIG. 6

【特許請求の範囲】
【請求項１】
カーネルモードにおけるマルウェアのリアルタイム検出およびマルウェアからの保護のための方法であって、
ユーザモードにおいて実行されているプロセスによって開始されたファイル操作要求を検出するステップと、
前記検出されたファイル操作要求に関連付けられたファイルバッファに関してマルウェア検出分析を行って、マルウェアの存在を示す挙動を検出するステップと、
前記マルウェアの前記存在を示す前記挙動を検出することに応答して、前記検出されたファイル操作要求を開始することを担当する前記プロセスを識別するステップと、
プログラムのブラックリストおよびプログラムのホワイトリストのうちの１つまたは複数において、前記識別されたプロセスの検索を行って、前記識別されたプロセスが信頼されたプロセスであるかどうかを決定するステップと、
前記識別されたプロセスが信頼されたプロセスではないと決定することに応答して、
前記識別されたプロセスに対してマルウェア修正アクションを実行するステップと、
前記マルウェアを記述する情報をクライアントデバイスに送信するステップと
を含むことを特徴とする方法。
【請求項２】
前記ファイル操作要求を検出する前記ステップは、
前記ファイル操作要求に対応するファイルハンドルから、前記ファイル操作要求が所定の動作に対応するかどうかを決定するステップと、
前記ファイル操作要求が所定の動作に対応すると決定することに応答して、前記ファイル操作要求をインターセプトするステップと
を含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記ファイル操作要求を前記インターセプトする前記ステップは、
フィルタマネージャによって、ファイル操作要求をインターセプトするためにミニフィルタドライバが登録されているかどうかを決定するステップと、
ファイル操作要求をインターセプトするために前記ミニフィルタドライバが登録されていると決定することに応答して、前記フィルタマネージャによって、前記ファイル操作要求を前記ミニフィルタドライバに送信するステップと
を含むことを特徴とする請求項２に記載の方法。
【請求項４】
前記マルウェア検出分析を行う前記ステップは、モンテカルロ近似、エントロピ決定、系列係数分析、算術平均決定、カイ二乗決定、および標準偏差決定のうちの１つまたは複数を行って、前記ファイルバッファ内のデータが暗号化されているかどうかを決定するステップを含むことを特徴とする請求項１に記載の方法。
【請求項５】
前記識別されたプロセスが信頼されたプロセスではないと前記決定するステップは、
プログラムの前記ブラックリスト上において前記識別されたプロセスを特定するステップをさらに含み、
前記マルウェア修正アクションを実行する前記ステップは、
前記検出されたファイル操作要求に関連付けられた書き込み操作を終了するステップと、
前記検出されたファイル操作要求をメモリから削除することによって、前記検出されたファイル操作要求を終了するステップと、
前記識別されたプロセスに関連付けられたディスクファイルイメージを隔離するステップと
をさらに含むことを特徴とする請求項１に記載の方法。
【請求項６】

プログラムの前記ホワイトリスト上において前記識別されたプロセスを特定することに応答して、ミニフィルタドライバによって、前記検出されたファイル操作要求を無視するステップをさらに含むことを特徴とする請求項１に記載の方法。
【請求項７】
前記識別されたプロセスが信頼されたプロセスであるかどうかを決定する前記ステップは、プログラムの前記ブラックリストまたはプログラムの前記ホワイトリスト上において前記プロセスを特定しないことに応答して、前記クライアントデバイスに前記識別されたプロセスを許可することを求める要求を送信するステップをさらに含むことを特徴とする請求項１に記載の方法。
【請求項８】
前記識別されたプロセスが信頼されたプロセスではないと前記決定するステップは、前記クライアントデバイスに前記識別されたプロセスを許可することを求める前記要求を前記送信することに応答して、前記識別されたプロセスが許可されないというメッセージを前記クライアントデバイスから受信するステップをさらに含むことを特徴とする請求項７に記載の方法。
【請求項９】
前記識別されたプロセスをプログラムの前記ブラックリストに追加するステップをさらに含むことを特徴とする請求項８に記載の方法。
【請求項１０】
前記識別されたプロセスが許可されたというメッセージを前記クライアントデバイスから受信することに応答して、前記識別されたプロセスをプログラムの前記ホワイトリストに追加するステップをさらに含むことを特徴とする請求項１に記載の方法。
【請求項１１】
命令を記憶する非一時的コンピュータ可読媒体であって、前記命令は、少なくとも１つのプロセッサによって実行されたとき、前記少なくとも１つのプロセッサに、
ユーザモードにおいて実行されているプロセスによって開始されたファイル操作要求を検出することと、
前記検出されたファイル操作要求に関連付けられたファイルバッファに関してマルウェア検出分析を行って、マルウェアの存在を示す挙動を検出することと、
前記マルウェアの前記存在を示す前記挙動を検出することに応答して、前記検出されたファイル操作要求を開始することを担当する前記プロセスを識別することと、
プログラムのブラックリストおよびプログラムのホワイトリストのうちの１つまたは複数において、前記識別されたプロセスの検索を行って、前記識別されたプロセスが信頼されたプロセスであるかどうかを決定することと、
前記識別されたプロセスが信頼されたプロセスではないと決定することに応答して、
　前記識別されたプロセスに対してマルウェア修正アクションを実行することと、
　前記マルウェアを記述する情報をクライアントデバイスに送信することと
を行わせることを特徴とする非一時的コンピュータ可読媒体。
【請求項１２】
前記ファイル操作要求を検出することを前記少なくとも１つのプロセッサに行わせる前記命令は、前記少なくとも１つのプロセッサに、
前記ファイル操作要求に対応するファイルハンドルから、前記ファイル操作要求が所定の動作に対応するかどうかを決定することと、
前記ファイル操作要求が所定の動作に対応すると決定することに応答して、前記ファイル操作要求をインターセプトすることと
を行わせる命令をさらに含むことを特徴とする請求項１１に記載の非一時的コンピュータ可読媒体。
【請求項１３】
前記ファイル操作要求をインターセプトすることを前記少なくとも１つのプロセッサに行わせる前記命令は、前記少なくとも１つのプロセッサに、

フィルタマネージャによって、ファイル操作要求をインターセプトするためにミニフィルタドライバが登録されているかどうかを決定することと、
ファイル操作要求をインターセプトするために前記ミニフィルタドライバが登録されていると決定することに応答して、前記フィルタマネージャによって、前記ファイル操作要求を前記ミニフィルタドライバに対して送信することと
を行わせる命令をさらに含むことを特徴とする請求項１２に記載の非一時的コンピュータ可読媒体。
【請求項１４】
前記マルウェア検出分析を行うことを前記少なくとも１つのプロセッサに行わせる前記命令は、前記少なくとも１つのプロセッサに、
モンテカルロ近似、エントロピ決定、系列係数分析、算術平均決定、カイ二乗決定、および標準偏差決定のうちの１つまたは複数を行って、前記ファイルバッファ内のデータが暗号化されているかどうかを決定することを行わせる命令をさらに含むことを特徴とする請求項１１に記載の非一時的コンピュータ可読媒体。
【請求項１５】
前記識別されたプロセスが信頼されたプロセスではないと決定することを前記少なくとも１つのプロセッサに行わせる前記命令は、前記少なくとも１つのプロセッサに、
プログラムの前記ブラックリスト上において前記識別されたプロセスを特定することを行わせる命令をさらに含み、
前記マルウェア修正アクションを実行することを前記少なくとも１つのプロセッサに行わせる前記命令は、前記少なくとも１つのプロセッサに、
前記検出されたファイル操作要求に関連付けられた書き込み操作を終了することと、
前記検出されたファイル操作要求をメモリから削除することによって、前記検出されたファイル操作要求を終了することと、
前記識別されたプロセスに関連付けられたディスクファイルイメージを隔離することとを行わせる命令をさらに含むことを特徴とする請求項１１に記載の非一時的コンピュータ可読媒体。
【請求項１６】
前記少なくとも１つのプロセッサによって実行されたとき、前記少なくとも１つのプロセッサに、
プログラムの前記ホワイトリスト上において前記識別されたプロセスを特定することに応答して、ミニフィルタドライバによって、前記検出されたファイル操作要求を無視することを行わせる命令をさらに記憶することを特徴とする請求項１１に記載の非一時的コンピュータ可読媒体。
【請求項１７】
前記識別されたプロセスが信頼されたプロセスであるかどうかを決定することを前記少なくとも１つのプロセッサに行わせる前記命令は、前記少なくとも１つのプロセッサに、
プログラムの前記ブラックリストまたはプログラムの前記ホワイトリスト上において前記プロセスを特定しないことに応答して、前記クライアントデバイスに前記識別されたプロセスを許可することを求める要求を送信することを行わせる命令をさらに含むことを特徴とする請求項１１に記載の非一時的コンピュータ可読媒体。
【請求項１８】
前記識別されたプロセスが信頼されたプロセスではないと決定することを前記少なくとも１つのプロセッサに行わせる前記命令は、前記少なくとも１つのプロセッサに、
前記クライアントデバイスに前記識別されたプロセスを許可することを求める前記要求を送信することに応答して、前記識別されたプロセスが許可されないというメッセージを前記クライアントデバイスから受信することを行わせる命令をさらに含むことを特徴とする請求項１７に記載の非一時的コンピュータ可読媒体。
【請求項１９】
前記少なくとも１つのプロセッサによって実行されたとき、前記少なくとも１つのプロ

セッサに、
前記識別されたプロセスをプログラムの前記ブラックリストに追加することを行わせる命令をさらに記憶することを特徴とする請求項１８に記載の非一時的コンピュータ可読媒体。
【請求項２０】
前記少なくとも１つのプロセッサによって実行されたとき、前記少なくとも１つのプロセッサに、
前記識別されたプロセスが許可されたというメッセージを前記クライアントデバイスから受信することに応答して、前記識別されたプロセスをプログラムの前記ホワイトリストに追加することを行わせる命令をさらに記憶することを特徴とする請求項１１に記載の非一時的コンピュータ可読媒体。
【請求項２１】
カーネルモードにおけるステガノグラフィのリアルタイム検出およびステガノグラフィからの保護のための方法であって、
ファイアウォール、オペレーティングシステム、または電子メールシステムを介して、ファイルの送信を検出するステップと、
前記ファイルのサイズを決定するステップと、
ファイルシステムから前記ファイルの記憶されたファイルサイズを取り出すステップと、
前記ファイルの前記決定されたサイズを前記ファイルの前記記憶されたファイルサイズと比較するステップと、
前記ファイルの前記決定されたサイズが前記ファイルの前記記憶されたファイルサイズよりも大きいことに応答して、前記ファイルに関してステガノグラフィ検出分析を実行するステップと、
前記ステガノグラフィ検出分析が前記ファイルにおけるステガノグラフィの存在を示すことに応答して、
ステガノグラフィ修正アクションを実行するステップ、および
前記ステガノグラフィを記述する情報をクライアントデバイスに対して送信するステップと
を含むことを特徴とする方法。
【請求項２２】
前記ファイルの前記サイズを決定する前記ステップは、
前記ファイルのセクションヘッダについてポインタを取得するステップであって、前記セクションヘッダは前記ファイルの複数のセクションに関連付けられている、該ステップと、
前記ファイルの前記複数のセクションの各セクションについて、前記セクションのサイズを決定するステップと、
前記ファイルの前記複数のセクションの各セクションの前記サイズを合計して、前記ファイルの前記サイズを決定するステップと
を含むことを特徴とする請求項２１に記載の方法。
【請求項２３】
前記ファイルの前記セクションヘッダに対する前記ポインタを取得する前記ステップは、
前記ファイルのファイル名または前記ファイルのパスを使用して前記ファイルを開くステップと、
前記ファイルのヘッダを読み取るステップと、
前記ヘッダからマジックナンバーを取り出すステップと、
前記マジックナンバーを検証して、前記ファイルの前記セクションヘッダについてポインタを取得するステップと
を含むことを特徴とする請求項２２に記載の方法。

【請求項２４】
前記ファイルに対して前記ステガノグラフィ検出分析を実行する前記ステップは、
前記ファイルにおける付加されたペイロードを識別するステップと、
前記付加されたペイロードを分析して、前記付加されたペイロードのファイルフォーマットを決定するステップと、
前記付加されたペイロードの前記ファイルフォーマットに基づいて、前記ステガノグラフィ検出分析を実行するステップと
を含むことを特徴とする請求項２１に記載の方法。
【請求項２５】
前記ファイルに対して前記ステガノグラフィ検出分析を実行する前記ステップは、
前記ファイルにおける付加されたペイロードを識別するステップと、
モンテカルロ近似、エントロピ決定、系列係数分析、算術平均決定、カイ二乗決定、および標準偏差決定のうちの１つまたは複数を行って、前記付加されたペイロード内のデータが暗号化されているかどうかを決定するステップと
を含むことを特徴とする請求項２１に記載の方法。
【請求項２６】
前記ファイルに対して前記ステガノグラフィ検出分析を実行する前記ステップは、
前記ファイルにおける付加されたペイロードを識別するステップと、
前記付加されたペイロード内の許可されていないデータの存在を識別するステップと
を含むことを特徴とする請求項２１に記載の方法。
【請求項２７】
前記ファイルに対して前記ステガノグラフィ検出分析を実行する前記ステップは、
前記ファイルにおける付加されたペイロードを識別するステップと、
前記付加されたペイロード内のアセンブリレベル命令またはマシンレベル命令の存在を識別するステップと
を含むことを特徴とする請求項２１に記載の方法。
【請求項２８】
前記ステガノグラフィ修正アクションを実行する前記ステップは、
前記ファイルの処理および送信を終了するステップと、
前記ファイルを隔離するステップと
を含むことを特徴とする請求項２１に記載の方法。
【請求項２９】
命令を記憶する非一時的コンピュータ可読媒体であって、前記命令は、少なくとも１つのプロセッサによって実行されたとき、前記少なくとも１つのプロセッサに、
ファイアウォール、オペレーティングシステム、または電子メールシステムを介して、ファイルの送信を検出することと、
前記ファイルのサイズを決定することと、
ファイルシステムから前記ファイルの記憶されたファイルサイズを取り出すことと、
前記ファイルの前記決定されたサイズを、前記ファイルの前記記憶されたファイルサイズと比較することと、
前記ファイルの前記決定されたサイズが前記ファイルの前記記憶されたファイルサイズよりも大きいことに応答して、前記ファイルについてステガノグラフィ検出分析を実行することと、
前記ステガノグラフィ検出分析が前記ファイルにおけるステガノグラフィの存在を示すことに対し応答して、
ステガノグラフィ修正アクションを実行すること、および
前記ステガノグラフィを記述する情報をクライアントデバイスに送信することと
を行わせることを特徴とする非一時的コンピュータ可読媒体。
【請求項３０】
前記ファイルの前記サイズを決定することを前記少なくとも１つのプロセッサに行わせ

る前記命令は、前記少なくとも１つのプロセッサに、
前記ファイルのセクションヘッダについてポインタを取得することであって、前記セクションヘッダは前記ファイルの複数のセクションに関連付けられている、該取得することと、
前記ファイルの前記複数のセクションの各セクションについて、前記セクションのサイズを決定することと、
前記ファイルの前記複数のセクションの各セクションの前記サイズを合計して、前記ファイルの前記サイズを決定することと
を行わせる命令を含むことを特徴とする請求項２９に記載の非一時的コンピュータ可読媒体。

【請求項３１】
前記ファイルの前記セクションヘッダについて前記ポインタを取得することを前記少なくとも１つのプロセッサに行わせる前記命令は、前記少なくとも１つのプロセッサに、
前記ファイルのファイル名または前記ファイルのパスを使用して前記ファイルを開くことと、
前記ファイルのヘッダを読み取ることと、
前記ヘッダからマジックナンバーを取り出すことと、
前記マジックナンバーを検証して、前記ファイルの前記セクションヘッダについてポインタを取得することと
を行わせる命令を含むことを特徴とする請求項３０に記載の非一時的コンピュータ可読媒体。

【請求項３２】
前記ファイルに関して前記ステガノグラフィ検出分析を実行することを前記少なくとも１つのプロセッサに行わせる前記命令は、前記少なくとも１つのプロセッサに、
前記ファイルにおける付加されたペイロードを識別することと、
前記付加されたペイロードを分析して、前記付加されたペイロードのファイルフォーマットを決定することと、
前記付加されたペイロードの前記ファイルフォーマットに基づいて、前記ステガノグラフィ検出分析を実行することと
を行わせる命令を含むことを特徴とする請求項２９に記載の非一時的コンピュータ可読媒体。

【請求項３３】
前記ファイルに関して前記ステガノグラフィ検出分析を実行することを前記少なくとも１つのプロセッサに行わせる前記命令は、前記少なくとも１つのプロセッサに、
前記ファイルにおける付加されたペイロードを識別することと、
モンテカルロ近似、エントロピ決定、系列係数分析、算術平均決定、カイ二乗決定、および標準偏差決定のうちの１つまたは複数を行って、前記付加されたペイロード内のデータが暗号化されているかどうかを決定することと
を行わせる命令を含むことを特徴とする請求項２９に記載の非一時的コンピュータ可読媒体。

【請求項３４】
前記ファイルに関して前記ステガノグラフィ検出分析を実行することを前記少なくとも１つのプロセッサに行わせる前記命令は、前記少なくとも１つのプロセッサに、
前記ファイルにおける付加されたペイロードを識別することと、
前記付加されたペイロード内の許可されていないデータの存在を識別することと
を行わせる命令を含むことを特徴とする請求項２９に記載の非一時的コンピュータ可読媒体。

【請求項３５】
前記ファイルに関して前記ステガノグラフィ検出分析を実行することを前記少なくとも１つのプロセッサに行わせる前記命令は、前記少なくとも１つのプロセッサに、

前記ファイルにおける付加されたペイロードを識別することと、
前記付加されたペイロード内のアセンブリレベル命令またはマシンレベル命令の存在を識別することと
を行わせる命令を含むことを特徴とする請求項２９に記載の非一時的コンピュータ可読媒体。
【請求項３６】
前記ステガノグラフィ修正アクションを実行することを前記少なくとも１つのプロセッサに行わせる前記命令は、前記少なくとも１つのプロセッサに、
前記ファイルの処理および送信を終了することと、
前記ファイルを隔離することと
を行わせる命令を含むことを特徴とする請求項２９に記載の非一時的コンピュータ可読媒体。
【請求項３７】
コンピュータシステムであって、
少なくとも１つのコンピュータプロセッサと、
命令を記憶する非一時的コンピュータ可読媒体と
を備え、
前記命令は、前記少なくとも１つのコンピュータプロセッサによって実行されたとき、前記少なくとも１つのプロセッサに、
ファイアウォール、オペレーティングシステム、または電子メールシステムを介して、ファイルの送信を検出することと、
前記ファイルのサイズを決定することと、
ファイルシステムから前記ファイルの記憶されたファイルサイズを取り出すことと、
前記ファイルの前記決定されたサイズを前記ファイルの前記記憶されたファイルサイズと比較することと、
前記ファイルの前記決定されたサイズが前記ファイルの前記記憶されたファイルサイズよりも大きいことに応答して、前記ファイルに関してステガノグラフィ検出分析を実行することと、
前記ステガノグラフィ検出分析が前記ファイルにおけるステガノグラフィの存在を示すことに応答して、
ステガノグラフィ修正アクションを実行すること、および
前記ステガノグラフィを記述する情報をクライアントデバイスに送信することと
を行わせることを特徴とするコンピュータシステム。
【請求項３８】
前記ファイルの前記サイズを決定することを前記少なくとも１つのコンピュータプロセッサに行わせる前記命令は、前記少なくとも１つのコンピュータプロセッサに、
前記ファイルのセクションヘッダについてポインタを取得することであって、前記セクションヘッダは前記ファイルの複数のセクションに関連付けられている、取得することと、
前記ファイルの前記複数のセクションの各セクションについて、前記セクションのサイズを決定することと、
前記ファイルの前記複数のセクションの各セクションの前記サイズを合計して、前記ファイルの前記サイズを決定することと
を行わせる命令を含むことを特徴とする請求項３７に記載のコンピュータシステム。
【請求項３９】
前記ファイルの前記セクションヘッダについて前記ポインタを取得することを前記少なくとも１つのコンピュータプロセッサに行わせる前記命令は、前記少なくとも１つのコンピュータプロセッサに、
前記ファイルのファイル名または前記ファイルのパスを使用して前記ファイルを開くことと、

前記ファイルのヘッダを読み取ることと、
前記ヘッダからマジックナンバーを取り出すことと、
前記マジックナンバーを検証して、前記ファイルの前記セクションヘッダについてポインタを取得することと
を行わせる命令を含むことを特徴とする請求項３８に記載のコンピュータシステム。
【請求項４０】
前記ファイルに関して前記ステガノグラフィ検出分析を実行することを前記少なくとも１つのコンピュータプロセッサに行わせる前記命令は、前記少なくとも１つのコンピュータプロセッサに、
前記ファイルにおける付加されたペイロードを識別することと、
前記付加されたペイロードを分析して、前記付加されたペイロードのファイルフォーマットを決定することと、
前記付加されたペイロードの前記ファイルフォーマットに基づいて、前記ステガノグラフィ検出分析を実行することと
を行わせる命令を含むことを特徴とする請求項３７に記載のコンピュータシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、一般にマルウェアの検出に関し、特に、カーネルモードにおけるマルウェアおよびステガノグラフィのリアルタイム検出ならびにマルウェアおよびステガノグラフィからの保護に関する。
【背景技術】
【０００２】
関連出願の相互参照
本出願は、参照によりその全体が組み込まれている、２０１７年５月３０日に出願された米国特許仮出願第６２／５１２，６５９号の利益を主張するものである。
【０００３】
マルウェア（ｍａｌｗａｒｅ）とは、所有者の認識または許可なしにコンピュータ、タブレット、またはデバイスに感染する可能性がある悪意のあるコンピュータソフトウェアプログラムを指す。ステガノグラフィは、デバイスおよびネットワークにマルウェアを感染させる１つのそのような方法である。
【０００４】
マルウェアは、ウイルス、ワーム、トロイの木馬、ボットネット、スパイウェア、およびアドウェアを含むことがある。ウイルスは、実行可能プログラムにアタッチした後にそれら自体を複製する。ワームはネットワークにわたってそれら自体を複製して、多数のデバイスに急速に感染する。トロイの木馬はそれら自体を正当なソフトウェアとして偽装し、ユーザの識別情報、パスワード、および他の個人情報を盗もうとする。ボットネットは、リモート制御される感染されたデバイスのグループである。個々のボット（デバイス）が、スパム電子メールを送るかまたはサービス妨害攻撃に参加するように指示されることが可能である。スパイウェアは、キーストローク、クレジットカード番号、および他の個人情報を捕捉するように設計されている。アドウェアは、デバイスに感染し、必要とされない広告をダウンロードし表示する。
【０００５】
従来のマルウェア防止ツールは、署名を検出して、マルウェアを隔離および修復し、または除去しようとすることがある。しかしながら、マルウェアプログラムの数は劇的に増加しており、署名は通常、知られているマルウェアのみについて作成される。したがって、従来の署名ベースの手法は通常、未知のマルウェアを識別または検出することができない。
【０００６】
さらに、ルールを使用した実行時ヒューリスティックスキャンに基づく従来の手法は、

多くの誤検出および検出漏れを発生することがある。仮想マシンにおいて疑わしいファイルを実行し悪意のある挙動を観察するサンドボックス化に基づく他の従来の手法では、サンドボックス（仮想マシンまたはコンテナ）内に自身があるかどうかを決定して検出を回避できるマルウェアを検出することが通常は不可能である。最後に、静的コード分析に基づく従来の手法もマルウェアを確実に検出することができない。

【図面の簡単な説明】

【０００７】

開示される実施形態は、詳細な説明、添付の特許請求の範囲、および添付の図（または図面）からより容易に明らかになる利点および特徴を有している。図の簡単な紹介は以下の通りである。

【０００８】

【図１】実施形態に従う、カーネルモードにおけるマルウェアおよびステガノグラフィのリアルタイム検出ならびにマルウェアおよびステガノグラフィからの保護のためのシステムの例示的なブロック図である。

【図２】実施形態に従う、プラットフォーム上のユーザモードにおいて実行されているアプリケーションに関するマルウェアのリアルタイム検出およびマルウェアからの保護の例示的なブロック図である。

【図３】実施形態に従う、マルウェアのリアルタイム検出およびマルウェアからの保護のための例示的なフィルタマネージャおよびミニフィルタドライバを示す図である。

【図４】実施形態に従う、マルウェアのリアルタイム検出およびマルウェアからの保護のためのボリュームシャドウサービス（ＶＳＳ）の例示的なコンポーネントを示す図である。

【図５】実施形態に従う、モンテカルロパイ近似に関する例示的なデータ点を示す図である。

【図６】実施形態に従う、マルウェアのリアルタイム検出およびマルウェアからの保護のための例示的なプロセスを示す図である。

【図７】実施形態に従う、カーネルモードにおけるステガノグラフィのリアルタイム検出およびステガノグラフィからの保護のための例示的なポータブル実行可能（ＰＥ）ファイルのコンポーネントを示す図である。

【図８】実施形態に従う、カーネルモードにおけるステガノグラフィのリアルタイム検出およびステガノグラフィからの保護のための例示的なプロセスを示す図である。

【図９】マシン可読媒体から命令を読み取ってそれらをプロセッサまたはコントローラにおいて実行することができる例示的なマシンのコンポーネントを示すブロック図である。

【発明を実施するための形態】

【０００９】

図面（図）および以下の説明は、単に例示のための好ましい実施形態に関する。以下の議論から、本明細書に開示される構造および方法の代替的実施形態が、特許請求の範囲の原理から逸脱することなく採用されてよい実施可能な代替形態として容易に認識されることに留意されたい。

【００１０】

ここで、いくつかの実施形態が詳細に参照され、それらの例が添付の図面に示される。実現可能な限り、同様または類似の参照番号が図面において使用されてよく、同様または類似の機能性を示してよいことに留意されたい。図は、単に例示を目的として、開示されるシステム（または方法）の実施形態を示す。以下の説明から、本明細書に示される構造および方法の代替的実施形態が、本明細書に説明される原理から逸脱することなく採用されてよいことは当業者には容易に理解される。

【００１１】

序論

従来のセキュリティ製品は、疑わしいアプリケーションプログラムインターフェース（ＡＰＩ）コールおよびアクションを探すことによって未知のマルウェアからデバイスを保

護するために、挙動分析および実行時ヒューリスティックスを含んでよい。マルウェアは、コンピュータおよびコンピュータシステムを損傷させまたは無効にすることが意図されたソフトウェアを指す。マルウェアは、ポリモーフィックまたはメタモーフィックなマルウェアを作成することによってセキュリティ製品による検出を回避する洗練されたプログラムが含むことがある。ポリモーフィックマルウェアは、異なる実行で新しい「署名」を生成する変異エンジンを使用して破壊的なコードを暗号化することによって変異する。メタモーフィックマルウェアは、実行可能コードを動的に再構築して悪意を分かりにくくする。検出を回避するために、マルウェアは、プッシュ、ポップ、ＮＯＰ、およびジャンプ命令などの冗長なプロセッサオペコードを追加して、実行ファイルの署名を変更するが、機能性に影響しないことが可能である。

【００１２】

ランサムウェアは、急成長しているマルウェアのカテゴリである。ランサムウェアは、ユーザのデバイスまたは個人データに対するアクセスを回復するために「身代金を支払う」ようにユーザに強制することを目的に、コンピュータ、タブレット、デバイス、またはスマートフォンに感染する種類のマルウェアである。いくつかの種類のランサムウェアは、ユーザデバイスまたはシステムをロックして、それらのデバイスまたはシステムにユーザがアクセスするのを防止することがある。他の種類のランサムウェアは、暗号化ソフトウェアを使用して、ワープロ文書、写真、音楽、ビデオ、電子メールなどのユーザの個人データを暗号化することがある。そのような場合、ユーザは、アクセスを回復するために身代金を支払うことを要求されることがある。ステガノグラフィは、デバイスおよびネットワークにランサムウェアを感染させる１つのそのような方法である。

【００１３】

ステガノグラフィは、コンピュータファイル、メッセージ、画像、またはビデオを別のコンピュータファイル、メッセージ、画像、またはビデオ内に隠す手法を指す。デジタルステガノグラフィにおいて、電子通信は、文書ファイル、画像ファイル、プログラム、またはプロトコルなどのトランスポート層内のステガノグラフィ符号化を含むことがある。メディアファイルは、それらのサイズが大きいのでステガノグラフィ送信のために使用されることがある。たとえば、送信者は、無害な画像ファイルから開始し、各百番目のピクセルの色をアルファベットの文字に対応するように調整することがある。

【００１４】

ランサムウェアを検出するための従来の方法は、マルウェアファイル署名の検出、実行時ヒューリスティックスキャン、サンドボックス化、静的コード分析などに依拠してよい。しかしながら、マルウェアファイル署名を検出することに基づく従来の方法は、以前に識別されたマルウェアのみを検出することがあり、自己変形するランサムウェアなどの新しい形態のランサムウェアから保護をできないことがある。実行時ヒューリスティックスキャンに基づく従来の方法は、ルールのセットを使用して誤検出および検出漏れを発生することがある。サンドボックス化に基づく従来の方法は、仮想マシンにおける疑わしいファイルを実行し、悪意のある挙動を観察してよい。しかしながら、ランサムウェアは、それがサンドボックス（仮想マシンまたはコンテナ）内にあるかどうかを決定し検出を回避できることがある。静的コード分析に基づく従来の方法は、実行可能コードを逆アセンブルし、解析ツリーを作成して、疑わしいＡＰＩコールを識別しようとしてよい。しかしながら、静的コード分析に基づくそのような従来の方法は、ランサムウェアを確実に検出することができない。

【００１５】

「パックされた」マルウェアおよび「隠されたマルウェア」は、従来は検出されず、ローカルデバイスのファイアウォール、ネットワークのファイアウォール、およびアンチウイルスソフトウェアを通過することがある。フィルタリングおよびディープパケット検査、侵入保護システム、アプリケーション認識などの従来のファイアウォール機能がしばしば使用される。しかしながら、従来のファイアウォールは、マルウェアを検出するためにポート割り当てに依拠する。したがって、実際のアプリケーション種類とアプリケーショ

ンについてのファイアウォールの仮定との間の関連付けが弱い。さらに、ディープパケット検査は、強力な暗号化のために終端点がファイアウォールではなく宛先であるときは価値が限られる。

【００１６】

構成概要

マルウェアのリアルタイム検出およびマルウェアからの保護のためのシステム、方法、および／またはコンピュータプログラム製品（たとえば、１つまたは複数の処理ユニットによって実行可能な命令を記憶するコンピュータ可読記憶媒体）が、例示的な実施形態によって開示される。コンピュータにおけるプロセッサは一般に、少なくとも２つの異なるモード、すなわちユーザモードとカーネルモードにおいて実行してよい。典型的には、アプリケーションはユーザモードにおいて実行してよく、コアオペレーティングシステムコンポーネントはカーネルモードにおいて実行してよい。

【００１７】

一実施形態において、ユーザモードにおいて実行されているプロセスによって開始されたファイル操作要求が検出される。検出されたファイル操作要求に関連付けられたファイルバッファに関してマルウェア検出分析が行われて、マルウェアの存在を示す挙動を検出する。マルウェアの存在を示す挙動を検出することに応答して、検出されたファイル操作要求を開始することを担当するプロセスが識別される。プログラムのブラックリストおよびプログラムのホワイトリストのうちの１つまたは複数において、識別されたプロセスの検索が行われて、識別されたプロセスが信頼されたプロセスであるかどうかを決定する。識別されたプロセスが信頼されたプロセスではないと決定することに応答して、識別されたプロセスに対してマルウェア修正アクションが実行される。マルウェアを記述する情報がクライアントデバイスに送信される。

【００１８】

開示されている実施形態は、悪意のある攻撃およびデータ損失からデバイスおよびネットワークを保護するために、セキュリティ脅威の統合されたリアルタイム検出を行う。静的分析が行われて、テストの配列を使用して、マルウェアに感染された可能性のあるファイルを求めて検索し、疑わしいプログラム命令を識別して、それがマルウェアであるかどうかを決めてよい。検出されると、バイトの一意のシーケンスが、実行を必要とせずに悪意のあるソフトウェアを識別し、それを正当なプログラムから区別する。動的分析は、実行中にアプリケーションの挙動を監視して、それがマルウェアを含むかどうかを決定する。マルウェアを直接識別することに加えて、システムの状態がリアルタイムにおいて監視される。

【００１９】

現在のマルウェアはポリモーフィックまたはメタモーフィックである場合があるので、マルウェアはファイル署名を使用する従来のアンチウイルスソフトウェアによる検出を回避することがある。一実施形態では、一意の状態ベースのメカニズムを使用して、許可なしにファイルが暗号化されているかどうかを検出する。担当するプロセスが識別され、他のデバイスから隔離される。これにより、マルウェアを事前に知ることを不要にする。データの状態の変化がマルウェアの識別を迅速かつ確実にする。統合されたステガノグラフィ検出が、デバイス上の実行から隠されたデータおよびマルウェアの存在を識別する。システムは、ファイアウォール上でインラインを実行して、隠されたデータを有するマルウェアおよびファイルがネットワークに入るのを防止する。それは、一緒に、静的分析、動的分析、システム状態変化の強みを活用して、より少ない誤検知およびより少ない検出漏れでマルウェアをより正確に検出する統合されたエンドツーエンドシステムとして働く。

【００２０】

さらに、カーネルモードにおけるステガノグラフィのリアルタイム検出およびステガノグラフィからの保護のためのシステム、方法、および／またはコンピュータプログラム製品（たとえば、１つまたは複数の処理ユニットによって実行可能な命令を記憶するコンピュータ可読記憶媒体）が、例示的な実施形態によって開示される。ファイアウォール、オ

ペレーティングシステム、または電子メールシステムを介するファイルの送信が検出される。ファイルのサイズが決定される。ファイルシステムからファイルの記憶されたファイルサイズが取り出される。ファイルの決定されたサイズは、ファイルの記憶されたファイルサイズと比較される。ファイルの決定されたサイズがファイルの記憶されたファイルサイズよりも大きいことに応答して、ファイルについてステガノグラフィ検出分析が実行される。ステガノグラフィ検出分析がファイルにおけるステガノグラフィの存在を示すことに応答して、ステガノグラフィ修正アクションが実行される。ステガノグラフィを記述する情報がクライアントデバイスに送信される。

【００２１】

開示されている実施形態は、許可されていないデータ暗号化、データ流出、ルートキットインストール、およびステガノグラフィを識別するために分析の組み合わせを統合することによって、既知と未知の両方のマルウェアおよびセキュリティ脅威から多くの種類のデバイスを保護することができる。このシステムおよび方法は、既存の技法と比較して、より少ない計算オーバヘッドおよびストレージ使用率で、より速くかつより正確にマルウェアを検出、隔離、分析、および除去するためのエンドツーエンド解決策をもたらす。ファイルシステムの状態変化のリアルタイム分析は、ユーザのデータが暗号化または削除される前にリアルタイム保護を可能にする。動的ＡＰＩ監視ヒューリスティックス、動的コード分析、トリップワイヤおよびハニーポットの作成は、ほぼリアルタイムで疑わしい挙動を発見する助けとなる。

【００２２】

開示されている実施形態は、システム構成（ＭＦＴ、ＭＢＲ、レジストリ、およびＷｉｎｄｏｗｓタスクマネージャ）の改ざんを積極的にチェックし、悪意のある変更を修正して、ユーザがロックアウトされていないことを保証する。ＭＦＴは、マスタファイルテーブルを指す。ＭＢＲは、マスタブートレコードを指す。Ｗｉｎｄｏｗｓレジストリは、オペレーティングシステムについて、およびアプリケーション、デバイスドライバ、セキュリティアカウントマネージャ（ＳＡＭ）に関する情報についての低レベル構成設定を記憶し、システムパフォーマンスカウンタにアクセスする。タスクマネージャは、プログラムの実行をスケジューリングする。集中化された詳細なロギングシステムは、システム管理者がそれらの環境におけるすべてのデバイスを管理し、様々なデータ分析の基盤を提供することを可能にする。

【００２３】

開示されている実施形態の利益および利点は、ランサムウェアが存在する場所の知識なしにシステムを継続的に洗浄することを含む。このアプローチの一部として、方法は、サーバ、たとえばＤＮＳサーバをデコミッションしてよい。結果は、ランサムウェアのエビデンスである状態変化の隔離および検出アプローチである。ポリモーフィックランサムウェアは、コンテナ内のペイロードを暗号化し、従来の方法によって検出不可能である署名を変更することができる。メタモーフィックランサムウェアは、意味のないマシン命令をコードに挿入することによってその署名を変更する。知られているマルウェアを検索する代わりに、開示されている実施形態はシステムにおける状態変化を探す。さらなる利点および利益は、マルウェアを識別するためにプログラムのブラックリストを使用する際の簡潔性を含む。したがって、開示されている実施形態は、開示されているシステムおよびその関係付けられたデータベースまたはサードパーティの脅威インテリジェンス／サービスプロバイダがプログラムのブラックリストをコンパイルおよび更新するので、必要なメンテナンスが少ない。

【００２４】

したがって、開示されている実施形態は、静的状態分析（ディスクのスキャン）およびリアルタイム分析を行ってよい。マルウェア署名は使用されないが、ファイルが暗号化されたかどうかを検出するために計算が行われる。Ｉ／Ｏ要求パケット内の読み取りバッファおよび書き込みバッファの両方が使用されてよい。したがって、追加のメモリ割り当てまたは追加の読み取り／書き込み操作が必要とされない。追加のメモリおよび計算を必要

とする後処理分析がない。別の実施形態において、開示されている方法およびシステムは、メモリベースの攻撃に対処するために使用されてよく、ファイルは、ディスク上ではなくメモリに記憶される。ファイル割り当てのメモリ内監視が行われ、ディスクに接触しないデータがスキャンされてよい。ファイアウォールとインラインで統合されたデバイス上での統計分析の組み合わせが、ネットワークおよびデバイスのための強力な保護を提供する。

【００２５】

マルウェアおよびステガノグラフィ検出および防止のための方法およびシステム

一実施形態において、カーネルモードにおけるマルウェアのリアルタイム検出およびマルウェアからの保護のための方法は、ユーザモードにおいて実行されているプロセスによって開始されたファイル操作要求を検出するステップを含む。検出されたファイル操作要求に関連付けられたファイルバッファに関してマルウェア検出分析が行われて、マルウェアの存在を示す挙動を検出する。マルウェアの存在を示す挙動を検出することに応答して、検出されたファイル操作要求を開始することを担当するプロセスが識別される。プログラムのブラックリストおよびプログラムのホワイトリストのうちの１つまたは複数において、識別されたプロセスの検索が行われて、識別されたプロセスが信頼されたプロセスであるかどうかを決定する。識別されたプロセスが信頼されたプロセスではないと決定することに応答して、識別されたプロセスに対してマルウェア修正アクションが実行される。マルウェアを記述する情報がクライアントデバイスに送信される。

【００２６】

一実施形態において、ファイル操作要求を検出するステップは、ファイル操作要求に対応するファイルハンドルから、ファイル操作要求が所定の動作に対応するかどうかを決定するステップを含む。ファイル操作要求が所定の動作に対応すると決定することに応答して、ファイル操作要求がインターセプトされる。

【００２７】

一実施形態において、ファイル操作要求をインターセプトするステップは、フィルタマネージャによって、ファイル操作要求をインターセプトするためにミニフィルタドライバが登録されているかどうかを決定するステップを含む。ファイル操作要求をインターセプトするためにミニフィルタドライバが登録されていると決定することに応答して、フィルタマネージャは、ファイル操作要求をミニフィルタドライバに送信する。

【００２８】

一実施形態において、マルウェア検出分析を行うステップは、モンテカルロ近似、エントロピ決定、系列係数分析、算術平均決定、カイ二乗決定、および標準偏差決定のうちの１つまたは複数を行って、ファイルバッファ内のデータが暗号化されているかどうかを決定するステップを含む。

【００２９】

一実施形態において、識別されたプロセスが信頼されたプロセスではないと決定するステップは、プログラムのブラックリスト上において識別されたプロセスを特定するステップをさらに含む。マルウェア修正アクションを実行するステップは、検出されたファイル操作要求に関連付けられた書き込み操作を終了するステップと、検出されたファイル操作要求をメモリから削除することによって、検出されたファイル操作要求を終了するステップと、識別されたプロセスに関連付けられたディスクファイルイメージを隔離するステップとをさらに含む。

【００３０】

一実施形態において、プログラムのホワイトリスト上において識別されたプロセスを特定することに応答して、ミニフィルタドライバは、検出されたファイル操作要求を無視する。

【００３１】

一実施形態において、識別されたプロセスが信頼されたプロセスであるかどうかを決定するステップは、プログラムのブラックリストまたはプログラムのホワイトリスト上にお

いてプロセスを特定しないことに応答して、識別されたプロセスを許可することを求める要求をクライアントデバイスに送信するステップをさらに含む。

【００３２】

一実施形態において、識別されたプロセスが信頼されたプロセスではないと決定するステップは、識別されたプロセスを許可することを求める要求をクライアントデバイスに送信することに応答して、識別されたプロセスが許可されないというメッセージをクライアントデバイスから受信するステップをさらに含む。

【００３３】

一実施形態において、識別されたプロセスがプログラムのブラックリストに追加される。

【００３４】

一実施形態において、識別されたプロセスが許可されたというメッセージをクライアントデバイスから受信することに応答して、識別されたプロセスがプログラムのホワイトリストに追加される。

【００３５】

一実施形態において、非一時的コンピュータ可読媒体が命令を記憶し、命令は、少なくとも１つのプロセッサによって実行されたとき、ユーザモードにおいて実行されているプロセスによって開始されたファイル操作要求を検出することを少なくとも１つのプロセッサに行わせる。検出されたファイル操作要求に関連付けられたファイルバッファに関してマルウェア検出分析が行われて、マルウェアの存在を示す挙動を検出する。マルウェアの存在を示す挙動を検出することに応答して、検出されたファイル操作要求を開始することを担当するプロセスが識別される。プログラムのブラックリストおよびプログラムのホワイトリストのうちの１つまたは複数において、識別されたプロセスの検索が行われて、識別されたプロセスが信頼されたプロセスであるかどうかを決定する。識別されたプロセスが信頼されたプロセスではないと決定することに応答して、識別されたプロセスに対してマルウェア修正アクションが実行される。マルウェアを記述する情報がクライアントデバイスに送信される。

【００３６】

一実施形態において、ファイル操作要求を検出することを少なくとも１つのプロセッサに行わせる命令は、ファイル操作要求に対応するファイルハンドルから、ファイル操作要求が所定の動作に対応するかどうかを決定することを少なくとも１つのプロセッサに行わせる命令をさらに含む。ファイル操作要求が所定の動作に対応すると決定することに応答して、ファイル操作要求がインターセプトされる。

【００３７】

一実施形態において、ファイル操作要求をインターセプトすることを少なくとも１つのプロセッサに行わせる命令は、フィルタマネージャによって、ファイル操作要求をインターセプトするためにミニフィルタドライバが登録されているかどうかを決定することを少なくとも１つのプロセッサに行わせる命令をさらに含む。ファイル操作要求をインターセプトするためにミニフィルタドライバが登録されていると決定することに応答して、フィルタマネージャは、ファイル操作要求をミニフィルタドライバに送信する。

【００３８】

一実施形態において、マルウェア検出分析を行うことを少なくとも１つのプロセッサに行わせる命令は、モンテカルロ近似、エントロピ決定、系列係数分析、算術平均決定、カイ二乗決定、および標準偏差決定のうちの１つまたは複数を行って、ファイルバッファ内のデータが暗号化されているかどうかを決定することを少なくとも１つのプロセッサに行わせる命令をさらに含む。

【００３９】

一実施形態において、識別されたプロセスが信頼されたプロセスではないと決定することを少なくとも１つのプロセッサに行わせる命令は、プログラムのブラックリスト上において識別されたプロセスを特定することを少なくとも１つのプロセッサに行わせる命令を

さらに含む。マルウェア修正アクションを実行することを少なくとも１つのプロセッサに行わせる命令は、検出されたファイル操作要求に関連付けられた書き込み操作を終了することと、検出されたファイル操作要求をメモリから削除することによって、検出されたファイル操作要求を終了することと、識別されたプロセスに関連付けられたディスクファイルイメージを隔離することとを少なくとも１つのプロセッサに行わせる命令をさらに含む。

【００４０】

一実施形態において、非一時的コンピュータ可読媒体は、少なくとも１つのプロセッサによって実行されたとき、プログラムのホワイトリスト上において識別されたプロセスを特定することに応答して、ミニフィルタドライバによって、検出されたファイル操作要求を無視することを少なくとも１つのプロセッサに行わせる命令をさらに記憶する。

【００４１】

一実施形態において、識別されたプロセスが信頼されたプロセスであるかどうかを決定することを少なくとも１つのプロセッサに行わせる命令は、プログラムのブラックリストまたはプログラムのホワイトリスト上においてプロセスを特定しないことに応答して、識別されたプロセスを許可することを求める要求をクライアントデバイスに送信することを少なくとも１つのプロセッサに行わせる命令をさらに含む。

【００４２】

一実施形態において、識別されたプロセスが信頼されたプロセスではないと決定することを少なくとも１つのプロセッサに行わせる命令は、識別されたプロセスを許可することを求める要求をクライアントデバイスに送信することに応答して、識別されたプロセスが許可されないというメッセージをクライアントデバイスから受信することを少なくとも１つのプロセッサに行わせる命令をさらに含む。

【００４３】

一実施形態において、非一時的コンピュータ可読媒体は、少なくとも１つのプロセッサによって実行されたとき、識別されたプロセスをプログラムのブラックリストに追加することを少なくとも１つのプロセッサに行わせる命令をさらに記憶する。

【００４４】

一実施形態において、非一時的コンピュータ可読媒体は、少なくとも１つのプロセッサによって実行されたとき、識別されたプロセスが許可されたというメッセージをクライアントデバイスから受信することに応答して、識別されたプロセスをプログラムのホワイトリストに追加することを少なくとも１つのプロセッサに行わせる命令をさらに記憶する。

【００４５】

一実施形態において、カーネルモードにおけるステガノグラフィのリアルタイム検出およびステガノグラフィからの保護のための方法が、ファイアウォール、オペレーティングシステム、または電子メールシステムを介して、ファイルの送信を検出するステップを含む。ファイルのサイズが決定される。ファイルシステムからファイルの記憶されたファイルサイズが取り出される。ファイルの決定されたサイズは、ファイルの記憶されたファイルサイズと比較される。ファイルの決定されたサイズがファイルの記憶されたファイルサイズよりも大きいことに応答して、ファイルに関してステガノグラフィ検出分析が実行される。ステガノグラフィ検出分析がファイルにおけるステガノグラフィの存在を示すことに応答して、ステガノグラフィ修正アクションが実行され、ステガノグラフィを記述する情報がクライアントデバイスに送信される。

【００４６】

一実施形態において、ファイルのサイズを決定するステップは、ファイルのセクションヘッダに対するポインタを取得するステップを含み、セクションヘッダはファイルの複数のセクションに関連付けられている。ファイルの複数のセクションの各セクションについて、セクションのサイズが決定される。ファイルの複数のセクションの各セクションのサイズが合計されて、ファイルのサイズを決定する。

【００４７】

一実施形態において、ファイルのセクションヘッダに対するポインタを取得するステップは、ファイルのファイル名またはファイルのパスを使用してファイルを開くステップを含む。ファイルのヘッダが読み取られる。ヘッダからマジックナンバーが取り出される。マジックナンバーが検証されて、ファイルのセクションヘッダに対するポインタを取得する。

【００４８】

一実施形態において、ファイルに関してステガノグラフィ検出分析を実行するステップは、ファイルにおける付加されたペイロードを識別するステップを含む。付加されたペイロードは分析されて、付加されたペイロードのファイルフォーマットを決定する。付加されたペイロードのファイルフォーマットに基づいて、ステガノグラフィ検出分析が実行される。

【００４９】

一実施形態において、ファイルに関してステガノグラフィ検出分析を実行するステップは、ファイルにおける付加されたペイロードを識別するステップを含む。モンテカルロ近似、エントロピ決定、系列係数分析、算術平均決定、カイ二乗決定、および標準偏差決定のうちの１つまたは複数が行われて、付加されたペイロード内のデータが暗号化されているかどうかを決定する。

【００５０】

一実施形態において、ファイルに関してステガノグラフィ検出分析を実行するステップは、ファイルにおける付加されたペイロードを識別するステップと、付加されたペイロード内の許可されていないデータの存在を識別するステップとを含む。

【００５１】

一実施形態において、ファイルに関してステガノグラフィ検出分析を実行するステップは、ファイルにおける付加されたペイロードを識別するステップと、付加されたペイロード内のアセンブリレベル命令またはマシンレベル命令の存在を識別するステップとを含む。

【００５２】

一実施形態において、ステガノグラフィ修正アクションを実行するステップは、ファイルの処理および送信を終了するステップと、ファイルを隔離するステップとを含む。

【００５３】

一実施形態において、非一時的コンピュータ可読媒体が命令を含み、命令は、少なくとも１つのプロセッサによって実行されたとき、ファイアウォール、オペレーティングシステム、または電子メールシステムを介して、ファイルの送信を検出することを少なくとも１つのプロセッサに行わせる。ファイルのサイズが決定される。ファイルシステムからファイルの記憶されたファイルサイズが取り出される。ファイルの決定されたサイズは、ファイルの記憶されたファイルサイズと比較される。ファイルの決定されたサイズがファイルの記憶されたファイルサイズよりも大きいことに応答して、ファイルに関してステガノグラフィ検出分析が実行される。ステガノグラフィ検出分析がファイルにおけるステガノグラフィの存在を示すことに応答して、ステガノグラフィ修正アクションが実行され、ステガノグラフィを記述する情報がクライアントデバイスに送信される。

【００５４】

一実施形態において、ファイルのサイズを決定することを少なくとも１つのプロセッサに行わせる命令は、ファイルのセクションヘッダに対するポインタを取得することを少なくとも１つのプロセッサに行わせる命令を含み、セクションヘッダはファイルの複数のセクションに関連付けられている。ファイルの複数のセクションの各セクションについて、セクションのサイズが決定される。ファイルの複数のセクションの各セクションのサイズが合計されて、ファイルのサイズを決定する。

【００５５】

一実施形態において、ファイルのセクションヘッダに対するポインタを取得することを少なくとも１つのプロセッサに行わせる命令は、ファイルのファイル名またはファイルの

パスを使用してファイルを開くことを少なくとも１つのプロセッサに行わせる命令を含む。ファイルのヘッダが読み取られる。ヘッダからマジックナンバーが取り出される。マジックナンバーは検証されて、ファイルのセクションヘッダに対するポインタを取得する。

【００５６】

一実施形態において、ファイルに関してステガノグラフィ検出分析を実行することを少なくとも１つのプロセッサに行わせる命令は、ファイルにおける付加されたペイロードを識別することを少なくとも１つのプロセッサに行わせる命令を含む。付加されたペイロードは分析されて、付加されたペイロードのファイルフォーマットを決定する。付加されたペイロードのファイルフォーマットに基づいて、ステガノグラフィ検出分析が実行される。

【００５７】

一実施形態において、ファイルに関してステガノグラフィ検出分析を実行することを少なくとも１つのプロセッサに行わせる命令は、ファイルにおける付加されたペイロードを識別することを少なくとも１つのプロセッサに行わせる命令を含む。モンテカルロ近似、エントロピ決定、系列係数分析、算術平均決定、カイ二乗決定、および標準偏差決定のうちの１つまたは複数が行われて、付加されたペイロード内のデータが暗号化されているかどうかを決定する。

【００５８】

一実施形態において、ファイルに関してステガノグラフィ検出分析を実行することを少なくとも１つのプロセッサに行わせる命令は、ファイルにおける付加されたペイロードを識別することと、付加されたペイロード内の許可されていないデータの存在を識別することとを少なくとも１つのプロセッサに行わせる命令を含む。

【００５９】

一実施形態において、ファイルに関してステガノグラフィ検出分析を実行することを少なくとも１つのプロセッサに行わせる命令は、ファイルにおける付加されたペイロードを識別することと、付加されたペイロード内のアセンブリレベル命令またはマシンレベル命令の存在を識別することとを少なくとも１つのプロセッサに行わせる命令を含む。

【００６０】

一実施形態において、ステガノグラフィ修正アクションを実行することを少なくとも１つのプロセッサに行わせる命令は、ファイルの処理および送信を終了することと、ファイルを隔離することとを少なくとも１つのプロセッサに行わせる命令を含む。

【００６１】

一実施形態において、コンピュータシステムが少なくとも１つのコンピュータプロセッサを備える。非一時的コンピュータ可読媒体が命令を記憶し、命令は、少なくとも１つのコンピュータプロセッサによって実行されたとき、ファイアウォール、オペレーティングシステム、または電子メールシステムを介して、ファイルの送信を検出することを少なくとも１つのプロセッサに行わせる。ファイルのサイズが決定される。ファイルシステムからファイルの記憶されたファイルサイズが決定される。ファイルの決定されたサイズは、ファイルの記憶されたファイルサイズと比較される。ファイルの決定されたサイズがファイルの記憶されたファイルサイズよりも大きいことに応答して、ファイルに関してステガノグラフィ検出分析が実行される。ステガノグラフィ検出分析がファイルにおけるステガノグラフィの存在を示すことに応答して、ステガノグラフィ修正アクションが実行される。ステガノグラフィを記述する情報がクライアントデバイスに送信される。

【００６２】

一実施形態において、ファイルのサイズを決定することを少なくとも１つのコンピュータプロセッサに行わせる命令は、ファイルのセクションヘッダに対するポインタを取得することを少なくとも１つのコンピュータプロセッサに行わせる命令を含み、セクションヘッダはファイルの複数のセクションに関連付けられている。ファイルの複数のセクションの各セクションについて、セクションのサイズが決定される。ファイルの複数のセクションの各セクションのサイズが合計されて、ファイルのサイズを決定する。

【００６３】
一実施形態において、ファイルのセクションヘッダに対するポインタを取得することを少なくとも１つのコンピュータプロセッサに行わせる命令は、ファイルのファイル名またはファイルのパスを使用してファイルを開くことを少なくとも１つのコンピュータプロセッサに行わせる命令を含む。ファイルのヘッダが読み取られる。ヘッダからマジックナンバーが取り出される。マジックナンバーは検証されて、ファイルのセクションヘッダに対するポインタを取得する。
【００６４】
一実施形態において、ファイルに関してステガノグラフィ検出分析を実行することを少なくとも１つのコンピュータプロセッサに行わせる命令は、ファイルにおける付加されたペイロードを識別することを少なくとも１つのコンピュータプロセッサに行わせる命令を含む。付加されたペイロードは分析されて、付加されたペイロードのファイルフォーマットを決定する。付加されたペイロードのファイルフォーマットに基づいて、ステガノグラフィ検出分析が実行される。
【００６５】
カーネルモードにおけるマルウェアおよびステガノグラフのリアルタイム検出ならびにマルウェアおよびステガノグラフからの保護
図１は、実施形態に従う、カーネルモードにおけるマルウェアおよびステガノグラフィのリアルタイム検出ならびにマルウェアおよびステガノグラフィからの保護のためのシステムの例示的なブロック図を示す。システムは、管理ノード１００、クラウドホスト１０５、およびセキュリティマネージャ１１５を含む。他の実施形態において、システムは、本明細書に説明されるものよりも、追加のまたは少ないコンポーネントを備える。同様に、機能は、ここで説明されるのと異なる方式でコンポーネントおよび／または異なるエンティティの間で分散されることが可能である。
【００６６】
管理ノード１００は、カーネルモードにおいてマルウェアおよびステガノグラフィから保護されるコンピュータシステムである。管理ノード１００は、（たとえば、Ｗｉｎｄｏｗｓ、ＭａｃＯＳ、もしくは別のオペレーティングシステムを実行している）コンピュータ、データセンタ、メインフレーム、またはストレージおよび計算能力を有する他の任意のデバイスであってよい。一実施形態において、管理ノード１００は、Ｉ／Ｏマネージャ１２０、Ｗｉｎｄｏｗｓサービスマネージャ１７０、レジストリ１７５、静的分析モジュール１８０、ストレージデバイス１５５、カーネル１６５、およびハードウェア抽象化層１６０を含む。他の実施形態において、管理ノード１００は、本明細書に説明されるものよりも、追加のまたは少ないコンポーネントを備える。同様に、機能は、ここで説明されるのと異なる方式でコンポーネントおよび／または異なるエンティティの間で分散されることが可能である。
【００６７】
一実施形態において、管理ノード１００はＷｉｎｄｏｗｓコンピュータである。カーネルドライバ１３０は、Ｉ／Ｏマネージャ１２０内のフィルタマネージャ１２５に動的にインストールされてよい。この実施形態は、Ｗｉｎｄｏｗｓプラットフォーム上でファイルシステムイベントをインターセプトするための高性能メカニズムを提供する。他の実施形態において、管理ノード１００は、特定のデバイスの検出システム能力を利用する。たとえば、この例におけるストレージデバイス１５５は、ＮＴＦＳファイルシステム、ＦＡＴ１６、またはＦＡＴ３２用にフォーマットされたボリュームであってよい。
【００６８】
管理ノード１００は、外界との間で入力および出力（Ｉ／Ｏ）を提供する１つまたは複数のデバイスを含んでよい。そのようなデバイスは、キーボード、マウス、オーディオコントローラ、ビデオコントローラ、ディスクドライブ、およびネットワークポートなどを含んでよい。一実施形態において、デバイスドライバが、そのようなデバイスと管理ノード１００上のオペレーティングシステムとの間のソフトウェア接続を提供してよい。カー

ネルモードＩ／Ｏマネージャ１２０は、アプリケーションとデバイスドライバによって提供されるインターフェースとの間の通信を管理する。デバイスはオペレーティングシステムと一致しなくてよい速度で動作することがあるため、オペレーティングシステムとデバイスドライバとの間の通信は、主にＩ／Ｏ要求パケットを通じて行われる。これらのパケットは、ネットワークパケットまたはＷｉｎｄｏｗｓメッセージパケットと同様であってよい。それらは、オペレーティングシステムから特定のドライバへ渡され、また１つのドライバから別のドライバへ渡される。

【００６９】

一実施形態において、Ｉ／Ｏマネージャ１２０は、管理ノード１００によって受信されたファイル操作要求（たとえば、読み取り、書き込み、ファイルオープンなど）を検出する。フィルタマネージャ１２５は、ファイル操作要求に対応するファイルハンドルから、ファイル操作要求が所定の動作に対応するかどうかを決定してよい。ファイルハンドルは、ファイルが開かれるときにオペレーティングシステムが一時的にファイルに割り当てる番号または識別子である。オペレーティングシステムは、ファイルをアクセスするときに内部でファイルハンドルを使用する。フィルタマネージャ１２５が、ファイル操作要求が所定の動作に対応すると決定した場合、フィルタマネージャ１２５は、マルウェア検出のためにファイル操作要求をインターセプトする。マルウェアの存在を示す挙動が見つけられた場合、Ｉ／Ｏマネージャ１２０は、検出されたファイル操作要求の開始を担当するユーザモードプロセスを識別してよい。

【００７０】

一実施形態において、フィルタマネージャ１２５は、Ｗｉｎｄｏｗｓと共にインストールされる。それは、ミニフィルタドライバがロードされたときのみにアクティブにされる。ミニフィルタドライバは、ファイルシステム操作をフィルタリングするドライバを指す。ミニフィルタドライバは、Ｉ／Ｏマネージャ１２０とベースファイルシステムとの間に配置されてよい。フィルタマネージャ１２５は、ターゲットボリュームに関するファイルシステムスタックにアタッチしてよい。ミニフィルタドライバは、ミニフィルタドライバがフィルタリングすることを選択したＩ／Ｏ操作に関してフィルタマネージャ１２５に登録することによってファイルシステムスタックに間接的にアタッチしてよい。

一実施形態において、ファイル操作要求をインターセプトするために、フィルタマネージャ１２５は、ファイル操作要求をインターセプトするためにミニフィルタドライバが登録されているかどうかを決定する。ファイル操作要求をインターセプトするためにミニフィルタドライバが登録されていると決定することに応答して、フィルタマネージャ１２５は、ファイル操作要求をミニフィルタドライバにて送信する。ファイル操作要求の生成を担当するユーザプロセッサがＩ／Ｏマネージャ１２０によって識別されていると、フィルタマネージャ１２５は、プログラムのブラックリストおよびプログラムのホワイトリストのうちの１つまたは複数において、識別されたプロセスの検索を行って、識別されたプロセスが信頼されたプロセスであるかどうかを決定してよい。

【００７１】

カーネルドライバ１３０は、Ｉ／Ｏ、プラグアンドプレイメモリ、プロセスおよびスレッド、ならびにセキュリティなどを管理するカーネルモードオペレーティングシステムコンポーネントの一部としてカーネルモードにおいて実行される。オペレーティングシステムそれ自体と同様に、カーネルドライバ１３０は、必要とされる機能性の明確に定義されたセットを有する個別のモジュールコンポーネントとして実装されてよい。カーネルドライバ１３０は、システム定義された標準ドライバルーチンのセットを供給してもよい。カーネルドライバ１３０は、実行の前および後にＩ／Ｏ要求パケットをインターセプトしてよい。Ｉ／Ｏ要求パケットは、ドライバによって互いおよびオペレーティングシステムと通信するために使用されるカーネルモード構造である。（図３に関して示され以下に説明される）ミニフィルタカーネルドライバは、ファイル操作のためのルーチンをサポートする。したがって、カーネルドライバ１３０は、ファイルオープン、読み取り、書き込み、クローズ、および他の操作を受け取りおよび処理するための高性能メカニズムである。一

実施形態において、カーネルドライバ１３０は、カーネルモード読み取りおよび書き込みバッファにアクセスして、プロセスが要求しているデータに対する迅速な統計分析を行う。

【００７２】

Ｗｉｎｄｏｗｓサービスマネージャ１７０は、Ｗｉｎｄｏｗｓサービスに関係付けられた共通のタスクを単純化するために使用されてよい。Ｗｉｎｄｏｗｓサービスは、管理ノード１００上でバックグラウンドにおいて動作する（デーモンに類似する）コンピュータプログラムである。Ｗｉｎｄｏｗｓサービスは、オペレーティングシステムが開始されバックグラウンドにおいて実行されるときに開始するように構成されてよく、それは、手動でまたはイベントによって開始されてよい。Ｗｉｎｄｏｗｓサービスマネージャ１７０は、Ｗｉｎｄｏｗｓを再起動することなくサービス（Ｗｉｎ３２とレガシドライバの両方）を作成し、既存のサービスを削除し、サービス構成を変更することができる。Ｗｉｎｄｏｗｓサービスマネージャ１７０は、ＧＵＩとコマンドラインモードの両方を有してよい。

【００７３】

レジストリ１７５は、オペレーティングシステムとレジストリ１７５を使用するアプリケーションとに関する低レベル設定を記憶する階層データストアである。カーネル１６５、デバイスドライバ、サービス、およびユーザインターフェースはすべて、レジストリ１７５を使用することができる。したがって、レジストリ１７５は、プログラムおよびハードウェア抽象化層１６０に関する情報、設定、オプション、および他の値を含む。プログラムがインストールされたとき、プログラムの場所、そのバージョン、およびプログラムの開始の仕方などの設定を含む新しいサブキーがすべてレジストリ１７５に追加される。レジストリ１７５は、マルウェアによってリブート後にそれらの実行をスケジューリングするために使用されるキーを含む可能性がある。

【００７４】

一実施形態において、静的分析モジュール１８０は、プログラムおよびカーネルモードドライバコードにおけるコーディングエラーを検出するコンパイル時静的検証ツールであってよい。Ｗｉｎｄｏｗｓサービスは、カーネルドライバ１３０の状態を監視してよく、レジストリキーおよび値を定期的に検証すること、隠されたプロセスを検索すること、およびシステム全体の静的スキャンを行うことなどのプロアクティブなマルウェア対策タスクを行ってよい。静的分析モジュール１８０は、すべてのファイルに関して分析を行うシステム全体のスキャンを管理してよい。これは、暗号化を検出すること、ステガノグラフィを識別すること、コンピュータ「ロックアウト」から保護すること、および改ざんのエビデンスに関するマスタファイルテーブル（ＮＴＦＳ　ＭＦＴ）およびマスタブートレコード（ＭＢＲ）の状態を監視することを含むが、これらに限定されない。また、静的分析モジュール１８０は、Ｗｉｎｄｏｗｓ　ＡＰＩを使用して、許可されていないプロセスから（図４に関して示され以下に説明される）ボリュームシャドウコピーサービス（ＶＳＳ）が無効にされているかどうかを決定してよい。実施形態において、未知のプロセスがＶＳＳを改ざんしている場合、静的分析モジュール１８０は、未知のプロセスがマルウェアであると検出してよい。そして、静的分析モジュール１８０は、管理ツールを介して誤検出を回避するために未知のプロセスがシステムプロセスであるかどうかを決定してよい。

【００７５】

ストレージデバイス１５５は、管理ノード１００上のデータおよびアプリケーションを記憶する管理ノード１００のコンポーネントである。ストレージデバイス１５５は、ＲＡＭ、キャッシュ、およびハードディスク、ならびに場合によっては光ディスクドライブおよび外部接続されたＵＳＢドライブを含んでよい。ストレージデバイス１５５は、データがどのように記憶され取り出されるかを制御するファイルシステムのためにフォーマットされる。ファイルシステムは、ＮＴＦＳファイルシステム、ＦＡＴ１６、ＦＡＴ３２などのいずれも含んでよい。ＮＴＦＳファイルシステムは、Ｗｉｎｄｏｗｓ　ＮＴファミリのファイルシステムである。ファイルアロケーションテーブル（ＦＡＴ）は、コンピュータファイルシステムアーキテクチャであり、業界標準ファイルシステムのファミリである。

ＦＡＴのファイルシステム変形例は、ＦＡＴ１６およびＦＡＴ３２である。

【００７６】

カーネル１６５は、管理ノード１００に対する制御を有する、管理ノード１００のオペレーティングシステムのコアであるコンピュータプログラムである。カーネル１６５は通常、起動時に（たとえば、ブートローダの後に）ロードされる。カーネル１６５は、起動の残り部分およびソフトウェアからの入出力要求を処理して、それらを管理ノード１００のプロセッサのためのデータ処理命令に変換する。カーネル１６５はまた、メモリ、ならびにキーボード、モニタ、プリンタ、およびスピーカなどの周辺機器を取り扱う。

【００７７】

ハードウェア抽象化層１６０は、管理ノード１００のオペレーティングシステムが、詳細なハードウェアレベルでなくより一般的または抽象的レベルでハードウェアデバイス（たとえば、図３を参照して以下に説明されるプロセッサ３１０）と対話することを可能にする、プログラミングの層である。ハードウェア抽象化は、プラットフォーム固有の詳細をエミュレートするソフトウェアルーチンであり、ハードウェアリソースに対する直接アクセスをプログラムに与える。ハードウェア抽象化層１６０を使用して、デバイス非依存の高性能アプリケーションが、ハードウェアに標準オペレーティングシステムコールを発行してよい。たとえば、Ｗｉｎｄｏｗｓ２０００は、ハードウェア抽象化層を含むいくつかのオペレーティングシステムのうちの１つである。

【００７８】

クラウドホスト１０５は、物理ウェブサーバの広範な基礎のネットワークからコンピューティングリソースを引き出す仮想サーバ上のホスティングを提供する。一実施形態において、クラウドホスト１０５は、クラウドベンダから仮想ハードウェア、ネットワーク、ストレージ、および複合ソリューションを使用してよい。クラウドホスティングは仮想化を通じて有効にされてよく、それにより、インフラストラクチャまたはデータセンタのコンピューティング容量全体が複数のユーザまたは管理ノードへ同時に分散され提供される。たとえば、物理サーバが仮想化および統合されて、いくつかのクラウドサーバをホストし、すべてがプロセッサ、メモリ、ストレージ、ネットワーク、および他のリソースを共有してよい。クラウドホスト１０５は、操作データに関して、ナイーブベイズ分類、線形回帰、ロジスティック回帰、およびビジネスインテリジェンス分析などの機械学習アルゴリズムを実行してよい。この情報は、マルウェア攻撃の範囲、感染されたデバイスを特定し、伝播を予測および防止するめに使用されることが可能である。

【００７９】

セキュリティマネージャ１１５は、管理ノード１００の企業規模のビューおよびそのポリシを提供する。それは、デバイス、仮想マシン、およびコンテナを作成、管理、配置、および監視するために使用される。セキュリティマネージャ１１５は、オンプレミス分析を行ってもよい。一実施形態において、特定のファイル操作要求の開始を担当する識別されたプロセスは、信頼されたプロセスではないと決定されてよい。セキュリティマネージャ１１５は、識別されたプロセスに対してマルウェア修復アクションを実行するために、管理ノード１００にてメッセージを送信してよい。管理ノード１００は、マルウェアを記述する情報をクライアントデバイスに送信してもよい。

【００８０】

クライアントデバイスは、デジタルコンテンツを消費すること、ソフトウェアアプリケーションを実行すること、ネットワーク１１０上で管理ノード１００にホストされまたは他の形式でそれと相互作用するウェブサイトを閲覧すること、およびファイルをダウンロードすることなどの機能を実行するために、ユーザによって使用される電子デバイスである。たとえば、クライアントデバイスは、スマートフォンもしくはタブレット、ノートブック、またはデスクトップコンピュータであってよい。さらに、クライアントデバイスは、家庭用電気製品のようなモノのインターネットに接続されたデバイス、またはさらに別のウェブサーバであってよい。クライアントデバイスは、表示デバイスを含んでよく、ユーザは、クライアントデバイスに記憶されまたは管理ノード１００からダウンロードされ

たデジタルコンテンツを、表示デバイスで見てよい。さらに、クライアントデバイスは、物理的および／または画面上ボタンなどのユーザインターフェース（ＵＩ）を含んでよく、ユーザは、ユーザインターフェースを用いて対話して、デジタルコンテンツを消費すること、デジタルコンテンツを取得すること、およびデジタルコンテンツを送信することなどの機能を実行してよい。

【００８１】

一実施形態において、セキュリティマネージャ１１５は、マルウェア修正アクションを実行するために、信号またはメッセージを管理ノード１００に送信してよい。マルウェア修正アクションは、検出されたファイル操作要求に関連付けられた書き込み操作を終了することを含んでよい。マルウェア修正アクションは、検出されたファイル操作要求をメモリから削除することによって、検出されたファイル操作要求を終了することを含んでよい。マルウェア修正アクションは、識別されたプロセスに関連付けられたディスクファイルイメージを隔離することを含んでよい。ディスクファイルイメージは、ディスク全体のすべてのコンテンツおよび構造を記憶するファイルである。ディスクは、光ディスク、ハードディスクドライブなどであってよい。ディスクファイルイメージは、ディスクボリュームまたは物理ディスクドライブ全体の正確なコピーであってよい。ディスクファイルイメージは、そのソースのすべてのプロパティ、すなわち、ファイル、フォルダ、プロパティ、ディスク名などを保持してよい。

【００８２】

一実施形態において、セキュリティマネージャ１１５は、ステガノグラフィ修正アクションを実行するために、信号またはメッセージを管理ノード１００に送信してよい。ステガノグラフィ修正アクションは、ファイアウォールを通過しようとしているファイルの処理および送信を終了することを含んでよい。ステガノグラフィ修正アクションは、ファイルを隔離することを含んでよい。

【００８３】

ファイアウォール１３５は、セキュリティルールに基づいて着信および発信のネットワークトラフィックを監視および制御するネットワークセキュリティシステムである。ファイアウォール１３５は、信頼された内部管理ノード１００と信頼されていない外部ネットワーク１１０との間のバリアを確立する。ファイアウォール１３５は、ネットワークファイアウォールまたはホストベースのファイアウォールであってよい。ファイアウォール１３５がホストベースのファイアウォールである場合、それは、管理ノード１００の内外へのネットワークトラックを制御するために、管理ノード１００内に配置されてよく、または管理ノード１００上で実行されてよい。

【００８４】

マルウェア分析モジュール１４０は、管理ノード１００に対する着信ファイルに関して、または検出されたファイル操作に関連付けられたファイルに関してマルウェア検出分析を行う。マルウェア分析モジュール１４０は、管理ノード１００内に配置されてよく、または管理ノード１００上で実行されてよい。一実施形態において、マルウェア分析モジュール１４０は、検出されたファイル操作要求に関連付けられたファイルバッファに関してマルウェア検出分析を行って、マルウェアの存在を示す挙動を検出してよい。同様に、マルウェア分析機能は、管理ノード１００の他のエンティティの間で分散されることが可能である。

【００８５】

一実施形態において、マルウェア分析モジュール１４０は、カーネルモードにおいてステガノグラフィのリアルタイム検出およびステガノグラフィからの保護を行ってよい。ファイアウォール、オペレーティングシステム、または電子メールシステムを介するファイルの送信が検出されると、マルウェア分析モジュール１４０は、ファイルのサイズを決定してよい。ファイルのサイズは、ファイルが含むデータの大きさ、あるいはそれが消費するストレージの大きさの尺度である。ファイルのサイズは通常、バイトに基づく測定の単位で表される。

【００８６】
一実施形態において、マルウェア分析モジュール１４０は、ファイルのセクションヘッダに対するポインタを取得することによってファイルのサイズを決定してよい。セクションヘッダは、ファイルの複数のセクションに関連付けられている。ファイルの複数のセクションの各セクションｉについて、マルウェア分析モジュール１４０は、セクションｉのサイズs_iを決定してよい。マルウェア分析モジュール１４０は、ファイルの複数のセクションの各セクションｉのサイズs_iを合計して、ファイルのサイズを$\Sigma_i s_i$として決定してよい。
【００８７】
一実施形態において、マルウェア分析モジュール１４０は、ファイルのファイル名またはファイルのパスを使用してファイルを開くことによって、ファイルのセクションヘッダに対するポインタを取得してよい。ファイルのファイル名は、ファイルを一意に識別するために使用される名前である。ファイルシステムは、ファイル名長さ、およびファイル名内の許可される文字に制限を課すことがある。ファイル名は、ホスト名、デバイス名、ディレクトリ（またはパス）、ファイルの基底名、種類（フォーマットまたは拡張子）、およびファイルのバージョンのうちの１つまたは複数を含んでよい。
【００８８】
マルウェア分析モジュール１４０は、ファイルのヘッダを読み取る。ファイルのヘッダは、通常、ファイルの先頭に記憶されるメタデータを含んでよい。メタデータは、ファイルフォーマットまたは含まれるデータの種類に応じて、他の領域、たとえばファイルの最後などに存在してもよい。ファイルのヘッダは、文字ベース（テキスト）、バイナリヘッダなどであってよい。ファイルのヘッダは、ファイルフォーマットを識別するとともに、（画像ファイルに関して）画像フォーマット、サイズ、解像度、および色空間などに関する情報を記憶してよい。
【００８９】
マルウェア分析モジュール１４０は、ヘッダからマジックナンバーを取り出してよい。マジックナンバーは、ファイルフォーマットまたはプロトコルを識別するために使用される数値またはテキスト値であってよい。たとえば、マジックナンバーは、ファイルのフォーマットを識別するために使用されるファイル内のバイトであってよい。通常、マジックナンバーは、ファイルの始まりに置かれた短いシーケンスのバイト（たとえば４バイト長）である。たとえば、ポータブル実行可能（ＰＥ）ファイルに関しては、１６進数の署名が「４Ｄ　５Ａ」であってよく、マジックナンバーは「ＭＺ」であってよい。マルウェア分析モジュール１４０は、マジックナンバーを検証して、ファイルのセクションヘッダに対するポインタを取得してよい。
【００９０】
ファイルシステムは、ファイルのファイルサイズであってよい。たとえば、ファイルシステムは、ファイルに関連付けられているストレージの大きさを示すファイルのバイト数を記憶してよい。記憶されたファイルサイズは、システム限界までの非負の整数バイトであってよい。別の例において、記憶されたファイルサイズは、物理ストレージデバイス上でファイルによって占有されたブロックまたはトラックの数であってよい。この例においては、ソフトウェアが正確なバイト数を追跡するために使用されてよい。マルウェア分析モジュール１４０は、管理ノード１００のファイルシステムからファイルの記憶されたファイルサイズを取り出してよい。ファイルシステムがサポートする最大ファイルサイズは、ファイルシステムの容量だけでなく、ファイルサイズ情報の記憶用に予約されたビットの数にも依存してよい。ＦＡＴ３２ファイルシステムにおける最大ファイルサイズは、たとえば、４ギガバイトよりも１バイト少ない４，２９４，９６７，２９５バイトである。
【００９１】
マルウェア分析モジュール１４０は、ファイルの決定されたサイズをファイルの記憶されたファイルサイズと比較してよい。ファイルの決定されたサイズがファイルの記憶されたファイルサイズよりも大きいことに応答して、マルウェア分析モジュール１４０は、フ

ァイルに関してステガノグラフィ検出分析を実行してよい。一実施形態において、マルウェア分析モジュール１４０は、ファイルにおける付加されたペイロードを識別することによって、ステガノグラフィ検出分析を実行してよい。付加されたペイロードは、マルウェアの実際の悪意ある目的を実行する本体またはデータである。（識別され除去されない場合に）ペイロードは、速度低下もしくはフリーズ、スパムの送信、データの暗号化、ディスク上のファイルの削除、システムのクラッシュ、またはファイルの破損などを管理ノード１００に行わせることがある。マルウェア分析モジュール１４０は、付加されたペイロードを分析して、付加されたペイロードのファイルフォーマットを決定してよい。付加されたペイロードのファイルフォーマットは、付加されたペイロードに情報が記憶（符号化）される方法の構造である。たとえば、付加されたペイロードは、画像もしくはラスタデータ用のＪＰＥＧもしくはＴＩＦＦ、ベクタデータ用のＡＩ（Ａｄｏｂｅ　Ｉｌｌｕｓｔｒａｔｏｒ）、または文書交換用のＰＤＦであってよい。マルウェア分析モジュール１４０は、付加されたペイロードのファイルフォーマットに基づいて、ステガノグラフィ検出分析を実行してよい。

【００９２】

一実施形態において、マルウェア分析モジュール１４０は、モンテカルロ近似、エントロピ決定、系列係数分析、算術平均決定、カイ二乗決定、および標準偏差決定のうちの１つまたは複数を行って、付加されたペイロード内のデータが暗号化されているかどうかを決定してよい。モンテカルロ近似の実行が、図５に関して示され以下に説明される。

【００９３】

一実施形態において、マルウェア分析モジュール１４０は、エントロピ決定を行って、付加されたペイロード内のデータが暗号化されているかどうかを決定してよい。エントロピは、

【００９４】

【数１】

$$H = -\sum_{i=0}^{255} P_i \log_2(P_i)$$

【００９５】

として、値の確率分布の負の対数を取って付加されたペイロードのエントロピを計算することによって、付加されたペイロードにおける情報コンテンツの量を測定する。

【００９６】

上記のエントロピ決定において、Ｈは、総エントロピであり、P_iは、付加されたペイロードから読み取られたバイトの値である。暗号化および難読化されたファイルは通常、プレーンテキストまたは構造化データファイルよりもはるかに高いエントロピを有する。エントロピＨは、エントロピ閾値と比較されてよい。閾値より上のエントロピは、付加されたペイロードが暗号化または圧縮されている可能性が高いことを示し、したがって、それはランサムウェアに影響されたおそれがある。マルウェア分析モジュール１４０は、セクション（バッファ）または付加されたペイロード全体に関してエントロピ計算を行って、付加されたペイロード内に隠された（「パックされた」）マルウェアの隠されたまたは暗号化されたコピーを検出してよい。

【００９７】

一実施形態において、マルウェア分析モジュール１４０は、系列係数分析を行って、付加されたペイロード内のデータが暗号化されているかどうかを決定してよい。系列係数分析は、特定の時間の期間にわたる同じ変数の観測値間の関係、この場合は、追加されたペイロードにおける各バイトの変化する値を記述する。系列係数分析は、付加されたペイロードにおけるバイトの値が相関されているかどうかを決定する。相関がない場合、それは、追加されたペイロードにおける後のバイトの値が前の値によって予測できないことを意味する。系列相関値が低いほど、強力な暗号化の確率が高い。変数の系列相関がゼロとし

て測定される場合、それは、相関が存在せず、観測値の各々が互いに独立していることを意味する。逆に、変数の系列相関が１に向かって傾斜する場合、それは、観測値が系列相関され、将来の観測値が過去の値によって影響されることを意味する。

【００９８】

一実施形態において、マルウェア分析モジュール１４０は、カイ二乗決定を行って、付加されたペイロード内のデータが暗号化されているかどうかを決定してよい。カイ二乗決定は、暗号化されたファイルから圧縮されたファイルを区別するために使用されてよい。カイ二乗決定は、観測されたデータを期待されたデータと比較するために一般的に使用される単純な統計的検定である。カイ二乗検定は、観測された分布が偶然による可能性を検定することが意図されている。それは、「適合度」統計とも呼ばれ、なぜならば、それは変数が独立である場合に観測された分布が期待された分布にいかに良く適合するかを測定するからである。圧縮されたペイロードは、高いエントロピおよび大きいカイ二乗値を有することになる。バイトの完全にランダムなペイロードの期待された値は、平均１２７．５（２５５／２）になるであろう。これは、暗号化されたファイル、圧縮されたファイル、および暗号化された圧縮されたファイルの決定を可能にする。カイ二乗値を計算するための公式は、

【００９９】

【数２】

$$\chi^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i}$$

【０１００】

である。

【０１０１】

一実施形態において、マルウェア分析モジュール１４０は、算術平均決定および標準偏差決定のうちの１つまたは複数を行って、付加されたペイロード内のデータが暗号化されているかどうかを決定する。付加されたペイロードが暗号化されている場合、付加されたペイロードのデータ値の算術平均は、およそ１２７．５（２５５／２）に等しいはずである。標準偏差σは、データ値の変動または分散の量を定量化するために使用される尺度である。算術平均および標準偏差は、付加されたペイロードの部分、および付加されたペイロード全体について計算される。マルウェア分析モジュール１４０は、オペレーティングシステムの内部Ｉ／Ｏバッファを直接読み取ってよいので、読み取りおよび書き込みオーバヘッドが低減される。これは、より多数の統計的決定が計算および分析されるのを可能にして、より少ないシステムリソースを使用して、より正確でより速い決定という結果となる。統計的決定は、データがアウトオブオーダで提供されても部分的および全体的値を提供することができる。そのようなアウトオブオーダ決定は、高性能、マルチスレッド、およびマルチプロセスの実施形態を可能にする。

【０１０２】

一実施形態において、マルウェア分析モジュール１４０は、付加されたペイロード内の許可されていないデータの存在を識別することによって、ステガノグラフィ検出分析を実行してよい。たとえば、マルウェア分析モジュール１４０は、許可されていないルートキットインストールまたはデータ暗号化を検出してよい。データに対する許可されていない変更の検出が、図４に関して以下に詳細に説明される。一実施形態において、マルウェア分析モジュール１４０は、許可されていないシステムが機密情報を収集しているディスク上での命令を識別してよい（アウトバウンド実施形態）。したがって、データの許可されていない送信は防止されることが可能である。一実施形態において、静的分析が、プログラムの実行なしにファイルの分析でマルウェアからの保護をするために使用される。インバウンド実施形態において、企業環境に入って来る許可されていないコード、たとえば、インターネットからダウンロードされたｍｐ３内に隠された悪意のあるコードのシーケン

スが、検出されてよい。
【０１０３】
一実施形態において、マルウェア分析モジュール１４０は、付加されたペイロード内のアセンブリレベル命令またはマシンレベル命令の存在を識別することによって、ステガノグラフィ検出分析を実行してよい。アセンブリレベル命令は、低水準プログラム言語を指し、これは、言語とアーキテクチャのマシンレベル命令との間に強い対応関係（ただし、しばしば一対一ではない）がある。マルウェア分析モジュール１４０は、疑わしい命令セット、たとえば、マシンまたはアセンブリレベル言語のインジケーションを識別する。実施形態において、方法は、部分的にファイルを逆アセンブルし、そのような疑わしい命令セットを探す。
【０１０４】
ステガノグラフィ検出分析がファイルにおけるステガノグラフィの存在を示すことに応答して、マルウェア分析モジュール１４０は、信号を管理ノード１００に送信してステガノグラフィ修正アクションを実行してよい。マルウェア分析モジュール１４０は、ステガノグラフィを記述する情報をクライアントデバイスに送信してよい。
【０１０５】
ルータ１４５は、管理ノード１００とネットワーク１１０との間でデータパケットを転送するネットワーキングデバイスである。ルータ１４５は、トラフィック検出機能を実行してもよい。ネットワーク１１０からデータパケットが入って来ると、ルータ１４５は、パケットにおけるネットワークアドレス情報を読み取って、最終的宛先を決定する。スイッチ１５０は、データの受信、処理、および宛先デバイスに対する転送のために、パケット交換を使用することによってネットワーク上でデバイス同士を接続するコンピュータネットワーキングデバイスである。一実施形態において、スイッチ１５０は、ＯＳＩモデルのデータリンク層（レイヤ２）でデータを処理および転送するためにハードウェアアドレスを使用するマルチポートネットワークブリッジである。
【０１０６】
ネットワーク１１０は、クライアントデバイスおよび管理ノード１００の間の通信を可能にする。この目的のために、ネットワーク１１０は、要求および対応するデータ（たとえば、ウェブページ上にポストされるべきファイルのコンテンツ）をクライアントデバイスから受信し、要求を管理ノード１００に転送する。同様に、ネットワーク１１０は、管理ノード１００から応答を受信し、応答をクライアントデバイスに転送する。
【０１０７】
ネットワーク１１０は、インターネットおよび携帯電話ネットワークを含むことができる。一実施形態において、ネットワーク１１０は、標準的な通信技術および／またはプロトコルを使用する。したがって、ネットワーク１１０は、イーサネット、８０２．１１、ロングタームエボリューション（ＬＴＥ）などの技術を使用するリンクを含むことができる。ネットワーク１１０上で使用されるネットワーキングプロトコルは、マルチプロトコルラベルスイッチング（ＭＰＬＳ）、伝送制御プロトコル／インターネットプロトコル（ＴＣＰ／ＩＰ）、ユーザデータグラムプロトコル（ＵＤＰ）、ＨＴＴＰ、簡易メール転送プロトコル（ＳＭＴＰ）、ファイル転送プロトコル（ＦＴＰ）などを含むことができる。ネットワーク１１０上で交換されるデータは、ハイパーテキストマークアップ言語（ＨＴＭＬ）、拡張マークアップ言語（ＸＭＬ）などを含む技術および／またはフォーマットを使用して表されることが可能である。また、リンクの全部または一部は、セキュアソケットレイヤ（ＳＳＬ）、トランスポート層セキュリティ（ＴＬＳ）、仮想プライベートネットワーク（ＶＰＮ）、インターネットプロトコルセキュリティ（ＩＰｓｅｃ）などの従来の暗号化技術を使用して暗号化されることが可能である。別の実施形態において、エンティティは、上記に説明されたものに代えてまたは加えて、カスタムおよび／または専用データ通信技術を使用することができる。
【０１０８】
プラットフォーム上のユーザモードおよびカーネルモードにおいて実行されているアプリ

ケーションに関するマルウェアの検出
図２は、実施形態に従う、プラットフォーム上のユーザモード２３５において実行されているアプリケーション２２５に関するマルウェアのリアルタイム検出およびマルウェアからの保護の例示的なブロック図を示す。示されているプラットフォームは、たとえば、Ｉｎｔｅｌ、ＡＭＤ、またはＡＲＭによって製造されたプロセッサに基づいている。プラットフォーム上のオペレーティングシステムは、ユーザモード２３５およびカーネルモード２４０を含む。
【０１０９】
一実施形態において、カーネルモード２４０は、オペレーティングシステムの最も低いレベルの最も信頼された機能に予約される。カーネルモード２４０において実行されるコードは、単一の仮想アドレス空間を共有する。したがって、カーネルモードドライバ（たとえば２００）は、他のドライバ（たとえば２０５）およびオペレーティングシステムそれ自体から隔離される。カーネルモード２４０において、実行中のコードは、基礎となるハードウェア（たとえば、図３を参照して以下に説明されるプロセッサ３１０）に対するアクセスを有する。それは、ＣＰＵ命令および参照メモリアドレスを実行する。
【０１１０】
プロセッサは、プロセッサ上で実行されているコードの種類に応じて２つのモード間で切り替わってよい。たとえば、アプリケーション２２５はユーザモードにおいて実行されてよく、コアオペレーティングシステムコンポーネントはカーネルモード２４０において実行されてよい。ドライバは、カーネルモード２４０またはユーザモード２３５において実行されてよい。他の実施形態において、プラットフォームは、本明細書に説明されるものよりも追加のまたは少ないコンポーネントを備える。同様に、機能は、ここで説明されるのと異なる方式でコンポーネントおよび／または異なるエンティティの間で分散されることが可能である。
【０１１１】
サービス２２０は、バックグラウンドにおいて動作するプログラムを指す（概念がデーモンに類似する）。ユーザモード２３５は、多くの異なる種類のオペレーティングシステム用に書かれたアプリケーション２２５を実行するサブシステム２３０を含む。ユーザモード２３５におけるサブシステム２３０は特定のシステムリソースに限定されるが、カーネルモード２４０は通常、システムメモリおよび外部デバイスに対する制限されないアクセスを有する。ユーザモード２３５は、Ｉ／Ｏマネージャ１２０を使用することによってＩ／Ｏ要求を適切なカーネルモードデバイスドライバ２００に渡すことができるサブシステムを含む。
【０１１２】
オペレーティングシステムは、ダイナミックリンクライブラリとして知られる共有ライブラリをサポートし、このライブラリは、１つのみのコピーがメモリにロードされた状態で複数のプロセスによって使用されることが可能であるコードライブラリである。たとえば、ＮＴＤＬＬ．ＤＬＬ２１５は、ＷｉｎｄｏｗｓネイティブＡＰＩ（Ｗｉｎ３２または他のＡＰＩサブシステムからのサポートなしに実行しなければならないオペレーティングシステムのユーザモードコンポーネントによって使用されるインターフェース）をエクスポートする。ＮＴＤＬＬ．ＤＬＬ２１５は、「ＮＴ　Ｌａｙｅｒ　ＤＬＬ」の記述を有するオペレーティングシステムによって作成されたファイルであり、ＮＴカーネル機能を含むファイルである。一実施形態において、ＮＴＤＬＬ．ＤＬＬ２１５は、ｃ：＼Ｗｉｎｄｏｗｓ＼ｓｙｓｔｅｍ３２またはｃ：＼ｗｉｎｎｔ＼ｓｙｓｔｅｍ３２ディレクトリに配置されてよく、ｃ：＼ｉ３８６ディレクトリに見出されることもある。
【０１１３】
カーネルモードＡＰＩ２１０は、（図１に関して上記に説明されている）Ｉ／Ｏマネージャ１２０およびフィルタマネージャ１２５とインターフェースする。カーネルモードデバイスドライバ２００は、管理ノード１００にアタッチされた特定の種類のデバイスを操作および制御するプログラムである。カーネルは、図１に関して上記に説明されている。

グラフィックスドライバ２０５は、特定のグラフィックデバイスと通信するためにカーネルモード２４０においてオペレーティングシステムよって使用されるソフトウェアを指す。ハードウェア抽象化層は図１に関して上記に説明されている。

【０１１４】

一実施形態において、アプリケーション２２５は、１つまたは複数の実行スレッドを含んでよい。リング３において実行されているとき（ユーザモード２３５）、アプリケーション２２５（スレッド）は、ＷｒｉｔｅＦｉｌｅ（）などのシステムサービスを要求してよい。ＮＴＤＬＬ．ＤＬＬ２１５は、ＳｙｓＥｎｔｅｒ　ｘ８６命令を呼び出してよく、スレッドのコンテキストがユーザモード２３５からカーネルモード２４０に変わる。コンテキストスイッチは、カーネルスケジューラがプロセッサ（またはコア）を１つのスレッドから別のスレッドに切り替えるときに発生してよい。この場合、スレッドは、リング３からリング０に変更されているだけである。それは、同じプロセッサまたはコア上に留まっている。より高い優先度のスレッドが、前のスレッドのプロセッサに割り当てられてよい（コンテキストスイッチ）。一実施形態において、コンテキストスイッチは、２つのスレッドが状態を変更したときに発生する。他のアーキテクチャ上では、割り込みが生成されてよい。各スレッドは、２つのスタックを有し、１つはユーザモード２３５に使用されるもので、もう１つはカーネルモード２４０に使用されるものである。割り込みが生成され、次いで、スレッドカーネルが、ＮｔＷｒｉｔｅＦｉｌｅ（）またはＺｗＷｒｉｔｅＦｉｌｅ（）などのカーネルモードネイティブＡＰＩ２１０を実行する。

【０１１５】

一実施形態において、アプリケーション２２５がユーザモード２３５において実行されるとき、オペレーティングシステムがアプリケーション２２５のためのプロセスを作成してよい。プロセスは、プライベート仮想アドレス空間およびプライベートハンドルテーブルをアプリケーション２２５に提供する。アプリケーションの仮想アドレス空間はプライベートであるため、１つのアプリケーションが別のアプリケーションに属するデータを変更することはできない。各アプリケーション２２５は隔離されて実行され、ユーザモードアプリケーションがクラッシュした場合、クラッシュはその１つのアプリケーションに限定される。他のアプリケーションおよびオペレーティングシステムは、クラッシュによって影響されない。一実施形態において、カーネルモード２４０における各スレッドは、単一の仮想アドレス空間を共有する。したがって、すべてのカーネルモードスレッドおよびユーザモードスレッドが可視である。

【０１１６】

一実施形態において、プロセッサは、複数のレベルのセキュリティを提供してよい。３２ビットおよび６４ビットＩｎｔｅｌおよびＡＭＤプロセッサの場合、カーネル１６５は、最も特権が与えられたリング０において実行されてよい。すべてのユーザアプリケーション２２５は、リング３において実行され、ダイナミックリンクライブラリ（ＤＬＬ）システムを介してカーネルサービスを要求する。すべてのユーザモード２３５要求は、ＮＴＤＬＬ．ＤＬＬ２１５を使用して、特定の関数パラメータを修正し、ＳｙｓＥｎｔｅｒを使用して要求スレッドをリング３からリング０に切り替える。ディスパッチャが要求を受信し、それをエグゼクティブのサービスに渡す。スケジューラは、実行する準備ができているスレッドを再検査する。コンテキストスイッチを引き起こすユーザからの特権モード要求の間に、より低い優先度のスレッドが優先割り込みされてよい。

【０１１７】

例示的なフィルタマネージャおよびミニフィルタドライバ

図３は、実施形態に従う、マルウェアのリアルタイム検出およびマルウェアからの保護のための例示的なフィルタマネージャ１２５ならびにミニフィルタドライバ３２０、３２５、および３３０を示す。他の実施形態において、構成は、本明細書に説明されるものよりも追加のまたは少ないコンポーネントを備える。同様に、機能は、ここで説明されるのと異なる方式でコンポーネントおよび／または異なるエンティティの間で分散されることが可能である。

【０１１８】
プロセッサ３１０上でユーザモード２３５において実行されているアプリケーション２２５またはプロセスは、ユーザ要求３００（たとえば、ファイルオープン要求などのファイル操作要求）を生成してよい。一実施形態において、ユーザモード２３５におけるプロセス２２５は、Ｗｉｎｄｏｗｓ　ＡＰＩでファイルを作成するためにコールを行う。このコールは、ファイルＩ／Ｏを求めるユーザ要求３００をトリガする（たとえば、Ｗｉｎｄｏｗｓ　ＮＴ　ＡＰＩコール）。要求３００は、ＮＴＤＬＬ．ＤＬＬ２１５を通じて進む。Ｉ／Ｏマネージャ１２０は、ユーザモード２３５において実行されているプロセス２２５によって開始されたファイル操作要求３００を検出する。一実施形態において、Ｉ／Ｏマネージャ１２０は、Ｗｉｎｄｏｗｓオペレーティングシステムの一部であってよい。Ｉ／Ｏマネージャ１２０は、ターゲットファイルがどこに配置されているか（たとえば、Ｄ：＼ｄｒｉｖｅ）を特定し、ファイルオープン要求３００をインターセプトすることにドライバが関心を有するかどうかを決定するためにフィルタマネージャ１２５にメッセージを送信する。フィルタマネージャ１２５は、特定のファイルシステムおよび特定のボリュームにアタッチされる。

【０１１９】
一実施形態において、フィルタマネージャ１２５はカーネルモード２４０において初期化される。フィルタマネージャ１２５は、ファイル操作要求３００に対応するファイルハンドルから、ファイル操作要求３００が所定の操作たとえばファイルオープン要求に対応するかどうかを決定してよい。フィルタマネージャ１２５は、ファイルシステムフィルタドライバにおいて一般的に必要な機能性を提示するカーネルモードドライバである。ミニフィルタドライバ（たとえばミニフィルタドライバＡ３２０）は、この機能性を使用するように書かれてよく、それによって、より高品質でより堅牢なドライバを作成するとともに開発プロセスを短縮する。ファイルハンドル（ファイル記述子と呼ばれることもある）は、パイプまたはネットワークソケットなどのファイルまたは他の入出力リソースにアクセスするために使用される抽象的インジケータ（たとえば数）である。ファイルが開かれるとき、要求されるファイルアクセスの種類、たとえば、読み取り、書き込み、共有、および排他などが決定される。ミニフィルタドライバＡ３２０またはＣ３３０が、ハンドル追加ステップを行う。ハンドル追加ステップは、ファイルハンドルが所定のものであるかどうかを決定し、それをツリーに格納する。それが強力な暗号化を用いてバッファを書き込んでいる場合は、所定のものである。ハンドルが所定のものでない場合、それは無視されることができる。

【０１２０】
ファイル操作要求３００が所定の操作に対応すると決定することに応答して、ファイル操作要求３００がインターセプトされる。一実施形態において、フィルタマネージャ１２５は、ファイル操作要求をインターセプトするためにミニフィルタドライバ（たとえばミニフィルタドライバＡ３２０）が登録されているかどうかを決定することによって、ファイル操作要求３００をインターセプトする。ミニフィルタドライバＡ３２０は、所定のイベント（たとえば、ファイルオープン（fopen）、読み取り、書き込み、クローズ、名前変更）についてフィルタマネージャ１２５に事前に登録されていてよい。ファイル操作要求をインターセプトするためにミニフィルタドライバＡ３２０が登録されていると決定することに応答して、フィルタマネージャ１２５は、ファイル操作要求３００をミニフィルタドライバＡ３２０に送信する。

【０１２１】
一例において、フィルタマネージャ１２５は、ミニフィルタドライバ（たとえばミニフィルタドライバＡ３２０）が要求３００をインターセプトすることに関心があるかどうかをチェックする。フィルタマネージャ１２５は、コールバックによってミニフィルタドライバＡ３２０を識別してよい。まず、ミニフィルタドライバＡ３２０は登録を行い、次いで、それは、どのイベントが関心を持たれているかを識別する。操作は、以下のように実装されてよい。

【０１２２】
【数３】

```
DRIVER_INITIALIZE DriverEntry;
NTSTATUS
DriverEntry (
   _In_ PDRIVER_OBJECT DriverObject,
   _In_ PUNICODE_STRING RegistryPath
   );

NTSTATUS
EnZooMessage (
   _In_ PVOID ConnectionCookie,
   _In_reads_bytes_opt_(InputBufferSize) PVOID InputBuffer,
   _In_ ULONG InputBufferSize,
   _Out_writes_bytes_to_opt_(OutputBufferSize,*ReturnOutputBufferLength) PVOID
OutputBuffer,
   _In_ ULONG OutputBufferSize,
   _Out_ PULONG ReturnOutputBufferLength
   );

NTSTATUS
EnZooConnect(
   _In_ PFLT_PORT ClientPort,
   _In_ PVOID ServerPortCookie,
   _In_reads_bytes_(SizeOfContext) PVOID ConnectionContext,
   _In_ ULONG SizeOfContext,
   _Flt_ConnectionCookie_Outptr_ PVOID *ConnectionCookie
   );

VOID
EnZooDisconnect(
   _In_opt_ PVOID ConnectionCookie
   );
```

【０１２３】
マルウェア検出分析は、検出されたファイル操作要求３００に関連付けられたファイルバッファに関して行われて、マルウェアの存在を示す挙動を検出する。カーネルモード２４０におけるミニフィルタドライバは、ファイルバッファに対するマルウェア検出分析を行って、許可されていない／疑わしい挙動を検出する。マルウェア検出分析は、モンテカルロ近似、エントロピ、および／または系列係数分析を含んでよい。分析は、ファイルバッファにおけるデータが暗号化されているかどうかを決定することを含む。たとえば、疑わしい書き込み操作が検出されることがある。ミニフィルタドライバは、オペレーティングシステムバッファからデータを直接読み取って、性能を増大し、統計分析のオーバヘッドを低減してよい。マルウェア分析は、上記で図１に関して説明された統計的技法を使用して、ファイルが暗号化されているかどうかを決定する。「カーネルバッファ分析」ステップは、ランサムウェアおよびマルウェア分析を行ってよい。ステガノグラフィ分析の一部が行われてもよい。したがって、ステガノグラフィは、複数のエンティティ、たとえば、静的（スキャン）、動的（リアルタイム）、ファイアウォール、ｓｍｔｐサーバなどによって行われることがある。

【０１２４】
マルウェアの存在を示す挙動を検出することに応答して、検出されたファイル操作要求３００を開始することを担当するプロセス２２５が識別される。ミニフィルタドライバＡ

３２０は、書き込み操作に関するマルウェア分析を行う。ミニフィルタドライバＡ３２０は、ファイルアクセス前操作（ファイル読み取り／書き込み要求）を取り扱う。フィルタマネージャ１２５は、ミニフィルタドライバＡ３２０にコールを送信し、ミニフィルタドライバＡ３２０は、カイ二乗、エントロピ、系列係数相関、およびモンテカルロパイ近似の組み合わせを決定して、それがファイルオープン操作３００を進めるべきか否かを決める。ミニフィルタドライバＡ３２０は、それがオペレーティングシステムカーネルＩ／Ｏバッファにおける書き込みデータを既に有するので、書き込みを分析することができる。ミニフィルタドライバＡ３２０は、マルウェア状態変化に関して書き込みバッファを分析する。主要なマルウェア検出分析が行われ、データが暗号化されていないと決定されたときのみにデータが書き込まれる。マルウェア分析が強力な暗号化を示さない場合、ＦｉｌｅＷｒｉｔｅ（）操作の成功が可能にされる。

【０１２５】

ミニフィルタドライバＣ３３０は、読み取りに関するマルウェア分析を行う。ミニフィルタドライバＣ３３０は、ファイルアクセス後操作も取り扱う。それは、マルウェア状態変化に関して読み取りバッファを分析する。要求３００がミニフィルタドライバＣ３３０に到達する前に、システムに対する状態変化（書き込み）がない。ミニフィルタドライバＡ３２０またはＣ３３０がマルウェアを示す状態変化を検出した場合、それらは、ファイル操作３３０を停止することができる。ミニフィルタドライバＣ３３０が「ファイル読み取り（fread）」操作を承認する場合、フィルタマネージャ２１５は、ファイルシステムドライバ３０５に要求を送信し、ファイルシステムドライバ３０５は、Ｉ／Ｏ要求パケットをストレージドライバスタック３１５に送る。ファイルシステムドライバ３０５は、リムーバブルメディア（たとえばＣＤ－ＲＯＭ）用のファイルシステムドライバ、新しいファイルシステムのためのモデルとして使用されるＷｉｎｄｏｗｓ ｉｎｂｏｘ ＦａｓｔＦＡＴファイルシステムに基づくファイルシステムドライバ、ファイル内のデータを検査するトランザクション対応ファイルスキャナなどであってよい。ミニフィルタドライバＣ３３０が再び呼び出され、バッファを検査し、フィルタマネージャ１２５に承認を送る。

【０１２６】

プロセッサ３１０を使用してデータが読み取られると、ＩＲＰがフィルタマネージャに戻される。ミニフィルタＣは、ＩＲＰにおけるデータを調べる。たとえば、書き込み操作の前に、ドライバが書き込みバッファを分析する場合、それは、エントロピ、カイ二乗、モンテカルロＰｉ近似、系列相関係数、平均、標準偏差、および他の統計値を計算して、許可されていないデータ暗号化、データ削除、または疑わしい挙動を検出する。ミニフィルタＡは、これらの統計に基づいて、暗号化されたデータをディスク１５５上のファイルに書き込むマルウェアからの保護をする。ミニフィルタＣは、以前に暗号化されたデータを識別し、データを読み取るプロセスからホワイトリストおよびブラックリストを構築することを助ける。ミニフィルタＡは、データが暗号化されないように保護をするが、ミニフィルタＣは、暗号化されたデータを復号することはできないので、それは、ファイルを使用しているプロセスを識別する。ミニフィルタＡは書き込み前操作検出として、ミニフィルタＣは読み取り後操作検出として最も良く説明される可能性がある。システムは、前および後操作についてそのデータ構造を更新し維持するように登録をする。

【０１２７】

ミニフィルタドライバＢ３２５は、サードパーティドライバである。開示されている実施形態は、ミニフィルタドライバＢ３２５を使用して、ファイルの削除、ファイルの名前変更、またはディクトリの変更を試みるマルウェアを検出してもよい。

【０１２８】

識別されたプロセス２２５の検索は、プログラムのブラックリストおよびプログラムのホワイトリストのうちの１つまたは複数において行われて、識別されたプロセス２２５が信頼されたプロセスであるかどうかを決定する。プログラムのブラックリストは、アクセスまたは実行する（実行）権限を与えられるべきではない知られている悪意のあるまたは疑わしいプログラムを含んでよい。これらのプログラムは通常、ウイルス、トロイの木馬

、ワーム、スパイウェア、キーロガー、および他のマルウェア形態など、悪意のあるソフトウェアを含む。ブラックリストに載せられるプログラムは、企業または個人に脅威を与えることが知られているユーザ、ビジネスアプリケーション、プロセス、ＩＰアドレス、および組織も含む。

【０１２９】

プログラムのホワイトリストは、管理ノード１００に対するアクセスを可能にされる許容可能なエンティティ（ソフトウェアアプリケーション、電子メールアドレス、ユーザ、プロセス、デバイスなど）のリストを含んでよい。ホワイトリストは、アプリケーション２２５を、それらのファイル名、サイズ、およびディレクトリパスに基づいて識別してよい。一実施形態において、ホワイトリストは、各コンポーネントまたは各ソフトウェア２２５の製造者または開発者に関連付けられた暗号学的ハッシュ技法およびデジタル署名の組み合わせを使用してよい。

【０１３０】

一例において、管理ノード１００は、プログラムのブラックリスト上において識別されたプロセス２２５を特定することによって、識別されたプロセス２２５が信頼されたプロセスではないと決定することがある。管理ノード１００は、マルウェアを記述する情報をクライアントデバイスに送信する。一例において、管理ノード１００は、プログラムのホワイトリスト上において識別されたプロセス２２５を特定することによって、識別されたプロセス２２５が信頼されたプロセスであると決定することがある。その場合、ミニフィルタドライバは、検出されたファイル操作要求を無視する。

【０１３１】

ミニフィルタドライバＡ３２０およびミニフィルタドライバＢ３３０はカーネルモード２４０において実行されるので、それらは、どのプロセスがファイルの状態を変更しているかを決定することができる。ファイルが暗号化されている、または大量のデータが削除されている場合、管理ノード１００は、ユーザに、ファイルシステムの状態をプロセス２２５が変更することを可能にしたいかどうかを尋ねてよい。ユーザが操作を承認した場合、それは許容され、処理されたイメージのＳＨＡ２５６ハッシュが任意選択でホワイトリストに記憶される。プロセスがマルウェアである場合、ＳＨＡ２５６ハッシュはブラックリストに追加される。プロセスが実行されたとき、ドライバはブラックリストをチェックし、ブラックリストに載せられている場合は実行を防止する。

【０１３２】

一実施形態において、管理ノード１００は、識別されたプロセス２２５が信頼されたプロセスであるかどうかを以下のように決定してよい。プログラムのブラックリストまたはプログラムのホワイトリスト上においてプロセス２２５を特定しないことに応答して、管理ノード１００は、クライアントデバイスに、識別されたプロセスを許可することを求める要求を送信してよい。管理ノード１００は、プロセス３００が許可されているかどうかを問い合わせるために、プロンプトがクライアントデバイスへ提示されるようにするデータを生成してよく、たとえば、プロンプトはＣＡＰＴＣＨＡを含んでよい。

【０１３３】

識別されたプロセス２２５を許可することを求める要求をクライアントデバイスに送信することに応答して、管理ノード１００は、識別されたプロセス２２５が許可されないというメッセージをクライアントデバイスから受信することがある。その場合、識別されたプロセス２２５は、マルウェア検出のためにプログラムのブラックリストに追加される。識別されたプロセス２２５が許可されたというメッセージをクライアントデバイスから受信することに応答して、識別されたプロセス２２５は、プログラムのホワイトリストに追加されてよい。

【０１３４】

識別されたプロセス２２５が信頼されたプロセスではないと決定することに応答して、識別されたプロセス２２５に対してマルウェア修正アクションが実行される。攻撃詳細はローカルにログ記録される。たとえば、ミニフィルタドライバＡ３２０は、ファイル操作

要求３００を停止、一時停止、または許可するためにメッセージをフィルタマネージャ２１５に送信してよい。一実施形態において、同様の技法が、ファイアウォール１３５とインラインでインバウンドファイルを検査するために使用される。マルウェア分析は、マルウェアがファイアウォール１３５を通過してネットワークのルータ１４５およびスイッチ１５０に達するのを防止するために使用される。インライン実施形態はステガノグラフィを検出してもよい。あらゆる疑わしいファイルがログ記録され隔離されるので、ユーザは、それが誤検出であった場合にファイルを復元することができる。

【０１３５】

ボリュームシャドウサービスの例示的なコンポーネント

図４は、実施形態に従う、マルウェアのリアルタイム検出およびマルウェアからの保護のためのボリュームシャドウサービス（ＶＳＳ）の例示的なコンポーネントを示す。ＶＳＳは、ＶＳＳコピーサービス４００、ＶＳＳリクエスタ４０５、ＶＳＳライタ４１０、ならびにＶＳＳプロバイダ４１５、４２０、および４２５を含む。他の実施形態において、ＶＳＳは、本明細書に説明されるものよりも追加のまたは少ないコンポーネントを備える。同様に、機能は、ここで説明されるのと異なる方式でコンポーネントおよび／または異なるエンティティの間で分散されることが可能である。

【０１３６】

ランサムウェアは、感染または暗号化されたファイルの回復を防止するためにＶＳＳを無効にしようとすることがある。本明細書に開示されている実施形態は、特定のデータ回復ＡＰＩを使用して、有用なバックアップが復元されてデータ損失を防止できることを確実にする。ＶＳＳは、許可されていない変更から保護をするために暗号化される構成データベースに読み取りおよび書き込みをする。ＶＳＳは、デバイスを分析し、コアおよびプロセッサ種類ならびに現在のワークロードに基づいて、そのデバイスに最適なリソース構成を自動的に作成する。プロセッサ情報およびメモリ情報が、スレッドプールのサイズを構成するために使用される。

【０１３７】

マルウェア検出および除去などのイベントが、ローカルログに書き込まれる。ローカルログは、管理ノード１００およびファイアウォール１３５から、セキュリティマネージャポリシによって指定された中央ログサーバに定期的に複製される。

【０１３８】

モンテカルロパイ近似のための例示的なデータ点

図５は、実施形態に従う、モンテカルロパイ近似に関する例示的なデータ点を示す図である。モンテカルロパイ近似は、暗号化されたファイルから圧縮されたファイルを区別するために使用されてよい。モンテカルロシミュレーションは、ファイルにおける値のランダム性の測定を可能にする。モンテカルロシミュレーションの１つのアプリケーションは、ファイルにおけるデータに基づいてＰｉ（π）の値を近似することである。ファイルに含まれる値がランダムであるほど、πの推定される値がより正確である。Ｐｉ（π）の値は、正方形におけるデータ点５１０の総数に対する内接単位円におけるデータ点５００の比によって計算される。

【０１３９】

図５は、内接単位円におけるデータ点５００、および正方形におけるデータ点５１０の総数を示す。計算された近似値がＰｉの知られている値に近いほど、それがデータ値のランダム性をより良く表す。完全な暗号化アルゴリズムは完全にランダムな値を有することになり、Ｐｉの正確な近似値を提供する。一実施形態において、システムは以下の決定を行う。

円面積（ＡｒｅａＣｉｒｃｌｅ）＝πr^2

正方形面積（ＡｒｅａＳｑｕａｒｅ）＝$(2r)^2=4r^2$

【０１４０】

半径５０５が１単位であり、円における点５００が（$x^2+y^2<=1$）によって与えられると仮定する。円の面積／正方形の面積＝（Ｐｉ×半径^2）／（４×半径^2）＝Ｐｉ／４

となる。したがって、点５１０の総数によって割られた円内部の点５００の数は、Ｐｉ／４によって与えられる。

【０１４１】

マルウェアのリアルタイム検出およびマルウェアからの保護のための例示的なプロセス

図６は、実施形態に従う、マルウェアのリアルタイム検出およびマルウェアからの保護のための例示的なプロセスを示す。一実施形態において、図６のプロセスは管理ノード１００によって行われる。他のエンティティ（たとえばマルウェア分析モジュール１４０）が、他の実施形態においてプロセスのステップの一部または全部を行ってよい。同様に、実施形態は、異なるおよび／もしくは追加のステップを含み、または異なる順序でステップを行ってよい。

【０１４２】

管理ノード１００は、ユーザモード２３５において実行されているプロセス２２５によって開始されたファイル操作要求３００を検出する６００。管理ノード１００は、ファイル操作要求３００に対応するファイルハンドルから、ファイル操作要求３００が所定の操作に対応するかどうかを決定することによって、ファイル操作要求３００を検出してよい。

【０１４３】

管理ノード１００は、検出されたファイル操作要求３００に関連付けられたファイルバッファに関してマルウェア検出分析を行って６０５、マルウェアの存在を示す挙動を検出する。マルウェア検出分析は、カイ二乗、エントロピ決定、系列係数相関、およびモンテカルロパイ近似の組み合わせを含んでよい。

【０１４４】

マルウェアの存在を示す挙動を検出することに応答して、管理ノード１００は、検出されたファイル操作要求３００を開始することを担当するプロセス２２５を識別する６１０。

【０１４５】

管理ノード１００は、プログラムのブラックリストおよびプログラムのホワイトリストのうちの１つまたは複数において、識別されたプロセス２２５の検索を行って６１５、識別されたプロセス２２５が信頼されたプロセスであるかどうかを決定する。プログラムのブラックリストは、アクセスまたは実行する（実行）権限を与えられるべきではない知られている悪意のあるまたは疑わしいプログラムを含んでよい。プログラムのホワイトリストは、管理ノード１００に対するアクセスを可能にされる許容可能なエンティティ（ソフトウェアアプリケーション、電子メールアドレス、ユーザ、プロセス、デバイスなど）のリストを含んでよい。

【０１４６】

識別されたプロセス２２５が信頼されたプロセスではないと決定することに応答して、管理ノード１００は、識別されたプロセス２２５に対してマルウェア修正アクションを実行し６２０、マルウェアを記述する情報をクライアントデバイスに送信する。マルウェア修正アクションは、検出されたファイル操作要求に関連付けられた書き込み操作を終了することを含んでよい。マルウェア修正アクションは、検出されたファイル操作要求をメモリから削除することによって、検出されたファイル操作要求を終了することを含んでよい。マルウェア修正アクションは、識別されたプロセスに関連付けられたディスクファイルイメージを隔離することを含んでよい。

【０１４７】

ステガノグラフィのリアルタイム検出およびステガノグラフィからの保護のためのポータブル実行可能（ＰＥ）ファイル

図７は、実施形態に従う、カーネルモードにおけるステガノグラフィのリアルタイム検出およびステガノグラフィからの保護のための例示的なポータブル実行可能（ＰＥ）ファイルのコンポーネントを示す。ＰＥフォーマットは、実行ファイル、オブジェクトコード、ＤＬＬ、ＦＯＮフォントファイル、ならびにＷｉｎｄｏｗｓオペレーティングシステム

の３２ビットおよび６４ビット版で使用される他のもののためのファイルフォーマットである。ＰＥフォーマットは、Ｗｉｎｄｏｗｓ　ＯＳローダがラップされた実行可能コードを管理するために必要な情報をカプセル化するデータ構造である。

【０１４８】

ＰＥヘッダ７６５は、複数のセグメントが任意のメモリアドレスでロードされるのを可能にする再配置情報を含むＤＯＳ実行可能ヘッダ７００を含む。ＤＯＳスタブ７０５は、ＭＳ－ＤＯＳにおいて実行される有効なアプリケーションである。それは、ＥＸＥイメージの先頭に配置される。セクションテーブルの各行（たとえば、７１５、７２０、および７２５）はセクションヘッダである。セクションヘッダはＮＵＬＬ７３０ターミネータを有してよい。各セクション（たとえば、７３５、７４５、および７５５）がＮＵＬＬターミネータを有してもよい。

【０１４９】

本明細書に開示されている実施形態は、カーネルモードにおけるステガノグラフィのリアルタイム検出およびステガノグラフィからの保護のための図７に示されたＰＥファイルフォーマットを使用する方法に関する。ステガノグラフィは、コンテナ内部にマルウェアを隠すために使用されてよい。コンテナは、ピクチャ、映画、音声ファイル、または実行ファイルであってよい。ステガノグラフィは、ピクチャ、ｍｐ３、またはｅｘｅファイル内に情報を隠すために使用されてよい。たとえば、１２８バイトテキストメッセージが４ＭＢピクチャ内に隠されてよい。ｅｘｅファイルが別のｅｘｅファイル内部に隠されてよい（パック）。マルウェアファイルはｐｋｚｉｐファイル内に隠されてよい。ユーザがウェブサイトを訪問しているとき、ウイルスのドライブバイダウンロードが発生することがある。マルウェアがユーザに送られることもある。次いで、それは、ユーザのメーリングリストなどにおいて、たとえば、パーソナライズされたクリスマスカードで各友達へ行くことがある。マルウェアは、数ヶ月の期間にわたってファイルを暗号化し、暗号化キーを除去することがある。従来のエッジファイアウォールは、添付ファイルがファイアウォールを通じて進むことを可能にされるので、ステガノグラフィを使用して隠されている隠れピクチャ、メッセージ、またはマルウェアを含むファイルを通常は検出できない。

【０１５０】

ファイアウォール、オペレーティングシステム、または電子メールシステムを介するファイルの送信が検出される。一実施形態において、ＰＥはパースされる。ＰＥを読み取りおよびパースする間に、Ｗｉｎｄｏｗｓ　ＥＸＥ、ＤＬＬ、フォント、システムドライバ、およびオブジェクトコードの構造が、疑わしいＡＰＩ使用について分析される。例は、悪意のあるプログラムがメモリセクションにコピーされ実行されることを可能にすることがある読み取り、書き込み、および実行許可を有するメモリセクションの割り当てである。一実施形態において、ＷｉｎｄｏｗｓＡＰＩは、ＧｅｔＭｏｄｕｌｅＦｉｌｅＮａｍｅＥｘ（）およびＣｒｅａｔｅＦｉｌｅ（）を呼び出すことによって提供されるプロセスの完全修飾名（ＦＱＦＮ）を使用してファイルを開くために使用される。ディスク上のイメージに対するハンドルが呼び出し元に返される。

【０１５１】

一実施形態において、ＰＥファイルのサイズが決定され、記憶されたファイルのファイルサイズと比較される。この実施形態は、悪意のあるｚｉｐファイルまたは添付された実行ファイルなどの許可されていないデータをイメージが含むかどうかを検出するために使用されてよい。この実施形態において、ＰＥファイルフォーマットの最後に記憶された隠された情報（たとえば、ＥＸＥ、ＤＬＬ、ＳＣＲ、ＳＹＳ、ＤＲＶ、ＡＣＭ、ＣＰＬ、ＳＣＲなど）が識別されてよい。ＰＥファイルのサイズを決定するために、ファイルがパースおよび分析される。ファイルは、ファイルの完全修飾ファイル名を使用して開かれる。ファイルのＤＯＳヘッダ７００がストレージデバイス１５５から読み取られる。ファイルが実行可能ファイルであるかどうかを決定するために、ＤＯＳヘッダ７００が「ＭＺ」で始まるかどうかが決定される。マジックナンバーがＤＯＳヘッダ７００から取り出される。マジックナンバーが検証されて、ファイルのセクションヘッダに対するポインタを取得

する。セクションヘッダで始まるファイルの各セクションについて、セクションの名前および属性が検証される。セクションのサイズが決定される。ファイルのサイズを決定し、マルウェアによってしばしば利用される非標準的なセクション名を識別するために、ファイルの各セクションの名前およびサイズが決定される。

【０１５２】

一実施形態において、Ｗｉｎｎｔ．ｈ　ＳＤＫヘッダファイルにおけるＩＭＡＧＥ＿ＤＯＳ＿ＨＥＡＤＥＲ構造がストレージデバイス１５５から読み取られる。ＤＯＳヘッダ７００はファイルの第１の部分である。このステップは、ＤＯＳヘッダ７００がＭＺ「ｘｘ　ｘｘ　ｘｘ」で開始するかどうかを決定する。ＤＯＳヘッダ７００がＭＺで始まる場合、それはＤＯＳまたはＷｉｎｄｏｗｓプログラムである可能性がある。ＤＯＳヘッダ７００がＭＺで始まらない場合、それは、実行ファイルでない（たとえば、ＪＰＧ、ＧＩＦなどである可能性がある）。この区別が、どの分析を適用するかを決定する。ＤＯＳヘッダ７００を読み取る目的は、ファイルが適切に形成されたことを確認することである。プロセスは、不正なヘッダの作成を探している。ＤＯＳヘッダ７００は、静的（不変）であり、日付およびタイムスタンプを含む。ＤＯＳヘッダ７００をパースする目的は、知られている優良なヘッダの既存のリストにない不正なヘッダの作成を検出することである。不正なヘッダ（ＰＥヘッダ）は、マルウェアコード（不正な命令）を伴うセクションに対するポインタを有する。本明細書に開示されている実施形態は、マルウェアが実行可能ファイルにおける圧縮されたペイロードとして隠される可能性があるため、実行可能ファイルと非実行可能ファイルを区別する。ファイルの種類の決定は、ファイルにおけるステガノグラフィを検出するために使用される特定の分析を決定するために使用される。

【０１５３】

数「ＭＺ」（ファイルの最初の数バイト）はマジックナンバーである。マジックナンバーを検証することによって取得されたポインタは、情報が配置されているファイルにおける部分につながる。ファイルが有効なＰＥファイル、たとえばＪＰＥＧまたはＧＩＦでない場合、それはマルウェアである可能性がある。一実施形態において、マジックナンバーは、ＩＭＡＧＥ＿ＤＯＳ＿ＨＥＡＤＥＲにおけるｅ＿ｍａｇｉｃ　ｍｅｍｂｅｒから取り出される。マジックナンバーを検証するために、ＤＯＳヘッダ７００における値「ｘｘ　ｘｘ　ｘｘ」が使用される。見つけられた値は、値０ｘ５Ａ４Ｄ（「ＭＺ」）を有するＭｉｃｒｏｓｏｆｔ　ＤＯＳ　ＩＭＡＧＥ＿ＤＯＳ＿ＳＩＧＮＡＴＵＲＥと比較される。値がＤＯＳ署名と一致しない場合、ファイルはＤＯＳまたはＷｉｎｄｏｗｓ実行ファイルではない。ファイルのフォーマットが何であってよいか、たとえば、ＤＯＣ、ＤＯＣＸ、ＰＰＴ、ＰＰＴＸ、ＸＬＳ、ＸＬＳＸ、ＭＰ３、ＧＩＦ、ＪＰＧ、ＰＮＧなどを決定するために、追加の命令が実行されてよい。マジックナンバーが検証されると、セクションヘッダに対するポインタが取得される。ＤＯＳマジックナンバーが検証されたので、Ｗｉｎｄｏｗｓ　ＰＥヘッダに対するポインタを作成するためにｅ＿ｌｆａｎｅｗメンバーが使用されてよい。ＩＭＡＧＥ＿ＮＴ＿ＨＥＡＤＥＲＳ３２ポインタは、ｅ＿ｌｆａｎｅｗ値にメモリバッファのサイズを加えることによって計算される。ＰＥヘッダに対するポインタは「０１　００ｈ」であるはずである。この場所は、番号「５０　４５　００ｈ」であるはずのＰＥ署名を含む。この場所が「５０　４５　００」でない場合、ファイルは疑わしいファイルである可能性がある。

【０１５４】

一実施形態において、ポインタは逆参照され、ＩＭＡＧＥ＿ＮＴ＿ＳＩＧＮＡＴＵＲＥ（０ｘ０００００４５５０）と比較されてよい。逆参照されたポインタの値がＩＭＡＧＥ＿ＮＴ＿ＳＩＧＮＡＴＵＲＥ署名と一致しない場合、ファイルはＷｉｎｄｏｗｓ実行ファイルではない。ファイルフォーマットが何であってよいか、たとえば、ＤＯＣ、ＤＯＣＸ、ＰＰＴ、ＰＰＴＸ、ＸＬＳ、ＸＬＳＸ、ＭＰ３、ＧＩＦ、ＪＰＧ、ＰＮＧなどを決定するために、追加の命令が実行されてよい。

【０１５５】

一実施形態において、ＩＭＡＧＥ＿ＳＥＣＴＩＯＮ＿ＨＥＡＤＥＲの位置が、ＩＭＡＧ

Ｅ＿ＮＴ＿ＨＥＡＤＥＲＳ３２のサイズを使用して決定される。ＰＥイメージにおけるセクションの数を含むＩＭＡＧＥ＿ＦＩＬＥ＿ＨＥＡＤＥＲにアクセスするために、ＩＭＡＧＥ＿ＮＴ＿ＨＥＡＤＥＲメンバーＦｉｌｅＨｅａｄｅｒが逆参照される。各セクションが分析されることができるように、カウンタ変数がゼロに初期化される。プロセスは、セクションの数が予想されているかどうかを決定する。追加のセクションについては疑わしく、マルウェアを含む可能性がある。各セクションについて、セクションの名前および属性が検証される。ファイルのサイズが、セクションのＳｉｚｅＯｆＲａｗＤａｔａメンバー、およびポインタのサイズとして決定される。このプロセスは、各セクションについて繰り返されてよい。最後のセクションのサイズは、ＳｉｚｅＯｆＲａｗＤａｔａメンバーにおけるバイトの数である。この結果は、ＰＥイメージがストレージデバイス上で占有するはずのバイトの数である。セクション分析によるセクションは、ファイルの全体のサイズを計算するために使用される。

【０１５６】

ファイルシステムから、ファイルの記憶されたファイルサイズが取り出される。一実施形態において、オペレーティングシステムは、ファイルシステムから、ＧｅｔＦｉｌｅＳｉｚｅ（）　ＡＰＩを使用して、ディスク上に記憶されたファイルサイズを取り出す。

【０１５７】

ファイルの決定されたサイズは、ファイルの記憶されたファイルサイズと比較される。一実施形態において、ファイルの決定されたサイズが記憶されたファイルサイズよりも大きい場合、データはＰＥファイルの最後に付加されてよい。戻りコードが、付加されるデータがないことを示す場合、ＰＥサイズと記憶されたファイルサイズとが等しい（ＰＥファイルに付加されるデータがない）。決定されたファイルサイズが記憶されたファイルサイズよりも大きいとき、これは追加のデータの存在を示す。

【０１５８】

ファイルの決定されたサイズがファイルの記憶されたファイルサイズよりも大きいことに応答して、ファイルに関してステガノグラフィ検出分析が実行される。一実施形態において、付加されたデータは、そのファイルフォーマットと、それが暗号化されているかどうかとを決定するために分析される。戻りコードが、データが付加されていることを示し、したがって、付加されたデータの隔離、削除、または除去などの定義されたポリシが実行されてよい。ステガノグラフィ検出分析は、ファイルに関して統計関数（エントロピ、カイ二乗など）を実行することを含む。行われる分析は、ファイル種類に依存する。ＧＩＦファイルの場合、ＺＩＰファイルに隠されている隠れデータが検索される。ＥＸＥファイルの場合、異なる分析が行われてよい。ｅｘｅファイルの最後を超えた情報が、エントロピ計算、カイ二乗計算、メジアン、および標準偏差計算を実行して暗号化を検出するために使用される。

【０１５９】

一実施形態において、静的分析アルゴリズムが、ステガノグラフィを検出するために使用される。この手法の利益および利点は、署名スキャンを使用することなくステガノグラフィ検出が行われてよいことである。隠された情報の存在が、インバウンドデータまたはアウトバウンドデータのいずれかにおいて検出される。ファイルの決定されたサイズと記憶されたファイルサイズとの間の比較が、より高価な分析を行うかどうかを決定するために使用される。ファイルサイズ比較は、付加されたペイロードがあるかどうかを決定する。ファイルサイズ比較が、ファイルサイズが通常であることを示すとき、高価な分析は行われない。したがって、デバイス上でファイアウォールとインラインでステガノグラフィを検出することによって、危険なファイルが、それらの秘密のペイロードを放出できる前に、検出、隔離、および除去されることが可能である。他の実施形態において、ステガノグラフィ検出は、ファイアウォール１３５または電子メールと統合されてよい。

【０１６０】

ステガノグラフィ検出分析がファイルにおけるステガノグラフィの存在を示すことに応答して、ステガノグラフィ修正アクションが実行される。ステガノグラフィを記述する情

報がクライアントデバイスに送信される。

【０１６１】

実施形態のさらなる利益および利点は、方法がファイアウォールにおいてステガノグラフィおよびランサムウェア検出を統合して各パケットをチェックすることである。方法の電子メールシステムとの統合により、各電子メールおよび添付ファイルのコンテンツをスキャンする。本発明は、署名ではなく、疑わしい命令セット、たとえば、マシンまたはアセンブリレベル言語のインジケーションを探す。一実施形態において、方法は、部分的にファイルを逆アセンブルし、そのような疑わしい命令セットを探す。

【０１６２】

カーネルモードにおけるステガノグラフィのリアルタイム検出およびステガノグラフィからの保護のためのプロセス

図８は、実施形態に従う、カーネルモードにおけるステガノグラフィのリアルタイム検出およびステガノグラフィからの保護のための例示的なプロセスを示す。一実施形態において、図８のプロセスは管理ノード１００によって行われる。他のエンティティ（たとえばマルウェア分析モジュール１４０）が、他の実施形態においてプロセスのステップの一部または全部を行ってよい。同様に、実施形態は、異なるおよび／もしくは追加のステップ含み、または異なる順序でステップを行ってよい。

【０１６３】

管理ノード１００は、ファイアウォール、オペレーティングシステム、または電子メールシステムを介するファイルの送信を検出する８００。一実施形態において、ＰＥはパースされる。ＰＥを読み取りおよびパースする間に、Ｗｉｎｄｏｗｓ　ＥＸＥ、ＤＬＬ、フォント、システムドライバ、およびオブジェクトコードの構造が、疑わしいＡＰＩ使用について分析される。

【０１６４】

管理ノード１００は、ファイルのサイズを決定する８０５。ファイルサイズ決定は、付加された悪意のあるｚｉｐファイルまたは実行ファイルなどの許可されていないデータをイメージが含むかどうかを検出するために使用されてよい。たとえば、ＰＥファイルフォーマットの最後に記憶された隠された情報（たとえば、ＥＸＥ、ＤＬＬ、ＳＣＲ、ＳＹＳ、ＤＲＶ、ＡＣＭ、ＣＰＬ、ＳＣＲなど）が識別されてよい。

【０１６５】

管理ノード１００は、ファイルシステムからファイルの記憶されたファイルサイズを取り出す８１０。一実施形態において、オペレーティングシステムは、ファイルシステムから、ＧｅｔＦｉｌｅＳｉｚｅ（）　ＡＰＩを使用して、ディスク上に記憶されたファイルサイズを取り出す。

【０１６６】

管理ノード１００は、ファイルの決定されたサイズをファイルの記憶されたファイルサイズと比較する８１５。一実施形態において、ファイルの決定されたサイズが記憶されたファイルサイズよりも大きい場合、データはＰＥファイルの最後に付加されてよい。戻りコードが、付加されるデータがないことを示す場合、ＰＥサイズと記憶されたファイルサイズとが等しい（ＰＥファイルに付加されるデータがない）。決定されたファイルサイズが記憶されたファイルサイズよりも大きいとき、これは追加のデータの存在を示す。

【０１６７】

ファイルの決定されたサイズがファイルの記憶されたファイルサイズよりも大きいことに応答して、管理ノード１００は、ファイルに関してステガノグラフィ検出分析を実行する８２０。ステガノグラフィ検出分析は、ファイルに関して統計関数（エントロピ、カイ二乗など）を実行することを含む。行われる分析は、ファイル種類に依存する。ＧＩＦファイルの場合、ＺＩＰファイルに隠されている隠れデータが検索される。ＥＸＥファイルの場合、異なる分析が行われてよい。ｅｘｅファイルの最後を超えた情報が、エントロピ計算、カイ二乗計算、メジアン、および標準偏差計算を実行して暗号化を検出するために使用される。

【０１６８】
ステガノグラフィ検出分析がファイルにおけるステガノグラフィの存在を示すことに応答して、管理ノード１００は、ステガノグラフィ修正アクションを実行し８２５、ステガノグラフィを記述する情報をクライアントデバイスに送信する。ステガノグラフィ修正アクションは、ファイアウォールを通過しようと試みているファイルの処理および送信を終了することを含んでよい。ステガノグラフィ修正アクションは、ファイルを隔離することを含んでよい。
代替的実施形態
代替的実施形態において、本明細書に開示されている方法およびシステムは、管理ノード１００上にローカルにまたはクラウド（たとえばクラウドホスト１０５）に記憶された機密データについての保護およびプライバシを強化するために使用されてよい。これらの代替的実施形態を使用して、予め設定された地理的境界を横切る機密データの許可されていないエクスポートが検出および／または防止されてよい。たとえば、実施形態は、特定の地理的領域に機密データをタグ付けし、データをその位置にロックするように使用され、その地理的領域からのデータの許可されていないエクスポートおよび／またはアクセスが監視および防止されるようにしてよい。したがって、代替的実施形態は、データ主体の個人データ、個人を識別できる情報のエクスポートに、ユーザにより大きな制御を提供してよい。また、代替的実施形態は、規制によって指定された合法的基準で行われない限りデータ処理を防止するための方法、およびデータ漏洩の効率的な報告を、企業に提供する。
加えて、代替的実施形態は、データが記憶されるときの仮名化および／または完全なデータ匿名化を企業が提供することを可能にする。一実施形態において、記憶された個人データが暗号化されて、結果の個人暗号化データは、正しい復号キーなしに特定のデータ主体に帰せられないようにされてよい。一実施形態において、トークン化が実装されてよく、それにより、機密データを、外因的なまたは悪用可能な意味または価値を有しない非機密代用物（トークン）に置き換える。トークン化は、データの種類または長さを変更せず、すなわち、それは、データの長さおよび種類に敏感なことがあるデータベースなどのレガシシステムによって処理されることが可能である。この手法の利点および利益は、従来の暗号化されたデータよりも少ない計算リソースおよび小さい記憶スペースで済むことである。保護されたデータに対するマルウェアまたはステガノグラフィ攻撃は、検出されたファイル操作要求に関連付けられたファイルに対するマルウェアまたはステガノグラフィ検出分析を行うことを含めて、開示されている実施形態を使用して、検出および防止されることが可能である。
【０１６９】
例示的なマシン
図９は、マシン可読媒体から命令を読み取ってそれらをプロセッサまたはコントローラにおいて実行することができる例示的なマシンのコンポーネントを示すブロック図である。具体的には、図９は、コンピュータシステム９００の例示的な形態においてマシンの概略図を示す。コンピュータシステム９００は、本明細書に説明されている方法論（またはプロセス）の任意の１つまたは複数をマシンに行わせるための命令９２４（たとえば、プログラムコードまたはソフトウェア）を実行するために使用されることが可能である。代替的実施形態において、スタンドアロンデバイス、または他のマシンに接続する接続（たとえばネットワーク化）されたデバイスとして動作する。ネットワーク化された配置において、マシンは、サーバ／クライアントネットワーク環境におけるサーバマシンもしくはクライアントマシンとして、またはピアツーピア（または分散された）ネットワーク環境におけるピアマシンとして動作してよい。
【０１７０】
一実施形態において、非一時的コンピュータ可読媒体は、少なくとも１つのプロセッサによって実行されたときに本明細書に説明されている動作をプロセッサに行わせる命令を記憶する。マシンは、サーバコンピュータ、クライアントコンピュータ、パーソナルコン

ピュータ（ＰＣ）、タブレットＰＣ、セットトップボックス（ＳＴＢ）、スマートフォン、モノのインターネット（ＩｏＴ）機器、ネットワークルータ、スイッチもしくはブリッジ、または、そのマシンによって行われるアクションを指定する命令９２４（順次または他の形式）を実行することができる任意のマシンであってよい。さらに、単一のマシンのみが示されているが、用語「マシン」は、本明細書に論じられている方法論の任意の１つまたは複数を実施する命令９２４を個別または共同で実行するマシンの任意の集合も含むように捉えられるべきである。

【０１７１】

例示的なコンピュータシステム９００は、１つまたは複数の処理ユニット（一般にプロセッサ９０２）を含む。プロセッサ９０２は、たとえば、中央処理装置（ＣＰＵ）、グラフィックス処理ユニット（ＧＰＵ）、デジタルシグナルプロセッサ（ＤＳＰ）、コントローラ、状態機械、１つもしくは複数の特定用途向け集積回路（ＡＳＩＣ）、１つもしくは複数の無線周波数集積回路（ＲＦＩＣ）、またはこれらの任意の組み合わせである。コンピュータシステム９００はまた、メインメモリ９０４を含む。コンピュータシステムは、ストレージユニット９１６を含んでよい。プロセッサ９０２、メモリ９０４、およびストレージユニット９１６は、バス９０８を介して通信する。

【０１７２】

加えて、コンピュータシステム９００は、静的メモリ９０６、ディスプレイドライバ９１０（たとえば、プラズマディスプレイパネル（ＰＤＰ）、液晶ディスプレイ（ＬＣＤ）、またはプロジェクタを駆動する）を含むことができる。コンピュータシステム９００はまた、英数字入力デバイス９１２（たとえばキーボード）、カーソル制御デバイス９１４（たとえば、マウス、トラックボール、ジョイスティック、モーションセンサ、または他のポインティング機器）、信号生成デバイス９１８（たとえばスピーカ）、および、やはりバス９０８を介して通信するように構成されたネットワークインターフェースデバイス９２０を含んでよい。

【０１７３】

ストレージユニット９１６は、本明細書に説明されている方法論または機能の任意の１つまたは複数を具現する命令９２４（たとえばソフトウェア）が記憶されるマシン可読媒体９２２を含む。命令９２４はまた、コンピュータシステム９００によるその実行中にメインメモリ９０４内またはプロセッサ９０２内（たとえば、プロセッサのキャッシュメモリ内）に完全にまたは少なくとも一部に存在してよく、メインメモリ９０４およびプロセッサ９０２もマシン可読媒体を構成する。命令９２４は、ネットワークインターフェースデバイス９２０を介してネットワーク９２６上で送信または受信されてよい。

【０１７４】

マシン可読媒体９２２は例示的実施形態において単一の媒体として示されているが、用語「マシン可読媒体」は、命令９２４を記憶することができる単一の媒体または複数の媒体（たとえば、集中化もしくは分散されたデータベースまたは関連付けられたキャッシュおよびサーバ）を含むように捉えられるべきである。用語「マシン可読媒体」はまた、マシンによって実行するための命令９２４を記憶することができ、本明細書に開示されている方法論の任意の１つまたは複数をマシンに実施させる、任意の媒体を含むように捉えられるべきである。用語「マシン可読媒体」は、固体メモリ、光媒体、および磁気媒体の形態でデータリポジトリを含むがそれらに限定されない。

【０１７５】

追加の考慮事項

本明細書を通じて、複数のインスタンスが、単一のインスタンスとして説明されたコンポーネント、動作、または構造を実施してよい。１つまたは複数の方法の個々の動作が別個の動作として示され説明されているが、個々の動作の１つまたは複数が同時に行われてよく、動作が示された順序で行われる必要はない。例示的な構成において別個のコンポーネントとして提示された構造および機能性は、結合された構造またはコンポーネントとして実施されてよい。同様に、単一のコンポーネントとして提示された構造および機能性は

、別個のコンポーネントとして実施されてよい。これらおよび他の変形、修正、追加、および改良は、本明細書の主題の範囲内に入る。

【０１７６】

本明細書では、特定の実施形態は、たとえば、図１ないし４、６ないし７、および９で示され説明されたように、論理もしくはいくつかのコンポーネント、モジュール、または機構を含むものとして説明されている。モジュールは、ソフトウェアモジュール（たとえば、マシン可読媒体に組み込まれたコード）またはハードウェアモジュールのいずれかを構成してよい。ハードウェアモジュールは、特定の動作を行うことができる有形のユニットであり、特定の方式で構成または配置されてよい。例示的な実施形態において、１つもしくは複数のコンピュータシステム（たとえば、スタンドアロン、クライアント、もしくはサーバコンピュータシステム）、またはコンピュータシステムの１つもしくは複数のハードウェアモジュール（たとえば、プロセッサもしくはプロセッサのグループ）が、本明細書に説明されているような特定の動作を行うように動作するハードウェアモジュールとして、ソフトウェア（たとえば、アプリケーションまたはアプリケーション部分）によって構成されてよい。

【０１７７】

種々の実施形態において、ハードウェアモジュールは機械的または電子的に実装されてよい。たとえば、ハードウェアモジュールは、特定の動作を行うために、たとえば、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）または特定用途向け集積回路（ＡＳＩＣ）のような専用プロセッサとして、永続的に構成された専用回路または論理を含んでよい。また、ハードウェアモジュールは、特定の動作を行うために、ソフトウェアによって一時的に構成された（たとえば、汎用プロセッサまたは他のプログラマブルプロセッサ内に含まれる）プログラマブル論理または回路を含んでもよい。ハードウェアモジュールを、機械的に実装するか、専用の永続的に構成された回路で実装するか、または一時的に構成された（たとえばソフトウェアによって構成された）回路で実装するかは、コストおよび時間を考慮して決定されてよいことは理解されよう。

【０１７８】

本明細書に説明されている例示的な方法の様々な動作は、該当する動作を行うように一時的に（たとえばソフトウェアによって）構成されまたは永続的に構成された１つまたは複数のプロセッサ、たとえばプロセッサ９０２によって、少なくとも部分的に行われてよい。一時的に構成されるか永続的に構成されるかにかかわらず、そのようなプロセッサは、１つまたは複数の動作または機能を実行するように動作するプロセッサで実施されるモジュールを構成してよい。本明細書で言及されるモジュールは、いくつかの例示的な実施形態において、プロセッサで実施されるモジュールを含む。

【０１７９】

１つまたは複数のプロセッサは、「クラウドコンピューティング」環境において、または「サービスとしてのソフトウェア）（ＳａａＳ）として、該当する動作の実行をサポートするように動作してもよい。たとえば、少なくとも一部の動作は、（プロセッサを含むマシンの例としての）コンピュータのグループによって行われてよく、これらの動作は、ネットワーク（たとえばインターネット）を介して、および１つまたは複数の適切なインターフェース（たとえばアプリケーションプログラムインターフェース（ＡＰＩ））を介してアクセス可能である。

【０１８０】

特定の動作の実行は、単一のマシン内に存在するだけでなくいくつかのマシンにわたって配置された１つまたは複数のプロセッサの間で分散されてよい。いくつかの例示的実施形態において、１つまたは複数のプロセッサまたはプロセッサで実施されるモジュールは、単一の地理的位置（たとえば、家庭環境、オフィス環境、またはサーバファーム内）に配置されてよい。他の例示的実施形態において、１つまたは複数のプロセッサまたはプロセッサで実施されるモジュールは、いくつかの地理的位置にわたって分散されてよい。

【０１８１】

本明細書のいくつかの部分は、マシンメモリ（たとえばコンピュータメモリ）内にビットまたはバイナリデジタル信号として記憶されたデータに対する操作のアルゴリズムまたは記号表現の観点で提示されている。これらのアルゴリズムまたは記号表現は、データ処理分野の当業者によって彼らの成果の内容を他の当業者に伝えるために使用される技法の例である。本明細書で使用される場合、「アルゴリズム」は、所望の結果に導く一貫した操作のシーケンスまたは同様の処理である。この文脈において、アルゴリズムおよび操作は物理量の物理的操作を含む。必須でないが典型的には、そのような量は、マシンによって記憶、アクセス、転送、組み合わせ、比較、または他の操作がされることが可能な電気、磁気、または光信号の形態を取ってよい。主に一般的な使用の理由から、「データ」、「コンテンツ」、「ビット」、「値」、「要素」、「シンボル」、「文字」、「用語」、「数」、または「数値」などの単語を使用して、そのような信号に言及することが便利な場合がある。しかしながら、これらの単語は便利なラベルに過ぎず、適切な物理量に関連付けられることになる。

【０１８２】

特に明記されない限り、「処理」、「コンピューティング」、「計算」、「決定」、「提示」、または「表示」などの言葉を使用する本明細書の説明は、１つもしくは複数のメモリ（たとえば、揮発性メモリ、不揮発性メモリ、もしくはこれらの組み合わせ）、レジスタ、または情報を受信、記憶、送信、もしくは表示する他のマシンコンポーネント内で、物理的（たとえば、電子的、磁気的、または光学的）量として表されるデータを操作または変換するマシン（たとえばコンピュータ）のアクションまたはプロセスを指してよい。

【０１８３】

本明細書で使用される場合、「一実施形態」または「実施形態」に対する言及は、実施形態に関連して説明される特定の要素、特徴、構造、または特性が少なくとも１つの実施形態に含まれることを意味する。本明細書における様々な箇所での「一実施形態において」という表現の出現は、必ずしもすべてが同じ実施形態を指すものではない。

【０１８４】

いくつかの実施形態は、「結合された」および「接続された」という表現をそれらの派生語と共に使用して説明されることがある。たとえば、いくつかの実施形態は、直接的な物理的または電気的接触をした２つ以上の要素を指すために「結合された」という用語を使用して説明されてよい。しかしながら、「結合された」という用語は、２つ以上の要素は互いに直接接触していないが互いに協働または相互作用することを意味してもよい。実施形態は、この文脈に限定されない。

【０１８５】

本明細書で使用される場合、用語「備える」、「備えている」、「含む」、「含んでいる」、「有する」、「有している」またはこれらの任意の他の変形は、非排他的包含を含むことが意図されている。たとえば、要素のリストを含むプロセス、方法、物品、または装置は、必ずしもそれらの要素のみに限定されず、明示的に挙げられない、またはそのようなプロセス、方法、物品、もしくは装置に固有である他の要素を含んでよい。さらに、逆に明示されていない限り、「または」は包含的論理和を指し、排他的論理和を指すものではない。たとえば、条件ＡまたはＢは、Ａが真であり（または存在し）Ｂが偽である（または存在しない）、Ａが偽であり（または存在せず）Ｂが真である（または存在する）、およびＡとＢの両方が真である（または存在する）のうちのいずれか１つによって満足される。

【０１８６】

また、本明細書の実施形態の要素およびコンポーネントを説明するために「ａ」または「ａｎ」の使用が採用される。これは、単に便宜のため、および請求される発明の一般的な意味を与えるために行われる。この説明は、１つまたは少なくとも１つを含むように読まれるべきであり、単数形は、それが別様に意味されることが明らかでない限り複数形も含む。

【０１８７】

当業者は、本開示を読めば、本明細書の開示された原理を通じてマルウェアを検出するためのシステムおよびプロセスに関するさらに追加の代替的構造および機能設計を理解するであろう。したがって、特定の実施形態および用途が図示および説明されているが、開示された実施形態は、本明細書に開示された正確な構成およびコンポーネントに限定されないことは理解されたい。本明細書に開示された方法および装置の配置、動作、および詳細において、当業者に明らかとなる様々な修正、変更、および変形が、添付の特許請求の範囲に規定された趣旨および範囲から逸脱することなく行われてよい。

【図１】

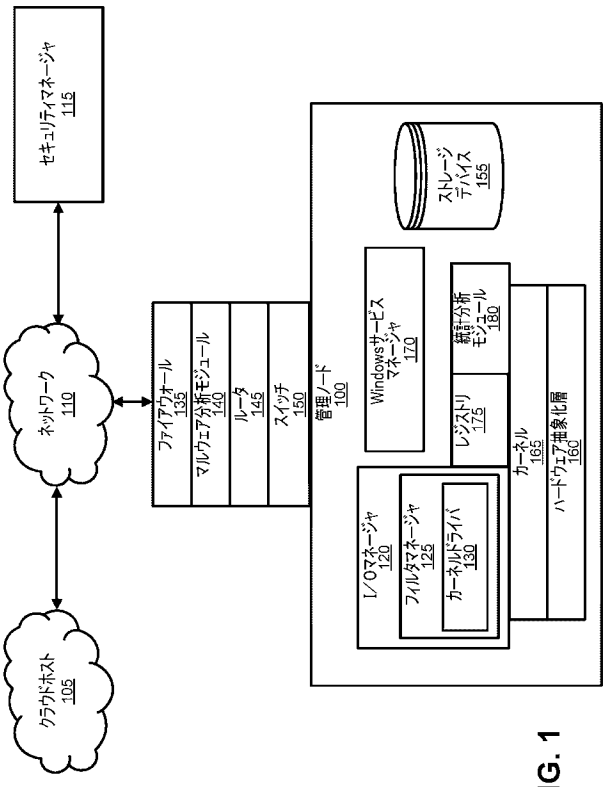

FIG. 1

【図２】

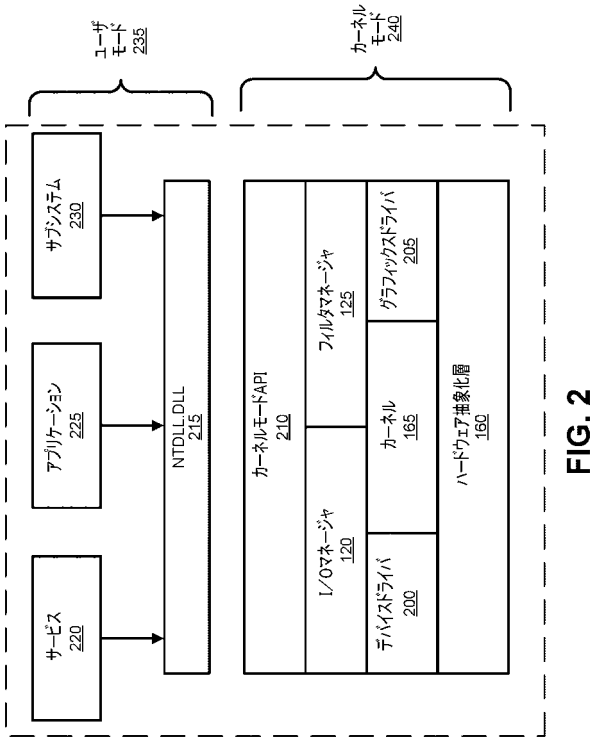

FIG. 2

【図３】

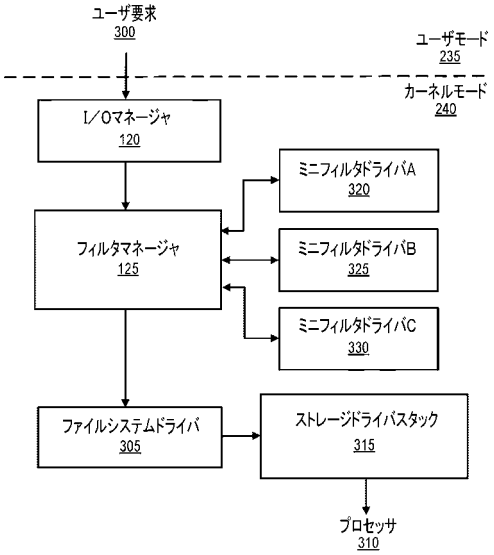

FIG. 3

【図４】

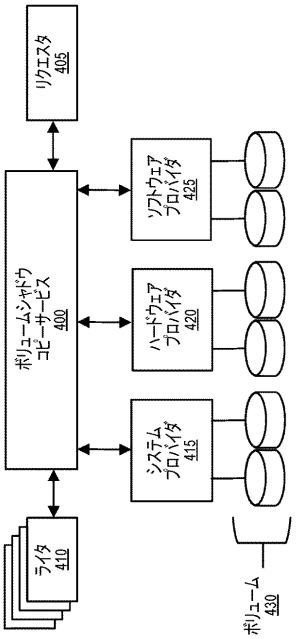

FIG. 4

【図５】

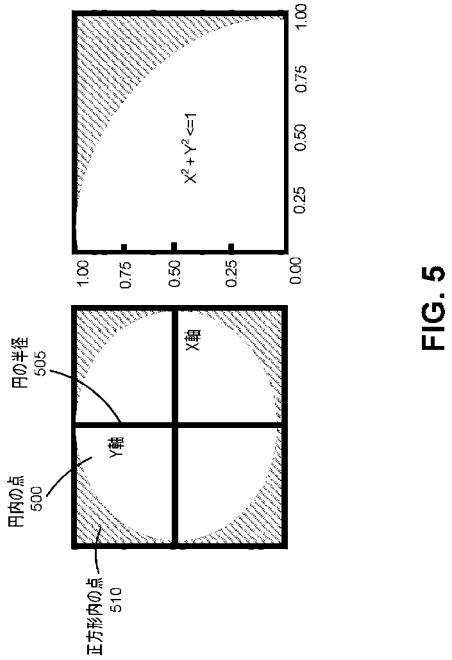

FIG. 5

【図６】

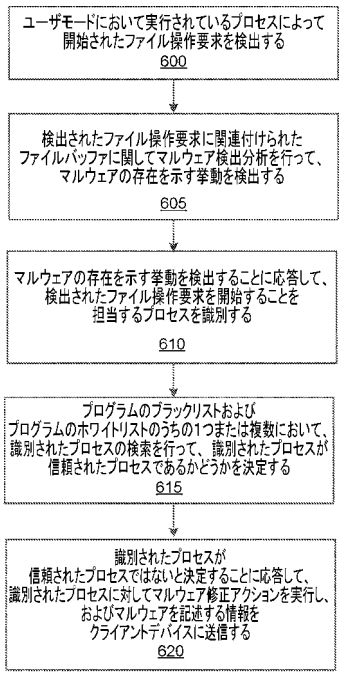

FIG. 6

【図７】

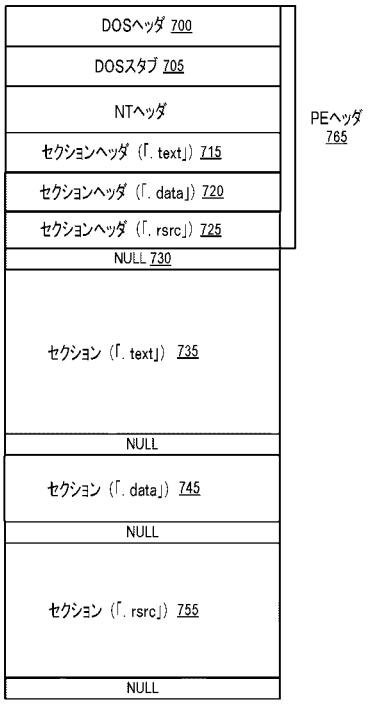

FIG. 7

【図８】

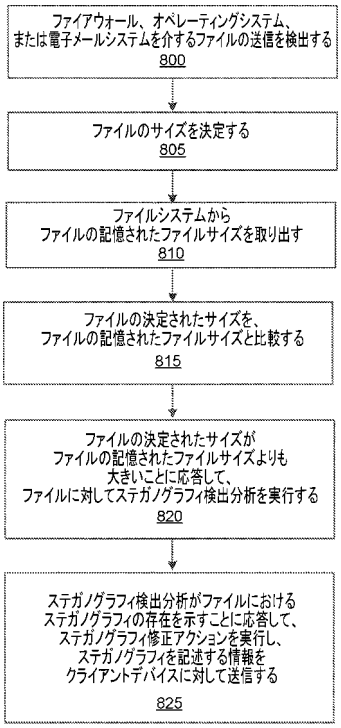

FIG. 8

【図９】

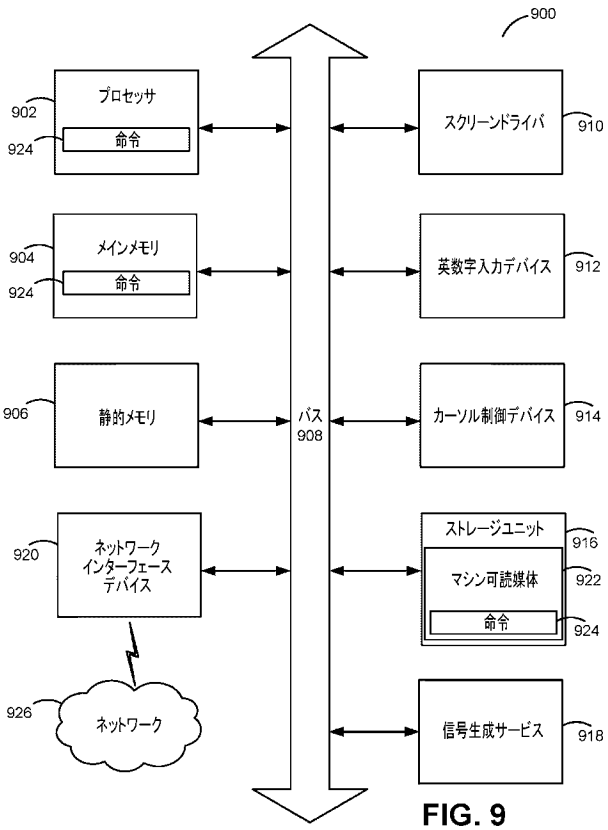

FIG. 9

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US18/35205

A. CLASSIFICATION OF SUBJECT MATTER
IPC - G06F 21/56 (2018.01)
CPC - G06F 21/566; H04L 63/145, 63/1425

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
See Search History document

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
See Search History document

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015/0172300 A1 (HOPLITE INDUSTRIES, INC.) 18 June 2015; paragraphs [0051], [0056], [0061], [0077], [0080], [0115], [0117], [0120], [0136], [0137], [0144]	1, 2, 4, 5, 7-12, 14, 15, 17-20
---		---
Y		3, 6, 13, 16
Y	US 2011/0209219 A1 (ZEITLIN, E et al.) 25 August 2011; paragraphs [0017], [0026], [0029]	3, 6, 13, 16
A	US 2009/0044024 A1 (OBERHEIDE, J et al.) 12 February 2009; entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 July 2018 (23.07.2018)	20 SEP 2018
Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US18/35205

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
See extra sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-20

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US18/35205

-***-Continued from Box No. III Observations where unity of invention is lacking-***-

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fee must be paid.

Group I: Claims 1-20 are directed towards a method to determine whether an identified process is a trusted process by searching a blacklist or whitelist.
Group II: Claim 21-40 are directed towards a method and system for comparing file sizes.

The inventions listed as Groups I and II do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons:

The special technical features of Group I include at least performing malware detection analytics on a file buffer; and performing a search for an identified process on one or more of a blacklist of programs and a whitelist of programs to determine whether the identified process is a trusted process, which are not present in Group II.

The special technical features of Group II include at least determining a size of the file; and retrieving a stored filesize of the file; and comparing the determined size of the file to the stored filesize of the file, which are not present in Group I.

The common technical features shared by Groups I and II are a method and non-transitory computer readable medium storing instructions that when executed by at least one processor, cause the at least one processor to execute instructions for: real-time detection of and protection from malware in a kernel mode; detecting an operation associated with a file; performing malware detection analytics on a file based on the operation associated with the file to detect behavior indicating presence of malware; and responsive to detecting the behavior indicating the presence of the malware, executing a malware remediation action, and transmitting information describing the malware to a client device.

However, these common features are previously disclosed by US 2015/0244679 A1 to CROWDSTRIKE, INC. (hereinafter "Crowdstrike"). Crowdstrike discloses a method and non-transitory computer readable medium storing instructions that when executed by at least one processor, cause the at least one processor to execute instructions (processor uses instructions in memory to implement kernel-level security; Fig. 1 and paragraph [0018]) for: real-time detection of and protection from malware in a kernel mode (interactions between the kernel-level security agent and the security service cloud enable a detection loop that defeats the malware update loop of malware developers and further enable the kernel-level security agent to perform updating while continuously (real-time) monitoring, eliminating (protection) dangerous gaps in security coverage; paragraph [0013]), comprising: detecting an operation associated with a file (kernel-level security agent components receive notifications of interesting events, such as file writes, from host operating system hooks or filter drivers; paragraph [0014]); performing malware detection analytics on a file based on the operation associated with the file to detect behavior indicating presence of malware (the security service cloud receives notifications of observed file write events from the kernel-level security agent, performs analysis of data associated with those events, and may determine that an interesting event is associated with malicious code; paragraphs [0013], [0014], [0030]); and responsive to detecting the behavior indicating the presence of the malware, executing a malware remediation action (the analysis module may determine that an interesting event may be associated with malicious code, and, in response, may invoke the healing module to perform healing of the computing devices associated with the interesting event; paragraph [0030]), and transmitting information describing the malware to a client device (the analysis module may determine that an interesting event may be associated with malicious code, and, in response, may provide the event and information about the associated malicious code to the computing device, e.g., for diagnostic or healing purposes; paragraphs [0030], [0033]).

Since the common technical features are previously disclosed by the Crowdstrike reference, these common features are not special and so Groups I and II lack unity.

フロントページの続き

(81)指定国・地域　AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT

（特許庁注：以下のものは登録商標）
１．ＷＩＮＤＯＷＳ

(72)発明者　ロバート　パイク
アメリカ合衆国　９８２９０　ワシントン州　スノホミッシュ　シダー　アベニュー　１１０　スイート　１０３　サイエンプティブ　テクノロジーズ　インコーポレイテッド内