【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成26年6月5日(2014.6.5)

【公表番号】特表2013-529335(P2013-529335A)
【公表日】平成25年7月18日(2013.7.18)
【年通号数】公開・登録公報2013-038
【出願番号】特願2013-508131(P2013-508131)
【国際特許分類】
Ｇ０６Ｆ　21/56　　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/00　　１５６Ｇ

【手続補正書】
【提出日】平成26年4月16日(2014.4.16)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
悪意のあるソフトウェア（マルウェア）を検出するために行動シグネチャを生成するコンピュータ実装方法であって、
コンピュータを使用して、マルウェアデータセットにマルウェアのマルウェア挙動トレースを収集する工程であり、前記マルウェア挙動トレースは、前記マルウェアによって実行された連続挙動について説明する、工程と、
コンピュータを使用して、グッドウェアデータセットにグッドウェアのグッドウェア挙動トレースを収集する工程であり、前記グッドウェア挙動トレースは、前記グッドウェアによって実行された連続挙動について説明する、工程と、
前記マルウェアに対する前記マルウェア挙動トレースを正規化してマルウェア挙動シーケンスを生成する工程と、
前記グッドウェアに対する前記グッドウェア挙動トレースを正規化してグッドウェア挙動シーケンスを生成する工程と、
同様のマルウェア挙動シーケンス及びグッドウェア挙動シーケンスをクラスタにまとめてクラスタリングする工程であり、前記クラスタ内の前記マルウェア挙動シーケンスは、マルウェアファミリの挙動について説明する、工程と、
前記クラスタを分析して前記マルウェアファミリのみに共通の挙動サブシーケンスを特定する工程と、
前記マルウェアファミリのみに共通の前記挙動サブシーケンスを使用して前記マルウェアファミリに対する行動シグネチャを作成する工程と
を含む、方法。
【請求項２】
前記行動シグネチャを作成する工程の後に、
新しいマルウェアの挙動トレースを収集する工程であって、前記新しいマルウェアは、以前は前記マルウェアデータセットのメンバーではない、工程と、
前記新しいマルウェアに対する前記挙動トレースを正規化して前記新しいマルウェアに対する挙動シーケンスを生成する工程と、
前記新しいマルウェアに対する前記挙動シーケンスがマルウェア挙動シーケンス及びグッドウェア挙動シーケンスのクラスタと整合するかどうか判断する工程と、

前記クラスタと整合する前記新しいマルウェアに対する前記挙動シーケンスに応じて、前記クラスタを分析して、前記クラスタ内の前記マルウェア挙動シーケンスおよび前記新しいマルウェアに対する前記挙動シーケンスのみに共通の新しい挙動サブシーケンスを特定する工程と、
前記新しい挙動サブシーケンスを使用して前記マルウェアファミリに対する新しい行動シグネチャを作成する工程と
をさらに含む、請求項１に記載の方法。
【請求項３】
前記マルウェア挙動トレース及びグッドウェア挙動トレースは、実行されたアプリケーションプログラミングインターフェース（ＡＰＩ）呼び出しについて説明する、請求項１に記載の方法。
【請求項４】
前記マルウェアに対する前記挙動トレースを正規化してマルウェア挙動シーケンスを生成する工程は、
マルウェア挙動トレース内の関連連続挙動をまとめて分類してオペレーションを形成する工程を含み、マルウェア挙動シーケンスは、１つまたは複数の連続挙動および１つまたは複数のオペレーションを含む、請求項１に記載の方法。
【請求項５】
同様のマルウェア挙動シーケンス及びグッドウェア挙動シーケンスをクラスタにまとめてクラスタリングする工程は、
前記マルウェア挙動シーケンス及びグッドウェア挙動シーケンスの間で編集距離を決定する工程と、
前記決定された編集距離に応じて前記マルウェア挙動シーケンス及びグッドウェア挙動シーケンスをクラスタリングする工程と
を含む、請求項１に記載の方法。
【請求項６】
前記クラスタを分析して前記マルウェアファミリのみに共通の挙動サブシーケンスを特定する工程は、
前記クラスタ内の前記マルウェア挙動シーケンスのみに共通の複数の候補サブシーケンスを特定する工程と、
前記マルウェア挙動シーケンス内のどこで前記候補サブシーケンスが現れるかを特定する工程と、
前記マルウェア挙動シーケンス内のどこで前記候補サブシーケンスが現れるかに応じて、前記候補サブシーケンスの中から前記挙動サブシーケンスを選択する工程と
を含む、請求項１に記載の方法。
【請求項７】
前記マルウェア挙動シーケンス内のどこで前記候補サブシーケンスが現れるかに応じて、前記候補サブシーケンスの中から前記挙動サブシーケンスを選択する工程は、
他の候補サブシーケンスより早期に前記マルウェア挙動シーケンスに現れた前記挙動サブシーケンスに応じて前記挙動サブシーケンスを選択する工程を含む、請求項６に記載の方法。
【請求項８】
クライアントのセキュリティモジュールに前記行動シグネチャを分配する工程をさらに含み、前記セキュリティモジュールは、前記行動シグネチャを使用して前記クライアント側に存在するマルウェアを検出するよう適合される、請求項１に記載の方法。
【請求項９】
悪意のあるソフトウェア（マルウェア）を検出するために行動シグネチャを生成するコンピュータシステムであって、
マルウェアデータセットにマルウェアのマルウェア挙動トレースを収集する工程であり、前記マルウェア挙動トレースは、前記マルウェアによって実行された連続挙動につい

て説明する、工程と、
グッドウェアデータセットにグッドウェアのグッドウェア挙動トレースを収集する工程であり、前記グッドウェア挙動トレースは、前記グッドウェアによって実行された連続挙動について説明する、工程と、
前記マルウェアに対する前記マルウェア挙動トレースを正規化してマルウェア挙動シーケンスを生成する工程と、
前記グッドウェアに対する前記グッドウェア挙動トレースを正規化してグッドウェア挙動シーケンスを生成する工程と、
同様のマルウェア挙動シーケンス及びグッドウェア挙動シーケンスをクラスタにまとめてクラスタリングする工程であり、前記クラスタ内の前記マルウェア挙動シーケンスは、マルウェアファミリの挙動について説明する、工程と、
前記クラスタを分析して前記マルウェアファミリのみに共通の挙動サブシーケンスを特定する工程と、
前記マルウェアファミリのみに共通の前記挙動サブシーケンスを使用して前記マルウェアファミリに対する行動シグネチャを作成する工程と
を含む工程を実行するために実行可能なコンピュータプログラムモジュールを格納する非一時的なコンピュータ可読記憶媒体と、
前記コンピュータプログラムモジュールを実行するためのコンピュータプロセッサと
を備える、コンピュータシステム。
【請求項１０】
前記工程は、
前記行動シグネチャを作成する工程の後に、
新しいマルウェアの挙動トレースを収集する工程であって、前記新しいマルウェアは、以前は前記マルウェアデータセットのメンバーではない、工程と、
前記新しいマルウェアに対する前記挙動トレースを正規化して前記新しいマルウェアに対する挙動シーケンスを生成する工程と、
前記新しいマルウェアに対する前記挙動シーケンスがマルウェア挙動シーケンス及びグッドウェア挙動シーケンスのクラスタと整合するかどうか判断する工程と、
前記クラスタと整合する前記新しいマルウェアに対する前記挙動シーケンスに応じて、前記クラスタを分析して、前記クラスタ内の前記マルウェア挙動シーケンスおよび前記新しいマルウェアに対する前記挙動シーケンスのみに共通の新しい挙動サブシーケンスを特定する工程と、
前記新しい挙動サブシーケンスを使用して前記マルウェアファミリに対する新しい行動シグネチャを作成する工程と
をさらに含む、請求項９に記載のコンピュータシステム。
【請求項１１】
前記マルウェアに対する前記挙動トレースを正規化してマルウェア挙動シーケンスを生成する工程は、
マルウェア挙動トレース内の関連連続挙動をまとめて分類してオペレーションを形成する工程を含み、マルウェア挙動シーケンスは、１つまたは複数の連続挙動および１つまたは複数のオペレーションを含む、請求項９に記載のコンピュータシステム。
【請求項１２】
前記クラスタを分析して前記マルウェアファミリのみに共通の挙動サブシーケンスを特定する工程は、
前記クラスタ内の前記マルウェア挙動シーケンスのみに共通の複数の候補サブシーケンスを特定する工程と、
前記マルウェア挙動シーケンス内のどこで前記候補サブシーケンスが現れるかを特定する工程と、
前記マルウェア挙動シーケンス内のどこで前記候補サブシーケンスが現れるかに応じて、前記候補サブシーケンスの中から前記挙動サブシーケンスを選択する工程と

を含む、請求項９に記載のコンピュータシステム。
【請求項１３】
前記マルウェア挙動シーケンス内のどこで前記候補サブシーケンスが現れるかに応じて、前記候補サブシーケンスの中から前記挙動サブシーケンスを選択する工程は、
他の候補サブシーケンスより早期に前記マルウェア挙動シーケンスに現れた前記挙動サブシーケンスに応じて前記挙動サブシーケンスを選択する工程を含む、請求項１２に記載のコンピュータシステム。
【請求項１４】
悪意のあるソフトウェア（マルウェア）を検出するために行動シグネチャを生成するための実行可能なコンピュータプログラムであって、
コンピュータに、
マルウェアデータセットにマルウェアのマルウェア挙動トレースを収集するための機能であり、前記マルウェア挙動トレースは、前記マルウェアによって実行された連続挙動について説明する、機能と、
グッドウェアデータセットにグッドウェアのグッドウェア挙動トレースを収集するための機能であり、前記グッドウェア挙動トレースは、前記グッドウェアによって実行された連続挙動について説明する、機能と、
前記マルウェアに対する前記マルウェア挙動トレースを正規化してマルウェア挙動シーケンスを生成するための機能と、
前記グッドウェアに対する前記グッドウェア挙動トレースを正規化してグッドウェア挙動シーケンスを生成するための機能と、
同様のマルウェア挙動シーケンス及びグッドウェア挙動シーケンスをクラスタにまとめてクラスタリングするための機能であり、前記クラスタ内の前記マルウェア挙動シーケンスは、マルウェアファミリの挙動について説明する、機能と、
前記クラスタを分析して前記マルウェアファミリのみに共通の挙動サブシーケンスを特定するための機能と、
前記マルウェアファミリのみに共通の前記挙動サブシーケンスを使用して前記マルウェアファミリに対する行動シグネチャを作成するための機能と
を実現させる、コンピュータプログラム。
【請求項１５】
前記行動シグネチャの作成の後に、
新しいマルウェアの挙動トレースを収集するための機能であって、前記新しいマルウェアは、以前は前記マルウェアデータセットのメンバーではない、機能と、
前記新しいマルウェアに対する前記挙動トレースを正規化して前記新しいマルウェアに対する挙動シーケンスを生成するための機能と、
前記新しいマルウェアに対する前記挙動シーケンスがマルウェア挙動シーケンス及びグッドウェア挙動シーケンスのクラスタと整合するかどうか判断するための機能と、
前記クラスタと整合する前記新しいマルウェアに対する前記挙動シーケンスに応じて、前記クラスタを分析して、前記クラスタ内の前記マルウェア挙動シーケンスおよび前記新しいマルウェアに対する前記挙動シーケンスのみに共通の新しい挙動サブシーケンスを特定するための機能と、
前記新しい挙動サブシーケンスを使用して前記マルウェアファミリに対する新しい行動シグネチャを作成するための機能と
をさらに実現させる、請求項１４に記載のコンピュータプログラム。
【請求項１６】
前記マルウェアに対する前記挙動トレースを正規化してマルウェア挙動シーケンスを生成する機能は、
マルウェア挙動トレース内の関連連続挙動をまとめて分類してオペレーションを形成する機能を含み、マルウェア挙動シーケンスは、１つまたは複数の連続挙動および１つまたは複数のオペレーションを含む、請求項１４に記載のコンピュータプログラム。

【請求項１７】
前記クラスタを分析して前記マルウェアファミリのみに共通の挙動サブシーケンスを特定する機能は、
前記クラスタ内の前記マルウェア挙動シーケンスのみに共通の複数の候補サブシーケンスを特定する機能と、
前記マルウェア挙動シーケンス内のどこで前記候補サブシーケンスが現れるかを特定する機能と、
前記マルウェア挙動シーケンス内のどこで前記候補サブシーケンスが現れるかに応じて、前記候補サブシーケンスの中から前記挙動サブシーケンスを選択する機能と
を含む、請求項１４に記載のコンピュータプログラム。
【請求項１８】
コンピュータを使用して、前記マルウェア挙動トレースを収集する工程は、
仮想コンピューティング環境で前記マルウェアの実行をエミュレートする工程と、
前記マルウェアによって行われる、オペレーティングシステムへのアプリケーションプログラミングインターフェース（ＡＰＩ）呼び出しのシーケンスを記録するために、エミュレートされた前記マルウェアの実行をモニタする工程と、
を含む、請求項１に記載の方法。
【請求項１９】
前記マルウェア挙動トレースを収集する工程は、
仮想コンピューティング環境で前記マルウェアの実行をエミュレートする工程と、
前記マルウェアによって行われる、オペレーティングシステムへのアプリケーションプログラミングインターフェース（ＡＰＩ）呼び出しのシーケンスを記録するために、エミュレートされた前記マルウェアの実行をモニタする工程と、
を含む、請求項９に記載のコンピュータシステム。
【請求項２０】
前記マルウェア挙動トレースを収集する機能は、
仮想コンピューティング環境で前記マルウェアの実行をエミュレートする機能と、
前記マルウェアによって行われる、オペレーティングシステムへのアプリケーションプログラミングインターフェース（ＡＰＩ）呼び出しのシーケンスを記録するために、エミュレートされた前記マルウェアの実行をモニタする機能と、
を含む、請求項１４に記載のコンピュータプログラム。