【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18年8月3日(2006.8.3)

【公表番号】特表2005-534092(P2005-534092A)
【公表日】平成17年11月10日(2005.11.10)
【年通号数】公開・登録公報2005-044
【出願番号】特願2004-522314(P2004-522314)
【国際特許分類】
Ｇ０６Ｆ　21/22　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　9/06　　６６０Ｎ

【手続補正書】
【提出日】平成18年6月6日(2006.6.6)
【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】
プログラムの潜在的にワームの挙動を自動的に決定する方法であって、
ネットワークの動作をエミュレートしない環境で前記プログラムの挙動プロファイルを決定すること、
ワームの挙動を示すプロファイルに対して前記決定された挙動プロファイルを比較すること、および、
前記比較の結果に基づいて潜在的にワームの挙動の表示を提供すること
を含み、
前記挙動プロファイルを前記決定するステップが、
少なくとも１つの既知の非ネットワーク環境で前記プログラムを実行すること、
前記環境を検査する自動化された方法を使用し、前記環境内で発生した変化がある場合に、前記変化を決定すること、および、
前記挙動プロファイルとして、すべての決定された変化を記録すること
を含む方法。
【請求項２】
前記既知の非ネットワーク環境が、ネットワーク関連機能を示すように見える能力を有する、請求項１に記載の方法。
【請求項３】
前記プログラムが前記環境がネットワーク機能を有するかどうか判定しようとすることに応答して、前記プログラムがワームの挙動を示す誘因として前記プログラムにネットワーク・アドレスを提供する、請求項１に記載の方法。
【請求項４】
前記既知の非ネットワーク環境が、存在しないローカル・ネットワーク関連リソースおよびローカル・ネットワーク関連オブジェクトの少なくとも１つを示す、請求項１に記載の方法。
【請求項５】
前記プログラムがファイルに関する情報を決定しようとすることに応答して、前記プログラムがワームの挙動を示す誘因として、前記ファイルが存在するかのように応答する、請求項１に記載の方法。

【請求項６】
前記プログラムがファイルに関する情報を決定しようとすることに応答して、前記プログラムがワームの挙動を示す誘因として、前記ファイルを返す前に前記ファイルを作成する、請求項１に記載の方法。
【請求項７】
前記プログラムが電子メール・プログラムに関する情報を決定しようとすることに応答して、前記プログラムがワームの挙動を示す誘因として、前記プログラムに前記情報を返す、請求項１に記載の方法。
【請求項８】
前記プログラムが電子メール・アドレス帳に関する情報を決定しようとすることに応答して、前記プログラムがワームの挙動を示す誘因として、前記プログラムに前記情報を返す、請求項１に記載の方法。
【請求項９】
プログラムの潜在的にワームの挙動の自動決定を行う記憶されたプログラムを実行する少なくとも１つのコンピュータを含むデータ処理システムであって、
ネットワークの動作をエミュレートしない環境で前記プログラムの挙動プロファイルを決定する手段と、
ワームの挙動を示す記憶されたプロファイルに対して前記決定された挙動プロファイルを比較する手段と、
前記比較の結果に基づいて潜在的にワームの挙動の表示を提供する手段と
を含み、前記挙動プロファイルを決定する手段が、
少なくとも１つの既知の非ネットワーク環境で前記プログラムを実行する手段と、
前記環境を検査する自動化方法を使用し、前記環境内で発生した変化がある場合に前記変化を決定する手段と、
前記挙動プロファイルとしてすべての決定された変化を記録する手段と
を含むデータ処理システム。
【請求項１０】
不揮発性メモリ・ストレージ・デバイスを有するデータ処理システムで実行されたとき、請求項１ないし８のいずれかに記載の方法を前記システムに実行させる命令を含むコンピュータ・プログラム製品。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００８
【補正方法】変更
【補正の内容】
【０００８】
第１の態様では、方法は、ネットワークの動作をエミュレートしない環境でプログラムの挙動プロファイルを決定すること、決定された挙動プロファイルをワームのような挙動を示すプロファイルと比較すること、および、比較の結果に基づいて潜在的なワームのような挙動の表示を提供することを含む。挙動プロファイルを決定するステップは、プログラムを少なくとも１つの既知の非ネットワーク環境で実行すること、環境を検査するのに自動化された方法を使用し、環境で起こった変化がある場合に前記変化を決定すること、および、前記挙動プロファイルとしてすべての決定された変化を記録することを含む。このようにして、観察された挙動のログ記録されたレコードを分析して、挙動がワームのような特性を有するプログラムを表すかどうか判定する。非ネットワーク環境は、ネットワークの実際の動作をエミュレートせずに、プログラムへのネットワークの外見をシミュレートすることができる。