【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25年5月23日(2013.5.23)

【公表番号】特表2012-501504(P2012-501504A)
【公表日】平成24年1月19日(2012.1.19)
【年通号数】公開・登録公報2012-003
【出願番号】特願2011-525271(P2011-525271)
【国際特許分類】
Ｇ０６Ｆ　21/56　　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　9/06　　６６０Ｎ

【手続補正書】
【提出日】平成24年3月21日(2012.3.21)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】０００２
【補正方法】変更
【補正の内容】
【０００２】
バイナリファイルは、しばしば多くのコンピューティング装置間で転送される。バイナリファイルを受け取るコンピューティング装置は、普通はファイルの発信元（出所）についてまたはそれが受け取るコードが安全かどうかを認識していない。コンピューティング装置の安全を確認するため、バイナリファイルを分解してマルウェア（例えば、ウイルス、ワーム、トロイの木馬、および／または同類のもの）が含まれていないかを見極めることができる。
一般的に、逆アセンブラは、バイナリファイルをマシン語からアセンブリ言語に変換する。いくつかの逆アセンブラは双方向性であり、専門のプログラマが注釈、修正、説明、または前記逆アセンブラがファイルをどのように解析するかの決定を行うことができる。例えば、逆アセンブラは、コードの新規機能または特別なセクションが現れたら信号を送ることができる。識別された動作が起こった場合、前記コードの特定のセクションは、後の参照用のためにラベル付けされる。しかしながら、既知の実行形式の解析は、通常、特別に訓練を受けた人員によって手動で、または統計的方法で自動的に実行される、時間のかかるプロセスであることがある。
この出願の発明に関連する先行技術文献情報としては、以下のものがある（国際出願日以降国際段階で引用された文献及び他国に国内移行した際に引用された文献を含む）。
【先行技術文献】
【特許文献】
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００３
【補正方法】変更
【補正の内容】
【０００３】
【特許文献１】　米国特許出願公開第２００８／０００５７９６号明細書
【特許文献２】　米国特許出願公開第２００８／０２０１７７９号明細書
【特許文献３】　米国特許出願公開第２００５／００８６５２６号明細書
【特許文献４】　米国特許出願公開第２００６／００７５５０４号明細書
【発明の概要】

【課題を解決するための手段】