(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6516870号
(P6516870)
(45)発行日　令和1年5月22日(2019.5.22)　(24)登録日　平成31年4月26日(2019.4.26)

(51)Int.Cl.　　F I
G06F 21/12 (2013.01)　　G06F 21/12 310
G06F 9/445 (2018.01)　　G06F 9/445

請求項の数 13　(全 16 頁)

(21)出願番号　特願2017-556821(P2017-556821)
(86)(22)出願日　平成29年1月25日(2017.1.25)
(65)公表番号　特表2018-525697(P2018-525697A)
(43)公表日　平成30年9月6日(2018.9.6)
(86)国際出願番号　PCT/EP2017/051476
(87)国際公開番号　WO2017/137256
(87)国際公開日　平成29年8月17日(2017.8.17)
審査請求日　平成30年2月9日(2018.2.9)
(31)優先権主張番号　102016201898.1
(32)優先日　平成28年2月9日(2016.2.9)
(33)優先権主張国　ドイツ(DE)

早期審査対象出願

(73)特許権者　517291346
シーメンス　アクチエンゲゼルシヤフト
Ｓｉｅｍｅｎｓ　Ａｋｔｉｅｎｇｅｓｅｌｌｓｃｈａｆｔ
ドイツ連邦共和国　Ｄ－８０３３３　ミュンヘン　ヴェアナー－フォン－シーメンス－シュトラーセ　１
Ｗｅｒｎｅｒ－ｖｏｎ－Ｓｉｅｍｅｎｓ－Ｓｔｒ．　１，　Ｄ－８０３３３　Ｍｕｅｎｃｈｅｎ，　Ｇｅｒｍａｎｙ
(74)代理人　100075166
弁理士　山口　巖
(74)代理人　100133167
弁理士　山本　浩

最終頁に続く

(54)【発明の名称】プログラム命令を安全に実行する方法及び該方法用プログラム

(57)【特許請求の範囲】
【請求項１】
コンピュータ支援によりアプリケーションのプログラム命令を安全に実行する方法であって、
製造者側において実行環境の学習モードを起動し、該起動した学習モードの間に前記実行環境においてアプリケーションを実行する第１の学習フェーズであって、選択されて予定されているアプリケーションシナリオに関してアプリケーションのプログラム命令を実行し、前記実行環境が、実行された該プログラム命令にアプリケーションシナリオ特有の第１の妥当性情報を割り当てる第１の学習フェーズと、
使用者側において前記実行環境の学習モードを起動し、該起動した学習モードの間に前記実行環境においてアプリケーションを実行する第２の学習フェーズであって、選択されて予定されているアプリケーションシナリオに関してアプリケーションのプログラム命令を実行し、前記実行環境が、実行された該プログラム命令にアプリケーションシナリオ特有の第２の妥当性情報を割り当てる第２の学習フェーズと、
前記実行環境の作業モードを起動する過程であって、該作業モードにおいて前記実行環境がプログラム命令の第１及び第２の前記妥当性情報をチェックし、プログラム命令の第１及び第２の前記妥当性情報に応じて前記実行環境がプログラム命令を実行する過程とを含む方法。
【請求項２】
前記実行されたプログラム命令が、アプリケーションの通過した実行経路に割り当てら

れ、該実行経路のそれぞれにアプリケーションシナリオ特有の第３の妥当性情報が割り当てられる、請求項１に記載の方法。
【請求項３】
前記実行環境として、プロセッサ、仮想マシン、オペレーティングシステムカーネル、及びメモリ管理ユニットを利用するオペレーティングシステムカーネルの１つ以上が使用される、請求項１又は２に記載の方法。
【請求項４】
トリガーによって、プログラム命令の前記妥当性情報の１つ以上が消去される、請求項１～３のいずれか１項に記載の方法。
【請求項５】
前記妥当性情報の１つ以上が安全保護されて記憶される、請求項１～４のいずれか１項に記載の方法。
【請求項６】
前記学習モードの起動が安全機構によって保護されている、請求項１～５のいずれか１項に記載の方法。
【請求項７】
前記妥当性情報の１つ以上が他の機器に提供される、請求項１～６のいずれか１項に記載の方法。
【請求項８】
少なくとも前記第１の学習フェーズを、機器、構造的に同じ試験機器、及び前記機器のシミュレーション環境の１つ以上で行う、請求項１～７のいずれか１項に記載の方法。
【請求項９】
前記妥当性情報の１つ以上を、プログラム命令に対し、命令ごとに、サブルーチンごとに、又はライブラリごとに、あるいはこれらの組み合わせで、割り当てる、請求項１～８のいずれか１項に記載の方法。
【請求項１０】
前記妥当性情報の１つ以上を有するプログラム命令に従属するプログラム命令に、該当する妥当性情報が割り当てられる、請求項１～９のいずれか１項に記載の方法。
【請求項１１】
前記妥当性情報のないプログラム命令を実行する際に報知情報を発する、請求項１～１０のいずれか１項に記載の方法。
【請求項１２】
前記作業モードの起動時に、前記妥当性情報のないプログラム命令がアプリケーションから取り除かれる、請求項１～１０のいずれか１項に記載の方法。
【請求項１３】
請求項１～１２のいずれか１項に記載の方法を実行するプログラム命令を含んだコンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、アプリケーションのプログラム命令を安全に実行するための方法及び実行環境に関する。
【背景技術】
【０００２】
現代の自動化システムでは、ＩＴシステム及びアプリケーション（ソフトウェア）が制御のために使用される。デジタル化の過程で、高度に分化した個別ソリューションが、包括的な多目的システムによって置き換えられている。これらの多目的システムは、（アプリケーションの）動的構成によって、各々の具体的な使用目的に適合させられる。この場合、その具体的な使用目的に使用されない機能がシステム上に残る。基本的には余分な／使用されない機能は、潜在的なリスクを意味する。当該機能は、（改ざんによって）意図

的に実行されて又は意図せずに実行されて、望ましくないシステム状態を招くことがある。その一例がＳＳＬ／ＴＬＳにおける「ハートブリード（Heartbleed）」バグであり、これは、該当するＳＳＬ／ＴＬＳライブラリの通常は必要とされない部分に長い間隠れていたバグである。それにもかかわらず、この機能は大抵のシステムにおいて提供されていて、利用されることがあり得た。

【０００３】

先行技術において、特許文献１、特許文献２、特許文献３、特許文献４、特許文献５、特許文献６、特許文献７及び特許文献８が知られている。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】米国特許：ＵＳ８，５３１，２４７Ｂ２
【特許文献２】米国特許：ＵＳ８，８９２，６１６Ｂ２
【特許文献３】米国特許：ＵＳ８，３００，８１１Ｂ２
【特許文献４】米国特許：ＵＳ９，１４７，０８８Ｂ２
【特許文献５】欧州特許：ＥＰ２６０５４４５Ｂ１
【特許文献６】欧州特許出願公開：ＥＰ２８７０５６５Ａ１
【特許文献７】欧州特許出願公開：ＥＰ２８９１１０２Ａ１
【特許文献８】米国特許：ＵＳ８，８４３，７６１，Ｂ２

【発明の概要】

【発明が解決しようとする課題】

【０００５】

本発明の課題は、アプリケーションのプログラム命令を安全に実行する方法及び実行環境について、より簡素に実施可能な方法及び実行環境を提供することにある。

【課題を解決するための手段】

【０００６】

上記課題は、独立形式請求項に記載された特徴によって達成される。引用形式請求項には本発明の有利な発展形態が記載されている。

【０００７】

一態様によれば、本発明は、コンピュータ支援によりアプリケーションのプログラム命令を安全に実行する、次の過程を含む方法に関する。

【０００８】

１つの過程において、実行環境の学習モードが起動される。

【０００９】

別の過程において、起動された学習モードの間に、実行環境においてアプリケーションが実行される。該アプリケーションのプログラム命令が、選択されて予定されているアプリケーションシナリオに関して実行され、実行環境は、実行されたプログラム命令に、アプリケーションシナリオ特有の第１の妥当性情報を割り当てる。

【００１０】

別の過程において、実行環境の作業モードが起動され、該作業モードにおいて実行環境がプログラム命令の第１の妥当性情報をチェックし、第１の妥当性情報に応じて実行環境がプログラム命令を実行する。

【００１１】

本願に関して、アプリケーションとは、実行可能なファイル又はプログラムライブラリの意味であり得る。

【００１２】

本願に関して、実行環境とは、仮想マシン、例えばＪａｖａ仮想マシン、プロセッサ又はオペレーティングシステム環境の意味であり得る（Javaは登録商標）。実行環境は、物理的演算処理ユニット（プロセッサ、マイクロコントローラ、ＣＰＵ、ＣＰＵコア）上で実現することができる。この場合、学習モードと作業モードにおけるアプリケーションの

実行を、同一の物理的演算処理ユニットで行うことができる。また、例えば学習モードにおけるアプリケーションの実行を、別の物理的演算処理ユニットにおいて行うこともできる。したがって、例えば学習は、専用の学習用演算処理ユニットにおいて行うことができる。作業モードでの実行は、例えば第２の演算処理ユニットにおいて行われ、学習時に確かめられた妥当性情報は、作業用（第２の）演算処理ユニットにおいて実行時に使用される。例えば、学習用演算処理ユニットによって確かめられた妥当性情報は、好ましくは改ざんに対して保護されて提供される。

【００１３】

本願に関して、プログラム命令とは、好ましくは使用されるライブラリを含む、全体として１つのアプリケーションをなすプログラム命令の意味であり得る。

【００１４】

本願に関して、実行経路とは、直接的に連続して実行可能な複数のプログラム命令からなるアプリケーション部分範囲、具体的に言えば、アプリケーションの特定の部分機能に割り当てられているアプリケーション部分範囲の意味であり得る。実行経路は、ある条件、例えば「Ｉｆ－Ｅｌｓｅ」条件に応じて実行される部分範囲であってもよい。

【００１５】

本願に関して、妥当性情報とは、第１の妥当性情報、第２の妥当性情報、及び第３の妥当性情報のいずれか又は全部の意味であり得る。

【００１６】

本願に関して、機器とは、例えば、消火システム用の制御機器、高電圧に対する電圧ピークを監視するための監視機器、又はフィールド（Field）機器の意味であり得る。

【００１７】

本願に関して、アプリケーションシナリオ又は選択されて予定されているアプリケーションシナリオとは、あるアプリケーションのための、ある特定の目的のためにのみ使用されるアプリケーションシナリオの意味であり得る。これは、例えば、発電所設備において電圧ピークを監視し、場合によっては制御に介入する制御機器（この制御機器上でアプリケーションが実行される）であり得る。この場合、制御機器が通信するハードウェアコンポーネント及びその作動環境が正確に確定されているのがよい。このことは、一例をあげると、特定の想定値範囲をもった入力値のみがアプリケーションに渡されること、そして、例えば高電圧に関して特定の電圧範囲を監視するために必要な機能又は当該機能のプログラム命令だけが使用されること、を意味し得る。低電圧用にしか使用されない機能は、高電圧用の、選択されて予定されているアプリケーションシナリオにおいて、実行もしくは使用されることはない。

【００１８】

本願に関して、「妥当性情報のない」とは、プログラム命令、サブルーチン／機能、及びプログラムライブラリのいずれか又は全部に、妥当性情報が割り当てられていないという意味であり得る。例えば、妥当性情報を格納できる所定のメモリ領域が各プログラム命令に割り当てられているならば、妥当性情報のないプログラム命令に関しては、このメモリ領域に、例えばゼロが格納されるか、又は当該プログラム命令に対して利用できる妥当性情報がないことを示すその他の値が格納される。あるいは、「妥当性情報のない」とは、プログラム命令に非妥当情報が割り当てられているという意味であってもよい。

【００１９】

本発明に係る方法によって、一例をあげると、妥当性情報のないプログラム命令の実行が抑制されるから、ある種の機器、例えばフィールド機器において実行されるアプリケーションのための高い安全性が達成される。このことは、例えば、実行されないプログラム命令が妥当性情報のないプログラム命令であり、従って妥当性情報をもっていないことを意味する。例えば、学習モードの起動前にはどのプログラム命令にも妥当性情報が割り当てられていないように、学習モードが作動する前に、存在する妥当性情報を選択的に消去するとよい。

【００２０】

作業モードの起動について、例えば、特にデジタル認証又はライセンスデータ構造の方式で、パスワード、ロック解除コード又は暗号などの安全対策により保護することも可能である。

【００２１】

例えば、作動の異なるモードも想定可能である。一例として、アプリケーションシナリオに関して実行されるプログラム命令をできるだけ完全に捉えるために、学習モードと作業モードとを並行して実行することもできる。あるいは、作業モードの起動で学習モードを自動的に終了させることも可能である。逆に、学習モードが起動された場合には、作業モードを自動的に終了とする。これは、実行環境の作動のモードの所望の挙動に従って好ましい仕様で構成される。

【００２２】

本発明に係る方法の他の態様では、第１の妥当性情報が製造者側における上述の第１の学習フェーズで割り当てられ、そして使用者側における第２の学習フェーズにおいて、実行環境が、アプリケーションシナリオ特有の第２の妥当性情報を、実行されるプログラム命令に割り当てる。

【００２３】

これによって妥当性情報の割り当てを改善することができる。例えば、アプリケーションの実行を目的とした機器の製作時に機能試験を実施する場合に、第１の学習フェーズを実行することによってこれは達成される。この後に第２の学習フェーズは、選択されて予定されているアプリケーションシナリオ、例えば給電系統における過負荷制御、を実行する該機器及びアプリケーションの使用者側で実行することができる。これにより使用者側では、妥当性情報を特定するための時間を短縮することができる。

【００２４】

本発明に係る方法の一態様では、実行されるプログラム命令が、アプリケーションの通過した実行経路に結びつけられ、アプリケーションシナリオ特有の第３の妥当性情報がそれぞれ実行経路に割り当てられる。

【００２５】

例えば「Ｉｆ－Ｅｌｓｅ」条件文の場合の実行経路にだけ妥当性情報を割り当てることによって、本発明に係る方法の実行時間を改善することができる。

【００２６】

本発明に係る方法の他の態様において、使用される実行環境は、プロセッサ、仮想マシン、及びオペレーティングシステムカーネル又はメモリ管理ユニットを用いたオペレーティングシステムカーネルのいずれか又は全部である。

【００２７】

アプリケーションによっては、これによって、例えばＪａｖａアプリケーションのバイトコードのプログラム命令に妥当性情報を割り当てる手法を通し、容易に実施できる選択肢が実現される。あるいは、プロセッサ上のマシン命令のそれぞれに妥当性情報を割り当てる手法を通し、アプリケーションの実行に対する非常に高い安全性が達成される。

【００２８】

あるいは、例えば、平均的な安全性を達成するために、アプリケーションのＣＰＵ命令（バイナリとも呼ばれる）に妥当性情報を割り当てることもできる。

【００２９】

例えば、妥当性情報を実行環境内に直接組み込むことが一般的には可能であり、このために実行環境内に専用のメモリ又はメモリ領域を設けることができる。あるいは、妥当性情報は、実行環境の外部に、例えば、好適には暗号化保護されたファイルとして保存することもできる。そして実行環境は、プログラムの実行時に、そのファイル内の妥当性情報にアクセスする。この場合、実行環境は、必要に応じて適切な暗号鍵を持つことが必要である。

【００３０】

本発明に係る方法の他の態様において、トリガーによって、プログラム命令の第１の妥

当性情報、第２の妥当性情報及び第３の妥当性情報のいずれか又は全部が消去される。

【００３１】

一例として、制御機器が、第１の電圧範囲の高電圧を監視するために使用された後で、今度は第２の電圧範囲の高電圧を監視するために使用することが意図されているという状況では、第１の電圧範囲の監視にもはや必要のない機能（又は該機能のプログラム命令）は、これ以上妥当性情報をもたないことが適切である。好ましくは安全機構、例えばパスワード又は暗号化保護された方法により保護されているトリガーによって、場合によっては妥当性情報を簡単に消去することができる。

【００３２】

本発明に係る方法の他の態様では、第１の妥当性情報、第２の妥当性情報及び第３の妥当性情報の１つ以上が安全保護（セキュリティプロテクト）されて記憶される。

【００３３】

妥当性情報は、例えば、妥当性情報を用いた対称暗号化、非対称暗号化又はデジタル署名のような暗号化方式が構築されることによって、安全保護されて記憶される。これにより妥当性情報のインテグリティ（完全性、整合性）がチェック可能である。この安全保護記憶は、妥当性情報が格納されているメモリモジュールを空間的にもアクセスできない（空間的にも保護されている）ように、アプリケーションが実行される機器、例えば高電圧を監視するための制御機器が封印可能であることによっても、達成可能である。このことは、本発明に係る方法の安全性がさらに高められるという利点を有する。

【００３４】

本発明に係る方法の他の態様では、学習モードの起動が安全機構によって保護される。

【００３５】

学習モードの起動あるいは作業モードの起動が安全機構によって保護されていることによって、本発明に係る方法のより高い安全性が達成される。安全モードは例えば暗号法により実現可能であり、又は、学習モードが予め定められた時点及び予め定められた状況のいずれか又は両方でのみ起動可能である。これは、例えばアプリケーションが実行される機器の製作中であってよい。この場合に封印可能なメモリユニットへのアクセスが存在するが、この封印可能なメモリユニットは、例えば通常動作中には（特に当該機器の使用現場での作業モードにおいては）アクセスできない。予め定められた時点は、例えばシステム試験の段階、又はその機器上でのアプリケーションのデバック作業時であってもよい。

【００３６】

本発明に係る方法の他の態様では、第１の妥当性情報、第２の妥当性情報及び第３の妥当性情報の１つ以上が他の機器に提供される。

【００３７】

これによって、できるだけ簡単なやり方で、同じアプリケーションシナリオを有するアプリケーションに対して妥当性情報を伝達することができる。発電所設備において、例えば異なる個所で同じ仕様で高電圧時の電圧ピークを監視するためにアプリケーションを有する複数の機器が使用される場合に、例えば、先ず、その１つの機器に関するプログラム命令のための妥当性情報とそれらのアプリケーションとを取得し、当該妥当性情報を、その他の機器に伝達することができる。この伝達のために、妥当性情報はこの場合も暗号により保護されていることが好ましく、該伝達は自動的に行われるのがよい。

【００３８】

本発明に係る方法の他の態様では、起動した学習モードの中の実行環境におけるアプリケーションの実行が、１つの機器、構造的に同じ試験機器、及び該機器のシミュレーション環境の１つ以上において行われる。

【００３９】

これによって妥当性情報をできるだけ簡単なやり方で取得することができる。

【００４０】

本発明に係る方法の他の態様では、第１の妥当性情報、第２の妥当性情報及び第３の妥当性情報の１つ以上が、プログラム命令に対し、少なくとも、命令ごと、サブルーチンご

と、又はライブラリごとに割り当てられる。

【００４１】

このように妥当性情報を柔軟に割り当てできることによって、例えばアプリケーションのプログラムコードにおける個々の行ごとに妥当性情報を割り当てるのではなくて、状況に応じて１つのサブルーチン／機能、又は１つのプログラムライブラリに、妥当性情報の１つを割り当てることができる。このことは、例えば、プログラム行ごとに妥当性情報を評価する必要がないことから、アプリケーションの実行時間が改善されるという利点を有する。

【００４２】

本発明に係る方法の他の態様では、第１の妥当性情報、第２の妥当性情報及び第３の妥当性情報の１つ以上を有するプログラム命令に従属するプログラム命令は、該当する妥当性情報を割り当てられる。

【００４３】

これによれば、例えばアプリケーションのプログラマによって、事前に妥当性情報を割り当てることができる。このことは、特に、１つのアプリケーションシナリオに必要な全ての妥当性情報を割り当てるための学習モードの時間を短縮することができるという利点を有する。

【００４４】

本発明に係る他の態様では、妥当性情報のないプログラム命令を実行する際に報知情報が提供される。

【００４５】

これによって、とりわけ、本来はアプリケーションシナリオにとって必要でないプログラム命令が実行される場合にこのことを認識することができる。この報知情報は、例えば制御コンソール又は安全監視システムに伝送することができるので、技術者は、例えば発電所設備において、アプリケーション及びそのアプリケーションがインストールされている機器をチェックすることができる。その結果、特に、アプリケーション、機器、又は該機器の作業環境の改ざんを認識することができる。この報知情報は、例えば、妥当性情報のないプログラム命令に対し記憶されている割込み又は例外によって発生させることができる。

【００４６】

本発明に係る方法の他の態様では、作業モードの起動時に妥当性情報のないプログラム命令がアプリケーションから取り除かれる。

【００４７】

これによって、該当アプリケーションから不要なプログラム命令が、あるいはプログラムコードも、取り除かれるので、アプリケーションの安全性が高められる。したがって、アプリケーションシナリオに使用されていないプログラム部分を攻撃者が利用できる可能性はない。

【００４８】

他の態様によれば、本発明は、コンピュータ支援によりアプリケーションのプログラム命令を安全に実行するための実行環境に関する。当該実行環境は、実行環境の学習モードを起動するための第１のスイッチングモジュールを含む。実行環境は、さらに、起動した学習モードの間に実行環境においてアプリケーションを実行するための実行モジュールを含み、アプリケーションのプログラム命令を、選択されて予定されているアプリケーションシナリオに関して実行し、実行環境が、アプリケーションシナリオ特有の第１の妥当性情報を、実行されたプログラム命令に割り当てる。実行環境は、さらに、実行環境の作業モードを起動するための第２のスイッチングモジュールを含み、作業モードにおいて実行環境がプログラム命令の第１の妥当性情報をチェックし、実行環境がプログラム命令を該プログラム命令の妥当性情報に応じて実行する。

【００４９】

第１のスイッチングモジュール及び第２のスイッチングモジュールは、例えば、学習モ

ード又は作業モードをそれぞれ起動させる集積型スイッチングモジュールとすることができる。

【００５０】

本発明に係る実行環境の第１の態様では、当該実行環境は、プロセッサ、仮想マシン、オペレーティングシステムカーネル、又はメモリ管理ユニットを使用するオペレーティングシステムカーネルである。

【００５１】

他の態様によれば、本発明は、本発明に係る実行環境を有するシステムに関する。

【００５２】

さらに、本発明は、本発明に係る方法を実行するプログラム命令を含んだコンピュータプログラムに関する。

【００５３】

さらに、本発明は、作成機器、例えば３次元プリンタや類似の機器を構成するプログラム命令を含んだコンピュータプログラムの一変形例に関する。該作成機器は、上述の本発明に係る実行環境がつくられるように、プログラム命令を用いて構成される。

【００５４】

さらに、本発明は、コンピュータプログラムを記憶するか提供する、あるいは記憶し提供する、提供装置に関する。該提供装置は、例えば、コンピュータプログラムを記憶するか提供する、あるいは記憶し提供する、データ媒体である。これに替えて又はこれに追加して、提供装置は、例えば、コンピュータプログラムを例えばデータストリームとして記憶する又は提供する、あるいは記憶し提供する、ネットワークサービス、コンピュータシステム、サーバシステム、特に分散コンピュータシステム、クラウドベースのコンピュータシステム、及び仮想コンピュータシステムの少なくともいずれかである。

【００５５】

当該提供は、例えば、コンピュータプログラム完成品のプログラムデータブロック又は命令データブロック、あるいはその両方の形式でのダウンロードとして、好ましくはファイル、特にダウンロードファイルとして、又はデータストリーム、特にダウンロードデータストリームとして、行われる。この提供は、例えば、複数の部分からなり、ピアツーピアネットワークを介してダウンロードされるか、又はデータストリームとして提供される、部分ダウンロードとして行われてもよい。このようなコンピュータプログラムは、例えばデータ媒体形式の提供装置を用いることによりシステム内に読み込まれ、プログラム命令の実行により、本発明に係る方法がコンピュータで実行されるか、又は本発明に係る実行環境をつくるように作成機器が構成される。

【００５６】

本発明の上述の特性、特徴及び利点ならびにこれらを達成する方法について、次の図面を参照して以下に説明する実施形態に基づいて、明らかにする。

【図面の簡単な説明】

【００５７】

【図１】本発明に係る方法の第１実施形態をフローチャートで概略的に示す。

【図２】本発明に係る方法の第２実施形態を具体的に示す。

【図３】本発明に係る方法の第３実施形態を具体的に示す。

【図４】第４実施形態に係る実行環境を示す。

【図５】実行環境を有するシステムを示す。

【発明を実施するための形態】

【００５８】

図面において、異なるものとして示していない限り、機能的に同じ要素には同じ符号を付してある。

【００５９】

以下の説明は、全ての実施形態に関係する。

【００６０】

図１は、本発明に係る方法１００の第１実施形態のフローチャートを示す。この方法１００は、コンピュータ又は機器、例えば消火システム用の制御機器、高電圧時に電圧ピークを監視するための監視機器、又はフィールド機器において、アプリケーションのプログラム命令を安全に実行するのに適している。

【００６１】

この場合、方法１００は、実行環境の学習モードを起動する第１過程１１０を含む。実行環境は、特にアプリケーションを実行するために用いられ、該実行環境は、プロセッサ、オペレーティングシステムリンカ（linker）、プログラムリンカ、又は、Ｊａｖａ仮想マシンの如き仮想プロセッサや仮想マシンである。学習モードの起動は、例えば、パスワード入力又は暗号化保護された利用者認証のような安全機構により保護されている。

【００６２】

方法１００は、起動した学習モードの間に実行環境においてアプリケーションを実行する第２過程１２０を含み、選択されて予定されているアプリケーションシナリオのためにアプリケーションのプログラム命令が実行され、実行環境が、実行されたプログラム命令に、第１のアプリケーションシナリオ特有の妥当性情報を割り当てる。このために、例えば、実行されたプログラム命令ごとに１つの妥当性情報が記憶されるデータ構造を使用するとよい。実行されなかったプログラム命令には、例えば非妥当情報が、例えばゼロ化データブロック、例外又は割込みの形式で割り当てられる。この場合のデータ構造は、先ず初期値として非妥当情報のみを含み、後にこの非妥当情報が、学習フェーズ中に部分的又は全体的に妥当性情報で上書きされる。

【００６３】

一変形例において、非妥当情報は、プログラム命令に対する妥当性情報が存在しないことによって決定される。

【００６４】

方法１００は、実行環境の作業モードを起動する第３過程１３０を含み、この作業モードにおいて実行環境がプログラム命令の第１の妥当性情報をチェックし、プログラム命令の第１の妥当性情報に応じて実行環境がプログラム命令を実行する。にもかかわらず、作業モード中に非妥当情報を有するプログラム命令が間違って実行されてしまいそうな場合には、例えば割り当てられた例外の送出、例えば、報知情報を使用して管理者へ通知することが可能である。あるいは、報知情報により、アプリケーション、実行環境、又はアプリケーションが実行される機器を、保護された状態に置くこともできる。そして、非妥当情報を有する当該プログラム命令は、実行されないことが好ましい。

【００６５】

作業モードの起動は、例えば、パスワード入力又は暗号化保護された利用者認証のような安全機構により保護されている。

【００６６】

本発明に係る方法１００によって、アプリケーション、例えばライブラリの使用されていない機能、又は動作中のアプリケーションの使用されていない機能は、アクセスできない状態におかれる。

【００６７】

この場合、使用されていないプログラム命令又はコード部分の識別は、できるだけ自動的に且つ使用者にとってわかりやすく行われる。このために、例えば、どのプログラム命令に妥当性情報が割り当てられたか、そしてどのプログラム命令に非妥当情報が割り当てられたか、を知らせる評価結果が提供されるとよい。

【００６８】

一例をあげると、開発者は、その評価結果の判定に基づいて、特定の入力データの範囲内でアプリケーションのために必要であるならば、なおも手動で個々のプログラム命令に妥当性情報を割り当てることができる。

【００６９】

換言するならば、実行環境は、学習モードにおいて、通過／到達した全ての実行経路の

プログラム命令を記録する。これは、例えば図２における第２実施形態に具体的に示されている。図２は、それぞれ妥当性情報Ｅを割り当てられたプログラム命令２１０の第１ブロックと、それぞれ非妥当情報ＮＥを割り当てられたプログラム命令２１５の第２ブロックと、それぞれ妥当性情報Ｅを割り当てられたプログラム命令２２０の第３ブロックとを示す。

【００７０】

学習モード中に、好ましくは全ての妥当な状態、つまり選択されて予定されているアプリケーションシナリオに関してアプリケーションが取り得る全ての状態を通る必要がある。

【００７１】

学習モードは、さまざまの時点で行うことができる。例えば以下のとおり。

【００７２】

あるアプリケーションシナリオのための学習フェーズは、例えば自動化設備のための検収／認可時のソフトウェア検証の際に行える。ただし、これは、機器の構成設定の封印時にも、アプリケーションのプログラムコードのロード又はインストール時にも行うことができる。この情報は、アプリケーションの実行されたプログラムコードと一緒に保存される。データ２２５、すなわち妥当性情報Ｅと非妥当情報ＮＥのいずれか又は両方は、プログラムコード中に直接、例えばオペレーションコードにおけるフラグとして、プログラムライブラリの入口点（関数）おけるフラグとして保存することができ、該フラグはオブジェクトコードの注釈又はバイナリコードの注釈とも呼ばれる。あるいは、当該データは個別のメタデータとして保存することもできる。

【００７３】

他の例では、コードが変更される。例えば標識されていないオペレーションコード、すなわち妥当性情報のないプログラム命令２１５は、ＮＯＰ、ＴＲＡＰ又は例外によって置き換えることもできる。

【００７４】

妥当性情報２２５を割り当てるために複数の学習フェーズを使用することもできる。

【００７５】

この場合、早ければ、特定の又は一般のアプリケーションシナリオが試験される、機器製造者のシステム試験において、第１の学習フェーズで学習モードを起動してもよい。これによって、アプリケーションの妥当性情報をもった基本構成を有するデータセットを生成することができる。

【００７６】

この予め生成された基本構成に対して、後に使用者において学習モードを改めて起動することによって、更なる構成をすることができる。これによって、機器の使用現場で直に行われる第２の学習フェーズを短縮することができ、したがって選択されて予定されているアプリケーションシナリオを短縮することができる。

【００７７】

この基本構成は、例えばシステム試験からのデータにより作成され、作成されたデータは、機器使用現場で作動する学習フェーズの間にさらに改善することができる。他の例では、学習されたデータ２２５（個別のメタデータ又は注釈付きのオブジェクトコード／バイナリコード）、すなわち妥当性情報と非妥当情報のいずれか又は両方は、暗号化保護された形式で、例えばデジタル符号化されたデータセットとして他の機器に提供することができる。

【００７８】

学習モードは種々の機器において起動でき、もしくは学習フェーズは種々の機器において実行することが可能である。例えば、次の機器において可能である。

・対象の機器自体、すなわち選択されて予定されているアプリケーションシナリオの使用を目的とした機器においてであり、

・構造的に同一の試験機器において（例えば、選択されて予定されているアプリケーショ

ンシナリオの使用時には動作しない）であり、
・対象の機器のシミュレーション環境において（デジタルツイン）である。
【００７９】
厳密な解釈では、起動された学習モードの間に、アプリケーションシナリオに関連する好ましくは全ての、後に実行される予定のプログラム部分（したがって、そのプログラム部分のプログラム命令）が、実際に実行される。
【００８０】
他の例では、曖昧（ファジー）学習も考えられる。すなわち、学習モードが起動される都度、広げられた範囲内のプログラム命令に、妥当性情報が割り当てられる。
【００８１】
この場合、例えばその都度異なる段階が考えられる。
【００８２】
段階「詳細（fine）」では、プログラム命令で使用される各命令、すなわちサブルーチン及びプログラムライブラリの命令にも、妥当性情報Ｅが割り当てられる。
【００８３】
段階「中間（medium）」では、実行されたプログラム命令のサブルーチンに妥当性情報Ｅが割り当てられる。ここでは、特に入れ子関数の場合に妥当性情報Ｅの割り当てのための煩雑性を少なくするために、例えばサブルーチンの呼出し深さも考慮することができる。
【００８４】
段階「粗（coarse）」では、アプリケーションによって使用されたプログラムライブラリにそれぞれ１つの妥当性情報Ｅが割り当てられ、それによって特に該当プログラムライブラリの全プログラム命令に対し１つの妥当性情報が割り当てられる。
【００８５】
これら段階の粒度（granularity）は、例えばアプリケーションのコード開発時に適切な構造ステートメントによって制御することもできる。この場合、開発者は、特定のプログラム命令及びそれに関係したプログラム命令、命令、サブルーチン又はプログラムライブラリに手動で妥当性情報を割り当てることができる。
【００８６】
このことは、例えば、従属関係を考慮できるように妥当性情報を考慮することによっても実現することができる。例えば第１の命令パスが妥当であるならば（この命令パスには以前から妥当性情報が割り当てられている）、自動的に、従属関係を有する第２の命令パスも同様に妥当である。この場合に、例えば、第２の命令パスに自動的に同様に妥当性情報が割り当てられるか、第２の命令パスはその従属関係の故に妥当である。換言するならば、例えば、第１の命令パスへの第２の命令パスの従属関係に基づいて、第１の命令パスの妥当性情報を第２の命令パスに引き継がせることができるということである。
【００８７】
作業モードでは、実行環境によって、妥当性情報Ｅが割り当てられているプログラム命令のみが受け入れられ、又は実行されることが好ましい。当該プログラム命令は、容認に標識されたプログラム命令と呼ぶこともできる。妥当性情報のないプログラム命令ＮＥ、すなわち容認に標識されていないプログラム命令へのジャンプがあった場合、これは例えば、例外となり、又は格納されていた異なる命令となり、あるいは換言するならば、例えば妥当でないプログラム命令を上書きした命令となる。
【００８８】
妥当性情報２２５の割り当て後に、機器が、再構成の結果、又は少し変更されたアプリケーションシナリオにおける使用の結果、拡張された又は新たな一連のプログラム命令、関数、サブルーチン、及びライブラリのいずれか１つ以上を必要とする場合には、例えば、構成データなどのトリガーや新たな学習フェーズにおける手動トリガーの１つ以上による制御で、割り当てられた妥当性情報２２５を再び取り除くことができる。この場合、学習モードが再び起動され、変更されたアプリケーションシナリオ又は再構成に応じて、妥

当性情報がプログラム命令に割り当てられる。これによって、以前は容認ではなかったプログラム命令（又は妥当性情報のないプログラム命令）を、再び使用可能にすることができる。コード領域がＮＯＰ、ＴＲＡＰ又は例外によって取り除かれている場合、これらのコード部分は、変更されていないアプリケーションのバックアップコピー又はそのプログラムライブラリから再読込可能である。

【００８９】

他の例において、本発明に係る方法は、ハードウェアで直接実現される。この場合には、作業環境であるプロセッサ、例えばＣＰＵが、第１モードすなわち学習モードと、第２モードすなわち作業モードとをもっている。第１モードでは、実行されたオペレーションコードが、したって実行されたプログラム命令が、標識されて、すなわち妥当性情報を割り当てられて、プログラムイメージ内に保存される。作業モードへの切替後には、アプリケーションの標識された命令のみが受け入れられる。

【００９０】

他の例において、本発明に係る方法は、仮想マシンの形式での作業環境により実現される。仮想マシンは、学習モードにおいて、アプリケーションの実行されたコード行を記録し、すなわちそのアプリケーションの実行されたプログラム命令を記録し、プログラム命令に割り当てられた妥当性情報を含んだプロトコルファイル（ログファイル）を生成する。妥当性情報の割り当ては、プロトコルファイルへの入力の発生時に直接行われる。

【００９１】

後に当該アプリケーションを実行するときに、仮想マシンは、作業モードにおいてプロトコルファイルを使用することにより、プログラム命令が実行されてよいかどうかをチェックする。プロトコルファイルのインテグリティ／信憑性は、例えばデジタル署名によって保護されているとよく、このデジタル署名は仮想マシンによってチェックされる。

【００９２】

図３は、本発明に係る方法の第３実施形態を例示する。この実施形態では、本発明に係る方法がオペレーティングシステムカーネルにより実現される。オペレーティングシステムカーネルの学習モードで、管理された環境、例えばデバッガにおいて、アプリケーションが開始される。実行されるプログラム命令３１０，３２０は、これらに妥当性情報が割り当てらていることによって取得される。そして、これらプログラム命令及び妥当性情報が記憶され得る。作業モードでは、プログラムコードを編成するために、したがってアプリケーションのプログラム命令を編成するために、実行時ローダがその妥当性情報を使用する。

【００９３】

例えば、実行されていない全てのコード行が、したがって妥当性情報のない全てのプログラム命令が、ＴＲＡＰによって置き換えられ得る。

【００９４】

他の例では、本発明に係る方法は、オペレーティングシステムカーネルによりメモリ管理ユニット（Memory Management Unit、略してＭＭＵ）を用いて、実現される。

【００９５】

アプリケーションが、オペレーティングシステムカーネルの学習モードにおいて、管理された環境、例えばデバッガにて開始される。実行されるプログラム命令は、これらそれぞれに妥当性情報が割り当てられることによって取得される。そして、これらプログラム命令及び妥当性情報は記憶可能である。

【００９６】

妥当性情報が割り当てられていないプログラム命令は、すなわち標識されていないコード部分とも呼ばれる妥当性情報のないプログラム命令は、メモリ管理ユニットによって実行不可又は読み出し不可として区別される。アクセス時に（外部メモリからキャッシュメモリへのプログラム命令の読み込み時に）、メモリ管理ユニットによってＴＲＡＰ又は割込み（Interrupt）がトリガーされるとよい。

【００９７】

図４は、アプリケーションのプログラム命令をコンピュータ支援によりセキュアに実行するための第４実施形態に係る実行環境４００を示す。実行環境４００は、第１のスイッチングモジュール４１０、実行モジュール４２０、第２のスイッチングモジュール４３０及びインターフェース４８５を含み、これらは第１のバス４８０を介して相互に通信可能に接続されている。

【００９８】

第１のスイッチングモジュール４１０は、実行環境４００の学習モードを起動する。

【００９９】

実行モジュール４２０は、起動された学習モードの間に実行環境４００においてアプリケーションを実行する。その際に、アプリケーションのプログラム命令が、選択されて予定されているアプリケーションシナリオのために実行され、実行環境４００が、アプリケーションシナリオ特有の第１の妥当性情報を、実行されたプログラム命令に割り当てる。

【０１００】

第２のスイッチングモジュール４３０が実行環境４００の作業モードを起動し、該作業モードにおいては実行環境４００がプログラム命令の第１の妥当性情報をチェックし、実行環境がプログラム命令を当該妥当性情報に応じて実行する。

【０１０１】

例えば、実行環境は、機器、例えばフィールド機器、制御機器又は測定機器において、プロセッサとして、又はチップ上の特に埋め込みＪａｖａ形式の仮想マシンとして、組み込まれているとよい。該機器はシステムの一部であり、該機器はデータバスを介して操作者のワークステーションに接続されている。

【０１０２】

例えば、図５にこのようなシステムを示す。具体的には、図５は、例えば発電所における高電圧用の監視システムなどのシステムを示す。

【０１０３】

ワークステーションは、例えばＩＢＭ準拠のコンピュータシステムであり、例えばディスプレイである表示機器５３２と、例えばコンピュータマウス５３３及びキーボード５３０である複数の入力機器とを含む。このワークステーションは、第３のバス５８０及び機器５０１の第２のインターフェース５７５を介して、機器５０１に通信可能に接続されている。第３のバス５８０は、例えばイーサネット（登録商標）バス又はユニバーサルシリアルバス（ＵＳＢ）であってよい。

【０１０４】

機器５０１は、選択されて予定されているアプリケーションシナリオ、例えば付設の測定方法を伴う高電圧監視におけるプログラム命令をコンピュータ支援により安全に実行するための実行環境４００を有する。機器５０１内では、例えば、実行環境は、インターフェース４８５により、第２のバス５８５を介して検出器５１０（例えば電圧センサ）と第２のインターフェース５７５とに接続されている。

【０１０５】

例えば高電圧や電圧ピークの監視中に、妥当性情報が割り当てられていないプログラム命令が実行される場合、実行環境は例外を送出することができ、そしてこの例外がワークステーションにおいて操作者に対し提示される。操作者は、場合によっては、アプリケーションの偶発的誤動作に関係があったかどうか、又はアプリケーションの改ざんが権限のない第三者によって行われたどうかのチェックをすることができる。

【０１０６】

本発明を実施形態よって詳しく図解、説明したが、本発明はそれら開示例に限定されず、当業者であればその記載から他の変形例を、本発明の保護の範囲を逸脱することなく導き出すことができる。

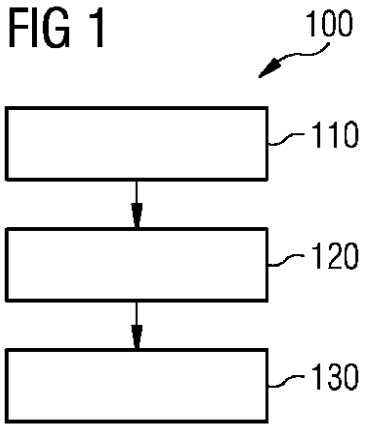
【符号の説明】

【０１０７】

１００　本発明に係る方法

１１０　実行環境の学習モードの起動
１２０　アプリケーションの実行
１３０　実行環境の作業モードの起動
２１０　妥当性情報Ｅを割り当てられたプログラム命令
２１５　非妥当情報ＮＥを割り当てられたプログラム命令
２２０　妥当性情Ｅを割り当てられたプログラム命令
２２５　妥当性情報
３１０　プログラム命令
３１５　プログラム命令
３２０　プログラム命令
４００　実行環境
４１０　第１のスィッチングモジュール
４２０　実行モジュール
４３０　第２のスィッチングモジュール
４８０　第１のバス
４８５　インターフェース
５０１　機器
５１０　検出器
５３０　キーボード
５３２　表示器
５３３　マウス
５７５　第２のインターフェース
５８０　第３のバス

【図１】



【図２】

FIG 2

225

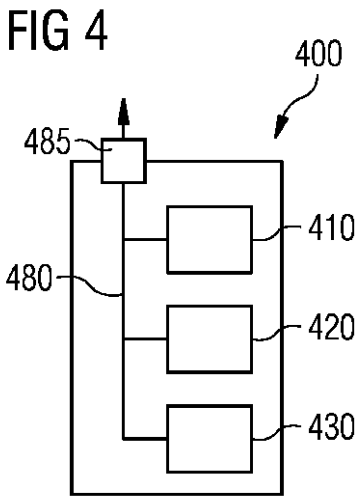
210	000000013FE38C74	cpm	qword ptr [rsp+0C0h], 0	E
	000000013FE38C7D	je	13FE38C99	E
215	000000013FE38C7F	cmp	dword ptr [rsp+0C8h], 80h	NE
	000000013FE38C8A	je	13FE38CB0h	NE
	000000013FE38C8C	cmp	dword ptr [rsp+0C8h], 0C0h	NE
	000000013FE38C97	je	13FE38CB0h	NE
220	000000013FE38C99	cpm	qword ptr [rsp+0C8h], 100h	E
	000000013FE38CA4	je	13FE38CB0h	E

【図３】

FIG 3

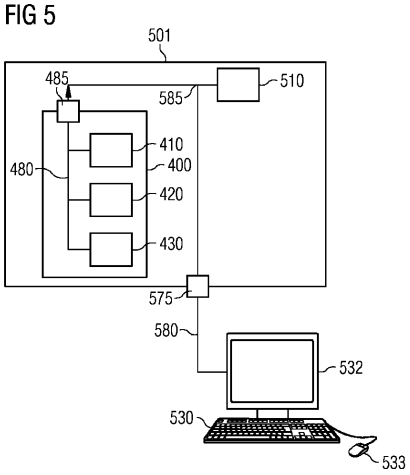
310	000000013FE38C74	cpm	qword ptr [rsp+0C0h], 0	
	000000013FE38C7D	je	13FE38C99	
315	000000013FE38C7F	int	2A	
	000000013FE38C8A	int	2A	
	000000013FE38C8C	int	2A	
	000000013FE38C97	int	2A	
320	000000013FE38C99	cpm	qword ptr [rsp+0C8h], 100h	
	000000013FE38CA4	je	13FE38CB0h	

【図４】



【図５】

FIG 5



フロントページの続き

(72)発明者　ファルク、ライナー
ドイツ連邦共和国　８５５８６　ポイング、プリメルヴェーク　９
(72)発明者　フィッシャー、カイ
ドイツ連邦共和国　８５５９８　バルトハム、ハインリッヒ－マルシュナー－シュトラーセ　７４
(72)発明者　ハインテル、マルクス
ドイツ連邦共和国　８１３７７　ミュンヒェン、プレラート－ヴェレンホーファー－シュトラーセ　３１
(72)発明者　メルリ、ドミニク
ドイツ連邦共和国　８６６０９　ドナウヴェルト、ヨハネス－クネーベル－シュトラーセ　１０
(72)発明者　アシャウアー、ハンス
ドイツ連邦共和国　８１８２９　ミュンヒェン、カロリーネ－ハーシェル－シュトラーセ　２３
(72)発明者　クラーゼン、ヴォルフガング
ドイツ連邦共和国　８５５２１　オットーブルン、ブレンナーシュトラーセ　２６
(72)発明者　プファウ、アクセル
ドイツ連邦共和国　８０３３３　ミュンヒェン、ガーベルスバーガー　シュトラーセ　４８デー
(72)発明者　パイカ、シュテファン
ドイツ連邦共和国　８５５７０　マルクト　シュヴァーベン、ブルガーフェルト　４７　デー
(72)発明者　シュナイダー、ダニエル
ドイツ連邦共和国　８０７９６　ミュンヒェン、ミッターマイアーシュトラーセ　２９

審査官　上島　拓也

(56)参考文献　特開平１１－１７５３６９（ＪＰ，Ａ）
特開２００７－２２０１０６（ＪＰ，Ａ）
特開２００９－１９９２１４（ＪＰ，Ａ）
国際公開第２０１１／０５５４１７（WO，Ａ1）
特開２０１６－０２１１６０（ＪＰ，Ａ）
特開２００８－２１７２３５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／１２
Ｇ０６Ｆ　９／４４５