(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4732651号
(P4732651)
(45)発行日　平成23年7月27日(2011.7.27)　(24)登録日　平成23年4月28日(2011.4.28)

(51)Int.Cl.　F I
G06F 21/22 (2006.01)　G06F 9/06 660J

請求項の数 4　(全 6 頁)

(21)出願番号	特願2001-525524 (P2001-525524)
(86)(22)出願日	平成12年9月18日 (2000.9.18)
(65)公表番号	特表2003-510684 (P2003-510684A)
(43)公表日	平成15年3月18日 (2003.3.18)
(86)国際出願番号	PCT/EP2000/009131
(87)国際公開番号	WO2001/022223
(87)国際公開日	平成13年3月29日 (2001.3.29)
審査請求日	平成19年9月18日 (2007.9.18)
(31)優先権主張番号	199 44 991.0
(32)優先日	平成11年9月20日 (1999.9.20)
(33)優先権主張国	ドイツ(DE)

(73)特許権者　596007511
ギーゼッケ　ウント　デフリエント　ゲーエムベーハー
Ｇｉｅｓｅｃｋｅ　＆　Ｄｅｖｒｉｅｎｔ　ＧｍｂＨ
ドイツ連邦共和国　Ｄ－８１６７７　ミュンヘン　プリンツレーゲンテンシュトラッセ　１５９
(74)代理人　100073184
弁理士　柳田　征史
(74)代理人　100090468
弁理士　佐久間　剛
(72)発明者　バルディシュヴァイラー，ミヒァエル
ドイツ連邦国　８１８２５　ミュンヘン　ハンスヤコブシュトラーセ　９９
最終頁に続く

(54)【発明の名称】プログラム実行を保護するための方法

(57)【特許請求の範囲】
【請求項１】
コンピュータを用いてサブプログラムの呼出し時におけるプログラムの実行を保護するための、呼び出されたサブプログラムが、呼出しプログラムから直接または間接的に渡されるデータのチェックを、前記呼び出されたサブプログラムの実行前または実行中に行う方法において：
－　コンピュータが、前記呼出しプログラムから前記呼び出されたサブプログラムに渡されるべきパラメータについて第１のチェックサムをつくるステップ（ステップ２）と；
－　コンピュータが、前記第１のチェックサムを専用に用意されたメモリ領域に格納するステップと；
－　コンピュータが、前記呼び出されたサブプログラムの実行の前に、該呼び出されたサブプログラムが受け取った前記パラメータについて第２のチェックサムをつくり（ステップ５）、前記第２のチェックサムと前記第１のチェックサムとが一致するか否かについてチェックするステップ（ステップ６）と；
－　コンピュータが、前記第１のチェックサムと前記第２のチェックサムとが一致しない場合には、前記プログラムを終了させるか（ステップ７）、またはエラーメッセージを出力するステップと；
を含むことを特徴とする方法。
【請求項２】
コンピュータが、前記第１のチェックサムを格納するステップにおいて、前記第１のチェ

ックサムをＲＡＭまたはレジスタ領域に格納することを特徴とする請求項１記載の方法。
【請求項３】
コンピュータが、呼出し関数のリターンアドレスを管理するテーブルにリターンアドレスが存在するか否かをチェックし、前記テーブル格納されたリターンアドレスと呼出しプログラムにより報告されたリターンアドレスとを比較し、前記テーブルに格納されたリターンアドレスが前記呼出しプログラムにより報告されたリターンアドレスとが異なるとき、前記プログラムを終了させるか、またはエラーメッセージを出力するステップを更に有する請求項１または２記載の方法。
【請求項４】
コンピュータが、サブプログラムの呼出し時に前記サブプログラムの実行に要するクロックサイクル数をカウントするタイマーをスタートさせ（ステップ２２）、前記タイマー値が、あらかじめ設定されたクロックサイクル数を超えると（ステップ２６）、前記プログラムを終了させるか、またはエラーメッセージを出力するステップを更に有する請求項１から３のいずれか１項記載の方法。
【発明の詳細な説明】
【０００１】
本発明は、特許請求項１にしたがう、プログラム実行を保護するための方法に関する。
【０００２】
例えばＩＣカード分野におけるような、保全関連アプリケーションでは特に、プログラム実行を不正操作から保護する必要がある。秘密データ、例えば秘密キーデータを保護するには、権限のない人間による読出しを防止するために、保護されるべきデータを暗号化形態で格納することが知られている。
【０００３】
しかし、秘密データへのアクセスは、プログラム実行に選択的に割込をかけ、選択的割込の繰返しにより秘密データが推定され得るエラーを暗号化ルーチンに生じさせることで達成することもできる。
【０００４】
そのような攻撃を避けるため、プログラム実行のエラーまたは妨害を確実に認知する必要がある。ドイツ国特許第ＤＥ３７　０９　５２４　Ｃ２号は、コンピュータのプログラムメモリのメモリセル内容をチェックするための方法を開示している。この特許では、様々なアドレス及びデータメモリ領域のメモリセル内容からつくられる、いくつかのチェックサムが格納される。チェックサムはコンピュータの作動開始時及び／または作動中に決定され、格納されたチェックサムと比較される。違いが確認されると、エラー信号が出力される。
【０００５】
ドイツ国特許第ＤＥ３７　０９　５２４　Ｃ２号により知られる方法は、主として、プログラムで用いられるデータの正しさをチェックするに適している。この特許は、プログラム実行の不正操作が特にプログラム呼出し時、すなわちサブプログラムまたは関数プログラムの実行時にも、あるいはその時に、なされ得るという事実を考慮していない。
【０００６】
したがって、本発明の課題はモジュール構成のプログラムの、特にサブプログラム呼出し時に、確実なチェックを可能にする方法を提示することである。
【０００７】
上記課題は、本発明にしたがい、呼出しプログラムから渡されるべきデータの確実な転送を確認するデータチェックを、呼び出されたプログラムが実行することより解決される。
【０００８】
本発明によりさらに、個々のプログラム部分が確実かつ完全に実行されることだけでなく、全プログラム実行が妨害されないこと及び不正操作を受けつけないことを保証する、保全性が達成される。
【０００９】

本発明の有利な実施形態は、呼出しプログラムが呼出しプログラムから呼び出されるプログラムに渡されるパラメータについてチェックサムを初めにつくり、このチェックサムが専用に用意されたメモリ領域に格納される。パラメータが渡された後に、呼び出されたプログラムも受け取ったパラメータについてチェックサムをつくる。呼出しプログラムと呼び出されたプログラムによりつくられたチェックサムが異なっていれば、プログラムは終了させられる。

【００１０】

このようにすれば、関数プログラム、特に保全関連データを実行する関数プログラムは開始時に不正操作に対して既に検査されており、よって不完全なパラメータをもつ呼び出されたプログラムの実行開始を阻止でき、エラーのあるデータの評価を行うことは許されない。

【００１１】

チェックサムを格納するために用意されるメモリ領域はＲＡＭまたはレジスタ領域につくられることが好ましい。

【００１２】

渡されるべきパラメータについてチェックサムをつくるための、別の、すなわち代替の実施形態は、リターンアドレスのチェックにより得られる。呼出し関数のリターンアドレスがテーブルに入れられ、呼び出されたプログラムはこのテーブルにより、呼出しプログラムから送られたリターンアドレスがテーブルにあるか否かをチェックできる。報告されたリターンアドレスが誤っている場合には、プログラムを中断できる。

【００１３】

別の代替の、すなわちさらなる保全チェックは、サブプログラムまたは関数プログラムの呼出し時にタイマーをスタートさせることにより行うことができる。

【００１４】

タイマーはプログラムの実行に必要なクロックサイクルをカウントする。正規のサブプログラム実行に必要なクロックサイクル数が、タイマーに対する限界値として初めにプリセットされる。プリセットされたクロック数をこえてもサブプログラムが終了しなければ、プログラムは終了させられる。

【００１５】

以下で、図１～３を参照して本発明をさらに詳細に説明する。

【００１６】

図１は、サブプログラム呼出し、特に関数呼出しの実行を説明しており、機能ステップ１～３は呼び出されるべきプログラムに関係し、機能ステップ４～８はサブプログラムの評価に関係する。

【００１７】

呼び出されるべきプログラムにおいて、初めにサブプログラムの実行に必要なパラメータがステップ１で与えられる。このパラメータについて、最も単純な場合にはパリティチェックからなる、チェックサムがステップ２でつくられる。一般的なチェックサム作成方法、例えばＣＲＣ(巡回冗長検査)またはＥＤＣも用い得ることは当然である。そのようにして決定されたチェックサムは専用に用意されたメモリ領域に書き込まれる。このメモリ領域は、揮発性メモリ(ＲＡＭ)または不揮発性で書換可能なメモリ(例えばＥＥＰＲＯＭ)とすることができる。

【００１８】

チェックサム１の作成及び格納に続いて、サブプログラム呼出しがステップ３で行われる。ステップ４はサブプログラムの実行の開始である。このサブプログラムでは、渡されたパラメータについてチェックサム２が初めにつくられる。チェックサム２は、呼出しプログラムにおいてチェックサム１を決定するために用いられた方法と同じ方法でつくられる。

【００１９】

次いで、チェックサムＰＳ１及びＰＳ２の一致についてのチェックがステップ６で行われ

る。２つのチェックサムが一致しないことがステップ６で確認されると、プログラムパラメータが渡されるときにエラーが生じたと想定することができ、これは秘密データの決定を目的とする意図的妨害の表れであり得る。一手段として、プログラムをステップ７で終了させることができ、あるいは対応する別の手段、例えばメインプログラムへのエラーメッセージがとられる。

【００２０】

チェックサムＰＳ１及びＰＳ２が一致することがステップ６で確認されれば、実際の関数実行が開始される。

【００２１】

図２は、リターンアドレスをチェックすることによりプログラム保護が可能であることを示す。リターンアドレスは、関数呼出し時にハードウエアによりスタックされる。本事例においても上述と同様に、サブプログラム呼出し時に、ステップ１１で呼出しプログラムからサブプログラムに情報(例えばリターンアドレス)が渡される。本発明にしたがえば、リターンアドレスはテーブル１７に管理され、サブプログラムの実行時に－リターンアドレスがステップ１２でＲＡＭに格納されている限りにおいて－ステップ１３でテーブル１７に基づいてチェックされるべきリターンアドレスが一致について初めに検査される。渡されたリターンアドレスがテーブルにないことがステップ１４で確認されると、ステップ１５でプログラムが終了させられる。そうでなければ関数プログラムの実行がステップ１６で開始される。

【００２２】

図３は、正しいプログラムの実行、すなわち妨害されていないプログラムの実行がタイマーを用いてチェックされる実施形態を示す。ステップ２１におけるサブプログラムの開始直後に、ステップ２２でタイマーがスタートされる。このタイマーは、サブプログラムの実行に必要な時間の測定、すなわちクロックサイクル数のカウントを行うように構成される。ステップ２２におけるタイマーのスタートに続いて、サブプログラムの関数がステップ２３で実行され、関数の終了後にステップ２４でタイマーが停止される。ステップ２５で、関数プログラムの実行に必要なクロック数がプリセットされたクロックサイクル数に一致するか否かがチェックされる。一致しなければ、プログラムはステップ２６で終了させられる。そうでなければプログラム実行がステップ２７で、例えばメインプログラムにジャンプして戻ることにより、続けられる。

【００２３】

図３は、関数または関数プログラムの実行後にタイマーが停止されてチェックされることを示す。実際上、タイマーがさらにチェックされる一定のポイントを関数プログラムに与えることにより保全性を高めることができる。これにより、エラーまたは攻撃があるにもかかわらず、関数プログラムの大部分が実行されてしまうことを防止できる。

【００２４】

あるいは、開始後、タイマー値を継続的に限界値と比較し、限界値に達するか限界値をこえた場合にプログラムを終了させるようにすることもできる。

【００２５】

図１～３による個々の例を、独立した、互換的手段として示した。これらの例を併用することにより保全性を高めることができる。チェックサム、リターンアドレス及びタイマーによるチェックを並行して行うことにより、最大の保全性が得られる。

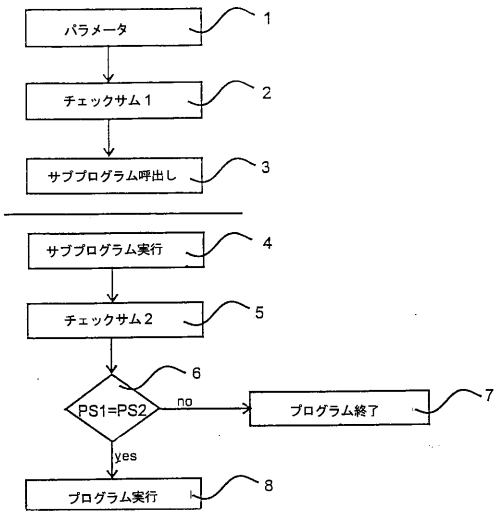
【図面の簡単な説明】

【図１】　チェックサムを用いるチェックに対するフローチャートを示す

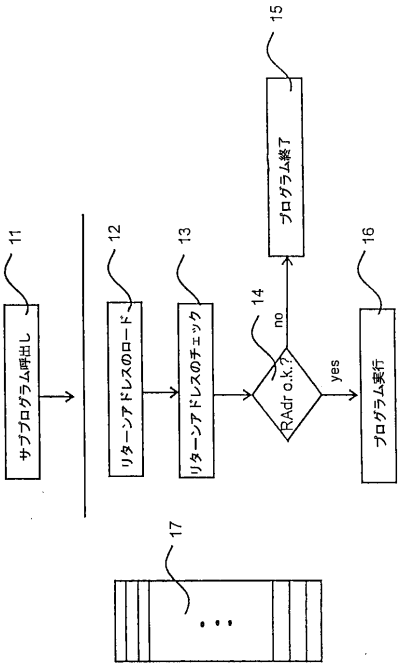
【図２】　リターンアドレステーブルを用いるチェックに対するフローチャートを示す

【図３】　タイマーを用いるチェックに対するフローチャートを示す

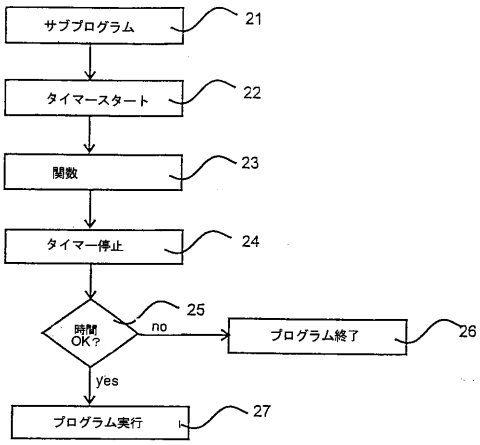
【図１】


パラメータ
1
チェックサム１
2
サブプログラム呼出し
3
サブプログラム実行
4
チェックサム２
5
PS1=PS2
6
no
プログラム終了
7
yes
プログラム実行
8

【図２】


11
サブプログラム呼出し
12
リターンアドレスのロード
13
リターンアドレスのチェック
14
RAdr o.k.?
no
15
プログラム終了
yes
16
プログラム実行
17

【図３】


サブプログラム
21
タイマースタート
22
関数
23
タイマー停止
24
時間 OK?
25
no
プログラム終了
26
yes
プログラム実行
27

フロントページの続き

審査官　後藤　彰

(56)参考文献　特開平　７－　８４７８６（ＪＰ，Ａ）
特開平　９－２８２１５６（ＪＰ，Ａ）
特開平　４－２５９０３６（ＪＰ，Ａ）
特開昭６２－　１９９３７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　21/22