(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6157811号
(P6157811)
(45)発行日　平成29年7月5日(2017.7.5)　(24)登録日　平成29年6月16日(2017.6.16)

(51)Int.Cl.　F I
G06F 9/445 (2006.01)　G06F 9/06 610K

請求項の数 6　外国語出願　(全 14 頁)

(21)出願番号　特願2012-166673(P2012-166673)
(22)出願日　平成24年7月27日(2012.7.27)
(65)公開番号　特開2013-178733(P2013-178733A)
(43)公開日　平成25年9月9日(2013.9.9)
審査請求日　平成27年6月18日(2015.6.18)
(31)優先権主張番号　13/193,718
(32)優先日　平成23年7月29日(2011.7.29)
(33)優先権主張国　米国(US)

前置審査

(73)特許権者　500520743
ザ・ボーイング・カンパニー
The Boeing Company
アメリカ合衆国、60606-2016
イリノイ州、シカゴ、ノース・リバーサイド・プラザ、100
(74)代理人　110002077
園田・小林特許業務法人
(72)発明者　リーギ,　ルイジ　ピー.
アメリカ合衆国　カリフォルニア　92653,　ラグーナ　ヒルズ,　ラルゴ　ドライヴ　24982

最終頁に続く

(54)【発明の名称】ブート前データ検証のための方法及びシステム

(57)【特許請求の範囲】
【請求項１】
航空機アビオニクスデバイス用のオペレーショナルフライトプログラム（ＯＦＰ）の実行用のデータの読み込みに先立って、前記ＯＦＰを定義するデータを検証する方法であって、
ａ）前記ＯＦＰを定義する、航空機内の１次データ記憶領域内のデータに対する第１の検証番号を計算するステップと、
ｂ）前記第１の検証番号と、航空機アビオニクスデバイスのブートＲＯＭに保存されている番号とを比較するステップと、
ｃ）前記第１の検証番号が前記保存されている番号と一致しないことを確認するステップと、
ｄ）前記第１の検証番号が前記保存されている番号と一致しないことの前記確認に基づき、前記１次データ記憶領域内のものと同一のＯＦＰを定義している、前記航空機内の２次データ記憶領域内のデータに対する第２の検証番号を計算するステップと、
ｅ）前記第２の検証番号と、前記航空機アビオニクスデバイスの前記ブートＲＯＭに保存されている前記番号とを比較するステップと、
ｆ）前記第２の検証番号と前記保存されている番号とが一致することを確認するステップと、
ｇ）前記第２の検証番号と前記保存された番号が一致することの確認に基づき、前記１次データ記憶領域内のデータを前記２次データ記憶領域内のデータで上書きするステップ

と、
ｈ）前記ＯＦＰを実行させるステップと、を含む方法。
【請求項２】
前記第１の検証番号を計算するステップ及び前記第２の検証番号を計算するステップの各々が、前記ＯＦＰのチェックサムを計算するステップを含む、請求項１に記載の方法。
【請求項３】
前記第１の検証番号を計算するステップ及び前記第２の検証番号を計算するステップの各々が、前記ＯＦＰを定義するデータのチェックサムを計算するため、前記ブートＲＯＭデバイス内の命令を実行するステップを含む、請求項１に記載の方法。
【請求項４】
航空機アビオニクスデバイスであって、
プロセシング装置と、
前記プロセシング装置によって基本入出力システムが実行されるブートＲＯＭと、
前記航空機アビオニクスデバイスに関連するオペレーショナルフライトプログラム（ＯＦＰ）のイメージを保存するように構成されている１次データ記憶領域と、
前記航空機アビオニクスデバイスに関連する前記ＯＦＰの追加イメージを保存するように構成された少なくとも一つの２次データ記憶領域と、を含み、
前記プロセッシング装置が、
前記１次データ記憶領域内に保存されている前記イメージに対する第１の検証番号を計算し、
前記１次データ記憶領域内に保存されている前記イメージに対して計算された前記第１の検証番号と、前記ブートＲＯＭに保存されている番号とを比較し、
前記１次データ記憶領域内に保存されている前記イメージに対する前記第１の検証番号が前記保存されている番号と一致しないことを確認し、
前記１次データ記憶領域内に保存されている前記イメージに対する前記第１の検証番号が前記保存されている番号と一致しないことの前記確認に基づき、前記少なくとも一つの２次データ記憶領域内の前記追加イメージに対する第２の検証番号であって、前記少なくとも一つの２次データ記憶領域内の前記追加イメージに対応するデータが前記１次データ記憶領域内のものと同一のＯＦＰを定義している、第２の検証番号を計算し、
前記少なくとも一つの２次データ記憶領域内に保存されている前記追加イメージに対して計算された前記第２の検証番号と、前記ブートＲＯＭに保存されている前記番号とを比較し、
前記第２の検証番号と前記保存されている番号とが一致することを確認し、
前記１次データ記憶領域の前記イメージを前記航空機アビオニクスデバイスに関連する前記ＯＦＰの前記追加イメージで上書きし、
前記２次データ記憶領域の前記追加イメージによって定義される前記ＯＦＰを実行する、ようにプログラムされている、航空機アビオニクスデバイス。
【請求項５】
前記第１及び第２の検証番号の各々が前記ＯＦＰに対するチェックサムを含む、請求項４に記載の航空機アビオニクスデバイス。
【請求項６】
前記少なくとも一つの２次データ記憶領域が、シリコンメモリデバイス、コンピュータハードドライブ、ＣＤ－ＲＯＭ、フラッシュドライブ、及びサムドライブのうちの少なくとも一つを含む、請求項４に記載の航空機アビオニクスデバイス。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の分野は概して、一又は複数のプログラムの実行を開始するＢＩＯＳ（基本入出力システム）を組み込むコンピュータベースシステムの起動に関し、より詳しくはこのようなプログラムのためのブート前データ検証を組み込む方法及びシステムに関する。

【背景技術】
【０００２】
該して、コンピュータシステムに最初の電源が投入されると、起動プログラムが動作し、不揮発性メモリに保存される。このような起動プログラムはブートファームウェアと呼ばれることがあり、口語的にはＢＩＯＳプログラムと呼ばれる。ＢＩＯＳプログラムは、標準的なパーソナルコンピュータから航空機内の航空電子工学機器（例えば、航空電子工学ユニットすなわち「ブラックボックス」）として配備される組み込みシステムにいたるまで、多数のコンピュータシステムで実行される。
【０００３】
ＢＩＯＳプログラムの実行は、ＢＩＯＳが実行される処理装置と通信可能に結合されているシステムコンポーネントの検出及び識別に有用である。例えば、コンピュータハードドライブ、表示装置、及び外部メモリデバイスは、ＢＩＯＳの実行によって識別及び処理されるが、このようなデバイス用のソフトウェアドライバは、ＢＩＯＳが操作をオペレーティングシステムに戻したときに読込まれる。幾つかのアプリケーションでは、ＢＩＯＳは実行すべき組込み試験（ＢＩＴ）を始動するソフトウェアを含むことができ、それによって、ハードドライブ、表示装置などが少なくとも部分的に動作していることを判断する。すなわち、プロセッサはデバイスと通信することができる。オペレーティングシステムを起動するＢＩＯＳの一部、又は航空機システムの場合には、動作を開始するデバイスに関連する飛行管制プログラム（ＯＦＰ）によって、最終的にＢＩＯＳの実行が完了する。
【０００４】
このようなシステムでは、ＢＩＯＳが動作してオペレーティングシステム又はＯＦＰの実行を開始する。しかしながら、ＢＩＯＳにはオペレーティングシステム又はＯＦＰの内容の検証を行える命令は含まれていない。そのため、オペレーティングシステム、ＯＦＰ、又は他のアプリケーションが破損している場合には、特定のシステムの動作には障害が発生するか、まったく動作しない。
【０００５】
航空機搭載の航空電子工学機器では、ＢＩＯＳ又はブートＲＯＭからＯＦＰを実行している場合には、誤った取り外し並びに交換作業が問題の原因となる。例えば、デバイスがＯＦＰを正しく実行していない場合には、航空電子工学デバイスは取り外し及び交換が行われ、取り外されたデバイスは整備倉庫に送られる。上述のように取り外されたデバイスに関する問題点は再現することができず、ＯＦＰが誤っていたと判断されることがしばしばある。そのため、修復作業はＯＦＰの再読込み、再試験、及び運用への復帰で構成されることになる。
【発明の概要】
【０００６】
本発明の態様によれば、プログラム実行のためのデータの読込みに先立って、実行可能なプログラムを定義するデータの検証方法が提示されている。この方法は、１次データ記憶領域内のデータ、実行可能なプログラムを定義するデータに対する検証番号を計算するステップ、計算された検証番号と保存されている番号とを比較するステップ、検証番号が保存されている番号と一致した場合に１次データ記憶領域内のプログラムを実行するステップ、１次データ記憶領域内で実行可能な同一のプログラムを２次データ記憶領域内で定義するデータに対して検証番号を計算するステップを含む。検証番号と保存されている番号とが一致しない場合には、２次データ記憶領域内のデータに対して計算した検証番号と保存されている番号とを比較し、２次データ記憶領域内のデータに対する検証番号と保存されている番号とが一致する場合には、該当するプログラムを実行し、２次データ記憶領域内のデータに対する検証番号と保存されている番号とが一致しない場合には、失敗したことを示す。好ましくは、この方法は、同一の実行可能なプログラムを定義するデータを含む各データ記憶領域に対して反復される手順ｄ）、ｅ）及びｆ）をさらに含む。好ましくは、この方法は、２次データ記憶領域に対して計算した検証番号と保存されている番

号とが一致しない場合に、２次データ記憶領域内のデータを１次記憶領域にコピーするステップをさらに含む。有利には、この方法は、航空機搭載電子工学機器に対して、飛行管制プログラムのチェックサムを計算するステップを含んでいてもよい。有利には、この方法は、実行可能なプログラムを定義するデータのチェックサムを計算するため、ブートＲＯＭデバイス内の命令を実行するステップを含んでいてもよい。有利には、この方法は、計算した検証番号と基本入出力システムに関連するメモリに保存されている番号とを比較するステップを含む。

【０００７】

本発明のさらなる態様によれば、処理装置、当該処理装置によって基本入出力が実行されるブートＲＯＭ、デバイスに関連する実行可能なアプリケーションのイメージを保存するように構成された１次データ記憶領域、及びデバイスに関連する実行可能なアプリケーションの少なくとも１つの追加イメージを保存するように構成された少なくとも１つの２次データ記憶領域を含むデバイスが提供される。デバイスは、１次データ記憶領域内に保存されたイメージ及び少なくとも１つの２次データ記憶領域内に保存された各イメージに対して個別に検証番号を計算し；各イメージに対して計算された個別の検証番号とブートＲＯＭに保存されている番号とを比較し；イメージに対して計算された検証番号が任意の１次又は２次データ記憶領域に保存された番号と一致し、イメージに対して計算した個別の検証番号が保存された番号と一致しなかった場合には、１次又は２次のデータ記憶領域の１つからイメージをコピーし；さらに１次及び２次データ記憶領域の１つの保存されたイメージによって定義されるプログラムを実行する、ようにプログラムされている。有利には、このデバイスは、航空機搭載の航空電子工学ユニットを含むことができる。有利には、このデバイスは、飛行管制プログラムを含むことができ、独立に計算された検証番号は飛行管制プログラム用のチェックサムを含むことができる。有利には、このデバイスは、前記１次及び２次データ記憶領域内の各イメージに対して個別に計算された検証番号が、イメージによって定義されたプログラムの実行前に保存されている番号と一致することを検証するように、プログラムすることができる。有利には、個別の検証番号を計算する場合に、実行可能なアップリケーションのイメージのチェックサムを計算する前記ブートＲＯＭ内の命令を実行するように、デバイスをプログラムすることができる。有利には、前記デバイスがランダムアクセスメモリを含む場合に、デバイスは前記データ記憶領域の一つからイメージをコピーするようにプログラムすることができ、個別に計算された検証番号は、実行のため前記ランダムアクセスメモリに保存された番号に一致する。有利には、デバイスは、シリコンメモリデバイス、コンピュータハードドライブ、ＣＤ－ＲＯＭ、フラッシュドライブ、及びサムドライブのいずれか一つを含んでいてもよい。

【０００８】

本発明のさらなる態様では、コンピュータ上で具現化されコンピュータで実行可能な命令を有する一又は複数のコンピュータで読み取り可能な記憶媒体が提供される。記憶媒体の少なくとも一部分は、実行可能なアプリケーションに関連するチェックサムを表わすデータを含む。少なくとも一つのプロセッサで実行した場合、コンピュータで実行可能な命令によって少なくとも一つのプロセッサは複数のデータ記憶領域内のデータ、同一の実行可能なプログラムを定義する各データ記憶領域内のデータに対して個別の検証番号を計算し、複数のデータ記憶領域内の各々に対して個別に計算された番号を保存されている番号と比較し、計算された検証番号が保存されている番号と一致しなかった場合、個別に計算された検証番号が複数のデータ記憶領域の中の任意の一つに保存された番号と一致する場合には複数のデータ記憶領域の一つのデータをコピーし、さらに、複数のデータ記憶領域の中の一つに保存されたデータによって定義されたプログラムを実行する。有利には、実行可能なアプリケーションは飛行管制プログラムを含んでいてもよい。有利には、コンピュータで実行可能な命令によって、少なくとも一つのプロセッサは、各データ記憶領域に対して計算された検証番号が、保存されているデータによって定義されたプログラムの実行に先立って、保存された番号と一致することを検証することができる。

【０００９】

しかも本発明のさらなる態様により、メモリソースからプログラムを実行する方法が提供されている。この方法は、複数のデータ記憶領域内のデータ、同一の実行可能なプログラムを定義する各データ記憶領域内のデータに対して個別の検証番号を計算するステップ、データ記憶領域内の各々に対して個別に計算された番号と保存されている番号とを比較するステップ、個別に計算された検証番号が保存されている番号と一致しなかった場合、個別に計算された検証番号が複数のデータ記憶領域の中の任意の一つに保存された番号と一致する場合には複数のデータ記憶領域の一つのデータを複製するステップ、さらに、複数のデータ記憶領域の中の一つに保存されたデータによって定義されたプログラムを実行するステップを含む。好ましくは、この方法は、各データ記憶領域に対して個別に計算された検証番号が、保存されているデータによって定義されたプログラムの実行に先立って、保存された番号と一致することを検証するステップをさらに含むことができる。有利には、個別の検証番号を計算する場合には、この方法は、航空機搭載の航空電子工学機器に対する飛行管制プログラムのチェックサムを計算するステップ、及び同一の実行可能なプログラムを定義するデータのチェックサムを計算するためのブートＲＯＭデバイス内の命令を実行するステップのうちの少なくとも一つを含むことができる。

【００１０】

既に説明した特徴、機能及び利点は、様々な実施形態で独立に実現することが可能であるか、以下の説明及び図面を参照してさらなる詳細が理解されうる、さらに別の実施形態で組み合わせることが可能である。

【図面の簡単な説明】

【００１１】

【図１】図１は検証プロセスのフロー図である。

【図２】図２は種々の記憶領域内のアプリケーションの複数のイメージを示す処理システムの図である。

【図３】図３はデータ処理システムの図である。

【図４】図４は検証プロセスのフロー図である。

【発明を実施するための形態】

【００１２】

説明されている実施形態は、例えば、実行前にデータが読み込まれる不揮発性メモリに保存されるデータ（例えば、オペレーティングシステムファイル、アプリケーション、及び例えば重要なシステムファイル、カーネルファイル、コンフィギュレーションファイルなどを含むコンピュータシステムの初期化に必要となるその他の情報）の検証を対象としている。例示的な実施形態では、検証試験が失敗した場合には（例えば、チェックサム試験が失敗する場合）、同一データの２次ソースを利用することができる。データの２次ソースが検証試験に合格した場合には、データは２次ソースに関連するメモリから読み込まれ、実行される。幾つかの実施形態では、検証済みの２次ソース内のデータのコピーは、１次メモリの中で検証できなかったデータを上書きすることがある。メモリデバイスの容量が増大し且つ物理的なサイズが小さくなるにつれて、３倍、４倍、５倍、さらにはｎ倍までのデータソースを想定することができるため、不具合の発生を示す前に実行用のアプリケーションの読み込み時に複数回の実行を試みることができる。このような実施形態はまた、他のソースからの有効なファイルで破損したファイルを上書きすることを可能にし、結果的に「自己修復」機能を提供する。

【００１３】

本明細書に記載されているように、基本入出力システム（ＢＩＯＳ）に追加命令が付加されている。この命令により、例えば、オペレーティングシステムの内容、アプリケーション及びシステムを初期化するための他の保存情報から構成されるデータの検証を実行することができる。単純な例では、ＢＩＯＳで実行される命令により、不揮発性メモリに保存された航空電子工学ユニットの飛行管制プログラム（ＯＦＰ）に対する計算を行い、航空電子工学ユニットすなわち「ブラックボックス」によって実行されるように意図することができる。ＢＩＯＳはさらに、計算されたチェックサムがＯＦＰ用に保存されたチェ

ックサムに等しく、チェックサムは例えばＢＩＯＳに関連するメモリに保存されていることを検証する。

【００１４】

図１に関してさらに説明されているように、チェックサムが等しい場合には、ＢＩＯＳによってＯＦＰの作動が許可される、及び／又はＯＦＰが実行される。チェックサムが等しくない場合には、ＢＩＯＳはＯＦＰの別のインスタンスが保存されている別のメモリロケーションに移動し、チェックサムの計算及び保存されているチェックサムに対する検証を可能にする。このプロセスは、検証可能なチェックサムを有するイメージが検出されるまで、ＯＦＰの複数のミラーイメージに対して反復することが可能で、検出された時点で当該イメージは実行可能となるか、実行可能となるメモリ内へ転送可能となる。さらに、チェックサム検証試験に合格するＯＦＰのイメージは、チェックサムが検証できないメモリロケーションにコピーすることが可能で、将来のシステムのブートアップで実行することができるＯＦＰの検証可能なコピーを生成することができる。この実施形態では、ＢＩＯＳが実行されるブートＲＯＭは、データの２次（３次など）ソースの（メモリ）ロケーションで構成されている。

【００１５】

上述の考え方は図１のフローチャート１０を用いて容易に視覚化することができる。実際の手順は様々な方法で実行可能であるが、一又は複数のデータソースがデータの１次ソースの読み込み、実行、及び交換のための機能を処理することによってアクセス可能であるという点において、すべてが一貫している。フローチャート１０を参照すると、１次データ記憶領域に対する検証番号は計算（１２）され、計算された検証番号はチェックサムなどの保存された値と比較（１４）される。検証番号と保存されている番号が一致する場合（１６）には、１次データ記憶領域に保存されているプログラムは読み込まれ、実行（１８）される。

【００１６】

検証番号と保存されている番号が一致しない場合（１６）には、１次データ記憶領域にあるべきデータの正確なコピーを含んでいなければならない２次データ記憶領域に対する検証番号が計算（２０）される。２次データ記憶領域に対して計算（２０）された検証番号は、保存されている番号と比較（２２）される。検証番号と２次データ記憶領域に関連して保存されている番号とが一致する場合（２４）には、２次データ記憶領域に保存されているプログラムは実行（２６）される。

【００１７】

検証番号と２次データ記憶領域に関連して保存されている番号とが一致しない場合（２４）には、ユニットは故障（２８）しているものとみなすことができる。２次データ記憶領域のプログラムの実行は、さまざまな方法で実現することができる。プログララムは２次データ記憶領域から直接実行すること（２６）が可能で、又は、１次データ記憶領域から実行できるように、２次データ記憶領域のデータは１次データ記憶領域にコピー（３０）することが可能である。代替的に、プログラムを２次記憶領域から実行し、次に一旦プログラムが読み込まれると自己修復機能として、１次記憶領域にコピー（３０）してもよい。別の実施形態では、２次データ記憶領域に保存されているプログラムは、当該プログラムが実行できるメモリから読み込まれる。

【００１８】

図１に関連する最も単純な実施例では、データ検証機能（計算された番号と保存されている番号との比較）が１次メモリロケーションに関して合格した場合には、このようなメモリロケーションでプログラムが実行される（１８）。しかしながら、当業者であれば、図１によって図解されたプロセスは必ずしも２個のデータ記憶領域に限定されないことを理解するであろう。ある種のアプリケーションでは、データ検証機能がｎ個のデータ記憶領域に関して実行されるものと想定されている。

【００１９】

特に、検証番号の計算は、チェックサムなどの値の計算を含むことがある。図２は、

１次データ記憶領域、２次データ記憶領域、３次記憶領域及びｎ次記憶領域などが複数の方法で具現化されうることを示している。図２で、プロセッサ１００はＢＩＯＳが保存されるブートＲＯＭデバイス１０２に結合している。ブートＲＯＭデバイス１０２の一部は、プロセッサ１００によって実行されるアプリケーションに対するチェックサム１０４（又は複数のアプリケーションに対する複数のチェックサム）を保存する。メモリ１１０は実行されるアプリケーションの１次イメージ１１２を含む。本明細書に記載されているように、プロセッサ１００、ブートＲＯＭ１０２、及びメモリ１１０を組み込んでいるデバイスは、複数のメモリデバイス、例えば、メモリデバイス１２０及び１３０を含むように構成されうる。図２の例に示したように、メモリデバイス１２０は実行されるアプリケーションの２つのイメージ（１２２及び１２４）で構成されており、メモリデバイス１３０は実行されるアプリケーションの単一イメージ１３２で構成されている。

【００２０】

メモリデバイス１２０の実施例では、データ記憶領域は単一メモリデバイス内で分離されたパーティションであってもよい。他の実施例では、データ記憶領域は物理的に分離されたメモリデバイス（例えば、ハードドライブ、シリコンメモリデバイス、ＣＤ－ＲＯＭ、フラッシュドライブ、サムドライブなど）として具現化されうる。さらに別の実施例では、データ記憶領域は同一形式の物理的に分離されたメモリデバイス（例えば、分離された回路基板上のメモリデバイス）として具現化されうる。また、本明細書で記載されている機能を実現するためには、多数の物理メモリデバイスの実施形態及び構成の組み合わせが利用可能である。

【００２１】

さらに、実施形態は飛行管制プログラムに限定されない。検証されるデータは、オペレーティングシステム、アプリケーション、及び／又はメモリに保存されるシステムの初期化に必要な他の情報を含みうる。この実施形態では、メモリに保存されるデータは、実行用に読み込まれる前に、又はＢＩＯＳがオペレーティングシステムにシステムの制御を引き渡す前に有効となる（検証される）。有効化が失敗した場合には、このようなデータの２次ソースが利用され、検証試験に合格するものとみなされる。

【００２２】

さらに、２次データソースの一つのデータをメモリから読み込んで１次データメモリにコピーすることができる。例えば、再度図２を参照すると、イメージ１１２が１次イメージであって、イメージ１１２に対して計算された検証がブートＲＯＭ１０２に保存されているチェックサム１０４とが一致せず、イメージ１３２がブートＲＯＭ１０２に保存されているチェックサムと一致しない場合には、ブートＲＯＭ１０２はイメージ１３２をメモリ１１０にコピーする命令を含むように構成することができ、各実施形態を説明するためにイメージ１１２は破損したものとみなし、上書きすることができる。

【００２３】

ある種のアプリケーションでは、例えば、上述の航空機搭載の航空電子工学システムでは、様々な場所での運用に必要となるソフトウェア及びデータを多数コピーすることにより、システムの冗長性が高まり、ブートアップ及び最終的にはシステムの運用を阻害する問題の自動訂正が可能になる。オペレータがいる場合でも、機能が自動化され、時間が節約される。

【００２４】

一つの実施形態では、本明細書に記載されているメソッド、システム、及びコンピュータで読み込み可能な媒体の技術的な効果は、（ａ）デバイスのデータ記憶領域内に実行可能なプログラムを構成するデータが、例えば、これらのデータが保存されているチェックサムに等しいことによって、予想通りであることを検証すること、（ｂ）検証試験に合格した場合、データ記憶デバイスに関連するプログラムを実行すること、（ｃ）デバイスの種々のデータ記憶領域内の実行可能なプログラムを構成するデータが、例えば、これらのデータが保存されているチェックサムに等しいことによって、予想通りであることを検証することを試みること、（ｄ）検証試験に合格した場合、種々のデータ記憶デバイスの

プログラムを実行すること、（ｅ）デバイスが後に元のデータ記憶領域からプログラムを実行できるように、種々のデータ記憶領域から元のデータ記憶領域にプログラムを潜在的にコピーすること、のうちの少なくとも一つを含む。

【００２５】

次に図３に注目すると、データ処理システムのより詳細な図が、例示的な実施形態に従って図解されている。この例示的な実施例では、データ処理システム３００は、通信ファブリック３０２を含み、これによりプロセッサ装置３０４、メモリ３０６、固定記憶域３０８、通信装置３１０、入出力（Ｉ／Ｏ）装置３１２、及び表示装置３１４の間の通信を可能にする。種々の実施形態では、システム３００は汎用パーソナルコンピュータ又は航空機搭載の航空電子工学ユニットを表わしている。

【００２６】

プロセッサ装置３０４は、メモリ３０６に読み込まれうるソフトウェアに対する命令を実行するように働く。プロセッサ装置３０４は、特定の実装に応じて、一又は複数のプロセッサの組であってもよく、あるいはマルチプロセッサコアであってもよい。さらに、プロセッサ装置３０４は、単一チップ上に様々な種類のプロセッサが共存する異種プロセッサシステムを一又は複数個使用して実装してもよい。別の例示的な実施例では、プロセッサ装置３０４は同一形式の複数のプロセッサを含む対称型マルチプロセッサシステムであってもよい。

【００２７】

メモリ３０６及び固定記憶域３０８は、ＯＦＰなどのアプリケーションのイメージ（又はイメージ群）が保存される様々な記憶デバイスの例である。本明細書で使用しているように、記憶デバイスは、一時的又は永続的に情報を保存することが可能な任意の数のハードウェアである。これらの例では、メモリ３０６は、例えば、限定しないが、ランダムアクセスメモリ（ＲＡＭ）又は他の好適な揮発性又は不揮発性の記憶デバイスであってもよい。メモリ３０６の一部は、先行するパラグラフで説明したように、ブートＲＯＭデバイスとして構成してもよい。固定記憶域３０８は特定の実装に応じて様々な形態をとりうる。例えば、限定しないが、固定記憶域３０８は一又は複数のコンポーネント又はデバイスを含みうる。例えば、固定記憶域３０８は、ハードドライブ、フラッシュメモリ、書換型光ディスク、書換型磁気テープ、又はこれらの組み合わせであってもよい。固定記憶域３０８によって使用される媒体は着脱式であってもよい。例えば、限定しないが、着脱式ハードドライブは固定記憶域３０８に使用しうる。

【００２８】

通信装置３１０はこれらの例では、他のデータ処理システム又はデバイスとの通信を提供する。これらの例では、通信装置３１０はネットワークインターフェースカード（ＮＩＣ）である。通信装置３１０は、物理的及び無線の通信リンクのいずれか一方又は両方を使用することによって、通信を提供することができる。

【００２９】

入出力装置３１２により、データ処理システム３００に接続可能な他のデバイスによるデータの入力及び出力が可能になる。例えば、限定しないが、入出力装置３１２はキーボード及びマウスによるユーザー入力のための接続を提供しうる。さらに、入出力装置３１２は出力をプリンタに送ってもよい。表示装置３１４はユーザーに情報を表示する機構を提供する。

【００３０】

オペレーティングシステム及びアプリケーション又はプログラムに対する命令は、固定記憶域３０８上に配置される。これらの命令は、プロセッサ装置３０４によって実行するため、メモリ３０６に読み込まれうる。異なる実施形態のプロセスは、メモリ３０６などのメモリに配置されうる命令を実装したコンピュータを使用して、プロセッサ装置３０４によって実行されうる。これらの命令はマシンコードと呼ばれ、プロセッサ装置３０４のプロセッサによって読み込まれ実行される。種々の実施形態のマシンコードは、メモリ３０６又は固定記憶域３０８など、種々の物理的な又は有形のコンピュータで読込可能な

媒体上に具現化しうる。

【００３１】

追加的に、又は代替的に、マシンコード３１６は、選択的に着脱可能でコンピュータで読込可能な媒体３１８上に機能的な形態で配置され、プロセッサ装置３０４での実行用のデータ処理システム３００に読込み又は転送することができる。マシンコード３１６及びコンピュータで読込可能な媒体３１８は、これらの実施例ではコンピュータプログラム製品３２０を形成する。１つの実施例では、コンピュータで読込可能な媒体３１８は、例えば、固定記憶域３０８の一部であるハードドライブなどの記憶デバイスに転送するための固定記憶域３０８の一部であるドライブまたは他のデバイスに挿入又は配置される光ディスク又は磁気ディスクなど、有形の形態をとりうる。有形の形態では、コンピュータで読込可能な媒体３１８はまた、データ処理システム３００に接続されているハードドライブ、サムドライブ、又はフラッシュメモリなどの固定記憶域の形態をとりうる。コンピュータで読込可能な媒体３１８の有形の形態はまた、コンピュータで記録可能な記憶媒体とも呼ばれる。幾つかの例では、コンピュータで読込可能な媒体３１８は着脱式ではないことがある。

【００３２】

代替的に、マシンコード３１６は、通信装置３１０との通信リンク及び／又は入出力装置３１２との接続によって、コンピュータで読取可能な媒体３１８からデータ処理システム３００に転送することができる。通信リンク及び／又は接続は、例示的な実施例で物理的なもの又は無線によるものでありうる。コンピュータで読込可能な媒体はまた、マシンコードを含む通信リンク又は無線転送など、無形の形態をとりうる。

【００３３】

幾つかの例示的な実施形態では、マシンコード３１６は、データ処理システム３００内で使用するため、他のデバイス又はデータ処理システムから、ネットワークを介して固定記憶域３０８へダウンロードすることができる。例えば、データ処理サーバーのコンピュータで読取可能な記憶媒体に保存されたマシンコードは、ネットワークを介してサーバーからデータ処理システム３００にダウンロードすることができる。マシンコード３１６を提供するデータ処理システムは、ホストコンピュータ、クライアントコンピュータ、又はマシンコード３１６を保存及び転送することができる他のデバイスであってもよい。

【００３４】

データ処理システム３００に対して例示されている種々のコンポーネントは、異なる実施形態が実装しうる方法に対して構造上の制限を設けることを意図していない。異なる例示的実施形態は、データ処理システム３００に対して図解されているコンポーネントに対して追加的又は代替的なコンポーネントを含むデータ処理システム内に実装しうる。図３に示した他のコンポーネントは、実施例とは異なることがある。

【００３５】

１つの実施例では、データ処理システム３００の記憶装置は、データを保存しうる任意のハードウェア装置である。メモリ３０６、固定記憶域３０８及びコンピュータで読込可能な媒体３１８は有形の記憶デバイスの例である。

【００３６】

他の実施例では、バスシステムは通信ファブリック３０２を実装するために使用可能で、システムバス又は入出力バスなどの一又は複数のバスを含みうる。言うまでもなく、このバスシステムは、当該バスシステムに結合された様々なコンポーネント又はデバイス間でのデータ転送を可能にする、任意の好適な形式のアーキテクチャを用いて実装することができる。また、通信装置は、モデム又はネットワークアダプタなど、データの送受信に使用される一又は複数のデバイスを含むことができる。さらに、メモリは例えば、限定しないが、通信ファブリック３０２によってアクセス可能な外部メモリ又はメモリ制御装置を介してみられるような、メモリ３０６又はキャッシュであってもよい。

【００３７】

図４は検証プロセスの代替的な実装を示すフロー図４００である。上述の実施形態は、

当該記憶領域からプログラムが実行されるとすぐに、適切なチェックサムを有するプログラム記憶領域が見つかるまで、プログラム記憶領域のチェックサムを計算するプロセスについて説明した。フローチャート４００は、第１のプログラム記憶領域がチェックサム試験に合格した場合でも、すべてのプログラム記憶領域が検証されるプロセスを図解している。すべてのプログラム記憶領域の内容を検証することにより、プログラム記憶領域２～ｎが破損しているが、プログラム記憶領域１は常に検証試験に合格しているため、このような破損は検出されない、というシナリオは回避される。もしプログラム記憶領域２～ｎの破損が検出されないままであると、プログラム記憶領域１が検証試験に合格しないことがあれば、プログラム記憶領域１～ｎを取り込んでいるユニットは不必要に動作不能となるだろう。

【００３８】

次にフローチャート４００を参照すると、１次アドレス（プログラム記憶領域１）用のデータ検証機能が実施される（４０２）。具体的には、先行する段落で説明した内容と同様に、検証番号が計算され、保存されている番号と比較され、比較の結果が保存される。データ検証機能は２次アドレス（プログラム記憶領域２）に対して実施（４０４）され、結果が保存される。同様に、ｎ次アドレス（プログラム記憶領域ｎ）の残りの部分に対しても実施され、結果が保存される。

【００３９】

一つのシナリオでは、すべてのプログラム記憶領域が検証試験に合格する。具体的には、プログラムが１次アドレスから実行されるポイントで、１次アドレスでの比較４１０が合格したこと、２次アドレスでの比較４１２が合格したこと、及びｎ次アドレスでの比較４１４が合格したことが検証されている。

【００４０】

別のシナリオでは、プログラム記憶領域の多く又はすべてが検証試験に合格しない。具体的には、１次アドレスでの比較４１０が合格しなかったこと、２次アドレスでの比較４２０が合格しなかったこと、及びｎ次アドレスのうちの一又は複数で比較４２２が合格しなかったことを検証した場合には、何であれ最終的に検証試験に合格したｎ次アドレスのうちの一つで最終的にプログラムが実行（４３０）される。ｎ次アドレスのうちの一つも合格しない場合には、ユニットの不具合（４２４）が発生し、通知（例えば、報告）されることがある。しかしながら、ｎ次アドレスのうちの一つで比較４２２が合格した場合には、そのプログラム記憶領域のデータが、１次プログラム領域、２次プログラム記憶領域、及び比較が合格しなかったｎ次プログラム記憶領域の任意の領域にコピー（４３０）される。次に、１次プログラム記憶領域、２次プログラム記憶領域又は比較が合格したｎ次プログラム記憶領域のうちの一つのいずれかからプログラムが実行（４３２）される。

【００４１】

１次アドレスでの比較４１０が合格せず、２次アドレスでの比較４２０が合格したが、ｎ次アドレスのうちの一又は複数で比較４４０のうちの一つが合格しなかったシナリオでは、２次プログラム記憶領域のデータが、１次プログラム記憶領域及び比較が合格しなかったｎ次プログラム記憶領域のいずれかにピー（４４２）され、プログラムは最終的に１次プログラム記憶領域、２次プログラム記憶領域又はｎ次プログラム記憶領域のうちの一つのいずれかから実行される。

【００４２】

同様に、１次アドレスでの比較４１０が合格せず、２次アドレスでの比較４２０が合格し、且つｎ次アドレスでの比較４４０のすべてが合格したシナリオでは、２次プログラム記憶領域又はｎ次プログラム記憶領域のうちの一つのデータが、１次プログラム記憶領域に複写（４５０）され、プログラムは最終的に１次プログラム記憶領域、２次プログラム記憶領域又はｎ次プログラム記憶領域のうちの一つのいずれかから実行（４５２）される。

【００４３】

最終的に、１次アドレスでの比較４１０が合格し、２次アドレスでの比較４１２が合格

し、且つｎ次アドレスでの比較４１４のうちの少なくとも一つが合格しなかったシナリオでは、１次プログラム記憶領域又は２次プログラム記憶領域のうちの一つのデータが、比較４１４が合格しなかったｎ次プログラム記憶領域に複写（４６０）され、プログラムは最終的に１次プログラム記憶領域、２次プログラム記憶領域又はｎ次プログラム記憶領域のうちの一つのいずれかから実行（４６２）される。

【００４４】

上述の方法及びシステム構成は、当該プログラムに対する１次記憶ローケーションが破損している場合であっても、プログラムを確実に実行するため、実行可能である。これまでは、又特に、航空機搭載の航空電子工学システムに関連してスペース及び重量が厳しく制約されている場合には、「追加の」プログラムイメージを保存するための単純な追加メモリのための物理的なスペースが確保できなかった。しかしながら、メモリデバイスの物理的な大きさが小さくなる一方で、記憶容量は増大し続けたため、本明細書に記載した構成が実現可能になってきた。種々の実施形態により、保存されているプログラムのイメージが破損している可能性がある場合でも、「健全」であることが確認されているアプリケーションイメージをコピーすることにより、ユニットは少なくとも一定のレベルでの自己修復を行うため、修理を目的とした航空機からのユニット取り外しを減らすことが可能になっている。

【００４５】

本明細書で使用しているように、「一つの」という語から始まって単数形で記載されている要素又はステップは、複数の要素又はステップを除外することが明示的に記載されていない限り、複数の要素又はステップを除外しないと理解すべきである。さらに、本発明の「一つの実施形態」又は「例示的実施形態」への言及は、記載されている機能をも取り込む付加的な実施形態の存在を除外するように解釈されることを意図していない。

【００４６】

種々の有利な実施形態の説明は、例示及び説明を目的として提示されているものであり、網羅的な説明であること、又は開示された形態に実施形態を限定することを意図していない。当業者には、多数の修正例及び変形例が明らかであろう。さらに、種々の有利な実施形態は、他の有利な実施形態に照らして別の利点を提供することができる。選択された一又は複数の実施形態は、実施形態の原理、実際の用途を最もよく説明するため、及び他の当業者に対し、様々な実施形態の開示と、考慮される特定の用途に適した様々な修正との理解を促すために選択及び記述されている。

【００４７】

本明細書では、最良のモードを含め、様々な実施形態を開示する実施例を使用しているため、当業者は任意の機器やシステムの作成ならびに使用、及び組込まれた任意の方法の実施を含む実施形態を実行することができる。特許可能な範囲は特許請求の範囲によって定義されており、当業者であれば想起される他の実施例も含みうる。このような他の実施例は、それらが特許請求の範囲の文字言語から逸脱しない構造要素を有する場合、あるいは、それらが特許請求の範囲の文字言語とごくわずかな相違を有する等価な構造要素を含んでいる場合は、特許請求の範囲の範囲内にあることを意図している。

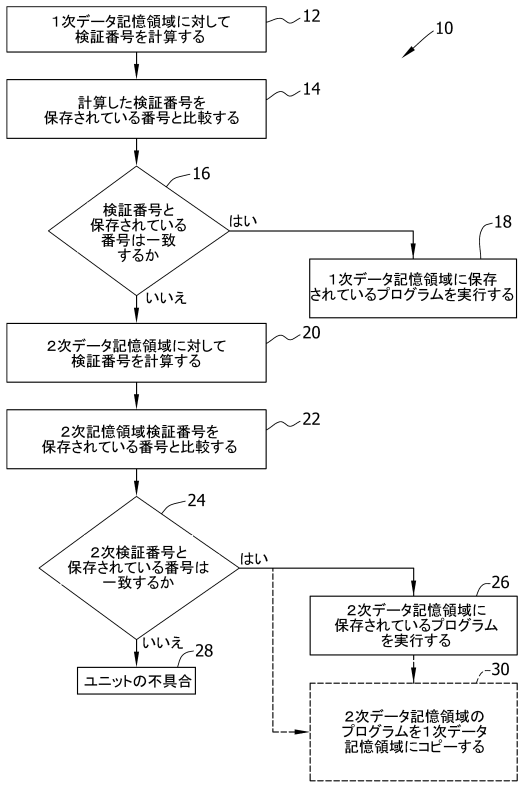
【符号の説明】

【００４８】

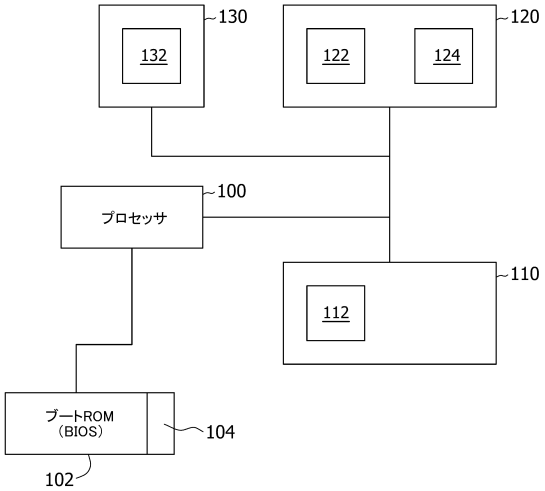
１００　プロセッサ
１０２　ブートＲＯＭ（ＢＩＯＳ）
１０４　チェックサム
１１２　アプリケーションの１次イメージ
１２０、１３０　メモリデバイス
１２２、１２４　アプリケーションのイメージ
１３２　アプリケーションの単一イメージ
３００　データ処理システム
３０２　通信ファブリック

３０４　プロセッサ装置
３０６　メモリ
３０８　固定記憶域
３１０　通信装置
３１２　入出力装置
３１４　表示装置
３１６　マシンコード
３１８　コンピュータで読込み可能な媒体
３２０　コンピュータプログラム製品

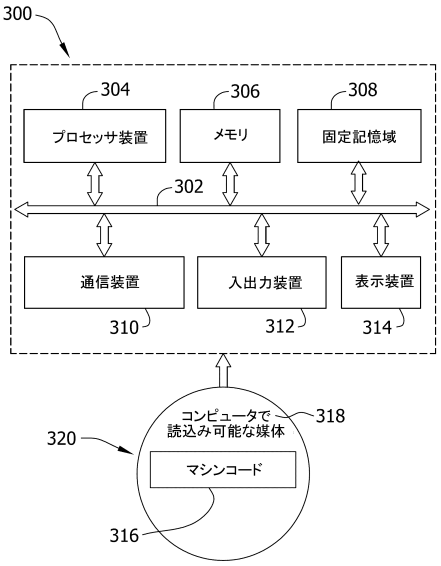
【図１】



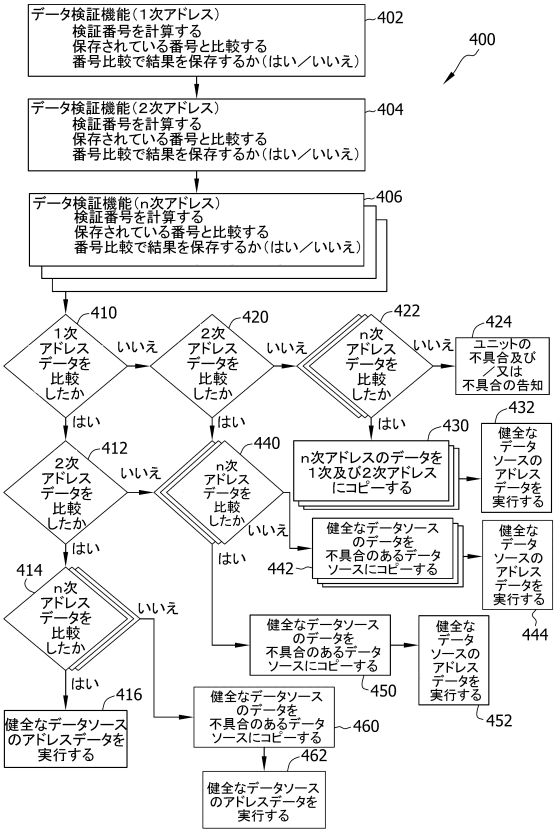
【図２】



【図３】


300
304
306
308
プロセッサ装置
メモリ
固定記憶域
302
通信装置
入出力装置
表示装置
310
312
314
コンピュータで
読込み可能な媒体
318
320
マシンコード
316

【図４】


400
データ検証機能（1次アドレス）
検証番号を計算する
保存されている番号と比較する
番号比較で結果を保存するか（はい／いいえ）
402
データ検証機能（2次アドレス）
検証番号を計算する
保存されている番号と比較する
番号比較で結果を保存するか（はい／いいえ）
404
データ検証機能（n次アドレス）
検証番号を計算する
保存されている番号と比較する
番号比較で結果を保存するか（はい／いいえ）
406
1次アドレスデータを比較したか
410
2次アドレスデータを比較したか
420
n次アドレスデータを比較したか
422
ユニットの不具合及び／又は不具合の告知
424
いいえ
はい
2次アドレスデータを比較したか
412
n次アドレスデータを比較したか
440
n次アドレスのデータを1次及び2次アドレスにコピーする
430
健全なデータソースのアドレスデータを実行する
432
健全なデータソースのデータを不具合のあるデータソースにコピーする
442
健全なデータソースのアドレスデータを実行する
444
n次アドレスデータを比較したか
414
健全なデータソースのデータを不具合のあるデータソースにコピーする
450
健全なデータソースのアドレスデータを実行する
452
健全なデータソースのアドレスデータを実行する
416
健全なデータソースのデータを不具合のあるデータソースにコピーする
460
健全なデータソースのアドレスデータを実行する
462

フロントページの続き

(72)発明者 ウィッカム, ティモシー エス.
アメリカ合衆国 カリフォルニア ９２６４７, ハンティントン ビーチ, コッド サークル １６９０１－ビー
(72)発明者 タルボット, マーク エー.
アメリカ合衆国 カリフォルニア ９２６４６, ハンティントン ビーチ, ダンブレック ドライヴ ９６３１
(72)発明者 ウェルブルック, グレゴリー エム.
アメリカ合衆国 カリフォルニア ９０８１５, ロング ビーチ, ラドガ アヴェニュー ２６４６
(72)発明者 ワン, チャーリー シー.
アメリカ合衆国 カリフォルニア ９２６４７, ハンティントン ビーチ, ウッドストリーム サークル １６９１１ ８０番
(72)発明者 ミレレス, オスカー
アメリカ合衆国 カリフォルニア ９０６３８, ラ ミラダ, マーレット ドライヴ １３０４７
(72)発明者 ルービン, マイケル ディー.
アメリカ合衆国 テキサス ７８６４１, リアンダー, サドル ブランケット プレイス ２７１９

審査官 石川 亮

(56)参考文献 特開２００８－０８４２９１（ＪＰ，Ａ）
特開２００６－２２９９５６（ＪＰ，Ａ）
特開２０１１－００８５５２（ＪＰ，Ａ）
特開２００９－１５５０９２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｆ ９／４４５
Ｇ０６Ｆ １１／００