

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第3671178号

(P3671178)

(45) 発行日 平成17年7月13日(2005. 7. 13)

(24) 登録日 平成17年4月22日(2005. 4. 22)

(51) Int. Cl.⁷

G06F 1/00

F I

G06F 9/06 660G

請求項の数 10 (全 19 頁)

(21) 出願番号	特願2002-523772 (P2002-523772)	(73) 特許権者	500470703
(86) (22) 出願日	平成13年8月28日 (2001. 8. 28)		コンテンツガード ホールディングズ インコーポレイテッド
(65) 公表番号	特表2004-507845 (P2004-507845A)		Content Guard Holdings, Inc.
(43) 公表日	平成16年3月11日 (2004. 3. 11)		アメリカ合衆国 19803 デラウェア州 ウィルミントン スイート 200-エム フォーク ロード 103
(86) 国際出願番号	PCT/US2001/026634		
(87) 国際公開番号	W02002/019598	(74) 代理人	100079049
(87) 国際公開日	平成14年3月7日 (2002. 3. 7)		弁理士 中島 淳
審査請求日	平成15年7月1日 (2003. 7. 1)	(74) 代理人	100084995
(31) 優先権主張番号	09/649, 838		弁理士 加藤 和詳
(32) 優先日	平成12年8月28日 (2000. 8. 28)	(74) 代理人	100085279
(33) 優先権主張国	米国 (US)		弁理士 西元 勝一
早期審査対象出願			

最終頁に続く

(54) 【発明の名称】 コンテンツ使用環境における完全性認証及び検証提供システム

(57) 【特許請求の範囲】

【請求項 1】

コンテンツ使用環境における完全性認証及び検証提供システムであって、
 該システムは、
 前記完全性認証及び検証デバイスと、
 前記完全性認証及び検証デバイスに接続される少なくとも一のユーザ・システムと、
 前記少なくとも一のユーザ・システムに少なくとも一のコンテンツを提供する少なくとも一のコンテンツ・プロバイダと、
 前記少なくとも一のユーザ・システムに前記少なくとも一のコンテンツのアクセスに使用する少なくとも一のアプリケーション、システム、又は、システムコンポーネントを提供する少なくとも一のコンテンツ使用システム／アプリケーション・プロバイダと、
 を備え、
 前記完全性認証及び検証デバイスは、
 前記少なくとも一のアプリケーション、システム又はシステムコンポーネントに関する認証情報を記憶するコンポーネント登録デバイスと、
 前記認証情報に基づいて設定される、前記少なくとも一のアプリケーション、システム又はシステムコンポーネントの真正性を決定するために使用される検証可能情報を含む少なくとも一の完全性プロファイルを記憶する完全性プロファイルデバイスと、
 を含み、
 前記完全性認証及び検証デバイスは、前記少なくとも一のコンテンツ・プロバイダの要

10

20

求に応じて、該少なくとも一のコンテンツ・プロバイダが前記少なくとも一のユーザ・システムに提供する保護された少なくとも一のコンテンツに対応するアプリケーション、システム又はシステム・コンポーネントに関する前記完全性プロファイルを、該少なくとも一のユーザ・システムに送信し、該完全性プロファイルにより該アプリケーション、システム又はシステム・コンポーネントの真正性が決定された場合、該少なくとも一のユーザ・システムにおいて該コンテンツの保護を解除してアクセス可能とする、
完全性認証及び検証提供システム。

【請求項 2】

前記完全性プロファイルが、前記コンポーネント登録デバイスに記憶された認証情報を有する登録されたアプリケーション、システム又はシステムコンポーネントの識別を含む、請求項 1 に記載のシステム。

10

【請求項 3】

前記プロファイルデバイスが、前記完全性プロファイルを保持するプロファイルデータベースを含む、請求項 1 に記載のシステム。

【請求項 4】

前記完全性プロファイルにおいて指定されるアプリケーション、システム又はシステムコンポーネントの識別のうち 1 つ以上を、コンテンツ使用環境の 1 つ以上のアプリケーション、システム又はシステムコンポーネントと比較することによって真正性を検証するプロファイル検証デバイスを更に含む、請求項 1 に記載のシステム。

【請求項 5】

20

前記 1 つ以上のアプリケーション、システム又はシステムコンポーネントに関する前記認証情報をコンテンツ使用アプリケーション、システム又はシステムコンポーネントプロバイダから取得し、前記認証情報を前記コンポーネント登録デバイスに提供する登録アプリケーションデバイスを更に含む、請求項 1 に記載のシステム。

【請求項 6】

前記完全性プロファイルが、前記環境の前記 1 つ以上のアプリケーション、システム又はシステムコンポーネントの識別を含む、請求項 1 に記載のシステム。

【請求項 7】

前記少なくとも一のコンテンツプロバイダは、ネットワークを介して前記コンテンツ使用環境において、前記完全性認証及び検証デバイスと接続されている、請求項 1 に記載のシステム。

30

【請求項 8】

前記少なくとも一のコンテンツ使用システム／アプリケーション・プロバイダは、ネットワークを介して前記コンテンツ使用環境において、前記完全性認証及び検証デバイス接続されている、請求項 1 に記載のシステム。

【請求項 9】

前記 1 つ以上のアプリケーション、システム又はシステムコンポーネントが真正ではないとプロファイル検証デバイスが判断した場合、前記少なくとも一のコンテンツへのアクセスを無効にする、請求項 1 に記載のシステム。

【請求項 10】

40

前記コンポーネント登録デバイスに記憶された前記 1 つ以上のアプリケーション、システム又はシステムコンポーネントに関する前記認証情報に基づいて前記完全性プロファイルを作成する作成デバイスを更に含む、請求項 1 に記載のシステム。

【発明の詳細な説明】

【0001】

本発明は、完全性の認証及び検証に関する。特に、本発明は、コンテンツ使用環境内での完全性の認証及び検証に関する。

【0002】

電子商取引によるデジタルドキュメントの広範囲に及ぶ配布を妨げる最も重要な問題の 1 つは、現在のところ、デジタルドキュメントの配布及び使用の際に、コンテンツ所有

50

者及びコンテンツプロバイダの知的財産権に対して有効な保護が存在しないことである。この問題を解決するための努力の成果が、知的財産権管理（I P R M）、デジタル財産権管理（D P R M）、知的財産管理（I P M）、デジタル権管理（D R M）、権利管理（R M）、及び電子著作権管理（E C M）と呼ばれるものである。

【0003】

コンテンツプロバイダは、所望の特徴及び／又は動作を有する認証されたアプリケーション及びシステムによるコンテンツの使用を望むことが多い。公開鍵基盤（P K I）を直接使用することにより、アプリケーション及びシステムのプロバイダは自身の製品を認証することができ、コンテンツプロバイダはコンテンツの使用に用いられるアプリケーション及びシステムの完全性を検証することができる。

10

【0004】

しかしながら、P K I を直接使用すると、ベンダとプロバイダとの間に多対多関係が生じてしまう。このタイプの関係は拡張性が良くないため、この関係の管理及び有効なリアルタイムの完全性の検証の達成は不可能ではないが困難である。

【0005】

コンテンツプロバイダは、所望の特徴及び／又は動作を有する認証されたアプリケーション及びシステムによるコンテンツの使用を望むことが多い。コンテンツ使用環境のこれらの面を制御することにより、コンテンツプロバイダは、例えばコピー、印刷、組込、配布などの使用を制限することができる。

【0006】

例えば、コンテンツプロバイダは、コンテンツの誤用からの保護を望み、コンテンツを使用するシステムが一定レベルのセキュリティ及び権利管理機能を有することを要求することもある。また、コンテンツプロバイダは、例えばデバッグ、ウイルス、妨害ルーチンなど、コンテンツ又は他の機密情報を押収するか又は「盗み出す」可能性のある、「異質な」アプリケーションがユーザシステムのコンテンツ使用アプリケーションと交信しないことの保証を望む場合がある。例えば、本願と共に出願され、その全ての内容が本明細書中に援用されている、「ドキュメント配布管理方法、標準レンダリングエンジンを用いた装置、並びに標準レンダリングエンジン制御方法及び装置」というタイトルの代理人整理番号111325 000002は、ユーザのドキュメントへのアクセスを制限するためにユーザシステムの機能性の管理を可能にしている。

20

【0007】

所与のアプリケーション及びシステムが所望の特徴及び動作を有することを認証するために、コンテンツの使用に必要な全てのアプリケーション及びシステムコンポーネントの検証を、検証アプリケーションによって確認する必要がある。

30

【0008】

本発明は、コンテンツ使用環境に認証サービス及び検証サービスを提供するシステム及び方法を説明する。このようなシステムでは、これらのサービスを提供する完全性認証及び検証デバイスが、コンテンツプロバイダとコンテンツ使用システム／アプリケーションプロバイダとの間に導入される。この認証デバイスは、各々のプロバイダからの個々のアプリケーション及び／又はシステムを登録し、コンテンツプロバイダに対してこれらのアプリケーション及び／又はシステムの完全性を所定の選択に従って認証する。このサービスの使用により、コンテンツプロバイダは完全性認証及び検証デバイスを「信用する」ことができる。この信用を用いて、プロバイダは、コンテンツの使用が許可されるアプリケーション及びシステムのセットのプロファイルを設定し、このプロファイルに従って、ユーザのアプリケーション及びシステムのセットが真正であることをユーザシステムにおいて検証する。

40

【0009】

特に、本発明のシステム及び方法は、例えばドキュメントなどのコンテンツの使用環境の完全性に対して認証サービス及び検証サービスを提供する。このようなシステムでは、これらのサービスを提供する完全性認証及び検証デバイスが、コンテンツプロバイダとコン

50

テンツ使用システム及びアプリケーションプロバイダとの間に導入される。コンテンツ使用システム及びアプリケーションプロバイダは、例えば、パーソナルコンピュータ、ハンドヘルドコンピュータ、PDA、マルチメディアディスプレイデバイス、DVDプレーヤ、分散型ネットワークが使用可能な電話、並びにワードプロセッサ、ドキュメントビューア、又はマルチメディアプレーヤなどのアプリケーションを分配することができる。完全性認証及び検証デバイスは、コンテンツ使用システム／アプリケーションプロバイダからの個々のアプリケーション及び／又はシステムを登録し、コンテンツプロバイダに対するこれらのアプリケーション及びシステムの完全性を認証する。このサービスを使用することにより、コンテンツプロバイダは完全性認証及び検証デバイスを選択する、即ち信用することができ、コンテンツの使用が許可されるアプリケーション及びシステムのセットのプロファイルを設定し、このプロファイルに従って、ユーザシステム上のアプリケーション及びシステムのセットが真正であることをユーザシステムにおいて検証することができる。このようにして、ユーザによって要求されるか又は提示されるコンテンツへのアクセス範囲又はコンテンツの制御範囲を制御することができる。

10

【0010】

ドキュメント（本明細書中ではこの用語が用いられる）は、配布又は転送される情報の任意の単位であり、通信文、本、雑誌、定期刊行物、新聞、他の文書、ソフトウェア、プラグイン、写真及び他の画像、オーディオクリップ及びビデオクリップ、並びに他のマルチメディア表現を含むがこれらに限定されない。ドキュメントは、用紙上に印刷された形で具体化されてもよいし、記憶媒体のデジタルデータとして具体化されてもよいし、例えばコンパクトディスク（CD）、デジタルビデオディスク（DVD）、レーザディスク、磁気媒体及び磁気光学媒体などを含む、周知であるか又は今後開発されるあらゆる他の多様な媒体又はソフトウェアとして具体化されてもよい。

20

【0011】

本発明のシステム及び方法は、完全性の認証サービス及び検証サービスを提供する。

【0012】

本発明は、コンテンツ使用システム環境用の完全性の認証サービス及び検証サービスのためのシステム及び方法を別個に提供する。

【0013】

また、本発明は、完全性プロファイルを決定するためのシステム及び方法を別個に提供する。

30

【0014】

更に、本発明は、1つ以上のシステム環境の完全性を検証するためのシステム及び方法を提供する。

【0015】

また、本発明は、完全性プロファイル、システム、及びシステムコンポーネント情報を管理するためのシステム及び方法を提供する。

【0016】

更に、本発明は、完全性プロファイルの使用を介してユーザシステムの完全性のチェックを行うシステム及び方法を提供する。

40

【0017】

具体的に、ドキュメントの発行元やディストリビュータのようなコンテンツプロバイダが完全性プロファイルの要求を開始する。この完全性プロファイルの要求は、完全性認証及び検証デバイスへ転送される。例えば、要求されたアプリケーション及びシステムコンポーネントの完全性プロファイルが存在していない場合、完全性認証及び検証デバイスは、例えば種々のシステムコンポーネント及び／又はアプリケーションをユーザに供給しているコンテンツ使用システム／アプリケーションプロバイダに問合せを行う。コンテンツ使用システム／アプリケーションプロバイダは、特定のアプリケーション又はシステムコンポーネントに関する認証情報を完全性認証及び検証デバイスに返送する。この認証情報により、ユーザのシステム上のアプリケーション又はシステムコンポーネントと、コンテン

50

ツ使用システム／アプリケーションプロバイダによって配布されたオリジナルのアプリケーション又はシステムコンポーネントとの間で比較又は完全性の検証を行うことができる。

【0018】

システムアプリケーション及びシステムコンポーネントの認証情報は、コンポーネントデータベースに記憶されている。コンテンツプロバイダのプロファイルは、プロファイルデータベースに記憶されている。あるいは、コンテンツ使用システム／アプリケーションプロバイダは、完全性検証及び認証デバイスが完全性プロファイルを決定する必要なく完全性認証及び検証デバイスの各々のデータベースに直接転送することのできる認証情報のデータベースを保持することができる。次に、決定された完全性プロファイルに対応する完全性プロファイル識別がコンテンツプロバイダに返送される。

10

【0019】

ドキュメントのディストリビュータなどのコンテンツプロバイダは、例えば、保護されたコンテンツをユーザに提供する。コンテンツプロバイダは、例えば使用許諾契約及び完全性プロファイル識別を含む、デジタルコンテンツの保護されたバージョンをユーザに転送する。完全性プロファイル識別は、例えば、保護されたコンテンツに関連して使用が許可されるアプリケーション及びシステムコンポーネント、及びこれらのシステム／アプリケーションの完全性プロファイルの識別を含む。

【0020】

コンテンツ使用システム／アプリケーションプロバイダから認証情報を得ると、完全性認証及び検証デバイスは、例えばユーザシステムの要求により完全性プロファイルをユーザシステムに転送する。この完全性プロファイルを用いて、ユーザシステムの完全性の検証を行うことができる。ユーザのシステムのコンポーネント／アプリケーションが真正であると判断された場合、ユーザのアプリケーション及びシステムは、例えば追加のプロファイル情報に従って、コンテンツプロバイダにより提供されるデジタルコンテンツにアクセスすることができる。

20

【0021】

しかしながら、完全性認証の要求はコンテンツプロバイダから開始しなくてもよい。反対に、例えば、保護されたコンテンツと共にコンテンツプロバイダからユーザのシステムに転送されるプロファイル識別情報に組み込まれたソフトウェアアプリケーションによって認証要求を開始することができる。

30

【0022】

あるいは、コンテンツプロバイダが、完全性検証及び認証システムとして機能することもできる。この場合、コンテンツプロバイダは、適切な認証情報を集め、コンテンツプロバイダ自身が使用するための完全性プロファイルを決定することにより、完全性の認証及び検証サービスそのものを行う。

【0023】

更に、コンテンツ使用アプリケーション／システムプロバイダが完全性認証及び検証デバイスとして動作することもできる。この場合、コンテンツ使用アプリケーション／システムプロバイダは、例えば、完全性プロファイルに関連するアプリケーション及び／又はシステムコンポーネントと一緒に供給することもできる。

40

【0024】

本発明のこれらの及び他の特徴及び利点は、下記の好適な実施の形態の詳細な説明において説明されるか又は明らかになる。

【0025】

本発明の好適な実施の形態は、図面を参照しながら詳しく説明される。

【0026】

本発明のシステム及び方法は、コンテンツ使用環境の完全性を決定するために認証サービス及び検証サービスを提供する。このシステムでは、完全性認証及び検証デバイスが、1つ以上のコンテンツプロバイダと、1つ以上のコンテンツ使用システム及びアプリケーシ

50

ョンプロバイダとの間に導入される。完全性認証及び検証デバイスは、コンテンツ使用アプリケーション及び／又はシステムプロバイダから認証情報を得る。この認証情報により、コンテンツプロバイダはコンテンツが提供される環境を信用することができる。よって、コンテンツ使用アプリケーション及びシステムプロバイダから受信した認証情報に基づいて完全性プロファイルが設定される。ユーザが、コンテンツプロバイダによって提供されたデジタルコンテンツを変更したり、修正したりしていないか、又は認可されていない態様で妨害する可能性がないかを確認するために、このプロファイルはユーザシステムに転送される。

【0027】

図1は、完全性の認証及び検証を行う例示的なシステムを示している。具体的には、完全性認証及び検証システム100は、完全性認証及び検証デバイス200、コンテンツプロバイダ及び／又はディストリビュータ300、ユーザシステム400、コンテンツ使用システム／アプリケーションプロバイダ500、コンポーネントデータベース260、並びにプロファイルデータベース270を含む。

【0028】

例示的な動作環境において、コンテンツ使用システム／アプリケーションプロバイダ500は、アプリケーション、システム、及び／又はソフトウェア／ハードウェアコンポーネントをユーザに提供する。ユーザシステム400は、コンテンツプロバイダ及びディストリビュータ300によって供給されるドキュメントなどのデジタルコンテンツの使用を可能にする。ユーザシステム400の完全性を検証するために、完全性認証及び検証デバイス200は、個々のアプリケーション、システム、及び／又はソフトウェア／ハードウェアコンポーネントに関する認証情報をコンテンツ使用システム／アプリケーションプロバイダ500から収集し、これを登録する。この認証情報を用いて、完全性認証及び検証デバイス200は1つ以上のアプリケーション、システム、及び／又はシステムコンポーネントの完全性プロファイルをコンテンツプロバイダ300からのサービス要求20に基づいて決定し、これを認証する。次に、ユーザシステム400の完全性を判断することができるように、この決定された完全性プロファイル50をユーザシステム400に転送する。

【0029】

動作として、コンテンツプロバイダ及びディストリビュータ300はドキュメントなどのデジタルコンテンツをユーザシステム400に提供する。ユーザシステム400は、ハードウェアコンポーネント及び／又は種々のソフトウェアアプリケーションなど、1つ以上のシステムコンポーネントを含む。通常、これらのアプリケーション及びハードウェア／ソフトウェアコンポーネントは、コンピュータサプライヤ、ソフトウェアウェアハウス、アプリケーションプロバイダなどの1つ以上のコンテンツ使用システム／アプリケーションプロバイダからユーザによって得られる。次に、ユーザによるドキュメントなどのコンテンツの使用を可能にするために、これらのアプリケーションやハードウェアコンポーネント及びソフトウェアコンポーネントがアセンブルされていない場合はユーザによってアセンブルされるか、又は必要に応じてインストールされる。

【0030】

このように、ユーザ環境のアプリケーション及びハードウェア／ソフトウェアを使用するうちに、ユーザはドキュメントなどの保護されたコンテンツを見たいと思う場合がある。従って、ユーザ400は、電子本、マルチメディアファイル、プレゼンテーション、フォームテンプレートなど1つ以上のドキュメントをコンテンツプロバイダ300から要求する。コンテンツプロバイダ及びディストリビュータ300は、この要求を受信するとすぐに、要求されたコンテンツを保護された形式でプロファイル識別10と共にエンドユーザ400に提供することができる。このプロファイル識別10は、例えば、保護されたコンテンツをどのアプリケーションで見ることができるかに関する詳細や、例えば、提供されたコンテンツを特定のソフトウェア／ハードウェア環境内で操作できる範囲を含む。

【0031】

更に、コンテンツプロバイダ 300 は完全性認証及び検証デバイス 200 にサービス要求 20 を転送することができる。サービス要求 20 は、例えば、コンテンツプロバイダ 300 が、ユーザシステム 400 に対して、配布された保護コンテンツの使用を許可したいコンポーネント及び／又はソフトウェアアプリケーションのリストを含む。完全性認証及び／又は検証デバイス 200 は、サービス要求において識別されたコンポーネント及びアプリケーション／ソフトウェアに対応する認証情報がコンポーネントデータベース 260 及び／又はプロファイルデータ 270 に記憶されているか否かを判断する。完全性認証及び検証デバイスがサービス要求 20 において指定された認証情報をもたない場合、完全性認証及び検証デバイス 200 は、特定のアプリケーション、システム、ハードウェア／ソフトウェアコンポーネントなどに関する認証情報を 1 つ以上のコンテンツ使用システム／アプリケーションプロバイダ 500 から要求することができる。この認証情報を用いて、完全性認証及び検証デバイス 200 はアプリケーション及びシステムコンポーネントに関する情報をコンポーネントデータベース 260 に記憶する。あるいは、完全性認証及び検証デバイス 200 は、1 つ以上のアプリケーションの完全性プロファイルを作成することができる。アプリケーション、システム、及びシステムコンポーネントの真正性を確認するこの情報を用いて、完全性認証及び検証デバイス 200 は完全性プロファイル 50 をユーザシステム 400 に転送する。この完全性プロファイル 50 は、ユーザシステム 400 のシステム、システムコンポーネント及び／又はアプリケーションの真正性を確認するために用いられる。ユーザのシステムコンポーネント及び／又はアプリケーションが真正であると判断した場合、保護されたコンテンツ 10 の保護が解除され、ユーザシステム 400 は保護されたコンテンツを見たり、完全性プロファイルに従ってコンテンツを操作することができる。

10

20

【0032】

図 2 は、本発明の例示的な実施の形態に従った完全性認証及び検証環境 100 のコンポーネントの概要を示している。具体的に、完全性認証及び検証環境 100 は、1 つ以上のコンテンツプロバイダ 300、1 つ以上のユーザシステム 400、1 つ以上の完全性認証及び検証デバイス 200、並びに 1 つ以上のコンテンツ使用システム／アプリケーションプロバイダ 500 を含む。

【0033】

コンテンツプロバイダ 300 は、例えばコントローラ 310、メモリ 320、I/O コントローラ 330、及びコンテンツデータベース 340 を含む。しかしながら、コンテンツプロバイダ 300 は従来の態様でコンテンツを配布してもよいことを理解すべきである。例えば、コンテンツプロバイダは、コンテンツを含むコンパクトディスクを配布してもよい。このコンパクトディスクは、例えば郵便サービスによってユーザに送付することができる。一般に、どのタイプの配布及び普及方法でも、本発明のシステム及び方法と同等に申し分なく機能する。

30

【0034】

完全性認証及び検証デバイス 200 は、コントローラ 210、メモリ 220、I/O コントローラ 230、デジタル署名デバイス 240、コンポーネント登録デバイス 250、コンポーネントデータベース 260、プロファイルデータベース 270、プロファイル作成デバイス 280、プロファイル配布デバイス 290、及びプロファイル検証デバイス 295 を含む。完全性認証及び検証デバイス 200 は、コンポーネント登録サービス及び完全性プロファイルサービスといったサービスを提供する。登録サービスは、各々のプロバイダからのアプリケーション、システム、及び／又はソフトウェア／ハードウェアコンポーネントを、意図される特徴、目的及び／又は動作を伴う真正性があるものとして登録することを可能にする。

40

【0035】

完全性プロファイルサービスは、完全性プロファイルの構築及び検索のためにコンテンツプロバイダに提供される。完全性プロファイルは、必要に応じてデジタル署名されるドキュメントであり、検証可能情報と、保護されたドキュメントのコンテンツを使用する登

50

録されたシステムコンポーネントのセットとを含む。完全性プロファイルが作成されると、完全性プロファイルの識別がコンテンツプロバイダに返送される。コンテンツプロバイダは、完全性プロファイル識別と、必要に応じて、保護されたドキュメントの使用ライセンスを含む。保護されたドキュメントのコンテンツが使用され、ユーザのシステム及び環境のローカル完全性検証を行う必要が生じた場合、完全性認証及び検証デバイス200から完全性プロファイルを検索してユーザシステムに送ることができる。

【0036】

ユーザシステム400は、コントローラ410、メモリ420、I/Oコントローラ430、記憶装置440、完全性認証デバイス450、及びプロファイル記憶装置460を含む。しかしながら、この例示的なユーザシステムはコンピュータのモデルに基づいていることを理解すべきである。しかし、ユーザシステムのコンポーネントは、例えば使用されているコンテンツのタイプによって変わる場合のあることを理解すべきである。一般に、完全性を検証することのできる部分を含むいずれのユーザシステムも、本発明のシステム及び方法と同等に申し分なく機能する。

【0037】

コンテンツ使用システム／アプリケーションプロバイダ500は、例えばコントローラ510、メモリ520、I/Oコントローラ530、登録アプリケーションデバイス540、アプリケーションデータベース550、及びシステムデータベース560を含む。しかしながら、コンテンツプロバイダ300と同様に、コンテンツ使用システム／アプリケーションプロバイダは、コンテンツ使用システム／アプリケーションプロバイダが供給するシステム及び／又はアプリケーションのタイプによっていくつかの異なる形をとることができる。例えば、コンテンツ使用システム／アプリケーションプロバイダ500が特定のハードウェアコンポーネントを供給する場合、コンテンツ使用システム／アプリケーションプロバイダ500はアプリケーションデータベース及びシステムデータベースを保持しない場合がある。あるいは、例えば、システム／デバイスコンポーネントサプライヤが、例えば認証情報をディスクで完全性認証及び検証デバイス200に直接送る場合がある。

【0038】

あるいは、コンテンツ使用システム／アプリケーションプロバイダ500は、完全性プロファイルの決定を容易にするためにコンテンツプロバイダ300と動作を連係する場合がある。一般に、コンテンツ使用システム／アプリケーションプロバイダは、ハードウェア又はソフトウェア及びこれに関する認証情報を供給可能ないずれのエンティティでもよい。

【0039】

この例示的な実施の形態において、コンテンツ使用システム／アプリケーションプロバイダ500は種々のシステムコンポーネントを含むものとして示されているが、コンテンツ使用システム／アプリケーションプロバイダ500は、例えばコンピュータディストリビュータ、ソフトウェアディベロッパ、ソフトウェアプロバイダ、ソフトウェアディストリビュータなどでもよいことを理解すべきである。よって、コンテンツ使用システム／アプリケーションプロバイダ500は、コンテンツプロバイダ300によって提供されるコンテンツの使用を可能にするデバイス及び／又はソフトウェアを供給することができる。

【0040】

完全性認証及び検証環境100の種々のコンポーネントは、リンク5を介してコンポーネント間で通信することができる。リンク5は、有線又は無線リンクでもよいし、接続されたエレメント間に電子データを供給することのできる周知の又は今後開発される任意の他のエレメントでもよい。例えば、リンク5は1つ以上の分散型ネットワークでもよく、これらを1つ以上の更なる完全性認証及び検証環境100に接続してもよいし、あるいは、コンテンツプロバイダ300、ユーザシステム400、コンテンツ使用システム／アプリケーションプロバイダ500、並びに完全性認証及び検証デバイス200のうち1種以上の複数のインスタンスに接続してもよい。

【0041】

例示的な動作環境において、コンテンツ使用システム／アプリケーションプロバイダ500は、アプリケーション、ソフトウェア及び／又はハードウェアをユーザに供給する。これらのアプリケーション、ソフトウェア及び／又はハードウェアは、例えばドキュメントを見るなど、コンテンツを使用するためにユーザによって用いられる。

【0042】

コンテンツプロバイダ300は、例えば、ユーザシステム400に位置するユーザの要求時に、ドキュメントなどのコンテンツをユーザシステム400に配布する。特に、ユーザシステム400からの要求をコンテンツプロバイダ300が受信することができる。I/Oコントローラ330を介して受信されるこの要求は、コントローラ310によってメモリ320と協働して処理され、要求されたコンテンツがコンテンツデータベース340から検索される。例えば、コンテンツプロバイダ300としては、オンラインコンテンツプロバイダ、ブックストア、ソフトウェアプロバイダ、又はドキュメントなどのコンテンツをユーザに提供することを望むあらゆる他のコンテンツプロバイダが可能である。

10

【0043】

コンテンツプロバイダ300は、ユーザシステム400からコンテンツ要求を受信すると、要求されたコンテンツと共に保護されたコンテンツに関する追加の情報をユーザシステムに返送する。この追加の情報は、プロファイル識別を含みうる。あるいは、追加の情報は、例えば、コンテンツを有効にする前にプロファイルの要求、従って完全性認証の要求をユーザシステムに指示する情報を含みうる。

【0044】

20

更に、追加の情報は、要求されたコンテンツを見たりコンテンツと対話する際にどのシステムコンポーネント及び／又はハードウェア／ソフトウェアをユーザのマシンで実行及び／又は使用できるかを識別することができる。

【0045】

従って、要求されたコンテンツ、追加の情報、及びプロファイル識別のうち1つ以上が、ユーザシステム400によってI/Oコントローラ430を介して受信され、コントローラ410の指示により、メモリ420及び記憶装置440のうち的一方又は双方に記憶される。

【0046】

1つの例示的な実施の形態において、コンテンツプロバイダ300は、完全性認証及び検証デバイス260からの、完全性プロファイルの要求などのサービス要求20を開始することができる。完全性認証及び検証デバイス260は、コントローラ210及びメモリ220と協働して、サービス要求をコンテンツプロバイダ300からI/Oコントローラ230を介して受信する。

30

【0047】

前述のように、完全性認証及び検証デバイス200はコンポーネントデータベース260及びプロファイルデータベース270を含む。コンポーネントデータベース260は、1つ以上のコンテンツ使用システム／アプリケーションプロバイダ500によって配布することのできるシステム及びシステムコンポーネントに関する認証情報を記憶する。同様に、プロファイルデータベース270は、検証可能情報と、1つ以上の個々のコンテンツプロバイダ300の保護されたドキュメントのコンテンツを使用する、登録されたシステムコンポーネントのセットとを記憶する。

40

【0048】

よって、完全性認証及び検証デバイス200は、コンテンツプロバイダ300から完全性プロファイルの要求を受信すると、コントローラ210の指示及びメモリ220の援助により、コンポーネントデータベース260及びプロファイルデータベース270を探索し、サービス要求における情報に対応する認証情報が既に存在するか否かを判断する。

【0049】

あるいは、完全性認証及び検証デバイス200はオンライン検証サービスを行うことができる。オンライン検証サービスは、例えば完全性認証及び検証デバイス200内で完全性

50

の検証をオンライン及びリアルタイムで行うために提供される。このサービスを開始するために、完全性オーセンティケーター(integrity authenticator)と呼ばれる1つのソフトウェアがユーザシステム400に転送される。完全性オーセンティケーターは、ローカルソフトウェア及び／又はハードウェアコンポーネントの情報の収集を可能にする。あるいは、完全性オーセンティケーターは、図2に示される完全性認証デバイス450のような専用デバイスでもよい。ローカルソフトウェア及び／又はハードウェアコンポーネントに関して集められた情報は、オンラインの完全性検証を行うことができるように、完全性プロファイル識別と共に完全性認証及び検証デバイス200に返送される。コンポーネント登録デバイス250は、各々のプロバイダからのソフトウェア／ハードウェアコンポーネントを調べ、識別情報をコンポーネントデータベース260に記憶する。ソフトウェア／ハードウェアコンポーネントに関する情報は、例えばハッシュ化されていてもよく、真正なソフトウェア／ハードウェアの識別としてハッシュ値を使用することができる。しかしながら、各ソフトウェア／ハードウェアコンポーネントを識別するための情報として、真正なハードウェア及び／又はソフトウェアの識別を可能にするあらゆる周知のスキーム又は今後開発されるスキームが可能であることを理解すべきである。

10

【0050】

特定のソフトウェア及び／又はハードウェアコンポーネントの登録は下記のように達成される。例えば、コンテンツ使用システム／アプリケーションプロバイダ500は登録サービスを要求するために完全性認証及び検証デバイス200と通信することができ、あるいは、完全性認証及び検証デバイス200は認証情報を確保するためにコンテンツ使用システム／アプリケーションプロバイダ500と通信することができる。この例では、例えば、プロバイダ名、コンポーネント識別（例えば、シリアル番号、バージョン番号、型番号など）などを含む特定のソフトウェア及び／もしくはハードウェア、又はアプリケーションそのものに関する情報を確保するために、登録アプリケーションデバイス540はコントローラ510、メモリ520、及びI/Oコントローラ530と協働してアプリケーションデータベース550及びシステムデータベース560のうち的一方又は双方を探索する。

20

【0051】

例えば、1つの特定の動作シナリオでは、特定のコンテンツ使用システム／アプリケーションプロバイダ500から認証情報を取得する代わりに、完全性認証及び検証デバイス200が、例えばソフトウェアプログラムなどの特定のアプリケーションをコンテンツ使用システム／アプリケーションプロバイダ500から実際に要求することができる。このように、完全性認証及び検証デバイス200は特定のソフトウェアアプリケーションをコンテンツ使用システム／アプリケーションプロバイダ500から直接確保することができるため、完全性認証及び検証デバイス200は認証情報を必要としない。

30

【0052】

コンポーネント登録デバイス250はコンポーネントの情報を検証し、必要に応じて、例えば真正なソフトウェア及び／又はハードウェアの識別として使用することのできるハッシュ値などを計算する。その後、コンポーネント登録デバイス250は、コンポーネント情報と例えばハッシュ値をコンポーネントデータベース260に記憶する。

40

【0053】

あるいは、コンテンツ使用システム／アプリケーションプロバイダ500は、ソフトウェア及び／又はハードウェアコンポーネントを登録アプリケーションデバイス540に送る代わりに、コンポーネント登録デバイス250と接続し、登録アプリケーションのような小さなソフトウェアアプリケーションをダウンロードして、これをローカルで実行することもできる。この登録アプリケーションは目的のソフトウェア／ハードウェアコンポーネントを調べ、このソフトウェア／ハードウェアコンポーネントに関する情報を、場合によってはハッシュ値などの完全性の値と共にコンポーネント登録デバイス250に送り返し、コンポーネント登録デバイス250はコンポーネントに関する認証情報をコンポーネントデータベース260に記憶することができる。

50

【0054】

あるいは、プロファイル作成デバイス280がソフトウェアの完全性プロファイルを構築する。特に、各ソフトウェアアプリケーションのハッシュ値などの完全性の値をコンポーネントデータベースから検索して記憶することができる。また、コンポーネント間の任意の対話関係もプロファイルに含まれる。この関係は、他のコンポーネントとの意図的でない対話を防ぐために、コンポーネントの呼出及び戻りシーケンスの識別に使用される。完全性プロファイルのコンテンツは、例えばデジタル署名され、得られた署名を完全性プロファイルに追加する。各完全性プロファイルは固有の識別に関連付けられている。

【0055】

図3は、入力、出力、並びに完全性認証及び検証デバイス200によって提供されるサービス及び動作の例示的なワークフローを示している。具体的に、コンポーネント登録サービスに関しては、コンポーネント識別と、必要に応じて、特定のコンポーネントに関するメタ情報がコンポーネント登録デバイス250に転送される。コンポーネント登録デバイス250は、例えば意図された特徴、目的、及び動作を有するコンポーネントをコンポーネントデータベースに登録する。次に、コンポーネント登録デバイス250は、登録されたコンポーネントの識別を例えばコンテンツ使用システム／アプリケーションプロバイダに返送し、例えばコンテンツプロバイダ300が識別を使用できるようにする。

【0056】

プロファイルの作成に関しては、プロファイル作成デバイス280は登録されたコンポーネントの識別を受信する。登録されたコンポーネントの識別は、関連するコンポーネントがある場合はそのコンポーネントに関する情報と組み合わせてデジタル署名され、プロファイルデータベースに記憶される。完全性プロファイル識別は要求者に返送される。

【0057】

同様に、プロファイル配布デバイス290は完全性プロファイル識別を受信する。この完全性プロファイル識別に対応する完全性プロファイルが利用可能であるか否かを判断するために、プロファイルデータベース270に対して問合せが行われる。完全性プロファイルが利用可能である場合、完全性プロファイルは要求者に返送される。そうでない場合、プロファイル作成デバイス280の援助によって完全性プロファイルを決定することができる。

【0058】

プロファイル検証デバイス295は、1つ以上のコンポーネントを識別する情報及び完全性プロファイル識別を受信する。プロファイル検証デバイスは、コンポーネント識別、完全性プロファイル識別、及び対応する完全性プロファイルを比較して検証データを決定する。プロファイル、コンポーネント及び識別が適合した場合、システムの完全性が検証されたことになる。そうでない場合、システムは完全性プロファイルにおいて指定されたものではないか、何らかの方法で改変されている。

【0059】

図4は例示的な完全性プロファイルを示している。この例示的な完全性プロファイルを、プロファイル作成デバイス280によって作成することができる。認証されたコンテンツプロバイダの完全性プロファイルを構築するために、完全性プロファイルの作成要求が開始される。例えば、プロバイダは完全性認証及び検証デバイス200と交信し、完全性プロファイルの作成を要求することができる。次に、プロバイダはソフトウェア及び／又はハードウェアコンポーネントの名のリストを完全性認証及び検証デバイス200に送る。プロファイル作成デバイス280は、完全性の値又はハッシュ値など、各々のコンポーネントの識別をコンポーネントデータベース260から検索する。プロファイル作成デバイス280は次に、各コンポーネントの完全性の値又はハッシュ値などの認証情報と、完全性プロファイル識別、バージョン番号、作成日、構築日、コンテンツプロバイダ名、そして例えば必要に応じて任意のソフトウェア及び／又はハードウェアコンポーネント間の対話関係のような他の情報を含む完全性プロファイルを決定する。

【0060】

プロファイル作成デバイス 280 は決定された完全性プロファイルをデジタル署名デバイス 240 に転送し、デジタル署名デバイス 240 はプロファイルのコンテンツに署名することができる。プロファイル作成デバイス 280 は署名されたプロファイルをプロファイルデータベース 270 に記憶し、プロファイル識別をコンテンツプロバイダ 300 に返送する。

【0061】

例えば、保護されたドキュメントのコンテンツの使用ライセンスを作成する際、コンテンツプロバイダ 300 は必要に応じて完全性プロファイル識別を使用ライセンスに含めることができる。ユーザシステム 400 において、完全性プロファイルは、環境呼出スタック内の全てのソフトウェア／ハードウェアコンポーネントを検証するために使用される。これにより、認可されたソフトウェア／ハードウェアコンポーネント又はこれらの任意の組み合わせによってのみ機密情報を使用できることが保証される。

10

【0062】

プロファイル配布デバイス 290 は、完全性プロファイルの取得要求を受け入れ、プロファイルデータベース 270 から完全性プロファイルを検索し、完全性プロファイルを各々の要求者に返送する。同様に、プロファイル検証デバイス 295 は 1 つ以上のシステム環境のユーザシステムの検証要求を受け入れる。プロファイル検証デバイス 295 は完全性プロファイルに従ってソフトウェア／ハードウェアに関する情報を集め、この情報をプロファイルに照らして検証し、検証結果を要求者に返送する。

【0063】

ユーザシステム 400 は完全性認証デバイス 450 を含む。完全性認証デバイス 450 は、例えば任意のコンテンツ使用アプリケーションにおいて作動する。

20

【0064】

よって、図 5 は、ユーザデバイス 400 における、システム完全性を検証するための例示的なシステム環境スタックを示している。具体的に、ユーザシステム環境スタックは、完全性オーセンティケータと 1 つ以上のシステムコンポーネントを含む。

【0065】

図 6 は環境スタックの一例を示しており、完全性オーセンティケータ、プラグイン、レンダリングアプリケーション、オペレーティングシステム、オペレーティングシステム (OS) ブートストラップ、及び各々のハードウェアを含む。

30

【0066】

例示的な動作環境において、完全性認証デバイス 450 は、その独自の暗号化／復号化鍵の対と、完全性認証及び検証デバイスの検証鍵とを含む。これらの鍵は、本発明の不正使用防止の見地のために、隠されている、及び／又は完全性認証デバイス 400 内に組み込まれている可能性がある。ユーザの個人情報の使用を必要とするアプリケーション又は機密ドキュメント及びデータを含むアプリケーションに関しては、完全性認証デバイス 450 は関連する完全性プロファイルを使用して、ユーザシステム環境における呼出スタックのソフトウェア／ハードウェアコンポーネントを全て検証することができる。

【0067】

完全性認証デバイス 450 はまず、完全性認証及び検証デバイスの認証鍵を用いてプロファイルの署名を検証する。図 7 乃至図 9 に示されるように、署名が検証されると、完全性認証デバイス 450 は現行の呼出スタックを調べ、完全性プロファイルにおいて提供される情報を用いて呼出スタック上の各ソフトウェア／ハードウェアコンポーネントを認証する。呼出スタックは、メモリアメージ及び関与する関数又は手続きからなるメモリの連続ブロックである。スタックは後入れ先出しの概念で動作し、スタックの基本動作はスタックの「プッシュ」とスタックの「ポップ」である。プッシュは、イメージをスタックに記憶してスタックの最上部の位置に進むために使用される。ポップは、データをスタックから除去してスタックの最上部を前の位置に復元するために使用される。

40

【0068】

呼出スタックでは、現在実行されている関数のイメージがスタックの最上部にある。現在

50

実行されている関数が次の関数を呼び出すと、次の関数のメモリエイジーが呼出スタックの最上部にプッシュされ、呼出スタックの最上部は次の関数のイメージを示す。スタックされたイメージの各部分は、呼び出された関数の実行が完了した後のアドレス又は戻り命令を含む。

【0069】

図10は、実行環境が保護される態様を示している。具体的には、完全性オーセンティケータ（IA）を保護するために、IAの実行は、IAの一部である信用あるアプリケーションによってモニタされる。例えばアプリケーションなどのモニタリングプロセスは、デバッガ、又はIAがシステム内のあらゆる他のプロセスもしくはアプリケーションによってモニタされることを防ぐことのできる特殊プロセスとすることができる。1つのプロセスでしかプロセスをデバッグすることができない環境では、信用あるモニタリングプログラムをデバッガとして実施することができる。モニタリングプログラムは信用あるアプリケーションであるため、モニタリングプログラムの完全性は現行の完全性プロファイル内になくなくてはならない。従って、IAは、信用あるアプリケーションをロードして実行する前に、このアプリケーションの完全性を検証する。信用あるモニタリングアプリケーションの機能は、他のプロセスによるIAのモニタリング、制御、及び捕捉を防ぐことである。信用あるモニタリングアプリケーションの他の機能は、現行の環境をモニタし、環境の変化が有効であるか否かを判断することである。しかしながら、IAと同様に、信用あるモニタリングアプリケーションも保護されなくてはならず、IAは、他のアプリケーションによるモニタリング、捕捉、及び／又は制御から信用あるモニタリングアプリケーションを保護するためのモニタとして動作する。この二重の保護メカニズムは、他のアプリケーションによる完全性オーセンティケータの実行のモニタリングを防ぐ閉システムを形成する。

【0070】

図11は、完全性認証及び検証デバイスの例示的な動作方法を示している。具体的に、制御はステップS100において開始し、ステップS110へ続く。ステップS110では、完全性プロファイルを決定する。次に、ステップS120では、完全性プロファイルを検証する。そして、ステップS130では、完全性プロファイルをユーザに転送する。制御はステップS140へ続く。

【0071】

ステップS140では、ユーザシステムの完全性を検証する。次に、ステップS150では、ユーザシステムが真正であるか否かを判断する。ユーザシステムが真正である場合、制御はステップS160へ続き、ユーザによる選択したコンテンツへのアクセスを許可する。そうでない場合、制御はステップS170へ移り、コンテンツへのアクセスを拒否するか又は無効にする。制御は次いでステップS180へ続き、ここで制御シーケンスが終了する。

【0072】

図12は、本発明に従ってコンポーネント／ハードウェア及び／又はソフトウェアを登録する例示的な方法を示している。具体的に、制御はステップS200において開始し、ステップS210へ続く。ステップS210では、登録サービスを開始する。次に、ステップS220では、コンポーネントサプライヤが特定のコンポーネント／ハードウェア及び／又はソフトウェアに関する認証情報を提供する。次に、ステップS230では、特定のコンポーネント／ハードウェア及び／又はソフトウェアに関する情報を検証する。制御は次にステップS240へ続く。

【0073】

ステップS240では、完全性の値を決定すべきか否かを判断する。完全性の値を決定する場合、制御はステップS250へ続き、完全性の値を決定する。そうでない場合、制御はステップS260へ移り、コンポーネント／ハードウェア及び／又はソフトウェアに関する認証情報を記憶する。

【0074】

次に、ステップS 2 7 0では、完全性の値を記憶するか否かを判断する。完全性の値を記憶する場合、制御はステップS 2 8 0へ続き、完全性の値を記憶する。そうでない場合、即ち完全性の値を記憶しない場合、制御はステップS 2 9 0へ移り、ここで制御シーケンスが終了する。

【0075】

図13は、本発明に従ってプロファイルを決定する例示的な方法を示している。具体的に、制御はステップS 3 0 0において開始し、ステップS 3 1 0へ続く。ステップS 3 1 0では、完全性プロファイルの決定を開始する。次に、ステップS 3 2 0では、コンポーネント及び／又はハードウェアもしくはソフトウェアの識別などの名を取得する。そして、ステップS 3 3 0では、コンポーネント／ハードウェア又はソフトウェアの識別を検索する。制御はステップS 3 4 0へ続く。

10

【0076】

ステップS 3 4 0では、完全性プロファイルを決定する。次に、ステップS 3 5 0では、完全性プロファイルをデジタル署名する。そして、ステップS 3 6 0では、デジタル署名された完全性プロファイルを記憶する。制御は次にステップS 3 7 0へ続く。

【0077】

ステップS 3 7 0では、署名された完全性プロファイルを、コンテンツ使用システム／アプリケーションプロバイダなどの要求者に転送する。制御は次にステップS 3 8 0へ続き、ここで制御シーケンスが終了する。

【0078】

20

図14は、本発明の1つの態様に従って完全性オーセンティケータの完全性を検証する例示的な方法を示している。制御はステップS 4 0 0において開始し、ステップS 4 1 0へ続く。ステップS 4 1 0では、完全性オーセンティケータの完全性を検証する。次に、ステップS 4 2 0では、完全性オーセンティケータが有効であるか否かを判断する。完全性オーセンティケータが有効である場合、制御はステップS 4 3 0へ続く。そうでない場合、制御はステップS 5 4 0へ移る。

【0079】

ステップS 4 3 0では、不正使用防止環境を確立する。次に、ステップS 4 4 0では、完全性プロファイルを検証する。そして、ステップS 4 5 0では、完全性プロファイルが有効であるか否かを判断する。完全性プロファイルが有効である場合、制御はステップS 4 6 0へ続く。そうでない場合、制御はステップS 5 4 0へ移る。

30

【0080】

ステップS 4 6 0では、完全性プロファイルをロードする。次に、ステップS 4 7 0では、図6に関連して示されるような現行の実行環境の呼出スタックを構築する。呼出スタックの最下部にはハードウェア及び／又はデバイスのセットがあり、ソフトウェアコンポーネントは全てスタックの最上部付近にある。スタック内のコンポーネントは、下にあるコンポーネントがそのすぐ上にあるコンポーネントを呼び出す、という関係にある。呼出スタックが構築されると、最後に実行されるコンポーネントの実行イメージを含む呼出スタックの最上部が位置付けられる。よって、スタック上の各コンポーネントの実行イメージは、呼出コンポーネントの識別を助ける。次に、ステップS 4 8 0では、識別呼出コンポーネントを検索する。制御は次にステップS 4 9 0へ続く。

40

【0081】

ステップS 4 9 0では、コンポーネントの完全性を完全性プロファイルに照らして検証する。次に、ステップS 5 5 0では、コンポーネントが有効であるか否かを判断する。コンポーネントが有効である場合、制御はステップS 5 1 0へ続く。そうでない場合、制御はステップS 5 4 0へ移る。

【0082】

ステップS 5 1 0では、スタックが空であるか否かを判断する。スタックが空である場合、制御はステップS 5 2 0へ移る。そうでない場合、制御はステップS 5 3 0へ移る。ステップS 5 2 0では、スタック内の次のコンポーネントを探し出し、この次のコンポーネ

50

ントを現行のスタックフレームとして設定する。制御は次にステップS480に戻り、検証を行う。

【0083】

ステップS530では完全性を検証し、制御はステップS550へ続き、ここで制御シーケンスが終了する。

【0084】

ステップS540では完全性のチェックに失敗し、制御はステップS550へ続き、ここで制御シーケンスが終了する。

【0085】

図1乃至図2に示されるように、完全性認証及び検証デバイスは、単一プログラム汎用コンピュータ又は個別プログラム汎用コンピュータにおいて実施されることが好ましい。しかしながら、専用コンピュータ、プログラム式マイクロプロセッサもしくはマイクロコントローラ及び周辺集積回路素子、ASIC、又は他の集積回路、デジタル信号プロセッサ、ディスクリットエレメント回路のようなハードワイヤード電子回路もしくは論理回路、又はPLA、PLD、FPGA、もしくはPALのようなプログラマブル論理デバイスなどにおいて、完全性認証及び検証デバイスを実施することもできる。一般に、図11乃至図14に示されるフローチャートを実施可能な有限マシンを実施することのできる任意のデバイスを使用して、完全性認証及び検証デバイスを実施することができる。

【0086】

更に、多様なコンピュータ又はワークステーションなどのハードウェアプラットフォームにおいて使用することができるポータブルソースコードを提供する環境内で、オブジェクト又はオブジェクト指向ソフトウェア開発技術を用いて、開示された方法を容易に実施することができる。あるいは、開示された完全性認証及び検証デバイスを、標準論理回路又はVLSI設計を用いたハードウェアにおいて部分的又は完全に実施することができる。本発明によるシステム及び方法の実施にソフトウェアを用いるかハードウェアを用いるかは、システムの速度及び／又は効率の要件、特定の機能、並びに使用されている特定のハードウェアシステム、ソフトウェアシステム、マイクロプロセッサシステム、又はマイクロコンピュータシステムによる。しかしながら、前述の完全性認証及び検証デバイス及び方法は、当業者により、本明細書中に提供された機能の説明から必要以上に実験することなく、コンピュータ分野の一般知識を共に用いて、あらゆる周知の又は今後開発されるシステム、構造、デバイス、及び／又はソフトウェアを用いて、ハードウェア又はソフトウェアにおいて容易に実施することができる。更に、開示された方法を、プログラムされた汎用コンピュータ、専用コンピュータ、マイクロプロセッサ、又はサーバなどで実行されるソフトウェアとして容易に実施することができる。この場合、サーバに存在するリソースとしてのJAVA（登録商標）もしくはCGIスクリプト、又は専用の完全性認証及び検証デバイス、ウェブブラウザ、ウェブTVインターフェース、PDAインターフェース、もしくはマルチメディアプレゼンテーションデバイスに組み込まれたルーチンとしてのグラフィックスワークステーションなど、パーソナルコンピュータ又はサーバに組み込まれたルーチンとして本発明の方法及びシステムを実施することができる。また、グラフィックスワークステーション又は専用の完全性認証及び検証デバイスのハードウェアシステム及びソフトウェアシステムなど、ソフトウェアシステム及び／又はハードウェアシステムに本発明のシステム及び方法を物理的に導入することによって完全性認証及び検証デバイスを実施することもできる。

【0087】

よって、完全性検証のシステム及び方法が本発明に従って提供されたことが明らかである。本発明はその好適な実施の形態に関連して説明されたが、多くの代替物、変更物及び変形物が当業者に明らかであることは明白である。従って、出願人は、本発明の趣意及び範囲内にあるこのような代替物、変更物、及び変形物を全て含むものと意図している。

【図面の簡単な説明】

【図1】 本発明による完全性認証及び検証システムの第1の例示的な実施の形態を示す

機能概要図である。

【図2】 本発明による完全性認証及び検証システムの第1の例示的な実施の形態を示す機能ブロック図である。

【図3】 本発明による例示的な完全性認証及び検証デバイスのワークフロー図である。

【図4】 本発明による完全性プロファイルの例示的な構造を示す図である。

【図5】 本発明による例示的な環境スタックを示す図である。

【図6】 本発明による例示的な環境スタックを示す図である。

【図7】 本発明による例示的なスタックのワークフローを示す図である。

【図8】 本発明によるスタックの例示的なワークフローを示す図である。

【図9】 本発明によるスタックを操作する例示的な方法を示す図である。

【図10】 本発明に従った、デバッグの使用によりダイナミックな不正使用を防止する例示的な方法を示す図である。

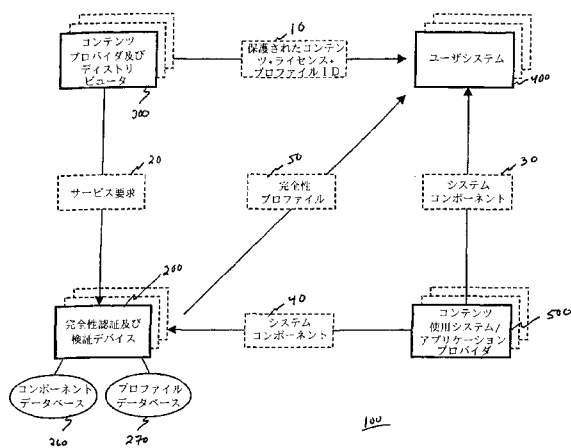
【図11】 本発明による完全性の認証及び検証方法の1つの例示的な実施の形態の概要を説明するフローチャートである。

【図12】 本発明によるアプリケーション及び／又はシステム登録方法の1つの例示的な実施の形態の概要を説明するフローチャートである。

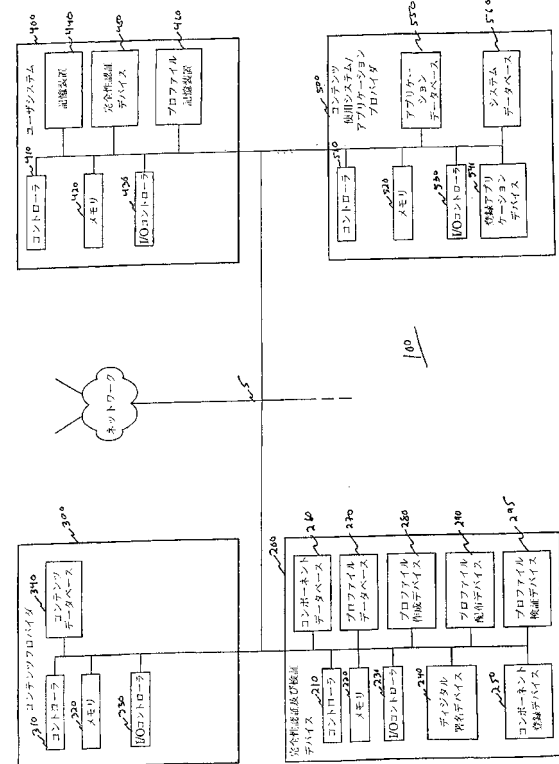
【図13】 本発明による完全性プロファイル決定方法の例示的な実施の形態の概要を説明するフローチャートである。

【図14】 本発明に従って完全性オーセンティケータの完全性を検証する方法の例示的な実施の形態の概要を説明するフローチャートである。

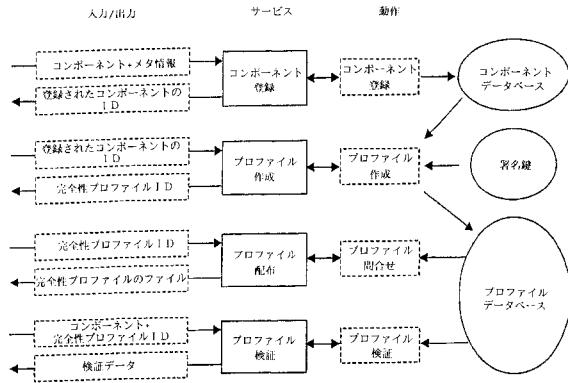
【図1】



【図2】

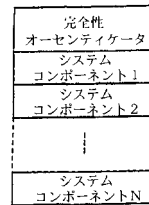


【図 3】



【図 5】

一般的なエンドユーザシステム環境スタック



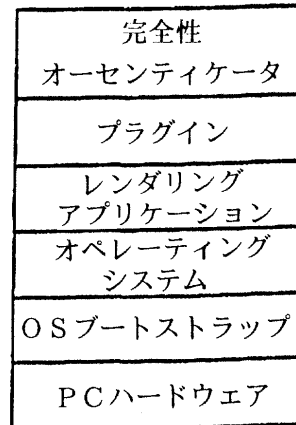
【図 6】

エンドユーザシステム環境スタックの例

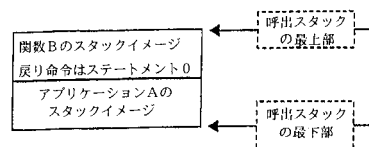
【図 4】

完全性プロファイルの構造

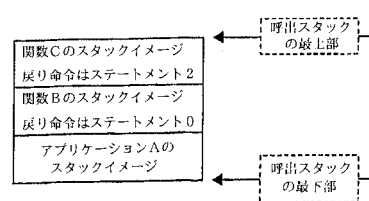
完全性プロファイル識別
完全性プロファイルのバージョン番号
作成日
作成者
コンテンツプロバイダの名及びID
コンポーネントの完全性の値（例えばハッシュ値）のリスト
（オプション）コンポーネント間の対話関係
完全性プロファイルのデジタル署名



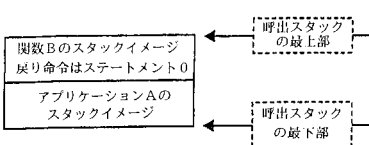
【図 7】



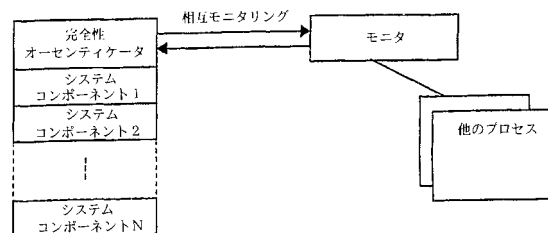
【図 8】



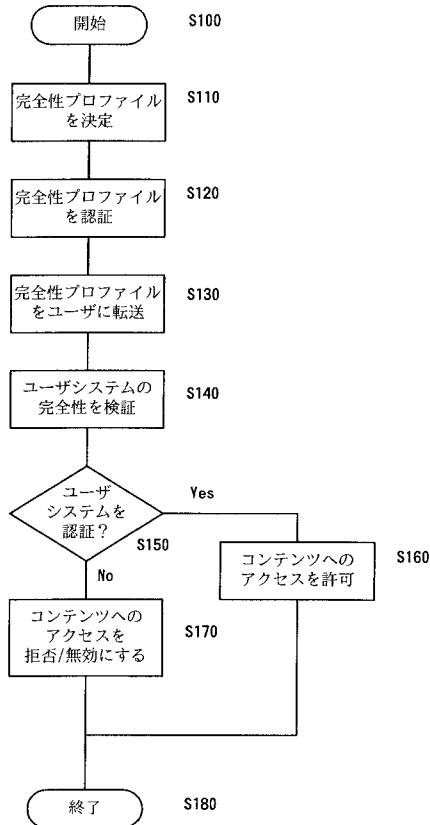
【図 9】



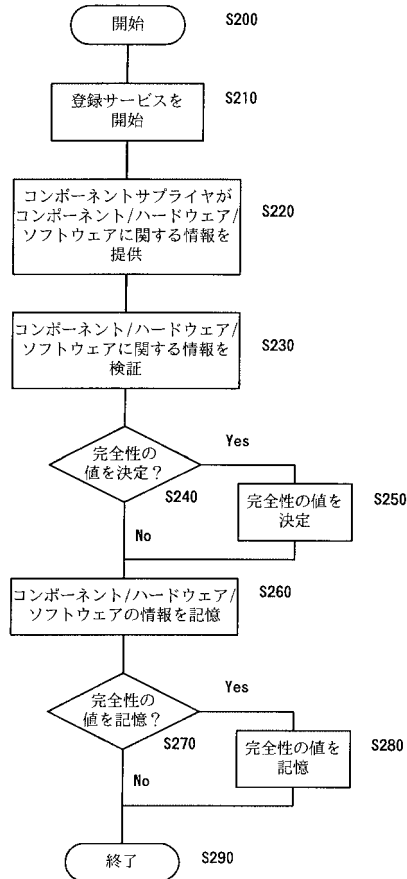
【図 10】

モニタリングを用いたダイナミックな不正使用の防止
（デバッグなど）による実行環境の保護

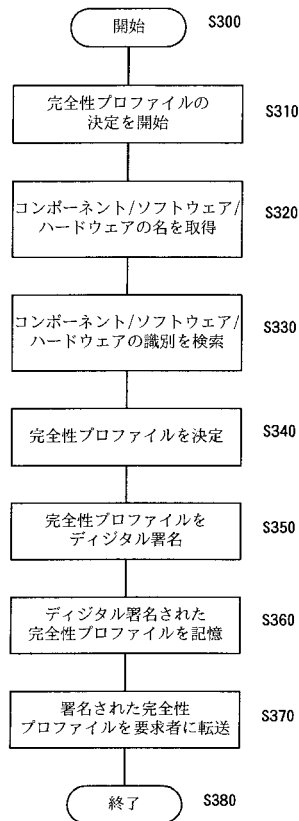
【図 1 1】



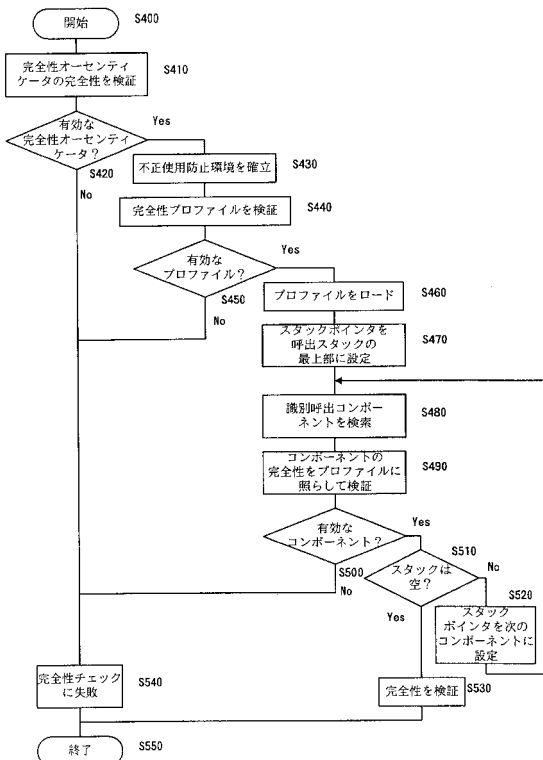
【図 1 2】



【図 1 3】



【図 1 4】



フロントページの続き

(72)発明者 タ、タン

アメリカ合衆国 92648 カリフォルニア州 ハンティングトン ビーチ ストラットン レ
ーン 18694

(72)発明者 ワン、シン

アメリカ合衆国 90503 カリフォルニア州 トーランス エメラルド ストリート 372
0 ナンバー ヴイ2

審査官 漆原 孝治

(56)参考文献 特開2000-207199 (JP, A)

(58)調査した分野(Int.Cl.⁷, DB名)

G06F 1/00