(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2012-520501
(P2012-520501A)
(43)公表日　平成24年9月6日(2012.9.6)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/00	(2006.01)	G06F 21/00	157C	
		G06F 21/00	157D	

審査請求 未請求　予備審査請求 未請求　（全 20 頁）

(21)出願番号	特願2011-553585 (P2011-553585)
(86)(22)出願日	平成22年3月10日 (2010.3.10)
(85)翻訳文提出日	平成23年8月3日 (2011.8.3)
(86)国際出願番号	PCT/IB2010/051027
(87)国際公開番号	WO2010/103466
(87)国際公開日	平成22年9月16日 (2010.9.16)
(31)優先権主張番号	12/402,777
(32)優先日	平成21年3月12日 (2009.3.12)
(33)優先権主張国	米国 (US)

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(74)代理人　100108501
弁理士　上野　剛史
(74)代理人　100112690
弁理士　太佐　種一
(74)代理人　100091568
弁理士　市位　嘉宏

最終頁に続く

(54)【発明の名称】周辺デバイスを用いた完全性検証

(57)【要約】
【課題】　周辺デバイスを用いた完全性検証のためのシステム及び方法を提供する。
【解決手段】　周辺デバイスが、コンピュータ、周辺デバイスと通信するように構成されたインターフェースと、コンピュータのオペレーティング・システムの完全性検証を実行するように構成された論理と、完全性検証の結果を表示するように構成されたディスプレイとを含む。周辺デバイスを用いたコンピュータの完全性検証のための方法が、周辺デバイスをコンピュータに接続することと、デバイスからコンピュータにチャレンジを送ることと、チャレンジ及びコンピュータ内に格納された情報を用いて認証データを計算することと、コンピュータ上で実行されるクライアント・プログラムによって、コンピュータから認証データを取り出すことと、認証データを周辺デバイスに送ることと、周辺デバイスによって認証データを検証することとを含む。
【選択図】　図２

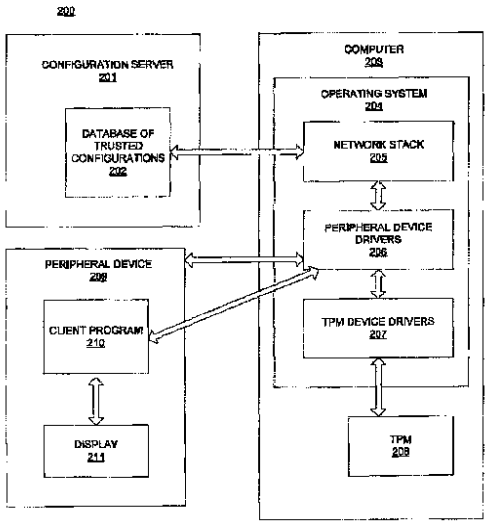


FIG. 2

【特許請求の範囲】
【請求項１】
周辺デバイスであって、
コンピュータ、前記周辺デバイスと通信するように構成されたインターフェースと、
前記コンピュータのオペレーティング・システムの完全性検証を実行するように構成された論理と、
前記完全性検証の結果を表示するように構成されたディスプレイと、
を含む周辺デバイス。
【請求項２】
前記インターフェースは、ＵＳＢ（ユニバーサル・シリアル・バス）インターフェースを含み、前記周辺デバイスは、ＵＳＢ周辺デバイスを含む、請求項１に記載の周辺デバイス。
【請求項３】
前記周辺デバイスは、読み取り専用デバイスである、請求項１に記載の周辺デバイス。
【請求項４】
前記コンピュータは、前記オペレーティング・システムに関する認証データを格納するように構成された、信頼できるプラットフォーム・モジュールを含む、請求項１に記載の周辺デバイス。
【請求項５】
前記論理は、前記コンピュータ上で実行されるように構成されたクライアント・プログラムを含み、前記クライアント・プログラムは、ネットワークを介して、構成サーバから、前記完全性検証を実行するために必要とされる情報を受信するようにさらに構成される、請求項１に記載の周辺デバイス。
【請求項６】
前記周辺デバイスは、完全性検証を実行するのに用いるための認証値の既知のリストを含む、請求項１に記載の周辺デバイス。
【請求項７】
前記周辺デバイスは、外部指紋読取装置をさらに含み、前記外部指紋読取装置は、完全性検証が成功した場合に、走査された指紋を前記コンピュータに送るように構成される、請求項１に記載の周辺デバイス。
【請求項８】
前記周辺デバイスは、キーボード、マウス、又はネットワーク・デバイスのうちの１つを含む、請求項１に記載の周辺デバイス。
【請求項９】
周辺デバイスを用いたコンピュータの完全性検証のための方法であって、
前記周辺デバイスを前記コンピュータに接続することと、
前記デバイスから前記コンピュータにチャレンジを送ることと、
前記チャレンジ及び前記コンピュータ内に格納された情報を用いて認証データを計算することと、
前記コンピュータ上で実行されているクライアント・プログラムによって、前記コンピュータから前記認証データを取り出すことと、
前記認証データを前記周辺デバイスに送ることと、
前記周辺デバイスによって前記認証データを検証することと、
を含む方法。
【請求項１０】
前記認証データは、前記コンピュータ上の信頼できるプラットフォーム・モジュールからの情報を用いて計算される、請求項９に記載の方法。
【請求項１１】
前記周辺デバイスにより前記検証の結果を表示することをさらに含む、請求項９に記載の方法。

【請求項１２】
構成サーバから、前記検証を実行するのに必要な情報を前記周辺デバイスにより受信することをさらに含む、請求項９に記載の方法。
【請求項１３】
前記周辺デバイスは、ユニバーサル・シリアル・バス（ＵＳＢ）デバイスを含む、請求項９に記載の方法。
【請求項１４】
周辺デバイスを用いてコンピュータの完全性を検証するためのシステムであって、
オペレーティング・システムを含むコンピュータと、
前記オペレーティング・システムの完全性検証を実行するように構成された、前記コンピュータと通信状態にある周辺デバイスと、
を含むシステム。
【請求項１５】
前記コンピュータは、前記オペレーティング・システムに関する認証データを格納するように構成された信頼できるプラットフォーム・モジュールを含む、請求項１４に記載のシステム。
【請求項１６】
前記周辺デバイスと通信状態にある構成サーバをさらに含む、請求項１４に記載のシステム。
【請求項１７】
前記周辺デバイスは、ユニバーサル・シリアル・バス（ＵＳＢ）デバイスである、請求項１４に記載のシステム。
【請求項１８】
前記ＵＳＢ周辺デバイスは、指紋スキャナをさらに含む、請求項１４に記載のシステム。
【請求項１９】
前記ＵＳＢ周辺デバイスは、前記完全性検証を実行するのに用いるための認証値の既知のリストを含む、請求項１４に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、一般に、コンピュータの完全性検証の分野に関する。
【背景技術】
【０００２】
ルートキット、トロイの木馬、又は他のタイプの悪質なコードが、コンピュータのオペレーティング・システムを危険にさらし、これによりコンピュータ上で実行されている全てのコードの信頼性が危険にさらされることがある。コンピュータが危険にさらされているかどうかの判断は、コンピュータが、検証可能な形で正常かつ信頼できるオペレーティング・システムによってブートされるかどうかの判断に関連する。コンピュータの信頼性検証のために、Trusted Platform Module（信頼できるプラットフォーム・モジュール、ＴＰＭ）技術（ＴＰＭに関する更なる情報については、http://www.trustedcomputinggroup.org/groups/tpmを参照されたい）を用いることができる。ＴＰＭは、ブート・プロセス中、コンピュータによって実行される全てのソフトウェアの計測値（measurement）を格納する、安全なハードウェアの記憶場所をコンピュータ上に提供し、その計測値を完全性検証のために用いることができる。
【０００３】
ＴＰＭは、多くの種類のパーソナル・コンピュータを含む、多くのコンピュータ・プラットフォーム内に含められる。ＴＰＭは、ハードウェアによって保護されている計測値及び格納されたログへの認証を行うことにより、コンピュータのブート時にコードの完全性を検証するのを可能にする。ハードウェアによって保護されている計測において、コンピ

ュータは、ブート・プロセスに関与する全てのコードの暗号ハッシュ値を作成し、これを安全なＴＰＭストレージ内に安全に格納する。次に、コンピュータは、暗号ハッシュ値についてのログ・エントリを作成し、該ログ・エントリをＴＰＭ内に安全に格納する。外部のハードウェアからのランダムに作成されたチャレンジ（challenge）に応答して、コンピュータが、ＴＰＭ内のログ・エントリから署名を生成し、これにより、ログ・エントリを既知の信頼できるコードと比較することによって、外部のハードウェアがログ・エントリを検証することが可能になると、格納されたログに対する認証が行われる。コンピュータの起動時に、これらに限定されるものではないが、基本入力／出力システム（ＢＩＯＳ）、ブートローダー、カーネル及び任意のアプリケーションを含む、コンピュータ上のコードが、まずメモリ内にロードされ、次に計測され、そして実行される。コードの計測値は、ＴＰＭのログ内に格納される。コードの実行を開始する前に、ログ・エントリが安全なＴＰＭ内に格納されるので、悪質なコードの部分が、関連したログ・エントリを消去することはできない。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

認証を完了するために、ＴＰＭは、チャレンジを出して認証を行い、これにより所定のコンピュータが信頼できるオペレーティング・システムによりブートされたかどうかを判断する、検証装置として知られる別個の信頼できるホストを必要とする。パーソナル・コンピュータの所有者が、検証装置として働くことができる別個のホストを有していない場合がある。別個の検証装置コンピュータを有していないユーザは、ＴＰＭ検証の利点を利用できない。

【課題を解決するための手段】

【０００５】

周辺デバイスの例示的な実施形態は、コンピュータ、周辺デバイスと通信するように構成されたインターフェースと、コンピュータのオペレーティング・システムの完全性検証を実行するように構成された論理と、完全性検証の結果を表示するように構成されたディスプレイとを含む。

【０００６】

周辺デバイスを用いたコンピュータの完全性検証のための方法の例示的な実施形態が、周辺デバイスをコンピュータに接続することと、デバイスからコンピュータにチャレンジを送ることと、チャレンジ及びコンピュータ内に格納された情報を用いて認証データを計算することと、コンピュータ上で実行されているクライアント・プログラムによって、コンピュータから認証データを取り出すことと、認証データを周辺デバイスに送ることと、周辺デバイスによって認証データを検証することとを含む。

【０００７】

周辺デバイスを用いてコンピュータの完全性を検証するためのシステムの例示的な実施形態が、オペレーティング・システムを含むコンピュータと、オペレーティング・システムの完全性検証を実行するように構成された、コンピュータと通信状態にある周辺デバイスとを含む。

【０００８】

この例示的な実施形態の技術を通して、さらなる特徴が実現される。他の実施形態は、本明細書で詳細に説明され、特許請求の範囲に記載された発明の一部とみなされる。例示的な実施形態の特徴をより良く理解するために、説明及び図面を参照されたい。

【０００９】

ここで、同様の要素が幾つかの図面において同様の番号で示されている図面を参照されたい。

【図面の簡単な説明】

【００１０】

【図１】完全性検証のために用いることができる周辺デバイスの実施形態を示す。

【図２】完全性検証のための周辺デバイスを組み込むシステムの実施形態を示す。
【図３】ＵＳＢ周辺デバイスを用いた完全性検証のための方法の実施形態を示す。
【図４】完全性検証の方法を示す。
【図５】周辺デバイスを用いた完全性検証のためのシステム及び方法と共に用いることができるコンピュータの実施形態を示す。
【発明を実施するための形態】
【００１１】
周辺デバイスを用いた完全性検証のためのシステム及び方法の実施形態が提供され、例示的な実施形態が以下に詳細に説明される。
【００１２】
コンピュータ上のＴＰＭは、これに限定されるものではないが、ユニバーサル・シリアル・バス（ＵＳＢ、ＵＢＳに関する一般的な情報については、http://www.usb.orgを参照されたい）周辺デバイスを含む、比較的小さく安価なタイプのハードウェアと通信して、コンピュータの完全性を検証することができる。周辺デバイスは、ＴＰＭ検証プロトコルを実行し、光を用いて又は他の適切な手段によって、例えば内蔵型ディスプレイ上に検証の結果を表示することができる。
【００１３】
ＵＳＢデバイスの実施形態は、サイズが小さなものとなる場合があり、幾つかの実施形態においては、ＵＳＢデバイスの形状は、キーフォブと似通ったものとなる場合がある。ＵＳＢデバイスが提供する機能は、変化に富んでいる。ＵＳＢデバイスは、これらに限定されるものではないが、ＵＳＢフラッシュ・メモリ・デバイス、８０２．１１　ＷＬＡＮ又はブルートゥース用の無線ネットワーク・アダプタのようなネットワーク・デバイス、キーボード、マウス、ウェブカム、暗号トークン、並びにＴＶ及びラジオ受信用のＤＶＢ－Ｔアダプタを含むことができる。
【００１４】
ＵＳＢデバイスは、ＵＳＢ規格に準拠する通信インターフェース又は相互接続部を含む。ＵＳＢの通信インターフェースは、プラグ・アンド・プレイ機能を提供する単一の標準化されたインターフェース・ソケットを用いて、多くの異なるタイプのＵＳＢ周辺デバイスをコンピュータに接続するのを可能にするように設計されたシリアル・バス・システムを含む。ＵＳＢデバイスを含むシステムは、３つの部分、すなわち、ＵＳＢホスト（例えば、ＵＳＢデバイスが接続されるコンピュータ）、ＵＳＢデバイス、及びＵＳＢ相互接続部に分けることができる。種々のバージョンの使用可能なＵＳＢ規格がある。ＵＳＢ１．１は、２つの速度、すなわち１．５Ｍビット／ｓにおける低速及び１２Ｍビット／ｓにおける最高速度をサポートする。ＵＳＢ２．０は、４８０Ｍビット／ｓにおけるより高い速度をサポートする。無線ＵＳＢのように、より速いバージョンのＵＳＢが開発中である。完全性検証のために用いられる周辺デバイスの実施形態は、任意の適切なバージョンのＵＳＢ技術を組み込むことができる。
【００１５】
ＵＳＢデバイスは、コンピュータのオペレーティング・システムと通信するために専用のデバイス・ドライバを必要とすることもあり、又は、ＵＳＢデバイスは、オペレーティング・システムが標準デバイス・ドライバを提供することができる、標準化されたデバイス・クラスに準拠することもある。デバイス・クラスは、ハブ・デバイス、メモリ・スティックのような大容量記憶装置、又はコンピュータ・キーボード及びマウスのようなヒューマン・インターフェース・デバイス、ネットワーク・インターフェース・デバイス等といった、様々なＵＳＢ周辺デバイスのために定義される。
【００１６】
図１は、完全性検証のための周辺デバイスとして用いることができる周辺デバイス１００の実施形態を示す。周辺デバイス１００は、マイクロプロセッサ・コア１０４と、メモリ・コントローラ１０５と、スタティックＲＡＭ１０１と、フラッシュ・メモリ１０２と、ＲＯＭ１０３と、割り込みコントローラ、タイマー及び電源管理を含むことができるシ

ステム・コントローラ１０７とを含む、組み込みシステムである。周辺デバイス１００内の通信コントローラは、ＵＳＡＲＴコントローラ１１１と、ＳＰＩコントローラ１１０と、Ｉ２Ｃコントローラ１０９と、ＵＳＢ通信コントローラ１１２とを含むことができる。周辺デバイス１００を含む種々のコンポーネントは、単一のシステム・オン・チップ（ＳＯＣ）デバイスによって、特定用途向け集積回路（ＡＳＩＣ）チップによって、又は幾つかの実施形態における幾つかの民生（ＣＯＴＳ）コンポーネントによって提供することができる。周辺デバイス１００の機能に応じて、特定機能向けハードウェア１１３が、システムを補完する。特定機能向けハードウェア１１３は、これに限定されるものではないが、ディスプレイ装置を含むことができる。周辺デバイス１００は、ＵＳＢクライアント・インターフェースを有する汎用組み込み型コンピュータ・デバイスの機能を果たすことができる。周辺デバイス１００上にロードされたソフトウェアが、デバイスの機能を決定することができる。

【００１７】

図２は、検証のための周辺デバイスを含むコンピュータ・システム２００の実施形態を示す。コンピュータ２０３は、オペレーティング・システム２０４を含み、このオペレーティング・システム２０４は、ネットワーク・スタック２０５、周辺デバイス・ドライバ２０６及びＴＰＭデバイス・ドライバ２０７をサポートする。ネットワーク・スタック２０５は、ネットワーク接続を介して構成サーバ２０１上の信頼できる構成のデータベース２０２及び周辺デバイス・ドライバ２０６と通信する。周辺デバイス・ドライバ２０６は、インターフェースを介して、周辺デバイス２０９上のクライアント・プログラム２１０と通信する。クライアント・プログラム２１０は、周辺デバイス２０９上のディスプレイ２１１と通信することができる。ＴＰＭデバイス・ドライバ２０７は、コンピュータ２０３上のＴＰＭ２０８と通信する。幾つかの実施形態においては、周辺デバイス２０９は、読み取り専用ＵＳＢデバイスとすることができる。

【００１８】

図３は、図２を参照して説明される周辺デバイスを用いた完全性検証のための方法３００の実施形態を示す。ブロック３０１において、コンピュータ２０３が、ブート・プロセスを開始し、ネットワーク・スタック２０５、周辺デバイス・ドライバ２０６、及びＴＰＭデバイス・ドライバ２０７を含むオペレーティング・システム２０４をブートする。ブロック３０２において、オペレーティング・システム２０４は、ＴＰＭデバイス・ドライバ２０７を介して、ブートされるソフトウェアについての認証データ及びログ情報をＴＰＭ２０８内に記録する。ブロック３０３において、周辺デバイス２０９が、コンピュータに接続される。周辺デバイス２０９との通信には、オペレーティング・システム２０４が、周辺デバイス２０９のデバイス・クラスと通信するのに適したドライバを持つことを必要とし得る。

【００１９】

ブロック３０４において、クライアント・プログラム２１０が起動される、すなわち、クライアント・プログラム２１０を、周辺デバイス２０９からロードし、コンピュータ２０３上で起動することができ、又は代替的に、クライアント・プログラム２１０をコンピュータ２０３上に予めインストールすることもできる。ブロック３０５において、ＴＰＭ２０８内に格納されている認証データの完全性検証が、周辺デバイスによって実行され、完全性検証は、図４に関して以下にさらに詳細に説明される。最後に、ブロック３０６において、周辺デバイス２０９は、ディスプレイ２１１を介して、検証の結果を知らせる。幾つかの実施形態においては、ディスプレイ２１１は、「ＯＫ」又は「ＦＡＩＬ」の語を表示して、検証の成功又は失敗を知らせることができ、或いは、ディスプレイ２１１は、緑色の光を示して検証の成功を知らせ、赤色の光を示して検証の失敗を知らせることもできる。

【００２０】

図４は、完全性検証のための方法４００の実施形態を示す。ブロック４０１において、周辺デバイス２０９は、ランダム・チャレンジを作成する。ブロック４０２において、ラ

ンダム・チャレンジが、クライアント・プログラム２１０に送られる。ブロック４０３において、クライアント・プログラム２１０は、ＴＰＭデバイス・ドライバ２０７を介して、チャレンジをＴＰＭ２０８に送る。ブロック４０４において、ＴＰＭ２０８は、チャレンジに応答して、署名された認証データ及びログ情報をクライアント・プログラム２１０に出力する。ブロック４０５において、クライアント・プログラム２１０は、認証データ及びログ情報を、検証を行う周辺デバイス２０９に送る。ブロック４０６において、認証データ及びログ情報は、周辺デバイス２０９によって検証される。周辺デバイス２０９による認証データ及びログ情報の検証は、種々の方法で実行することができる。周辺デバイス２０９は、コンピュータ２０３上のＴＰＭ２０８から受け取った認証及びログ情報を、許容可能な認証値の既知のリストと比較することができる。クライアント・プログラム２１０はまた、周辺デバイス２０９がログ・データから認証データを検証するのを可能にする証明書のリストをコンパイルすることもでき、又はクライアント・プログラムが、ネットワーク接続を介して、信頼できる構成のデータベース２０２から正確性の証明書を獲得することができる。

【００２１】

認証データを検証するために、周辺デバイス２０９は、許容可能な認証値のリストへのアクセスを必要とする。周辺デバイス２０９はまた、いずれかのサードパーティ証明書を作成するのに用いられる鍵のような、証明書の検証のために必要ないずれかの情報を必要とすることもできる。幾つかの実施形態において、周辺デバイス２０９は、この情報を有するように事前構成される。代替的な実施形態において、周辺デバイス２０９は、構成サーバ２０１からこの情報をダウンロードすることができる。鍵をダウンロードするために、周辺デバイス２０９は、公開鍵をダウンロードするために、周辺デバイス・ドライバ２０６及びネットワーク・スタック２０５を介して、これに限定されるものではないが、セキュア・ソケット・レイヤ（ＳＳＬ）接続を含む、構成サーバ２０１への接続を確立することができる。このようなダウンロードは、ユーザからの要求時に実行することができ、又は、周辺デバイス２０９が用いられる度に自動的に実行することができる。周辺デバイス２０９がオフラインであるか、又は何らかの他の理由で最新の鍵情報をダウンロードすることができない場合、周辺デバイス２０９は、構成サーバ２０１から獲得した最新の情報を用いることができる。

【００２２】

幾つかの実施形態において、周辺デバイス２０９の機能は、キーボード又は周辺ハードウェアの他の部分に組み込むことができる。幾つかの実施形態においては、周辺デバイス２０９は、これに限定されるものではないが、指紋読み取り又はデータ・ストレージを含む、付加的な機能を持つことができる。ＴＰＭ検証プロセスが成功した場合には、周辺デバイス２０９は、付加的な機能をイネーブルにすることができる。外部指紋読取装置を含む周辺デバイス２０９は、走査された指紋をコンピュータに送る前に、コンピュータ２０３の完全性を検証することができる。このようにして、走査された指紋が信頼できるコンピュータのみに送られることを保証することができる。

【００２３】

図５は、ソフトウェア内に組み込まれたような周辺デバイスを用いた完全性検証のためのシステム及び方法の例示的な実施形態により利用することができる、能力を有するコンピュータ５００の例を示す。上述の種々の動作は、コンピュータ５００の能力を利用することができる。コンピュータ５００の能力の１つ又は複数は、本明細書において説明されるいずれの要素、モジュール、アプリケーション及び／又はコンポーネント内にも組み込むことができる。

【００２４】

コンピュータ５００は、これらに限定されるものではないが、ＰＣ、ワークステーション、ラップトップ、ＰＤＡ、パーム・デバイス、サーバ、ストレージ等を含む。一般に、ハードウェア・アーキテクチャに関しては、コンピュータ５００は、ローカル・インターフェース（図示せず）を介して通信可能に結合される、１つ又は複数のプロセッサ５１０

、メモリ５２０、並びに１つ又は複数の入力及び／又は出力（Ｉ／Ｏ）デバイス５７０を含むことができる。ローカル・インターフェースは、例えば、これに限定されるものではないが、当技術分野において知られているような、１つ又は複数のバス、或いは他の有線接続若しくは無線接続とすることができる。ローカル・インターフェースは、通信を可能にするために、コントローラ、バッファ（キャッシュ）、ドライバ、中継器、及び受信機のような、付加的な要素を有することができる。さらに、ローカル・インターフェースは、前述のコンポーネント間の適切な通信を可能にするために、アドレス、制御及び／又はデータ接続を含むことができる。

【００２５】

プロセッサ５１０は、メモリ５２０内に格納することができるソフトウェアを実行するためのハードウェア・デバイスである。プロセッサ５１０は、事実上、いずれかの特注又は市販のプロセッサ、中央演算処理装置（ＣＰＵ）、データ信号プロセッサ（ＤＳＰ）、又はコンピュータ５００と関連した幾つかのプロセッサ間の補助プロセッサとすることができ、プロセッサ５１０は、（マイクロチップの形態の）半導体ベースのマイクロプロセッサ又はマクロプロセッサとすることができる。

【００２６】

メモリ５２０は、揮発性メモリ要素（例えば、ダイナミック・ランダム・アクセス・メモリ（ＤＲＡＭ）、スタティック・ランダム・アクセス・メモリ（ＳＲＡＭ）のようなランダム・アクセス・メモリ（ＲＡＭ））及び不揮発性メモリ要素（例えば、ＲＯＭ、消去可能プログラマブル読み取り専用メモリ（ＥＰＲＯＭ）、電子的消去可能プログラマブル読み取り専用メモリ（ＥＥＰＲＯＭ）、プログラマブル読み取り専用メモリ（ＰＲＯＭ）、テープ、コンパクト・ディスク読み取り専用メモリ（ＣＤ－ＲＯＭ）、ディスク、ディスケット、カートリッジ、カセット又はその種の他のもの等）のいずれか１つ又はこれらの組み合わせを含むことができる。さらに、メモリ５２０は、電子式、磁気式、光学式、及び／又は他のタイプのストレージ媒体を組み込むこともできる。メモリ５２０は、種々のコンポーネントが互いに遠く離れて配置されるが、プロセッサ５１０によってアクセスすることができる、分散型アーキテクチャを有し得ることに留意されたい

【００２７】

メモリ５２０内のソフトウェアは、各々が論理関数を実行するための実行可能な命令の順序付きリストを含む、１つ又は複数の別個のプログラムを含むことができる。メモリ５２０内のソフトウェアは、例示的な実施形態に従った、適切なオペレーティング・システム（Ｏ／Ｓ）５５０、コンパイラ５４０、ソース・コード５３０、及び１つ又は複数のアプリケーション５６０を含む。示されるように、アプリケーション５６０は、例示的な実施形態の特徴及び動作を実行するための多数の機能コンポーネントを含む。コンピュータ５００のアプリケーション５６０は、例示的な実施形態に従った、種々のアプリケーション、計算ユニット、論理、機能ユニット、プロセス、動作、仮想エンティティ、及び／又はモジュールを表すことができるが、アプリケーション５６０は、限定することを意図するものではない。

【００２８】

オペレーティング・システム５５０は、他のコンピュータ・プログラムの実行を制御し、スケジューリング、入力－出力制御、ファイル及びデータ管理、メモリ管理、並びに通信制御及び関連サービスを提供する。例示的な実施形態を実施するためのアプリケーション５６０は、全ての市販のオペレーティング・システム上で適用可能である。

【００２９】

アプリケーション５６０は、ソース・プログラム、実行可能プログラム（オブジェクト・コード）、スクリプト、又は実行される１組の命令を含むいずれかの他のエンティティとすることができる。ソース・プログラムである場合には、プログラムは、通常、ＯＳ５５０と接続して適切に動作するように、メモリ５２０内に含まれることも含まれないこともある、（コンパイラ５４０のような）コンパイラ、アセンブラ、インタープリタ等を介して翻訳される。さらに、アプリケーション５６０は、これに限定されるものではない

が、データ・クラス及び方法を有するオブジェクト指向プログラミング言語、又はこれらに限定されるものではないが、例えばＣ、Ｃ＋＋、Ｃ＃、Ｐａｓｃａｌ、ＢＡＳＩＣ、ＡＰＩ呼び出し、ＨＴＭＬ、ＸＨＴＭＬ、ＸＭＬ、ＡＳＰスクリプト、ＦＯＲＴＲＡＮ、ＣＯＢＯＬ、Ｐｅｒｌ、Ｊａｖａ、ＡＤＡ，．ＮＥＴ等の、ルーチン、サブルーチン及び／又は関数を有する手続き型プログラミング言語を含む、いずれかのタイプの使用可能なプログラミング言語として書くことができる。

【００３０】

Ｉ／Ｏデバイス５７０は、例えば、これらに限定されるものではないが、マウス、キーボード、スキャナ、マイクロフォン、カメラ等のような入力デバイスを含むことができる。さらに、Ｉ／Ｏデバイス５７０はまた、例えば、これらに限定されるものではないが、プリンタ、ディスプレイ等の出力デバイスを含むこともできる。最後に、Ｉ／Ｏデバイス５７０は、例えば、これらに限定されるものではないが、ＮＩＣ又は変調器／復調器（遠隔デバイス、他のファイル、デバイス、システム、又はネットワークにアクセスするための）、無線周波数（ＦＲ）又は他の送受信機、電話インターフェース、ブリッジ、ルータ等の、入力及び出力の両方を通信するデバイスをさらに含むことができる。Ｉ／Ｏデバイス５７０はまた、インターネット又はイントラネットのような、種々のネットワークにわたって通信するためのコンポーネントを含むこともできる。

【００３１】

コンピュータ５００がＰＣ、ワークステーション等である場合には、メモリ５２０内のソフトウェアは、基本入力出力システム（ＢＩＯＳ）（簡単にするために省略されている）をさらに含むことができる。ＢＩＯＳは、起動時にハードウェアを初期化し、試験し、Ｏ／Ｓ５５０を開始し、ハードウェア・デバイス間のデータ転送をサポートする、１組の本質的なソフトウェア・ルーチンである。ＢＩＯＳは、ＲＯＭ、ＰＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ等のような、いずれかのタイプの読み取り専用メモリ内に格納され、コンピュータ５００が作動されたときに、ＢＩＯＳを実行することができる。

【００３２】

コンピュータ５００が動作中のとき、プロセッサ５１０は、メモリ５２０内に格納されたソフトウェアを実行し、メモリ５２０との間でデータを通信し、一般にソフトウェアによってコンピュータ５００の動作を制御するように構成される。アプリケーション５６０及びＯＳ５５０は、プロセッサ５１０によって、全体的に又は部分的に読み取られ、恐らくはプロセッサ５１０内にバッファリングされ、その後実行される。

【００３３】

アプリケーション５６０がソフトウェア内に実装されているとき、アプリケーション５６０は、いずれかのコンピュータ関連のシステム又は方法によって、又はそれと接続して用いるための、事実上いずれかのコンピュータ可読媒体上に格納することができることに留意すべきである。本明細書の文脈においては、コンピュータ可読媒体は、コンピュータ関連のシステム又は方法によって、又はそれと接続して用いるためのコンピュータ・プログラムを収容し、又は格納することができる、電子式、磁気式、光学式、又は他の物理デバイス若しくは手段とすることができる。

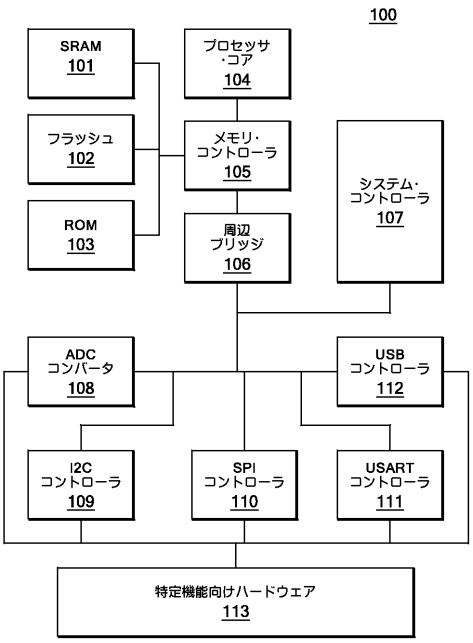
【００３４】

アプリケーション５６０は、コンピュータ・ベースのシステム、プロセッサ収容システム、又は命令実行システム、装置又はデバイスから命令をフェッチし、命令を実行することができる他のシステムのような、命令実行システム、装置、又はデバイスによって、又はそれと接続して用いるためのいずれかのコンピュータ可読媒体において具体化することができる。本明細書の文脈においては、「コンピュータ可読媒体」とは、命令実行システム、装置又はデバイスによって、又はそれと接続して用いるためのプログラムを格納し、通信し、伝播し、又は移送することができるいずれかの手段とすることができる。コンピュータ可読媒体は、例えば、これらに限定されるものではないが、電子的、磁気的、光学的、電磁気的、赤外線、又は半導体のシステム、装置、デバイス又は伝播媒体とすることができる。

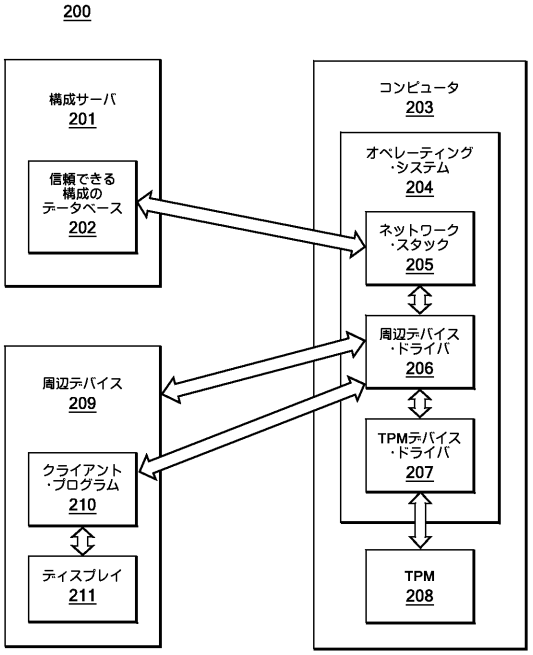
【００３５】
コンピュータ可読媒体のより具体的な例（非網羅的なリスト）は、以下のもの、すなわち、１つ又は複数の配線を有する電気的接続（電子的）、ポータブル・コンピュータ・ディスケット（磁気的又は光学的）、ランダム・アクセス・メモリ（ＲＡＭ）（電子的）、読み取り専用メモリ（ＲＯＭ）（電子的）、消去可能プログラマブル読み取り専用メモリ（ＥＰＲＯＭ、ＥＥＰＲＯＭ又はフラッシュ・メモリ）（電子的）、光媒体（光学的）及びポータブル・コンパクト・ディスク・メモリ（ＣＤＲＯＭ、ＣＤ　Ｒ／Ｗ）（光学的）を含むことができる。プログラムは、例えば紙又は他の媒体の光学操作を介して電子的に取り込み、次いで必要に応じて、コンパイルするか、解釈するか、又は適切な方法で処理し、次いでコンピュータのメモリに格納することができることから、コンピュータ可動媒体は、プログラムが印刷又はパンチされた紙又は別の適切な媒体とすることさえ可能であることに留意されたい。
【００３６】
アプリケーション５６０がハードウェア内に実装されている例示的な実施形態においては、アプリケーション５６０は、各々が当技術分野において周知の以下の技術、すなわち、データ信号上で論理関数を実行するための論理ゲートを有する個別論理回路、適切な組み合わせ論理ゲートを有する特定用途向け集積回路（ＡＳＩＣ）、プログラマブル・ゲート・アレイ（ＰＧＡ）、フィールド・プログラマブル・ゲート・アレイ（ＦＰＧＡ）等のいずれか１つ又はこれらの組み合わせによって実行することができる。
【００３７】
例示的な実施形態の技術的な効果及び利点は、検証装置の役割を果たすために、別個の本格的で一般的に高価な機械なしで、コンピュータのオペレーティング・システムを危険にさらさないことを検証する能力を含み、セキュリティの向上を可能にする。
【００３８】
本明細書で用いられる用語は、特定の実施形態を説明する目的のためのものにすぎず、本発明を限定することを意図するものではない。本明細書で用いられる場合、文脈から明らかにそうでないことが示されていない限り、「ａ」、「ａｎ」及び「ｔｈｅ」の単数形は、複数形も同様に含むことが意図される。「含む（ｃｏｍｐｒｉｓｅｓ）」及び／又は「含んでいる（ｃｏｍｐｒｉｓｉｎｇ）」という用語は、本発明において用いられる場合、言明された特徴、整数、ステップ、動作、要素、及び／又はコンポーネントの存在を特定するものではあるが、１つ又は複数の他の特徴、整数、ステップ、動作、コンポーネント、及び／又はそれらの群の存在又は追加を排除するものではないこともさらに理解されるであろう。
【００３９】
以下の特許請求の範囲における全ての「手段又はステップと機能との組合せ」要素の対応する構造、材料、行為及び均等物は、その機能を、明確に特許請求されているように他の特許請求された要素と組み合わせて実行するための、いかなる構造、材料又は行為をも含むことが意図される。本発明の説明は、例示及び説明の目的で提示されたものであるが、網羅的であることを意図するものではなく、本発明を開示された形態に限定することを意図するものでもない。本発明の範囲及び思想から逸脱することのない多くの変更及び変形が、当業者には明らかである。実施形態は、本発明の原理及び実際の用途を最も良く説明するため、及び、当業者が本発明を種々の変更を有する種々の実施形態について企図される特定の使用に好適なものとして理解することを可能にするために、選択及び記載された。
【符号の説明】
【００４０】
１００：周辺デバイス
１０１：スタティックＲＡＭ
１０２：フラッシュ・メモリ
１０３：ＲＯＭ

１０４：マイクロプロセッサ・コア
１０５：メモリ・コントローラ
１０７：システム・コントローラ
１０９：Ｉ２Ｃコントローラ
１１０：ＳＰＩコントローラ
１１１：ＵＳＡＲＴコントローラ
１１２：ＵＳＢ通信コントローラ
１１３：特定機能向けハードウェア
２００：コンピュータ・システム
２０１：構成サーバ
２０２：構成のデータベース
２０３、５００：コンピュータ
２０４、５５０：オペレーティング・システム
２０５：ネットワーク・スタック
２０６：周辺デバイス・ドライバ
２０７：ＴＰＭデバイス・ドライバ
２０８：ＴＰＭ
２０９：周辺デバイス
２１０：クライアント・プログラム
２１１：ディスプレイ
３００、４００：方法
５１０：プロセッサ
５２０：メモリ
５３０：ソース・コード
５４０：コンパイラ
５６０：アプリケーション
５７０：入力及び/又は出力（Ｉ／Ｏ）デバイス

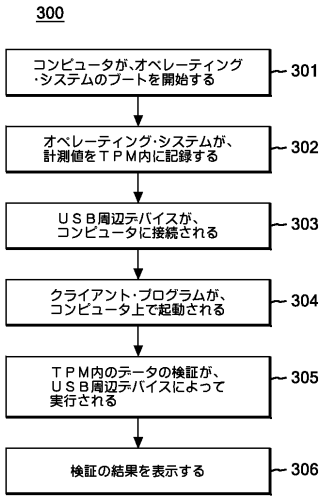
【図１】


100
SRAM
101
プロセッサ
・コア
104
フラッシュ
102
メモリ・
コントローラ
105
システム・
コントローラ
107
ROM
103
周辺
ブリッジ
106
ADC
コンバータ
108
USB
コントローラ
112
I2C
コントローラ
109
SPI
コントローラ
110
USART
コントローラ
111
特定機能向けハードウェア
113

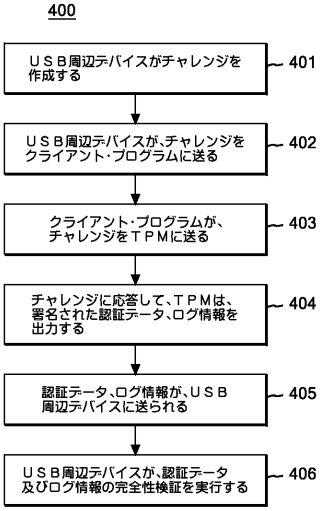
【図２】


200
構成サーバ
201
信頼できる
構成の
データベース
202
コンピュータ
203
オペレーティング
・システム
204
ネットワーク
・スタック
205
周辺デバイス
・ドライバ
206
TPMデバイス
・ドライバ
207
TPM
208
周辺デバイス
209
クライアント
・プログラム
210
ディスプレイ
211

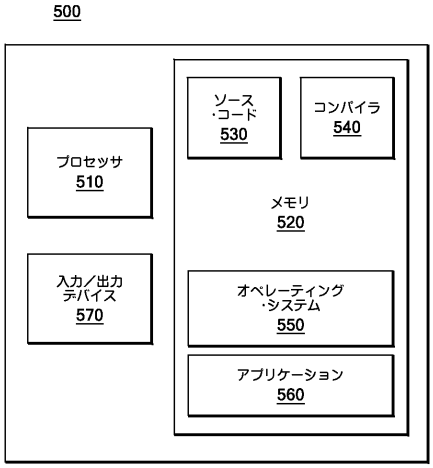
【図３】


300
コンピュータが、オペレーティング
・システムのブートを開始する
301
オペレーティング・システムが、
計測値をＴＰＭ内に記録する
302
ＵＳＢ周辺デバイスが、
コンピュータに接続される
303
クライアント・プログラムが、
コンピュータ上で起動される
304
ＴＰＭ内のデータの検証が、
ＵＳＢ周辺デバイスによって
実行される
305
検証の結果を表示する
306

【図４】


400
ＵＳＢ周辺デバイスがチャレンジを
作成する
401
ＵＳＢ周辺デバイスが、チャレンジを
クライアント・プログラムに送る
402
クライアント・プログラムが、
チャレンジをＴＰＭに送る
403
チャレンジに応答して、ＴＰＭは、
署名された認証データ、ログ情報を
出力する
404
認証データ、ログ情報が、ＵＳＢ
周辺デバイスに送られる
405
ＵＳＢ周辺デバイスが、認証データ
及びログ情報の完全性検証を実行する
406

【図５】



【手続補正書】
【提出日】平成23年10月28日(2011.10.28)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
周辺デバイスであって、
コンピュータ、前記周辺デバイスと通信するように構成されたインターフェースと、
前記コンピュータのオペレーティング・システムの完全性検証を実行するように構成された論理と、
前記完全性検証の結果を表示するように構成されたディスプレイと、
を含む周辺デバイス。
【請求項２】
前記インターフェースは、ＵＳＢ（ユニバーサル・シリアル・バス）インターフェースを含み、前記周辺デバイスは、ＵＳＢ周辺デバイスを含む、請求項１に記載の周辺デバイス。
【請求項３】
前記周辺デバイスは、読み取り専用デバイスである、請求項１に記載の周辺デバイス。
【請求項４】
前記コンピュータは、前記オペレーティング・システムに関する認証データを格納するように構成された、信頼できるプラットフォーム・モジュールを含む、請求項１に記載の周辺デバイス。

【請求項５】
前記論理は、前記コンピュータ上で実行されるように構成されたクライアント・プログラムを含み、前記クライアント・プログラムは、ネットワークを介して、構成サーバから、前記完全性検証を実行するために必要とされる情報を受信するようにさらに構成される、請求項１に記載の周辺デバイス。
【請求項６】
前記周辺デバイスは、完全性検証を実行するのに用いるための認証値の既知のリストを含む、請求項１に記載の周辺デバイス。
【請求項７】
前記周辺デバイスは、外部指紋読取装置をさらに含み、前記外部指紋読取装置は、完全性検証が成功した場合に、走査された指紋を前記コンピュータに送るように構成される、請求項１に記載の周辺デバイス。
【請求項８】
前記周辺デバイスは、キーボード、マウス、又はネットワーク・デバイスのうちの１つを含む、請求項１に記載の周辺デバイス。
【請求項９】
周辺デバイスを用いたコンピュータの完全性検証のための方法であって、
前記周辺デバイスを前記コンピュータに接続することと、
前記デバイスから前記コンピュータにチャレンジを送ることと、
前記チャレンジ及び前記コンピュータ内に格納された情報を用いて認証データを計算することと、
前記コンピュータ上で実行されているクライアント・プログラムによって、前記コンピュータから前記認証データを取り出すことと、
前記認証データを前記周辺デバイスに送ることと、
前記周辺デバイスによって前記認証データを検証することと、
を含む方法。
【請求項１０】
前記認証データは、前記コンピュータ上の信頼できるプラットフォーム・モジュールからの情報を用いて計算される、請求項９に記載の方法。
【請求項１１】
前記周辺デバイスにより前記検証の結果を表示することをさらに含む、請求項９に記載の方法。
【請求項１２】
構成サーバから、前記検証を実行するのに必要な情報を前記周辺デバイスにより受信することをさらに含む、請求項９に記載の方法。
【請求項１３】
前記周辺デバイスは、ユニバーサル・シリアル・バス（ＵＳＢ）デバイスを含む、請求項９に記載の方法。
【請求項１４】
周辺デバイスを用いてコンピュータの完全性を検証するためのシステムであって、
オペレーティング・システムを含むコンピュータと、
前記オペレーティング・システムの完全性検証を実行するように構成された、前記コンピュータと通信状態にある周辺デバイスと、
を含むシステム。
【請求項１５】
前記コンピュータは、前記オペレーティング・システムに関する認証データを格納するように構成された信頼できるプラットフォーム・モジュールを含む、請求項１４に記載のシステム。
【請求項１６】
前記周辺デバイスと通信状態にある構成サーバをさらに含む、請求項１４に記載のシス

テム。
【請求項１７】
前記周辺デバイスは、ユニバーサル・シリアル・バス（ＵＳＢ）デバイスである、請求項１４に記載のシステム。
【請求項１８】
前記周辺デバイスは、指紋スキャナをさらに含む、請求項１４に記載のシステム。
【請求項１９】
前記周辺デバイスは、前記完全性検証を実行するのに用いるための認証値の既知のリストを含む、請求項１４に記載のシステム。
【請求項２０】
周辺デバイス（２０９）を用いたコンピュータ（２０３）の完全性検証のための方法（３００）であって、
前記コンピュータ（２０３）が、周辺デバイス・ドライバ（２０６）及びＴＰＭデバイス・ドライバ（２０７）を含むオペレーティング・システム（２０４）のブートを開始するステップ（３０１）と、
前記コンピュータ（２０３）に含まれるオペレーティング・システム（２０４）が、ＴＰＭデバイス・ドライバ（２０７）を介して、ブートされるソフトウエアについての認証データ及びログ情報を前記コンピュータ（２０３）上のＴＰＭ（２０８）に記録するステップ（３０２）と、
前記周辺デバイス（２０９）を前記コンピュータ（２０３）に接続される（３０３）ことに応答して、周辺デバイス（２０９）上のクライアント・プログラム（２１０）を前記コンピュータ（２０３）上にロードして、または、予めインストールしておき、起動するステップ（３０４）と、
前記周辺デバイス（２０９）が、ＴＰＭ（２０８）に記録されている認証データの完全性検証を実行するステップ（３０５）と、
認証データの完全性検証の結果（成功又は失敗）を、ディスプレイ（２１１）を介して表示するステップ（３０６）とを有する、
前記方法（３００）。
【請求項２１】
請求項２０の方法（３００）における、前記周辺デバイス（２０９）が、ＴＰＭ（２０８）に記録されている認証データの完全性検証を実行するステップ（３０５）が、
前記周辺デバイス（２０９）が、ランダム・チャレンジを作成するステップ（４０１）と、
ランダム・チャレンジをクライアント・プログラム（２１０）に送るステップ（４０２）と、
クライアント・プログラム（２１０）が、ＴＰＭデバイス・ドライバ（２０７）を介して、ランダム・チャレンジをＴＰＭ（２０８）に送るステップ（４０３）と、
ＴＰＭ（２０８）が、送られたランダム・チャレンジに応答して、記録されている認証データ及びログ情報を、前記周辺デバイス（２０９）に送り、クライアント・プログラム（２１０）に出力するステップ（４０４、４０５）と
前記周辺デバイス（２０９）が、認証データ及びログ情報の完全性検証を実行するステップ（４０６）とを有する、
前記方法（４００）。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2010/051027

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009/049510 A1 (ZHANG XINWEN [US] ET AL) 19 February 2009 (2009-02-19) the whole document	1-4, 6-11, 13-15, 17-19
A	BAJIKAR S: "Trusted Platform Module (TPM) based Security on Notebook PCs - White Paper" INTERNET CITATION, [Online] 20 June 2002 (2002-06-20), XP002259678 Retrieved from the Internet: URL:http://www.intel.com/design/mobile/platform/downloads/trusted platform module white paper pdf> [retrieved on 2003-10-28] the whole document	1-4, 6-11, 13-15, 17-19

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 June 2010	23/09/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Mäenpää, Jari

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2010/051027

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-4, 6-11, 13-15, 17-19

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

International Application No. PCT/IB2010/051027

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-4, 6-11, 13-15, 17-19

A peripheral device, method and system comprising a display configured to display a result of the integrity verification of a computer by a peripheral device.

---

2. claims: 5, 12, 16

A peripheral device, method and system for verifying integrity of a computer using a peripheral device wherein a configuration server is in communication with the peripheral device.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2010/051027

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009049510 A1	19-02-2009	NONE	

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PE,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
１．ＪＡＶＡ

(72)発明者 ヘルマン、レトー、ヨーゼフ
スイス連邦国 ＣＨ－８８０３ リュシュリコン ソイマーシュトラーセ ４
(72)発明者 ユーリッヒ、クラウス
スイス連邦国 ＣＨ－８８０３ リュシュリコン ソイマーシュトラーセ ４
(72)発明者 シュンター、マティアス
スイス連邦国 ＣＨ－８８０３ リュシュリコン ソイマーシュトラーセ ４