(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6301582号
(P6301582)
(45)発行日　平成30年3月28日(2018.3.28)　(24)登録日　平成30年3月9日(2018.3.9)

(51)Int.Cl.　　F I
G06F 21/57 (2013.01)　　G06F 21/57 350
G06F 9/4401 (2018.01)　　G06F 9/06 610K

請求項の数 10　(全 19 頁)

(21)出願番号　特願2013-1237(P2013-1237)
(22)出願日　平成25年1月8日(2013.1.8)
(65)公開番号　特開2013-143143(P2013-143143A)
(43)公開日　平成25年7月22日(2013.7.22)
審査請求日　平成27年9月3日(2015.9.3)
審判番号　不服2017-2339(P2017-2339/J1)
審判請求日　平成29年2月17日(2017.2.17)
(31)優先権主張番号　13/346,574
(32)優先日　平成24年1月9日(2012.1.9)
(33)優先権主張国　米国(US)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100192636
弁理士　加藤　隆夫
(72)発明者　ソォン・ジョシュアヌ
アメリカ合衆国，カリフォルニア州　９４０８５，サニーヴェイル，エスカロン・アヴェニュ　１０５５番，９０６号

最終頁に続く

(54)【発明の名称】信頼されるネットワーク・ブートのシステムおよび方法

(57)【特許請求の範囲】
【請求項１】
サーバーの信頼されるネットワーク・ブーティングのためのシステムであって、当該システムは：
ブーティング・イメージを含むブーティング・サーバーと；
前記ブーティング・サーバーの前記ブーティング・イメージを用いてブートするネットワーク・サーバーであって、前記ブーティング・イメージの測定値を得る信頼アンカーを含むネットワーク・サーバーと；
ネットワークへのアクセスを制御するネットワーク・コントローラであって、前記ネットワーク・サーバーが前記ネットワークにアクセスすることを許可する前に前記ブーティング・イメージの前記測定値を検証する、ネットワーク・コントローラとを有し、
前記信頼アンカーは、スタートアップ時に前記ネットワーク・サーバーによって最初に実行されるプログラムの測定値を得て、そのプログラムの測定値を前記ネットワーク・コントローラに送り、
前記信頼アンカーは、前記ネットワーク・サーバー内の信頼プロセッサである、または、前記ネットワーク・サーバー内の信頼されるプラットフォーム・モジュール（TPM）チップである、
システム。
【請求項２】
前記ブーティング・サーバーが、ブート前実行環境プロトコルに従って前記ネットワー

ク・サーバーと通信する、請求項１記載のシステム。
【請求項３】
前記信頼アンカーが、前記ブーティング・イメージのハッシュ値を生成することによって前記ブーティング・イメージの前記測定値を得る、請求項１記載のシステム。
【請求項４】
前記ネットワーク・コントローラが前記ブーティング・イメージの前記測定値を検証することを、前記信頼アンカーによって得られた前記ブーティング・イメージの前記測定値を、前記ブーティング・イメージの検証済みの測定値と比較することによって検証する、請求項１記載のシステム。
【請求項５】
前記ネットワーク・コントローラは、前記ネットワーク・サーバーが前記ネットワークにアクセスすることを許可する前に前記信頼アンカーの署名を検証する、請求項１記載のシステム。
【請求項６】
ネットワーク・サーバー内の信頼アンカーとして動作するプロセッサであって：
前記信頼アンカーは、前記ネットワーク・サーバー内の信頼プロセッサである、または、前記ネットワーク・サーバー内の信頼されるプラットフォーム・モジュール（TPM）チップであり、
前記ネットワーク・サーバーによってブートするために使用される、第一のネットワークを通じて受信されたブーティング・イメージの測定値を取得する工程と；
前記ブーティング・イメージの前記測定値を、第二のネットワークへのアクセスを得るための検証のために送る工程と；
スタートアップ時に前記ネットワーク・サーバーによって最初に実行されるプログラムの測定値を得て、そのプログラムの測定値をネットワーク・コントローラに送る工程とを実行するよう適応された、
プロセッサ。
【請求項７】
検証のために署名を送る工程を実行するようさらに適応されている、請求項６記載のプロセッサ。
【請求項８】
前記ブーティング・イメージの前記測定値を取得する工程が、前記ブーティング・イメージについてのハッシュ値を生成することを含む、請求項６記載のプロセッサ。
【請求項９】
前記ネットワーク・サーバーの信頼されるネットワーク・ブーティングのためのシステムであって：
当該システム内で前記ネットワーク・サーバーの前記信頼アンカーとして動作する請求項６記載のプロセッサと；
前記ネットワーク・サーバーによってブートするときに使用される前記ブーティング・イメージを含むブーティング・サーバーとを有する、
システム。
【請求項１０】
前記ブーティング・イメージの前記測定値を検証し、前記第二のネットワークへのアクセスを制御するネットワーク・コントローラをさらに有する、請求項９記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本稿で論じる実施形態はデジタル処理システムに関する。
【背景技術】
【０００２】
データ・クラウドのようなデータ・ネットワークは、ウェブベースのアプリケーション

のようなネットワーク・ベースのツールを通じてユーザーに計算、ソフトウェア、データ・アクセス、ストーレジ・サービスおよびその他のサービスを提供する一つまたは複数のサーバーおよび他のデジタル処理型コンポーネントを使って形成されうる。一般に、ユーザーは、ネットワーク内での位置付けのために、ネットワーク・プロバイダーにソフトウェア、データまたは他のオブジェクトを提供しうる。ユーザーはのちに、ネットワーク・ベースのツールを使って該ソフトウェア、データまたは他のオブジェクトにアクセスしうる。

【発明の概要】

【発明が解決しようとする課題】

【０００３】

データ・ネットワーク・プロバイダーの責任は、ネットワークへのユーザー・アクセスを提供し、ユーザーのソフトウェア、データ、物理的および個人的セキュリティならびにネットワーク上に記憶されている素性情報（identity）を安全に維持するためのセキュリティを提供することでありうる。このセキュリティを提供するために、ネットワーク・プロバイダーは、信頼されるサーバー、データベースおよび他のデジタル型コンポーネントのみがネットワークにアクセスすることを保証するよう試みてもよい。

【０００４】

本願で特許請求される主題は、何らかの欠点を解消するまたは上記のような環境でのみ機能する実施形態には限定されない。むしろ、この背景は、本稿に記載されるいくつかの実施形態を実施しうる一つの例示的な技術分野を例示するために与えているだけである。

【課題を解決するための手段】

【０００５】

ある実施形態のある側面によれば、システムは、ブーティング・イメージを含んでいてもよいブーティング・サーバーと、前記ブーティング・サーバーからの前記ブーティング・イメージを用いてブートしてもよいネットワーク・サーバーとを含んでいてもよい。前記ネットワーク・サーバーは、前記ブーティング・イメージの測定値を得る信頼アンカーを含んでいてもよい。本システムはさらに、ネットワークへのアクセスを制御するネットワーク・コントローラを含んでいてもよい。前記ネットワーク・コントローラは、前記ネットワーク・サーバーが前記ネットワークにアクセスすることを許可する前に前記ブーティング・イメージの前記測定値を検証してもよい。

【０００６】

実施形態の目的および利点は、請求項において具体的に記載される要素および組み合わせによって実現され、達成されるであろう。

【０００７】

以上の概括的な記述および以下の詳細な記述は例示および説明するものであり、特許請求される発明を制約するものではないことを理解しておくべきである。

【図面の簡単な説明】

【０００８】

例示的な実施形態について、付属の図面を使ってさらに具体的かつ詳細に記述し、説明する。

【図１】ネットワーク・サーバーの信頼されるネットワーク・ブーティングを提供するシステムを示す図である。

【図２】ネットワーク・サーバーの信頼されるネットワーク・ブーティングを提供するシステムの一部を示す図である。

【図３】ネットワーク・サーバーの信頼されるネットワーク・ブーティングを提供するシステムの一部を示す図である。

【図４】複数のネットワーク・サーバーの信頼されるネットワーク・ブーティングを提供するシステムを示す図である。

【図５】みな本稿に記載される少なくともいくつかの実施形態に基づいて構成される、サーバーの信頼されるネットワーク・ブーティングのための方法の例示的なフローチャート

である。

【発明を実施するための形態】

【０００９】

データ・クラウドのようなデータ・ネットワークは、一つまたは複数のサーバーおよび他のコンポーネントから形成されうる。データ・ネットワークが形成されるときおよび何らかの動作条件の間に、追加的なサーバーが該データ・ネットワークに追加されてもよい。データ・ネットワークにサーバーを追加するためには、サーバーはまずローカルにブートされるまたはネットワーク・ブートされうる。安全なデータ・ネットワークの場合、該安全なデータ・ネットワークの健全性を維持するため、信頼されるサーバーのみが該安全なデータ・ネットワークに参加しうる。

【００１０】

安全なデータ・ネットワークに参加してもよい信頼されるサーバーを確立するために、サーバーは、該安全なデータ・ネットワークによって信頼される信頼アンカーを含んでいてもよい。信頼アンカーは、そのサーバーによって実行される内部ソフトウェアまたはファームウェアおよびネットワーク・ブーティング・プロセスの間にネットワークを通じてダウンロードされるソフトウェアを測定してもよい。一般に、信頼アンカーは、ブートされたあとにサーバーの状態を補足してもよい。信頼アンカーは測定結果を、安全なデータ・ネットワークへのアクセスを制御するネットワーク・コントローラに送ってもよい。ネットワーク・コントローラは、信頼アンカーによって取られた測定値を使ってそのサーバーが信頼される状態にあることを検証してもよい。サーバーは信頼される状態にあれば、サーバーは安全なデータ・ネットワークに参加することが許されてもよい。

【００１１】

本発明のさらなる詳細および実施形態について、付属の図面を参照しつつ説明する。

【００１２】

図１は、少なくとも本稿に記載されるいくつかの実施形態に基づいて構成された、ネットワーク・サーバーの信頼されるネットワーク・ブーティングのための備えを提供する。システム１００は、ネットワーク・サーバー１１０、ブーティング・サーバー１３０、セキュリティで保護された（secured）ネットワーク・コントローラ１５０およびセキュリティで保護されたネットワーク１６０を通信可能に結合するネットワーク１４０を含んでいてもよい。

【００１３】

図示した実施形態によれば、システム１００は、リモート・サーバーをブートするよう動作してもよく、次いで該リモート・サーバーがセキュリティで保護されたネットワーク１６０に加入させられてもよい。ネットワーク・サーバー１１０は、セキュリティで保護されたネットワーク１６０に加入させられてもよいリモート・サーバーの例である。システム１００はまずネットワーク・サーバー１１０を電源投入してもよく、ネットワーク・サーバー１１０内の信頼アンカー１２０を使ってネットワーク・サーバー１１０によって実行される初期ソフトウェアまたはファームウェアを測定してもよい。次いでネットワーク・サーバー１１０は、ブーティング・サーバー１３０を使ってネットワーク１４０からブートしてもよい。ネットワーク・サーバー１１０はブーティング・イメージおよび他のソフトウェア・モジュールをブーティング・サーバー１３０から受け取る際、信頼アンカー１２０はブーティング・イメージおよびソフトウェア・モジュールを測定してもよい。

【００１４】

ネットワーク・サーバー１１０がブートされたのち、信頼アンカー１２０は初期ソフトウェア、ブーティング・イメージおよびソフトウェア・モジュールの測定結果を、署名されたレポートにおいて、セキュリティで保護されたネットワーク・コントローラ１５０に送ってもよい。セキュリティで保護されたネットワーク・コントローラ１５０は、信頼アンカー１２０が信頼されうることを検証するために、信頼アンカー１２０の署名を検査してもよい。セキュリティで保護されたネットワーク・コントローラ１５０は次いで初期ソフトウェア、ブーティング・イメージおよびソフトウェア・モジュールの測定値を検証し

て、ネットワーク・サーバー１１０が信頼されうるか否かを判定してもよい。

【００１５】

セキュリティで保護されたネットワーク・コントローラ１５０がネットワーク・サーバー１１０が信頼されることを検証したのち、ネットワーク・サーバー１１０は、セキュリティで保護されたネットワーク１６０に参加することが許される。ネットワーク・サーバー１１０が信頼されると判明しなかった場合には、ネットワーク・サーバー１１０はセキュリティで保護されたネットワーク１６０へのアクセスを拒否されてもよい。システム１００はこのようにして、ネットワーク・サーバー１１０のような個々の信頼されるリモート・サーバーがネットワーク・ブートされ、セキュリティで保護されたネットワーク１６０に参加させられることを許容する構造を提供する。セキュリティで保護されたネットワーク・コントローラ１５０は、個々のリモート・サーバーがセキュリティで保護されたネットワーク１６０に参加することを許容する前に、個々のリモート・サーバー内の信頼されるアンカーを信頼するだけでよい。対照的に、他のネットワーク・ブーティング環境は、個々のリモート・サーバーがセキュリティで保護されたネットワークに参加することを許容する前に、信頼の複数のレイヤーを発達させることを必要とすることがある。

【００１６】

信頼のレベルまたはネットワーク・サーバー１１０のようなリモート・サーバーがいかにして信頼されると判定されるかはさまざまでありうる。いくつかの実施形態では、リモート・サーバーは、該リモート・サーバーもその上で走るファームウェアもしくはソフトウェアのいずれも、いかなる源によっても、システム１００の運用者の知らないうちに危殆化、変更、改変または他の仕方で影響されていない場合に、信頼されると考えられてもよい。いくつかの実施形態では、リモート・サーバーは、該リモート・サーバー内の信頼アンカーが、該リモート・サーバーまたはその上で走るファームウェアもしくはソフトウェアのいずれかが、何らかの源によって、システム１００の運用者の知らないうちに危殆化、変更、改変または他の仕方で影響されていないかどうかを検出できない場合に、信頼されると考えられてもよい。同様に、いくつかの実施形態では、リモート・サーバーは、該リモート・サーバー内の信頼アンカーが検証され、該信頼アンカーが該リモート・サーバーまたはその上で走るファームウェアもしくはソフトウェアのいずれかが、システム１００の運用者の知っているうちまたは知らないうちに危殆化、変更、改変または他の仕方で影響されていないかどうかを検出できない場合に、信頼されると考えられてもよい。同様に、いくつかの実施形態では、リモート・サーバーは、該リモート・サーバー内の信頼アンカーが検証され、該信頼アンカーが該リモート・サーバーまたはその上で走るファームウェアもしくはソフトウェアのいずれかに対する軽微な変更または改変しか検出できない場合に、信頼されると考えられてもよい。以上から、サーバーの信頼されるネットワーク・ブートが一般にどのようなことに関わるか、また種々の度合いの信頼が存在でき、ネットワークの運用者によって定義されうることが理解されるはずである。

【００１７】

図２は、本稿に記載される少なくともいくつかの実施形態に基づいて構成された、ネットワーク・サーバーの信頼されるネットワーク・ブーティングを提供することを支援しうるサブシステム２００を示している。サブシステム２００はネットワーク２４０を通じてブーティング・サーバー２３０に通信可能に結合されるネットワーク・サーバー２１０を含んでいてもよい。ネットワーク・サーバー２１０は、プロセッサ２１２と、スタートアップ記憶装置２１４と、プログラム記憶装置２１６と、該プロセッサ２１２、スタートアップ記憶装置２１４およびプログラム記憶装置２１６を信頼アンカー２２０に接続する通信バス２１８とを含んでいてもよい。信頼アンカー２２０は信頼プロセッサ２２２および第一、第二、第三および第四の記憶ユニット２２３、２２４、２２５、２２６を含んでいてもよい。

【００１８】

いくつかの実施形態に基づくネットワーク・サーバー２１０の信頼されるネットワーク・ブートを実行するために、ネットワーク・サーバー２１０はまず電源投入される。電源

投入時に、プロセッサ２１２は、スタートアップ記憶装置２１４に記憶されたプログラムにアクセスしてもよい。いくつかの実施形態では、スタートアップ記憶装置２１４は、これに限られないが、フラッシュ・メモリ、読み出し専用メモリおよび磁気メモリを含む不揮発性メモリの任意の型であってもよい。いくつかの実施形態では、スタートアップ記憶装置２１４に保持されるプログラムは、スタートアップ時にネットワーク・ブーティングのための基本機能を実行するためにネットワーク・サーバー２１０によって使用される基本入出力システム（BIOS: basic input/output system）ファームウェアであってもよい。

【００１９】

電源投入時に、信頼プロセッサ２２２はまた、スタートアップ記憶装置２１４内のプログラムを読み、測定する。いくつかの実施形態では、信頼プロセッサ２２２は、そのプログラムの確率論的に一意的な識別子である値を生成することによってそのプログラムを測定してもよい。該識別子は、これに限られないが、ハッシュ値、チェックサム、フィンガープリントまたはチェック・ディジットといったものである。いくつかの実施形態では、信頼プロセッサ２２２は、プログラムがプロセッサ２１２によって実行される前に、該プログラムを読み、測定してもよい。いくつかの実施形態では、信頼プロセッサ２２２は、プログラムがプロセッサ２１２によって実行されたあとに該プログラムを読み、測定してもよい。信頼プロセッサ２２２は、プログラムの測定結果を第一、第二、第三または第四の記憶ユニット２２３、２２４、２２５、２２６の一つに保存する。

【００２０】

ネットワーク・サーバー２１０がスタートアップ記憶装置２１４からプログラムをロードしたのち、ネットワーク・サーバー２１０は、ネットワーク２４０上でブーティング・サーバー２３０を位置特定するために、該プログラムにより一つまたは複数の動作を実行してもよい。ブーティング・サーバー２３０を位置特定したのち、ネットワーク・サーバー２１０はブーティング・サーバー２３０からブーティング・イメージをダウンロードしてもよい。ブーティング・イメージはプログラム記憶装置２１６に保存されてもよい。いくつかの実施形態では、プログラム記憶装置２１６は、これに限られないが、フラッシュ・メモリを含む任意の書き込み可能な不揮発性メモリまたはこれに限られないがDRAM、SRAMその他のような任意の型のRAMを含むまたは任意の揮発性メモリであってもよい。ネットワーク・サーバー２１０は、プログラム記憶装置２１６からブーティング・イメージをロードし、実行してもよい。

【００２１】

信頼プロセッサ２２２はまた、ブーティング・サーバー２３０からのブーティング・イメージを測定してもよい。いくつかの実施形態では、信頼プロセッサ２２２は、ブーティング・イメージの確率論的に一意的な識別子である値を生成することによってブーティング・イメージを測定してもよい。該識別子は、これに限られないが、ハッシュ値、チェックサム、フィンガープリント、チェック・ディジットまたはランダム化関数といったものである。いくつかの実施形態では、信頼プロセッサ２２２は、ブーティング・イメージがプログラム記憶装置２１６に保存されるまたはプロセッサ２１２によって実行される前にブーティング・イメージを測定してもよい。いくつかの実施形態では、信頼プロセッサ２２２は、ブーティング・イメージがプロセッサ２１２によって実行されたあとにブーティング・イメージを測定してもよい。信頼プロセッサ２２２はブーティング・イメージの測定結果を、占有されていない第一、第二、第三または第四の記憶ユニット２２３、２２４、２２５、２２６の一つに保存する。

【００２２】

ブーティング・イメージがプロセッサ２２２によって実行される際、該ブーティング・イメージはネットワーク・サーバーに、ブーティング・サーバー２３０からソフトウェア・モジュールをダウンロードするよう指令してもよい。各ソフトウェア・モジュールは、ネットワーク・サーバー２１０によってプログラム記憶装置２１６内に記憶されてもよく、次いでプロセッサ２１２によってロードされ、実行されてもよい。ソフトウェア・モジ

ュールは、オペレーティング・システム、仮想マシン・マネージャまたは他のプログラムをネットワーク・サーバー２１０上で実行するためのソフトウェア・プログラムを含んでいてもよい。

【００２３】

信頼プロセッサ２２２はまた、ブーティング・サーバー２３０からのソフトウェア・モジュールを測定してもよい。いくつかの実施形態では、信頼プロセッサ２２２は、ソフトウェア・モジュールの確率論的に一意的な識別子である値を生成することによってソフトウェア・モジュールを測定してもよい。該識別子は、これに限られないが、ハッシュ値、チェックサム、フィンガープリント、チェック・ディジットまたはランダム化関数といったものである。いくつかの実施形態では、信頼プロセッサ２２２は、ソフトウェア・モジュールがプログラム記憶装置２１６に保存されるまたはプロセッサ２１２によって実行される前にソフトウェア・モジュールを測定してもよい。いくつかの実施形態では、信頼プロセッサ２２２は、ソフトウェア・モジュールがプロセッサ２１２によって実行されたあとにソフトウェア・モジュールを測定してもよい。信頼プロセッサ２２２は各ソフトウェア・モジュールの測定結果を、占有されていない第一、第二、第三または第四の記憶ユニット２２３、２２４、２２５、２２６の一つに保存する。

【００２４】

いくつかの実施形態では、信頼アンカー２２０は、ブーティング・サーバー２３０またはネットワーク２４０に接続されている他の任意のサーバーからダウンロードされたファームウェア、ソフトウェア、モジュール、コンポーネント、プログラム、イメージまたは他のオブジェクトの全部を、あるいは場合によってはその部分集合もしくは一部のみを測定するよう動作してもよい。代替的または追加的に、信頼アンカー２２０は、ネットワーク・サーバー２１０によって実行されるファームウェア、ソフトウェア、モジュール、コンポーネント、プログラム、イメージまたは他のオブジェクトの全部を、または場合によってはその部分集合もしくは一部のみを測定するよう動作してもよい。代替的または追加的に、信頼アンカー２２０は、ネットワーク・サーバー２１０上の任意の型のメモリに記憶されているファームウェア、ソフトウェア、モジュール、コンポーネント、プログラム、イメージまたは他のオブジェクトの全部を、または場合によってはその部分集合もしくは一部のみを測定するよう動作してもよい。

【００２５】

信頼アンカー２２０は各測定結果を、記憶ユニット２２３、２２４、２２５、２２６のような個々の記憶ユニットに記憶してもよい。信頼アンカー２２０は、たとえば信頼アンカー２２０によって取られてもよい測定値の数に依存して、四つより多くまたは四つより少ない記憶ユニットを含んでいてもよい。いくつかの実施形態では、記憶ユニット２２３、２２４、２２５、２２６は、信頼アンカー２２０内の個々のレジスタであってもよい。いくつかの実施形態では、記憶ユニット２２３、２２４、２２５、２２６は信頼アンカー２２０内のメモリ・デバイス内の、異なる、アドレス指定可能な位置であってもよい。

【００２６】

いくつかの実施形態では、信頼アンカー２２０は信頼されるプラットフォーム・モジュール（TPM: trusted platform module）セキュリティ・デバイスまたはチップであってもよい。いくつかの実施形態では、信頼アンカー２２０は、別の型の暗号プロセッサまたは暗号マイクロプロセッサであってもよい。いくつかの実施形態では、信頼アンカー２２０は、本稿に記載される機能を実行できる他の型の装置であってもよい。

【００２７】

いくつかの実施形態では、ネットワーク・サーバー２１０は、ブーティング・サーバー２３０を位置特定し、これと通信するための標準的なプロトコルを実装してもよい。たとえば、いくつかの実施形態では、ネットワーク・サーバー２１０は、ブート前実行環境プロトコルまたは他のネットワーク・ブーティング・プロトコルに従ってネットワーク２４０上でブートしてもよい。さらに、いくつかの実施形態では、ネットワーク・サーバー２１０、ブーティング・サーバー２３０およびネットワーク２４０は、ネットワーク・サー

バー２１０がネットワーク２４０上でブートできるようにするため、図示または議論されたもの以外の追加的なコンポーネントを含んでいてもよい。たとえば、ネットワーク２４０は動的ホスト構成設定プロトコル（DHCP: dynamic host configuration protocol）サーバーおよび一つもしくは複数のルータを含んでいてもよい；ブーティング・サーバー２３０は、ブーティング・イメージおよびソフトウェア・モジュールを記憶するファイル・サーバー、トリビアル・ファイル転送プロトコル（TFTP: trivial file transfer protocol）およびプロキシDHCPサーバーを含んでいてもよい；ネットワーク・サーバー２１０はネットワークを通じて通信するための一つまたは複数のハードウェア・コンポーネントを含んでいてもよい。

【００２８】

図３は、本稿に記載される少なくともいくつかの実施形態に基づいて構成された、ネットワーク・サーバーの信頼されるネットワーク・ブーティングを提供することを支援しうるサブシステム３００を示している。サブシステム３００は、図２に関して記載された、セキュリティで保護されたネットワーク・コントローラ３５０およびセキュリティで保護されたネットワーク３６０にネットワーク３４０を通じて通信可能に結合されているネットワーク・サーバー２１０を含んでいてもよい。

【００２９】

図２に関して述べたようにしてネットワーク・サーバー２１０がブートされ、セキュリティで保護されたネットワーク３６０にアクセスする準備ができ、信頼アンカー２２０がネットワーク・サーバー２１０上またはネットワーク・サーバー２１０内で走っているすべての該当するオブジェクトを測定し終わったのち、信頼アンカー２２０はレポートを生成してもよい。レポートを生成するために、信頼アンカー２２０は、以前に測定され、記憶ユニット２２３、２２４、２２５、２２６に記憶された測定値すべてを総合してもよい。レポートは、各測定値が何を表すかを同定するよう、各測定値についての識別子を含んでいてもよい。レポートをまとめたのち、信頼アンカー２２０はそのレポートに署名し、ネットワーク３４０を通じてセキュリティで保護されたネットワーク・コントローラ３５０に送ってもよい。いくつかの実施形態では、レポートに署名することは、信頼アンカー２２０が該信頼アンカー２２０に関連付けられた確率論的に一意的な識別子をレポート内に含めることを含んでいてもよい。

【００３０】

セキュリティで保護されたネットワーク・コントローラ３５０は信頼アンカー２２０からレポートを受け取る。レポートを受け取ったのち、セキュリティで保護されたネットワーク・コントローラ３５０内の検証モジュール３５２がレポートの測定値、署名、タイムスタンプおよび他の要素を検証してもよい。セキュリティで保護されたネットワーク・コントローラ３５０はまた、信頼アンカー２２０の署名と、信頼アンカー２２０によって測定された各オブジェクトについての信頼される測定値とを含むデータベース３５４を含んでいてもよい。

【００３１】

レポートを検証するため、検証モジュール３５２は、レポートの署名をデータベース３５４内の署名と比較することによって、レポート中の信頼アンカー２２０の署名を検証してもよい。それらの署名が同一であれば、検証モジュール３５２はレポートが信頼される、既知の信頼アンカー２２０によって生成されたことを確証しうる。

【００３２】

検証モジュール３５２は、レポートの測定値をデータベース３５４からの検証された測定値と比較することによって、レポート内の核測定値を検証し続けてもよい。測定値におけるいかなる相違も、ネットワーク・サーバー２１０上またはネットワーク・サーバー２１０内で走っているオブジェクトが改変または変更されていることを示しうる。いくつかの実施形態では、任意の測定値における変動が、ネットワーク・サーバー２１０が信頼されないことがありうることを示しうる。

【００３３】

いくつかの実施形態では、検証モジュール３５２はまた、レポートのタイムスタンプおよびレポートの他の諸側面を検証してもよい。たとえば、いくつかの実施形態では、レポートのタイムスタンプが、レポートが、該レポートを受信する前の所定の時間内に生成されたのでないことを示す場合、検証モジュール３５２はネットワーク・サーバー２１０が信頼されないことがありうると判定してもよい。たとえば、レポートが、該レポートを受信する前の所定の時間内に生成されたのでない場合、ネットワーク・サーバー２１０はルビーとする時間を有していたことがありうる。これは、レポートがネットワーク・サーバー２１０の状態を正確に反映しないことがありうることを意味する。

【００３４】

検証モジュール３５２がレポートを検証する場合、検証モジュール３５２はネットワーク・サーバー２１０が信頼されると示してもよい。すると、セキュリティで保護されたネットワーク・コントローラ３５０は信頼されるネットワーク・サーバー２１０がセキュリティで保護されたネットワーク３６０に参加することを許容してもよい。検証モジュール３５２がレポートを検証できない場合、ネットワーク・サーバー２１０は信頼されると考えられないことがありうる。セキュリティで保護されたネットワーク・コントローラ３５０は信頼されないネットワーク・サーバー２１０に、信頼されるネットワーク３６０へのアクセスを拒否してもよい。いくつかの実施形態では、セキュリティで保護されたネットワーク・コントローラ３５０は、ネットワーク・サーバー２１０が信頼されなかったことを示すメッセージをネットワーク管理者に送ってもよい。いくつかの実施形態では、セキュリティで保護されたネットワーク・コントローラ３５０は、ネットワーク・サーバー２１０において信頼を発達させるステップを講じてもよい。これは、ネットワーク・サーバー２１０をリブートすることまたは図２に示されるブーティング・サーバー２３０のようなブーティング・サーバーをリブートすることを含んでいてもよい。

【００３５】

いくつかの実施形態では、ネットワーク３４０は図２に示したネットワーク２４０と同じであってもよい。いくつかの実施形態では、セキュリティで保護されたネットワーク３６０は、一つまたは複数のサーバーを使って実装されるセキュリティで保護されたネットワーク環境であってもよい。たとえば、セキュリティで保護されたネットワーク３６０はクラウド環境、クラスター・コンピューティング・ネットワーク、分散処理ネットワークまたは他の任意の型のセキュリティで保護されたネットワークであってもよい。いくつかの実施形態では、セキュリティで保護されたネットワーク・コントローラ３５０は、ネットワーク３４０およびセキュリティで保護されたネットワーク３６０とネットワーク接続された、サーバーまたは他の何らかのプロセッサもしくはコンピューティング装置であってもよい。いくつかの実施形態では、データベース３５４はセキュリティで保護されたネットワーク・コントローラ３５０の外に位置され、セキュリティで保護されたネットワーク・コントローラ３５０とネットワーク接続されているのでもよい。

【００３６】

図３に示したサブシステム３００を使えば、セキュリティで保護されたネットワーク・コントローラ３５０は、ひとたび信頼アンカー２２０の署名が検証されたら、ネットワーク・サーバー２１０内の信頼アンカー２２０を信頼するだけでよい。セキュリティで保護されたネットワーク・コントローラ３５０は、ブーティング・サーバー、ネットワーク３４０、ネットワーク・サーバー２１０または他の何らかのコンポーネントもしくはオブジェクトを信頼する必要はないことがある。サブシステム３００はまた、他のネットワーク接続されたブーティング・システムとは対照的に、複数のレイヤーの信頼が確立されることを要求しないことがある。むしろ、サブシステム３００は、信頼アンカー２２０との単一レイヤーの信頼に依拠できる。

【００３７】

システム３００は、いくつかの実施形態では、信頼アンカー２２０を危殆化して、信頼アンカー２２０にレポートを偽造させることによって、あるいはネットワーク・コントローラ３５０を危殆化して既知の測定データを変更することによってのみ危殆化されうる。

よって、意図的なものであれ意図的でないものであれ、ネットワーク・サーバー２１０の状態に影響しうるネットワーク・サーバー２１０、ブーティング・サーバーおよびネットワーク３４０内のいかなる攻撃、改変または変更も、ネットワーク・サーバー２１０がセキュリティで保護されたネットワーク３６０に参加することが許される前に、発見されうる。こうして、セキュリティで保護されたネットワーク３６０の安全性が維持されうる。さらに、サブシステム３００は、ネットワーク・サーバー２１０のネットワーク・ブーティングを許容しつつ、この安全性を提供しうる。サーバーのネットワーク・ブーティングは、図４に示されるシステムにおいてスケーラビリティを提供しうる。

【００３８】

図４は、本稿に記載される少なくともいくつかの実施形態に基づいて構成された、複数のネットワーク・サーバーの信頼されるネットワーク・ブーティングを提供するシステム４００を示している。システム４００は第一、第二および第三のネットワーク・サーバー４１０、４１２、４１４と；ブーティング・サーバー４３０と；セキュリティで保護されたネットワーク・コントローラ４５０と；セキュリティで保護されたネットワーク４６０とを通信可能に結合するネットワーク４４０を含んでいてもよい。第一、第二および第三のネットワーク・サーバー４１０、４１２、４１４はそれぞれ第一、第二および第三の信頼アンカーを含んでいてもよい。第一、第二および第三の信頼アンカー４２０、４２２、４２４のそれぞれは、セキュリティで保護されたネットワーク・コントローラ４５０によって知られていてもよい個々の、一意的な署名を有していてもよい。ネットワーク・サーバー４１０、４１２、４１４のそれぞれによって実行される第一のプログラムならびにブーティング・サーバー４３０内のブーティング・イメージおよびソフトウェア・モジュールのそれぞれの検証された測定値もセキュリティで保護されたネットワーク・コントローラ４５０によって知られていてもよい。

【００３９】

図示した実施形態によれば、システム４００は、第一、第二および第三のネットワーク・サーバー４１０、４１２、４１４をブートし、それぞれにセキュリティで保護されたネットワーク４６０にアクセスすることを許容するよう動作しうる。システム４００は、ブーティング・サーバー４３０を使って、第一、第二および第三のネットワーク・サーバー４１０、４１２、４１４それぞれの、ネットワーク４４０を通じたネットワーク・ブートを実行してもよい。第一、第二および第三のネットワーク・サーバー４１０、４１２、４１４がブートし、ブーティング・サーバー４３０からソフトウェア・モジュールをロードする際、対応する信頼アンカー４２０、４２２、４２４が初期プログラム、ブーティング・イメージおよびソフトウェア・モジュールを測定していてもよい。

【００４０】

第一、第二および第三のネットワーク・サーバー４１０、４１２、４１４のそれぞれがブートしたのち、各信頼アンカー４２０、４２２、４２４は初期プログラム、ブーティング・イメージおよびソフトウェア・モジュールのそれぞれの測定値を、署名されたレポートにおいて、セキュリティで保護されたネットワーク・コントローラ４５０に送ってもよい。セキュリティで保護されたネットワーク・コントローラ４５０は、各信頼アンカー４２０、４２２、４２４が信頼されうることを検証するために、信頼アンカー４２０、４２２、４２４の署名を検査してもよい。セキュリティで保護されたネットワーク・コントローラ４５０は次いで、各信頼アンカー４２０、４２２、４２４からの初期プログラム、ブーティング・イメージおよびソフトウェア・モジュールの測定値を検証して、ネットワーク・サーバー４１０、４１２、４１４のそれぞれが信頼されうるか否かを判定してもよい。セキュリティで保護されたネットワーク・コントローラ４５０がネットワーク・サーバー４１０、４１２、４１４のそれぞれが信頼されることを検証したのち、ネットワーク・サーバー４１０、４１２、４１４は、セキュリティで保護されたネットワーク４６０に参加することが許されてもよい。

【００４１】

いくつかの実施形態では、ネットワーク・サーバー４１０、４１２、４１４は同時にブ

ートし、ソフトウェア・モジュールをロードしてもよい。いくつかの実施形態では、ネットワーク・サーバー４１０、４１２、４１４は一つずつブートし、ソフトウェアをロードしてもよいし、あるいはネットワーク・サーバー４１０、４１２、４１４の何らかの組み合わせが同時にブートし、ソフトウェアをロードしてもよい。いくつかの実施形態では、信頼アンカー４２０、４２２、４２４は、各ネットワーク・サーバー４１０、４１２、４１４がブートし、ソフトウェアをロードしたのちに、同時にそれぞれのレポートを送ってもよい。いくつかの実施形態では、信頼アンカー４２０、４２２、４２４は、個々のネットワーク・サーバー４１０、４１２、４１４がブートし、ソフトウェア・モジュールをロードするのを完了したのちに、他のネットワーク・サーバー４１０、４１２、４１４の状態に関わりなく、セキュリティで保護されたネットワーク・コントローラ４５０にそれぞれのレポートを送ってもよい。いくつかの実施形態では、セキュリティで保護されたネットワーク・コントローラ４５０は、ネットワーク・サーバー４１０、４１２、４１４のそれぞれに、同時にまたは個々にセキュリティで保護されたネットワーク４６０へのアクセスを認めてもよい。

【００４２】

図５は、本稿に記載される少なくともいくつかの実施形態に基づいて構成された、図１に示されるネットワーク・サーバー１１０のようなサーバーの信頼されるネットワーク・ブーティングを提供する方法５００を示している。開始するために、ブロック５２５において、図１に示した信頼アンカー１２０のようなサーバー内の信頼アンカーが、ブーティング・サーバーから当該サーバーにダウンロードされたブーティング・イメージを測定してもよい。いくつかの実施形態では、信頼アンカーは、ブーティング・イメージがサーバー上のメモリに記憶される前にブーティング・イメージを測定してもよい。他の実施形態では、信頼アンカーは、ブーティング・イメージがサーバー上のメモリに記憶されたあとでブーティング・イメージを測定してもよい。いくつかの実施形態では、信頼アンカーは、プログラムの測定を、そのプログラムの確率論的に一意的な識別子である値を生成することによって行ってもよい。該識別子は、これに限られないが、ハッシュ値、チェックサム、フィンガープリント、チェック・ディジットまたはランダム化関数といったものである。信頼アンカーは、プログラムの測定結果を、信頼アンカー内のメモリに記憶してもよい。いくつかの実施形態では、信頼アンカーは測定値をレジスタに記憶してもよい。いくつかの実施形態では、信頼アンカーは信頼されるプラットフォーム・モジュール・チップであってもよく、測定値を、測定値の安全な記憶および報告のための備えを提供するプラットフォーム構成設定レジスタに記憶してもよい。

【００４３】

ブーティング・イメージは次いで、サーバーによってロードされ、実行されてもよい。ブーティング・イメージの指令に従って、ブロック５３０において、サーバーは、ブーティング・サーバーから一つまたは複数のモジュールをダウンロードする一つまたは複数の動作を実行してもよい。これらのモジュールは、ソフトウェア、ファームウェア、イメージ、プログラムまたは他のオブジェクトであってもよい。いくつかの実施形態では、これらのモジュールは、仮想プラットフォーム・マシンのためのソフトウェアまたは他の型のオペレーティング・システムであってもよい。ブロック５３５において、信頼アンカーはブーティング・サーバーからダウンロードされた前記一つまたは複数のモジュールを測定してもよい。信頼アンカーは、ダウンロードされたモジュールの測定値を信頼アンカー内のメモリに記憶してもよい。いくつかの実施形態では、信頼アンカーは、ダウンロードされたモジュールがサーバー上に保存される前に、該ダウンロードされたモジュールを測定してもよい。いくつかの実施形態では、信頼アンカーは、ダウンロードされたモジュールがサーバー上に保存されたあとに、該ダウンロードされたモジュールを測定してもよい。

【００４４】

ダウンロードされたモジュールがロードされ、システム上で実行するのち、ブロック５４０において、信頼アンカーは、信頼アンカーが取った測定値の一部または全部を含むレポートを生成してもよい。たとえば、いくつかの実施形態では、信頼アンカーは、ブーテ

ィング・イメージおよびダウンロードされたモジュールの測定値を含んでいてもよい。レポートを生成したのち、ブロック５４５において、信頼アンカーはレポートに署名してもよい。信頼アンカーは、信頼アンカーに対して確率的に一意的である署名または鍵をもってレポートに署名してもよい。いくつかの実施形態では、信頼アンカーの署名または鍵は、RSA鍵のような値であってもよい。

【００４５】

ブロック５５０において、信頼アンカーは署名されたレポートを、図１に示したネットワーク・コントローラ１６０のようなネットワーク・コントローラに送ってもよい。ブロック５５５では、ネットワーク・コントローラはレポート上の署名を検証してもよい。いくつかの実施形態では、ネットワーク・コントローラはレポート上の署名を、該署名を、該レポートを生成した信頼アンカーの既知の署名と比較することによって、検証してもよい。レポートの署名が検証されたら、つまりレポートの署名が、そのレポートを生成して送った信頼アンカーの既知の署名に一致したら、方法５００はブロック５６０に進んでもよい。いくつかの実施形態では、ネットワーク・コントローラは、方法５００がブロック５６０に進む前に、タイムスタンプのようなレポートの他の諸側面をも検証してもよい。レポートの署名が検証されない場合には、方法５００はブロック５８０に進んでもよい。

【００４６】

ブロック５６０では、ネットワーク・コントローラはレポート中の測定値を検証してもよい。いくつかの実施形態では、ネットワーク・コントローラはレポート内の測定値を、該測定値を既知の測定値と比較することによって検証してもよい。たとえば、レポート内のブーティング・イメージの測定値は既知の検証されたブーティング・イメージ測定値と比較されてもよい。それらの測定値が等しいと見なされる場合、ブーティング・イメージは検証されうる。つまり、ブーティング・イメージは変更、改変または調整されていない。レポート内のすべての測定値が検証されたら、方法５００はブロック５７０に進んでもよい。測定値のいずれかが検証されない場合には、方法５００はブロック５８０に進んでもよい。

【００４７】

ブロック５７０では、サーバーは、セキュリティで保護されたネットワーク・コントローラによって、信頼されると見なされてもよく、セキュリティで保護されたネットワークへのアクセスを認められてもよい。対照的に、ブロック５８０では、サーバーは信頼されないと見なされ、セキュリティで保護されたネットワークへのアクセスを拒否されてもよい。

【００４８】

サーバーが信頼されると見なされないのはさまざまな理由でありうる。追加的または代替的に、サーバーにダウンロードされたブーティング・イメージまたはソフトウェア・モジュールが改変または変更されて、信頼アンカーによって取られた測定値がネットワーク・コントローラによって記憶されている測定値と等しくないことがありうる。このような状況を正すため、サーバーは、リブートされて、問題が単に測定の誤りであったかどうかを判定するために改めて測定値が取られてもよい。追加的または代替的に、システム管理者が通知を受け、サーバーおよび／またはブーティング・サーバーにサービスしてもよい。

【００４９】

もう一つの例として、サーバーは、レポート上の署名がそのレポートを送らなかった信頼アンカーに対応する場合に、信頼されないと見なされてもよい。追加的または代替的に、サーバーは、署名が正しくない場合に信頼されないと見なされてもよい。これらの状況を正すために、サーバーがリブートされ、レポートを生成し直してもよいし、あるいはシステム管理者がサーバーを検査してもよい。もう一つの例として、サーバーは、レポートのタイムスタンプが古くなっている場合に信頼されないと見なされてもよい。追加的または代替的に、サーバーは、レポートがネットワーク・コントローラに通信されないまたはレポートがネットワーク・コントローラに送信される際に壊される場合に信頼されないと

見なされてもよい。これらの状況を正すため、サーバーはリブートされてレポートを生成し直してもよいし、あるいはシステム管理者が通知を受けてサーバーとネットワーク・コントローラとの間のネットワークを検査してもよい。

【００５０】

当業者は、この、および本稿で開示される他のプロセスおよび方法について、それらのプロセスおよび方法において実行される機能が異なる順序で実装されてもよいことを理解するであろう。さらに、概説されたステップや動作は単に例として与えられているのであり、開示される実施形態の本質を損なうことなく、ステップや動作の一部は任意的であってもよく、より少数のステップや動作に組み合わされてもよく、あるいは追加的なステップや動作に拡張されてもよい。

【００５１】

たとえば、いくつかの実施形態では、ブロック５２５においてブーティング・イメージを測定する前に、サーバーが電源投入されてもよい。サーバーが電源投入される際、サーバー内の信頼アンカーが、電源投入時にサーバーによって最初に実行されるプログラムを測定してもよい。プログラムは次いで、ブーティング・プロセスを開始するためにサーバーによってロードされ、実行されてもよい。いくつかの実施形態では、プログラムは、ブート前実行環境プロトコルのような、ネットワーキング・ブーティング・プロトコルに従う動作を含んでいてもよい。いくつかの実施形態では、該プログラムに続いて、サーバーは、図１に示したブーティング・サーバー１３０のような、ブーティング・イメージのダウンロード元となるブーティング・サーバーを位置特定するための一つまたは複数の動作を実行してもよい。いくつかの実施形態では、ブーティング・サーバーの位置特定は、DHCPサーバーを位置特定し、IPアドレスを取得することを含んでいてもよい。

【００５２】

ある実施形態に基づく図５の方法５００の例は次のようになる。データ・クラウドが追加的な容量を扱うために追加的なサーバーを必要とすることがある。データ・クラウドに通信可能にリンクされている、信頼されるプラットフォーム・モジュール（TPM）チップのような信頼アンカーが電源投入されてもよい。サーバーのBIOSがTPMチップによって測定されてもよく、TPMチップ内のレジスタに記憶されてもよい。BIOSは、ブート前実行環境（PXE: pre-boot execution environment）プロトコルのような、ネットワーク・ブーティングのためのネットワーク・ブーティング・プロトコルを含んでいてもよい。サーバーは該プロトコルに従い、PXEサーバーと接続を確立してもよい。

【００５３】

ブーティング・イメージはPXEサーバーから当該サーバーにダウンロードされてもよい。ブーティング・イメージがダウンロードされる際にTMPチップがブーティング・イメージを測定して、測定値をそのレジスタの一つに記憶してもよい。ブーティング・イメージはロードされ、実行されてもよく、サーバーに、オペレーティング・システムのソフトウェア・モジュールをPXEサーバーからダウンロードするよう指令してもよい。ソフトウェア・モジュールがダウンロードされる際、TPMチップは各ソフトウェア・モジュールを測定し、測定値をそのレジスタ内に記憶してもよい。ソフトウェア・モジュールがロードされ、サーバー上で実行されたのち、TPMチップは、そのレジスタに記憶されている測定値を含むレポートを生成し、該レポートに署名し、該レポートをデータ・クラウドへのアクセスを管理するネットワーク・コントローラに送ってもよい。

【００５４】

ネットワーク・コントローラは、PXEサーバーからのブーティング・イメージおよびソフトウェア・イメージならびに当該サーバーのBIOSの既知の測定値と、TPMチップの署名とを含んでいてもよい。この情報を使って、ネットワーク・コントローラはレポート内のBIOS、ブーティング・イメージおよびソフトウェア・イメージの署名および測定値を、それらをBIOS、ブーティング・イメージおよびソフトウェア・イメージの既知の署名および測定値と比較することによって、検証してもよい。測定値のすべてが検証されたら、ネットワーク・コントローラはそのサーバーが信頼されてもよいことを知り、そのサーバーに

データ・クラウドへのアクセスを認める。測定値の一つまたはレポートの他の側面が検証されない場合には、ネットワーク・コントローラはそのサーバーに、データ・クラウドへのアクセスを拒否してもよい。

【００５５】

本稿に記載される実施形態は、以下に論じるように、さまざまなコンピュータ・ハードウェアまたはソフトウェア・モジュールを含む特殊目的または汎用目的のコンピュータの使用を含んでいてもよい。

【００５６】

本稿に記載される実施形態は、コンピュータ実行可能な命令を担持するもしくは有するコンピュータ可読媒体またはその上に記憶されるデータ構造を使って実装されてもよい。そのようなコンピュータ可読媒体は、汎用目的または特殊目的のコンピュータによってアクセス可能ないかなる利用可能な媒体であってもよい。限定ではなく例として、そのようなコンピュータ可読媒体は、RAM、ROM、EEPROM、CD-ROMまたは他の光学式ディスク記憶、磁気ディスク記憶または他の磁気記憶装置、あるいはコンピュータ実行可能な命令の形の所望されるプログラム・コード手段またはデータ構造を担持もしくは記憶するために使用でき、汎用目的または特殊目的のコンピュータによってアクセスされうる他の任意の媒体を含むことができる。情報がネットワークまたは他の通信接続（有線、無線、または有線と無線の組み合わせ）を通じてコンピュータに転送または提供されるとき、コンピュータは適正にその接続をコンピュータ可読媒体と見なす。よって、そのようないかなる接続も適正にコンピュータ可読媒体と称される。上記のさまざまな組み合わせも、コンピュータ可読媒体の範囲内に含められるべきである。

【００５７】

コンピュータ実行可能な命令はたとえば、汎用目的コンピュータ、特殊目的コンピュータまたは特殊目的処理装置にある種の機能または一群の機能を実行させる命令およびデータを含む。本願の主題は、構造的な特徴および／または方法論上の工程に固有の言辞で記述されているが、付属の請求項において定義される主題は必ずしも上記の個別的な特徴や工程に限定されないことは理解しておくべきである。むしろ、上記の個別的な特徴や工程は請求項を実装する例示的な形として開示されているのである。

【００５８】

本稿での用法では、用語「モジュール」および「コンポーネント」は、コンピューティング・システム上で実行されるソフトウェア・オブジェクトまたはルーチンを指しうる。本稿に記載される種々のコンポーネント、モジュール、エンジンおよびサービスは、コンピューティング・システム上で実行されるオブジェクトまたはプロセスとして（たとえば別個のスレッドとして）実装されてもよい。本稿に記載されるシステムおよび方法は好ましくはソフトウェアで実装されるが、ハードウェアまたはソフトウェアとハードウェアの組み合わせでの実装も可能であり、考えられている。本稿において、「コンピューティング・エンティティ」は、本稿で先に定義したような任意のコンピューティング・システムまたはコンピューティング・システム上で実行される任意のモジュールもしくはモジュールの組み合わせでありうる。

【００５９】

本稿に記載されるあらゆる例および条件付きの言辞は、本発明および当該技術を進歩させるために発明者によって寄与される概念を理解する上で読者を助ける教育的な目的を意図されているのであって、そのような特定的に記載された例や条件に限定することなく解釈されるものとする。また、明細書におけるそのような例の編成は本発明の優位または劣位を示すことには関係しない。本発明の実施形態について詳細に記載してきたが、本発明の精神および範囲から外れることなく、それにさまざまな変更、置換および改変がなしうることは理解しておくべきである。

以上の実施例を含む実施形態に関し、さらに以下の付記を開示する。

（付記１）

サーバーの信頼されるネットワーク・ブーティングのためのシステムであって：

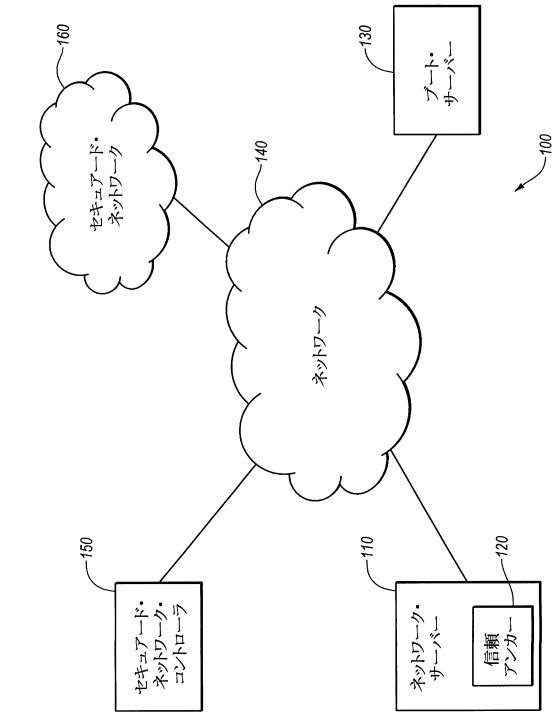
ブーティング・イメージを含むブーティング・サーバーと；
前記ブーティング・サーバーの前記ブーティング・イメージを用いてブートするネットワーク・サーバーであって、前記ブーティング・イメージの測定値を得る信頼アンカーを含むネットワーク・サーバーと；
ネットワークへのアクセスを制御するネットワーク・コントローラであって、前記ネットワーク・サーバーが前記ネットワークにアクセスすることを許可する前に前記ブーティング・イメージの前記測定値を検証する、ネットワーク・コントローラとを有する、
システム。
（付記２）
前記信頼アンカーが前記ネットワーク・サーバー内の信頼プロセッサである、付記１記載のシステム。
（付記３）
前記信頼アンカーが前記ネットワーク・サーバー内の信頼されるプラットフォーム・モジュール（TPM）チップである、付記２記載のシステム。
（付記４）
前記ブーティング・サーバーが、ブート前実行環境プロトコルに従って前記ネットワーク・サーバーと通信する、付記１記載のシステム。
（付記５）
前記信頼アンカーが、前記ブーティング・イメージのハッシュ値を生成することによって前記ブーティング・イメージの前記測定値を得る、付記１記載のシステム。
（付記６）
前記ネットワーク・コントローラが前記ブーティング・イメージの前記測定値を検証することを、前記信頼アンカーによって得られた前記ブーティング・イメージの前記測定値を、前記ブーティング・イメージの検証済みの測定値と比較することによって検証する、付記１記載のシステム。
（付記７）
前記ネットワーク・コントローラは、前記ネットワーク・サーバーが前記ネットワークにアクセスすることを許可する前に前記信頼アンカーの署名を検証する、付記１記載のシステム。
（付記８）
前記信頼アンカーは、スタートアップ時に前記ネットワーク・サーバーによって最初に実行されるプログラムの測定値を得て、そのプログラムの測定値を前記ネットワーク・コントローラに送る、付記１記載のシステム。
（付記９）
サーバーの信頼されるネットワーク・ブーティングのための方法であって：
ネットワーク・サーバーにダウンロードされたブーティング・イメージの測定値を、前記ネットワーク・サーバー内の信頼アンカーを使って取得して；
前記ブーティング・イメージを使って前記ネットワーク・サーバーをブートして；
前記ブーティング・イメージの前記測定値を検証のために送ることを含む、
方法。
（付記１０）
前記ブーティング・イメージの前記測定値を取得する処理が、前記ブーティング・イメージについてのハッシュ値を生成することを含む、付記９記載の方法。
（付記１１）
前記ブーティング・イメージの前記測定値の検証が、前記信頼アンカーによって得られた前記ブーティング・イメージの前記測定値を、前記ブーティング・イメージの検証済みの測定値と比較することによって実行される、付記１０記載の方法。
（付記１２）
さらに前記信頼アンカーの署名を検証することを含む、付記９記載の方法。
（付記１３）

前記ネットワーク・サーバーにダウンロードされた各ソフトウェア・モジュールを測定することをさらに含む、付記９記載の方法。
（付記１４）
前記ブーティング・イメージの前記測定値が検証された場合に前記ネットワーク・サーバーをネットワークに参加させることをさらに含む、付記９記載の方法。
（付記１５）
ネットワーク・サーバー内の信頼アンカーとして動作するプロセッサであって：
前記ネットワーク・サーバーによってブートするために使用される、第一のネットワークを通じて受信されたブーティング・イメージの測定値を取得する工程と；
前記ブーティング・イメージの前記測定値を、第二のネットワークへのアクセスを得るための検証のために送る工程とを実行するよう適応された、
プロセッサ。
（付記１６）
検証のために署名を送る工程を実行するようさらに適応されている、付記１５記載のプロセッサ。
（付記１７）
スタートアップ時に前記ネットワーク・サーバーによって最初に実行されるプログラムを測定する工程をさらに実行するよう適応されている、付記１５記載のプロセッサ。
（付記１８）
前記ブーティング・イメージの前記測定値を取得する工程が、前記ブーティング・イメージについてのハッシュ値を生成することを含む、付記１５記載のプロセッサ。
（付記１９）
前記ネットワーク・サーバーの信頼されるネットワーク・ブーティングのためのシステムであって：
当該システム内で前記ネットワーク・サーバーの前記信頼アンカーとして動作する付記１５記載のプロセッサと；
前記ネットワーク・サーバーによってブートするときに使用される前記ブーティング・イメージを含むブーティング・サーバーとを有する、
システム。
（付記２０）
前記ブーティング・イメージの前記測定値を検証し、前記第二のネットワークへのアクセスを制御するネットワーク・コントローラをさらに有する、付記１９記載のシステム。
【符号の説明】
【００６０】
１００　システム
１１０　ネットワーク・サーバー
１２０　信頼アンカー
１３０　ブート・サーバー
１４０　ネットワーク
１５０　セキュアード・ネットワーク・コントローラ
１６０　セキュアード・ネットワーク
２００　サブシステム
２１０　ネットワーク・サーバー
２１２　プロセッサ
２１４　スタートアップ記憶
２１６　プログラム記憶
２２０　信頼アンカー
２２２　信頼プロセッサ
２３０　ブート・サーバー
２４０　ネットワーク

３００　サブシステム
３４０　ネットワーク
３５０　セキュアード・ネットワーク・コントローラ
３５２　検証モジュール
３５４　データベース
３６０　セキュアード・ネットワーク
４００　システム
４１０，４１２，４１４　ネットワーク・サーバー
４２０，４２２，４２４　信頼アンカー
４３０　ブート・サーバー
４４０　ネットワーク
４５０　セキュアード・ネットワーク・コントローラ
４６０　セキュアード・ネットワーク
５００　方法
５２５　ブート・イメージを計測
５３０　ソフトウェア・モジュールをダウンロード
５３５　ソフトウェア・モジュールを計測
５４０　計測値を用いてレポートを生成
５４５　レポートに署名
５５０　レポートをネットワーク・コントローラに送信
５５５　レポート中の署名を検証
５６０　レポート中の計測値を検証
５７０　セキュアード・ネットワークへのサーバー・アクセスを承認
５８０　セキュアード・ネットワークへのサーバー・アクセスを拒否

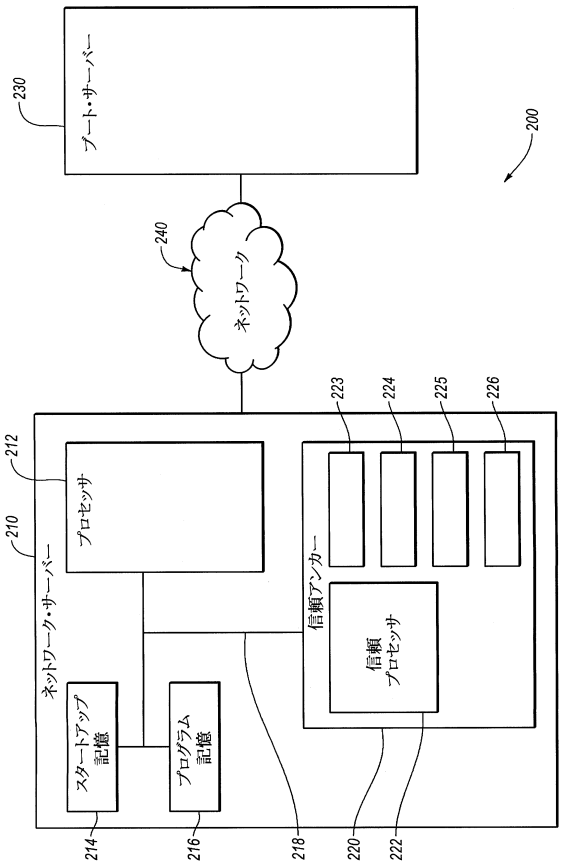
【図１】

ネットワーク・サーバーの信頼されるネットワーク・ブーティングを提供するシステムを示す図



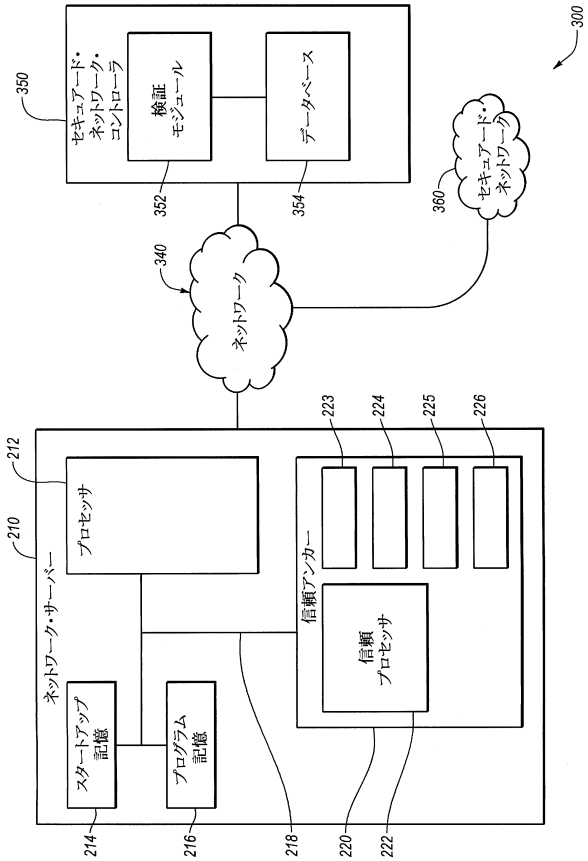
【図２】

ネットワーク・サーバーの信頼されるネットワーク・ブーティングを提供するシステムの一部を示す図



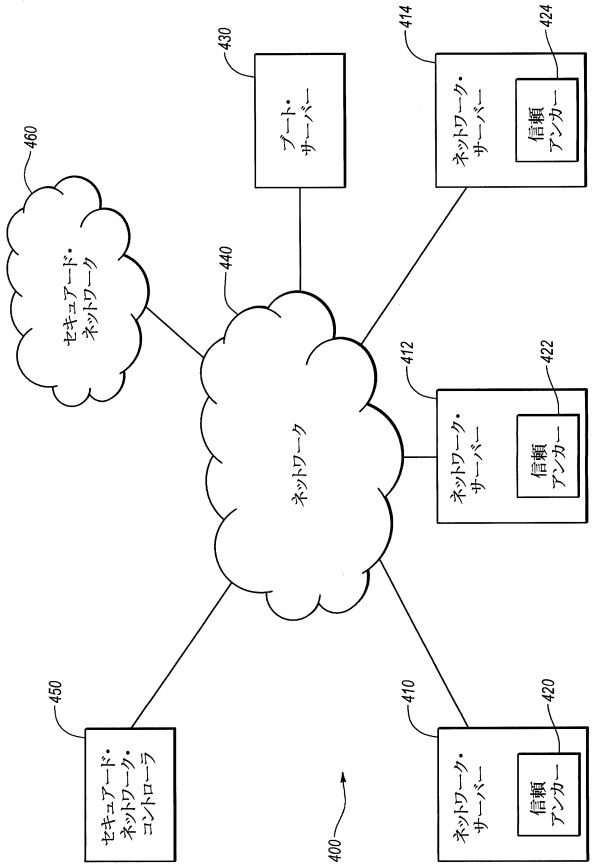
【図３】

ネットワーク・サーバーの信頼されるネットワーク・ブーティングを提供するシステムの一部を示す図



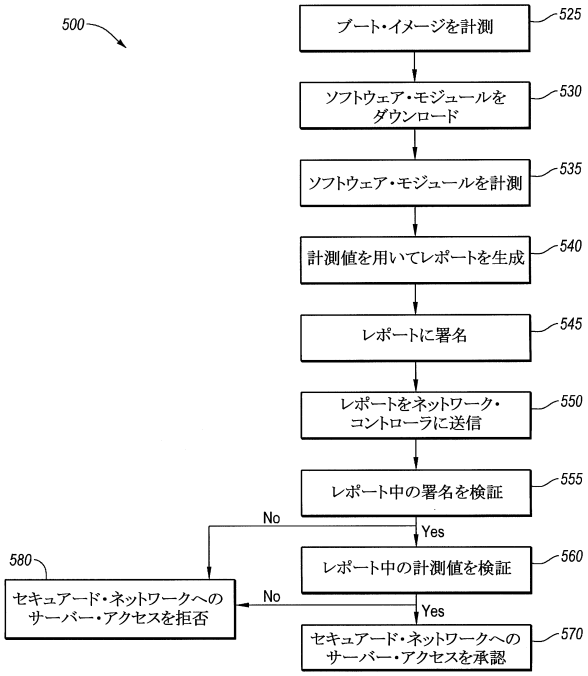
【図４】

複数のネットワーク・サーバーの信頼されるネットワーク・ブーティングを提供するシステムを示す図



【図５】

みな本稿に記載される少なくともいくつかの実施形態に基づいて構成される、サーバーの信頼されるネットワーク・ブーティングのための方法の例示的なフローチャート



フロントページの続き

(72)発明者 ゴードン・ジョゼフ
アメリカ合衆国，カリフォルニア州 ９４７０４，バークレー，カールトン・ストリート ２０１９番

合議体
審判長 高木 進
審判官 辻本 泰隆
審判官 須田 勝巳

(56)参考文献 特開２００６－１７２３７６（ＪＰ，Ａ）
国際公開第２００９／１０７３４９（WO，Ａ1）
特開２００７－９４８７９（ＪＰ，Ａ）
大原 久樹，システム全体のセキュリティ強化を支援する仮想化応用技術，ＣＯＭＰＵＴＥＲ ＷＯＲＬＤ Ｇｅｔ Ｔｅｃｈｎｏｌｏｇｙ Ｒｉｇｈｔ，株式会社ＩＤＧジャパン，２００８年1月1日，第5巻，第1号，６０～６３頁
早川 薫，プラットフォーム部分認証，電子情報通信学会技術研究報告，社団法人電子情報通信学会，２０１１年7月２１日，Ｖｏｌ．１１１，Ｎｏ．１６３，１９～２４頁

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F21/00-21/88
G06F9/445