(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-18786
(P2005-18786A)
(43)公開日　平成17年1月20日(2005.1.20)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 9/445	G06F 9/06	610J	5B076
G06F 13/00	G06F 13/00	530A	
	G06F 9/06	640A	

審査請求 未請求　請求項の数 20　ＯＬ　（全 16 頁）

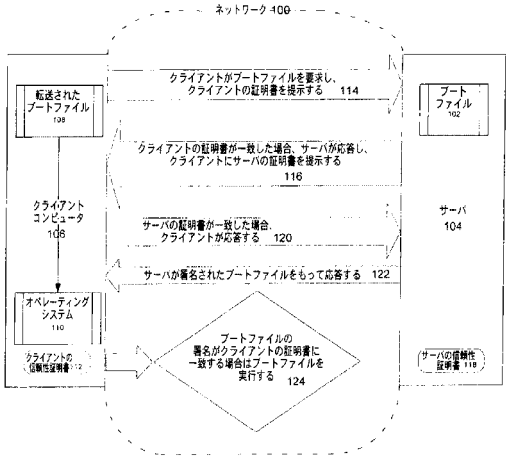
(21)出願番号　特願2004-188927(P2004-188927)
(22)出願日　平成16年6月25日(2004.6.25)
(31)優先権主張番号　10/609,152
(32)優先日　平成15年6月27日(2003.6.27)
(33)優先権主張国　米国(US)

(71)出願人　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　ウェスリー　ジー．ミラー
アメリカ合衆国　９８０５２　ワシントン州　サマミッシュ　ノースイースト　２１　プレイス　２３２１７

Ｆターム(参考)　5B076 AA13　BB06

(54)【発明の名称】サーバからクライアントに送信されたブートファイルの３方向の検証および認証

(57)【要約】
【課題】　サーバからプレインストール環境を有するクライアントにブートファイルを転送する方法およびシステムを提供すること。
【解決手段】　サーバはクライアントを認証する。クライアントはサーバを認証する。認証されたサーバから認証されたクライアントにブートファイルが転送される。このブートファイルをクライアントによって認証した後に実行して、オペレーティングシステムを作成することができる。
【選択図】　図１



【特許請求の範囲】
【請求項１】
サーバからクライアントにブートファイルを転送する方法であって、
前記サーバが前記クライアントを認証するステップと、
前記クライアントが前記サーバを認証するステップと、
前記認証されたサーバから前記認証されたクライアントに前記ブートファイルを転送するステップと
を備えることを特徴とする方法。
【請求項２】
前記認証されたクライアントが、前記転送されたブートファイルを認証するステップをさらに備えることを特徴とする請求項１に記載の方法。
【請求項３】
前記認証されたクライアントが、前記認証されたブートファイルを実行するステップをさらに備えることを特徴とする請求項２に記載の方法。
【請求項４】
無効または失効した証明書を有するクライアントは、前記サーバによって認証または応答されないことを特徴とする請求項１に記載の方法。
【請求項５】
無効または失効した証明書を有するサーバは、前記クライアントによって受信確認が返されないことを特徴とする請求項１に記載の方法。
【請求項６】
署名が正しくない、前記クライアントによって受信されたブートファイルは、前記クライアントによって実行されないことを特徴とする請求項１に記載の方法。
【請求項７】
前記転送されたブートファイルは署名を含み、前記クライアントは前記署名を確認することを特徴とする請求項１に記載の方法。
【請求項８】
サーバからｐｒｅ－ＯＳ環境を有するクライアントにネットワークを介してブートファイルを転送する方法であって、
クライアントの信頼性の証明書を前記クライアントにインストールするステップと、
前記クライアントが、前記サーバが前記クライアントに前記ブートファイルを転送するように前記ネットワークを介して要求するステップと、
前記クライアントが、前記インストールされたクライアントの信頼性証明書を、前記ネットワークを介して送信するステップと、
前記サーバが、前記受信されたクライアントの信頼性証明書により前記クライアントを認証するステップと、
前記サーバから前記認証されたクライアントに前記ブートファイルを転送するステップと
を備えることを特徴とする方法。
【請求項９】
前記認証されたクライアントが前記転送されたブートファイルを認証するステップと、
前記認証されたクライアントが前記認証されたブートファイルを実行するステップと
をさらに含むことを特徴とする請求項８に記載の方法。
【請求項１０】
ネットワークを介してサーバからｐｒｅ－ＯＳ環境を有するクライアントにブートファイルを転送する方法であって、
クライアントの信頼性の証明書を前記クライアントにインストールするステップと、
前記クライアントが前記ネットワークを介して、前記サーバから前記クライアントに前記ブートファイルを転送するように要求するステップと、
前記クライアントが、前記インストールされたクライアントの信頼性の証明書を、前記

ネットワークを介して送信するステップと、
前記クライアントが前記サーバから前記ブートファイルを受信するステップと
を備えることを特徴とする方法。
【請求項１１】
前記認証されたクライアントが、前記転送されたブートファイルを認証するステップと、
前記認証されたクライアントが、前記認証されたブートファイルを実行するステップと
をさらに備えることを特徴とする請求項１０に記載の方法。
【請求項１２】
サーバからｐｒｅ－ＯＳ環境を有するクライアントにネットワークを介してブートファイルを転送する方法であって、
前記クライアントが、前記サーバから前記クライアントに前記ブートファイルを転送するように前記ネットワークを介して要求するステップと、
前記サーバが、サーバの信頼性証明書を前記ネットワークを介して前記クライアントに送信するステップと、
前記クライアントが、前記受信されたサーバの信頼性の証明書により前記サーバを認証するステップと、
前記クライアントが、前記認証されたサーバから前記クライアントに前記ブートファイルを転送するように前記ネットワークを介して要求するステップと、
前記クライアントによる要求に応答して、前記認証されたサーバから前記クライアントに前記ブートファイルを転送するステップと
を備えることを特徴とする方法。
【請求項１３】
サーバからｐｒｅ－ＯＳ環境を有するクライアントにネットワークを介してブートファイルを転送する方法であって、
前記サーバから前記クライアントに前記ブートファイルを転送することを求める前記クライアントからの要求を、前記サーバが前記ネットワークを介して受信するステップと、
前記サーバが、以前にインストールされたクライアントの信頼性証明書を前記ネットワークを介して前記クライアントから受信するステップと、
前記サーバが、前記受信されたクライアントの信頼性証明書により前記クライアントを認証するステップと、
前記サーバが前記認証されたクライアントに前記ネットワークを介して前記ブートファイルを送信するステップと
を備えることを特徴とする方法。
【請求項１４】
サーバからｐｒｅ－ＯＳ環境を有するクライアントにネットワークを介してブートファイルを転送する方法であって、
前記クライアントが、前記サーバから前記クライアントに前記ブートファイルを転送するように前記ネットワークを介して要求するステップと、
前記クライアントが前記ネットワークを介して、サーバの信頼性証明書を前記サーバから受信するステップと、
前記クライアントが、前記受信されたサーバの信頼性証明書により前記サーバを認証するステップと、
前記クライアントが前記ネットワークを介して、前記認証されたサーバから前記クライアントに前記ブートファイルを転送するように要求するステップと、
前記クライアントの要求に応答して、前記認証されたサーバから前記クライアントへの前記ブートファイルを受信するステップと
を備えることを特徴とする方法。
【請求項１５】
無効または失効した証明書を有するサーバは、前記クライアントによって受信確認が返

されないことを特徴とする請求項１４に記載の方法。
【請求項１６】
前記転送されたブートファイルは署名を含み、前記クライアントは前記署名を確認することを特徴とする請求項１４に記載の方法。
【請求項１７】
署名が正しくない、前記クライアントによって受信されたブートファイルは、前記クライアントによって実行されないことを特徴とする請求項１４に記載の方法。
【請求項１８】
サーバからｐｒｅ－ＯＳ環境を有するクライアントにネットワークを介してブートファイルを転送する方法であって、
前記クライアントが、前記サーバから前記クライアントに前記ブートファイルを転送するように前記ネットワークを介して要求するステップと、
前記クライアントによる要求に応答して前記サーバから前記クライアントに前記ブートファイルを転送するステップと、
前記クライアントが前記転送されたブートファイルを認証するステップと、
前記認証されたクライアントが前記認証されたブートファイルを実行するステップと
を備えることを特徴とする方法。
【請求項１９】
前記転送されたブートファイルは署名を含み、前記クライアントは前記署名を確認することを特徴とする請求項１８に記載の方法。
【請求項２０】
署名が正しくない、前記クライアントによって受信されたブートファイルは、前記クライアントによって実行されないことを特徴とする請求項１９に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、クライアント、サーバ、およびブートファイルの検証および認証の分野に関する。より詳細には、本発明は、ネットワークを介してサーバに接続されたプレオペレーティングシステム環境にあるクライアントとの関連で行われるブートファイルの検証および認証に関する。
【背景技術】
【０００２】
プレオペレーティングシステム（ｐｒｅ－ＯＳ）のパーソナルコンピュータ（ＰＣ）をネットワークブートする際に伴う大きな問題の１つは、そのようなＰＣの安全性をサーバに対して検証することが難しいこと、および／または検証できないことである。また、多くのサーバは、そのクライアントを認証することができず、多くのクライアントは、そのサーバの整合性および／またはサーバからクライアントに提供されるブートファイルの整合性を検証することができない。さらに、オペレーティングシステムがインストールされていない新しいＰＣ、あるいは損傷したＰＣをブートする際には著しい制限がある。
【発明の開示】
【発明が解決しようとする課題】
【０００３】
特にｐｒｅ－ＯＳ環境で、クライアント、サーバ、またはブートファイルの整合性を検証する必要性がある。また、クライアントをブートし、ＯＳを導入するためのより安全で堅牢な方式を提供するために、クライアントがＯＳの状態に関係なく安全にブートすることを可能にする必要性もある。
【課題を解決するための手段】
【０００４】
プレインストール環境をクライアントに配置することにより、および、プレインストール環境にクライアント、サーバ、あるいはブートファイルの整合性を検証することができ

るコンポーネントを配置することにより、本発明は、クライアントをブートし、ＯＳを導入するためのより安全で堅牢な方式を提供する。また、ＯＳの状態に関係なくクライアントが安全にブートできるようにすることにより、クライアントをブートし、ＯＳを導入するためのより安全で堅牢な方式が得られる。したがって、本発明は、３つのコンポーネント、すなわちクライアント、サーバ、ブートファイルのいずれかまたはすべての整合性を検証するために使用できるプレインストール環境の非常駐（in-resident）コンポーネントを提供するシステムおよび方法に対する必要性を満たす。

【０００５】

概して、本発明は、ネットワーク環境でオペレーティングシステムのブートを検証し、認証するシステムおよび方法である。従来のネットワークを利用したブートは、サーバ／クライアントのための検証および認証のコンポーネントを含まない。本発明は、サーバ／クライアントを認証および確認するための３方向の認証フレームワークを提供する。本発明は、クライアントコンポーネントとサーバコンポーネントの両方にあるデジタル証明書などの検証機構を利用する。検証機構を交換することにより、クライアントはサーバに対して自身を認証することができ、サーバはクライアントに対して自身を認証することができ、クライアントは、サーバから送信されたブートファイルが正しく検証されることを確認することができる。

【０００６】

本発明の一態様によれば、ある方法は、サーバからｐｒｅ－ＯＳ環境を有するクライアントにネットワークを介してブートファイルを転送する。この方法は、クライアントの信頼性の証明書をクライアントにインストールすること、クライアントが、サーバがクライアントにブートファイルを転送するようにネットワークを介して要求すること、クライアントが、インストールされたクライアントの信頼性証明書を、ネットワークを介して送信すること、サーバが、受信されたクライアントの信頼性証明書によりクライアントを認証すること、サーバがクライアントを認証するのに応答して、サーバからネットワークを介してサーバの信頼性証明書をクライアントに送信すること、クライアントが、受信されたサーバの信頼性証明書によりサーバを認証すること、認証されたクライアントが、ネットワークを介して、認証されたサーバが認証されたクライアントにブートファイルを転送するように要求すること、認証されたクライアントによる要求に応答して、認証されたサーバから認証されたクライアントにブートファイルを転送すること、認証されたクライアントが転送されたブートファイルを認証すること、および、認証されたクライアントが認証されたブートファイルを実行することを備える。

【０００７】

別の形態では、本発明は、サーバからクライアントにブートファイルを転送する方法を備え、この方法は、サーバがクライアントを認証すること、クライアントがサーバを認証すること、および、認証されたサーバから認証されたクライアントにブートファイルを転送することを備える。

【０００８】

別の形態で、本発明は、ネットワークを介してサーバからｐｒｅ－ＯＳ環境を有するクライアントにブートファイルを転送する方法を備える。この方法は、クライアントにクライアントの信頼性の証明書をインストールすること、クライアントがネットワークを介して、サーバがクライアントにブートファイルを転送することを要求すること、クライアントが、インストールされたクライアントの信頼性の証明書をネットワークを介して送信すること、サーバが、受信されたクライアントの信頼性の証明書によりクライアントを認証すること、および、サーバから認証されたクライアントにブートファイルを転送することを備える。

【０００９】

別の形態で、本発明は、サーバからｐｒｅ－ＯＳ環境を有するクライアントにネットワークを介してブートファイルを転送する方法を備え、この方法は、クライアントにクライアントの信頼性証明書をインストールすること、クライアントが、サーバからクライアン

トにブートファイルを転送するようにネットワークを介して要求すること、クライアントがネットワークを介して、インストールされたクライアントの信頼性の証明書を送信すること、および、クライアントがサーバからブートファイルを受信することを備える。

【００１０】

別の形態で、本発明は、サーバからｐｒｅ－ＯＳ環境を有するクライアントにネットワークを介してブートファイルを転送する方法を備える。この方法は、サーバからクライアントにブートファイルを転送することを求めるクライアントからの要求を、サーバがネットワークを介して受信すること、サーバが、以前にインストールされたクライアントの信頼性証明書をネットワークを介してクライアントから受信すること、サーバが、受信されたクライアントの信頼性証明書によりクライアントを認証すること、および、サーバから認証されたクライアントにブートファイルを転送することを備える。

【００１１】

別の形態で、本発明は、サーバからｐｒｅ－ＯＳ環境を有するクライアントにネットワークを介してブートファイルを転送する方法を備え、この方法は、クライアントが、サーバからクライアントにブートファイルを転送するようにネットワークを介して要求すること、サーバがネットワークを介してサーバの信頼性証明書をクライアントに送信すること、クライアントが、受信されたサーバの信頼性の証明書でサーバを認証すること、クライアントが、認証されたサーバからクライアントにブートファイルを転送するようにネットワークを介して要求すること、および、クライアントによる要求に応答して、認証されたサーバからクライアントにブートファイルを転送することを備える。

【００１２】

別の形態で、本発明は、サーバからｐｒｅ－ＯＳ環境を有するクライアントにネットワークを介してブートファイルを転送する方法を備え、この方法は、サーバからクライアントにブートファイルを転送することを求めるクライアントからの要求をサーバがネットワークを介して受信すること、サーバが、以前にインストールされたクライアントの信頼性証明書をネットワークを介してクライアントから受信すること、サーバが、受信されたクライアントの信頼性証明書によりクライアントを認証すること、および、サーバが認証されたクライアントにネットワークを介してブートファイルを送信することを備える。

【００１３】

別の形態で、本発明は、サーバからｐｒｅ－ＯＳ環境を有するクライアントにネットワークを介してブートファイルを転送する方法を備え、この方法は、クライアントが、サーバからクライアントにブートファイルを転送するようにネットワークを介して要求すること、クライアントがネットワークを介して、サーバの信頼性証明書をサーバから受信すること、クライアントが、受信されたサーバの信頼性証明書でサーバを認証すること、クライアントがネットワークを介して、認証されたサーバからクライアントにブートファイルを転送するように要求すること、クライアントの要求に応答して、認証されたサーバからクライアントへのブートファイルを受信することを備える。

【００１４】

別の形態で、本発明は、サーバからｐｒｅ－ＯＳ環境を有するクライアントにネットワークを介してブートファイルを転送する方法を備える。この方法は、クライアントが、サーバからクライアントにブートファイルを転送するようにネットワークを介して要求すること、クライアントによる要求に応答してサーバからクライアントにブートファイルを転送すること、クライアントが転送されたブートファイルを認証すること、認証されたクライアントが認証されたブートファイルを実行することを備える。

【００１５】

別の形態で、本発明は、ブートファイルを転送するシステムを備え、このシステムは、クライアントと、ブートファイルを有するサーバと、クライアントをサーバに対して認証するソフトウェアと、サーバをクライアントに対して認証するソフトウェアと、認証されたサーバから認証されたクライアントにブートファイルを転送するソフトウェアとを備える。

【００１６】
別の形態で、本発明は、ネットワークを介してサーバからｐｒｅ－ＯＳ環境を有するクライアントにブートファイルを転送するためのコンピュータ可読媒体を備える。この媒体は、クライアントが、サーバからクライアントにブートファイルを転送するようにネットワークを介して要求するための命令と、クライアントがネットワークを介して、以前にインストールされたクライアントの信頼性証明書を送信するための命令と、サーバからのブートファイルをクライアントが受信するための命令とを有する。
【００１７】
別の形態で、本発明は、ネットワークを介してサーバからｐｒｅ－ＯＳ環境を有するクライアントにブートファイルを転送するためのコンピュータ可読媒体を備える。この媒体は、サーバからクライアントにブートファイルを転送することを求めるクライアントからの要求をネットワークを介してサーバが受信するための命令と、サーバが、以前にインストールされたクライアントの信頼性証明書をネットワークを介してクライアントから受信するための命令と、サーバが、受信されたクライアントの信頼性証明書によりクライアントを認証するための命令と、サーバから認証されたクライアントにブートファイルを転送する命令とを有する。
【００１８】
別の形態で、本発明は、ネットワークを介してサーバからｐｒｅ－ＯＳ環境を有するクライアントにブートファイルを転送するためのコンピュータ可読媒体を備える。この媒体は、サーバからクライアントにブートファイルを転送することを求めるクライアントからの要求をネットワークを介してサーバが受信するための命令と、サーバがネットワークを介して、以前にインストールされたクライアントの信頼性証明書をクライアントから受信するための命令と、サーバが、受信されたクライアントの信頼性証明書によりクライアントを認証するための命令と、サーバが認証されたクライアントにネットワークを介してブートファイルを送信するための命令とを有する。
【００１９】
別の形態で、本発明は、ネットワークを介してサーバからｐｒｅ－ＯＳ環境を有するクライアントにブートファイルを転送するためのコンピュータ可読媒体を備え、この媒体は、クライアントが、サーバからクライアントにブートファイルを転送するようにネットワークを介して要求するための命令と、クライアントがネットワークを介してサーバからサーバの信頼性証明書を受信するための命令と、クライアントが、受信されたサーバの信頼性証明書によりサーバを認証するための命令と、クライアントが、認証されたサーバからクライアントにブートファイルを転送するようにネットワークを介して要求するための命令と、クライアントの要求に応答して、認証されたサーバからクライアントへのブートファイルを受信するための命令とを備える。
【００２０】
あるいは、本発明は、この他各種の方法および装置を備えることができる。
【００２１】
この他の特徴は、以下の説明から一部が明らかになり、一部は以下の説明で指摘される。
【発明を実施するための最良の形態】
【００２２】
本発明は、ブート対象のクライアントに格納されたデジタル証明書、または他のデジタル形態の証明、または検証機構と、ブートサーバに格納された別のデジタル証明書、他のデジタル形態の証明、または検証機構を備える。本発明によるアーキテクチャおよび方法は３方向の認証を可能にする。証明書が内蔵されたｐｒｅ－ＯＳ環境を含むクライアントは、サーバからのブートファイル要求を（ＰＸＥまたは他の関連付けプロトコルを介して）行う。ＰＸＥ（Preboot Execution Environment）は、まだオペレーティングシステムがロードされていないネットワークコンピュータが、遠隔から管理者によって構成され、ブートされることを可能にする業界標準のクライアント／サーバインタフェースである

。ＰＸＥコードは通例、読み取り専用メモリチップまたはブートディスクに記憶されて新しいコンピュータと共に配送され、このコードによりコンピュータ（クライアント）はネットワークサーバと通信することができ、クライアントマシンが遠隔から構成され、そのマシンのオペレーティングシステムが遠隔からブートされることができる。ＰＸＥは次の３つの事項を提供する。

【００２３】

１）ダイナミックホスト構成プロトコル（ＤＨＣＰ）。クライアントがＩＰアドレスを受け取ってネットワークサーバへのアクセス権を得ることを可能にする。

２）クライアントの基本入出力システム（ＢＩＯＳ）によって使用されるアプリケーションプログラムインタフェース（ＡＰＩ）のセット、または、オペレーティングシステムのブートおよびその他の構成ステップを自動化する、ダウンロードされたネットワークブートストラッププログラム（ＮＢＰ）。

３）ＰＸＥ　ＲＯＭチップまたはブートディスクのＰＸＥコードを初期化する標準的方法。

【００２４】

サーバとクライアント間の最初の接続は、通例はクライアントからの要求によって開始されるが、様々なシナリオが企図される。サーバとクライアント間の最初の接続時には、どちらの方向にも信頼が確立されていない。すなわち、サーバによるクライアントの信頼もクライアントによるサーバの信頼も確立されていない。サーバがクライアントから要求を受信した後に、クライアントは自身の資格証明または証明書を提示する。そして、サーバは、クライアントが提示した証明書が有効であるか、失効していないかを判定する。有効でないか、失効している場合、サーバは応答しない。証明書が有効である場合、サーバは自身の証明書をもって応答する。クライアントは次いで、同様の分析を行ってサーバの信頼性および失効ステータスを判定する。サーバが信頼できることをクライアントが確認した場合、クライアントは実際のブートファイルを求めるさらなる要求を行う。サーバは、デジタル署名されたファイルをもって応答する。クライアントは、自身のローカル証明書を使用してそのファイルを調べて、ファイルの署名が正当なものかどうかを判定する。デジタル署名が正当なものであれば、クライアントはブートファイルを実行する。

【００２５】

図１は、本発明によるクライアントとサーバ間の通信を示すブロック図である。詳細には、図１には、ネットワーク１００を介してサーバ１０４からｐｒｅ－ＯＳ環境を有するクライアントコンピュータ１０６にブートファイル１０２を転送するシステムおよび方法を示している。一般に、ブートとは、コンピュータを始動またはリセットするプロセスである。最初に電源が投入されるか、またはリセットされると、コンピュータはブートファイルを実行して、自身のオペレーティングシステムをロードし、開始するか、かつ／または使用のためにコンピュータを準備する。

【００２６】

クライアント１０６の転送されたブートファイル１０８がクライアントによって実行されて、クライアントのオペレーティングシステム１１０を作成、再作成、変更、拡張、または強化することができる。概して、本発明による認証は次の１または複数を含む。サーバ１０４によるクライアント１０６の認証、および／またはクライアント１０６によるサーバ１０４の認証、および／または、認証されたサーバ１０４から認証されたクライアント１０６に認証されたブートファイル１０２を転送して、転送されたブートファイルをクライアント１０６上に作成し、そのファイルが認証および実行されてクライアント１０６のオペレーティングシステム１１０に作用できること。

【００２７】

図２は、本発明による方法およびシステムの動作を説明する流れ図である。図１および２には、ネットワーク１００を介してサーバ１０４からｐｒｅ－ＯＳ環境を有するクライアント１０６に１または複数のブートファイル１０２を転送する方法を示す。最初に２０２で、クライアントの信頼性の証明書１１２がクライアント１０６にインストールされる

。このインストール（ならびにクライアントとサーバ間の他の通信）は、手動で、またはネットワーク１００を介して実現されることができる。図１の矢印１１４で示されるように、２０４で、クライアント１０６は、クライアント１０６にブートファイル１０２を転送するようにネットワーク１００を介してサーバ１０４に要求し、２０６でクライアントは、インストールされたクライアントの信頼性の証明書１１２をネットワークを介して送信することによって自身の資格証明を提示する。２０８で、サーバ１０４は、受信したクライアントの信頼性の証明書１１２によってクライアントを認証する。クライアントが信頼できない場合（例えばクライアントの証明書が無効である、有効期限が切れている、または失効している場合）、プロセスは終了する。

【００２８】

図１の矢印１１６で表されるように、クライアントの証明書１１２が、サーバ１０４が保持しているか、アクセスできる信頼できるクライアントの既存のリストと一致して、クライアント１０６がサーバ１０４にとって信頼できる場合は、２１０で、サーバ１０４は、サーバによるクライアントの認証に応答して、ネットワーク１００を介してサーバの信頼性の証明書１１８をクライアント１０６に送信する。

【００２９】

２１２で、クライアント１０６は、受信したサーバの信頼性の証明書１１８でサーバ１０４を認証する。サーバ１０４が信頼できない場合（例えばサーバの証明書が無効、有効期限が切れている、あるいは失効している場合）、プロセスは終了する。クライアント１０６は、いくつかの方式の１つでサーバの証明書１１８を認証することができる。例えば、サーバの証明書１１８は、クライアントの証明書１１２に対応することができる。これに対して、サーバの証明書１１８は、クライアントが保持するか、アクセス権を持つ信頼性できるサーバの既存のリストと一致することができ、一致すればサーバ１０４がクライアント１０６にとって信頼できることになる。図１の矢印１２０で示されるように、クライアント１０６は、サーバの証明書１１８が一致するか、正当性が確認された場合にサーバ１０４に応答する。詳細には、２１４で、認証されたクライアントは、ネットワークを介して、認証されたサーバが認証されたクライアントにブートファイル１０２を転送するように要求する。図１の矢印１２２で表されるように、サーバ１０４は、ブートファイル１０２に署名を付加することによって応答し、２１６で、認証されたクライアントからの要求に応答して、署名されたブートファイルを認証されたサーバから認証されたクライアントに転送する。

【００３０】

次いで、２１８で、認証されたクライアントは、ブートファイルの署名がクライアント証明書および／またはサーバ証明書に対応することを確認することにより、転送された署名済みのブートファイルを認証する。詳細には、転送されたブートファイルは、クライアントの信頼性証明書に対応するサーバの署名を含んでいるはずであり、クライアントは、署名が自身の信頼性証明書に対応することを検証する（図２の１２４参照）。ブートファイルが認証されない場合（例えばブートファイルの署名が正しくない場合、ファイルが無効である、有効期限が切れている、または失効している場合）、プロセスは終了する。２２０で、認証されたブートファイルがクライアントにより実行されてオペレーティングシステム１１０を作成する。

【００３１】

また、本発明によるシステムおよび方法はクライアントの認証のみを含んでもよいことが企図される。この実施形態は次のように実施される。クライアントの信頼性の証明書１１２がクライアント１０６にインストールされる。この証明書は、手動で、ネットワーク１００を介して、またはサーバ１０４によってインストールされることができる。クライアントは、ネットワークを介して、サーバからクライアントにブートファイルを転送するように要求する。クライアントはネットワークを介して、インストールされた自身の信頼性の証明書を送信する。サーバは、受信したクライアントの信頼性の証明書によってクライアントを認証し、サーバから認証されたクライアントにブートファイル１０２を転送す

る。任意で、ブートファイルは署名されてもよく、認証されたクライアントは、転送された署名済みのブートファイルを認証した後にブートファイルを実行してもよい。

【００３２】

クライアントから見ると、クライアント認証のシステムおよび方法は、クライアントにインストールされたクライアントの信頼性の証明書を含むことになる。クライアントは、サーバからクライアントにブートファイルを転送することを要求するソフトウェア（または転送を促すマニュアル）を有する。クライアントはネットワークを介して、インストールされたクライアントの信頼性の証明書を送信し、サーバからブートファイルを受信する。任意で、認証されたクライアントは、転送されたブートファイルを認証してから実行してもよい。

【００３３】

サーバから見ると、クライアント認証のシステムおよび方法は、サーバがクライアントにブートファイルを転送することを求める要求を、ネットワークを介してクライアントから受信するサーバ上のソフトウェアを含む。このソフトウェアは、ネットワークを介して、以前にクライアントにインストールされたクライアントの信頼性の証明書も受信する。サーバは、受信したクライアントの信頼性の証明書でクライアントを認証するソフトウェアを含む。そして、サーバのソフトウェアは、サーバから認証されたクライアントに（任意で署名された）ブートファイルを転送する。

【００３４】

また、本発明によるシステムおよび方法は、サーバの認証のみを含んでもよいことも企図される。この実施形態では、クライアント１０６は、サーバ１０４からクライアントにブートファイル１０２を転送するようにネットワーク１００を介して要求する。サーバは、ネットワークを介して、サーバの信頼性の証明書１１８をクライアントに送信する。クライアントは、受信したサーバの信頼性の証明書でサーバを認証する。クライアントはネットワークを介して、認証されたサーバからクライアントにブートファイルを転送するように要求する。クライアントの要求に応答して、認証されたサーバからクライアントにネットワークを介してブートファイルが転送される。任意で、ブートファイルに署名してクライアントによって認証できるようにしてもよい。

【００３５】

サーバから見ると、サーバ認証のシステムおよび方法は、サーバからクライアントにブートファイルを転送することを求めるクライアントからの要求を、ネットワークを介して受信するソフトウェア、あらかじめインストールされたクライアントの信頼性の証明書をクライアントからネットワークを介して受信するソフトウェア、受信したクライアントの信頼性の証明書でクライアントを認証するソフトウェア、およびネットワークを介して（任意で署名された）ブートファイルを認証されたクライアントに送信するソフトウェアを含む。

【００３６】

クライアントから見ると、サーバ認証のシステムおよび方法は、サーバからクライアントにブートファイルを転送するようにネットワークを介して要求するソフトウェア、ネットワークを介してサーバの信頼性の証明書をサーバから受信するソフトウェア、受信したサーバの信頼性の証明書によってサーバを認証するソフトウェア、認証されたサーバがブートファイルをクライアントに転送するようにネットワークを介して要求するソフトウェア、およびクライアントの要求に応答して認証されたサーバから（任意で署名された）ブートファイルを受信するソフトウェアを含むことになる。

【００３７】

また、本発明によるシステムおよび方法はブートファイルの認証だけを含んでもよいことも企図される。この実施形態では、クライアント１０６は、ネットワーク１００を介して、サーバ１０４からクライアントにブートファイル１０２を転送するように要求する。クライアントの要求に応答して、署名されたブートファイルがサーバからクライアントに転送される。クライアントは転送された署名済みのブートファイルを認証し、認証された

ブートファイルを実行する。

【００３８】

クライアントがそのオペレーティングシステムを作成するために使用されるブートファイルの構成要素としてデジタル署名または他のデジタル形式の証明機構を含めることにより、クライアント、サーバ、およびブートファイルの徹底した検証を行うことができる。クライアントソフトウェアが、読み取り可能なコンピュータ可読メモリ（ＣＲＭ）デバイスに存在する場合でも、あるいは読み取り／書き込みのコンピュータ可読メモリ（ＣＲＭ）デバイスに存在する場合でも、プレインストール環境は次の事柄を行うことができる。

【００３９】

サーバが信頼できることを検証する。

クライアントが信頼できることをサーバに対して認証する、および

ブートファイルの整合性を検証する。

【００４０】

あるいは、上記のように異なる部分を実施して、クライアントの整合性だけを証明する、サーバの整合性だけを証明する、またはブートファイルの整合性だけを証明して、異なるセキュリティの層を可能にすることもできる。本発明による安全な解決法の１つは、上記３つすべてを可能にし、したがって、このプロセスの安全でないすべてのステップを確認するものである。

【００４１】

以下に述べる認証をパスしない場合の指針も危険性を低減するために実施されることができる。

【００４２】

証明書が無効または失効しているクライアントは、サーバによって応答されない。

証明書が無効または失効しているサーバは、クライアントによって受信確認が返されない。

【００４３】

署名が正しくない受信ブートファイルはクライアントによって実行されない。本発明は特に、ネットワーク展開に携わる会社および展開／管理に携わる会社に適用することができる。本発明は、従来技術によって満たされていない法人顧客のニーズである、ネットワークのブートプロトコルの安全確保を対象とする。

【００４４】

図３に、クライアント１０６または１０４とすることができるコンピュータ１３０の形態の汎用コンピューティングデバイスの一例を示す。本発明の一実施形態では、コンピュータ１３０のようなコンピュータが、他の図に示され、ここで説明されるクライアントおよび／またはサーバとして使用するのに適している。コンピュータ１３０は、１または複数のプロセッサあるいは処理装置１３２と、システムメモリ１３４を有する。図の実施形態で、システムバス１３６は、システムメモリ１３４を含む各種のシステム構成要素をプロセッサ１３２に結合する。バス１３６は、各種のバスアーキテクチャのいずれかを使用したメモリバスまたはメモリコントローラ、ペリフェラルバス、アクセラレーテッドグラフィックポート、およびプロセッサバスあるいはローカルバスを含む数種のバス構造の１または複数を表す。これらに限定しないが、そのようなアーキテクチャの例には、ＩＳＡ（Industry Standard Architecture）バス、ＭＣＡ（Micro Channel Architecture）バス、ＥＩＳＡ（Enhanced ISA）バス、ＶＥＳＡ（Video Electronics Standards Association）ローカルバス、およびメザニンバスとも称するＰＣＩ（Peripheral Component Interconnect）バスが含まれる。

【００４５】

コンピュータ１３０は通例、少なくとも何らかの形態のコンピュータ可読媒体を有する。コンピュータ可読媒体は、揮発性および不揮発性の媒体、取り外し可能および取り外し不能の媒体を含み、コンピュータ１３０からアクセスできる任意の利用可能媒体でよい。これに限定しないが、例として、コンピュータ可読媒体は、コンピュータ記憶媒体と通信

媒体を含む。コンピュータ記憶媒体は、コンピュータ可読命令、データ構造、プログラムモジュール、または他のデータなどの情報を記憶するための方法または技術として実施された揮発性および不揮発性の媒体、取り外し可能および取り外し不能の媒体を含む。例えば、コンピュータ記憶媒体には、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリまたは他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ）または他の光ディスク記憶、磁気カセット、磁気テープ、磁気ディスク記憶または他の磁気記憶装置、または所望の情報を記憶するのに使用されることができ、コンピュータ１３０によるアクセスが可能な任意の他の媒体が挙げられる。通信媒体は通例、コンピュータ可読命令、データ構造、プログラムモジュール、またはその他のデータを、搬送波などの変調データ信号または他のトランスポート機構として実施し、任意の情報伝達媒体を含む。当業者は、信号中に情報を符号化する形でその特性の１または複数を設定または変化させた変調データ信号に精通している。有線ネットワークや直接配線接続などの有線媒体、および音響、ＲＦ、赤外線、その他の無線媒体などの無線媒体は通信媒体の例である。上記の媒体の組み合わせもコンピュータ可読媒体の範囲に含まれる。

【００４６】

システムメモリ１３４は、取り外し可能および／または取り外し不能、揮発性および／または不揮発性メモリの形態のコンピュータ記憶媒体を含む。図の実施形態では、システムメモリ１３４は、読み取り専用メモリ（ＲＯＭ）１３８とランダムアクセスメモリ（ＲＡＭ）１４０を含む。起動時などにコンピュータ１３０内の要素間の情報転送を助ける基本ルーチンを含んだ基本入出力システム１４２（ＢＩＯＳ）は、通例ＲＯＭ１３８に記憶される。ＲＡＭ１４０は通例、処理装置１３２から即座にアクセスできる、かつ／または処理装置１３２によって現在操作中のデータおよび／またはプログラムモジュールを保持する。その例として、これに限定しないが、図３にはオペレーティングシステム１４４、アプリケーションプログラム１４６、他のプログラムモジュール１４８、およびプログラムデータ１５０を示す。

【００４７】

コンピュータ１３０は、この他の取り外し可能／取り外し不能、揮発性／不揮発性のコンピュータ記憶媒体も含むことができる。例えば、図３には、取り外し不能、不揮発性の磁気媒体の読み書きを行うハードディスクドライブ１５４を示す。図３には、取り外し可能、不揮発性の磁気ディスク１５８の読み書きを行う磁気ディスクドライブ１５６、およびＣＤ－ＲＯＭや他の光学媒体などの取り外し可能、不揮発性の光ディスク１６２の読み書きを行う光ディスクドライブ１６０も示す。この例示的動作環境で使用できる他の取り外し可能／取り外し不能、揮発性／不揮発性の記憶媒体には、これらに限定しないが、磁気テープカセット、フラッシュメモリカード、デジタル多用途ディスク、デジタルビデオテープ、ソリッドステートＲＡＭ、ソリッドステートＲＯＭなどが含まれる。ハードディスクドライブ１５４、磁気ディスクドライブ１５６、および光ディスクドライブ１６０は、通例、インタフェース１６６などの不揮発性メモリインタフェースによってシステムバス１３６に接続される。

【００４８】

上述し、図３に示すこれらドライブまたはその他の大容量記憶装置とそれらに関連付けられたコンピュータ記憶媒体は、コンピュータ１３０のコンピュータ可読命令、データ構造、プログラムモジュール、および他のデータの記憶を提供する。図３では、例えば、ハードディスクドライブ１５４にオペレーティングシステムシステム１７０、アプリケーションプログラム１７２、他のプログラムモジュール１７４、およびプログラムデータ１７６が記憶されている。これらのコンポーネントは、オペレーティングシステム１４４、アプリケーション１４６、他のプログラムモジュール１４８、およびプログラムデータ１５０と同じものでも、異なるものでもよいことに留意されたい。この図では、オペレーティングシステム１７０、アプリケーションプログラム１７２、他のプログラムモジュール１７４、およびプログラムデータ１７６には、それらが少なくとも異なるコピーであることを表すために異なる符号が付されている。

【００４９】
ユーザは、キーボード１８０およびポインティングデバイス１８２（マウス、トラックボール、ペン、タッチパッドなど）などの入力装置またはユーザインタフェース選択装置を通じてコンピュータ１３０にコマンドと情報を入力することができる。他の入力装置（図示せず）としては、マイクロフォン、ジョイスティック、ゲームパッド、衛星受信アンテナ、スキャナなどが可能である。これらおよびその他の入力装置は、システムバス１３６に結合されたユーザ入力インタフェース１８４を通じて処理装置１３２に接続されるが、パラレルポート、ゲームポート、ユニバーサルシリアルバス（ＵＳＢ）など他のインタフェースおよびバス構造で接続することも可能である。モニタ１８８あるいは他のタイプの表示装置もビデオインタフェース１９０などのインタフェースを介してシステムバス１３６に接続される。モニタ１８８に加えて、コンピュータはしばしば、プリンタやスピーカなどの他の周辺出力装置（図示せず）を含み、その出力装置は出力周辺インタフェース（図示せず）を通じて接続することができる。

【００５０】
コンピュータ１３０は、リモートコンピュータ１９４などの１または複数のコンピュータとの論理接続を使用するネットワーク環境で動作することができる。リモートコンピュータ１９４は、パーソナルコンピュータ、サーバ、ルータ、ネットワークＰＣ、ピアデバイス、あるいはその他の一般的なネットワークノードでよく、通例はコンピュータ１３０との関連で上述した要素の多くまたはすべてを含む。図３に示す論理接続には、ローカルエリアネットワーク（ＬＡＮ）１９６とワイドエリアネットワーク（ＷＡＮ）１９８が含まれるが、他のネットワークを含むことも可能である。ＬＡＮ１３６および／またはＷＡＮ１３８は、有線ネットワーク、無線ネットワーク、その２つの組み合わせなどである。このようなネットワーキング環境は、オフィス、企業内のコンピュータネットワーク、イントラネット、および世界規模のコンピュータネットワーク（インターネットなど）に一般的に見られる。

【００５１】
ローカルエリアネットワークの環境で使用される場合、コンピュータ１３０は、ネットワークインタフェースあるいはアダプタ１８６を通じてＬＡＮ１９６に接続される。ワイドエリアネットワークの環境で使用される場合、コンピュータ１３０は通例、インターネットなどのＷＡＮ１９８を通じて通信を確立するためのモデム１７８または他の手段を含む。モデム１７８は、内蔵型でも外付け型でもよく、ユーザ入力インタフェース１８４または他の適切な機構を介してシステムバス１３６に接続される。ネットワーク環境では、コンピュータ１３０との関連で図示したプログラムモジュールまたはその一部は、遠隔のメモリ記憶装置（図示せず）に記憶されることができる。例として、これに限定しないが、図３ではリモートアプリケーションプログラム１９２がメモリ装置に存在する。図のネットワーク接続は例示的なものであり、コンピュータ間に通信リンクを確立する他の手段を使用してよいことは理解されよう。

【００５２】
一般に、コンピュータ１３０のデータプロセッサは、異なる時にコンピュータの各種のコンピュータ可読記憶媒体に記憶される命令によってプログラムされる。プログラムおよびオペレーティングシステムは、典型的には、例えばフロッピー（登録商標）ディスクあるいはＣＤ－ＲＯＭで配布される。そこからコンピュータの補助記憶装置にインストールまたはロードされる。実行時に、それらプログラムおよびオペレーティングシステムの少なくとも一部分がコンピュータの電子主記憶装置にロードされる。ここに記載される本発明は、そのような媒体が、マイクロプロセッサまたは他のデータプロセッサと連動して下記で述べるステップを実施する命令またはプログラムを含む場合には、上記およびその他各種タイプのコンピュータ可読記憶媒体を含む。本発明は、ここに記載される方法および技術に従ってプログラムされた場合にはコンピュータ自体も含む。

【００５３】
説明のために、オペレーティングシステムなどのプログラムおよびその他の実行可能な

プログラムコンポーネントはここでは個別のブロックとして示される。ただし、そのようなプログラムおよびコンポーネントは、様々な時にコンピュータの種々の記憶コンポーネントに存在し、コンピュータのデータプロセッサによって実行されることが理解されよう。

【００５４】

コンピュータ１３０を含む例示的なコンピューティングシステム環境との関連で説明されたが、本発明は、この他の多数の汎用または特殊目的のコンピューティングシステム環境または構成で動作することができる。このコンピューティングシステム環境は、本発明の使用または機能性の範囲について何らの制限を示唆するものではない。さらに、このコンピューティングシステム環境は、例示的動作環境に示す構成要素の１つまたは組み合わせに関連する依存性または必要性を有するものとも解釈すべきでない。本発明とともに使用するのに適する可能性があるよく知られるコンピューティングシステム、環境、および／または構成の例には、これらに限定しないが、パーソナルコンピュータ、サーバコンピュータ、ハンドヘルドまたはラップトップ型機器、マルチプロセッサシステム、マイクロプロセッサを利用したシステム、セットトップボックス、プログラム可能な家電製品、携帯電話、ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータ、上記のシステムまたは機器を含む分散コンピューティング環境などが含まれる。

【００５５】

本発明は、１または複数のコンピュータまたは他のデバイスによって実行されるプログラムモジュールなどのコンピュータ実行可能命令に概ね即して説明されることができる。一般に、プログラムモジュールには、これらに限定しないが、特定のタスクを行うか、特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、およびデータ構造が含まれる。本発明は、通信ネットワークを通じてリンクされた遠隔の処理デバイスによってタスクが行われる分散コンピューティング環境で実施することもできる。分散コンピューティング環境では、プログラムモジュールは、メモリ記憶装置を含むローカルおよびリモート両方の記憶媒体に配置されることができる。

【００５６】

動作中、コンピュータ１３０は、ブートファイル１０２などのコンピュータ実行可能命令を実行する。

【００５７】

以下の例で本発明をさらに説明する。コンピュータ１３０がサーバ１０４として使用される場合、そのメモリは、サーバの信頼性の証明書１１８と、上述したクライアント１０６と通信し、クライアント１０６を認証するソフトウェアとを含む。コンピュータ１３０がクライアント１０６として使用される場合、そのメモリは、クライアントの信頼性の証明書１１２と、上述したサーバ１０４と通信するソフトウェア、サーバ１０４を認証するソフトウェア、ブートファイル１０２を認証するソフトウェア、ブートファイル１０２を実行するソフトウェアとを含む。

【００５８】

本発明またはその実施形態の要素を紹介する際、冠詞「ａ」、「ａｎ」、「ｔｈｅ」、および「前記」は、その要素が１または複数あることを意味するものとする。用語「～を備える」、「～を含む」、および「～を有する」は、包含的な意味とし、列挙された要素以外にさらに要素があってよいことを意味するものとする。

【００５９】

上記の内容から、本発明のいくつかの目的が達成され、他の有利な結果が実現されることが理解されよう。

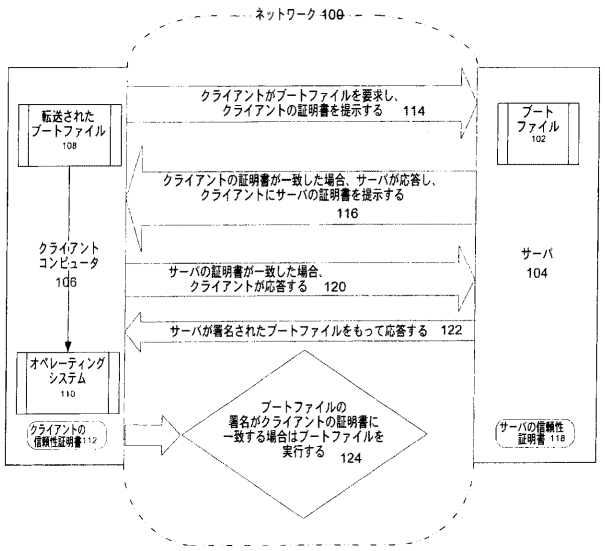
【００６０】

本発明の範囲から逸脱することなく上記の構成、製品、および方法には各種の変更を加えることができるので、上記の説明中に含まれ、添付図面に図示されるすべての事項は、例証を目的とし、限定的な意味に解釈すべきでない。

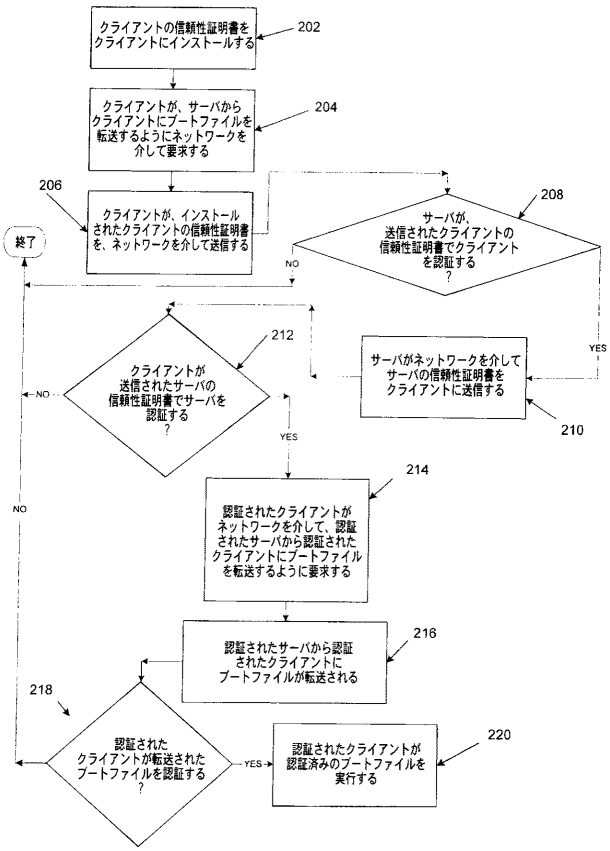
【図面の簡単な説明】

【００６１】
【図１】本発明によるクライアントとサーバ間の通信を表すブロック図である。
【図２】本発明による方法とシステムの動作を説明する流れ図である。
【図３】本発明を実施することが可能な適切なコンピューティングシステム環境の一例を示すブロック図である。
【符号の説明】
【００６２】
１００　ネットワーク
１０２　ブートファイル
１０４　サーバ
１０６　クライアントコンピュータ
１０８　転送されたブートファイル
１１０　オペレーティングシステム
１１２　クライアントの信頼性証明書
１１８　サーバの信頼性証明書

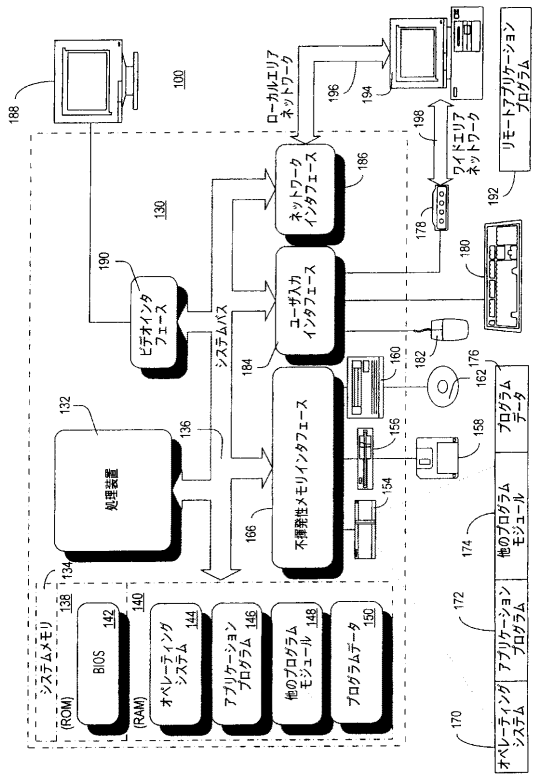
【図１】



【図２】



【図３】


100
188
ローカルエリアネットワーク
196
194
198
ワイドエリアネットワーク
リモートアプリケーションプログラム
192
ネットワークインタフェース
186
130
190
ビデオインタフェース
178
180
ユーザ入力インタフェース
システムバス
184
182
160
176
162
132
処理装置
136
不揮発性メモリインタフェース
156
158
154
166
プログラムデータ
他のプログラムモジュール
174
134
138
システムメモリ
(ROM)
BIOS
142
140
(RAM)
オペレーティングシステム
144
アプリケーションプログラム
146
他のプログラムモジュール
148
プログラムデータ
150
172
アプリケーションプログラム
170
オペレーティングシステム