(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4800719号
(P4800719)
(45)発行日　平成23年10月26日(2011.10.26)　(24)登録日　平成23年8月12日(2011.8.12)

(51)Int.Cl.　　F I
G06F 21/22 (2006.01)　　G06F 9/06 660N
G06F 21/20 (2006.01)　　G06F 15/00 330A

請求項の数 20　(全 12 頁)

(21)出願番号　特願2005-268551(P2005-268551)
(22)出願日　平成17年9月15日(2005.9.15)
(65)公開番号　特開2006-85714(P2006-85714A)
(43)公開日　平成18年3月30日(2006.3.30)
審査請求日　平成20年9月12日(2008.9.12)
(31)優先権主張番号　10/941,594
(32)優先日　平成16年9月15日(2004.9.15)
(33)優先権主張国　米国(US)

(73)特許権者　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　マーティン　エル．ホラディ
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

最終頁に続く

(54)【発明の名称】悪意のある通信の影響を受けやすいネットワークを介したソフトウェアの展開および受信

(57)【特許請求の範囲】
【請求項１】
デプロイメント・サーバで、リファレンス・コンピュータから、オペレーティング・システムを含むイメージを受信すること、
前記受信したイメージがロックされていない場合、希望しない通信を禁止するファイアウォールであって、前記デプロイメント・サーバによって使用されるポート以外の他のポートとの通信をコンピュータが行うことを禁止するファイアウォールを設定する前記イメージのセキュリティ設定を、前記デプロイメント・サーバで編集することによって、前記受信したイメージをロックすること、
ネットワークを介して前記コンピュータに、前記ロックされたイメージを展開すること
前記デプロイメント・サーバで、前記コンピュータに、前記ロックされたイメージをブートするように指示すること、
前記デプロイメント・サーバで、前記コンピュータに通信を要求し、ソフトウェア・アップデートを受信するよう指示すること
前記デプロイメント・サーバで、前記ソフトウェア・アップデートが成功したことを示す通知を、前記コンピュータから受信すること、および
前記通知を受け取った後、前記デプロイメント・サーバで、前記コンピュータに、前記ファイアウォールのポートを開き、前記ネットワークを介して潜在的に悪意のある通信を許可するよう指示すること
を備えることを特徴とする方法。

【請求項２】
前記リファレンス・コンピュータはリファレンス・サーバであり、前記受信したイメージをロックすることは、前記デプロイメント・サーバが前記リファレンス・サーバに、安全なソースまたは安全なポートを介する以外の前記ネットワークを介した希望しない通信を禁止するよう指示すること、および
前記リファレンス・サーバから、前記オペレーティング・システムを含むロックされたイメージを前記デプロイメント・サーバが受信すること
をさらに含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記リファレンス・サーバに指示することは、前記リファレンス・サーバにファイアウォールを使用可能にするよう指示することを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】
前記リファレンス・サーバに指示することは、前記リファレンス・サーバにＩＰＳｅｃプロトコルを追加するよう指示することを備えることを特徴とする請求項２に記載の方法。
【請求項５】
前記ロックされたイメージは、前記ネットワークを介して送信される、希望しない、潜在的に悪意のある通信を禁止することができることを特徴とする請求項１に記載の方法。
【請求項６】
前記ロックされたイメージは、前記ロックされたイメージが展開されたソースから以外の希望しない通信を禁止することができることを特徴とする請求項１に記載の方法。
【請求項７】
前記ソフトウェア・アップデートは、悪意のあるコードに対するオペレーティング・システムの耐性を向上させるのに有効であることを特徴とする請求項１に記載の方法。
【請求項８】
前記コンピュータは、ベア・コンピュータであることを特徴とする請求項１に記載の方法。
【請求項９】
前記コンピュータは、ベア・サーバであることを特徴とする請求項１に記載の方法。
【請求項１０】
前記コンピュータに通信を要求するよう指示することは、前記コンピュータに、前記ネットワークを介したアップデート・サーバからの通信を要求するよう指示することを備えることを特徴とする請求項１に記載の方法。
【請求項１１】
前記受信することおよび前記指示することは、前記ネットワークを介して通信されること特徴とする請求項１に記載の方法。
【請求項１２】
前記ネットワークは、インターネットと通信することができるイントラネットであることを特徴とする請求項１に記載の方法。
【請求項１３】
前記コンピュータによって、
ネットワークを介して、オペレーティング・システムを含むロックされたイメージを受信すること、
１つまたは複数の安全なソースまたは１つまたは複数の安全なポートを介する以外の希望しない通信を禁止するのに有効なセキュリティ設定を有する前記ロックされたイメージをブートすることと、
前記安全なソースから、または前記安全なポートを介して、指示を受信すること、
前記指示に従って、前記ネットワークを介してソフトウェア・アップデートを受信すること、

前記オペレーティング・システムのセキュリティを向上させるのに有効な前記ソフトウェア・アップデートを適用すること、および
前記ネットワークを介した潜在的に悪意のある通信を許可すること
を実行すること
さらに備えることを特徴とする請求項１乃至１２のいずれかに記載の方法。
【請求項１４】
前記ロックされたイメージは、前記ネットワークを介してデプロイメント・サーバから受信されることを特徴とする請求項１３に記載の方法。
【請求項１５】
受信すること、ブートすること、命令を受信すること、前記命令に従うこと、適用すること、および許可することのうちの少なくとも４つは、人間との対話なしに実施されることを特徴とする請求項１３に記載の方法。
【請求項１６】
前記アップデートを受信することは、アップデート・ソースから通信を要求する指示を受信し、前記アップデートを前記アップデート・ソースに要求することを備えることを特徴とする請求項１３に記載の方法。
【請求項１７】
前記許可することは、前記ネットワークを介する、希望しない、潜在的に悪意のある、通信を許可することを備えることを特徴とする請求項１３に記載の方法。
【請求項１８】
前記許可することは、前記セキュリティ設定を、希望しない、潜在的に悪意のある、通信を許可するように変更することを備えることを特徴とする請求項１７に記載の方法。
【請求項１９】
前記ロックされたイメージを受信することは、前記ロックされたイメージをブートすること、前記アップデートを受信すること、前記アップデートを適用することは、ユーザとの対話なしに実施されることを特徴とする請求項１３に記載の方法。
【請求項２０】
請求項１乃至１９のいずれかに記載の方法をコンピュータに実行させるプログラムを有する１つまたは複数のコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークを介したソフトウェアの展開（deploying）および受信に関する。
【背景技術】
【０００２】
新しい、ベア・サーバ（オペレーティング・システムを含まないサーバ）をネットワークに追加する最も迅速で容易な方法の１つは、ネットワークにそれを接続し（plug into）、ネットワーク上でデプロイメント・サーバを使用して、ベア・サーバにオペレーティング・システムのイメージ（image）を展開する（deploy）ことである。ベア・サーバは、このイメージを、そのハードディスク・ドライブ、または等価の記憶装置に保存し、次いでリブートすることができる。それ（ベア・サーバ）は、リブートすると、新しく展開されたオペレーティング・システム（newly deployed operating system）を使用して稼働することができる。
【０００３】
あるイメージによってベア・サーバに展開されたオペレーティング・システムは、しばしば、時代にそぐわなくなる。しかし、現在のものにアップデートすることが必要であり、安全性を確保することが好ましい。時代にそぐわなくなったオペレーティング・システムを含むサーバは、ネットワークにリンクされているのであれば、通常、現在のアップデートを含むインターネット・サイトまたはイントラネット・サーバから、ネットワークを

介してこうしたアップデートを得ることができる。
【０００４】
しかし、ネットワークは、それがイントラネットであるとしても、ウイルスや他のネットワーク・ベースの攻撃など、悪意のある通信の影響を受けやすい可能性がある。このために、サーバはしばしば、ネットワークを介して悪意のあるコードによる攻撃を受ける前に、こうしたアップデートを取得することができない。サーバがネットワーク上でそのオペレーティング・システムを使用して稼働を開始する時点と、サーバが現在のアップデートをダウンロードしてインストールを完了する時点との間のその時間に、ウイルスやトロイの木馬などの悪意のあるコードは、そのサーバを攻撃する可能性がある。多くの悪意プログラムが、時代にそぐわなくなった（旧式の）オペレーティング・システムを実行するサーバを破壊する（corrupt）のには１秒とかからないので、これは真の危険である。たとえば、ＭＳブラスタ・ウイルスは、適切なソフトウェア・アップデートを行っていないサーバを、１０分の１秒以内で破壊することができる。
【０００５】
この問題を部分的に対抗する（combat）ために、ベア・サーバを、たとえばケーブルを両方のサーバに手作業で接続することによって、ネットワークに接続することなしに、デプロイメント・サーバに接続することができる。このケーブルを介して、デプロイメント・サーバは、オペレーティング・システムを含むイメージをベア・サーバに展開することができる。次いで、サーバは、そのオペレーティング・システムでリブートされることができる。これが行われると、オペレーティング・システムを最適に安全な（セキュリティ保護された）状態にするために、アップデートを、通常は手作業で、コンパクト・ディスクを用いてインストールすることができる。アップデートされると、サーバを、ネットワークに接続することができる。
【０００６】
【特許文献１】米国特許第６，３４７，３９７号明細書
【特許文献２】米国特許第６，３６０，３６５号明細書
【特許文献３】米国特許第６，３８９，５９２号明細書
【特許文献４】米国特許第６，４１８，５５４号明細書
【特許文献５】米国特許第６，４８７，７１８号明細書
【特許文献６】米国特許第６，５８７，８３７号明細書
【特許文献７】米国特許第６，６１１，８１２号明細書
【特許文献８】米国特許第６，６１８，８５７号明細書
【特許文献９】米国特許出願公開第２００１／０，０１６，８８０号明細書
【特許文献１０】米国特許出願公開第２００２／０，１３１，０７２号明細書
【特許文献１１】米国特許出願公開第２００２／０，１６５，８６４号明細書
【特許文献１２】米国特許出願公開第２００３／０，００９，６５７号明細書
【特許文献１３】米国特許出願公開第２００３／０，１４５，３１７号明細書
【特許文献１４】米国特許出願公開第２００４／０，００６，６８９号明細書
【発明の開示】
【発明が解決しようとする課題】
【０００７】
上述した部分的な解決策は、攻撃に対するサーバの脆弱性を低減することができるが、この作業は時間がかかる。情報技術の専門家は、ベア・サーバをデプロイメント・サーバに直接に接続し、イメージを展開し、アップデートをインストールし、デプロイメント・サーバからそのサーバを切り離して、次いでそれをネットワークに接続するのに多くの時間を費やす可能性がある。
【０００８】
また、この問題を部分的に対抗するために、オペレーティング・システムおよびアップデートは、サーバをネットワークに接続する前に、通常多くのコンパクト・ディスクを用いて、ベア・サーバ上に手作業でインストールすることができる。しかし、オペレーティ

ング・システムおよびアップデートを手作業でインストールすることは、時間がかかり、退屈なことでもあり、またそれぞれのサーバについて、時間がかかる可能性がある。

【０００９】

したがって、悪意のある通信の影響を受けやすいネットワークを介して、サーバにオペレーティング・システムおよびアップデートを展開するための、安全な（セキュリティ保護された）やり方が求められている。

【課題を解決するための手段】

【００１０】

ネットワークを介してベア・コンピュータへの、オペレーティング・システム、およびそのオペレーティング・システムのアップデートの安全な（セキュリティ保護された）展開かつ／またはその受信を可能にするシステムおよび／または方法（「ツール」）が説明される。ある実施形態では、たとえば、このツールは、オペレーティング・システムを含むイメージを安全に（セキュリティ保護された方法で）展開し、またそのオペレーティング・システムのアップデートの安全な（セキュリティ保護された）受信を可能にし、その両方ともを、悪意の通信の影響を受けやすいネットワークを介して行う。第２の実施形態では、たとえば、このツールは、コンピュータによって実行されるときに、該コンピュータがネットワークを介して、悪意のあるかつ／または希望しない通信（unsolicited communications）を受信することを禁止するオペレーティング・システムを、ネットワークを介してコンピュータに展開する。第３の実施形態では、たとえば、このツールは、ネットワークに追加されたベア・コンピュータが、ネットワークを介して通信される悪意のあるコードの影響を受ける前に、ネットワークを介してそれに展開され、更新されたオペレーティング・システムを持つことを可能にする。

【発明を実施するための最良の形態】

【００１１】

同じ番号を、すべての開示および図面を通して使用して、同様のコンポーネントおよび特徴を参照する。

【００１２】

例示的なアーキテクチャ

図１を参照すると、リファレンス（参照）サーバ１０２、デプロイメント・サーバ１０４、アップデート・サーバ１０６、サーバ・ラック１０８を含む例示的なアーキテクチャ１００が示されている。リファレンス・サーバ、デプロイメント・サーバ、アップデート・サーバは、３つの別個のサーバとして示されているが、任意の組合せで、１つまたは複数のサーバに組み合わせることができる。デプロイメント・サーバは、以下で述べるプロセスのうちの１つまたは複数を実施することができるコンピュータ読取り可能媒体を含む。こうした媒体は、たとえば、デプロイメント・アプリケーション１１０およびロック・アプリケーション１１２を含むことができる。ロック・アプリケーションは、デプロイメント・アプリケーションの一部として示されているが、それぞれ、別個のものとすることも、組み合わせることもできる。アップデート・サーバは、その操作、たとえば、時代にそぐわない（旧式の）オペレーティング・システムを更新し、そのセキュリティ機能を向上させるために、ここではソフトウェア・パッチ、修正などを展開する（deploy）ことができるコンピュータ読取り可能媒体をも含む。

【００１３】

３つの例示的なベア・コンピュータ、すなわち、ラック１０８内のベア・サーバ１１４、ベア・スタンドアロン・サーバ１１６、およびベア・デスクトップ１１８もまた示されている。それぞれのベア・コンピュータは、そのベア・コンピュータが、たとえばデプロイメント・アプリケーション１１０に要求し、そこからの基本命令を受信し、それに従うことを可能にするのに十分なほどのソフトウェアまたはハードウェア・アプリケーションを含んでいる。

【００１４】

アーキテクチャ１００は、ネットワーク１２０を介して通信する。そのネットワークは

、ネットワーク・ベースの攻撃などの悪意のある通信の影響を受けやすい通信ネットワークである。このネットワークは、ネットワークを介して悪意のあるコードを送信することができるインターネットや、イントラネット内の破壊されたコンピュータ、などの安全でないソースと通信するイントラネットを含むことができる。

【００１５】

ロックされたイメージの作成

図２を参照すると、ロックされたイメージを作成するための例示的なプロセス２００が示されている。このプロセスは、ロック・アプリケーション１１２などを用いて、デプロイメント・サーバ１０４によって実施される個々の操作または行為を表す一連のブロックとして示されている。本明細書で述べるこのおよび他のプロセスは、任意の適切なハードウェア、ソフトウェア、ファームウェア、またはその組合せで実装することができる。ソフトウェアおよびファームウェアの場合、こうしたプロセスは、コンピュータ実行可能命令として実装される１組の操作を表す。

【００１６】

ブロック２０２で、ロック・アプリケーション１１２を使用するデプロイメント・サーバ１０４は、リファレンス・サーバ１０２に、信頼できないソースとの通信は禁止し、しかし、デプロイメント・サーバなどの少なくとも１つの信頼できるソースとの通信は許可するよう指示する。禁止される通信は、リファレンス・サーバが希望しないすべての通信を含むことも、（信頼できるソースから許されたもの以外の）希望する、または希望しないすべての通信を含むこともある。

【００１７】

ある実施形態では、ロック・アプリケーションは、デプロイメント・サーバによって使用されるポート以外のいずれのポートとも通信することを禁じるファイアウォールを使用可能にするよう、リファレンス・サーバに指示することによって、通信を選択的に禁止することができる。別の実施形態では、ロック・アプリケーションは、デプロイメント・サーバ（および、場合によってはアップデート・サーバ１０６）以外のいずれのコンピュータとも通信することを禁じることができるＩＰＳｅｃ（「Internet Protocol Security」：インターネット・プロトコル・セキュリティ）などの１つまたは複数のプロトコルを使用可能にするよう、リファレンス・サーバに指示することによって、それを行う。両方の実施形態において、リファレンス・サーバは、安全に（セキュリティ保護された方法で）動作するようにその設定を変更するように指示されるが、少なくとも１つの信頼できるソースとの通信を許可するように指示される。

【００１８】

こうした設定は、リファレンス・サーバのメモリ内に格納される。このために、リファレンス・サーバのメモリのイメージは、オペレーティング・システムおよびこうした設定を含むことができる。このイメージをブートするベア・コンピュータは、こうした設定をもつオペレーティング・システムを実行することができ、それによって、潜在的に危険な通信は禁止するが、信頼できるソースとの通信は許可する。イメージを受信するベア・コンピュータが、デスクトップ、または他の非サーバ・コンピュータである場合、リファレンス・サーバは、リファレンス・デスクトップ、または他の非サーバリファレンス・コンピュータであることもできる。

【００１９】

ブロック２０４で、デプロイメント・サーバ１０４は、オペレーティング・システムを含むイメージを受信する。後述するように、デプロイメント・サーバは、ある実施形態では、ブロック２０４および２０６を、また別の実施形態では、ブロック２０２および２０４を実施する。このイメージは、図１のリファレンス・サーバから、または別のリファレンス・コンピュータ（図示せず）から受信することができる。そのイメージが、たとえばブロック２０２の動作の結果として、ロックされる場合、デプロイメント・サーバは、ブロック２０６に進まない。イメージがロックされない場合、デプロイメント・サーバは、ブロック２０６に進む。別の実施形態では、デプロイメント・サーバは、イメージがベア

・サーバに保存された後ではあるが、ベア・サーバがリブートする（図示せず）前まで、イメージをロックするのを待つ。

【００２０】

ブロック２０６で、デプロイメント・サーバは、ロック・アプリケーション１１２を介して、オペレーティング・システムを含むイメージを編集する。この編集は、デプロイメント・サーバ１０４などの少なくとも１つの信頼できるソースからのものを除いて、希望しない通信を禁止するようセキュリティ設定を変更することによって、イメージをロックすることを備えることができる。禁止される通信は、オペレーティング・システムを実行するコンピュータが希望しないすべての通信を含むことも、（信頼できるソースから許可されたもの以外の）希望する、または希望しないすべての通信を含むこともある。ロック・アプリケーションは、イメージのセキュリティ設定を、ブロック２０２で述べたファイアウォールなどのファイアウォールを追加したり、または作動させたりするように編集することによって、それを行うことができる。ロック・アプリケーションは、たとえば、ブロック２０２で述べたＩＰＳｅｃプロトコルを含むようにイメージのセキュリティ設定を編集することによって、それを行うこともできる。したがって、ロック・アプリケーションは、イメージ内のソフトウェアを実行するコンピュータによる潜在的に危険な通信は禁じるが、信頼できるソースとの通信は許可するように、イメージをロックする。

【００２１】

ロックされたイメージの展開（deploying）およびオペレーティング・システムのアップデート

図３を参照すると、悪意のある通信の影響を受けやすい脆弱なネットワークを介して、オペレーティング・システムを含むイメージを安全に（セキュリティ保護された方法で）展開し、またオペレーティング・システムのアップデートの安全な（セキュリティ保護された）受信を可能にするための例示的なプロセス３００が示されている。このプロセスは、たとえばデプロイメント・アプリケーション１１０を用いて、デプロイメント・サーバ１０４によって実施される個々の操作および行為を表す一連のブロックとして示されている。ロックされたイメージ、およびオペレーティング・システムのアップデートを安全に（セキュリティ保護された方法で）受信するための例示的なプロセス３０２もまた示されている。プロセス３０２は、ベア・サーバ１１４によって、またはそれに対して実施される操作または行為を表す一連のブロックとして示されている。

【００２２】

ブロック３０４で、ベア・コンピュータは、ネットワーク１２０に接続される。スタンドアロン・サーバ１１６やデスクトップ１１８など、他のベア・コンピュータを代わりにネットワークに接続することができるけれども、現在述べてようとしている実施形態では、ベア・サーバ１１４が、ラック１０８を介してネットワークに接続される。

【００２３】

ブロック３０６で、ベア・サーバは、ネットワークを介して通信し、オペレーティング・システムを要求する。このベア・サーバは、オペレーティング・システムを有さないので、大抵の場合、ネットワーク上の悪意のあるコードに対してまだ脆弱ではない。

【００２４】

ブロック３０８で、デプロイメント・サーバ１０４は、オペレーティング・システムを求める要求を受信する。ブロック３１０で、デプロイメント・サーバは、デプロイメント・アプリケーション１１０を介して、オペレーティング・システムを含むロックされたイメージをベア・サーバに安全に（セキュリティ保護された方法で）展開する。一部の実施形態では、このブロックで、デプロイメント・サーバは、ソフトウェア・アップデートをも展開する。このロックされたイメージは、プロセス２００の結果としてもたらされることもある。現在述べている実施形態では、このロックされたイメージは、ベア・サーバによって実行されるときに（したがって、このサーバは、もはやベア・状態ではない）、デプロイメント・サーバ以外のソースからの、またはデプロイメント・サーバによって使用されるポート以外のポートからの、希望しない通信の受信を許可しないもの（イメージ）で

ある。

【００２５】

ブロック３１２で、ベア・サーバは、ネットワークを介して、ロックされたイメージを安全に（セキュリティ保護された方法で）受信し、それをメモリに格納する。ロックされたイメージを安全に（セキュリティ保護された方法で）受信することによって、ベア・サーバは、伝送中に悪意の通信の影響を受けずに、ロックされたイメージを受信することができる。このロックされたイメージの安全な（セキュリティ保護された）通信によって、それが第３者によって傍受されまたは監視されることを防止することもできる。ある実施形態では、ベア・サーバは、ロックされたイメージと共に、またはその一部として、アップデートをも受信する。ブロック３１４で、ベア・サーバは、それがロックされたイメージを受信したことを伝える。ブロック３１６で、デプロイメント・サーバは、ベア・サーバから、それがロックされたイメージを受信したことを示す通信を受信する。ブロック３１８で、デプロイメント・サーバは、デプロイメント・アプリケーションを介して、ロックされたイメージをブートするようベア・サーバに指示する。

【００２６】

ブロック３２０で、ベア・サーバは、リブートし、それによって、オペレーティング・システムおよびその安全な（セキュリティ保護された）設定を含むイメージを実行する。このベア・サーバは、オペレーティング・システムを有するので、この時点ではもはやベア・状態ではなく、安全な（セキュリティ保護された）モードで稼働している。このベア・サーバは、そのイメージ内の設定および／またはソフトウェアのために、信頼できない、または潜在的に悪意のある通信を禁止することができる。このベア・サーバは、それがネットワーク１２０に接続されているにも関わらず、またネットワークを介して送信される悪意のある通信に対して違った方法では脆弱であり得た、時代にそぐわないオペレーティング・システムで潜在的に動作しているとしても、安全に（セキュリティ保護された方法で）動作することができる。

【００２７】

ブロック３２２で、ベア・サーバ１１４は、オペレーティング・システムが実行されていること、および／またはブートが成功したことをデプロイメント・サーバに知らせる。

【００２８】

ブロック３２４で、デプロイメント・サーバ１０４は、この情報を受信する。ブロック３２６で、デプロイメント・サーバは、デプロイメント・アプリケーション１１０を介して、アップデートを安全に（セキュリティ保護された方法で）受信し、かつ／またはインストールするようベア・サーバに指示する。現在述べている実施形態では、デプロイメント・サーバは、ベア・サーバに、アップデート・サーバ１０６との通信を開始するよう指示する。別の実施形態では、デプロイメント・サーバは、ベア・サーバのオペレーティング・システムにアップデートを安全に（セキュリティ保護された方法で）送信し、アップデート・サーバのような別個のアップデート・ソースを使用しないでこうしたアップデートを追加するようそれに指示する。さらに別の実施形態では、アップデートは、ブロック３１０で送信され、ブロック３１２で受信されたイメージと共に、またはその一部として受信される。この実施形態では、デプロイメント・サーバは、ベア・サーバに、既に受信されているアップデートをインストールするように指示する。こうした実施形態のうちのいずれかで受信されたアップデートは、ベア・サーバ上のオペレーティング・システムまたは他のソフトウェアを更新するのに有効であることができ、またソフトウェア・パッチ、修正などを含むことができる。こうしたアップデートは、以下でより詳細に述べる、ベア・サーバによって、その後に受信される様々な悪意のあるコードに対する耐性を向上させることができる。

【００２９】

ブロック３２８で、ベア・サーバは、アップデートを安全に（セキュリティ保護された方法で）受信するよう指示する命令を受信する。現在述べている実施形態では、ベア・サーバは、デプロイメント・サーバから命令を受信する。

【００３０】
ブロック３３０で、ベア・サーバは、安全な（セキュリティ保護された）通信を開始して、アップデートを安全に（セキュリティ保護された方法で）受信する。現在述べている実施形態では、ベア・サーバは、アップデート・サーバ１０６からの通信を要求する。ベア・サーバのセキュリティ設定は、請求されていない通信の受信を防止するように構成されているが、ベア・サーバは、アップデート・サーバから通信を請求することは許されている。そうすることによって、要求されたアップデート・サーバからのアップデートまたは他の情報が、オペレーティング・システムを実行するベア・サーバによって受信することができる。一方、要求されていない他の情報は、そのセキュリティ設定のために、ベア・サーバによって拒否されることができ、それによって、ベア・サーバがアップデートを受信することを可能にしながら、希望しない悪意のあるコードからベア・サーバを保護する。

【００３１】
ブロック３３２で、ベア・サーバは、安全に（セキュリティ保護された方法で）アップデートを受信し、そのオペレーティング・システムに適用する。こうしたアップデートは、たとえば、ブロック３３０で要求されたアップデート・サーバから、またはデプロイメント・サーバから直接に、ネットワークを介して受信することができる。この安全な（セキュリティ保護された）アップデート受信によって、ベア・サーバは、ネットワークを介して通信される悪意のあるコードに対して脆弱であった最初の時点の状態が無くなり、悪意のある通信の影響を受けやすいネットワークを介して、更新されたオペレーティング・システムを有することができる。

【００３２】
ブロック３３４で、ベア・サーバは、それがオペレーティング・システムを更新したことを伝える。ブロック３３６で、デプロイメント・サーバは、この通信を受信する。

【００３３】
ブロック３３８で、デプロイメント・サーバは、ベア・サーバに、潜在的に悪意のある通信を開始するよう指示する。オペレーティング・システムが更新されたので、ベア・サーバは、ネットワークを介して通信される悪意のあるコード、および攻撃に対して、よりよく自己防衛することができる。ある実施形態では、潜在的に悪意のある通信を開始する前に、ベア・サーバのオペレーションをさらにセキュリティ保護するために、デプロイメント・サーバは、ファイアウォールまたはＩＰＳｅｃプロトコルを送信し、かつ／またはベア・サーバにそれをインストールするよう指示する。

【００３４】
ブロック３４０で、ベア・サーバは、たとえばプロダクション操作モード（production mode of operation）を開始することによって、ネットワークを介して、潜在的に悪意のある通信を開始する。ベア・サーバは、たとえば特定のポートを開くことによって、それを行うことができる。たとえばベア・サーバがウェブ・サーバとなる場合、それは、ポート８０を開いて、それがインターネットを介して他のサーバと通信できるようにし得る。

【００３５】
現在述べている実施形態では、デプロイメント・サーバおよびデプロイメント・アプリケーションの行為（act）のすべてではないとしても、そのほとんどが、自動的に、ユーザ対話なしに実施することができる。これによって、ユーザは、ベア・サーバまたは他のベア・コンピュータをネットワークに接続し、さらなる対話を行わずに、オペレーティング・システムが更新される前にネットワークを介してベア・サーバを悪意のあるコードにさらされることなく、ベア・サーバを更新されたオペレーティング・システムで動作させることができる。

【００３６】
結論
上述のツールは、悪意のある通信の影響を受ける可能性のあるネットワークを介した、オペレーティング・システムおよびアップデートの安全な（セキュリティ保護された）展

開および／または受信を可能にする。本発明について、構造上の特徴および／または方法論的な行為（act）に特有の言語で説明したが、添付の特許請求の範囲中に定められた本発明は、説明した特定の特徴または行為に必ずしも限定されないことを理解されたい。そうではなく、特定の特徴または行為（act）は、特許請求の範囲に記載された本発明を実施する例示的な形として開示されている。

【図面の簡単な説明】

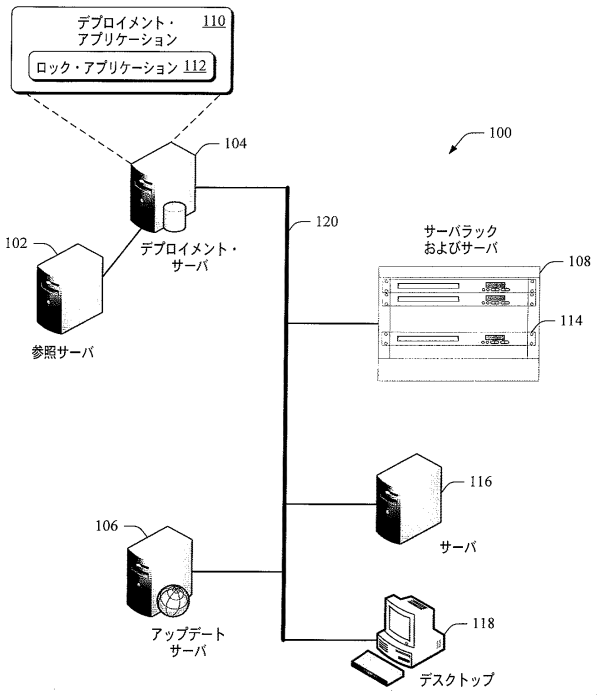
【００３７】

【図１】例示的なサーバ、悪意のある通信の影響を受けやすいネットワーク、およびベア・コンピュータを含む例示的なアーキテクチャを示す図である。

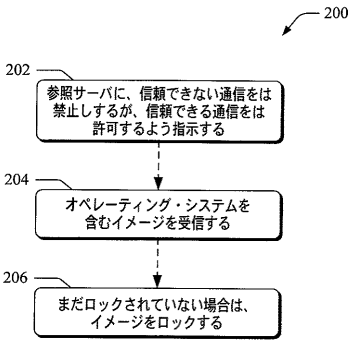
【図２】オペレーティング・システムを含むロックされたイメージを作成するための例示的なプロセスのフローチャートである。

【図３】悪意のある通信の影響を受けやすいネットワークを介して、ロックされたイメージおよびアップデートを展開および受信するための例示的なプロセスのフローチャートである。

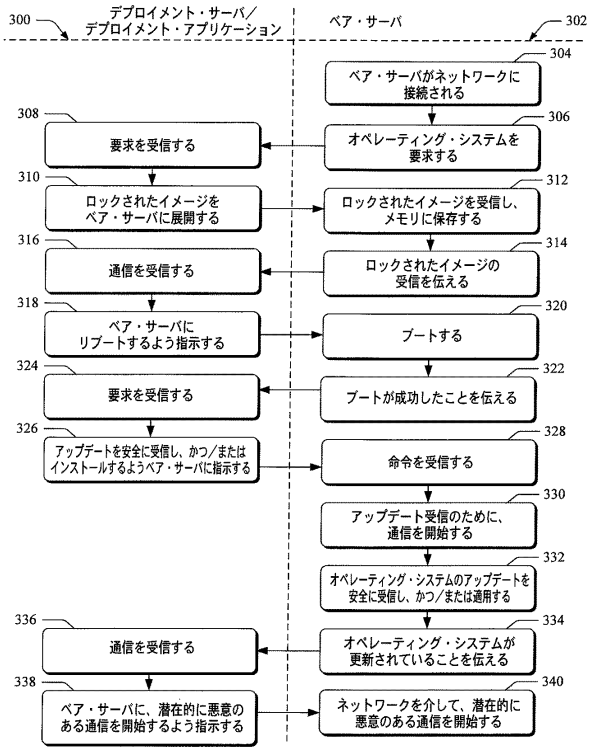
【図１】



【図２】



【図３】


300
デプロイメント・サーバ／
デプロイメント・アプリケーション
ベア・サーバ
302
304
ベア・サーバがネットワークに
接続される
306
オペレーティング・システムを
要求する
308
要求を受信する
310
ロックされたイメージを
ベア・サーバに展開する
312
ロックされたイメージを受信し、
メモリに保存する
316
通信を受信する
314
ロックされたイメージの
受信を伝える
318
ベア・サーバに
リブートするよう指示する
320
ブートする
324
要求を受信する
322
ブートが成功したことを伝える
326
アップデートを安全に受信し、かつ／または
インストールするようベア・サーバに指示する
328
命令を受信する
330
アップデート受信のために、
通信を開始する
332
オペレーティング・システムのアップデートを
安全に受信し、かつ／または適用する
336
通信を受信する
334
オペレーティング・システムが
更新されていることを伝える
338
ベア・サーバに、潜在的に悪意の
ある通信を開始するよう指示する
340
ネットワークを介して、潜在的に
悪意のある通信を開始する

フロントページの続き

(72)発明者　ムケシュ　カルキ
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　パルタサラティ　ナラヤナン
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

審査官　後藤　彰

(56)参考文献　特開２００６－０１８６０８（ＪＰ，Ａ）
特開２００６－０４０１１５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２２
Ｇ０６Ｆ　２１／２０