(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5518865号
(P5518865)

(45)発行日　平成26年6月11日(2014.6.11)　(24)登録日　平成26年4月11日(2014.4.11)

(51)Int.Cl.　F I
G06F 21/56 (2013.01)　G06F 21/00 156A
G06F 21/57 (2013.01)　G06F 21/00 157A

請求項の数 6　(全 15 頁)

(21)出願番号　特願2011-525050 (P2011-525050)
(86)(22)出願日　平成21年7月31日 (2009.7.31)
(65)公表番号　特表2012-510650 (P2012-510650A)
(43)公表日　平成24年5月10日 (2012.5.10)
(86)国際出願番号　PCT/US2009/052438
(87)国際公開番号　WO2010/025007
(87)国際公開日　平成22年3月4日 (2010.3.4)
審査請求日　平成24年7月24日 (2012.7.24)
(31)優先権主張番号　12/199,812
(32)優先日　平成20年8月28日 (2008.8.28)
(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　100140109
弁理士　小野　新次郎
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100101373
弁理士　竹内　茂雄
(74)代理人　100118902
弁理士　山本　修
(74)代理人　100153028
弁理士　上田　忠

最終頁に続く

(54)【発明の名称】感染したホストによる攻撃からの仮想ゲストマシンの保護

(57)【特許請求の範囲】
【請求項１】
仮想化環境において、マルウェアに感染したホストマシンからゲストマシンを保護するための方法であって、
前記ホストマシン上に実現されるゲストのヘルスエージェントが、前記ホストマシン上に実現されるホストのヘルスエージェントに、前記ホストマシンのヘルスを示す１つ又は複数の要素を検査するための検査要求を送信するステップと、
前記ホストのヘルスエージェントが、前記検査要求に応答して、前記１つ又は複数の要素を検査し、検査実施後、前記ホストマシンのヘルスを示す準拠の宣言を前記ゲストのヘルスエージェントに送信するステップと、
前記ゲストのヘルスエージェントが、前記準拠の宣言を準拠ポリシーと比較して、前記ホストマシンが前記準拠ポリシーに準拠しているか否かを判定するステップと、
前記ホストマシンが前記準拠ポリシーに準拠していると判定された場合に、仮想化環境を作成するために、前記ゲストマシンが起動処理を継続するステップと、
前記ホストマシンが前記準拠ポリシーに準拠していないと判定される場合に、前記ゲストマシンが前記起動処理を終了するステップと
を備えたことを特徴とする方法。
【請求項２】
前記１つ又は複数の要素は、セキュリティパッチ状態、アンチウイルスのソフトウェアの存在、アンチマルウェアソフトウェアの存在、ウイルスの署名の状態、マルウェアの署

名の状態、前記ホストマシンが前記ゲストマシンを実行するために認証されることを示す証明書又はファイルのレジストリー鍵の存在、ファイヤーウォールの存在、又は前記ファイヤーウォールの設定状態の少なくとも１つを含むことを特徴とする請求項１に記載の方法。

【請求項３】

コンピューター読み取り可能な媒体に格納された命令を受け取るステップをさらに含み、前記ホストマシン上に配置された１つ又は複数のプロセッサーにより実行されるとき、前記ホストのヘルスエージェント又は前記ゲストのヘルスエージェントを実装することを特徴とする請求項１又は２に記載の方法。

【請求項４】

前記コンピューター読み取り可能な媒体は、前記仮想化環境において使用されるデスクトップ画像をさらに含む記憶媒体であることを特徴とする請求項３に記載の方法。

【請求項５】

前記デスクトップ画像は、前記準拠ポリシー、データー、ユーザー設定、ユーザー優先権又はアプリケーションの１つもしくは複数を含むことを特徴とする請求項４に記載の方法。

【請求項６】

前記ホストマシンが前記準拠ポリシーに準拠していないと判定されるとき、エラーメッセージを表示するステップをさらに含み、前記エラーメッセージが前記ホストマシンの前記準拠ポリシーに準拠しないことを示し、前記準拠しないことの修正が実行される可能性があることの通知を提供することを特徴とする請求項１又は２に記載の方法。

【発明の詳細な説明】

【背景技術】

【０００１】

仮想化は、あるコンピューティングリソースを他から隔離又は分離させることにより、ＩＴ(Information Technology)インフラストラクチャーをより効果的及び効率的に利用可能にする広範囲の関わりで重要な戦略である。この戦略は、データーセンターからデスクトップへのコンピューティングの積み重ねのすべてのレイヤーに適用される可能性がある。静的コンピューティング環境で典型的であるように多様なレイヤーを一緒にロックするよりむしろ、つまりＯＳ(Operating System)からハードウェア、アプリケーションからＯＳ、及びユーザーインターフェースからローカルのコンピューティングデバイスであり、仮想化は、互いに有するこれらの部分の直接の依存をなくすことを狙う。

【０００２】

このようなデーターセンターからデスクトップへの仮想化は、新しいハードウェア又は設定コンポーネントを獲得することなく、迅速に新しい性能を展開することを可能にする。テスト要件及びアプリケーションの互換性の問題が少なくなり、自動処理が簡略化し、障害リカバリーの性能の実装がより簡単になる。デスクトップ上での仮想化は、顧客又は会社の従業員が、必要なアプリケーションがどこに配置されていたとしてもそれらにアクセスすることが可能になるインフラストラクチャーを作成するのに役立つ。例えば、ユーザーは、ゲストマシンを実装するために仮想化の製品及び技術を使用して、仮想的に任意の位置からホストマシンを使用し、それらのアプリケーション、データー、設定及び優先度の性能の全てにおいて、パーソナライズ化されたデスクトップにアクセスできる。

【０００３】

この背景技術は、続く詳細な説明及び概要の簡単な背景を導くために提供される。この背景技術は請求された主題の範囲を決定する際に考慮されることを意図しておらず、上記の不利又は問題の任意又は全てを解決するために請求された主題を限定するものとして見られることも意図していない。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

仮想化環境において、ゲストマシンが、不健全(unhealthy)に感染したホストマシン上で操作可能であり、ホストマシンにより攻撃されているゲストマシンの脅威は、（現在のセキュリティのパッチを最新にすること、アンチウイルスプログラムを実行すること、ゲストマシンを実行するために認証すること等の）適用可能なポリシーに準拠することにより健全であるか否か、及び、ゲストマシンのセキュリティを妨害又は侵害する可能性のある悪意のソフトウェア又はマルウェア(malware)から自由であるか否かを判定するために、ホストマシンが監視される編成により対処される。ホストマシンが準拠していないことが発見される場合、ゲストマシンがホストマシン上に起動すること又はネットワークに接続することのいずれかを防ぎ、仮想化環境の全体が準拠していて、データー及びアプリケーション等を含んでいるゲストマシンが、不健全なホストマシン上で実行している悪意のあるコードを介して、それに対して立ち上げられる可能性のある攻撃に対して保護されるか又は準拠していないことを修正できるまでネットワークから隔離することを保証する。

【０００５】

多様な例示的な例において、ゲストマシン上で実行しているゲストのヘルスエージェント(health agent)は、ゲスト上に格納された又は準拠ポリシーサーバーから受け取った１以上の準拠ポリシーでホストの準拠を検査するためのゲストの起動処理の間にホストマシン上のホストのヘルスエージェントと通信するように構成される。ホストマシンが準拠していないことが発見される場合、ゲストマシンがユーザーにエラーメッセージを表示する可能性があるので、ホストマシンの準拠していないことを修正できる。例えば、適切なパッチをインストールすること、アンチウイルスアプリケーション又はアップデートを除くこと等による。ホストマシンが既に準拠している場合、又は準拠となるように修正されていた後の場合、ゲストマシンは仮想化環境を実現するためのブート処理を完了することができ、ユーザーのデスクトップ、アプリケーション及びデーターは、ゲストマシン上で使用可能となる。

【０００６】

ホストマシンの準拠状態は、仮想化の環境が初期化されて操作可能である後に、定期的に検査される可能性もある。例えば、ゲストマシンが企業又は会社のネットワーク等のネットワークへの接続を試みる場合、ゲストのヘルスエージェントは、ホストマシンの現在のヘルスを示すホストのヘルスエージェントから準拠の宣言を要求する可能性がある。ネットワークアクセスが許可される前に、施行ポイントにより要求された１以上のポリシーで、ホストマシンの準拠を検証するために、ネットワーク上のリモートのポリシーの施行ポイントに、ゲストのヘルスエージェントにより準拠の宣言を、転送することができる。準拠の宣言が、ホストマシンが適用可能なポリシーに準拠しない（これはホストが危険にさらされており、マルウェアにより感染及び／又は侵害される高い可能性を有することを示す）ことを示す場合、ネットワークアクセスは拒否される。ユーザーはエラーメッセージを提供される可能性があるので、ネットワークアクセスをもう一度試みる前に準拠していないことが修正される可能性がある。

【０００７】

ホストマシンのヘルスの検査の別の例において、仮想化環境の完全性が侵害されている疑いがある場合、ゲストのヘルスエージェントは、適用可能なポリシーへの継続した準拠を検証及び又は確認するために、ホストのヘルスエージェントから準拠の宣言を要求する可能性がある。例えば、ＥＳＡＳ(Enterprise Security Assessment Sharing)セキュリティモデル下のセキュリティ評価は、ネットワーク内のセキュリティ関連情報を監視するために編成されるエンドポイント（つまりセキュリティのゲートウェイのデバイス）で受け取られる可能性がある。この受け取られたセキュリティ評価は、仮想化環境が侵害される疑いを引き起こす可能性がある。ホストマシンを巻き込んでいるセキュリティ事故が疑いを確認又は拒絶するために起きたか否かを判定するために、又はホストの更なる分析を引き起こすために、この準拠の宣言を使用できる。ホストマシンが侵害されていることが確認された場合、ホストマシンを巻き込んでいるセキュリティ事故が対処及び修正されるまで、ゲストマシン上の操作は中断され、ネットワーク接続要求は拒否される等の可能性が

ある。
【０００８】
有利なことに、ホスト上のマルウェアからの攻撃に対してゲストマシンを保護するための現在の編成は、仮想化された環境においてセキュリティを高めることを可能にする。コンピューティングリソースの分離の基本の仮想化の本質が保持される一方で、ゲストマシン及びホストマシンのセキュリティ分析は、適用可能なポリシーへのホストマシンの準拠を検査及び高める目的で繋げられる。
【課題を解決するための手段】
【０００９】
この概要は、詳細な説明において下記でさらに説明される簡略化された形式における概念の選択を紹介するために提供される。この概要は、請求された主題の主要な特徴又は重要な特徴を特定することを意図せず、特許請求された主題の範囲を判定する助けとして使用されることも意図していない。
【図面の簡単な説明】
【００１０】
【図１】ホストマシン上で操作可能な仮想化の構造を示す図である。
【図２】ゲストマシンがネットワークへの接続を有するホストマシン上で操作可能である仮想化環境を示す図である。
【図３】ゲストマシン及びホストマシン上で操作可能なコンポーネントを示す図である。
【図４】ホストマシンのヘルスがゲストマシンの起動で検査される第１の例示的な用途シナリオのフローチャートを示す図である。
【図５】ホストマシンのヘルスが定期的に検査される第２の例示的な用途シナリオのフローチャートを示す図である。
【図６】チャネルが複数のエンドポイント間で共有されるセキュリティ評価を可能にするために提供される例示的ＥＳＡＳを示す図である。
【図７】セキュリティ評価が適用可能なポリシーでホストマシンの準拠の検査を引き起こすために使用される例示的シナリオを示す図である。
【発明を実施するための形態】
【００１１】
図面において同様の参照番号は同様の要素を示している。
【００１２】
仮想化は、多くの方法で今日コンピューティングを劇的に変えている破壊的技術である。例えば仮想化は、ユーザー（つまり消費者企業の従業員等の又はビジネスユーザー）が、彼らのデスクトップＰＣ(Personal Computer)から離れるとき、彼ら自身のラップトップコンピューターを運ばなければならないのを回避することを可能にする。代わりに、彼らは、ＵＳＢ(Universal Serial Bus)ドライブ等の携帯できるストレージデバイス上に彼らのデスクトップの画像を運ぶことができ、家のＰＣ、ホテルのキオスク、空港、図書館又はサイバーカフェで公然にアクセス可能なＰＣ、友人の家のコンピューター等の任意のホストコンピューター上の仮想のゲストとしてデスクトップを実行することができる。
【００１３】
ホスト及び１以上のゲストマシンのオペレーティングシステムが実行するパーティションと呼ばれる隔離した複数の論理ユニットを作成することにより、ＰＣ等のホストマシン１００上で仮想化環境をセットアップすることができる。図１に示すように、仮想化環境１０２は、ゲストマシンをサポートする１以上の子パーティション$１１０_{1 \cdots N}$を作成するために使用される可能性のあるルートパーティション１０６を通常含む。いくつかの場合において、子パーティションはそれ自身の更なる子パーティションを発生させることも可能である。ルートパーティション１０６は、ホストマシンについてのオペレーティングシステムを含み、中央処理装置、メモリー及び他のハードウェアリソースを含むホストのハードウェアへの直接のアクセスを有する。
【００１４】

仮想化のソフトウェアレイヤー１１６は、パーティション及びホストマシン上のハードウェア１２０間で編成される。この例において、仮想化ソフトウェアは、パーティション間の通信をサポートするこのレイヤー１１６における論理チャネル上で子パーティション１１０にハードウェア１２０の仮想のビューを見せるハイパーバイザーを含む。ゲストマシンから仮想ハードウェアへの要求は、論理チャネル上で親又はルートパーティションに向けられる。ルートパーティションはその後、要求を管理し、チャネル上に応答を返すことになる。要求及び応答処理の全体は、ゲストマシン上で実行しているオペレーティングシステムに完全に明白である。

【００１５】

仮想化がうまく実行し、かなりの柔軟性及び経済価値を提供する一方で、ホストマシンがウイルス、トロイの木馬、キーロガー等のマルウェアで感染されるとき、潜在的なセキュリティの脅威が存在する。ゲストマシンが子パーティション１１０上で開始されると、ホスト上のマルウェアは、ゲスト上のデーターを盗む又は改ざんする機会を提供される可能性がある。さらに、ゲストマシンがリモートの企業ネットワーク等のネットワークへアクセスするために使用される場合、マルウェアはゲストマシンを介してネットワーク上のリソース及びデーターへの不正アクセスを獲得する可能性がある。

【００１６】

ＮＡＰ／ＮＡＣ(Network Access Protection/Control)等のセキュリティソリューションが、所与の準拠ポリシーに適合することを検証することにより、ゲストマシンのヘルスを検査するために利用可能である。例えば、ポリシーは、ゲストマシンが最近のセキュリティパッチで十分にアップデートされていて現在の署名に最新で、実行しているアンチウイルス又はアンチマルウェアのソフトウェアプログラムを有し、適切に構成されているソフトウェアのファイヤーウォールを有すこと等を指定する可能性がある。しかし、現在のソリューションは、ゲストマシンのためだけの準拠の検査を実行し、ホストマシンのヘルスを無視する。従って、ゲストマシンが十分に準拠し健全であることを見つけられるときでさえ、現在のソリューションはホストマシン上に常駐される可能性のあるマルウェアへのゲストマシンの露出に対処しない。

【００１７】

図２は、感染したホストによる攻撃からゲストマシンを保護するための現在の編成が実施される可能性のある例示的な仮想化環境２００を示している。仮想のゲストマシン２０５は、リモートの会社のネットワーク２２３（コーポネット(corponet)）等のネットワークへの接続２１５を有するＰＣ等のホストマシン２１０上で操作可能である。ネットワーク接続２１５は、例えばＶＰＮ(Virtual Private Network)、ＳＳＬ(Secure Sockets Laer)ベースのＶＰＮ、ＶＰＮ over ＩＰＳｅｃ(Internet Protocol Security over VPN）、及び同様のものを含む様々なリモートのネットワーキングプロトコルのうちの１つを使用して実施することができる。代替として、ネットワーク接続２１５は、例えば、本出願の譲受人により所有され、その全体を本明細書に参照して組み込まれる「Globally Distributed Infrastructure for Secure Content Management」というタイトルで２００８年６月２９日に出願された米国特許出願番号12/164,078において説明されているように、グローバルＳＣＭ(Secure Content Management)インフラストラクチャーを使用して実施することができる。

【００１８】

コーポネット２２３におけるネットワーク接続２１５のエンドポイントは、下記で詳細に説明される準拠ポリシーサーバー２３０とともにポリシー施行ポイント２２６である。（図２におけるデーター２３４により集合的に特定される）企業リソース及びデーターは、コーポネット２２３において利用可能であり、窃盗及び悪意のある攻撃に対して保護することを所望するいくつかの権利財産、慎重に扱うべき及び／又は機密情報を通常含む。コーポネット２２３は、ビジネス又は企業の従業員のＩＴニーズをサポートするために要求される可能性のあるものとして、クライアントコンピューター、ワークステーション、ラップトップ、モバイルデバイス及び同様のもの（図示せず）等の他のデバイスをサポー

トするために通常編成される。他のデバイスは、コーポネット２２３でローカルに展開されるか又はいくつかの場合にコーポネットからリモートで展開されるかのいずれかの可能性がある。

【００１９】

エッジファイアウォール２３９は、インターネット２４２等のコーポネット及び外部ネットワーク間のトラフィックを監視するために設定されるコーポネット２２３における境界に配置される。電子メール及びウェブサーバー及びデーターベース等の外部リソース２４５はインターネット２４２上で通常アクセス可能である。

【００２０】

ユーザーは、示されるＵＳＢドライブ等のポータブルのストレージメディア２５３からホストマシン２１０へユーザーのデスクトップ画像２５０をロードすることにより、仮想化環境２００を作成する可能性がある。ポータブルのストレージメディア２５３はいくつかの場合において仮想化ソフトウェア１１６を含む可能性もある。デスクトップ画像２５０が子パーティションに転送されて仮想化ソフトウェアが操作可能であるとき、ゲストマシン２０５がホストマシン２１０上でインスタンス化され、ホスト上のデスクトップ、アプリケーション、データー、設定及び優先度を含んでいるユーザーのコンピューターを仮想化する。ゲストマシン２０５上で仮想化されるオブジェクト（つまりアプリケーション、データー等）の特別な混合は実装により変えることができ、全てのオブジェクトがそれぞれの実装により仮想化される必要はないことに留意する。

【００２１】

ホストマシン２１０はコーポネット２２３から通常リモートで位置付けられ、セキュリティ保護の観点からコーポネットの一方として密接に制御又は監視されないことの多い、キオスク、図書館等の公にアクセス可能なＰＣ、又は家ベースのコンピューターを含む可能性がある。その結果、（参照番号２５２により示される）マルウェアは、ゲストマシン２０５の侵害についての可能性を有するホストマシンに感染する可能性がある。

【００２２】

図３に示すように、ホストマシン２１０上のマルウェアの脅威を対処するために、ホストのヘルスエージェント３０５は、ホスト上で実行するように設定され、準拠ポリシー３０８へのホストの適合性を検査する。準拠ポリシー３０８は、いくつかの実装における子パーティション上で最初に初期化されるときにゲストマシン２０５上にローカルに格納される可能性があるか、又はその他における準拠ポリシーサーバー２３０（図２）から取り出される可能性がある。準拠ポリシー３０８はホストマシン２１０についての最小の受け入れ可能なヘルスの条件を通常指定することになる。このような条件は実装により変わるか、又はセキュリティ管理者により設定することが可能である。例えば、準拠ポリシー３０８は、ホストマシン２１０が最新のセキュリティアップデートでパッチをあてられ、アンチウイルス製品又はサービスにより保護することを指定することができる。単一のポリシーがこの例において例示的に使用される一方で、一部のアプリケーションにおいて、複数の準拠ポリシーが利用される可能性がある。

【００２３】

ホストのヘルスエージェント３０５及びローカルに格納された準拠ポリシーは、ポータブルのストレージメディア２５３（図２）に格納され、初期化の間、ホストマシン及びゲストマシンの各々に転送することができる。一部の実装において、ホストのヘルスエージェント３０５は、ホストマシン２１０上で実行する可能性があるか、さもなければ同様のＮＡＰ機能を含む可能性のある、ＮＡＰクライアント若しくは他のコンポーネント又はエージェントの一部として実装される可能性がある。

【００２４】

ホストのヘルスエージェント３０５は、例えばセキュリティパッチの状態（「状態」という用語は、最後のパッチが何か及びいつインストールされたかを意味する）、アンチウイルス及び／又はアンチマルウェアのソフトウェアの存在、ウイルス又はマルウェアの署名のアップデートの存在、ホストマシンがゲストマシンを実行するために認証されること

を示す（例えばホストマシンが企業又はコーポネットのＩＴ資産である）ための指定の証明書／ファイル／登録キーの存在、適切に設定されたソフトウェアのファイヤーウォールの存在等を含むホストマシンのヘルスを示す様々な要素を検査できる。ここに挙げられた要素は例示であることを意図し、特定の実装のニーズを満たすために要求される他の要素も利用することができることに留意する。

【００２５】

ホストのヘルスエージェント３０５はさらに、ゲストマシン２０５のコンポーネントである対応するゲストのヘルスエージェント３１２と通信するように構成される。特にホストのヘルスエージェント３０５は、ホストのヘルスエージェントが検査を実行した後に、ホストマシンのヘルスを示す準拠の宣言３２０を生成し得る。準拠の宣言３２０は、例えばゲストのヘルスエージェントからの要求に応答して、ゲストのヘルスエージェント３１２にホストのヘルスエージェント３０５により送ることができる。選択的に、ホストのヘルスエージェント３０５は、他のトリガー又は条件の発生で、若しくは所定の時刻に、自身の主導で準拠の宣言３２０を送信することができる。

【００２６】

ホストのヘルスエージェント３０５は、ゲストのヘルスエージェント３１２の代わりに、準拠ポリシーサーバー２３０（又はポリシー施行ポイント２２６）に準拠の宣言３２０を送るように構成することができる。この場合に、準拠ポリシーサーバー２３０は準拠の宣言３２０を確認することができる。ホストマシン２１０が適用可能なポリシーに準拠していることが発見される場合、準拠ポリシーサーバー２３０はホストのヘルスエージェント３０５に署名されたヘルスの証明書３２２を発行することができる。ホストのヘルスエージェント３０５は、ゲストのヘルスエージェント３１２からの要求を受け取るとき、署名されたヘルス証明書３２２をゲストのヘルスエージェントに送信することができる。

【００２７】

ゲストのヘルスエージェント３１２は、ゲストマシン２０５が操作し得る安全な仮想化環境が存在するかどうかを判定するために、ローカルに準拠の宣言３２０（又は署名されたヘルス証明書３２２）を使用することができる。さらにゲストマシン２０５は、外部ネットワーク又はコーポネット２２３（図２）にアクセスするとき、準拠の宣言３２０（又は署名されたヘルス証明書３２２）をポリシー施行ポイント２２６に転送することができる。これらの用途のそれぞれはさらに、下記の図４及び図５におけるフローチャートに示した用途シナリオにおいてさらに示している。フローチャートは、図２及び図３で示した要素を指し、添付のテキストで説明する。

【００２８】

図４は、ホストのヘルスエージェント３０５が、ホスト上のゲストマシン２０５の起動又は初期化処理におけるいくつかのポイントで、ホストマシン２１０のヘルスを検査する、第１の例示的な用途シナリオ４００のフローチャートを示している。例えば、図書館、キオスク又はサイバーカフェといった公共の場所に配置され得る未知のホストマシン上で、ユーザーがゲストマシンとしてデスクトップ画像２５０を開始することを試み度に、検査を行うことができる。ゲストのヘルスエージェント３１２が始動するポイントで（４１５）、ゲストマシン２０５がブート処理を開始するとき（参照番号４１０により参照される）、シナリオ４００は開始する。

【００２９】

ゲストのヘルスエージェント３１２は、ホストマシン２１０のヘルスを検査することをホストのヘルスエージェント３０５に要求して（４２０）、ホストのポリシー３０８への準拠を確かめることができる。上述したように、検査された特定の要素及びポリシー３０８により課された要件は実装により変えることができる。ホストのヘルスエージェント３０５は、要求に応答可能なようにヘルスの検査を実行し（４２５）、ゲストのヘルスエージェント３１２に準拠の宣言３２０を提供する（４３０）。上述したように代替として、ホストのヘルスエージェント３０５は、準拠ポリシーサーバー２３０に準拠の宣言３２０を提供し、ホストマシン２１０が適用可能なポリシーに準拠していると判定される場合に

、署名されたヘルスの証明書３２２を戻して受け取る。
【００３０】
ゲストのヘルスエージェント３１２は、ホストのヘルスエージェント３０５から受け取った準拠の宣言３２０を、準拠ポリシー３０８と比較する（４３５）。（判定ブロック４４０において）ホストマシン２１０が準拠していると判定される場合（又は署名されたヘルス証明書３２２が準拠していることを示す場合）、ゲストマシン２０５は結果を通してその起動処理を続けることが許可される（４４５）。これにより仮想化環境２００が作成されることが可能となるので、ユーザーのデスクトップ、アプリケーション、設定、優先、データー等の１以上がゲストマシン２０５上に提供される（４０６）。
【００３１】
ゲストのヘルスエージェントがホストマシン上に存在しないか、又は、ポリシー３０８に対する準拠の宣言３２０の比較が、ホストマシン２１０がポリシーに準拠しないことを示す場合、エラーメッセージは、ゲストマシン２０５上で実行しているユーザーインターフェースを介して表示されることがある（４５０）。エラーメッセージは、ホストマシン２１０の準拠していないことを示す詳細な通知を与えることができるので、ユーザーはホスト上の問題の修正を試みることができる。例えば、ホストマシン２１０が重要なセキュリティパッチを逃す場合、ユーザーは、ホストをポリシー３０８の準拠に持ち込むために、パッチのダウンロード及びインストールを行い得る。一度そのように修正されると、ゲストマシン２０５はブート処理（４５５）を続けることができるので、仮想化環境がユーザーのために作成される（４６０）
【００３２】
図５は、ホストのヘルスエージェント３０５がホストマシン２１０のヘルスを定期的に検査する第２の例示的な用途シナリオ５００のフローチャートを示している。この例において、ゲストマシン２０５がコーポネット２２３等の外部ネットワークにアクセスすることを試みるときに、この検査は実行される（５０５）。
【００３３】
ポリシー施行ポイント２２６は、ネットワーク接続２１５で上記試みを確認するとき、コーポネット２２３への接続が完了することとなる前に作成された準拠の宣言を要求する（５１０）。それに応じて、ゲストのヘルスエージェント３１２はホストのヘルスエージェント３０５から準拠の宣言３２０を要求し（５１５）、ホストのヘルスエージェントはホストマシン２１０のヘルス検査を実行し、これにより準拠の宣言を生成する（５２０）。上述したように、代替的に、ホストのヘルスエージェント３０５は、準拠ポリシーサーバー２３０に準拠の宣言３２０を提供し、ホストマシン２１０が適用可能なポリシーに準拠していると判定される場合に、署名されたヘルスの証明書３２２を戻して受け取ることができる。
【００３４】
ゲストのヘルスエージェント３１２は、ポリシー施行ポイント２２６に準拠の宣言３２０を転送する（５２５）。ポリシー施行ポイント２２６は適用可能な準拠ポリシーに対する宣言を比較する（５３０）。通常、適用可能なポリシーは準拠ポリシーサーバー２３０により提供されることになる。さらに、ローカルに格納されたポリシー３０８の場合において上述されたように、１又は複数のポリシーは、所与の実装におけるホストマシン２１０へ適用される可能性がある。（判定ブロック５３５において）ホストのヘルスエージェント３０５からの準拠の宣言は、ホストマシン２１０が適用可能なポリシーに準拠していることを示す場合（又は署名されたヘルスの証明書３２２が準拠していることを示す場合）、ポリシー施行ポイント２２６はゲストマシン２０６がコーポネット２２３へアクセスすることを許可する（５４０）。
【００３５】
ゲストのヘルスエージェントがホストマシン上に存在しておらず、又は、準拠ポリシーサーバー２３０により供給されるポリシーに対する準拠の宣言３２０の比較が、ホストマシン２１０がポリシーに準拠しないことを示す場合、ポリシー施行ポイント２２６はネッ

トワークアクセスを拒否し（５４５）、エラーメッセージがゲストマシン２０５上に実行しているユーザーインターフェースを介して表示される可能性がある（５５０）。エラーメッセージはホストマシン２１０の準拠していないことの詳細の通知を与えることができるので、ユーザーはホスト上の準拠の問題を修正することを試みることができる。例えばホストマシン２１０がホスト上で実行しているアンチウイルス製品についてのマルウェアの署名の最新のアップデートを逃す場合、ユーザーは署名のアップデートのダウンロード及びインストールを行うことができ、ホストを適用可能なポリシーの準拠に持ち込むことができる。そのように修正される場合、ゲストマシン２０５は、準拠施行ポイント２２６によりネットワークアクセスを許可されるので（５５５）、ゲストマシンにおけるユーザーはデーターストア２３４に書き込み及びデーターストア２３４から読み出し、及び／又はインターネットベースのリソース２４５にアクセスをすることができる。

【００３６】

ホストのヘルスエージェント３０５は他の環境の下でホストマシン２１０のヘルスを検査するために利用されることもある。例えば、仮想化環境の完全性が侵害される疑いのある場合、ゲストのヘルスエージェントは、適用可能なポリシーへの継続した準拠を検証及び／又は確認するために、ホストのヘルスエージェントからヘルスの宣言を要求することができる。一つの例示的な例において、ＥＳＡＳセキュリティモデル下のセキュリティ評価はこのような疑いを引き起こすために受け取られる可能性がある。

【００３７】

図６は、セキュリティ評価がエンドポイント６１０$_{1，2、…N}$と呼ばれる複数のセキュリティゲートウェイ間で共有されることを可能にするためにチャネル６０５が提供される例示的ＥＳＡＳ編成６００を示している。企業のネットワークセキュリティについてのＥＳＡＳベースのセキュリティモデルは、本出願の譲受人により所有され、その全体を本明細書に参照して組み込まれる「Enterprise Security Assessment Sharing」というタイトルで、２００７年3月１４日に出願された米国特許出願番号11/724,061において説明され、これは、セキュリティ事故の高められた検知を提供し、企業規模の閲覧を可能にし、セキュリティ事故への自動的な応答についての明白でかつ単純で一元化された企業規模の応答ポリシーをセキュリティ管理者が定義しかつ施行することを可能にする。

【００３８】

ＥＳＡＳは企業のセキュリティ環境においてエンドポイント間のセキュリティ関連情報を共有することを可能にするセキュリティ評価と呼ばれる意味抽象(semantic abstraction)に依存する。この例では、企業のセキュリティ環境は、コーポネット２２３（図２）もユーザーもマシンも含むことができ、例えばグローバルＳＣＭインフラストラクチャーを使用した分散編成を（ゲストマシン２０５及びホストマシン２１０を含んで）サポート又は包含する。

【００３９】

セキュリティ評価は、コンピューター、ユーザー、サービス、ウェブサイト、データー又は企業等、全体としての環境において興味のあるオブジェクトについて収拾される情報（つまりいくつかの状況におけるデーター）への広範囲の文脈上の意味(contextual meaning)のエンドポイントによる暫定的な割り当てとして定義される。セキュリティ評価は、環境におけるオブジェクトが検知された事故の重大度（例えば、低、中間、高、重要）とともに「侵害される(compromise)」又は「攻撃下」等の特定の評価カテゴリーになることを明らかにするために、エンドポイントについて簡潔な語彙を利用する。

【００４０】

セキュリティ評価は、いくつかの不確定さがあり、制限された時間の間は有効であるので、暫定的である。セキュリティ評価の暫定的な性質は、文脈上の意味の割り当てにおいてエンドポイントが有する信頼のレベルを表現する信用分野、及びセキュリティ評価が有効であると期待される時間期間のエンドポイントの見積もりを反映するＴＴＬ(time-to-live)分野である、構成要素のうちの２つにおいて反映される。従って例えば、１以上のセキュリティ事故のエンドポイントの現在の理解を考慮して、特定のマシンは重大度の危機

的なレベルでかつ中間の信用度、及び３０分のＴＴＬを有して侵害されることを明らかにするために、セキュリティ評価がエンドポイントにより使用される可能性がある。

【００４１】

様々なタイプのセキュリティ評価は、任意の所与の企業ネットワーク環境において利用することができる。これらは例えば、評価のカテゴリー及びオブジェクトタイプの様々な組み合わせを含み得る。

【００４２】

ＥＳＡＳは通常多くの利点を提供する。簡潔な語彙を有するセキュリティ評価を採用することにより、企業におけるデーター全体の複雑さは大幅に減らされ、意味のある情報のみがエンドポイント間で共有される。セキュリティ評価の使用により、中央の格納位置における大量の生のデーターを収集する必要性も取り除き、これにより非常に拡張性の高い企業セキュリティのソリューションを費用対効果ベースで構築することが可能になる。さらに、新しいエンドポイントはオンデマンドの拡張性でわかりやすく展開され得る。セキュリティ評価は、既存のエンドポイント内の任意の応答ポリシーを再設定する必要なく新しいエンドポイント及び既存のエンドポイント間で共有することができる。新しいエンドポイントは、既存のエンドポイントが既に理解された意味抽象を使用して、セキュリティ評価の新しいソースとして単に機能する。セキュリティ評価の利用により、企業規模のセキュリティポリシーは、各エンドポイントが企業内で作成することがあるセキュリティイベントの全てを理解することなく、非常にコンパクトで明白な方法論を使用して設置することも可能にし、その後、各イベントについてのそれぞれの動作を説明することを試みる。

【００４３】

ＥＳＡＳセキュリティモデル下において、企業ネットワークのユーザーは企業環境におけるＩＴアセットの利用を支配するセキュリティポリシーが課される。特に、セキュリティポリシーは通常、少なくとも一部でエンドポイント６１０により施行される。セキュリティポリシーは通常、ユーザーがどの情報にアクセスすることがあるか、どの種類の情報がアクセスされ得るか、及び、許容できかつ許容できない振る舞いがいつか、企業内の監査実務等を支配する。

【００４４】

例えばエンドポイント６１０は、企業内のセキュリティ関連データーの異なる部分に関して監視、評価及び動作を取るセキュリティ製品を含むことがある。例えば図６に示すように、コーポネット２２３は、エッジファイヤーフォール製品610_1、１以上の特化した事業用(line-of-business)のセキュリティゲートウェイ製品610_2、ホストのセキュリティ製品610_Nを含むセキュリティ製品の組み合わせを利用することがある。この特定の例示的な例では利用しない一方で、他のタイプのセキュリティ製品も、例えばビジネスセキュリティゲートウェイ、情報漏えい保護ゲートウェイ、ウェブアプリケーション保護製品を含むＮＩＤＳ(Network intrusion detection system)製品、ＵＴＭ(Unified Thread Management/Security Incident Management)製品、ＳＥＭ／ＳＩＭ(Security Event Management/Security Incident Management)製品、ＮＡＰ製品、並びに使用可能なヘルスの監視及び設定管理製品（例えばマイクロソフト社のウィンドウズ（登録商標）のアップデートのサービス）を含む特定の実装の必要性に依存して利用されることもある。

【００４５】

エッジファイヤーフォールはインターネットベースの脅威からコーポネット２２３を保護するために編成されるセキュリティ製品である一方で、アプリケーション及びデーターへのリモートアクセスをユーザーに提供する。例えばエッジファイヤーフォールはマイクロソフト社のＩＳＡ(Internet Security an Acceleration)（登録商標）サーバーにより具現化することができる。事業用のセキュリティ製品は、アンチウイルス及びアンチスパムの保護を提供するためにコーポネット２２３において使用される例えばマイクロソフト社のＥｘｃｈａｎｇｅ（登録商標）等の電子メールアプリケーションを含む様々な事業用のアプリケーションを保護する。ホストのセキュリティ製品の商業の例は、マイクロソフ

ト社のＴＭＧ(Threat Management Gateway)製品であり、企業のデスクトップ、ラップトップ及びサーバーオペレーティングシステムについて一元化されたマルウェアの保護を提供する。

【００４６】

最も典型的なＥＳＡＳの実装において、ＥＳＡＳ中央サーバー６１６と呼ばれる特化したエンドポイントも利用されることがある。ＥＳＡＳ中央サーバー６１６はセキュリティ評価チャネル６０５に接続され、全てのセキュリティ評価への登録、セキュリティ評価のロギング、及び環境におけるセキュリティ事故に応答してエンドポイント６１０によって取られるローカルの動作をもロギングすることにより、集中型の会計ポイントとして動作する。ＥＳＡＳ中央サーバー６１６は、エンドポイント６１０の全体及びそれぞれとして企業の歴史及び現在の状態の包括的なビューを管理者に提供する。セキュリティ評価の利用は、管理者が企業全体に渡って検知される事故への応答ポリシーをコンパクト及び効率的に設定することを可能にする。セキュリティ評価は、企業規模のセキュリティの応答ポリシーを定義するために、自然のアンカー(natural anchor)又は開始ポイントとして機能する。簡素化及び一貫した管理インターフェースは従って、企業全体に渡るセキュリティ評価の各タイプについて所望の応答を定義することができる。

【００４７】

エンドポイント６１０はさらに、この環境において動作するセキュリティ評価チャネル上にセキュリティ評価を発行すると同時に、他のエンドポイントにより発行される利用可能なセキュリティ評価のサブセットに登録するための機能を実現する。アクティブである（つまり評価がまだ有効であることを示すＴＴＬを有する）この環境において存在するセキュリティ評価は、このようなエンドピント６１０に自身のローカルに利用可能な情報を見るための新しい方法を与えるセキュリティコンテキストを提供するために機能する。

【００４８】

つまり、セキュリティコンテキストは、潜在的なセキュリティ事故の検知の質を大きく高めるために、エンドポイント６１０が様々な異なるソースから受け取られ、オブジェクトのタイプに渡るセキュリティ評価から証拠を結合又は相関することを可能にする。エンドポイント６１０はその後、応答ポリシーのセットに従って、セキュリティ評価のそれぞれのタイプについて（別のエンドポイントから受け取られたか又はエンドポイント自身により内部で生成されたかのいずれかである）、ローカルの動作又は応答が適切かに関しての判定を行う。事故の検知は、セキュリティコンテキストが、（ほとんどが任意のコンテキストの不足のために完全に不適切である）企業を通して大量の生のデーターを共有する負担なく、セキュリティ評価の形式で、企業規模の情報の分散された処理を可能にするので、効率的及び費用効果的の両方である。エンドポイント６１０はローカルの動作を促進したセキュリティ評価の期限切れの上で（つまり、セキュリティ評価がＴＴＬフィールドにおいて指定された有効期限を超える）、ローカルの動作をロールバックするようさらに編成される。

【００４９】

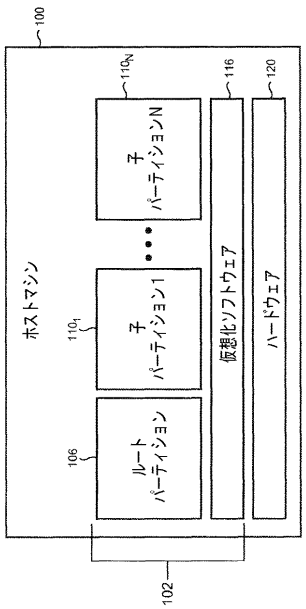
この例示的な例において、ゲストマシン２０５は、ホストマシン２１０を巻き込むセキュリティ事故を特定するセキュリティ評価チャネル６０５上で受け取られるセキュリティ評価への登録者としても構成される。従ってセキュリティ評価チャネル６０５は、例えばＶＰＮ／ＳＳＬ接続を通して又はグローバルＳＣＭアクセスを使用してゲストマシンに仮想的及び論理的に拡張される可能性がある。

【００５０】

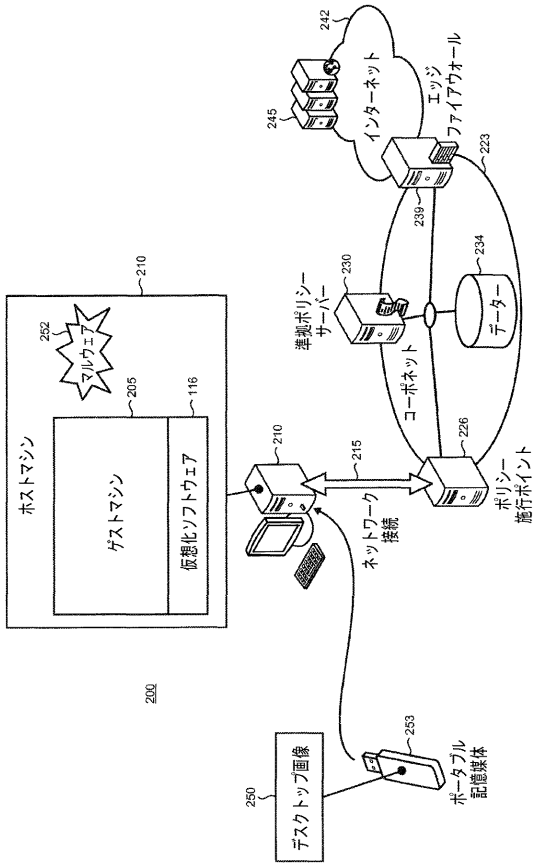
図７は、セキュリティ評価が適用可能なポリシーへのホストマシンの準拠の検査を引き起こすのに使用される例示的なシナリオ７００を示している。シナリオ７００は４つの段階で説明することができる。参照番号７１０により示すように、ホストが振る舞いについての最もありがちな説明がセキュリティ侵害の存在であるインターネット２４２にあまりに多くの接続を作成するので、エッジファイヤーフォール６１０$_1$は例えばホストマシン２１０が潜在的に侵害されることを最初に示す。

【００５１】
第２に、エッジファイヤーフォール６１０$_1$は、エンドポイント６１０に登録するためのセキュリティ評価チャネル６０５上に、参照番号７２０により示すようにホストマシンが高い重大性及び高い信用で「侵害」される疑いを示すセキュリティ評価を送る。第３に、ゲストマシン２０５はホストを巻き込むセキュリティ評価への登録者であるので、セキュリティ評価チャネル６０５上でセキュリティ評価７２０を受け取ることになる。セキュリティ評価７２０はホストマシン上のルートパーティションが悪意のある目的で接続を作るマルウェアを含む疑いを起こす。このような疑いが確認される場合、仮想化環境は不健全である可能性があり、ゲストマシン２０５は危険にさらされている可能性がある。従って、受け取られたセキュリティ評価７２０は、ホストマシン２１０のヘルスの検査を実行するためにホストのヘルスエージェント３０５に対してゲストのヘルスエージェント３１２からの要求を引き起こすために使用することができる。ホストのヘルスエージェント３０５は要求に応答可能なように検査を実行し、ゲストのヘルスエージェント３１２への結果を示すために準拠の宣言３２０を提供する。準拠の宣言３２０は問題を示し、その後ユーザーは通知される可能性があるので、修正を達成できる。
【００５２】
さらに、いくつかの実装において、セキュリティ評価７２０を受け取る登録エンドポイント６１０$_{1，2、…N}$及びＥＳＡＳ中央サーバー６１６は、動作を引き起こすための自身の相関ルール及びローカルに利用可能なデーターの適用を通して特定のセキュリティの見解を適用するのに使用することができる。エンドポイント６１０の動作はゲストマシン２０５上で実行でき、ホストマシン上で検知されるセキュリティ事故によりゲストが侵害されていたか否かを検査し、任意の侵害を修正及び／又は健全であるとして検証されるまでゲストマシンをコーポネット又は他のＩＴオブジェクトから隔離する。エンドポイント６１０によりとられる動作はホストマシン２１０に代替的に適用される可能性がある一方で、いくつかの実装においてゲストマシン２０５及びホストマシン２１０の両方が動作の目的である可能性がある。典型的に、取られる特定の動作及び適用されるＩＴオブジェクトは、コーポネット又は企業環境において設定及び実装される応答ポリシーに支配される。
【００５３】
図７における参照番号７４０により選択的に示されるように、受け取られたセキュリティ評価に応答してエンドポイント６１０により取られる動作は、オンデマンドのアンチウイルスのスキャンを実行するホストのセキュリティエンドポイント６１０$_N$を例示的に含む。さらに、示されるように、事業用のセキュリティエンドポイント６１０$_2$はインスタントメッセージ（ＩＭ）又は電子メールのトラフィックを一時的に中断することができる。ＥＳＡＳ中央サーバー６１６はセキュリティ分析者（例えば管理者）に警告を発し、セキュリティ評価及び呼び出された全ての動作のログも取る。これらの動作が例示として意図され、他のエンドポイントにより取られる他の動作が所与の実装及び用途シナリオの必要性を満たすために利用され得ることが強調される。
【００５４】
主題は、構造的な特徴及び／又は方法論的な動作のために特有の言語において説明したが、添付の特許請求の範囲に定義された主題は、上述の特有の特徴又は動作に限定される必要性はないと理解される。さらに、上述の特有の特徴及び動作は特許請求の範囲を実装するための例示的な形式として開示される。

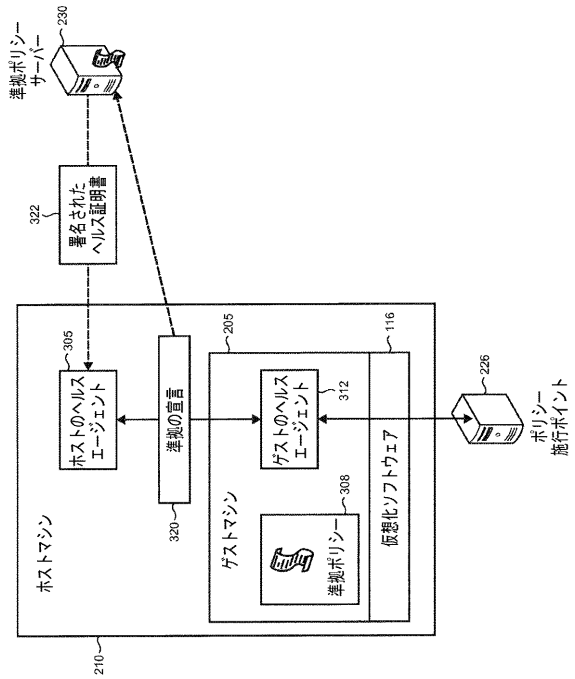
【図１】


100
ホストマシン
ルート
パーティション
106
子
パーティション1
110₁
子
パーティションN
110N
仮想化ソフトウェア
116
ハードウェア
120
102

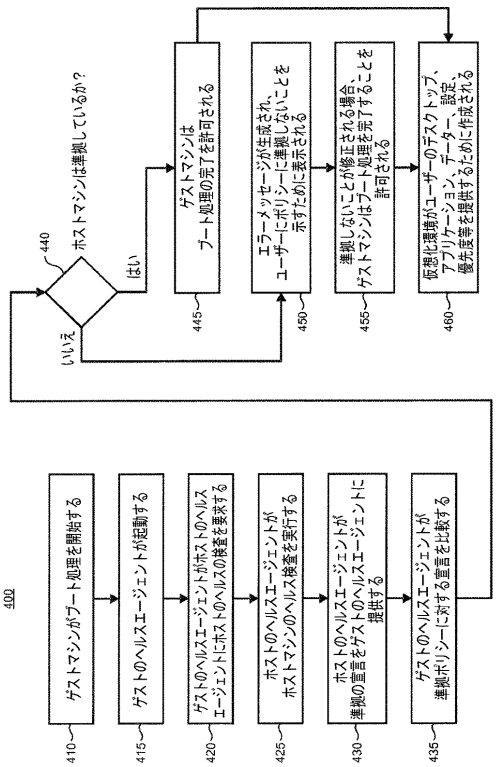
【図２】


242
インターネット
エッジ
ファイアウォール
223
245
239
234
データー
準拠ポリシー
サーバー
230
コーポネット
210
252
マルウェア
205
116
ホストマシン
ゲストマシン
仮想化ソフトウェア
215
226
ポリシー
施行ポイント
ネットワーク
接続
200
253
ポータブル
記憶媒体
250
デスクトップ画像

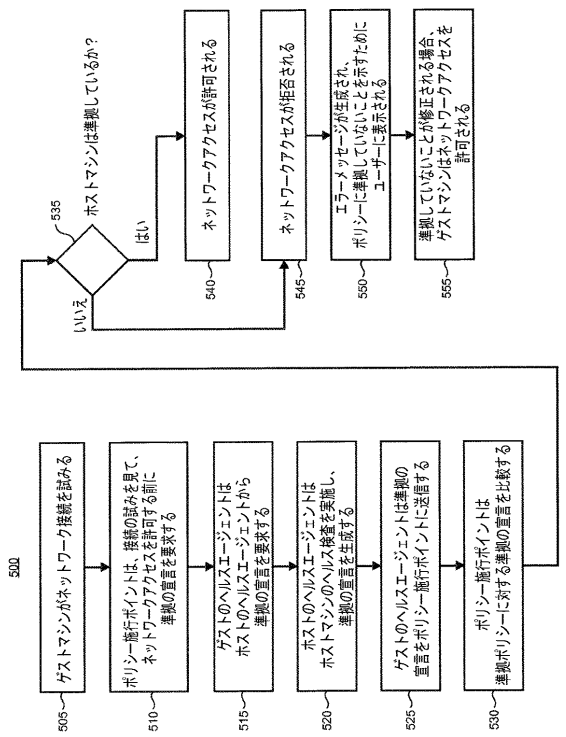
【図３】


準拠ポリシー
サーバー
230
署名された
ヘルス証明書
322
305
ホストのヘルス
エージェント
準拠の宣言
320
205
ゲストのヘルス
エージェント
312
116
ゲストマシン
準拠ポリシー
308
仮想化ソフトウェア
ホストマシン
210
226
ポリシー
施行ポイント

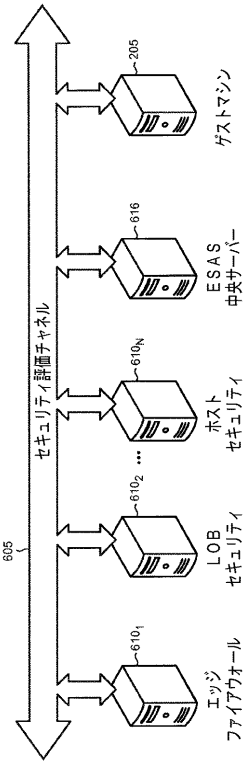
【図４】


400
ゲストマシンがブート処理を開始する
410
ゲストのヘルスエージェントが起動する
415
ゲストのヘルスエージェントがホストのヘルス
エージェントにホストのヘルスの検査を要求する
420
ホストのヘルスエージェントが
ホストマシンのヘルス検査を実行する
425
ホストのヘルスエージェントが
準拠の宣言をゲストのヘルスエージェントに
提供する
430
ゲストのヘルスエージェントが
準拠ポリシーに対する宣言を比較する
435
ホストマシンは準拠しているか？
440
はい
いいえ
ゲストマシンは
ブート処理の完了を許可される
445
エラーメッセージが生成され、
ユーザーにポリシーに準拠しないことを
示すために表示される
450
準拠しないことが修正される場合、
ゲストマシンはブート処理を完了することを
許可される
455
仮想化環境がユーザーのデスクトップ、
アプリケーション、データ、設定、
優先度等を提供するために作成される
460

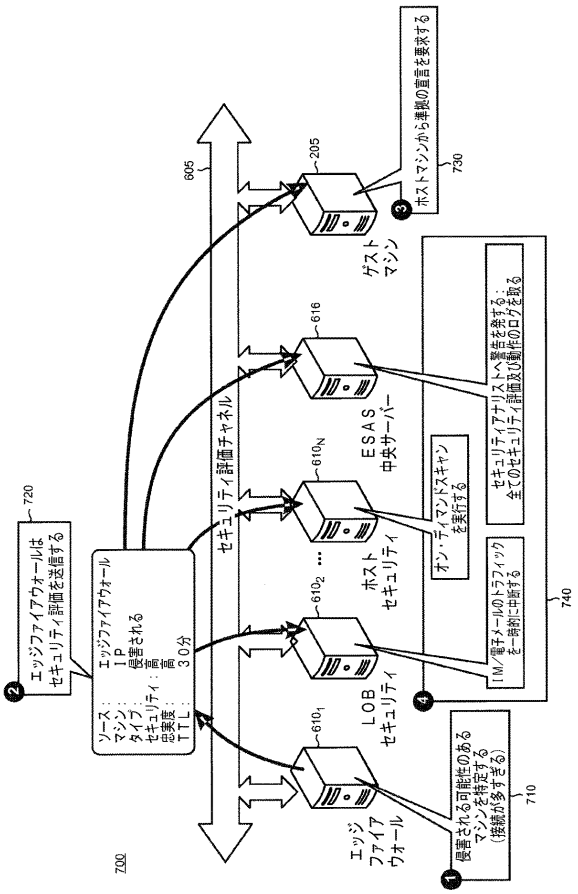
【図５】


500
ゲストマシンがネットワーク接続を試みる
505
ポリシー施行ポイントは、接続の試みを見て、ネットワークアクセスを許可する前に準拠の宣言を要求する
510
ゲストのヘルスエージェントはホストのヘルスエージェントから準拠の宣言を要求する
515
ホストのヘルスエージェントはホストマシンのヘルス検査を実施し、準拠の宣言を生成する
520
ゲストのヘルスエージェントは準拠の宣言をポリシー施行ポイントに送信する
525
ポリシー施行ポイントは準拠ポリシーに対する準拠の宣言を比較する
530
535
ホストマシンは準拠しているか？
はい
いいえ
ネットワークアクセスが許可される
540
ネットワークアクセスが拒否される
545
エラーメッセージが生成され、ポリシーに準拠していないことを示すためにユーザーに表示される
550
準拠していないことが修正される場合、ゲストマシンはネットワークアクセスを許可される
555

【図６】


600
605
セキュリティ評価チャネル
610₁
エッジファイアウォール
610₂
LOBセキュリティ
610N
ホストセキュリティ
616
ESAS中央サーバー
205
ゲストマシン

【図７】


700
605
セキュリティ評価チャネル
710
侵害される可能性のあるマシンを特定する（接続が多すぎる）
1
エッジファイアウォール
エッジファイアウォールはセキュリティ評価を送信する
2
720
ソース：
マシン：
IP
タイプ：
侵害される
セキュリティ：
宣言：
信頼度：
TTL：
30分
610₁
LOBセキュリティ
610₂
610N
ホストセキュリティ
616
ESAS中央サーバー
205
ゲストマシン
ホストマシンから準拠の宣言を要求する
3
730
オン・ディマンドスキャンを実行する
IM/電子メールのトラフィックを一時的に中断する
4
セキュリティアナリストへ警告を発する；全てのセキュリティ評価及び操作のログを取る
740

フロントページの続き

(74)代理人 100120112
弁理士 中西 基晴
(74)代理人 100147991
弁理士 鳥居 健一
(74)代理人 100119781
弁理士 中村 彰吾
(74)代理人 100162846
弁理士 大牧 綾子
(74)代理人 100173565
弁理士 末松 亮太
(74)代理人 100138759
弁理士 大房 直樹
(74)代理人 100091063
弁理士 田中 英夫
(72)発明者 ジョン ネイシュタット
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 エルシーエー－インターナショナル パテンツ内
(72)発明者 ノーム ベン－ヨチャナン
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 エルシーエー－インターナショナル パテンツ内
(72)発明者 ニーウ ニース
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 エルシーエー－インターナショナル パテンツ内

審査官 宮司 卓佳

(56)参考文献 国際公開第２００７／１３６１９２（WO，Ａ１）
国際公開第２００５／０９６１２１（WO，Ａ１）
特開２００７－２２６２７７（ＪＰ，Ａ）
特開２００８－１６５７９４（ＪＰ，Ａ）
国際公開第２００７／００７８０５（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／５６
Ｇ０６Ｆ ２１／５７