(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2006-166312
(P2006-166312A)
(43)公開日　平成18年6月22日(2006.6.22)

(51)Int.Cl.		F I		テーマコード（参考）
H04L 12/66	(2006.01)	H04L 12/66	B	5K030

審査請求 未請求　請求項の数 5　ＯＬ　（全 8 頁）

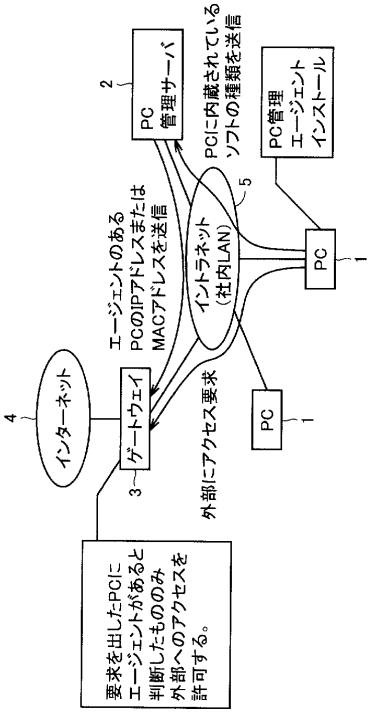
(21)出願番号　特願2004-358014 (P2004-358014)
(22)出願日　平成16年12月10日 (2004.12.10)

(71)出願人　000002130
住友電気工業株式会社
大阪府大阪市中央区北浜四丁目５番３３号
(74)代理人　100064746
弁理士　深見　久郎
(74)代理人　100085132
弁理士　森田　俊雄
(74)代理人　100083703
弁理士　仲村　義平
(74)代理人　100096781
弁理士　堀井　豊
(74)代理人　100098316
弁理士　野田　久登
(74)代理人　100109162
弁理士　酒井　將行

最終頁に続く

(54)【発明の名称】インターネットのアクセス制御方法

(57)【要約】
【課題】　ＰＣ管理エージェントが実装されていないＰＣからのインターネットへのアクセスを禁止するように制御するインターネットのアクセス制御方法を提供すること。
【解決手段】　ＰＣ１に実装されたＰＣ管理エージェントが、ＰＣ管理エージェントが実装されていることを示す情報をＰＣ管理サーバ２に送信する。ＰＣ管理サーバ２は、ＰＣ管理エージェントからその情報を受信したことを示す情報をゲートウェイ３に送信する。そして、ゲートウェイ３がＰＣ管理サーバ２からその情報を受信した場合、当該ＰＣからのインターネットへのアクセスを許可し、ＰＣ管理サーバ２からその情報を受信しない場合、当該ＰＣからのインターネットへのアクセスを禁止する。したがって、ＰＣ管理エージェントが実装されていないＰＣ１を容易に特定することができ、そのＰＣ１からのインターネット４へのアクセスを禁止することが可能となる。
【選択図】　図１



【特許請求の範囲】
【請求項１】
イントラネットに接続された複数のコンピュータおよび管理サーバと、前記イントラネットとインターネットとの間に設けられたゲートウェイとを含んだシステムにおけるインターネットのアクセス制御方法であって、
コンピュータに実装された管理エージェントが、該管理エージェントが実装されていることを示す第１の所定情報を前記管理サーバに送信するステップと、
前記管理サーバが前記管理エージェントから前記第１の所定情報を受信したことを示す第２の所定情報を前記ゲートウェイに送信するステップと、
前記ゲートウェイが前記管理サーバから前記第２の所定情報を受信した場合、当該コンピュータからの前記インターネットへのアクセスを許可し、前記管理サーバから前記第２の所定情報を受信しない場合、当該コンピュータからの前記インターネットへのアクセスを禁止するステップとを含む、インターネットのアクセス制御方法。
【請求項２】
前記第１の所定情報は、前記管理エージェントが実装されたコンピュータに実装されているソフトウェアに関する情報である、請求項１記載のインターネットのアクセス制御方法。
【請求項３】
前記第２の所定情報を前記ゲートウェイに送信するステップは、前記管理サーバが、設定されたインターネット利用可能条件を参照し、前記管理エージェントが実装されたコンピュータに実装されているソフトウェアに関する情報が前記インターネット利用可能条件を満たしている場合に、前記第２の所定情報を前記ゲートウェイに送信するステップを含む、請求項２記載のインターネットのアクセス制御方法。
【請求項４】
前記第２の所定情報は、コンピュータのインターネットプロトコルアドレスまたはメディアアクセスコントロールアドレスである、請求項１～３のいずれかに記載のインターネットのアクセス制御方法。
【請求項５】
イントラネットに接続された複数のコンピュータと、前記イントラネットとインターネットとの間に設けられたゲートウェイとを含んだシステムにおけるインターネットのアクセス制御方法であって、
前記ゲートウェイが、管理エージェントを実装したコンピュータからインターネットへのアクセスを受けた場合、当該アクセスを許可するステップと、
前記ゲートウェイが、管理エージェントを実装しないコンピュータからインターネットへのアクセスを受けた場合、当該アクセスを禁止するステップとを含む、インターネットのアクセス制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、社内ＬＡＮ（Local Area Network）などのイントラネットに接続されたパーソナルコンピュータ（以下、ＰＣと略す。）によるインターネットへのアクセスを制御する方法に関し、特に、ＰＣ管理エージェントがインストールされていないＰＣからのインターネットへのアクセスを禁止したインターネットのアクセス制御方法に関する。
【背景技術】
【０００２】
近年、インターネットが全世界的に普及し、多くの利用者がインターネットにアクセスするようになってきている。その一方で、インターネットに対する不正アクセスを防止するための技術が種々開発されている。これに関連する技術として、特開２００１－２９５５２１号公報および特開２００４－３０３７４号公報に開示された発明がある。
【０００３】

特開２００１－２９５５２１号公報に開示されたセキュリティガードキーシステムは、ライセンス情報を記憶する記憶部および通信手段を備えた鍵部と、鍵部と情報の授受を行う通信手段および鍵部の情報に基づいて特定のユーザに資源の使用権を付与するライセンス管理装置とを備えた鍵読み書き装置によって構成され、通信手段は、情報家電または家庭用情報ネットワークに対応する汎用の通信プロトコルを備えたものである。

【０００４】

また、特開２００４－３０３７４号公報に開示された情報処理装置は、ネットワークを介してユーザの装置に接続可能であり、或るコンテンツの要求の受信に応答して、ライセンス・ポリシーに従ってその或るコンテンツの送信に適用可能な少なくとも１つのセキュリティ方式の識別を送信し、そのコンテンツがその１つのセキュリティ方式で受信され得る場合に、その１つのセキュリティ方式でコンテンツを送信する。そして、ユーザの装置は、或るコンテンツの要求を送信し、コンテンツの受信および再生に利用可能な少なくとも１つのセキュリティ方式の識別を送信し、ライセンス・ポリシーに従ってその１つのセキュリティ方式で送信されたコンテンツを受信するものである。

【特許文献１】特開２００１－２９５５２１号公報

【特許文献２】特開２００４－３０３７４号公報

【発明の開示】

【発明が解決しようとする課題】

【０００５】

インターネットにアクセスするシステムの形態の１つとして、社内ＬＡＮなどのイントラネットに接続されたＰＣから、ＰＲＯＸＹサーバなどのゲートウェイを介してインターネットにアクセスするものを挙げることができる。

【０００６】

しかしながら、不正なプログラムがインストールされたＰＣが存在し、このＰＣがイントラネットに接続されている場合、このＰＣからのインターネットへのアクセスを防止することができないといった問題点があった。

【０００７】

また、上述した特開２００１－２９５５２１号公報および特開２００４－３０３７４号公報に開示された発明を用いても、このような問題点を解決することはできない。

【０００８】

本発明は、上記問題点を解決するためになされたものであり、その目的は、ＰＣ管理エージェントが実装されていないＰＣからのインターネットへのアクセスを禁止するように制御するインターネットのアクセス制御方法を提供することである。

【課題を解決するための手段】

【０００９】

本発明のある局面に従えば、イントラネットに接続された複数のコンピュータおよび管理サーバと、イントラネットとインターネットとの間に設けられたゲートウェイとを含んだシステムにおけるインターネットのアクセス制御方法であって、コンピュータに実装された管理エージェントが、管理エージェントが実装されていることを示す第１の所定情報を管理サーバに送信するステップと、管理サーバが管理エージェントから第１の所定情報を受信したことを示す第２の所定情報をゲートウェイに送信するステップと、ゲートウェイが管理サーバから第２の所定情報を受信した場合、当該コンピュータからのインターネットへのアクセスを許可し、管理サーバから第２の所定情報を受信しない場合、当該コンピュータからのインターネットへのアクセスを禁止するステップとを含む。

【００１０】

好ましくは、第１の所定情報は、管理エージェントが実装されたコンピュータに実装されているソフトウェアに関する情報である。

【００１１】

さらに好ましくは、第２の所定情報をゲートウェイに送信するステップは、管理サーバが、設定されたインターネット利用可能条件を参照し、管理エージェントが実装されたコ

ンピュータに実装されているソフトウェアに関する情報がインターネット利用可能条件を満たしている場合に、第２の所定情報をゲートウェイに送信するステップを含む。

【００１２】

好ましくは、第２の所定情報は、コンピュータのインターネットプロトコルアドレスまたはメディアアクセスコントロールアドレスである。

【００１３】

本発明の別の局面に従えば、イントラネットに接続された複数のコンピュータと、イントラネットとインターネットとの間に設けられたゲートウェイとを含んだシステムにおけるインターネットのアクセス制御方法であって、ゲートウェイが、管理エージェントを実装したコンピュータからインターネットへのアクセスを受けた場合、当該アクセスを許可するステップと、ゲートウェイが、管理エージェントを実装しないコンピュータからインターネットへのアクセスを受けた場合、当該アクセスを禁止するステップとを含む。

【発明の効果】

【００１４】

管理サーバが、管理エージェントが実装されていることを示す第１の所定情報を受信したことを示す第２の所定情報をゲートウェイに送信するので、ゲートウェイは第２の所定情報を参照することにより、管理エージェントが実装されていないコンピュータを特定することができ、そのコンピュータからのインターネットへのアクセスを禁止することが可能となった。

【００１５】

また、第１の所定情報は、管理エージェントが実装されたコンピュータに実装されているソフトウェアに関する情報であるので、管理サーバはこの情報をコンピュータから受信しているか否かによって、管理エージェントが実装されていないコンピュータを容易に特定することが可能となった。

【００１６】

また、管理サーバが、設定されたインターネット利用可能条件を参照し、管理エージェントが実装されたコンピュータに実装されているソフトウェアに関する情報がインターネット利用可能条件を満たしている場合に、第２の所定情報をゲートウェイに送信するので、インターネットへのアクセスを禁止するコンピュータの条件を細かく設定できるようになり、コンピュータの不正使用を効率的に防止することが可能となった。

【００１７】

また、第２の所定情報は、コンピュータのインターネットプロトコルアドレスまたはメディアアクセスコントロールアドレスであるので、インターネットへのアクセスを許可するコンピュータを容易に特定することが可能となった。

【発明を実施するための最良の形態】

【００１８】

図１は、本発明の実施の形態におけるシステムの概略構成を示すブロック図である。このシステムは、社内ＬＡＮなどのイントラネット５に接続された複数のＰＣ１と、イントラネット５に接続され、ＰＣ１から送信される情報を管理するＰＣ管理サーバ２と、ＰＣ１からのインターネット４へのアクセスを中継するＰＲＯＸＹサーバなどによって構成されるゲートウェイ３とを含む。

【００１９】

ＰＣ１に、ソフトウェアであるＰＣ管理エージェントがインストールされて起動されると、このＰＣ管理エージェントはＰＣ１に内蔵されているソフトウェアに関する情報などをＰＣ管理サーバ２に送信する。

【００２０】

ＰＣ管理サーバ２は、ＰＣ１から内蔵されているソフトウェアに関する情報を受信すると、そのＰＣ１にＰＣ管理エージェントがインストールされていると判断し、ＰＣ管理エージェントがインストールされているＰＣの識別情報、たとえばＩＰ（Internet Protocol）アドレス、ＭＡＣ（Media Access Control）アドレスなどをゲートウェイ３に送信す

る。
【００２１】
望ましくは、ゲートウェイ３からの要求に対してＰＣ管理サーバ２から所定の情報が送信される。
【００２２】
ゲートウェイ３は、ＰＣ管理サーバ２からＰＣ管理エージェントがインストールされているＰＣの識別情報を受信すると、ＰＣ１からインターネット４へのアクセスがあったときに、ＰＣ管理エージェントがインストールされているＰＣの識別情報を参照する。そして、ＰＣ管理エージェントがインストールされているＰＣからのアクセスを許可し、ＰＣ管理エージェントがインストールされていないＰＣからのアクセスを禁止する。
【００２３】
図２は、本発明の実施の形態におけるシステムのインターネットのアクセス制御方法を説明するためのフローチャートである。まず、ＰＣ１における処理手順を説明する。ＰＣ利用者がＰＣ１を介してゲートウェイ３に、利用者のＩＤ、パスワードなどの情報を登録することにより、ゲートウェイ使用登録を行なう（Ｓ１１）。
【００２４】
次に、ＰＣ利用者がＰＣ管理エージェントをＰＣ１にインストールする（Ｓ１２）。そして、ＰＣ管理エージェントが起動されると、ＰＣ利用者に基本情報を入力させる（Ｓ１３）。この基本情報には、ＰＣの保有部門、利用形態、ＰＣタイプ、使用者ＩＤ、利用者名、Ｅ－ｍａｉｌアドレスなどの情報が含まれる。
【００２５】
新規ソフトウェアが導入されると（Ｓ１４）、ＰＣ管理エージェントはＰＣ利用者に新規ソフトウェアのライセンス有無の入力を行なわせる（Ｓ１５）。
【００２６】
ＰＣ管理エージェントは、ＰＣ管理サーバ２からＰＩＮＧ送信を受信すると、ＰＩＮＧ応答を行なう（Ｓ１６）。このＰＩＮＧ応答には、ＩＰアドレス、ＭＡＣアドレスなどの情報が含まれる。そして、ＰＣ管理エージェントは、基本情報、ライセンス情報などの情報をＰＣ管理サーバ２に送信する（Ｓ１７）。このときＰＣ管理サーバ２に送信する情報として、ＰＣ１にインストールされているソフトウェアに関する情報も含まれる。
【００２７】
ＰＣ１からインターネット４へのアクセス要求を送信するとき（Ｓ１８）、後述するゲートウェイ３の処理によってインターネット４へのアクセスが禁止された場合は、ゲートウェイ３からアクセス禁止の通知を受ける。また、インターネット４へのアクセスが許可されると、ゲートウェイ３からインターネット４へのアクセス要求が送出される。
【００２８】
次に、ＰＣ管理サーバ２の処理手順について説明する。まず、ＰＣ管理サーバ２が起動されると、サーバの管理者にＰＣのインターネット利用可能条件を入力させる（Ｓ２１）。このインターネット利用可能条件には、たとえばインターネット４へのアクセスを禁止する条件である、ＰＣ管理エージェント未実装のＰＣ、ウィルス駆除ソフト未導入のＰＣ、ウィルス駆除ソフトが最新状態でないＰＣ、ＯＳが所定のものでないＰＣ、ＭＡＣアドレスが不正使用でないＰＣ、使用禁止ソフトを実装しているＰＣ、違法コピーソフトを導入しているＰＣなどの条件が含まれる。
【００２９】
次に、ＰＣ管理エージェントから受信したＰＣ情報を参照し、インターネット利用可能条件を満たすか否かを判定することによって、インターネット利用可能ＰＣを抽出する（Ｓ２２）。そして、一定周期でゲートウェイ３にこのインターネット利用可能ＰＣに関する情報を送信する（Ｓ２３）。このインターネット利用可能ＰＣに関する情報は、ＰＣのＩＰアドレス、ＭＡＣアドレスなどの情報である。
【００３０】
次に、ＰＣ管理サーバ２は、登録されている全ＩＰアドレスに対してＰＩＮＧを送信し

（Ｓ２４）、ＰＩＮＧ応答を受けて不正使用ＩＰを検出すると、不正使用テーブルを作成する（Ｓ２５）。そして、ＰＣ管理サーバ２は、ＰＣ管理エージェントから送信される情報を受信し（Ｓ２６）、これらの情報によってＰＣ情報を更新する（Ｓ２７）。そして、ステップＳ２２に戻って、以降の処理を繰返す。

【００３１】

次に、ゲートウェイ３における処理手順を説明する。まず、ゲートウェイ管理サーバは、管理者にＰＣ緊急対応テーブルを入力させる（Ｓ３１）。このＰＣ緊急対応テーブルとは、ＰＣ管理サーバ２の障害時でも利用者によるインターネット利用を確保するために設けられるものであり、チェック対象サブネット、チェック除外ＩＰアドレスなどの情報が格納される。ＰＣ管理サーバ２の障害時には、ゲートウェイ管理サーバはＰＣ緊急対応テーブルを参照して、ゲートウェイサーバに利用者テーブルおよびＰＣテーブルの情報を送信する。

【００３２】

ゲートウェイ管理サーバは、ＰＣ１によるゲートウェイ使用登録があると、ＰＣ１から利用者の情報を受信し、利用者テーブルを更新する（Ｓ３２）。

【００３３】

また、ゲートウェイ管理サーバは、ＰＣ管理サーバ２からインターネット利用可能ＰＣに関する情報を受信すると（Ｓ３３）、その情報によってＰＣテーブルを更新する（Ｓ３４）。そして、一定間隔で利用者テーブルおよびＰＣテーブルの情報をゲートウェイサーバに送信する（Ｓ３５）。

【００３４】

ゲートウェイサーバは、ゲートウェイ管理サーバから利用者テーブルおよびＰＣテーブルの情報を受信する（Ｓ３６）。そして、ＰＣ１からインターネット４へのアクセス要求があると、利用者テーブルの内容を参照して、そのアクセスが許可された利用者のものであるか否かを判定する（Ｓ３７）。許可された利用者でなければ（Ｓ３７，Ｎｏ）、インターネット４へのアクセスがあったＰＣ１に対してアクセス禁止を通知する（Ｓ３８）。

【００３５】

また、許可された利用者であれば（Ｓ３７，Ｙｅｓ）、ＰＣテーブルを参照して、そのアクセスに含まれるＩＰアドレスまたはＭＡＣアドレスがＰＣテーブルに含まれる情報と一致するか否かを判定して、そのアクセスが許可されたＰＣからのものであるか否かを判定する（Ｓ３９）。許可されたＰＣでなければ（Ｓ３９，Ｎｏ）、インターネット４へのアクセスがあったＰＣ１に対してアクセス禁止を通知する（Ｓ４０）。また、許可されたＰＣであれば（Ｓ３９，Ｙｅｓ）、インターネット４へのアクセスを許可し（Ｓ４１）、アクセス要求をインターネット４へ送出する。

【００３６】

以上説明したように、本実施の形態におけるインターネットのアクセス制御方法によれば、ＰＣ管理サーバは、ＰＣ管理エージェントがインストールされていないＰＣから所定の情報を受信しないので、そのＰＣがインターネット利用可能ＰＣから除外される。したがって、そのＰＣからインターネット４に対するアクセスがあった場合でも、そのアクセスが禁止されることになる。

【００３７】

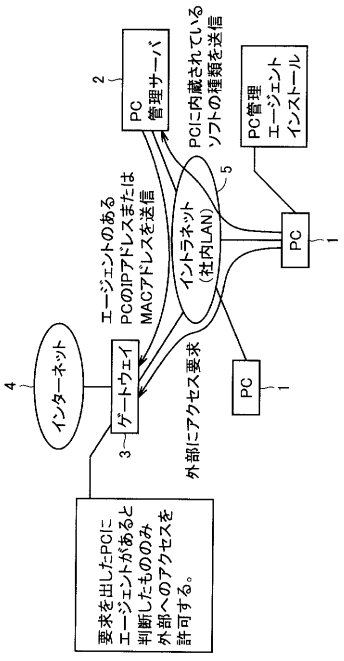
一般に、会社などからの指示に従っていないＰＣ利用者は、不正使用を検出するソフトウェアの導入を拒む傾向にある。しかしながら、本実施の形態においては、ＰＣ管理エージェントがインストールされてない場合には、そのＰＣからのインターネットへのアクセスが禁止されるので、ＰＣ利用者は業務に支障をきたすことになり、ＰＣ管理エージェントの実装を徹底させることが可能となった。

【００３８】

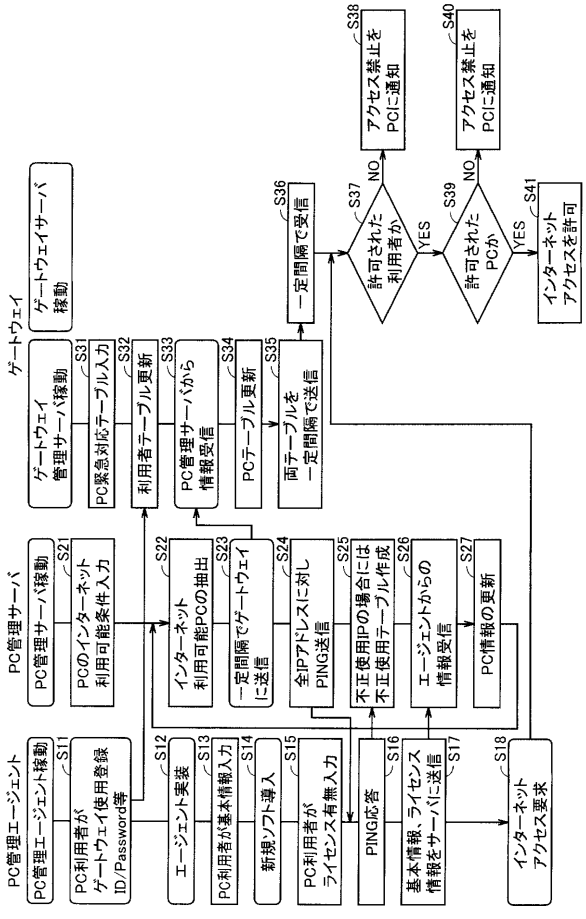
また、ＰＣ管理サーバ２にインターネット利用可能条件を入力するようにしたので、インターネット４へのアクセスを禁止するＰＣの条件を細かく設定できるようになり、ＰＣの不正使用を効率的に防止することが可能となった。

【００３９】
今回開示された実施の形態は、すべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。
【図面の簡単な説明】
【００４０】
【図１】本発明の実施の形態におけるシステムの概略構成を示すブロック図である。
【図２】本発明の実施の形態におけるシステムのインターネットのアクセス制御方法を説明するためのフローチャートである。
【符号の説明】
【００４１】
１　ＰＣ、２　ＰＣ管理サーバ、３　ゲートウェイ、４　インターネット、５　イントラネット。

【図１】



【図２】



フロントページの続き

(72)発明者　大釜　秀作
大阪市此花区島屋一丁目１番３号　住友電気工業株式会社大阪製作所内
(72)発明者　佐々木　利夫
大阪市此花区島屋一丁目１番３号　住友電気工業株式会社大阪製作所内

Ｆターム(参考) 5K030 GA15　HA08　HC01　HC14　HD03　JA07　JA11　LC13　LD20