

【特許請求の範囲】**【請求項 1】**

セキュリティ関連ファイルを保持するセキュリティサーバと接続可能な端末装置であって、

前記セキュリティサーバにアクセスし、セキュリティ関連ファイルの更新要否を確認する確認処理部と、

前記セキュリティ関連ファイルの更新要否の確認の結果、前記セキュリティ関連ファイルの更新が必要である場合には、前記セキュリティサーバに対し、セキュリティ関連ファイルの更新のためのダウンロード手続を開始するとともに、少なくとも前記ダウンロードが完了するまで、他の情報処理装置へのデータ送受信を禁止化する通信制御部と、を備えること、

を特徴とする端末装置。

【請求項 2】

請求項 1 に記載の端末装置において、

前記通信制御部は、前記セキュリティサーバへのアクセスと、所定のローカルエリアネットワークへのアクセスとを択一的に許可すること、

を特徴とする端末装置。

【請求項 3】

請求項 1 又は 2 に記載の端末装置において、

前記通信制御部は、前記所定のローカルエリアネットワークとの間に V P N (V i r t u a l P r i v a t e N e t w o r k) を構成可能な場合に、前記所定のローカルエリアネットワークに限ってアクセスを許可し、他のネットワークへのアクセスを禁止すること、

を特徴とする端末装置。

【請求項 4】

請求項 1 乃至 3 いずれかに記載の端末装置において、

前記セキュリティ関連ファイルは、コンピュータウイルスの感染検査に用いるためのウイルス定義ファイルであること、

を特徴とする端末装置。

【請求項 5】

セキュリティ関連ファイルを保持するセキュリティサーバと接続可能な端末装置における通信制御方法であって、

他の端末へのデータ送受信操作が行われた場合に、前記端末装置が、前記セキュリティサーバにアクセスし、セキュリティ関連ファイルの更新要否を確認し、

前記セキュリティ関連ファイルの更新が必要である場合には、前記端末装置は、前記セキュリティサーバに対し、セキュリティ関連ファイルの更新のためのダウンロード手続を開始するとともに、少なくとも前記ダウンロードが完了するまで、他の情報処理装置へのデータ送受信を禁止化し、

前記セキュリティ関連ファイルの更新が不要である場合には、前記データ送受信操作に応じた通信処理を実行すること、

を特徴とする通信制御方法。

【請求項 6】

請求項 5 に記載の通信制御方法において、

前記端末装置のアクセス先は、前記セキュリティサーバと所定のローカルエリアネットワークのいずれかを択一的に選択可能に制限されていること、

を特徴とする通信制御方法。

【請求項 7】

請求項 5 又は 6 に記載の通信制御方法において、

前記端末装置は、所定のローカルエリアネットワークとの間に V P N (V i r t u a l P r i v a t e N e t w o r k) を構成可能な場合に限り、前記所定のローカルエリ

10

20

30

40

50

アネットワークに限りアクセスできるよう制限されていること、
を特徴とする通信制御方法。

【請求項 8】

請求項 5 乃至 7 いずれかーに記載の通信制御方法において、
前記セキュリティ関連ファイルは、コンピュータウイルスの感染検査に用いるためのウイルス定義ファイルであること、
を特徴とする通信制御方法。

【請求項 9】

セキュリティ関連ファイルを保持するセキュリティサーバと接続可能な端末装置を構成するコンピュータにおいて、他の端末へのデータ送受信処理に先立って実行されるプログラムであって、

前記コンピュータをして、前記セキュリティサーバにアクセスさせ、セキュリティ関連ファイルの更新要否を確認する処理を行わせるとともに、

前記確認の結果、セキュリティ関連ファイルの更新が必要である場合には、前記コンピュータをして、前記セキュリティサーバに対し、セキュリティ関連ファイルの更新のためのダウンロードを実行させるとともに、少なくとも前記ダウンロードが完了するまで、他の情報処理装置へのデータ送受信を禁止化する処理を行わせ、

前記セキュリティ関連ファイルの更新が不要である場合には、前記コンピュータをして、前記データ送受信操作に応じた通信処理を行わせること、
を特徴とするプログラム。

10

20

【請求項 10】

セキュリティ関連ファイルを保持するセキュリティサーバと接続可能な端末装置を構成するコンピュータにおいて、他の端末へのデータ送受信処理に先立って実行されるプログラムであって、

前記コンピュータをして、前記セキュリティサーバにアクセスさせ、セキュリティ関連ファイルの更新要否を確認する処理を行わせるとともに、

前記確認の結果、セキュリティ関連ファイルの更新が必要である場合には、前記コンピュータをして、前記セキュリティサーバに対し、セキュリティ関連ファイルの更新のためのダウンロード手続を開始させるとともに、少なくとも前記ダウンロードが完了するまで、他の情報処理装置へのデータ送受信を禁止化する処理を行わせ、

前記セキュリティ関連ファイルの更新が不要である場合には、前記コンピュータをして、前記データ送受信操作に応じた通信処理を行わせること、
を特徴とするプログラム。

30

【請求項 11】

請求項 9 に記載のプログラムにおいて、

前記コンピュータをして、前記セキュリティサーバへのアクセスと、所定のローカルエリアネットワークへのアクセスとを択一的に行わせること、
を特徴とするプログラム。

【請求項 12】

請求項 9 又は 10 に記載のプログラムにおいて、

前記所定のローカルエリアネットワークとの間に VPN (Virtual Private Network) を構成可能な場合に限り、前記所定のローカルエリアネットワークに限りアクセスできるよう制限すること、
を特徴とするプログラム。

40

【請求項 13】

請求項 9 乃至 11 いずれかーに記載のプログラムにおいて、

前記セキュリティ関連ファイルは、コンピュータウイルスの感染検査に用いるためのウイルス定義ファイルであること、
を特徴とするプログラム。

【発明の詳細な説明】

50

【技術分野】

【0001】

本発明は、端末装置、通信制御方法、及び、プログラムに関し、特に、システムのセキュリティを維持する上で重要なセキュリティ関連ファイルの更新状況に応じて、端末装置からのデータ送受信を制限する技術に関する。

【背景技術】

【0002】

ウイルス定義ファイルや各種プログラム（各種通信プログラム、オペレーティングシステムを含む。以下、これらをセキュリティ関連ファイルという）の更新の可否をチェックして、ユーザに知らせることが行われているが、基本的には、ユーザ自身の判断に委ねられているのが現状である。例えば、ワクチンソフトの提供方法に関するものであるが、特開2002-259150号公報には、ワクチンソフトの提供を望む利用者のワクチンソフト関連情報を得ておき、新種のウイルスに対応した最新ワクチンソフトが提供され次第、速やかに当該利用者の端末に最新ワクチンソフトを送信可能とした保守サーバ装置が紹介されているが、これについても、ユーザが予め最新ワクチンソフトの送付を希望していることが条件となっていることに変わりはない。

【特許文献1】特開2002-259150号公報

【発明の開示】

【発明が解決しようとする課題】

【0003】

インターネットを介して自宅等から企業内LAN（Local Area Network）へアクセスする場合がある。この企業内LANに接続された各種の情報資源を保護する上で、より安全性を高めるには、こうした自宅等のパーソナル・コンピュータのセキュリティも確認しておく必要がある。しかしながら、上述のとおり、セキュリティ関連ファイルの更新の可否は、ユーザ自身の判断に委ねられており、セキュリティ教育によって解決せざるを得ないのが現状である。

【0004】

本発明は、上記事情に鑑みてなされたものであって、その目的とするところは、セキュリティ関連ファイルの更新の可否判定を自動化するとともに、セキュリティレベルの低い場合には、自動的に、他の情報処理装置へのデータの送受信やネットワークへのアクセスを回避させる端末装置、通信制御方法、及び、プログラムを提供することにある。

【課題を解決するための手段】

【0005】

前記課題を解決するための手段を提供する本発明の第1の視点によれば、セキュリティ関連ファイルを保持するセキュリティサーバと接続可能な端末装置であって、前記セキュリティサーバにアクセスし、セキュリティ関連ファイルの更新可否を確認する確認処理部と、前記セキュリティ関連ファイルの更新可否の確認の結果、前記セキュリティ関連ファイルの更新が必要である場合には、前記セキュリティサーバに対し、セキュリティ関連ファイルの更新のためのダウンロード手続を開始するとともに、少なくとも前記ダウンロードが完了するまで、他の情報処理装置へのデータ送受信を禁止化する通信制御部とを備える端末装置が提供される。

【0006】

前記セキュリティ関連ファイルは、更新を行わないことによって、システムに影響を及ぼしうるファイルやプログラムであれば、特に限定するものではないが、より端的に効果を奏効しうるものとして、コンピュータウイルスの感染検査に用いられるウイルス定義ファイルを挙げることができる。

【0007】

また、本発明の第2の視点によれば、上記端末装置を用いて行う通信制御方法、及び、上記端末装置に実装するプログラムが提供される。

【発明の効果】

【0008】

本発明によれば、ユーザのセキュリティ意識に関係なく、セキュリティの低い端末から他の情報処理装置へのアクセスを遮断し、ネットワークのセキュリティが低下してしまう事態を阻止することができる。

【発明を実施するための最良の形態】

【0009】

続いて、本発明のその好ましい実施の形態について図面を参照して詳細に説明する。図1は、本発明の一実施の形態に係る端末装置及びこの端末装置からアクセスしうる接続先を表した図である。図1を参照すると、端末装置1、インターネット2、ファイアウォール3、セキュリティサーバ4、企業名LAN5とが示されている。

10

【0010】

端末装置1は、パーソナル・コンピュータ、ワークステーション、PDA(Personal Digital Assistant)等の情報処理装置であり、セキュリティ関連ファイルの管理等を行うセキュリティ関連ファイル管理部11、通信制御部12を備えている。

【0011】

ファイアウォール(Fire Wall)3は、端末装置1の属するネットワークとインターネット2間における通信を制御する装置であり、例えば、企業内のLAN5にアクセスする場合にはVPN31を経由することを始めとする所定のセキュリティポリシーを適用する。また、ファイアウォール3は、セキュリティサーバ4へのアクセスを常時可能とするアクセスルートを有している。

20

【0012】

セキュリティサーバ4は、ワクチンソフト開発業者、通信事業者、ユーザ企業等によって運営管理されるサーバ装置であって、随時、ウイルス定義ファイル等のセキュリティ関連ファイルの更新を受け付け保持するとともに、少なくとも端末装置1からの照会に応じてセキュリティ関連ファイルのバージョン情報を応答する機能と、端末装置1からの求めに応じて最新のセキュリティ関連ファイルを送信する機能を有している。

【0013】

図2は、端末装置1の詳細構成を表したブロック図である。図2を参照すると、端末装置1のセキュリティ関連ファイル管理部11は、更新状態イニシャライズ部13、更新要否確認処理部14、更新処理部15とから構成されている。また、端末装置1は、図示しないそのメモリ装置に、ウイルス定義ファイル等のセキュリティ関連ファイルと、これらのセキュリティ関連ファイル群の更新状態を記憶保持している。また、通信制御部12は、前記セキュリティ関連ファイルの更新状態に応じて、IPアドレス等でそれぞれ特定されるセキュリティサーバ4への経路、企業内LAN5への経路、インターネットへの経路を択一的に切換えて通信を許可するよう動作する。

30

【0014】

図3は、セキュリティ関連ファイルの更新状態と、通信制御部12の切り替え動作の関係を表した図である。図中、セキュリティ関連ファイルの更新状態が未確認である状態とは、セキュリティ関連ファイルが最新版であることが確認されていない状態であり、セキュリティ関連ファイルの更新状態が最新更新状態である状態とは、セキュリティ関連ファイルが最新版であることを確認できた状態である。従って、予め定めるセキュリティ関連ファイルがいずれも最新版である場合は、通信制御部12は、ユーザの求めに従って、セキュリティサーバ4、企業内LAN5、インターネット2それぞれに接続を切り替える。一方、セキュリティ関連ファイルが最新版であることを確認できない場合は、通信制御部12は、セキュリティサーバ4への接続のみを許可することとなる。

40

【0015】

続いて、本実施の形態に係る端末装置1の動作について、図面を参照して詳細に説明する。図4は、本発明に係る端末装置において、接続要求がなされる度に実行される処理の流れを表したフローチャートである。図4を参照すると、まず、端末装置1は、更新状態

50

イニシャライズ部 13 を起動して、予め定めるセキュリティ関連ファイルの更新状態を「未確認」に初期化する（ステップ S001）。続いて、端末装置 1 は、更新要否確認処理部 14 を起動し、セキュリティサーバ 4 に接続を行って（ステップ S002）、当該セキュリティ関連ファイルの最新バージョン情報を取得する（ステップ S003）。

【0016】

続いて、端末装置 1 の更新要否確認処理部 14 は、端末装置 1 側の当該セキュリティ関連ファイルのバージョン情報を取得し、これらを照合する（ステップ S004、S005）。この結果、セキュリティ関連ファイルの更新が必要と判断した場合には（ステップ S005 の No）、端末装置 1 は、更新処理部 15 を起動して、当該セキュリティ関連ファイルの更新処理を行わせる（ステップ S007）。

10

【0017】

図 5 は、更新処理部 15 による、セキュリティ関連ファイルの更新処理の流れを表したフローチャートである。図 5 を参照すると、まず、更新処理部 15 は、セキュリティサーバ 4 から、最新版のセキュリティ関連ファイルをダウンロードする（ステップ S101）。ダウンロードが完了すると、更新処理部 15 は、当該セキュリティ関連ファイルをインストールするとともに当該セキュリティ関連ファイルの更新状態を書き換える（ステップ S102）。

【0018】

更に、上記各処理が完了すると、更新処理部 15 は、セキュリティ・プログラムを再起動し、セキュリティ関連ファイルを利用したウイルス感染検査やシステムチェックを実行する（ステップ S103）。

20

【0019】

再度図 4 に戻って説明を続けると、端末装置 1 は、セキュリティ関連ファイルの更新処理が不要であると判断した場合（ステップ S005 の Yes）、又は、セキュリティ関連ファイルの更新処理が正常に終了すると（ステップ S008 の Yes）、ユーザから求められた接続先への接続処理が開始される（ステップ S006）。

【0020】

一方、端末装置 1 は、ステップ S007 にてセキュリティ関連ファイルの更新に失敗した場合には、端末装置 1 の接続要求を拒否する（ステップ S008 の No）。

【0021】

図 6 は、接続処理の流れを表したフローチャートである。図 6 を参照すると、端末装置 1 は、セキュリティ関連ファイルの更新状態を参照し、図 3 に例示される更新状態と接続可能な接続先との関係から、接続可能な接続先が指定されている場合は、当該接続先のみへの経路を構成する。一方、接続可能な接続先が指定されていない場合は、端末装置 1 の接続要求を拒否する。

30

【0022】

以上、上記した実施の形態の説明からも明らかなとおり、本発明によれば、セキュリティ関連ファイルが更新されていないセキュリティの低い端末装置をして、ユーザの意思に拘わりなく、自動的に当該事実を検知させ、保護すべき企業内ネットワークへのアクセスを制限することができる。

40

【0023】

上記した実施の形態における、セキュリティ関連ファイルとしては、ウイルス定義ファイルを挙げることができるが、その他、更新を怠ることによってシステムに影響を及ぼしうるファイルやプログラムであれば、特に限定することなく適用しうるものであることは、本発明の原理からして明らかである。例えば、ウイルス感染有無を検知するウイルスチェッカープログラム、オペレーティングシステムや電子メール閲覧プログラム（メーラー）等の最新バージョンへの更新がなされていない場合などに、他の端末装置、サーバを含む各種情報処理装置へのデータ送受信やネットワークへのアクセスを制限することができる。

【0024】

50

また、上記した実施の形態では、端末装置 1 の属するネットワークにファイアウォール 3 を設けて企業内 LAN 5 への経路を制限することとしているが、本構成は、企業内 LAN 5 のセキュリティを向上させるための一手法に過ぎず、特に限定するものでないことは勿論である。

【0025】

また、上記した実施の形態では、セキュリティ関連ファイルの更新が必要である場合、端末装置の更新処理部が、自動的にセキュリティサーバ 4 から最新のセキュリティ関連ファイルをダウンロードし、インストールするものとして、その概要を説明したが、より確実なファイル更新を期す立場からすれば、更新処理部が、自動ダウンロードと自動インストールを行なうことが好ましいといえる。しかしながら、ユーザの意識向上を図るため、この手続に入る前、或いは、その手続の過程に、何らかのユーザの操作を介在させることも可能である。例えば、セキュリティ関連ファイルの更新が必要である場合、ダウンロード手続の開始確認ウインドウを表示し、ユーザの承認を得た上で、セキュリティ関連ファイルのダウンロードを開始するようにしてもよいし、セキュリティ関連ファイルのダウンロード後、その指示を得てからインストールを開始するようにしても良い。

10

【0026】

また、上記した実施の形態では、端末装置の通信制御部は、インターネットへの接続も許可することとしているが、よりセキュアな運用を行う観点からすれば、セキュリティ関連ファイルが最新のものであり、かつ、接続先となるローカルエリアネットワークとの間に VPN を構成可能な場合にのみ、特定のローカルエリアネットワークへのアクセスができるよう通信制御を行うようにしてもよい。このようにすれば、企業等が、社員等に対して端末装置を貸与し、自宅等から企業内のネットワークへの接続を認めるような運用を行う場合においても、VPN を介さない接続が行われて、盗聴、改ざんが行われたり、好ましくないソフトウェアが組み込まれる等の事態を防止することができる。

20

【0027】

また、上記した実施の形態では、図 3 に示されたとおり、セキュリティ関連ファイルの更新状態を最新のものであるか否かという 2 つの状態では、通信制御部 12 に切換え動作を行わせることとしているが、セキュリティ関連ファイルの更新日付により管理することも可能である。例えば、セキュリティ関連ファイルの更新日から一定期間を経過していない場合は、更新を要しないと判定させることが可能である。また同様に、セキュリティ関連ファイルのバージョン情報により管理することも可能である。例えば、端末装置 1 側のセキュリティ関連ファイルのバージョンと、最新バージョンとの間に重要な更新がなされていない場合等は、更新を要しないと判定させることが可能である。

30

【図面の簡単な説明】

【0028】

【図 1】本発明の一実施の形態に係る端末装置及びこの端末装置からアクセスしうる接続先を表した図である。

【図 2】本発明の一実施の形態に係る端末装置の構成を表したブロック図である。

【図 3】セキュリティ関連ファイル更新状態に応じたアクセス制御を説明するための図である。

40

【図 4】本発明の一実施の形態の動作を説明するための図である。

【図 5】本発明の一実施の形態の動作を説明するための図である。

【図 6】本発明の一実施の形態の動作を説明するための図である。

【符号の説明】

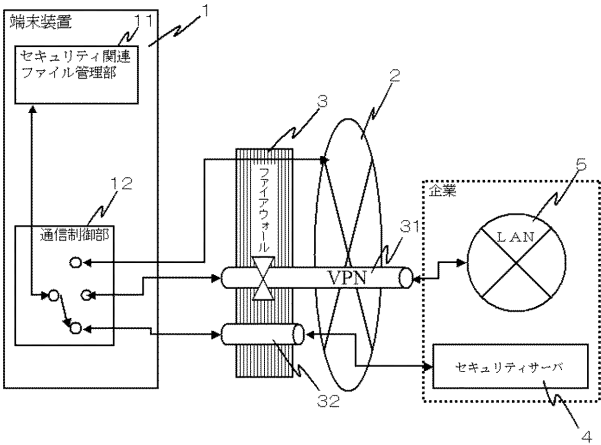
【0029】

- 1 端末装置
- 2 インターネット
- 3 ファイアウォール
- 4 セキュリティサーバ
- 5 企業名 LAN

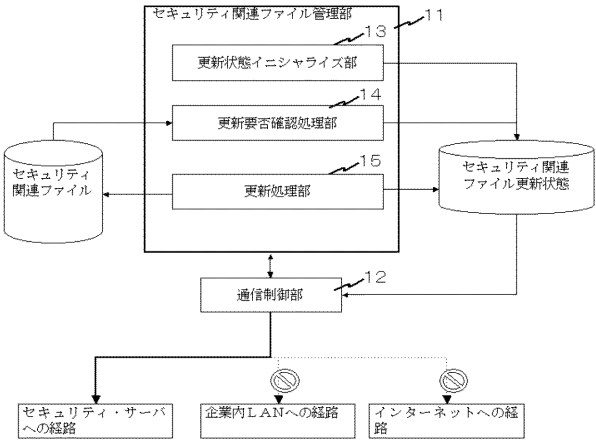
50

- 1 1 セキュリティ関連ファイル管理部
- 1 2 通信制御部
- 1 3 更新状態イニシャライズ部
- 1 4 更新要否確認処理部
- 1 5 更新処理部

【図 1】



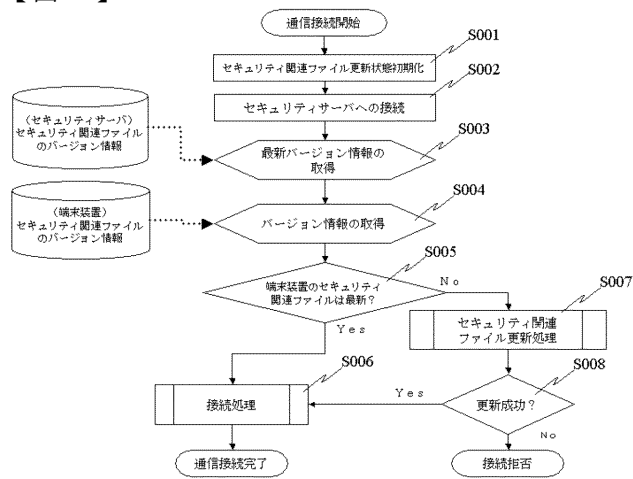
【図 2】



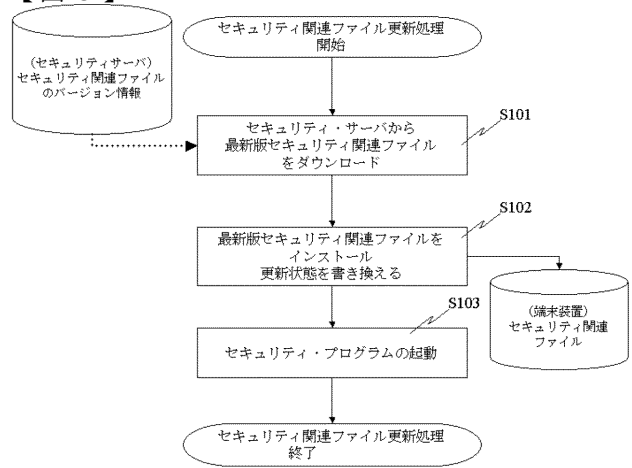
【図 3】

セキュリティ関連ファイル 更新状態	接続先		
	セキュリティ サーバ	企業内 LAN	インターネット
未確認	可	不可	不可
最新更新状態	可	可	可

【図 4】



【図 5】



【図 6】

