(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3995338号
(P3995338)
(45)発行日　平成19年10月24日(2007.10.24)　(24)登録日　平成19年8月10日(2007.8.10)

(51)Int.Cl.		F I		
G06F 13/00	(2006.01)	G06F	13/00	351Z
G06F 21/20	(2006.01)	G06F	15/00	330A
H04L 9/32	(2006.01)	H04L	9/00	675D
H04L 29/02	(2006.01)	H04L	13/00	301B

請求項の数 4　(全 15 頁)

(21)出願番号　特願平10-146200
(22)出願日　平成10年5月27日(1998.5.27)
(65)公開番号　特開平11-338799
(43)公開日　平成11年12月10日(1999.12.10)
審査請求日　平成15年12月19日(2003.12.19)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100074099
弁理士　大菅　義之
(74)代理人　100067987
弁理士　久木元　彰
(72)発明者　中川　　格
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　西ヶ谷　岳
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】ネットワーク接続制御方法及びシステム

(57)【特許請求の範囲】

【請求項１】

外部ネットワークとローカルエリアネットワークを相互に接続するネットワーク接続制御方法であって、

前記外部ネットワーク内のユーザによる前記ローカルエリアネットワークへのアクセス時に、該ユーザに対する認証チェックを実行し、

該認証チェックの結果に基づいて、前記ローカルエリアネットワーク内のリソースにアクセスするためのリソース要求を前記ユーザから受信し、

該リソース要求と前記認証チェックの結果に基づいて、該リソース要求によって要求されている前記ローカルエリアネットワーク内のリソースに対するアクセス権を算出し、

該算出されたアクセス権に基づいて前記リソースにアクセスする、

過程を含むネットワーク接続制御方法において、

前記アクセスされたリソースを、該リソース内のデータにアクセスするためのアクセスプログラムを含む移動コードとして、前記ユーザが操作するクライアント装置に送信し、

前記クライアント装置は、該移動コードを受信して実行することにより、前記リソース内のデータにアクセスする、

過程を含むことを特徴とするネットワーク接続制御方法。

【請求項２】

外部ネットワーク内のクライアント装置とローカルエリアネットワーク内のリソース提供サーバ装置とを相互に接続するネットワーク接続制御システムであって、前記外部ネッ

トワーク内のクライアント装置のユーザによる前記ローカルエリアネットワーク内のリソース提供サーバ装置へのアクセス時に、該ユーザに対する認証チェックを実行する認証チェックサーバ装置と、

該認証チェックの結果に基づいて、前記リソース提供サーバ装置が提供するリソースにアクセスするためのリソース要求を前記ユーザから受信し、該リソース要求と前記認証チェックの結果に基づいて、該リソース要求によって要求されている前記リソース提供サーバ装置が提供するリソースに対するアクセス権を算出し、前記リソース要求と前記アクセス権とを前記リソース提供サーバ装置に中継するリソース管理サーバ装置と、

を含むネットワーク接続制御システムにおいて、

前記リソース提供サーバ装置は、前記リソース要求されたリソースを、該リソース内のデータにアクセスするためのアクセスプログラムを含む移動コードとして生成して前記ユーザが操作するクライアント装置に送信し、

前記クライアント装置は、該移動コードを受信して実行することにより、前記リソース内のデータにアクセスする、

ことを特徴とするネットワーク接続制御システム。

【請求項３】

外部ネットワークとローカルエリアネットワークを相互に接続するネットワーク接続制御プロセスであって、

前記外部ネットワーク内のユーザによる前記ローカルエリアネットワークへのアクセス時に、該ユーザに対する認証チェックを実行し、

該認証チェックの結果に基づいて、前記ローカルエリアネットワーク内のリソースにアクセスするためのリソース要求を前記ユーザから受信し、

該リソース要求と前記認証チェックの結果に基いて、該リソース要求によって要求されている前記ローカルエリアネットワーク内のリソースに対するアクセス権を算出するプロセスをコンピュータに実行させるプログラムを格納する記録媒体において、

前記プロセスは、さらに前記リソース要求されたリソースを、該リソース内のデータにアクセスするためのアクセスプログラムを含む移動コードとして生成して前記ユーザが操作するクライアント装置に送信するものであることを特徴とする記録媒体。

【請求項４】

クライアントから個別サーバのリソースをアクセスする方法であって、前記クライアントは、前記アクセスされるべきリソースを該リソース内のデータと該データにアクセスするためのアクセスプログラムを含む暗号化された移動コードとして、前記個別サーバから受信して、これを実行することにより、前記リソースにアクセスすることを特徴とするリソースアクセス方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、インターネットとローカルエリアネットワーク（ＬＡＮ）を相互に接続し、インターネットからＬＡＮへのアクセスを許しつつ、ＬＡＮ内の資源を安全に保護するための、ファイアウォール技術に関する。

【０００２】

【従来の技術】

、

従来、ファイアウォールは、パケットフィルタリング方式、或いは、アプリケーションゲートウェイとしてのフィルタリング方式により実装されている。これらは、いずれも各サービス毎に、外部から内部へのアクセスを許可するか否かを決定するものである。

【０００３】

【発明が解決しようとする課題】

社内ＬＡＮがインターネットに接続される際に、外部からの不正な攻撃から社内リソースを守るためのファイアウォールでは、デフォルトでは全てのアクセスが禁止され、特定の

アクセスだけが個別に許可されるという方式が採用されている。
【０００４】
このため、サービスを第１基準、ユーザを第２基準としてフィルタリングする現在の方式では、ほとんどすべてのネットワークサービスが使用できなくなり、正当なユーザまでも快適なインターネットサービスを受けられないという不自由を強いられてきた。
【０００５】
一方、最近における社内ユーザの要望の多様化に対応して、それぞれの要求に応じてネットワーク上のサービスを社内外で利用できるようにしてゆくと、ファイアウォールにおいて多くのサービスのためのデータを通過させる結果となり、セキュリティの維持が困難になる。
【０００６】
更に、現在普及しつつあるリモートアクセスでは、認証チェックの後に社内ＬＡＮ上のマシンへのログインを許可するという形態が採用されているため、１回の攻撃で大きな被害を受ける可能性がある。
【０００７】
このように、従来の方式では、社外から社内リソースを利用できるサービスを増やすと、保護すべき社内リソースが危険にさらされる可能性が急激に増大してしまうという問題点を有していた。
【０００８】
本発明の課題は、フィルタリングの方式を変更することでファイアウォールの利便性を格段に向上させ、更に従来と同等のセキュリティレベルを確保することにある。
【０００９】
【課題を解決するための手段】
本発明は、外部ネットワーク（社外ネットワーク）とローカルエリアネットワーク（社内ネットワーク）を相互に接続するネットワーク接続制御方法を前提とする。
【００１０】
本発明ではまず、外部ネットワーク内のユーザ（クライアントマシン３０１上のユーザ）によるローカルエリアネットワークへのアクセス時に、そのユーザに対する認証チェックが実行される（認証チェックサーバ１０１）。
【００１１】
次に、その認証チェックの結果に基づいて、ローカルエリアネットワーク内のリソースにアクセスするためのリソース要求がユーザから受信される（リソース管理サーバ１０２）。
【００１２】
次に、そのリソース要求と認証チェックの結果に基づいて、そのリソース要求によって要求されているローカルエリアネットワーク内のリソースに対するアクセス権が算出される（リソース管理サーバ１０２）。
【００１３】
そして、その算出されたアクセス権に基づいてリソースへのアクセスが実行される（リソース管理サーバ１０２）。
ここで、アクセスされたリソースは、ユーザが操作するクライアント装置に移動コードとして送信され、クライアント装置は、その移動コードを受信して実行することにより、リソース内のデータにアクセスするように構成される。
【００１４】
【発明の実施の形態】
以下、図面を参照しながら、本発明の実施の形態について詳細に説明する。
＜本発明の実施の形態の特徴＞
本実施の形態は、ユーザを第１基準、サービスを第２基準としてフィルタリングを行うことにより、社員であればデフォルトで全てのアクセスが許可され、社外のユーザに対してはデフォルトで全てのアクセスが禁止される、というユーザ毎に別々のポリシーに従って

、社内リソースを外部からの攻撃から守り、社内ユーザの要望の多様化を満足させることができるという特徴を有する。

【００１５】

また、本実施の形態では、認証チェックの後に社内ネットワーク内のマシンにログインを許可するという従来の方式から、要求のあった社内リソースだけを外部に送信するという方式に変更することにより、１回の攻撃で生じ得る被害の規模を従来より小規模に抑えることができるという特徴を有する。

【００１６】

より具体的には、本実施の形態では、社内リソースとして、社内に届いた電子メールのようなテキスト情報やマルチメディア情報などと、開発中のシステムなどのアプリケーションプログラム・データなどとが区別されず、社内で所有されるアプリケーションなどが社内リソースの１つと位置づけされることにより、社外と社内にあるアプリケーションを連携させて動作させることも可能となる。

【００１７】

このように、本実施の形態では、フィルタリングの方式を変更することでファイアウォールの利便性を格段に向上させ、更にユーザの認証チェックと社内リソースへのアクセス制御を個別に行うことでセキュリティ機構を２重化し、従来と同等のセキュリティレベルを確保することが可能となる。

＜本発明の実施の形態の構成＞

図１は、本発明の実施の形態のシステム構成図である。

【００１８】

まず、社内ネットワーク内に設置される認証チェックサーバ１０１は、ｔｅｌｎｅｔ，ｆｔｐ，ｈｔｔｐ等の複数種類のサービス・リクエストを受信するためのサービス・リクエスト用ポートを少なくとも１つ有し、かつユーザの認証チェックを行う機構を有する。このサーバ１０１は、社外ネットワーク内のインターネットサービスプロバイダ（ＩＳＰ）１０４を介してインターネットに接続される。

【００１９】

社内ネットワーク内に設置されるリソース管理サーバ１０２は、社内ネットワーク内のリソースを管理する機能を有し、かつユーザの属性や信頼度に応じて、各社内リソースに対するアクセス権を制限する機構を有する。このサーバ１０２は、認証チェックサーバ１０１と接続される。

【００２０】

なお、リソース管理サーバ１０２と認証チェックサーバ１０１の接続は、図１に示されるように直接接続されてもよいし、図２に示されるようにパケットフィルタリングルータ２０１を介して接続されてもよい。

【００２１】

社内ネットワーク内に設置される個別サーバ１０３は、ｔｅｌｎｅｔ，ｆｔｐ，ｈｔｔｐ等の各種サービスを提供する。なお、このサーバ１０３は、リソース管理サーバ１０２と同一であってもよい。

＜本発明の実施の形態の動作原理＞

上述の実施の形態の構成の動作原理について、まず説明する。

【００２２】

認証チェックサーバ１０１には、ユーザＩＤ及び認証用パスワードが事前に登録される。認証チェックサーバ１０１にユーザＩＤが登録されていない場合には、そのユーザは社外ユーザとして認識される。

【００２３】

認証用パスワードには、公開鍵暗号方式で利用されるパスフレーズ又はいわゆる使い捨てパスワード等を採用でき、ユーザＩＤには、電子メールアドレスを採用することができる。

【００２４】

社内リソースにアクセスしたいユーザは、認証チェックサーバ１０１に接続し、それに対してサービス・リクエストと、ユーザＩＤ及び認証用パスワードを送信する。

【００２５】

サービス・リクエストを受け取った認証チェックサーバ１０１は、受信したユーザＩＤ及び認証用パスワードを、登録されているユーザＩＤ及び認証用パスワードと照合することにより、そのユーザの信頼度を算出する。

【００２６】

その後、認証チェックサーバ１０１は、クライアントマシンとの間に、リソース要求を受け付けるための準備としてポート（ソケット）を開ける。

クライアントマシンは、このポートに対して、使用したい社内リソースの論理名をリソース要求として送信する。このリソースの指定は、例えばＵＲＬ（ユニフォームト・リソース・ロケータ）形式を採る。

【００２７】

認証チェックサーバ１０１は、クライアントマシンから送られてきたリソース要求と、それに先だって算出している前述のユーザの信頼度とを、リソース管理サーバ１０２に送信する。

【００２８】

リソース管理サーバ１０２は、認証チェックサーバ１０１からリソース要求及びユーザの信頼度を受信すると、そのリソース要求に含まれる社内リソースの論理名から、その社内リソースを提供する個別サーバ１０３を見つける。更に、リソース管理サーバ１０２は、認証チェックサーバ１０１から受信したユーザの信頼度から、要求されている社内リソースに対するに対するアクセス権を決定し、個別サーバ１０３に対して、そのリソース要求とアクセス権を送信すると共に、要求されている社内リソースを提供するプログラムコード（移動コード）を要求する。

【００２９】

リソース管理サーバ１０２からリソース要求及びアクセス権と移動コードの要求とを受信した個別サーバ１０３は、要求された移動コードを生成し、その移動コード中に、リソース管理サーバ１０２から受け取ったアクセス権、クライアント識別コード、及びプログラムの生存期限（Expire Date ）等の個別設定を埋め込む。その後、個別サーバ１０３は、その移動コードをリソース管理サーバ１０２に返送する。

【００３０】

リソース管理サーバ１０２は、上記個別サーバ１０３から上記移動コードを受け取ると、それを認証チェックサーバ１０１に返送する。

認証チェックサーバ１０１は、リソース管理サーバ１０２から上記移動コードを受け取ると、上記リソース要求を送信したユーザの登録されているパスワード（公開鍵等）を用いてその移動コードを暗号化し、上記リソース要求を送信したクライアントマシンに返送する。

【００３１】

暗号化された移動コードを受け取ったクライアントマシンは、認証チェック時にユーザが認証チェックサーバ１０１に送信したパスフレーズを使用して、そのユーザの秘密鍵を取り出し、その秘密鍵を用いて上記暗号化された移動コードを復号し、その移動コードのプログラムを実行する。この結果、ユーザが要求した社内リソースが、クライアントマシン上に再現される。

【００３２】

クライアントマシン上に再現された社内リソースは、それ自身に埋め込まれているアクセス権とクライアント識別コードを参照することにより、そのアクセス権を超えるアクセス要求を制限する。

＜本発明の実施の形態の具体的動作＞

上述の動作原理に基づく本発明の実施の形態の具体的な動作について、図３～図６の動作説明図と、図７～図９のシーケンス図と、図１０～図１２のプログラム例に基づいて、以

下に順次説明する。

【００３３】

以下の説明においては、認証チェックサーバ１０１における認証チェックは公開鍵暗号方式に基づいて実行され、認証用パスワードにはパスフレーズが使用され、ユーザＩＤには電子メールアドレスが使用されることとする。

【００３４】

そして、認証チェックサーバ１０１は、各ユーザ情報として、そのユーザの電子メールアドレスと公開鍵とを対に持つ。

認証チェックサーバ１０１では、図３に示されるように、認証チェックのためのサーバプログラムであるゲートキーパ３０３が、認証チェック用ポート（ソケット）のみを常時開いている状態にある。どのようなネットワークサービスが利用される場合にも、まずこの認証チェック用ポートへの接続が実行され、認証チェックが行われる。ゲートキーパ３０３が上記ポートを開く際には、例えば図１１のステップ１に示されるプログラムコードが実行される。

【００３５】

ユーザは、クライアントマシン３０１上のクライアントアプリケーション３０２（図３）を実行して、社内ネットワーク内のネットワークサービスを要求する場合、まずクライアントマシン３０１から認証チェックサーバ１０１に認証チェック要求が発行される（図７のＳ１）。この場合、クライアントアプリケーション３０２では、例えば図１０のステップ１及び２に示されるプログラムコードが実行される。ステップ１では、認証チェックサーバ１０１が指定され、ステップ２では、その認証チェックサーバ１０１の認証チェック用ポートへの接続が実行される。

【００３６】

認証チェックサーバ１０１への接続に成功すると、ユーザは、クライアントマシン３０１上に表示されるウインドウを使って、ユーザＩＤと認証用パスワードを入力する。ユーザＩＤは、ユーザの電子メールアドレスであり、認証用パスワードは、公開鍵と秘密鍵を生成した際のパスフレーズである。

【００３７】

認証チェックサーバ１０１内のゲートキーパ３０３は、クライアントマシン３０１からユーザＩＤと認証用パスワードを受信すると、認証用パスワードをユーザの公開鍵を使って復号した後、まず受信したユーザＩＤが認証チェックサーバ１０１内の特には図示しないユーザデータベースに登録されているか否か、及び登録されている場合に受信した認証用パスワードが上記ユーザデータベース内の認証用パスワードと一致するか否かを認証チェックする（図７のＳ２）。この場合、ゲートキーパ３０３では、例えば図１１のステップ２及び３に示されるプログラムコードが実行される。ステップ２では、ユーザＩＤと認証用パスワードの受信処理が実行され、ステップ３では、認証チェック処理が実行される。

【００３８】

続いて、ゲートキーパ３０３は、上記認証チェック結果を使用して、上記ユーザデータベースを参照することにより、上記ユーザの信頼度を計算する（図７のＳ２）。この場合、ゲートキーパ３０３では、例えば図１１のステップ４に示されるプログラムコードが実行される。

【００３９】

ユーザＩＤであるユーザの電子メールアドレスが上記ユーザデータベースに登録されておりかつ認証用パスワードが正しい場合には、ユーザが多くのサービスを利用できるように、そのユーザに対して高い信頼度が与えられる。

【００４０】

ユーザＩＤが上記ユーザデータベースに登録されていない場合には、そのユーザは社外ユーザであるとみなされ、そのユーザに対して低い信頼度が与えられる。この場合には、社内ユーザへの電子メールの受付けなど、認証チェックの不要なサービスのみが提供される。

【００４１】
ユーザＩＤが上記ユーザデータベースに登録されておりかつ認証用パスワードが正しくない場合は、そのアクセスは「攻撃（アタック）」であると判定され、そのアクセスが拒否される。
【００４２】
認証チェックが正しく行われると、ゲートキーパ３０３は、そのユーザからのリソース要求を受け付けるためのポート（ソケット）（許可・接続用ポート）を確保し、そのポートに関連付けて、クライアントマシン３０１とリソース管理サーバ１０２間で通信されるリソース関連情報を中継するための中継サーバを起動した後、クライアントマシン３０１に、上記許可・接続用ポートを通知する（図７のＳ３）。この場合、ゲートキーパ３０３では、例えば図１１のステップ５～８に示されるプログラムコードが実行される。ステップ５では、信頼度がボーダラインより高いか否かが判定される。ステップ６では、許可・接続用ポート番号が動的に確保される。ステップ７では、上記ポート番号を使う上記中継サーバが起動される。ステップ８では、その起動に成功した場合に上記ポート番号がクライアントマシン３０１に通知される。
【００４３】
クライアントマシン３０１上で実行されているクライアントアプリケーション３０２は、認証チェックサーバ１０１から上記許可・接続用ポートを通知されると、まず、リソース要求を予め定められたデータフォーマットで組み立てた後、ユーザからそのユーザの秘密鍵を取り出すためのパスフレーズを受け取ることによって、その秘密鍵を取り出し、その秘密鍵を使って、上記リソース要求を暗号化する。続いて、クライアントアプリケーション３０２は、上述の通知されたポートを使って、上述の暗号化されたリソース要求を送信する（図７のＳ４）。この場合に、クライアントアプリケーション３０２では、例えば図１０のステップ３のプログラムコードが実行される。
【００４４】
認証チェックサーバ１０１で実行されている中継サーバは、クライアントマシン３０１から受信したリソース要求を、それを送信したユーザに対応する公開鍵で復号した後、その復号されたリソース要求に、それを送信したユーザに対して計算されているユーザの信頼度（図７のＳ２参照）を埋め込み、そのリソース要求をリソース管理サーバ１０２に送信する（図７のＳ５）。
【００４５】
リソース管理サーバ１０２において実行されているリソースマネージャ３０４（図３参照）は、社内リソースの論理名からそれに対応する社内リソースを提供する個別サーバ１０３を探すためのダイレクトリを、社外にいるユーザに社外ネットワークを介して提供すると共に、クライアントマシン３０１から上記社内リソースへのアクセス権を決定する機構を有する。
【００４６】
より具体的には、リソース管理サーバ１０２は、認証チェックサーバ１０１からリソース要求を受信すると、そのリソース要求を構文解析してそのリソース名とユーザの信頼度を抽出した後に、それらの情報を使ってそのリソースに対するアクセス権を計算する（図７のＳ６）。アクセス権としては、例えば社内ユーザであればリード及びライト可能、社外ユーザであればリードオンリー、社外秘リソースについては社外ユーザはアクセス禁止といったアクセス権が計算される。この場合、リソースマネージャ３０４では、例えば図１２のステップ１～３のプログラムコードが実行される。ステップ１では、リソース要求の受信処理が実行される。ステップ２では、受信されたリソース要求に対する構文解析処理が実行されることによって、そのリソース名とユーザの信頼度を含むデータ組ｐが抽出される。ステップ３では、そのデータ組ｐに対するアクセス権の計算処理が実行される。
【００４７】
なお、アクセス権の決定は、個別サーバ１０３が行ってもよい。
続いて、リソース管理サーバ１０２は、上記構文解析したリソース要求に対応するネット

ワークサービスを提供する個別サーバ１０３を見つけ、それに対し、上記構文解析したリソース要求とアクセス権とを送信すると共に、要求されている社内リソースを提供する前述の移動コードである中継エージェントを要求する（図７のＳ７）。この場合、リソースマネージャ３０４では、例えば図１２のステップ４及び５のプログラムコードが実行される。ステップ４では、許可しうるアクセス権が得られたか否かが判定される。ステップ５では、個別サーバ１０３に対するリソース要求及びアクセス権と、中継エージェントの要求とが送信される。

【００４８】

リソース管理サーバ１０２からリソース要求及びアクセス権と中継エージェントの要求とを受信した個別サーバ１０３は、要求された中継エージェントを生成し、その中継エージェント中に、リソース管理サーバ１０２から受け取ったアクセス権、クライアント識別コード、及びプログラムの生存期限（Expire Date ）等の個別設定を埋め込む（図７のＳ８）。この中継エージェントは、例えばサン・マイクロシステムズ社が開発しているＪＡＶＡ言語による移動コードとして記述され、社内ネットワーク及び社外ネットワーク内を自由に移動できるほか、社内リソースのコンテンツとそのコンテンツにアクセスするためのインタフェース（メソッド）を含んでいる。

【００４９】

その後、個別サーバ１０３は、図４に示されるようにして、その中継エージェントをリソース管理サーバ１０２に返送する（図７のＳ９）。

リソース管理サーバ１０２で実行されているリソースマネージャ３０４は、上記個別サーバ１０３から上記中継エージェントを受け取ると、図４に示されるように、それを認証チェックサーバ１０１に返送する（図７のＳ１０）。この場合に、リソースマネージャ３０４では、例えば図１２のステップ６のプログラムコードが実行される。

【００５０】

認証チェックサーバ１０１で実行されている前述した中継サーバは、リソース管理サーバ１０２から上記中継エージェントを受け取ると、図４に示されるように、上記リソース要求を送信したユーザの登録されている公開鍵を用いてその中継エージェントを暗号化し（図４の認証チェックサーバ１０１内の鍵マーク）、上記リソース要求を送信したクライアントマシン３０１に返送する（図７のＳ１１）。

【００５１】

暗号化された中継エージェントを受け取ったクライアントマシン３０１は、認証チェック時にユーザが認証チェックサーバ１０１に送信したパスフレーズを使用して、そのユーザの秘密鍵を取り出し、図４に示されるように、その秘密鍵を用いて上記暗号化された中継エージェント４０１を復号し（図４のクライアントマシン３０１内の鍵マーク）、その中継エージェントのプログラムを実行する（図７のＳ１２）。この場合、クライアントマシン３０１で実行されているクライアントアプリケーション３０２では、例えば図１０に示されるステップ４～６のプログラムコードが実行される。ステップ４では、中継エージェント４０１が受信されたか否かが判定される。ステップ５では、中継エージェント４０１が復号される。ステップ６では、復号された中継エージェント４０１が実行される。

【００５２】

この結果、ユーザが要求した社内リソースが、クライアントマシン上に再現される。ユーザは、クライアントマシン３０１において、図５に示されるように、社内ネットワーク内の個別サーバ１０３とは非同期に、クライアントマシン３０１上に再現された社内リソースにアクセスすることができる。

【００５３】

クライアントマシン３０１上で実行される中継エージェント４０１は、それ自身に埋め込まれているアクセス権とクライアント識別コードを参照することにより、そのアクセス権を超えるアクセス要求を制限する。

【００５４】

クライアントマシン３０１において社内リソースに対するデータの書き戻し要求が発生し

た場合について、図６の動作説明図と、図８及び図９のシーケンス図とを用いて説明する。図８は、クライアントマシン３０１が社内リソースを受信した時点と書き戻し要求の時点とで時間差があまりない場合のシーケンス図であり、図９は、その時間差がある場合のシーケンス図である。以下の説明では、これらの図を同時に参照しながら説明する。

【００５５】

まず、クライアントマシン３０１において書き戻し要求が発生すると（図８又は図９のＳ１）、クライアントマシン３０１において実行されている中継エージェント４０１は、それに含まれているコードによって、その要求を発生させたユーザのアクセス権をチェックする（図８又は図９のＳ２）。

【００５６】

アクセスＯＫならば、中継エージェント４０１は、認証チェックサーバ１０１に対して、認証チェック要求を発行する（図８又は図９のＳ３。この認証チェック要求には、図７のＳ１の場合と同様に、ユーザＩＤと認証用パスワードが含まれる。

【００５７】

認証チェックサーバ１０１内のゲートキーパ３０３は、クライアントマシン３０１からユーザＩＤと認証用パスワードを受信すると、それに対応するユーザの接続開始時からの経過時間をチェックする（図８のＳ４又は図９のＳ４´）。

【００５８】

ゲートキーパ３０３は、その経過時間が所定時間以下で、そのユーザからのリソース要求を受け付けるための許可・接続用ポート（図７のＳ３参照）がまだ開いている場合には、クライアントマシン３０１にその許可・接続用ポートを通知する（図８のＳ５）。

【００５９】

一方、ゲートキーパ３０３は、その経過時間が所定時間を超えており、そのユーザからのリソース要求を受け付けるための許可・接続用ポートが既に閉じられている場合には、図７のＳ２の場合と同様の認証チェック及び信頼度計算処理を実行し（図９のＳ４´）、その結果確保された許可・接続用ポートをクライアントマシン３０１に通知する（図９のＳ５）。

【００６０】

クライアントマシン３０１上で実行されている中継エージェント４０１は、認証チェックサーバ１０１から上記許可・接続用ポートを通知されると、図７のＳ４の場合と同様にして、まず書き戻し要求を予め定められたデータフォーマットで組み立てた後、認証チェック時にユーザが認証チェックサーバ１０１に送信したパスフレーズを使用して、そのユーザの秘密鍵を取り出し、その秘密鍵を使って、社内リソースに対して書き戻される新たなコンテンツを含む書き戻し要求を暗号化する。続いて、中継エージェント４０１は、上述の通知されたポートを使って、上述の暗号化された書き戻し要求を送信する（図８又は図９のＳ６）。

【００６１】

認証チェックサーバ１０１で実行されている中継サーバは、クライアントマシン３０１から受信した書き戻し要求を、それを送信したユーザに対応する公開鍵で復号した後、その復号された書き戻し要求に、それを送信したユーザに対して以前に（図８の場合）又は新たに（図９の場合）計算されたユーザの信頼度を埋め込み、その書き戻し要求をリソース管理サーバ１０２に送信する（図８又は図９のＳ７）。

【００６２】

リソース管理サーバ１０２で実行されているリソースマネージャ３０４は、認証チェックサーバ１０１から上記書き戻し要求を受信すると、図７のＳ６の場合と同様に、その要求を構文解析してそのリソース名とユーザの信頼度を抽出した後に、それらの情報を使ってそのリソースに対するアクセス権を計算する（図８又は図９のＳ８）。

【００６３】

リソース管理サーバ１０２は、上記構文解析した書き戻し要求に対応するネットワークサービスを提供する個別サーバ１０３を見つけ、それに対し、上記構文解析した書き戻し要

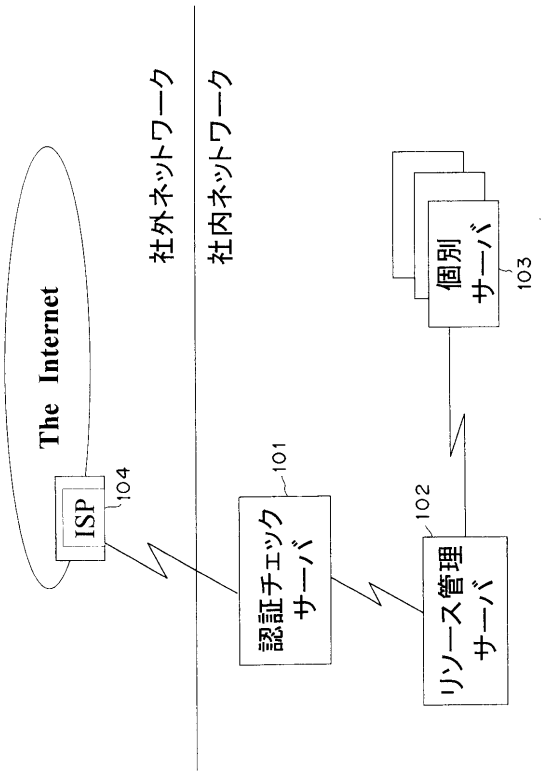
求とアクセス権とを送信する（図８又は図９のＳ９）。
【００６４】
リソース管理サーバ１０２から書き戻し要求とアクセス権を受信した個別サーバ１０３は、そのアクセス権に基づいてその書き戻し要求に含まれるコンテンツを社内リソースに書き戻す。
【００６５】
書き戻しに成功すると、個別サーバ１０３からクライアントマシン３０１に、書き戻し成功の通知が返送されて、書き戻し処理が完了する（図８又は図９のＳ１０）。
【００６６】
クライアントマシン３０１で実行される中継エージェント４０１は、その実行経過時間が、その中継エージェント４０１自身に設定されている生存期限を超えると、自動的にそれ自身のプロセスを消滅させる。
【００６７】
【発明の効果】
本発明によれば、ユーザを第１基準、サービスを第２基準としてフィルタリングを行うことにより、社員であればデフォルトで全てのアクセスが許可され、社外のユーザに対してはデフォルトで全てのアクセスが禁止される、というユーザ毎に別々のポリシーに従って、社内リソースを外部からの攻撃から守り、社内ユーザの要望の多様化を満足させることが可能となる。
【００６８】
また、認証チェックの後に社内ネットワーク内のマシンにログインを許可するという従来の方式から、要求のあった社内リソースだけを外部に送信するという方式に変更されることにより、１回の攻撃で生じ得る被害の規模を従来より小規模に抑えることが可能となる。
【００６９】
より具体的には、社内リソースとして、社内に届いた電子メールのようなテキスト情報やマルチメディア情報などと、開発中のシステムなどのアプリケーションプログラム・データなどとが区別されず、社内で所有されるアプリケーションなどが社内リソースの１つと位置づけされることにより、社外と社内にあるアプリケーションを連携させて動作させることも可能となる。
【００７０】
このように、本発明によれば、フィルタリングの方式を変更することでファイアウォールの利便性を格段に向上させ、更にユーザの認証チェックと社内リソースへのアクセス制御を個別に行うことでセキュリティ機構を２重化し、従来と同等のセキュリティレベルを確保することが可能となる。
【図面の簡単な説明】
【図１】本発明の実施の形態のシステム構成図（その１）である。
【図２】本発明の実施の形態のシステム構成図（その２）である。
【図３】本発明の実施の形態の動作説明図（その１）である。
【図４】本発明の実施の形態の動作説明図（その２）である。
【図５】本発明の実施の形態の動作説明図（その３）である。
【図６】本発明の実施の形態の動作説明図（その４）である。
【図７】クライアント－サーバ間のサービスの確立シーケンスを示す図である。
【図８】更新時の手続きシーケンスを示す図（リソースを受け取った時と書き戻し時に時間差があまりない場合）である。
【図９】更新時の手続きシーケンスを示す図（リソースを受け取った時と書き戻し時に時間差がある場合）である。
【図１０】クライアントアプリケーションのプログラムの例を示す図である。
【図１１】ゲートキーパのプログラムの例を示す図である。
【図１２】リソースマネージャのプログラムの例を示す図である。

【符号の説明】

１０１	認証チェックサーバ
１０２	リソース管理サーバ
１０３	個別サーバ
１０４	インターネットサービスプロバイダ（ＩＳＰ）
２０１	パケットフィルタリングルータ
３０１	クライアントマシン
３０２	クライアントアプリケーション
３０３	ゲートキーパ
３０４	リソースマネージャ
３０５	社内リソース群

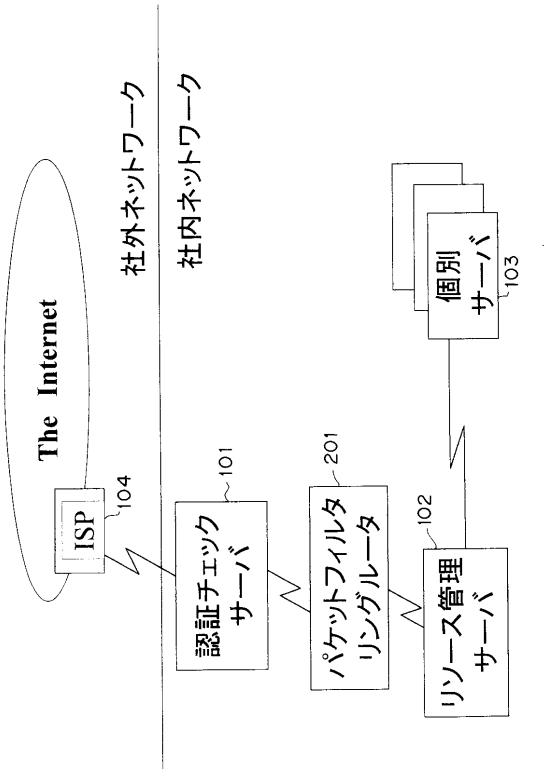
【図１】

本発明の実施の形態のシステム構成図（その１）



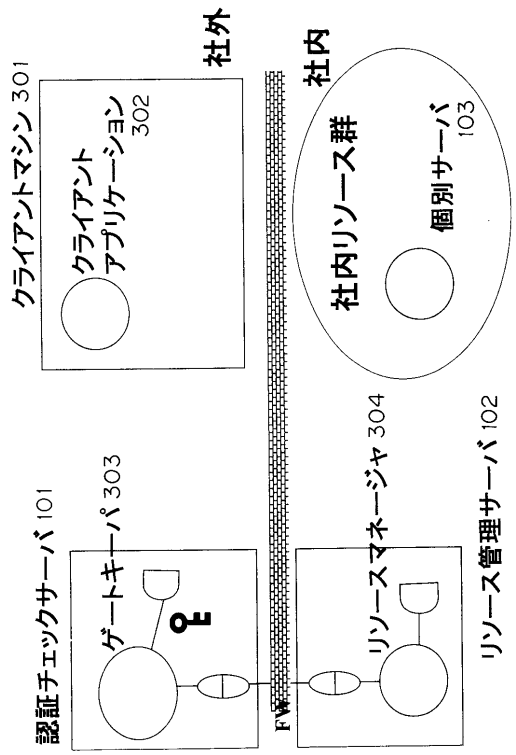
【図２】

本発明の実施の形態のシステム構成図（その２）



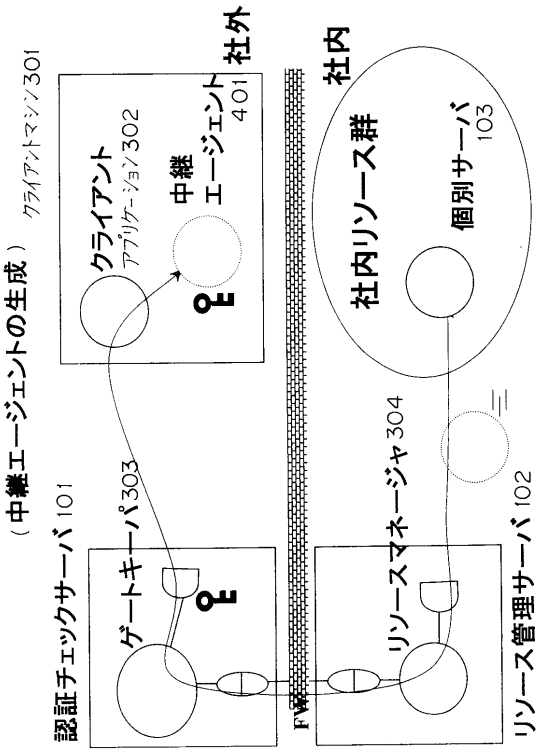
【図３】

本発明の実施の形態の動作説明図（その1）



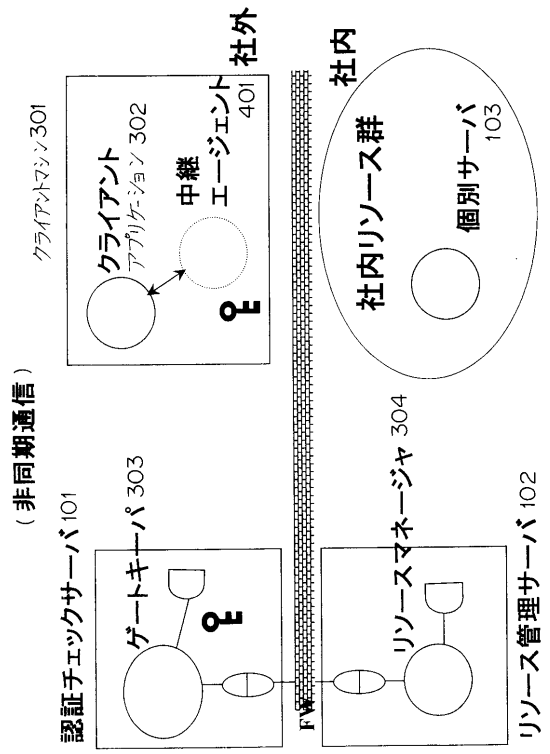
【図４】

本発明の実施の形態の動作説明図（その2）



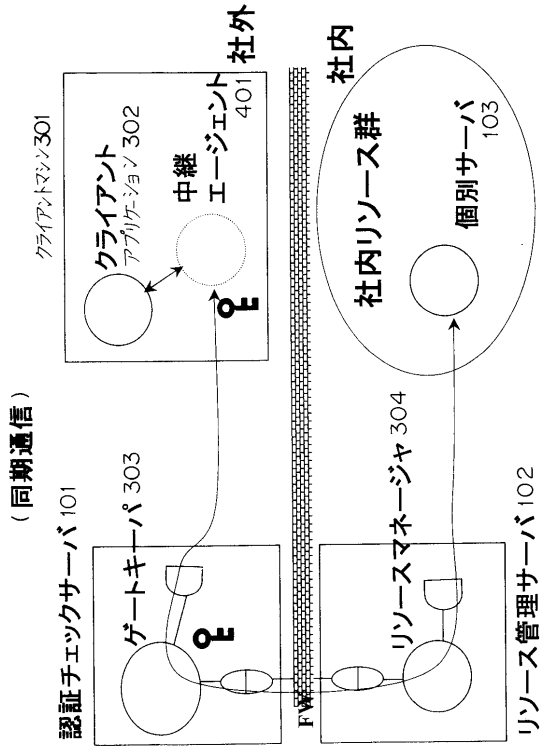
【図５】

本発明の実施の形態の動作説明図（その3）

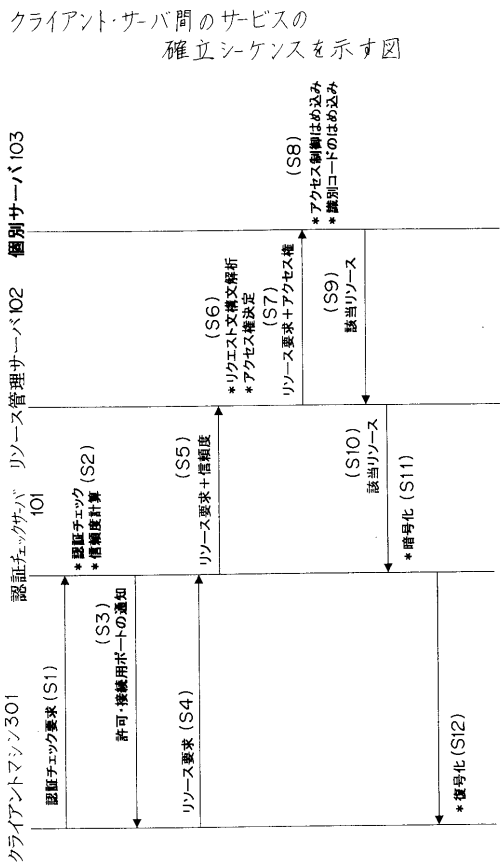


【図６】

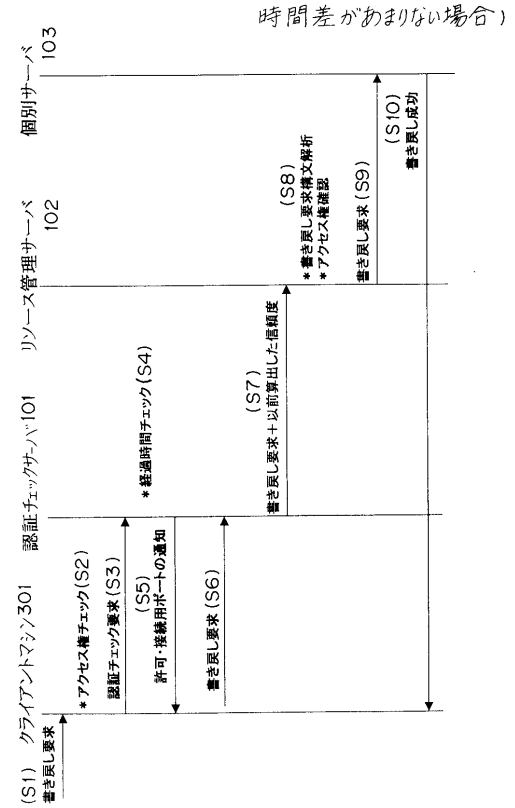
本発明の実施の形態の動作説明図（その4）



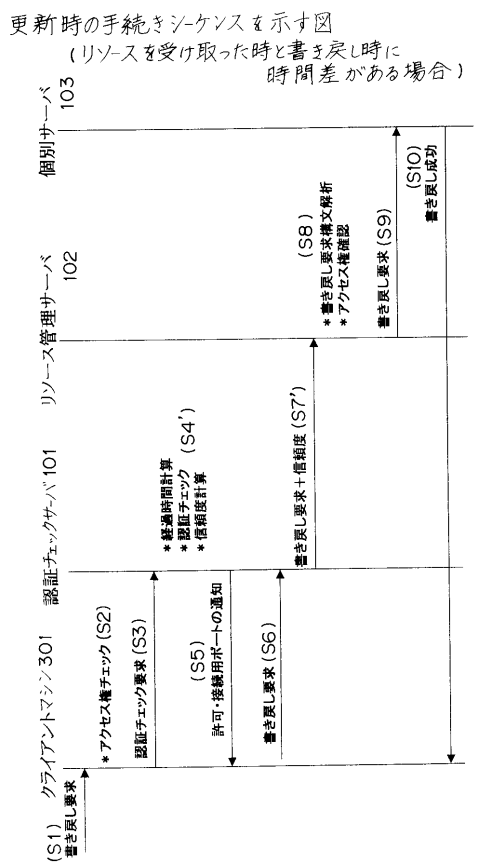
【図７】



【図８】



【図９】



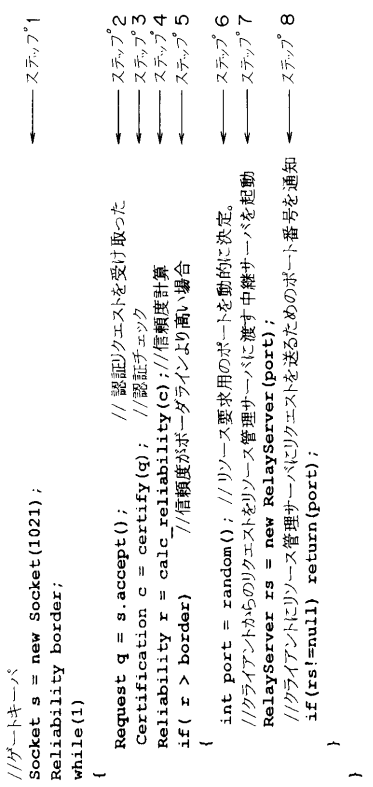
【図１０】

クライアントアプリケーションのプログラムの例を示す図

```
//ゲートキーパが動作している、認証チェックサーバのホスト名          ←― ステップ1
String CertServer = "cert.server.domain";
//ゲートキーパ(認証サーバ内)に接続後、ウィンドウが現れる。IDとパスワードを入力する。  ←― ステップ2
//認証に成功したらポート番号が返る
int port = GetCertification(CertServer,1021);
if( port != -1)
{
  // 認証に成功したら中継エージェント(プログラム)を要求。読み・書き・実行をしたい。  ←― ステップ3
  EncryptedAgent ea = send(CertServer, port, request, "rwx");
  if(ea != null) //中継エージェントを暗号化された移動コードとして得られた場合      ←― ステップ4
  {
    RelayAgent ra = decrypt(ea);//移動コードを復号化し中継エージェントを得る      ←― ステップ5
    ra.exec(); //中継エージェントを実行して社内リソースをクライアント上に再現      ←― ステップ6
  }
}
```

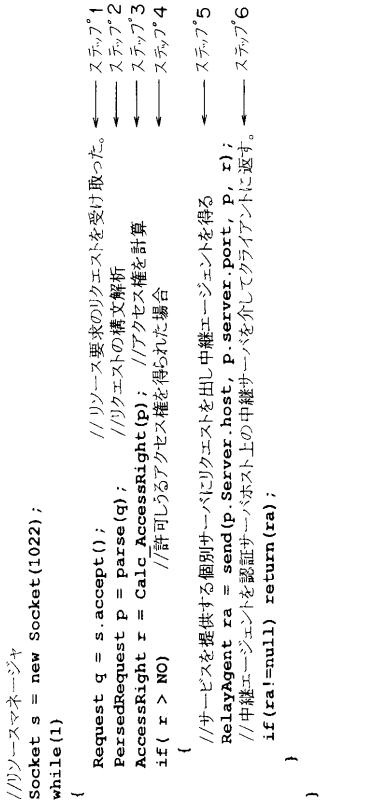
【図１１】

ゲートキーパのプログラムの例を示す図



【図１２】

リソースマネージャのプログラムの例を示す図



フロントページの続き

(72)発明者　飯田　　一朗
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　石井　茂和

(56)参考文献　特開平０９－２５２３２３（ＪＰ，Ａ）
特開平１０－０２８１４４（ＪＰ，Ａ）
特開平１０－１２６４４０（ＪＰ，Ａ）
特開平１０－１３５９４２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　13/00
G06F　21/20
H04L　 9/32
H04L　29/02
WPI(DIALOG)
JSTPlus(JDream2)