(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2004-220120
(P2004-220120A)
(43)公開日　平成16年8月5日(2004.8.5)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 15/00	G06F 15/00	330A	5B017
G06F 12/00	G06F 12/00	537A	5B082
G06F 12/14	G06F 12/14	310K	5B085
G06F 13/00	G06F 13/00	351Z	5B089
H04L 9/32	H04L 9/00	675A	5J104

審査請求 未請求　請求項の数 11　ＯＬ　（全 16 頁）

(21)出願番号　特願2003-3696(P2003-3696)
(22)出願日　平成15年1月9日(2003.1.9)

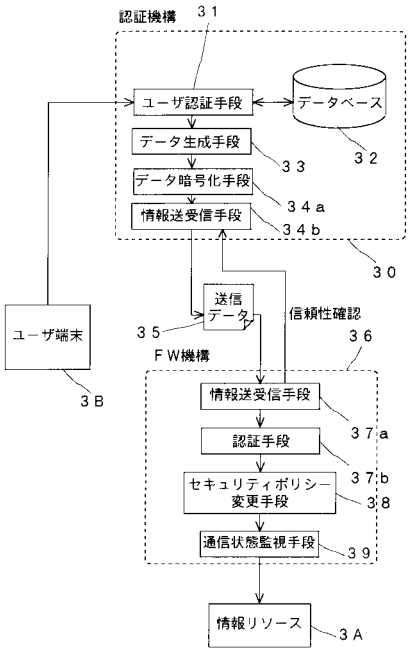
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100069981
弁理士　吉田　精孝
(72)発明者　佐藤　大輔
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　中原　慎一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5B017 AA01 BA06 BB06 CA07 CA16
5B082 EA11
5B085 AA08 AE01 AE23 AE29 BA06
BG02 BG03 BG04 BG07

最終頁に続く

(54)【発明の名称】ネットワークセキュリティシステム、アクセス制御方法、認証機構、ファイアウォール機構、認証機構プログラム、ファイアウォール機構プログラム及びその記録媒体

(57)【要約】
【課題】認証機構とＦＷが連携した並列型ＳＳＯにおいて、管理者が認証機構のセキュリティポリシーを再設定することなしにユーザ毎にアクセス制御を行い、負荷を分散するとともに、プロトコル等に依存しないネットワークセキュリティシステム及びその方法等を提供する。
【解決手段】認証機構３０は、ユーザ情報をデータベース３２に蓄積されたユーザ情報とユーザがアクセスしたい情報リソース３Ａとの対応情報と比較し、ユーザを認証するユーザ認証手段３１と、ユーザの送信元情報を取得し、情報リソース３Ａへのアクセス権限と併せてデータ３５を生成するデータ生成手段３３等を有し、ファイアウォール機構３６は、復号されたデータを解析し読み込み、該解析されたデータを基に、セキュリティポリシーを自動的に変更するセキュリティポリシー変更手段３８等を有する。
【選択図】　図３



【特許請求の範囲】
【請求項１】
情報リソースが、セキュリティポリシーに基づき稼動するファイアウォール機構に守られ、ユーザの認証を行う認証機構により認証されたユーザが、該ファイアウォール機構を通じて該情報リソースにアクセスするネットワークセキュリティシステムにおいて、
前記認証機構は、
ユーザ情報とユーザがアクセスしたい情報リソースとの対応情報を蓄積するデータベースと、
ユーザ情報を前記データベースに蓄積された対応情報と比較し、ユーザが情報リソースにアクセスする権限を有していることを認証するユーザ認証手段と、
ユーザの送信元情報を取得し、情報リソースへのアクセス権限と併せてデータを生成するデータ生成手段と、
前記データを暗号化して送信データを生成するデータ暗号化手段と、
該送信データを前記ファイアウォール機構へ送信しかつ該ファイアウォール機構からの種々の情報を受信する情報送受信手段とを有し、
前記ファイアウォール機構は、
前記認証機構から送信された送信データを受信し、かつ種々の情報を送信する情報送受信手段と、
前記送信データを復号し前記認証機構の認証を行う認証手段と、
前記復号されたデータを解析し読み込み、該解析されたデータを基に、セキュリティポリシーを自動的に変更するセキュリティポリシー変更手段とを有する
ことを特徴とするネットワークセキュリティシステム。
【請求項２】
ユーザ端末と情報リソースとの通信を監視し、通信の終了を検知するとアクセス許可の取り消しをセキュリティポリシー変更手段に要請する通信状態監視手段を有すると共に、
前記セキュリティポリシー変更手段は、前記通信状態監視手段によるアクセス許可取り消しの要請に従いセキュリティポリシーを変更する機能を有する
ことを特徴とする請求項１記載のネットワークセキュリティシステム。
【請求項３】
セキュリティポリシーに基づき稼動するファイアウォール機構により、情報リソースを不正なアクセスから防御するにあたり、ユーザの認証を行う認証機構により認証されたユーザのみを該ファイアウォール機構を通じて該情報リソースにアクセスできるようになしたアクセス制御方法において、
前記認証機構が、
ユーザ情報の入力を受け付ける工程と、
ユーザ情報を、ユーザ情報とユーザがアクセスしたい情報リソースとの対応情報を蓄積するデータベースに蓄積された対応情報と比較し、ユーザが情報リソースにアクセスする権限を有していることを認証する工程と、
ユーザの送信元情報を取得し、ユーザが情報リソースにアクセスする権限と併せてデータを生成する工程と、
前記データを暗号化して送信データを生成する工程と、
該送信データを前記ファイアウォール機構へ送信する工程とを有し、
前記ファイアウォール機構が、
前記認証機構から送信された前記送信データを受信する工程と、
前記送信データを復号し前記認証機構を認証する工程と、
前記復号されたデータを解析し読み込み、解析されたデータを基に、セキュリティポリシーを自動的に変更する工程とを有する
ことを特徴とするアクセス制御方法。
【請求項４】
前記ファイアウォール機構では、ユーザ端末と情報リソースとの通信を監視し、通信の終

了を検知するとセキュリティポリシーを変更しアクセス許可を取り消す工程を有する
ことを特徴とする請求項３記載のアクセス制御方法。
【請求項５】
情報リソースがファイアウォール機構に守られ、認証されたユーザのみが該情報リソースにアクセスできるネットワークセキュリティシステムにおいてユーザの認証を行う認証機構であって、
ユーザ情報とユーザアクセスしたい情報リソースとの対応情報を蓄積するデータベースと、
ユーザ情報を前記データベースに蓄積された対応情報と比較し、ユーザが情報リソースにアクセスする権限を有していることを認証するユーザ認証手段と、
ユーザの送信元情報を取得し、ユーザが情報リソースにアクセスする権限と併せてデータを生成するデータ生成手段と、
前記データを暗号化して送信データを生成するデータ暗号化手段と、
該送信データを前記ファイアウォール機構へ送信しかつ該ファイアウォール機構からの種々の情報を受信する情報送受信手段とを有する
ことを特徴とする認証機構。
【請求項６】
認証装置によって認証されたユーザのみがファイアウォール機構を通じて情報リソースにアクセスできるネットワークセキュリティシステムにおいて不正なアクセスを防御するファイアウォール機構であって、
前記認証装置から送信されたユーザの送信元情報とユーザの情報リソースへのアクセス権限とを含む送信データを受信し、かつ種々の情報を送信する情報送受信手段と、
前記送信データを復号し、前記認証装置を認証する認証手段と、
前記復号されたデータを解析し読み込み、該解析されたデータを基に、セキュリティポリシーを自動的に変更するセキュリティポリシー変更手段とを有する
ことを特徴とするファイアウォール機構。
【請求項７】
ユーザ端末と情報リソースとの通信を監視し、通信の終了を検知するとアクセス許可の取り消しを前記セキュリティポリシー変更手段に要請する通信状態監視手段を有すると共に、
前記セキュリティポリシー変更手段は、前記通信状態監視手段によるアクセス許可取り消しの要請に従いセキュリティポリシーを変更する機能を有する
ことを特徴とする請求項６記載のファイアウォール機構。
【請求項８】
情報リソースがファイアウォール機構に守られ、ユーザの認証を行う認証機構により認証されたユーザが該ファイアウォール機構を通じて該情報リソースにアクセスするネットワークセキュリティシステムにおける認証機構を実現する認証機構プログラムであって、
該プログラムはコンピュータに、
ユーザ情報が入力されると、該ユーザ情報と、ユーザ情報とユーザがアクセスしたい情報リソースとの対応情報を蓄積するデータベースに蓄積された対応情報とを比較させ、ユーザが情報リソースにアクセスする権限を有していることを確認させ、ユーザの送信元情報を取得、ユーザが情報リソースにアクセスできる権限と併せてデータを生成させ、前記データを暗号化させ、前記ファイアウォール機構へ送信させる動作を実現する
ことを特徴とする認証機構プログラム。
【請求項９】
情報リソースが、セキュリティポリシーに基づき稼動するファイアウォール機構に守られ、ユーザの認証を行う認証機構により認証されたユーザが該ファイアウォール機構を通じて該情報リソースにアクセスするネットワークセキュリティシステムにおける、ファイアウォール機構を実現するファイアウォール機構プログラムであって、
該プログラムはコンピュータに、

前記認証機構から送信されたユーザの送信元情報とユーザの情報リソースへのアクセスする権限とを暗号化された状態で含む送信データを受信すると、該データを復号させ、前記復号されたデータを解析させ読み込ませ、解析されたデータを基に、セキュリティポリシーを自動的に変更させる動作を実行する
ことを特徴とするファイアウォール機構プログラム。
【請求項１０】
ユーザ端末と情報リソースとの通信を監視させ、通信の終了を検知するとセキュリティポリシーを変更させ、アクセスの許可を取り消させる
ことを特徴とする請求項９記載のファイアウォール機構プログラム。
【請求項１１】
請求項８乃至１０何れか１項記載のプログラムを記録したプログラム記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、ネットワークに接続した計算機のセキュリティに関するものであり、特に、ファイアウォール機構（以下、ＦＷと略す）と本人認証機構の連携による情報リソースへのアクセス制御装置及び方法等に関する。
【０００２】
【従来の技術】
ネットワークにおいてサービスを提供する、すなわち、情報リソースを公開するためには、外部からの様々な脅威を想定し、予め対策を講じておくことが必要である。ネットワーク上のサービス提供システムを保護するため、予め情報リソースの利用者として認められた利用者を登録しておき、情報リソースへアクセスする前に本人認証を行い、登録ユーザとして認められた利用者のみに情報リソースへのアクセスを許可するというような本人認証機構や、ＩＰアドレス、プロトコル、ポート番号等について、予め設定、または許可された値を持つ者以外の通過を許さないＦＷによる防御システム等が一般的に使用されている。
【０００３】
本人認証機構では、ベーシック認証やＣＡ（Ｃｅｒｔｉｆｉｃａｔｉｏｎ Ａｕｔｈｏｒｉｔｙ）のようなＩＤ、パスワード、ＰＫＩ（Ｐｕｂｌｉｃ Ｋｅｙ Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）を用いた本人認証や、クッキーを用いたＷｅｂサーバにおける本人認証等が一般に行われている。
【０００４】
ＦＷによる防御システムでは、予め定義されたセキュリティポリシーに基づくルールベース（以下、単にセキュリティポリシーと呼ぶ）に従いアクセス制御を行う。このアクセス制御には主に、（１）ＩＰアドレス、ポート番号、プロトコルタイプ等を判別したパケット通過の制御（パケットフィルタリング）、（２）外部ネットワークとの通信を代理サーバが行うことによりアプリケーションレベルでの制御（アプリケーションレベル・ゲートウェイ（プロキシ））があり、近年のＦＷ製品は、（１）に加え（２）の機能もある程度兼ね備えたものが主流となっている（例えば、非特許文献１参照）。
【０００５】
他のＦＷによる防御システムでは、例えば、ＣｈｅｃｋＰｏｉｎｔ社の製品であるＦｉｒｅＷａｌｌ－１は、メモリ上に動的に通信の状態を保持するステートテーブルを持ち、情報リソース利用要求に対して最初のパケットのみをセキュリティポリシーを参照して検査することで、アプリケーションレベルの制御を可能とする。つまり、一旦、ＦＷを通過した後の通信状態を、ステートテーブルを参照することによって動的に制御できる（例えば、非特許文献２参照）。
【０００６】
しかし、最初のパケットを検査するためのセキュリティポリシー自体は、ＦＷ管理者が静的に設定しておく必要があり、アクセスに対する動的な制御という点で見ると、アクセス

後のパケット通過に関する動的制御や、不法アクセス検出後の情報リソースの保護（例えば、特許文献１参照）は可能だが、アクセス自体を動的に制御する、すなわち、セキュリティーポリシーを動的に更新することは、従来のＦＷでは行われていない。

【０００７】

上記のような本人認証とＦＷによるアクセス制御（（２）のプロキシ機能）を組み合わせ、独立させ、認証やアクセス制御をユーザやサービス提供者に代わり集中して行う方式をＳｉｎｇｌｅ　Ｓｉｇｎ　Ｏｎ（以下、ＳＳＯ）と呼ぶ。ＳＳＯは大きく２種類に分けることができる。１つは本人認証機能とアクセス制御機能を併せ持つＳＳＯサーバを配置し、必ずそのサーバを通して保護対象のリソースとアクセスさせる方式で、情報リソースから見てＳＳＯサーバはプロキシサーバの役割を担うため、リバースプロキシ方式と呼ばれる（例えば、特許文献２参照）。もう１つは、ＳＳＯサーバが本人認証と同時にクッキーやチケット等で情報を払い出し、それを保護対象情報リソースに予め組み込まれたモジュールが解釈することによりアクセス制御を行う方式で、エージェントモジュール方式と呼ばれる。この場合は、前者のようにＳＳＯサーバと保護対象の情報リソースとを直列に接続する必要はない。このことから、以降、前者を直列型ＳＳＯ、後者を並列型ＳＳＯと呼ぶ。直列型ＳＳＯの例としては、Ｎｏｖｅｌ社のｉＣｈａｉｎ（登録商標）や、日本ＨＰのＩｃｅＷａｌｌ（登録商標）ＳＳＯ、並列型ＳＳＯの例としては、エントラスト社のＧｅｔＡｃｃｅｓｓ（登録商標）やネテグリティ社のＳｉｔｅＭｉｎｄｅｒ等が挙げられる（例えば、非特許文献３）。

【０００８】

【特許文献１】

特許第３１６５３６６号公報

【特許文献２】

特開２００２－１３２７１４号公報

【非特許文献１】

エドワード・アモロソ、ロナルド・シャープ著、「ＦＷを知る」、株式会社ピアソン・エデュケーション、２０００年４月１０日、ｐ．４３－５０

【非特許文献２】

「ＦｉｒｅＷａｌｌ－１導入の手引き」、ＣｈｅｃｋＰｏｉｎｔ社、２０００年１月、ｐ．４６

【非特許文献３】

日経インターネットテクノロジー「サーベイ：Ｗｅｂ向けシングル・サインオン製品　ＥＣでの利用が急増、マルチドメインやモバイルへの対応も進む」、２００１年４月、ｐ．１９０～１９９

【０００９】

【発明が解決しようとする課題】

複数のサービスをネットワーク上から提供する、または、ネットワーク上の複数サービスを連携させて一連の処理を行う場合、サービスを利用するユーザの観点からすると、各サービスの認証は統一されていることが望ましい。そのような場合のネットワークセキュリティシステムに関する課題を述べる。

【００１０】

本人認証機構では、自らが保有するチェックリストにより登録ユーザ毎、情報リソース（サービス）毎のアクセス制御を可能とする。しかし、当該認証機構を利用せずにサービス主体にアクセスするユーザに対して制御を行うことができなかった（欠点１）。

【００１１】

一方、ＦＷはサービスのゲートウェイとして設置されるため、サービスにアクセスするためには必ず通過せねばならず、セキュリティポリシーの設定次第で、セキュリティの強度を上げることが可能である。しかし、ＦＷにおいてアクセス制御を行うセキュリティーポリシー設定は、静的に定義するものであるため、特定のユーザを通過させるには、管理者がＦＷの設定を直接書き換える必要があった（欠点２）。前述のＦｉｒｅＷａｌｌ－１に

おいてもこの点は変わらない。

【００１２】

両者の機能を利用し、サービス提供主体（サーバ）自身がユーザ認証とアクセス制御を行うことが広く行われているが、複数サービスを同時に利用する場合や、複数のサービスが連携して一連の処理を行う時には、サービスを利用するユーザ側にとっては認証が統一されていることが重要である。また、システムを管理する側にとっては、認証機構とアクセス制御機能とを適切に分離して、サービス提供サーバの負荷を下げることが重要である。

【００１３】

認証機構とアクセス制御機能を個別で利用した場合、または、ＦＷを個別に利用した場合では、それぞれ上述の欠点１、２を抱えているので、これらの欠点を補う形で両者を連携させたネットワークセキュリティシステムを構築する必要がある。現在は、上述のＳＳＯを適用することで複数サービス（サーバ）を同時に利用する場合及び複数サービスの連携した処理を行う場合の、各サービスにおける認証の統一と、アプリケーションレベルでの動的なアクセス制御を実現している。

【００１４】

以下、図を用いて、従来のＳＳＯの特徴と課題について説明する。

【００１５】

図１は直列型ＳＳＯ、図２は並列型ＳＳＯの構成例である。図中において、１１、２１はユーザ端末、１２、２２は認証を行うインタフェースを構成する認証機構、１３、２３はユーザ情報を格納するデータベースである。また、１４、２４はＦＷ、１５－１、１５－２、１５－３、２５－１、２５－２、２５－３は、それぞれＦＷ１４、ＦＷ２４に保護された情報リソースである。２６は認証機構２２によって発行されたクッキーで、対象情報リソースのＵＲＬ等、アクセスするために必要な情報が記載されている。２７－１、２７－２、２７－３はそれぞれ情報リソース２５－１、２５－２、２５－３に組み込まれたモジュールで、クッキー２６を解釈し通過制御を行う。このモジュール２７－１、２７－２、２７－３は、認証機構２２に対応した専用のモジュールで、保護対象の情報リソースには必ず組み込まれなければならない。

【００１６】

図１において、情報リソース１５－１にアクセスする場合、ユーザ端末１１から認証機構１２、認証機構１２からＦＷ１４、ＦＷ１４から情報リソース１５－１の経路でセッションが張られる。このシステムでは、第三者から情報リソースへの直接アクセスを防ぐため、保護対象の情報リソースへの経路は全てＳＳＯサーバとなる認証機構１２を経由する構成にする必要がある。従って、保護された他の情報リソースにアクセスする場合でも、同様の経路を辿らなければならない。その結果、認証機構１２にアクセス負荷が集中し、セキュリティシステム全体での性能ネックを引き起こす可能性がある。

【００１７】

一方、図２の並列型ＳＳＯの構成例を見ると、ユーザ端末２１から認証機構２２への経路と、ユーザ端末２１からＦＷ２４への経路を並列経路とすることで、図１の認証機構１２と比較して認証機構２２の負荷の減少を実現している。図２におけるセキュリティシステムの動作は、まず認証機構２２において、認証に成功すると対象の情報リソース（ここでは情報リソース２５－１）にアクセスするための情報を記載したクッキー２６が、認証機構２２により発行され、ユーザ端末２１からＦＷ２４、ＦＷ２４から情報リソース２５－１の経路を辿り、モジュール２７－１によってクッキー２６の情報が解釈され、セッションが張られるという流れとなる。このシステムでは、図１の直列型ＳＳＯの構成例に比べて、負荷が分散するという点で優れているが、クッキーを使用することや、専用のエージェントモジュールを情報リソースに組み込まなければならない等、プロトコル、ＯＳ、等システム構成条件がより限定されるという欠点がある。

【００１８】

本発明の目的は、並列型の機能配置をとることで直列型ＳＳＯの課題である負荷を分散し、並列ＳＳＯにおけるアクセス制御方法をプロトコル、ＯＳ等に依存しないネットワーク

セキュリティシステム及びその方法等を提供することにある。具体的には、認証機構とＦＷを連携させ、ＦＷに認証機構との通信機能とパケット通過制御設定等のセキュリティポリシーを自動的に変更する機能を持たせることで、当該認証機構を利用せずにサービス主体にアクセスするユーザはＦＷを通過できないように為し、また、管理者が直接セキュリティポリシーの再設定を行うことなしにユーザ及び情報リソース毎に柔軟なアクセス制御を行うことを目的としている。

【００１９】

【課題を解決するための手段】

本発明では前記目的を達成するため、請求項１では、図３に示すように、情報リソースが、セキュリティポリシーに基づき稼動するファイアウォール機構に守られ、ユーザの認証を行う認証機構により認証されたユーザが、該ファイアウォール機構を通じて該情報リソースにアクセスするネットワークセキュリティシステムにおいて、前記認証機構３０は、ユーザ情報とユーザがアクセスしたい情報リソース３Ａとの対応情報を蓄積するデータベース３２と、ユーザ情報を前記データベース３２に蓄積された対応情報と比較し、ユーザが情報リソース３Ａにアクセスする権限を有していることを認証するユーザ認証手段３１と、ユーザの送信元情報を取得し、情報リソース３Ａへのアクセス権限と併せてデータを生成するデータ生成手段３３と、前記データを暗号化して送信データ３５を生成するデータ暗号化手段３４ａと、該送信データを前記ファイアウォール機構３６へ送信しかつ該ファイアウォール機構３６からの種々の情報を受信する情報送受信手段３４ｂとを有し、前記ファイアウォール機構３６は、前記認証機構３０から送信された前記送信データ３５を受信し、かつ種々の情報を送信する情報送受信手段３７ａと、前記送信データを復号し前記認証装置を認証する認証手段３７ｂと、前記復号されたデータを解析し読み込み、該解析されたデータを基に、セキュリティポリシーを自動的に変更するセキュリティポリシー変更手段３８とを有することを特徴とするネットワークセキュリティシステムをもって解決手段とする。

【００２０】

請求項１の発明によれば、並列型ＳＳＯにおいて、エージェントモジュールを利用せずに、認証機構３０を通さずに情報リソース３Ａに直接アクセスするユーザに対してアクセスを禁止することができ、アクセス対象の情報リソースが通信に使用するプロトコルによらず、ユーザのアクセスを動的に制御できる。また、ユーザの増減やアクセス対象の変更等を動的に、しかもセキュリティ強度に影響を与えることなく変更できる。

【００２１】

請求項２では、ユーザ端末３Ｂと情報リソース３Ａとの通信を監視し、通信の終了を検知するとアクセス許可の取り消しをセキュリティポリシー変更手段３８に要請する通信状態監視手段３９を有すると共に、前記セキュリティポリシー変更手段３８は、前記通信状態監視手段３９によるアクセス許可取り消しの要請に従いセキュリティポリシーを変更する機能を有することを特徴とする請求項１記載のネットワークセキュリティシステムをもって解決手段とする。

【００２２】

請求項２の発明によれば、ユーザ端末３Ｂと情報リソース３Ａ間の通信が終了すると、自動的にアクセスを断絶させることができる。

【００２３】

請求項３では、セキュリティポリシーに基づき稼動するファイアウォール機構により、情報リソースを不正なアクセスから防御するにあたり、ユーザの認証を行う認証機構により認証されたユーザのみを該ファイアウォール機構を通じて該情報リソースにアクセスできるようになしたアクセス制御方法において、前記認証機構が、ユーザ情報の入力を受け付ける工程と、該ユーザ情報を、ユーザ情報とユーザがアクセスしたい情報リソースとの対応情報を蓄積するデータベースに蓄積された対応情報と比較し、ユーザが情報リソースにアクセスする権限を有していることを認証する工程と、ユーザの送信元情報を取得し、ユーザが情報リソースにアクセスする権限と併せてデータを生成する工程と、前記データを

暗号化して送信データを生成する工程と、該送信データを前記ファイアウォール機構へ送信する工程とを有し、前記ファイアウォール機構が、前記認証機構から送信された前記送信データを受信する工程と、前記送信データを復号し前記認証機構を認証する工程と、前記復号されたデータを解析し読み込み、解析されたデータを基に、セキュリティポリシーを自動的に変更する工程とを有することを特徴とするアクセス制御方法をもって解決手段とする。

【００２４】

請求項３の発明によれば、並列型ＳＳＯにおいて、エージェントモジュールを利用せずに、認証機構を通さずに情報リソースに直接アクセスするユーザに対してアクセスを禁止することができ、アクセス対象の情報リソースが通信に使用するプロトコルによらず、ユーザのアクセスを動的に制御できる。また、ユーザの増減やアクセス対象の変更等を動的に、しかもセキュリティ強度に影響を与えることなく変更できる。

【００２５】

請求項４では、前記ファイアウォール機構では、ユーザ端末と情報リソースとの通信を監視し、通信の終了を検知するとセキュリティポリシーを変更しアクセス許可を取り消す工程を有することを特徴とする請求項３記載のアクセス制御方法をもって解決手段とする。

【００２６】

請求項４の発明によれば、ユーザ端末と情報リソース間の通信が終了すると、自動的にアクセスを断絶させることができる。

【００２７】

請求項５では、図３に示すように、情報リソースがファイアウォール機構に守られ、認証されたユーザのみが該情報リソースにアクセスできるネットワークセキュリティシステムにおいてユーザの認証を行う認証機構であって、ユーザ情報とユーザがアクセスしたい情報リソース３Ａとの対応情報を蓄積するデータベース３２と、ユーザ情報を前記データベース３２に蓄積された対応情報と比較し、ユーザが情報リソース３Ａにアクセスする権限を有していることを認証するユーザ認証手段３１と、ユーザの送信元情報を取得し、ユーザが情報リソース３Ａにアクセスする権限と併せてデータを生成するデータ生成手段３３と、前記データを暗号化して送信データ３５を生成する送信データ暗号化手段３４ａと、該送信データを前記ファイアウォール機構３６へ送信しかつ該ファイアウォール機構３６からの種々の情報を受信する情報送受信手段３４ｂとを有することを特徴とする認証機構をもって解決手段とする。

【００２８】

請求項５の発明によれば、ユーザの送信元情報とユーザが情報リソース３Ａにアクセスする権限とを併せてデータを生成することができる。

【００２９】

請求項６では、図３に示すように、認証機構によって認証されたユーザのみがファイアウォール機構を通じて該情報リソースにアクセスできるネットワークセキュリティシステムにおいて不正なアクセスを防御するファイアウォール機構であって、前記認証機構３０から送信されたユーザの送信元情報とユーザの情報リソース３Ａへのアクセス権限とを含む送信データ３５を受信し、かつ種々の情報を送信する情報送受信手段３７ａと、前記送信データを復号して前記認証機構を認証する認証手段３７ｂと、前記復号されたデータを解析し読み込み、該解析されたデータを基に、セキュリティポリシーを自動的に変更するセキュリティポリシー変更手段３８とを有することを特徴とするファイアウォール機構をもって解決手段とする。

【００３０】

請求項６の発明によれば、ユーザのアクセスを動的に許可することができる。

【００３１】

請求項７では、ユーザ端末３Ｂと情報リソース３Ａとの通信を監視し、通信の終了を検知するとアクセス許可の取り消しを前記セキュリティポリシー変更手段３８に要請する通信状態監視手段３９を有すると共に、前記セキュリティポリシー変更手段３８は、前記通信

状態監視手段３９によるアクセス許可取り消しの要請に従いセキュリティポリシーを変更する機能を有することを特徴とする請求項６記載のファイアウォール機構をもって解決手段とする。

【００３２】

請求項６の発明によれば、ユーザ端末３Ｂと情報リソース３Ａ間の通信が終了すると、自動的にアクセスを断絶させることができる。

【００３３】

【発明の実施の形態】

本発明の一実施形態について、図４～図８を用いて説明する。

【００３４】

図４は本発明を適用したネットワークセキュリティシステムの一実施形態の構成図である。４１はユーザ端末、４２はユーザを認証する認証サーバ、４３はユーザＩＤ、パスワード等のユーザ情報とユーザがアクセスを許されている情報リソースとの対応情報を蓄積するデータベース、４４は認証サーバ４２とデータベース４３とを含む認証機構、４５は情報リソース４８－１、４８－２、４８－３を不正なアクセスから防御するＦＷ機構、４６はＩＰアドレス等のユーザの送信元情報とユーザのＦＷ４５へのアクセス権限とからなり暗号化された送信データ、４７は情報リソース４８－１、４８－２、４８－３にユーザがアクセスするための条件を保持するセキュリティポリシー定義領域である。ユーザ端末４１、認証サーバ４２、及びＦＷ４５がインターネットにより接続されている。

【００３５】

ユーザ端末４１からインターネットを介して認証サーバ４２に対して情報リソース４８－１へのアクセス要求、例えばＷｅｂページにおいてユーザＩＤやパスワード等のユーザ情報が入力されると、認証サーバ４２はデータベース４３にユーザ情報と情報リソース４８－１との対応情報を照会し、情報リソース４８－１へのアクセス権限を確認した場合のみＦＷ４５と通信を行う。この時、ＦＷ４５におけるセキュリティポリシーは、ユーザが情報リソース４８－１にアクセスできるように書き換えられる。

【００３６】

図５は、図４のネットワークセキュリティシステムにおいて認証機構４４を中心に示した図である。

【００３７】

図５において、５０は例えばＷｅｂページ等においてユーザＩＤ、パスワード等を入力する認証Ｉ／Ｆ、５１は認証Ｉ／ＦにおいてＩＰアドレス等のユーザの送信元情報を取得する送信元情報取得機能、５２はデータベース４３に格納されているユーザ情報とユーザがアクセスを許されている情報リソースとの対応を表す情報リソース・ユーザ対応リスト、５３はデータベース４３と連携し、情報リソース・ユーザ対応リスト５２を照会し、ユーザの情報リソースに対するアクセス権限の有無を確認し、ユーザ認証の成否を決定するデータベース連携機能、５４はユーザ情報とユーザのデータベース連携機能５３において確認されたユーザのアクセス権限とをデータとして生成するデータフォーマット生成機能、５５はデータを書き込むためのデータテンプレート、５６は生成された暗号化される前のデータ、５７は生成されたデータを秘密鍵により暗号化し、電子署名を付し送信データ４６を生成するデータ暗号化機能、５８は送信データ４６をＦＷ４５へ送信し、ＦＷ４５から送信データ４６の受信確認通知や通信開始可能通知を受信する情報送受信機能である。

【００３８】

この構成により、認証機構４４は、ユーザ端末４１から認証Ｉ／Ｆ５０においてユーザＩＤ、パスワード等のユーザ情報が入力されると、送信元情報取得機能５１がプロトコルヘッダ等からＩＰアドレス等のユーザの送信元情報を取得する。続いて、データベース連携機能５３が、データベース４３に情報リソース・ユーザ対応リスト５２の照会を行い、ユーザ情報が情報リソース・ユーザ対応リスト５２に含まれていれば、ユーザを認証する。次に、データフォーマット生成機能５４がユーザの送信元情報とリソース・ユーザ対応リスト５２とを併せてデータテンプレート５５に従い配備し、データ５６を生成する。そし

て、データ暗号化機能５７がデータ５６を秘密鍵により暗号化し、また電子署名を付し、ＦＷ４５へ送信する送信データ４６を生成する。そして、情報送受信機能５８によりＦＷ４５へ送信データ４６を送信する。ＦＷ４５から送信データ４６の受信確認通知、通信開始可能通知を情報送受信機能５８により受信すると、認証Ｉ／Ｆ５０を通じてユーザが情報リソースと通信できることを通知する。

【００３９】

図６は、図４のネットワークセキュリティシステムにおいてＦＷ４５を中心に示した図である。

【００４０】

図６において、６０は認証機構４４から送信データ４６を受信し、送信データ４６を受信した時に認証機構４４へ送信データ４６の受信確認通知を送信し、ユーザの情報リソースへのアクセスが許可されると、認証機構４４へ通信開始可能通知を送信する情報送受信機能、６１は認証機構４４から送信データ４６を受信すると認証機構４４へ送信データ４６の受信確認通知を送信する前に、送信データ４６を公開鍵により復号し、また電子署名のチェックにより認証機構４４が正当な認証機構であり安全に通信できることを確認し認証機構を認証する認証機構認証機能、６２は復号された送信データ４６を解析、解釈する受信データ解析機能、６３は受信データ解析機能６２の解釈の内容に応じてセキュリティポリシー定義領域６４内のセキュリティポリシーに基づくアクセス許可リスト６５－１、６５－２、６５－３を自動的に編集するセキュリティポリシー編集機能である。アクセス許可リスト６５－１、６５－２、６５－３はそれぞれ情報リソース６６－１、６６－２、６６－３に対応しており、例えば、アクセス許可リスト６５－１がアクセス許可状態に書き換えられると、ユーザ端末４１は情報リソース６６－１にアクセスできるようになる。６７は保護された情報リソースへのアクセスを許可されたユーザ端末４１の情報リソースとの通信状況を監視し通信の終了を検知すると、ユーザ端末４１へのアクセスを遮断するため、再びセキュリティーポリシー定義領域６４におけるアクセス許可リストを書き換えるようにセキュリティーポリシー編集機能６３へ通知する通信状態監視機能である。通信状態監視機能６３は、ＦＷ４５上の全ての着信、発信パケットの取得、検査、パケット内全データの解析、保存が可能である。

【００４１】

この構成によりＦＷ４５は、認証機構４４から送信データ４６を情報送受信機能６０により受信すると、認証機構認証機能６１がデータ暗号化機能５７が有する秘密鍵に対応した公開鍵により送信データ４６を復号し、また電子署名をチェックすることにより認証機構４４を認証する。認証機構４４の認証を行うと、情報送受信機能６０は、認証機構４４に対して送信データ４６の受信確認通知を送信する。続いて、受信データ解析機能６２が復号された送信データ４６を解析、解釈すると、セキュリティポリシー編集機能６３がセキュリティーポリシー定義領域６４のアクセス許可リストを自動的に編集する。例えば、ユーザ端末４１が情報リソース６６－１に対してアクセスを要求しているならば、アクセス許可リスト６５－１を、アクセス許可に書き換える。このとき、情報送受信機能６０は、認証機構４４に対して通信開始可能通知を送信する。アクセス許可リスト６５－１が書き換えられ、ユーザ端末４１と情報リソース６６－１との通信が始まると、通信状態監視機能６７が通信状況を監視し、通信が終了すると、両者間のアクセスを遮断するために、アクセス許可リスト６５－１をアクセスを許可しない状態に書き換えるようにセキュリティポリシー編集機能６３に通知する。この通知をうけたセキュリティポリシー編集機能６３は、アクセス許可リスト６５－１はユーザ端末４１の情報リソース６６－１へのアクセスを許可しない状態に書き換える。そして、ユーザ端末４１、情報リソース間６６－１間の通信は終了する。

【００４２】

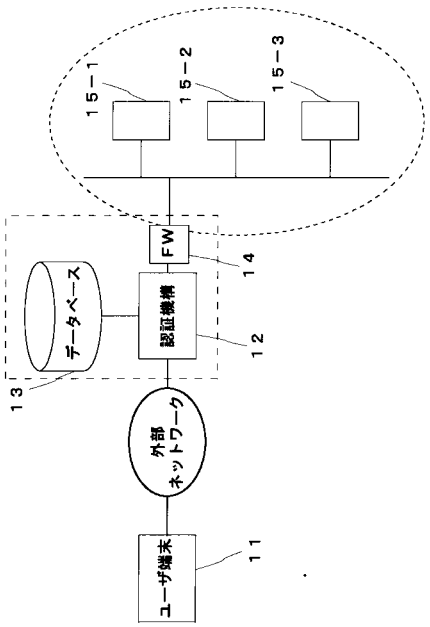
図７は、図５に示した認証機構４４を構成する認証サーバ４２とデータベース４３とＦＷ４５の連携によって実行されるユーザ認証、情報リソースへのアクセス制御に関して、主に認証サーバ４２とデータベース４３側の処理の流れを表すフローチャートである。

【００４３】
認証Ｉ／Ｆ５０にユーザ端末４１からユーザＩＤ、パスワード等のユーザ情報がフォーマットに従い入力されると（Ｓ７－１）、送信元情報取得機能５１がユーザ端末４１のＩＰアドレス等の送信元情報を取得し（Ｓ７－２）、該ユーザ情報を基にデータベース連携機能５３が、データベース４３に保存されている情報リソースと登録ユーザのリソース・ユーザ対応リスト５２を参照し（Ｓ７－３）、ユーザ端末４１が指定する情報リソースに対するアクセス権限の有無を判定する（Ｓ７－４）。データベース連携機能５３はアクセス権限があることを確認すると、リソース・ユーザ対応リスト５２より情報リソース、ユーザ情報を抽出し、予め取得済のユーザのＩＰアドレス等と共にデータフォーマット生成機能５４へ通知する。データフォーマット生成機能５４は、受け取った情報を決められたデータフォーマットに従って、データテンプレート５５に書き込み、データ５６を生成する（Ｓ７－５）。データ５６を生成すると、データ暗号化機能５７は、データに署名を付し（Ｓ７－６）、データ５６をデータ暗号化機能５７により暗号化し送信データ４６とし（Ｓ７－７）、情報送受信機能５８によってＦＷ４５へ送信する（Ｓ７－８）。そして、ＦＷ４５から送信された送信データ４６の受信確認通知を受信する（Ｓ７－９）。続いて、ＦＷ４５から通信開始可能通知を受信する（Ｓ７－１０）。最後に、通信開始可能通知を受信した情報送信機能５８は、それがＦＷ４５からのものであるとデータ暗号化機能５７により確認すると、認証Ｉ／Ｆ５０はユーザ認証が成功し、情報リソースとの通信が可能となったことをユーザ端末４１にＷｅｂページ等を介して表示する（Ｓ７－１１）、
図８は図６に示したＦＷ４５と認証機構４４との連携によって実行されるユーザ認証、情報リソースへのアクセス制御に関して、主にＦＷ４５側の処理の流れを表すフローチャートである。ユーザ端末４１は、情報リソース６６－１へのアクセスを希望するとする。
【００４４】
認証装置４４から送信された送信データ４６を情報送受信機能６０により受信すると、認証機構認証機能６１は秘密鍵で送信データ４６を復号し（Ｓ８－１）、また電子署名をチェックすることで認証機構が正当で安全に通信できることを確認する（Ｓ８－２）。認証機構４４へ受信確認通知を送信し（Ｓ８－３）、受信した送信データ４６を受信データ解析機能６２により解析、解釈を開始する（Ｓ８－４）。データの解析結果にしたがって、受信データ解析機能６２はセキュリティポリシー編集機能６３へ、ユーザ端末４１の情報リソース６６－１へのアクセス許可登録を要求し（Ｓ８－５）、要求をうけたセキュリティポリシー編集機能６３は、セキュリティポリシー定義領域６４から情報リソース６６－１のアクセス許可リスト６５－１を呼び出し（Ｓ８－６）、アクセス許可リスト６５－１をユーザ端末４１が情報リソース６６－１にアクセスできるように編集する。つまり、ユーザ端末４１のＩＰアドレスを登録する（Ｓ８－７）。これにより、ユーザ端末４１は、情報リソース６６－１と通信できるようになり、情報送受信機能６０は通信開始可能通知を認証機構４４を経てユーザ端末４１へ送信する（Ｓ８－８）。ユーザ端末４１は、認証機構４４の認証Ｉ／Ｆ５０にて通信開始可能通知を確認後、通信を開始する。通信状態監視機能６７はユーザ端末４１と情報リソース６６－１との通信状況を監視し、通信の終了を検知すると（Ｓ８－９）、セキュリティポリシー編集機能６３へユーザ端末４１の情報リソース６６－１へのアクセスの許可の削除を要求する（Ｓ８－１０）。これを受け、セキュリティポリシー編集機能６３は再びアクセス許可リスト６５－１を呼び出し（Ｓ８－１１）、ユーザ端末４１の情報リソース６６－１へのアクセス許可を取りやめるよう編集する。つまり、ユーザ端末４１のＩＰアドレスを削除する（Ｓ８－１２）。
【００４５】
上述の例の他にも、情報リソースにユーザが直接アクセスしてきた場合、認証機構４４へ自動的に転送する、またはパケット解析を行いユーザ情報を取得した後、認証機構４４へ転送し照会を行うといった形態も考えられる。
【００４６】
図９は、図６に示したＦＷ４５における通信状態監視機能６７がユーザ端末４１と情報リソース、例えば情報リソース６６－１との通信を監視する際の流れを詳細に示すフローチ

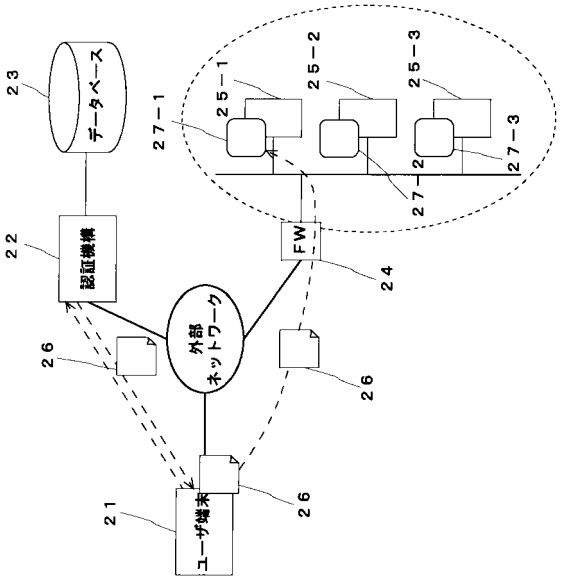
ャートである。図８ではＳ８－８からＳ８－１１に相当する。
【００４７】
ＦＷ４５がユーザ端末４１からのアクセスを検知すると（Ｓ９－１）、ＦＷ４５の通信状態監視機能６７は着信パケットを捕捉し、パケット内データを取得する（Ｓ９－２）。その最初の着信パケットが、ＦＷ４５におけるセキュリティポリシー定義領域６４のセキュリティポリシーに一致しているかどうかを判定し（Ｓ９－３）、一致していればパケットはＦＷ４５を通過し、ユーザと情報リソース間の通信が開始される（Ｓ９－４）。通信開始後、タイマーがセットされ（Ｓ９－５）、タイマー処理がスタートする。通信中、ＦＷ４５は全ての着信及び発信パケットを捕捉し、パケット内部情報を取得、解析、保存する（Ｓ９－６）。保存したパケット内部情報を時系列に従って累積させていくことで、通信状況を示す通信状態情報を構築する（Ｓ９－７）。この通信状態情報を新たに取得したパケット内部情報と照合することで、通信の整合性を判断する（Ｓ９－８）。通信に整合性があると判断された時点でタイマーは一度リセットされる。また、捕捉したパケットを適宜サンプリングし、セキュリティポリシーに一致しているかを検査するステップ（Ｓ９－３）を処理に組み込むことも十分例として考えられる。通信の終了を示すパケットを検知した場合（Ｓ９－９）、通信終了と認識し、通信状態監視機能６７はセキュリティポリシー編集機能６３へアクセス許可削除要求を出し（Ｓ９－１０）アクセス許可リストを変更する。通信が異常終了した場合、基本的にはタイムアウト処理を行い、タイムアウトをもって通信終了と認識する。また、通信中、単にタイムアウトが起こった場合も同様に通信終了と認識する。
【００４８】
尚、本発明は、図４乃至図６の構成図に示された機能を実現する認証機構プログラムあるいはファイアウォール機構プログラム、または図７乃至図９のフローチャートに示される手順を備えるプログラムによって実現することができる。
【００４９】
【発明の効果】
以上説明したように、本発明によれば、認証機構を通さずに保護情報リソースに直接アクセスするユーザに対してアクセスを禁止することができ、アクセス対象情報リソースが通信に使用するプロトコルによらず動的にユーザのアクセスを制御できる。また、並列型ＳＳＯにおいてアクセス制御を行うモジュールとユーザの認証機構が分離しているので、ユーザの増減やアクセス対象の変更等を動的に、しかもセキュリティ強度に影響を与えることなく変更できる。ここでは並列型ＳＳＯで通常必要とされるエージェントモジュールを必要としない。
【図面の簡単な説明】
【図１】従来の直列型ＳＳＯにおけるシステム構成図
【図２】従来の並列型ＳＳＯにおけるシステム構成図
【図３】認証機構とＦＷの機能ブロック図
【図４】本発明を適用したネットワークセキュリティシステムの一実施形態の構成図
【図５】図４のネットワークセキュリティーシステムにおいて認証機構を中心に示した機能構成図
【図６】図５のネットワークセキュリティーシステムにおいてＦＷを中心に示した機能構成図
【図７】本実施形態における認証機構側のフローチャート
【図８】本実施形態におけるＦＷ側のフローチャート
【図９】本実施形態におけるＦＷの通信監視のフローチャート
【符号の説明】１１、２１、３Ｂ、４１…ユーザ端末、１２、２２、３０、４４…認証機構、１３、２３、３２、４３…データベース、１４、２４、３６、４５…ＦＷ、１５－１、１５－２、１５－３、２５－１、２５－２、２５－３、３Ａ、４８－１、４８－２、４８－３、６６－１、６６－２、６６－３…情報リソース、２６…クッキー、２７－１、２７－２、２７－３…モジュール、３１…ユーザ認証手段、３３…データ生成手段、３４ａ

…データ暗号化手段、３４ｂ、３７ａ…情報送受信手段、３７ｂ…認証手段、５６…データ、３８…セキュリティポリシー変更手段、３９…通信状態監視手段、４２…認証サーバ、３５、４６…送信データ、４７、６４…セキュリティポリシー定義領域、５０…認証Ｉ／Ｆ、５１…送信元情報取得機能、５２…リソース・ユーザ対応リスト、５３…データベース連携機能、５４…データフォーマット生成機能、５５…データテンプレート、５７…データ暗号化機能、５８、６０…情報送受信機能、６１…認証機構認証機能、６２…受信データ解析機能、６３…セキュリティポリシー編集機能、６５－１、６５－２、６５－３…アクセス許可リスト、６７…通信状態監視機能。

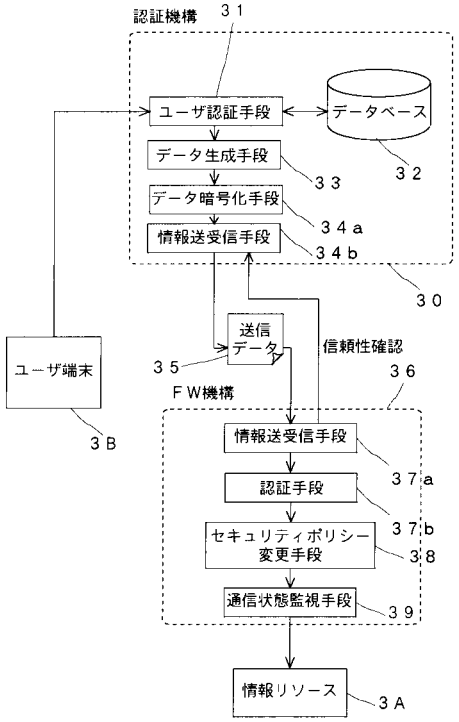
【図１】



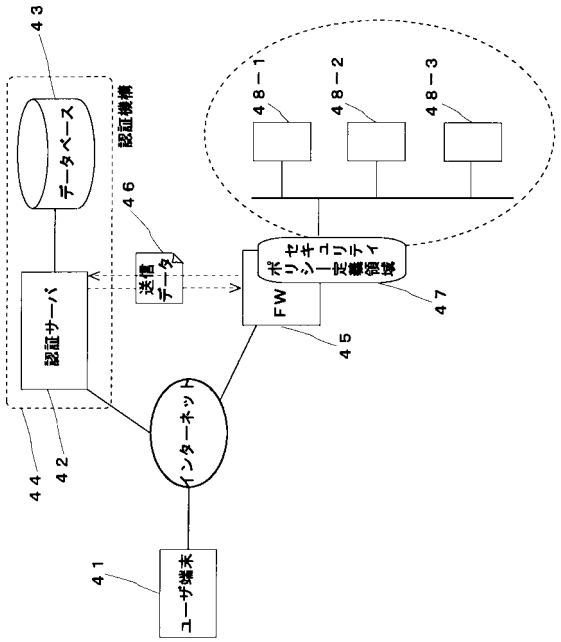
【図２】



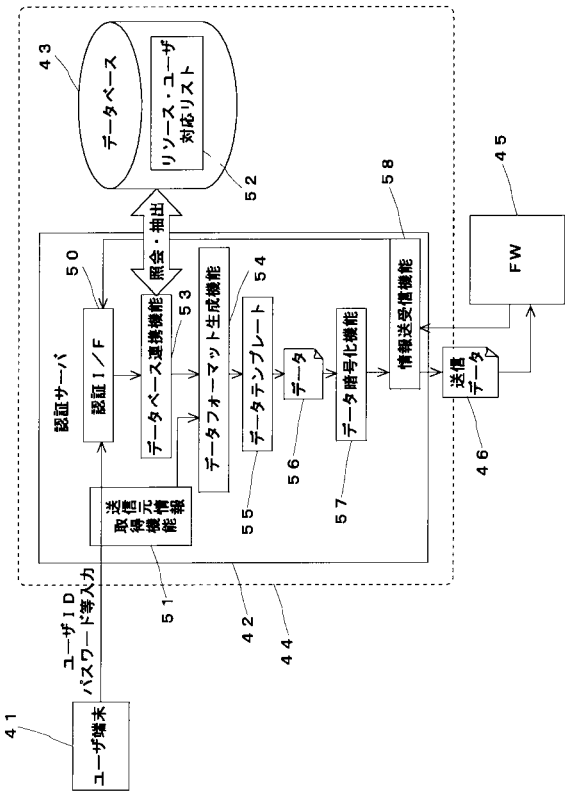
【図３】


認証機構
31
ユーザ認証手段
データベース
32
データ生成手段
33
データ暗号化手段
34a
情報送受信手段
34b
30
送信データ
35
信頼性確認
36
ユーザ端末
3B
FW機構
情報送受信手段
37a
認証手段
37b
セキュリティポリシー変更手段
38
通信状態監視手段
39
情報リソース
3A

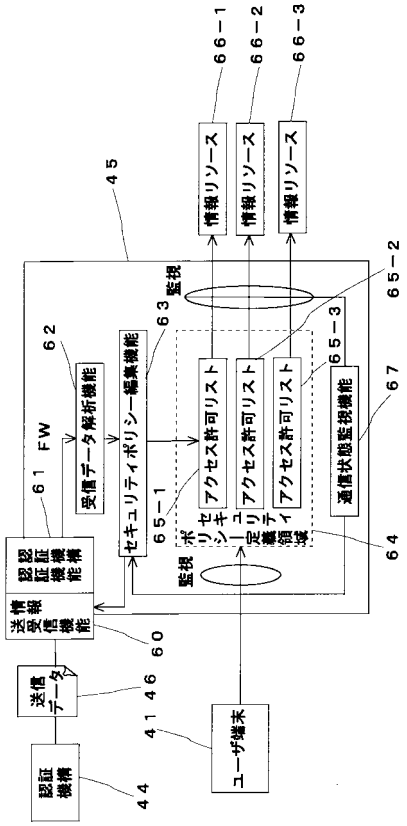
【図４】


43
データベース
認証機構
48-1
48-2
48-3
46
送信データ
ポリシー定義機構
FW
47
認証サーバ
45
インターネット
44
42
41
ユーザ端末

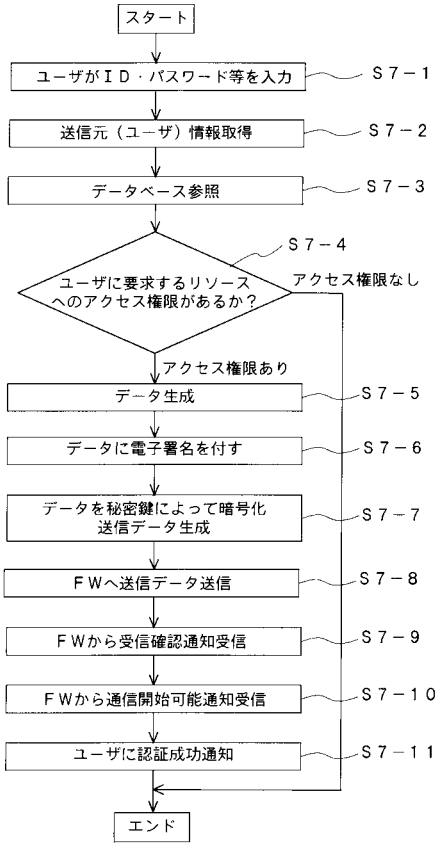
【図５】


43
データベース
リソース・ユーザ対応リスト
52
照会・抽出
58
45
FW
50
認証サーバ
認証I/F
53
データベース連携機能
データフォーマット生成機能
54
データテンプレート
データ
56
データ暗号化機能
57
情報送受信機能
送信データ
46
送信元情報機能
51
55
42
44
ユーザID
パスワード等入力
41
ユーザ端末

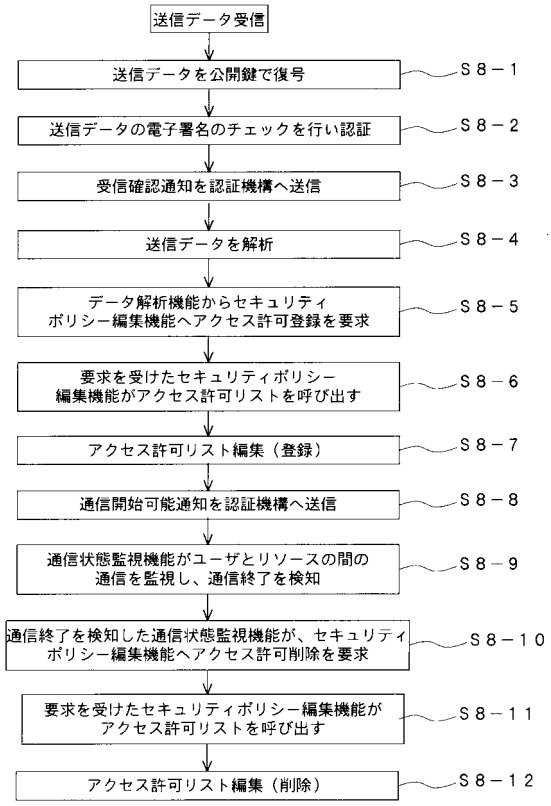
【図６】


66-1
66-2
66-3
情報リソース
情報リソース
情報リソース
45
監視
63
65-2
62
FW
61
受信データ解析機能
セキュリティポリシー編集機能
65-1
アクセス許可リスト
アクセス許可リスト
アクセス許可リスト
65-3
通信状態監視機能
67
ポリシー定義機構
64
監視
認証機能
送信機能
60
送信データ
46
41
ユーザ端末
認証機構
44

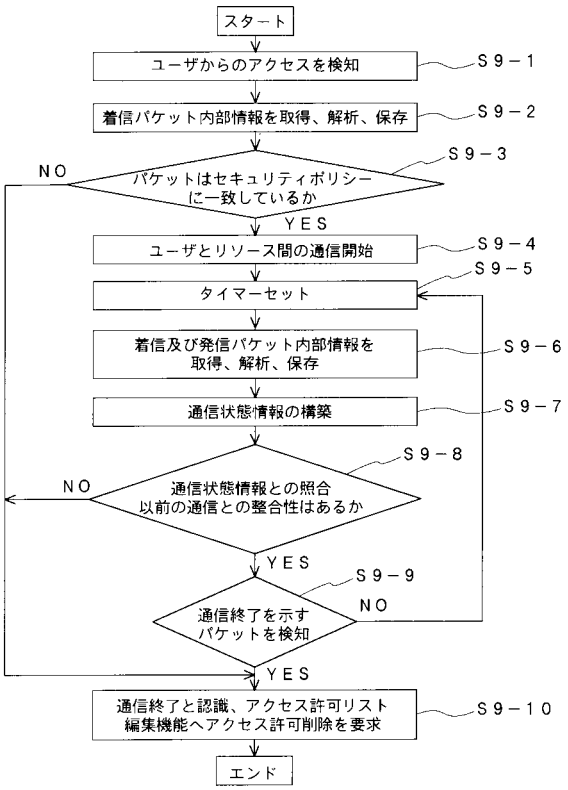
【図７】


スタート
ユーザがＩＤ・パスワード等を入力
Ｓ７－１
送信元（ユーザ）情報取得
Ｓ７－２
データベース参照
Ｓ７－３
Ｓ７－４
ユーザに要求するリソースへのアクセス権限があるか？
アクセス権限なし
アクセス権限あり
データ生成
Ｓ７－５
データに電子署名を付す
Ｓ７－６
データを秘密鍵によって暗号化送信データ生成
Ｓ７－７
ＦＷへ送信データ送信
Ｓ７－８
ＦＷから受信確認通知受信
Ｓ７－９
ＦＷから通信開始可能通知受信
Ｓ７－１０
ユーザに認証成功通知
Ｓ７－１１
エンド

【図８】


送信データ受信
送信データを公開鍵で復号
Ｓ８－１
送信データの電子署名のチェックを行い認証
Ｓ８－２
受信確認通知を認証機構へ送信
Ｓ８－３
送信データを解析
Ｓ８－４
データ解析機能からセキュリティポリシー編集機能へアクセス許可登録を要求
Ｓ８－５
要求を受けたセキュリティポリシー編集機能がアクセス許可リストを呼び出す
Ｓ８－６
アクセス許可リスト編集（登録）
Ｓ８－７
通信開始可能通知を認証機構へ送信
Ｓ８－８
通信状態監視機能がユーザとリソースの間の通信を監視し、通信終了を検知
Ｓ８－９
通信終了を検知した通信状態監視機能が、セキュリティポリシー編集機能へアクセス許可削除を要求
Ｓ８－１０
要求を受けたセキュリティポリシー編集機能がアクセス許可リストを呼び出す
Ｓ８－１１
アクセス許可リスト編集（削除）
Ｓ８－１２

【図９】


スタート
ユーザからのアクセスを検知
Ｓ９－１
着信パケット内部情報を取得、解析、保存
Ｓ９－２
Ｓ９－３
ＮＯ
パケットはセキュリティポリシーに一致しているか
ＹＥＳ
ユーザとリソース間の通信開始
Ｓ９－４
Ｓ９－５
タイマーセット
着信及び発信パケット内部情報を取得、解析、保存
Ｓ９－６
通信状態情報の構築
Ｓ９－７
Ｓ９－８
ＮＯ
通信状態情報との照合以前の通信との整合性はあるか
ＹＥＳ
Ｓ９－９
通信終了を示すパケットを検知
ＮＯ
ＹＥＳ
通信終了と認識、アクセス許可リスト編集機能へアクセス許可削除を要求
Ｓ９－１０
エンド

フロントページの続き

Ｆターム(参考) 5B089 GA11 GA21 HA10 JB22 KA17
5J104 AA07 AA12 KA01 PA07