(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4315696号
(P4315696)
(45)発行日　平成21年8月19日(2009.8.19)　(24)登録日　平成21年5月29日(2009.5.29)

(51)Int.Cl.　F I
*G06F 13/00 (2006.01)*　G06F 13/00 353C
G06F 13/00 351Z

請求項の数 7　(全 31 頁)

(21)出願番号　特願2003-32727(P2003-32727)
(22)出願日　平成15年2月10日(2003.2.10)
(65)公開番号　特開2004-5427(P2004-5427A)
(43)公開日　平成16年1月8日(2004.1.8)
審査請求日　平成17年6月9日(2005.6.9)
(31)優先権主張番号　特願2002-93954(P2002-93954)
(32)優先日　平成14年3月29日(2002.3.29)
(33)優先権主張国　日本国(JP)

(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　100092152
弁理士　服部　毅巖
(72)発明者　益重　明徳
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　平尾　幸夫
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　安部　雅英
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】ホスト端末エミュレーションプログラム、中継用プログラムおよびホスト端末エミュレーション方法

(57)【特許請求の範囲】
【請求項１】
非同期の双方向通信を行う第１のプロトコルの通過を拒否し、一方からの要求に受信側が応答する手順で通信を行う第２のプロトコルの通過を許可するファイアウォールを経由して接続され、前記第１のプロトコルによる遠隔地からの対話型操作が可能なホストコンピュータに対する端末機能を実現するためのホスト端末エミュレーションプログラムにおいて、
コンピュータに、
前記ファイアウォールを経由して接続された中継装置との間で、前記第２のプロトコルのデータを受信するための受信用接続を予め確立し、
操作入力に応答して前記ホストコンピュータにデータを送信する際に、前記中継装置に対し、前記第２のプロトコルのデータを送信するための送信用接続を確立し、
操作入力に応答して前記第１のプロトコルのデータ形式で作成された送信データを前記第２のプロトコルのデータ形式に変換し、変換された前記送信データを、前記送信用接続を用いて前記第２のプロトコルで前記中継装置に送信し、
前記ホストコンピュータから出力されたホスト発データを、前記受信用接続を用いて前記中継装置から前記第２のプロトコルで受信し、前記第１のプロトコルのデータ形式に変換する、
処理を実行させることを特徴とするホスト端末エミュレーションプログラム。
【請求項２】

前記ホストコンピュータから出力された前記ホスト発データを受信した際には、再度、前記中継装置との間で、前記第２のプロトコルのデータを受信するための受信用接続を確立することを特徴とする請求項１記載のホスト端末エミュレーションプログラム。

【請求項３】

前記受信用接続の確立可能期間のタイムアウトが発生した際には、再度、前記中継装置との間で、前記第２のプロトコルのデータを受信するための受信用接続を確立することを特徴とする請求項１記載のホスト端末エミュレーションプログラム。

【請求項４】

前記受信用接続を確立する際には、前記中継装置内の前記ホストコンピュータからのデータ受信を待機する機能の起動要求を、前記中継装置に対して出力することを特徴とする請求項１記載のホスト端末エミュレーションプログラム。

【請求項５】

ネットワーク上で一意に識別可能な識別情報を生成するか、または前記中継装置で生成された前記識別情報を受け取り、前記中継装置との前記送信用接続および前記受信用接続の確立の際には、前記識別情報を含む接続要求を前記中継装置に送信することを特徴とする請求項１記載のホスト端末エミュレーションプログラム。

【請求項６】

非同期の双方向通信を行う第１のプロトコルの通過を拒否し、一方からの要求に受信側が応答する手順で通信を行う第２のプロトコルの通過を許可するファイアウォールを経由して接続されるクライアントコンピュータと、前記第１のプロトコルによる遠隔地からの対話型操作が可能なホストコンピュータとの間のデータを中継するための中継用プログラムにおいて、

コンピュータに、

前記クライアントコンピュータとの間で、前記第２のプロトコルによる受信用接続を予め確立し、

前記クライアントコンピュータからデータを受け取る際に、前記クライアントコンピュータとの間で前記第２のプロトコルによる送信用接続を確立し、

前記クライアントコンピュータから送られた送信データを前記第１のプロトコルのデータ形式に変換し、変換された前記送信データを、前記送信用接続を用いて前記ホストコンピュータに送信し、

前記第１のプロトコルにより前記ホストコンピュータから送られた前記第１のプロトコルのデータ形式のホスト発データを、前記第２のプロトコルのデータ形式に変換し、変換された前記ホスト発データを、前記受信用接続を用いて前記クライアントコンピュータに送信する、

処理を実行させることを特徴とする中継用プログラム。

【請求項７】

非同期の双方向通信を行う第１のプロトコルの通過を拒否し、一方からの要求に受信側が応答する手順で通信を行う第２のプロトコルの通過を許可するファイアウォールを経由して接続され、前記第１のプロトコルによる遠隔地からの対話型操作が可能なホストコンピュータに対する端末機能を実現するためのホスト端末エミュレーション方法において、

前記ファイアウォールを経由して接続された中継装置との間で、前記第２のプロトコルのデータを受信するための受信用接続を予め確立し、

操作入力に応答して前記ホストコンピュータにデータを送信する際に、前記中継装置に対し、前記第２のプロトコルのデータを送信するための送信用接続を確立し、

操作入力に応答して前記第１のプロトコルのデータ形式で作成された送信データを前記第２のプロトコルのデータ形式に変換し、変換された前記送信データを、前記送信用接続を用いて前記第２のプロトコルで前記中継装置に送信し、

前記ホストコンピュータから出力されたホスト発データを、前記受信用接続を用いて前記中継装置から前記第２のプロトコルで受信し、前記第１のプロトコルのデータ形式に変換する、

ことを特徴とするホスト端末エミュレーション方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はホスト端末エミュレーションプログラム、中継用プログラムおよびホスト端末エミュレーション方法に関し、特にゲートウェイを経由したホストと端末間の通信を行うためのホスト端末エミュレーションプログラム、中継用プログラム、およびホスト端末エミュレーション方法に関する。

【０００２】

【従来の技術】

従来のコンピュータネットワークの仕組みとして、データ処理を集中して行うホストコンピュータ（以下、単にホストという）に対して端末装置（以下、単に端末という）により対話型でアクセスする方法がある。対話型のアクセスとは、所定のアカウントでホストにログインし、操作入力に応答したコマンドをホストに入力したり、ホストからの出力データを表示したりするアクセス形態である。このようなシステムは、ホスト集中処理システムと呼ばれる。

【０００３】

ホスト集中処理システムでは、データ処理がホストで集中して行われ、端末では複雑なデータ処理は行われない。そのため、端末は、操作入力内容をホストに送信する機能と、ホストから送られてきた情報を表示する機能とを備えていればよい。このような端末として、ダム端末が多く用いられていた。

【０００４】

最近は、コンピュータネットワークとして、クライアントサーバシステムが用いられることが多くなっている。クライアントサーバシステムは、ワークステーションやパーソナルコンピュータなど、それぞれスタンドアロンとしても機能できるコンピュータ同士をネットワーク接続したシステムである。

【０００５】

クライアントサーバシステムが普及したことにより、各ユーザが、クライアントコンピュータ（以下、単にクライアントという）として機能するワークステーションやパーソナルコンピュータを１台ずつ使用できるようになった。ただし、従来からのホスト集中処理に適した業務も残っているため、同一ネットワーク上に、ホスト集中処理システムとクライアントサーバシステムとの両方が構築されることがある。

【０００６】

そこで、近年は、アプリケーションソフトにより、端末としての機能をクライアントに実装し、クライアントに実装された端末の機能を用いてホストを利用する手法が主流になっている。以下、このようなシステムを、ホスト連携処理システムと呼ぶ。

【０００７】

現在、ホスト連携処理としては、ＴＮ(TelNet)プロトコル（TN3270標準（RFC1646）、TN3270E標準（RFC1647）に準拠などがある）などのインターネット／イントラネット用のプロトコルを利用した通信が実現されている。また、永続性のあるＴＣＰ／ＩＰソケットコネクションを通してクライアントシステムとサーバシステムとを接続し、同様に永続性のあるＴＣＰ／ＩＰソケットコネクションを通してサーバシステムと従来型のホストシステムを接続する技術も考えられている（たとえば、特許文献１参照）。これらの技術により、ホスト連携処理が可能となる。

【０００８】

なお、クライアントからホストへのアクセスは、基本的にはＬＡＮ(Local Area Network)経由で行われるが、電話回線の利用などにより、クライアントと遠隔地のホストとの連携を実現する技術も一般的に用いられている。

【０００９】

また、最近はインターネットの普及により、クライアントとホストとの連携の分野でもイ

ンターネット経由、あるいはＴＣＰ／ＩＰ(Transmission Control Protocol/Internet Protocol)、もしくはＴＣＰ／ＩＰ上のアプリケーションプロトコルを利用した遠隔ホストとの連携技術が確立されている。インターネット経由でホストの機能を利用できることで、ホスト集中処理システムの利便性が向上する。

【００１０】

ところが、インターネット／イントラネット上のネットワーク通信は、セキュリティ上の問題を伴う。インターネット／イントラネットでのセキュリティ上の問題として、以下の４点が挙げられる。

【００１１】

（１）不正アクセスなどのネットワーク攻撃（保護されたネットワーク内のコンピュータを標的とした不正な通信）を受けやすい。

（２）なりすまし（発信元を偽ってアクセスする行為）が可能である。

【００１２】

（３）通信データの盗み読み（他人宛の通信データを不正に取得して、内容を読み取る行為）が可能である。

（４）通信データの改竄（他人宛の通信データの内容を、不正に書き換える行為）が可能である。

【００１３】

インターネット／イントラネットのインフラ上では、上記に挙げたような不正行為を完全に防ぐことは事実上不可能である。そこで不正行為を受けても損害に至らないようにする工夫が必要となる。なお、イントラネットではインターネットに比べれば悪意を持つ第三者の数は少ないと思われるが、存在しないことが保証されるわけではない。よって、イントラネットの危険性はインターネットと同等である。

【００１４】

これらのセキュリティ上の問題の解決手段として様々なものが考案されているが、一般的には次のような対策がとられている。

（１）不正アクセスなどのネットワーク攻撃に対しては、ネットワークを通過するプロトコルを制限することで対応できる。すなわち、全てのプロトコルの通過を許可して、あらゆる攻撃に備えることは困難であり、また膨大なコストが掛かる。そこで、ファイアウォールなどで監視対象のプロトコルやＴＣＰ／ＩＰ接続のポート番号を必要最低限（たとえば、ＨＴＴＰ(HyperText Transfer Protocol)、ＰＯＰ(Post Office Protocol)／ＳＭＴＰ(Simple Mail Transfer Protocol)のみ）に限定する。これにより、注意する対象を狭い範囲に絞り込めるため、安全性を向上させる事ができる。

【００１５】

（２）なりすましに対しては、相手の認証を行うことで対処できる。すなわち、接続した相手が、自分が想定した相手であることを、パスワードなどにより認証する。これにより、相手になりすましている者との通信を防ぐことができる。

【００１６】

（３）通信データの盗み読みに対しては、データの暗号化によって対処することができる。データを暗号化すれば、通信データの内容が、第三者にとって理解不能になる。そのため盗み読み行為の対象となっても、データの内容を知られる事を防ぐことができる。

【００１７】

（４）通信データの改竄に対しては、受信データ毎に改竄の有無を検出することで対処できる。受信データが改竄されたことが検出できれば、改竄されたデータが送られてきても、そのデータを誤って使用することを避ける事ができる。その場合、正しいデータを受け取れるまで相手にデータ再送を要求することで、正しいデータを取得することができる。

【００１８】

【特許文献１】

特表２００１－５０９２８６号公報（第１図）

【００１９】

【発明が解決しようとする課題】
しかし、インターネットやイントラネットを介してホスト連携処理を行う場合、以下の様な理由により、従来の技術では対処不可能なセキュリティ上の問題が発生する。
【００２０】
ホスト連携処理に用いられるＴＮプロトコルは、不正アクセスなどのネットワーク攻撃の対策として、一般的には遮断されている。すなわち、ホスト連携処理を行わないインターネット／イントラネット環境では、ファイアウォールによる通信の制限機能を越えてＴＮ接続で運用することはできない。
【００２１】
ところが、インターネットやイントラネットを介してホスト連携通信を行うには、ファイアウォールによるＴＮプロトコルの通信制限を解除する必要がある。すると、ファイアウォールを経由したＴＮプロトコルでのホスト連携通信が可能となると同時に、危険なセキュリティホールが発生する。
【００２２】
なお、ファイアウォールを通過可能に設定されているＨＴＴＰプロトコルを利用してホスト連携処理を実現できれば、ＴＮプロトコルの通信制限を解除せずにすみ、セキュリティ上の信頼性を維持できる。ただし、ＨＴＴＰプロトコルを用いてホスト連携通信を行うには、以下のような技術的な問題点がある。
【００２３】
すなわち、ホスト集中処理システムでは、ホスト端末とホストとの間の通信が非同期の双方向通信であることが必要である。これは、インターネットやイントラネットを介してホスト連携処理を行う場合にも、任意のタイミングで発生する双方向の通信を処理できなければならないことを意味する。
【００２４】
ところが、ＨＴＴＰクライアントとウェブサーバとの間のＨＴＴＰ通信プロトコルでは、常にクライアント側からの要求にウェブサーバが応答する手順で行われる。この手順を普通に利用する限りは、ホスト側から発せられる任意のタイミングの通信をクライアント側へ送信することができない。従って、クライアント側からの要求にサーバが応答する手順のプロトコルを利用して、非同期の双方向通信を可能とするための新たな技術が必要となる。また、特許文献１のように永続的なコネクションを利用してＨＴＴＰクライアントとウェブサーバとを接続してしまうと、悪意の第３者に対し、ホストに接続されたコネクションを解析するための時間を十分に与えることになる。その結果、ファイアウォールで保護されるべきシステムのセキュリティ低下を招いてしまう。
【００２５】
本発明はこのような点に鑑みてなされたものであり、保護されたネットワーク内のホストと、そのネットワーク外のクライアントとによるホスト連携通信を、安全に行うことができるホスト端末エミュレーションプログラム、中継用プログラム、およびホスト端末エミュレーション方法を提供することを目的とする。
【００２７】
【課題を解決するための手段】
本発明の第１の態様では上記課題を解決するために、図１に示すようなホスト端末エミュレーションプログラムが提供される。本発明に係るホスト端末エミュレーションプログラムは、そのホスト端末エミュレーションプログラムを実行するコンピュータを、第１のプロトコルの通過を拒否するファイアウォール２と接続させ、ファイアウォール２を経由して第１のプロトコルによる遠隔地からの対話型操作が可能なホストコンピュータ４に対する端末機能を実現するためのプログラムである。本発明に係るホスト端末エミュレーションプログラムは、コンピュータに以下の処理を実行させることができる。
【００２８】
コンピュータは、第１のプロトコルとファイアウォール２の通過が許可された第２のプロトコルとの相互のデータ形式変換機能を有し、ファイアウォール２を経由して接続された

中継装置３との間で、第２のプロトコルのデータを受信するための受信用接続を予め確立する（ステップＳ１）。次に、コンピュータは、操作入力に応答してホストコンピュータ４にデータを送信する際に、中継装置３に対し、第２のプロトコルのデータを送信するための送信用接続を確立する（ステップＳ２）。送信用接続を用いて、操作入力されたデータを第２のプロトコルで中継装置３に送信する（ステップＳ３）。受信用接続を用いて、ホストコンピュータ４から出力されたデータを、中継装置３から第２のプロトコルで受信する（ステップＳ９）。

【００２９】

このようなホスト端末エミュレーションプログラムによれば、ホスト端末エミュレーションプログラムを実行するコンピュータは、ファイアウォール２を通過可能な第２のプロトコルにより、中継装置３に対してデータを送信する。また、第２のプロトコルによる受信用接続を予め確立していることで、ホストコンピュータ４からいつデータが出力されても、すぐに、中継装置３を介してそのデータがコンピュータで受信される。

【００３０】

また、本発明の第２の態様では上記課題を解決するために、ファイアウォールを経由して接続されるクライアントコンピュータと、第１のプロトコルによる遠隔地からの対話型操作が可能なホストコンピュータとの間のデータを中継するための中継用プログラムにおいて、コンピュータに、前記クライアントコンピュータとの間で、前記ファイアウォールの通過が許可された第２のプロトコルによる受信用接続を予め確立し、前記クライアントからデータを受け取る際に、前記クライアントとの間で前記第２のプロトコルによる送信用接続を確立し、前記送信用接続を用いて、前記クライアントコンピュータから送られたデータを、前記第１のプロトコルに変換して前記ホストコンピュータに送信し、前記第１のプロトコルにより前記ホストコンピュータから送られたデータを、前記第２のプロトコルに変換して、前記受信用接続を用いて前記クライアントコンピュータに送信する、処理を実行させることを特徴とする中継用プログラムが提供される。

【００３１】

このような中継用プログラムを実行するコンピュータによれば、コンピュータにより、クライアントコンピュータとの間で、第２のプロトコルによる受信用接続が予め確立される。また、コンピュータにより、クライアントからデータを受け取る際に、クライアントコンピュータとの間で第２のプロトコルによる送信用接続が確立される。そして、コンピュータにより、送信用接続を用いて、クライアントコンピュータから送られたデータが第１のプロトコルに変換され、ホストコンピュータに送信される。また、コンピュータにより、第１のプロトコルによりホストコンピュータから送られたデータが、第２のプロトコルに変換され、受信用接続を用いてクライアントコンピュータに送信される。

【００３２】

また、本発明の第３の態様では上記課題を解決するために、第１のプロトコルの通過を拒否するファイアウォールを経由して接続され、前記第１のプロトコルによる遠隔地からの対話型操作が可能なホストコンピュータに対する端末機能を実現するためのホスト端末エミュレーション方法において、前記第１のプロトコルと前記ファイアウォールの通過が許可された第２のプロトコルとの相互のデータ形式変換機能を有し、前記ファイアウォールを経由して接続された中継装置との間で、前記第２のプロトコルのデータを受信するための受信用接続を予め確立し、操作入力に応答して前記ホストコンピュータにデータを送信する際に、前記中継装置に対し、前記第２のプロトコルのデータを送信するための送信用接続を確立し、前記送信用接続を用いて、操作入力されたデータを前記第２のプロトコルで前記中継装置に送信し、前記受信用接続を用いて、前記ホストコンピュータから出力されたデータを、前記中継装置から前記第２のプロトコルで受信する、ことを特徴とするホスト端末エミュレーション方法が提供される。

【００３３】

このようなホスト端末エミュレーション方法によれば、上記本発明の第１の態様に係るホスト端末エミュレーションプログラムを実行するコンピュータと同様の処理が行われる。

【００３９】
【発明の実施の形態】
以下、本発明の実施の形態を図面を参照して説明する。
まず、実施の形態に適用される発明の概要について説明し、その後、本発明の実施の形態の具体的な内容を説明する。
【００４０】
図１は、実施の形態に適用される発明の概念図である。図１に示すように、ホスト連携処理システムは、クライアントコンピュータ（クライアント）１、ファイアウォール２、中継装置３、およびホストコンピュータ（ホスト）４で構成される。クライアント１とファイアウォール２とは、ネットワーク５に接続されている。また、ファイアウォール２、中継装置３およびホスト４は、ネットワーク６に接続されている。ネットワーク６は、ファイアウォール２によってネットワーク５に接続されたコンピュータからのアクセスに対して保護されている。
【００４１】
ここで、ホスト４は、第１のプロトコルにより、対話型のアクセスが可能である。対話型のアクセスとは、たとえば、ｔｅｌｎｅｔのように、ホスト４にログインして、対話型で相互作用の入出力を行うアクセス形態である。対話型のアクセスでは、ホスト４への入力と、ホスト４からの出力（入力に対する応答に限らない）とが任意のタイミングで行われる。対話型のアクセスを行うためのプロトコルとしては、たとえば、ＴＮプロトコルがある。
【００４２】
また、ファイアウォール２は、第１のプロトコルの通信を遮断している。すなわち、ネットワーク５上から、直接ホスト４に第１のプロトコルによるアクセスはできない。なお、ファイアウォール２は、第２のプロトコルによる通信は許可している。
【００４３】
そこで、クライアント１をホスト４の端末として機能させるために、以下のような処理が行われる。なお、中継装置３は、第１のプロトコルと第２のプロトコルとの相互のデータ形式変換機能を有している。
【００４４】
まず、クライアント１は、ファイアウォール２を経由して接続された中継装置３との間で、第２のプロトコルのデータを受信するための受信用接続を予め確立する（ステップＳ１）。次に、クライアント１は、操作入力に応答してホスト４にデータを送信する際に、中継装置３に対し、第２のプロトコルのデータを送信するための送信用接続を確立する（ステップＳ２）。そして、送信用接続を用いて、操作入力されたデータを第２のプロトコルで中継装置３に送信する（ステップＳ３）。
【００４５】
中継装置３は、クライアント１から受け取ったデータを第１のプロトコルのデータに変換する（ステップＳ４）。そして、中継装置３は、第１のプロトコルに変換されたデータを、ホスト４に対して送信する（ステップＳ５）。
【００４６】
ホスト４では、対話型の入力が行われると共に、データ処理が実行される（ステップＳ６）。このデータ処理は、クライアント１から送られたデータ（たとえば、ホスト連携）に応じた処理の場合もあるし、所定のタイミングで開始され、出力先としてクライアント１が予め指定された処理の場合もある。
【００４７】
ホスト４のデータ処理が終了すると、処理結果が第１のプロトコルにより、対話型の出力として、ホスト４から中継装置３に送信される（ステップＳ７）。すると、中継装置３は、処理結果のデータ形式を第２のプロトコルに変換して、受信用接続を用いて、処理結果のデータをクライアント１に送信する（ステップＳ８）。そのデータがクライアント１で受信され、表示される（ステップＳ９）。

【００４８】
これにより、ファイアウォール２において、第１のプロトコルの通信を遮断したまま、クライアント１とホスト４との間で、ホスト連携が可能となる。第１のプロトコルがファイアウォール２において遮断されることで、ネットワーク６内のコンピュータに対する第１のプロトコルによる不正アクセスを防止できる。
【００４９】
すなわち、第１のプロトコルは、遠隔地からの対話型操作が可能なプロトコルであるため、ファイアウォール２を通過させてしまうと、保護されたネットワーク６内の全てのコンピュータが、第１のプロトコルによる不正アクセスの危険にさらされてしまう。本発明のように、第１のプロトコルによるアクセスをファイアウォール２で遮断すれば、第１のプロトコルによる不正アクセスから、ネットワーク６上のコンピュータが守られる。
【００５０】
しかも、受信用接続を予め確立しておくことにより、ホスト４から任意のタイミングでデータが出力されても、そのデータをクライアント１で受信することができる。すなわち、ホスト４からファイアウォール２を介して接続されたクライアント１が、ホスト４に直結（たとえば、シリアル通信ケーブルによる接続）された端末（たとえば、ダム端末）と同様に機能することができる。
【００５１】
ところで、図１に示す処理において、中継装置３を一般的なサーバと捉えた場合、クライアント１側からの要求にサーバ（中継装置３）が応答する手順で通信を行うプロトコルを用いた非同期の双方向通信が実現されている。この場合のサーバは、中継装置３からデータの中継機能（ホスト４とのコネクション確立機能やプロトコル変換機能）は不要である。非同期の双方向通信であれば、クライアントとサーバとの双方から、任意のタイミングでデータを相手に送信することが可能となる。たとえば、通信プロトコルとしてＨＴＴＰプロトコルを用いた場合、ウェブサーバからＨＴＴＰクライアントに対して能動的にデータを配信し、そのデータの内容をＨＴＴＰクライアントに表示させることも可能となる。
【００５２】
しかも、クライアントとサーバとの間のコネクションは、データの受け渡しが行われる毎に切断することができる。この場合、クライアントは、受信用接続を用いてデータを受け取ると、既存の受信用接続を切断し、次のデータ受信用に、受信用接続を再度確立する。これにより、悪意の第３者によりコネクションの内容が解析される危険性が減る。その結果、永続的な１つのコネクションを用いて双方向通信を行う場合に比べ、高いセキュリティを保つことができる。
【００５３】
［第１の実施の形態］
図２は、第１の実施の形態に係るホスト連携処理のシステム構成例を示す図である。第１の実施の形態では、複数のクライアント１００，１００ａが、インターネット１０を介してファイアウォール２１０に接続されている。同様に、複数のクライアント４１０，４２０がイントラネット２０を介してファイアウォール２１０に接続されている。ファイアウォール２１０は、基幹ネットワーク３０を介して、中継用コンピュータ３００、ＴＮ接続ゲートウェイ２２０、およびホスト２３０に接続されている。ここで、基幹ネットワーク３０は、外部からの不正なアクセスに対して、高いセキュリティが要求されるコンピュータネットワークである。
【００５４】
クライアント１００，１００ａ，４１０，４２０は、ホスト端末機能を有するコンピュータである。ホスト端末機能は、アプリケーションソフトウェアによって実現されている。ホスト端末機能としては、たとえば、ＴＮプロトコルによる通信機能がある。ここで、ＴＮプロトコルは、telnet（仮想端末）のコマンドでホスト連携用データストリームを伝送するための仕掛け（＝プロトコル）である。ＴＮプロトコルとtelnetの違いは、telnetがパソコン通信のように１文字毎の伝送であり入力フィールドのようなものがないのに対し

、ＴＮプロトコルではブロック単位の転送でありフィールドや属性などの制御が可能となる点である。

【００５５】

ファイアウォール２１０は、インターネット１０から基幹ネットワーク３０へのアクセスを制限するためのコンピュータである。アクセス制限は、ポート番号を指定して行うことができる。第１の実施の形態では、ＨＴＴＰによるアクセスのみを通過させ、他のアクセスを遮断する。一般的に、ＨＴＴＰのポート番号は８０である。ＨＴＴＰは、ウェブサーバにおいて、コンテンツの配信に利用されるプロトコルである。そのため、ＨＴＴＰ通信に対する不正アクセス等からウェブサーバを保護するための様々な技術が考えられている。したがって、ＨＴＴＰ通信がファイアウォール２１０を通過できるようにしても、基幹ネットワーク３０内の安全性を保つことが可能である。

【００５６】

中継用コンピュータ３００は、クライアント１００，１００ａ，４１０，４２０とホスト２３０との間の通信データを中継するコンピュータである。具体的には、中継用コンピュータ３００は、クライアント１００，１００ａ，４１０，４２０から出力されたＨＴＴＰ要求をファイアウォール２１０を介して受信すると、そのＨＴＴＰ要求をＴＮプロトコルのデータに変換する。中継用コンピュータ３００は、ＴＮプロトコルに変換されたデータを、ＴＮ接続ゲートウェイ２２０を介してホスト２３０に送信する。また、中継用コンピュータ３００は、ホスト２３０から出力されたＴＮプロトコルの応答データを受信すると、そのＴＮプロトコルの応答データをＨＴＴＰによる応答データ（ＨＴＴＰ応答）に変換する。そして、中継用コンピュータ３００は、ＨＴＴＰ応答を、ファイアウォール２１０を介して、クライアント１００，１００ａ，４１０，４２０宛てに、ＨＴＴＰで送信する。

【００５７】

ＴＮ接続ゲートウェイ２２０は、ＴＮプロトコルによるホスト２３０との間の通信を行うためのゲートウェイである。第１の実施の形態では、中継用コンピュータ３００を経由して、ＴＮプロトコルの要求を受け取り、そのＴＮプロトコルの要求に従って、ホスト２３０にアクセスする。

【００５８】

ホスト２３０は、各種データ処理を実行する汎用コンピュータである。ホスト２３０は、たとえば、クライアント１００，１００ａ，４１０，４２０からの要求に応答して処理を実行する。また、ホスト２３０は、予め設定された時刻に、予め指定された処理を自動的に実行し、処理結果をクライアント１００，１００ａ，４１０，４２０に送信する場合もある。

【００５９】

図３は、本発明の実施の形態に用いるクライアントのハードウェア構成例を示す図である。クライアント１００は、ＣＰＵ(Central Processing Unit)１０１によって装置全体が制御されている。ＣＰＵ１０１には、バス１０７を介してＲＡＭ(Random Access Memory)１０２、ハードディスクドライブ（ＨＤＤ:Hard Disk Drive）１０３、グラフィック処理装置１０４、入力インタフェース１０５、および通信インタフェース１０６が接続されている。

【００６０】

ＲＡＭ１０２には、ＣＰＵ１０１に実行させるＯＳ(Operating System)のプログラムやアプリケーションプログラムの少なくとも一部が一時的に格納される。また、ＲＡＭ１０２には、ＣＰＵ１０１による処理に必要な各種データが格納される。ＨＤＤ１０３には、ＯＳやアプリケーションプログラムが格納される。

【００６１】

グラフィック処理装置１０４には、モニタ１１が接続されている。グラフィック処理装置１０４は、ＣＰＵ１０１からの命令に従って、画像をモニタ１１の画面に表示させる。入力インタフェース１０５には、キーボード１２とマウス１３とが接続されている。入力イ

ンタフェース１０５は、キーボード１２やマウス１３から送られてくる信号を、バス１０７を介してＣＰＵ１０１に送信する。

【００６２】

通信インタフェース１０６は、インターネット１０に接続されている。通信インタフェース１０６は、インターネット１０を介して、他のクライアントとの間でデータの送受信を行う。

【００６３】

以上のようなハードウェア構成によって、第１の実施の形態のクライアント１００の処理機能を実現することができる。なお、図３には、クライアント１００のハードウェア構成例を示したが、他のクライアント１００ａ，４１０，４２０、ファイアウォール２１０、中継用コンピュータ３００、ＴＮ接続ゲートウェイ２２０、およびホスト２３０も同様のハードウェア構成で実現することができる。

【００６４】

ところで、図２に示したシステムは、ファイアウォール２１０で保護された基幹ネットワーク３０内のホスト２３０と、その基幹ネットワーク３０外のクライアント１００，１００ａ，４１０，４２０との間のホスト連携処理を実現するものである。ＨＴＴＰは、クライアント１００，１００ａ，４１０，４２０からの要求に対して応答を行う構造で完結するプロトコルである。すなわち、ＨＴＴＰの要求を受け付ける側（ウェブサーバ）は、クライアント１００，１００ａ，４１０，４２０からの要求がない限り、クライアント１００，１００ａ，４１０，４２０へのデータ送信は行わない。そのため通常の手段では、ＨＴＴＰで双方向発のリアルタイム通信を実現することができない。

【００６５】

一方、ホスト連携処理は、ホスト端末側、ホスト２３０側どちらからも任意のタイミングで通信が発生する通信である。そこで、第１の実施の形態では、以下のような機能によって、ＨＴＴＰを介したホスト連携処理を実現する。

【００６６】

図４は、ホスト連携処理に必要な機能を示すブロック図である。図４に示すように、クライアント１００は、ホスト端末エミュレータ１１０、プロトコル制御部１２０、およびＨＴＴＰ制御部１３０を有している。また、中継用コンピュータ３００は、ウェブサーバ３１０と中継デーモン３２０とを有している。

【００６７】

クライアント１００内のホスト端末エミュレータ１１０は、ホスト２３０の端末として機能する。具体的には、ホスト端末エミュレータ１１０は、ユーザからのキーボード１２やマウス１３に対する操作入力を検知し、操作入力に応じた入力データを、ＴＮプロトコルでプロトコル制御部１２０に渡す。また、ホスト端末エミュレータ１１０は、プロトコル制御部１２０から画面表示用のデータ（たとえば、キャラクタコード）をＴＮプロトコルで受け取ると、受け取ったデータに応じた情報（たとえば、キャラクタコードに対応する文字）をクライアント１００のモニタ１１に表示する。

【００６８】

また、ホスト端末エミュレータ１１０は、起動された直後にも、ホストからのデータ受信の待機を中継用コンピュータ３００に指示するデータ（受信要求）を、ＴＮプロトコルでプロトコル制御部１２０に渡す。さらに、ホスト端末エミュレータ１１０は、受信要求に対する応答を受け取ったときには、再度、受信要求を、ＴＮプロトコルでプロトコル制御部１２０に渡す。

【００６９】

プロトコル制御部１２０は、ホスト端末エミュレータ１１０とＨＴＴＰ制御部１３０との間で受け渡されるデータのプロトコル変換を行う。具体的には、プロトコル制御部１２０は、ホスト端末エミュレータ１１０から渡された入力データを、ＨＴＴＰプロトコルのデータ（ＨＴＴＰ要求）に変換し、ＨＴＴＰ制御部１３０に渡す。また、プロトコル制御部１２０は、ＨＴＴＰ制御部１３０からＨＴＴＰプロトコルの受信データ（ＨＴＴＰ応答）

を受け取ると、そのデータを、ホスト端末エミュレータ１１０が表示可能なデータ（たとえば、キャラクタコード）に変換して、ホスト端末エミュレータ１１０に渡す。

【００７０】

ＨＴＴＰ制御部１３０は、中継用コンピュータ３００との間のＨＴＴＰによる通信を行う。具体的には、ＨＴＴＰ制御部１３０は、プロトコル制御部１２０から渡されたＨＴＴＰ要求を、インターネット１０を介して、中継用コンピュータ３００宛てに送信する。また、ＨＴＴＰ制御部１３０は、インターネット１０を介して、中継用コンピュータ３００からのＨＴＴＰ応答を受信し、そのＨＴＴＰ応答をプロトコル制御部１２０に渡す。

【００７１】

中継用コンピュータ３００内のウェブサーバ３１０は、ウェブページの閲覧サービスを提供するサーバである。ウェブサーバ３１０は、ウェブページの閲覧要求を受け付けたり、ウェブページを構成するコンテンツを配信するために、ＨＴＴＰによる通信機能を有している。第１の実施の形態では、ウェブサーバ３１０が有するＨＴＴＰの通信機能を利用して、中継用コンピュータ３００とクライアント１００との間のＨＴＴＰ要求やＨＴＴＰ応答の送受信を行う。

【００７２】

また、ウェブサーバ３１０は、拡張機能として、要求代理部３１１と応答待機部３１２とを有している。

要求代理部３１１は、ＨＴＴＰ要求を受信した際に起動される。起動された要求代理部３１１は、ＨＴＴＰ要求により送られたデータの内容を中継デーモン３２０に渡す。その後、要求代理部３１１は、ホスト２３０からの応答があるまで待機する。そして、要求代理部３１１は、データを受信したことによるホスト２３０からの結果通知を中継デーモンから受け取ると、その結果通知をＨＴＴＰ応答としてクライアント１００に送信する。

【００７３】

応答待機部３１２は、受信要求のＨＴＴＰ要求を受信した際に起動される。起動された応答待機部３１２は、ホスト２３０からの応答があるまで待機する。そして、応答待機部３１２は、ホスト２３０が処理を実行したことによる結果通知を中継デーモン３２０から受け取ると、その結果通知に基づいて、受信要求に対するＨＴＴＰ応答を生成して、クライアント１００に送信する。

【００７４】

なお、要求代理部３１１と応答待機部３１２とは、共通のプログラムに基づいて実行させることができる。たとえば、ＩＳＡＰＩ(Internet Server Application Program Interface)に従って記述されたプログラムにおいて、要求代理部３１１と応答待機部３１２との処理機能を定義しておく。そして、ＨＴＴＰ要求において、そのプログラムの実行を指定する。その際、ＨＴＴＰ要求内に、要求代理部３１１と応答待機部３１２とのどちらの機能を起動するのかを指定するパラメタを含めておく。これにより、中継用コンピュータ３００では、ＨＴＴＰ要求に応じた拡張機能（要求代理部３１１または応答待機部３１２）が実行される。

【００７５】

中継デーモン３２０は、ウェブサーバ３１０とホスト２３０との間のデータの送受信を中継する。なお、第１の実施の形態では、中継用コンピュータ３００とホスト２３０との間のデータの送受信は、ＴＮプロトコルで行われる。

【００７６】

このとき、中継用コンピュータ３００からホスト２３０に対してＴＮプロトコルによる直接のデータ入出力を行うこともできるし、ＴＮ接続ゲートウェイ２２０を介してデータ入出力を行うこともできる。ＴＮ接続ゲートウェイ２２０を介してデータ入出力を行う場合、中継デーモン３２０は、ウェブサーバ３１０から受け取ったデータを、ＴＮプロトコルのデータに変換し、ＴＮ接続ゲートウェイ２２０に渡す。ホスト２３０に対して入力されたデータに対する結果通知は、ＴＮ接続ゲートウェイ２２０を介して、ホスト２３０から中継デーモン３２０へ渡される。

【００７７】
ホスト２３０からの結果通知を受け取った中継デーモン３２０は、その結果通知をウェブサーバ３１０に渡す。
このような構成のシステムでは、クライアント１００と中継用コンピュータ３００との間に、２つの通信経路３０，４０が確立される。図４では、通信経路３０，４０を点線の枠で示している。通信経路３０は、クライアント１００からホスト２３０へデータを送信するための通信経路である。通信経路４０は、ホスト２３０からのデータをクライアント１００で受信するための通信経路である。
【００７８】
データ送信の通信経路３０で通信を行う際には、クライアント１００と中継用コンピュータ３００との間は、送信用接続（コネクション）３１が確立される。送信用接続３１は、ＨＴＴＰ制御部１３０からウェブサーバ３１０に対して、データをホスト２３０に入力するためのＨＴＴＰ要求が出されたときから、そのＨＴＴＰ要求に対するＨＴＴＰ応答が返されるまでの間確立している。
【００７９】
データ受信の通信経路４０で通信を行う際には、クライアント１００と中継用コンピュータ３００との間は、受信用接続（コネクション）４１が確立される。受信用接続４１は、ＨＴＴＰ制御部１３０からウェブサーバ３１０に対して、受信要求のＨＴＴＰ要求が出されたときから、そのＨＴＴＰ要求に対するＨＴＴＰ応答が返されるまでの間確立している。ただし、ＨＴＴＰ応答が返されると、即座に、次の受信要求のＨＴＴＰ要求が出される。そのため、受信用接続４１は、途中で瞬間的に接続状態が途絶えることはあるが、実質的には常時確立している。ここでいう実質的に受信用接続４１が常時確立しているとは、ホスト２３０からデータがいつ出力されても、そのデータをクライアント１００に送信できることを意味する。
【００８０】
なお、クライアント１００と中継用コンピュータ３００との間のＨＴＴＰによる通信は、ＳＳＬ(Secure Sockets Layer)によってセキュリティを確保することができる。ＳＳＬでは、認証局の署名の入った証明書を使ったウェブサーバ３１０の認証を行うことができる。さらにＳＳＬでは、クライアント１００とウェブサーバ３１０間での通信内容の暗号化を行うことができる。
【００８１】
次に、図２～図４に示したシステムにおけるホスト連携処理について具体的に説明する。図５は、第１の実施の形態における状態遷移例を示す図である。図５の例では、クライアント１００、ウェブサーバ３１０、中継デーモン３２０およびホスト２３０における状態遷移が示されている。
【００８２】
図５（Ａ）は、ホスト端末エミュレータ起動時の状態を示している。ホスト端末エミュレータ１１０が起動されると、クライアント１００からウェブサーバ３１０へ受信要求のＨＴＴＰ要求が送信される。そのＨＴＴＰ要求を受信したウェブサーバ３１０では、応答待機部３１２が起動される。その後、応答待機部３１２は、結果通知の受信待ちの状態となる。
【００８３】
なお、ホスト端末エミュレータ１１０は、クライアント１００に対して、ホスト端末エミュレーションプログラムの実行要求が入力されたときに起動される。
図５（Ｂ）は、操作入力時の状態を示している。クライアント１００に対してホスト２３０に入力すべきデータ（たとえば、ホスト２３０に実行させるべきコマンド）の操作入力が行われると、クライアント１００からウェブサーバ３１０へ、データ送信のＨＴＴＰ要求が送信される。ウェブサーバ３１０は、データ送信のＨＴＴＰ要求を受信すると、要求代理部３１１を起動し、その要求代理部３１１にＨＴＴＰ要求に含まれるデータを渡す。起動された要求代理部３１１は、受け取ったデータを中継デーモン３２０に渡し、ホスト

２３０への対話型のデータ入力を依頼する。中継デーモン３２０は、受け取ったデータをＴＮプロトコルのデータ形式に変換し、ＴＮ接続ゲートウェイ２２０を介してホスト２３０に送信する。すると、ホスト２３０において、受信したデータに応じたデータ処理が実行される。たとえば、受信したデータが、ファイルのコピーコマンドであれば、ホスト２３０がファイルのコピーを実行する。

【００８４】

また、中継デーモン３２０は、データ送信が完了したことを示す結果通知を要求代理部３１１に渡す。すると、要求代理部３１１は、受信した結果通知をウェブサーバ３１０に渡して、終了する（要求代理部３１１自身の機能を停止する）。ウェブサーバ３１０は、要求代理部３１１から受け取った送信完了を示すデータをＨＴＴＰ応答として、クライアント１００に送信する。

【００８５】

なお、応答待機部３１２は、受信待ち状態のままである。

図５（Ｃ）は、データ処理終了時の状態を示している。ホスト２３０においてデータ処理が終了すると、処理結果を示すデータ（ホスト発データ）が、ホスト２３０から中継デーモン３２０に送信される。たとえば、ホスト２３０において、ファイルのコピーが行われたのであれば、コピーの正常終了等を示すメッセージが、ホスト２３０から中継デーモン３２０に送信される。

【００８６】

中継デーモン３２０は、ホスト発データを受信して、ホスト発データを結果通知として応答待機部３１２に渡す。応答待機部３１２は、結果通知をウェブサーバ３１０に渡して、終了する（応答待機部３１２自身の機能を停止する）。ウェブサーバ３１０は、ホスト発データを含むデータを、受信通知のＨＴＴＰ応答としてクライアント１００に送信する。クライアント１００は、ホスト発データを処理する。たとえば、クライアント１００は、ホスト発データを画面に表示する。

【００８７】

図５（Ｄ）は、受信通知またはタイムアウトのＨＴＴＰ応答取得時の状態を示している。受信通知またはタイムアウトのＨＴＴＰ応答を受信したクライアント１００からウェブサーバ３１０へ、受信要求のＨＴＴＰ要求が送信される。そのＨＴＴＰ要求を受信したウェブサーバ３１０では、応答待機部３１２が起動される。その後、応答待機部３１２は、結果通知の受信待ちの状態となる。

【００８８】

このように、ウェブサーバ３１０では、応答待機部３１２が受信待ち状態で、ホスト２３０からのデータの受信を待つことにより、ホスト２３０がどのようなタイミングでホスト発データを送信しても、すぐにホスト発データをクライアント１００に送信することができる。

【００８９】

以下に、クライアント１００からのデータ送信時と、クライアント１００におけるデータ受信時との処理の流れについて説明する。

図６は、クライアントからホストへのデータ送信の流れを示すシーケンス図である。なお、図６では、ファイアウォール２１０とＴＮ接続ゲートウェイ２２０とを省略している。

【００９０】

クライアント１００は、ユーザからの操作入力に応答して、ＨＴＴＰ要求をウェブサーバ３１０に送信する（ステップＳ１１）。ウェブサーバ３１０は、ＨＴＴＰ要求に応答して要求代理部３１１を起動し、起動した要求代理部３１１にＨＴＴＰ要求に含まれるデータを渡す（ステップＳ１２）。要求代理部３１１は、受け取ったデータを、中継デーモン用のデータ形式に変換して、中継デーモン３２０に渡す（ステップＳ１３）。中継デーモン３２０は、要求代理部３１１から受け取ったデータをＴＮプロトコルのデータに変換して、ホスト２３０に送信する（ステップＳ１４）。

【００９１】

中継デーモン３２０は、データをホスト２３０に送信した後、送信完了の結果通知を、要求代理部３１１に渡す（ステップＳ１５）。結果通知を受け取った要求代理部３１１は、結果通知をウェブサーバ３１０に渡して、処理を終了する（ステップＳ１６）。ウェブサーバ３１０は、要求代理部３１１から受け取った送信完了を示す結果通知をＨＴＴＰ応答として、クライアント１００に送信する（ステップＳ１７）。

【００９２】

このようにして、クライアント１００からのデータを、ホスト２３０に渡すことができる。たとえば、ユーザがクライアント１００に対して、コマンドを入力すれば、そのコマンドがホスト２３０に渡される。そして、コマンドに従ったデータ処理が、ホスト２３０で実行される。

【００９３】

ここで、クライアント１００からウェブサーバ３１０へ送信するＨＴＴＰ要求には、少なくとも要求代理部３１１の起動要求と、ホスト２３０に渡すべきデータとが含められる。

【００９４】

図７は、データ送信時のＨＴＴＰ要求のデータ構造例を示す図である。図７に示すＨＴＴＰ要求５１は、ＰＯＳＴメソッドを使用した場合の例である。

ＨＴＴＰ要求５１は、ＵＲＩ(Uniform Resource Identifiers)部（相対パス部５１ａと相対パス部５１ａの後ろに「？」で接続されているパラメタ部５１ｂ）とＨＴＴＰボディー部５１ｃとに分かれる。

【００９５】

ＵＲＩ部の相対パス部５１ａには、要求代理部３１１の処理が記述されたプログラムの相対パスが設定される。図７の例では、ＵＲＩ部の相対パス部５１ａに「abc.com/ex.exe」と設定されている。

【００９６】

パラメタ部５１ｂとＨＴＴＰボディー部５１ｃとには、起動された要求代理部３１１に渡されるデータが設定される。そのデータには、「send」（送信要求であることを示す）、「phd」（ホスト接続設定情報）、「guid」（端末識別情報）、「len」（ホスト通信データ情報）などが含まれている。

【００９７】

次に、ホスト２３０からクライアント１００へデータを送信するための処理について説明する。

ここで、ホスト２３０からクライアント１００へのデータ送信処理を説明する前に、ホスト２３０からクライアント１００へデータを送信するための技術的な課題について説明する。

【００９８】

一般のホスト集中処理システムでは、ホスト端末とホストとの間の通信は非同期の双方向通信である。そのため、ホスト連携の通信を実現するプロトコルでは、任意のタイミングで発生する双方向の通信を処理できなければならない。しかし、ＨＴＴＰクライアントとウェブサーバのＨＴＴＰ通信プロトコルの手順は、常にクライアント側からの要求にウェブサーバが応答する手順で行われている。この手順を普通に利用する限りは、ホスト側から発せられる任意のタイミングの通信をクライアント側へ送信することができない。

【００９９】

そこで、第１の実施の形態では、ウェブサーバ３１０上の拡張機能としてホスト発の通信を待ち続ける応答待機部３１２を生成しておく。これによって、ホスト発の任意のタイミングの通信を一般のウェブサーバを利用して端末側に通知することを可能にしている。

【０１００】

すなわち、クライアント１００とウェブサーバ３１０との間に、予め（ホスト２３０からデータ送信の要求が出される前に）受信用接続を確立する。受信用接続は、クライアント１００がホスト２３０側からのデータ待ち受けるものである。クライアント１００とウェ

ブサーバ３１０との間には、常に１つ以上の受信用接続を確立してデータを待ち続ける。１つの受信用接続は、ホスト２３０側からクライアント１００側に通信データが送信されたときに切断されるが、その後すぐに再び受信用接続を確立され、データ待ち受け状態が維持される。

【０１０１】

図８は、ホスト発のデータをクライアントで受信するための処理の流れを示すシーケンス図である。なお、図８では、ファイアウォール２１０とＴＮ接続ゲートウェイ２２０とを省略している。

【０１０２】

クライアント１００は、ホスト端末エミュレータ１１０が起動されると、受信要求のＨＴＴＰ要求をウェブサーバ３１０に送信する（ステップＳ２１）。これにより、クライアント１００とウェブサーバ３１０との間に、データ受信用接続が確立する。すると、ウェブサーバ３１０は、応答待機部３１２を起動し、起動された応答待機部３１２にデータを渡す（ステップＳ２２）。応答待機部３１２は、データを解析し、中継デーモン用データ形式に変換する。そして、応答待機部３１２は、中継デーモン用データ形式のデータを中継デーモン３２０に渡す（ステップＳ２３）。以後、応答待機部３１２は、受信データの待ち受け状態となる。

【０１０３】

ホスト２３０は、クライアント１００に結果を通知すべき処理が実行されると、中継デーモン３２０に対してデータ（ホスト発データ）を送信する（ステップＳ２４）。ホスト発データを受け取った中継デーモン３２０は、データを受信したことを示す結果通知を応答待機部３１２に渡す（ステップＳ２５）。応答待機部３１２は、受け取った結果通知に含まれるホスト発データを、ＨＴＴＰ形式のＨＴＴＰ応答に変換して、ウェブサーバ３１０に渡す（ステップＳ２６）。その後、応答待機部３１２の処理が終了する。ウェブサーバ３１０は、ホスト発データの受信通知を意味するＨＴＴＰ応答を、クライアント１００に送信する（ステップＳ２７）。すると、クライアント１００は、再度、受信要求のＨＴＴＰ要求をウェブサーバ３１０に送信する（ステップＳ２１）。これにより、クライアント１００とウェブサーバ３１０との間に、データ受信用接続が再度確立し、応答待機部３１２が待ち受け状態となる。

【０１０４】

このようにして、ホスト２３０からのデータを、任意のタイミングでクライアント１００に渡すことができる。たとえば、ホスト２３０において、クライアント１００から受け取ったコマンドに応じた処理が完了すると、処理完了を示すメッセージがホスト２３０からクライアント１００に送信される。

【０１０５】

ここで、クライアント１００からウェブサーバ３１０へ送信するデータ受信時のＨＴＴＰ要求には、少なくとも応答待機部３１２の起動要求が含められる。

図９は、データ受信時のＨＴＴＰ要求のデータ構造例を示す図である。図９に示すＨＴＴＰ要求５２は、ＧＥＴメソッドを使用した場合の例である。

【０１０６】

ＨＴＴＰ要求５２は、プログラムの相対パス部５２ａとパラメタ部５２ｂとに分かれる。相対パス部５２ａには、応答待機部３１２の処理が記述されたプログラムの相対パスが設定される。図９の例では、相対パス部５２ａに「abc.com/ex.exe」と設定されている。

【０１０７】

パラメタ部５２ｂには、起動された応答待機部３１２に渡されるデータが設定される。パラメタ部５２ｂは、相対パス部５２ａの後ろに「？」で接続されている。パラメタ部５２ｂのデータには、「Recv」（受信要求であることを示す）、「phd」（ホスト接続設定情報）、「guid」（端末識別情報）などが含まれている。

【０１０８】

次に、クライアント１００と中継用コンピュータ３００との内部で行われる処理手順につ

いて説明する。
図１０は、クライアントで行われる処理の手順を示すフローチャートである。なお、図１０に示す処理は、ホスト端末エミュレータ１１０が起動されたときに開始される。以下、図１０に示す処理をステップ番号に沿って説明する。
【０１０９】
［ステップＳ３１］クライアント１００は、ホストにおいて各クライアントを一意に識別可能な端末識別情報（端末ＩＤ）を生成する。一意に識別可能なＩＤとして、たとえば、イーサネット（登録商標）のハードウェアアドレスを使用することができる。
【０１１０】
なお、端末ＩＤを中継用コンピュータ３００から取得するようにしてもよい。この場合、中継用コンピュータ３００が、クライアント１００を一意に識別可能な端末識別情報を生成して、クライアント１００に通知する。クライアント１００は、通知された端末識別情報を保持しておき、ステップＳ３１の処理の際に読み出す。
【０１１１】
［ステップＳ３２］クライアント１００は、受信要求のＨＴＴＰ要求を中継用コンピュータ３００に対して送信する。具体的には、ホスト端末エミュレータ１１０が、受信要求のデータをプロトコル制御部１２０に渡す。プロトコル制御部１２０は、そのデータをＨＴＴＰに従ったデータに変換してＨＴＴＰ制御部１３０に渡す。すると、ＨＴＴＰ制御部１３０が、ＨＴＴＰ要求としてインターネット１０を介して中継用コンピュータ３００にＨＴＴＰで送信する。なお、ＨＴＴＰ要求には端末識別情報が含まれる。
【０１１２】
［ステップＳ３３］クライアント１００は、操作入力の有無を検出する。ここでいう操作入力は、起動されているホスト端末エミュレータ１１０に対する操作入力である。操作入力がある場合には、処理がステップＳ３４に進められる。操作入力がない場合には、処理がステップＳ３５に進められる。
【０１１３】
［ステップＳ３４］クライアント１００は、データ送信のＨＴＴＰ要求を中継用コンピュータ３００に対して送信する。具体的には、ホスト端末エミュレータ１１０が、操作入力で入力されたデータをプロトコル制御部１２０に渡す。プロトコル制御部１２０は、受け取ったデータをＨＴＴＰ形式のデータに変換して、ＨＴＴＰ制御部１３０に渡す。ＨＴＴＰ制御部１３０は、受け取ったデータを、データ送信のＨＴＴＰ要求として中継用コンピュータ３００に対して送信する。
【０１１４】
［ステップＳ３５］クライアント１００のホスト端末エミュレータ１１０は、受信通知のＨＴＴＰ応答があるか否かを判断する。ＨＴＴＰ応答がある場合、処理がステップＳ３６に進められる。ＨＴＴＰ応答がない場合、処理がステップＳ３３に進められる。
【０１１５】
［ステップＳ３６］クライアント１００のホスト端末エミュレータ１１０は、受信通知のＨＴＴＰ応答がホスト発データを含むか否かを判断する。ホスト発データを含まない場合とは、タイムアウトの受信通知である。ホスト発データを含む場合、処理がステップＳ３７に進められる。ホスト発データを含まない場合、処理がステップＳ３２に進められる。
【０１１６】
［ステップＳ３７］クライアント１００のホスト端末エミュレータ１１０は、ホスト発データを処理する。たとえば、ホスト端末エミュレータ１１０は、ホスト発データをモニタ１１に表示する。その後、処理がステップＳ３２に進められる。
【０１１７】
次に、中継用コンピュータ３００における処理について説明する。
図１１は、中継用コンピュータの処理手順を示すフローチャートである。以下、図１１に示す処理をステップ番号に沿って説明する。
【０１１８】

［ステップＳ４１］ウェブサーバ３１０は、ＨＴＴＰ要求を受信したか否かを判断する。ＨＴＴＰ要求を受信した場合、処理がステップＳ４２に進められる。ＨＴＴＰ要求を受信していな場合、処理がステップＳ５０に進められる。

【０１１９】

［ステップＳ４２］ウェブサーバ３１０は、受信したＨＴＴＰ要求がデータ送信を指示するＨＴＴＰ要求か、データの受信を指示するＨＴＴＰ要求かを判断する。たとえば、図７に示したＨＴＴＰ要求５１の様に、パラメタに送信要求（Send)が含まれていれば、データ送信のＨＴＴＰ要求であることがわかる。また、図９に示したＨＴＴＰ要求５２の様に、パラメタに受信要求(Recv)が含まれていれば、受信要求のＨＴＴＰ要求であることがわかる。送信要求であれば、処理がステップＳ４４に進められる。受信要求であれば、処理がステップＳ４３に進められる。

【０１２０】

［ステップＳ４３］ウェブサーバ３１０は、応答待機部３１２を起動する。

［ステップＳ４４］ウェブサーバ３１０は、要求代理部３１１を起動し、送信要求のＨＴＴＰ要求に含まれるデータを、要求代理部３１１に渡す。すると、要求代理部３１１は、ウェブサーバ３１０から受け取ったデータを中継デーモン３２０に渡し、ホスト２３０へのデータ送信を依頼する。

【０１２１】

［ステップＳ４５］中継デーモン３２０は、要求代理部３１１から受け取ったデータをＴＮプロトコルのデータに変換する。

［ステップＳ４６］中継デーモン３２０は、ＴＮプロトコルのデータを、ＴＮ接続ゲートウェイ２２０経由でホスト２３０に送信する。

【０１２２】

［ステップＳ４７］中継デーモン３２０は、送信完了の結果通知を生成し、要求代理部３１１に渡す。

［ステップＳ４８］要求代理部３１１は、送信完了の結果通知をウェブサーバ３１０に渡して終了する。

【０１２３】

［ステップＳ４９］ウェブサーバ３１０は、送信完了の結果通知をＨＴＴＰ応答としてクライアント１００に送信する。その後、処理はステップＳ５４に進められる。

【０１２４】

［ステップＳ５０］中継デーモン３２０は、ホスト発データを受信したか否かを判断する。ホスト発データを受信した場合、処理がステップＳ５１に進められる。ホスト発データを受信していなければ、処理がステップＳ５４に進められる。

【０１２５】

［ステップＳ５１］中継デーモン３２０は、受信通知の結果通知を生成し、応答待機部３１２に渡す。

［ステップＳ５２］応答待機部３１２は、受け取った受信通知をウェブサーバ３１０に渡して終了する。

【０１２６】

［ステップＳ５３］ウェブサーバ３１０は、受信通知の結果通知をＨＴＴＰ応答としてクライアント１００に送信する。その後、処理はステップＳ５４に進められる。

【０１２７】

［ステップＳ５４］ウェブサーバ３１０は、応答待機部３１２の待機時間がタイムアウト（所定の最大待機時間に達すること）となったかを判断する。タイムアウトになった場合には、処理がステップＳ５５に進められる。タイムアウトになっていない場合には、処理がステップＳ４１に進められる。

【０１２８】

［ステップＳ５５］ウェブサーバ３１０は、応答待機部３１２を終了させる。

［ステップＳ５６］ウェブサーバ３１０は、タイムアウトの結果通知を、ＨＴＴＰ応答と

してクライアント１００に送信する。その後、処理がステップＳ４１に進められる。
【０１２９】
以上のようにして、次のような効果が得られる。
・安全性の高いホスト連携通信が可能となる。
ＨＴＴＰプロトコルでのホスト連携通信を実現する事により、ファイアウォールなどのネットワークのセキュリティポリシーを緩める（ＴＮプロトコルの接続を許可するなど）ことなくインターネット／イントラネット経由のホスト通信を行うことができる。
【０１３０】
・既存のホスト通信機能の資産を流用できる。
ＨＴＴＰプロトコルでのホスト通信は従来にない新しいホスト接続形態であるが、既存のホスト通信プロトコル（ＴＮプロトコルなど）とＨＴＴＰプロトコルとの中継機能を介して実現するため、既存のホスト通信用ゲートウェイなどの通信資産をそのまま流用する事が可能である。
【０１３１】
・既存のウェブサーバとその機能を利用できる。
クライアントと中継用コンピュータとの間にＨＴＴＰプロトコルでの通信処理を実装する必要があるが、本実施の形態ではこれを一般的なウェブサーバとその拡張プログラム（ＣＧＩ(Common Gateway Interface)など）の機能を利用して実現している。これにより、中継用コンピュータ側のＨＴＴＰ機能の開発が不要となる。しかも、ウェブサーバの持つ機能を流用できるため、例えば利用するウェブサーバがＳＳＬ通信を実装していればサーバ側のＳＳＬ通信処理の開発は不要である。
【０１３２】
このように、第１の実施の形態によれば、ホスト集中処理を用いたサービスを、インターネットを介して安全に行うことができる。たとえば、単純にＣＧＩを用いただけのＨＴＴＰクライアントサーバシステムでは、クライアントからの要求が出されない限り、サーバからクライアントへ応答データを送信することができないが、第１の実施の形態のホスト連携処理を用いれば、ホスト側から任意のタイミングでデータをクライアントに送信することが可能となる。これにより、従来のインターネットに関連する技術では実施できなかったサービスを提供することもできる。
【０１３３】
たとえば、株の売買を行う個人投資家の場合、株価が値上がりしたときに即座に売り注文を出して、売買を成立させたいという要求がある。このような取引の場合、株価が値上がりしてから数十秒後に情報を受け取っても、その間に第３者の売り注文が先に出されると、株価が値下がりしてしまう。そのため、個人投資家は、株価が変化した時点で、即座に株価情報を取得する必要がある。第１の実施の形態によれば、ホスト２３０からクライアント１００へ、いつでもデータを送信できる。そのため、株価に変更があった時に、即座に、ホスト２３０から個人投資家の使用するクライアント１００へ株価データを送信できる。
【０１３４】
これにより、目的の銘柄の株価が変わった時点で、すぐにその情報をクライアントで取得することができる。したがって、個人投資家は、株式の売買のタイミングを逃さずにすむ。
【０１３５】
また、各クライアントから出力されるＨＴＴＰ要求には、ホスト２３０が各クライアントを一意に識別可能な端末識別情報が含まれているため、ホスト２３０や中継用コンピュータ３００において、複数のクライアントを個別に認識することができる。また、プロキシ経由のクライアントであっても、ホスト２３０や中継用コンピュータ３００において、そのクライアントを他のコンピュータと区別することができる。
【０１３６】
［第２の実施の形態］

次に、第２の実施の形態について説明する。第２の実施の形態は、ウェブサーバを利用せずにホスト連携処理を行うものである。

【０１３７】

図１２は、第２の実施の形態に係るホスト連携処理のシステム構成例を示す図である。図１２に示す構成は、中継用コンピュータ５００の構成以外は、図４に示した第１の実施の形態の構成と同様である。そこで、図１２において、第１の実施の形態と同様の構成要素には、図４と同じ符号を付し説明を省略する。

【０１３８】

第２の実施の形態における中継用コンピュータ５００は、ウェブサーバは有しておらず、中継デーモン５１０がＨＴＴＰの通信を行う。すなわち、図４に示した第１の実施の形態では、ウェブサーバ３１０のＨＴＴＰ通信機能を利用するために、中継用コンピュータ３００内にウェブサーバ３１０を導入している。しかし、図１２に示すように、中継デーモン５１０が直接クライアント１００とＳＳＬによりデータを保護したＨＴＴＰ通信を行うことができれば、中継用コンピュータ５００がウェブサーバを有していなくてもよい。

【０１３９】

この場合、要求代理部５１１と応答待機部５１２との機能が、中継デーモン５１０内に設けられる。要求代理部５１１の機能は、図４に示した第１の実施の形態における要求代理部３１１の機能と同様である。また、応答待機部５１２の機能は、図４に示した第１の実施の形態における応答待機部３１２の機能と同様である。

【０１４０】

このようなシステムによれば、ホスト端末エミュレータ１１０が起動されると、クライアント１００から中継用コンピュータ５００に対して、応答待機要求を示すＨＴＴＰ要求が送信される。すると、中継用コンピュータ５００とクライアント１００との間に、受信用接続４１が確立する。同時に、中継デーモン５１０内に、応答待機部５１２が起動される。これにより、中継デーモン５１０は、ホスト２３０からのデータ待ち状態となり、ホスト２３０からクライアント１００に対するデータを、いつでも受け付け可能となる。

【０１４１】

その後、クライアント１００のホスト端末エミュレータ１１０に対して操作入力が行われると、クライアント１００と中継用コンピュータ５００との間で、送信用接続３１が確立される。そして、送信用接続３１を用いて、クライアント１００から中継用コンピュータ５００へデータ送信のＨＴＴＰ要求が送信される。すると、中継用コンピュータ５００の中継デーモン５１０において要求代理部５１１が生成される。生成された要求代理部５１１は、クライアント１００から送られたＨＴＴＰのデータをＴＮプロトコルのデータに変換し、ＴＮ接続ゲートウェイ２２０を介してホスト２３０に送信する。同時に、中継デーモン５１０は、クライアント１００に対して、送信完了のＨＴＴＰ応答を送信し送信用接続を切断するとともに、要求代理部５１１を終了する。

【０１４２】

ホスト２３０で処理が実行され、クライアント１００に対するデータ（ホスト発データ）が出力されると、中継デーモン５１０がホスト発データを受信する。中継デーモン５１０は、ＴＮプロトコルのホスト発データをＨＴＴＰの受信通知に変換する。そして、中継デーモン５１０は、受信通知のＨＴＴＰ応答を、応答待機部５１２に渡す。応答待機部５１２は、受信通知のＨＴＴＰ応答をクライアント１００に送信する。その後、応答待機部５１２の処理が終了すると共に、受信用接続が遮断される。

【０１４３】

受信通知のＨＴＴＰ応答を受け取ったクライアント１００は、ＨＴＴＰ応答に含まれるデータを表示すると共に、中継用コンピュータ５００に対して待機要求のＨＴＴＰ要求を送信する。これにより、再度、受信用接続４１が確立される。

【０１４４】

このようにして、第２の実施の形態においても、第１の実施の形態と同様に、クライアント１００とホスト２３０との間で、ホスト連携処理を実現することができる。その結果、

ホスト２３０から任意の時刻に出力される対データを、ＨＴＴＰ通信によってクライアント１００に送信することができる。

【０１４５】

［他の応用例等］

上記の第１の実施の形態のシステムを、既存のネットワーク環境上に構築する場合、たとえば、図１３に示すようなシステム構成とすることができる。

【０１４６】

図１３は、既存のネットワーク環境上にホスト連携処理機能を構築した例を示す図である。

クライアント１００ａは、パーソナルコンピュータ用のＯＳで制御されたコンピュータである。ＯＳとしては、たとえば、米マイクロソフト社のWindows（登録商標）を使用することができる。この場合、WinInet（インターネットアクセス機能を持ったクライアントアプリケーションを開発するためのＡＰＩ）ライブラリを利用して、ホスト端末エミュレータ１１０ａに、ＳＳＬ通信が可能なＨＴＴＰ制御部１３０ａを実装することができる。

【０１４７】

また、クライアント１００ａの端末識別情報としては、グローバル・ユニークＩＤ(GUID)を用いることができる。

ファイアウォール２１０ａは、ＨＴＴＰ通信のポート毎の通過許否を設定できるコンピュータであればよい。たとえば、ＵＮＩＸ（登録商標）のＯＳ上でファイアウォールを構築することができる。

【０１４８】

中継用コンピュータ３００ａは、たとえば、米マイクロソフト社のWindowsNTServer4.0（登録商標）やWindows2000Server（登録商標）によって構築することができる。その場合、ウェブサーバ３１０ａとして、ＩＩＳ（Internet Information Service）を利用することができる。ＩＩＳでウェブサーバ３１０ａを構築した場合、要求代理部３１１ａや応答待機部３１２ａの機能を、ＨＴＴＰホスト通信用のＩＳＡＰＩ(Internet Server API)で実装することができる。

【０１４９】

中継デーモン３２０ａは、ＩＳＡＰＩで実装された要求代理部３１１ａや応答待機部３１２ａとの通信を、メールスロット（プロセス通信を行うための手段の一つ）を経由して行うことができる。

【０１５０】

ＴＮ接続ゲートウェイ２２０ａは、たとえば、富士通株式会社のＦＮＡServer（登録商標）を使用することができる。

ホスト２３０ａには、ＴＮプロトコルなどの遠隔地から端末を接続するプロトコルに対応した各種汎用コンピュータを使用することができる。

【０１５１】

図１３に示したような構成のシステムによって、本発明の第１と第２の実施の形態を実現することができる。

なお、第１と第２の実施の形態の説明では、ホスト端末エミュレータ１１０、プロトコル制御部１２０、およびＨＴＴＰ制御部１３０を個別の要素として説明したが、プロトコル制御部１２０とＨＴＴＰ制御部１３０との機能は、ホスト端末エミュレータ１１０に組み込まれていてもよい。

【０１５２】

また、上記の処理機能は、汎用的なサーバコンピュータとクライアントコンピュータとによって実現することができる。その場合、中継用コンピュータ３００が有すべき機能の処理内容を記述した中継プログラム、およびクライアント１００が有すべき機能の処理内容を記述したホスト端末エミュレーションプログラムが提供される。中継用プログラムをサーバコンピュータで実行することにより、中継用コンピュータ３００の処理機能がサーバコンピュータ上で実現される。また、ホスト端末エミュレーションプログラムをクライア

ントコンピュータで実行することにより、クライアント１００の処理機能がクライアントコンピュータ上で実現される。

【０１５３】

処理内容を記述した中継用プログラムやホスト端末エミュレーションプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体としては、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリなどがある。磁気記録装置には、ハードディスク装置（ＨＤＤ）、フレキシブルディスク（ＦＤ）、磁気テープなどがある。光ディスクには、ＤＶＤ(Digital Versatile Disc)、ＤＶＤ－ＲＡＭ(Random Access Memory)、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)、ＣＤ－Ｒ(Recordable)／ＲＷ(ReWritable)などがある。光磁気記録媒体には、ＭＯ(Magneto-Optical disc)などがある。

【０１５４】

中継用プログラムやホスト端末エミュレーションプログラムを流通させる場合には、たとえば、各プログラムが記録されたＤＶＤ、ＣＤ－ＲＯＭなどの可搬型記録媒体が販売される。また、ホスト端末エミュレーションプログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータからクライアントコンピュータにホスト端末エミュレーションプログラムを転送することもできる。

【０１５５】

中継用プログラムを実行するサーバコンピュータは、たとえば、可搬型記録媒体に記録された中継用プログラムを、自己の記憶装置に格納する。そして、サーバコンピュータは、自己の記憶装置から中継用プログラムを読み取り、中継用プログラムに従った処理を実行する。なお、サーバコンピュータは、可搬型記録媒体から直接中継用プログラムを読み取り、その中継用プログラムに従った処理を実行することもできる。

【０１５６】

ホスト端末エミュレーションプログラムを実行するクライアントコンピュータは、たとえば、可搬型記録媒体に記録されたホスト端末エミュレーションプログラムもしくはサーバコンピュータから転送されたホスト端末エミュレーションプログラムを、自己の記憶装置に格納する。そして、クライアントコンピュータは、自己の記憶装置からホスト端末エミュレーションプログラムを読み取り、ホスト端末エミュレーションプログラムに従った処理を実行する。なお、クライアントコンピュータは、可搬型記録媒体から直接ホスト端末エミュレーションプログラムを読み取り、そのホスト端末エミュレーションプログラムに従った処理を実行することもできる。また、クライアントコンピュータは、サーバコンピュータからホスト端末エミュレーションプログラムが転送される毎に、逐次、受け取ったホスト端末エミュレーションプログラムに従った処理を実行することもできる。

【０１５７】

なお、中継装置を一般的なサーバと捉えた場合、クライアントからの要求にサーバが応答する手順で通信を行うプロトコルを用いた非同期の双方向通信を実現するためのプログラムが提供される。すなわち、サーバ側のプログラムとして、前記中継プログラムから中継機能以外の通信処理が記述されたサーバプログラムが提供される。また、クライアント側のプログラムとして、クライアントからの要求にサーバが応答する手順で通信を行うプロトコルを用いた非同期の双方向通信をサーバとの間で実現するための処理が記述された通信プログラムが提供される。これらのプログラムも中継プログラムやホスト端末エミュレーションプログラムと同様に、可搬型記録媒体に記録して流通させたり、ネットワークを介して受け渡したりすることができる。

【０１５８】

（付記１）　第１のプロトコルの通過を拒否するファイアウォールを経由して接続され、前記第１のプロトコルによる遠隔地からの対話型操作が可能なホストコンピュータに対する端末機能を実現するためのホスト端末エミュレーションプログラムにおいて、

コンピュータに、

前記第１のプロトコルと前記ファイアウォールの通過が許可された第２のプロトコルとの

相互のデータ形式変換機能を有し、前記ファイアウォールを経由して接続された中継装置との間で、前記第２のプロトコルのデータを受信するための受信用接続を予め確立し、
操作入力に応答して前記ホストコンピュータにデータを送信する際に、前記中継装置に対し、前記第２のプロトコルのデータを送信するための送信用接続を確立し、
前記送信用接続を用いて、操作入力されたデータを前記第２のプロトコルで前記中継装置に送信し、
前記受信用接続を用いて、前記ホストコンピュータから出力されたデータを、前記中継装置から前記第２のプロトコルで受信する、
処理を実行させることを特徴とするホスト端末エミュレーションプログラム。

【０１５９】

（付記２）　前記ホストコンピュータから出力されたデータを受信した際には、再度、前記中継装置との間で、前記第２のプロトコルのデータを受信するための受信用接続を確立することを特徴とする付記１記載のホスト端末エミュレーションプログラム。

【０１６０】

（付記３）　前記受信用接続の確立可能期間のタイムアウトが発生した際には、再度、前記中継装置との間で、前記第２のプロトコルのデータを受信するための受信用接続を確立することを特徴とする付記１記載のホスト端末エミュレーションプログラム。

【０１６１】

（付記４）　前記第２のプロトコルは、前記中継装置がウェブサーバ機能によってコンテンツの配信に利用されるプロトコルであることを特徴とする付記１記載のホスト端末エミュレーションプログラム。

【０１６２】

（付記５）　前記第２のプロトコルは、要求と応答との組が一回行われる毎に、接続の確立と遮断とを行うことの可能なプロトコルであることを特徴とする付記１記載のホスト端末エミュレーションプログラム。

【０１６３】

（付記６）　前記受信用接続を確立する際には、前記中継装置内の前記ホストコンピュータからのデータ受信を待機する機能の起動要求を、前記中継装置に対して出力することを特徴とする付記１記載のホスト端末エミュレーションプログラム。

【０１６４】

（付記７）　ネットワーク上で一意に識別可能な識別情報を生成するか、または前記中継装置で生成された前記識別情報を受け取り、前記中継装置との送信接続および受信接続の確立の際には、前記識別情報を含む接続要求を前記中継装置に送信することを特徴とする付記１記載のホスト端末エミュレーションプログラム。

【０１６５】

（付記８）　ファイアウォールを経由して接続されるクライアントコンピュータと、第１のプロトコルによる遠隔地からの対話型操作が可能なホストコンピュータとの間のデータを中継するための中継用プログラムにおいて、
コンピュータに、
前記クライアントコンピュータとの間で、前記ファイアウォールの通過が許可された第２のプロトコルによる受信用接続を予め確立し、
前記クライアントコンピュータからデータを受け取る際に、前記クライアントコンピュータとの間で前記第２のプロトコルによる送信用接続を確立し、
前記送信用接続を用いて、前記クライアントコンピュータから送られたデータを、前記第１のプロトコルに変換して前記ホストコンピュータに送信し、
前記第１のプロトコルにより前記ホストコンピュータから送られたデータを、前記第２のプロトコルに変換して、前記受信用接続を用いて前記クライアントコンピュータに送信する、
処理を実行させることを特徴とする中継用プログラム。

【０１６６】

（付記９）　第１のプロトコルの通過を拒否するファイアウォールを経由して接続され、前記第１のプロトコルによる遠隔地からの対話型操作が可能なホストコンピュータに対する端末機能を実現するためのホスト端末エミュレーション方法において、
前記第１のプロトコルと前記ファイアウォールの通過が許可された第２のプロトコルとの相互のデータ形式変換機能を有し、前記ファイアウォールを経由して接続された中継装置との間で、前記第２のプロトコルのデータを受信するための受信用接続を予め確立し、
操作入力に応答して前記ホストコンピュータにデータを送信する際に、前記中継装置に対し、前記第２のプロトコルのデータを送信するための送信用接続を確立し、
前記送信用接続を用いて、操作入力されたデータを前記第２のプロトコルで前記中継装置に送信し、
前記受信用接続を用いて、前記ホストコンピュータから出力されたデータを、前記中継装置から前記第２のプロトコルで受信する、
ことを特徴とするホスト端末エミュレーション方法。

【０１６７】

（付記１０）　ファイアウォールを経由して接続されるクライアントコンピュータと、第１のプロトコルによる遠隔地からの対話型操作が可能なホストコンピュータとの間のデータを中継するためのデータ中継方法において、
前記クライアントコンピュータとの間で、前記ファイアウォールの通過が許可された第２のプロトコルによる受信用接続を予め確立し、
前記クライアントコンピュータからデータを受け取る際に、前記クライアントコンピュータとの間で前記第２のプロトコルによる送信用接続を確立し、
前記送信用接続を用いて、前記クライアントコンピュータから送られたデータを、前記第１のプロトコルに変換して前記ホストコンピュータに送信し、
前記第１のプロトコルにより前記ホストコンピュータから送られたデータを、前記第２のプロトコルに変換して、前記受信用接続を用いて前記クライアントコンピュータに送信する、
ことを特徴とするデータ中継方法。

【０１６８】

（付記１１）　第１のプロトコルの通過を拒否するファイアウォールを経由して接続され、前記第１のプロトコルによる遠隔地からの対話型操作が可能なホストコンピュータに対する端末機能を有するホスト端末装置において、
前記第１のプロトコルと前記ファイアウォールの通過が許可された第２のプロトコルとの相互のデータ形式変換機能を有し、前記ファイアウォールを経由して接続された中継装置との間で、前記第２のプロトコルのデータを受信するための受信用接続を予め確立する受信用接続確立手段と、
操作入力に応答して前記ホストコンピュータにデータを送信する際に、前記中継装置に対し、前記第２のプロトコルのデータを送信するための送信用接続を確立する送信用接続確立手段と、
前記送信用接続確立手段が確立した前記送信用接続を用いて、操作入力されたデータを前記第２のプロトコルで前記中継装置に送信する送信手段と、
前記受信用接続確立手段が確立した前記受信用接続を用いて、前記ホストコンピュータから出力されたデータを、前記中継装置から前記第２のプロトコルで受信する受信手段と、
を有することを特徴とするホスト端末装置。

【０１６９】

（付記１２）　ファイアウォールを経由して接続されるクライアントコンピュータと、第１のプロトコルによる遠隔地からの対話型操作が可能なホストコンピュータとの間のデータを中継するための中継装置において、
前記クライアントコンピュータとの間で、前記ファイアウォールの通過が許可された第２のプロトコルによる受信用接続を予め確立する受信用接続確立手段と、
前記クライアントコンピュータからデータを受け取る際に、前記クライアントコンピュー

タとの間で前記第２のプロトコルによる送信用接続を確立する送信用接続確立手段と、
前記送信用接続確立手段が確立した前記送信用接続を用いて、前記クライアントコンピュータから送られたデータを、前記第１のプロトコルに変換して前記ホストコンピュータに送信し、
前記第１のプロトコルにより前記ホストコンピュータから送られたデータを、前記第２のプロトコルに変換して、前記受信用接続確立手段が確立した前記受信用接続を用いて前記クライアントコンピュータに送信する、
ことを特徴とする中継装置。
【０１７０】
（付記１３）　第１のプロトコルの通過を拒否するファイアウォールを経由して接続され、前記第１のプロトコルによる遠隔地からの対話型操作が可能なホストコンピュータに対する端末機能を実現するためのホスト端末エミュレーションプログラムを記録したコンピュータ読み取り可能な記録媒体において、
前記コンピュータに、
前記第１のプロトコルと前記ファイアウォールの通過が許可された第２のプロトコルとの相互のデータ形式変換機能を有し、前記ファイアウォールを経由して接続された中継装置との間で、前記第２のプロトコルのデータを受信するための受信用接続を予め確立し、
操作入力に応答して前記ホストコンピュータにデータを送信する際に、前記中継装置に対し、前記第２のプロトコルのデータを送信するための送信用接続を確立し、
前記送信用接続を用いて、操作入力されたデータを前記第２のプロトコルで前記中継装置に送信し、
前記受信用接続を用いて、前記ホストコンピュータから出力されたデータを、前記中継装置から前記第２のプロトコルで受信する、
処理を実行させることを特徴とするホスト端末エミュレーションプログラムを記録したコンピュータ読み取り可能な記録媒体。
【０１７１】
（付記１４）　ファイアウォールを経由して接続されるクライアントコンピュータと、第１のプロトコルによる遠隔地からの対話型操作が可能なホストコンピュータとの間のデータを中継するための中継用プログラムを記録したコンピュータ読み取り可能な記録媒体において、
前記コンピュータに、
前記クライアントコンピュータとの間で、前記ファイアウォールの通過が許可された第２のプロトコルによる受信用接続を予め確立し、
前記クライアントコンピュータからデータを受け取る際に、前記クライアントコンピュータとの間で前記第２のプロトコルによる送信用接続を確立し、
前記送信用接続を用いて、前記クライアントコンピュータから送られたデータを、前記第１のプロトコルに変換して前記ホストコンピュータに送信し、
前記第１のプロトコルにより前記ホストコンピュータから送られたデータを、前記第２のプロトコルに変換して、前記受信用接続を用いて前記クライアントコンピュータに送信する、
処理を実行させることを特徴とする中継用プログラムを記録したコンピュータ読み取り可能な記録媒体。
【０１７２】
（付記１５）　クライアント側からの要求にサーバが応答する手順で通信を行うプロトコルを用いて、前記サーバとの間の通信機能を実現するための通信プログラムにおいて、
コンピュータに、
前記サーバとの間で、前記プロトコルのデータを受信するための受信用接続を予め確立し、
操作入力に応答してデータを送信する際に、前記サーバに対し、前記プロトコルのデータを送信するための送信用接続を確立し、

前記送信用接続を用いて、操作入力されたデータを前記プロトコルで前記サーバに送信し、
前記受信用接続を用いて、前記サーバから出力されたデータを前記プロトコルで受信する、
処理を実行させることを特徴とする通信プログラム。
【０１７３】
（付記１６）　クライアント側からの要求にサーバが応答する手順で通信を行うプロトコルを用いて、前記サーバとの間の通信機能をクライアント側で実現するための通信方法において、
前記サーバとの間で、前記プロトコルのデータを受信するための受信用接続を予め確立し、
操作入力に応答してデータを送信する際に、前記サーバに対し、前記プロトコルのデータを送信するための送信用接続を確立し、
前記送信用接続を用いて、操作入力されたデータを前記プロトコルで前記サーバに送信し、
前記受信用接続を用いて、前記サーバから出力されたデータを前記プロトコルで受信する、
ことを特徴とする通信方法。
【０１７４】
（付記１７）　クライアント側からの要求にサーバが応答する手順で通信を行うプロトコルを用いて、前記サーバとの間の通信機能を備えたクライアントコンピュータにおいて、
前記サーバとの間で、前記プロトコルのデータを受信するための受信用接続を予め確立する受信用接続確立手段と、
操作入力に応答してデータを送信する際に、前記サーバに対し、前記プロトコルのデータを送信するための送信用接続を確立する送信用接続確立手段と、
前記送信用接続確立手段が確立した前記送信用接続を用いて、操作入力されたデータを前記プロトコルで前記サーバに送信する送信手段と、
前記受信用接続確立手段が確立した前記受信用接続を用いて、前記サーバから出力されたデータを前記プロトコルで受信する受信手段と、
を有することを特徴とするクライアントコンピュータ。
【０１７５】
（付記１８）　クライアント側からの要求にサーバが応答する手順で通信を行うプロトコルを用いて、前記サーバとの間の通信機能を実現するための通信プログラムを記録したコンピュータ読み取り可能な記録媒体において、
前記コンピュータに、
前記サーバとの間で、前記プロトコルのデータを受信するための受信用接続を予め確立し、
操作入力に応答してデータを送信する際に、前記サーバに対し、前記プロトコルのデータを送信するための送信用接続を確立し、
前記送信用接続を用いて、操作入力されたデータを前記プロトコルで前記サーバに送信し、
前記受信用接続を用いて、前記サーバから出力されたデータを前記プロトコルで受信する、
処理を実行させることを特徴とする通信プログラムを記録したコンピュータ読み取り可能な記録媒体。
【０１７６】
【発明の効果】
以上説明したように本発明に係るホスト端末エミュレーションプログラム、中継用プログラム、およびホスト端末エミュレーション方法では、ゲートウェイの通過が遮断されるプロトコルでホストコンピュータとホスト連携を行う中継装置に対して、ゲートウェイを通

過可能なプロトコルのデータを受信するための受信用接続を予め確立し、受信用接続を用いて、ホストコンピュータから出力されたデータを、中継装置から受信するようにした。これにより、ホストコンピュータを含む保護されたネットワークの安全性を損なわずに、保護されたネットワークの外部からホストコンピュータに対するホスト連携による入出力が可能となる。

【図面の簡単な説明】

【図１】実施の形態に適用される発明の概念図である。

【図２】第１の実施の形態に係るホスト連携処理のシステム構成例を示す図である。

【図３】本発明の実施の形態に用いるクライアントのハードウェア構成例を示す図である。

【図４】ホスト連携処理に必要な機能を示すブロック図である。

【図５】第１の実施の形態における状態遷移例を示す図である。図５（Ａ）は、ホスト端末エミュレータ起動時の状態を示しており、図５（Ｂ）は、操作入力時の状態を示しており、図５（Ｃ）は、データ処理終了時の状態を示しており、図５（Ｄ）は、受信通知またはタイムアウトのＨＴＴＰ応答取得時の状態を示している。

【図６】クライアントからホストへのデータ送信の流れを示すシーケンス図である。

【図７】データ送信時のＨＴＴＰ要求のデータ構造例を示す図である。

【図８】ホスト発のデータをクライアントで受信するための処理の流れを示すシーケンス図である。

【図９】データ受信時のＨＴＴＰ要求のデータ構造例を示す図である。

【図１０】クライアントで行われる処理の手順を示すフローチャートである。

【図１１】中継用コンピュータの処理手順を示すフローチャートである。

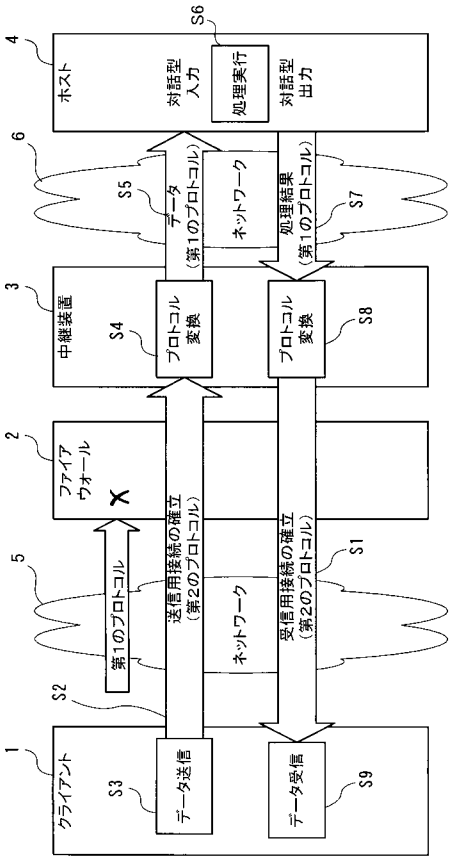
【図１２】第２の実施の形態に係るホスト連携処理のシステム構成例を示す図である。

【図１３】既存のネットワーク環境上にホスト連携処理機能を構築した例を示す図である。

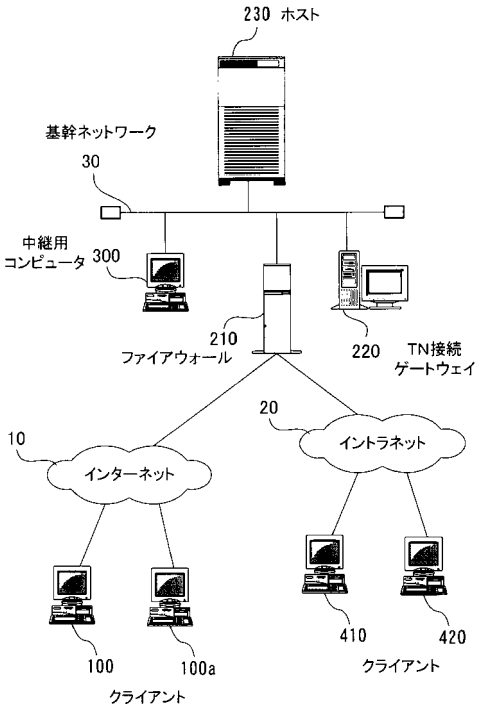
【符号の説明】

１　クライアント
２　ファイアウォール
３　中継装置
４　ホスト
５，６　ネットワーク
１０　インターネット
２０　イントラネット
３０　基幹ネットワーク
１００，１００ａ，４１０，４２０　クライアント
２１０　ファイアウォール
２２０　ＴＮ接続ゲートウェイ
２３０　ホスト
３００　中継用コンピュータ

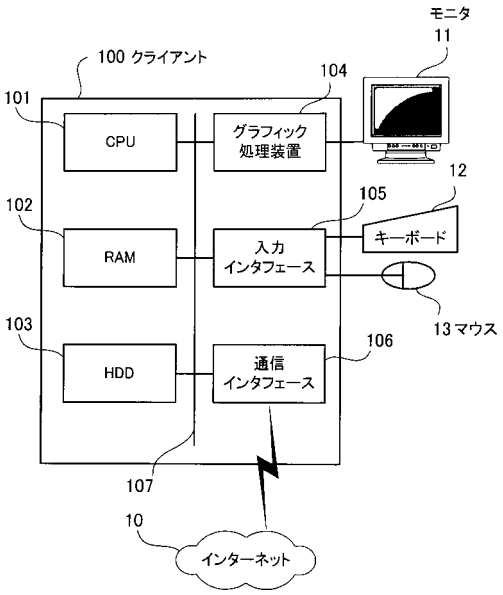
【図１】


ホスト
対話型入力
処理実行
対話型出力
S6
S5
データ（第1のプロトコル）
ネットワーク
処理結果（第1のプロトコル）
S7
中継装置
S4
プロトコル変換
プロトコル変換
S8
ファイアウォール
第1のプロトコル
送信用接続の確立（第2のプロトコル）
ネットワーク
受信用接続の確立（第2のプロトコル）
S1
S2
クライアント
S3
データ送信
データ受信
S9

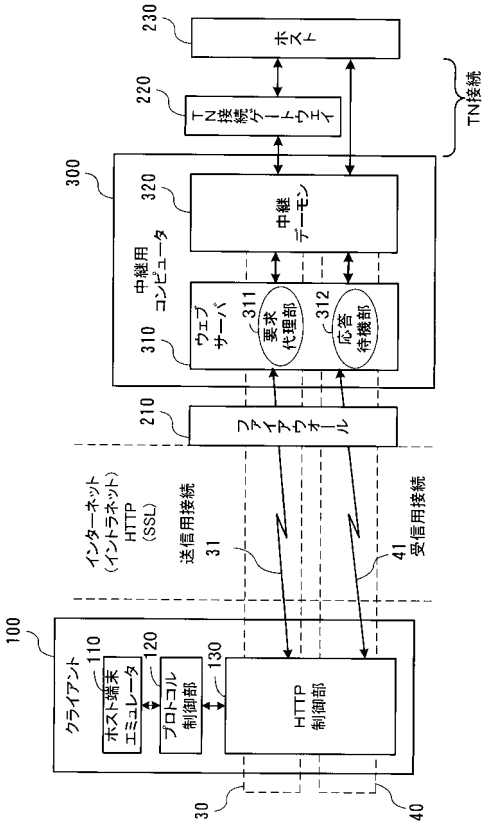
【図２】


230 ホスト
基幹ネットワーク
30
中継用コンピュータ 300
210
ファイアウォール
220
TN接続ゲートウェイ
20
イントラネット
10
インターネット
410
420
100
100a
クライアント
クライアント

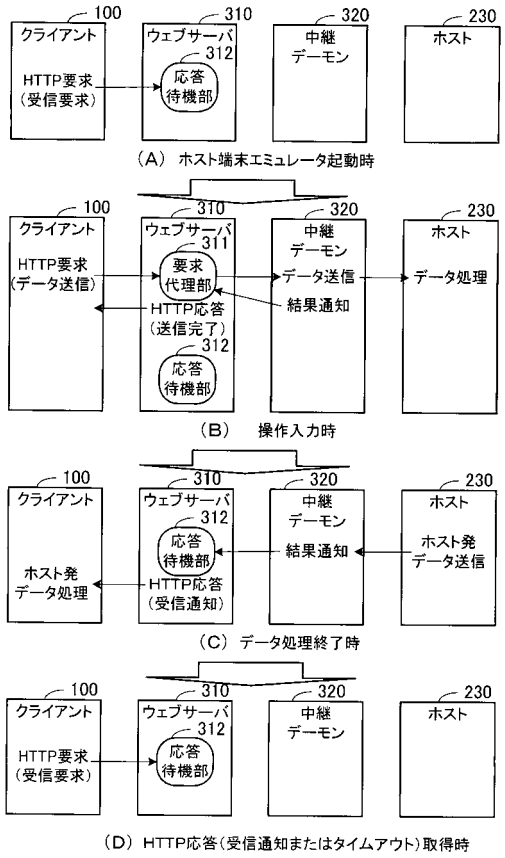
【図３】


モニタ
11
100 クライアント
104
101
CPU
グラフィック処理装置
12
105
102
RAM
入力インタフェース
キーボード
13 マウス
103
HDD
通信インタフェース
106
107
10
インターネット

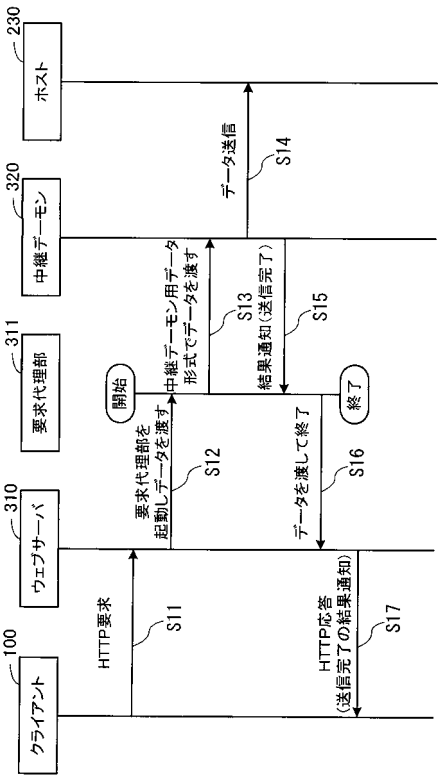
【図４】


230
ホスト
220
トンネル接続ゲートウェイ
TN接続
300
中継用コンピュータ
320
中継デーモン
ウェブサーバ
311
要求代理部
312
応答待機部
310
210
ファイアウォール
インターネット（イントラネット）
HTTP（SSL）
送信用接続
31
41
受信用接続
100
クライアント
110
ホスト端末エミュレータ
120
プロトコル制御部
130
HTTP制御部
30
40

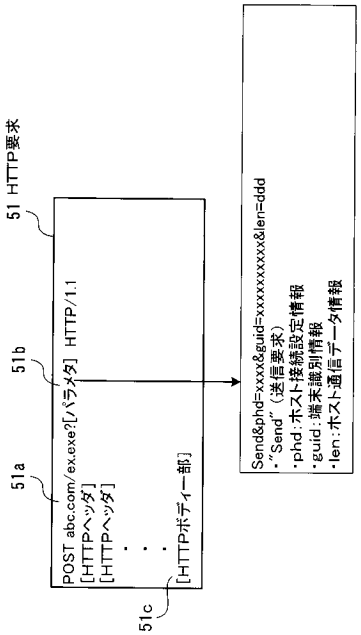
【図５】


100
クライアント
HTTP要求
（受信要求）
310
ウェブサーバ
312
応答
待機部
320
中継
デーモン
230
ホスト
（A） ホスト端末エミュレータ起動時
HTTP要求
（データ送信）
311
要求
代理部
データ送信
結果通知
データ処理
HTTP応答
（送信完了）
（B） 操作入力時
ホスト発
データ送信
HTTP応答
（受信通知）
（C） データ処理終了時
（D） HTTP応答（受信通知またはタイムアウト）取得時

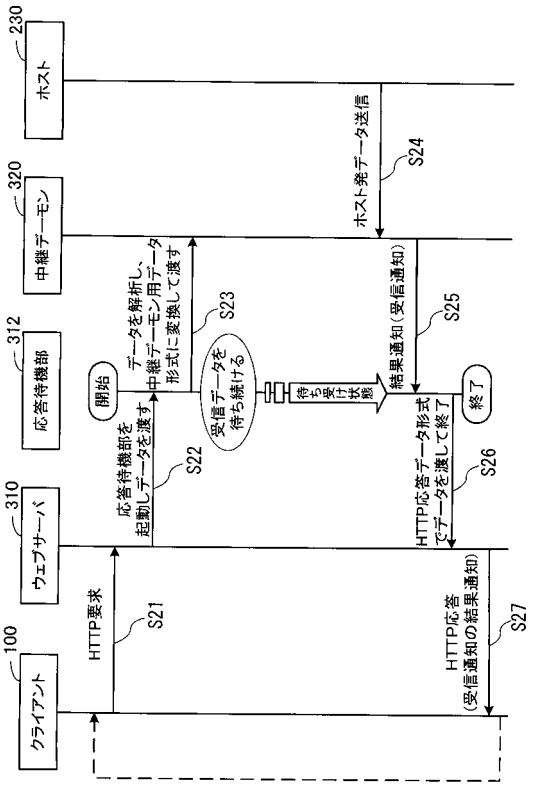
【図６】


230
ホスト
320
中継デーモン
311
要求代理部
310
ウェブサーバ
100
クライアント
データ送信
S14
開始
中継デーモン用データ
形式でデータを渡す
S13
結果通知（送信完了）
S15
要求代理部を
起動しデータを渡す
S12
データを渡して終了
S16
終了
HTTP要求
S11
HTTP応答
（送信完了の結果通知）
S17

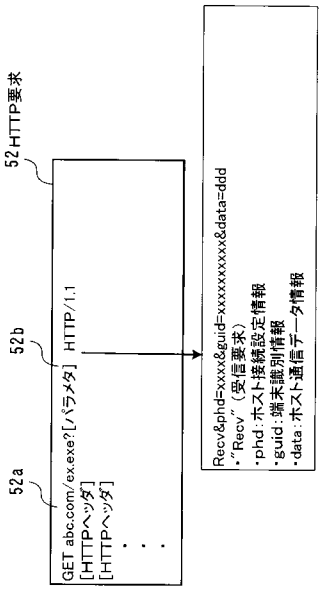
【図７】


51 HTTP要求
51a
51b
51c
POST abc.com/ex.exe?[パラメタ] HTTP/1.1
[HTTPヘッダ]
[HTTPヘッダ]
[HTTPボディー部]
Send&phd=xxxx&guid=xxxxxxxxxx&len=ddd
・"Send"（送信要求）
・phd：ホスト接続設定情報
・guid：端末識別情報
・len：ホスト通信データ情報

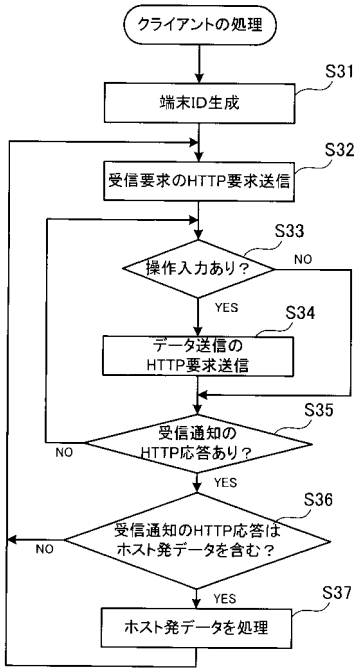
【図８】


230
ホスト
320
中継デーモン
312
応答待機部
310
ウェブサーバ
100
クライアント
ホスト発データ送信
S24
開始
データを解析し、
中継デーモン用データ
形式に変換して渡す
S23
受信データを
待ち続ける
待ち受け状態
結果通知（受信通知）
S25
応答待機部を
起動しデータを渡す
S22
HTTP応答データ形式
でデータを渡して終了
S26
終了
HTTP要求
S21
HTTP応答
（受信通知の結果通知）
S27

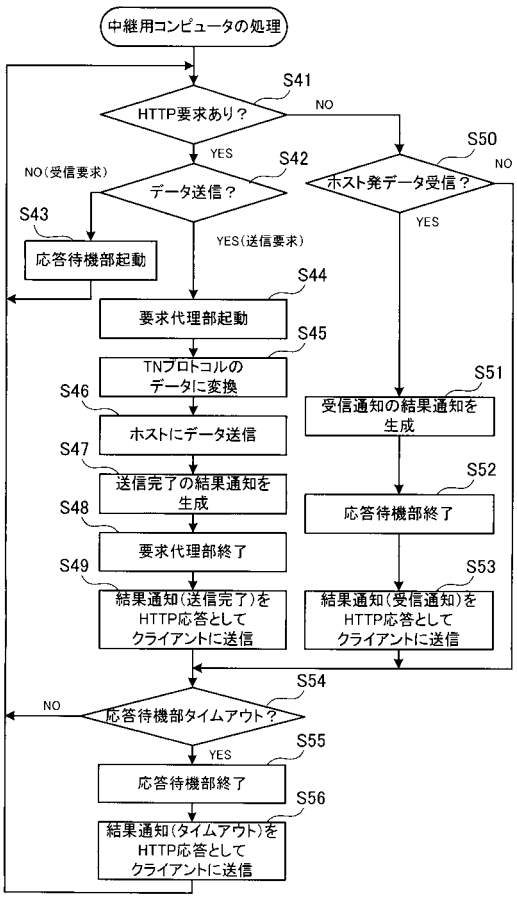
【図９】



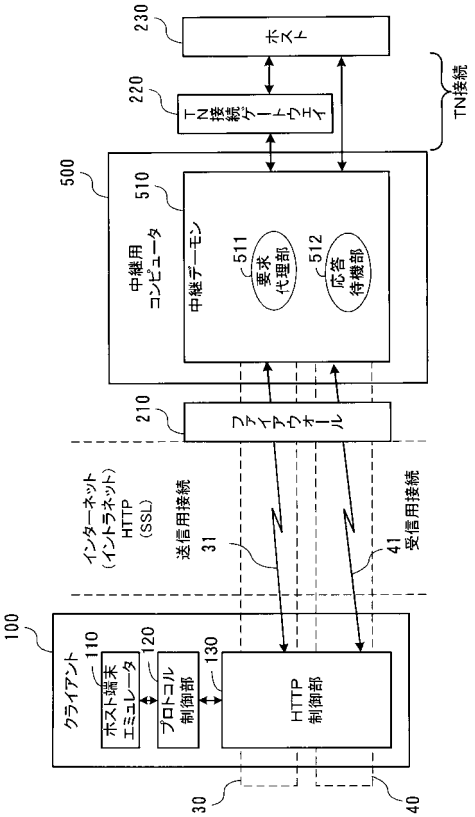

【図１０】



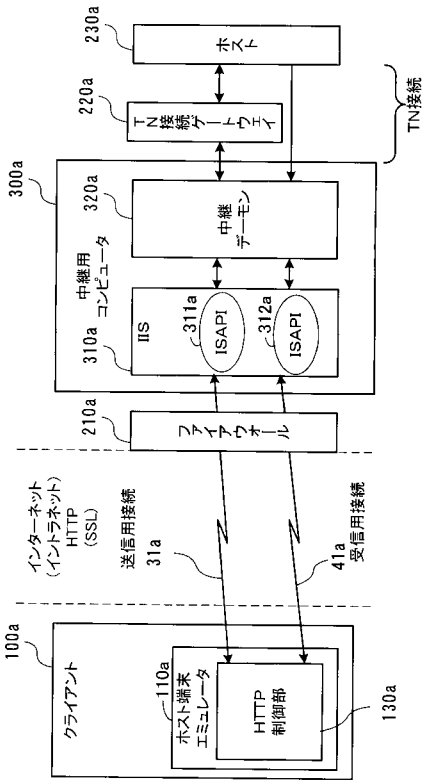

【図１１】




【図１２】



【図１３】


230a
ホスト
220a
TN接続ゲートウェイ
TN接続
300a
320a
中継デーモン
中継用コンピュータ
310a
IIS
311a
ISAPI
312a
ISAPI
210a
ファイアウォール
インターネット（イントラネット）
HTTP
（SSL）
送信用接続
31a
41a
受信用接続
100a
クライアント
110a
ホスト端末エミュレータ
HTTP制御部
130a

フロントページの続き

審査官　須藤　竜也

(56)参考文献　特開２００１－０８６１６３（ＪＰ，Ａ）
特開平０８－３１４８３５（ＪＰ，Ａ）
特開平１０－２８５２１６（ＪＰ，Ａ）
特開２０００－１５１６９３（ＪＰ，Ａ）
特開２０００－１７２５９７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 13/00