

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2004 年 12 月 23 日 (23.12.2004)

PCT

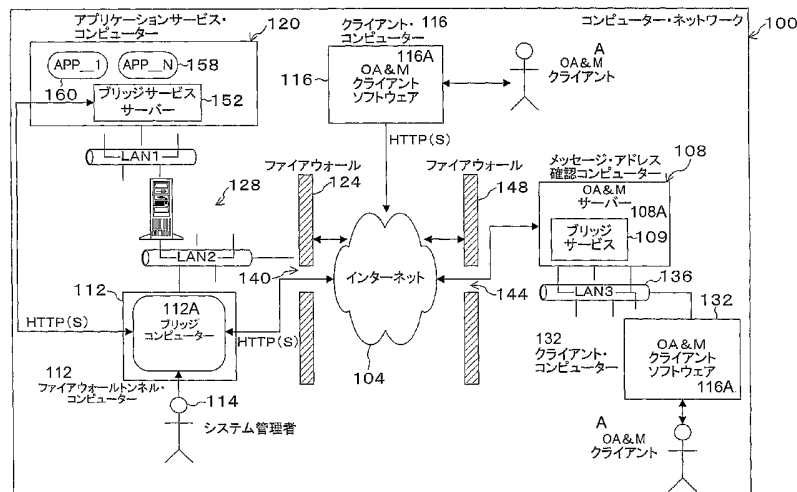
(10) 国際公開番号
WO 2004/111864 A1

- (51) 国際特許分類: **G06F 13/00** (OZDEMIR, Hasan Timucin). リー, コウチュ (LEE, Kou Chu). チュクラル, アミット (THUKRAL, Amit).
- (21) 国際出願番号: PCT/JP2004/008183
- (22) 国際出願日: 2004 年 6 月 4 日 (04.06.2004)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ: 10/454,336 2003 年 6 月 4 日 (04.06.2003) US
- (71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真 1006 番地 Osaka (JP).
- (74) 代理人: 前田 弘, 外 (MAEDA, Hiroshi et al.); 〒5410053 大阪府大阪市中央区本町 2 丁目 5 番 7 号 大阪丸紅ビル Osaka (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 大田 直行 (OTOSHI, Naoyuki). オズドミール, ハサン ティムチン
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, SL, SZ, TZ, UG, ZM, ZW),

/ 続葉有 /

(54) Title: INTERNET SECURE COMMUNICATION DEVICE AND COMMUNICATION METHOD

(54) 発明の名称: インターネットセキュア通信装置及び通信方法



- | | |
|------------------------------------|---|
| 100...COMPUTER NETWORK | 108...MESSAGE ADDRESS CONFIRMATION COMPUTER |
| 120...APPLICATION SERVICE COMPUTER | 108A...OA&M SERVER |
| 152...BRIDGE SERVICE SERVER | 109...BRIDGE SERVICE |
| 116...CLIENT COMPUTER | 112...FIREWALL TUNNEL COMPUTER |
| 116A...OA&M CLIENT SOFTWARE | 112A...BRIDGE COMPUTER |
| A...OA&M CLIENT | 104...INTERNET |
| 124...FIREWALL | 132...CLIENT COMPUTER |
| 148...FIREWALL | 114...SYSTEM ADMINISTRATOR |

(57) Abstract: There are provided a communication device and a communication method capable of passing through a firewall without rebuilding a network security device. In an environment where an application service is protected by a firewall, during use of the Internet, access from a client to the application service is permitted when message instances between

/ 続葉有 /



KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

- 国際調査報告書
- 請求の範囲の補正の期限前の公開であり、補正書受理の際には再公開される。

the client and application service corresponding to a first arbitrary message in a message address confirmation computer and a second arbitrary message in a firewall tunnel computer are valid. The firewall tunnel computer and the message address confirmation computer are connected directly to the Internet by the secure protocol.

(57) 要約:

ネットワークセキュリティ装置の再構築を行わずに、ファイアウォールを通過することのできる装置及び通信方法を提供する。

アプリケーションサービスがファイアウォールによって保護されている環境で、インターネット使用時に、メッセージ・アドレス確認コンピュータ内部の第1の任意のメッセージおよび、ファイアウォールトンネル・コンピュータ内部の第2の任意のメッセージに対応するクライアントとアプリケーションサービスの間の各々のメッセージインスタンスが有効な時、クライアントからアプリケーションサービスへのアクセスを許可する。

ファイアウォールトンネル・コンピュータとメッセージ・アドレス確認コンピュータはセキュア・プロトコルにより、インターネットに直接接続されている。

明細書

インターネットセキュア通信装置及び通信方法

技術分野

本発明は、アプリケーションサービス・コンピュータがファイアウォールのようなセキュリティ装置によって通常のインターネット・アクセスから一般に保護されるインターネットの使用において、クライアント・コンピュータと、アプリケーションサービス・コンピュータとの間のインターネットセキュア通信装置及び通信方法に関する。

背景技術

ネットワーク通信はファイアウォールや、NAT (Network Address Translator) のようなネットワークセキュリティ装置が、常に拡大するコンピュータシステム・グループのインターネットへのインタフェースとして使用される限りにおいて、複雑度を増してきている。これらのセキュリティ装置によって明らかになる重要な難題は、セキュリティ装置によってNATやファイアウォールの“背後”にある装置へ到達できないようにするため、他の正当なユーザーは、(しばしば、遠隔手続き呼び出し又は“RPC”通信による) サーバーとクライアントの間の広範囲のアクセスが、インターネットの通過に失敗することである。

リモートアクセス (例えば、制限のない、インスタントメッセージ、IPテレフォニーや、セキュリティカメラのトラブル解決等) を必要とするアプリケーションは、そのような接続性の難題が問題となる。この点において、そのようなタイプのアプリケーションに対するアプリケーション・サーバーは、しばしばリモートマネジメントに対して、Hyper Text Transfer Protocol (HTTP) のインタフェースを実装する。不幸にも、そのようなアプリケーション・サーバーは、中央のコンピュータメンテナンスグループから遠隔地に、重要な企業アプリケーションを実装しており、それらのインターネットを用いたメンテナンスのインタフェースは、対応するファイアウォールのため、メンテナンス部門によって利用できないよう

になっている。マネジメントインタフェースを使用する必要があるとき（そして皮肉にも、リモートマネジメントインタフェースは、NAT／ファイアウォールによってブロックすること以外に使用される時）、企業の職員は、それゆえにしばしば、重要な調整手続きを、作用させるコンピューターのある場所に物理的に輸送する必要がある。もちろんこの点において、ネットワークセキュリティは、システムに実装された調整基準として継続する必要がある。しかし、この継続したセキュリティのコストとお金は重要である。

（共にファイアウォールの背後にある）2つのドメインの間の接続性が必要な時、2つのドメイン上のアプリケーション間でメッセージを交換できるように、システム管理者はそのファイアウォールに、あるポートを空ける必要がある。このことは不幸にも、セキュリティの特徴を侵害するため、大多数の客にとって容認できる解ではない。

ファイアウォールとNATを通過する接続性は、コストとセキュリティの観点から強く望まれているにも関わらず、そのような通信の中でもセキュリティが継続するように、それらの特定のプロトコルの要求に従ってそれらのセキュリティ装置にアクセスするいまだ唯一の手段である必要がある。必要なのは、インターネットからファイアウォールを通過するセキュリティアクセス・アプリケーションサーバーへの通り道であり、そのような便利で、低コストのファイアウォール保護されたLANは、インターネットを横切り、ファイアウォールが許可された周りの、セキュアな広く双方向の通信を行うと認識されているそれらのアプリケーション・サーバーが必要な時に接続される。また、インターネットを横断する広く双方向の通信の性能を可能にするためにファイアウォールを再構成する必要があることが、強く望まれる。

従来のネットワークシステムおよび方法は、図4に示すように、HTTPプロトコルに従うリクエストにデータを添付して送信するためのHTTPクライアント機能411が搭載された通信対象機器410と、それを操作しあるいは監視する管理装置としてのパソコン420で構成され、パソコン420はインターネット401に接続され、通信対象機器410は企業のファイアウォール430の内側に設置されている。一般にファイアウォール430は、内側から外側に向けたHTTPリクエストの packets と、このHTTPリクエストに対応するHTTPレスポンスの packets を通過さ

れるように設定されている。前述のように通信対象機器 410 は HTTP クライアント機能 411 を有しており、HTTP リクエストとして GET 又は POST メソッドに送信したいデータを添付してパソコン 420 に送信する。この HTTP リクエストに対してパソコン 420 が HTTP リクエストを返信すると、前述のように HTTP レスポンスはファイアウォール 430 を通過することができるので、通信対象機器 410 は、パソコン 420 からのレスポンスを受信することができる。例えば、特開 2001-154953 号公報（第 4-5 頁、第 3 図）。

解決課題

しかしながら、従来のネットワークシステムおよび方法では、ファイアウォールや NAT を通過させたいアプリケーションを全て HTTP プロトコルに従ったアプリケーションとして実装する必要がある、すでに企業内に資産として保有する膨大なアプリケーションソフトウェアの資産を廃棄しなければならないという問題があった。

発明の開示

本発明は、従来の問題を解決するためになされたものであり、資産として存在する膨大なアプリケーションを変更することなく、ファイアウォールや NAT を通過させることを可能とするインターネットセキュア通信装置、および方法を提供することを目的とする。

本発明の第 1 の態様では、メッセージ・アドレス確認コンピュータに対する第 1 の任意のメッセージ、およびアプリケーションサービス・コンピュータへインターネットへのインタフェースおよび前記メッセージ・アドレス確認コンピュータへの前記インターネットへのインタフェースを提供するファイアウォールトンネル・コンピュータに対する第 2 の任意のメッセージ、に対して前記クライアント・コンピュータと前記アプリケーションサービス・コンピュータ間の各コンピュータ・メッセージ・インスタンスを有効にする手段で構成され、前記インターネットの使用を通じて、前記クライアント・コンピュータから前記アプリケーションサービス・コンピュータにアクセスすることを特徴とする。

本発明の第2の態様では、前記第1の任意のメッセージは、前記クライアント・コンピュータの識別子に関連する前記ファイアウォールトンネル・コンピュータの識別子で構成されることを特徴とする。

本発明の第3の態様では、前記第1の任意のメッセージは、さらに前記ファイアウォールトンネル・コンピュータの前記識別子と前記クライアント・コンピュータの前記識別子に関連する前記アプリケーションサービス・コンピュータの識別子で構成されることを特徴とする。

本発明の第4の態様では、前記識別子は、前記アプリケーションサービス・コンピュータの論理識別子で構成されることを特徴とする。

本発明の第5の態様では、前記識別子は、前記アプリケーションサービス・コンピュータのアプリケーションの論理識別子で構成されることを特徴とする。

本発明の第6の態様では、前記第2の任意のメッセージは、前記アプリケーションサービス・コンピュータの識別子で構成されることを特徴とする。

本発明の第7の態様では、前記第2の任意のメッセージは、さらに前記クライアント・コンピュータの識別子で構成されることを特徴とする。

本発明の第8の態様では、前記第1の任意のメッセージは、前記ファイアウォールトンネル・コンピュータによって前記メッセージ・アドレス確認コンピュータ内に定義されることを特徴とする。

本発明の第9の態様では、さらに、前記アプリケーションサービス・コンピュータによって前記クライアント・コンピュータのパスワードを有効にする手段を有することを特徴とする。

本発明の第10の態様では、さらに、前記メッセージ・アドレス確認コンピューターによって前記ファイアウォールトンネル・コンピューターのパスワードを有効にする手段を有することを特徴とする。

本発明の第11の態様では、前記メッセージ・アドレス確認コンピューターは、第1の所有者に所有される手段を有し、前記アプリケーションサービス・コンピューターと前記ファイアウォールトンネル・コンピューターは第2の所有者に所有される手段を有するとともに、前記第1の所有者と第2の所有者は、前記第1の所有者が前記第1の任意のメッセージを編集しないようにすることを合意するように構成する手段を有することを特徴とする。

本発明の第12の態様では、前記ファイアウォールトンネル・コンピューターは、外部へのHTTPプロトコル通信が通過できるようにファイアウォールによって設定されたファイアウォールのポートを通じてインターネットに接続するインタフェースを有し、前記ファイアウォールは、基本的に恒久的にいかなる内部への通信もブロックするように設定され、前記ファイアウォールを通過する双方向のメッセージを許可するように前記ファイアウォールのポートを再設定することが必要でないように、内部への通信は前記外部への通信と相互的でないことを特徴とする。

この構成により、アプリケーションサービス・コンピューターにアクセスする各々のクライアント・コンピューターをアプリケーションの論理識別子とクライアント・コンピューターの識別子を対応させてアドレス毎に識別し、パスワードで管理することができる。また、クライアント・コンピューターからアプリケーションサービス・コンピューターへのアクセスをHTTPプロトコル通信を用いてブリッジするため、ファイアウォールのセキュリティ設定を損なうことなく、安全に通信することができる。

本発明の第13の様態では、アプリケーションサービス・コンピューターとインターネットへのデータ通信を行うファイアウォールトンネル・コンピューターと、前記

インターネットから前記ファイアウォールトンネル・コンピュータへのデータ通信を行い、前記インターネットからクライアント・コンピュータへのデータ通信を行うメッセージ・アドレス確認コンピュータと、前記メッセージ・アドレス確認コンピュータ内の第1の任意のデータベース、および前記ファイアウォールトンネル・コンピュータ内の第2の任意のデータベースに対する、前記クライアント・コンピュータと前記アプリケーションサービス・コンピュータ間の前記通信の各コンピュータメッセージのインスタンスの検証手段で構成され、前記インターネットの使用を通じて、前記クライアント・コンピュータから前記アプリケーションサービス・コンピュータにアクセスすることを特徴とする。

本発明の第14の様態では、前記第1の任意のメッセージのデータベースは、前記クライアント・コンピュータに対する識別子に関連した、前記ファイアウォールトンネル・コンピュータに対する識別子を有するデータレコードで構成し、前記データレコードのアドレスは前記ファイアウォールトンネル・コンピュータから、前記第1の任意のデータベースのメッセージの中に定義されることを特徴とする。

本発明の第15の様態では、前記データレコードは、さらに前記アプリケーションサービス・コンピュータに対する識別子で構成することを特徴とする。

本発明の第16の様態では、前記第2の任意のメッセージのデータベースは、前記アプリケーションサービス・コンピュータに対する識別子を有するデータレコードで構成されることを特徴とする。

本発明の第17の様態では、前記第2の任意のメッセージのデータベースは、さらに前記クライアント・コンピュータに対する識別子を有することを特徴とする。

この構成により、クライアント・コンピュータの識別子と、ファイアウォールトンネル・コンピュータの識別子と、アプリケーションサービス・コンピュータの識別子をデータレコードとして持つデータベースで管理し、各メッセージのインスタ

ンスを検証する手段を有するようにしたため、メッセージの有効性を検証することができる。

本発明の第18の様態では、アプリケーションサービス・コンピューター、およびインターネットとデータ通信を行う、ファイアウォールトンネル・コンピューターであって、前記ファイアウォールトンネル・コンピューターは、クライアント・コンピューターと前記アプリケーションサービス・コンピューターとの間の前記データ通信の各コンピューターメッセージのインスタンスを有効にするようにプログラムされており、前記インターネットから前記ファイアウォールトンネル・コンピューターへのデータ通信と、前記インターネットから前記クライアント・コンピューターへのデータ通信を行うメッセージ・アドレス確認コンピューターであって、前記メッセージ・アドレス確認コンピューターは、前記クライアント・コンピューターと、前記アプリケーションサービス・コンピューターとの間の前記データ通信の各コンピューターメッセージのインスタンスを有効にするようにプログラムされており、前記インターネットの使用を通じて、前記クライアント・コンピューターから前記アプリケーションサービス・コンピューターへアクセスすることを特徴とする。

本発明の第19の様態では、前記メッセージ・アドレス確認コンピューターは、前記クライアント・コンピューターに対する識別子と関連した、前記ファイアウォールトンネル・コンピューターに対する識別子を有する任意のデータベースを有することを特徴とする。

本発明の第20の様態では、前記メッセージ・アドレス確認コンピューターと、前記ファイアウォールトンネル・コンピューターは、前記ファイアウォールトンネル・コンピューターが、前記メッセージ・アドレス確認コンピューターの中にある、前記任意のデータベースを変更することを可能にするようにプログラムされていることを特徴とする。

この構成により、本発明をプログラムしたインターネットセキュア通信装置を実現

することができる。

本発明の第21の様態では、メッセージ・アドレス確認コンピューター内の第1の任意のメッセージ、およびファイアウォールトンネル・コンピューター内の第2の任意のメッセージに対する、クライアント・コンピューターとアプリケーションサービス・コンピューターとの間の各コンピューターメッセージのインスタンスを有効にする手段を有し、前記ファイアウォールトンネル・コンピューターは、前記インターネットとのインタフェースを有し、前記メッセージ・アドレス確認コンピューターは、前記インターネットとのインタフェースを有し、前記インターネットの使用を通じて、前記クライアント・コンピューターから、前記アプリケーションサービス・コンピューターへアクセスすることを特徴とする。

本発明の第22の様態では、さらに、前記ファイアウォールトンネル・コンピューターによって、前記第1の任意のメッセージを定義する手段を有することを特徴とする。

この構成により、クライアント・コンピューターおよびアプリケーションサービス・コンピューターは、ファイアウォールトンネル・コンピューターとメッセージ・アドレス確認コンピューターを経由して、インターネットにアクセスすることができる。

本発明の第23の様態では、前記ファイアウォールトンネル・コンピューターは、ブリッジ・コンピューターのプログラムを実行し、前記アプリケーションサービス・コンピューターの中のアプリケーション・プログラムは、前記メッセージ・アドレス確認コンピューターによって、HTTPメッセージ配送メカニズムが生成されるように、前記ブリッジ・コンピューターのプログラムを制御することを特徴とする。

本発明の第24の様態では、前記ファイアウォールトンネル・コンピューターは、ブリッジ・コンピューターのプログラムを実行し、前記ブリッジ・コンピューターのプログラムは、前記メッセージ・アドレス確認コンピューターへのHTTP接続の開

始、および前記アプリケーションサービス・コンピュータへのH T T P接続の開始によって、ブリッジ・コンピュータのソフトウェアのインスタンスを生成し、前記メッセージ・アドレス確認コンピュータは前記ブリッジ・コンピュータのソフトウェアのインスタンスを認証することを特徴とする。

本発明の第25の様態では、前記ファイアウォールトンネル・コンピュータは、ブリッジ・コンピュータのプログラムを実行し、前記ブリッジ・コンピュータのプログラムは、前記メッセージ・アドレス確認コンピュータへのH T T P接続の開始、および前記アプリケーションサービス・コンピュータへのH T T P接続の開始によって、ブリッジ・コンピュータのソフトウェアのインスタンスを生成し、前記ブリッジ・コンピュータのプログラムは、各々の前記H T T P接続に対して定義された、送信メッセージ・バッファと受信メッセージ・バッファからなる一对のメッセージ・バッファを定義し、前記一对のメッセージ・バッファは、メッセージを前記メッセージ・アドレス確認コンピュータ内で実行されているブリッジサービスのプログラムと、前記アプリケーションサービス・コンピュータ内で実行されているブリッジサービス・サーバーのプログラムの間を双方向に転送することを特徴とする。

この構成により、アプリケーションサービス・コンピュータのアプリケーションは、ファイアウォールトンネル・コンピュータとメッセージ・アドレス確認コンピュータがH T T Pプロトコルで接続されるように制御し、ファイアウォールトンネル・コンピュータとアプリケーションサービス・コンピュータのアプリケーションは、H T T Pプロトコルによりブリッジ接続し、ブリッジ・コンピュータのプログラムは、送受信メッセージ・バッファを定義し、メッセージ・バッファを用いてメッセージ・アドレス確認コンピュータとファイアウォールトンネル・コンピュータを双方向に転送することができる。

本発明の第26の様態では、前記ファイアウォールトンネル・コンピュータは、トランスポート層とメッセージ処理層を持つブリッジ・コンピュータのプログラムを実行し、前記トランスポート層は、前記メッセージ・アドレス確認コンピュータ

へ第1のHTTP接続および、前記アプリケーションサービス・コンピュータへ第2のHTTP接続を開始し、前記メッセージ処理層は、各々の前記HTTP接続に対して定義された、送信メッセージ・バッファと受信メッセージ・バッファからなる一対のメッセージ・バッファを定義し、前記トランスポート層は、前記メッセージ・アドレス確認コンピュータから前記第1の接続を経由する通信の第1のメッセージを検索し、前記メッセージ処理層は、前記第1のメッセージに書かれた許可ルールを実行し、前記メッセージ処理層は、前記第1のメッセージを前記第1の接続の受信メッセージ・バッファから前記第2の接続の送信メッセージ・バッファへ移動し、前記トランスポート層は、前記第2の接続を経由して、前記アプリケーションサービス・コンピュータへ前記第1のメッセージを送信し、前記トランスポート層は、前記アプリケーションサービス・コンピュータから前記第2の接続を経由する通信の第2のメッセージを検索し、前記メッセージ処理層は前記第2のメッセージに書かれた許可ルールを実行し、前記メッセージ処理層は、前記第2のメッセージを前記第2の接続の受信メッセージ・バッファから前記第1の接続の送信メッセージ・バッファへ移動し、前記トランスポート層は、前記第1の接続を経由して、前記メッセージ・アドレス確認コンピュータへ前記第1のメッセージを送信することを特徴とする。

本発明の第27の様態では、前記通信中のメッセージは、異なるアプリケーションに対して、各々異なるプロトコルが組み立てられていることを特徴とする。

本発明の第28の様態では、前記ファイアウォールトンネル・コンピュータは、トランスポート層とメッセージ処理層を持つブリッジ・コンピュータのプログラムを実行し、前記トランスポート層は、前記メッセージ・アドレス確認コンピュータへの多数のメッセージと、前記アプリケーションサービス・コンピュータへの多数のメッセージを多重化送信することを特徴とする。

本発明の第29の様態では、前記ファイアウォールトンネル・コンピュータは、トランスポート層とメッセージ処理層を持つブリッジ・コンピュータのプログラムを実行し、前記トランスポート層は、前記メッセージ・アドレス確認コンピュータ

内のブリッジサービス・プログラムからの多数のメッセージ、および前記アプリケーションサービス・コンピューターからの多数のメッセージを多重化受信することを特徴する。

この構成により、ファイアウォールトンネル・コンピューターは、メッセージ・アドレス確認コンピューターとアプリケーションサービス・コンピューターの間に、プロトコルごとに異なるメッセージを生成して1つのHTTP接続を開始し、異なるプロトコル・メッセージを1つのHTTP接続で多重化通信を行うことができる。

本発明の第30の様態では、前記ファイアウォールトンネル・コンピューターは、トランスポート層とメッセージ処理層を持つブリッジ・コンピューターのプログラムを実行し、前記トランスポート層は、前記メッセージ・アドレス確認コンピューターと十分な多数のHTTP接続、および前記アプリケーションサービス・コンピューターと十分な多数のHTTP接続を生成し、全てのメッセージのレイテンシーは、予め定義されたレイテンシー値の範囲内で持続し、全てのメッセージのスループットは予め定義されたスループット値の範囲内で持続することを特徴とする。

この構成により、メッセージ・アドレス確認コンピューターとアプリケーションサービス・コンピューターの間でのHTTP接続に対して、メッセージのレイテンシーとスループットを保証することができる。

本発明の第31の様態では、多数のファイアウォールトンネル・コンピューターは、前記メッセージ・アドレス確認コンピューターと通信し、各々のファイアウォールトンネル・コンピューターは、前記メッセージを可能にするブリッジコンピューター・プログラムを実行することを特徴とする。

本発明の第32の様態では、多数のファイアウォールトンネル・コンピューターは、前記メッセージ・アドレス確認コンピューターと通信し、各々のファイアウォールトンネル・コンピューターは、前記メッセージを可能にするブリッジコンピューター・

プログラムを実行し、前記メッセージ・アドレス確認コンピューターは、前記多数のファイアウォールトンネル・コンピューター内のブリッジコンピューター・プログラムと通信するブリッジサービス・プログラムを実行することを特徴とする。

この構成により、ファイアウォールトンネル・コンピューターおよびメッセージ・アドレス確認コンピューターの機能をプログラムで実現することができる。

本発明の第33の様態では、各コンピューターメッセージのインスタンスを有効にする手段は、さらに各々の前記ファイアウォールトンネル・コンピューター内のブリッジコンピューター・プログラムと、前記メッセージ・アドレス確認コンピューター内のブリッジサービス・プログラムで構成され、前記ブリッジサービス・プログラムは、各前記ブリッジコンピューター・プログラムに対して、送信メッセージ・バッファを定義し、前記ブリッジサービス・プログラムは、その各々の前記送信メッセージ・バッファ内の各前記ブリッジコンピューター・プログラムと通信する各メッセージ・インスタンスをバッファすることを特徴とする。

本発明の第34の様態では、前記ブリッジサービス・プログラムは、1つのブリッジコンピューター・プログラムから送信された多数のメッセージをバッファすることを特徴とする。

この構成により、ブリッジサービス・プログラムは多数のメッセージをバッファして多重化処理を行うことができる。

本発明の第35の様態では、各コンピューターメッセージのインスタンスを有効にする手段は、さらに各々の前記ファイアウォールトンネル・コンピューター内のブリッジコンピューター・プログラムと、前記メッセージ・アドレス確認コンピューター内のブリッジサービス・プログラムで構成され、前記ブリッジサービス・プログラムは、各ブリッジコンピューター・プログラムによって送信された多数のメッセージを受け入れることが可能であり、前記ブリッジサービス・プログラムは、各前記ブリッ

ジコンピュータ・プログラムに対して送信メッセージ・バッファを定義し、前記ブリッジサービス・プログラムは、その各々の前記送信メッセージ・バッファ内の各前記ブリッジコンピュータ・プログラムと通信する各メッセージ・インスタンスをバッファし、前記ブリッジサービス・プログラムは、各メッセージを同一数のアプリケーションメッセージキューに転送することを特徴とする。

この構成により、ブリッジコンピュータ・プログラムとブリッジサービス・プログラムは、相互にメッセージを交換して通信し、アプリケーションごとにメッセージキューを保持して処理することができる。

図面の簡単な説明

図1は、本発明の実施の形態における、インターネットの使用を通じたメッセージ・インスタンスを接続するコンピュータネットワーク、メッセージ・アドレス確認コンピュータと、ファイアウォールトンネル・コンピュータの概略構成を示すブロック図である。

図2は、本発明の実施の形態における、図1のネットワークに従って登場するメッセージ管理に対するソフトウェアブリッジ・アーキテクチャを示すブロック図である。

図3は、本発明の実施の形態における、第1の情報処理プラットフォーム（IPP）と第2の情報処理プラットフォーム（IPP）間の相互メッセージ詳細を示すブロック図である。

図4は、従来のネットワークシステムおよび方法の概略構成を示すブロック図である。

発明を実施するための最良の形態

以下、本発明の実施の形態のインターネットセキュア通信装置、および方法について図面を用いて説明する。

発明の概略としては、（インターネットに接続する正当なユーザーとして、メッセージ・アドレス確認コンピュータに認識されるブリッジコンピュータが走行する）ファイアウォールトンネル・コンピュータは、クライアント・コンピュータ

とアプリケーションサービス・コンピュータとの間のファイアウォールで保護された通常のセキュア通信を行うインターネットと（あるいは、比喩的にいえばトンネルを通過して）インタフェースを取る。メッセージ・アドレス確認コンピュータは、正当なインターネット接続ユーザーとしてクライアント・コンピュータとファイアウォールトンネル・コンピュータに認識されたもののみ、インターネットに接続する。クライアント・コンピュータ、ファイアウォールトンネル・コンピュータ、およびメッセージ・アドレス確認コンピュータは、グループ内の職員に高く信頼された企業内の機能グループに所属することが望ましい。そのようなグループの例としては、ある企業内のオペレーション・管理・保守サービス（O A & M）グループとして任命されたコンピュータグループが挙げられる。

任意のメッセージ・データは、メッセージ・アドレス確認コンピュータ内のデータベースとしてよりも、ファイアウォールトンネル・コンピュータ内のデータベースとして確立される。クライアント・コンピュータからアプリケーションサービス・コンピュータへ通信するコンピュータメッセージの各々のインスタンスは、その後、メッセージ・アドレス確認コンピュータのデータベース（第1の任意のデータベース）に対する確認プロセス（第1の任意のメッセージの確認）を経て、アプリケーションサービス・コンピュータのファイアウォールトンネル・コンピュータのデータベース（第2の任意のデータベース）に対する確認プロセス（第2の任意のメッセージの確認）を通過して、そこからアプリケーションサービス・コンピュータに到達する。アプリケーションサービス・コンピュータからクライアント・コンピュータへ通信するコンピュータメッセージの各々のインスタンスは、アプリケーションサービス・コンピュータのデータベースに対する確認プロセスを経て、メッセージ・アドレス確認コンピュータのデータベースに対する確認プロセスと、クライアント・コンピュータのファイアウォールトンネル・コンピュータのデータベースに対する確認プロセスを通過して、クライアント・コンピュータに到達する。

O A & Mセンターのメッセージ・アドレス確認コンピュータのデータベースは基本的に、ファイアウォールトンネル・コンピュータのシステム管理（第1の所有者）者の管理下にある。これらのいかなるシステム管理者も、かれらのファイアウォールトンネル・コンピュータからO A & Mセンターへログインし、（メッセージ・

アドレス確認コンピューター内のデータベースに、) OA&Mセンター内のメッセージ・アドレス確認コンピューターと、アプリケーションサービス・コンピューター、ファイアウォールトンネル・コンピューター、およびシステム管理者(第2の所有者)のLAN内にあるファイアウォールトンネル・コンピューターとの間をブリッジする任意のメッセージを生成する。このことは、OA&Mセンター内のメッセージ・アドレス確認コンピューターからアプリケーションサービス・コンピューターへのアクセス経路を提供する。接続性が確立された後、OA&Mクライアント・コンピューターは、システム管理者によって作られた、OA&Mセンター内のメッセージ・アドレス確認コンピューターから、ファイアウォールトンネル・コンピューターを経由して、アプリケーションサービス・コンピューターに続く"トンネル"を用いてアプリケーションサービス・コンピューターにアクセスする。システム管理者は又、ファイアウォールトンネル・コンピューター内に、OA&Mセンター内のメッセージ・アドレス確認コンピューターからの任意のメッセージを許可する。クライアント・コンピューターとアプリケーションサービス・コンピューターとの間の各々のメッセージ・インスタンスは、インターネット接続可能なブリッジ機能を有効にするコンピューター(OA&Mセンター内のファイアウォールトンネル・コンピューターとメッセージ・アドレス確認コンピューター)の任意のメッセージからの確認を受ける。

図1はインターネット104の使用を通じたメッセージ・インスタンスを接続するコンピューターネットワーク100、メッセージ・アドレス確認コンピューター108と、ファイアウォールトンネル・コンピューター112の概略構成を示すブロック図である。クライアント・コンピューター116と、アプリケーションサービス・コンピューター120は、インターネット104からのメッセージを交換する。保護されたファイアウォール124は、(LAN1とLAN2が相互接続された)ローカルエリアネットワーク128をインターネット104への通常のアクセスから保護する。クライアント・コンピューター132は、(1つの実装として、LAN136は企業イントラネット136である)LAN136を経由して、メッセージ・アドレス確認コンピューター108とインターネット104に接続している。ファイアウォール148は、第2のクライアント・コンピューター132、メッセージ・アドレス確認コンピューター108、およびLAN136をインターネット104への通常のアクセ

スから保護する。アプリケーションサービス・コンピューター 120 は、アプリケーション 160 とアプリケーション 158 を実行する。アプリケーションサービス・コンピューター 120 はまた、ブリッジサービス・サーバー 152 を実行する。ブリッジサービス・サーバー 152 は、ファイアウォールトンネル・コンピューター 112（および、メッセージ・アドレス確認コンピューター 108）を経由して、クライアント（例えば、クライアント・コンピューター 116）から受信したメッセージ・インスタンスに応答して、メッセージ・インスタンスにファイアウォールトンネル・コンピューター 112 への経路を指示する。

メッセージ・アドレス確認コンピューター 108 は、むしろインターネット 104 の正当なユーザーとして特定のクライアント（例えばクライアント 116）とそのファイアウォールトンネル・コンピューター（例えばファイアウォールトンネル・コンピューター 112）を認識するためだけに、HTTPS（HTTP セキュアプロトコル）を経由してインターネット 104 に接続する。これらの HTTP セキュアプロトコルのインターネット 104 への“トンネル”アクセスは、ファイアウォール 124 のトンネル接続 140 と、ファイアウォール 148 のトンネル接続 144 に象徴的に図示される。関連して、ファイアウォール 124 のトンネル接続 140 と、ファイアウォール 148 のトンネル接続 144 は、それらに対応するファイアウォールを物理的にバイパスし、この明細書に記述されているように、メッセージごとのアドレスの任意の正当な方法論によって、セキュリティをデータの的に支持する。HTTP セキュアプロトコルの代わりに、別の実装では、ネットワークの所有者の特定の要望に対して、暗号のアプローチが適切なセキュリティを提供する。1 つの実装では、個別にポートの設定が可能なファイアウォールの 1 つのポートは、HTTP プロトコル接続のために空けられ、メッセージ・アドレス確認コンピューター 108 および／又は、ファイアウォールトンネル・コンピューター 112 は、HTTP プロトコルに設定されたポートに単一の接続を提供する。

ファイアウォールトンネル・コンピューター 112 のシステム管理者 114 は、必要な認証とプライバシーを満たしてメッセージ・アドレス確認コンピューター 108 にログインした後、メッセージ・アドレス確認コンピューター 108 とアプリケーションサービス・コンピューター 120 の間に“トンネル”を生成する。システム管理者

は基本的に、メッセージ・アドレス確認コンピューター108への接続の全てを制御し、行動の自由に於いて、物理的あるいはデータの接続を終端する。接続はファイアウォール124のいかなるポートを空けることを要求しないため、企業ネットワーク128は、外部のアタッカーから保護される。アプリケーションサービス・コンピューター120と、メッセージ・アドレス確認コンピューター108との間に一度トンネルが確立されると、メッセージ・アドレス確認コンピューター108のクライアント（クライアント・コンピューター116や、クライアント・コンピューター132などのOA&Mクライアント）は、メッセージ・アドレス確認コンピューター108と（ファイアウォールトンネル・コンピューター112によって許可された）ファイアウォールトンネル140を経由して、アプリケーションサービス・コンピューター120にアクセスする。

システム全体のデザインは、HTTP上に走行するキューメカニズムがベースとなる。キュー・パラダイムは、`createQueue()`、`removeQueue()`、`sendSynch()`、`sendAsynch()` メッセージといったシンプルなプリミティブを提供する。“タイムアウトにより引き抜く”と“最大数のメッセージを回復する”は、クライアントにメッセージ・インスタンスを突き戻すために使用される。

（`SessionInBox`、`MaxNumberOfMsgs`、`TimeOut`）の優先属性形式の中のプリミティブな`getMessages` コマンドは、アプリケーション・キューにアドレスされたメッセージを回復するために使用される。1つ又は（最大限の）複数のメッセージに含まれる返信メッセージは、適切なキュー（とそれらのキューで処理要求を待つアプリケーション）に発送される。

各メッセージは、メッセージ・ボディとメッセージ・ヘッダを運ぶ封筒を含んでいる。ファイアウォールトンネル・コンピューター112で実行されるブリッジ・ソフトウェアは、一つの実装ではスタンドアロン・プログラムとして走行する。別の実装では、ブリッジ・ソフトウェアは、ブラウザ内の署名されたアプレットとして走行する。一つの実装では、アプレットバージョンのブリッジ・ソフトウェアは、インターネット・エクスプローラー内で実行し、マイクロソフトJVMあるいはサンJavaプラグインと一緒に機能する。

メッセージ・アドレス確認コンピューター108のデータベースの任意の構造は、

最小で、各々のデータレコードがファイアウォールトンネル・コンピューター 1 1 2 とクライアント・コンピューター 1 1 6 (あるいは、クライアント・コンピューター 1 3 2) を任意の対のアドレスとして区別する 1 セットのデータレコードで構成される。もう 1 つの実装では、ファイアウォールトンネル・コンピューター 1 1 2 とクライアント・コンピューター 1 1 6 (あるいはクライアント・コンピューター 1 3 2) のアドレスの任意の識別子は、アプリケーションサービス・コンピューター 1 2 0 の任意のアドレスによって 3 つ揃いに拡張される。さらに別の実装では、アプリケーションサービス・コンピューター 1 2 0 の任意のアドレスは、特定のアプリケーション 1 6 0 又は、1 5 8 で任意の識別子に、さらに拡張される。

ファイアウォールトンネル・コンピューター 1 1 2 のデータベースの任意の構造は、最小で、各々のデータレコードがアプリケーションサービス・コンピューター 1 2 0 の任意のアドレスとして区別する 1 セットのデータレコードで構成される。別の実装では、アプリケーションサービス・コンピューター 1 2 0 の任意の識別子は、クライアント・コンピューター 1 1 6 (あるいは 1 3 2) のアドレスの任意の識別子によって拡張される。さらに別の実装では、アプリケーションサービス・コンピューター 1 2 0 の任意のアドレスは、特定のアプリケーション 1 6 0 又は 1 5 8 の任意の識別子によって、さらに拡張される。

アプリケーションサービス・コンピューター 1 2 0 上のブリッジサービス・サーバー 1 5 2 は、オプションでパスワード保護、任意のアドレス識別子確認、又は特有のアプリケーション (1 5 8、1 6 0) が要求するようなものを実行する。

図 2 は、図 1 のネットワークに従って登場するメッセージ管理に対するソフトウェアブリッジ・アーキテクチャ 2 0 0 を示すものである。トンネル (1 4 0, 1 4 4) の両側のブリッジ・サービス 2 0 4, 2 0 8 は、インターネット 1 0 4 への適切な“トンネル”を通して送信する前の、整列した、あるいは整列していない情報処理プラットフォーム (IPP: Information Processing Platform) のメッセージを重要視する。整列した、あるいは整列していない他に、ブリッジ・サービス 2 0 4 と 2 0 8 は、同期メッセージと非同期メッセージを送信する能力と、メッセージを受信する能力を提供する。ブリッジ・ソフトウェア 2 1 4 は、メッセージ・アドレス確認のソフトウェアを含む。ブリッジ・サービス 2 0 4 とブリッジ・ソ

フトウェア 214 の間、およびブリッジ・サービス 208 とブリッジ・ソフトウェア 214 の間の HTTP (S) 通信は、HTTP (S) の中で SSL (Secure Socket Layer) 又は TLS (Transport Layer Security) を用いることによって守られる。

さらに詳細に説明する。ブリッジ・サービス 204 と 208 は Java サブレット技術によって、好んで実装される。ブリッジ・サービス 204 と 208 は、(ファイアウォールトンネル・コンピューター 112 で実行されるインスタンスに対して) ブリッジ・ソフトウェア 214 にログイン、リモートキューの生成、そしてメッセージの送受信を許可する。各ログインは適切なサービスのセッションを生成し、キューはメッセージ配送に対するそのセッションと連携する。ブリッジ・サービス 204 と 208 と、ブリッジ・ソフトウェア 214 は、ドメイン間の転送メッセージに対するブリッジ・キューと IPP キューの間のマッピングを含む。メッセージは、別のブリッジ・サービス (例えばドメイン B のブリッジ・サーバー 208) に送信するために、ブリッジ・サービス (例えば、ドメイン A のブリッジ・サーバー 204) 内にキューイングされる。

1 つの実装において、ブリッジ・ソフトウェア 214 は 2 つの層を持つ。第 1 の層は各々のブリッジ・サービス (204、および／又は 208) とメッセージを交換する HTTP 接続を提供するトランスポート層である。第 2 の層は、各々のブリッジ・サービス 204 又は、208 にメッセージ・インスタンス配送するメッセージ処理層である。1 つの実装では、トランスポート層は以下のようなインタフェースを提供する。

- Send (非同期送信)
- SendAndWait (同期送信)
- Receive (メッセージキューの受信)
- ReceiveAndReply (コールバック関数のためのメッセージ受信)

これらのインタフェースコマンド呼び出しは、メッセージ処理層および／又は、ブリッジ・サービス 204 および／又は 208 を経由してアクセスすることができるアプリケーションの間の相互作用に対して、柔軟性を提供する。

(例えばファイアウォールトンネル・コンピューター 112 で実行されている) ブ

ブリッジ・ソフトウェア 214 は、ブリッジ・サービス 204（例えば、メッセージ・アドレス確認コンピュータ 108 内で走行するブリッジ・サービス 109）とブリッジ・サービス 208（例えば、アプリケーションサービス・コンピュータ 120 内で走行するブリッジサービス・サーバー 152）への HTTP 接続を開始する。接続の初期化フェーズは、メッセージ・アドレス確認コンピュータ 108 によるブリッジ・ソフトウェア接続のインスタンスの認証を含む。ブリッジ・ソフトウェア 214 は、ユーザ（例えばシステム管理者）によって、あるいはアプリケーション・プログラムによって、メッセージ・アドレス確認コンピュータ 108 とアプリケーション・サーバーとの間を直接接続するトンネルを生成するように実行される。ブリッジ・ソフトウェア 214 は、ブリッジ・サービス 204 への HTTP 接続（第 1 の HTTP 接続）、および／又はブリッジ・サービス 208 への HTTP 接続（第 2 の HTTP 接続）に対して、送信メッセージ・バッファと受信メッセージ・バッファのペアを定義する。ブリッジ・ソフトウェア 214 のトランスポート層は、ブリッジ・サービス 204、および／又は 208 からメッセージを引き出す。ブリッジ・ソフトウェア 214 のトランスポート層は、また、ブリッジ・サービス 204、および／又は 208 にメッセージを送信する。ブリッジ・ソフトウェア 214 のトランスポート層は、また、必要な時にブリッジ・サービス 204、および／又は 208 との単一のインタラクションの中で複数のメッセージの送受信を行う。ブリッジ・ソフトウェア 214 のトランスポート層は、メッセージの順番を保ちながら、メッセージのレイテンシーを減らし、メッセージのスループットを増加させるためにブリッジ・サービス 204、および／又は 208 との複数の接続を生成する。メッセージ処理層は、ブリッジ・サービス 204、および／又は 208 との各々の接続に対して、送信メッセージ・バッファと受信メッセージ・バッファを生成する。ブリッジ・ソフトウェア 214 のメッセージ処理層は、ブリッジ・サービス 204 に関連付けられた送信メッセージから、ブリッジ・サービス 208 に関連付けられた受信メッセージへ、メッセージを移動する。また、ブリッジ・ソフトウェア 214 のメッセージ処理層は、ブリッジ・サービス 208 に関連付けられた送信メッセージから、ブリッジ・サービス 204 に関連付けられた受信メッセージへ、メッセージを移動する。メッセージの送信に対して、適切な許可チェックを実行した後、各々のメッセージの移動が行われる。メッセージの

交換は、通常各々異なるアプリケーションに対して異なるプロトコルに従って構成される。

ブリッジ・サービス 204、および／又は 208 は、ブリッジ・ソフトウェア 214 によって許可された各々の接続に対して、送信メッセージ・バッファを生成する。ブリッジ・サービス 204、および／又は 208 は、送信メッセージ・バッファに関連付けられた特定のブリッジ・ソフトウェアのインスタンスに結びつけられたメッセージをバッファする。ブリッジ・ソフトウェア 214 のトランスポート層は、関連する送信バッファからメッセージを引き出す。ブリッジ・サービス 204、および／又は 208 は、必要に応じてブリッジ・ソフトウェア・プログラムによって引き出し要求を開始された、メッセージを同時に処理する。ブリッジ・サービス 204、および／又は 208 は、ブリッジ・ソフトウェア・プログラムによって、適切なローカル、あるいはリモートのアプリケーション・キュー（図 3 の相互メッセージの詳細 300 を参照）に送信されたメッセージを転送する。

1 つの実装では、ブリッジ・サービス・ソフトウェア（サーバー・ソフトウェア 204 又は 208）は、アプリケーション・サーバーが走行している（この例では、アプリケーションサービス・コンピューターとファイアウォールトンネル・コンピューターは CPU と可能ならばディスクを共有して、論理的に分離されたものとして効果的に構成されたものであるかもしれない）ホスト・コンピューター上で実行される。しかしながら、むしろ、ファイアウォールトンネル・ソフトウェアは、サーバー 120 のような分離されたアプリケーション・サーバーにアクセスする 1 つのホストに置かれる。

システム管理者 114 は、インターネット 104 を経由して、OA&M センターのメッセージ・アドレス確認コンピューター 108 上のブリッジ・ソフトウェア 214 にアクセスする。よりよい実装では、OA&M センターのメッセージ・アドレス確認コンピューター 108 は、システム管理者 114 をユーザ名とパスワードによって認証する。

ここで論じたネットワーキング方法の利点は、多岐に渡る。アプリケーション・サーバーは NAT / ファイアウォールの後ろに置くことができ、アプリケーション・サーバーへの接続性を実現するために、ネットワーク管理者からのいかなる設定も必要

としない。NAT／ファイアウォールの内側からインターネット104への全ての接続が空けられており、“穴”は、特別にNAT／ファイアウォールを通して“穴”を空けられた“もの”ではない。このため、メッセージングはNATの特徴（例えば、対称あるいは、双方向の特徴）に依存しない。システム管理者114は、いつでもブリッジを止めることができる。メッセージのトラフィックはSSL又はTLSによって守られる。そして、クライアントは企業イントラネット136又は、インターネット104のいずれにも置くことができる。ブリッジサービス・サーバー152は、アプリケーション・サーバー（例えばサーバー120）にアクセスできる限り、顧客ネットワークのどこにでも走ることができる。例えば、アプリケーション・サーバーと同じ場所に置かれたシステム管理者のマシン上でも走ることができ、インターネット104からアクセスすることができない別のマシンでも走ることができ、インターネット104からアクセスすることができない別のマシンでも走ることができる。（ブリッジ・サービスがシステム管理者のマシンで実行される時、ブリッジ・サービスは、メッセージ・アドレス確認コンピューター108と、アプリケーション・サーバーとの間のブリッジを提供することに対して排他的に開始される。ブリッジサービス・サーバーが、インターネット104からアクセス可能なマシン上で走行する時、システム管理者114は、インターネット104からファイアウォールトンネル・コンピューターに対しブリッジサービス・サーバーにアクセスすることができるよう、対応するファイアウォールを設定する。このような特徴は、システム管理者114に、ブラウザの使用により、インターネット104上のどこからもトンネルを確立することを可能にする。）

革新の別の利点は、保護された通信プロトコルが、インターネットとアプリケーション・サービス・コンピューターのネットワークの間にインストールされたファイアウォール／NAT装置の再構成を必要としないコンピューター・システム・インフラストラクチャ内に、外へ向かう経路を許可することである。この点に関して、ファイアウォールトンネル・コンピューター112が、ファイアウォール124により外部へのHTTPプロトコル通信が継続することを可能にするようにファイアウォールのポート接続を設定することで、インターネット104に接続する時、アプリケーション間の双方向のマルチプロトコルのメッセージング（例えば、クライアント・コン

ピューターとアプリケーション・サービスの間のメッセージング)を許可するために、内部への通信に対する特定のファイアウォールのポートの再設定を行う必要がない。

1つの実装では、ブリッジ・ソフトウェアは、ウェブ・ブラウザ内のグラフィカル・ユーザ・インタフェースを通して、システム管理者114の制御下にある。別の実装では、ここで論じたようなHTTP/HTTPSのブリッジ・ソフトウェアを経由して、インターネットに保護されたアクセスを行うように設定された要望のアプリケーション・プログラムがあるコンピュータのアクセスは、アプリケーション・プログラムの制御下にある。どちらの場合も、アプリケーションサービス・コンピュータが走行するネットワーク上のファイアウォール/NAT装置の再設定は必要でない。

1つの実装では、アプリケーション・サービス・コンピュータ120は、LAN128には接続されておらず、それゆえにファイアウォールトンネル・コンピュータ112とのポイント・ツー・ポイント経由を除いて、インターネット104へのアクセスを行わない。また別の実装では、アプリケーション・サービス・コンピュータ120はLAN128に接続されておらず、HTTP/HTTP(S)上で、双方向のメッセージングを用いて、インターネット104に直接アクセスし、ここで論じたような、HTTP/HTTP(S)上の暗黙に保護された双方向のメッセージングを提供するブリッジ・ソフトウェアを実行する。

1つの実装では、これまで論じてきた方法は、複数の企業が、インターネットの使用を通じてアプリケーション・サービス・コンピュータにアクセスしているクライアント・コンピュータから、ネットワーク通信を可能にするサービスに加入することを可能にし、そのインターネットでは、アプリケーション・サービス・コンピュータは、ファイアウォールのようなセキュリティ機器によって、一般のインターネット・アクセスから保護されており、メッセージ・アドレス確認コンピュータは、トンネルの保守を可能にするサービスとして利用できる。この例では、メッセージ・アドレス確認コンピュータの所有者は、アプリケーション・サービス・コンピュータおよび対応するファイアウォールトンネル・コンピュータの所有者に同意する。同意では、例えば、アプリケーションの加入者の任意のメッセージ識別子を変更しないという条件があり、このため、アプリケーションの所有者のセキュリティの権利は保護される。

図3において、第1の情報処理プラットフォーム（IPP）312と第2の情報処理プラットフォーム（IPP）302の間の相互メッセージ詳細300は、ファイアウォールトンネルを可能にするネットワークリンクをさらに拡張するアプリケーション間の、マルチプロトコル通信をサポートするメッセージ指向ミドルウェアを示している。この点において、情報処理プラットフォーム312と302は、ともにアプリケーション・サービス・コンピューター120に類似しており、コンピューター・ネットワーク100に対して論じてきた方法、あるいは地形に従った通信の中でメッセージを交換する。個別メッセージは、IPP312の中の多重化装置304の中で多重化され、IPP302の中で、復号されてアプリケーション・キュー308に配送される。各々のアプリケーション（例として、相互メッセージ詳細300に示す、APP__11、APP__1N、APP__21、APP__2N）は、アプリケーションを実行するIPPの復号装置からメッセージを受信するため、それぞれ自分のアプリケーション・キュー（例の中で、IPP302の中のAPP__11に特に関連付けられたキュー308）を持つ。アプリケーション310は、多重化装置304内で、メッセージを優先的に多重化する特定のメッセージフォーマット（プロトコル）を定義する。そのような専用の受信キューは、アプリケーション・サービス・コンピューターのネットワーク100に、同期・非同期にメッセージを配送し、アプリケーション開発者に対して、広範囲で柔軟性のある通信ミドルウェアを提供する。専用のキューはまた、同じ情報処理プラットフォーム（の“スレッド”）の中で走行するアプリケーションの間、および／また、異なる情報処理プラットフォーム（の“プロセス”）の中で走行するアプリケーションの間で、柔軟なメッセージ交換の基礎を提供する。

このような発明の実施の形態によれば、アプリケーションサービス・コンピューターとファイアウォールトンネル・コンピューター間、およびファイアウォールトンネル・コンピューターとメッセージ・アドレス確認コンピューター間、メッセージ・アドレス確認コンピューターとクライアント・コンピューター間にブリッジを行い、ファイアウォールとトンネルしてHTTP（S）プロトコルにて接続し、メッセージ・アドレス確認コンピューターは、メッセージのアドレスからインターネットの正当なユーザであるもののみに、ファイアウォールトンネル・コンピューターへの経路を指示することにより、セキュリティを確保し、ファイアウォールに特別な設定を行うこ

となくアプリケーションに通信のアクセス経路を提供することが可能となる。また、メッセージのキューを設けてアプリケーションごとにキューを設け、情報処理プラットフォームにて多重化通信を行うようにするため、効率的に通信を行うことができる。また、アプリケーションのプロトコル通信をブリッジするため、アプリケーションに特別な仕組みは不要となる。

発明の説明は本来単に典型的なものに過ぎない。従って、発明の要旨からそれるものでないバリエーションは、発明の範囲内にあるものと意図する。そのようなバリエーションは、発明の精神と範囲に背くものであると注意する。

請求の範囲

1. メッセージ・アドレス確認コンピュータに対する第1の任意のメッセージ、およびアプリケーションサービス・コンピュータへインターネットへのインタフェースおよび前記メッセージ・アドレス確認コンピュータへの前記インターネットへのインタフェースを提供するファイアウォールトンネル・コンピュータに対する第2の任意のメッセージに対してクライアント・コンピュータと前記アプリケーションサービス・コンピュータ間の各コンピュータ・メッセージ・インスタンスを有効にする手段で構成され、

前記インターネットの使用を通じて、前記クライアント・コンピュータから前記アプリケーションサービス・コンピュータにアクセスする

ことを特徴とするインターネットセキュア通信方法。

2. 前記第1の任意のメッセージは、前記クライアント・コンピュータの識別子に関連する前記ファイアウォールトンネル・コンピュータの識別子で構成されることを特徴とする請求項1に記載のインターネットセキュア通信方法。

3. 前記第1の任意のメッセージは、さらに前記ファイアウォールトンネル・コンピュータの前記識別子と前記クライアント・コンピュータの前記識別子に関連する前記アプリケーションサービス・コンピュータの識別子で構成されることを特徴とする請求項2に記載のインターネットセキュア通信方法。

4. 前記識別子は、前記アプリケーションサービス・コンピュータの論理識別子で構成されることを特徴とする請求項3に記載のインターネットセキュア通信方法。

5. 前記識別子は、前記アプリケーションサービス・コンピュータのアプリケーションの論理識別子で構成されることを特徴とする請求項3に記載のインターネットセキュア通信方法。

6. 前記第2の任意のメッセージは、前記アプリケーションサービス・コンピュータの識別子で構成される

ことを特徴とする請求項1に記載のインターネットセキュア通信方法。

7. 前記第2の任意のメッセージは、さらに前記クライアント・コンピュータの識別子で構成される

ことを特徴とする請求項6に記載のインターネットセキュア通信方法。

8. 前記第1の任意のメッセージは、前記ファイアウォールトンネル・コンピュータによって前記メッセージ・アドレス確認コンピュータ内に定義される

ことを特徴とする請求項1に記載のインターネットセキュア通信方法。

9. 前記アプリケーションサービス・コンピュータによって前記クライアント・コンピュータのパスワードを有効にする手段を有する

ことを特徴とする請求項1に記載のインターネットセキュア通信方法。

10. 前記メッセージ・アドレス確認コンピュータによって前記ファイアウォールトンネル・コンピュータのパスワードを有効にする手段を有する

ことを特徴とする請求項1に記載のインターネットセキュア通信方法。

11. 前記メッセージ・アドレス確認コンピュータは、第1の所有者に所有される手段を有し、前記アプリケーションサービス・コンピュータと前記ファイアウォールトンネル・コンピュータは、第2の所有者に所有される手段を有するとともに、

前記第1の所有者と第2の所有者は、前記第1の所有者が前記第1の任意のメッセージを編集しないようにすることを合意するように構成する手段を有する

ことを特徴とする請求項1に記載のインターネットセキュア通信方法。

12. 前記ファイアウォールトンネル・コンピュータは、外部へのHTTPプロ

トコル通信が通過できるようにファイアウォールによって設定されたファイアウォールのポートを通じてインターネットに接続するインタフェースを有し、

前記ファイアウォールは、基本的に恒久的にいかなる内部への通信もブロックするように設定され、前記ファイアウォールを通過する双方向のメッセージを許可するように前記ファイアウォールのポートを再設定することが必要でないように、内部への通信は前記外部への通信と相互的でない

ことを特徴とする請求項 1 に記載のインターネットセキュア通信方法。

13. アプリケーションサービス・コンピュータとインターネットへのデータ通信を行うファイアウォールトンネル・コンピュータと、前記インターネットから前記ファイアウォールトンネル・コンピュータへのデータ通信を行い、前記インターネットからクライアント・コンピュータへのデータ通信を行うメッセージ・アドレス確認コンピュータと、前記メッセージ・アドレス確認コンピュータ内の第 1 の任意のデータベース、および前記ファイアウォールトンネル・コンピュータ内の第 2 の任意のデータベースに対する、前記クライアント・コンピュータと前記アプリケーションサービス・コンピュータ間の前記通信の各コンピュータメッセージのインスタンスの検証手段で構成され、

前記インターネットの使用を通じて、前記クライアント・コンピュータから前記アプリケーションサービス・コンピュータにアクセスする

ことを特徴とするインターネットセキュア通信方法。

14. 前記第 1 の任意のメッセージのデータベースは、前記クライアント・コンピュータに対する識別子に関連した、前記ファイアウォールトンネル・コンピュータに対する識別子を有するデータレコードで構成し、前記データレコードのアドレスは前記ファイアウォールトンネル・コンピュータから、前記第 1 の任意のデータベースのメッセージの中に定義される

ことを特徴とする請求項 13 に記載のインターネットセキュア通信方法。

15. 前記データレコードは、さらに前記アプリケーションサービス・コンピュ

ターに対する識別子で構成する

ことを特徴とする請求項 14 に記載のインターネットセキュア通信方法。

16. 前記第2の任意のメッセージのデータベースは、前記アプリケーションサービス・コンピュータに対する識別子を有するデータレコードで構成される

ことを特徴とする請求項 13 に記載のインターネットセキュア通信方法。

17. 前記第2の任意のメッセージのデータベースは、さらに前記クライアント・コンピュータに対する識別子を有する

ことを特徴とする請求項 16 に記載のインターネットセキュア通信方法。

18. アプリケーションサービス・コンピュータ、およびインターネットとデータ通信を行う、ファイアウォールトンネル・コンピュータであって、前記ファイアウォールトンネル・コンピュータは、クライアント・コンピュータと前記アプリケーションサービス・コンピュータとの間の前記データ通信の各コンピュータメッセージのインスタンスを有効にするようにプログラムされており、前記インターネットから前記ファイアウォールトンネル・コンピュータへのデータ通信と、

前記インターネットから前記クライアント・コンピュータへのデータ通信を行うメッセージ・アドレス確認コンピュータであって、前記メッセージ・アドレス確認コンピュータは、前記クライアント・コンピュータと、前記アプリケーションサービス・コンピュータとの間の前記データ通信の各コンピュータメッセージのインスタンスを有効にするようにプログラムされており、前記インターネットの使用を通じて、前記クライアント・コンピュータから前記アプリケーションサービス・コンピュータへアクセスする

ことを特徴とするインターネットセキュア通信装置。

19. 前記メッセージ・アドレス確認コンピュータは、前記クライアント・コンピュータに対する識別子と関連した、前記ファイアウォールトンネル・コンピュータに対する識別子を有する任意のデータベースを有する

ことを特徴とする請求項 18 に記載のインターネットセキュア通信装置。

20. 前記メッセージ・アドレス確認コンピューターと、前記ファイアウォールトンネル・コンピューターは、前記ファイアウォールトンネル・コンピューターが、前記メッセージ・アドレス確認コンピューターの中にある、前記任意のデータベースを変更することを可能にするようにプログラムされている

ことを特徴とする請求項 19 に記載のインターネットセキュア通信装置。

21. メッセージ・アドレス確認コンピューター内の第1の任意のメッセージ、およびファイアウォールトンネル・コンピューター内の第2の任意のメッセージに対する、クライアント・コンピューターとアプリケーションサービス・コンピューターとの間の各コンピューターメッセージのインスタンスを有効にする手段を有し、

前記ファイアウォールトンネル・コンピューターは、前記インターネットとのインタフェースを有し、

前記メッセージ・アドレス確認コンピューターは、前記インターネットとのインタフェースを有し、

前記インターネットの使用を通じて、前記クライアント・コンピューターから、前記アプリケーションサービス・コンピューターへアクセスする

ことを特徴とするインターネットセキュア通信装置。

22. 前記ファイアウォールトンネル・コンピューターによって、前記第1の任意のメッセージを定義する手段を有する

ことを特徴とする請求項 21 に記載のインターネットセキュア通信装置。

23. 前記ファイアウォールトンネル・コンピューターは、ブリッジ・コンピューターのプログラムを実行し、

前記アプリケーションサービス・コンピューターの中のアプリケーション・プログラムは、前記メッセージ・アドレス確認コンピューターによって、HTTPメッセージ配送メカニズムが生成されるように、前記ブリッジ・コンピューターのプログラム

を制御する

ことを特徴とする請求項 1 に記載のインターネットセキュア通信方法。

24. 前記ファイアウォールトンネル・コンピューターは、ブリッジ・コンピューターのプログラムを実行し、

前記ブリッジ・コンピューターのプログラムは、前記メッセージ・アドレス確認コンピューターへの HTTP 接続の開始、および前記アプリケーションサービス・コンピューターへの HTTP 接続の開始によって、ブリッジ・コンピューターのソフトウェアのインスタンスを生成し、

前記メッセージ・アドレス確認コンピューターは、前記ブリッジ・コンピューターのソフトウェアのインスタンスを認証する

ことを特徴とする請求項 12 に記載のインターネットセキュア通信方法。

25. 前記ファイアウォールトンネル・コンピューターは、ブリッジ・コンピューターのプログラムを実行し、

前記ブリッジ・コンピューターのプログラムは、前記メッセージ・アドレス確認コンピューターへの HTTP 接続の開始、および前記アプリケーションサービス・コンピューターへの HTTP 接続の開始によって、ブリッジ・コンピューターのソフトウェアのインスタンスを生成し、

前記ブリッジ・コンピューターのプログラムは、各々の前記 HTTP 接続に対して定義された、送信メッセージ・バッファと受信メッセージ・バッファからなる一対のメッセージ・バッファを定義し、

前記一対のメッセージ・バッファは、メッセージを前記メッセージ・アドレス確認コンピューター内で実行されているブリッジサービスのプログラムと、前記アプリケーションサービス・コンピューター内で実行されているブリッジサービス・サーバーのプログラムの間を双方向に転送する

ことを特徴とする請求項 12 に記載のインターネットセキュア通信方法。

26. 前記ファイアウォールトンネル・コンピューターは、トランスポート層とメ

ッセージ処理層を持つブリッジ・コンピュータのプログラムを実行し、

前記トランスポート層は、前記メッセージ・アドレス確認コンピュータへ第1のHTTP接続および、前記アプリケーションサービス・コンピュータへ第2のHTTP接続を開始し、

前記メッセージ処理層は、各々の前記HTTP接続に対して定義された、送信メッセージ・バッファと受信メッセージ・バッファからなる一対のメッセージ・バッファを定義し、

前記トランスポート層は、前記メッセージ・アドレス確認コンピュータから前記第1の接続を経由する通信の第1のメッセージを検索し、

前記メッセージ処理層は、前記第1のメッセージに書かれた許可ルールを実行し、

前記メッセージ処理層は、前記第1のメッセージを前記第1の接続の受信メッセージ・バッファから前記第2の接続の送信メッセージ・バッファへ移動し、

前記トランスポート層は、前記第2の接続を経由して、前記アプリケーションサービス・コンピュータへ前記第1のメッセージを送信し、

前記トランスポート層は、前記アプリケーションサービス・コンピュータから前記第2の接続を経由する通信の第2のメッセージを検索し、

前記メッセージ処理層は前記第2のメッセージに書かれた許可ルールを実行し、

前記メッセージ処理層は、前記第2のメッセージを前記第2の接続の受信メッセージ・バッファから前記第1の接続の送信メッセージ・バッファへ移動し、

前記トランスポート層は、前記第1の接続を経由して、前記メッセージ・アドレス確認コンピュータへ前記第1のメッセージを送信する

ことを特徴とする請求項12に記載のインターネットセキュア通信方法。

27. 前記通信中のメッセージは、異なるアプリケーションに対して、各々異なるプロトコルが組み立てられている

ことを特徴とする請求項12に記載のインターネットセキュア通信方法。

28. 前記ファイアウォールトンネル・コンピュータは、トランスポート層とメッセージ処理層を持つブリッジ・コンピュータのプログラムを実行し、

前記トランスポート層は、前記メッセージ・アドレス確認コンピューターへの多数のメッセージと、前記アプリケーションサービス・コンピューターへの多数のメッセージを多重化送信する

ことを特徴とする請求項 1 2 に記載のインターネットセキュア通信方法。

29. 前記ファイアウォールトンネル・コンピューターは、トランスポート層とメッセージ処理層を持つブリッジ・コンピューターのプログラムを実行し、

前記トランスポート層は、前記メッセージ・アドレス確認コンピューター内のブリッジサービス・プログラムからの多数のメッセージ、および前記アプリケーションサービス・コンピューターからの多数のメッセージを多重化受信する

ことを特徴する請求項 1 2 に記載のインターネットセキュア通信方法。

30. 前記ファイアウォールトンネル・コンピューターは、トランスポート層とメッセージ処理層を持つブリッジ・コンピューターのプログラムを実行し、

前記トランスポート層は、前記メッセージ・アドレス確認コンピューターと十分な多数の HTTP 接続、および前記アプリケーションサービス・コンピューターと十分な多数の HTTP 接続を生成し、

全てのメッセージのレイテンシーは、予め定義されたレイテンシー値の範囲内で持続し、

全てのメッセージのスループットは予め定義されたスループット値の範囲内で持続する

ことを特徴とする請求項 1 2 に記載のインターネットセキュア通信方法。

31. 多数のファイアウォールトンネル・コンピューターは、前記メッセージ・アドレス確認コンピューターと通信し、

各々のファイアウォールトンネル・コンピューターは、前記メッセージを可能にするブリッジコンピューター・プログラムを実行する

ことを特徴とする請求項 1 2 に記載のインターネットセキュア通信方法。

32. 多数のファイアウォールトンネル・コンピュータは、前記メッセージ・アドレス確認コンピュータと通信し、

各々のファイアウォールトンネル・コンピュータは、前記メッセージを可能にするブリッジコンピュータ・プログラムを実行し、

前記メッセージ・アドレス確認コンピュータは、前記多数のファイアウォールトンネル・コンピュータ内のブリッジコンピュータ・プログラムと通信するブリッジサービス・プログラムを実行する

ことを特徴とする請求項1に記載のインターネットセキュア通信方法。

33. 各コンピュータメッセージのインスタンスを有効にする手段は、さらに各々の前記ファイアウォールトンネル・コンピュータ内のブリッジコンピュータ・プログラムと、前記メッセージ・アドレス確認コンピュータ内のブリッジサービス・プログラムで構成され、

前記ブリッジサービス・プログラムは、各前記ブリッジコンピュータ・プログラムに対して、送信メッセージ・バッファを定義し、

前記ブリッジサービス・プログラムは、その各々の前記送信メッセージ・バッファ内の各前記ブリッジコンピュータ・プログラムと通信する各メッセージ・インスタンスをバッファする

ことを特徴とする請求項21に記載のインターネットセキュア通信装置。

34. 前記ブリッジサービス・プログラムは、1つのブリッジコンピュータ・プログラムから送信された多数のメッセージをバッファする

ことを特徴とする請求項33に記載のインターネットセキュア通信装置。

35. 各コンピュータメッセージのインスタンスを有効にする手段は、さらに各々の前記ファイアウォールトンネル・コンピュータ内のブリッジコンピュータ・プログラムと、前記メッセージ・アドレス確認コンピュータ内のブリッジサービス・プログラムで構成され、

前記ブリッジサービス・プログラムは、各ブリッジコンピュータ・プログラムに

よって送信された多数のメッセージを受け入れることが可能であり、

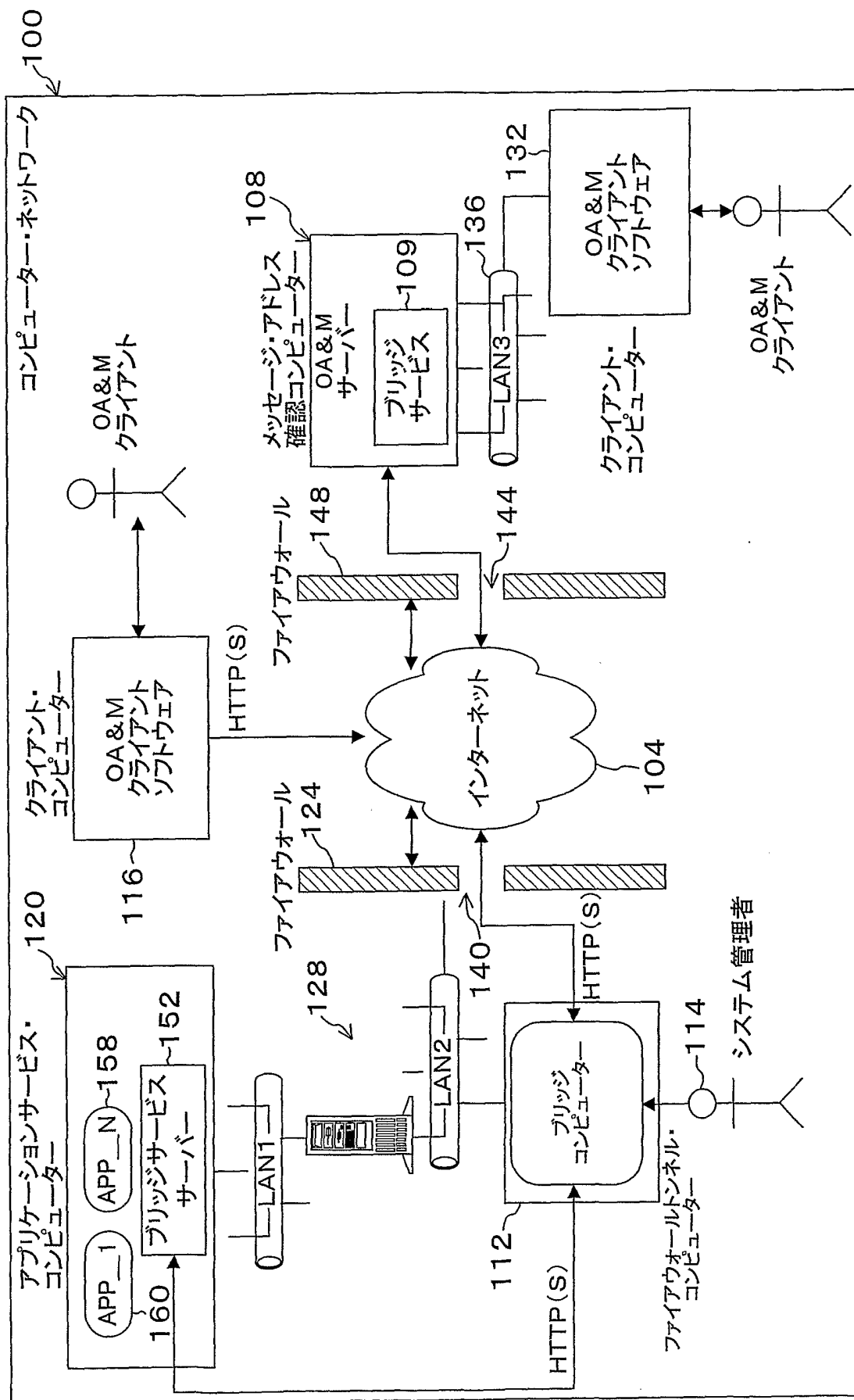
前記ブリッジサービス・プログラムは、各前記ブリッジコンピューター・プログラムに対して送信メッセージ・バッファを定義し、

前記ブリッジサービス・プログラムは、その各々の前記送信メッセージ・バッファ内の各前記ブリッジコンピューター・プログラムと通信する各メッセージ・インスタンスをバッファし、

前記ブリッジサービス・プログラムは、各メッセージを同一数のアプリケーションメッセージキューに転送する

ことを特徴とする請求項 21 に記載のインターネットセキュア通信装置。

FIG.1



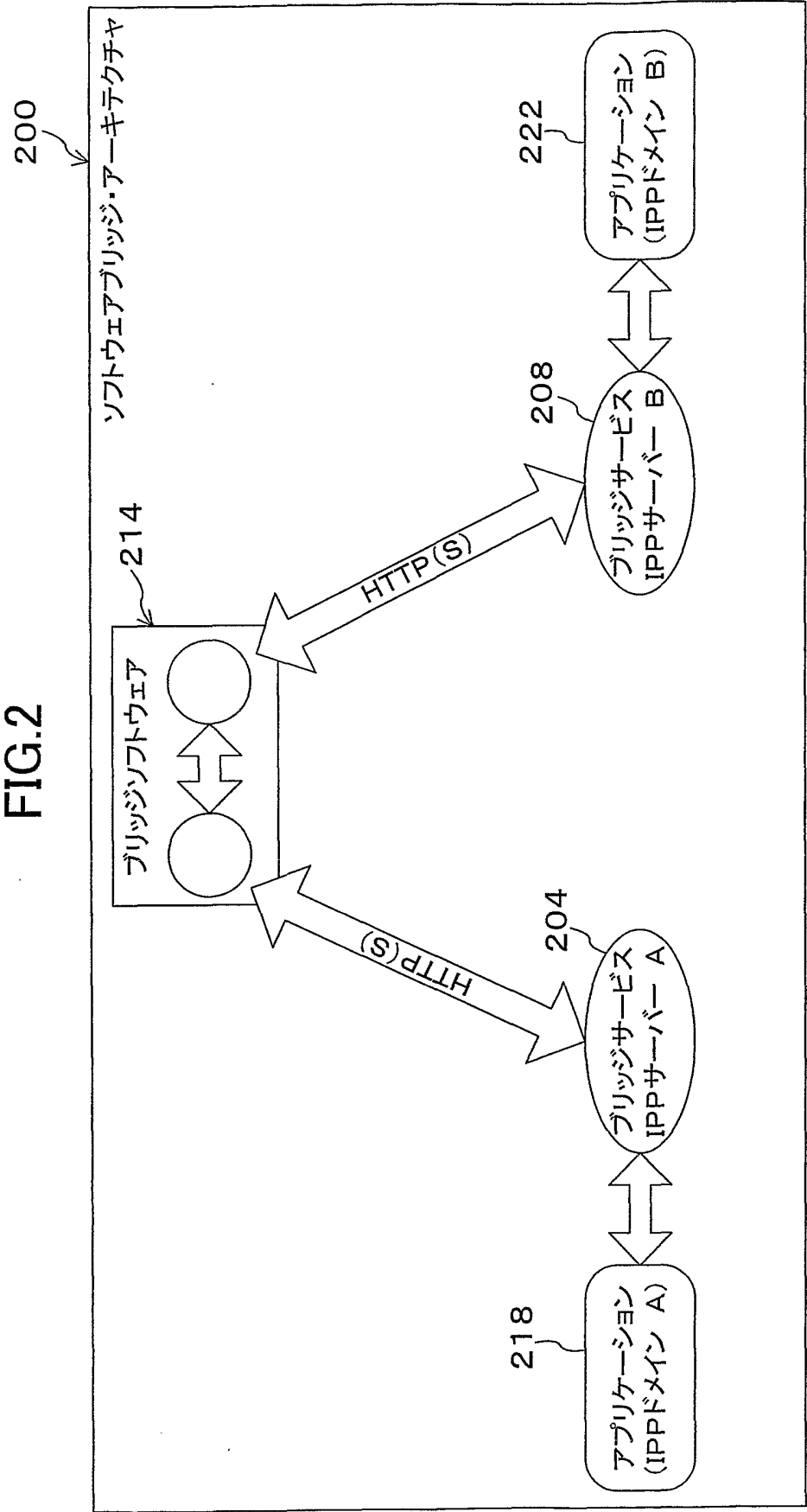


FIG.3

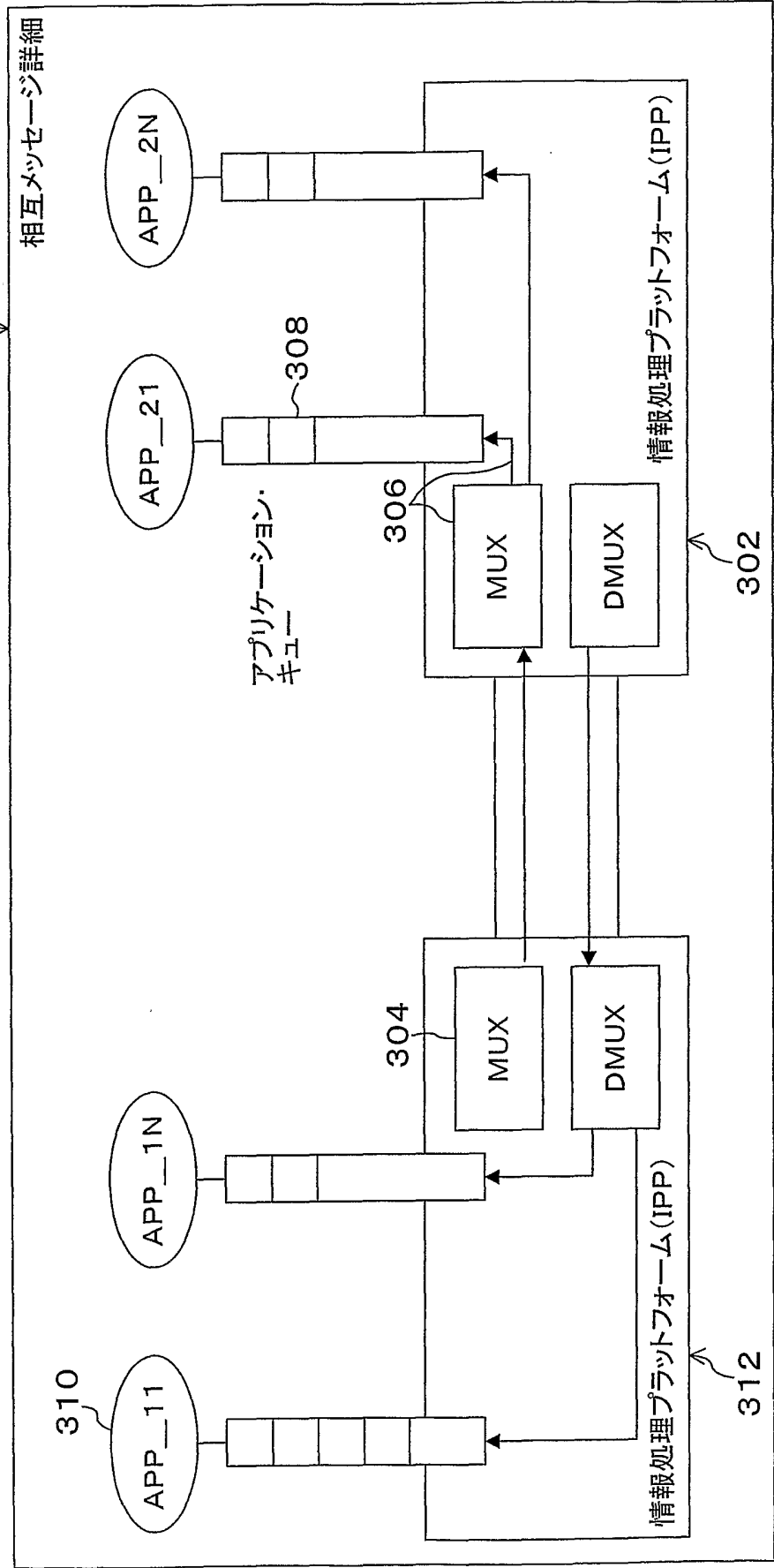
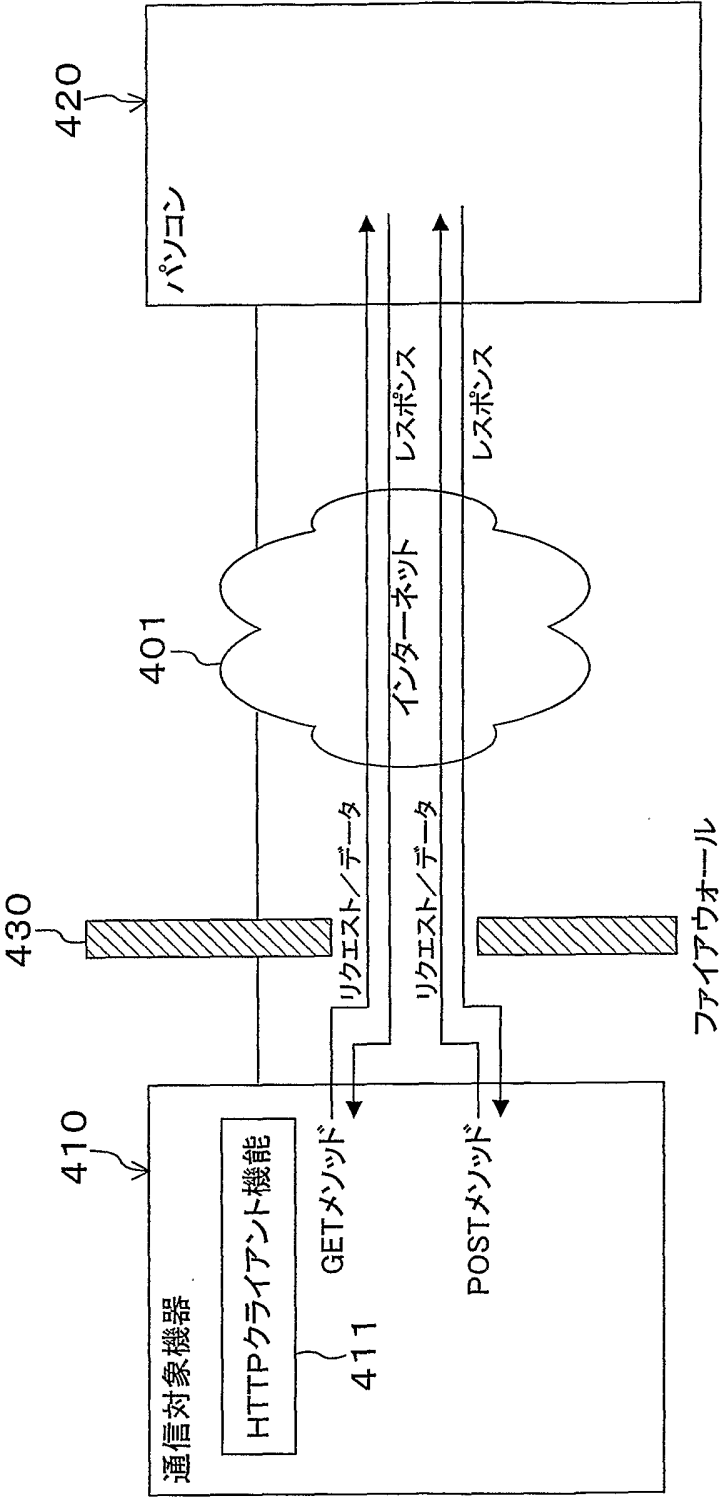


FIG.4



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/008183

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F13/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004

Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST FILE[FAIAWORU*(TONNERU+TONNERINGU)] (in Japanese)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 10-154118 A (Hitachi, Ltd.), 09 June, 1998 (09.06.98), Page 4, column 5, line 45 to column 6, lines 7, 36 to page 5, column 8, line 25; Fig. 7 (Family: none)	1-35
Y	JP 2002-271396 A (International Business Machines Corp.), 20 September, 2002 (20.09.02), Page 7, column 12, line 8 to page 8, column 14, line 43; Fig. 3 & GB 2365668 A	1-23, 27-29, 31-35

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
28 September, 2004 (28.09.04)Date of mailing of the international search report
12 October, 2004 (12.10.04)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/008183

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2000-216780 A (Hitachi, Ltd.), 04 August, 2000 (04.08.00), Page 8, lines 14, 11 to 41 (Family: none)	9-10
Y	JP 2002-190821 A (Fujitsu Ltd.), 05 July, 2002 (05.07.02), Page 5, column 7, line 6 to column 8, line 47; Fig. 3 & US 2002/0083191 A1	24-26, 30
A	JP 2000-207320 A (Sun Micro Systems Inc.), 28 July, 2000 (28.07.00), Full text; Figs. 1 to 6 & EP 969368 A3 & US 6233688 B1	1-35
A	JP 9-214556 A (Toshiba Corp.), 15 August, 1997 (15.08.97), Full text; Figs. 1 to 32 & US 6092191 A	1-35

A. 発明の属する分野の分類 (国際特許分類 (IPC))		
Int. Cl ⁷ G06F 13/00		
B. 調査を行った分野		
調査を行った最小限資料 (国際特許分類 (IPC))		
Int. Cl ⁷ G06F 13/00		
最小限資料以外の資料で調査を行った分野に含まれるもの		
日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2004年 日本国登録実用新案公報 1994-2004年 日本国実用新案登録公報 1996-2004年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語) JICST科学技術文献ファイル「ファイアウォール* (トンネル+トンネリング)」		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 10-154118 A (株式会社日立製作所) 1998.06.09, 第4頁, 第5欄, 第45行-第6欄, 第7 行, 第36行-第5頁, 第8欄, 第25行, 第7図 (ファミリーなし)	1-35
Y	JP 2002-271396 A (インターナショナル・ビジネ ス・マシーンズ・コーポレーション), 2002.09.20, 第7頁, 第12欄, 第8行-第8頁, 第14欄, 第43行, 第3図 &GB 2365668 A	1-23, 27-29 , 31-35
☒ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日 28.09.2004	国際調査報告の発送日 12.10.2004	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 石井 茂和	5R 8837
電話番号 03-3581-1101 内線 6790		

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2000-216780 A (株式会社日立製作所) 2000.08.04, 第8頁, 第14行, 第11-41行 (ファミリーなし)	9-10
Y	JP 2002-190821 A (富士通株式会社) 2002.07.05, 第5頁, 第7欄, 第6行-第8欄, 第47 行, 第3図 & US 2002/0083191 A1	24-26, 30
A	JP 2000-207320 A (サン・マイクロシステムズ・インコーポレーテッド) 2000.07.28, 全文, 第1-6図 & EP 969368 A3 & US 6233688 B1	1-35
A	JP 9-214556 A (株式会社東芝) 1997.08.15, 全文, 第1-32図 & US 6092191 A	1-35