

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5044646号
(P5044646)

(45) 発行日 平成24年10月10日(2012.10.10)

(24) 登録日 平成24年7月20日(2012.7.20)

(51) Int.Cl.		F I			
GO6F	13/00	(2006.01)	GO6F	13/00	510A
HO4L	12/66	(2006.01)	GO6F	13/00	351Z
			HO4L	12/66	B

請求項の数 13 (全 21 頁)

(21) 出願番号	特願2009-516071 (P2009-516071)	(73) 特許権者	310021766 株式会社ソニー・コンピュータエンタテインメント 東京都港区港南1丁目7番1号
(86) (22) 出願日	平成19年5月25日(2007.5.25)	(74) 代理人	100108006 弁理士 松下 昌弘
(86) 国際出願番号	PCT/JP2007/000561	(72) 発明者	前川 博俊 東京都港区南青山二丁目6番21号 株式会社ソニー・コンピュータエンタテインメント内
(87) 国際公開番号	W02008/146328	(72) 発明者	尾山 一文 東京都港区南青山二丁目6番21号 株式会社ソニー・コンピュータエンタテインメント内
(87) 国際公開日	平成20年12月4日(2008.12.4)		
審査請求日	平成21年6月9日(2009.6.9)		

最終頁に続く

(54) 【発明の名称】 サーバシステム、通信方法、コンピュータ、プログラムおよび記録媒体

(57) 【特許請求の範囲】

【請求項1】

ネットワークを介してクライアント装置と通信するサーバシステムであって、
 第1のファイアウォールと、
 前記第1のファイアウォールおよび前記ネットワークを介して前記クライアント装置と接続する第1のサーバと、
 前記第1のファイアウォールを介さずに、前記ネットワークを介して前記クライアント装置と接続する第2のサーバと
 を有し、
 前記第1のサーバが、前記ネットワーク上のグローバルIPアドレスが割り当てられていない前記第2のサーバに対して、前記サーバシステム内の通信回線を介してSTUN機能により、前記グローバルIPアドレスを割り当て、
 前記第1のサーバが、前記第1のファイアウォールを介して前記クライアント装置との間でHTTPプロトコルによる通信を行い、前記第2のサーバに割り当てた前記グローバルIPアドレスを前記クライアント装置に送信し、
 前記第2のサーバが、前記割り当てられた前記グローバルIPアドレスを用いて前記クライアント装置とP2P型通信プロトコルによる通信を行い、当該通信において、前記クライアント装置と第1のサーバとの間で前記第1のファイアウォールを介してHTTPプロトコルによる通信によって取得した暗号鍵を用いて、データを暗号化して前記第1のファイアウォールを介さずに前記クライアント装置に送信する

10

20

サーバシステム。

【請求項 2】

前記第 1 のサーバは、

前記第 1 のクライアント装置とセキュリティが要求される処理を行うフロントエンドサーバ機能部と、

データベースアクセス処理またはファイルシステム共有関連処理のプログラムを実行し、コンテンツデータを前記サーバシステム内の通信回線を介して前記第 2 のサーバに送信するバックエンドサーバ機能部と、

前記フロントエンドサーバ機能部と前記バックエンドサーバ機能部との間の通信でファイアウォール機能を発揮する第 2 のファイアウォールと、

前記バックエンドサーバ機能部と前記第 2 のサーバとの間の通信でファイアウォール機能を発揮する第 3 のファイアウォールと

を有する請求項 1 に記載のサーバシステム。

10

【請求項 3】

前記第 1 のサーバは、所定のサイトから前記クライアント装置にダウンロードされたクライアントアプリケーションプログラムを起動し、

前記第 2 のサーバは、前記クライアント装置の前記起動されたクライアントアプリケーションプログラムと通信を行う

請求項 1 に記載のサーバシステム。

【請求項 4】

前記第 2 のサーバは、前記クライアント装置が実行する前記クライアントアプリケーションプログラムに対応したサーバアプリケーションプログラムを実行する

請求項 3 に記載のサーバシステム。

20

【請求項 5】

前記第 2 のサーバは、少なくとも一つの管理プロセッサと、複数の計算実行プロセッサとで前記サーバアプリケーションプログラムを実行する

請求項 1 に記載のサーバシステム。

【請求項 6】

前記第 2 のサーバは、ネットワーク上のアプリケーション情報を取得し、当該情報を前記クライアント装置に送信し、

前記クライアント装置は、前記第 2 のサーバから取得した情報を基に、前記クライアントアプリケーションプログラムを取得する

請求項 4 に記載のサーバシステム。

30

【請求項 7】

前記第 1 のサーバおよび前記第 2 のサーバの機能は、同一の回路あるいは異なる処理回路によって実現されている

請求項 1 に記載のサーバシステム。

【請求項 8】

前記クライアント装置と前記第 2 のサーバとの間の通信時に、ネットワーク上でグローバルに前記第 2 のサーバを特定するグローバルアドレスと、前記第 1 のサーバおよび前記第 2 のサーバ側でローカルに前記第 2 のサーバを特定するローカルアドレスとの間でアドレス変換を行うアドレス変換手段

をさらに有する請求項 1 ~ 7 のいずれかに記載のサーバシステム。

40

【請求項 9】

前記第 2 のサーバは、複数の演算機能モジュールを有し、各演算機能モジュールがアプリケーションプログラムを個別に実行し、

前記第 1 のサーバは、前記演算機能モジュールの各々に固有のグローバルアドレスおよびポートの組み合わせを割り当て、

前記演算機能モジュールは、自らが実行するアプリケーションプログラムに対応する、グローバルアドレスおよびポートの組み合わせ情報を基に、前記クライアント装置との通

50

信を行う

請求項 1 ~ 8 のいずれかに記載のサーバシステム。

【請求項 10】

ファイアウォールと、

前記ファイアウォールおよびネットワークを介してクライアント装置と接続する第 1 のサーバと、

前記ファイアウォールを介さずに、前記ネットワークを介して前記クライアント装置と接続する第 2 のサーバと

を有するサーバシステムがネットワークを介して前記クライアント装置と通信する通信方法であって、

10

前記第 1 のサーバが、前記ネットワーク上のグローバル IP アドレスが割り当てられていない前記第 2 のサーバに対して、前記サーバシステム内の通信回線を介して STUN 機能により、前記グローバル IP アドレスを割り当て、

前記第 1 のサーバが、前記ファイアウォールを介して前記クライアント装置との間で HTTP プロトコルによる通信を行い、前記第 2 のサーバに割り当てた前記グローバル IP アドレスを前記クライアント装置に送信し、

前記クライアント装置が、前記ファイアウォールを介して HTTP プロトコルによる通信を前記第 1 のサーバとの間で行って暗号鍵を取得あるいは特定し、

前記第 2 のサーバが、前記割り当てられた前記グローバル IP アドレスを用いて前記クライアント装置と P2P 型通信プロトコルによる通信を行い、当該通信において、前記クライアント装置が前記取得あるいは特定した暗号鍵を用いて、データを暗号化して前記ファイアウォールを介さずに前記クライアント装置に送信する

20

通信方法。

【請求項 11】

第 1 のサーバとのサーバ側のファイアウォールを介した通信に用いられるデータと、第 2 のサーバとの前記ファイアウォールを介さない通信に用いられるデータとを送受信するインタフェースと、

処理回路とを有し、

前記処理回路は、

ネットワーク上のグローバル IP アドレスが割り当てられていない前記第 2 のサーバに対して前記第 1 のサーバが割り当てた前記グローバル IP アドレスを、前記ファイアウォールおよび前記ネットワークを介して、前記第 1 のサーバとの間で HTTP プロトコルによる通信を行って取得し、

30

前記ファイアウォールを介して HTTP プロトコルによる通信を前記第 1 のサーバとの間で行って暗号鍵を取得あるいは特定し、

前記割り当てられた前記グローバル IP アドレスを用いて前記第 2 のサーバと P2P 型通信プロトコルによる通信を行い、当該通信において受信した前記暗号鍵で暗号化されたデータを復号する

コンピュータ。

【請求項 12】

第 1 のサーバとのサーバ側のファイアウォールを介した通信と、第 2 のサーバとの前記ファイアウォールを介さない通信とを行うコンピュータが実行するプログラムであって、

ネットワーク上のグローバル IP アドレスが割り当てられていない前記第 2 のサーバに対して前記第 1 のサーバが割り当てた前記グローバル IP アドレスを、前記ファイアウォールおよび前記ネットワークを介して、前記第 1 のサーバとの間で HTTP プロトコルによる通信を行って取得する第 1 の手順と、

40

前記ファイアウォールを介して HTTP プロトコルによる通信を前記第 1 のサーバとの間で行って暗号鍵を取得あるいは特定する第 2 の手順と、

前記割り当てた前記グローバル IP アドレスを用いて前記第 2 のサーバと P2P 型通信プロトコルによる通信を行い、当該通信において受信した前記暗号鍵で暗号化されたデー

50

タを復号する第3の手順と

を前記コンピュータに実行させるプログラム。

【請求項13】

第1のサーバとのサーバ側のファイアウォールを介した通信と、第2のサーバとの前記ファイアウォールを介さない通信とを行うコンピュータが実行するプログラムを記録する記録媒体であって、

ネットワーク上のグローバルIPアドレスが割り当てられていない前記第2のサーバに対して前記第1のサーバが割り当てた前記グローバルIPアドレスを、前記ファイアウォールおよび前記ネットワークを介して、前記第1のサーバとの間でHTTPプロトコルによる通信を行って取得する第1の手順と、

前記ファイアウォールを介してHTTPプロトコルによる通信を前記第1のサーバとの間で行って暗号鍵を取得あるいは特定する第2の手順と、

前記割り当てた前記グローバルIPアドレスを用いて前記第2のサーバとP2P型通信プロトコルによる通信を行い、当該通信において受信した前記暗号鍵で暗号化されたデータを復号する第3の手順と

を前記プログラムは前記コンピュータに実行させる記録媒体。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、サーバとクライアント装置との間で通信を行う場合に用いられるサーバシステム、通信方法、コンピュータ、プログラムおよび記録媒体に関するものである。

【背景技術】

【0002】

例えば、ネットワーク上のコンテンツの販売サイトなどのサーバに端末からアクセスし、購入するコンテンツを指定して電子決済を行った後に、コンテンツデータをダウンロードする場合がある。

このようなシステムにおいて、サーバ側には、単数または複数のファイアウォールが構築されており、サーバと端末との間の通信は全てファイアウォールを介して行われる。

これにより、サーバをネットワーク上のコンピュータからの不正な攻撃から防御している。

【発明の開示】

【発明が解決しようとする課題】

【0003】

しかしながら、上述した従来のシステムでは、ネットワーク上のコンピュータからの不正な攻撃からサーバを防御できる反面、正当なクライアント装置がサーバからコンテンツデータ等をダウンロードする場合に、ファイアウォールを介することで応答性が悪いという問題がある。

また、クライアント装置とサーバ間でのアプリケーション構築と実行の柔軟性に欠けるという問題がある。

【0004】

本発明はかかる事情に鑑みてなされたものであり、その目的は、高い安全性と応答性とを兼ね備えたサーバシステム、通信方法、コンピュータ、プログラムおよび記録媒体を提供することにある。

【課題を解決するための手段】

【0005】

上述した従来技術の問題を解決し、上述した目的を達成するために、第1の観点の発明のサーバシステムは、ネットワークを介してクライアント装置と通信するサーバシステムであって、第1のファイアウォールと、前記第1のファイアウォールおよび前記ネットワークを介して前記クライアント装置と接続する第1のサーバと、前記第1のファイアウォールを介さずに、前記ネットワークを介して前記クライアント装置と接続する第2のサー

10

20

30

40

50

バとを有し、前記第1のサーバが、前記ネットワーク上のグローバルIPアドレスが割り当てられていない前記第2のサーバに対して、前記サーバシステム内の通信回線を介してSTUN機能により、前記グローバルIPアドレスを割り当て、前記第1のサーバが、前記第1のファイアウォールを介して前記クライアント装置との間でHTTPプロトコルによる通信を行い、前記第2のサーバに割り当てた前記グローバルIPアドレスを前記クライアント装置に送信し、前記第2のサーバが、前記割り当てられた前記グローバルIPアドレスを用いて前記クライアント装置とP2P型通信プロトコルによる通信を行い、当該通信において、前記クライアント装置と第1のサーバとの間で前記第1のファイアウォールを介してHTTPプロトコルによる通信によって取得した暗号鍵を用いて、データを暗号化して前記第1のファイアウォールを介さずに前記クライアント装置に送信する。

10

【0006】

第2の観点の通信方法は、ファイアウォールと、前記ファイアウォールおよびネットワークを介してクライアント装置と接続する第1のサーバと、前記ファイアウォールを介さずに、前記ネットワークを介して前記クライアント装置と接続する第2のサーバとを有するサーバシステムがネットワークを介して前記クライアント装置と通信する通信方法であって、前記第1のサーバが、前記ネットワーク上のグローバルIPアドレスが割り当てられていない前記第2のサーバに対して、前記サーバシステム内の通信回線を介してSTUN機能により、前記グローバルIPアドレスを割り当て、前記第1のサーバが、前記ファイアウォールを介して前記クライアント装置との間でHTTPプロトコルによる通信を行い、前記第2のサーバに割り当てた前記グローバルIPアドレスを前記クライアント装置に送信し、前記クライアント装置が、前記ファイアウォールを介してHTTPプロトコルによる通信を前記第1のサーバとの間で行って暗号鍵を取得あるいは特定し、前記第2のサーバが、前記割り当てられた前記グローバルIPアドレスを用いて前記クライアント装置とP2P型通信プロトコルによる通信を行い、当該通信において、前記クライアント装置が前記取得あるいは特定した暗号鍵を用いて、データを暗号化して前記ファイアウォールを介さずに前記クライアント装置に送信する。

20

【0007】

第3の観点の発明のコンピュータは、第1のサーバとのサーバ側のファイアウォールを介した通信に用いられるデータと、第2のサーバとの前記ファイアウォールを介さない通信に用いられるデータとを送受信するインタフェースと、処理回路とを有し、前記処理回路は、ネットワーク上のグローバルIPアドレスが割り当てられていない前記第2のサーバに対して前記第1のサーバが割り当てた前記グローバルIPアドレスを、前記ファイアウォールおよび前記ネットワークを介して、前記第1のサーバとの間でHTTPプロトコルによる通信を行って取得し、前記ファイアウォールを介してHTTPプロトコルによる通信を前記第1のサーバとの間で行って暗号鍵を取得あるいは特定し、前記割り当てられた前記グローバルIPアドレスを用いて前記第2のサーバとP2P型通信プロトコルによる通信を行い、当該通信において受信した前記暗号鍵で暗号化されたデータを復号する。

30

【0008】

第4の観点の発明のプログラムは、第1のサーバとのサーバ側のファイアウォールを介した通信と、第2のサーバとの前記ファイアウォールを介さない通信とを行うコンピュータが実行するプログラムであって、ネットワーク上のグローバルIPアドレスが割り当てられていない前記第2のサーバに対して前記第1のサーバが割り当てた前記グローバルIPアドレスを、前記ファイアウォールおよび前記ネットワークを介して、前記第1のサーバとの間でHTTPプロトコルによる通信を行って取得する第1の手順と、前記ファイアウォールを介してHTTPプロトコルによる通信を前記第1のサーバとの間で行って暗号鍵を取得あるいは特定する第2の手順と、前記割り当てた前記グローバルIPアドレスを用いて前記第2のサーバとP2P型通信プロトコルによる通信を行い、当該通信において受信した前記暗号鍵で暗号化されたデータを復号する第3の手順とを前記コンピュータに

40

50

実行させる。

【 0 0 0 9 】

第 5 の観点の発明の記録媒体は、第 1 のサーバとのサーバ側のファイアウォールを介した通信と、第 2 のサーバとの前記ファイアウォールを介さない通信とを行うコンピュータが実行するプログラムを記録する記録媒体であって、ネットワーク上のグローバル IP アドレスが割り当てられていない前記第 2 のサーバに対して前記第 1 のサーバが割り当てた前記グローバル IP アドレスを、前記ファイアウォールおよび前記ネットワークを介して、前記第 1 のサーバとの間で HTTP プロトコルによる通信を行って取得する第 1 の手順と、前記ファイアウォールを介して HTTP プロトコルによる通信を前記第 1 のサーバとの間で行って暗号鍵を取得あるいは特定する第 2 の手順と、前記割り当てた前記グローバル IP アドレスを用いて前記第 2 のサーバと P 2 P 型通信プロトコルによる通信を行い、当該通信において受信した前記暗号鍵で暗号化されたデータを復号する第 3 の手順とを前記プログラムは前記コンピュータに実行させる。

10

【 発明の効果 】

【 0 0 1 0 】

本発明によれば、高い安全性と応答性とを兼ね備えたサーバシステム、通信方法、コンピュータ、プログラムおよび記録媒体を提供することにある。

【 発明を実施するための最良の形態 】

【 0 0 1 1 】

以下、本発明の実施形態に係わるネットワークシステム 1 について説明する。

図 1 は、本実施形態に係わるネットワークシステム 1 の全体構成図である。

図 1 に示すように、ネットワークシステム 1 は、例えば、クライアント装置 1 1 - n、サーバセンタ 2 1 を有する。ここで、n は「1 n N」の整数である。

本実施形態において、フロントエンドサーバ機能部 3 3 が本発明に用いられる第 1 のサーバの一例であり、演算機能部 4 3 が本発明に用いられる第 2 のサーバの一例である。

【 0 0 1 2 】

クライアント装置 1 1 - n は、例えば、演算機能および NAT 機能を有する。

【 0 0 1 3 】

サーバセンタ 2 1 は、例えば、ファイアウォール機能部 3 1、フロントエンドサーバ機能部 3 3、ファイアウォール機能部 3 5、バックエンドサーバ機能部 3 7、ファイアウォール機能部 3 9、NAT (Network Address Translation) 機能部 4 1、メディアータ 4 2 および演算機能部 4 3 を有する。

20

30

【 0 0 1 4 】

ファイアウォール機能部 3 1 は、ネットワーク 9 を介したクライアント装置 1 1 - n との間の通信においてファイアウォール機能を発揮する。

本実施形態において、ファイアウォール機能とは、ファイアウォールを通過する全ての通信に、予め規定したポリシー（ルール）を適用（強制）する機能を示す。

ファイアウォール機能には、例えば、アクセス制限、アドレス変換、ユーザ認証、ログ収集 / 解析、コンテンツフィルタリングおよびルーティング等の機能がある。

ファイアウォール機能は、OS (Operation System) およびアプリケーションの少なくとも一方で実現される。

40

【 0 0 1 5 】

フロントエンドサーバ機能部 3 3 は、STUN (Simple Traversal of UDP Through NAT s) サーバ機能を発揮する。

すなわち、フロントエンドサーバ機能部 3 3 は、ネットワーク 9 内でユニークなアドレス（グローバル IP アドレス）を持つ。

フロントエンドサーバ機能部 3 3 は、STUN 機能により、グローバル IP アドレスが割り当てられていない演算機能部 4 3 とサーバセンタ 2 1 内の通信回線を介して通信を行うことで、演算機能部 4 3 に対してグローバル IP アドレスを割り当てる。グローバル I

50

Pアドレスは、例えば、128ビットデータである。

フロントエンドサーバ機能部33は、演算機能部43に割り当てた上記グローバルIPアドレスを接続情報として、クライアント装置11-nに送信する。

演算機能部43に割り当てた上記グローバルIPアドレスは、クライアント装置11-nと演算機能部43の通信時にNAT機能部41によるNAT機能によって、通信対象の演算機能部43を特定する内部アドレスとの間で相互に変換される。

なお、フロントエンドサーバ機能部33と演算機能部43との間のSTUN機能に基づく通信は、サーバシステム21内のパスを介して行われる。

また、好適には、クライアント装置11-nに対しても、NAT機能部41によるNAT機能を用いてグローバルIPアドレスが適宜割り当てられ、通信に用いられる。

本実施形態において、クライアント装置11-nとフロントエンドサーバ機能部33との間の通信には、HTTP(HyperText Transfer Protocol)等のプロトコルが用いられる。

本実施形態において、クライアント装置11-nとフロントエンドサーバ機能部33との間の通信は、クレジット決済等の高いセキュリティが要求される処理に用いられる。

【0016】

ファイアウォール機能部35は、フロントエンドサーバ機能部33とバックエンドサーバ機能部37との間の通信においてファイアウォール機能を発揮する。

バックエンドサーバ機能部37は、SQL等を基にしたデータベースアクセス処理、NFS等のファイルシステム共有関連処理等のプログラムを実行する。

バックエンドサーバ機能部37は、上記プログラムに基づいて、例えば、コンテンツデータや所定のコンテンツ空間データ等を演算機能部43に送信する。

ファイアウォール機能部39は、バックエンドサーバ機能部37と演算機能部43との間の通信においてファイアウォール機能を発揮する。

【0017】

メディアータ42は、クライアント装置11-nにアプリケーション情報を提供する。

【0018】

演算機能部43は、複数の演算機能モジュール45-1~45-mを有し、それぞれがアプリケーションプログラムAP-Sを実行する。

演算機能部43は、アプリケーションプログラムAP-Sに基づいて、楽曲等のオーディオデータ、アルバムジャケット画像等イメージデータ等のコンテンツデータをクライアント装置11-nに送信する。

また、演算機能部43は、例えば、所定の空間内での各コンテンツの座標や、書誌事項を示すテキストデータ等をクライアント装置11-nに送信する。

このとき、演算機能部43からクライアント装置11-nへの送信は、送信データを暗号化して行われる。クライアント装置11-nは、例えば、ファイアウォール機能部31との間の通信によって暗号鍵を取得し、その暗号鍵を用いて、演算機能部43との間の通信を行う。

本実施形態において、クライアント装置11-nと演算機能部43との間の通信には、クライアント装置11-nとファイアウォール機能部31との通信とは異なるP2P型の通信プロトコルが用いられる。すなわち、演算機能部43に割り当てた上記グローバルIPアドレスを用いて、クライアント装置11-nとの間で直接の通信が行われる。

この直接のP2P通信は、複数のクライアント装置11-nあるいは複数の演算機能部43に対しても可能である。その場合、相互のアドレス参照は、例えば、相互に全ての参照を保持するFCG(Fully Connected Graph)方式を用いる。参照をハッシュテーブルに管理しそれを当該ノードに分散させるDHT(Distributed Hash Table)によるChord方式など、他の方法でももちろん構わない。

演算機能部43は、ファイアウォール機能部39を介して、バックエンドサーバ機能部37が提供するデータベースアクセス処理およびファイルシステム共有関連処理により、コンテンツデータ等を受信する。

10

20

30

40

50

【 0 0 1 9 】

[クライアント装置 1 1 - n]

クライアント装置 1 1 - n は、ゲーム機、パーソナルコンピュータあるいは携帯電話機等の電子機器である。

図 2 は、図 1 に示すクライアント装置 1 1 - n の機能ブロック図である。

図 2 に示すように、クライアント装置 1 1 - n は、例えば、インタフェース 6 1、ディスプレイ 6 2、操作部 6 3、メモリ 6 4 および処理回路 6 5 を有する。

【 0 0 2 0 】

インタフェース 6 1 は、ネットワーク 9 を介したデータの送受信のためのインタフェースである。

ディスプレイ 6 2 は、処理回路 6 5 が生成した画面情報に応じた画像を表示する。

操作部 6 3 は、キーボードやコントローラなどの操作手段であり、ユーザの操作に応じた操作信号を処理回路 6 5 に出力する。

メモリ 6 4 は、処理回路 6 5 が実行するクライアントアプリケーションプログラム P R G - T を記憶する。メモリ 6 4 は、半導体メモリの他、光メモリ、光磁気メモリ等のその他の記録媒体でもよい。

処理回路 6 5 は、クライアントアプリケーションプログラム P R G - T を実行して本実施形態で説明するクライアント装置 1 1 - n の処理を統括的に制御する。

【 0 0 2 1 】

[フロントエンドサーバ機能部 3 3]

図 3 は、図 1 に示すフロントエンドサーバ機能部 3 3 の機能ブロック図である。

図 3 に示すように、フロントエンドサーバ機能部 3 3 は、例えば、インタフェース 7 1、メモリ 7 4 および処理回路 7 5 を有する。

【 0 0 2 2 】

インタフェース 7 1 は、ネットワーク 9 を介したデータの送受信のためのインタフェースである。

メモリ 7 4 は、処理回路 7 5 が実行するサーバアプリケーションプログラム P R G - S F を記憶する。メモリ 7 4 は、半導体メモリの他、光メモリ、光磁気メモリ等のその他の記録媒体でもよい。

処理回路 7 5 は、サーバアプリケーションプログラム P R G - S F を実行して本実施形態で説明するフロントエンドサーバ機能部 3 3 の処理を統括的に制御する。

処理回路 7 5 は、サーバアプリケーションプログラム P R G - S F を実行してフロントエンドサーバ機能部 3 3 の動作を統括的に制御する。

【 0 0 2 3 】

[演算機能部 4 3]

図 4 は、図 1 に示す演算機能部 4 3 に複数存在する演算機能モジュール 4 5 - 1 ~ 4 5 - m のそれぞれの機能ブロック図である。

図 4 に示すように、演算機能モジュール 4 5 - 1 ~ 4 5 - m は、例えば、インタフェース 8 1、メモリ 8 4 および処理回路 8 5 を有する。

演算機能モジュール 4 5 - 1 ~ 4 5 - m の処理回路 8 5 は、少なくとも一つの管理プロセッサと、複数の計算実行プロセッサとで構成される。上記複数の計算実行プロセッサの処理は、例えば、上記管理プロセッサによって管理される。

ここで、クライアント装置 1 1 - n とフロントエンドサーバ機能部 3 3 との間の通信プロトコルとしては、例えば、H T T P 等のサーバ主導型のものが用いられる。これに対して、クライアント装置 1 1 - n と演算機能部 4 3 との間の通信プロトコルとしては、前述のように、P 2 P 型の通信プロトコル等が用いられる。

【 0 0 2 4 】

演算機能部 4 3 が例えば複数のクライアント装置 1 1 - n のクライアントアプリケーションプログラム P R G - T と通信しながら処理を行う場合に、上記複数の計算実行プロセッサの各々に、上記複数のクライアントアプリケーションプログラム P R G - T のうち対

10

20

30

40

50

応するクライアントアプリケーションプログラム P R G - T と通信を行うサーバアプリケーションプログラム P R G - S A を実行させる。

処理回路 8 5 は、例えば、クライアント装置 1 1 - n にコンテンツデータ等を送信する場合に、当該コンテンツデータを所定の暗号化鍵で暗号化する。

処理回路 8 5 は、当該暗号化鍵として、例えば、クライアント装置 1 1 - n とフロントエンドサーバ機能部 3 3 との間の通信によって特定された暗号鍵を用いる。このようにコンテンツデータを暗号化することで、クライアント装置 1 1 - n と演算機能部 4 3 との間の通信が傍受された場合でも、コンテンツデータを保護できる。

【 0 0 2 5 】

インタフェース 8 1 は、ネットワーク 9 を介したデータの送受信のためのインタフェースである。

メモリ 8 4 は、処理回路 8 5 が実行するサーバアプリケーションプログラム P R G - S A を記憶する。メモリ 8 4 は、半導体メモリの他、光メモリ、光磁気メモリ等のその他の記録媒体でもよい。

処理回路 8 5 は、サーバアプリケーションプログラム P R G - S A を実行して本実施形態で説明する演算機能部 4 3 の動作を統括的に制御する。

【 0 0 2 6 】

[クライアント・サーバの接続動作]

図 5 は、クライアント・サーバの接続動作を説明するためのフローチャートである。

以下、図 5 に示す各ステップについて説明する。

ステップ S T 1 1 :

クライアント装置 1 1 - n の処理回路 6 5 は、例えば、ポータルサイトから、ネットワーク 9 およびファイアウォール機能部 3 1 を介して、フロントエンドサーバ機能部 3 3 と通信を行い、フロントエンドサーバ機能部 3 3 の S T U N サーバ機能により、メディアータ 4 2 との接続情報を取得する。

当該接続情報は、例えば、メディアータ 4 2 に割り当てられたグローバル I P アドレスやポート等の情報である。

上記通信は、H T T P 等の通信プロトコルを基に、ファイアウォール機能部 3 1 を介してセキュアな状態で行われる。

【 0 0 2 7 】

ステップ S T 1 2 :

クライアント装置 1 1 - n の処理回路 6 5 は、ステップ S T 1 1 で取得した接続情報を基に、N A T 機能部 4 1 を介して、メディアータ 4 2 にアクセスを行い、メディアータ 4 2 からアプリケーション情報を受信する。

なお、メディアータ 4 2 は、演算機能部 4 3 が実行するサーバアプリケーションプログラムに対応したアプリケーション情報をクライアント装置 1 1 - n に送信する。当該アプリケーション情報は、クライアント装置 1 1 - n が利用可能なアプリケーションの内容の紹介等である。

ステップ S T 1 3 :

クライアント装置 1 1 - n の処理回路 6 5 は、ステップ S T 1 2 で取得したアプリケーション情報を基に、所定のサイトからクライアントアプリケーションプログラム P R G - T をダウンロードする。

なお、クライアント装置 1 1 - n は、フロントエンドサーバ機能部 3 3 あるいはメディアータ 4 2 からクライアントアプリケーションプログラム P R G - T をダウンロードしてもよい。

【 0 0 2 8 】

ステップ S T 1 4 :

クライアント装置 1 1 - n の処理回路 6 5 は、ステップ S T 1 3 でダウンロードしたクライアントアプリケーションプログラム P R G - T を実行する。

クライアント装置 11 - n の処理回路 65 は、上記実行するクライアントアプリケーションプログラム P R G - T に基づいて、ネットワーク 9 およびファイアウォール機能部 31 を介して、フロントエンドサーバ機能部 33 にアクセスを行う。

そして、クライアント装置 11 - n の処理回路 65 は、フロントエンドサーバ機能部 33 の S T U N サーバ機能により、演算機能部 43 のグローバル I P アドレスおよびポート情報を取得して、演算機能部 43 との間の接続を確立する。

なお、演算機能部 43 は、複数の演算機能モジュール 45 - 1 ~ 45 - m を有し、各演算機能モジュール 45 - 1 ~ 45 - m がサーバアプリケーションプログラムを個別に実行する。このとき、上記 S T U N 機能により、各演算機能モジュール 45 - 1 ~ 45 - m に固有の I P アドレスおよびポートの組み合わせを割り当て、演算機能モジュール 45 - 1 ~ 45 - m が自らが実行するアプリケーションプログラムに対応する、I P アドレスおよびポートの組み合わせ情報を基に、クライアント装置 11 - n との通信を行う。

なお、クライアント装置 11 - n およびそれと通信を行う演算機能部 43 は、当該ステップ S T 14 の通信により、クライアント装置 11 - n と演算機能部 43 との間の通信に用いる暗号鍵を取得あるいは特定する。

【 0 0 2 9 】

ステップ S T 15 :

クライアント装置 11 - n の処理回路 65 は、ステップ S T 14 で確立した接続を基に、演算機能部 43 と通信を行う。当該通信では、前述のように、H T T P 以外の P 2 P 型の通信プロトコルが用いられる。

このとき、演算機能部 43 は、クライアント装置 11 - n に対応したサーバアプリケーションプログラム P R G - S A を実行する。当該サーバアプリケーションプログラム P R G - S A は、例えば、フロントエンドサーバ機能部 33 によって起動される。当該起動されるタイミングは、クライアント装置 11 - n がクライアントアプリケーションプログラム P R G - T をダウンロードしたタイミング、あるいは起動したタイミングである。

クライアント装置 11 - n は、当該通信により、演算機能部 43 から暗号化されたコンテンツデータをダウンロードし、キャッシュメモリに書き込む。

クライアント装置 11 - n は、ダウンロード時あるいは使用時に、フロントエンドサーバ機能部 33 との間の通信で取得した暗号鍵を用いて、コンテンツデータを復号する。

【 0 0 3 0 】

[オート (自動) クルーズ動作例]

以下、上述したコンテンツデータのダウンロードが採用されるオートクルーズ動作例について説明する。

オートクルーズ動作とは、例えば、所定の空間内にコンテンツデータの属性を基に当該コンテンツデータの座標を規定し、当該空間内でユーザ座標 (後述するカメラ位置) を自動移動させ、ユーザ座標に対応したコンテンツデータを再生等する動作である。当該オートクルーズ動作においては、空間内でのユーザ座標の移動に伴い、その座標に対応したコンテンツデータをダウンロードするものである。なお、空間内におけるユーザ座標の移動は、オートクルーズ (自動) および手動を切り換えてもよいし、何れか一方のみでもよい。

図 6 は、図 1 に示すネットワークシステム 1 において、オートクルーズ動作をする場合の機能ブロック図である。

図 6 に示すように、クライアント装置 11 - n は、例えば、クルーズ管理部 101、キャッシュ管理部 103、ローカルキャッシュ 105、自動クルーズ処理部 107、ビューア 109、オーディオ管理部 111 およびレンダリング部 113 を機能として有する。

図 6 に示すクライアント装置 11 - n の上記機能は、図 2 に示す処理回路 65 がクライアントアプリケーションプログラム P R G - T を実行して実現される。

また、サーバセンタ 21 内の演算機能部 43 は、例えば、空間サーバ機能 121、空間データベース 122 およびコンテンツデータベース 123 を機能として有する。

図 6 に示す演算機能部 43 の上記機能は、図 4 に示す処理回路 85 がサーバアプリケー

10

20

30

40

50

ションプログラム P R G - S A を実行して実現される。

【 0 0 3 1 】

図 7 は、上記オートクルーズ動作を説明するためのフローチャートである。

ステップ S T 2 1 :

クライアント装置 1 1 - n の処理回路 6 5 は、例えば、図 5 を用いて前述した処理により、サーバセンタ 2 1 内の演算機能部 4 3 との間に接続が確立したか否かを判断し、確立したと判断した場合にはステップ S T 2 2 に進む。

【 0 0 3 2 】

ステップ S T 2 2 :

クライアント装置 1 1 - n の処理回路 6 5 は、図 5 に示すステップ S T 1 3 でダウンロードしたクライアントアプリケーションプログラム P R G - T を起動する。

処理回路 6 5 によるクライアントアプリケーションプログラム P R G - T の起動は、例えば、フロントエンドサーバ機能部 3 3 からの命令によって行われてもよい。

これにより、図 6 に示すクライアント装置 1 1 - n 内の各機能ブロックが起動される。

ステップ S T 2 3 :

図 6 に示すクルーズ管理部 1 0 1 が、空間サーバ 1 2 1 から空間データおよびコンテンツデータを受信する。空間サーバ 1 2 1 は、空間データベース 1 2 2 から空間データを取得し、コンテンツデータベース 1 2 3 からコンテンツデータを取得する。

具体的には、図 4 に示す演算機能部 4 3 の処理回路 8 5 が、サーバアプリケーションプログラム P R G - S A に基づいて、バックエンドサーバ機能部 3 7 からファイアウォール機能部 3 9 を介して、空間データおよびコンテンツデータを受信し、これを暗号化する。

そして、処理回路 8 5 は、上記暗号化したコンテンツデータを、図 5 のステップ S T 1 4 で確立した接続を基に、クライアント装置 1 1 - n に送信する。

クライアント装置 1 1 - n のクルーズ管理部 1 0 1 は、受信した空間データおよびコンテンツデータを、キャッシュ管理部 1 0 3 の機能を基にローカルキャッシュ 1 0 5 に書き込む。

【 0 0 3 3 】

ステップ S T 2 4 :

クライアント装置 1 1 - n のビューア 1 0 9 が、ローカルキャッシュ 1 0 5 から空間データおよびコンテンツデータを読み出して、それに応じたビュー（画面）をディスプレイ 6 2 に表示する。

ステップ S T 2 5 :

クライアント装置 1 1 - n のクルーズ管理部 1 0 1 は、次に使用する空間データおよびコンテンツデータを、空間サーバ機能 1 2 1 から取得し、これをローカルキャッシュ 1 0 5 に書き込む。

【 0 0 3 4 】

ステップ S T 2 6 :

クライアント装置 1 1 - n のクルーズ管理部 1 0 1 は、図 2 に示す操作部 6 3 から一定期間、操作信号を発生していない（ユーザによる操作が一定期間行われていない）と判断するとステップ S T 2 7 に進み、そうでない場合はステップ S T 2 8 に進む。

ステップ S T 2 7 :

クルーズ管理部 1 0 1 は、自動クルーズ処理部 1 0 7 による制御に切り換える。

【 0 0 3 5 】

ステップ S T 2 8 :

クライアント装置 1 1 - n のビューア 1 0 9 は、自動クルーズ処理部 1 0 7 によって決定されたカメラ位置（ビューとして表示するコンテンツ空間内の対象）に対応したコンテンツデータをローカルキャッシュ 1 0 5 から読み出してレンダリング部 1 1 3 でイメージ再生する。

オーディオ管理部 1 1 1 は、上記カメラ位置に対応したコンテンツデータのオーディオデータの再生を行う。

10

20

30

40

50

【 0 0 3 6 】

ステップ S T 2 9 :

クライアント装置 1 1 - n のクルーズ管理部 1 0 1 は、移動したカメラ位置に応じて、次に使用する空間データおよびコンテンツデータを、空間サーバ機能 1 2 1 から取得し、これをローカルキャッシュ 1 0 5 に書き込む。

その後、クルーズ管理部 1 0 1 は、ステップ S T 2 4 の処理に戻る。

【 0 0 3 7 】

[クライアント追加時の動作例]

図 8 は、図 1 に示すネットワークシステム 1 に新たなクライアント装置 1 1 - n が追加された場合の動作例を説明するためのフローチャートである。

10

ステップ S T 3 1 :

フロントエンドサーバ機能部 3 3 の処理回路 7 5 は、クライアント装置 1 1 - n からの要求により、新たなクライアント装置 1 1 - n が追加されたと判断すると、ステップ S T 3 2 に進む。

【 0 0 3 8 】

ステップ S T 3 2 :

フロントエンドサーバ機能部 3 3 の処理回路 7 5 は、追加されたクライアント装置 1 1 - n が実行するクライアントアプリケーションプログラム P R G - C に対応したサーバアプリケーションプログラム P R G - S F を特定する。

そして、処理回路 7 5 は、上記特定したサーバアプリケーションプログラム P R G - S F を演算機能部 4 3 に起動させる。

20

【 0 0 3 9 】

ステップ S T 3 3 :

演算機能部 4 3 は、ステップ S T 3 2 で起動したサーバアプリケーションプログラム P R G - S F を基に、クライアント装置 1 1 - n と通信を行う。

【 0 0 4 0 】

[通信の切り換え動作例]

クライアント装置 1 1 - n と演算機能部 4 3 とが P 2 P で通信中に例えば決済等の処理が発生すると、通信がファイアウォール 3 1 を介したクライアント装置 1 1 - n とフロントエンドサーバ機能部 3 3 との間の通信に切り換わる。

30

そして、クライアント装置 1 1 - n とフロントエンドサーバ機能部 3 3 との間のセキュアな通信により決済が終了すると、再びクライアント装置 1 1 - n と演算機能部 4 3 との間の P 2 P 通信に切り替わり、決済済みの暗号化されたコンテンツデータを演算機能部 4 3 からクライアント装置 1 1 - n にダウンロードする。

【 0 0 4 1 】

以上説明したように、ネットワークシステム 1 によれば、クライアント装置 1 1 - n はファイアウォールを介さずに演算機能部 4 3 から暗号化されたコンテンツデータをダウンロードするため、応答性がよい。

また、ネットワークシステム 1 によれば、クライアント装置 1 1 - n と演算機能部 4 3 との間の通信の確立を、ファイアウォール機能部 3 1 を介したクライアント装置 1 1 - n と演算機能部 4 3 との間の通信によって得た通信情報を基に行うため、手続きの安全性を高めることができる。

40

また、ネットワークシステム 1 によれば、クライアント装置 1 1 - n が実行するクライアントアプリケーションプログラム P R G - T に対応したサーバアプリケーションプログラム P R G - S A を演算機能部 4 3 が実行するため、アプリケーション構成の柔軟性が高まる。

【 0 0 4 2 】

また、ネットワークシステム 1 によれば、フロントエンドサーバ機能部 3 3 と演算機能部 4 3 とを個別に機能させることで、複数のクライアント装置 1 1 - n とサーバを含めたネットワークとしてのアプリケーションの構築が容易になる。すなわち、独立のノードとそ

50

の機能があってそれらが接続されるというのではなく、クライアント装置 1 1 - n 上の機能とサーバ上の機能を含めたアプリケーションが組み易い。

【 0 0 4 3 】

なお、ネットワークシステム 1 は、ネットワーク OS あるいはネットワークミドルウェアとして機能するサーバ装置としてサーバセンタ 2 1 を実現できる。

サーバセンタ 2 1 は、内部プロセッサ間のネットワーク接続と、従来型サーバネットワーク接続を組み合わせて、内部プロセッサネットワークを効果的に実現したものである。

【 0 0 4 4 】

本発明は上述した実施形態には限定されない。

すなわち、当業者は、本発明の技術的範囲またはその均等の範囲内において、上述した実施形態の構成要素に関し、様々な変更、コンビネーション、サブコンビネーション、並びに代替を行ってもよい。

例えば、上述した実施形態では、ファイアウォール機能部 3 1 が STUN 機能により演算機能部 4 3 にグローバル IP アドレスを割り当てる場合を例示したが、STUN 機能以外の機能により割り当てを行ってもよい。

上述した実施形態では、演算機能部 4 3 がバックエンドサーバ機能部 3 7 からファイアウォール機能部 3 9 を介してコンテンツデータを受信する場合を例示したが、ファイアウォール機能部 3 9 は設けなくてもよいし、あるいはサーバセンタ 2 1 以外のサーバからコンテンツデータをダウンロードしてもよい。

【 0 0 4 5 】

また、図 1 に示すサーバセンタ 2 1 の各機能は、機能モジュールとしてそれぞれが存在すれば、それらの機能が同一あるいは異なるハードウェアの何れで実現されているかは問わない。例えば、図 9 に示すように、図 3 に示すフロントエンドサーバ機能部 3 3 および図 4 に示す演算機能部 4 3 の双方の機能を実現するサーバ機能部 2 0 0 を設けてもよい。この場合には、サーバ機能部 2 0 0 のメモリ 2 7 4 に前述したプログラム PRG - SF, PRG - SA を記憶し、これらのプログラムを処理回路 2 7 5 が実行することで、インタフェース 2 7 1 を介してクライアント装置 1 1 - 1 と通信を行い、前述したフロントエンドサーバ機能部 3 3 および演算機能部 4 3 の双方の機能を発揮する。

【産業上の利用可能性】

【 0 0 4 6 】

本発明は、ファイアウォールを介した通信を行う通信システムに適用可能である。

【図面の簡単な説明】

【 0 0 4 7 】

【図 1】図 1 は、本実施形態に係わるネットワークシステムの全体構成図である。

【図 2】図 2 は、図 1 に示すクライアント装置の機能ブロック図である。

【図 3】図 3 は、図 1 に示すフロントエンドサーバ機能部の機能ブロック図である。

【図 4】図 4 は、図 1 に示す演算機能部に複数存在する演算機能モジュールそれぞれの機能ブロック図である。

【図 5】図 5 は、図 1 に示すクライアント・サーバの接続動作を説明するためのフローチャートである。

【図 6】図 6 は、図 1 に示すネットワークシステムにおいて、オートクルーズ動作をする場合の機能ブロック図である。

【図 7】図 7 は、オートクルーズ動作を説明するためのフローチャートである。

【図 8】図 8 は、図 1 に示すネットワークシステムに新たなクライアント装置が追加された場合の動作例を説明するためのフローチャートである。

【図 9】図 9 は、図 1 に示すネットワークシステムのサーバ機能の変形例を説明するための図である。

【符号の説明】

【 0 0 4 8 】

1 1 - n ... クライアント装置、 2 1 ... サーバセンタ、 3 1 ... ファイアウォール機能部、

10

20

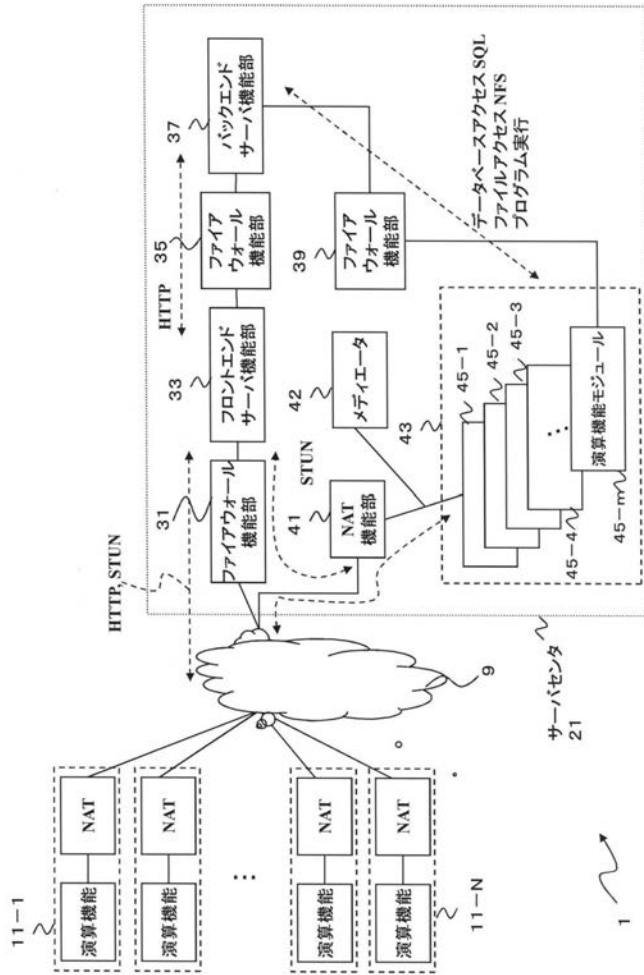
30

40

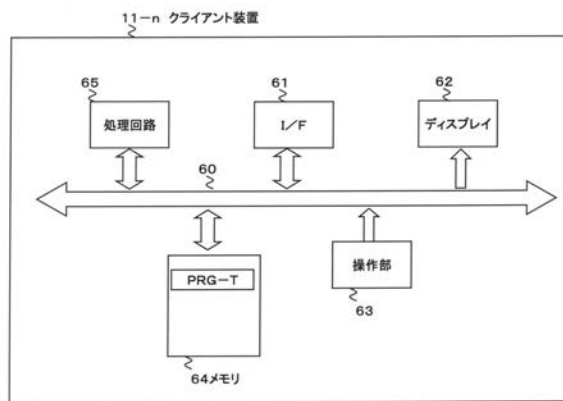
50

3 3 ... フロントエンドサーバ機能部、3 5 ... ファイアウォール機能部、3 7 ... バックエンドサーバ機能部、3 9 ... ファイアウォール機能部、4 1 ... NAT機能部、4 2 ... メディエータ、4 3 ... 演算機能部、4 5 - 1 ~ 4 5 - m ... 演算機能モジュール、6 1 ... インタフェース、6 2 ... ディスプレイ、6 3 ... 操作部、6 4 ... メモリ、6 5 ... 処理回路、7 1 ... インタフェース、7 4 ... メモリ、7 5 ... 処理回路、8 1 ... インタフェース、8 4 ... メモリ、8 5 ... 処理回路、1 0 1 ... クルーズ管理部、1 0 3 ... キャッシュ管理部、1 0 5 ... ローカルキャッシュ、1 0 7 ... 自動クルーズ処理部、1 0 9 ... ビューア、1 1 1 ... オーディオ管理部、1 1 3 ... レンダリング部

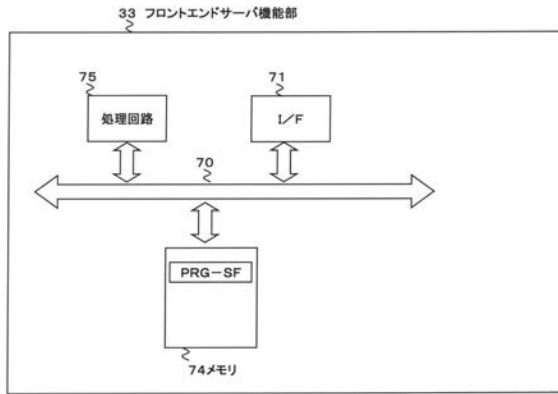
【 図 1 】



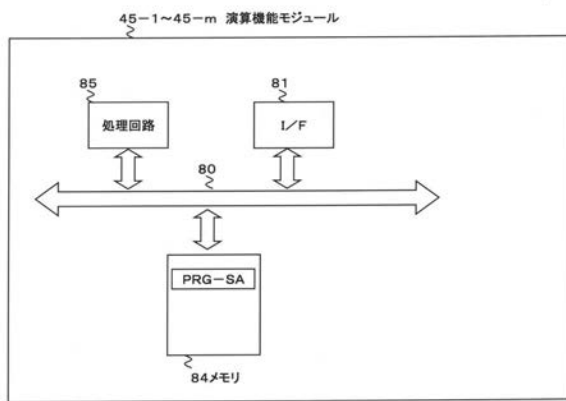
【 図 2 】



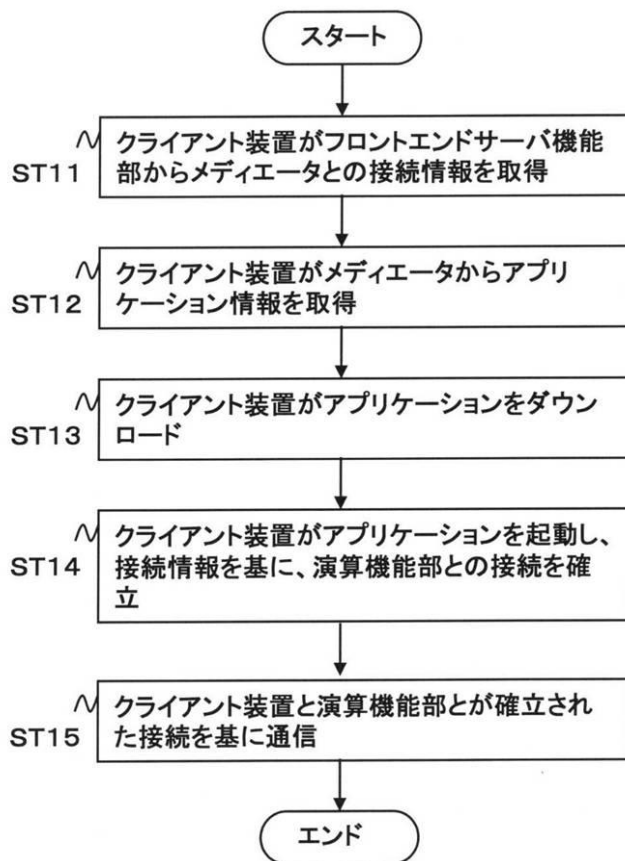
【図3】



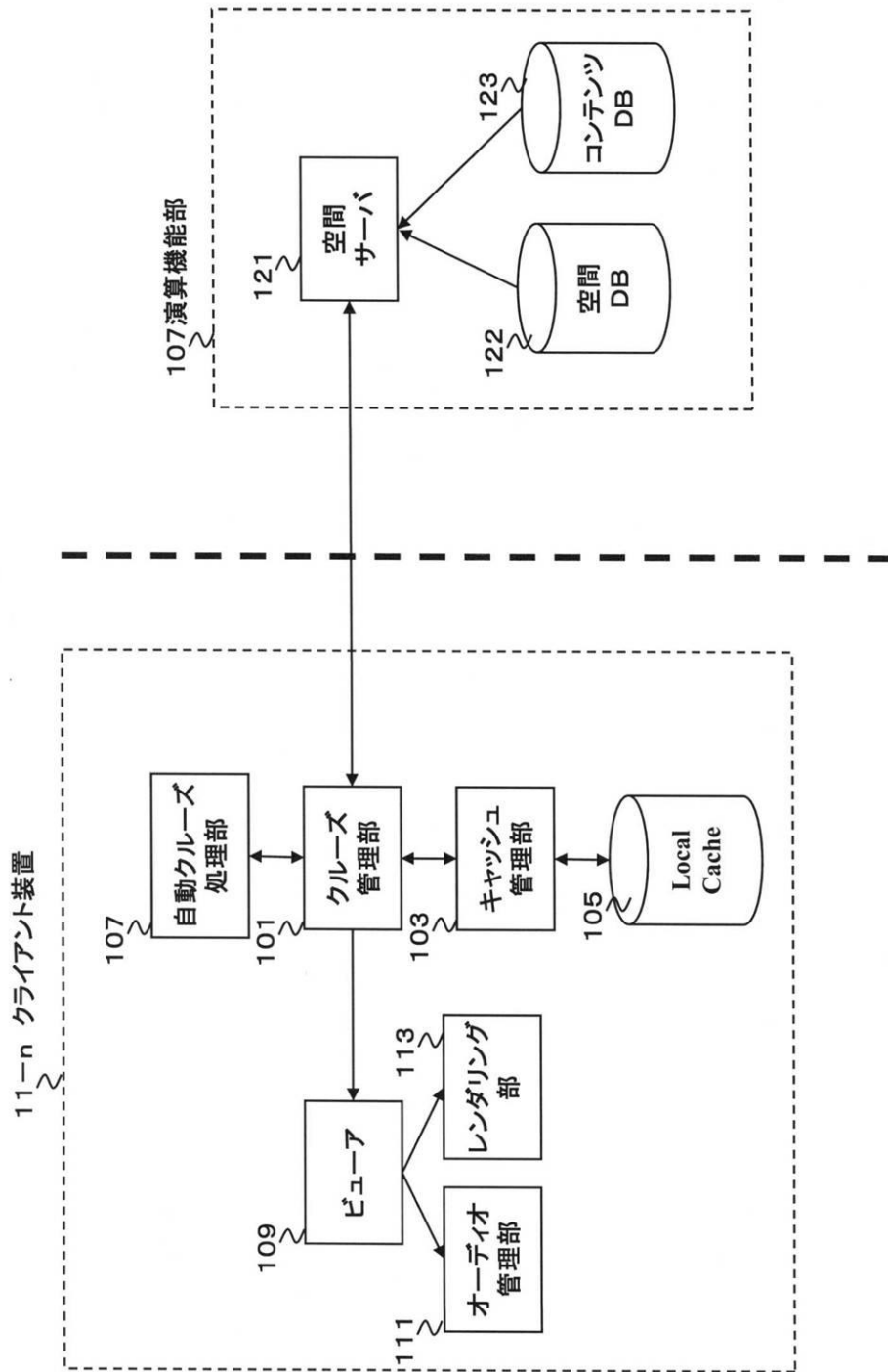
【図4】



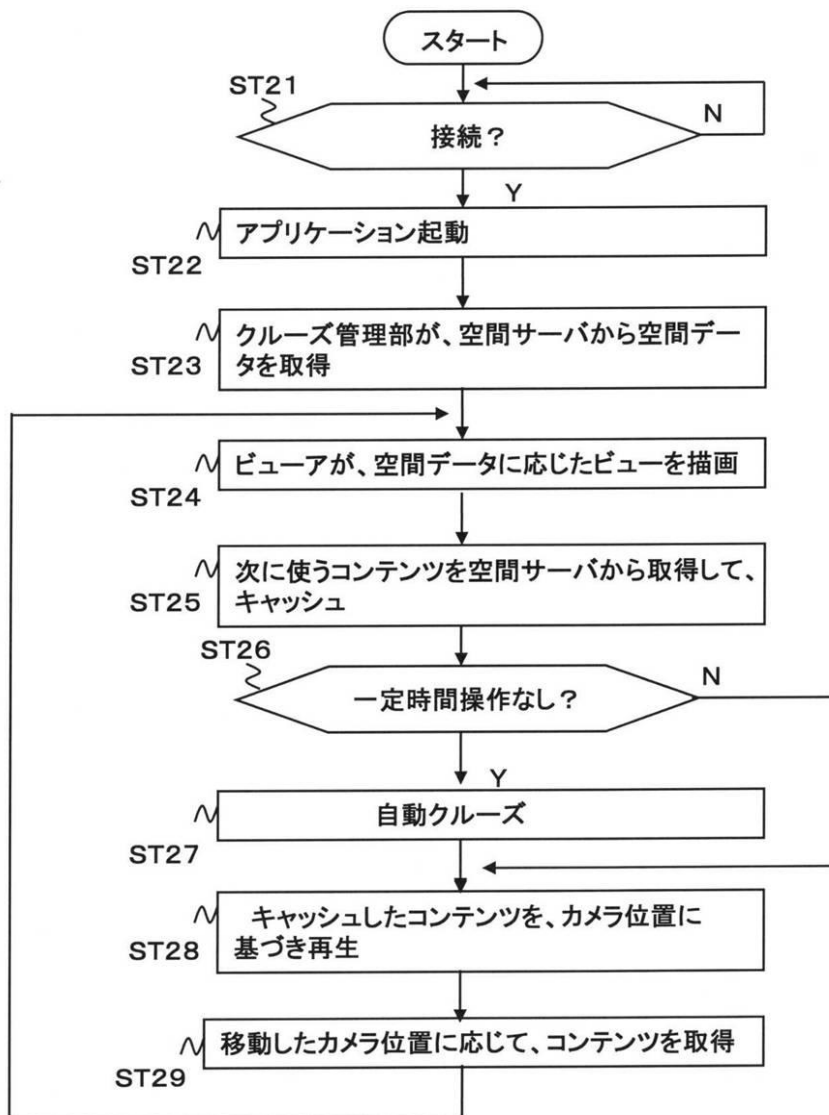
【図5】



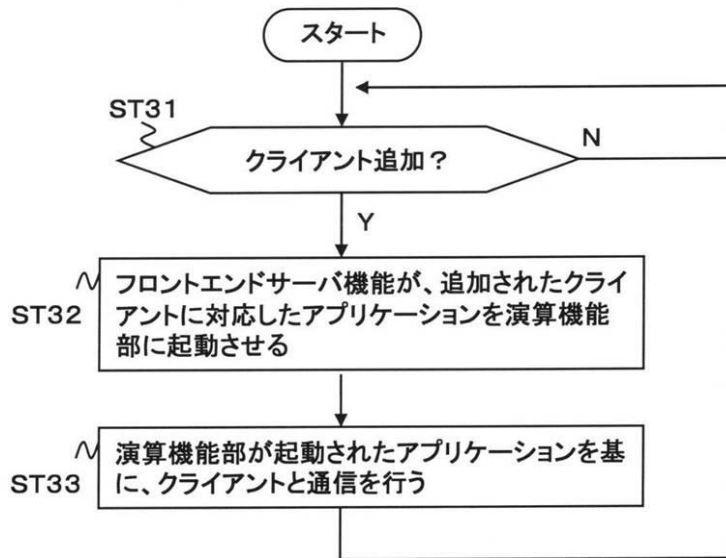
【図6】



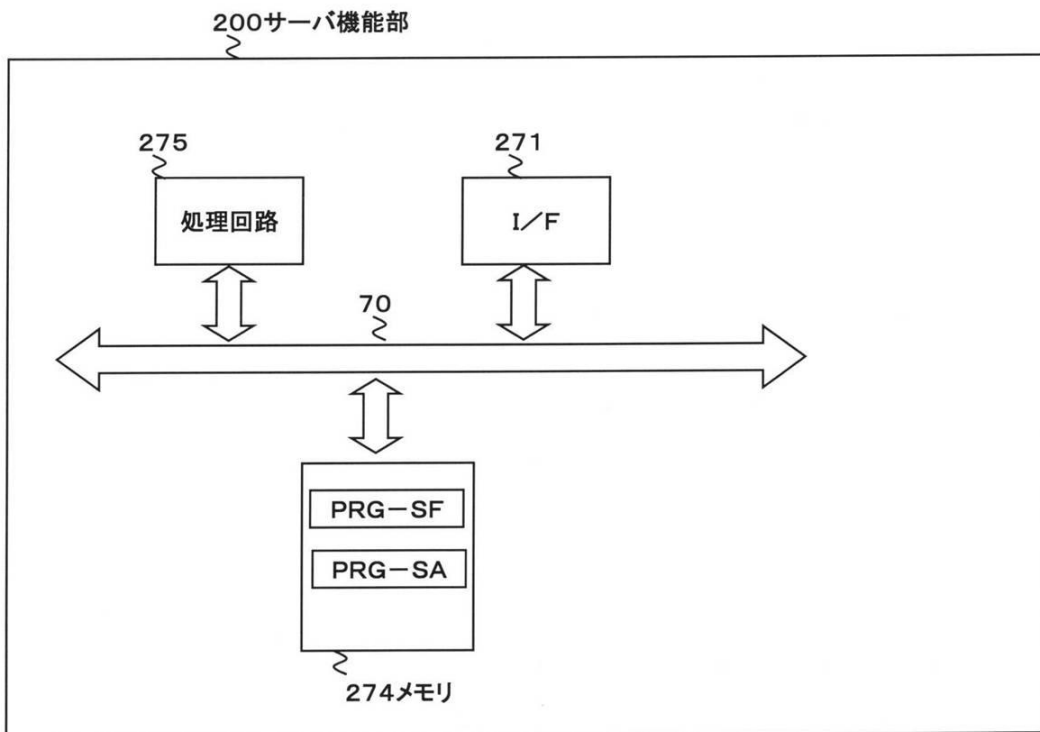
【図7】



【図8】



【図9】



フロントページの続き

(72)発明者 広井 順

東京都港区南青山二丁目6番21号 株式会社ソニー・コンピュータエンタテインメント内

審査官 古河 雅輝

(56)参考文献 特表2005-528004(JP,A)

特開2005-352639(JP,A)

特開平11-167535(JP,A)

特開2005-309821(JP,A)

特開2000-049867(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06F 12/14

G06F 13/00

G06F 21/02-21/06

G06F 21/24

H04L 12/00-12/26

H04L 12/50-12/66