

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2006 年 3 月 16 日 (16.03.2006)

PCT

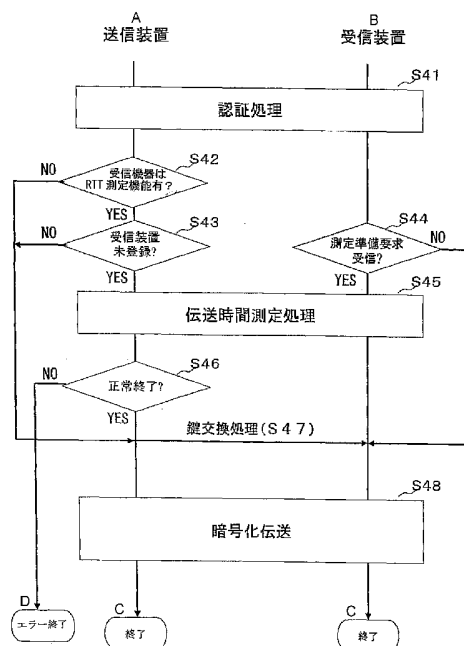
(10) 国際公開番号
WO 2006/028094 A1

- (51) 国際特許分類:
H04L 9/32 (2006.01) H04L 12/28 (2006.01)
G09C 1/00 (2006.01) H04L 12/56 (2006.01)
- (21) 国際出願番号: PCT/JP2005/016335
- (22) 国際出願日: 2005 年 9 月 6 日 (06.09.2005)
- (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:
特願2004-259213 2004 年 9 月 7 日 (07.09.2004) JP
- (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).
- (72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 綾木 靖 (AYAKI, Yasushi). 飯塚 裕之 (IITSUKA, Hiroyuki). 臼木 直司 (USUKI, Naoshi).
- (74) 代理人: 新居 広守 (NIJ, Hiromori); 〒5320011 大阪府大阪市淀川区西中島 3 丁目 1 番 2 6 号 新大阪末広センタービル 3 F 新居国際特許事務所内 Osaka (JP).

[続葉有]

(54) Title: COMMUNICATION APPARATUS

(54) 発明の名称: 通信装置



- A TRANSMITTING APPARATUS
B RECEIVING APPARATUS
S41 AUTHENTICATION PROCESS
S42 DOES RECEIVING DEVICE HAVE RTT MEASURING FUNCTION?
S43 IS RECEIVING APPARATUS UNREGISTERED?
S44 HAS MEASUREMENT PREPARATION REQUEST BEEN RECEIVED?
S45 TRANSMISSION TIME MEASUREMENT PROCESS
S46 NORMALLY TERMINATED?
S47 KEY EXCHANGE PROCESS
S48 ENCRYPTED TRANSMISSION
D ERRONEOUS END
C END

(57) Abstract: The conventional data transmitting/receiving system has problems that a verification process time cannot be precisely measured because it is added to a transmission time and then measured; there is a need to provide a separate authentication process required for a transmission time measurement process; and that an unnecessary key exchange process is executed. A transmitting apparatus (a) shares authentication information with a request source that requests a transmission of content data, (b) transmits to the request source a measurement request generated by using the authentication information, (c) receives, as a response to the measurement request, from the request source a measurement response generated by using the authentication information shared by the request source, (d) measures, as a round-trip delay time, a time from the transmission of the measurement request until the reception of the measurement response, (e) transmits, before the transmission of the measurement request, to the request source a measurement preparation request for requesting a preparation required for generating the measurement response, and (f) determines, after the measurement of the round-trip delay time, that the request source is an appropriate apparatus as a destination of transmitting the content data if the round-trip delay time is equal to or less than a reference value so that the correctness of the measurement response is verified and if the correctness of the measurement request is verified at the request source.

(57) 要約: 従来のデータ送受信システムでは、検証処理時間が伝送時間に加算されて測定され正確な測定が出来ない、伝送時間測定処理に必要な認証処理を別途設ける必要がある、不要な鍵交換処理を実行するという課題があった。送信装置は、(a) コンテンツデータの送信を要求する要求元との間で認証情報を共有し、(b) 認証情報を使用して生成した測定要求を、前記要求元に送信し、(c) 要求元で共有されている認証情報を使用して生成される測定応答を、測定要求に対する応答として要求元から受信し、(d) 測定要求を送信してから測定応答

を受信するまでの時間を、往復遅延時間として測定し、(e) 測定要求を送信する前に、測定応答の生成に要する下準備を要求する測定準備要求を、要求元に送信し、(f) 往復遅延時間の測定後に、往復遅延時間が基準値以下であり、測定応答が正しいと検証され、かつ要求元において測定要求が正しいと検証された場合は、要求元がコンテンツデータの送

[続葉有]

WO 2006/028094 A1



- (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, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (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,

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, IS, IT, LT, LU, LV, 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).

添付公開書類:

— 国際調査報告書

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。

明 細 書

通信装置、通信システム、通信方法、媒体及びプログラム

技術分野

- [0001] 本発明は、暗号化されたコンテンツデータを送信または受信する通信装置、特に、伝送時間に基づいて、コンテンツデータの送信先または送信元が制限される通信装置に関する。

背景技術

- [0002] 近年、家庭内の装置をネットワークで接続し、各種コンテンツの共有を図る家庭内ネットワークが実現されつつある。家庭内ネットワークの実現形態のひとつとして、家庭内にルータを設け、そのルータにPCやデジタルテレビなどの各装置と、コンテンツを蓄積するAVサーバとをスター型で接続する形態が考えられる。ルータは、家庭内のネットワークと家庭外のネットワークとを接続するものである。家庭内のAVサーバは、このルータを介して家庭外のネットワークから取得された各種コンテンツや、ネットワーク以外の手段、例えばデジタル放送により放送された各種コンテンツなどを一旦蓄積し、各機器からの要求に応じて各種コンテンツを要求した受信装置へ送信する機能を有する。
- [0003] 一方、新作の映画や有料放送のテレビ番組、音楽などの著作権保護が必要なデータを扱う場合において、著作権を保護する必要がある。著作権を保護するための有力な方法として、著作権保護を必要とするデータを暗号化してデータの利用に制限を加える方法がある。
- [0004] 例えば、映像音声データ(以下、AVデータと記す。)を、ネットワークを利用して伝送する際に、AVデータの著作権を保護する必要がある場合、そのAVデータを暗号化して伝送することが行われている。これを実現する例として、DTCP-IP(Digital Transmission Protection over Internet Protocol)方式が規格化されている。
- [0005] DTCP-IP方式では、認証機能と鍵の無効化機能を備えており、AVデータを伝送する際に、不正な機器を排除し、AVデータなどの著作権保護が必要なデータを

暗号化して伝送することにより著作権の保護を実現している。

- [0006] また、著作権保護が必要なAVデータの利用において、一般に家庭内における個人的利用に限定されているため、家庭内のAVサーバから家庭外の不特定の受信装置に対してAVデータを無制限に配信することも制限する必要がある。
- [0007] DTCP-IP方式では、送信するコマンドの到達範囲を制限するために、生存時間(TTL:Time To Live)を用いている。なお、TTLは、IPv4におけるパケットの生存時間(Time To Liveフィールドの値)を表しており、IPv6では、中継数(Hop Limitフィールドの値)に相当するものである。これは、IPパケットヘッダに含まれるTTLフィールドに設定された値によって、IPパケットが経由できるルータの数を設定することができるというものである。
- [0008] しかし、IPパケットヘッダのTTLフィールドは改竄に対し保護されていないため、中継機器によって改竄が可能であるという課題を有している。
- [0009] そのため、DTCP-IP方式において、AVデータを送信する送信装置とAVデータを受信する受信装置との間の往復の伝送時間であるRTT(Round Trip Time)を測定して、所定の制限時間より短いと判定した場合に認証を許可する送受信システムが提案されている(例えば特許文献1を参照。)
- [0010] このようなデータ送受信システムにおいて、測定要求を送信してから、その応答を受信するまでの時間を測定することで往復伝送時間RTTを測定する場合に、不正な機器が間に介在すると、測定したRTTが実際より短くなってしまう可能性がある。そのため、測定要求と要求応答とのハンドシェイク中に不正な機器が介在していないか検証するため、測定要求を受信する装置側と要求応答を受信する装置側との両方で検証処理を実行する必要がある。
- [0011] 以下、従来のデータ送受信システムについて図1及び図2を参照して説明する。
- [0012] 図1は送信装置及び受信装置における暗号化伝送時の認証処理から暗号化伝送までの処理の流れを示す図である。
- [0013] 同図に示されるように、まず、受信装置は、認証要求を送信装置に送信して測定用認証処理S101を開始し、送信装置及び受信装置は認証処理S101終了後、伝送時間測定処理S102を実行して受信装置のRTTを測定し、RTTが基準値以下の場

合は、鍵交換用認証処理S103を実行し、認証処理が成功すると鍵交換処理S104を実行する。

- [0014] 鍵交換処理終了後、送信装置はAVデータを暗号化して送信し、受信装置は鍵交換処理で受信した交換鍵を使用して復号鍵を生成し、暗号化された受信データを復号処理する。(S105)。
- [0015] 図2は伝送時間測定処理S102の詳細な処理の流れを示す図である。
- [0016] まず、送信装置は送信装置測定情報を生成して、測定要求に格納して送信する(S111)。受信装置は受信した送信装置測定情報を検証し(S112)、不正であればエラー終了し、正しい場合は受信機測定情報を生成し(S113)、測定要求応答に格納して送信し、送信装置は測定要求応答を受信するとRTTを測定する(S114)。
- [0017] 続いて、送信装置はRTTの測定値をチェックし(S115)、基準値(Tmax)以下であれば、測定を終了して次の処理に進む。基準値より大きい場合は、測定回数をチェックし(S116)、所定回数に達していない場合は、S111に戻り、測定を繰り返す。受信装置は、測定要求応答送信後、要求受信待ち状態になっており、測定要求を受信した場合、S111に戻り、測定を繰り返す(S117)。
- [0018] 次に送信装置は受信した測定要求応答に格納されている受信装置測定情報が正しいか、検証し(S118)、不正であればエラー終了する。正しい場合は、測定値が基準値以下でありかつ正しい値であると判定する。

特許文献1:特開2004-194295号公報(第11ページ)

発明の開示

発明が解決しようとする課題

- [0019] しかしながら、上記したような従来のデータ送受信システムにおける伝送時間測定処理は、受信装置において、測定要求受信時に、送信装置測定情報を検証してから測定要求応答を送信するため、検証処理時間が伝送時間に加算されて測定され、正確なRTT測定が出来ないという課題がある。また、従来のデータ送受信システムは、伝送時間測定処理用の認証処理を別途設けているため、処理が複雑になるという課題と、伝送時間測定のみ行いたい場合でも、不要な鍵交換処理を実行するという課題がある。

[0020] そこで、本発明は、正確に伝送時間を測定できると共に、暗号化伝送用の認証処理を共用でき、かつ、不要な鍵交換処理を実行しない通信装置、通信システム、通信方法、媒体及びプログラムを提供することを目的とする。

課題を解決するための手段

[0021] 上記目的を達成するために、本発明に係る通信装置は、(a)コンテンツデータの送信に対する要求に応答する通信装置であって、(a1)前記コンテンツデータの送信を要求する要求元との間で認証情報を共有する認証手段と、(a2)前記認証情報を使用して生成した測定要求を、前記要求元に送信する測定要求送信手段と、(a3)前記要求元で共有されている認証情報を使用して生成される測定応答を、前記測定要求に対する応答として前記要求元から受信する測定応答受信手段と、(a4)前記測定要求を送信してから前記測定応答を受信するまでの時間を、往復遅延時間として測定する往復遅延時間測定手段と、(a5)前記往復遅延時間の測定後に、前記往復遅延時間が基準値以下であり、前記測定応答が正しいと検証され、かつ前記要求元において前記測定要求が正しいと検証されたことを確認した場合は、前記要求元が前記コンテンツデータの送信先として適格な装置であると判定する判定手段とを備える。

[0022] さらに、(a6)前記通信装置は、前記測定要求を送信する前に、前記測定応答の生成に要する下準備を要求する測定準備要求を、前記要求元に送信する測定準備要求送信手段を備えるとしてもよい。

[0023] さらに、(a7)前記判定手段は、前記認証情報を使用して生成した第1の検証情報と、前記要求元で認証情報を使用して生成された第2の検証情報とが一致する場合は、前記測定応答が正しいと検証するとしてもよい。

[0024] または、上記目的を達成するために、本発明に係る通信装置は、(b)コンテンツデータの送信を要求する通信装置であって、(b1)前記コンテンツデータの送信に対する要求に応答する要求先との間で認証情報を共有する認証手段と、(b2)前記要求先で共有されている認証情報を使用して生成された測定要求を、前記要求先から受信する測定要求受信手段と、(b3)前記認証情報を使用して生成した測定応答を、前記測定要求に対する応答として前記要求先に折り返し送信する測定応答送信手

段と、(b4)前記測定要求が正しいか検証する判定手段とを備える。

[0025] さらに、(b5)前記測定要求を受信する前に、前記測定応答の生成に要する下準備を要求する測定準備要求を、前記要求先から受信する測定準備要求受信手段を備えるとしてもよい。

[0026] なお、本発明は、通信装置として実現されるだけではなく、データ通信網を介して相互に接続されている要求先の通信装置(サーバ)と要求元の通信装置(クライアント)とを備える通信システムとしてもよい。

[0027] また、通信装置(サーバまたはクライアント)を制御する通信方法、通信方法をコンピュータシステムなどに実行させる通信プログラム、通信プログラムを記録した記録媒体としても実現されるとしてもよい。

発明の効果

[0028] 以上説明したところから明らかなように、本発明は、測定値が基準値以下の場合に受信装置側の検証処理を実行し、伝送時間測定用の認証処理を暗号化伝送用の認証処理で共用し、測定開始要求で測定が起動された場合は、測定処理と登録処理のみ実行することにより、正確に伝送時間を測定できると共に、既存の認証処理を共用でき、かつ不要な鍵交換処理を実行しない伝送時間測定方法、データ送受信システム、媒体及び情報集合体を提供することが出来る。

図面の簡単な説明

[0029] [図1]図1は、従来のデータ送受信システムにおける暗号化伝送時の処理シーケンスを示す図である。

[図2]図2は、従来のデータ送受信システムにおける伝送時間測定処理の処理シーケンスを示す図である。

[図3]図3は、本発明の実施の形態1および実施の形態2におけるデータ送受信システムの構成を示す図である。

[図4]図4は、本発明の実施の形態1における送信装置の構成を示す図である。

[図5]図5は、本発明の実施の形態1における受信装置の構成を示す図である。

[図6]図6は、本発明の実施の形態1における、暗号化伝送時の処理シーケンスを示す図である。

[図7]図7は、本発明の実施の形態1における、伝送時間測定処理の処理シーケンスを示す図である。

[図8]図8は、本発明の実施の形態2における送信装置の構成を示す図である。

[図9]図9は、本発明の実施の形態2における受信装置の構成を示す図である。

[図10]図10は、本発明の実施の形態2において、送信装置が伝送時間測定を起動する場合の処理シーケンスを示す図である。

[図11]図11は、本発明の実施の形態2において、受信装置が伝送時間測定を起動する場合の処理シーケンスを示す図である。

符号の説明

- [0030]
- 1 AVサーバ
 - 2 デジタルテレビ
 - 3 PC
 - 4 ルータ
 - 5 ルータ
 - 6 PC
 - 7 デジタルテレビ
 - 21 送受信部
 - 22 暗号処理部
 - 23 鍵交換処理部
 - 24 認証処理部
 - 25 伝送時間測定処理部
 - 26、27 受信装置登録部
 - 28 測定開始処理部
 - 31 送受信部
 - 32 復号処理部
 - 33 鍵交換処理部
 - 34 認証処理部
 - 35 伝送時間測定処理部

36 測定開始処理部

発明を実施するための最良の形態

[0031] (実施の形態1)

以下、本発明の実施の形態1について図3から図7までを用いて詳細に説明する。

[0032] <概要>

本実施の形態において、(a)コンテンツデータの送信に対する要求に応答する通信装置(以下、送信装置と呼称する。)は、(a1)コンテンツデータの送信を要求する要求元との間で認証情報を共有し、(a2)認証情報を使用して生成した測定要求を、要求元に送信し、(a3)要求元で共有されている認証情報を使用して生成される測定応答を、測定要求に対する応答として要求元から受信し、(a4)測定要求を送信してから測定応答を受信するまでの時間を、往復遅延時間として測定し、(a5)測定要求を送信する前に、測定応答の生成に要する下準備を要求する測定準備要求を、要求元に送信し、(a6)往復遅延時間の測定後に、往復遅延時間が基準値以下であり、測定応答が正しいと検証され、かつ要求元において測定要求が正しいと検証された場合は、要求元が前記コンテンツデータの送信先として適格な装置であると判定することを特徴とする。

[0033] また、(b)コンテンツデータの送信を要求する通信装置(以下、受信装置と呼称する。)は、(b1)コンテンツデータの送信に対する要求に応答する要求先との間で認証情報を共有し、(b2)要求先で共有されている認証情報を使用して生成された測定要求を、要求先から受信し、(b3)認証情報を使用して生成した測定応答を、測定要求に対する応答として要求先に折り返し送信し、(b4)測定要求を受信する前に、測定応答の生成に要する下準備を要求する測定準備要求を、要求先から受信することを特徴とする。

[0034] そして、データ通信網を介して相互に接続されている送信装置と受信装置とを備える通信システム(以下、データ送受信システムと呼称する。)において、本実施の形態における伝送時間測定方法に基づいて、測定工程で測定した測定値が所定値以下である場合に、互いに相手装置から受信した測定情報が正しいかどうかを検証し、正しい場合には測定値が正確な値であると判断する。

[0035] また、本実施の形態のデータ送受信システムは、認証処理を実行した後、送信装置は、受信装置が登録されていない場合、測定手段によって往復遅延時間を測定し、判定手段によって測定値が正確な値であると判定した場合に鍵交換処理を実行し、受信装置が登録されている場合、続いて鍵交換処理を実行する。

[0036] 以上の点を踏まえて、本実施の形態におけるデータ送受信システム、および伝送時間測定方法について説明する。

[0037] <構成>

図3は、本実施の形態のデータ送受信システムを構成する送信装置及び受信装置を示す図であり、送信装置であるAVサーバ、受信装置であるPC、デジタルテレビ、およびルータの接続図である。

[0038] 図3に示されるように、家庭内には、AVサーバ1、デジタルテレビ2、PC3、およびルータ4が設置されている。ルータ4とAVサーバ1、デジタルテレビ2はイーサネット(登録商標)で接続されており、ルータ4とPC3は無線メディア(IEEE802. 11b)で接続されている。

[0039] またルータ4は、インターネットを介して家庭外のルータ5と接続される。ルータ5は、受信装置であるPC6、デジタルテレビ7と接続されている。ここで、ルータ5とPC6はイーサネット(登録商標)で接続されており、ルータ5とデジタルテレビ7は無線メディア(IEEE802. 11b)で接続されている。

[0040] 図4に、送信装置であるAVサーバ1の構成を示す。

[0041] 図4に示されるように、AVサーバ1は、送受信部21、暗号処理部22、鍵交換処理部23、認証処理部24、伝送時間測定処理部25、受信装置登録部26から構成される。ここで、伝送時間測定処理部25は、本発明における、測定準備要求送信手段、測定準備応答受信手段、測定準備手段、測定要求送信手段、測定応答受信手段、測定手段及び判定手段に、受信装置登録部26は登録手段および登録確認手段にそれぞれ対応する。

[0042] 送受信部21は、AVデータをネットワークに送信し、またネットワークに接続されている他の機器とコマンドなどを送受信するためのデジタルインターフェースである。

[0043] 暗号処理部22は、コンテンツ記録部(図示せず)から再生されたAVデータを暗号

化する。

- [0044] 鍵交換処理部23は、受信装置がAVデータの暗号を復号するために使用する交換鍵を生成し、認証処理部24から受信した認証情報を使用して暗号化して送受信部21を介して出力する。
- [0045] 認証処理部24は、受信装置から認証要求を受信して認証処理を行い、受信装置と認証情報を共有するとともに、受信装置のRTT測定機能の有無を示すフラグ情報を証明情報と共に受信する。
- [0046] 伝送時間測定処理部25は、測定準備要求、測定要求を生成して、送受信部21を介して送信し、受信した測定準備要求応答、測定要求応答を処理する。また、測定要求を送信してから測定要求応答を受信するまでの往復遅延時間であるRTTを測定し、所定の基準値以下である場合は、検証要求を生成して送受信部21を介して送信し、受信した検証要求応答を処理して、測定したRTTが正しいか判定する。
- [0047] 受信装置登録部26は、伝送時間測定処理部25によってRTTが基準値以下であると判定された受信装置のデバイスIDを格納する。ここで、デバイスIDとは、予め鍵管理センターから与えられているものであり、機器を特定するための情報である。
- [0048] 受信装置であるデジタルテレビ2、PC3、PC6、デジタルテレビ7のデータ送受信部はそれぞれ同様の構成を持つ。図5に受信装置(デジタルテレビ2など。)のデータ送受信部の構成を示す。
- [0049] 図5に示されるように、受信装置(デジタルテレビ2など。)は、送受信部31、復号処理部32、鍵交換処理部33、認証処理部34、伝送時間測定処理部35から構成される。ここで、伝送時間測定処理部35は本発明における、測定準備要求受信手段、測定準備応答送信手段、測定準備手段、測定要求受信手段、測定応答送信手段及び検証手段に対応する。
- [0050] 送受信部31は、ネットワークを介して送信されたAVデータを受信し、またネットワークに接続されている他の機器とコマンドなどを送受信するためのデジタルインターフェースである。
- [0051] 復号処理部32は、鍵交換処理部33から送信された交換鍵を受信し、受信した交換鍵を使用して復号鍵を生成し、送受信部31を介してAVデータを受信し、受信した

AVデータの暗号を復号する。復号処理部32で復号されて平文になったAVデータは、デコーダ(図示せず)でデコードされ、モニタ(図示せず)に表示される。

[0052] 鍵交換処理部33は、送受信部31を介して交換鍵を受信し、また、認証処理部34から送信された認証情報を受信し、受信した認証情報を使用して、受信した交換鍵を処理して復号処理部32に送信する。

[0053] 認証処理部34は、送受信部31を介して、AVサーバ1の認証処理部24に対して認証開始を要求し、認証処理を実行して認証情報をAVサーバ1の認証処理部24と共有する。また、受信装置のRTT測定機能の有無を示すフラグ情報を証明情報と共に送受信部31を介してAVサーバ1に送信する。

[0054] 伝送時間測定処理部35は、送受信部31を介して、AVサーバ1から送信される測定準備要求、測定要求、検証要求を受信処理し、測定準備要求、測定要求応答及び検証要求応答を生成して、送受信部31を介してAVサーバ1に送信する。

[0055] <動作>

次に、上記のように構成された本実施の形態の動作を説明する。

[0056] 図6は、送信装置(AVサーバ1)及び受信装置(デジタルテレビ2)における暗号化伝送時の認証処理から暗号化伝送までの処理の流れを示す図である。

[0057] 図6に示されるように、まず、受信装置の認証処理部34は、認証要求を送信装置に送信して認証処理(S41)を開始する。

[0058] 認証処理(S41)終了後、送信装置の伝送時間測定処理部25は、認証処理(S41)において受信した受信装置のRTT測定機能の有無を示すフラグ情報をチェックし(S42)、RTT測定機能を有する場合は次の処理(S43)に進む。RTT測定機能を有さない場合は鍵交換処理(S47)に進む。

[0059] 次に、送信装置の受信装置登録部26は、受信装置が登録されているかどうか判定し(S43)、未登録であれば、次の伝送時間測定処理(S45)に進む。登録されている場合は鍵交換処理(S47)に進む。

[0060] 受信装置は、認証処理(S41)終了後、要求受信待ち状態になっており、受信した要求をチェックし(S44)、測定準備要求を受信した場合は、伝送時間測定処理(S45)に進む。交換鍵を受信した場合は、鍵交換処理(S47)に進む。

- [0061] 送信装置は、伝送時間測定処理(S45)終了後、伝送時間測定処理が正常に終了したかどうか確認し(S46)、正常に終了していれば、鍵交換処理(S47)を実行し、正常に終了していなければ送信処理をエラー終了する。
- [0062] 受信装置は、伝送時間測定処理(S45)終了後、要求受信待ち状態になっており、交換鍵を受信した場合は、鍵交換処理(S47)を実行する。
- [0063] 送信装置は、鍵交換処理(S47)が終了すると、コンテンツデータを暗号化して送信し、受信装置は、暗号化されたコンテンツデータを受信して、復号処理する(S48)。
- [0064] 図7は、伝送時間測定処理(S45)の詳細な処理の流れを示す図である。
- [0065] 図7に示されるように、まず、送信装置及び受信装置は、測定準備工程として、測定準備要求送信工程(S51)～測定準備工程(S53)を実行する。送信装置は、測定番号Nを格納した測定準備要求を受信装置に送信し(S51)、送信装置測定情報を生成する。受信装置は、測定準備要求に対する応答として、測定準備要求応答を送信装置に送信する(S52)。送信装置は、測定準備要求応答を受信すると、測定処理の準備をし、また、受信装置は、測定準備応答送信後、受信装置測定情報を生成し、測定処理の準備をする(S53)。
- [0066] 測定準備工程において、送信装置測定情報及び受信装置測定情報は、以下の手順で生成される。まず、認証処理部24または認証処理部34から供給されるKauth(96bit)と測定回数値N(初期値0)とを使用して、共通の秘密情報である共通検証情報Kvrfy(160bit)を生成する。共通検証情報Kvrfy(160bit)を、Kvrfy(上位80bit)とKvrfy(下位80bit)とに分割する。送信装置は、Kvrfy(上位80bit)を送信装置測定情報とし、Kvrfy(下位80bit)を受信装置測定情報の検証用情報として用意する。受信装置は、Kvrfy(下位80bit)を受信装置測定情報とし、Kvrfy(上位80bit)を送信装置測定情報の検証用情報として用意する。
- [0067] 次に、送信装置及び受信装置は、測定工程として、測定要求送信工程(S54)及びRTT測定工程(S55)を実行する。送信装置は、送信装置測定情報を測定要求に格納して送信し、受信装置は、測定工程として、受信装置測定情報を測定要求応答に格納して送信する(S54)。このとき、送信装置は、受信装置が応答する測定要求応答を受信してRTTを測定する(S55)。

- [0068] 続いて、送信装置及び受信装置は、判定工程として、基準値判定工程(S56)～受信装置検証情報検証工程(S64)を実行する。送信装置は、測定値(RTT)をチェックし(S56)、基準値(Tmax)以下であれば(S56:YES)、測定を終了して、次の処理に進む。基準値より大きい場合は(S56:NO)、測定回数をチェックし(S57)、所定回数に達していない場合は(S57:YES)、測定準備要求送信工程(S51)に戻り測定を繰り返す。このとき、受信装置は、測定要求応答送信後、要求受信待ち状態になっており、測定準備要求を受信した場合は、測定準備要求応答工程(S52)に戻る。そして、繰り返し測定につきあう(S58)。
- [0069] 次に、送信装置は、受信した測定要求応答に格納されている受信装置測定情報を、用意しておいた検証用情報と比較し(S59)、一致しない場合は(S59:NO)、エラー終了する。一致する場合は(S59:YES)、検証要求を送信する(S60)。受信装置は、検証要求を受信すると、測定要求に格納されていた送信装置測定情報を、用意しておいた検証用情報と比較して(S61)、一致しない場合は(S61:NO)、エラー終了し、一致する場合は(S61:YES)、認証情報Kauthから受信装置検証情報を生成し(S62)、受信装置検証情報を検証要求応答に格納して送信する(S63)。
- [0070] 送信装置は、受信した受信装置検証情報を検証して最終的に測定値が正しい値であることを検証する(S64)、不正な場合は(S64:NO)、エラー終了し、正しい場合は(S64:YES)、次の登録処理に進む。
- [0071] 最後に、送信装置は、判定処理において測定値が基準値以下でありかつ、正しいと判定された受信装置のデバイスIDを受信装置登録部26に登録する(S65)。
- [0072] 例えば、図3における各装置間の伝送で、イーサネット(登録商標)の往復遅延時間を0.02ms(ミリ秒)、無線(802.11b)の往復遅延時間を3ms、ルータの処理遅延時間を0.5ms、インターネットの往復遅延時間を10ms、受信装置の処理遅延時間を0.2msとする。さらに、ここでは、ルータ2台が経路上に存在する場合を想定する。これにより、送信装置であるAVサーバ1と各受信装置との間の伝送時間(RTT)は、家庭内装置間では、以下の(1)、(2)のようになる。また、家庭内装置と家庭外装置との間では、以下の(3)、(4)のようになる。
- (家庭内装置間)

(1) デジタルテレビ2とのRTT(T_1) = $0.02 + 0.02 + 0.2 = 0.24\text{ms}$

(2) PC3とのRTT(T_2) = $0.02 + 3 + 0.2 = 3.22\text{ms}$

(家庭内装置－家庭外装置間)

(3) PC6とのRTT(T_3) = $0.02 + 0.5 \times 4 + 10 + 0.02 + 0.2 = 12.24\text{ms}$

(4) デジタルテレビ7とのRTT(T_4) = $0.02 + 0.5 \times 4 + 10 + 3 + 0.2 = 15.22\text{ms}$

[0073] ここで、基準値 $T_{\text{max}} = 7\text{ms}$ とすると、家庭内の装置であるデジタルテレビ2、PC3については、RTTが7ms以下であるので、受信装置は登録される。そして、これらの家庭内の装置との間で、鍵交換処理(S47)、暗号化伝送処理(S48)が実行される。一方、家庭外の装置であるPC6及びデジタルテレビ7については、RTTが7msより大であるため、受信装置は登録されない。そして、これらの家庭外の装置との間で、鍵交換処理(S47)、暗号化伝送処理(S48)は実行されない。

[0074] 以上の動作により、RTTの測定値が基準値以下であり、かつ受信装置のRTTとして正しいと判定したとき、鍵交換処理が実行され、受信装置は、暗号化されたデータを復号することができる。

[0075] 以上のように、本実施の形態の伝送時間測定方法は、測定工程で測定した測定値が所定値以下である場合に、互いに相手装置から受信した測定情報が正しいかどうかを検証する。このことにより、受信装置は、測定要求処理中に検証処理を実行しないため、検証処理時間が、伝送時間に加算されず、正確な往復遅延時間を測定することができる。このように、本実施の形態固有の効果をすることができる。

[0076] また、本実施の形態のデータ送受信システムは、認証処理を実行した後、送信装置は、受信装置が登録されていない場合は、測定手段によって往復遅延時間を測定し、判定手段によって測定値が正確な値であると判定した場合に、鍵交換処理を実行する。一方、受信装置が登録されている場合は、続いて鍵交換処理を実行するため、鍵交換を実行するための認証処理を変更することなく、伝送時間測定のための認証処理として共用することができる。このように、本実施の形態固有の効果をすることができる。

[0077] なお、本実施の形態では、認証情報から共通検証情報を生成し、共通検証情報を

受信装置測定情報と送信装置測定情報とを分割して生成した。しかし、他の手段を用いて測定情報を生成してもよい。

[0078] さらに、本実施の形態では、送信装置は、測定準備要求送信後に送信装置測定情報を生成する。しかし、測定要求を送信する前であれば、別のタイミングで生成してもよい。

[0079] さらに、本実施の形態では、受信装置として台数が4台の場合について説明した。しかし、これに限らず、他の任意の台数が接続されていても構わない。

[0080] さらに、本実施の形態では、ネットワークの伝送メディアとしてイーサネット(登録商標)とIEEE802. 11bの場合について説明した。しかし、IEEE802. 11a/g/nやBluetooth等、他の伝送メディアを使用しても構わない。

[0081] さらに、本実施の形態では、基準値を7msとした。しかし、これに限らず、他の基準値を設定してもよい。

[0082] (実施の形態2)

以下、本発明の実施の形態2について図8から図11を参照して詳細に説明する。

[0083] <概要>

本実施の形態におけるデータ送受信システムは、送信装置もしくは受信装置が測定開始要求を送信した場合は、認証処理を実行した後、測定手段によって伝送時間を測定し、判定手段によって測定値が正確な値であると判定した場合に受信装置を登録し、鍵交換処理を実行しない。

[0084] <構成>

本実施の形態のデータ送受信システムを構成する送信装置及び受信装置は、実施の形態1と同様に図3で示される。

[0085] 図8に、本実施の形態における送信装置であるAVサーバ1の構成を示す。

[0086] AVサーバ1は、送受信部21、暗号処理部22、鍵交換処理部23、認証処理部24、伝送時間測定処理部25、受信装置登録部27、測定開始処理部28から構成される。ここで、伝送時間測定処理部35は本発明における測定準備手段、測定手段及び判定手段に、受信装置登録部27は登録手段、登録確認手段及び登録解除手段に、測定開始処理部28は測定開始手段にそれぞれ対応する。

- [0087] 本実施の形態における送信装置の構成が実施の形態1の構成と異なるのは受信装置登録部27と測定開始処理部28であり、他の構成部分は同一であるため説明を省略する。
- [0088] 受信装置登録部27は、伝送時間測定処理部25によってRTTが基準値以下であると判定された受信装置のデバイスIDを格納して受信装置を登録する。また、登録後所定の有効時間が経過した時、登録を解除する。
- [0089] 測定開始処理部28は、上記有効時間の残り時間をチェックし、残り時間が0になったとき、測定開始要求を送信し、測定処理のための認証処理を開始する。また、測定開始要求を受信した場合も、測定処理のための認証処理を開始する。
- [0090] 図9に受信装置(デジタルテレビ2)のデータ送受信部の構成を示す。
- [0091] 受信装置は、送受信部31、復号処理部32、鍵交換処理部33、認証処理部34、伝送時間測定処理部35、測定開始処理部36から構成される。ここで、伝送時間測定処理部35は、本発明における測定準備要求受信手段、測定準備応答送信手段、測定準備手段、測定要求受信手段、測定応答送信手段及び検証手段、測定開始処理部は測定開始判定手段、測定開始要求送信手段、測定開始応答受信手段に対応する。
- [0092] 本実施の形態における受信装置の構成が実施の形態1の構成と異なるのは測定開始処理部36であり、他の構成部分は同一であるため説明を省略する。
- [0093] 測定開始処理部36は、暗号化されたデータの受信終了時または、認証処理と鍵交換処理の間に伝送時間測定処理が実行されなかった場合、鍵交換処理終了時に、測定開始要求を送信して測定処理のための認証処理を開始する。また、測定開始要求を受信した場合も測定処理のための認証処理を開始する。
- [0094] <動作>
本実施の形態におけるデータ送信システムの動作について図10及び図11を参照して説明する。
- [0095] 図10は本実施の形態において、送信装置が測定処理を起動する場合の動作シーケンスを示す。
- [0096] 送信装置の測定開始処理部28は、受信装置登録部27において管理される登録

の有効時間をチェックし(S81)、有効時間の残り時間が0か判定し、0であるときは受信装置に測定開始要求を送信する(S83)。受信装置の測定開始処理部36は、受信した要求をチェックし(S82)、測定開始要求を受信すると、応答を送信し(S84)、認証処理部34に対し認証開始を要求し、認証処理部34は、認証要求を発行して認証処理を実行する(S85)。この認証処理(S85)は、鍵交換処理を実行する場合の認証処理(S41)と同一の処理を共用する。

[0097] 認証処理(S85)が終了すると、送信装置の伝送時間測定処理部25は、伝送時間測定処理(S86)を実行し、測定値が基準値以下であり、かつ測定値が正しいと判定した場合は、受信装置を登録し、処理を終了する。測定開始要求を送信することで測定を起動した場合は、鍵交換処理を実行しない。なお、伝送時間測定処理(S85)の詳細動作は図7で示した実施の形態1における伝送時間測定処理(S45)と同一である。

[0098] この場合は、受信装置の登録を常に有効にすることができる。このため、暗号化伝送のために鍵交換処理を実行するにあたって、伝送時間測定処理を実行する必要が無い。

[0099] 図11は、本実施の形態において、受信装置が測定処理を起動する場合の動作シーケンスを示す。

[0100] 受信装置の測定開始処理部36は、受信されるデータをチェックし、暗号化されたデータの受信終了時、または認証処理と鍵交換処理の間に伝送時間測定処理が実行されなかった場合は、鍵交換処理による交換鍵受信時に、測定開始を決定し(S91)、送信装置に測定開始要求を送信する(S93)。送信装置の測定開始処理部28は、受信した要求をチェックし(S92)、測定開始要求を受信すると、応答を送信する(S94)。そして、受信装置は、応答を受信すると、認証処理部34に対して、認証開始を要求する。認証処理部34は、認証要求を発行して認証処理を実行する(S95)。この認証処理(S95)は、鍵交換処理を実行する場合の認証処理(S41)と同一の処理を共用する。

[0101] 認証処理(S95)が終了すると、送信装置の伝送時間測定処理部35は、伝送時間測定処理(S96)を実行し、測定値が基準値以下であり、かつ測定値が正しいと判定

した場合は、受信装置を登録し、処理を終了する。測定開始要求を送信することで測定を起動した場合は、鍵交換処理を実行しない。伝送時間測定処理(S96)の詳細動作は、図7で示した実施の形態1における伝送時間測定処理(S45)と同一である。

[0102] この場合も、受信装置の登録を常に有効にすることができる。このため、暗号化伝送のために鍵交換処理を実行するにあたって、伝送時間測定処理を実行する必要が無い。

[0103] 以上のように、本実施の形態のデータ送受信システムは、送信装置もしくは受信装置が測定開始要求を送信した場合において、認証処理を実行した後、測定手段によって伝送時間を測定し、判定手段によって測定値が正確な値であると判定した場合に受信装置を登録する。これにより、鍵交換を実行するための認証処理を変更することなく、伝送時間測定のための認証処理として共用することができ、かつ不要な鍵交換処理を実行しないという本実施の形態固有の効果を得ることができる。

[0104] また、本実施の形態のデータ送受信システムにおける送信装置は、登録の有効時間の残り時間をチェックして伝送時間測定を起動するため、登録が無効になることが無く、暗号化伝送を行うために認証処理及び鍵交換処理を実行する際には、伝送時間測定処理を実行する必要がないため、伝送開始時の遅延時間を短縮できるという本実施の形態固有の効果を得ることができる。

[0105] また、本実施の形態のデータ送受信システムにおける受信装置は、暗号化されたデータの受信終了時、または、認証処理と鍵交換処理の間に伝送時間測定処理が実行されなかった場合、交換鍵受信時に伝送時間測定を起動するため、登録が無効になることが無く、暗号化伝送を行うために認証処理及び鍵交換処理を実行する際には、伝送時間測定処理を実行する必要がないため、伝送開始時の遅延時間を短縮できるという本実施の形態固有の効果を得ることができる。さらに、交換鍵受信時に伝送時間測定を起動する場合は、認証鍵交換処理と同一のセッションを使用して測定開始処理及び測定処理が実行できるという本実施の形態固有の効果を得ることができる。

[0106] なお、本実施の形態では、送信装置は、登録の有効時間の残り時間が0になったと

きに伝送時間測定を起動しているが、残り時間が所定値以下の場合に起動してもよいし、残り時間と他の条件を組み合わせで起動してもよい。

[0107] さらに、本実施の形態では、受信装置は、暗号化されたデータの受信終了時、または交換鍵受信時に伝送時間測定を起動しているが、送信装置における自装置の登録の残り時間を推定し、残り時間に余裕があると推定した場合は、伝送時間測定を起動しなくてもよい。

[0108] さらに、本発明のデータ送受信システムの機能をコンピュータにより実行させるためのプログラム及び／またはデータを担持した媒体であって、コンピュータにより処理可能なことを特徴とする媒体も本発明に属する。

[0109] さらに、本発明のデータ送受信システムの機能をコンピュータにより実行させるためのプログラム及び／またはデータであることを特徴とする情報集合体も本発明に属する。

[0110] さらに、本発明のデータとは、データ構造、データフォーマット、データの種類などを含む。

[0111] さらに、本発明の媒体とは、ROM等の記録媒体、インターネット等の伝送媒体、光・電波・音波等の伝送媒体を含む。

[0112] さらに、本発明の担持した媒体とは、例えば、プログラム及び／またはデータを記録した記録媒体、やプログラム及び／またはデータを伝送する伝送媒体等を含む。

[0113] さらに、本発明のコンピュータにより処理可能とは、例えば、ROMなどの記録媒体の場合であれば、コンピュータにより読みとり可能であることであり、伝送媒体の場合であれば、伝送対象となるプログラム及び／またはデータが伝送の結果として、コンピュータにより取り扱えることであることを含む。

[0114] さらに、本発明の情報集合体とは、例えば、プログラム及び／またはデータ等のソフトウェアを含むものである。

[0115] さらに、以上説明した様に、本発明の構成は、ソフトウェア的に実現してもよいし、ハードウェア的に実現してもよい。

産業上の利用可能性

[0116] 本発明は、暗号化されたデータを送受信する送受信システム、伝送時間測定方法

に関するものであり、家庭内ネットワーク等におけるAVデータ伝送に有用である。

請求の範囲

- [1] コンテンツデータの送信に対する要求に応答する通信装置であって、
前記コンテンツデータの送信を要求する要求元との間で認証情報を共有する認証手段と、
前記認証情報を使用して生成した測定要求を、前記要求元に送信する測定要求送信手段と、
前記要求元で共有されている認証情報を使用して生成される測定応答を、前記測定要求に対する応答として前記要求元から受信する測定応答受信手段と、
前記測定要求を送信してから前記測定応答を受信するまでの時間を、往復遅延時間として測定する往復遅延時間測定手段と、
前記往復遅延時間の測定後に、前記往復遅延時間が基準値以下であり、前記測定応答が正しいと検証され、かつ前記要求元において前記測定要求が正しいと検証されたことを確認した場合は、前記要求元が前記コンテンツデータの送信先として適格な装置であると判定する判定手段と
を備えることを特徴とする通信装置。
- [2] 前記通信装置は、さらに、
前記測定要求を送信する前に、前記測定応答の生成に要する下準備を要求する測定準備要求を、前記要求元に送信する測定準備要求送信手段
を備えることを特徴とする請求項1に記載の通信装置。
- [3] 前記判定手段は、前記認証情報を使用して生成した第1の検証情報と、前記要求元で前記認証情報を使用して生成された第2の検証情報とが一致する場合は、前記測定応答が正しいと検証する
ことを特徴とする請求項2に記載の通信装置。
- [4] 前記認証情報は、前記要求元が往復遅延時間の測定に対応する機能を有するか否かが特定されるフラグと、前記フラグに対する証明情報とを含み、
前記通信装置は、さらに、
前記フラグに基づいて、前記要求元が往復遅延時間の測定に応じる機能を有するか否かを判断する測定機能判断手段を備え、

前記測定準備要求送信手段は、前記機能を有する場合は、前記測定準備要求を送信し、前記機能を有しない場合は、前記測定準備要求を送信しない

ことを特徴とする請求項3に記載の通信装置。

[5] 前記通信装置は、さらに、

前記要求元が前記コンテンツデータの送信先として適格な装置である場合は、前記要求元が識別される装置識別情報を一覧表に登録する登録手段と、

前記測定準備要求を前記要求元に送信する前に、前記装置識別情報が前記一覧表に登録されているか否かを確認する登録確認手段と

を備え、

前記測定準備要求送信手段は、前記一覧表に登録されている場合は、前記測定準備要求を送信せず、前記一覧表に登録されていない場合は、前記測定準備要求を送信する

ことを特徴とする請求項3に記載の通信装置。

[6] 前記通信装置は、さらに、

前記装置識別情報に設定された登録有効期間が経過すると、前記装置識別情報の登録を解除する登録解除手段

を備えることを特徴とする請求項5に記載の通信装置。

[7] 前記要求元は、前記下準備として、前記測定準備要求を受信してから前記測定要求を受信するまでの間に、前記要求元との間で共有する認証情報を使用して、要求元情報を生成し、前記要求元情報を分割して第1の要求元部分情報と第2の要求元部分情報とを生成する場合において、

前記通信装置は、さらに、

前記認証情報を使用して、前記要求元情報と共通する要求先情報を生成し、前記要求先情報を分割して第1の要求先部分情報と第2の要求先部分情報とを生成する測定準備手段と、

前記第2の要求元部分情報と前記第1の要求先部分情報とが一致する場合は、前記測定応答の送信元が真正の要求元であると判断する要求元検証手段と

を備え、

前記測定応答受信手段は、前記第2の要求元部分情報を含む応答を、前記測定応答として前記要求元から受信する

ことを特徴とする請求項3に記載の通信装置。

- [8] 前記要求元は、前記第2の要求先部分情報と前記第1の要求元部分情報とが一致する場合は、前記測定要求の送信元が真正の要求先であると判断し、前記第2の検証情報を生成する場合において、

前記検証手段は、

前記測定要求の送信元が真正の要求先であるか否かを検証することを要求する検証要求を、前記要求元に送信する検証要求送信手段と、

前記第2の検証情報を含む検証応答を、前記検証要求に対する応答として前記要求元から受信する検証応答受信手段と

を備え、

前記測定要求送信手段は、

前記第2の要求先部分情報を含む要求を、前記測定要求として前記要求元に送信する

ことを特徴とする請求項7に記載の通信装置。

- [9] 前記通信装置は、さらに、

前記装置識別情報の登録を解除するまでの残り時間に基づいて、前記往復遅延時間の測定を開始するか否かを判定する測定開始判定手段と、

前記残り時間が所定の時間以下である場合に、測定開始要求を前記要求元に送信する測定開始要求送信手段と、

前記測定開始要求に対する応答として測定開始応答を前記要求元から受信する測定開始応答受信手段と

を備え、

前記認証手段は、前記測定開始応答を前記要求元から受信した後に、前記要求元との間で認証情報を共有する

ことを特徴とする請求項6に記載の通信装置。

- [10] 前記通信装置は、さらに、

前記往復遅延時間の測定を開始するか否かを判定する測定開始判定手段と、
前記往復遅延時間の測定を開始する場合は、前記往復遅延時間の測定を開始することを通知する測定開始要求を、前記要求元に送信する測定開始要求送信手段と、
、
前記測定開始要求に対する応答として測定開始応答を前記要求元から受信する測定開始応答受信手段と
を備え、
前記認証手段は、前記測定開始応答を前記要求元から受信した後に、前記要求元との間で認証情報を共有する
ことを特徴とする請求項1に記載の通信装置。

- [11] 前記通信装置は、さらに、
前記往復遅延時間の測定を開始することを要求する測定開始要求を前記要求元から受信する測定開始要求受信手段と、
前記測定開始要求に対する応答として測定開始応答を前記要求元に送信する測定開始応答送信手段と
を備え、
前記認証手段は、前記測定開始応答を前記要求元に送信した後に、前記要求元との間で認証情報を共有する
ことを特徴とする請求項1に記載の通信装置。

- [12] コンテンツデータの送信を要求する通信装置であって、
前記コンテンツデータの送信に対する要求に応答する要求先との間で認証情報を共有する認証手段と、
前記要求先で共有されている認証情報を使用して生成された測定要求を、前記要求先から受信する測定要求受信手段と、
前記認証情報を使用して生成した測定応答を、前記測定要求に対する応答として前記要求先に折り返し送信する測定応答送信手段と、
前記測定要求が正しいか検証する判定手段と
を備えることを特徴とする通信装置。

- [13] 前記通信装置は、さらに、
前記測定要求を受信する前に、前記測定応答の生成に要する下準備を要求する測定準備要求を、前記要求先から受信する測定準備要求受信手段
を備えることを特徴とする請求項12に記載の通信装置。
- [14] 前記要求先は、前記要求元との間で共有する認証情報を使用して、要求先情報を生成し、前記要求先情報を分割して第1の要求先部分情報と第2の要求先部分情報とを生成する場合において、
前記通信装置は、さらに、
前記下準備として、前記測定準備要求を受信してから前記測定要求を受信するまでの間に、前記認証情報を使用して、前記要求先情報と共通する要求元情報を生成し、前記要求元情報を分割して第1の要求元部分情報と第2の要求元部分情報とを生成する測定準備手段と、
前記測定要求の送信元が真正の要求先であるか否かを検証することを要求する検証要求を、前記要求先から受信する検証要求受信手段と、
前記第2の要求先部分情報と前記第1の要求元部分情報とが一致する場合は、前記測定要求の送信元が真正の要求先であると判断する要求先検証手段と、
前記測定要求の送信元が真正の要求先である場合は、前記認証情報を使用して、前記要求先との間で前記往復遅延時間の測定が行われたことを通知する検証情報を生成する検証情報生成手段と、
前記検証情報を含む検証応答を、前記検証要求に対する応答として前記要求先に送信する検証応答送信手段と
を備え、
前記測定要求受信手段は、前記第2の要求先部分情報を含む要求を、前記測定要求として前記要求先から受信する
ことを特徴とする請求項13に記載の通信装置。
- [15] 前記要求先は、前記第2の要求元部分情報と前記第1の要求先部分情報とが一致する場合は、前記測定応答の送信元が真正の要求元であると判断する場合において、

前記測定応答送信手段は、前記第2の要求元部分情報を含む応答を、前記測定応答として前記要求先に送信する

ことを特徴とする請求項14に記載の通信装置。

[16] 前記通信装置は、さらに、

前記往復遅延時間の測定を開始させるか否かを判定する測定開始判定手段と、
前記往復遅延時間の測定を開始させる場合は、前記往復遅延時間の測定を開始させることを要求する測定開始要求を前記要求先に送信する測定開始要求送信手段と、

前記測定開始要求に対する応答として測定開始応答を前記要求先から受信する測定開始応答受信手段と

を備え、

前記認証手段は、前記測定開始応答を前記要求先から受信した後に、前記要求先との間で認証情報を共有する

ことを特徴とする請求項12に記載の通信装置。

[17] 前記測定開始判定手段は、前記コンテンツデータの受信が終了したか否かを判定し、

前記測定開始要求送信手段は、前記コンテンツデータの受信が終了した場合は、前記測定開始要求を前記要求先に送信する

ことを特徴とする請求項16に記載の通信装置。

[18] 前記通信装置は、さらに、

前記コンテンツデータの送信に使用される鍵を交換する鍵交換手段を備え、

前記測定開始判定手段は、認証してから鍵を交換するまでの間に、前記往復遅延時間が測定されたか否かを判定し、

前記測定開始要求送信手段は、前記往復遅延時間が測定されなかった場合は、前記鍵を交換した後に、前記測定開始要求を前記要求先に送信する

ことを特徴とする請求項16に記載の通信装置。

[19] 前記通信装置は、さらに、

前記往復遅延時間の測定を開始することを通知する測定開始要求を前記要求先

から受信する測定開始要求受信手段と、

前記測定開始要求に対する応答として測定開始応答を前記要求先に送信する測定開始応答送信手段と

を備え、

前記認証手段は、前記測定開始応答を前記要求先に送信した後に、前記要求先との間で認証情報を共有する

ことを特徴とする請求項12に記載の通信装置。

[20] データ通信網を介して相互に接続されている請求項1に記載の通信装置と請求項12に記載の通信装置とを備えることを特徴とする通信システム。

[21] コンテンツデータの送信に対する要求に応答する要求先の通信装置と、前記コンテンツデータの送信を要求する要求元の通信装置との間の通信を制御する通信方法であって、

前記要求先において、前記要求元との間で認証情報を共有する要求先認証ステップと、

前記要求元において、前記要求先との間で認証情報を共有する要求元認証ステップと、

前記要求先において、前記認証情報を使用して生成した測定要求を、前記要求元に送信する測定要求送信ステップと、

前記要求元において、前記要求先で共有されている認証情報を使用して生成された測定要求を、前記要求先から受信する測定要求受信ステップと、

前記要求元において、前記認証情報を使用して生成した測定応答を、前記測定要求に対する応答として前記要求先に折り返し送信する測定応答送信ステップと、

前記要求先において、前記要求元で共有されている認証情報を使用して生成される測定応答を、前記測定要求に対する応答として前記要求元から受信する測定応答受信ステップと、

前記要求先において、前記測定要求を送信してから前記測定応答を受信するまでの時間を、往復遅延時間として測定する往復遅延時間測定手段と、

前記要求先において、前記測定要求を送信する前に、前記測定応答の生成に要

する下準備を要求する測定準備要求を、前記要求元に送信する測定準備要求送信ステップと、

前記要求元において、前記測定要求を受信する前に、前記測定応答の生成に要する下準備を要求する測定準備要求を、前記要求先から受信する測定準備要求受信ステップと、

前記要求先において、前記往復遅延時間の測定後に、前記往復遅延時間が基準値以下であり、前記測定応答が正しいと検証され、かつ前記要求元において前記測定要求が正しいと検証された場合は、前記要求元を前記コンテンツデータの送信先として適格な装置であると判定する判定ステップと

を含むことを特徴とする通信方法。

[22] コンテンツデータの送信に対する要求に応答する通信装置を制御する通信プログラムであって、

前記コンテンツデータの送信を要求する要求元との間で認証情報を共有する認証ステップと、

前記認証情報を使用して生成した測定要求を、前記要求元に送信する測定要求送信ステップと、

前記要求元で共有されている認証情報を使用して生成される測定応答を、前記測定要求に対する応答として前記要求元から受信する測定応答受信ステップと、

前記測定要求を送信してから前記測定応答を受信するまでの時間を、往復遅延時間として測定する往復遅延時間測定ステップと、

前記測定要求を送信する前に、前記測定応答の生成に要する下準備を要求する測定準備要求を、前記要求元に送信する測定準備要求送信ステップと、

前記往復遅延時間の測定後に、前記往復遅延時間が基準値以下であり、前記測定応答が正しいと検証され、かつ前記要求元において前記測定要求が正しいと検証されたことを確認した場合は、前記要求元が前記コンテンツデータの送信先として適格な装置であると判定する判定ステップと

をコンピュータシステムに実行させることを特徴とする通信プログラム。

[23] コンテンツデータの送信を要求する通信装置を制御する通信プログラムであって、

前記コンテンツデータの送信に対する要求に応答する要求先との間で認証情報を共有する認証ステップと、

前記要求先で共有されている認証情報を使用して生成された測定要求を、前記要求先から受信する測定要求受信ステップと、

前記認証情報を使用して生成した測定応答を、前記測定要求に対する応答として前記要求先に折り返し送信する測定応答送信ステップと、

前記測定要求を受信する前に、前記測定応答の生成に要する下準備を要求する測定準備要求を、前記要求先から受信する測定準備要求受信ステップと、

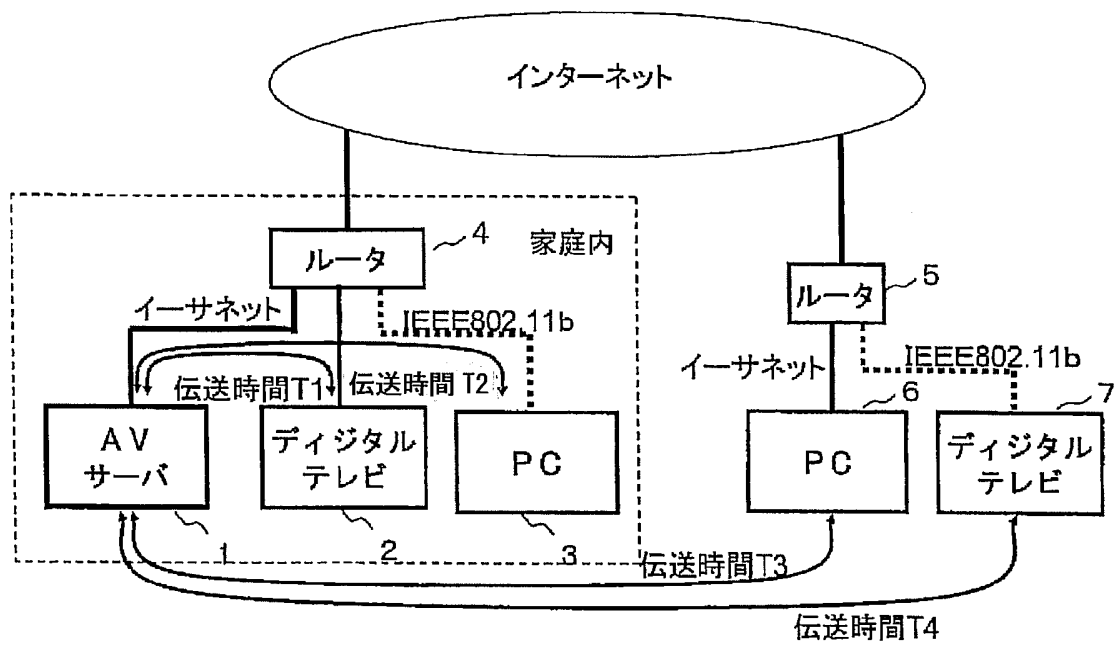
前記測定要求が正しいか検証する判定ステップと

をコンピュータシステムに実行させることを特徴とする通信プログラム。

[24] 請求項22に記載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。

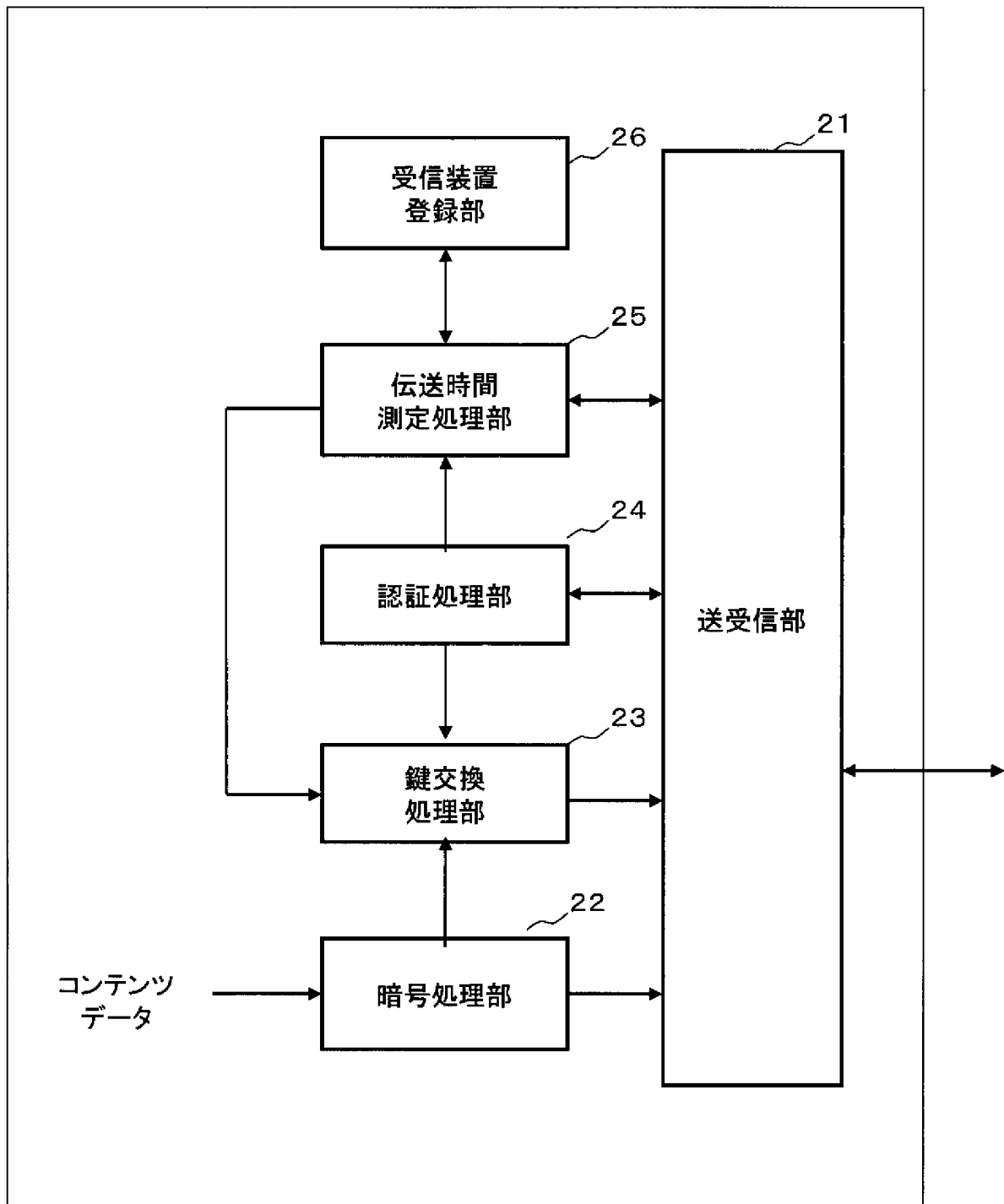
[25] 請求項23に記載の通信プログラムを記録したコンピュータ読み取り可能な記録媒体。

[図1]

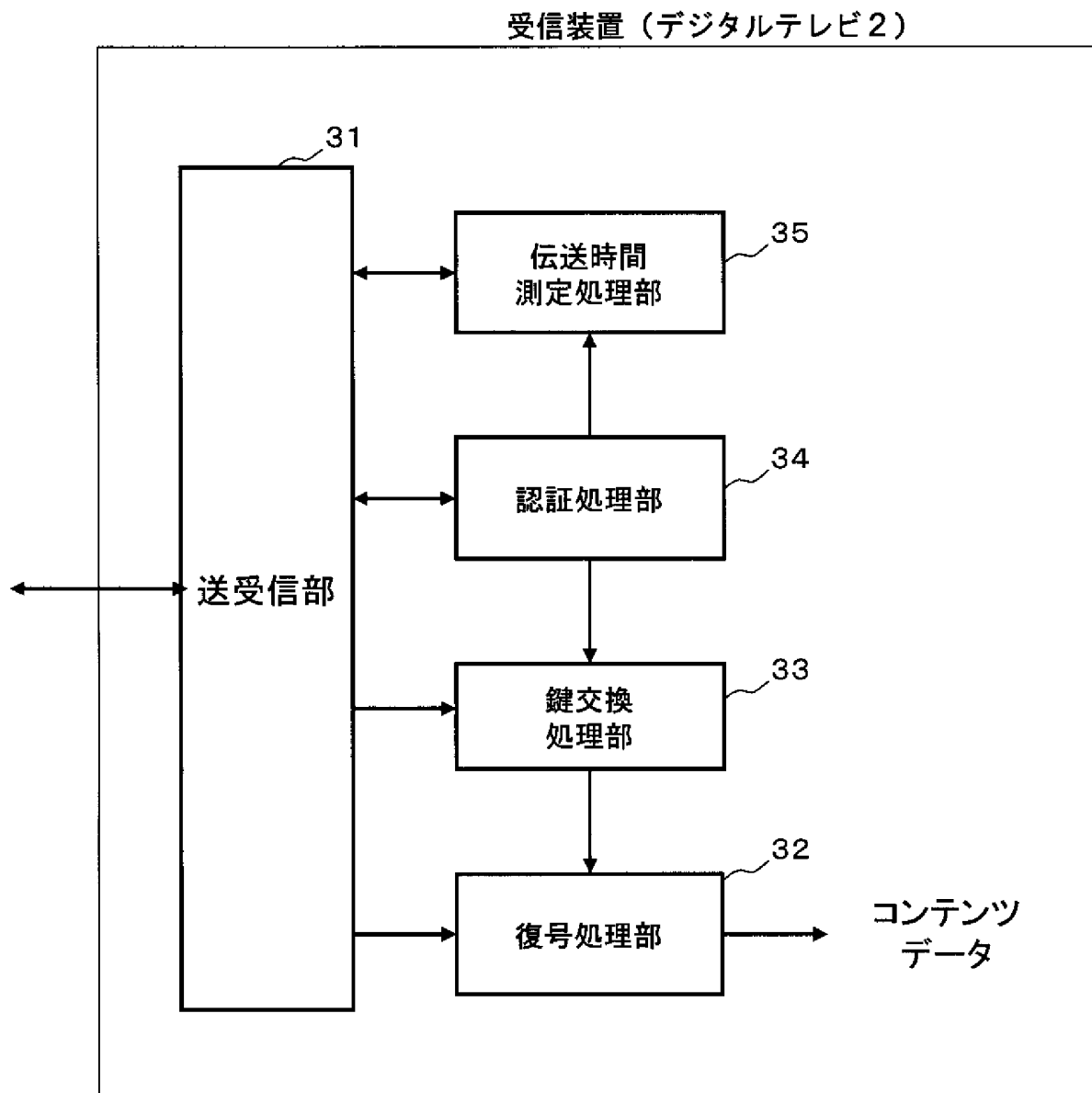


[図2]

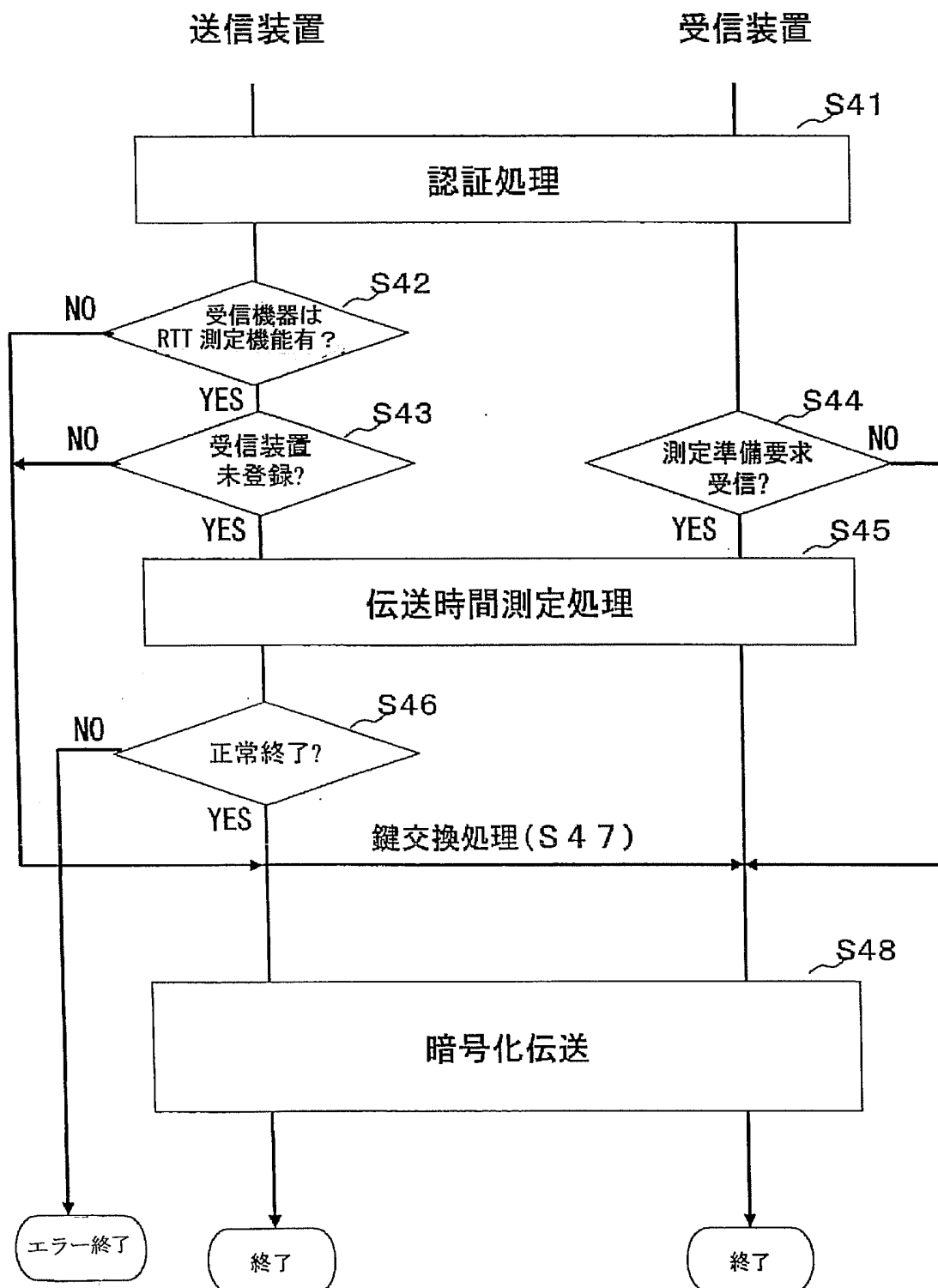
送信装置（AVサーバ1）



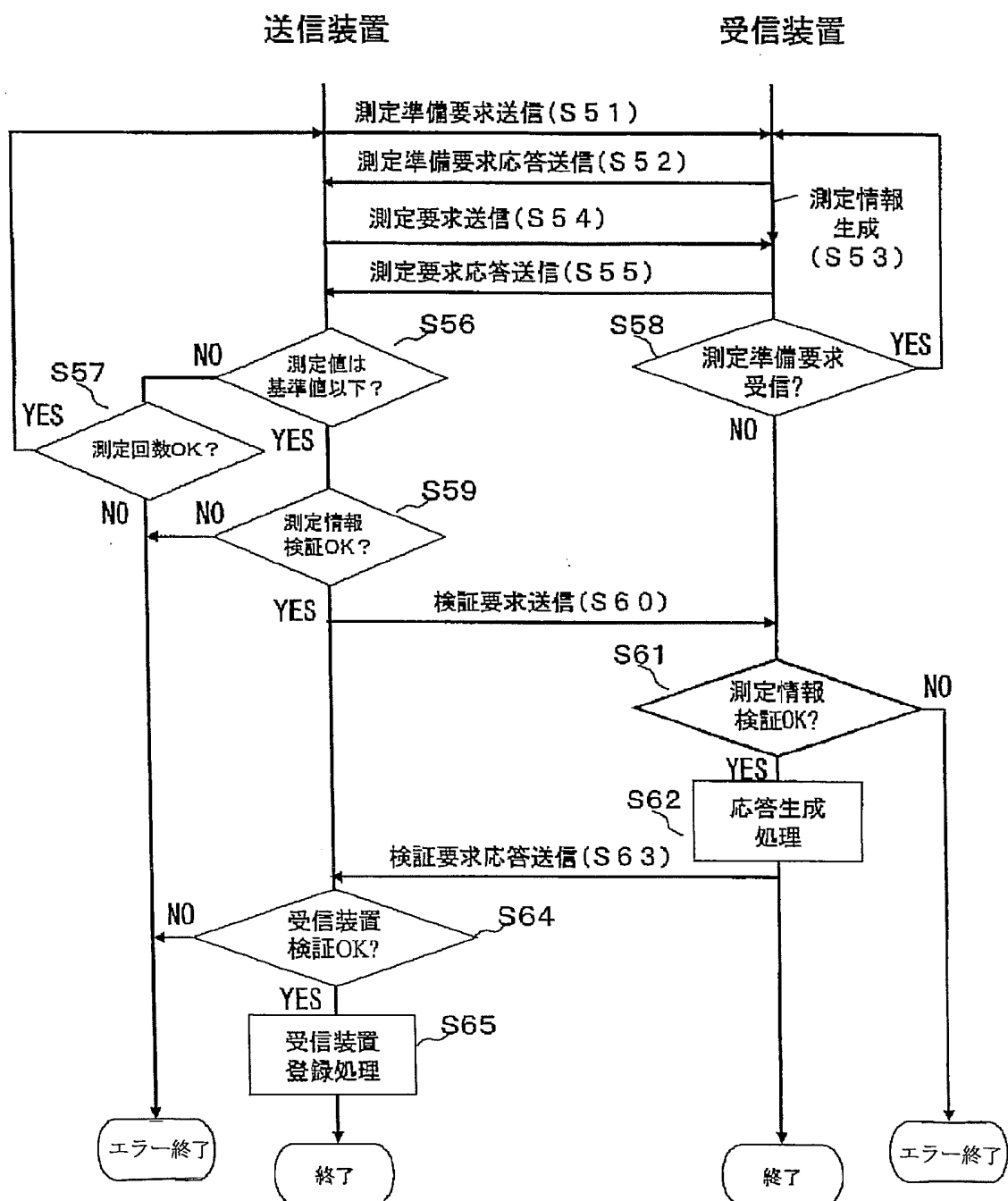
[図3]



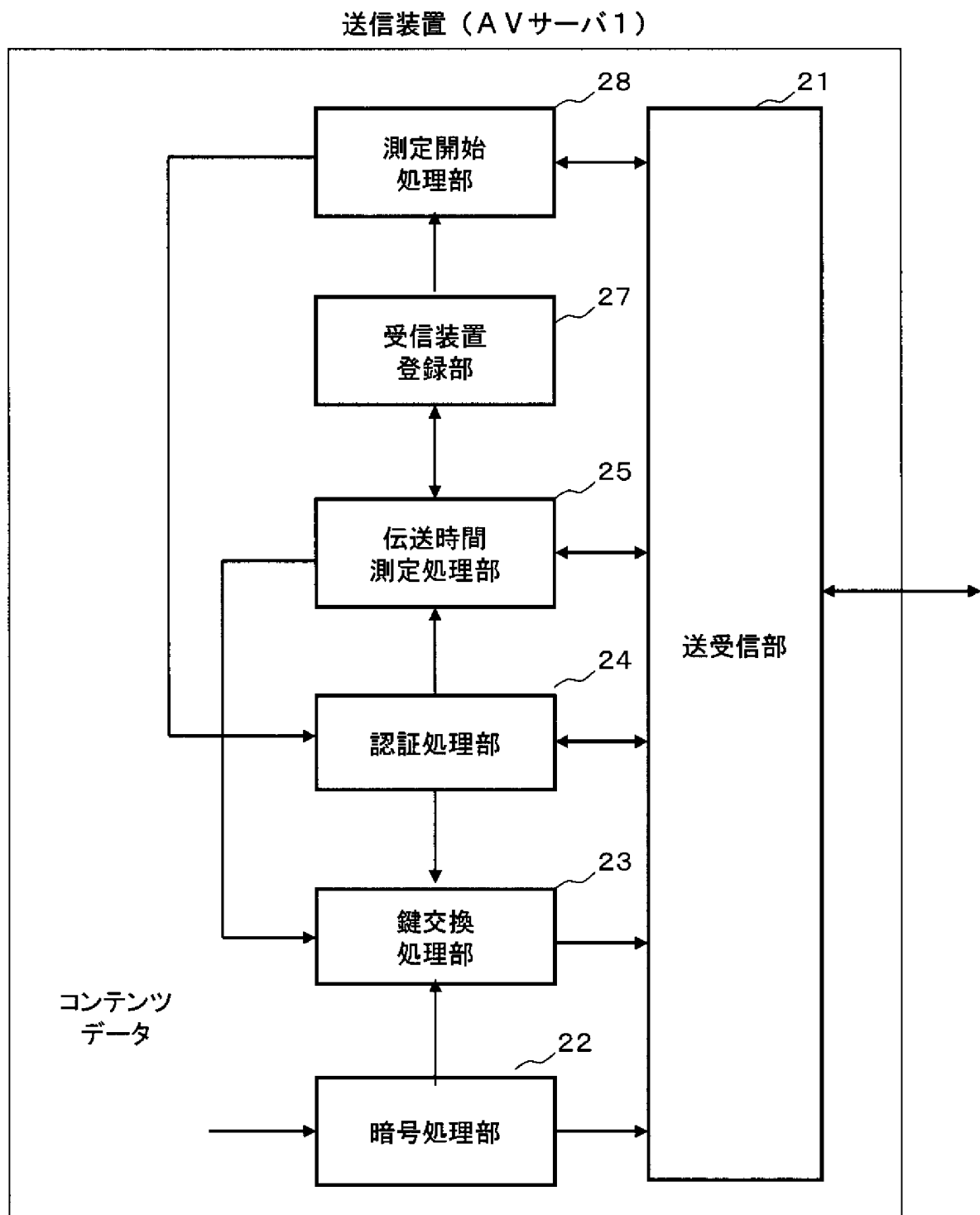
[図4]



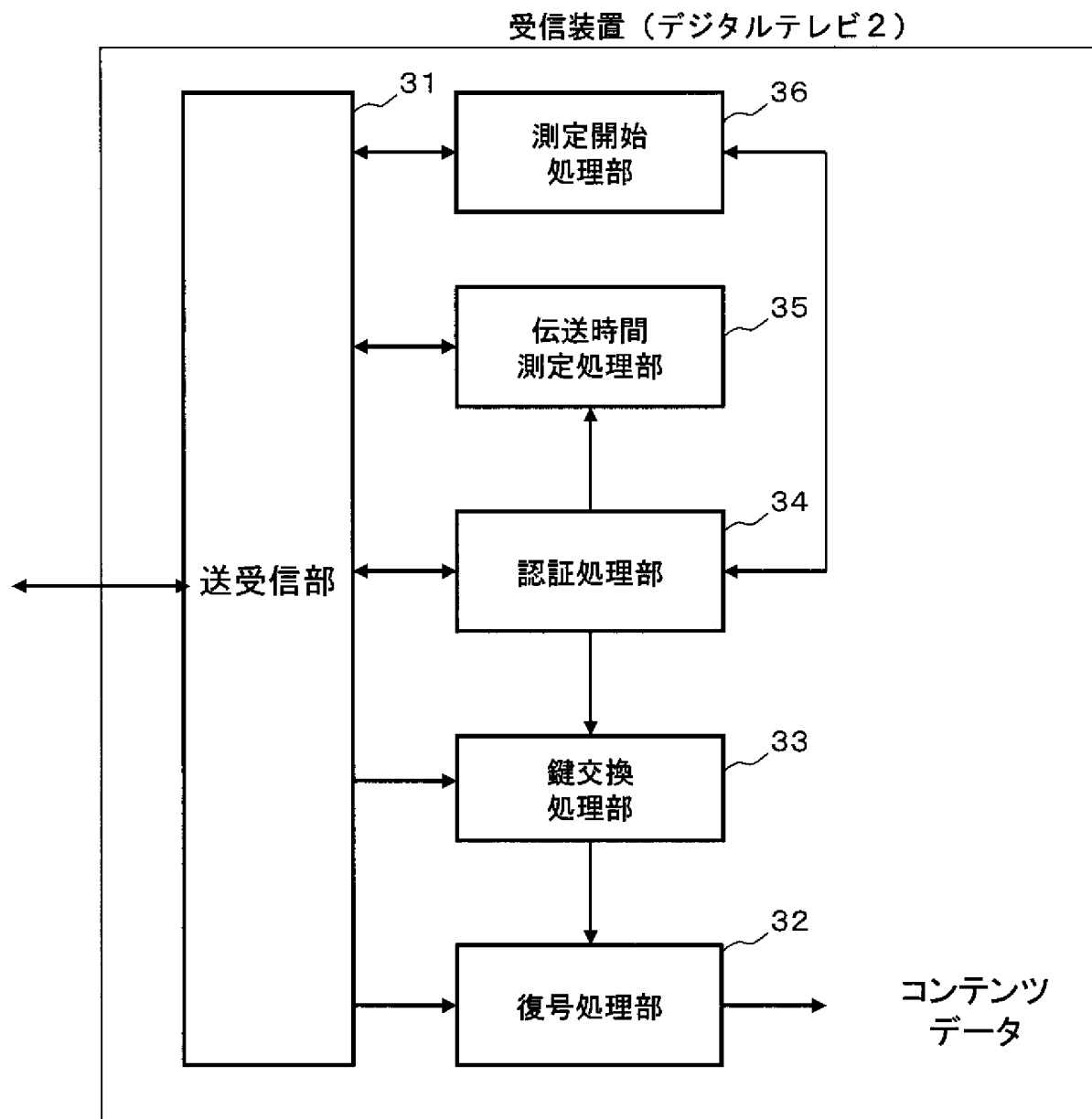
[図5]



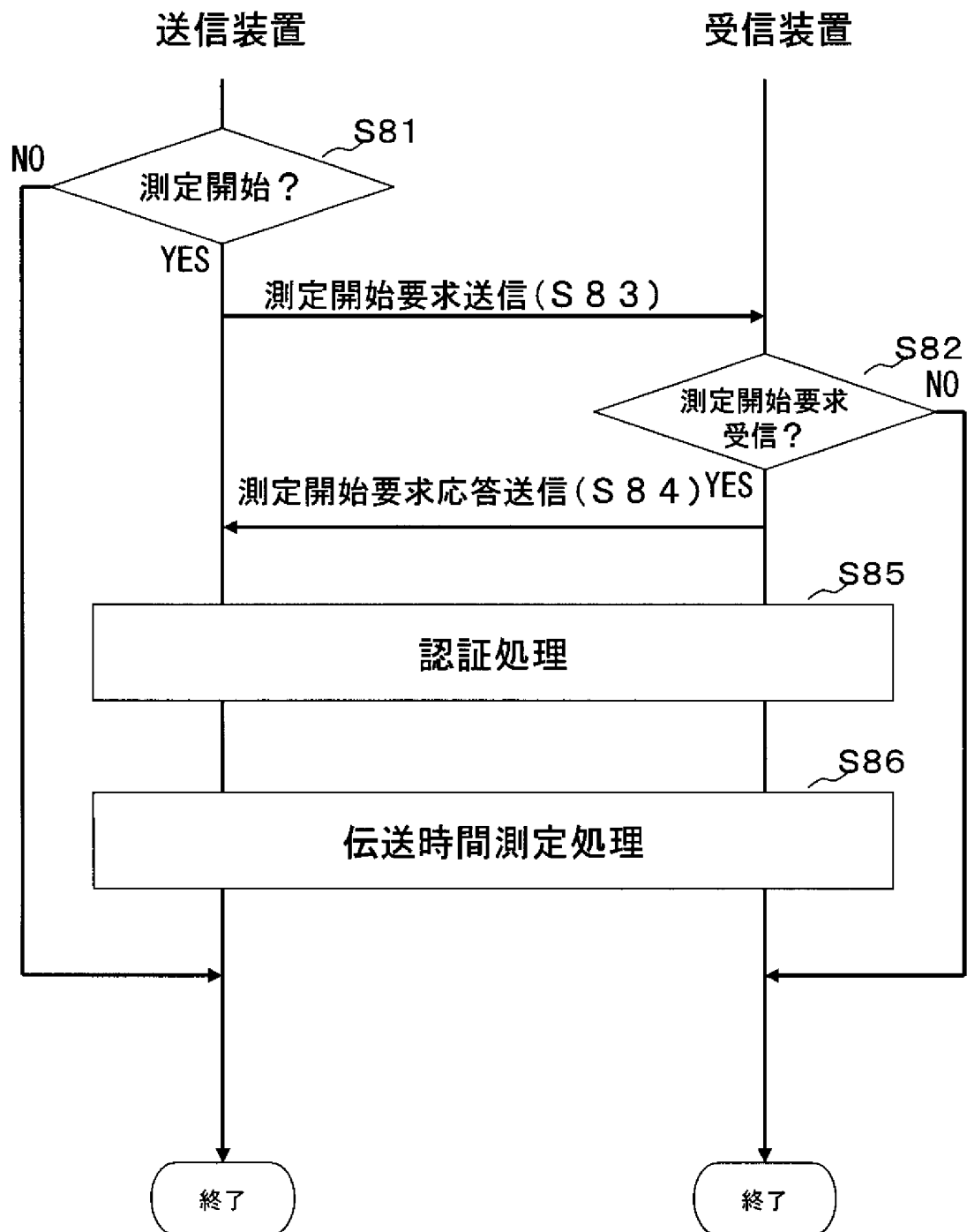
[図6]



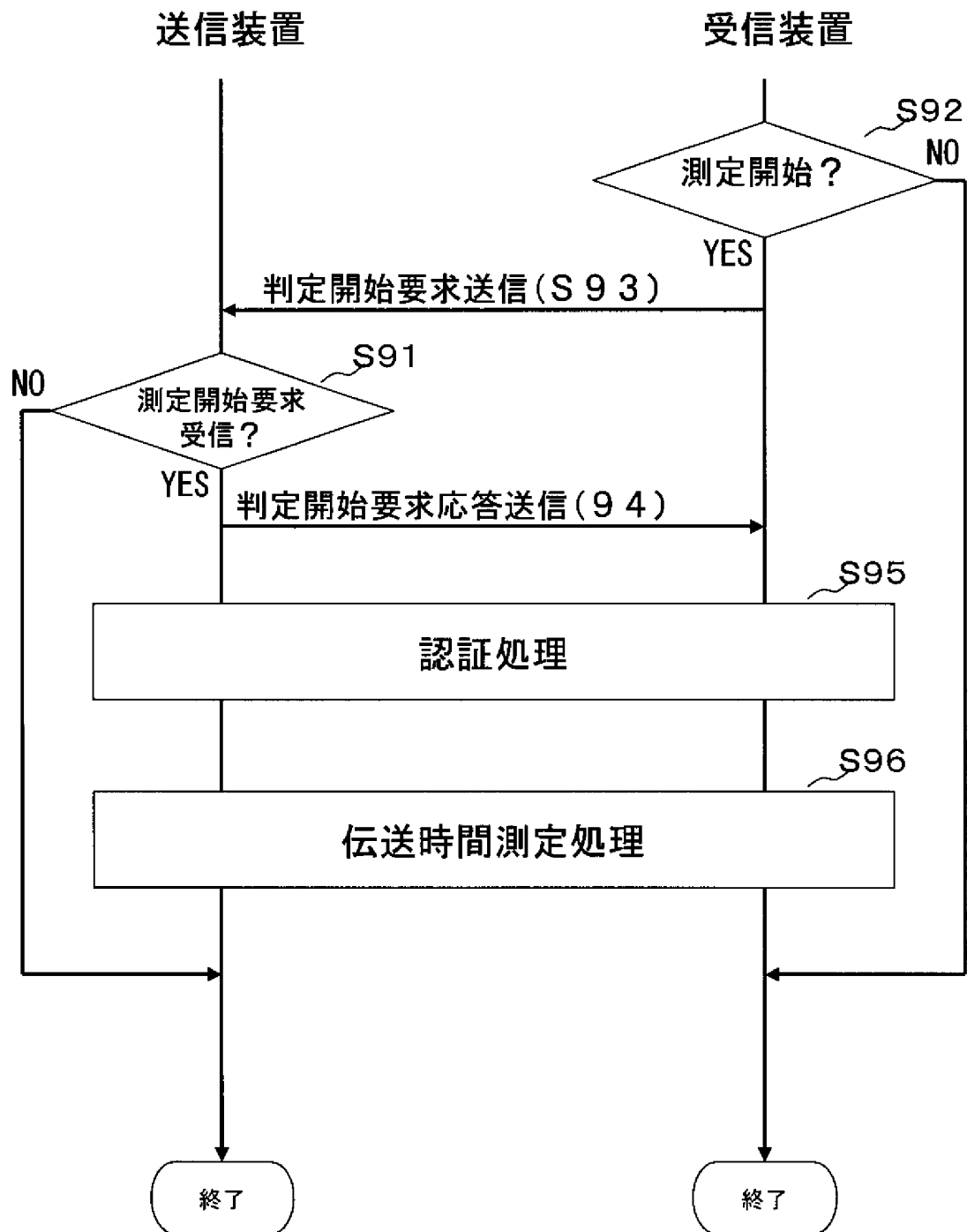
[図7]



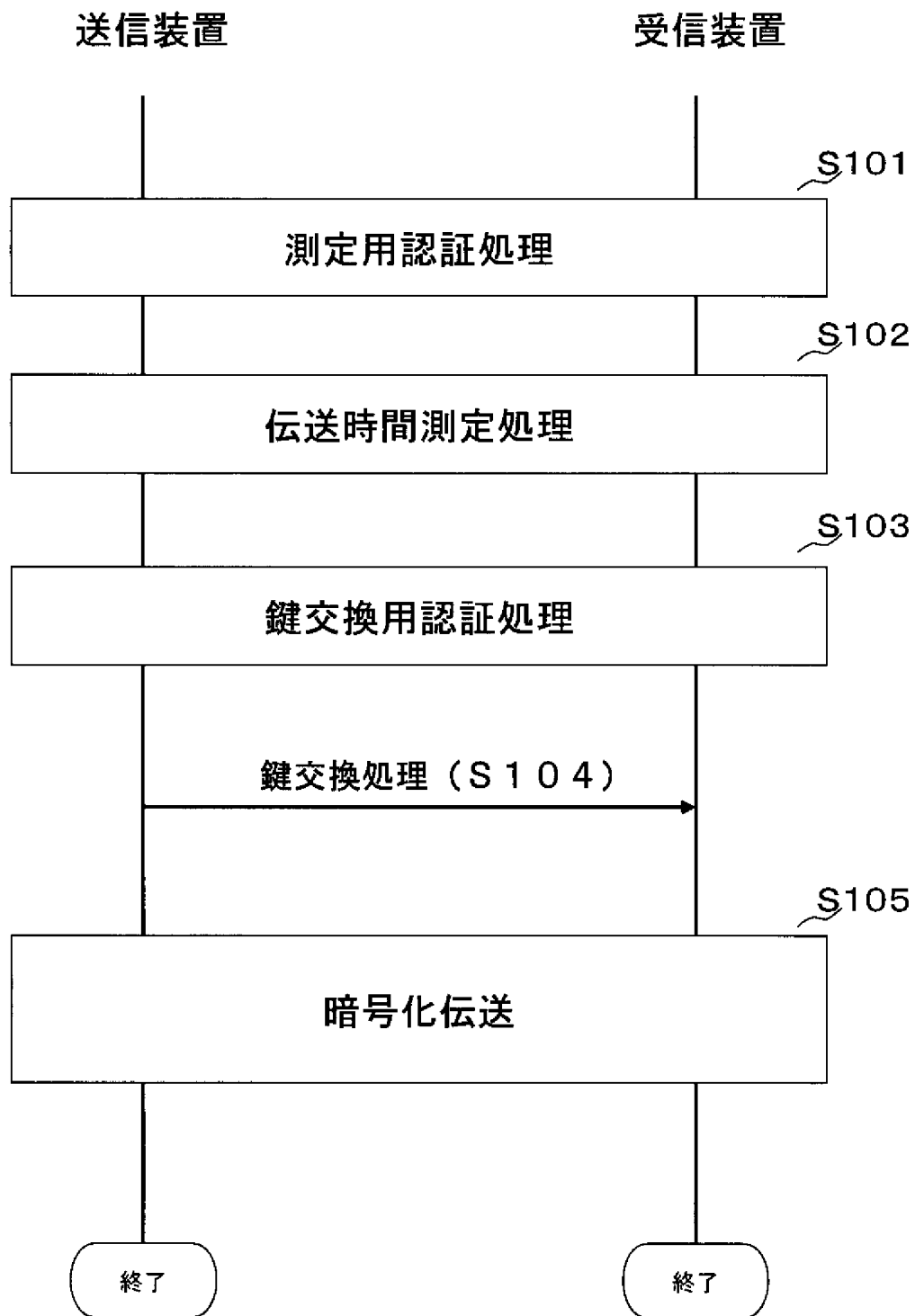
[図8]



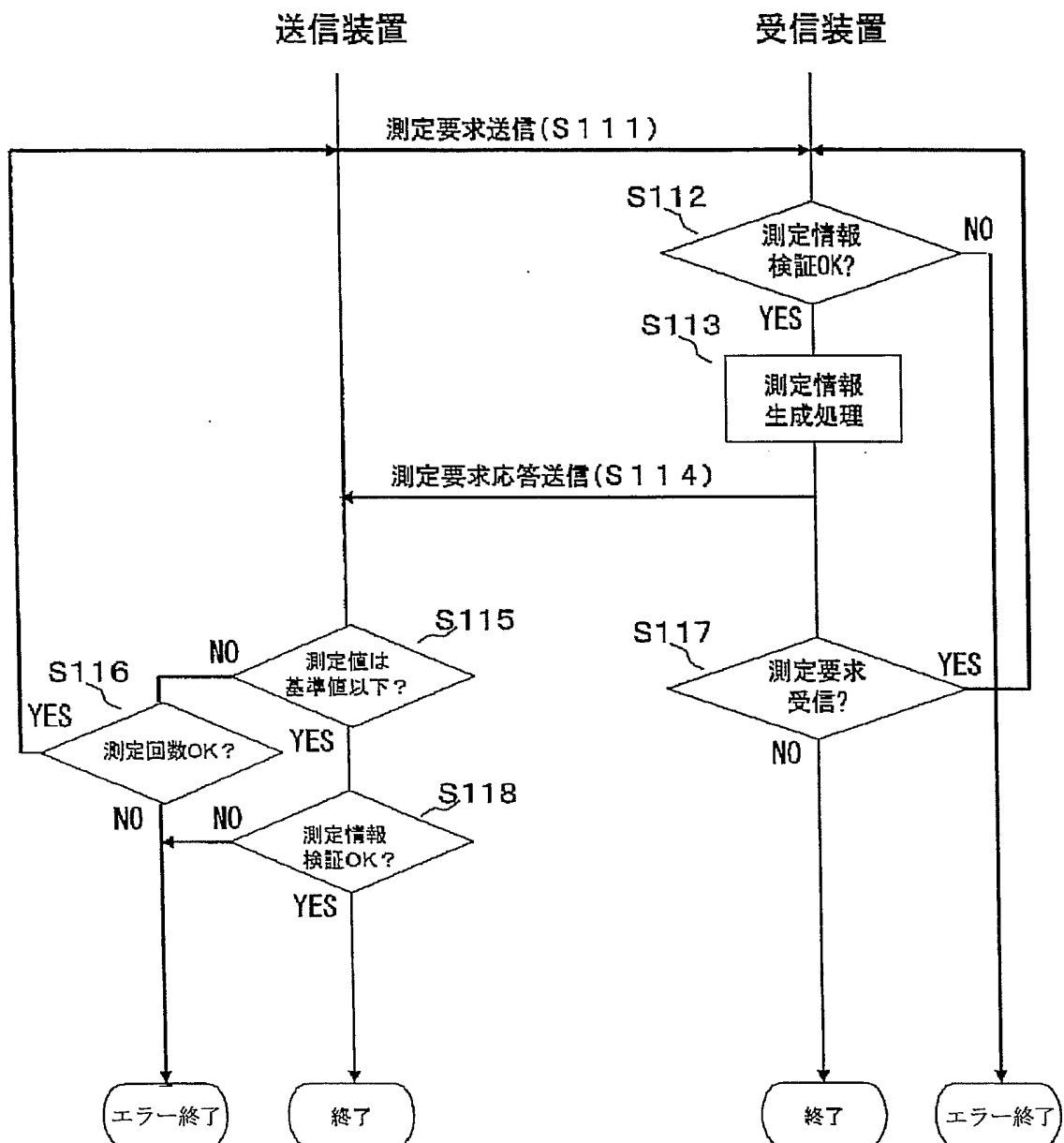
[図9]



[図10]



[図11]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/016335

A. CLASSIFICATION OF SUBJECT MATTER H04L9/32 (2006.01), G09C1/00 (2006.01), H04L12/28 (2006.01), H04L12/56 (2006.01) 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) H04L9/32 (2006.01), G09C1/00 (2006.01), H04L12/28 (2006.01), H04L12/56 (2006.01) Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005 Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005 Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	"DRM Dai 2 Bu Network o Zentei ni Secure no Wa o Hirogeru", Nikkei Electronics, 5 Gatsu 10 Kago, No.873, 10 May, 2004 (10.05.04), CS-ND-2004-01642-003, pages 88 to 95	1-8,12-17, 20-25 9-11,18,19
Y A	JP 2004-194295 A (Matsushita Electric Industrial Co., Ltd.), 08 July, 2004 (08.07.04), Full text; all drawings & WO 2004/036840 A	1-8,12-17, 20-25 9-11,18,19
Y	JP 2002-108819 A (Toshiba Corp.), 12 April, 2002 (12.04.02), Par. Nos. [0006], [0010], [0011]; Figs. 1 to 7 (Family: none)	5, 6
☒ 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 22 November, 2005 (22.11.05)		Date of mailing of the international search report 06 December, 2005 (06.12.05)
Name and mailing address of the ISA/ Japanese Patent Office		Authorized officer
Facsimile No.		Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/016335

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 05-284499 A (NEC Corp.), 29 October, 1993 (29.10.93), Par. Nos. [0011], [0012]; Fig. 1 (Family: none)	17
A	JP 2001-285283 A (Toshiba Corp.), 12 October, 2001 (12.10.01), Full text; all drawings (Family: none)	1-25

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl. **H04L9/32** (2006.01), **G09C1/00** (2006.01), **H04L12/28** (2006.01), **H04L12/56** (2006.01)

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. **H04L9/32** (2006.01), **G09C1/00** (2006.01), **H04L12/28** (2006.01), **H04L12/56** (2006.01)

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	1971-2005年
日本国実用新案登録公報	1996-2005年
日本国登録実用新案公報	1994-2005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)

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 A	“DRM第2部 ネットワークを前提にセキュアの輪を広げる”, 日経エレクトロニクス, 5月10日号, 第873号, 2004.05.10, CS-ND-2004-01642-003, p. 88-95	1-8, 12-17, 20 -25 9-11, 18, 19
Y A	JP 2004-194295 A (松下電器産業株式会社) 2004.07.08, 全文, 全図 & WO 2004/036840 A	1-8, 12-17, 20 -25 9-11, 18, 19

☒ 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

の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

22.11.2005

国際調査報告の発送日

06.12.2005

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
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)

青木 重徳

5S

4229

電話番号 03-3581-1101 内線 3546

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 2002-108819 A (株式会社東芝) 2002. 04. 12, 第【0006】段落, 第【0010】, 【0011】段落, 図1-7 (ファミリーなし)	5, 6
Y	JP 05-284499 A (日本電気株式会社) 1993. 10. 29, 第【0011】, 【0012】段落, 図1 (ファミリーなし)	17
A	JP 2001-285283 A (株式会社東芝) 2001. 10. 12, 全文, 全図 (ファミリーなし)	1-25