(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2009 年7 月23 日 (23.07.2009)

PCT

(10) 国際公開番号
WO 2009/091036 A1

(51) 国際特許分類:
G06F 21/20 (2006.01) *H04L 9/32* (2006.01)
G09C 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2009/050558

(22) 国際出願日: 2009 年1 月16 日 (16.01.2009)

(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2008-009769 2008 年1 月18 日 (18.01.2008) JP

(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 Kanagawa (JP). 日本放送協会 (NIPPON HOSO KYOKAI) [JP/JP]; 〒1508001 東京都渋谷区神南二丁目２番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 榊原 宏紀 (SAKAKIHARA, Hironori). 本田 文雄 (HONDA, Fumio). 岩松 昇 (IWAMATSU, Noboru). 石川 清彦 (ISHIKAWA, Kiyohiko). 砂崎 俊二 (SUNASAKI, Syunji). 藤井 亜里砂 (FUJII, Arisa).

(74) 代理人: 河野 登夫 (KOHNO, Takao); 〒5400035 大阪府大阪市中央区釣鐘町二丁目４番３号 河野特許事務所 Osaka (JP).

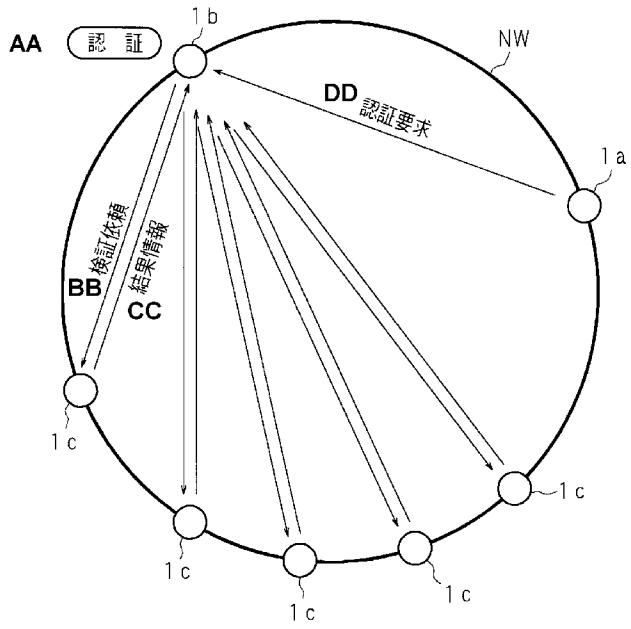
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE,

[続葉有]

(54) **Title:** AUTHENTICATION SYSTEM, AUTHENTICATION DEVICE, AND COMPUTER PROGRAM

(54) 発明の名称: 認証システム、認証装置及びコンピュータプログラム

[図7]



AA AUTHENTICATION
BB VERIFICATION REQUEST
CC RESULT INFORMATION
DD AUTHENTICATION REQUEST

(57) Abstract: Disclosed are an authentication system for alleviating a processing load and communication load on a management node device for managing all node devices when authentication is performed between the node devices in a Peer-to-Peer communication system for relaying a message between the node devices with one another, an authentication device, and a computer program. A node to be authenticated (1a) requests the authentication by transmitting information on the authentication to an authentication node (1b). The authentication node (1b) requests a plurality of selected verification nodes (1c, 1c,…) to verify the authentication information.The authentication node (1b) then authenticates the node to be authenticated (1a) on the basis of the results of the verification received from each of the verification nodes (1c, 1c,…) and a weighted value indicating the reliability of each verification by the verification nodes (1c, 1c,…).

(57) 要約: ノード装置間で相互にメッセージを中継するＰｅｅｒ－ｔｏ－Ｐｅｅｒ型の通信システムにおいて、ノード装置間で認証を行う場合に、全てのノード装置を管理する管理用ノード装置に関する処理負荷及び通信負荷を軽減する認証システム、認証装置及びコンピュータプログラムを提供する。 被認証ノードｌａが、認証ノードｌｂへ認証情報を送信することで認証を要求し、認証ノードｌｂは、選択した複数の検証ノードｌｃ，ｌｃ，…に認証情報の検証を依頼する。そして認証ノードｌｂは、各検証ノードｌｃ，ｌｃ，…から受信した検証の結果及び各検証ノ

[続葉有]

WO 2009/091036 A1

DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, 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

ードｌｃ，１ｃ，…の検証に対する夫々の信頼性を示す加重値に基づいて、認証ノードｌａを認証する。

明 細 書

認証システム、認証装置及びコンピュータプログラム

技術分野

[0001] 本発明は、通信網を介して通信することが可能な複数のノード装置を備え、一のノード装置の認証情報の正当性を、他の複数のノード装置が記録している検証情報に基づいて検証することで前記一のノード装置を認証する認証システム、該認証システムにて用いられる認証装置、及び該認証装置を実現するコンピュータプログラムに関する。

背景技術

[0002] クライアントーサーバ(以下、C－Sという)型とは異なり、クライアント装置(ノード装置)間で相互にメッセージを中継するPeer－to－Peer(以下、P2Pという)型の通信システムが注目されている。P2P型の通信システムでは、ノード装置間でファイルの検索、転送等の通信処理を行うため、C－S型の様に特定のサーバ装置の処理負荷が増大するということがないという利点がある。

[0003] サーバ装置からファイルを配信するC－S型の通信システムでは、配信先のクライアント装置に対し、サーバ装置が認証処理を行うことにより、著作権保護、秘密保護等の保護を行い、ファイルの不正な流出を防止している。P2P型の通信システムでは、その利点を活かすため、ノード装置間での認証を行い、ファイルの不正な流出を防止する認証システムの構築が必要となる。

[0004] 図1は、従来の認証システムの構成を概念的に示す模式図である。図1は、P2P型の通信システムを構成する通信網及び複数のノード装置を示している。各ノード装置には、識別情報としてノードIDが付与されている。ノードIDは、例えば通信網への接続時に、全てのノード装置のノードIDを管理する管理用ノード装置から付与される。また各ノード装置は、論理空間であるハッシュ空間上におけるノード装置の位置を示す位置情報としてピア情報を保持している。ピア情報は、ノード装置に付与されているノードIDをハッシュ関数で処理することにより導出されるハッシュ値であり、ピア情報により、複数のノード装置を例えば160bitのハッシュ空間上にランダム性を持って

一様に分布させることが可能となる。例えばノード装置AのノードIDをIDA とすると、ノード装置Aのピア情報HA はハッシュ関数SHA－1を用いた下記の式(a)により、001．．100等の2進数で示される160bitの値として導出される。

[0005] HA ＝SHA－1(IDA) …式(a)

但し、HA :ノード装置Aのピア情報

IDA :ノード装置AのノードID

SHA－1() :ハッシュ関数

[0006] P2P型の認証システムでは、下記の式(b)にて導出されるノード装置Aに係る情報HA+αを用いて認証処理を行う。図1では、ノード装置X(以降、認証ノードXという)がノード装置A(以降、被認証ノードAという)を認証する処理を模式的に示している。例えば被認証ノードAが通信網に接続した際に、管理用ノード装置は、被認証ノードAに対してノードIDを付与し、被認証ノードAの認証に用いる認証情報を、ノードIDに基づき選択した複数のノード装置Y1, Y2, …, Y10(以降、検証ノードY1, Y2, …, Y10という)へ夫々送信する。そして複数の検証ノードY1, Y2, …, Y10は、受信した被認証ノードAの認証情報を、被認証ノードAの認証情報の検証に用いる検証情報として記録する。なお管理用ノード装置は、式(b)にて導出される被認証ノードAに係る情報が示すハッシュ空間上の位置に近い位置を示すピア情報に係る複数のノード装置を、被認証ノードAのピア情報の送信先として選択する。ここでハッシュ空間上の位置が近いとは、例えば互いのハッシュ値の上位ビットが一致している状況である。

[0007] HA+α＝SHA－1(IDA+α) …式(b)

但し、HA+α :ノード装置Aに係る情報

IDA :ノード装置AのノードID

SHA－1() :ハッシュ関数

α :定数

[0008] 被認証ノードAは、認証ノードXに対して認証を要求する場合、自らのノードID及び認証情報を含む認証要求を認証ノードXへ送信する。認証ノードXは、被認証ノードのノードIDに基づいて被認証ノードに係る情報を上記の式(b)にて導出し、導出した

被認証ノードに係る情報にて示される論理空間上の位置に近いピア情報に係る複数のノード装置を選択する。このとき検証ノードY1，Y2，…，Y10が選択されたものとする。認証ノードXは、選択した検証ノードY1，Y2，…，Y10へ、被認証ノードAの認証情報の正当性の検証を依頼する検証依頼を送信する。検証依頼には、被認証ノードAの認証情報が含まれている。検証ノードY1，Y2，…，Y10は、被認証ノードAに係る検証情報の有無の判定、及び検証情報を有する場合に、認証情報及び検証情報の照合により、認証情報の正当性を検証する。そして検証ノードY1，Y2，…，Y10は、検証した結果を示す結果情報を認証ノードXへ送信する。

[0009] 認証ノードXは、検証ノードY1，Y2，…，Y10から受信した夫々の結果情報に基づいて、被認証ノードAを認証し、認証に成功した場合、ファイルの送信等のサービスを提供する。なお受信した複数の結果情報にて示される検証の結果が一致していない場合、即ち認証情報の正当性の判定結果に差異がある場合が生じ得る。例えば一部の検証ノードが有している検証情報が古い場合、検証依頼に対して不正なノード装置が結果情報を返した場合等の状況である。検証の結果が一致しない場合、認証ノードXは、認証情報を管理用ノード装置へ送信して認証情報の正当性の判定を依頼したり、また結果情報による判定結果に基づく多数決を行うことにより、認証の成否を判定する。この様なP2P型の認証システムは、例えば特許文献1に開示されている。

特許文献1：特開2006－185171号公報

発明の開示

発明が解決しようとする課題

[0010] しかしながら従来のP2P型の認証システムにおいて、認証を行うノード装置が依頼した検証の結果が一致しない場合、管理用ノード装置に認証情報の正当性の判定を依頼する方法では、特定の管理用ノード装置の処理負荷が増大することになり、P2P型の利点を損なうという問題がある。

[0011] また多数決にて判定する方法では、例えば正当性の判定を依頼したノード装置に古い検証情報を有するノード装置が多数含まれていると誤判定を行うことになるので、正確性に欠けるという問題がある。

[0012] 本発明は斯かる事情に鑑みてなされたものであり、検証を依頼した複数のノード装置に対する信頼性を示す加重値を加味して結果情報に基づく認証を行う。これにより管理用ノード装置の処理負荷を増大させることなく、また正確性を向上させることが可能な認証システム、該認証システムにて用いられる認証装置、及び該認証装置を実現するコンピュータプログラムの提供を目的とする。

課題を解決するための手段

[0013] 第1の認証システムは、通信網を介して相互に通信することが可能な複数のノード装置を備え、一のノード装置の認証情報の正当性を、他の複数のノード装置が記録している検証情報に基づいて検証することで前記一のノード装置を認証する認証システムにおいて、第1のノード装置は、自らの認証情報を第2のノード装置へ送信する手段を備え、前記第2のノード装置は、受信した認証情報の正当性の検証を依頼する複数の第3のノード装置を選択する手段と、選択した複数の第3のノード装置へ夫々認証情報を送信する手段とを備え、前記第3のノード装置の夫々は、前記第1のノード装置の認証情報の正当性の検証に用いる検証情報を記録する手段と、受信した認証情報及び記録している検証情報に基づいて、認証情報の正当性を検証する手段と、検証した結果を示す結果情報を前記第2のノード装置へ送信する手段とを備え、前記第2のノード装置は、更に、前記複数の第3のノード装置の検証に対する夫々の信頼性を示す加重値を導出する加重値導出手段と、前記複数の第3のノード装置から受信した夫々の結果情報及び夫々の加重値に基づいて、前記第1のノード装置を認証する手段とを備えることを要件とする。

[0014] 第2の認証システムは、通信網を介して相互に通信することが可能な複数のノード装置を備え、一のノード装置の認証情報の正当性を、他の複数のノード装置が記録している検証情報に基づいて検証することで前記一のノード装置を認証する認証システムにおいて、第1のノード装置は、自らの認証情報を第2のノード装置へ送信する手段を備え、前記第2のノード装置は、前記第1のノード装置及び第2のノード装置以外の複数のノード装置が、前記第1のノード装置の認証情報の正当性を検証する場合の検証に対する夫々の信頼性を示す加重値を導出する加重値導出手段と、導出した加重値に基づいて、加重値を導出した複数のノード装置から、認証情報の正

当性の検証を依頼する複数の第3のノード装置を選択する手段と、選択した複数の第3のノード装置へ夫々認証情報を送信する手段とを備え、前記各第3のノード装置の夫々は、前記第1のノード装置の認証情報の正当性の検証に用いる検証情報を記録する手段と、受信した認証情報及び記録している検証情報に基づいて、認証情報の正当性を検証する手段と、検証した結果を示す結果情報を前記第2のノード装置へ送信する手段とを備え、前記第2のノード装置は、更に、前記複数の第3のノード装置から受信した夫々の結果情報及び前記加重値導出手段により導出した前記複数の第3のノード装置に対する加重値に基づいて、前記第1のノード装置を認証する手段とを備えることを要件とする。

[0015] 第3の認証システムは、第1又は第2の認証システムにおいて、前記第2のノード装置は、前記個々のノード装置を識別する識別情報及び所定の関数に基づいて、前記各ノード装置の論理空間上の位置を示す位置情報を導出する手段を更に備え、前記加重値導出手段は、位置情報から求まる前記第1のノード装置からの距離に基づいて夫々の加重値を導出する様に構成してあることを要件とする。

[0016] 第4の認証システムは、第1乃至第3のいずれかの認証システムにおいて、前記加重値導出手段は、前記第3のノード装置の夫々の検証の履歴に基づいて加重値を導出する様に構成してあることを要件とする。

[0017] 第5の認証システムは、第1乃至第4のいずれかの認証システムにおいて、前記各ノード装置に関する情報を管理する管理用ノード装置を更に備え、該管理用ノード装置は、前記各ノード装置について、個々のノード装置を識別する識別情報及び認証情報を記録する手段と、前記各ノード装置の識別情報及び所定の関数に基づいて、前記各ノード装置の論理空間上の位置を示す位置情報を導出する手段と、導出した位置情報から求まる一のノード装置から他の各ノード装置までの夫々の論理空間上の距離に基づき、前記一のノード装置の認証情報を送信する複数のノード装置を選択する手段と、選択した前記複数のノード装置へ、前記一のノード装置の認証情報を検証情報として送信する手段とを備えることを要件とする。

[0018] 第6の認証システムは、第5の認証システムにおいて、前記第2のノード装置は、更に、検証情報が正当でないと判定した前記第3のノード装置に対して導出した加重

値が所定値以上であるか否かを判定する手段と、加重値が所定値以上であると判定した場合に、当該加重値に係る前記第3のノード装置を示す情報を、前記管理用ノード装置へ送信する手段とを備えることを要件とする。

[0019] 第7の認証システムは、第5又は第6の認証システムにおいて、前記一のノード装置は、更に、自らの検証情報の再送信を要求する再送信要求を前記管理用ノード装置へ送信する手段を備え、前記管理用ノード装置は、更に、受信した再送信要求の送信元のノード装置の認証情報を、論理空間上の距離に基づいて選択された複数のノード装置へ、前記一のノード装置の検証情報として送信する手段を備えることを要件とする。

[0020] 第8の認証システムは、第1乃至第7のいずれかの認証システムにおいて、前記複数のノード装置へ放送に係る放送情報を送信する放送装置を更に備え、前記第2のノード装置は、更に、認証に成功した前記第1のノード装置へ、該第1のノード装置が受信した放送情報の欠落箇所を送信する手段を備えることを要件とする。

[0021] 第9の認証装置は、複数のノード装置との相互の通信を媒介する通信網に接続し、一のノード装置の認証情報の正当性を、他の複数のノード装置に検証を依頼することで前記一のノード装置を認証する認証装置において、前記一のノード装置から、該一のノード装置の認証情報を受信する手段と、受信した認証情報の正当性の検証を依頼する複数の他のノード装置を選択する手段と、選択した複数の他のノード装置へ夫々認証情報を送信する手段と、前記他のノード装置の夫々から、認証情報に基づく検証結果を示す結果情報を受信する手段と、前記他のノード装置夫々の検証に対する夫々の信頼性を示す加重値を導出する手段と、受信した夫々の結果情報及び夫々の加重値に基づいて、前記一のノード装置を認証する手段とを備えることを要件とする。

[0022] 第10のコンピュータプログラムは、複数のノード装置との相互の通信を媒介する通信網に接続してあるコンピュータに、一のノード装置の認証情報の正当性を、他の複数のノード装置に検証を依頼することで前記一のノード装置を認証させるコンピュータプログラムにおいて、コンピュータに、前記一のノード装置から、該一のノード装置の認証情報を受信した場合に、受信した認証情報の正当性の検証を依頼する複数

の他のノード装置を選択させる手順と、選択した複数の他のノード装置へ夫々認証情報を送信させる手順と、前記他のノード装置の夫々から、認証情報に基づく検証結果を示す結果情報を受信したときに、前記他のノード装置夫々の検証に対する夫々の信頼性を示す加重値を導出させる手順と、受信した夫々の結果情報及び夫々の加重値に基づいて、前記一のノード装置を認証させる手順とを実行させることを要件とする。

[0023] 第1及び第5の認証システム、第9の認証装置並びに第10のコンピュータプログラムでは、ノード装置間で認証を行うので、特定の管理用ノード装置の処理負荷の増大を招くことが無く、信頼性を加味して認証を行うので、単なる多数決による認証より正確性を向上させることが可能である。

[0024] 第2の認証システムでは、信頼性の高い第3のノード装置に検証を依頼して、正確性を向上させることが可能である。

[0025] 第3及び第4の認証システムでは、認証の正確性を向上させることが可能である。

[0026] 第6の認証システムでは、正当でないと判定した第3のノード装置を不正等の可能性があるノード装置として、管理用ノード装置にて管理するが、信頼性が高いと見なしたノード装置のみを管理することにより、管理用ノード装置の処理負荷の増大を抑止することが可能である。

[0027] 第7の認証システムでは、例えば認証に失敗した場合に、認証を依頼したノード装置が、管理用ノード装置に対して自らの検証情報の再配布を依頼することにより、新たな状態で再度認証を行うことが可能となる。

[0028] 第8の認証システムでは、例えば放送の受信に適用した場合で、欠落が生じたときに、放送装置に放送情報の再送信を依頼するのではなく、ノード装置間で相互補完を行うことが可能となる。

発明の効果

[0029] 本願は、通信網を介して相互に接続する複数のノード装置を用い、一のノード装置の認証情報の正当性を、他の複数のノード装置が記録している検証情報に基づいて検証する内容を開示する。第1のノード装置は、自らの認証情報を第2のノード装置へ送信する。第2のノード装置は、受信した認証情報の正当性の検証を依頼する複

数の第3のノード装置を選択し、選択した複数の第3のノード装置へ夫々認証情報を送信する。各第3のノード装置は、第1のノード装置の認証情報の正当性の検証に用いる検証情報を記録してあり、受信した認証情報及び記録している検証情報に基づいて、認証情報の正当性を検証し、検証した結果を示す結果情報を第2のノード装置へ送信する。第2のノード装置は、更に、複数の第3のノード装置の検証に対する夫々の信頼性を示す加重値を導出し、複数の第3のノード装置から受信した夫々の結果情報及び夫々の加重値に基づいて、第1のノード装置を認証する。

[0030] この構成により、本願では、ノード装置間で認証を行うので、特定の管理用ノード装置の処理負荷の増大を招くことがなく、また検証の結果が一致していない場合であっても、信頼性を加味して認証を行うので、単なる多数決による認証より正確性を向上させることが可能である等、優れた効果を奏する。

[0031] 本願は、第2のノード装置が、導出した加重値に基づいて、認証情報の正当性の検証を依頼する複数の第3のノード装置を選択する内容を開示する。

[0032] この構成により、本願では、信頼性の高い第3のノード装置に対して検証を依頼することができるので、認証に係る正確性を向上させることが可能である等、優れた効果を奏する。

[0033] 本願は、第3のノード装置までの論理空間上の距離に基づいて加重値を導出する内容を開示する。

[0034] この構成により、本願では、論理空間上の距離が近い程、最新の検証情報を記録しているとの前提に基づき、検証情報が新しく信頼性が高いと推定されるノード装置の加重値を高くし、認証の正確性を向上させることが可能である等、優れた効果を奏する。

[0035] 本願は、第3のノード装置が過去に検証を行った回数、過去の通信結果等のP2Pに関する貢献度の履歴に基づいて加重値を導出する内容を開示する。

[0036] この構成により、本願では、実績を加味して認証の正確性を向上させることが可能である等、優れた効果を奏する。

[0037] 本願は、第2のノード装置が、受信した複数の結果情報にて示される検証の結果が一致していない場合に、認証情報が正当でないとした第3のノード装置に対して導出

した加重値が所定値以上であるか否かを判定し、加重値が所定値以上であると判定したときに、当該加重値に係る第3のノード装置を示す情報を、管理用ノード装置へ送信する内容を開示する。

[0038] この構成により、本願では、正当でないと判定した第3のノード装置を不正等の可能性があるノード装置として、管理用ノード装置にて管理する。但し、信頼性が高いと見なしたノード装置のみを重要視して管理することにより、例えば古い検証情報を有している可能性が高く信頼性の低いノード装置まで通知することがないので、管理用ノード装置の処理負荷の増大を抑止することが可能である等、優れた効果を奏する。

[0039] 本願は、ノード装置が、自らの検証情報の再送信を要求する再送信要求を管理用ノード装置へ送信し、管理用ノード装置は、受信した再送信要求の送信元のノード装置の認証情報を、論理空間上の距離に基づいて選択された複数のノード装置へ、一のノード装置の検証情報として送信する。

[0040] この構成により、本願では、例えば認証に失敗した場合に、認証を依頼したノード装置が、管理用ノード装置に対して自らの検証情報の再配布を依頼するので、新たな状態で再度認証を依頼することが可能となる等、優れた効果を奏する。

[0041] 本願は、衛星放送等の放送を行う放送装置が、複数のノード装置へ放送に係る放送情報を送信する放送を行い、第2のノード装置は、認証に成功した第1のノード装置へ、第1のノード装置が受信した放送情報の欠落箇所を送信する。

[0042] この構成により、本願では、ノード装置が受信した放送情報に欠落が生じた場合に、ノード装置間で相互補完を行う際の認証に適用することが可能である。従って欠落箇所が生じた場合であっても、放送装置に対して再送信の依頼等の必要が無く、しかも欠落の補完に際し、認証処理を行うので、放送の不正な受信を防止することが可能である等、優れた効果を奏する。

図面の簡単な説明

[0043] [図1]従来の認証システムの構成を概念的に示す模式図である。

[図2]本発明の実施の形態1に係る認証システムの構成例を概念的に示す模式図である。

[図3]本発明の実施の形態1に係る認証システムにて用いられる各種装置のハード

ウェアの構成例を示すブロック図である。

[図4]本発明の実施の形態1に係る認証システムにて用いられるノード装置のソフトウェアの構成例を示す機能ブロック図である。

[図5]本発明の実施の形態1に係る認証システムにて用いられるノード装置のノード情報記録テーブルの記録内容の一例を示す概念図である。

[図6]本発明の実施の形態1に係る認証システムにて用いられる各種装置の認証情報配信処理の一例を示すシーケンス図である。

[図7]本発明の実施の形態1に係る認証システムの認証処理の概要を示す説明図である。

[図8]本発明の実施の形態1に係る認証システムにて用いられる各種装置の認証処理の一例を示すシーケンス図である。

[図9]本発明の実施の形態1に係る認証システムにて用いられる認証ノードが導出する加重値の例を示す図表である。

[図10]本発明の実施の形態2に係る認証システムにて用いられる各種装置の認証処理の一例を示すシーケンス図である。

[図11]本発明の実施の形態3に係る認証システムにて用いられる各種装置の認証処理の一例を示すシーケンス図である。

[図12]本発明の実施の形態4に係る認証システムにて用いられるノード装置のソフトウェアの構成例を示す機能ブロック図である。

[図13]本発明の実施の形態4に係る認証システムにて用いられる各種装置の検証情報再配信処理の一例を示すシーケンス図である。

[図14]本発明の実施の形態5に係る認証システムの構成例を概念的に示す模式図である。

[図15]本発明の実施の形態5に係る認証システムにて用いられる各種装置のハードウェアの構成例を示すブロック図である。

[図16]本発明の実施の形態5に係る認証システムにて用いられるノード装置のソフトウェアの構成例を示す機能ブロック図である。

[図17]本発明の実施の形態5に係る認証システムにて用いられる各種装置の放送

処理の一例を示すシーケンス図である。

符号の説明

[0044] 1 ノード装置

1a 被認証ノード

1b 認証ノード

1c 検証ノード

1d 第1ノード装置

1e 第2ノード装置

10 制御部

11 補助記憶部

12 記録部

13 記憶部

14 通信部

15 入力部

16 出力部

17 受信部

10a 認証情報送信手段

10b 検証依頼ノード選択手段

10c 検証依頼送信手段

10d 検証情報記録手段

10e 認証情報検証手段

10f 結果情報送信手段

10g 加重値導出手段

10h 認証手段

10i 認証結果通知手段

10j ピア情報導出手段

10k 検証情報再配信要求手段

10l 放送情報受信手段

12a 検証情報記録テーブル

12b ノード情報記録テーブル

2 管理用ノード装置

3 放送装置

100 コンピュータプログラム

NW 通信網

発明を実施するための最良の形態

[0045] 以下、本発明をその実施の形態を示す図面に基づいて詳述する。

[0046] 実施の形態1.

図2は、本発明の実施の形態1に係る認証システムの構成例を概念的に示す模式図である。図2中1，1，…は、本発明の認証装置として機能する複数のノード装置である。各ノード装置1，1，…は、通信網NWに接続し、通信網NWを介して各種情報（ファイル）の検索、転送等の通信を相互に行うPeer－to－Peer（以下、P2Pという）型の通信システムを構成している。また通信網NWには、全てのノード装置1，1，…に関する情報を管理する管理用ノード装置2が接続されている。

[0047] 図3は、本発明の実施の形態1に係る認証システムにて用いられる各種装置のハードウェアの構成例を示すブロック図である。ノード装置1は、装置全体を制御し、各種処理を実行するCPU等の制御部10と、本発明のコンピュータプログラム100及びデータ等の各種情報を記録したCD－ROM等の記録媒体から各種情報を読み取るCD－ROMドライブ等の補助記憶部11と、補助記憶部11により読み取った各種情報を記録するハードディスク等の記録部12と、一時的に発生する情報を記憶するRAM等の記憶部13とを備えている。そしてノード装置1は、記録部12に記録したコンピュータプログラム100を記憶部13に記憶させ、制御部10の制御にて実行することにより、本発明の認証装置に係る機能等の様々な機能を実現する。さらにノード装置1は、通信網NWに接続して通信を行う通信ポート等の通信部14と、マウス及びキーボード等の入力部15と、モニタ及びプリンタ等の出力部16とを備えている。

[0048] 管理用ノード装置2は、制御部20、記録部21、記憶部22、通信部23、入力部24及び出力部25を備えている。管理用ノード装置2の記録部21の記録領域の一部は

、各ノード装置1，1，…を夫々識別する識別情報であるノードIDと、各ノード装置1，1，…のIPアドレス及びポート番号と、各ノード装置1，1，…の認証情報と、各ノード装置1，1，…のピア情報とを対応付けて記録するノードテーブル21aとして用いられている。ピア情報とは、ノード装置1に付与されているノードIDをハッシュ関数で処理することにより導出されるハッシュ値であり、ピア情報により、複数のノード装置1，1，…を例えば160bitのハッシュ空間上にランダム性を持って一様に分布させることが可能となる。例えばノード装置AのノードIDをIDA とすると、ノード装置Aのピア情報HA はハッシュ関数SHA－1を用いた下記の式（1）により、001．．100等の2進数で示される160bitの値として導出される。

[0049] HA ＝SHA－1（IDA ） …式（1）

但し、HA ：ノード装置Aのピア情報

IDA ：ノード装置AのノードID

SHA－1（）：ハッシュ関数

[0050] 図4は、本発明の実施の形態1に係る認証システムにて用いられるノード装置1のソフトウェアの構成例を示す機能ブロック図である。ノード装置1は、本発明のコンピュータプログラム100を制御部10にて実行することにより、認証情報送信手段10a、検証依頼ノード選択手段10b、検証依頼送信手段10c、検証情報記録手段10d、認証情報検証手段10e、結果情報送信手段10f、加重値導出手段10g、認証手段10h、認証結果通知手段10i、ピア情報導出手段10j等の各種プログラムモジュールとして様々な機能を実現する。

[0051] 認証情報送信手段10aは、認証を要求するノード装置1が認証情報の送信に用いるプログラムモジュールである。検証依頼ノード選択手段10bは、要求に応じて認証を行うノード装置1が、認証情報の正当性の検証を依頼する複数のノード装置1，1，…の選択に用いるプログラムモジュールである。検証依頼送信手段10cは、認証を行うノード装置1が、選択した複数のノード装置1，1，…への認証情報の送信の依頼に用いるプログラムモジュールである。検証情報記録手段10dは、管理用ノード装置2から配信される検証情報の記録に用いるプログラムモジュールである。認証情報検証手段10eは、検証を依頼されたノード装置1が、認証情報及び検証情報に基づく

認証情報の正当性の検証に用いるプログラムモジュールである。結果情報送信手段10fは、検証を依頼されたノード装置1が、検証した結果を示す結果情報の送信に用いるプログラムモジュールである。加重値導出手段10gは、認証を行うノード装置1が、検証を行った各ノード装置1，1，…の検証に対する夫々の信頼性を示す加重値の導出に用いるプログラムモジュールである。認証手段10hは、認証を行うノード装置1が、結果情報及び加重値に基づいて、認証を要求したノード装置1の認証に用いるプログラムモジュールである。認証結果通知手段10iは、認証結果及び認証に関する情報の他の装置への通知に用いるプログラムモジュールである。ピア情報導出手段10jは、認証を行うノード装置1が、ノードID及びハッシュ関数に基づくピア情報の導出に用いるプログラムモジュールである。

[0052] またノード装置1は、本発明のコンピュータプログラム100を制御部10にて実行することにより、記録部12の記録領域の一部を、検証情報記録テーブル12a、ノード情報記録テーブル12b等の各種テーブルとして使用する。検証情報記録テーブル12aは、他のノード装置1，1，…のノードIDに対応付けて検証情報を記録するテーブルである。ノード情報記録テーブル12bは、各ノード装置1，1，…に関する各種情報を記録するテーブルである。

[0053] 図5は、本発明の実施の形態1に係る認証システムにて用いられるノード装置1のノード情報記録テーブル12bの記録内容の一例を示す概念図である。ノード情報記録テーブル12bには、他のノード装置1，1，…に関するIPアドレス、ポート番号、ノードID、ピア情報、転送量、検証回数、P2P貢献度等の各項目のデータが対応付けられたレコードとして記録されている。

[0054] ピア情報は、ノードID及びハッシュ関数に基づき導出される論理空間上の位置を示す情報である。転送量は、当該レコードに係るノード装置1と送受信したファイルのデータ転送量の総計である。検証回数は、当該レコードに係るノード装置1に検証依頼し、正当な結果情報を返した回数である。P2P貢献度とは、転送量、検証回数、検証により正当と判定した回数等のP2Pに関する処理の要素に基づき所定の方法で算出した指標値である。なおP2P貢献度としては、データ転送量、検証回数等の要素以外に、例えば自機に対してファイルを提供した回数等の様々な要素を加味して

設定することが可能である。

[0055] 次に本発明の各種装置の処理について説明する。図6は、本発明の実施の形態1に係る認証システムにて用いられる各種装置の認証情報配信処理の一例を示すシーケンス図である。通信網NWに接続した一のノード装置1は、制御部10の制御により、自らのIPアドレス及び認証情報を通信部14から通信網NWを介して管理用ノード装置2へ送信する。

[0056] IPアドレス及び認証情報を一のノード装置1から受信した管理用ノード装置2は、制御部20の制御により、一のノード装置1に対してノードIDを付与し(S101)、付与したノードID及びハッシュ関数SHA－1に基づいてピア情報を導出し(S102)、ノードID、認証情報及びピア情報をノードテーブル21aに記録する(S103)。また管理用ノード装置2は、付与したノードID及びピア情報を通信部23から通信網NWを介して、一のノード装置1へ送信し、一のノード装置1は、受信したノードID及びピア情報を自らのノードID及びピア情報として設定する。

[0057] さらに管理用ノード装置2は、制御部20の制御により、下記の式(2)により、一のノード装置1のノードIDから導出した一のノード装置1に係る情報にて示される論理空間上の位置に近いピア情報が付与された他の複数のノード装置1，1，…を、一のノード装置1の認証情報の送信先として選択する(S104)。

[0058] HA+α＝SHA－1(IDA+α) …式(2)

但し、HA+α：ノード装置Aに係る情報

IDA ：ノード装置AのノードID

SHA－1()：ハッシュ関数

α：定数

[0059] ステップS104において、管理用ノード装置2は、一のノード装置1のピア情報にて示される論理空間上の位置と、ノードテーブル21aに記録している他の全てのノード装置1，1，…の夫々のピア情報にて示される論理空間上の位置との間の距離を夫々算出する。ピア情報にて示される位置間の距離は、ピア情報同士の排他的論理和として算出することができる。管理用ノード装置2は、算出した距離が近い順に所定個数のノード装置1，1，…及び／又はピア情報間の距離が所定値以下であるノード

装置1，1，…を選択する。式(2)にて求められる一のノード装置1に係る情報とは、ピア情報と同次元の論理空間上の位置を示す位置情報である。なおステップS104の選択に際し、一のノード装置1のピア情報が示す位置からの距離に基づいて選択する様にしても良い。

[0060] そして管理用ノード装置2は、制御部20の制御により、選択した他の複数のノード装置1，1，…へ、一のノード装置1のIPアドレス、ポート番号、ノードID及びピア情報と、一のノード装置1の認証情報とを通信部23から通信網NWを介して送信する(S105)。なお認証情報は、一のノード装置1の検証情報として送信される。またピア情報は、ノードIDから導出することができるため、ピア情報の送信を省略することも可能である。

[0061] IPアドレス、ポート番号、ノードID、ピア情報及び検証情報(認証情報)を受信した他のノード装置1は、制御部10の制御に基づく検証情報記録手段10dの処理により、受信したノードID及び検証情報を対応付けたレコードとして検証情報記録テーブル12aに記録し、IPアドレス、ポート番号、ノードID及びピア情報を対応付けたレコードとしてノード情報記録テーブル12bに記録する(S106)。この様にして認証情報配信処理が実行される。なお一のノード装置1の検証情報を、論理空間上の近い位置にある他の複数のノード装置1，1，…へ配信する処理は、前述した処理に限るものではなく、送受信する情報、タイミング、処理の順等、適宜設定することが可能であり、また他のP2Pに関する技術を転用する様にしても良い。例えば管理用ノード装置2は、ステップS105において、一のノード装置1のノードID又はピア情報を送信し、他のノード装置1は、一のノード装置1のピア情報に対し、過去の通信履歴を参照して自らのピア情報との距離の関係が所定値以下である、自らが最も近いノード装置1である等の所定条件を満足する場合、管理用ノード装置2に対し、認証情報の送信を要求する様にしても良い。

[0062] 図7は、本発明の実施の形態1に係る認証システムの認証処理の概要を示す説明図である。本発明の認証処理では、第1のノード装置1(以降、被認証ノード1aという)が、第2のノード装置1(以降、認証ノード1bという)へ認証情報を送信することで認証を要求する。認証ノード1bは、所定の方法で選択した複数の第3のノード装置1，1，

…(以降、検証ノード1c，1c，…という)に認証情報の検証を依頼する。検証ノード1c，1c，…は、夫々認証情報を検証し、検証した結果を示す結果情報を認証ノード1bへ送信する。認証ノード1bは、結果情報にて示される検証の結果に基づいて認証の正否を判定する。認証処理は、例えば被認証ノード1aが、認証ノード1bに対して、ファイルの送信等の通信処理を依頼する場合の前処理として実行される。

[0063] 図8は、本発明の実施の形態1に係る認証システムにて用いられる各種装置の認証処理の一例を示すシーケンス図である。被認証ノード1aは、コンピュータプログラム100を実行する制御部10の制御に基づく認証情報送信手段10aの処理により、自らのノードID及び認証情報を含む認証要求を通信部14から通信網NWを介して認証ノード1bへ送信する(S201)。

[0064] 認証要求を受信した認証ノード1bは、コンピュータプログラム100を実行する制御部10の制御に基づくピア情報導出手段10jの処理により、受信した被認証ノード1aのノードID及び予め記録している所定のハッシュ関数に基づいてピア情報及び被認証ノード1aに係る情報を導出する(S202)。

[0065] 認証ノード1bは、制御部10の制御に基づく検証依頼ノード選択手段10bの処理により、ステップS202にて導出した被認証ノード装置1aに係る情報にて示される論理空間上の位置に近いピア情報が付与された複数のノード装置1，1，…を、認証情報の検証を依頼する検証ノード1c，1c，…として選択する(S203)。

[0066] ステップS203において、認証ノード1bは、被認証ノード1aに係る情報にて示される論理空間上の位置と、ノード情報記録テーブル12bに記録している他のノード装置1，1，…の夫々のピア情報にて示される論理空間上の位置との間の距離を夫々算出する。そして認証ノード1bは、算出した距離が近い順に所定個数のノード装置1，1，…及び／又はピア情報間の距離が所定値以下であるノード装置1，1，…を検証ノード1c，1c，…として選択する。なお過去の通信により、被認証ノード1aの検証情報を記録しているノード装置1，1，…が判明している場合、当該ノード装置1，1，…の中で距離が近いノード装置1，1，…が検証ノード1c，1c，…として選択される。

[0067] 認証ノード1bは、制御部10の制御に基づく検証依頼送信手段10cの処理により、ステップS203にて選択した検証ノード1c，1c，…へ、被認証ノード1aの認証情報の

正当性の検証を依頼する検証依頼を通信部14から通信網NWを介して送信する(S204)。ステップS204にて送信される検証依頼には、被認証ノード1aのノードID、認証ノード1bのノードID、被認証ノード1aの認証情報等の情報が含まれている。

[0068] 検証依頼を受信した検証ノード1cは、コンピュータプログラム100を実行する制御部10の制御に基づく認証情報検証手段10eの処理により、受信した検証依頼に含まれる認証情報及び検証情報記録テーブル12aに記録している検証情報に基づいて認証ノード1bの認証情報の正当性を検証する(S205)。ステップS205では、受信した検証依頼に含まれる被認証ノード1aのノードIDに対応付けて記録されている検証情報を検証情報記録テーブル12aから抽出する。そして抽出した検証情報と、受信した検証依頼に含まれる認証情報とを照合することにより、正当性を検証する。なお検証情報記録テーブル12aに、検証依頼に含まれる被認証ノード1aのノードIDに対応する検証情報が記録されていない場合、不正な認証情報であるとの検証結果を出力する。

[0069] そして検証ノード1cは、制御部10の制御に基づく結果情報送信手段10fの処理により、検証した結果を示す結果情報を通信部14から通信網NWを介して認証ノード1bへ送信する(S206)。ステップS206にて送信される結果情報には、被認証ノード1aのノードID、検証結果、検証ノード1cのノードID等の情報が含まれている。

[0070] 各検証ノード1c, 1c, …から結果情報を受信した認証ノード1bは、制御部10の制御に基づくピア情報導出手段10jの処理により、夫々の結果情報に含まれるノードID及び予め記録している所定のハッシュ関数に基づいて、各検証ノード1c, 1c, …のピア情報を導出する(S207)。ステップS207では、管理用ノード装置2が用いたハッシュ関数と同様のハッシュ関数を用いるため、管理用ノード装置2が導出するピア情報と同様の値が導出される。

[0071] 認証ノード1bは、制御部10の制御に基づく加重値導出手段10gの処理により、検証に対する夫々の信頼性を示す加重値を導出する(S208)。

[0072] ステップS208にて導出する加重値について説明する。認証ノード1bは、各検証ノード1c, 1c, …を信頼性の高い順に並べ替えを行い、信頼性が高い順に大きい値となる様に各検証ノード1c, 1c, …の加重値を導出する。信頼性の高さは、ステップS

208にて導出したピア情報及び／又はノード情報テーブル12bに記録されているP2P貢献度に基づいて決定される。例えば導出したピア情報にて示される論理空間上の位置が被認証ノード1aに係る情報に近い順に各検証ノード1c，1c，…の信頼性が高くなる。論理空間上の位置が近い検証ノード1c，1c，…に対しては、管理用ノード装置2から最新のピア情報が配信されているとの前提に基づいて信頼性が高いと推定することができるからである。またノード情報テーブル12bに記録されているP2P貢献度が高い順に各検証ノード1c，1c，…の信頼性が高くなる。P2P貢献度が高い検証ノード1cは、過去の検証の履歴から信頼性が高いと推定することができるからである。更にはピア情報にて求まる信頼性及びP2P貢献度にて求まる信頼性を示す値の合算、平均等の所定の方法で求めることにより各検証ノード1c，1c，…の信頼性を導出することができる。

[0073] 図9は、本発明の実施の形態1に係る認証システムにて用いられる認証ノード1bが導出する加重値の例を示す図表である。図9に示す図表は、信頼性の順位と加重値との関係の例を示している。図9の例1は、信頼性が最も高い信頼性1位の検証ノード1cの加重値として0．5が導出され、信頼性2位の検証ノード1c及び信頼性3位の検証ノード1cに対しては加重値として0．25が導出されることを示している。なお例1では、信頼性4位以下の検証ノード1c，1c，…に対する加重値は0となる。図9の例2は、信頼性一位の検証ノード1c及び信頼性2位の検証ノード1cに対し、加重値として0．5が導出されることを示している。なお例2では、信頼性3位以下の検証ノード1c，1c，…に対する加重値は0となる。図9の例3は、信頼性が高い順に加重値として0．4、0．3、0．2、そして0．1が導出されることを示している。図9に示した加重値は一例であり、認証システムの目的、仕様等の要因に応じて適宜設定することが可能である。

[0074] シーケンス図に戻り、認証ノード1bは、制御部10の制御に基づく認証手段10hの処理により、複数の検証ノード1c，1c，…から受信した結果情報に含まれる夫々の検証結果、及び導出した夫々の検証ノード1c，1c，…に対する加重値に基づいて、被認証ノード1aの認証を行う（S209）。ステップS209において、認証ノード1bは、正当であると判定した検証ノード1c，1c，…に対して点数1を付与し、不正であると判定し

た検証ノード1c，1c，…に対して点数0を付与し、夫々の点数に加重値を乗じて合計する。即ち正当であると判定した検証ノード1c，1c，…に対応する加重値を合計する。そして合計値が予め設定されている0．5、0．6等の所定値以上である場合に、認証ノード1bは、被認証ノード1aが正当であるとして認証成功との判定を行う。合計値が所定値未満である場合、認証は失敗となる。

[0075] 認証ノード1bは、制御部10の制御に基づく認証結果通知手段10iの処理により、認証結果を通信部14から通信網NWを介して被認証ノード1aへ送信する（S210）。ステップS210にて送信される認証結果には、被認証ノード1aのノードID、認証の成否を示す認証結果、認証ノード1bのノードID等の情報が含まれている。そして認証ノード1bは、認証が成功である場合、認証ノード1bに対して、ファイルの送信等の通信処理を実行する。

[0076] また認証ノード1bは、制御部10の制御に基づく認証結果通知手段10iの処理により、認証が失敗であると判定した場合の被認証ノード1aのノードIDを通知する認証失敗通知及び認証情報が正当でないと判定した検証ノード1c，1c，…のノードIDを通知する不正判定ノード通知を通信部14から通信網NWを介して管理用ノード装置2へ送信する（S211）。ステップS211にて送信される認証失敗通知には、被認証ノード1aのノードID、認証の成否を示す認証結果、認証ノード1bのノードID等の情報が含まれている。また不正判定ノード通知には、被認証ノード1aのノードID、検証結果、認証が失敗であると判定した検証ノード1cのノードID等の情報が含まれている。認証が成功であると判定した場合、認証失敗通知の送信は行われない。但し、不正判定ノード通知は、認証結果の如何に関わらず送信される。なお全ての検証結果が、被認証ノード1aの正当性を認める内容である場合、ステップS211以降の処理は実行されない。更に認証ノード1bは、認証処理の結果に基づいて、ノード情報テーブル12bを更新する。なおステップS211において、認証が失敗であり、認証情報が正当でないと判定した結果情報を返した検証ノード1c，1c，…が多数である場合、認証情報が正当であると判定した検証ノード1c，1c，…の方が不正なノード装置である可能性がある。従ってこの様な場合、認証情報が正当でないにも拘わらず、認証情報が正当であるとの結果情報を返した検証ノード1c，1c，…を認証が正当でないとし

た検証ノード1c，1c，…であると見なす。

[0077] 認証失敗通知及び不正判定ノード通知を受信した管理用ノード装置2は、制御部20の制御により、通知された被認証ノード1a及び検証ノード1c，1c，…のノードIDを検証する検証処理を実行する（S212）。ステップS212の検証処理とは、通知された被認証ノード1a及び検証ノード1c，1c，…の正当性を判定し、対応する処理である。検証処理において管理用ノード装置2は、被認証ノード1aを不正なノードであると判定した場合、被認証ノード1aに対する不正ノード一覧（ブラックリスト）への登録等の所定の不正ノード対応処理を実行し、検証ノード1c，1c，…を不正なノードであると判定した場合、不正であると判定した検証ノード1c，1c，…に対する所定の不正ノード対応処理を実行する。

[0078] ステップS212の検証処理において、通知された被認証ノード1aが正当なノードであると判定した場合で、通知された検証ノード1c，1c，…に正当なノードが含まれる場合、管理用ノード装置2は、通信部23から通信網NWを介して、正当な検証ノード1c，1c，…に対して、被認証ノード1aの認証情報（検証情報）を再配信する（S213）。ステップS213の検証情報の再配信は検証ノード1c，1c，…が古い検証情報を記録しているとの推定に基づいて行う処理である。なお被認証ノード1aが不正なノードであると判定した場合又は通知された検証ノード1c，1c，…に正当なノードが含まれていないと判定した場合、ステップS213の再配信処理は実行されない。この様にして、認証処理が実行される。

[0079] 実施の形態2.

実施の形態2は、実施の形態1の認証処理において、検証を依頼する検証ノードの絞り込みを行う形態である。なお以降の説明において、実施の形態1と同様の構成については、実施の形態1と同様の符号を付すものとする。実施の形態2に係る認証システム及び各種装置の構成例は実施の形態1と同様であるので、実施の形態1を参照するものとし、その説明を省略する。また実施の形態2に係る認証システムの認証情報配信処理は、実施の形態1と同様であるので実施の形態1を参照するものとし、その説明を省略する。

[0080] 図10は、本発明の実施の形態2に係る認証システムにて用いられる各種装置の認

証処理の一例を示すシーケンス図である。被認証ノード1a及び認証ノード1bは、実施の形態1の認証処理のステップS201～S203に係る処理と同様に、認証情報の送信から検証ノード1c，1c，…の選択までの処理を実行する。

[0081] 認証ノード1bは、コンピュータプログラム100を実行する制御部10の制御に基づく加重値導出手段10gの処理により、選択した検証ノード1c，1c，…の検証に対する夫々の信頼性を示す加重値を導出する（S301）。ステップS301における加重値の導出は、実施の形態1に係る認証処理のステップS207における加重値の導出と実質的に同様であるが、図9に例示した図表の例より多くの検証ノード1c，1c，…に対して0より大きい有意な加重値を導出する様にしても良い。

[0082] 認証ノード1bは、制御部10の制御に基づく検証依頼ノード選択手段10bの処理により、導出した加重値に基づいて、加重値を導出した検証ノード1c，1c，…から、認証情報の正当性の検証を依頼する複数の検証ノード1c，1c，…を再選択する（S302）。ステップS302では、加重値が所定値以上又は加重値が高い順に所定数の検証ノード1c，1c，…を選択することにより、最初に選択した検証ノード1c，1c，…に対する絞り込みを行う。

[0083] そして認証ノード1b及び検証ノード1c，1c，…は、実施の形態1の認証処理のステップS204以降の処理を実行する。この様にして認証処理が実行される。

[0084] 実施の形態3.

実施の形態3は、実施の形態1の認証処理において、認証処理を行った認証ノードが、認証情報が正当でないと判定した検証ノードの中で、加重値が高い検証ノードのみのノードIDを管理用ノード装置に通知する形態である。なお以降の説明において、実施の形態1と同様の構成については、実施の形態1と同様の符号を付すものとする。実施の形態3に係る認証システム及び各種装置の構成例は実施の形態1と同様であるので、実施の形態1を参照するものとし、その説明を省略する。また実施の形態3に係る認証システムの認証情報配信処理は、実施の形態1と同様であるので実施の形態1を参照するものとし、その説明を省略する。

[0085] 図11は、本発明の実施の形態3に係る認証システムにて用いられる各種装置の認証処理の一例を示すシーケンス図である。被認証ノード1a、認証ノード1b及び検証

ノード1c，1c，…は、実施の形態1の認証処理のステップS201～S210に係る処理と同様に、認証情報の送信から認証結果の送信までの処理を実行する。

[0086] 認証ノード1bは、コンピュータプログラム100を実行する制御部10の制御に基づく認証結果通知手段10iの処理により、認証情報が正当でないと判定した検証ノード1c，1c，…に対して導出した加重値が0．5、0．3等の所定値以上であるか否かを判定する（S401）。ステップS401の代替処理として、加重値が高い方から所定順位までの検証ノード1c，1c，…であるか否かを判定する様にしても良い。なお認証ノード1bが受信した全ての検証結果が一致していた場合、ステップS401以降の処理は実行されない。

[0087] そして認証ノード1bは、制御部10の制御に基づく認証結果通知手段10iの処理により、不正判定ノード通知を通信部14から通信網NWを介して管理用ノード装置2へ送信する（S402）。ステップS402において、不正判定ノード通知には、被認証ノード1aの認証情報が正当でないと判定した検証ノード1c，1c，…の中で、加重値が所定値以上の検証ノード1c，1c，…のノードIDが含まれているが、加重値が所定値未満の検証ノード1c，1c，…のノードIDは含まれていない。

[0088] そして認証ノード1b及び検証ノード1c，1c，…は、実施の形態1の検証処理のステップS212以降の処理を実行する。実施の形態3では、加重値が低い検証ノード1c，1c，…に関する不正ノード判定通知の管理用ノード装置2への送信を制限することにより、管理用ノード装置2に関する通信負荷、及び管理用ノード装置2の検証、再配信等の管理処理に係る処理負荷を軽減することが可能である。この様にして、認証処理が実行される。

[0089] 実施の形態4．

実施の形態4は、実施の形態1の認証処理において、認証が失敗であることを示す認証結果を受信した被認証ノードが、認証情報（検証情報）の再配信を管理用ノード装置2へ要求する形態である。なお以降の説明において、実施の形態1と同様の構成については、実施の形態1と同様の符号を付すものとする。実施の形態4に係る認証システム及び各種装置のハードウェアの構成例は実施の形態1と同様であるので、実施の形態1を参照するものとし、その説明を省略する。

[0090] 図12は、本発明の実施の形態4に係る認証システムにて用いられるノード装置1のソフトウェアの構成例を示す機能ブロック図である。ノード装置1は、本発明のコンピュータプログラム100を制御部10にて実行することにより、認証情報送信手段10a、検証依頼ノード選択手段10b、検証依頼送信手段10c、検証情報記録手段10d、認証情報検証手段10e、結果情報送信手段10f、加重値導出手段10g、認証手段10h、認証結果通知手段10i、ピア情報導出手段10j、検証情報再配信要求手段10k等の各種プログラムモジュールとして様々な機能を実現する。検証情報再配信要求手段10kは、管理用ノード装置2に対し、検証情報の再配信の要求に用いるプログラムモジュールである。

[0091] またノード装置1は、本発明のコンピュータプログラム100を制御部10にて実行することにより、記録部12の記録領域の一部を、検証情報記録テーブル12a、ノード情報記録テーブル12b等の各種テーブルとして使用する。

[0092] 次に本発明の実施の形態4に係る各種装置の処理について説明する。実施の形態4に係る認証システムの認証情報配信処理及び認証処理は、実施の形態1と同様であるので実施の形態1を参照するものとし、その説明を省略する。

[0093] 図13は、本発明の実施の形態4に係る認証システムにて用いられる各種装置の検証情報再配信処理の一例を示すシーケンス図である。認証ノード1bは、実施の形態1の認証処理のステップS210として示した様に、認証結果を被認証ノード1aへ送信する。認証結果を受信した被認証ノード1aは、受信した認証結果の内容を検出し、認証が失敗であると検出した場合、以降に示す検証情報再配信処理を実行する。

[0094] 被認証ノード1aは、コンピュータプログラム100を実行する制御部10の制御に基づく検証情報再配信要求手段10kの処理により、認証が失敗であることを示す認証結果をモニタである出力部16から出力する(S501)。認証結果を確認した使用者は、再認証の依頼を前提として、検証情報の再配信を要求する場合、入力部15を用いて所定の入力操作を行う。

[0095] 被認証ノード1aは、コンピュータプログラム100を実行する制御部10の制御に基づく検証情報再配信要求手段10kの処理により、入力部15から入力操作を受け付け(S502)、自らの検証情報(認証情報)の再送信を要求する再送信要求を、通信部14

から通信網NWを介して管理用ノード装置2へ送信する(S503)。ステップS503にて送信する再送信要求には、被認証ノード1aのノードID等の情報が含まれている。

[0096] 再送信要求を受信した管理用ノード装置2は、制御部20の制御により、受信した再送信要求に含まれるノードID及びハッシュ関数SHA－1に基づいて被認証ノード1aに係る情報を導出し(S504)、導出した被認証ノード1aに係る情報にて示される論理空間上の位置に近いピア情報が付与された複数のノード装置1，1，…を、被認証ノード1aの検証情報の送信先として選択する(S505)。

[0097] そして管理用ノード装置2は、制御部20の制御により、被認証ノード1aのノードIDに対応付けて記録されているIPアドレス、ポート番号、ノードID、ピア情報及び検証情報(認証情報)をノードテーブル21aから抽出し(S506)、被認証ノード1aのIPアドレス、ポート番号、ノードID、ピア情報及び検証情報(認証情報)を、通信部23から通信網NWを介してステップS505にて選択した複数のノード装置1，1，…へ送信する(S507)。

[0098] IPアドレス、ポート番号、ノードID、ピア情報及び検証情報(認証情報)を受信したノード装置1は、制御部10の制御に基づく検証情報記録手段10dの処理により、受信したノードID及び検証情報を対応付けたレコードとして検証情報記録テーブル12aに記録し、IPアドレス、ポート番号、ノードID及びピア情報を対応付けたレコードとしてノード情報記録テーブル12bに記録する(S508)。

[0099] そして管理用ノード装置2は、検証情報の再配信を行ったことを、被認証ノード1aに通知し、被認証ノード1aは、再度、認証ノード1bに対して認証要求を送信し、認証処理が開始される。被認証ノード1aに対してピア情報(ノードID)が付与された後、新たに通信網NWに接続したノード装置1に対して、被認証ノード1aに係る情報に近い一のピア情報(ノードID)が付与された場合、新たに接続したノード装置1は、被認証ノード1aの正当性を検証する検証ノード1cとなり得るが、被認証ノード1aの検証情報を記録していないため、被認証ノード1aの認証情報を不正であると判定する。検証情報再配信処理は、この様な状況に対して有効に機能する。

[0100] 実施の形態5.

実施の形態5は、実施の形態1の認証システムを、衛星放送等の放送の補完に適

用する形態である。なお以降の説明において、実施の形態1と同様の構成については、実施の形態1と同様の符号を付すものとする。

[0101] 図14は、本発明の実施の形態5に係る認証システムの構成例を概念的に示す模式図である。図14中3は、衛星放送を行う地上局、地上波放送を行う放送局等の放送装置である。放送装置3は、放送コンテンツである放送情報を放送波に重畳し、放送衛星、中継局等の中継装置を介して複数のノード装置1，1，…へ送信する放送を行う。各ノード装置1，1，…は、放送波を受信し、受信した放送波に重畳された放送情報に基づく映像及び音声の出力等の処理を行う。なお降雨、降雪、放送波の伝送経路の切替等の要因により、ノード装置1が受信した放送情報に、正常にデータを受信していない欠落箇所が生じる場合がある。放送情報に、欠落箇所が存在する場合、各ノード装置1，1，…は、欠落箇所を相互に補完する。

[0102] 図15は、本発明の実施の形態5に係る認証システムにて用いられる各種装置のハードウェアの構成例を示すブロック図である。ノード装置1は、制御部10、補助記憶部11、記録部12、記憶部13、通信部14、入力部15、出力部16、及びチューナ等の受信部17を備えており、本発明のコンピュータプログラム100を実行する。受信部17は、放送波を受信し、受信した放送波から放送情報を抽出する。

[0103] 管理用ノード装置2の構成は、実施の形態1と同様であるので、実施の形態1を参照するものとし、その説明を省略する。放送装置3は、制御部30、放送波を送信する送信部31等の様々な機構を備えている。

[0104] 図16は、本発明の実施の形態5に係る認証システムにて用いられるノード装置1のソフトウェアの構成例を示す機能ブロック図である。ノード装置1は、本発明のコンピュータプログラム100を制御部10にて実行することにより、認証情報送信手段10a、検証依頼ノード選択手段10b、検証依頼送信手段10c、検証情報記録手段10d、認証情報検証手段10e、結果情報送信手段10f、加重値導出手段10g、認証手段10h、認証結果通知手段10i、ピア情報導出手段10j、放送情報受信手段10l等の各種プログラムモジュールとして様々な機能を実現する。放送情報処理手段10lは、放送情報の補完等の放送情報に関する様々な処理に用いるプログラムモジュールである。

[0105] またノード装置1は、本発明のコンピュータプログラム100を制御部10にて実行する

ことにより、記録部12の記録領域の一部を、検証情報記録テーブル12a、ノード情報記録テーブル12b等の各種テーブルとして使用する。また記録部12には、放送情報を受信する正規の契約を結んでいることを証明する証明書情報が記録されている。証明書情報は、事前に放送事業者から例えば通信網NWを介して配布されるデータであり、放送情報の受信に用いるグループIDが含まれている。

[0106] 次に本発明の実施の形態5に係る各種装置の処理について説明する。実施の形態5に係る認証システムの認証情報配信処理は、実施の形態1と同様であるので、実施の形態1を参照するものとし、その説明を省略する。

[0107] 図17は、本発明の実施の形態5に係る認証システムにて用いられる各種装置の放送処理の一例を示すシーケンス図である。なお以降の説明において、欠落箇所を要求するノード装置1を第1ノード装置1dとし、欠落箇所を送信するノード装置1を第2ノード装置1eとして説明する。放送装置3は、制御部30の制御により、送信部31から、放送波に重畳して放送情報を送信(放送)する(S601)。

[0108] 第1ノード装置1dは、コンピュータプログラム100を実行する制御部10の制御に基づく放送情報受信手段101の処理により、受信部17にて受信した放送波に基づく放送情報を記録部12に記録し(S602)、記録した放送情報の欠落箇所の有無を検出する(S603)。ステップS603の欠落箇所の検出は、エラーチェックに関する様々な既存技術が適宜用いられる。

[0109] ステップS603において、欠落箇所を有すると検出した場合、第1ノード装置1dは、制御部10の制御に基づく放送情報受信手段101の処理により、他のノード装置1に対し、当該欠落箇所を記録しているか否かの問い合わせを行う(S604)。

[0110] 第1ノード装置1dは、制御部10の制御により、ステップS604の問い合わせにより、欠落箇所を記録していることが判明した他のノード装置1(第2ノード装置1e)との間で認証処理を実行する(S605)。ステップS605の認証処理は、実施の形態1にて説明した認証処理である。なお認証処理において、欠落箇所を要求する第1ノード装置1dが、被認証ノード1aとなり、欠落箇所を記録している第2ノード装置1eが、認証ノード1bとなる。なお認証処理において用いられる論理空間上の位置を示す情報の導出に際し、定数αとして証明書情報のグループIDが用いられる。

[0111] 認証が成功した場合、第2ノード装置1eは、制御部10の制御により、通信部14から通信網NWを介して第1ノード装置1dへ、放送情報の欠落箇所を送信する(S606)。この様にして放送情報の欠落箇所を相互に補完することにより、放送事業者は、放送情報の配信を保障することができ、放送装置3は放送情報の再送信等の処理を実行する必要がないので放送装置3に関する処理負荷及び通信負荷を軽減し、またグループIDにより放送情報の不正入手を防止することが可能である。

[0112] 前記実施の形態1乃至5は、本発明の無限にある実施の形態の一部を例示したに過ぎず、信頼性を示す加重値及び検証結果を示す結果情報に基づいて認証を行うのであれば、各種ハードウェア及びソフトウェア等の構成、その他認証に関する手順は、適宜設計することが可能である。

[0113] また前記実施の形態1乃至5は、夫々独立して実行することも可能であるが、必要に応じて適宜組み合わせて実行することが可能である。

請求の範囲

[1] 通信網を介して相互に通信することが可能な複数のノード装置を備え、一のノード装置の認証情報の正当性を、他の複数のノード装置が記録している検証情報に基づいて検証することで前記一のノード装置を認証する認証システムにおいて、

第1のノード装置は、

自らの認証情報を第2のノード装置へ送信する手段を備え、

前記第2のノード装置は、

受信した認証情報の正当性の検証を依頼する複数の第3のノード装置を選択する手段と、

選択した複数の第3のノード装置へ夫々認証情報を送信する手段と

を備え、

前記第3のノード装置の夫々は、

前記第1のノード装置の認証情報の正当性の検証に用いる検証情報を記録する手段と、

受信した認証情報及び記録している検証情報に基づいて、認証情報の正当性を検証する手段と、

検証した結果を示す結果情報を前記第2のノード装置へ送信する手段と

を備え、

前記第2のノード装置は、更に、

前記複数の第3のノード装置の検証に対する夫々の信頼性を示す加重値を導出する加重値導出手段と、

前記複数の第3のノード装置から受信した夫々の結果情報及び夫々の加重値に基づいて、前記第1のノード装置を認証する手段と

を備えることを特徴とする認証システム。

[2] 通信網を介して相互に通信することが可能な複数のノード装置を備え、一のノード装置の認証情報の正当性を、他の複数のノード装置が記録している検証情報に基づいて検証することで前記一のノード装置を認証する認証システムにおいて、

第1のノード装置は、

自らの認証情報を第2のノード装置へ送信する手段を備え、

前記第2のノード装置は、

前記第1のノード装置及び第2のノード装置以外の複数のノード装置が、前記第1のノード装置の認証情報の正当性を検証する場合の検証に対する夫々の信頼性を示す加重値を導出する加重値導出手段と、

導出した加重値に基づいて、加重値を導出した複数のノード装置から、認証情報の正当性の検証を依頼する複数の第3のノード装置を選択する手段と、

選択した複数の第3のノード装置へ夫々認証情報を送信する手段と

を備え、

前記各第3のノード装置の夫々は、

前記第1のノード装置の認証情報の正当性の検証に用いる検証情報を記録する手段と、

受信した認証情報及び記録している検証情報に基づいて、認証情報の正当性を検証する手段と、

検証した結果を示す結果情報を前記第2のノード装置へ送信する手段と

を備え、

前記第2のノード装置は、更に、

前記複数の第3のノード装置から受信した夫々の結果情報及び前記加重値導出手段により導出した前記複数の第3のノード装置に対する加重値に基づいて、前記第1のノード装置を認証する手段と

を備えることを特徴とする認証システム。

[3] 前記第2のノード装置は、

前記個々のノード装置を識別する識別情報及び所定の関数に基づいて、前記各ノード装置の論理空間上の位置を示す位置情報を導出する手段を更に備え、

前記加重値導出手段は、位置情報から求まる前記第1のノード装置からの距離に基づいて夫々の加重値を導出する様に構成してあることを特徴とする請求項1又は請求項2に記載の認証システム。

[4] 前記加重値導出手段は、前記第3のノード装置の夫々の検証の履歴に基づいて加

重値を導出する様に構成してあることを特徴とする請求項1乃至請求項3のいずれかに記載の認証システム。

[5] 前記各ノード装置に関する情報を管理する管理用ノード装置を更に備え、

該管理用ノード装置は、

前記各ノード装置について、個々のノード装置を識別する識別情報及び認証情報を記録する手段と、

前記各ノード装置の識別情報及び所定の関数に基づいて、前記各ノード装置の論理空間上の位置を示す位置情報を導出する手段と、

導出した位置情報から求まる一のノード装置から他の各ノード装置までの夫々の論理空間上の距離に基づき、前記一のノード装置の認証情報を送信する複数のノード装置を選択する手段と、

選択した前記複数のノード装置へ、前記一のノード装置の認証情報を検証情報として送信する手段と

を備える

ことを特徴とする請求項1乃至請求項4のいずれかに記載の認証システム。

[6] 前記第2のノード装置は、更に、

検証情報が正当でないと判定した前記第3のノード装置に対して導出した加重値が所定値以上であるか否かを判定する手段と、

加重値が所定値以上であると判定した場合に、当該加重値に係る前記第3のノード装置を示す情報を、前記管理用ノード装置へ送信する手段と

を備えることを特徴とする請求項5に記載の認証システム。

[7] 前記一のノード装置は、更に、

自らの検証情報の再送信を要求する再送信要求を前記管理用ノード装置へ送信する手段を備え、

前記管理用ノード装置は、更に、

受信した再送信要求の送信元のノード装置の認証情報を、論理空間上の距離に基づいて選択された複数のノード装置へ、前記一のノード装置の検証情報として送信する手段を備える

ことを特徴とする請求項5又は請求項6に記載の認証システム。

[8] 前記複数のノード装置へ放送に係る放送情報を送信する放送装置を更に備え、

前記第2のノード装置は、更に、

認証に成功した前記第1のノード装置へ、該第1のノード装置が受信した放送情報の欠落箇所を送信する手段を備える

ことを特徴とする請求項1乃至請求項7のいずれかに記載の認証システム。

[9] 複数のノード装置との相互の通信を媒介する通信網に接続し、一のノード装置の認証情報の正当性を、他の複数のノード装置に検証を依頼することで前記一のノード装置を認証する認証装置において、

前記一のノード装置から、該一のノード装置の認証情報を受信する手段と、

受信した認証情報の正当性の検証を依頼する複数の他のノード装置を選択する手段と、

選択した複数の他のノード装置へ夫々認証情報を送信する手段と、

前記他のノード装置の夫々から、認証情報に基づく検証結果を示す結果情報を受信する手段と、

前記他のノード装置夫々の検証に対する夫々の信頼性を示す加重値を導出する手段と、

受信した夫々の結果情報及び夫々の加重値に基づいて、前記一のノード装置を認証する手段と

を備えることを特徴とする認証装置。

[10] 複数のノード装置との相互の通信を媒介する通信網に接続してあるコンピュータに、一のノード装置の認証情報の正当性を、他の複数のノード装置に検証を依頼することで前記一のノード装置を認証させるコンピュータプログラムにおいて、

コンピュータに、

前記一のノード装置から、該一のノード装置の認証情報を受信した場合に、受信した認証情報の正当性の検証を依頼する複数の他のノード装置を選択させる手順と、

選択した複数の他のノード装置へ夫々認証情報を送信させる手順と、

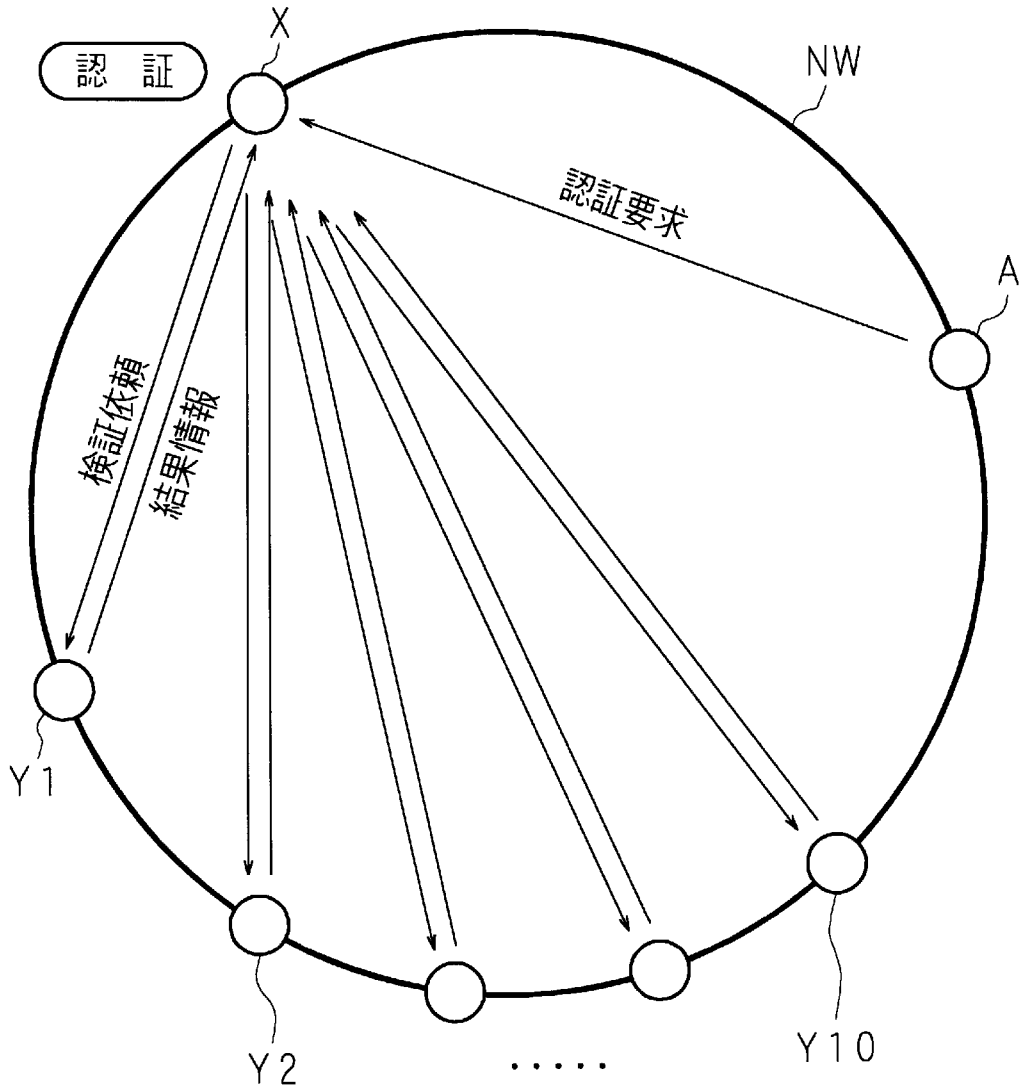
前記他のノード装置の夫々から、認証情報に基づく検証結果を示す結果情報を受

信したときに、前記他のノード装置夫々の検証に対する夫々の信頼性を示す加重値を導出させる手順と、

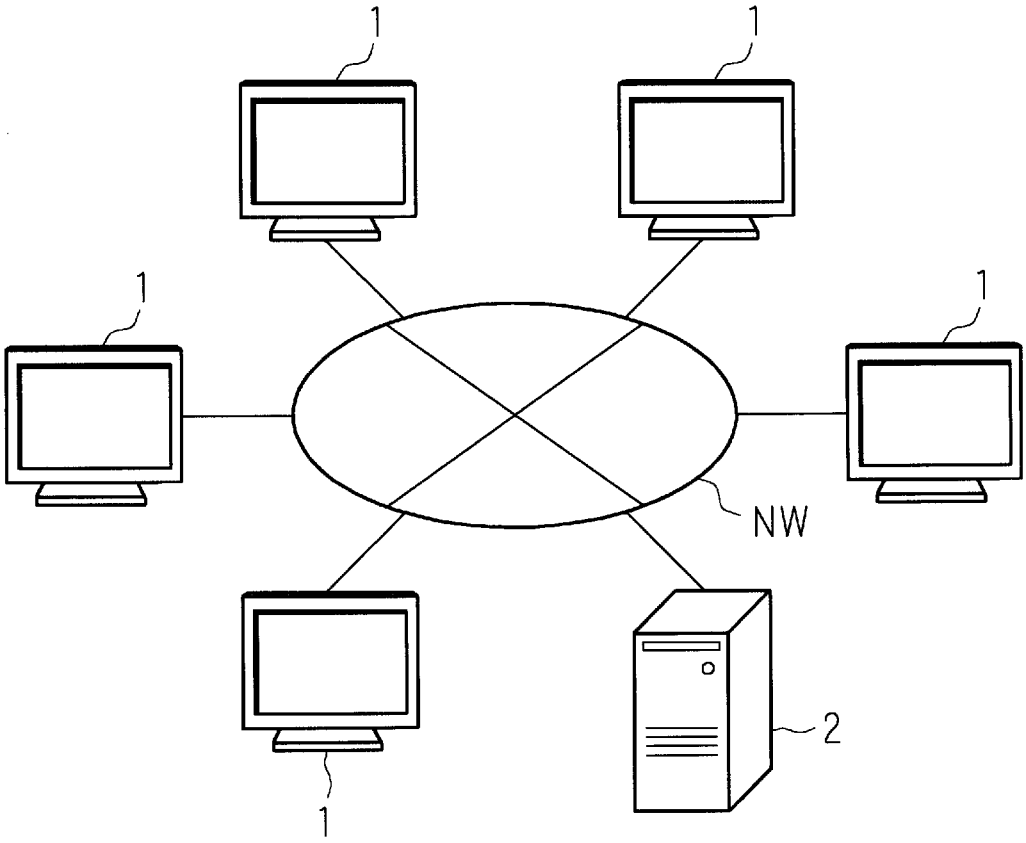
受信した夫々の結果情報及び夫々の加重値に基づいて、前記一のノード装置を認証させる手順と

を実行させることを特徴とするコンピュータプログラム。

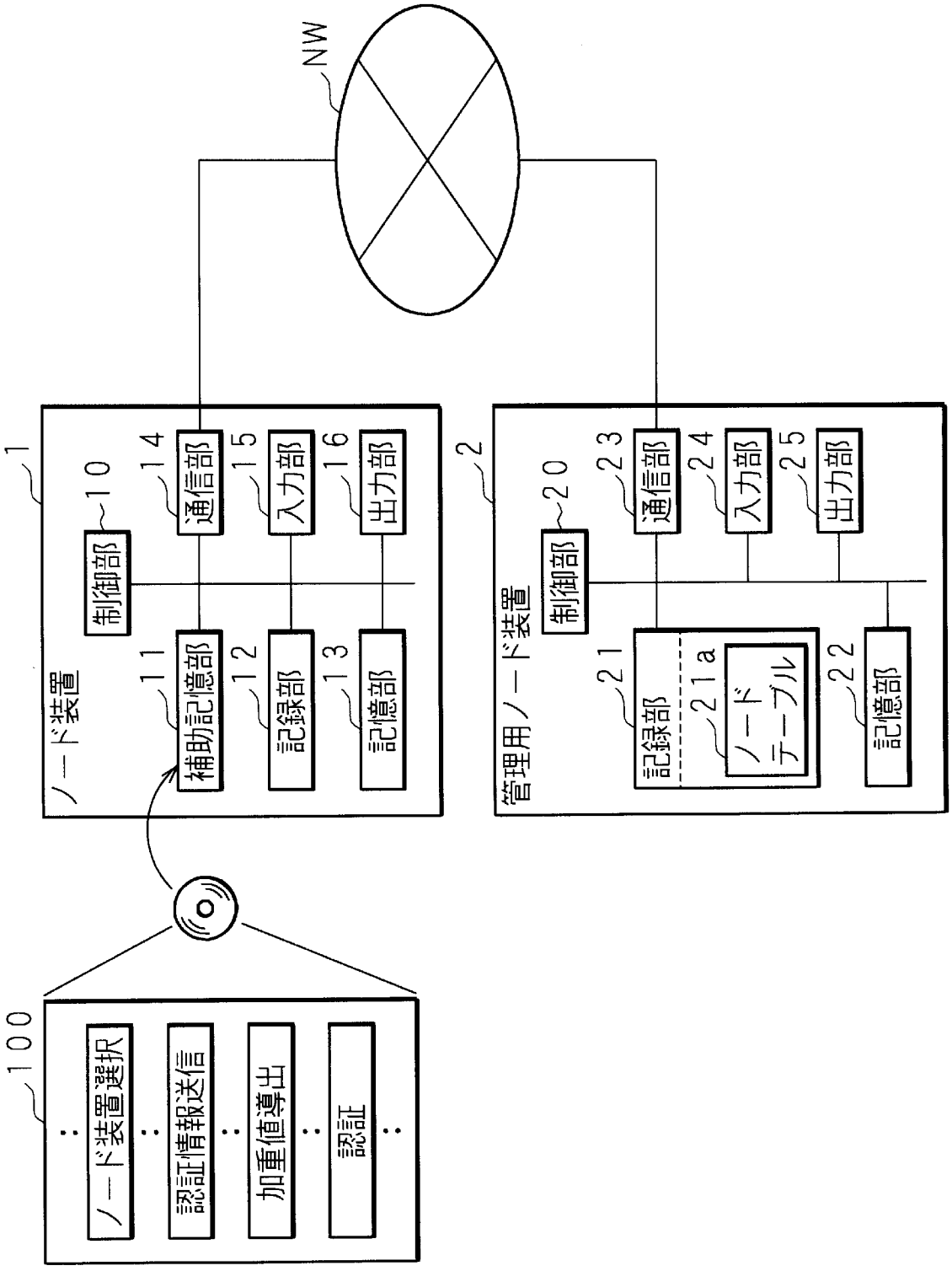
[図1]



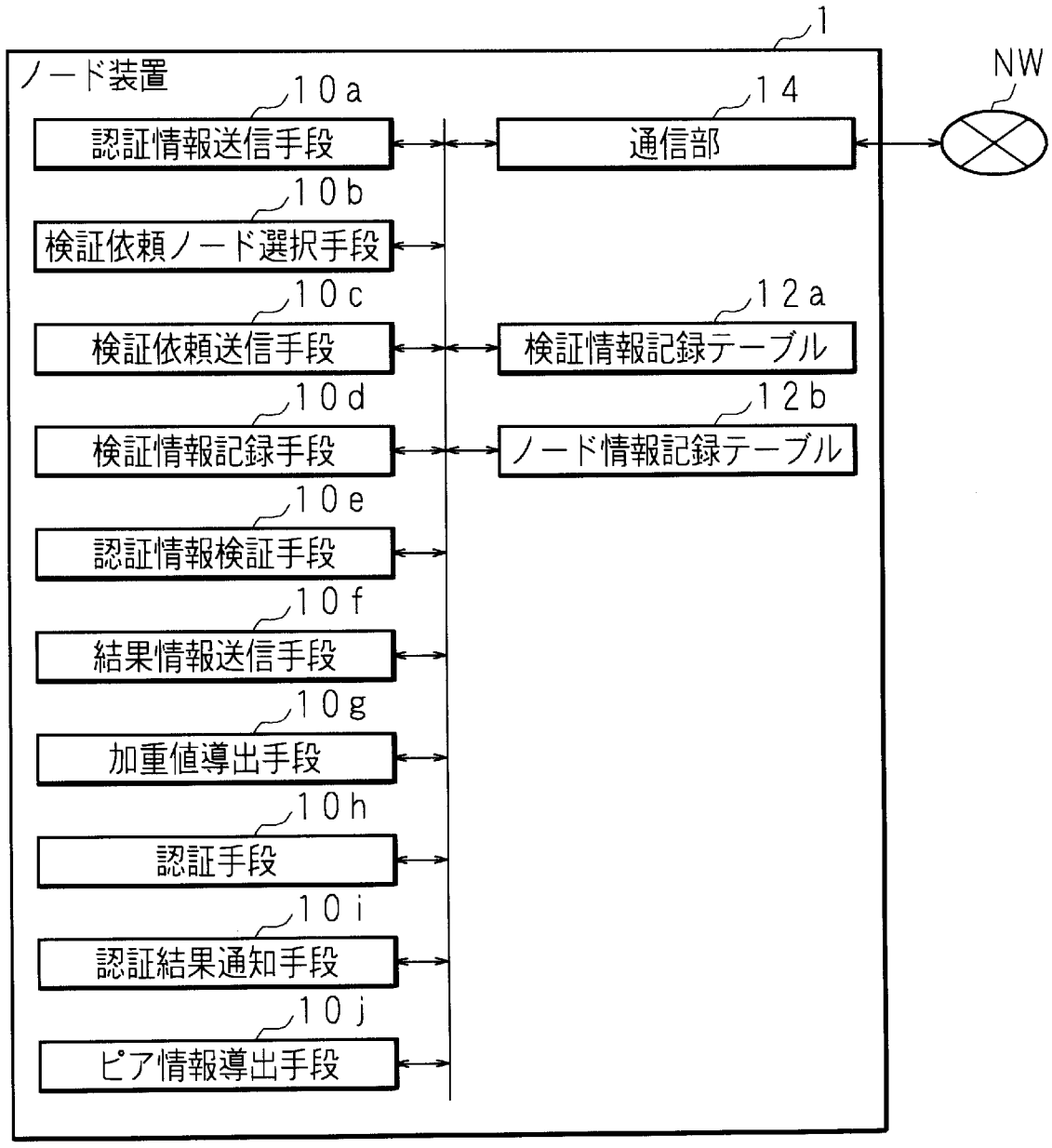
[図2]



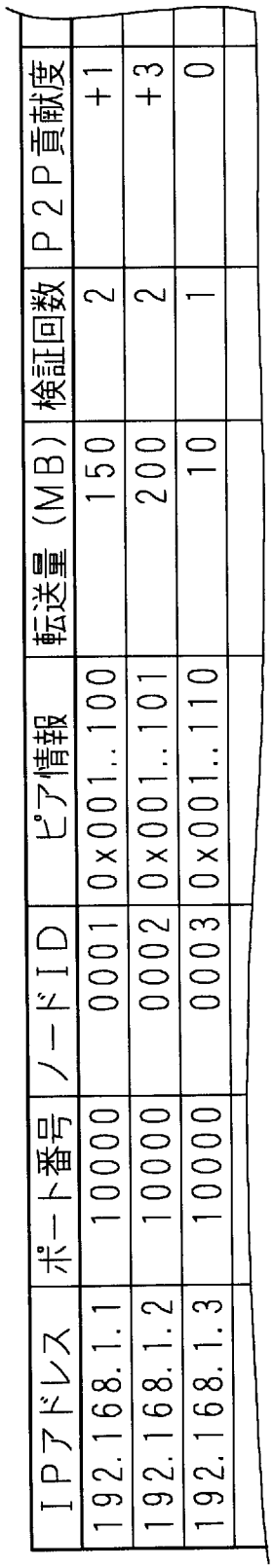
[図3]


NW
1
ノード装置
制御部
10
通信部
14
入力部
15
出力部
16
補助記憶部
11
記録部
12
記憶部
13
2
管理用ノード装置
制御部
20
通信部
23
入力部
24
出力部
25
記録部
21
21a
ノードテーブル
記憶部
22
100
ノード装置選択
認証情報送信
加重値導出
認証

[図4]

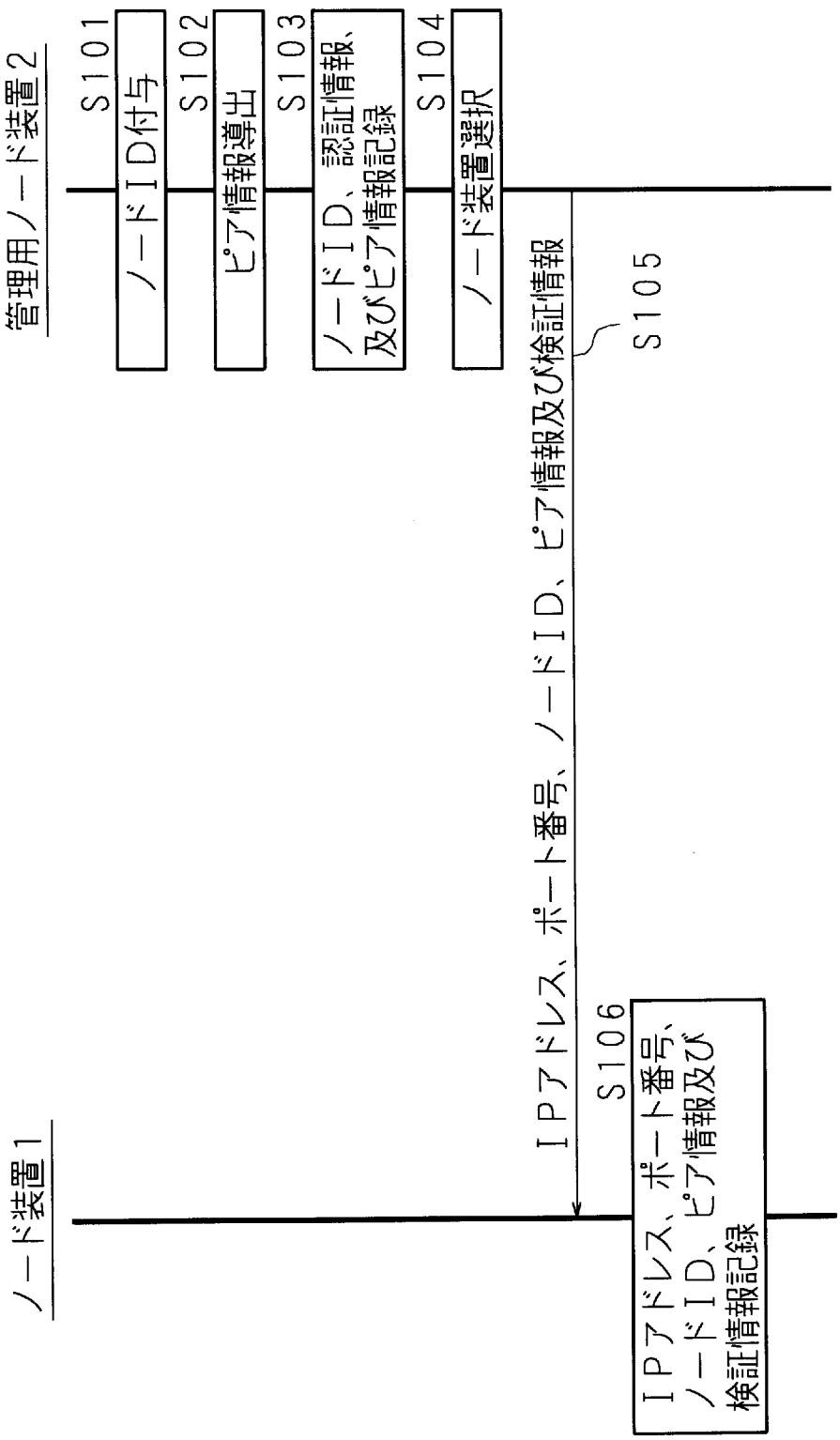

1
ノード装置
NW
10a
認証情報送信手段
14
通信部
10b
検証依頼ノード選択手段
10c
検証依頼送信手段
12a
検証情報記録テーブル
10d
検証情報記録手段
12b
ノード情報記録テーブル
10e
認証情報検証手段
10f
結果情報送信手段
10g
加重値導出手段
10h
認証手段
10i
認証結果通知手段
10j
ピア情報導出手段

[図5]

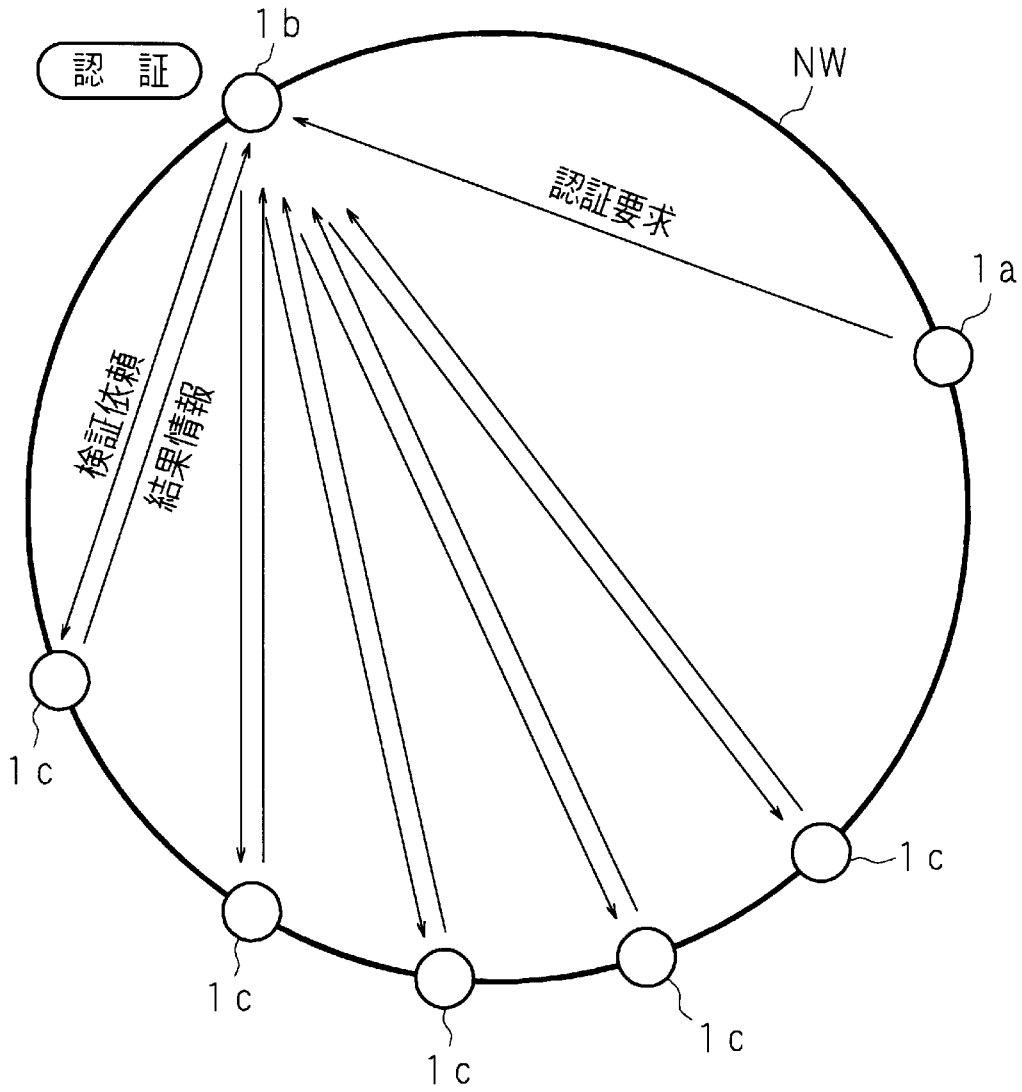


IPアドレス	ポート番号	ノードID	ピア情報	転送量（MB）	検証回数	P2P貢献度
192.168.1.1	10000	0001	0x001..100	150	2	+1
192.168.1.2	10000	0002	0x001..101	200	2	+3
192.168.1.3	10000	0003	0x001..110	10	1	0

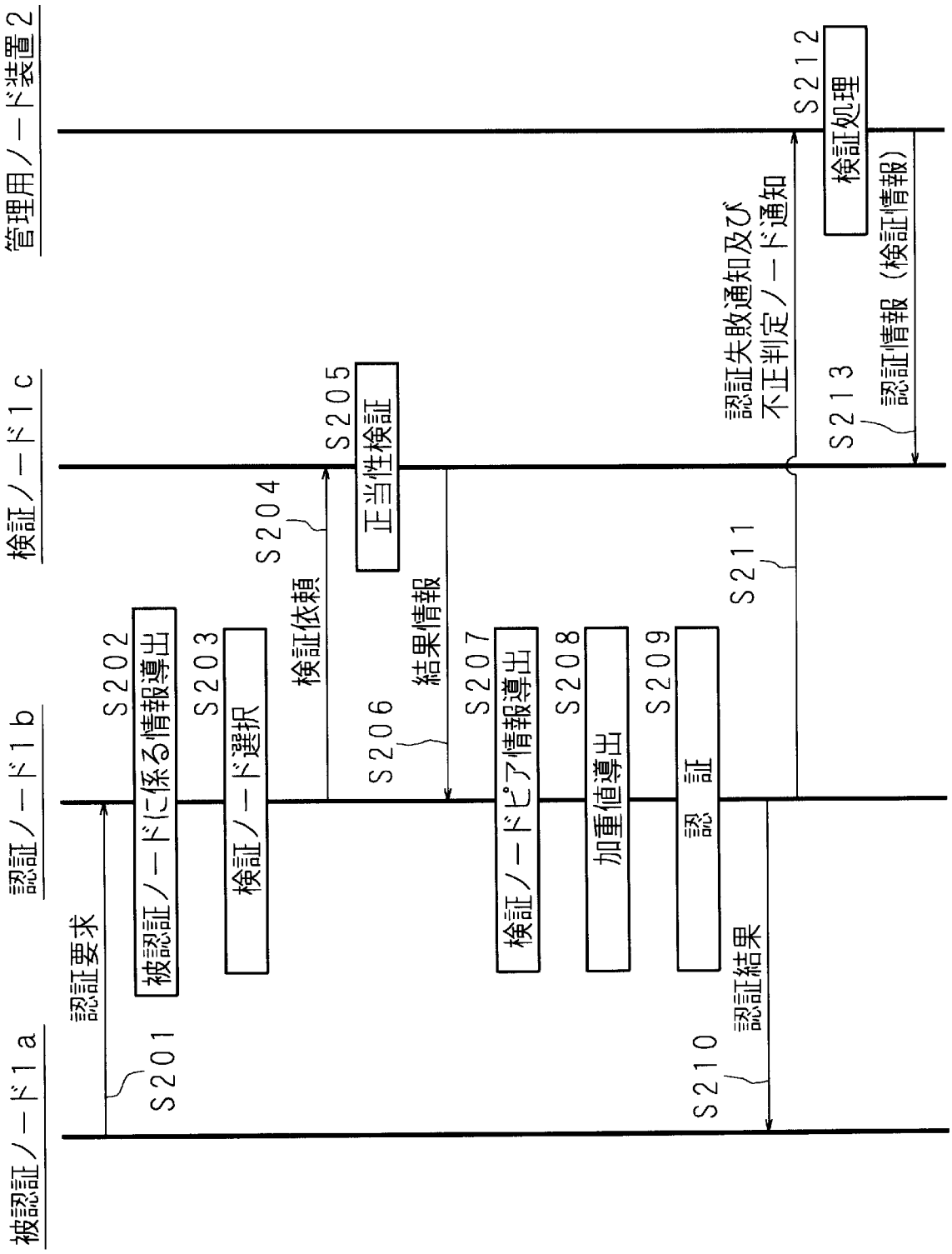
[図6]


管理用ノード装置2
ノード装置1
S101
ノードID付与
S102
ピア情報導出
S103
ノードID、認証情報、及びピア情報記録
S104
ノード装置選択
IPアドレス、ポート番号、ノードID、ピア情報及び検証情報
S105
S106
IPアドレス、ポート番号、ノードID、ピア情報及び検証情報記録

[図7]



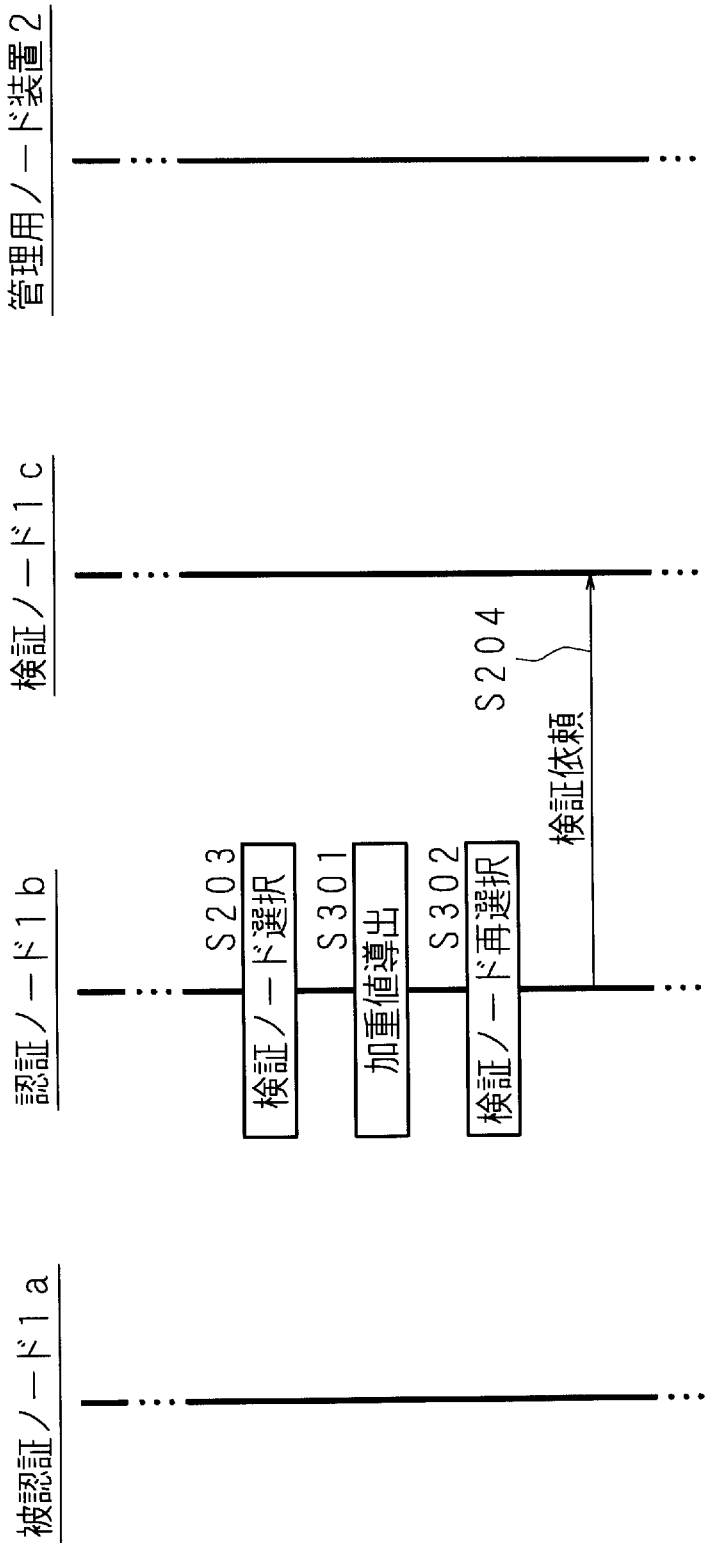
[図8]


被認証ノード1a
認証ノード1b
検証ノード1c
管理用ノード装置2
認証要求
S201
S202
被認証ノードに係る情報導出
S203
検証ノード選択
S204
検証依頼
S205
正当性検証
S206
結果情報
S207
検証ノードピア情報導出
S208
加重値導出
S209
認証
S210
認証結果
S211
認証失敗通知及び
不正判定ノード通知
S212
検証処理
S213
認証情報（検証情報）

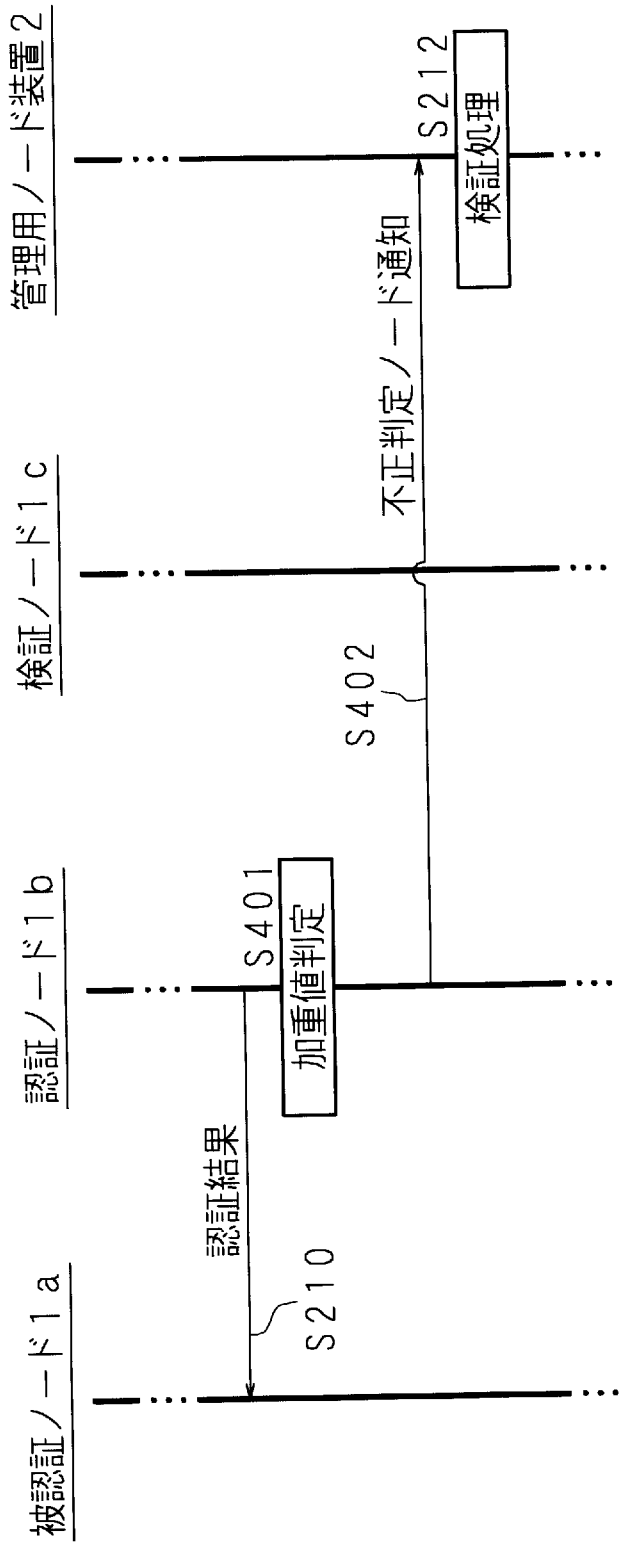
[図9]

	信頼性１位	信頼性２位	信頼性３位	信頼性４位	信頼性５位
例　1	0.5	0.25	0.25	−	−
例　2	0.5	0.5	−	−	−
例　3	0.4	0.3	0.2	0.1	−

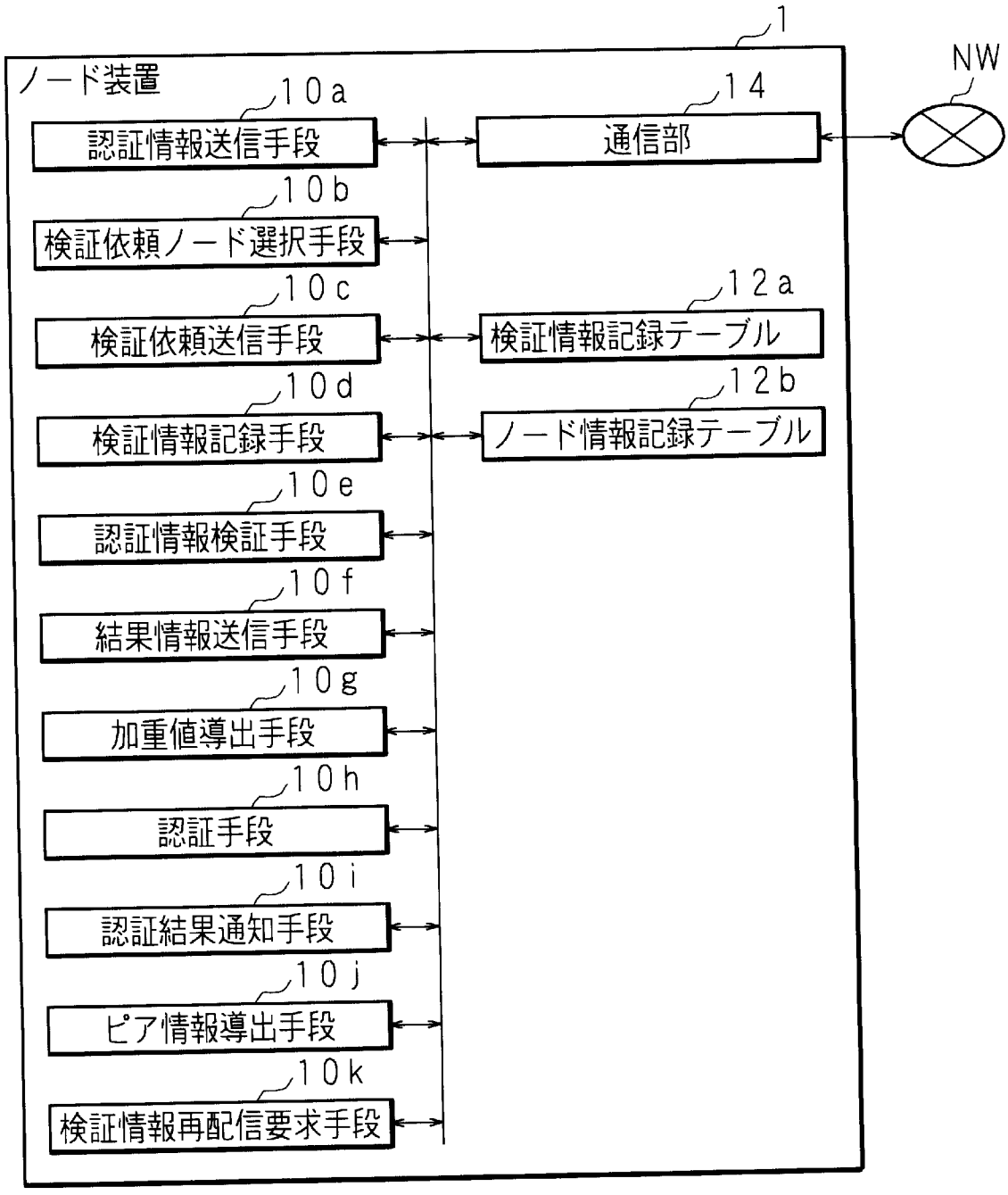
[図10]


被認証ノード1a
認証ノード1b
検証ノード1c
管理用ノード装置2
S203
検証ノード選択
S301
加重値導出
S302
検証ノード再選択
S204
検証依頼

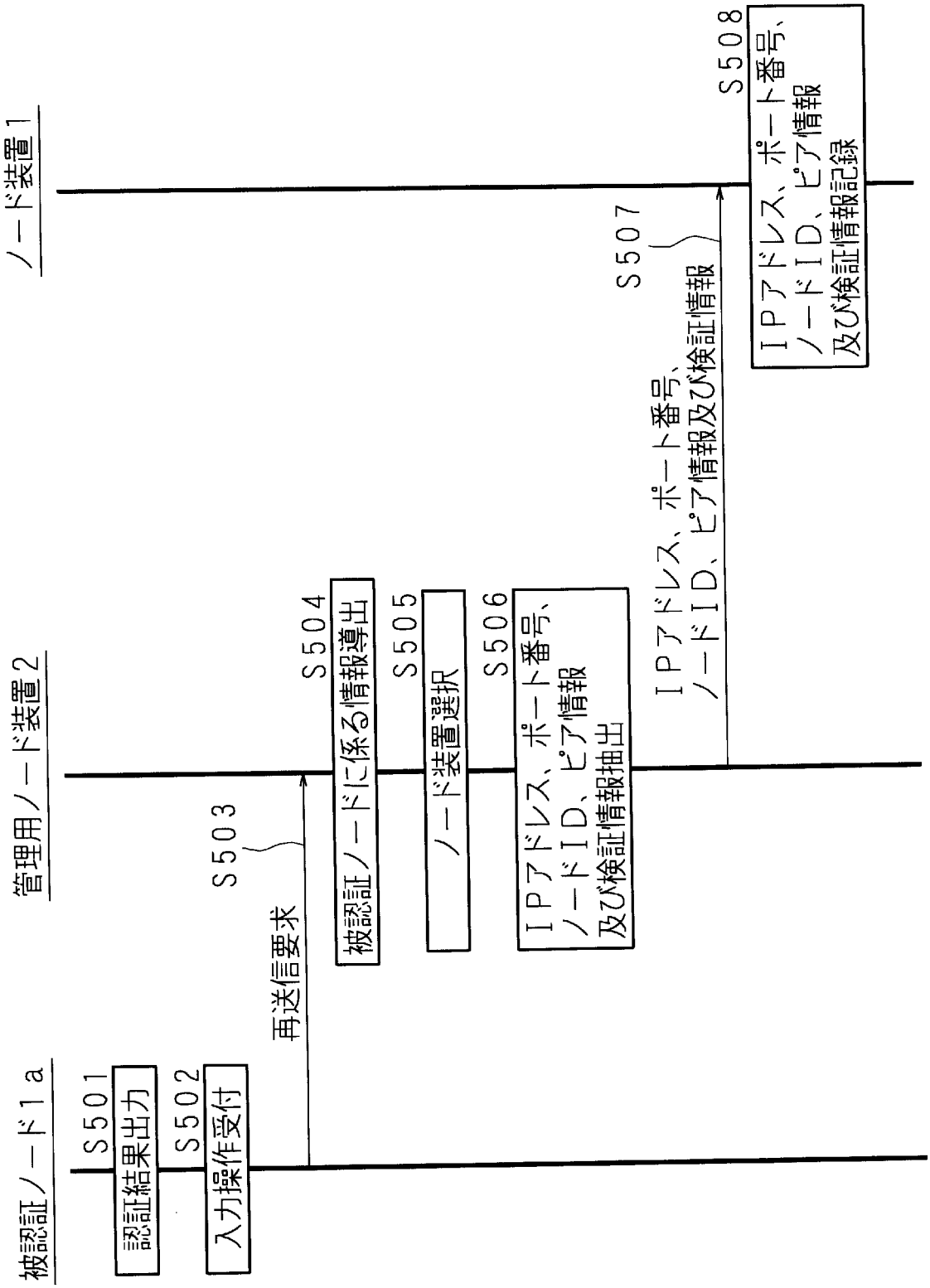
[図11]


被認証ノード1a
認証ノード1b
検証ノード1c
管理用ノード装置2
認証結果
S210
S401
加重値判定
S402
不正判定ノード通知
S212
検証処理

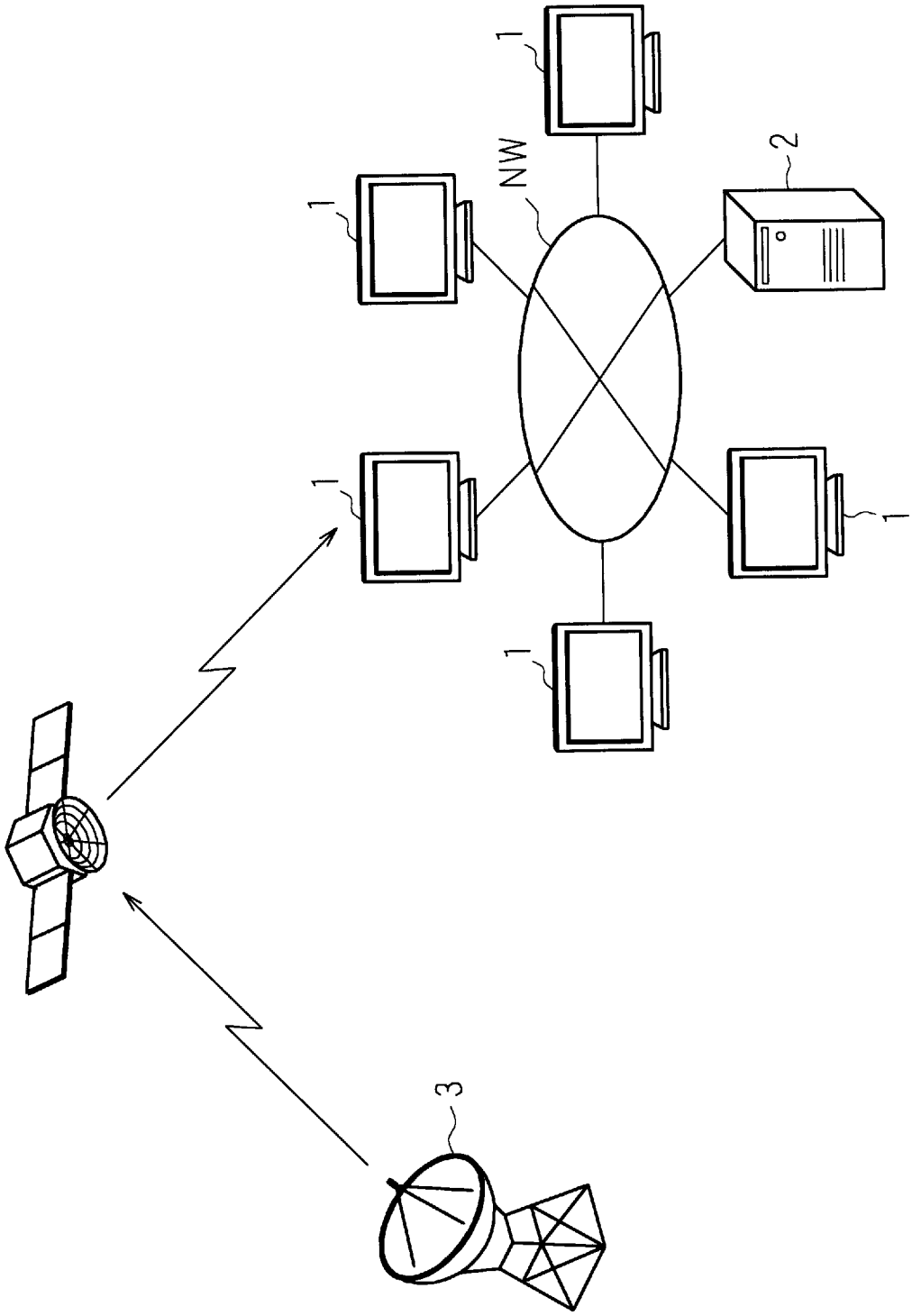
[図12]


1
NW
ノード装置
10a
認証情報送信手段
14
通信部
10b
検証依頼ノード選択手段
10c
検証依頼送信手段
12a
検証情報記録テーブル
10d
検証情報記録手段
12b
ノード情報記録テーブル
10e
認証情報検証手段
10f
結果情報送信手段
10g
加重値導出手段
10h
認証手段
10i
認証結果通知手段
10j
ピア情報導出手段
10k
検証情報再配信要求手段

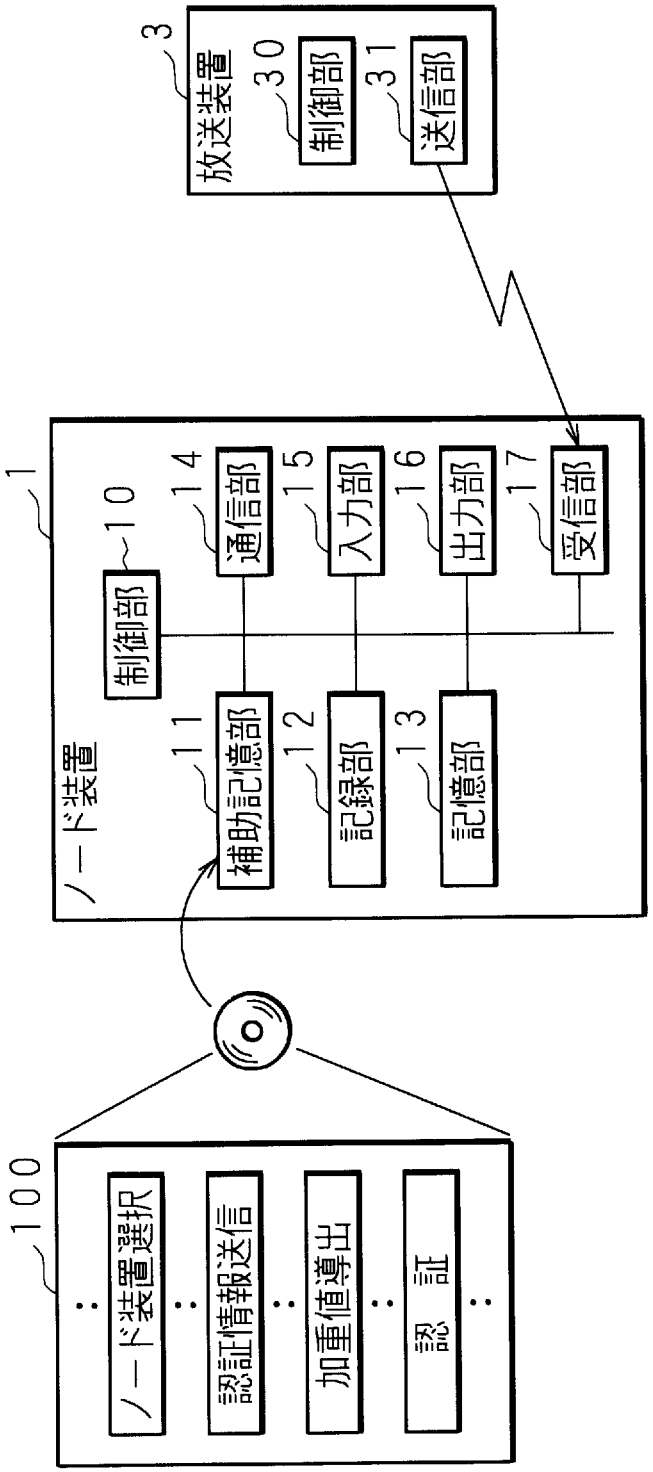
[図13]


被認証ノード1a
管理用ノード装置2
ノード装置1
S501
認証結果出力
S502
入力操作受付
S503
再送信要求
S504
被認証ノードに係る情報導出
S505
ノード装置選択
S506
IPアドレス、ポート番号、
ノードID、ピア情報
及び検証情報抽出
S507
IPアドレス、ポート番号、
ノードID、ピア情報及び検証情報
S508
IPアドレス、ポート番号、
ノードID、ピア情報
及び検証情報記録

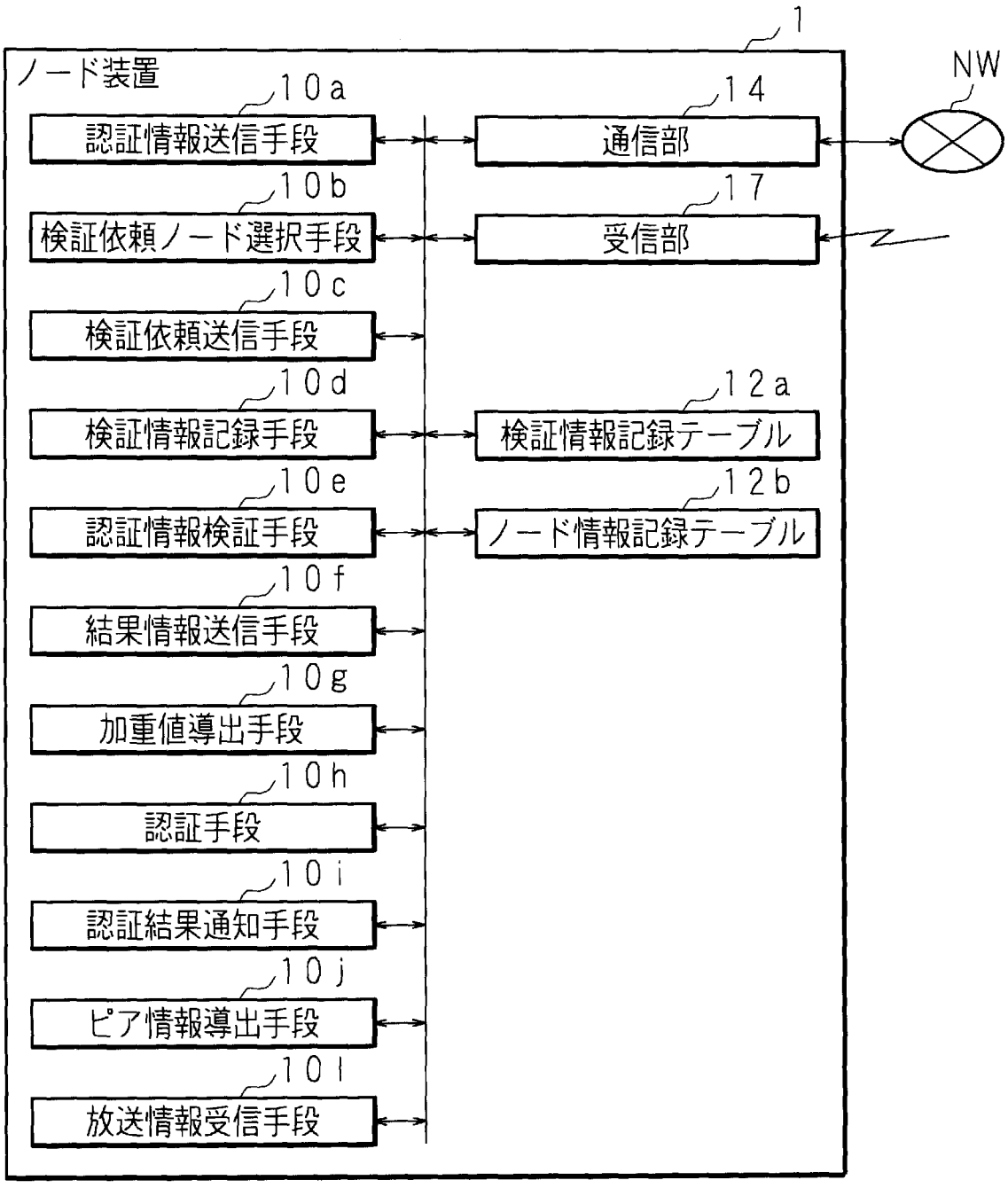
[図14]



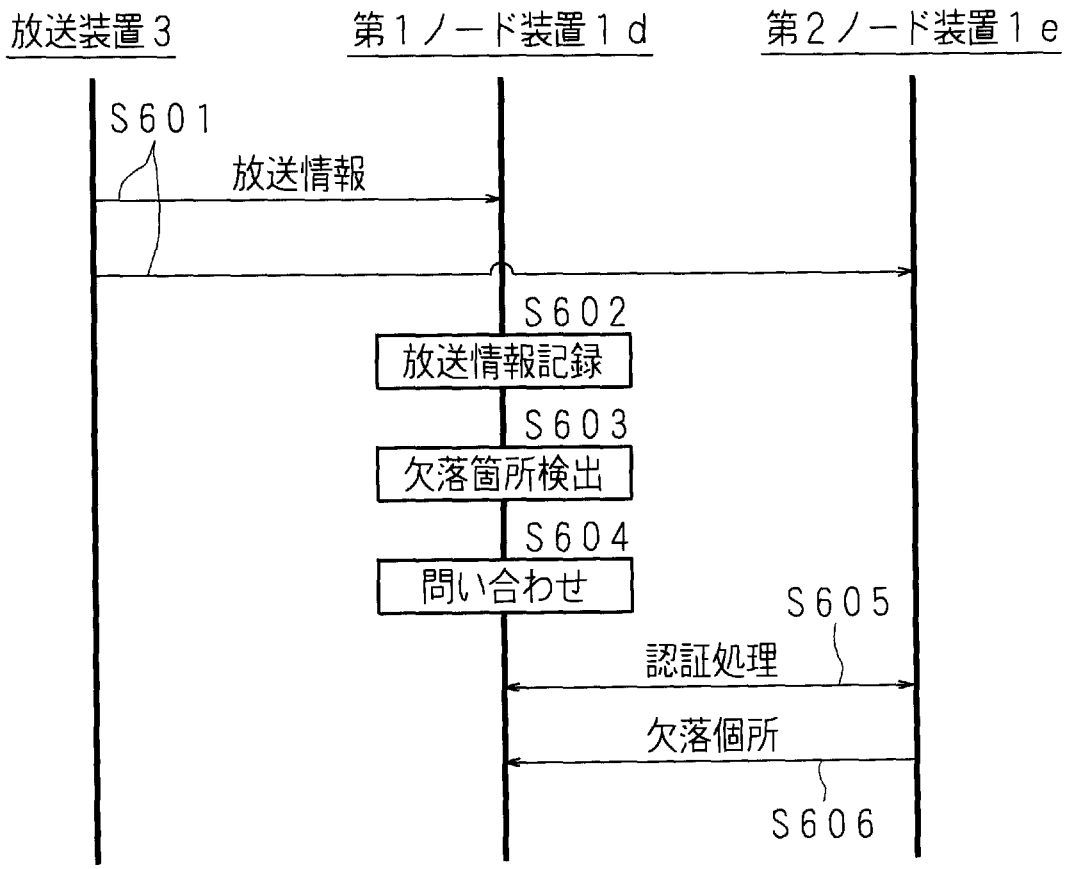
[図15]


3
放送装置
30
制御部
31
送信部
1
ノード装置
10
制御部
14
通信部
15
入力部
16
出力部
17
受信部
11
補助記憶部
12
記録部
13
記憶部
100
ノード装置選択
認証情報送信
加重値導出
認証

[図16]


1
ノード装置
NW
10a
認証情報送信手段
14
通信部
10b
検証依頼ノード選択手段
17
受信部
10c
検証依頼送信手段
10d
検証情報記録手段
12a
検証情報記録テーブル
10e
認証情報検証手段
12b
ノード情報記録テーブル
10f
結果情報送信手段
10g
加重値導出手段
10h
認証手段
10i
認証結果通知手段
10j
ピア情報導出手段
10l
放送情報受信手段

[図17]


放送装置３
第１ノード装置１ｄ
第２ノード装置１ｅ
Ｓ６０１
放送情報
Ｓ６０２
放送情報記録
Ｓ６０３
欠落箇所検出
Ｓ６０４
問い合わせ
Ｓ６０５
認証処理
欠落個所
Ｓ６０６

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/050558

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/20(2006.01)i, *G09C1/00*(2006.01)i, *H04L9/32*(2006.01)i

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)
G06F21/20, G09C1/00, H04L9/32

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 1996-2009
Kokai Jitsuyo Shinan Koho 1971-2009 Toroku Jitsuyo Shinan Koho 1994-2009

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	JP 2006-185171 A (Brother Industries, Ltd.), 13 July, 2006 (13.07.06), Par. Nos. [0002] to [0007], [0023], [0059] to [0077], [0146] to [0151] & WO 2006/070536 A1	1,2,5,7-10 3,4,6
Y A	JP 2007-87081 A (Oki Electric Industry Co., Ltd.), 05 April, 2007 (05.04.07), Par. Nos. [0037] to [0038], [0056] (Family: none)	1,2,5,7-10 3,4,6
A	JP 2007-272583 A (Waseda University), 18 October, 2007 (18.10.07), Abstract; Par. Nos. [0084] to [0094]; Fig. 13 (Family: none)	1-10

☒ 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	Date of mailing of the international search report
12 February, 2009 (12.02.09)	24 February, 2009 (24.02.09)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/050558

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2004-355358 A (Nippon Telegraph And Telephone Corp.), 16 December, 2004 (16.12.04), Abstract; Par. Nos. [0001] to [0005] (Family: none)	1-10
A	Hiroshi SUNAGA, The General Review of P2P[II]: P2P Technologies, THE JOURNAL OF THE INSTITUTE OF ELECTRONICS, INFORMATION AND COMMUNICATION ENGINEERS, 01 October, 2004 (01.10.04), Vol.87, No.10, pages 887 to 896.	1-10

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００９／０５０５５８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/20(2006.01)i, G09C1/00(2006.01)i, H04L9/32(2006.01)i

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.　G06F21/20, G09C1/00, H04L9/32

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	１９７１－２００９年
日本国実用新案登録公報	１９９６－２００９年
日本国登録実用新案公報	１９９４－２００９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	JP 2006-185171 A (ブラザー工業株式会社) 2006.07.13, 段落【0002】-【0007】,【0023】,【0059】-【0077】,【0146】-【0151】 & WO 2006/070536 A1	1,2,5,7-10 3,4,6
Y A	JP 2007-87081 A (沖電気工業株式会社) 2007.04.05, 段落【0037】-【0038】,【0056】（ファミリーなし）	1,2,5,7-10 3,4,6

☑　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 １２．０２．２００９	国際調査報告の発送日 ２４．０２．２００９
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）　５Ｓ　３１４５ 赤穂　州一郎 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
A	JP 2007-272583 A (学校法人早稲田大学) 2007.10.18, 要約, 段落【0084】-【0094】, 図13 (ファミリーなし)	1-10
A	JP 2004-355358 A (日本電信電話株式会社) 2004.12.16, 要約, 段落【0001】-【0005】 (ファミリーなし)	1-10
A	須永　宏　Hiroshi　SUNAGA, Ｐ２Ｐ総論［ＩＩ］－Ｐ２Ｐテクノロジー－　The General Review of P2P[II]: P2P Technologies, 電子情報通信学会誌　第８７巻　第１０号　THE JOURNAL OF THE INSTITUTE OF ELECTRONICS,INFORMATION AND COMMUNICATION ENGINEERS, 2004.10.01, 第87巻, p.887-896.	1-10