(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3999527号
(P3999527)
(45)発行日　平成19年10月31日(2007.10.31)　(24)登録日　平成19年8月17日(2007.8.17)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 675B
H04L 9/08 (2006.01)　　H04L 9/00 601F

請求項の数 15　(全 20 頁)

(21)出願番号　特願2002-38928(P2002-38928)
(22)出願日　平成14年2月15日(2002.2.15)
(65)公開番号　特開2003-244136(P2003-244136A)
(43)公開日　平成15年8月29日(2003.8.29)
審査請求日　平成17年2月10日(2005.2.10)

(73)特許権者　501381642
株式会社　アンクル
東京都千代田区神田須田町１丁目１０番８号
(73)特許権者　398069333
株式会社ビットメディア
東京都渋谷区渋谷２－７－５
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100092196
弁理士　橋本　良郎
(74)代理人　100091351
弁理士　河野　哲

最終頁に続く

(54)【発明の名称】コンピュータネットワークの認証方法及びデータ配信方法

(57)【特許請求の範囲】

【請求項１】

コンピュータネットワーク上に接続された複数のノード間の認証機能を実現し、暗号化鍵データと復号化鍵データとを組として使用する公開鍵暗号方式を利用する認証方法であって、

前記各ノードは、データを送信する上流ノード、データを受信する下流ノード、または下流ノードであって、かつ上流ノードとしても機能する中継ノードのいずれかとして動作するように構成されて、

前記復号化鍵データを前記上流ノードに対して提供し、前記暗号化鍵データを使用して正当な下流ノードを識別するノード識別情報を含む認証用情報を暗号化した接続認証用鍵データを前記下流ノードまたは前記中継ノードに対して提供するための鍵データ提供手段を有し、

下流ノードは、前記鍵データ提供手段から所定の手順で取得した前記接続認証用鍵データを接続要求対象の上流ノードに送信するステップと、

上流ノードは、前記鍵データ提供手段から取得した前記復号化鍵データを使用して下流ノードから受信した前記接続認証用鍵データを復号化し、当該復号化された接続認証用鍵データに含まれる認証用情報を使用して当該下流ノードに対する認証処理を実行するステップと、

中継ノードは、下流ノードとして他の上流ノードから取得した前記復号化鍵データを使用して他の下流ノードから取得した前記接続認証用鍵データを復号化し、当該復号化され

た接続認証用鍵データに含まれる認証用情報を使用して当該他の下流ノードに対する認証処理を実行するステップと
を具備したことを特徴とする認証方法。
【請求項２】
前記鍵データ提供手段は、
前記コンピュータネットワークに接続された特定ノードまたは鍵配付用サーバから構成されて、
前記復号化鍵データを前記公開鍵データとして、また前記暗号化鍵データを秘密鍵データとして保管し、
前記上流ノードからの要求に応じて前記復号化鍵データを送信し、
前記下流ノードからの要求に応じて、前記暗号化鍵データにより当該下流ノードのノード識別情報を含む認証用情報を暗号化した前記接続認証用鍵データを生成し提供するように構成されていることを特徴とする請求項１に記載の認証方法。
【請求項３】
特定の上流ノードのみが前記鍵データ提供手段から前記復号化鍵データを提供されて、
前記中継ノードは、前記特定の上流ノードから前記復号化鍵データを受信し、さらに相対的に下流ノードとなる他の中継ノードに当該復号化鍵データを送信するように構成されていることを特徴とする請求項１または請求項２のいずれか１項に記載の認証方法。
【請求項４】
前記下流ノード及び前記中継ノードはそれぞれ、前記鍵データ提供手段から決済処理を含む所定の手順で前記接続認証用鍵データを取得することを特徴とする請求項１から請求項３のいずれか１項に記載の認証方法。
【請求項５】
前記上流ノード又は前記中継ノードは、
下流ノードからの接続要求に応じて、当該下流ノードから送信された平文の認証用情報と前記接続認証用鍵データとを受信し、
前記鍵データ提供手段あるいは前記上流ノードから予め取得した前記復号化鍵データを使用して前記接続認証用鍵データから復号化した認証用情報と、前記平文の認証用情報との照合結果が一致しているときに、当該下流ノードが正当な下流ノードであると認定することを特徴とする請求項１から請求項４のいずれか１項に記載の認証方法。
【請求項６】
コンピュータネットワーク上に接続された複数のノード間の認証機能であって、暗号化鍵データと復号化鍵データとを組として使用する公開鍵暗号方式を利用する認証機能を実現するためのプログラムであって、
前記各ノードは、前記プログラムを実行するコンピュータを有し、データを送信する上流ノード、データを受信する下流ノード、または下流ノードであって、更に上流ノードとしても機能する中継ノードのいずれかとして動作するように構成されて、
所定の手順により前記復号化鍵データを前記上流ノードに対して提供し、前記暗号化鍵データを使用して正当な下流ノードを識別するノード識別情報を含む認証用情報を暗号化した接続認証用鍵データを前記下流ノードまたは前記中継ノードに対して提供するための鍵データ提供手段とのデータ送受信機能と、
下流ノードとしては、前記鍵データ提供手段から所定の手順で取得した前記接続認証用鍵データを接続要求対象の上流ノードに送信する機能と、
上流ノードとしては、前記鍵データ提供手段から取得した前記復号化鍵データを使用して下流ノードから受信した前記接続認証用鍵データを復号化し、当該復号化された接続認証用鍵データに含まれる認証用情報を使用して当該下流ノードに対する認証処理を実行する機能と、
中継ノードとしては、下流ノードとして他の上流ノードから取得した前記復号化鍵データを使用して他の下流ノードからの前記接続認証用鍵データを復号化し、当該復号化された接続認証用鍵データに含まれる認証用情報を使用して当該他の下流ノードに対する認証

処理を実行する機能と
を前記コンピュータに実現させるためのプログラム。
【請求項７】
前記上流ノード又は前記中継ノードとしては、
下流ノードからの接続要求に応じて、当該下流ノードから送信された平文の認証用情報と前記接続認証用鍵データとを受信する機能と、
前記鍵データ提供手段あるいは前記上流ノードから予め取得した前記復号化鍵データを使用して前記接続認証用鍵データから復号化した認証用情報と、前記平文の認証用情報との照合結果が一致しているときに、当該下流ノードが正当な下流ノードであると認定する機能とを前記コンピュータに実現させることを特徴とする請求項６に記載のプログラム。
【請求項８】
コンピュータネットワーク上に接続された複数のノード間の認証処理を伴なうデータ分散配信機能を実現するデータ配信方法であって、
前記各ノードは、データの配信源となる上流ノード、データを受信する下流ノード、または相対的に下流ノードまたは上流ノードとして機能する中継ノードのいずれかとして動作するように構成されて、
暗号化鍵データと復号化鍵データとを組として使用する公開鍵暗号方式において、所定の手順により前記復号化鍵データを前記上流ノードに対して提供し、前記暗号化鍵データを使用して、正当な下流ノードを識別するノード識別情報及び配信対象のデータを識別するデータ識別情報を含む認証用情報を暗号化した接続認証用鍵データを前記下流ノードまたは前記中継ノードに対して提供するための鍵データ提供手段を有し、
前記上流ノードは、
前記下流ノード又は前記中継ノードからのデータ配信要求に応じて、前記鍵データ提供手段から取得した前記復号化鍵データを使用して、前記下流ノード又は前記中継ノードから受信した前記接続認証用鍵データを復号化するステップと、
前記復号化ステップにより復号化された前記認証用情報と、前記下流ノード又は前記中継ノードから受信した平文の前記認証用情報との照合を実行するステップと、
前記照合ステップにより照合結果が一致したときに、配信要求を行なった下流ノード又は中継ノードを正当なノードであると認定し、前記認証用情報に含まれる前記データ識別情報に対応するデータを当該正当なノードに配信するステップと
を有する処理を実行するように構成されているデータ配信方法。
【請求項９】
前記上流ノードは、前記照合ステップにより正当であると認定された中継ノードに対して、要求に応じて復号化鍵データを配信するステップを実行し、
前記中継ノードは、
前記下流ノード又は相対的に下流ノードである他の中継ノードからのデータ配信要求に応じて、前記上流ノードから取得した前記復号化鍵データを使用して、前記下流ノード又は前記他の中継ノードから受信した前記接続認証用鍵データを復号化するステップと、
前記復号化ステップにより復号化された前記認証用情報と、前記下流ノード又は前記他の中継ノードから受信した平文の前記認証用情報との照合を実行するステップと、
前記照合ステップにより照合結果が一致したときに、配信要求を行なった下流ノード又は他の中継ノードを正当なノードであると認定し、前記認証用情報に含まれる前記データ識別情報に対応するデータで、前記上流ノードから配信されたデータを当該正当なノードに配信するステップと
を有する処理を実行するように構成されている請求項８に記載のデータ配信方法。
【請求項１０】
コンピュータネットワーク上に接続された複数のノード間の認証処理を伴なうデータ分散配信機能を実現するプログラムであって、
前記各ノードは、前記プログラムを実行するコンピュータを有し、データの配信源となる上流ノード、データを受信する下流ノード、または相対的に下流ノードまたは上流ノー

ドとして機能する中継ノードのいずれかとして動作するように構成されて、
暗号化鍵データと復号化鍵データとを組として使用する公開鍵暗号方式において、所定の手順により前記復号化鍵データを前記上流ノードに対して提供し、前記暗号化鍵データを使用して、正当な下流ノードを識別するノード識別情報及び配信対象のデータを識別するデータ識別情報を含む認証用情報を暗号化した接続認証用鍵データを前記下流ノードまたは前記中継ノードに対して提供するための鍵データ提供手段とのデータ送受信機能と、
前記上流ノードとしては、
前記下流ノード又は前記中継ノードからのデータ配信要求に応じて、前記鍵データ提供手段から取得した前記復号化鍵データを使用して、前記下流ノード又は前記中継ノードから受信した前記接続認証用鍵データを復号化する機能と、
前記復号化機能により復号化された前記認証用情報と、前記下流ノード又は前記中継ノードから受信した平文の前記認証用情報との照合を実行する機能と、
前記照合機能により照合結果が一致したときに、配信要求を行なった下流ノード又は中継ノードを正当なノードであると認定し、前記認証用情報に含まれる前記データ識別情報に対応するデータを当該正当なノードに配信する機能と
を前記コンピュータに実現させるためのプログラム。
【請求項１１】
前記上流ノードとしては、前記照合機能により正当であると認定された中継ノードに対して、要求に応じて復号化鍵データを配信する機能を前記コンピュータに実現させて、
前記中継ノードとしては、
前記下流ノード又は相対的に下流ノードである他の中継ノードからのデータ配信要求に応じて、前記上流ノードから取得した前記復号化鍵データを使用して、前記下流ノード又は前記他の中継ノードから受信した前記接続認証用鍵データを復号化する機能と、
前記復号化機能により復号化された前記認証用情報と、前記下流ノード又は前記他の中継ノードから受信した平文の前記認証用情報との照合を実行する機能と、
前記照合機能により照合結果が一致したときに、配信要求を行なった下流ノード又は他の中継ノードを正当なノードであると認定し、前記認証用情報に含まれる前記データ識別情報に対応するデータで、前記上流ノードから配信されたデータを当該正当なノードに配信する機能と
を前記コンピュータに実現させることを特徴とする請求項１０に記載のプログラム。
【請求項１２】
コンピュータネットワーク上に接続された複数のノード間の認証処理を伴なうコンテンツ分散配信機能を実現するコンテンツ配信方法であって、
前記各ノードは、コンテンツ配信サービスを行なう配信源ノード、当該コンテンツ配信サービスを受けるユーザノード、またはコンテンツ配信の中継ノードとして機能する中継ノードのいずれかとして動作するように構成されて、
暗号化鍵データと復号化鍵データとを組として使用する公開鍵暗号方式において、所定の手順により前記復号化鍵データに対応する認証用マスタ鍵データを前記配信源ノードに対して提供し、
かつ前記ユーザノード又は前記中継ノードからの要求に応じて、所定の手順により、前記暗号化鍵データを使用して正当なノードを識別するノード識別情報及び配信対象のコンテンツを識別するコンテンツ識別情報を含む認証用情報を暗号化した電子チケットを前記ユーザノードまたは前記中継ノードに対して提供するための電子チケット提供手段を有し、
前記配信源ノードは、
前記ユーザノード又は前記中継ノードからのコンテンツ配信要求に応じて、前記電子チケット提供手段から取得した前記認証用マスタ鍵データを使用して、前記ユーザノード又は前記中継ノードから受信した前記電子チケットを復号化するステップと、
前記復号化ステップにより復号化された前記認証用情報と、前記ユーザノード又は前記中継ノードから受信した平文の前記認証用情報との照合を実行するステップと、

前記照合ステップにより照合結果が一致したときに、配信要求を行なったユーザノード又は中継ノードを正当なノードであると認定し、前記認証用情報に含まれる前記コンテンツ識別情報に対応するコンテンツを当該正当なノードに配信するステップと
を有する処理を実行するように構成されているコンテンツ配信方法。
【請求項１３】
前記配信源ノードとしては、前記照合ステップにより正当であると認定された中継ノードに対して、要求に応じて前記認証用マスタ鍵データを配信する機能を有し、
前記中継ノードとしては、
前記ユーザノードからのコンテンツ配信要求に応じて、前記配信源ノードから取得した前記認証用マスタ鍵データを使用して、前記ユーザノードから受信した前記電子チケットを復号化するステップと、
前記復号化ステップにより復号化された前記認証用情報と、前記ユーザノードから受信した平文の前記認証用情報との照合を実行するステップと、
前記照合ステップにより照合結果が一致したときに、配信要求を行なったユーザノードを正当なノードであると認定し、前記認証用情報に含まれる前記コンテンツ識別情報に対応するコンテンツで、前記配信源ノードから配信されたコンテンツを当該正当なノードに配信するステップと
を有する処理を実行するように構成されている請求項１２に記載のコンテンツ配信方法。
【請求項１４】
前記接続認証用鍵データは、配布期間または配布時間の制限が設定されていることを特徴とする請求項１から請求項５のいずれか１項に記載の認証方法。
【請求項１５】
前記中継ノードは、コンテンツ配信サービスを受ける前記ユーザノードの機能を有することを特徴とする請求項１２に記載のコンテンツ配信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、一般的にはコンピュータネットワークでの認証方法に関し、特に、複数のノード間で認証機能を分散する方法に関する。
【０００２】
【従来の技術】
近年、インターネットを代表とする情報通信ネットワーク又はコンピュータネットワークの環境下において、ブロードバンド化の推進により、主として動画（映像）や音声のコンテンツ情報の伝送を容易に行なうことが可能になりつつある。ブロードバンド化のネットワーク環境としては、例えばＡＤＳＬ（asymmetric digital subscriber line）伝送方式やＣＡＴＶ（cable television）ネットワークを利用した有線通信方式以外に、携帯電話などの無線通信方式（移動体通信方式）によるネットワーク環境も含まれる。
【０００３】
ところで、インターネットに接続されるユーザ端末としては、パーソナルコンピュータ、ディジタル情報機器、携帯電話（ＰＨＳも含む）、あるいは無線通信機能を有する携帯型情報端末（ＰＤＡ：personal digital assistant）等が含まれる。ブロードバンド化のネットワーク環境下では、これらのユーザ端末により、例えばストリームデータを受信して、ユーザの違和感を伴なうことなく、動画や音声のコンテンツ情報を再生することが可能となる。
【０００４】
従来では、インターネットによる情報サービスや、個人間の情報交換では、文字情報や静止画像が主体であり、動画や音声などのストリームデータの通信は限定されたものであった。従って、今後、ブロードバンド化のネットワーク環境の普及に伴なって、ストリーム配信サービス事業などのビジネス分野だけでなく、ユーザ間で個人的情報を交換するプライベートの分野でも、ストリームデータの配信が容易になる。

【０００５】
【発明が解決しようとする課題】
一般的に、コンピュータネットワーク環境下においては、例えば動画や音声等のストリームデータの配信を行なうストリーム配信サービス事業などのビジネス分野や、個人的情報を交換するプライベートの分野でも、正当なデータの送受信先を特定するための認証機能が必要不可欠である。
【０００６】
従来から、コンピュータネットワークでの認証機能を実現するための各種の方式が開発または提案されている。従来の認証方式は、例えばプロバイダやサービス事業者等が運営するサーバの管理下で機能することが一般的である。例えば、インターネット上において、仲介サーバにより、ユーザ端末間でのファイル交換を仲介するための情報サービスが実現されている。この場合、各ユーザ端末の認証処理は、仲介サーバにより実行されている。
【０００７】
一方、近年では、例えば動画や音声等のストリームデータの配信を行なうストリーム配信サービス事業では、サーバに対する過大負荷が問題になっている。この問題の解決策として、サーバの機能を分散させる技術が注目されている。具体的には、例えばメインサーバと中継サーバとからなるストリームデータの分散配信方式などが提案されている。しかしながら、認証機能は特定のサーバなどによる集中方式が一般的である。即ち、コンピュータネットワーク環境下では、有効な認証機能を含むデータ分散配信方式は、現時点では実現されていない。
【０００８】
そこで、本発明の目的は、インターネットなどのコンピュータネットワーク環境において、有効な認証機能を含むデータ分散配信方式を実現できる認証方法を提供することにある。
【０００９】
【課題を解決するための手段】
本発明の観点は、例えばインターネットのコンピュータネットワーク環境下において、特定のサーバを使用することなく、複数のユーザ端末間で例えばストリームデータなどを分散配信できるデータ分散配信方式に適用できる有効な認証方法に関する。
【００１０】
本発明の観点による認証方法は、コンピュータネットワーク上に接続された複数のノード間の認証機能を実現し、暗号化鍵データと復号化鍵データとを組として使用する公開鍵暗号方式を利用する認証方法であって、
各ノードは、データを送信する上流ノード、データを受信する下流ノード、または下流ノードであって、更に上流ノードとしても機能する中継ノードのいずれかとして動作するように構成されて、
復号化鍵データを上流ノードに対して提供し、暗号化鍵データを使用して正当な下流ノードを識別するノード識別情報を含む認証用情報を暗号化した接続認証用鍵データを下流ノードまたは中継ノードに対して提供するための鍵データ提供手段を有し、
下流ノードは、鍵データ提供手段から所定の手順で取得した接続認証用鍵データを接続要求対象の上流ノードに送信するステップと、上流ノードは、鍵データ提供手段から取得した復号化鍵データを使用して下流ノードから受信した接続認証用鍵データを復号化し、当該復号化された接続認証用鍵データに含まれる認証用情報を使用して当該下流ノードに対する認証処理を実行するステップと、中継ノードは、下流ノードとして他の上流ノードから取得した復号化鍵データを使用して他の下流ノードからの接続認証用鍵データを復号化し、当該復号化された接続認証用鍵データに含まれる認証用情報を使用して当該他の下流ノードに対する認証処理を実行するステップとから構成される。
【００１１】
このような構成の認証方法であれば、公開鍵暗号方式を利用した複数のノード間の接続に関する認証機能を、各ノードに分散させることができる。従って、各ノード間で、例えば

ストリームデータの分散配信を実現するときに、当該データ分散配信に適用する認証機能も分散できる。具体的には、ユーザ端末である上流ノードを配信源として、中継ノード及び下流ノードに対してストリームデータが分散配信される場合に、当該上流ノードから中継ノードを介して、復号化鍵データを分散配信することができる。また、中継ノードは、相対的な上流ノード（最上流ノード又は中継ノード）から取得した復号化鍵データを使用して、接続要求している下流ノードに対する認証処理を実行できる。従って、特定のサーバが集中的に認証処理を実行する方式ではなく、認証機能も分散できるデータ分散配信方式を実現することができる。

【００１２】

なお、鍵データ提供手段は、通常では、例えばサービス業者が運営する鍵配付サーバに相当する。当該サービス業者は、配信源となる上流ノードを操作するユーザとの契約に基づいて、復号化鍵データ及び接続認証用鍵データを配付する。ここで、鍵データ提供手段は、サーバではなく、特定のサービス業者が取り扱う記憶媒体（例えばＣＤ－ＲＯＭ）でもよい。具体的には、復号化鍵データまたは接続認証用鍵データが格納された記憶媒体を、各ノードを操作するユーザが特定のサービス業者から提供される仕組みでもよい。

【００１３】

【発明の実施の形態】

以下図面を参照して、本発明の実施の形態を説明する。

【００１４】

（システムの基本的構成）

図２は、本実施形態に関するストリーム分散配信システムの概念を示す図である。

【００１５】

本システムは、特にブロードバンドのインターネット等のコンピュータネットワーク環境を想定し、当該ネットワークに接続された複数のノード１０により、例えばストリームデータを分散配信する構成である。ここで、ストリームデータとは、動画（映像）や音声等のコンテンツ情報を含む連続的ディジタルデータを意味する。

【００１６】

また、ノード１０とは、ネットワークに接続した装置（デバイス）の総称であり、いわゆるユーザ端末（クライアント）、サーバ、ルータ等の中継装置、データ（パケット）交換装置等を意味する。ユーザ端末としては、具体的には、パーソナルコンピュータ、ディジタル情報機器、携帯電話（ＰＨＳも含む）、あるいは無線通信機能を有する携帯型情報端末（ＰＤＡ）等のデバイスを意味する。また、ユーザ端末としては、前記のデバイス単体だけでなく、ルータや無線ＬＡＮ（local area network）により構成されるシステムを意味する場合もある。

【００１７】

本システムでは、例えば配信源となる上流ノード１０（Ａ）は、相対的に下流ノードとなるノード１０（Ｂ）にストリームデータを送出する。ノード１０（Ｂ）は、他の下流ノード１０に対して相対的に上流ノードとして動作し、受信したストリームデータを再生（視聴）すると共に、他の下流ノード１０に中継する。この場合、ノード１０（Ｂ）は、許容負荷が許せば、複数の下流ノード１０に対してストリームデータを中継する。

【００１８】

要するに、本システムは、インターネット上に接続された各ノード１０が上流ノードまたは下流ノードとして動作し、上流ノードから下流ノードへと例えばストリームデータの中継を実行する。このようなシステムにより、高性能のデータ配信用サーバを要することなく、例えば低コストのパーソナルコンピュータなどにより、データ分散配信機能を実現することができる。ここで、上流ノードとは、自ノードに対して上流であり、ストリームデータの送出元ノード（配信源ノード）または中継ノードである。また、下流ノードとは、自ノードから見てストリームデータの送出先ノードである。下流ノードは、ストリームデータを受信する受信ノード、または更に下流ノードに対して送出する中継ノードとして機能することができる。

【００１９】
図３は、本システムの具体的構成の一例を示すブロック図である。
【００２０】
本システムの具体的想定としては、多数のユーザ端末であるノード１０や、後述するサーバ２０（ノードの一種）がインターネット１００に接続されて、インターネット１００を介して、ストリーム分散配信系に参加したユーザ端末に対してストリームが配信される構成である。
【００２１】
各ノード１０は、例えばＡＤＳＬ伝送方式やＣＡＴＶネットワーク、または携帯電話などの移動体通信方式（無線通信方式）を使用して、常時接続型の高速回線によりインターネットに接続される環境を想定している。
【００２２】
あるノード１０は、例えばパーソナルコンピュータ（ＰＣ）１１とルータ１２とを有するユーザ端末である。これらのノード１０は、インターネット１００を介して受信したストリームを、例えばＰＣ１１のディスプレイ上に再生し、かつ他の下流ノード１０へ中継する。また、あるノード１０は、例えばＰＣ１１とディジタルビデオカメラ（ＤＶＣ）１３とを有する。このノード１０は上流ノードとして、ＤＶＣ１３により撮影した映像（音声を含む）からなるストリームを、ＰＣ１１にセットされたソフトウェア（同実施形態のメイン構成要素）により送出するユーザ端末である。
【００２３】
（ノードの構成）
サーバ２０を除く各ノード１０に関して、図３を参照して、同実施形態のユーザ端末として動作するノード１０の構成を説明する。
【００２４】
同実施形態のノード１０は、コンピュータ（マイクロプロセッサ）と、当該コンピュータにセットされるソフトウェアとから構成される。ここで、各ノード１０は、全て同一のソフトウェア構成を有し、ストリームの送出、受信、中継、再生、及び認証の各機能を実現する。なお、同実施形態のソフトウェア構成は、特定のＯＳ（operating system）には依存しない仕様である。
【００２５】
本ソフトウェア構成は、主として、メッセージ（制御情報）を交換することにより、各ノード１０間の論理的な接続関係であるネットワーク接続形態（トポロジ：topology）を構成する機能を実現する機能部、ストリームデータの送出（中継を含む）、受信、再生の各機能を実現する機能部、ユーザとの入出力インターフェースであるＧＵＩ（graphical user interface）機能を実現する機能部、及び認証機能部を有する。
【００２６】
同実施形態では、サーバ２０は、各ノード１０の認証処理に必要な鍵データをを配布するために、例えばサービス提供業者が運営する鍵配付サーバを想定する。サーバ２０は、後述するように、公開鍵暗号方式による鍵データを提供する。各ノード１０は、サーバ２０から提供された鍵データを使用して、接続要求を行なう下流ノードの認証処理を実行する。
【００２７】
（認証方法）
以下図１、及び図４から図８のフローチャートを参照して、同実施形態の認証方法を説明する。
【００２８】
同実施形態では、図１に示すように、インターネット上に接続された各ノード１０の中で、データ配信源ノードとして最上流に位置する上流ノード１０Ａを想定する。当該上流ノード１０Ａは、例えば動画又は音声等のコンテンツ情報を含むデータ（ストリームデータ）３００を配信する。

【００２９】
ノード１０Ｂは、当該上流（配信源）ノード１０Ａに接続して、データ３００を受信する下流ノードとして機能し、かつ上流ノードとしても機能する中継ノードである。当該中継ノード１０Ｂは、上流ノード１０Ａから受信したデータ（ストリームデータ）３００を、配信を要求している下流ノード１０Ｃに送信する中継処理を実行する。ここでは、下流ノード１０Ｃは、配信されたデータを受信して再生する処理を実行するだけで、中継ノードとしては機能しないものと想定する。
【００３０】
鍵配付サーバ２０は、前述したように、例えばサービス提供業者が運営するサーバを想定する。ここでは、当該サービス提供業者は、上流（配信源）ノード１０Ａを操作するユーザとの契約に基づいて、当該コンテンツ情報（ＩＤ情報により識別される）の分散配信に伴なう各ノードの認証処理に必要な各種の鍵データを提供する。なお、当該サーバ２０の鍵配付機能は、ユーザが操作するノードに設定されるサーバ機能により実現される構成でもよい。
【００３１】
（公開鍵の発行手順）
同実施形態の認証方法は、公開鍵暗号方式の鍵データを使用する認証機能を実現している。以下図１と共に、図４及び図５のフローチャートを参照して、サーバ２０の鍵データの発行手順を説明する。
【００３２】
まず、上流（配信源）ノード１０Ａは、データ３００の配信を行なう前に、配信先として正当な下流ノードを認証するための鍵データの発行をサーバ２０に要求する。具体的には、図４（Ａ）に示すように、上流ノード１０Ａは、鍵発行要求メッセージ（ＰＲ）をサーバ２０に送信する（ステップＳ１）。ここで、当該メッセージ（ＰＲ）には、例えば配信するコンテンツ情報を識別するためのＩＤ情報（コンテンツＩＤ）と、配信源ノード１０Ａを識別するためのパスワードとを含む。
【００３３】
一方、サーバ２０は、同図（Ｂ）に示すように、配信源ノード１０Ａから鍵発行要求メッセージ（ＰＲ）を受信すると、当該メッセージ（ＰＲ）に含まれるパスワードに基づいて、予めなされた契約による正当な上流ノードであるか否かを認証する。サーバ２０は、正当な上流ノードであると認定すると、公開鍵暗号方式における公開鍵データ（Ｋｐ）と秘密鍵データ（Ｋｓ）とをペアとする鍵データを生成する（ステップＳ１１，Ｓ１２）。即ち、サーバ２０は、メッセージ（ＰＲ）に含まれるコンテンツＩＤに対応する公開鍵データ（Ｋｐ）と秘密鍵データ（Ｋｓ）とを生成する。
【００３４】
サーバ２０は、生成した秘密鍵データ（Ｋｓ）をコンテンツＩＤに関連付けして、秘密鍵データベース２００に登録する（ステップＳ１４）。また、サーバ２０は、生成した公開鍵データ（Ｋｐ）を含む応答メッセージを、配信源ノード１０Ａに返信する（ステップＳ１３）。
【００３５】
配信源ノード１０Ａは、サーバ２０から応答メッセージを受信すると、当該メッセージに含まれる公開鍵データ（Ｋｐ）を、コンテンツＩＤに関連付けして内部の記憶装置（例えばディスクドライブ）に保存する（ステップＳ２，Ｓ３）。
【００３６】
以上のようにして、配信源ノード１０Ａは、ストリームデータなどのデータ３００の配信を行なう前に、認証処理に必要な公開鍵データ（Ｋｐ）をサーバ２０から取得することができる。配信源ノード１０Ａは、当該公開鍵データ（Ｋｐ）を使用して、後述するように、自ノードに対して接続要求をしてきたノードが正当なノードであるか否かを判定する認証処理を実行する。ここで、正当であると認証されるノードとは、例えばデータ配信を受けるための料金決済に伴なって、サーバ２０から接続認証用鍵データ（Ｔ）を取得したノ

ードである。
【００３７】
ここで、後述するように、接続認証用鍵データ（Ｔ）は、秘密鍵データ（Ｋｓ）により暗号化された鍵データである。一方、公開鍵データ（Ｋｐ）は、当該接続認証用鍵データ（Ｔ）を復号化するための鍵データである。従って、秘密鍵データ（Ｋｓ）は、暗号化鍵データに相当する。また、公開鍵データ（Ｋｐ）は、復号化鍵データに相当する。
【００３８】
（接続鍵の発行手順）
下流ノード１０Ｂは、配信源ノード１０Ａに接続要求して、例えばストリームデータなどのデータ配信サービスを受ける。下流ノード１０Ｂは、配信源ノード１０Ａに接続するための接続鍵の発行をサーバ２０に要求する。具体的には、図５（Ａ）に示すように、下流ノード１０Ｂは、接続鍵の発行要求メッセージ（ＩＲ）をサーバ２０に送信する（ステップ２１）。ここで、当該メッセージ（ＩＲ）には、例えば配信するコンテンツ情報を識別するためのコンテンツＩＤ（Ｇ）と、当該ノード１０Ｂを識別するためのノード識別情報（Ｈ）を含む。ノード識別情報（Ｈ）は、例えばノード１０Ｂに使用されているネットワークのＭＡＣアドレスや、マイクロプロセッサのシリアル番号等のハードウェアの識別番号である。
【００３９】
一方、サーバ２０は、同図（Ｂ）に示すように、ノード１０Ｂから発行要求メッセージ（ＩＲ）を受信すると、ストリームデータの配信サービスを受けるための料金の決済処理を実行する（ステップＳ３１，Ｓ３２）。この決済処理では、サーバ２０は、例えば料金をノード１０Ｂ側の表示画面上に表示し、またクレジットカード番号の入力を促す。ノード１０Ｂからクレジットカード番号が入力されると、サーバ２０は、当該クレジットカードから料金を引き落とすための所定の決済処理を実行する。
【００４０】
ここで、サーバ２０を運営する当該サービス提供業者は、上流（配信源）ノード１０Ａを操作するユーザとの契約に基づいて、当該コンテンツ情報（ＩＤ情報により識別される）の分散配信に伴なう認証処理に必要な鍵データを提供するための料金の決済処理を実行する。要するに、サーバ２０は、認証処理に必要な鍵データの保管や、取り扱いに関して、上流（配信源）ノード１０Ａを操作するユーザとの契約に基づいて一種の代行業務を行なうことになる。
【００４１】
次に、サーバ２０は、秘密鍵データベース２００から、コンテンツＩＤ（Ｇ）に対応する秘密鍵データ（Ｋｓ）を取り出す（ステップＳ３３）。サーバ２０は、取り出した秘密鍵データ（Ｋｓ）を使用して、コンテンツＩＤ（Ｇ）とノード識別情報（Ｈ）とを暗号化した接続認証用鍵データ（Ｔ）を生成する（ステップＳ３４）。サーバ２０は、生成した接続認証用鍵データ（Ｔ）を含む応答メッセージを、下流ノード１０Ｂに返信する（ステップＳ３５）。即ち、サーバ２０は、秘密鍵データ（Ｋｓ）を暗号化鍵データとして保管している。
【００４２】
下流ノード１０Ｂは、サーバ２０から応答メッセージを受信すると、当該メッセージに含まれる接続認証用鍵データ（Ｔ）を内部の記憶装置（例えばディスクドライブ）に保存する（ステップＳ２２，Ｓ２３）。
【００４３】
以上のようにして、下流ノード１０Ｂは、ストリームデータの配信サービスを受けるために、料金の決済処理に伴なって、接続認証用鍵データ（Ｔ）をサーバ２０から取得することができる。サーバ２０は、配信源ノード１０Ａのユーザに対して、契約に基づいた料金を決済する。具体的には、例えばサーバ２０を運営する業者は、ノード１０Ｂのエンドユーザが支払う料金から所定の手数料を差し引いて、配信源ノード１０Ａのユーザの口座に振り込むような処理を実行する。ここで、配信源ノード１０Ａのユーザとは、例えばコン

テンツ情報の所有者や、コンテンツ配信サービス事業者などに相当する。

【００４４】

（接続鍵による認証手順）

下流ノード１０Ｂは、図６（Ａ）に示すように、配信源ノード１０Ａに対して、ストリームデータの配信を受けるための接続要求メッセージ（ＣＲ）を送信して、当該データ配信を要求する（ステップＳ４１）。下流ノード１０Ｂは、接続要求メッセージ（ＣＲ）には、接続認証用鍵データ（Ｔ）、ストリームコンテンツを識別するためのコンテンツＩＤ（Ｇ）、及び当該ノード１０Ｂを識別するためのノード識別情報（Ｈ）を含ませる（ステップＳ４２）。ここで、接続認証用鍵データ（Ｔ）は、前述したように、サーバ２０が保管する秘密鍵データ（Ｋｓ）により暗号化されたデータである。一方、コンテンツＩＤ（Ｇ）及びノード識別情報（Ｈ）は、暗号化されていない平文データである。

【００４５】

一方、上流ノードである配信源ノード１０Ａは、同図（Ｂ）に示すように、下流ノード１０Ｂから接続要求メッセージ（ＣＲ）を受信すると、内部記憶装置からコンテンツＩＤ（Ｇ）に対応する公開鍵データ（Ｋｐ）を取り出す（ステップＳ５１，Ｓ５２）。配信源ノード１０Ａは、取り出した公開鍵データ（Ｋｐ）を使用して、接続認証用鍵データ（Ｔ）を復号化してコンテンツＩＤ（Ｇ）とノード識別情報（Ｈ）とを復元する（ステップＳ５３）。即ち、サーバ２０は、公開鍵データ（Ｋｐ）を復号化鍵データとして提供する。

【００４６】

次に、配信源ノード１０Ａは、接続認証用鍵データ（Ｔ）から復元したコンテンツＩＤ（Ｇ）とノード識別情報（Ｈ）のそれぞれと、下流ノード１０Ｂから平文データとして受信したコンテンツＩＤ（Ｇ）とノード識別情報（Ｈ）とのそれぞれとを照合する（ステップＳ５４）。この照合処理の結果に従って、配信源ノード１０Ａは、一致すれば認証成功として、接続要求してきた下流ノード１０Ｂが正当なノード（対価を支払ったユーザ）であると判定する（ステップＳ５５のＹＥＳ）。認証成功の場合には、配信源ノード１０Ａは、所定のストリームデータを、接続要求してきた下流ノード１０Ｂに対して送出（提供）する。

【００４７】

下流ノード１０Ｂは、認証された場合、即ち接続要求が受理された場合には、配信源ノード１０Ａから送出されるストリームデータを受信し、表示画面上で再生するなどの処理を実行する（ステップＳ４３のＹＥＳ）。

【００４８】

一方、認証失敗の場合には、配信源ノード１０Ａは、当該認証失敗を通知するためのメッセージを下流ノード１０Ｂに返信する（ステップＳ５５のＮＯ，Ｓ５６）。下流ノード１０Ｂは、接続要求が受理されないため、処理終了となる（ステップＳ４３のＮＯ）。この場合には、不正な接続認証用鍵データが使用されているか、あるいは認証処理に誤りなどが発生している可能性がある。このため、下流ノード１０Ｂは、前述の処理を再実行するか、またはサーバ２０から接続認証用鍵データの再取得処理を実行することになる。

【００４９】

以上のようにして、配信源ノード１０Ａは、予めサーバ２０から取得した公開鍵データ（Ｋｐ）を使用して、データ配信サービスを要求してきた下流ノード１０Ｂが正当なユーザであるか否かを認証する。下流ノード１０Ｂが料金決済に伴なって発行された接続認証用鍵データ（Ｔ）を取得していれば、正当なノードであると認証されて、所望のコンテンツ情報（ここでは、ストリームデータ）の提供を受けることができる。

【００５０】

（中継処理の手順）

同実施形態では、ネットワーク接続された各ノード１０（１０Ａ，１０Ｂも含む）は、他の上流ノードから受信したデータ（ストリームデータ）を、他の下流ノードに中継する機能を有する。従って、図１に示すように、配信源ノード１０Ａからデータ配信サービスを提供された下流ノード（中継ノード）１０Ｂは、上流ノードとして他の下流ノード１０Ｃ

からの要求に応じて、受信したストリームデータを中継する。このようなデータ中継においても、同実施形態の認証機能により、送出先のノード１０Ｃが正当なノードであるか否かを認証できる。以下、図７のフローチャートを参照して説明する。

【００５１】

データ中継処理を実行する中継ノード１０Ｂは、配信源ノード１０Ａから公開鍵データ（Ｋｐ）の提供を受ける（ステップＳ６１）。中継ノード１０Ｂは、取得した公開鍵データ（Ｋｐ）を、コンテンツＩＤに関連付けして内部の記憶装置（例えばディスクドライブ）に保存する。

【００５２】

中継ノード１０Ｂは、下流ノード１０Ｃから接続要求メッセージ（ＣＲ）を受信すると、内部記憶装置から公開鍵データ（Ｋｐ）を取り出して、前述の認証処理を実行する（ステップＳ６３）。即ち、下流ノード１０Ｃは、ストリーム配信サービスを受けるために、料金の決済処理に伴なって、接続認証用鍵データ（Ｔ）をサーバ２０から事前に取得する。中継ノード１０Ｂは、取り出した公開鍵データ（Ｋｐ）を使用して、下流ノード１０Ｃから送信された接続認証用鍵データ（Ｔ）を復号化してコンテンツＩＤ（Ｇ）とノード識別情報（Ｈ）とを復元する。そして、中継ノード１０Ｂは、接続認証用鍵データ（Ｔ）から復元したコンテンツＩＤ（Ｇ）とノード識別情報（Ｈ）のそれぞれと、下流ノード１０Ｃから平文データとして受信したコンテンツＩＤ（Ｇ）とノード識別情報（Ｈ）とのそれぞれとを照合する。

【００５３】

中継ノード１０Ｂは、照合処理の結果が一致すれば認証成功として、接続要求してきた下流ノード１０Ｃが正当なノード（対価を支払ったユーザ）であると判定する（ステップＳ６４のＹＥＳ）。認証が失敗した場合には、接続要求（ストリーム配信要求）が受理できないことを下流ノード１０Ｃに通知する（ステップＳ６４のＮＯ）。

【００５４】

ここで、正当なノードであると認証した下流ノード１０Ｃが中継ノードとして動作可能であれば、中継ノード１０Ｂは、前記の公開鍵データ（Ｋｐ）を提供する処理を実行してもよい（ステップＳ６５，Ｓ６６）。中継ノード１０Ｂは、認証成功の場合には、所定のストリームデータを、接続要求してきた下流ノード１０Ｃに対して送出（提供）する（ステップＳ６７）。

【００５５】

このようなストリーム中継処理により、配信源ノード１０Ａは、ストリーム配信を要求する全ての下流ノード１０に対してストリームデータを送出することなく、下流ノード（１０Ｂ）を中継ノードとして、間接的なストリーム配信機能を実現することができる。これにより、配信源ノード１０Ａのストリーム配信に伴なう負荷を大幅に軽減することができる。この場合、同実施形態の認証機能を利用することにより、中継ノード１０Ｂは、配信源ノード１０Ａと同様に、ストリーム配信サービスを要求する下流ノード１０Ｃが正当なノード（対価を支払ったユーザ）であるか否かを認証できる。

【００５６】

（鍵データの消去手順）

同実施形態では、配信源ノード１０Ａは、ストリーム配信を行なう前に、認証機能に必要な鍵データの発行をサーバ２０に要求して、公開鍵データ（Ｋｐ）を取得する。この鍵データ（Ｋｐ）は、秘密鍵データ（Ｋｓ）とペアであり、配信するストリームコンテンツ（ＩＤ情報により識別）に対応付けされたものである。従って、例えば当該ストリームコンテンツの配信を停止して、鍵データ（Ｋｐ，Ｋｓ）を無効にする場合には、例えば配信源ノード１０Ａからの要求に応じて、サーバ２０が発行した秘密鍵データ（Ｋｓ）を登録から消去し、結果として鍵データ（Ｋｐ，Ｋｓ）を無効にするための手順を用意することが必要である。以下、図８のフローチャートを参照して、鍵データの消去手順を説明する。

【００５７】

図８（Ａ）に示すように、ここでは、配信源ノード１０Ａは、鍵消去要求メッセージをサ

ーバ２０に送信する（ステップＳ７１）。当該メッセージには、配信するストリームコンテンツを識別するためのコンテンツＩＤと、配信源ノード１０Ａからの要求であることを認証するためのパスワードとを含む。

【００５８】

一方、サーバ２０は、同図（Ｂ）に示すように、配信源ノード１０Ａから鍵消去要求メッセージを受信すると、予め登録しているコンテンツＩＤとパスワードとに基づいて、鍵消去要求元のノード１０Ａが正当なノードであるか否かを判定するための認証処理を実行する（ステップＳ８１，Ｓ８２）。認証が失敗した場合には、サーバ２０は、正当なノードではないと判定し、消去拒否メッセージを要求元のノード１０Ａに送信する（ステップＳ８３のＮＯ，Ｓ８４）。

【００５９】

認証が成功した場合には、サーバ２０は、秘密鍵データベース２００からコンテンツＩＤに対応する秘密鍵データ（Ｋｓ）を特定して、登録から消去する処理を実行する（ステップＳ８３のＹＥＳ，Ｓ８５）。サーバ２０は、消去処理が完了すると、消去完了メッセージを、配信源ノード１０Ａに返信する（ステップＳ８６）。

【００６０】

配信源ノード１０Ａは、サーバ２０から消去完了メッセージを受信すると、当該秘密鍵データ（Ｋｓ）に対応する公開鍵データ（Ｋｐ）を内部の記憶装置（例えばディスクドライブ）から消去してもよい（ステップＳ７２）。

【００６１】

以上のようにして、配信源ノード１０Ａは、所定のストリームコンテンツの配信サービスを停止して、鍵データ（Ｋｐ，Ｋｓ）を無効にする場合に、サーバ２０に対して発行した秘密鍵データ（Ｋｓ）を登録から消去させることができる。従って、配信源ノード１０Ａは、ストリームコンテンツに対応付けされた秘密鍵データ（Ｋｓ）と公開鍵データ（Ｋｐ）とのペアからなる鍵データ（Ｋｐ，Ｋｓ）を無効にすることができる。

【００６２】

（セキュリティに関する効果）

同実施形態の認証方法では、コンテンツＩＤ（Ｇ）及びノード識別情報（Ｈ）については、平文データであるため、第三者が容易に取得することができる。しかしながら、接続認証用鍵データ（Ｔ）は、サーバ２０により保管されている秘密鍵データ（暗号化鍵データ）（Ｋｓ）により暗号化されている。従って、第三者には、正当な接続認証用鍵データ（Ｔ）を作成することは困難である。換言すれば、同実施形態の認証方法は、秘密鍵データ（Ｋｓ）を保管するサーバ２０（特定のユーザ端末でもよい）のみが正当な接続認証用鍵データ（Ｔ）を発行することを保証できる。

【００６３】

また、公開鍵データ（Ｋｐ）と接続認証用鍵データ（Ｔ）は、ユーザ端末に保持されるため、第三者に漏洩する可能性がある。しかしながら、公開鍵暗号方式では、一般的に、公開鍵データ（Ｋｐ）と接続認証用鍵データ（Ｔ）との組み合わせから、秘密鍵データ（Ｋｓ）を算出することは困難である。この場合、有効な接続認証用鍵データ（Ｔ）の配付期間（又は時間）を制限することにより、仮に不正なユーザが接続認証用鍵データ（Ｔ）を偽造することを未然に防止することができる。

【００６４】

更に、正当な接続認証用鍵データ（Ｔ）は、コンテンツＩＤ（Ｇ）とノード識別情報（Ｈ）との正当な組み合わせにおいてのみ有効となる。従って、正当な下流ノードとは異なる下流ノードは、認証されず、データ配信を受けることはできない。また、正当な下流ノードであっても、該当するコンテンツ情報以外のコンテンツ情報の配信を受けることはできない。

【００６５】

（本実施形態を適用したビジネスモデル）

以下図９を参照して、本実施形態を適用したビジネスモデルの具体例を説明する。

【００６６】
同ビジネスモデルは、特に、ブロードバンド（広帯域で常時接続型）のインターネット上で、ディジタルコンテンツを多数のユーザに対して分散配信するサービス事業を想定する。
【００６７】
具体的には、電子チケットの配布サービスを運営する事業者（以下、ＴＳＰ：Ticket Service Provider）と、電子チケットに基づいてコンテンツを配信するサービスを行う事業者（以下、ＣＳＰ：Contents Service Provider）とによるコンテンツ配信サービスを想定する。ユーザ（要するに一般消費者）は、ＴＳＰから電子チケットを購入することにより、ＣＳＰから所望のコンテンツの配信を受けることができる。
【００６８】
ここで、電子チケットとは、本実施形態での接続認証用鍵データ（Ｔ）に相当する。また、当該モデルでは、電子チケットを認証するための認証マスターキー（以下マスタ鍵データと表記する）が使用される。このマスタ鍵データとは、本実施形態での復号化鍵データ（公開鍵データ）に相当する。
【００６９】
図９は、コンテンツ配信サービスを実現するための仕組みを示す。ここでは、電子チケットの配布を行うためのサーバ（以下、ＤＴＳ：Digital Ticket Server）９０、及び複数のノード９１～９４がインターネット上に常時接続されている状態を想定する。上流ノードに相当するノード９１は、ＣＳＰが運営するコンテンツ配信ノード（以下、配信源ノード）である。中継ノード又は下流ノードに相当する各ノード９２～９４は、一般ユーザが保有し、操作するパーソナルコンピュータ（ＰＤＡ等の携帯型情報端末も含む）である。また、ＤＴＳは、電子チケットの配布を行うＴＳＰにより運営されている。
【００７０】
配信源ノード９１は、ＤＴＳ９０から、コンテンツの配信に必要な認証情報として、マスタ鍵データ（Ｋｐ）の提供を受ける。また、ＣＳＰ（コンテンツ配信ノード９１）は、ＴＳＰ（ＤＴＳ９０）からコンテンツ配信の対価を受け取り、また逆にＴＳＰ（ＤＴＳ９０）に手数料を支払う。即ち、ＴＳＰは、ＣＳＰとユーザ（ノード９２～９４）間での取引額から一部を手数料として徴収する。ユーザは、コンテンツ配信の対価として、電子チケット料をＴＳＰに支払う。
【００７１】
（電子チケット発行準備の手順）
発行準備の手順として、ＣＳＰ（配信源ノード９１）が、ユーザに配布したいコンテンツに関して、ＤＴＳ９０に対してマスタ鍵データ（Ｋｐ）の発行を要求する（プロセス９１Ａ）。この要求を受けて、ＤＴＳ９０の認証マスターキー発行機能部９００は、コンテンツ識別情報（ＣＩＤ：Contents ID。ユニークな番号等）と、暗号化鍵データ（Ｋｓ）と復号化鍵データ（Ｋｐ）との鍵ペア（公開鍵暗号方式における秘密鍵と公開鍵に相当）を生成し、これら３つのデータの組を鍵データベース９０３に登録する（プロセス９０Ａ）。ＤＴＳ９０は、復号化鍵データ（Ｋｐ）を、マスタ鍵データとしてＣＳＰ（配信源ノード９１）に返信する（プロセス９１Ｂ）。
【００７２】
ここで、ＴＳＰ（ＤＴＳ９０）は、この鍵データベース９０３への登録とマスタ鍵データ（Ｋｐ）の返信に伴なって、ＣＳＰ（配信源ノード９１）に対して手数料を請求する。具体的には、ＤＴＳ９０に接続された課金・決済システム９０２との連携により、ＣＳＰの銀行口座からの引き落とし手続きなどのオンライン決済処理が実行される。即ち、プロセス９０Ｃは、マスタ鍵データ（Ｋｐ）の発行に伴なう料金課金処理である。
【００７３】
以上のような準備が完了すると、ＣＳＰ（配信源ノード９１）は、インターネット上において、ＷＷＷのホームページ（Ｗｅｂページ）や電子メール、または雑誌などの紙媒体を介して、一般ユーザに対して当該コンテンツの配信サービスについての広告宣伝等を行な

うことになる。このとき、通常では、当該コンテンツを特定するためのＣＩＤを掲示することになる。

【００７４】

（電子チケット発行の手順）

次に、コンテンツ配信サービスに伴なう電子チケットの発行手順を説明する。

【００７５】

ここでは、当該コンテンツの配信を受けたいユーザが操作する各ノード９２～９４において、便宜的に、ノード９２を中継ノードと呼び、これ以外の各ノード９３，９４をユーザノードと呼ぶ。中継ノード９２は、ユーザノードとして機能すると共に、配信源ノード９１からのコンテンツを各ユーザノード９３，９４に中継する機能を有する。

【００７６】

当該コンテンツの配信を受けたいユーザ（中継ノード９２及びユーザノード９３，９４）はそれぞれ、通常では、ＣＳＰ（配信源ノード９１）の広告宣伝（Ｗｅｂページ等）から当該ＣＩＤを取得する。ユーザ（ノード９２～９４）はそれぞれ、ＣＩＤとユーザの識別情報ＵＩＤとを含めた電子チケット発行要求をＤＴＳ９０に送信する（プロセス９２Ｄ，９３Ｂ，９４Ａ）。ＵＩＤは、いわばノード識別情報であり、具体的には例えばユーザが使用しているパーソナルコンピュータのハードウェア識別情報等である。これらのＣＩＤとＵＩＤとの組み合わせ情報は、当該ユーザが当該コンテンツの配信を受けることを特定できる認証用情報である。

【００７７】

ＤＴＳ９０の電子チケット発行機能部９０１は、当該電子チケット発行要求を受信すると、鍵データベース９０３からＣＩＤに対応した暗号化鍵データ（Ｋｓ）を取り出す（プロセス９０Ｂ）。そして、電子チケット発行機能部９０１は、この暗号化鍵データ（Ｋｓ）を使用して、前記ＣＩＤとＵＩＤとを含む認証用情報を暗号化する。この暗号化データを電子チケット（接続認証用鍵データＴ）として生成し、各ユーザ（ノード９２～９４）のそれぞれに返信する（プロセス９２Ｅ，９３Ｃ，９４Ｃ）。

【００７８】

このような電子チケットの発行方法であれば、ユーザが電子チケット（Ｔ）を不正に生成（偽造）することは困難である。即ち、電子チケット（Ｔ）を生成するために必要な暗号化鍵データ（秘密鍵データＫｓ）は、ＤＴＳ９０の内部にのみ存在し、秘匿されているためである。

【００７９】

また、電子チケット（Ｔ）は、ユーザ固有の情報であるＵＩＤを含めて暗号化されたデータである。従って、同一のコンテンツ（ＣＩＤ）に対応するチケットでありながら、ユーザ（即ち、ノード）ごとに異なるデータ（ビット列）から構成されている。このため、他のユーザが、不正に電子チケットを盗用して、別のパーソナルコンピュータ（ノード）を使用して、当該コンテンツを要求しても、その接続認証の過程で盗用された電子チケットを検出することが可能である。

【００８０】

電子チケットの発行に関して、ＴＳＰ（配信源ノード９１）は、ユーザに対して、電子チケットの発行（即ち、コンテンツの配信）の対価を請求する。具体的には、ＤＴＳ９０に接続された課金・決済システム９０２との連携により、発行に伴なう前記手数料分を差し引いた額をＣＳＰの銀行口座に入金するといったオンライン決済処理が実行される（料金課金のプロセス９０Ｄ）。この場合、課金・決済システム９０２は、通常では、電子チケットの発行要求の受付時に、入力されたユーザのクレジットカード番号で決済することになる。

【００８１】

（コンテンツ配信の手順）

以上のようにして、ＣＳＰ（配信源ノード９１）はマスタ鍵データ（Ｋｐ）を取得し、また各ユーザ（ノード９２～９４）はそれぞれ電子チケット（Ｔ）を取得する。このような

状況を前提として、コンテンツ分散配信の手順を説明する。

【００８２】

ここでは、便宜的に、中継ノードとしても機能するユーザノード９２が、配信源ノード９１に対してコンテンツ（Ｃ）の配信要求を実行する（プロセス９２Ｃ）。このとき、中継ノード９２は、電子チケット（Ｔ）、及び平文のＣＩＤとＵＩＤとを含む認証用情報を送信する。

【００８３】

ＣＳＰ（配信源ノード９１）は、受信した電子チケット（Ｔ）をマスタ鍵データ（Ｋｐ）で復号化し、認証用情報であるＣＩＤとＵＩＤとを取り出す。そして、配信源ノード９１は、復号化した認証用情報と、平文の認証用情報（ＣＩＤとＵＩＤ）とを照合し、照合結果が一致すれば、当該中継ノード９２を正当なユーザノードであると認定する。換言すれば、当該ユーザからの電子チケット（Ｔ）は、ＤＴＳ９０から正規の手順で取得した正当なものであると認定する。

【００８４】

このような認証処理により、正当なユーザノード（中継ノード９２）に対して、当該電子チケット（Ｔ）に対応するコンテンツ（Ｃ）を送信する（プロセス９１Ｄ）。ここで、ＣＳＰ（配信源ノード９１）は、認証が成功したユーザノードからマスタ鍵データ（Ｋｐ）を要求されたときには、コンテンツ（Ｃ）と共にマスタ鍵データ（Ｋｐ）を提供してもよい（プロセス９１Ｃ）。

【００８５】

要するに、中継ノードとして機能するユーザノード９２は、受信したコンテンツ（Ｃ）を自身が利用すると共に、他のユーザノード９３，９４に対して、当該コンテンツ（Ｃ）をＣＳＰに代わって配信（中継）する（プロセス９２Ｂ，９２Ｆ）。このとき、前記のように、中継ノード９２は、マスタ鍵データ（Ｋｐ）を取得することにより、ＣＳＰ（配信源ノード９１）と同様に、他のユーザノード９３，９４を認証できる権限（いわば論理的権限）を備えることになる。具体的には、中継ノード９２は、コンテンツ配信を要求する他のユーザノード９３，９４から電子チケット（Ｔ）を受信すると、前記と同様の認証処理を実行する（プロセス９３Ａ，９４Ｂ）。

【００８６】

更に、中継ノード９２は、コンテンツの中継と共に、要求されたユーザノード９３，９４に対して、マスタ鍵データ（Ｋｐ）を中継する（９２Ａ，９２Ｇ）。従って、各ユーザノード９３，９４は、単にコンテンツを利用するユーザとしてだけでなく、中継ノードとして機能することができる。

【００８７】

以上のように、電子チケットの発行に基づいて、コンテンツを配信するコンテンツ配信サービスの仕組みを実現することができる。この仕組みは、配信源ノード９１から複数のユーザノード９２～９４に対してコンテンツを配信するだけでなく、多数のユーザノードが相互に連携して、コンテンツの分散配信を実現できる。また、コンテンツ配信に伴なう認証機能を各ユーザノードに分散させることにより、認証処理に関するアクセス処理の集中化を回避することが可能となる。

【００８８】

従って、結果的に配信源ノード９１を頂点とするコンテンツ配信ツリーを形成し、スケーラブルに限界なく成長させることができる。これにより、各ノードには高い性能が要求されずに、多数のユーザノードに対してコンテンツ配信を行なうサービスを実現できる。また、当該分散配信サービスは、単なるファイル等のコンテンツ配信だけでなく、ライブの音声・ビデオといったストリームデータの配信の場合にも有効である。

【００８９】

【発明の効果】

以上詳述したように本発明によれば、インターネットなどのコンピュータネットワーク環境において、特定のサーバに負荷が集中することなく、公開鍵暗号方式を利用した複数の

ノード間の接続に関する認証機能を、各ノードに分散させることができる。従って、有効な認証機能を含むデータ分散配信方式を適用するビジネスモデルを実現することができる。

【図面の簡単な説明】

【図１】本発明の実施形態に関する認証方法を説明するための概念図。

【図２】同実施形態に関するストリーム分散配信システムの概念を示す図。

【図３】同実施形態に関するシステムの具体的構成の一例を示すブロック図。

【図４】同実施形態に関する公開鍵の発行手順を説明するためのフローチャート。

【図５】同実施形態に関する接続鍵の発行手順を説明するためのフローチャート。

【図６】同実施形態に関する接続鍵による認証手順を説明するためのフローチャート。

【図７】同実施形態に関するストリーム中継処理の手順を説明するためのフローチャート。

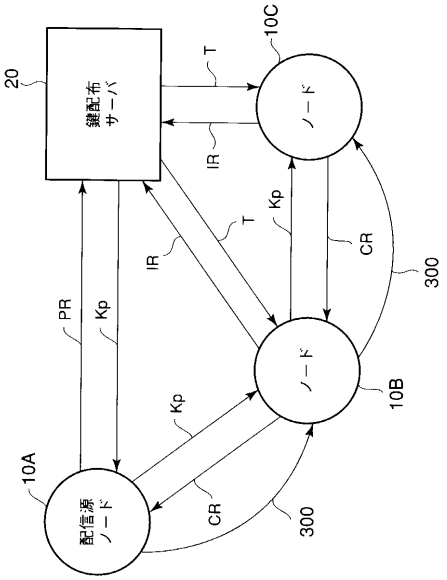
【図８】同実施形態に関する鍵データの消去処理の手順を説明するためのフローチャート。

【図９】同実施形態を適用したビジネスモデルを説明するためのブロック図。

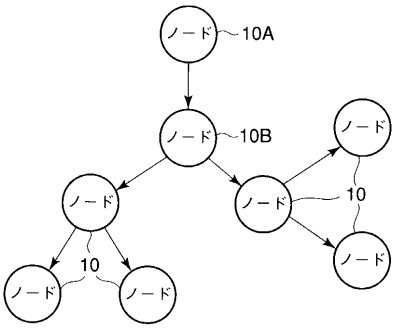
【符号の説明】

１０…ノード
１０Ａ…配信源ノード
１０Ｂ…下流ノード（中継ノード）
１０Ｃ…下流ノード
１１…パーソナルコンピュータ（ＰＣ）
１２…ルータ
１３…ディジタルビデオカメラ（ＤＶＣ）
２０…サーバ
１００…インターネット
２００…秘密鍵データベース（ＤＢ）

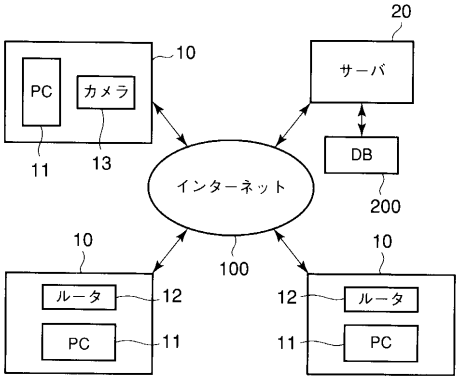
【図１】


鍵配布サーバ
20
ノード
10C
T
IR
Kp
CR
300
PR
10B
10A
配信源ノード

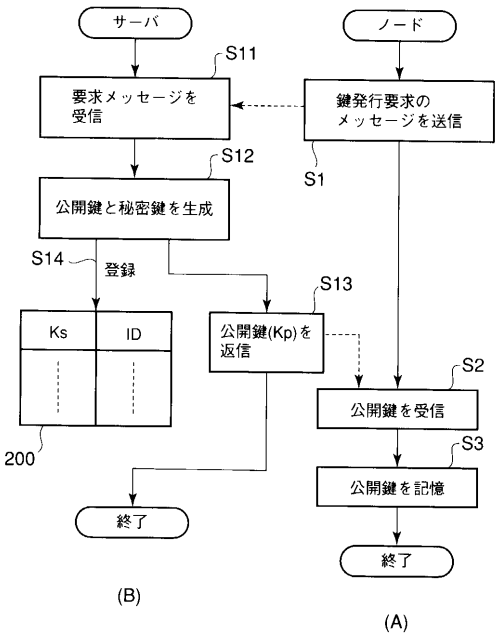
【図２】


ノード
10A
10B
10

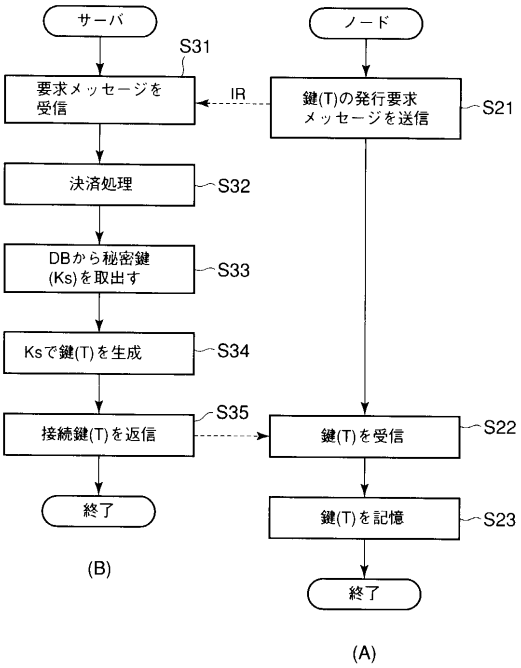
【図３】


20
サーバ
10
PC
カメラ
11
13
DB
200
インターネット
100
ルータ
12
PC
11

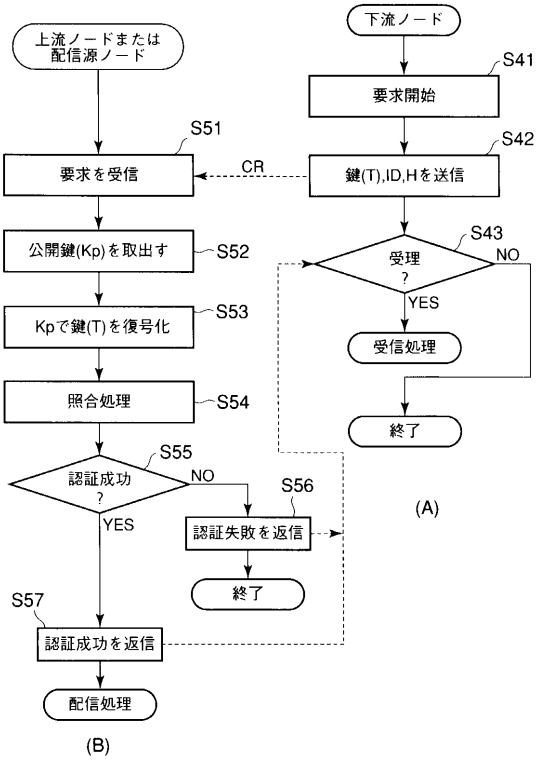
【図４】


サーバ
ノード
S11
要求メッセージを受信
鍵発行要求のメッセージを送信
S1
S12
公開鍵と秘密鍵を生成
S14
登録
S13
Ks
ID
公開鍵(Kp)を返信
200
S2
公開鍵を受信
S3
公開鍵を記憶
終了
終了
(B)
(A)

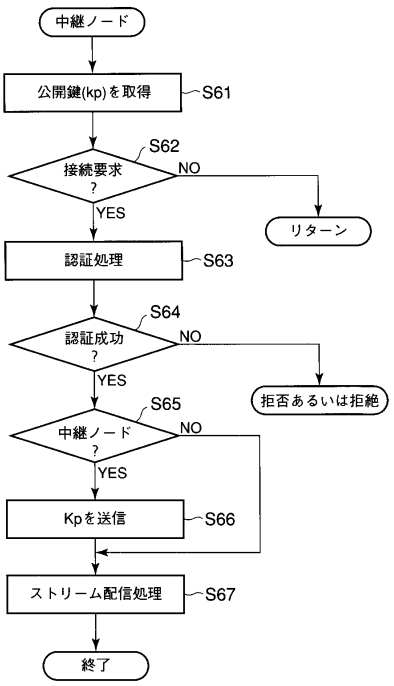
【図５】


サーバ
ノード
S31
要求メッセージを受信
IR
鍵(T)の発行要求メッセージを送信
S21
決済処理
S32
DBから秘密鍵(Ks)を取出す
S33
Ksで鍵(T)を生成
S34
接続鍵(T)を返信
S35
鍵(T)を受信
S22
終了
鍵(T)を記憶
S23
終了
(B)
(A)

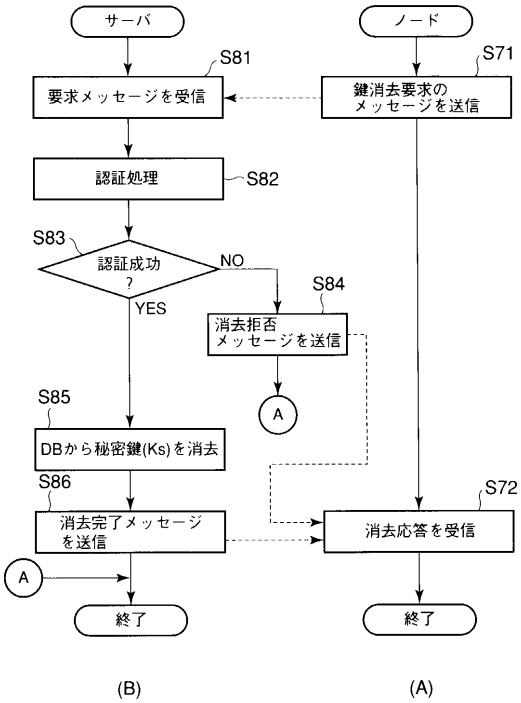
【図６】


上流ノードまたは配信源ノード
下流ノード
S41
要求開始
S42
鍵(T),ID,Hを送信
CR
S51
要求を受信
S52
公開鍵(Kp)を取出す
S53
Kpで鍵(T)を復号化
S54
照合処理
S55
認証成功？
NO
YES
S56
認証失敗を返信
終了
S57
認証成功を返信
配信処理
(B)
S43
受理？
NO
YES
受信処理
終了
(A)

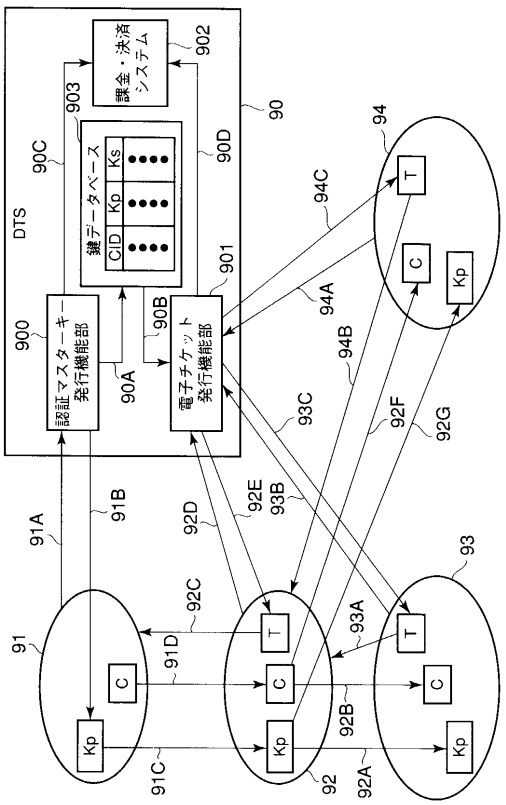
【図７】


中継ノード
公開鍵(kp)を取得
S61
S62
接続要求？
NO
YES
リターン
認証処理
S63
S64
認証成功？
NO
YES
拒否あるいは拒絶
S65
中継ノード？
NO
YES
Kpを送信
S66
ストリーム配信処理
S67
終了

【図８】


サーバ
ノード
S81
要求メッセージを受信
S71
鍵消去要求のメッセージを送信
認証処理
S82
S83
認証成功？
NO
YES
S84
消去拒否メッセージを送信
A
S85
DBから秘密鍵(Ks)を消去
S86
消去完了メッセージを送信
A
終了
S72
消去応答を受信
終了
(B)
(A)

【図９】


DTS
90
課金・決済システム
902
903
鍵データベース
Ks
Kp
CID
90C
90D
認証マスターキー発行機能部
900
90A
90B
電子チケット発行機能部
901
94
94C
94A
94B
T
C
Kp
93C
92F
92G
91A
91B
92D
92E
93B
93
91
92C
93A
91D
92B
91C
92
92A

フロントページの続き

(74)代理人 100088683
弁理士 中村 誠
(72)発明者 齊藤 ▲隆▼之
東京都世田谷区東玉川１－４１－２
(72)発明者 高野 雅晴
神奈川県横浜市港北区菊名２－１７－１

審査官 中里 裕正

(56)参考文献 小宅宏明, ＩＣカードを利用したピア・ツー・ピアによるコミュニケーションプラットフォームの提案, 情報処理学会研究報告, 日本, 社団法人情報処理学会, ２００２年 1月２４日, Vol. 2002/No.6, 13-18
LifeStyle, ビットメディアなど, ホリプロと提携してP2P事業に向けた実証実験, 日本, ２００２年 2月１３日, ＵＲＬ, http://plusd.itmedia.co.jp/broadband/0202/13/bitmedia.html

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 9/32
H04L 9/08
JSTPlus(JDream2)