

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2003 年 2 月 13 日 (13.02.2003)

PCT

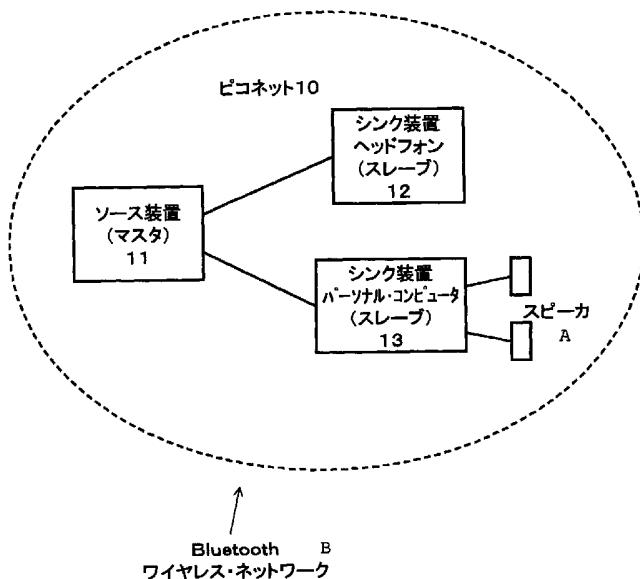
(10) 国際公開番号
WO 03/013068 A1

- (51) 国際特許分類: H04L 12/28 (72) 発明者; および
(21) 国際出願番号: PCT/JP02/07714 (75) 発明者/出願人 (米国についてのみ): 川村 晴美 (KAWA-MURA, Harumi) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP).
(22) 国際出願日: 2002 年 7 月 30 日 (30.07.2002) 嶋久登 (SHIMA, Hisato) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP).
(25) 国際出願の言語: 日本語
(26) 国際公開の言語: 日本語 (74) 代理人: 山田 英治, 外 (YAMADA, Eiji et al.); 〒104-0041 東京都中央区新富一丁目 1 番 7 号 銀座ティークエビル 澤田・宮田・山田特許事務所 Tokyo (JP).
(30) 優先権データ: 特願 2001-229078 2001 年 7 月 30 日 (30.07.2001) JP (81) 指定国 (国内): CN, JP, KR, US.
(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 号 Tokyo (JP). (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR).

[続葉有]

(54) Title: RADIO COMMUNICATION SYSTEM, RADIO COMMUNICATION CONTROL APPARATUS, RADIO COMMUNICATION CONTROL METHOD, RECORDING MEDIUM, AND COMPUTER PROGRAM

(54) 発明の名称: 無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラム



(57) Abstract: When transmitting data to be protected such as audio data by Bluetooth connection, authentication difficulty is switched according to the processing ability of the device to be a communication mate. Accordingly, even a device having a low processing ability can perform Bluetooth communication based on SDMI. Moreover, when the communication mate is a device having a high processing ability such as a personal computer, it is possible to provide sufficient countermeasure for hacking.

10...PICO NET
11...SOURCE DEVICE (MASTER)
12...SINK DEVICE HEADPHONE (SLAVE)
13...SINK DEVICE PERSONAL COMPUTER (SLAVE)
A...LOUDSPEAKER
B...BLUETOOTH WIRELESS NETWORK

[続葉有]



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。

(57) 要約:

オーディオ・データなどプロテクションを施す必要があるデータをBluetooth接続により伝送する場合、通信相手となる機器の処理能力に応じて認証の難易度を切り替える。したがって、低い処理能力の機器であっても、SDMIに準拠したBluetooth通信を行うことができる。また、通信相手がパーソナル・コンピュータのように高い処理能力を持つ機器に対しては、十分なハッキング対策を施すことができる。

明 細 書

無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びに
コンピュータ・プログラム

5

[技術分野]

本発明は、複数の機器間をワイヤレスで接続するための無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムに係り、特に、所定の通信セル内でワイヤレス接続された機器間でオーディオ・データを伝送するための無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムに関する。

さらに詳しくは、本発明は、Bluetoothのように1台のマスタ (master) 機器と複数台のスレーブ (slave) 機器によって構成されるピコネット (piconet) 内において機器間でオーディオ・データを伝送するための無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムに係り、特に、オーディオ・データなどのデジタル・データに所定のプロテクションを施しながらBluetooth機器間で伝送する無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムに関する。

15
20

[背景技術]

最近、デジタルVTRやMD (ミニディスク (商標)) 記録再生装置などのデジタル記録装置が普及し始めている。さらに、記録機能を備えたDVD (デジタルビデオディスク (商標)) あるいはデジタル・バーサタイル・ディスク) 装置も登場し、パーソナル・コンピュータ (PC) などの機器に搭載されるようになってきている。

25

このようなデジタル情報記録装置によれば、デジタル形式のデータやコンテン

ツの複製や改竄は極めて容易であり、著作権侵害の危険に無防備にさらされているとさえ言える。したがって、著作権法やその他の複製に関する法規制を強化するだけでは不十分であり、情報技術の観点からもデータやコンテンツの正当な利用を支援し若しくは不正利用を排除して、著作権の保護を拡充する必要があると

5 思料される。

例えば、デジタル音楽の著作権保護を目的として、1998年に米国大手レコード会社などが中心となってSDMI (Secure Digital Music Interactive) なるフォーラムが設立された。SDMIでは、基本的には、何らプロテクションが
10 掛けられていない状態でデジタル形式のコンテンツを機器外に出力することを禁止している。したがって、オーディオ再生機器からスピーカやヘッドフォンなどのレンダリング (Rendering) 装置にコンテンツをデジタル出力する場合、あるいは、DVD-Rドライブやパーソナル・コンピュータ (PC) などのレコーディング (Recording) 装置にコンテンツをデジタル出力する場合などにおいて、伝送
15 されるデータ・コンテンツをプロテクトすることが必須 (すなわち、"unprotected digital out"の禁止) とされている。

例えば、SDMIでは、ポータブル音楽プレーヤで著作権を保護する仕組みとして"Screening"という機能が規定されている。Screeningとは、ポータブル・デバイス (PD) のメモリ・レコーダ上にコピーしてよいコンテンツか否かを検査する仕組みであり、電子透かしを利用することが既に合意さ
20 れている。例えば、不正に配信されたコンテンツや、既に1回 (若しくは許容回数だけ) コピーされたコンテンツからはもはやコピーできないように、電子透かしによってScreeningをかけることができる。

このようなSDMIの要請は、ポータブル機器間をケーブル接続する場合は勿論のこと、ワイヤレスで機器間接続する場合においても必須とされている。

25 ところで、最近では、近距離無線通信の代表例である"Bluetooth"が、普及し始めて、各種の情報機器に搭載されている。Bluetoothは、さまざまな業界に対して適用可能なワイヤレス接続インターフェースを提供する標準規格であり、"Bluetooth SIG (Special Interest Group)"にその運営や管理などが委ねられている。

Bluetoothは、2.4GHzのISM (Industry Science Medical) バンドと呼ばれるグローバルな無線周波数を使用し、全体のデータ伝送速度は1 Mbpsであり、その中には電話の音声伝送に利用可能な64 kbpsの同期伝送チャンネルと、データ伝送のための非同期伝送チャンネルが設けられている。

- 5 前者の同期伝送チャンネルは、SCO (Synchronous Connection Oriented Link) 伝送方式が採用され、回線接続に適用される。また、後者の非同期伝送チャンネルは、ACL (Asynchronous Connection Less Link) 伝送方式が採用され、パケット交換によるデータ伝送に適用される。Bluetoothによる機器間の接続範囲は10m程度であるが、追加増幅器を使用することによって、さらに10
- 10 0mまで延長することができる。

- Bluetoothの技術仕様は、「コア (Core)」と「プロファイル (Profile)」に大別される。コアは、Bluetoothが提供するワイヤレス接続の基礎を定義する。これに対し、プロファイルは、Bluetoothのコアに基づいて各種の機能やアプリケーションを開発して機器に組み込む際に、
- 15 機器間の相互接続性を保証するための各機能毎に規定された技術要件の集まりである。

- Bluetoothのプロファイルは複数存在し、その組み合わせにより1つのアプリケーション (「利用モデル (Usage)」とも呼ぶ) を提供する。実際には、アプリケーションを提供するプロファイルの組み合わせがコアとともにBluetooth製品に実装されることになる。
- 20

例えば、携帯電話やパーソナル・コンピュータ関連のプロファイルを始めとして、自動車、ネットワーク、プリンタ、オーディオ、ビデオなど、さまざまなBluetoothプロファイルが想定される。

- 例えば、オーディオ・データの伝送用のプロファイルとして、"Bluetooth Advanced Audio Distribution Protocol" (A2DP) を挙げることができる。このプロファイルによれば、AV再生機器とスピーカやヘッドフォンなどのレンダリング装置とのワイヤレス接続や、AV再生機器とのDVD-Rドライブやパーソナル・コンピュータ (PC) などのレコーディング装置とのワイヤレス接続を実現することができる。
- 25

この種のBluetooth搭載のAV機器においても、先述したSDMIに準拠するためには、“unprotected digital out”を禁止するための仕組み、すなわち、デジタル伝送されるオーディオ・データをプロテクトするための仕組みを装備する必要がある。

- 5 Bluetoothセキュリティは、ある特定の2端末間で「リンク・キー(Link Key)」と呼ばれる共通のパラメータを設定することを基本として、マスタと各スレーブ間で1対1のセキュリティが管理される(リンク・キーは第3者には開示されない)。

- 10 ここで、デジタル・データをプロテクトする要素としては、「盗み取り(盗み聴き)」対策のための暗号化(encryption)と、「なりすまし」対策のための認証(authentication)という2つに大別される。

- Bluetooth SIGでは、コンテンツのプロテクション方式に関しては関与していないため、各ベンダの責任でコンテンツのプロテクションを行わなければならない。しかしながら、Bluetooth搭載のオーディオ機器間で
15 の認証方式は、Bluetooth層ではなく、その上位のアプリケーション層で実装しなければならない。

本発明者等は、Bluetooth通信をヘッドフォンやスピーカなどのレンダリング(すなわち聴くだけ)の用途に使用する場合と、レコーディングの用途に使用する場合とでは、プロテクションの仕組みが異なるものと思料する。

- 20 レコーディングに関しては、Music Downloadの場合のように、アプリケーション毎に充分納得のいく高い強度レベルのプロテクションが採用される場合が多い。

- これに対し、レンダリングに関しては、どの程度の強度とするかまで規定しているケースは少ない。例えば、ヘッドフォンのように処理能力の低いCPUが搭載されている機器に対して高いレベルのプロテクションを要求又は必須とすることは困難である。
25

例えば、i-LINK(IEEE 1394)用のコピー・プロテクション規格であるDTCP(Digital Transmission Content Protection)のFull authenticationを適用するためには、MIPS R4000 100MHzのC

5

P Uで計算しておおよそ6 0 0 m sの演算時間を要する負荷となる。このようなC P Uのコストや処理時間をヘッドフォンのような末端のポータブル機器に課することは現実的ではない。また、バッテリー駆動を基本とするポータブル機器においては、システム・デザイン上で消費電力が大きな問題となり、このような過大なレ

5 ベルの認証方式を一律に採用することは困難である。

一方において、レコーディング機能を装備したパーソナル・コンピュータ（P C）がレンダリング用途であると偽って不正に記録することを防止しなければならない。

10 ヘッドフォンのような演算能力が低い機器に対して採用し易いように、レンダリング用途として、例えば8ビットのキーを用いた認証方式を採用した場合、演算能力が高いパーソナル・コンピュータから簡単に破られてしまい、プロテクションを行う意味が薄れてしまう。

[発明の開示]

15

本発明の目的は、所定の通信セル内でワイヤレス接続された機器間でオーディオ・データを好適に伝送することができる、優れた無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムを提供することにある。

20

本発明のさらなる目的は、B l u e t o o t hのように1台のマスタ（ma s t e r）機器と複数台のスレーブ（s l a v e）機器によって構成されるピコネット（p i c o n e t）内において機器間でオーディオ・データを好適に伝送することができる、優れた無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムを提供することにある。

25

本発明のさらなる目的は、オーディオ・データなどのデジタル・データに所定のプロテクションを施しながらB l u e t o o t h機器間で伝送することができる、優れた無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムを提供することにある。

6

本発明は、上記課題を参酌してなされたものであり、その第1の側面は、所定の無線セル内でデータ・ストリームを送信するS o u r c e装置とデータ・ストリームを受信するS i n k装置とからなる無線通信システムであって、

前記S i n k装置の処理能力を判別する判別手段と、

- 5 該判別された前記S i n k装置の処理能力に応じて、前記S o u r c e装置と前記S i n k装置間の認証方式を決定する認証制御手段と、
を具備することを特徴とする無線通信システムである。

但し、ここで言う「システム」とは、複数の装置（又は特定の機能を実現する機能モジュール）が論理的に集合した物のことを言い、各装置や機能モジュール

- 10 が単一の筐体内にあるか否かは特に問わない。

また、前記無線セルは、例えばB l u e t o o t hワイヤレス・ネットワークにより構築される「ピコネット」である。ピコネット内では、通信秩序を維持する1台のマスタ装置が複数台のスレーブ装置と1対1のB l u e t o o t h通信を行なうことができる。

- 15 前記判別手段は、前記S i n k装置が処理能力の低い第1のタイプの装置か、又は、処理能力の高い第2のタイプの装置かを判別する。また、前記認証制御手段は、前記S i n k装置が第1のタイプの場合は比較的簡単な認証方式を採用し、前記S i n k装置が第2のタイプの場合は比較的複雑な認証方式を採用する。

- 20 本発明の第1の側面に係る無線通信システムによれば、オーディオ・データなどプロテクションを施す必要があるデータをB l u e t o o t h接続により伝送する場合、通信相手となる機器の処理能力に応じて認証方式の難易度を切り替えることで、適切なコンテンツ・プロテクションを行なうことができる。したがって、ヘッドフォンのようなレンダリング機能しか持たない低い処理能力の機器であっても、SDMIに準拠したB l u e t o o t h通信を行なうことができる。

- 25 また、通信相手がパーソナル・コンピュータのように高い処理能力を持つ機器に対しては、十分なハッキング対策を施すことができる。

前記判別手段は、前記S i n k装置からの自己申告を基に前記S i n k装置の処理能力を判別するようにしてもよい。例えば、オーディオ伝送用のA V D T P（Audio Video Distribution Transport Protocol）プロトコルで定義される

Stream Get Capability コマンドを用いて前記Sink装置からの自己申告を基に前記Sink装置の処理能力を判別することができる。

また、前記判別手段は、例えば、AVDTPプロトコルで定義される Security Control コマンドを用いて前記Sink装置に処理能力を問い合わせることができる。

また、前記判別手段は、前記Sink装置の種別を基に前記Sink装置の処理能力を判別するようにしてもよい。例えば、問い合わせ (Inquiry) 処理手順の際に入手した Class of Device 情報を基に、前記Sink装置の処理能力を判別することができる。

また、前記判別手段は、前記Sink装置がサポートするサービスを基に前記Sink装置の処理能力を判別するようにしてもよい。例えば、サービス・ディスカバリ (Service Discovery) によって取得された前記Sink装置が対応するサービス (プロトコル又はプロファイル) によってその処理能力を判別することができる。

例えば、前記判別手段は、前記Sink装置がA2DP (Bluetooth Advanced Audio Distribution Profile) にのみ対応している場合には、前記Sink装置が処理能力の低い第1のタイプであると判断することができる。

あるいは、前記判別手段は、前記Sink装置がPAN (Personal Area Network)、LAN (LAN Access Profile)、Object Push、又は、File Transferのうち少なくとも1つのプロファイルに対応している場合には、前記Sink装置が処理能力の低い第1のタイプではないと判断することができる。

また、本発明の第2の側面は、所定の無線セル内でSink装置に対してデータ・ストリームを送信する無線通信制御装置又は無線通信制御方法であって、

前記Sink装置の処理能力を判別する判別手段又はステップと、
該判別された前記Sink装置の処理能力に応じて、前記Source装置との前記Sink装置間の認証方式を決定する認証制御手段又はステップと、
を具備することを特徴とする無線通信制御装置又は無線通信制御方法である。

前記無線セルは、例えばBluetoothワイヤレス・ネットワークにより

構築される「ピコネット」である。ピコネット内では、通信秩序を維持する1台のマスタ装置が複数台のスレーブ装置と1対1のBluetooth通信を行うことができる。また、本発明の第2の側面に係る無線通信制御装置又は無線通信制御方法を、Bluetoothピコネット内のマスタ装置に実装することができる。

前記判別手段又はステップは、前記Sink装置が処理能力の低い第1のタイプの装置か、又は、処理能力の高い第2のタイプの装置かを判別する。また、前記認証制御手段は、前記Sink装置が第1のタイプの場合は比較的簡単な認証方式を採用し、前記Sink装置が第2のタイプの場合は比較的複雑な認証方式を採用する。

本発明の第2の側面に係る無線通信制御装置又は無線通信制御方法によれば、オーディオ・データなどプロテクションを施す必要があるデータをBluetooth接続により伝送する場合、通信相手となる機器の処理能力に応じて認証方式の難易度を切り替えることで、適切なコンテンツ・プロテクションを行なうことができる。したがって、ヘッドフォンのようなレンダリング機能しか持たない低い処理能力の機器であっても、SDMIに準拠したBluetooth通信を行なうことができる。また、通信相手がパーソナル・コンピュータのように高い処理能力を持つ機器に対しては、十分なハッキング対策を施すことができる。

前記判別手段又はステップは、前記Sink装置からの自己申告を基に前記Sink装置の処理能力を判別するようにしてもよい。例えば、オーディオ伝送用のAVDTPプロトコルで定義されるStream Get Capabilityコマンドを用いて前記Sink装置からの自己申告を基に前記Sink装置の処理能力を判別することができる。

また、前記判別手段又はステップは、例えば、AVDTPプロトコルで定義されるSecurity Controlコマンドを用いて前記Sink装置に処理能力を問い合わせることができる。

また、前記判別手段又はステップは、前記Sink装置の種別を基に前記Sink装置の処理能力を判別するようにしてもよい。例えば、問い合わせ(Inquiry)処理手続の際に入手したClass of Device情報を基に、前記Sink

装置の処理能力を判別することができる。

また、前記判別手段又はステップは、前記Sink装置がサポートするサービスを基に前記Sink装置の処理能力を判別するようにしてもよい。例えば、サービス・ディスカバリによって取得された前記Sink装置が対応するサービス

5 によってその処理能力を判別することができる。

例えば、前記判別手段又はステップは、前記Sink装置がA2DPにのみ対応している場合には、前記Sink装置が処理能力の低い第1のタイプであると判断することができる。

あるいは、前記判別手段又はステップは、前記Sink装置がPAN、LAN、

10 Object Push、又は、File Transferのうち少なくとも1つのプロファイルに対応している場合には、前記Sink装置が処理能力の低い第1のタイプではないと判断することができる。

また、本発明の第3の側面は、所定の無線セル内でSink装置に対するデータ・ストリームの送信制御をコンピュータ・システム上で実行するように記述されたコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ・ソフトウェアは、

15

前記Sink装置の処理能力を判別する判別ステップと、

該判別された前記Sink装置の処理能力に応じて、前記Source装置と

20 の前記Sink装置間の認証方式を決定する認証制御ステップと、

を具備することを特徴とする記憶媒体である。

本発明の第3の側面に係る記憶媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・ソフトウェアをコンピュータ可読な形式で提供する媒体である。このような媒体は、例えば、CD

25 (Compact Disc) やFD (Flexible Disk)、MO (Magneto-Optical disc) などの着脱自在で可搬性の記憶媒体である。あるいは、ネットワーク（ネットワークは無線、有線の区別を問わない）などの伝送媒体などを經由してコンピュータ・ソフトウェアを特定のコンピュータ・システムに提供することも技術的に可能である。

- このような記憶媒体は、コンピュータ・システム上で所定のコンピュータ・ソフトウェアの機能を実現するための、コンピュータ・ソフトウェアと記憶媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、本発明の第3の側面に係る記憶媒体を介して所定のコンピュータ・ソフトウェアをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の第1の側面に係る無線通信システム、あるいは第2の側面に係る無線通信制御装置及び無線通信制御方法と同様の作用効果を得ることができる。
- 10 また、本発明の第4の側面は、所定の無線セル内でSink装置に対するデータ・ストリームの送信制御をコンピュータ・システム上で実行するように記述されたコンピュータ・プログラムであって、
- 前記Sink装置の処理能力を判別する判別ステップと、
- 該判別された前記Sink装置の処理能力に応じて、前記Source装置と
- 15 の前記Sink装置間の認証方式を決定する認証制御ステップと、
- を具備することを特徴とするコンピュータ・プログラムである。
- 本発明の第4の側面に係るコンピュータ・プログラムは、コンピュータ・システム上で所定の処理を実現するようにコンピュータ可読形式で記述されたコンピュータ・プログラムを定義したものである。換言すれば、本発明の第4の側面に
- 20 係るコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の第1の側面に係る無線通信システム、あるいは第2の側面に係る無線通信制御装置及び無線通信制御方法と同様の作用効果を得ることができる。
- 25 本発明のさらに他の目的、特徴や利点は、後述する本発明の実施形態や添付する図面に基づくより詳細な説明によって明らかになるであろう。

[図面の簡単な説明]

図1は、本発明の一実施形態に係るBluetoothピコネット10内の構成を模式的に示した図である。

図2は、図1に示したBluetoothピコネット10を構成するSource装置としてのオーディオ・プレーヤ（マスタ）11と、Sink装置としてのヘッドフォン（スレーブ）12の構成を模式的に示した図である。

図3は、オーディオ伝送用のプロファイル”Bluetooth Advanced Audio Distribution Profile”（A2DP）のプロファイル・スタック構造を模式的に示した図である。

図4は、AVDTPプロトコルにおける接続確立手続（Connection Establishment）のシーケンスを示した図である。

図5は、AVDTPプロトコルで定義されているSecurity Control手続のシーケンスを示した図である。

図6は、Bluetoothワイヤレス・ネットワークにおけるオーディオ・ストリーミングの流れとパケット・フォーマットを模式的に示した図である。

図7は、Source装置11とSink装置12間でのGAVDPに従ってストリーミングのセットアップと解放を行うためのSource装置とSink装置間での処理の流れを示した図である。

図8は、AVDTPプロトコルで定義されている認証手続きに成功した場合にシーケンスを示した図である。

図9は、AVDTPプロトコルで定義されている認証手続きに失敗した場合にシーケンスを示した図である。

図10は、本実施形態に係るBluetoothピコネット10において、Source装置11とSink装置12間で行われる認証の処理手順の概念を示したブロック図である。

図11は、”Stream Get Capability”のコマンドに使用されるデータ・フレームの構造を示した図である。

図12は、”Stream Get Capability”コマンドに対するレスポンスに使用されるデータ・フレームの構造を示した図である。

図13は、”Stream Set Configuration”のコマンド及びレスポンスに使用され

るデータ・フレームの構造を示した図である。

図14は、"Security Control"コマンドに使用されるデータ・フレームの構造を示した図である。

図15は、"Security Control"コマンドに対するレスポンスに使用されるデータ・フレームの構造を示した図である。

図16は、タイプ問い合わせ時の"Security Control"コマンドの"Content Protection Scheme Dependent"フィールドの構成を示した図である。

図17は、タイプ問い合わせ時の"Security Control"コマンドに対するレスポンスの"Content Protection Scheme Dependent"フィールドの構成を示した図である。

図18は、Class of Device情報フィールドのデータ構造を模式的に示した図である。

図19は、Bluetooth Assigned Numbers が規定する Major Device Class の割り当てを示した図である。

図20は、認証時の"Security Control"コマンドの"Content Protection Scheme Dependent"フィールドの構成を示した図である。

図21は、認証時の"Security Control"コマンドに対するレスポンスの"Content Protection Scheme Dependent"フィールドの構成を示した図である。

図22は、Source装置がSink装置のタイプ判別を行うことにより認証を行うための処理手順（前半）を示したフローチャートである。

図23は、Source装置がSink装置のタイプ判別を行うことにより認証を行うための処理手順（後半）を示したフローチャートである。

図24は、UUIDの例（抜粋）を示した図である。

[発明を実施するための最良の形態]

以下、図面を参照しながら本発明の実施形態について詳解する。

本発明に係る認証方式によれば、認証に成功した場合に限り通信相手はレンダ

リング用途でストリームを受ける機器であるとみなすことができる。この結果、伝送データのレコーディングが行われることを想定せず、比較的低い強度のプロテクションを以って伝送データを保護することができる。

- 以下、Bluetoothでオーディオ伝送を行う場合を例にとって、図面を
5 参照しながら本発明の実施形態について詳解する。

Bluetoothは、2.4GHzのISM (Industry Science Medical) バンドと呼ばれるグローバルな無線周波数を使用し、全体のデータ伝送速度は1 Mbpsであり、その中には電話の音声伝送に利用可能な64 kbpsの同期伝送チャンネルと、データ伝送のための非同期伝送チャンネルが設けられている。

- 10 前者の同期伝送チャンネルは、SCO (Synchronous Connection Oriented Link) 伝送方式が採用され、回線接続に適用される。また、後者の非同期伝送チャンネルは、ACL (Asynchronous Connection Less Link) 伝送方式が採用され、パケット交換によるデータ伝送に適用される。

- Bluetoothの技術仕様は、「コア (Core)」と「プロファイル (Profile)」に大別される。コアは、Bluetoothが提供するワイヤレス接続の基礎を定義する。これに対し、プロファイルは、Bluetoothのコアに基づいて各種の機能やアプリケーションを開発して機器に組み込む際に、機器間の相互接続性を保証するための各機能毎に規定された技術要件の集まりである。Bluetoothのプロファイルは複数存在し、その組み合わせにより
15 1つのアプリケーション (「利用モデル (Usage)」とも呼ぶ) を提供する。実際には、アプリケーションを提供するプロファイルの組み合わせがコアとともにBluetooth製品に実装されることになる。

- Bluetoothは、1対1のケーブル代替接続だけではなく、1対多の簡易ワイヤレス・ネットワークの構築も提供する。このため、Bluetooth
25 通信に関わる機器群の中の1つに制御機能を与えることで通信の秩序を保つようにしている。制御機能を与えられた機器のことを「マスタ (Master)」機器と呼び、それ以外を「スレーブ (Slave)」機器と呼ぶ。また、マスタ及びスレーブとなった機器群が通信状態にあるネットワークのことを「ピコネット (piconet)」と呼ぶ。

ピコネット内では、「ピコネット内同期」がとられており、通信状態にあるすべてのBluetooth機器は、マスタ機器を基準とした同一の周波数ホッピング・パターンと時間スロットを有している状態にある。時間スロットはマスタ機器が提供するBluetoothクロックを基準として各スレーブ機器が形成する。

ピコネット内には、必ず1つだけマスタ機器が存在し、このマスタ機器が1台以上のスレーブを制御しながら通信を行なう。また、ピコネット内では、すべてのパケットはマスタ機器とスレーブ機器の間でのみ受信され、スレーブ機器同士が直接通信を行なうことはできない。

- そして、1つのピコネット内で同じ通信できるスレーブは最大7台までと決められている。これらにマスタ機器を含めて、最大で8台のBluetooth機器がピコネット内で同時通信を行なうことができる。

- ここで、オーディオ・ビジュアル（AV）機器の分野において、Bluetooth通信を導入した場合、ステレオ・コンボやメディア・プレイヤなどのオーディオ・データ・ストリームの出力源となるSource装置11をマスタとして定義する一方で、ヘッドフォンやパーソナル・コンピュータ（PC）などのオーディオ出力ターゲットとなるSink装置をスレーブ機器として定義することができる。図1には、このように構成されたBluetoothピコネット10内の構成を模式的に示している。

- 〔従来の技術〕の欄でも既に述べたように、このようにオーディオ伝送に適用されたBluetoothワイヤレス・ネットワークがSDMI (Secure Digital Music Interactive) に準拠するためには、Source装置11からSink装置12へ向かう伝送路に対して、“unprotected digital out”を禁止するための仕組み、すなわち、デジタル伝送されるオーディオ・データをプロテクトするための仕組みを装備する必要がある。

デジタル・データをプロテクトする要素としては、「盗み取り（盗み聴き）」対策のための暗号化（encryption）と、「なりすまし」対策のための認証（authentication）の2つに大別される。

本実施形態に係るBluetoothワイヤレス・ネットワークでは、前者の

暗号化に関しては、Bluetooth層で定義された暗号化方式をそのまま適用するので、本明細書では詳細な説明を省略する。

- また、後者の認証方式に関しては、Bluetooth層ではなく、その上位のアプリケーション層で実装する。本実施形態に係る認証方式は、認証に成功した場合に限り通信相手はレンダリング用途でストリームを受ける機器であるとみなして、伝送データのレコーディングが行われることを想定せず、比較的低い強度のプロテクションを以って伝送データをプロテクトするが、その詳細な説明は後述に譲る。

- 図2には、図1に示したBluetoothピコネット10を構成するSource装置としてのオーディオ・プレーヤ（マスタ）11と、Sink装置としてのヘッドフォン（スレーブ）12の構成を模式的に示している。

- Source装置としてのオーディオ・プレーヤ11は、Bluetoothインターフェース・ブロック11Aと、信号生成ブロック11Bと、プレーヤ制御ブロック11Cと、システム制御ブロック11Dとで構成され、Bluetoothピコネット10内ではマスターとして機能する。

Bluetoothインターフェース・ブロック11Aは、ピコネット10内におけるBluetoothワイヤレス接続を実現するための機能ブロックであり、ピコネット10内におけるスレーブ機器12、13との制御信号の交換やオーディオ・データの伝送などを行う。

- 信号生成ブロック11Bは、オーディオ信号を生成するための機能ブロックである。

プレーヤ制御ブロック11Cは、オーディオ・プレーヤ11上におけるメディアの再生、停止、一時停止、早送り、巻き戻しなどのメディア再生制御機能を実現するための機能ブロックである。

- システム制御ブロック11Dは、Bluetoothピコネット10内における各スレーブ機器12、13の統合的な制御を実現するための機能ブロックである。本実施形態では、システム制御ブロック11Dは、AV機器間のオーディオ・データの伝送用のプロファイルである”Advanced Audio Distribution Profile”（A2DP）におけるSourceの機能を管理するようになっている。

A2DPプロファイルは、Bluetoothピコネット10内でのオーディオ伝送のプロテクトも規定している。Bluetoothセキュリティは、ある特定の2端末間で「リンク・キー(Link Key)」と呼ばれる共通のパラメータを設定することを基本として、マスタと各スレーブ間で1対1のセキュリティが管理される(リンク・キーは第3者には開示されない)。

オーディオ・データをプロテクトする要素としては、「盗み取り(盗み聴き)」対策のための暗号化(encryption)と、「なりすまし」対策のための認証(authentication)という2つに大別される。本実施形態では、暗号化に関しては、Bluetooth層で定義されている暗号化方式を使用する。また、認証方式に関しては、A2DPプロファイルでは規定されていないので、上位のアプリケーション層(後述)において、本発明に固有の認証方式を実装する。本発明に係る認証方式によれば、Source装置11は、認証に成功した場合に限り通信相手はレンダリング用途でストリームを受けるSink機器であるとみなすことができる。この結果、Source装置側では、Sink装置において伝送データのレコーディングが行われることを想定せず、比較的低い強度のプロテクションを以って伝送データを保護することができる。

ヘッドフォン12は、Bluetoothインターフェース・ブロック12Aと、ヘッドフォン制御ブロック12Bと、信号処理ブロック12Cとで構成される、レンダリング専用のSink装置である。

Bluetoothインターフェース・ブロック12Aは、Bluetoothピコネット10内におけるBluetoothワイヤレス接続を実現するための機能ブロックであり、マスタ装置としてのオーディオ・プレーヤ11との制御信号の交換、並びにオーディオ・データの受信などを行う。

ヘッドフォン制御ブロック12Bは、ボリューム・アップ、ボリューム・ダウン、ミュートなどヘッドフォン12による音声出力機能を実現するための機能ブロックである。

信号処理ブロック12Cは、Bluetoothワイヤレス通信によりマスタ装置11から受信されたオーディオ信号を処理する機能ブロックである。

本実施形態では、ヘッドフォン12は、従来のオーディオ伝送用のプロファイ

ル” Bluetooth Advanced Audio Distribution Profile ” (A 2 D P) に対応した従来と同様のスレーブ装置として構成することができる。

図 3 には、オーディオ伝送用のプロファイル”Bluetooth Advanced Audio Distribution Profile ” (A 2 D P) のプロファイル・スタック構造を模式的に

5 図解している。

同図において、ベースバンド層、LMP層、L 2 C A P層、SDP層、及び、A V D T P層の各層は、B l u e t o o t hコアで定義されたB l u e t o o t hプロトコルである。このうちベースバンド層、LMP層、L 2 C A P層は、O S I (Open Systems Interconnect : 開放型システム間相互接続) 基本参照モデル

10 の第 1 層及び第 2 層に相当する。

SDP層は、B l u e t o o t hサービス・ディスカバリ・プロトコル(Service Discovery Protocol) を規定するプロトコル層である。システム・コントローラとしてのマスタ装置 1 1 は、このSDPプロトコルを用いて、同じB l u e t o o t hピコネット 1 0 内のスレーブ機器 1 2 , 1 3 が備える機能又はサービスを

15 検出することができる。

A V D T P (Audio/Video Distribution Transport Protocol) 層は、B l u e t o o t hピコネット 1 0 内におけるオーディオ伝送の処理手順やメッセージ交換を規定するプロトコル層であり、データ・ストリームのパラメータのネゴシエーションを行うシグナリング・エンティティと、データ・ストリーム自体を取り

20 扱うトランスポート・エンティティとからなる。

A 2 D Pでは、B l u e t o o t hベースバンド層での暗号化をオプションとして実装することが可能である。A 2 D Pでは、プロテクションに関して規定はしない。暗号化方式及び認証方式に関しては、A 2 D Pの各プロテクション方式毎に定める。

25 アプリケーション層は、S o u r c e装置 1 1 又はS i n k装置 1 2 においてアプリケーション・サービスやトランスポート・サービスの各パラメータを設定するエンティティで構成される。アプリケーション層は、オーディオ・ストリーム・データを規定の packets ・フォーマットに適合させる処理も行なう。

本実施形態では、アプリケーション層は、B l u e t o o t hピコネット 1 0

内におけるオーディオ伝送のための認証方式も実装する。この認証方式によれば、Source装置11は、認証に成功した場合に限り通信相手はレンダリング用途でストリームを受けるSink機器であるとみなすことができる。この結果、Source装置11は、Sink装置側で伝送データのレコーディングが行われることを想定せず、比較的低い強度のプロテクションを以って伝送データを保護することができる。

図3に示したプロファイル・スタック上では、Bluetoothピコネット10内のSource装置11とSink装置12, 13間でのオーディオ伝送における設定、制御、操作を行なうことができる。但し、このプロファイル・スタックでは、1対多のデータ配信を行なうことはできない。

また、Source装置11とSink装置12, 13間でのオーディオ伝送には、無線信号処理や、データ・ストリームのバッファリングや符号化／復号化のためにある程度の遅延が存在する。

また、このプロファイル・スタックを実装するためには、オーディオ・データの伝送レートは、Bluetoothリンク上で使用可能なビット・レートよりも充分小さくしなければならない。これは、聴覚可能なノイズや音飛びの原因となるパケット消失の影響をなくすためのパケット再伝送を行なうためである。

Bluetoothワイヤレス・ネットワークにおけるオーディオ伝送を行うためのプロトコルであるAVDTPは、「シグナリング」と「ストリーミング」という2つの機能に大別される。

ストリーミングは、オーディオ信号をリアルタイム伝送することを規定する。また、シグナリングは、Source装置から送信されたオーディオ・ストリームをSink装置側で受信処理できるように、フォーマットなどのネゴシエーションを行う。このネゴシエーション・パラメータの1つとして、コンテンツ・プロテクション (Content Protection: CP) のタイプがある。

Bluetooth AV伝送に適用するプロテクション方式はあらかじめBluetooth SIGに登録しておき、Bluetooth SIG側では各プロテクション方式に対して識別情報 (ID) を割り振る。このIDについては、"Bluetooth Assigned Numbers"で参照すること

ができる。勿論、登録されたプロテクション方式の内容については、Bluetoothの仕様書には何ら記述されない。例えば、本発明に係るコンテンツ・プロテクション方式も、Bluetooth SIGの管轄外でライセンスすることにより、規制を設けることもできる。

- 5 AVDTPプロトコルでは、接続確立手続 (Connection Establishment) において、"Stream Get Capability" コマンドを用いて、Source 装置はオーディオ伝送先となる Sink 装置が対応しているプロテクション方式を調べる。また、Source 装置は、"Stream Set Configuration" コマンドにより ID を指定することにより、適用するプロテクション方式を Sink 装置に設定する (AVDTPプロトコルでは、コンテンツのプロテクション方式の ID は、Bluetooth Assigned Numbers に登録されるので、一義に決まる)。

- 図 4 には、AVDTP プロトコルにおける接続確立手続 (Connection Establishment) のシーケンスを示している。AVDTP プロトコルでは Bluetooth デバイスの Stream 入出力口として Stream End Point
- 15 Point を規定している。Source 装置は、"Stream End Point Discovery" コマンドを用いて、Sink 装置が何系統のストリームに対応しているか、及び、それぞれに対応しているストリーム・タイプ (オーディオかビデオか) について調べる。次いで、Source 装置は、"Stream Get Capability" を用いて、オーディオ伝送先となる Sink 装置が対応しているプロテクション方式を調べる。
- 20 その後、Source 装置が Open コマンドを Sink 装置に送ることにより、Source 装置と Sink 装置はともに「オープン」状態になる。

- Bluetooth オーディオ伝送において適用するプロテクション方式に応じてその後の処理方法は異なるが、本実施形態では、アプリケーション層において、AVDTP プロトコルで定義されている "Security Control" コマンドを用いて Sink 装置の認証を行なうことによってプロテクションを行なう ("Security Control" コマンドのパラメータは、各プロテクション方式毎に定義することができる)。
- 25

図 5 には、AVDTP プロトコルで定義されている Security Control 手続のシーケンスを示している。図示の通り、オープン状態又はストリ

ーミング状態で”Security Control”コマンドの処理が行なわれる。この処理によってBluetooth伝送のステートの変化は生じない。

- 本実施形態では、Source装置11は、認証に成功した場合に限り通信相手はレンドリング用途でストリームを受けるSink機器であるとみなすことによ
- 5 よって、Sink装置において伝送データのレンドリングのみが行なわれる（言い換えれば、レコーディングは行なわれない）ことを想定したオーディオ伝送を行なうが、その詳細については後述に譲る。

- ストリーミングに関しては、オーディオ伝送のためのプロファイルである”Advanced Audio Distribution Profile”（A2DP）に記されている。図6には、
- 10 Bluetoothワイヤレス・ネットワークにおけるオーディオ・ストリーミングの流れとパケット・フォーマットを模式的に示している。

- オーディオ・コンテンツのストリーミングを開始したいときには、まず、ストリーミング・コネクションのセットアップを行う。このセットアップ処理手続の間、各装置間でオーディオ・ストリーミングのための適切なパラメータを選択す
- 15 る。アプリケーション・サービス・ケイパビリティと、トランスポート・サービス・ケイパビリティという2種類のサービスが構成される。A2DPプロファイルでは、シグナリング処理手続に必要なオーディオ仕様パラメータを規定している。

- A2DPのアプリケーション・サービス・ケイパビリティは、オーディオCODEC
- 20 DECケイパビリティとコンテンツ・プロテクション・ケイパビリティとで構成される。

また、トランスポート・サービス・ケイパビリティは、ストリーミング・パケットを好適に取り扱うことができるように、AVDTPプロトコルで提供されているサービスを選択する。

- 25 ストリーミング接続が確立すると、ストリーミング開始処理手続が実行される。AVDTPプロトコルを用いてストリーミング伝送を行なう際の処理手続については、”Generic Audio/Video Distribution Profile”（GAVDP）で規定されている。

Source装置とSink装置はともに「ストリーミング状態」になり、オ

オーディオ・ストリームの送受信を即座に行なうことができる。Source装置は”Send Audio Stream”処理手順を用いてオーディオ・データの送信を行ない、これに対し、Sink装置は”Receive Audio Stream”処理手順を用いてオーディオ・データの受信を行なう。

- 5 「オープン状態」にあるときに、Source装置又はSink装置がオーディオ・ストリームの送受信を開始したいときには、GAVDPで定義されているストリーミング開始 (Start Streaming) 処理手順を開始しなければならない。

- ”Send Audio Stream”処理手順では、Source装置は、シグナリング・セッションで、伝送データを選択されたフォーマットに符号化する。Source装置のアプリケーション層では、符号化データを定義されたメディア・ペイロード (MP) フォーマットに適合させる。コンテンツ・プロテクション (CP) を利用する場合には、コンテンツ・プロテクション方式に依存したCPヘッダを、暗号化されたオーディオ・コンテンツの先頭に付加する。

- その後、ストリーム・データは、インターフェース経由でAVDTP層で処理され、AVDTPプロトコルで定義されるトランスポート・サービスを用いて、トランスポート・チャンネルから送出される。

一方、Sink装置側のAVDTP層は、AVDTPプロトコルで定義されるトランスポート・サービスを用いて、トランスポート・チャンネルから受信して、インターフェース経由でアプリケーション層に受信ストリームを渡す。

- 20 コンテンツ・プロテクション方式が作動している場合、Sink装置側のアプリケーション層は、CPヘッダの解析や暗号化コンテンツの解読を行なう。そして、オーディオ・データ・フレームは、所定のコーディング方式により復号化されて、オーディオ出力 (レンダリング) などに利用される。

- 図7には、Source装置11とSink装置12間でのGAVDPに従ってストリーミングのセットアップと解放を行うためのSource装置とSink装置間での処理の流れを詳細に示している。但し、同図中で”*”が付されたものは”Generic Access Profile” (GAP) で規定されている処理手順であり、また、”**”が付されたものは”Service Discovery Protocol” (SDP) で定義されている処理手順であると理解されたい。GAP及びSDPは、Bluetooth

thの共通基本機能である。

まず、Bluetoothピコネット10内のマスタでもあるSource装置11は、該ピコネット10内にどのようなスレーブが存在するかを調べるために、Inquiry（問合せ）を行なうためのIQパケットをピコネット10内でブロードキャストする。

Inquiryを受信したスレーブとしてのSink装置12は、自身のBluetoothアドレス（BD_ADDR）やクロックの情報、機種種の属性（Class of Device）を通知するためのFHSパケットを返信する。

Source装置11は、ピコネット内の各スレーブから受信したFHSパケットのデータを基に、どのスレーブと接続するかを選択する。ここでは、説明の便宜上、Sink装置12を選択したものとする。

Name Discovery処理手続では、マスタとしてのSource装置11は、Page（呼び出し送信）により、スレーブとしてのSink装置12に宛てて、マスタの属性を通知して、マスタ及びスレーブ間で1対1の処理を経て通信フェーズに遷移する。そして、Name Requestにより、接続相手のBluetooth Device Nameを取得する。

次いで、リンク確立（Link Establishment）処理手続では、BluetoothデバイスとしてのSource装置11とSink装置12間の物理リンクを構築する。このリンク確立処理手続の中には、Bluetoothベースバンド層（図3を参照のこと）における認証（Authentication）や暗号化のネゴシエーションも含まれる。但し、Bluetoothセキュリティは誤接続防止、盗聴防止を目的としているので、本発明に係る認証方式とは相違する、という点を充分理解されたい。

次いで、サービス・ディスカバリ（Service Discovery）、すなわち、スレーブが備える機能又はサービスを検出するために、SDP用のL2CAPチャンネル（論理リンク・チャンネル）を張り、SDPプロトコルによりSink装置12がどのようなサービスに対応しているか（すなわち、Sink装置12が対応しているプロトコル、プロファイルなどの情報）を知る。

そして、SDP用のL2CAPチャンネルを解放してから、AVDTPシグナ

リングのためのL2CAPチャンネルを張る。既に述べたように、接続確立 (Connection Establishment) 処理手順の中で、オーディオCODEC、サンプリング周波数などの情報を基に、コンテンツ・プロテクション方式に関する情報の開示及び設定が行なわれる。

- 5 本実施形態では、Source装置11は、AVDTPプロトコルにおける接続確立手順 (Connection Establishment) において (図4を参照のこと)、“Stream Set Configuration”コマンドによりIDを指定することにより、適用するプロテクション方式をSink装置12に設定する。また、AVDTPプロトコルで定義されている“Security Control”コマンドを用いて (図5を参照のこと)、Sink装置12のタイプ (すなわち、レンダリング用途でストリームを受ける機器であるか、又は、レコーディング用途でストリームを受ける機器か) を認証する。
- 10 ヘッドフォンであるSink装置12は自分自身がレンダリング用途の機器であることを提示することによって、Source装置11側では、Sink装置12においてレンダリング用途で伝送データ・ストリームを受けることを想定した
- 15 認証方式が採用される。

- 認証に成功して、Sink装置12がレンダリング用途の機器であることが明らかになった場合には、GAVDPで定義されているストリーミング開始 (Start Streaming) 処理手順を経て、オーディオ・ストリームの伝送が行なわれる。図8には、認証に成功したときのシーケンスを示している。同図に示すように、オープン状態において、Source装置は、内部イベントの発生に応答して
- 20 “Security Control”コマンドを発行して認証を行ない、これに成功すると、内部的なストリーミングの開始に応じて“Start Streaming”コマンドを発行して、Sink装置へのストリーミング伝送を行なう。

- 一方、認証に失敗した場合には、Source装置11側ではアプリケーション層に通知され、オーディオ・ストリームの伝送は行なわれない。図9には、認証に失敗したときのシーケンスを示している。同図に示すように、オープン状態において、Source装置は、内部イベントの発生に応答して“Security Control”コマンドを発行して認証を行ない、これに失敗すると内部的な接続解放に
- 25 応答して、“Connection Release”コマンドを発行してSink装置との接続を

切断して、アイドル状態に遷移する。

図10には、本実施形態に係るBluetoothピコネット10において、Source装置11とSink装置12間で行われる認証の処理手順の概念を図解している。

- 5 Source装置11で発生した乱数 x は、制御信号の一種としてSink装置12に伝送される。同図に示す例では、Source装置11とSink装置12はともに、 $f(x)$ で示される認証アルゴリズムを共有しており、Sink装置12は受け取った入力 x に対して演算を実行して、その演算結果 $f'(x)$ をSource装置11に制御信号の一種として送信する。そして、Source
- 10 装置11は、乱数 x から自分自身で算出した結果 $f(x)$ とSink装置12から受信した演算結果 $f'(x)$ とを比較して、これらが一致するか否かで認証の判断を行なう。

- 本実施形態に係る認証方式の特徴は、Source装置11は、認証の対象とするSink装置12のタイプによって演算方式 $f(x)$ を切り替えるという点
- 15 にある。ここで言うSink装置のタイプは、該装置がヘッドフォンなどの処理能力の低い機器か(Type 1)、又は、パーソナル・コンピュータ(PC)などの処理能力の高い機器か(Type 2)で区分される。

- 例えば、通信相手となるSink装置がヘッドフォン12のように処理能力の低い機器の場合には、Source装置11は、発生する乱数 x を8ビットにする
- 20 とともに、演算 $f(x)$ をビットシフトなどの簡単な演算方式にする。ヘッドフォンのように処理能力の低い機器すなわちType 1の場合、一般に、比較的低い処理能力のCPUが搭載されているので、あまり強度の高くCPUの処理負荷の高い認証処理を行なうのには向いていない。

- これに対し、通信相手となるSink装置がパーソナル・コンピュータ(PC)
- 25 13のように、比較的高い処理能力のCPUが搭載されている装置の場合には、上述したような簡単な演算方式では、容易に「なりすまし」が行なわれて、コンテンツを十分にプロテクトすることができない。したがって、Sink装置がType 2の場合には、Source装置11は、発生する乱数 x を64ビット又は128ビットなどの長いものにするとともに、演算 $f(x)$ を楕円関数などの

比較的複雑なものを採用する。

なお、認証の演算として、ここでは乱数を入力して演算を行なう例を挙げたが、乱数だけではなく、例えばSink装置のBluetoothアドレス(BD_ADDR)など装置固有のデータを用いることにより、認証の強度をさらに向上させること

5 ができる。

上述したように通信相手となるSink装置の用途に応じて認証方式を切り換える場合において、最も重要となるのは、Sink装置のタイプの判別方法である。例えば、本発明に係る認証方式には非対応（すなわち、ライセンスでの規制範囲外）のパーソナル・コンピュータが「ヘッドフォンである」となりすまして、
10 不正にストリーム・データを記録してしまうような事態を防止しなければならない。

なお、認証演算による負荷が重たい機器（例えば、PCのように高い演算機能を持つ機器）は基本的にType 2を採用する。本発明に係る認証方式では、逆にType 1の対象機器を絞り込む。

15 Sink装置のタイプ（Type 1，Type 2）の判別方法について、以下に詳解する。

（1）自己申告

Source機器から”Stream Get Capability”コマンドを受け取ったSink装置は、本実施形態に係るコンテンツ・プロテクション方式に対応していることをCP-TYPEで示す。”Stream Get Capability”のコマンド及びレスポンスに
20 使用されるデータ・フレームの構造を図11及び図12にそれぞれ示しておく。

本実施形態に係るコンテンツ・プロテクション方式に対応しているSource装置は、Sink装置に対して、”Stream Set Configuration”コマンドを送り、本プロテクション方式を適用するようにセットする。”Stream Set Configuration”
25 のコマンド及びレスポンスに使用されるデータ・フレームの構造を図13に示しておく。

次いで、Source装置は、”Security Control”コマンドを用いて、Sink装置に対してタイプを問い合わせる。”Security Control”のコマンド及びレスポンスに使用されるデータ・フレームの構造を図14及び図15にそれぞれ示し

ておく。また、タイプ問い合わせ時のこれらコマンド及びレスポンスにおける”Content Protection Scheme Dependent”フィールドの構成を図16及び図17にそれぞれ示しておく。

”Content Protection Scheme Dependent”フィールドのフィールド長は、コマンド・レスポンス種別により可変長とするが、タイプ問い合わせコマンドの場合は1バイトとし、4ビットでコマンド・レスポンスの種別を示すとともに、4ビットでパラメータを示す。また、タイプ問い合わせコマンドでは、レスポンスの際に4ビットでタイプを示す。Type 1の場合は”0001”となり、Type 2の場合は”0010”となる。

10 (2) Type 1の確認

Sink装置がType 2を自己申告した場合には、Type 2に適合した方式で認証が行なわれる。また、Sink装置がType 1及びType 2以外の値を返してきた場合には、そこで認証は失敗とする。また、Sink装置がType 1を自己申告した場合は、さらにその確認のために以下の処理手順を実行する。

(2-1) Class of Device

Source装置は、Inquiry処理手順の際に、Sink装置のClass of Deviceを入手するので(図7を参照のこと)、ここではSink装置のClass of Device情報を基にSink装置のタイプの確認を行なうことができる。”Bluetooth Assigned Numbers”に規定されているように、各Bluetooth機器は自分が何者であるかを、”Major Device Class”及び”Minor Device Class”で示すようになっている。Sink装置のMajor Device Classが”Computer”の場合は、このSink装置はType 2による認証の対象であり、Type 1であることを自己申告したということは「なりすまし」であると解釈する。すなわち、Sink装置のMajor Device Classが”Computer”の場合は、認証はここで失敗とする。

図18には、Class of Device情報フィールドのデータ構造を模式的に示している。同図に示すように、当該フィールドの先頭から12ビット目からの5ビットがMajor Device Classに割り当てられている。また、Bluetooth

Assigned Numbersが規定するMajor Device Classの割り当てを図19に示しておく。

(2-2) プロファイル

Major Device Class が"Computer"でなくても、高機能な装置であれば、簡単な
5 認証方式であるType 1の対象とはならない。そこで、Source装置は、Sink装置がオーディオ伝送以外にサポートしているBluetoothアプリケーション・プロファイルがあるかどうかを調べる。SDPによりBluetooth機器のサポート・プロファイルを知ることができる。

10 Sink装置がA2DP以外のプロファイルをサポートしていない場合には、このSink装置をType 1すなわちレンダリング用途としての認証の対象であると認定する。

また、Sink装置がこれら以外のプロファイルに対応している場合には、対応しているプロファイルを基に判断する。Sink装置が、"Personal Area Network" (PAN)、"LAN Access Profile" (LAN)、Object Push、又は、File Transferのいずれかのプロファイルをサポートしている場合には、このSink装置をType 2としての認証の対象であると認定して、認証はここで失敗とする。

(3) 認証

Source装置は、Sink装置がType 1又はType 2のいずれであるかの認証を、"Security Control"コマンドを用いて行う。認証時における該コマンドのコマンド及びレスポンスにおける"Content Protection Scheme Dependent"フィールドの構成を図20及び図21にそれぞれ示しておく。

図22及び図23には、Source装置11がSink装置12のタイプ判別を行うことにより認証を行なうための処理手順をフローチャートの形式で示している。以下、これらのフローチャートに従って、本実施形態に係る認証処理について説明する。

Source装置11は、Sink装置12とはBluetoothベースバンド層において接続が確立され、呼び出し (Page) によりSink装置の装置種別 (Class of Device) を取得しているとともに、SDPプロトコルによりS

ink装置がサポートしているサービス（対応しているプロトコルやプロファイル）を取得しているものとする。

Source装置11は、AVDTPプロトコルに従い、Sink装置12に”Stream Get Capability”コマンドを送信して、そのレスポンスのCP_TYPE
5 が示す値を基に、Sink装置12が本発明に係るコンテンツ・プロテクション方式に対応するか否かを判別する（ステップS1）。

CP_TYPEを基に、Sink装置12が本プロテクション方式に対応していない場合には、本処理ルーチン全体を終了する。

一方、Sink装置12が本プロテクション方式に対応していると判断された
10 場合には、Source装置11は、Sink装置12に対して、”Stream Set Configuration”コマンドを送り、本プロテクション方式を適用するようにセットする（ステップS2）。ここまでの手続は、AVDTPプロトコルに従って行なうことができる。

次いで、Source装置11のアプリケーション層は、”Security Control”
15 コマンドを用いて、Sink装置12に対してタイプを問い合わせる（ステップS3）。ここで行なわれるタイプ問い合わせすなわち認証処理は、Sink装置12からの自己申告に基づく。ここで言うSink装置12のタイプは、該装置がヘッドフォンなどの処理能力の低い（Type1）、又は、パーソナル・コンピュータ（PC）などの処理能力の高い機器か（Type2）で区分される。

Sink装置12がType1以外の値を返してきた場合には（ステップS4）、
20 さらに、Sink装置12がType2を自己申告したか否かを判別する（ステップS5）。

Sink装置12がType2を自己申告した場合には（ステップS5）、本処理ルーチン全体を終了して、以後、Type2に適合した方式で認証が行われる
25 （ステップS6）。Type2に適合した認証方式とは、例えば、図10に示す認証メカニズムにおいて、Source装置11が、発生する乱数xを64ビット又は128ビットなどの長いものにするとともに、演算f(x)を楕円関数などの比較的複雑なものを採用することによって実現される。

Type2に適合した認証に成功した場合には（ステップS7）、本処理ルーチン

ンは成功裏に終了する。これに対し、Type 2 認証に失敗した場合には、認証は失敗として、本処理ルーチン全体を終了する。また、Sink 装置 1 2 が Type 2 以外の値を返してきた場合には (ステップ S 5)、そこで認証は失敗として、本処理ルーチン全体を終了する。

- 5 また、Sink 装置 1 2 が Type 1 を自己申告した場合には (ステップ S 4)、さらに、Sink 装置 1 2 の装置種別 (Class of Device) を確認する (ステップ S 8)。Sink 装置 1 2 の Class of Device は、Name Discovery 処理手続時に行われる呼び出し (Page) によって既に取得されている。

- 10 Sink 装置 1 2 の Major Device Class が "Computer" の場合は、この Sink 装置 1 2 は Type 2 による認証の対象であり、Type 1 であることを自己申告したということは「なりすまし」とであると解釈する (ステップ S 8)。すなわち、Sink 装置の Major Device Class が "Computer" の場合は、認証はここで失敗とする。

- 15 他方、Major Device Class が "Computer" でなくても、高機能な装置であれば、簡単な認証方式である Type 1 の対象とはならない。そこで、Source 装置 1 1 は、Sink 装置 1 2 がオーディオ伝送以外にサポートしている Bluetooth アプリケーション・プロファイルがあるかどうかを調べる (ステップ S 1 2)。

- 20 Sink 装置 1 2 が A 2 D P 以外のプロファイルをサポートしていない場合には、この Sink 装置 1 2 を Type 1 の認証の対象であると認定して、Type 1 に適合した方式で認証を行う (ステップ S 1 0)。Type 1 に適合した認証方式とは、例えば、図 1 0 に示す認証メカニズムにおいて、Source 装置が、発生する乱数 x を 8 ビットにするとともに、演算 $f(x)$ にビットシフトなどの比較的簡単なものを採用することによって実現される。Type 1 に適合した認
25 証に成功した場合には (ステップ S 1 1)、本処理ルーチンは成功裏に終了する。これに対し、Type 1 認証に失敗した場合には、認証は失敗として、本処理ルーチン全体を終了する。

また、Sink 装置 1 2 が A 2 D P 以外のプロファイルをサポートしている場合には、さらに、Sink 装置 1 2 が、"Personal Area Network" (PAN)、"LAN

Access Profile” (LAN)、Object Push Profile、又は、File Transfer Profileのいずれかをサポートしているか否かを判別する (ステップS8)。

5 Sink装置12が、“Personal Area Network” (PAN)、“LAN Access Profile” (LAN)、Object Push Profile、又は、File Transfer Profileのいずれかをサポートしている場合には (ステップS9)、このSink装置12をType2の認証の対象であると認定して、認証はここで失敗とする。

10 他方、Sink装置12が、“Personal Area Network” (PAN)、“LAN Access Profile” (LAN)、Object Push Profile、又は、File Transfer Profileのいずれもサポートしていない場合には (ステップS9)、このSink装置12をType1の認証の対象であると認定して、Type1に適合した方式で認証を行い、本処理ルーチン全体を終了する (同上)。

15 なお、SDPのBluetooth Profile Descriptor Listにはその機器が対応しているプロファイルが列挙されている。そして、Bluetooth Assigned Numbersで各プロファイルにUUIDが割り振られている。図24には、UUIDの例 (抜粋)を示している。上述したステップS9及びS12では、このBluetooth Profile Descriptor ListのUUIDを参照することによって、機器がサポートしているプロファイルを判断することができる。

20

追補

以上、特定の実施形態を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。

25 本明細書では、本発明をBluetoothワイヤレス・ネットワークに適用した場合を例にとって説明してきたが、本発明の要旨は必ずしもこれに限定されるものではなく、同様の機器情報、サービス情報を取り扱う他の有線及び無線伝送システムにおいても本発明を適用することができる。

要するに、例示という形態で本発明を開示してきたのであり、本明細書の記載

内容を限定的に解釈するべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

[産業上の利用可能性]

5

本発明によれば、所定の通信セル内でワイヤレス接続された機器間でオーディオ・データを好適に伝送することができる、優れた無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムを提供することができる。

10 また、本発明によれば、Bluetoothのように1台のマスタ(master)機器と複数台のスレーブ(slave)機器によって構成されるピコネット(piconet)内において機器間でオーディオ・データを好適に伝送することができる、優れた無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムを提供することができる。

15 また、本発明によれば、オーディオ・データなどのデジタル・データに所定のプロテクションを施しながらBluetooth機器間で伝送することができる、優れた無線通信システム、無線通信制御装置及び無線通信制御方法、記憶媒体、並びにコンピュータ・プログラムを提供することができる。

20 本発明によれば、オーディオ・データなどプロテクションを施す必要があるデータをBluetooth接続により伝送する場合、通信相手となる機器の処理能力に応じて認証の難易度を切り替えることができ、Bluetoothによるセキュアなオーディオ伝送を実現することができる。したがって、ヘッドホンのような低い処理能力の機器であっても、SDMIに準拠したBluetooth通信を行なうことができる。また、通信相手がパーソナル・コンピュータのよう
25 に高い処理能力を持つ機器に対しては、十分なハッキング対策を施すことができる。

請求の範囲

1. 所定の無線セル内でデータ・ストリームを送信するS o u r c e装置とデータ・ストリームを受信するS i n k装置とからなる無線通信システムであって、
- 5 前記S i n k装置の処理能力を判別する判別手段と、
該判別された前記S i n k装置の処理能力に応じて、前記S o u r c e装置との前記S i n k装置間の認証方式を決定する認証制御手段と、
を具備することを特徴とする無線通信システム。
- 10 2. 前記判別手段は、前記S i n k装置が処理能力の低い第1のタイプの装置か、又は、処理能力の高い第2のタイプの装置かを判別する、
ことを特徴とする請求項1に記載の無線通信システム。
- 15 3. 前記認証制御手段は、前記S i n k装置が第1のタイプの場合は比較的簡単な認証方式を採用し、前記S i n k装置が第2のタイプの場合は比較的複雑な認証方式を採用する、
ことを特徴とする請求項2に記載の無線通信システム。
- 20 4. 前記判別手段は、前記S i n k装置からの自己申告を基に前記S i n k装置の処理能力を判別する、
ことを特徴とする請求項1に記載の無線通信システム。
- 25 5. 前記判別手段は、前記S i n k装置の種別を基に前記S i n k装置の処理能力を判別する、
ことを特徴とする請求項1に記載の無線通信システム。
6. 前記判別手段は、前記S i n k装置がサポートするサービスを基に前記S i n k装置の処理能力を判別する、
ことを特徴とする請求項1に記載の無線通信システム。

7. 前記無線セルは、Bluetoothワイヤレス・ネットワークにより構築され、

前記判別手段は、オーディオ伝送用のAVDTP (Audio Video Distribution Transport Protocol) プロトコルで定義される Stream Get Capability コマンドを用いて前記Sink装置からの自己申告を基に前記Sink装置の処理能力を判別する、
5 ことを特徴とする請求項1に記載の無線通信システム。

8. 前記無線セルは、Bluetoothワイヤレス・ネットワークにより構築され、
10

前記判別手段は、オーディオ伝送用のAVDTP (Audio Video Distribution Transport Protocol) プロトコルで定義される Security Control コマンドを用いて前記Sink装置に処理能力を問い合わせる、
ことを特徴とする請求項1に記載の無線通信システム。

15

9. 前記無線セルは、Bluetoothワイヤレス・ネットワークにより構築され、

前記判別手段は、問い合わせ (Inquiry) 処理手順の際に入手した Class of Device 情報を基に、前記Sink装置の処理能力を判別する、
20 ことを特徴とする請求項1に記載の無線通信システム。

10. 前記無線セルは、Bluetoothワイヤレス・ネットワークにより構築され、

前記判別手段は、サービス・ディスカバリ (Service Discovery) によって取得された前記Sink装置が対応するサービス (プロトコル又はプロファイル) によってその処理能力を判別する、
25 ことを特徴とする請求項1に記載の無線通信システム。

11. 前記判別手段は、前記Sink装置がA2DP (Bluetooth Advanced Audio

Distribution Profile) にのみ対応している場合には、前記Sink装置が処理能力の低い第1のタイプであると判断する、
ことを特徴とする請求項10に記載の無線通信システム。

- 5 12. 前記判別手段は、前記Sink装置がPAN (Personal Area Network)、LAN (LAN Access Profile)、Object Push、又は、File Transferのうち少なくとも1つのプロファイルに対応している場合には、前記Sink装置が処理能力の低い第1のタイプではないと判断する、
ことを特徴とする請求項10に記載の無線通信システム。

10

13. 所定の無線セル内でSink装置に対してデータ・ストリームを送信する無線通信制御装置であって、

前記Sink装置の処理能力を判別する判別手段と、

該判別された前記Sink装置の処理能力に応じて、前記Source装置と

- 15 の前記Sink装置間の認証方式を決定する認証制御手段と、
を具備することを特徴とする無線通信制御装置。

14. 前記判別手段は、前記Sink装置が処理能力の低い第1のタイプの装置か、又は、処理能力の高い第2のタイプの装置かを判別する、

- 20 ことを特徴とする請求項13に記載の無線通信制御装置。

15. 前記認証制御手段は、前記Sink装置が第1のタイプの場合は比較的簡単な認証方式を採用し、前記Sink装置が第2のタイプの場合は比較的複雑な認証方式を採用する、

- 25 ことを特徴とする請求項14に記載の無線通信制御装置。

16. 前記判別手段は、前記Sink装置からの自己申告を基に前記Sink装置の処理能力を判別する、

ことを特徴とする請求項13に記載の無線通信制御装置。

17. 前記判別手段は、前記Sink装置の種別を基に前記Sink装置の処理能力を判別する、
ことを特徴とする請求項13に記載の無線通信制御装置。
- 5 18. 前記判別手段は、前記Sink装置がサポートするサービスを基に前記Sink装置の処理能力を判別する、
ことを特徴とする請求項13に記載の無線通信制御装置。
- 10 19. 前記無線セルは、Bluetoothワイヤレス・ネットワークにより構築され、
前記判別手段は、オーディオ伝送用のAVDTP (Audio Video Distribution Transport Protocol) プロトコルで定義されるStream Get Capability コマンドを用いて前記Sink装置からの自己申告を基に前記Sink装置の処理能力を判別する、
15 ことを特徴とする請求項13に記載の無線通信制御装置。
- 20 20. 前記無線セルは、Bluetoothワイヤレス・ネットワークにより構築され、
前記判別手段は、オーディオ伝送用のAVDTP (Audio Video Distribution Transport Protocol) プロトコルで定義されるSecurity Control コマンドを用いて前記Sink装置に処理能力を問い合わせる、
ことを特徴とする請求項13に記載の無線通信制御装置。
- 25 21. 前記無線セルは、Bluetoothワイヤレス・ネットワークにより構築され、
前記判別手段は、問い合わせ (Inquiry) 処理手順の際に入手したClass of Device 情報を基に、前記Sink装置の処理能力を判別する、
ことを特徴とする請求項13に記載の無線通信制御装置。

22. 前記無線セルは、Bluetoothワイヤレス・ネットワークにより構築され、

前記判別手段は、サービス・ディスカバリ (Service Discovery) によって取得された前記Sink装置が対応するサービス (プロトコル又はプロファイル) によってその処理能力を判別する、
5 ことを特徴とする請求項13に記載の無線通信制御装置。

23. 前記判別手段は、前記Sink装置がA2DP (Bluetooth Advanced Audio Distribution Profile) にのみ対応している場合には、前記Sink装置が処理
10 能力の低い第1のタイプであると判断する、
ことを特徴とする請求項22に記載の無線通信制御装置。

24. 前記判別手段は、前記Sink装置がPAN (Personal Area Network)、LAN (LAN Access Profile)、Object Push、又は、File Transferのうち少なくとも1つのプロファイルに対応している場合には、前
15 記Sink装置が処理能力の低い第1のタイプではないと判断する、
ことを特徴とする請求項22に記載の無線通信制御装置。

25. 所定の無線セル内でSink装置に対するデータ・ストリームの送信を制御する無線通信制御方法であって、

前記Sink装置の処理能力を判別する判別ステップと、

該判別された前記Sink装置の処理能力に応じて、前記Source装置との前記Sink装置間の認証方式を決定する認証制御ステップと、
を具備することを特徴とする無線通信制御方法。

25

26. 前記判別ステップでは、前記Sink装置が処理能力の低い第1のタイプの装置か、又は、処理能力の高い第2のタイプの装置かを判別する、
ことを特徴とする請求項25に記載の無線通信制御方法。

27. 前記認証制御ステップでは、前記Sink装置が第1のタイプの場合は比較的簡単な認証方式を採用し、前記Sink装置が第2のタイプの場合は比較的複雑な認証方式を採用する、
ことを特徴とする請求項26に記載の無線通信制御方法。

5

28. 前記判別ステップでは、前記Sink装置からの自己申告を基に前記Sink装置の処理能力を判別する、
ことを特徴とする請求項25に記載の無線通信制御方法。

10 29. 前記判別ステップでは、前記Sink装置の種別を基に前記Sink装置の処理能力を判別する、
ことを特徴とする請求項25に記載の無線通信制御方法。

15 30. 前記判別ステップでは、前記Sink装置がサポートするサービスを基に前記Sink装置の処理能力を判別する、
ことを特徴とする請求項25に記載の無線通信制御方法。

31. 前記無線セルは、Bluetoothワイヤレス・ネットワークにより構築され、
20 前記判別ステップでは、オーディオ伝送用のAVDTP (Audio Video Distribution Transport Protocol) プロトコルで定義される Stream Get Capability コマンドを用いて前記Sink装置からの自己申告を基に前記Sink装置の処理能力を判別する、
ことを特徴とする請求項25に記載の無線通信制御方法。

25

32. 前記無線セルは、Bluetoothワイヤレス・ネットワークにより構築され、

前記判別ステップでは、オーディオ伝送用のAVDTP (Audio Video Distribution Transport Protocol) プロトコルで定義される Security Control

コマンドを用いて前記Sink装置に処理能力を問い合わせる、
ことを特徴とする請求項25に記載の無線通信制御方法。

33. 前記無線セルは、Bluetoothワイヤレス・ネットワークにより構築され、

前記判別ステップでは、問い合わせ(Inquiry) 処理手順の際に入手したClass of Device 情報を基に、前記Sink装置の処理能力を判別する、
ことを特徴とする請求項25に記載の無線通信制御方法。

10 34. 前記無線セルは、Bluetoothワイヤレス・ネットワークにより構築され、

前記判別ステップでは、サービス・ディスカバリ(Service Discovery) によって取得された前記Sink装置が対応するサービス(プロトコル又はプロファイル) によってその処理能力を判別する、

15 ことを特徴とする請求項25に記載の無線通信制御方法。

35. 前記判別ステップでは、前記Sink装置がA2DP (Bluetooth Advanced Audio Distribution Profile) にのみ対応している場合には、前記Sink装置が処理能力の低い第1のタイプであると判断する、

20 ことを特徴とする請求項34に記載の無線通信制御方法。

36. 前記判別ステップでは、前記Sink装置がPAN(Personal Area Network)、LAN (LAN Access Profile)、Object Push、又は、File Transferのうち少なくとも1つのプロファイルに対応している場合には、前記Sink装置が処理能力の低い第1のタイプではないと判断する、

25 ことを特徴とする請求項34に記載の無線通信制御方法。

37. 所定の無線セル内でSink装置に対するデータ・ストリームの送信制御をコンピュータ・システム上で実行するように記述されたコンピュータ・ソフト

ウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ・ソフトウェアは、

前記Sink装置の処理能力を判別する判別ステップと、

該判別された前記Sink装置の処理能力に応じて、前記Source装置と

5 の前記Sink装置間の認証方式を決定する認証制御ステップと、

を具備することを特徴とする記憶媒体。

38. 所定の無線セル内でSink装置に対するデータ・ストリームの送信制御をコンピュータ・システム上で実行するように記述されたコンピュータ・プログ

10 ラムであって、

前記Sink装置の処理能力を判別する判別ステップと、

該判別された前記Sink装置の処理能力に応じて、前記Source装置との前記Sink装置間の認証方式を決定する認証制御ステップと、

を具備することを特徴とするコンピュータ・プログラム。

1/14

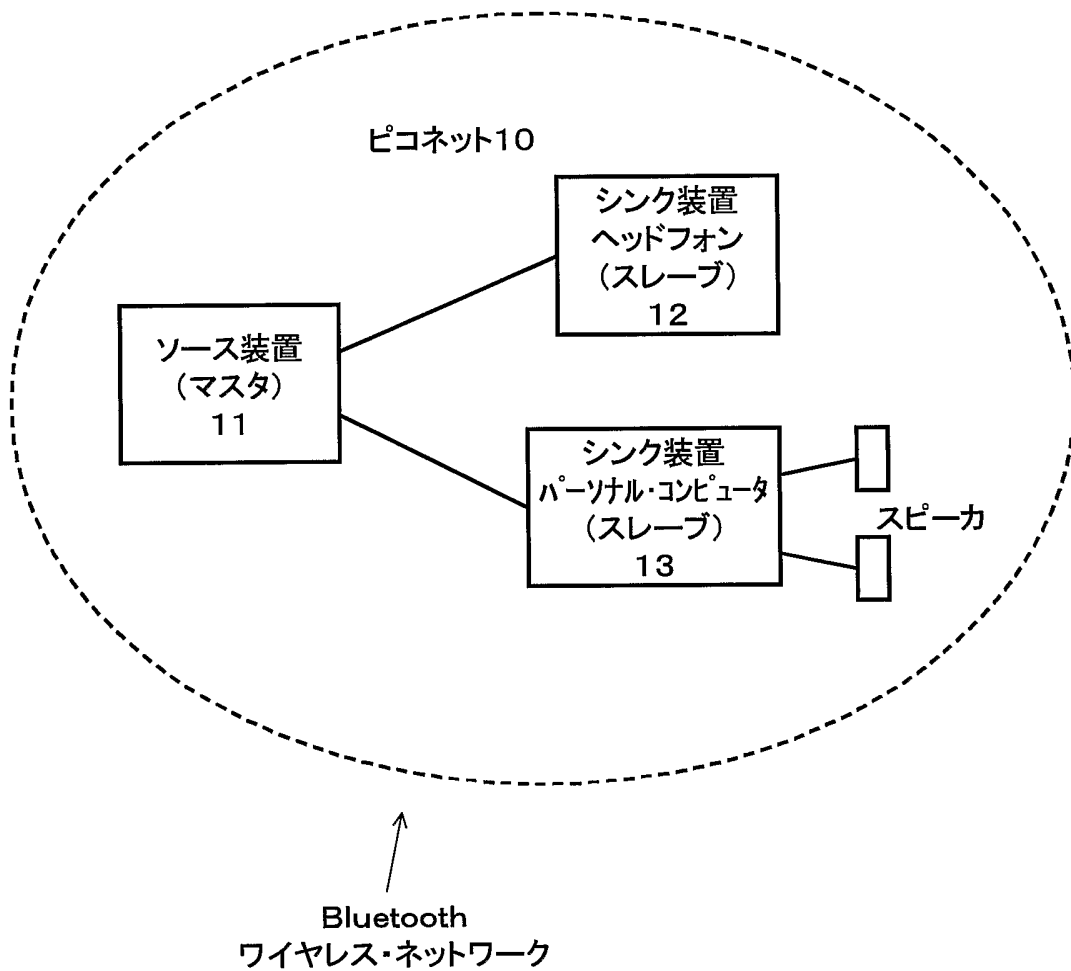


図 1

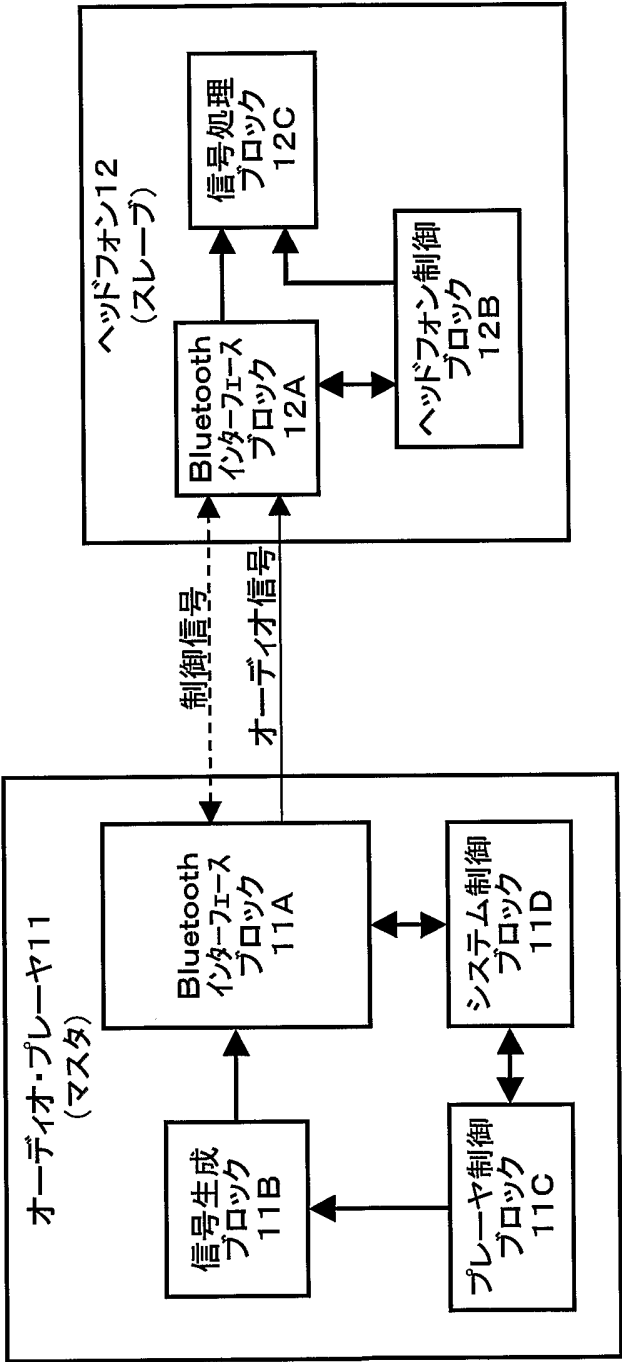


図2

3/14

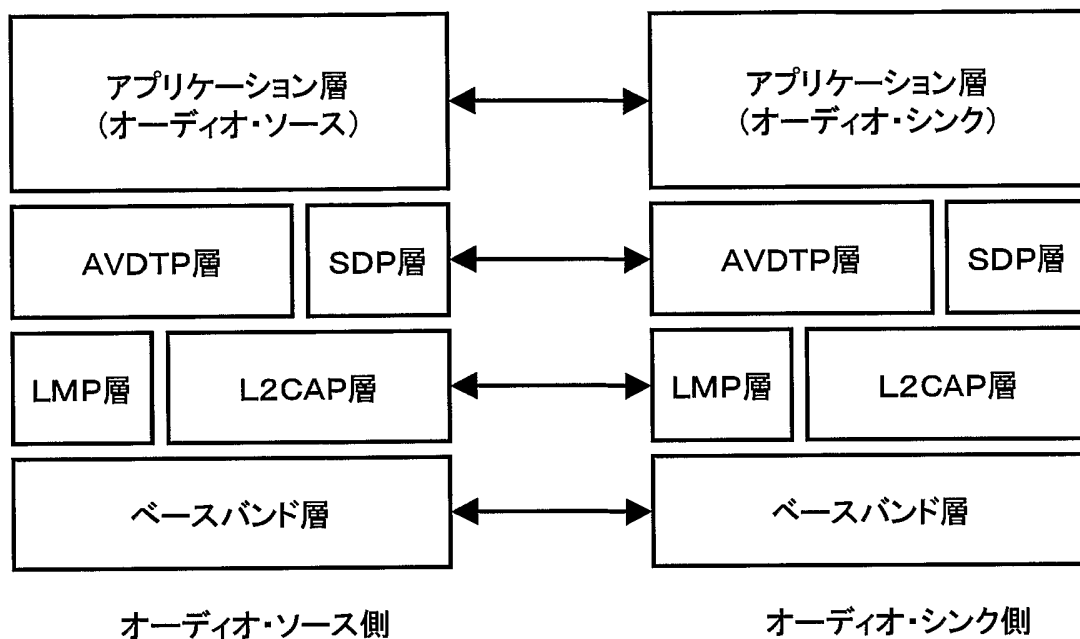


図3

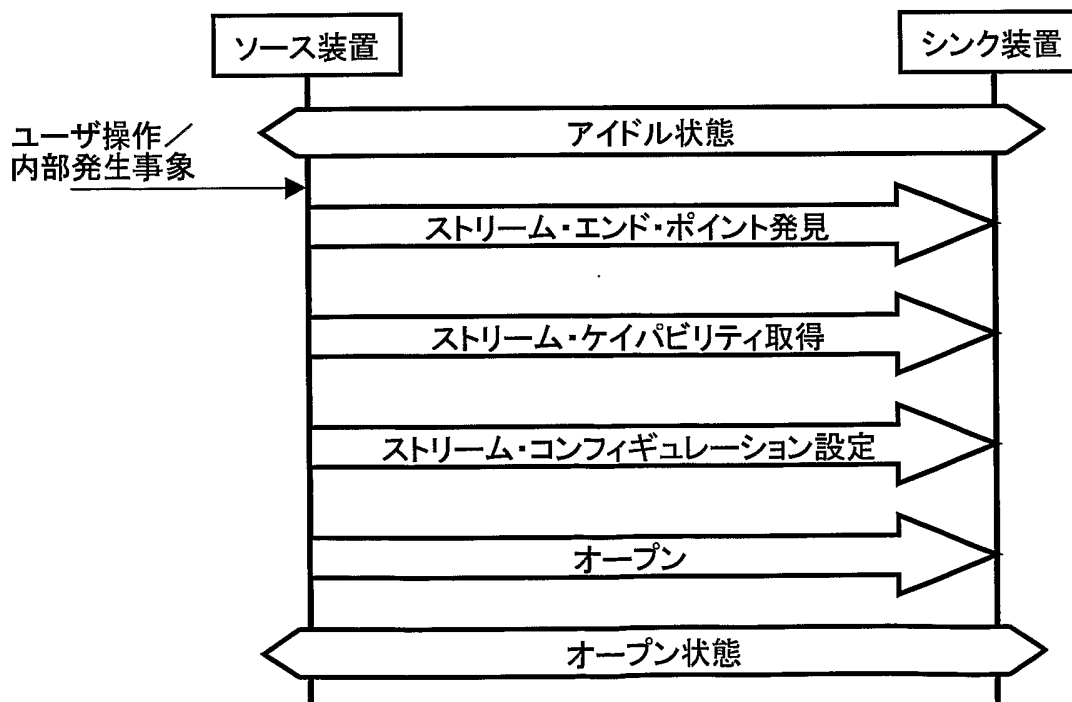


図4

4/14

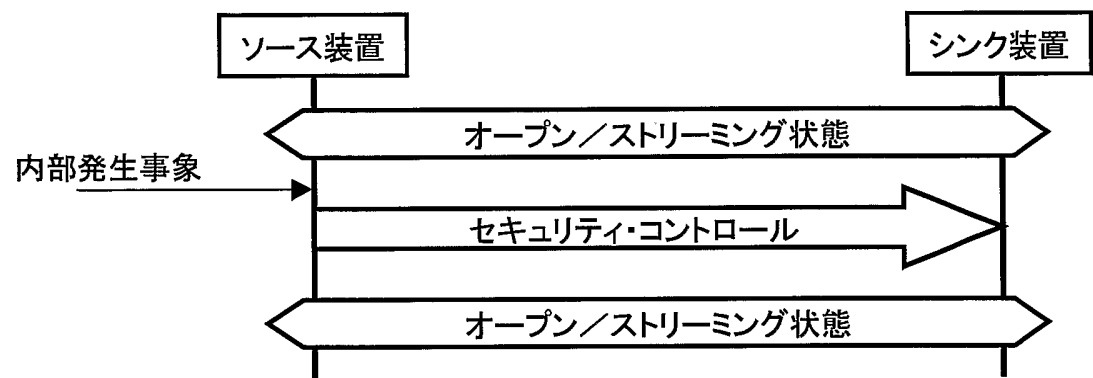


図5

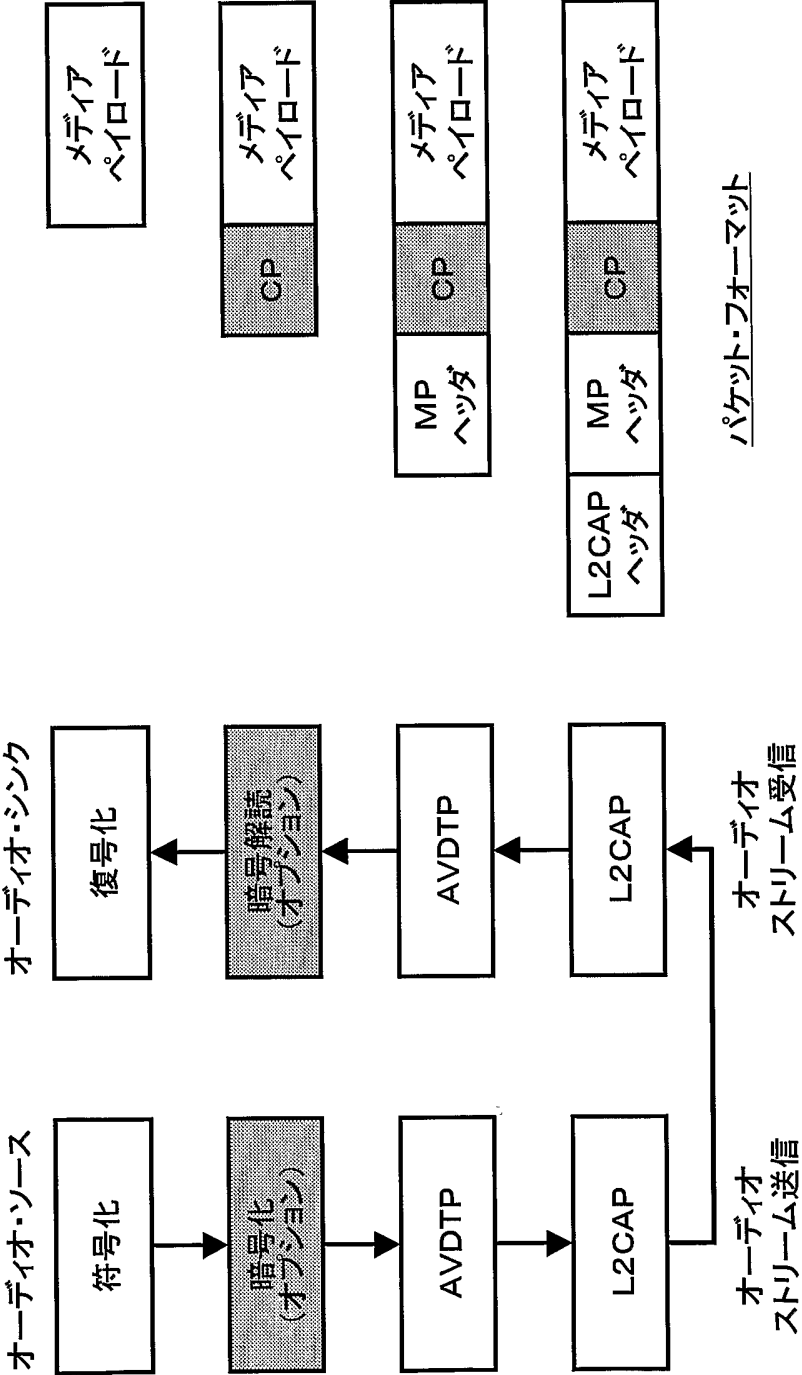


図6

6/14

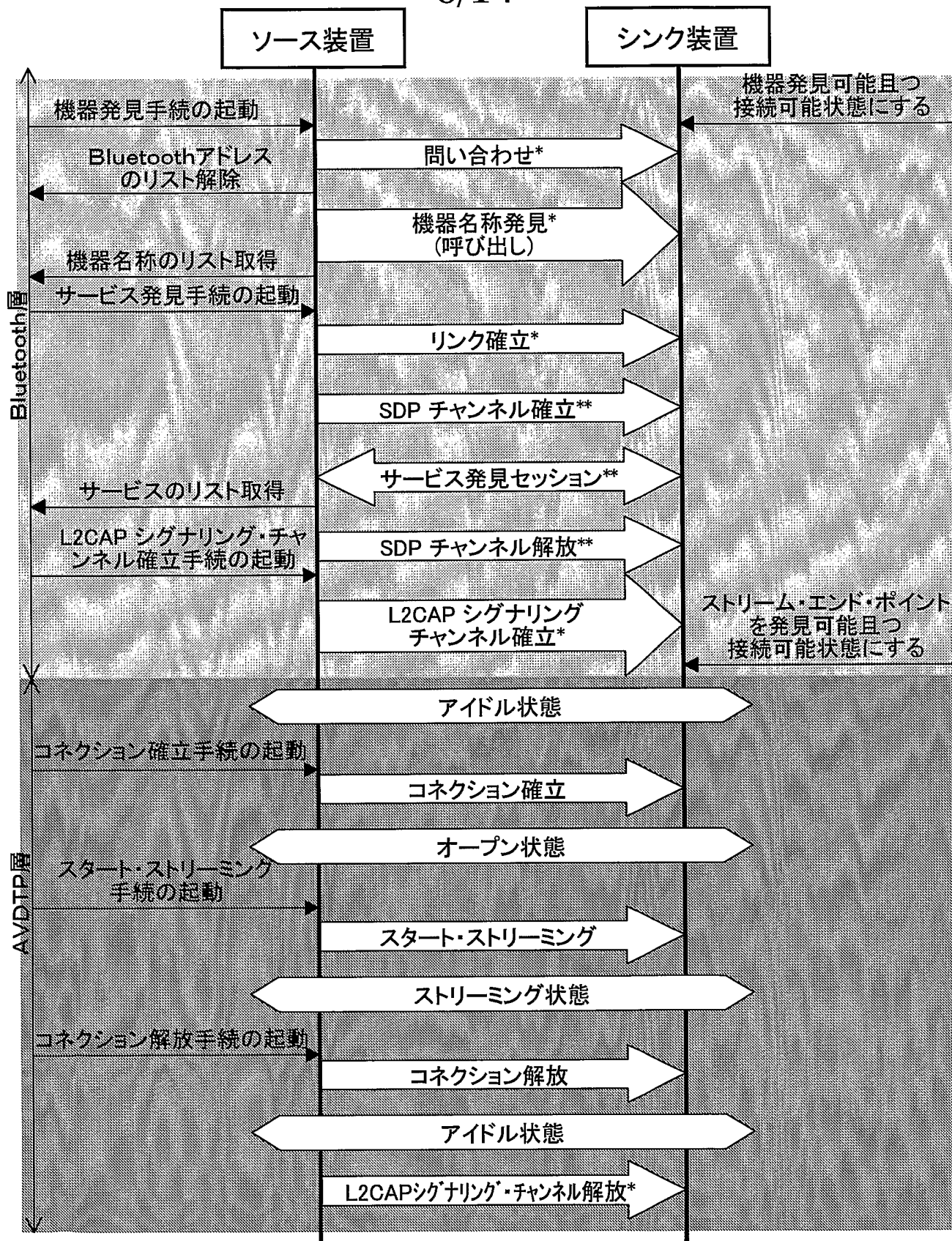


図7

7/14

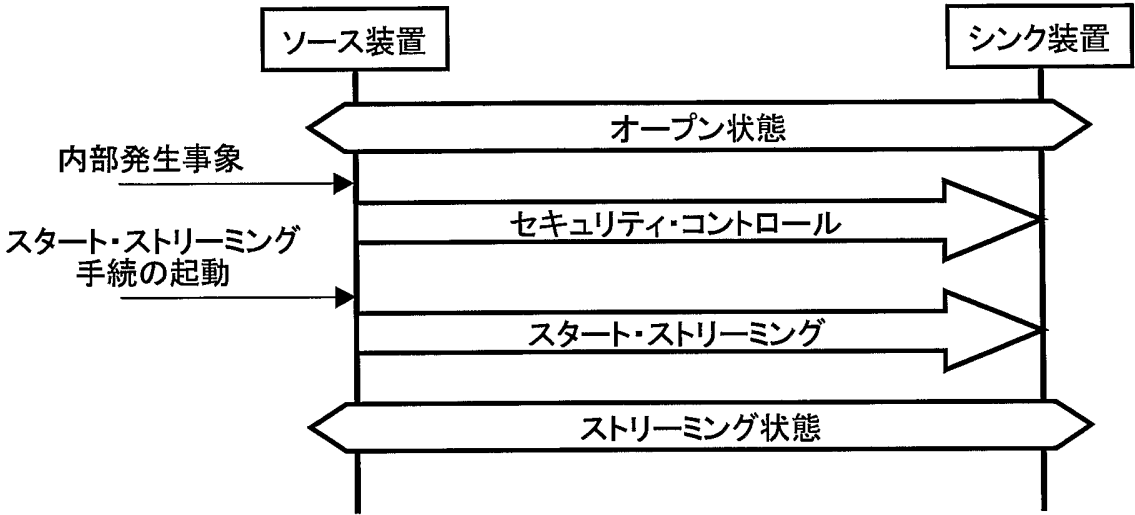


図8

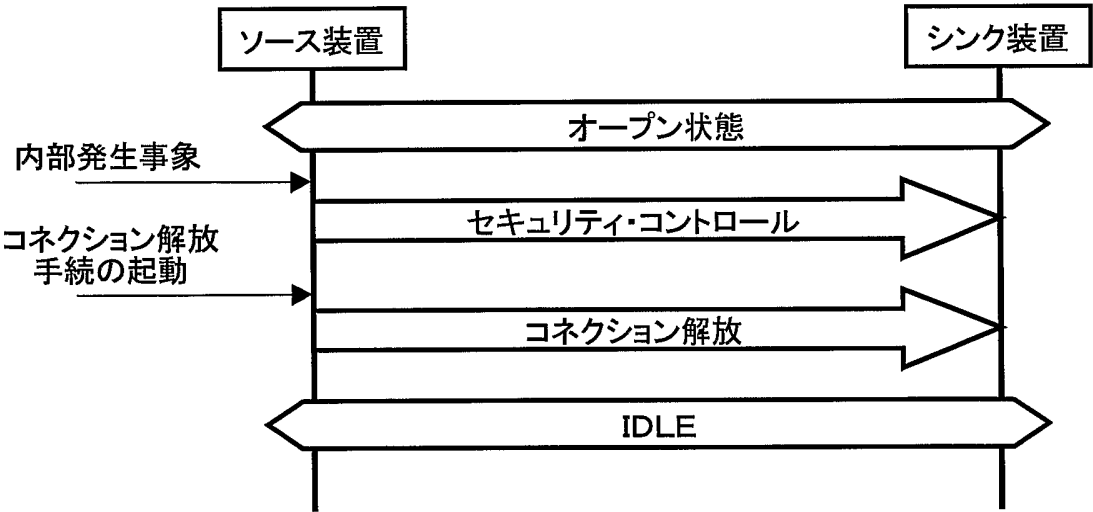


図9

8/14

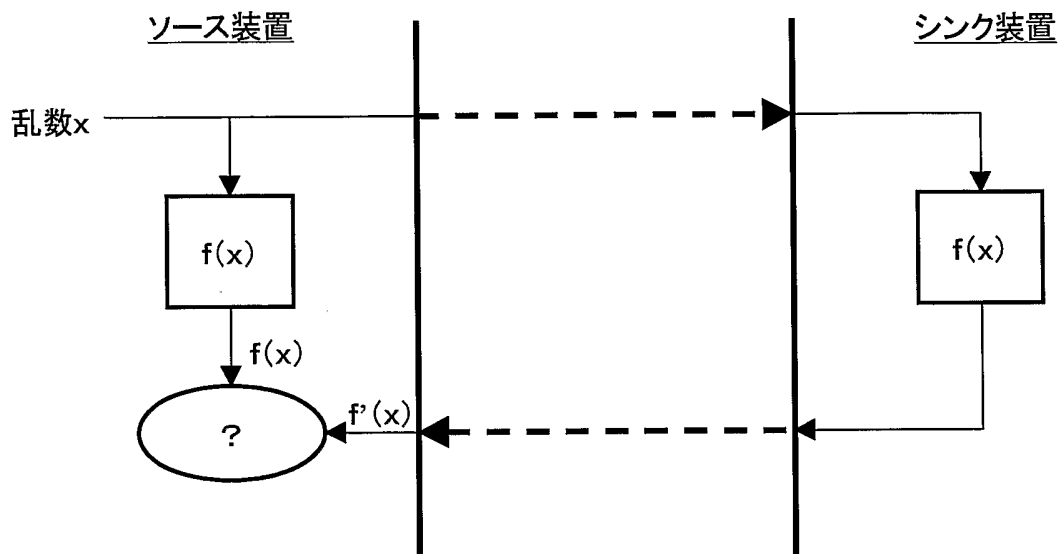


図10

7	6	5	4	3	2	1	0	Octet
シグナリング・ヘッダ								0
0	0	AVDTP_GET_CAPABILITIES						1
ストリーム・エンドポイント識別子 (SEID)						1	1	2

図11

7	6	5	4	3	2	1	0	Octet
シグナリング・ヘッダ								0
1	0	AVDTP_GET_CAPABILITIES						1
ストリーム・エンド・ポイント識別子 (SEID)						使用中	1	2
サービス・ケイパビリティ								3

図12

9/14

7	6	5	4	3	2	1	0	Octed
サービス・カテゴリ=コンテンツ・プロテクション								0
Length Of Service Capabilities(LOSC)=0x02								1
CP_TYPE_LSB								2
CP_TYPE_MSB								3

図13

7	6	5	4	3	2	1	0	Octed
シグナリング・ヘッダ								0
0	0	AVDTP_SECURITY_CONTROL						1
ストリーム・エンド・ポイント識別子(SEID)						1	1	2
Content Protection Scheme Dependent								⋮

図14

7	6	5	4	3	2	1	0	Octed
シグナリング・ヘッダ								0
1	0	AVDTP_SECURITY_CONTROL						1
ストリーム・エンド・ポイント識別子(SEID)						1	1	2
Content Protection Scheme Dependent								3

図15

10/14

コマンド種別:タイプ問い合わせ	0	0	0	0
-----------------	---	---	---	---

図16

レスポンス種別:タイプ	値(0~15)
-------------	---------

図17

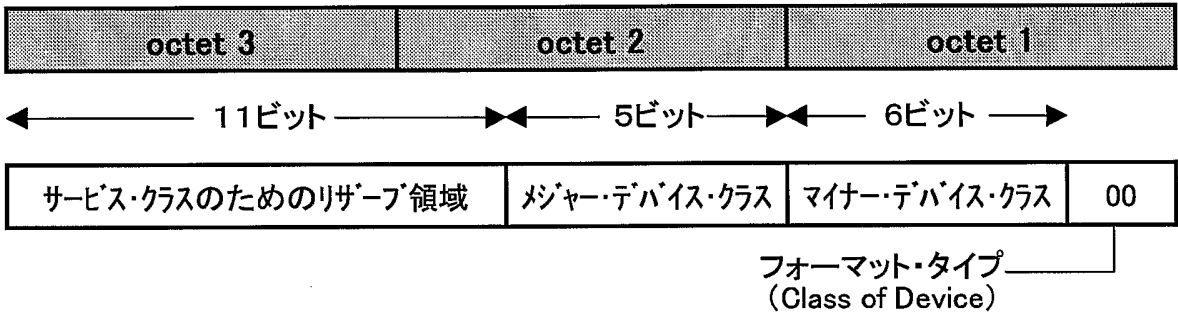


図18

12 11 10 9 8	メジャー・デバイス・クラス
0 0 0 0 0	その他
0 0 0 0 1	コンピュータ(デスクトップ、ノートブック、PDA、オルガナイザ)
0 0 0 1 0	電話(セルラ、コードレス、公衆電話、モデム、...)
0 0 0 1 1	LAN/ネットワークのアクセス・ポイント
0 0 1 0 0	音響/映像(ヘッドセット、スピーカ、ステレオ、ビデオ・ディスプレイ、VCR)
0 0 1 0 1	周辺機器(マウス、ジョイスティック、キーボード)
0 0 1 1 0	画像処理(印刷、スキャナ、カメラ、ディスプレイ、...)
1 1 1 1 1	分類されない特定のデバイス・コード
X X X X X	予約された他のすべての値

図19

11/14

コマンド種別：認証	0	0	0	0
x				

図20

レスポンス種別：認証	0	0	0	0
f(x)				

図21

12/14

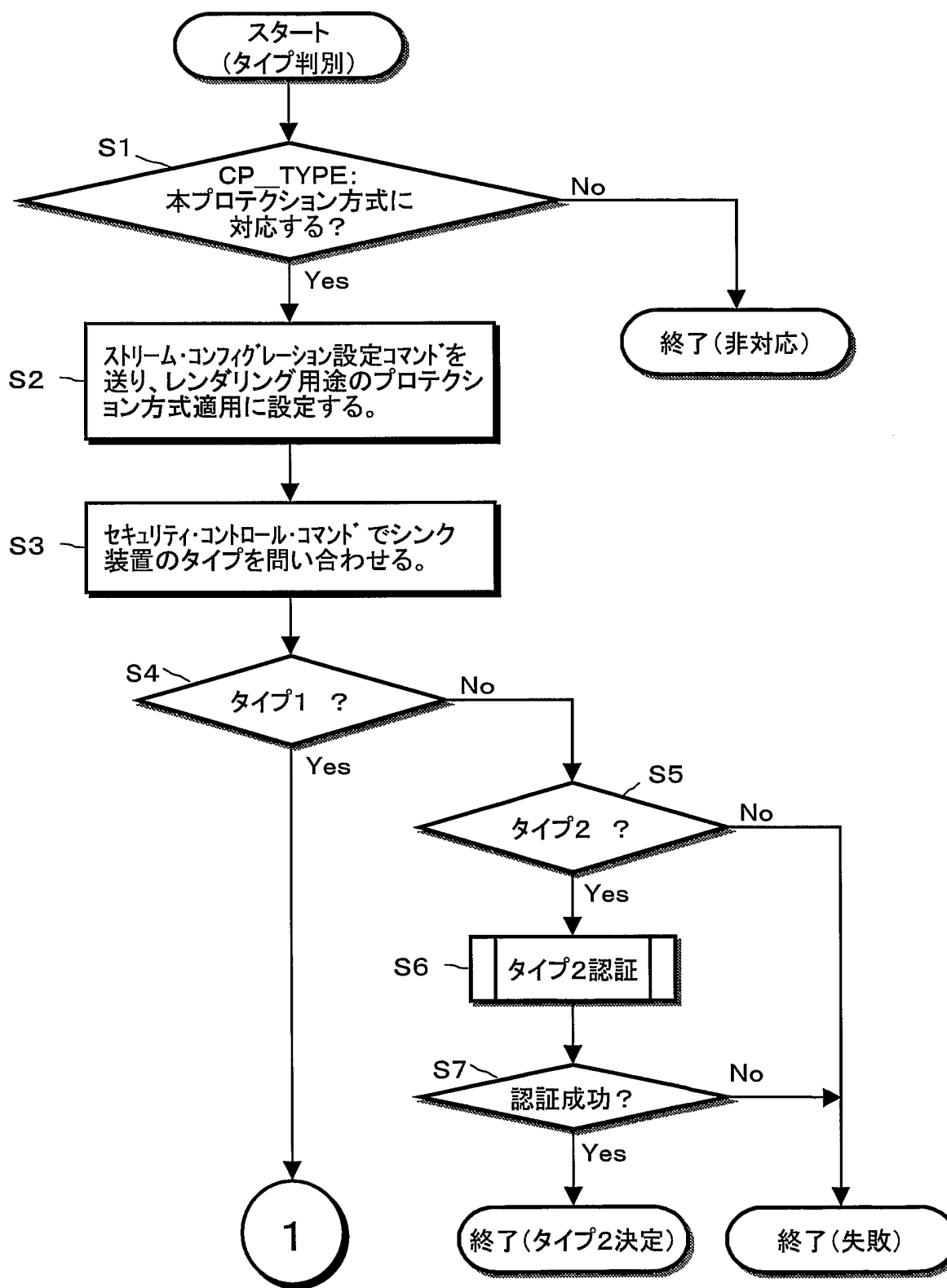


図22

13/14

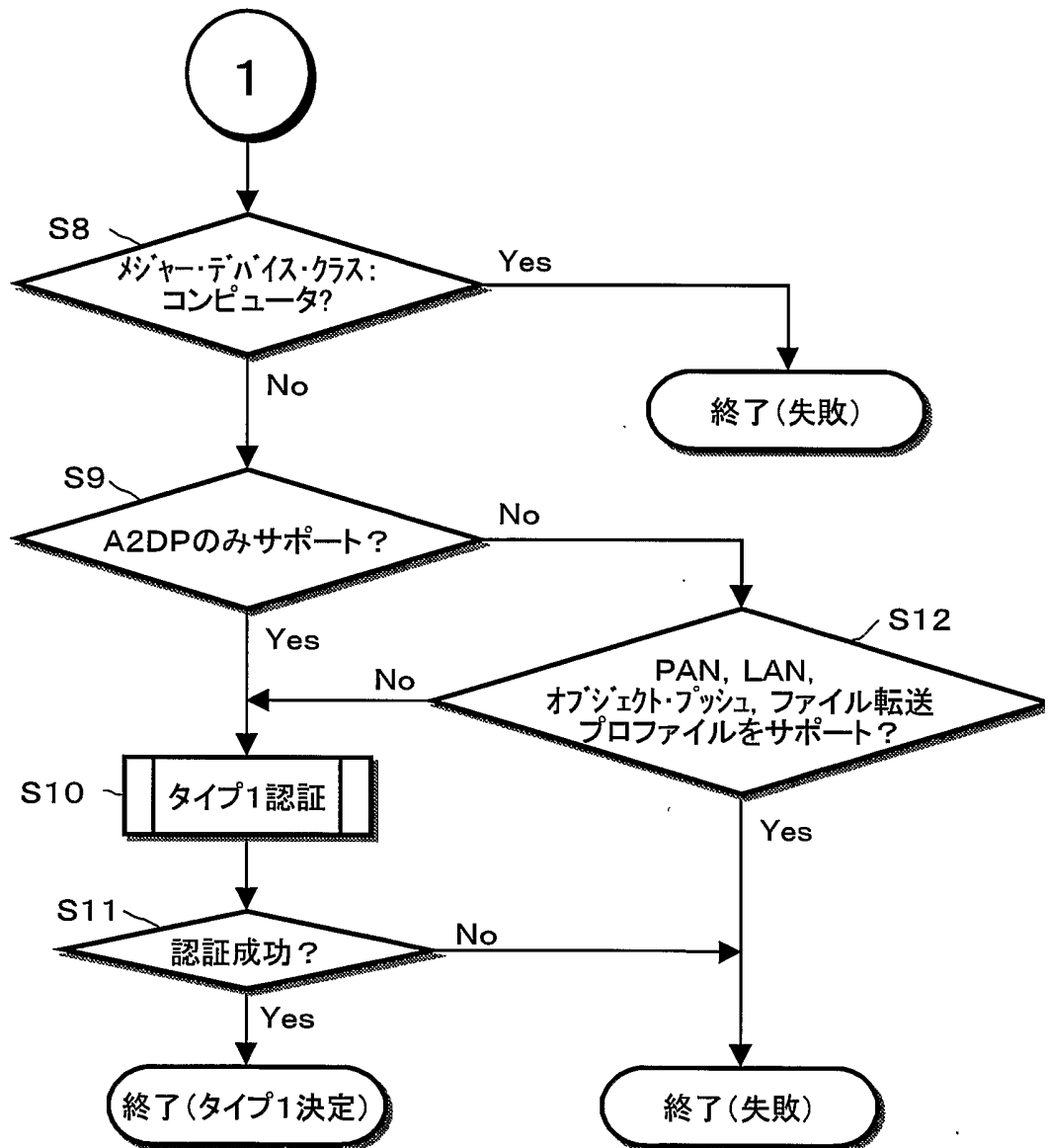


図23

14/14

Profile Name	UUID
シリアル・ポート	0x1101
LAN アクセス	0x1102
ダイヤルアップ・ネットワーキング	0x1103
オブジェクト・プッシュ	0x1105
ファイル・トランスファー	0x1106
ヘッドセット	0x1108
アドバンスト・オーディオ ディストリビューション	0x110D
A/V リモート・コントロール	0x110F
PAN	0x1115

図24

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/07714

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl.⁷ H04L12/28

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.⁷ H04L12/28, H04L9/00-9/04, H04K1/00-3/00, G06F15/00

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

Jitsuyo Shinan Koho 1940-2002

Kokai Jitsuyo Shinan Koho 1971-2002

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	JP 2000-59323 A (Matsushita Electric Industrial Co., Ltd.), 25 February, 2000 (25.02.00), Full text	1-3, 13-15, 25-27, 37, 38
A	& WO 99/41910 A1 & EP 977436 A & CN 1263669 T	4-12, 16-24, 28-36
Y	JP 6-261033 A (Nippon Telegraph And Telephone Corp.), 16 September, 1994 (16.09.94), Full text	1-3, 13-15, 25-27, 37, 38
A	(Family: none)	4-12, 16-24, 28-36

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

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier document but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search
25 October, 2002 (25.10.02)Date of mailing of the international search report
12 November, 2002 (12.11.02)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/07714

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 8-297638 A (Nippon Telegraph And Telephone Corp.), 12 November, 1996 (12.11.96),	1-3, 13-15, 25-27, 37, 38
A	Full text (Family: none)	4-12, 16-24, 28-36
P, A	JP 2001-312472 A (Toshiba Corp.), 09 November, 2001 (09.11.01), Full text (Family: none)	1-38

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L12/28

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. Cl⁷ H04L12/28Int. Cl⁷ H04L9/00-9/04Int. Cl⁷ H04K1/00-3/00Int. Cl⁷ G06F15/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1940-2002

日本国公開実用新案公報 1971-2002

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	JP 2000-59323 A (松下電器産業株式会社) 200 0.02.25, 全文 & WO99/41910 A1 & E P 977436 A & CN 1263669 T	1-3, 13 -15, 25 -27, 37, 38
A		4-12, 16-24, 28-36

☒ 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

25.10.02

国際調査報告の発送日

12.11.02

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)

宮 島 郁 美



5X 8523

電話番号 03-3581-1101 内線 3595

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	J P 6-261033 A (日本電信電話株式会社) 1994. 09. 16, 全文 (ファミリーなし)	1-3, 13 -15, 25 -27, 37, 38
A		4-12, 16-24, 28-36
Y	J P 8-297638 A (日本電信電話株式会社) 1996. 11. 12, 全文 (ファミリーなし)	1-3, 13 -15, 25 -27, 37, 38
A		4-12, 16-24, 28-36
PA	J P 2001-312472 A (株式会社東芝) 2001. 1 1. 09, 全文 (ファミリーなし)	1-38