

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2012-142005

(P2012-142005A)

(43) 公開日 平成24年7月26日(2012.7.26)

(51) Int.Cl.	F I	テーマコード (参考)
G06Q 30/06 (2012.01)	G06F 17/60 302E	5J104
G06Q 30/04 (2012.01)	G06F 17/60 332	
G06Q 10/00 (2012.01)	G06F 17/60 506	
H04L 9/08 (2006.01)	H04L 9/00 601B	
	H04L 9/00 601E	

審査請求 有 請求項の数 22 O L (全 15 頁)

(21) 出願番号 特願2012-41522 (P2012-41522)
 (22) 出願日 平成24年2月28日 (2012.2.28)
 (62) 分割の表示 特願2001-502379 (P2001-502379)
 の分割
 原出願日 平成11年6月2日 (1999.6.2)

(特許庁注：以下のものは登録商標)

1. GSM

(71) 出願人 509243296
 スイスコム (シュバイツ) アーゲー
 スイス国. CH-3050 ベルン, アル
 ティフェンアウシュトラッセ 6
 (74) 代理人 100094112
 弁理士 岡部 譲
 (74) 代理人 100064447
 弁理士 岡部 正夫
 (74) 代理人 100128657
 弁理士 三山 勝巳
 (74) 代理人 100160967
 弁理士 ▲濱▼口 岳久
 (72) 発明者 フーバー, アドリアノ
 スイス国. シーエッチー6600 ロカル
 ノ, ヴィア エフ. カボネリ 35
 最終頁に続く

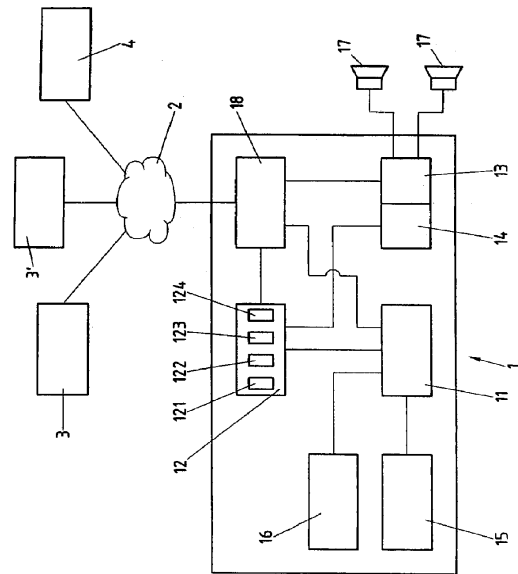
(54) 【発明の名称】 メディア・オブジェクトを注文および送達するための方法およびそれに適した設備

(57) 【要約】 (修正有)

【課題】 デジタル・メディア・オブジェクトを販売および使用するための方法、ならびにこれに適した移动通信端末を提供する。

【解決手段】 メディア・オブジェクトがユーザによってその移动通信端末1を用いてセンタ3から注文され、センタ3から無線ネットワーク2を通じて移动通信端末1に伝送され、そこで伝送されたメディア・オブジェクトはメモリ12中に記憶され、記憶されたメディア・オブジェクトに含まれるメディア・コンテンツは前記通信端末1のメディア再生モジュール(13)を通じて適当なメディアによって再生される。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

デジタル・メディア・オブジェクト(6)を注文および送達するための方法であって

、
移動通信端末(1)によって、少なくとも1つのオブジェクト識別名を含むデジタル・メディア・オブジェクト(6)のためのオブジェクト注文が移動無線ネットワーク(2)を通じてセンタ(3)に送達され、

オブジェクト識別名に割り当てられたメディア・オブジェクト(6)は、センタ(3)から移動無線ネットワーク(2)を通じて通信端末(1)に送達されて、ここでメモリ(12)に記憶され、

通信端末(1)のメディア再生モジュール(13)が、記憶されたメディア・オブジェクト(6)の中に含まれるメディア・コンテンツ(62)を適当なメディアを通じて再生する方法。

【請求項 2】

メディア・オブジェクト(6)のメディア・コンテンツ(62)が、通信端末(1)への伝送の前に、このメディア・オブジェクト(6)に割り当てられた第1鍵(7)によって暗号化されること、およびメディア・コンテンツ(62)が、メディア再生モジュール(13)による再生の前に、解読された第1鍵(7")によって解読されることを特徴とする請求項1に記載の方法。

【請求項 3】

前記第1通信端末(1)中に記憶されたメディア・オブジェクト(6)を、この第1通信端末(1)のユーザが選択して、第2の前記通信端末(1)に転送することができ、その際このメディア・オブジェクト(6)のメディア・コンテンツ(62)は暗号化されたままであることを特徴とする請求項2に記載の方法。

【請求項 4】

メディア・オブジェクト(6)に割り当てられた鍵(7)が、公開第2鍵(9)によって暗号化された状態で当該通信端末(1)に転送され、そこで専用第3鍵(9')によって解読され、公開第2鍵(9)と専用第3鍵(9')からなる鍵の対は、当該通信端末(1)のユーザに割り当てられることを特徴とする請求項2または3に記載の方法。

【請求項 5】

個別に、または前記メディア・オブジェクト(6)に割り当てられた第1鍵(7)とともに、このメディア・オブジェクト(6)の使用条件(8)に関する記載事項も前記通信端末(1)に転送されることを特徴とする請求項4に記載の方法。

【請求項 6】

メディア・オブジェクト(6)のメディア・コンテンツ(62)を解読するために、このメディア・オブジェクト(6)に割り当てられた解読済みの第1鍵(7")が保護されて通信端末(1)の解読モジュール(14)に引き渡されることを特徴とする請求項4または5に記載の方法。

【請求項 7】

メディア・オブジェクト(6)が、当該メディア・オブジェクト(6)を取り寄せることができる前記センタ(3)に関する記載事項を含むことを特徴とする請求項1から6のいずれか一項に記載の方法。

【請求項 8】

メディア・オブジェクト(6)が、鍵サーバ(3')に関する記載事項を含み、これによって暗号化された第1鍵(7')を取り寄せることができることを特徴とする請求項2から7のいずれか一項に記載の方法。

【請求項 9】

当該通信端末(1)の鍵取り寄せモジュール(122)が、暗号化された第1鍵(7')を自動的に鍵サーバ(3')から要求し、受け取り、記憶することを特徴とする請求項8に記載の方法。

10

20

30

40

50

【請求項 10】

メディア・オブジェクト(6)が、メディア・オブジェクト(6)のメディア・コンテンツ(62)に関する記載事項、例えば価格表、題名記載事項、再生継続時間、または再生見本を含むことを特徴とする請求項1から9のいずれか一項に記載の方法。

【請求項 11】

メディア・オブジェクト(6)のメディア・コンテンツ(62)の再生について支払うために、前記メディア・オブジェクト(6)に割り当てられた金額が、前払いされて当該通信端末(1)のチップカード(5)に記憶された金額(51)から課金されることを特徴とする請求項1から10のいずれか一項に記載の方法。

【請求項 12】

メディア・オブジェクト(6)のメディア・コンテンツ(62)の再生回数が当該通信端末(1)においてカウントされること、および前記回数がライセンス・サーバ(4)に伝送されることを特徴とする請求項1から11のいずれか一項に記載の方法。

【請求項 13】

移動無線ネットワーク(2)を通じて拡張データを受信することができ、少なくとも1つのプロセッサ(11)およびこれに接続されたメモリ(12)を含む通信端末(1)において、少なくとも1つのメモリ(12)が、移動無線ネットワーク(2)を通じて受信されるデジタル・メディア・オブジェクト(6)を記憶できるような大きさであり、通信端末(1)が、移動無線ネットワーク(2)を通じて通信できるようになっており、通信端末(1)はプログラム式注文モジュール(121)を含み、このモジュールは、少なくとも1つのオブジェクト識別名を含むデジタル・メディア・オブジェクト(6)のオブジェクト注文を、移動無線ネットワーク(2)を通じてセンタ(3)へ送達できるように構成され、通信端末(1)はメディア再生モジュール(13)を含み、このモジュールは、デジタル・メディア・オブジェクト(6)の1つに含まれるメディア・コンテンツ(62)を適当なメディアを通じて再生するように構成され、

注文モジュール(121)が、オブジェクト識別名に割り当てられた、センタ(3)から移動無線ネットワーク(2)を通じて通信端末(1)に送達されたメディア・オブジェクト(6)を、メモリ(12)に記憶するように構成されていることを特徴とする通信端末(1)。

【請求項 14】

解読モジュール(14)を含み、この解読モジュールは、メディア・オブジェクト(6)の暗号化されたメディア・コンテンツ(62')を、このメディア・オブジェクト(6)に割り当てられた第1鍵(7)によって解読するように構成されていることを特徴とする請求項13に記載の通信端末(1)。

【請求項 15】

転送機能を含み、この転送機能は、記憶されたメディア・オブジェクト(6)を第2移動通信端末(1)に転送し、この場合、このメディア・オブジェクト(6)のメディア・コンテンツ(62')は暗号化されたままであることを特徴とする請求項14に記載の通信端末(1)。

【請求項 16】

鍵取り寄せモジュール(122)を含み、このモジュールは、前記メディア・オブジェクト(6)に割り当てられた鍵(7)を移動無線ネットワーク(2)を通じて鍵サーバ(3')から取り寄せるように構成されており、また通信端末(1)は第2解読機能(59)を含み、この解読機能(59)は、公開第2鍵(9)によって暗号化される受信された第1鍵(7')を専用第3鍵(9')を用いて解読するように構成されており、公開第2鍵(9)と専用第3鍵(9')からなる鍵の対は通信端末(1)のユーザに割り当てられることを特徴とする請求項14または15に記載の通信端末(1)。

【請求項 17】

鍵取り寄せモジュール(122)が、個別に、またはメディア・オブジェクト(6)に割り当てられた第1鍵(7)とともに、このメディア・オブジェクト(6)の使用条件(

10

20

30

40

50

8)に関する記載事項も取り寄せるように構成されていることを特徴とする請求項16に記載の通信端末(1)。

【請求項18】

第2解読機能(59)が、解読された第1鍵(7")を保護した状態で解読モジュール(14)に引き渡すように構成されていることを特徴とする請求項16または17に記載の通信端末(1)。

【請求項19】

鍵取り寄せモジュール(122)が、暗号化された第1鍵(7')を、メディア・オブジェクト(6)中に含まれる鍵サーバ(3')に関する記載事項に基づいて、鍵サーバ(3')から自動的に取り寄せるように構成されていることを特徴とする請求項16から18のいずれか一項に記載の通信端末(1)。

10

【請求項20】

決済モジュール(123)を含み、この決済モジュール(123)は、メディア・オブジェクト(6)のメディア・コンテンツ(62)を再生する際に、このメディア・オブジェクト(6)に割り当てられた金額を、前払いされて通信端末(1)のチップカード(5)に記憶された金額(51)から課金するように構成されていることを特徴とする請求項13から19のいずれか一項に記載の通信端末(1)。

【請求項21】

ライセンス・モジュール(52)を含み、このライセンス・モジュール(52)は、メディア・オブジェクト(6)のメディア・コンテンツ(62)の再生回数を通信端末(1)においてカウントし、この回数をライセンス・サーバ(4)に送達するように構成されていることを特徴とする請求項13から20のいずれか一項に記載の通信端末(1)。

20

【請求項22】

メモリ(12)が少なくとも1つのメモリ領域をチップカード(5)の上を含むこと、および専用第3鍵(3')がこの確実なメモリ領域に記憶されていることを特徴とする請求項13から21のいずれか一項に記載の通信端末(1)。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、メディア・オブジェクトを注文および送達するための方法およびそれに適した設備に関する。本発明は特に、デジタル・メディア・オブジェクトを注文および送達するための方法およびそれに適した設備に関する。

30

【背景技術】

【0002】

特にインターネットの普及によって、例えばソフトウェア・メディア・コンテンツ、テキスト・メディア・コンテンツ、グラフィック・メディア・コンテンツ、画像メディア・コンテンツ、オーディオ・メディア・コンテンツ、ビデオ・メディア・コンテンツ、または組合せマルチメディア・コンテンツを有するデジタル・メディア・オブジェクトを、インターネットを通じて提供し、インターネットからダウンロードしてパソコンに一時的に記憶し、これらを例えばコンパクト・ディスクなどのデータ・キャリアによって適当な例えば移動式メディア再生装置に転送し、このメディア再生装置によって再生し、またはパソコンがこれに適している場合にはパソコンによってこれを再生することが、ますます人気を高めている。デジタル・メディア・オブジェクトのために必要な伝送時間と記憶容量を減らすために、メディア・オブジェクトは圧縮された形で記憶および伝送し、再生の前またはその間に解凍することが典型的である。デジタル・メディア・オブジェクトの記憶、それぞれの圧縮/解凍のための規格、例えばMPEG-3(Moving Picture Expert Group)が使用可能であり、これは今後もさらに発展することが期待される。メディア・オブジェクトの再生に確かに興味を持つであろう多くのユーザは、インターネットからパソコンにメディア・オブジェクトを購入するために自分が指定されること、およびメディア・オブジェクトを再生するためには、扱い易い移動可

40

50

能なメディア再生装置によって先ずパソコンからこのメディア再生装置に転送しなければならないことを、大きな制限として感じる。

【0003】

特許出願EP804012では、マルチメディア受信のためのマルチメディア端末と方法が記載されており、これによって、MPEGデータまたはDABデータ(Digital Audio Broadcasting)などのマルチメディアを、特に無線ネットワークを通じて受信し、ユーザに再生することができる。EP804012に記載のマルチメディア端末は、移動無線電話などの双方向通信端末を含み、これを用いてマルチメディア・プログラムを、通信ネットワークを通じて注文してマルチメディア端末にロードすることができる。EP804012に記載の教示では、需要が多い場合には、注文されたマルチメディア・プログラムの引渡しのために必要な資源、例えば通信ネットワークおよび/または所轄のサーバは過負荷となり、ユーザにきちんとサービスすることがもはやできなくなる恐れがある。

10

【先行技術文献】

【特許文献】

【0004】

【特許文献1】国際公開第99/09718号

【特許文献2】特開平10-198610号公報

【特許文献3】特開平10-269290号公報

【特許文献4】特開平10-269289号公報

【特許文献5】特開平11-96258号公報

【特許文献6】特開平10-154185号公報

20

【発明の概要】

【発明が解決しようとする課題】

【0005】

本発明の課題は、特に上述の欠点のない、メディア・オブジェクトの注文および送達のための新しいさらによつた方法とこれに適した設備を提案することである。

【発明の効果】

【0006】

本発明により、この目的は特に独立請求項の要素によって達成される。その上に、さらなる有利な実施形態が従属請求項および説明から明らかになる。

30

例えばソフトウェア・メディア・コンテンツ、テキスト・メディア・コンテンツ、グラフィック・メディア・コンテンツ、画像メディア・コンテンツ、オーディオ・メディア・コンテンツ、ビデオ・メディア・コンテンツ、または組合せマルチメディア・コンテンツを有するデジタル・メディア・オブジェクトを、あるセンタから無線ネットワーク、例えば移動電話用無線ネットワーク、DAB無線ネットワーク(Digital Audio Broadcasting)、衛星ベースの無線ネットワーク、またはその他の無線ネットワークを通じて、移動体通信端末に転送し、ここでメモリの中にデジタル・メディア・オブジェクトを記憶する。またこの通信端末のメディア再生モジュールはメディア・オブジェクトの中に含まれたメディア・コンテンツを適当なメディアを通じて、例えば電気音響変成器によって音波として、またはディスプレイによって光波として再生する。デジタル・データをセンタから受信することができる通信端末とメディア再生モジュールとの組合せは、移動するユーザがメディア・オブジェクトを受信して再生することができる、この場合パソコンを指定する必要はなく、またメディア・オブジェクト自体をさまざまな装置の間で伝送する必要がないという利点を有する。

40

【0007】

ユーザが少なくとも1つのメディア・オブジェクトを少なくとも1つのセンタから注文し、このユーザは通信端末によって、少なくとも1つのオブジェクト識別名を包含するオブジェクト注文を移動無線ネットワーク、例えばGSMネットワーク、UMTSネットワーク、またはその他の移動ネットワークを通じてセンタに伝送し、その際、オブジェクト

50

識別名に割り当てられたメディア・オブジェクトはセンタから通信端末へ伝送される。これは、ユーザが自分の通信端末に記憶されたメディア・オブジェクトを再生できるのみならず、その上になおも自分から目的を持って自発的に所望したメディア・オブジェクトを再生のために取り寄せることができるという利点を有する。

【0008】

上述の目的は、本発明によれば、特にデジタル・メディア・オブジェクトのためのオブジェクト注文がセンタにおいて受け取られ、どの注文メディア・オブジェクトがどのセンタ決定時点に入手できるかについての記載事項が、当該通信端末に送達されること、および、当該通信端末は決定された時点に自動的にセンタと連絡を取り、この決定された時点に転送可能なメディア・オブジェクトをセンタから取り寄せることによって達成される。これは、センタがメディア・オブジェクトを伝送する際に必要な資源の満載を計画できるという利点を有する。

10

【0009】

メディア・オブジェクトのメディア・コンテンツが、通信端末への伝送の前に、第1のこのメディア・オブジェクトに割り当てられた鍵によって暗号化され、再生の前にこの第1鍵によって再び解読されることは好ましい。これによって、不当なユーザは当該のメディア・オブジェクトを不当に再生することができず、この場合、個別の第1鍵のメディア・オブジェクトへの割当てが、各メディア・オブジェクトの使用の管理を可能にし、各メディア・オブジェクトについてユーザに、例えば相応の支払いに対して鍵を自由に使用できるようにする。

20

【0010】

ある変形実施形態では、第1通信端末に記憶されたメディア・オブジェクトをこの第1通信端末のユーザが選択して、第2通信端末に転送することができ、この場合に前述のメディア・オブジェクトのメディア・コンテンツは暗号化されたままである。これは、異なるユーザは当該メディア・オブジェクトをこのメディア・オブジェクトに割り当てられた鍵なしでは再生できずに、ユーザ間での間接的な普及の可能にする。第1通信端末から第2通信端末への転送は、有線または無線のインターフェイスを通じて、例えば赤外線インターフェイス、例えば高速赤外線(HSIR)インターフェイスまたはIrDAインターフェイス(Infrared Data Association)、誘導インターフェイス、例えば無線周波数識別(RFID)インターフェイス、ホームRF(Radio Frequency)インターフェイス、欧州デジタル・コードレスフォン(DECT)インターフェイスまたはその他のコードレス遠隔通信システム(CTS)インターフェイス、または高周波無線インターフェイス、例えばいわゆる「ブルートゥース・インターフェイス」を通じて行われる。

30

【0011】

第1の上述のメディア・オブジェクトに割り当てられた鍵が、公開第2鍵によって通信端末に転送され、そこで専用第3鍵によって解読され、この場合、公開第2鍵と専用第3鍵から成る一対の鍵がその都度通信端末の当該ユーザに割り当てられることは好ましい。これによって、その都度メディア・オブジェクトに割り当てられた鍵を安全に正当なユーザに転送することができ、このユーザは、暗号化のために使用される公開第2鍵に付属する専用第3鍵を自由に使用する。

40

【0012】

ある変形実施形態では、第1のメディア・オブジェクトに割り当てられた鍵とは個別にまたは共に、このメディア・オブジェクトのための使用条件に関する記載事項もまた通信端末に転送される。これによって、この鍵により直接に使用権と価格表もまた、例えば当該メディア・オブジェクトの1回および/または多数回しかし時間的に制限された再生のためのライセンス料金および/または価格表、場合によっては限られた期間または限られた再生回数に関する記載事項も共に転送することができる。

【0013】

ある変形実施形態では、メディア・オブジェクトのメディア・コンテンツを解読するた

50

めに、前記メディア・オブジェクトに割り当てられた解読された第1鍵が安全に通信端末の解読モジュールに渡される。すなわち、通信端末における解読モジュールの実施と完成に応じて処置が取られ、これによって、解読された第1鍵を解読モジュールへの移送の際に不当に読むことは不可能である。

【0014】

メディア・オブジェクトがメディア・コンテンツに追加的に解読されていないオブジェクト情報を含むことは好ましく、この情報は、前記通信端末によって移動無線ネットワークを通じてセンタから取り寄せて、通信端末のディスプレイに表示することができ、この際、通信端末のユーザはオブジェクトの注文のために少なくとも1つのメディア・オブジェクトを決定し、そこでユーザは通信端末の操作要素によって対応するオブジェクト情報
10
を表示されたオブジェクト情報のリストから選択する。解読されていないオブジェクト情報は、例えばメディア・オブジェクトに関する価格表、メディア・オブジェクトの標識、例えば楽曲またはビデオの題名、メディア・オブジェクトの再生時間、メディア・オブジェクトの短い再生試供品、メディア・オブジェクトの1つまたは複数の解説者および/または作者、およびメディア・オブジェクトのオブジェクト識別名を含む。

【0015】

メディア・オブジェクトのオブジェクト情報が、このメディア・オブジェクトを入手することができるセンタに関する記載内容を含むことは好ましい。この記載内容を通信端末から、例えば当該のセンタと自動的に連絡をとるために使用することができる。

【0016】

メディア・オブジェクトのオブジェクト情報が、符号化された第1鍵を入手可能にする鍵サーバに関する記載内容を含むことは好ましい。これは、鍵が通信端末を通じて自動的に鍵サーバから入手でき、鍵サーバは例えば上記のセンタにおいて、または個別に実施される。
20

【0017】

ある変形実施形態では、メディア・オブジェクトのメディア・コンテンツの再生に対する支払いのために、このメディア・オブジェクトに割り当てられた金額が、前払いされて通信端末のチップカード例えばSIMカード(加入者識別モジュール)に記憶された金額に借方記入される。

【0018】

ある変形実施形態では、メディア・オブジェクトのメディア・コンテンツの再生回数が通信端末においてカウントされ、この調査された回数はライセンス・サーバに転送され、このライセンス・サーバは例えば上記のセンタにおいて、または個別に実施される。これは、これによって再生回数に依存するライセンス料金を計算できるという利点を有する。
30

【0019】

ある変形実施形態では、上記の専用第3鍵が通信端末のチップカードに記憶され、これは、当該ユーザの専用鍵を通信端末から遠ざけることができるという利点を有する。

【図面の簡単な説明】

【0020】

【図1】通信端末が無線ネットワークを通じてセンタと接続されている、メディア再生モジュールを有する通信端末を概略的に示すブロック図である。
40

【図2】第1鍵によるメディア・オブジェクトの暗号化と解読、ならびに公開第2鍵によるこの第1鍵の暗号化、および専用第3鍵によるこの第1鍵の解読を概略的に示す流れ図である。

【発明を実施するための形態】

【0021】

次に、本発明の一実施形態を例を用いて説明する。実施形態の例は添付の図面に示されている。

【0022】

図1において、参照記号1は通信端末を示し、これは適当なラジオ・モジュール18に
50

よって、例えば移動電話用の移動無線ネットワーク、例えばGSMネットワーク、UMTSネットワークまたは別の移動無線ネットワーク、DAB無線ネットワーク（デジタル音声ネットワーク）、衛星ベースの無線ネットワークまたは別の無線ネットワークを含む無線ネットワーク2を通じて、デジタル・データ、特にデジタル・メディア・オブジェクト、例えばソフトウェア・コンテンツ、テキスト・コンテンツ、グラフィック・コンテンツ、画像コンテンツ、音声コンテンツ、ビデオ・コンテンツ、または組合せマルチメディア・コンテンツを有するデジタル・メディア・オブジェクトを、センタ3から受信して、適当なデジタル・データ用のメモリ12に、例えばRAM（Random Access memory）に、ハード記憶ディスク上に、コンパクト・ディスク上に、または別の書込み可能なデータ・キャリア上に記憶することができる。書込み可能なデータ・キャリアはチップカードの形で、例えば拡張された記憶領域を有するSIMカードまたはこの目的のために適したチップカードでも実施することができ、このカードを例えば撮影個所を通じて遠隔可能に通信端末1と接続することができる。

【0023】

ここで、センタ3は無線ネットワーク2に直接接続されるべきではなく、センタは全く他の図示されていない装置を通じて無線ネットワーク2に接続できることに言及しなければならない。センタ3は例えば、直接または間接に無線ネットワーク2を通じてメディア・オブジェクトを通信端末1に転送するために、必要なソフトウェア構成部分およびハードウェア構成部分をいつでも使える商習慣上の通信サーバである。例えばセンタ3は、DAB送信機（Digital Audio Broadcasting）を含み、またはDAB送信機への入口を有し、またはセンタ3は短メッセージ・サービス・センタ（Short Message Service Center、SMSC）を含み、または短メッセージ・サービス・センタへの入口を有し、これを通じてプログラムを伴うデジタル・データ、それぞれの短メッセージ、例えばSMS短メッセージまたはUSSD短メッセージを、通信端末1の対応するラジオ・モジュール18に転送することができる。センタ3は、センタがラジオ・モジュール18のデータを例えば短メッセージの中に、例えばSMS短メッセージまたはUSSD短メッセージの中に、例えば前述の短メッセージ・サービス・センタを通じて受け取ることができる。センタ3は例えばインターネットにも接続可能であり、インターネットにおいて通信端末1は移動無線ネットワーク、例えばGSMネットワークまたはUMTSネットワークを通じて、インターネット・サービス・プロバイダを介して機会を使用することができる。後で説明する鍵サーバ3 およびライセンス・サーバ4を、センタ3においてまたは個別に、センタ3について説明したものと同様に実行することができる。

【0024】

図1に示すように、通信端末1は、少なくとも1つのプロセッサ11およびデータを具備する処理手段11を含み、プロセッサ11は、ラジオ・モジュール18と前記のメモリ12とに接続され、データは例えば受信機18から受信されるデータで、このデータをメモリ12にファイルし、その都度メモリ12に記憶されたデータ、特にデジタル・メディア・オブジェクトを取り出して処理することができる。プロセッサ11はメモリ12の中で、後で説明するプログラム式ソフトウェア・モジュール121、12、123、124も取り出して、このプログラム式ソフトウェア・モジュール121、12、123、124を実行することができる。

【0025】

プロセッサ11はさらに、操作エレメント15例えばキーボードおよびディスプレイ16例えばLCDディスプレイ（Liquid Crystal Display）に接続され、ユーザから命令およびデータを受け取り、あるいはデータ、情報、特にメディア・オブジェクトの視覚メディア・コンテンツ、およびユーザのためのストラクションを見えるように表示する。

【0026】

図2に示すように、メディア・オブジェクト6は上述のように、メディア・コンテンツ

62とオブジェクト情報61を含む。オブジェクト情報61は、当該メディア・オブジェクト6についての記載事項、例えばメディア・オブジェクト6に関する価格表、メディア・オブジェクト6の表示、例えば楽曲またはビデオの題名、メディア・オブジェクト6のオブジェクト識別名、メディア・オブジェクト6のメディア形式、メディア・オブジェクト6の再生期間、メディア・オブジェクト6の短い暗号化されていない再生見本、またはメディア・オブジェクト6の1つまたは複数の解説者および/または作者を含む。オブジェクト情報61はその上に、当該メディア・オブジェクト6を引き合いに出すことができる記載事項、例えば呼出し番号、当該センタ3のネットワーク・アドレスまたはURLアドレス(Universal Resource Locator)を含む。メディア・オブジェクト6のメディア・コンテンツが圧縮形、例えばMPEG-3(Moving Picture Expert Group)書式または別の適当な書式で、好ましくは当該メディア・オブジェクト6に割り当てられた第1鍵によって暗号化され、通信端末1に転送され、そこで記憶されることは好ましい。メディア・オブジェクト6への第1鍵7の割当ては、こうして各メディア・オブジェクト6のメディア・コンテンツ62を適当な鍵によって暗号化できるという利点を有する。メディア・オブジェクト6は、例えばデータバンクまたはセンタ3のファイル・サーバに既に圧縮されて暗号化されたメディア・コンテンツに記憶され、この際、メディア・オブジェクト6に割り当てられた第1鍵7は上述の鍵サーバ3にアクセスできるように記憶され、鍵サーバ3はプログラム式ソフトウェア・モジュールとして、センタ3のサーバまたは個別のサーバで実行される。その上に上述のオブジェクト情報61が、当該メディア・オブジェクト6を解読するための第1鍵7を引き合いに出すことができる記載事項、例えば呼出し番号、当該鍵センタ3のネットワーク・アドレスまたはURLアドレス(Universal Resource Locator)を含むことは好ましい。

【0027】

図2に示すように、メディア・オブジェクト6のメディア・コンテンツ62は、第1のメディア・オブジェクト6に割り当てられた鍵7、および例えばプログラム式ソフトウェア機能としてセンタ3で実行される第1暗号化機能70とによって、暗号化される。暗号化されたメディア・コンテンツ62は上述のように通信端末1に転送される。第1鍵7は、例えば当該ユーザに割り当てられた公開第2鍵9と専用第3鍵9とからなる鍵の対によって安全に転送される。第1鍵7は、例えば第2暗号化機能90、例えばセンタ3または鍵サーバ3におけるプログラム式ソフトウェア機能を通じて、公開第2鍵9によって暗号化される。暗号化された第1鍵7は、例えば上記の無線ネットワーク2を通じて通信端末1に転送され、ここで第2解読機能59を通じて専用第3鍵9によって解読される。暗号化された第1鍵7または解読された第1鍵7は、通信端末1において例えば通信端末1のチップカード5に記憶され、チップカード5上には図1に示すメモリ12の少なくとも一部分が存在し、または後述の解読モジュール14では外から見えない。解読された第1鍵7が通信端末1特にチップカード5に記憶されている場合には、このために必要な記憶領域はルーザーには読めないはずである。チップカード5は例えばSIMカード(加入者識別モジュール)であり、この上に例えば1つ(または複数)の専用第3鍵9も記憶される。暗号化された第1鍵7、または解読された第1鍵7、および専用第3鍵9のチップカード5への記憶は、このチップカード5を通信端末1から離すことによって、通信端末1の中に記憶されたメディア・オブジェクト6の暗号化されたメディア・コンテンツ62を不当なユーザは解読および再生ができないという利点を有する。第2解読機能59は例えば1つのプログラム式ソフトウェア機能であり、これは例えばチップカード5に記憶されてプロセッサ11例えばチップカード5上のプロセッサを通じて実行されるソフトウェア機能である。しかし第2解読機能59を解読モジュール14の中に統合することもできる。公開第2鍵9は例えばSIMカードなどのチップカード5に記憶され、通信端末1の照会にあたってその都度センタ3または鍵サーバ3に転送される。公開第2鍵9もセンタ3あるいは鍵サーバ3の首唱によってチップカード5で読み取られ、または場合によってはTTPサーバ(Trusted Third Part

y)によって取り寄せることができる。

【0028】

メディア・オブジェクト6のメディア・コンテンツ62の解読は、解読モジュール14において実施され、このモジュールは、圧縮された形で暗号化されて転送され記憶されたメディア・コンテンツ62を、当該メディア・オブジェクト6に割り当てられた解読された第1鍵7によって解読し、解読されたメディア・コンテンツをメディア再生モジュール13にさらに導く。メディア再生モジュール13は、解読されたメディア・オブジェクトを解凍し、メディア形式に応じてその中に含まれるデジタル・データを場合によってはアナログ信号に変換する機能を有し、このアナログ信号を例えばラウドスピーカまたはヘッドホンなどの電子音響変換機17にかけることができる。解読モジュール14およびメディア再生モジュール13は、例えばプログラム式ソフトウェア・モジュールとしてこれに適した信号プロセッサで、または統合されたスイッチ・ネットワークとして個別または共通チップで実行することができる。ここで、電子音響変換機17は単に変換の例として理解すべきこと、およびメディア・オブジェクト6のメディア・コンテンツ62はそのメディア形式に応じて適切なメディアに関するさまざまな方法で再生できることに言及すべきである。こうして、例えばテキスト、グラフィック、画像、ビデオ、視覚的現実シーケンスなどのメディア・オブジェクトをディスプレイ16に表示し、光波によって再生することができ、この際、例えば複合マルチメディア・オブジェクトを多くのメディアを通じて光波および音波によって再生することができる。

10

【0029】

図2にはさらに、追加的に第1鍵7によって、当該鍵7に割り当てられた当該メディア・オブジェクト6のための使用条件8に関する記載内容も提供でき、この使用条件は例えば鍵7と共に暗号化または解読された状態で通信端末1に転送できることが示されている。さらにこの使用条件8に関する記載内容を、対応する暗号化された第1鍵7または解読された第1鍵7とともに記憶することができる。使用条件8は例えば、当該メディア・オブジェクト6の一回および/または複数回であるが時間的に限られた再生に関するライセンス料金および/または価格表を、場合によっては限られた期間または限られた再生回数に関する記載事項とともに包含する。

20

【0030】

上述の図1に示す注文モジュール121は、通信端末1のユーザがセンタ3からメディア・オブジェクト6に関する暗号化されていないオブジェクト情報61を取り出し、これをディスプレイ16に表示し、そして通信端末1の操作エレメント15によってざっと見て、場合によっては利用可能な暗号化された再生された見本を再生し、望みのメディア・オブジェクトを操作エレメント15によって選択し、少なくとも1つのオブジェクト識別名を含む対応するオブジェクト注文をセンタ3に伝達することを可能にするプログラム式ソフトウェア・モジュールである。注文モジュール121は例えば、ブラウザの形で、例えば直接アクセスのための、またはWAP(Wireless Application Protocol)に基づくインターネットブラウザとして実行される。

30

【0031】

センタ3では、受信されたオブジェクト注文は記憶され、注文されたメディア・オブジェクト6はセンタ3によって、センタ3を通じて決定された時点で当該の通信端末1に伝送される。本発明によれば、オブジェクト注文はセンタ3において受け取られ、どのメディア・オブジェクト6がセンタ3によって決められたどの時点で使用可能であるかに関する記載事項が、当該通信端末1に伝送される。当該通信端末1の注文モジュール121は、センタ3によって決められた時点を注文されたメディア・オブジェクト6の伝送のために受け取り、これを記憶し、記憶された時点で自動的にセンタ3と連絡を取り、ここで決められた時点で転送可能なメディア・オブジェクト6を受け取る。伝送のための時点はセンタ3によって、この際に利用された資源、例えば無線ネットワーク2の容量またはデータバンクあるいはセンタ3のファイル・サーバができるだけ最適に利用されるように決められる。メディア・オブジェクト6の引渡しとともに、同時にまたこのメディア・オブジ

40

50

ェクトに割り当てられた第1鍵7も伝送することができ、またはこの鍵7は後述するように個別に伝送することができる。注文されたメディア・オブジェクト6の伝送はバックグラウンド処理として実行することができ、この際注文されたメディア・オブジェクト6は例えば電話通話と平行して個別のデータ・チャンネルを通じて運送される。ここで、注文されたメディア・オブジェクト6を直ちに伝送することを要望することはユーザにとって可能にもすることができ、この際これは例えばより高い料金の対応賃率モデルによって接続できることに言及すべきである。

【0032】

上述の注文モジュール121によるメディア・オブジェクト6の注文に対する代替案として、ユーザはまた例えばメディア・オブジェクト6を予約することができ、例えばこの場合、ユーザは自分が指定したメディア・オブジェクト6、例えば特定の芸術家のメディア・コンテンツ62を有する最新のメディア・オブジェクト6を、時間的に限られた予約で、または時間の制限なしにセンタ3のドライブによる取消しまで要求する。

10

【0033】

センタ3へのリターン・チャンネルのために、ラジオ・モジュール18は、無心ネットワーク2を通じてセンタ3と通信するために適用な送信機および別の構成部分を自由に使用することができ、例えばラジオ・モジュール18は移動無線電話通信モジュールの機能性を、例えばGSMネットワークまたはUMTSネットワークを通じてセンタ3と直接双方向に通信するため、もしくはインターネット・サービス・プロバイダを通じてインターネットに接続されたセンタ3を利用するために、GSMモジュールまたはUMTSモジュールを自由に使う。

20

【0034】

鍵取り寄せモジュール122はさらに別のプログラム式ソフトウェア・モジュールであり、このモジュールは、当該メディア・オブジェクト6に割り当てられてこの当該メディア・オブジェクト6のメディア・コンテンツ62の解読に必要な上述の第1鍵7を上述の鍵サーバ3から取り寄せることを可能にし、この場合、鍵取り寄せモジュール122はこのために、上述の公開第2鍵9を鍵サーバ3に伝送することができる。このために例えば、取り寄せたメディア・オブジェクト6のために、自動的にこのメディア・オブジェクト6に割り当てられた第1鍵7、およびこの暗号化された鍵7とともにまたは個別に転送されるこのメディア・オブジェクト6のための使用条件8についての記載事項を取り寄せるために、注文モジュール122は鍵モジュール123を使用することができ、この際、当該メディア・オブジェクト6のオブジェクト情報61の中に記憶された所轄の鍵サーバ3に関する記載事項が使用される。第1鍵7の当該メディア・オブジェクト6への割当ては、例えば、鍵取り寄せモジュール122が注文モジュール121によって保存されるオブジェクト識別名を鍵サーバ3に伝送し、上述のように解読される対応するトランザクションの中で鍵サーバ3によって保持される第1鍵7を通信端末1における再生の際に、当該メディア・オブジェクト6に割り当てるように、起こることができる。さらに別の変形実施形態では、第1鍵7とともに例えば鍵7の構成要素として、鍵7がセンタ3において割り当てられるメディア・オブジェクト6のオブジェクト識別名を、通信端末1に転送することができる。

30

40

【0035】

オブジェクト管理モジュール124は、メモリ12の中に記憶されたメディア・オブジェクト6を管理するために、通信端末1のユーザが例えば操作エレメント15を用いて起動させることのできる、さらに別のクログラムされたソフトウェア・モジュールである。オブジェクト管理モジュール124の制御は、ユーザによって通信端末1操作エレメント15によって、例えば通信端末1のディスプレイ16において表示されるメニュー・オプションを用いて行われる。オブジェクト管理モジュール124は、例えば記憶されたメディア・オブジェクト6の列挙および分類、ならびにその再生および消去のための列挙されたメディア・オブジェクト6の選択を可能にする。オブジェクト管理モジュール124は、例えば選択されたメディア・オブジェクト6をラジオ・モジュール18または図示され

50

ていない有線または無線のインターフェイスによって第2通信端末1に転送するために、プログラム式転送機能も含み、この際、この転送ではメディア・オブジェクト6のメディア・コンテンツ62は暗号化されたままで、第1のこのメディア・オブジェクトに割り当てられた鍵7は第2通信端末1によって、前述のように鍵サーバ3から取り寄せなければならない。上述の無線インターフェイスは例えば赤外線インターフェイス、例えば高速赤外線(HSIR)インターフェイスまたはIrDAインターフェイス(Infrared Data Association)、誘導インターフェイス、例えば無線周波数識別(RFID)インターフェイス、ホームRF(無線周波数)インターフェイス、欧州デジタル・コードレスフォン(DECT)インターフェイスまたはその他のコードレス遠隔通信システム(CTS)インターフェイス、または高周波無線インターフェイス、例えばいわゆる「ブルートゥース・インターフェイス」を通じて行われる。

10

【0036】

あるメディア・オブジェクト6が再生のために選択された場合には、選択されたメディア・オブジェクト6のメディア・コンテンツ62、ならびにこのメディア・オブジェクト6に割り当てられた暗号化されている第1鍵7または対応する解読された第1鍵7は解読モジュール14に引き渡される。ここで、解読された第1鍵7の解読モジュール14への引渡しは、鍵7が不当に読まれたりコピーされたりできないように保護されて行われることに言及すべきである。例えば、暗号化された第1鍵7のみが通信端末1に、例えばチップカード5に記憶されることが可能であり、そしてその都度上述のように解読モジュール14への引渡しの前に、第2解読機能59において解読されることが可能である。解読された第1鍵7の解読モジュール14への保護された引渡しは、例えばさらに別の暗号化によって、または解読モジュール14の外側から解読された鍵7を読むことができないように第2解読機能59を直接解読モジュール14において行うことによって起る。

20

【0037】

ここで、メディア・オブジェクト6は例えばユーザが選ぶことのできる特別のモードで、通信端末1において受け入れる際にオブジェクトとして記憶されるのではなく、このメディア・コンテンツ62は再生のためのバッファ・メモリを通じて解読モジュール14に導かれ(このメディア・オブジェクト6に割り当てられた暗号化されている第1鍵7または対応する解読された第1鍵7とともに)、この際、無線ネットワーク2の転送速度または容量が十分であれば、この特別のストリーム様式のみが実行可能である。

30

【0038】

メディア・オブジェクト6の購入と再生の決済のためには、前払いまたは後払いを許すさまざまな変形がある。例えば、上述のチップカード5は前払いされた金額51を含むことができ、この金額から例えば各メディア・オブジェクト6または各第1鍵7の購入の際に、およびメディア・オブジェクト6の各再生の際に、もしくは第1鍵7の各利用の際に、例えば前述のオブジェクト情報61または利用条件8の中に含まれる価格表に対応する額が引き去られる。この仕事および負担は、例えば決済モジュール123つまりプログラム式ソフトウェア・モジュールによって実施することができる。しかしこの決済モジュール123は、課すべき金額が例えばラジオ・モジュール8によって図示されていない決済ユニットに、書面による会計処理を通じたさらなる決済のために例えば電話請求書の一部として、または銀行口座の借方記入を通じてさらに回されるように、実施することもできる。

40

【0039】

メディア・オブジェクト6の著作権に関するライセンス料金の決済については、通信端末1における各メディア・オブジェクトの再生が、例えばライセンス・モジュール52における該当するプログラム式ソフトウェア機能によって計算され、このソフトウェア機能は例えばチップカード5に記憶され、この中に確かめた再生回数をユーザが上書きすることはできない。この計算は各メディア・オブジェクト6について、例えば第1鍵7を利用する度に固有に行われ、この利用は例えば解読モジュール14からライセンス・モジュ

50

ール52に伝えられる。伝えられた再生回数は、例えば定期的に、例えば毎日、または所定の支払い期に達する度に、例えばラジオ・モジュール18によって、さらなる処理のために、センタ3または個別のコンピュータにおいて実行されるライセンス・サーバ4に伝送される。

【0040】

決済すべき金額はまた、ユーザが実際に行った再生時間についてのみ課されるように、有効再生持続時間に関連付けることができる。この有効再生持続時間を間違いなく決定するために、通信端末1のユーザが操作できない時間参照、およびユーザが上書きできない保護されたメモリ領域が必要である。

【0041】

当業者には、データ、特にメディア・オブジェクト6および鍵の記憶、およびプログラム式ソフトウェア機能とモジュールの記憶を通信端末1において組織化すること、すなわちさまざまなメモリ12に分割すること、プログラム式ソフトウェア機能およびソフトウェア・モジュールをその実施のために、さまざまな処理手段11すなわちさまざまな多くの可能なプロセッサに配分することに、さまざまな可能性があることが理解されよう。

【0042】

鍵および/またはメディア・オブジェクト、ならびにこのメディア・オブジェクトの再生についての決済の他に、本発明による通信端末1を販売するかまたは賃貸すること、または従来の通信端末用の、例えば移動無線電話またはラップトップコンピュータまたは掌上コンピュータ用の拡張モジュールを販売することも関心事となる可能性があり、この拡張モジュールは例えばチップカードの形でこのような従来の通信端末を、本発明による通信端末1のように設置できるように拡張する。また、プログラム式ソフトウェア・モジュールが記憶されたデータ・キャリアを放逐し、ソフトウェア・モジュールが前述のセンタ3、鍵サーバ3、およびライセンス・サーバ4のように設置できるように、このソフトウェアが従来の通信サーバを制御することにも関心を寄せることができる。

【符号の説明】

【0043】

- 1 通信端末
- 2 無線ネットワーク（移動無線ネットワーク）
- 3 センタ
- 3 鍵サーバ
- 4 ライセンス・サーバ
- 5 チップカード（SIMカード）
- 6 メディア・オブジェクト
- 7 第1鍵
- 7 暗号化された第1鍵
- 7 記憶されて解読された第1鍵
- 8 使用条件（使用権、価格表）
- 9 公開第2鍵
- 9 専用第3鍵
- 11 処理手段（プロセッサ）
- 12 メモリ
- 13 メディア再生モジュール
- 14 解読モジュール
- 15 操作エレメント
- 16 ディスプレイ
- 17 音響変換機
- 18 ラジオ・モジュール
- 51 前払いされた金額
- 52 ライセンス・モジュール

10

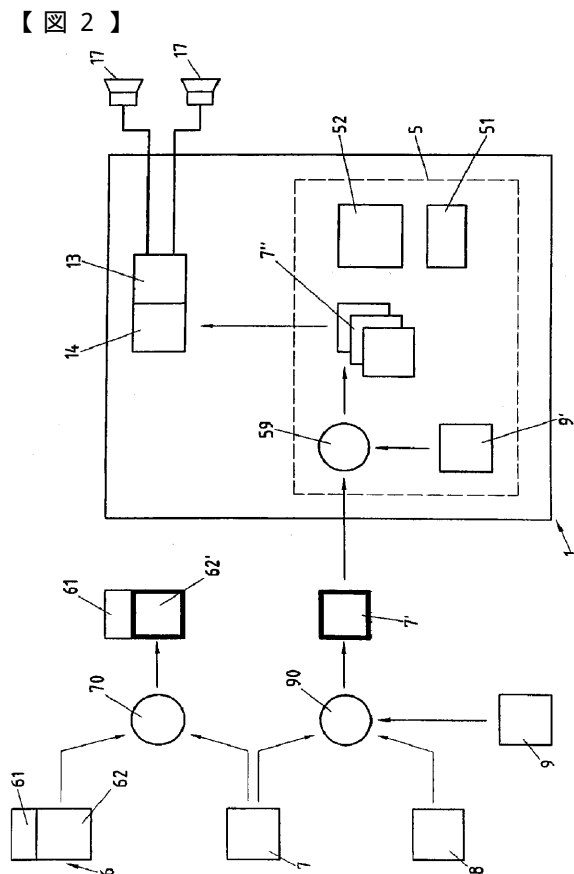
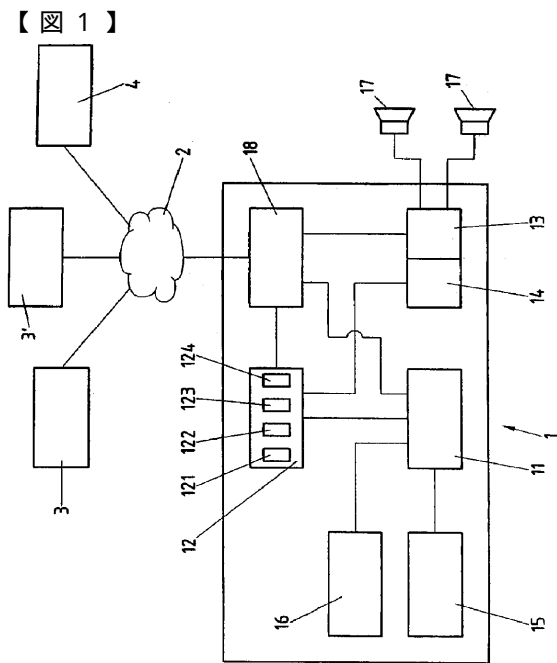
20

30

40

50

- 5 9 第 2 解読機能
- 6 1 オブジェクト情報
- 6 2 メディア・コンテンツ
- 6 2 暗号化されたメディア・コンテンツ
- 7 0 第 1 暗号化機能
- 9 0 第 2 暗号化機能
- 1 2 1 注文モジュール
- 1 2 2 鍵取り寄せモジュール
- 1 2 3 決済モジュール
- 1 2 4 オブジェクト管理モジュール



フロントページの続き

(72)発明者 カバノ, クラウディオ

スイス国 . シーエッチ - 3 0 0 6 ベルン, スペルテリニシュトラッセ 1 2

Fターム(参考) 5J104 AA16 EA19 NA35 NA37 PA01