(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2006-525592
(P2006-525592A)
(43)公表日　平成18年11月9日(2006.11.9)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/00	(2006.01)	G06F	15/00	330Z	5B285
G09C 1/00	(2006.01)	G09C	1/00	640E	5J104

審査請求 未請求　予備審査請求 未請求　（全 18 頁）

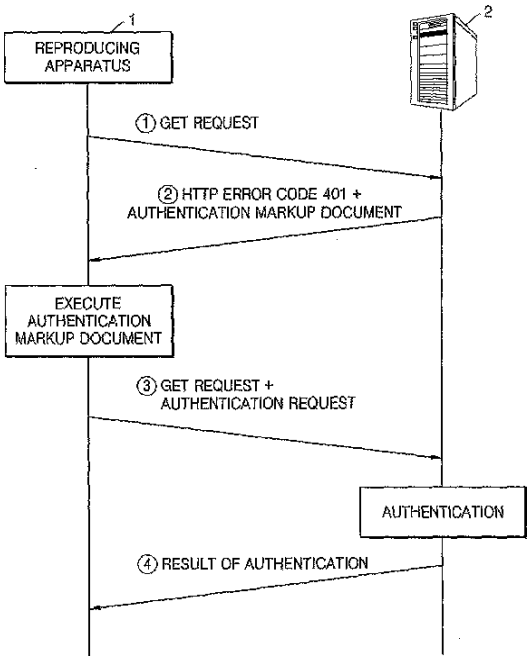
(21)出願番号	特願2006-507830 (P2006-507830)
(86)(22)出願日	平成16年4月30日 (2004.4.30)
(85)翻訳文提出日	平成17年10月28日 (2005.10.28)
(86)国際出願番号	PCT/KR2004/001008
(87)国際公開番号	WO2004/097661
(87)国際公開日	平成16年11月11日 (2004.11.11)
(31)優先権主張番号	10-2003-0028039
(32)優先日	平成15年5月1日 (2003.5.1)
(33)優先権主張国	韓国 (KR)
(31)優先権主張番号	10-2003-0066023
(32)優先日	平成15年9月23日 (2003.9.23)
(33)優先権主張国	韓国 (KR)

(71)出願人　503447036
サムスン　エレクトロニクス　カンパニー　リミテッド
大韓民国キョンギ－ド，スウォン－シ，ヨントン－ク，マエタン－ドン　４１６
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重
(72)発明者　チョン，ヒョン－グォン
大韓民国　１３５－１２０　ソウル　カンナム－グ　シンサ－ドン　５６９（３０２）

最終頁に続く

(54)【発明の名称】認証方法及びその装置

(57)【要約】
認証方法、そのサーバー及びその再生装置を提供する。（ａ）再生装置から認証の必要なコンテンツの要請に応答して、認証を実行するためのプログラムコードを伝送するステップと、（ｂ）プログラムコードが再生装置で実行されて送られた、認証のための識別情報を受信して認証を行うステップと、（ｃ）認証の結果、成功であれば、要請されたコンテンツを再生装置に伝送し、失敗であれば、失敗を知らせるメッセージを再生装置に伝送するステップとを含む。これにより、新たなフォーマットのディスクが製作され、新たなフォーマットのコンテンツが開発されるごとに、コンテンツ提供者が要求する新たな方式のディスク認証のための方法を支援する必要がなく、単にディスクのタイプによってそのディスクに記録されたデータを読み取る機能のみを追加することにより、再生装置は、多様な認証方法を支援せずとも、多様な認証方法を要求する多様なサーバーに接続及び認証して所定コンテンツをダウンロードできる。



【特許請求の範囲】
【請求項１】
（ａ）再生装置からの認証が必要なコンテンツの要請に応答して、認証を実行するためのプログラムコードを伝送するステップと、
（ｂ）前記プログラムコードが前記再生装置で実行されて送られた、認証のための識別情報を受信して認証を行うステップと、
（ｃ）認証の結果、成功であれば、要請されたコンテンツを前記再生装置に伝送し、失敗であれば、失敗を知らせるメッセージを前記再生装置に伝送するステップと、を含むことを特徴とする認証方法。
【請求項２】
前記（ａ）ステップは、
前記プログラムコードとして認証マークアップ文書を伝送するステップを含むことを特徴とする請求項１に記載の認証方法。
【請求項３】
前記（ａ）ステップは、
ＨＴＴＰ　４０１エラーコードを使用して前記プログラムコードを伝送するステップを含むことを特徴とする請求項１に記載の認証方法。
【請求項４】
（ａ）サーバーから受信したプログラムコードを実行することにより、認証のための識別情報を前記サーバーに伝送するステップと、
（ｃ）認証成功であれば、要請されたコンテンツを前記サーバーから受信し、認証失敗であれば、失敗を知らせるメッセージを前記サーバーから受信するステップと、を含む認証方法。
【請求項５】
前記（ａ）ステップは、
前記プログラムコードを実行して、ディスクの種類及び前記ディスクに記録されたコンテンツの形態を備える所定情報を、前記ディスクから抽出して前記サーバーに伝送するステップを含むことを特徴とする請求項４に記載の認証方法。
【請求項６】
コントローラの制御によりディスクからデータを読み取ってバッファに提供するリーダと、
前記データをバッファリングするバッファと、
インターネットを介してサーバーに接続し、前記サーバーから受信したプログラムコードを実行し、実行結果により得られた認証のための識別情報を前記サーバーに伝送し、認証成功であれば、要請されたコンテンツを前記サーバーから受信して再生し、認証失敗であれば、失敗を知らせるメッセージを前記サーバーから受信してディスプレーヤーにディスプレイするプレゼンテーションエンジンが内蔵されたコントローラと、を備えることを特徴とする再生装置。
【請求項７】
前記プレゼンテーションエンジンは、前記プログラムコードを実行して、ディスクの種類及び前記ディスクに記録されたコンテンツの形態を含む所定情報を、前記ディスクから抽出して前記サーバーに伝送することを特徴とする請求項６に記載の再生装置。
【請求項８】
前記プレゼンテーションエンジンは、前記プログラムコードとして認証マークアップ文書を実行するためのＡＰＩを支援することを特徴とする請求項６に記載の再生装置。
【請求項９】
（ａ）再生装置からコンテンツの要請及びコンテンツＩＤを受信するステップと、
（ｂ）所定の索引番号を生成するステップと、
（ｃ）前記索引番号に対応する認証問題情報を、前記コンテンツＩＤに対応する暗号キーを利用して暗号化するステップと、

（ｄ）前記暗号化された認証問題情報及び前記索引番号を備える所定の認証データを前記再生装置に伝送するステップと、
（ｅ）前記再生装置から所定の復号化の実行結果である認証解答情報及び索引番号を受信して認証を行うステップと、を含むことを特徴とするコンテンツサーバーでの認証方法。
【請求項１０】
前記（ｃ）ステップは、
（ｃ１）前記コンテンツＩＤに対応するタイトルキー及び前記索引番号に一方向関数を適用して暗号キーを生成するステップと、
（ｃ２）前記索引番号に対応する認証問題情報を、前記暗号キーを利用して暗号化するステップと、を含むことを特徴とする請求項９に記載のコンテンツサーバーでの認証方法。
【請求項１１】
前記（ｄ）ステップは、
前記再生装置に前記暗号化された認証問題情報、前記索引番号及び前記再生装置で行う復号化方法を指示する情報を伝送するステップであることを特徴とする請求項９に記載のコンテンツサーバーでの認証方法。
【請求項１２】
前記（ｄ）ステップは、
前記再生装置に前記暗号化された認証問題情報、前記索引番号及び前記再生装置で行う復号化プログラムコードを伝送するステップであることを特徴とする請求項９に記載のコンテンツサーバーでの認証方法。
【請求項１３】
前記（ｅ）ステップは、
（ｅ１）前記再生装置から前記認証問題情報及び前記索引番号を利用した所定の復号化の実行結果である認証解答情報及び索引番号を受信するステップと、
（ｅ２）前記再生装置から受信した索引番号に対応する認証問題情報と前記認証解答情報とを比較して、二つの情報が同じであれば、前記コンテンツの要請を承認し、二つの情報が異なれば、コンテンツ要請を拒否するステップと、を含むことを特徴とする請求項９に記載のコンテンツサーバーでの認証方法。
【請求項１４】
（ａ）コンテンツサーバーにコンテンツを要請し、コンテンツＩＤを伝送するステップと、
（ｂ）前記サーバーから暗号化された認証問題情報及び索引番号を備える所定の認証データを受信するステップと、
（ｃ）前記コンテンツＩＤに対応するタイトルキー及び前記索引番号に一方向関数を適用して復号化キーを生成するステップと、
（ｄ）前記復号化キーを利用して、前記暗号化された認証問題情報を復号化して認証解答情報を生成するステップと、
（ｅ）前記サーバーに前記認証解答情報及び前記索引番号を伝送するステップと、を含むことを特徴とする再生装置での認証方法。
【請求項１５】
前記（ｂ）ステップは、前記サーバーから暗号化された認証問題情報、索引番号及び前記（ｄ）ステップで行う復号化方法を指示する情報を受信するステップであることを特徴とする請求項１４に記載の再生装置での認証方法。
【請求項１６】
前記（ｂ）ステップは、前記サーバーから暗号化された認証問題情報、索引番号及び所定の復号化プログラムコードを受信するステップであり、
前記（ｄ）ステップは、前記復号化プログラムコードを実行して、前記暗号化された認証問題情報を復号化するステップであることを特徴とする請求項１４に記載の再生装置で

の認証方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、マークアップ言語を使用して製作されたインタラクティブコンテンツを再生する再生装置において、インターネットまたはディスクからインタラクティブコンテンツをダウンロードしたり、読み出す再生装置に関する。
【背景技術】
【０００２】
従来のディスクに記録されるか、インターネットのサーバーに存在するコンテンツ識別情報は、別途に決まっていなかった。したがって、従来には、再生装置が直接そのコンテンツを識別して、ディスクが正品であるか否かを認証した。すなわち、ＣＤに記録されたコンテンツの場合、トラックの演奏時間及びトラック数によりタイトルを識別し、ＤＶＤ－ＶＩＤＥＯの場合、タイトルの数、チャプターの数及びタイトルの再生時間により識別し、ＤＶＤ－ＡＵＤＩＯの場合、アルバムの数、グループの数、トラックの数及びトラックの演奏詩間により識別した。また、サーバーの認証を経た後に、所定コンテンツをサーバーから取り込むことができた。
【０００３】
しかし、従来の認証方式によれば、再生装置は、毎回コンテンツのフォーマットが変更される度に新たな識別情報を認識し、これに基づいてディスクを認証する方法を内蔵せねばならないという不便さが存在する。さらに、コンテンツを提供する会社（例、ＣＤＤＢ等）ごとに、コンテンツを識別する方式がそれぞれ異なって決まっており、再生装置がこれを何れも支援することは、事実上不可能である。
【０００４】
コンテンツがインターネットのサーバーに存在する場合にも同様である。相異なる認証方式を採用する複数のサーバーから所定コンテンツをダウンロードするためには、再生装置は、あらゆるサーバーに対してその認証方式を支援せねばならない。
【発明の開示】
【発明が解決しようとする課題】
【０００５】
本発明が達成しようとする技術的課題は、ディスク及びインターネットから所定のコンテンツをダウンロードする再生装置において、ディスクに記録されたコンテンツにより複数の相異なる認証方式を採用するインターネットサーバーから所定コンテンツをダウンロードしようとする場合、その認証方式を何れも支援せずとも、認証を行える方法、そのサーバー及びその再生装置を提供するところにある。
【０００６】
また、本発明が達成しようとする技術的課題は、ディスク及びインターネットからコンテンツをダウンロードする再生装置が、インターネット上のコンテンツサーバーからの所定のコンテンツのダウンロードを要請する場合に、認証に使用される暗号化方式をあらかじめ決めずに、コンテンツの要請時にサーバーが決定する暗号化及び復号化方式を利用して認証する方法を提供するところにある。
【課題を解決するための手段】
【０００７】
前記技術的課題は、本発明によって、（ａ）再生装置からの認証が必要なコンテンツの要請に応答して、認証を実行するためのプログラムコードを伝送するステップと、（ｂ）前記プログラムコードが前記再生装置で実行されて送られた、認証のための識別情報を受信して認証を行うステップと、（ｃ）認証の結果、成功であれば、要請されたコンテンツを前記再生装置に伝送し、失敗であれば、失敗を知らせるメッセージを前記再生装置に伝送するステップと、を含む認証方法により達成される。
【０００８】

前記（ａ）ステップは、前記プログラムコードとして認証マークアップ文書を伝送するステップを含むことが好ましく、特に、ＨＴＴＰ　４０１エラーコードを使用して前記プログラムコードを伝送するステップを含むことが好ましい。

【０００９】

また、前記技術的課題は、（ａ）サーバーから受信したプログラムコードを実行することにより、認証のための識別情報を前記サーバーに伝送するステップと、（ｃ）認証成功であれば、要請されたコンテンツを前記サーバーから受信し、認証失敗であれば、失敗を知らせるメッセージを前記サーバーから受信するステップと、を含む認証方法によっても達成される。

【００１０】

前記（ａ）ステップは、前記プログラムコードを実行して、ディスクの種類及び前記ディスクに記録されたコンテンツの形態を備える所定情報を、前記ディスクから抽出して前記サーバーに伝送するステップを含むことが好ましい。

【００１１】

一方、本発明の他の分野によれば、前記技術的課題は、コントローラの制御によりディスクからデータを読み取ってバッファに提供するリーダと、前記データをバッファリングするバッファと、インターネットを介してサーバーに接続し、前記サーバーから受信したプログラムコードを実行し、実行結果により得られた認証のための識別情報を前記サーバーに伝送し、認証成功であれば、要請されたコンテンツを前記サーバーから受信して再生し、認証失敗であれば、失敗を知らせるメッセージを前記サーバーから受信してディスプレーヤーにディスプレイするプレゼンテーションエンジンが内蔵されたコントローラと、を備える再生装置によっても達成される。

【００１２】

前記プレゼンテーションエンジンは、前記プログラムコードを実行して、ディスクの種類及び前記ディスクに記録されたコンテンツの形態を含む所定情報を、前記ディスクから抽出して前記サーバーに伝送することが好ましく、前記プログラムコードとして認証マークアップ文書を実行するためのＡＰＩ（アプリケーションプログラミングインターフェース）を支援することが特に好ましい。

【００１３】

一方、本発明の他の分野によれば、前記技術的課題は、再生装置からコンテンツの要請及びコンテンツＩＤを受信するステップと、所定の索引番号を生成するステップと、前記索引番号に対応する認証問題情報を、前記コンテンツＩＤに対応する暗号キーを利用して暗号化するステップと、前記暗号化された認証問題情報及び前記索引番号を備える所定の認証データを前記再生装置に伝送するステップと、前記再生装置から所定の復号化の実行結果である認証解答情報及び索引番号を受信して認証を行うステップと、を含むコンテンツサーバーでの認証方法により達成される。

【００１４】

また、一方、本発明の他の分野によれば、前記技術的課題は、コンテンツサーバーにコンテンツを要請し、コンテンツＩＤを伝送するステップと、前記サーバーから暗号化された認証問題情報及び索引番号を備える所定の認証データを受信するステップと、前記コンテンツＩＤに対応するタイトルキー及び前記索引番号に一方向関数を適用して復号化キーを生成するステップと、前記復号化キーを利用して、前記暗号化された認証問題情報を復号化して認証解答情報を生成するステップと、前記サーバーに前記認証解答情報及び前記索引番号を伝送するステップと、を含む再生装置での認証方法により達成される。

【発明を実施するための最良の形態】

【００１５】

以下、添付された図面を参照して、本発明の好ましい実施形態を詳細に説明する。

【００１６】

図１は、本発明を説明するための概要図である。

【００１７】

図１に示すように、再生装置１は、ＨＴＴＰ（ハイパーティストトランスファープロトコル）（ＲＦＣ２６１６）に基づいてＧＥＴ要求により、所定のコンテンツをサーバー２に要請する（１）。サーバー２は、再生装置１が要求される認証を受けていなければ、ＨＴＴＰの４０１エラーと共に、認証のための認証マークアップ文書を再生装置１に送る（２）。再生装置１は、受信された認証マークアップ文書を実行する。認証マークアップ文書は、認証過程を行うために、再生装置１に設置されて実行される一種のプログラムである。本実施形態で認証マークアップ文書は、認証のためのＪＡＶＡ（登録商標）Ｓｃｒｉｐｔコードを有している。認証マークアップ文書が実行になれば、その結果、認証のために必要な識別情報が生成され、生成された識別情報は、ＧＥＴ要求によりサーバー２に伝えられる（３）。サーバー２は、受信された識別情報を確認して認証を行い、認証結果を再び再生装置１に送る（４）。

【００１８】

過程（１）では、再生装置１からサーバー２に、次のようなＨＴＴＰヘッダーが伝送される。

【００１９】

ＧＥＴ／ｐｒｏｐｒｉａｔｅｍａｔｅｒｉａｌ.ｃｇｉ ＨＴＴＰ／１.０
Ｄａｔｅ：Ｆｒｉ，２０ Ｓｅｐ １９９６ ０８：２０：５８ ＧＭＴ
Ｃｏｎｎｅｃｔｉｏｎ：Ｋｅｅｐ－Ａｌｉｖｅ
Ｕｓｅｒ－Ａｇｅｎｔ：ＥＮＡＶ １.０（ＳＤＰ－１００）

過程（２）では、サーバー２から再生装置１に、次のようなＨＴＴＰヘッダー及び認証マークアップ文書が伝送される。この時、Ｃｏｏｋｉｅを使用してサーバー認証要求番号を含みうる。これは、再生装置１が認証されたように、エミュレートすることを防止するためである。

【００２０】

ＨＴＴＰ／１.０ ４０１ Ｕｎａｕｔｈｏｒｉｚｅｄ
Ｄａｔｅ：Ｆｒｉ，２０ Ｓｅｐ １９９６ ０８：２０：５８ ＧＭＴ
Ｓｅｒｖｅｒ：ＥＮＡＶ １.０（ＮＣＳＡ／１.５.２）
Ｌａｓｔ－ｍｏｄｉｆｉｅｄ：Ｆｒｉ，２０ Ｓｅｐ １９９６ ０８：１７：５８ ＧＭＴ
Ｃｏｎｔｅｎｔ－ｔｙｐｅ：ｔｅｘｔ／ｘｍｌ＋ｈｔｍｌ
Ｃｏｎｔｅｎｔ－ｌｅｎｇｔｈ：２００
Ｓｅｔ－Ｃｏｏｋｉｅ：ｓｅｒｖｅｒ＿ｒｅｑ＝“１２３４５０９８７６１２３４５０９８７６”；Ｖｅｒｓｉｏｎ＝“１”；Ｐａｔｈ＝“／”

認証マークアップ文書は、次の通りである。

【００２１】

【表１】

```
<html>

<head>

<title>Authentication is required</title>

</head>

<body>

<object data=" dvd://video_ts/video_ts.ifo"  id=" player"  />

<script src=" cookieutil.js"  language=" Javascript"  />

<script language=" Javascript"  />

seed = 100123;

setCookie( “hashKey” ,player.getHashKey(seed));

setCookie( “authoringtype” ,player.authotingType);

setCookie( “disctype” ,player.discType);

location.href = “propriatematerial.cgi” ;

</script>

</body>

</html>
```

過程（３）では、再生装置１からサーバー２に、次のようなＨＴＴＰヘッダーが伝送される。

【００２２】

ＧＥＴ／ｐｒｏｐｒｉａｔｅｍａｔｅｒｉａｌ.ｃｇｉＨＴＴＰ／１.０
Ｄａｔｅ：Ｆｒｉ，２０　Ｓｅｐ　１９９６　０８：２０：５８　ＧＭＴ
Ｃｏｎｎｅｃｔｉｏｎ：Ｋｅｅｐ－Ａｌｉｖｅ
Ｕｓｅｒ－Ａｇｅｎｔ：：ＥＮＡＶ　１.０（ＳＤＰ－１００）
Ｃｏｏｋｉｅ：＄Ｖｅｒｓｉｏｎ＝“１”；
ｓｅｒｖｅｒ＿ｒｅｑ＝“１２３４５０９８７６１２３４５０９８７６”；＄Ｐａｔｈ＝“／”と、
ｈａｓｈｋｅｙ＝“１２３ＡＢ１２３４”；＄Ｐａｔｈ＝“／”
ｄｉｓｃｔｙｐｅ＝“１”；＄Ｐａｔｈ＝“／”

過程（４）では、サーバー２から再生装置１に、次のようなＨＴＴＰヘッダーと、認証成功または認証失敗を知らせるマークアップ文書とが共に伝送される。この時、サーバー２は、ＨＴＴＰヘッダーにＣｏｏｋｉｅを使用して、次に接近する時に認証を証明する接近識別子を挿入して再生装置１に伝達できる。

【００２３】

ＨＴＴＰ／１.０　２００　Ｆｏｒｂｉｄｄｅｎ
Ｄａｔｅ：Ｆｒｉ，２０　Ｓｅｐ　１９９６　０８：２０：５８　ＧＭＴ
Ｓｅｒｖｅｒ：ＥＮＡＶ　１.０（ＮＣＳＡ／１.５.２）
Ｌａｓｔ－ｍｏｄｉｆｉｅｄ：Ｆｒｉ，２０　Ｓｅｐ　１９９６　０８：１７：５８　ＧＭＴ
Ｃｏｎｔｅｎｔ－ｔｙｐｅ：ｔｅｘｔ／ｘｍｌ＋ｈｔｍｌ
Ｃｏｎｔｅｎｔ－ｌｅｎｇｔｈ：８３
Ｓｅｔ－Ｃｏｏｋｉｅ：ｓｅｒｖｅｒ＿ｒｅｑ＝“１２３４５０９８７６１２３４５０９８７６”；Ｖｅｒｓｉｏｎ＝“１”；Ｐａｔｈ＝“／”

失敗を知らせるマークアップ文書は、次の通りである。

【００２４】

【表２】

```
<html>

<head>

<title>Access denied</title>

</head>

<body>

The access is denied because of using illegal disc.

</body>

</html>
```

成功を知らせるマークアップ文書は、次の通りである。

【００２５】

【表３】

```
<html>

<head>

<title>Access accepted</title>

</head>

<body>

The access is accepted because of using legal disc.

</body>

</html>
```

このように、本発明によれば、画面上への出力のためではなく、認証のみのための認証マークアップ文書が、サーバー２から再生装置１に伝送されることにその特徴がある。ＨＴＴＰを利用する場合、４０１エラーコードを利用することが好ましい。

【００２６】

図２は、本発明に係る再生装置１のブロック図である。図２に示すように、再生装置１は、リーダ１１、バッファ１２、コントローラ１３及びディスプレーヤー１４を備える。プレゼンテーションエンジン１５は、コントローラ１３に内蔵されている。プレゼンテーションエンジン１５は、サーバー２に接続して本発明に係る認証を行うために、サーバー２からダウンロードした認証マークアップ文書を実行する。すなわち、プレゼンテーションエンジン１５は、マークアップ文書及びそれに含まれたスクリプトプログラムを解析する解析エンジンであり、インターネットに接続して、サーバー２から所定のコンテンツをダウンロードするブラウザーである。

【００２７】

リーダ１１は、コントローラ１３の制御により、ディスクに記録されたコンテンツを読み出してバッファ１２に提供する。バッファ１２は、リーダ１１から提供されるか、またはプレゼンテーションエンジン１５によりサーバー２から伝送されたコンテンツをバッファリングする。ディスプレーヤー１４は、認証成功であれば、サーバーから伝送されたコンテンツをディスプレイし、認証失敗であれば、認証失敗を知らせるメッセージをディスプレイする。

【００２８】

一方、プレゼンテーションエンジン１５は、認証マークアップ文書を実行するために、

次のようなＡＰＩを支援する。ＡＰＩは、ディスクから認証のための識別情報を抽出するために使用される。

【００２９】

１．［ｏｂｊ］.ｄｉｓｃＴｙｐｅ

１）内容：

ディスク種類を知らせる。

【００３０】

２）リターン値：

０＝Ｃｏｍｐａｃｔ　Ｄｉｓｃ

１＝ＤＶＤ－ＲＯＭ

２＝ＤＶＤ－Ｒ

３＝ＤＶＤ－ＲＡＭ

４＝ＤＶＤ－ＲＷ

５＝ＤＶＤ＋ＲＷ

２．［ｏｂｊ］.ａｕｔｈｏｒｉｎｇＴｙｐｅ

１）内容：

オーサリングした形態を知らせる。

【００３１】

２）リターン値：

０＝ＣＤＤＡ

１＝ＤＶＤ－Ｖｉｄｅｏ

２＝ＤＶＤ－Ａｕｄｉｏ

３．［ｏｂｊ］.ｇｅｔＨａｓｈＫｅｙ（ｓｅｅｄ）

１）内容：

ｓｅｅｄとディスクの種類とによってディスク上で情報を読み取る。

【００３２】

２）媒介変数：

ｓｅｅｄ：ＣＤＤＡ－ＴＴＨＨＭＭＳＳＦＦ形式のトラック別の時間組合わせ及びフレーム内での部分値

ＤＶＤ－Ｖｉｄｅｏ－３２ｂｉｔ　ｌｏｇｉｃａｌ　ｓｅｃｔｏｒ番号及びセクター内で読み取ろうとする部分値

ＤＶＤ－Ａｕｄｉｏ－３２ｂｉｔ　ｌｏｇｉｃａｌ　ｓｅｃｔｏｒ番号及びセクター内で読み取ろうとする部分値

３）リターン値：

指示された位置から抽出された値

ＣＤＤＡ－フレーム内での部分値

ＤＶＤ－Ｖｉｄｅｏ－ｌｏｇｉｃａｌ　ｓｅｃｔｏｒ番号から抽出されたセクターのデータの部分値

ＤＶＤ－Ａｕｄｉｏ－ｌｏｇｉｃａｌ　ｓｅｃｔｏｒ番号から抽出されたセクターのデータの部分値

図３は、本発明の好ましい実施形態に係る認証をディスプレーヤー１４の画面と関連して説明するための参考図である。図３に示すように、ユーザーが再生装置１を使用してディスクに記録された所定コンテンツを鑑賞するか（１）、またはインターネットからダウンロードした所定のコンテンツを鑑賞する途中に（２）、ディスプレーヤー１４の画面に表示されたボタンを押して（３）、認証の必要な他のコンテンツを鑑賞しようとすれば、本発明に係る認証のための認証マークアップ文書がインターネットから再生装置１に伝えられ（４）、伝えられた認証マークアップ文書は再生装置１で実行されて、認証のための識別情報が再びインターネットに伝えられて認証が行われる。認証が成功すれば、インターネットから所望のコンテンツが提供されて、画面にディスプレイされるが（５）、認証が失敗すれば、認証失敗を知らせるメッセージが画面にディスプレイされる（６）。

【００３３】
前記のような構成に基づいて、本発明の好ましい実施形態に係る認証方法を説明すれば、次の通りである。
【００３４】
図４は、本発明の好ましい実施形態に係る認証方法を説明するためのフローチャートである。図４に示すように、開始文書として指定されたマークアップ文書を読み取った後（ステップ４０１）、実行して画面に表示し、表示されたマークアップ文書によりユーザーと相互動作する（ステップ４０２）。相互動作中、ユーザーが他のコンテンツの表示を要求すれば（ステップ４０３）、そのコンテンツがディスクに記録されていれば、ディスクから読み取る（ステップ４０４）。要求されたコンテンツがインターネットに保存されていれば、そのコンテンツをサーバー２に要求する（ステップ４０５）。接近するためには、必ず認証が必要な場合、サーバー２は、認証マークアップ文書を再生装置１に送り（ステップ４０６）、再生装置１は、認証マークアップ文書を画面に表示せずに実行することにより、サーバー２に認証を要求する（ステップ４０７）。認証が失敗すれば（ステップ４０８）、再生装置１は、認証失敗を知らせるメッセージを画面に表示する（ステップ４０９）。認証が成功すれば（ステップ４０８）、サーバー２は、コンテンツを再生装置１に送り、再生装置１は、ダウンロードされたコンテンツを再生する（ステップ４１０）。
【００３５】
認証なしにも接近可能なコンテンツである場合、サーバー２は、認証マークアップ文書を送らずに、要求されたコンテンツを直ちに送る。これにより、再生装置１は、サーバー２が送ったコンテンツを再生する（ステップ４１０）。
【００３６】
以下では、コンテンツの再生装置１からコンテンツサーバー２へのコンテンツ要請がある場合（前記の図４の４０５ステップ）の認証方法に関する。
【００３７】
図５は、本発明の他の実施形態に係る認証方法の概要を示すフローチャートである。図５に示すように、本発明による認証方法は、コンテンツの再生装置１とコンテンツサーバー２とのデータ交換により行われる。再生装置１は、インターネットまたはディスクからインタラクティブコンテンツをダウンロードして読み出す装置である。このために再生装置は、ディスク及びインターネット上のコンテンツを読み取るリーダ、リーダが読み取ったコンテンツをバッファリングするバッファ、リーダがディスクとインターネットのうち、どこからコンテンツをダウンロードするかを指示し、認証作業を行うコントローラ、そして、ダウンロードしたコンテンツをディスプレイできるように処理するプレゼンテーションエンジンなどを備える。
【００３８】
再生装置１は、ディスク上に保存されておらず、インターネット上で読み取るべきコンテンツがある時、コンテンツサーバー２にコンテンツ要請信号を送る（ステップ５０１）。この時、所望のコンテンツＩＤを共に伝送する（ステップ５０２）。
【００３９】
サーバー２は、再生装置からコンテンツの要請及びコンテンツＩＤを受信した後、認証データを生成して（ステップ５０３）、再生装置に伝送する（ステップ５０４）。認証データには、暗号化された認証問題情報、索引番号、認証のための復号化方法などが含まれるが、再生装置は、これを利用して認証のための復号化を行った後（ステップ５０５）、その結果である認証解答情報及び索引番号をサーバーに伝送する（ステップ５０６）。サーバーは、再生装置が行う復号化方法を指示するデータ、または復号化を行うプログラムコード自体を伝送できる。
【００４０】
プログラムコードは、再生装置で直ちに実行できる形態で形成されるか、またはマークアップ言語文書から形成されうる。マークアップ言語文書とは、ＨＴＭＬ（ハイパーテキストマークアップランゲージ）、ＸＭＬ（エクステンシブルマークアップランゲージ）な

どのマークアップ言語で作成された文書はもとより、スクリプト言語、Ｊａｖａ（登録商標）言語などで作成されたソースコードがリンクまたは挿入された文書を総称し、さらに、マークアップ言語文書にリンクされたファイルを網羅する意味として使用される。

【００４１】

再生装置で行われうるプログラムの形態が何であるか確認するために、サーバーと再生装置とのデータ交換が追加的に行われうる。再生装置は、コントローラでプログラムが実行されるため、コントローラが解析できる形態が何であるかをサーバーに知らせる。

【００４２】

認証解答情報は、サーバーが送った認証データを実行して生成された結果であるが、サーバーは、再生装置からこれを受信して認証を行う（ステップ５０７）。認証解答情報は、暗号化された認証問題情報を復号化した結果を含むが、サーバーは、自身が有している認証問題情報のうち、再生装置が送った索引番号に対応するものを、再生装置が送った認証解答情報と比較して、同じものであるか否かを確認する。以後、サーバーは、認証結果を再生装置に伝送して、コンテンツ要請に対する認証を完了する（ステップ５０８）。

【００４３】

認証が成功した場合、サーバーは、認証成功を知らせるメッセージを伝送した後、再生装置が要請したコンテンツを伝送し、再生装置は、これを処理して再生する。

【００４４】

図６は、本発明の他の実施形態に係る認証方法の詳細フローチャートである。図６に示すように、サーバーで認証データを生成し、再生装置でこれを利用して認証解答情報を生成する過程を詳細に図示している。

【００４５】

サーバーは、再生装置からコンテンツＩＤ（ＣＩＤ）を受信した後（ステップ６１０）、索引番号（ＩＤ）を生成する（ステップ６１０）。索引番号（ＩＤ）は、認証問題情報（Ｍ）に対応する符号であるが、再生装置から認証解答情報（ｍ）を受信した後に、これと比較するために、認証データ生成時に使用した認証問題情報を探す時に使用される。索引番号は、サーバーが有している認証問題情報の番号のうち、何れか一つを選択するが、各コンテンツの要請に対応して順次に指定されてもよく、ランダムに指定されてもよい。

【００４６】

サーバーは、再生装置が要請したコンテンツＩＤに対応するタイトルキー（Ｋｓ）及び索引番号（ＩＤ）に一方向関数を適用して暗号キー（Ｋａ）を生成する（ステップ６１２）。タイトルキー（Ｋｓ）は、コンテンツＩＤ（ＣＩＤ）のそれぞれに唯一に対応するが（ステップ６１１）、これは、サーバー及び再生装置が何れも有していなければならない情報である。一方向関数とは、順方向の関数は存在するが、逆方向の関数が存在していないということを意味する。索引番号（ＩＤ）及びタイトルキー（Ｋｓ）を一方向関数に代入して暗号キー（Ｋａ）を生成できるが、暗号キー（ｋａ）及び索引番号（ＩＤ）からタイトルキー（Ｋｓ）を探し出すことはできない。

【００４７】

図６に示す実施形態による認証方法を、ユーザー名及び暗号を利用する通常の認証方法と比較すると、コンテンツＩＤ（ＣＩＤ）は、ユーザー名に対応し、タイトルキー（Ｋｓ）は、暗号に対応している。本実施形態の認証方法の特徴は、通常の認証方法において、暗号に該当するタイトルキー（Ｋｓ）がインターネット上に伝送されないということである。インターネット上に伝えられる情報は、索引番号、認証問題情報及び認証解答情報であるが、それらは、タイトルキーを利用して生成されるものであって、各認証ごとに異なる内容を有する。もし、不法なユーザーが認証問題情報及びそれに対応する認証解答情報を知り得る場合にも、コンテンツＩＤ（ＣＩＤ）に対応するタイトルキー（Ｋｓ）が分からないため、コンテンツ要請を承認され得ない。

【００４８】

認証問題情報（Ｍ）は、要請されたコンテンツ情報の一部または任意のデータを使用することが可能である。また、非常に長い文字列を使用して、不法なユーザーの認証の試み

を阻止することも可能である。

【００４９】

サーバー２は、暗号キー（ｋａ）を利用して認証問題情報（Ｍ）を暗号化する（ステップ６１３）。サーバーは、暗号化された認証問題情報（｛Ｍ｝ｋａ）、索引番号（ＩＤ）、及び復号化関数に対する情報（ＩＦＮ）を再生装置に伝送する（ステップ６２０）。

【００５０】

復号化関数に対する情報は、再生装置が実行可能な関数のうち、何れか一つを指定するものであるか、または再生装置が実行可能な復号化プログラムコード自体であることも可能である。このように、コンテンツ要請の認証に使用する暗号化方式及び復号化方式を再生装置の製作時にあらかじめ決定せずに、認証時にコンテンツサーバーが決定できるため、再生装置は、多様な認証を支援できる。

【００５１】

再生装置１は、サーバー２から暗号化された認証問題情報（｛Ｍ｝ｋａ）、索引番号（ＩＤ）、及び復号化関数に対する情報（ＩＦＮ）を受信した後（ステップ６２０）、コンテンツＩＤ（ＣＩＤ）に対応するタイトルキー（Ｋｃ）及び索引番号（ＩＤ）に一方向関数を適用して復号化キー（Ｋｂ）を生成する（ステップ６３０）。再生装置で使用される一方向関数も、サーバーでの一方向関数と同様に、復号化キー及び索引番号を利用してタイトルキーが分からない関数を使用する。

【００５２】

生成された復号化キー（Ｋｂ）を利用して、サーバーから伝えられた暗号化された認証問題情報（（｛Ｍ｝ｋａ）を復号化して認証解答情報（ｍ）を生成する（ステップ６３１）。適法なユーザーによる再生装置の認証である場合、認証解答情報（ｍ）は、サーバーで使用された認証問題情報（Ｍ）と同じものになる。

【００５３】

再生装置１は、サーバー２に認証解答情報（ｍ）及び索引番号（ＩＤ）を伝送し（ステップ６４０）、サーバーは、受信した索引番号に対応する認証問題情報と、再生装置が送った認証解答情報とを比較する（ステップ６４１）。比較結果、二つの情報が同じであれば、認証成功メッセージを送ってコンテンツ要請を承認し（ステップ６４３）、該当コンテンツを再生装置に伝送する。一致しなければ、認証に失敗したというメッセージを再生装置に送って、コンテンツ要請を拒否する（ステップ６４２）。

【００５４】

本発明による認証方法は、再生装置１が、自身がコンテンツをダウンロードされようとするサーバーが適法なサーバーであるか否かを認証する時や、自身がダウンロードされたコンテンツが適法なものであるかを確認する場合に、若干の変形により適用されうる。再生装置１は、所定の認証問題情報と、これに対応する索引番号とを生成し、これを図２でサーバー２が行う各ステップを経て、サーバー２に暗号化された認証問題情報、索引番号及び復号化方法を指示する情報を伝送する。サーバー２は、図６で再生装置１が行う各ステップを経て、復号化の結果である認証解答情報及び索引番号を再生装置に伝送する。再生装置１は、サーバーから受信した認証解答情報及び索引番号に対応する認証問題情報を比較して、サーバーが適法なサーバーであるか否かを確認できる。

【００５５】

一方、前記の認証方法は、コンピュータプログラムで作成可能である。前記プログラムを構成するコード及びコードセグメントは、当業界のコンピュータプログラマーによって容易に推論されうる。また、前記プログラムは、コンピュータで読み取り可能な情報記録媒体に保存され、コンピュータによって読み取り及び実行されることにより認証方法を具現する。前記情報記録媒体は、磁気記録媒体、光記録媒体、及びキャリアウェーブ媒体を含む。

【産業上の利用可能性】

【００５６】

前記のように、本発明によれば、新たなフォーマットのディスクが製作され、新たなフ

ォーマットのコンテンツが開発される度に、コンテンツの提供者が要求する新たな方式のディスク認証のための方法を支援する必要がなく、単にディスクのタイプによってそのディスクに記録されたデータを読み取る機能のみを追加することにより、再生装置は、多様な認証方法を支援せずとも、多様な認証方法を要求する多様なサーバーに接続及び認証して、所定コンテンツをダウンロードできる。

【００５７】

これにより、ユーザーが、自身が使用するディスクが不法なものであるか、あるいは合法的なものであるかを判断できる。また、コンテンツ提供者は、認証されたユーザーのみにコンテンツを提供できるため、コンテンツの価値を高めうる。

【００５８】

さらに、本発明による認証方法によれば、コンテンツ要請の認証に使用する暗号化方式及び復号化方式を、再生装置の製作時にあらかじめ決定せずに、認証時にコンテンツサーバーが決定できるため、再生装置は、多様な認証を支援できる。また認証において、暗号となるタイトルキーをインターネット上に伝送せずに、タイトルキーに一方向関数を適用して暗号化を行った結果のみを伝送するため、不法なユーザーの認証を防止できる。

【図面の簡単な説明】

【００５９】

【図１】本発明を説明するための概要図である。

【図２】本発明に係る再生装置のブロック図である。

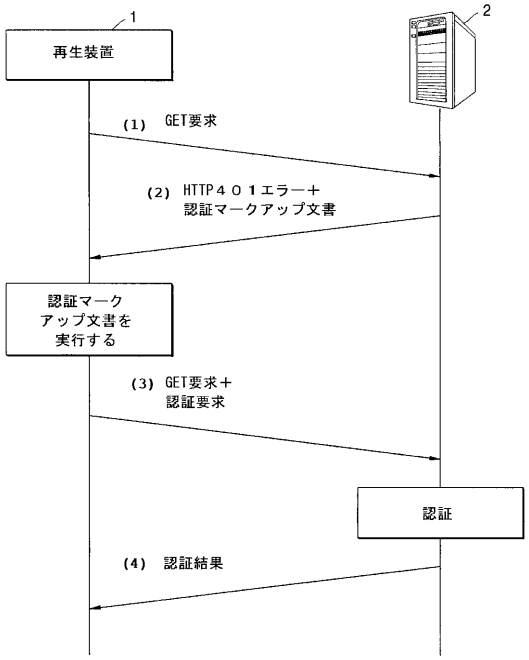
【図３】本発明の好ましい実施形態に係る認証をディスプレーヤーの画面に関連して説明するための参考図である。

【図４】本発明の好ましい実施形態に係る認証方法を説明するためのフローチャートである。

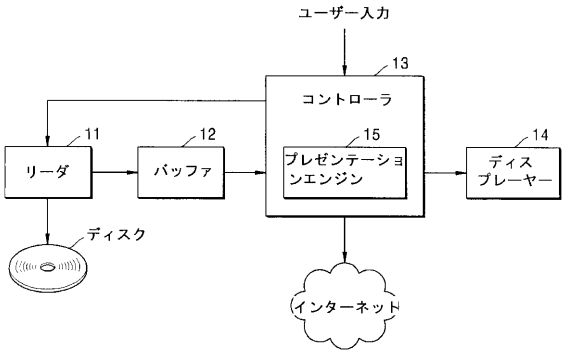
【図５】本発明の他の実施形態に係る認証方法の概要を示すフローチャートである。

【図６】本発明の他の実施形態に係る認証方法の詳細フローチャートである。

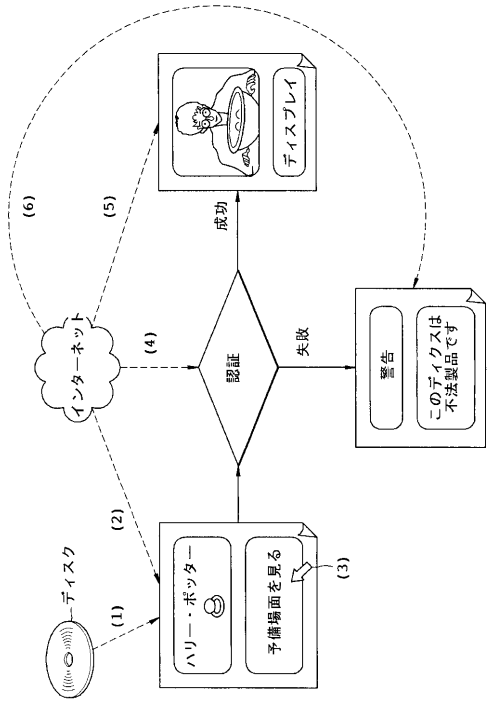
【図１】



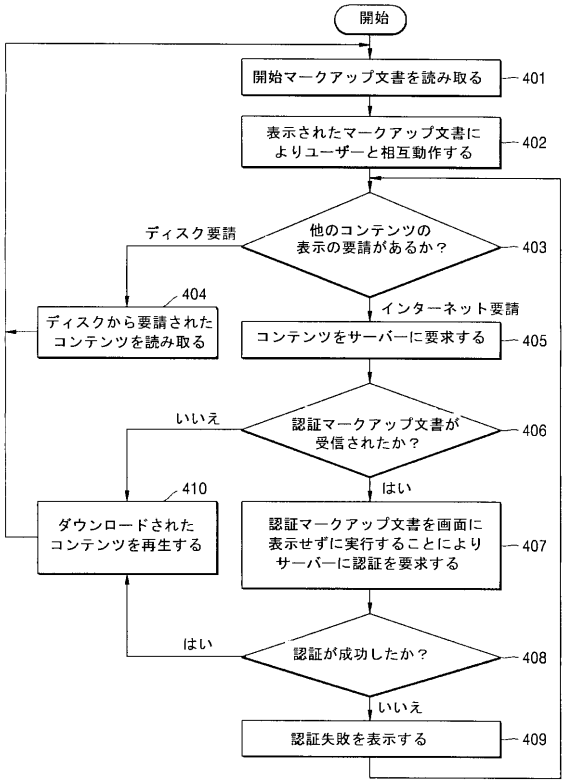
【図２】



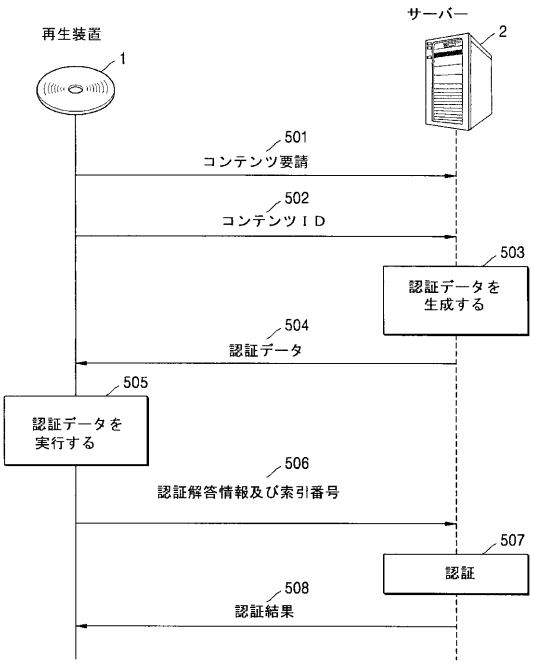
【図３】


ディスプレイ
成功
(6)
(5)
インターネット
(4)
認証
失敗
警告
このディスクは不法製品です
(2)
ディスク
(1)
ハリー・ポッター
予備場面を見る
(3)

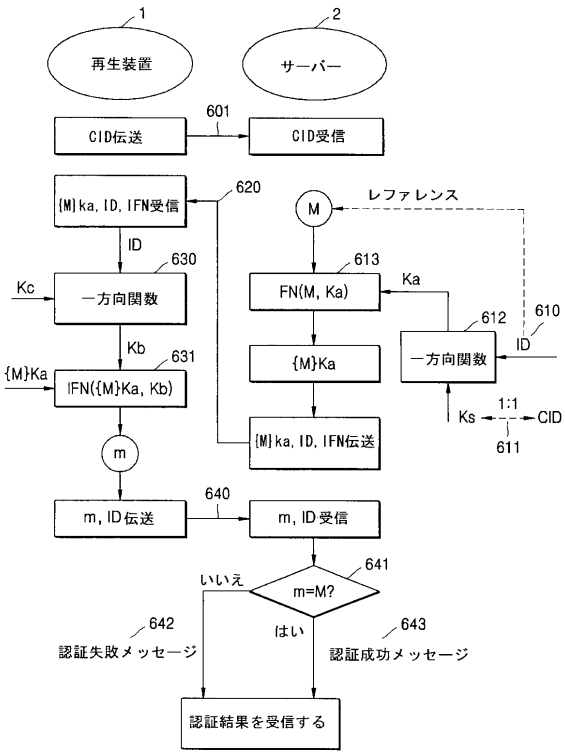
【図４】


開始
開始マークアップ文書を読み取る
401
表示されたマークアップ文書によりユーザーと相互動作する
402
他のコンテンツの表示の要請があるか？
403
ディスク要請
インターネット要請
404
ディスクから要請されたコンテンツを読み取る
コンテンツをサーバーに要求する
405
認証マークアップ文書が受信されたか？
406
いいえ
はい
410
ダウンロードされたコンテンツを再生する
認証マークアップ文書を画面に表示せずに実行することによりサーバーに認証を要求する
407
認証が成功したか？
408
はい
いいえ
認証失敗を表示する
409

【図５】


再生装置
1
サーバー
2
501
コンテンツ要請
502
コンテンツＩＤ
503
認証データを生成する
504
認証データ
505
認証データを実行する
506
認証解答情報及び索引番号
507
認証
508
認証結果

【図６】


1
2
再生装置
サーバー
601
CID伝送
CID受信
620
{M}ka, ID, IFN受信
M
レファレンス
ID
630
613
Kc
一方向関数
FN(M, Ka)
Ka
612
610
Kb
631
{M}Ka
IFN({M}Ka, Kb)
{M}Ka
一方向関数
ID
Ks
1:1
CID
611
m
{M}ka, ID, IFN伝送
640
m, ID伝送
m, ID受信
641
いいえ
m=M?
はい
642
認証失敗メッセージ
643
認証成功メッセージ
認証結果を受信する

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2004/001008

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 G06F 17/00

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)
IPC7 G06F17/00, G06F19/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
JP, KR : IPC as above

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	KR10-2003-6643 A (SAMSUNG CORP.) 23.JAN.2003 abstract, page 3 line44~62	1-16
Y	KR10-2000-72758 A (CHO BAESU) 05.DEC.2000 abstract, page3	1-16
A	KR10-2002-88737 A (BIZMODELLINE CORP.) 29.NOV.2002 See the whole document	1-16

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

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 JULY 2004 (16.07.2004)	19 JULY 2004 (19.07.2004)

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
920 Dunsan-dong, Seo-gu, Daejeon 302-701,
Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer
SONG, Dae Jong
Telephone No. 82-42-481-5992

Form PCT/ISA/210 (second sheet) (January 2004)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

Ｆターム(参考) 5B285 AA01 BA09 CA16
5J104 KA02 PA14