(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2006-303697
(P2006-303697A)
(43)公開日　平成18年11月2日(2006.11.2)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/08	(2006.01)	H04L	9/00	601B	5C164
H04N	7/16	(2006.01)	H04N	7/16	Z	5J104
			H04L	9/00	601E	

審査請求 有　請求項の数 6　OL　（全 23 頁）

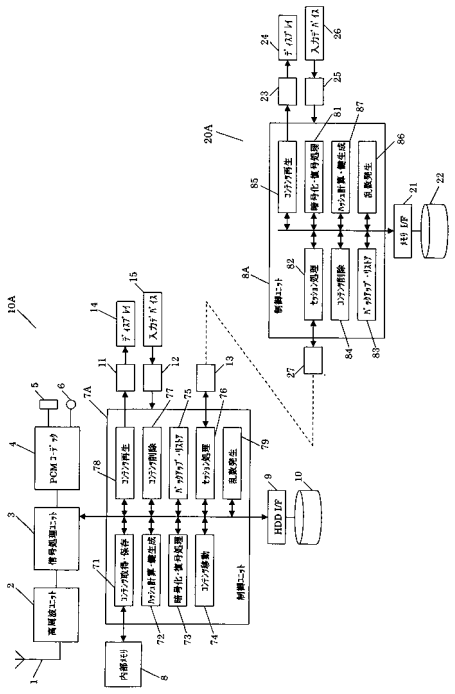
(21)出願番号　特願2005-119832 (P2005-119832)
(22)出願日　平成17年4月18日 (2005.4.18)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100109900
弁理士　堀口　浩
(72)発明者　佐藤　順
東京都青梅市末広町２丁目９番地　株式会社東芝青梅事業所内
(72)発明者　渡邊　恵古
東京都青梅市末広町２丁目９番地　株式会社東芝青梅事業所内
(72)発明者　寺内　亨
東京都青梅市末広町２丁目９番地　株式会社東芝青梅事業所内

最終頁に続く

(54)【発明の名称】情報端末装置

(57)【要約】
【課題】　バックアップ又は移動先でのコンテンツ再生を可能とすると共に、他の機器からの要求に応じて送信するコンテンツを他の機器で再生可能とする。
【解決手段】　制御ユニット８Ａは、メモリ２２に記憶されているバックアップ又は移動されたコンテンツの再生要求があると、このコンテンツのダウンロード日時を読み出して携帯端末１０Ａに対して暗号化鍵の生成を要求する。また、パーソナルコンピュータ２０Ａで携帯端末１０Ａに対するコンテンツのインポート要求が入力されると、要求されたコンテンツをハッシュ計算・鍵生成機能８７で生成した暗号鍵で復号可能な状態から、ハッシュ計算・鍵生成機能７２で生成された暗号化鍵で復号できる状態に変換する。
【選択図】図１



【特許請求の範囲】
【請求項１】
他の機器からバックアップ又は移動によって取得した前記他の機器でのみ再生可能に設定されているコンテンツファイルと、自己で再生可能なコンテンツファイルとを記憶する記憶手段と、
コンテンツの再生要求があると、該再生要求で指定されたコンテンツを含むコンテンツファイルから該コンテンツを復号する鍵情報の生成に必要な鍵生成情報を取得し、該鍵生成情報を前記他の機器へ送信する鍵生成要求手段と、
前記他の機器で生成された鍵情報を受信すると、該鍵情報を用いてコンテンツの復号を行う復号処理手段と、
前記復号処理手段によって復号されたコンテンツを再生する再生手段と
を具備することを特徴とする情報端末装置。
【請求項２】
暗号化されたコンテンツ、このコンテンツを暗号化する第２の鍵によって暗号化された第１の鍵、及びこの第１の鍵を暗号化する第２の鍵の生成に必要な鍵生成情報を含むコンテンツファイルを記憶する記憶手段と、
上記記憶手段に記憶されているコンテンツファイルを他の機器へ移動する要求があると、該他の機器に対し、前記鍵生成情報と共に第３の鍵の生成を要求する鍵生成要求手段と、
前記要求に応じて前記他の機器から前記鍵生成情報を利用して生成された第３の鍵を受信する受信手段と、
前記第受信手段によって第３の鍵を受信すると、前記鍵生成情報を利用して第２の鍵を生成して前記第１の鍵を復号し、該復号した第１の鍵を第３の鍵を用いて暗号化する暗号化・復号処理手段と、
前記コンテンツファイルの第２の鍵によって暗号化された第１の鍵を、前記第３の鍵によって暗号化された第１の鍵に変更した後に、該コンテンツファイルを前記他の機器に送信する送信手段と
を具備することを特徴とする情報端末装置。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、携帯電話機やＰＤＡ（Personal Digital Assistant）等の通信機能を有する情報端末装置に係わり、特にコンテンツサーバからコンテンツを取得して保存すると共に、このコンテンツを再生する機能を備えた情報端末装置に関する。
【背景技術】
【０００２】
近年、音楽コンテンツ等のリッチコンテンツをコンテンツサーバから情報端末装置に配信サービスが普及し始めている。この種のサービスを利用する情報通信端末では、コンテンツサーバからダウンロードしたコンテンツをメモリに一旦記憶し、ユーザの再生操作に応じて保存したコンテンツの再生を行っている。
【０００３】
一方、コンテンツを蓄積するメモリとしてハードディスク（ＨＤＤ）を採用する情報端末装置があるが、メモリとしてハードディスクを用いた場合、フラッシュメモリ等を用いる場合と比べ、多くのコンテンツを記憶することが可能となる。しかしながら、ハードディスクは一般的に衝撃に対して弱く壊れやすいという欠点がある。特に、携帯電話機のように手に持って利用する頻度が高い場合は、落下によってハードディスクが壊れるリスクも高くなる。
【０００４】
そこで、ハードディスクに記憶されたコンテンツを外部の記憶装置にバックアップしておき、ハードディスクの障害などによりコンテンツが使用できなくなった場合に、バック

アップしたコンテンツを上記外部の記憶装置からハードディスクにリストアできるようにすることが望まれている。

【０００５】

例えば、バックアップサーバを設け、通信端末がコンテンツサーバから利用条件を付したコンテンツをダウンロードするときに、コンテンツサーバは上記バックアップサーバのネットワークアドレスをコンテンツに付して送信する。そして、コンテンツを受信した通信端末は、取得したコンテンツをバックアップする際に、コンテンツに付されたネットワークアドレスをもとにコンテンツをバックアップサーバに送信し、バックアップサーバは上記通信端末から送信されたコンテンツを、上記通信端末の電話番号と対応付けて保存することが知られている（例えば、特許文献１を参照。）。

ところが、この仕組みでは、バックアップ専用のサーバを設けなければならないため、コンテンツ販売者や利用条件の管理者にとって設備投資が必要となる。

【０００６】

一方、通信端末からパーソナルコンピュータにバックアップすることも考えられており、この場合、通信端末のハードディスクに記憶されたコンテンツをその権利情報を含めて暗号化し、この暗号化されたコンテンツと権利情報とをパーソナルコンピュータにコピーする。そして、ハードディスクの障害等によりコンテンツが消失した場合に、パーソナルコンピュータにコピーしていたコンテンツと権利情報とを通信端末のハードディスクにリストアするものである。

【０００７】

さらに、通信端末のメモリを有効利用するために、通信端末のメモリからパーソナルコンピュータにコンテンツと権利情報を移動させることや、バックアップしたコンテンツと権利情報を通信端末から削除することも可能である。

【特許文献１】特開２００４－４８１８０公報

【発明の開示】

【発明が解決しようとする課題】

【０００８】

ところが、上記のように通信端末で取得したコンテンツをパーソナルコンピュータにバックアップや移動を行った場合、このコンテンツを再生させるとき、画面サイズの大きなパーソナルコンピュータでの再生を行いたいとの要求がある。

【０００９】

しかしながら、コンテンツを任意の機器で自由に再生可能とすることは著作権上の問題がある。

【００１０】

この発明は上記事情を考慮してなされたもので、その目的は、パーソナルコンピュータに移動またはバックアップしたコンテンツを、このパーソナルコンピュータで再生可能とし、かつ著作権上の管理を適正に行えるようにした情報端末装置を提供することである。

【課題を解決するための手段】

【００１１】

上記目的を達成するために、この発明に係わる情報端末装置では、他の機器からバックアップ又は移動によって取得した前記他の機器でのみ再生可能に設定されているコンテンツファイルと、自己で再生可能なコンテンツファイルとを記憶する記憶手段と、コンテンツの再生要求があると、該再生要求で指定されたコンテンツを含むコンテンツファイルから該コンテンツを復号する鍵情報の生成に必要な鍵生成情報を取得し、該鍵生成情報を前記他の機器へ送信する鍵生成要求手段と、前記他の機器で生成された鍵情報を受信すると、該鍵情報を用いてコンテンツの復号を行う復号処理手段と、前記復号処理手段によって復号されたコンテンツを再生する再生手段とを具備することを特徴としている。

【００１２】

また、他の発明に係わる情報端末装置では、暗号化されたコンテンツ、このコンテンツを暗号化する第２の鍵によって暗号化された第１の鍵、及びこの第１の鍵を暗号化する第

２の鍵の生成に必要な鍵生成情報を含むコンテンツファイルを記憶する記憶手段と、上記記憶手段に記憶されているコンテンツファイルを他の機器へ移動する要求があると、該他の機器に対し、前記鍵生成情報と共に第３の鍵の生成を要求する鍵生成要求手段と、前記要求に応じて前記他の機器から前記鍵生成情報を利用して生成された第３の鍵を受信する受信手段と、前記第受信手段によって第３の鍵を受信すると、前記鍵生成情報を利用して第２の鍵を生成して前記第１の鍵を復号し、該復号した第１の鍵を第３の鍵を用いて暗号化する暗号化・復号処理手段と、前記コンテンツファイルの第２の鍵によって暗号化された第１の鍵を、前記第３の鍵によって暗号化された第１の鍵に変更した後に、該コンテンツファイルを前記他の機器に送信する送信手段とを具備することを特徴としている。

【発明の効果】

【００１３】

この発明では、携帯端末で取得したコンテンツを他の機器にバックアップや移動を行った際、バックアップや移動先の機器でも所定の条件を満たすことで上記コンテンツを再生させることが可能となる。

【００１４】

また、ある機器で取得し、かつ該機器でのみ再生可能なコンテンツを指定した他の機器でのみ再生可能なファイルに変換することで、所望とする機器を選択して再生することが可能となる。

【発明を実施するための最良の形態】

【００１５】

（第１の実施形態）

図１は、この発明に係わる携帯端末と、該携帯端末に接続されたパーソナルコンピュータとを示したブロック図である。

【００１６】

まず同図の携帯端末１０Ａの構成について説明する。

図示しない基地局から送信された無線信号は、アンテナ１で受信された後に高周波ユニット２に入力される。高周波ユニット２では、受信された無線信号のダウンコンバートを行って中間周波信号を求め、さらに直交復調処理、ＲＡＫＥ受信機による各パスの逆拡散及び合成処理等が行われる。そして、上記ＲＡＫＥ受信機から出力された受信パケットデータは信号処理ユニット３に入力される。

【００１７】

信号処理ユニット３は、例えばＤＳＰ（Digital Signal Processor）で構成され、前記受信パケットデータを先ずメディア毎に分離し、この分離したメディア毎のデータに対してそれぞれ復号処理を施す。

例えば、受信パケットデータにオーディオデータが含まれていれば、このオーディオデータをスピーチコーデックにより復号する。また、受信パケットデータにビデオデータが含まれていれば、このビデオデータをビデオコーデックにより復号する。さらに、受信パケットデータがダウンロードコンテンツであれば、このコンテンツを伸長した後、制御ユニット７Ａに対して出力する。

【００１８】

上記復号処理により得られたディジタルオーディオ信号は、ＰＣＭ符号処理部（以後、ＰＣＭコーデックと称する）４によりＰＣＭ復号された後、増幅されてスピーカ５により出力される。また、ビデオコーデックにより復号されたディジタルビデオ信号は、制御ユニット７Ａから表示インタフェース（表示Ｉ／Ｆ）１１に供給され、表示ディスプレイ１４に表示される。

【００１９】

一方、マイクロホン６に入力された話者の音声信号は、図示しない増幅器により増幅された後にＰＣＭコーデック４でＰＣＭ符号化され、これによりディジタルオーディオ信号となって信号処理ユニット３に入力され圧縮符号化される。また、図示しないカメラから出力されるビデオ信号や、制御ユニット７Ａで作成されたメール等のテキストデータがあ

る場合は、これらも圧縮符号化される。そして圧縮符号化された各送信データは送信パケットデータに多重化された後、高周波ユニット２に入力される。

【００２０】

高周波ユニット２では、上記送信パケットデータに対してスペクトラム拡散処理、ＰＱＳＫ（Quadrature Phase Shift Keying）方式等のディジタル変調方式を使用した変調処理、無線信号へのアップコンバートが行われる。そして、このアップコンバートにより生成された無線送信信号は、電力増幅されると共に送信フィルタリング処理されてからアンテナ１を介して基地局に向けて送信される。

【００２１】

ところで、携帯端末１０Ａは、記憶媒体として内部メモリ８とハードディスク（ＨＤＤ）１０とを備えている。このうち、内部メモリ８は例えばＥＥＰＲＯＭから成り、外部インタフェース（外部Ｉ／Ｆ）１３を介して接続されたパーソナルコンピュータ２０Ａからアクセス不可能な記憶媒体であり、これに対してＨＤＤ１０は、パーソナルコンピュータ２０Ａがデータの書込み、および読出しを行うことのできる記憶媒体である。

【００２２】

制御ユニット７Ａは、例えばマイクロコンピュータ（ＣＰＵ：Central Processing Unit）を備えたもので、この発明に係わる制御機能として、コンテンツ取得・保存処理機能７１、ハッシュ計算・鍵生成機能７２、暗号化・復号処理機能７３、コンテンツ移動処理機能７４、バックアップ／リストア機能７５、セッション処理機能７６、コンテンツ削除処理機能７７、コンテンツ再生処理機能７８、及び乱数発生機能７９とを有している。なお、これらの機能は、いずれもプログラムを上記マイクロコンピュータが実行することによって実現することができる。

【００２３】

続いて、制御ユニット７Ａが有する各機能について説明する。

コンテンツ取得・保存機能７１は、図示しないコンテンツサーバに保存されているコンテンツデータをダウンロードする処理を行う。ダウンロードされるコンテンツは、ビデオデータとオーディオデータとを含んで構成されるが、再生回数や再生期間などが設定されたコンテンツの場合は、この再生回数や再生期間などの利用条件が権利情報として含まれる。そして、ダウンロードしたコンテンツをダウンロード日時と共に内部メモリ８に保存し、その後、入力インタフェース（入力Ｉ／Ｆ）１４を介して接続された入力デバイス１５より、内部メモリ８からＨＤＤ１０に移動する要求が入力されると、コンテンツを暗号化してＨＤＤ１０に移動される。

なお、コンテンツの暗号化は、後述のハッシュ計算・鍵生成機能７２で生成された暗号化鍵を用い暗号化・復号処理機能７３によって実施される。

【００２４】

ハッシュ計算・鍵生成機能７２は、コンテンツをダウンロードしたときに付与されるダウンロード日時及び／又は乱数発生部７９で発生した乱数と、携帯端末１０Ａにユニークに割り当てられている電話番号又は機器固有ＩＤとに基づいて暗号化鍵の生成を行い、更に、Ｉ／Ｆ１３に接続されたパーソナルコンピュータ２０Ａから受信した暗号化鍵転送要求を受け、この暗号化鍵転送要求に含まれるダウンロード日時及び／又は乱数を読み出し、携帯端末１０Ａ内のメモリに記憶されている電話番号又は機器固有ＩＤとを用いて暗号化鍵の生成を行う。また、パーソナルコンピュータ２０Ａとの間でセキュアセッションを確立するときに必要なハッシュ計算もここで行われる。

【００２５】

暗号化・復号処理機能７３は、コンテンツ取得・保存機能７１およびコンテンツ再生処理機能７６からの要求に基づき、ハッシュ計算・鍵生成機能７２によって生成された暗号化鍵を用いて暗号化されているコンテンツ（以下、暗号化されているコンテンツを、暗号化コンテンツと称する）の復号処理、およびコンテンツの暗号化処理を行う。また、パーソナルコンピュータ２０Ａとの間でセキュアセッションを確立するときに必要な暗号・復号処理もここで行われる。なお、暗号化方式としては、例えばＡＥＳ（Advanced Encrypt

ion Standard）が用いられる。

【００２６】

コンテンツ移動機能７４は、ＨＤＤ１０に記憶された暗号化コンテンツを、外部Ｉ／Ｆ１３を介して接続されたパーソナルコンピュータ２０Ａのメモリに移動させる処理を行う。なお、暗号化コンテンツの移動とは、パーソナルコンピュータ２０Ａのメモリ２２に暗号化コンテンツを記憶させ、ＨＤＤ１０から暗号化コンテンツを消去することを意味している。

【００２７】

バックアップ／リストア機能７５は、ＨＤＤ１０に記憶された暗号化コンテンツのコピーを外部Ｉ／Ｆ１３を介して接続されたパーソナルコンピュータ２０Ａに転送し、パーソナルコンピュータ２０Ａのメモリ２２にバックアップさせるとともに、ユーザ操作に応じてパーソナルコンピュータ２０Ａのメモリから暗号化コンテンツを転送させてＨＤＤ１０にリストアする処理を実行する。

このバックアップでは、パーソナルコンピュータ２０Ａに転送された暗号化コンテンツは携帯端末１０ＡのＨＤＤ１０にも存在する。

【００２８】

セッション処理機能７６は、外部Ｉ／Ｆ１３を介して接続されたパーソナルコンピュータ２０Ａとの間で暗号化コンテンツなど各種データの送受信を行うときに、パーソナルコンピュータ２０Ａとの間でセッションを形成する。また、暗号化鍵を携帯端末１０Ａからパーソナルコンピュータ２０Ａに送信するときや、携帯端末１０Ａとパーソナルコンピュータ２０Ａとの間で認証を行うときは、形成するセッションはセキュアなセッションを形成する。このセキュアなセッションの形成について後に詳述する。

【００２９】

コンテンツ削除機能７７は、入力デバイス１５から入力された削除要求に応じて内部メモリ８およびＨＤＤ１０に記憶されているコンテンツの削除を行う。このとき、コンテンツに対応して記憶されているダウンロード日時、乱数、権利情報の削除も行われる。

【００３０】

再生処理機能７８は、入力デバイス１５から入力されたコンテンツ再生要求に基づいて動作し、指定された暗号化コンテンツをＨＤＤ１０から読み出し、またコンテンツを内部メモリ８から読み出して再生処理を行う。なお、暗号化コンテンツを再生する場合は、ハッシュ計算・鍵生成手段７２で生成された暗号化鍵が利用される。

【００３１】

乱数発生機能７９は、暗号鍵生成やセキュアなセッション形成などに利用される乱数の生成を行う。

【００３２】

また、携帯端末１０Ａには、液晶表示器などのディスプレイ１４、０～９のうちの１つの数字と少なくとも１つのアルファベットの入力を行うテンキー、メニュー表示やメール機能を起動するための機能を有する機能キーからなる入力デバイス１５も備えられている。

【００３３】

なお、外部Ｉ／Ｆ１３はＵＳＢ（Universal Serial Bus）ケーブルのような有線ケーブルの接続可能なインタフェースや、Ｂｌｕｅｔｏｏｔｈ（登録商標）のような無線ＬＡＮによって通信するインタフェースなど、任意のインタフェースを利用することが可能である。

【００３４】

続いてパーソナルコンピュータ２０Ａの構成について説明する。

制御ユニット８Ａも、携帯端末１０ＡのようにＣＰＵを備えており、暗号化・復号処理機能８１、セッション処理機能８２、バックアップ・リストア機能８３、コンテンツ削除機能８４、コンテンツ再生処理機能８５、乱数発生機能８６、ハッシュ計算・鍵生成機能８７の各機能を、プログラムを実行することで実現することができる。

【００３５】
暗号化・復号処理機能８１は、コンテンツ再生処理機能８５からの再生要求に基づき、携帯端末１０Ａで生成された暗号化鍵を用いて暗号化コンテンツの復号処理を行う。
【００３６】
セッション処理機能８２は、携帯端末１０Ａとの間で暗号化コンテンツなどの各種データの送受信を行うときに、携帯端末１０Ａとの間でセッションを形成する。そして、暗号化鍵の生成を要求する際の処理、即ち、暗号化コンテンツと対応して記憶されているダウンロード日時及び／または乱数の携帯端末１０Ａへの送信、携帯端末１０Ａで生成された暗号化鍵を受信するときにはセキュアなセッションを形成する。
【００３７】
バックアップ・リストア機能８３は、携帯端末１０Ａから暗号化コンテンツのバックアップ要求を受信すると、携帯端末１０Ａから送られてきた暗号化コンテンツとダウンロード日時及び／又は乱数をメモリ２２へ記憶する処理を実行するとともに、メモリ２２に記憶されている暗号化コンテンツのリストア要求を受信すると、メモリ２２から暗号化コンテンツを読み出して、携帯端末１０Ａへ送信する処理を行う。
【００３８】
コンテンツ削除機能８４は、入力デバイス２６から入力された削除要求に応じてメモリ２２に記憶されている暗号化コンテンツの削除を行う。
【００３９】
コンテンツ再生処理機能８５は、入力デバイス２６から入力されたコンテンツ再生要求に基づいて動作し、指定された暗号化コンテンツに対応して記憶されているダウンロード日時及び／又は乱数を読み出し、携帯端末１０Ａに対して暗号化鍵の転送要求を行う。そして、携帯端末１０Ａから暗号化鍵を受け取ると、この暗号化鍵を利用して復号されたコンテンツをディスプレイ２４に表示させる。
【００４０】
乱数発生機能８６は、セッション処理機能８２が携帯端末１０Ａとの間でセキュアなセッションを形成する際に利用する乱数を発生させる。
【００４１】
ハッシュ計算・鍵生成機能８７は、携帯端末１０Ａとの間でセキュアセッションを確立するときに必要なハッシュ計算や、コンテンツの暗号化および復号に必要な暗号化鍵の生成を行う。
【００４２】
また、パーソナルコンピュータ２０Ａには、液晶表示器などのディスプレイ１４、アルファベットやひらがな、数字などを入力するための入力デバイス２６、そして携帯端末１０Ａと通信を行うための外部Ｉ／Ｆ２７を備えている。
次に、以上のように構成された携帯端末１０Ａとパーソナルコンピュータ２０Ａの動作について説明する。
【００４３】
（１）コンテンツの取得・保存動作
図２は携帯端末１０Ａのコンテンツの取得・保存の動作を示している。
コンテンツ取得・保存機能７１は、入力デバイス１５から入力されたコンテンツのダウンロード要求を受けると、基地局（図示せず）を介して図示しないコンテンツサーバからコンテンツをダウンロードする（ステップ２ａ）。なお、このコンテンツのダウンロードは、事前にコンテンツサーバから取得したコンテンツリストから所望とするコンテンツを選択することによって行われる。
【００４４】
ダウンロード要求を行ったコンテンツが基地局を介してダウンロードされると、制御ユニット７Ａは携帯端末１０Ａの内部クロックから取得したダウンロード日時を上記コンテンツに付加する（ステップ２ｂ）。
【００４５】

なお、ステップ２ｂでコンテンツに付加されるダウンロード日時は、携帯端末１０Ａの内部クロックを利用するのではなく、基地局から受信する基準時刻を利用することも可能である。

【００４６】

そして、ダウンロード日時の付与されたコンテンツは内部メモリ８に保存される（ステップ２ｃ）。

【００４７】

その後、内部メモリ８にコンテンツのダウンロードが完了し、ディスプレイ２４にＨＤＤへの移動を問い合わせる表示がなされ、これに応じて入力デバイス１５から内部メモリ８に保存した上記コンテンツをＨＤＤ１０に移動する要求があると（ステップ２ｄのＹｅｓ）、コンテンツ取得・保存機能７１は、内部メモリ８に保存され、ＨＤＤ１０へ移動する要求のあったコンテンツに対応して記憶されているダウンロード日時を読み出してハッシュ計算・鍵生成機能７２に暗号化鍵の生成を要求し、この要求を受けたハッシュ計算・鍵生成機能７２は、上記ダウンロード日時と携帯端末１０Ａの電話番号とを用いて暗号化鍵の生成を行う（ステップ２ｅ）。

【００４８】

ハッシュ計算・鍵生成機能７２で暗号化鍵が生成されると、暗号化・復号処理機能７３は、この生成された暗号化鍵を用いてコンテンツの暗号化処理を行い暗号化コンテンツを作成する（ステップ２ｆ）。

【００４９】

そして、コンテンツの暗号化処理が終了すると、コンテンツ取得・保存機能７１は、ダウンロード日時と暗号化コンテンツをＨＤＤＩ／Ｆ９を介してＨＤＤ１０に移動し、内部メモリ８から移動したコンテンツの削除を行い（ステップ２ｇ）、ダウンロードの処理を完了させる。

【００５０】

以上のようにしてダウンロードしたコンテンツのＨＤＤ１０への保存が完了したとき、ＨＤＤ１０では、図３に示すように、ダウンロード日時と暗号化コンテンツが対応付けられて保存される。

【００５１】

一方、内部メモリ８にダウンロードしたコンテンツの保存が完了した後に、ＨＤＤへの移動を行わないとの選択が入力デバイス１５から入力された場合も（ステップ２ｄのＮｏ）、コンテンツのダウンロードが完了する。

【００５２】

（２）コンテンツのバックアップ

ＨＤＤ１０は一般的に衝撃に弱く故障しやすいため、ＨＤＤ１０に記憶された暗号化コンテンツをパーソナルコンピュータ等の外部の端末にバックアップさせる。例えば、パーソナルコンピュータ２０Ａに暗号化コンテンツをバックアップする際、携帯端末１０Ａの外部Ｉ／Ｆ１３とパーソナルコンピュータ２０Ａの外部Ｉ／Ｆ２７間をＵＳＢケーブル等で接続し、暗号化コンテンツのバックアップを行う。

【００５３】

図４は、ＨＤＤ１０に記憶されているコンテンツのバックアップ動作を示した図である。

【００５４】

ユーザがパーソナルコンピュータ２０Ａの入力デバイス２６を操作し、携帯端末１０ＡのＨＤＤ１０に記憶されているコンテンツのバックアップを指示すると（ステップ４ａ）、制御ユニット８Ａのセッション処理機能８２は、外部Ｉ／Ｆ２７を介して携帯端末１０Ａのセッション処理機能７６との間でセッションを形成する処理を実行する（ステップ４ｂ）。

【００５５】

セッションの形成が完了すると、バックアップ・リストア機能８３は、外部Ｉ／Ｆ２７

を介して携帯端末１０ＡのＨＤＤ１０にアクセスして記憶されているコンテンツのタイトルを取得してディスプレイ２４に一覧リストとして表示させる（ステップ４ｃ）。なお、コンテンツのタイトルは暗号化されずに暗号化コンテンツと共に保存されているものとする。

【００５６】

この表示された一覧からバックアップするコンテンツの指示があると（ステップ４ｅ）、バックアップ・リストア機能８３は、ＨＤＤ１０から指定されたダウンロード日時と暗号化コンテンツを読み出して、メモリ２２に保存し（ステップ４ｆ）、バックアップの処理が完了する。このとき、メモリ２２にバックアップされた暗号化コンテンツとダウンロード日時は図５に示すように、互いに対応付けられて記憶される。

【００５７】

以上のようにして携帯端末１０Ａにダウンロードされたコンテンツのバックアップが行われる。

【００５８】

また、バックアップした暗号化コンテンツを携帯端末１０ＡのＨＤＤ１０にリストアする場合は、同様にパーソナルコンピュータ２０Ａと携帯端末１０ＡをＵＳＢケーブルなどで接続し、入力デバイス２６を操作することで実行する。

【００５９】

なお、上記説明では、パーソナルコンピュータ２０Ａを操作してコンテンツのバックアップを行うとしているが、このようなバックアップは携帯端末１０Ａから行うことも可能である。この場合、入力デバイス１５を操作してディスプレイ１４に表示されたメニューからコンテンツのバックアップ機能を選択し、ＨＤＤ１０に記憶されているコンテンツの一覧リストからバックアップするコンテンツを選択することで、セッション処理機能７６とセッション処理機能８２によって形成されたセッションを介してパーソナルコンピュータ２０Ａのメモリ２２に暗号化コンテンツとダウンロード時刻の保存が行われる。

【００６０】

また、上記説明は、コンテンツ及び暗号化コンテンツに対応してダウンロード日時が保存されるとしているが、ダウンロード日時に代えて乱数発声機能７９によって生成された乱数を保存してもよく、また、ダウンロード日時と共に乱数を保存してもよい。このような場合、ハッシュ計算・鍵生成機能７２では、乱数を用い、またはダウンロード日時と乱数を用いて暗号化鍵の生成を行う。

【００６１】

（３）コンテンツの移動

ＨＤＤ１０に保存したコンテンツの数が多くなり一部のコンテンツを他の機器に移動することや、保存したコンテンツを他の機器で再生するために移動することが行われる。

【００６２】

図６はダウンロードによってＨＤＤ１０に保存されたコンテンツをパーソナルコンピュータ２０Ａに移動させる動作を説明した図である。

【００６３】

まず、携帯端末１０Ａの入力デバイス１５を操作してＨＤＤ１０に記憶されているコンテンツの一覧を表示する要求があると、制御ユニット７ＡはＨＤＤ１０に記憶されている各コンテンツのタイトルを読み出してディスプレイ１４に表示させる（ステップ６ａ）。

【００６４】

そして、ディスプレイ１４に表示されているコンテンツの一覧からパーソナルコンピュータ２０Ａに移動するコンテンツの選択が行われると（ステップ６ｂ）、コンテンツ移動処理機能７４は指定された暗号化コンテンツとこれに対応して記憶されているダウンロード日時を読み出し、外部Ｉ／Ｆ１３を介しセッション処理機能７６とセッション処理機能８２によって形成されたセッションを介してパーソナルコンピュータ２０Ａに前記読み出した暗号化コンテンツとダウンロード日時の送信を行う（ステップ６ｃ）。この送信処理が完了すると、コンテンツ移動処理機能７４はコンテンツ削除機能７７に対してパーソナ

ルコンピュータ２０Ａに移動させたコンテンツの削除を指示し、これに応じてコンテンツ削除機能は指示された暗号化コンテンツとダウンロード日時をＨＤＤ１０から削除し（ステップ６ｄ）、コンテンツの移動する処理が完了する。

【００６５】

一方、携帯端末１０Ａからパーソナルコンピュータ２０Ａに送信された暗号化コンテンツとダウンロード日時は制御ユニット８Ａによってメモリ２２に記憶される。

【００６６】

（４）パーソナルコンピュータでのコンテンツ再生

続いて、バックアップや移動処理されたコンテンツをパーソナルコンピュータ２０Ａで再生する処理について説明する。

【００６７】

上記の通り、パーソナルコンピュータ２０Ａのメモリ２２にバックアップや移動されたコンテンツは暗号化コンテンツとして記憶されており、またこの暗号化コンテンツとともに記憶されているのはダウンロード日時のみであるため、コンテンツを暗号化した暗号化鍵を生成することはできない。

【００６８】

そこでここでは、バックアップや移動の処理によってメモリ２２に記憶されたコンテンツの再生を行う場合、携帯端末１０Ａに対して暗号化鍵の生成を要求し、この要求によって携帯端末１０Ａで生成された暗号化鍵を受け取ることでパーソナルコンピュータ２０Ａでのコンテンツ再生を実現することとしている。即ち、暗号化コンテンツの暗号化鍵を生成できる携帯端末１０Ａが外部Ｉ／Ｆ２７を介して接続されることを、再生の一条件としている。

【００６９】

以下、図７を用いてパーソナルコンピュータ２０Ａで暗号化コンテンツを再生する処理について説明する。

【００７０】

まず、パーソナルコンピュータ２０Ａの入力デバイス２６が操作され、メモリ２２に記憶されているコンテンツの一覧表示の要求があると（ステップ７ａ）、制御ユニット８Ａはメモリ２２記憶されているコンテンツのタイトルを読み出してディスプレイ２４に表示させる（ステップ７ｂ）。図８は、このときにディスプレイ２４に表示されたコンテンツの一覧の例を示しており、３つのタイトル「ＡＡＡ」、「ＢＢＢ」、そして「ＣＣＣ」が表示されている。そして、タイトル「ＡＡＡ」のみタイトルの頭に「†」が表示されているが、この記号はタイトル「ＡＡＡ」のコンテンツは携帯端末１０Ａからバックアップまたは移動されたことを意味している。

【００７１】

入力デバイス２６を操作してディスプレイ２４に表示された一覧から再生するコンテンツの選択が行われると（ステップ７ｃのＹＥＳ）、制御ユニット８Ａは再生指示されたコンテンツが携帯端末１０Ａからバックアップ又は移動されたコンテンツである可能確認を行う（ステップ７ｄ）。この確認は、携帯端末１０Ａから受けた暗号化コンテンツをメモリ２２に記憶する際にバックアップ又は移動されたことを示すフラグを設けることで容易に実現することができる。また、ダウンロード日時をバックアップ又は移動されたコンテンツしか持たない仕組みとした場合は、このダウンロード日時の有無によって判断することも可能である。

【００７２】

ここで、タイトル「ＡＡＡ」の再生が指示されると（ステップ７ｄのＹＥＳ）、制御ユニット８Ａはタイトル「ＡＡＡ」は携帯端末１０Ａからバックアップまたは移動された暗号化コンテンツであるため、メモリ２２からこの暗号化コンテンツに対応して記憶されているダウンロード日時を読み出し、セッション処理機能８２とセッション処理機能７６とで形成されたセッションを介して携帯端末１０Ａに暗号化鍵の転送を要求する（ステップ７ｅ）。そして、この要求を行った後、セッション処理機能８２に対してセキュアなセッ

ションの形成を要求して携帯端末１０Ａから暗号化鍵を秘匿に入手する処理を行い、携帯端末１０Ａがダウンロード日時と電話番号から生成した暗号化鍵を受信する（ステップ７ｇ）。暗号化鍵が入手されると、暗号化・復号処理機能８１は、この暗号化鍵を用いてタイトル「ＡＡＡ」の暗号化コンテンツの復号処理を行い（ステップ７ｇ）、復号されたコンテンツはコンテンツ再生処理機能８５によってディスプレイ２４に再生される。

【００７３】

ここでセッション処理機能７６とセッション処理機能８２との間で形成されるセキュアなセッション、即ち、暗号化鍵を秘匿に入手する手順について説明する

図９は暗号化鍵を秘匿に入手するための流れを説明している。

【００７４】

まず、制御ユニット８Ａの暗号化・復号処理機能８１は、乱数発生機能８６によって発生された乱数ＲＡＮａを、認証鍵Ｋａを用いて暗号化（図９のＥ）する（ステップ９ａ）。そして、この暗号化された乱数Ｅ［ＲＡＮａ］は、外部Ｉ／Ｆ２７を介して携帯端末１０Ａに送られる。

【００７５】

携帯端末１０Ａの制御ユニット７Ａが上記暗号化された乱数Ｅ［ＲＡＮａ］を受信すると、この暗号化された乱数Ｅ［ＲＡＮａ］を暗号化・復号処理機能７３に渡し、暗号化・復号処理機能８１が用いたのと同一の認証鍵Ｋａを用いて復号処理を行い、乱数ＲＡＮａを抽出する（ステップ９ｂ）。また、暗号化・復号処理機能７３は、認証鍵Ｋａを用い、暗号化された乱数Ｅ［ＲＡＮａ］に対する一方向性関数の処理（図９のＧ）を施してＴＯＫＥＮａを求める（ステップ９ｃ）。そしてこの求められたＴＯＫＥＮａは外部Ｉ／Ｆ１３を介してパーソナルコンピュータ２０Ａへと送信される。

【００７６】

なお、上記一方向性関数とは、図１０に示すように、入力ｄ１に対して入力ｄ２を用いて暗号化処理を施すと共に、この暗号化によって得られた結果と入力ｄ１との排他的論理和（ＥｘＯＲ）の演算を行う処理のことである。そして、上記の例では、入力ｄ１が暗号化された乱数、入力ｄ２が認証鍵Ｋａに対応している。

【００７７】

一方、暗号化・復号処理部８１でも暗号化された乱数Ｅ［ＲＡＮａ］と認証鍵Ｋａを用いて同様の一方向性関数の処理を行ってＴＯＫＥＮａ’を求め（ステップ９ｄ）、制御ユニット８Ａは、このＴＯＫＥＮａ’と携帯端末１０Ａから受信したＴＯＫＥＮａとが一致するかの認証を行う（ステップ９ｅ）。

【００７８】

上記認証処理が終わると、制御ユニット７Ａの暗号化・復号処理機能７３は、乱数発生機能７９によって発生された乱数ＲＡＮｂを、認証鍵Ｋａを用いて暗号化する（ステップ９ｆ）。そして、この暗号化された乱数Ｅ［ＲＡＮｂ］を外部Ｉ／Ｆ１３を介してパーソナルコンピュータ２０Ａに送られる。

【００７９】

パーソナルコンピュータ２０Ａの制御ユニット８Ａが上記暗号化された乱数Ｅ［ＲＡＮｂ］を受信すると、この暗号化された乱数Ｅ［ＲＡＮｂ］を暗号化・復号処理機能８１に渡し、暗号化・復号処理機能７３が用いたのと同一の認証鍵Ｋａを用いて復号処理を行い、乱数ＲＡＮｂを抽出する（ステップ９ｇ）。また、暗号化・復号処理機能８１は、認証鍵Ｋａを用い、暗号化された乱数Ｅ［ＲＡＮｂ］に対する一方向性関数の処理を施してＴＯＫＥＮｂを求める（ステップ９ｈ）。そしてこの求められたＴＯＫＥＮｂは外部Ｉ／Ｆ２７を介して携帯端末１０Ａへと送信される。

【００８０】

一方、暗号化・復号処理機能７３でも暗号化された乱数Ｅ［ＲＡＮｂ］と認証鍵Ｋａを用いて同様の一方向性関数の処理を行ってＴＯＫＥＮｂ’を求め（ステップ９ｉ）、制御ユニット７Ａは、このＴＯＫＥＮｂ’とパーソナルコンピュータ２０Ａから受信したＴＯＫＥＮｂとが一致するかの認証を行う（ステップ９ｊ）。

【００８１】
以上のような２度の認証作業がいずれも一致との判断で終了すると、続いて暗号化鍵の転送処理が実施される。
【００８２】
携帯端末１０Ａのハッシュ計算・鍵生成機能７２は、乱数発生機能７９で生成された上記乱数ＲＡＮｂと復号処理で抽出した乱数ＲＡＮａとのＥｘＯＲ演算を行い（ステップ９ｋ）、更にこの演算結果に秘密鍵Ｋｎを用いて一方向性関数の処理を行い（ステップ９ｌ）、セッション鍵Ｓｋを求める。
【００８３】
なお、ここでは図１０の入力ｄ１が上記ＥｘＯＲ演算の結果、ｄ２が秘密鍵Ｋｎに対応する。
【００８４】
一方、パーソナルコンピュータ２０Ａのハッシュ計算・鍵生成機能８７でも乱数発生機能８６で生成された上記乱数ＲＡＮａと復号処理で抽出した乱数ＲＡＮｂとのＥｘＯＲ演算を行い（ステップ９ｍ）、更にこの演算結果に同一の秘密鍵Ｋｎを用いて一方向性関数の処理を行い（ステップ９ｎ）、セッション鍵Ｓｋを求める。
【００８５】
以上のように求められた２つのセッション鍵Ｓｋは、同じ乱数と同じアルゴリズムで生成されるため、同じ鍵として得られる。
【００８６】
セッション鍵Ｓｋの生成が終わると、通信端末１０Ａの暗号化・復号処理機能７３は、上記パーソナルコンピュータ２０Ａから受信したダウンロード日時と自己の電話番号又は機器固有ＩＤとを用いて暗号化鍵の生成を行い（ステップ９ｏ）、更にこの生成した暗号化鍵を、上記セッション鍵Ｓｋを用いて暗号化して（ステップ９ｐ）、パーソナルコンピュータ２０Ａに対して送信する。
【００８７】
パーソナルコンピュータ２０Ａは、ハッシュ計算・鍵生成機能８７で求めたセッション鍵Ｓｋを用いて暗号化された暗号化鍵の復号する処理を行い（ステップ９ｒ）、そして、得られた暗号化鍵を用いて暗号化されたコンテンツの復号処理が行われる。
【００８８】
また、図７のステップ７ｃで再生指示以外の入力があると、この入力が終了を指示するものであるか確認し（ステップ７ｈ）、終了以外の指示（ステップ７ｈのＮｏ）、例えば一覧のスクロールや、タイトルを選択するための上下方向への移動である場合は、指示された処理を行った後に次の入力を待つためステップ７ｃに戻り、終了が指示された場合は（ステップ７ｈのＹＥＳ）、コンテンツを再生するための機能を終了し、例えば待ち受け画面に戻る。
【００８９】
また、ステップ７ｄで再生の指示されたコンテンツが携帯端末１０Ａからバックアップや移動されたコンテンツ以外のコンテンツであった場合、即ち、図８のタイトル「ＢＢＢ」やタイトル「ＣＣＣ」が選択された場合は、制御ユニット８Ａはコンテンツ再生処理機能８５に再生を指示し、これを受けたコンテンツ再生処理機能８５は、メモリ２２からタイトル「ＢＢＢ」又はタイトル「ＣＣＣ」に対応したコンテンツを読み出してディスプレイ２４に表示させる。
【００９０】
なお、タイトル「ＢＢＢ」やタイトル「ＣＣＣ」のコンテンツが暗号化されている場合は、ハッシュ計算・鍵生成機能８７に鍵の生成を促し、生成された暗号化鍵を用いて暗号化・復号処理機能８１で復号されたコンテンツが再生される。
【００９１】
以上のような仕組みにより、ユーザに割り当てられた電話番号のような情報を用いて生成された暗号化鍵で暗号化されたコンテンツであっても、バックアップや移動を行った先

の機器においても再生することが可能となり、かつ、コンテンツが制限なく利用されることを防止できる。

【００９２】

（第２の実施形態）

続いてこの発明の第２の実施形態について説明する。

【００９３】

この実施形態では、パーソナルコンピュータがコンテンツサーバからインタネットなどを経由してダウンロードしたコンテンツや、ＣＤ－ＲＯＭなどの記憶媒体から取り込んだコンテンツを携帯端末に移動（インポート）させて利用することを想定したもので、パーソナルコンピュータに特有の情報、例えば機器番号を用いて生成された暗号化鍵（以下、ＰＣバインド鍵と称する）を用いて暗号化されたコンテンツ鍵を含むコンテンツから、携帯端末に特有の情報である電話番号もしくは乱数を用いて生成された暗号化鍵（以下、ユーザバインド鍵と称する）を用いて暗号化したコンテンツ鍵を含むコンテンツに変換してから携帯端末に移動させることを特徴としている。

【００９４】

（１）コンテンツのインポート

図１１は、コンテンツサーバからダウンロードしたコンテンツ、又はＣＤ－ＲＯＭなどの記憶媒体から取り込んだコンテンツのファイルフォーマットの一例を示した図であり、このフォーマットではコンテンツＣは、コンテンツ鍵Ｋｃによって暗号化された暗号化コンテンツＥＫｃ［Ｃ］を格納するエリア１１ａ、ＰＣバインド鍵Ｋｂ又はユーザバインド鍵Ｋｂ’によって暗号化されたコンテンツ鍵ＥＫｂ［Ｋｃ］又はＥＫｂ’［Ｋｃ］を格納するエリア１１ｂ、そしてＰＣバインド鍵やユーザバインド鍵の生成に必要な情報（例えば、ダウンロード時刻、乱数など）のそれぞれを格納するエリア１１ｃから構成されている。

【００９５】

以下、パーソナルコンピュータ２０Ａから携帯端末１０Ａにコンテンツを移動する処理について図１２を用いて説明する。

【００９６】

携帯端末１０Ａとパーソナルコンピュータ２０ＡがＵＳＢバスなどによって接続されている状態で、入力デバイス２６からコンテンツのインポート機能（メモリ２２で記憶しているコンテンツファイルをＨＤＤ１０に移動させるための処理を実行する機能）が起動されると、制御ユニット８Ａは、メモリ２２からコンテンツに関する情報、例えば各コンテンツのタイトルを読み出し、一覧としてディスプレイ２４に表示する（ステップ１２ａ）。

【００９７】

この状態で、制御ユニット８Ａは、入力デバイス２６から移動（インポート）を行うコンテンツの選択がされたか監視し（ステップ１２ｂ）、選択があるとメモリ２２からコンテンツに対応して記憶されているバインド鍵生成情報を読み出し（ステップ１２ｃ）、携帯端末１０Ａに対して読み出した鍵生成情報を含んだユーザバインド鍵Ｋｂ’の生成及び送信を要求する（ステップ１２ｄ）。

【００９８】

携帯端末１０Ａが外部Ｉ／Ｆ１３を介して鍵の生成及び送信の要求を受けると（ステップ１２ｅ）、ハッシュ計算・鍵生成機能７２は、この要求に含まれているバインド鍵生成情報を抽出し、携帯端末１０Ａに固有な情報（例えば、機器番号や電話番号）と組み合わせてユーザバインド鍵Ｋｂ’を生成し、生成されたユーザバインド鍵Ｋｂ’は制御ユニット７Ａによってパーソナルコンピュータ２０Ａに送信される（ステップ１２ｆ）。

【００９９】

なお、上記ユーザバインド鍵が生成されて送信されるまでの手順は、秘匿性を保つために、セッション処理機能７６とセッション処理機能８２との間でセキュアなセッションを行った上で実行されることが好ましい。例えば、図９で説明した処理と同じようなセッシ

ョン鍵Ｓｋを生成し、送受信するバインド鍵生成情報やユーザバインド鍵Ｋｂ’を暗号化した上で送受信すればよい。

【０１００】

続いて、パーソナルコンピュータ２０Ａの制御ユニット８Ａが携帯端末１０Ａからユーザバインド鍵を受信すると、暗号化・復号処理機能８１は、上記バインド鍵生成情報とパーソナルコンピュータ（ＰＣ）に固有な情報（聞き番号など）とを組み合わせてＰＣバインド鍵Ｋｃを生成し、ＰＣバインド鍵Ｋｃで暗号化されているコンテンツ鍵Ｋｃを復号し（ステップ１２ｇ）、その後、ユーザバインド鍵Ｋｂ’を用いてコンテンツ鍵Ｋｃを暗号化する（ステップ１２ｈ）。

【０１０１】

上記処理が終了すると、コンテンツファイルは図１３に示されるように、コンテンツ鍵Ｋｃで暗号化されたコンテンツＥＫｃ［Ｃ］１３ａ、ユーザバインド鍵Ｋｂ’で暗号化されたコンテンツ鍵ＥＫｂ’［Ｋｃ］１３ｂ、そして鍵生成情報１３ａで構成され、制御ユニット８Ａはこのコンテンツファイルを携帯端末１０Ａに対して送信する（ステップ１２ｉ）。

【０１０２】

そして、携帯端末１０Ａは、パーソナルコンピュータ２０Ａから移動が指示されたコンテンツファイルを受信した後、ＨＤＤ１０への格納を行って（ステップ１２ｊ）、移動（インポート）の処理が終了する。

【０１０３】

（２）コンテンツの再生

上記のようにしてパーソナルコンピュータ２０Ａから携帯端末１０Ａへのコンテンツのインポートが完了すると、携帯端末１０Ａでのコンテンツ再生が可能となる。

【０１０４】

図１４は、インポートしたコンテンツを携帯端末１０で再生する処理を説明した図である。

【０１０５】

まず、入力デバイス１５が操作されてコンテンツを再生させる機能が起動されると（ステップ１４ａ）、制御ユニット７ＡはＨＤＤ１０に記憶されているコンテンツのタイトルを読み出してリストとしてディスプレイ１４に表示させる（ステップ１４ｂ）。このとき、カーソルはリストの最初のタイトルに設定されている。

【０１０６】

続いて制御ユニット７Ａは入力デバイス１５からの入力を待ち、再生要求があると（ステップ１４ｃのＹＥＳ）、カーソルが設定されているコンテンツファイルをＨＤＤ１０から読み出してこのファイルに含まれている乱数ＲＡＮを抽出してハッシュ計算・鍵生成機能７２にユーザバインド鍵Ｋｂ’の生成を要求する（ステップ１４ｄ）。

【０１０７】

ユーザバインド鍵Ｋｂ’が生成されると、制御ユニット７Ａは暗号化されたコンテンツ鍵ＥＫｂ’［Ｋｃ］をコンテンツファイルから抽出してユーザバインド鍵Ｋｂ’とともに暗号化・復号処理機能７３に復号処理を要求する（ステップ１４ｅ）。この要求があると、暗号化・復号処理機能７３ではユーザバインド鍵Ｋｂ’を用いて暗号化されたコンテンツ鍵ＥＫｂ’［Ｋｃ］を復号してコンテンツ鍵Ｋｃを求める（ステップ１４ｆ）。

【０１０８】

そして、コンテンツ鍵Ｋｃが求まると、制御ユニット７Ａは更に暗号化・復号処理機能７３に対して暗号化コンテンツＥＫｃ［Ｃ］の復号を要求し、暗号化・復号処理機能７３によってコンテンツＣが得られる（ステップ１４ｇ）。

【０１０９】

このようにして得られたコンテンツＣはコンテンツ再生処理機能７８によってディスプレイ１４に表示される（ステップ１４ｈ）。

【０１１０】

一方、ステップ１４ｃで再生要求以外の入力が入力デバイス１５から指示されると、この入力がコンテンツの再生を終了させる処理であるか判断して、終了処理であれば、待ちうけ画面などに復帰し（ステップ１４ｊのＹＥＳ）、終了処理以外の入力であればこの入力に係る処理（例えば、リスト間のカーソル移動、頁切り替えなど）を行って次の入力を待つ（ステップ１４ｊのＮＯ）。

【０１１１】

以上のような仕組みにより、ある機器でのみ再生が認められているコンテンツを他の機器に移動させて再生することが可能となるとともに、コンテンツが制限なく利用されることを防止できる。

【図面の簡単な説明】

【０１１２】

【図１】この発明の携帯端末とパーソナルコンピュータの構成を示すブロック図。

【図２】コンテンツの取得・保存処理の手順を示すフローチャート。

【図３】取得したコンテンツが携帯端末のハードディスクに記憶されている状態を示す図。

【図４】バックアップの手順を示すフローチャート。

【図５】バックアップしたコンテンツがパーソナルコンピュータのメモリに記憶されている状態を示す図。

【図６】携帯端末からパーソナルコンピュータへコンテンツを移動する手順を示すフローチャート。

【図７】バックアップまたは移動したコンテンツをパーソナルコンピュータで再生させるときの手順を示したフローチャート。

【図８】パーソナルコンピュータのディスプレイに表示されたコンテンツのリストの例を示す図。

【図９】携帯端末とパーソナルコンピュータ間でセキュアなセッションを形成する手順を示したフローチャート。

【図１０】セキュアなセッションを形成する過程で行われる一方向性関数の処理を示した図。

【図１１】取得したコンテンツのファイルフォーマットの一例を示した図。

【図１２】パーソナルコンピュータで記憶しているコンテンツを携帯端末にインポートするときの手順を示したフローチャート。

【図１３】携帯端末にインポートするために変換されたコンテンツファイルの一例を示す図。

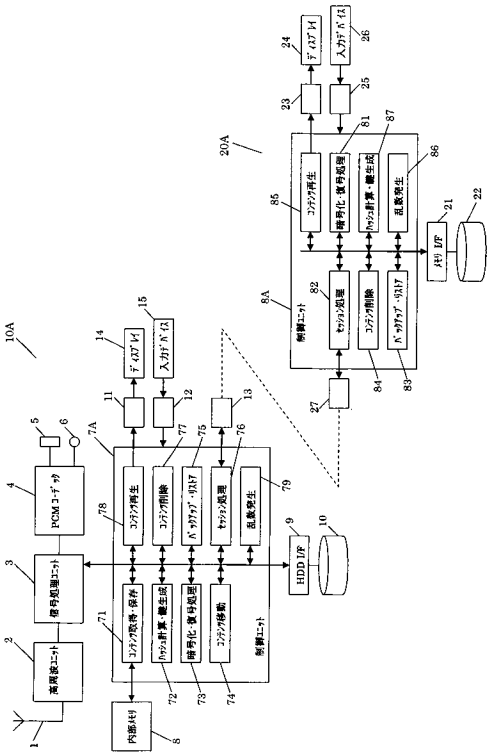
【図１４】パーソナルコンピュータから携帯端末にインポートしたコンテンツを再生するときの手順を示したフローチャート。

【符号の説明】

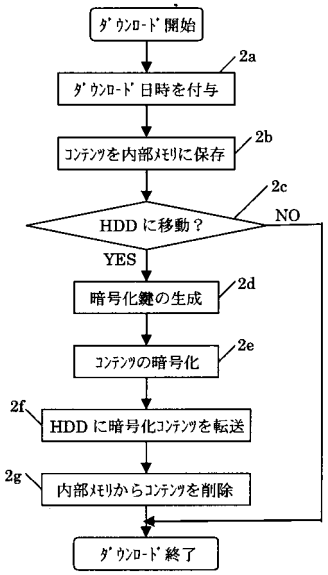
【０１１３】

１・・・アンテナ、２・・・高周波ユニット、３・・・信号処理ユニット、４・・・ＰＣＭコーデック、５・・・スピーカ、６・・・マイク、７Ａ，８Ａ・・・制御ユニット、８・・・内部メモリ、９・・・
ＨＤＤＩ／Ｆ、１０・・・ハードディスク（ＨＤＤ）、１１，２３・・・表示Ｉ／Ｆ、１２，２５・・・入力Ｉ／Ｆ、１３，２７・・・外部Ｉ／Ｆ、１４，２４・・・ディスプレイ、１５，２６・・・入力デバイス、２１・・・メモリＩ／Ｆ、２２・・・メモリ、７１・・・コンテンツ取得・保存
機能、７２，８７・・・ハッシュ計算・鍵生成機能、７３，８１・・・暗号化・復号処理機能、７４・・・コンテンツ移動処理機能、７５，８３・・・バックアップ・リストア機能、７６，８２・・・セッション処理機能、７７，８４・・・コンテンツ削除機能、７８，８５・・・コンテン
ツ再生処理機能、７９，８６・・・乱数発生機能。

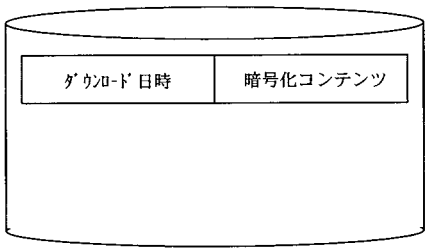
【図１】



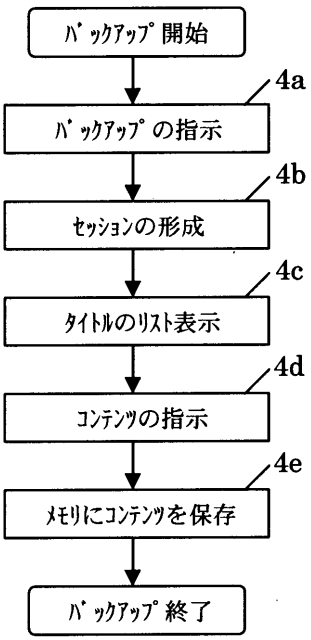
【図２】


ダウンロード開始
2a
ダウンロード日時を付与
2b
コンテンツを内部メモリに保存
2c
HDD に移動？
NO
YES
2d
暗号化鍵の生成
2e
コンテンツの暗号化
2f
HDD に暗号化コンテンツを転送
2g
内部メモリからコンテンツを削除
ダウンロード終了

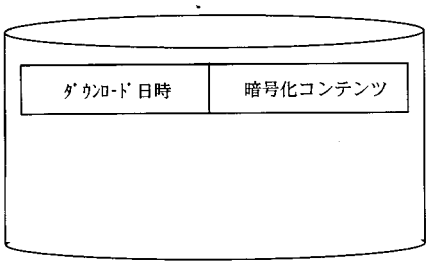
【図３】


ダウンロード日時
暗号化コンテンツ

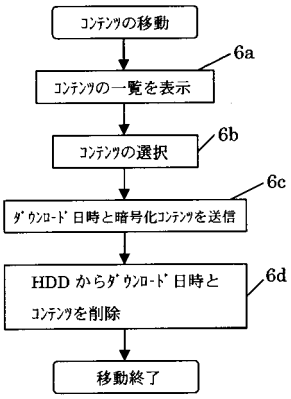
【図４】


バックアップ開始
4a
バックアップの指示
4b
セッションの形成
4c
タイトルのリスト表示
4d
コンテンツの指示
4e
メモリにコンテンツを保存
バックアップ終了

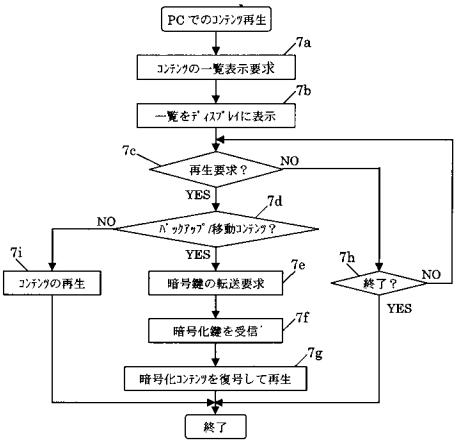
【図５】


ﾀﾞｳﾝﾛｰﾄﾞ日時
暗号化コンテンツ

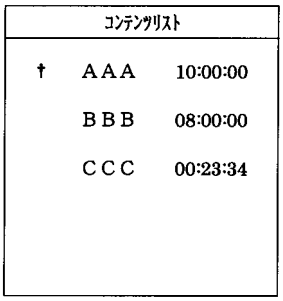
【図６】


ｺﾝﾃﾝﾂの移動
6a
ｺﾝﾃﾝﾂの一覧を表示
6b
ｺﾝﾃﾝﾂの選択
6c
ﾀﾞｳﾝﾛｰﾄﾞ日時と暗号化ｺﾝﾃﾝﾂを送信
HDD からﾀﾞｳﾝﾛｰﾄﾞ日時と
ｺﾝﾃﾝﾂを削除
6d
移動終了

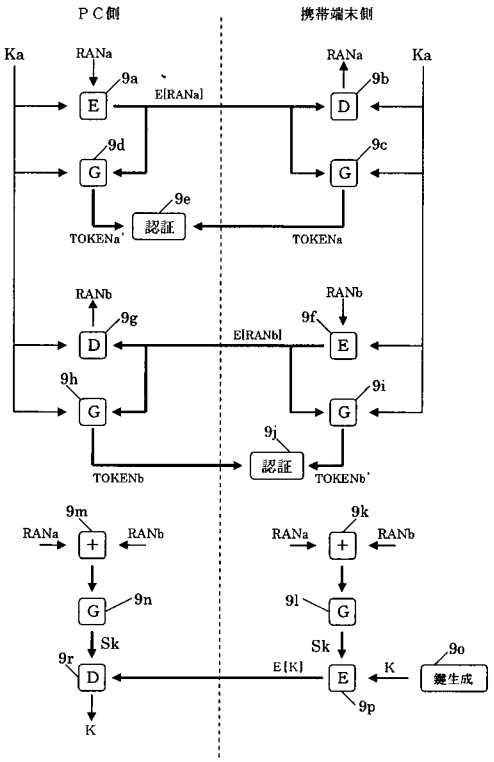
【図７】


PC でのｺﾝﾃﾝﾂ再生
7a
ｺﾝﾃﾝﾂの一覧表示要求
7b
一覧をﾃﾞｨｽﾌﾟﾚｲに表示
7c
再生要求？
NO
YES
7d
ﾊﾞｯｸｱｯﾌﾟ/移動ｺﾝﾃﾝﾂ？
NO
YES
7i
ｺﾝﾃﾝﾂの再生
暗号鍵の転送要求
7e
7h
終了？
NO
YES
暗号化鍵を受信
7f
暗号化ｺﾝﾃﾝﾂを復号して再生
7g
終了

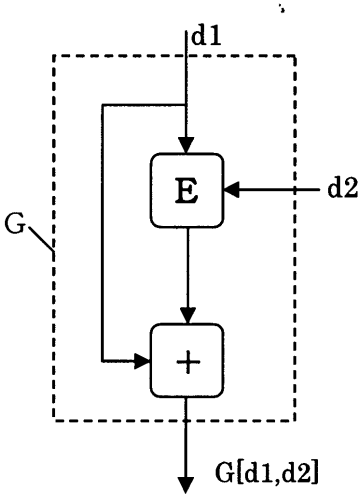
【図８】


ｺﾝﾃﾝﾂﾘｽﾄ
AAA 10:00:00
BBB 08:00:00
CCC 00:23:34

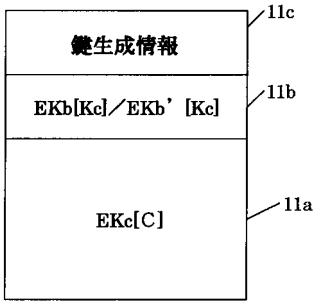
【図９】



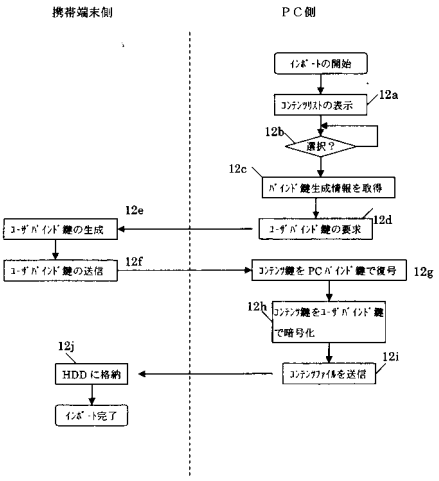
【図１０】



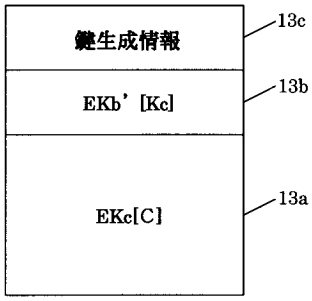
【図１１】



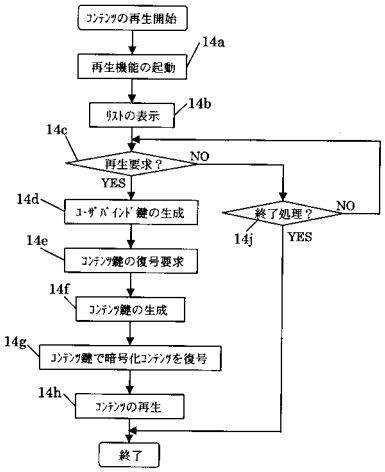
【図１２】



【図１３】



【図１４】



【手続補正書】
【提出日】平成18年7月5日(2006.7.5)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ダウンロードしたコンテンツを第１の鍵を用いて暗号化する第１の暗号化手段と、
自端末に割当てられた識別情報を記憶する第１の記憶手段と、
前記暗号化手段によって暗号化された暗号化コンテンツと、コンテンツのダウンロード日時とを対応付けて記憶する第２の記憶手段と、
前記識別情報と前記ダウンロード日時とを用いて第２の鍵を生成する鍵生成手段と、
この生成された第２の鍵を用いて前記第１の鍵を暗号化する第２の暗号化手段と、
外部機器との間でデータの送受信を行う送受信手段と、
前記暗号化コンテンツ、前記暗号化された第１の鍵、および前記ダウンロード日時とを対応付けて外部機器に移動させるコンテンツ移動手段とを有し、
前記送受信手段を介して外部機器からダウンロード日時を含む鍵生成要求を受信すると、
前記鍵生成手段は、この要求に含まれる前記ダウンロード日時と前記第１の記憶手段に記憶されている識別情報とを用いて第２の鍵を生成し、
前記送受信手段は、前記鍵生成手段によって生成された第２の鍵を前記外部機器に対して送信することを特徴とする情報端末装置。
【請求項２】

ダウンロードしたコンテンツを第１の鍵を用いて暗号化する第１の暗号化手段と、
自端末に割当てられた通信に利用する識別情報を記憶する第１の記憶手段と、
前記暗号化手段によって暗号化された暗号化コンテンツと、コンテンツのダウンロード日時とを対応付けて記憶する第２の記憶手段と、
前記識別情報と前記ダウンロード日時とを用いて第２の鍵を生成する鍵生成手段と、
この生成された第２の鍵を用いて前記第１の鍵を暗号化する第２の暗号化手段と、
外部機器との間でデータの送受信を行う送受信手段と、
前記暗号化コンテンツ、前記暗号化された第１の鍵、および前記ダウンロード日時とを対応付けて外部機器に移動させるコンテンツ移動手段とを有し、
前記送受信手段を介して外部機器からダウンロード日時を含む鍵生成要求を受信すると、
前記鍵生成手段は、この要求に含まれる前記ダウンロード日時と前記第１の記憶手段に記憶されている識別情報とを用いて第２の鍵を生成し、
前記送受信手段は、前記鍵生成手段によって生成された第２の鍵を前記外部機器に対して送信することを特徴とする情報端末装置。

【請求項３】
ダウンロードしたコンテンツを第１の鍵を用いて暗号化する第１の暗号化手段と、
自端末に割当てられた電話番号を記憶する第１の記憶手段と、
前記暗号化手段によって暗号化された暗号化コンテンツと、コンテンツのダウンロード日時とを対応付けて記憶する第２の記憶手段と、
前記電話番号と前記ダウンロード日時とを用いて第２の鍵を生成する鍵生成手段と、
この生成された第２の鍵を用いて前記第１の鍵を暗号化する第２の暗号化手段と、
外部機器との間でデータの送受信を行う送受信手段と、
前記暗号化コンテンツ、前記暗号化された第１の鍵、および前記ダウンロード日時とを対応付けて外部機器に移動させるコンテンツ移動手段とを有し、
前記送受信手段を介して外部機器からダウンロード日時を含む鍵生成要求を受信すると、
前記鍵生成手段は、この要求に含まれる前記ダウンロード日時と前記第１の記憶手段に記憶されている電話番号とを用いて第２の鍵を生成し、
前記送受信手段は、前記鍵生成手段によって生成された第２の鍵を前記外部機器に対して送信することを特徴とする情報端末装置。

【請求項４】
認証処理手段を更に有し、この認証処理手段は、前記送受信手段が前記外部機器から受信した鍵生成要求に基づいて生成された前記第２の鍵を該外部機器へ送信する前に、該外部機器との間で認証処理を実行することを特徴とする請求項１、２、または３に記載の情報端末装置。

【請求項５】
コンテンツを第１の鍵を用いて暗号化する第１の暗号化手段と、
自端末に割当てられた電話番号を記憶する第１の記憶手段と、
前記暗号化手段によって暗号化された暗号化コンテンツと、コンテンツのダウンロード日時とを対応付けて記憶する第２の記憶手段と、
前記電話番号と前記ダウンロード日時とを用いて第２の鍵を生成する鍵生成手段と、
この生成された第２の鍵を用いて前記第１の鍵を暗号化する第２の暗号化手段と、
外部機器との間でデータの送受信を行う送受信手段と、
前記暗号化コンテンツ、前記暗号化された第１の鍵、および前記ダウンロード日時とを対応付けて外部機器に移動させるコンテンツ移動手段とを有し、
前記送受信手段を介して外部機器からダウンロード日時を含む鍵生成要求を受信すると、
前記鍵生成手段は、この要求に含まれる前記ダウンロード日時と前記第１の記憶手段に記憶されている電話番号とを用いて第２の鍵を生成し、

前記送受信手段は、前記鍵生成手段によって生成された第２の鍵を前記外部機器に対して送信することを特徴とする情報端末装置。
【請求項６】
ダウンロードしたコンテンツを第１の鍵を用いて暗号化する第１の暗号化手段と、
自端末に割当てられた電話番号を記憶する第１の記憶手段と、
前記暗号化手段によって暗号化された暗号化コンテンツと、コンテンツのダウンロード日時とを対応付けて記憶する第２の記憶手段と、
少なくとも前記電話番号と前記ダウンロード日時とを含む鍵生成情報を用いて第２の鍵を生成する鍵生成手段と、
この生成された第２の鍵を用いて前記第１の鍵を暗号化する第２の暗号化手段と、
外部機器との間でデータの送受信を行う送受信手段と、
前記暗号化コンテンツ、前記暗号化された第１の鍵、および前記電話番号を除いた鍵生成情報とを対応付けて外部機器に移動させるコンテンツ移動手段とを有し、
前記送受信手段を介して外部機器から前記電話番号を除いた鍵生成情報を含む鍵生成要求を受信すると、
前記鍵生成手段は、この要求に含まれる前記電話番号を除いた鍵精製情報と前記第１の記憶手段に記憶されている電話番号とを用いて第２の鍵を生成し、
前記送受信手段は、前記鍵生成手段によって生成された第２の鍵を前記外部機器に対して送信することを特徴とする情報端末装置。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００１１
【補正方法】変更
【補正の内容】
【００１１】
上記目的を達成するために、この発明に係わる情報端末装置では、ダウンロードしたコンテンツを第１の鍵を用いて暗号化する第１の暗号化手段と、自端末に割当てられた識別情報を記憶する第１の記憶手段と、前記暗号化手段によって暗号化された暗号化コンテンツと、コンテンツのダウンロード日時とを対応付けて記憶する第２の記憶手段と、前記識別情報と前記ダウンロード日時とを用いて第２の鍵を生成する鍵生成手段と、この生成された第２の鍵を用いて前記第１の鍵を暗号化する第２の暗号化手段と、外部機器との間でデータの送受信を行う送受信手段と、前記暗号化コンテンツ、前記暗号化された第１の鍵、および前記ダウンロード日時とを対応付けて外部機器に移動させるコンテンツ移動手段とを有し、前記送受信手段を介して外部機器からダウンロード日時を含む鍵生成要求を受信すると、記鍵生成手段は、この要求に含まれる前記ダウンロード日時と前記第１の記憶手段に記憶されている識別情報とを用いて第２の鍵を生成し、前記送受信手段は、前記鍵生成手段によって生成された第２の鍵を前記外部機器に対して送信することを特徴としている。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００１２
【補正方法】削除
【補正の内容】
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００１３
【補正方法】変更
【補正の内容】
【００１３】
この発明では、携帯端末で取得したコンテンツを他の機器にバックアップや移動を行っ

た際、コンテンツが制限なく利用されるのを防止しつつ、バックアップや移動先の機器でもコンテンツを利用することを可能とする。

【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００１４
【補正方法】削除
【補正の内容】

フロントページの続き

Ｆターム(参考) 5C164 FA08 PA04 PA21 SC02P TA06P UC22P
5J104 AA12 AA16 EA04 EA15 EA16 JA03 NA02 NA37