

(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2006-269055

(P2006-269055A)

(43) 公開日 平成18年10月5日(2006.10.5)

(51) Int.C1.		F 1	テーマコード (参考)	
G 1 1 B	20/10	(2006.01)	G 1 1 B	20/10 H 5 B 0 1 7
HO 4 N	5/765	(2006.01)	HO 4 N	5/91 L 5 C 0 5 3
HO 4 N	5/781	(2006.01)	HO 4 N	5/781 5 1 O Z 5 C 1 6 4
HO 4 N	7/173	(2006.01)	HO 4 N	7/173 6 3 O 5 D 0 4 4
GO 6 F	21/24	(2006.01)	G 1 1 B	20/10 D

審査請求 未請求 請求項の数 12 O L 外国語出願 (全 87 頁) 最終頁に続く

(21) 出願番号	特願2006-77577 (P2006-77577)	(71) 出願人	50218642 マーベル ワールド トレード リミテッド
(22) 出願日	平成18年3月20日 (2006.3.20)		バルバドス国 ビービー 14027, セントマイケル、ブリトンズ ヒル、ガンサイ
(31) 優先権主張番号	11/085, 761		トロード、エル ホライズン
(32) 優先日	平成17年3月21日 (2005.3.21)	(74) 代理人	100104156 弁理士 龍華 明裕
(33) 優先権主張国	米国 (US)	(72) 発明者	サハット スタルジャ アメリカ合衆国、94022 カリフォルニア州、ロス アルトス ヒルズ、エレナ ロード 27330
(31) 優先権主張番号	11/174, 176		
(32) 優先日	平成17年7月1日 (2005.7.1)		
(33) 優先権主張国	米国 (US)		
			F ターム (参考) 5B017 AA07 BA07 BA08 BB10 CA07 CA15

最終頁に続く

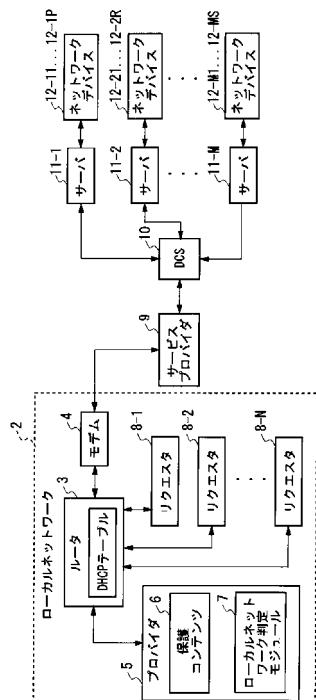
(54) 【発明の名称】保護コンテンツ配信ハードディスクドライブシステム

(57) 【要約】

【課題】ネットワークによってプロバイダネットワークデバイスと通信するハードディスクドライブ(HDD)システムを提供する。

【解決手段】ハードディスクドライブ(HDD)システムは、不揮発的な方法でユーザアクセス可能セクション及び隠しセクションにデータを記憶する不揮発性HDDメモリを備える。ハードディスクドライブ(HDD)制御モジュールは、HDD不揮発性メモリと通信し、プロバイダネットワークデバイスにコンテンツを選択的に要求してプロバイダネットワークデバイスからコンテンツを受信し、且つ、要求されたコンテンツを不揮発性HDDメモリの隠しセクションに記憶する。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

ネットワークによってプロバイダネットワークデバイスと通信するハードディスクドライブ(HDD)システムであって

不揮発的な方法でユーザアクセス可能セクション及び隠しセクションにデータを記憶する不揮発性HDDメモリと、

前記HDD不揮発性メモリと通信し、前記プロバイダネットワークデバイスにコンテンツを選択的に要求して前記プロバイダネットワークデバイスからコンテンツを受信し、且つ、前記要求されたコンテンツを前記不揮発性HDDメモリの前記隠しセクションに記憶する、ハードディスクドライブ(HDD)制御モジュールと、
を備える、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項 2】

前記要求を前記プロバイダネットワークデバイスへ送信した後、前記HDD制御モジュールは、鍵要求を受信し、該鍵要求に応答して、前記プロバイダネットワークデバイスへ鍵を送信する、請求項1に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項 3】

前記プロバイダネットワークデバイスから前記HDDシステムによって受信された、前記要求されたコンテンツは、前記鍵を使用して暗号化される、請求項2に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項 4】

前記HDD制御モジュールは、前記要求されたコンテンツを解読する、請求項3に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項 5】

前記要求されたコンテンツは、同じく前記不揮発性HDDメモリの前記隠し部分に書き込まれる使用量データを含み、前記HDD制御モジュールは、前記使用量データが、許可された使用を超過したことを示すと、前記要求されたコンテンツを利用不能にする、請求項1に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項 6】

前記HDDシステムは、前記要求されたコンテンツを前記不揮発性HDDメモリから消去する、請求項5に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項 7】

前記使用量データは、許可された所定の使用回数を指定する、請求項5に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項 8】

前記使用量データは、許可された使用期間を指定する、請求項5に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項 9】

前記HDDシステムは、前記ネットワークと無線で通信する、請求項1に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項 10】

前記HDDシステムは、媒体によって前記ネットワークと通信する、請求項1に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項 11】

前記プロバイダネットワークデバイスは、デジタル多用途ディスク(DVD)システムを含む、請求項1に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項 1 2】

請求項 1 1 に記載の前記 H D D システムを備え、前記 D V D システム及び前記ネットワークをさらに備える、ネットワーク接続された D V D / H D D システム。

【請求項 1 3】

ネットワークによってプロバイダネットワークデバイスと通信するハードディスクドライブ (H D D) システムであって、

不揮発的な方法で、ユーザアクセス可能セクション及び隠しセクションにデータを記憶するための不揮発性メモリ手段と、

前記不揮発性メモリ手段と通信し、前記プロバイダネットワークデバイスにコンテンツを選択的に要求して前記プロバイダネットワークデバイスからコンテンツを受信し、且つ、前記要求されたコンテンツを前記不揮発性メモリ手段の前記隠しセクションに記憶するための制御手段と、

を備える、ネットワークによってプロバイダネットワークデバイスと通信する H D D システム。

【請求項 1 4】

前記要求を前記プロバイダネットワークデバイスへ送信した後、前記制御手段は、鍵要求を受信し、該鍵要求に応答して、前記プロバイダネットワークデバイスへ鍵を送信する、請求項 1 3 に記載の、ネットワークによってプロバイダネットワークデバイスと通信する H D D システム。

【請求項 1 5】

前記プロバイダネットワークデバイスから前記システムによって受信された、前記要求されたコンテンツは、前記鍵を使用して暗号化される、請求項 1 4 に記載の、ネットワークによってプロバイダネットワークデバイスと通信する H D D システム。

【請求項 1 6】

前記制御手段は、前記要求されたコンテンツを解読する、請求項 1 5 に記載の、ネットワークによってプロバイダネットワークデバイスと通信する H D D システム。

【請求項 1 7】

前記要求されたコンテンツは、同じく前記不揮発性メモリ手段の前記隠し部分に書き込まれる使用量データを含み、前記制御手段は、前記使用量データが、許可された使用を超過したことを示すと、前記要求されたコンテンツを利用不能にする、請求項 1 3 に記載の、ネットワークによってプロバイダネットワークデバイスと通信する H D D システム。

【請求項 1 8】

前記システムは、前記要求されたコンテンツを前記不揮発性メモリ手段から消去する、請求項 1 7 に記載の、ネットワークによってプロバイダネットワークデバイスと通信する H D D システム。

【請求項 1 9】

前記使用量データは、許可された所定の使用回数を指定する、請求項 1 7 に記載の、ネットワークによってプロバイダネットワークデバイスと通信する H D D システム。

【請求項 2 0】

前記使用量データは、許可された使用期間を指定する、請求項 1 7 に記載の、ネットワークによってプロバイダネットワークデバイスと通信する H D D システム。

【請求項 2 1】

前記 H D D システムは、前記ネットワークと無線で通信する、請求項 1 3 に記載の、ネットワークによってプロバイダネットワークデバイスと通信する H D D システム。

【請求項 2 2】

前記 H D D システムは、媒体によって前記ネットワークと通信する、請求項 1 3 に記載の、ネットワークによってプロバイダネットワークデバイスと通信する H D D システム。

【請求項 2 3】

前記プロバイダネットワークデバイスは、デジタル多用途ディスク (D V D) システムを含む、請求項 1 3 に記載の、ネットワークによってプロバイダネットワークデバイスと

10

20

30

40

50

通信する HDD システム。

【請求項 24】

請求項 23 に記載の前記 HDD システムを備え、前記 DVD システム及び前記ネットワークをさらに備える、ネットワーク接続された DVD / HDD システム。

【請求項 25】

ネットワークによってプロバイダネットワークデバイスと通信するハードディスクドライブ (HDD) システムを動作させる方法であって、

ユーザアクセス可能セクション及び隠しセクションに不揮発的な方法でデータを記憶すること、

前記プロバイダネットワークデバイスにコンテンツを選択的に要求して前記プロバイダネットワークデバイスからコンテンツを受信すること、及び 10

前記要求されたコンテンツを前記隠しセクションに記憶すること、を含む、ネットワークによってプロバイダネットワークデバイスと通信する HDD システムを動作させる方法。

【請求項 26】

鍵要求を受信すること、及び該要求を前記プロバイダネットワークデバイスへ送信した後に、前記鍵要求に応答して、前記プロバイダネットワークデバイスへ鍵を送信すること、をさらに含む、請求項 25 に記載の、ネットワークによってプロバイダネットワークデバイスと通信する HDD システムを動作させる方法。

【請求項 27】

前記プロバイダネットワークデバイスから前記 HDD システムによって受信された、前記要求されたコンテンツを、前記鍵を使用して暗号化すること、をさらに含む、請求項 26 に記載の、ネットワークによってプロバイダネットワークデバイスと通信する HDD システムを動作させる方法。

【請求項 28】

前記要求されたコンテンツを解読すること、をさらに含む、請求項 27 に記載の、ネットワークによってプロバイダネットワークデバイスと通信する HDD システムを動作させる方法。

【請求項 29】

使用量データを含む要求されたコンテンツを前記隠し部分に書き込むこと、及び 30
前記使用量データが、許可された使用を超えたことを示すと、前記要求されたコンテンツを利用不能にすること、をさらに含む、請求項 25 に記載の、ネットワークによってプロバイダネットワークデバイスと通信する HDD システムを動作させる方法。

【請求項 30】

前記要求されたコンテンツを前記隠しセクションから消去すること、をさらに含む、請求項 29 に記載の、ネットワークによってプロバイダネットワークデバイスと通信する HDD システムを動作させる方法。

【請求項 31】

前記使用量データを使用して、許可された所定の使用回数を指定すること、をさらに含む、請求項 29 に記載の、ネットワークによってプロバイダネットワークデバイスと通信する HDD システムを動作させる方法。 40

【請求項 32】

前記使用量データを使用して、許可された使用期間を指定すること、をさらに含む、請求項 27 に記載の、ネットワークによってプロバイダネットワークデバイスと通信する HDD システムを動作させる方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ネットワークに関し、より詳細には、保護コンテンツの安全な配信を可能に 50

するネットワークシステムに関する。

【0002】

この出願は、2005年3月21日に出願された、米国特許出願第11/085,761号の継続出願である。この出願は、2005年1月19日に出願された米国特許出願第11/039,288号に関連する。上記出願の開示は、参照によりその全内容が本明細書に援用される。

【背景技術】

【0003】

顧客はしばしば、デジタル多用途ディスク（DVD）のビデオコンテンツを購入する。DVDプレイヤは、テレビ（TV）又は他のビデオモニタにビデオコンテンツを出力するのに使用することができる。DVDプレイヤの中には、複数のDVDのうちの1つを選択して再生することを可能にするための回転トレーを含むことができるものがある。場合によつては、顧客がその顧客の家の或る部屋の第1のTVでDVDコンテンツを見たいときに、DVDプレイヤが別の部屋に位置し、その別の部屋の第2のTVに接続されている場合がある。その結果、DVDプレイヤを第2のTVから切り離して、第1のTVのある部屋へ移動させ、第1のTVに再び接続する必要がある。或いは、顧客が第2のDVDプレイヤを有する場合、顧客は、DVDをその他の方のプレイヤへ移動させる。

【0004】

この問題に対する1つの可能な解決法は、DVDコンテンツを別のDVDにコピーすることを含む。DVDプレイヤは、通常、1つのDVDプレイヤしか含まず、これが、DVDのコピーを難しくしている。DVDをコピーするには、ユーザは、DVDコンテンツをハードドライブシステムにコピーしなければならない。通常、デジタル著作権管理（DRM）等のコピープロテクト方式は、一部のコピーが著作権法の下で保護されている場合があるにもかかわらず、このようなコピーを阻止する。これは、一部には、データがDVDプレイヤによって解読及び/又は復号され、したがって、データが他のデバイスへ出力される時に非保護形式になることに起因している。この解決法も、追加DVDプレイヤを必要とする。

【発明の開示】

【課題を解決するための手段】

【0005】

ネットワークにおいてコンテンツを配信するためのシステムは、コンテンツを記憶するメモリを備える。プロバイダネットワークデバイスが、このメモリと通信する。リクエスタネットワークデバイスが、コンテンツのコピーを要求する。プロバイダネットワークデバイスは、リクエスタネットワークデバイスのローカル/リモートステータスを判断し、リクエスタネットワークデバイスがコンテンツを要求し、且つ、ローカルステータスを有する場合に、コンテンツのコピーをリクエスタネットワークデバイスへ選択的に送信する。

【0006】

他の特徴では、プロバイダネットワークデバイスは、デジタル多用途ディスク（DVD）システムを含む。リクエスタネットワークデバイスは、ハードディスクドライブ（HDD）システムを含む。プロバイダネットワークデバイスは、リクエスタネットワークデバイスのローカル/リモートステータスを判断するローカルネットワーク判断モジュールを含む。プロバイダネットワークデバイスは、リクエスタネットワークデバイスの応答時間に基づいて、ローカル/リモートステータスを判断する。

【0007】

他の特徴では、サーバが、プロバイダネットワークデバイスと通信し、ローカルネットワークデバイスの識別データを記憶する。プロバイダネットワークデバイスは、識別データに基づいてローカル/リモートステータスを判断する。識別データは、ローカルネットワークデバイスの媒体アクセス制御（MAC）アドレスを含む。

【0008】

10

20

30

40

50

他の特徴では、HDDシステムは、不揮発的な方法でデータを記憶し、ユーザアクセス可能セクション及び隠しセクションを含む、不揮発性HDDメモリを備える。ハードディスクドライブ(HDD)制御モジュールが、このHDD不揮発性メモリと通信し、プロバイダネットワークデバイスにコンテンツを選択的に要求してプロバイダネットワークデバイスからコンテンツを受信し、要求されたコンテンツを不揮発性HDDメモリの隠しセクションに記憶する。

【0009】

他の特徴では、要求をプロバイダネットワークデバイスへ送信した後、HDD制御モジュールは、鍵要求を受信し、この鍵要求に応答して、プロバイダネットワークデバイスへ鍵を送信する。プロバイダネットワークデバイスからHDDシステムによって受信された、要求されたコンテンツは、鍵を使用して暗号化される。HDD制御モジュールは、要求されたコンテンツを解読する。要求されたコンテンツは、同じく不揮発性HDDメモリの隠し部分に書き込まれる使用量データを含み、HDD制御モジュールは、使用量データが、許可された使用を超過したことを示すと、要求されたコンテンツを利用不能にする。HDDシステムは、要求されたコンテンツを不揮発性HDDメモリから消去する。使用量データは、許可された所定の使用回数を指定する。使用量データは、許可された使用期間を指定する。HDDシステムは、ネットワークと無線で通信する。HDDシステムは、有線媒体によってネットワークと通信する。

【0010】

他の特徴では、DVDシステムは、コンテンツを記憶する不揮発性メモリを備える。DVD制御モジュールが、この不揮発性メモリと通信し、リクエスタネットワークデバイスからコンテンツの要求を選択的に受信する。DVD制御モジュールは、要求されたコンテンツを送信する前に、リクエスタネットワークデバイスに鍵を要求し、この鍵要求をHDDシステムへ送信した後に、HDDシステムから鍵を受信するのに必要な時間を求める。鍵が所定の期間内に受信された場合に、DVDシステムは、要求されたコンテンツをHDDシステムへ送信する。この所定の期間は单一ホップ期間又は2ホップ期間にほぼ等しい。DVDシステムは、要求されたコンテンツをHDDシステムへ送信する前に、要求されたコンテンツを暗号化する。DVD制御モジュールは、HDDシステムへ送信される、要求されたコンテンツに、使用量データを含める。使用量データは、許可された使用回数を指定する。使用量データは、許可された使用期間を指定する。

【0011】

ネットワークにおいてコンテンツを配信するためのシステムは、コンテンツを記憶するためのメモリ手段を備える。プロバイダネットワーク手段が、このメモリ手段との通信を提供する。リクエスタネットワーク手段が、コンテンツのコピーを要求する。プロバイダネットワーク手段は、リクエスタネットワーク手段のローカル/リモートステータスを判断し、リクエスタネットワーク手段がコンテンツを要求し、且つ、ローカルステータスを有する場合に、コンテンツのコピーをリクエスタネットワーク手段へ選択的に送信する。

【0012】

他の特徴では、プロバイダネットワーク手段は、デジタル多用途ディスク(DVD)システムを含む。リクエスタネットワーク手段は、ハードディスクドライブ(HDD)システムを含む。プロバイダネットワーク手段は、リクエスタネットワーク手段のローカル/リモートステータスを判断するためのローカルネットワーク判断手段を含む。プロバイダネットワーク手段は、リクエスタネットワーク手段の応答時間に基づいて、ローカル/リモートステータスを判断する。サーバ手段が、プロバイダネットワーク手段との通信を受け持ち、ローカルネットワーク手段の識別データを記憶する。プロバイダネットワーク手段は、識別データに基づいてローカル/リモートステータスを判断する。識別データは、ローカルネットワーク手段の媒体アクセス制御(MAC)アドレスを含む。

【0013】

他の特徴では、HDDシステムは、不揮発的な方法でデータを記憶し、ユーザアクセス可能セクション及び隠しセクションを含む、不揮発性HDDメモリ手段を備える。ハード

10

20

30

40

50

ディスクドライブ(HDD)制御手段が、このHDD不揮発性メモリ手段と通信し、プロバイダネットワーク手段にコンテンツを選択的に要求してプロバイダネットワーク手段からコンテンツを受信し、要求されたコンテンツを不揮発性HDDメモリ手段の隠しセクションに記憶する。要求をプロバイダネットワーク手段へ送信した後、HDD制御手段は、鍵要求を受信し、この鍵要求に応答して、プロバイダネットワーク手段へ鍵を送信する。プロバイダネットワーク手段からHDDシステムによって受信された、要求されたコンテンツは、鍵を使用して暗号化される。HDD制御手段は、要求されたコンテンツを解読する。要求されたコンテンツは、同じく不揮発性HDDメモリ手段の隠し部分に書き込まれる使用量データを含み、HDD制御手段は、使用量データが、許可された使用を超過したことを示すと、要求されたコンテンツを利用不能にする。

10

【 0 0 1 4 】

他の特徴では、HDDシステムは、要求されたコンテンツを不揮発性HDDメモリ手段から消去する。使用量データは、許可された所定の使用回数を指定する。使用量データは、許可された使用期間を指定する。HDDシステムは、ネットワークと無線で通信する。HDDシステムは、有線媒体によってネットワークと通信する。

【 0 0 1 5 】

他の特徴では、DVDシステムは、コンテンツを記憶するための不揮発性メモリ手段を備える。DVD制御手段が、この不揮発性メモリ手段と通信し、リクエスタネットワーク手段からコンテンツの要求を選択的に受信する。DVD制御手段は、要求されたコンテンツを送信する前に、リクエスタネットワーク手段に鍵を要求し、この鍵要求をHDDシステムへ送信した後に、HDDシステムから鍵を受信するのに必要な時間を求める。鍵が所定の期間内に受信された場合に、DVD制御手段は、要求されたコンテンツをHDDシステムへ送信する。この所定の期間は単一ホップ期間又は2ホップ期間にほぼ等しい。DVD制御手段は、要求されたコンテンツをHDDシステムへ送信する前に、要求されたコンテンツを暗号化する。DVD制御手段は、HDDシステムへ送信される、要求されたコンテンツに、使用量データを含める。使用量データは、許可された使用回数を指定する。使用量データは、許可された使用期間を指定する。DVDシステムは、ネットワークと無線で通信する。DVDシステムは、有線媒体によってネットワークと通信する。

20

【 0 0 1 6 】

ネットワークにおいてコンテンツを配信するための方法は、メモリにコンテンツを記憶すること、このメモリと通信するプロバイダネットワークデバイスを設けること、コンテンツのコピーを要求するリクエスタネットワークデバイスを設けること、リクエスタネットワークデバイスのローカル／リモートステータスを判断すること、及び、リクエスタネットワークデバイスがコンテンツを要求し、且つ、ローカルステータスを有する場合に、コンテンツのコピーをリクエスタネットワークデバイスへ選択的に送信すること、を含む。

30

【 0 0 1 7 】

他の特徴では、プロバイダネットワークデバイスは、デジタル多用途ディスク(DVD)システムを含む。リクエスタネットワークデバイスは、ハードディスクドライブ(HDD)システムを含む。この方法は、リクエスタネットワークデバイスのローカル／リモートステータスを判断することを含む。この方法は、リクエスタネットワークデバイスの応答時間に基づいて、ローカル／リモートステータスを判断することを含む。この方法は、ローカルネットワークデバイスの識別データを記憶することを含み、プロバイダネットワークデバイスは、この識別データに基づいてローカル／リモートステータスを判断する。この方法は、ローカルネットワークデバイスの媒体アクセス制御(MAC)アドレスを記憶することを含む。この方法は、HDDシステムのユーザアクセス可能セクション及び隠しセクションに不揮発的な方法でデータを記憶すること、プロバイダネットワークデバイスにコンテンツを選択的に要求してプロバイダネットワークデバイスからコンテンツを受信すること、及び、要求されたコンテンツを不揮発性HDDメモリの隠しセクションに記憶すること、を含む。

40

50

【0018】

他の特徴では、この方法は、鍵要求を受信すること、及び、この要求をプロバイダネットワークデバイスへ送信した後、この鍵要求に応答して、プロバイダネットワークデバイスへ鍵を送信すること、を含む。この方法は、プロバイダネットワークデバイスからHDDシステムによって受信された、要求されたコンテンツを、鍵を使用して暗号化することを含む。この方法は、要求されたコンテンツを解読することを含む。この方法は、使用量データを含む要求されたコンテンツを、不揮発性HDDメモリの隠し部分に書き込むこと、及び、使用量データが、許可された使用を超過したことを示すと、要求されたコンテンツを利用不能にすること、を含む。

【0019】

10
さらに他の特徴では、この方法は、要求されたコンテンツを不揮発性HDDメモリから消去することを含む。この方法は、使用量データを使用して、許可された所定の使用回数を指定することを含む。この方法は、使用量データを使用して、許可された使用期間を指定することを含む。この方法は、コンテンツを記憶すること、及び、リクエスタネットワークデバイスからコンテンツの要求を選択的に受信すること、を含む。この方法は、要求されたコンテンツを送信する前に、リクエスタネットワークデバイスに鍵を要求すること、及び、この鍵要求をHDDシステムへ送信した後に、HDDシステムから鍵を受信するのに必要な時間を求めること、を含む。

【0020】

20
他の特徴では、この方法は、鍵が所定の期間内に受信された場合に、要求されたコンテンツをHDDシステムへ送信することを含む。この所定の期間は単一ホップ期間又は2ホップ期間にほぼ等しい。この方法は、要求されたコンテンツをHDDシステムへ送信する前に、要求されたコンテンツを暗号化することを含む。この方法は、要求されたコンテンツ内の使用量データをHDDシステムへ送信することを含む。使用量データは、許可された使用回数を指定する。使用量データは、許可された使用期間を指定する。

【0021】

ネットワークによってプロバイダネットワークデバイスと通信するハードディスクドライブ(HDD)システムは、不揮発的な方法で、ユーザアクセス可能セクション及び隠しセクションにデータを記憶する不揮発性HDDメモリを備える。ハードディスクドライブ(HDD)制御モジュールが、このHDD不揮発性メモリと通信し、プロバイダネットワークデバイスにコンテンツを選択的に要求してプロバイダネットワークデバイスからコンテンツを受信し、要求されたコンテンツを不揮発性HDDメモリの隠しセクションに記憶する。

【0022】

30
他の特徴では、要求をプロバイダネットワークデバイスへ送信した後、HDD制御モジュールは、鍵要求を受信し、この鍵要求に応答して、プロバイダネットワークデバイスへ鍵を送信する。プロバイダネットワークデバイスからHDDシステムによって受信された、要求されたコンテンツは、鍵を使用して暗号化される。HDD制御モジュールは、要求されたコンテンツを解読する。要求されたコンテンツは、同じく不揮発性HDDメモリの隠し部分に書き込まれる使用量データを含み、HDD制御モジュールは、使用量データが、許可された使用を超過したことを示すと、要求されたコンテンツを利用不能にする。HDDシステムは、要求されたコンテンツを不揮発性HDDメモリから消去する。使用量データは、許可された所定の使用回数を指定する。使用量データは、許可された使用期間を指定する。HDDシステムは、ネットワークと無線で通信する。HDDシステムは、媒体によってネットワークと通信する。

【0023】

40
他の特徴では、プロバイダネットワークデバイスは、デジタル多用途ディスク(DVD)システムを含む。ネットワーク接続されたDVD/HDDシステムは、HDDシステムを備え、さらに、DVDシステム及びネットワークも備える。

【0024】

10

20

30

40

50

ネットワークによってプロバイダネットワークデバイスと通信するハードディスクドライブ（HDD）システムは、不揮発的な方法で、ユーザアクセス可能セクション及び隠しセクションにデータを記憶するための不揮発性メモリ手段を備える。制御手段が、この不揮発性メモリ手段と通信し、プロバイダネットワークデバイスにコンテンツを選択的に要求してプロバイダネットワークデバイスからコンテンツを受信し、要求されたコンテンツを不揮発性メモリ手段の隠しセクションに記憶する。

【0025】

要求をプロバイダネットワークデバイスへ送信した後、制御手段は、鍵要求を受信し、この鍵要求に応答して、プロバイダネットワークデバイスへ鍵を送信する。プロバイダネットワークデバイスからこのシステムによって受信された、要求されたコンテンツは、鍵を使用して暗号化される。制御手段は、要求されたコンテンツを解読する。要求されたコンテンツは、同じく不揮発性メモリ手段の隠し部分に書き込まれる使用量データを含み、制御手段は、使用量データが、許可された使用を超過したことを示すと、要求されたコンテンツを利用不能にする。

【0026】

他の特徴では、このシステムは、要求されたコンテンツを不揮発性メモリ手段から消去する。使用量データは、許可された所定の使用回数を指定する。使用量データは、許可された使用期間を指定する。HDDシステムは、ネットワークと無線で通信する。HDDシステムは、媒体によってネットワークと通信する。

【0027】

他の特徴では、プロバイダネットワークデバイスは、デジタル多用途ディスク（DVD）システムを含む。ネットワーク接続されたDVD/HDDシステムは、HDDシステムを備え、さらに、DVDシステム及びネットワークも備える。

【0028】

ネットワークによってプロバイダネットワークデバイスと通信するハードディスクドライブ（HDD）システムを動作させる方法は、ユーザアクセス可能セクション及び隠しセクションに不揮発的な方法でデータを記憶すること、プロバイダネットワークデバイスにコンテンツを選択的に要求してプロバイダネットワークデバイスからコンテンツを受信すること、及び、要求されたコンテンツを隠しセクションに記憶すること、を含む。

【0029】

他の特徴では、この方法は、鍵要求を受信すること、及び、この要求をプロバイダネットワークデバイスへ送信した後、この鍵要求に応答して、プロバイダネットワークデバイスへ鍵を送信すること、を含む。この方法は、プロバイダネットワークデバイスからHDDシステムによって受信された、要求されたコンテンツを、鍵を使用して暗号化することを含む。この方法は、要求されたコンテンツを解読することを含む。この方法は、使用量データを含む要求されたコンテンツを、隠し部分に書き込むこと、及び、使用量データが、許可された使用を超過したことを示すと、要求されたコンテンツを利用不能にすること、を含む。この方法は、要求されたコンテンツを隠しセクションから消去することを含む。この方法は、使用量データを使用して、許可された所定の使用回数を指定することを含む。この方法は、使用量データを使用して、許可された使用期間を指定することを含む。

【0030】

ネットワークによってリクエスタネットワークデバイスと通信するデジタル多用途ディスク（DVD）システムは、コンテンツを記憶する不揮発性メモリを備える。制御モジュールが、この不揮発性メモリと通信し、リクエスタネットワークデバイスからコンテンツの要求を選択的に受信し、ローカル／リモートステータスを判断し、リクエスタネットワークデバイスがローカルステータスを有する場合には要求されたコンテンツを送信し、リクエスタネットワークデバイスがリモートステータスを有する場合には要求されたコンテンツを送信しない。

【0031】

他の特徴では、制御モジュールは、要求されたコンテンツを送信する前に、リクエスタ

10

20

30

40

50

ネットワークデバイスに鍵を要求する。制御モジュールは、この鍵要求を送信した後に、リクエスタネットワークデバイスから鍵を受信するのに必要な時間を求める。制御モジュールは、鍵が所定の期間内に受信された場合に、要求されたコンテンツをリクエスタネットワークデバイスへ送信する。この所定の期間は単一ホップ期間又は2ホップ期間にほぼ等しい。制御モジュールは、要求されたコンテンツをリクエスタネットワークデバイスへ送信する前に、要求されたコンテンツを暗号化する。制御モジュールは、リクエスタネットワークデバイスへ送信される、要求されたコンテンツに、使用量データを含める。使用量データは、許可された使用回数を指定する。使用量データは、許可された使用期間を指定する。DVDシステムは、ネットワークと無線で通信する。DVDシステムは、媒体によってネットワークと通信する。

10

【0032】

他の特徴では、リクエスタネットワークデバイスは、ハードディスクドライブ(HDD)システムを含む。ネットワーク接続されたDVD/HDDシステムは、DVDシステムを備え、さらに、HDDシステム及びネットワークも備える。

【0033】

ネットワークによってハードリクエスタネットワークデバイスと通信するデジタル多用途ディスク(DVD)システムは、コンテンツを記憶する不揮発性メモリ手段を備える。制御手段が、この不揮発性メモリ手段と通信し、リクエスタネットワークデバイスからコンテンツの要求を選択的に受信し、ローカル/リモートステータスを判断し、リクエスタネットワークデバイスがローカルステータスを有する場合には要求されたコンテンツを送信し、リクエスタネットワークデバイスがリモートステータスを有する場合には要求されたコンテンツを送信しない。

20

【0034】

他の特徴では、制御手段は、要求されたコンテンツを送信する前に、リクエスタネットワークデバイスに鍵を要求する。制御手段は、この鍵要求を送信した後に、リクエスタネットワークデバイスから鍵を受信するのに必要な時間を求める。制御手段は、鍵が所定の期間内に受信された場合に、要求されたコンテンツをリクエスタネットワークデバイスへ送信する。この所定の期間は2ホップ期間にほぼ等しい。この所定の期間は単一ホップ期間にほぼ等しい。制御手段は、要求されたコンテンツをリクエスタネットワークデバイスへ送信する前に、要求されたコンテンツを暗号化する。制御手段は、リクエスタネットワークデバイスへ送信される、要求されたコンテンツに、使用量データを含める。使用量データは、許可された使用回数を指定する。使用量データは、許可された使用期間を指定する。制御手段は、ネットワークと無線で通信する。DVDシステムは、媒体によってネットワークと通信する。

30

【0035】

他の特徴では、リクエスタネットワークデバイスは、ハードディスクドライブ(HDD)システムを含む。ネットワーク接続されたDVD/HDDシステムは、DVDシステムを備え、さらに、HDDシステム及びネットワークも備える。

【0036】

ネットワークによってハードリクエスタネットワークデバイスと通信するデジタル多用途ディスク(DVD)システムを動作させる方法は、不揮発性メモリにコンテンツを記憶すること、リクエスタネットワークデバイスからコンテンツの要求を選択的に受信すること、ローカル/リモートステータスを判断すること、リクエスタネットワークデバイスがローカルステータスを有する場合には要求されたコンテンツを送信すること、及び、リクエスタネットワークデバイスがリモートステータスを有する場合には要求されたコンテンツを送信しないこと、を含む。

40

【0037】

他の特徴では、この方法は、要求されたコンテンツを送信する前に、リクエスタネットワークデバイスに鍵を要求することを含む。この方法は、この鍵要求を送信した後に、リクエスタネットワークデバイスから鍵を受信するのに必要な時間を求めることを含む。こ

50

の方法は、鍵が所定の期間内に受信された場合に、要求されたコンテンツをリクエスタネットワークデバイスへ送信することを含む。この方法は、この所定の期間を2ホップ期間にほぼ等しく設定することを含む。この方法は、この所定の期間を単一ホップ期間にほぼ等しく設定することを含む。この方法は、要求されたコンテンツをリクエスタネットワークデバイスへ送信する前に、要求されたコンテンツを暗号化することを含む。この方法は、リクエスタネットワークデバイスへ送信される、要求されたコンテンツに、使用量データを含めることを含む。使用量データは、許可された使用回数を指定する。使用量データは、許可された使用期間を指定する。

【0038】

ネットワークにおいてコンテンツを配信するためのシステムは、コンテンツを記憶するメモリと、このメモリと通信するプロバイダネットワークデバイスと、を備える。メディアサーバが、プロバイダネットワークデバイスと通信する。リクエスタネットワークデバイスが、コンテンツのコピーを要求する。メディアサーバは、リクエスタネットワークデバイスのローカル／リモートステータスを判断し、リクエスタネットワークデバイスがコンテンツを要求し、且つ、ローカルステータスを有する場合に、プロバイダネットワークデバイスがリクエスタネットワークデバイスへコンテンツのコピーを送信することを選択的に可能にする。

【0039】

他の特徴では、プロバイダネットワークデバイスは、デジタル多用途ディスク（DVD）システムを含む。リクエスタネットワークデバイスは、ハードディスクドライブ（HDD）システムを含む。メディアサーバは、リクエスタネットワークデバイスのローカル／リモートステータスを判断するローカルネットワーク判断モジュールを含む。メディアサーバは、リクエスタネットワークデバイスの応答時間に基づいて、ローカル／リモートステータスを判断する。

【0040】

他の特徴では、サーバが、メディアサーバと通信し、ローカルネットワークデバイスの識別データを記憶する。メディアサーバは、この識別データに基づいてローカル／リモートステータスを判断する。或いは、メディアサーバが、ローカルネットワークデバイスの識別データを記憶し、この識別データに基づいてローカル／リモートステータスを判断する。識別データは、ローカルネットワークデバイスの媒体アクセス制御（MAC）アドレスを含む。

【0041】

他の特徴では、HDDシステムは、不揮発的な方法でデータを記憶し、且つ、ユーザアクセス可能セクション及び隠しセクションを含む、不揮発性HDDメモリを備える。ハードディスクドライブ（HDD）制御モジュールが、このHDD不揮発性メモリと通信し、メディアサーバにコンテンツを選択的に要求して、プロバイダネットワークデバイス及び／又はメディアサーバの少なくとも1つからコンテンツを受信し、要求されたコンテンツを不揮発性HDDメモリの隠しセクションに記憶する。要求をメディアサーバへ送信した後、HDD制御モジュールは、鍵要求を受信し、この鍵要求に応答して、メディアサーバ及び／又はプロバイダネットワークデバイスの少なくとも1つへ鍵を送信する。プロバイダネットワークデバイス及び／又はメディアサーバの少なくとも1つからHDDシステムによって受信された、要求されたコンテンツは、鍵を使用して暗号化される。HDD制御モジュールは、要求されたコンテンツを解読する。要求されたコンテンツは、同じく不揮発性HDDメモリの隠し部分に書き込まれる使用量データを含む。HDD制御モジュールは、使用量データが、許可された使用を超過したことを示すと、要求されたコンテンツを利用不能にする。HDDシステムは、要求されたコンテンツを不揮発性HDDメモリから消去する。使用量データは、許可された所定の使用回数を指定する。使用量データは、許可された使用期間を指定する。HDDシステムは、ネットワークと無線で通信する。HDDシステムは、有線媒体によってネットワークと通信する。

【0042】

10

20

30

40

50

DVDシステムは、コンテンツを記憶する不揮発性メモリを備える。DVD制御モジュールが、この不揮発性メモリと通信し、リクエスタネットワークデバイス及び/又はメディアサーバの少なくとも1つからコンテンツの要求を選択的に受信する。メディアサーバは、要求されたコンテンツを送信する前に、リクエスタネットワークデバイスに鍵を要求し、この鍵要求をHDDシステムへ送信した後に、HDDシステムから鍵を受信するのに必要な時間を求める。鍵が所定の期間内に受信された場合に、メディアサーバは、DVDシステムが、要求されたコンテンツをHDDシステム及び/又はメディアサーバの少なくとも1つへ送信することを可能にする。この所定の期間は2ホップ期間にほぼ等しい。この所定の期間は単一ホップ期間にほぼ等しい。

【0043】

他の特徴では、DVDシステム及び/又はメディアサーバの少なくとも1つは、要求されたコンテンツをHDDシステムへ送信する前に、要求されたコンテンツを暗号化する。DVD制御モジュール及び/又はメディアサーバの少なくとも1つは、HDDシステムへ送信される、要求されたコンテンツに、使用量データを含める。使用量データは、許可された使用回数を指定する。使用量データは、許可された使用期間を指定する。DVDシステムは、ネットワークと無線で通信する。DVDシステムは、有線媒体によってネットワークと通信する。

【0044】

ネットワークにおいてコンテンツを配信するためのシステムは、コンテンツを記憶するためのメモリ手段を備える。プロバイダネットワーク手段が、このメモリ手段との通信を提供する。メディアサービング手段が、プロバイダネットワーク手段との通信を受け持つ。リクエスタネットワーク手段が、コンテンツのコピーを要求する。メディアサービング手段は、リクエスタネットワーク手段のローカル/リモートステータスを判断し、リクエスタネットワーク手段がコンテンツを要求し、且つ、ローカルステータスを有する場合に、プロバイダネットワーク手段が、コンテンツのコピーをリクエスタネットワーク手段へ送信することを選択的に可能にする。

【0045】

他の特徴では、プロバイダネットワーク手段は、デジタル多用途ディスク(DVD)システムを含む。リクエスタネットワーク手段は、ハードディスクドライブ(HDD)システムを含む。メディアサービング手段は、リクエスタネットワーク手段のローカル/リモートステータスを判断するためのローカルネットワーク判断手段を含む。メディアサービング手段は、リクエスタネットワーク手段の応答時間に基づいて、ローカル/リモートステータスを判断する。サーバ手段が、プロバイダネットワーク手段との通信を受け持つ、ローカルネットワーク手段の識別データを記憶する。メディアサービング手段は、識別データに基づいてローカル/リモートステータスを判断する。或いは、メディアサービング手段が、ローカルネットワーク手段の識別データを記憶する。識別データは、ローカルネットワーク手段の媒体アクセス制御(MAC)アドレスを含む。

【0046】

他の特徴では、HDDシステムは、不揮発的な方法でデータを記憶し、且つ、ユーザーアクセス可能セクション及び隠しセクションを含む、不揮発性HDDメモリ手段を備える。ハードディスクドライブ(HDD)制御手段が、このHDD不揮発性メモリ手段と通信し、メディアサービング手段にコンテンツを選択的に要求して、メディアサービング手段からコンテンツを受信し、要求されたコンテンツを不揮発性HDDメモリ手段の隠しセクションに記憶する。要求をメディアサービング手段へ送信した後、HDD制御手段は、鍵要求を受信し、この鍵要求に応答して、プロバイダネットワーク手段及び/又はメディアサービング手段の少なくとも1つへ鍵を送信する。プロバイダネットワーク手段及び/又はメディアサービング手段の少なくとも1つからHDDシステムによって受信された、要求されたコンテンツは、鍵を使用して暗号化される。HDD制御手段は、要求されたコンテンツを解読する。要求されたコンテンツは、同じく不揮発性HDDメモリ手段の隠し部分に書き込まれる使用量データを含み、HDD制御手段は、使用量データが、許可された使

10

20

30

40

50

用を超過したことを示すと、要求されたコンテンツを利用不能にする。HDDシステムは、要求されたコンテンツを不揮発性HDDメモリ手段から消去する。使用量データは、許可された所定の使用回数を指定する。使用量データは、許可された使用期間を指定する。HDDシステムは、ネットワークと無線で通信する。HDDシステムは、有線媒体によってネットワークと通信する。

【0047】

他の特徴では、DVDシステムは、コンテンツを記憶する不揮発性メモリ手段と、この不揮発性メモリ手段と通信し、メディアサービング手段からコンテンツの要求を選択的に受信するためのDVD制御手段とを備える。メディアサービング手段は、要求されたコンテンツを送信する前に、リクエスタネットワーク手段に鍵を要求し、この鍵要求をHDDシステムへ送信した後に、HDDシステムから鍵を受信するのに必要な時間を求める。鍵が所定の期間内に受信された場合に、DVD制御手段及び/又はメディアサービング手段の少なくとも1つは、要求されたコンテンツをHDDシステムへ送信する。この所定の期間は2ホップ期間にほぼ等しい。この所定の期間は単一ホップ期間にほぼ等しい。DVD制御手段及び/又はメディアサービング手段の少なくとも1つは、要求されたコンテンツをHDDシステムへ送信する前に、要求されたコンテンツを暗号化する。DVD制御手段及び/又はメディアサービング手段の少なくとも1つは、HDDシステムへ送信される、要求されたコンテンツに、使用量データを含める。使用量データは、許可された使用回数を指定する。使用量データは、許可された使用期間を指定する。DVDシステムは、ネットワークと無線で通信する。DVDシステムは、有線媒体によってネットワークと通信する。

【0048】

ネットワークにおいてコンテンツを配信するための方法は、メモリにコンテンツを記憶すること、このメモリと通信するプロバイダネットワークデバイスを設けること、このプロバイダネットワークデバイスと通信するメディアサービングデバイスを設けること、コンテンツのコピーを要求するリクエスタネットワークデバイスを設けること、メディアサービングデバイスを使用してリクエスタネットワークデバイスのローカル/リモートステータスを判断すること、及び、リクエスタネットワークデバイスがコンテンツを要求し、且つ、ローカルステータスを有する場合に、コンテンツのコピーをリクエスタネットワークデバイスへ選択的に送信すること、を含む。

【0049】

他の特徴では、プロバイダネットワークデバイスは、デジタル多用途ディスク(DVD)システムを含む。リクエスタネットワークデバイスは、ハードディスクドライブ(HDD)システムを含む。この方法は、リクエスタネットワークデバイスのローカル/リモートステータスを判断することを含む。この方法は、リクエスタネットワークデバイスの応答時間に基づいて、ローカル/リモートステータスを判断することを含む。この方法は、ローカルネットワークデバイスの識別データを記憶することを含む。メディアサービングデバイスは、この識別データに基づいてローカル/リモートステータスを判断する。この方法は、ローカルネットワークデバイスの媒体アクセス制御(MAC)アドレスを記憶することを含む。

【0050】

他の特徴では、この方法は、HDDシステムのユーザアクセス可能セクション及び隠しセクションに不揮発的な方法でデータを記憶すること、メディアサービングデバイスを介して、プロバイダネットワークデバイスにコンテンツを選択的に要求してプロバイダネットワークデバイスからコンテンツを受信すること、及び、要求されたコンテンツを不揮発性HDDメモリの隠しセクションに記憶すること、を含む。

【0051】

他の特徴では、この方法は、鍵要求を受信すること、及び、この要求をメディアサービングデバイスへ送信した後、この鍵要求に応答して、メディアサービングデバイスへ鍵を送信すること、を含む。この方法は、プロバイダネットワークデバイス及び/又はメディ

10

20

30

40

50

アーサービングデバイスの少なくとも 1 つから HDD システムによって受信された、要求されたコンテンツを、鍵を使用して暗号化することを含む。この方法は、要求されたコンテンツを解読することを含む。この方法は、使用量データを含む要求されたコンテンツを、不揮発性 HDD メモリの隠し部分に書き込むこと、及び、使用量データが、許可された使用を超過したことを示すと、要求されたコンテンツを利用不能にすること、を含む。

【 0 0 5 2 】

他の特徴では、この方法は、要求されたコンテンツを不揮発性 HDD メモリから消去することを含む。この方法は、使用量データを使用して、許可された所定の使用回数を指定することを含む。この方法は、使用量データを使用して、許可された使用期間を指定することを含む。

10

【 0 0 5 3 】

この方法は、コンテンツをプロバイダネットワークデバイスに記憶すること、及び、メディアアーサービングデバイスを介して、リクエスタネットワークデバイスからコンテンツの要求を選択的に受信すること、を含む。この方法は、要求されたコンテンツを送信する前に、リクエスタネットワークデバイスに鍵を要求すること、及び、この鍵要求を HDD システムへ送信した後に、HDD システムから鍵を受信するのに必要な時間を求めること、を含む。この方法は、鍵が所定の期間内に受信された場合に、要求されたコンテンツを HDD システムへ送信することを含む。この所定の期間は 2 ホップ期間にほぼ等しい。この所定の期間は単一ホップ期間にほぼ等しい。この方法は、要求されたコンテンツを HDD システムへ送信する前に、要求されたコンテンツを暗号化することを含む。この方法は、要求されたコンテンツ内の使用量データを HDD システムへ送信することを含む。使用量データは、許可された使用回数を指定する。使用量データは、許可された使用期間を指定する。

20

【 0 0 5 4 】

本発明のさらに別の適用分野は、以下に設けられた発明を実施するための最良の形態から明らかになる。発明を実施するための最良の形態及び具体的な例は、本発明の好ましい実施の形態を示しているが、単なる例示を目的としており、本発明の範囲を限定することを目的とするものでないことが理解されるべきである。

30

【 0 0 5 5 】

本発明は、発明を実施するための最良の形態及び添付図面からより十分に理解されることになる。

【 発明を実施するための最良の形態 】

【 0 0 5 6 】

好ましい実施の形態（複数可）の以下の説明は、本質的に単なる例示であり、決して、本発明、その用途、又は使用を限定することを目的とするものではない。本明細書では、モジュール又はデバイスという用語は、説明する機能を提供する 1 つ若しくは 2 つ以上のソフトウェアプログラム若しくはファームウェアプログラム、組み合わせ論理回路、及び / 又は他の適切なコンポーネントを実行する特定用途向け集積回路（ASIC）、電子回路、プロセッサ（共有、専用、又はグループ）、及びメモリを指す。明確にするために、図面では、同様の要素を特定するのに同じ参照符号を使用するものとする。

40

【 0 0 5 7 】

次に図 1 を参照して、ローカルネットワーク 2 は、ルータ 3、モdem 4、及びプロバイダネットワークデバイス 5 を含む。このプロバイダネットワークデバイス 5 は、以下に説明するように、1 つ又は 2 つ以上のローカルリクエスタネットワークデバイスに保護コンテンツ 6 を選択的に供給する。プロバイダネットワークデバイス 5 は、ローカルネットワーク判断モジュール 7 を含むネットワーク互換デバイスである。1 つ又は 2 つ以上のリクエスタネットワークデバイス 8 - 1、8 - 2、... 及び 8 - N（リクエスタ 8 と総称する）は、保護コンテンツ 6 のコピーを選択的に要求する。十分理解できるように、ルータ 3 及びワイヤライイン接続が示されているが、当業者には、他のネットワーク構成も明らかであろう。他のネットワーク構成には、無線アクセスポイント（AP）、アドホックネットワ

50

ーク接続構成、及び／又は無線ネットワーク構成が含まれるが、これらに限定されるものではない。プロバイダネットワークデバイス5は、保護コンテンツ6用の不揮発性メモリ等のメモリを含むものとして示されているが、保護コンテンツ6は、プロバイダネットワークデバイス5の内部及び／又は外部に記憶することができる。

【0058】

モデル4は、ブロードバンドサービスプロバイダ9に接続されている。このブロードバンドサポートプロバイダ9は、ビデオコンテンツ、デジタルコンテンツ、分散通信システム(DCS)10へのブロードバンド接続、及び／又は他のネットワークサービスを提供する。サービスプロバイダ9は、有線接続若しくは無線接続、同軸ケーブル、デジタル加入者線(DSL)、衛星、及び／又は他の任意の接続システム若しくは接続方法を使用してブロードバンドアクセスを提供することができる。

10

【0059】

DCS10は、1つ又は2つ以上のサーバ11-1、11-2、…、及び11-Mによって、ネットワークデバイス12-11、12-12、…、12-1P、12-21、12-22、…、12-2P、…、及び12-M1、12-M2、…、12-MP(ネットワークデバイス12と総称する)に接続されている。ローカルネットワーク判断モジュール7は、リクエスタネットワークデバイスが保護コンテンツ6のコピーを要求した時に、当該リクエスタネットワークデバイスがローカルステータスを有するのか、それともリモートステータスを有するのかを選択的に判断する。この手法は、リモートネットワークデバイスによる保護コンテンツへのアクセスを阻止することによってセキュリティを増大させる。

20

【0060】

ローカルネットワーク判断モジュール7がリクエスタネットワークデバイスのローカル／リモートステータスを判断するための方法には多くの異なる方法がある。たとえば、いくつかの実施態様では、プロバイダネットワークデバイス5は、リクエスタネットワークデバイスからの応答を受信するのに必要な時間を求めることによってローカル／リモートステータスを判断する。応答時間が所定の期間よりも小さい場合には、リクエスタネットワークデバイスは、ローカルステータスを有すると判断される。応答時間が所定の期間よりも大きい場合には、リクエスタネットワークデバイスは、リモートステータスを有し、保護コンテンツのコピーは拒否される。サービスプロバイダ9、DCS10、及びサーバ11を介したリモートネットワークデバイス12へのデータの送信及び受信に必要な時間は、ローカルリクエスタネットワークデバイスが応答するのに必要な時間よりも極めて大きい。換言すれば、所定の期間は、ローカルリクエスタネットワークデバイスによって必要とされる応答時間よりも大きく、且つ、リモートリクエスタネットワークデバイスによって必要とされる応答時間よりも小さく設定される。

30

【0061】

他の実施態様では、プロバイダネットワークデバイスは、動的ホスト構成プロトコル(DHCP)サーバのDHCPテーブルをチェックして、ローカルネットワークデバイスの媒体アクセス制御(MAC)アドレスを求める。リクエスタネットワークデバイスが、そのテーブルのローカルMACアドレスと一致した場合、リクエスタネットワークデバイスは、ローカルステータスを有し、保護コンテンツのコピーを送信することができる。一致しない場合、リクエスタネットワークデバイスは、リモートステータスを有し、保護コンテンツのコピーは送信されない。

40

【0062】

さらに他の実施態様では、プロバイダネットワークデバイス5は、サービスプロバイダ9(及びDCS10)に対するルータ3又はモデル4の外部ポートを一時的にブロックするためのメッセージをルータ3へ送信することができる。外部ポートのブロック後、プロバイダネットワークデバイス5は、リクエスタネットワークデバイスがまだ通信可能であるかどうかを判断する(この判断は、リクエスタネットワークデバイスがローカルステータスを有する場合に真となる)。プロバイダネットワークデバイスが、要求側ネットワー

50

クデバイスと通信できる場合、プロバイダネットワークデバイスは、コピープロテクトされたコンテンツを送信する。当業者には十分理解できるよう、これらの手法の1つ又は2つ以上を組み合わせることもでき、且つ／又は、他の手法を使用して、リクエスタネットワークデバイスのローカル／リモートステータスを判断することもできる。

【0063】

以下の説明部分は、プロバイダネットワークデバイスとしてDVDシステム及び／又はDVD／HDD結合システムを使用し、リクエスタネットワークデバイスとしてDVD／HDD結合システム及び／又はHDDシステムを含む別のネットワークデバイスを使用するが、当業者には、他のプロバイダネットワークデバイス及び／又はリクエスタネットワークデバイスを使用できることが十分理解されよう。また、当業者には、DVDシステム及びHDDシステムと共に以下で説明する実施態様のすべてが、他の任意の適切なネットワークデバイスと共に実施できることも理解されよう。

10

【0064】

次に図2を参照して、ネットワーク接続された第1の例示のDVD及びHDDのシステムの機能ブロック図が示されている。ローカルネットワーク13は、媒体16によってサービスプロバイダ18と通信するモデル14を含む。サービスプロバイダ18は、インターネット、LAN、WAN、他の分散ネットワーク等の分散通信システム(DCS)22への接続を提供し、且つ／又は、ビデオコンテンツ、電話サービス等の他のネットワークサービスを提供する。モデル14は、ルータ28に接続することができる。ルータ28は、複数のネットワークデバイス30-1、30-2、…、及び30-N(一括してネットワークデバイス30)をモデル14に接続する。ネットワークデバイスの1つ30-1は、ハードディスクドライブ(HDD)システム34に接続されている。HDDシステム34は、テレビ又はモニタ38に接続することができる。このテレビ又はモニタ38も、媒体16に、直接又はセットトップボックス(図示せず)を通じて接続することができ、サービスプロバイダ18からコンテンツを受信することができる。

20

【0065】

ローカルネットワーク13は、ルータ28及び1つ又は2つ以上の無線局42-1、42-2、…、及び42-N(一括して無線局42)と通信するアクセスポイント(AP)40を含むことができる。AP40は、ルータ28に接続されたものとして示されているが、APの機能及びルータの機能は、単一のデバイスに結合することができる。或いは、結合されたAP／ルータをモデル14に直接接続することもできる。さらに他のタイプのネットワーク構成及び接続も当業者には明らかであろう。

30

【0066】

ネットワークデバイス30-2は、ルータ28と通信し、2005年1月19日に出願された米国特許出願第11/039,288号に図示及び説明されたもの等のDVDプレイヤ又はDVD／HDD結合プレイヤ44(以下、共に「DVDプレイヤ44」と呼ぶ)と通信する。この米国特許出願は、参照によりその全内容が本明細書に援用される。次に、DVDプレイヤ44は、テレビ又はモニタ46と通信することができる。テレビ又はモニタ46は、媒体16又はセットトップボックス50に接続することができる。サービスプロバイダ18は、DCS22へのブロードバンドアクセス、ビデオコンテンツ、及び／又は他のサービスを提供する。1つ又は2つ以上の他のサーバ54-1及び54-2(一括してサーバ54)は、ネットワークデバイス60、コンピュータ62、携帯情報端末(PDA)等のインターフェースをDCS22に提供する。

40

【0067】

いくつかの実施態様では、テレビ又はモニタ38のユーザは、DVDプレイヤ44に関連したDVDコンテンツにアクセスしたい場合がある。まず、HDD34は、利用可能なコンテンツのリストをDVDプレイヤに要求することができる。DVDプレイヤは、利用可能なコンテンツのリストを送信する。HDD34は、そのリストから選択されたコンテンツのコピーを要求するメッセージを、ネットワークを介してDVDプレイヤ44へ送信する。DVDシステムは、HDDシステムがローカルステータスを有するかどうかを判断

50

する。HDDシステム又は他のリクエスタネットワークデバイスがローカルステータスを有する場合、コンテンツファイルが送信される。HDDシステム又は他のリクエスタネットワークデバイスがリモートステータスを有する場合、要求は拒否される。ローカル／リモートステータスの判断は、応答時間、DHCPテーブルのMACアドレス、外部ポートの断線及び対応するダイアログ、並びに／又は他の適切な方法に基づいて行うことができる。

【0068】

いくつかの実施態様では、DVDプレイヤ44は、HDD34に鍵を要求することによって応答する。DVDプレイヤ44は、HDD34が応答するのに必要な時間を求めるタイムを始動する。HDD34は、要求された鍵をDVDプレイヤ44へ送信する。DVDプレイヤ44は、HDD34が所定の時間内に応答したかどうかを判断する。

【0069】

HDD34が所定の時間内に応答した場合、DVDプレイヤ44は、選択されたコンテンツを鍵でスクランブルして、そのスクランブルされたコンテンツをネットワークによりHDD34へ送信する。HDD34は、そのコンテンツを鍵でスクランブル解除し、テレビ又はモニタ38でコンテンツの再生を可能にする。十分理解できるように、鍵の交換は、HDDが利用可能なコンテンツを最初に要求する時に早めに行うこともできる。

【0070】

また、HDD34は、使用を制約するDVDプレイヤから使用量データを受信することもできる。たとえば、この使用量データは、N回の再生及び／又は所定の期間の間の再生を許可することができる。使用量データに指定されたような許可された使用期間が経過した後、HDD34は、ビデオコンテンツを利用不能にする。たとえば、HDDはビデオコンテンツを消去する場合がある。

【0071】

いくつかの実施態様では、HDD34は、ユーザアクセス可能セクション及び隠しセクションを含む。DVDプレイヤ44からのビデオコンテンツは、DVDプレイヤ44の隠しセクションに記憶される。HDD34によって提供される鍵は、公開／私有鍵暗号化システム及び／又は他の適切なデータ暗号化の一部とすることができます。或いは、他の形式の、鍵に基づくスクランブルを実行することもできる。

【0072】

DVDプレイヤが単一のDVDプレイヤである場合、DVDプレイヤは、そのDVDプレイヤのDVDで利用可能なコンテンツのリストを送信する。DVDプレイヤが回転トレーを含む場合、DVDプレイヤは、回転トレーのDVDから入手できるDVDコンテンツのリストを送信する。DVDプレイヤがDVD／HDD結合プレイヤである場合、DVD／HDDプレイヤは、関連したHDDに記憶されたDVDコンテンツと共に、そのプレイヤの1つ又は複数のDVDで利用可能なDVDコンテンツのリストを送信する。

【0073】

次に図3～図5を参照して、本発明のさまざまな例示の構成が示されている。これらの実施態様では、プロバイダネットワークデバイスは、DVDシステム及び／又はDVD／HDD結合システムを含み、リクエスタネットワークデバイスは、HDDシステム及び／又はDVD／HDD結合システムを含む。図3では、HDD34は、局42-1によってネットワークに接続されている。局42-1は、AP40と無線通信を行う。DVDプレイヤ44及びテレビ46は、ネットワークデバイス30-2及び媒体16によってルータ28に接続されている。図4では、HDD34は、ネットワークデバイス30-1及び媒体16によってルータ28に接続されている。DVDプレイヤ44は、局42-2によってネットワークに接続されている。局42-2は、AP40と無線通信を行う。図5では、HDD34及びDVDプレイヤ44は、1つ又は2つ以上の局42-1及び／又は42-2によってネットワークに接続されている。他のさまざまなネットワーク構成が当業者には明らかであろう。

【0074】

10

20

30

40

50

次に図6を参照して、例示のリクエスタネットワークデバイスは、HDD P C B 114を有するHDDシステム110を含む。バッファ118は、読み出しデータ、書き込みデータ、及び/又は、HDDシステム110の制御に関連した揮発性制御データを記憶する。バッファ118は、通例、待ち時間の小さな揮発性メモリを使用する。たとえば、SDRAM又は他のタイプの待ち時間の小さなメモリを使用することができる。また、フラッシュメモリ等の不揮発性メモリ119も、不揮発性制御コード等の重要なデータを記憶するのに設けることができる。

【0075】

HDD P C B 114に配置されたプロセッサ122は、HDDシステム110のオペレーションに関係したデータ処理及び/又は制御処理を実行する。ハードディスク制御モジュール(HDC)126は、入出力インターフェース124、並びに、スピンドル/音声コイルモータ(VCM)ドライバ若しくはモジュール130及び/又は読み出し/書き込みチャネルモジュール134と通信する。HDC126は、スピンドル/VCMドライバ130、読み出し/書き込みチャネルモジュール134、及びプロセッサ122、並びに、インターフェース124を介したホスト135とのデータ入出力の制御を調整する。

【0076】

書き込みオペレーション中、読み出し/書き込みチャネルモジュール134は、読み出し/書き込みデバイス159に書き込まれるデータを符号化する。読み出し/書き込みチャネルモジュール134は、信頼性のために書き込み信号を処理し、たとえば、誤り訂正符号化(ECC)、ランレングス制限符号化(RLL)等を適用することができる。読み出しオペレーション中、読み出し/書き込みチャネルモジュール134は、読み出し/書き込みデバイス159のアナログ読み出し信号出力をデジタル読み出し信号に変換する。次に、変換された信号は、既知の技法によって検出されて復号され、HDDに書き込まれたデータが回復される。

【0077】

ハードディスクドライブアセンブリ(HDDA)150は、1つ又は2つ以上のハードドライブプラッタ152を含む。このハードドライブプラッタ152は、磁界を記憶する磁気コーティングを含む。プラッタ152は、154に概略的に示すスピンドルモータによって回転する。一般に、スピンドルモータ154は、読み出し/書き込みオペレーション中、制御された速度でハードドライブプラッタ152を回転させる。1つ又は2つ以上の読み出し/書き込みアーム158が、プラッタ152に対して移動し、ハードドライブプラッタ152からデータを読み出し、且つ/又は、ハードドライブプラッタ152へデータを書き込む。スピンドル/VCMドライバ130は、スピンドルモータ154を制御する。スピンドルモータ154は、プラッタ152を回転させる。また、スピンドル/VCMドライバ130は、たとえば、音声コイルアクチュエータ、ステッパモータ、又は他の任意の適切なアクチュエータを使用して、読み出し/書き込みアーム158を位置付ける制御信号も生成する。

【0078】

読み出し/書き込みデバイス159は、読み出し/書き込みアーム158の遠位端の近くに配置される。読み出し/書き込みデバイス159は、磁界を生成するインダクタ等の書き込み素子を含む。また、読み出し/書き込みデバイス159は、プラッタ152の磁界を検知する読み出し素子(磁気抵抗(MR)素子等)も含む。HDDA150は、アナログ読み出し/書き込み信号を増幅するプリアンプ回路160を含む。データの読み出し時に、プリアンプ回路160は、読み出し素子からの低レベルの信号を増幅して、その増幅された信号を読み出し/書き込みチャネルモジュール134に出力する。データの書き込み時に、読み出し/書き込みデバイス159の書き込み素子を流れる書き込み電流が生成される。この書き込み電流はスイッチングされて、正極性又は負極性を有する磁界を生成する。正極性又は負極性は、ハードドライブプラッタ152によって記憶され、データを表すのに使用される。

【0079】

10

20

30

40

50

次に図 7 A 及び図 7 B を参照して、例示のプロバイダネットワークデバイスは、DVD システム 210 を含む。DVD PCB 214 は、バッファ 218 を含む。このバッファ 218 は、読み出しデータ、書き込みデータ、及び / 又は、DVD システム 210 の制御に関連した揮発性制御コードを含む。バッファ 218 は、SDRAM や他のタイプの待ち時間の小さなメモリ等の揮発性メモリを使用することができる。また、フラッシュメモリ等の不揮発性メモリ 219 も、DVD 書き込みフォーマット及び / 又は他の不揮発性制御コードに関するデータ等の重要なデータに使用することができる。DVD PCB 214 に配置されたプロセッサ 222 は、DVD システム 210 のオペレーションに関係したデータ処理及び / 又は制御処理を実行する。また、プロセッサ 222 は、必要に応じて、コピーブロテクトの復号及び / 又は圧縮 / 伸張も実行する。DVD 制御モジュール 226 は、入出力インターフェース 224、並びに、スピンドル / フィードモータ (FM) ドライバ 230 及び / 又は読み出し / 書き込みチャネルモジュール 234 と通信する。DVD 制御モジュール 226 は、スピンドル / FM ドライバ、読み出し / 書き込みチャネルモジュール 234、及びプロセッサ 222、並びに、インターフェース 224 を介したデータ入出力の制御を調整する。

【0080】

書き込みオペレーション中、読み出し / 書き込みチャネルモジュール 234 は、光学式読み出し / 書き込み (ORW) デバイス又は光学式読み出し専用 (OR (optical read only)) デバイス 259 によって DVD プラッタに書き込まれるデータを符号化する。読み出し / 書き込みチャネルモジュール 234 は、信頼性のために信号を処理し、たとえば、ECC、RLL 等を適用することができる。読み出しオペレーション中、読み出し / 書き込みチャネルモジュール 234 は、ORW デバイス又は OR デバイス 259 のアナログ出力をデジタル信号に変換する。次に、変換された信号は、既知の技法によって検出され復号され、DVD に書き込まれたデータが回復される。

【0081】

DVD アセンブリ (DVA) 250 は、データを光学的に記憶する DVD プラッタ 252 を含む。プラッタ 252 は、254 に概略的に示すスピンドルモータによって回転する。スピンドルモータ 254 は、読み出し / 書き込みオペレーション中、制御された速度及び / 又は可変速度で DVD プラッタ 252 を回転させる。ORW デバイス又は OR デバイス 259 が、DVD プラッタ 252 に対して移動し、DVD プラッタ 252 からデータを読み出し、且つ / 又は、DVD プラッタ 252 へデータを書き込む。ORW デバイス又は OR デバイス 259 は、通常、レーザ及び光センサを含む。

【0082】

DVD 読み出し / 書き込みシステム及び DVD 読み出し専用システムでは、レーザは、読み出しオペレーション中、ランド及びピットを含む DVD 上のトラックに向けられる。光センサは、ランド / ピットによって引き起こされた反射を検知する。いくつかの読み出し / 書き込み (RW) アプリケーションでは、書き込みオペレーション中、DVD プラッタのダイ層を過熱するのにもレーザが使用される場合がある。ダイが或る温度に過熱されると、ダイは、透明になり、或る 2 進数値を表す。ダイが別の温度に過熱されると、ダイは、不透明になり、他の 2 進数値を表す。DVD を書き込むための他の技法を使用することができる。

【0083】

スピンドル / FM ドライバ 230 は、スピンドルモータ 254 を制御する。スピンドルモータ 254 は、DVD プラッタ 252 を制御可能に回転させる。また、スピンドル / FM ドライバ 230 は、たとえば、音声コイルアクチュエータ、ステッパモータ、又は他の任意の適切なアクチュエータを使用して、フィードモータ 258 を位置付ける制御信号も生成する。フィードモータ 258 は、通常、ORW デバイス又は OR デバイス 259 を、DVD プラッタ 252 に対して半径方向に移動させる。レーザドライバ 261 は、読み出し / 書き込みチャネルモジュール 234 の出力に基づいて、レーザドライブ信号を生成する。DVA 250 は、アナログ読み出し信号を増幅するプリアンプ回路 260 を含む。

10

20

30

40

50

データの読み出し時に、プリアンプ回路 260 は、ORWデバイス又はORデバイスからの低レベルの信号を増幅して、その増幅された信号を読み出し／書き込みチャネルモジュールデバイス 234 に出力する。

【0084】

DVDシステム 210 は、コーデックモジュール 240 をさらに含む。このコーデックモジュール 240 は、MPEG フォーマットのいずれか等のビデオの符号化及び／又は復号を行う。音響デジタル信号プロセッサ及び／若しくはモジュール 242、並びに／又は、ビデオデジタル信号プロセッサ及び／若しくはモジュール 244 は、音響信号処理及び／又はビデオ信号処理をそれぞれ実行する。

【0085】

HDDシステム 110 と同様に、DVDシステム 210 の複数の部分は、1つ又は2つ以上の集積回路 (IC) 又はチップによって実施することができる。たとえば、プロセッサ 222 及び DVD 制御モジュール 226 は、単一のチップによって実施することができる。スピンドル／FM ドライバ 230 及び／又は読み出し／書き込みチャネルモジュール 234 も、プロセッサ 222、DVD 制御モジュール 226 と同じチップによって実施することができ、且つ／又は、追加されたチップによって実施することができる。また、DVD A 250 以外の DVD システム 210 のほとんども、SOC として実施することができる。

【0086】

次に図 7C を参照して、本発明のいくつかの実施態様による例示の DVD / HDD 結合システム 280 の簡略機能ブロック図が示されている。この DVD / HDD 結合システムは、プロバイダネットワークデバイス又はリクエスタネットワークデバイスとして使用することができる。DVD / HDD 結合システム 280 は、不揮発性メモリ 290 及び揮発性メモリ 292 と通信する結合システム制御モジュール 284 を含む。これらのメモリは、DVD 及び HDD の双方のオペレーション用のデータを記憶する。システム制御モジュール 284 は、インターフェース 294 を介して、ホスト 298 のインターフェース 296 と通信する。いくつかの実施態様では、インターフェース 294 及び 296 は、シリアル ATA インターフェース、ファイバチャネル (FC)、シリアル接続小型コンピュータシステムインターフェース (SAS)、又は、他の適切なインターフェースである。

【0087】

DVD / HDD 結合システムは、DVD システム及び HDD システムの双方を制御する。DVD / HDD システムは、システム全体のコストを低減し、改善された機能及び性能を提供する。コストは、DVD 及び HDD の双方のデータストレージ用の単一のDRAM 及びフラッシュメモリの使用を通じて削減される。単一の電源装置が必要とされ、また、外部接続の個数の削減が必要とされ、これによって、コストがさらに低減される。

【0088】

これに加えて、DVD / HDD 統合システムにより、コピープロテクトされたコンテンツを HDD へ直接、ビットごとにコピーすることが可能になる。換言すれば、コピープロテクト方式もデジタル著作権管理 (DRM) も解読することなく、且つ、大幅なオペレーティングシステムの関与も必要とすることなく、コピープロテクトされたコンテンツをコピーすることができる。従来の別々の DVD システム及び HDD システムは、出力する前に、DVD が DRM 又は他のコピープロテクトを復号／解読する必要がある。DRM 又は他のコピープロテクトは、HDD へのその後のコピーを許可する場合もあるし、許可しない場合もある。システムを結合することによって、DRM 又はコピープロテクトは元のままの状態であるので、コピープロテクト方式又は DRM 方式のセキュリティが内蔵されていることに起因して、追加機能が提供される。たとえば、単一の DVD ドライブのコピー操作は、コピープロテクト又は DRM を取り除くことなくサポートされる。これに加えて、HDD は、仮想 DVD チェンジャとして動作することもできる。DVD / HDD 結合システムのさらに他の変形は、2005年1月19日に出願された米国特許出願第 11 / 039,288 号に図示して説明されている。

10

20

30

40

50

【 0 0 8 9 】

次に図8を参照して、いくつかの実施態様に従ってHDDの不揮発性メモリ300をユーザアクセス可能エリア及び隠しエリアに区画することが示されている。HDDの不揮発性メモリ300は、ユーザアクセス可能な第1の部分304、及び、ユーザがアクセス可能でない（すなわち、隠された）第2の部分308に割り当てられる。第2の隠し部分308は、本発明のいくつかの実施態様による以下の方法の1つ又は2つ以上で使用される。隠し部分308は、コピーされるDVDのコンテンツを記憶するのに使用される。これに加えて、HDDの隠し部分308は、仮想DVD回転トレーを提供するのにも使用される。換言すれば、複数のDVDをHDDにコピーすることができ、後日、プレイバックすることができる。

10

【 0 0 9 0 】

次に図9Aを参照して、ネットワークデバイスによって実行されるステップが示されている。制御はステップ350において開始する。ステップ352において、制御は、プロバイダネットワークデバイスが保護コンテンツのコピーの要求を受信したかどうかを判断する。受信していない場合、制御はステップ352へ戻る。ステップ352が真である場合、制御は、ステップ354において、リクエスタネットワークデバイスがローカルネットワークに位置しているかどうかを判断する。ステップ354が偽である場合、制御は、要求を拒否し、ステップ352へ戻る。ステップ354が真である場合、プロバイダネットワークデバイスは、保護コンテンツのコピーをリクエスタネットワークデバイスへ送信する。

20

【 0 0 9 1 】

プロバイダネットワークデバイスは、リクエスタネットワークデバイスがローカルネットワークに存在するかどうかを、任意の適切な方法で判断する。たとえば、リクエスタネットワークデバイスの応答時間を所定のしきい値と比較することができる。他の実施態様では、プロバイダネットワークデバイスは、ファイルが送信される前に、リクエスタネットワークデバイスのローカル/リモートステータスを確認できるように、一時的に、ルータ又はモデルの外部ポートをブロックするように要求することができる。他の実施態様では、ローカルサーバに照会して、ローカルネットワークデバイスを判断することができる。ローカル/リモートステータスを判断するためのさらに他の方法を使用することもできる。

30

【 0 0 9 2 】

次に図9Bを参照して、外部ポートを一時的にブロックすることによってローカル/リモートステータスを判断するためのステップが示されている。制御はステップ360で開始する。ステップ362において、制御は、プロバイダネットワークデバイスが、コピープロテクトされたファイルの要求を受信したかどうかを判断する。ステップ362が偽である場合、制御はステップ362へ戻る。ステップ362が真である場合、制御は、ステップ364に続き、ステップ364において、プロバイダネットワークデバイスは、ルータ又はモデルの外部ポートをブロックするように要求する。ステップ368において、プロバイダネットワークデバイスは、リクエスタネットワークデバイスがローカルステータスを有するかどうかを判断する。たとえば、プロバイダネットワークデバイスは、リクエスタネットワークデバイスにメッセージを送信して、応答を待つことができる。ステップ368が偽である場合、プロバイダネットワークデバイスは要求を拒否し、制御はステップ362へ戻る。ステップ368が真である場合、プロバイダネットワークデバイスは、ステップ370において、ファイルのコピーをリクエスタネットワークデバイスへ送信する。プロバイダネットワークデバイスは、ステップ374において、ルータ又はモデルの外部接続又はポートのブロックを解除する。

40

【 0 0 9 3 】

次に図9Cを参照して、ローカルサーバ（DHCPサーバ等）を調べてローカル/リモートステータスを判断するためのステップが示されている。制御はステップ380で開始する。ステップ382において、制御は、プロバイダネットワークデバイスが、コピー

50

ロテクトされたファイルの要求を受信したかどうかを判断する。ステップ382が偽である場合、制御はステップ382へ戻る。ステップ382が真である場合、制御は、ステップ384に続き、ステップ384において、プロバイダネットワークデバイスは、サーバに照会して、ローカルネットワークデバイスの識別情報を得る。この識別情報は、MACアドレスを含むことができる。ただし、他のタイプの識別情報を使用することもできる。ステップ386において、プロバイダネットワークデバイスは、リクエスタネットワークデバイスがローカルステータスを有するかどうかを判断する。ステップ386が偽である場合、プロバイダネットワークデバイスは要求を拒否し、制御はステップ382へ戻る。ステップ386が真である場合、プロバイダネットワークデバイスは、ステップ388において、ファイルのコピーをリクエスタネットワークデバイスへ送信する。

10

【0094】

次に図9Dを参照して、ネットワークシステムによって実行されるステップが包括的に400で示されている。ステップ402において、制御は開始する。ステップ404において、プロバイダネットワークデバイスは、リクエスタネットワークデバイスがコンテンツのコピーを要求しているかどうかを判断する。要求していないと判断した場合、制御はステップ404へ戻る。要求していると判断した場合、制御は、ステップ408に続き、プロバイダネットワークデバイスは、リクエスタネットワークデバイスに鍵を要求する。ステップ412において、プロバイダネットワークデバイスはタイマを始動する。

20

【0095】

ステップ416において、プロバイダネットワークデバイスは、鍵が受信されたかどうかを判断する。鍵が受信されておらず、且つ、(いくつかの実施態様では)所定の期間を超過していない場合、制御はステップ416に続く。そうでない場合、制御はステップ420に続き、プロバイダネットワークデバイスはタイマを停止する。ステップ422において、制御は、タイマが所定の期間よりも短いかどうかを判断する。

20

【0096】

いくつかの実施態様では、所定の期間は、パケットが1つ又は2つのホップを進むのに必要とする時間以下にされる。応答時間を制限することによって、セキュリティが追加して提供される。ホームネットワークの外部のコンピュータ又は他のデバイスが応答するのに必要な時間は、この所定の期間を超過する。換言すれば、ホームネットワークの外部に接続されたコンピュータ62等のコンピュータ又はネットワークデバイス60等の他のネットワークデバイスからの鍵を含んだパケットは、1つ又は2つのホップを超える。これは、モデム及びサービスプロバイダを通過するのに必要な時間に起因するものである。

30

【0097】

ステップ422が偽である場合、制御はステップ404へ戻る。ステップ422が真である場合、プロバイダネットワークデバイスは、ステップ426において、コンテンツを鍵で暗号化又はスクランブルして、その暗号化又はスクランブルされたコンテンツをネットワークにより要求側デバイスへ送信し、制御はステップ404に続く。

40

【0098】

次に図10を参照して、リクエスタネットワークデバイスからのコピープロテクトされたファイルのプレイバックをN回許可するための方法のステップが示されている。制御はステップ600で開始する。ステップ602において、制御は、コピープロテクトされたファイルがリクエスタネットワークデバイスに記憶されているかどうか判断する。記憶されていないと判断した場合、制御はステップ602へ戻る。ステップ602が真である場合、制御は、ステップ604において、そのファイルにN=1を設定する。ステップ606において、制御は、リクエスタネットワークデバイスに記憶された、コピープロテクトされたファイルが再生されたかどうかを判断する。ステップ606が偽である場合、制御はステップ606へ戻る。ステップ606が真である場合、制御は、ステップ610において、Nをインクリメントする。ステップ614において、制御は、N=N_{max}であるかどうかを判断する。ステップ614が偽である場合、制御はステップ606へ戻る。ステップ614が真である場合、制御は、ステップ618において、コピープロテクトされ

50

たファイルを消去するか、又は、それ以外にそのファイルをリクエスタネットワークデバイスから利用不能にし、制御はステップ 602 へ戻る。

【0099】

次に図 11 を参照して、リクエスタネットワークデバイスに記憶された、コピープロテクトされたファイルを再生できる時間を制限するための方法のステップが示されている。制御はステップ 640 で開始する。ステップ 644 において、制御は、コピープロテクトされたファイルがリクエスタネットワークデバイスに記憶されているかどうか判断する。ステップ 644 が偽である場合、制御はステップ 644 へ戻る。ステップ 644 が真である場合、制御はステップ 646 に続き、タイマをセットする。ステップ 648 において、制御は、タイマが満了したかどうかを判断する。ステップ 648 が偽である場合、制御はステップ 648 へ戻る。ステップ 648 が真である場合、制御は、ステップ 652 において、コピープロテクトされたファイルをリクエスタネットワークデバイスから消去し、制御はステップ 644 に続く。タイマを説明したが、任意の使用量測定及び／又は比較を行うことができる。たとえば、日付及び／又は時刻のスタンプを使用して、現在の日付及び／又は時刻と比較することができる。さらに他のタイプの使用量データも当業者には明らかであろう。

【0100】

次に図 12A を参照して、プロバイダ 702 からリクエスタ 704 へ保護コンテンツを供給するのにメディアサーバ 700 を使用することができる。メディアサーバ 700、プロバイダ 702、及びリクエスタ 704 を接続するものとしてルータが示されているが、アドホックネットワークモード、ピアツーピアモード、他の手法等の他のネットワーク構成及び接続も使用することができるが、これらに限定されるものではない。いくつかの実施態様では、メディアサーバは、上述したようなローカル／リモートステータス判断モジュール 701 を含む。メディアサーバ 700 は、利用可能なコンテンツのリストをリクエスタ 704 に提供する。リクエスタ 704 はコンテンツを要求する。メディアサーバ 700 は、リクエスタがローカルネットワークに存在することを、上述した方法のいずれかで確認する。リクエスタ 704 がローカルネットワークに存在する場合、メディアサーバ 700 は、プロバイダ 702 にコンテンツを要求する。プロバイダ 702 は、コンテンツをリクエスタ 704 へ直接送信するか、又は、メディアサーバ 700 へ送信する。メディアサーバ 700 は、コンテンツをリクエスタ 704 へ送信する。

【0101】

次に図 12B 及び図 13 を参照して、メディアサーバ 700 は、DVD システム 710 から HDD システム 712 へ保護コンテンツを供給する。DVD システム 710 及び HDD システム 712 は、上述した実施形態で説明したように実施することができる。図 13 では、メディアサーバ 700 を、図示したようなネットワークで実施することができる。本明細書で説明した他のネットワーク構成、さらにはそれ以外のネットワーク構成等の他のネットワーク構成も検討することができる。メディアサーバは、有線形式又は無線形式でネットワークに接続することができる。

【0102】

次に図 14 を参照して、本発明によるメディアサーバによって実行されるステップを示すフローチャートが示されている。制御はステップ 720 において開始する。ステップ 722 において、制御は、サーバが、保護ファイルのコピーの要求をリクエスタから受信したかどうかを判断する。ステップ 722 が偽である場合、制御はステップ 722 へ戻る。ステップ 722 が真である場合、メディアサーバは、リクエスタがローカルステータスを有するかどうかを判断する。リクエスタのローカルステータスは、上述した方法のいずれかで判断することができる。真である場合、サーバは、プロバイダにファイルを要求し、ファイルをリクエスタへ送信する。或いは、プロバイダは、ファイルをリクエスタへ直接送信することもできる。

【0103】

当業者は、この時点で、上記説明から、本発明の広い教示をさまざまな形態で実施でき

10

20

30

40

50

ることを十分理解することができる。したがって、本発明は、その特定の例に関して説明されているが、他の変更は、図面、明細書、及び添付の特許請求の範囲を検討すると当業者には明らかであるので、本発明の真の範囲はそのように限定されるべきではない。

【図面の簡単な説明】

【0104】

【図1】ローカルネットワークの1つ又は2つ以上のリクエスタネットワークデバイスにデジタル保護コンテンツを提供するプロバイダネットワークデバイスの機能ブロック図。

【図2】モデムと通信する、本発明によるネットワーク接続された第1の例示のDVD及びHDDのシステムの機能ブロック図。

【図3】モデムと通信する、本発明によるネットワーク接続された第2の例示のDVD及びHDDのシステムの機能ブロック図。 10

【図4】モデムと通信する、本発明によるネットワーク接続された第3の例示のDVD及びHDDのシステムの機能ブロック図。

【図5】モデムと通信する、本発明によるネットワーク接続された第4の例示のDVD及びHDDのシステムの機能ブロック図。

【図6】HDDシステムを含む例示のリクエスタネットワークデバイスの機能ブロック図。 15

【図7A】読み出し専用オペレーションを有するDVDシステムを含む例示のプロバイダネットワークデバイスの機能ブロック図。

【図7B】読み出し/書き込みオペレーションを有するDVDシステムを含む例示のプロバイダネットワークデバイスの機能ブロック図。 20

【図7C】DVD/HDD結合システムを含むプロバイダネットワークデバイス又はリクエスタネットワークデバイスの機能ブロック図。

【図8】図6のHDDの不揮発性メモリのユーザアクセス可能セクション及び隠しセクションを示す図。

【図9A】プロバイダネットワークデバイス及び/又はリクエスタネットワークデバイスによって実行されるセキュリティのステップを示すフローチャート。

【図9B】プロバイダネットワークデバイス及び/又はリクエスタネットワークデバイスによって実行されるセキュリティのステップを示すフローチャート。

【図9C】プロバイダネットワークデバイス及び/又はリクエスタネットワークデバイスによって実行されるセキュリティのステップを示すフローチャート。 30

【図9D】プロバイダネットワークデバイス及び/又はリクエスタネットワークデバイスによって実行されるセキュリティのステップを示すフローチャート。

【図10】リクエスタネットワークデバイスからのコピープロテクトされたファイルのブレイバックをN回許可するための方法のステップを示すフローチャート。

【図11】リクエスタネットワークデバイスに記憶された、コピープロテクトされたファイルを再生できる時間を制限するための方法のステップを示すフローチャート。

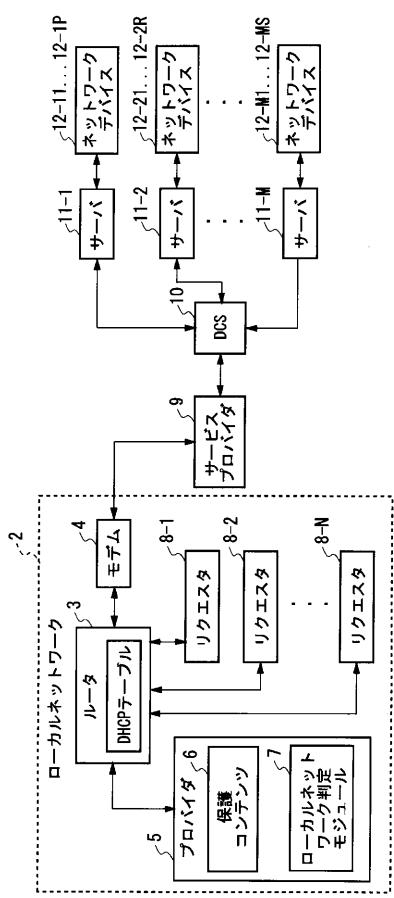
【図12A】プロバイダからリクエスタへ保護コンテンツを供給するメディアサーバを含むネットワークの機能ブロック図。

【図12B】DVDシステムからHDDシステムへ保護コンテンツを供給するメディアサーバを含むネットワークの機能ブロック図。 40

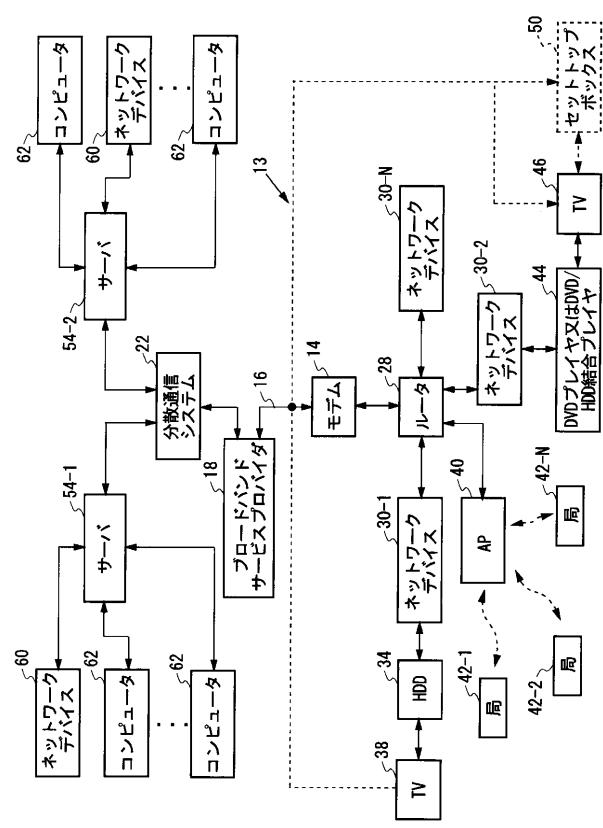
【図13】例示のネットワーク構成におけるメディアサーバを示す図。

【図14】本発明によるメディアサーバによって実行されるステップを示すフローチャート。

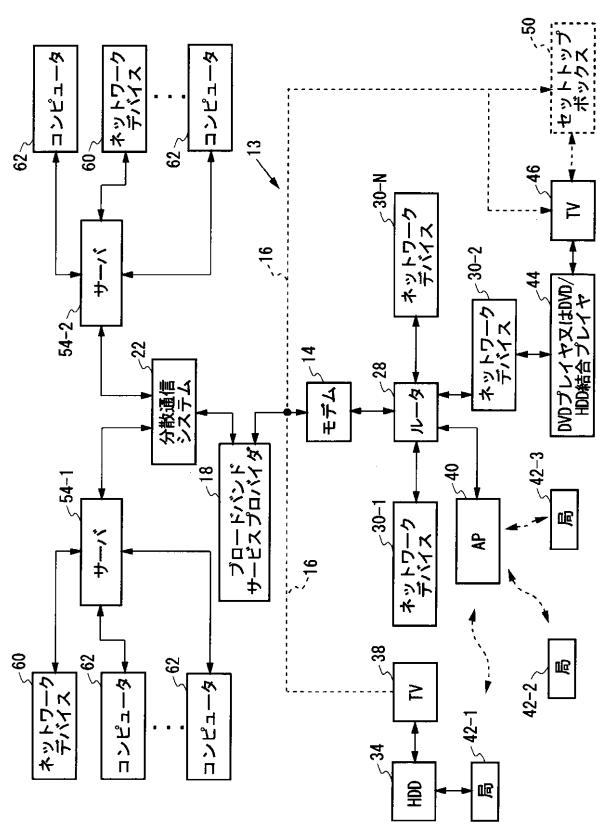
【図 1】



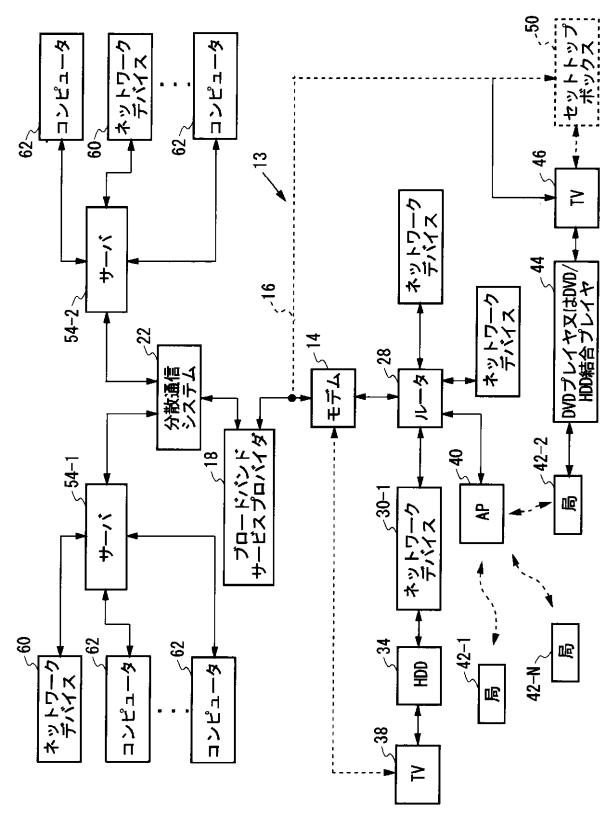
【図 2】



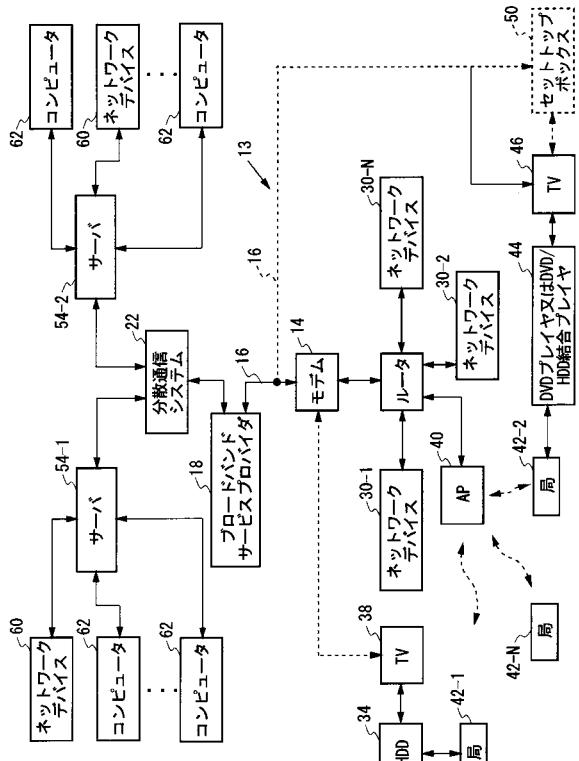
【図 3】



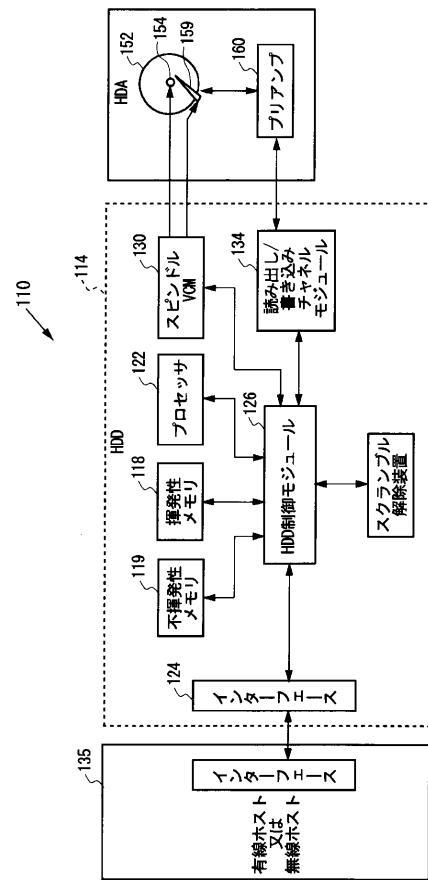
【図 4】



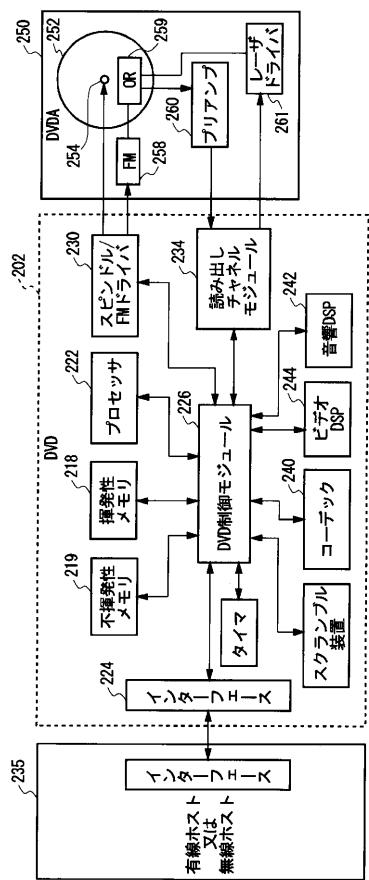
【 四 5 】



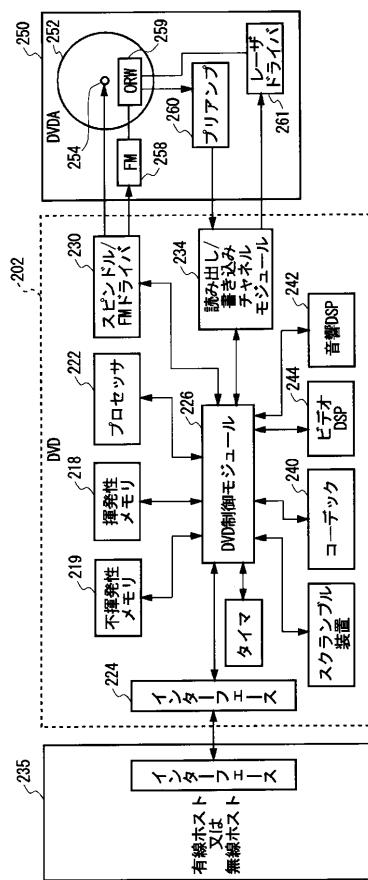
【 四 6 】



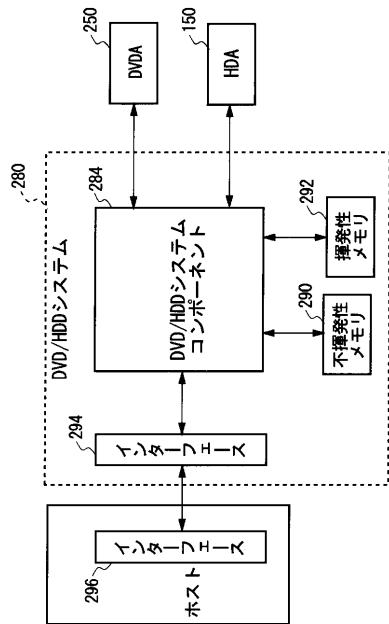
【 図 7 A 】



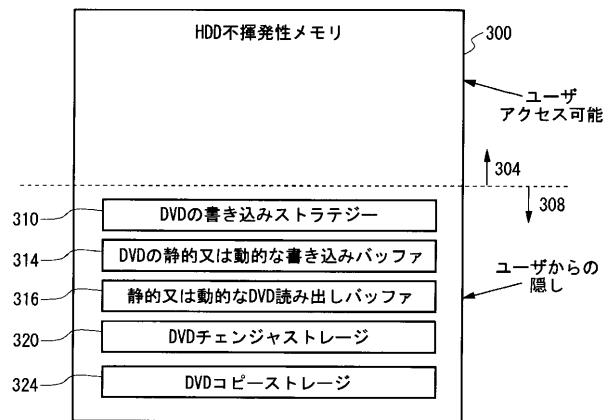
【 図 7 B 】



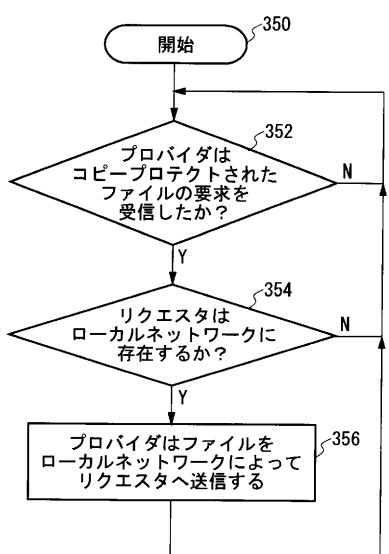
【図7C】



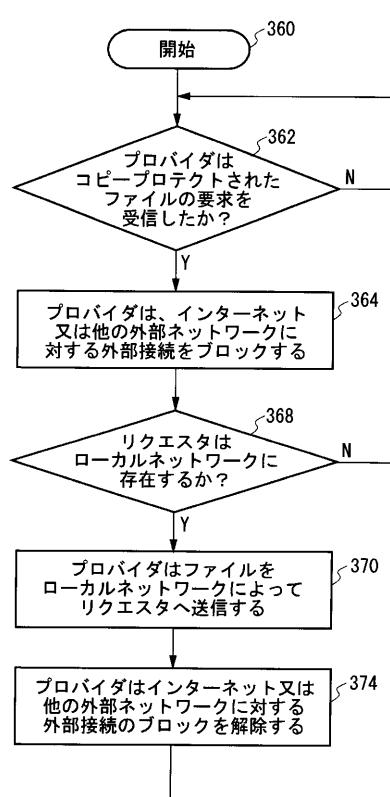
【図8】



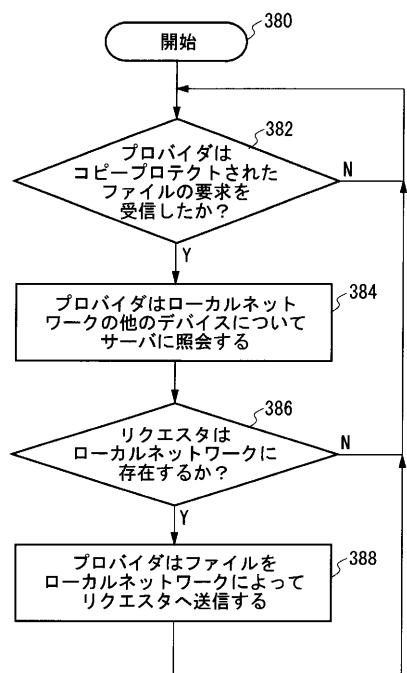
【図9A】



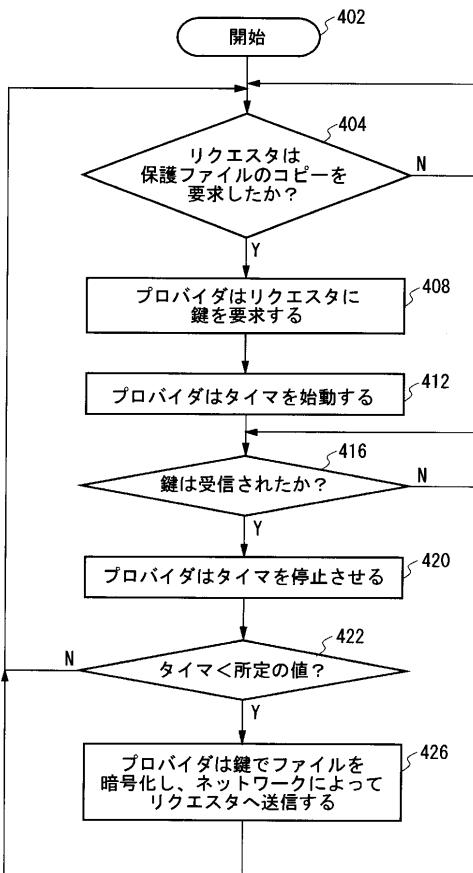
【図9B】



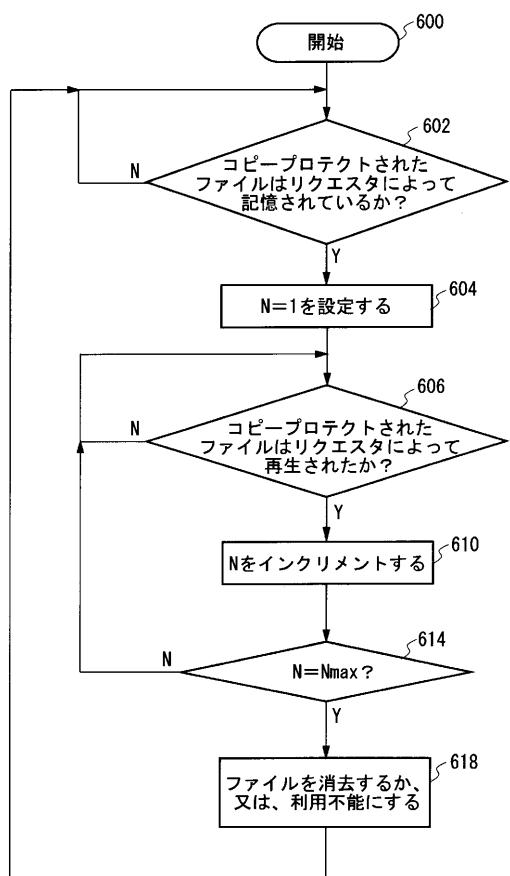
【図9C】



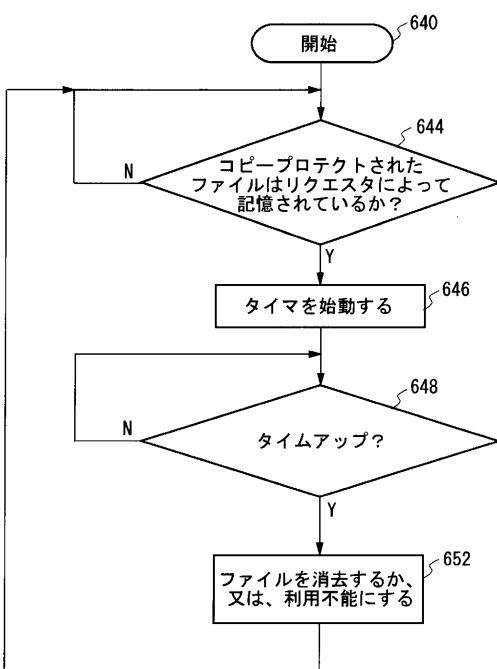
【図9D】



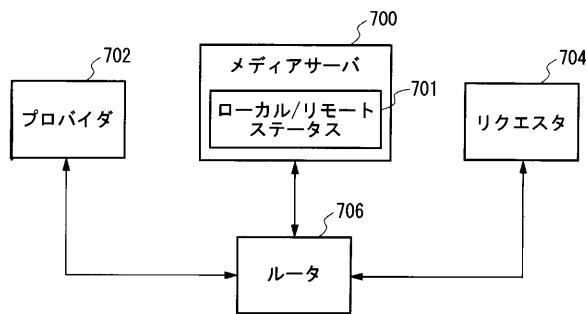
【図10】



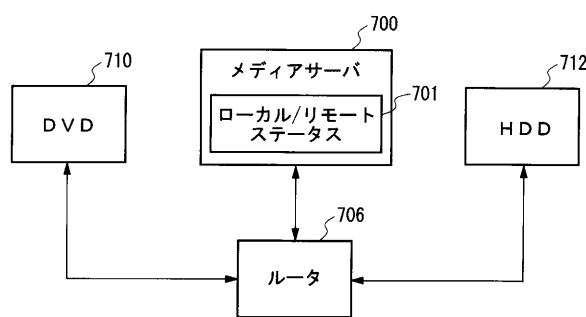
【図11】



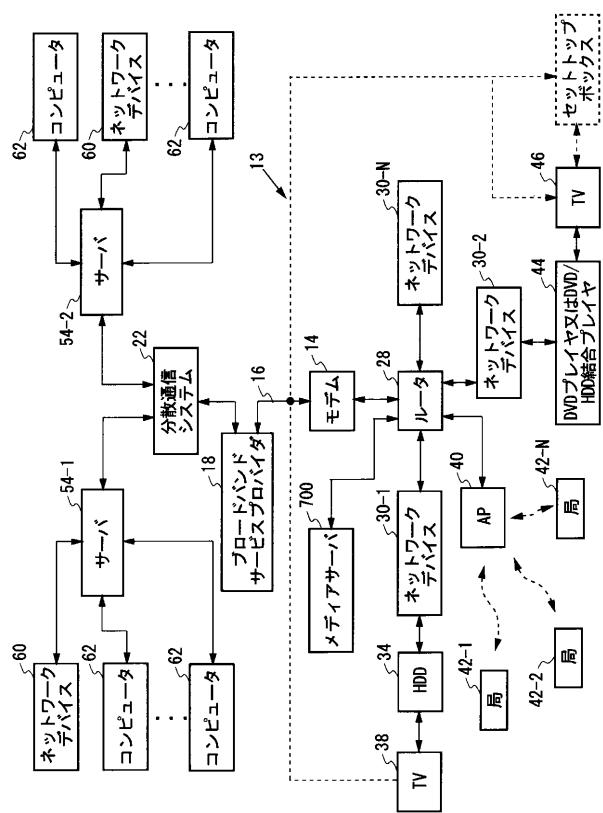
【 义 1 2 A 】



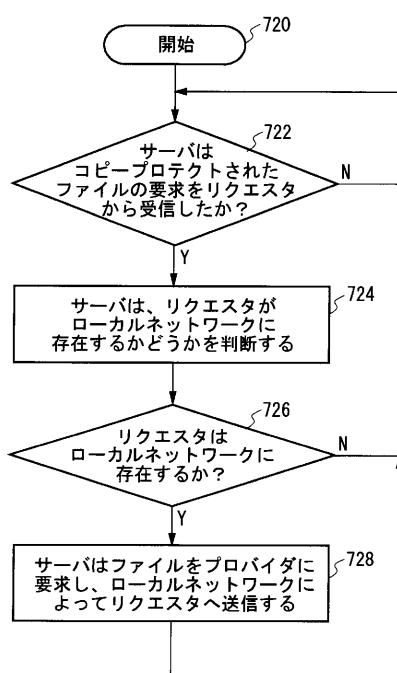
【 図 1 2 B 】



【図13】



【 図 1 4 】



【手続補正書】

【提出日】平成18年3月23日(2006.3.23)

【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】

ネットワークによってプロバイダネットワークデバイスと通信するハードディスクドライブ(HDD)システムであって

不揮発的な方法でユーザアクセス可能セクション及び隠しセクションにデータを記憶する不揮発性HDDメモリと、

前記HDD不揮発性メモリと通信し、前記プロバイダネットワークデバイスにコンテンツを選択的に要求して前記プロバイダネットワークデバイスからコンテンツを受信し、且つ、前記要求されたコンテンツを前記不揮発性HDDメモリの前記隠しセクションに記憶する、ハードディスクドライブ(HDD)制御モジュールと、

を備える、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項2】

前記要求を前記プロバイダネットワークデバイスへ送信した後、前記HDD制御モジュールは、鍵要求を受信し、該鍵要求に応答して、前記プロバイダネットワークデバイスへ鍵を送信する、請求項1に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項3】

前記プロバイダネットワークデバイスから前記HDDシステムによって受信された、前記要求されたコンテンツは、前記鍵を使用して暗号化される、請求項2に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項4】

前記HDD制御モジュールは、前記要求されたコンテンツを解読する、請求項3に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項5】

前記要求されたコンテンツは、同じく前記不揮発性HDDメモリの前記隠し部分に書き込まれる使用量データを含み、前記HDD制御モジュールは、前記使用量データが、許可された使用を超過したこと示すと、前記要求されたコンテンツを利用不能にする、請求項1に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項6】

前記HDDシステムは、前記要求されたコンテンツを前記不揮発性HDDメモリから消去する、請求項5に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項7】

前記使用量データは、許可された所定の使用回数を指定する、請求項5に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項8】

前記使用量データは、許可された使用期間を指定する、請求項5に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項9】

前記HDDシステムは、前記ネットワークと無線で通信する、請求項1に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項 10】

前記HDDシステムは、媒体によって前記ネットワークと通信する、請求項1に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項 11】

前記プロバイダネットワークデバイスは、デジタル多用途ディスク(DVD)システムを含む、請求項1に記載の、ネットワークによってプロバイダネットワークデバイスと通信するHDDシステム。

【請求項 12】

請求項11に記載の前記HDDシステムを備え、前記DVDシステム及び前記ネットワークをさらに備える、ネットワーク接続されたDVD/HDDシステム。

フロントページの続き

(51)Int.Cl.

F I

テーマコード(参考)

G 06 F 12/14 520 F

G 06 F 12/14 520 P

F ターム(参考) 5C053 FA13 FA15 FA23 FA24 GB11 GB21 JA22 LA06 LA11 LA15
5C164 UA22S UA53S UB37P
5D044 AB05 AB07 BC01 CC04 DE17 DE50 GK17 HL08 HL11

【外國語明細書】

HARD DISK DRIVE SYSTEM FOR DISTRIBUTING PROTECTED CONTENT

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of United States Patent Application No. 11/085,761 filed on March 21, 2005. This application is related to United States Patent Application No. 11/039,288 filed on January 19, 2005. The disclosures of the above applications are incorporated herein by reference in their entirety.

FIELD OF THE INVENTION

[0002] The present invention relates to networks, and more particularly to network systems that allow secure distribution of protected content.

BACKGROUND OF THE INVENTION

[0003] Consumers often purchase video content on digital versatile discs (DVDs). A DVD player may be used to output the video content to a television (TV) or other video monitor. Some DVD players may include a carousel for allowing selection and play of one of a plurality of DVDs. In some situations, a consumer may want to view the DVD content on a first TV in one room of the consumer's home when the DVD player is located and connected to a second TV in another room. As a result, the DVD player needs to be disconnected from the second TV, moved to the room with the first TV and

reconnected to the first TV. Alternately, if the consumer has a second DVD player, the consumer moves the DVD to the other player.

[0004] One possible solution to this problem involves copying the DVD content onto another DVD. DVD players typically include only one DVD player, which makes copying DVDs difficult. To copy the DVD, the user must copy the DVD contents to a hard drive system. Typically, copy protection schemes such as digital rights management (DRM) prevent such copying despite the fact that some copying may be allowed under the copyright laws. This is due, in part, to the fact that the data is decrypted and/or decoded by the DVD player and is therefore in an unprotected form when it is output to other devices. This solution also requires an additional DVD player.

SUMMARY OF THE INVENTION

[0005] A system for distributing content in a network comprises memory that stores content. A provider network device communicates with the memory. A requester network device requests a copy of the content. the provider network device determines a local/remote status of the requester network device and selectively sends a copy of the content to the requester network device when the requester network device requests content and has a local status.

[0006] In other features, the provider network device includes a digital versatile disc (DVD) system. The requester network device includes a hard disk drive (HDD) system. The provider network device includes a local network

determining module that determines the local/remote status of the requester network device. The provider network device determines the local/remote status based on a response time of the requester network device.

[0007] In other features, a server communicates with the provider network device and stores identification data of local network devices. The provider network device determines the local/remote status based on the identification data. The identification data comprises medium access control (MAC) addresses of the local network devices.

[0008] In other features, the HDD system comprises nonvolatile HDD memory that stores data in a nonvolatile manner and that includes a user accessible section and a hidden section. A hard disk drive control (HDD) module communicates with the HDD nonvolatile memory, selectively requests and receives content from the provider network device and stores the requested content in the hidden section of the nonvolatile HDD memory.

[0009] In other features, after sending the request to the provider network device, the HDD control module receives a key request and transmits a key to the provider network device in response to the key request. The requested content received by the HDD system from the provider network device is encrypted using the key. The HDD control module decrypts the requested content. The requested content includes usage data that is also written to the hidden portion of the nonvolatile HDD memory and wherein the HDD control module makes the requested content unavailable when the usage data indicates allowable use is over. The HDD system deletes the requested content from the

nonvolatile HDD memory. The usage data specifies a predetermined number of allowable uses. The usage data specifies a duration of allowable usage. The HDD system communicates wirelessly with the network. The HDD system communicates with the network over a wired medium.

[0010] In other features, the DVD system comprises nonvolatile memory that stores content. A DVD control module communicates with the nonvolatile memory and selectively receives requests for content from the requester network device. The DVD control module requests a key from the requester network device before sending the requested content and determines an amount of time that is required to receive the key from the HDD system after sending the key request to the HDD system. The DVD system sends the requested content to the HDD system if the key is received within a predetermined period. The predetermined period is approximately equal to a single or two-hop period. The DVD system encrypts the requested content before sending the requested content to the HDD system. The DVD control module includes usage data in the requested content that is transmitted to the HDD system. The usage data specifies a number of allowable uses. The usage data specifies a duration of allowable usage.

[0011] A system for distributing content in a network comprises memory means for storing content. Provider network means for providing communicates with the memory means. Requester network means requests a copy of the content. The provider network means determines a local/remote status of the requester network means and selectively sends a copy of the

content to the requester network means when the requester network means requests content and has a local status.

[0012] In other features, the provider network means includes a digital versatile disc (DVD) system. The requester network means includes a hard disk drive (HDD) system. The provider network means includes local network determining means for determining the local/remote status of the requester network means. The provider network means determines the local/remote status based on a response time of the requester network means. Server means for serving communicates with the provider network means and stores identification data of local network means. The provider network means determines the local/remote status based on the identification data. The identification data comprises medium access control (MAC) addresses of the local network means.

[0013] In other features, the HDD system comprises nonvolatile HDD memory means for storing data in a nonvolatile manner and that includes a user accessible section and a hidden section. Hard disk drive control (HDD) means communicates with the HDD nonvolatile memory means, selectively requests and receives content from the provider network means and stores the requested content in the hidden section of the nonvolatile HDD memory means. After sending the request to the provider network means, the HDD control means receives a key request and transmits a key to the provider network means in response to the key request. The requested content received by the HDD system from the provider network means is encrypted using the key. The HDD control means decrypts the requested content. The requested content includes

usage data that is also written to the hidden portion of the nonvolatile HDD memory means and wherein the HDD control means makes the requested content unavailable when the usage data indicates allowable use is over.

[0014] In other features, the HDD system deletes the requested content from the nonvolatile HDD memory means. The usage data specifies a predetermined number of allowable uses. The usage data specifies a duration of allowable usage. The HDD system communicates wirelessly with the network. The HDD system communicates with the network over a wired medium.

[0015] In other features, the DVD system comprises nonvolatile memory means for storing content. DVD control means communicates with the nonvolatile memory means and selectively receives requests for content from the requester network means. The DVD control means requests a key from the requester network means before sending the requested content and determines an amount of time that is required to receive the key from the HDD system after sending the key request to the HDD system. The DVD control means sends the requested content to the HDD system if the key is received within a predetermined period. The predetermined period is approximately equal to a single or two-hop period. The DVD control means encrypts the requested content before sending the requested content to the HDD system. The DVD control means includes usage data in the requested content that is transmitted to the HDD system. The usage data specifies a number of allowable uses. The usage data specifies a duration of allowable usage. The DVD system

communicates wirelessly with the network. The DVD system communicates with the network over a wired medium.

[0016] A method for distributing content in a network comprises storing content in memory; providing a provider network device that communicates with the memory; providing a requester network device that requests a copy of the content; determining a local/remote status of the requester network device; and selectively sending a copy of the content to the requester network device when the requester network device requests content and has a local status.

[0017] In other features, the provider network device includes a digital versatile disc (DVD) system. The requester network device includes a hard disk drive (HDD) system. The method includes determining the local/remote status of the requester network device. The method includes determining the local/remote status based on a response time of the requester network device. The method includes storing identification data of local network devices, wherein the provider network device determines the local/remote status based on the identification data. The method includes storing medium access control (MAC) addresses of the local network devices. The method includes storing data in a nonvolatile manner in user accessible and a hidden sections of the HDD system; selectively requesting and receiving content from the provider network device; and storing the requested content in the hidden section of the nonvolatile HDD memory.

[0018] In other features, the method includes receiving a key request and transmitting a key to the provider network device in response to the key request after sending the request to the provider network device. The method

includes encrypting the requested content received by the HDD system from the provider network device using the key. The method includes decrypting the requested content. The method includes writing the requested content includes usage data to the hidden portion of the nonvolatile HDD memory; and making the requested content unavailable when the usage data indicates allowable use is over.

[0019] In yet other features, the method includes deleting the requested content from the nonvolatile HDD memory. The method includes specifying a predetermined number of allowable uses using the usage data. The method includes specifying a duration of allowable usage using the usage data. The method includes storing content; and selectively receiving requests for content from the requester network device. The method includes requesting a key from the requester network device before sending the requested content; and determining an amount of time that is required to receive the key from the HDD system after sending the key request to the HDD system.

[0020] In other features, the method includes sending the requested content to the HDD system if the key is received within a predetermined period. The predetermined period is approximately equal to a single or two-hop period. The method includes encrypting the requested content before sending the requested content to the HDD system. The method includes transmitting usage data in the requested content to the HDD system. The usage data specifies a number of allowable uses. The usage data specifies a duration of allowable usage.

[0021] A hard disk drive (HDD) system that communicates with a provider network device over a network comprises nonvolatile HDD memory that stores data in a nonvolatile manner in user accessible and hidden sections. A hard disk drive control (HDD) module communicates with the HDD nonvolatile memory, selectively requests and receives content from the provider network device and stores the requested content in the hidden section of the nonvolatile HDD memory.

[0022] In other features, after sending the request to the provider network device, the HDD control module receives a key request and transmits a key to the provider network device in response to the key request. The requested content received by the HDD system from the provider network device is encrypted using the key. The HDD control module decrypts the requested content. The requested content includes usage data that is also written to the hidden portion of the nonvolatile HDD memory and wherein the HDD control module makes the requested content unavailable when the usage data indicates allowable use is over. The HDD system deletes the requested content from the nonvolatile HDD memory. The usage data specifies a predetermined number of allowable uses. The usage data specifies a duration of allowable usage. The HDD system communicates wirelessly with the network. The HDD system communicates with the network over a medium.

[0023] In other features, the provider network device includes a digital versatile disc (DVD) system. A networked DVD/HDD system comprises the HDD system and further comprises the DVD system and the network.

[0024] A hard disk drive (HDD) system that communicates with a provider network device over a network comprises nonvolatile memory means for storing data in a nonvolatile manner in user accessible and hidden sections. Control means communicates with the nonvolatile memory means, selectively requests and receives content from the provider network device and stores the requested content in the hidden section of the nonvolatile memory means.

[0025] After sending the request to the provider network device, the control means receives a key request and transmits a key to the provider network device in response to the key request. The requested content received by the system from the provider network device is encrypted using the key. The control means decrypts the requested content. The requested content includes usage data that is also written to the hidden portion of the nonvolatile memory means and wherein the control means makes the requested content unavailable when the usage data indicates allowable use is over.

[0026] In other features, the system deletes the requested content from the nonvolatile memory means. The usage data specifies a predetermined number of allowable uses. The usage data specifies a duration of allowable usage. The HDD system communicates wirelessly with the network. The HDD system communicates with the network over a medium.

[0027] In other features, the provider network device includes a digital versatile disc (DVD) system. A networked DVD/HDD system comprises the HDD system and further comprises the DVD system and the network.

[0028] A method for operating a hard disk drive (HDD) system that communicates with a provider network device over a network comprises storing data in a nonvolatile manner in user accessible and hidden sections; selectively requesting and receiving content from the provider network device; and storing the requested content in the hidden section.

[0029] In other features, the method includes receiving a key request and transmitting a key to the provider network device in response to the key request after sending the request to the provider network device. The method includes encrypting the requested content received by the HDD system from the provider network device using the key. The method includes decrypting the requested content. The method includes writing requested content including usage data to the hidden portion; and making the requested content unavailable when the usage data indicates allowable use is over. The method includes deleting the requested content from the hidden section. The method includes specifying a predetermined number of allowable uses using the usage data. The method includes specifying a duration of allowable usage using the usage data.

[0030] A digital versatile disc (DVD) system that communicates with a requester network device over a network comprises nonvolatile memory that stores content. A control module communicates with the nonvolatile memory, selectively receives requests for content from the requester network device, determines a local/remote status, sends the requested content if the requester network device has a local status and that does not send the requested content if the requester network device has a remote status.

[0031] In other features, the control module requests a key from the requester network device before sending the requested content. The control module determines an amount of time that is required to receive the key from the requester network device after sending the key request. The control module sends the requested content to the requester network device if the key is received within a predetermined period. The predetermined period is approximately equal to a single or two-hop period. The control module encrypts the requested content before sending the requested content to the requester network device. The control module includes usage data in the requested content that is transmitted to the requester network device. The usage data specifies a number of allowable uses. The usage data specifies a duration of allowable usage. The DVD system communicates wirelessly with the network. The DVD system communicates with the network over a medium.

[0032] In other features, the requester network device includes a hard disk drive (HDD) system. A networked DVD/HDD system comprises the DVD system and further comprises the HDD system and the network.

[0033] A digital versatile disc (DVD) system that communicates with a hard requester network device over a network comprises nonvolatile memory means that stores content. Control means communicates with the nonvolatile memory means, selectively receives requests for content from the requester network device, determines a local/remote status, sends the requested content if the requester network device has a local status and does not sends the requested content if the requester network device has a remote status.

[0034] In other features, the control means requests a key from the requester network device before sending the requested content. The control means determines an amount of time that is required to receive the key from the requester network device after sending the key request. The control module sends the requested content to the requester network device if the key is received within a predetermined period. The predetermined period is approximately equal to a two-hop period. The predetermined period is approximately equal to a single-hop period. The control module encrypts the requested content before sending the requested content to the requester network device. The control means includes usage data in the requested content that is transmitted to the requester network device. The usage data specifies a number of allowable uses. The usage data specifies a duration of allowable usage. The control module communicates wirelessly with the network. The DVD system communicates with the network over a medium.

[0035] In other features, the requester network device includes a hard disk drive (HDD) system. A networked DVD/HDD system comprises the DVD system and further comprises the HDD system and the network.

[0036] A method for operating a digital versatile disc (DVD) system that communicates with a hard requester network device over a network comprises storing content in nonvolatile memory; selectively receiving requests for content from the requester network device; determining a local/remote status; sending the requested content if the requester network device has a local status; and not

sending the requested content if the requester network device has a remote status.

[0037] In other features, the method includes requesting a key from the requester network device before sending the requested content. The method includes determining an amount of time that is required to receive the key from the requester network device after sending the key request. The method includes sending the requested content to the requester network device if the key is received within a predetermined period. The method includes setting the predetermined period approximately equal to a two-hop period. The method includes setting the predetermined period approximately equal to a single-hop period. The method includes encrypting the requested content before sending the requested content to the requester network device. The method includes including usage data in the requested content that is transmitted to the requester network device. The usage data specifies a number of allowable uses. The usage data specifies a duration of allowable usage.

[0038] A system for distributing content in a network comprises memory that stores content and a provider network device that communicates with the memory. A media server communicates with the provider network device. A requester network device requests a copy of the content. The media server determines a local/remote status of the requester network device and selectively enables the provider network device to send a copy of the content to the requester network device when the requester network device requests content and has a local status.

[0039] In other features, the provider network device includes a digital versatile disc (DVD) system. The requester network device includes a hard disk drive (HDD) system. The media server includes a local network determining module that determines the local/remote status of the requester network device. The media server determines the local/remote status based on a response time of the requester network device.

[0040] In other features, a server communicates with the media server and stores identification data of local network devices. The media server determines the local/remote status based on the identification data. Alternately, the media server stores identification data of local network devices, wherein the media server determines the local/remote status based on the identification data. The identification data comprises medium access control (MAC) addresses of the local network devices.

[0041] In other features, the HDD system comprises nonvolatile HDD memory that stores data in a nonvolatile manner and that includes a user accessible section and a hidden section. A hard disk drive control (HDD) module communicates with the HDD nonvolatile memory, selectively requests content from the media server and receives content from at least one of the provider network device and/or the media server and stores the requested content in the hidden section of the nonvolatile HDD memory. After sending the request to the media server, the HDD control module receives a key request and transmits a key to at least one of the media server and/or the provider network device in response to the key request. The requested content received by the HDD

system from at least one of the provider network device and/or the media server is encrypted using the key. The HDD control module decrypts the requested content. The requested content includes usage data that is also written to the hidden portion of the nonvolatile HDD memory. The HDD control module makes the requested content unavailable when the usage data indicates allowable use is over. The HDD system deletes the requested content from the nonvolatile HDD memory. The usage data specifies a predetermined number of allowable uses. The usage data specifies a duration of allowable usage. The HDD system communicates wirelessly with the network. The HDD system communicates with the network over a wired medium.

[0042] The DVD system comprises nonvolatile memory that stores content. A DVD control module communicates with the nonvolatile memory, and selectively receives requests for content from at least one of the requester network device and/or the media server. The media server requests a key from the requester network device before sending the requested content and determines an amount of time that is required to receive the key from the HDD system after sending the key request to the HDD system. The media server enables the DVD system to send the requested content to at least one of the HDD system and/or the media server if the key is received within a predetermined period. The predetermined period is approximately equal to a two-hop period. The predetermined period is approximately equal to a single-hop period.

[0043] In other features, at least one of the DVD system and/or the media server encrypts the requested content before sending the requested content to the HDD system. At least one of the DVD control module and/or the media server includes usage data in the requested content that is transmitted to the HDD system. The usage data specifies a number of allowable uses. The usage data specifies a duration of allowable usage. The DVD system communicates wirelessly with the network. The DVD system communicates with the network over a wired medium.

[0044] A system for distributing content in a network comprises memory means for storing content. Provider network means for providing communicates with the memory means. Media serving means for serving communicates with the provider network means. Requester network means requests a copy of the content. The media serving means determines a local/remote status of the requester network means and selectively enables the provider network means to send a copy of the content to the requester network means when the requester network means requests content and has a local status.

[0045] In other features, the provider network means includes a digital versatile disc (DVD) system. The requester network means includes a hard disk drive (HDD) system. The media serving means includes local network determining means for determining the local/remote status of the requester network means. The media serving means determines the local/remote status based on a response time of the requester network means. Server means for

serving communicates with the provider network means and stores identification data of local network means. The media serving means determines the local/remote status based on the identification data. Alternately, the media serving means stores identification data of local network means. The identification data comprises medium access control (MAC) addresses of the local network means.

[0046] In other features, the HDD system comprises nonvolatile HDD memory means for storing data in a nonvolatile manner and that includes a user accessible section and a hidden section. Hard disk drive control (HDD) means communicates with the HDD nonvolatile memory means, selectively requests and receives content from the media serving means and stores the requested content in the hidden section of the nonvolatile HDD memory means. After sending the request to the media serving means, the HDD control means receives a key request and transmits a key to at least one of the provider network means and the media serving means in response to the key request. The requested content received by the HDD system from at least one of the provider network means and/or the media serving means is encrypted using the key. The HDD control means decrypts the requested content. The requested content includes usage data that is also written to the hidden portion of the nonvolatile HDD memory means and the HDD control means makes the requested content unavailable when the usage data indicates allowable use is over. The HDD system deletes the requested content from the nonvolatile HDD memory means. The usage data specifies a predetermined number of allowable uses. The usage

data specifies a duration of allowable usage. The HDD system communicates wirelessly with the network. The HDD system communicates with the network over a wired medium.

[0047] In other features, the DVD system comprises nonvolatile memory means for storing content DVD control means that communicates with the nonvolatile memory means, for selectively receiving requests for content from the media serving means. The media serving means requests a key from the requester network means before sending the requested content and determines an amount of time that is required to receive the key from the HDD system after sending the key request to the HDD system. At least one of the DVD control means and/or the media serving means sends the requested content to the HDD system if the key is received within a predetermined period. The predetermined period is approximately equal to a two-hop period. The predetermined period is approximately equal to a single-hop period. At least one of the DVD control means and the media serving means encrypts the requested content before sending the requested content to the HDD system. At least one of the DVD control means and/or the media serving means includes usage data in the requested content that is transmitted to the HDD system. The usage data specifies a number of allowable uses. The usage data specifies a duration of allowable usage. The DVD system communicates wirelessly with the network. The DVD system communicates with the network over a wired medium.

[0048] A method for distributing content in a network comprises storing content in memory; providing a provider network device that communicates with

the memory; proving a media serving device that communicates with the provider network device; providing a requester network device that requests a copy of the content; determining a local/remote status of the requester network device using the media serving device; and selectively sending a copy of the content to the requester network device when the requester network device requests content and has a local status.

[0049] In other features, the provider network device includes a digital versatile disc (DVD) system. The requester network device includes a hard disk drive (HDD) system. The method includes determining the local/remote status of the requester network device. The method includes determining the local/remote status based on a response time of the requester network device. The method includes storing identification data of local network devices. The media serving device determines the local/remote status based on the identification data. The method includes storing medium access control (MAC) addresses of the local network devices.

[0050] In other features, the method includes storing data in a nonvolatile manner in user accessible and hidden sections of the HDD system; selectively requesting and receiving content from the provider network device via the media serving device; and storing the requested content in the hidden section of the nonvolatile HDD memory.

[0051] In other features, the method includes receiving a key request and transmitting a key to the media serving device in response to the key request after sending the request to the media serving device. The method includes

encrypting the requested content received by the HDD system from at least one of the provider network device and/or the media serving device using the key. The method includes decrypting the requested content. The method includes writing the requested content includes usage data to the hidden portion of the nonvolatile HDD memory; and making the requested content unavailable when the usage data indicates allowable use is over.

[0052] In other features, the method includes deleting the requested content from the nonvolatile HDD memory. The method includes specifying a predetermined number of allowable uses using the usage data. The method includes specifying a duration of allowable usage using the usage data.

[0053] The method includes storing content in the provider network device; and selectively receiving requests for content from the requester network device via the media serving device. The method includes requesting a key from the requester network device before sending the requested content; and determining an amount of time that is required to receive the key from the HDD system after sending the key request to the HDD system. The method includes sending the requested content to the HDD system if the key is received within a predetermined period. The predetermined period is approximately equal to a two-hop period. The predetermined period is approximately equal to a single-hop period. The method includes encrypting the requested content before sending the requested content to the HDD system. The method includes transmitting usage data in the requested content to the HDD system. The usage

data specifies a number of allowable uses. The usage data specifies a duration of allowable usage.

[0054] Further areas of applicability of the present invention will become apparent from the detailed description provided hereinafter. It should be understood that the detailed description and specific examples, while indicating the preferred embodiment of the invention, are intended for purposes of illustration only and are not intended to limit the scope of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0055] The present invention will become more fully understood from the detailed description and the accompanying drawings, wherein:

[0056] FIG. 1 is a functional block diagram of a provider network device that provides protected digital content to one or more requester network devices in a local network;

[0057] FIG. 2 is a functional block diagram of a first exemplary networked DVD and HDD system according to the present invention that communicates with a modem;

[0058] FIG. 3 is a functional block diagram of a second exemplary networked DVD and HDD system according to the present invention that communicates with a modem;

[0059] FIG. 4 is a functional block diagram of a third exemplary networked DVD and HDD system according to the present invention that communicates with a modem;

[0060] FIG. 5 is a functional block diagram of a fourth exemplary networked DVD and HDD system according to the present invention that communicates with a modem;

[0061] FIG. 6 is a functional block diagram of an exemplary requester network device including a HDD system;

[0062] FIG. 7A is a functional block diagram of an exemplary provider network device including a DVD system with read-only operation;

[0063] FIG. 7B is a functional block diagram of an exemplary provider network device including a DVD system with read-write operation;

[0064] FIG. 7C is a functional block diagram of a provider or requester network device that includes a combined DVD/HDD system;

[0065] FIG. 8 illustrates user accessible and hidden sections of nonvolatile memory of the HDD of FIG. 6;

[0066] FIGs. 9A-9D are flowcharts illustrating security steps performed by the provider and/or requester network devices;

[0067] FIG. 10 is a flowchart illustrating steps of a method for allowing playback of a copy protected file from the requester network device N times;

[0068] FIG. 11 is a flowchart illustrating steps of a method for limiting the amount of time that a copy protected file stored on the requester network device can be played;

[0069] FIG. 12A is a functional block diagram of a network including a media server that serves protected content from a provider to a requester;

[0070] FIG. 12B is a functional block diagram of a network including a media server that serves protected content from a DVD system to a HDD system;

[0071] FIG. 13 illustrates the media server in an exemplary network configuration; and

[0072] FIG. 14 is a flowchart illustrating steps performed by the media server according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0073] The following description of the preferred embodiment(s) is merely exemplary in nature and is in no way intended to limit the invention, its application, or uses. As used herein, the term module or device refers to an application specific integrated circuit (ASIC), an electronic circuit, a processor (shared, dedicated, or group) and memory that execute one or more software or firmware programs, a combinational logic circuit, and/or other suitable components that provide the described functionality. For purposes of clarity, the same reference numbers will be used in the drawings to identify similar elements.

[0074] Referring now to FIG. 1, a local network 2 includes a router 3, a modem 4, and a provider network device 5, which selectively provides protected content 6 to one or more local requester network devices as will be described below. The provider network device 5 is a network compatible device that includes a local network determining module 7. One or more requester network devices 8-1, 8-2, ... and 8-N (collectively referred to as requesters 8) selectively

request copies of the protected content 6. As can be appreciated, while the router 3 and wire line connections are shown, other network configurations will be apparent to skilled artisans including but not limited to wireless Access Points (AP), ad-hoc network connection configurations, and/or wireless network configurations. While the provider network device 5 is shown to include memory such as nonvolatile memory for the protected content 6, the protected content 6 may be stored internally and/or externally from the provider network device 5.

[0075] The modem 4 is connected to a broadband service provider 9, which provides video content, digital content, a broadband connection to a distributed communications system (DCS) 10, and/or other network services. The service provider 9 may provide broadband access using wired or wireless connections, coaxial cable, digital subscriber line (DSL), satellite and/or any other connection system or method.

[0076] The DCS 10 is connected by one or more servers 11-1, 11-2, ..., and 11-M to network devices 12-11, 12-12, ..., 12-1P, 12-21, 12-22, ..., 12-2P, ..., and 12-M1, 12-M2, ..., 12-MP (collectively referred to as network devices 12). The local network determining module 7 selectively determines whether the requester network device has a local or remote status when the requester network device requests a copy of the protected content 6. This approach increases security by preventing access to the protected content by remote network devices.

[0077] There are many different ways for the local network determining module 7 to determine the local/remote status of a requester network device.

For example in some implementations, the provider network device 5 determines local/remote status by determining the amount of time that is required to receive a response from the requester network device. If the response time is less than a predetermined period, then the requester network device is determined to have a local status. If not, the requester network device has a remote status and the copy of the protected content is denied. The amount of time that is required to send and receive data via the service provider 9, DCS 10 and servers 11 to the remote network devices 12 is significantly greater than the amount of timer required by a local requester network device to respond. In other words, the predetermined period is set greater than the response time required by local requester network devices and less than the response time required by remote requester network devices.

[0078] In other implementations, the provider network device checks a dynamic host configuration protocol (DHCP) table in a DHCP server to determine medium access control (MAC) addresses of local network devices. If the requester network device matches a local MAC address in the table, then the requester network device has a local status and the copy of the protected content can be sent. If not, the requester network device has a remote status and the copy of the protected content is not sent.

[0079] In still other implementations, the provider network device 5 may send a message to the router 3 to temporarily block external ports of the router 3 or modem 4 to the service provider 9 (and DCS 10). After blocking the external ports, the provider network device 5 determines whether the requester network

device is still able to communicate (which will be true if the requester network device has a local status). If the provider network device can communicate with the requesting network device, the provider network device sends the copy protected content. As can be appreciated by skilled artisans, one or more of these approaches may be combined and/or other approaches may be used to determine the local/remote status of the requester network device.

[0080] While portions of the following description employ a DVD system and/or a combined DVD/HDD system as the provider network device and another network device including a combined DVD/HDD system and/or a HDD system as the requester network device, skilled artisans will appreciate that other provider and/or requester network devices may be used. Skilled artisans will also appreciate that all of the implementations that are described below in conjunction with DVD and HDD systems can be implemented with any other suitable network devices.

[0081] Referring now to FIG. 2, a functional block diagram of a first exemplary networked DVD and HDD system is shown. A local network 13 includes a modem 14 that communicates over medium 16 with a service provider 18. The service provider 18 provides a connection to a distributed communications system (DCS) 22 such as the Internet, LAN, WAN, or other distributed network and/or provides other network services such as video content, telephone services and the like. The modem 14 can be connected to a router 28, which connects multiple network devices 30-1, 30-2, ..., and 30-N (collectively network devices 30) to the modem 14. One of the network devices

30-1 is connected to a hard disk drive (HDD) system 34, which may be connected to a television or monitor 38. The television or monitor 38 may also be connected to the medium 16 either directly or through a set top box (not shown) and receive content from the service provider 18.

[0082] The local network 13 may include an access point (AP) 40 that communicates with the router 28 and one or more wireless stations 42-1, 42-2, ..., and 42-N (collectively wireless stations 42). While the AP 40 is shown connected to the router 28, the AP and router functions may be combined in a single device. Alternately, a combined AP/router may be directly connected to the modem 14. Still other types of network configurations and connections will be apparent to skilled artisans.

[0083] The network device 30-2 communicates with the router 28 and with a DVD player or a combined DVD/HDD player 44 (both referred to hereinafter as "DVD player 44") such as the one shown and described in U.S. Patent Application Serial No. 11/039,288, filed January 19, 2005, which is hereby incorporated by reference in its entirety. The DVD player 44, in turn, may communicate with a television or monitor 46, which may be connected to the medium 16 or to a set top box 50. The service provider 18 provides broadband access to the DCS 22, video content and/or other services. One or more other servers 54-1 and 54-2, (collectively servers 54) provide an interface for network devices 60, computers 62, personal digital assistants (PDAs), etc. to the DCS 22.

[0084] In some implementations, the user of the television or monitor 38 may desire access to DVD content associated with the DVD player 44.

Initially, the HDD 34 may request a list of available content from the DVD player.

The DVD sends a list of available content. The HDD 34 sends a message to the DVD player 44 via the network requesting a copy of content selected from the list. The DVD system determines whether the HDD system has a local status. If the HDD system or other requester network device has local status, the content file is sent. If the HDD system or other requester network device has a remote status, the request is denied. The local/remote status determination can be made based upon response time, MAC addresses in the DHCP table, external port disconnection and corresponding dialogue, and/or other suitable methods.

[0085] In some implementations, the DVD 44 responds by requesting a key from the HDD 34. The DVD 44 begins a timer that determines the amount of time that is required by the HDD 34 to respond. The HDD 34 sends the requested key to the DVD 44. The DVD 44 determines whether the HDD 34 responded within a predetermined amount of time.

[0086] If the HDD 34 responds within the predetermined amount of time, the DVD 44 scrambles the selected content with the key and sends the scrambled content over the network to the HDD 34. The HDD 34 descrambles the content with the key and allows replay of the content at the television or monitor 38. As can be appreciated, the key exchange can also occur earlier when the HDD initially requests the list of available content.

[0087] The HDD 34 may also receive usage data from the DVD player that constrains use. For example, the usage data may allow N replays and/or replay for a predetermined period. After the allowed usage period is over as

specified in the usage data, the HDD 34 makes the video content unavailable.

For example, the HDD may delete the video content.

[0088] In some implementations, the HDD 34 includes a user accessible section and a hidden section. The video content from the DVD 44 is stored in the hidden section of the DVD 44. The key that is provided by the HDD 34 may be part of a public/private key encryption system and/or other suitable data encryption. Alternately other forms of key-based scrambling can be performed.

[0089] If the DVD player is a single DVD player, the DVD sends a list of content available on the DVD in the DVD player. If the DVD player includes a carousel, the DVD player sends a list of DVD content available from DVDs in the carousel. If the DVD player is a combined DVD/HDD player, the DVD/HDD player sends a list of DVD content available on the DVD or DVDs in the player along with DVD content stored on the associated HDD.

[0090] Referring now to FIGs. 3-5, various exemplary configurations of the present invention are shown. In these implementations, the provider network device includes a DVD system and/or a combined DVD/HDD system and the requester network device includes a HDD system and/or a combined DVD/HDD system. In FIG. 3, the HDD 34 is connected to the network by the station 42-1, which wirelessly communicates with the AP 40. The DVD 44 and television 46 are connected by the network device 30-2 and medium 16 to the router 28. In FIG. 4, the HDD 34 is connected by the network device 30-1 and medium 16 to the router 28. The DVD 44 is connected to the network by the station 42-2,

which wirelessly communicates with the AP 40. In FIG. 5, the HDD 34 and DVD 44 are connected by one or more stations 42-1 and/or 42-2 to the network. Various other network configurations will be apparent to skilled artisans.

[0091] Referring now to FIG. 6, an exemplary requester network device includes a HDD system 110 with a HDD PCB 114. A buffer 118 stores read, write and/or volatile control data that is associated the control of the HDD system 110. The buffer 118 usually employs volatile memory having low latency. For example, SDRAM or other types of low latency memory may be used. Nonvolatile memory 119 such as flash memory may also be provided to store critical data such as nonvolatile control code.

[0092] A processor 122 arranged on the HDD PCB 114 performs data and/or control processing that is related to the operation of the HDD system 110. A hard disk control module (HDC) 126 communicates with an input/output interface 124 and with a spindle/voice coil motor (VCM) driver or module 130 and/or a read/write channel module 134. The HDC 126 coordinates control of the spindle/VCM driver 130, the read/write channel module 134 and the processor 122 and data input/output with a host 135 via the interface 124.

[0093] During write operations, the read/write channel module 134 encodes the data to be written onto a read/write device 159. The read/write channel module 134 processes the write signal for reliability and may apply, for example, error correction coding (ECC), run length limited coding (RLL), and the like. During read operations, the read/write channel module 134 converts an analog read signal output of the read/write device 159 to a digital read signal.

The converted signal is then detected and decoded by known techniques to recover the data that was written on the HDD.

[0094] A hard disk drive assembly (HDDA) 150 includes one or more hard drive platters 152 that include magnetic coatings that store magnetic fields. The platters 152 are rotated by a spindle motor that is schematically shown at 154. Generally the spindle motor 154 rotates the hard drive platter 152 at a controlled speed during the read/write operations. One or more read/write arms 158 move relative to the platters 152 to read and/or write data to/from the hard drive platters 152. The spindle/VCM driver 130 controls the spindle motor 154, which rotates the platter 152. The spindle/VCM driver 130 also generates control signals that position the read/write arm 158, for example using a voice coil actuator, a stepper motor or any other suitable actuator.

[0095] The read/write device 159 is located near a distal end of the read/write arm 158. The read/write device 159 includes a write element such as an inductor that generates a magnetic field. The read/write device 159 also includes a read element (such as a magneto-resistive (MR) element) that senses the magnetic field on the platter 152. The HDDA 150 includes a preamp circuit 160 that amplifies the analog read/write signals. When reading data, the preamp circuit 160 amplifies low level signals from the read element and outputs the amplified signal to the read/write channel module 134. While writing data, a write current is generated that flows through the write element of the read/write device 159. The write current is switched to produce a magnetic field having a positive

or negative polarity. The positive or negative polarity is stored by the hard drive platter 152 and is used to represent data.

[0096] Referring now to FIGs. 7A and 7B, an exemplary provider network device includes a DVD system 210. A DVD PCB 214 includes a buffer 218 that stores read data, write data and/or volatile control code that is associated the control of the DVD system 210. The buffer 218 may employ volatile memory such as SDRAM or other types of low latency memory. Nonvolatile memory 219 such as flash memory can also be used for critical data such as data relating to DVD write formats and/or other nonvolatile control code. A processor 222 arranged on the DVD PCB 214 performs data and/or control processing that is related to the operation of the DVD system 210. The processor 222 also performs decoding of copy protection and/or compression/decompression as needed. A DVD control module 226 communicates with an input/output interface 224 and with a spindle/feed motor (FM) driver 230 and/or a read/write channel module 234. The DVD control module 226 coordinates control of the spindle/FM driver, the read/write channel module 234 and the processor 222 and data input/output via the interface 224.

[0097] During write operations, the read/write channel module 234 encodes the data to be written by an optical read/write (ORW) or optical read only (OR) device 259 to the DVD platter. The read/write channel module 234 processes the signals for reliability and may apply, for example, ECC, RLL, and the like. During read operations, the read/write channel module 234 converts an analog output of the ORW or OR device 259 to a digital signal. The converted

signal is then detected and decoded by known techniques to recover the data that was written on the DVD.

[0098] A DVD assembly (DVDA) 250 includes a DVD platter 252 that stores data optically. The platter 252 is rotated by a spindle motor that is schematically shown at 254. The spindle motor 254 rotates the DVD platter 252 at a controlled and/or variable speed during the read/write operations. The ORW or OR device 259 moves relative to the DVD platter 252 to read and/or write data to/from the DVD platter 252. The ORW or OR device 259 typically includes a laser and an optical sensor.

[0099] For DVD read/write and DVD read only systems, the laser is directed at tracks on the DVD that contain lands and pits during read operations. The optical sensor senses reflections caused by the lands/pits. In some DVD read/write (RW) applications, a laser may also be used to heat a die layer on the DVD platter during write operations. If the die is heated to one temperature, the die is transparent and represents one binary digital value. If the die is heated to another temperature, the die is opaque and represents the other binary digital value. Other techniques for writing DVDs may be employed.

[0100] The spindle/FM driver 230 controls the spindle motor 254, which controllably rotates the DVD platter 252. The spindle/FM driver 230 also generates control signals that position the feed motor 258, for example using a voice coil actuator, a stepper motor or any other suitable actuator. The feed motor 258 typically moves the ORW or OR device 259 radially relative to the DVD platter 252. A laser driver 261 generates a laser drive signal based on an

output of the read/write channel module 234. The DVDA 250 includes a preamp circuit 260 that amplifies analog read signals. When reading data, the preamp circuit 260 amplifies low level signals from the ORW or OR device and outputs the amplified signal to the read/write channel module device 234.

[0101] The DVD system 210 further includes a codec module 240 that encodes and/or decodes video such as any of the MPEG formats. Audio and/or video digital signal processors and/or modules 242 and 244, respectively, perform audio and/or video signal processing, respectively.

[0102] As with the HDD system 110, portions of the DVD system 210 may be implemented by one or more integrated circuits (IC) or chips. For example, the processor 222 and the DVD control module 226 may be implemented by a single chip. The spindle/FM driver 230 and/or the read/write channel module 234 may also be implemented by the same chip as the processor 222, the DVD control module 226 and/or by additional chips. Most of the DVD system 210 other than the DVDA 250 may also be implemented as a SOC.

[0103] Referring now to FIG. 7C, a simplified functional block diagram of an exemplary combined DVD/HDD system 280 according to some implementations of the present invention is shown. The combined DVD/HDD system can be used as a provider or requester network device. The combined DVD/HDD system 280 includes a combined system control module 284 that communicates with nonvolatile memory 290 and volatile memory 292, which stored data for both DVD and HDD operation. The system control module 284

communicates via an interface 294 with an interface 296 of a host 298. In some implementations, the interfaces 294 and 296 are serial ATA interfaces, Fiber Channels (FC), serial attached small computer system interfaces (SAS), or other suitable interfaces.

[0104] The combined DVD/HDD system controls both DVD and HDD systems. The DVD/HDD system reduces overall system cost and provides improved functionality and performance. Cost is reduced through the use of a single DRAM and flash memory for both the DVD and HDD data storage. A single power supply and a reduced number of external connections are required, which further reduces cost.

[0105] In addition, the unified DVD/HDD system allows copy protected content to be copied bit-by-bit to directly to the HDD. In other words, the copy protected content can be copied without decrypting the copy protection scheme or digital rights management (DRM) and without requiring significant operating system involvement. Conventional separate DVD and HDD systems require the DVD to decode/decrypt the DRM or other copy protection prior to output. The DRM or other copy protection may or may not allow subsequent copying to the HDD. By combining the systems, additional functionality is provided due to the built-in security of the copy protection or DRM scheme since the DRM or copy protection remains intact. For example, single DVD drive copy operations are supported without removal of the copy protection or DRM. Additionally, the HDD can operate as a virtual DVD changer. Still other

variations of the combined DVD/HDD system are shown and described in U.S.

Patent Application Serial No. 11/039,288, filed on January 19, 2005.

[0106] Referring now to FIG. 8, partitioning of the nonvolatile memory 300 of the HDD into user accessible and hidden areas according to some implementations is shown. The nonvolatile memory 300 of the HDD is allocated into a first portion 304 that is user accessible and a second portion 308 that is not user accessible (or hidden). The second hidden portion 308 is used in one or more of the following ways according to some implementations of the invention. The hidden portion 308 is used to store the contents of a DVD that is to be copied. In addition, the hidden portion 308 of the HDD is used to provide a virtual DVD carousel. In other words, multiple DVDs may be copied to the HDD and played back at a later date.

[0107] Referring now to FIG. 9A, steps performed by the network devices are shown. Control begins in step 350. In step 352, control determines whether the provider network device receives a request for a copy of protected content. If not, control returns to step 352. If step 352 is true, control determines whether the requester network device is located on the local network in step 354. If step 354 is false, control denies the request and returns to step 352. If step 354 is true, the provider network device sends a copy of the protected content to the requester network device.

[0108] The provider network device determines whether the requester network device is on the local network in any suitable fashion. For example, a response time of the requester network device can be compared to a

predetermined threshold. In other implementations, the provider network device can temporarily request that the external ports of the router or modem be blocked so that the provider network device can confirm the local/remote status of the requester network device before the file sent. In other implementations, a local server can be queried to determine the local network devices. Still other methods for determining local/remote status may be used.

[0109] Referring now to FIG. 9B, steps for determining local/remote status by temporarily blocking an external port are shown. Control begins with step 360. In step 362, control determines whether the provider network device receives a request for a copy protected file. If step 362 is false, control returns to step 362. If step 362 is true, control continues with step 364 where the provider network device requests the external ports of the router or modem to be blocked. In step 368, the provider network device determines whether the requester network device has a local status. For example, the provider network device may send a message to the requester network device and wait for a response. If step 368 is false, the provider network device denies the request and control returns to step 362. If step 368 is true, the provider network device sends a copy of the file to the requester network device in step 370. The provider network device unblocks the external connection or port of the router or modem in step 374.

[0110] Referring now to FIG. 9C, steps for consulting a local server (such as a DHCP server) to determine the local/remote status are shown. Control begins with step 380. In step 382, control determines whether the

provider network device receives a request for a copy protected file. If step 382 is false, control returns to step 382. If step 382 is true, control continues with step 384 where the provider network device queries the server for identification of local network devices. The identification can include MAC addresses although other identification types can be used. In step 386, the provider network device determines whether the requester network device has a local status. If step 386 is false, the provider network device denies the request and control returns to step 382. If step 386 is true, the provider network device sends a copy of the file to the requester network device in step 388.

[0111] Referring now to FIG. 9D, steps performed by the network system are shown generally at 400. In step 402, control begins. In step 404, the provider network device determines whether a requester network device requests a copy of the content. If not, control returns to step 404. Otherwise control continues with step 408 and the provider network device requests a key from the requester network device. In step 412, the provider network device starts a timer.

[0112] In step 416, the provider network device determines whether the key is received. If the key is not received and (in some implementations) the predetermined period has not been exceeded, control continues with step 416. Otherwise, control continues with step 420 and the provider network device stops the timer. In step 422, control determines whether the timer is less than a predetermined period.

[0113] In some implementations, the predetermined period is less than or equal to the amount of time that a packet would require to travel one or two hops. By limiting the response time, additional security is provided. The amount of time that would be required for a computer or other device outside of the home network to respond will exceed the predetermined period. In other words, a packet containing a key from a computer such as computer 62 or other network device such as network device 60 that is connected outside of the home network will exceed one or two hops. This is due to the time required to pass through the modem and the service provider.

[0114] If step 422 is false, control returns to step 404. If step 422 is true, the provider network device encrypts or scrambles the content with the key and sends the encrypted or scrambled content over the network to the requesting device in step 426 and control continues with step 404.

[0115] Referring now to FIG. 10, steps of a method for allowing playback of a copy protected file from the requester network device N times are shown. Control begins with step 600. In step 602, control determines whether copy protected files have been stored on the requester network device. If not, control returns to step 602. If step 602 is true, control sets N=1 for the file in step 604. In step 606, control determines whether the copy protected file stored on requester network device has been played. If step 606 is false, control returns to step 606. If step 606 is true, control increments N in step 610. In step 614, control determines whether N = N_{max}. If step 614 is false, control returns to step 606. If step 614 is true, control deletes or otherwise makes the copy protected

file unavailable from the requester network device in step 618 and control returns to step 602.

[0116] Referring now to FIG. 11, steps of a method for limiting the amount of time that a copy protected file stored on the requester network device can be played are shown. Control begins with step 640. In step 644, control determines whether the copy protected file has been stored on the requester network device. If step 644 is false, control returns to step 644. Otherwise, control continues with step 646 and sets a timer. In step 648, control determines whether the timer is up. If step 648 is false, control returns to step 648. If step 648 is true, control deletes the copy protected file from the requester network device in step 652 and control continues with step 644. While a timer is described, any usage measurement and/or comparison may be performed. For example, a date and/or time stamp may be used and compared to current data and/or time. Still other usage data types will be apparent to skilled artisans.

[0117] Referring now to FIG. 12A, a media server 700 can be used to serve protected content from a provider 702 to a requester 704. While a router is shown connecting the media server 700, the provider 702 and the requester 704, other network configurations and connections may be used such as but not limited to ad-hoc network modes, peer to peer modes, and other approaches. In some implementations, the media server includes a local/remote status determining module 701, as previously described above. The media server 700 provides a list of available content to the requester 704. The requester 704 requests content. The media server 700 confirms that the requester is on the

local network in any of the ways described above. If the requester 704 is on the local network, the media server 700 requests the content from the provider 702. The provider 702 sends the content directly to the requester 704 or to the media server 700, which sends the content to the requester 704.

[0118] Referring now to FIGs. 12B and 13, the media server 700 serves protected content from a DVD system 710 to a HDD system 712. The DVD system 710 and the HDD system 712 can be implemented as described in the embodiments set forth above. In FIG. 13, the media server 700 can be implemented in a network as shown. Other network configurations such as those described herein as well as other network configurations are contemplated. The media server can be connected to the network in a wired or wireless manner.

[0119] Referring now to FIG. 14, a flowchart illustrating steps performed by the media server according to the present invention are shown. Control begins in step 720. In step 722, control determines whether the server receives a request for a copy of a protected file from the requester. If false, control returns to step 722. If true, the media server determines whether the requester has a local status. The local status of the requester may be determined in any of the ways described above. If true, the server requests the file from the provider and sends the file to the requester. Alternately, the provider may send the file directly to the requester.

[0120] Those skilled in the art can now appreciate from the foregoing description that the broad teachings of the present invention can be implemented in a variety of forms. Therefore, while this invention has been

described in connection with particular examples thereof, the true scope of the invention should not be so limited since other modifications will become apparent to the skilled practitioner upon a study of the drawings, the specification and the following claims.

CLAIMS

What is claimed is:

1. A hard disk drive (HDD) system that communicates with a provider network device over a network, comprising:

nonvolatile HDD memory that stores data in a nonvolatile manner in user accessible and hidden sections; and

a hard disk drive control (HDD) module that communicates with said HDD nonvolatile memory, that selectively requests and receives content from the provider network device and that stores said requested content in said hidden section of said nonvolatile HDD memory.

2. The HDD system of Claim 1 wherein after sending said request to the provider network device, said HDD control module receives a key request and transmits a key to the provider network device in response to said key request.

3. The HDD system of Claim 2 wherein said requested content received by said HDD system from the provider network device is encrypted using said key.

4. The HDD system of Claim 3 wherein said HDD control module decrypts said requested content.

5. The HDD system of Claim 1 wherein requested content includes usage data that is also written to said hidden portion of said nonvolatile HDD memory and wherein said HDD control module makes said requested content unavailable when said usage data indicates allowable use is over.

6. The HDD system of Claim 5 wherein said HDD system deletes said requested content from said nonvolatile HDD memory.

7. The HDD system of Claim 5 wherein said usage data specifies a predetermined number of allowable uses.

8. The HDD system of Claims 5 wherein said usage data specifies a duration of allowable usage.

9. The HDD system of Claim 1 wherein said HDD system communicates wirelessly with the network.

10. The HDD system of Claim 1 wherein said HDD system communicates with the network over a medium.

11. The HDD system of Claim 1 wherein the provider network device includes a digital versatile disc (DVD) system.

12. A networked DVD/HDD system comprising said HDD system of Claim 11 and further comprising said DVD system and said network.

13. A hard disk drive (HDD) system that communicates with a provider network device over a network, comprising:

nonvolatile memory means for storing data in a nonvolatile manner in user accessible and hidden sections; and
control means for communicating with said nonvolatile memory means, for selectively requesting and receiving content from the provider network device and for storing said requested content in said hidden section of said nonvolatile memory means.

14. The HDD system of Claim 13 wherein after sending said request to the provider network device, said control means receives a key request and transmits a key to the provider network device in response to said key request.

15. The HDD system of Claim 14 wherein said requested content received by said system from the provider network device is encrypted using said key.

16. The HDD system of Claim 15 wherein said control means decrypts said requested content.

17. The HDD system of Claim 13 wherein requested content includes usage data that is also written to said hidden portion of said nonvolatile memory

means and wherein said control means makes said requested content unavailable when said usage data indicates allowable use is over.

18. The HDD system of Claim 17 wherein said system deletes said requested content from said nonvolatile memory means.

19. The HDD system of Claim 17 wherein said usage data specifies a predetermined number of allowable uses.

20. The HDD system of Claims 17 wherein said usage data specifies a duration of allowable usage.

21. The HDD system of Claim 13 wherein said HDD system communicates wirelessly with the network.

22. The HDD system of Claim 13 wherein said HDD system communicates with the network over a medium.

23. The HDD system of Claim 13 wherein the provider network device includes a digital versatile disc (DVD) system.

24. A networked DVD/HDD system comprising said HDD system of Claim 23 and further comprising said DVD system and said network.

25. A method for operating a hard disk drive (HDD) system that communicates with a provider network device over a network, comprising:

storing data in a nonvolatile manner in user accessible and hidden sections;

selectively requesting and receiving content from the provider network device; and

storing said requested content in said hidden section.

26. The method of Claim 25 further comprising receiving a key request and transmitting a key to the provider network device in response to said key request after sending said request to the provider network device.

27. The method of Claim 26 further comprising encrypting said requested content received by said HDD system from the provider network device using said key.

28. The method of Claim 27 further comprising decrypting said requested content.

29. The method of Claim 25 further comprising:
writing requested content including usage data to said hidden portion; and

making said requested content unavailable when said usage data indicates allowable use is over.

30. The method of Claim 29 further comprising deleting said requested content from said hidden section.

31. The method of Claim 29 further comprising specifying a predetermined number of allowable uses using said usage data.

32. The method of Claims 27 further comprising specifying a duration of allowable usage using said usage data.

ABSTRACT OF THE DISCLOSURE

A hard disk drive (HDD) system that communicates with a provider network device over a network comprises nonvolatile HDD memory that stores data in a nonvolatile manner in user accessible and hidden sections. A hard disk drive control (HDD) module communicates with the HDD nonvolatile memory, selectively requests and receives content from the provider network device and stores the requested content in the hidden section of the nonvolatile HDD memory.

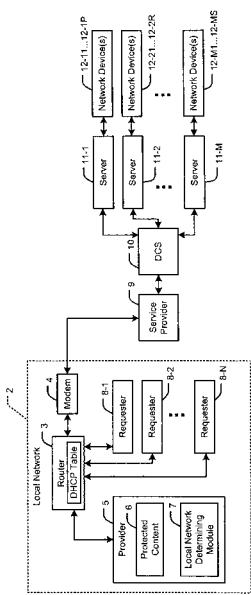


FIG. 1

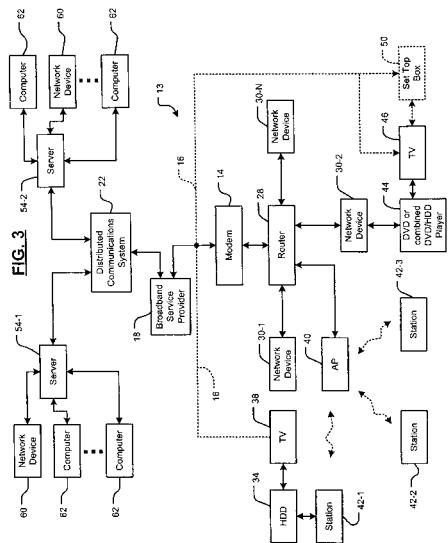


FIG. 3

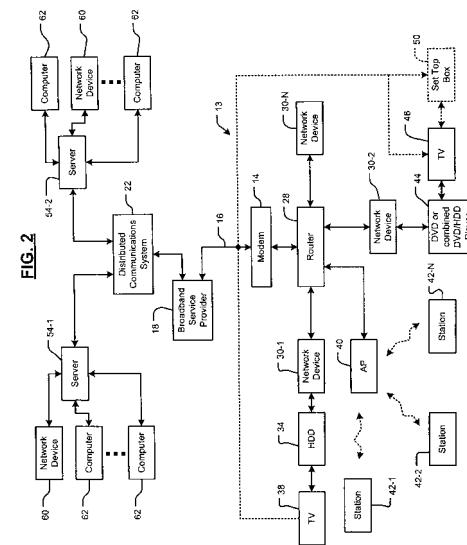


FIG. 2

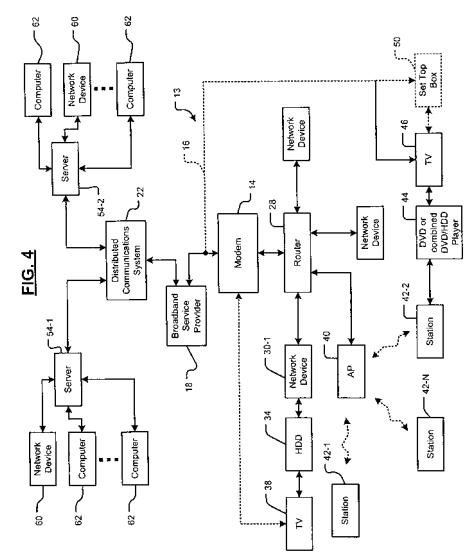


FIG. 4

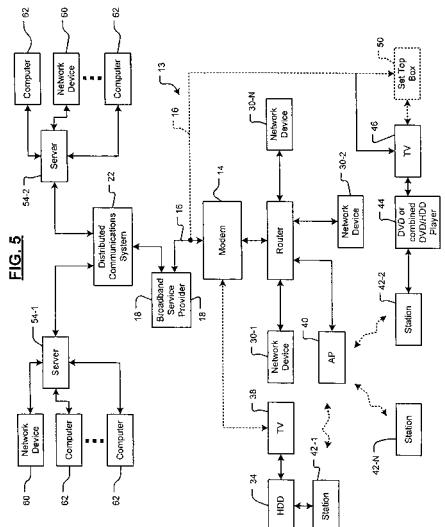


FIG. 5

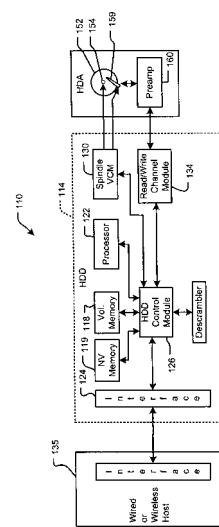


FIG. 6

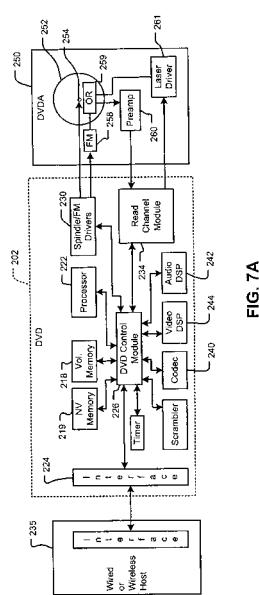


FIG. 7A

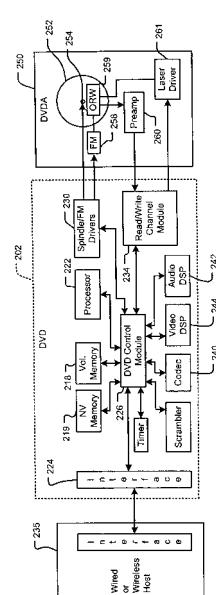


FIG. 7B

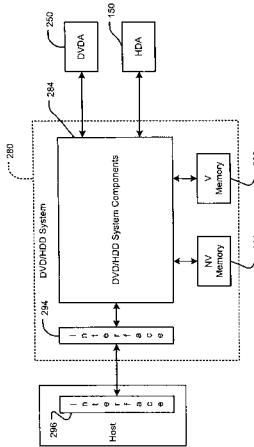


FIG. 7C

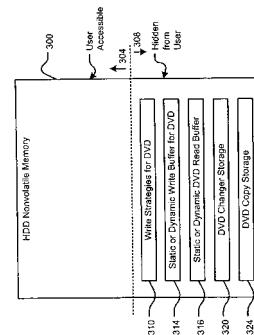


FIG. 8

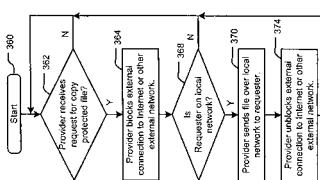


FIG. 9B

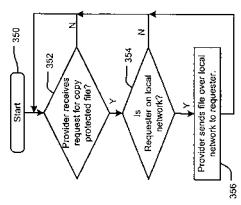


FIG. 9A

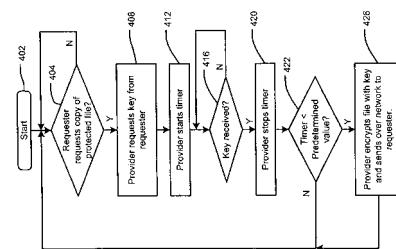


FIG. 9D

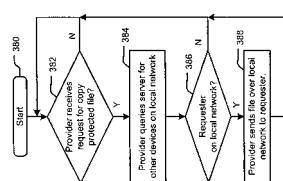


FIG. 9C

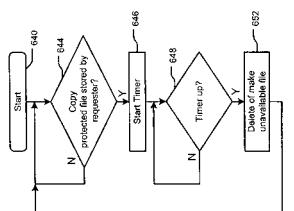


FIG. 11

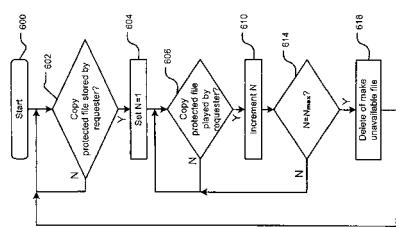


FIG. 10

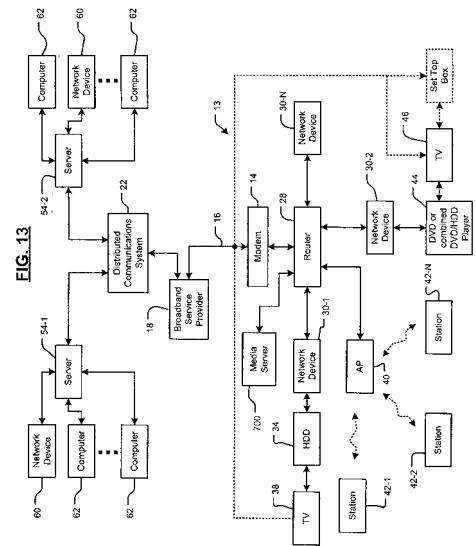


FIG. 13

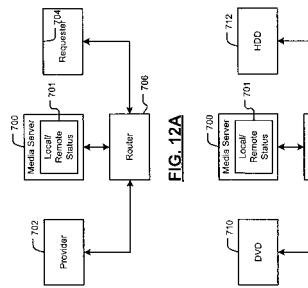


FIG. 12A

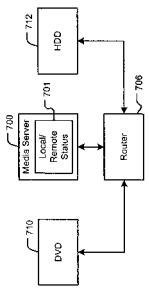


FIG. 12B

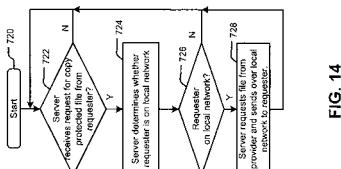


FIG. 14