社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2004－MBL－28 (14)
2004／3／4

小型モバイルコンピュータを用いたプロバイダ主体コンテンツ管理方式の提案

石井秀典† 海谷治彦† 海尻賢二†

デジタルコンテンツ流通市場の課題として、デジタルコンテンツの利用管理と、著作者の権利を保護することが重要である。本論文ではコンテンツ管理を自立的に行なう小型モバイルコンピュータ(MicroPC)をコンテンツ利用者が使用することで、デジタルコンテンツの適切な管理を行なう方法を提案する。MicroPCはコンテンツやその再生用アプリケーション、コンテンツプロバイダ独自のプログラム(サービスアプリ)を格納できる大容量メモリを持ち、USBなどの高速汎用入出力を持つ。また、利用回数や利用期間などの利用制御情報の管理、アクセス制御も自立的に行なう。これによってコンテンツ利用者は、MicroPCを利用したいPCに接続するだけで、自分が取得したコンテンツを自由に利用することができる。

A Contents Management Based on A Small Mobile Computer

HIDENORI ISHII† ,HARUHIKO KAIYA† and KENJI KAIJIRI†

One of major challenge in distributing digital contents is the management of digital contents and protection of author's copyright. The conventional technique, Software DRM(Digital Rights Management), is a common way to control digital contents, but it has some inconvenience. This paper proposes an efficient way of such management using a mobile computer. We call such system as 'MicroPC'. MicroPC has large storage so as to store the contents themselves and players for them, and has common interfaces such as USB. Users of MicroPC may simply attach it to their own or public PC, and they can easily enjoy digital contents. Independent of users, MicroPC can manage the contents and their audits, and report how may times/hours the users use each content to contents' provider.We develop a prototype system of MicroPC and clarify its advantages and problems.

1. はじめに

近年、普及しつつあるICカードはクレジットカード大の大きさで、内部にマイクロコンピュータを持ち、データを保存したりコマンドを実行できる。当初テレフォンカードの代替として普及してきたが、そのセキュリティの高さからクレジットカードや交通機関のチケットなどにも利用されつつある4)。しかし、その形状の制限から搭載できるメモリが限られている。

一方、半導体メモリはダイスサイズの縮小や生産技術の向上により価格が低下し、PC以外の様々な機器に搭載されている。特に不揮発メモリの1つであるフラッシュメモリはPDAやポータブルデジタル音楽プレーヤ、デジタルカメラなどに幅広く使用されている1)。データストレージとして利用されるUSBメモリは、非常に手軽に利用できUSB2.0に対応したデバイスでは480Mbpsの高速なバス速度をサポートしている。現在のPCはほぼ標準で使用可能となっているが、ICカードとは違いUSBストレージには処理能力はなくPCからの制御によって動作している2)。

また、近年、高速光回線などネットワークインフラの整備が進み、ユビキタスネットワークと呼ばれるようにいつでも、どこからでもアクセスできる環境も整いつつある。これにともない、デジタルコンテンツが大量に扱われるようになってきた。ネットワーク中心時代からからコンテンツ中心時代へと変化しているといわれているように、関心がインターネットそのものから、インターネットでやり取りされるサービスや情報、つまりどのようなコンテンツがやり取りされるかに変わってくる5)。それにつれて、デジタルコンテンツ流通市場の課題として、デジタルコンテンツの利用管理と、著作者の権利を保護することが重要となってきている6)。

本研究では、小型モバイルコンピュータを用いたプロバイダ主体コンテンツ管理方式とそのためのデバイ

† 信州大学 情報工学科
Faculty of Infomation Engineering, Shinshu University

ス(MicroPC)を提案し、そのプロトタイプを作成する。本方式では利用者端末内のコンテンツ及びライセンスを管理するのではなく、小型コンピュータ(MicroPC)がコンテンツとライセンスの両方を内部で保持し、管理する。そのため悪意ある利用者がコンテンツやライセンスに対して不正を働くことができない。

本論文は以下の構成になっている。第2節ではMicroPCに関する関連技術を述べる。第3節では、コンテンツ流通及び管理における課題と、利用者、コンテンツ提供者からみた利便性について述べ、その解決法について触れる。第4節では本論文で提案するMicroPCの利用者からみた機能について紹介し、第5ではMicroPCが実装すべきシステム要件を項目ごとに述べる。さらに、第6では作成したプロトタイプを紹介し考察する。

2. 関連技術

2.1 DRM(Digital Rights Management)

従来の利用管理方式は暗号化されたデジタルコンテンツと復号化するための鍵、鍵に対応した利用制御情報などをメディアに保存し、使用時に適宜読み出すことによって実現されている。この方法を用いた場合、不正コピー防止のために他のハードウェアでのコンテンツの利用が制限されており、利便性に欠いたものとなっている。また、復号化鍵やメディア内部に保存されている利用制御情報そのものが改変されてしまう危険性もある。つまり、利用者が取得したコンテンツはコンテンツプロバイダ(コンテンツ提供者)からはどうすることもできず、ユーザが不正を働くことを防止できない。利用者のすべての操作はユーザ側に権利があり、ユーザ主体のコンテンツ管理がされているのである。このようなコンテンツ管理では著作者の権利が充分に保護できない。

2.2 スマートカード

内部に処理コマンドとデータを保存することができ、$25mm^2$ 四方のマイクロプロセッサを搭載するカードデバイスで、一種のポータブルコンピュータである。パスワードや秘密鍵などの重要な情報を保存するための非常にセキュアなストレージとして利用することができる。利用者認証を内部で行なうため、利用者の認証情報が外部に漏洩する恐れがない。また、データの読込み、書込みを内部のプログラムを通して行なうことができるので、強固なセキュリティを実現している。さらに、カード内にプログラムを追加することができる。しかしストレージ容量が少く、DRMの課題を解決することができない。

3. コンテンツ流通の課題と解決法

MicroPCはデジタルコンテンツ流通において、内部処理という機能に着目したデバイスで、大容量ストレージを持ち、内部でプログラムの実行及び、データの保存ができる。また、MicroPCは利用者の意志で内部の情報を操作することができないため、安全にコンテンツの管理を行なうことができる。

3.1 コンテンツ管理の課題

デジタルコンテンツ流通における外からの脅威を、その主体ごとに表1に示す7)。また、デジタルコンテンツ管理における利用者、コンテンツプロバイダから見た利便性について表2, 表3に示す。

表1 コンテンツ流通時の脅威

主体	外からの脅威		
機器の利用者	機器内部解析/露呈		1-1
	なりすまし	機器の偽装	1-2
		再送攻撃	1-3
網または機器の利用者	認証局またはデバイス別の秘密鍵推定		1-4
	デバイス別秘密鍵または一時的な秘密鍵露呈		1-5
製造者	鍵情報漏洩		1-6
PCの利用者	ソフトウェアの解析		1-7

表2 利用者としての利便性

利便性	
2-1	利用した分だけの課金
2-2	コンテンツのスムーズな移動
2-3	他人のなりすましによる不正使用の防止
2-4	オフラインでのコンテンツ利用

表3 コンテンツプロバイダとしての利便性

利便性	
3-1	コンテンツの配信後のコンテンツ管理
3-2	コンテンツ配信後のコンテンツ課金情報の取得
3-3	ライセンスのハードウェア消去による削除確実性

これらの脅威、利便性に対して従来のソフトウェアDRM技術では不充分な面もあった。しかし、内部処理の利点とDRMを組み合わせたMicroPCでは(1-7)以外の脅威に対してに有効である。また 利用者から見た利便性(表2)や、コンテンツプロバイダから見た利便性(表3)についても内部処理は有効である。以下にそれぞれの脅威について述べる。

3.2 内部処理の利点を活かした解決法

- (1-1)についてはMicroPC自体が自立した専用ハードウェアであるため、内部プログラムで実装され

ている動作以外行なわない。そのため、不正なデータの吸出し、改変は不可能である。また内部にコンテンツとライセンスを保持するため (2-2)(2-3) に対しても有効である。異なった PC で利用する場合は MicroPC を繋ぎ変えるだけでよい。

- (1-2) については利用開始時に認証局から割り当てられた証明書を MicroPC に埋めこむ。MicroPC と配信サーバの接続の際には、サーバ認証、クライアント (MicroPC) 認証が行なわれる。お互いの認証が成功すると、共通セッション鍵で暗号化して直接接続される。したがって、MicroPC は配信サーバから直接コンテンツやライセンスを受け取ることになり、悪意のある利用者からのなりすましや盗聴を防止できる。
- (1-4) については証明書失効リストを確認することよって露呈した秘密鍵を確実に失効することができる。
- (1-3)(1-5) については個別公開鍵を用いた暗号化を行なうことによって防ぐことができる 7)。
- (2-1),(3-2) については MicroPC がアプリケーションに対してコンテンツを送信する回数、つまり利用回数を内部で記録し、コンテンツの更新、削除を行なう際に配信コンテンツに送信することによって可能となる。
- (2-3) については、利用者がコンテンツを利用する際、パスワード及び証明書による利用者とアプリケーションの認証を行なう。
- (3-1) の実現のためには、サービスアプリを用いる。サービスプロバイダがコンテンツごとまたは、コンテンツの種類ごとにサービスアプリを作成する。利用者がコンテンツを利用する際に、MicroPC 内部で対応するサービスアプリが動作し、コンテンツに処理を加えることができる。例えば、有効期限外の音楽コンテンツに対しては、楽曲の一部だけを利用可能にするなどである。
- (3-3) については MicroPC では利用制御情報が MicroPC 外部に移動することがないので、利用者がその情報をコピーすることや編集することはできない。よってライセンス削除の確実性が高い。また、MicroPC にサービスアプリを導入することにより、サービスアプリがコンテンツを削除することも可能である。

4. MicroPC を用いたコンテンツの利用法

本章では利用者から見た MicroPC を用いたコンテンツの利用について述べる。

端末との接続

MicroPC は利用者端末に接続することにより、端末のプライベートネットワークのマシンとして認識され、IP が割り当てられる (図 1)。

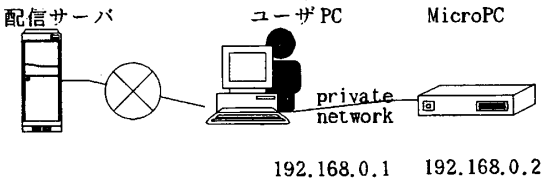

図 1 MicroPC の接続形態

4.1 ブラウザからの操作

以下の項目は利用者端末のブラウザ上から行なう。

利用者登録

・利用者情報をブラウザから MiroPC に登録する

会員登録

・利用者情報と MicroPC の証明書を配信サーバに登録する

コンテンツ/サービスアプリの取得

・配信サーバに接続する

・コンテンツリストからコンテンツ/サービスアプリの取得ボタンを押下する

・MicroPC は要求されたコンテンツ/サービスアプリ及び利用制御情報を取得し、MicroPC 内に登録する

コンテンツ/サービスアプリの削除

・MicroPC に登録されているコンテンツ/サービスアプリの削除ボタンを押下する

4.2 ブラウザ/アプリケーションからの操作

以下の操作はブラウザもしくは専用アプリケーションから行なう。

コンテンツの利用

コンテンツデータを利用者端末に残さないために、既存のストリーミングを使った利用と専用アプリケーションを使った利用が考えられる。

(1) ストリーミング

・ブラウザから MicroPC 内に登録されているコンテンツの取得ボタンを押下する

・対応するストリーミングソフトが動作し、コンテンツを利用する

(2) その他

・専用アプリケーションを取得する

・専用アプリケーションで MicroPC に接続しコンテンツを利用する

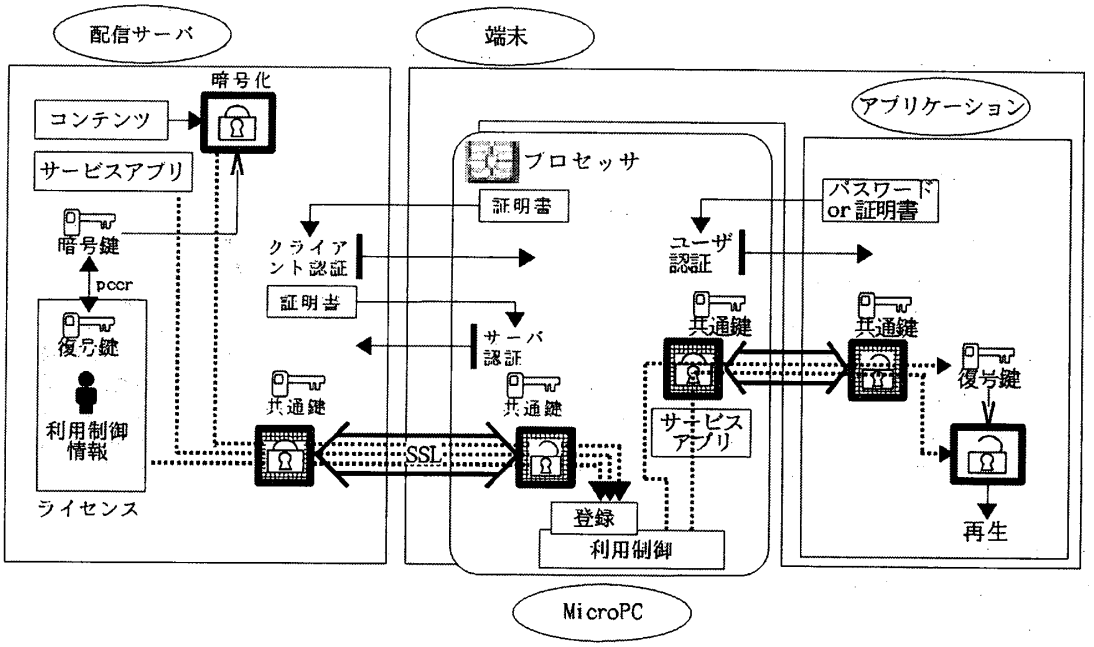

図 2　MicroPC を用いたコンテンツ/ライセンスの流れ

5. 管理システム

本節では 4 節で述べた機能におけるシステム要件について項目ごとに述べる。

通　　信

MicroPC と外部のやり取りはすべて暗号化し、悪意のある者が不正を働くことを防止する。

利用者がブラウザでコンテンツ/サービスアプリの取得☆ボタン、や削除ボタンを押下したとき、ブラウザから MicroPC への命令は http リクエストで送信され、内部のプロセッサで解析された処理される。

利用者登録

入力された利用者情報に基づいて、認証局に証明書の発行を依頼し、受け取った証明書を MicroPC 内に登録する。

会 員 登 録

指定された配信サーバと証明書をやり取りし、利用者情報を送信する。会員登録したサーバをサーバリストとして登録する。

認　　証

外部との接続時には必ず認証が行なわれる。MicroPC の認証には配信サーバ接続時に行なわれるサーバ認証とクライアント (MicroPC) 認証、そして利用者を特定する為のユーザ認証の三つの認証が存在する。

☆ データの移動は、MicroPC も一台のマシンとして認識されるため、区別のために配信サーバ →MicroPC の移動を取得、MicroPC→アプリケーションを再生とする。

サーバ認証は、MicroPC が配信サーバのなりすまし防止のために行なう。また、クライアント認証は配信サーバが行なう。これにより MicroPC のなりすまし防止を行なうとともに MicroPC の特定を行なう。MicroPC の証明書には利用者を特定するための情報が入力されており、その情報から配信サーバは利用者を特定する。

これらの認証時に SSL 接続の準備が行なわれ、最後に共通鍵暗合方式で通信路が確保される。

ユーザ認証は、利用者が MicroPC を利用する際に MicroPC によって行なわれ、MicorPC に登録された利用者かどうかを確認する。

MicroPC の証明書は利用者が認証局から個人情報を特定できる証明書として取得し、MicroPC に格納する (図 3)。配信サーバからコンテンツを取得するためには事前に MicroPC 証明書を用いて利用者情報を登録しておく必要がある。

コンテンツ (もしくはサービスアプリ) の取得

コンテンツの取得要求を受けると、MicroPC は指定された配信サーバとの間で、証明書による認証を行ない、セキュアな通信路を確立する。次に配信サーバから利用者に要求されたコンテンツとライセンスを受け取ると内部の記憶領域に保存し、それぞれ登録する。

コンテンツの削除

コンテンツの削除要求をうけると、内部からコンテンツを削除する。そして配信サーバに接続し、利用制御情報をサーバに送信する。これにより利用者のコン

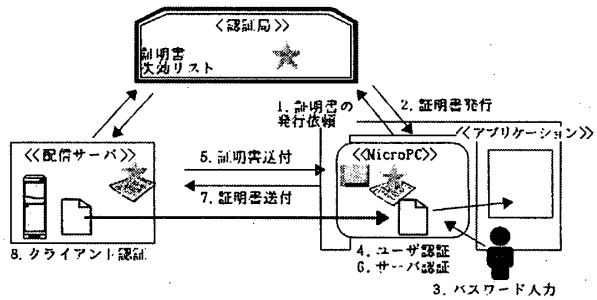

図 3　証明書/コンテンツの流れ

テンツの利用状況を知らせる。

コンテンツの利用

MicroPC 内に保持されているコンテンツの利用は、アプリケーションと MicroPC との間にはられるセキュアな通信路を通じて利用が可能となる。アプリケーションからコンテンツを要求すると MicroPC では利用制御情報をもとにアクセス制御を行なう。対応したサービスアプリがある場合はそのサービスアプリに渡され、サービスアプリ固有の処理されてからアプリケーションに渡される。

コンテンツデータを端末に残さないために、コンテンツを端末に送信する方法としてストリーミングデータとして送信する方法と利用者が専用アプリケーションを用いて利用する方法が考えられる。アプリケーションはコンテンツを利用する場合、コンテンツ再生後、利用者の端末にあるコンテンツデータを強制的に削除する必要がある。また、ストリーミング方式で利用する場合、MicroPC はストリーミングサーバとして動作する。

利用者側の準備としてはストリーミングソフトや専用アプリケーションを端末にインストールする必要があるが、これらは MicroPC から Applet のように自動的にダウンロード/実行する仕組を提供することもできる。

利 用 制 御

利用制御情報は MicroPC 内部で保持し、利用制御情報の更新、削除を MicroPC 自身が行なうため、利用者は制御情報を操作することができない。また、ユーザ PC とは独立して時間を管理するため、利用者環境に左右されず正確な利用期限制御が行なえる。

プロバイダ主体

コンテンツプロバイダはコンテンツに対して処理を行なうプログラムを独自に開発することができ、コンテンツが利用者に配信された後でもプロバイダ主体でコンテンツの管理を行なうことができる。

コンテンツ管理

コンテンツに関連付けられた様々なコンテンツ情報をもとに MicroPC が独自にコンテンツを管理するため、利用者がその管理を行なう必要がない。コンテンツリストのさまざまな View が提供される。

6. 実　　装

本章では本方式を用いて実装したプロトタイプシステムについて紹介する。

6.1 プロトタイプシステム

目　　的

本プロトタイプシステムは以下の検証を目的として実装した。

- MicroPC と配信サーバ間の通信
- 利用者からみた利便性の調査
- コンテンツプロバイダからみた利便性の調査
- 実装における課題の発見

実　　装

本プロトタイプシステムは三つの部分から成り立つ。

・コンテンツ配信サーバ

・利用者端末

・MicroPC

なお、認証局に関してはコンテンツ配信サーバと同一マシンを使用した。

MicroPC に関しては、該当するようなデバイスが手近になかったため、一台の PC を仮想的に MicroPC と見立てて実装を行なった。

また、利用者端末と MicroPC の接続には通常のイーサーネットを用いたが、USB を用いた接続とは本質的な違いはない。

HTTP リクエストを解析し SSL に変換するプロトコルとして図 5 で示すプロトコルを用いる。図 5 は配信サーバに接続し会員登録する様子を示している。会員登録では利用者登録、サーバ登録を行ない、最後に会員専用サイトを表示される。

利用者登録、サーバ登録後の接続は、リクエスト先のアドレスが登録されていればすぐに SSL Handshake を行なう。

実 行 例

図 4 はプロトタイプの実装画面で利用者が端末のブラウザから MicroPC に接続し、配信サーバからのコンテンツリストを表示している。

6.2 評　　価

実験を通して、ブラウザ-MicroPC 間、MicroPC-配信サーバ間のリクエスト変換やメッセージパッシング、コンテンツの利用制御に関しても意図した通りの動作

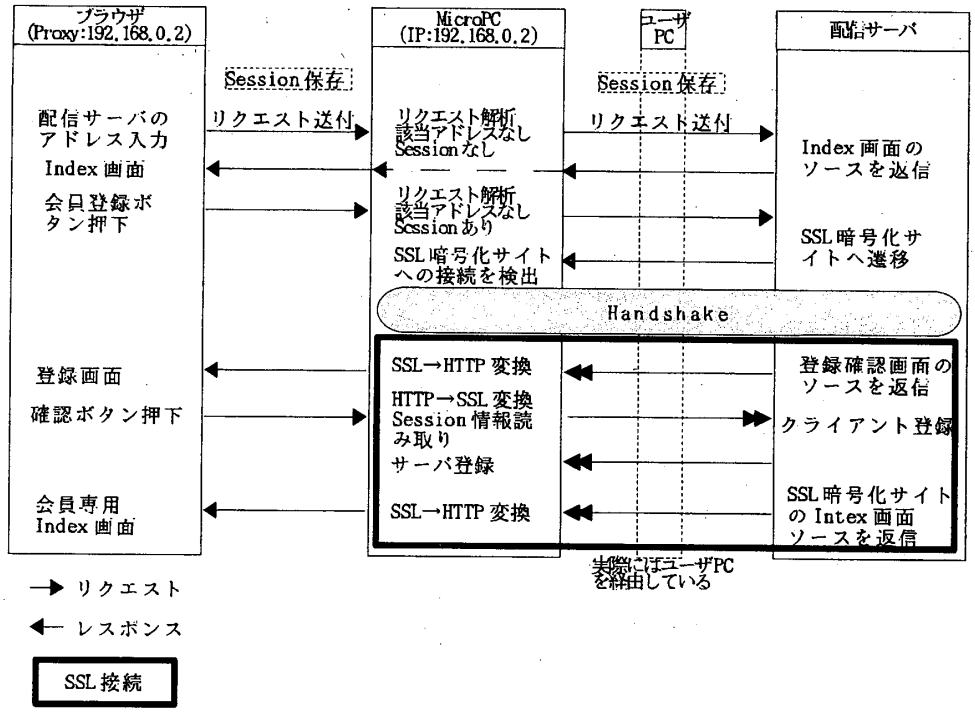

図 5　利用者登録

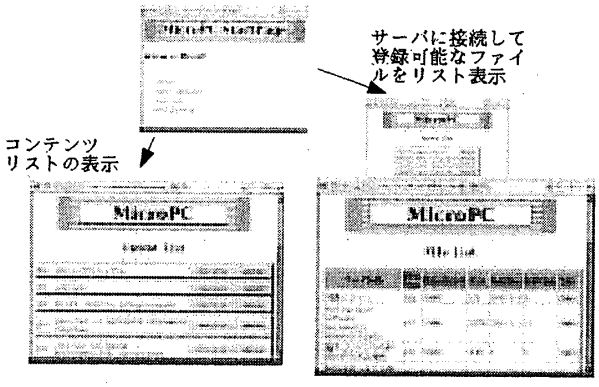

図 4　利用者端末からブラウザで見た様子

が確認できた。また、サービス・アプリにより、MicroPC 内でプロバイダが意図した処理を、コンテンツに対して行なうことができた。

そして、さまざまな Web アプリケーションで実績がある SSL 通信を使用しているため、MicroPC とサーバとの通信はセキュアな通信が望める。また、暗号化通信がサーバから MicroPC まで直接行なわれるため、中継するユーザ PC にもその内容を秘密にすることができ、データの盗聴といった行為を防ぐことができた。

また、ユーザインタフェースの構成では利用者が求める要求を Web 画面にボタンとして配置した。MicroPC がブラウザから送られてくる Http リクエストを解析して、暗号化通信に変換しているため、利用者は MicroPC を操作しているという感覚もなく扱うことができた。

問題点として、本来プライベートネットワークのパケットが他のネットワークへ出るために IP マスカレードの設定が必要である。今回行なった実験では利用者端末に Linux を用いており、知識があれば比較的容易に行なうことができたが、一般的には煩雑である。

7. 今後の課題

今後の課題として、今回提案したコンテンツ管理方式の詳細な仕様の策定、ハードウェア要件の決定、実装などがある。

8. ま と め

本稿では、現状の DRM システムの問題点を指摘し、より強固で柔軟な小型モバイルコンピュータを用いたプロバイダ主体コンテンツ管理方式を提案した。コンテンツのハードウェア保護を目的とした本方式は、利用者の管理下にないコンテンツ管理デバイスを利用者に配布し、それを利用者の PC に接続することで、利用者はコンテンツを利用できる。またコンテンツの管理や利用制限情報管理などはハードウェア内で一括して行ない、外部との通信は暗号化されるので、悪意ある利用者のライセンス違犯を防ぐことができる。さらに、コンテンツ管理デバイス自体が利用制御情報を持

つため、利用者がマシンを変えたり、OSを入れ換えたりしても以前取得したコンテンツが利用可能である。サービスアプリを実装することによりプロバイダ主体のコンテンツ管理が可能となるなど、さまざまな利点がある。

今後は詳細な仕様決定、ハードウェア要件の検討を行なっていく予定である。

参 考 文 献

1) Michael Kanellos, Flash Forward, March 27 2003, http://news.com.com/2009-1040-994240.html
2) Universal Serial Bus, Mass Storage Class, http://www.usb.org/home
3) Uwe Hansmann, Martin S. Nicklous, Thomas Schack, Achim Schneider, Frank Seliger, Smart Card Application Development Using Java -Second Edition [Springer]
4) IC カードシステム利用促進協議会, http://www.jicsap.com/
5) David C. Mochella 覇者の未来 IDG コミュニケーションズ
6) 櫻井紀彦,"コンテンツ流通における著作権保護技術の動向", 情報処理学会論文誌,vol.42 No.SIG 15,pp-63-77,2001
7) 畠山卓久、丸山秀史、千葉哲央, 音楽コンテンツの超流通とセキュリティ,FUJITSU.52,5,p.473-481,2001 年 9 月