別添１

平成 22 年度「新 ICT 利活用サービス創出支援事業」

書店店頭とネットワークでの電子出版の販売を実現する

ハイブリッド型電子出版流通の基盤技術の標準化および実証

ハイブリッド型電子出版流通における、権利保護技術の運用のためのガイドライン案

第 1.0 版

平成 23 年 3 月 31 日

株式会社インフォシティ

目次

図表インデックス

1. 本書の位置づけ

本書は、「平成 22 年度新 ICT 利活用サービス創出支援事業」書店店頭とネットワークでの電子出版の販売を実現するハイブリッド型電子出版流通の基盤技術の標準化および実証に関するハイブリッド型電子出版流通における、権利保護技術の運用のためのガイドライン案である。

1.1. ガイドライン案作成の背景・目的

コンテンツ分野は、文化的側面のみならず、経済成長を支える成長産業としても、政府にとって重要な位置づけとなっており、官民一体となって取り組みを推進しているところである。

近年、映像や音声などのデジタルコンテンツをインターネットで配信することや、光ディスクなどの記録媒体で流通させるなど、多様な流通経路への流通が盛んに行われるようになった。デジタルコンテンツは、配信や蓄積が容易である一方、権利者の許可を得ることなく複製、再送信するなどの不法行為を行うことも容易であることから、権利保護技術の開発の在り方が注目をされている。

デジタルコンテンツの多様な配信・流通モデルとして新たに提案されたハイブリッド型電子出版流通における権利保護に関するガイドライン案をデジタル・ネットワーク社会における出版物の利活用の推進に関する懇談会の技術ＷＴ報告や平成 21 年度補正予算「ユビキタス特区事業」ハイブリッド型デジタル（電子）出版流通の基盤技術開発における実証実験など結果を踏まえ策定する。

ハイブリッド型電子出版流通を市場で早期に拡大するにあたっては、複数の販売事業者の参加を可能とし、また電子出版を閲覧する端末においても複数のメーカーでの開発が可能となる流通基盤技術の標準化が必要不可欠である。

ハイブリッド型電子出版流通の標準化においては、国際的な流通形態とするために、メモリカード市場で 7 割以上のシェアを持ち、全世界の 90%以上の携帯電話にスロットが搭載されるフラッシュメモリ型カード：SD カードを採用し、SD カードの国際技術規格化機関である SD-Card Association (9.2 参照：以下 SDA)の規格に準拠し、さらにハイブリッド型電子出版流通に必要な仕様の拡張を検討する。

本書「ハイブリッド型電子出版流通における、権利保護技術の運用のためのガイドライン案」は、ハイブリッド型電子出版流通における権利保護技術の運用方法であり、電子出版販売サービス事業者がサービス提供を行う際や端末メーカーが端末を開発する際に準拠すべきものである。

1.2. 本書の構成

次章以降では、以下に記述する内容を中心に記述する。

第 2 章では、まず、ハイブリッド型電子出版流通の提案背景、意義などを「デジタル・ネットワーク社会における出版物の利活用の推進に関する懇談会」報告書（以下 懇談会報告書）の基本的視点を踏まえ説明する。次に、ハイブリッド型電子出版流通のあるべき姿を描き、権利保護に関する要件を物理メディア、クライアント、配信サーバ、権利保護技術（Digital Rights Management：以下 DRM）に分けて導出する。

第 3 章では、デジタルコンテンツの権利を保護するための一般的な DRM についての概要説明の後、DRM の問題点、現状について簡潔にまとめる。次に、現状の電子出版における DRM について外観するとともに、DRM の主要な機能、使用許諾条件について、説明する。

第 4 章では、ハイブリッド型電子出版流通におけるコンテンツ保護の要件について、前年度実証実験結果を踏まえて、要件を展開するとともに、ガイドラインで推奨するコンテンツ保護の仕組みを導出する。

第 5 章では、ハイブリッド型電子出版流通における物理メディアとして SD カードを利用する根拠を述べ、SD カードの著作権保護機能を利用した際の各種機能の実現方法やユースケース、留意点などを述べる。更に、SD カードを利用する際に必要となる SDA 規格と 4C Entity LLC（9.3 参照：以下 4C）規格についての概要を説明する。

第 6 章では 4C の規定する SDSD-CPRM をベースに基本的な DRM システムを構築し、これをハイブリッド型電子出版流通に適合するよう拡張を加えている。さらに、本ガイドラインで必要とする DRM と他の DRM との比較も行う。

第 7 章では本ガイドラインにおけるシステムモデルを提示し、想定するサービスモデルからライセンスサーバの構成、提供する機能を示す。

第 8 章では本ガイドラインにおける Web ストアサーバ、マスタリング製造装置、ライセンスサーバやクライアント等の各システム要素に要求されるセキュリティ項目を示す。

第 9 章は参考資料として、SD カード、SD-Card Association、4C Entity LLC について説明する。

2. ハイブリッド型電子出版流通の技術的要件の導出

2.1. ハイブリッド型電子出版流通とは

ハイブリッド型電子出版流通は、デジタルコンテンツの新しい販売形態として、これまでのインターネット上で販売するオンライン販売に加えて、DVD や SD メモリカードといったメディアにコンテンツを収納して書店店頭などで販売するパッケージ販売を併せ持つ、オンラインとパッケージをハイブリッドに組み合わせ販売の形を呼ぶ。こうしたハイブリッド型の流通は、利用者の所有間やネットワーク環境による利用の制限からの解放などの利便性を享受できる。

一方、このような環境変化によって、デジタルコンテンツ市場が拡大、サービス基盤の整備により、コンテンツ提供者にとっても市場参入がし易くなることにより、市場の相乗的な広がりが期待される。

ハイブリッド型電子出版流通は既存の紙の出版物に加え、電子出版の形態をパッケージ型とネットワーク型の両方を併用することで、既存の流通基盤を用いて、パッケージを販売しつつ、ネットワークを通じてオンラインでの電子出版を行う流通形態である。

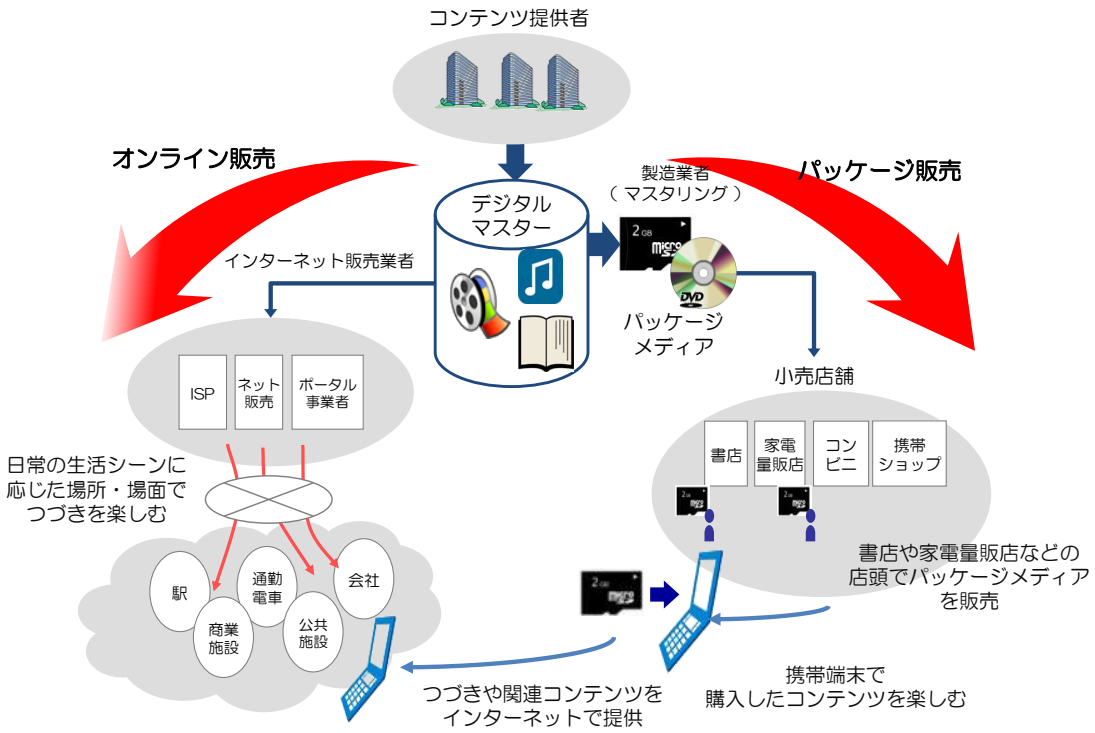


図 2-1：ハイブリッド型電子出版流通

2.1.1. ハイブリッド型電子出版流通の特徴

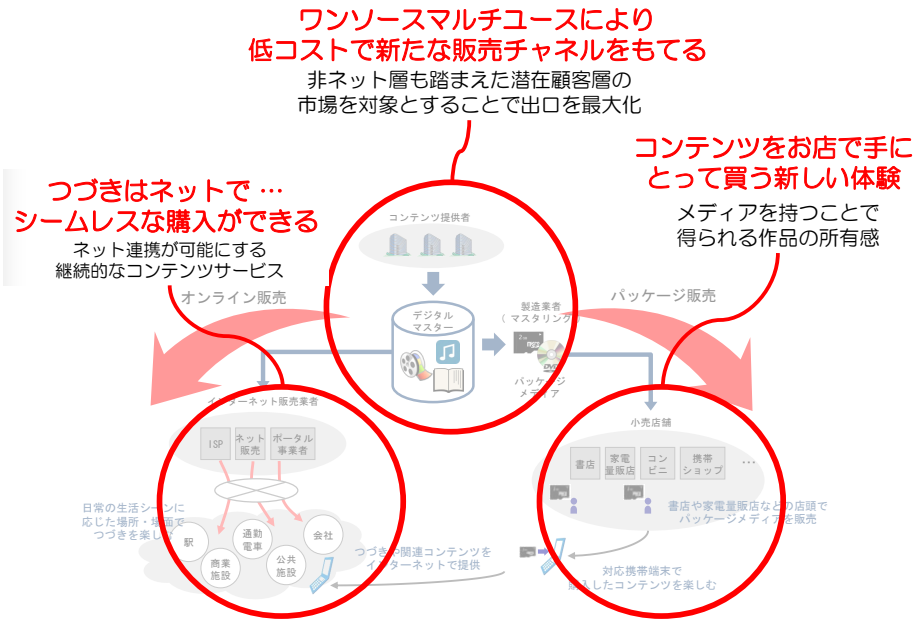


図 2-2：ハイブリッド型電子出版流通の特徴

ハイブリッド型電子出版流通には３つの大きな特徴がある。

1. コンテンツ提供者は同じ形式のコンテンツを利用（ワンソースマルチユース）して低コストで、新たなパッケージ販売チャネルを持つことができる。
   すなわち、パッケージ販売チャネルによりインターネット利用とは疎遠の非ネット層を踏まえた潜在顧客層の市場を掘り起こすことで、コンテンツの出口を拡大することが可能である。
2. ネット販売と同じコンテンツのパッケージ販売が可能なことから、ユーザはコンテンツを店頭で手にとって買うという新しい体験ができる。しかも、メディアを持つことで作品の所有感が得られる。
3. ネット連携によって、パッケージ販売されたコンテンツのつづきはネットで購入というシームレスなサービスも可能となる。
   例えば、パッケージ販売されたコンテンツにはシリーズ物のコンテンツが多数収容されているが、パッケージ購入時には最初の 1 冊のみ閲覧可能になっている。残りのコンテンツはインターネットを介して、閲覧権利を購入することで閲覧可能とする。こうすることで、パッケージ販売価格を低く設定するとともに、パッケージ購入後のアフターマーケットでの更なる販売機会を創出する。

この様に、ハイブリッド型電子出版流通はオンライン販売とオフライン販売のそれぞれの良さを保ちつつ、双方をつなぎ合わせることによる新たな良さを生み出す可能性を持っている。

2.2. 技術要求事項の導出

デジタル・ネットワーク社会における出版物の利活用の推進に関する懇談会の技術ＷＴにおいては、デジタル・ネットワーク社会における出版物の利活用の推進に関する技術的な問題について専門的な見地から検討を進めてきた。その際、幅広い技術的課題を具体的に検討するため、想定される技術的目標をあらかじめ設定した上で整理を行ってきた。

こうしたハイブリッド型電子出版流通に対する技術的要件を懇談会報告技術的目標から導き出す。

2.2.1. 懇談会報告技術的目標の技術的課題の解決

１．「オープン型電子出版環境」の実現と「知のインフラ」へのアクセス環境の整備

① 我が国における表現の多様性の確保、利用者の多様な電子出版へのアクセスの確保、電子出版市場の拡大及び日本の出版コンテンツの世界発信の推進の観点から、多様なプレイヤが連携して電子出版の提供を展開すること、利用者が国内外の豊富なコンテンツに簡便・自由にアクセスすることを可能とする「オープン型電子出版環境」の実現に必要な技術的課題

② 国立国会図書館のデジタル・アーカイブを始めとする知のインフラの構築、国民へのアクセス環境の整備のため、必要な技術的課題について検討を行う。

技術的課題を具体的に検討するために、以下の10項目のアジェンダを設定した上で、当該アジェンダを実現するため解決しなくてはならない課題、解決方策、求められる取組の方向性等について整理する。

【アジェンダ】
【１】電子出版を様々なプラットフォーム、様々な端末で利用できるようにする。
【２】電子出版を様々なプラットフォーム、様々な端末で提供できるようにする。
【３】海外の出版物に自由にアクセスできるようにするとともに、日本の出版物を世界へ発信する。
【４】電子出版を紙の出版物と同様に長い期間にわたって利用できるようにする。
【５】あらゆる出版物を簡単に探し出して利用することができるようにする。
【６】出版物間で、字句、記事、目次、頁等の単位での相互参照を可能とし、関連情報・文献の検証や記録を容易にする。
【７】電子出版を紙の出版物と同様に貸与することができるようにする。
【８】出版物のつくり手、売り手の経済的な利益を守る。読み手の安心・安全を守る。
【９】出版物のつくり手の意図を正確に表現できるようにする。
【10】障がい者、高齢者、子ども等の身体的な条件に対応した利用を増進する。

2.2.2. 具体的検討

示されたアジェンダのうち【1】、【2】、【4】、【7】、【8】は特に、ハイブリッド型電子出版流通に対する要求事項を示唆している。

2.2.2.1. 懇談会報告書の 2.1 での指摘事項

【1】電子出版を様々なプラットフォーム、様々な端末で利用できるようにする。
【2】電子出版を様々なプラットフォーム、様々な端末で提供できるようにする。

（1）多様なファイルフォーマットの存在と電子出版のワークフロー出版物のつくり手に係る電子出版の生産性向上を図りつつ、電子出版を様々なプラットフォーム、様々な端末において利用・提供できるようにするためには、ファイルフォーマットの標準化（オープン化）を推進する必要がある。

我が国において、電子出版を様々なプラットフォームや様々な端末に向けて提供することに必ずしも成功してこなかった。

この結果、出版物のつくり手は、新しい端末や新しいプラットフォームが登場するたびにそれぞれに最適化した電子出版に作り直す必要があり、一つの作品に対していくつものファイルを作らなくてはならない状況（ワンコンテンツ・マルチファイル）にある。

懇談会報告書の 2.1 から導かれる技術的要求事項

- 電子出版のワークフロー出版物のつくり手に係る電子出版の生産性向上
- 様々なプラットフォーム、様々な端末において利用・提供可能なこと

2.2.2.2. 懇談会報告書の 2.3 での指摘事項

【4】電子出版を紙の出版物と同様に長い期間にわたって利用できるようにする。

（1）異なる電子出版端末・プラットフォーム間の相互運用性の向上

紙の出版物を購入した場合、利用者は、出版物が物理的に滅失するまで利用することが可能である。

一方、例えば携帯コミックを購入した場合には、端末機種や契約する携帯会社を変更すること等によって、変更後の端末に移行して利用することができない場合が多い[25]。

また、電子出版端末・プラットフォームの提供者が市場から撤退した場合においては、購入した電子出版がその後に利用できなくなる懸念がある。

こうした点から、現在の電子出版は、紙の出版物と比べて、利用者に購入した実感（所有感）を与えられていないのではないかという指摘がある。

電子出版市場の一層の拡大を展望したとき、紙と同様に長期間にわたる利用が可能となるよう電子出版の普遍性とオープン性を求める利用者ニーズに応えていく必要があるものと考えられる。

このような観点から、異なる電子出版端末・プラットフォーム間の相互運用性を向上するための技術的な検討が必要である。

25 携帯端末内の電子出版コンテンツへのアクセスについて、ＳＩＭカードによって制御している場合には、変更前の端末においても電子出版が利用できなくなる場合がある。

（２）公共財としての電子出版の保存

公表され広く利用される出版物について、いずれは公共財として、公的なアーカイブで保管し長期的な利用を保証する仕組みを構築することは、我が国の出版文化が育んだ知的資産の次代への継承と、新たな創造の基盤となるものであり、未来の国民への責任を有する国の極めて重要な役割のひとつである。

しかしながら、例えば、過去のフロッピーディスクやCD-ROM形態で流通していた出版物のすべてについて利用環境を再現することは事実上困難となっており、こうした過去の事例も踏まえ、今後の電子出版については、民間での対応が難しい超長期（数十年を超える期間）にわたる利用環境の再現を可能とするよう、権利面での対応を含めた確かな技術的な仕組みを検討する必要がある。

こうした超長期の利用保証の検討にあたっては、長期（数年から数十年）の利用の保証を期待されている民間の商用サービスの提供者と、超長期の利用の保証を求められている公的アーカイブとの間の相互協力が不可欠である。このため、今後の電子出版の時代を見据えて、その超長期の利用を保証する観点から、電子出版の収集・保存の公的な仕組みについて、関係者において検討を進めることが適当である。

また、我が国では、国立国会図書館において、納本制度等に基づき収集・保存している紙の出版物等についてデジタル化が進められており、知的資産の次代への継承と新たな創造の基盤を構築する観点から、国立国会図書館における出版物のデジタル保存に係る取組を継続・拡充していく必要がある。

懇談会報告書の 2.3 から導かれる技術的要件

- 電子出版を紙の出版物と同様に長い期間にわたって利用できること
- 異なる電子出版端末・プラットフォーム間の相互運用性の確保
- 利用者に購入した実感（所有感）を与えられること
- 公共財として長期間電子出版の保存ができること

2.2.2.3. 懇談会報告書の 2.6 での指摘事項

【７】電子出版を紙の出版物と同様に貸与[31]することができるようにする。

（１）家族や友人など特定のコミュニティ内での貸与

① 紙の出版物の特定のコミュニティ内での貸与

紙の出版物においては、利用者は購入した出版物について、家族や友人など特定のコミュニティ内で貸し借りが行われている。

自分が読んで感銘を受け、読む価値のあるものだと感じた本について、教育の観点から

子に貸与する、共感や親交を深める観点から友人や恋人に貸与するといったように、特定の人々の間のコミュニケーションを深める手段としての機能を紙の出版物は果たしてきた。

② 電子出版の特定のコミュニティ内での貸与

電子出版においては、利用者が購入した電子出版について、家族や友人など特定のコミュニティ内で貸し借りすることは、基本的にはできていないが、ビジネス上のオプションの１つとして、こうした利用者の利便性を高める貸与サービスが実現されることも考えられる。

利用者利便の向上の観点から、電子出版について特定のコミュニティ内での貸与を可能とするサービスが、ビジネス上の判断に基づいて実現される場合、電子出版の貸与について特定のコミュニティ内に限定するための技術的な仕組みや、一定期間経過後に電子出版のデータを消去する技術的な仕組み、貸与回数を制限する技術的な仕組み等、出版物のつくり手､売り手の理解を得るための技術的なスキームについて検討されることが望ましい。

（２）図書館による貸与

① 紙の出版物の図書館による貸与

紙の出版物においては、学校図書館や公共図書館、大学図書館、国立国会図書館等が購入し所蔵する出版物について、児童・生徒・学生の教育のため、市民の社会教育のため、国民の知への公平なアクセスの確保を図るため、貸与が行われている。

31 「貸与」という言葉について、ここでは、個人が購入した紙の出版物若しくは電子出版を特定の人に利用させる又は図書館が購入した紙の出版物若しくは電子出版を公共サービスとして国民に利用させることを意味するものとして取り扱う。貸与を受ける者から対価をとるかどうかを決めることについては論じない。

② 米国における図書館による電子出版の貸与

米国や韓国等では、電子出版についても、図書館による貸与が一定の制限を加えた上で一般化しつつある。

米国においては様々な方法により電子出版の貸与が行われているが､例えば､約6,000 の公共図書館は、SONYと協力し、紙の出版物の貸与に類似した方法で、電子出版端末（「Reader」）を通じた電子出版の貸与を実施している[32]。

公共図書館が電子出版の貸与を行える種類・冊数は、当該公共図書館がエージェントを通じて出版社等に支払う予算額の限度に合わせて制限される仕組みとなっており、また、利用者がダウンロードした電子出版のデータは、一定期間経過後、読み出し不可になるよう技術的な制御が施されている。

コピー機により複製されたり、イメージデータ化してネット流通されたりという危険を防ぐことが困難な紙の出版物よりも、電子出版による貸与の方が出版物のつくり手の権利利益を技術的な制御により守りやすいという側面もあると考えられる。

③ 我が国における図書館による電子出版の貸与

我が国における図書館による電子出版の貸与は、実験的な取組の範疇に留まっており、利用者が一定の制限のもと図書館から電子出版の貸与を受けるということはほとんど行われていない。

図書館による電子出版の貸与を巡っては、様々な考え方[33]があるが、今後は、米国等の先行事例において、当該貸与を可能としている出版物のつくり手、売り手側の要求条件や利用者側の要求条件の在り方（アクセスエリアの制限、新刊本の電子貸出禁止期間設定、ライセンス数の制限、図書館と書店の棲み分け等）などを調査整理し、技術的な裏付けを考えていくことは、我が国における図書館による電子出版の貸与を考える上で有効と考えられる。

このため、今後関係者により進められる図書館による電子出版に係る公共サービスの具体的な運用方法に係る検討に資するよう、米国等の先行事例の調査、図書館や出版物のつくり手、売り手等の連携による必要な実証実験の実施等を進め、こうした取組について国が側面支援を行うことが適当である。

32 当該貸与サービスの実現に当たっては、出版社・関連団体との包括契約に係る代理契約交渉や、各図書館の既存のウェブページに併せたバーチャルブランチ（電子図書館ブランチ）の開設、各図書館の予算に合わせて提供するデジタルデータの提供、図書館員への教育サポート等を行うエージェントが、技術面も含めてバックエンドで役割を果たしている。利用者は、居住する地域の公共図書館から貸出カードの発行を受け、ウェブ上の当該公共図書館の電子図書館ブランチにアクセスし、貸出カード番号を入力した上で、電子出版をダウンロードし、電子出版端末（「Reader」）に転送して電子出版を利用できる。

33 他の先進国で行われているように、図書館が出版社等へ一定の利用料を支払った上で利用者が図書館による電子出版の貸与を受けるということができないとすれば、児童・生徒・学生の教育、市民の社会教育、国民の知への公平なアクセスの確保に支障が生じて、世界の流れから我が国だけが取り残される懸念を指摘する考え方がある。

一方で、紙の出版物について、商業的な販売と図書館による貸与が共存できているのは、紙の出版物においては物理的な品切れや絶版があるため、出版市場ではカバーできない利用者のニーズへの対応という観点から、図書館の果たす役割が認められているのであり、電子出版については、物理的な品切れや絶版はなくなるため、電子出版市場において存在し続け、商業サービスにより利用者のニーズに対応することが可能であることから、図書館の果たす役割はないと指摘する考え方もある。

また、国立国会図書館は、納本制度に基づいて国内で出版されたすべての出版物を収集・保存する我が国唯一の法定納本図書館であり、特別な存在であることから、一定期間経過後に電子出版のデータを消去する技術的な仕組みや、デジタル放送の私的録画機器に係るダビング１０のように貸与回数を制限する技術的な仕組み等について検討した上で、国立国会図書館による電子出版の貸与が許容可能かどうか検討することが必要と指摘する考え方もある。

さらに、既に出版された出版物のうち、出版物のつくり手、売り手がビジネスを放棄している出版物、あるいは出版物のつくり手、売り手が主体的に提供できない出版物に限って電子出版の貸与を行う等、出版市場ではカバーできない利用者のニーズへの対応等を図書館がデジタルにより充実させていくべきであり、出版社等にとって非常に負担となるデジタル化等についての連携、出版社等の販売に利する情報の橋渡し等も期待できるため、小さくても始めることが大事であると指摘する考え方もある。

懇談会報告書の 2. 6 から導かれる技術的要件

- 電子出版を紙の出版物と同様に貸与することができること
- 図書館による電子出版の貸与ができること

2.2.2.4. 懇談会報告書の 2.7 での指摘事項

【８】出版物のつくり手、売り手の経済的な利益を守る。読み手の安心・安全を守る。

（１）認証課金プラットフォームの構築

我が国の電子出版市場は携帯電話向けを中心に発展してきており、市場全体（2008 年度464 億円）の86％[34]を占めている。

我が国において、携帯電話を中心としてビジネスが形成されてきたのは、携帯電話端末の普及、いつでもどこでも閲覧可能なユーザビリティという要因に加え、携帯事業者が認証・課金を行い通信料金の請求と共に一括請求する認証課金サービス（認証課金プラットフォーム）が、少額決済を円滑に運用できるモデルとして有効に機能してきたという側面が大きい。

一方、従来の携帯電話とは異なる、iPhone、iPad、アンドロイド携帯等の汎用のスマートフォン・端末の普及が急速に進展しつつあり、出版物のつくり手、売り手は、こうした汎用端末での電子出版コンテンツの決済の在り方について検討する必要性が増している。

上述のような汎用端末においては、利用者に対して独自のID認証、課金手段を提供すること、すなわち、PCと同様に、独自の認証課金プラットフォームを構築・提供することが可能である[35]。

独自に認証課金プラットフォームを構築・提供することにより、スマートフォン・端末の提供者等の認証課金プラットフォームを利用する場合に比べて、課金コストの削減や、マルチプラットフォームに対応した統合的な顧客サービスの提供、記事単位等の提供・課金等、電子出版の提供に当たっての自由度を高められる可能性がある。

このため、課金やID等に関する技術、少額課金を可能とするシステム構築等の在り方について、あくまで自らの必要性、ビジネス上の判断に基づいて検討することが望ましい。

（２）不正流通への対策

我が国の漫画コミックは、海外においても大変な人気を誇っているが、このために、発刊日の翌日にはスキャナ等により印刷物から画像ファイル化されたコンテンツが中国語等に翻訳され不正にインターネット上で流通する等、海賊版のインターネット流通が大きな問題となっている。

こうした不正流通対策として、インターネット上の不正流通の抑止技術や海賊版の検知技術の開発、監視・排除の仕組みの検討等、関係者を中心に官民を挙げた取組を進めることが必要である。

（３）電子出版と書店

書店は出版界における顧客接点という役割、また地域における国民の文化拠点という役割も担ってきている。

今後、電子出版が普及する局面においても、ゼロサムではなくプラスサムに、紙と電子の総体として市場拡大が図られるよう、新たな技術やサービスの導入等、書店の創意工夫が活発となる環境整備が図られることが望ましい。

この点、電子出版について、ネットでのオンライン販売と、書店でのパッケージ（SDカード）販売の両方を行い、書店で購入したSDカード内の電子出版の続きをネットで購入し

ダウンロードするなど、ネットと書店を連携させるための実証が行われた[36]。

また、店頭にフェリカ対応のデジタルサイネージ（電子看板）を設置し、携帯電話をかざすことで電子出版の試し読みや有料の電子出版をダウンロードできるようにする仕組みの試行が始まっている[37]。

今後、読者のための地域の拠点である書店を通じて電子出版と紙の出版物、ネットワーク流通と店頭パッケージ流通というハイブリッドな流通を実現することでシナジー効果を発揮できるよう検討していく必要がある。

34 出典：インプレスＲ＆Ｄ「電子書籍ビジネス調査報告書 2009」

35 例えば、米アマゾン社は、Kindle for iPhone、Kindle for iPad というiPhone、iPad 上のビューアアプリから、自社サイトへのリンクにより、アマゾンのID 認証、ID に関連づけられたクレジット課金といった独自の認証課金基盤プラットフォームにより電子出版を販売しており、利用者は、アマゾンのキンドルでも、iPhone でも、iPad でも、PC でも、購入者した電子出版をアンビエントに利用することができる。

36 第３回技術WT 岩浪構成員資料「ハイブリッド型デジタルコンテンツ流通の概要と実証実験プロジェクトについて」

37 東京都書店商業組合とACCESS グループが共同で運営する携帯電話向け電子出版販売サイト「Booker's」に関する活動の一環。

懇談会報告書の 2.7 から導かれる技術的要件

- 認証課金プラットフォームの構築
- 不正流通対策
- 電子出版と書店販売の連携できる流通モデル

2.2.3. 技術的要件のまとめ

懇談会報告書の 2.1 から 2.7 から導かれる技術的要件を流通モデル、プラットフォーム、運用性、権利保護の観点から整理すると以下のようになる。

［流通モデル］

- 電子出版と書店販売の連携できる流通モデルの構築
  ネット配信とパッケージが両立すること

［プラットフォーム］

- 様々なプラットフォーム、様々な端末において利用・提供可能なこと
- 異なる電子出版端末・プラットフォーム間の相互運用性の確保
- 認証課金プラットフォームの構築

［運用性］

- 電子出版を紙の出版物と同様に長い期間にわたって利用できること
- 公共財として長期間電子出版の保存ができること
- 利用者に購入した実感（所有感）を与えられること

- 電子出版を紙の出版物と同様に貸与することができること
- 図書館による電子出版の貸与ができること
  電子出版データを物理メディアに格納ができること
  物理メディアに格納された電子出版データの閲覧ができる

［権利保護］

- 不正流通対策
  電子出版物の不正コピーができない仕掛けを講ずる
  海賊版コンテンツを検出、排除できる仕組みを講ずる

例として、正当なコンテンツであることを保証する仕掛けとこれを検証する仕組みを再生側に持たせるなどが考えられる。

2.3. ハイブリッド型電子出版流通のあるべき姿

ここでは、ハイブリッド型電子出版流通のあるべき姿を流通モデル、プラットフォーム、運用性、権利保護の観点別に整理する。

2.3.1. ［流通モデル］

- 電子出版と書店販売の連携できる流通モデルの構築

現在の電子出版されたコンテンツの流通はネット配信中心であり、紙の出版物の流通とは分離されている。サービス利用者から見れば、電子出版物のサービス提供者と紙出版のサービス提供者は異なっている。

こうしたネット配信中心の電子出版は現状の出版物の流通をいわゆる中抜きという形態に移行せしめる可能性を持っている。紙出版を提供するサービス提供者は電子出版データの提供から排除され、既存の売り手の経済的な利益を守ることができない流通構造が構築される可能性が高い。

ハイブリッド型電子出版流通は、紙出版物を扱うサービス提供者も参画できるような流通構造を構築することを目指し、電子出版データをパッケージ化によって、紙出版の流通経路で物販を可能とし、出版物のつくり手、売り手の経済的な利益を守ることも可能である。

図を用いて説明する。現状の紙出版と電子出版の関係は完全に分離されている。すなわち、電子出版のサービス提供者と紙の出版物のサービス提供者（書店）はそれぞれ提供するサービスが異なり、互いのインターラクションはない。一方、ハイブリッド型電子出版流通では従来紙の出版物を提供してきた書店は電子出版物をパッケージの形態でも提供することで、新たに電子出版物のサービスも行えるようになる。

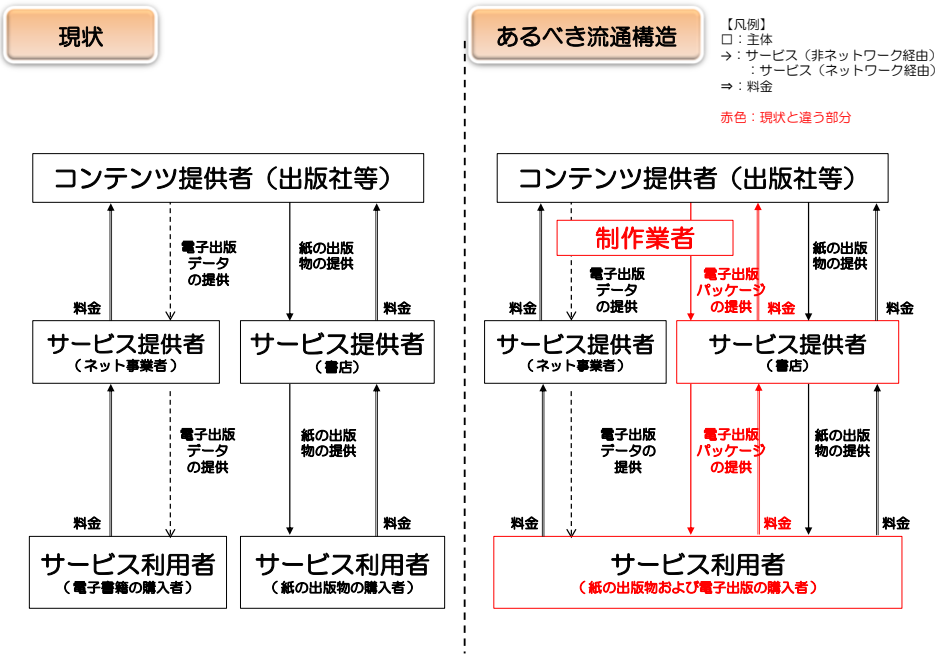


図 2-3：流通モデル

2.3.2. ［プラットフォーム］

- 様々なプラットフォーム、様々な端末において利用・提供可能なこと
- 異なる電子出版端末・プラットフォーム間の相互運用性の確保
- 認証課金プラットフォームの構築

特に、ユーザの観点からすれば、様々な端末で電子出版物の利用可能なことは重要である。現在、電子出版物を閲覧する端末は、タブレット型、スマートフォン、専用端末、PC、従来型携帯電話など多種に渡る。購入した電子出版物はユーザの所有するどの端末でも閲覧できることが求められる。

また、コンテンツ提供の観点から、コンテンツ提供者が様々なプラットフォームで自身の電子出版コンテンツ提供のできるは、コンテンツ提供の販路の拡大の観点から求められる。

異なるプラットフォームで購入した電子出版物であってもユーザの端末で閲覧できるという相互運用性の確保が求められる。

認証課金プラットフォームは決済において個人情報を扱うが、電子出版物の権利保護は個人情報を必ずしも必要としない。逆に、権電子出版物の権利保護に個人情報を持ち込むことは、個人情報保護という別の問題を持ち込むことになる。従って、認証課金プラットフォームは電子出版物の権利保護とは独立に扱うことにする。

2.3.3. ［運用性］

- 電子出版を紙の出版物と同様に長い期間にわたって利用できること
- 公共財として長期間電子出版の保存ができること
- 利用者に購入した実感（所有感）を与えられること
- 電子出版を紙の出版物と同様に貸与することができること
- 図書館による電子出版の貸与ができること

電子出版データの物理メディアを用いてパッケージ化により、運用性で指摘された課題はほぼ解決できる。ただし、パッケージ化された物理メディアには最低でも不正コピー防止機能が備わっていなければならない。音楽 CD 様な物理メディアでは不正コピー防止機能が備わっていないため、貸与先での不正コピーを防止することができないからである。

パッケージ化された電子出版物は物理メディア自体が存在するため、紙の出版物と同様に保存が可能である。紙の出版と異なるところは、物理メディアとそれを閲覧するための閲覧ビューワが必要な点にある。長い期間にわたって利用できるためには、物理メディアと閲覧ビューワがあれば閲覧が可能となる、いわゆる、オフライン動作が可能であることである。また、閲覧ビューワ自体が様々な端末で動作することと、閲覧ビューワを長期間維持・供給しつづける仕組みが併せて求められる。このためには、ある特定の企業にシステム自体が帰属するようなクローズドモデルでは、当該企業の事業撤退により、電子出版物の長期間の利用が不可能となるという問題が生ずるため、オープンなシステムが求めら

れる。

パッケージ化された電子出版物は物理メディアが存在するため、利用者に購入した実感を与えることができる。また、パッケージ化された電子出版物にしか与えられない特典などを付加することで、パッケージ化された電子出版物の価値を高めるなどの方策を講ずることもできる。

パッケージ化された電子出版物は物理メディアを貸与することで紙の出版物と同様に貸与ができる。ただし、貸与された側に、それを閲覧するための閲覧ビューワが必要にはなる。

図書館による電子出版の貸与は物理メディアに電子出版物を格納することでも実現ができる。ただし、閲覧期間、コピー禁止などの電子出版物に対する使用許諾条件を付加する必要がある。こうした使用許諾条件を付加することで、物理メディア自体の返却の必要がなくなるため、読み手にとって利便性が向上する。

2.3.4. ［権利保護］

- 電子出版物の不正コピーができない仕掛けを講ずる
- 海賊版コンテンツを検出、排除できる仕組みを講ずる
- 不正流通対策

不正流通の根源は電子出版コンテンツデータの不正コピーにある。一旦、不正コピーができれば、インターネットなどの手段で、加速度的に不正コピーされたコンテンツデータは全世界へと広がっていく。このため、コンテンツ提供者の立場からはこれを防止する対策が必須である。このため、電子出版コンテンツデータを音楽 CD ディスク様に平文データで格納することはできない。不正コピーを防止するためには、大きく分類して、コンテンツの制作段階、コンテンツの流通段階、ユーザの手に渡った段階での対策が必要となる。特にフォーカスしなければならないのはコンテンツの流通段階、ユーザの手に渡った段階での対策である。

ところが、こうした不正コピー対策はともするとユーザ利便性を阻害することになりやすい傾向にあるため、DRM（Digital Rights Management）の導入に当たっては以下の項目に留意する必要がある。

- パッケージ化された物理メディアには最低でも不正コピー防止機能が備わっていなければならない。また、使用許諾条件も不正コピー防止機能で保護できるようになっていなければならない。
- 閲覧ビューワは不正コピー防止機能のある物理メディアをアクセスし、これをセキュアに復号して表示できなければならない。また、電子出版物に付随した使用許諾条件に従って動作しなければならない。
- 使用許諾条件はコンテンツを提供する際に、適宜付与できなければならない。
- 使用許諾条件は改ざんされぬよう保護されていなければならない。また、閲覧ビューワが改ざんを検出したときには動作を中止しなければならない。
- 物理メディアと閲覧ビューワのみでの再生が可能でなくてはならない。すなわち、

再生時ネットワーク認証などネットワーク接続を前提としない、いわゆる、オフライン動作が可能でなくてはならない。

- 不正コピー防止機能により、ユーザ利便性を著しく損なうことがあってはならない。

海賊版コンテンツとして、コンテンツの不正コピーの他に、紙出版物からスキャンして作成された電子出版データがある。最近、自炊と呼ばる自分が購入した紙の出版物を電子データに変換して、これをビューワで閲覧することが盛んに行われるようになった。個人的な使用の範囲であれば著作権上の問題は生じないが、これをインターネットを介して配布すれば、いわゆる海賊版コンテンツに早変わりする。最近、こうしたコンテンツが Apple Store を通じて販売されたという事例がある。自炊は一般ユーザが容易に入手できるツールだけでできるだけに、海賊版コンテンツ作成の敷居も下がっている。

- 海賊版コンテンツを排除するために、正当なコンテンツであることを保証する仕掛けとこれを検証する仕組みを再生側に持たせ、不正なコンテンツの再生を行わないなどの手だてを講ずること。

2.4. 技術要件のまとめ

DRM は流通モデル、プラットフォーム、運用性で列挙された要件を満足できるものでなければならない。以下、それぞれのの要素に対する技術要件をまとめる。

2.4.1. 物理メディア

パッケージ化された物理メディアには最低でも不正コピー防止機能が備わっていなければならない。また、使用許諾条件も不正コピー防止機能で保護できるようになっていなければならない。

2.4.2. クライアント

クライアントは不正コピー防止機能のある物理メディアをアクセスし、これをセキュアに復号して表示できなければならない。また、電子出版物に付随した使用許諾条件に従って動作しなければならない。クライアントは使用許諾条件の改ざんを検出し、改ざんあった場合に動作を中止しなければならない。

2.4.3. DRM およびクライアント

海賊版コンテンツを排除するため、DRM は正当なコンテンツであることを保証する手だてを備え、クライアントはこれを検証する仕組みを備え、不正なコンテンツを検出したときには動作を中止できなくてはならない。

2.4.4. 配信サーバ

使用許諾条件はコンテンツ提供者がコンテンツを提供する際に、購買されたコンテンツ単位で適宜付与できなければならない。

2.4.5. DRM システム全体

物理メディアとクライアントのみでの再生が可能でなくてはならない。すなわち、再生時ネットワーク認証などネットワーク接続を前提としない、いわゆる、オフライン動作も可能であるなど複数の異なる電子出版サービスに対応できることが必要とされる。また、不正コピー対策がユーザ利便性を阻害してはならない、一方、不正機器を排除する仕組みを備えることが必要である。

3. DRM（Digital Rights Management）について

3.1. DRM とは

デジタルデータとして表現されたコンテンツの著作権を保護し、デジタルデータの利用や複製を制御する技術の総称である。

画像や映像、音楽、電子出版などのデジタルコンテンツは、アナログコンテンツとは異なりコピーを重ねても劣化しないことが利点である。一方、不法コピーでもオリジナルと変わらない品質が保持されるため、不法コピーされたデジタルコンテンツはコンテンツ提供者の死活問題ともなる。近年のインターネットの普及や USB メモリや光学メディアなど外部機器の大容量対応化の流れは安易なコピーを後押し、更に、インターネットでの配布など不正コンテンツの波及を後押しする材料ともなってきた。DRM はこのような不法利用の制限を効果的に行うものである。

コンテンツの配布側、再生側双方が DRM 対応のハードウェアやソフトウェアを使用することで、著作権に違反したコンテンツの流通を防止する。

3.2. DRM の問題点

DRM 対応のコンテンツは提供者側が推奨する特定の環境に依存することもあり、ユーザの自由な利用を制限するという問題点もある。例えば、Linux 環境では DRM 対応の音楽コンテンツはほとんど利用できないなどはこの一例である。また、OS のバージョンアップや再生機器の追加や変更などの場合には、ユーザは注意深く対応しないと購入したコンテンツを失ってしまう場合もある。コンテンツ提供者側の撤退や大幅なシステム変更も皆無とは言えないため、ユーザの恒久的なコンテンツ利用が保証されるかどうかも疑問視されている。さらに、著作権法で認められている抜粋や譲渡などの行為がほとんどの DRM 対応のコンテンツでは制限されてしまう。

現状の DRM には、制限や問題はあるものの、よりスマートでセキュアな環境への研究と模索が常に行われている分野でもある。

3.3. 各種 DRM の現状について

[コンテンツ形式との関係]
DRM 方式には、保護するコンテンツ形式との関係から、次の三つの形態がある。

- 特定のコンテンツ形式と特定の DRM 方式が不可分となっているもの（合体型）
- 仕組み上は独立であるが、特定のコンテンツ形式と特定の DRM 方式を組み合わせることを前提としているもの（併用型）
- コンテンツ形式と DRM 方式は独立で、任意の組み合わせが可能なもの（独立型）

たとえば EPUB は、使用すべきあるいはサポートする DRM 方式は特に定めず、必要とあれば、任意の DRM 方式を追加（META-INF/rights.xml というファイルに記述）できるから、それ自体は独立型だが、アップルは iBooks で EPUB コンテンツを FairPlay 方式でパッケージして配布するので、iBooks の商品としては併用型となる。コンテンツ形式と DRM の関係は独立型が望ましい。

3.4. 現状の電子出版での DRM とコンテンツフォーマット

3.4.1. [Apple iBooks]

コンテンツ形式: EPUB
DRM 方式: FairPlay
関係: 併用型
コンテンツ形式との関係: 併用型アップルが QuickTime 用に開発した DRM で、iTunes Store で用いられている。

3.4.2. [Amazon Kindle Books]

コンテンツ: AZW/Topaz
DRM: AZW/Topaz 専用
関係: 合体型

3.4.3. [Adobe Digital Editions]

コンテンツ: PDF/ EPUB
DRM: ADEPT
関係: 併用型
形態: マスター／ユーザ型
アドビは、Adobe Contents Server と Adobe Digital Editions の組み合わせで電子出版物の配信環境を提供している。

3.4.4. [SONY Reader]

コンテンツ: PDF /EPUB
DRM: ADEPT を採用（上記 Adobe 方式を参照）
関係: 併用型

3.4.5. [Google]

Google Books - DRM なしの無料 EPub ブックを配布
Google Editions - DRM ありの有料サービス
コンテンツ: EPUB
DRM: ADEPT を採用（上記 Adobe 方式を参照）
関係: 併用型

3.4.6. [Barnes & Noble Nook eReader]

コンテンツ: EPUB/ PDF

DRM: Adobe ADEPT の変形

関係: 併用型

このように、コンテンツフォーマットは EPUB を採用するケースが圧倒的に多く、DRM は Adobe DRM を用いるているケースが多い。この理由は EPUB フォーマットがオープンであること Adobe DRM の供与もオープンであることから、比較的簡単に、市場参入が可能であることによる。

3.5. DRM の主要な機能

DRM の主要な機能として、サーバ認証、機器バインド、メディアバインド、ドメイン機能の 4 つがある。それぞれの機能について説明を行っていく。

表 3-1：DRM の主要機能

DRM主要機能

	サーバ認証	機器バインド	メディアバインド	ドメインサポート
特徴	再生時にサーバでユーザ認証を行い、再生を許可する	再生端末／アプリに埋め込まれた秘密情報で再生処理を行う	メディアにコンテンツを保護記録する。特定メディア以外での再生は不可。	複数機器でのコンテンツの共有を可能とする。
ネットワーク処理	再生時必須	再生時不要	再生時不要	再生時不要
不正機器／不正ユーザの無効化	サーバでのユーザ認証時に不正機器／不正ユーザの無効化可能	サーバ認証との組み合わせにより、不正ローカル機器を無効化可能	不正機器の無効化可能	サーバ認証との組み合わせにより、不正ローカル機器を無効化可能

3.5.1. サーバ認証

サーバ認証はインターネットに接続された機器の正当性を認証サーバで認証する仕組みである。認証サーバによって接続された機器が不正と判断された場合は無効化され、以後、コンテンツの再生などはできなくなる。この機能は主に、ストリーミングモデルやクラウドモデルで用いられる。この場合、機器は必ずインターネット接続を前提とし、接続される毎に認証が行われる。この機能の最大の欠点は、再生時に必ずインターネット接続を必

要とするため、インターネット接続ができない場合、当該機器は再生に使用できないことである。

サーバ認証機能は、不正機器の無効化にも利用することができる。既に、不正機器であることが何らかの方法で、認証サーバ側で把握できていれば、当該機器がインターネット接続されたタイミングでサーバ認証をかけることで、当該機器を無効化することができる。認証サーバ接続を強制的に促す方法として、コンテンツの利用期間を限定し、再利用のための利用期間更新のため、サーバ接続を必須とするなどの方法が考えられる。

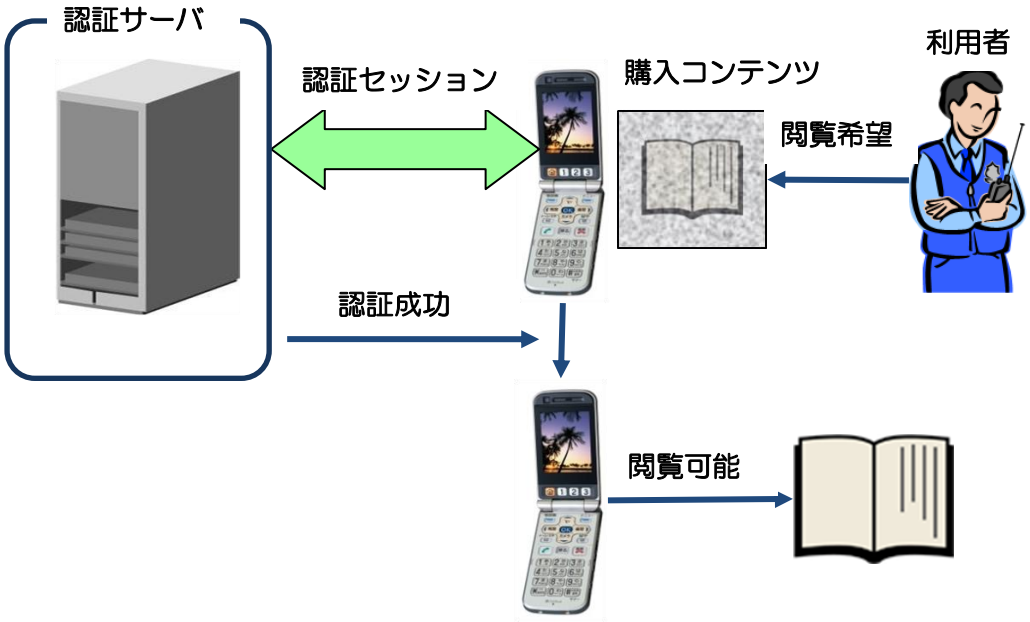


図 3-1：サーバ認証

3.5.2. 機器バインド

機器バインドは、ダウンロードされたコンテンツを当該機器のみでしか使用できないようにする機能である。コンテンツをダウンロードした携帯電話やパーソナルコンピュータのみでしかコンテンツ再生が行えない場合はこの機能を利用している。機器バインドはダウンロードしたコンテンツを当該機器の固有情報で暗号化しておけば簡単に実現できるので、導入しやすい反面、利用者が購入したコンテンツを自身が所有する様々な機器で利用したいという要望に応えられないため、評判が悪い。しかし、コンテンツの安全性の観点からはダウンロードした機器以外にはコンテンツを持ち出せないという点で優れている。

たとえ物理メディアに書き出してもローカル機器固有の情報に基づいて秘密情報を保護する場合は機器バインドに分類される。その理由はローカル機器固有の情報に基づいて物理メディアに書き出した場合、当該物理メディアは当該ローカル機器においてのみ使用可能なため、メディアバインド機能の持つ、正当な機器であればどの機器でも使用できるという要件を満たさないからである。

3.5.3. メディアバインド

メディアバインドは物理メディアにコンテンツを保護して記録し、正当な機器でのみで再生可能な機能である。基本的な保護技術として、CPRM や AACS などが利用され、物理メディアとしては、DVD や Blue-Ray や SD カードなどが用いられている。

この機能の最大の特徴は再生時にインターネット接続を必要としないため、いわゆる、オフライン動作が可能な点にある。ただし、機器は物理メディアを扱うことができなきてはならない。光学ディスクはこれを扱うための機械的ドライブを機器に備えなくてはならないので、携帯機器には不向きという欠点もある。

メディアバインドは機器バインドされたコンテンツを一定の使用許諾条件のもとで、物理メディアに出力する際にも用いられる。例えば、地上波デジタル録画コンテンツを光ディスクに Copy するのもメディアバインド機能を用いた例である。メディアバインドを用いたコンテンツは物理メディアとして、単体で流通可能な形態であることが利点である。

3.5.4. ドメイン機能

ドメイン機能はドメイン管理サーバを介し、複数の端末機器で利用者が購入したコンテンツを共有するネットワーク連携の仕組みである。（ただし、コンテンツの共有にはコンテンツ保有者が、複数の端末機器でのコンテンツの共有を許諾した場合のみ適用される。）

この機能の導入の背景には、オンライン販売で購入したコンテンツは配信を受けた端末機器でしか使用できない機器バインドによる利用者の不便を解消するために導入された。利用者が自分の持つ複数の機器をドメイン管理サーバに登録することで、配信を受けた端末機器以外でも当該コンテンツの再配信により当該コンテンツを利用できる機能である。ドメイン管理サーバに登録できる端末機器数には一定の制限が設定されることが多いが、通常の利用範囲での齟齬は生じない設定で運用される。この機能を用いると単に機器バインド機能しか有していない端末機器でも対応できるという利点がある。

ドメイン機能は、利用者が特定できることを前提に、一度購入したコンテンツに関しては、利用者がドメイン登録した機器に対しては、新たに無償でコンテンツを配信するなどして、利用者の利便性の改善を図る場合も含まれる。

図 3-2：ドメイン機能

3.6. DRM における使用許諾条件

使用許諾条件は売り方や値付けなど、ビジネス形態と深いかかわりあいを持つ。ここでは DRM におけるコンテンツの使用許諾条件について説明する。

3.6.1. 使用許諾条件の例

使用許諾条件はコンテンツ提供者がコンテンツをどの様な使用条件で販売するか、コンテンツの販売時点で付与することができる。使用許諾条件は購買した個人毎に異なることもあり、特に販売価格との兼ね合いになることが多い。例えば、再生可能時間を設定した使用許諾条件はいわゆるレンタルに相当するため、買い取りに比べ、販売価格は安価に設定される場合が多い。こうした意味から、使用許諾条件はビジネスモデルと密接な関わり合いがある。

なお、使用許諾条件は改ざん防止の手だてが施され、かつ、クライアントでチェックが行われ、クライアントは使用許諾条件に従った動作をしなければならない。こうしたことから、使用許諾条件はコンテンツを暗号化する暗号鍵に付加されることがある。

3.6.1.1. コンテンツの Move 制御

コンテンツの合法的なコピーが許されない場合、すでに機器内に存在する再生可能なコンテンツを他の機器で再生したい場合にこの機能を利用する。ダビング 10 が解禁になる以前の地上波デジタル放送の録画では広くこの機能が用いられていた。再生可能なコンテンツは常に、1 個しか存在しない。Move が行われると Move 元の機器でのコンテンツ再生は不可能となり、代わりに、Move 先の機器でのみコンテンツの再生が可能となる。Move 作業中に電源断などの障害が発生するとどちらの機器でもコンテンツ再生が行えなくなるなどの問題点も含んでいる。

3.6.1.2. コンテンツのコピー回数制御

この使用許諾条件はコンテンツの合法的なコピーの回数を制御する。ダビング１０と同じように、コピーを行う度に、コピー回数は減じられる。コピーを禁止する場合はこのカウンタをゼロに設定する。コピー禁止の場合はコンテンツの Move は許諾することで、他の機器でのコンテンツ利用を認める設定をすることが多い。

この使用許諾条件を用いることで、利用者の持つ複数の機器でのコンテンツの閲覧が可能となる。合法的なコピーを行うためには使用許諾条件に従って、安全にコンテンツのコピーを行う機器（専用アプリケーション）が必要であり、PC が母艦として用いられる。

3.6.1.3. 再生開始時期制御

この使用許諾条件はコンテンツ再生を開始する時期を制御する。映画の様に、封切り以前にはその映画は見られないのと同様、ある時期以降からのコンテンツ再生を可能とする。事前に発売し、封切り時期の設定を可能とする。先行予約販売などに使用できる機能である。特に、ダウンロードを主眼としたネット販売では、発売と同時に配信サーバへのダウンロード要求が集中し、通信トラフィックを著しく低下させることがある。この使用許諾条件を利用することで、発売日以前のダウンロードが可能となり、通信トラフィックの平

準化に貢献する。

3.6.1.4.再生終了時期制御

この使用許諾条件はコンテンツ再生が不能となる時期を制御できる。コマーシャルなどが付加されたコンテンツはコマーシャルの契約有効期間を越えた場合、コマーシャルの契約上の理由から、コンテンツ再生をできなくする必要が生ずる場合がある。この使用許諾条件はこうした場合に有効である。

3.6.1.5.再生回数制御

コンテンツの再生回数を制御できる使用許諾条件である。ただし、何をもって当該コンテンツを再生したと定義次第で、利用者の感覚と食い違いが生ずる場合もある。例えば、1 ページでも再生すれば、当該コンテンツを再生したと定義したとすると、再生回数は 1 回とカウントされるため、利用者からのクレームにもなる。逆に、全てのページを再生した場合のみ、再生回数を 1 回とカウントする定義すれば、最終ページを再生しなければ、何回でも再生できるため、コンテンツ提供者からは不満が出る可能性がある。

実際に使用するのが難しい使用許諾条件ではあるが、回数の設定やコンテンツ再生定義を工夫することにより、利用できる可能性がある。

3.6.1.6.再生可能期間制御

この使用許諾条件はコンテンツの再生期間を制御する。例えば、ここに 1 週間と記載されると再生可能な期間は最初に再生をしてから 1 週間はコンテンツ再生が可能となる。いわゆる、レンタルモデルの実現を可能とする使用許諾条件である。

再生開始時期制御や再生終了時期制御などを併用して運用もできる。現在ビデオレンタルなどで行われている 1 週間貸し出しは、再生可能期間を 1 週間に設定し、更に、再生終了時期を貸し出し後、1 週間後の時期に設定すれば、同じことができる。

3.6.1.7.プリント出力制御

電子出版特有の使用許諾条件である。電子出版物を紙にプリントアウトすることで、紙の出版物に容易に変換できるため、プリント出力について許諾するか、プリント回数を含め設定することができる。

4. ハイブリッド型電子出版流通におけるコンテンツ保護の要件

4.1. 前年度実証実験を踏まえて

平成 21 年度補正予算「ユビキタス特区事業」ハイブリッド型デジタル（電子）出版流通の基盤技術開発における実証実験では以下のコンテンツ保護要件を定義し、システム開発を行った。ここでは先年度の実証実験で定義されたコンテンツ保護要件を検証しつつ、更に深掘りしていく。（図 4-1 は先年度概要報告から引用した。）

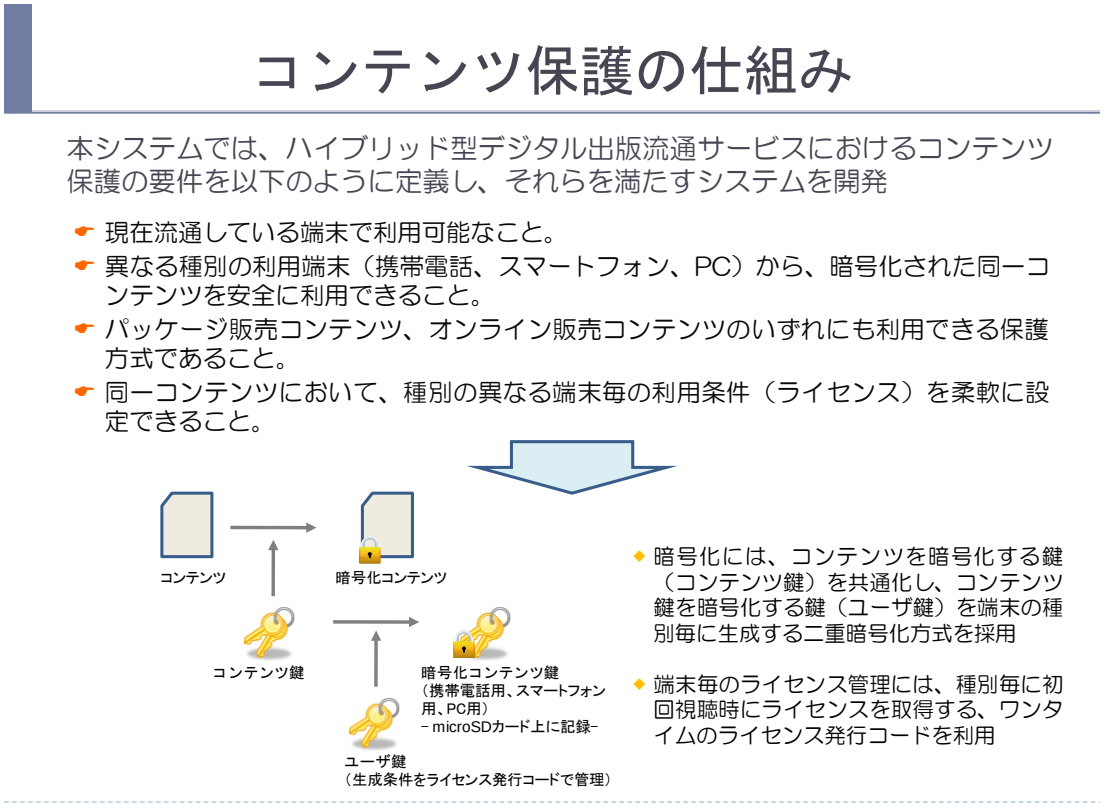


図 4-1：ハイブリッド型電子出版流通コンテンツ保護要件

ハイブリッド型電子出版流通コンテンツ保護要件として、以下の 4 点が挙げられている。

- 要件１：現在流通している端末で利用可能なこと。
- 要件２：異なる種別の利用端末（携帯電話、スマートフォン、PC）から、暗号化された同一コンテンツを安全に利用できること。
- 要件３：パッケージ販売コンテンツ、オンライン販売コンテンツのいずれにも利用できる保護方式であること。
- 要件４：同一コンテンツにおいて、種別の異なる端末毎の利用条件（ライセンス）を柔軟に設定できること。

4.2. 利用者における評価

平成 21 年度補正予算「ユビキタス特区事業」ハイブリッド型デジタル（電子）出版流通の基盤技術開発における実証実験結果は以下の通りである。

電子出版物の購入に関しては、パッケージ購入から、続きをオンライン購入するコンセプトには 8 割が利用意向を示し、受け入れられる可能性が高いと思われる。特に、有料の電子出版利用者やコミック利用金額に高めの支出を行っている層は、初回のパッケージ購入の後、続きのパッケージ購入或いは続きをオンライン購入という形で、パッケージ購入を支持している。

また、購入パッケージの中に未購入の商品が含まれることに対しては、利用者に対しコンテンツデータの先渡しが可能であるため、コンテンツデータのダウンロードを省き、コンテンツデータのダウンロード時間の短縮という点も支持されている。その一方で、購入したパッケージの中の商品にまたお金を払うことに対する抵抗感を指摘する声もある。

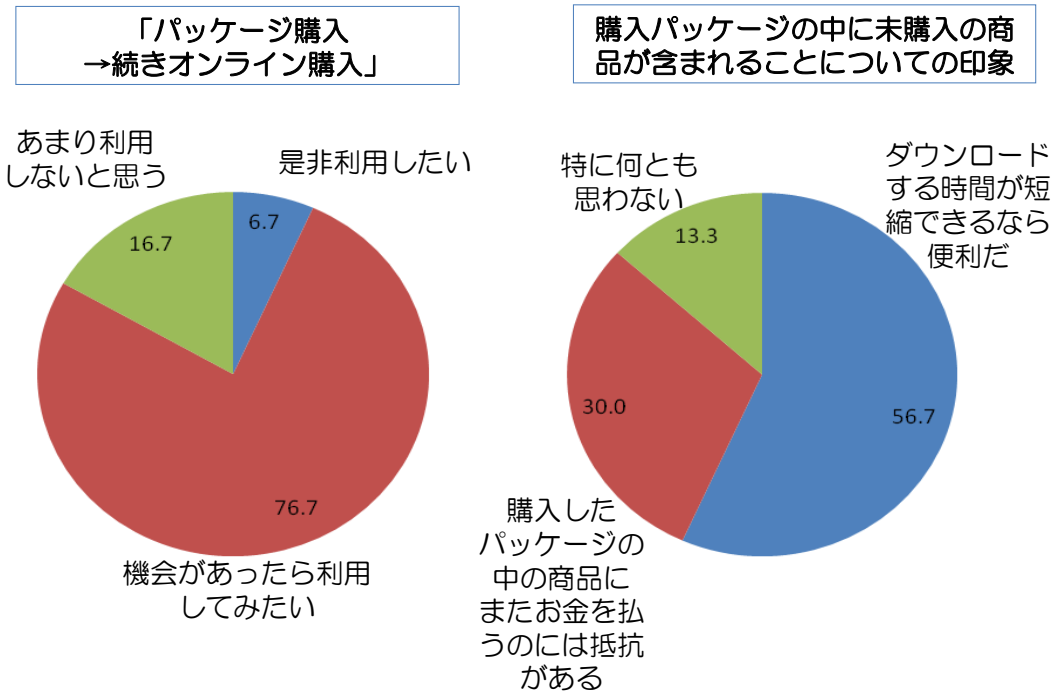


図 4-2：前年度実証実験結果

4.3. コンテンツ保護要件の展開

4.3.1. 要件１の展開

この背景にはある一定条件を満たす端末を利用可能とすることで、コンテンツを閲覧する機会を増やすことにある。電子出版流通においても、入り口に相当する電子出版コンテンツと出口に相当する端末を増やすことが普及のための王道である。新たに投入される端末の他、既に流通している端末を出口として利用することができれば、短期間に出口を増加させることが可能である。

既に、流通している端末機器のハードウェア資源を増強することは不可能であるから、ソフトウェアのアップデートで対応せざるを得ないため、端末機器にはソフトウェアのアップデート機能がなくてはならない。既に流通した端末機器はハイブリッド電子出版流通に対応したソフトウェアを持っていないからである。但し、アップデートをオンラインで行うか、PC などを介してオフラインで行うかの方法は問わない。

端末機器は少なくともパッケージ販売コンテンツとオンライン販売コンテンツのいずれかに対応できるためには、端末機器の能力として、ネット接続機能、物理メディアサポート機能のいずれかを有していることである。どちらもサポートできない端末機器には対応できない。

結論としては対象となる端末機器以下のようになる。

- ネット機能も物理メディアもサポートできない機器は除外
- ネット機能だけをサポートできる端末機器はオンライン販売に対応
  → コンテンツ保護は機器バインドで実現
- 物理メディアサポートをできる端末機器はオフライン販売に対応
  → コンテンツ保護はメディアバインドで実現
- 両方の機能をサポートできる端末機器はオンライン販売、オフライン販売の両方に対応
  → コンテンツ保護はメディアバインドで実現

つまり、新たに対応する端末機器はオンライン販売、オフライン販売の両方に対応しなければならないが、既に流通している端末機器ではいずれか一方の販売形態しか対応できない。

オフライン販売されたコンテンツをネット機能だけをサポートしている端末機器で閲覧したり、オンライン販売されたコンテンツを物理メディアだけをサポートしている機器で閲覧したい場合の解決策を講ずる必要がある。DRM の説明で述べた通り、ドメイン管理はサーバを介し、複数の端末機器で購入したコンテンツを共有する仕組みである。ただし、コンテンツの共有にはコンテンツ保有者が、複数の端末機器でのコンテンツの共有を許諾した場合のみ適用される。

4.3.2. 要件２の展開

暗号化された同一コンテンツを利用できるという要件はコンテンツ配信サーバ側のスト

レージサーバ或いは処理サーバに過大な資源を要求することが理由である。
　コンテンツデータは容量が大きいため、複数のコンテンツデータの保存には膨大な記憶容量を必要とする。コンテンツの暗号化を利用者毎に行う方法は、暗号化されたコンテンツは利用者の数だけ必要するため、これらを保存する場合は保存容量が利用者の数に比例するので、配信サーバ側の保存容量が膨大になる。必要保存量は利用者数 X コンテンツ数 X コンテンツデータとなる。この方法は利用者増加に従って、配信サーバの増強を絶えず行う必要が生ずるため、配信インフラ投資がコンテンツ提供者には重荷となる。

　一方、利用者毎にコンテンツデータを暗号化することを回避するには、コンテンツデータを都度暗号化することによりコンテンツデータの記憶容量を抑制する方法が考えられる。しかし、この方法は暗号化サーバに高いスループットが要求される。利用者数の増大に伴い、やはり、配信インフラの増強が必要となり、配信には不向きである。
　更に、物理メディアへのプリレコードの際に、大量の異なるデータの書き込みが必要となり、書き込み装置コストの上昇や生産性の面で不利である。従って、利用者毎の固有化を暗号化コンテンツで行うのは非実現的で避けるべきである。

4.3.3. 要件３の展開

　パッケージ販売コンテンツ、オンライン販売コンテンツのいずれでも利用できることはハイブリッド電子出版流通においてはコンセプトそのものである。DRM はどちらも統一的に扱えることがエレガントである。更に、要件１を満足させるためには DRM には４つの機能を備えなければならない。

4.3.4. 要件４の展開

　暗号化された同一コンテンツを利用するため、利用者毎に異なる使用許諾条件を付与できる仕組みが必要となる。これも DRM システムを実現する際の要求事項となる。

4.4. ガイドラインで推奨するコンテンツ保護の仕組み

　以上、要件１から要件４までの展開結果をもとに本ガイドラインで推奨するコンテンツ保護の仕組みについて述べる。

4.4.1. コンテンツ毎に一つの暗号鍵を用いることによる暗号化コンテンツデータの共通化

4.4.1.1. 暗号化コンテンツとその暗号鍵（コンテンツ鍵）の関係

　この理由は要件２でも述べたとおり、コンテンツデータ自体の容量が大きいため、コンテンツ配信側の負担が大きいことにある。コンテンツデータ自体の保存に必要な記憶容量が大きいこととコンテンツデータの暗号化、復号に潤沢な計算資源を必要とすることにある。また、コンテンツの暗号化を利用者毎に行う方法は、暗号化されたコンテンツは利用者の数だけ必要となるため、利用者増加に従って、配信サーバの増強を絶えず行う必要が

生ずるため、配信インフラ投資がコンテンツ提供者には重荷となるからである。
一方、利用者毎にコンテンツデータを暗号化することを回避する方法である都度暗号化は暗号化サーバに高いスループットが要求するため、利用者数の増大に伴い、やはり、配信インフラの増強が必要となる。更に、物理メディアへのプリレコのときは、大量の異なるデータ書き込みが必要となり、書き込み装置コストの上昇や生産性の面で不利である。
従って、利用者毎の固有化は暗号化コンテンツで行うのは非実現的で避けるべきである。

利用者に配送するコンテンツ暗号鍵はどうすれば良いか？
配信サーバから安全に該当コンテンツの暗号鍵を配送する仕組みが必要である。
ワンタイムのセッション鍵を配信サーバと端末機器間で生成し、これで当該暗号鍵を暗号化して配送する。共通秘密鍵や公開鍵を用いた方法など様々あるが、特に問題点はない。配送された当該暗号鍵を安全に端末機器で保護すれば良い。
物理メディアにプリレコードする場合は、物理メディアで暗号鍵を安全に保護する仕組みが必要である。また、書き込み機器と物理メディア間のインタフェイスは安全性が保証されなければならない。すなわち、暗号鍵が平文状態で物理メディアに送られることは避けなければならない。

利用者の端末機器では暗号鍵はどのように保護されるか？
コンテンツデータ毎に同一の暗号鍵をそのまま保存することは、どこか一箇所でハッキングされコンテンツ鍵が流出すると対象となるコンテンツは全てハッキングされたことになる。こうした事態に至らぬよう、利用者端末機器毎（物理メディアも含む）に異なった形式で暗号鍵を保存しておくかなければならない。端末機器や物理メディアには安全にコンテンツ鍵などの秘密情報を格納する仕組みが必要とされる。

◊　**当該暗号鍵を端末機器固有の暗号化鍵に付け替える方法**
当該暗号鍵を端末機器固有の暗号化鍵に付け替える方法として、コンテンツデータの暗号化し直しがある。こうした再暗号化処理は端末機器内で安全に行われなければならない。これは配送用の暗号化と格納用の暗号化とを区別する考え方に基づく。この方法は様々なDRMからのコンテンツを受け入れる点で、汎用性が高い。しかし、配送用に暗号化されたコンテンツデータを端末機器内部で一旦復号し、端末機器固有の暗号鍵で再暗号化しなければならず、端末機器の処理負担が大きい。

◊　**当該暗号鍵を端末機器固有の形式に変換する方法**
当該暗号鍵を端末機器固有の形式に変換する方法として、配送された暗号鍵を端末機器内で固有の暗号で暗号化して保存する方法がある。この方法の場合、コンテンツデータの再暗号化は行われないため、前述の方法に比べ、端末機器の処理の観点からは有利である。従って、配送された暗号鍵を端末機器内で固有の暗号で暗号化して保存する方法が端末機器の実装、安全性の面から有利であると結論付けできる。

4.4.2. 一重鍵と二重鍵との相違点

一重鍵方式においては保護の対象は暗号化に用いたコンテンツ鍵である。コンテンツ鍵を保護することにより、結果的にコンテンツデータ保護が可能となる。コンテンツ鍵とコンテンツデータは強連結の関係にある。保護すべきコンテンツ鍵はコンテンツデータの個数だけ必要とし、かつコンテンツ鍵とコンテンツデータは分離して扱うことができない。メディアバインドだけの機能を実現したい場合は一重鍵方式でも十分対応できる。

メディアバインド、機器バインドはともに、端末機器の固有情報あるいは物理メディアの固有情報を用いて、コンテンツ鍵をローカルに保護するため、コンテンツ鍵を発行するサーバからは管理できない難点がある。

一方、二重鍵方式においては、コンテンツ鍵を暗号化するのに用いた暗号鍵（図中ではユーザ鍵と表示）である。ユーザ鍵を保護することにより、暗号化に用いたコンテンツ鍵と使用許諾条件の保護が可能となり、コンテンツ鍵によって暗号化されたコンテンツデータは間接的に保護される。つまり、二重鍵方式はコンテンツ鍵とコンテンツデータは弱連結の関係にある。このため、コンテンツ鍵とコンテンツデータは分離して扱うこともできる。なお、二重鍵方式は一重鍵方式を包含する関係にある。

原理的にはユーザ鍵はコンテンツデータの個数に依らず 1 個でも良いが、ユーザ鍵を複数個用意し、ユーザ鍵自体にもそれぞれ使用許諾条件を設定し、ユーザ鍵とサービスを関連付ければ、複数の使用許諾条件の異なるサービスを互いに独立に制御することもできる。

4.4.3. 二重鍵暗号方式のメリット

二重鍵方式においては、端末機器の再生時にコンテンツ鍵とコンテンツデータが揃っていれば良いだけで、コンテンツデータとコンテンツ鍵の入手のタイミングを制限しない。すなわち、入手が同時であっても、コンテンツデータの入手が先行しても、コンテンツ鍵の入手が先行するといういずれの場合も許容される。このため、多様なビジネスモデルを構築できる利点を有している。

二重鍵のメリットは利用者にコンテンツ鍵を配送する場合にも効果を発揮する。すなわち、機器固有情報が鍵を配信する鍵サーバと端末機器間で秘密情報として共有していれば、ユーザ鍵を用いて暗号化されたコンテンツの暗号鍵はすでに、固有情報化されているので、これをそのまま機器あるいは物理メディアに格納するだけで良い。従って、コンテンツ鍵の配送、保存には安全性を求める必要がない。暗号化コンテンツを再生する場合のみ、端末機器に安全性を求めるだけで済む。また、コンテンツ鍵に使用許諾条件を付加することも、ユーザ鍵を物理メディアの固有情報として利用することにより容易に行えるので、メディアバインド機能についても二重鍵方式での対応が可能である。

機器バインド機能についても前述のユーザ鍵を機器固有情報として利用すれば、二重鍵方式で実現できる。ただし、機器はユーザ鍵を安全に保管できなければならない。この場合、ユーザ鍵は鍵サーバの管理下に置くことができる。

また、ドメイン参加も二重鍵方式は簡単に実現ができる。ユーザ鍵レベルで同一ドメイン管理をすれば良いからである。このため、オフライン販売された物理メディアをドメイン参加させるなどして、オンライン販売にしか対応できない機器バインドであってもコンテンツの共有が可能となる。

以上の観点からすれば、二重鍵方式はオンライン販売におけるコンテンツ鍵の安全な配送および保存、オフライン販売におけるメディアバインド機能の実現が容易にできるため、機器を DRM の統一的な支配下に置くことができる。ハイブリッド型電子出版流通では二重鍵方式の持つメリットを上手に活用している。

［まとめ］

二重鍵方式における基本的技術要件は、ユーザ鍵が適切な方法で安全に保護されなければならないということである。ユーザ鍵を導入することで、同じアーキテクトを用いることで、機器、物理メディアを意識することなく統一的に扱うことができる。

更に、ドメイン管理機能を併用することで、利用者の持つ機器間での購入コンテンツの相互利用が可能となる。

4.4.4. 補足：公開鍵方式は何故、コンテンツ暗号に用いられないか？

共通鍵暗号方式に比べ暗号化、復号に時間がかかる。RSA では 1000 ビット以上を推奨していることから分かるように、共通鍵暗号方式に比べ鍵長が長い。このため、データ量の多いコンテンツデータの復号は端末機器に潤沢な計算資源を求めることになり、その結果、機器コスト上昇、消費電力の上昇など端末機器への負担が大きい。

また、公開鍵と秘密鍵のペアを用いるため、配信側は利用者毎に設定される公開鍵で都度コンテンツデータを暗号化しなくてはならない。従って、暗号化された同一コンテンツを利用ができない。従って、公開鍵を用いてコンテンツデータを暗号化する方法は採用することは得策でないため、一般的に用いられてない。

5. ハイブリッド型電子出版流通における物理メディアについて

5.1. パッケージに用いる物理メディアにおける SD カードの必然性

パッケージ化されたデジタルコンテンツを格納する物理メディアは、その物理的形状に加え、入手性、コスト、対応機器の多さ、ユーザからの支持を考慮しなければならない。

パッケージ化されたデジタルコンテンツを格納する物理メディアは、大別すると CD-ROM や DVD-ROM などの光ディスク系とフラッシュメモリを用いた半導体メモリ系の２つが候補に挙げられる。

光ディスク系は現在すでに、デジタルコンテンツの配布メディアとして広く普及しており、入手性、コストの面では優れているものの、対応機器に光ディスクドライブを要する点で、モバイル機器における搭載には難点がある。

一方、フラッシュメモリを用いた半導体メモリ系はビット単価コストで、光ディスク系には劣るものの、近年の半導体微細化技術の進展により、フラッシュメモリの大容量化には目を見張るものがあり、ビット単価コストも以前とは比べものにならないほど改善してきている。特に、少量多品種生産になれば、パッケージ全体のコスト差は更に小さくなる。

フラッシュメモリを用いた半導体メモリ系は光ディスク系のように、光ディスクドライブに代わり、スロットを使用するため、小型かつ低消費電力を特徴とし、モバイル機器でも搭載が可能であることから、対応機器の多さで光ディスク系をはるかに凌ぐ。

フラッシュメモリを用いた半導体メモリには、SD カード、MMC カード、コンパクトフラッシュカード、USB フラッシュメモリなど様々な形状を持つメモリメディアが現存する。

フラッシュメモリを用いたメモリメディアにおけるシェアは SD カードがメモリカードとしての de-facto の地位を固めつつあり、携帯電話におけるサポートに至っては 90%に達している。de-facto の地位にあるということは User に対する認知度、入手性の点で極めて有利である。SD カードは全数 CPRM（Copy Protection for Recordable Media）という著作権保護機能が搭載されている。（CPRM については後述）

SD カードと並んで、普及率、認知度の高いのは USB フラッシュメモリである。USB フラッシュメモリは接続端子が USB であるマスストレージであることを除けば、これといった標準仕様は存在せず、個別に保護機能のあるもの無いもの様々な仕様が存在する。

商品パッケージについて、平成 21 年度補正予算「ユビキタス特区事業」ハイブリッド型デジタル出版流通の基盤技術開発実証実験において利用者調査が行われている。

購入したい商品パッケージタイプで最も高く支持されていたのは「SD ビデオタイプ」で、4 割強の支持を集めている。特に有料の電子出版物利用者に限れば、7 割以上が支持しているという結果が得られている。支持の理由はコンパクトさ、収納性、パッケージデザイン、機能のバランスなどが挙げられている。また、利用しやすいと思う購入場所では書店やコンビニエンスストアで 9 割弱を占め、紙出版物と同様な感覚を利用者が抱いていることをうかがわせる。

図 5-1：商品パッケージに関する利用者調査

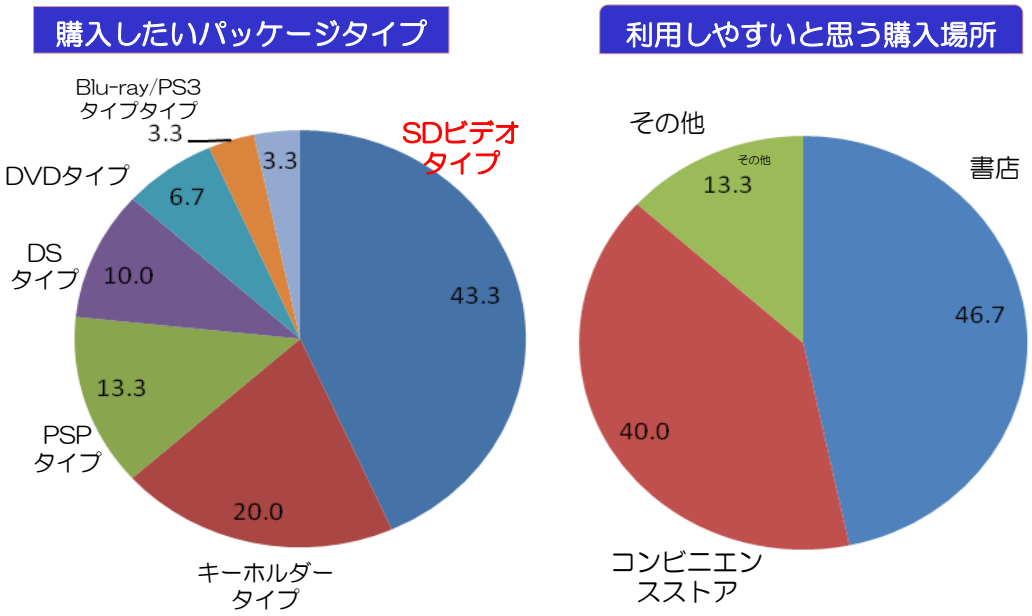


図 5-2：商品パッケージに関する利用者調査結果

SD カードの普及率と認知度、全数 CPRM という著作権保護機能の搭載、前年度の実証実験結果を加味すれば、パッケージ化されたデジタルコンテンツを格納する物理メディアは SD カードを用いることが極めて妥当であると結論付けられる。

5.2. SD カードの著作権保護機能とその利用方法

前述の通り、物理メディアとして SD カードを選択した場合、これをどの様に利用すれば良いかを以下に述べる。

5.2.1. メディアバインド機能の実現

物理メディアとして SD カードの有するコンテンツ保護機能 CPRM(Content Protection for Recordable Media)を利用することにより、パッケージ販売に必要となるメディアバインド機能が容易に実現できる。なお、SD カードの CPRM を利用したアプリケーションには着うた、ワンセグ録画再生などがある。

ここで、SD カードにおけるコンテンツ保護について説明する。不正コピー防止はコンテンツデータの暗号化とコンテンツデータを暗号・復号化するためのコンテンツ鍵を SD カード内で保護することにより行われる。

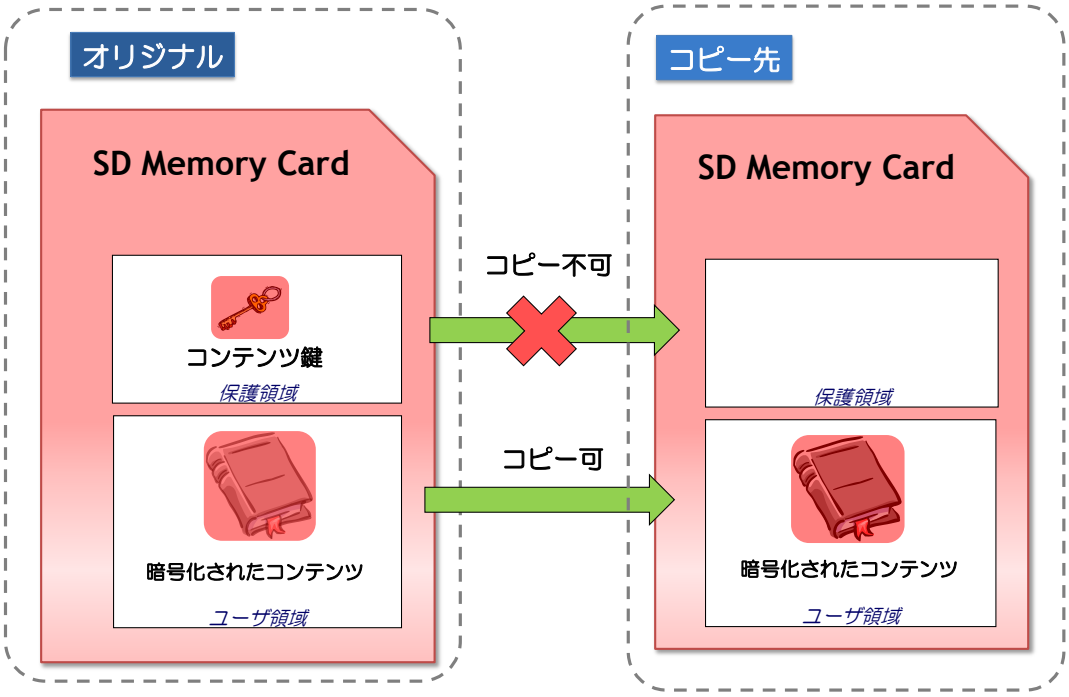


図 5-3：SD カードにおけるコンテンツ保護

SD カードのメモリはホスト機器との認証なしにアクセスできるユーザ領域とホスト機器との認証を必要とする保護領域から構成される。典型的な使用方法として、暗号化されたコンテンツデータはユーザ領域に格納し、コンテンツ鍵は保護領域に格納する方法がある。通常の使用方法ではホスト機器は保護領域のアクセスができないので、保護領域に格納されたコンテンツ鍵はコピーできない。ホスト機器は暗号化されたコンテンツデータのみコピーできる。ホスト機器を用いてオリジナルの SD カードのコピーを行うと、コピー先の SD カードでは暗号化されたコンテンツデータを復号するためのコンテンツ鍵のコピーができない。このため、コピー先の SD カードを用いて、コンテンツデータの再生はで

きない。

すなわち、単なる暗号化されたコンテンツデータのみでは不正コピーの目的である再生可能なコンテンツデータのコピーを達成することができないため、コンテンツ保護ができる。すなわち、SD カードが保護領域に保護したいデータとしてコンテンツ鍵を安全に保持することで、コンテンツ保護を実現する。

SD カードの保護領域をアクセスするためには、ホスト機器に Device Key と呼ばれる秘密情報を持たせる。Device Key は SD カードの保護領域をアクセスするための SD カードとホスト機器との認証に使用されるとともに、SD カードの保護領域にあるデータを復号するためにも使用される。Device Key は 4C とライセンス契約を結び、供給を受けなくてはならない。Device Key は厳重な扱いを要する秘密情報であり、その扱い方は 4C の規則に従わなければならない。

5.2.1.1.SD カードにおける権利保護されたコンテンツの復号

ここでは、SD カードにおける権利保護されたコンテンツの基本的な復号方法について説明する。

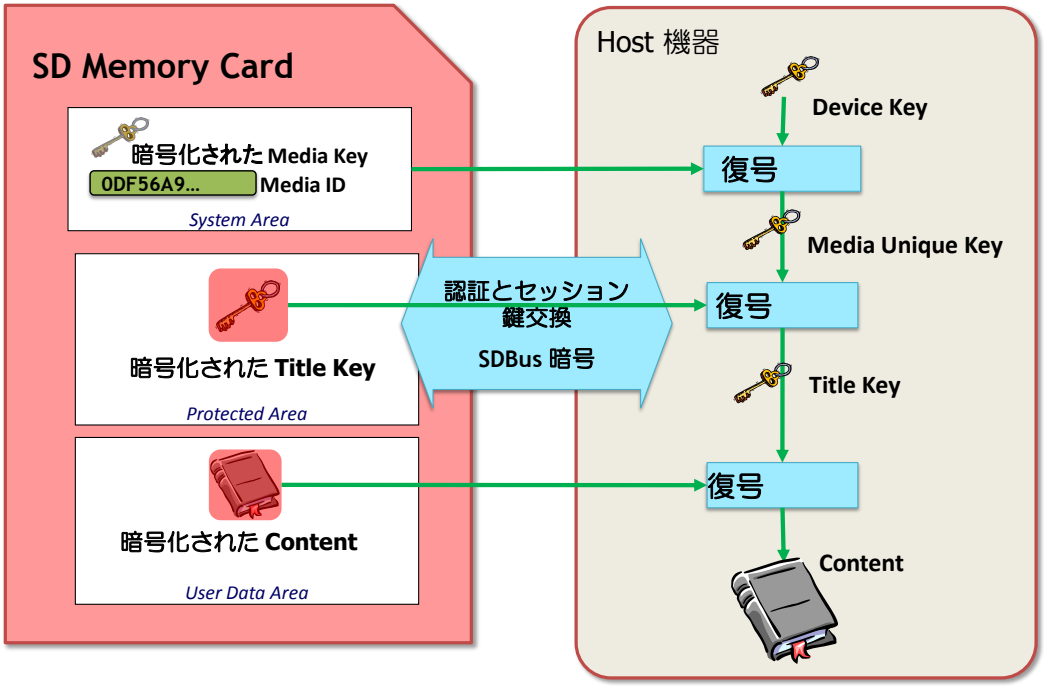


図 5-4：SD カードにおける権利保護されたコンテンツの復号

SD カードの内部構造を更に詳細に分類すると３つメモリ領域で構成される。システム領域、保護領域、ユーザ領域の３つである。システム領域は読み出し専用のメモリ領域で、ここには暗号化された Media Key と SD カードで固有な Media ID が格納されている。Media

Key と Media ID を用いて、SD カード毎に固有な Media Unique Key が生成される。

SD カードと Host 機器の認証については詳細は割愛するが、Host 機器が Device Key を用いて SD カードに格納された暗号化され Media Key を復号し、Host 機器内で Media Unique Key を計算し、これが SD カードの持つ Media Unique Key と一致したときのみ認証に成功する。

保護領域へのアクセスは SD カードと Host 機器の認証が成功したときのみ可能である。アクセスする際、セッション毎に SD カードと Host 機器の間で異なるセッション鍵を交換し、これを用いて保護領域のデータを暗号化（SD Bus 暗号）して出力することで、SD カードの出力を観測して、保護領域内のデータを推測するという攻撃を防いでいる。

なお、保護領域に格納されるデータは SD カードの Media Unique Key で暗号化されているため、Host 機器側では、SD Bus 暗号を復号した後、Media Unique Key を用いて更に復号することで、コンテンツ鍵を取得し、暗号化されたコンテンツを復号する。

なお、Host 機器の実装には 4C の定めるロバストネスルールが適用される。

5.2.1.2. SD カードにおける二重鍵暗号方式の実現

前章で二重鍵方式を採用することにより、オンライン販売とパッケージ販売の両方を極めて能率良く、かつ安全に行えることも併せて述べた。

既に、4C では SD カードにおける権利保護に関して、２つの規格を用意している。SD-CPRM と SDSD-CPRM である。これら 2 つの規格について説明する。

（www.4centity.com/docs/**SDSD-CPRM**_WP_R2-121107.pdf）

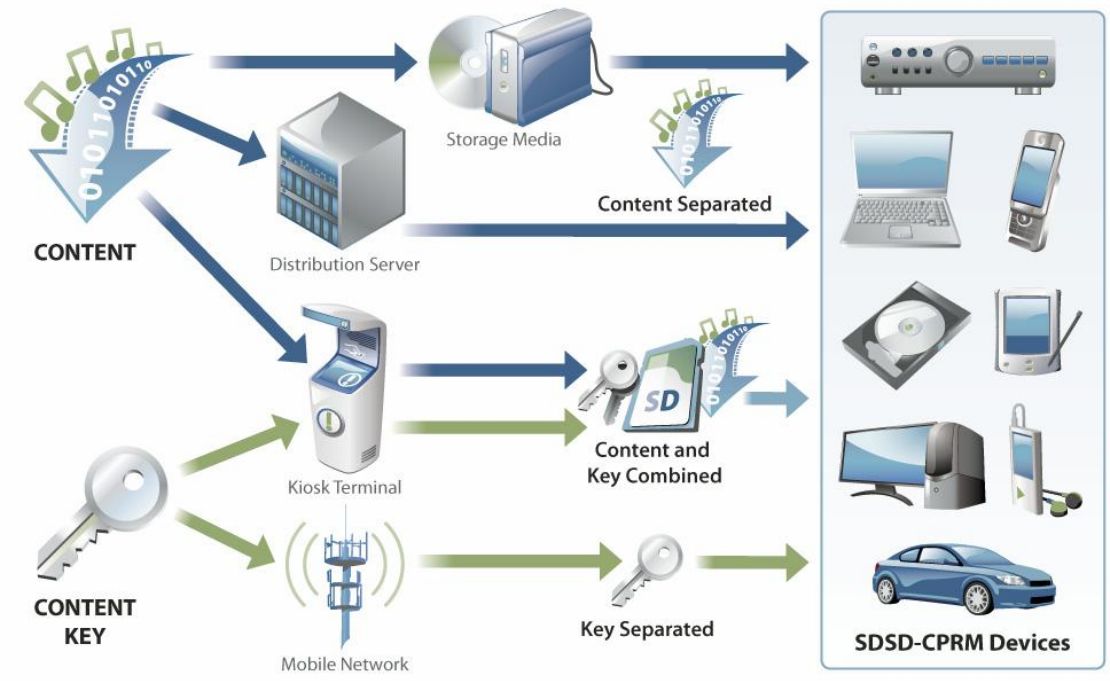


図 5-5：SDSD-CPRM 全体図（SDSD-CPRM White Paper より引用）

SDSD-CPRM においてはコンテンツ鍵保護のために、SD カードの CPRM に二重鍵構造を

採用し、コンテンツとコンテンツ鍵を分離して扱うことにより、コンテンツ鍵とコンテンツを別々に SDSD-CPRM Device に配送することを可能としている。また SD カードにコンテンツとコンテンツ鍵をバインドするメディアバインドもサポートしている。コンテンツとコンテンツ鍵を分離して扱うために、二重鍵構造を採用している。

SDSD-CPRM はビデオコンテンツを店頭型 KIOSK 端末で SD カードにダウンロードするサービスとして、米国で採用された例がある。http://www.modsystems.com/

SD-CPRM および SDSD-CPRM 規格はオープンかつ、国際的に認知度の高い規格であるため、今後の普及を考慮すればこれらの規格を利用することが戦略的に重要である。

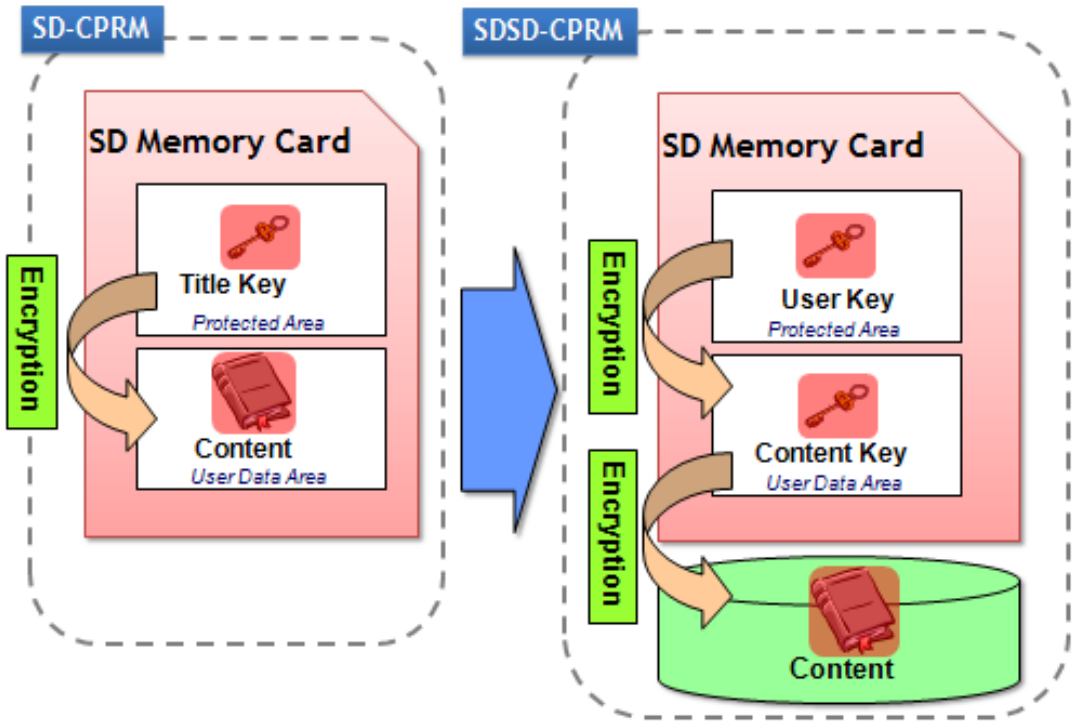


図 5-6：SD カードにおける一重鍵と二重鍵方式

図 5-6 において、SD-CPRM においてはデジタルコンテンツの暗号鍵（タイトル鍵：コンテンツ鍵と同義）は SD カードの保護領域に格納され保護されている。保護対象はコンテンツデータである。SD-CPRM においてはタイトル鍵とコンテンツデータは同一 SD カードに格納されていなければならない。これを狭義のメディアバインドと呼ぶ。

なお、詳細に言えば、保護領域に格納されたデータは SD カードの Media 固有鍵で更に暗号化されて保護されているが、これは前述の一重鍵方式に分類される。

一方、SDSD-CPRM においてはユーザ鍵が SD カードの保護領域で保護され、デジタルコンテンツの暗号化に用いた暗号鍵（タイトル鍵とコンテンツ鍵は同じ意味）は当該ユーザ鍵によって暗号化され、SD カードの通常領域に格納される。更に、デジタルコンテンツデータは当該コンテンツ鍵によって暗号化される。これは前述の二重鍵方式に分類される。

SDSD-CPRM において、保護対象はコンテンツ鍵であり、本質的にデジタルコンテンツの種別に影響を受けない構成となっている。SDSD-CPRM の場合、コンテンツデータは同一の SD カードに格納しても、別の記憶媒体にあっても良い。SD カードにコンテンツ鍵とコンテンツデータを格納した状態を広義のメディアバインドと呼ぶ。

オフライン販売に用いる物理メディアに SD カードを利用する場合には二重鍵による広義のメディアバインド機能を使用する。

5.2.2. ユースケース

SDSD-CPRM を利用することで実現できる様々なユースケースについて説明する。
SD カードには複数のコンテンツ鍵を収容し、コンテンツの暗号化を解くための鍵束として用いている。

5.2.2.1. ユースケース1

図 5-7：ユースケース 1

ユースケース1 は SD カードを鍵束として、様々な機器でコンテンツの閲覧ができる場合を想定している。コンテンツ自体は暗号化されているため、事前に様々な機器に格納しておいても著作権管理上安全である。暗号化されたコンテンツを閲覧するためのコンテンツ鍵は SD カードに安全に格納されている。

こうした状況で、鍵束である SD カードをいずれかの機器に装着すれば、該当機器でコンテンツの閲覧ができる。

5.2.2.2.ユースケース２

図 5-8：ユースケース 2

このユースケースは SD カードにコンテンツも格納して、ブリッジメディアとして使用することを想定している。これは SD カードの最も基本的な使い方で、メディアバインド型と呼ばれる。

この例では暗号化されたコンテンツのアーカイブとしてパソコンのハードディスクを利用している。SD カードにアーカイブされた暗号化コンテンツを全てコピーする必要はない。再生に必要なものだけを選択して、SD カードにコピーすれば良い。SD カードにある暗号化コンテンツは必要に応じて削除できる。SD カードの使い回しが可能である。

プリレコードされた SD カードもこのユースケースに分類される。

5.2.2.3.ユースケース３

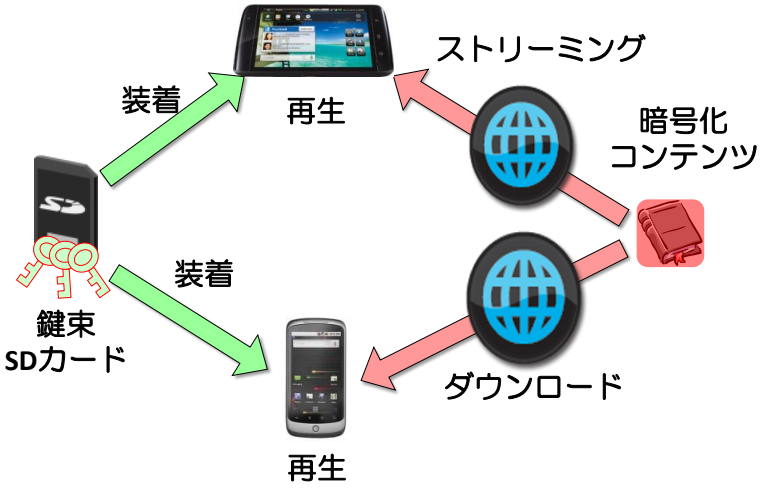


図 5-9：ユースケース 3

このユースケースは定期購読など予めコンテンツを閲覧する権利が先に取得されていて、

対応するコンテンツが無い場合や SD カードをコンテンツ鍵だけ格納する、いわゆる鍵束として使用する場合を想定している。コンテンツ鍵に対応する暗号化コンテンツをインターネット経由でダウンロード或いはストリーミングで取得することで、コンテンツの閲覧が可能となる。

5.2.2.4. ユースケース４

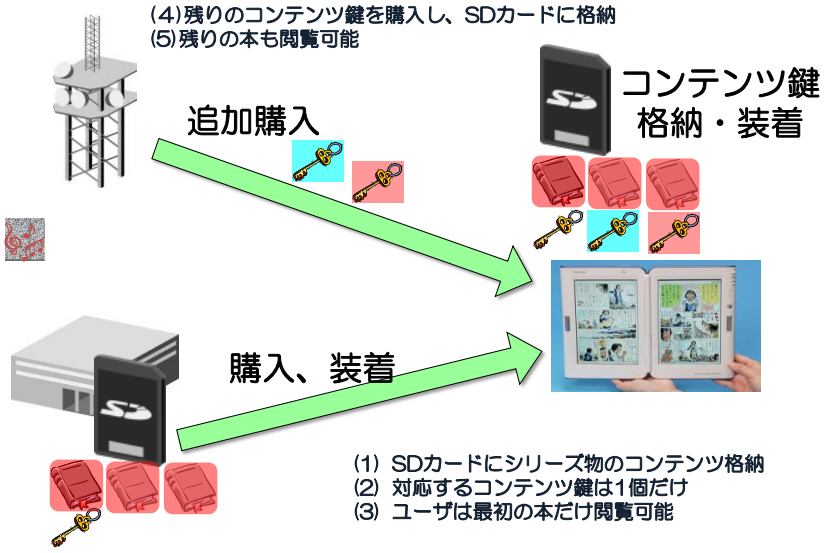


図 5-10：ユースケース４

このユースケースはパッケージ販売とネット販売の連携例である。ハイブリッド電子出版流通ならではのユースケースと言える。

プリレコードされた SD カードにはシリーズ物の暗号化されたコンテンツが複数格納されているとする。例えば、電子出版物で、コミックの場合、1 冊のデータ容量は 50MB 前後であるのに対し、SD カードの容量がそれを遙かに上回るため、複数のコミックを収容することが可能である。

一方、販売価格を考えると複数冊のコミックが閲覧できる状態とすれば、販売価格を上げざるを得ない。このユースケースにおいては、販売価格は 1 冊分としながら、複数の暗号化コンテンツを SD カードに同時に収容することで、利用者への暗号化コンテンツの配送の手間を省きつつ、アフターマーケットでの販売をも可能としている。利用者は対応するコンテンツ鍵のみを取得することで、SD カードに収容された続きのコンテンツを閲覧することができる。コンテンツ鍵のデータ量は高々1kB 程度なので、暗号化コンテンツデータのダウンロードに比べ、通信網のトラフィックの負担も極端に軽く、携帯電話などでの利用に好適である。

5.2.2.5. 貸与の例

プリレコードされた SD カードには所有者に関する情報はない。このため、その SD カードを貸与することができる。当該 SD カードを貸与することは、紙の出版物と同等の形態

であり、貸与する側はコンテンツの閲覧ができなくなる。物理メディアに格納された状態であれば、貸与は簡単に実現できる。

5.2.2.6.図書館貸し出し

図書館での貸し出しの基本は閲覧期限を設けることである。閲覧期限は使用許諾条件で設定可能である。閲覧期限の過ぎたコンテンツは紙の本のように、返却する必要がなく、利用者への利便性が向上する。

貸し出しの形態は図書館窓口、インターネットを通じたオンラインの２つが考えられる。コンテンツ格納の観点からは、SD カードを利用する場合や PC 等へのダウンロードが考えられる。貸し出しの形態とコンテンツ格納を組み合わせることで、様々な貸し出し形態に対応できる。すなわち、図書館窓口での貸し出しは SD カードを利用する方法が適しており、オンラインでは SD カードの利用や PC 利用など、利用者の持つ端末機器の特性に合わせれば良い。

5.2.3. SD カードの著作権保護機能を使うための留意点

ここでは SD カードの著作権保護機能を利用するための留意点について述べる。

5.2.3.1. SDA 規格と 4C 規格について

SD カードの著作権保護機能（SD カードの保護領域の利用）を利用するためには、SDA と 4C という２つの団体の規格に準拠しなければならない。（単に SD カードの通常領域だけを利用する場合、SD カードをアクセスするためには SDA の物理規格、ファイルシステム規格に準拠しなければならない。）

SDA アプリケーション規格は SD カードの通常領域の利用に関わる規格であり、これに準拠することでホストのアプリケーション間のインターオペラビリティが担保できる。つまり、SDA アプリケーション規格に準拠して SD カードに書き込まれたデータを SDA アプリケーション規格に準拠したホスト機器であれば組み合わせに関係なく、SD カードのコンテンツを再生することができる。なお、SDA アプリケーション規格は SD カードの通常領域における管理ファイルや SD カードにおけるコンテンツフォーマットおよび格納フォーマットや管理ファイルを用いたホスト機器の動作などを規定する。

一方、4C 規格は SDA で規格されたアプリケーション規格で規定されたコンテンツデータの保護方法、保護領域の使用方法、アプリケーション特有の使用許諾条件などを規定する。

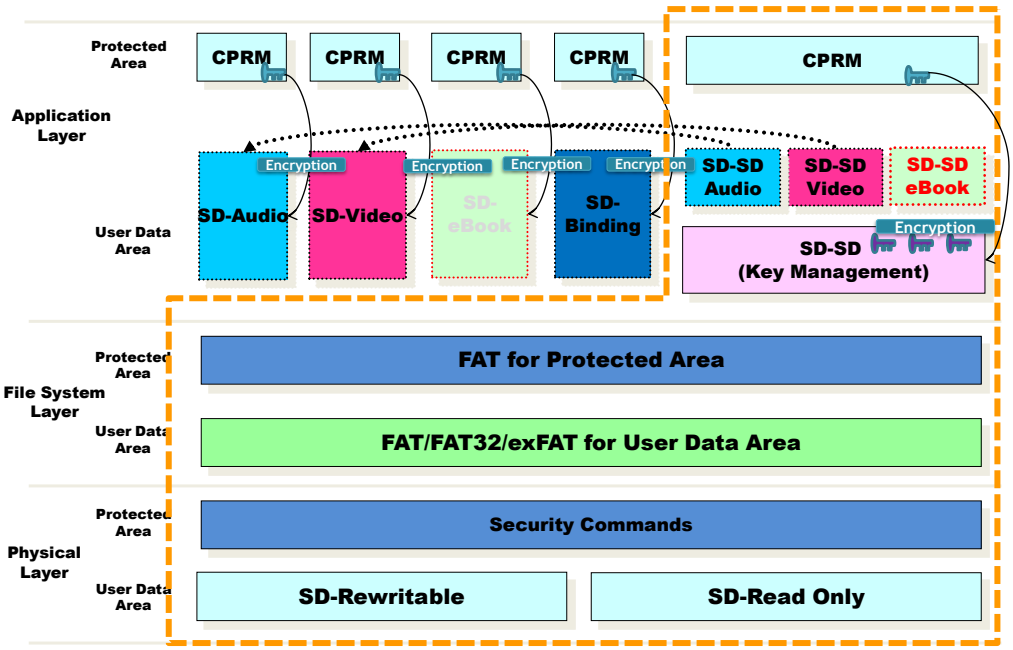


図 5-11：SDA 規格と 4C 規格の関係

しかしながら、現状では二重鍵を扱う SDA の規格、4C 規格は既に策定されているものの、SDA における電子出版に対応するアプリケーション規格（SD-SD eBook）が策定されていないため、4C 規格も電子出版に対応する保護規格が策定されていない。このため、SD カードを用いての電子出版流通は行うことができない状況にある。

こうした背景から、電子出版に対応する SDA 規格、4C 規格を策定する必要性がある。このため、SDA においては SD-SD eBook Profile 策定、4C においては対応する保護規格の策定を行った。（詳細は「SD カードに特定の電子出版コンテンツフォーマットを収容する方法の規格化（SD-SD eBook 規格の改訂版案）」参照のこと）

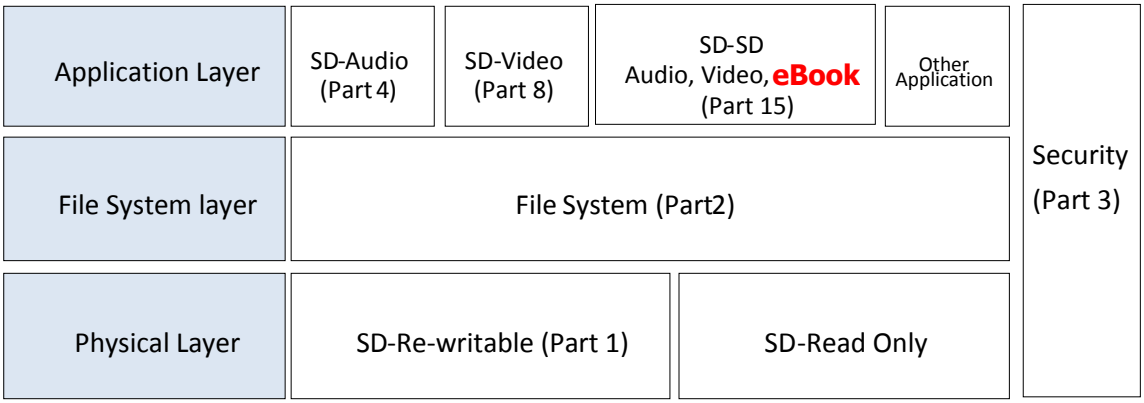


図 5-12：SDA 規格の構成

図 5-12 に SDA 規格の構成を示した。以下、それぞれについて説明する。

- Application Layer

SD カードを利用する用途ごとに、データの様式、および、SD カード上でのデータ保存様式に関する規定である。オーディオデータを扱う場合は”Part 4.SD-Audio”、映像データを扱う場合には”Part.8 SD-Video”が，二重鍵方式を扱う場合は SD-SD (Part 15)が利用される。Part 15 では Audio Profile、Video Profile は策定されているが、電子出版を扱う eBook Profile は平成 21 年度時点では未策定である。

- File Sysytem Layer

SDA の定める SD カード上でのファイルシステムに関する規定である。
SD カードによって、FAT16、FAT32、EX-FAT が採用されている。SD カードの格納容量によってファイルシステムが異なるため、SD カードを扱うホスト機器（SDA ではこう呼ぶ）によっては扱うことができない SD カードがある。（詳細は付録参照）

- Phisycal Layer

SDA の定める SD カードに関する物理的、電気的な規定である。SD カードの入出力インタフェイスの高速化により、何度も改訂がなされているがバックワードコンパチビリティは確保されている。

- Security System

SDA の定めるコンテンツ保護方式のためのコマンドインタフェイスに関する規定である。SD カード内部の処理は 4C の定める CPRM 規格を参照している。4C の規格では、メディアごと、用途ごとに、規格が細分化されており、SDA のそれぞれのアプリケーション規格に対応する規格が決められている。

SD-SD の規格は、既に Application Layer の規格として”Part.15 SD Separate Delivery”として、基本的な事項が定められており、さらに、利用する用途ごとに追加規定が設けられている。現時点では、”Audio Profile Addendum”と、”Video Profile Addendum”が定められている。これに”eBook Profile Addendum”を追加策定する必要がある。

5.2.4. SDA 規格と 4C 規格の概要説明

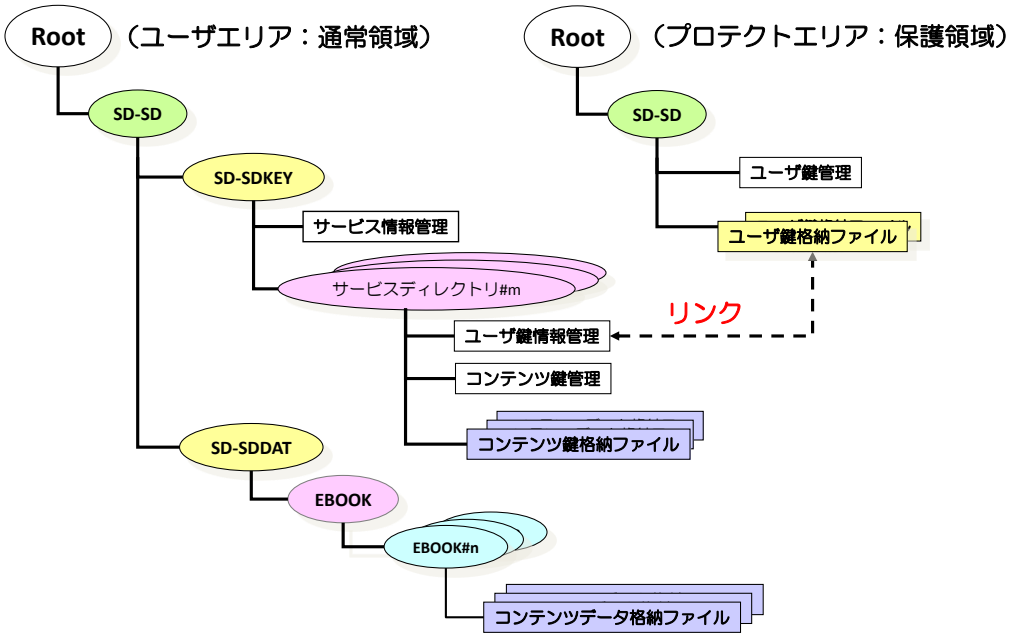


図 5-13：SD-SD (Part 15)における SD カード内の概略構造

図 5-13 に、SD-SD 規格で扱う SD カード内の概略構造を示す。

SDA の SD-SD 規格では SD カードの Root ディレクトリの下に SD-SD という名の専用ディレクトリが作られる。更に、SD-SD ディレクトリの下に鍵管理用のディレクトリ SD-SDKEY とコンテンツデータ管理用のディレクトリ SD-SDDAT が作られる。鍵管理はサービス情報管理とサービス毎に作られるサービスディレクトリから構成される。各サービスディレクトリの下に、ユーザ鍵情報管理とユーザ鍵毎にコンテンツ鍵管理が行われる。

一方、SD-SDDAT の下にはコンテンツが電子出版であれば、EBOOK ディレクトリが形成され、その下で、電子出版管理とコンテンツデータ格納管理が行われる。

SD カードのプロテクトエリアには、4C 規格に基づき、Root ディレクトリの下に SD-SD

ディレクトリが形成され、その下でユーザ鍵管理が行われる。ユーザエリアのユーザ鍵情報はプロテクトエリアにあるユーザ鍵のポインタ情報として使用され、プロテクトエリアとユーザエリアのリンクとして働く。

5.2.4.1. サービス

ユーザ鍵は原理的には SD カードに１つあれば事足りるが、コンテンツ配信では複数の配信元が想定されるため、配信元の区別が必要となる。また一つのユーザ鍵で全てのコンテンツ鍵を管理することは万一のユーザ鍵の破損などで全てのコンテンツ鍵が使用不可能となる問題があるため、SD-SD 規格では SDSD-ID（サービス ID）によるサービスという概念を導入し、配信元の区別ができるようになっている。また、ユーザ鍵は最大 100 個のコンテンツ鍵を管理するという制限を加えている。

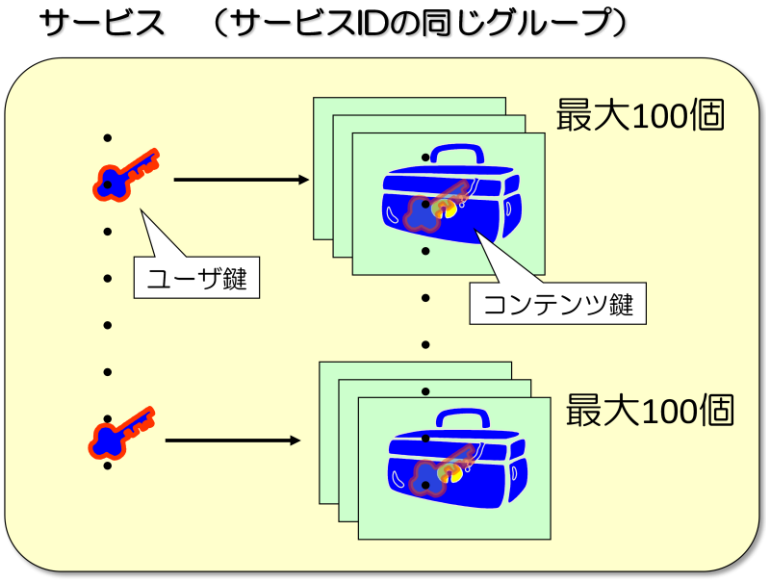


図 5-14：SD-SD 規格におけるサービス

5.2.4.2. コンテンツ ID とユーザ鍵 ID

1 つのユーザ鍵が管理できるコンテンツ鍵の個数に制限があるため、１つのサービスに複数個のユーザ鍵が存在することが想定される。鍵サーバにコンテンツ鍵の発行依頼をするとき、どのユーザ鍵を用いて暗号化すれば良いか、ユーザ鍵を特定する必要が生ずる。ユーザ鍵は秘密鍵であるため、これをそのまま使うのはセキュリティ上問題が生ずる可能性があり、ユーザ鍵を特定するためユーザ鍵 ID を用いる。ユーザ鍵とユーザ鍵 ID は鍵サーバが SD カード毎に対応づけて発行管理する。

注：コンテンツ ID は、SD カードにコンテンツを収容する際に用いる ID を指し、SDA 規格で定義された用語である。

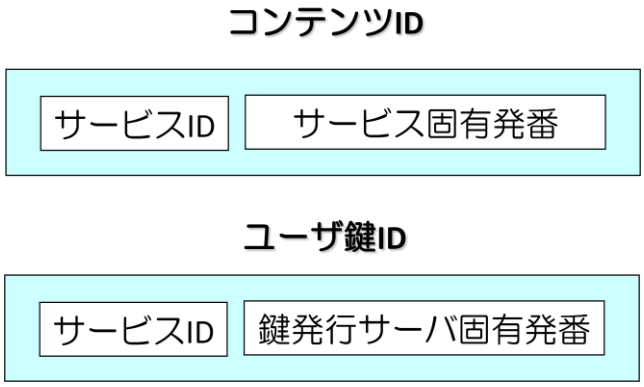


図 5-15：コンテンツ ID とユーザ鍵 ID

コンテンツ ID とユーザ鍵 ID は同一サービス内では同じサービス ID が付与される。これにより、ユーザ鍵、コンテンツ鍵、暗号化されたコンテンツデータのどれからも、サービスを特定できる仕組みになっている。

5.2.4.3. コンテンツ鍵の構造

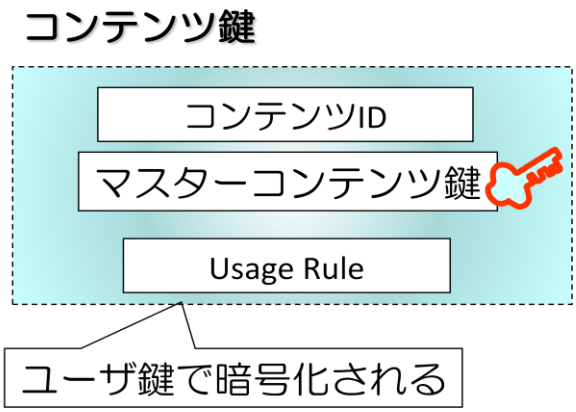


図 5-16：コンテンツ鍵と Usage Rule

コンテンツ鍵はコンテンツ ID、マスターコンテンツ鍵、Usage Rule で構成され、ユーザ鍵で暗号化され、SD カードのユーザエリアに格納される。SD カードのユーザデータエリアはユーザから自由にアクセスができるので、Usage Rule が改竄されていないかの正当性を調べるため、Hash 値によるチェックが行われる。Hash 値はある 1 つのユーザ鍵が管理しているコンテンツ鍵の全ての Usage Rule データをもとに計算が行われ、SD カードのプロテクトエリアに格納される。Hash 計算はコンテンツ鍵を新たに取得して登録する際やコンテンツ鍵を用いてコンテンツの再生を行うときに必要となる。

5.2.4.4. 暗号化されたコンテンツの閲覧

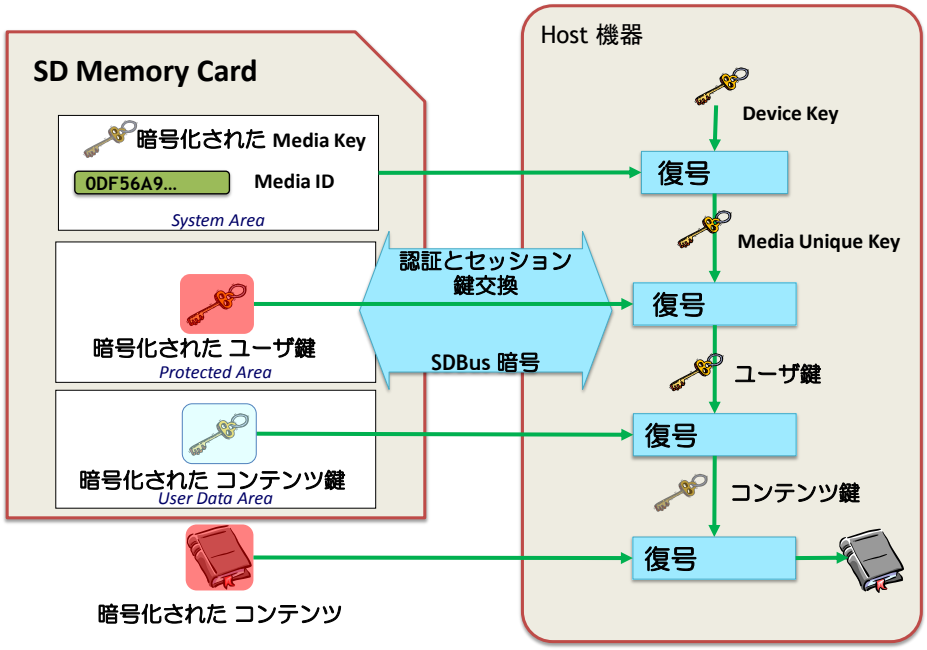


図 5-17：SDSD-CPRM におけるコンテンツの復号

コンテンツを再生するためには同じコンテンツ ID を持つコンテンツ鍵と暗号化されたコンテンツデータが必要である。更に、コンテンツ鍵に Usage Rule が付加されている場合は Hash 値の正当性をチェックした後、再生が行われる。再生は、コンテンツ鍵の暗号化に用いたユーザ鍵を用いて、コンテンツ鍵を復号してマスターコンテンツ鍵を取り出し、これを用いて暗号化されたコンテンツデータを復号する。これらの処理はセキュアに行われる必要があり、SDSD-CPRM でホスト機器の動作の規定がなされている。

6. ハイブリッド型電子出版流通における DRM システム

6.1. SDSD-CPRM をベースとした配信 DRM システム

SDSD-CPRM をベースとした基本的な配信 DRM システムについて説明する。
ユーザ鍵の発行管理、コンテンツ鍵の発行管理、コンテンツデータの暗号化・管理などを行う鍵サーバ、コンテンツ鍵や暗号化されたコンテンツなどを送付する通信路と SDSD-CPRM 準拠クライアントから構成される。

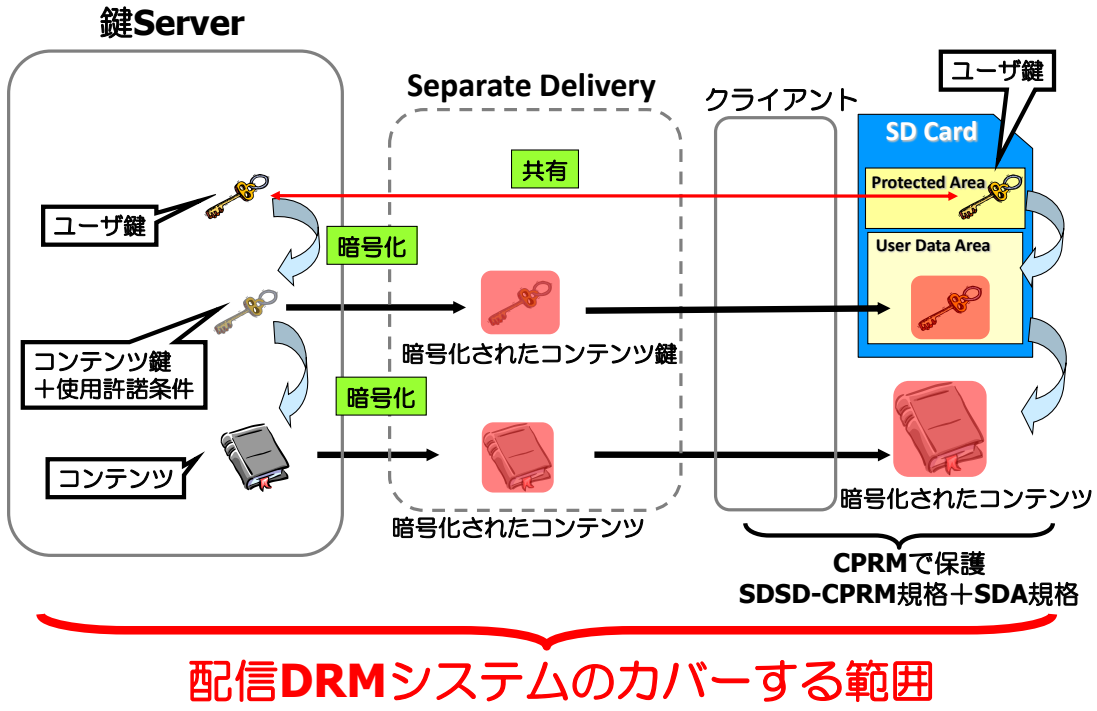


図 6-1：SDSD-CPRM をベースとした配信 DRM システム

SDSD-CPRM においては、既に、クライアントにユーザ鍵が安全に届けられた状態を前提として、SD カードの保護領域にユーザ鍵をどの様に格納し、どの様に利用するかについてやコンテンツ鍵に付随した使用許諾条件に従って動作するクライアントの振る舞いなどを規定している。

すなわち、SDSD-CPRM はクライアントおよび SD カードに関する規定であるため、配信 DRM はこれをベースにユーザ鍵をクライアントに向けて発行する手順やコンテンツ鍵をクライアントに発行する手順などを追加規定する。

SDSD-CPRM ではこうした配信を考慮した上で策定されているので、SDSD-CPRM で定義された要素を組み合わせることで実現できる範囲にある。

注：クライアントとホスト機器の関係

ホスト機器は SD カードを扱える機器を指し、SDA 規格で定義された用語である。一方、クライアントはホスト機器を包含し、より一般的に機器或いはソフトウェアなどを指す用語として用いている。

6.2. SDSD-CPRM への追加手順の概要

6.2.1. ユーザ鍵の共有

コンテンツ鍵は SD カード固有のメディア ID に関連づけられたユーザ鍵によって更に暗号化され、SD カードのプロテクトエリア（保護領域）に格納されている。

ユーザ鍵を外部に設けられた鍵サーバと SD カードで共有する秘密鍵とすることで、SD カードへのコンテンツ配信が可能となる。鍵サーバは SD カードのメディア ID と発行したユーザ鍵とを関連づけるデータベースを持つ。

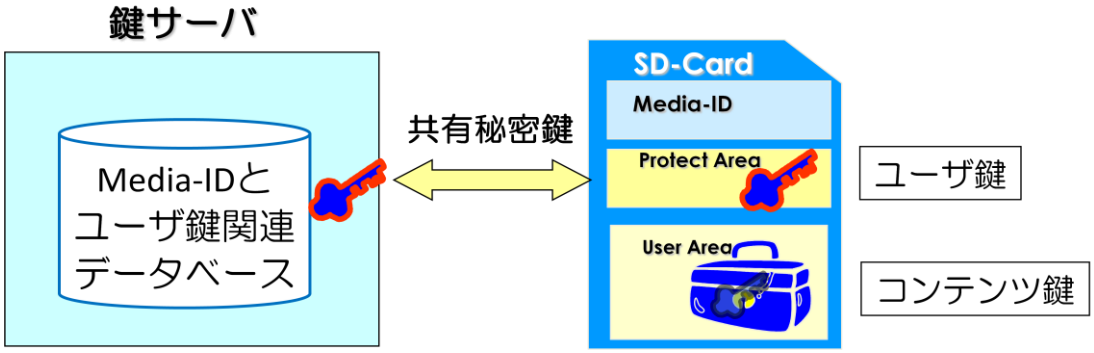


図 6-2：ユーザ鍵共有

6.2.2. コンテンツ鍵の発行

既に、SD カードの保護領域にユーザ鍵が格納されている場合、クライアントは鍵サーバに該当サービスのユーザ鍵 ID と対象となるコンテンツ鍵を特定する識別コード（コンテンツ ID）を通知する。鍵サーバは通知されたユーザ鍵 ID に対応したユーザ鍵とコンテンツ ID からマスターコンテンツ鍵をそれぞれ割り出し、マスターコンテンツ鍵をユーザ鍵で暗号化し、クライアントに送付する。マスターコンテンツ鍵は１つのコンテンツにつき１つだが、ユーザ鍵を用いて暗号化することにより、SD カード毎に固有のコンテンツ鍵が生成される。コンテンツを特定するために、コンテンツ ID をコンテンツ鍵、暗号化されたコンテンツデータにそれぞれ付与する。

コンテンツ鍵を発行する時点で、使用許諾条件である Usage Rule を合わせて付与することができる。

ユーザ鍵で暗号化されたコンテンツ鍵は途中で盗み取られても他のクライアントではユーザ鍵が異なることから、利用できないため、本質的に安全である。従って、ユーザ鍵で暗号化されたコンテンツ鍵を配送する通信路にはセキュリティを要求しない。また、クライアントは自身の SD カードの通常領域に暗号化されたコンテンツ鍵を SDA 規格の定める所定の形式で格納するだけで良い。暗号化されたコンテンツはコンテンツ鍵の取得時点と同時の場合も勿論あるが、先でも後でも良く、コンテンツ閲覧時点で、クライアントが取得していれば良い。

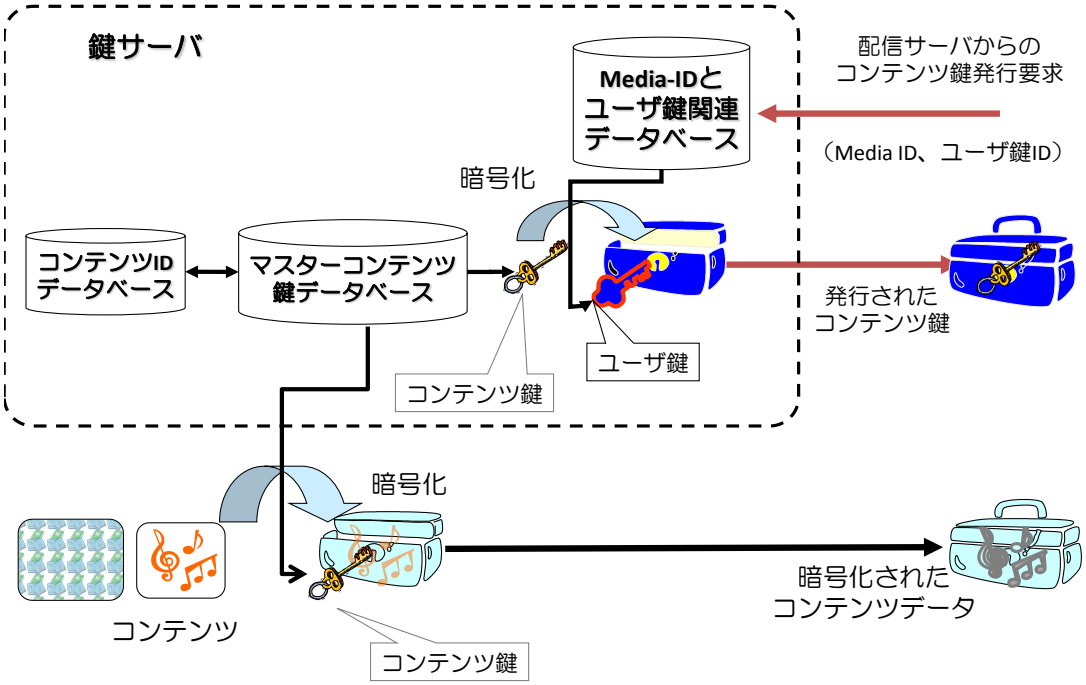


図 6-3：鍵発行管理サーバ

6.2.3. サービスへの新規加入

配信元からコンテンツを購入するには、サービスに加入する必要がある。サービスに加入するためには SD カードのプロテクトエリアにその配信サービスで使用するユーザ鍵を書き込む必要がある。

「サービスへの新規加入」とは、一度も SD-SD サービスで使用されていない SD カードを使用して、コンテンツの購入が行えるようにユーザ鍵などの情報を登録することを言う。

こうした SD カードにはプロテクトエリア、ユーザエリアともに、SD-SD 規格で定められたディレクトリ、ファイルが全く存在しない。このため、必要なディレクトリやファイルを生成し、ファイル内に SD-SD 規格で定められたデータを格納する必要がある。サービス加入完了とは、SD カードの所定の場所にサービス情報、ユーザ鍵、ユーザ鍵情報などが格納され、管理可能な状態となることである。これらの必要情報はサービスアプリが配信サイトと通信して取得する。

SD カードをプリレコードする際も同じプロセスを必要とする。

6.2.3.1.1. SD カードの保護領域にユーザ鍵が格納されていない場合（初期登録）

クライアントは SD カードの Media ID を鍵サーバに通知する。鍵サーバはユーザ鍵とユーザかご ID を生成し、Media ID と関連付けして、内部のデータベースに保持するとともに、これをクライアントに送付する。送付されたユーザ鍵は Media ID の異なる他の SD カードでは使用できないので、通信路の安全性は本質的には必要はない。クライアントは送

付されたユーザ鍵を保護領域に格納する。クライアントが SD カードの保護領域をアクセスするため、クライアントは SDSD-CPRM に準拠していなければならない。

注 1：鍵サーバの Media ID とユーザ鍵の関連づけデータベースと不一致なユーザ鍵が SD カードに格納された場合、当該 SD カードを扱うクライアントがコンテンツ鍵を要求しても Media ID が異なるため、鍵サーバは別のユーザ鍵を用いてコンテンツ鍵を暗号化して送付するか、未登録 Media ID としてコンテンツ鍵の送付を拒否するか、新たなユーザ鍵を発行するかのいずれかの動作をする。仮にコンテンツ鍵が送付されても、当該 SD カードの保護領域に格納されたユーザ鍵では送付されたコンテンツ鍵の復号はできないことから安全性は高い。

注 2：SDSD-CPRM ではユーザ鍵は複数個の設定が可能で、一旦登録されたユーザ鍵は対で発行されたユーザ鍵 ID で識別する。

6.3. 本ガイドラインにおける DRM

前述の SDSD-CPRM をベースとした基本的な配信 DRM では、SD カードの著作権保護に対応できない端末機器に適用できない。4.3.1 で述べたように、現在流通している端末機器の中にはそもそも SD カード自体を扱えない機器や SD カードの著作権保護機能に対応できない端末機器も存在する。こうした端末機器でもハイブリッド電子出版流通の恩恵が得られるようにするため、SDSD-CPRM のコンセプトを継承した拡張 SDSD-CPRM をベースとした配信 DRM に加え、更にドメイン機能を付加したものを本ガイドラインにおける DRM としてとする。本ガイドラインにおける DRM では、プリレコードされた SD カードのコンテンツも利用できる。

拡張 SDSD-CPRM とは仮想 SD カードという概念を導入し、SD カードの扱えない端末機器に独自に保護領域を確保し、SDSD-CPRM のコンセプトである保護領域でユーザ鍵を保護することで SD カードの扱えない端末機器も SDSD-CPRM に対応した端末機器として扱うものである。

6.3.1. 仮想 SD カードの導入

端末機器内部に SD カードの様な保護領域を形成することで、端末機器が SD カードと同様に利用できる仕組みを仮想 SD カードと称する。SD カードの Media ID に相当する拡張 Media ID は鍵サーバが付与し、鍵サーバでは SD カードと同等に扱う。

仮想 SD カードを形成するためには、端末機器が鍵サーバと通信できなくてはならない。従って、端末機器は少なくともネット接続機能をサポートしていなければならない。また、拡張 Media ID は改ざんを受けぬようにしなければならない。端末機器自体を仮想 SD カード化することで、端末機器の保護領域でユーザ鍵を保護すれば、SD カードと同様に利用する事ができる。端末機器を仮想 SD カード化するためには専用のアプリケーションを端末機器にインストールする必要がある。図 6-4 における Secure Module がその役割を果たしている。

こうした仮想 SD カード化された端末機器はオンライン販売に対応することが可能となる。コンテンツを機器バインドで扱うが、通常の機器バインドと異なる点は機器固有情報として、鍵サーバが発行したユーザ鍵でコンテンツ鍵を保護していることである。

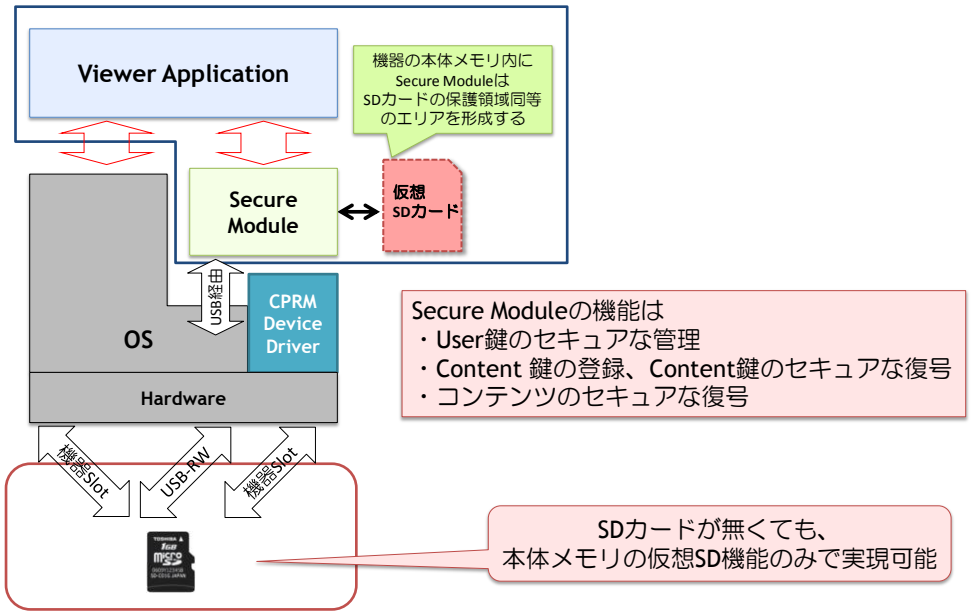


図 6-4：仮想 SD カードの説明図

図 6-4 について説明する。仮想 SD カードは SD カードの保護領域に相当するメモリ領域で、機器の本体メモリ内に Secure Module と呼ばれるソフトウェアが確保する領域である。Secure Module は自身が秘密に保持する暗号鍵によって、保護領域に格納されたユーザ鍵などの秘密情報を保護する。この領域は Secure Module を介してしか正当にアクセスできないように実装する。また、機器が SD カードをセキュアに扱える場合は、Secure Module は CPRM Device Driver を介してアクセスする機能があっても良い。鍵サーバからは SD カードとして扱われる。

6.3.2. ドメイン機能の追加

しかし、仮想 SD カード化された端末機器はオフライン販売向けにプリレコードされた SD カードを扱うことはできない。しかし、機器単独ではこの課題は対応できない。そもそも SD カードを扱える環境を端末機器が装備していないからである。このため、DRM システム全体で救済する仕組みとして、ドメイン機能を用いる。

ドメイン機能は複数機器とサーバ連携を基本とし、PC などネット接続と SD カードが扱える機器を用い、利用者が購入したコンテンツを配信側で権利登録できるライツロッカー（Rights Locker）システムを用いて、利用者の購入ライブラリに取り込んだ後、仮想 SD カードにあらためてダウンロードし、プリレコードされたコンテンツの閲覧を可能とする。（ライツロッカーについては 7 章で述べる。）

6.3.3. 本ガイドラインの推奨する DRM システム

図 6-5 に本ガイドラインの推奨する DRM システム概観を示した。本ガイドラインの推奨する DRM システム SDSD-CPRM をベース（図中の赤枠部分に相当）とし、これを仮想

SD カードまで拡張した拡張 SDSD-CPRM に、更にシステム側（ライツロッカー）でドメイン機能をサポートした DRM システムである。

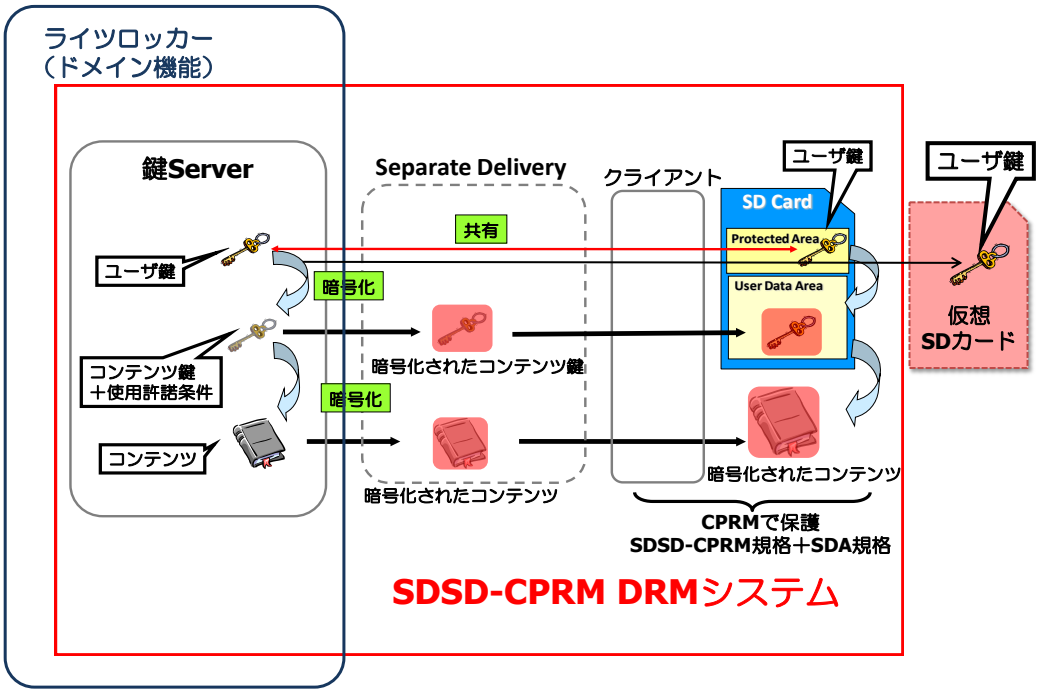


図 6-5：本ガイドラインの DRM システム概観図

6.4. 他の DRM との比較

表 6-1：各種 DRM 機能比較

	サーバ認証	ローカル機器バインド	メディアバインド	ドメインサポート
特徴	再生時にサーバでユーザ認証を行い、再生を許可する	再生端末／アプリに埋め込まれた秘密情報で再生処理を行う	メディアにコンテンツを保護記録する。特定メディア以外での再生は不可。	複数機器でのコンテンツの共有を可能とする。
ネットワーク処理	再生時必須	再生時不要	再生時不要	再生時不要
不正機器／不正ユーザの無効化	サーバでのユーザ認証時に不正機器／不正ユーザの無効化可能	サーバ認証との組み合わせにより、不正ローカル機器を無効化可能	不正機器の無効化可能	サーバ認証との組み合わせにより、不正ローカル機器を無効化可能
本ガイドライン	●	●	●	●
OMA	●	●	▲(1)	●
Adobe Content Server	●	●	×	●
PlayReady	●	●	×	●
FairPlay	●	●	×	●

(1) 仕様上は可能だがサポートできるメディアが存在しない。

各種 DRM と本ガイドラインの最大の違いはメディアバインド機能サポート必須としている点にある。ハイブリッド型電子出版流通では物理メディアのサポートができなければ成立しないからである。この要求条件に見合った他の DRM としては OMA があるが、これはあくまで仕様上であり、現状では OMA をサポートできるメディアは存在しない。

表 6-2：各種 DRM 比較

	ガイドライン	OMA2.0	Adobe Content Server	PlayReady	FairPlay
策定元	4C　Entity LLC CPRM規格＋拡張	Open Mobile Alliance	Adobe	Micro Soft	Apple
仕様のオープン性	○	○	○	○	なし
コンテンツ依存性	なし	なし	あり EPUB,PDFのみ	なし	あり EPUBのみ
OS依存性	なし	なし	なし	なし	あり
DRM分類	独立型	独立型	併用型	独立型	併用型
実績	映像・音楽など CPRMは広く利用	国内ではなし 国外不明	電子出版では最も多くの採用	映像・音楽向けサービス実施中	iPad, Iphone向け
事業継続性	代替ベンダによる開発や事業の継続可能	代替ベンダによる開発や事業の継続可能	一社単独での技術提供	一社単独での技術提供	一社単独での技術提供
既存のマーケットとの親和性	紙媒体と同一の配信経路を活用した記録済みメディアの販売が可能	ネットワーク配信仕様上はメディアの併用も可能	ネットワーク配信のみ	ネットワーク配信のみ	ネットワーク配信のみ

6.4.1. 本ガイドライン

本ガイドラインでは DRM の基本的機能は 4C の策定した SDSD-CPRM とし、これをもとに、配信に拡張した仕様となっている。従って、仕様のオープン性は高く、後述のガイドライン仕様をもとにすれば誰でも参画が可能である。このため、事業継続性に関しても、代替ベンダの参画が可能であるから、可能である。コンテンツ依存性は SDSD-CPRM 自体がコンテンツ鍵を保護することからも分かるように、コンテンツそのものに対する依存性は本質的にない。SDSD-CPRM は SD カードを扱えれば良く、OS 依存性はない。DRM としては任意のコンテンツとの組み合わせが可能であり、独立型に分類される。SDSD-CPRM のアプリケーションとして映像 KIOSK 販売(www.**modsystems**.com/)での実績があり、SD-CPRM は着うた、ワンセグ録画再生などで採用されている。

6.4.2. OMA2.0

OMA2.0 は Open Mobile Alliance (http://www.openmobilealliance.org/) が策定した汎用性の高い DRM である。DRM にフォーカスして仕様を策定しているところに大きな特徴がある。仕様のオープン性、コンテンツの依存性、OS 依存性はなく、DRM と しては独立型に分類される。OMA 仕様に基づき、参画各社が得意とするコンポーネントを開発提供するスキームのため、事業も代替ベンダを見つけることで継続可能である。OMA 仕様の最大の問題は実装規定がないため、コンポーネントの実装セキュリティが開発各社に委ねられている。このため、OMA に対応できる物理メディアが現在存在しない。仕様上からはハイブリッド型電子出版流通に適合する DRM である。

6.4.3. Adobe Content Server

Adobe Content Server は米国 Adobe 社が独自で開発した DRM である。http://www.adobe.com/jp/products/contentserver/）

Adobe 社は仕様概要を公開し、これを販売しているため、オープン性はある。（http://www.adobe.com/products/digitaleditions/pdfs/adobe_ebook_platform_whitepaper.pdf）

仕様上、コンテンツ依存性は無いもののと推察されるが、EPUB と pdf のみにコンテンツフォーマットを限定しており、DRM 分類では併用型として運用している。Adobe Content Server は現在の電子出版では最も多くの採用実績がある。事業継続性に関しては Adobe 社単独での技術提供のため、Adobe 社がサポートを中止すれば、Adobe Content Server をベースとして電子出版は立ち至らなくなる危険性がある。Adobe Content Server はネットワーク配信のみのサポートであるため、ハイブリッド型電子出版流通に適合できない DRM である。

6.4.4. PlayReady

PlayReady は米国 MicroSoft 社が独自開発した DRM である。従来同社が提供していた Windows Media DRM に比べ、高い柔軟性を提供できるとされている。この DRM は携帯電話業界に照準を定めたもので、ゲームなどの実行ファイルも含め、複数のファイルタイプをサポートする他、ドメインサポートにより、デバイス間のコンテンツの転送や他の DRM システムとの相互運用性もサポートする。

PlayReady にはコンテンツ依存性はない。従来の Windows Media DRM にあった OS 依存性もなく、DRM 分類からは独立型となる。映像・音楽向けにサービス提供されており実績もある。しかし、事業継続性に関しては MicroSoft 社単独での技術提供のため、MicroSoft 社がサポートを中止すれば、PlayReady をベースとして電子出版は立ち至らなくなる危険性がある。PlayReady 自体はデバイスの種類を問わないため物理メディアのサポートも可能かと推察されるが、現状ではネットワーク配信のみのサポートであるため、ハイブリッド型電子出版流通に適合できない DRM であると判断される。

6.4.5. FairPlay

FairPlay は米国 Apple 社が iTunes サービスのために開発した同社独自の DRM である。同社は垂直統合型のビジネスモデルで、コンテンツ配信から端末機器までをカバーしているため、FairPlay の仕様を公開していない。電子出版におけるサポートコンテンツは EPUB のみである。OS 依存性については、iPad、iPhone に関しては Apple 独自 OS、PC においては Windows もサポートする。Apple 社の事業戦略から、DRM の他社への提供は現状では考えられず、物理メディアサポートは現状ではなく、もっぱらネットワーク配信のみである。ハイブリッド型電子出版流通に適合できない DRM であると判断される。

7. 本ガイドラインにおけるシステムモデルおよび提供機能

7.1. ハイブリッド型電子出版流通のシステムモデルの導出

7.1.1. 一般的な Web ストアのシステムモデル

一般的な電子出版流通のシステムモデル

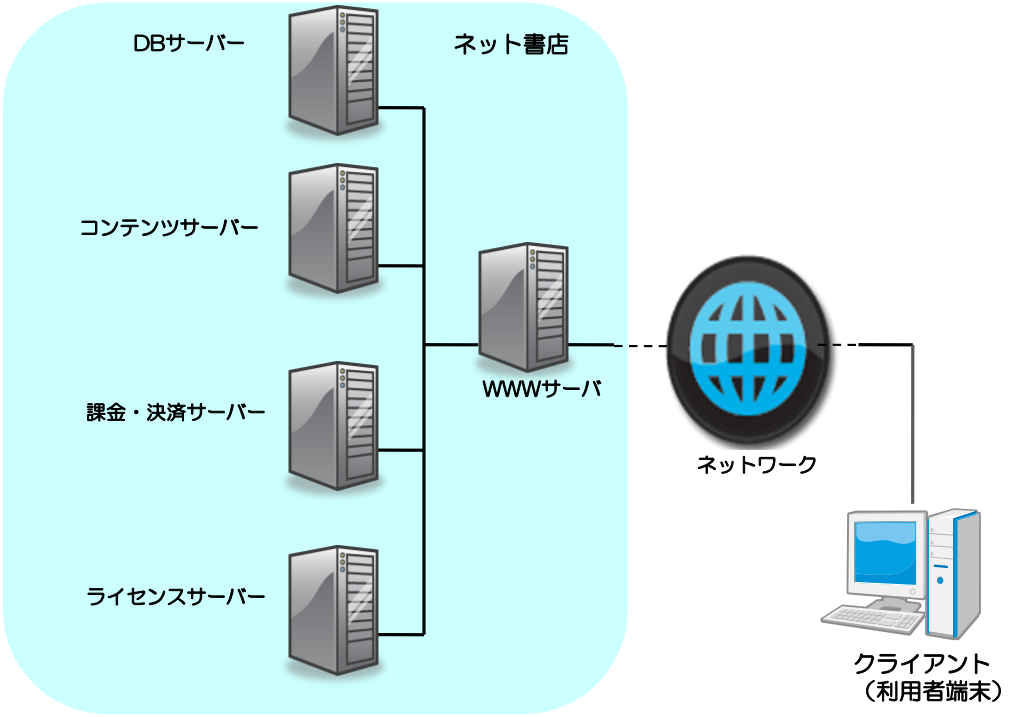


図 7-1：一般的な電子出版流通のシステムモデル

一般的なネット書店の構成は DB サーバ、コンテンツサーバ、課金・決済サーバ、ライセンスサーバと利用者端末(クライアント)との窓口の WWW サーバなどから構成される。図中の各サーバの役割は、次のとおりである。

- WWW サーバ

  HTML サーバであり、利用者が直接的に接続するサーバで、Web サーバーという呼び方をすることもある。WWW コンテンツを配信する役割を持つサーバである。利用者が画面で見る内容を構成して配信する。また、利用者が画面をクリックしたり、入力した文字を他のサーバに伝えて、検索や並べ替え、購入、ダウンロードなどの処理を実行させる。

- データベース（DB）サーバ

  取引データや商品情報など，EC(Electronic Commerce)で必要な様々なデータを管理するためのサーバである。基本的に WWW サーバと連携して機能する。例えば，取引情報などは WWW サーバ経由でデータベース・サーバに格納され、商品情報

などは，データベース・サーバ上に格納されている情報が、WWW サーバの要求に応じて取り出されるといった仕組みが一般的である。

- コンテンツサーバ

  ネット書店の場合は、商材である電子書籍のコンテンツを保存するサーバである。

- 課金・決済サーバ

  課金、および、決済を行うサーバである。課金とは、サービスの利用に対して料金をかけることである。課金の方式によって固定性、従量制、半従量制、従量課金上限制、定額従量制、キャップ制、ハドソン課金方式、カールソン課金方式などに分けられる。

  課金が、利用者との契約状況を管理するのに対して、金銭の授受に相当する処理が決済である。

  特に、ネット書店などで行われる電子決済では、ある商品またはサービスの代価としてお金を支払う場合、硬貨や紙幣などの現金で支払うのではなく、電子データをやり取りすることで支払いを行う。電子決済は、広義にはオンラインバンキングを利用した銀行振り込みやクレジットカード番号やそれに付随する各種情報をやりとりするカード決済が含まれるが、狭義には、インターネットなどでの商品・サービスの購入のために開発された仕組みのことを指す。決済方式としては、いろいろな分類方法があるが、サービスや商品購入と決済の時間的関係からの分類では、プリペイド方式、ジャストペイ方式、ポストペイ方式に分けられる。

- ライセンスサーバ（DRM：Digital Rights Management）

  コンテンツの不正利用、不正コピーを防ぐために、コンテンツデータに暗号を施して配信する。一般的には、利用者ごとに異なる暗号鍵を生成して、生成した暗号鍵を用いてコンテンツを暗号化する。

  ライセンスサーバでは、課金サーバなどと連携して、正規の利用者からのコンテンツの配信要求があると、暗号鍵の生成、コンテンツの暗号化処理をしたうえで配信する。また、暗号化したコンテンツを復号するための鍵を生成して、配信する。

この構成はネット書店のサーバで全て完結したモデルであるが、ハイブリッド型電子出版流通におけるコンテンツの権利保護の観点からは、プリレコードする SD カードに対するライセンスサーバの役割が欠落している。また、販売においては顧客情報として個人情報などプライバシー情報を扱わざるを得ない場合が生ずるが、ライセンスサーバにおいては必ずしも必要としない。

コンテンツの権利保護の観点から、ライセンスサーバを Web ストアから分離することで、Web ストアとマスタリングの両方に関われるようするとともに、プライバシー情報には一切タッチしないモデルを採用することにした。

7.1.2. 本ガイドラインでにおけるシステムモデル

本ガイドラインは前述の通り、ライセンスサーバを独立して配置し、Web ストアとマスタリングシステムとの両方から利用できるシステムモデルを採用した。

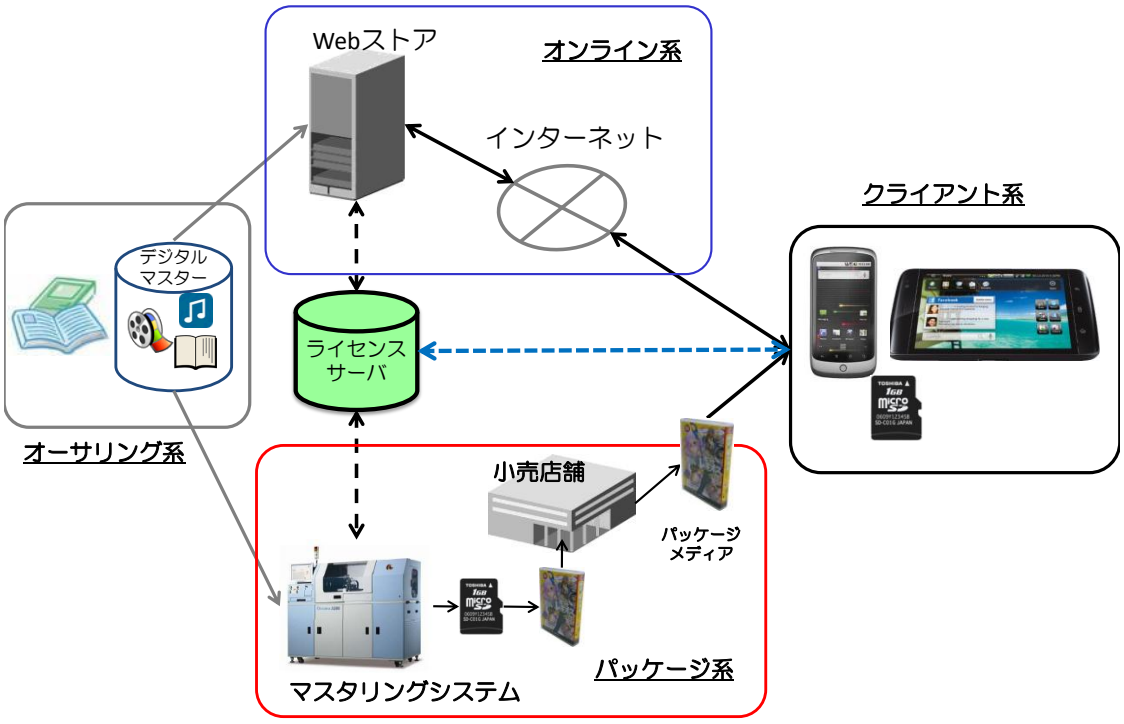


図 7-2：本ガイドラインにおけるシステムモデル

本ガイドラインのシステムモデルは大雑把に分類すると 5 つに分類される。オーサリング系、オンライン系、パッケージ系、クライアント系とライセンスサーバである。オーサリング系で電子化されたデジタルマスターは、Web ストアからインターネット経由でクライアントに配信されるオンライン系と電子化された電子出版物を SD カードに書き込み、パッケージ化され小売店舗で販売するパッケージ系を通じて、クライアントに届けられる。

Web ストアは WWW サーバ、DB サーバ、コンテンツサーバ、課金・決済サーバなどから構成される。デジタルコンテンツの権利保護はライセンスサーバとクライアント間で担保され、オンライン系で販売されたコンテンツとパッケージ化されて販売されたコンテンツも同等の扱いを受ける。

なお、デジタルコンテンツの権利保護の観点から、オーサリング系はコンテンツの権利保護の直接的な範囲に入れないこととした。

7.2. 本ガイドラインにおけるサービスモデル

本ガイドラインにおけるサービスモデルにおいて、実エンティティとステークホルダがどのように関わり、何を行うか、権利を扱うライセンスサーバが実エンティティとどの様

に連携すれば良いかを明らかにすることでライセンスサーバが提供する権利保護に関する機能を洗い出す。なお、付箋の「システム連携」とあるシーンはライセンスサーバが何らかの関わりあいを持つシーンを指す。

図 7-3 の説明を行う。本ガイドラインにおけるサービスモデルではステークホルダは、コンテンツ保有者（出版社）、コンテンツ配信サービス業者（書店）、パッケージ製造業者、利用者が登場する。

一方、実エンティティとして、実店舗、Web ストア、パッケージ製造システム、ライセンスサーバ、および利用者の PC ライブラリ、閲覧ビューワが登場する。

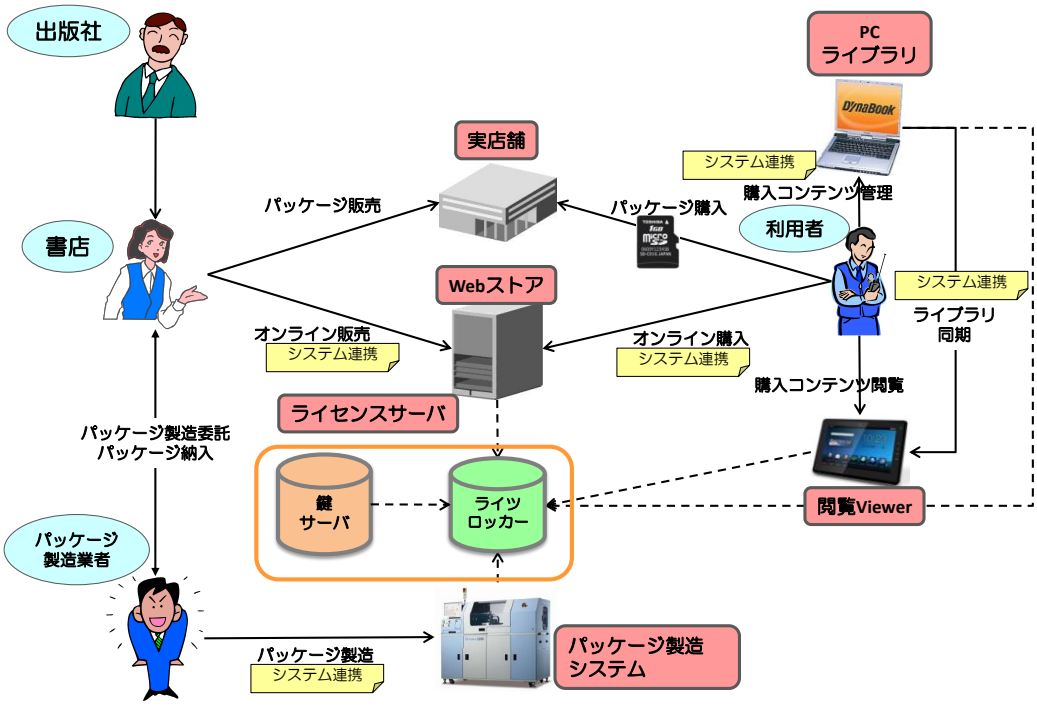


図 7-3：本ガイドラインの想定サービスモデル

まず、本ガイドラインの想定サービスモデルにおけるステークホルダの役割を説明する。

- コンテンツ保有者

コンテンツ保有者はコンテンツ配信サービス事業者へのコンテンツ提供する出版社などで、コンテンツ配信業者にコンテンツの利用許諾や紙出版物をコンテンツデータの提供などを行う。デジタル化されたコンテンツの利用許諾条件はコンテンツ保有者とコンテンツ配信業者間の契約で取り決められる。

- コンテンツ配信サービス業者

コンテンツ配信サービス業者は電子書籍のコンテンツをユーザに対して、物販・配信するサービスを提供する。コンテンツ配信サービス業者はコンテンツ保有者との契約によりコンテンツ配信の権利許諾やパッケージ販売権を受ける。

Web ストアを用い、コンテンツ販売機能（ユーザ認証・課金・決済・暗号化コンテンツ管理/配信・暗号化コンテンツ鍵配信等）を提供する。
また、オーサリングされたコンテンツの Web ストアへの登録も行う。

- パッケージ製造事業者

パッケージ製造業者はコンテンツ配信サービス事業者から委託を受け、SD カードにコンテンツをプリレコードしたパッケージを製造し、書店などに納入する。

- 利用者

端末を通じ、暗号化コンテンツ、および暗号化コンテンツ鍵を受信し、受信したコンテンツの復号・再生を行い、コンテンツ利用をする。端末は各種 ID・鍵をセキュアに管理しコンテンツのセキュリティを保証する。

次に実エンティティについて説明を加える。

- Web ストア

コンテンツ配信サービス業者がオンラインコンテンツ販売のために利用する Web サーバである。Web サーバはコンテンツ販売機能（ユーザ認証・課金・決済・暗号化コンテンツ管理/配信・暗号化コンテンツ鍵配信等）とオーサリングされたコンテンツの Web ストアへの登録機能などがある。ライセンスサーバと連携して、コンテンツの権利保護を実現する。

- ライセンスサーバ

ライツロッカー、鍵サーバから構成され、Web ストアに対して、関する各種 ID・鍵の発行サービスの提供を行う。また、サービス事業者のサービス ID、サービス名称の管理を行う。また、パッケージ製造システムとも連携し、製造した SD カードのプリレコードされたのユーザ鍵の登録を受ける。本ガイドラインにおけるコンテンツの権利保護中心的役割を担う。

- パッケージ製造システム

SD カードにコンテンツ復号に必要なコンテンツ、コンテンツ鍵、ユーザ鍵をプリレコードし、パッケージ販売用の商品を製造する。ライセンスサーバにユーザ鍵など SD カードにプリレコードした権利保護情報を登録する。本ガイドラインにおける権利保護の対象となる。

- PC ライブラリ、閲覧ビューワ（クライアント）

利用者が購入コンテンツの取得、管理、閲覧に利用する端末（クライアントとも呼ぶ）。
暗号化コンテンツおよびコンテンツ鍵を用い、コンテンツの権利保護上安全な管理、再生などを行う機能を持つ。ライセンスサーバとクライアント間でコンテンツのセキュリティを担保する。本ガイドラインにおける権利保護の対象となる。

7.2.1. ライセンスサーバの構成

ライセンスサーバは拡張SDSD-CPRMのDRMシステムにおける鍵サーバとドメイン機能をサポートするライツロッカーシステムから構成される。Web サーバとのインターラクションは鍵サーバとライツロッカーの両方があるが、上位レイヤに位置するライツロッカーシステムに窓口を一本化した方がインタフェイスの簡略化の観点から望ましい。

ライツロッカーは Web ストアやクライアントなどとの窓口としてサービスを提供する。また、鍵サーバはライツロッカーからのみ、リクエストを受け付け、Web サーバとのインタフェイスを一本化した。そのため、ライツロッカーシステムはコンテンツ配信サービス事業者の Web ストアと鍵サーバの間に設置され、鍵サーバと連携し、クライアントの権限情報を Web ストアに提供する。

利用者はクライアントを介して、Web ストアに SA-ID（Service_Account-ID）を用いて、Web ストアのドメインにログインする。Web ストアは自身が持つ認証システムで、SA-ID の正当性をチェックする。Web ストアとライセンスサーバはゲートウェイサーバを介して接続される。ライセンスサーバに既に利用者のドメインが形成されている場合（Domain-ID がライセンスサーバ内で発行され、登録がなされている状態）、Web ストアは SA-ID と利用者所有のコンテンツ ID を利用者のドメインに登録するようライセンスサーバに要求し、ライセンスサーバはデータベースに登録する。

複数の Web サーバから利用者がコンテンツを購入してもライツロッカーは利用者が購入したコンテンツを全て共有できるようにするため、ライツロッカー内では独自のアカウント ID（Domain_Account ID: DA-ID）を発行し、Web ストアで発行されたサービスアカウント ID（Service_Account ID: SA-ID）と対応付けを行う。

また、ドメインには利用者の持つクライアント機器も登録することができる。ライセンスサーバは利用者のクライアント機器に対して、仮想 SD カード ID（ExMID:Extended Media ID）を発行し、該当する利用者の Domain-ID と関連づけ、データベースに登録する。こうすることで、利用者は自身の所有するクライアント機器で購入したコンテンツの共有ができる。共有の方法は該当する ExMID を有する機器に対して、利用者が購入したコンテンツのコンテンツ鍵を発行し、これを Web サーバ経由で利用者のクライアント機器の配送することで実現する。

ライセンスサーバを構成するライツロッカーと鍵サーバはデータベースを共有する。

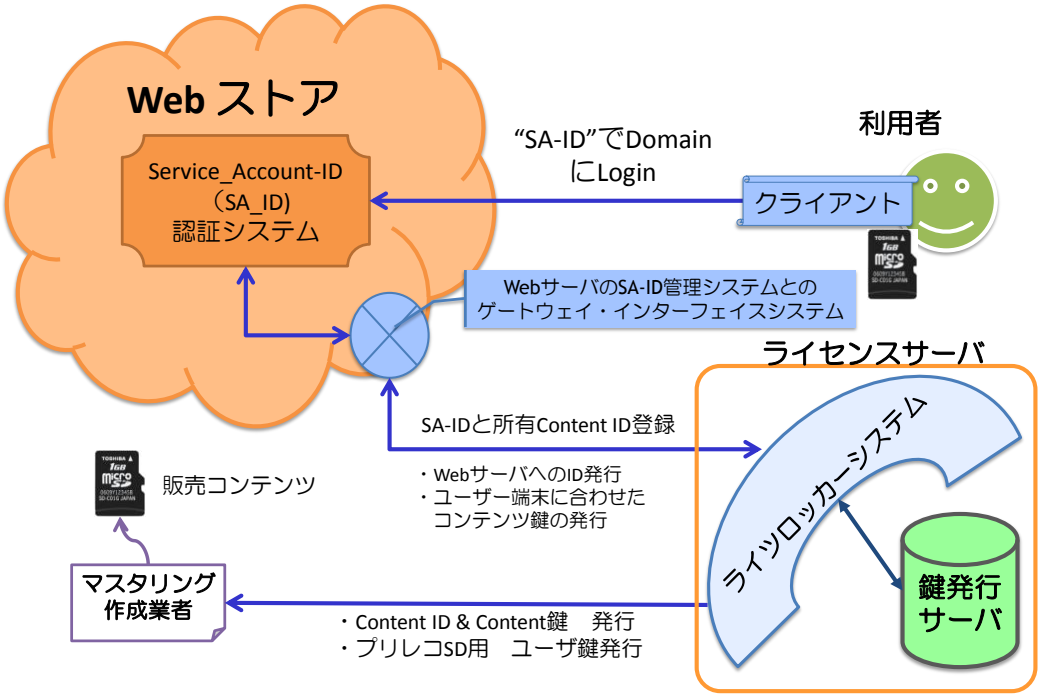


図 7-4：本ガイドラインにおける簡略化したシステムモデル

7.2.2. ライセンスサーバで扱う各種 ID 等

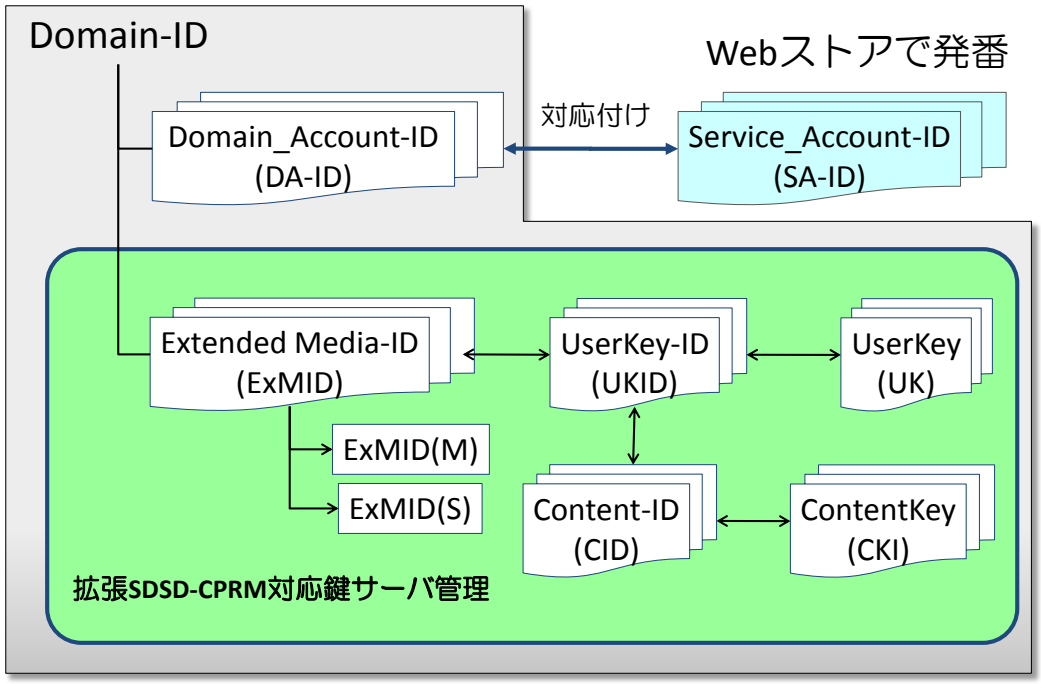


図 7-5：ガイドラインで扱う各種 ID 等の関係

図 7-5 に本ガイドラインで扱う各種 ID 等の関連を示した。各 ID 等の説明を行う。

- Service_Account ID(SA-ID):Web ストアで発行された利用者に対するアカウント ID。Web ストアにログインするために用いられる。DA-ID と関連づけられる。
- Domain ID:Web サーバの発行要請に従い、ライセンスサーバが発行する ID。利用者毎に一つ発行される。Web ストア側で SA-ID と個人情報をもとに関連づけられる。ライセンスサーバ側には個人を特定する情報は保持しない。
- Domain_Account ID(DA-ID):ライセンスサーバ内のライツロッカーで発行するアカウント ID。Web ストア側で発行された SA-ID と関連づけられる。
- Extended Media ID(ExMID):ライセンスサーバが発番する ID で、仮想 SD カード機器用 ExMID(M)と SD カード用 ExMID(C)がある。ExMID(C)は SD カードの MID をもとに仮想 SD カード機器と SD カードの区別ができる機器種別フラグなどを組み合わせで構成される。また、ExMID(M)の MID 相当部分はライセンスサーバが発行する。ExMID は、ユニークな発番体系を持つ。
- User Key ID(UKID):SDA 規格および 4C 規格で規定された ID。ユーザ鍵を特定するために使用される。UKID もライセンスサーバが発行する。
- User Key(UK):4C 規格で規定された秘密鍵。ライセンスサーバとクライアント間での共有秘密鍵で、ライセンスサーバが発行する。UKID と ExMID 間の関係をライセンスサーバは保持する。UK を特定するために、UKID が用いられる。
- Content ID(CID):SDA 規格および 4C 規格で規定された ID。コンテンツを特定するための ID。CID の発行はライセンスサーバが行う。対応するコンテンツ鍵(CK)も同時に生成され、CID が付与される。CID は Web ストア側の配信コンテンツ管理用にも用いられる。
- Content Key(CK):4C 規格で規定された各コンテンツデータを暗号化するための鍵。コンテンツマスター鍵とも呼ぶ。CK は鍵サーバが発行する。CK には CID、使用許諾条件も合わせて付加される。使用許諾条件は Web ストアからの CK 払い出し要請時に Web サーバ側で自由に設定ができる。クライアントに配送される CK は対応するクライアントの UK で暗号化され、Web ストア経由で、該当するクライアントに配送される。UK で暗号化された CK は CKI(Content Key Information)と SDA 規格および 4C 規格では表現される。

また、複数の Web ストアから利用者がコンテンツを購入しても利用者が購入したコンテンツを全て共有できる仕様をライツロッカーは提供することで、利用者利便性を確保する。

7.2.3. ライツロッカーシステムのポリシー

本ガイドラインは前述の通り、ライセンスサーバを独立して配置し、Web ストアとマスタリングシステムとの両方から利用できるシステムモデルを採用し、また、Web サーバとのインターラクションを上位レイヤに位置するライツロッカーシステムに窓口を一本化し、インタフェイスの簡略化を図った。

ライツロッカーの提供する機能を策定するにあたり、ライツロッカーの基本ポリシーを記述する。

(1) 処理の正当性について

各種の鍵/ID の発行やドメイン参加要求など処理の正当性の判定は、サービス事業者で行う。そのため、正当なサービス事業者からの処理要求に対し、ライツロッカーは無条件に処理を行い、処理要求結果をサービス業者に返送する。なお、サービス業者が正当なものであることの担保は双方で共有する通信秘密情報を用いたセッション確立をもって判断する。

(2) デジタルライツの判断について

ライツロッカーは、正当なサービス事業者からの要求に対し、その時点の保有コンテンツやドメインに関する情報を提供するが、デジタルライツ上の判断は行わない。コンテンツ共有や再取得、コンテンツリストア等のデジタルライツ上の処理は、コンテンツ保有者との契約条件に基づきサービス事業者にて判断するものとする。

(3) ライツロッカーの位置づけについて

エンドユーザへのサービス提供は、サービス事業者が行う。そのため、エンドユーザがライツロッカーへ直接接続することはない。また、エンドユーザとライツロッカーの間に契約関係は存在しない。

7.3. サービスモデルにおけるユースケース

ライツロッカーの提供する機能を洗い出すため、想定サービスモデルのシステム連携シーンからビジネスユースケースを列挙する。

ユースケースは、電子書籍の Web ストアへの登録に関連するもの、ストアアカウントに関連するもの、端末に関連するもの、電子書籍の購入に関連するもの、パッケージ製造に関連するものに分けられ、図の緑で示したユースケースにおいて、ライツロッカーとのシステム連携が発生する。

7.3.1. オンラインコンテンツ販売/購入シーン

図 7-6 はオンラインコンテンツ販売のための準備のためのビジネスユースケース図である。

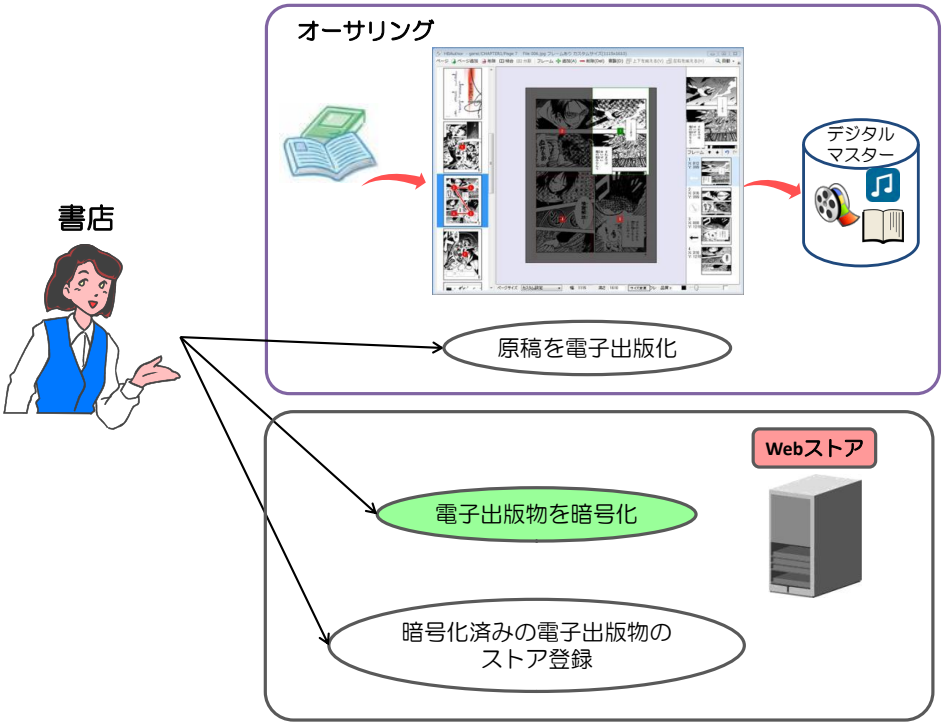


図 7-6：オンラインコンテンツの作成と登録

オンラインコンテンツを準備するためには、オーサリングを行い、デジタルマスターを作成する。次に、デジタルマスター化されたコンテンツデータを暗号化し、Web ストアに登録する。このためにはコンテンツデータの暗号化のためのコンテンツ鍵の生成とコンテンツ ID の発番が必要で、システム連携が発生する。原稿を電子化するシーンと既に暗号化済みの電子出版物のストア登録はライツロッカーと独立に作業ができるため、除外する。

ここで抽出されたシステム連携対象のユースケースは次の 1 項目である。

- 電子書籍を暗号化する

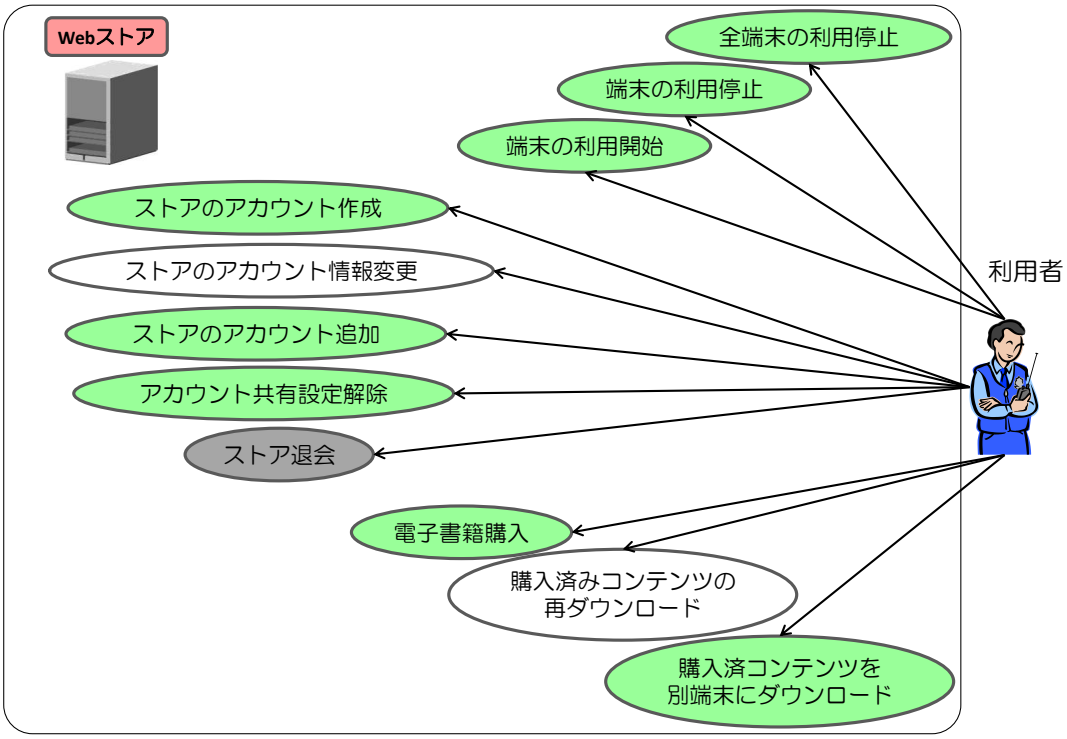


図 7-7：オンラインコンテンツ販売/購入のビジネスユースケース

このユースケースは、ストアアカウントに関連するもの、端末に関連するもの、電子書籍の購入に関連するものに分けられ、図の緑で示したユースケースにてシステム連携が発生する。具体的には以下のユースケースがシステム連携対象となる。なお、「ストアを退会する」ユースケースは連携する必要性が少ないため、グレーで示し連携対象外とする。ここで、抽出されたシステム連携を必要とするユースケースは以下の通りである。

- ストアのアカウントの作成
- ストアのアカウントの追加
- アカウント共有設定の解除

- 端末の利用開始
- 端末の利用停止
- 全端末の利用停止

- 電子書籍の購入
- 購入済コンテンツを別の端末にダウンロード

7.3.2. コンテンツ管理シーン

図 7-8 は購入したコンテンツの管理、ライブラリ管理のビジネスユースケース図である。

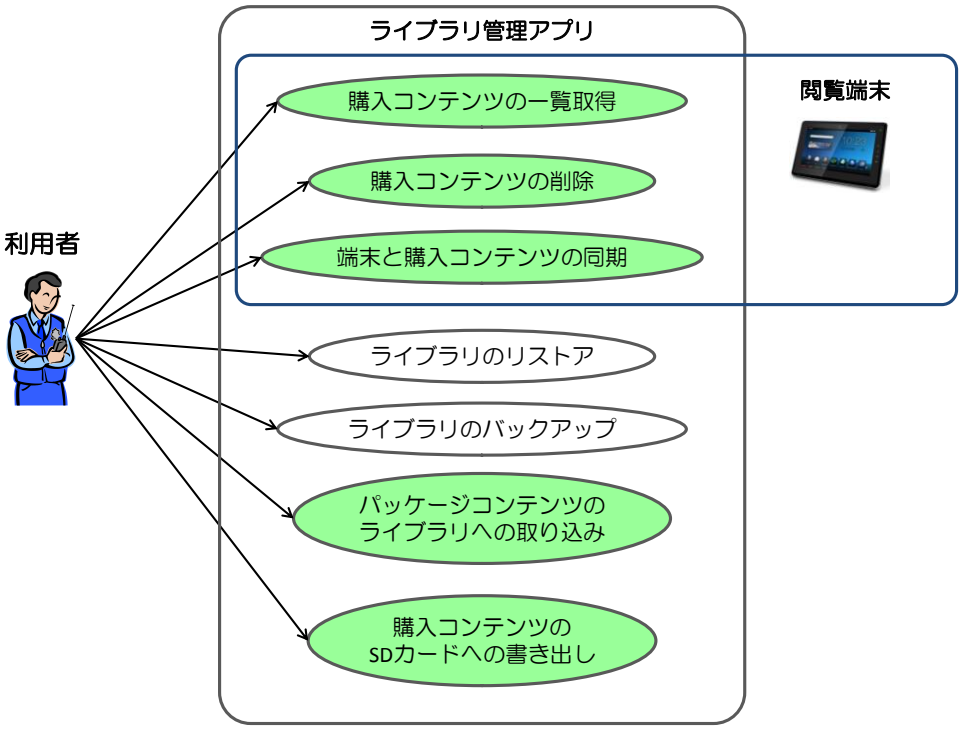


図 7-8：購入コンテンツの管理、ライブラリ管理

ユースケースは購入コンテンツ管理に関連するもの、ライブラリ管理に関連するもの、プリレコ取り込み・SD カード書き出しに関連するものに分けられ、図の緑で示したユースケースにてシステム連携が発生する。ここで、抽出されたシステム連携を必要とするユースケースは以下の通りである。

- 購入コンテンツの一覧取得
- 購入コンテンツの削除
- 端末と購入コンテンツの同期
- プリレコのコンテンツのライブラリ取り込み
- 購入コンテンツの SD カードへの書き出し

7.3.3. プリレコ製造シーン

プリレコを製造するビジネスユースケース図である。

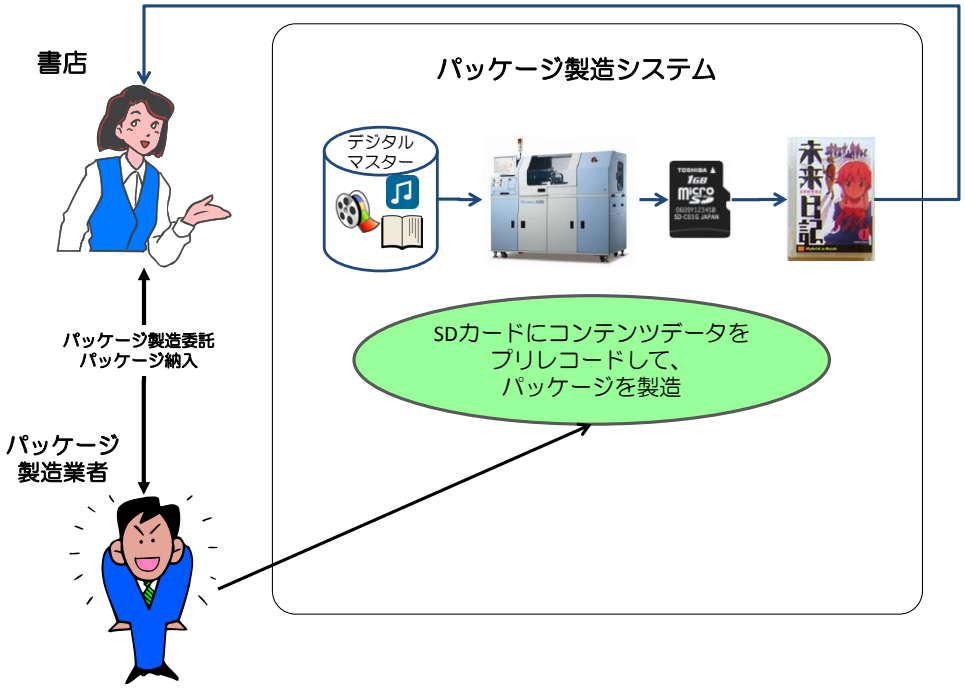


図 7-9：パッケージ製造

ユースケースのプリレコード製造について説明する。ライツロッカーとパッケージ製造装置間をオンラインで接続し、SD カードに書き込むユーザ鍵と SD カード用 Extended Media ID を都度払い出す方法と、パッケージ製造装置でユーザ鍵と SD カード用 Extended Media ID をオフラインで生成し、それらを一括してライツロッカーに登録するバッチ登録処理の２つが考えられる。ここでは、常時オンライン接続という条件に比べ、バッチ登録処理の方が、ライツロッカーとの通信トランザクションが少なく、SD カードへの書き込みスループットが向上するという理由から、バッチ登録処理によるシステム連携とした。

・ プリレコ SD カードの製造

7.4. ユースケースごとにシステムとの連携が必要となる機能

前節で抽出した Web ストアあるいはパッケージ製造システムとライツロッカーとの連携機能をビジネスシーンのユースケースごとに列挙したものが次の表である。

表 7-1：ユースケースごとに必要となる連携機能

No.	ビジネスシーン	ビジネスユースケース	必要となる連携機能
1	電子書籍販売	原稿を電子書籍化する	-
2		電子書籍を暗号化する	コンテンツ鍵発行機能
3		暗号化済の電子書籍をストアに登録する	-
4	電子書籍購入	ストアのアカウントを作成する	Domain Account ID 発行機能
5			仮想 SD カード機器用 Extended Media ID 発行機能
6			SD カード用 Extended Media ID 発行機能
7			ユーザ鍵発行機能
8			ドメイン情報取得機能
9			ドメイン作成機能
10			ドメイン登録機能（端末）
11		ストアのアカウント情報を変更する	-
12		ストアのアカウントを追加する	User Account ID 発行機能
13			ドメイン情報取得機能
14			ドメイン作成機能
15			ドメイン登録機能（アカウント）
16		アカウント共有設定を解除する	ドメイン離脱フロー（アカウント）
17		ストアを退会する	-
18		端末の利用を開始する	Domain Account ID 発行機能
19			仮想 SD カード機器用 Extended Media ID(M)発行機能
20			SD カード用 Extended Media ID(S)発行機能
21			ユーザ鍵発行機能
22			ドメイン情報取得機能
23			ドメイン作成機能
24			ドメイン登録機能（端末）
25		端末の利用を停止する	ドメイン離脱フロー（端末）
26		全端末を利用停止する	ドメイン初期化機能
27		電子書籍を購入する	暗号化コンテンツ鍵発行機能
28		購入済コンテンツを再度ダウンロードする	-
29		購入済コンテンツを別の端末でダウンロードする	暗号化コンテンツ鍵再発行機能
30	コンテンツ管理	購入済コンテンツの一覧を取得する	購入済コンテンツ一覧取得機能

31		購入済コンテンツを削除する	購入済コンテンツ削除機能
32		端末と購入済コンテンツの同期を取る	暗号化コンテンツ鍵再発行機能
33		ライブラリをリストアする	-
34		ライブラリをバックアップする	-
35		プリレコのコンテンツをライブラリに取り込む	コンテンツ move 機能(プリレコ→ライブラリ)
36		ライブラリのコンテンツを SD カードに書き出す	コンテンツ move 機能（ライブラリ→SD カード）
37	プリレコ製造	プリレコを製造する	発行済み SD カード用 Extended Media ID 取込機能
38			発行済みユーザ鍵取込機能

7.5. ライツロッカー提供機能一覧

表 7-1 で必要とされる連携機能をライツロッカーの機能として整理しなおしたものが表 7-2 である。

表 7-2：ライツロッカー提供機能

No.	機能名	内容
1	getEncryptedContentKey	暗号化コンテンツ鍵の取得 (コンテンツ登録時)
2	getExtendedMediaIDforVirtualSDCardMachine	仮想SDカード機器用ExtendedMediaIDの新規取得
3	getExtendedMediaIDforSDCard	SDカード用Media ID（TSMID）の新規取得
4	getUserKey	ユーザ鍵/IDの新規取得
5	getDomainInfo	所属しているドメイン情報の取得
6	createDomain	ドメインの新規作成 (ドメイン作成時にDomain Account IDを自動登
7	registerMachineToDomain	ドメインへの機器登録
8	registerAccountToDomain	ドメインへのアカウント追加登録
9	leaveMachineDomain	ドメインからの機器離脱
10	refreshDomain	ドメイン全機器の初期化
11	leaveAccountDomain	ドメインからのアカウント離脱
12	getLibraryList	ドメインに所属するコンテンツIDのリスト取得
13	getSharedEncryptedContentKey	ライブラリ同期による暗号化コンテンツ鍵の再取
14	getChallengeR1	チャレンジ取得 (SDカード→ドメインのコンテンツMove時)
15	registerContentToDomain	コンテンツIDのドメイン登録 (SDカード→ドメインのコンテンツMove時)
16	deleteContentFromDomain	ドメインからコンテンツIDの削除 (ドメイン→SDカードMove時)
17	getDomain Account ID	Domain Account D（DA-ID）の新規取得
18	getContentKeyID	コンテンツ鍵/ID取得（コンテンツ制作・暗号化
19	getChallengeR1	チャレンジ取得 (プリレコユーザ鍵登録時)
20	registerUseKeys	プリレコユーザ鍵登録

7.5.1. ライツロッカー提供機能説明

ライツロッカーがどこに提供する機能かを整理したものが図 7-10 である。対象はマスタリング装置、Web ストアサーバ、Web ストアサーバを経由したクライアント向けの 3 種類である。図中の番号は表 7-2 の番号と対応している。

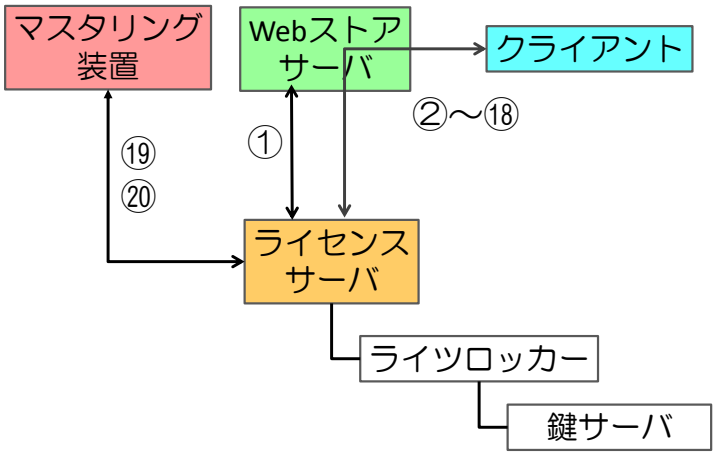


図 7-10：ライツロッカー提供機能関連図

(1) getEncryptedContentKey （暗号化コンテンツ鍵取得）
ライツロッカーシステムは、サービス事業者からコンテンツ鍵の発行要求を受け取る。これに対し、コンテンツ鍵/ID を新規に発行し返信する。あるいは、要求パラメータにて既存コンテンツ ID を指定した場合は既存のコンテンツ鍵を再発行し返信する。本機能はコンテンツ制作時の暗号鍵取得用であり、エンドユーザのクライアント端末は関連しない。

(2) getExtendedMediaIDforVirtualSDCardMachine （仮想 SD カード機器用 Extended Media ID 新規取得）
ライツロッカーシステムは、クライアント端末からの仮想 SD カード機器 ID 発行要求をサービス事業者経由で受け取る。これに対し、鍵サーバは ExMID(M)を新規発行し、サービス事業者を経由してクライアント端末へ返信する。

(3) getExtendedMediaIDforSDCard （SD カード用 Extended Media ID 新規取得）
SD カード識別子としてライツロッカーシステムが独自に発行するユニーク ID を SD カード用 Extended Media ID(ExMID(C))と呼ぶ。ExMID(C)は SD カードの MID 部分を含み、仮想 SD カード機器 IDExMID(M)と区別できる拡張部が付加されている。ライツロッカーシステムは、クライアント端末からの ExMID(C)発行要求をサービス事業者経由で受け取る。これに対し、鍵サーバは ExMID(C)を新規発行し、サービス事業者を経由してクライアント端末へ返信する。

(4)　getUserKey　（ユーザ鍵/ID 新規取得）
ライツロッカーシステムは、クライアント端末からのユーザ鍵/ユーザ鍵 ID 発行要求をサービス事業者経由で受け取る。これに対し、ユーザ鍵/ユーザ鍵 ID を新規発行し、サービス事業者を経由してクライアント端末へ返信する。

(5)　getDomainInfo　（ドメイン情報取得）
ライツロッカーシステムは、クライアント端末からのドメイン情報要求をサービス事業者経由で受け取る。これに対し、クライアントの DA-ID が所属するドメインを検索し、そのドメインの情報をサービス事業者経由で返信する。

(6)　createDomain　（ドメイン作成）
ライツロッカーシステムは、クライアント端末からのドメイン新規作成要求をサービス事業者経由で受け取る。これに対し、ドメインを新たに作成する。

(7)　registerMachineToDomain　（ドメイン機器登録）
ライツロッカーシステムは、クライアント端末から、機器をドメインへ登録する要求をサービス事業者経由で受け取る。これに対し、その機器をドメインへ登録する。

(8)　registerAccountToDomain　（ドメインアカウント追加登録）
ライツロッカーシステムは、クライアント機器から、DA-ID をドメインへ登録する要求をサービス事業者経由で受け取る。これに対し、その DA-ID をドメインへ追加登録する。

(9)　leaveMachineDomain　（ドメイン機器離脱）
ライツロッカーシステムは、クライアント機器から、仮想 SD カード機器をドメインから離脱する要求をサービス事業者経由で受け取る。これに対し、その ExMID(M)をドメインから離脱させる。

(10)　refreshDomain　（ドメイン機器初期化）
ライツロッカーシステムは、クライアント機器から、所属するドメイン内の機器すべてを強制休止する要求をサービス事業者経由で受け取る。これに対し、そのドメインに所属する全機器を強制休止状態に変更する。これにより新たな機器をドメインへ登録できるようにする。

(11)　leaveAccountDomain　（ドメインアカウント離脱）
ライツロッカーシステムは、クライアント機器から、DA-ID をドメインから離脱する要求をサービス事業者経由で受け取る。これに対し、その DA-ID をドメインから離脱させ、ドメイン無所属状態に変更にする。

(12)　getLibraryList　（ライブラリリスト取得）

ライツロッカーシステムは、クライアント機器から、ドメインに登録されているコンテンツ ID のリスト要求をサービス事業者経由で受け取る。これに対し、ドメイン内に登録されているコンテンツ ID リストを返信する。

(13)　getSharedEncryptedContentKey　（暗号化コンテンツ鍵再取得）
ライツロッカーシステムは、クライアント機器から、ドメインに登録されているコンテンツ ID の暗号化コンテンツ鍵の再発行要求をサービス事業者経由で受け取る。これに対し、コンテンツ ID がドメインに登録されているか否かをチェックし、ユーザ鍵で暗号化したコンテンツ鍵を返信する。本機能はドメイン上のライブラリとクライアント端末でのライブラリの同期を取る目的で利用される。

(14)　getChallengeR1　（Move 用チャレンジ取得/プリレコユーザ鍵登録用チャレンジ取得）
ライツロッカーシステムは、クライアント機器から、チャレンジ/レスポンス認証に用いるチャレンジデータの発行要求をサービス事業者経由で受け取る。これに対し、チャレンジデータを発行し返信する。本機能は SD カードからライツロッカー上のドメインへコンテンツを Move する際、およびプリレコユーザ鍵登録の際に利用される。

(15)　registerContentToDomain　（コンテンツ ID のドメイン登録）
ライツロッカーシステムは、クライアント機器から、チャレンジ/レスポンス方式で暗号化した登録データをサービス事業者経由で受け取る。これに対し、登録データを復号しコンテンツ ID をドメインへ登録する。本機能は上記(14)と一対で、SD カードからライツロッカー上のドメインへコンテンツを Move する際に利用される。

(16)　deleteContentFromDomain　（ドメインからコンテンツ ID 削除）
ライツロッカーシステムは、クライアント機器から、ドメインからコンテンツ ID を削除する要求をサービス事業者経由で受け取る。これに対し、当該コンテンツ ID をドメインから削除する。本機能はドメインから SD カードへコンテンツを Move する際に利用される。

(17)　getDomainAccountID　（Domain アカウント ID 取得）
ライツロッカーシステムは、クライアント機器から、Domain アカウント ID（DA-ID）の発行要求をサービス事業者経由で受け取る。これに対し、DA-ID を新規に発行し、返信する。

(18)　getContentKeyID　（コンテンツ鍵/ID 取得）
ライツロッカーシステムは、サービス事業者からコンテンツ鍵の発行要求を受け取る。これに対し、コンテンツ鍵/ID を新規に発行し返信する。あるいは、要求パラメータにて既存コンテンツ ID を指定した場合は既存のコンテンツ鍵を再発行し返信する。本機能はコンテンツ制作時の暗号鍵取得用であり、エンドユーザのクライアント端末は関連し

ない。

(19) getChallengeR1 （チャレンジ取得）
ライツロッカーシステムは、プリレコ SD カード製造事業者から、チャレンジ/レスポンス認証に用いるチャレンジデータの発行要求を受け取る。これに対し、チャレンジデータを発行し返信する。本機能はプリレコユーザ鍵登録の際に利用される。

(20) registerUserKeys （プリレコユーザ鍵登録）
ライツロッカーシステムは、プリレコ SD カード製造事業者から、チャレンジ/レスポンス方式で暗号化した登録データを受け取る。これに対し、登録データを復号しユーザ鍵/ID、ExMID(C)等をデータベースに登録する。本機能は上記(19)と一対で、プリレコ SD カード製造事業者によって発行されたユーザ鍵/ID、ExMID(C)等をデータベースに登録する目的で利用される。

8. 本ガイドラインにおけるシステムセキュリティ

8.1. コンテンツデータの暗号とコンテンツ鍵の暗号

コンテンツデータとコンテンツ鍵は通常の使用法でアクセス可能な領域に格納される。このため、コンピュテーションパワーに物を言わせた総当りによる攻撃（「ブルートフォースアタック」）に耐えられる暗号強度が要求される。近年のコンピュータ処理能力の著しい向上により、鍵長の短い暗号は容易にブルートフォースアタックによって破られる危険性が高まってきた。

AES は共通鍵暗号において実質的にデファクト・スタンダードとしての地位を確立しつつあり、主要な標準化規格である米国政府標準暗号、電子政府推奨暗号(CRYPTREC)、欧州連合推奨暗号、ISO/IEC 国際標準暗号、インターネット標準暗号のいずれの規格でも 128 ビット・共通鍵ブロック暗号の標準に認定されていることを鑑み、本ガイドラインでもコンテンツデータの暗号とコンテンツ鍵の暗号は AES128 ビットを推奨する。

8.2. システム間セキュリティ

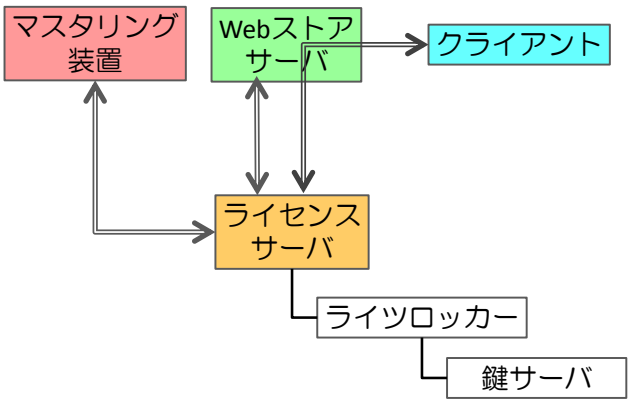


図 8-1：システム間セキュリティ対象

図 8-1 に本ガイドラインにおけるシステム間のセキュリティ対象区間を二重線矢印で表示した。これらの通信区間ではシステム間セキュリティに配慮しなければならない。

8.2.1. ライセンスサーバとマスタリング製造装置間

あらかじめマスタリング製造装置とライセンスサーバ(実質はライツロッカーシステム)の双方で通信秘密情報を共有する。本ガイドラインにおいて、マスタリング製造装置はオフライン動作で SD カードに秘密情報を書き込むことができるため、書き込まれたデータをバッチ処理でライセンスサーバのデータベースに反映させる必要がある。

ライツロッカーシステムの提供する機能(19)チャレンジ取得と(20)プリレコユーザ鍵登録を用いて、ライセンスサーバのデータベースに反映させる。

マスタリング製造装置とライセンスサーバ間の通信は、HTTPS を推奨する。マスタリン

グ製造装置とライセンスサーバ間の通信は IP アドレスによる接続制限を行うことで、ライセンスサーバなど脅威の低減を図る。

8.2.2. ライセンスサーバと Web ストアサーバ間

ライセンスサーバが発行するプライベート認証局の SSL クライアント証明書を Web ストアサーバにインストールし、Web ストアサーバとライセンスサーバ間の認証を行う。

あらかじめ Web ストアサーバとライセンスサーバの双方で通信秘密情報を共有する。

本ガイドラインにおいては、Web ストアサーバとライセンスサーバ間では Web ストアサーバがコンテンツを暗号化、登録を行うため、コンテンツ鍵とコンテンツ ID を必要とする。ライセンスサーバは Web ストアサーバの要請により、コンテンツ鍵を発行し、秘密情報を用いた暗号化処理によりデータをセキュアに配信する。

ライツロッカーシステムの提供する機能(1)暗号化コンテンツ鍵取得を用いて、ライセンスサーバに要求する。

Web ストアサーバとライセンスサーバ間の通信は、HTTPS を推奨する。Web ストアサーバとライセンスサーバ間の通信は IP アドレスによる接続制限を行うことで、ライセンスサーバへのハッキングなど脅威の低減を図る。

8.2.3. Web ストアサーバを経由したライセンスサーバとクライアント間

クライアント端末機器とライツロッカー間の通信においてはセキュアセッションを必ずしも必要とはしないが、通信路での改ざんなどの妨害を阻止するため、秘密情報を共有することで、Web サーバを介して、ライセンスサーバは通信秘密情報を用いた暗号化処理により、ライツロッカーシステムとクライアント端末機器間の end to end でセキュアな配信を実現する。

ライセンスサーバの提供する機能(2)から(18)はクライアントからの要求に応える機能である。

なお、上記の秘密情報は、ライセンスサーバ側では複数持つため、どの秘密情報を使っているかを特定するため、秘密情報 ID を使用して指定をする。

8.3. 各システム要素に要求されるセキュリティ項目

8.3.1. Web ストアサーバ

本ガイドラインに準拠する Web ストアサーバは以下のセキュリティ項目を満足しなければならない。

- Web ストアサーバはライセンスサーバから発行されたコンテンツ鍵を自身で保護した状態で保存しなければならない。
- Web ストアサーバはライセンスサーバから発行されたコンテンツ鍵を用いたコンテンツの暗号化処理をセキュアに行わなければならない。

8.3.2. マスタリング製造装置

本ガイドラインに準拠するマスタリング製造装置は以下のセキュリティ項目を満足しなければならない。

- マスタリング製造装置は SD カードの保護領域をセキュアにアクセスしなければならい。
- マスタリング製造装置は SD カードにプリレコードした保護すべき情報はセキュアに管理しなければならない。
- マスタリング製造装置はライセンスサーバにユーザ鍵など SD カードにプリレコードした権利保護情報を適宜、登録しなければならない。

8.3.3. ライセンスサーバ

本ガイドラインに準拠するライセンスサーバは以下のセキュリティ項目を満足しなければならない。

- ライセンスサーバは自身の管理するデータベースをセキュアに管理しなければならない。
- ライセンスサーバは予め登録された Web ストアサーバ、マスタリング製造装置以外からのアクセスを拒否しなければならない。

8.3.4. クライアント

8.3.4.1. クライアントに対するセキュリティ項目

本ガイドラインに準拠するクライアントは以下のセキュリティ項目を満足しなければならない。

- クライアントはライセンスサーバから発行されたユーザ鍵を SD カード或いは仮想 SD カードの保護領域にセキュアに保存すなければならない。
- クライアントはSDカード或いは仮想SDカードの保護領域をセキュアにアクセスできなければならない。
- クライアントはコンテンツをセキュアに復号して表示できなければならない。
- クライアントはユーザ鍵に付随した使用許諾条件に従って動作しなければならない。
- クライアントはコンテンツ鍵に付随した使用許諾条件に従って動作しなければならない。クライアントは使用許諾条件の改ざんを検出し、改ざんを発見した場合は、該当するコンテンツの復号を中止しなければならない。
- クライアントはコンテンツの正当性を検証し、不正なコンテンツを検出したときには動作を中止できなくてはならない。

8.3.4.2. クライアントに対するロバストネスルール

コンテンツやアクセスのための鍵の秘密情報や使用許諾条件（Usage Rule）は機器内での処理などで外部から簡単に読み出されない仕様を施す必要がある。また秘密情報の取り扱いは運営上の規定が必要となる。

以下に、4C で規定する基準の例を列挙する。クライアントは 4C で規定するロバストネ

スルールに準じて実装されなければならない。

8.3.4.3. 取り扱いの考慮が必要な情報

秘匿が必要なデータ

- コンテンツのアクセスに必要なデバイスに与えられるデバイス鍵（SD カードの場合）
- コンテンツのアクセスに必要なデバイスが自身で持つ秘密鍵（仮想 SD カードの場合）
- コンテンツの復号に必要な鍵
- 復号されたコンテンツ

改ざん防止が必要なデータ

- ✧ Usage Rule
- ✧ Usage Rule に従った出力制御情報

特にデバイス鍵に関しては、漏洩するとすべてのコンテンツへのアクセスが可能となるため、提供する際に必要最低限のごく限られたメンバへのみ開示を許可するよう義務付けられること。

コンテンツへのアクセス制限

機器内で復号したコンテンツデータをユーザが容易にアクセスできる経路やメモリ上に伝送または記録してはならない。具体的には PCMCIA、IEEE1394、Cardbus などがそれに該当する。ただし Memory buses、CPU buses などの機器 chip 内で動作する伝送路は該当しないものとする。コンテンツは通常、データ圧縮された形で配布されており、その圧縮データと非圧縮データとで取り扱いを分ける考え方もある。その場合、圧縮データは非圧縮データと比較してより小さなデータで配布が用意であることを考慮して取り扱いを厳しく設定するなどの差をつけてもよい。

8.3.4.4. 実装例

ソフトウェアの場合、一例として実行プログラムのステップ解析が困難となるプログラムの暗号化やソースコードスパゲティ化等によるソフトウェア耐タンパ実装による保護が一般的である。またソースコードにデジタル署名を施す等で、実行コードの改ざんの検出を行い、改ざんが検出された場合には処理が停止する仕組みを盛り込む方式も行われている。近年のコンピュータ環境では立ち上げ時に想定したプログラム、アプリケーション以外を排除し、搭載されているプログラム、アプリケーションに対しては秘密情報の管理を提供するシステムも提案されており、そういったものを利用することでも実現可能である。

ハードウェアの場合、多くの場合においては LSI などのハードウェアチップと処理を行うプロセスを記述したミドルウェアを実行することの組み合わせで処理が行われる。この場合にはデバイス鍵などの秘匿すべき情報に関してはハードウェアチップ内でのみ復号された形で利用され、万が一ハードウェアチップ外へ書きだす必要がある場合には一定強度以上の暗号化された形での出力がなされる。またその際の暗号化は

チップ毎に異なる固有鍵を設定することが望ましく、またその情報はデバイス鍵と同等の運用ルールで管理される必要がある。

8.3.4.5. 機器クラックに対抗するための機器の強靭性基準

機器が不正改変された場合に機器認証や暗号復号の機能が働かなくなるような設計

•シリコン回路やファームウエアにおいてデバイス鍵や暗号アルゴリズムが"容易に"読みこまれないように設計されること。ここでの"容易に"に関しては二つのレベルを定義する。

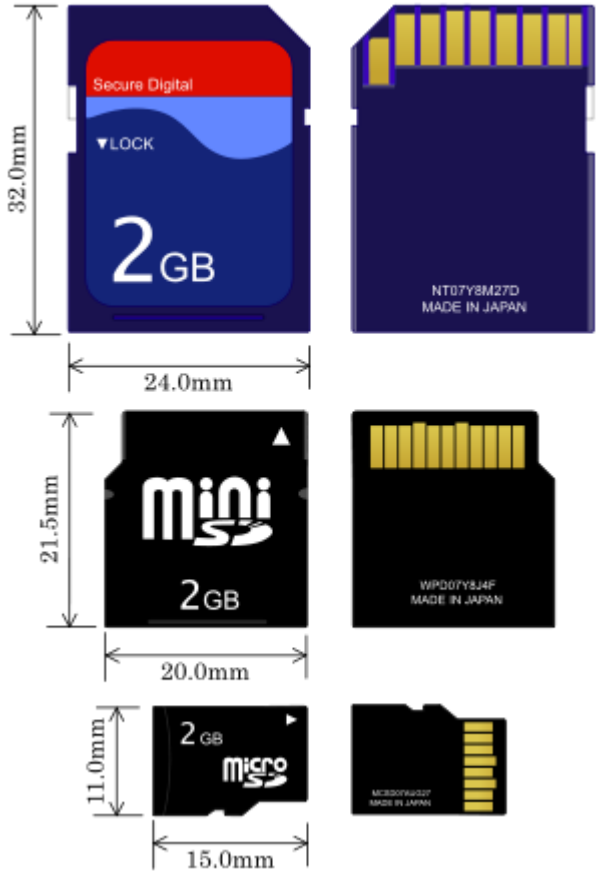
（1）一般的に入手が容易な汎用ツールまたは解析ツールによって不正な改ざん解析はできないような対策が施されていること。汎用ツールとしてはスクリュードライバー、ジャンパー、クリップ、ファイルエディター、半田ごてなどが該当する。解析ツールとしては一般ユーザが利用する安価なメモリ解析ツール、デバッガー、デコンパイラー、ソフトウェア解析ツールなどが該当する。

（2）製品製造者が利用するプロフェッショナルツールによって不正な改ざんや解析を行う場合には困難さが伴うこと。プロフェッショナルツールとしては、回路アナライザ、Chip disassembly system、回路エミュレーターが該当する。当該機器専用の解析ツールや NDA 対象のツールはこれに該当しない。

9. 参考資料

9.1. SD カードについて

SD カードはフラッシュメモリを用いたメモリカードである。形状は Normal、mini、micro の 3 種類がある。形状の違いはあるが機能的な違いはない。変換アダプタを併用することで、形状変換が可能である。現在、携帯電話や TabletPC などでは micro タイプが用いられている。mini は当初、携帯電話用に開発されたが、よりスケールファクタの小さい micro の規格化により、今後市場から姿を消すことが予想される。



SD カードはそのメモリ容量によって、2GB 未満の Normal Capacity、2GB 以上 32GB 未満の HC (High Capacity)、32GB 以上 2TB 未満の XC (eXtended Capacity)の 3 タイプの規格が整備されている。

SD カードの容量種別による互換性について、図 9-1 図を用いて説明する。SD カードは容量帯によって内部のファイルシステムが異なるため、Host 機器が異なるファイルシステムに対応しているかどうかで、該当する SD カードが扱えるかが決まる。例えば、2GB 未満の Normal Capacity の SD カードしか扱えない Host 機器は FAT12/16 のファイルシステムしか対応していないため、FAT32 をファイルシステムに持つ 2GB 以上 32GB 未満の HC (High Capacity)の SD カードを扱うことができない。しかし、SD カードを扱う Host 機器は下位互換性を確保することが SDA で規定されているため、HC (High Capacity)の SD カードを扱える Host 機器は Normal Capacity の SD カードも扱うことができる。従って、Normal

Capacity の SD カードしか対応しない機器では HC などの上位規格の SD カードは扱えないので注意が必要である。逆の言い方をすれば、Normal Capacity の SD カードはどの Host 機器でも対応する。

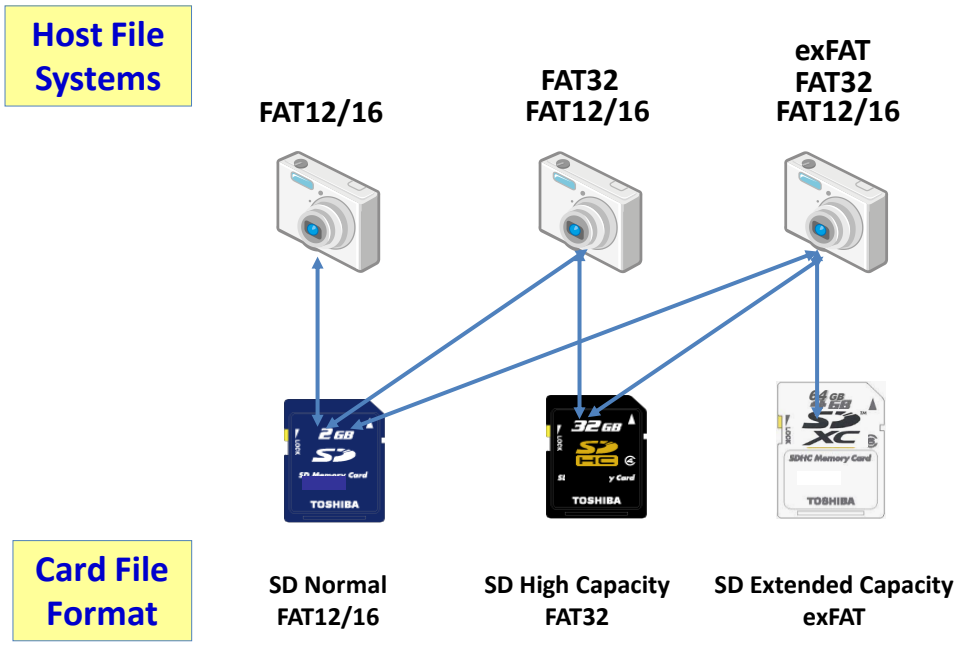


図 9-1：SD カードの容量種別による互換性

9.2. SD-Card Association(SDA)について

SD-Card Association は、市場をリードする SD テクノロジーの利便性を活用して業界標準を設定し、消費者電気製品、無線通信、およびデジタルイメージングとネットワーキング製品の開発を促進しているテクノロジー企業による地球規模のエコシステムである。

SD アソシエーションは、パナソニック、サンディスク、および東芝の三社によって、2000 年 1 月に設立された。業界全般にわたる新しい組織として、さまざまなアプリケーションにおける SD 製品の採用拡大を目指し、業界標準を設定してきた。今日、SD-Card Association は、SD テクノロジーを使用した製品の設計、開発、製造、または販売に携わる約 1,300 社の会員企業を擁している。

SD テクノロジーは、事実上の業界標準として、十数種類もの製品ラインで、400 以上のブランドの 8,000 を超すモデルに採用されている。

SD アソシエーションのメンバーシップでは、完全な SD 技術仕様の最新情報を提供している。これにより会員企業は、標準に準拠し、他の SD 機器と互換性を有するように設計した製品とソリューションを開発できる。会員は、委員会やワーキング部会などの SD-Card

Association のアクティビティへの参加機会を有し、業界をリードするメモリカードのテクノロジーの発展と機器標準の運用を展開している。

9.3. 4C Entity LLC(4C)について

デジタルコンテンツの著作権保護技術をライセンスする目的で構成された、4 つの企業（IBM,Intel,松下電器、東芝）からなる組織体。

以上