システム開発
19-F-4

高信頼・高セキュリティ光ディスク媒体の活用システム開発に関するフィージビリティスタディ

報　告　書

― 要　旨 ―

平成 20 年 3 月

財団法人　機械システム振興協会
委託先　財団法人デジタルコンテンツ協会

KEIRIN
この事業は、競輪の補助金を受けて実施したものです。
URL : http://ringring-keirin.jp/

序

わが国経済の安定成長への推進にあたり、機械情報産業をめぐる経済的、社会的諸条件は急速な変化を見せており、社会生活における環境、都市、防災、住宅、福祉、教育など、直面する問題の解決を図るためには技術開発力の強化に加えて、多様化、高度化する社会的ニーズに適応する機械情報システムの研究開発が必要であります。

このような社会情勢の変化に対応するため、財団法人機械システム振興協会では、財団法人日本自転車振興会から機械工業振興資金の交付を受けて、システム技術開発調査研究事業、システム開発事業、新機械システム普及促進事業を実施しております。

このうち、システム技術開発調査研究事業及びシステム開発事業については、当協会に総合システム調査開発委員会(委員長：東京大学名誉教授 藤正 巖氏）を設置し、同委員会のご指導のもとに推進しております。

本「高信頼・高セキュリティ光ディスク媒体の活用システム開発に関するフィージビリティスタディ」は、上記事業の一環として、当協会が財団法人 デジタルコンテンツ協会に委託し、実施した成果をまとめたもので、関係諸分野の皆様方のお役に立てれば幸いであります。

平成２０年３月

財団法人 機械システム振興協会

はじめに

本報告書は、財団法人デジタルコンテンツ協会（DCAj）が、財団法人機械システム振興協会から平成１９年度事業として受託した「高信頼・高セキュリティ光ディスク媒体の活用システム開発に関するフィージビリティスタディ」の成果をまとめたものである。

近年、個人情報のみならず国家機密に属する情報の流出を含めた情報漏洩が多発しており情報管理に対する社会的関心が一段と高まってきている。医師法２４条に規定された診療録（カルテ）の保存義務は５年間だが、昨今の社会情勢を反映して、カルテを電子化し長期保存する必要性がクローズアップされつつある。また、J-SOX 法により本年４月以降に開始される事業年度から財務会計報告書の提出など内部統制が求められるようになるが、財務帳票などは改ざん防止の観点から、高解像度のフルカラー・スキャナーを用い、帳票の質感やインクのにじみ感までも再現可能に保存することが要求されている。　従って、レントゲン写真のような大容量データを含む電子カルテや高解像度のスキャナを用いた財務帳票などの大容量データを長期間保存するためには大容量且つ真正性、見読性及び保存性に優れ、ＯＳとアプリケーションを自己完結的に収納（タイムカプセル化）し、ＯＳや暗号アルゴリズムの陳腐化による復元性の喪失を防ぐことが重要である。以上の状況から、高セキュリティで寿命の長い光ディスク媒体開発への期待が大きくなっている。

本フィージビリティスタディ（以下「本スタディ」という）は、これらの社会的情勢を踏まえ、前述の要求課題に対する解決方法となる可能性の高い高度暗号チップ搭載光ディスクシステムにつき、研究及び検証のための実験を行い、高度暗号チップ搭載光ディスクシステムの検討・改良及び実用化を目指すものである。

本スタディの実施にあたり、ご指導・ご支援をいただいた関係の官庁、関係機関の各位に感謝の意を表します。

平成２０年３月

財団法人　デジタルコンテンツ協会

目　次

１　スタディの目的

政府が発表したe-Japan戦略Ⅱ加速化パッケージで挙げられた重点分野のe-文書法が平成１７年４月１日より施行された。それに伴い、法律で定められた書類だけでなくデジタルコンテンツによる文化をはじめ、行政、学術研究、医療、教育などにおいて幅広くデジタルデータによるアーカイブが急速に増えつつある。しかし、一方で、その保存などの信頼性については技術的な根拠が明確にされておらず、また、違法コピーや不正利用などによる被害も急増し、デジタルコンテンツビジネスの将来への懸念がなされている。

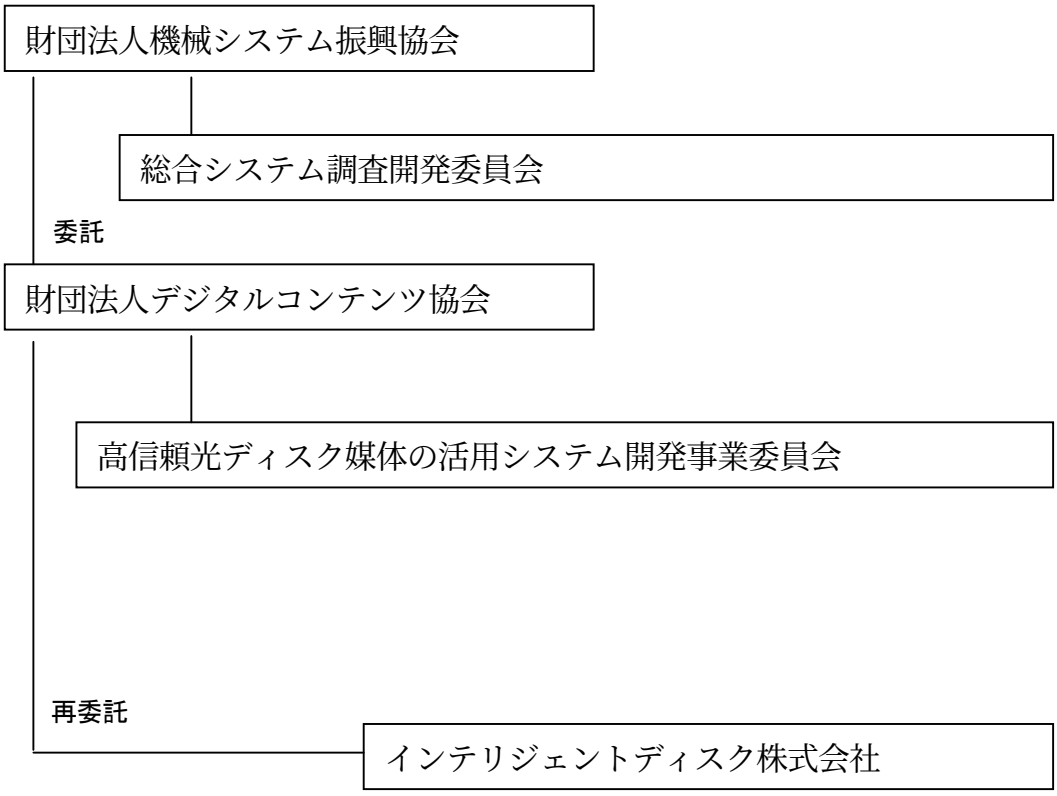
本スタディでは１８年度までに研究された、高信頼性光ディスク媒体の応用研究と組み合わせて、「高度暗号チップ内蔵大容量光ディスク」を利用したコンテンツ流通・管理システムを開発することにより、安全かつ安価なコンテンツ流通・管理を実現し、デジタルコンテンツビジネスの発展に寄与することを目指す。

高信頼性・高セキュリティの記録媒体の普及は、デジタルコンテンツ業界が渇望するものであり、本スタディの成果により、同産業界のさらなる発展と、文書の電子化及び、デジタルコンテンツの普及促進が期待される。

2　スタディの実施体制

財団法人機械システム振興協会内に「総合システム調査開発委員会」を、財団法人デジタルコンテンツ協会内に当協会会員会社と外部有識者などからなる「高信頼光ディスク媒体の活用システム開発事業委員会」を設置してフィージビリティスタディを実施した。

また、高信頼光ディスクシステムの課題基礎検討、改良試作とシステム検討業務は、財団法人デジタルコンテンツ協会よりインテリジェントディスク株式会社に再委託を行った。



総合システム調査開発委員会委員名簿

（順不同・敬称略）

委員長	東京大学 名誉教授	藤　正　　巖
委　員	埼玉大学総合研究機構 地域共同研究センター 教授	太　田　公　廣
委　員	独立行政法人産業技術総合研究所 エレクトロニクス研究部門 副研究部門長	金　丸　正　剛
委　員	独立行政法人産業技術総合研究所 産学官連携推進部門 産学官連携コーディネータ	志　村　洋　文
委　員	東北大学大学院 工学研究科　教授 （未来科学技術共同研究センター長）	中　島　一　郎
委　員	東京工業大学大学院 総合理工学研究科 教授	廣　田　　薫
委　員	東京大学大学院 工学系研究科 准教授	藤　岡　健　彦
委　員	東京大学大学院 新領域創成科学研究科 教授（副研究科長）	大　和　裕　幸

高信頼光ディスク媒体の活用システム開発事業委員会名簿

（順不同・敬称略）

委員長	サイバー大学 ＩＴ総合学部 学部長・教授 東京大学名誉教授	石 田　晴 久
副委員長	東京電力株式会社 技術開発本部 技術開発研究所 お客さま情報技術グループ マネージャー	中 村　正 規
委　員	富士通株式会社 電子デバイス事業本部 基盤商品マーケッティング統括部 統括部長代理	尾 崎　浩 司
委　員	インテリジェントディスク株式会社 取締役	後 藤　富 雄
委　員	パナソニック インダストリー セールス株式会社 広域営業本部 東部営業チーム 主事	福　田　　潔
オブザーバ	インテリジェントディスク株式会社	
	代表取締役社長	重 富　孝 士
	取締役	刈 本　博 保
	取締役	安 田　　洋
事務局	財団法人デジタルコンテンツ協会	
	常務理事、　(兼)事業開発本部長	田 中　誠 一
	事業開発本部　先導的事業推進部長	大 橋　淑 郎
	事業開発本部　先導的事業推進部　研究主幹	千 葉　祐 治
	事業開発本部　先導的事業推進部　研究主幹	土 屋　光 久
	事業開発本部　主任	須 藤　智 明

3　スタディの内容

(1)　システム開発

平成１７年度、平成１８年度に行ったスタディの結果にもとづき、高度暗号チップ搭載光ディスクの試作で判明した課題解決を含め、Blu-ray ディスクへのチップ搭載時の安定動作、大容量かつ安全なファイルシステムの試作と、評価を行った。

１）大容量化の要求への対応と、平成１８年度スタディで判明した課題を解決するため、Blu-ray ディスクの高度暗号チップを搭載する技術の改良開発を行った。
ディスク媒体への半導体ベアチップとプリントアンテナの実装を検討した。

２）Blu-ray ディスク R/W（リーダライタ）のドライブへの実装方法の改良開発を行った。

３）大容量光ディスク媒体への ROM データ、RAM データの書き込み及びテスト方法の改良開発を行った。
大容量光ディスクのパーシャル ROM 化の可能性を検討した。

４）利用目的に応じた暗号チップの最適化の調査、技術検討を行った。
セキュリティ強度、対タンパ性、メモリサイズ、演算能力、チップサイズ、チップ製造コスト、耐久年数などを調査検討した。

(2)　実証実験・評価

試作した機器、装置及び、システムでの評価を行った。

１）暗号チップ搭載 Blu-ray ディスクと専用ドライブでの機能試験、評価を行った。

２）光ディスクの大容量/保存性と暗号チップ搭載の安全性を生かしたアプリケーションシステムの実証試験として、東京電力㈱のセキュアネットワークシステム(FACCIO)を利用し、安心･安全なファイル管理システム実証実験を行った。

(3)　実用化システムに向けた課題と検討

実証実験・評価結果から、将来目指すシステムの姿及び、仕様を検討した。

１）コンテンツ流通／保存・管理システムの展開の検討として、主としてビジネス関連業界における導入方法、手段の検討を行った。

２）個人ユーザの利便性と安全・安心を実現するための手段としての高信頼･高セキュリティ光ディスク媒体利用システムの検討を行った。

第１章　システム開発

1.1　光ディスクへの高度暗号チップの搭載

高度暗号チップ搭載光ディスクシステムは①Blu-ray やDVD-RAMに書き込み･読み出しできる光ディスクドライブ、②アンテナと高度暗号チップが搭載された光ディスク、③リーダ･ライタ側アンテナから高度暗号チップにパワーを供給すると同時に信号の入出力処理を行うリーダ･ライタから構成される。　図1.1-1は本システムのドライブの内部構造の概要を模式的にあらわしている。リーダ･ライタからの情報データ（212kbps）で13.56MHzの搬送波を変調して、高度暗号チップが搭載されているフレキシブル・フイルム上のアンテナに供給される。

高度暗号チップはその情報データから認証処理、個人データなどを暗号処理して書き込み・読込むことができる。また、光ディスクへの情報データの書き込み・読み出し時に利用される暗号コードを生成することができる。次に個人認証処理や情報データの出力をリーダ･ライタを通じてパソコン側で処理できる。

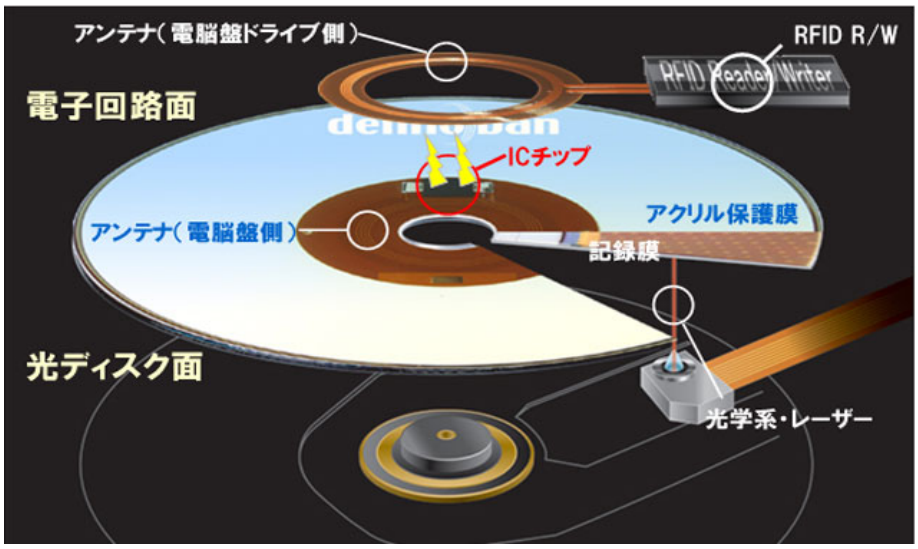


図1.1-1　光ディスクドライブの構造

ディスクに搭載された高度暗号チップは、表1.1-1の高度暗号チップ仕様に示しているように、ISO1443-Bのインタフェースで、32bit　CPU、ユーザエリアとして３２KBのFRAM領域を持っている。さらに、暗号系ソフトもT-DES、RSA及び擬似乱数生成が可能である。

これらを用いて、暗号の生成、認証処理、また個人データの保存などを行っている。

ディスクの光記録面に保存されるファイルを暗号化する暗号コードを生成し、暗号化した上で高度暗号チップのFRAM領域に保管している。

ところで従来の高度暗号チップが搭載されていない光ディスクでは光ディスクドライブからファイルをユーザによって丸コピーされてしまう可能性がある。

もし、その中に情報データの復号を行うキーが入っている時は、暗号コードは解析されてしまう危険性がある。

しかし IC カードのセキュリティ同様に高度暗号チップに保管されている暗号コードは、暗号化されて保管されていること、また FRAM という圧電素子でできていることもあり、チップに化学的な方法を駆使しても暗号コードを読込むことはほとんど不可能である。

表 1.1-1　高度暗号チップの仕様

＜ハード＞	
インタフェース	ISO14443-B（106、212kbps）
CPU	32bit FR コア（RISC）
FRAM	32KB
SRAM	8 KB
ROM	128KB
<ソフト＞	
暗号系	JavaCard2.2_01 搭載 T-DES、RSA（1024bit,512bit）
擬似乱数生成	

しかし、高度暗号チップを Blu-ray ディスク上に搭載するには、以下の物理的な課題を解決する必要がある。

① 光ディスクドライブのスピンドルモータから磁気的なノイズや金属（光ディスク記録面の金属薄膜またはリーダ・ライタ側のアンテナを保持するフレーム、ホルダープレートの金属）による渦電流損に対しても影響されないようにする。

② ディスクの回転安定性のために、アンテナの重量を軽減化し、かつ点対称形状になるようにして高速回転時のバランスを保つ構造にする。

③ 通信に影響する電磁パラメータの許容範囲を広げ、各種ディスクの材料構成によらず対応できるようにする。

④ 共振周波数 13.56MHz に対応するようにアンテナフイルムの材質やトリマコンデンサの搭載などを検討する。

⑤ DVD-RAM、Blu-ray ディスクや他のディスクにも貼付可能にするため、ディスク表面にアンテナを貼合わせる構成にする。

⑥ 安価で製造工程的にも容易な構成にする。

などの課題を解決しなければならない。特に Blu-ray ディスクでは DVD-RAM に比べ、光記録密度がさらに高くなるので、回転安定性の条件はさらに厳しくなるものと予想していた。さらに、リーダ･ライタの課題としては、以下に示すような課題がある。

従来のような大型リーダ・ライタでは薄型のノートパソコンに搭載はできない、さらにコスト面も含めて課題がある。

また、光ディスクドライブのマーケットは軽量･薄型化の方向にあり、薄型光ディスクドライブに搭載できるようにリーダ･ライタを小型化する。

リーダ・ライタの機能を光ディスクのドライブ回路と一体化して、部品点数、製造工程数の削減を図る。

これらの課題を解決するため以下の開発を行った。

1.1.1 Blu-ray ディスクへのアンテナ実装

（1）ディスク側のアンテナ形状

Blu-ray ディスクドライブの場合、リーダ・ライタ側のアンテナ側に高速回転を行う。

ディスクを固定するため、永久磁石が内蔵されたクランパーが設置されている。図 1.1-１に全体の構成を示しているが､クランパーはリーダ･ライタのアンテナ側に挿入される形で配置されている。また、図 1.1.1-1 にリーダ・ライタ側アンテナ周辺の断面構造を示している。

このような構造を持っているため、クランパーによる電磁特性への影響とスピンドルモータからの通信に影響する電磁特性と金属体による渦電流損をディスク側のアンテナとの相対的な位置関係を検討した。

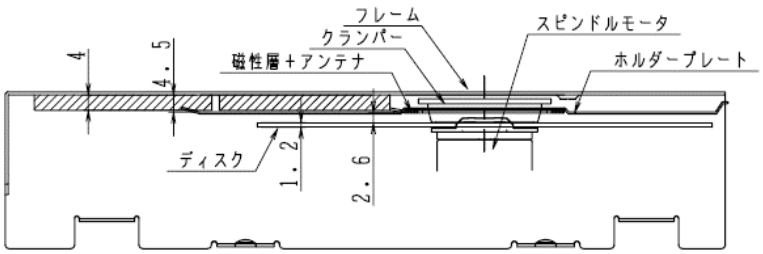


図 1.1.1-1 リーダ・ライタ側アンテナ周辺の断面構造

図 1.1.1-2 に示すように光ディスク側では、Blu-ray ディスクの記録層が金属膜に相当し、またリーダ・ライタ側のアンテナ側では、フレームの金属板が金属パッケージに相当する構造でありそれからの渦電流により生じる磁界により搬送波（13.56MHｚ）が打ち消される可能性がある。実験結果として、Blu-ray ディスク側のフレキシブル・フイルム上に形成されたアンテナでは、その裏面から磁性薄膜を削除することに成功したが、リーダ・ライタ側の磁性薄膜は必要であることがわかったので、そこに至った経緯を、以下のとおり説明する。

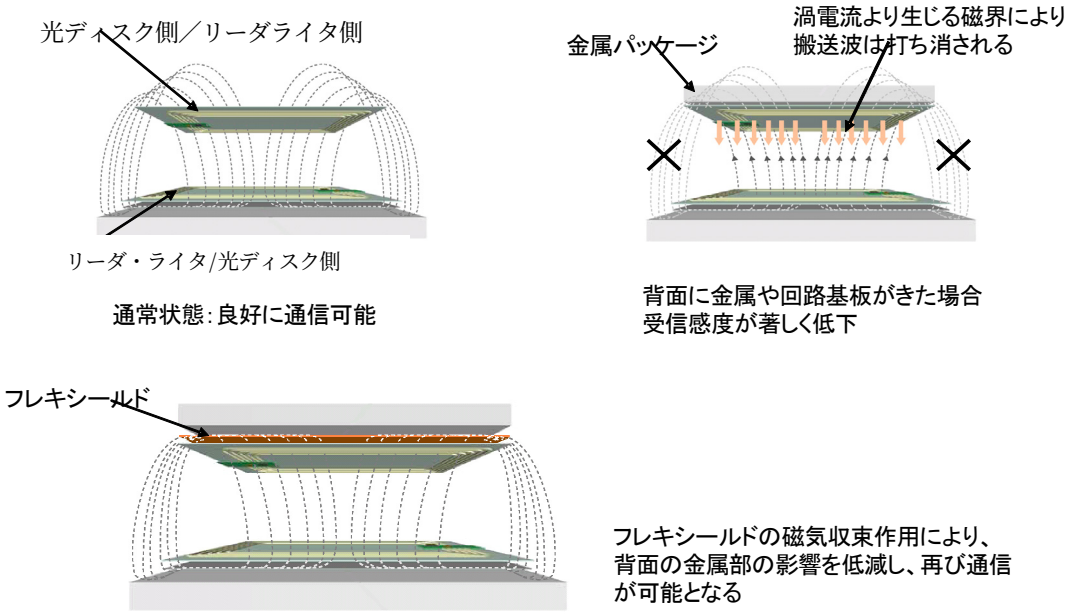


図 1.1.1-2　RFID におけるフレキシールドの効果

フレキシブル・フィルムのアンテナ部の裏面に磁性層（フレキシールド）を形成して、光記録面の、金属系材料の影響を低減し、信号の通信状態を改善することが考えられる。　上記金属系材料の影響を表した例が図 1.1.1-3 であり、磁性膜を裏面にもつアンテナの 100mm上方での磁界強度を、複素透磁率をパラメータにして解析したものである。このことから類推されるように、複素透磁率が小さく、初透磁率が高い磁性膜の方が磁界強度が高くなることがわかったので当初その方向で検討が行われた。しかし、光ディスクのアンテナの外径と記録面が垂直方向で 1.25mm、水平方向で 2mm離れていることと、光ディスクの記録面の金属が薄いこともあり渦電流損の影響が小さいことがわかった。

また、光ディスクのアンテナ外径は、リーダ･ライタ側のアンテナの内径と水平方向で 2.5mm、垂直方向 2.6mmしか離れていないので電磁的な結合性が強いことも確認した。

かかる検討の結果、光ディスク側アンテナの裏面に磁性膜を形成しなくても、リーダ･ライタへの書き込み・読み出しが可能であることを確かめ、磁性膜を削除できることがわかった。その結果、光ディスクのアンテナの厚みを 0.25mm薄くすることに成功した。

一方、光ディスクドライブのチャッキングプレートはマグネットを有するので、光ディスクが高速回転することによる交流磁界の影響が考えられる。しかし、搬送波（13.56MHz）に比べて低周波であるので、リーダ･ライタの通信への影響は無視できるものと考えられる。

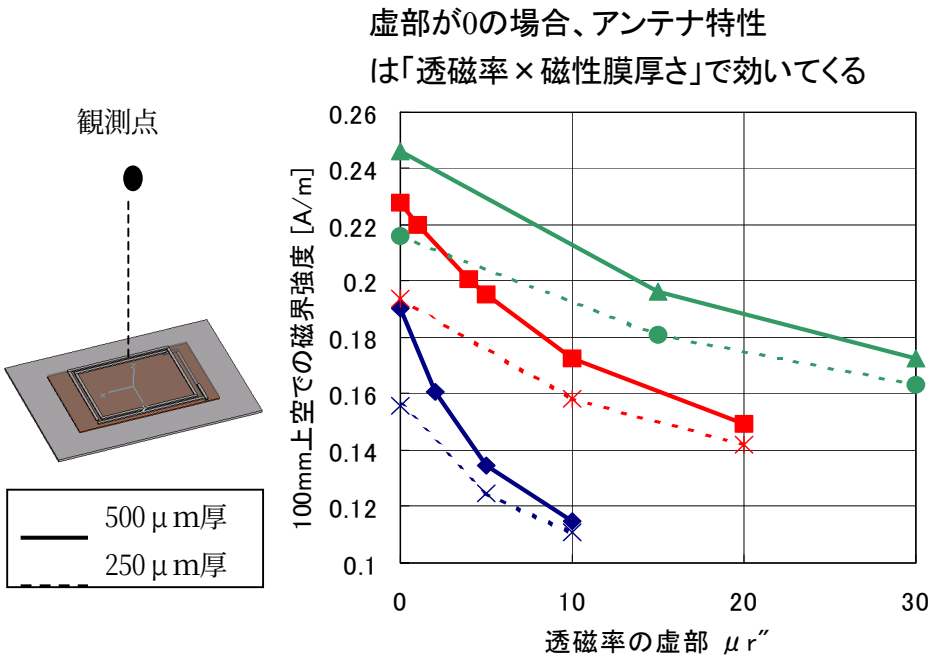


図 1.1.1−3 磁性膜を裏面にもつアンテナ上空での磁界強度

次に、高度暗号チップ搭載光ディスクの場合、アンテナは中空でなければならないが、図 1.1.1-4 に示すように、中空の面積を大きくすると磁界強度が低くなることがわかった。

しかし、リーダ・ライタ側のアンテナと Blu-ray ディスクのアンテナとは垂直方向で 2.6mm水平方向で 2.5mmしか離れていないので、磁界強度の低下が、それほど生じないという解析結果でもある。そこで Blu-ray ディスクでは、①リーダ・ライタ側のアンテナ形状がクランパーのためにサイズが決められているので、リーダ・ライタ側のアンテナ内径 35mmに近く②Blu-ray の金属膜の内径 36mmより狭く③クランパーの永久磁石の内径 13mmより広く④さらに中空の面積をより小さくということで、Blu-ray ディスク側のアンテナ構造は図 1.1.1-5 に示すように内径 25mm、外径 30mmを持つアンテナ形状にした。

また回転安定性のため、チップと対称位置にチップ重量と同等のバランサーを配置している。これにより回転安定性をもたせている。また、チップとバランサーの軸に左右対称に配置しているホールは、フレキシブル・フイルムを量産工程でハンドリングしやすいように糸を通すガイドのためのホールであり、左右対称に配置されている。

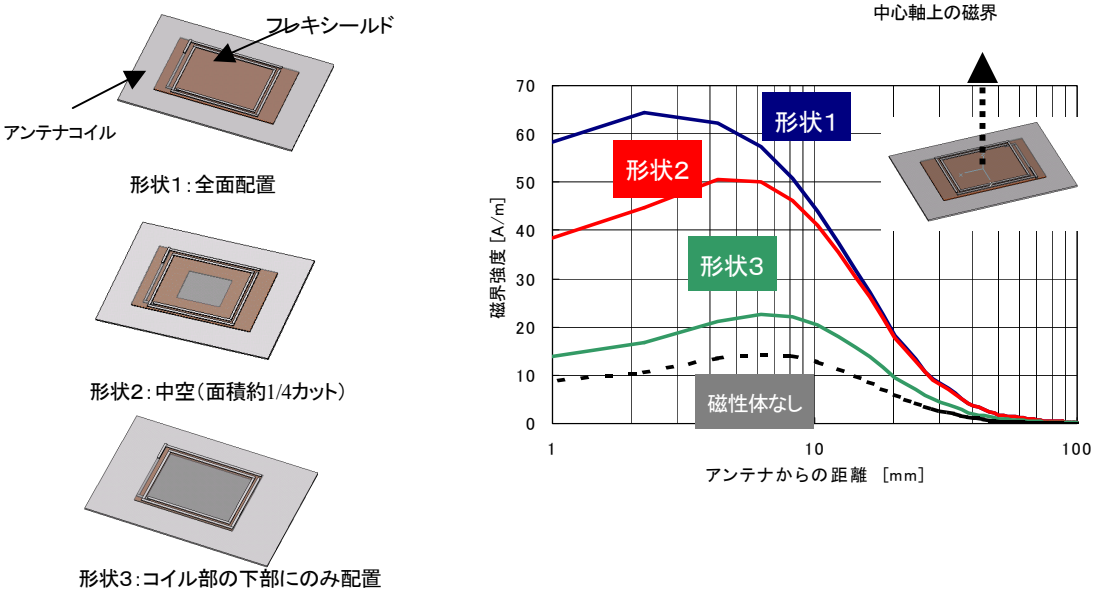


図1.1.1-4　磁性体の形状がアンテナ特性に与える影響について

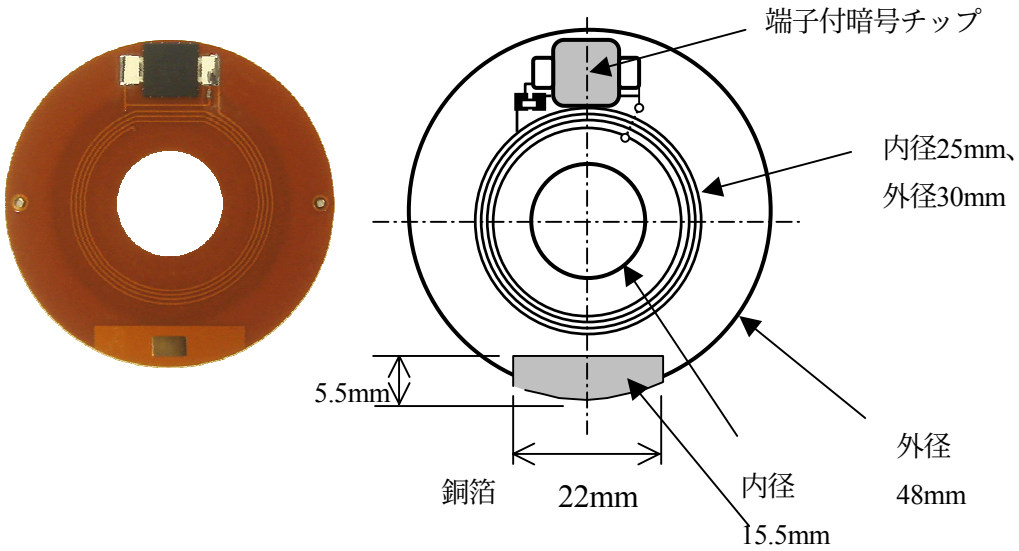


図 1.1.1-5 アンテナ形状

上記のような検討結果 Blu-ray ディスク側アンテナ構造を図 1.1.1-6 に示す構造にした。

①T 社 Blu-ray 高度暗号チップ搭載光ディスク

②P 社 Blu-ray 高度暗号チップ搭載光ディスク

図 1.1.1-6　Blu-ray ディスク側アンテナ構造

4 ターンアンテナと F 社製 IC チップ(32 ビット CPU、112KB－ROM、32KB－RAM、暗号系コプロセサー、5.5mm□)を電極モジュール 14mm×8mm□に搭載し、電極 2 端子をアンテナと半田付けする。さらに、専用治工具でフレキシブル・フイルムを光ディスクホールの中心と合わせて、光ディスクと両面接着テープで貼り付ける。

この構成にこだわったのは、デバイスドライバの関係から、当初 DVD-RAM しか利用できなかったものが、今回は Blu-ray 及び DVD+RW においても利用できることになったため、メディア間による互換性の向上並びに、運用上のコスト削減につながるので、この形状で開発を進めることにした。

（2）ディスク側のアンテナの電気的特性

実験では、ドライブを P 社製としたが、ディスクは P 社製と T 社製の Blu-ray ディスク５０GB リライタブルディスクを利用した。

Blu-ray ディスクでは、ディスク裏面に貼り付けたアンテナと記録膜は 1.35mmしか離れていないため、光ディスクの金属系記録膜及び、通信に影響するスピンドルモータからの電磁特性と、金属体による渦電流損、及びアンテナ間の相対的な位置関係などを総合的に実験・検討して、磁性膜の削除を可能にし、さらに、アンテナの内径及び外径の寸法も割り出した。

一方、光ディスクドライブのチャッキングプレートはマグネットを有するので、光ディスクが高速回転することによる交流磁界の影響が考えられる。しかし、搬送波（13.56MHz）に比べて低周波であるので、リーダ･ライタの通信への影響は無視できるものと考えられる。

さらに、アンテナの共振周波数を 13.56MH z に合わせるために、ループアンテナのターン数、フレキシブルフィルムによる静電容量、トリマコンデンサの容量などを実験で確認した。表 1.1.1-1 に共振周波数とアンテナ形状、トリマコンデンサ容量の関係を示している。

表 1.1.1 - 1　共振周波数とアンテナ形状、トリマコンデンサ容量

			C[pF]			f_0[MHz]		
径 (φ)	ターン	L[uH]	Chip のみ	Chip +トリマmin.	Chip +トリマmax.	Chip のみ	Chip +トリマmin.	Chip +トリマmax.
30	4	1.23	63.2	79.2（71.2）	153.2（108.2）	18.05	16.13（17.01）	11.59（13.80）
	5	1.93	63.2	79.2（71.2）	153.2（108.2）	14.41	12.87（13.58）	9.26（11.01）
	6	2.77	63.2	79.2（71.2）	153.2（108.2）	12.03	10.75（11.33）	7.73（9.19）
32	4	1.32	63.2	79.2（71.2）	153.2（108.2）	17.43	15.57（16.42）	11.19（13.32）
	5	2.06	63.2	79.2（71.2）	153.2（108.2）	13.95	12.46（13.14）	8.96（10.66）
	6	2.97	63.2	79.2（71.2）	153.2（108.2）	11.62	10.38（10.94）	7.46（8.88）

また、Blu-ray ディスクの金属面の構造及びスピンドルモータからの通信に影響する電磁特性と、金属体による渦電流損をアンテナとの相対的な位置関係を調整した構造にしていること並びに、ディスク側に貼り付けたアンテナと記録面が、垂直距離で 1.35mm、水平距離で 3mm離れていることから、磁性膜を削除したアンテナであってかつ、高速回転中であっても、暗号チップへの信号のリーダ・ライタからの書き込み･読出しができた。

1.2　ディスクドライブへのリーダ・ライタとアンテナの実装

1.2.1　Blu-ray ドライブへのアンテナ実装方式

（1）リーダ・ライタ側のアンテナ形状

従来のノートパソコンに搭載した薄型のドライブのアンテナは、フィルム上に、スパイラルに形成された 4 ターンアンテナとリードとで形成し、光ディスクドライブのホルダープレートの裏面に、磁性シートを介して貼り付けた。

図 1.2.1-1 に磁性シートをホルダープレート相当の金属の間にはさんだ場合の電界強度を示している。これによると、磁性シートがない場合極端に電界強度が低下することがわかる。

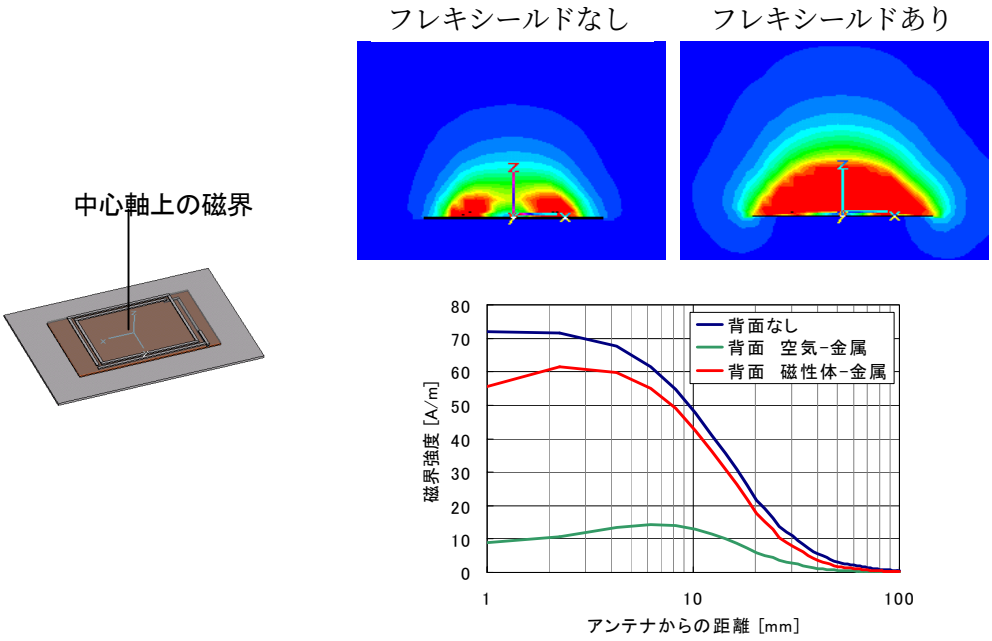


図 1.2.1-1　磁性シート有無による磁界強度

Blu-ray ドライブでは、Blu-ray ディスク側アンテナに対抗して、光ディスクドライブ上蓋ホルダープレートに中空のリーダ・ライタ側アンテナが貼り付けられている。

図 1.1.1-1 にリーダ・ライタ側アンテナ周辺の断面構造を示し、図 1.2.1-2 に平面構造を示すが、クランパーがあるために、アンテナを中空にしなければいけない。

これは、今まで解析してきた図 1.1.1-4 で示したように、①中空の場合電解強度が低下してしまうこと、また図 1.2.1-1 に示すように、②磁性体がなく金属が背面にある場合も電界強度が低下すること、がわかっているので厳しい条件になる。

Blu-ray ディスク側アンテナとリーダ・ライタ側アンテナとの距離を少なくし、できる限り磁気還流をスムースにするために、アンテナ周りの磁性シートの面積を大きくする必要がある。そこで、アンテナの内径を 34mm、外径を 38mmとし、磁性シートはクランパーの位置関係で内径 34mmにせざるを得ないが、外径はできるだけ広くすることが望ましいので、45mm（または 40mm）にし、ディスクの回転を安定させるために永久磁石が挿入されているクランパーの形状は、テーパーの深い部分で 29mmφとなっている。

また、ホルダープレートの開口部は、34mmφになっているので、リーダ・ライタ側アンテナの内径を 34mmφにし、Ｍ社製の、2007 年 11 月から市販されている Blu-ray ディスクドライブでは、クランパーを保持するホルダープレート形状が凹部になっているので、リーダ・ライタ側のアンテナの外径を 40mmφと小さくし、搭載した（図 1.2.1-3）。

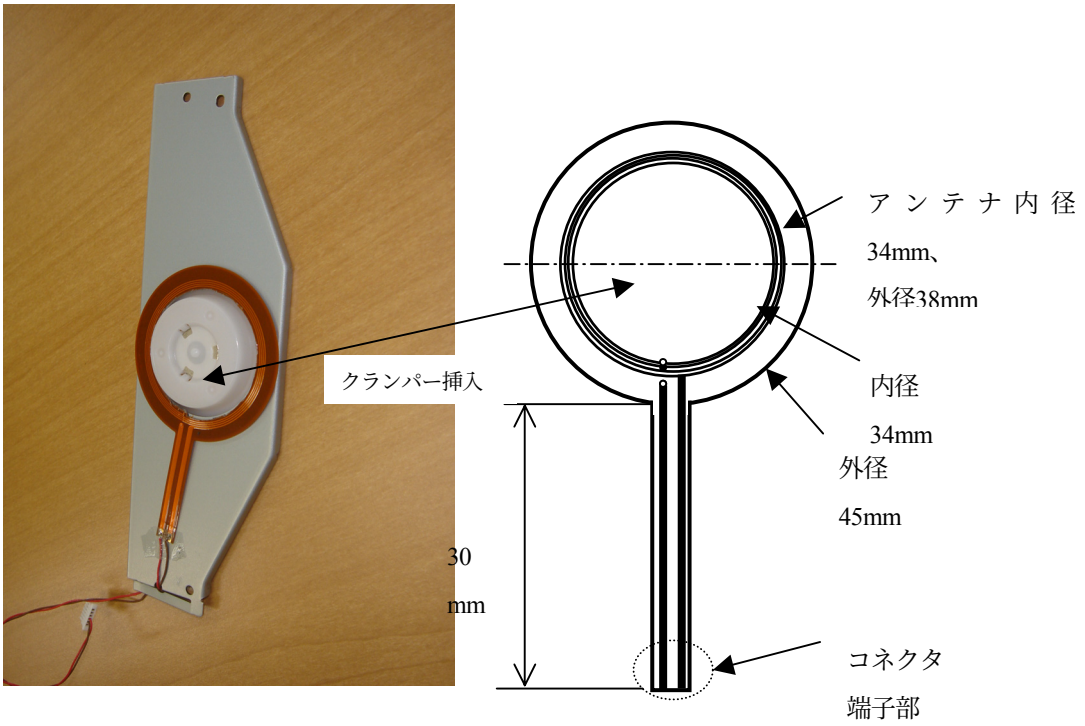


図 1.2.1-2　リーダ・ライタ側のアンテナ平面形状

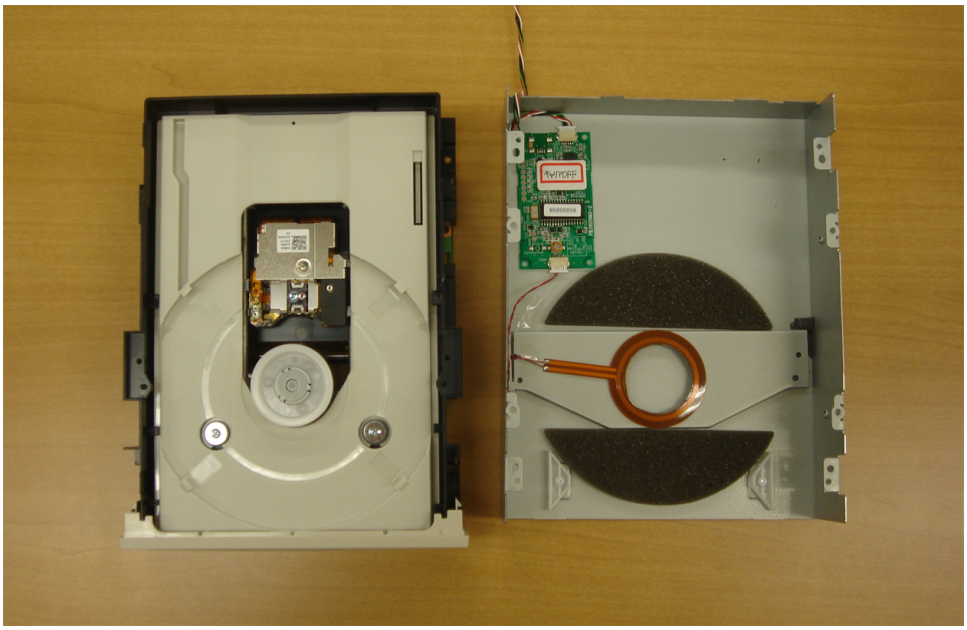


図 1.2.1-3　リーダ・ライタ側のアンテナを Blu-ray ドライブに搭載

（2）特性評価

光ディスクドライブのホルダープレートにリーダ・ライタ側のアンテナを貼り付ける場合、磁性シートをはさんで貼り付けることにより、電波漏れの軽減と輻射電波を吸収する機能が改

善される。

また、リード線を含む配線は長さや形状により浮遊容量が大きくなるのでリーダ・ライタ回路のトリマコンデンサを調整し、出力を最大になるようにすることで調整している。

図 1.2.1-4 に示すのは、永久磁石の入っているクランパーをリーダ・ライタ側のアンテナに挿入した場合のリーダ・ライタの出力特性である。

実験条件として､クランパーがない状態でリーダ･ライタ側からディスク側の暗号チップに、通信情報で変調された 13.56MHｚの搬送波信号を入力しておき、そのときのアンテナの信号レベルを、ワンターンコイルで検出し、数値をオシロスコープで計測しておく。

次にリーダ・ライタ側にクランパーを挿入した状態にして読み出し時の出力信号を検出したところ、クランパーの有無による差異は５%以下の小さい出力変動であった。

さらに、クランパーを挿入した状態でディスクを回転させながら、リーダ・ライタの高度暗号チップへのデータの書き込み・読み出し実験を行いクランパーがあってもデータの書き込み・読み出しができていることを確認した。

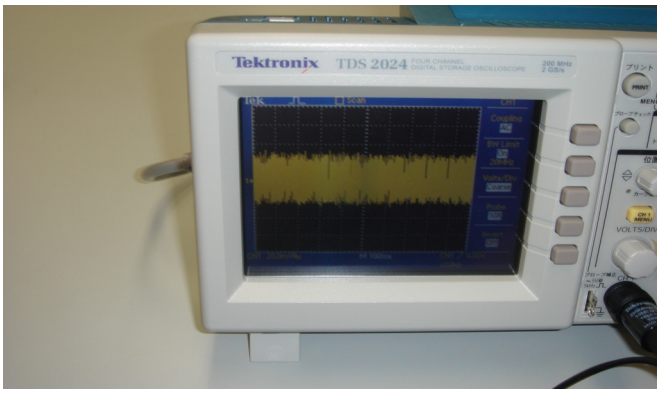


図 1.2.1-4　クランパー挿入時の R/W 信号

さらに、Blu-ray ディスクを今回試作した Blu-ray ディスクドライブに挿入し、Blu-ray ディスクが回転状態で高度暗号チップに書き込み・読み出しができていることを確認した。

当初、磁束が完全に還流できないのでないかと予想していたが、電磁的な面での問題が発生しなかった。この場合も暗号チップからの書き込み・読み出しができること、及び光記録面のデータを書き込み・読み出しができることを確認した。

上記のようにクランパー及びスピンドルの電磁的な効果については、影響が少ないことが判明したが、Blu-ray ディスクドライブは回転状態が不安定である場合、光記録面のデータを書き込み・読み出しができない状態になる。

例えば、クランパーがリーダ・ライタ側のアンテナに接触するようなことがあれば、光記録面のデータを書き込み･読み出しができない状態になることがあった。

そのため、リーダ・ライタ側のアンテナ内径を配線の内周ぎりぎりまで大きくして、クランパーとの接触を防いだ。

以上のように、Blu-ray ディスクドライブのリーダ・ライタ側のアンテナ構造を内周 34mmφ、外周 40mmφと小型化し、DVD-RAM 時に使っていたリーダ・ライタ側のアンテナ形状から大幅に変更したが、その場合も Blu-ray ディスクを今回試作した Blu-ray ディスクドライブに挿入し、Blu-ray ディスクが回転状態で高度暗号チップに書き込み・読み出しができていることを確認した。

また光記録面のデータを書き込み・読み出しができることを確認した。

1.2.2　高度暗号チップを搭載した Blu-ray ディスクでの書き込み･読み出し実験

（1）回転安定性に関して～ディスク側のアンテナ～

Blu-ray ディスクでは、従来の DVD-RAM や DVD-RW と比較して、構造及び記録密度に大きな違いがあり､上記で述べてきたように光記録面の書き込み･読出しでは回転を安定にすることが課題であった。

そこで、ディスク側のアンテナを貼り付けていない状態での、光ディスク記録面へのデータの書き込み・読み出し（2 倍速で 45GB のリライタブル領域への書き込み・読み出し）のチェック、風切音の発生（振動センサでの出力の確認）の有無を確認した上で、暗号チップなしでコイルのみが形成されているフィルムを専用治工具で貼付けデータ記録の書き込み・読み出しを行い、データ入出力ができることを確認した。

風切音の発生の許容値を振動センサを用いて判断した。

図 1.2.2-1 に振動センサによる測定回路を示している。

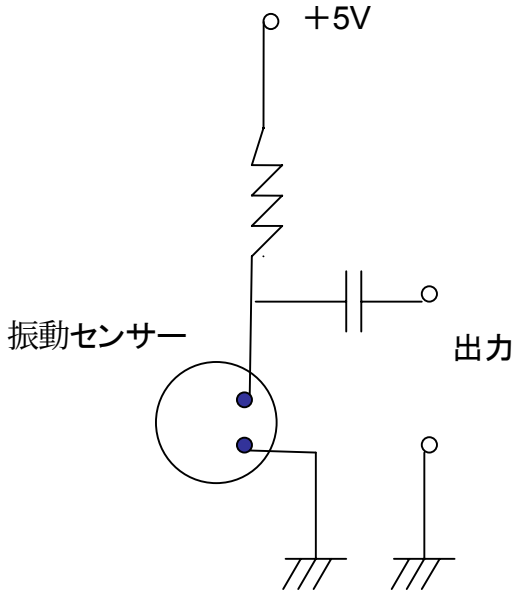


図 1.2.2-1　振動センサ回路図

また設置場所であるが、評価の場合はクランパーの近傍に振動センサを配置しているが、実機の場合は外側ケースのディスク回転の中心軸近傍で測定している。

2 つの評価においては検出される出力値は当然異なり、表 1.2.2-1 に示しているのは、クランパー近傍に音響センサを設置した場合である。サンプルとしては、光ディスクのチップを搭載型とチップ搭載しないもの及びチップ搭載を行っているが対称性が保持されていないあえて加重を付加するなどを行ったディスクで確認した。

また図 1.2.2-2 にベアの暗号チップをラミネートコートで埋め込んだ形のディスクを形成し、回転の安定性（ ◎ ）を確認した。

図 1.2.2-3 にディスクのアンテナを 35mmφとアンテナ部分だけを残して、5.5mm□のベアチップを搭載した場合、風きり音などが発生せず回転安定性（ ◎ ）が良いことがわかった。さらに図 1.1.1-4 には 1.0mm□の 8bit のベアチップを搭載した場合も、風きり音などが発生せず回転安定性（ ◎ ）が良いことがわかった。

表 1.2.2-1 にその結果をまとめている。

これらより、アンテナを含め重量バランスが対称的に配置されていて、かつ暗号チップが薄型であれば、回転安定性が良くなることがわかった。

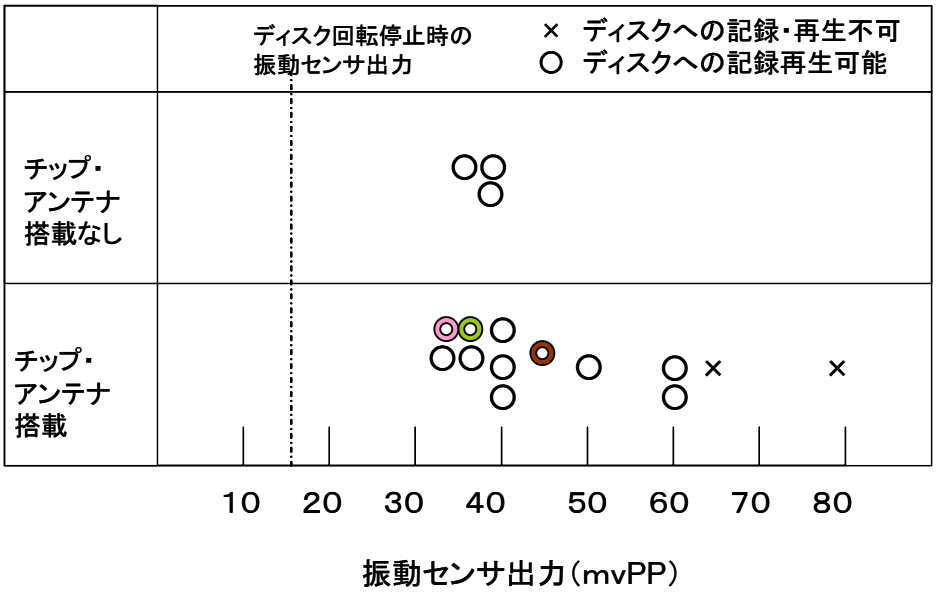


表 1.2.2-1 振動センサによる回転安定性の評価

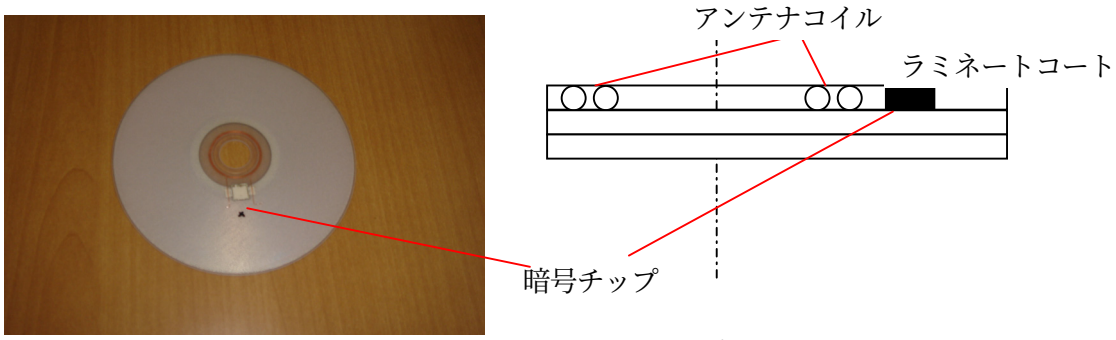


図 1.2.2-2　チップを埋め込んだディスク

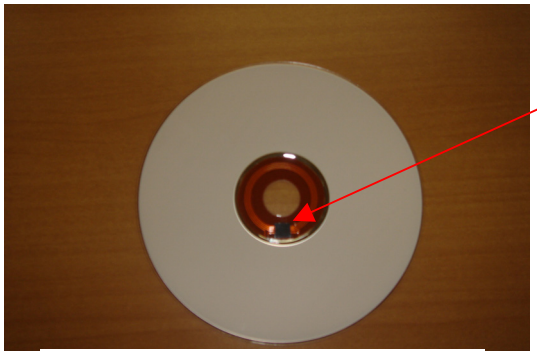


図 1.2.2-3　35㎜φのアンテナに
5.5mm□のベアチップを搭載

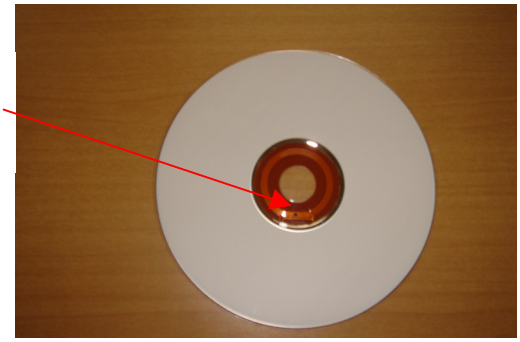


図 1.2.2-4　35㎜φのアンテナに
1mm□のベアチップを搭載

即ち回転不安定性が音響センサで検出することができるとすれば、この回路で６０ｍＶ超えると、回転が不安定であるので、そのときにディスクにデータを記録・再生ができなくなることがわかった。

このような実験結果から暗号チップアンテナコイルに搭載したフィルムを専用治工具で貼付けデータ記録の書き込み･読み出し（2 倍速で５０GB のリライタブル領域への書き込み･読み出し）を行ったところ、４５GB のリライタブル領域を持つデータ入出力ができること、振動センサの検出では、通常の工程を詳細に管理すれば専用治工具で作成されたアンテナを搭載したディスクもアンテナを搭載していないディスクと同等レベルにできることを確認した。

また、T 社製の Blu-ray ディスクはディスクのホール付近にテープが貼られているので音響を吸収しやすくなっていることがわかった。

ところでチップの軽量化ではベアチップをアンテナのリードにフエースボンディングする方法が技術的に確立していること、またオプションとして色々な形状を持つアンテナを形成した薄膜が、製造されていることを確認した。

これを製造しているメーカ数社に打診したところ技術的に問題がないことが指摘され技術的

な可能性は確認できた。

しかしコストが必要以上にかかることもわかった。

さらにアンテナフイルムの薄膜化に関しては、ディスク形成プロセス工程においてまずベアチップの製造を導入しない限り先行できないので、今後暗号チップにおいて、８bit 用の安価で量産向けのチップを搭載する際に、この確立した技術を使うことにした。

（２）回転安定性に関して～リーダ・ライタ側のアンテナ～

ところで、磁石が挿入されているクランパーとリーダ・ライタ側のアンテナはできる限りディスク側の内径の形状と相対的な位置関係にあるので内径を広げるわけに行かず、Blu-ray ドライブのクランパー径とほぼ同一の形状にならざるを得ないが、もし回転中にクランパーとアンテナが接触する構造であれば、Blu-ray の記録面への書き込み･読み出しができなくなることも確認している。

そこで、リーダ･ライタ側のアンテナの内径をホルダープレートの開口部の直径と同じ 34mmφと広くして、その接触による障害を防止した。

（３）Blu-ray ディスクでの書き込み･読み出し実験

当初、DVD-RAM で蓄積してきた技術では、Blu-ray のディスクへの書き込み･読み出しが難しいのでないかと考えていた。

しかし、専用治工具で製作しさらに振動センサなどであらかじめ不良品を除去するような工程を通せば、従来の技術を使えることがわかった。

即ち、通常の貼り付け工程で作成された Blu-ray ディスクに動画データ（１００MB)、静止画データ（１０MB）及びテキストデータ（１００KB）を書き込み･読み出しを何度も行い、2 倍速で 45GB のリライタブル領域への書き込み･読み出しができることを確認した。

図 1.2.2-5 は Blu-ray ディスクドライブをパソコンに接続し、書き込み･読み出しを行った写真である。　併せて、図 1.2.2-6 にパソコンに接続した Blu-ray ディスクドライブを接続したときのシステム構成である。Blu-ray ディスクドライブは機種によって異なる SATA（Serial ATA）または IDE でパソコンと接続している。

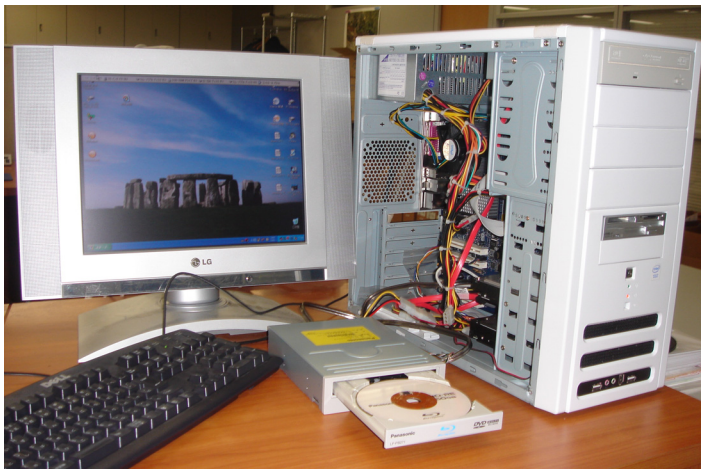


図 1.2.2-5　パソコンに接続した高度暗号チップ搭載 Blu-ray ディスクドライブ

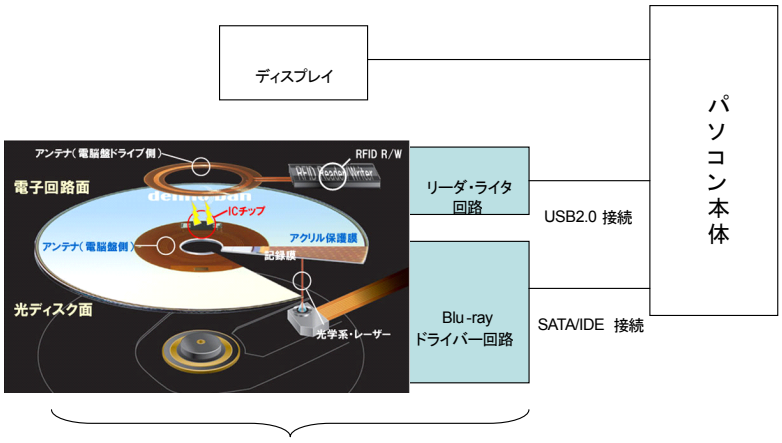


図 1.2.2-6 高度暗号チップ搭載 Blu-ray ディスクドライブとパソコンの接続系統図

1.2.3　リーダ・ライタ

Suica や Edy で利用されているリーダ・ライタは、非接触及びモバイル型であるカードとリーダ・ライタとの間隔を 10cm 位まで離しても無線入出力ができるようにするため、無線出力としてハイパワーが必要であることから大型になっていた。

また、リーダ･ライタを搭載した本体機自体が大型でもあることから、小型化にする必要性もなかった。しかし、薄型ノートパソコンや薄型光ディスクドライブに搭載するときには従来のような大型のリーダ･ライタを搭載することはできない。

一方、独自に開発した小型リーダ・ライタの場合、ディスク上に配置されたアンテナは高速回転しているものの、リーダ・ライタ側のアンテナとは、その相対的位置は 2.6mmと固定しており、大きな無線パワーを必要としない。

むしろ電波漏れなどを防ぐため低出力で実現できたほうがよい。

このような点から、小型のリーダ・ライタは以下の仕様を満足するように設計している。

①リーダ・ライタからの無線出力をできる限り低出力に抑えること。

②スピンドルモータからのノイズに対しても影響を受けにくくすること。

③スリムタイプの光ディスクドライブにも搭載できるようにするため、できるだけ薄くコンパクトにすること。

④汎用性を確保するために、USB 駆動ができること。

⑤専用機であるため不必要な機能を削除し、部品点数を極力削減すること。

できれば、光ディスクドライブの回路と一体成型をすることにより、工数の削減と部品点数の削減を図りたい。

⑥光ディスク記録面での書き込み･読み出し時に、リーダ・ライタからの信号によって影響

を受けないようにする。

１.2.3.1 構成

独自開発したリーダ･ライタは RF 部、CPU 部、USB からできており、RF 部から 4 ターンコイルのリーダ･ライタ側アンテナに接続している。

USB 部からはパソコンの USB2.0 端子と接続できるようにしており、光ディスクドライブの回路とは独立に形成されている。

さらに、35mm（W）×70mm（D）×4.5mm（H）と薄型構造を持ち、リーダ･ライタ側アンテナと接続してノート型パソコンに組み込むことができる。

また、USB 端子で接続するので、通常のパソコンにも容易に接続できる。

電気的特性は ISO14443TYPE-B に準拠し、搬送周波数は 13.56MHz である。

1.2.3.2 電気的特性評価とソフト評価

（1）リーダ・ライタ側のトリマコンデンサの調整

高度暗号チップを搭載した Blu-ray ディスクのアンテナとトリマコンデンサの設定は、量産工程で設定して出荷しているので、変更できない。

そこで、リーダ・ライタ側のトリマコンデンサを微調整して、搬送波 13.56MHz に調整している。

調整方法は、リーダ･ライタからディスクの暗号チップに書き込み･読み出し信号を連続的に出力し､リーダ･ライタ側のアンテナとリーダ･ライタの接続部にワンターンコイルを挿入して、トリマコンデンサを調整しながら、オシロスコープでその最大出力を測定する。

送信電力は 47.544mV/m（10m にて）以下になっているので、従来のリーダ･ライタに比べて低く抑えられており、また、設置場所も、Blu-ray ディスクドライブのホルダープレートとフレームの金属板の中に挿入されているので、スピンドルモータからのノイズの影響は少なくなっている。

しかし、リーダ･ライタを通常 ON にしておくと、時々光ディスクドライブの書き込み・読み出し動作に影響が出ることがわかったので、通常は OFF にして、リーダ･ライタから暗号チップに書き込み・読み出し時だけ ON にするようにファームの書き換えを行った。

また、USB 接続でパソコン側と接続されているので、汎用性のある構成にしている。

（2）ドライバソフト

リーダ・ライタのドライバ機能を提供する Windows 版ライブラリ及び Linux 版ライブラリの仕様概要を以下に示す。

(a) Windows 対応

リーダ・ライタのドライバ機能を提供するWindows版ライブラリは、表1.2.3.2-1Windows対応ドライバソフトに示すような内容で構成されている。

表 1.2.3.2-1Windows 対応ドライバソフトのリスト

＜実行環境＞
Windows 2000 及び Windows XP FTDI 社製 Virtual COM Port ドライバ
＜ファイル形式＞
Windows ダイナミックリンクライブラリ ライブラリのファイル名：dennouban.dll ソースファイルの構成： libdennouban.c ライブラリ本体 dennouban.h　API 関数のインタフェース記述 demo.c　　サンプルプログラム

⑹　Linux 対応

新型リーダ･ライタのドライバ機能を提供する Linux 版ライブラリは、表 1.2.3.2-２Linux 対応ドライバソフトのリストに示すような内容で構成されている。

表 1.2.3.2-２　Linux 対応ドライバソフトのリスト

＜実行環境＞	
Fedora Core 5 i386 版 FTDI 社製 Virtual COM Port ドライバ	
＜ファイル形式＞	
Linux 共有ライブラリ ライブラリのファイル名：libdennouban.so ソースファイルの構成：	
libdennouban.c	ライブラリのソース
dennouban.h	インタフェース記述
demo.c	サンプルプログラムのソース
Makefile	GNU make 用の Makefile

（3）ファームウエア

新型リーダ・ライタでは、ISO14443 Reader IC である MF RC531（以下 RC531 と称す）を制御し暗号チップ搭載ディスクとのやりとりを行っている。

表 1.2.3.2-3、表 1.2.3.2-4 にファームウエアの仕様で示すような開発環境で開発し、また制御ファーム仕様を示している。

表1.2.3.2-3 ファームウエアの仕様（開発環境）

＜開発環境＞
Windows 2000、ＸＰの動作するパソコン（IBM-PC/AT 互換機） ・Renesas 統合開発環境（High-Performance Embedded Workshop） ・Renesas コンパイラ・パッケージ（アセンブラ・リンカ含む） ・E8 エミュレータ及び付属開発ツール ・その他、Windows で動作する各種アプリケーション （汎用エディタや検索ツールなど） ・CPU はルネサス R8C/10 グループ、R5F21104FP プロセッサを使用。 ・システムクロック 16Mhz ・ROM は内蔵 16KB ・RAM は内蔵の 1KB

表1.2.3.2-4 ファームウエアの仕様（制御ファーム仕様）

＜制御ファーム仕様＞
１）CPU　　：R5F21104FP（ルネサス）
２）リーダ IC　　：MF RC531（フィリップス）
３）通信制御　　：ISO14443B のコマンド制御 ：ISO14443B の通信プロトコル制御
４）MF RC531 レジスタ制御 ：送信出力制御 ：送信変調制御 ：受信アンプゲイン制御 ：テストシグナル制御
５）上位との通信制御　　：USB によるシリアル通信 （USB 用 IC　FT232RQ を使用）

（４）高度暗号チップチップへの書き込み・読み出し

パソコンとリーダ･ライタとを USB で接続し、暗号チップのシリアル No.（これは一度書き込むと消去できない）とユーザ情報、バージョン情報、機器や個人の属性情報、を高度暗号チップにリーダ・ライタから書き込み・読み出しできることを確認している。

また高速回転する高度暗号チップ搭載の Blu-ray ディスクでも、同一の情報を書き込み・読み出しできることを確認している。

（５）　信頼性評価試験

新型リーダ・ライタの信頼性評価を恒温恒湿槽内で保持した状態で確認する。

＜試験概要＞

恒温恒湿槽内に暗号チップ内蔵ディスクシステム一式を入庫し、各検査 PC 間を USB 延長ケーブルで接続して恒温恒湿槽内の温度を 0℃～50℃まで設定しながら動作確認用プログラムの実行と結果に問題がないことを確認する。

1.2.3.4　光ディスクドライブと一体型になったリーダ･ライタ

前述した仕様で作成されたものが今回の Blu-ray ディスクドライブに搭載されているが、DVD-RAM ドライブではさらに、ドライブ回路と一体形成した図 1.2.3.4-1 に示す構造を持つリーダ・ライタを設計した。

光ディスクドライブの回路のベースになっているのはTEAC社製のDV-W28PU-A40である。

光ディスクドライブとリーダ･ライタは､ＵＳＢでパソコンのＵＳＢ端子に接続されている。

この開発により以下の内容が実現できた。

① 配線などの長さが固定化されたこと、設置場所が固定化されたことによりアンテナの浮遊容量のバラつきが少なくなり、調整用トリマコンデンサの調整が容易になった。

② 光ディスクドライブと一体形成にしたことにより部品点数の削減と工数の削減が図られたことにより量産化のめどがついた(図 1.2.3.4-2)。

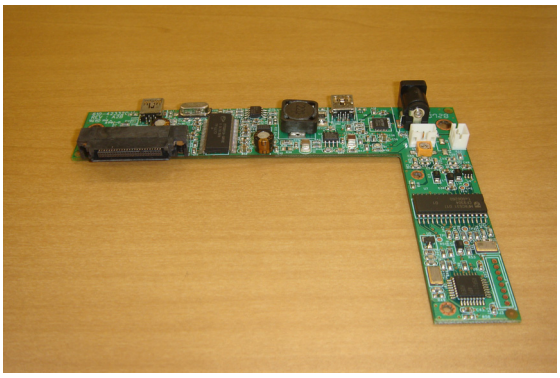


図 1.2.3.4-1　光ディスクドライブ回路と一体化形成されたリーダ･ライタ

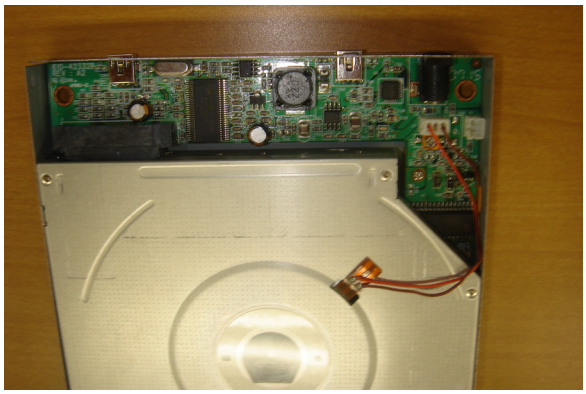


図 1.2.3.4-2　光ディスクドライブ回路と一体型リーダ・ライタのドライブへの搭載

1.2.4　指紋認証装置の搭載

指紋認証は､世界の１人１人が異なる指紋を持つことから､従来犯罪捜査に利用されてきた。

グローバル経済では、企業や政府が電子的な取引や情報システムに頼らなければならない状況になったことから、銀行や企業などのセキュリティを必要とする分野から導入されている。

現在では、軽量小型化された装置で指紋を認証することができるので、パソコンの個人認証用ツールの一つとして搭載されるようになった。

（１）ハード構成

図 1.2.4-1 に S 社製の指紋認証装置の外観を示している。また、表 1.2.4-1 に指紋認証装置の仕様を示している。初回に、特異点抽出法により検出されたデータを通常はパソコンのハード

ディスクのファイルの中に保存しておき、次回の指紋認証時前述のデータと照合することにより、個人認証を行っている。

しかし、高度暗号チップ搭載光ディスクシステムでは、光ディスクと高度暗号チップがハードディスクの役割を担うので、指紋認証用データ約１００KB を光ディスク側に保存し、パスワードなどは高度暗号チップに暗号化して保存している。

そこで、パスワードが入力されると暗号チップが照合し、次に光ディスクの指紋認証データと入力された指紋認証データとが照合されて、合致すれば情報データを書き込み・読み出しができる仕組みになっている。

これは、光ディスクの大容量性を利用しているのと高度暗号チップのセキュリティ性を利用している。

図 1.2.4-1 指紋認証装置の概観

表 1.2.4-1 指紋認証装置の仕様

インタフェース		USB 1.1
外形寸法		25.3(W)×67.7(H)×40.7(D)mm
質量		103g
供給電圧		DC5V±5%
センサ	**読取技術**	SEIR(表面突起不規則反射方式による光学式)
	読取領域	13×15mm
照合	**解像度**	500dpi±0.2%
	照合方式	特異点抽出法
	時間	1 秒以内

（２） 指紋認証装置のソフトウェア

最大 10 人のユーザをエントリでき、高度で正確な指紋認証システムを構築する。

また、当社のような高度暗号チップ搭載の光ディスクドライブのように、リーダ･ライタから暗号チップを介して暗号コードを書き込み･読み出しするようなカスタム化を図ることもできる。128 ビットの暗号化アルゴリズムでフォルダ単位の暗号化する機能を持っているので、指

紋認証を行えば暗号化されたフォルダへのアクセス、データの層ができる。また、リムーバルディスクのフォルダの暗号化も可能になる。

例えば、暗号化した指紋があれば会社で暗号化した光ディスクドライブを自宅で復号することも可能である。

指紋の暗号化された情報をパスワードごとで判定しているので、パスワードに 10 人の指の指紋を登録しておけば、最大 10 人までの光ディスク上の暗号フォルダを共有できる。

また、登録されたユーザの情報（ユーザ ID、ドメイン名、指紋情報など）を光ディスクドライブに保存し、指紋認証装置の再インストール時にそのバックアップデータを復元することができる。

また、データのバックアップや復元時には必ず管理者の指紋認証が必要になるので、セキュリティは保護される。

図 1.2.4-2 に指紋認証の画面を表示している。使用者の名前またはパスワードを入力後、次に指定すべき指を決めて後、指紋認証装置に指定した指の 1 本の指をかざして、4 回指紋を認証させデータを光ディスクに保存する。

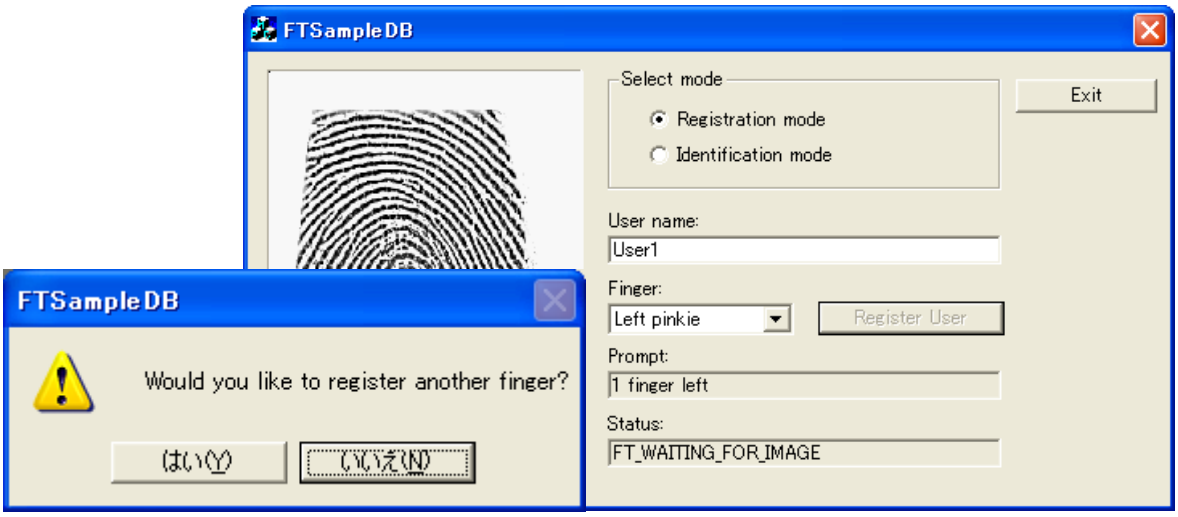


図 1.2.4-2 指紋認証の画面

指紋認証装置は USB でパソコンに接続し、解像度５００dpi の表面突起不規則反射方式による光学方式で、指紋データを入力する。それを、特異点抽出法でデータを作成する。

暗号チップには、使用者名またはパスワードを書き込み、また特異点抽出法で作成されたデータは光ディスクに保存する仕組みにしている。

この時点でディスク保管者と指紋の個人データとが結合されることになる。

次に個人認証をこの光ディスクを用いて行う場合、使用者名またはパスワードと指紋認証装置からの特異点抽出データと登録されたデータとを比較参照して、合致していれば、光ディスクの情報データにアクセスできるようになる。

合致していない場合は、再度指紋認証を行うことが必要である。

（3）利用形態

企業や官庁で指紋認証をセンタサーバで管理することが通常行われている。

しかし内部犯行などでその指紋認証データが盗難された場合、指紋は個人にとって一生変更できない性質のデータであるので、この問題は現在社会問題になっていないが、大きな課題になることが予想される。センタサーバに指紋情報がたとえ高度に暗号化されて入っていても、それが将来も解読できないと言うことはいえないからである。

基本的には個人データ特に生体情報など、一生涯変更できないデータは個人が管理・保管しておくことが大切であると考えられる。

当社の開発したシステムでは、光ディスクや暗号チップに個人のデータを保存し、それを物理的に個人が管理することを基本にしている。

指紋認証の場合、指紋認証の一部データを暗号チップに、それ以外を光ディスク側に保存している。これから個人情報の保護と言うことが言われる現状をみると、この考え方が今後浸透していくものと考えられる。

1.3 光ディスクの ROM・RAM 構造化方式の改良

従来、いわゆる PC/AT 互換仕様の PC においては、光ディスクドライブが認識されると、そのドライブのドライブレター（ドライブ C,D,E……など）は、当該ドライブに装着された光ディスク上の論理パーティションに対してでなく、当該ドライブそのものに対して唯一つアサインされる仕様となっている。

このことと、光ディスクからオペレーティングシステムを起動する場合、CD-ROM 用をルーツとして策定され各種仕様拡張がなされた読み出し専用の ISO-9660 ファイルシステムが通常使用されること、との２つの理由により、起動可能なオペレーティングシステムを有する光ディスクは全面が当然読み出し専用(ROM)となり、データの書き込みができる RAM パーティションは持つことができないというのが常識とされてきた。

高度暗号チップ搭載光ディスクの用途を考えると上記の制約は不都合であるので、この制約を破る検討を行った結果、平成１８年度に一枚の DVD-RAM メディア上の最大４GB の範囲に Linux OS とアプリケーションプログラムを格納した ROM 部と、仮想ファイルシステムを利用したユーザデータ保管用の RAM 部を並存させることに成功した。

本年度は、さらに大容量の光ディスクである Blu-ray ディスク上に同様の ROM 部と RAM 部を実現する方法の検討を行い、幾つかの方法案の考察と、比較的実験しやすい ISO-9660 ファイルシステムの延長上の一方式につき実験を行った。

その結果、ISO-9660 ファイルシステムの延長上でも、Linux カーネルに少しの修正を加えれば、Blu-ray メディア上に、従来の４GB の枠を超えて所要の構造を実現できる見通しを得た。

しかし、ディスクの生産性も考慮すると、数十ギガバイトを超えるような容量を有する光ディスク媒体においては、生産時に大量データを一括書き込みする様な一括的プレマスタリング

の方法でなく、データが追加されるたびに必要分だけ光ディスク面を初期化してゆくタイプの方式の方が適しており、これについてはさらに開発を進める必要があることがわかった。

1.3.1 ROM・RAM 構造化の従来方式

PC/AT 互換仕様の PC において光ディスクからオペレーティングシステムを起動する場合、ISO-9660 ファイルフォーマットが使用される理由は、オペレーティングシステム起動中の大量のファイルアクセスを、最小限のファイル検索時間で実現するのに ISO-9660 は特に適した読み取り専用のファイルシステムだからである。

よって、本検討においても、基本システムは ISO-9660 を用いる起動時の機能性は温存しつつ、起動後は ISO-9660 ファイルシステムに内包させた、仮想ファイルシステムを、ISO-9660 の特殊性とは関係なく、任意のファイルシステムとして普通にアクセスできるように工夫した点が画期的であった。

1.3.2 ROM・RAM 構造化方式の改良

上オペレーティングシステムの起動の為には ISO-9660 ファイルシステムを使用するメリットは極めて大きいので、従来方式の長所を温存しつつ、従来方式で上限とされてきた４GB のファイルサイズ制限を越えるには、またその場合、ISO-9660 そのものや Linux OS 自体の仕様外にはなるが、Linux OS としてどんな振る舞いを示し、どんな制約が生じるか、の検討を行ってみた。

1.3.2.1 超 ISO-9660 Blu-ray ディスクの試作

ベースとして使用した Linux ディストリビューションは、slax と ubuntu を検討し、実験にはツールの充実度の点で ubuntu を選んだ。

1.3.2.2 試作した超 IISO-9660 Blu-ray ディスクからの Linux OS の起動実験

ISO-9660 の El Torito Extention は正常に機能し、Linux (ubuntu-ja-6.10)は約２分３０秒で正常に起動した。 基本機能に特に異常は認められなかった。

1.3.2.3 試作超 ISO-9660 Blu-ray ディスク上の 4GB 超部分からのデータ読み取り実験

約 6.8GB の超 ISO-9660 イメージを Blu-ray ディスク上に作り、このイメージを外部 USB メモリにコピーする実験を行った結果、データは正常にアクセスされ、正常にコピーできることを確認した。

1.3.2.4 試作 Blu-ray ディスク上の ４GB 超部分へのデータ書き込み実験

実験の結果、今回使用した ubuntu-ja-6.10 Linux の、オフセット値を指定するタイプのマウントコマンドは、４GB 超部分に対し、正常に動作しない事象が認められた。

原因を調査の結果、Linux カーネルのマウントコマンドを中心に簡単な修正を行うことで解決できる可能性が高いことがわかった。　この点は引き続き確認する。

1.3.2.5　本方式の問題点

この検討により ISO-9660 に内包した仮想化ファイルシステムでも４GB 超のデータを扱える見通しが付いたが、この方法では、例えば２５ギガバイトの Blu-ray ディスクの場合、２時間程度の書き込み時間が掛かることとなり、量産性に問題がある。

1.3.3　他方式の考察

ここまでの検討を鑑み、更なる改良方式を考察した。

1.3.3.1　ISO-9660 ファイルシステムのインクリメンタルライト

前 1.3.2 では ISO-9660 ファイルシステムに一気に３GB のボリュームを増築したが、これをもっと小分けにして、例えば数メガバイト以下の単位に分けて分割追加方式でマウントし、それらのファイルを一元アクセスする方法が考えられる。

この方式の実現の為にも前記 1.3.2.3 のマウントコマンドの修正は必須である。

1.3.3.2　ISO-9660 → UDF2.X ブリッジ式

OS の起動のみを ISO-9660 で行い、起動後、ファイルシステムを UDF2.X にブリッジする。開発規模が大きいが、将来的にはこの方式が有望と考えられる。

UDF2.X に切り替え後、マウント・レイニアストラテジーを採用、データ追加にしたがってバックグランドフォーマッティングを行うというものである。

1.3.4　物理的パーシャル ROM 化の検討

①物理的パーシャル ROM とは：

記録可能な光ディスクなどで、書込可能な領域（RAM 領域）以外の、書き込みできない読出専用の領域（ROM 領域）を、ディスク基板の成型時にスタンパーからの転写で作成する方法を物理的パーシャル ROM と定義する。

デュプリケーションにより ROM 領域を書き込み、論理的に再書き込みや消去を禁止する方法に比べて、生産性が桁違いに良いことと ROM 領域に収録したＯＳやアプリケーションソフトなどが、ハッカーやコンピュータウイルスなどにより、不正に書換えられるリスクを回避できると言うメリットがある。

但し、物理的パーシャル ROM を実現するためには専用のスタンパーの開発を含め、本格的な技術開発が必要となる。

②物理的パーシャル ROM の技術開発：

物理的パーシャル ROM の基本技術は既に開発されており、１９９１年７月に、リコーが物理的パーシャル CD-R の技術開発に成功。

１９９２年に三菱化成（現、三菱化学）が世界で初めて光磁気ディスク（MO）を用いて物理的パーシャル ROM ディスクを、「HYBRID MO」の名前で商品化した。

富士通も１９９２年に物理的パーシャル ROM 光磁気ディスクを発表している。

また、２００５年にはリコーが、物理的パーシャル ROM の構造を持つ CD-R を「ハイブリッド CD-R」として商品化し、「インテリジェント CD-R ディスク」と命名した。

③OS 内蔵型パーシャル ROM 開発の課題と今後の見通し：

パソコンの主流である PC/AT 機は、光ディスクドライブをマウントする際に一個のパーティションしか認めていない。

しかも､光ディスクから OS を高速起動する為には ISO9660 フォーマットを用いることになるが､その場合､DVD-RAM のような書き換え可能型（RAM）光ディスクを用いても ISO9660 フォーマット処理後はすべて読み出し専用（ROM）としてマウントされるので、OS の高速起動が可能な形式で且つパーシャル ROM 構造を持つ光ディスクは実現できなかった。

一方、本報告書第１章の３．で詳述したとおり、DVD-RAM に VFS(Virtual File System) を encapsulate することにより､OS や基本アプリケーションを ISO9660 フォーマットで記録済みの光ディスクに、論理的に RAM 領域を形成することに成功している。

現在は、デュプリケーションの手法を用いてこのプロセスを形成しているが、同じプロセスをスタンピングにより形成すれば量産性が飛躍的に高まりコストダウンにつながると思われる。

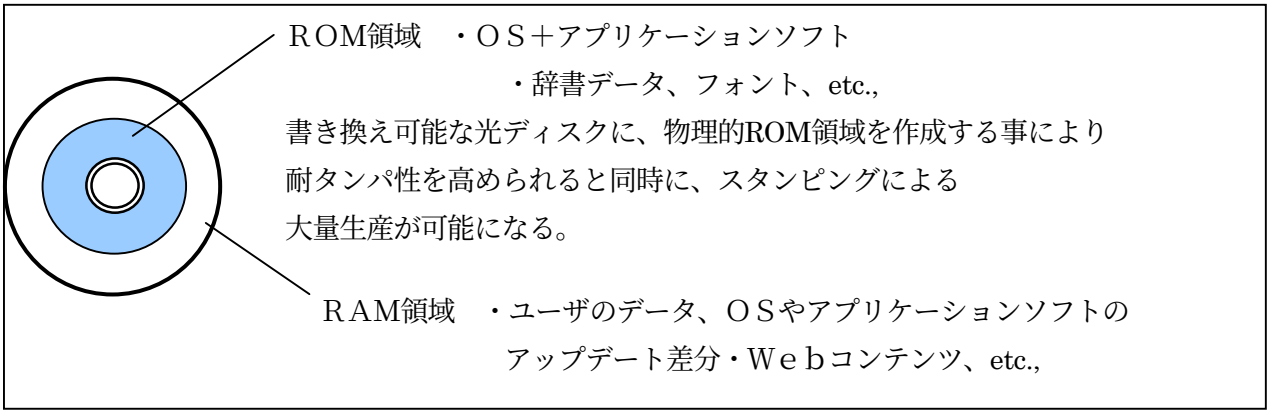


図　1.3.3-1　物理的パーシャルROMディスクの構造

1.4　暗号チップの最適化の検討

暗号のシステムを構成する場合、ハード的な対応とソフト的な対応の役割分担を明確にしたうえで、セキュリティ効果を有効に活用しなければならない。

高度暗号チップ搭載光ディスクシステムでは暗号を構築する部分は､パソコン側､リーダ・ライタ側、高度暗号チップ搭載光ディスクの暗号チップそして光ディスクの記録面と４箇所が考えられさらにオプションとして RTC や指紋認証が付属できるので多重のセキュリティシステムが構成される。

ここでは、高度暗号チップを搭載した DVD-RAM ディスクで行った検討内容を示す。

1.4.1 暗号チップのセキュリティレベル

パソコン側のセキュリティレベルは、Windows の場合と Linux とでは大きく違っており、Linux の方がオープンソースゆえに開発者としてハンドリングがし易くかつセキュリティへの対応が迅速にできる。

リーダ・ライタ側には、８ビットマイコンが搭載されており、ここでリーダ・ライタを含めた光ディスクドライブを認証することが可能である。

高度暗号チップ搭載光ディスクに搭載されている高度暗号チップは、X 線などの放射線に強い FRAM で形成されており EPROM に比較して化学的な処方でもその記録内容を解読できない耐タンパ性を有している。また暗号系も RSA（256bit、512bit、1024bit 対応）や T-DES も搭載されている。

従って、通常の方法では書込まれている内容をコピーすることはできない。

光ディスクの記録面では、高度暗号チップの暗号コードを利用したコードで情報のデータを暗号化している、また指紋認証などの容量が大きいデータの一部を高度暗号チップと分担して記録している。表 1.4.1-1 に暗号に関る部分と特徴と機能を示している。

表 1.4.1-1 暗号化に関する部分の特徴と役割分担

	特徴	利用方法
高度暗号チップ	CPU 32bit メモリ 32KB	責任者名、ユーザ名、パスフレーズ 期間限定、開始日、終了日、指紋認証のユーザ名
リーダ・ライタ	CPU 8bit メモリ 1 KB	光ディスク装置の認証
光ディスク (DVD-RAM/ Blu-ray)	メモリ 4.7GB/50GB	指紋認証抽出データ、 暗号化された情報データ
パソコン （ハードディスク）	CPU 32bit D-RAM ～1GB HDD 数百GB	情報データの暗号化・復号処理、 指紋認証データの一時保管

1.4.2　暗号チップと光ディスクに書込まれたデータの暗号化の分担

（1）Windows に暗号システムを搭載した場合

表 1.4.2-1 に Windows で構成された高度暗号チップに書込まれた内容を示す。

事務所内で高度暗号チップ搭載光ディスクシステムを責任者と複数のクライアントが、利用する場合を想定して、その機能を紹介する。責任者が、情報データを入力し、それは責任者と１クライアントしか読み出しできないようになっている。

責任者は自身のパスワードで情報データを読み込みできるが、クライアントは責任者があらかじめ設定した Pass phrase の入力 や使用回数の制限、使用開始の日時、終了の日時、そして責任者の面前で行ったクライアント自身の指紋認証の制約を受ける。即ち、この光ディスクの利用では責任者はパスワード及びパスフレーズだけでデータ読み出しができる。

次にクライアント側が情報データを読込む際、前述の様々な制約条件が加わることになる。これらの一連の入力画面を図 1.4.2-1～図 1.4.2-3 までに示している。

表 1.4.2-1　高度暗号チップに書込まれているデータ

チップ内容	備考
データフラグ	チップの内容を読む時、このフラグをチェックする。
責任者名	初期化の時設定した責任者の名前
責任者のパスワード	初期化の時設定した責任者のパスワード
Passphrase	初期化の時設定した責任者のPassphrase
使用回数	使用者の使用可能回数
開始日付	使用者の使用開始日付
終了日付	使用者の使用終了日付
指紋ファイル名	指紋ファイルの名前
指紋認証フラグ	指紋認証必要性の確認。

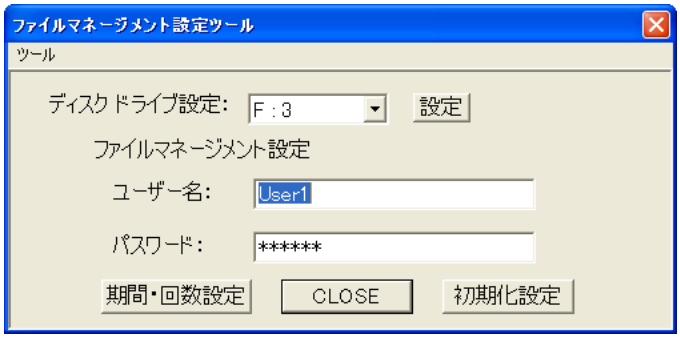


図 1.4.2-1　ファイルマネージメント設定画面

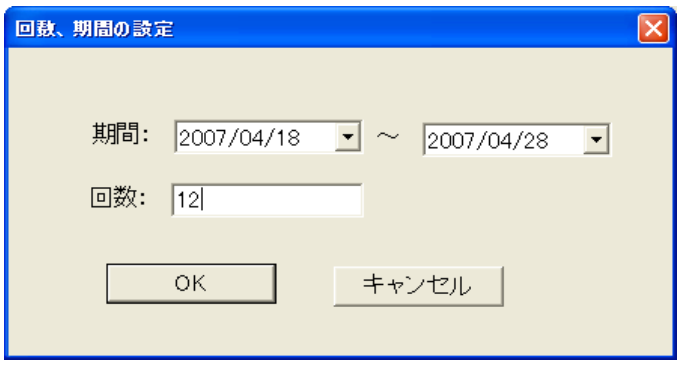


図 1.4.2-2 期間限定、利用回数設定画面

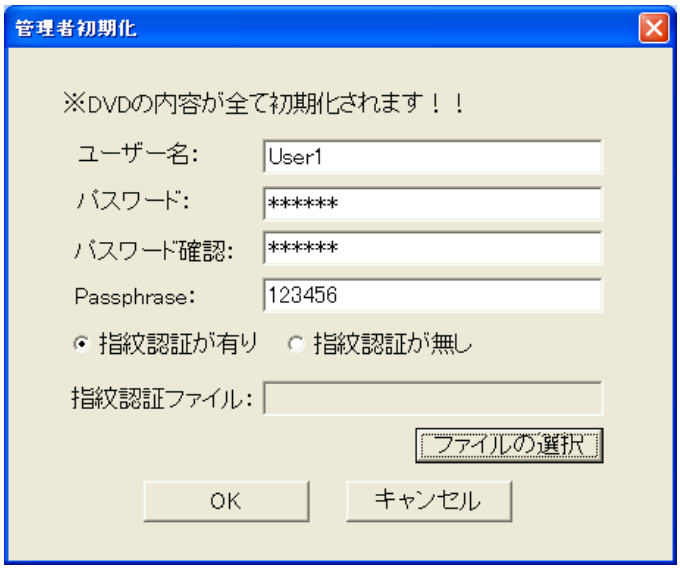


図 1.4.2-3 責任者名、パスワード、利用者のパスワードと指紋認証

次にこの一連のフローチャートを図 1.4.2-４に示している。

光記録部、暗号チップ部、指紋認証装置それぞれが分担している機能をフローチャートとあわせて記載している。フローチャートでは左からパソコン及びリーダ・ライタでの処理、暗号チップ部での処理、光記録部での処理、指紋認証での処理とそれぞれの役割を分担しながら、一連の処理を実行している。責任者の場合、暗号チップに保存中の責任者名、責任者のパスワード、パスフレーズを認識できれば高度暗号チップ搭載光ディスクが利用できる。部下やクライアントの場合、暗号チップ部に保存されているパスフレーズ、使用期限（使用開始日、使用終了日)、使用回数との照合と指紋認証装置への入力データと光記録部に保存されている指紋データの照合ができれば、高度暗号チップ搭載光ディスクが利用できる。また、高度暗号チップ搭載光ディスクの中の動画、静止画、テキストデータなどは、AES で暗号化されて処理されて

いる。高度暗号チップ搭載光ディスクのフォルダに対してデータをドラッグ＆ドロップすれば、暗号化及び復号ができるので、簡便な利用が図れる。また、リーダ・ライタは、１台ごとにシリアルナンバーが異なり、専用ドライブ自体の認証を行えるようになっている。

このように、従来パソコン側で暗号処理のすべてを行っていたが、暗号チップ部や光記録部並びに指紋認証装置でそれぞれの特長を生かし、その役割を分担しながらセキュリティ強度を強化している。

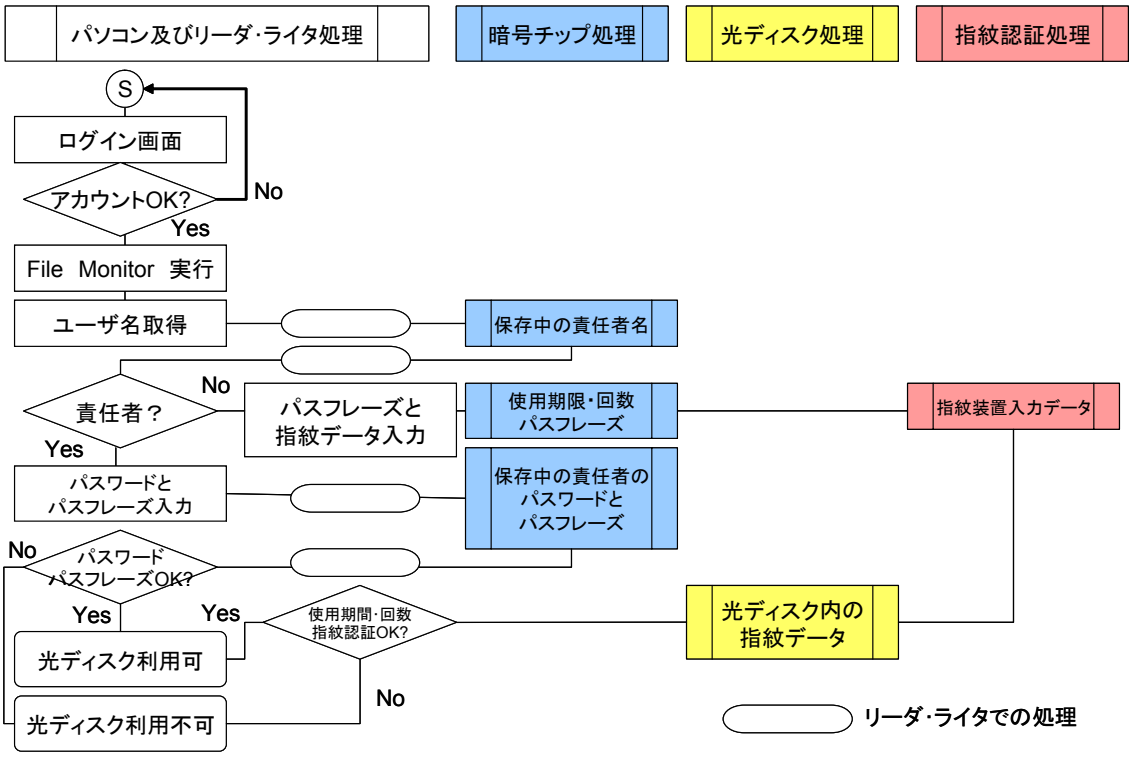


図 1.4.2-4　パソコン、高度暗号チップ、光ディスク、指紋認証の役割分担

（2）Linux に暗号システムを搭載した場合

高度暗号チップ搭載の Blu-ray ディスクに暗号システム TRUECRYPT を含む Linux　OS（SLAX）を搭載した。図 1.4.2-5 に一連のフローチャートを記載している。高度暗号チップに入力されているデジタルデータが規定値か否かを判断した後、個人がパスワードを入力し、暗号ソフト TRUECRYPT を開くことができる。そうすると暗号フォルダが開かれ、各種データ（動画（100MB)、静止画（10MB)、テキストデータ（1MB））を取り出すことができる。

また、各種データファイルを暗号化して、フォルダに入力すれば、データファイルは暗号化されてフォルダに格納される。これらの一連の処理を終了する場合は、BOX　CLOSE をクリックすれば暗号処理のプログラムは終了する。この場合、高度暗号チップに入力されているデジタルデータの規定値のチェックは最初に確認されているので、暗号系の処理の伴わないファイルの処理はできる。すべてのデータ処理が終了しパソコンを停止させて、再起動した場合は上記フローを経ない限り～即ち高度暗号チップのデジタルデータの規定値を確認できない場合～暗号系ソフトが利用できなくなっている。

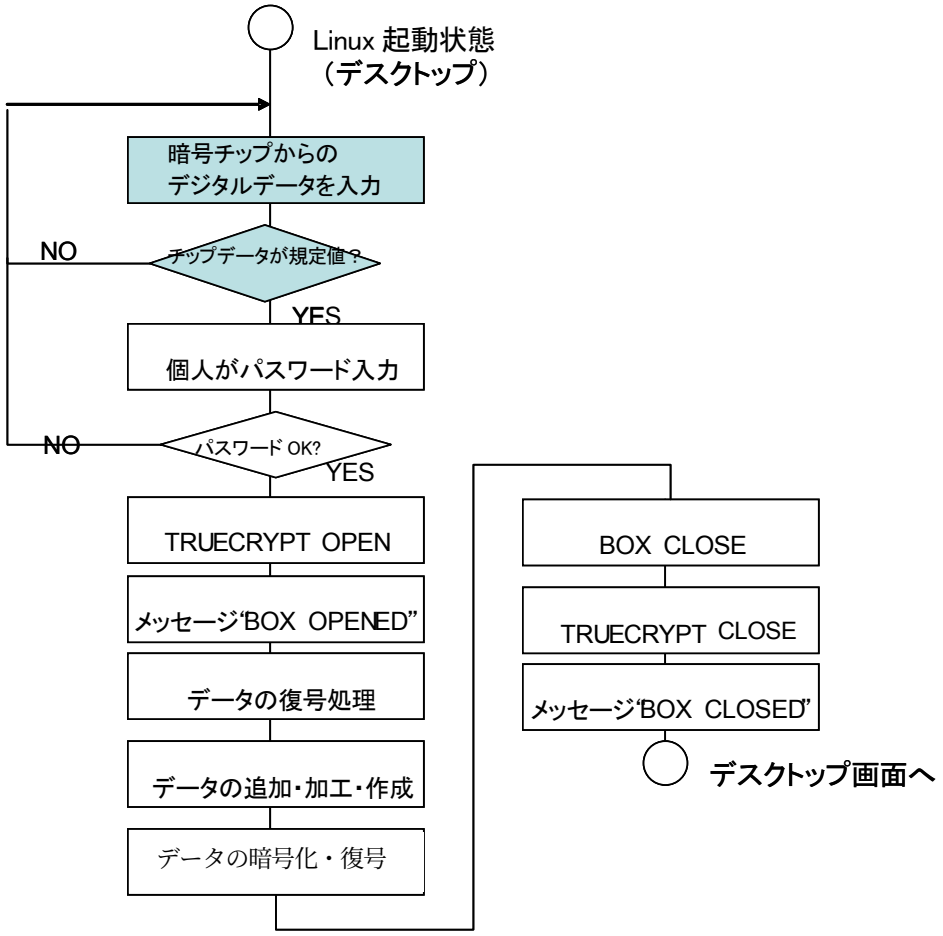


図 1.4.2-5　暗号チップ搭載 Blu-ray ディスクに Linux

1.4.3　耐タンパ性

（1）耐タンパ性技術

高度暗号チップ搭載光ディスクで実現するシステムは、暗号技術やデジタル署名などの情報セキュリティ技術を基盤として構築されている。

そのようなシステムは、暗号化・復号・署名生成のための鍵をはじめとする秘密情報を厳重に管理することが非常に重要である。

このため、耐タンパ性を有するモジュールが重要である。

耐タンパ性を有するモジュールとは、暗号化・復号・署名生成のための鍵をはじめとする秘密情報や秘密情報の処理メカニズムを外部から不当に観測・改変することや秘密情報を処理するメカニズムを不当に改変することが極めて困難であるように意図して作られたハードウェアやソフトウェアのモジュールである。

1.4.3.1 半導体デバイスに対する耐タンパ技術

ハードウェアに対する耐タンパ技術、特に高度暗号チップのような半導体デバイスにおいては、以下のようなものが知られている[1]。

(a) 暗号チップ回路とメモリなどを１チップ化：

暗号回路とメモリ回路を別のＬＳＩにすると、インタフェース回路のパッド部分や配線部分にロジックアナライザのプローブをあてられ、流れる信号を解析されてしまう。

１チップ化することで、プローブを当てるのを困難にする。

(b) チップを何重もの膜で覆う：

膜をはがして中身を覗こうとすると、回路パターンまで原型をとどめないくらい壊してしまう。

(c) チップ表面を絶縁膜とアルミ薄膜などで覆う：

ＬＳＩパッケージを壊して中身を観察しても、回路パターンが外部からは判別できないようにする。

(d) 消費電流の変動を抑える：

ＬＳＩの消費電流の変化を詳細に調べることによって、暗号演算の処理段階のヒントをつかむことができる。所謂 Differential Power analysis(PDA)法である。

これを防ぐために処理内容と消費電力が連動しないようにする。

(e) ＬＳＩの検査用パッドを除去する：

ＬＳＩ検査用パッドが残っていると内部動作を解析しやすい。

そこで検査終了後などにアドレス・パッドを除去する。

(f) 光によってメモリの記憶内容を消去する：

パッケージを壊してＬＳＩの回路パターンなどを露出させると、暗号鍵データやプログラムなどを記憶していたメモリの内容が消去されてしまうようにする。

(g) 異常なクロック周波数や電源電圧では動作を止める：

極めて遅い、または高いクロック周波数でＬＳＩを動作させると、内部の動作を解析するきっかけを与えることがある。

そこで正常に動作するクロック周波数に幅を設けて、それ以外の範囲では動作しないようにする。

電源電圧についても同じである。

(h) バスのスクランブル：

バスを流れる信号の解析を困難にするため、バスを流れる信号のスクランブルを行う。

1.4.3.2 ソフトウェアに対する耐タンパ技術

ソフトウェアに対する耐タンパ技術としては、以下のものが知られている。

(a) 実行コードの暗号化：

コードを暗号化し、実行時に必要な部分のみがメモリ上に復号するようにすることで、ディスアセンブルなどの静的解析を困難にする。

(b) 難読化：

対象となるコードを等価でかつわかりにくいコードに置き換えることでディスアセンブルなどの静的解析を困難にする。

具体的な技術として、オブフスケーション変換（Obfuscation Transformation） がある（難読化技術は、概念的にも技術的にもオブフスケーション変換と非常に似ていることから、オブフスケーション変換に含むものとする）。

オブフスケーション変換は、解析者の不正な解析行為が困難に成るように、プログラムの等価変換を行う。

例えば、ループ構造のようにプログラムの記述の中で頻繁に現れるような構造や、置き換え可能な命令群に着目して、プログラムを等価変換する。

これにより、プログラムが実現する機能の理解を困難にする。

オブフスケーション変換は、一般的なプログラム言語で記述されたプログラムに耐タンパ性を付加することができ、安価で利便性が高い。

また、これまでの耐タンパソフトウェア技術では最も盛んに研究されてきているものである。

(c) 改ざん検出コードの挿入：

処理をバイパスするなどのモジュール改ざんを防ぐために、モジュールの Hash 値を随時検証するメカニズムを組込む。

(d) デバッガ検知コードの挿入：

デバッガが起動されているかをモニターするコードを埋め込み、実行時にデバッガが起動されている場合にはモジュールを強制終了するなどの処理を行うこと。

1.4.3.3 耐タンパ対応暗号チップの一例

現在のところ、耐タンパ性を要求する FIPS 140-1 Level4 Physical Protection requirements

を満たす認可製品の数は数えるほどしかなく、研究に関しての公開 情報は非常に限られている。

これは、この分野の研究の多くが民間企業の研究所で行われており、その内容が企業秘密または知的所有権として扱われているからである。

幸いにも、今回の研究開発に使用したＦ社製、高度暗号チップでの耐タンパ性の内容は公開されている（Ｆ社　技術情報誌[2]）ので、解説しておく。

マルチアプリケーションに対応したこのスマートカード用暗号化チップは，侵入攻撃への対策としてこの構成を持っている。

ＦＲＡＭのアクセスコントロールに加え、ＦＲＡＭ領域のセクタ分けを行い、セキュリティレジスタの設定に従って、セクタごとにリード/ライトのプロテクト設定が可能である。

この設定に違反したアクセスが発生すると、アクセス可否信号によりシステムバス上の例外割込み信号が発生し、プロセッサに通知される機構も実装されている。

また、電圧の降下も検出し、システムに通知する一方で、アクセス中のデータの保証も行っている。

このように、プロセッサコア部やロジックコントローラ、暗号マクロのリソースを混在して配線することで、スクランブルが掛かった状況になっているため、表面からの観察では配線接続を特定することができない。

さらに実際のプロセス技術では、配線層間膜の平坦化や多層配線・ダミー配線、メタルカバー膜を用いることで、表面や表面から次下層のパターンとの配線接続を観察することも困難にしている。

また FM マクロ構成は、プロセッサの論理アドレスから遊離した物理アドレス配置を有している。論理アドレス上は連続した 32 ビット長のデータでも物理的には点在するため、侵入攻撃の手法によってその位置を探し出し、かつ、ビットごとに読出すことはほとんど不可能となっている。

1.4.4　プロセッサ、演算性能、メモリサイズ、耐久年数

1.4.4.1 プロセッサ、演算性能

高度暗号チップ内蔵プロセッサに要求される機能と性能は用途に応じて、一義的には定まらないが、今回の試作で使用したＦ社製、マルチアプリケーションスマートカードに対応可能な、暗号化チップを参考に説明する。

①マルチアプリケーション対応チップのファームウエア構造

マルチアプリケーション対応の暗号チップのファームウエアの構成は図 1.4.4.1-1　のようになる[2]。シリコンハードウエア（暗号チップのハード）の上に基本ファームウエア（OS）を載せ、各アプリケーションを安全に選択的に実行できるようにセキュリティも考慮されたようになっている。

この場合の各アプリケーションは不揮発性メモリである FRAM 上にロードし常駐させて実

行したり、不要になったアプリケーションは削除して別のアプリケーションに入れ替えたりするなどの機能を持たせる。

このプロセッサは外部とのインタフェースを能動的に（インテリジェント機能）行い、アクセスコントロール（認証、資格制限など）を行うのでそのための高機能が求められる。

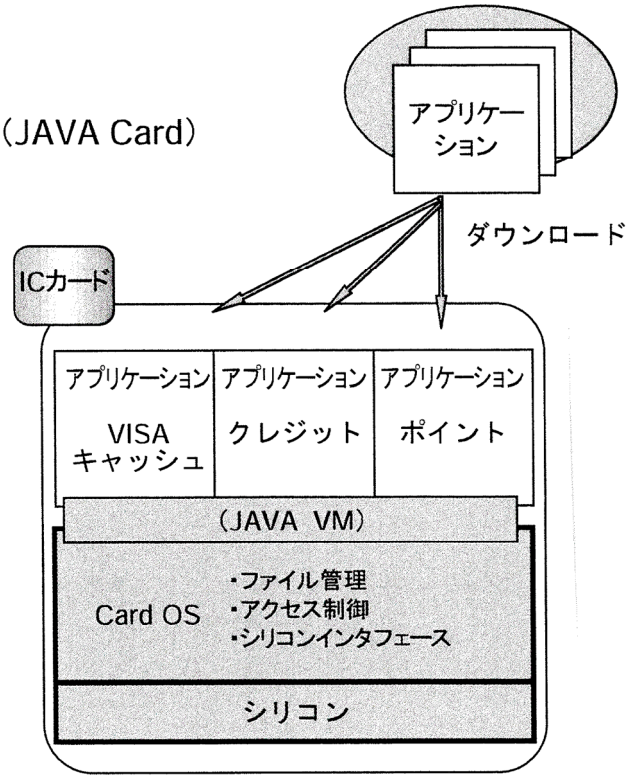


図1.4.4.1-1　マルチアプリケーション対応型スマートカードのファームウエア構成[2]

このスマートカードの例では、キャッシュカード、クレジットカード、ポイントカードに対応するアプリケーションプログラムをＪＡＶＡ言語で書いたアプレットとして、カードＯＳの上に作られた、ＪＡＶＡの実行環境（ＪＡＶＡ　VM）に向けて、ダウンロードされるような構造になっている。

シリコンと書かれた暗号チップハードの上に、ROM化されたカードＯＳとＪＡＶＡ VMの全体が、耐タンパ性の考慮された半導体チップとして一体構造につくり込まれている。

ＪＡＶＡカードＡＰＩはＪＡＶＡ言語で書かれたアプリケーションを、異なったカードＯＳでできたスマートカードでも共通に利用するための仕様である[3]。

将来、これと殆んど同じＡＰＩを持たせたマルチアプリケーション向きのスマートカード用チップを搭載すれば、「ＪＡＶＡディスク」と呼ぶにふさわしい高度暗号チップ搭載光ディスクが実現する。

Blu-ray のような大容量光ディスクに適応させた「ＪＡＶＡディスク」がインターネットに

接続されたパソコンや情報家電で利用されるようになれば、パソコンでのｅコマースやＥトレードでの音楽、映画のダウンロード購入を、サービス事業者の多彩なサービスに対応させながら、安全に運用できる仕組みの実現の可能性が見えてきた。

1.4.4.2　耐久年数（寿命）

半導体デバイスの耐用年数は、デバイス構成素子としての配線、酸化膜およびトランジスタなどの耐久性によって決まるが、その耐久性は、製品設計時の信頼性設計により半導体デバイスに造り込まれる。

耐用年数は標準品の場合､推奨条件内での使用で少なくとも 10 年持つように設計されており、実際には数十年 と安定した動作をすることもあるが、その保証はされていない。

ただし、使用条件や保存条件を限定することにより、長期保存光ディスクの要求する、耐用年数の保証を得ることは、詳細なシミュレーションと加速度試験評価が必要ではあるが、可能であろうと思われる。

半導体メーカ発行の半導体デバイス/信頼性ハンドブックによると半導体の耐用年数を決める経年変化による故障のモードは次のように分類されている[4]。

これらの中でも、MOSLSI の微細化につれて薄膜化が進むゲート酸化膜の酸化膜経時破壊（TDDB：TimeDependent Dielectric Breakdown）や、配線の微細化による電流密度の増加が金属原子を運んで断線や短絡に繋がるエレクトロマイグレーションなどに起因するものが注目される。

具体的には、それぞれの現象に対して目的の耐用年数を確保するための、造り込みが設計時になされるが、一般的な半導体デバイスでは１０年の耐用年数の保証をすることが多い。

これ以上の耐用年数を必要とする場合には、特別に仕様を明示して、メーカから耐用年数の保証を得る必要がある。

一般にはこのためのコストアップは当然生ずるので、メーカとの交渉が必要である。

長期保存を目的とした高度暗号チップ搭載光ディスクに搭載する高度暗号チップの保存期間を例えば３０年と仮定した場合、非通電の保存期間が大半を占めることを考慮し、耐用年数のシミュレーションを行えば通常の造り込みで、実現できる可能性も、あると思われる。

高度暗号チップには、ROM・RAM 以外に不揮発性メモリを搭載している。

耐用年数の造り込みにはこの部分の信頼性設計が重要であるが、ＥＥＰＲＯＭ, ＦＲＡＭともに１０年は保証されているが、現状それ以上の保証はされていない。

現世代の不揮発性メモリの欠点を補う次世代不揮発性メモリの実用化も臨まれている。

候補としてはＭＲＡＭ　磁気メモリ(MRAM: Magnetresistive Random Access Memory)、

ＰＲＡＭ　相変化メモリ(PRAM：Phase change Random Access Memory)

ＲｅＲＡＭ　抵抗変化メモリ　(ReRAM: Resistance change Random Access Memory)などがある、これらはいずれも書き換え回数が飛躍的、殆ど無制限になるが、記憶の保存期間も１

０年以上を保証するにはチップ全体の耐用年数の信頼性設計が必要である。

ＲＦ暗号化チップに搭載する場合の問題は書き込み時の電力消費をどれだけ抑えられるかが大きな課題である。

1.4.4.3　メモリサイズ

暗号チップに搭載される ROM・RAM、不揮発性メモリのサイズは１００バイト程度から、数十キロバイトまで多くの種類がある[5]。

このようなものの中から用途に応じて選択することになる。

Ｉ社のチップの例では、Mifare®(*) インタフェース仕様を持ち、１KバイトのＥＥＰROMを搭載し、そのメモリを各１６バイト構成の４ブロックからなる１６セクタに分け、各ブロックはメモリ領域へのアクセス条件が定義できる構造になっている。

Ｉ社のもう一つのチップでは、ＩＳＯ１４４４３ＴｙｐｅAインタフェース仕様を持ち、EEPROM のサイズは１６０バイト、７７バイト、２５６０バイトの製品がある。

このメモリはマルチアプリケーション対応できるよう柔軟に設計されており、１４の独立したセキュアー・データ・セグメントに分けることができる。

また、各セグメントのサイズはアプリケーション側の設計で定義できるようになっている。

欧米での普及が目覚しい Mifare®仕様と、日本で高い普及率のフェリカ仕様とはＩＳＯ１４４４３のＴｙｐｅA、ＴｙｐｅCで定義されているが、この両方のインタフェースとさらにＴｙｐｅＢも包含した共通規格がＮＦＣ（Near Field Communicatinn）Forum で策定され、電子タグから銀行カードまでの多彩な応用向けに、用途に応じたサイズのメモリサイズを選定できるようになりつつあるのでさらに選択肢は広がっている。

* Mifare® is a registered trademark of NXP Semiconductors.

[参考文献]

[1]財団法人日本規格協会、平成１４年度　耐タンパ性調査研究委員会報告書,
　平成１５年３月
[2]富士通株式会社、FIND vol.21 No.4 2003
[3]情報処理振興協会、平成１１年度　スマートカードの安全性に関する調査報告書、
　平成１２年２月
[4]NEC エレクトロニクス、半導体　品質/信頼性ハンドブック、October 2007
[5]Infineon 社、INFINEON CHIP CARD IC PORTFOLIO 、2007/2008
　URL; http://www.infineon.com/security

第 2 章　実証実験、評価

2.1　暗号チップ搭載 Blu-ray ディスクと専用ドライブの機能試験

“ ROM・RAM 構造 Linux OS ”が利用できる Blu-ray、DVD-RAM、DVD＋RW があるが、その用途によって使い方が異なる。

価格重視であれば DVD＋RW が最も安価であり、データ保存などの記録容量を大きくとりたい場合は Blu-ray が最適である。

その利用方法については利用者の考え方に依存するが、記録データをライブラリとして残しておきたい場合は、高記録容量を持つ DVD-RAM や Blu-ray となる。

機能試験項目

1）　高度暗号チップ搭載光ディスク搭載のディスクをドライブに挿入し、情報データ（映像データ：容量 100MB　静止画データ：容量 10MB　テキストデータ：容量１MB）を５回書き込み･読み出しする。

2）　上記データを PC 上で暗号化して、同じく書き込み･読み出しを行う。

3）　高度暗号チップの暗号コードでデータを暗号化し、上記情報データを書き込み･読み出しする。

4）　高度暗号チップに責任者及びクライアントの属性データを入出力する。

上記試験内容を行ったディスプレイ画面を図 2.1-1 に示す。

図 2.1-1 は、静止画データ（POWER　POINT）のデータを暗号化して光記録部に入力し、それを復号したときのデータである。

併せて、動画データ（１００MB）も書き込み・読み出しができていることを確認した。

暗号チップ部に書込まれている内容は、データ暗号チップ SERIAL　NO（さらに暗号化して書込まれている）から利用しているドライブ、ポート、責任者名、パスワード、クライアント名、パスフレーズ、期間限定（開始日時、終了日時）、利用できる回数、指紋認証データなどである。

それらの書き込み・読出しができることを確認した。このように１）～４）について暗号チップ部並びに光記録部への書き込み･読み出しが行われていることを確認した。

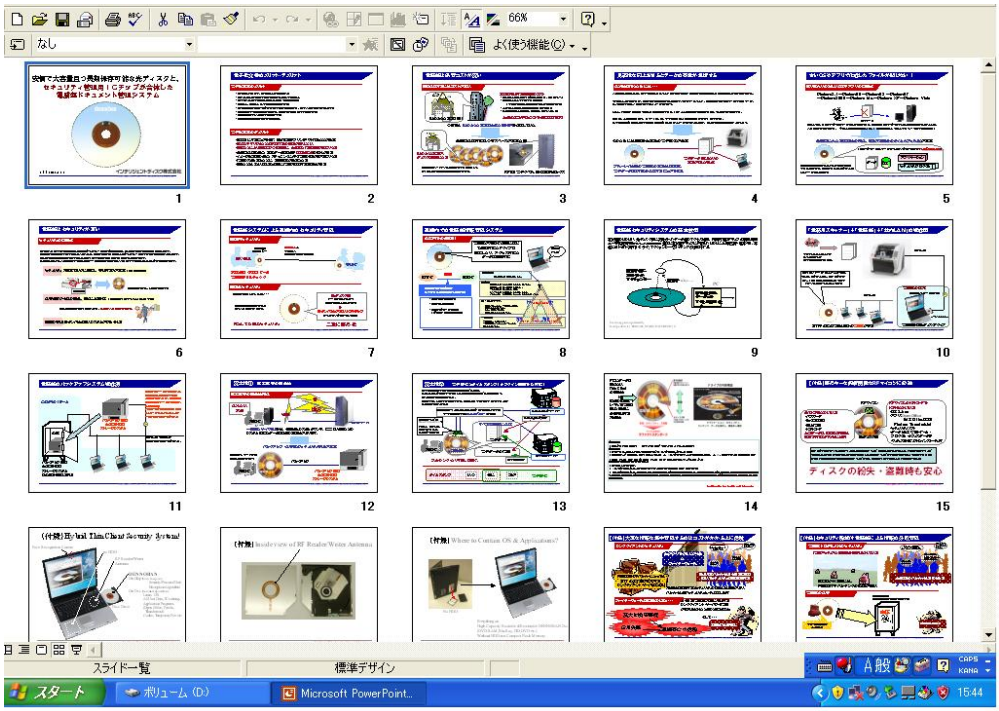


図 2.1-1 静止画データの入出力（データ容量：１４MB）

2.1.1　暗号チップ搭載ディスクと専用ドライブによるファイル管理

図 2.1.1-1 と図 2.1.1-2 に、高度暗号チップ搭載光ディスクシステム搭載の Blu-ray ドライブ及び DVD-RAM ドライブの外観を示している。

また、図 2.1.1-3 にノートパソコン（HDD 及び DVD-RAM 内蔵）に外付けされた状態の、高度暗号チップ搭載光ディスクシステムを示している。

図 2.1.1-1-1Blu-ray ドライブの概観

図 2.1.1-2 DVD-RAM ドライブの概観

図 2.1.1-3　ノートパソコン（DVD-RAM 内蔵）に外部光ディスクを接続

Blu-ray ディスクはフォーマット時でユーザ領域が４５GB になるので、DVD-RAM の補助記録メディアとしての利用法も検討し、この中に動画データや静止画データ及び暗号ソフト TRUCRYPT を利用して、暗号化して書き込み･読み出しする実験を行った。

容量が 4.7GB である DVD-RAM とは異なり、容量が 50GB であるので、当初から提案している会社でのセキュリティ権限を明確にした文書保管と管理に最適なシステムであることを確認した。

2.2　セキュアネットワークシステム（FACCIO）

インターネット技術の普及は我々の生活に便利さを与えたが、その一方で詐称や個人情報漏洩といった犯罪が発生している。

安全で信頼できるクローズドなネットワーク基盤システムとして『FACCIO』を東京電力株式会社が提案している。

FACCIO は、ネットワークを利用するにあたってユーザ認証が必要なこと及びソフトウェアをネットワークに接続する前提としてソフトウェア自身の認定が必要であるという制約を設けた、仮想ネットワーク形成システムである。

サーバ側のエージェントが利用者の登録、管理を行い、加入者のネット上での通信はすべて実 IP アドレスを使わず利用者名だけで行うため、ネット上での各種危険にさらされることがないという特徴を持つ。

本章においては、高度暗号チップ搭載光ディスクと FACCIO の組合せの、情報通信サービスへの適用手法についてのべる。

2.2.1　デジタルコンテンツの流通・管理における現状分析と課題

デジタルコンテンツの流通・管理において、コンテンツ著作権などの保護とともに、利用者の個人情報保護が大きな課題となっている。

また、事業者－利用者間の接触機会創出・相互関係維持（情報通信に関する事業者サービス提供）という、相反する 2 つの課題が従来からある。

この課題を解決するための一手法として本章では、現実の世界にある事業者サービス及び利用者を、情報流通媒介用エージェントの形で仮想化し関係を維持するモデルに置き換え、その実装として、個人情報保護機能を有する FACCIO システムについて述べる。

情報システム構築のアプローチとして、現実世界の手順や情報を忠実に情報システムへ置き換えるだけでなく、オブジェクト指向[1]あるいはエージェント指向[2]といったモデル化や、個人情報という現実世界の情報の流通を制御しコミュニケーションを限定する手法が提案されているが[3]、利用者への負担感及び不安感を減少させるためのアプローチは、引き続き課題となっている。

2.2.2　FACCIO のモデル

(1)　DRM 及び個人情報保護における要件

(a) 事業者－利用者間コミュニケーションにおける事業者側から見た課題

商取引以前及び商取引行動後の事業者－利用者間の関係を維持･向上させるために商品購入客･見込み客向けに個別化された WWW ページやメーリングリストを用意するといった手法があるが、事業者側から見た課題として下記が挙げられる。

- 利用者の個人情報は流出させたくない
- 優良な利用者とのみ顧客アンケート調査､特典配布といったコミュニケーションを維持継続したい

(b) 事業者－利用者間コミュニケーションにおける利用者側から見た課題

利用者側は、事業者が保有する情報そのものについては興味があるが、課題として下記が挙げられる。

- 個人情報の事業者への提供は避けたい
- 興味のある事業者との関係は継続したい

(2)　モデル化とアクセス制御

個人情報保護及び事業者－利用者間コミュニケーションの要件を満たすために、利用者及び事業者サービスという現実世界の物体を、ソフトウェアオブジェクト（以後エージェント）として仮想世界に表現・維持し、当該エージェント経由にてコミュニケーションを実現するという実世界仮想化モデルを提案する。利用者は必要とするエージェントのみを維持し不必要なエージェントを削除することにより、情報をフィルタすることができる。

事業者側から見ると、事業者から利用者に対しエージェントを配信すること及びエージェン

トを経由し情報を配信することにより、利用者の個人情報がなくともエージェント経由にて事業者サービスを提供することが可能となる（図 - 2.2 - 01 参照)。

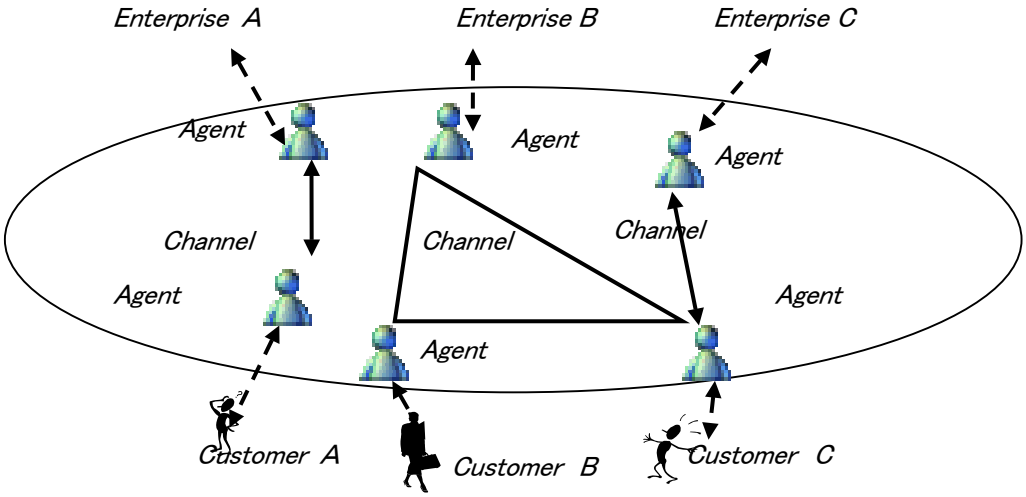


図 2.2.2 - 1 モデル

(3) コミュニケーション手法

事業者サービス提供用に、チャンネルと呼ぶ仮想化した通信路をソフトウェア上定義する。このチャンネルに対し通信を行うことにより､従来はメール･ウェブブラウザと使い分けていたインタフェースを、ひとつに統一することができる。これを用いてコンテンツ送受、コンテンツ着信確認、事業者サービスの公開を実現する（図 - 2.2 - 02)。

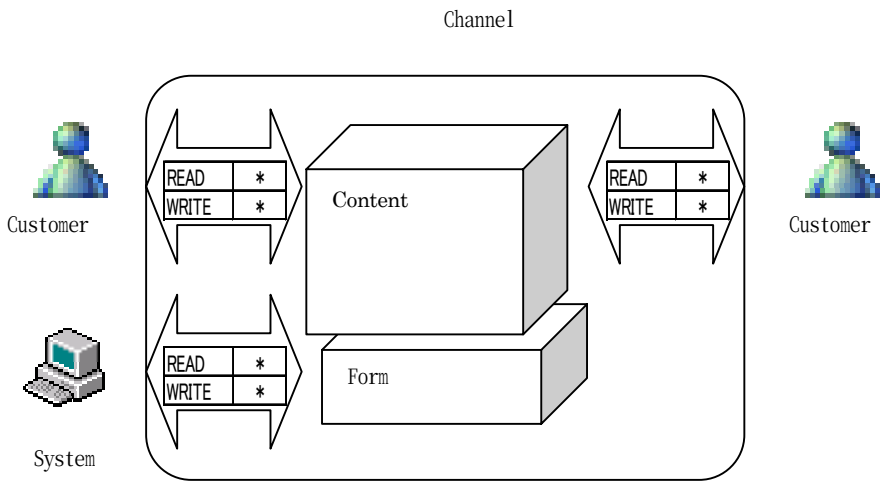


図 2.2.2-2 コミュニケーション手法

2.2.3 FACCIO のアクセス制御

(1) アクセス制御権限

アクセス制御用に、チャンネル参加権・チャンネル読取権・チャンネル書き込み権・利用者一覧権・チャンネル作成権・チャンネル招待権・権限付与権の各権限を定義した。

権限を有する利用者は、チャンネルへ参加する、コンテンツを読み取る、コンテンツを書き込む、利用者の利用者名を閲覧する、チャンネルを新規に作成する、チャンネルに他の利用者を招待する、利用者へ権限を付与するといった行為を実行できる。

(2) アクセス制御手法

これらの権限をシステム管理者が利用者へ直接付与することができ、またシステム管理者が権限付与権を利用者へ付与すると利用者同士にて権限の伝搬を実現することができる。

2.2.4 FACCIO の個人情報保護手法

(1) 個人情報保護において求められること

(a) 個人情報漏洩のソフトウェア側対策

(サーバ詐称)

おとりサーバへの誘導、偽サーバなりすましといったフィッシングと呼ばれる不法行為に対する対策が必要とされている。

(クライアント詐称)

クライアントデータを削除あるいはクライアント側データをメールに添付するようなウィルス・トロイの木馬といった不正なソフトウェアに対する防止策が必要とされている。

(b) 個人情報の通信路盗み見対策

(中間者攻撃)

通信プログラムが正規なものであったとしても、ネットワークを流通するデータを盗み見るといった中間者攻撃と呼ばれる攻撃手法がある。

これに対し、通信路を暗号化するといった防止策が必要とされている。

(c) 個人情報漏洩の被害防止策

(本人認証)

データが盗み見られることがなく通信が終了したとしても、不正利用者の悪意のある操作などにより個人情報が漏洩する場合がある。

また、利用者が正規であっても操作ミスなどにより個人情報が漏洩する可能性もある。

これらに対し仮に個人情報が流出したとしても内容を読み取ることができないデータ暗号化

といった防止策や、データに対する適切なアクセス制御が必要とされている。
　また、データ自身の安全性（ウィルスが含まれていない、など）も必要とされている。

⑵　課題を解決するための方策

（a）既存の方策

（既存１）セキュアサーバ
　既存の個人情報保護手法として、個人情報をサーバへ暗号化通信路などの通信路を経由し送付し、サーバへ保存させる構成とし、サーバへ保存する際にデータそのものもシステム側で強制的に暗号化させる方法がある。
　これを用いると前記のサーバ詐称には対応できるが、クライアント側に対する対策は課題である。
（既存２）セキュアゲートウェイ
　既存の個人情報保護手法として、ネットワークへの接続ゲートウェイサーバーにおいてメールなどの個人情報を強制的に暗号化させ送信しクライアント側で復号する方法がある。
　これを用いると中間者攻撃には対応できるが、サーバ側及びクライアント側のデータ復号後のデータ保護は課題である。
（既存３）セキュアクライアント
　既存の個人情報保護手法として、クライアント側、例えばローカル PC 側に個人情報を暗号化するソフトウェアを配置し、ローカル PC 側にデータを保存する際には暗号化を任意あるいは強制にて実施させる方法がある。
　これを用いるとクライアント側には対応できるが、ネットワーク上の不正サーバや通信経路の暗号化に対する対策は課題である。

（b）既存の方策における課題

　前記の既存の方策のとおり、既存の個人情報保護方策事例が幾つか提案されているが、これらをトータルに解決するためには、前記で述べた個人情報保護上求められていることを根源的に解決する必要がある。そのための課題は以下のとおりである。
（課題１）オープンなネットワーク
　近年､誰にでも開かれたオープンなネットワークであるインターネットの利用が進んでいる。オープンなネットワークにおいて、一つの端末から別の端末へは、基本としてリーチャブルである。
　例えば、インターネットにおいては TCP/IP といったプロトコルを用いて自由に通信が可能である。
　従って例えば、クライアント側において、個人情報が自動的にネットワークに発信されてしまうようなウィルスに感染した場合、インターネット上にそのデータがノード（クライアント

やサーバ）からノードへ自由に流通してしまうことになる。
　また、正規利用者の操作であっても、間違ったデータをメールに添付し送付してしまった場合、データの流通・拡散を防止することは難しいといった課題があった。
（課題２）オープンなシステム
　インターネットなどのオープンなネットワークにおいては、利用者は性善であることを前提としているため、インターネットプロバイダとの契約といったネットワーク接続の許可があればどのようなプログラムもネットワークに接続することができる。
　従って、おとりサーバを配置するといった不正に対しそれを防止する方法がなく課題であった。また、クライアント側ソフトウェアも、ソフトウェア作成とネットワーク上への配置は自由に可能であり不正なソフトウェアが流通するという課題があった。
　加えて、送信データの中にウィルスなどが混入していた場合、データなどを暗号化されていたとしても、復号した時にウィルスに感染し被害がネットワーク全体に広がるといったことも課題であった。

⑶　FACCIO の個人情報保護手法
　前記の既存の方策の課題に対し、FACCIO を用いると、その課題解決要件を満たすクローズドなネットワークシステムを構成できる。

（a）クローズドなネットワーク
　FACCIO を用いてクローズなネットワークを構成することができるのは、FACCIO が下記の要件を満たしているためである。
（要件１）本人認証に基づくアクセス制御
　FACCIO は利用者に対するアクセス制御を実施しており、データに対しアクセス権などを適切に付与することによりネットワークをサブネットに区切りリーチャブルなノードを制限することを柔軟に設定できる。
　従って、たとえ正規利用者が操作ミスなどを行ったとしても、そのデータの流通サブネットは限定されており、かつログをトレースすることでデータ配布先を後から確認することができる。
　従って FACCIO は本人認証の要件を満たしている。
（要件２）セキュアな通信路
　クライアントとサーバ間では暗号化通信を行う。
　これは、クライアントがサーバと接続しセッションを確立する際に、暗号化通信路を構成することにより実現される。
　また、FACCIO の基本として認証されたプログラムやデータのみが流通システムである。
　データについても、認定済みのデータのみが流通する。
　これは、外部から FACCIO にデータがインポートされる際に、FACCIO 側から認証された

プログラムのみがインポートを行うことにより実現している。
従って FACCIO は中間者攻撃に対する要件を満たしている。

（b）クローズドなシステム
（要件３）認証されたサーバ
FACCIO の基本は、認証されたプログラムやデータのみで構成された流通システムである。
サーバについても、FACCIO 側から認証されたプログラムだけが、FACCIO に接続される。従って FACCIO はサーバ詐称に対する要件を満たしている。
（要件４）認証されたクライアント
FACCIO は、基本的に認証されたプログラムやデータのみで構成された流通システムである。
クライアントについても、FACCIO 側から認証されたプログラムだけが、FACCIO に接続される。これは、FACCIO 側の運用者が事前にクライアントプログラムを認証し、FACCIO サーバに配置し、クライアントプログラムがダウンロードする構成とすることにより実現している。従って FACCIO はクライアント詐称に対する要件を満たしている。
全体として FACCIO は、個人情報の保護において求められる安全の要件を満たしているシステムである（図 2.2.4-1）。

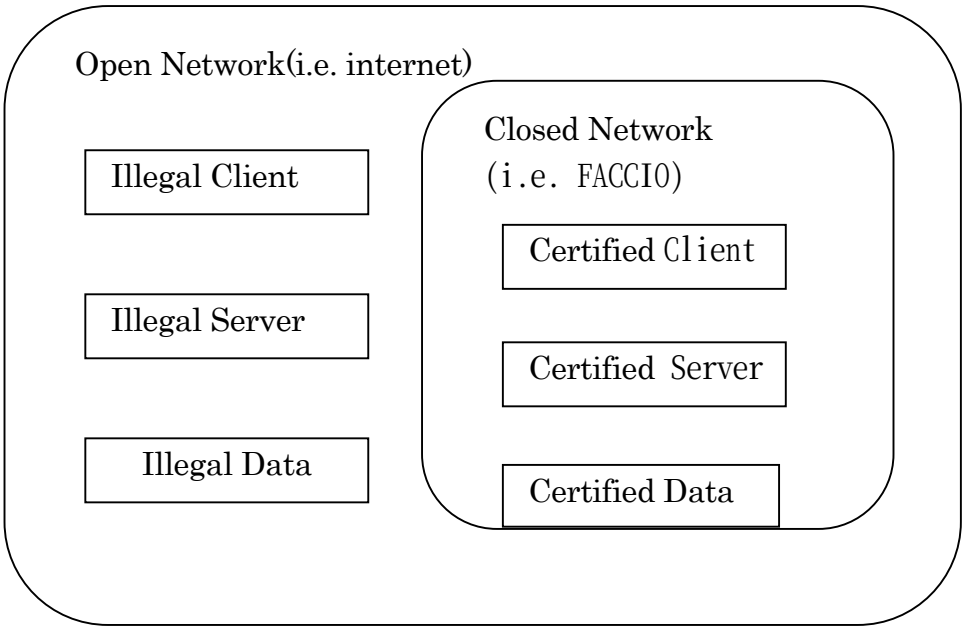


図 2.2.4-1 クローズドなネットワークシステム

2.2.5 システム構成

本モデルの実装を行った。システムはサーバサイド及びクライアントサイドに分散配置される Java プログラムにて実現した。利用者は各事業者サービスへクライアント経由にてアクセスする（図 2.2.5-1 参照）。現在、アプリケーション機能として、ホワイトボード（マウス操

作による線画、自己画面キャプチャ画像及び一般電子画像共有）、音声送受、ファイル交換、テキスト送受を実現している。

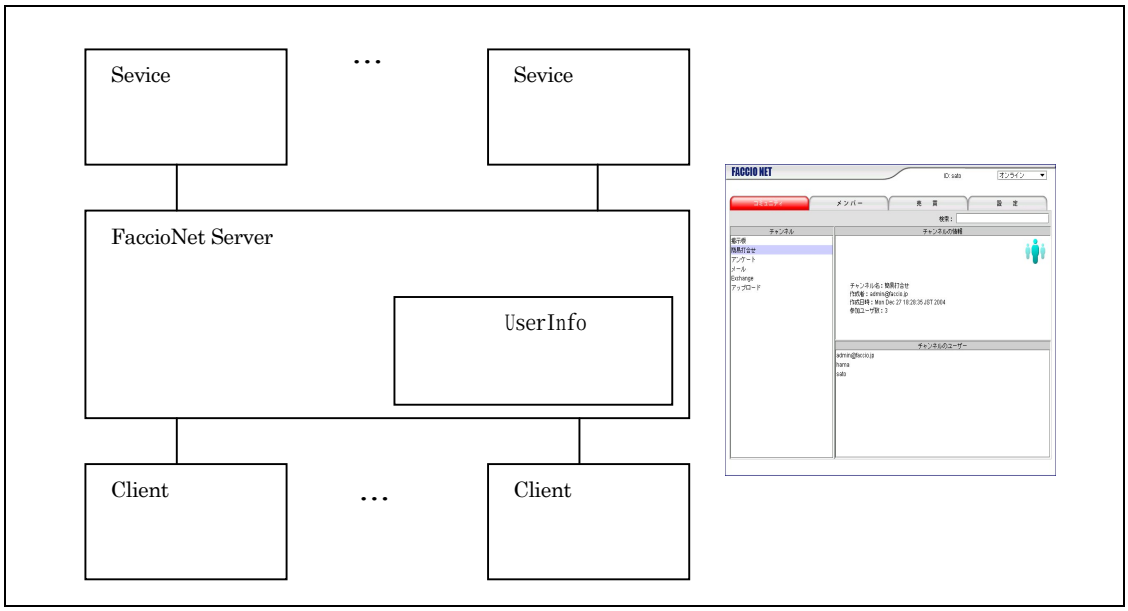


図 2.2.5-1 システム構成

2.2.6 コンテンツ流通・管理への高度暗号チップ搭載光ディスクと FACCIO の応用

高度暗号チップ搭載光ディスクと FACCIO を組み合せることによるコンテンツ流通･管理への応用手法について述べる。

(1) 応用において求められる安全性

現状のコンテンツ流通やネットコマースにおいては、利用者は自分の個人情報（名前、性別、年齢、住所、口座番号、趣味など）を一括通知しているが、個人情報のうち、各々のサービス提供に不必要な情報まで各事業者へ通知する必要はない（配送業者には品物の名前や価格を通知する必要はないし、コンテンツ配信事業者に住所・名前・銀行口座番号などを通知する必要はない。また、決済業者には住所・品名を通知する必要はない）。

つまり、利用者の個人情報は事前に許可された事業者にのみへ通知され、コンテンツ流通やネットコマースにおける利用者の個人情報保護という安全が確保される必要がある。

(2) 応用手法検討

前記の、求められる安全性を確保するために、高度暗号チップ搭載光ディスクと FACCIO の組合せを利用する手法について述べる。

コンテンツ流通やネットコマースにおいて個人情報を保護するためには、情報を漏れないシステムへ隔離し保護する手法が考えられる。

そのために、本人認証に際し、高度暗号チップ搭載光ディスク及び FACCIO を適用する。

適用箇所は以下のとおりである。

（a）本人認証への高度暗号チップ搭載光ディスクの適用

本人認証の手法としてパスワードなどの本人の記憶に頼る方式がよく用いられるが、パスワード漏洩などの安全上の課題がある。

そのため、利用者の安心・安全を確保するために、本人認証手法として高度暗号チップ搭載光ディスク技術を適用する。

（b）ソフトウェア認証及び中間者攻撃に対処するクローズドなネットワーク

フィッシングといったサーバ詐称、ウィルスに感染したソフトといったクライアント詐称、通信経路傍受といった中間者攻撃に対し、それぞれを個別に対処する方式がよく用いられる。しかしながら新たな攻撃手法が日々発生するという現状があるため、不法者のいない安全なネットワークを確保したいという根源的な課題がある。

そのため、安心・安全を確保するために、ネットワーク上にクローズドなネットワークを実現する FACCIO 技術を適用する。

⑶　応用事例

コンテンツ流通の例としてメールマガジンサービス及びネットショッピングサービスの提供事例について述べる。

このサービスには商品配送サービス及び銀行・信販会社の決済サービスが含まれる（図 2.2.6-1 参照）。　この例において各サービス事業者が保有する個人情報を示す。

・メールマガジンサービス者： 利用者のニックネームのみ

・ネットショッピングサービス事業者： 利用者の口座登録名のみ

・商品配送サービス事業者： 利用者の希望配送先

・決済サービス事業者： 利用者の口座ＩＤ・暗証№など

各サービス事業者が所有する個人情報を限定することにより、個人情報の不要な拡散を防いでいる。

実際のサービス提供方法は以下のとおりである。

（メールマガジンサービス）

商品情報などを利用者へダイレクトに表示するメール型の情報提供サービスを、メールサービスエージェントから利用者側のフロントエンドサービス（利用者側エージェント）へ提供する。（ネットショッピングサービス）

ネットショッピングサービスとフロントエンドサービス間にて、商品購入意志表示(図中①)、代金提示・決済方法の確認（図中②）の情報を授受する。加えてフロントエンドサービスは決済サービスへ銀行振込指示を、及び商品配送サービスへ商品配送先を通知する（図中③）。また、決済サービスは銀行振込指示があったことをネットショッピングサービスへ通知する（図中④）。引き続き、ネットショッピングサービスは商品配送サービスへ商品配送指示を通知し、商品配送サービスは商品配送後商品配送済み通知をネットショッピングサービスへ通知する（図中⑤）。ネットショッピングサービスは決済サービスへ商品配送が完了したことを通知し

加えて振込を指示する（図中⑥）。

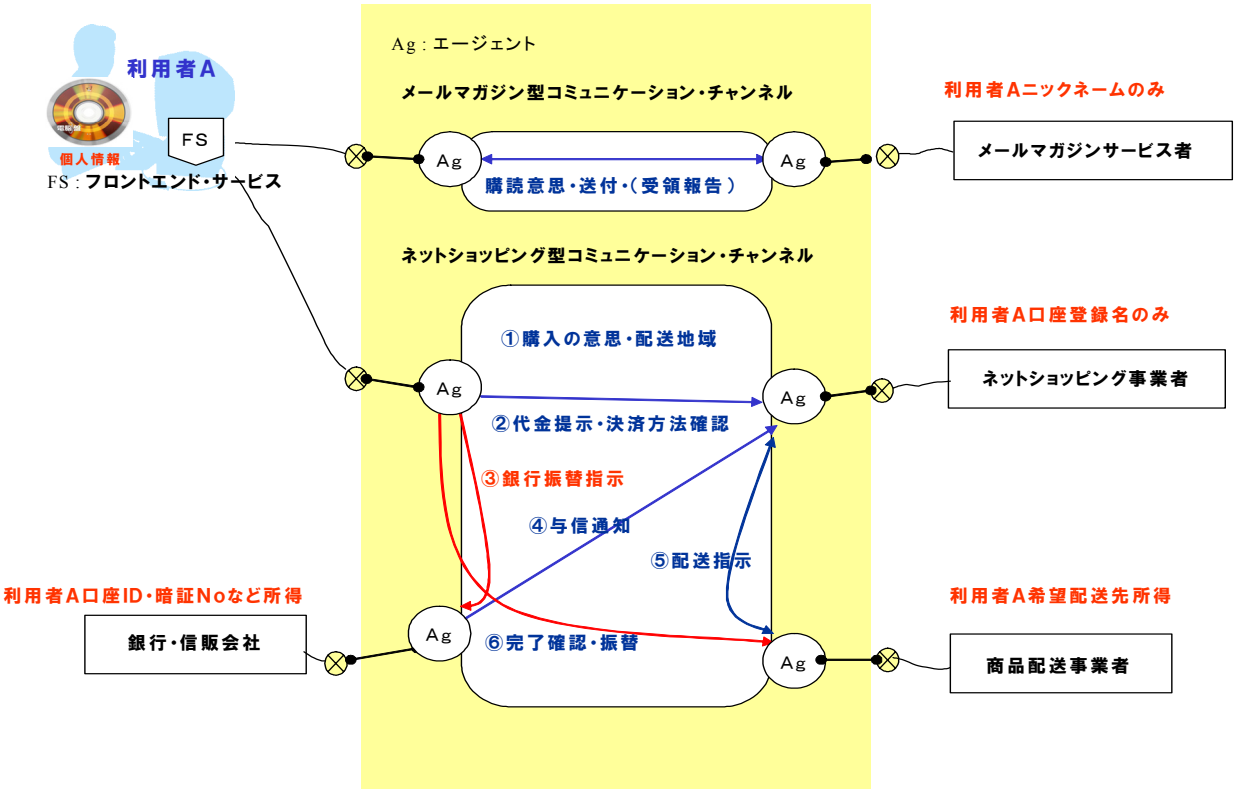


図 2.2.6-1 組合せ応用

(4)　検討結果

このように、事業者が所有する個人情報をクローズドなネットワークの中へ限定することによって、利用者は商品配送サービス事業者のみに自宅住所を提供し、ネットショッピングサービス事業者へは提供しないというシステムを実現できる。また、高度暗号チップ搭載光ディスクを用いることで、本人認証が強化されたシステムを実現できる。

従って、高度暗号チップ搭載光ディスクと FACCIO を組み合せることによって、コンテンツ流通・管理における個人情報の保護が確保され、コンテンツのネット販売、ネットにおける商品販売などにおける安心・安全が確保される。よって、高度暗号チップ搭載光ディスクと FACCIO の組合せは、各種サービスの提供に有効に適用できることがわかった。

参考文献：

［1］OMG：“ Common Facilities RFP-4 CBO&BOF ”、OMG Document ad/97-10-02（1997）
［2］吉田 仙、亀井 剛次、大黒 毅、桑原 和宏：“ Shine：ネットワークコミュニティ支援シ

ステムのエージェント指向フレームワーク ”、電子情報通信学会技術報告　OFS2001-13、AI2001-18 （2001）
［3］西田　玄、 林 良一、高倉 健：“ 個人情報の保護と流通の両立を目指した個人情報活用システム ”、 情報処理学会研究報告 DPS107-10（2002）

2.3　実証実験システム

2.3.1　実験の目的

使い放題など通信料金の定額制サービスなど有線電話系、携帯電話、ＰＨＳ無線電話系ネットワークアクセス手段が多様化し、何時でも何処からでも使いたいときにインターネットが利用できるようになってきた。

また､通信料金の定額制サービスなどによりネットワークに常時接続の利用者が増えている。今やインターネットは日常なくてはならないインフラ技術である。インターネットは、デジタル化が可能な全ての情報が分散配置された膨大な共有空間であり、日々成長を続けている。

書籍やＣＤなどをインターネット上で販売するネット書店がある。実際の書店では売り場面積に限りがあるため､「パレートの法則」に従って売れ行き上位２０%の商品を中心に陳列される。それに対してネット書店は売り場面積の制約がないため人気の高い商品から人気の低い商品まで揃えているので、実際の書店で手に入れられない商品も購入できる。また、日本全国から購入できる利便性もあり人気のサービスである。

このサービスの発展系として直接コンテンツを取り扱うサービスがでてきた。例えば、インターネットによる音楽ダウンロード販売や映像のライブ中継配信が代表的な例である。このような取引を d-Commerce と呼ぶ。

d-Commerce の大きな課題としてコンテンツ制作者の著作権保護問題がある。従来のネット書店ではいわば電子カタログショップで商品は実世界でったのに対し、d-Commerce では取り扱う商品は情報財である。情報財とは Varian が定義した言葉で「あらゆるデータのうちデジタル化可能なもの」の総称である。情報財は制作のための初期コストは大きいが、再生産コストや流通コストはほぼゼロである特性を持っている。そのため、権利者や権利保持者に無断で複製・改変され、インターネットを介して流通・取引される事例があとを絶たない。ファイル交換ソフト P2P を利用した音楽や映像データの交換･利用による著作権侵害事件は記憶に新しいところである。これを解決する技術として DRM(Digital Rights Management)がある。DRM の役割は、楽曲、写真、イラスト、映画、TV 番組、雑誌記事、小説、電子商取引でやりとりされる契約書、政府刊行物、公文書など情報財の著作権保護及び著作隣接権の保護、違法複製や違法販売の防止、信憑性の保証、情報漏洩の防止にある。d-Service は d-Commerce を中心に発展してきたが、個人情報の照会や申請、情報財の共同作業など活用場面は広がるだろう。今後は、ネット上のサービスは Web2.0 が示唆するよう、個別 Web サービスを相互に連携し高機能で利便性の高いサービスが出現する。安心、安全なサービスを提供するためにはサービス指向型 DRM アーキテクチャが必要である。

高度暗号チップ搭載光ディスクと FACCIO を組込み d-Service の実証試験環境を構築し、
情報財利用者の認証機能
情報財の流出防止機能
情報財の参照、改変、保存、廃棄機能
情報財の分散管理機能
について検証する。

2.3.2 ポリシーの定義

システムのポリシーは、その目的に応じて異なる。実証試験にあたり利用目的及びそのポリシーについて定義をしておく。この実証試験システムではネットワーク内で管理された共同作業空間と個人が管理する高度暗号チップ搭載光ディスク内で情報財（コンテンツ）を分散管理することを目的とする。

ポリシーは企業ごとに異なる、今回の実験では、サーバ、ネットワーク、クライアントを無菌状態にしたかったので、以下のとおり、最も厳しい設定を採用した。

- 情報財は共同作業空間と高度暗号チップ搭載光ディスク内にのみ保存される
- 二つの保存空間はクローズなネットワークで接続され、それ以外のネットワークからの接続は許されない。
- ネットワークあるいは外部記憶装置を介しての情報財の流出あるいは取り込みは許されない。
- 高度暗号チップ搭載光ディスクには、配布時にインストールされたソフトウェア以外は利用できない
- 高度暗号チップ搭載光ディスクの利用者はその存在が証明されている。
- 高度暗号チップ搭載光ディスクをパソコンから起動したときポリシーが有効となる。

と定義する。図 2.3.2-1 にポリシィーの定義の概念図を示す。

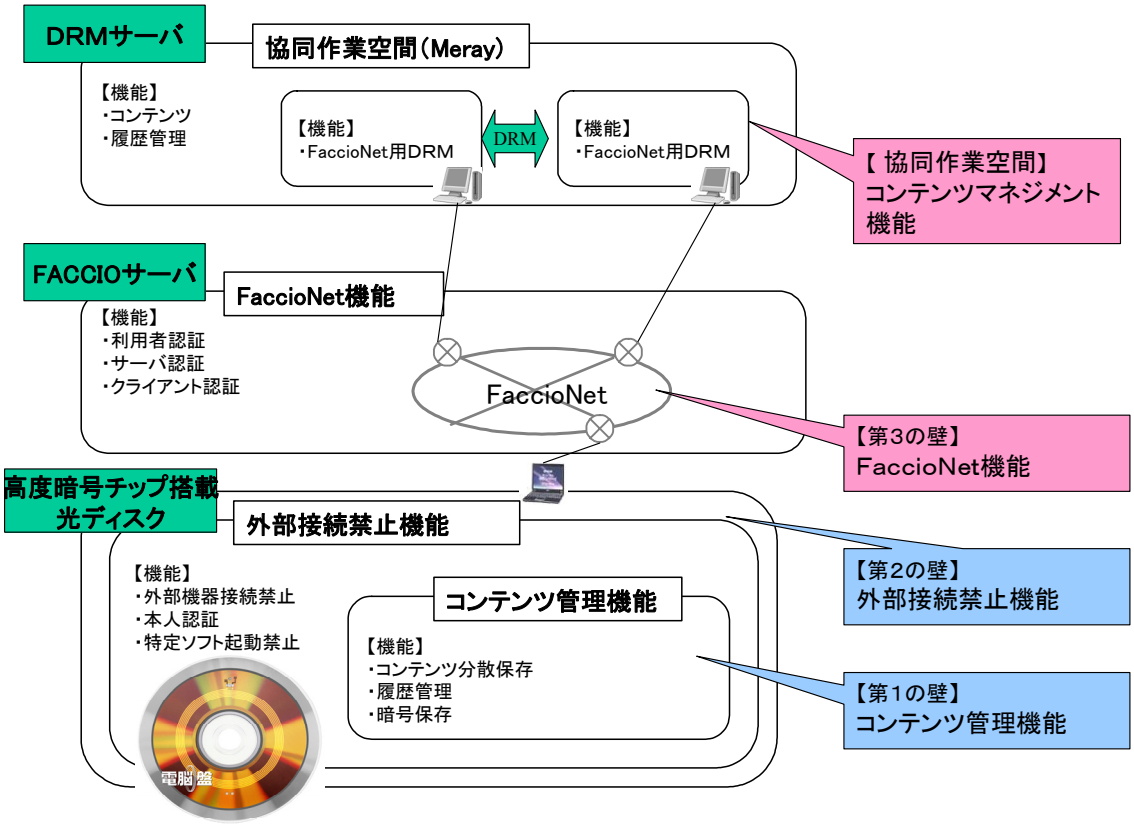


図 2.3.2-1　ポリシーの定義

2.3.3　実験システムのハードウェア構成

図 2.3.3-1 に実験システムのハードウェア構成を示す。

この実験システムは FACCIO サービスサーバ、ストレージサービスサーバ、パソコン、を無線ＬＡＮで接続したネットワークである。

FACCIO サーバはシステムの利用者とチャンネルのアクセス権限を管理するサーバで、これら管理情報に基づき情報財の配信を行う。

ストレージサービスサーバは情報財を管理するサーバである。

利用者は高度暗号チップ搭載光ディスクをパソコンから起動し利用する。

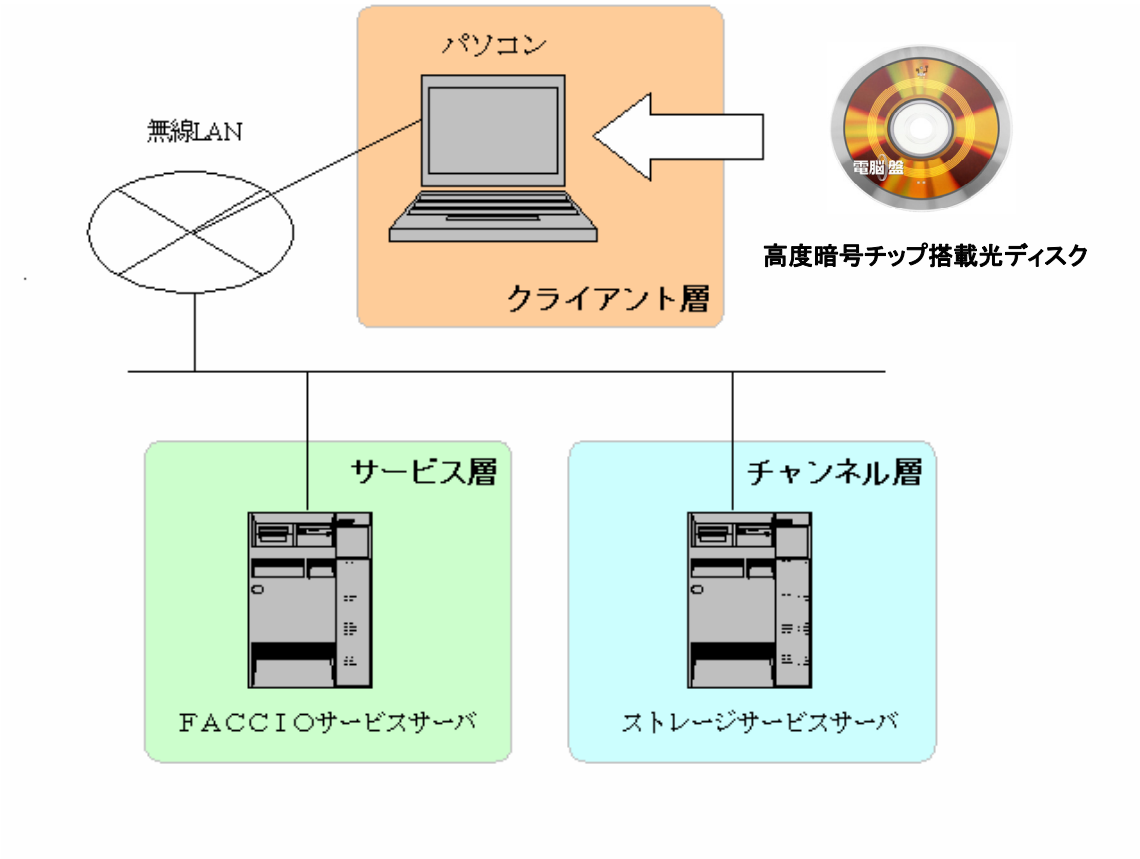


図 2.3.3-1　実験システムのハード構成

2.3.4　実験システムのソフトウェア構成

高度暗号チップ搭載光ディスクのＲＯＭ領域には、OS(Linux)、FACCIO ユーザインタフェース、オフィスソフト OpenOffice、暗号化ソフト TrueCrypt が組み込まれている。

また、FACCIO サービスサーバには FACCIO 利用者管理システム、FACCIO が、ストレージサーバにはＤＲＭソフトウェアＭＥＲＡＹが組み込まれている。

2.3.5　実験システムの構築

2.3.2 で定義したポリシーに基づき実験システムの設定を行った。

設定は、実験システムの利用者の登録、チャンネルの設定を行う。

それぞれの設定について具体的に述べる。

(1) 利用者登録

表 2.3.5-1 に今回の実験に参加する利用者の一覧を示す。

FACCI0 ではチャンネルに接続される全てのノード（人間、ハードウェア）を利用者として事前登録する。

この実験では、A さん、B さんの２名を設定した。

A さんは一般の利用者で情報財の閲覧、提供の権限をもつ。

Bさんは共有空間の責任者で情報共有空間への登録、削除、更新時に情報財の審査をする権限を持つ特別の人である。

利用者 Meray は情報財が格納されたサーバで、AさんあるいはBさんとチャンネルで接続される。　Meray-admin は FACCIO のシステム管理者である。

利用者の登録・更新・削除やチャンネルの作成・変更・削除などの権限をもつ。

表 2.3.5-1　実験に参加する利用者の一覧

利用者名	パスワード	種別
A	A	一般利用者
B	B	共有空間管理者
Meray	Meray	ストレージサービスサーバ
Meray-admin	Meray-admin	FACCIO システム管理者

(2) チャンネルの設定

今回の実験では「高信頼 Disc プロジェクト」と「連絡用」という名前の二つのチャンネルを設定した。図 2.3.5-1 にチャンネル名「高信頼 Disc プロジェクト」と「連絡用」の設定画面を示し、図 2.3.5-2 にユーザ登録画面を示す。

「連絡用」チャンネルでは、登録、閲覧、編集、更新、削除、複製、名称変更、外にコピー、外からコピーの操作権限を、Aさん、Bさんに与えている。また、Bさんはコミュニティ「連絡用」の場の管理者であると同時に、情報材の DRM 管理者でもある。

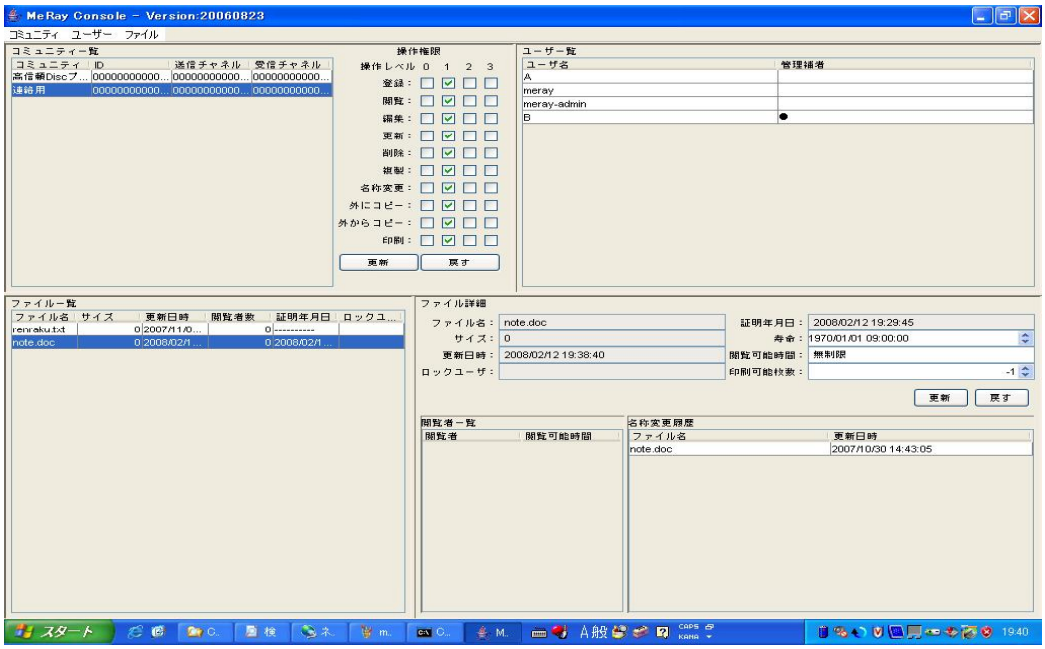


図 2.3.5-1　チャンネル設定画面例

ユーザ名	パスワード	種別
A	A	一般利用者 （チャンネル参加者）
B	B	管理者 （チャンネル参加者）
Meray	Meray	Merayサーバ（サーバ自身もチャンネルへ参加）
Meray-admin	Meray-admin	Merayサーバの管理者（チャンネル設定等を行う）

図 2.3.5-2　ユーザ登録画面例

(3) ユーザインタフェース

図 2.3.5-3 にユーザインタフェース画面例を示す。

コミュニティファイル一覧の領域はネットストレージパネル、ローカルパネル（閲覧）、ローカルパネル（編集）の３領域で構成している。

ネットストレージパネル領域にはストレージサービスサーバに保存された情報財の一覧が表示される。

利用者はネットストレージパネルに表示されて情報財のアイコンをローカルパネル領域へドラッグアウトし、閲覧あるいは編集を行う。

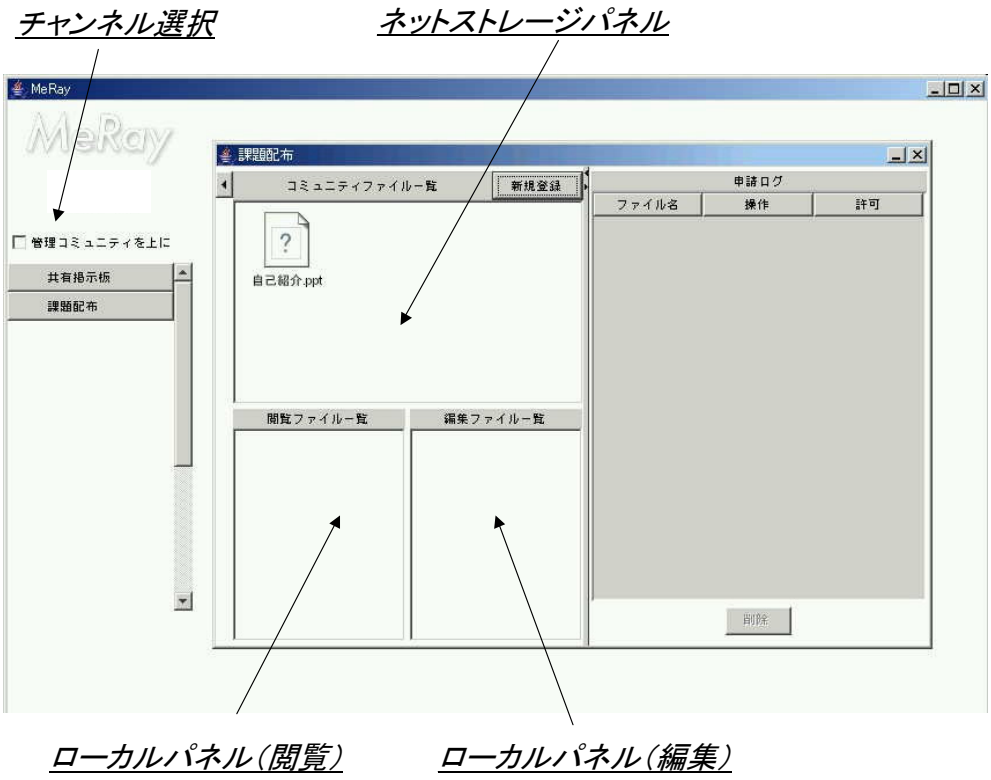


図 2.3.5-3　ユーザインタフェース画面例

2.3.6　実証試験

2.3.1 実験の目的で述べたように、安心、安全なサービスを提供するサービス指向型 DRM アーキテクチャの検証を行う。

d-Service 環境下では提供するサービスが破壊されずに閉ざされたサービス空間の中で情報財が扱われることが重要である。

また、情報財の参照、改変、保存、廃棄時においても情報財の正当性が保証されねばならない。

そこでまず、情報財をサービス空間内に閉じこめる実験を行い、次に、情報財の参照、改変、保存、廃棄の操作時に情報財の著作権が保証されることを実験した。

(1) システム認証

高度暗号チップ搭載光ディスクの ROM 領域には d-service に必要なソフトウェアを記録し、利用者に配布される。

この時点で、高度暗号チップ搭載光ディスクはサービス事業者から正規のサービスが保証されている。　高度暗号チップ搭載光ディスクをパソコンから起動すると

① 高度暗号チップに記録されたシステム ID の照合が行われこのサービスが正規のものであることが確認される。

② OS 起動時に、内蔵 HD や USB メモリ、FD などの外部記憶装置がアンマウントされ、遮断される。

③ ネットワークフィルタによりネットワークの接続先が制限され、手順を踏みクローズドな情報空間が形成される。

図 2.3.6-1 はシステム認証後の状態 d-service の状態を示す。

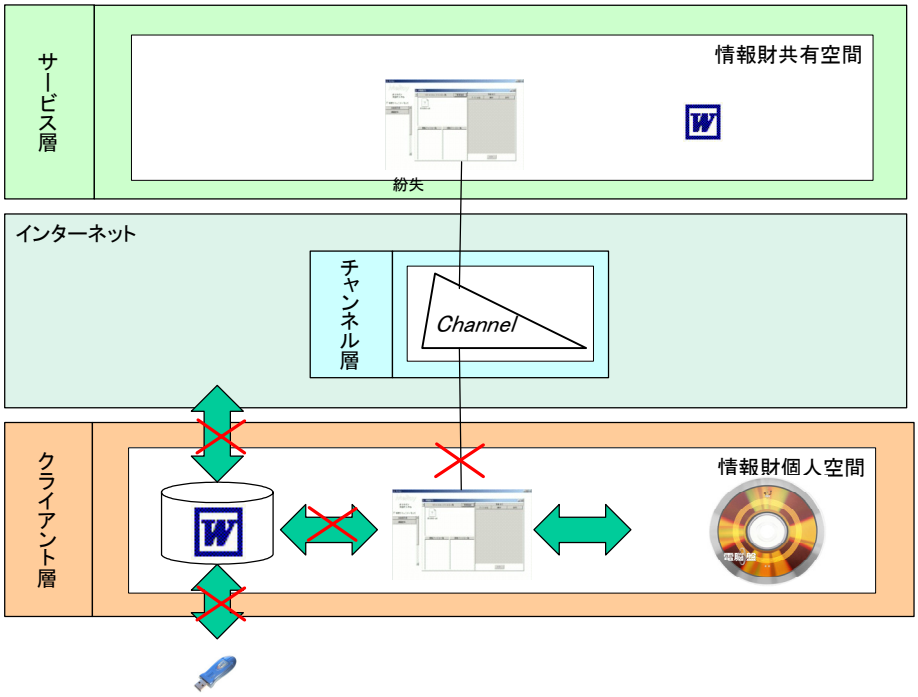


図 2.3.6-1　システム認証後の状態

(1) 利用者認証

FACCIO サービスサーバへ利用者の ID とパスワードの照会を行い、チャンネルに接続される。

この時点で、閉塞された d-service 空間が構築される。

この閉塞空間はシステムが終了するまで維持される。

今回の実験では ID とパスワードを利用者が直接入力したが、高度暗号化チップ搭載光ディスクのチップ内に ID とパスワードを記録しておき、生体認証装置などで個人認証後 FACCIO サービスサーバに照会する方法をとればセキュリティポリシーはより高まる（図 2.3.6-2 参照）。

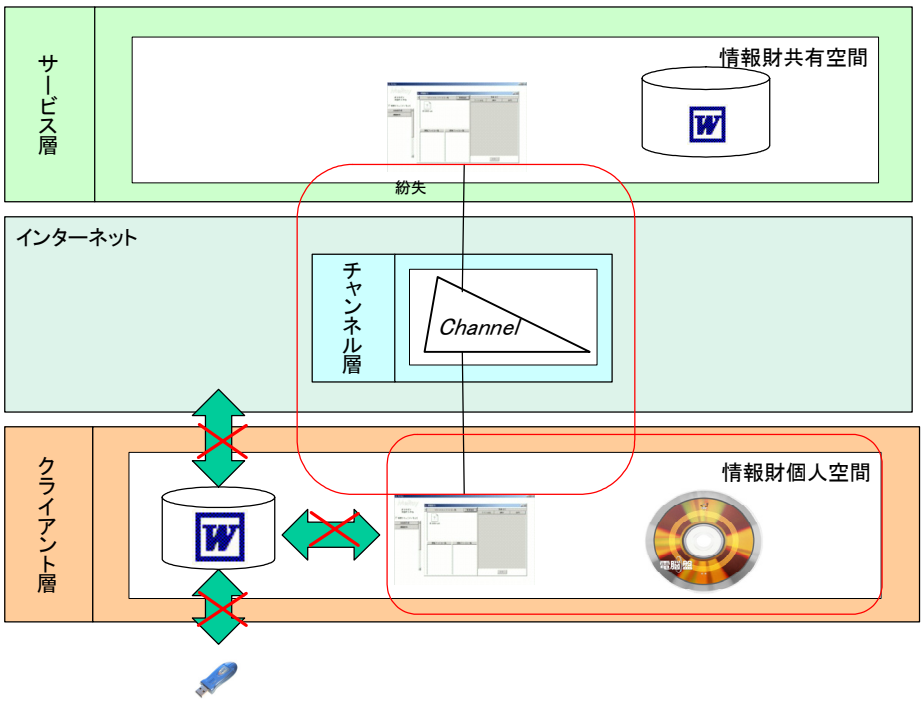


図 2.3.6-2　利用者認証後の状態

(2) 情報財の審査

情報共有空間へ情報財を登録、改変、破棄の操作時には、

- 情報共有空間のコンセプトに合致した内容か
- 既存の著作物の著作権や人格権が守られているか

などの観点で情報空間の責任者が審査し、審査に合格した情報財だけが公開される。

また、情報財の変遷は全て DB に記録され情報財のバージョンが管理される。

情報財のメタ情報として、ファイル名、ファイルサイズ、更新日時、証明年月日、寿命、閲覧可能時間、印刷可能枚数、更新日時が DB で管理される。

これらのメタデータは、登録、改変、破棄の操作時に記録される。

図 2.3.6-3 に情報財の登録、改変、破棄時の状態を示す。

図 2.3.6-4 から図 2.3.6-7 に情報財登録時の画面遷移を示す。

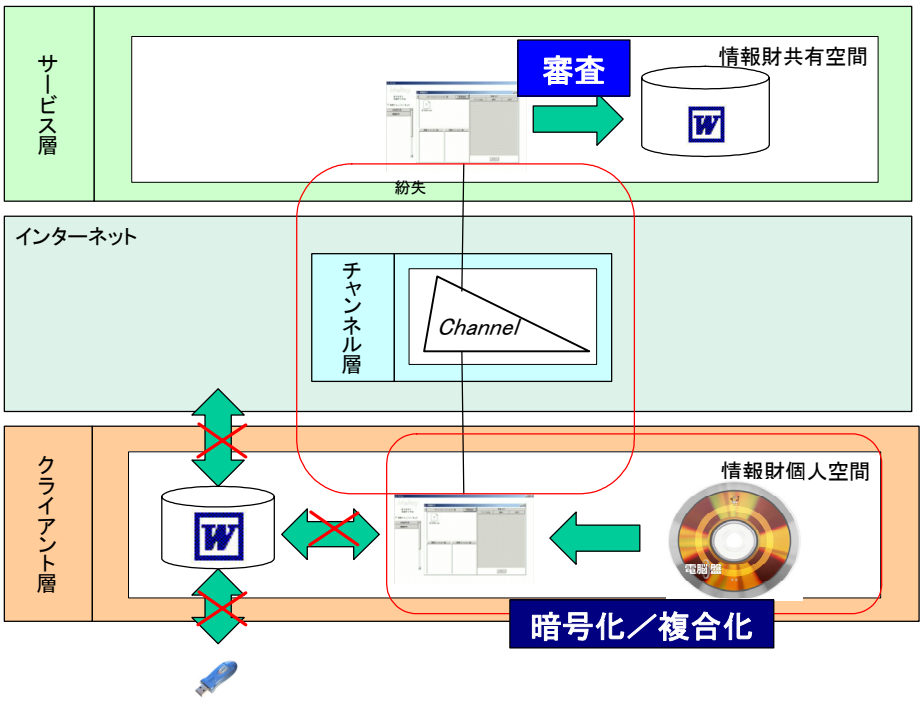


図 2.3.6-3　情報財の登録、改変、破棄時の状態

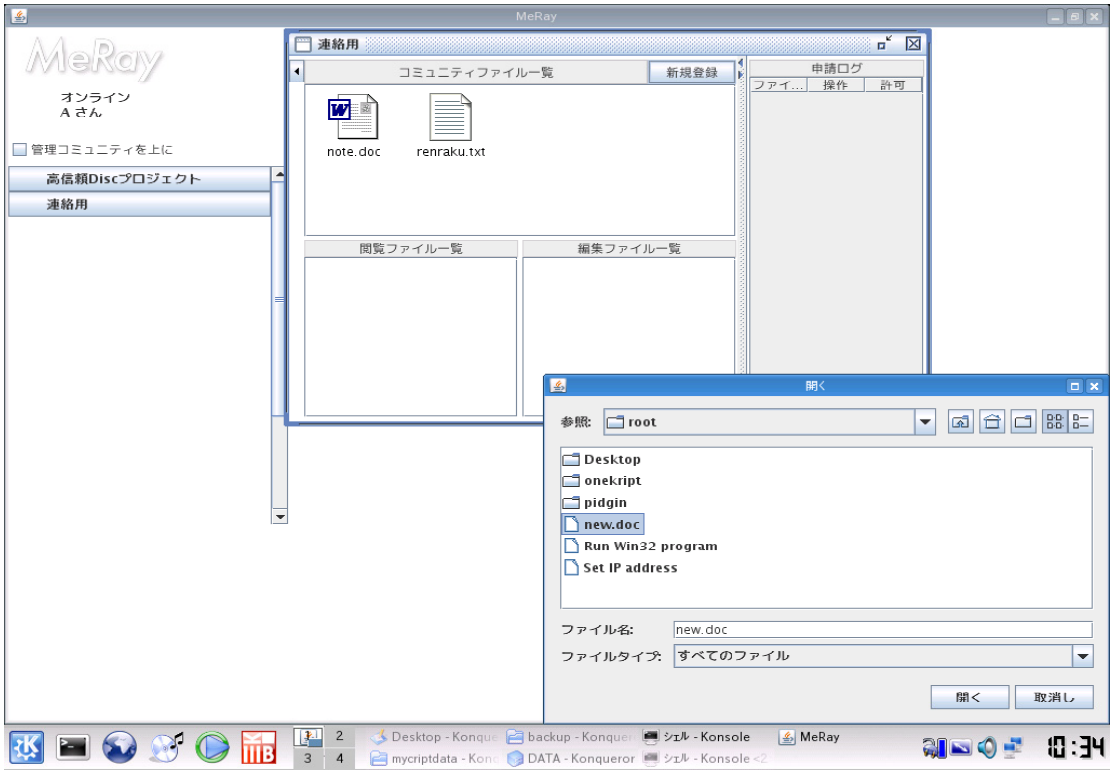


図 2.3.6-4　情報財登録選択操作時の画面

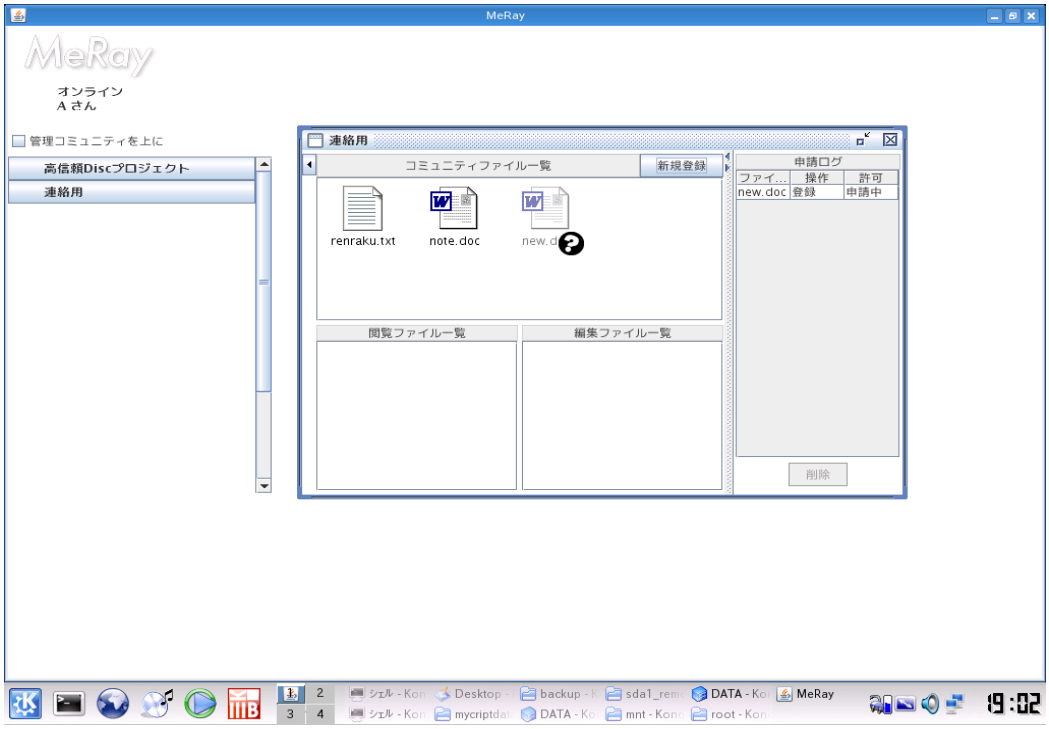


図 2.3.6-5　情報財登録申請中の画面

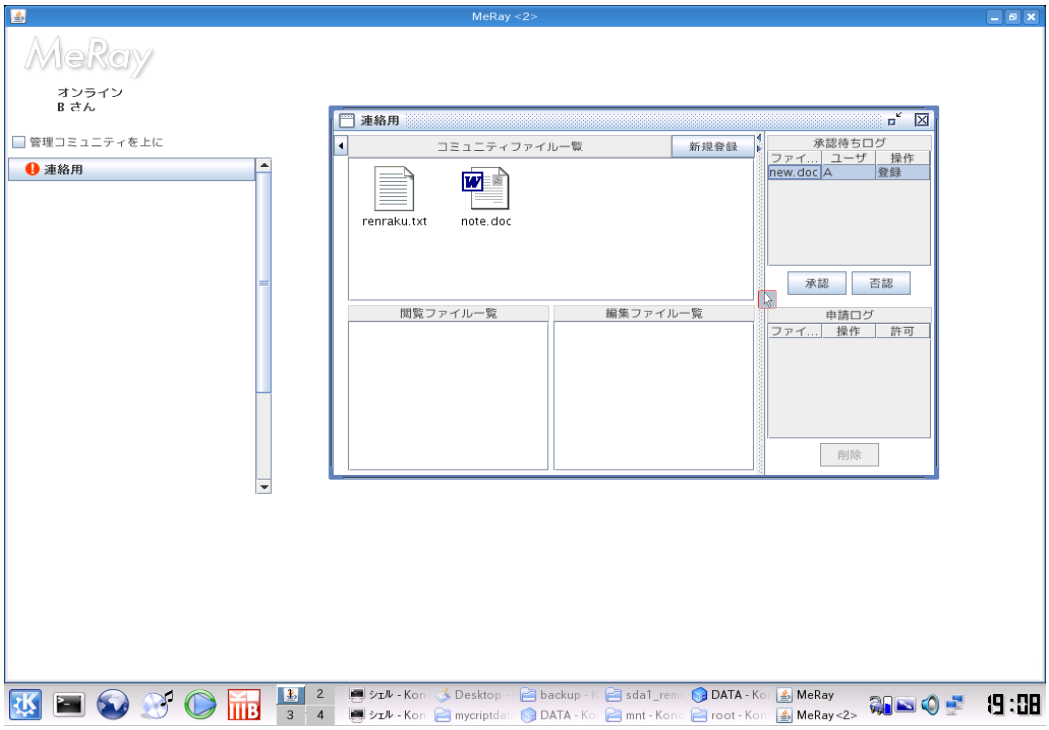


図 2.3.6-6　情報財登録審査の画面

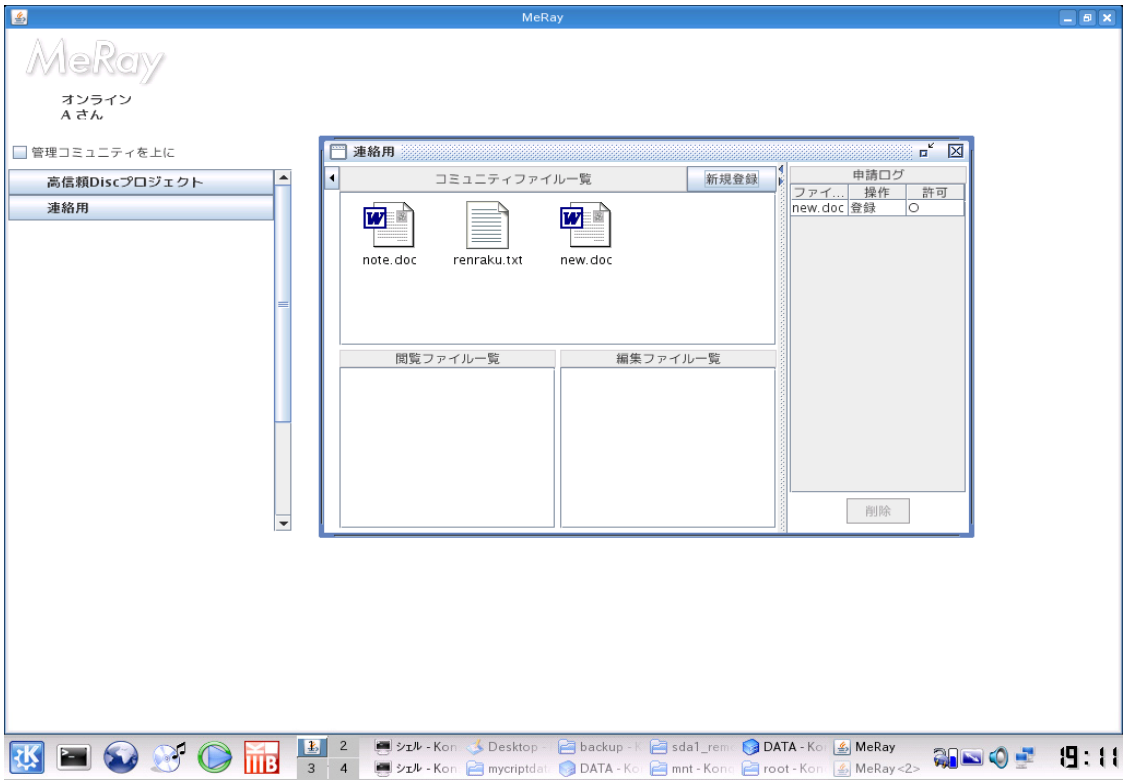


図 2.3.6-7　情報財登録完了査の画面

2.3.7　実証試験の評価

実証試験を行い、以下を確認した。

① ネットワークや外部機器からのコンテンツ流出防止

ＯＳ設定にて外部メディアのマウントを禁止し外部メディアによる不正流出を防止できた。また、ネットワークの接続は FACCIO のセッション管理により接続先が限定され、ネットワークからの不正流出を防止できた。

② コンテンツの分散管理

ストレージサービスサーバからダウンロードしたコンテンツは、暗号チップ搭載光ディスクのＲＡＭ領域に暗号化されて記録されることを確認した。

また、サーバと暗号チップ搭載光ディスクにコンテンツを分散保管できることを確認した。　両記録メディアに格納されたコンテンツの I/O 履歴はそれぞれ独立して管理されるので、改ざん行為の監視も可能である。

参考文献：

［1］山口　英，金野和弘：“ＤＲＭにおける脆弱性について”，情報処理　VOL.46　NO.6 643-647 （2005）

第３章　　実用化システムの課題と検討

3.1　ビジネス分野に於ける電子(化)文書などの保存・管理の課題

インターネットの普及とデジタル技術が融合した現代では、ビジネス分野に於ける電子(化)文書などの保存並びに管理に於いて、過去のアナログ時代には想定されなかった、別次元の課題と取り組む必要がある。

しかもそれらの課題は電子(化)文書のメリットの裏返しとしてのデメリットである。

よって此処に電子(化)文書のメリットとデメリットを列挙(図 3.1–1 参照)することにより、ビジネス分野に於ける電子(化)文書などの保存・管理の課題を浮き上がらせると共に、それらの課題に対する解決方策を提案する。

尚、ここでは便宜的に、紙文書をスキャンしてイメージデータ化した電子化文書と、当初から電子データである電子文書を総称して「電子(化)文書」と称する。

3.1.1　電子(化)文書のメリット

① 保存場所をとらず、保存コストが軽減される

膨大な資料のスペースを効率よく活用をするために、パソコンから紙媒体に印刷せずに直接電子媒体に出力する。

既に紙媒体に印刷されている文書はスキャニングでデジタルデータに変換し、電子媒体に保存する。

その形式のままでの長期保存が可能になればこれまで必要だった紙文書の書類保管スペースは必要無くなり、保存コストの削減につながる。

② 離れた場所での文書のやりとりが迅速かつ低コスト

電子化により、様々な人の閲覧が可能になる。

また、情報に高度なセキュリティやパスワードなどを設定することができるので、情報の閲覧を制限することも可能になり、情報漏洩防止などセキュリティ対策の強化を図ることができる。

③ 保管された文書の中からほしい情報を簡単に検索

電子化した文書に目次やページ数をつけて管理することで必要なデータの検索が容易にできるようになり、文書データの損失・散在による再利用の非効率化を防ぎ、業務のスピードアップや合理化によるコスト削減が可能となる。

④ 低コスト、短時間、かつ大量に複製が可能

紙媒体から複製を作成する場合は物理的複製を繰り返すことになるので、時間と手間とコストが嵩むことになる。

一方、電子(化)文書の場合は、紙媒体に換算すれば数百ページに及ぶような大容量のデータであれ、また同一文書を大量に複製する場合であれ、低コスト且つ短時間で複製の作成が

可能である。

⑤ 保存記録のバックアップや別地分散管理が容易となり、災害への対応力が向上する

電子(化)文書の大半は一枚の記録型ＤＶＤに収まることから、長期保存の記憶媒体は少なくとも正、副２式を作成し、不測の事態に備える必要がある。

尚、不慮の災害に備え、１式は同一災害が及ばない遠隔地（別地）に分散保存することが望ましい。

⑥ 過去の文書を容易に再利用でき、効率的な新規文書作成が可能

電子文書であれば、過去の文書を容易に編集・加工することができる。

例えば、過去の文書の一部をコピーし文字のフォントやサイズを変更して新たな文書の一部として貼り付けることにより、効率的に新規文書を作成することが可能になる（電子化文書であっても、電子データから直接、ＰＤＦなどでイメージ化した場合は、容易に編集・加工可能)。

⑦ 多数の送付先への文書配信が手軽

１９８０年代迄は、商社や外務省などでは大型コンピュータを用いたテレックス網を国内外に張り巡らせることにより、多数の相手先に対し文書を瞬時に同報し情報の共有化を図ってきた。

一方、斯かる大規模な情報化投資に耐えられない一般の企業や個人の間では主にファックスが文書配信の手段として用いられてきたが、ファックスは一回の文書配信毎に一つの電話回線を占有することから効率が悪く、多数の送付先への文書配信は時間と通信費用が嵩む逐次同報しか手段が無かった。

この状況を一変させたのが電子メールの登場である。パソコンとインターネットの普及により、一般の家庭から世界中の送付先へ瞬時に電子メールを同報し、情報を共有化することが可能になった。

⑧ 技術革新の速度が相対的に早い

Windows95 の時代にはインターネットへの接続に特別な技術が求められたことから、インターネットはまだ一般の人々にはなじみの薄い技術であった。

その後、Windows98 から Windows XP に至る１０年間の Windows OS の変遷の課程に於いて、最も劇的に改善したのはインターネットへの接続が簡単にできるようになったと言う点である。

また、ネットへ接続する回線自体もこの１０年の間にダイヤルアップによるナローバンドから ADSL や光ファイバーによるブロードバンドへ進化し、接続料金も割高な従量課金から安価な定額制へと移行した。

わずか１０年の間に、技術的にも料金体系的にも斯かる劇的変遷を遂げた情報通信技術は未だ嘗てない。

斯かる劇的な技術革新と料金体系の変遷こそが現在のインターネットの普及をもたらしたことは言を待たない。

3.1.2　電子(化)文書のデメリットと課題の抽出（太字／アンダーライン付）

① 直接目にすることができず、表示装置やプリントアウト行為などが必要

電子(化)文書は、パソコンやディスプレイなどの装置がなければ見ることができない。

従って電子(化)文書を保存している企業では、例えば税務調査の際などに、必要とする文書をすぐに目に見えるような明瞭な状態でディスプレイやプリンタに出力し、確認できるようにしておかなければならないが、このことを見読性の確保と言う。

具体的な要件となるのは、例えばイメージスキャナの階調や解像度の設定であり、カラーで読み取る際には 256 階調で 150dpi 以上が目安となる。

② 改ざんやすり替えなどの不正行為の痕跡が残りにくい

電子(化)文書は、痕跡を残さずに改ざんできる、コピーを容易に作成できる、ファイルの日付を書き換えることができるといった、紙文書にはない特性を備えている。

従って電子(化)文書を保存している企業では、電子(化)文書が事故や操作ミスによって消去してしまうことを防止し、改ざんや消去があった事実を確認できるようにしておかなければならないが、このことを**完全性の確保**と言う。

③ 複製などにより短時間且つ広範囲に、大規模な情報漏洩が起こりうる

電子(化)文書の完全性を確保するためには、許可した人以外はアクセスできないといった管理が必要になるが、そこで求められるのが**機密性の確保**である。

従って電子(化)文書を保存している企業では、完全性と機密性を確保し、適切で安全な文書管理を実現する上で「いつ、誰が、どの電子(化)文書にアクセスしたか」を確実に把握していることが重要になる。

④ 長期保存の場合、文書データの消失や互換性喪失の虞がある

電子(化)文書を数十年単位で長期保存する場合、ＯＳやアプリケーション並びに暗号アルゴリズムの陳腐化により、復元性の喪失をきたす虞がある。

このことは、Windows95 で作成された電子(化)文書が Windows XP や Windows Vista で復元できないケースが多発していることからも明らかである。

従って電子(化)文書を保存している企業では、長期保存用記憶媒体に対し物理的復元可能性のみならず、**論理的復元可能性**も同時に確保する必要がある。

⑤ イメージ化文書の場合、スキャニングに伴う情報の劣化などが起こりうる

スキャンして作成する電子化文書の見読性には、2 つの観点がある。

1 つは、スキャンしたものをコンピュータ上で表示したり、印刷したりした場合に、元の紙文書に書いてあった必要な情報が読めるようにしなければならないという点であるが、これは一般的レベルの見読性さえ確保していれば十分である。

ここで問題になるのは、もう一方の　観点である「元の紙文書に改ざんがなかったかを後から検証できる程度に鮮明にスキャンしなければならない」という点である。

即ち、改ざんが問題となるような文書については、紙文書の状態で改ざんされた場合の

改ざん痕がわかる程度の色数や階調、及び解像度でスキャンすることが求められる。

例えば、紙文書に手書きで書かれた数字が改ざんされていないかを検証する場合、いろいろなやり方が考えられるが、余分な数字を書き加えられていないかを判定するには、筆跡の違いがわかる程度の解像度が必要である。

場合によっては、使用されたインクの色の違いがわかる程度の色数を再現する必要さえある。

また､修正液で消したり､その上に別の数字を書かれていたりしないかを判定するには、使用している紙文書の紙色に対して修正液の色の違いがわかる程度の、色数と解像度が求められることになる。

従って原本性の確保が求められる文書をイメージ化して保存している企業に於いては、高解像度でスキャンすることに伴う大容量データを、長期保存可能な大容量の記憶媒体が不可欠と言える。

⑥ 情報管理システム導入などに、初期投資が必要となる

電子(化)文書は、必要に応じてすぐに確認できるように管理しなければ活用することができない。

そこで求められるのが、文書をインデックスで検索し表示する情報管理システムなどを整備しておくことが求められる（このことを検索性の確保と言う）。

従って電子(化)文書を保存している企業では、ファイル名だけではなく、業務形態に応じて、例えば契約日時といったインデックスで検索できるように情報システムを整備しておく必要があることから、初期投資が必要となる。

⑦ HDD は、扱いを誤ると瞬時に情報が消滅する危険性がある

HDD は故障が多く、一旦トラブルが起こると瞬時に情報が消滅する危険性がある。

また HDD は、緻密な回転機構を有する精密機械であり、長期間通電しない状態で保存すると潤滑油その他の劣化により、使用不可能になる可能性が高い。

従って HDD は長期保存用記憶媒体としては物理的復元可能性に欠けると同時に、メディア自体が重く嵩張ることから可搬性に乏しく、データの完全消去が困難であり、廃棄した HDD から情報が漏洩する危険性を内在している。

3.1.3　シンクライアントシステムに於いて、電子(化)文書を長期保存する場合の課題

① シンクライアントシステムが注目される背景：

情報漏洩防止の観点から近年、大企業を中心に HDD を有しないシンクライアント端末が普及し始めた。

即ち、企業内で管理している個人情報などが外部に流出する事件が多発し、これの対策に企業は取り組むようになってきたが、多数の社員が使うパソコンに重要情報が保存されている現状ではセキュリティ対策が困難である一方、シンクライアントの、端末側にデータを残さない特性が、情報漏洩対策に効果的であるとして注目を集めるようになった。

また、シンクライアントシステムではソフトウェアの更新やメンテナンスを一括管理できることから、TOC (Total Cost of Ownership)を削減できる点も注目されている。

② シンクライアントシステムに於いて、電子(化)文書を長期保存する場合の課題：

電子(化)文書の長期保存に於いては、本報告書 3.1.2「電子(化)文書のデメリットと課題の抽出（太字／アンダーライン付)」の④「長期保存の場合、文書データの消失や互換性喪失の虞がある」の項でも言及したとおり、ＯＳやアプリケーション並びに暗号アルゴリズムの陳腐化により、復元性の喪失をきたす虞がある。

一方、シンクライアントシステムの欠点としてよく挙げられる課題に「アプリケーションの互換性の欠如」がある。

即ち、シンクライアントシステムに於いては、ユーザが社内で過去に開発したアプリケーションは、そのままでは動作しない可能性が高い。

さらに、市販のサードパーティ製ソフトウェアは、元々、ライセンスの関係から複数のユーザを想定して設計／開発されていないので、アプリケーションが独自に単一のＰＣ上での多重起動を制限していたり、ローカルシステム上の特定の名前のファイルにユーザ設定を書き込む仕組みになっていたりするケースが多く、個々のユーザに対応したエントリを持つことができない構成になっている。

従って、シンクライアントシステムに適合させる為にはプログラムを書き換える必要がある。

然るに、数十年単位の長期保存となるとシンクライアントシステム自体が全く別のものに変わっている可能性が高く、数十年前のＯＳ、アプリケーション、暗号アルゴリズム、などで構成されたレガシーシステムとの互換性を長期間保持することは非現実的と言える（因みに、社会保険庁は数十年前の極めて非効率なレガシーシステムを保持する為に、年間数百億円単位の費用を投じており、国会で問題になったことは記憶に新しい)。

3.1.4 課題と解決方策

課題その①：見読性の確保（図 3.1.4-1 参照）

見読性とは、必要に応じ電子(化)文書に記録された事項（スキャナで読み取ることにより作成された場合には、必要とされる程度の色数や階調、及び解像度で読み取られた書面の内容）を出力することにより、直ちに整然とした形式及び明瞭な状態で使用に係るコンピュータその他の機器に表示し、書面を作成できること。

解決方策：

保存義務のある情報の見読性が確保されている要件として、情報の内容を必要に応じて肉眼で見読可能な状態に容易にできること、及び情報の内容を必要に応じて直ちに書面に表示できることが、制度上求められる。

例えば、長期保存する電子(化)文書がいつでも見読できるようにするため、文書管理者は、文書管理規定に保存の規定を定義し、それが規定どおり実施されているか１年ごとに監査することなどが求められる。

また、電子媒体に保存された情報は、電子媒体から取り出すのに何らかのアプリケーションが必要であり、表示の為の編集前提となるマスター、利用者テーブルなどが別に存在したりする可能性がある。

これらの見読化手段が日常的に、必要に応じて、必要な場所で、正常に動作することが求められるが、OS、アプリケーション、セキュリティアルゴリズム、などを自己完結的に内蔵した高度暗号チップ搭載光ディスクは、HDD を取り外したフリーアドレス型パソコンがインフラとして整備された環境に於いては、ディスク一枚でこの見読性を充足することができる。

さらに、肉眼で見読可能な状態に容易にできる状態に保つ為の具体的な要件となるのは、例えばイメージスキャナの階調や解像度の設定であり、カラーで読み取る際には 256 階調で 150dpi 以上が目安となる。

従って、大容量の長期保存用記憶媒体が必要となる。

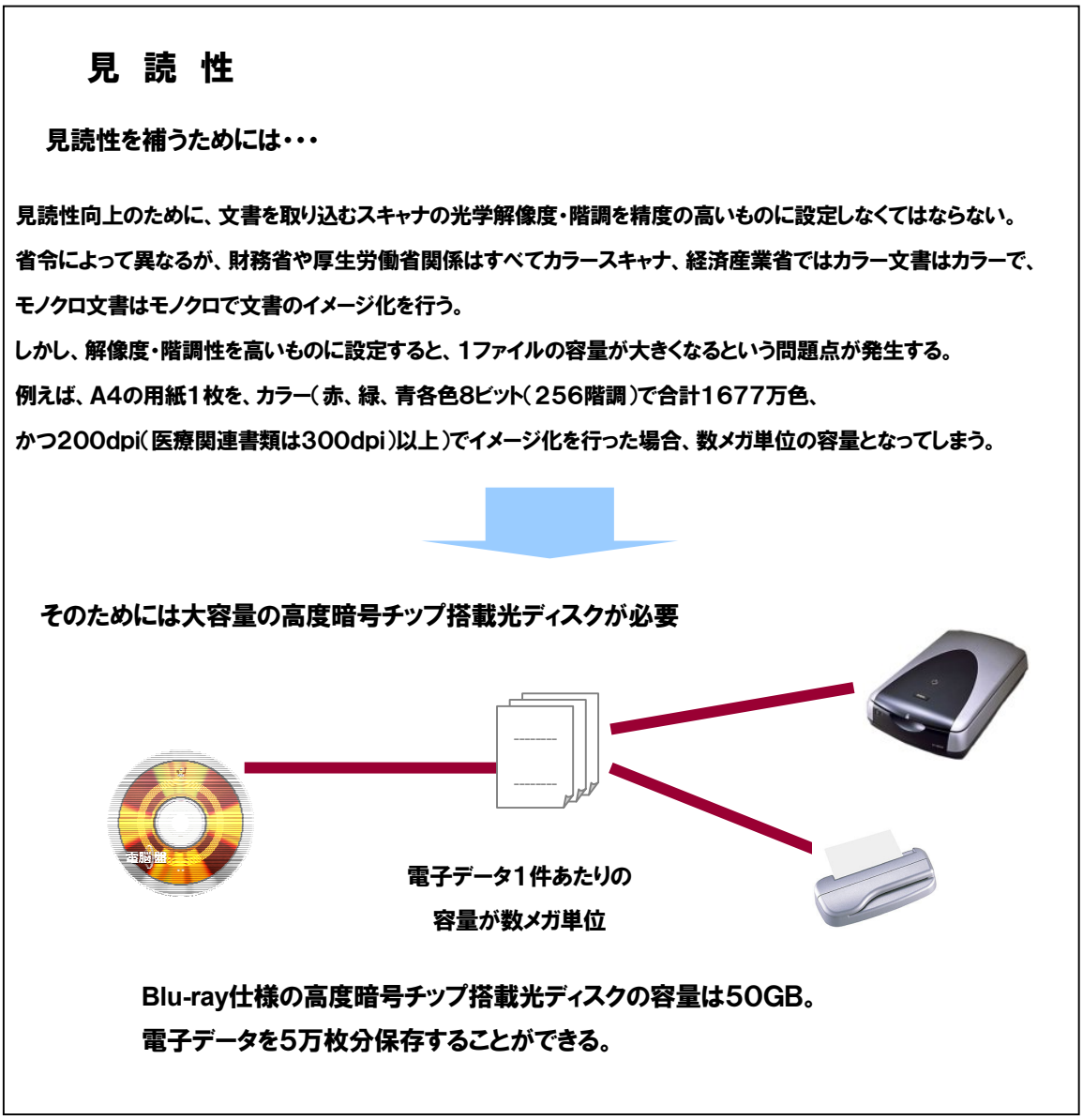


図 3.1.4-1　見読性を確保するためには大容量の長期保存用記憶媒体が必要

課題その②：完全性の確保

完全性の要件は次の３点である。即ち、

完全性の要件１：電子(化)文書に記録された事項が保存義務期間中に滅失し、または毀損することを防止する措置を講じていること。

完全性の要件２：電子(化)文書に記録された事項について、保存義務期間の間に於いて当該記録事項の改変または当該電磁的記録の消去の有無またはその内容を確認することができる措置を講じていること。

完全性の要件３：電子(化)文書に記録された事項について、保存義務期間の間に於いて当該記

録事項の改変または当該電子ファイルの消去を抑止する措置を講じていること。

解決方策：

要件１の災害対策に関しては、長期保存の記憶媒体を少なくとも正、副２式を作成し、不測の事態に備える必要がある。

尚、不慮の災害に備え、１式は同一災害が及ばない遠隔地（別地）に分散保存（図3.1.4-2 参照）することが望ましいとされているが、この要件は2.2アプリケーションシステムに於いて詳述したとおり、東京電力のFACCIOと高度暗号チップ搭載光ディスクの組み合わせで解決可能である。

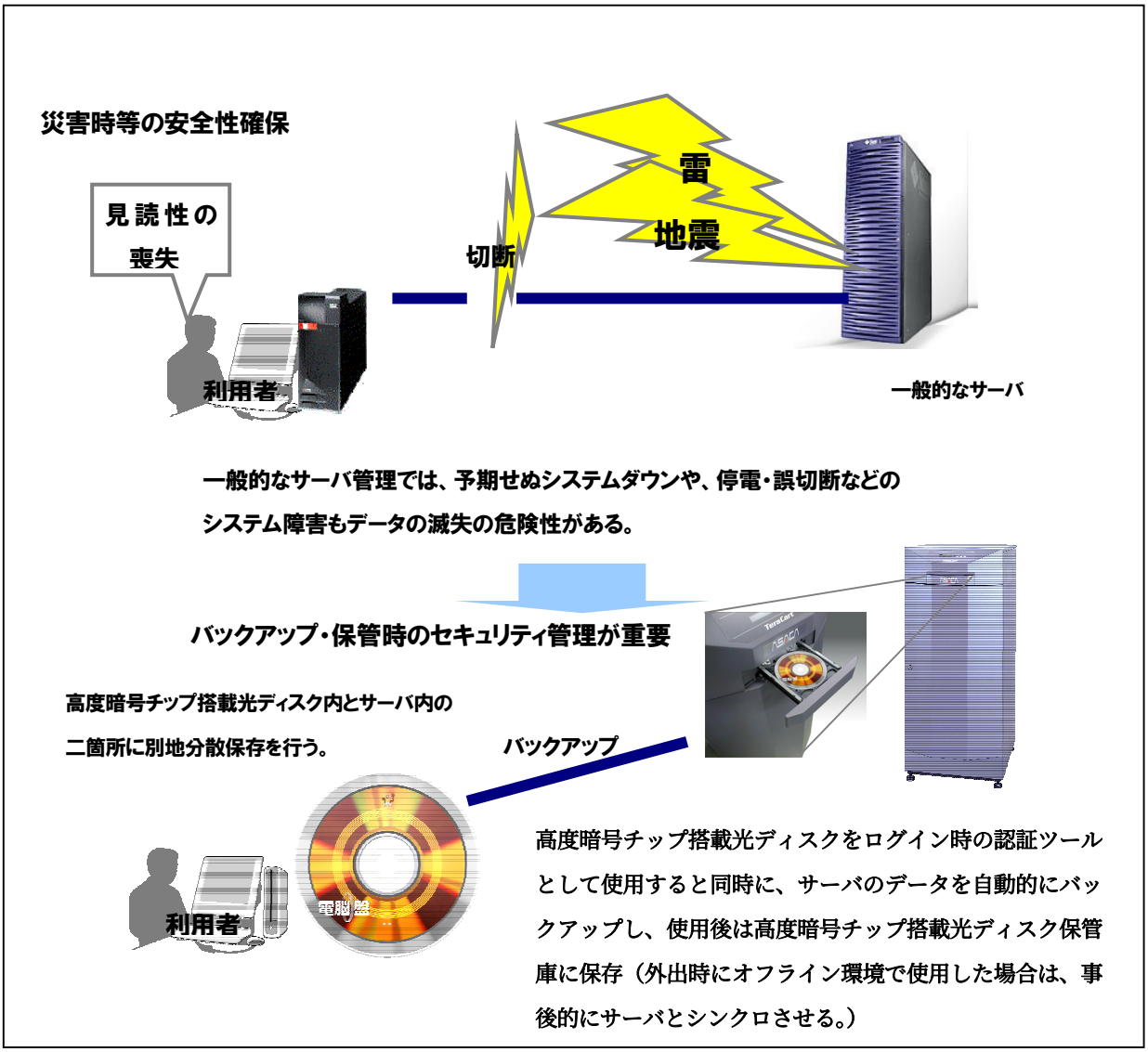


図 3.1.4-2　不慮の災害に備え別地に分散保存

解決方策：

要件２と要件３の改ざん履歴の確認及び改ざんの抑止（図 3.1.4-3 参照）に関しては、タイムスタンプ及び電子署名に加えて、電子データ自体の、例えば、ハッシュ値を高度暗号チップ搭載光ディスクに搭載された**高度暗号チップ**が自律的に管理することにより実現可能。

因みに、タイムスタンプ並びに電子署名は有効期限があるので、電子(化)文書の長期保存用媒体自体が自律的に電子データ自体のハッシュ値を管理することは、長期保存電子(化)文書の原本性を確保することにもつながる。

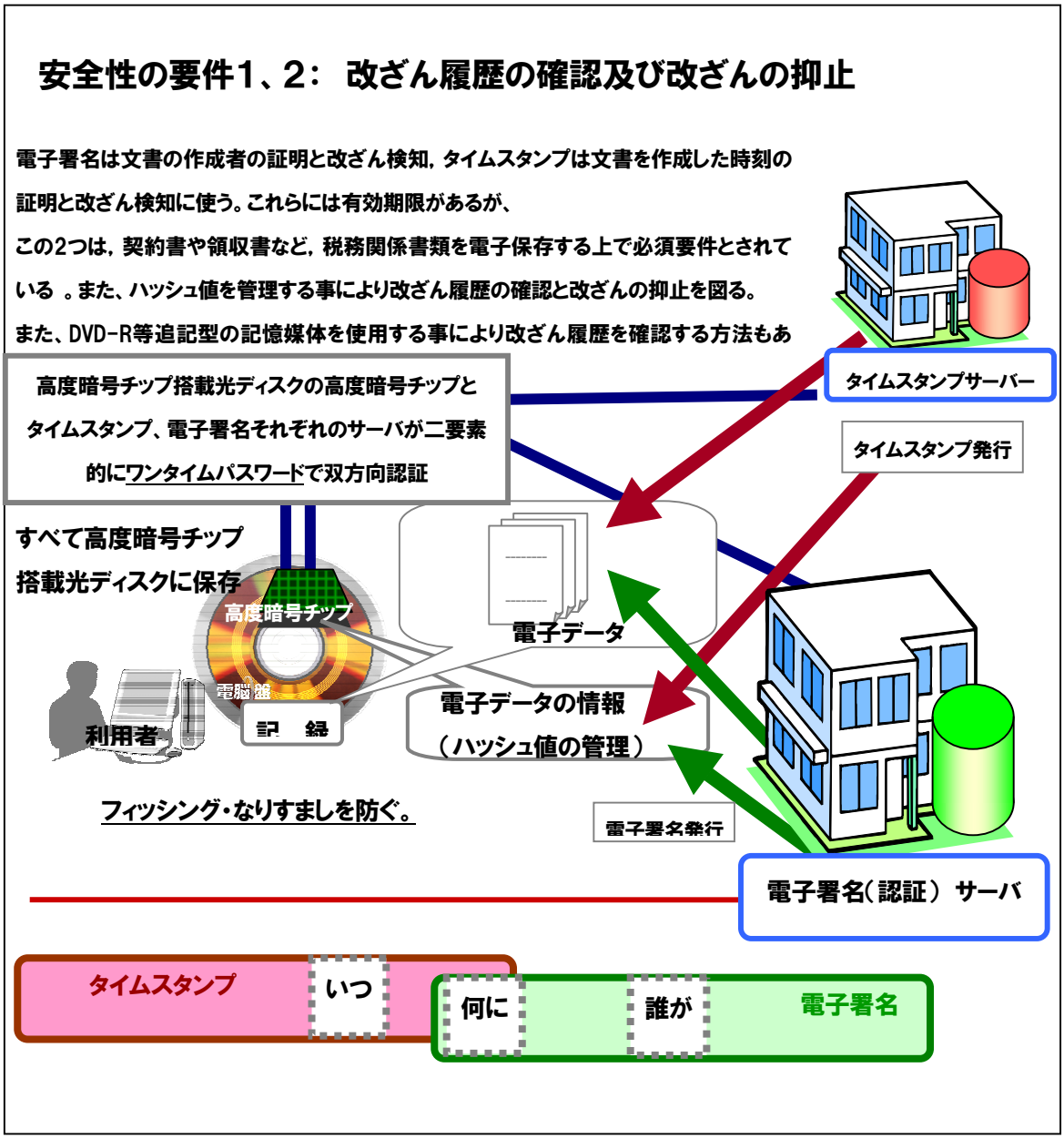


図 3.1.4-3　改ざん履歴の確認及び改ざんの抑止

課題その③：機密性の確保（図 3.1.4-4 参照）

電子(化)文書の完全性を確保するためには、許可した人以外はアクセスできないといった管理が必要となる。

そこで求められるのが機密性と完全性の確保である。

解決方策：

高度暗号チップ搭載光ディスクの高度暗号チップが自律的に利用者を認証し、利用許可を得ている専用ドライブを認証すると共に、電子データ自体のハッシュ値を管理することにより原本性を確保する機能を備えた、東京電力のFACCIO（2.2 アプリケーションシステム参照）と高度暗号チップ搭載光ディスクの組み合わせで解決可能である。

即ち、高度暗号チップ搭載光ディスクが、自律的にユーザを認証すると同時に、FACCIOサーバとの間で、ワンタイムパスワードなどを用いて、高度暗号チップ搭載光ディスクとFACCIOサーバを、相互に認証する。

また、高度暗号チップ搭載光ディスクは、専用ドライブのリーダ・ライタに組み込まれたマイコンのＩＤを認証することも可能であり、許可されたＩＤ番号を持つ専用ドライブだけでしか高度暗号チップ搭載光ディスクにアクセスできないように仕組むことができる。

さらに、専用ドライブにロケーションスタンプ機能を組み込むことにより、決められた場所でしか使用できないように仕組むこともできる。

これらの機能を組み合わせることにより、電子(化)文書の機密性と完全性を確保することが可能になる。

機密性並びに完全性及び原本性の確保

セキュリティの問題点

保存される電子(化)文書の中には、他者のプライバシー情報や営業秘密等、公開になじまない性質のものもある。この場合大量の電子(化)文書が盗み見られ、漏洩が発生することによりプライバシーの侵害などが生じる恐れがあり得る。また保存用の記憶媒体を保管場所から持ち出す不正行為を防止することも重要な要件となり得る。 従って、電子(化)文書に於いては、機密性と完全性の確保が重要になる。
そのためシステムへの不正なアクセス及びデータの不正な変更を発見する為の電子書名とタイムスタンプが必要となるが、タイムスタンプ並びに電子署名は有効期限があるので、電子(化)文書の長期保存用媒体自体が自律的に電子データ自体のハッシュ値を管理する事は、長期保存電子(化)文書の原本性を確保する事にもつながる。

セキュリティ	利用者をいかに認証し、管理するかが重要(例:生体認証)

生体認証

高度暗号チップ搭載光ディスクシステム自体が、自律的に生体認証を行い、閲覧を可能にする。

保管場所からの持ち出し	IT化による対応 (例:高度暗号チップによる管理)

社外に高度暗号チップ搭載光ディスクを不正に持ち出されても、高度暗号チップ搭載光ディスクの高度暗号チップが、利用許可を得ている専用ドライブ(不正持ち出し防止機能搭載)内のR/Wに組み込まれたIDを、自律的に認証するので、不正使用ができない。

履歴の管理	タイムスタンプ、電子署名に加えて高度暗号チップ搭載光ディスクの高度暗号チップが、電子データ自体のハッシュ値を自律的に管理する事により電子(化)文書の原本性を確保

図3.1.4-4　機密性並びに原本性の確保

課題その④：長期保存用記憶媒体の物理的並びに論理的復元可能性（図 3.1.4-5 参照）

長期保存用記憶媒体は、経年変化による劣化に耐え物理的復元可能性を保持することと同時に、ＯＳやアプリケーションの変遷に影響されない、論理的復元可能性も求められる。

解決方策：100 年を超す長期保存性が立証されている長寿命光ディスクをベースにした高度暗号チップ搭載光ディスクに、Linux OS とアプリケーションを自己完結的に収納（タイムカプセル化）することにより、OS や暗号アルゴリズムの陳腐化による復元性の喪失を防ぐことができる。但し、タイムカプセル化した電子(化)文書の長期保存用記憶媒体は、PC のチップセットなどに対応したハードウエアドライバーを一定期間毎にアップデートする必要がある。また、超長期間の保存に際しては、長期保存対象電子(化)文書の保管部署毎に一定台数の互換性確認済 PC を同時に保存する必要があるかも知れない。その場合でも、記憶媒体の数からすれば極めて少ない台数の PC で済むはずである。

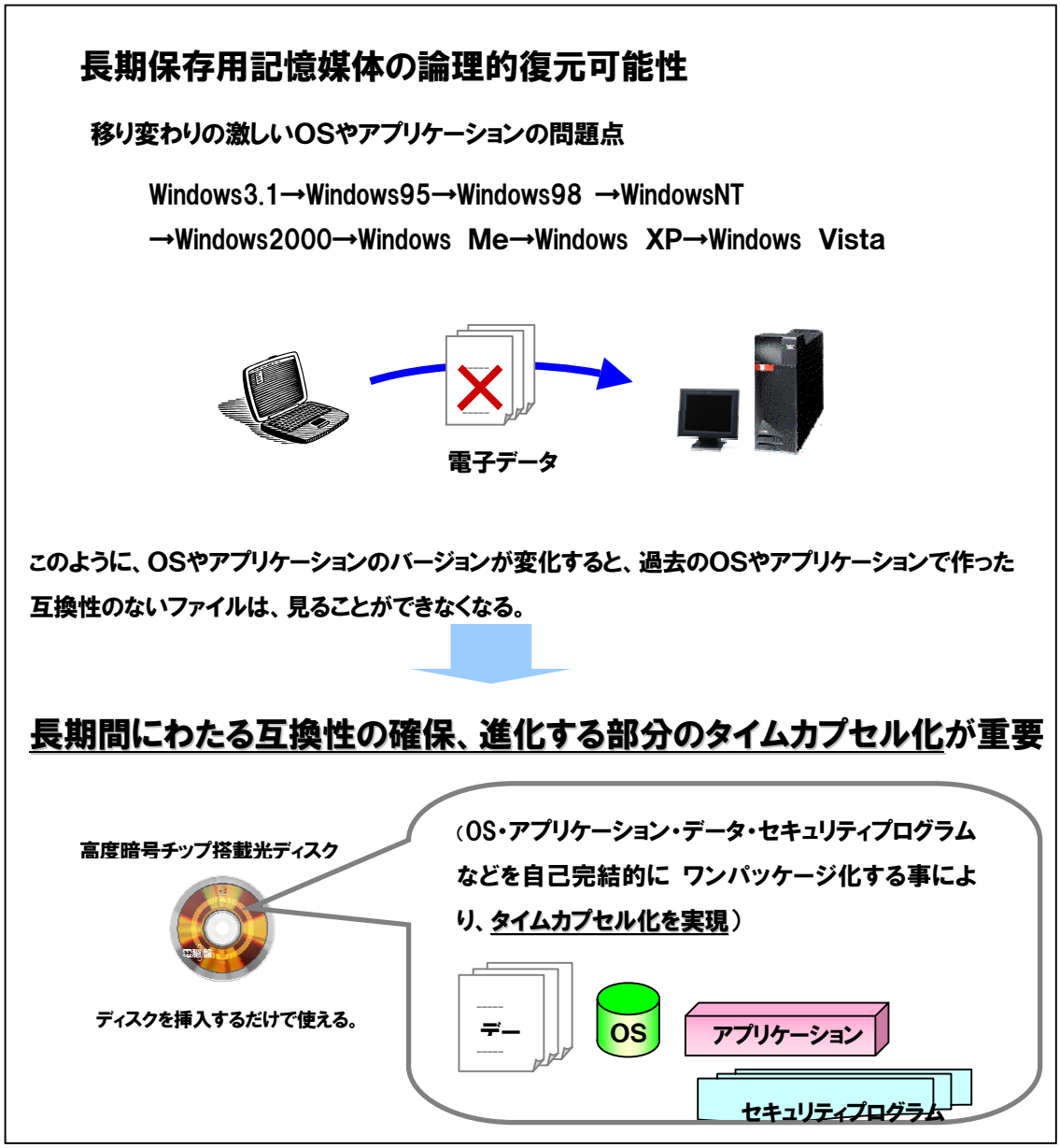


図 3.1.4-5　　長期保存用記憶媒体の論理的復元可能性

課題その⑤：イメージ化文書に於ける原本性の確保

改ざんが問題となるような文書については、紙文書の状態で改ざんされた場合の改ざん痕がわかる程度の色数（報告書では階調）や解像度でスキャンすることが求められる。

しかしながら、スキャンした後の画像データに対して画像加工を施して改ざんする場合、元の紙文書なしに、最終的な電子化文書だけで必ず見破るというのは技術的に極めて困難である。

また、デジタルデータ（例えば、Word 文書）から直接イメージ化した電子化文書（例えば、ＰＤＦなど）の場合、容易にデジタルデータに戻し改ざんすることができる。

改ざん後に再度イメージ化すれば、改ざんを見破るのはかなり困難である。

解決方策：

原本性の確保を求められる文書の改ざん履歴の確認及び改ざんの抑止に関しては、例えば財務省や厚生労働省関係はすべてカラースキャナ、経済産業省ではカラー文書はカラーで、モノクロ文書はモノクロで文書のイメージ化を行うことを求めている。

しかし、解像度・階調性を高いものに設定すると、１ファイルの容量が大きくなるという問題が発生する。

例えば、Ａ４の用紙１枚を、カラー（赤、緑、青各色８ビット（２５６階調）で合計１６７７万色、かつ２００ｄｐｉ（医療関連書類は３００ｄｐｉ）以上）でイメージ化を行った場合、数メガ単位の容量となってしまう。

しかも電子(化)文書は、一期分を一枚の電子媒体に保存することが望ましいとされている。

従って、原本性の確保を求められる文書をスキャンしてイメージ化した電子化文書の場合、少なくとも７～８ＧＢ以上の大容量高度暗号チップ搭載光ディスクを用いて保存することが望ましい。

また、電子化したイメージ化文書の原本性確保は、タイムスタンプ及び電子署名に加えて、電子データ自体のハッシュ値を高度暗号チップ搭載光ディスクに搭載された**高度暗号チップ**が自律的に管理することにより実現可能。因みに、タイムスタンプ並びに電子署名は有効期限があるので、電子(化)文書の長期保存用媒体自体が自律的に電子データ自体のハッシュ値を管理することは、**長期保存電子(化)文書の原本性を確保**することにもつながる。

上表では、「1」に「く」のような書き加えをして「4」に改変、「3」に「ε」のような書き加えをして「8」に改変、）「5」を修正液で消した上に文字を新しく書いて「9」に改変している
上記の改変の有無を、スキャンした画像から判定できるかを確認するために、改変した紙面のスキャン要件をさまざまに変更した

２００４年に経済産業省の「文書の電磁的保存などに関する検討委員会」がまとめた報告書で示している色数や解像度（モノクロ 2 値 200dpi／モノクロ中間調 150dpi／カラー24bit 150dpi）は、これらの改ざん痕を知るためには明らかに不十分といえる。

逆に言うと、改ざんの有無を確認する必要があるような文書については、個別により厳しい条件が示されると考えるか、スキャンした元の紙文書を保管しておく必要が出てくる。

課題その⑥：検索性と完全性の両立（図 3.1.4-6-Ⅰ、Ⅱ 参照）

多量の電子(化)文書が蓄積されている場合、正当なアクセス権限者が必要な電子(化)文書を簡単に見つけ出せる環境整備が必要である。

そのため情報システムの検索機能を活用し、電子(化)文書の検索を必要に応じ行えるための規則体系及び体制が必要となり、初期投資が必要となる。

また、CD-R、ハードディスクといった記憶媒体は、経年劣化する。

そのため媒体の損壊により、保管している電子(化)文書が滅失または毀損してしまう恐れがある。

さらに、予期せぬシステムダウンや、停電・誤切断などのシステム障害による滅失の危険も想定する必要がある。

そのため保存義務が課されている期間を通じて、必要に応じバックアップを行い、元の保管場所とは異なる場所に保管し、原本性と作成者の特定をするための電子署名、作成日を特定するためのタイムスタンプを行う必要がある。

解決方策：

経年劣化の問題は長期保存に適した高度暗号チップ搭載光ディスクを用いることにより解決可能である。

むしろ問題になるのは保存義務が課されている期間を通じて長期保存の記憶媒体を別地に分散保存することの実践可能性である。

電子(化)文書の保存・管理は日常業務にビルトインされることになる、従って、実務担当者への負担が少なく、経済合理性に適った電子(化)文書の保存・管理システムを構築することが望まれるが、FACCIO＋高度暗号チップ搭載光ディスクを用いた情報管理システムは次のような特徴を有する。

即ち、FACCIO サーバへのログイン管理は、高度暗号チップ搭載光ディスクの高度暗号チップが自律的にユーザを認証することにより実現する。

また、コンピューティングパワーが必要なデータ処理は FACCIO サーバ側で行い、結果を FACCIO サーバ側と高度暗号チップ搭載光ディスク側に別地分散保存する。

FACCIO サーバに於ける電子(化)文書の保存は高度暗号チップ搭載光ディスクのバックアップと位置づけ、年単位の保存期間（必要に応じて FACCIO サーバ側でも長期保存用のバックアップディスクを作成）とし、高度暗号チップ搭載光ディスクへの電子(化)文書の保存期間は、法令の定める期間とする（数年～数十年／ＯＳやアプリケーションを内蔵しタイムカプセル化）。

さらに、電子化したイメージ化文書の原本性確保は、タイムスタンプ及び電子署名に加えて電子データ自体のハッシュ値を高度暗号チップ搭載光ディスクに搭載された高度暗号チップ

が自律的に管理することにより実現可能。

しかも、FACCIO＋高度暗号チップ搭載光ディスクを用いた情報管理システムは、大規模なシステム構築を必要としないので初期投資が軽減される上に、ＯＳやアプリケーションの大半は無償の Linux で構成されるので TOC (Total Cost of Ownership)が極めて低い。

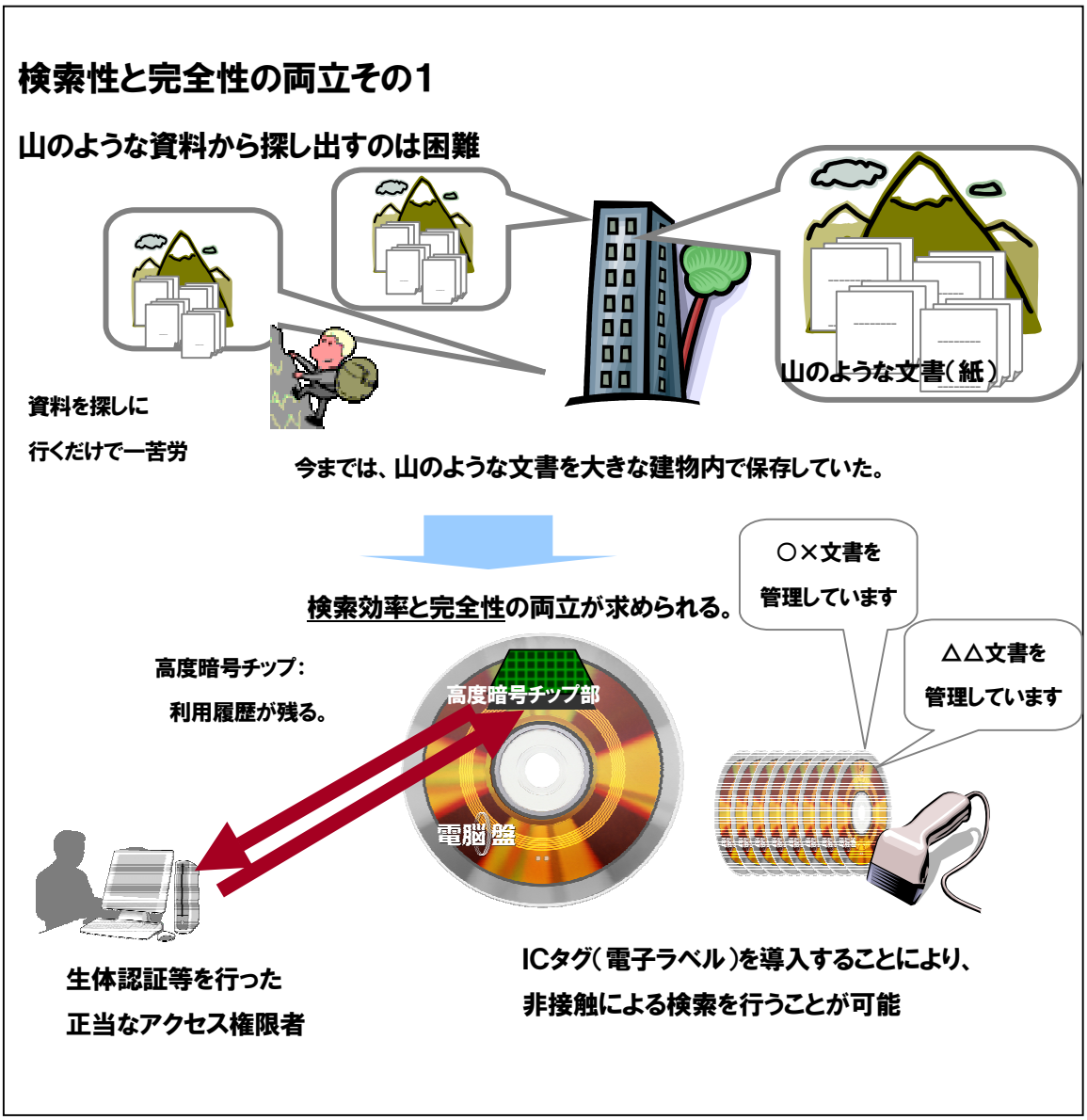


図 3.1.4-6- Ⅰ　検索性と完全性の両立その１

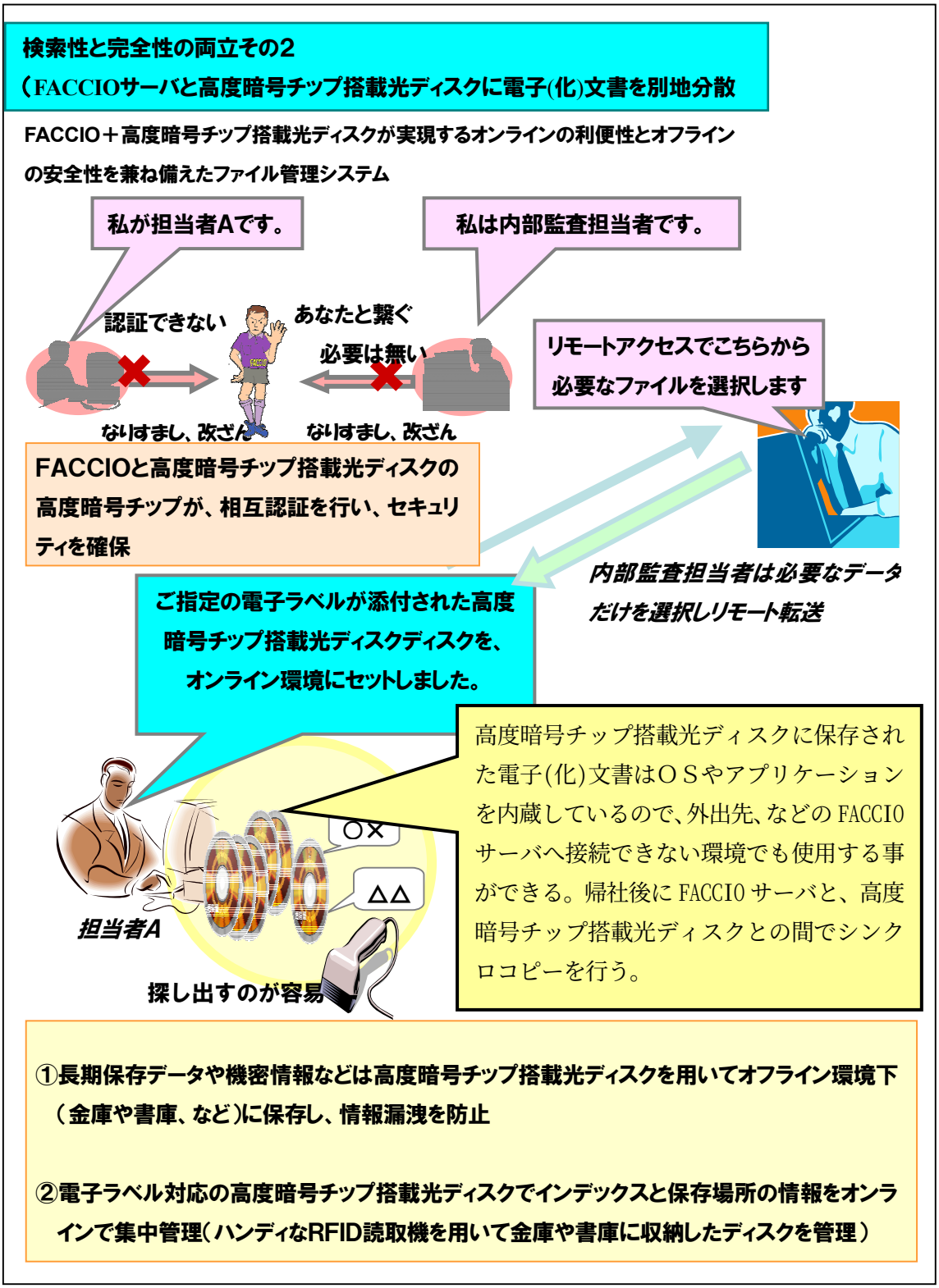


図 3.1.4-6-Ⅱ　検索性と完全性の両立その２

課題その⑦：物理的復元可能性

HDD は故障が多く、一旦トラブルが起こると瞬時に情報が消滅する危険性がある。

また HDD は、緻密な回転機構を有する精密機械であり、長期間通電しない状態で保存すると潤滑油その他の劣化により、使用不可能になる可能性が高い。

従って HDD は、長期保存用記憶媒体としては物理的復元可能性に欠けると同時に、メディア自体が重く嵩張ることから可搬性に乏しく、データの完全消去が困難であり、廃棄した HDD から情報が漏洩する危険性を内在している。

解決方策：

高信頼ディスクシステムは、HDD のような ドライブ一体型の記憶媒体ではなく、ドライブと分離した記憶媒体だけを長期保存するシステムである。

しかも、高度暗号チップ搭載光ディスクは、素材的にも、構造的にも、経年劣化の影響を受けにくい特徴がある。また、光ディスクの読み取り面が汚れたり傷ついたりした場合でも、ディスクの表面をミクロン単位で研磨することにより修復できる可能性が高い。

従って、高度暗号チップ搭載光ディスクは物理的復元可能性が高いと言える。

さらに、高度暗号チップ搭載光ディスクは、軽くてコンパクトな上に、素材がプラスチックなので、薬品による化学的破壊及び、加熱や裁断による物理的破壊による情報の完全消去が容易であり、廃棄したディスクからの情報漏洩の危険性は少ない。その上、高度暗号チップ搭載光ディスクは高度暗号チップで守られているので、万一、ディスクを破壊せずに廃棄した場合でも、不正取得による情報漏洩の可能性は極めて低いと言える。

課題その⑧：シンクライアントシステムに於ける、レガシーシステムとの互換性の保持

ユーザが社内で過去に開発したアプリケーションや、市販のサードパーティ製ソフトウェアは、個々のユーザに対応したエントリを持つことができない構成になっているケースが多く、シンクライアントシステムに適合させる為にはプログラムを書き換える必要がある。

然るに、数十年単位の長期保存となるとシンクライアントシステム自体が全く別のものに変わっている可能性が高く、数十年前のＯＳ、アプリケーション、暗号アルゴリズム、などで構成されたレガシーシステムとの互換性を長期間保持することは非現実的と言える。

解決方策：

FACCIO サーバに於ける電子(化)文書の保存は高度暗号チップ搭載光ディスクのバックアップと位置づけ、年単位の保存期間（必要に応じて FACCIO サーバ側でも長期保存用のバックアップディスクを作成）とし、高度暗号チップ搭載光ディスクへの電子(化)文書の保存期間は、法令の定める期間とする(数年～数十年／ＯＳやアプリケーションを内蔵しタイムカプセル化)。

即ち、高度暗号チップ搭載光ディスクをタイムカプセル化することにより、経済合理性に適う方法で、数十年前のＯＳ、アプリケーション、暗号アルゴリズム、などで構成されレガシー

システムとの互換性を長期間保持することが可能になる。

さらに、電子化したイメージ化文書の原本性確保は、タイムスタンプ及び電子署名に加えて、電子データ自体のハッシュ値を高度暗号チップ搭載光ディスクに搭載された高度暗号チップが自律的に管理することにより実現可能。

しかも、FACCIO＋高度暗号チップ搭載光ディスクを用いた情報管理システムは、大規模なシステム構築を必要としないので初期投資が軽減される上に、ＯＳやアプリケーションの大半は無償の Linux で構成されるので TOC (Total Cost of Ownership)が極めて低い。

3.2　個人ユーザの利便性と安心・安全の確保及び課題の抽出（太字／アンダーライン付）

① 大半のユーザがパソコンに対し切実に求めているのは、際限なく追加の費用負担を求められるセキュリティ対策ソフトとのしがらみから解放され、煩わしい操作や頻繁なアップデートなしにコンピュータウイルスやハッカーなどの脅威から自分のパソコン環境を守りたいという点である。

この課題を解決する為には、Windows のセキュリティホールを完全に塞ぎ、コンピュータウイルスやハッカーからの攻撃を無力化するか、**Windows のセキュリティホールを皆無にすることは非現実的**であるとの認識に立ち、全く別の解決方策を模索するかの二者択一と思われるが、矛盾と言う熟語の語源をひもとく迄もなく、後者を選択せざるを得ないのが現実である。

② ユーザは、パソコンを起動するたびに、先ずログインＩＤとパスワードの入力を求められ、続いて各アプリケーションやウェブサイトへアクセスするたびにそれぞれ異なるＩＤとパスワードの入力を求められる。

また、ＩＤやパスワードの漏洩によるトラブルが多発していることから、厳格なアクセス管理を行っているサイト（金融機関他）では、パスワードを頻繁に変更することを要求してくる。

これはＩＤやパスワード漏洩によるトラブルのリスクをユーザ側に一方的に押しつけているだけであり、根本的な問題解決につながらないのは明らかである。

よって、**ＩＤやパスワード管理のリスクと煩わしさを一挙に解決する革新的な方策が求められている**。

③クレジットカード情報開示の脅威

ウェブサイトから物品やサービス並びにコンテンツを購入する場合、個人情報を開示することなく代金を決済するには電子マネーを含むプリペイドマネーが便利だが、規格が乱立しており対応可能なショップも非常に少ない。

特に海外のウェブサイトはクレジットカードしか対応していないケースが大半だが、スキミングやフィッシングなどのネット犯罪が怖くて購入を断念する人が多い。

一方、オンラインショッピングが普及し、クレジットカードそのものを持っていなくてもク

レジットカード情報だけで決済ができるようになり、第三者にクレジットカード情報を不正使用されるなどの危険性も高まっている。

実際、平成１７年6月１７日（日本時間１８日)、マスターカード・インターナショナルの外部委託先である米国のデータ処理会社のコンピュータが外部からの不正アクセスを受け、マスターカード会員約1,390万人分のデータが流出した可能性があり、また、他のカード会社分を含めると約4,000万人分の顧客データが当該データ処理会社から流出した可能性があると発表された。

しかもその内、約77,000人分の日本のカード利用者の情報が流出した可能性があり、平成１７年6月２８日時点ですでに約740件、約１億1,000万円の不正使用があったことが判明している。

また、個人のプライバシー保護の観点からも、ウェブサイトから物品やサービス並びにコンテンツを購入するたびに、個人情報を含む**クレジットカード情報を開示させられることに抵抗感を持つユーザも多い**。

従ってプリペイドマネーの匿名性とクレジットカードの汎用性を兼ね備え、ユーザとコンテンツホールダの双方から支持されるＤＲＭ機能を有し、安全性と利便性に富んだウェブサイト上での決済システムに対する社会的ニーズは極めて高いと言える。

3.2.1　課題と解決方策その①：Windows のセキュリティホール

一昨年の暮れにマイクロソフト社が鳴り物入りで発表した Windows Vista の最大のセールスポイントは、ハッカーやウィルスに対する万全のセキュリティ技術とデジタルコンテンツを不正にダビングしたりダウンロードしたりする著作権侵害行為に対する革新的なＤＲＭ管理技術（AACS）を施した、と言う点であった。

しかしながら、Windows Vista ベータ版の発表直後にセキュリティソフト大手のシマンテック社から深刻な脆弱性を指摘されたし、ハリウッドの大手スタジオや世界的大手ＡＶ機器メーカの参加を得て、マイクロソフトの強力なイニシャティブの基に開発したＤＲＭ管理技術である AACS（Blu-ray 並びにＨＤ－ＤＶＤにも標準搭載）によるコピーガードも今や、あっさりと突破してしまうリッピングツール（DVDFab HD Decrypter や AnyDVD、など）がウェブサイトからフリーやお試し期間付のシェアウエアとしてダウンロードできる状態にある（http://cowscorpion.com/MultimediaTools/DVDFabHDDecrypter.html 参照)。

しかして、Windows Vista の発売後も、世界中のコンピュータセキュリティ関係者は、Windows Vista の脆弱性に対する攻撃うける度に事後的な対策を繰り返す、と言うエンドレスゲームを強いられている。

従って、ウィルスやハッカーなどの脅威から自分のパソコン環境を守るためには、相変わらず最新のセキュリティソフトを購入するか、有償でアップデートすることを求められる上に、コンピュータの動作速度が低下したり煩わしい操作を強いられたりすることを我慢しなければならないのが現状である。

この悪しきパラドクスから抜けだし、追加の費用負担を求められることなく、煩わしい操作や頻繁なアップデートなしにコンピュータウイルスやハッカーなどの脅威からユーザのパソコン環境を守るためには、ＯＳ、基本アプリケーション、セキュリティアルゴリズム、などを多様化することにより、用途や個々のユーザのニーズに照らし最適な組み合わせを選択することを可能にして世界中のハッカーやコンピュータウイルス作成者の攻撃対象を分散し、攻撃者から経済合理性と挑戦意欲を奪うことが重要である。

この課題を解決する為の方策として、目的に応じた Linux OS とアプリケーションを選択し、高度暗号チップ搭載光ディスクに収納することにより、非画一的なパソコン環境の実現を目指すことが考えられる。

また、コンピュータウイルスやハッカー対策の面で従来とは全く異なる方法としては、例えば、ＯＳや基本アプリケーションを ROM 化することにより攻撃者によるシステムの改ざんを防ぐ方法や、高度暗号チップとセキュリティアルゴリズムの組み合わせを多様化して Break Once Run Every where（BORE）を防ぐことなどが考えられる。

3.2.2　課題と解決方策その②：アプリケーション毎に異なるＩＤとパスワード

高度暗号チップ搭載光ディスクに搭載された高度暗号チップが、自律的にパスワードや生体情報を管理してユーザを認証する。

しかも、パソコンやウェブサイト側のサーバなど外部装置との間は高度暗号チップ搭載光ディスクがワンタイムパスワードで自動的に認証するように仕組むこともできる。

従って、ユーザはシステム起動時に高度暗号チップ搭載光ディスクから正当なユーザであることを認証してもらうだけで済むことになり、システム起動後は、アプリケーションやウェブサイトへアクセスするたびに要求されるＩＤやパスワードの管理は全て高度暗号チップ搭載光ディスクが代行してくれることになる（図 3.2.2-1 参照）。

かくして高度暗号チップ搭載光ディスクはユーザの分身そのものになるわけであり、万一紛失したり盗まれても不正使用されたり情報を盗まれたりするリスクは非常に低い。

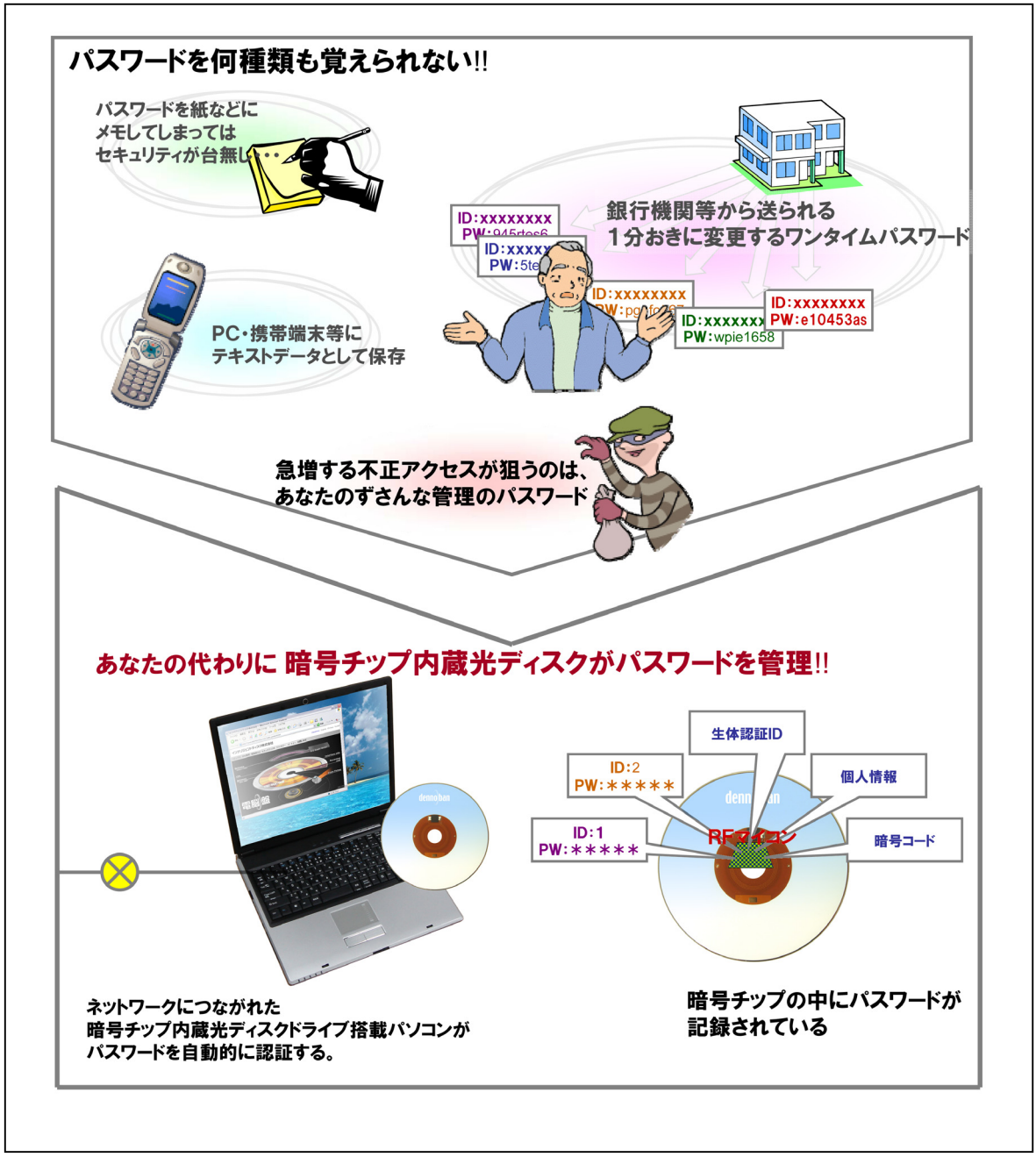


図 3.2.2-1　ＩＤとパスワードの管理は高度暗号チップ搭載光ディスクにお任せ

3.2.3　クレジットカード情報開示の脅威

ウェブサイトでの決済の大半はクレジットカードが主流であり、クレジットカードの情報を開示したくないユーザにとっては極めて不便である。

この問題を解決する方法として、高度暗号チップ搭載光ディスクの高度暗号チップに対し、お財布携帯や Suica 並びに Edy などのプリペイドカード用のリーダ・ライタ端末経由プリペイドマネーとして予め入金しておき、ウェブサイトのショップに対してはワンタイムのクレジッ

トカード番号で決済する方法が考えられる。

このシステムはDepositとCreditの両方の特徴を有することから仮にデポクレ（図3.2.3-1、2 参照）と称する。

デポクレを使用することにより個人情報を開示することなく、世界中のウェブサイトから安心・安全に物品やサービス並びにコンテンツなどを購入することが可能になると思われる。

デポクレを実現するためにはクレジットカード会社の協力が必要となる。

即ち、本来クレジットカード会社は個人に対し与信限度を設定するが、デポクレにおいては高度暗号チップ搭載光ディスクに搭載された高度暗号チップに予め入金された残高の範囲において、高度暗号チップ搭載光ディスクというインテリジェントな媒体に対し与信限度を設定することになる。

しかして、ユーザは匿名による安全性を確保した上でウェブサイトでのショッピングを楽しめるようになるので、ユーザの利便性が大いに向上する。実際、我々が店頭で買い物をする際に個人情報の開示を求められるケースは極めて少ないことから、ウェブサイトでのショッピングにおいても匿名による安全性を確保することは極めて重要と言えよう。

勿論、クレジットカード会社にショッピングの履歴が知られることを承知すれば、プリペイドマネーの代わりに個人の与信限度をベースとしたシステムの利用も考えられる。

しかも、デポクレシステムでは、パソコンのHDDに何もデータが残らないので安心である。

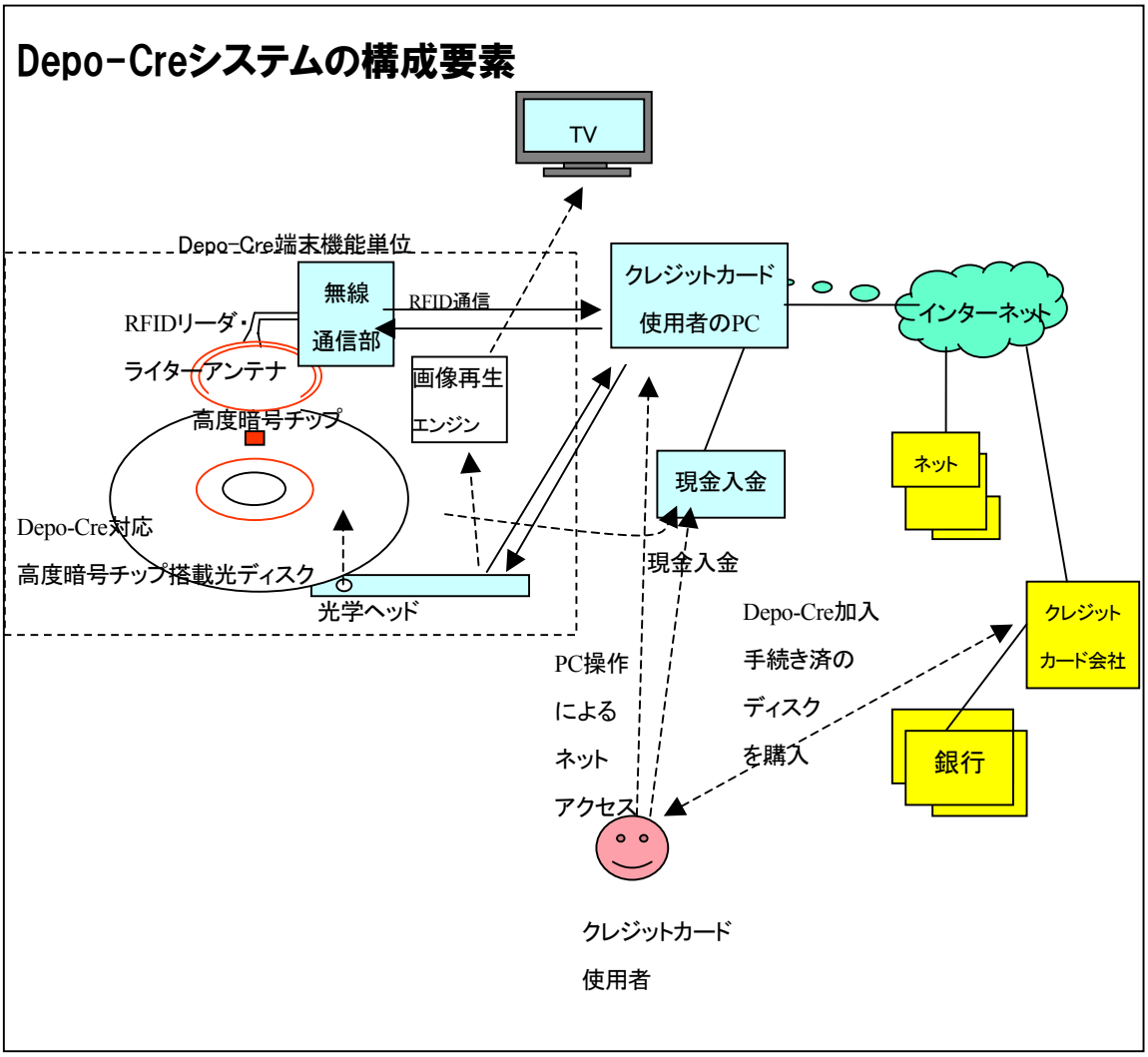


図 3.2.3-1　DepoCre システム構成要素

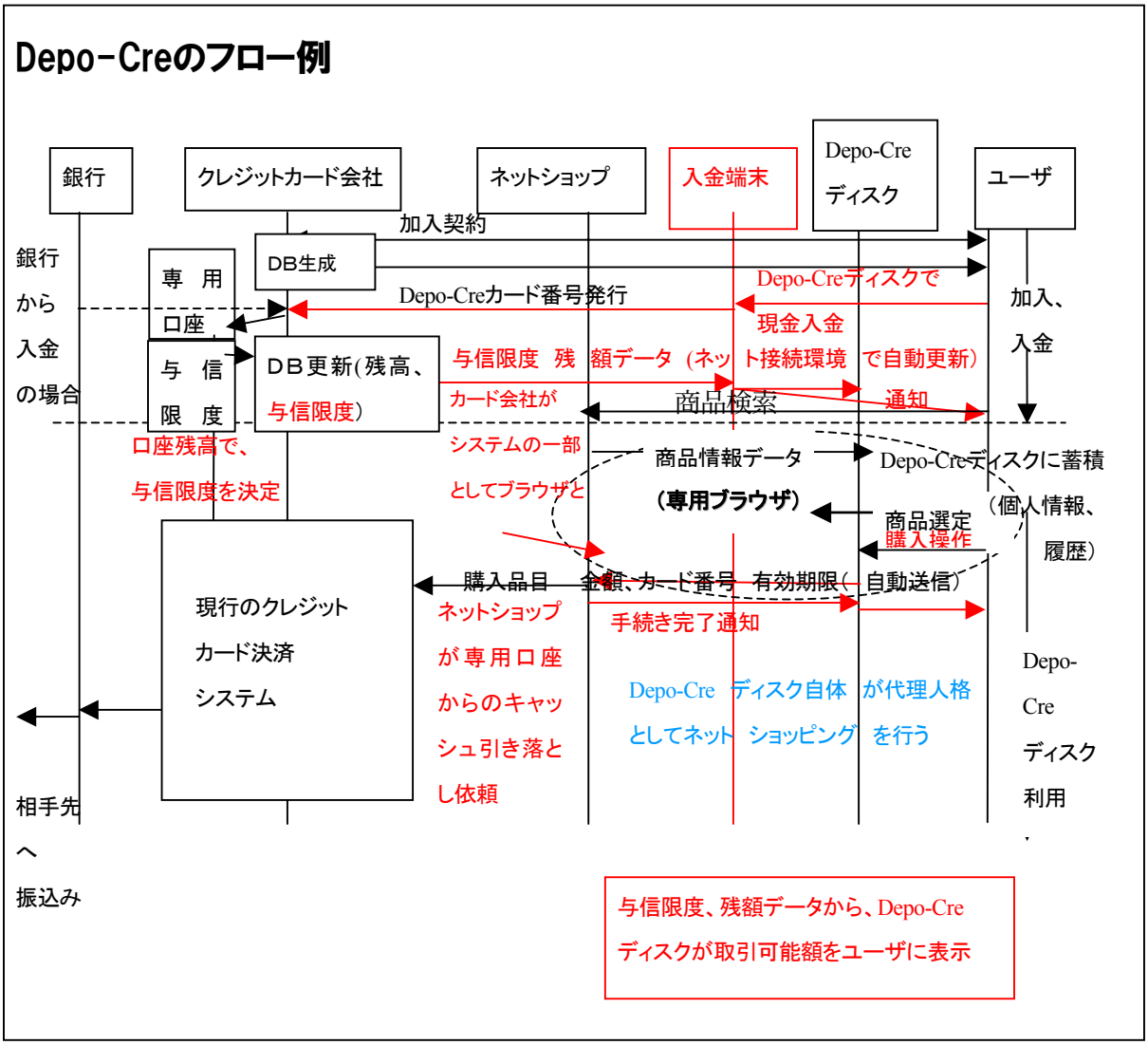


図 3.2.3-2　DepoCre システムのフロー例

3.3　長期保存ファイルの課題

マルチメディア社会が浸透し、オフィスなどでも各種のデータの電子化が進んでいるし、パソコンやワープロで作成した資料や書類などを保存するだけでなく、紙に印刷された書類まで、電子化する動きも活発となってきている。

今までは、大事なことは紙に書き、関連するものをまとめて綴じて、文書毎に定められた保存期間毎に分類して文書保存箱に収納し、それぞれ定められた書棚や倉庫に保存しておくのが一般的であり、つい最近までこの形態が取られてきた。これに対し紙ではかさばる、持ち運びに不便といった欠点や、紙の傷み（酸性紙の問題、貴重な書類・書籍の場合は取り扱いからの傷み）の問題から、マイクロフィルム撮影や、大口径（１２センチ）の光ディスクに、レーザーディスクと同じアナログの画像情報として保管する形がとられてきたが、最近ではパソコン

の発達、ネットワーク技術の進展から、手軽に書類をデジタル化して取り扱えるようになり、光ディスクに保存したり、インターネットで利用したりできる形にするなど、さまざまな方法の利用が始まっている。

また、このような技術の発展だけでなく、政府が提唱している高度情報通信社会、電子政府の構築、情報公開法の制定などで政府内部の電子化が進み出し、これらの政策が民間にも大きな影響を与えており、さらに、民間企業では、品質保証関係であるＩＳＯ９０００番シリーズやＩＳＯ１４０００の取得が、取引上必要となるほか、ＰＬ法や民事訴訟法、さらには特許問題も含めて、さまざまな電子ファイルを長期保存する必要に迫られている。

しかし、情報のデジタル化はまだ緒に就いたばかりのテーマであり、デジタルファイルの長期保存に関しても、デジタルファイルを格納する記憶媒体自体の、経年劣化に対する、物理的復元性と併せて、ファイルフォーマットの論理的復元性に於いて課題を残している。

また、電子署名やタイムスタンプの有効期限は通常３年程度で切れることから、長期保存ファイルの真正性を如何に確保するかということも重要な課題である。

因みに、官公庁で作成される公文書の中で、１０年以上の長期保存が義務づけられているのは以下（表 3.3-1）のとおりである。

表 3.3-1　行政文書の最低保存期間基準 [2]

施行令別表第２に定める最低保存期間			該当する行政文書の類型
行政文書の区分		保存期間	
一	イ　法律または政令の制定、改正または廃止その他の案件を閣議にかけるための決裁文書	三十年	・ 条約その他の国際約束の署名または締結のための決裁文書 ・ 法律の制定・改廃の決裁文書 ・ 特殊法人の設立・廃止の決裁文書 ・ 基本的な計画の策定・変更・廃止の決裁文書 ・ 予算・組織・定員の基本的事項の決裁文書

	ロ　特別の法律により設立され、かつ、その設立に関し行政官庁の認可を要する法人（以下「認可法人」という。）の新設または廃止に係る意思決定を行うための決裁文書		・ 認可法人の設立・廃止の決裁文書
	ハ　イまたはロに掲げるもののほか、国政上の重要な事項に係る意思決定を行うための決裁文書		・ 関係閣僚会議付議のための決裁文書 ・ 政務次官会議付議のための決裁文書 ・ 事務次官など会議付議のための決裁文書
	ニ　内閣府令、省令その他の規則の制定、改正または廃止のための決裁文書		・ 府省令などの制定・改廃のための決裁文書 ・ 行政文書の管理に関する定め
	ホ　行政手続法（平成５年法律第 88 号）第２条第３号に規定する許認可など（以下単に「許認可など」という。）をするための決裁文書であって、当該許認可などの効果が 30 年間存続するもの		・ 公益法人設立許可の決裁文書 ・ 事業免許、資格免許などの許認可の決裁文書
	ヘ　国または行政機関を当事者とする訴訟の判決書		・ 判決書（正本）
	ト　国有財産法（昭和 23 年法律第 73 号）第 32 条に規定する台帳		・ 国有財産台帳
	チ　決裁文書の管理を行うための帳簿		・ 決裁簿
	リ　施行令第 16 条第１項第 10 号の帳簿		・ 行政文書ファイル管理簿
	ヌ　公印の制定、改正または廃止を行うための決裁文書		・ 公印の制定、改正または廃止を行うための決裁文書

	ル　イからヌまでに掲げるもののほか、行政機関の長がこれらの行政文書と同程度の保存期間が必要であると認めるもの		・ 特殊法人または認可法人の管理のための台帳
二	イ　内閣府設置法第 37 条若しくは第 54 条、宮内庁法第 16 条第１項または国家行政組織法第８条の機関の答申、建議または意見が記録されたもの	十年	・ 審議会などの答申、建議または意見
	ロ　行政手続法第５条第１項の審査基準、同法第 12 条第１項の処分基準その他の法令の解釈または運用の基準を決定するための決裁文書		・ 法令の解釈・運用基準の決裁文書 ・ 許認可などの審査基準 ・ 不利益処分の処分基準
	ハ　許認可などをするための決裁文書であって、当該許認可などの効果が 10 年間存続するもの（一の項ホに該当するものを除く。）		・ 有効期間が 10 年以上の許認可などをするための決裁文書
	ニ　イからハまでに掲げるもののほか、所管行政上の重要な事項に係る意思決定を行うための決裁文書（一の項に該当するものを除く。）		・ 条約その他の国際約束の解釈・運用基準の決裁文書 ・ 所管行政に係る重要な政策の決定に係る決裁文書
	ホ　不服申立てに対する裁決または決定その他の処分を行うための決裁文書		・ 行政不服申立て、行政審判その他の争訟の裁決書、裁定書、決定書
	ヘ　栄典または表彰を行うための決裁文書		・ 叙勲、褒章または各種表彰の決裁文書

	ト　イからへまでに掲げるもののほか、行政機関の長がこれらの行政文書と同程度の保存期間が必要であると認めるもの（一の項に該当するものを除く。）		・政策決定の基礎となった国際会議などの決定 ・概算要求書

一方、民間企業や医療法人などに於いては、ほとんどの書類は、自主的に、決定することができるが、一部の書類では、法律でその保存期間を決められている、例えば、以下（表3.3-2）のとおりである。

表3.3-2　民間企業に於ける公的文書の最低保存期間基準

（今後、規制緩和などにより変更される場合がありえる。）

文書の種類	保存期間	法律
株主総会議事録、商業帳簿、取締役会議事録	十年	商法
仕訳帳、総勘定元帳などの帳簿、棚卸表、賃借対照表、損益計算書、注文書・見積書・契約書の控え	七年	所得税法、法人税法
財産形成非課税貯蓄申込書・移動申請書	五年	所得税法
雇用保険被保険者に関する書類	四年	雇用保険法
労働者名簿、雇入、解雇、退職に関する書類	三年	労働基準法
健康保険の被保険者資格取得確認通知書	二年	健康保険法

（このほか医療関係では、診療録（カルテやレントゲンフィルム）などは医師法、歯科医師法などで5年間の保存が義務付けられている。）

上記の別表3.3-2でも明らかなとおり、民間企業や医療法人などに於いては、法律により長期保存が義務づけられている文書は数少ないが、昨今の社会情勢から、実質的に長期保存が必要とされる文書は概ね以下（表3.3-3）のとおりである。

表3.3-3　長期保存が必要な文書の概要[3]

番号	主な事業区分	長期保存が必要な文書
1	社会基盤となっている事業	交通、上下水道、電力、通信、産業プラント関係の

		設計書、マニュアル、図面など
2	製造業系	ＰＬ法などに関連した設計書、図面、検査、販売の記録 ソフトウェアなどの知的所有権保全文書など
3	食品系	特許申請の記録書類など
4	製薬業系	新薬申請書類、特許申請の記録書類、など
5	流通関係	契約書、物品移動の記録、倉庫の搬入・搬出などの記録
6	金融関係	契約書、約款、申込書、など
7	医療	カルテ（法的には５年だが、昨今の社会情勢からして長期保存の必要性が高まっている）
8	公証役場	公正証書、定期借地権契約など
9	行政文書	行政審判の決済など
１０	その他	各種議事録（役員会など）、楽譜などの知的所有権の保全

3.3.1 J-SOX 法対応などにおける長期保存ファイルの必要性

日本版ＳＯＸ法や J-SOX 法とも呼ばれているのは、2006 年 6 月に「外国証券業者に関する法律」、「有価証券に係る投資顧問業の規制などに関する法律」、「抵当証券業の規制などに関する法律」、「金融先物取引法」を廃止し「証券取引法」と統合して「金融商品取引法」としたものの一部をさしている。

即ち、日本版 SOX 法（J-SOX 法）と呼ぶ場合は、「金融商品取引法」の中の、内部統制の整備と、内部統制報告書の提出義務について記載した部分を示している。

内部統制とは、基本的に、業務の有効性及び効率性、財務報告の信頼性、事業活動に関わる法令などの遵守並びに資産の保全の４つの目的が達成されているとの合理的な保証を得るために、業務に組み込まれ、組織内のすべての者によって遂行されるプロセスをいい、統制環境、リスクの評価と対応、統制活動、情報と伝達、モニタリング（監視活動）及びＩＴ（情報技術）統制への対応の６つの基本的要素から構成される。

即ち、J-SOX 法とは、要約すると、文書化による内部統制の確立と言えよう。

今後、文書の電子化が急速に進展することを踏まえると、電子(化)文書の、見読性、完全性、機密性、原本性、真正性、検索性、並びに長期保存媒体の物理的並びに論理的復元可能性が、J-SOX 法に於いて重要なファクターとなるのは確実と思われる。

また、J-SOX 法以外でも、例えばＰＬ法（製造物責任法）関連で昨今、２０年以上前に製造した家庭用器具の経年劣化による事故が相次いでおり､関連メーカはその対応に追われている。

その際、過去の顧客データ（返信保証書カード、愛用者カード、修理名簿、など）が残っていれば迅速な対応が可能となり、結果的に企業の評価を高め、比較的少ない費用で事故に対処できることになるのだが、実際は、個人情報保護法施行やセキュリティ重視の風潮を受けて、日本の主な企業では法定保存期間（１０年）が過ぎた顧客データの大半を破棄しているケースが多いと思われる。

斯かる事例を勘案するに、電子(化)文書の法定保存期間は最低限の保存期間と位置づけ、必要に応じて１０年～５０年（住宅、公共建造物、など）内外の長期に亘って、見読性、完全性、機密性、原本性、真正性、検索性、並びに長期保存媒体の物理的並びに論理的復元可能性を確保した状態で保存することの必要性が顕在化してきたと言えよう。

3.3.2　内部統制におけるメール監査システム

電子メールの利用は、ビジネスだけでなく個人にまで幅広く普及し、手紙やはがきなどの郵便より、利用頻度は高くなっている。

今やビジネスには欠かせない情報の交換手段となり、重要な取引情報や書類が、電子メール本文、あるいは添付ファイルとして交換されている。

そこで、セキュリティ対策上、また万が一のトラブル発生に備えて、電子メールの保存・管理がより重要になってきた。米国の SOX 法（米国企業再生法）では、オフバランス取引（簿外取引）などで、契約書を明確にする目的や、購入依頼書を作成する目的で交換された電子メールは、取引レポートとして保存することが求められており、会計監査に関するドキュメントとして、最低７年間の保存が求められている。

電子メールアーカイブシステムは、これらの要求に応えるためのシステムであり、ユーザが削除したメールも保存したり、保存されているメールの内容を改ざんできないようにしたりする。またメールサーバに蓄積される全ての電子メールを対象としているため、メールボックスの容量削減のため、経過時間や容量サイズによってデータを、光ディスクなどの二次記録装置に移して長期保存する仕組みになっている。

最近では、企業内の不祥事に関して警察などが家宅捜査を行うときには、まずメールの記録を確保することから始めるとも言われており、企業や職員自身の潔白を証明するために、大切なシステムといえる。

従って、長期保存用記憶媒体自体の改ざん防止や電子署名並びにタイムスタンプの真正性管理が重要なファクターとして注目されることになる。

3.3.3　IT 内部統制におけるセキュリティ及びデジタルフォレンジック（図 3.3-3-1 参照）

ここで言うＩＴ内部統制とは、組織目標を達成するために予め適切な方針及び手続を定め、それを踏まえて、業務の実施において組織の内外のＩＴに対し適切に対応することをいう。

ＩＴへの対応は、内部統制の他の基本的要素と必ずしも独立に存在するものではないが、組織の業務内容がＩＴに大きく依存している場合や組織の情報システムがＩＴを高度に取り入れている場合などには、内部統制の目的を達成するために不可欠の要素として、内部統制の有効性に係る判断の規準となる。

従って、「ＩＴ統制」への対応が重要となるが、「ＩＴ統制」は「業務処理統制の中のＩＴによる統制」と「ＩＴ全般統制」の大きく２つにわかれる。

「業務処理統制の中のＩＴによる統制」とは、個々のアプリケーション・システム（販売管理システム、会計システムなど）において、承認された取引がすべて正確に処理され、記録されるようコンピュータ・プログラムに組み込まれた統制のことであり、実際の業務プロセスの一部をＩＴが担っている中で、その ERP などのアプリケーションやＩＴ環境が持つ認証や牽制機能、不正データチェックや外部インタフェースの完全性確保、監査証跡（ログ）管理などをさす。 一方「ＩＴ全般統制」とは、ＩＴを利用した業務処理統制が有効に機能する環境を保証する間接的な統制のことをさす。

ＩＴ戦略策定やＩＴ組織、アクセス権管理、ＩＴ教育、ＩＴリスク評価、情報資産管理などの「ＩＴ組織レベル統制」と、開発業務プロセスレベル統制」とがある。ＩＴの統制を有効なものとするために経営者が設定する目標を、ＩＴの統制目標と呼ぶ。ＩＴの統制目標としては、例えば、次のものが挙げられる。

a．有効性及び効率性：情報が業務に対して効果的、効率的に提供されていること
b．準拠性：情報が関連する法令や会計基準、社内規則などに合致して処理されていること
c．信頼性：情報が組織の意思・意図に沿って承認され、漏れなく正確に記録・処理されること（正
当性、完全性、正確性）
d．可用性：情報が必要とされるときに利用可能であること
e．機密性：情報が正当な権限を有する者以外に利用されないように保護されていること

即ち、ＩＴ統制の目標は、セデジタルフォレンジックレンジックをキーワードとして策定されていることが明白である。

そもそも、デジタルフォレンジック（Digital Forensics）とは、「法の」あるいは「法廷の」といった意味を持ラテン語 forensis からきたものであり、デジタルフォレンジック研究会ではデジタルフォレンジックを、「インシデントレスポンス（incident response）や法的紛争・訴訟に対し、電磁的記録の証拠保全及び調査・分析を行うと共に、電磁的記録の改ざん・毀損などについての分析・情報収集などを行う一連の科学的調査手法・技術を言う」と定義している。

因みに、デジタルフォレンジック研究会では、インシデントレスポンスを、「コンピュータや

ネットワークなどの資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示など、並びにそれらへ至る為の行為（事象）などに対する対応」と定義している。従って、デジタルフォレンジックとは、企業や民間団体が、自己の保有するコンピュータやサーバなどに対する不正侵入などの攻撃を検知すれば、応急処置をするだけでなく、証拠となり得るデータを保存し、被害の程度や侵入経路並びに想定される侵入者を分析することにより、当該攻撃に関し、自らが訴訟するか、または訴訟された場合に備える為の、内部統制を構成する概念の一つと言えるであろう。

即ち、刑事事件の捜査に於いて警察は、事件として起訴されることを前提として、科学警察研究所（科研）などによる証拠の収集と保存を行うが、企業の内部統制に於いても同様の対応を取ることが求められるということであり、J-SOX 法に対応する為には、不正侵入の証拠性だけでなく、財務会計情報などの情報改ざんや個人情報や機密情報などの漏洩及びセクハラや詐欺などの不正行為がなかったかの証拠性も大切となる。

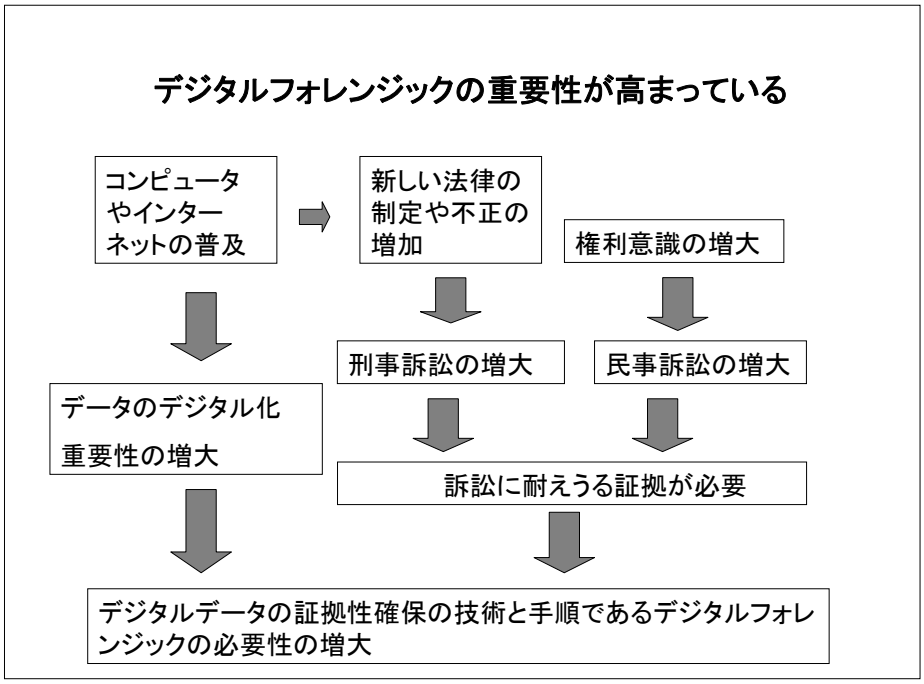


図 3.3-3-1　デジタルフォレンジックが注目され始めた背景 [4]

3.3.4　デジタルフォレンジックと人格権

プライバシーの権利は、今日、日本に於いても、日本国憲法第１３条に基礎づけられるいわゆる「新しい人権」の一つとして、裁判に於いても、具体的な権利を認められる確立した人権となった。

プライバシーの内実は、各個人が、一人の人格的自律主体として、社会に於いて自己実現を

遂げていく為に必要とされるものであって、社会状況が変化すれば、それに応じて変化し得るものである。

従って、今日の情報化社会い於いては、プライバシー権を単に消極的に「私生活をみだりに公開されない保証」ととらえるのではなく、「自己についての情報をコントロールする権利」として、広い積極的な権利と考えるのが一般的になっている。

よって、指紋や掌紋などの生体情報は、正しく自己情報そのものであり、改変不可能であることから、斯かる情報をコントロールする権利は、日本国憲法第１３条に基礎づけられる「新しい人権」の一つと言えるであろう。

因みに、２００６年１２月１１日に、東京都北区が全職員（約3，０００人）を対象に区役所内部の情報システム利用時の本人確認（利用者権限の認証）方法に、生体認証システムを導入したところ、一部の職員が、前述の「自己情報コントロール権」を盾に、自己の生体情報登録を拒否したと言われている。

これは、自己の生体情報を、他人の管理下にあるサーバに登録することは、「自己情報コントロール権」を侵害する行為であるとの見解に基づき、生体情報の登録を拒否したものと思われる。

企業や官公庁などの組織に於いて、内部統制は今後益々強化されるものと思われることから、内部統制上の要請に基づくデジタルフォレンジック手法の導入は増加する一方であろう。

しかしながら、デジタルフォレンジック上の手法として「生体認証」を導入する場合は、「自己情報コントロール権」との調和を如何に図るか、が重要な課題となる。

3.3.5　課題解決方策としての高度暗号チップ搭載光ディスク媒体のタイムカプセル化

上場企業のみならず、官公庁を含む主な組織体は今、社会的要請として、内部統制の充実を求められているが、この内部統制に於いて重要な位置を占めるのがＩＴ技術に裏打ちされたセキュリティとデジタルフォレンジックであることは 3.3.3 で述べたとおりである。

従って、ここでは如何にしてセキュリティ及びデジタルフォレンジック上の課題を解決すると同時に、日本国憲法第１３条に基礎づけられる「自己情報コントロール権」との調和を図る方法として、高度暗号チップ搭載光ディスク媒体のタイムカプセル化を提唱する。

即ち、自己のコントロール下に置くことが可能な高度暗号チップ搭載光ディスク媒体が、自律的に生体情報を管理しユーザを認証することで、「自己情報コントロール権」との調和を図ることが可能であると同時に、内部統制上必要とされるセキュリティを確保することができる。

また、デジタル化されたファイルの長期保存性に関しては、3.1.4「課題と解決方法」でも述べたとおり、100 年を超す長期保存性が立証されている長寿命光ディスクをベースにした高度暗号チップ搭載光ディスクに、Linux OS とアプリケーションを自己完結的に収納（タイムカプセル化）することにより、OS や暗号アルゴリズムの陳腐化による復元性の喪失を防ぐことができる。

従って、3.3「長期保存ファイルの課題」で提起された課題の大半は、「高度暗号チップ搭載

光ディスク媒体のタイムカプセル化」で解決可能と思われる。

3.4　高度暗号チップ搭載光ディスク実用化システム検討のまとめ

昨今の社会情勢から、電子(化)文書を長期保存することの必要性が高まっており、長期保存用媒体の選定と、デジタルフォレンジックに対応した保存方法の確立が求められている。

適切な管理の下に製造された光ディスクが長期保存用媒体として最適であることは、平成１９年３月に上梓した「高信頼（長寿命・高セキュリティ）光ディスク媒体の活用システムの開発に関するフィージビリティスタディ」で発表したとおりである。

従って、今回は高度暗号チップ搭載光ディスク実用化システムの課題とその解決方策について検討した。

先ず、デジタルデータの大容量化に伴い高度暗号チップ搭載光ディスクも大容量への対応が求められることから、５０ＧＢの記憶容量を持つ Blu-ray ディスクを高度暗号チップ搭載光ディスク化するための検討を行い、課題の抽出と解決方策の策定を実施した。

次に、セキュリティを一層向上させること並びに将来の量産化を踏まえて、高度暗号チップ搭載光ディスクに、スタンピング方式による物理的 ROM・RAM 構造を設けることの可能性を検討し、技術的に可能であることが判明した。

さらに、高度暗号チップ搭載光ディスクと東京電力が開発した安全性の高いネットワークである FACCIO とを組み合わせることにより､安全で信頼できるクローズドなネットワーク基盤を構築できることがわかった。

最後に、J-SOX 法やＰＬ法などとの関わりから、電子(化)文書を長期保存する際の課題を抽出し解決方策を策定した。　ここで判明したことは、訴訟社会への移行に伴い、裁判における電磁的記録の証拠保全に係わる包括的手法であるデジタルフォレンジックとの関わりが避けて通れないということである。　一方、このデジタルフォレンジックという考え方自体が日本社会には馴染みが薄く、日本的社会風土との親和性は決して高くない。　従って、今回の報告書作成にあたっては、高度暗号チップ搭載光ディスクとデジタルフォレンジックとの関わりを念頭におきながら、高度暗号チップ搭載光ディスクの実用化システムに係わる課題の検討と、解決方策の策定を行った。

3.4.1　平成１８年度～１９年度検討結果の総括

１．情報のデジタル化に伴う「媒体に於ける物質的枠組みの消滅」:

① アナログ情報時代の情報処理に於いては、文字情報や絵は紙、動画を含む画像・音声情報は磁気テープやレコード盤ないしは銀塩フィルムと言った具合に、情報の形態と用途に応じてそれぞれ対応する媒体が物質的に異なっていた。

一方、電気的情報通信技術の登場により、一部の情報が物質を伴わずに送れるようになったが、電気的通信路の利用コストが高い上に、電話／ファックスやＴＶと言った具合に、用途別に異なった装置を必要としており、様々な物理的制約要因が残っていた。

② 国家や地方自治､などの官公庁は言うに及ばず､営利企業から非営利の慈善団体に至るまで、現代社会に於ける営みの様々な形式・手順・規則・法律、などの社会的枠組みは全てアナログ情報処理を前提として成り立っている（各種書類の管理、著作権管理、など)。
③ デジタル情報化の急激な進展により、物理的媒体を特定することなく、情報を記録、伝送、蓄積することが可能となった。

即ち、媒体に於ける物質的枠組みの消滅が起こりつつあると言える。

例えば、i mode の登場以来携帯電話は飛躍的発展を遂げ、今や通話、メール、ウェブブラウジング、カメラ／ビデオ、テレビ、電子マネー、などの複合機能を持った万能媒体に進化している。

本来、このように急激な変化が社会に受け入れられることは希であるが、携帯電話の場合は正しく「携帯性」が社会的ニーズに合致したが故に、斯かる急激な進化を遂げることができたと言えよう。

２．媒体の物質的枠組みの消滅がもたらす社会的枠組みの混乱：

① 数千年間に亘りアナログ情報処理を前提として成り立ってきた社会的枠組みに対し、 パソコンとインターネットの融合による ICT（情報通信技術）がもたらした衝撃は、正しく破壊的であり、特に法律や各種規制の面で大きな混乱をもたらしている。

例えば、文書の電子化に起因する深刻な情報漏洩や改ざんによる不正行為及び OS やアプリケーション、などの論理的経年劣化による長期保存媒体の復元性喪失、ダビングしても劣化しないコンテンツの著作権管理に関する諸問題、など、枚挙にいとまがないほどである。

② HDD の大容量化に伴い、従来は用途別に個々のメディア、例えばオーディオはＣＤ、ビデオはＤＶＤに記録・保存されていたコンテンツやデータが、パソコンの HDD に包括的且つ無秩序に記録・保存されるようになった。

このことはユーザに利便性をもたらすと同時に、パソコンのクラッシュにより貴重なコンテンツやデータが瞬時に喪失したり、ファイル交換ソフトにより国家的機密情報が漏洩したり、と言った社会的諸問題を惹起している。

しかも、防衛省のように組織を挙げて大々的対策を講じたにも拘わらず、これらの問題が繰り返し起こっていると言うことは、媒体の物質的枠組みの消滅がもたらす社会的枠組みの混乱が如何に深刻且つ根元的な問題であるかということの証である。

３．デジタル化による媒体の物質的枠組みの消滅と既存の社会的枠組みとの調和：

① 今、最も混乱している社会的枠組みは、官公庁並びに企業の情報管理と言えるであろう。

前出の防衛省に於ける情報漏洩の問題にしても、紙媒体の時代であれば、国家機密文書と娯楽雑誌が一冊の本に併せて製本されることはあり得ないわけであり､国家機密文書を娯楽雑誌と同じ感覚で管理することもあり得なかったであろう。

即ち、国家機密文書はそれらしく装丁されており、娯楽雑誌との違いは一目瞭然である

ことから、自ずと厳重な管理を行うようになるのである。

一方、あらゆる情報が包括的に記録・保存されているパソコンの HDD に於いては、情報は論理的な隔壁により区分けされ保存されているだけであり、ハッカーやウィルスあるいは内部犯行者による論理的な攻撃により隔壁を突破される危険性を内包している。

また、物理的媒体としては一台のパソコンであり、通常、保存されている情報ごとの重要性の違いを外観から判断することは困難である。

② 一方、OS やアプリケーションを起動ディスクの形式で組み込んだ高度暗号チップ搭載光ディスクであれば、レーベル面の印刷やディスクのパッケージデザインを工夫することにより、国家機密文書をそれらしい外観に仕上げることが可能である。

また、予めパソコンから HDD を取り外しておけば機密データがパソコンの HDD に残ることはなく、さらに高度暗号チップ搭載光ディスクの高度暗号チップが使用条件（ユーザ、使用可能なドライブ、タイムスタンプ、ロケーションスタンプ、アクセス権限、など）を自律的に認証し機密データのセキュリティを確保するので安心である。

③ 高度暗号チップ搭載光ディスクは、適度なサイズと安価なコストから、紙媒体と同じような感覚で、用途やジャンル毎に使用し保管することができる。

即ち、処理すべきテーマ毎に高度暗号チップ搭載光ディスクを専用ドライブに挿入して使用し、処理が終わったディスクは、文書管理・保存規定に沿って保管することができるので、アナログ情報処理を前提として成り立ってきた社会的枠組みとの親和性が高いと言える。

一方、高度暗号チップ搭載光ディスク対応の、HDD を持たないパソコンには、ユーザのデータは一切残留しない。

よって、一台のパソコンを複数のユーザで共有する、フリーアドレスシステム端末として使用可能である。

従って、当該インフラが整備された環境下であれば、軽くコンパクトな高度暗号チップ搭載光ディスク一枚で、見読性、完全性、機密性、原本性、真正性、検索性、並びに長期保存媒体の物理的並びに論理的復元可能性を確保することが可能となり、デジタル化による媒体の物質的枠組みの消滅と既存の社会的枠組みとを調和させることができる。

【参考文献】

[1]2006 年１月１７日付 ITmedia エンタープライズ

[2] 行政文書の管理方策に関するガイドラインについて／平成１２年２月２５日各省庁事務連絡会議申合せ

[3] TNF-2005408ST、2005 年 8 月 15 日 JIS 解説案 V2.1

[4]特定非営利活動法人　デジタルフォレンジック研究会編「デジタルフォレンジック事典」

第 4 章　スタディの今後の課題及び展開

4.1　システム開発

4.1.1　高度暗号チップ搭載光ディスク

これまでスタディを通して、DVD-RAM や Blu-ray などの光ディスク媒体に対し、RF 通信機能を持たせた高度暗号チップを搭載し、光ディスクドライブ側に搭載したリーダ・ライタとの間で、ディスクが回転中にもデータ通信を安定に行う為の、チップとアンテナの形状、配置、機械的構造、電磁気的影響を排除するための磁気シートの導入など、基本的な設計手法は確立した。

この基礎データをもとに、今後目的に応じた適切な高度暗号チップ搭載光ディスクを開発することができる。その場合の課題は、用途に応じた最適な高度暗号チップの選択、量産性、信頼性を考慮したアンテナとチップの実装方式の採用、必要に応じた半導体チップの長期信頼性の保証などであるが、いずれも用途が定まれば解決できるだけの技術水準に達していることがこれまでのスタディで分かった。従って、今後の展開としては、具体的なアプリケーションを見つけ、上記課題を解決することにより、高度暗号チップ搭載光ディスクの普及を促進するための市場開拓に取り組むことが課題となる。

4.1.2　リーダ・ライタ内蔵光ディスクドライブ

リーダ･ライタの物理的サイズは、LSI の進歩によりさらに小さくなり、ドライブの回路の一部に組み込むことも物理的に可能である。一方、パソコンにおいては、RF リーダ･ライタのアンテナをキーボードの周辺に配置した機種が最近登場してきた。仮に、このアンテナ部だけを、当該パソコンの内蔵光ディスクドライブの中にも配置すれば、リーダ･ライタ内蔵ドライブが実現する。理論的にはこのようなことは可能ではあるが、現実的には、これを推進するフェリカ･カードグループとの業務提携が必要である。高度暗号チップにプリペイドカード機能を持たせること自体は実現できるので、これからは、既存のカードグループとの提携などの戦略的ビジネスプランを立案し、実行できるだけの能力を有する企業及び官公庁などの組織を、当該ビジネスの事業主体として参入させることが課題となる。

4.1.3　大容量光ディスクでの ROM・RAM 領域の確保

今回のスタディにより、ISO-9660 に内包した仮想化ファイルシステムでも 4 GB 超のデータを扱える見通しが付いたが、この方式は、ディスク製造時にプリマスタリングにより、ディスク上の使用するエリア全体のデータイメージを予め作成しておき、それをディスクに書き込む時間が必要なので、例えば２５ギガバイトの Blu-ray ディスクの場合、２時間程度の書き込み時間が必要となる。この問題を解決するためには、データが追加されるたびに必要な分だけ、光ディスク面を初期化してゆく（incremental write）方式の方が適していることが、今回のスタディにより判明した。今後、この方式を具体的に実現することにより実用性の向上を図るこ

とが課題となる。

4.2 応用システムの検討

本年度は、高度暗号チップ搭載光ディスクの大容量性及び長期保存性と、高度暗号チップのセキュリティ機能を生かしたアプリケーションシステムの実証試験として、高度暗号チップ搭載光ディスクに東京電力の FACCIO/DRMClient を搭載し、文書の協同作成や集中・分散保存の実験を行い、セキュアな環境でコンテンツを保存できることを確認出来た。今後はこのシステムを、運用面での制約が多い、現行の大規模なシンクライアント/サーバシステムに替えて、小規模で融通性に富む、新しいコンセプトのシステムとして提唱し、具体的採用事例を作り上げることが最大の課題である。我が国のお家芸であった光ディスク事業も今や、新興国への技術移転が急速に拡大しており、我が国独自の技術的優位性が失われつつある現状において、高度暗号チップ搭載光ディスクとその応用システムを、日本発の新たなデファクトスタンダードとして世界に提唱し、利便性と安全性を兼ね備えた、コンテンツ流通・保存用メディアとして認められることをめざした戦略的取り組みが求められる。

システム開発　　19-F-4

高信頼・高セキュリティ光ディスク媒体の活用システムの開発に関するフィージビリティスタディ
報告書　(要旨)

平成 20 年 3 月

作　成　　財団法人 機械システム振興協会
東京都港区三田一丁目４番 28 号
TEL 03－3454－1311

委託先　　財団法人デジタルコンテンツ協会
東京都千代田区一番町２３－３
TEL 03－3512－3903