

## クライアント上の情報セキュリティ技術の技術概要

### 1. 技術分野の概観

#### (1) 背景

近年、パーソナルコンピュータの高性能化とインターネットの急激な普及に伴い、従来は考慮されることの少なかったクライアント側（エンドユーザ）の情報セキュリティが注目を集めている。ここ数年に限定しても、クライアント上の情報セキュリティに関する主なトピックとしては、

- ・ 音楽コンテンツなどの不正コピーの蔓延
- ・ コンピュータ内の情報が漏洩することなどによるプライバシーの侵害や金銭的被害
- ・ コンピュータウイルスやワームの広範な感染

などが挙げられる。ここでクライアントにおける情報セキュリティに特徴的なのは、ユーザデータの保護に強く関係するという点である。例えば、コンピュータ内の情報が漏洩することなどによるプライバシーの侵害や金銭的被害とは、クライアント上に保存されたデータの機密性の保護が破れたことによる。また、コンピュータウイルスやワームの蔓延というのは、ユーザデータの完全性が保たれなくなった結果として可用性が失われたと解釈することができる。しかし、音楽コンテンツなどの不正コピーの蔓延は、ユーザデータそのものに関する問題であるにも係わらず、従来のセキュリティの概念（機密性・完全性・可用性）で捉えることが困難である。この意味で、クライアント上の情報セキュリティを考える際に最も重要なのは、著作権保護や不正コピー防止技術を含んだユーザデータ保護であることがわかる。

著作権保護や不正コピー防止技術が従来の情報セキュリティ技術に比べて技術的に異なる点は、実は要素技術という面ではあまり相違はない。つまり、この基盤にあるのは暗号技術や認証技術である。しかし、質的に最も大きな相違といえるのは、伝統的な情報セキュリティでは主に外部からの攻撃を想定するのに対して、クライアント上の情報セキュリティでは、時として正当なアクセス権限を持つユーザやデータの所有者からの攻撃をも想定しなければならない点にある。

この特質は特にクライアントマシンにおいて顕著なものであり、伝統的な情報セキュリティの枠内で捉えることが難しい原因ともなっている。本標準技術集では、特に従来の情報セキュリティの枠内では捉えることが困難な、クライアント上のセキュリティ技術に焦点を絞り、その標準的な技術を可能な限り体系的に整理することを試みている。ただし、クライアント上のセキュリティ技術に限定したとしてもその対象領域は広範であるため、ここでは、古くからよく知られ、体系化されているネットワーク上の暗号・認証技術や狭義のネットワークセキュリティ技術を除くこととした。

## (2) 歴史

狭義のクライアント上の情報セキュリティ技術の歴史は、PCの普及とほぼ軌を一にしているが、その萌芽はPC誕生以前に遡ることができる。ここでは、クライアント上の情報セキュリティ技術の中心を占めるデータ保護技術、特に不正コピー防止や著作権管理技術とその背景となった社会状況に焦点を絞って、その歴史的な発展について概観する(表1)。

コンピュータ上の不正コピー防止技術は、現在では音楽や映像ソフトの不正コピーの文脈で語られる場合が多いが、当初は主にコンピュータプログラムの違法コピーに焦点が当てられていた。コンピュータソフトウェアが市場性のあるコンテンツであると認識されるようになったのは、ミニコンピュータの登場以降とされる<sup>1</sup>。それ以前のコンピュータプログラムは基本的にオーダーメイドであり、それが単独で流通するようなことはなかった。ミニコンピュータ向けのパッケージソフトの登場に伴い、違法コピーの問題がクローズアップされるようになったが、当初は内部犯行、つまり開発者による別会社への持ち出しが主要な問題とされ、この防止のためにソフトウェアバースマーク技術が導入された。ソフトウェアバースマークは一種の電子透かしとも考えられる。1970年代後半になると、ソフトウェアの不正コピーを防止する技術が導入されるようになったが、これは主にプロセッサシリアル番号など、ハードウェアを用いたプロテクションが用いられている。

1977年にアップルコンピュータからPCの普及に大きな功績のあったApple IIの販売が開始された。翌1978年にはPC用としては世界初のフロッピーディスクドライブDisk IIが発売され、ソフトウェア流通の基盤が整った。PCにはプロセッサシリアル番号が無く、ミニコンと同様のプロテクション技術の利用は出来なかったことから、当時は主にフロッピーディスクに特殊な書き込み技術を適用することでコピー防止を図ることが多かった。1981年にIBM PC、1984年にその後継機であるIBM PC/ATの販売が開始され、PCの一般への普及が急速に始まった。また1983年には家庭用ゲーム機として爆発的に普及した任天堂ファミリーコンピュータの販売が開始された。PCにおける不正コピー防止技術の発展はこのころからしばらく停滞する一方、家庭用ゲーム機向けのソフトウェアには主にハードウェアベースの不正コピー防止技術が採用されることになった。

これらコンピュータの発展とは並行して、音楽や映像コンテンツについての不正コピー防止技術も開発されてきた。1975年に家庭用のビデオデッキが開発されてから1980年代中旬にかけて、複数の不正コピー防止用の技術が開発されている。一方では、家庭における私的録画の正当性が議論されたのもこの時期である。1984年に米最高裁判所はいわゆるベータマックス裁判において、私的録画は合憲であるとともに合法的な用途のある技術はその違法な利用について責任を負わないとする有名な判決を下した。この判例はその後のNapster裁判においても引用されるなど、その後の不正コピー問題に大きな影響を与えた。1982年になるとCDが発売され、コンテンツのデジタル化に先鞭をつけた。

---

<sup>1</sup> Ross Anderson, "情報セキュリティ技術大全", 日経BP社, 2002年9月9日, ISBN4-822-8142-6

表 1. クライアント上の情報セキュリティ(著作権保護と不正コピー関連)に関する年表

年代	イベント
1960 年代	ミニコンの登場
1970 年代中旬	ミニコン向けパッケージソフトウェアの登場
	ソフトウェアバースマークの導入(退職者によるソフトウェア持ち出しの防止)
1975 年	家庭用ビデオデッキ発売 Sony SL-6300
1976 年	アップルコンピュータ設立、同年 Apple I を発売
1977 年	Apple II 発売
1970 年代後半	著作権保護メカニズムの導入(プロセッサシリアル番号等)
	業務用 TV ゲーム(インベーダーゲーム等)の ROM イメージコピーが問題になる
	Apple II の DISK II(フロッピードライブ)の機能を活用したコピープロテクション技術が多く考案される
1980 年	米国著作権法改正によりプログラム及び DB に著作権が認められる
1981 年	IBM PC 発売
1982 年	IBM 産業スパイ事件が発生、ソフトウェアの著作権に注目があつまる
	CD (Compact Disc) 発売
1983 年	家庭用ゲーム機(任天堂ファミリーコンピュータ)発売
	森による超流通の提案
1984 年	現在の PC の原型である IBM PC/AT が発売される
	私的録画は合憲(米ベータマックス裁判)
1980 年代前半	家庭用ビデオの違法コピー防止・スクランプリング技術が相次いで開発される
1980 年代中旬	家庭用のソフトウェア市場がゲーム機市場と PC 市場に大きく分かれる。
1986 年	日本でも著作権法改正されプログラムの著作権が認められる
1996 年	「著作権条約」「実演・レコード条約」が WIPO(世界知的所有権機関)で締結
1998 年	SDMI(Secure Digital Music Initiative)が結成される
	DMCA(Digital Millenium Copyright Act)が成立(2000 年施行)し、著作権保護回避を禁止
1999 年	全米レコード協会 RIAA が Napster を提訴
	著作権保護技術「MagicGate」を採用したマジックゲート メモリースティックが発売
	著作権保護技術 DTCP(Digital Transmission Content Protection)第 1 版が発行される
2000 年	米における CD 出荷額が落ち込み、全米レコード協会 RIAA はその原因を Internet にあると推測
	アメリカ映画協会(MPAA)が DVD の暗号解読ソフトを掲載した雑誌を訴える
2001 年	P2P による音楽コンテンツの共有が Napster 裁判で違法とされる
	著作権管理関係のワークショップ 2001ACM Workshop on Digital Rights Management が開催
	日本でファイル交換ソフトを利用した著作権(送信可能化権)侵害容疑の逮捕者が出る
2002 年	著作権保護特許で有名な InterTrust 社が Sony/Philips 社に買収される

1987年にはテープメディアでデジタル録音の可能な DAT が発売された。しかし、国際レコード・ビデオ製作者連盟（IFPI：International Federation of the Phonographic Industry）は不正コピー問題が解決されていないという理由で、DAT の販売に強硬に反対したことなどから、DAT は発売早々、一時販売停止に追い込まれた。そのため DAT には SCMS（Serial Copy Management System）と呼ばれる多重ダビングを防ぐ技術が導入されたが、発売当初の混乱などの理由で DAT 自体が広く普及することは無かった。なお SCMS はその後発売された MD にも採用されている。

1990年代末になると、PCの性能向上に伴いPC上で音楽や映像を扱うことが一般化してきた。さらにインターネットの発展と相まって、不正コピー問題は大きな社会問題となった。1999年になると、米国においてCDの売上に翳りが見られるようになったこともあり、全米レコード協会（RIAA：Recording Industry Association of America）はインターネット上の不正コピーを強く糾弾するようになった。RIAAによるNapsterの提訴<sup>2</sup>はその一環である。

このような中で著作権保護技術に対する社会的なニーズは急激に高まってきた。先駆的な業績として1983年の森による超流通の提案があるが、ネットワーク上のコンテンツ流通を想定した不正コピー対策技術や著作権管理技術が発達したのは1990年前半から中旬にかけてである。現在の不正コピー対策技術や著作権管理技術の多くは、この時代に完成したといえよう。例えば、著作権対策の取られていない音楽メディア（MP3等）に対する著作権保護技術を開発しようとする試みとして、1998年にSDMI（Secure Digital Music Initiative）が結成<sup>3</sup>された（2001年に活動中断）。また、1999年にはDTCP（Digital Transmission Content Protection）の第1版が公表<sup>4</sup>されると共に、著作権保護技術が適用されたICメモリデバイス（メモリースティック<sup>5</sup>）が発売されている。これらの研究開発の活発化を受けて、2001年にはACM（Association for Computing Machinery）学会で著作権管理に係るワークショップ（ACM Workshop on Digital Rights Management）が開催<sup>6</sup>されるなど、独立した学問分野としても認められるようになってきている。ビジネス面でも、2002年には著作権保護技術に関する特許で知られるInterTrust社がソニーとオランダフィリップス社に買収されるなどの動きがある。

本技術集では主に1990年代中旬以降に開発された技術を対象とするが、これら技術の基礎となった技術については可能な限り収録することに努めている。

---

<sup>2</sup> RIAA, "Recording Industry Sues Napster for Copyright Infringement", <http://www.riaa.com/news/newsletter/press1999/120799.asp>, 1999

<sup>3</sup> Secure Digital Music Initiative, <http://www.sdmi.org/index.htm>

<sup>4</sup> Digital Transmission Licensing Administrator, <http://www.dtcp.com/>

<sup>5</sup> Sony, "小型IC記録メディア『メモリースティック』の新たな提案", <http://www.sony.co.jp/SonyInfo/News/Press/199909/99-072/>, 1999

<sup>6</sup> 2003年度の開催要領は以下のサイトで見ることが出来る  
<http://www.acm.org/sigs/sigsac/ccs/CCS2003/drm.html>

## 2. 標準技術集の構成

### (1) 定義

本標準技術集で用いる語句について以下のように定義すると共に、本標準技術集の対象範囲を規定する。

- ・ クライアント: パーソナルコンピュータおよびその周辺機器を対象とする。
- ・ 情報セキュリティ技術: 情報セキュリティ技術の中で、ユーザデータの保護と、ユーザデータ保護のためのアクセス制御、利用管理技術を主たる対象とする。また、これらの要素技術が組み合わされて実現されるアーキテクチャと、その依拠するトラステッドシステムについても対象とする。
- ・ ユーザ(もしくはエンドユーザ): クライアントの利用者。
- ・ ユーザデータ: クライアント上に保存されるデータであって、ユーザが管理するデータ。OSなどのシステム基盤が利用するデータを除いたもの。文書ファイル、マルチメディアデータ、プログラムなどが対象となる。

したがって、本標準技術集「クライアント上の情報セキュリティ技術」とは、概ね「パーソナルコンピュータおよびその周辺機器におけるユーザデータの保護を目的とした技術」と規定される。

なお、本技術集では以下のような技術分野は対象外とする。

対象外の技術分野例:

- ・ ネットワークセキュリティ技術、サーバサイドセキュリティ技術
- ・ 暗号技術(AES等)・認証技術(PKI等)
- ・ 不正アクセス・ウィルス・ワーム対策
- ・ アクセス制御の中でもシングルサインオンなど、データ保護の観点と関係ないもの
- ・ セキュアプログラミング
- ・ アナログ化されたコンテンツ(印刷後等)の保護技術
- ・ サーバ側のコンテンツ配信技術および違法コンテンツ検知技術
- ・ 課金・クリアリング

ただし、耐タンパ技術、データ消去技術、メモリ保護・OSの排他制御技術の内、クライアント上の情報・データ保護の観点から行われたものについては取り上げた場合がある。境界領域に関しては、ケースバイケースで判断した。

### (2) 技術分野の構成

次に、クライアント上の情報セキュリティ技術に含まれる主要技術分野の構成とその概念整理を行う。

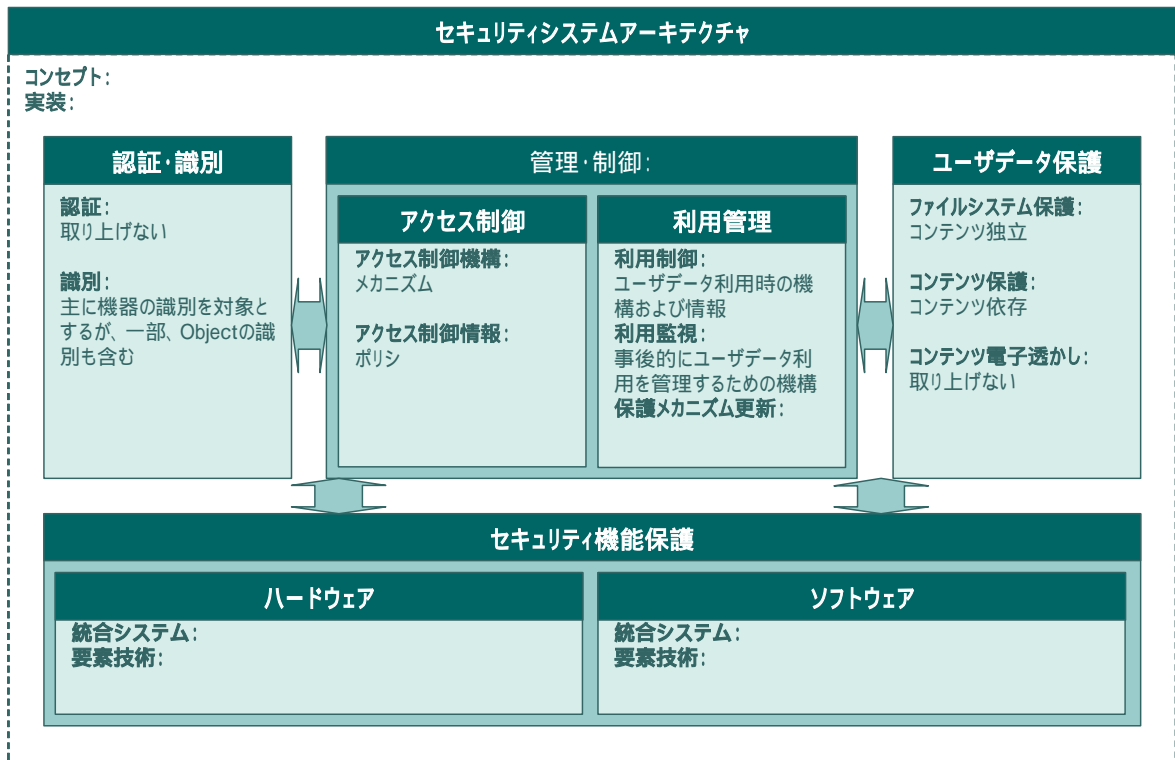


図 1. クライアント上の情報セキュリティ技術の構成と概念

(a) セキュリティシステムアーキテクチャ

ユーザデータ、特に著作者がユーザとは別に存在するコンテンツの保護を考えた場合、認証、アクセス制御、利用管理などの要素技術だけに着目することは木を見て森を見ないという事態に陥る。一般に、コンテンツの管理技術（著作権管理技術）の提案は、要素技術として提案されるよりも、当該コンテンツの配信、流通、データ保護、課金などをまとめたアーキテクチャの実装として提案される場合が多い。

また、これらの具体的な提案の背後には、より抽象的なコンセプトの提案がある。近年ではこれらのコンセプトについても特許化されることが多いため、ここでは標準技術集の対象とした。

(b) 認証・識別

個人・機器の認証・識別については、データ保護に密接な関係のある機器、メディア、データの識別以外はここではとりあげない。

(c) 管理・制御

管理・制御とはユーザデータの管理とその利用制御を行う技術分類である。これらはアクセス制御と利用管理に分けられる。

#### (c-1) アクセス制御

サブジェクトに対する制御技術についてまとめる。ここではメカニズム（アクセス制御機構）とポリシ（アクセス制御情報）という観点から整理を試みている、

#### (c-2) 利用管理

ユーザデータ（オブジェクト）に関する制御や管理を主な対象とする。ただし、技術内容によってはアクセス制御もしくはユーザデータ保護と厳密に分離することは困難な場合がある。利用管理は、1）利用制御、2）利用監視、3）保護メカニズム更新の各技術分野から構成される。

利用制御では、利用時における利用管理を対象とする。利用監視では、主に事後的な利用管理に用いるメカニズムについて対象とする。保護メカニズム更新には、CRL やブラックリストなどが含まれる。

#### (d) ユーザデータ保護

ユーザデータ保護とは、機密性、完全性、（可用性）を保護することを言う。主に OS で提供されるコンテンツ独立の技術分野について、「ファイルシステム保護」、コンテンツもしくはメディア依存の分野は「コンテンツ保護」と分類した。

なお、ユーザデータ保護技術のうち、コンテンツ電子透かしについては網羅性のため項目としては残すが、既存技術集への参照にとどめる。

#### (e) セキュリティ機能保護

以上のようなセキュリティ機能を実現するために必要となるハードウェア、ソフトウェアの基盤。なお、ISO/IEC 15408<sup>7</sup>（JIS X 5070）において規定されるセキュリティ機能保護とは、ユーザデータの保護を指すのではなく、セキュリティ機能が利用するデータを保護するための機構のこととされる。もちろん両者を厳密に分離することは不可能である。

---

<sup>7</sup> 情報処理推進機構セキュリティセンター, "セキュリティ評価・認証", <http://www.ipa.go.jp/security/index.html>

### 3. 技術動向

#### (1) セキュリティシステムアーキテクチャ

セキュリティシステムアーキテクチャの技術動向について一言でまとめると、理論から具体的実装に移っている段階であるといえる。理論面を見た場合、先駆的な業績として1983年の森による超流通の提案<sup>8</sup>がある。超流通システムでは、ユーザは計算機にSUM( Software Usage Monitor )を取り付け、プログラムが実行されるとSUMはプログラムに電子的に添付された使用条件をもとに使用記録を作成・管理する。ユーザはあらかじめ設定された条件にしたがって使用記録を転送することによって課金される。超流通においては従来の有体物の取引では不可能であったような、試用課金、従量課金、特別許諾、無料だが使用状況の報告を義務付けるものなど、様々な課金形態が可能であり(図2)、コンテンツの特色に応じて自由に選択することができる。超流通モデルの実現例としては、例えばケータイ de ミュージック<sup>9</sup>などがある。

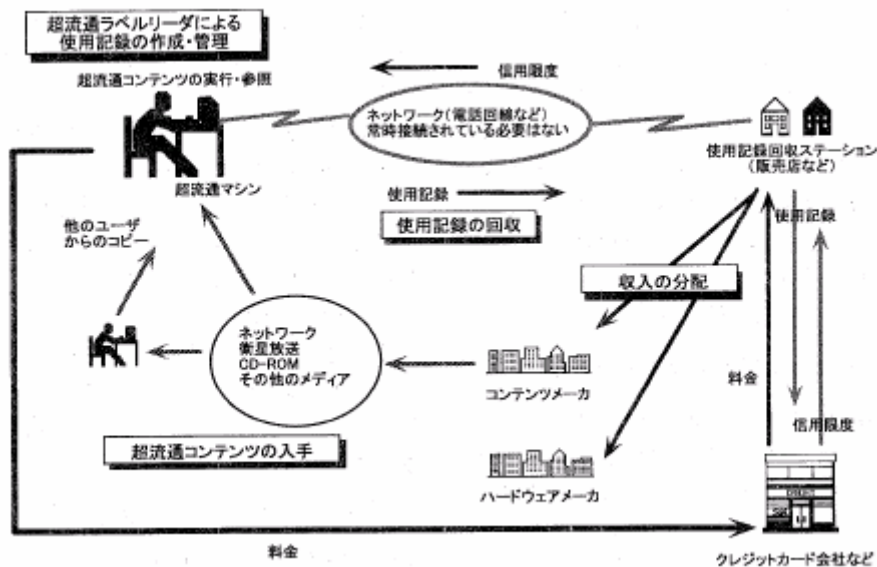


図2. 超流通システムの一例

出典:「マルチメディア社会をめぐる法律問題 - 知的財産権を中心として - 7. 超流通: 知的財産権処理のための電子技術」,「情報処理学会論文誌 Vol.37 No.2」(1996年2月) 森亮一、河原正治、大瀧保広著、(社)情報処理学会発行、158頁、図1、超流通システムの一例

ただし、森の当初の超流通は、利用時・実行時における制御・課金を重視し、ユーザに

<sup>8</sup> 森亮一, "ソフトウェア・サービスについて", JECC ジャーナル, No.3, pp.16-26 (1983)

<sup>9</sup> ケータイ de ミュージック・コンソーシアム,  
[http://www.keitaide-music.org/index\\_j.html](http://www.keitaide-music.org/index_j.html)

よるコピー・流通は自由とする概念であったが、コンテンツホルダの意向や著作権法の問題もあり、コピー・流通をも自由とするサービスを実際に提供しようとするところは稀である。したがって、現在の著作権管理システムは、メディアやコンテンツの性質に応じて多種多様な仕組みが提案されている。BS デジタル放送のための著作権管理システムである、B-CAS<sup>10</sup>や、前述した SCMS、DTCP はその代表的な例である。

なお、ユーザデータ保護という観点からは、チェックインチェックアウトの仕組みが使われることも多いが、これについては管理・制御の項で述べる。

## (2) 認証・識別

個人・機器の認証・識別は、それ自身で大きな技術分野を構成している。本標準技術集ではデータ保護に密接な関係のある機器、データの識別と認証に焦点を絞る。

データ保護という観点から識別という問題を考えると、現在の技術的、あるいは商業的な焦点はデータの識別をどのように行うかに置かれている。特に近年注目が集まっているのはコンテンツ識別子と呼ばれる分野である。コンテンツ識別子にはいくつものバリエーションがあるが、どのように ID を付与するのか、どのように ID を埋め込むのかという観点が分類することが出来る。どのように ID を付与するかという方法には大きく分けて二通りあり、あらかじめセンター等で割り振った ID をコンテンツ ID とする方法と、コンテンツ自体の情報（たとえばハッシュ値）をコンテンツ ID とする方法がある。どのように ID を埋め込むかという方法にも大きく二通りあり、メタデータとして明示的に埋め込む方法と、電子透かし技術を用いる方法がある。これらの手法にはそれぞれ一長一短があり、用途に応じて使い分けられている。

コンテンツ識別という問題に大規模に取り組んだ初期の事例としては、データ保護という観点からは若干離れるが、米国で 1998 年に始まり、現在は世界中で利用されている DOI(Digital Object Identifier)システム<sup>11</sup>がある。これは主に書籍を対象とするもので、書籍情報を記述するメタデータのセットと一意に識別可能な ID を持つ。メタデータという文脈の中では、より初期の例として Dublin Core<sup>12</sup>などの例があるが、Dublin Core では一意に識別可能な ID のラベルは定義しているが、具体的な ID 付与までは未定義である。最近では、国内でもコンテンツ ID フォーラム<sup>13</sup>などの活動なされている。

一方、データ保護という観点から認証という問題を考えると、クライアントシステム間の認証、例えば PC と周辺機器の認証であるとか、PC とメディアの認証という問題が主要な論点である。代表的な例として、PC における不正コピーの防止を目的として dongle と呼ばれる装置が実用化されてきた。これは、PC のシリアルポートやパラレルポートに接続さ

---

<sup>10</sup> (株) ビーエス・コンディショナルアクセスシステムズ, <http://www.b-cas.co.jp/>

<sup>11</sup> International DOI Foundation, "The Digital Object Identifier System", <http://www.doi.org/>

<sup>12</sup> Dublin Core Metadata Initiative, <http://dublincore.org>

<sup>13</sup> コンテンツ ID フォーラム, <http://www.cidf.org/japanese/index.html>

れるハードウェアキーであり、最近では USB に接続されるものが一般化している。商用の技術でこの認証についての詳細を公開している例は殆どないが、一部の技術は標準化されることで技術情報が開示されている。

また、個人の認証という観点からは IC カードの利用が期待されている。特に企業などの組織内への普及が進んでおり、これを用いたシングルサインオン技術も開発されている。しかし読取装置が必要とされるために、クライアントセキュリティという観点からは一般への普及はこれからである。

例えば、DTCP は、オーディオやビデオなどのコンテンツの不正コピー、不正な取り出し、不正な改ざんなどを防ぐ暗号プロトコルであり、IEEE1394 等を用いたデバイス間での認証を行っている。DTCP の認証プロトコル AKE (Device Authentication and Key Exchange) では Full Authentication もしくは Restricted Authentication と呼ばれる認証を行い、鍵交換を行っている。

新しいデバイスが開発される度に新しい認証プロトコルが開発される状況は今後しばらく続くと思われるが、基本となる認証アルゴリズムにはそれほど新しいものはなく、認証技術の基本的な技術（チャレンジレスポンス等）が今後も用いられていくだろう。

### (3) 管理・制御

#### (3-1) アクセス制御

アクセス制御技術については、アクセス制御ポリシーの記述方法とその制御機構という観点から制御することができる。アクセス制御機構という観点からは従来からのリファレンスマニタ（アクセス制御モニタ）という考えがほぼ全てを包含している。一方、ポリシーについてはいくつかの考え方がある。現在、ユーザデータ保護という観点で多く用いられているのは、アクセス制御マトリクスである。現在ほぼ全てのクライアントデータ保護技術はアクセス制御マトリクスとその派生技術と考えられ、近い将来も大勢に変更はないだろう。しかし、多階層のアクセス制御やロールベースのアクセス制御も一部システムで導入が始まっていることから、特に企業や組織内のクライアントでは今後重要になると考えられる。

#### (3-2) 利用管理

利用管理技術はユーザデータ保護技術の中核をなすこともあり、さまざまな技術・手法が開発されている。特に利用制御については、チェックインチェックアウト、コピーの世代管理、コンテンツの移動、使用回数制限、使用期間制限、使用場所制限など、さまざまな目的・用途の技術が提案され実装されている。歴史的に見ても、DAT に採用されたコピー管理技術が SCMS(Serial Copy Management System)であったことを考えれば、デジタルコンテンツの管理技術として、利用制御技術は著作権管理の中核をなしてきたし、これからも中核であり続けるだろう。

利用管理技術に分類される技術の中で、現在大きな研究開発対象となっているのがその周辺分野にあたる利用監視技術と、保護システム更新技術である。これらは、利用制御技術を運用していく上で不可欠な技術分野であり、近年研究開発が活発化しているのは、著作権管理技術の実用化が進んでいることと関係がある。

利用監視技術の基本は、利用のログをクライアントシステムやセンター等に残すというものであるが、近年では一歩進んで、トレイタートレーシング (traitor tracing) と呼ばれる技術開発が活発化している。トレイタートレーシングとは、不正な端末の監視追跡を行う技術である。

また、保護システム更新技術とは、データ保護に用いられる暗号鍵が一般に流出したり、暗号システムが危殆化したり、もしくはトレイタートレーシングの結果不正な端末を発見した場合に、鍵や暗号システムを更新したり、端末の無効化を行うための技術である。DVDにもこの種の技術 (CPPM: Content Protection for Pre-Recorded Media<sup>14</sup>) が用いられていることは広く知られているが、これは正しく CSS と呼ばれる DVD のスクランプリング技術が破られたために考案されたものである。

#### (4) ユーザデータ保護

ユーザデータ (オブジェクト) の保護技術は利用管理技術と並んで、クライアント上の情報セキュリティ技術の中で核をなすものである。ユーザデータ保護技術には OS で提供されるコンテンツ独立の技術分野としてファイルシステム保護技術と、コンテンツやメディアに依存したコンテンツ保護技術から構成されている。もちろんこれらのデータ保護技術のベースには暗号技術が存在しているが、暗号技術自体は本標準技術集の対象としない。

ファイルシステム保護技術の主要な技術には、暗号化ファイルシステムがある。暗号化ファイルシステムは既に Microsoft Windows 2000 から、そのファイルシステム NTFS の標準機能 EFS<sup>15</sup>として組み込まれているため、一般にも広く活用されている。近い将来には PC に暗号化 HW が組み込まれることが想定されているため、暗号化ファイルシステムはより広範に用いられると共に、本技術が著作権管理技術ともリンクすることが想定される。また、近年では PC のネットワーク化が進んでいることから、PC 上のデータをネットワーク上で分散保存することでデータ保護を行う研究も行われている。多少変わった例では、P2P ソフトとして有名な Winny の暗号化機能は、データ保護を目的としたというよりも、匿名性を高める目的で使われている。

コンテンツ保護化としては、暗号化技術、カプセル化技術、複製防止・原本性保障技術などがある。ここでの暗号化技術では、暗号技術そのものではなく、周辺機器やメディアに依存する部分を対象とする。したがって、この部分の技術は周辺機器やメディア毎にあ

---

<sup>14</sup> 4C Entity, <http://www.4centity.com/>

<sup>15</sup> Microsoft Corp., "Encrypting File System for Windows 2000", <http://www.microsoft.com/windows2000/techinfo/howitworks/security/encrypt.asp>

るといっても過言ではない。ただしそこで用いられている暗号技術は概ね標準的な技術が用いられる傾向にあり、その意味では同種の技術として考えても良い。

カプセル化技術について厳密に定義することは困難だが、単なる暗号化ではなく、その利用制御に関する情報や、ライセンスに関する情報を含むものと定義すれば、非常に広範に用いられている技術といえる。例えば、Microsoft の Windows Media で用いられている Windows Media Rights Manager<sup>16</sup>では、コンテンツのパッケージに際して、単に暗号化するだけでなくライセンスサーバ(コンテンツの復号鍵を持つサーバ)への URL 情報などを含んだ形でパッケージされる。このカプセル化技術は、もともとは超流通の提案に含まれると解釈される。

複製防止・原本性保障技術については、商用で利用されている例は少ない。ソフトウェアだけで実現することは困難であるためハードウェアと組み合わせられる手法が検討されている。

なお、ユーザデータ保護技術のうち、コンテンツ電子透かしについては網羅性のため項目としては残すが、既存技術集を参照されたい。

#### (5) セキュリティ機能保護

以上のようなセキュリティ機能を実現するために必要となるハードウェア、ソフトウェアの基盤技術であり、最近注目を浴びている。しかし歴史的に見れば、新しい概念ではなく、その殆どが汎用機の時代が開発され、実際に汎用機の上で利用されているものである。例えばセキュリティ機能保護技術の一つとして取り上げたサンドボックスを実現するための手法である仮想機械 (Virtual Machine) は Java 等により有名になった技術であるが、もともとは汎用機 (IBM OS/360) の上で実用化されたものである。このように、近年クライアントシステム、特に PC のセキュリティ強化が叫ばれるようになって、PC の汎用機化が進むという一種の先祖返り現象が見られる。逆に言えば、新しいセキュリティ保護のコンセプトの研究が最近停滞気味であることを示しているといえよう。

セキュリティ機能保護について特に注目される動向として、PC における次世代セキュリティプラットフォームとして提案されている Intel 社の LaGrande<sup>17</sup>や Microsoft 社の NGSCB (Next-Generation Secure Computing Base<sup>18</sup>) がある。技術的な新規性はともかく、その影響の大きさを考えると、クライアント上の情報セキュリティ技術を考える上で注視していく必要がある。

一方、耐タンパ技術に関しては攻撃手法の高度化に伴い、防御側の技術である耐タンパ

---

<sup>16</sup> Microsoft Corp., "Digital Rights Management",  
<http://www.microsoft.com/windows/windowsmedia/drm.aspx>

<sup>17</sup> Intel Corp., "LaGrande Technology Policy on Owner/User Choice and Control",  
[ftp://download.intel.com/technology/security/downloads/LT\\_policy\\_statement\\_0\\_8.pdf](ftp://download.intel.com/technology/security/downloads/LT_policy_statement_0_8.pdf)

<sup>18</sup> Microsoft Corp., "Next-Generation Secure Computing Base",  
<http://www.microsoft.com/resources/ngscb/default.mspx>

技術も発展を続けている。特にソフトウェアの耐タンパ技術は比較的最近の技術であり、今後の発展が期待されている。