CMP(Crypto Microprocessor)を使用した超流通システムの一構成方法

末松 俊成
ナカミチ株式会社
〒187-8501 東京都 小平市 鈴木町 1-153
TEL:042-345-3353
E-mail:t-suem@nakamichi.co.jp

今井 秀樹
東京大学 生産技術研究所
〒106-8558 東京都 港区 六本木 7-22-1
TEL:03-3402-6231
E-mail:imai@iis.u-tokyo.ac.jp

あらまし 暗号化／復号機能をもつマイクロプロセッサである CMP(Crypto Microprocessor)を利用した超流通システムについて述べる。CMP は暗号化／復号機能、秘密メモリ、CPU を内蔵する。ソフトウェア（プログラムやデータ）は、メモリや記憶装置内では暗号化され、CMP はソフトウェアを実行中に部分的に復号し、復号された形を見られないように処理できる。このため、ソフトウェアのセキュリティを強化できる。CMP を利用することにより、超流通システムの課金処理やソフトウェアの使用記録の管理を安全に処理するシステムを、ソフトウェアによって構築する事が可能になる。また、ソフトウェアによって構築するシステムであるため、バージョンアップなどのメンテナンスが行い易いという利点もある。

キーワード CMP、マイクロプロセッサ、超流通、ソフトウェア流通、情報セキュリティ、著作権

A Construction Method for SD Systems Which Make Use of the CMP

Toshinari SUEMATSU
Nakamichi Corp.
1-153 Suzuki-cho,Kodaira,Tokyo 187-8501
TEL:042-345-3353
E-mail:t-suem@nakamichi.co.jp

Hideki IMAI
University of Tokyo
7-22-1 Roppongi,Minato-ku,Tokyo 106-8558
TEL:03-3402-6231
E-mail:imai@iis.u-tokyo.ac.jp

Abstract In this paper, we present a new SD(Super distribution) System which makes use of the CMP(Crypto microprocessor). CMP contains encipher/decipher units, a secret memory, and CPUs(Central processing unit). Software(programs and data) are enciphered in memory and storage devices, and the CMP deciphers the enciphered software piecemeal as executing, so that software can be securely executed without disclosing the deciphered form. Therefore, security of software is protected strictly. Using CMP for the SD system makes it secure to manage fees and records of uses of software. In addition its maintenance is easy, because the whole SD system is constructed by software.

Key words CMP, Microprocessor, Super distribution, Software distribution, Information security, Copyright

1. まえがき

コンピュータ上で使用されるソフトウェア（本稿では、プログラムやディジタルデータなどの総称とする）の不正使用や違法コピーを防ぎ、ソフトウェア製作者の権利を保護することは、ソフトウェアの健全な流通・利用・発展を進める上で重要な問題である。

ソフトウェア開発者が適正な利益を確保できるようになれば、流通するソフトウェアの価格は下がり、正規ユーザが支払うべき対価も低くなるという好循環が期待できる。また、ソフトウェア開発者は、この利益をより優れたソフトウェアの開発に投資することができ、ソフトウェア業界の発展につながる。

このような目的をもった新しいソフトウェア流通システムとして超流通が知られている[1-4]。これは、ソフトウェアの使用記録を管理し、それを回収することによって料金を徴収するシステムである。このシステム上では、ソフトウェアは全くまたはほとんど無料（媒体や手数料などの必要最小限の代金）で配布し、利用者がソフトウェアを使用したとき，その頻度に応じて課金を行う。

従来のように，ソフトウェアを「所有」することに対価を支払うのではなく、「使用」することに対価を支払うことを可能にするシステムである。

ソフトウェアの使用時に課金するため、コピーを防ぐ必要はない。ユーザはソフトウェアを自由にコピーして使用することができる。

一方、ソフトウェアの秘密を守り、不正使用を防ぐ方法として、CMP（Crypto Microprocessor）が知られている[5-7]。

通常のマイクロプロセッサは、機械語と呼ばれる命令に従って処理を行う。マイクロプロセッサが処理する命令は、主記憶メモリに置かれ、これはデバッガなどのツールによって比較的簡単に見る事ができる。このため、機械語を理解する攻撃者が処理内容の解析を行い、重要な情報を得ようとするのを防ぐ事は困難である。

例を挙げると、暗号化したデータをソフトウェアで復号するシステムの場合、復号処理をデバッガなどのツールを用いて解析されて、コンピュータの主記憶メモリに現れる復号鍵や復号データを盗み見られる危険がある。

これに対し CMP は、主記憶メモリや外部記憶装置上ではソフトウェアを暗号化しておき、CMP内部で復号して処理することが可能である。このため、復号した機械語やデータを外部に見せることなく処理でき、ソフトウェアの安全性を高められる。

本稿では、CMP を利用することによって安全性と利便性を高めた超流通システムを提案する。

2. CMP を利用することの意義

まず、従来提案された典型的な超流通システムについて説明しておく。超流通システム上でユーザが使用するソフトウェアを、超流通ソフトウェアと呼ぶ。超流通ソフトウェアには、課金情報を含む超流通ラベルが付加される。ユーザが使用するコンピュータには、SUM（Software Usage Monitor）または超流通ラベルリーダと呼ばれる専用のハードウェアが取り付けられ、これが超流通ソフトウェアの実行の制御と超流通ラベルに従った課金処理を行う。SUM に貯えられたソフトウェアの使用記録と課金情報は、通信回線などを通じて超流通システムを運用する管理センタに回収され、決済が行われる。

この方式を普及させるには、まず SUM という専用ハードウェアの規格化を進め、これを普及させなければならない。また、運用開始後に鍵の変更やシステムの変更を行おうとすると、ハードウェアの交換が必要など、運用上の問題が考えられる。

これに対して、SUM の機能をコンピュータ上のソフトウェアによって実現し、特別なハードウェアを使用せずに超流通システムを実現するシステムが提案されている[8]。しかし、この方式は、全ての処理をソフトウェアが行うため、セキュリティの面で十分とは言えない。

CMP 内蔵コンピュータを使用することによって、上記の問題を解決することができる。

CMP も、超流通に使用することだけを目的とした場合には、SUM と同じように専用のハードウェアと見なすこともできる。しかし、SUM と異なり、次の利点がある。

(1) CMP は超流通以外にも、ソフトウェアやデ

ータの暗号化などに幅広く応用できる。例えば、コピー自由の買い取り方式ソフトウェアなどが簡単に実現できる（4.で説明）。

(2) SUMは、その内部で処理するデータだけを守ることができるが、外部（主記憶メモリや外部記憶装置上）に置いてCPUが処理するソフトウェアは保護できない。CMPは、これら外部のソフトウェアも含めて保護できるので、セキュリティの向上が見込める。

(3) CMP上で実行するソフトウェアによってシステムを構築するため、システムのバージョンアップなどの作業を効率的に行うことができる。ハードウェアであるSUMの場合、システムの変更には大きな手間とコストが必要とされる。

超流通に限らず、CMPは今後のコンピュータシステムのセキュリティを考える上において、重要な位置を占めることが予想される。このCMPを超流通にも利用することで、CMPの普及を促し、ソフトウェアの健全な流通、著作権の保護といった環境が整備されてゆくことが期待される。

3. CMPの概要

本システムで使用するCMPを図1に示す。これは、次の特徴を持つ（詳しくは文献[5]参照）。

- CMPは、暗号処理ユニットを内蔵したマイクロプロセッサである。
- ソフトウェアは、ハードディスクなどの記憶装置や主記憶メモリ上では暗号化された状態で保管される。
- ソフトウェアは、CMP内部で復号して処理される。このためソフトウェアの秘密を守ることができる。
- 復号鍵を知らないと、デバッグも不可能。
- 2重鍵方式の採用。個々のCMPに固有の秘密鍵を持たせ、これは作業鍵の暗号化／復号に用いる。ソフトウェアの暗号化／復号には作業鍵を用いる。
- アドレスによるデータスクランブル機能の採用。ソフトウェアは、メモリ上の相対アドレスに応じたデータスクランブルをかけ、その後に暗号化する。このため、同じ値が続いた場合でも、暗号化データは場所によって異なる値となり、解読を困難にできる。当然、復号の際にはデスクランブル処理が必要である。
- ソフトウェアの一部だけ暗号化することも可能とする。このため暗号化／復号の制御ユニットを内蔵する。
- ソフトウェア処理途中で暗号処理のON/OFF切り替えができるような手段を持つ。
- CMP内部に、秘密メモリを持ち、ソフトウェアが任意の値を隠すことができる。

秘密メモリについて説明しておこう。これは、CMP内部に隠されたメモリで、コンピュータの電源を切ってもその内容が保持される。データのアクセス方法に制限を加えて、ソフトウェアが任意に決定した秘密の値を隠しておけるようにしたものである。

代表的な使用例としては、外部記憶装置上に作成されるファイルに秘密の値を書き込み、それをCMP内の秘密メモリにも保管しておくことで、ファイルの改ざんを検出するのに使用できる。

次に秘密メモリの特徴を示す。

- CMPを通して値の書き込みはできるが、値の読み出しはできない。
- 値の保管場所を指定するのに、メモリのアドレスではなく、パスワードを使用する。データを保管する場所はCMPが勝手に選択するので、パスワードを知らないとデータにアクセスできない。パスワードは、秘密メモリに秘密データを書き込むソフトウェアが適当に選択する。
- 秘密メモリに保管した値と外部から与えられた値とを照合し、一致するかどうかを知ることができる。すなわち、値を記録したソフトウェアは、その値をファイルに保管しておき、この値と秘密メモリの値を照合することによってファイルの正当性を確認できる。
- 秘密値を書き換えるには、パスワード、元のデータ、書き換え後のデータをCMPに渡さなければならない。
- 秘密値を消去するには、パスワード、元のデータをCMPに渡さなければならない。

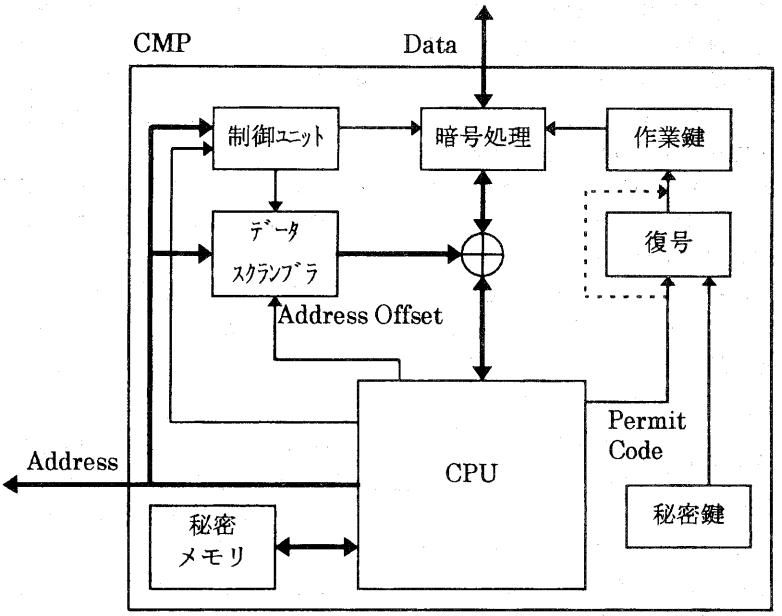

図1 CMP 構成 A

秘密メモリのデータの照合／変更／消去を行うには、パスワードと秘密値の両方を知らなければならない。これによって不正な書き換えを防ぐ事ができる。

秘密メモリは、CMP 上で使用することに効果がある。仮に通常のマイクロプロセッサに同様の機能を付けたとしても、秘密メモリにアクセスする機械語をデバッガなどで解析されるとパスワードや秘密値などが簡単に知られてしまう事になる。

秘密メモリの具体的な使用方法については、6.を参照されたい。

4. 買い取り方式ソフトウェア

CMP の基本的な使用方法として、ユーザがソフトウェアのコピーを自由に取る事ができ、かつ利用を CMP ごとに制限できる買い取り方式のソフトウェア流通がある。この方法について簡単に説明しておく。

- CMP メーカは、CMP の SN（Serial Number）ごとの秘密鍵と公開鍵を保管する。秘密鍵は CMP 内部に封じ込められる。
- ユーザは、自身の CMP の SN から作業鍵暗号化用公開鍵 K_{CMP} を入手する。
- 暗号化ソフトウェアを購入し、ソフトウェア供給者に CMP の公開鍵 K_{CMP} を連絡する。ユーザが CMP の SN を連絡し、ソフトウェア供給者が CMP メーカから K_{CMP} を入手しても良い。
- ソフトウェア供給者は、ソフトウェアの復号鍵 K_{SFT}（作業鍵）を K_{CMP} によって暗号化した Permit Code である P_{SFT} をユーザに送付する。

$$P_{SFT} = E_{CMP}(K_{SFT}) \quad (1)$$

- ユーザは CMP に P_{SFT} を入力することにより暗号化ソフトウェアが使用可能になる。

式(1)において、$E_X(D)$ は鍵 K_X でデータ D を暗号化したことを表すものとする。

Permit Code は、暗号化ソフトウェアの使用を特定の CMP に対し許可するものである。これを CMP にセットする方法としては、次のようなものが考えられる。

- 暗号化ソフトウェアを実行する前に、Permit Code 設定用のプログラム(暗号化されていない) を用いて設定する。
- 暗号化ソフトウェアの起動部だけは暗号化しない処理とし、その部分で Permit Code の設定を行う。

Permit Code は、CMP の SN とソフトウェアの暗号化鍵 K_{SFT} との組み合わせによって決定される。他のソフトウェアや CMP では利用できない。

本方式によれば、ソフトウェアを使用できるのは、自身の CMP に対応した Permit Code を入手した正規ユーザだけであるため、ソフトウェアのコピーを制限する必要は無い。

これにより、ソフトウェア供給者の権利を保護しつつ、ユーザにもコピープロテクトなどの不便を与えずに済む。

この方法は、各 CMP が固有の秘密鍵を持つことを利用している。この秘密鍵を直接ソフトウェアの暗号化／復号に使用することも考えられるが、その場合ソフトウェア供給者は CMP ごとに異なる鍵で暗号化したソフトウェアを配布しなければならず、運用上の手間が大きい。

本方式によれば、ソフトウェアの暗号化鍵 (K_{SFT}) は一つで良く、各 CMP ごとにソフトウェアの使用を許可する Permit Code を配布するだけで良い。また、ソフトウェアの暗号化鍵を一つに限定せず、必要に応じて地域別、バージョン別などに応じて変えることも可能である。

なお、Permit Code は、ユーザではなく CMP に対して与えられるものであることに注意しなければならない。複数のコンピュータを所有するユーザが、全てのコンピュータ上でこのソフトウェアを使用することを希望する場合、各コンピュータには異なる CMP が入っているため、所有するコンピュータの数だけ Permit Code を入手する必要がある。

5. 超流通システムの構成

CMP 内蔵コンピュータを使用した超流通システムについて述べる。超流通システムを構成するソフトウェアは、次のように分類できる。

(a) 超流通システム・インストールプログラム
(b) 管理センタとの通信プログラム
(c) 使用管理プログラム
(d) 使用権利データファイル
(e) 超流通ソフトウェア

(a)～(d)は超流通システムを利用できる環境を整えるためのもので、これらをまとめて超流通システムソフトウェアと呼ぶ事にする。これらは暗号化されたソフトウェアであり、管理センタなどから入手する。

(e)はユーザが実際に利用したい超流通ソフトウェアで、その開発者が配布するものである。この暗号化鍵は、各開発者がソフトウェアごとに設定する。

これらのソフトウェアは、暗号化して処理内容が第 3 者に知られないようにする。必要ならば、課金処理のように重要な部分だけを暗号化し、その他の部分は暗号化しないという形式を取る事もできる。暗号化しないことの利点としては、復号処理を省略できるため、高速に実行できることが挙げられる。この方式を取る場合、安全性と実用性を考慮し、暗号化する部分としない部分を慎重に決定する必要があろう。

以降(a)～(e)のソフトウェアについて説明する。

超流通システム・インストールプログラムは、超流通システムをコンピュータの記憶装置（ハードディスクなど）にインストールするものである。

管理センタとの通信プログラムは、使用記録、課金情報、使用権利データなどを、通信回線を通して管理センタとの間で送受信するためのプログラムである。

使用管理プログラムは、使用記録の管理や課金処理を行う。

使用権利データファイルは、当ユーザに与えられた超流通ソフトウェアの使用権利の残高を示すものである。この値が残っている間は超流通ソフトウェアを利用できる。このファイルには、ユーザの使用記録が記録されていき、ユーザが使用する間、使用済み権利の記録と未使用の権利の合計は常に一定の値になる。

超流通ソフトウェアは、超流通システム上で利用できるプログラムやデータである。超流通システムをインストールし、環境が整った後にこれらのソフトウェアを、ユーザが利用できる。

超流通ソフトウェアは、次の特徴を持つものとする。

- ソフトウェア識別用の超流通ソフトウェアID（SD-ID）を持つ。
- 必要に応じ、超流通ラベルを持つ。
- 超流通システムがインストールされない環境では、実行できないようになっている。

各超流通ソフトウェアの課金情報は、従来のシステムでは、超流通ソフトウェアに組み込まれた超流通ラベルに記録されることとされていた（超流通ラベル添付方式）。これに対し、文献[9]のように超流通ラベルを管理センタが配布する方式も提案されている（超流通ラベル配布方式）。本システムは、上記いずれも利用可能であり、併用もできる。このため、各ソフトウェア製作者が好きな方を選択すれば良い。

使用管理プログラムは、超流通ソフトウェアの中に超流通ラベルを見つければ、それに従って課金処理を行い、超流通ラベルが無い場合には、SD-ID を管理センタに通知して、対応する課金情報（超流通ラベル）を受け取り、SD-IDと共に内部テーブルに登録する。以降、課金処理はこのテーブルを参照して行う（詳細は文献[9]参照）。当然このテーブルは暗号化によって保護される。

本システムは、ソフトウェアによって構築するので、必要に応じてシステムをバージョンアップするなど、柔軟な対応が可能である。

使用料金の決済方法は、ユーザがあらかじめセンタから使用権利を購入し、その権利データをユーザの記憶装置にインストールし、これを超流通ソフトウェアの使用に応じて減算するシステムとする。プリペイドカードなどと同じ前払い方式である。

使用記録を残しておき、後で清算する方法も可能であるが、使用記録をユーザの記憶装置内に置いておくと、ユーザによって使用記録を抹消される恐れがあるため、前払い方式の方が無難であろう。前払い方式の場合、権利データを改ざんしたり消したりした場合、ユーザが権利を失い不利益を被ることになるため不正を抑止する効果が期待できる。

6. 超流通システム利用の手続き

6.1.登録

管理センタに連絡し、ユーザ登録を行う。登録に最低限必要な情報は、次のようなものであろう。

- 氏名
- 住所
- 連絡先（電話、FAX、E-Mail など）
- 口座番号またはクレジット番号（権利データ購入などの決済に使用）
- CMP のシリアル番号
- CMP の公開鍵(K_{CMP})

登録が済んだら、センタは超流通ソフトウェアのインストールプログラムと、超流通システムの暗号化鍵 K_{SD} を K_{CMP} で暗号化した P_{SD} をユーザに渡す。ここで

$$P_{SD} = E_{CMP}(K_{SD}) \qquad (2)$$

である。P_{SD} を受け取ったユーザは、公開鍵 K_{CMP} に対応する CMP を内蔵するコンピュータ上で超流通システムを利用することが許可される。他のコンピュータで使用するには、別途 Permit Code を入手する必要がある。

なお K_{SD} は超流通システム全体で共通にしても良いし、必要に応じて地域、バージョンなどの条件によって変えても良い。

6.2.インストール

ユーザは、入手した P_{SD} と超流通システム・インストールプログラムによって超流通システムをインストールする。その結果、5.で示したファイルがユーザのコンピュータ上に構築される。この時点では、使用権利データファイルは、残高が 0 になっており、超流通ソフトウェアが実行できない。

このときインストールプログラムは、秘密の値を任意（乱数など）に生成し、残高 0 の使用権利データファイルと CMP 内部の秘密メモリの両方に記録する。この作業によって、使用権利データファイルが、この CMP 上で使用できる環境が整う。この秘密値が一致しない使用権利データは、この CMP の元では利用することができない。

6.3.使用権利の入手

ユーザは、インストールプログラムによって作成された（残高 0 かつ秘密値が記録された）使用権利データファイルを管理センタに送付し、権利データを充当してもらう。管理センタは対価をユーザの口座から引き落とす手続きを行い、ユーザに使用権利データファイルを返送する。

このとき、使用権利データファイル中の秘密データは変更してはならない。これを変更してしまうと、ユーザの持つ CMP 上で利用できなくなる。

ユーザは、権利が充当された使用権利データファイルを受け取り、自己のシステムにインストールする。基本的には権利 0 のファイルに上書きすれば良い。しかし、この処理も専用のインストールプログラムが行い、秘密値が一致するかなどを確認の上ファイルの更新を行うようにした方が安全である。

6.4.超流通ソフトウェアの実行

以上で超流通ソフトウェアを使用する環境が整ったので、ユーザは希望する超流通ソフトウェアを入手し、自己のコンピュータ上で実行できる。超流通ソフトウェアの使用状況は、使用管理プログラムによって管理され、既定の条件に従って使用権利データファイルの権利データが減算されるとともに、使用記録が使用権利データファイルに追加される。

使用権利データファイルの内容を書き換えるときは、秘密データの値も更新し、その値を秘密データファイルと CMP の秘密メモリの両方に保管し直す。

秘密値を変更するのは、ユーザの不正利用を防ぐためである。例えば、ユーザが使用権利が一杯の状態の使用権利データファイルのコピーを保管しておき、残高が少なくなってきたときに、このファイルを上書きして残高を増やそうとしたとする。使用権利が一杯のときの秘密値が A、その後、ソフトウェアを使用して権利残高が減少したときの秘密値が B であったとする。ユーザが残高を増やそうとして、使用権利データファイルを上書きすると、ファイルの秘密値は A に変わってしまう。一方 CMP が保管する秘密値は B であるため、ソフトウェアはこの両者の値が一致しないことからファイルの改ざんが行われたことを知ることができる。

使用権利データファイルの残高が 0 になった場合は、6.3 の手続きと同様に権利データの補充を行う。このとき、管理センタに送付した使用権利データファイルにユーザの使用記録が保管されているため、管理センタは使用記録を回収できる。

7. 超流通システムの意義

単に従量制の課金を行うだけであれば、文献[5]に示されるように、ソフトウェア供給者とユーザの間だけでも運用は可能で、超流通のような大規模なシステムは不要に感じられるかも知れない。しかし、各ソフトウェア供給者が別々の方法で課金処理を構築すると、ユーザは、異なった種類の課金処理システムをインストールし、別々に決済しなければならないという不便が生じる。また、似たような課金処理システムをいくつも開発することは、社会全体としてみたときに無駄が多い。

超流通システムを導入する意義は、課金システムを統一する事によって、登録や決済にかかるユーザの手間を最小限にし、かつ課金処理システムに関するソフトウェア開発者の負担を軽減できることであろう。また、システムが統一される事で各ソフトウェアの互換性が高くなり、超流通ソフトウェアの開発効率と品質の向上が期待できる。

8. むすび

本稿では CMP を利用することによって、利便性と安全性を向上させた超流通システムについて述べた。

CMP は、超流通システム、超流通ソフトウェアのいずれも暗号化した状態で実行できるため、ソフトウェアの内容を攻撃者が解読することは困難で、高い安全性を実現できる。

ソフトウェアによって構築するシステムであるため、専用ハードウェアの SUM を使用する従来のシステムに比べると、バージョンアップなどにかかる手間は格段に小さくでき、システムのメンテナンスが容易になる。

復号鍵は、超流通ソフトウェアごとに自由に設定できるので、あるソフトウェアの復号鍵が何らかの手段で攻撃者に知られたとしても、シ

ステム全体にその影響が及ぶことはない。

仮に超流通システムソフトウェアの復号鍵が知られたとしても、バージョンアップなどの際に鍵を変更することで、被害の拡大を食い止めることができる。

現時点で考えられる問題としては、次のようなものが挙げられる。

- ハードディスクのクラッシュなどによって使用権利データファイルを紛失したときの対応。
- 1 ユーザが複数のコンピュータを所有する場合、別々に Permit Code を入手しなければならない。
- 使用権利データファイルが特定のコンピュータ専用になってしまう。

これらは今後改善していく事が望まれる。

参考文献

(1) 森 亮一, 河原 正治:"歴史的必然としての超流通", 情報処理学会 超編集・超流通・超管理のアーキテクチャ シンポジウム論文集, Vol.94, No.1, pp.67-76(1994-02).

(2) 森 亮一:"超流通の構造、防御、人々の利益--定義と基本式--", 信学技報, ISEC94-13 (1994-09).

(3) 河原 正治:"超流通における電子オブジェクト課金方式の検討", 信学技報, ISEC94-15(1994-09).

(4) 鳥居 直哉, 木島 裕二, 勝山 恒男, 小森 宰次:"超流通のためのシステムアーキテクチャ", 信学技報, ISEC94-21(1994-09).

(5) 末松 俊成, 今井 秀樹:"CMP(Crypto Microprocessor)の一構成方法とその応用例", ISEC98-8(1998-05).

(6) Robert M.Best:"Crypto Microprocessor for Executing Enciphered Programs", United States patent, 4278837(1981-07).

(7) Robert M.Best:"Crypto Microprocessor That Executes Enciphered Programs", United States patent, 4465901(1984-08).

(8) 末松 俊成, 今井 秀樹:"超流通ラベルリーダを使用しない超流通システムの一構成法", SCIS96 講演論文集, SCIS96-14B(1996-01).

(9) 末松 俊成, 今井 秀樹:"超流通ラベル配布型超流通システム", 第 19 回情報理論とその応用シンポジウム予稿集別刷, pp.301-304 (1996-12).