マルチメディア通信と分散処理　97－22
コンピュータセキュリティ　8－22
（2000．3．22）

MCMPを利用したデータ保護方式に関する一考察

末松 俊成
ソニー株式会社 大崎東 TEC
〒141-0032 東京都品川区大崎 1-11-1
TEL:03-5435-3156
E-mail:suematsu@strg.sony.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 現在のコンピュータ／ネットワーク社会において、ソフトウェア（プログラムやディジタルデータなど）の違法コピーや不正使用を防ぎ、著作者の権利を保護することには困難な問題が多く残されている。このような現状を改善するには Multipurpose Crypto Microprocessor（MCMP）が有効である。MCMP は、内部に暗号化／復号機能を内蔵したマイクロプロセッサであり、ソフトウェアを安全に実行することができる。本稿では、コンピュータシステムにおけるデータ保護について考察し、データ保護システムの一例として MCMP を利用した音楽データ保護方式（配信システム）を示す。

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

A Consideration on Data Security Based on MCMP

Toshinari SUEMATSU
Sony Corp. Osaki East Tec.
1-11-1 Osaki Shinagawa-ku, Tokyo, 141-0032
TEL:03-5435-3156
E-mail: suematsu@strg.sony.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 current computer/network environment, it is very difficult to defend software (programs and digital data, etc.) against infringement or illegal copy for the protection of developer's copyrights. Multipurpose Crypto Microprocessor(MCMP) is an effective solution for this purpose. The MCMP is a microprocessor which contains encryption/decryption units in it. Therefore it can execute software securely. In this paper, we consider data security on a computer system. Then we present a secure music data distribution system which makes use of MCMP.

Key words MCMP, CMP, Microprocessor, Copyright protection, Software distribution, Information security

1. まえがき

コンピュータ上で使用されるソフトウェア（プログラムやデータなどの総称）を、改ざん、違法コピーなどの不正使用から防ぐことはコンピュータ社会における重要な課題である。

近年コンピュータやネットワーク上の犯罪が増えてきており、その対応が望まれている。このような背景の中、コンピュータ用のソフトウェアに対して電子認証や暗号化技術が採用されるなど、ソフトウェア保護の必要性の認識と実用化が進みつつあるが、いまだに大部分のソフ

トウェアは無防備な形で流通している。

ソフトウェア保護に有効な一手段としてMCMP (Multipurpose Crypto Microprocessor)が知られている[1]。これは、文献[1]では CMPと呼ばれていたが、それ以前に提案されていた専用の組み込みプログラムだけを実行できる簡単な構成の CMP[2,3]と区別するため、本稿ではMCMP と呼ぶことにする。

MCMP は暗号化されたソフトウェアをチップ内部で復号しながら処理することが可能なもので、コンピュータ上で実行するプログラムを不正使用などから保護するのに適している。本稿では、ソフトウェア保護に関する現状の問題点について触れ、ソフトウェア保護の強化が必要であることを示す。次に MCMP を利用した音楽データの保護方式（配信システム）の構成例を示し、その安全性について検討する。

2. ソフトウェア保護の現状

近年 MP3 という音楽データ圧縮形式で音楽が不正に配布されていることが社会的な問題としてとりあげられている。現在のコンピュータ社会では、このような不正を物理的な機構によって防ぐことはあまり行われておらず、ユーザの倫理観に訴えるか、法律によって取り締まることで抑止するのみであった。

ここで、次のような例について考えてみる。ある個人（または団体・法人など）が所有する土地が、多くの人が往来する場所のそばにあると仮定する。

① この土地には不正侵入を防ぐ処置が全く施されておらず、何の抵抗も無く入れるような状況になっており、ここが個人の所有物であることが一目ではわかりにくいとする。他人の土地に無断で入ってはいけないことは、ほとんどの人が知っているはずであるが、実際には、他人の土地であることに気づかずに入ったり、知っていても罪悪感を感じないために入ってしまう人が多いであろう。このような人々に対して法的な処罰を加えることには問題が多いと考えられる。

② 土地の周囲に柵を作り、無断侵入禁止を訴える看板を見やすい場所に立てるなどして、無断で入ってはいけないことが誰にでも簡単に分かるようにする。このような対策を施すことで不正侵入を抑止できる。中には柵を乗り越えたり壊したりして中に侵入する者が現れるかも知れないが、この場合は不正行為であることが誰の目にも明らかであるため、法的な処罰を加えることが可能である。

③ さらに強固な方法として、非常に高くて丈夫な壁を作る、鉄条網や高圧線を張り巡らせる、柵の周囲にセンサーを取り付けて不正侵入を検出する、などが考えられる。手段を決定する場合には、コストと得られる効果のバランスを良く考える必要がある。また、このような手段を強化しすぎると、この土地に入る必要のある人々にとっては不便を強いられることになるので注意が必要である。

最近はコンピュータやネットワーク上のセキュリティに関する意識も高まってきており、コンピュータ用のソフトウェアに対して電子認証や暗号化技術が採用されるなど、ソフトウェア保護の実用化が進みつつあるものの、ほとんどのソフトウェアは無防備に流通しているのが現状である。誰でも手軽にコピーできる環境が整っている状況でありながら、不正使用の禁止を訴えている現状は前記①のケースに近いと考えることができよう。このため、ソフトウェアが保護されていることをユーザが一目で理解できるような環境を整えることが先決である。その上で初めて倫理や法律が有効に機能すると考えられる。具体的には、次のような手法が考えられる。

a) 自由にコピーして良いものと、コピーが制限されるものの区別が簡単にできるようにする。
b) 不正使用を防ぐ機構を用意する。

上記 a)の対策は前記例の②にあたり、b)の対策は前記例の③に相当すると考えられる。a)の具体例としては、電子透かし技術を利用した著作権情報の表示、ソフトウェアの暗号化が挙げられよう。前者は著作権の表示、後者は暗号化されていることで、ユーザに不正使用が許されないソフトウェアであることを認識させることができる。電子透かし技術は b)の機能は持たないが、暗号化は b)の機能を併せ持つ。

表 1 外部攻撃と内部攻撃の比較

	外部攻撃	内部攻撃
攻撃	第三者	ユーザ自身
防御	ユーザ、コンピュータ、ソフトウェア	コンピュータ、ソフトウェア
攻撃対象	ユーザが所有するソフトウェア、通信内容など	他者が権利を有するソフトウェアなど

3.外部攻撃と内部攻撃

コンピュータ上のソフトウェアに対する攻撃の形態は、コンピュータの外部から行われる外部攻撃とコンピュータの内部から行われる内部攻撃に分類することができる。ここでは、これらについて考察する。

3.1.外部攻撃

外部攻撃とは、攻撃の対象となるコンピュータを直接操作しない第三者が、ネットワークなどを通して攻撃を加えるものである。例としては、電子メールなど他人が送受信するデータを盗み見または改ざんすることや、ネットワークを通して他人のコンピュータに侵入し、ソフトウェアの改ざん、データの盗み見、不正コピーを行うことなどが挙げられる。外部攻撃においては、ユーザのプライバシーが侵害されたり、各個人のソフトウェアが第三者の攻撃によって損害を被る。これを防ぐため、コンピュータとそのユーザが一体となって外部からの攻撃に対抗する。一例として、暗号化プログラムによってネットワーク上に流すデータを暗号化するなどの対策が挙げられる。このケースでは、暗号化はユーザの手によって行われるため、そのプロセスを外部の攻撃者によって解析される可能性は低く、プログラムによる暗号処理を行っても問題は少ない。

3.2.内部攻撃

これに対し、コンピュータを直接操作するユーザ自身が攻撃者となって自分の所有するコンピュータ内のソフトウェアを攻撃する内部攻撃という形態が考えられる。例としては、ソフトウェアの違法コピーや有料ソフトウェアを無料で使用できるように改ざんすることなどがあげられる。この攻撃の防御は、外部攻撃の場合に比べ非常に困難である。なぜなら、暗号化によってデータを保護しようとしても、その処理を行うプログラムは攻撃者であるユーザの手元で実行される。現状のコンピュータにおいては、攻撃者であるユーザがコンピュータと暗号に関する専門知識を持ち、さらにデバッガなどのプログラム解析ツールを使いこなす能力の持ち主であった場合、プログラムを使用した暗号処理によって秘密を守り通すことは基本的には不可能と言える。暗号化や復号などのプロセスを解析され、秘密鍵や復号データなどの重要なデータを盗み出される危険が高い。表 1 に外部攻撃と内部攻撃の比較を示す。

先に挙げた MP3 の問題は、コンピュータを使用するユーザが、CD などの音楽データを MP3 に変換し、それを第三者に譲渡したり、ホームページにアップロードしたりするものである。このとき音楽データの変換はユーザの手元で行われるため、これは内部攻撃である。このように現在流通しているソフトウェアは、内部攻撃に対しては無防備のものが多いと言えよう。

外部攻撃は、第三者からの攻撃によって個人のプライバシーが侵害されるなどの被害を受けるものであるため、一般的な関心も高い。一方、内部攻撃はユーザ自身が行い、ユーザの利益につながるものであり、被害を受けるのはソフトウェア製作・販売者という一般ユーザにとっては身近ではない団体または個人であるため人々の関心は薄い。しかし著作権保護の観点からすると内部攻撃を防ぐことは非常に重要である。

4.MCMP の概要

内部攻撃からソフトウェアを保護するのに有

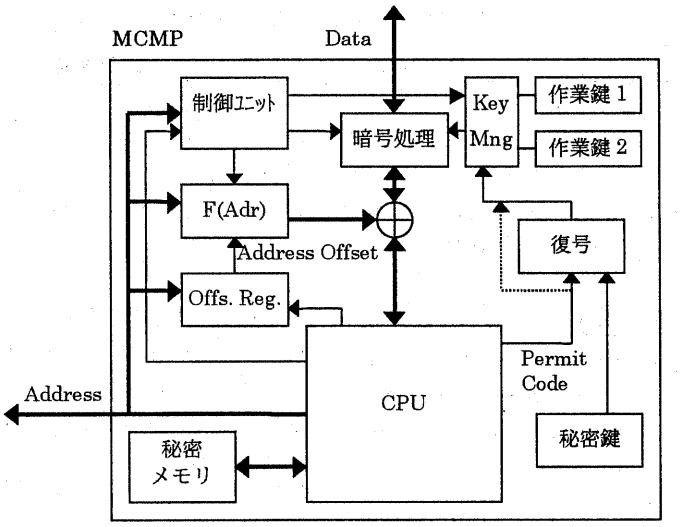

図1 MCMP 構成例

効なのが MCMP である[1]。

図1は代表的な MCMP の構成例である。CPU と同じ機能に加え、入出力するデータを暗号化／復号する暗号処理ユニット、暗号処理ユニット用の作業鍵、データを暗号化する前（または復号の後）にメモリ上のデータのアドレスに応じてスクランブルをかけるデータスクランブラ（F(Adr)）、アドレスに関連する処理をリロケータブルにするためのオフセットレジスタ（Offs.Reg.）、暗号処理やスクランブル処理をコントロールする制御ユニット、アプリケーションが秘密のデータを隠すことができる秘密メモリ、作業鍵を外部から安全に取り込むための階層鍵方式を実現する秘密鍵と暗号処理機構などを有する。

MCMP の外部においては、ソフトウェアを暗号化された状態でしか見ることができず、プログラム解析ツールを使用したとしても復号鍵を知らないとその処理内容を理解することはできないため、内部攻撃を防ぐのに有効である。

5. 音楽データの保護システム

MCMP によってソフトウェアの保護を実現するには、MCMP を内蔵するコンピュータを開発し普及させなければならない。しかし現在数多く流通している主要な CPU に置きかえられる MCMP を開発し、それを搭載するコンピュータを普及させることは、そう簡単なことではない。MCMP の普及を促すためには、より簡便に導入できる方法を考える必要がある。ここでは、従来のコンピュータに、MCMP を搭載する拡張ユニットを追加したシステムによって音楽データを保護する方式について考える。

MCMP 拡張ユニットに必要な機能は以下の通りである。

- メイン CPU または周辺機器とデータをやり取りする機能。
- メイン CPU の制御下で MCMP 用の暗号化プログラムをダウンロードし実行する機能。

上記の条件が満たされるものであれば、拡張ユニットをコンピュータに接続する手段は何でも良い。例としては、コンピュータの汎用拡張スロット、PC カードスロット、SCSI などの汎用インタフェースなどが考えられる。以降では拡張スロットに増設する MCMP 拡張ユニットについて話を進めることにする。

ユーザは MCMP 拡張ユニットを組み込んだコンピュータを所有しており、その MCMP のシリアル番号を i とする。この MCMP は秘密鍵 K_{CSi}

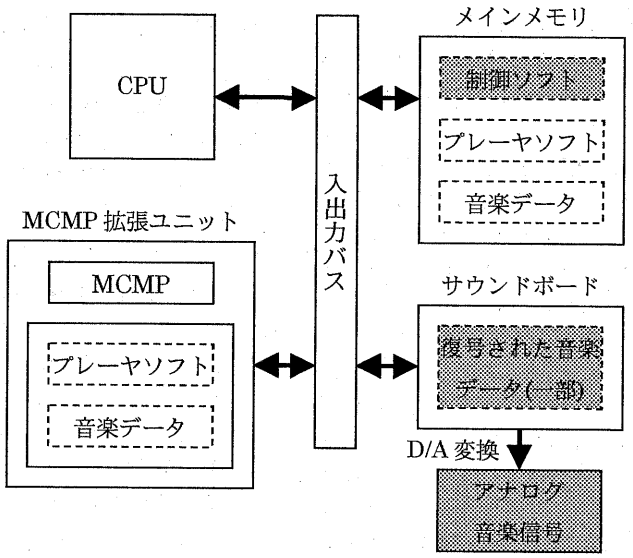

図 2 暗号化音楽プレーヤ

を内蔵しており、これと対になる公開鍵 K_{CPi} が存在する。個々の MCMP に組み込まれる秘密鍵は MCMP メーカーが管理するもので、ユーザはもとより他の誰も知ることができない。これに対し公開鍵は、MCMP のシリアル番号さえ知っていれば誰でも入手することができるものとする。音楽データを演奏するプレーヤソフトウェアは固有の鍵 K_{PS} で暗号化されて配布される。ユーザは所有する MCMP の公開鍵 K_{CPi} を開発元に渡す。開発元はこれで K_{PS} を暗号化して P_{PSi} を作成しユーザに送付する。この作業鍵 K_{PS} を暗号化した P_{PSi} を Permit Code と呼ぶことにする。

$$P_{PSi} = E_{CPi}(K_{PS})$$

ここで $E_{XY}(D)$とは、鍵 K_{XY} でデータ D を暗号化することを示すものとする。ユーザは P_{PSi} を MCMP に取り込ませることで、このプレーヤソフトを実行できる。P_{PSi} の添字 i はこの Permit Code が MCMP-i に対してのみ有効であることを示している。

ユーザは次に希望する音楽データを音楽データ配信センタなどから入手する。このとき音楽データは、それぞれ固有の秘密鍵 K_{Mn} で暗号化されている。K_{Mn} は個々の音楽データごとに異なり、n が音楽を特定する番号を表すものとする。ユーザは、暗号化された音楽データとそれを使用するための Permit Code である P_{Mni} を入手する。

$$P_{Mni} = E_{CPi}(K_{Mn})$$

P_{Mni} の添字 n と i は、この Permit Code が音楽データ n と、MCMP-i の組み合わせに対してのみ有効であることを示している。

さらに、これらの暗号化ソフトウェアを MCMP 拡張ボードに転送したり、実行を制御するための制御ソフトが必要である。この制御ソフトは CPU の下で動作する暗号化されない通常のプログラムである。以上のソフトウェアによって次の手順によって音楽を再生する。

まず CPU は制御ソフトによってプレーヤソフトと P_{PSi} を MCMP 拡張ボードに転送し、プレーヤソフトを起動する。次にプレーヤソフトが演奏する音楽データを要求し、CPU は制御ソフトによって音楽データ n と P_{Mni} を MCMP 拡張ボードに転送する。プレーヤソフトは、MCMP 内部で自身の復号鍵 K_{PS} と音楽データの復号鍵 K_{Mn} を適宜切り替えながら音楽を再生し、コンピュータの入出力バスを介してサウンドボードに音楽情報を送信する。サウンドボードは、それ

を D/A 変換してアナログの音声信号として出力する。本方式の構成を図 2 に示す。図 2 のうち背景色の付いた部分は暗号化されていないソフトウェアを示している。

この例のように 2 種類の鍵を高速に切り替えて使い分けるためには、図 1 に示したように作業鍵を MCMP の中に複数保管できるようになっていると良い。鍵の管理は、図 1 中の鍵管理ユニット（Key Mng）が行う。

図 2 に示すように、保護しなければならないプレーヤソフトと音楽データは、暗号化された状態のまま MCMP 拡張ユニットに転送され、MCMP 内部で復号されながら処理される。制御ソフトは暗号化ソフトウェアを MCMP 拡張ユニットに転送したり、実行を開始するだけのものであるため保護の必要は無い。音を出すためにはサウンドボードに復号したデータを渡す必要があるため、MCMP 拡張ユニットからサウンドボードに必要最小限の数のデータをリアルタイムで供給する。

本方式において、プレーヤソフト、音楽データは共に暗号化によって保護されており、それぞれ対応する Permit Code を持つ正規ユーザ以外は使用できない。これらの暗号化されているソフトウェアのコピーは自由に行うことが許され、ユーザ間で音楽データやプレーヤソフトを受け渡ししても構わない。たとえば音楽データを保管していたハードディスクが壊れたような場合に、その音楽データのコピーを知人からもらうことが合法的に行える。プレーヤソフトや音楽データは基本的には無料で良いが、流通経路によっては媒体の代金や必要最小限の手数料などの支払いが必要な場合もあり得る。

これに対して Permit Code の入手は通常有料となる。これを紛失した場合は、Permit Code を再発行してもらう必要がある。MCMP のシリアル番号とソフトウェアの種類から、一度発行した Permit Code であることがわかれば、再発行は可能であろう。

本方式は、ソフトウェアを入手するためではなく、使用するために対価を支払うという意味で、超流通[4-6]の一つの形態と言えよう。

次に本方式の安全性について検討する。本方式への攻撃としては、次のものが考えられる。

① K_{PS}、K_{Mn} を解読する。
② K_{CSi} を解読する。
③ 入出力バスに流れるデータを何らかの方法で取りこみ、復号された音楽データを再構築する。
④ アナログで出力された音楽信号を録音する。

上記①の攻撃に対する強さは、MCMP の耐タンパ性、プレーヤソフトならびに音楽データの暗号化方式などに依存するが、暗号に関する専門知識を持たない普通のハッカーなどに対しては十分安全であろう。②の攻撃に対する強さは MCMP の耐タンパ性、MCMP が採用する公開鍵方式に依存する。一般に、これは①よりも安全と考えられる。暗号に関する知識の無い攻撃者が選ぶ手段としては③と④が考えられるが、③のように入出力バス上のデータを取りこむためには、専用のハードウェアかソフトウェアツールが必要と考えられ、手間と費用がかかる。④の方法は録音機を持つユーザであれば可能である。このように人間が知覚できるアナログの形になってしまったデータのコピーを防ぐことは困難である。しかし、一旦アナログに変換したものであるため、データの品質は劣化する。

前記③の攻撃を防ぐには、入出力バスを通るデータを暗号化する必要がある。このためには、サウンドボードの中に暗号を復号する機能を持たせなければならない。さらに言うとサウンドボード上においても D/A 変換器の前で復号データを捕捉される可能性があるので、これも防ごうとすると、D/A コンバータに暗号の復号機能を組み込む必要がある。このコストはサウンドボードを購入するユーザが負担することになろうが、ユーザにとってメリットが無いため、どのようにして普及させるかが問題である。③の攻撃を行うようなユーザは限られると考えられるので、コストに対する効果の観点からも有効な対策とは言いにくい。③の攻撃で最も問題なのは、入出力バスを通る音楽信号を捕捉し、暗号化されない別の形式のファイルに変換するようなツールを作成されて流布されることである。このような違法コピーを助長する行為に対して

は、法的手段などにより厳しく取り締まることで抑止するのが現実的と考えられる。

ところで、本方式によって配布される音楽データは保護されるが、同じ音楽が既存のCD（コンパクト・ディスク）などのデータ保護機構の無い流通形式で配布されていると、このデータからMP3などの形式に変換されてしまい、簡単に不正コピーが作成されてしまう。このように他の流通媒体から簡単に攻撃が可能であると、本方式の意味は希薄になってしまう。したがって、不正使用を防ぐには、暗号化された形でのみディジタル音楽データを流通させる必要がある。

6. むすび

本稿では、コンピュータを操作するユーザ自身が攻撃者となる内部攻撃を防ぐことは現在のコンピュータの構成では困難であること、この問題の解決にはMCMPが有効であることを示した。次にMCMPによるデータ保護の一例として、音楽データ保護システムを示した。本方式の特徴は次の通りである。

- 従来のコンピュータにMCMPを搭載した拡張ユニットを追加することでデータ保護システムを実現する。MCMP対応のコンピュータを普及させるよりも導入が簡単である。
- メインCPUは暗号化されたソフトウェアをMCMP拡張ユニットに転送し、セキュリティを必要とする処理をこの拡張ユニットに任せる。MCMP拡張ユニット内では暗号化されたままの状態でソフトウェアが処理される。
- 暗号化された音楽データは、基本的に無料で自由に配布することができる。また、この音楽データは誰でも自由にコピーを取ることが許される。
- 利用者はソフトウェアを自身のMCMPで使用するためのPermit Codeを入手することによって音楽を聞くことができるようになる。これにより音楽データの使用を正規ユーザに限定できる。

これらの特徴から、本方式はネットワーク上などで音楽データを配信するのに適している方式と言えよう。

本稿では、最も防御が困難と考えられる内部攻撃を防ぐという観点からMCMPの有効性について説明してきたが、当然ソフトウェアのセキュリティに関わる他の用途にも有効である。MCMPは暗号化／復号の機能を内蔵しているため、暗号化／復号処理をソフトウェアで行うよりも安全かつ高速に行うことができる。

最後に、本方式の攻撃方法について触れた。しかし、最大の問題は同じ音楽データが、CDなどの既存の流通媒体で暗号化されない形で流通することであろう。ソフトウェアの著作権保護を強化するためには、保護されない形でのデータの流通を許さないような社会基盤の整備が必要になると考えられる。

注）本研究は、ソニー(株)が実用化しているメモリースティック用の著作権保護方式であるMagicGate,OpenMGとは関係ありません。

参考文献

(1) 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).

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

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

(4) 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).

(5) 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).

(6) 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).