MCMPを利用したコンピュータウィルス対策

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:03-5435-3138
E-mail:suematsu@strg.sony.co.jp

今井 秀樹
東京大学 生産技術研究所
〒153-8505 東京都目黒区駒場 4-6-1
TEL:03-5452-6230
E-mail:imai@iis.u-tokyo.ac.jp

あらまし 近年のインターネットの急激な拡大・普及に伴い，多くの人々が電子メール，WWW(world wide web)，電子商取引などのサービスを利用するようになった．その一方で，コンピュータウィルスや不正アクセスなどのインターネット上の犯罪も増えてきている．インターネットやコンピュータのセキュリティを考える上で，コンピュータウィルス対策は非常に重要な課題の一つであるが，現在のコンピュータ環境においては，いまだに抜本的な対策が見出されていない．本稿ではMCMP(Multipurpose Crypto Microprocessor)を利用したコンピュータウィルス対策方法について述べる．

キーワード MCMP，CMP，マイクロプロセッサ，コンピュータウィルス，ウィルス対策，ネットワークセキュリティ

Anti-virus Measures Based on MCMP

Toshinari SUEMATSU
Sony Corp. Osaki East Tec.
1-11-1, Osaki Shinagawa-ku, Tokyo,
141-0032, Japan
TEL:03-5435-3138
E-mail: suematsu@strg.sony.co.jp

Hideki IMAI
University of Tokyo
4-6-1, Komaba, Meguro-ku, Tokyo,
153-8505, Japan
TEL:03-5452-6230
E-mail:imai@iis.u-tokyo.ac.jp

Abstract Use of the Internet has spread rapidly in recent years, and a significant number of people use e-mail(electronic mail), www(world wide web), e-commerce(electronic commerce) etc.. On the other hand, malicious crimes on the Internet such as computer virus, unauthorized access, and so on have been increasing. It is one of the most important matter for internet and computer security to defend a computer from computer viruses, but there is no fundamental measures for computer viruses in the current computer environment. In this paper, we present anti-virus measures based on the MCMP (Multipurpose Crypto Microprocessor).

Key words MCMP, CMP, Microprocessor, Computer virus, Anti-virus, Network security

1. まえがき

近年のインターネットの急激な拡大・普及に伴い，あらゆる情報の入手や電子商取引などがインターネットを利用して行われるようになってきており，インターネットはさまざまなコミュニケーションの手段として，欠く事のできないものとなっている．この利便性の拡大の反面，ネットワークにおけるデータの盗み見，不正アクセス，コンピュータウィルスの流布などの不正行為による脅威が大きな問題になってきた．

これに対し，インターネットのセキュリティ向上のため暗号技術を導入したり，不正アクセス行為の禁止等に関する法律が施行されるなど，各種の対応が検討されているものの，いまだに多くの問題を抱えている．中でもコンピュータウィルスに対しては，抜本的な対策が見出されていないのが実情である．

本稿ではまずコンピュータウィルスに関する現状の問題点について述べ，次に暗号化機能を持ったマイクロプロセッサであるMCMP[3,4]を用いることによってコンピュータウィルスを防ぐ方法について考察する．

2. コンピュータウィルス

2.1.コンピュータウィルスの定義

通産省（現 経済産業省）の「コンピュータウィルス対策基準」によると[1,2]，コンピュータウィルス（以降単にウィルスと記す）とは，第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムで次に示す機能のうち一つ以上を有するものとされている．

(1) 自己伝染機能
(2) 潜伏機能
(3) 発病機能

ウィルスは，以前はフロッピーディスクなどの記憶媒体を介して感染するものが多かったが，インターネットが発達した現在では，電子メールやネットワークを通じて感染することが多い．ウィルスに感染した場合の症状は千差万別であるが，代表的な例として，次のようなものが挙げられる[2]．

- 音楽を演奏したり，異常なメッセージを表示する．
- 画面表示が崩れる．
- システムが立ち上がらない，または立ち上げに異常に時間がかかる．
- システムがハングする．
- ファイルの削除，破壊．
- ディスクの破壊．

一般にウィルスは，ファイルを書換えることで感染するため，システム内の全てのファイルサイズやファイル作成日をチェックすることで，感染を検出できる場合もある．しかし，ファイルサイズや作成日をごまかすことも可能なため，この方法によるチェックでは不充分である．現在の代表的なウィルス対策は以下の通りである[1,2]．

- ワクチンソフトウェアを使用して検出・駆除を行う．
- 電子メールに添付されているファイルや外部から持ちこまれたフロッピーディスク等の取扱に注意する
- ウィルスの兆候と思われる症状が見られたら，すぐにウィルス検査を行う．

ワクチンソフトウェアは，あらかじめデータベース（ウィルス定義）に登録されているウィルスのパターンを使用してウィルスを検出･駆除するもので，基本的には既知のウィルスに対して効果のあるものである．中には未知のウィルスの検出機能を持つワクチンソフトウェアもあるが，新種のウィルスに対しての効果は限られており，完全に防ぐことは難しい．このため，現状ではワクチンソフトウェアを導入し，常に最新のワクチンソフトウェアと定義ファイルを入手し続けるように留意すると共に，ウィルスの侵入経路となるフロッピーディスクや電子メールの添付ファイルなどの取り扱いに注意を払う必要がある．

ローカルなネットワークを保護するための方法としてファイアウォールが知られているが，この方法は自組織内部のネットワークに不正にアクセスされることは防げるものの，インターネット上をデータとして伝送されるウィルスの侵入を防ぐことはできない．

以上のように現状ではコンピュータウィルスへの抜本的な対策は無く，感染の可能性を低くするための予防処置や，感染後の対処などに留まっている．

2.2.ウィルスの種類

コンピュータウィルスはプログラムの一種であり，コンピュータが理解し処理できる命令語で作成されている．プログラム構造の観点からウィルスを見た場合，次の 3 種類に大別できる．

- 機械語ウィルス
  コンピュータの CPU が直接処理できる機械語で作成されたプログラム
- マクロウィルス
  ワードプロセッサなどの特定のアプリケーションプログラム（以降アプリケーションと記す）が処理できるマクロ言語で書かれたプログラムで，アプリケーションの文書ファイルなどに寄生する
- 中間言語ウィルス
  Java，ActiveX などの中間言語で書かれたプログラム

機械語ウィルスは，その機械語を処理できる特定の CPU 上でしか実行することができない．例えば，Windows[1]を OS とするコンピュータ用 CPU と，Macintosh[2]とは CPU の機械語の互換性が無いため，一方の CPU 用の機械語ウ

[1] Windows は Microsoft Corporation の登録商標です．
[2] Macintosh はアップルコンピュータ社の登録商標です．

ィルスは他方のシステムには感染しない. また, ファイルへのアクセスなどは OS に依存した処理になるため, CPU が同じであっても OS が異なるとウィルスは正しく動作しないことが多い.

これに対し, マクロウィルスはアプリケーション等が仲介してマクロを実行するため, 機械語レベルでの互換性は必要とせず, 同じマクロをサポートするシステムであれば, CPU や OS が異なっていてもマクロウィルスを実行することができる. マクロは特定のアプリケーション上でしか実行することはできないという制限があるものの, 世界中に普及しているメールソフトやワードプロセッサなどのマクロで書かれたウィルスは, OS や CPU を選ばずに動作し, 感染の範囲も広いので脅威である. また, 一般にマクロによるプログラムの作成は, 機械語に比べて容易であるため, ウィルスを作成するためのしきいが低いこともウィルスが発生しやすい要因となる.

さらに Java や ActiveX などの中間言語で書かれたウィルスも存在する. この中間言語は CPU や OS に依存せず, これらをサポートする仮想マシンを持つ全ての PC 上で動作する. インターネットに接続してホームページなどを閲覧する機能を持つコンピュータは全てこの種のウィルスに感染する可能性があるため脅威である.

以上に示したようにウィルスが感染するためには, 共通のプラットホームが必要である. 現在のコンピュータ社会は, 利便性とコストを優先して発展してきた結果, 限られた CPU, OS, アプリケーションが世界的に普及している. このように利用環境がある程度統一されることは互換性や利便性などの面では当然望ましいことであるが, 反面ウィルスの増殖しやすい環境を与えることにもつながる.

3. MCMP によるウィルス対策

ウィルスの感染を防ぐには, ウィルスを記述したプログラムをコンピュータが実行しないように制限することが必要である. この目的の為に, 暗号化機能を持った CPU である MCMP[3,4]を利用することを考える. MCMP は内部に暗号処理機能を持ち, 暗号化されたソフトウェアを指定された復号鍵によって復号しながら実行する機能を持つ. このときソフトウェアは実行に先立ちメモリ上で復号されることはなく, 暗号化されたままの状態で MCMP 内部に取りこまれ, 内部で復号されて実行されるので, ハッカーなどに復号されたプログラムを盗み見られる心配が無い. MCMP 上では暗号化の有無や鍵を変える事で, プログラムを理解できない状況を作り出すことができるので, このことを利用してコンピュータウィルスを防ぐ方法について考察する.

3.1. 機械語ウィルス対策

対象とするコンピュータには MCMP が内蔵されており, プログラムやデータを暗号化したまま実行できる環境が整っているとする. またこの MCMP は, 暗号化しないプログラムを実行する機能, 個々のプログラムやデータごとに復号鍵を変える機能を持っているものとする[3,4]. ここでウィルス対策のために次のようにコンピュータの利用環境を設定する.

(1) まず, 暗号化しない状態で OS や各種のアプリケーションをインストールする.
(2) そのコンピュータ上のプログラムを暗号化するための鍵を決定する.
(3) OS を含む全てのプログラムを, 選んだ鍵で暗号化する.
(4) MCMP に対し, プログラムを実行する際にプログラムが暗号化されているかどうかに関らず, 常時同じ復号鍵を使用するように設定する.

この例では, MCMP は入力されたプログラムを, それが暗号化されているか否かや鍵の種類を確認せずに盲目的に決められた鍵で復号しながら実行しようとするので, 同じ暗号化方式でかつ同じ鍵で暗号化されたプログラムしか正しく実行できない. ここに暗号化されないプログラム（ウィルス）が入ってきたとすると, そのプログラムは MCMP 内部で全く別のでたらめなデータに変換されてしまい実行することができない. 現在流通しているウィルスは暗号化されないプログラムであるため, この方法によって防ぐことが可能である.

例えば電子メール等に添付された実行形式ファイルのウィルスを, ユーザが誤って実行しようとしても MCMP がそれをプログラムとして実行できないため安全である. 仮にウィルスを暗号化して流布させたとしても, 復号鍵が偶然一致しない限り実行できない. 鍵を適切に選んでおけば, 偶然一致する確率は限りなく 0 に近くできる.

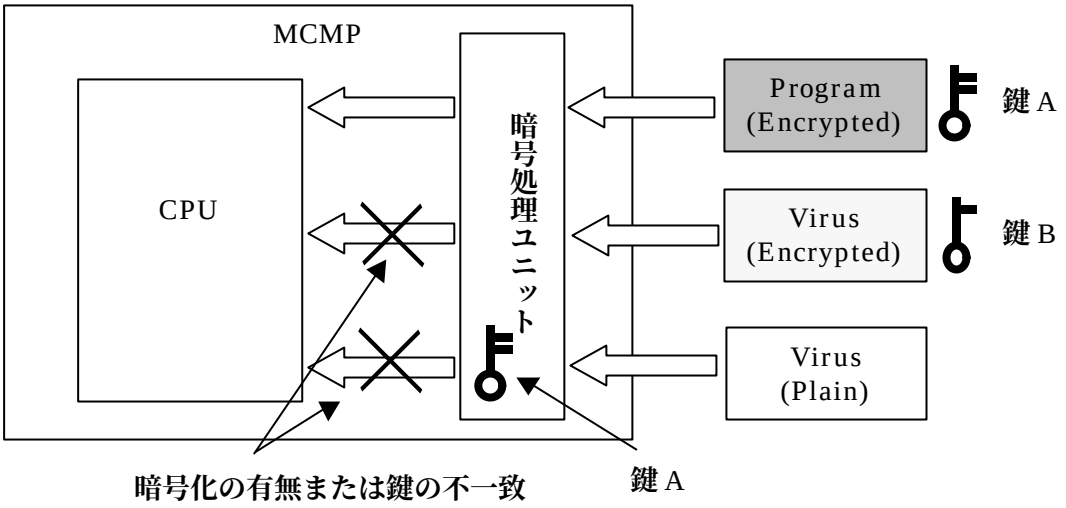

図 1 MCMP による機械語ウィルス防御

例えば図 1 において，MCMP は復号鍵 A でプログラムを復号して実行するが，復号鍵 B の暗号化ウィルスや, 暗号化されていないウィルスはこの MCMP では実行されず，感染もしない.

以上の説明ではコンピュータ上の全てのプログラムを同一の鍵で暗号化するとしたが, 個々のプログラムごとに鍵を変えても良い.

この方法により, 機械語ウィルスをほぼ完全に防ぐことができる．ただし，外部から受け取ったプログラムをユーザが不注意に自身のコンピュータ用の鍵で暗号化して実行し, それがウィルスだった場合には感染することになるので注意が必要である.

以上では元々暗号化されていないプログラムをユーザが暗号化するという前提で話を進めてきたが，MCMP が普及したとすれば，当然あらかじめ暗号化されたプログラムが流通することになると思われる[3,4]．これらの暗号化プログラムについては, 新たに別の暗号化を施す必要はなく, そのまま実行すれば良い. このケースにおいて, ある暗号化プログラムが全てのユーザに対して共通の鍵を使用していたと仮定すると，攻撃者がその鍵を見つけ，それで暗号化したウィルスを作成すれば, そのプログラムには感染することになる. したがって暗号化プログラムを配布する場合には, 地域, 時期, ユーザなどの違いに応じて鍵を換えておくことが望ましい．こうしておけば，仮にある鍵が攻撃者に知られたとしても, ウィルスの感染を限られた範囲に限定することができる.

機械語ウィルスは，OS などのシステムの基幹をなす部分, 中間言語を処理する仮想マシン, アプリケーションなどのあらゆるプログラムに感染する可能性があり, それらの動作を全く別のものに変えてしまう能力を持つ. 後述するマクロウィルスや中間言語ウィルスへの対策も, 機械語ウィルスを防ぐことができない環境では, 機械語ウィルスによってセキュリティ機能を無効にされる可能性がある．したがって MCMP によって機械語ウィルスの感染を防ぐことは, コンピュータウィルス対策の基盤となる最も重要な技術である.

3.2.マクロウィルス対策

マクロウィルスはデータに感染するので, マクロウィルスを防ぐには, コンピュータ内のデータ全てを暗号化しておくことが有効である. 簡単な例としては, 機械語ウィルス対策の場合と同様に, コンピュータ内の全てのデータを一つの鍵で暗号化し, それを処理する際にはデータが実際に暗号化されているかどうかに拘わらず, 常にあらかじめ決められた鍵を使って復号しながら処理すれば良い.

なお, データを暗号化する鍵はプログラムを暗号化する鍵と同じでも良いし別でも良い. また，個々のデータごとに鍵を換えても良い.

このとき, 外部から侵入したマクロウィルスを含むデータが暗号化されていないとすると, アプリケーションにとって認識できない無意

味なデータにしか見えず, 開くことができない. マクロウィルス自体も無意味なデータにしか見えないため, 実行されず感染もしない. 現行のコンピュータでは, データをうっかり開いてしまってウィルスに感染するといったトラブルが数多く起こっているが, 本手法においてはこのような不注意による感染は起こらない.

反面, 外部から入ってくるデータは鍵が一致しない限り処理できず, 外部とのデータ交換が自由にできないという問題が生じる. 例えば電子メールのように他のコンピュータと通信する場合, 暗号化されずに外から入ってくるデータを読み取ることができないことになる. 信頼できる相手に対しては暗号化鍵を事前に教えておくことで通信することが可能になろう. しかしこの場合, 鍵を知る相手がウィルスを含むファイルを暗号化して送ってくるとそれは実行可能であるため感染してしまう危険があるので注意が必要である.

ネットワークに対して情報発信することだけを目的としたコンピュータの場合, 外部からのデータを受け入れる必要は無いので, 内部のプログラムとデータを全て暗号化しておき, 外部に発信するデータだけを復号して出すように運用することが可能である. このような用途に限れば, 前記のマクロウィルス対策は有効である.

ところで, 現在のコンピュータでも電子メールの内容を暗号化して送ることが行われているが, これは通信路上での盗み見を防ぐことを目的とするものであり, メールソフトがデータを受信したときに復号するため, データにウィルスが感染していた場合はそれも復号されて実行可能な状態になってしまうため, ウィルスの感染を防ぐことはできない. 本方式とは異なることに注意されたい.

外部と自由にデータのやりとりをしたければ, 暗号化されないデータを受け入れるようにする必要がある. この場合にマクロウィルスの感染を防ぐには, アプリケーションに対してマクロ実行機能を制限する機能を追加することが有効である. 以下にその例を示す.

(1) マクロ実行全てを禁止
(2) ファイルを開いたときなどのマクロ自動実行機能を禁止
(3) 外部の装置に命令を発行したり, ファイルの移動/コピー/削除などのシステムに影響を与える可能性のある処理を禁止

上記(1)を禁止にしておけば, マクロは実行されないので安全であるが, いちいち禁止を解除しなければマクロが使えないのは不便である. (1)は許可しても, (2)と(3)を禁止にしておくことで, 危険なマクロの実行をほぼ抑制できると考えられる.

さらに, マクロ実行の制限を次に示すような条件によって使い分けることが考えられる.

(A) 暗号化されていないデータに対してはマクロ実行を制限し, 暗号化されたデータに対してはマクロ実行を有効にする. 暗号化されたデータに対して鍵の種類に応じて制限の有無を分けることも可能.
(B) マクロ実行の制限を, データファイルごとに選択できる機能を設け, 未知のデータに対してはマクロ実行を制限し, 安全であることが確認されたデータに対してはマクロ機能を有効にする.
(C) リムーバブルディスクのデータや, 電子メールの添付ファイルなどの, ウィルスの感染経路になる可能性の高いものに対してはマクロ実行を制限する.

これら(1)～(3), (A)～(C)の機能をうまく組み合わせて運用することで, ユーザの利便性をほとんど犠牲にせずにウィルスの感染を防ぐことが可能になろう.

3.3.中間言語ウィルス対策

中間言語ウィルス対策は, マクロウィルスのケースに似ている. Java アプレットを含む Web 文書などは不特定多数がアクセスするものであるため, 個々のユーザに合わせて暗号化することは困難であり, かつホームページの作成者が信頼できるとは限らないため, そのデータが暗号化されていても安全とは言えない. このため, MCMP を使って暗号化データだけを処理するという対策は取れない.

ホームページを見るための中間言語プログラムは, あらかじめコンピュータにインストールされているものと, ネットワークを通じて（動的または静的に）配信されるものとがある. あらかじめインストールされているものについてはウィルス検査して安全性を確認した上で暗号化して保護すれば良い. 問題は, ネットワーク上から配信されるものである. これの対策としては, 次のようなものが考えられる.

(1) 中間言語プログラムは, 中間言語を実行する仮想マシンの外側であるユーザのディスクやメモリ, ネットワークなどの情報に

は一切アクセスできない仕様とする.

(2) ネットワークを通して外部から送られてくる中間言語の実行を禁止する機能.

(3) ディジタル署名などによって各 URL (Uniform Resource Locator)の信頼性を確認する手段を設け，信頼できる URL に限り中間言語の配信を許す機能.

(4) ユーザが指定した URL に限り中間言語の配信を許す機能

Java には，すでに(1)の仕様が盛込まれており，Java 仮想マシンにセキュリティホールなどが無いとすれば, 仮にウィルスが侵入しても, ユーザのコンピュータに深刻な影響を及ぼすことは無いと考えられる. さらにセキュリティを高めたい場合は，上記(2)の対策をしておけば, とりあえず外部から危険なプログラムが侵入することは避けられるが, 各コンテンツを十分に楽しむことができない．(2)の対策は採らなくても(3)と(4)の機能をうまく使い分けることができれば, 利便性をあまり損なわずに安全性の向上を図ることができると考えられる.

4. むすび

本稿で述べたウィルス対策についてまとめておく.

- 機械語ウィルス対策としては MCMP を用いて自身のコンピュータにインストールしたプログラムを全て暗号化する.
- マクロウィルス対策としては，マクロ機能の実行を制限する機能を持つアプリケーションだけを使用するようにする.
- 中間言語ウィルス対策としては，中間言語プログラムによってコンピュータに深刻な危害を及ぼされないように設計され，さらに中間言語プログラムの実行を制限できる機能を持った仮想マシンを使用する.

以上のように MCMP を使用するとともに, アプリケーションと仮想マシンを改善することにより, 利便性の犠牲を最小限にしつつウィルスの侵入を防ぐことが可能となる.

ここで重要なのは MCMP を使用しない場合, 機械語プログラムであるアプリケーションと仮想マシンがウィルスに感染することを防げないことである. これらがウィルスに感染するとマクロや中間言語ウィルスへの対策が無効にされてしまい, セキュリティシステムが崩壊する恐れがある．MCMP によって機械語ウィルスの感染を完全に防いでおけばこの心配は無くなり，安全な環境を実現できる．このように MCMP によって機械語ウィルスを防ぐことは, マクロや中間言語ウィルス対策を含めた全てのウィルス対策の基盤となる非常に重要な技術である.

但し，これらの対策を取ったとしても，ユーザが不注意な操作をすればウィルスに感染する可能性は残されるため, 運用にあたっては十分な注意が必要である.

参考文献

(1) “コンピュータウィルス対策基準”,通商産業省告示第 535 号,平 9 年 9 月.

(2) IPA ホームページ http://www.ipa.go.jp/security/index.html

(3) 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).

(4) 末松俊成,今井秀樹:”MCMP を利用したデータ保護方式に関する一考察”,情報処理学会研究報告,2000-DPS-97/2000-CSEC-8,22 (2000-03).