明　細　書

データプロテクト方式

技術分野

本発明はアプリケーションソフトウエア、OS、等のソフトウエアを含むデータ、情報をプロテクトする方式に関する。

背景技術

現在、アプリケーションプログラム、OS用ソフトウエア、ユーティリティプログラム等のデータ或いは情報の無断コピーは、日常的であってしかも無断コピーによる不正使用にたいする防御について充分なものは、未だ提案されるに到っていない。

発明の開示

本発明は上記した従来技術の欠点を解決し、ユーザーは、所定のソフトウエアーを含むデータを適宜にかつ容易に使用しえるとともに、他のユーザーに対しては不正なソフトウエアー等のデータの使用を効率的に防止しうるデータのプロテクト方式を提供することを目的とする。

即ち、本発明に係るデータプロテクト方式は、センタが特別なアルゴリズム、すなわちセンタだけが秘密に保持するセンタアルゴリズムを作成し、センタは、ソフトウエアを含むデータ並びにユーザのそれぞれに用いられる各データ並びにユーザの識別子にセンタアルゴリズムを施して各データ並びにユーザに専用な秘密アルゴリズムを作成し、ユーザにデータを供給するという準備を行った後、データの供給体は、ユーザの識別子と供給対象となるデータの秘密ア

ルゴリズムとにより、供給対象となるデータとユーザとの間で同一の暗号鍵を作成し、この暗号鍵に基づいて直接的又は間接的に供給対象となるデータの一部又は全部を暗号化してユーザへ供給し、ユーザは、供給されたデータの識別子と自己の秘密アルゴリズムとにより供給されたデータとユーザとの間で同一の暗号鍵を作成し暗号化データを直接的又は間接的に復号化するように構成されたデータプロテクト方式である。

図面の簡単な説明

第1図～第3図は、本発明の実施方法を説明する図である。

発明を実施するための最良の形態

本発明は上記したように、ソフトウエアを含むデータ、情報等に関する秘密を保持し、且つそれ等の不正な複写を防止するものであり、以下の具体例に於いては、特にソフトウエアを保護する場合を例にとって本発明の説明を行うが、本発明は係る具体例のみに限定されるものではない。

即ち、本発明は、センタが特別なアルゴリズム、すなわちセンタだけが秘密に保持するセンタアルゴリズムを作成し、センタは、ソフトウエア並びにユーザのそれぞれに固有で公開され且つ半固定的に用いられる各ソフトウエア並びにユーザの識別子にセンタアルゴリズムを施して各ソフトウエア並びにユーザに専用な秘密アルゴリズムを作成し、ユーザ及びソフトウエアに供給するという準備を行った後、ソフトウエア供給体とユーザとの間で、ソフトウエアの供給が生じた場合、ソフトウエア供給体は、ユーザの識別子を供給対象となるソフトウエアの秘密アルゴリズムに入力することによって、供給対象となるソフトウエアとユーザとの間で同一且つ固有の暗

号鍵を作成し、この暗号鍵に基づいて直接的又は間接的に供給対象となるソフトウエアの一部又は全部を暗号化してユーザへ供給し、ユーザは、使用時、供給されたソフトウエアの識別子を自己の秘密アルゴリズムに入力することによって、供給されたソフトウエアとユーザとの間で同一且つ固有の暗号鍵を作成し暗号化ソフトウエアを直接的又は間接的に復号化する方式により、正当なユーザは、簡単な操作によりソフトウエアの使用ができるが、その他のユーザは、コピーはできても使用ができないソフトウエアプロテクト方式を実現したものである。

つまり、本発明は、センタ（管理機関）が設けられており、センタは、センタアルゴリズムを秘密に保持する。

センタは、このセンタアルゴリズムとユーザ及びソフトウエアの識別子（名前、住所、管理番号、任意の符号、記号、数字等）から秘密アルゴリズムを作成し、ユーザ及びソフトウエアに配布する。尚、識別子は、公開、非公開、又は固有で公開され且つ半固定的に用いられるものであることが例示される。センタがソフトウエアに対して作成した秘密アルゴリズムを供給する相手となるソフトウエアとは、例えばソフトウエア自体、ソフトウエア供給体、あるいはその両者等である。

ここでソフトウエアとは、例えばアプリケーションプログラム、OSプログラム、ユーティリティプログラム、その他のプログラム及びデータを示すものであり、センタで作成される秘密アルゴリズムは、このソフトウエアの内容を問わずユーザへの供給の対象となる１つ１つのそれぞれに配布されるものである。

ソフトウエア供給体とは、ソフトウエアをユーザへ供給するものであって、例えばソフトハウス、関連メーカ、小売店、（Vender）、ソフトウエアを供給するソフトウエア、又は装置、その他有償、

間接的に無償でユーザへ対象となるソフトウエアを供給する存在である。

このソフトウエア供給体はセンタと合体する場合もあり、センタはユーザと合体する場合もある。尚、ソフトウエア供給体もソフトウエアを使用する立場になればユーザとなるのである。

尚、ユーザ及びすくなくともターゲットとなったソフトウエアは、予めまたは、各動作の直前までにセンタから秘密アルゴリズム、識別子の供給を受けているものとする。

ユーザとは、使用者の他、例えば使用者が直接又は間接に所有するソフトウエアを実行させる装置、その付属装置、あるいは、ソフトウエア自体、等が示される。

本発明の動作概要は、図１に示す様なものとなる。

ソフトウエア供給体からユーザに配布されるプログラム（Ｐ）の一部を、プログラム固有の第２暗号鍵（Ｋ）と暗号化アルゴリズムによりあらかじめ暗号化しておく（Ｐ′）。ユーザは、プログラムをインストールする際に、自らの識別子(IDu) をソフトウエア供給体に申請する。

ソフトウエア供給体では、申請された識別子(IDu) と、プログラム固有の秘密アルゴリズムを用いて第１暗号鍵を作成し、この第１暗号鍵と暗号化アルゴリズムを用いて先の第２暗号鍵Ｋを暗号化し（Ｋ′）、この（Ｋ′）をユーザに配布する。

ユーザは、配布された暗号化第２暗号鍵（Ｋ′）と、暗号化プログラム（Ｐ′）に添付（あるいは別添）のインストールソフトを用いて暗号化プログラム（Ｐ′）をインストールする。

インストールソフトは、暗号化第２暗号鍵（Ｋ′）を含んだローダを作成し、暗号化プログラム（Ｐ′）とリンクする。ローダは、実行する度にユーザの秘密アルゴリズムとプログラムの識別子を用

いて共有鍵（第１暗号鍵）を作成し、復号アルゴリズムと共に暗号化第２暗号鍵（Ｋ′）を復号化して第２暗号鍵を作成し、この第２暗号鍵と復号化アルゴリズムによって暗号化プログラム（Ｐ′）を復号する（Ｐ）。

尚、上記は、暗号鍵を２つ用いてプログラムに暗号化復号化を施すものであり、間接的方法であるが、この様な複数の暗号鍵を使用する間接的方法に限らず１つの暗号鍵（自己の秘密アルゴリズムと相手の識別子とから得られる共有鍵）を使用してプログラムを暗号化復号化する直接的方法であってもよい。

センタアルゴリズムの作成方法、秘密アルゴリズムの作成方法、及び共有する暗号鍵の作成方法、エンティティ、識別子の定義等、共有鍵を作成するまでの行程に係わる方法及び内容は、特開昭63年第 36634号公報、特開昭63年第107667号公報に記載されている通りである。

尚、識別子を秘密アルゴリズムに施す場合、上述の公報に記載されている方式の他、論文（松本、高嶋、今井“簡易型一方向性アルゴリズムの構成”信学技報IT89-23, July 1989）に記載された方式が好適に利用される。

又、２つ以上の暗号化乃至復号化アルゴリズムは、同一であってもよい。これは例えば、DES (Data Encyption Standard) 方式、FEAL (Fast Data Encipherment Algorithm) 方式等が示されるが、速度、暗号の程度によっては、その他の方式が採用されてもよい。

実施例１

図２は、本発明の１実施例を説明するための図である。尚、センタについては上述したものであり説明は省略した。

条　件

①ユーザは、センタから秘密アルゴリズム及び本人認証アルゴリズムを記憶した担体（例えば、ICカード、ディスケットその他の記憶媒体等）及びこの担体と共同して動作する担体実行装置及び識別子を所有する。ソフトウエア供給体も同様に、アルゴリズムを記憶した担体及び担体実行装置を所有している。尚、ソフトウエア供給体は、特に担体及び担体実行装置という構成でアルゴリズムを所有している必要はない。

②バックアップは自由に行なえる。

③全ソフトハウス（ソフトウエア供給体）、全プログラムについて汎用である。

環境及び定義

ソフトハウス（ソフトウエア供給体）：販売するプログラム（P）に固有の秘密アルゴリズム（プログラム識別子をIDp とする）を管理する。

販売する際は、プログラム（P）の一部を任意（ただしPに固有）の乱数（K）（第2暗号鍵）と暗号化アルゴリズムとを用いて暗号化したプログラム（P′）を配布する。（P′）は、実行できないファイルである。

暗号化プログラム（P′）を購入したユーザが、自らの識別子(IDu)を申請するので、正規ユーザからの申請であれば識別子(IDu)と、秘密アルゴリズムを用いて第1暗号鍵を作成し、この第1暗号鍵と暗号化アルゴリズムを用いて第2暗号鍵である乱数（K）を暗号化して暗号化乱数（K′）を作成し、ユーザに対して暗号化乱数（K′）を配布する（K′には、第1暗号鍵作成システムに付随するデータを含む。）

ユーザ：購入したプログラムをインストールする際に、ソフトハウスに対して自らの識別子(IDu) を申請する。尚、申請しなくても

よい場合もある。

ソフトハウスから送られてくるK′をインストールソフトに入力する。インストールソフトにより作成されたローダを用いてプログラムを使用する。

インストールソフト：ユーザにより入力された識別子(IDp)、暗号化乱数（K′）を用いてローダを作成し、暗号化プログラム（P′）とリンクする。このインストールソフトは、暗号化プログラム（P′）に添付、又は別途購入（無料配布）され、すべてのプログラムに共通である。

ローダ：ユーザが所持する担体及び担体実行装置を用い、自らファイル中に所持するプログラムの識別子(IDp)、暗号化乱数（K′）をパラメータとして与え、暗号化プログラム（P′）を復号しプログラム（P）を得る。但し、Pはメモリ上にのみ存在し、ファイル化はされない。また、P′は、必要とされる部分だけが復号され、完全な形としてのプログラム（P）は存在しない。また、ローダには復号ルーチンは存在しない。

担体実行装置：ターゲットプログラム実行装置（例えばパソコン、オフコン、WSその他の実行装置）と一体化、別体化、内蔵化して接続（赤外線、電気、光、超音波、電波等の様式で）された装置であって例えば、担体（例えばICカードディスケットその他の記憶媒体）のリーダ、ライター機構を具備するものであり、内部に復号プログラム（復号アルゴリズム）(Adapter Cipher Engine : ACE)を内蔵し、担体が出力する乱数（K）を基に、暗号化プログラム（P′）を復号する。乱数（K）は、担体実行装置でのみ存在し、外部には出力されない。

また、将来性を考え、ACE は、バージョンアップ又は、ACE そのものの変更(DES→FEAL等）を可能とするのが望ましい。尚、担体及

び担体実行装置は、一例であって、その他これらを合体させターゲットプログラム実行装置に内蔵化、一体化、別体化させたものあるいはプリンタ用接続インタフェース、ＲＳ２３２Ｃ等の接続部に付属的又は中継的に接続させたものあるいは、プログラム化し、ターゲットプログラム実行装置内部で動作させるもの等であってもよい。

又、担体実行装置はＩＣカード等の別体化した担体を使用せず、担体の機能を内蔵化した１つの装置としても良い。

処理手順

（１）ソフトハウス側の処理～プログラムの配布前～

・ソフトハウスは、ターゲットとするプログラム（Ｐ）を複数のローダブルモジュールに分割する。また、全モジュールが、一度にメモリ上にロードされない様に、プログラムを設計する。

・分割したそれぞれのモジュールの、任意の一部を暗号化する。暗号部のアドレス情報は、暗号化プログラム（Ｐ′）中に存在する。アドレス情報自体も暗号化されていても良い。

・暗号化に用いる乱数（第２暗号鍵）（Ｋ）は、プログラム毎にユニークである。更に、モジュール毎にユニークとしても良い。

・この暗号化の手段は、担体実行装置内蔵の復号プログラム（復号アルゴリズム）ACE で対応できる方法ならば、どのような方法でも構わない。ソフトウエア供給体が独自のACE を用意し、ユーザに配布するのであれば、全ソフトウエア供給体共通でなくとも良い。

（２）ユーザ側の処理～プログラム購入時～

（担体、担体実行装置、インストールソフトは既に用意されているとする）

・ソフトウエア供給体に対して、ユーザ登録し、本人識別子を申請する。

（３）ソフトハウス側の処理～ユーザ登録時～

・ユーザが申請した識別子(IDu) と、配布したプログラムに固有の秘密アルゴリズム（Xp）を用いて、乱数（K）を暗号化する（K′）。

尚、秘密アルゴリズム（Xp）を使用する際、図２では、パスワード符号(PIN-P) を入力し、本人認証アルゴリズム(CHA-P) によって本人と一致不一致を判断している。本人認証アルゴリズム(CHA-P) 及びパスワード符号(PIN-P) は、センタから秘密アルゴリズム（Xp）が提供される際、一緒に添付されて来るものであるが、その使用は任意であり、又センタからの提供も任意である。ユーザ側の本人認証アルゴリズム(CHP-U) 及びパスワード符号(PIN-U) も同様である。

ソフトウエア供給体は、暗号化乱数（K′）をユーザに送付する。送付の方法は、電話、ファックス、パソコン通信、又はフロッピー等どのような方法でも構わない（Pの暗号化にDES を用いた場合、ユーザに送付する情報量は、例えば16バイト（文字列に変換して32文字）となる。）。また、プログラムの識別子(IDp) は、暗号化乱数（K′）と共にユーザに通知しても良いが、暗号化プログラム（P′）配布時に、パッケージに印刷する等の方法も可能である。

（４）ユーザ側の処理～プログラムインストール時～

・ユーザは、インストールソフトを起動し、送られてきた暗号化乱数（K′）と、プログラム識別子(IDp) を入力する。

・インストールソフトは、入力された暗号化乱数（K′）とプログラム識別子(IDp) を用いてローダを作成し、暗号化プログラム（P′）とリンクする（ローダ付きP′）。ローダとは、OS（MS-DOS等）が処理できるユーティリティであり、OSと、暗号化プログラム（P′）の仲介をする。この時点では、まだ暗号化プログラム（P′

）は暗号化されたままである。

（５）ユーザ側の処理～プログラム実行時～

・ローダ付きＰ′を起動し、担体の本人認証を行なう。

・ローダは、プログラム識別子(IDp）と秘密アルゴリズム（Xu）から第１暗号鍵(Kup）を作成し、暗号化乱数（Ｋ′）を担体実行装置に与え、第１暗号鍵(Kup）と復号プログラム（Ｄ）により、暗号化乱数（Ｋ′）を復号させる。但し、復号した乱数（Ｋ）は、担体実行装置の中にとどまり、外部には出力されない。

・ローダは、担体実行装置に暗号化プログラム（Ｐ′）の暗号部分を与え、復号プログラム（DE）と乱数（Ｋ）によって復号させ、プログラムＰを得て実行させる。

・ローダは常にプログラム（Ｐ）の実行状態を監視し、暗号化プログラム（Ｐ′）の暗号部分が読み込まれる度に、担体実行装置に復号させる。

尚、暗号化プログラム（Ｐ′）は、それ自体では解読不可能であることからさまざまな態様で正当なユーザのみに配送可能となる。これは例えば、

・CD-ROM等の高容量記録媒体中に秘密アルゴリズムを既にまたは予約した状態で付帯する複数のプログラム（但し、パスワードを与えないと機能が制限されている）を収録し、秘密アルゴリズムを既にまたは予約した状態で付帯するユーザは試用の後、気に入ったプログラムのパスワード、識別子、を使用料を払って取得する態様。

等である。

尚、ソフトウエア供給体にとっても以下のような利便性がある。

・ソフトウエア供給体は、暗号化したプログラムをプレスすれば良いので、量産できる。

・必要とするハードウェアは、複数のソフトウエア供給体で使用で

きる。

更に他の実施例を図３に示す。図３は、図２で示した実施例においてさらに第３の暗号鍵及び暗号アルゴリズム、復号アルゴリズムを加えたものである。

第１の暗号鍵(Kup)は、秘密アルゴリズムと相手（ユーザからすればターゲットプログラム）の識別子(IDp)を施して算術的に得られる。ソフトウエア供給体においては、(Kpu)で示されている。

第２の暗号鍵（ｒ）は、乱数等の任意に設定されたものである。第３の暗号鍵（Ｋ２）も第２暗号鍵と同様任意に設定されたものである。

ソフトウエア供給体は、プログラム（Ｐ）の一部乃至全部を、第３暗号鍵（Ｋ２）と暗号アルゴリズム（Ｅ３）とにより暗号プログラム（Ｐ′）に変換する。

更に、ソフトウエア供給体は、第３暗号鍵（Ｋ２）の一部乃至全部を、第２暗号鍵（ｒ）と暗号アルゴリズム（Ｅ２）とにより暗号化第３暗号鍵（Ｋ２′）に変換する。

更に、ソフトウエア供給体は、第２暗号鍵（ｒ）の一部乃至全部を、第１暗号鍵(Kpu)と暗号アルゴリズム（Ｅ１）とにより暗号化第２暗号鍵（Ｅ（ｒ））に変換する。

ソフトウエア供給体は、暗号プログラム（Ｐ′）、暗号化第２暗号鍵（Ｅ（ｒ））、暗号化第３暗号鍵（Ｋ２′）をユーザに供給する。

ユーザは、暗号化第２暗号鍵（Ｅ（ｒ））を第１暗号鍵(Kup)と復号アルゴリズム（Ｄ１）とにより、復号化した第２暗号鍵（ｒ）を作成し、この第２暗号鍵（ｒ）と復号アルゴリズム（Ｄ２）とにより暗号第３暗号鍵（Ｋ２′）を復号化して第３暗号鍵（Ｋ２）を作成する。

この第３暗号鍵（Ｋ２）と復号アルゴリズム（Ｄ３）とにより暗号化プログラム（Ｐ′）を復号化してプログラム（Ｐ）作成する。

以上が図３の概略的動作を説明したものであるが、その他の動作は、図２の説明の通りである。

産業上の利用可能性

以上詳述した通り本発明は、センタという機関を通じてソフトウエア並びにユーザは固有の秘密アルゴリズムと識別子を付与されているという環境において、ユーザは、暗号化されたソフトウエアを所持し、必要なときだけ自分の秘密アルゴリズムにソフトウエアの識別子を入力するだけで、これを簡単に復号使用できることから、操作が簡単で、しかも、ユーザは、秘密アルゴリズムを所有してさえいれば、あとは、ソフトウエアが追加、変更されようと、識別子が入手できる限りそのソフトウエアが使用出来ることとなり、ユーザの負担は、小さくなる。

これに対し、その他のユーザにとっては、暗号化されたソフトウエアを入手してもその解読は、ほぼ不可能であることから、充分なプロテクトがなされるものである。

請 求 の 範 囲

1．センタが特別なアルゴリズム、すなわちセンタだけが秘密に保持するセンタアルゴリズムを作成し、センタは、データ並びにユーザのそれぞれに用いられる各データ並びにユーザの識別子にセンタアルゴリズムを施して各データ並びにユーザに専用な秘密アルゴリズムを作成し、ユーザ及びデータに供給するという準備を行った後、データの供給体は、ユーザの識別子と供給対象となるデータの秘密アルゴリズムとにより、供給対象となるデータとユーザとの間で同一の暗号鍵を作成し、この暗号鍵に基づいて直接的又は間接的に供給対象となるデータの一部又は全部を暗号化してユーザへ供給し、ユーザは、供給されたデータの識別子と自己の秘密アルゴリズムとにより供給されたデータとユーザとの間で同一の暗号鍵を作成し暗号化データを直接的又は間接的に復号化することを特徴とするデータプロテクト方式。

2．上記データが、ソフトウエアである事を特徴とする請求範囲第1項記載のデータプロテクト方式。

3．更に、乱数を用いて、共通鍵を暗号化する事を特徴とする請求範囲第1項記載のデータプロテクト方式。

4．更に、第2の鍵を用いて、データを暗号化する事を特徴とする請求範囲第1項記載のデータプロテクト方式。

CLMS