明　細　書

ソフトウェアの防衛のシステム

技術分野

本発明はソフトウェアの防衛のシステムに関する。本発明によるシステムは例えばアプリケーションソフトウェア、オペレイティングシステム、等のソフトウェアを保護しソフトウェアウィルスの侵入から防御するために用いられる。

背景技術

現在、アプリケーションプログラム、オペレイティングシステム用ソフトウェア、ユーティリティプログラム等の無断コピーは、日常的であるが、無断コピーによる不正使用に対する防御について充分なものは、得られていない。又、プログラムに対し、そのプログラムを改ざんまたは破壊する目的で作られたプログラム等のいわゆるウィルスの混入から、防御するための手段についても未だ充分なものが得られていない。そこで、防御するための適切な手段が望まれている。

発明の開示

本発明の１つの目的は、正当なユーザは簡単な操作によりソフトウェアの使用はできるが、その他のユーザは、そのソフトウェアの使用を不可能とし、又、ウィルスの侵入によるデータソフトウェアの改ざん等があった場合にこれを検出、警報するようにしたソフトウェアの防衛システムを実現することにある。

本発明においては、ソフトウェア供給部は、供給対象のプログラ

ムをセンタ部およびユーザ部へ供給する準備を行い、センタ部は、該供給されるプログラムに所定の変換を施して変換プログラムを作成し該変換プログラムをユーザへ供給する準備を行い、ユーザ部は、プログラム使用時該プログラムに所定の変換を施して変換プログラムを作成し該変換プログラムとセンタ部から供給される変換プログラムを比較し、該比較の結果両者が一致した場合のみ、プログラムを実行する、ことを特徴とするソフトウェアの防衛のシステム、が提供される。

また本発明においては、ソフトウェア供給部は、供給対象のプログラムを第1の鍵によって暗号化して暗号化プログラムを作成し、第1の鍵を第2の鍵によって暗号化して暗号化第1鍵を作成し、センタ部へ該暗号化プログラムを供給し、ユーザ部へ該暗号化プログラムおよび該暗号化第1鍵を供給する準備を行い、センタ部は、供給される該暗号化プログラムに所定の変換を施して変換プログラムを作成し、該変換プログラムに第3の鍵を用いて暗号化変換プログラムを作成し、第4の鍵を用いて第3の鍵を暗号化し、暗号化第3鍵を作成し、ユーザ部へ該暗号化変換プログラム、暗号化第3鍵を供給する準備を行い、ユーザ部は、プログラム使用時に、該暗号化プログラムに所定の変換を施して変換プログラムを作成し、該暗号化第3鍵を第5の鍵によって復号化して第3鍵を作成し、暗号化変換プログラムを該第3鍵を用いて復号化して復号化変換プログラムを作成し、復号化変換プログラムと変換プログラムを比較し、該比較の結果両者が一致した場合のみ第6の鍵によって復号化した第1鍵によって復号化したプログラムを実行する、ことを特徴とするソフトウェアの防衛のシステム、が提供される。

図面の簡単な説明

第１図は本発明の一実施例としてのソフトウェア防衛システムが適用されるべき情報処理回路網を示し、第２図は本発明の他の実施例による同様の回路網を示す。

発明実施の最良の形態

本発明の一実施例としてのソフトウェア防衛システムが適用される情報処理回路網が第１図に示される。第１図に於て（１）は、ソフトウェアハウスであり、主にソフトウェアを供給する為の存在であり、上述した様な構成を有するものであって、販売するプログラム（Ｐ）の一部、又は全部をプログラム固有の任意の鍵（Ｋ）を用いて暗号化し暗号化プログラム（P_1)を作成する。このP_1は実行できないものである。又このP_1をソフト管理センタ部（２）に登録する。

暗号化プログラムP_1を購入したユーザ部（３）からの申請により、そのユーザの公開鍵Ｐ（ｕ）を使用してＫを暗号化し（K_1)、この暗号化鍵K_1をユーザ部（３）に配付する。

ソフトウェア管理センタ（２）には変換装置（21）および暗号化装置（22)，（23）が設けられる。ソフトウェア管理センタ（２）において、ソフトウェアハウスが登録したP_1を何らかのハッシュ（Hash）関数を用いて圧縮し圧縮暗号化プログラム（P_2)としこれをP_1に固有の任意の鍵（ｒ）を用いて暗号化しP_3を作成する。この時に使用した鍵（ｒ）をソフト管理センタ部の秘密鍵Ｓ（sc）を用いて暗号化しr_1を作成する、r_1，P_3はユーザ部を特定せず予め作成出来るので、ソフトウェアハウスが販売するP_1と同じ記憶媒体に納めてもよい。

ユーザ部（３）において、プログラムを購入したとき又はその後に、プログラム購入の通知および鍵配付の申請をソフトウェアハウ

ス（１）に通信する。ソフトウェアハウスから送られてくるK_1を、インストールソフトに入力する、ユーザ部は、インストールソフトにより作成されたローダと情報担体装置（31）を用いてプログラム実行する。装置（31）はプログラム実行装置（32）に付属する情報担体装置である。装置（31）は、プログラム実行装置と接続されている。プログラム実行装置には、キーボードディスプレイの他、ハードディスク、磁気ディスク等の記憶装置、及びその入出力装置も付属されている場合もある。

情報担体装置（31）に、復号装置(311)，(312)，(315)，(316)、変換装置(314)、および比較装置(317)が設けられている。情報担体装置（31）はユーザ部の秘密鍵及び復号プログラム、認証プログラムが納められており、ユーザ部がプログラムを実行させようとするパソコンの、プリンターポート又は、RS232Cポート、その他に接続し各データ（K_1，P_1，r_1，P_3)の復号化や、プログラム認証を行うものである。なおRS232Cはインターフェイスに関するアメリカ電子工業会による規格である。なお、情報担体装置（31）は例えばパーソナルコンピュータと接続可能なICカードであってもよい。

第１図に於て、暗号化手段11，12，22，23はDES，FEAL(登録商標)の暗号アルゴリズム等で構成されるがこれに限定されるものではない。これらの暗号化手段は、全部異なってもよいし、全部同一であってもよい。復号化手段311，312，315，316は暗号化手段Ｅと各々対になったものであってその構成はDES，FEAL(登録商標）の復号アルゴリズムで構成されるが、これに限定されるものではない。

秘密鍵Ｓ（ｕ），Ｐ（sc）は、予めユーザ部に供給されるものであって、ここでは、情報担体（31）内部のメモリに書き込まれている。ユーザ部が所有するハッシュ関数からなる変換手段 314も予め情報担体に内蔵されるか、プログラム実行装置の記憶媒体にアルゴ

リズムとして記憶されている。また、その代りに、ソフトウェアハウス（１）から供給される暗号化プログラム（P_1)暗号化された固有の鍵（K_1)及びセンタから供給される暗号化された鍵（r_1)及び、暗号化圧縮暗号プログラム（P_2)の一部又は全部をプログラム実行装置の磁気ディスク、RAM，ROM、光磁気ディスクへ記憶させ、主な処理をプログラム実行装置で行うものであってもよい。

暗号用の鍵の使用方法としては、好適には公開鍵方式、キイプレディストリビューション(KPS) 方式等が使用される。公開鍵方式は、公開鍵、公開鍵に関する公開ファイル、秘密鍵を予め作成し、秘密鍵を各々に配付し、秘密に管理させる方式である。これらの作成、配付は、主にセンタの作業によるものであるが、特に限るものでなく、ユーザ、ソフトウェア供給部、これらの組合せ等であってもよい。公開鍵、秘密鍵の具体的内容の構成方法は、従来公知のものである。

キイプレディストリビューション(KPS) 方式は、相手の識別子を自分固有の秘密アルゴリズムに施して相手と共有の鍵を作成する方式である。秘密アルゴリズムの作成等の操作は主としてソフトウェア管理センタ部に於て行われる。ソフトウェア管理センタ部は独立的にセンタアルゴリズムを有する。このセンタアルゴリズムにユーザ、ソフトウェア及びソフトウェア供給体の識別子を施して、各々固有に所持される秘密アルゴリズムを作成する。

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63-36634号公報、特開昭63－107667号公報等に記載されている。

センタ部の操作はユーザ部、ソフトウェア供給部、これらの組合せが行ってもよい。なお上述した鍵の使用方式は好適な一例であり、

これらに限られるものではない。又、暗号アルゴリズムは、データ暗号化標準(DES)、高速データ暗号化アルゴリズム（FEAL)(登録商標）等既存するものであれば構わないものである。

ここでソフトウェアは、例えばアプリケーションプログラム、オペレイティングシステムプログラム、ユーティリティプログラム、その他のプログラムを意味する。ソフトウェア供給部は、ソフトウェアをユーザ部へ供給するものであって、例えばソフトウェアハウス、関連メーカ、小売店、ベンダ、ソフトウェアを供給するソフトウェア、又は装置、その他有償、間接的に無償でユーザ部へ対象となるソフトウェアを供給する存在である。ソフトウェア供給部はセンタ部と合体する場合もあり、センタ部はユーザ部と合体する場合もある。なおソフトウェア供給部もソフトウェアを使用する立場になればユーザ部となるのである。第１図に示される回路網におけるユーザ部は、使用者自体、使用者が所有するソフトウェアがプログラム実行を行わせる装置、それに付属する装置、ソフトウェア自体、等の形をとる。

第１図の情報処理回路網の動作が以下に記述される。動作条件として、条件、（１）ユーザ部は、そのユーザ部の秘密鍵が入っている情報担体を所有する、（２）正規のユーザ部でなければターゲットプログラムは動作しない、（３）バックアップは自由に行える、（４）データ改変チェックによりウィルス対策を可能とさせる、が前提とされる。

動作において、まず、ソフトウェアハウス（１）等からユーザ部（３）に配付されるプログラム（Ｐ）の一部又は全部を、プログラム固有の鍵（Ｋ）により予め DES等の暗号アルゴリズムを用いて暗号化しておく（P_1)。次にP_1をソフト管理センタ部（２）に登録する。

ソフト管理センタ部（２）ではこのP_1を何らかのハッシュ関数を用いて圧縮しP_2を生成し、DES等の暗号アルゴリズムを用いて暗号化しP_3とする。この時使用した鍵ｒをソフト管理センタ部（２）の秘密鍵Ｓ（sc）を用いて暗号化しておく（r_1）。

ユーザ部はP_1，r_1，P_3を入手した時又は、その後ソフトウェアハウス等にその旨を知らせる。ソフトウェアハウスではプログラム固有の鍵Ｋをそのユーザの公開鍵Ｐ（ｕ）を使用して暗号化しK_1を生成しそのK_1をユーザに配付する。ユーザはK_1，P_1，r_1，P_3を専用のインストールソフトを用いてインストールする。

ユーザ部は、プログラムを実行しようとする度にローダソフトが情報担体（31）を用いてP_1を復号化（Ｐ）し更にハッシュ関数によりP_2を生成する、又、r_1をソフト管理センタ部の公開鍵Ｐ（sc）で復号化しｒとし、このｒを用いてP_3を復号化しP_2とし、先に出力したP_2と比較することによりP_1が改ざんされていないかを点検することを可能とさせる。

暗号化アルゴリズムP_1及び暗号化鍵r_1、暗号化圧縮アルゴリズムP_3はユーザ部を特定しないので予め作成も可能、又配付元もソフトウェアハウス、ソフト管理センタのいずれでもよい。

情報担体（31）は、上述した様にプログラム実行装置に付属して使用されるものであるが小型且つ軽量で、場所をとらない形状を有することが好適である。その代りとして、この付属品を特に必要とせず、プログラム実行装置自体がすべてを行う場合もある。

本発明の他の実施例としてのソフトウェア防衛システムが適用される情報処理回路網が第２図に示される。第２図の回路網においては、ソフトウェア供給部としてのソフトウェアハウス（１）であって暗号化装置（11），（12）、および鍵形成装置（13）を包含するものが設けられる。ソフトウェアハウス（１）においてプログラム

（P）の一部、又は全部がプログラム固有の鍵（K）により暗号化され、暗号化されたプログラムP_1が作成される。このプログラムP_1は実行できないものである。この暗号化されたプログラムP_1はソフト管理センタ部に登録される。

暗号化されたプログラムP_1を購入したユーザ部からの申請により、そのユーザ部の識別子を用いて KPSによる共有暗号鍵K（SI・A)を作成し、これを使用してKを暗号化し（K_1)、ユーザ部にK_1を配付する。（Aはユーザ部の識別子を、X（SI）はアルゴリズムをあらわす。）

ソフトウェア管理センタ部（２）には、変換装置（21）、暗号化装置（22)，(23）、および鍵形成部（24）が設けられる。ソフト管理センタ部（２）において、ソフトウェアハウスが登録したP_1を何らかのハッシュ関数を用いて圧縮し（P_2)、更にこれを暗号化されたプログラムP_1に固有の鍵（ｒ）を用いて暗号化しP_3を作成する。この時に使用した鍵（ｒ）をソフトウェア供給体又はソフトウェアとユーザとの共有暗号鍵K（SI・A)を用いて暗号化しr_1を作成する。P_3はユーザを特定せず予め作成出来るので、ソフトウェアハウスが販売するP_1と同じ記憶媒体に納めてもよい。ソフト管理センタは、ソフトウェアハウスが所有する秘密アルゴリズムを予めまたは逐時的に所有する。なおソフト管理センタ部は固有の秘密アルゴリズムを所有する場合もある。この場合は、ユーザ部へ圧縮ソフト等を送付する場合、ユーザ部の識別子をセンタの秘密アルゴリズムに施して鍵を生成し、ユーザ部は、センタ部の識別子を自分の秘密アルゴリズムに施して鍵を生成することも可能となる。

ユーザ部（３）において、プログラムを購入したときまたはその後に、該購入を鍵配付の申請として、ソフトウェアハウスに、通知する。ユーザ部において、ソフトウェアハウスから送られてくるK_1

がインストールソフトに入力され、インストールソフトにより作成されたローダと情報担体装置(231) を用いてプログラムが実行される。プログラム実行装置用の情報担体装置（31）は、プログラム実行装置と接続されている。プログラム実行装置には必要に応じ、キーボードディスプレイの他、ハードディスク、磁気ディスク等の記憶装置、及びその入出力装置も付属されている場合もある。ユーザ部（３）において、ソフトウェアハウスの識別子SIが鍵生成装置(313) に供給される。（X（A）はアルゴリズムをあらわす。）

情報担体（31）にはユーザ部の秘密鍵及び復号プログラム、認証プログラムが納められており、ユーザ部がプログラムを実行させようとするパソコンの、プリンターポート又は、RS232Cポート、その他に接続し各データ（K_1，P_1，r_1，P_3)の復号化や、プログラム認証を行うものである。

第２図の回路網における暗号化手段11，12，22，23はDES，FEAL（登録商標）の暗号アルゴリズム等で構成されるがそれに限定されるものではない。これらの暗号化手段は、全部異なってもよいし、全部同一であってもよい。復号化手段311，312，315，316は暗号化手段と各々対になったものであってその構成はDES，FEAL(登録商標)の復号アルゴリズムで構成されるが、それに限定されるものではない。

秘密アルゴリズムは、予めユーザ部に供給されるものであって、ここでは、情報担体（31）内部のメモリに書き込まれている。又ユーザ部が所有するハッシュ関数からなる変換手段 314も予め情報担体に内蔵されるか、プログラム実行装置の記憶媒体にアルゴリズムとして記憶されている。

ソフトウェアハウス（１）から供給される暗号化プログラム（P_1）暗号化された固有の鍵（K_1)及びセンタ部から供給される暗号化さ

れた鍵（r_1)及び、暗号化圧縮暗号プログラム（P_3)の一部又は全部をプログラム実行装置の磁気ディスク、RAM，ROM、光磁気ディスクへ記憶させ、主な処理をプログラム実行装置で行うことが可能である。ユーザ部が用いるソフトウェア供給部又はソフトウェアの識別子Aはソフトウェアハウスが販売するP_1と同じ記憶媒体に納めてもよい。

第2図の情報処理回路網の動作が以下に記述される。動作条件として、条件（1）ユーザ部は、そのユーザ部の秘密アルゴリズムが入っている情報担体を所有する、（2）正規ユーザ部でなければターゲットプログラムは動作しない、（3）バックアップは自由に行える、（4）データ改ざんチェックにより、ウィルス対策を可能とさせる、が前提とされる。

動作において、まず、ソフトウェアハウス（1）等からユーザ（3）に配付されるプログラム（P）の一部又は全部を、プログラム固有の鍵（K）により予め DES等の暗号アルゴリズムを用いて暗号化しておく（P_1)、次にP_1をソフト管理センタ部（2）登録する。ソフト管理センタ部（2）ではこのP_1を何らかのハッシュ関数を用いて圧縮しP_2を生成し、 DES等の暗号アルゴリズムを用いて暗号化しP_3とする、又この時使用した鍵rをソフトウェア供給部又はソフトウェアとユーザ部との共有暗号鍵K（SI・A)を用いて暗号化しておく（r_1)。

ユーザ部はP_1，r_1，P_3を受理したときまたはその後に、ソフトウェアハウス等にこの受理を通知する。

ソフトウェア供給部はプログラム固有の鍵Kをそのソフトウェア供給部又はソフトウェアとユーザ部との共有暗号鍵K（SI・A)を使用して暗号化して暗号化鍵K_1を生成し該暗号化鍵K_1をユーザ部に配付する。ユーザ部において、専用のインストールソフトを用い

てK$_1$，P$_1$，r$_1$、およびP$_3$のインストールを行う。

ユーザ部において、プログラムを実行しようとするたびにローダソフトが情報担体（31）を用いてP$_1$を復号化し（P）、更にハッシュ関数によりP$_2$を生成する。r$_1$をソフトウェア供給部又はソフトウェアとユーザ部との共有暗号鍵K（SI・A)で復号化しrとし、このrを用いてP$_3$を復号化しP$_2$とし、先に出力したP$_2$と比較することによりP$_1$が改ざんされていないかを点検することを可能にする。改ざんが発見された場合には警報を発生させることが可能である。

暗号化アルゴリズムP$_1$及び暗号化圧縮アルゴリズムP$_3$はユーザを特定しないから、予め作成することが可能であり、ソフトウェアハウス、ソフトウェア管理センタ部のいずれから配付を行うことも可能である。

情報担体（31）は、上述した様にプログラム実行装置に付属して使用されるものであり、小型且つ軽量で、場所をとらない形状を有することが好適である。その代りとして、この付属品を特に必要とせずに、プログラム実行装置自体が全てを行うことも可能である。

第１図、第２図の回路網において、正当なユーザ部は簡単な操作によりソフトウェアの使用が許容され、その他のユーザ部は、そのソフトウェアの使用が許容されないようにすることができ、又、そのソフトウェアに対し、いわゆるウィルスの侵入によるデータソフトウェアの改ざん等があった場合には、これを検出、警報することができることが理解されるであろう。

請 求 の 範 囲

1．ソフトウェア供給部は、供給対象のプログラムをセンタ部及びユーザ部へ供給する準備を行い、

センタ部は、供給された該プログラムに所定の変換を施して変換プログラムを作成し該変換プログラムをユーザへ供給する準備を行い、

ユーザ部は、プログラム使用時、該プログラムに所定の変換を施して変換プログラムを作成し、この変換プログラムとセンタ部から供給される変換プログラムとを比較し、

比較の結果両者が一致した場合のみ、プログラムを実行することを特徴とするソフトウェアの防衛のシステム。

2．前記プログラムは暗号化され、ユーザ部がすくなくとも実行可能としたとき復号化される請求の範囲1記載のシステム。

3．センタ部からユーザ部へ供給される変換プログラムは暗号化され、ユーザ部が少くともプログラムを使用する時、復号化される請求の範囲1記載のシステム。

4．ソフトウェア供給部において、ユーザ部からの申請又は公開ファイルにもとづき公開鍵によりプログラムが暗号化され、ユーザ部において、秘密鍵により該暗号化されたプログラムが復号化される請求の範囲2記載のシステム。

5．センタ部はセンタ部の秘密鍵により変換プログラムを暗号化し、ユーザは、センタ部の公開鍵により暗号化された変換プログラムを復号化する請求の範囲3記載のシステム。

6．ソフトウェア供給体は、ユーザ部の識別子を、ソフトウェア又はソフトウェア供給体固有の秘密アルゴリズムに施して、ユーザ部との共通鍵を作成して前記プログラムを暗号化し、ユーザ部は、

* C L M S *

ソフトウェア又はソフトウェア供給体の識別子をユーザ部固有の秘密アルゴリズムに施してソフトウェア又はソフトウェア供給部との共通鍵を作成して暗号化したプログラムを復号化する請求の範囲2記載のシステム。

7．センタ部は、ユーザ部の識別子をソフトウェア又はソフトウェア供給体固有の秘密アルゴリズムに施してユーザ部とソフトウェア又はソフトウェア供給体間の共通鍵を作成して前記変換プログラムを暗号化し、ユーザ部は、ソフトウェア供給部の識別子をユーザ固有の秘密アルゴリズムに施してソフトウェア又はソフトウェア供給部との共通鍵を作成して暗号化した前記変換プログラムを復号化する請求の範囲3記載のシステム。

8．ソフトウェア供給部は、供給対象のプログラムを第1の鍵によって暗号化して暗号化プログラムを作成し、第1の鍵を第2の鍵によって暗号化して暗号化第1鍵を作成し、センタ部へ該暗号化プログラムを供給し、ユーザ部へ該暗号化プログラムおよび該暗号化第1鍵を供給する準備を行い、

センタ部は、供給される該暗号化プログラムに所定の変換を施して変換プログラムを作成し、該変換プログラムに第3の鍵を用いて暗号化変換プログラムを作成し、第4の鍵を用いて第3の鍵を暗号化し、暗号化第3鍵を作成し、ユーザ部へ該暗号化変換プログラム、暗号化第3鍵を供給する準備を行い、

ユーザ部は、プログラム使用時に、該暗号化プログラムに所定の変換を施して変換プログラムを作成し、該暗号化第3鍵を第5の鍵によって復号化して第3鍵を作成し、暗号化変換プログラムを該第3鍵を用いて復号化して復号化変換プログラムを作成し、復号化変換プログラムと変換プログラムを比較し、比較の結果両者が一致した場合のみ、第6の鍵によって復号化した第1鍵によって復号化し

* C L M S *

たプログラムを実行することを特徴とするソフトウェアの防衛のシステム。

9．第2の鍵はユーザ部の公開鍵であり、第6の鍵は、ユーザ部の秘密鍵であり、第4の鍵はセンタ部の秘密鍵であり、第5の鍵は、センタ部の公開鍵である請求の範囲8記載のソフトウェア防衛方式。

10．第2の鍵は、ユーザ部の識別子をソフトウェア供給部又はソフトウェアの秘密アルゴリズムに施して得られたユーザ部との共通鍵であり、第5の鍵及び第6の鍵は、ソフトウェア供給部又はソフトウェアの識別子をユーザ部の秘密アルゴリズムに施して得られたソフトウェア供給部又はソフトウェアとの共通鍵であり、第4の鍵は、ユーザ部の識別子をセンタ部が所有するソフトウェア供給部又はソフトウェアの秘密アルゴリズムに施して得られたユーザ部との共通鍵である請求の範囲8記載のシステム。