(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3689431号
(P3689431)
(45)発行日　平成17年8月31日(2005.8.31)　(24)登録日　平成17年6月17日(2005.6.17)

(51)Int.Cl.[7]　F I
G06F 1/00　G06F 1/00 370E
G06F 9/06　G06F 9/06 550A

請求項の数 28　(全 12 頁)

(21)出願番号　特願平10-548145
(86)(22)出願日　平成10年4月29日(1998.4.29)
(65)公表番号　特表2000-516373(P2000-516373A)
(43)公表日　平成12年12月5日(2000.12.5)
(86)国際出願番号　PCT/US1998/008374
(87)国際公開番号　WO1998/050842
(87)国際公開日　平成10年11月12日(1998.11.12)
審査請求日　平成12年4月21日(2000.4.21)
(31)優先権主張番号　08/848,963
(32)優先日　平成9年5月2日(1997.5.2)
(33)優先権主張国　米国(US)

(73)特許権者
フェニックス　テクノロジーズ，リミテッド
アメリカ合衆国　９５１３４　カリフォルニア州，サン　ホセ，イースト　プルメリア　ドライブ　４１１
(74)代理人
弁理士　平木　祐輔
(74)代理人
弁理士　関谷　三男
(74)代理人
弁理士　中村　和男

最終頁に続く

(54)【発明の名称】暗号化キーの安全処理のための方法及び装置

(57)【特許請求の範囲】
【請求項１】
安全プロセッサモードを有するメインシステムプロセッサを使用した、暗号化キーの安全処理の方法であって、
安全プロセッサモードの最中、又は電源投入初期化手順の最中に、暗号化キー、暗号化プログラム、及びその他の必要な暗号化データを安全メモリにロッドする段階と、前記安全メモリに記憶された前記暗号化キーを使って、前記安全プロセッサモードにおいて、又は前記電源投入初期化手順の最中に、前記暗号化プログラムを実行する段階と、を備えることを特徴とする方法。
【請求項２】
前記安全メモリは、前記プロセッサが安全プロセッサモードにある間に、前記プロセッサによってアクセスできるだけであることを特徴とする請求の範囲１に記載の方法。
【請求項３】
前記安全プロセッサモードは、他のプロセッサ割込による割込が不可能な最高割込処理モードであることを特徴とする請求の範囲２に記載の方法。
【請求項４】
前記ロードの段階は、電源投入初期化手順の最中に実行され、また、前記実行の段階は、オペレーティングシステムがロードされた後に実行されることを特徴とする請求の範囲１に記載の方法。
【請求項５】

前記暗号化プログラム及びデータは、電源投入初期化手順の最中にロードされ、そして、前記暗号化キーは、オペレーティングシステムがロードされた後に初期化された安全プロセッサモードの最中にロードされることを特徴とする請求の範囲４に記載の方法。

【請求項６】

前記暗号化キーを前記安全メモリにロードする前に、個人同定番号（PIN）を検証する段階をさらに備えることを特徴とする請求の範囲３に記載の方法。

【請求項７】

前記電源投入初期化の最中に前記暗号化プログラムをロードする段階の後は、他の処理による前記安全メモリへのアクセスを妨げるためにシステム構成が要求した場合には、前記安全メモリをロックする段階をさらに備えることを特徴とする請求の範囲５に記載の方法。

【請求項８】

前記プロセッサはIntel３８６ファミリーコンパチブルプロセッサ、又はこれ以降のx８６モデルプロセッサであり、前記安全プロセッサモードはシステム管理モード（SMM）であることを特徴とする請求の範囲３に記載の暗号化キーの安全処理の方法。

【請求項９】

前記安全メモリはシステム管理ランダムアクセスメモリ（SMRAM）であり、前記プロセッサの初期化段階はシステム管理割込（SMI）を呼出す段階を備えることを特徴とする請求の範囲８に記載の方法。

【請求項１０】

PINを検証する前記段階は、

トークンから暗号化キーを読出す段階と、

ユーザにPINの入力を要求する段階と、

前記PINを使って前記キーを解読する段階と、

ダイジェストを生成するために、前記暗号化したキー上でハッシュ機能を実行する段階と、

前記生成されたダイジェストをシステムBIOSに記憶されたダイジェストと比較する段階と、

を備えることを特徴とする請求の範囲６に記載の方法。

【請求項１１】

メインシステムプロセッサを使用した、暗号化キーの安全処理の方法であって、

ユーザの個人同定番号（PIN）を検証する段階と、

前記ユーザのPINが検証された場合に、トークンに記憶された暗号化プログラム、及びその他の必要な暗号化データを安全メモリにロードする段階と、

他の処理による前記安全メモリへのアクセスを妨げるためにシステム構成が要求した場合、前記暗号化プログラム及びその他のデータをロードした前記安全メモリをロックする段階と、

前記安全プロセッサモードから出て、通常のブートアップ手順を継続する段階と、

を備えることを特徴とする方法。

【請求項１２】

オペレーティングシステムがロードされた後に初期化された安全プロセッサモードの最中に、暗号化キーが前記安全メモリにロードされることを特徴とする請求の範囲１１に記載の方法。

【請求項１３】

オペレーティングシステムがロードされる前に、暗号化キーが、前記暗号化プログラム及びその他のデータと共に前記安全メモリにロードされることを特徴とする請求の範囲１１に記載の方法。

【請求項１４】

前記ユーザのPINを検証する前に、前記トークンが使用可能であるかどうかを決定する段階をさらに備えることを特徴とする請求の範囲１１に記載の方法。

【請求項１５】
PINを検証する前記段階は、
前記トークンから暗号化キーを読出す段階と、
ユーザにPINの入力を要求する段階と、
前記PINを使って前記キーを解読する段階と、
ダイジェストを生成するために、前記暗号化したキー上でハッシュ機能を実行する段階と、
前記生成されたダイジェストをシステムBIOSに記憶されたダイジェストと比較する段階と、
を備えることを特徴とする請求の範囲１４に記載の方法。
【請求項１６】
前記安全メモリは、前記プロセッサが安全プロセッサモードにある間に、前記プロセッサによってアクセスできるだけであることを特徴とする請求の範囲１１に記載の方法。
【請求項１７】
前記安全プロセッサモードは、他のプロセッサ割込による割込が不可能な最高割込処理モードであることを特徴とする請求の範囲１６に記載の方法。
【請求項１８】
前記プロセッサはIntel３８６ファミリーコンパチブルプロセッサ、又はこれ以降のx８６プロセッサであり、前記安全プロセッサモードはシステム管理モード（SMM）であることを特徴とする請求の範囲１１に記載の方法。
【請求項１９】
前記安全メモリはシステム管理ランダムアクセスメモリ（SMRAM）であり、前記プロセッサの初期化段階はシステム管理割込（SMI）を呼出す段階を備えることを特徴とする請求の範囲１８に記載の方法。
【請求項２０】
アプリケーションが安全サービスを要求した場合に、前記プロセッサは前記安全モードへと初期化され、オペレーティングシステムはスリープモードに置かれ、前記暗号化プログラムが実行されることを特徴とする請求の範囲１２に記載の方法。
【請求項２１】
暗号化キーを安全処理する安全処理装置であって、前記装置が、安全プロセッサモードを有するメインシステムプロセッサと、前記プロセッサが前記安全プロセッサモードにある間に、前記プロセッサによってアクセスできるだけである安全メモリと、トークンに記憶された暗号化キー、プログラム、及び関連データとを備え、前記暗号化キー、プログラム、及び関連データは、電源投入初期化の最中、又は安全プロセッサモードの最中に前記安全メモリに記憶され、電源投入初期化の最中又は安全プロセッサモードの最中に、前記暗号化キー、プログラム、及び関連データがプロセッサによって処理されることを特徴とする安全処理装置。
【請求項２２】
前記安全プロセッサモードは、他のプロセッサ割込による割込が不可能な最高割込処理モードであることを特徴とする請求の範囲２１に記載の安全処理装置。
【請求項２３】
前記暗号化キーとプログラムを前記安全メモリにロードする前に、前記トークンが使用可能であるかどうかを決定するトークン決定手段をさらに備えることを特徴とする請求の範囲２２に記載の安全処理装置。
【請求項２４】
前記トークンが使用可能であると決定した後、また、前記暗号化キー及びプログラムをロードする前に、ユーザのPINを検証する個人同定番号（PIN）検証手段をさらに備えることを特徴とする請求の範囲２３に記載の安全処理装置。
【請求項２５】
前記プロセッサはIntel３８６ファミリーコンパチブルプロセッサ、又はこれ以降のx８６

プロセッサであり、前記安全プロセッサモードはシステム管理モード（SMM）であることを特徴とする請求の範囲２４に記載の安全処理装置。
【請求項２６】
前記安全メモリはシステム管理ランダムアクセスメモリ（SMRAM）であり、システム管理割込（SMI）を呼出すことにより、前記プロセッサが前記システム管理モード（SMM）に初期化されることを特徴とする請求の範囲２５に記載の安全処理装置。
【請求項２７】
前記PIN検証手段は、
前記トークンから暗号化キーを読出す読出手段と、
ユーザにPINの入力を要求するPIN要求手段と、
前記PINを使って前記キーを解読する解読手段と、
ダイジェストを生成するために、前記暗号化したキー上でハッシュ機能を計算するハッシュ機能計算手段と、
前記生成されたダイジェストをシステムBIOSに記憶されたダイジェストと比較する比較手段と、
を備えることを特徴とする請求の範囲２４に記載の安全処理装置。
【請求項２８】
他の処理による前記安全メモリへのアクセスを妨げるためにシステム構成が要求した場合に、前記メモリをロックするためのロック手段をさらに備えることを特徴とする請求の範囲２３に記載の安全処理装置。
【発明の詳細な説明】
発明の背景
1．発明の範囲
本発明は一般に、コンピュータ安全保護に関するものであり、さらに、暗号化キーを安全処理するための方法及び装置に関するものである。
2．関連技術の説明
コンピュータの安全性の問題により、ユーザは秘密の情報を保護するための膨大な手段の実行を促されている。コンピュータシステムは、正式に認証されたユーザのみがシステム資源にアクセスできる様々なタイプのアクセス規制を採用している。秘密の情報を公開ネットワークを介して送信する際に割込や解読から保護するために、複合暗号化及び解読アルゴリズムが使用されている。さらに、ユーザ認証、特権アクセスの許可、安全なオンライン電子商業の促進のために、デジタルサイン、デジタル封筒、証明、認証、非拒絶（non-repudiation）のような新規の技術が使用されている。これら全ての技術は、情報を保護するために「キー」と呼ばれるある形式の「機密」情報を必要とする。データの保護、アクセス許可、ユーザ認証等に使用される秘密キーは、総体的に「暗号化キー」と呼ばれる。これらの暗号化キーを最も効果的にするには、安全危害処理によって「機密」情報が漏れることないように、これらの暗号化キーを安全環境において扱うべきである。暗号化技術については、本明細書中で参照しているJohn Wiley & Sons,Inc.発行、Bruce Schneier著のApplied Cryptography,第2版(1996年)に一般的に説明されている。
例えば、遠隔ユーザアクセスの1方法は、トークンに記憶された秘密キーを使用し、また、challenge/response同定として知られている。トークンは、フロッピーディスク、Fortezzaカード、PCMCIAカード、スマートカード、またさらにはソフトウェア内にのみ存在する「仮想」スマートカードといったあらゆるタイプの脱着可能な記憶装置で構成することができる。トークンを物理的に所有することにより、ユーザは遠隔サーバへのアクセスを許可される。このスキームにおいて、ホストがユーザにchallengeとして乱数を送信する。ユーザは、challengeの数学的計算と、ホストとユーザの両者が知っている秘密キーに基づいてresponseを返送する。両者の側において同様の計算を個別に行うことにより、最終的にユーザの同一性が決定される。公開ネットワーク上で捕獲される可能性を排除するために、秘密キー自体は絶対に送信されない。
しかし、ユーザのコンピュータ上でresopnseと秘密キーを処理することは安全性の問題を

引起す。ユーザは秘密キー、認証プログラムを監視することができ、秘密キー及び/又は認証プログラムをコピーすることができる。コンピュータ上で実行されているその他のソフトウェアも秘密の情報を監視及びコピーすることが可能である。従って、秘密キーと認証プログラムは、ユーザや他のコンピュータ処理による不当な変更や監視が不可能な安全環境において処理されるべきである。

秘密キーと認証プログラムを不当な変更から保護するために、スマートカードの使用が好ましい方法であるとされてきた。スマートカードは各々クレジットカードの大きさのプラスチックカードであり、特別タイプの埋込み型集積回路を備えている。この集積回路は電子形式の情報を含有し、カードの領域内で情報を処理する。秘密キーと、必要なあらゆる暗号化/解読アルゴリズム又は認証プログラムがスマートカード内で処理されるため、外部処理が秘密の情報を監視することができない。ユーザは、スマートカードの内部処理を見ることもできない。一般に、スマートカードは以下の構成部分から成る。

・マイクロプロセッサ（通常8ビット）
・EEPROM（通常8～32キロビット）
・オンチップオペレーションシステム
・埋込み型の暗号化ソフトウェア（DES、ゼロ・ナレッジ、又はRSAアルゴリズムのいずれかを実行する）
・EEPROMに事前にプログラムされた永久PINで暗号化された秘密キー

秘密キーに基づいた全てのオペレーションがその境界内で実行されるため、スマートカードは、秘密キーの記憶及び処理を行うための安全環境を提供する。従って、秘密キー又は暗号化アルゴリズムが外界に露出することは絶対になく、そのため、不正ユーザがこれらを観察することは不可能である。スマートカードはパスワード妥当性検査スキームの実行にだけでなく、暗号化/解読アルゴリズム、ユーザ認証、非拒絶（non-repudiation）方法の実行にも使用されてきた。データ処理のために秘密情報を要求するあらゆるアプリケーションは、スマートカードの安全処理環境を利用するように適応することができる。しかし、物理スマートカードスキームは高価であり、また、システムにアクセスするためには各ユーザが物理スマートカードとスマートカードリーダを所有しなければならないために面倒である。現在スマートカードリーダは少数購入の場合1つが約100ドルであり、スマートカード自体は1枚約6～8ドルである。各コンピュータに物理カードリーダをインストールするには、小規模の実施であってもかなりの費用がかかってしまう。

物理スマートカード認証システムの実施に関連する費用を改めるために、数社の企業が「仮想スマートカード」の使用を提案している。現在実施されているように、仮想スマートカードはソフトウェア内に存在し、アプリケーションとして実行される。通常、秘密キーはハードドライブ又はフロッピーディスクに記憶され、個人同定番号（PIN）によって保護される。従って、仮想スマートカードソフトウェアと、関連するPINを有するマシンは全て遠隔システムにアクセスすることが可能である。しかしながら、このアプローチには、秘密キーの処理が「オープン」に行われるという問題が伴う。すなわち、秘密キーがシステムメモリ内に読出され、「オープン」モードでロックを解かれてしまう。これにより、キーとその処理が、同一のシステム上で実行されているその他の処理によって不当に変更される可能性が生じる。

従って、暗号化キー、アルゴリズム、関連するプログラムが安全処理環境において記憶、処理され、また、他のシステム処理によるアクセス、ユーザによる監視が不可能であるコンピュータ完全システムが望ましい。また、この安全システムが、さらに周辺機器を追加する必要なく、現在あるハードウェアを使用することが望ましい。

発明の概要

本発明は、安全プロセッサモード及び関連する安全メモリを使用して、暗号化キーを安全に記憶及び処理するための方法及び装置である。プロセッサは、他の割込による割込が不可能な安全処理モードに初期化される。プロセッサが安全処理モードにない場合には、どんな処理も関連する安全メモリにアクセスすることはできない。実行時間中に、プロセッサが安全処理モードに入る際には、オペレーティングシステムは中断される。

暗号化形式で記憶された暗号化キーは、フロッピーディスク、CD-ROM、ドングル等の脱着可能な記憶装置内に常駐している。システムが安全プロセッサモードに入ると、システムが脱着可能な記憶装置から安全メモリ内に暗号化キーを読出す。プロセッサが安全モードに入ると、システムBIOS内に記憶されている必要な暗号化キープログラムも、安全メモリ内にロードされる。必要であれば、他の処理による記憶されたデータへのアクセスを防止するために安全メモリがロックされる。キーとプログラムが安全メモリ内にロードされると、ユーザは脱着可能な記憶装置を除去するように促され、プロセッサが安全モードから出る。従って、キーとプログラムの安全メモリ内へのローディングを、オペレーティングシステム及びその他の処理を見ることはできない。

安全メモリ内に記憶された秘密キーのロックを解くために、ユーザはPINを入力するように要求される。安全キーを安全メモリ内にローディングすることにより、また、PINでキーのロックを解くことにより、システムは物理スマートカードと同様の機能を有する。アプリケーションは、あたかもシステムに物理スマートカードが接続しているかのように暗号化サービスを要求することができる。アプリケーションが暗号化サービスを要求する度に、プロセッサが、要求されたオペレーションを実行するために安全プロセッサモードに入る。従って、秘密キーの記憶及び処理はオペレーティングシステム及びその他の処理には見えない。キーをクリアするために、ユーザはシステムに安全メモリをクリアするように要求することができる。

ここで説明したように、システムは、安全キーと要求された暗号化プログラムを安全メモリ内にロードするために安全プロセッサモードに入る。システムは、キーと要求された暗号化プログラムをロード及び処理するために、ブート時間において、又は実行時間中ならいつでも安全モードに入ることができる。しかし、ほかに実行されている処理はないため、キーのロード又は処理のためにプロセッサがブート時間中に安全モードにある必要はない。従って、ハードウェアを追加する必要なく、暗号化キーの安全処理が得られる。

【図面の簡単な説明】

添付の図面に図示した以下の説明を考慮することで、本発明の目的及び利点と共に本発明の正確な特性が容易に明白になるであろう。

第1図は、本発明を利用した電源投入手順を示すフローチャートである。

第2図は、本発明の実行時間処理を示すフローチャートである。

第3図は、ユーザの個人同定番号（PIN）を妥当性検査するための好ましい方法を示すフローチャートである。

第4図は、シークレットキーの実行時間ローディングを示すフローチャートである。

第5図は、本発明の装置を示すブロック図である。

好ましい実施例の説明

以下に示す説明は、あらゆる当業者に本発明を作成及び使用させるためのものであり、また、発明者が本発明の最適モードでの実行を述べたものである。しかし、ここでは本発明の基本的な原理を特に暗号化キーの安全処理の方法及び装置に画定しているので、当業者には様々な変更が可能であることが容易にわかるであろう。

本発明は、トークン上に、また、関連する特別安全メモリ範囲に供給された暗号化キーの処理に特別の安全処理モードを使用している。安全モードの1例として、Intel x86（80386以降）プロセッサアーキテクチャのシステム管理モード（SMM）、及び互換性のあるプロセッサである。関連するメモリはシステム管理RAM（SMRAM）として知られている。プロセッサのシステム管理モード（SSM）とシステム管理RAM（SMRAM）は両方共オペレーティングシステムとそのアプリケーションにとって透明である。暗号化キーとアルゴリズムは、一旦SMRAM内に記憶されるとSMMの最中に使用することができるため、暗号化キーとその処理が露呈することは絶対にない。そのため、この方法と装置は、高価なスマートカードハードウェアを使用する必要のない安全な暗号化キーの処理を提供し、また、仮想スマートカード処理よりも安全である。

次に、第1図を参照して本発明の好ましい実施例を説明する。以下に示す好ましい実施例の説明は、コンピュータシステムの電源投入手段に適応する。電源投入手順の最中はオペ

レーティングシステムがロードされていないため、暗号化キーとプログラムの内容を監視する処理なしで暗号化キーとプログラムをロードすることができるので、SMMに入ることは厳密に必要というわけではない。本発明の範囲を逸脱しない限り、SMMを呼出すことにより、本発明をシステムオペレーションのその他の段階で使用することが可能である。

段階1においてコンピュータシステムが電源投入され、段階2においてIntel x86（80386以降）のプロセッサのシステム管理モード（SMM）が初期化される。段階3では、コンピュータシステムに「トークン」が接続されているかどうかを決定する。「トークン」は、磁気ストリップ、PCMCIAカード、フロッピーディスク、CD-ROM又はその他の類似する脱着可能記憶装置といった、あらゆるタイプの脱着可能な物理記憶装置を含む。トークンは暗号化キー、及び暗号化プログラムに必要なその他のあらゆる情報を含んでいる。しかし、物理スマートカードと異なり、メインシステムプロセッサにおいて処理が安全モードで実行されるため、トークンは独自のプロセッサや付随するハードウェアを備えている必要がない。そのため、これらの脱着可能な記憶装置は物理スマートカードよりもずっと安価である。

システム中にトークンがない場合には、段階10において通常システムのブート・アップが継続するが、システムはいかなるスマートカードの機能も持たない。でなければ、ユーザの個人同定番号（PIN）が段階4で証明される。従って、本発明は、トークンに加えてPINを要求することによって、単一パスワードスキームよりも確実な安全性を提供する「2要素認証」を実行する。この方法で使用す2つの「要素」は、ユーザのPINと機密暗号化キーである。両要素を要求することにより機密侵害の危険が大幅に減少する。本発明はPINを要求しなくても実行可能であるが、これによって機密の利点は減少してしまう。段階5においてユーザのPINが妥当でない場合、段階10において通常システムのブートアップが継続するが、システムはいかなるスマートカードの機能も持たない。

ユーザのPINが検証されると、トークン上に記憶された暗号化キーがシステム管理RAM（SMRAM）内にロードされる。暗号化プログラム、及び暗号化処理に必要と思われるその他のあらゆるデータ又は情報も、段階6でSMRAM内にロードされる。これは、最初に暗号化プログラムと、関連するアルゴリズムが記憶されており、これらに変更を加えていない場合には重要でない。最初にアルゴリズムを、BIOSフラッシュROM上に、又はフロッピーディスク上に記憶することができる。好ましい実施例において、暗号化プログラムとアルゴリズムはシステムBIOSにロードされる。

次に、SMRAMが段階7においてロックされる。これにより、SMRAMに記憶されたデータへのその他の処理によるアクセスが防止される。安全プロセッサモードの最中にのみメモリにアクセスできるように意図的に設計されている場合には、他の構成又はハードウェア解決手段にさらなるロック段階を設ける必要はない。暗号化キーと、関連するアルゴリズムの転送がブート時間中に完了しているため、暗号化処理が他の処理によって変更されてしまう心配がない（同時に実行されている処理はない）。さらに、SMRAMの内容のオペレーティングシステムによる変更を防止するために、SMRAMは、オペレーティングシステムのロード以前にロックされ、チップセットによって隠されている。従って、システム管理モードは物理スマートカードと似た安全な処理環境を提供するが、ハードウェアの追加を必要とせず、物理スマートカードよりも安価である。

段階8でユーザは、システムのインテグリティを保証するために物理トークンを除去するように求められる。トークンを除去すると（段階9）、通常システムのブート手順は段階10において継続する。従って、本発明は、コストをかけずに、物理スマートカードに関連した安全特性を提供する。所望であれば、電源投入手順時に暗号化キーの処理を行うことができる。しかし、好ましい実施例では、スマートカードの機能を擬似するためにアプリケーションプログラムが安全サービスを要求するまで、この処理は実行されない。

第2図に本発明の好ましい実施例の実行時間処理を示している。段階20において、遠隔サーバのような安全コンピュータシステム又はネットワークにアクセスする必要のあるアプリケーションプログラムが、本発明の安全サービスルーチンを呼出す。次に段階21において、安全サービスルーチンがソフトウェアシステム管理割込（SMI）を呼出す。SMIはInte

l x86アーキテクチャにおける最高レベルの割込モードであり、その他の割込みによる割込ができないようになっている。SMIはシステムプロセッサをSMMに初期化する。プロセッサがSMMになると、段階22でソフトウェアSMIハンドラが安全機能を呼出す。段階23において安全機能が、SMRAMに記憶された暗号化キー及びプログラムにアクセスする。プロセッサがSMM内の要求された安全処理を実行する。この処理は、文書の暗号化/暗号解読、パスワード妥当性検査用の安全キー処理、ユーザ認証等を含むことができる。処理が完了すると、段階24においてプロセッサがSMMを実行し、段階25において通常システムオペレーションが継続する。段階２５で、適切な暗号化情報が提供される。処理全体は、プロセッサ上で既に実行されているアプリケーションには不可視である安全モード及び安全メモリ範囲で起こる。また、物理スマートカードの不在によってアプリケーションプログラムが影響されることはない。

本発明をさらに説明するために、本発明を利用するべく改良を加えた、一般の仮想スマートカードの使用について考える。ユーザは、ソフトウェアアプリケーションプログラムを使って遠隔サーバにログオンすることができる。ユーザにアクセスを許容する前に、遠隔サーバはchallengeを発行し、適切なresponseを期待する。遠隔サーバからchallengeを受信すると、ユーザは、responseを遠隔サーバに返却するために計算するべく、応答計算機プログラムを呼出す。応答計算機プログラムは、ソフトSMIを介して、challengeストリングをメインシステムプロセッサに伝達する（段階20、21）。この時点でSMMに換わり、全体のオペレーティングシステムとそのアプリケーションが「スリープモード」に入る。次に、暗号化キーとchallengeに基づいてresponseを計算するオペレーションが実行される（段階22、23）。responseが応答計算機プログラムに伝達され、オペレーティングシステムが再開する（団塊25）。応答計算機プログラムがresponseを遠隔サーバに送信し、認証処理が完了する。オペレーティングシステムは応答計算処理に全く気付いていないため、応答計算処理に干渉することができない。

上述した第1図、第2図の説明では、暗号化キーとプログラムは、ブート時間中は安全メモリ内にロードされ、後のシステムオペレーションに処理されると仮定されている。また、ロードが安全モード、すなわちSMMで行われる限り、暗号化キーとプログラムを、既にシステムがブートした後にロードしてもよい。また、暗号化キーとプログラムを別々の時間にロードすることもできる。この実行は、複数のユーザが使用し、従って複数のキーを有するコンピュータにとって有効である。ここで、複数のキーは全て完全に同一の処理アルゴリズムに依存している。各ユーザが安全サービスを要求するため、アルゴリズムはブート時間に、キーは後でロードする。当業者には、ローディングと処理が安全メモリを使って安全プロセッサモードで実行される限り、暗号化キーとプログラムのローディング及び処理の、本発明の範囲内にける多くの変更が可能であることが明白であろう。

第1図において、ユーザは電源投入手順中にPINを入力し、安全暗号化キーのロックを解く。オペレーティングシステムのローディング前にPINの入力を要求することにより、その他のプログラムによってPINに割込が入ることがない。また、安全の利点は減少するが、PINを要求せずに本発明を実行することが可能である。また所望であれば、オペレーティングシステムをロードした後でも、処理の様々な段階においてPINを要求することができる。例えば、特定のアプリケーションにおいて、システムがブートした後にトークンを使用することが可能である。この場合、入力したPINが、ソフトSMIを介して、暗号化データ及びプログラムと共にSMM処理へ伝達される。暗号化キーの処理の最中はオペレーティングシステムは「スリープモード」にされる。

第3図に、電源投入時に使用するPIN検証方法の好ましい実施例（段階4）を示す。段階30でPIN検証処理が始まり、トークン上に記憶した暗号化したキーを読出す。段階32で、ユーザはPINの入力を促される。次に、段階33において、キーの解読のためにPINが使用される。段階34で、キーのダイジェストを生成するためにハッシュ機能が使用される。ハッシュ機能は、キーの固定の長さの表面を出力として生成する、キーレスの数学的機能である。ハッシュ機能には例えば、MDS、SHA、RIPEMD-160がある。段階34でハッシュ機能によって生成されたダイジェストは、システムBIOSに記憶されたダイジェストのコピーと比較さ

れる。この比較の結果が段階36に戻される。ダイジェストが一致した場合、第1図の段階5においてPINが検証される。PINが検証されたら、次にトークンの内容をSMRAM内にロードすることができる。従って、トークンが盗難にあった場合でも、PIN検証段階がシステム安全の層を追加して非許可のアクセスを阻止する。

第4図は、既にシステムがブートした後に安全キーがロードされた本発明の例を示す。必要な暗号化プログラムは、ブート手順の間に既にSMRAM内にロードされていると考えられる。上述したように、この実施例は、同一の暗号化アルゴリズムが異なる安全キーを有する異なるユーザによって使用された状況においても有効である。段階41において、ユーザのアプリケーションプログラムがユーザに対してPINの入力を要求し、SMIを呼出す。段階42において、プロセッサがSMMを入力し、ユーザはトークン（脱着可能な記憶装置）の挿入を要求される。段階43において、トークンに記憶された暗号化キーがSMRAMにロードされ、また段階44において、PINを使って暗号化されたキーの解読が行われる。段階45で、ダイジェストを生成するためにハッシュ機能を使用してキーが処理される。段階46で、ハッシュされたダイジェストとBIOSに記憶されたダイジェストとが比較される。ダイジェストが一致した場合、段階47においてPINが検証され、段階48においてキーがSMRAMにロードされる。PINが検証されないと、キーはSMRAMにロードされない。段階49において、システムの安全性を確実にするためにユーザはトークンを除去するよう促され、次に段階50において、プロセッサがSMMを出る。これで、本発明は、現在のユーザのアプリケーションが必要とするあらゆる安全サービスの要求を処理する準備ができた。また、所望であれば、暗号化処理を段階48と段階49の間で迅速に実行することもできる。

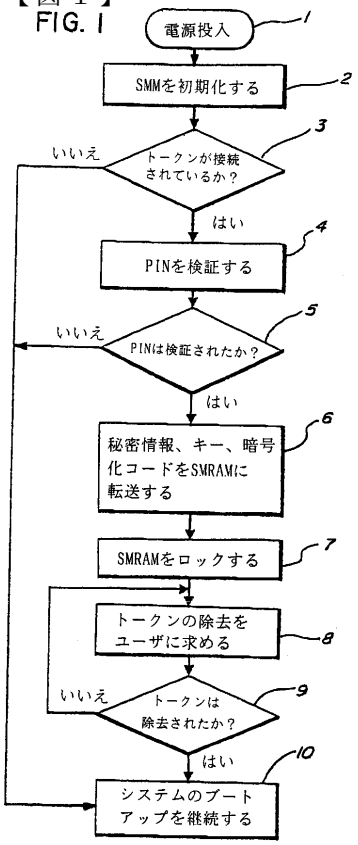
第5図は本発明による装置のブロック図である。コンピュータシステム60は、他の割込によって割込まれない安全処理モードを備えた中央処理ユニット（CPU）64を設けている。CPU 64は割込ライン641を備えており、この割込ライン641上で、安全モード割込がCPU 64を安全モードに初期化する。安全メモリ66はCPU 64と接続しており、CPU 64が安全処理モードにある場合に、CPU 64のみが安全メモリ66にアクセスできる。メインシステムメモリ68もCPU 64と接続しており、オペレーティングシステム及びアプリケーションプログラムによって使用される。システムBIOS 62はPINのハッシュされたダイジェスト621を記憶する。このダイジェストは、キーボード70を介してユーザが入力したPINから算出されたダイジェストと比較されている。トークンリーダ72は、トークン74に記憶された暗号化されたキー、データ及びプログラムを読出す。トークンリーダ72は、トークン74の存在又は不在を検出するためのセンサを備えている。本発明の装置のオペレーションは、本発明の方法と、付随するフローチャートに関連して上述した通りである。

本発明は、あらゆるタイプの暗号化キーの記憶及び処理に適用できることに留意すること。暗号化キーは、対称的キーシステムにおける暗号化キー、又は、公開キー暗号化システムで使用されるようなプライベートキーであってよい。本発明を利用すれば、実際に物理スマートカードを採用する費用をかけることなく、スマートカードの安全処理機構が達成される。これは、暗号化キーを処理及び記憶するソフトウェアのみを使用するその他のあらゆるアプリケーションと同様に、仮想スマートカードの安全性を向上するために使用することができる。

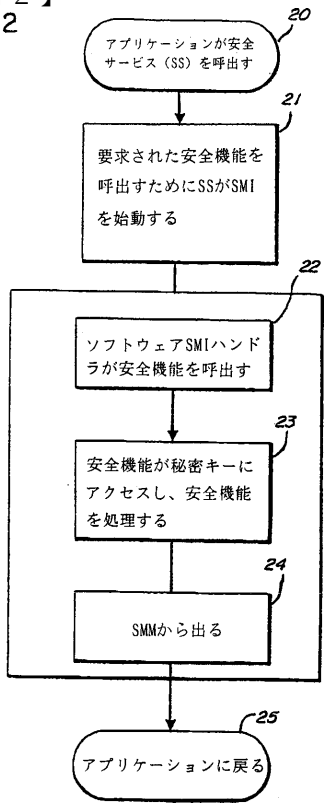
本明細書中では、Intel x86コンパチブルアーキテクチャ（80386以降）を参照して好ましい実施例を説明したが、本発明は、他の割込によって割込まれることのない安全処理モードと、プロセッサが安全処理モードにある間にのみアクセスできる安全メモリ範囲とを備えたあらゆるプロセッサアーキテクチャに適用することができる。最もよく知られたプロセッサは、第1の要求を満たすことが可能な最高レベルの割込レベルを備えており、また、メモリの要求はプロセッサ外部のチップセット又は論理の適切な設計で満たすことができる。

当業者には、本発明の範囲及び精神を逸脱しない限り、上述した好ましい実施例に様々な改良及び変更が可能なことがわかるであろう。従って、付属の請求の範囲内において、本発明を、ここで特定した説明以外の方法で実施することが可能であることが理解されるべきである。

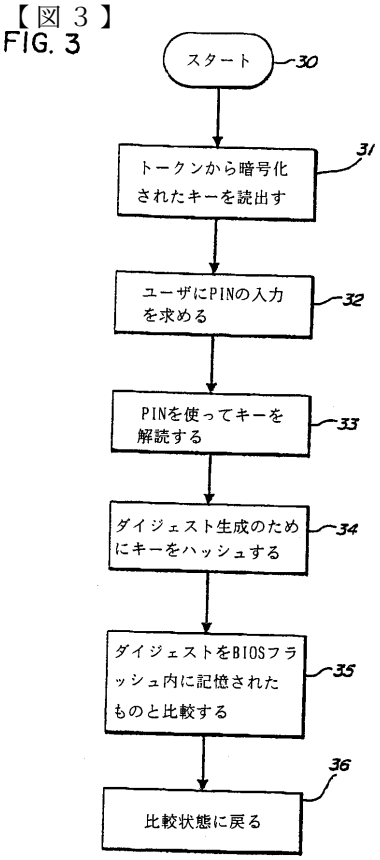
【図１】
FIG. 1



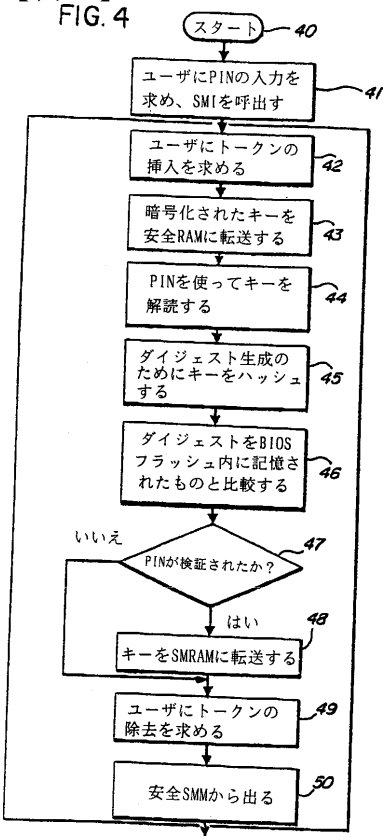
【図２】
FIG. 2



【図３】
FIG. 3

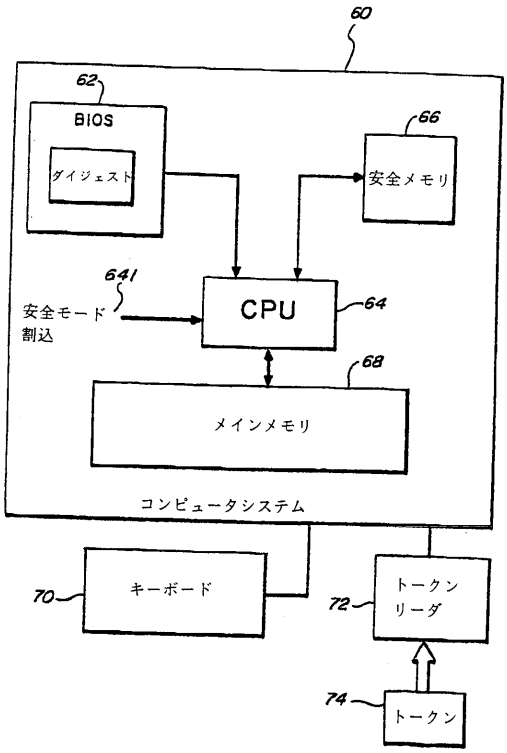


【図４】
FIG. 4



【図５】

FIG. 5


60
62
BIOS
ダイジェスト
66
安全メモリ
641
安全モード
割込
CPU
64
68
メインメモリ
コンピュータシステム
70
キーボード
72
トークン
リーダ
74
トークン

フロントページの続き

(72)発明者　ヴ，ソン，トラン
アメリカ合衆国　９２６４９　カリフォルニア州，ハンティングトン　ビーチ，マクファーデン　アベニュー　５１７１
(72)発明者　ファン，クァン
アメリカ合衆国　９２７８２　カリフォルニア州，ツサン，サラトガ　ドライブ　１３２８１

審査官　鈴木　匡明

(56)参考文献　米国特許第０５６１５２６３（ＵＳ，Ａ）
国際公開第９５／０２４６９６（WO，Ａ１）
英国特許出願公開第０２２５９１６６（ＧＢ，Ａ）
国際公開第９３／０１７３８８（WO，Ａ１）
特開平１０－２２２３６５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
G06F　1/00
G06F　9/06