(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2009-526472
(P2009-526472A)
(43)公表日　平成21年7月16日(2009.7.16)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601C	5B017
H04L 9/10	(2006.01)	H04L	9/00	621A	5J104
G06F 21/24	(2006.01)	H04L	9/00	601E	
		G06F	12/14	540P	
		G06F	12/14	540A	

審査請求 未請求　予備審査請求 未請求　（全 18 頁）

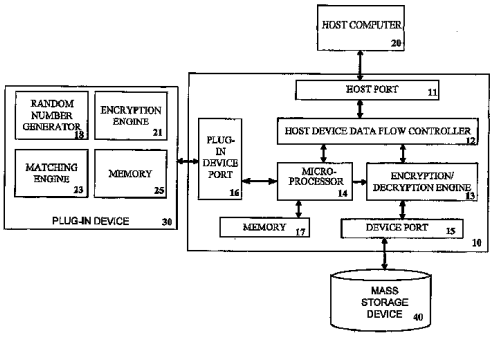
(21)出願番号　特願2008-554211 (P2008-554211)
(86)(22)出願日　平成18年2月9日(2006.2.9)
(85)翻訳文提出日　平成20年9月22日(2008.9.22)
(86)国際出願番号　PCT/US2006/004800
(87)国際公開番号　WO2007/094763
(87)国際公開日　平成19年8月23日(2007.8.23)

(71)出願人　591225523
アトメル・コーポレイション
ＡＴＭＥＬ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国、９５１３１　カリフォルニア州、サン・ノゼ、オーチャード・パークウェイ、２３２５
(74)代理人　100089266
弁理士　大島　陽一
(72)発明者　カオ、シャオビン
中華人民共和国２０００３１上海・フェンヤンロード　ナンバー　１３８
(72)発明者　リ、チ
中華人民共和国２０００３１上海・フェンヤンロード　ナンバー　１３８

最終頁に続く

(54)【発明の名称】実時間鍵生成を含むデータ・セキュリティ

(57)【要約】
【課題】　よりロバストなデータ保護方法を提供する。
【解決手段】　データ・セキュリティを与える方法を提供する。セキュリティ・デバイス（１０）及びプラグイン・デバイス（３０）は、データの暗号化及び復号を可能にするように連動して働く。シークレットは、セキュリティ・デバイス（１０）またはプラグイン・デバイス（３０）のいずれか一方によって格納される。シークレットは鍵を作成することが求められるが、鍵はシークレットのみから作成されることができない。許可されていないデバイスまたはユーザは、それによって鍵へのアクセスが阻止される。
【選択図】　図２



【特許請求の範囲】
【請求項１】
セキュリティ・デバイスにおいてデータ・セキュリティを与える方法であって、
対応する記憶装置へ／からのデータの暗号化または復号を制御するようなセキュリティ・デバイスに、プラグイン・デバイスを結合するステップと、
データ暗号化または復号動作が必要とされるとき、プラグイン・デバイスからシークレットを検索するステップと、
前記シークレットからホスト・シードを回復するステップと、
前記ホスト・シードから、データの暗号化または復号に使われる鍵を生成するステップとを含むことを特徴とする方法。
【請求項２】
前記鍵を用いてデータを暗号化または復号するステップを更に含むことを特徴とする請求項１の方法。
【請求項３】
前記シークレットからホスト・シードを回復する前記ステップが、乱数を用いて混合シードを逆スクランブルするステップを含むことを特徴とする請求項１の方法。
【請求項４】
前記プラグイン・デバイスから前記乱数を受信するステップを更に含むことを特徴とする請求項３の方法。
【請求項５】
前記ホスト・シードから鍵を生成する前記ステップが、前記ホスト・シード及びデバイス・シードから前記鍵を生成するステップを含むことを特徴とする請求項１の方法。
【請求項６】
前記方法が、前記シークレットの検索の前に前記セキュリティ・デバイスを認証するステップを更に含むことを特徴とする請求項１の方法。
【請求項７】
前記認証するステップが、
乱数を暗号化して、暗号化された乱数を生成するステップと、
前記暗号化された乱数を前記プラグイン・デバイスに送信するステップと、
前記プラグイン・デバイスから成功メッセージを受信ステップとを含むことを特徴とする請求項６の方法。
【請求項８】
前記プラグイン・デバイスを首尾よく認証するステップが、ホスト・シードから鍵を生成する前記ステップを実行するように要求されることを特徴とする請求項６の方法。
【請求項９】
前記プラグイン・デバイスがセキュリティ・デバイスから切断されていることを検出するステップと、
前記切断の検出に応じて、前記鍵をメモリから削除するかあるいは暗号化または復号機能をディセーブルするステップとを更に含むことを特徴とする請求項１の方法。
【請求項１０】
データ・セキュリティを与える方法であって、
安全な暗号化または復号動作の促進の要求を受信するステップと、
ランダムに生成される数を提供するステップと、
ホスト・シード及び前記ランダムに生成される数から生成されるシークレットを受信するステップと、
前記シークレットを実行時まで記憶するステップとを含むことを特徴とする方法。
【請求項１１】
前記混合シードのリクエスタを認証するステップと、
前記リクエスタを首尾よく認証した後に前記リクエスタに前記混合シードを提供するステップを更に含むことを特徴とする請求項１０の方法。

【請求項１２】
前記リクエスタを認証するステップが、
ランダムに生成される数を暗号化して、ローカルで暗号化されたランダムに生成される数を生成するステップと、
前記ローカルで暗号化されたランダムに生成される数を、前記リクエスタから受信した暗号化されたランダムに生成される数と比較するステップと、
一致があるか否かを判定し、もしあれば、前記シークレットを前記リクエスタに提供するステップを含むことを特徴とする請求項１１の方法。
【請求項１３】
前記リクエスタから受信した一連のデータと記憶されている一連のデータとが一致するか否かを判定するステップを含む、妥当性検査ステップを実行するステップを更に含むことを特徴とする請求項１１の方法。
【請求項１４】
前記提供するステップで提供される前記ランダムに生成される数が、ローカルで暗号化されたランダムに生成される数を生成するように暗号化された前記ランダムに生成される数であることを特徴とする請求項１１の方法。
【請求項１５】
データ・セキュリティを与えるためのプラグイン・デバイスであって、
乱数を生成するための乱数ジェネレータと、
前記乱数を暗号化するための暗号化エンジンと、
前記暗号化された乱数を、受信された暗号化された乱数と比較するためのマッチング・エンジンと、
両乱数が一致したと前記マッチング・エンジンが判断したらセキュリティ・デバイスと共有されるシークレットを格納するためのメモリとを含むことを特徴とするプラグイン・デバイス。
【請求項１６】
前記マッチング・エンジンが、前記暗号化エンジンによって暗号化された数と受信された暗号化された数とが一致するか否かを判定するように構成されていることを特徴とする請求項１５のプラグイン・デバイス。
【請求項１７】
前記メモリが、前記乱数ジェネレータによって生成された乱数と組み合わされている混合シードを格納するように構成されていることを特徴とする請求項１５のプラグイン・デバイス。
【請求項１８】
前記メモリが、前記乱数ジェネレータによって生成された乱数を暗号化するために前記暗号化エンジンによって用いられる認証鍵を格納するように構成され、
前記マッチング・エンジンが、前記暗号化鍵を用いて暗号化された乱数と受信された暗号化された乱数とが一致するか否かを判定することを特徴とする請求項１５のプラグイン・デバイス。
【請求項１９】
前記プラグイン・デバイスがスマートカードであることを特徴とする請求項１５のプラグイン・デバイス。
【請求項２０】
セキュリティ・デバイスであって、
ホスト・シードを受信するためにホストコンピュータに接続するための手段と、
デバイス・シードまたは乱数のうち少なくとも一方を格納するように構成されているメモリと、
前記ホスト鍵をシークレット内に隠し、前記シークレットから前記ホスト・シードを抽出し、前記ホスト・シードから鍵を生成するが、但しそれは前記シークレットを格納する認証されたデバイスに結合されているときのみであるように構成されたプロセッサとを含

むことを特徴とするセキュリティ・デバイス。
【請求項２１】
前記セキュリティ・デバイスと前記認証されたデバイス間での前記シークレットの通信を可能にするようにプラグイン・デバイスに接続するための手段を更に含むことを特徴とする請求項２０のセキュリティ・デバイス。
【請求項２２】
データ記憶装置に接続するための手段を更に含み、前記データ記憶装置が前記鍵を用いて暗号化されたデータを格納することを特徴とする請求項２０のセキュリティ・デバイス。
【請求項２３】
データを保護するためのシステムであって、
ホストコンピュータと、
セキュリティ・デバイスとを含み、前記セキュリティ・デバイスが、
ホスト・シードを受信するために前記ホストコンピュータに接続するための手段と、
デバイス・シードまたは乱数のうち少なくとも一方を格納するように構成されているメモリと、
前記ホスト鍵をシークレット内に隠し、前記シークレットから前記ホスト・シードを抽出し、前記ホスト・シードから鍵を生成するが、但しそれは前記シークレットを格納する認証可能デバイスに結合されているときのみであるように構成されたプロセッサとを含み、
前記システムが、更に
前記乱数を生成し、前記シークレットを格納するように構成された認証可能デバイスと、
暗号化されたデータを格納するためのデータ記憶装置とを含むことを特徴とするシステム。
【請求項２４】
前記セキュリティ・デバイスが、前記データ記憶装置に接続するための手段を更に含むことを特徴とする請求項２３のシステム。
【請求項２５】
前記プロセッサが、前記ホスト・シード及び前記デバイス・シードからの鍵を生成することを特徴とする請求項２３のシステム。
【請求項２６】
コンピュータ読み取り可能な媒体であって、プロセッサによって実行されるとき、
対応する記憶装置へ／からのデータの暗号化または復号を制御するようなセキュリティ・デバイスに、プラグイン・デバイスを結合する動作と、
データ暗号化または復号動作が必要とされるとき、プラグイン・デバイスからシークレットを検索する動作と、
前記シークレットからホスト・シードを回復する動作と、
前記ホスト・シードから、データの暗号化または復号に用いられる鍵を生成する動作とを前記プロセッサに実行させるような命令を含むコンピュータ読み取り可能な媒体。
【請求項２７】
鍵を用いて前記前記データを暗号化または復号する動作を前記プロセッサに実行させるための命令を更に含むことを特徴とする請求項２６のコンピュータ読み取り可能な媒体。
【請求項２８】
前記シークレットからホスト・シードを回復する前記動作が、乱数を用いて混合シードを逆スクランブルする動作を含むことを特徴とする請求項２６のコンピュータ読み取り可能な媒体。
【請求項２９】
前記プラグイン・デバイスから前記乱数を受信する動作を前記プロセッサに実行させるための命令を更に含むことを特徴とする請求項２６のコンピュータ読み取り可能な媒体。

【請求項３０】
前記ホスト・シードから鍵を生成する動作が、前記ホスト・シード及びデバイス・シードから前記鍵を生成する動作を含むことを特徴とする請求項２６のコンピュータ読み取り可能な媒体。
【請求項３１】
前記方法が、前記シークレットの検索の前に前記セキュリティ・デバイスを認証する動作を更に含むことを特徴とする請求項２６のコンピュータ読み取り可能な媒体。
【請求項３２】
前記認証する動作が、
乱数を暗号化して、暗号化された乱数を生成する動作と、
前記暗号化された乱数を前記プラグイン・デバイスに送信する動作と、
前記プラグイン・デバイスから成功メッセージを受信する動作とを含むことを特徴とする請求項３１のコンピュータ読み取り可能な媒体。
【請求項３３】
前記プラグイン・デバイスを首尾よく認証する動作が、前記ホスト・シードから鍵を生成する前記動作を実行するように要求されることを特徴とする請求項３１のコンピュータ読み取り可能な媒体。
【請求項３４】
前記プラグイン・デバイスがセキュリティ・デバイスから切断されていることを検出する動作と、
前記切断の検出に応じて、前記鍵をメモリから削除するかあるいは暗号化または復号機能をディセーブルする動作とを前記プロセッサに実行させるような命令を更に含むことを特徴とする請求項２６のコンピュータ読み取り可能な媒体。
【請求項３５】
コンピュータ読み取り可能な媒体であって、プロセッサによって実行されるとき、
安全な暗号化または復号動作の促進の要求を受信する動作と、
ランダムに生成される数を提供する動作と、
ホスト・シード及び前記ランダムに生成される数から生成されるシークレットを受信する動作と、
前記シークレットを実行時まで記憶する動作とを前記プロセッサに実行させるような命令を含むコンピュータ読み取り可能な媒体。
【請求項３６】
前記混合シードのリクエスタを認証する動作と、
前記リクエスタを首尾よく認証した後に前記リクエスタに前記混合シードを提供する動作とを前記プロセッサに実行させるような命令を更に含むことを特徴とする請求項３６のコンピュータ読み取り可能な媒体。
【請求項３７】
前記リクエスタを認証する前記動作が、
前記ランダムに生成される数を暗号化して、ローカルで暗号化されたランダムに生成される数を生成する動作と、
前記ローカルで暗号化されたランダムに生成される数を、前記リクエスタから受信した暗号化されたランダムに生成される数と比較する動作と、
一致があるか否かを判定し、もしあれば、前記シークレットを前記リクエスタに提供する動作とを含むことを特徴とする請求項３６のコンピュータ読み取り可能な媒体。
【請求項３８】
前記リクエスタから受信した一連のデータと記憶されている一連のデータとが一致するか否かを判定するステップを含む、妥当性検査ステップを実行する動作を前記プロセッサに実行させるような命令を更に含むことを特徴とする請求項３６のコンピュータ読み取り可能な媒体。
【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、データ・セキュリティに関する。
【背景技術】
【０００２】
今日のデジタル世界において、情報は以前より容易にアクセス可能になっている。商取引は、益々デジタル通信に依存している。しかしながら、デジタル通信技術の普及と使い勝手の良さには、それと引き換えに相当な代償が払われている。すなわち、情報の安全性を脅かす増大した脅威に曝されているのである。情報の記憶、検索及び転送は、従来のデジタル通信技術によって既に容易なものとなっている。必要なのは、価値ある情報を保護するための同様に容易な手段である。
【発明の開示】
【発明が解決しようとする課題】
【０００３】
図１を参照すると、従来のホストコンピュータ２０が、データを格納するために大容量記憶装置４０と通信している。多くの場合、ホストコンピュータ２０のユーザが望むのは、大容量記憶装置４０に格納されたデータを、許可されたユーザしかデータにアクセスできないように、安全に保つことである。ユーザは、多数の従来のデータ保護方法の中から選択できる。例えば、ユーザは、データへのアクセスをパスワード保護することができる。しかしながら、もしもハードディスクが大容量記憶装置４０から取り外されて非保護のコンピュータにインストールされれば、パスワード保護は失われるかもしれず、データは公然と曝されかねない。別の従来のデータ保護方法は、ソフトウエアまたはハードウエア（または両者の組合せ）暗号化技術を用いたものである。ソフトウエア暗号化に関連する不利点には、メモリ資源要求と非実時間処理とが含まれる。一部のハードウエア暗号化技術は、ハードウエア・デバイス内に、例えばハードディスク、フレキシブルディスク、ＥＥＰＲＯＭ、フラッシュまたは記録可能な光ディスクなどの記憶媒体上に、鍵を格納する必要がある。しかしながら、既知のハードウエア暗号化技術は、鍵がハードウエア・デバイスに格納されるかあるいはハードウエア・デバイスからロードされるとき、鍵を保護しない。ハードウエア・デバイスはまた、スパイ・プログラムに影響され易い。従って、重要なデータを保護するためのよりロバストな方法が望ましい。
【課題を解決するための手段】
【０００４】
一部の実施形態において、セキュリティ・デバイスにおいてデータ・セキュリティ（データの安全保護）を与える方法が提供される。この方法は、セキュリティ・デバイスにプラグイン・デバイスを結合するステップを含み、セキュリティ・デバイスは、対応する記憶装置へ／からのデータの暗号化または復号を制御する。データ暗号化または復号動作が必要とされるとき、プラグイン・デバイスからシークレットが検索される。シークレットからホスト・シードが回復される。ホスト・シードから、データの暗号化または復号に使われる鍵が生成される。
【０００５】
一部の実施形態において、データ・セキュリティを与える方法は、安全な暗号化または復号動作の促進の要求を受信するステップと、ランダムに生成される数を提供するステップと、ホスト・シード及びランダムに生成される数から生成されるシークレットを受信するステップと、シークレットを実行時まで記憶するステップとを含む。
【０００６】
一部の実施形態において、データ・セキュリティを与えるためのプラグイン・デバイスは、乱数を生成するための乱数ジェネレータと、乱数を暗号化するための暗号化エンジンと、その暗号化された乱数を、受信された暗号化された乱数と比較するためのマッチング・エンジンと、両乱数が一致したとマッチング・エンジンが判断したらセキュリティ・デバイスと共有されるシークレットを格納するためのメモリとを含む。

【０００７】
一部の実施形態において、セキュリティ・デバイスは、ホスト・シードを受信するためにホストコンピュータに接続するための手段と、デバイス・シードまたは乱数のうち少なくとも一方を格納するように構成されているメモリと、ホスト鍵をシークレット内に隠し、シークレットからホスト・シードを抽出し、ホスト・シードから鍵を生成するが、但しそれはシークレットを格納する認証されたデバイスに結合されているときのみであるように構成されたプロセッサとを含む。
【０００８】
一部の実施形態において、データを保護するためのシステムは、ホストコンピュータと、セキュリティ・デバイスと、認証可能デバイスと、データ記憶装置とを含む。セキュリティ・デバイスは、ホスト・シードを受信するためにホストコンピュータに接続するための手段と、デバイス・シードまたは乱数のうち少なくとも一方を格納するように構成されているメモリと、ホスト鍵をシークレット内に隠し、シークレットからホスト・シードを抽出し、ホスト・シードから鍵を生成するが、但しそれはシークレットを格納する認証可能デバイスに結合されているときのみであるように構成されたプロセッサとを含む。認証可能デバイスは、乱数を生成し、シークレットを格納するように構成されている。データ記憶装置は、暗号化されたデータを格納する。
【０００９】
本明細書に記載されている方法及びデバイスは、次に挙げる利点のうち１つ若しくは複数を提供するかあるいは１つも提供しないことがある。プラグイン・デバイスはデータセキュリティ・デバイスと共に一緒に、ロバストなデータ・セキュリティの方法を提供することができる。混合シード（mixed seed）などの秘密情報が、プラグイン・デバイス上に格納されることができる。混合シード及び／またはプラグイン・デバイスは、重要なデータの暗号化または復号のための鍵を生成するために必要とされることがある。しかしながら、プラグイン・デバイスがあっても、それ単独では、鍵を生成するのに不十分である。暗号化／復号鍵を作成するために、セキュリティ・デバイス上に格納される情報も必要とされる。鍵を生成するためにプラグイン・デバイス及びセキュリティ・デバイスの両方が必要とされるので、セキュリティ・デバイスがあっても、それ単独では、暗号化／復号鍵を生成するのにも不十分である。プラグイン・デバイスまたはセキュリティ・デバイスのいずれかが情報漏洩されても、鍵は漏洩されない。
【００１０】
本発明の１若しくは複数の実施形態の詳細は、添付の図面及び以下の説明に記載されている。本発明の他の機能、目的及び利点は、説明及び図面から、そして特許請求の範囲から、明らかになるであろう。
【発明を実施するための最良の形態】
【００１１】
図２を参照すると、データセキュリティ・デバイスとプラグイン・デバイスとが、共同で、記憶装置に格納されたデータを保護することができる。データセキュリティ・デバイス１０が、ホストデバイス（例えばホストコンピュータ２０）、プラグイン・デバイス３０及び記憶装置（例えば大容量記憶装置４０）に、様々な通信媒体を介して接続されている。通信媒体は、それぞれのデバイス間に信号経路形成し、電気的形式、光学的形式、ＲＦまたは他の通信媒体の形をとることができる。
【００１２】
ホストデバイスは、コンピュータの形であることができ、コンピュータとして示されている。記憶装置は、大容量記憶装置の形であることができ、大容量記憶装置として示されている。ホストコンピュータ２０及び大容量記憶装置４０が参照されているが、この参照は単なる例示に過ぎない。セキュリティ・デバイス１０及びプラグイン・デバイス３０は、他のホストデバイス（例えば、パーソナルコンピュータ、ラップトップコンピュータ、ＰＤＡ、アクセスポイント、携帯用電子機器、ゲーム機、セットトップボックス、または他の情報処理装置）及び他の記憶装置（例えば、ハードドライブ、光学式ドライブ、フラ

ッシュドライブなど）と対応付けられる場合がある。同様に、個々の構成要素が参照されているが、ホストデバイス、プラグイン・デバイス、セキュリティ・デバイス及び記憶装置のうちの１つ若しくは複数は、１つにまとめられることができる。例えば、一実施形態において、セキュリティ・デバイス１０は、１若しくは複数のホストデバイスに結合されるように構成されたディスクキーデバイス（例えばフラッシュまたはディスクＵＳＢドライブ）内に大容量記憶装置４０と一体化されることができる。

【００１３】

データセキュリティ・デバイス

【００１４】

データセキュリティ・デバイス１０は、記憶装置に格納される（及び／または記憶装置から検索される）データの暗号化及び復号に用いるための１若しくは複数の鍵を生成するべく、ホストデバイス及びプラグイン・デバイスと共に働くように動作する。然るべく、データセキュリティ・デバイス１０は、３つの主要なインタフェース、即ち、ホストインタフェース（例えば、ホストコンピュータ２０と通信するためのホストポート１１）と、プラグイン・デバイスインタフェース（例えば、プラグイン・デバイス・ポート１６）と、記憶装置インタフェース（例えば、大容量記憶装置４０と通信するためのデバイスポート１５）とを含む。図示されている特定のインプリメンテーションにおいて、データセキュリティ・デバイス１０は、プラグイン・デバイス３０に直接アクセスするためのプラグイン・デバイス・ポート１６を含む。データセキュリティ・デバイス１０とプラグイン・デバイス間、ホストデバイスと記憶装置間の他の通信構成も可能である。詳細に後述するように、プラグイン・デバイス３０は、大容量記憶装置４０に格納されたデータを暗号化または復号するために用いられる鍵を生成するために必要なシークレット情報を格納及び検索する。一実施形態において、データセキュリティ・デバイス１０はまた、ホストデバイス・データフロー・コントローラ１２と、暗号化／復号エンジン１３とを含み、前者はホストコンピュータ２０へ行くかまたはホストコンピュータ２０から来るデータを管理し、後者は大容量記憶装置４０へ行くデータを暗号化するかあるいは大容量記憶装置４０、マイクロプロセッサ１４及びメモリ１７から来るデータを復号するためのものである。

【００１５】

ホストポート１１は、ホストコンピュータ２０及びホストデバイス・データフロー・コントローラ１２と通信している。ホストポート１１は、ホストコンピュータ２０からコマンド及びデータを受信し、そのコマンド及びデータを処理するためにホストデバイス・データフロー・コントローラ１２へ伝達する。ホストポート１１はまた、大容量記憶装置４０からホストコンピュータ２０へ、返却データ及び実行されたコマンドの状態を伝達する。一実施形態において、ホストコンピュータ２０及びセキュリティ・デバイス１０は、任意の適切なタイプのホスト側バス、例えば、ＰＣＩ、ＰＣＩｅ（PCI express）、ＵＳＢ、１３９４、ＡＴＡ、シリアルＡＴＡ、ＳＣＳＩ、またはファイバ・チャネルなどと接続されている。

【００１６】

ホストデバイス・データフロー・コントローラ１２は、ホストポート１１、暗号化／復号エンジン１３及びマイクロプロセッサ１４と通信している。ホストデバイス・データフロー・コントローラ１２は、ホストポート１１からコマンド及びデータを受信し、そのコマンド及びデータを２つのカテゴリーで処理する。第１のカテゴリーは、大容量記憶装置４０にアクセスするためのコマンドを含む。第２のカテゴリーは、鍵管理コマンドを含む。他のコマンドカテゴリーも可能である。ホストデバイス・データフロー・コントローラ１２は、大容量記憶装置４０にアクセスするためのコマンド及び対応するデータを暗号化／復号エンジン１３へ伝達する。ホストデバイス・データフロー・コントローラ１２は、鍵管理コマンド及び対応するデータをマイクロプロセッサ１４へ伝達する。ホストデバイス・データフロー・コントローラ１２はまた、暗号化／復号エンジン１３及びマイクロプロセッサ１４から、返された状態情報及びデータを受信し、それらを必要に応じてホストポート１１を用いてホストコンピュータに提供する。

【００１７】
暗号化／復号エンジン１３は、ホストデバイス・データフロー・コントローラ１２及びマイクロプロセッサ１４と通信している。暗号化／復号エンジン１３は、ホストコンピュータ２０から大容量記憶装置４０へ移動するデータを暗号化し、大容量記憶装置４０からホストコンピュータ２０へ移動するデータを復号する。一実施形態において、暗号化／復号エンジン１３は、コマンド及び対応する返された状態情報を処理しない（即ち、情報を必要に応じて何も変えずにそのまま通過させることができる）。詳細に後述するように、マイクロプロセッサ１４は、暗号化／復号エンジン１３によってデータを暗号化／復号するために用いられる鍵を生成する。暗号化／復号エンジン１３は、例えばＡＥＳ及びＤＥＳなどの公開されかつベリファイ（検証）されたアルゴリズムから選択される暗号化／復号アルゴリズム、または他の適切なアルゴリズムを用いることができる。

【００１８】
マイクロプロセッサ１４は、ホストデバイス・データフロー・コントローラ１２、暗号化／復号エンジン１３、プラグイン・デバイス・ポート１６及びメモリ１７と通信している。マイクロプロセッサが参照されているが、マイクロコントローラまたは他のコントローラを含む他の処理装置も可能である。一実施形態において、マイクロプロセッサ１４は、データセキュリティ・デバイス１０の種々の操作処理を制御するが、そのような処理には、ホストコンピュータ２０からの（例えば、データの記憶または検索あるいはホスト・シードの処理の）要求へのレスポンスの送信、プラグイン・デバイス３０へのデータの格納及びプラグイン・デバイス３０からのデータのローディングが含まれる。マイクロプロセッサ１４はまた、暗号化及び復号のための鍵の生成も制御する。

【００１９】
マイクロプロセッサ１４は、メモリ１７から命令を検索するかあるいはメモリ１７にデータを格納することができる。メモリ１７は、ランダムアクセスメモリ、読出し専用メモリ（ＥＰＲＯＭなどを含む）、フラッシュメモリなどを含む揮発性及び／または不揮発性メモリを含むことができる。

【００２０】
デバイスポート１５は、暗号化／復号エンジン１３及び大容量記憶装置４０と通信している。デバイスポート１５は、大容量記憶装置４０から報告されたコマンド状態及びデータを受信し、そのコマンド状態及びデータを暗号化／復号エンジン１３へ伝達する。デバイスポート１５はまた、逆方向に、暗号化／復号エンジン１３からコマンド及びデータを受信し、そのコマンド及びデータを大容量記憶装置４０へ伝達する。セキュリティ・デバイス１０を大容量記憶装置４０に接続するデバイス側バスは、ホスト側バスと同じタイプでも異なるタイプでもよい。いずれか一方のバスは、ベンダ固有バスとして画定されることもできる。

【００２１】
プラグイン・デバイス・ポート１６は、プラグイン・デバイス３０及びマイクロプロセッサ１４と通信している。プラグインポートが参照されているが、他の、プラグイン・デバイスと通信する手段も可能である。詳細に後述するように、プラグイン・デバイス３０は、別な方法で（すなわち、プラグイン接続によらないで）セキュリティ・デバイスに結合されることもある。従って、本明細書中の記載は単なる例に過ぎない。プラグイン・デバイス・ポート１６は、マイクロプロセッサ１４によって制御されることができ、プラグイン・デバイス３０への書き込み及びプラグイン・デバイス３０からの読出しなどのプラグイン・デバイス３０へのアクセスが可能になる。一部の実施形態において、データセキュリティ・デバイス１０は、ＩＳＯ－７８１６などの特定のプラグイン・デバイス規格に準拠するように構成されたインタフェースを有する。一実施形態において、プラグイン・デバイス・ポート１６は、セキュリティ・デバイス１０とプラグイン・デバイス３０の間で情報を伝送するための安全なチャネルを提供する。一部の実施形態において、データは、指定されたプラグイン・デバイス・データ転送プロトコルを用いてプラグイン・デバイス３０へ／から安全に転送される。プラグイン・デバイス３０とセキュリティ・デバイス

１０の間を移動するデータは、ＤＥＳ、ＡＥＳまたは３ＤＥＳなどによって暗号化されることもできる。プラグイン・デバイス３０は、物理的にセキュリティ・デバイス１０に極めて近接して配置されることができる。一部の実施形態において、プラグイン・デバイス３０は、セキュリティ・デバイス１０のレセプタクルに差し込まれる。

【００２２】

プラグイン・デバイス

【００２３】

一例として、セキュリティ・デバイス１０とのインタフェースをとり、大容量記憶装置に格納されたデータの暗号化及び／または復号を可能にするのに必要なシークレットを格納するデバイスとして、プラグイン・デバイスが参照されている。デバイスが他の手段によってセキュリティ・デバイス１０に結合されることができることは、当業者であれば分かるであろう。プラグイン・デバイスの特性は、セキュリティ・デバイスから取り外される（例えば通信的及び／または物理的に切断される）能力、認証ケイパビリティ及びシークレットを格納する能力を含む。用いられることができるプラグイン・デバイスの一例は、スマートカードである。ＵＳＢデバイス、チップカード、ＥＥＰＲＯＭ、フラッシュ、またはＩＣ（集積回路）カードを含む他のタイプのデバイスも可能である。一実施形態において、プラグイン・デバイス３０は、乱数ジェネレータ１８、暗号化エンジン２１、マッチング・エンジン２３及びメモリ２５を含む。

【００２４】

乱数ジェネレータ１８は、プラグイン・デバイス３０とセキュリティ・デバイス１０の間の認証プロトコルにおいて用いるための乱数または擬似乱数を生成するために用いられることができる。認証プロトコルについては、以下に詳細に述べる。

【００２５】

暗号化エンジン２１は、プラグイン・デバイスが作られる時に与えられる鍵（例えば認証鍵）を用いて乱数ジェネレータ１８によって生成される乱数を暗号化するために用いられることができる。暗号化エンジンの使用の詳細については、以下に述べる。

【００２６】

マッチング・エンジン２３は、認証プロトコルの一部として用いられ、プラグイン・デバイス３０により受信されるセキュリティ・デバイス１０からの数またはデータ列が、プラグイン・デバイス３０によって生成または格納される数またはデータ列と一致する（例えば、暗号化エンジン２１によって生成されるデータと一致する）か否かを判定することができる。マッチング・エンジン２３のプロセス及び認証プロトコルについては、以下に詳細に述べる。

【００２７】

上記した構成要素を含むシステムは、暗号化されたデータを格納しかつアクセスするために用いられる。安全な暗号化及び復号方法については、本明細書でさらに述べる。

【００２８】

図３を参照すると、データを安全に暗号化または復号するための方法が示されている。この方法は、安全な通信システムの様々な他の構成要素と通信する処理装置において実行されることができる。処理は、（例えばデータセキュリティ・デバイス１０によってホストコンピュータ２０から）ホスト・シードを受信することから始まる（ステップ１１０）。ホスト・シードからシークレットが生成される（例えば、セキュリティ・デバイス１０は、ホスト・シード及び乱数から混合シードを生成することができる）（ステップ１２０）。本明細書では、混合シードは、万一情報が漏洩した（セキュリティが侵害された）場合にホスト・シードを秘すために用いることができるようなホスト・シードから作成されるデータ構造を指す。混合シードを生成するための１つの方法は、ホスト・シードを混合要素（例えば乱数または擬似乱数）と混合するステップを含む。混合シードは、安全に記憶されることができ、ホスト・シードは必要な場合に逆演算を用いて（例えば混合要素を用いて）回復されることができる。混合シードを生成する詳細については、以下に詳細に述べる。シークレット（例えば混合シード）は、その後、個別の安全なデバイスに提供さ

れかつ格納される（例えばミックスシードは格納のためにプラグイン・デバイス３０に提供される）（ステップ１３０）。

【００２９】

個別の安全なデバイスは、必要に応じて切り離されることができる。結合されるときに（例えば、プラグイン・デバイス３０がセキュリティ・デバイス１０に結合されるときに）、認証プロセスが実行されることができる（例えば、セキュリティ・デバイス１０がプラグイン・デバイス３０を認証する）（ステップ１４０）。認証プロトコルについては、以下に詳細に述べる。実行時に（例えばデータの暗号化または復号が必要なときに）、シークレット（例えば混合シード）は検索されることができる（例えば、セキュリティ・デバイス１０は、混合シードをプラグイン・デバイス３０から呼び戻す）。シークレットは、暗号化／復号（Ｅ／Ｄ）鍵を生成するために用いられる（ステップ１６０）。Ｅ／Ｄ鍵の生成は、シークレットからのホスト・シードの回復と、Ｅ／Ｄ鍵を生成するためのホスト・シードのデバイス・シードとの混合または別な方法とを含むことができる。Ｅ／Ｄ鍵の生成については、以下に詳細に述べる。その後、Ｅ／Ｄ鍵は、データ（例えば、ホストコンピュータ２０と大容量記憶装置４０を移動するデータ）を暗号化及び復号するために（例えばセキュリティ・エンジン１０によって）用いられることができる（ステップ１７０）。記載されているプロセスは、セキュリティ・デバイスがオンザフライでかつプラグイン・デバイスの認証後にのみＥ／Ｄ鍵を生成できるようにする。一実施形態において、暗号化及び復号のために用いられるＥ／Ｄ鍵は、特定の暗号化または復号動作に必要とされる間だけ維持される。代わりに、Ｅ／Ｄ鍵は、プラグインカード３０がセキュリティ・デバイス１０に接続されている間だけ維持されることができる。ひとたびプラグイン・デバイス３０がセキュリティ・デバイス１０から切断されたら、Ｅ／Ｄ鍵は、メモリから消去されるか、暗号化／復号エンジン１２がディセーブルされるかのいずれかである。前述のステップの多くについて、本明細書でさらに述べる。前述のステップについて図２に示されている通信システムを参照しながら説明するが、とは言っても、当業者は、説明されている方法が他の別個のまたは統合されたシステムによって実行されることができることを理解されたい。

【００３０】

シークレットの生成

【００３１】

図４を参照すると、ホストデバイスから受信したホスト・シードを処理し、個別のデバイスに格納されるシークレットを生成する方法が示されている。このプロセスは、セキュリティ・デバイス１０が、シークレット（例えば混合シード）を、プラグイン・デバイス３０が格納するようにプラグイン・デバイス３０に発行するプロセスを含む。セキュリティ・デバイス１０は、プラグイン・デバイス３０がプラグイン・デバイス・ポート１６に接続されていることを検出することができ、あるいは、ホストコンピュータ２０から発行プロセス開始の要求を受信することができる。いずれの場合でも、セキュリティ・デバイス１０は、ホストデバイス（例えばホストコンピュータ２０）からホスト・シードを受信する（ステップ２１０）。一実施形態において、ホストコンピュータ２０は、ホスト・シードを暗号化し、暗号化されたホスト・シードをセキュリティ・デバイス１０へ送信する。その代わりに、ホスト・シードは、暗号化されないことがあり、別途の暗号化なしに安全な通信リンクによって伝送されることがある。ホスト・シードが暗号化されるならば、セキュリティ・デバイス１０（例えばマイクロプロセッサ１４）は、暗号化されたホスト・シードを復号してホスト・シードを回復する（ステップ２２０）。その後、シークレットが生成される（ステップ２３０）。

【００３２】

一実施形態において、シークレットは、プラグインカード３０によって生成されるデータ（例えば、プラグインカード３０によって生成される乱数または擬似乱数）とホスト・シードの混合物である。一部の実施形態において、マイクロプロセッサ１４は、プラグイン・デバイス３０に乱数生成の要求を送信する。プラグイン・デバイスの乱数ジェネレー

タ１８は乱数を生成し、プラグイン・デバイス３０はその数をマイクロプロセッサ１４に送信する。他の実施形態において、セキュリティ・デバイスは、乱数を生成するかあるいはメモリ１７から乱数を検索する。乱数は、ランダムまたは擬似ランダムであることができる。マイクロプロセッサ１４は、その後、乱数を用いてホスト・シードをスクランブルしてシークレット（本明細書では「混合シード」と呼ぶ。）を生成する。

【００３３】

その後、シークレット（例えば混合シード）は、プラグイン・デバイス３０へ伝達されて格納されることができる（例えば、マイクロプロセッサ１４は、混合シードをプラグイン・デバイスのメモリ２５に送信することができる）（ステップ２４０）。一部の実施形態において、１つの混合シードしかプラグイン・デバイス３０上に格納されることができない。

【００３４】

一部の実施形態において、オリジナルのプラグイン・デバイス３０が改ざんされるかあるいは失われたら、システムは、新たなプラグイン・デバイス３０にシークレットを発行することができる。例えば、新たなプラグイン・デバイス３０がシークレットを格納するように要求されたら、セキュリティ・デバイス１０は、自らのメモリから乱数を呼び戻し、ホストデバイスからホスト・シードを要求し、シークレット（例えば混合シード）を生成し直すことができる。セキュリティ・デバイス１０は、その後、新たなプラグイン・デバイス３０へ混合シードを発行することができる。

【００３５】

プラグイン・デバイスとの通信

【００３６】

上記したように、セキュリティ・デバイス１０は、シークレットの転送を含めてプラグイン・デバイス３０と通信することができる。通信は、後述するような認証ルーチンを含むことができる。認証は、プラグイン・デバイス３０がセキュリティ・デバイス１０に結合されるたびに行われることができる。セキュリティ・デバイス１０及びプラグイン・デバイス３０を認証するための１つのプロトコルが参照されている。この１つのプロトコルは例示的なものであり、他のプロトコルが用いられることもできる。同様に、認証プロトコルにおいて用いられることができる認証鍵を参照されたい。認証鍵は、製造中または他の状態を含めて種々の手段によって、プラグイン・デバイス３０及びセキュリティ・デバイス１０の両方に知られるように作られることができる。認証鍵は、認証プロセス中に用いられるようにセキュリティ・デバイス１０及びプラグイン・デバイス３０の両方に格納される。一部の実施形態において、認証鍵は、ホストコンピュータ２０によって割り当てられる。任意選択で、追加的な安全保護のために、ＰＩＮがプラグイン・デバイス３０及びセキュリティ・デバイス１０に割り当てられることもできる。ＰＩＮは、ホストコンピュータ２０に知られていないが、セキュリティ・デバイス１０及びプラグイン・デバイス３０にのみ知られている数である場合がある。

【００３７】

一部の実施形態において、セキュリティ・デバイス１０は、プラグイン・デバイス３０にシークレット（例えば混合シード）を発行する前に、プラグイン・デバイス３０を認証する。認証プロセスはプラグイン・デバイス３０がセキュリティ・デバイス１０に接続されるたびに用いられることができ、セキュリティ・デバイス１０はデータの暗号化または復号に用いられる。ユーザがプラグイン・デバイス３０をセキュリティ・デバイス１０のポート（例えばプラグイン・デバイス・ポート１６）に結合するとき、セキュリティ・デバイス１０はプラグイン・デバイス３０を検出する。プラグイン・デバイス３０及びセキュリティ・デバイス１０は、データ・セキュリティを確実にするための一方向または両方向チャレンジに関与する場合がある。一部の実施形態において、ホストコンピュータ２０からの要求により認証プロセスが始まる。

【００３８】

図５を参照すると、認証とシークレット・シェアリングを組み合せた方法の一実施形態

が示されており、ここでは、セキュリティ・デバイス１０（そのステップは実線で示されている）及びプラグイン・デバイス３０（そのステップは破線で示されている）が各々認証／シェアリング方法のステップを実行する。このプロセスは、セキュリティ・デバイス１０が乱数の要求をプラグイン・デバイス３０に送信することから始まる（ステップ４０５）。プラグイン・デバイス３０は、要求を受信し（ステップ４１０）、乱数を生成する（ステップ４１５）。乱数は、シークレット（例えば混合シード）を生成するために用いられた数と同じ数または異なる数であることができる（例えば、認証プロセスの一部として、プラグイン・デバイスは、プラグイン・デバイス及びセキュリティ・デバイスの両者が正しい認証鍵及びＰＩＮ（詳細に後述）を有することを確認するために用いられる乱数を生成することがある（このプロセスはそれ自体、上記したシークレット・シェアリング・プロセスから切り離されることがある））。プラグイン・デバイス３０は、乱数を含むレスポンスをデバイス１０に送信する（ステップ４２０）。乱数の伝送は、安全な通信リンク上で行われるかあるいは別な方法で安全にされることができる。

【００３９】

デバイス１０は、乱数を受信し（ステップ４２５）、受信した乱数を暗号化する（ステップ４３０）。セキュリティ・デバイス１０は、セキュリティ・デバイス１０及びプラグイン・デバイス３０の両方に知られている認証鍵を用いて乱数を暗号化する。一実施形態において、認証鍵は、発行中にプラグイン・デバイス３０に書き込まれる。セキュリティ・デバイス１０は、乱数の暗号化のためのＤＥＳ、３ＤＥＳまたはＡＥＳなどの規格を用いることができる。他の適切な鍵またはアルゴリズムも、両者がプラグイン・デバイス３０及びセキュリティ・デバイス１０に知られている限り、用いられることがある。

【００４０】

セキュリティ・デバイス１０は、暗号化された乱数と共に外部認証要求をプラグイン・デバイス３０に送り返す（ステップ４３５）。セキュリティ・デバイス１０からの受信された通信と並行してまたはそれに応えて、プラグイン・デバイスの暗号化エンジン２１はまた、その認証鍵及び暗号化アルゴリズム（セキュリティ・デバイス１０で用いられているものと同じであると仮定する）を用いて乱数を暗号化する（ステップ４４０）。その後、プラグイン・デバイス３０は、プラグイン・デバイスの暗号化された乱数がセキュリティ・デバイスの暗号化された乱数と一致するか否かをチェックする（ステップ４４５）。２つの暗号化された数が一致しなければ、プラグイン・デバイス３０は、セキュリティ・デバイス１０に失敗レスポンスを送信し、チャレンジは終了する。２つの暗号化された数が一致すれば、プラグイン・デバイスは成功レスポンスを送信することができる（ステップ４５０）。認証プロセスは、これで完了する。

【００４１】

任意選択で、セキュリティ・デバイス１０は、認証後にプラグイン・デバイス３０の更なる妥当性検査を行う。妥当性検査ステップは、プラグイン・デバイス３０がセキュリティ・デバイス１０につながれることを確実にすることができる。妥当性検査部分において、セキュリティ・デバイス１０は、個人認証番号（ＰＩＮ）検証要求をＰＩＮと共にプラグイン・デバイス３０に送信する（ステップ４５５）。プラグイン・デバイス３０は、その格納されたＰＩＮが受信されたＰＩＮと等しいかチェックする（ステップ４５５）。ＰＩＮが一致しなければ、プラグイン・デバイス３０は失敗レスポンスを送信し、チャレンジは終了する。ＰＩＮが一致すれば、プラグイン・デバイス３０は成功レスポンスを送信し、チャレンジは成功裡に終了する。ＰＩＮ検証は、特定のプラグイン・デバイス３０を特定のセキュリティ・デバイス１０に結び付けるために用いられることができる。一実施形態において、ＰＩＮは、プラグイン・デバイスがホスト要求によって初期化されるときに生成される。

【００４２】

上記した中では特定の認証プロトコルを参照しているが、互いに通信している通信相手の一方または双方をベリファイするものを含めて他の認証スキームも可能である。さらに、プラグイン・デバイス３０またはセキュリティ・デバイス１０のいずれか一方によって

実行されている特定の動作が参照されているが、それらの動作は、代わりの実装において代わりの認証プロトコルを用いて他方によって実行されることもできる。

【００４３】

暗号化／復号プロセス

【００４４】

ひとたびプラグイン・デバイス３０及びセキュリティ・デバイス１０が認証（必要に応じてＰＩＮ妥当性検査を含む）を首尾よく完了したら、セキュリティ・デバイス１０は、図６に示されているように、鍵（Ｅ／Ｄ鍵）を生成し、暗号化／復号プロセスを開始することができる。一実施形態において、セキュリティ・デバイスは、Ｅ／Ｄ鍵を生成する前に、プラグイン・デバイス３０を認証しなければならない。セキュリティ・デバイス１０は、プラグイン・デバイス３０からシークレット（例えば混合シード）を検索（または受信）する（ステップ５１０）。ホスト・シードは、その後、シークレットから回復される（ステップ５２０）。混合シードが用いられるとき、セキュリティ・デバイス１０（例えばセキュリティ・デバイス１０のマイクロプロセッサ１４）は、前に受信した乱数を用いて混合シードを逆スクランブルすることによって混合シードからホスト・シードを復元することができる。一部の実施形態において、セキュリティ・デバイス１０は、必要に応じてホスト・シードを抽出するために検索のための乱数を格納する。その後、Ｅ／Ｄ鍵が生成される（ステップ５３０）。一実施形態において、マイクロプロセッサ１４は、ホスト・シードをデバイス・シードと合わせて、Ｅ／Ｄ鍵を生成する。一実施形態において、セキュリティ・デバイス１０が初期化されるときにデバイス・シードが生成される。一実施形態において、各セキュリティ・デバイスは固有のデバイス・シードを有する。デバイス・シードは、後に続く検索のためにメモリ１７内に格納されることができる。最後に、暗号化／復号エンジン１２はイネーブルされることができ、つまり、エンジンは、ひとたびＥ／Ｄ鍵を持てば、暗号化または復号を開始することができる（ステップ５４０）。

【００４５】

一部の実施形態において、セキュリティ・デバイス１０は、プラグイン・デバイス３０が取外しまたは切断されるときを検出することができる。セキュリティ・デバイス１０は、暗号化／復号エンジン１３を停止させ、ホストコンピュータ２０が大容量記憶装置４０へ／からそれ以上データを格納したりアクセスしたりしないようにすることができる。一部の実施形態において、プラグイン・デバイス３０が取り外されたことをセキュリティ・デバイス１０が検出したとき、セキュリティ・デバイスはメモリからＥ／Ｄ鍵を一掃する。

【００４６】

システムについて、１つのホストを有するものとして述べてきたが、複数のホストがセキュリティ・デバイス１０と通信することもできる。プラグイン・デバイス３０がセキュリティ・デバイス１０と通信している限り、セキュリティ・デバイス１０は、ホストの各々がデータに安全にアクセスしたり格納したりできるようにすることができる。

【００４７】

一部の実施形態において、システムのコンフィギュレーションは、図２に示されているシステムから変更されている。ホストコンピュータ２０は、プラグイン・デバイス３０、大容量記憶装置４０及びセキュリティ・デバイス１０に接続することができる。ホストコンピュータ２０は、必要に応じて、暗号化または復号されるデータをセキュリティ・デバイス１０及び大容量記憶装置４０に／から渡すことができる。

【００４８】

高度に安全な鍵管理技術を用いてデータの暗号化及び復号を行うための方法が記載されている。本明細書に記載の方法は、実行時にのみ存在する鍵を生成する。鍵は、メモリ内に格納されず、セキュリティ・デバイスへ／から転送されない。それゆえ、鍵は、プラグイン・デバイス及びセキュリティ・デバイスが一緒に用いられないとき、例えばプラグイン・デバイスまたはセキュリティ・デバイスが個々に盗まれたとき、メモリから検索されることができない。これは、正規のセキュリティ・デバイス及び正規のプラグイン・デバ

イスの両方を持たない何者かに鍵がアクセスされることを防ぐ。

【００４９】

一実施形態において、プラグイン・デバイスはＥ／Ｄ鍵を格納しないが、むしろ混合シード（即ち、ホスト・シード及び乱数のハイブリッド）を格納する。ホスト・シードは、Ｅ／Ｄ鍵を生成するためにデバイス・シードと組み合わされる前に、先ず、混合シードから抽出される。デバイスだけを制御してもデバイス・シードへのアクセスを与えることにしかならず、それではＥ／Ｄ鍵を生成するのに不十分である。プラグイン・デバイスを制御しても混合シードを提供するだけであり、それもまたＥ／Ｄ鍵を復元するのに不十分である。それゆえ、正しいプラグイン・デバイス及び正しいセキュリティ・デバイスの両方が一緒に所望のＥ／Ｄ鍵を生成するために必要とされる。プラグイン・デバイス、大容量記憶装置とセキュリティ・デバイス間のデータ接続、またはセキュリティ・デバイスの情報が個々に洩らされることがあっても、データは尚も安全である。

【００５０】

大容量記憶装置４０は、物理的にセキュリティ・デバイス１０の近くに配置される必要がない。大容量記憶装置４０とセキュリティ・デバイス１０間で伝送されるいかなる情報も暗号化されるので、部外者、即ちホストコンピュータ２０のユーザ以外の何者かによるアクセスは、暗号化されたデータへのアクセスが許されるだけである。

【００５１】

本発明の多くの実施形態について述べてきた。それにもかかわらず、本発明の真の趣旨及び範囲から逸脱することなく種々の変更がなされ得ることを理解されたい。例えば、プラグイン・デバイスは、集積回路を含むか、あるいは、ユーザが運搬及び持ち運びし易い小型の別の読み取り可能な媒体に置き換えることができる。混合シードがプラグイン・デバイスからセキュリティ・デバイスへ転送される前に、代わりの、または追加の検証ステップが開始されることができる。本明細書に記載の乱数またはＰＩＮは、記号、文字、また時には数、またはその組合せを含むようなパスワードまたは文字列と交換されることができる。よって、特許請求の範囲内に他の実施形態が含まれる。

【図面の簡単な説明】

【００５２】

【図１】記憶装置と通信しているホストコンピュータの回路図。

【図２】プラグイン・デバイスと通信するように構成されたセキュリティ・デバイスの回路図。

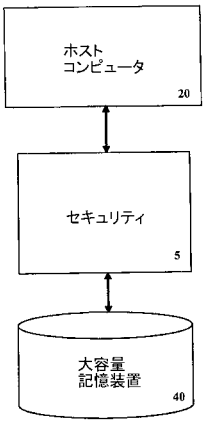
【図３】セキュリティのためのプラグイン・デバイスを準備し、使用するためのフロー図。

【図４】プラグイン・デバイスへのシークレットの発行を説明するフロー図。

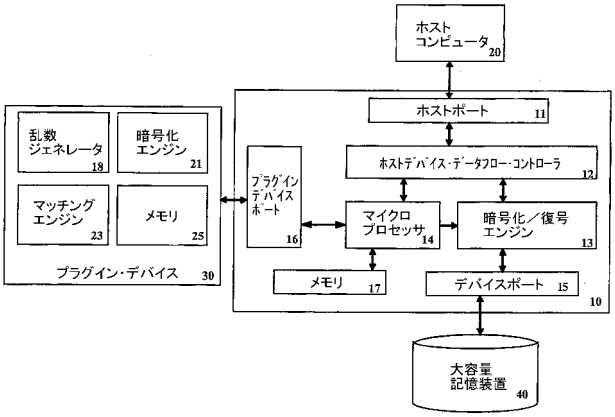
【図５】プラグイン・デバイス及びセキュリティ・デバイスを認証及びベリファイするためのフロー図。

【図６】プラグイン・デバイスからシークレットをロードして鍵を生成するためのフロー図。

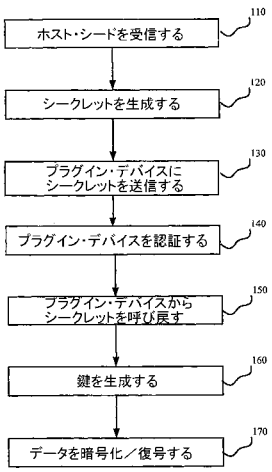
【図１】


ホスト
コンピュータ
20
セキュリティ
5
大容量
記憶装置
40

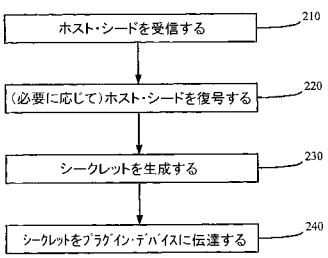
【図２】


ホスト
コンピュータ
20
ホストポート
11
乱数
ジェネレータ
18
暗号化
エンジン
21
マッチング
エンジン
23
メモリ
25
プラグイン・デバイス
30
プラグイン
デバイス
ポート
16
ホストデバイス・データフロー・コントローラ
12
マイクロ
プロセッサ
14
暗号化／復号
エンジン
13
メモリ
17
デバイスポート
15
10
大容量
記憶装置
40

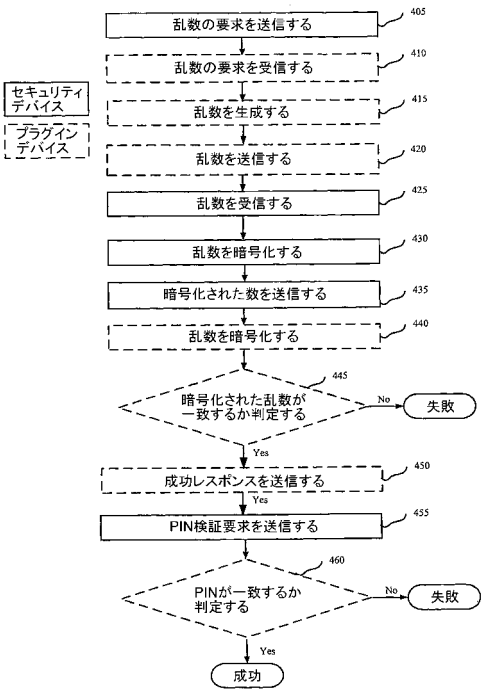
【図３】


ホスト・シードを受信する
110
シークレットを生成する
120
プラグイン・デバイスに
シークレットを送信する
130
プラグイン・デバイスを認証する
140
プラグイン・デバイスから
シークレットを呼び戻す
150
鍵を生成する
160
データを暗号化／復号する
170

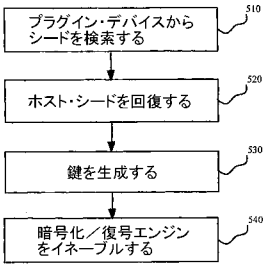
【図４】


ホスト・シードを受信する
210
(必要に応じて)ホスト・シードを復号する
220
シークレットを生成する
230
シークレットをプラグイン・デバイスに伝達する
240

【図５】


セキュリティ
デバイス
プラグイン
デバイス
乱数の要求を送信する
405
乱数の要求を受信する
410
乱数を生成する
415
乱数を送信する
420
乱数を受信する
425
乱数を暗号化する
430
暗号化された数を送信する
435
乱数を暗号化する
440
暗号化された乱数が
一致するか判定する
445
No
失敗
Yes
成功レスポンスを送信する
450
Yes
PIN検証要求を送信する
455
PINが一致するか
判定する
460
No
失敗
Yes
成功

【図６】


プラグイン・デバイスから
シードを検索する
510
ホスト・シードを回復する
520
鍵を生成する
530
暗号化／復号エンジン
をイネーブルする
540

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,LY,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 フェン、イ
中華人民共和国２００００３１上海・フェンヤンロード ナンバー １３８
(72)発明者 ワン、チンヘン
中華人民共和国２００００３上海・フェンヤンロード ナンバー １３８

Ｆターム(参考) 5B017 AA03 BA07 CA16
5J104 AA07 AA16 AA32 AA41 EA04 EA08 EA16 EA18 FA00 JA03
KA02 NA02 NA33 NA37 NA40 PA07