(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2005-521278
(P2005-521278A)
(43)公表日　平成17年7月14日(2005.7.14)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/08	H04L	9/00	601D	5J104
	H04L	9/00	601E	

審査請求 未請求　予備審査請求 未請求　（全 15 頁）

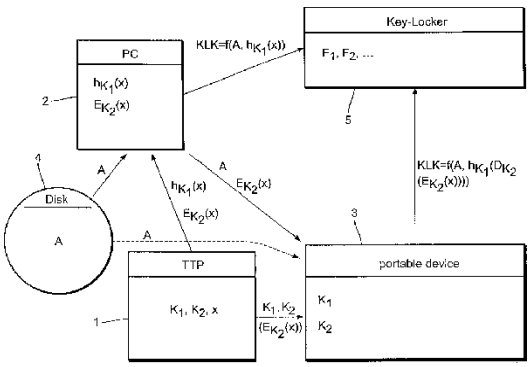
(21)出願番号	特願2003-577101 (P2003-577101)
(86)(22)出願日	平成15年2月19日 (2003.2.19)
(85)翻訳文提出日	平成16年9月16日 (2004.9.16)
(86)国際出願番号	PCT/IB2003/000682
(87)国際公開番号	WO2003/079166
(87)国際公開日	平成15年9月25日 (2003.9.25)
(31)優先権主張番号	02076070.8
(32)優先日	平成14年3月18日 (2002.3.18)
(33)優先権主張国	欧州特許庁 (EP)

(71)出願人　590000248
コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ
Ｋｏｎｉｎｋｌｉｊｋｅ　Ｐｈｉｌｉｐｓ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｎ．Ｖ．
オランダ国　５６２１　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　１
Ｇｒｏｅｎｅｗｏｕｄｓｅｗｅｇ　１，５６２１　ＢＡ　Ｅｉｎｄｈｏｖｅｎ，Ｔｈｅ　Ｎｅｔｈｅｒｌａｎｄｓ
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介

最終頁に続く

(54)【発明の名称】コンテンツへのアクセスを制御するための方法及びシステム

(57)【要約】
本発明は、コンテンツへのアクセスを制御するための方法とアクセス制御システムに関するものであり、前記コンテンツはキー・ロッカー鍵（KLK）により暗号化されたキー・ロッカー（5）に格納されたコンテンツ鍵（F1、F2）により暗号化される。前記コンテンツを使用する装置（3）を更新する必要なく、PCアプリケーション又はPCアプリケーションを作動するコンピュータ（2）を更新することにより、アクセス制御システムのセキュリティを回復させるために、－暗号ユニット（1）により、少なくとも２つのアクセス鍵（K1、K2）と、１つの文字列（x）とを定めるステップと、－少なくとも２つの暗号値（h、E）を得る前記アクセス鍵（K1、K2）を使用して、前記暗号ユニット（1）により前記文字列（x）を暗号化するステップと、－前記コンテンツにアクセスするように適合されたコンピュータ（2）に前記暗号値（h、E）を格納し、前記コンピュータ（2）が前記キー・ロッカー鍵（KLK）を計算することを可能にするステップと、－前記コンテンツにアクセスし、前記コンピュータ（2）又は前記暗号ユニット（1）のいずれかから装置（



【特許請求の範囲】
【請求項１】
コンテンツへのアクセスを制御する方法であって、
前記コンテンツが、キー・ロッカー鍵により暗号化されたキー・ロッカーに格納されたコンテンツ鍵により暗号化され、
－暗号ユニットにより、少なくとも２つのアクセス鍵と、１つの文字列とを定めるステップと、
－少なくとも２つの暗号値を得る前記アクセス鍵を使用して、前記暗号ユニットにより前記文字列を暗号化するステップと、
－前記コンテンツにアクセスするように適合されたコンピュータに前記暗号値を格納し、前記コンピュータが前記キー・ロッカー鍵を計算することを可能にするステップと、
－前記コンテンツにアクセスし、前記コンピュータ又は前記暗号ユニットのいずれかから装置に前記暗号値のうちの少なくとも１つを送出するように適合された装置に前記アクセス鍵を格納し、前記装置が前記キー・ロッカー鍵を計算することを可能にするステップと
を有する方法。
【請求項２】
請求項１に記載の方法であって、
前記コンテンツと前記キー・ロッカーが、情報媒体、特にCD又はDVDのような光ディスクに格納され、
前記キー・ロッカー鍵が、前記情報媒体の固有の媒体識別子と、前記暗号値のうちの１つから導かれる方法。
【請求項３】
請求項２に記載の方法であって、
前記情報媒体にアクセスした時に、前記媒体識別子が前記コンピュータにより前記情報媒体から読み取られ、
前記情報媒体にアクセスした時に、前記媒体識別子が前記コンピュータから前記装置に送出され、又は前記情報媒体から前記装置により読み取られる方法。
【請求項４】
請求項１に記載の方法であって、
前記コンテンツが、MP3ファイルのようなデータファイルを有し、
前記データファイルが、異なるコンテンツ鍵によりそれぞれ暗号化され、
前記コンテンツ鍵が前記キー・ロッカーに格納され、
前記データファイルが、前記暗号値と共に前記コンピュータから前記装置に送出される方法。
【請求項５】
請求項１に記載の方法であって、
まず、前記受領された暗号値を解読することにより前記文字列を再構成し、次に、前記再構成された文字列を暗号化してその他の暗号値を得ることにより、前記キー・ロッカー鍵が、前記アクセス鍵と前記受領された暗号値を使用して前記装置により計算される方法。
【請求項６】
請求項１に記載の方法であって、
前記暗号ユニットが、第１の可変の文字列と、第２の固定の文字列とを定め、前記第２の固定の文字列も前記装置に格納され、
前記少なくとも２つの暗号値のうちの１つが、前記第１の文字列のみを暗号化することにより得られ、前記少なくとも２つの暗号値のうちの１つが、前記第１と第２の文字列の組み合わせを暗号化することにより得られる方法。
【請求項７】
請求項６に記載の方法であって、
前記第２の文字列が、第１の可変の文字列部分と第２の固定の文字列部分とを有し、

前記第１の文字列部分が、前記暗号ユニットから直接に、又は前記コンピュータを介して、前記装置に送出され、
前記第２の文字列部分が、前記装置に格納される方法。
【請求項８】
請求項１に記載の方法であって、
前記文字列は、定期的に、又はコンピュータに格納された前記暗号値が手を加えられたときに更新される方法。
【請求項９】
コンテンツへのアクセスを制御するためのアクセス制御システムであって、
前記コンテンツが、キー・ロッカー鍵により暗号化されたキー・ロッカーに格納されたコンテンツ鍵により暗号化され、
－少なくとも２つのアクセス鍵と、１つの文字列とを定め、少なくとも２つの暗号値を得る前記アクセス鍵を使用して、前記文字列を暗号化するための暗号ユニットと、
－前記コンテンツにアクセスし、前記暗号値を格納するように適合されたコンピュータであって、前記コンピュータが前記キー・ロッカー鍵を計算することを可能にするコンピュータと、
－前記コンテンツにアクセスし、前記コンピュータ又は前記暗号ユニットのいずれかから前記暗号値のうちの少なくとも１つを受領するように適合された装置であって、前記装置が前記キー・ロッカー鍵を計算することを可能にする装置と
を有するアクセス制御システム。
【請求項１０】
コンテンツへのアクセスを制御するためのアクセス制御システムで使用するための暗号ユニットであって、
前記コンテンツが、キー・ロッカー鍵により暗号化されたキー・ロッカーに格納されたコンテンツ鍵により暗号化され、
前記暗号ユニットが、少なくとも２つのアクセス鍵と、１つの文字列とを定め、少なくとも２つの暗号値を得る前記アクセス鍵を使用して、前記文字列を暗号化するように適合され、
前記暗号値が、前記コンテンツにアクセスするように適合されたコンピュータに格納され、前記コンピュータが前記キー・ロッカー鍵を計算することを可能にし、
前記アクセス鍵が、前記コンテンツにアクセスするように適合された装置に格納され、
前記暗号値のうちの少なくとも１つが、前記コンピュータ又は前記暗号ユニットのいずれかから前記装置に送出され、前記装置が前記キー・ロッカー鍵を計算することを可能にする暗号ユニット。
【請求項１１】
コンテンツへのアクセスを制御するためのアクセス制御システムで使用するためのコンピュータであって、
前記コンテンツが、キー・ロッカー鍵により暗号化されたキー・ロッカーに格納されたコンテンツ鍵により暗号化され、
少なくとも２つのアクセス鍵と１つの文字列が定められ、前記文字列が、少なくとも２つの暗号値を得る暗号ユニットにより前記アクセス鍵を使用して暗号化され、
前記コンピュータが、前記コンテンツにアクセスし、前記暗号値を格納するように適合され、前記コンピュータが前記キー・ロッカー鍵を計算することを可能にし、
前記アクセス鍵が、前記コンテンツにアクセスするように適合された装置に格納され、
前記暗号値のうちの少なくとも１つが、前記コンピュータ又は前記暗号ユニットのいずれかから前記装置に送出され、前記装置が前記キー・ロッカー鍵を計算することを可能にするコンピュータ。
【請求項１２】
コンテンツへのアクセスを制御するためのアクセス制御システムで使用するための装置であって、

前記コンテンツが、キー・ロッカー鍵により暗号化されたキー・ロッカーに格納されたコンテンツ鍵により暗号化され、
少なくとも２つのアクセス鍵と１つの文字列が定められ、前記文字列が、少なくとも２つの暗号値を得る暗号ユニットにより前記アクセス鍵を使用して暗号化され、
前記暗号値が、前記コンテンツにアクセスするように適合されたコンピュータに格納され、前記コンピュータが前記キー・ロッカー鍵を計算することを可能にし、
前記装置が、前記コンテンツにアクセスし、前記アクセス鍵を格納し、前記コンピュータ又は前記暗号ユニットのいずれかから前記暗号値のうちの少なくとも１つを受領するように適合され、前記装置が前記キー・ロッカー鍵を計算することを可能にする装置、
【請求項１３】
コンピュータプログラムが請求項９に記載のアクセス制御システムの１つ以上の要素で動作するときに、請求項１に記載の方法のステップをコンピュータに実行させるためのコンピュータプログラムコード手段を有するコンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンテンツへのアクセスを制御する方法に関するものであり、前記コンテンツはキー・ロッカー鍵（KLK）により暗号化されたキー・ロッカーに格納されたコンテンツ鍵により暗号化される。本発明は、対応するアクセス制御システムと、そのようなアクセス制御システムで使用するための暗号ユニットと、コンピュータと、装置に更に関するものである。更に、本発明はコンピュータプログラムに関する。
【背景技術】
【０００２】
インターネットは、デジタル音楽を配信するための最も重要な手段のうちの１つになったと広くみなされている。大いに減少した配信コストや、より多くのカタログの可用性のような多くの利点にも関わらず、解決される必要のある多数の欠点が依然として存在する。コピープロテクトの欠如は、主要なレコードラベルがこの領域に入ることを妨げる主要な問題である。プロテクトされた音楽をダウンロードするために特別の（加入者に基づく）サービスを開始することが意図される。特別のPCアプリケーションが、MP3ファイルのような暗号化ファイルをダウンロードし、一般的なPCに基づくCD又はDVDレコーダを使用して、それをCD-Rディスクのような記録可能情報媒体に格納するために支給される。暗号化ファイルは、PCで、及び携帯用MP3-CDプレイヤのような一般の又は少し適合させた装置で再生され得る。暗号化ファイルの鍵は、いわゆるキー・ロッカーに格納され、そのキー・ロッカーはその目的のために引き当てられたディスクの領域である。キー・ロッカー自体は、鍵（全システムに及び秘密であり、通常は固有のディスク識別子から生成されたいわゆるキー・ロッカー鍵）で暗号化される。留意すべき点は、この目的に適合された如何なる装置でディスクが再生され得ることを確保するために、グローバルの秘密の使用が必要になる点である。
【発明の開示】
【発明が解決しようとする課題】
【０００３】
前述のPCアプリケーションは暗号化ファイルを再生することができるため、それはキー・ロッカー鍵へのアクセスを有する。従って、それはグローバルの秘密へのアクセスをも有する。PCソフトウェアは比較的容易にハッキングされることが周知であるため、セキュリティの視点から、このことは弱点である。従って、グローバルの秘密が短時間で損なわれることが予期される。セキュリティ侵害を修復するためにPCアプリケーションを更新されたものに交換することは、比較的容易である。しかし、携帯用MP3-CDプレイヤのようなハードウェア装置を交換することは不可能である。
【課題を解決するための手段】
【０００４】

従って、装置のハードウェアを変更する必要なく、PCアプリケーションを交換することによりセキュリティ侵害からの回復を可能にする方法を提供することが本発明の目的である。そのようなシステムとコンピュータプログラムでの使用のためにアクセス制御システム及び装置を提供することが本発明の目的である。

【０００５】

この目的は、請求項１に記載のコンテンツへのアクセスを制御する方法によって達成され、前記方法は、

－暗号ユニットにより、少なくとも２つのアクセス鍵と、１つの文字列とを定めるステップと、

－少なくとも２つの暗号値を得る前記アクセス鍵を使用して、前記暗号ユニットにより前記文字列を暗号化するステップと、

－前記コンテンツにアクセスするように適合されたコンピュータに前記暗号値を格納し、前記コンピュータが前記キー・ロッカー鍵を計算することを可能にするステップと、

－前記コンテンツにアクセスし、前記コンピュータ又は前記暗号ユニットのいずれかから装置に前記暗号値のうちの少なくとも１つを送出するように適合された装置に前記アクセス鍵を格納し、前記装置が前記キー・ロッカー鍵を計算することを可能にするステップとを有する。

【０００６】

本発明は、装置がコンピュータと異なる秘密を利用すべきであるという考えに基づく。コンピュータをハッキングすることは比較的容易であるため、コンピュータがハッキングされたときに装置により使用される鍵が損失され、又は損なわれることが回避されなければならない。暗号ユニットにより定められたアクセス鍵を使用して、暗号ユニット（例えば、装置の製造者、サービスプロバイダ又はコンテンツプロバイダのような信頼を受けたサードパーティ）により定められた暗号値を作ることにより、及び前記アクセス鍵と前記文字列ではなく、前記暗号値をコンピュータにのみ提供することにより、前記のことが本発明に従って回避される。前記アクセス鍵は、装置にのみ提供され、その装置は、全ての機能が通常はそのハードウェアに埋め込まれているため、容易にハッキングされ得ない。暗号値を作るためのアクセス鍵と文字列と暗号化機能は、文字列が既知である場合にキー・ロッカー鍵を計算することが容易であるが、暗号値が既知であっても文字列が未知である場合にはアクセス鍵を計算することが困難又はほぼ不可能であるように選択される。

【０００７】

このように、文字列はトラップドア（trapdoor）の役割をする。コンピュータが壊されたが、装置のアクセス鍵が依然として未知である場合、コンピュータで作動するPCアプリケーションを交換することにより、又は別に選択された文字列の使用により作られた新しい暗号値をコンピュータに提供することにより、アクセス制御システムの更新が可能である。このように、新しい鍵で装置を更新する必要はないが、コンピュータを介して行われ得る前記暗号鍵のうちの１つを装置に提供することのみが必要である。

【０００８】

留意すべき点は、暗号化という用語は、秘密鍵と公開鍵の対の使用又は（共謀の耐性の）一方向のハッシュ関数の使用のような、如何なる方法の暗号化を含む点である。

【０００９】

本発明の好ましい実施例が、従属項に定められる。好ましくは請求項１に記載の方法を実施し、暗号ユニットとコンピュータと装置を有するアクセス制御システムが、請求項９に定められる。本発明は、請求項１０ないし１２のうちのいずれか１項に記載のアクセス制御システムでの使用のための暗号ユニットと、コンピュータと、装置とに更に関係する。コンピュータプログラムが請求項９に記載のアクセス制御システムの１つ以上の要素で動作するときに請求項１に記載の方法のステップをコンピュータに実行させるためのコンピュータプログラムコード手段を有する、本発明によるコンピュータプログラムは、請求項１３に定められる。

【００１０】

好ましい実施例によると、コンテンツとキー・ロッカーが情報媒体（特にCD又はDVDのような光ディスク）に格納され、キー・ロッカー鍵は、前記情報媒体の固有の媒体識別子と、前記暗号値のうちの１つから導かれる。好ましくは、キー・ロッカー鍵を計算するために使用される暗号値は装置に格納又は提供されないが、前記暗号値は少なくとも２つのアクセス鍵と他の暗号値の使用により装置で作られる。

【００１１】

以前の実施例に基づいて、情報媒体にアクセスした時に媒体識別子が前記コンピュータにより情報媒体から読み取られ、情報媒体にアクセスした時に媒体識別子がコンピュータから装置に送出され、又は情報媒体から装置により読み取られることが、更に好ましい。従って、装置が情報媒体に直接アクセスし（例えばインターネットからダウンロードされたコンテンツが格納されたディスクを再生する）、又はコンピュータのみが情報媒体にアクセスし、固有の媒体識別子を読み取り、媒体識別子と必要な暗号値と共にコンテンツを装置に送出し、コンテンツにアクセスするためのコンテンツ鍵を得るために必要なキー・ロッカー鍵を再構成した後に、その装置が如何なる時でもコンテンツを再生することが可能になる。

【００１２】

本発明の更なる態様において、コンテンツはMP3ファイルのようなデータファイルを有し、そのデータファイルは異なるコンテンツ鍵によりそれぞれ暗号化され、前記コンテンツ鍵は前記キー・ロッカーに格納される。更に、前記データファイルは暗号値と共にコンピュータから装置に送出される。留意すべき点は、“コンテンツ”は音声データを意味するだけでなく、何らかの装置で再生又は使用されることがある画像、映像又はソフトウェアデータのようなその他の種類のデータを含むことがあるという点である。同様に、“装置”という用語は、携帯用MP3-CDのような音声再生装置に限定されず、映像カメラ、写真カメラ、ハンドヘルドコンピュータ又は携帯用ゲーム装置のような如何なる種類のデータを再生又は使用するためのその他の装置を含むことがある。

【００１３】

好ましくは、キー・ロッカー鍵は、アクセス鍵と受領された暗号値を使用して装置により計算される。第１のステップでは、暗号ユニットにより定められた文字列が、受領された暗号値、好ましくは前記アクセス鍵のうちの１つを使用して再構成される。第２のステップでは、その結果（すなわち再構成された文字列）が第２のアクセス鍵を使用して暗号化され、キー・ロッカー鍵を計算するために必要な他の暗号値を得る。従って、装置はコンピュータに提供された全ての暗号値を受領する必要がなく、前記暗号値のうちの１つで十分である。

【００１４】

本発明のその他の実施例によると、暗号ユニットは、第１の可変の文字列と、第２の固定の文字列とを定め、その第２の固定の文字列も装置に格納される。少なくとも２つの暗号値のうちの１つは第１の文字列のみを暗号化することにより得られ、第２の暗号値は前記第１と第２の文字列の組み合わせ（例えば前記２つの文字列の2を法とする加算の結果）を暗号化することにより得られる。このことは、コンピュータのハッキングにより暗号値が失われても、アクセス鍵と第１の可変の文字列の情報があまり失われないため、全体のアクセス制御システムのセキュリティを更に改善する。従って、付加的な第２の文字列の使用により、自由に使えるより多くの暗号文を有する敵対者に対して、アクセス制御システムが更に安全になる。更なる実施例でアクセス制御システムのセキュリティを更に改善するために、第２の文字列は第１の可変の文字列部分と第２の固定の文字列部分とを有する。この実施例において、第１の文字列部分は暗号ユニットから直接に、又はコンピュータを介して、装置に送出され、第２の文字列部分はアクセス鍵と共に当初から既に装置に格納される。従って、更新時に暗号ユニットは新しい第１の文字列と第２の文字列の新しい第１の文字列部分とを選択するのみである。このことは、新しい第２の文字列を導き、結果として新しい暗号鍵を導く。コンピュータ又はそこで作動するアプリケーションが更新される毎に第２の文字列も変更され得るという事実は、プレーンテキストの更なるラ

ンダム性を導入し、それにより暗号値から情報があまり得られることができない。

【００１５】

前述の通り、コンピュータに格納された暗号値は、手を加えられたときに更新されることが好ましい。その他に又は更に、それはアクセス制御システムのセキュリティを改善するために定期的に更新されることもある。

【００１６】

次に、本発明が図面を参照して更に詳細に説明される。

【発明を実施するための最良の形態】

【００１７】

図１に示される本発明によるアクセス制御システムは、信頼を受けたサードパーティ（TTP）のような暗号ユニット1と、パーソナルコンピュータ（PC）のようなコンピュータ2と、携帯用CDプレイヤ、MP3-CDプレイヤ（例えばPhilips eXpaniumの修正版）又はDVDプレイヤのような装置3と、CD若しくはDVD、半導体フラッシュカード又は取り外し可能ハードディスクのような記録可能又は書換可能ディスクのような情報媒体4とを有し、その情報媒体4に特定の領域又は特定の方法でキー・ロッカー5が格納される。情報媒体4は、固有の識別子と、コンピュータ2に提供されなければならない潜在的な他のデータを更に有する。このデータの全体のセットが記号Aで示される。情報媒体4は、好ましくは記録可能又は書換可能な形式であり、それにより例えばインターネット上のサーバからコンピュータ2によりダウンロードされた音声、映像又はソフトウェアデータのような如何なる種類のデータがそれに格納され得る。

【００１８】

暗号ユニット1は、文字列$x \in Z_2^m$と２つのアクセス鍵$K_1, K_2 \in Z_2^k$とをランダムに選択する。コンピュータ2とそこで作動するPCアプリケーションは、次のデータ：秘密の暗号値$h_{K1}(x) \in Z_2^l$（$l \leqq m$）と、好ましくは秘密の暗号値$E_{K2}(x) \in Z_2^m$とを運ぶ。関数hは、一方向関数又は暗号化関数Eであることがあり、すなわちそれらは好ましくは異なる。暗号値$h_{K1}(x)$と$E_{K2}(x)$の双方は、暗号ユニット1により作られ、格納のためコンピュータ2に送出される。

【００１９】

装置3は、暗号値$h_{K1}(x)$と$E_{K2}(x)$を受領しないが、暗号鍵$h_{K1}(x)$と$E_{K2}(x)$を作るために使用される鍵K_1とK_2（すなわちアクセス鍵K_1、K_2）は、定められた文字列xを暗号化し、暗号値$h_{K1}(x)$と$E_{K2}(x)$を生じるために使用される暗号関数h_{K1}とE_{K2}の鍵である。

【００２０】

キー・ロッカー鍵KLKは、$KLK=f(A,h_{K1}(x))$としてコンピュータ2により計算される。関数fは、データAとKLKとf自体が既知である場合に暗号値$h_{K1}(x)$を導くことが依然として困難であるように選択される。従って、fのための一方向関数又は暗号化関数を選択することが推奨される。

【００２１】

インターネットからデータをダウンロードした後に、このデータはディスク4に格納され、又は如何なる場所で使用するために例えばディスク4により装置3に例えば携帯用MP3プレイヤに格納され得る音楽を含むMP3ファイルを送出される。前記ファイルにアクセスするために、装置3は最初にキー・ロッカーにアクセスし、そのファイルを解読するためのコンテンツ鍵F_1、F_2等を得る必要がある。キー・ロッカー5にアクセスするために、キー・ロッカー鍵KLKは次の通り：$KLK=f(A,h_{K1}(D_{K2}(E_{K2}(x))))$、装置により計算され得ることが必要になる。ここで$D_{K2}$は暗号化関数$E_{K2}$に対応する解読化関数である。暗号値$E_{K2}(x)$を解読することにより、文字列xが得られ、その文字列xに暗号化関数h_{K1}が適用される。関数fは、コンピュータ2により適用される関数fと同一である。必要なデータセットAは、ディスク4から直接又は好ましくはコンピュータ2を介して受領され、それから暗号値$E_{K2}(x)$が好ましくは秘密のチャネルを介して更に受領される。しかし、暗号値$E_{K2}(x)$はまた、アクセス鍵K_1、K_2と共に暗号ユニット1から直接受領され得る。

【００２２】

従って、文字列xはトラップドア（trapdoor）の役割をする。xをランダムに選択することは容易である。xが既知である場合、キー・ロッカー鍵KLKを計算することは容易であるが、xが未知である場合には、暗号値$h_{K1}(x)$と$E_{K2}(x)$が既知である場合でも鍵K_1を計算することが不可能なほど困難である。コンピュータ2又はそのPCアプリケーションが破壊されたが、秘密鍵K_1、K_2が依然として未知である場合、別に選択されたデータxを備えたものに基づいてPCアプリケーションを交換することにより、又は新しい文字列xをコンピュータ2に提供する（すなわち、暗号ユニット1が新しいストリングxを選択し、暗号値$h_{K1}(x)$、$E_{K2}(x)$を計算し、それをコンピュータ2に提供する）ことにより、アクセス制御システムは容易に更新され得る。従って、暗号ユニット1から装置3に新しいデータを全く提供する必要がなく、コンピュータ2から新しい暗号値$E_{K2}(x)$を受領する必要があるのみである。

【００２３】

例えばコンピュータ2から装置3への転送中に妨害されて暗号値$E_{K2}(x)$が既知である場合、アクセス鍵K_2についての情報が全く漏洩しないことがわかる。暗号値$h_{K1}(x)$と$E_{K2}(x)$の双方が既知であるようにコンピュータ2が破壊された場合ですら、（情報理論上の観点から）アクセス鍵K_1、K_2についての半分のみの情報が漏洩することが更にわかる。

【００２４】

図２は、本発明によるアクセス制御システムの改善された実施例のブロック図を示したものである。前記システムは、図１に示されたシステムと同じ構成要素を有する。暗号ユニット1がまた固定文字列$c \in Z_2^m$をランダムに選択するという事実に違いがある。コンピュータ2は、以下の暗号値：hK1(x)と

【００２５】

【数１】

$$E_{K2}(x \oplus c)$$

を有する。装置はこの固定文字列を１つの付加的な秘密として取得する。また、図１を参照して前述した通り、コンピュータ2はキー・ロッカー鍵KLKを計算する。しかし、装置3は次の関係：

【００２６】

【数２】

$$KLK=f(A,h_{K1}(D_{K2}(E_{K2}(x\oplus c))\oplus c))$$

に従って別にキー・ロッカー鍵KLKを計算する。この計算を可能にするために、装置3はコンピュータ2から、又はその他に暗号ユニット1から暗号値

【００２７】

【数３】

$$E_{K2}(x\oplus c)$$

を備えられていなければならない。

【００２８】

図１に示されるシステムと比較して、暗号値$h_{K1}(x)$と

【００２９】

【数４】

$$E_{K2}(x\oplus c)$$

が明かされることにより、アクセス鍵K_1とK_2と文字列cについての情報があまり漏洩しない。このことにより、自由に使えるより多くの暗号文を有する敵対者に対してアクセス制

御システムが更に安全になる。

【００３０】

本発明によるアクセス制御システムの更に別の実施例が図３に示される。パラメータｃがもはや固定ではなく、PCアプリケーション又はコンピュータ2が更新される如何なる時にも変更され得るという事実に、図２に示されるシステムに関する差がある。従って、関数は次：

【００３１】

【数５】

$$g:Z_2^m \times Z_2^m: (c_1, c_2) \rightarrow c \equiv g(c_1, c_2)$$

のように定められる。この関数gは、特有のアプリケーションの制約に従って選択される。パラメータcとc_1とc_2は、必ずしも同じビット長を有する必要はない。２つのパラメータのうちの１つ、特に図２に示される実施例の文字列cと交換する文字列部分c_2は、装置3に格納され、それ故に固定である。可変の文字列部分c_1を変更することにより、計算文字列cが変更される。更新時に、暗号ユニット1は新しい文字列部分c_1を選択し、文字列c=g(c_1,c_2)を計算する。コンピュータ2でデータ$h_{K1}(x)$とc_1と

【００３２】

【数６】

$$E_{K2}(x \oplus c)$$

が格納される。前述の通り、コンピュータ2はキー・ロッカー鍵を計算し、装置3は以下の関係：

【００３３】

【数７】

$$KLK = f(A, h_{K1}(D_{K2}(E_{K2}(x \oplus c)) \oplus g(c_1, c_2)))$$

に従ってキー・ロッカー鍵を計算することができる。その関数は装置にのみ既知であり、PCアプリケーションをハッキングすることにより損なわれ得ない。PCアプリケーション又はコンピュータ2が更新される毎に、暗号ユニット1は異なる文字列x、c_1を選択する。このことは新しいストリングcを導き、結果として新しい暗号値$h_{K1}(x)$と

【００３４】

【数８】

$$E_{K2}(x \oplus c)$$

を導く。PCアプリケーション又はコンピュータ2が更新される毎に文字列cも変更され得るという事実は、プレーンテキストxと

【００３５】

【数９】

$$x \oplus c$$

のランダム性を更に導入する。従って、暗号文$h_{K1}(x)$と

【００３６】

【数１０】

$$(x \oplus c)$$

からあまり情報が得られることができない。

【００３７】

図１に示されるアクセス制御システムによると、プレーンテキストxのみがランダムに選択される。（情報理論上の観点から）アクセス鍵K_1、K_2についての全ての情報が明らかにされる前に、4kビットの暗号文が明らかにされなければならないことがわかる。キーの長さが暗号文の長さと同位である場合、このことは、コンピュータ2のPCアプリケーションが２回破壊された後に生じる。従って、単一性の距離を増加させるために、暗号値h、Eより大きい長さのアクセス鍵K_1、K_2を使用することがより有利である。留意すべき点は、よい暗号化関数E_Kの場合のアクセス鍵K1、K2を見つけることが依然として計算上実行不可能であるため、このことは、アクセス制御システムが実際に破壊されることを意味するものではない点である。

【００３８】

図２に示される実施例によると、文字列xとcは当初のみにランダムに選択され得る。３回の更新の後に、キーの長さが暗号値のものと匹敵すると仮定すると、原則的にアクセス鍵K_1、K_2を決定する十分な情報が利用可能であることがわかる。また、前記と同じ理由のため、暗号値より長いアクセス鍵を使用することが有利である。しかし、よい暗号化関数h_{K1}、E_{K2}のため、それは依然として計算上実行不可能である。

【００３９】

最後に、図３に示される実施例によると、新しい文字列xと文字列部分c_1は更新毎に選択され得る。アクセス鍵K_1、K_2と文字列部分c_2についての不確定性が、既知の暗号文の数に依存しないことがわかる。従って、このシステムのセキュリティレベルは、以前に示されたシステムのセキュリティレベルより高くなる。

【００４０】

留意すべき点は、同じようにパラメータcが変更され得ると、アクセス鍵K_1とK_2も変更され得る点である。更なる関数がこのことを可能にするために定められなければならない。

【図面の簡単な説明】

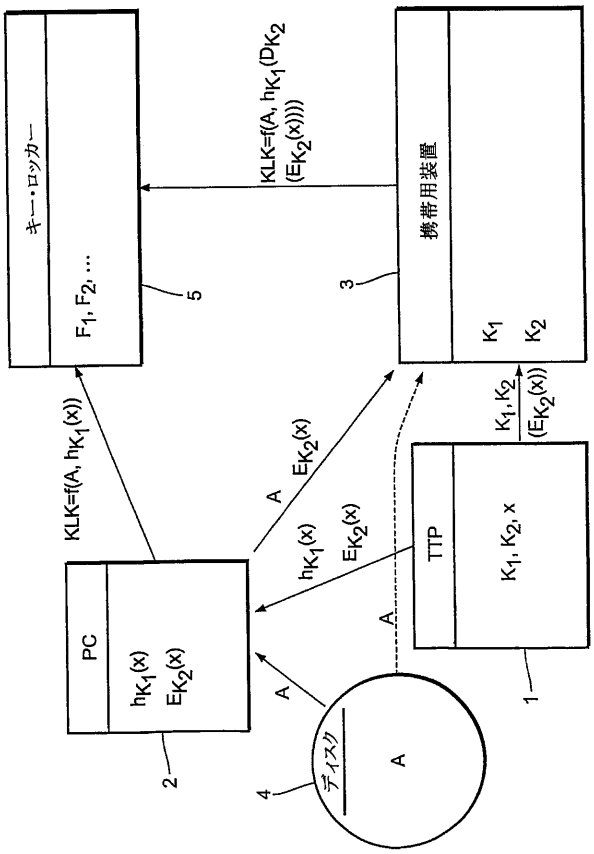
【００４１】

【図１】本発明によるアクセス制御の第１の実施例のブロック図を示したものである。

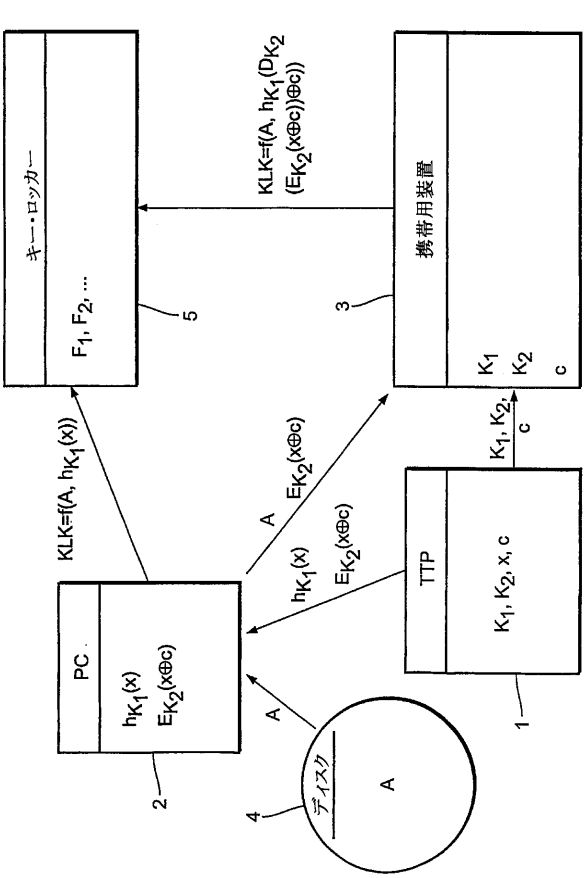
【図２】本発明によるアクセス制御システムの第２の実施例のブロック図を示したものである。

【図３】本発明によるアクセス制御システムの第３の実施例のブロック図を示したものである。

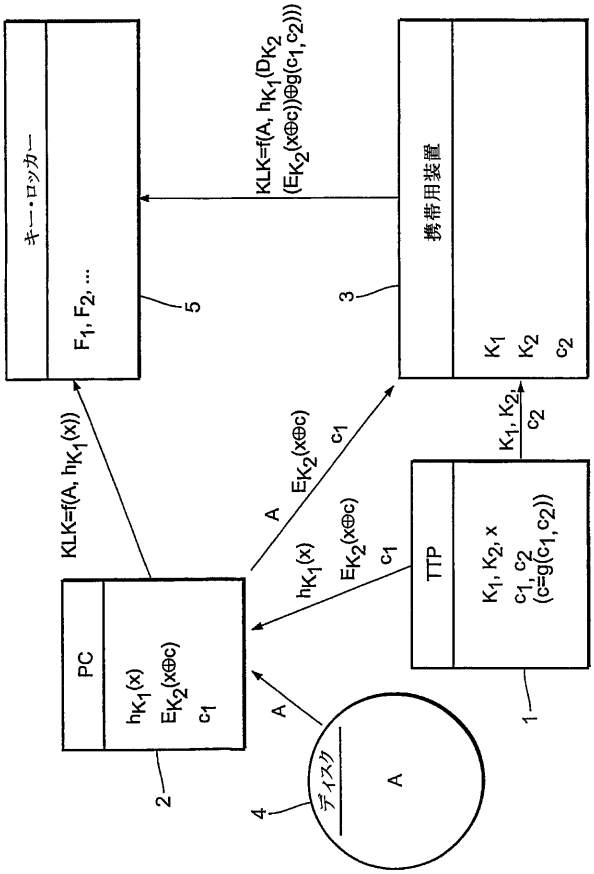
【図１】


キー・ロッカー
F1, F2, ...
5
KLK=f(A, hK1(DK2 (EK2(x))))
携帯用装置
3
K1
K2
KLK=f(A, hK1(x))
A
EK2(x)
hK1(x)
EK2(x)
K1, K2
(EK2(x))
PC
hK1(x)
EK2(x)
2
TTP
K1, K2, x
1
A
ディスク
4

【図２】


キー・ロッカー
F1, F2, ...
5
KLK=f(A, hK1(DK2 (EK2(x⊕c))⊕c))
携帯用装置
3
K1
K2
c
KLK=f(A, hK1(x))
A
EK2(x⊕c)
hK1(x)
EK2(x⊕c)
K1, K2, c
PC
hK1(x)
EK2(x⊕c)
2
TTP
K1, K2, x, c
1
A
ディスク
4

【図３】


キー・ロッカー
F1, F2, ...
5
KLK=f(A, hK1(DK2 (EK2(x⊕c)⊕g(c1,c2))))
携帯用装置
3
K1
K2
c2
KLK=f(A, hK1(x))
A
EK2(x⊕c)
c1
hK1(x)
EK2(x⊕c)
c1
K1, K2,
c2
PC
hK1(x)
EK2(x⊕c)
c1
2
TTP
K1, K2, x
c1, c2
(c=g(c1, c2))
1
A
ディスク
4

【国際調査報告】

INTERNATIONAL SEARCH REPORT

PCT/IB 03/00682

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 875 813 A (SONY CORP) 4 November 1998 (1998-11-04) page 2, line 7 - line 32 page 4, line 40 -page 8, line 30	1-13
Y	MENEZES, OORSCHOT, VANSTONE: "Handbook of applied cryptography, PASSAGE" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS, CRC PRESS, 1997, pages 498-499, 546-548, 551-553, XP002238742 BOCA RATON, FL, USA ISBN: 0-8493-8523-7 page 498 -page 499 page 546 -page 548 page 551 -page 553	1-13

-/--

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

° Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 April 2003	08/05/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Carnerero Álvaro, F

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

PCT/IB 03/00682

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,A	WO 02 095748 A (KONINKL PHILIPS ELECTRONICS NV) 28 November 2002 (2002-11-28) abstract	1-13

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

PCT/IL 03/00682

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0875813 A	04-11-1998	JP 10301492 A	13-11-1998
		EP 1298517 A1	02-04-2003
		EP 0875813 A2	04-11-1998
		TW 379308 B	11-01-2000
		US 6256391 B1	03-07-2001
WO 02095748 A	28-11-2002	WO 02095748 A2	28-11-2002
		US 2003007437 A1	09-01-2003

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,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,IT,LU,MC,NL,PT,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,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(74)代理人 100107766
弁理士 伊東 忠重
(72)発明者 テュイルス, ピム テー
オランダ国, ５６５６ アーアー アインドーフェン, プロフ・ホルストラーン ６
(72)発明者 スターリング, アントニウス アー エム
オランダ国, ５６５６ アーアー アインドーフェン, プロフ・ホルストラーン ６
Ｆターム(参考) 5J104 EA17 EA18 EA26

【要約の続き】
3）に前記暗号値（E）のうちの少なくとも１つを送出するように適合された装置（3）に前記アクセス鍵（K1、K2）を格納し、前記装置（3）が前記キー・ロッカー鍵（KLK）を計算することを可能にするステップとを有する方法が提案される。