(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5248153号
(P5248153)

(45)発行日　平成25年7月31日(2013.7.31)　(24)登録日　平成25年4月19日(2013.4.19)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601B
G06K 17/00	(2006.01)	H04L	9/00	601E
G06K 19/07	(2006.01)	G06K	17/00	S
		G06K	19/00	N

請求項の数 25　(全 19 頁)

(21)出願番号　特願2008-66756(P2008-66756)
(22)出願日　平成20年3月14日(2008.3.14)
(65)公開番号　特開2009-225062(P2009-225062A)
(43)公開日　平成21年10月1日(2009.10.1)
審査請求日　平成23年3月11日(2011.3.11)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100089118
弁理士　酒井　宏明
(72)発明者　加藤　拓
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　佐藤　順
東京都港区芝浦一丁目１番１号　株式会社東芝内
(72)発明者　松川　伸一
東京都港区芝浦一丁目１番１号　東芝ソリューション株式会社内

最終頁に続く

(54)【発明の名称】情報処理装置、方法及びプログラム

(57)【特許請求の範囲】
【請求項１】
各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第２秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第２鍵管理情報と、前記各情報処理装置に対して割り当てられる装置秘密鍵のうちの少なくとも１つである第２装置秘密鍵とを記憶する他の情報処理装置と相互認証を行う情報処理装置であって、
前記各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第１秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第１鍵管理情報と、前記複数の装置秘密鍵のうちの少なくとも１つである第１装置秘密鍵とを記憶する記憶手段と、
前記第１鍵管理情報に含まれる暗号化秘密鍵セットのうち、前記第１装置秘密鍵によって復号可能な少なくとも１つの暗号化秘密鍵の特定に利用する指定情報を、前記他の情報処理装置に送信する第１送信手段と、
前記第２鍵管理情報に含まれる暗号化秘密鍵セットのうち、前記指定情報により特定される暗号化秘密鍵を、前記他の情報処理装置から受信する受信手段と、
前記受信手段が受信した暗号化秘密鍵を前記第１装置秘密鍵で復号することにより、前記第２鍵管理情報に秘匿状態で含まれる前記第２秘密鍵を取得する取得手段と、
前記第２秘密鍵を用いて、前記他の情報処理装置と認証処理を行う認証手段とを備えることを特徴とする情報処理装置。

【請求項２】
前記第１送信手段は、前記指定情報と、前記第１鍵管理情報とを前記他の情報処理装置に送信し、
前記受信手段は、前記第１送信手段が送信した前記第１鍵管理情報と、前記他の情報処理装置が記憶する前記第２鍵管理情報との新旧に応じて、前記指定情報によって特定される暗号化秘密鍵を受信する
ことを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記第１送信手段は、前記指定情報と、新旧を比較可能な比較管理情報を含む前記第１鍵管理情報とを前記他の情報処理装置に送信する
ことを特徴とする請求項２に記載の情報処理装置。
【請求項４】
前記第２秘密鍵を用いて、前記受信手段が受信した暗号化秘密鍵を変換して応答データを生成する生成手段と、
前記応答データを前記他の情報処理装置に送信する第２送信手段とを更に備える
ことを特徴とする請求項１乃至３のいずれか一項に記載の情報処理装置。
【請求項５】
前記受信手段は、前記応答データに応じて、前記他の情報処理装置から、前記第２鍵管理情報の全てを更に受信する
ことを特徴とする請求項４に記載の情報処理装置。
【請求項６】
前記第１装置秘密鍵は、前記第１鍵管理情報に含まれる暗号化秘密鍵セットのうちの少なくとも１つを復号可能であって、
前記第１送信手段は、前記指定情報と、前記第１鍵管理情報とを前記他の情報処理装置に送信する
ことを特徴とする請求項４又は５に記載の情報処理装置。
【請求項７】
前記受信手段は、前記応答データに応じて、前記他の情報処理装置から、前記第２鍵管理情報の全て又は一部を更に受信し、
前記記憶手段によって記憶される前記第１鍵管理情報を、前記第２鍵管理情報に置き換える第１置換手段を更に備える
ことを特徴とする請求項６に記載の情報処理装置。
【請求項８】
前記受信手段が受信した暗号化秘密鍵が、前記第２鍵管理情報に含まれる暗号化秘密鍵セットのうちの少なくとも１つと一致するか否かを判断する判断手段を更に備え、
前記第１置換手段は、前記判断手段の判断の結果が肯定的である場合、前記記憶手段に記憶される前記第１鍵管理情報を、前記第２鍵管理情報に置き換える
ことを特徴とする請求項７に記載の情報処理装置。
【請求項９】
前記認証手段は、前記判断手段の判断の結果が否定的である場合、前記認証処理を中断する
ことを特徴とする請求項８に記載の情報処理装置。
【請求項１０】
前記記憶手段は、前記情報処理装置を一意に識別可能な第１識別情報を更に記憶しており、
各情報処理装置には、装置秘密鍵が一意に割り当てられており、
前記第１送信手段は、前記指定情報と、前記第１鍵管理情報と、前記第１識別情報とを、前記他の情報処理装置に送信し、
前記生成手段は、前記第１秘密鍵と前記第１識別情報とを用いて秘密固有鍵を生成し、
前記秘密固有鍵を用いて前記受信手段が受信した暗号化秘密鍵を変換して応答データを

生成する
ことを特徴とする請求項４乃至９のいずれか一項に記載の情報処理装置。
【請求項１１】
前記記憶手段は、前記情報処理装置を一意に識別可能な第１識別情報と、前記第１鍵管理情報と前記第１識別情報を用いて生成される秘密固有鍵とを更に記憶しており、
前記判断手段の判断の結果が肯定的である場合、前記記憶手段によって記憶された前記秘密固有鍵を、前記第２鍵管理情報と前記第１識別情報とを用いて生成される秘密固有鍵に置き換える第２置換手段を更に備える
ことを特徴とする請求項４乃至９のいずれか一項に記載の情報処理装置。
【請求項１２】
前記認証手段は、前記秘密固有鍵を用いて、前記認証処理を行う
ことを特徴とする請求項１０又は１１に記載の情報処理装置。
【請求項１３】
各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第２秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第２鍵管理情報と、前記各情報処理装置に対して割り当てられる装置秘密鍵のうちの少なくとも１つである第２装置秘密鍵とを記憶する他の情報処理装置と相互認証を行う情報処理装置であって、
前記各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第１秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第１鍵管理情報と、前記各情報処理装置に対して割り当てられる装置秘密鍵のうちの少なくとも１つである第１装置秘密鍵とを記憶する記憶手段と、
前記第１鍵管理情報に含まれる暗号化秘密鍵セットのうち、第２装置秘密鍵によって復号可能な少なくとも１つの暗号化秘密鍵を特定する指定情報を、前記他の情報処理装置から受信する受信手段と、
前記第１鍵管理情報に含まれる暗号化秘密鍵セットのうち、前記指定情報により特定される暗号化秘密鍵を前記他の情報処理装置へ送信する第１送信手段と、
前記第１秘密鍵に基づいて、前記他の情報処理装置と暗号通信を行うための認証処理を行う認証手段とを備える
ことを特徴とする情報処理装置。
【請求項１４】
前記受信手段は、前記指定情報と、前記他の情報処理装置が利用可能な前記第２鍵管理情報とを前記他の情報処理装置から受信し、
前記受信手段が受信した前記第２鍵管理情報と、前記記憶手段に記憶された前記第１鍵管理情報との新旧を比較する第１比較手段を更に備え、
前記第１送信手段は、前記第１比較手段の比較結果に応じて、前記記憶手段によって記憶された前記第１鍵管理情報に含まれる暗号化秘密鍵セットの中から、前記指定情報によって特定される暗号化秘密鍵を前記他の情報処理装置に送信する
ことを特徴とする請求項１３に記載の情報処理装置。
【請求項１５】
前記受信手段は、前記指定情報に加え、前記他の情報処理装置が記憶する前記第２鍵管理情報と、を前記他の情報処理装置から受信する
ことを特徴とする請求項１４に記載の情報処理装置。
【請求項１６】
前記記憶手段は、新旧を比較可能な比較管理情報を含む前記第１鍵管理情報を記憶し、
前記受信手段は、前記指定情報と、新旧を比較可能な比較管理情報を含む前記第２鍵管理情報とを、前記他の情報処理装置から受信し、
前記第１比較手段は、前記受信手段が受信した前記第２鍵管理情報に含まれる比較管理情報と、前記記憶手段によって記憶された前記第１鍵管理情報に含まれる比較管理情報との新旧を比較することにより、前記第１鍵管理情報と前記第２鍵管理情報との新旧を比較

する
ことを特徴とする請求項１４又は１５に記載の情報処理装置。
【請求項１７】
前記第１比較手段による比較の結果、前記第２鍵管理情報が、前記第１鍵管理情報より新しい場合、前記第１鍵管理情報を前記第２鍵管理情報へ置き換える第１置換手段を更に備える
ことを特徴とする請求項１４乃至１６のいずれか一項に記載の情報処理装置。
【請求項１８】
前記受信手段は、前記第１秘密鍵を用いて前記第１鍵管理情報に含まれる暗号化秘密鍵セットのうちの、前記指定情報によって特定される暗号化秘密鍵を変換した応答データを前記他の情報処理装置から更に受信し、
前記第１装置秘密鍵を用いて、前記第１鍵管理情報に含まれる暗号化秘密鍵セットのうちの１つを復号することにより、前記第１秘密鍵を取得する取得手段と、
前記第１秘密鍵を用いて、前記第１送信手段が送信した暗号化秘密鍵を変換して変換データを生成する生成手段と、
前記変換データと、前記応答データとを比較する第２比較手段と、
前記第２比較手段による比較の結果、前記変換データと前記応答データとが一致する場合、前記記憶手段によって記憶され且つ前記第１送信手段が送信した暗号化秘密鍵を含む前記第１鍵管理情報の全てを前記他の情報処理装置に送信する第２送信手段とを更に備える
ことを特徴とする請求項14乃至１７のいずれか一項に記載の情報処理装置。
【請求項１９】
前記受信手段は、前記他の情報処理装置の前記指定情報に加え、前記他の情報処理装置が利用可能な前記第２鍵管理情報と、前記他の情報処理装置を一意に識別可能な第２識別情報とを前記他の情報処理装置から受信し、
前記生成手段は、前記取得手段が取得した前記第１秘密鍵及び前記第２識別情報を用いて秘密固有鍵を生成し、これを用いて、前記第１送信手段が送信した前記暗号化秘密鍵を変換した変換データを生成する
ことを特徴とする請求項１８に記載の情報処理装置。
【請求項２０】
前記記憶手段は、前記第１鍵管理情報、前記第１識別情報、及び前記第１装置秘密鍵を用いて生成される秘密固有鍵を記憶しており、
前記第１比較手段による比較の結果、前記受信手段が受信した前記第２鍵管理情報が、前記記憶手段によって記憶された前記第１鍵管理情報より新しい場合、前記記憶手段によって記憶された前記秘密固有鍵を、前記第２鍵管理情報及び前記第１識別情報を用いて生成される秘密固有鍵に置き換える第２置換手段を更に備える
ことを特徴とする請求項１９に記載の情報処理装置。
【請求項２１】
前記認証手段は、前記第１秘密鍵に基づいて生成された秘密固有鍵を用いて、前記認証処理を行う
ことを特徴とする請求項１９又は２０に記載の情報処理装置。
【請求項２２】
前記認証手段は、前記第２比較手段による比較の結果、前記変換データと前記応答データとが一致しない場合、前記認証処理を中断する
ことを特徴とする請求項１８乃至２１のいずれか一項に記載の情報処理装置。
【請求項２３】
各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第２秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第２鍵管理情報と、前記各情報処理装置に対して割り当てられる装置秘密鍵のうちの少なくとも１つである第２装置秘密鍵とを記憶する他の情報処理装置と相互認証

を行う情報処理装置で実現される情報処理方法であって、
前記情報処理装置は、前記各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第１秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第１鍵管理情報と、前記複数の装置秘密鍵のうちの少なくとも１つである第１装置秘密鍵とを記憶する記憶手段を備え、
前記第１鍵管理情報に含まれる暗号化秘密鍵セットのうち、前記第１装置秘密鍵によって復号可能な少なくとも１つの暗号化秘密鍵の特定に利用する指定情報を、前記他の情報処理装置に送信する送信ステップと、
前記第２鍵管理情報に含まれる暗号化秘密鍵セットのうち、前記指定情報により特定される暗号化秘密鍵を、前記他の情報処理装置から受信する受信ステップと、
前記受信ステップで受信した暗号化秘密鍵を前記第１装置秘密鍵で復号することにより、前記第２鍵管理情報に秘匿状態で含まれる前記第２秘密鍵を取得する取得ステップと、
前記秘密鍵に基づいて、前記他の情報処理装置と認証処理を行う認証ステップとを含むことを特徴とする情報処理方法。
【請求項２４】
各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第２秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第２鍵管理情報と、前記各情報処理装置に対して割り当てられる装置秘密鍵のうちの少なくとも１つである第２装置秘密鍵とを記憶する他の情報処理装置と相互認証を行う情報処理装置で実行される情報処理プログラムであって、
前記情報処理装置は、前記各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第１秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第１鍵管理情報と、前記複数の装置秘密鍵のうちの少なくとも１つである第１装置秘密鍵とを記憶する記憶手段を備え、
前記第１鍵管理情報に含まれる暗号化秘密鍵セットのうち、前記第１装置秘密鍵によって復号可能な少なくとも１つの暗号化秘密鍵の特定に利用する指定情報を、前記他の情報処理装置に送信する送信ステップと、
前記第２鍵管理情報に含まれる暗号化秘密鍵セットのうち、前記指定情報により特定される暗号化秘密鍵を、前記他の情報処理装置から受信する受信ステップと、
前記受信ステップで受信した暗号化秘密鍵を前記第１装置秘密鍵で復号することにより、前記第２鍵管理情報に秘匿状態で含まれる前記第２秘密鍵を取得する取得ステップと、
前記秘密鍵に基づいて、前記他の情報処理装置と認証処理を行う認証ステップとを含むことを特徴とする情報処理プログラム。
【請求項２５】
各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第２秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第２鍵管理情報と、前記各情報処理装置に対して割り当てられる装置秘密鍵のうちの少なくとも１つである第２装置秘密鍵とを記憶する他の情報処理装置と相互認証を行う情報処理装置であって、前記各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第１秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第１鍵管理情報と、前記各情報処理装置に対して割り当てられる装置秘密鍵のうちの少なくとも１つである第１装置秘密鍵とを記憶する記憶手段を備える情報処理装置で実行される情報処理プログラムであって、
前記第１鍵管理情報に含まれる暗号化秘密鍵セットのうち、第２装置秘密鍵によって復号可能な少なくとも１つの暗号化秘密鍵を特定する指定情報を、前記他の情報処理装置から受信する受信ステップと、
前記第１鍵管理情報に含まれる暗号化秘密鍵セットのうち、前記指定情報により特定される暗号化秘密鍵を前記他の情報処理装置へ送信する送信ステップと、
前記秘密鍵に基づいて、前記他の情報処理装置と認証処理を行う認証ステップとを含むことを特徴とする情報処理プログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、不正な機器や不正な記憶媒体を無効化するために更新され得る鍵管理情報を用いて相互認証を行う情報処理装置、方法及びプログラムに関する。
【背景技術】
【０００２】
従来より、ＳＤカードでは、読み書きされるコンテンツを保護するための仕組みとして、Content Protection for Recordable Media（ＣＰＲＭ）と呼ばれるコンテンツ保護技術が採用されている。また、コンテンツを保護するための暗号化に用いられる暗号化鍵などの管理情報をＳＤカードに読み書きするための仕組みとして、認証方式が採用されている。ＳＤカードでは、不正機器を無効化するための仕組みとして、ＭＫＢ（Media Key Block）と呼ばれる鍵管理情報を利用する技術が採用されている。不正機器とは、コンテンツ保護技術によりコンテンツに施されている保護を取り外したり、コンテンツの改竄を行ったり、あるいはコンテンツの改竄が可能となっていたりする機器のことである。鍵管理情報は、これを技術ライセンス団体が発行する時点で不正機器として認知されている機器において、ＳＤカード等の記憶媒体に記憶された暗号化コンテンツを復号できなくすること（不正機器の無効化又は不正機器の排除）を実現するための管理情報である。具体的には、鍵管理情報とは、特定のメディア鍵が複数の異なるデバイス鍵で各々暗号化された複数の暗号化メディア鍵を含むものである。メディア鍵とは、通信を行う双方の機器や記憶媒体において認証に用いられる鍵情報である。デバイス鍵とは、各機器や各記憶媒体に対して一意に割り当てられた鍵情報であり、少なくとも１つのデバイス鍵が機器や記憶媒体に各々記憶される。この秘密鍵で復号されるメディア鍵を無効にする新たな鍵管理情報を生成してこれを用いて相互認証を行うことにより、不正機器に対する認証が成功しなくなる。この結果、不正機器を無効化することができる。従って、利用される鍵管理情報は、記憶媒体の製造時点において判明している不正機器の情報を反映した最新のものでなければ、不正機器の無効化が健全且つ効率的に実現されなくなってしまう。このため、ＳＤカードでは、鍵管理情報をより新しいものに更新するための仕組みも導入されている。
【０００３】
ＳＤカードは、ＤＶＤ（Digital Versatile Disc）等の光磁気ディスクとは異なり、データの記憶のためのフラッシュメモリ以外に、コントローラが内蔵されている。このコントローラにより、不正機器ではない正当な機器でしか暗号化鍵や鍵管理情報などのデータの書き込みや読み出しをできないようにするための相互認証が情報処理装置との間で行われる。一方、ＨＤ ＤＶＤ(High Definition DVD)やBlu-ray Discでは、Advanced Access Content System（ＡＡＣＳ）というコンテンツ保護技術が採用されている（例えば非特許文献１参照）。この技術では、目的と名称こそ同じＭＫＢと呼ばれているがデータ構造の全く異なる鍵管理情報が利用されている。
【０００４】
【非特許文献１】Advanced Access Content System（ＡＡＣＳ）(http://www.aacsla.com/specifications/specs091/ＡＡＣＳ_Spec_Common_0.91.pdf)
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかし、このようなＣＰＲＭやＡＡＣＳなどで利用されているコンテンツ保護技術において、不正に製造された記憶媒体を無効化することは実際には容易ではない。例えば、記憶媒体に記憶された秘密鍵を特定することにより、不正に作成された機器や記憶媒体を無効化することができるが、不正に作成された機器や記憶媒体が保有する秘密鍵を特定することは困難であるからである。このため、不正に製造された機器や記憶媒体を効率的に無効化することが望まれていた。
【０００６】

本発明は、上記に鑑みてなされたものであって、記憶媒体における処理負担を増大させずに、不正に製造された機器や記憶媒体を効率的に無効化することが可能な情報処理装置、方法及びプログラムを提供することを目的とする。

【課題を解決するための手段】

【０００７】

本発明は、各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第２秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第２鍵管理情報と、前記各情報処理装置に対して割り当てられる装置秘密鍵のうちの少なくとも１つである第２装置秘密鍵とを記憶する他の情報処理装置と相互認証を行う情報処理装置であって、前記各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第１秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第１鍵管理情報と、前記複数の装置秘密鍵のうちの少なくとも１つである第１装置秘密鍵とを記憶する記憶手段と、前記第１鍵管理情報に含まれる暗号化秘密鍵セットのうち、前記第１装置秘密鍵によって復号可能な少なくとも１つの暗号化秘密鍵の特定に利用する指定情報を、前記他の情報処理装置に送信する第１送信手段と、前記第２鍵管理情報に含まれる暗号化秘密鍵セットのうち、前記指定情報により特定される暗号化秘密鍵を、前記他の情報処理装置から受信する受信手段と、前記第１受信手段が受信した暗号化秘密鍵を前記第１装置秘密鍵で復号することにより、前記第２鍵管理情報に秘匿状態で含まれる前記第２秘密鍵を取得する取得手段と、前記第２秘密鍵を用いて、前記他の情報処理装置と認証処理を行う認証手段とを備えることを特徴とする。

【０００８】

また、本発明は、各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第２秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第２鍵管理情報と、前記各情報処理装置に対して割り当てられる装置秘密鍵のうちの少なくとも１つである第２装置秘密鍵とを記憶する他の情報処理装置と相互認証を行う情報処理装置であって、前記各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第１秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第１鍵管理情報と、前記各情報処理装置に対して割り当てられる装置秘密鍵のうちの少なくとも１つである第１装置秘密鍵とを記憶する記憶手段と、前記第１鍵管理情報に含まれる暗号化秘密鍵セットのうち、第２装置秘密鍵によって復号可能な少なくとも１つの暗号化秘密鍵を特定する指定情報を、前記他の情報処理装置から受信する受信手段と、前記第１鍵管理情報に含まれる暗号化秘密鍵セットのうち、前記指定情報により特定される暗号化秘密鍵を前記他の情報処理装置へ送信する第１送信手段と、前記第１秘密鍵に基づいて、前記他の情報処理装置と暗号通信を行うための認証処理を行う認証手段とを備えることを特徴とする。

【０００９】

また、本発明は、各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第２秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第２鍵管理情報と、前記各情報処理装置に対して割り当てられる装置秘密鍵のうちの少なくとも１つである第２装置秘密鍵とを記憶する他の情報処理装置と相互認証を行う情報処理装置で実現される情報処理方法であって、前記情報処理装置は、前記各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第１秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第１鍵管理情報と、前記複数の装置秘密鍵のうちの少なくとも１つである第１装置秘密鍵とを記憶する記憶手段を備え、前記第１鍵管理情報に含まれる暗号化秘密鍵セットのうち、前記第１装置秘密鍵によって復号可能な少なくとも１つの暗号化秘密鍵の特定に利用する指定情報を、前記他の情報処理装置に送信する送信ステップと、前記第２鍵管理情報に含まれる暗号化秘密鍵セットのうち、前記指定情報により特定される暗号化秘密鍵を、前記他の情報処理装置から受信する受信ステップと、前記受信ステ

ップで受信した暗号化秘密鍵を前記第１装置秘密鍵で復号することにより、前記第２鍵管理情報に秘匿状態で含まれる前記第２秘密鍵を取得する取得ステップと、前記秘密鍵に基づいて、前記他の情報処理装置と認証処理を行う認証ステップとを含むことを特徴とする。

【００１０】

また、本発明は、各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第２秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第２鍵管理情報と、前記各情報処理装置に対して割り当てられる装置秘密鍵のうちの少なくとも１つである第２装置秘密鍵とを記憶する他の情報処理装置と相互認証を行う情報処理装置で実行される情報処理プログラムであって、前記情報処理装置は、前記各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第１秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第１鍵管理情報と、前記複数の装置秘密鍵のうちの少なくとも１つである第１装置秘密鍵とを記憶する記憶手段を備え、前記第１鍵管理情報に含まれる暗号化秘密鍵セットのうち、前記第１装置秘密鍵によって復号可能な少なくとも１つの暗号化秘密鍵の特定に利用する指定情報を、前記他の情報処理装置に送信する送信ステップと、前記第２鍵管理情報に含まれる暗号化秘密鍵セットのうち、前記指定情報により特定される暗号化秘密鍵を、前記他の情報処理装置から受信する受信ステップと、前記受信ステップで受信した暗号化秘密鍵を前記第１装置秘密鍵で復号することにより、前記第２鍵管理情報に秘匿状態で含まれる前記第２秘密鍵を取得する取得ステップと、前記秘密鍵に基づいて、前記他の情報処理装置と認証処理を行う認証ステップとを含むことを特徴とする。

【００１１】

また、本発明は、各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第２秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第２鍵管理情報と、前記各情報処理装置に対して割り当てられる装置秘密鍵のうちの少なくとも１つである第２装置秘密鍵とを記憶する他の情報処理装置と相互認証を行う情報処理装置であって、前記各情報処理装置に対して割り当てられる装置秘密鍵の中から選択された複数の装置秘密鍵のそれぞれで暗号化された第１秘密鍵である暗号化秘密鍵を１つ以上含む暗号化秘密鍵セットを含む第１鍵管理情報と、前記各情報処理装置に対して割り当てられる装置秘密鍵のうちの少なくとも１つである第１装置秘密鍵とを記憶する記憶手段を備える情報処理装置で実行される情報処理プログラムであって、前記第１鍵管理情報に含まれる暗号化秘密鍵セットのうち、第２装置秘密鍵によって復号可能な少なくとも１つの暗号化秘密鍵を特定する指定情報を、前記他の情報処理装置から受信する受信ステップと、前記第１鍵管理情報に含まれる暗号化秘密鍵セットのうち、前記指定情報により特定される暗号化秘密鍵を前記他の情報処理装置へ送信する送信ステップと、前記秘密鍵に基づいて、前記他の情報処理装置と認証処理を行う認証ステップとを含むことを特徴とする。

【発明の効果】

【００１２】

本発明によれば、記憶媒体における処理負担を増大させずに、不正に製造された機器や記憶媒体を効率的に無効化することが可能になる。

【発明を実施するための最良の形態】

【００１３】

以下に添付図面を参照して、この発明にかかる情報処理装置、方法及びプログラムの最良な実施の形態を詳細に説明する。

【００１４】

（１）構成

本実施の形態においては、ＡＡＣＳなどで利用しているＭＫＢを鍵管理情報として用いる。また、相互認証を行う２つの情報処理装置として、ＳＤカードのようにコントローラ

とセキュリティ機能としてアクセス制限の掛けられた記憶領域とを有するメモリカードと、当該メモリカードにデータを読み書きするアプリケーションを実行するホストとを例にして説明する。

【００１５】

ホストは、装置全体を制御するＣＰＵ（Central Processing Unit）等の制御装置と、各種データや各種アプリケーション等の各種プログラムを記憶するＲＯＭ（Read Only Memory）やＲＡＭ（Random Access Memory）等の記憶装置とこれらを接続するバスとを少なくとも備えており、通常のコンピュータを利用したハードウェア構成となっている。また、ホストには、情報を表示する表示装置と、ユーザの指示入力を受け付けるキーボードやマウス等の入力装置と、外部装置の通信を制御する通信Ｉ／Ｆ（interface）とが有線又は無線により各々接続される。一方、メモリカードは、ＣＰＵ、ＲＯＭ及びＲＡＭを有するコントローラと、各種データや各種プログラムを記憶領域とを有する。

【００１６】

図１は、本実施の形態にかかるホストとメモリカードとの構成の概要を示す図である。まず、鍵管理情報の使用に関連して、メモリカード５０に記憶されるデータ及びホスト１００に記憶されるデータについて各々説明する。メモリカード５０は、記憶領域として、更新可能メモリ５１と、更新不可メモリ５２と、アクセス制限の掛けられた記憶領域（図示せず）とを有する。更新可能メモリ５１は、データを更新可能に記憶する記憶領域である。更新可能メモリ５１には、MKB_cと、メディアユニーク鍵Kmu_cとが記憶されている。更新不可メモリ５２は、データを更新不能に記憶する記憶領域である。更新不可メモリ５２には、メディアＩＤと、デバイス鍵セットと、デバイス情報番号Device-info（device-node）とが記憶される。メディアＩＤとは、メモリカード５０を一意に識別可能な媒体識別情報であり、識別情報に相当する。MKB_cは、複数のデバイス鍵のそれぞれで暗号化されたメディア鍵（秘密鍵）である複数の暗号化メディア鍵（暗号化秘密鍵）を含む鍵管理情報である。デバイス鍵セットは、メモリカード５０やホスト１００などの各情報処理装置に対して割り当てられた鍵情報であり、暗号化メディア鍵を復号可能なデバイス鍵を少なくとも１つ含む鍵情報であり、装置秘密鍵に相当する。尚、ここでは、デバイス鍵セットは、各情報処理装置に対して一意に割り当てられているものとする。デバイス情報番号は、デバイス鍵セットを識別可能なインデックス情報である。デバイス情報番号は、指定情報に相当し、ＭＫＢに含まれる暗号化メディア鍵を特定するために用いられる。暗号化メディアユニーク鍵は、メディアＩＤを用いてメディア鍵が暗号化されたものであり、秘密固有鍵に相当する。

【００１７】

尚、ここでは、鍵管理情報について、メモリカード５０が記憶しているものと、ホスト１００が記憶しているものとを区別する必要がある場合には、前者をMKB_cと記載し、後者をMKB_Hと記載し、これらを区別する必要がない場合には単にＭＫＢと記載する。また、デバイス鍵セットについて、メモリカード５０が記憶しているものと、ホスト１００が記憶しているものとを区別する必要がある場合には、前者を$Kd_{c\ i}$と記載し、後者を$Kd_{H\ i}$と記載する。また、メディア鍵について、MKB_cに基づいて復号されるものと、MKB_Hに基づいて復号されるものとを区別する必要がある場合には、前者をKm_cと記載し、後者をKm_Hと記載し、これらを区別する必要がない場合には単にＫｍと記載する。また、メディアユニーク鍵について、MKB_cに基づいて生成されるものと、MKB_Hに基づいて生成されるものとを区別する必要がある場合には、前者をKmu_cと記載し、後者をKmu_Hと記載し、これらを区別する必要がない場合には単にＫｍｕと記載する。

【００１８】

ここで、ＭＫＢのデータ構成について図２を用いて説明する。同図に示されるように、ＭＫＢは、バージョン番号と、メディア鍵検証用レコードと、複数の暗号化メディア鍵とを含む。バージョン番号は、ＭＫＢのバージョンを示し、ＭＫＢの新旧を比較可能な情報（比較管理情報）である。メディア鍵検証用レコードは、メモリカード５０がホスト１０

０からＭＫＢを受け取った場合に当該ＭＫＢを検証するために用いられる。具体的には、メディア鍵検証用レコードは、固定データ（例えば、‘０１２３４ＸＸＸ’などの数列）をメディア鍵Ｋｍで暗号化したものである。固定データはメモリカード５０に別途予め記憶される。暗号化メディア鍵は、１つのディスク情報番号又はディスク情報番号のグループ毎に、１つずつレコードが分かれてＭＫＢに含まれる。例えば、ディスク情報番号‘１’に対応する１つの暗号化メディア鍵と、ディスク情報番号‘１００’～‘１９９’に対応する１つの暗号化メディア鍵とが別々のレコードして含まれる。各ディスク情報番号には上述したようにデバイス鍵セットが対応しているから、各暗号化メディア鍵は、ディスク情報番号に対応するデバイス鍵セットに含まれるデバイス鍵の１つによって復号可能である。

【００１９】

図１の説明に戻る。ホスト１００は、メモリカード５０と同様に、更新可能メモリ１０１と、更新不可メモリ１０２とを有する。更新可能メモリ１０１には、MKB_Hが記憶される。このMKB_Hは、ホスト１００で実行されるアプリケーションの製造（或いは出荷）時にホスト１００に書き込まれるようにしても良いし、出荷後にネットワークや他のメディアを使ってホスト１００に配布されるようにしても良い。更新不可メモリ１０２には、更新可能メモリ１０１に記憶されたMKB_Hを復号するために必要なデバイス鍵セット$Kd_{h\ i}$が記憶される。

【００２０】

次に、上述のハードウェア構成において、メモリカード５０においてＣＰＵがＲＯＭや記憶領域に記憶された各種プログラムを実行することにより実現される各種機能のうち本実施の形態に特有の機能について説明する。尚、ここでは、メモリカード５０は、利用可能な鍵管理情報として、更新可能メモリ５１に記憶されているMKB_cを用いるものとする。メモリカード５０は、送信部５３と、復号部５４と、一方向性関数部５５と、一方向性関数部５６と、ＭＫＢ検証・更新部５７と、認証及び鍵交換実行部５８との各機能を実現させる。送信部５３は、更新可能メモリ５１に記憶されているMKB_cと、更新不可メモリ５２に記憶されているメディアＩＤ及びデバイス情報番号とをホスト１００に送る。復号部５４は、MKB_cがホスト１００に記憶されているMKB_Hより古い場合、MKB_Hの一部のレコードであって、自身のデバイス情報番号によって特定される暗号化メディア鍵、即ち、自身のデバイス情報番号によって識別されるデバイス鍵セット$Kd_{c\ i}$に対応した暗号化メディア鍵をホスト１００から受け取る。そして、復号部５４は、受け取った暗号化メディア鍵を、デバイス鍵セット$Kd_{c\ i}$に含まれるデバイス鍵のうち１つのデバイス鍵を用いて復号して、メディア鍵Km_Hを求める。一方向性関数部５５は、メディアＩＤを用いてメディア鍵Km_Hを一方向性関数演算により変換して、メディアユニーク鍵Kmu_Hを求める。一方向性関数部５６は、メディアユニーク鍵Kmu_Hを用いて、復号部５４が受け取った暗号化メディア鍵を一方向性関数演算により変換して応答データＫｒｃを生成し、これをホスト１００に送る。ＭＫＢ検証・更新部５７は、ホスト１００での検証結果に応じてMKB_Hの全てをホスト１００から受け取り、これを検証する。そして、ＭＫＢ検証・更新部５７は、当該検証結果に応じて、更新可能メモリ５１に記憶されたMKB_cをMKB_Hに置き換えると共に、更新可能メモリ５１に記憶されたメディアユニーク鍵Kmu_cを、一方向性関数部５５がMKB_Hから求めたメディアユニーク鍵Kmu_Hに置き換える。認証及び鍵交換実行部５８は、ホスト１００と共有されるメディアユニーク鍵Ｋｍｕを用いて、暗号通信を行うための認証及び鍵交換処理を実行する。

【００２１】

次に、ホスト１００の制御装置が記憶装置や外部記憶装置に記憶された各種プログラムを実行することにより実現される各種機能のうち本実施の形態に特有の機能について説明する。ホスト１００は、ＭＫＢ検証・更新部１０３と、ＭＫＢ処理部１０４と、一方向性関数部１０５と、指定レコード選択処理部１０６と、一方向性関数部１０７と、データ検証処理部１０８と、認証及び鍵交換実行部１０９との各機能を実現させる。ＭＫＢ検証・更新部１０３は、MKB_c、メディアＩＤ及びデバイス情報番号をメモリカード５０から

受け取ると、更新不可メモリ１０２に記憶されているデバイス鍵セット$Kd_{H\,i}$を用いてMKB_cの正当性を検証する。また、ＭＫＢ検証・更新部１０３は、MKB_cと、更新可能メモリ１０１に記憶されているMKB_Hとの新旧を比較する。MKB_Hの方が古い場合、ＭＫＢ検証・更新部１０３は、更新可能メモリ１０１に記憶されているMKB_HをMKB_cに置き換える。一方、MKB_Hの方が新しい場合、ＭＫＢ検証・更新部１０３は、デバイス情報番号を指定レコード選択処理部１０６に送る。

【００２２】

指定レコード選択処理部１０６は、更新可能メモリ１０１に記憶されているMKB_Hの一部のレコードであって、ＭＫＢ検証・更新部１０３から受け取ったデバイス情報番号によって特定される暗号化メディア鍵、即ち、当該デバイス情報番号によって識別されるデバイス鍵セット$Kd_{c\,i}$に対応した暗号化メディア鍵をメモリカード５０に送る。ＭＫＢ処理部１０４は、指定レコード選択処理部１０６がメモリカード５０に送った暗号化メディア鍵を、更新不可メモリ１０２に記憶されているデバイス鍵セット$Kd_{H\,i}$に含まれるデバイス鍵の１つを用いて復号して、メディア鍵Km_Hを求める。一方向性関数部１０５は、メモリカード５０から受け取ったメディアＩＤを用いて、ＭＫＢ処理部１０４が求めたメディア鍵Km_Hを一方向性関数演算により変換して、メディアユニーク鍵Kmu_Hを求める。一方向性関数部１０６は、一方向性関数部１０５が求めたメディアユニーク鍵Kmu_Hを用いて、指定レコード選択処理部１０６がメモリカード５０に送った暗号化メディア鍵を一方向性関数演算により変換して、変換データＫｒｈを求める。データ検証処理部１０８は、指定レコード選択処理部１０６が行った暗号化メディア鍵の送信に応答してメモリカード５０から応答データＫｒｃを受け取ると、応答データＫｒｃと、変換データＫｒｈとを比較することにより、当該応答データＫｒｃを検証する。そして、データ検証処理部１０８は、当該検証結果に応じて、MKB_Hの全てをメモリカード５０に送る。

【００２３】

（２）動作

次に、本実施の形態にかかるホスト１００とメモリカード５０とで行う処理の手順について図３を用いて説明する。メモリカード５０は、自身に記憶されているMKB_c、メディアＩＤ及びデバイス情報番号をホスト１００に送る（ステップＳ１）。ホスト１００は、MKB_c、メディアＩＤ及びデバイス情報番号をメモリカード５０から受け取ると（ステップＳ２）、更新不可メモリ１０２に記憶されているデバイス鍵セット$Kd_{H\,i}$を用いてMKB_cの正当性を検証すると共に、当該MKB_cと、更新可能メモリ１０１に記憶されているMKB_Hとの新旧を比較する（ステップＳ３～Ｓ４）。MKB_cの正当性は、デバイス鍵セットに含まれるデバイス鍵のうち１つを用いてMKB_Hを復号してメディア鍵Km_cを求めることにより行う。また、MKB_cとMKB_Hとの新旧の比較は、各々に含まれるバージョン番号を比較することにより行う。より新しいバージョン番号を含む方を新のＭＫＢとする。この比較の結果、MKB_cとMKB_Hとの新旧が同じである場合(ステップＳ４：ＮＯ，ステップＳ５：ＹＥＳ)、ホスト１００は、ステップＳ２で受け取ったメディアＩＤを用いて、ステップＳ３で求めたメディア鍵Km_cを一方向性関数演算により変換して、メディアユニーク鍵Kmu_cを求め（ステップＳ６）、ステップＳ１０に進む。MKB_Hの方が古い場合（ステップＳ４：ＮＯ，ステップＳ５：ＮＯ）、ホスト１００は、ステップＳ６と同様にしてメディアユニーク鍵Kmu_cを求めた後（ステップＳ７）、更新可能メモリ１０１に記憶されているMKB_HをMKB_cに置き換えて（ステップＳ８）、ステップＳ１０に進む。

【００２４】

MKB_Hの方が新しい場合（ステップＳ４：ＹＥＳ）、ホスト１００は、メモリカード５０に記憶されたMKB_cを更新する更新処理を行う（ステップＳ９）。図４は、更新処理の手順を示すフローチャートである。まず、ホスト１００は、MKB_Hの一部のレコードであって、ステップＳ２で受け取ったデバイス情報番号によって特定される暗号化メディア鍵、即ち、当該デバイス情報番号によって識別されるデバイス鍵セット$Kd_{c\,i}$に対応した暗号化メディア鍵をメモリカード５０に送る（ステップＳ２０）。メモリカード５

０は、暗号化メディア鍵を受け取ると（ステップＳ２１）、これを、更新不可メモリ５２に記憶されているデバイス鍵セット$Kd_{c\ i}$に含まれるデバイス鍵のうち１つを用いて復号して、メディア鍵Km_Hを求める。そして、メモリカード５０は、更新不可メモリ５２に記憶されているメディアＩＤを用いて、メディア鍵Km_Hを一方向性関数演算により変換して、メディアユニーク鍵Kmu_Hを求める（ステップＳ２２）。次いで、メモリカード５０は、ステップＳ２２で求めたメディアユニーク鍵Kmu_Hを用いて、ステップＳ２１で受け取った暗号化メディア鍵を一方向性関数演算により変換して応答データＫｒｃを生成し、これをホスト１００に送る（ステップＳ２３）。この応答データＫｒｃは、ホスト１００がステップＳ２０で送った暗号化メディア鍵に対してメモリカード５０がメディアユニーク鍵Kmu_Hを正しく求めたことをホスト１００に伝えるためのものである。ここでは、応答データＫｒｃは、ステップＳ２２で求めたメディア鍵Km_Hを知らなければ求めることができないデータであり、且つステップＳ２２で求めたメディア鍵Km_H又はメディアユニーク鍵Kmu_Hが第３者に露呈することのないデータでなければならないものとする。このため、ステップＳ２３では、応答データＫｒｃの生成にメディアユニーク鍵Kmu_Hを用いるものの、これを鍵とした一方向性関数を用いて、応答データＫｒｃを変換している。これにより、第３者に露呈することなく、ステップＳ２０で送った暗号化メディア鍵を正しく受信したことと、当該暗号化メディア鍵に対してメモリカード５０が求めたメディアユニーク鍵Kmu_Hを正しく求めたこととをホスト１００に伝えることができる。

【００２５】

一方、ホスト１００は、ステップＳ２０でメモリカード５０に送った暗号化メディア鍵を、更新可能メモリ１０１に記憶されているデバイス鍵セット$Kd_{H\ i}$に含まれるデバイス鍵のうち１つを用いて復号して、メディア鍵Km_Hを求める（ステップＳ２４）。そして、ホスト１００は、ステップＳ２でメモリカード５０から受け取ったメディアＩＤを用いてメディア鍵Km_Hを一方向性関数演算により変換して、メディアユニーク鍵Kmu_Hを求める。そして、ホスト１００は、メディアユニーク鍵Kmu_Hを用いて、ステップＳ２０でメモリカード５０に送った暗号化メディア鍵を一方向性関数演算により変換して、変換データＫｒｈを求める（ステップＳ２５）。そして、ホスト１００は、ステップＳ２３でメモリカード５０から送られた応答データＫｒｃを受け取ると（ステップＳ２６）、当該応答データＫｒｃを検証するために、応答データＫｒｃと、ステップＳ２４で求めた変換データＫｒｈとを比較する（ステップＳ２７）。これらが一致しない場合（ステップＳ２８：ＮＯ）、ホスト１００は、メモリカード５０が無効化されていた又は何らかのエラーが生じたと判断して、処理を終了する。応答データＫｒｃと、変換データＫｒｈとが一致する場合（ステップＳ２８：ＹＥＳ）、ホスト１００は、メモリカード５０が無効化されておらず正当なメモリカードであると判断して、ステップＳ２０で一部のレコードのみを送っていたMKB_Hについてその全てをメモリカード５０に送る（ステップＳ２９）。

【００２６】

一方、メモリカード５０は、MKB_Hを受け取ると（ステップＳ３０）、当該MKB_Hに含まれるメディア鍵検証用レコードを利用して、当該MKB_Hが、その一部のレコードとして、ステップＳ２１で受け取った暗号化メディア鍵を含むものであるか否かを検証する（ステップＳ３１）。即ち、メモリカード５０は、ステップＳ２１で受け取った暗号化メディア鍵が、ステップＳ３０で受け取ったMKB_Hに含まれる暗号化メディア鍵のうちの少なくとも１つとして送信されたものであるか否かを判断する。具体的には、メモリカード５０は、ステップＳ２１で受け取った暗号化メディア鍵から求めたメディア鍵Km_Hを用いてメディア鍵検証用レコードを復号して固定データを取得する。当該固定データが予め記憶しているものと一致する場合、メモリカード５０は、ステップＳ３０で受け取ったMKB_Hが、その一部のレコードとして、ステップＳ２１で受け取った暗号化メディア鍵を含むものであると判断する。この場合、ステップＳ３２の判断結果が肯定的となり、メモリカード５０は、更新可能メモリ５１に記憶されているMKB_cを、ステップＳ３０

で受け取ったＭＫＢ$_{H}$に置き換える。また、メモリカード５０は、ＭＫＢ$_{H}$に含まれる暗号化メディア鍵のうち、更新不可メモリ５２に記憶されているデバイス鍵セットＫｄ$_{c\ i}$に対応した暗号化メディア鍵を、当該デバイス鍵セットＫｄ$_{c\ i}$のうち１つのデバイス鍵を用いて復号して、メディア鍵Ｋｍ$_{H}$を求める。そして、メモリカード５０は、更新不可メモリ５２に記憶されているメディアＩＤを用いて、メディア鍵Ｋｍ$_{H}$を一方向性関数演算により変換して、メディアユニーク鍵Ｋｍｕ$_{H}$を求め、更新可能メモリ５１に記憶されているメディアユニーク鍵Ｋｍｕ$_{c}$をメディアユニーク鍵Ｋｍｕ$_{H}$に置き換える（ステップＳ３３）。尚、ステップＳ３２の判断結果が否定的である場合は、メモリカード５０は、何らかのエラーが生じたと判断して、処理を終了する。以上のようにして、ホスト１００とメモリカード５０とはＭＫＢ$_{H}$の更新処理を行う。

【００２７】

即ち、ＭＫＢ$_{H}$の方が新しい場合には、以上のような更新処理の結果、ホスト１００とメモリカード５０とはメディアユニーク鍵Ｋｍｕ$_{H}$を共有することになる。一方、ＭＫＢ$_{H}$の方が古い場合又はＭＫＢ$_{H}$とＭＫＢ$_{c}$との新旧が同じである場合、ステップＳ６の後に、ホスト１００とメモリカード５０とはメディアユニーク鍵Ｋｍｕ$_{c}$を共有していることになる。このような状況において、図３のステップＳ１０では、ホスト１００とメモリカード５０とは、共有するメディアユニーク鍵を用いて、暗号通信に用いるセッション鍵を生成するための認証及び鍵交換処理を行う。セッション鍵の生成には、従来のメモリカードで使われている鍵交換方式など様々な方式を利用することができる。認証及び鍵交換処理での認証が成功すると、ホスト１００は、メモリカード５０においてアクセス制限の掛けられた記憶領域へのデータの読み書きが可能になる。この記憶領域へのデータの読み書きの際に、ホスト１００とメモリカード５０とは、生成されたセッション鍵を用いて暗号通信を行うことになる。

【００２８】

尚、ＭＫＢ$_{c}$の方が新しい場合（ステップＳ４：ＮＯ，ステップＳ５：ＮＯ）、ステップＳ８でＭＫＢ$_{H}$がＭＫＢ$_{c}$に置き換えられるが、当該ＭＫＢ$_{c}$によってホスト１００が無効化されている場合には、ホスト１００がステップＳ７で求めたメディアユニーク鍵と、メモリカード５０が求めたメディアユニーク鍵とは一致しないことになる。この場合、ステップＳ１０での認証及び鍵交換処理での認証は成功しない。従って、この場合、無効化された不正なホストによって、メモリカード５０に対するデータの読み書きはできないことになる。

【００２９】

以上のように、ホスト１００だけでなく、コントローラを内蔵したメモリカード５０にも、ＭＫＢ（鍵管理情報）を復号するために必要なデバイス鍵を含むデバイス鍵セットを記憶する。そして、ホスト１００とメモリカード５０とが互いに自身が記憶しているデバイス鍵セットを用いて、ＭＫＢにより秘匿されているメディア鍵を復号する。更に、両者が、メディアＩＤを用いてメディア鍵を変換したメディユニーク鍵が一致した場合にのみ、相互認証を継続できるようにする。また、メモリカード５０に秘匿されているデバイス鍵セットを無効化したＭＫＢを、コンテンツ保護方式を管理する管理団体が効率的に生成可能にするための仕組みとして、ＭＫＢを復号する処理の一部をホスト１００に依頼する機能を追加する。これにより、正当に製造されたメモリカード５０をリバースエンジニアリングすることによって当該メモリカード５０に記憶されていたデバイス鍵セットを含む全ての情報を取り出し、取り出した情報を利用して不正なメモリカード(クローン記憶媒体)が製造された場合に、クローン記憶媒体に記憶されているデバイス鍵セットを管理団体が効率的に特定することができるようになる。

【００３０】

即ち、本実施の形態によれば、ＣＰＲＭやＡＡＣＳで実現されているように、不正機器を無効化する機能に加えて、メモリカードのような記憶媒体が不正に製造された場合に、当該不正な記憶媒体を効率的に無効化する機能を実現させることができる。

【００３１】

[変形例]
なお、本発明は前記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、前記実施形態に開示されている複数の構成要素の適宜な組み合わせにより、種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。さらに、異なる実施形態にわたる構成要素を適宜組み合わせてもよい。また、以下に例示するような種々の変形が可能である。

【００３２】
＜変形例１＞
上述した実施の形態において、ホスト１００又はメモリカード５０で実行される各種プログラムを、インターネット等のネットワークに接続されたコンピュータ上に格納し、ネットワーク経由でダウンロードさせることにより提供するように構成しても良い。また、ホスト１００は、ＣＤ－ＲＯＭ、フレキシブルディスク（ＦＤ）、ＣＤ－Ｒ、ＤＶＤ（Digital Versatile Disc）等のコンピュータで読み取り可能な記憶媒体からデータを読み出すドライブを備え、記憶媒体に記憶された各種プログラムを、当該ドライブを介して読み出してこれをインストールすることにより提供するように構成しても良い。

【００３３】
＜変形例２＞
上述した実施の形態において、相互認証を行う２つの情報処理装置として、ホスト１００と、メモリカード５０とを例にして説明した。しかし、相互認証を行う２つの情報処理装置はこれらに限らない。また、一方の情報処理装置としてメモリカード５０にＭＫＢ、デバイス鍵セット、メディアＩＤ及びメディアユニーク鍵が予め記憶される構成とした。しかし、当該一方の情報処理装置自体にこれらの情報が記憶されるのではなく、例えば、当該一方の情報処理装置はデバイス鍵を保有し、自身に着脱自在に装着され且つＭＫＢ、メディアＩＤ及びメディアユニーク鍵が記憶されている記憶媒体からこれらの情報を取得するようにしても良い。即ち、この場合、当該一方の情報処理装置は、利用可能な鍵管理情報として、記憶媒体に記憶されているＭＫＢを用いる。

【００３４】
また、相互認証を行う２つの情報処理装置は、ＤＶＤなどの光磁気ディスクにデータの読み書きを行うドライブと、ドライブを介して光磁気ディスクにデータの読み書きを行う情報処理装置（ＰＣにインストールされるアプリケーション）とであっても良い。この場合、より複製されやすいアプリケーションがインストールされる情報処理装置が上述のメモリカード５０と同様の機能を実現させ、ドライブが上述のホスト１００と同様の機能を実現させるようにする。このような構成においては、アプリケーションが秘匿しているデバイス鍵に対応したデバイス情報番号をドライブに送り、ドライブは光磁気ディスクに記録されているＭＫＢから受信したデバイス情報番号に対応した暗号化メディア鍵を取り出し、アプリケーション側に送り返すことになる。このような構成によれば、このアプリケーションを不正に複製した不正アプリケーションが出回った場合に、当該不正アプリケーションに記憶されているデバイス鍵セットを管理団体が特定できるようになる。

【００３５】
なお、ドライブは常に光磁気ディスクからＭＫＢを読み出すだけでなく、自身の不揮発性メモリにＭＫＢを記憶しておき、光磁気ディスクとアプリケーションとの両方から送られてくる各ＭＫＢを用いて不揮発性メモリ内のＭＫＢを最新の状態に更新しておくこともできる。

【００３６】
＜変形例３＞
上述した実施の形態において、メモリカード５０には、メディアユニーク鍵が記憶されるとしたが、これに限らず、メディア鍵が記憶されるようにしても良い。この場合、ステップメモリカード５０は、ステップＳ２２でメディアユニーク鍵を求めることなく、ステップＳ２３で、メディア鍵を用いて暗号化メディア鍵を変換して応答データＫｒｃを生成

してこれをホスト１００に送る。一方、ホスト１００は、ステップＳ２４で、メディアユニーク鍵を求めることなく、ステップＳ２５で、メディア鍵を用いて暗号化メディア鍵を変換して変換データＫｒｈを生成する。そして、ホスト１００は、応答データＫｒｃと変換データＫｒｈとを比較して、比較結果に応じて、$ＭＫＢ_{H}$の全てをメモリカード５０に送る。そして、ホスト１００は、メモリカード５０と共有されるメディア鍵を用いて、ステップＳ１０の認証及び鍵交換処理を行えば良い。このような構成によっても、不正なメモリカードに記憶されているデバイス鍵セットを管理団体が効率的に特定することができるようになる。

【００３７】

＜変形例４＞

上述した実施の形態において、ステップＳ２０ではホスト１００は、メディア鍵を暗号化した暗号化メディア鍵をメモリカード５０に送るようにしたが、これに限らず、例えばこのときホスト１００は、都度、乱数を発生させ、当該乱数及びメディア鍵をデバイス鍵で暗号化したデータ（暗号化データ）をメモリカード５０に送るようにしても良い。この場合、ホスト１００は、図５に示されるように、乱数発生器１１２を有する。指定レコード選択処理部１０６は、乱数発生器１１２が発生させた乱数、更新可能メモリ１０１に記憶された$ＭＫＢ_{H}$及びデバイス情報番号を用いて、暗号化データを生成してこれをメモリカード５０に送信する。このような構成によれば、このときホスト１００が、デバイス情報番号に対応する暗号化メディア鍵が同じであるメモリカード５０に対して送るデータを都度変更することができる。メモリカード５０がこのデータを上述と同様にメディアユニーク鍵で変換してホスト１００に送信する応答データも都度異なり得る。このため、ホスト１００は、メモリカード５０が応答データを不正に取得して送信したとしても、当該メモリカード５０が不正な機器であるとして、当該メモリカード５０にＭＫＢの全てを送信しないようにすることができる。尚、この場合、$ＭＫＢ_{H}$には、各レコードとして、メディア鍵及び乱数を各デバイス鍵で各々暗号化したものを予め含ませるようにしても良い。

【００３８】

又は、ホスト１００は、$ＭＫＢ_{H}$に含まれるバージョン番号及びメディア鍵をデバイス鍵で暗号化したデータをメモリカード５０に送るようにしても良い。この場合、$ＭＫＢ_{H}$には、各レコードとして、メディア鍵及びバージョン番号を各デバイス鍵で各々暗号化したものを予め含ませるようにしても良い。更に、ホスト１００は、乱数、$ＭＫＢ_{H}$に含まれるバージョン番号及びメディア鍵を暗号化したデータをメモリカード５０に送るようにしても良い。この場合、$ＭＫＢ_{H}$には、各レコードとして、乱数、バージョン番号及びメディア鍵を各デバイス鍵で各々暗号化したものを予め含ませるようにしても良い。

【００３９】

＜変形例５＞

上述した実施の形態において、ＭＫＢに含まれる新旧を比較可能な比較管理情報として、バージョン番号を用いたが、これに限らず、例えば、ＭＫＢの作成日付などであっても良い。

【００４０】

＜変形例６＞

上述した実施の形態において、$ＭＫＢ_{c}$と$ＭＫＢ_{H}$との新旧が同じである場合、ステップＳ６では、ホスト１００は、メディアユニーク鍵Ｋｍｕを、$ＭＫＢ_{c}$に基づいて求めたが、これに限らず、$ＭＫＢ_{H}$に基づいて求めても良い。

【００４１】

＜変形例７＞

上述した実施の形態において、メモリカード５０は、ステップＳ１で、デバイス情報番号を暗号化してホスト１００に送り、ホスト１００は、ステップＳ２０で、暗号化メディア鍵をメディアユニーク鍵$Ｋｍｕ_{c}$で暗号化してメモリカード５０に送るように構成しても良い。図６は、この場合のホスト１００とメモリカード５０との構成の概要を示す図である。同図に示されるように、ホスト１００は、暗号化部５９と、復号部６０との機能を

更に実現させる。暗号化部５９は、更新不可メモリ５２に記憶されているデバイス情報番号を、更新可能メモリ５１に記憶されているメディアユニーク鍵Kmu_cを用いて暗号化して送信部５３に送る。送信部５３は、当該暗号化されたデバイス情報番号（暗号化デバイス情報番号）と、更新可能メモリ５１に記憶されているMKB_cと、更新不可メモリ５２に記憶されているメディアＩＤとをホスト１００に送る。復号部６０は、メディアユニーク鍵Kmu_cで更に暗号化された暗号化メディア鍵である第２暗号化メディア鍵を受け取り、更新可能メモリ５１に記憶されているメディアユニーク鍵Kmu_cを用いて第２暗号化メディア鍵を復号して、暗号化メディア鍵を求め、これを復号部５４に送る。

【００４２】

一方、ホスト１００は、復号部１１０と、暗号化部１１１との各機能を更に実現させる。復号部１１０は、メモリカード５０から送られた暗号化バイス情報番号を、ＭＫＢ検証・更新部１０３がメモリカード５０から受け取ったMKB_cに基づいて一方向性関数部１０５が求めたメディアユニーク鍵Kmu_cを用いて復号して、デバイス情報番号を求めて、これを指定レコード選択処理部１０６に送る。指定レコード選択処理部１０６は、更新可能メモリ１０１に記憶されているMKB_Hの一部のレコードであって、復号部１１０から受け取ったデバイス情報番号によって識別されるデバイス鍵セット$Kd_{c\ i}$に対応した暗号化メディア鍵を暗号化部１１１に送る。暗号化部１１１は、指定レコード選択処理部１０６から受け取った暗号化メディア鍵を、ＭＫＢ検証・更新部１０３がメモリカード５０から受け取ったMKB_cに基づいて一方向性関数部１０５が求めたメディアユニーク鍵Kmu_cを用いて暗号化してこれをメモリカード５０に送る。

【００４３】

以上のような構成によれば、ホストとメモリカードとの間で通信される情報の秘匿性をより高めつつ、不正に製造されたメモリカードを効率的に無効化することが可能になる。

【００４４】

＜変形例８＞

上述した実施の形態において、メモリカード５０は、一方向性関数部５５，５６を備え、データの変換を一方向性関数演算により行ったが、これに限らず、データの変換をその他の演算により行う変換部を備えるようにしても良い。ホスト１００についても同様に、一方向性関数部１０５，１０７に限らず、データの変換をその他の演算により行う変換部を備えるようにしても良い。

【００４５】

＜変形例９＞

上述した実施の形態において、識別情報としてメディアＩＤを用いたが、これに限らず、識別情報は、情報処理装置を一意に識別可能な情報であれば良い。また、装置秘密鍵としてデバイス鍵を用いたが、これに限らず、装置秘密鍵は、各情報処理装置に対して割り当てられた鍵情報であれば良い。更に、指定情報としてデバイス情報番号を用いたが、これに限らず、指定情報は、ＭＫＢに含まれる暗号化メディア鍵を特定する情報であれば良い。

【図面の簡単な説明】

【００４６】

【図１】一実施の形態にかかるホストとメモリカードとの構成の概要を示す図である。

【図２】同実施の形態にかかるＭＫＢのデータ構成を例示する図である。

【図３】同実施の形態にかかるホスト１００とメモリカード５０とで行う処理の手順を示すフローチャートである。

【図４】同実施の形態にかかる更新処理の手順を示すフローチャートである。

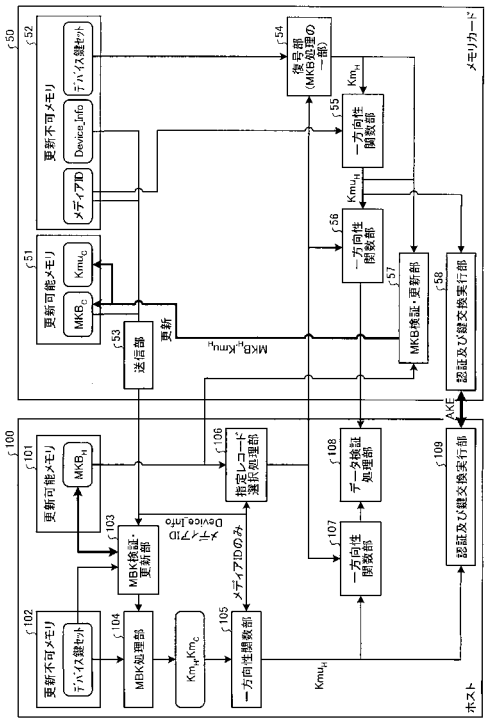
【図５】一実施の形態の一変形例にかかるホスト１００とメモリカード５０との構成の概要を示す図である。

【図６】一実施の形態の一変形例にかかるホスト１００とメモリカード５０との構成の概要を示す図である。

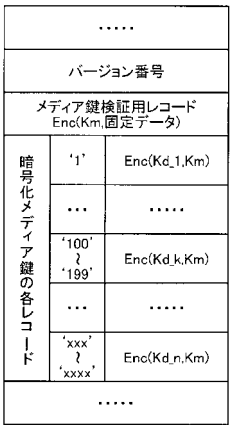
【符号の説明】

【００４７】
５０　メモリカード
５１　更新可能メモリ
５２　更新不可メモリ
５３　送信部
５４　復号部
５５　一方向性関数部
５６　一方向性関数部
５７　ＭＫＢ検証・更新部
５８　認証及び鍵交換実行部
５９　暗号化部
６０　復号部
１００　ホスト
１０１　更新可能メモリ
１０２　更新不可メモリ
１０３　ＭＫＢ検証・更新部
１０４　ＭＫＢ処理部
１０５　一方向性関数部
１０６　指定レコード選択処理部
１０７　一方向性関数部
１０８　データ検証処理部
１０９　認証及び鍵交換実行部
１１０　復号部
１１１　暗号化部

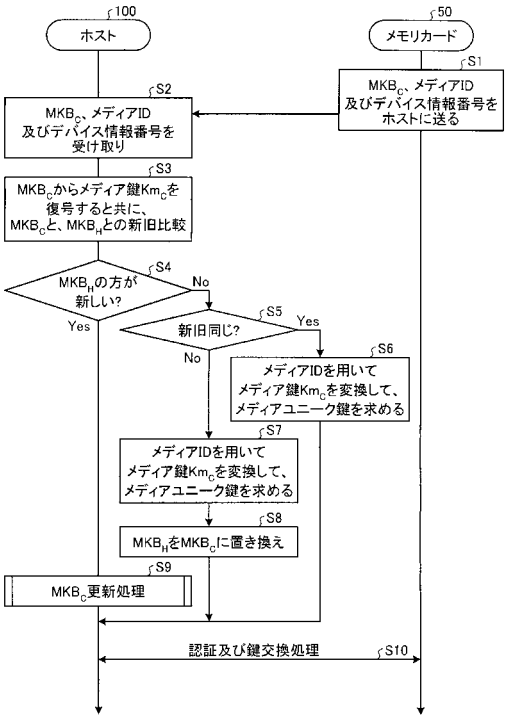
【図１】



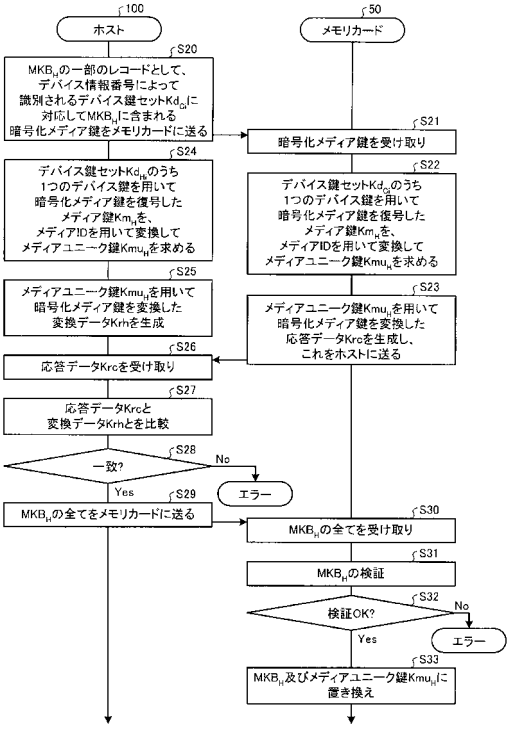
【図２】



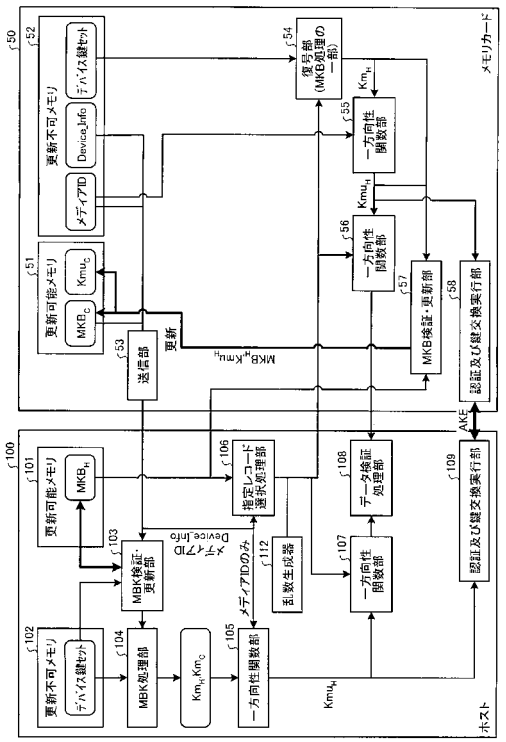
【図３】


100
ホスト
50
メモリカード
S1
MKB$_C$、メディアID及びデバイス情報番号をホストに送る
S2
MKB$_C$、メディアID及びデバイス情報番号を受け取り
S3
MKB$_C$からメディア鍵Km$_C$を復号すると共に、MKB$_C$と、MKB$_H$との新旧比較
S4
MKB$_H$の方が新しい?
No
Yes
S5
新旧同じ?
Yes
No
S6
メディアIDを用いてメディア鍵Km$_C$を変換して、メディアユニーク鍵を求める
S7
メディアIDを用いてメディア鍵Km$_C$を変換して、メディアユニーク鍵を求める
S8
MKB$_H$をMKB$_C$に置き換え
S9
MKB$_C$更新処理
認証及び鍵交換処理
S10

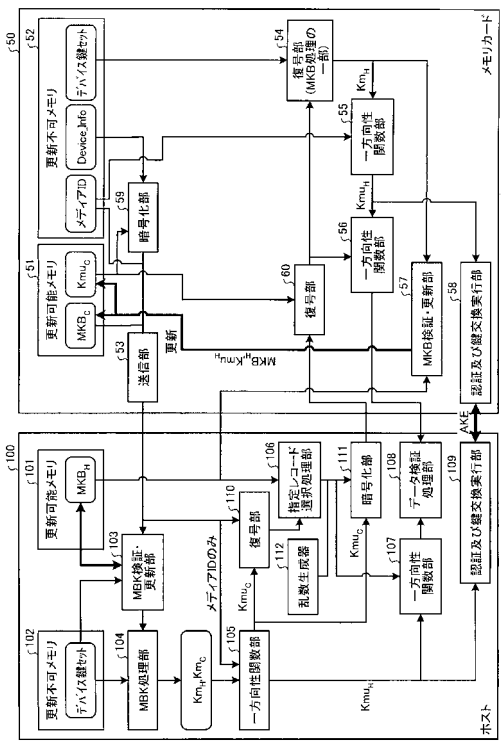
【図４】


100
ホスト
50
メモリカード
S20
MKB$_H$の一部のレコードとして、デバイス情報番号によって識別されるデバイス鍵セットKd$_{Ci}$に対応してMKB$_H$に含まれる暗号化メディア鍵をメモリカードに送る
S21
暗号化メディア鍵を受け取り
S22
デバイス鍵セットKd$_{Ci}$のうち1つのデバイス鍵を用いて暗号化メディア鍵を復号したメディア鍵Km$_H$を、メディアIDを用いて変換してメディアユニーク鍵Kmu$_H$を求める
S23
メディアユニーク鍵Kmu$_H$を用いて暗号化メディア鍵を変換した応答データKrcを生成し、これをホストに送る
S24
デバイス鍵セットKd$_{Hi}$のうち1つのデバイス鍵を用いて暗号化メディア鍵を復号したメディア鍵Km$_H$を、メディアIDを用いて変換してメディアユニーク鍵Kmu$_H$を求める
S25
メディアユニーク鍵Kmu$_H$を用いて暗号化メディア鍵を変換した変換データKrhを生成
S26
応答データKrcを受け取り
S27
応答データKrcと変換データKrhとを比較
S28
一致?
No
Yes
エラー
S29
MKB$_H$の全てをメモリカードに送る
S30
MKB$_H$の全てを受け取り
S31
MKB$_H$の検証
S32
検証OK?
No
Yes
エラー
S33
MKB$_H$及びメディアユニーク鍵Kmu$_H$に置き換え

【図５】


50
メモリカード
52
更新不可メモリ
デバイス鍵セット
Device_Info
メディアID
51
更新可能メモリ
Kmu$_C$
MKB$_C$
53
送信部
更新
MKB$_H$,Kmu$_H$
54
復号部(MKB処理の一部)
Km$_H$
55
一方向性関数部
Kmu$_H$
56
一方向性関数部
57
MKB検証・更新部
58
認証及び鍵交換実行部
AKE
100
ホスト
101
更新可能メモリ
MKB$_H$
103
MKB検証・更新部
メディアID
Device_Info
102
更新不可メモリ
デバイス鍵セット
104
MKB処理部
Km$_H$,Km$_C$
105
一方向性関数部
メディアIDのみ
106
指定レコード選択処理部
107
一方向性関数部
108
データ検証処理部
109
認証及び鍵交換実行部
112
乱数生成器
Kmu$_H$

【図６】


50
メモリカード
52
更新不可メモリ
デバイス鍵セット
Device_Info
メディアID
59
暗号化部
51
更新可能メモリ
Kmu$_C$
MKB$_C$
60
復号部
53
送信部
更新
MKB$_H$,Kmu$_H$
54
復号部(MKB処理の一部)
Km$_H$
55
一方向性関数部
Kmu$_H$
56
一方向性関数部
57
MKB検証・更新部
58
認証及び鍵交換実行部
AKE
100
ホスト
101
更新可能メモリ
MKB$_H$
103
MKB検証・更新部
メディアIDのみ
110
復号部
Kmu$_C$
102
更新不可メモリ
デバイス鍵セット
104
MKB処理部
Km$_H$,Km$_C$
105
一方向性関数部
106
指定レコード選択処理部
111
暗号化部
Kmu$_C$
107
一方向性関数部
108
データ検証処理部
109
認証及び鍵交換実行部
112
乱数生成器
Kmu$_H$

フロントページの続き

審査官　松平　英

(56)参考文献　特開２００１－２４９６９５（ＪＰ，Ａ）
特表２００３－５２６１７４（ＪＰ，Ａ）
特開２００２－１５１４７（ＪＰ，Ａ）
特表２００５－５０２９７５（ＪＰ，Ａ）
特開２００５－３４１１５６（ＪＰ，Ａ）
特開２００６－９９２１８（ＪＰ，Ａ）
特開２００９－４８５４２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／００
Ｇ０９Ｃ　　１／００
Ｇ０６Ｆ　２１／２４
Ｇ０６Ｋ　１７／００
Ｇ０６Ｋ　１９／００
Ｇ１１Ｂ　２０／１０
Ｈ０４Ｎ　　５／９１