(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-30102
(P2004-30102A)
(43)公開日　平成16年1月29日(2004.1.29)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 3/06	G06F 3/06	304H	5B017
G06F 12/14	G06F 12/14	320F	5B058
G06K 17/00	G06K 17/00	C	5B065
	G06K 17/00	D	

審査請求 未請求　請求項の数 16　OL　（全 46 頁）

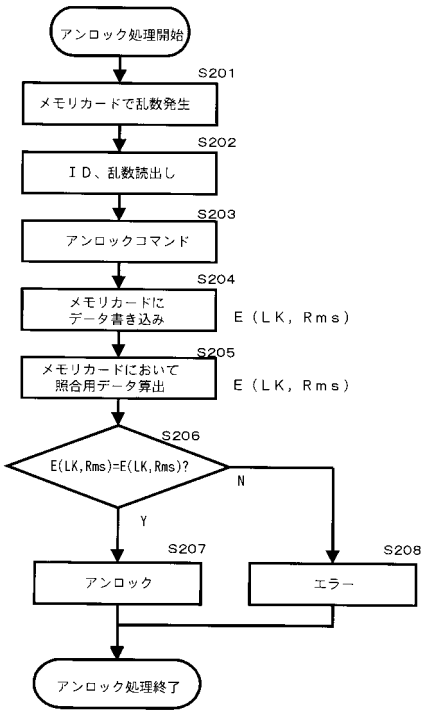
(21)出願番号　特願2002-183881(P2002-183881)
(22)出願日　平成14年6月25日(2002.6.25)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番３５号
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100101801
弁理士　山田　英治
(74)代理人　100086531
弁理士　澤田　俊夫
(72)発明者　岡上　拓己
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　中西　健一
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】情報記憶装置、およびメモリアクセス制御システム、および方法、並びにコンピュータ・プログラム

(57)【要約】
【課題】メモリのアクセス制御処理としてのロック、アンロックをアクセス要求元の出力するキーセットの検証に基づいて実行する装置および方法を提供する。
【解決手段】メモリカード等の情報記憶装置において、ＰＣ等の情報処理装置からメモリのロック処理要求コマンド、またはロック解除要求であるアンロック処理要求コマンドを入力し、入力コマンドに応じた処理を実行する際に、情報処理装置がＩＤおよびロックキー（ＬＫ）からなる正当なキーセットを有しているか否かの検証処理を、ＬＫ＝Ｈ（ＬＭＫ，ＩＤ）の関係からなるロックマスターキー（ＬＭＫ）を適用して実行する。検証の成立を条件として、前記コマンドに基づく処理を実行する。
【選択図】　図８



【特許請求の範囲】
【請求項１】
データ記憶用のメモリと、該メモリに対するアクセス制御を実行する制御部とを有する情報記憶装置であり、
前記制御部は、
情報処理装置から前記メモリのロック処理要求コマンド、またはロック解除要求であるアンロック処理要求コマンドを入力し、入力コマンドに応じた処理を実行する構成であるとともに、
前記コマンドを出力した情報処理装置に対応して設定された識別子（ＩＤ）に基づいて、前記情報処理装置が、該識別子（ＩＤ）を含む正当なキーセットを有しているか否かの検証処理を実行し、該検証の成立を条件として、前記コマンドに基づく処理を実行する構成であることを特徴とする情報記憶装置。
【請求項２】
前記情報処理装置の有するキーセットは、
情報処理装置の固有ＩＤ（ＩＤ）と、該固有ＩＤに対応するロックキー（ＬＫ）からなるキーセット［ＩＤ，ＬＫ］であり、
前記情報記憶装置は、
ＬＫ＝Ｈ（ＬＭＫ，ＩＤ）の関係、すなわち、ＩＤに対するロックマスターキー（ＬＭＫ）を適用したハッシュ値としてロックキー（ＬＫ）の算出が可能なロックマスターキー（ＬＭＫ）を有し、
前記制御部は、
情報処理装置から入力する情報処理装置固有のキーセットの検証を前記ロックマスターキー（ＬＭＫ）を適用したハッシュ値算出により取得したロックキー（ＬＫ）に基づいて実行する構成であることを特徴とする請求項１に記載の情報記憶装置。
【請求項３】
前記制御部は、
乱数発生処理を実行し、情報処理装置の所有するロックキー（ＬＫ）に基づく前記乱数（Ｒｍｓ）の暗号化データ［Ｅ（Ｌｋ，Ｒｍｓ）］を該情報処理装置から受信し、該受信暗号化データと、
前記ハッシュ値算出による取得したロックキー（ＬＫ）に基づいて算出した暗号化データ［Ｅ（Ｌｋ，Ｒｍｓ）］との照合を含む検証処理を実行する構成であることを特徴とする請求項２に記載の情報記憶装置。
【請求項４】
前記制御部は、
前記情報処理装置からの入力コマンドがロックコマンドである場合、
前記情報処理装置から識別子（ＩＤ）を入力し、
該入力識別子（ＩＤ）に基づいて、検証処理を実行する構成であることを特徴とする請求項１に記載の情報記憶装置。
【請求項５】
前記制御部は、
前記情報処理装置からの入力コマンドがアンロックコマンドである場合、
ロック処理実行に際して情報処理装置から入力し、メモリに格納した識別子（ＩＤ）を、該メモリから読み出し、読み出した識別子（ＩＤ）に基づいて、検証処理を実行する構成であることを特徴とする請求項１に記載の情報記憶装置。
【請求項６】
データ記憶用のメモリと、該メモリに対するアクセス制御を実行する制御部とを有する情報記憶装置と、前記情報記憶装置に対するインタフェースを有し、該インタフェースを介して情報記憶装置内のメモリアクセスを実行する情報処理装置とを有するメモリアクセス制御システムであり、
前記情報処理装置は、

識別子（ＩＤ）およびロックキー（ＬＫ）を含むキーセットを記憶手段に格納し、
前記情報記憶装置の制御部は、
情報処理装置から前記メモリのロック処理要求コマンド、またはロック解除要求であるアンロック処理要求コマンドを入力し、入力コマンドに応じた処理を実行する構成であるとともに、
前記コマンドの入力を行なった情報処理装置に対応して設定された識別子（ＩＤ）に基づいて、前記情報処理装置が、該識別子（ＩＤ）を含む正当なキーセットを有しているか否かの検証処理を実行し、該検証の成立を条件として、前記コマンドに基づく処理を実行する構成であることを特徴とするメモリアクセス制御システム。
【請求項７】
前記情報処理装置の有するキーセットは、
情報処理装置の固有ＩＤ（ＩＤ）と、該固有ＩＤに対応するロックキー（ＬＫ）からなるキーセット［ＩＤ，ＬＫ］であり、
前記情報記憶装置は、
ＬＫ＝Ｈ（ＬＭＫ，ＩＤ）の関係、すなわち、ＩＤに対するロックマスターキー（ＬＭＫ）を適用したハッシュ値としてロックキー（ＬＫ）の算出が可能なロックマスターキー（ＬＭＫ）を有し、
前記情報記憶装置の制御部は、
情報処理装置から入力する情報処理装置固有のキーセットの検証を前記ロックマスターキー（ＬＭＫ）を適用したハッシュ値算出により取得したロックキー（ＬＫ）に基づいて実行する構成であることを特徴とする請求項６に記載のメモリアクセス制御システム。
【請求項８】
前記情報記憶装置の制御部は、
乱数発生処理を実行し、情報処理装置の所有するロックキー（ＬＫ）に基づく前記乱数（Ｒｍｓ）の暗号化データ［Ｅ（Ｌｋ，Ｒｍｓ）］を該情報処理装置から受信し、該受信暗号化データと、
前記ハッシュ値算出による取得したロックキー（ＬＫ）に基づいて算出した暗号化データ［Ｅ（Ｌｋ，Ｒｍｓ）］との照合を含む検証処理を実行する構成であることを特徴とする請求項７に記載のメモリアクセス制御システム。
【請求項９】
前記情報記憶装置の制御部は、
前記情報処理装置からの入力コマンドがロックコマンドである場合、
前記情報処理装置から識別子（ＩＤ）を入力し、
該入力識別子（ＩＤ）に基づいて、検証処理を実行する構成であることを特徴とする請求項６に記載のメモリアクセス制御システム。
【請求項１０】
前記情報記憶装置の制御部は、
前記情報処理装置からの入力コマンドがアンロックコマンドである場合、
ロック処理実行に際して情報処理装置から入力し、メモリに格納した識別子（ＩＤ）を、該メモリから読み出し、読み出した識別子（ＩＤ）に基づいて、検証処理を実行する構成であることを特徴とする請求項６に記載のメモリアクセス制御システム。
【請求項１１】
データ記憶用のメモリと、該メモリに対するアクセス制御を実行する制御部とを有する情報記憶装置におけるメモリアクセス制御方法であり、
情報処理装置から前記メモリのロック処理要求コマンド、またはロック解除要求であるアンロック処理要求コマンドを入力するステップと、
前記コマンドを出力した情報処理装置に対応して設定された識別子（ＩＤ）に基づいて、前記情報処理装置が、該識別子（ＩＤ）を含む正当なキーセットを有しているか否かの検証処理を実行する検証ステップと、
前記検証の成立を条件として、前記コマンドに基づく処理を実行するステップと、

を有することを特徴とするメモリアクセス制御方法。
【請求項１２】
前記情報処理装置の有するキーセットは、
情報処理装置の固有ＩＤ（ＩＤ）と、該固有ＩＤに対応するロックキー（ＬＫ）からなるキーセット［ＩＤ，ＬＫ］であり、
前記情報記憶装置は、
ＬＫ＝Ｈ（ＬＭＫ，ＩＤ）の関係、すなわち、ＩＤに対するロックマスターキー（ＬＭＫ）を適用したハッシュ値としてロックキー（ＬＫ）の算出が可能なロックマスターキー（ＬＭＫ）を有し、
前記検証ステップは、
情報処理装置から入力する情報処理装置固有のキーセットの検証を前記ロックマスターキー（ＬＭＫ）を適用したハッシュ値算出により取得したロックキー（ＬＫ）に基づく検証処理を実行するステップを含むことを特徴とする請求項１１に記載のメモリアクセス制御方法。
【請求項１３】
前記検証ステップは、
乱数発生処理を実行し、情報処理装置の所有するロックキー（ＬＫ）に基づく前記乱数（Ｒｍｓ）の暗号化データ［Ｅ（Ｌｋ，Ｒｍｓ）］を該情報処理装置から受信し、該受信暗号化データと、
前記ハッシュ値算出による取得したロックキー（ＬＫ）に基づいて算出した暗号化データ［Ｅ（Ｌｋ，Ｒｍｓ）］との照合を含む検証処理を実行するステップを含むことを特徴とする請求項１２に記載のメモリアクセス制御方法。
【請求項１４】
前記検証ステップは、
前記情報処理装置からの入力コマンドがロックコマンドである場合、
前記情報処理装置から識別子（ＩＤ）を入力し、該入力識別子（ＩＤ）に基づいて、検証処理を実行するステップを含むことを特徴とする請求項１１に記載のメモリアクセス制御方法。
【請求項１５】
前記検証ステップは、
前記情報処理装置からの入力コマンドがアンロックコマンドである場合、
ロック処理実行に際して情報処理装置から入力し、メモリに格納した識別子（ＩＤ）を、該メモリから読み出し、読み出した識別子（ＩＤ）に基づいて、検証処理を実行するステップを含むことを特徴とする請求項１１に記載のメモリアクセス制御方法。
【請求項１６】
データ記憶用のメモリと、該メモリに対するアクセス制御を実行する制御部とを有する情報記憶装置におけるメモリアクセス制御処理を実行するコンピュータ・プログラムであって、
情報処理装置から前記メモリのロック処理要求コマンド、またはロック解除要求であるアンロック処理要求コマンドを入力するステップと、
前記コマンドを出力した情報処理装置に対応して設定された識別子（ＩＤ）に基づいて、前記情報処理装置が、該識別子（ＩＤ）を含む正当なキーセットを有しているか否かの検証処理を実行する検証ステップと、
前記検証の成立を条件として、前記コマンドに基づく処理を実行するステップと、
を有することを特徴とするコンピュータ・プログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、情報記憶装置、メモリアクセス制御システム、および方法、並びにコンピュータ・プログラムに関する。さらに詳細には、メモリカード等の情報記憶装置の格納データ

に対する様々な態様でのアクセス制限構成を実現し、情報記憶装置内のメモリのロック処理またはアンロック処理を情報記憶装置の有する識別子等によって構成されるキーセットの検証に基づいて実行し、セキュアなメモリアクセス制御管理を実現する情報記憶装置、メモリアクセス制御システム、および方法、並びにコンピュータ・プログラムに関する。

【０００２】

【従来の技術】

ＰＣ（Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ）、ＰＤＡ（Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｔｓ）、デジタルカメラ、データ記録再生装置、あるいはゲーム機器等、様々な情報処理装置では、ハードディスク、ＤＶＤ、ＣＤ、メモリカード等、様々な記憶媒体を利用したデータの記録、再生処理が実行される。

【０００３】

昨今では、フラッシュメモリ等によって構成されるメモリ部と、ＣＰＵ等によって構成される制御部とを備えた小型のカード型メモリ装置が、音楽データ、画像データ、プログラム等、様々なソフトウエアデータ（コンテンツ（Ｃｏｎｔｅｎｔ））の記憶手段として多く利用されている。

【０００４】

メモリカード等に格納されたデータの読み出し、あるいはデータ書き込みは、メモリカード・インタフェースを有する機器にカードを装着し、インタフェースを介してデータ転送を行なうことにより可能となる。メモリ装置を利用したデータ記録再生は、誰もが自由に実行できる構成とすることも可能であるが、例えばパスワード設定、あるいは暗号処理などによって、特定ユーザ、あるいは特定機器のみに対してメモリ・アクセスを許可し、権限を持たない第三者によるアクセスを排除した、いわゆるアクセ制限構成が実現されている。

【０００５】

例えばアクセス権限を有するユーザのみが知り得るパスワードを設定して、情報再生装置としてのコンテンツ利用機器から、メモリカード等のコンテンツ格納機器に対してパスワードを転送し、メモリカード側の制御部（ＣＰＵ等）においてパスワードの検証を実行して、検証成立を条件として、メモリカード等のコンテンツ格納機器から、情報再生装置としてのコンテンツ利用機器に対してコンテンツを出力する構成、あるいは、情報再生装置としてのコンテンツ利用機器と、メモリカード等のコンテンツ格納機器間において相互認証処理を実行して、相互認証が成立したことを条件として、メモリカード等のコンテンツ格納機器から、情報再生装置としてのコンテンツ利用機器に対してコンテンツを出力する構成等がある。

【０００６】

【発明が解決しようとする課題】

このように、データ（コンテンツ）利用権限を確認した上でデータを利用可能とする形態は、様々な形態がある。

【０００７】

しかしながら、メモリカード等のデータ記憶装置は、ＰＣ、ＰＤＡ、デジタルカメラ等、様々な機器に装着可能であり、これらの機器で、相互に１つのメモリカードを利用する場合も多い。このようなデータ利用形態において、メモリカードを機器に装着する毎に上述したパスワード検証処理、認証処理等の実行が要求されると、データ読み取りあるいはデータ書き込み等の処理に至るまでに時間を要し、処理効率が低下することになる。

【０００８】

本発明は、上述の問題点に鑑みてなされたものであり、情報記憶装置内のメモリのロック処理またはアンロック処理を情報記憶装置の有する識別子等によって構成されるキーセットの検証に基づいて実行し、セキュアなメモリアクセス制御管理を実現した情報記憶装置、メモリアクセス制御システム、および方法、並びにコンピュータ・プログラムを提供することを目的とする。

【０００９】

【課題を解決するための手段】
本発明の第１の側面は、
データ記憶用のメモリと、該メモリに対するアクセス制御を実行する制御部とを有する情報記憶装置であり、
前記制御部は、
情報処理装置から前記メモリのロック処理要求コマンド、またはロック解除要求であるアンロック処理要求コマンドを入力し、入力コマンドに応じた処理を実行する構成であるとともに、
前記コマンドを出力した情報処理装置に対応して設定された識別子（ＩＤ）に基づいて、前記情報処理装置が、該識別子（ＩＤ）を含む正当なキーセットを有しているか否かの検証処理を実行し、該検証の成立を条件として、前記コマンドに基づく処理を実行する構成であることを特徴とする情報記憶装置にある。
【００１０】
さらに、本発明の情報記憶装置の一実施態様において、前記情報処理装置の有するキーセットは、情報処理装置の固有ＩＤ（ＩＤ）と、該固有ＩＤに対応するロックキー（ＬＫ）からなるキーセット［ＩＤ，ＬＫ］であり、前記情報記憶装置は、ＬＫ＝Ｈ（ＬＭＫ，ＩＤ）の関係、すなわち、ＩＤに対するロックマスターキー（ＬＭＫ）を適用したハッシュ値としてロックキー（ＬＫ）の算出が可能なロックマスターキー（ＬＭＫ）を有し、前記制御部は、情報処理装置から入力する情報処理装置固有のキーセットの検証を前記ロックマスターキー（ＬＭＫ）を適用したハッシュ値算出により取得したロックキー（ＬＫ）に基づいて実行する構成であることを特徴とする。
【００１１】
さらに、本発明の情報記憶装置の一実施態様において、前記制御部は、乱数発生処理を実行し、情報処理装置の所有するロックキー（ＬＫ）に基づく前記乱数（Ｒｍｓ）の暗号化データ［Ｅ（Ｌｋ，Ｒｍｓ）］を該情報処理装置から受信し、該受信暗号化データと、前記ハッシュ値算出による取得したロックキー（ＬＫ）に基づいて算出した暗号化データ［Ｅ（Ｌｋ，Ｒｍｓ）］との照合を含む検証処理を実行する構成であることを特徴とする。
【００１２】
さらに、本発明の情報記憶装置の一実施態様において、前記制御部は、前記情報処理装置からの入力コマンドがロックコマンドである場合、前記情報処理装置から識別子（ＩＤ）を入力し、該入力識別子（ＩＤ）に基づいて、検証処理を実行する構成であることを特徴とする。
【００１３】
さらに、本発明の情報記憶装置の一実施態様において、前記制御部は、前記情報処理装置からの入力コマンドがアンロックコマンドである場合、ロック処理実行に際して情報処理装置から入力し、メモリに格納した識別子（ＩＤ）を、該メモリから読み出し、読み出した識別子（ＩＤ）に基づいて、検証処理を実行する構成であることを特徴とする。
【００１４】
さらに、本発明の第２の側面は、
データ記憶用のメモリと、該メモリに対するアクセス制御を実行する制御部とを有する情報記憶装置と、前記情報記憶装置に対するインタフェースを有し、該インタフェースを介して情報記憶装置内のメモリアクセスを実行する情報処理装置とを有するメモリアクセス制御システムであり、
前記情報処理装置は、
識別子（ＩＤ）およびロックキー（ＬＫ）を含むキーセットを記憶手段に格納し、
前記情報記憶装置の制御部は、
情報処理装置から前記メモリのロック処理要求コマンド、またはロック解除要求であるアンロック処理要求コマンドを入力し、入力コマンドに応じた処理を実行する構成であるとともに、
前記コマンドの入力を行なった情報処理装置に対応して設定された識別子（ＩＤ）に基づ

いて、前記情報処理装置が、該識別子（ＩＤ）を含む正当なキーセットを有しているか否かの検証処理を実行し、該検証の成立を条件として、前記コマンドに基づく処理を実行する構成であることを特徴とするメモリアクセス制御システムにある。

【００１５】

さらに、本発明のメモリアクセス制御システムの一実施態様において、前記情報処理装置の有するキーセットは、情報処理装置の固有ＩＤ（ＩＤ）と、該固有ＩＤに対応するロックキー（ＬＫ）からなるキーセット［ＩＤ，ＬＫ］であり、前記情報記憶装置は、ＬＫ＝Ｈ（ＬＭＫ，ＩＤ）の関係、すなわち、ＩＤに対するロックマスターキー（ＬＭＫ）を適用したハッシュ値としてロックキー（ＬＫ）の算出が可能なロックマスターキー（ＬＭＫ）を有し、前記情報記憶装置の制御部は、情報処理装置から入力する情報処理装置固有のキーセットの検証を前記ロックマスターキー（ＬＭＫ）を適用したハッシュ値算出により取得したロックキー（ＬＫ）に基づいて実行する構成であることを特徴とする。

【００１６】

さらに、本発明のメモリアクセス制御システムの一実施態様において、前記情報記憶装置の制御部は、乱数発生処理を実行し、情報処理装置の所有するロックキー（ＬＫ）に基づく前記乱数（Ｒｍｓ）の暗号化データ［Ｅ（Ｌｋ，Ｒｍｓ）］を該情報処理装置から受信し、該受信暗号化データと、前記ハッシュ値算出による取得したロックキー（ＬＫ）に基づいて算出した暗号化データ［Ｅ（Ｌｋ，Ｒｍｓ）］との照合を含む検証処理を実行する構成であることを特徴とする。

【００１７】

さらに、本発明のメモリアクセス制御システムの一実施態様において、前記情報記憶装置の制御部は、前記情報処理装置からの入力コマンドがロックコマンドである場合、前記情報処理装置から識別子（ＩＤ）を入力し、該入力識別子（ＩＤ）に基づいて、検証処理を実行する構成であることを特徴とする。

【００１８】

さらに、本発明のメモリアクセス制御システムの一実施態様において、前記情報記憶装置の制御部は、前記情報処理装置からの入力コマンドがアンロックコマンドである場合、ロック処理実行に際して情報処理装置から入力し、メモリに格納した識別子（ＩＤ）を、該メモリから読み出し、読み出した識別子（ＩＤ）に基づいて、検証処理を実行する構成であることを特徴とする。

【００１９】

さらに、本発明の第３の側面は、

データ記憶用のメモリと、該メモリに対するアクセス制御を実行する制御部とを有する情報記憶装置におけるメモリアクセス制御方法であり、

情報処理装置から前記メモリのロック処理要求コマンド、またはロック解除要求であるアンロック処理要求コマンドを入力するステップと、

前記コマンドを出力した情報処理装置に対応して設定された識別子（ＩＤ）に基づいて、前記情報処理装置が、該識別子（ＩＤ）を含む正当なキーセットを有しているか否かの検証処理を実行する検証ステップと、

前記検証の成立を条件として、前記コマンドに基づく処理を実行するステップと、

を有することを特徴とするメモリアクセス制御方法にある。

【００２０】

さらに、本発明のメモリアクセス制御方法の一実施態様において、前記情報処理装置の有するキーセットは、情報処理装置の固有ＩＤ（ＩＤ）と、該固有ＩＤに対応するロックキー（ＬＫ）からなるキーセット［ＩＤ，ＬＫ］であり、前記情報記憶装置は、ＬＫ＝Ｈ（ＬＭＫ，ＩＤ）の関係、すなわち、ＩＤに対するロックマスターキー（ＬＭＫ）を適用したハッシュ値としてロックキー（ＬＫ）の算出が可能なロックマスターキー（ＬＭＫ）を有し、前記検証ステップは、情報処理装置から入力する情報処理装置固有のキーセットの検証を前記ロックマスターキー（ＬＭＫ）を適用したハッシュ値算出により取得したロックキー（ＬＫ）に基づく検証処理を実行するステップを含むことを特徴とする。

【００２１】
さらに、本発明のメモリアクセス制御方法の一実施態様において、前記検証ステップは、乱数発生処理を実行し、情報処理装置の所有するロックキー（ＬＫ）に基づく前記乱数（Ｒｍｓ）の暗号化データ［Ｅ（Ｌｋ，Ｒｍｓ）］を該情報処理装置から受信し、該受信暗号化データと、前記ハッシュ値算出による取得したロックキー（ＬＫ）に基づいて算出した暗号化データ［Ｅ（Ｌｋ，Ｒｍｓ）］との照合を含む検証処理を実行するステップを含むことを特徴とする。
【００２２】
さらに、本発明のメモリアクセス制御方法の一実施態様において、前記検証ステップは、前記情報処理装置からの入力コマンドがロックコマンドである場合、前記情報処理装置から識別子（ＩＤ）を入力し、該入力識別子（ＩＤ）に基づいて、検証処理を実行するステップを含むことを特徴とする。
【００２３】
さらに、本発明のメモリアクセス制御方法の一実施態様において、前記検証ステップは、前記情報処理装置からの入力コマンドがアンロックコマンドである場合、ロック処理実行に際して情報処理装置から入力し、メモリに格納した識別子（ＩＤ）を、該メモリから読み出し、読み出した識別子（ＩＤ）に基づいて、検証処理を実行するステップを含むことを特徴とする。
【００２４】
さらに、本発明の第４の側面は、
データ記憶用のメモリと、該メモリに対するアクセス制御を実行する制御部とを有する情報記憶装置におけるメモリアクセス制御処理を実行するコンピュータ・プログラムであって、
情報処理装置から前記メモリのロック処理要求コマンド、またはロック解除要求であるアンロック処理要求コマンドを入力するステップと、
前記コマンドを出力した情報処理装置に対応して設定された識別子（ＩＤ）に基づいて、前記情報処理装置が、該識別子（ＩＤ）を含む正当なキーセットを有しているか否かの検証処理を実行する検証ステップと、
前記検証の成立を条件として、前記コマンドに基づく処理を実行するステップと、
を有することを特徴とするコンピュータ・プログラムにある。
【００２５】
【作用】
本発明の構成によれば、メモリカード等の情報記憶装置において、ＰＣ等の情報処理装置からメモリのロック処理要求コマンド、またはロック解除要求であるアンロック処理要求コマンドを入力し、入力コマンドに応じた処理を実行する際に、コマンドを出力した情報処理装置に対応して設定された識別子（ＩＤ）に基づいて、情報処理装置が、該識別子（ＩＤ）を含む正当なキーセットを有しているか否かの検証処理を実行し、該検証の成立を条件として、前記コマンドに基づく処理を実行する構成としたので、セキュアな管理下でのメモリアクセス制御が実現される。
【００２６】
さらに、本発明の構成によれば、情報処理装置に固有ＩＤ（ＩＤ）と、該固有ＩＤに対応するロックキー（ＬＫ）からなるキーセット［ＩＤ，ＬＫ］を格納し、一方、情報記憶装置は、ＬＫ＝Ｈ（ＬＭＫ，ＩＤ）の関係、すなわち、ＩＤに対するロックマスターキー（ＬＭＫ）を適用したハッシュ値としてロックキー（ＬＫ）の算出が可能なロックマスターキー（ＬＭＫ）を格納し、情報処理装置から入力する情報処理装置固有のキーセットの検証を前記ロックマスターキー（ＬＭＫ）を適用したハッシュ値算出により取得したロックキー（ＬＫ）に基づいて実行する構成としたので、複数の異なるロックキー（ＬＫ）に対する検証を１つのロックマスターキー（ＬＭＫ）に基づいて実行することが可能となる。
【００２７】
さらに、本発明の構成によれば、情報処理装置の検証において、情報記憶装置側で乱数発

生処理を実行し、情報処理装置の所有するロックキー（ＬＫ）に基づく乱数（Ｒｍｓ）の暗号化データ［Ｅ（Ｌｋ，Ｒｍｓ）］を該情報処理装置から受信し、該受信暗号化データと、ハッシュ値算出による取得したロックキー（ＬＫ）に基づいて算出した暗号化データ［Ｅ（Ｌｋ，Ｒｍｓ）］との照合を実行する構成としたので、照合毎に異なる乱数を適用した検証が可能となり、過去の照合履歴データを利用した不正アクセスが排除可能となる。

【００２８】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、ＣＤやＦＤ、ＭＯなどの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【００２９】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づく、より詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【００３０】

【発明の実施の形態】

以下、本発明の情報記憶装置、メモリアクセス制御処理の実施例詳細について、図面を参照して詳細に説明する。

【００３１】

まず、本発明の情報記憶装置を適用したデータ利用構成の概要について、図１を参照して説明する。情報処理装置２０は、例えばＰＣ（Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ）２１、ＰＤＡ（Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｔｓ）２２、携帯通信端末２３、デジタルカメラ２４等、情報記憶装置３０を装着し、情報記憶装置３０からの情報を出力可能な機器である。

【００３２】

これらの情報処理装置２０は、例えばフラッシュメモリ等の不揮発性メモリ（ＮＶＭ：Ｎｏｎ－Ｖｏｌａｔｉｌｅ Ｍｅｍｏｒｙ）を搭載したメモリカード３０を装着し、メモリカード３０に対してデータを格納し、あるいはメモリカードに格納されたデータの読み出しを実行する。

【００３３】

ＰＣ（Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ）２１、２２、ＰＤＡ（Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｔｓ）２３、携帯通信端末２４、デジタルカメラ２５の各々は、１つのメモリカード３０を相互に利用する場合もある。例えばデジタルカメラ２５で撮影した画像データをメモリカード３０に格納し、その後、メモリカード３０をＰＣ２１に装着して格納画像データの表示、画像処理等を実行したり、あるいは、ＰＣ２１において、インターネット等のネットワークを介して、またはＣＤ、ＤＶＤ等を介して入手した音楽データ等のコンテンツをメモリカード３０に格納し、その後、コンテンツを格納したメモリカード３０をＰＤＡ２２に装着して、外出先で、ＰＤＡ２２を用いてコンテンツを再生するなどの利用が行なわれる。

【００３４】

図２にメモリカード等の情報記憶装置を装着可能な情報処理装置の構成例を示す。ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）１０１は、各種アプリケーションプログラム、ＯＳ（Ｏｐｅｒａｔｉｎｇ Ｓｙｓｔｅｍ）を実行するプロセッサである。後段で詳細に説明する情報記憶装置に対するアクセス制限処理としてのロック処理、アンロック処理におけるハッシュ値算出、乱数生成等を含む各種暗号処理、およびコマンド送受信等における制御を実行する。

【００３５】
ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）１０２は、ＣＰＵ１０１が実行するプログラムや演算用のパラメータのうちの固定データ等を格納する。後段で詳細に説明する情報記憶装置に対する対するアクセス制限処理としてのロック処理、アンロック処理プログラム等が格納される。ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）１０３は、ＣＰＵ１０１の実行プログラムに適用する情報や、その実行において適宜変化するパラメータ等を格納する。
【００３６】
ＤＳＰ（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｌ　Ｐｒｏｃｅｓｓｏｒ）１０４は、例えばメモリカード等の情報記憶装置２００から記憶装置Ｉ／Ｆ１１３を介して入力したコンテンツの再生処理の際の暗号処理、イコライザ調整（音声信号の周波数帯域に対応した利得の調整）、圧縮伸長（エンコード／デコード）処理等を実行する。
【００３７】
復号、伸長されたコンテンツは、デジタルアナログ変換回路１０５でアナログ音声信号に変換され、増幅回路１０６において増幅された後、音声出力部１０７を介して出力する。また、画像データの出力は、表示コントローラ１０８を介してＬＣＤ等の表示部１０９において実行される。入力Ｉ／Ｆ１１２からは、外部ソースからデジタル信号、またはアナログ信号を入力し、アナログ信号入力時にはＡ／Ｄ変換する。Ａ／Ｄ変換は、入力される入力信号をデジタル信号へ変換する。また、外部ソースからの入力デジタル信号は、ＳＲＣ（サンプリングレートコンバータ）により、所定のサンプリング周波数、量子化ビット数を持つデジタル信号に変換されて入力される。
【００３８】
入出力Ｉ／Ｆ１１５は、外部機器を接続するインタフェースであり、例えばＵＳＢ，ＩＥＥＥ１３９４等の接続態様による接続を行ない接続された機器とのデータ転送が実行される。
【００３９】
次に、図３を参照して、フラッシュメモリ等の不揮発性メモリ（ＮＶＭ：Ｎｏｎ－Ｖｏｌａｔｉｌｅ　Ｍｅｍｏｒｙ）を搭載したメモリカード等の情報記憶装置２００の構成例を示す。フラッシュメモリは、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ　Ｅｒａｓａｂｌｅ　Ｐｒｏｇｒａｍｍａｂｌｅ　ＲＯＭ）と呼ばれる電気的に書き換え可能な不揮発性メモリの一形態である。従来のＥＥＰＲＯＭは、１ビットを２個のトランジスタで構成するために、１ビット当たりの占有面積が大きく、集積度を高くするのに限界があったが、フラッシュメモリは、全ビット一括消去方式により１ビットを１トランジスタで実現することが可能となった。
【００４０】
このようなフラッシュメモリを持つ情報記憶装置２００は、ＰＣ、ＰＤＡ、デジタルカメラ等の情報処理装置に装着され、情報処理装置から入力するデータを、メモリ部２２０に格納し、また、メモリ部２２０に格納されたデータを情報処理装置に対して出力する。
【００４１】
情報記憶装置２００は、さらに制御部２１０を有し、制御部２１０は、各種プログラムを実行するプロセッサとしてのＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）２１１、ＣＰＵ２１１が実行するプログラムや演算用のパラメータのうちの固定データ等を格納するＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）２１２、ＣＰＵ２１１の実行プログラムに適用する情報や、その実行において適宜変化するパラメータ等を格納するＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）２１３を有する。
【００４２】
なお、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）２１３は、後段で詳細に説明する情報記憶装置に対する対するアクセス制限処理としてのロック処理、アンロック処理によって変化するロック状態の状態値データの格納領域としても使用される。
【００４３】

制御部２１０は、さらに、情報処理装置間とのデータ入出力用のインタフェースとしての機器インタフェース２１４、メモリ部２２０とのデータ入出力用のインタフェースとしてのメモリインタフェース２１６を有する。

【００４４】

ＣＰＵ２１１は、後段で詳細に説明する情報処理装置との間で実行されるアクセス制限処理としてのロック処理、アンロック処理におけるハッシュ値算出、乱数生成等を含む各種暗号処理、およびコマンド送受信等における制御を実行する。

【００４５】

［ロックマスターキー（ＬＭＫ）に基づく処理］

次に、情報記憶装置に対するアクセス制限機構の一処理例として、ロックマスターキー（ＬＭＫ）を適用したロック処理及びアンロック処理について説明する。図４を参照して本処理例、すなわちロックマスターキー（ＬＭＫ）を適用した処理の概要を説明する。

【００４６】

メモリカード等の情報記憶装置３２０のコンテンツ等のデータ格納領域であるフラッシュメモリ等によって構成されるメモリ部（図３のメモリ部２２０）に対するアクセス制限を有効にする処理をロック処理とし、アクセス制限を解除する処理をアンロック処理とする。このロック処理およびアンロック処理を実行するのが、ホスト装置３１０である。

【００４７】

ホスト装置３１０は、先に図１、図２を参照して説明したように、メモリカード等の情報記憶装置３２０とのデータ転送を実行するインタフェースを有し、情報記憶装置３２０に対するデータ書き込みあるいは情報記憶装置３２０からのデータ読み出しを実行してデータ利用を行なうＰＣ、ＰＤＡ、デジタルカメラ、ＤＳＣ（Ｄｉｇｉｔａｌ　Ｓｔｉｌｌ　Ｃａｍｅｒａ）等の情報処理装置を含む。さらに、ホスト装置３１０には、メモリカード等の情報記憶装置３２０に対するロック処理／アンロック処理実行専用機器としてのロック・アンロック用機器３１２も含まれる。

【００４８】

ロック・アンロック用機器３１２は、ロック・アンロック処理アルゴリズムを実行する制御手段としてのＣＰＵ、およびデータ格納メモリとしてのＲＯＭ，ＲＡＭを有し、さらにメモリカード等の情報記憶装置３２０の装着、データ転送を実行するインタフェースを有し、情報記憶装置３２０に対するロック処理およびアンロック処理専用の機器として構成される。

【００４９】

以下の説明では、情報記憶装置３２０に対してロック処理、アンロック処理を実行する機器、すなわち、ＰＣ，ＰＤＡ他の情報処理装置と、ロック・アンロック用機器３１２を含めてホスト装置と呼ぶ。

【００５０】

ホスト装置内のＲＯＭ等のメモリ３１５には、各ホスト装置固有の識別子としてのＩＤ（例えば１６バイトデータ）と、ロック処理、アンロック処理に適用する鍵データとしてのロックキー（ＬＫ）（例えば８バイトデータ）が格納される。ホスト装置の有する各ホスト装置固有の識別子（ＩＤ）と、ロックキー（ＬＫ）のセット［ＩＤ，ＬＫ］をキーセットと呼ぶ。

【００５１】

一方、メモリカード等の情報記憶装置３２０内の制御部内のＲＯＭ等のメモリ３２５には、ロックマスターキー（ＬＭＫ）が格納される。これらの情報は、例えば各機器の製造時に各機器に対して書き込まれ、ユーザによる書き換え不可能なデータとされる。

【００５２】

情報記憶装置３２０に格納されるロックマスターキー（ＬＭＫ）と、ホスト装置に格納されるＩＤと、ロックキー（ＬＫ）とは、以下の関係を持つ。

ＬＫ＝Ｈ（ＬＭＫ，ＩＤ）

【００５３】

なお、Ｈ（Ｘ，Ｙ）は、キーＸを適用したメッセージＹに対するハッシュ値算出処理を示す。すなわち、ＩＤに対して、ロックマスターキー（ＬＭＫ）を適用したハッシュ値算出処理によりＩＤに対応するロックキー（ＬＫ）が求められる。

【００５４】

ハッシュ関数は、一方向性関数であり、その出力から逆に入力を求めるのは非常に困難となる関数である。上記式においては、各ホスト装置に固有のＩＤに対して、ロックマスターキー（ＬＭＫ）を鍵として一方向性関数を適用して、その出力を各ホスト装置に固有のＩＤに対応するロックキー（ＬＫ）とした設定である。ハッシュ・アルゴリズムとしてはＭＤ５，ＳＨＡなどが適用可能である。

【００５５】

（ロック処理）

次に上述したロックマスターキー（ＬＭＫ）を適用したロック処理、すなわち情報記憶装置に対するアクセス制限を有効にする処理について説明する。

【００５６】

図５にロック処理におけるホスト装置と、情報記憶装置間で実行される処理シーケンス図を示す。ホスト装置と、情報記憶装置は、それぞれ相互にデータ転送可能に接続されている。まず、ホスト装置が、乱数発生コマンドを情報記憶装置に対して出力する。乱数発生コマンドを受信した情報記憶装置は、所定長、例えば１６バイト乱数（Ｒｍｓ）の発生処理を実行し、発生乱数（Ｒｍｓ）をホスト装置に対して送信する。なお、情報記憶装置は、発生乱数（Ｒｍｓ）を制御部内のＲＡＭ等のメモリに格納しておく。

【００５７】

情報記憶装置から乱数（Ｒｍｓ）を受信したホスト装置は、予めホスト装置内のメモリに格納済みのロックキー（ＬＫ）を暗号処理キーとした受信乱数（Ｒｍｓ）の暗号処理：Ｅ（ＬＫ，Ｒｍｓ）を実行する。なお、Ｅ（Ｘ，Ｙ）は、キー［Ｘ］を適用したメッセージ［Ｙ］の暗号処理を示す。暗号処理アルゴリズムは様々なアルゴリズムの適用が可能であり、例えばＤＥＳ暗号処理アルゴリズムが適用される。

【００５８】

ホスト装置は、ロックキー（ＬＫ）を暗号処理キーとした受信乱数（Ｒｍｓ）の暗号処理：Ｅ（ＬＫ，Ｒｍｓ）を実行し、その結果データ［Ｅ（ＬＫ，Ｒｍｓ）］と、ホスト装置が予めホスト装置内のメモリに格納しているホスト装置固有の識別子（ＩＤ）とを、ロックコマンドとともに情報記憶装置に送信する。

【００５９】

データ：ＩＤ，Ｅ（ＬＫ，Ｒｍｓ）を受信した情報記憶装置は、まず、受信したＩＤに対して、自己のメモリに格納されているロックマスターキー（ＬＭＫ）を適用したハッシュ値算出処理により、受信ＩＤに対応するロックキー（ＬＫ）を算出する。すなわち、

ＬＫ＝Ｈ（ＬＭＫ，ＩＤ）

により、受信ＩＤに対応するロックキー（ＬＫ）を算出する。なお、受信ＩＤは、自己のメモリに格納保持する。受信ＩＤは、後述するアンロック処理の際に利用する。

【００６０】

さらに、情報記憶装置は、自己のメモリに格納した乱数Ｒｍｓに対して、上述のハッシュ値算出により求めたロックキー（ＬＫ）を適用した暗号処理：Ｅ（ＬＫ，Ｒｍｓ）を実行し、ホスト装置から受信した暗号処理データ：Ｅ（ＬＫ，Ｒｍｓ）と一致するか否かの照合処理を実行する。なお、暗号処理アルゴリズムはホスト装置と同一のアルゴリズムであれば、様々なアルゴリズムの適用が可能である。

【００６１】

ホスト装置からの受信データ：Ｅ（ＬＫ，Ｒｍｓ）と、自身が算出した暗号処理データ：Ｅ（ＬＫ，Ｒｍｓ）とが一致すれば、正当なＩＤとＬＫの組データを持つホスト装置からのロック処理要求であると判定しロック処理を実行し、ロック完了通知をホスト装置に対して送信する。情報記憶装置は、ロック処理を実行したホスト装置のキーセット［ＩＤ，ＬＫ］をフラッシュメモリ等の不揮発性メモリ（ＮＶＭ：Ｎｏｎ－Ｖｏｌａｔｉｌｅ　Ｍ

ｅｍｏｒｙ）によって構成されるメモリ部２２０に格納保持する。
【００６２】
ホスト装置からの受信データ：Ｅ（ＬＫ，Ｒｍｓ）と、自身が算出した暗号処理データ：Ｅ（ＬＫ，Ｒｍｓ）とが不一致の場合は、正当なＩＤとＬＫの組データを持つホスト装置では無いと判定し、不正機器からのロック処理要求であると判定し、ロック処理を行なわずエラー通知をホスト装置に送信する。
【００６３】
なお、情報記憶装置の実行するロック処理は、コンテンツ等のデータ格納領域であるフラッシュメモリ等によって構成されるメモリ部（図３のメモリ部２２０）に対するアクセスを、次に説明するアンロック処理を実行することを条件として許可する設定とする処理である。
【００６４】
次に、図６に示すフローチャートを参照して、ロック処理の手順について説明する。ステップＳ１０１において、情報記憶装置としてのメモリカードが、ホスト装置からの乱数発生要求コマンドの受信に基づいて、乱数（Ｒｓｍ）を発生する。発生した乱数は、ステップＳ１０２において、ホスト装置によって読み出され、ステップＳ１０３において、ロックコマンドとともに、ホスト装置のＩＤ、および乱数（Ｒｍｓ）をホスト装置のロックキー（ＬＫ）で暗号化したデータ：Ｅ（ＬＫ，Ｒｍｓ）を情報記憶装置としてのメモリカードに送信する。
【００６５】
ステップＳ１０４において、メモリカードは、受信したＩＤ、および暗号化データ：Ｅ（ＬＫ，Ｒｍｓ）とを情報記憶装置内のメモリに書き込む。ステップＳ１０５において、メモリカードは、自身のメモリに格納したロックマスターキー（ＬＭＫ）を適用して、受信ＩＤのハッシュ値算出、すなわち、
Ｈ（ＬＭＫ，ＩＤ）＝ＬＫ
を実行し、受信ＩＤに対応するロックキー（ＬＫ）を算出する。
【００６６】
さらに、メモリカードは、算出したロックキー（ＬＫ）に基づいて、先にステップＳ１０１で発生した乱数（Ｒｍｓ）の暗号化処理を実行して、暗号化データ：Ｅ（ＬＫ，Ｒｍｓ）を照合用データとして算出する。
【００６７】
次に、メモリカードは、ステップＳ１０６において、ステップＳ１０５で算出した暗号化データ：Ｅ（ＬＫ，Ｒｍｓ）と、ステップＳ１０３でロックコマンドとともにホスト装置から受信し、ステップＳ１０４で、メモリに格納した暗号化データ：Ｅ（ＬＫ，Ｒｍｓ）との比較照合処理［Ｅ（ＬＫ，Ｒｍｓ）＝Ｅ（ＬＫ，Ｒｍｓ）？］を実行する。
【００６８】
この比較照合処理において、両値が等しければ、ホスト装置は、正当な正しいＩＤとロックキー（ＬＫ）の組データを保有した正当な機器であると判定し、ステップＳ１０７においてロックコマンドに応じたロック処理、すなわち、後述するアンロック処理の成功を条件としてメモリに対するアクセスを可能とする設定を実行する。この際、情報記憶装置は、ロック処理を実行したホスト装置のキーセット［ＩＤ，ＬＫ］をフラッシュメモリ等の不揮発性メモリ（ＮＶＭ：Ｎｏｎ－Ｖｏｌａｔｉｌｅ　Ｍｅｍｏｒｙ）によって構成されるメモリ部２２０に格納保持する。
【００６９】
一方、ステップＳ１０６の比較照合処理において、両値が等しくないと判定されると、ステップＳ１０８において、ロックコマンドを送信してきたホスト装置は、正しいＩＤとロックキー（ＬＫ）の組データを保有していない不正機器であると判定し、ロック処理を実行せず、エラー通知をホスト装置に対して送信する。
【００７０】
（アンロック処理）

次に上述したロックマスターキー（ＬＭＫ）を適用したロック処理によるロックを解除するアンロック処理、すなわち情報記憶装置に対するアクセス制限を解除する処理について説明する。

【００７１】

図７にアンロック処理におけるホスト装置と、情報記憶装置間で実行される処理シーケンス図を示す。ホスト装置と、情報記憶装置は、それぞれ相互にデータ転送可能に接続されている。まず、ホスト装置が、乱数発生コマンドを情報記憶装置に対して出力する。乱数発生コマンドを受信した情報記憶装置は、所定長、例えば１６バイト乱数（Ｒｍｓ）の発生処理を実行し、発生乱数（Ｒｍｓ）と、先のロック処理の際にメモリに格納済みのホスト装置のＩＤ、すなわちロック処理を実行したホスト装置のＩＤをホスト装置に対して送信する。なお、情報記憶装置は、発生乱数（Ｒｍｓ）を制御部内のＲＡＭ等のメモリに格納しておく。

【００７２】

情報記憶装置からＩＤと、乱数（Ｒｍｓ）を受信したホスト装置は、まず、受信ＩＤが自己のＩＤと一致するか否かを判定する。一致していない場合は、他のホスト装置によるロックが実行されていることになり、そのロックを解除することはできない。

【００７３】

受信ＩＤが自己のＩＤと一致する場合は、そのホスト装置自身が実行したロックであり、解除処理としてのアンロックが可能となる。この場合、ホスト装置は、予めホスト装置内のメモリに格納済みのロックキー（ＬＫ）を暗号処理キーとした受信乱数（Ｒｍｓ）の暗号処理：Ｅ（ＬＫ，Ｒｍｓ）を実行し、その結果データを、アンロックコマンドとともに情報記憶装置に送信する。

【００７４】

暗号化データ：Ｅ（ＬＫ，Ｒｍｓ）を受信した情報記憶装置は、まず、自己のメモリに格納されているホスト装置ＩＤ、すなわち、ロック処理を実行したホスト装置のＩＤを読み出して、読み出したＩＤに対して、ロックマスターキー（ＬＭＫ）を適用したハッシュ値算出処理により、ロック処理を実行したホスト装置のＩＤに対応するロックキー（ＬＫ）を算出する。すなわち、

ＬＫ＝Ｈ（ＬＭＫ，ＩＤ）

により、ロック処理を実行したホスト装置のＩＤに対応するロックキー（ＬＫ）を算出する。

【００７５】

さらに、情報記憶装置は、自己のメモリに格納した乱数Ｒｍｓに対して、上述のハッシュ値算出により求めたロックキー（ＬＫ）を適用した暗号処理：Ｅ（ＬＫ，Ｒｍｓ）を実行し、ホスト装置から受信した暗号処理データ：Ｅ（ＬＫ，Ｒｍｓ）と一致するか否かの照合処理を実行する。

【００７６】

ホスト装置からの受信データ：Ｅ（ＬＫ，Ｒｍｓ）と、自身が算出した暗号処理データ：Ｅ（ＬＫ，Ｒｍｓ）とが一致すれば、正当なＩＤとＬＫの組データを持つホスト装置からのアンロック処理要求であると判定しアンロック処理を実行し、アンロック完了通知をホスト装置に対して送信する。不一致の場合は、正当なＩＤとＬＫの組データを持つホスト装置では無いと判定し、不正機器からのアンロック処理要求であると判定し、アンロック処理を行なわずエラー通知をホスト装置に送信する。

【００７７】

なお、情報記憶装置の実行するアンロック処理は、ロック処理の解除を意味し、コンテンツ等のデータ格納領域であるフラッシュメモリ等によって構成されるメモリ部（図３のメモリ部２２０）に対するアクセスを許可する設定とする処理である。

【００７８】

次に、図８に示すフローチャートを参照して、アンロック処理の手順について説明する。ステップＳ２０１において、情報記憶装置としてのメモリカードが、ホスト装置からの乱

数発生要求コマンドの受信に基づいて、乱数（Ｒｓｍ）を発生する。発生した乱数は、ステップＳ２０２において、先にロック処理を実行したホスト装置のＩＤとともに、ホスト装置によって読み出される。

【００７９】

ホスト装置は、メモリカードから読み出したＩＤと自己のホストＩＤが一致することで、アンロック可能と判断し、ステップＳ２０３において、アンロックコマンドとともに、受信乱数（Ｒｍｓ）をホスト装置のロックキー（ＬＫ）で暗号化したデータ：Ｅ（ＬＫ，Ｒｍｓ）を情報記憶装置としてのメモリカードに送信する。

【００８０】

ステップＳ２０４において、メモリカードは、受信した暗号化データ：Ｅ（ＬＫ，Ｒｍｓ）とを情報記憶装置内のメモリに書き込む。ステップＳ２０５において、メモリカードは、先のロック処理時にメモリに格納したロック処理を実行したホスト装置ＩＤを読み出して、読み出したＩＤに対して、自身のメモリに格納したロックマスターキー（ＬＭＫ）を適用してハッシュ値算出、すなわち、

Ｈ（ＬＭＫ，ＩＤ）＝ＬＫ

を実行し、ＩＤに対応するロックキー（ＬＫ）を算出する。

【００８１】

さらに、メモリカードは、算出したロックキー（ＬＫ）に基づいて、先にステップＳ２０１で発生した乱数（Ｒｍｓ）の暗号化処理を実行して、暗号化データ：Ｅ（ＬＫ，Ｒｍｓ）を照合用データとして算出する。

【００８２】

次に、メモリカードは、ステップＳ２０６において、ステップＳ２０５で算出した暗号化データ：Ｅ（ＬＫ，Ｒｍｓ）と、ステップＳ２０３でアンロックコマンドとともにホスト装置から受信し、ステップＳ２０４で、メモリに格納した暗号化データ：Ｅ（ＬＫ，Ｒｍｓ）との比較照合処理［Ｅ（ＬＫ，Ｒｍｓ）＝Ｅ（ＬＫ，Ｒｍｓ）？］を実行する。

【００８３】

この比較照合処理において、両値が等しければ、ホスト装置は、正当な正しいＩＤとロックキー（ＬＫ）の組データを保有した正当な機器であると判定し、ステップＳ２０７においてアンロックコマンドに応じたアンロック処理、すなわち、メモリに対するアクセスを可能とする設定を実行する。一方、ステップＳ２０６の比較照合処理において、両値が等しくないと判定されると、ステップＳ２０８において、アンロックコマンドを送信してきたホスト装置は、ロック処理を実行した正しいＩＤとロックキー（ＬＫ）の組データを保有したホスト装置ではないと判定し、アンロック処理、すなわちロック解除を実行せず、エラー通知をホスト装置に対して送信する。

【００８４】

上述したように、本処理例によれば、ホスト装置ＩＤと対応するロックキー（ＬＫ）の正当な組み合わせデータを持つホスト装置のみが、情報記憶装置に対するロック処理が実行でき、また、ロック解除としてのアンロック処理は、ロック処理を実行したホスト装置によってのみ可能となる。また、上述のロック処理およびアンロック処理において、情報記憶装置のみがホスト装置の認証処理を実行するいわゆる片側認証処理を実行する構成であるので、ホスト装置側の処理負担が軽減され、効率的な処理が可能となる。

【００８５】

また、上述したロック処理、アンロック処理は、情報記憶装置側において、その処理毎に発生した乱数を適用する構成であるので、過去の処理における記録データを適用することは不可能であり、過去処理のトレースに基づく不正処理を効果的に防止できる。

【００８６】

［機器グループでのロック処理構成］

上述したロック処理、アンロック処理は、１つのホスト装置毎に情報記憶装置が対応する処理として実行され、ロックを実行したホスト装置のみがアンロック処理が可能となる構成例であった。しかし、複数のホスト装置が、１つの情報記憶装置（メモリカード）を利

用する構成においては、あるホスト装置（機器Ａ）でデータを格納しロックした情報記憶装置（メモリカード）を他のホスト装置（機器Ｂ）で利用したいといった状況が発生する。

【００８７】

このような場合、ホスト装置（機器Ａ）でロック解除処理を行なわない限り、ホスト装置（機器Ｂ）ではロツク解除が実行できないことになる。以下では、このような場合に対応可能な構成、すなわち複数のホスト装置によって構成されるホスト装置のグループにおいて、各ホスト装置各々がロック処理アンロック処理を実行可能とした処理例について説明する。まず、図９を参照して本処理例の概要を説明する。

【００８８】

メモリカード等の情報記憶装置５２０のコンテンツ等のデータ格納領域であるフラッシュメモリ等によって構成されるメモリ部（図３のメモリ部２２０）に対するアクセス制限を有効にする処理をロック処理とし、アクセス制限を解除する処理をアンロック処理とする。この点は、前述した処理例と同様である。ロック処理およびアンロック処理を実行するのが、ホスト装置５１０である。

【００８９】

ホスト装置５１０は、先に図１、図２を参照して説明したように、メモリカード等の情報記憶装置５２０とのデータ転送を実行するインタフェースを有し、情報記憶装置５２０に対するデータ書き込みあるいは情報記憶装置５２０からのデータ読み出しを実行してデータ利用を行なうＰＣ、ＰＤＡ、デジタルカメラ、ＤＳＣ（Ｄｉｇｉｔａｌ　Ｓｔｉｌｌ　Ｃａｍｅｒａ）等の情報処理装置を含み、さらに、メモリカード等の情報記憶装置５２０に対するロック処理、アンロック処理実行専用機器としてのロック・アンロック用機器５１２も含まれる。

【００９０】

ホスト装置内のＲＯＭ等のメモリ５１５には、各ホスト装置固有の識別子としてのＩＤｓ（例えば１６バイトデータ）と、ロック処理、アンロック処理に適用する鍵データとしてのロックキー（ＬＫｓ）（例えば８バイトデータ）が格納される。このＩＤｓ，ＬＫｓは前述の処理例におけるＩＤ，ＬＫに対応するデータの組であり、上述の処理と同様のロック処理、アンロック処理に適用可能である。

【００９１】

このＩＤｓ、ＬＫｓは、プライマリＩＤ、プライマリロックキーであり、各ホスト装置の製造時にホスト装置内のＲＯＭ等のメモリに書き込まれ、ユーザによる書き換え不可能なデータとされる。これらのプライマリＩＤ（ＩＤｓ）、プライマリロックキー（ＬＫｓ）は、上述したＬＭＫ適用処理と全く同様、ホスト装置対情報記憶装置の１対１対応のロック処理、アンロック処理に適用できる。この、各ホスト装置に固有のプライマリＩＤ、プライマリロックキーからなるキーセット：［ＩＤｓ，ＬＫｓ］をプライマリキーセットと呼ぶ。

【００９２】

このプライマリキーセット：［ＩＤｓ，ＬＫｓ］を適用したロック処理をスタンダードロック処理と呼び、ホスト装置としての情報処理装置からスタンダードロックコマンドを情報記憶装置に対して出力することでスタンダードロックが実行され、アンロックコマンドの出力によりアンロック処理が実行される。

【００９３】

ホスト装置内のＲＯＭ等のメモリ５１５には、さらに、他のホスト装置に対してコピー供給可能なキーセットとしてのサブＩＤとサブロックキーの組データとしてのサブキーセット：［ＩＤｅｎ，ＬＫｅｎ］（ｎ＝１，２，・・）が１以上格納可能となる。

【００９４】

このサブキーセット：［ＩＤｅｎ，ＬＫｅｎ］は、複数のホスト装置において共通に格納可能な鍵であり、後述する処理手順により、他のホスト装置に格納済みのサブキーセット：［ＩＤｅｎ，ＬＫｅｎ］は、情報記憶装置を介して他のホスト装置にコピー格納するこ

とが可能である。

【００９５】

サブキーセット：［ＩＤｅｎ，ＬＫｅｎ］を適用して、情報記憶装置（メモリカード）に対してロック処理を実行し、ロック処理に適用したサブキーセットを、情報記憶装置（メモリカード）を介して他のホスト装置にコピー出力可能とした態様のロック処理をエクスポートロック処理と呼ぶ。

【００９６】

このサブキーセット：［ＩＤｅｎ，ＬＫｅｎ］を適用したロック処理をエクスポートロック処理と呼び、ホスト装置としての情報処理装置からエクスポートロックコマンドを情報記憶装置に対して出力することでエクスポートロックが実行され、アンロックコマンドの出力によりアンロック処理が実行される。

【００９７】

エクスポートロックのなされた情報記憶装置（メモリカード）から、ホスト装置が入手したサブキーセット：［ＩＤｅｎ，ＬＫｅｎ］は、そのホスト装置内のメモリに書き込み可能となる。このサブキーセットのコピー書き込み処理をインプリント処理と呼ぶ。インプリント処理により、同一のサブキーセット：［ＩＤｅｎ，ＬＫｅｎ］を有する複数のホスト装置からなるグループが形成される。

【００９８】

このように、サブキーセット：［ＩＤｅｎ，ＬＫｅｎ］は、外部に出力可能な設定としたロック処理、すなわちエクスポート（ｅｘｐｏｒｔ）ロック処理に適用可能なキーセットであり、それぞれ、ＩＤ，ＬＫに［ｅ］を添えて示す。［ｅｎ］のｎは、サブキーセットナンバーを示し、設定したグループ数に相当する。

【００９９】

各ホスト装置は、複数の異なるサブキーセットを格納可能である。例えば、サブキーセット１：［ＩＤｅ１，ＬＫｅ１］を、ホスト装置としてのＰＣ（Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ）－ａ，ＰＣ－ｂ，ＰＤＡ（Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｔｓ）－ａの３つのホスト装置からなるグループの共有サブキーセット（サブ１）として設定し、サブキーセット２：［ＩＤｅ２，ＬＫｅ２］を、ＰＣ－ａ，ＰＤＡ－ａ．ＰＤＡ－ｂのグループの共有サブキーセット（サブ２）として設定した場合、各ホスト装置は、それぞれのプライマリＩＤ（ＩＤｓ）、プライマリロックキー（ＬＫｓ）からなるプライマリキーセット［ＩＤｓ，ＬＫｓ］をメモリに格納するとともに、

ＰＣ－ａは、［ＩＤｅ１，ＬＫｅ１］，［ＩＤｅ２，ＬＫｅ２］

ＰＣ－ｂは、［ＩＤｅ１，ＬＫｅ１］

ＰＤＡ－ａは、［ＩＤｅ１，ＬＫｅ１］，［ＩＤｅ２，ＬＫｅ２］

ＰＤＡ－ｂは、［ＩＤｅ２，ＬＫｅ２］

の各サブＩＤとサブロックキーからなるサブキーセットを、それぞれ格納することになる。

【０１００】

これらのサブＩＤとサブロックキーの組データからなるサブキーセット：［ＩＤｅｎ，ＬＫｅｎ］を自己のメモリ５１５内に書き込むことで、１以上のホスト装置からなるホスト装置グループ－ｎの構成メンバーとなることができ、グループｎのメンバは、共通に保有するサブＩＤ（ＩＤｎ）、共通のサブロックキー（ＬＫｎ）を適用して、１つの情報記憶装置（メモリカード）に対するロック処理、アンロック処理が可能となる。

【０１０１】

一方、メモリカード等の情報記憶装置５２０内の制御部内のＲＯＭ等のメモリ５２５には、ロックマスターキー（ＬＭＫ）が格納される。情報記憶装置５２０に格納されるロックマスターキー（ＬＭＫ）と、ホスト装置に格納されるＩＤ（ＩＤｓおよびＩＤｅｎを含む）と、ロックキー（ＬＫ（ＬＫｓとＬＫｅｎを含む））とは、以下の関係を持つ。

ＬＫ＝Ｈ（ＬＭＫ，ＩＤ）

【０１０２】

このロックマスターキー（ＬＭＫ）と、ＩＤ，ＬＫとの対応は、前述のＬＭＫの適用処理と全く同様であり、プライマリＩＤ（ＩＤｓ）に対するロックマスターキーＬＭＫを適用したハッシュ値算出処理により、プライマリロックキー（ＬＫｓ）が算出され、サブＩＤ（ＩＤｅｎ）に対するロックマスターキーＬＭＫを適用したハッシュ値算出処理により、サブロックキー（ＬＫｅｎ）が算出される。

【０１０３】

プライマリキーセット［ＩＤｓ，ＬＫｓ］と、サブキーセット［ＩＤｅｎ，ＬＫｅｎ］を利用したロック処理態様について、図１０を参照して説明する。ロック処理態様には、図１０（ａ）～（ｃ）に示す３つの態様がある。

【０１０４】

（ａ）は、各ホスト装置５１０に固有のプライマリＩＤ（ＩＤｓ）と、プライマリロックキー（ＬＫｓ）とからなるプライマリキーセット［ＩＤｓ，ＬＫｓ］５３１を適用したスタンダードロック処理である。

【０１０５】

プライマリキーセット：［ＩＤｓ，ＬＫｓ］５３１を適用したスタンダードロック処理は、ホスト装置５１０から情報記憶装置５２０に対してスタンダードロックコマンドを出力することで実行され、アンロックコマンドの出力によりアンロック処理が実行される。

【０１０６】

スタンダードロック処理がなされると、ロック情報記憶装置（メモリカード）５２０の記憶部（フラッシュメモリ）のスタンダードロックキーセット格納領域５４１にプライマリキーセット［ＩＤｓ，ＬＫｓ］が格納される。このロック処理が実行されると、スタンダードロックに適用したプライマリキーセット［ＩＤｓ，ＬＫｓ］は、ロック情報記憶装置（メモリカード）５２０から外部に出力されることはなく、ロック解除（アンロック）処理が実行できるのは、同一のプライマリキーセット［ＩＤｓ，ＬＫｓ］を有するホスト装置、すなわちスタンダードロック処理を実行した唯一のホスト装置となる。

【０１０７】

プライマリＩＤ（ＩＤｓ）、プライマリロックキー（ＬＫｓ）からなるプライマリキーセット［ＩＤｓ，ＬＫｓ］は、上述したＬＭＫ適用処理と全く同様、ホスト装置対情報記憶装置の１対１対応のロック処理、アンロック処理に適用でき、図５乃至図８を参照して説明した処理と同様な処理でのロック処理、アンロック処理が可能である。

【０１０８】

（ｂ）は、複数のホスト装置が共有可能なサブＩＤ（ＩＤｅｎ）と、サブロックキー（ＬＫｅｎ）とからなるサブキーセット［ＩＤｅｎ，ＬＫｅｎ］５３２を適用したエクスポートロック処理である。

【０１０９】

サブキーセット［ＩＤｅｎ，ＬＫｅｎ］５３２を適用したエクスポートロック処理は、ホスト装置５１０から情報記憶装置５２０に対してエクスポートロックコマンドを出力することで実行され、アンロックコマンドの出力によりアンロック処理が実行される。

【０１１０】

エクスポートロック処理がなされると、ロック情報記憶装置（メモリカード）５２０の記憶部（フラッシュメモリ）のエクスポートロックキーセット格納領域５４２にサブキーセット［ＩＤｅｎ，ＬＫｅｎ］が格納される。このロック処理が実行された場合、エクスポートロックに適用したサブキーセット［ＩＤｅｎ，ＬＫｅｎ］は、後段で詳細に説明するインプリント処理を実行することで、他のホスト装置が、ロック情報記憶装置（メモリカード）５２０から入手することが可能となる。

【０１１１】

このエクスポートロック処理が実行された場合、ロック解除（アンロック）処理が実行できるのは、ロック処理を実行したホスト装置と、インプリント処理によって、エクスポートロックに適用したサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を入手したホスト装置となる。

【０１１２】
（ｃ）は、各ホスト装置５１０が共有可能なサブＩＤ（ＩＤｅｎ）と、サブロックキー（ＬＫｅｎ）とからなるサブキーセット［ＩＤｅｎ，ＬＫｅｎ］５３２を適用したスタンダードロック処理である。この処理をグループロックと呼ぶ。
【０１１３】
サブキーセット［ＩＤｅｎ，ＬＫｅｎ］５３２を適用したスタンダードロック処理、すなわちグループロック処理は、ホスト装置５１０から情報記憶装置５２０に対してスタンダードロックコマンドを出力することで実行され、アンロックコマンドの出力によりアンロック処理が実行される。ただし、この処理の際に適用するキーセットは、サブキーセット［ＩＤｅｎ，ＬＫｅｎ］５３２となる。
【０１１４】
これは、基本的には、スタンダードロックと同様の処理であり、適用するキーセットをサブキーセット［ＩＤｅｎ，ＬＫｅｎ］５３２とした処理である。このグループロック処理がなされると、ロック情報記憶装置（メモリカード）５２０の記憶部（フラッシュメモリ）のスタンダードロックキーセット格納領域５４１にサブキーセット［ＩＤｅｎ，ＬＫｅｎ］が格納される。このロック処理が実行されると、グループロックに適用したサブキーセット［ＩＤｅｎ，ＬＫｅｎ］は、スタンダードロックキーセット格納領域５４１に格納されるので、ロック情報記憶装置（メモリカード）５２０から外部に出力されることはない。
【０１１５】
このグループロックの解除（アンロック）処理が実行できるのは、同一のサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を有するホスト装置である。ただし、この場合、グループロックを実行したホスト装置のみならず、すでに同一のサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を事前に入手したホスト装置が含まれる。
【０１１６】
例えば、事前に同一のサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を適用したエクスポートロック処理が行なわれ、そのエクスポートロック処理の実行時にインプリント処理により同一のサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を入手し、メモリに格納しているホスト装置は、アンロックが可能となる。
【０１１７】
サブキーセット［ＩＤｅｎ，ＬＫｅｎ］を適用したスタンダードロック、すなわちグループロックにおけるロック処理、アンロック処理のシーケンスは、上述したＬＭＫ適用処理と同様のシーケンス（図５乃至図８参照）となる。ただし、ロック／アンロックを実行できるホスト装置が、インプリント処理により複数になり得る点が異なる。
【０１１８】
以下、複数のホスト装置において共有可能なサブＩＤ（ＩＤｅｎ）、サブロックキー（ＬＫｅｎ）、すなわち、サブキーセット［ＩＤｅｎ，ＬＫｅｎ］を適用したロック処理、および、情報記憶装置（メモリカード）を介したホスト装置に対するサブキーセット［ＩＤｅｎ，ＬＫｅｎ］のコピー格納処理（インプリント処理）および、エクスポートロックの解除としてのアンロック処理について説明する。
【０１１９】
（サブキーセットに基づくロック処理）
まず、サブＩＤ（ＩＤｅｎ）、サブロックキー（ＬＫｅｎ）からなるサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を適用した情報記憶装置（メモリカード）に対するロック処理の詳細について説明する。
【０１２０】
前述したように、サブキーセット：［ＩＤｅｎ，ＬＫｅｎ］を適用した情報記憶装置（メモリカード）に対するロック処理により、ロック処理に適用したサブキーセットを、情報記憶装置（メモリカード）を介して他のホスト装置にコピー出力可能としたエクスポートロック処理が可能となる。

【０１２１】
図１１にサブキーセットに基づくロック処理におけるホスト装置と、情報記憶装置間で実行される処理シーケンス図を示す。ホスト装置と、情報記憶装置は、それぞれ相互にデータ転送可能に接続されている。
【０１２２】
なお、情報記憶装置は、図１１に示すロックステータスフラグ５５１を有し、情報記憶装置におけるロック状態を示す値を保持する。上段のＮＶＭは、図３において説明したフラッシュメモリ等によって構成されるメモリ部２２０のＮＶＭ（Ｎｏｎ－Ｖｏｌａｔｉｌｅ　Ｍｅｍｏｒｙ）領域に格納されるフラグであり、下段は、制御部２１０内のＲＡＭ２１３に格納されるフラグである。情報記憶装置の電源オフにより、ＲＡＭ内のフラグは消去されるが、ＮＶＭのフラグデータは維持される。従ってＲＡＭのフラグの書き換えに応じて、ＮＶＭに対するフラグデータのコピーが実行され、電源オフ後、新たに電源オンとなった場合に、ＮＶＭのフラグ情報がＲＡＭにコピーされる。なおＳＬはスタンダードロック、ＥＬはエクスポートロックであり、１がロック状態、０が非ロック状態を示す。
【０１２３】
スタンダードロックは、ロックに適用したキーセット［ＩＤ，ＬＫ］の外部出力を認めないロック態様であり、エクスポートロックは、ロックに適用したキーセット［ＩＤ，ＬＫ］の外部出力を認めたロック態様であり、ＳＬ＝１は、スタンダードロック状態であること、ＥＬ＝１は、エクスポートロック状態であることを示している。
【０１２４】
情報記憶装置（メモリカード）は、スタンダードロックに適用したキーセットと、エクスポートロックに適用したキーセットとをそれぞれ格納するデータ格納領域をメモリ部（フラッシュメモリ（ＮＶＭ））内に有する。
【０１２５】
初期状態としては、図に示すように、ＳＬ＝０，ＥＬ＝０であり、スタンダードロック（ＳＬ）、エクスポートロック（ＥＬ）のいずれも行われていない、すなわちすべてのホスト装置が情報記憶装置のメモリ部に対してアクセス可能な状態である。
【０１２６】
この初期状態において、まず、ホスト装置が、乱数発生コマンドを情報記憶装置に対して出力する。乱数発生コマンドを受信した情報記憶装置は、所定長、例えば１６バイトの乱数（Ｒｍｓ）の発生処理を実行し、発生乱数（Ｒｍｓ）をホスト装置に対して送信する。なお、情報記憶装置は、発生乱数（Ｒｍｓ）を制御部内のＲＡＭ等のメモリに格納しておく。
【０１２７】
情報記憶装置から乱数（Ｒｍｓ）を受信したホスト装置は、予めホスト装置内のメモリに格納済みのサブロックキー（ＬＫｅｎ）を暗号処理キーとした受信乱数（Ｒｍｓ）の暗号処理：Ｅ（ＬＫｅｎ，Ｒｍｓ）を実行する。暗号処理アルゴリズムは様々なアルゴリズムの適用が可能であり、例えばＤＥＳ暗号処理アルゴリズムが適用される。
【０１２８】
ホスト装置は、サブロックキー（ＬＫｅｎ）を暗号処理キーとした受信乱数（Ｒｍｓ）の暗号処理：Ｅ（ＬＫｅｎ，Ｒｍｓ）を実行し、その結果データ［Ｅ（ＬＫｅｎ，Ｒｍｓ）］と、ホスト装置が予めホスト装置内のメモリに格納しているサブロックキー（ＬＫｅｎ）に対応する組みデータとしてのサブＩＤ（ＩＤｅｎ）とを、ロックコマンドとともに情報記憶装置に送信する。
【０１２９】
データ：ＩＤｅｎ，Ｅ（ＬＫｅｎ，Ｒｍｓ）を受信した情報記憶装置は、まず、受信したサブＩＤ（ＩＤｅｎ）に対して、自己のメモリに格納されているロックマスターキー（ＬＭＫ）を適用したハッシュ値算出処理により、受信サブＩＤ（ＩＤｅｎ）に対応するサブロックキー（ＬＫｅｎ）を算出する。すなわち、
ＬＫｅｎ＝Ｈ（ＬＭＫ，ＩＤｅｎ）

により、受信サブＩＤ（ＩＤｅｎ）に対応するサブロックキー（ＬＫｅｎ）を算出する。なお、受信サブＩＤ（ＩＤｅｎ）は、自己のメモリに格納保持する。受信サブＩＤ（ＩＤｅｎ）は、後述するアンロック処理の際に利用される。

【０１３０】

さらに、情報記憶装置は、自己のメモリに格納した乱数Ｒｍｓに対して、上述のハッシュ値算出により求めたサブロックキー（ＬＫｅｎ）を適用した暗号処理：Ｅ（ＬＫｅｎ，Ｒｍｓ）を実行し、ホスト装置から受信した暗号処理データ：Ｅ（ＬＫｅｎ，Ｒｍｓ）と一致するか否かの照合処理を実行する。なお、暗号処理アルゴリズムはホスト装置と同一のアルゴリズムであれば、様々なアルゴリズムの適用が可能である。

【０１３１】

ホスト装置からの受信データ：Ｅ（ＬＫｅｎ，Ｒｍｓ）と、自身が算出した暗号処理データ：Ｅ（ＬＫｅｎ，Ｒｍｓ）とが一致すれば、正当なサブＩＤ（ＩＤｅｎ）と、サブロックキー（ＬＫｅｎ）の組データを持つ正当なホスト装置からのロック処理要求であると判定しエクスポートロック処理を実行し、ロック完了通知をホスト装置に対して送信する。不一致の場合は、正当なサブＩＤ（ＩＤｅｎ）とサブロックキー（ＬＫｅｎ）の組データを持つホスト装置では無いと判定し、不正機器からのロック処理要求であると判定し、エクスポートロック処理を行なわずエラー通知をホスト装置に送信する。

【０１３２】

なお、情報記憶装置の実行するエクスポートロック処理は、コンテンツ等のデータ格納領域であるフラッシュメモリ等によって構成されるメモリ部（図３のメモリ部２２０）に対するアクセスを、次に説明するサブＩＤ、サブロックキーを適用したアンロック処理を実行することを条件として許可する設定とする処理であり、エクスポートロックに適用されたエクスポートキーセット：［ＩＤｅｎ，ＬＫｅｎ］を情報記憶装置（メモリカード）のメモリ部（フラッシュメモリ（ＮＶＭ））のエクスポートロックキーセット格納領域に格納する。さらに、ロックステータスフラグの書き換えを実行する。

【０１３３】

エクスポートロックが実行されると、図に示すように、ロックステータスフラグは、エクスポートロックが有効な状態を示すフラグ：ＥＬ＝１がＮＶＭ，ＲＡＭそれぞれに格納される。これらのフラグは、まず情報記憶装置の制御部内のＲＡＭ２１３（図３参照）にＥＬ＝１が設定された後、ＮＶＭ（フラッシュメモリによって構成されるメモリ部２２０）にＥＬ＝１がコピーされる。この状態で、情報記憶装置の電源がオフとなると、ＲＡＭのフラグ情報は消去されるが、ＮＶＭのフラグ情報は維持され、その後、再び情報記憶装置の電源がオンとなると、ＮＶＭのフラグ情報（ＥＬ＝１）がＲＡＭにコピーされ、制御部２１０（図３参照）は、ＲＡＭのフラグ情報（ＥＬ＝１）に基づく処理を行なう。

【０１３４】

フラグ情報がＥＬ＝１である場合は、エクスポートロック状態であることを示し、情報記憶装置（メモリカード）のＮＶＭ（フラッシュメモリによって構成されるメモリ部２２０）のエクスポートロックキーセット格納領域に格納されたサブキーは、後述するインプリント処理によって他のホスト装置に出力可能となる。

【０１３５】

次に、図１２に示すフローチャートを参照して、エクスポートロック処理の手順について説明する。ステップＳ３０１において、情報記憶装置としてのメモリカードが、ホスト装置からの乱数発生要求コマンドの受信に基づいて、乱数（Ｒｓｍ）を発生する。発生した乱数は、ステップＳ３０２において、ホスト装置によって読み出され、ステップＳ３０３において、ロックコマンドとともに、ホスト装置の記憶部に格納済みのサブＩＤ（ＩＤｅｎ）を取得し、さらに、受信乱数（Ｒｍｓ）をホスト装置の記憶部に格納済みのサブロックキー（ＬＫｅｎ）で暗号化し、データ：Ｅ（ＬＫｅｎ，Ｒｍｓ）を生成し、これらの連結データ：ＩＤｅｎ，Ｅ（ＬＫｅｎ，Ｒｍｓ）を情報記憶装置としてのメモリカードに送信する。

【０１３６】

ステップＳ３０４において、メモリカードは、受信したサブＩＤ（ＩＤｅｎ）、および暗号化データ：Ｅ（ＬＫｅｎ，Ｒｍｓ）とを情報記憶装置内のメモリに書き込む。ステップＳ３０５において、メモリカードは、自身のメモリに格納したロックマスターキー（ＬＭＫ）を適用して、受信サブＩＤ（ＩＤｅｎ）のハッシュ値算出、すなわち、
Ｈ（ＬＭＫ，ＩＤｅｎ）＝ＬＫｅｎ
を実行し、受信サブＩＤ（ＩＤｅｎ）に対応するサブロックキー（ＬＫｅｎ）を算出する。

【０１３７】

さらに、メモリカードは、算出したサブロックキー（ＬＫｅｎ）に基づいて、先にステップＳ３０１で発生した乱数（Ｒｍｓ）の暗号化処理を実行して、暗号化データ：Ｅ（ＬＫｅｎ，Ｒｍｓ）を照合用データとして算出する。

【０１３８】

次に、メモリカードは、ステップＳ３０６において、ステップＳ３０５で算出した暗号化データ：Ｅ（ＬＫｅｎ，Ｒｍｓ）と、ステップＳ３０３でロックコマンドとともにホスト装置から受信し、ステップＳ３０４で、メモリに格納した暗号化データ：Ｅ（ＬＫｅｎ，Ｒｍｓ）との比較照合処理［Ｅ（ＬＫｅｎ，Ｒｍｓ）＝Ｅ（ＬＫｅｎ，Ｒｍｓ）？］を実行する。

【０１３９】

この比較照合処理において、両値が等しければ、ホスト装置は、正当な正しいサブＩＤ（ＩＤｅｎ）とサブロックキー（ＬＫｅｎ）の組データとしてのサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を保有した正当な機器であると判定し、ステップＳ３０７においてロックコマンドに応じたロック処理、すなわち、後述するサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を適用したロックの解除処理としてのアンロック処理の成功を条件としてメモリに対するアクセスを可能とする設定を実行する。この際、前述のロックステータスフラグをＥＬ＝１に設定する。

【０１４０】

一方、ステップＳ３０６の比較照合処理において、Ｅ（ＬＫｅｎ，Ｒｍｓ）＝Ｅ（ＬＫｅｎ，Ｒｍｓ）が成立しないと判定されると、ステップＳ３０８において、ロックコマンドを送信してきたホスト装置は、正しいサブＩＤ（ＩＤｅｎ）とサブロックキー（ＬＫｅｎ）の組データを保有していない不正機器であると判定し、ロック処理を実行せず、エラー通知をホスト装置に対して送信する。

【０１４１】

上述した処理に従って、エクスポートロックのなされた情報記憶装置は、ロック処理を実行したサブＩＤ（ＩＤｅｎ）とサブロックキー（ＬＫｅｎ）の組データとして、同一のサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を保有したホスト装置であれば、前述の［ロックマスターキー（ＬＭＫ）に基づく処理］において説明したアンロック処理と、同様の処理手続きによってアンロックが可能となる。すなわち、適用するＩＤとロックキーを、サブＩＤ（ＩＤｅｎ）とサブロックキー（ＬＫｅｎ）に置き換えることでアンロックが可能となる。

【０１４２】

しかし、ロック処理を実行したサブキーセット［ＩＤｅｎ，ＬＫｅｎ］と同一のキーセットを保有していない他のホスト装置は、ロック処理に適用されたサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を取得しない限り情報記憶装置のロック解除、すなわちアクセスができない。

【０１４３】

正当なプライマリＩＤ（ＩＤｓ）とプライマリロックキー（ＬＫｓ）の組データとしてのプライマリーキーセット［ＩＤｓ，ＬＫｓ］を持つホスト装置は、エクスポートロックのなされた情報記憶装置に格納されているサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を情報記憶装置から取得することが可能であり、取得したサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を適用してロックを解除することが可能となる。情報記憶装置を介したサブキーセット［

ＩＤｅｎ，ＬＫｅｎ］の取得をインプリント処理と呼ぶ。
【０１４４】
このように、あるサブキーセット［ＩＤｅｎ，ＬＫｅｎ］に基づいて、ロック状態とされ、そのサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を他のホスト装置に出力可能なロック状態をエクスポートロック状態と呼ぶ。
【０１４５】
ホスト装置は、エクスポートロック状態にある情報記憶装置から、エクスポートロック処理に適用されたサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を取得（インプリント）することで、同一のサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を保有する複数のホスト装置によって構成されるグループの構成メンバーとなり、その後、取得したサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を適用してロックを解除することができる。以下、このインプリントおよび、ロック解除処理（アンロック処理）の詳細について説明する。
【０１４６】
（インプリントおよびアンロック処理）
ホスト装置が、上述したエクスポートロック処理によるロックがなされている情報記憶装置から、サブロックキー（ＬＫｅｎ）と、サブＩＤ（ＩＤｅｎ）とからなるサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を取得するインプリント処理と、エクスポートロック処理によるロックがなされている情報記憶装置のロックを解除するアンロック処理について説明する。
【０１４７】
図１３にホスト装置と、情報記憶装置間で実行されるインプリント処理とアンロック処理の処理シーケンス図を示す。ホスト装置と、情報記憶装置は、それぞれ相互にデータ転送可能に接続されている。なお、情報記憶装置のロックステータスフラグは、図に示すように、エクスポートロックが有効である状態を示すＥＬ＝１がＮＶＭ，ＲＡＭにそれぞれ設定されているものとする。
【０１４８】
ホスト装置は、情報記憶装置に対するエクスポートロックに適用したサブＩＤ（ＩＤｅｎ）とサブロックキー（ＬＫｅｎ）とからなるサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を有しておらず、情報記憶装置は、サブキーセット［ＩＤｅｎ，ＬＫｅｎ］をエクスポートキー格納領域に格納している。情報記憶装置は、いわゆるエクスポートロック状態にある。
【０１４９】
まず、ホスト装置が、乱数発生コマンドを情報記憶装置に対して出力する。乱数発生コマンドを受信した情報記憶装置は、所定長、例えば１６バイト乱数（Ｒｍｓ）の発生処理を実行し、発生乱数（Ｒｍｓ）と、先のエクスポートロック処理の際にメモリに格納済みのサブＩＤ（ＩＤｅｎ）、すなわちエクスポートロック処理に適用されたサブキーセット［ＩＤｅｎ，ＬＫｅｎ］中のサブＩＤ（ＩＤｅｎ）をホスト装置に対して送信する。なお、情報記憶装置は、発生乱数（Ｒｍｓ）を制御部内のＲＡＭ等のメモリに格納しておく。
【０１５０】
情報記憶装置からサブＩＤ（ＩＤｅｎ）と、乱数（Ｒｍｓ）を受信したホスト装置は、まず、受信サブＩＤ（ＩＤｅｎ）が自己のプライマリＩＤ（ＩＤｓ）と一致するか否かを判定する。一致していれば、前述のＬＭＫ適用処理（図７参照）と同様のプライマリロックキー（ＬＫｓ）を適用したアンロックが可能である。
【０１５１】
受信サブＩＤ（ＩＤｅｎ）が自己のプライマリＩＤ（ＩＤｓ）と一致していない場合は、他のホスト装置によるロックが実行されていることになるが、この受信サブＩＤ（ＩＤｅｎ）、およびサブロックキー（ＬＫｅｎ）を取得するインプリント処理により、サブキーセット［ＩＤｅｎ，ＬＫｅｎ］を適用したエクスポートロックを実行した他のホスト装置と同一のグループに属することが可能となる。
【０１５２】
すなわち、インプリント処理を実行して、サブＩＤ（ＩＤｅｎ）、サブロックキー（ＬＫ

ｅｎ）をそれぞれ取得し、これらの組データとしてのサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を自己のメモリに格納し、グループに属するホスト装置となり、取得したサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を適用してエクスポートロックの解除が可能となる。インプリント処理を実行する場合、ホスト装置は、情報記憶装置から受信したサブＩＤ（ＩＤｅｎ）をメモリに格納する。

【０１５３】

インプリント処理を実行するホスト装置は、次に、予めホスト装置内のメモリに格納済みのプライマリロックキー（ＬＫｓ）を暗号処理キーとした受信乱数（Ｒｍｓ）の暗号処理：Ｅ（ＬＫｓ，Ｒｍｓ）を実行し、その結果データとプライマリＩＤ（ＩＤｓ）とを、スタンダードロックコマンドとともに情報記憶装置に送信する。なおこのロック処理は、すでに、サブロックキー（ＬＫｅｎ）によるエクスポートロックがなされている情報記憶装置に対してさらにプライマリロックキー（ＬＫｓ）によるスタンダードロックをかける処理であるのでオーバーロック処理と呼ぶ。

【０１５４】

ホスト装置から、プライマリＩＤ（ＩＤｓ）と暗号化データ：Ｅ（ＬＫｓ，Ｒｍｓ）を受信した情報記憶装置は、まず、受信したプライマリＩＤ（ＩＤｓ）に対して、ロックマスターキー（ＬＭＫ）を適用したハッシュ値算出処理により、プライマリＩＤ（ＩＤｓ）に対応するプライマリロックキー（ＬＫｓ）を算出する。すなわち、

ＬＫｓ＝Ｈ（ＬＭＫ，ＩＤｓ）

により、プライマリＩＤ（ＩＤｓ）に対応するプライマリロックキー（ＬＫｓ）を算出する。

【０１５５】

さらに、情報記憶装置は、自己のメモリに格納した乱数Ｒｍｓに対して、上述のハッシュ値算出により求めたプライマリロックキー（ＬＫｓ）を適用した暗号処理：Ｅ（ＬＫｓ，Ｒｍｓ）を実行し、ホスト装置から受信した暗号処理データ：Ｅ（ＬＫｓ，Ｒｍｓ）と一致するか否かの照合処理を実行する。

【０１５６】

ホスト装置からの受信データ：Ｅ（ＬＫｓ，Ｒｍｓ）と、自身が算出した暗号処理データ：Ｅ（ＬＫｓ，Ｒｍｓ）とが一致すれば、正当なプライマリＩＤ（ＩＤｓ）と、プライマリロックキー（ＬＫｓ）の組データとしてのプライマリキーセット［ＩＤｓ，ＬＫｓ］を持つホスト装置からのオーバーロック処理要求であると判定しオーバーロック処理を実行し、オーバーロック完了通知をホスト装置に対して送信する。

【０１５７】

ホスト装置からの受信データ：Ｅ（ＬＫｓ，Ｒｍｓ）と、自身が算出した暗号処理データ：Ｅ（ＬＫｓ，Ｒｍｓ）とが不一致の場合は、正当なプライマリＩＤ（ＩＤｓ）と、プライマリロックキー（ＬＫｓ）の組データとしてのプライマリキーセット［ＩＤｓ，ＬＫｓ］を持つホスト装置では無いと判定し、不正機器からのオーバーロック処理要求であると判定し、オーバーロック処理を行なわずエラー通知をホスト装置に送信する。

【０１５８】

なお、情報記憶装置の実行するオーバーロック処理は、エクスポートロック状態にさらにスタンダードロックを重ねて行なった状態とするもので、情報記憶装置のロックステータスフラグは、図に示すように、エクスポートロックが有効である状態を示すＥＬ＝１がＮＶＭ，ＲＡＭにそれぞれ設定され、さらに、オーバーロック処理により、スタンダードロックが有効である状態を示すＳＬ＝１がＲＡＭに設定される。なお、ＲＡＭに設定されたフラグ情報は、電源オフ以前にＮＶＭにコピーされる。

【０１５９】

さらに、オーバーロック完了通知を受信したホスト装置は、インプリント処理および、ロック解除を続けて行なうものとする。ホスト装置は、再度、乱数発声コマンドを情報記憶装置に送信する。

【０１６０】

乱数発生コマンドを受信した情報記憶装置は、新たに第２の乱数（Ｒｍｓ２）の発生処理を実行し、
発生乱数（Ｒｍｓ２）と、
スタンダードロックを実行したホスト装置のプライマリＩＤ（ＩＤｓ）と、
エクスポートロック処理に適用されたサブＩＤ（ＩＤｅｎ）と、さらに、
サブＩＤ（ＩＤｅｎ）に対応するサブロックキー（ＬＫｅｎ）をプライマリＩＤ（ＩＤｓ）対応するプライマリロックキー（ＬＫｓ）によって暗号化した暗号化データ：Ｅ（ＬＫｓ，ＬＫｅｎ）の連結データ、
すなわち、
ＩＤｓ，Ｒｍｓ２，ＩＤｅｎ，Ｅ（ＬＫｓ，ＬＫｅｎ）
をホスト装置に対して送信する。なお、情報記憶装置は、発生乱数（Ｒｍｓ２）を制御部内のＲＡＭ等のメモリに格納しておく。

【０１６１】

情報記憶装置からデータ：ＩＤｓ，Ｒｍｓ２，ＩＤｅｎ，Ｅ（ＬＫｓ，ＬＫｅｎ）を受信したホスト装置は、まず、暗号化データ：Ｅ（ＬＫｓ，ＬＫｅｎ）を自身のメモリに格納されたプライマリロックキー（ＬＫｓ）を適用して復号し、サブロックキー（ＬＫｅｎ）を取得する。これは、先に取得したサブＩＤ（ＩＤｅｎ）に対応するサブロックキー（ＬＫｅｎ）であり、取得したサブーキーセット［ＩＤｅｎ，ＬＫｅｎ］をメモリに格納する。このインプリント手続きにより、このホスト装置は、グループＮｏ．ｎのグループに属することができる。

【０１６２】

次に、ホスト装置は、情報記憶装置のロック解除処理を続けて実行する。ホスト装置は、情報記憶装置から受信した暗号化データ：Ｅ（ＬＫｓ，ＬＫｅｎ）に対するプライマリロックキー（ＬＫｓ）を適用した復号により取得したサブロックキー（ＬＫｅｎ）に基づいて、情報記憶装置から受信した乱数（Ｒｍｓ２）の暗号化処理を実行し、暗号化データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）を生成して、アンロックコマンドとともに情報記憶装置に送信する。

【０１６３】

ホスト装置から、アンロックコマンドとともに暗号化データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）を受信した情報記憶装置は、まず、自身のメモリに格納済みのサブＩＤ（ＩＤｅｎ）に対して、ロックマスターキー（ＬＭＫ）を適用したハッシュ値算出処理により、サブＩＤ（ＩＤｅｎ）に対応するサブロックキー（ＬＫｅｎ）を算出する。すなわち、
ＬＫｅｎ＝Ｈ（ＬＭＫ，ＩＤｅｎ）
により、サブＩＤ（ＩＤｅｎ）に対応するサブロックキー（ＬＫｅｎ）を算出する。

【０１６４】

さらに、情報記憶装置は、自己のメモリに格納した乱数Ｒｍｓ２に対して、上述のハッシュ値算出により求めたサブロックキー（ＬＫｅｎ）を適用した暗号処理：Ｅ（ＬＫｅｎ，Ｒｍｓ２）を実行し、ホスト装置から受信した暗号処理データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）と一致するか否かの照合処理を実行する。

【０１６５】

ホスト装置からの受信データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）と、自身が算出した暗号処理データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）とが一致すれば、正当なサブＩＤ（ＩＤｅｎ）と、サブロックキー（ＬＫｅｎ）の組データを持つホスト装置からのロックの解除、すなわちアンロック処理要求であると判定しアンロック処理を実行し、アンロック完了通知をホスト装置に対して送信する。

【０１６６】

ホスト装置からの受信データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）と、自身が算出した暗号処理データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）とが不一致の場合は、正当なサブＩＤ（ＩＤｅｎ）と、サブロックキー（ＬＫｅｎ）の組データとしてのサブーキーセット［ＩＤｅｎ，ＬＫｅｎ］を持つホスト装置では無いと判定し、不正機器からのアンロック要求であると判定し、

アンロック処理を行なわずエラー通知をホスト装置に送信する。

【０１６７】

アンロック処理により、ロックステータスフラグは、ＥＬ＝１からＥＬ＝０に変更され、またエクスポートロックに対するオーバーロックとして設定されたスタンダードロックも解除されＳＬ＝１からＳＬ＝０に変更される。すなわち、スタンダードロックは、エクスポートロックの解除に併せて解除される。

【０１６８】

なお、ロックステータスフラグの変更シーケンスは、まず、制御部内のＲＡＭの格納フラグが書き替えられ、その後、適宜、例えば電源オフ実行前にＮＶＭにＲＡＭ内のフラグ情報がコピーされ、電源再投入時には、ＮＶＭのフラグ情報がＲＡＭにコピーされるシーケンスであり、制御部は、ＲＡＭのフラグ情報に基づくアクセス制限処理を実行する。

【０１６９】

次に、図１４および図１５に示すフローチャートを参照して、エクスポートロック処理によるロックがなされている情報記憶装置から、サブロックキー（ＬＫｅｎ）と、サブＩＤ（ＩＤｅｎ）からなるサブーキーセット［ＩＤｅｎ，ＬＫｅｎ］を取得するインプリント処理と、エクスポートロック処理によるロックがなされている情報記憶装置のロックを解除するアンロック処理の手順について説明する。

【０１７０】

ステップＳ４０１において、情報記憶装置としてのメモリカードが、ホスト装置からの乱数発生要求コマンドの受信に基づいて、乱数（Ｒｓｍ）を発生する。発生した乱数は、ステップＳ４０２において、先にエクスポートロック処理を実行したホスト装置が情報記憶装置に送信し、情報記憶装置のメモリ部のエクスポートロックキーセット格納領域に格納されたサブＩＤ（ＩＤｅｎ）とともに、ホスト装置によって読み出される。ホスト装置は、この時点で、サブキーセット［ＩＤｅｎ，ＬＫｅｎ］中のサブＩＤ（ＩＤｅｎ）を取得する。

【０１７１】

ホスト装置は、メモリカードから読み出したサブＩＤ（ＩＤｅｎ）と自己のプライマリＩＤ（ＩＤｓ）が一致しないことの確認により、情報記憶装置が、スタンダードロック状態ではなく、エクスポートロック状態にあると判断する。ホスト装置は、次に、ステップＳ４０３において、オーバーロックとしてのスタンダードロックコマンドとともに、受信乱数（Ｒｍｓ）をホスト装置のプライマリロックキー（ＬＫｓ）で暗号化したデータ：Ｅ（ＬＫｓ，Ｒｍｓ）と、自己のプライマリＩＤ（ＩＤｓ）を情報記憶装置としてのメモリカードに送信する。

【０１７２】

ステップＳ４０４において、情報記憶装置（メモリカード）は、ホスト装置から受信したプライマリＩＤ（ＩＤｓ）と、暗号化データ：Ｅ（ＬＫｓ，Ｒｍｓ）とを情報記憶装置内のメモリに書き込む。ステップＳ４０５において、メモリカードは、受信したプライマリＩＤ（ＩＤｓ）に対して、自身のメモリに格納したロックマスターキー（ＬＭＫ）を適用してハッシュ値算出、すなわち、

Ｈ（ＬＭＫ，ＩＤｓ）＝ＬＫｓ

を実行し、プライマリＩＤ（ＩＤｓ）に対応するプライマリロックキー（ＬＫｓ）を算出する。

【０１７３】

さらに、メモリカードは、算出したプライマリロックキー（ＬＫｓ）に基づいて、先にステップＳ４０１で発生した乱数（Ｒｍｓ）の暗号化処理を実行して、暗号化データ：Ｅ（ＬＫｓ，Ｒｍｓ）を照合用データとして算出する。

【０１７４】

次に、メモリカードは、ステップＳ４０６において、ステップＳ４０５で算出した暗号化データ：Ｅ（ＬＫｓ，Ｒｍｓ）と、ステップＳ４０３でスタンダードロックコマンドとともにホスト装置から受信し、ステップＳ４０４で、メモリに格納した暗号化データ：Ｅ（

ＬＫｓ，Ｒｍｓ）との比較照合処理［Ｅ（ＬＫｓ，Ｒｍｓ）＝Ｅ（ＬＫｓ，Ｒｍｓ）？］を実行する。

【０１７５】

この比較照合処理において、両値が等しければ、ホスト装置は、正当な正しいプライマリＩＤ（ＩＤｓ）とプライマリロックキー（ＬＫｓ）の組データとしてのプライマリキーセット［ＩＤｓ，ＬＫｓ］を保有した正当な機器であると判定し、ステップＳ４０７においてスタンダードロックコマンドに応じたスタンダードロック処理を実行する。これは、エクスポートロック状態にさらにスタンダードロックを重ねて行なうオーバーロック処理である。情報記憶装置のロックステータスフラグは、エクスポートロック、スタンダードロックがともに有効である状態を示すＥＬ＝１、ＳＬ＝１がＲＡＭに設定される。

【０１７６】

一方、ステップＳ４０６の比較照合処理において、両値が等しくないと判定されると、ステップＳ４０８において、スタンダードロックコマンドを送信してきたホスト装置は、正当なプライマリＩＤ（ＩＤｓ）とプライマリロックキー（ＬＫｓ）の組データとしてのプライマリキーセット［ＩＤｓ，ＬＫｓ］を保有したホスト装置ではないと判定し、オーバーロック処理を実行せず、エラー通知をホスト装置に対して送信する。

【０１７７】

ステップＳ４０７のオーバーロック処理としてのスタンダードロックが行われ、さらに。インプリント処理、ロック解除を実行する場合は、図１５のステップＳ５０１に進む。

【０１７８】

オーバーロック完了通知を受信したホスト装置は、再度、乱数発生コマンドを情報記憶装置に送信し、乱数発生コマンドを受信した情報記憶装置は、ステップＳ５０１において、新たに第２の乱数（Ｒｍｓ２）の発生処理を実行する。

【０１７９】

ステップＳ５０２において、ホスト装置は、
乱数（Ｒｍｓ２）と、
スタンダードロックを実行したホスト装置のプライマリＩＤ（ＩＤｓ）、
サブＩＤ（ＩＤｅｎ）、さらに、
サブＩＤ（ＩＤｅｎ）に対応する組みデータとしてのサブロックキー（ＬＫｅｎ）をプライマリＩＤ（ＩＤｓ）対応する組みデータとしてのプライマリロックキー（ＬＫｓ）によって暗号化した暗号化データ：Ｅ（ＬＫｓ，ＬＫｅｎ）、
これらの連結データ、すなわち、［ＩＤｓ，Ｒｍｓ２，ＩＤｅｎ，Ｅ（ＬＫｓ，ＬＫｅｎ）］を情報記憶装置から読み出す。

【０１８０】

ステップＳ５０３において、ホスト装置は、情報記憶装置に対するロック解除要求としてのアンロックコマンドを送信する。ホスト装置は、このアンロックコマンドに、暗号化データＥ（ＬＫｅｎ，Ｒｍｓ２）を併せて送信する。

【０１８１】

暗号化データＥ（ＬＫｅｎ，Ｒｍｓ２）の生成手法は、以下の手順に従ったものである。
ステップＳ５０２において、情報記憶装置からデータ：ＩＤｓ，Ｒｍｓ２，ＩＤｅｎ，Ｅ（ＬＫｓ，ＬＫｅｎ）を読み出したホスト装置は、まず、暗号化データ：Ｅ（ＬＫｓ，ＬＫｅｎ）を自身のメモリに格納されたプライマリロックキー（ＬＫｓ）を適用して復号し、サブロックキー（ＬＫｅｎ）を取得する。これは、先に取得したサブＩＤ（ＩＤｅｎ）に対応するサブロックキー（ＬＫｅｎ）である。次に、ホスト装置は、サブロックキー（ＬＫｅｎ）に基づいて、情報記憶装置から受信した乱数（Ｒｍｓ２）の暗号化処理を実行し、暗号化データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）を生成する。

【０１８２】

なお、ホスト装置は、取得したサブキーセット：［ＩＤｅｎ，ＬＫｅｎ］をメモリに格納して、インプリント処理は完了する。すなわち、インプリント処理により、このホスト装置は、グループＮｏ．ｎのグループに属する。

【０１８３】
ステップＳ５０４において、ホスト装置から、暗号化データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）を受信した情報記憶装置は、受信データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）をメモリに書き込む。さらにステップＳ５０５において、照合用データの算出を実行する。
【０１８４】
照合用データの算出処理は、以下の手順で実行する。まず、自身のメモリに格納済みのサブＩＤ（ＩＤｅｎ）に対して、ロックマスターキー（ＬＭＫ）を適用したハッシュ値算出処理により、サブＩＤ（ＩＤｅｎ）に対応するサブロックキー（ＬＫｅｎ）を算出する。すなわち、
ＬＫｅｎ＝Ｈ（ＬＭＫ，ＩＤｅｎ）
により、サブＩＤ（ＩＤｅｎ）に対応するサブロックキー（ＬＫｅｎ）を算出する。さらに、ステップＳ５０１で発生しメモリに格納した乱数Ｒｍｓ２に対して、上述のハッシュ値算出により求めたサブロックキー（ＬＫｅｎ）を適用した暗号処理：Ｅ（ＬＫｅｎ，Ｒｍｓ２）を実行し照合用データを生成する。
【０１８５】
ステップＳ５０６において、情報記憶装置は、照合用データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）と、ホスト装置から受信した暗号処理データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）と一致するか否かの照合処理を実行する。
【０１８６】
ホスト装置からの受信データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）と、自身が算出した暗号処理データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）とが一致すれば、正当なサブＩＤ（ＩＤｅｎ）と、サブロックキー（ＬＫｅｎ）の組データとしてのサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を持つホスト装置からのロックの解除、すなわちアンロック処理要求であると判定し、ステップＳ５０７に進み、アンロック処理を実行し、アンロック完了通知をホスト装置に対して送信する。不一致の場合は、正当なサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を持つホスト装置では無いと判定し、不正機器からのアンロック処理要求であると判定し、アンロック処理を行なわずステップＳ５０８において、エラー通知をホスト装置に送信する。
【０１８７】
本処理例に従えば、複数のホスト装置が、共通のサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を保有し、１つの情報記憶装置（メモリカード）を利用したロック、アンロックが可能となる。また、サブキーセット［ＩＤｅｎ，ＬＫｅｎ］は、エクスポートロックを実行することにより、情報記憶装置を介して他のホスト装置にコピー格納するこが可能であり、柔軟なグループ形成が可能となる。また、サブキーセット［ＩＤｅｎ，ＬＫｅｎ］のホスト装置に対するコピー、すなわちインプリントにおいては、正当なプライマリＩＤ（ＩＤｓ）とプライマリロックキー（ＬＫｓ）を所有し、オーバーロック処理が実行可能であることが条件となるので、不正機器に対するサブキーセット［ＩＤｅｎ，ＬＫｅｎ］のコピー（インプリント）は防止可能となる。
【０１８８】
なお、先に図１０（ｃ）を参照して説明したように、サブキーセット［ＩＤｅｎ，ＬＫｅｎ］を適用したスタンダードロック処理（＝グループロック処理）の実行も可能であり、このグループロック処理を実行した場合は、サブキーセット［ＩＤｅｎ，ＬＫｅｎ］は、情報記憶装置のスタンダードロックキー格納領域（図１０参照）に格納され、他のホスト装置に対するコピー出力はなされない。すなわち、すでに同一のサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を取得済みのホスト装置のみが、インプリント処理を伴わない通常のアンロック処理によりアクセス可能となる。
【０１８９】
［ロック状態フラグの維持構成］
上述した「機器グループでのロック処理構成」において、エクスポートロック状態にある情報記憶装置に対してアンロックを実行すると、全てのロックステータス（状態）フラグがリセット、すなわち、エクスポートロック解除を示すＥＬ＝０，スタンダードロック解

除を示すＳＬ＝０がＮＶＭ，ＲＡＭに設定される。このように、ＥＬ＝０，ＳＬ＝０の設定のまま、電源をオフにし、その後、電源を再度オンとした場合、ＮＶＭには、ＥＬ＝０，ＳＬ＝０が設定されているので、制御部のＲＡＭもＳＬ＝０，ＥＬ＝０の設定状態となり、全てのロック状態が解放され、各ホスト装置が自由にメモリに対するアクセスを行なうことが可能となる。

【０１９０】

このようにロックが解除された情報記憶装置は、紛失、盗難等により、不正な第三者に取得された場合、自由にメモリアクセスが可能となる。このような状況は、秘密情報を格納する場合には好ましいとは言えない。

【０１９１】

以下に説明する例は、上記問題点に鑑みてなされたものであり、ホスト装置がアンロック処理により、エクスポートロックの解除を行なった後に電源をオフとした場合においてもエクスポートロック状態を維持する構成としたものであり、情報記憶装置が、再度電源オンとなった場合、エクスポートロックの解除処理を条件としてメモリアクセスを許容する構成とした例である。

【０１９２】

本構成例は、先に「機器グループでのロック処理構成」において図９を参照して説明したと同様、ホスト装置内のＲＯＭ等のメモリには、プライマリＩＤ（ＩＤｓ）、プライマリロックキー（ＬＫｓ）からなるプイマリキーセット［ＩＤｓ，ＬＫｓ］が格納され、さらに、エクスポートロック処理に適用可能なサブＩＤとサブロックキーの組データとしてのサブキーセット［ＩＤｅｎ，ＬＫｅｎ］（ｎ＝１，２，・・）が１以上格納可能な構成であり、メモリカード等の情報記憶装置内の制御部内のＲＯＭ等のメモリには、ロックマスターキー（ＬＭＫ）が格納される。情報記憶装置に格納されるロックマスターキー（ＬＭＫ）と、ホスト装置に格納されるＩＤ（ＩＤｓおよびＩＤｅｎを含む）と、ロックキー（ＬＫ（ＬＫｓとＬＫｅｎを含む））とは、以下の関係を持つ。

ＬＫ＝Ｈ（ＬＭＫ，ＩＤ）

【０１９３】

ホスト装置によるプライマリＩＤ（ＩＤｓ）、プライマリロックキー（ＬＫｓ）に基づくロック処理、アンロック処理は、前述の［ロックマスターキー（ＬＭＫ）に基づく処理］において説明したと同様のシーケンスによって実行され、また、サブＩＤ（ＩＤｅｎ）、サブロックキー（ＬＫｅｎ）に基づくロック処理は、前述の［機器グループでのロック処理構成］において説明したと同様のシーケンスによって実行される。以下、本処理例におけるインプリントおよびアンロック処理におけるロックステータスフラグの維持処理について説明する。

【０１９４】

（インプリントおよびアンロック処理におけるロックステータスフラグの維持処理）

ホスト装置が、エクスポートロック処理によるロックがなされている情報記憶装置から、サブロックキー（ＬＫｅｎ）と、サブＩＤ（ＩＤｅｎ）とからなるサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を取得するインプリント処理と、エクスポートロック処理によるロックがなされている情報記憶装置のロックを解除するアンロック処理、さらに、情報記憶装置が実行するロックステータスフラグの維持処理について図１６以下を参照して説明する。

【０１９５】

図１６に示すシーケンス図は、先に、［機器グループでのロック処理構成］において図１３を参照して説明したホスト装置と、情報記憶装置間で実行されるインプリント処理とエクスポートロックのアンロック処理の処理シーケンス図と基本的に同一であり、処理手順も同様である。

【０１９６】

ただし、シーケンス図の最終処理として実行されるアンロック完了通知の後に、情報処理装置がＮＶＭフラグ設定処理を実行する点が異なる。すなわち、前述の［機器グループでのロック処理構成］において説明した処理では、エクスポートロックのアンロックが実行

されると、エクスポートロック解除を示すＥＬ＝０，スタンダードロック解除を示すＳＬ＝０がＮＶＭ，ＲＡＭに設定されていた。しかし、本構成では、ＮＶＭに、エクスポートロック、スタンダードロックがなされていることを示すＥＬ＝１，ＳＬ＝１を設定する。

【０１９７】

図１７を参照して、ＮＶＭに対するロックステータスフラグ設定処理の詳細について説明する。図１７の処理フローは、図１６（図１３と同様）のシーケンス図においてロック解除要求（アンロックコマンド）を受信した以降の情報記憶装置における処理手順を説明するフローである。

【０１９８】

まず、ステップＳ６０１において、情報記憶装置（メモリカード）がロックの解除要求（アンロックコマンド）を受信すると、情報記憶装置は、アンロックコマンドの実行可否を判定するための検証処理として、ステップＳ６０２において、ホスト装置から、アンロックコマンドとともに受信した暗号化データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）と、自身が生成した暗号化データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）との照合処理を実行する。この処理は、［機器グループでのロック処理構成］において説明したと同様の処理である。

【０１９９】

ホスト装置からの受信データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）と、自身が算出した暗号処理データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）とが一致しない場合は、ステップＳ６０７において、エラー通知をホストに返して処理を終了する。

【０２００】

一方、ホスト装置からの受信データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）と、自身が算出した暗号処理データ：Ｅ（ＬＫｅｎ，Ｒｍｓ２）とが一致した場合は、、正当なサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を持つホスト装置からのアンロック処理要求であると判定し、ステップＳ６０３において、アンロック処理を実行し、アンロック完了通知をホスト装置に対して送信する。

【０２０１】

さらに、情報記憶装置（メモリカード）は、ステップＳ６０４において、制御部のＲＡＭに格納されているロックステータスフラグ（ＳＬ＝１，ＥＬ＝１）をＮＶＭにコピーし、ＮＶＭのロックステータスフラグをＳＬ＝１，ＥＬ＝１に設定する。ＳＬ＝１は、スタンダードロックがなされていること、ＥＬ＝１は、エクスポートロックがなされていることを示す。

【０２０２】

ステップＳ６０４のフラグコピー処理が終了すると、さらに、ステップＳ６０５において、制御部のＲＡＭのロックステータスフラグ（ＳＬ＝１，ＥＬ＝１）のリセット、すなわちＲＡＭのロックステータスフラグをＳＬ＝０，ＥＬ＝０に設定する。ＳＬ＝０は、スタンダードロックがなされていないこと、ＥＬ＝０は、エクスポートロックがなされていないことを示す。

【０２０３】

この設定状態、すなわちＲＡＭのロックステータスフラグがＳＬ＝０，ＥＬ＝０の設定においてはメモリアクセスが自由に実行可能となり、アンロック処理を実行したホスト装置は、情報記憶装置のメモリ（図３のメモリ部２２０）に対するアクセスが可能となる。

【０２０４】

しかし、その後、情報記憶装置（メモリカード）がホスト装置から抜き取られるなどにより、情報記憶装置（メモリカード）に対する電源供給がストップし、再度、電源オンとなった時点で、ＮＶＭに設定されたロックステータスフラグ（ＳＬ＝１，ＥＬ＝１）情報が制御部のＲＡＭにロードされ、制御部は、ＲＡＭに設定されたロックステータスフラグ（ＳＬ＝１，ＥＬ＝１）に基づく処理を行なうことになる。図１８の処理フローを参照して、情報記憶装置の電源再投入後の処理について説明する。

【０２０５】

図１８の処理フローは、一旦、情報記憶装置の電源がオフとされ、再度、電源オン状態に

移行した場合の処理を示している。

【０２０６】

ステップＳ７０１において、情報記憶装置（メモリカード）がホスト装置にセットされることなどにより、電源オフ状態からオン状態に移行すると、情報記憶装置は、ステップＳ７０２において、ＮＶＭに格納してあるロックステータスフラグ（ＳＬ，ＥＬ）を制御部のＲＡＭにコピーする。制御部は、ＲＡＭのステータスフラグに応じて制御を実行する。

【０２０７】

ステップＳ７０３において、接続されたホスト装置からメモリアクセス要求、あるいはアンロックコマンドを入力すると、情報記憶装置の制御部は、ＲＡＭのロックステータスフラグを参照する。

【０２０８】

ステップＳ７０４において、ＲＡＭのステータスフラグがＥＬ＝１であると判定されると、ステップＳ７０５において、ロック解除処理（図１３～図１５参照）を実行する。この際、ホストが、その情報記憶装置のエクスポートロックに適用されたサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を有していない場合は、インプリント処理を実行することが必要となる。この処理において、先に図１３～図１５を参照して説明した検証により正当なホスト装置からのアンロック要求であることが確認されるとアンロック処理が実行（ステップＳ７０８：Ｙｅｓ）され、ステップＳ７０９においてメモリアクセスが許可される。検証により不正なホスト装置からのアンロック要求であると判定されるとアンロック処理が実行されず、（ステップＳ７０８：Ｎｏ）、エラー通知（Ｓ７１０）がなされる。

【０２０９】

また、ステップＳ７０４において、ＲＡＭのステータスフラグがＥＬ＝０であると判定されると、ステップＳ７０６において、ＲＡＭのステータスフラグがＳＬ＝１であるかい中が判定される。ＲＡＭのステータスフラグがＳＬ＝１であると判定されると、ステップＳ７０７において、スタンダードロック解除処理（図７～図８参照）を実行する。先に図７～図８を参照して説明した検証により正当なホスト装置からのアンロック要求であることが確認されるとアンロック処理が実行（ステップＳ７０８：Ｙｅｓ）され、ステップＳ７０９においてメモリアクセスが許可される。検証により不正なホスト装置からのアンロック要求であると判定されるとアンロック処理が実行されず、（ステップＳ７０８：Ｎｏ）、エラー通知（Ｓ７１０）がなされる。

【０２１０】

ステップＳ７０４において、ＲＡＭのステータスフラグがＥＬ＝０であると判定され、ステップＳ７０６において、ＲＡＭのステータスフラグがＳＬ＝０であると判定されると、ロック状態にはないことになり、ステップＳ７０９に進み、メモリアクセスが許可されることになる。

【０２１１】

先に、図１６，図１７を参照して説明したように、あるホスト装置により、エクスポートロックが解除され、その後電源がオフとなった場合は、ＮＶＭのロックステータスフラグがＳＬ＝１，ＥＬ＝１に設定され、その後、電源オンとなった時点で、ＲＡＭのロックステータスフラグがＳＬ＝１，ＥＬ＝１に設定されることになり、図１８の処理フローにおけるステップＳ７０４の判定（ＥＬ＝１？）がＹｅｓとなり、ステップＳ７０５の処理、すなわち、エクスポートロック解除処理（図１３～図１５参照）を条件としたメモリアクセス許可処理が行なわれることになる。

【０２１２】

上述したように、本処理例においては、ロック処理またはアンロック処理に適用可能なキーセットの外部出力が許容されるロック状態であるエクスポートロック（ＥＬ）状態であるか否か、および、ロック処理またはアンロック処理に適用可能なキーセットの外部出力が許容されないロック状態であるスタンダードロック（ＳＬ）状態であるか否かについて判別可能な状態情報からなるロックステータスフラグのアンロック処理前の情報をＮＶＭに格納する構成としたので、情報記憶装置の電源オフ後の電源再投入時に、ＮＶＭに格納

されたフラグに基づいて、アンロック処理前のロック状態を忠実に再現することが可能となる。

【０２１３】

本処理例によれば、例えば、あるホスト装置が、エクスポートロックの解除を行なった場合でも、エクスポートロック状態を維持し、情報記憶装置の電源オフ後、再度電源オンとなった場合において、ロックの解除処理を条件としたメモリアクセスの許可が可能となる。従って、正当なプライマリキーセット［ＩＤｓ，ＬＫｓ］を有するホスト装置が前述のオーバーロック処理を含む所定の手続きを実行した場合にのみロック解除が可能となり、不正な装置からのアクセス排除が可能となる。

【０２１４】

［特定データ領域読み出し検出による自動ロック処理］

次に、情報記憶装置（メモリカード）からホスト装置に対するデータの読み出しを情報記憶装置の制御部において監視し、ある予め定められたデータ領域（例えば特定クラスタ）の読み出し実行をトリガとして、ロック処理を実行する処理例について説明する。

【０２１５】

情報記憶装置（メモリカード）のメモリ部（図２のメモリ部２２０）に格納されるデータの読み出しは、例えば格納データに応じて生成される再生管理ファイル（ＰＢＬＩＳＴ）によって管理され、制御部では、再生管理ファイルに従って、メモリ部（図２のメモリ部２２０）からデータを読み出して、ホスト装置に出力する。

【０２１６】

データが読み出される場合、情報記憶装置の制御部は、読み出しデータの監視を行なうことが可能である。例えば、ＡＴＲＡＣ３で圧縮されたオーディオデータは、所定のデータ単位としてのクラスタを読み出しデータ単位として監視することができる。

【０２１７】

図１９に示すように、ＡＴＲＡＣ３で圧縮されたオーディオデータは、最小データ単位としてのＳＵ（サウンドユニット）を複数集めたクラスタ、さらに複数のクラスタによってパーツが構成される。ＳＵ（サウンドユニット）は、４４．１ｋＨｚのサンプリング周波数で得られた１０２４サンプル分（１０２４×１６ビット×２チャンネル）のオーディオデータを約１／１０に圧縮した数百バイトのデータであり、クラスタは、複数のＳＵ（たとえばＳＵ４２個）によって構成されるデータである。１クラスタが４２個のＳＵで構成される場合、１クラスタで約１秒の音を表すことができる。

【０２１８】

各クラスタには、各クラスタ固有の論理番号が付与され、論理番号による管理がなされる。情報記憶装置の制御部２１０（図３参照）は、特定クラスタの読み出しの有無を論理番号に基づいてチェックすることができる。例えば、出力データがある音楽コンテンツであるときに、その音楽コンテンツのイントロ、あるいはさび部分に相当する１以上のクラスタの論理番号を、そのコンテンツに対応するロック対応クラスタとして抽出し、抽出したクラスタ論理番号をコンテンツに対応する登録情報として設定して、コンテンツを格納するメモリ部（フラッシュメモリ）に併せて格納する。

【０２１９】

コンテンツの読み出し時に、登録情報を情報記憶装置の制御部内のメモリ（ＲＡＭ）に一次格納し、制御部において、読み出しコンテンツのクラスタと、ロック対応クラスタとの照合処理を実行し、読み出しコンテンツのクラスタがロック対応クラスタの論理番号に一致した場合に、ロック処理を実行する。なお、ロック処理のタイミングは、ロック対応クラスタの読み出し開始時点、ロック対応クラスタの読み出し終了時点、あるいは、ロック対応クラスタを持つコンテンツ全体の読み出し終了時点等、様々な設定が可能であり、設定に応じた検出処理を実行して、設定条件検出に基づいてロック処理を行なう。ロックが実行された場合は、再度の読み出しは、アンロック処理を実行することが必要となる。

【０２２０】

以下、図２０を参照して、情報記憶装置の制御部２１０において、メモリ部２２０（図３

参照）から特定データ領域（例えば特定クラスタ）が読み出されたことを条件としてロック処理を実行する処理について説明する。

【０２２１】

なお、図２０の処理フローでは、簡単のためにスタンダードロック（ＳＬ）についてのみ記載しているが、エクスポートロック（ＥＬ）についても同様の処理が可能である。

【０２２２】

まず、ステップＳ８０１において、情報記憶装置の電源がオンされると、ステップＳ８０２において、ＮＶＭに格納されたロックステータスフラグが制御部２１０（図３参照）のＲＡＭ２１３にコピー格納される。制御部は、ＲＡＭ２１３のステータスフラグに応じた制御を実行する。

【０２２３】

ステップＳ８０３において、スタンダードロックがＳＬ＝１であるか否か、すなわちロック状態にあるか否かが判定される。ＳＬ＝１である場合は、ステップＳ８０４においてアンロック処理が実行される。アンロック処理は、例えば図７、図８を参照して説明した処理と同様の処理である。

【０２２４】

ホスト装置が正当なプライマリＩＤとプライマリロックキーを保有していることが、情報記憶装置における検証処理により検証され、アンロックが成功する（Ｓ８０５：Ｙｅｓ）と、ステップＳ８０６に進む。アンロックに失敗した場合は、ステップＳ８１０においてホスト装置に対するエラー通知が実行されて処理を終了する。

【０２２５】

ステップＳ８０６では、アンロック成功に基づいて、ＲＡＭ，ＮＶＭのロックステータスフラグの更新、すなわち、ロック解除状態を示すＳＬ＝０の設定処理が実行される。

【０２２６】

次に、ホスト装置からのデータ読み出しが開始されると、情報記憶装置の制御部は、ステップＳ８０７において、あらかじめ設定されたロック対応クラスタの読み出し処理の有無の監視を実行する。ロック対応クラスタのデータ読み出しを検出すると、ステップＳ８０８において、制御部２１０（図３参照）のＲＡＭ２１３のロックステータスフラグをロック状態（ＳＬ＝１）に設定する。さらに、ステップＳ８０９において、ＮＶＭのロックステータスフラグをロック状態（ＳＬ＝１）に設定する。

【０２２７】

このように、所定のクラスタの読み出し処理を行なうことにより、ロックがかけられ、その後、再度読み出し処理を実行する場合は、アンロック処理が必要となる。アンロック処理は、ロックを実行したと同一のプライマリＩＤ（ＩＤｓ）とプライマリロックキー（ＬＫｓ）を有するホスト装置のみが可能となり、ロックされた情報記憶装置（メモリカード）が無秩序に利用されることが防止されることになる。

【０２２８】

なお、ロック情報は、情報記憶装置の電源オフ時に解除される設定、あるいは、前述したように、電源オフ時にもロックステータスフラグをＮＶＭに置き、電源再投入時にＮＶＭのロックステータスフラグを制御部のＲＡＭにコピーして、電源オフ前のロック状態を維持して再現する構成としてもよい。

【０２２９】

このように本処理例においては、アンロック処理後、データ読み出し処理を実行する場合、１度限りの読み出しを可能とした、いわゆるリードワンスのアクセス制限処理構成が実現される。

【０２３０】

なお、図２０の処理例ではスタンダードロックについてのみ示したが、エクスポートロックにおいても同様の構成、すなわち、所定のデータ領域の読み出しをトリガとしてエクスポートロックをかける構成とすることが可能である。

【０２３１】

［ホスト装置におけるロック状態提示構成］
次に、様々なロック状態を取り得る情報記憶装置に対するアクセスを実行するホスト装置において、情報記憶装置のロック状態を検出するための提示構成および提示処理について説明する。
【０２３２】
図２１にロック／アンロック専用機器におけるロック状態提示インジケータと、各種処理スイッチを持つ構成例を示す。情報記憶装置としてのメモリカード７１０とデータ転送可能なインタフェースを持つロック／アンロック専用機器７２０は、ロック状態インジケータとして、
ロック解除状態を示す［Ｕｎｌｏｃｋｅｄ］インジーケータ７２１
ロック状態を示す［Ｌｏｃｋｅｄ］インジーケータ７２２
エクスポートロック状態を示す［Ｅ－Ｌｏｃｋｅｄ］インジーケータ７２３
エラー通知を示す［ＥＲＲ］インジーケータ７２４
を有する。
【０２３３】
また、各種処理要求スイッチとして、
ロック解除処理要求スイッチとしての［Ｕｎｌｏｃｋ］スイッチ７３１
プライマリキーセットによるスタンダードロック処理要求スイッチとしての［Ｐ－Ｌｏｃｋ］スイッチ７３２
サブキーセットによるスタンダードロック（グループロック）処理要求スイッチとしての［Ｇ－Ｌｏｃｋ］スイッチ７３３
サブキーセットによるエクスポートロック処理要求スイッチとしての［Ｅ－Ｌｏｃｋ］スイッチ７３４を有する。
【０２３４】
さらに、図２１（ｂ）に示すロック／アンロック専用機器の例は、上記スイッチの他に、エクスポートロック状態にある情報記憶装置に格納されたサブＩＤ（ＩＤｅｎ）とサブロックキー（ＬＫｅｎ）、すなわちサブキーセット［ＩＤｅｎ，ＬＫｅｎ］とをホスト装置に格納するインプリント処理のみの実行要求スイッチとしての［Ｉｍｐｒｉｎｔ］スイッチ７３５を有する。
【０２３５】
なお、図２１には、ロック／アンロック専用機器のインジケータ構成と処理要求スイッチ構成例を示したが、先に説明したように、ホスト装置には、ＰＣ，ＰＤＡ等の情報処理装置、ＤＳＣ等のデジタルカメラ、携帯通信端末等の様々な装置が含まれ、これらの装置においては、それぞれの入力手段を介した情報記憶装置（メモリカード）に対するコマンド送出構成が可能である。また、ロック状態表示処理も、それぞれの機器においてＬＣＤ等のディスプレイに表示したり、あるいは、音声、アラーム等により通知する構成とすることが可能である。
【０２３６】
図２２以下を参照して、ホスト装置におけるロック状態提示処理、およびホスト装置から情報記憶装置（メモリカード）に対するコマンド送信処理について説明する。
【０２３７】
図２２は、例えば、ホスト装置に対して情報記憶装置（メモリカード）を接続したときに実行されるロック状態読み出し処理を説明するフローである。ロック状態読み出し処理は、ユーザによるコマンド入力によって実行する構成としてもよいが、ホスト装置に対して情報記憶装置（メモリカード）を接続したときに自動実行する構成としてもよい。
【０２３８】
ステップＳ９０１において、ロック状態が情報記憶装置から読み出される。この状態情報は、先に説明した情報記憶装置の制御部２１０（図３参照）のＲＡＭ２１３に格納されたロックステータスフラグに基づく。ステップＳ９０２において、このロック状態読み出し情報に基づいて、ロック状態に対応するインジケータ７２１～７２４が点灯する。すなわ

ち、スタンダードロック、グループロックが実行されている場合は、ロック状態を示す［Ｌｏｃｋｅｄ］インジーケータ７２２が表示（点灯）され、エクスポートロックが実行されている場合は、エクスポートロック状態を示す［Ｅ－Ｌｏｃｋｅｄ］インジーケータ７２３が表示（点灯）され、ロック状態にない場合は、ロック解除状態を示す［Ｕｎｌｏｃｋｅｄ］インジーケータ７２１が表示（点灯）される。

【０２３９】

次に、図２３を参照して、ロック処理要求、実行に基づくインジケータ表示処理について説明する。ロック処理は、図２１の、処理要求スイッチ７３２～７３４のスイッチによる入力に基づいて実行される。

【０２４０】

プライマリＩＤ（ＩＤｓ）と、プライマリロックキー（ＬＫｓ）のプライマリキーセット［ＩＤｓ，ＬＫｓ］を適用したスタンダードロック処理要求の場合は、［Ｓ－Ｌｏｃｋ］スイッチ７３２による入力、サブＩＤ（ＩＤｅｎ）と、サブロックキー（ＬＫｅｎ）のサブキーセット［ＩＤｅｎ，ＬＫｅｎ］を適用したエクスポートロック処理要求の場合は、Ｅ－Ｌｏｃｋ］スイッチ７３４による入力、サブキーセット［ＩＤｅｎ，ＬＫｅｎ］を適用したスタンダードロック、すなわちグループロック処理要求の場合は、［Ｇ－Ｌｏｃｋ］スイッチ７３３による入力を実行する。。

【０２４１】

これらのいずれかの入力を受けると、ステップＳ９１１において、情報記憶装置（メモリカード）のロック状態を検出し、アンロック状態でない場合は、ステップＳ９１４において、エラー（ＥＲＲ）インジケータ表示を行なう。アンロック状態である場合は、ステップＳ９１２において、スタンダードロック処理、またはエクスポートロック処理、またはグループロック処理のいずれかを実行し、ロック処理完了の後、ホスト装置の対応ロックインジケータ、すなわち、ロック状態を示す［Ｌｏｃｋｅｄ］インジーケータ７２２、またはエクスポートロック状態を示す［Ｅ－Ｌｏｃｋｅｄ］インジーケータ７２３の表示を実行する。

【０２４２】

次に、図２４を参照して、アンロック処理時におけるホスト装置の操作、インジケータ表示について説明する。

【０２４３】

アンロック処理は、図２１におけるアンロック要求スイッチ７３１の押下により実行される。アンロック要求スイッチの押下により、まず、情報記憶装置のロック状態検出が実行される。状態検出は、先に説明した制御部内のＲＡＭのロックステータスフラグに基づいて実行される。ロック状態にない場合（ステップＳ９２１：Ｎｏ）は、ステップＳ９２３においてエラー（ＥＲＲ）インジケータ７２４の表示を実行する。

【０２４４】

また、ステップＳ９２２のロック状態読み出しにおいて、情報記憶装置がエクスポートロック状態にあるかスタンダードロック状態にあるかが判定される。先に説明したロックステータスフラグに基づいてエクスポートロック状態にあるかスタンダードロック状態にあるかを識別する。識別結果に基づいて、図２１に示すロック状態に対応するインジケータ７２１～７２４が点灯する。

【０２４５】

まず、エクスポートロックである場合（ステップＳ９２４：Ｙｅｓ）は、先に図１６乃至図１８を参照して説明したインプリントおよびアンロック処理を実行する。すなわちステップＳ９２５に示すプライマリＩＤ（ＩＤｓ）とプライマリロックキー（ＬＫｓ）によるオーバーロック処理、ステップＳ９２６のサブＩＤ（ＩＤｅｎ）と、サブロックキー（ＬＫｅｎ）のインプリント（入力格納）処理、さらに、ステップＳ９２７におけるサブＩＤ（ＩＤｅｎ）と、サブロックキー（ＬＫｅｎ）を適用したロック解除処理である。この処理の詳細は、先に図１６乃至図１８を参照して説明した通りである。これらの処理により、ロックが解除されると、ステップＳ９２８において、ロック解除インジケータ７２１が

表示される。

【０２４６】

ステップＳ９２４において、エクスポートロック以外のロック状態、すなわちスタンダードロック状態である場合は、ステップＳ９２９において、スタンダードロックがなされているか否かが判定され、スタンダードロックありの場合は、ステップＳ９３０において、アンロック処理を実行する。このアンロック処理に適用するキーセットは、プライマリーキーセット［ＩＤｓ，ＬＫｓ］、あるいはグループロックである場合は、サブキーセット［ＩＤｅｎ，ＬＫｅｎ］である。この処理により、ロックが解除されると、ステップＳ９２８において、ロック解除インジケータ７２１が表示される。

【０２４７】

ステップＳ９２４において、エクスポートロック以外のロック状態であり、ステップＳ９２９において、スタンダードロックでないと判定されると、ステップＳ９３１に進み、エラー（ＥＲＲ）インジケータ７２４が表示される。

【０２４８】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０２４９】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【０２５０】

例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ　Ｄｉｓｃ　Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ），ＭＯ（Ｍａｇｎｅｔｏ　ｏｐｔｉｃａｌ）ディスク，ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

【０２５１】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【０２５２】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【０２５３】

【発明の効果】

以上説明してきたように、本発明の構成によれば、メモリカード等の情報記憶装置において、ＰＣ等の情報処理装置からメモリのロック処理要求コマンド、またはロック解除要求であるアンロック処理要求コマンドを入力し、入力コマンドに応じた処理を実行する際に、コマンドを出力した情報処理装置に対応して設定された識別子（ＩＤ）に基づいて、情

報処理装置が、該識別子（ＩＤ）を含む正当なキーセットを有しているか否かの検証処理を実行し、該検証の成立を条件として、前記コマンドに基づく処理を実行する構成としたので、セキュアな管理下でのメモリアクセス制御が実現される。

【０２５４】

さらに、本発明の構成によれば、情報処理装置に固有ＩＤ（ＩＤ）と、該固有ＩＤに対応するロックキー（ＬＫ）からなるキーセット［ＩＤ，ＬＫ］を格納し、一方、情報記憶装置は、ＬＫ＝Ｈ（ＬＭＫ，ＩＤ）の関係、すなわち、ＩＤに対するロックマスターキー（ＬＭＫ）を適用したハッシュ値としてロックキー（ＬＫ）の算出が可能なロックマスターキー（ＬＭＫ）を格納し、情報処理装置から入力する情報処理装置固有のキーセットの検証を前記ロックマスターキー（ＬＭＫ）を適用したハッシュ値算出により取得したロックキー（ＬＫ）に基づいて実行する構成としたので、複数の異なるロックキー（ＬＫ）に対する検証を１つのロックマスターキー（ＬＭＫ）に基づいて実行することが可能となる。

【０２５５】

さらに、本発明の構成によれば、情報処理装置の検証において、情報記憶装置側で乱数発生処理を実行し、情報処理装置の所有するロックキー（ＬＫ）に基づく乱数（Ｒｍｓ）の暗号化データ［Ｅ（Ｌｋ，Ｒｍｓ）］を該情報処理装置から受信し、該受信暗号化データと、ハッシュ値算出による取得したロックキー（ＬＫ）に基づいて算出した暗号化データ［Ｅ（Ｌｋ，Ｒｍｓ）］との照合を実行する構成としたので、照合毎に異なる乱数を適用した検証が可能となり、過去の照合履歴データを利用した不正アクセスが排除可能となる。

【図面の簡単な説明】

【図１】本発明の情報記憶装置の利用形態の概要について説明する図である。

【図２】情報記憶装置を利用するホスト装置のハード構成例を示す図である。

【図３】情報記憶装置のハード構成例を示す図である。

【図４】本発明の情報記憶装置、およびホスト装置の格納データについて説明する図である。

【図５】情報記憶装置に対するロック処理における情報記憶装置とホスト装置間の通信処理シーケンスについて説明する図である。

【図６】情報記憶装置に対するロック処理を説明する処理フローを示す図である。

【図７】情報記憶装置に対するアンロック処理における情報記憶装置とホスト装置間の通信処理シーケンスについて説明する図である。

【図８】情報記憶装置に対するアンロック処理を説明する処理フローを示す図である。

【図９】本発明の情報記憶装置、およびホスト装置の格納データについて説明する図である。

【図１０】本発明の情報記憶装置に対するロック処理態様について説明する図である。

【図１１】情報記憶装置に対するサブキーセットを適用したロック処理における情報記憶装置とホスト装置間の通信処理シーケンスについて説明する図である。

【図１２】情報記憶装置に対するサブキーセットを適用したロック処理を説明する処理フローを示す図である。

【図１３】情報記憶装置に対するインプリントおよびサブキーセットを適用したアンロック処理における情報記憶装置とホスト装置間の通信処理シーケンスについて説明する図である。

【図１４】情報記憶装置に対するインプリントおよびサブキーセットを適用したアンロック処理について説明するフロー図である。

【図１５】情報記憶装置に対するインプリントおよびサブキーセットを適用したアンロック処理について説明するフロー図である。

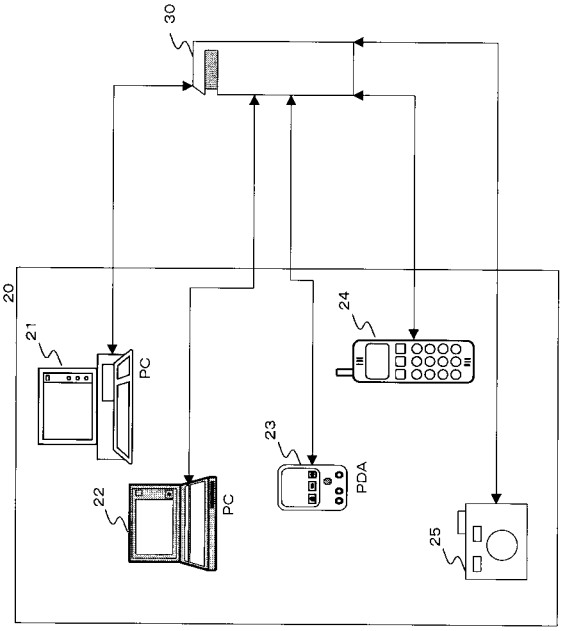
【図１６】情報記憶装置に対するインプリントおよびサブキーセットを適用したアンロック処理における情報記憶装置とホスト装置間の通信処理シーケンスについて説明する図である。

【図１７】情報記憶装置に対するインプリントおよびサブキーセットを適用したアンロッ

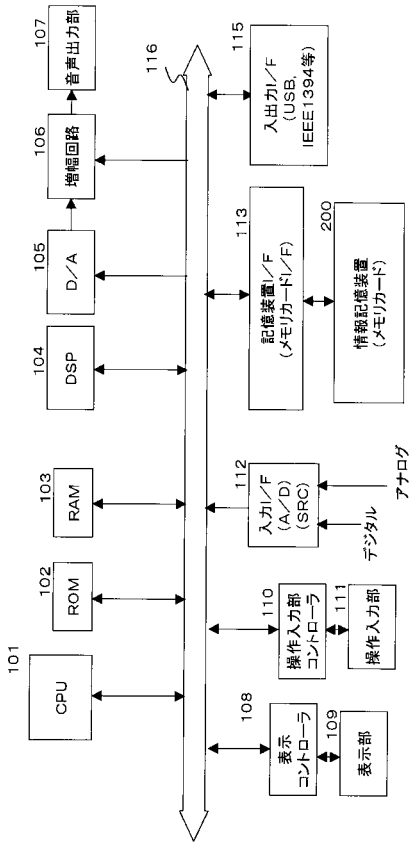
ク処理におけるロックステータスフラグの更新処理について説明するフロー図である。
【図１８】情報記憶装置に対するアンロック処理におけるロックステータスフラグ参照処理について説明するフロー図である。
【図１９】情報記憶装置に対するデータ格納態様としてのクラスタ構成について説明する図である。
【図２０】特定データ領域（クラスタ）読み出しに基づくロック処理について説明するフロー図である。
【図２１】情報記憶装置に対するロック／アンロック実行機器の構成について説明する図である。
【図２２】ホスト装置におけるロック状態読み出し処理フロー図である。
【図２３】ホスト装置におけるロック処理時における処理、およびインジケータ表示処理を説明するフロー図である。
【図２４】ホスト装置におけるアンロック処理時における処理、およびインジケータ表示処理を説明するフロー図である。
【符号の説明】
２０　ホスト装置
２１，２２　ＰＣ
２３　ＰＤＡ
２４　携帯通信端末
２５　デジタルカメラ
３０　情報記憶装置（メモリカード）
１０１　ＣＰＵ（Ｃｅｎｔｒａｌ　ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）
１０２　ＲＯＭ（Ｒｅａｄ－Ｏｎｌｙ－Ｍｅｍｏｒｙ）
１０３　ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）
１０４　ＤＳＰ
１０５　Ｄ／Ａ変換器
１０６　増幅回路
１０７　音声出力部
１０８　表示コントローラ
１０９　表示部
１１０　操作入力コントローラ
１１１　操作入力部
１１２　入力Ｉ／Ｆ
１１３　記憶装置Ｉ／Ｆ
１１４　情報記憶装置
１１５　入出力Ｉ／Ｆ
１１６　バス
２００　情報記憶装置
２１０　制御部
２１１　ＣＰＵ（Ｃｅｎｔｒａｌ　ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）
２１２　ＲＯＭ（Ｒｅａｄ－Ｏｎｌｙ－Ｍｅｍｏｒｙ）
２１３　ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）
２１４　機器インタフェース
２１５　メモリインタフェース
２２０　メモリ部
３１０　ホスト装置
３１２　ロック・アンロック機器
３１５　メモリ
３２０　情報記憶装置
３２５　メモリ

５１０　ホスト装置
５１２　ロック・アンロック機器
５１５　メモリ
５２０　情報記憶装置
５２５　メモリ
５３１　プライマリキーセット
５３２　サブキーセット
５４１　スタンダードロックキーセット格納領域
５４２　エクスポートロックキーセット格納領域
５５１　ロックステータスフラグ
７１０　情報記憶装置
７２０　ホスト装置
７２１～７２４　インジケータ
７３１～７３５　スイッチ

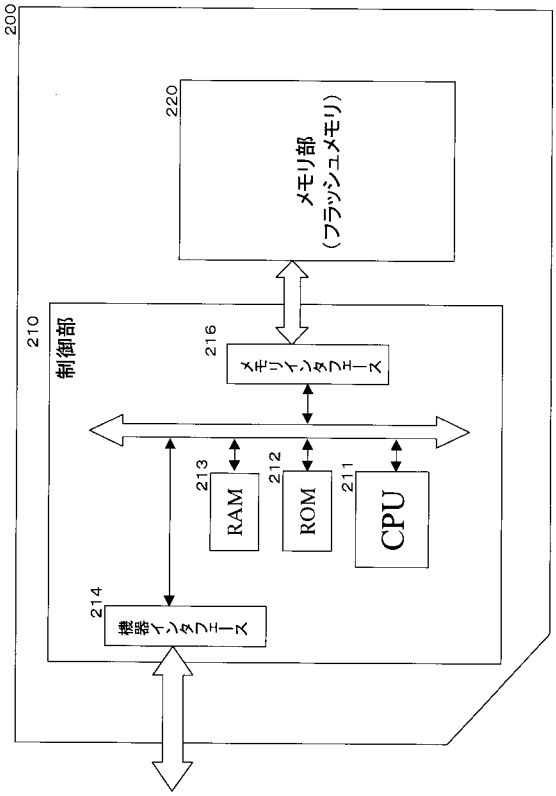
【図１】



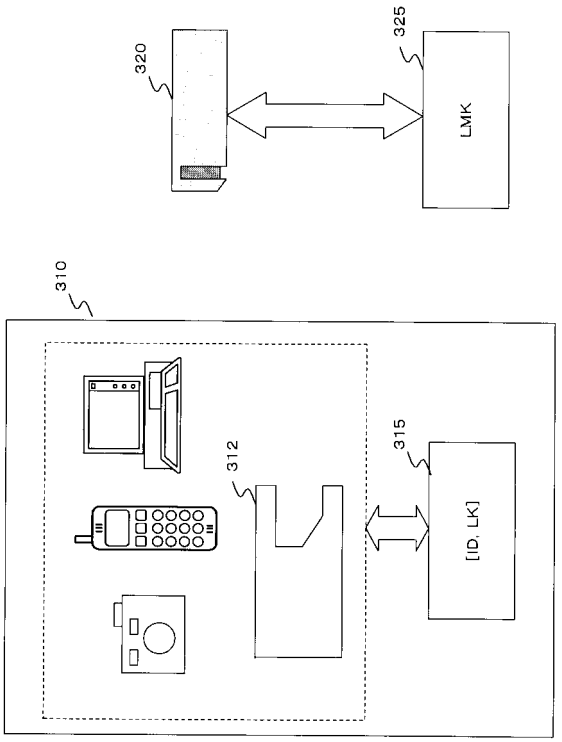
【図２】



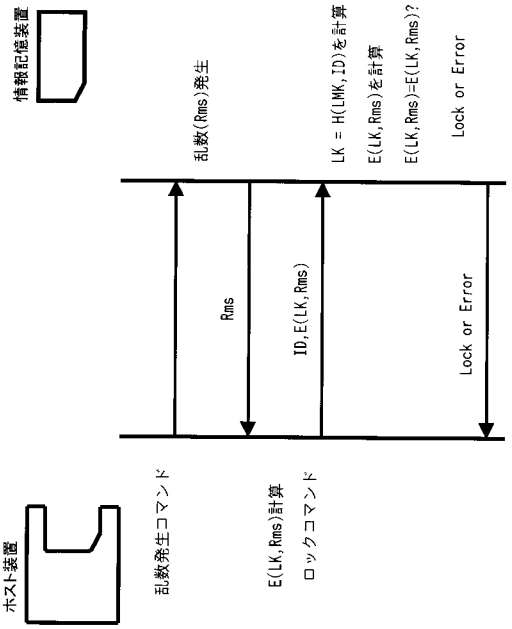
【図３】


200
220
メモリ部
(フラッシュメモリ)
210
制御部
216
メモリインタフェース
213
RAM
212
ROM
211
CPU
214
機器インタフェース

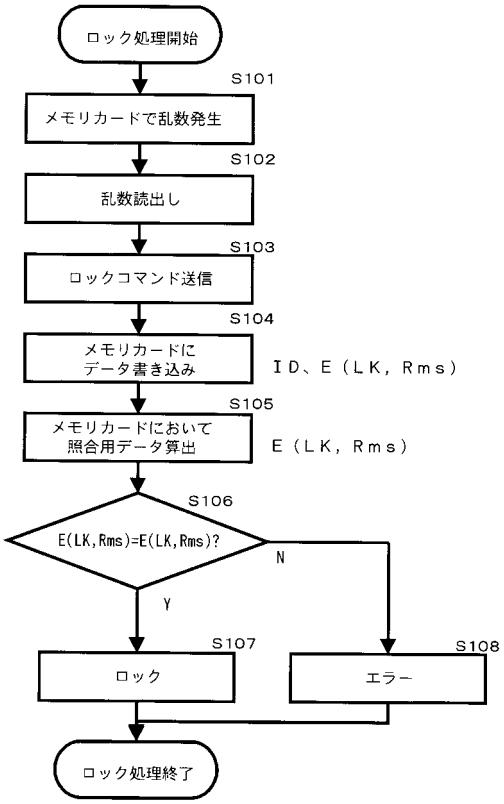
【図４】


320
325
LMK
310
312
315
[ID, LK]

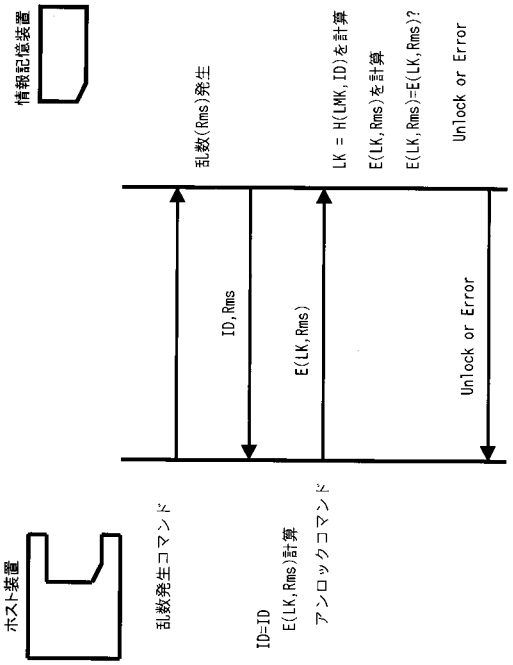
【図５】


情報記憶装置
乱数(Rms)発生
LK = H(LMK, ID)を計算
E(LK,Rms)を計算
E(LK,Rms)=E(LK,Rms)?
Lock or Error
Rms
ID,E(LK,Rms)
Lock or Error
ホスト装置
乱数発生コマンド
E(LK,Rms)計算
ロックコマンド

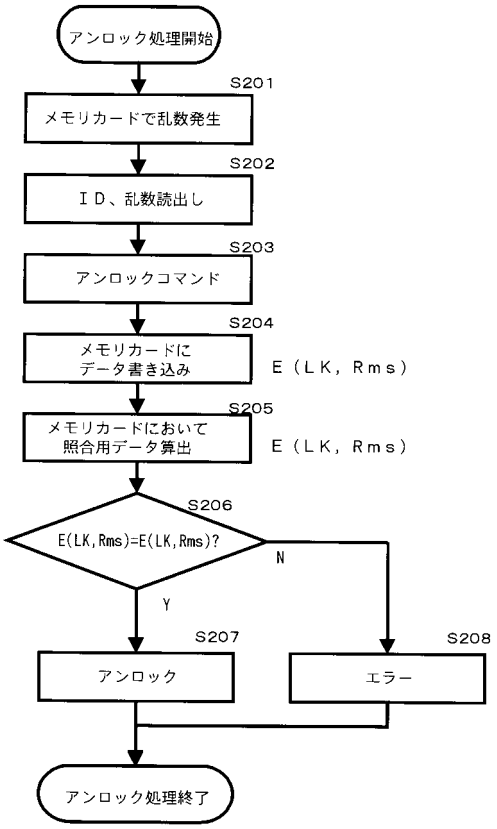
【図６】


ロック処理開始
S101
メモリカードで乱数発生
S102
乱数読出し
S103
ロックコマンド送信
S104
メモリカードに
データ書き込み
ID、E(LK, Rms)
S105
メモリカードにおいて
照合用データ算出
E(LK, Rms)
S106
E(LK,Rms)=E(LK,Rms)?
N
Y
S107
ロック
S108
エラー
ロック処理終了

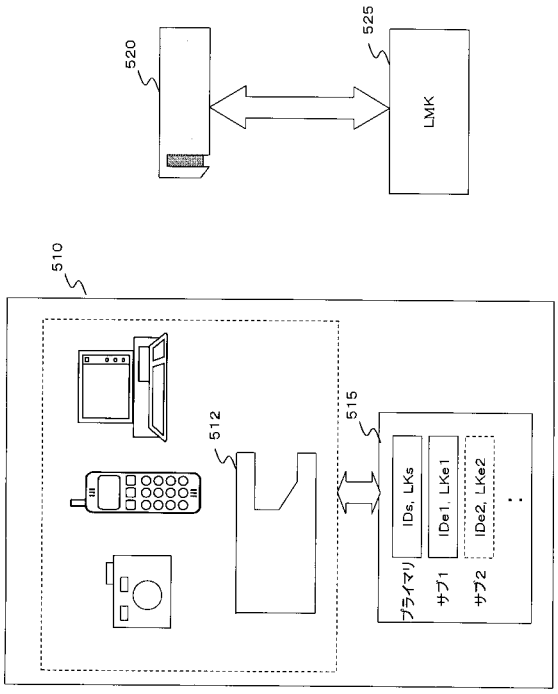
【図７】


情報記憶装置
乱数(Rms)発生
LK = H(LMK, ID)を計算
E(LK, Rms)を計算
E(LK, Rms)=E(LK, Rms)?
Unlock or Error
ID, Rms
E(LK, Rms)
Unlock or Error
ホスト装置
乱数発生コマンド
ID=ID
E(LK, Rms)計算
アンロックコマンド

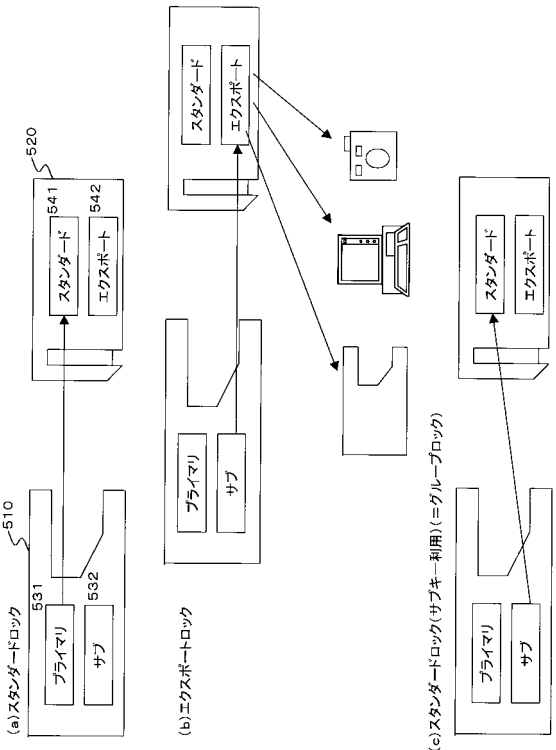
【図８】


アンロック処理開始
S201
メモリカードで乱数発生
S202
ＩＤ、乱数読出し
S203
アンロックコマンド
S204
メモリカードにデータ書き込み
E（LK, Rms）
S205
メモリカードにおいて照合用データ算出
E（LK, Rms）
S206
E(LK, Rms)=E(LK, Rms)?
N
Y
S207
アンロック
S208
エラー
アンロック処理終了

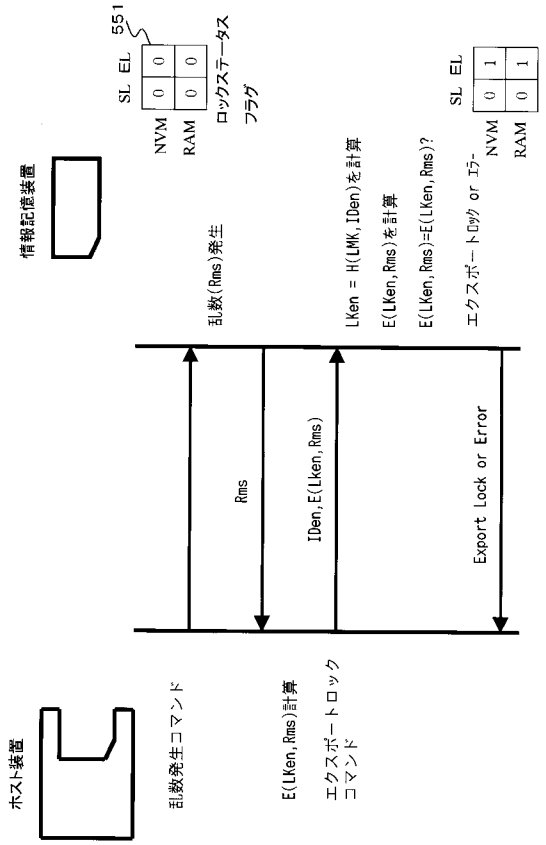
【図９】


520
525
LMK
510
512
515
IDs, LKs
IDe1, LKe1
IDe2, LKe2
プライマリ
サブ1
サブ2

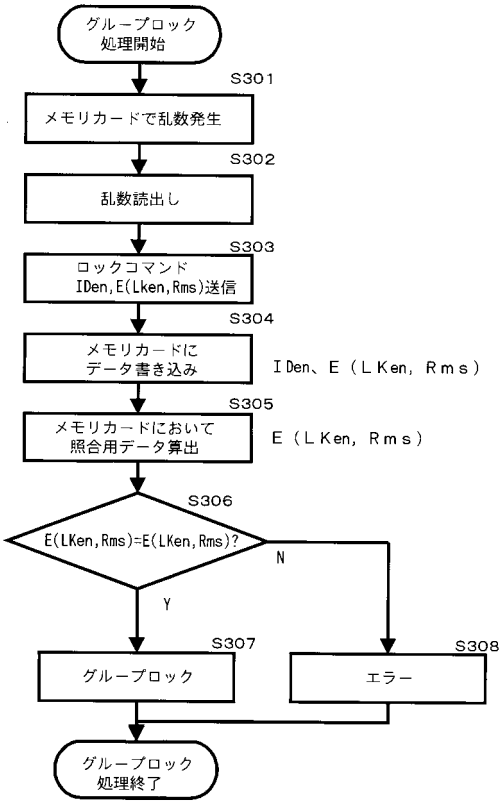
【図１０】


520
541
542
スタンダード
エクスポート
510
531
532
プライマリ
サブ
(a)スタンダードロック
(b)エクスポートロック
(c)スタンダードロック(サブキー利用)(=グループロック)

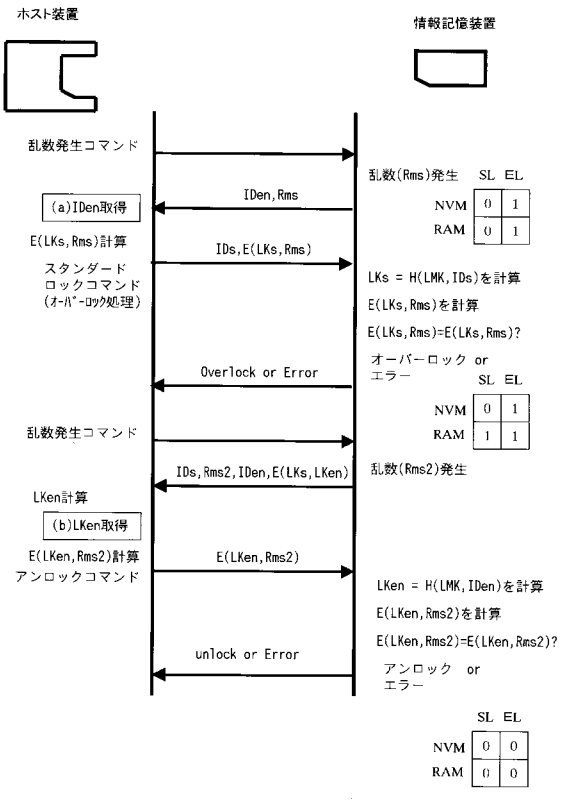
【図１１】



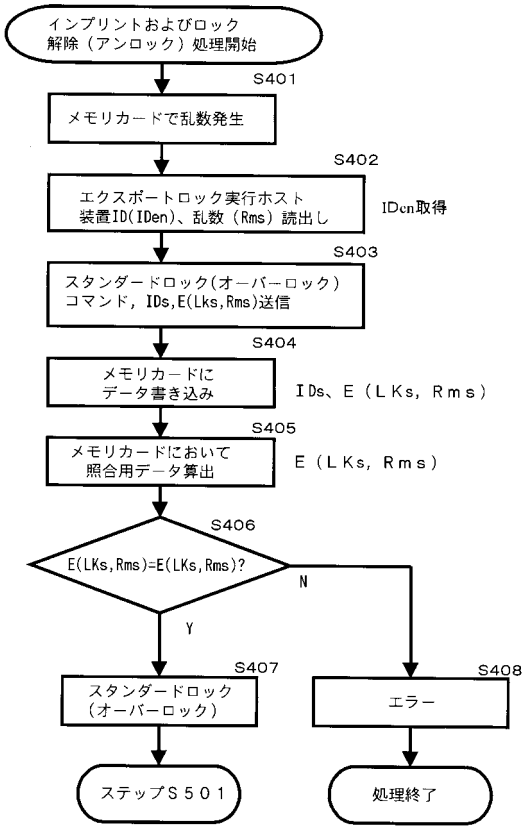
【図１２】



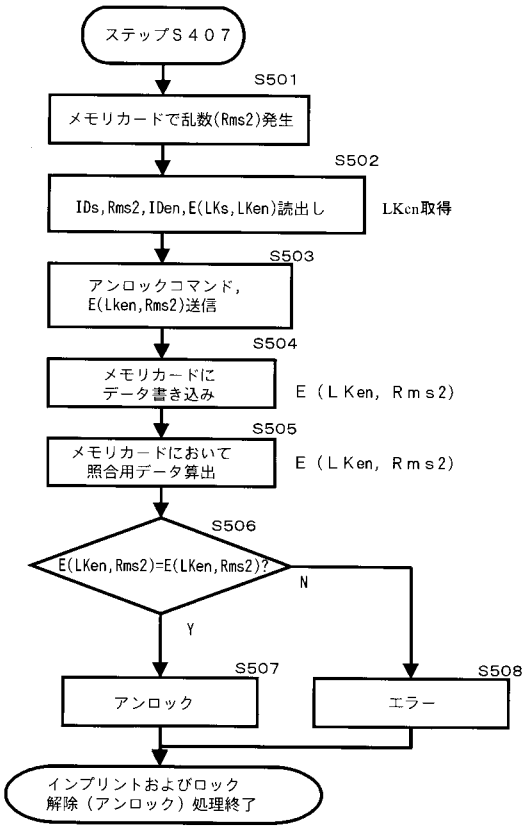
【図１３】



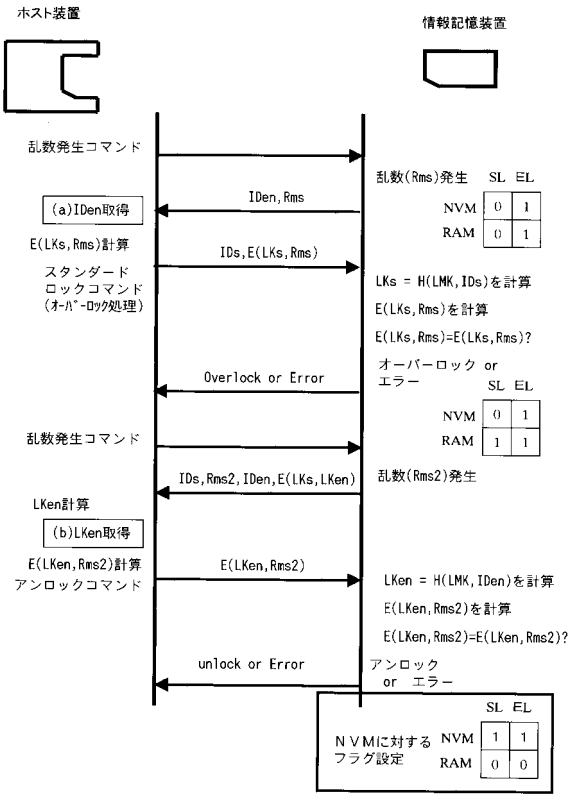
【図１４】



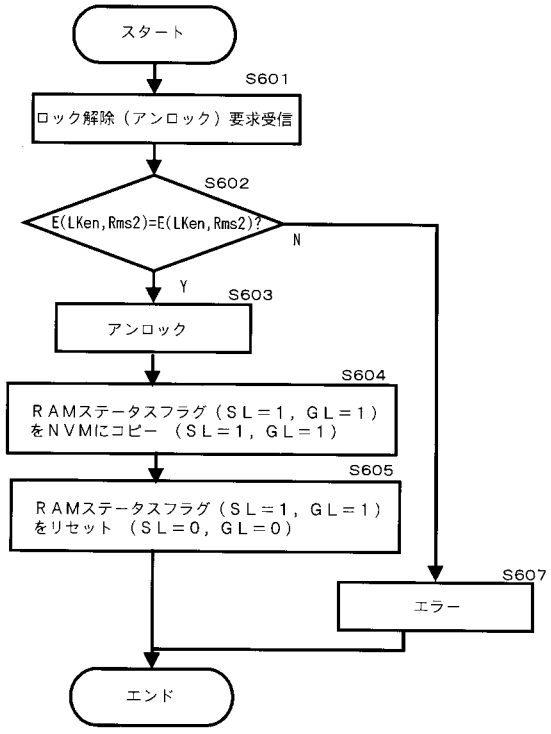
【図１５】



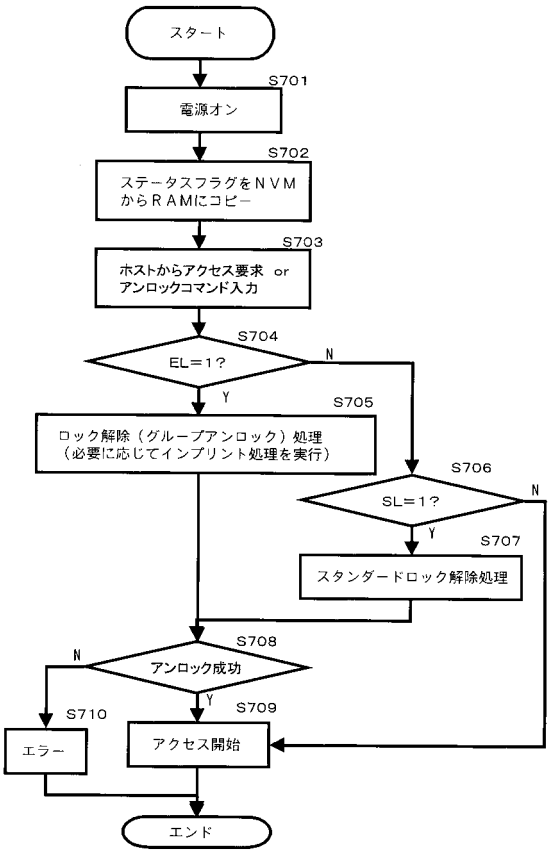
【図１６】



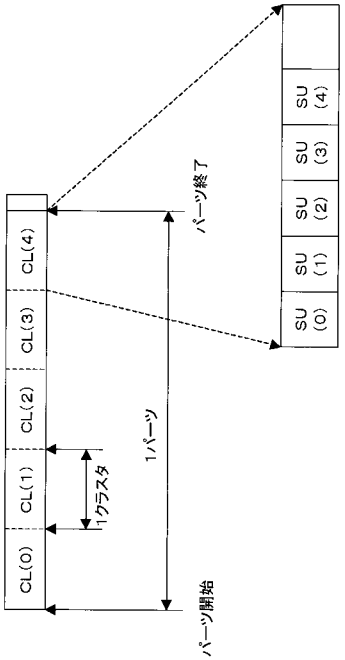
【図１７】



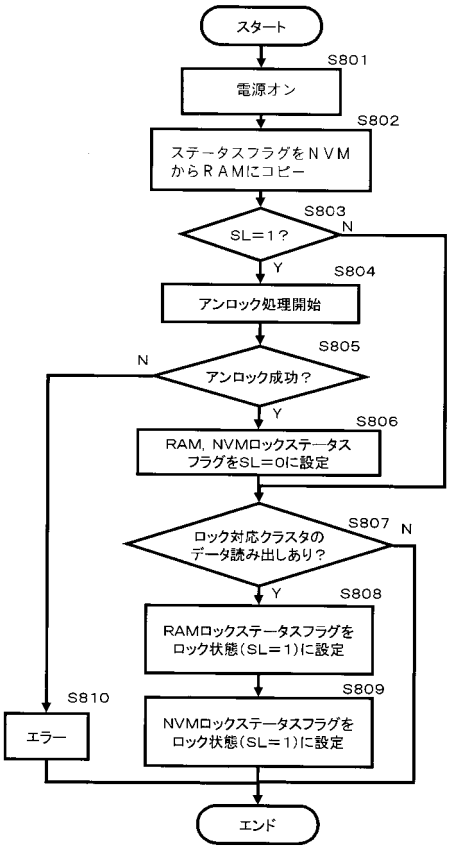
【図１８】



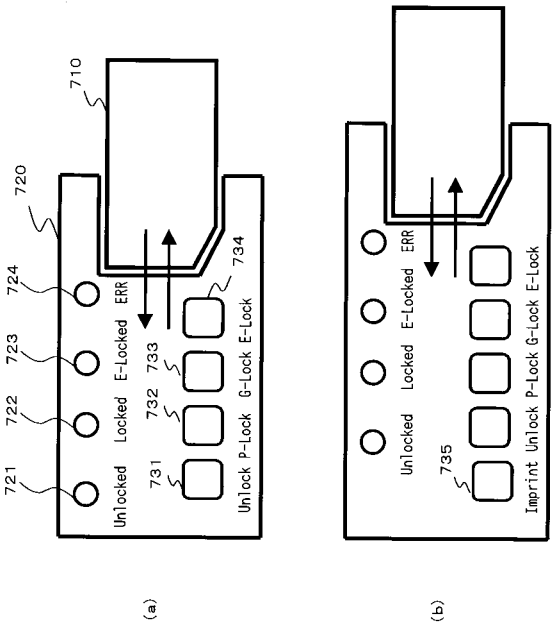
【図１９】



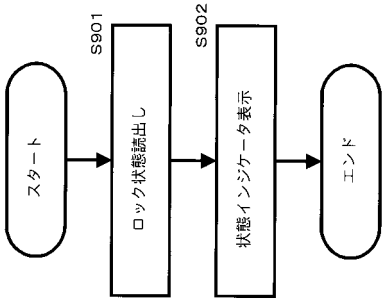
【図２０】



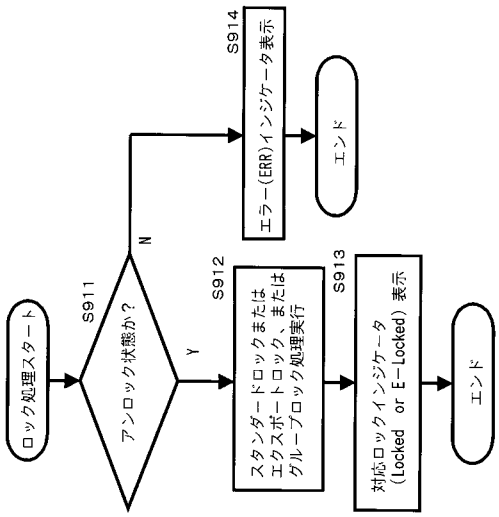
【図２１】



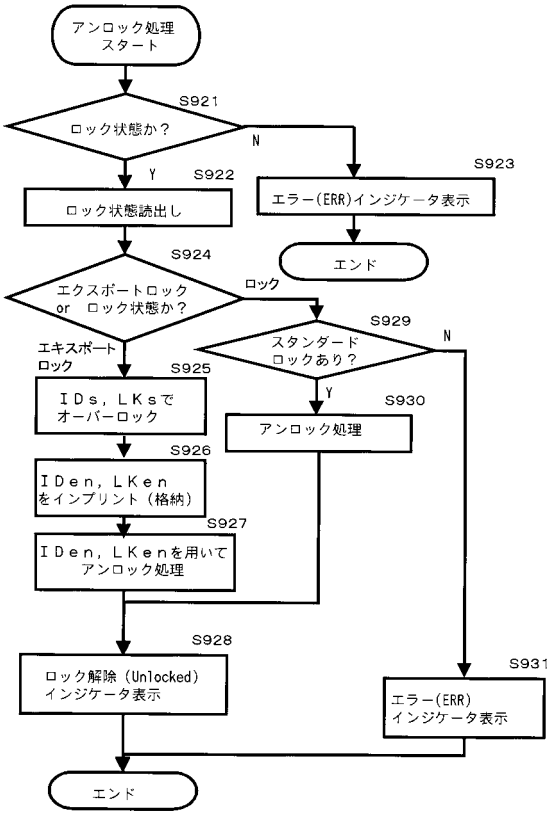
【図２２】



【図２３】


ロック処理スタート
S911
アンロック状態か？
N
Y
S912
スタンダードロックまたは
エクスポートロック、または
グループロック処理実行
S913
対応ロックインジケータ
(Locked or E-Locked) 表示
エンド
S914
エラー(ERR)インジケータ表示
エンド

【図２４】


アンロック処理
スタート
S921
ロック状態か？
N
Y
S922
ロック状態読出し
S923
エラー(ERR)インジケータ表示
エンド
S924
エクスポートロック
or ロック状態か？
ロック
S929
スタンダード
ロックあり？
N
Y
エキスポート
ロック
S925
IDs, LKsで
オーバーロック
S930
アンロック処理
S926
IDen, LKen
をインプリント（格納）
S927
IDen, LKenを用いて
アンロック処理
S928
ロック解除（Unlocked）
インジケータ表示
S931
エラー(ERR)
インジケータ表示
エンド

フロントページの続き

(72)発明者　田代　淳
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　大久保　英明
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

Ｆターム(参考) 5B017 AA06 BB09 BB10 CA14
5B058 CA26 CA27 KA08 KA31
5B065 BA09 CA02 CA15 CC08 PA01 PA14