(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2009-543208
(P2009-543208A)
(43)公表日　平成21年12月3日(2009.12.3)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330A	5B285
H04L 9/32	(2006.01)	G06F	15/00	330G	5J104
		H04L	9/00	675B	
		H04L	9/00	673Z	

審査請求 未請求　予備審査請求 未請求　（全 76 頁）

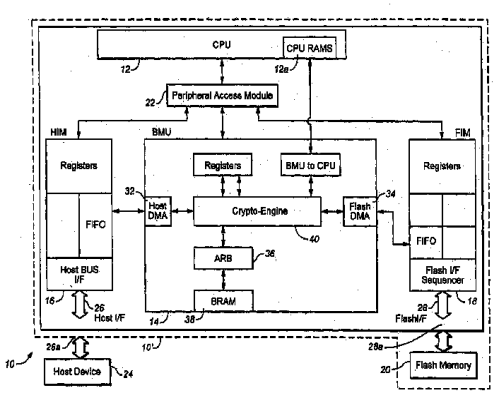
(21)出願番号　特願2009-518324 (P2009-518324)
(86)(22)出願日　平成19年6月28日 (2007.6.28)
(85)翻訳文提出日　平成21年3月4日 (2009.3.4)
(86)国際出願番号　PCT/US2007/015304
(87)国際公開番号　WO2008/013656
(87)国際公開日　平成20年1月31日 (2008.1.31)
(31)優先権主張番号　60/819,507
(32)優先日　平成18年7月7日 (2006.7.7)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　11/557,028
(32)優先日　平成18年11月6日 (2006.11.6)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　11/557,010
(32)優先日　平成18年11月6日 (2006.11.6)
(33)優先権主張国　米国 (US)

(71)出願人　506197901
サンディスク　コーポレイション
アメリカ合衆国、９５０３５、カリフォルニア州、ミルピタス、マッカシー　ブルバード　６０１
(74)代理人　100075144
弁理士　井ノ口　壽
(72)発明者　ホルツマン，マイケル
アメリカ合衆国、９５０１４、カリフォルニア州、クペルティーノ、バーンハート　プレイス　７６０２
(72)発明者　バージライ，ロン
イスラエル国、２５１４７、クファール－ブラディム、メロン　ストリート　６７

最終頁に続く

(54)【発明の名称】証明書連鎖を使用するコンテンツ管理システムおよび方法

(57)【要約】
証明書連鎖の中の連続する証明書文字列は、それらの文字列がベリファイされるのと同じ順序で、メモリ装置によって順次受信される。最後の文字列を除く各文字列は、順序の中の次の文字列で上書きできる。



【特許請求の範囲】
【請求項１】
第１の事業体を第２の事業体によって認証する方法であって、
第２の事業体に対して第１の事業体を認証するため、第２の事業体にて証明書連鎖を受信するステップであって、前記証明書連鎖は複数の連続する証明書文字列を含み、前記文字列はそれぞれ少なくとも１つの証明書を含む、ステップと、
前記第２の事業体が、前記証明書連鎖内の証明書文字列をある１つの順序でベリファイするステップであって、連鎖内の前記証明書文字列は第２の事業体にて前記順序で受信される、ステップと、
第２の事業体にて完全な証明書連鎖が受信されたか否かを検出するステップと、
を含む方法。
【請求項２】
請求項１記載の方法において、
前記検出するステップは、第２の事業体によって受信される証明書のうちの少なくとも１つの証明書が証明書連鎖における最後の証明書か否かを検出する方法。
【請求項３】
請求項２記載の方法において、
受信した証明書をベリファイするステップをさらに含む方法。
【請求項４】
請求項２記載の方法において、
連鎖の中の最後の証明書は、これが証明書連鎖における最後の証明書であることの指示を収容し、前記検出するステップは前記指示を検出する方法。
【請求項５】
請求項２記載の方法において、
第１の事業体はメモリ装置を備え、第２の事業体はホスト装置を備え、前記メモリ装置は取り外し可能な状態で前記ホスト装置へ接続する方法。
【請求項６】
請求項５記載の方法において、
連鎖における最後の証明書の受信後を除く各証明書文字列の受信後に、第２の事業体が、順序の中の次の証明書文字列を求める要求を第１の事業体へ送信するステップをさらに含む方法。
【請求項７】
請求項６記載の方法において、
第２の事業体からの各要求に応じて、第１の事業体が、証明書文字列のうちのいずれか１つを第２の事業体へ送信するステップをさらに含む方法。
【請求項８】
請求項１記載の方法において、
第２の事業体はメモリ装置を備え、第１の事業体はホスト装置を備え、前記メモリ装置は取り外し可能な状態で前記ホスト装置へ接続する方法。
【請求項９】
請求項１記載の方法において、
第２の事業体は、メモリカードを備える方法。
【請求項１０】
請求項１記載の方法において、
第２の事業体に対して第１の事業体を認証するため、前記証明書文字列を前記順序に従い第２の事業体へ連続的に送信するステップをさらに含む方法。
【請求項１１】
請求項１記載の方法において、
証明書文字列の各々は１つの証明書を含み、前記第２の事業体はメモリ装置を備え、前記方法は、第２の事業体で受信した証明書をメモリ装置に蓄積するステップをさらに含み

、メモリに蓄積される連鎖内の最後の証明書を除く各証明書は、第２の事業体で受信される次の証明書によって上書きされる方法。
【請求項１２】
請求項１１記載の方法において、
メモリ装置で１つの証明書を蓄積するにあたって十分なメモリ空間より多くは割り当てないステップをさらに含む方法。
【請求項１３】
第１の事業体を第２の事業体によって認証する方法であって、
第２の事業体に対して第１の事業体を認証するため、第２の事業体へ証明書連鎖を送信するステップであって、前記証明書連鎖は複数の連続する証明書文字列を含み、前記文字列はそれぞれ少なくとも１つの証明書を含む、ステップと、
前記第２の事業体が、前記証明書連鎖内の証明書文字列をある１つの順序で連続的にベリファイするステップであって、連鎖内の証明書文字列は前記順序で送信される、ステップと、
を含む方法。
【請求項１４】
請求項１３記載の方法において、
前記第２の事業体はベリファイプロセスの中で第２の事業体へ送信される証明書をベリファイし、第２の事業体へ送信される証明書のうちの少なくとも１つの証明書がベリファイプロセスに失敗する場合、前記方法は、ベリファイプロセスを終了するステップと、終了の指示を第１の事業体へ送信するステップとをさらに含む方法。
【請求項１５】
請求項１４記載の方法において、
第１の事業体にて指示を受信し、かつ前記指示を受信する場合に送信することを停止するステップをさらに含む方法。
【請求項１６】
請求項１３記載の方法において、
第２の事業体へ送信される連鎖の中の最後の証明書は、これが証明書連鎖における最後の証明書であることの指示を収容する方法。
【請求項１７】
請求項１３記載の方法において、
第１の事業体はメモリ装置を備え、第２の事業体はホスト装置を備え、前記メモリ装置は取り外し可能な状態で前記ホスト装置へ接続する方法。
【請求項１８】
請求項１７記載の方法において、
連鎖における最後の証明書文字列の受信後を除く各証明書文字列の受信後に、第２の事業体が、順序の中の次の証明書文字列を求める要求を第１の事業体へ送信するステップをさらに含む方法。
【請求項１９】
請求項１８記載の方法において、
第２の事業体からの各要求に応じて、第１の事業体が、証明書文字列のうちのいずれか１つを第２の事業体へ送信するステップをさらに含む方法。
【請求項２０】
請求項１３記載の方法において、
第２の事業体はメモリ装置を備え、第１の事業体はホスト装置を備え、前記メモリ装置は取り外し可能な状態で前記ホスト装置へ接続する方法。
【請求項２１】
請求項１３記載の方法において、
各証明書文字列は１つの証明書を含み、前記第２の事業体はベリファイプロセスの中で受信する証明書をベリファイし、前記送信するステップは、第２の事業体に対して第１の

事業体を認証するため、第２の事業体へ送信される証明書のうちの少なくとも１つの証明書がベリファイプロセスに失敗する場合を除き、連鎖内の全ての証明書が送信されるまで、証明書連鎖を第２の事業体へ順次送信する方法。

【請求項２２】

請求項１３記載の方法において、

第２の事業体は、メモリカードを備える方法。

【請求項２３】

請求項１３記載の方法において、

証明書文字列の各々は１つの証明書を含み、前記第２の事業体はメモリを含み、第２の事業体で受信した証明書をメモリに蓄積するステップをさらに含み、メモリに蓄積される連鎖内の最後の証明書を除く各証明書は、第２の事業体で受信される次の証明書によって上書きされる方法。

【請求項２４】

請求項２３記載の方法において、

メモリ装置で１つの証明書を蓄積するにあたって十分なメモリ空間より多くは前記証明書の蓄積のために割り当てないステップをさらに含む方法。

【請求項２５】

第１および第２の事業体間での相互認証の方法であって、

（ａ）第２の事業体に対して第１の事業体を認証するため、第２の事業体にて第１の証明書連鎖を受信するステップであって、前記第１の証明書連鎖は複数の連続する証明書文字列を含み、前記第１の連鎖の中の文字列はそれぞれ少なくとも１つの証明書を含み、前記第２の事業体は前記第１の証明書連鎖の中の証明書文字列を第１の順序で連続的にベリファイし、第１の連鎖の中の前記証明書文字列は第２の事業体にて前記第１の順序で連続的に受信される、ステップと、

（ｂ）第２の事業体にて第１の事業体から完全な第１の証明書連鎖が受信されたか否かを検出するステップと、

（ｃ）第１の事業体に対して第２の事業体を認証するため、第１の事業体にて第２の証明書連鎖を受信するステップであって、前記第２の証明書連鎖は複数の連続する証明書文字列を含み、前記第２の連鎖の中の各文字列は少なくとも１つの証明書を含み、前記第１の事業体は前記第２の証明書連鎖の中の証明書文字列を第２の順序で連続的にベリファイし、第２の連鎖の中の証明書文字列は第２の順序で連続的に受信される、ステップと、

（ｄ）第１の事業体にて第２の事業体から完全な第２の証明書連鎖が受信されたか否かを検出するステップと、

を含む方法。

【請求項２６】

請求項２５記載の方法において、

（ｂ）または（ｄ）で検出するステップは、受信する証明書のうちの少なくとも１つの証明書が第１または第２の証明書連鎖における最後の証明書か否かを検出する方法。

【請求項２７】

請求項２６記載の方法において、

ベリファイプロセスで（ａ）または（ｃ）の後に受信する証明書をベリファイするステップと、第１または第２の事業体へ送信される証明書のうちの少なくとも１つの証明書がベリファイプロセスに失敗する場合に前記プロセスを終了するステップとをさらに含む方法。

【請求項２８】

請求項２６記載の方法において、

第１または第２の連鎖の中の最後の証明書は、これがそのような証明書連鎖における最後の証明書であることの指示を収容する方法。

【請求項２９】

請求項２５記載の方法において、

第１の事業体はメモリ装置を備え、第２の事業体はホスト装置を備え、前記メモリ装置は取り外し可能な状態で前記ホスト装置へ接続する方法。
【請求項３０】
請求項２９記載の方法において、
第１および第２の事業体のいずれか一方が、第１または第２の連鎖における最後の証明書文字列の受信後を除く（ａ）または（ｃ）における各証明書文字列の受信後に、第１または第２の順序の中の次の証明書文字列を求める要求を他方の事業体へ送信するステップをさらに含む方法。
【請求項３１】
請求項３０記載の方法において、
第１および第２の事業体のいずれか一方が、他方の事業体からの各要求に応じて、証明書文字列のうちのいずれか１つを他方の事業体へ送信するステップをさらに含む方法。
【請求項３２】
請求項２５記載の方法において、
第２の事業体はメモリ装置を備え、第１の事業体はホスト装置を備え、前記メモリ装置は取り外し可能な状態で前記ホスト装置へ接続する方法。
【請求項３３】
請求項３２記載の方法において、
第２の事業体は、メモリカードを備える方法。
【請求項３４】
請求項３３記載の方法において、
第２の事業体に対して第１の事業体を認証するため、第１の証明書連鎖を第２の事業体へ順次送信するステップをさらに含む方法。
【請求項３５】
請求項２５記載の方法において、
第１または第２の事業体にて（ａ）または（ｃ）で順次受信する証明書文字列をメモリに蓄積するステップをさらに含み、メモリに蓄積される第１または第２の連鎖内の最後の証明書を除く各証明書文字列は、（ａ）または（ｃ）で順次受信する第１または第２の証明書順序の中の次の文字列によって上書きされる方法。
【請求項３６】
請求項３５記載の方法において、
メモリで証明書文字列のうちのいずれか１つを蓄積するにあたって十分なメモリ空間より多くは割り当てないステップをさらに含む方法。
【請求項３７】
第１の事業体にあるデータに第２の事業体によりアクセスするシステムにであって、前記システムは前記第２の事業体を備え、前記第２の事業体は、第２の事業体から第１の事業体へ順次送信されるように構成された連鎖内に証明書を備え、順次送信される連鎖の最後の証明書は、これが証明書連鎖における最後の証明書であることの指示を収容するシステム。
【請求項３８】
請求項３７記載のシステムにおいて、
第１の事業体にて受信した後の証明書を蓄積する記憶装置をさらに備え、前記記憶装置は、記憶装置に蓄積された各証明書を、第１の事業体で受信する連鎖内の最後の証明書を除く連鎖内の次の証明書で上書きするシステム。
【請求項３９】
請求項３８記載のシステムにおいて、
第１の事業体で受信する証明書を蓄積するため、１つの証明書を蓄積するにあたって十分なメモリ空間より多くは割り当てないシステム。
【請求項４０】
請求項３７記載のシステムにおいて、

第１の事業体にある前記データは暗号化され、前記第２の事業体は前記データを復号化するための鍵をさらに備え、前記証明書連鎖は鍵が本物であることを証明し、前記鍵には長さがあり、第２の事業体へ送信される連鎖の中の各証明書の長さは鍵の長さの約４倍を上回らないシステム。

【請求項４１】

請求項３７記載のシステムにおいて、

前記第１の事業体は不揮発性メモリ装置を備え、前記第２の事業体は前記メモリ装置へ取り外し可能な状態で接続されるホスト装置を備えるシステム。

【請求項４２】

ホスト装置へデータを供給するメモリシステムであって、

データを蓄積できる不揮発性メモリと、

前記ホスト装置がメモリシステムへ取り外し可能な状態で接続される場合、前記不揮発性メモリの中にあるデータへの前記ホスト装置によるアクセスを認証プロセスを通じて制御するコントローラと、を備え、

前記ホスト装置は、複数の証明書文字列を含む証明書連鎖をメモリシステムへ送信し、各文字列は少なくとも１つの証明書を含み、前記コントローラは証明書文字列をある１つの順序で連続的にベリファイし、前記文字列は前記順序で送信され、前記コントローラは、前記不揮発性メモリで各証明書文字列を蓄積させ、かつ前記不揮発性メモリに蓄積された少なくとも１つの証明書文字列を前記文字列の後にホスト装置から受信する証明書文字列で上書きさせるメモリシステム。

【請求項４３】

請求項４２記載のメモリシステムにおいて、

前記コントローラは、各証明書文字列を随時一度に蓄積するにあたって十分なメモリ空間より多くは割り当てないメモリシステム。

【請求項４４】

請求項４２記載のメモリシステムにおいて、

前記コントローラは、前記ホスト装置から受信する証明書のうちの少なくとも１つの証明書が証明書連鎖における最後の証明書か否かを検出するメモリシステム。

【請求項４５】

請求項４４記載のメモリシステムにおいて、

連鎖の中の最後の証明書は、これが証明書連鎖における最後の証明書であることの指示を収容し、前記コントローラは前記指示を検出するメモリシステム。

【請求項４６】

請求項４２記載のメモリシステムにおいて、

メモリシステムは、メモリカードを備えるメモリシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、一般的にはメモリシステムに関し、具体的には汎用コンテンツ制御機能を備えるメモリシステムに関する。

【背景技術】

【０００２】

関連出願の相互参照

本願は、２００６年７月７日に出願された米国仮特許出願第６０／８１９，５０７号（特許文献１）の利益を主張する。

【０００３】

本願は、２００５年１２月２０日に出願された米国特許出願第１１／３１３，８７０号（特許文献２）に関し、この出願は２００４年１２月２１に出願された米国仮特許出願第６０／６３８，８０４号（特許文献３）の利益を主張する。本願はさらに、２００５年１２月２０日に出願された米国特許出願第１１／３１４，４１１号（特許文献４）に関する

。本願はさらに、２００５年１２月２０日に出願された米国特許出願第１１／３１４，４１０号（特許文献５）に関する。本願はさらに、２００５年１２月２０日に出願された米国特許出願第１１／３１３，５３６号（特許文献６）に関する。本願はさらに、２００５年１２月２０日に出願された米国特許出願第１１／３１３，５３８号（特許文献７）に関する。本願はさらに、２００５年１２月２０日に出願された米国特許出願第１１／３１４，０５５号（特許文献８）に関する。本願はさらに、２００５年１２月２０日に出願された米国特許出願第１１／３１４，０５２号（特許文献９）に関する。本願はさらに、２００５年１２月２０日に出願された米国特許出願第１１／３１４，０５３号（特許文献１０）に関する。

【０００４】

本願は、２００６年１１月６日に出願されたHoltzmanらの「Content Control Method Using Certificate Chains 」という米国特許出願第１１／５５７，０２８号（特許文献１１）と、２００６年１１月６日に出願されたHoltzmanらの「Content Control System Using Certificate Chains 」という米国特許出願第１１／５５７，０１０号（特許文献１２）と、２００６年１１月６日に出願されたHoltzmanらの「Content Control Method Using Certificate Revocation Lists 」という米国特許出願第１１／５５７，００６号（特許文献１３）と、２００６年１１月６日に出願されたHoltzmanらの「Content Control System Using Certificate Revocation Lists 」という米国特許出願第１１／５５７，０２６号（特許文献４）と、２００６年１１月６日に出願されたHoltzmanらの「Content Control Method Using Versatile Control Structure」という米国特許出願第１１／５５７，０４９号（特許文献１５）と、２００６年１１月６日に出願されたHoltzmanらの「Content Control System Using Versatile Control Structure」という米国特許出願第１１／５５７，０５６号（特許文献１６）と、２００６年１１月６日に出願されたHoltzmanらの「Method for Controlling Information Supplied From Memory Device」という米国特許出願第１１／５５７，０５２号（特許文献１７）と、２００６年１１月６日に出願されたHoltzmanらの「System for Controlling Information Supplied From Memory Device」という米国特許出願第１１／５５７，０５１号（特許文献１８）と、２００６年１１月６日に出願されたHoltzmanらの「Control Method Using Identity Objects 」という米国特許出願第１１／５５７，０４１号（特許文献１９）と、２００６年１１月６日に出願されたHoltzmanらの「Control System Using Identity Objects 」という米国特許出願第１１／５５７，０３９号（特許文献２０）とに関する。

【０００５】

これらの特許出願は、あたかも本願にもれなく記載されているかのごとく、それぞれの全体が本願明細書において参照により援用されている。

【０００６】

フラッシュメモリカード等の記憶装置が、写真等のデジタルコンテンツを記憶する記憶媒体として好んで使われるようになっている。フラッシュメモリカードはタイプの異なるメディアコンテンツの配布に使われる場合がある。コンピュータ、デジタルカメラ、携帯電話機、個人用携帯情報端末（ＰＤＡ）、ＭＰ３プレーヤをはじめとするメディアプレーヤ等のホスト装置の多様化が進み、フラッシュメモリカードに記憶されたメディアコンテンツを再生できるようになっている。このため、フラッシュメモリカードやその他の可搬型記憶装置がデジタルコンテンツの配布手段として幅広く利用される可能性が大きい。

【０００７】

デジタルコンテンツの所有者と配布者にとって最大の関心事のひとつは、インターネット等のネットワークからのダウンロードまたは記憶装置上でのコンテンツの配布を通じて配布された後のコンテンツに対するアクセスを、権限を持つ当事者だけに許可することである。不正アクセスを防ぐ一方法では、コンテンツへのアクセスを当事者に許諾する前に当事者のアイデンティティを立証するシステムを使用する。公開鍵基盤（ＰＫＩ）等はこの目的のために開発されたシステムである。ＰＫＩシステムでは、証明局（ＣＡ）という信用機関から人や組織のアイデンティティを証明するための証明書が発行される。アイデ

ンティティの立証を望む組織や人等の当事者は、それぞれのアイデンティティを証明するにあたって十分な証拠を証明局に登録する。ＣＡに対して当事者のアイデンティティが証明されたら、ＣＡからそのような当事者に証明書が発行される。この証明書は通常、証明書を発行したＣＡの名称と、証明書の発行を受けた当事者の名称と、当事者の公開鍵と、ＣＡの秘密鍵で署名された当事者の公開鍵（通常は公開鍵のダイジェストを暗号化することにより署名）とを含む。

【０００８】

ＣＡの公開鍵と秘密鍵にはつながりがあり、公開鍵を用いて暗号化されたデータは秘密鍵によって復号化でき、その逆も可能である。したがって、秘密鍵と公開鍵とは、一対の鍵をなす。RSA Security Inc. の２００２年６月１４日付「PKCS#1 v2.1:RSA Cryptography Standard 」では、暗号法のための一対の秘密鍵および公開鍵が説明されている。ＣＡの公開鍵は公に利用できる。したがって、ある当事者が相手方から提示される証明書の真偽をベリファイするなら、ベリファイする側はＣＡの公開鍵を使用し、証明書の中にある公開鍵の暗号化ダイジェストを復号化アルゴリズムを用いて復号化するだけでよい。この復号化アルゴリズムもまた、通常ならば証明書の中で特定される。証明書の中にある公開鍵の復号化ダイジェストが証明書の中にある暗号化されていない公開鍵のダイジェストに一致するなら、ＣＡの信用とＣＡの公開鍵の真正性とに基づき、証明書の公開鍵に改竄がなく本物であることが証明される。

【０００９】

ある当事者のアイデンティティをベリファイするにあたって、ベリファイする側は通常、質問（例えば、乱数）を送り、相手方には自身の証明書と質問に対する回答（すなわち、相手方の秘密鍵で暗号化された乱数）の送信を求める。回答と証明書が届いたら、ベリファイする側はまず、証明書の公開鍵が真正か否かを前述したプロセスでベリファイする。公開鍵の真正がベリファイされる場合、ベリファイする側は証明書の中にある公開鍵を使って回答を復号化し、その結果を当初送信した乱数に比較する。それらが一致する場合は相手方が正しい秘密鍵を所持していることを意味し、これをもって相手方は自身のアイデンティティを証明したことになる。証明書の中の公開鍵が真正でないか、あるいは復号化された回答が質問に一致しないと、認証は失敗に終わる。したがって、自身のアイデンティティを証明することを望む当事者は、証明書と対応する秘密鍵の両方を所持する必要がある。

【００１０】

前述したメカニズムにより、ことによると互いを信用できない２つの当事者でも、前述したプロセスを用いて相手方の証明書の中にある相手方の公開鍵をベリファイすることよって信用を成立させることができる。国際電気通信連合（ＩＴＵ）電気通信標準化部門（ＩＴＵ－Ｔ）の勧告Ｘ．５０９は証明書の枠組みを定める規格書である。証明書とその運用に関する詳しい情報はこの規格書で確認できる。

【００１１】

運営管理と大規模組織の便宜を図るため、ルートＣＡと呼ばれる上位ＣＡが証明書発行の責務をいくつかの下位ＣＡに委譲するとよい場合がある。例えば２レベル階層において、最上位のルートＣＡは下位ＣＡの公開鍵が真正であることを証明するための下位ＣＡに証明書を発行する。そして、下位ＣＡは前述した登録プロセスを通じて当事者に証明書を発行する。ベリファイプロセスは証明書連鎖の頂点から始まる。ベリファイする側はまず、ルートＣＡの公開鍵（真正と判明）を使用して、下位ＣＡの公開鍵の真性をベリファイする。下位ＣＡの公開鍵の真性がベリファイされたら、下位ＣＡから証明書の発行を受けた当事者の公開鍵の真性を、下位ＣＡのベリファイ済み公開鍵を用いてベリファイできる。このように、ルートＣＡと下位ＣＡとによって発行される証明書により、アイデンティティベリファイの対象となる当事者の２つの証明書からなる連鎖が形成される。

【００１２】

勿論、証明書階層のレベルは２レベルを上回ることもあり、ルートＣＡを除く下位レベルのＣＡはその権限を上位ＣＡから受け取り、上位ＣＡによって発行された公開鍵を含む

証明書を所持する。したがって、相手方の公開鍵の真性をベリファイするには、ルートＣＡに至る経路、すなわち証明書の連鎖をたどる必要がある。換言すると、アイデンティティを立証するには、アイデンティティを証明する必要がある側が自身の証明書からルートＣＡ証明書にかけて一連の証明書を提示する必要がある。

【００１３】

前に指摘したように、ルート証明書と、ＣＡへ発行される全ての証明書、例えば前述した証明書階層の中で下位ＣＡへ発行される証明書は、公開される。今のところ、アイデンティティを証明するための証明書の提示には２通りの形式がある。最初の形式では、認証を受けようとする側がＣＡによって発行された自身の証明書を提示するだけであり、この証明書は証明書連鎖の中で最後の証明書にあたる。この証明書の発行元にあたるＣＡの公開鍵をベリファイする側が持っていない場合、ＣＡの公開鍵を入手してベリファイを行うかどうかはベリファイする側次第となる。ベリファイする側は、下位ＣＡの公開鍵をベリファイするために上位証明局の公開鍵が必要となる場合、証明書の中にある発行元の名前をもとに上位ＣＡの公開鍵と証明書に至る経路をたどる必要がある。このプロセスは、ベリファイする側が、さらなるベリファイがなくとも真正であることが分かる公開鍵のＣＡに到達するまで続く。

【００１４】

証明書認証の第２の形式では、認証を受けようとする側から連鎖内の証明書がすべて提示されるが、それらの証明書は特定の順序で提示されるとは限らない。ベリファイする側へ送信される連鎖の中での証明書の正確な順序に関する情報を、証明書と併せて、認証を受けようとする側が提示しても、この情報がメッセージの後ろの方にあるなら、ベリファイする側は、証明書連鎖全体が届くまで証明書の正確な順序を知ることができない。

【００１５】

第１の証明書交換・ベリファイ形式では、ベリファイする側が不在の証明書にアクセスできることが前提になっている。不在の証明書を入手するためにコンピュータや携帯電話機等の装置でインターネット等のネットワークへアクセスすることはできても、これを果たすためにフラッシュメモリカード等の記憶装置そのものが使われたわけではない。

【００１６】

第２の証明書交換・ベリファイ形式では、ベリファイする装置へ送信されるメッセージの中で全ての証明書が提示されるため、ベリファイする装置が証明書を入手する必要はない。しかし、証明書が特定の順序で送信されるとは限らず、連鎖における証明書の順序に関する情報はメッセージのどこか、例えばメッセージの末尾に現れる。これは、連鎖の中のいずれかの証明書をベリファイのために解析する前に、全ての証明書を受信し蓄積しなければベリファイにかかれないことを意味する。これはコンピュータ、ＰＤＡ、携帯電話機等のホスト装置にとって問題にならないかもしれないが、記憶装置にとって問題になることがある。記憶装置の内蔵メモリ容量と処理能力があまりにも限られていると、長い証明書文字列を蓄積し効率よく解析することができない。

【００１７】

前述した様々な課題と問題のため、記憶装置とホスト装置で現在使われているシステムで完全に満足のいくものはない。したがって、より良い特性を備える改良されたシステムの提供が望まれる。

【先行技術文献】

【特許文献】

【００１８】

【特許文献１】米国仮特許出願第６０／８１９，５０７号
【特許文献２】米国特許出願第１１／３１３，８７０号
【特許文献３】米国仮特許出願第６０／６３８，８０４号
【特許文献４】米国特許出願第１１／３１４，４１１号
【特許文献５】米国特許出願第１１／３１４，４１０号
【特許文献６】米国特許出願第１１／３１３，５３６号

【特許文献７】米国特許出願第１１／３１３，５３８号
【特許文献８】米国特許出願第１１／３１４，０５５号
【特許文献９】米国特許出願第１１／３１４，０５２号
【特許文献１０】米国特許出願第１１／３１４，０５３号
【特許文献１１】米国特許出願第１１／５５７，０２８号
【特許文献１２】米国特許出願第１１／５５７，０１０号
【特許文献１３】米国特許出願第１１／５５７，００６号
【特許文献１４】米国特許出願第１１／５５７，０２６号
【特許文献１５】米国特許出願第１１／５５７，０４９号
【特許文献１６】米国特許出願第１１／５５７，０５６号
【特許文献１７】米国特許出願第１１／５５７，０５２号
【特許文献１８】米国特許出願第１１／５５７，０５１号
【特許文献１９】米国特許出願第１１／５５７，０４１号
【特許文献２０】米国特許出願第１１／５５７，０３９号
【発明の概要】
【００１９】
証明書連鎖は複数の連続する証明書文字列を含む。それぞれの文字列は少なくとも１つの証明書を含む。ベリファイする事業体にこれらの文字列が届くと、ベリファイする事業体はこれらの文字列を順次ベリファイする。証明書の文字列がベリファイと同じ順序で受信されるならば、前述した問題は回避される。このようなやり方で証明書の文字列を受信し、かつ完全な証明書連鎖を受信するならば、記憶装置を使って連鎖内の証明書の真性をベリファイすることは容易い。
【００２０】
証明書連鎖の中で連続する証明書文字列がベリファイと同じ順序で順次受信されるなら、ある１つの証明書文字列を受信しベリファイした後には、この証明書文字列の中にある情報はもはや必要でなくなる。もうひとつの実施形態によると、受信されメモリ装置に蓄積された少なくとも１つの証明書文字列は、順序の中の後続する文字列で上書きできる。かくして、ベリファイにあたって連鎖内の証明書の蓄積に要する蓄積容量は格段に減らすことができる。
【００２１】
ここで参照する特許、特許出願、記事、書籍、仕様書、規格書、その他の出版物、文書、物事はいずれも、あらゆる目的のためにその全体が本願明細書において参照により援用されている。援用する出版物、文書、または物事のいずれかと本願明細書の本文との間で用語の定義または使用に矛盾や食い違いがある場合、本願明細書における用語の定義または使用が優先するものとする。
【図面の簡単な説明】
【００２２】
【図１】本発明を例示するのに有用である、ホスト装置と通信するメモリシステムのブロック図である。
【図２】本発明の種々の実施形態を例示するのに有用である、特定のパーティションと暗号化ファイルへのアクセスをアクセス方針と認証手続きとによって制御するメモリの種々のパーティションと種々のパーティションに記憶される非暗号化および暗号化ファイルとの概略図である。
【図３】メモリ内の種々のパーティションを示すメモリの概略図である。
【図４】本発明の種々の実施形態を例示するのに有用である、パーティション内のいくつかのファイルが暗号化される図３に示すメモリの種々のパーティションのファイルロケーションテーブルの概略図である。
【図５】本発明の種々の実施形態を例示するのに有用である、アクセス制御記録グループ内のアクセス制御記録と対応する鍵参照符との概略図である。
【図６】本発明の種々の実施形態を例示するのに有用である、アクセス制御記録グループ

とアクセス制御記録とによって形成されるツリー構造の概略図である。
【図７】ツリーの形成プロセスを例示するための、アクセス制御記録グループからなる３つの階層ツリーを示すツリーの概略図である。
【図８Ａ】システムアクセス制御記録を作成し、かつ使用する場合にホスト装置とメモリカード等のメモリ装置とによって実行されるプロセスを示すフローチャートである。
【図８Ｂ】システムアクセス制御記録を作成し、かつ使用する場合にホスト装置とメモリカード等のメモリ装置とによって実行されるプロセスを示すフローチャートである。
【図９】種々の実施形態を例示するのに有用である、システムアクセス制御記録を使ってアクセス制御記録グループを作成するプロセスを示すフローチャートである。
【図１０】アクセス制御記録を作成するプロセスを示すフローチャートである。
【図１１】階層ツリーの一応用を例示するのに有用である、２つのアクセス制御記録グループの概略図である。
【図１２】特定の権利を委譲するプロセスを示すフローチャートである。
【図１３】図１２の委譲プロセスを例示するための、アクセス制御記録グループとアクセス制御記録との概略図である。
【図１４】暗号化および／または復号化の目的で鍵を作成するプロセスを示すフローチャートである。
【図１５】アクセス制御記録に従いアクセス権および／またはデータアクセス権限を削除するプロセスを示すフローチャートである。
【図１６】アクセス権および／またはアクセス権限が削除されたか、あるいは期限切れになった場合にアクセスを要求するプロセスを示すフローチャートである。
【図１７Ａ】本発明の種々の実施形態の例示に有用である、認証ルール構造と暗号鍵アクセス許諾方針の構成を示す概略図である。
【図１７Ｂ】本発明の種々の実施形態の例示に有用である、認証ルール構造と暗号鍵アクセス許諾方針の構成を示す概略図である。
【図１８】方針に従い被保護情報へのアクセスを制御する代替的な方法を示すデータベース構造のブロック図である。
【図１９】パスワードを用いた認証プロセスを示すフローチャートである。
【図２０】多数のホスト証明書連鎖を示す図である。
【図２１】多数のデバイス証明書連鎖を示す図である。
【図２２】一方向および相互認証方式のプロセスを示すプロトコル図である。
【図２３】一方向および相互認証方式のプロセスを示すプロトコル図である。
【図２４】本発明の一実施形態を例示するのに有用である、証明書連鎖の図である。
【図２５】本発明の別の実施形態を例示するための、メモリ装置へ最終証明書を送信する場合のホストによって送信される証明書バッファに先行する制御セクタ内の情報を示す表であって、この証明書が証明書連鎖における最終証明書であることを伝える標示を示す。
【図２６】メモリカードがホスト装置を認証する認証方式でカードとホストのプロセスをそれぞれ示すフローチャートである。
【図２７】メモリカードがホスト装置を認証する認証方式でカードとホストのプロセスをそれぞれ示すフローチャートである。
【図２８】ホスト装置がメモリカードを認証する認証方式でカードとホストのプロセスをそれぞれ示すフローチャートである。
【図２９】ホスト装置がメモリカードを認証する認証方式でカードとホストのプロセスをそれぞれ示すフローチャートである。
【図３０】本発明の別の実施形態を例示するための、メモリ装置に記憶された証明書失効リストがホスト装置によって検索される場合にホスト装置とメモリ装置とによってそれぞれ実行されるプロセスを示すフローチャートである。
【図３１】本発明の別の実施形態を例示するための、メモリ装置に記憶された証明書失効リストがホスト装置によって検索される場合にホスト装置とメモリ装置とによってそれぞれ実行されるプロセスを示すフローチャートである。

【図３２】本発明のさらに別の実施形態を示すための、証明書失効リスト内のフィールドを示す証明書失効リストの図である。
【図３３】証明書失効リストを使って証明書をベリファイするカードとホストのプロセスをそれぞれ示すフローチャートである。
【図３４】証明書失効リストを使って証明書をベリファイするカードとホストのプロセスをそれぞれ示すフローチャートである。
【図３５】カードがホストへ送信されるデータに署名し、かつホストからのデータを復号化するカードプロセスを示すフローチャートである。
【図３６】カードがホストへ送信されるデータに署名する場合のホストプロセスを示すフローチャートである。
【図３７】ホストが暗号化データをメモリカードへ送信する場合のホストプロセスを示すフローチャートである。
【図３８】一般情報および非公開情報クエリのプロセスをそれぞれ示すフローチャートである。
【図３９】一般情報および非公開情報クエリのプロセスをそれぞれ示すフローチャートである。
【図４０Ａ】本発明の一実施形態を例示するための、ホスト装置へ接続されたメモリ装置（フラッシュメモリカード等）におけるシステムアーキテクチャの機能ブロック図である。
【図４０Ｂ】図４０ＡのＳＳＭコアの内部ソフトウェアモジュールの機能ブロック図である。
【図４１】使い捨てパスワードを生成するシステムのブロック図である。
【図４２】使い捨てパスワード（ＯＴＰ）シード提供とＯＴＰ生成とを示す機能ブロック図である。
【図４３】シード提供段階を示すプロトコル図である。
【図４４】使い捨てパスワード生成段階を示すプロトコル図である。
【図４５】ＤＲＭシステムを示す機能ブロック図である。
【図４６】ライセンスオブジェクトの中で鍵が提供される場合のライセンス提供とコンテンツダウンロードのプロセスを示すプロトコル図である。
【図４７】再生操作のプロセスを示すプロトコル図である。
【図４８】ライセンスオブジェクトの中で鍵が提供されない場合のライセンス提供とコンテンツダウンロードのプロセスを示すプロトコル図である。
【００２３】
図面は、本発明の態様の様々な実施形態の特徴を示すものである。説明を簡潔にするため、本願では同じ構成要素を同じ数字で標示する。
【発明を実施するための形態】
【００２４】
図１のブロック図は、本発明の様々な態様を実装できる代表的なメモリシステムを示す。図１に示すように、メモリシステム１０は、中央演算処理装置（ＣＰＵ）１２と、バッファ管理部（ＢＭＵ）１４と、ホストインターフェイスモジュール（ＨＩＭ）１６と、フラッシュインターフェイスモジュール（ＦＩＭ）１８と、フラッシュメモリ２０と、周辺アクセスモジュール（ＰＡＭ）２２とを含む。メモリシステム１０は、ホストインターフェイスバス２６とポート２６ａとを通じてホスト装置２４と通信する。フラッシュメモリ２０はＮＡＮＤタイプのものであってもよく、ホスト装置２４のためのデータ記憶域を提供し、ホスト装置２４はデジタルカメラ、パーソナルコンピュータ、個人用携帯情報端末（ＰＤＡ）、ＭＰ３プレーヤ等のデジタルメディアプレーヤ、携帯電話機、セットトップボックス、その他のデジタル装置または家電品であってもよい。ＣＰＵ１２のソフトウェアコードもフラッシュメモリ２０に記憶できる。ＦＩＭ１８は、フラッシュインターフェイスバス２８とポート２８ａとを通じてフラッシュメモリ２０へ接続する。ＨＩＭ１６はホスト装置への接続に適している。周辺装置アクセスモジュール２２はＣＰＵ１２との通

信においてＦＩＭ、ＨＩＭ、およびＢＭＵ等の適切なコントローラモジュールを選択する。一実施形態において、点線の枠内にあるシステム１０の全構成要素をメモリカードまたはスティック１０’等の単独装置で囲い込み、好ましくはこれに封入してもよい。メモリシステム１０は脱着自在な状態でホスト装置２４へ接続されるため、多数の異なるホスト装置からシステム１０の内容にアクセスできる。

【００２５】

以降の説明ではメモリシステム１０をメモリ装置１０と呼ぶ場合があり、あるいは単にメモリ装置または装置と呼ぶ場合がある。ここではフラッシュメモリを参照しながら本発明を例示するが、本発明は、磁気ディスク、光ＣＤ等のタイプの異なるメモリや他の書き換え可能な不揮発性メモリシステムにも応用できる。

【００２６】

バッファ管理部１４は、ホストダイレクトメモリアクセス（ＨＤＭＡ）３２と、フラッシュダイレクトメモリアクセス（ＦＤＭＡ）３４と、アービタ３６と、バッファランダムアクセスメモリ（ＢＲＡＭ）３８と、クリプトエンジン４０とを含む。アービタ３６は共有バスアービタであるため、常に１つのみのマスタまたはイニシエータ（ＨＤＭＡ３２、ＦＤＭＡ３４、またはＣＰＵ１２）が稼動し、そのスレーブまたはターゲットはＢＲＡＭ３８である。アービタは、しかるべきイニシエータ要求をＢＲＡＭ３８へ振り向ける役割を果たす。ＨＤＭＡ３２とＦＤＭＡ３４は、ＨＩＭ１６、ＦＩＭ１８、およびＢＲＡＭ３８、またはＣＰＵランダムアクセスメモリ（ＣＰＵ　ＲＡＭ）１２ａ間でデータの転送を担当する。ＨＤＭＡ３２の動作とＦＤＭＡ３４の動作は従来どおりであり、ここで詳述する必要はない。ＢＲＡＭ３８は、ホスト装置２４とフラッシュメモリ２０との間で受け渡しされるデータを記憶するために使用する。ＨＤＭＡ３２とＦＤＭＡ３４は、ＨＩＭ１６／ＦＩＭ１８およびＢＲＡＭ３８またはＣＰＵ　ＲＡＭ１２ａ間でデータを転送し、さらにセクタの終了を指示する役割を果たす。

【００２７】

メモリシステム１０は、一実施形態において、暗号化および／または復号化に用いる鍵値を生成し、この値は、好ましくはホスト装置２４等の外部装置にとって事実上アクセス不能である。代替的に、システム１０の外部で、例えばライセンスサーバによって、鍵値を生成し、システム１０へ送信することもできる。鍵値を生成する方法にかかわりなく、いったんシステム１０に記憶された鍵値にアクセスできるものは認証済み事業体のみとなる。しかし、ホスト装置はメモリシステム１０におけるデータの読み書きをファイルの形で行うため、暗号化と復号化は通常であればファイル単位で行われる。メモリ装置１０は、タイプが異なる他の多数の記憶装置と同様に、ファイルを管理しない。メモリ２０は、ファイルの論理アドレスを識別するファイルアロケーションテーブル（ＦＡＴ）を記憶するが、このＦＡＴにアクセスし管理するのは通常であればホスト装置２４であって、コントローラ１２ではない。このため、ある特定のファイルのデータを暗号化する場合、コントローラ１２はメモリ２０におけるこのファイルのデータの論理アドレスをホスト装置に送信してもらう必要があり、このため、システム１０はこのファイルのデータを見つけ、システム１０のみが使用できる鍵値を使ってデータを暗号化および／または復号化できる。

【００２８】

ファイルデータの暗号処理においてホスト装置２４とメモリシステム１０の双方が同じ鍵を参照するための名前を用意するため、ホスト装置は、システム１０によって生成されるか、あるいはシステム１０へ送信される各鍵値につき参照符を提供し、この参照符とは要するに鍵ＩＤであってもよい。ホスト２４は、システム１０によって暗号処理される各ファイルに鍵ＩＤを割り振り、システム１０は、データの暗号処理に用いる各鍵値にホストから提供される鍵ＩＤを割り振る。よって、ホストはデータの暗号処理を要求するときに、その要求を、鍵ＩＤと、メモリ２０から取り出すか、またはメモリ２０に記憶するデータの論理アドレスと併せて、システム１０へ送信する。システム１０は鍵値を生成または受信し、ホスト２４から提供される鍵ＩＤをその値に割り振り、暗号処理を実行する。

メモリシステム１０の動作を変える必要はなく、メモリシステム１０は、鍵値に対する独占的アクセス等、鍵を使った暗号処理を完全に制御できる。換言すると、いったん鍵値がシステム１０に記憶されるか、あるいはシステム１０によって生成されたら、システムは、ＦＡＴの独占的制御によるファイルの管理をホスト２４に任せつつ、暗号処理に用いる鍵値の管理を一手に引き受ける。鍵値がメモリシステム１０に記憶された後、ホスト装置２４はデータの暗号処理に用いる鍵値の管理に関与しない。

【００２９】

ホスト２４から提供される鍵ＩＤとメモリシステムへ送信されるか、あるいはメモリシステムによって生成される鍵値は、一実施形態において、これ以降「コンテンツ暗号化鍵」もしくはＣＥＫと呼ぶ数量の２つの属性を形成する。ホスト２４は１つ以上のファイルに鍵ＩＤを割り振ってもよく、組織化されていないデータあるいは完全なファイルの形に組織化されたデータばかりでなく何らかのやり方で組織化されたデータに鍵ＩＤを割り振る場合がある。

【００３０】

システム１０で保護されたコンテンツや領域にユーザまたはアプリケーションがアクセスするには、システム１０に予め登録された信用証明を使って認証を受ける必要がある。信用証明はアクセス権に関連付けられ、この信用証明によって特定のユーザまたはアプリケーションにアクセス権が付与される。このような事前登録ではユーザまたはアプリケーションのアイデンティティおよび信用証明の記録をシステム１０に記憶し、ユーザまたはアプリケーションによって判定されたそのようなアイデンティティおよび信用証明に応じてアクセス権が割り振られ、ホスト２４を通じて提供される。事前登録が完了した後、メモリ２０へのデータ書き込みを要求するユーザまたはアプリケーションは、自身のアイデンティティおよび信用証明と、データを暗号化するための鍵ＩＤと、暗号化されたデータを記憶するところの論理アドレスとを、ホスト装置を通じて提供する必要がある。システム１０は鍵値を生成または受信し、ホスト装置から提供される鍵ＩＤをこの値に割り振り、書き込みデータの暗号化に用いる鍵値の鍵ＩＤをこのユーザまたはアプリケーションの記録またはテーブルに記憶する。そして、システム１０はデータを暗号化し、ホストによって指定されたアドレスに暗号化されたデータを記憶するほか、生成または受信した鍵値を記憶する。

【００３１】

メモリ２０から暗号化データを読み出すことを要求するユーザまたはアプリケーションは、自身のアイデンティティおよび信用証明と、要求するデータの暗号化に使われた鍵の鍵ＩＤと、暗号化データが記憶されているところの論理アドレスとを提供する必要がある。システム１０は、ホストから提供されたユーザまたはアプリケーションのアイデンティティおよび信用証明を自身の記録に記憶されたものに突き合せる。システム１０は、それらが一致する場合、ユーザまたはアプリケーションから提供された鍵ＩＤと関連付けられた鍵値を自身のメモリから取り出し、ホスト装置が指定するアドレスに記憶されたデータを鍵値を用いて復号化し、復号化したデータをユーザまたはアプリケーションへ送信する。

【００３２】

認証のための信用証明を暗号処理に用いる鍵の管理から分離することにより、異なる信用証明で共通のデータアクセス権を有することが可能となる。つまり、信用証明がそれぞれ異なる１グループのユーザまたはアプリケーションは同じ鍵にアクセスして同じデータにアクセスできても、このグループ以外のユーザはアクセスできない。１グループ内のすべてのユーザまたはアプリケーションが同じデータにアクセスする場合でも、それらのユーザまたはアプリケーションの権利が依然として異なる場合がある。読み出し限定のアクセス権を有するものもあれば、書き込みアクセス権のみを有するものもあれば、両方を有するものもある。ユーザまたはアプリケーションのアイデンティティおよび信用証明と、アクセスできる鍵ＩＤと、各々の鍵ＩＤに関連するアクセス権との記録を維持するシステム１０では、正式に認証されたホスト装置の管理下で鍵ＩＤを追加または削除したり、特

定のユーザまたはアプリケーションの鍵ＩＤと関連付けられたアクセス権を変更したり、あるユーザまたはアプリケーションから別のユーザまたはアプリケーションにアクセス権を委譲できるほか、ユーザまたはアプリケーションの記録またはテーブルを削除または追加することもできる。記憶された記録では、特定の鍵へのアクセスにおいてセキュアチャネルを特定することができる。認証は、対称または非対称アルゴリズムとパスワードを使って果たすことができる。

【００３３】

とりわけ重要なこととして、メモリシステム１０の中で保護されたコンテンツは移動できる。鍵値へのアクセスがメモリシステムによって制御される実施形態において、メモリシステムまたはこのシステムを内蔵する記憶装置がある１つの外部システムから別の外部システムへ移される場合、そこに記憶されたコンテンツの安全は保たれる。鍵がメモリシステムによって生成されようが、メモリシステムの外から届くものであろうが、外部システムは、メモリシステムによって完全に統制されたやり方で認証されない限り、システム１０のコンテンツにアクセスできない。そのとおりに認証された後でもアクセスはメモリシステムによって全面的に制御され、外部システムによるアクセスのあり方は、メモリシステムに予め設定された記録に従って制御される。このような記録に準拠しない要求は拒否される。

【００３４】

コンテンツ保護の柔軟性を高めるため、これ以降パーティションと呼ぶメモリの特定領域が想定され、このパーティションには正式に認証されたユーザまたはアプリケーションのみがアクセスできる。これを前述した鍵方式のデータ暗号化機能と組み合わせることにより、システム１０のデータ保護能力は向上する。図２に示すように、フラッシュメモリ２０の記憶容量は、多数のパーティション、すなわちユーザ領域またはパーティションとカスタムパーティションに分割できる。ユーザ領域またはパーティションＰ０には、すべてのユーザまたはアプリケーションが認証なしでアクセスできる。ユーザ領域に記憶されたデータのビット値のすべてがいずれのアプリケーションまたはユーザでも読み書きできるが、読み出しデータが暗号化されている場合、復号化の権限を有していないユーザまたはアプリケーションは、ユーザ領域に記憶されたビット値表現の情報にアクセスできない。例えば、ユーザ領域Ｐ０に記憶されたファイル１０２および１０４がこれにあたる。１０６等のユーザ領域には暗号化されていないファイルも記憶され、すべてのアプリケーションおよびユーザがこれを読み出し、解釈できる。ファイル１０２および１０４等の暗号化されたファイルは錠前の記号を関連付けて表示されている。

【００３５】

権限のないアプリケーションまたはユーザはユーザ領域Ｐ０で暗号化されたファイルを解釈できないが、そのようなアプリケーションまたはユーザであってもファイルを削除したり破壊したりすることは可能であり、用途によっては好ましくない場合がある。このため、メモリ２０には、パーティションＰ１およびＰ２等の事前の認証なくしてアクセスできない被保護カスタムパーティションもある。この用途の実施形態に使える認証プロセスをこれより説明する。

【００３６】

同じく図２に示されているように、メモリ２０のファイルには様々なユーザまたはアプリケーションがアクセスする。そこで図２には、ユーザ１および２とアプリケーション１～４（装置上で実行）が示されている。これらの事業体は、これより説明する認証プロセスによって認証された後にメモリ２０の被保護コンテンツへのアクセスが認められる。このプロセスでは、アクセスを要求する事業体をロール方式のアクセス制御のためにホスト側で識別する必要がある。そこでアクセスを要求する事業体はまず、「私はアプリケーション２であってファイル１を読み出したい」等の情報を供給することによって自身を識別する。コントローラ１２はそのアイデンティティと、認証情報と、要求とを、メモリ２０またはコントローラ１２に記憶された記録に突き合せる。すべての要件が満たされる場合、そのような事業体にアクセスが認められる。図２に示すように、ユーザ１はパーティシ

ョンＰ１のファイル１０１を読み書きでき、Ｐ０ではファイル１０６に対する無制限の読み出し・書き込み権利を有しているが、これ以外に読み出し可能なファイルはファイル１０２および１０４のみである。他方、ユーザ２は、ファイル１０１および１０４へのアクセスを許可されないが、ファイル１０２に対する読み出し・書き込みアクセス権は有している。図２に示すように、ユーザ１および２のログインアルゴリズム（ＡＥＳ）は同じであるが、アプリケーション１および３のログインアルゴリズムはそれぞれ異なり（例えば、ＲＳＡと００１００１）、ユーザ１および２のものとも異なる。

【００３７】

セキュアストレージアプリケーション（ＳＳＡ）は本発明の一実施形態を例示するメモリシステム１０のセキュリティアプリケーションであり、前述した機能の多くはこれを用いて実行できる。ＳＳＡはソフトウェアまたはコンピュータコードとして実装でき、メモリ２０またはＣＰＵ１２の不揮発性メモリ（図示せず）に記憶されたデータベースがＲＡＭ１２ａに読み込まれ、ＣＰＵ１２によって実行される。次の表には、ＳＳＡに言及する場合に用いる頭字語が記されている。

定義、頭字語、および略語

ＡＣＲ	アクセス制御記録
ＡＧＰ	ＡＣＲグループ
ＣＢＣ	連鎖ブロック暗号
ＣＥＫ	コンテンツ暗号化鍵
ＥＣＢ	電子コードブック
ＡＣＡＭ	ＡＣＲ属性管理
ＰＣＲ	権限制御記録
ＳＳＡ	セキュアストレージアプリケーション
事業体	単独の実体を有し（ホスト側）、ＳＳＡにログインすることによりその機能を利用するもの

【００３８】

ＳＳＡシステムの説明

ＳＳＡの主な役割はデータの保護と保全とアクセス制御である。データとは、いくつかの大容量記憶装置に一目瞭然な状態で記憶される場合があるファイルである。ＳＳＡシステムは記憶システムの上部に位置し、記憶されたホストファイルのためのセキュリティ層を加え、後述するセキュリティデータ構造を通じてセキュリティ機能を提供する。

【００３９】

ＳＳＡの主な仕事は、メモリに記憶された（保護された）コンテンツに関わる様々な権利を管理することである。メモリアプリケーションは、複数の記憶コンテンツに対する複数のユーザおよびコンテンツ権利を管理する必要がある。ホストアプリケーションは提示されたドライブとパーティションをホスト側から看取するほか、記憶装置に記憶されたファイルの位置を管理し表現するファイルアロケーションテーブル（ＦＡＴ）を看取する。

【００４０】

この場合の記憶装置はパーティションに分割されたＮＡＮＤフラッシュチップを使用するが、他の可搬型記憶装置も使用でき、本発明の範囲内にある。これらのパーティションは一連の論理アドレスであり、その境界は開始アドレスと終端アドレスで区切られる。したがって、所望により、非表示のパーティションへのアクセスに制限を設けることができ、それにはソフトウェア（メモリ２０に記憶されたソフトウェア等）によってそのような

境界内のアドレスにそのような制限を関連付ける。ＳＳＡは、自身が管理する論理アドレスの境界によってパーティションを完全に認識する。ＳＳＡシステムはパーティションを用いて権限を有していないホストアプリケーションからデータを物理的に保護する。ホストにとってのパーティションは、データファイルが記憶されるところの専有空間を規定するメカニズムである。これらのパーティションを公開する場合、記憶装置にアクセスできる者であれば誰でも装置におけるこれらのパーティションの存在を看取して認識し、パーティションを非公開にする場合もしくは非表示にする場合、選ばれたホストアプリケーションのみがこれらのパーティションにアクセスでき、記憶装置におけるこれらの存在をも認識できる。

【００４１】

図３はメモリのパーティションＰ０、Ｐ１、Ｐ２、およびＰ３を示すメモリの概略図であり（言うまでもなく５つ以上のパーティションが使われることも、あるいは３つ以下のパーティションが使われることもある）、Ｐ０はいずれの事業体でも認証なしでアクセスできる公開パーティションである。

【００４２】

非公開パーティション（Ｐ１、Ｐ２、またはＰ３等）の中にあるファイルへのアクセスは非表示にされる。ホストによるパーティションへのアクセスを阻止することにより、フラッシュ装置（例えば、フラッシュカード）はパーティションの中でデータファイルの保護を達成する。しかし、この種の保護は、非表示パーティションの中で論理アドレスに記憶されたデータへのアクセスに制限を設けることによって、非表示パーティションの中にあるすべてのファイルを囲い込むものである。換言すると、一連の論理アドレスに制限を関連付けるものである。そのパーティションへアクセスできるユーザ／ホストはいずれも、内部にあるすべてのファイルに無制限にアクセスできる。ファイル（またはファイル群）を互いに分離するため、ＳＳＡシステムは鍵と鍵の参照符すなわち鍵ＩＤとを用いて別の保護・保全レベルをファイル（またはファイル群）単位で提供する。様々なメモリアドレスでデータを暗号化するのに用いられる鍵値の鍵参照符すなわち鍵ＩＤは、暗号化データを収容する容器または領域にたとえることができる。このため、図４では、鍵ＩＤと関連付けられた鍵値を用いて暗号化されたファイルを取り囲む領域として鍵参照符すなわち鍵ＩＤ（例えば、「鍵１」および「鍵２」）が示されている。

【００４３】

図４を参照し、例えばファイルＡは鍵ＩＤで囲まれていないため、いずれの事業体でも認証なしでファイルＡにアクセスできる。公開パーティションの中にあるファイルＢはいずれの事業体でも読み出しや上書きを行えるが、その中のデータはＩＤ「鍵１」を有する鍵で暗号化されているため、このような鍵にアクセスできるこのような事業体でない限り、ファイルＢの中にある情報にはアクセスできない。このような鍵値と鍵参照符すなわち鍵ＩＤの使用は、前述したパーティションによる保護とは異なり、論理的な保護のみを提供する。つまり、パーティション（公開または非公開）にアクセスできるホストであればいずれでもそのパーティションの中で暗号化データを含むデータを読み書きできる。しかし、データは暗号化されているため、権限を有していないユーザはデータを壊すことしかできない。権限を有していないユーザは、好ましくは発覚することなくこのデータを変更できない。暗号化および／または復号化鍵へのアクセスを制限することにより、権限を有する事業体のみにデータの使用を認めることができる。Ｐ０ではファイルＢおよびＣも鍵ＩＤ「鍵２」を有する鍵を使って暗号化されている。

【００４４】

データの機密保護と保全は、コンテンツ暗号化鍵（ＣＥＫ）をＣＥＫ当たり１つずつ使用する対称暗号化法で提供できる。ＳＳＡの実施形態では、ＣＥＫの鍵値がフラッシュ装置（例えば、フラッシュカード）によって生成または受信され、内部でのみ使用され、外部に対して秘密に保たれる。暗号化されるデータでハッシュ計算を行うか、あるいは暗号を連鎖ブロック化することによってデータ保全を徹底することもできる。

【００４５】

パーティション内のすべてのデータが異なる鍵によって暗号化され、異なる鍵ＩＤが割り振られるわけではない。公開またはユーザファイルの中またはオペレーティングシステム領域（すなわち、ＦＡＴ）の中で、論理アドレスに鍵または鍵参照符が割り振られない場合があり、この場合、パーティション自体にアクセスできる事業体であればいずれでもこれにアクセスできる。

【００４６】

鍵やパーティションの作成や、パーティションにおけるデータの読み書きや、鍵の使用を望む事業体は、アクセス制御記録（ＡＣＲ）を通じてＳＳＡシステムにログインする必要がある。ＳＳＡシステムにおけるＡＣＲの特権はアクションと呼ばれる。どのＡＣＲでも３種類のアクション、すなわちパーティションおよび鍵／鍵ＩＤの作成と、パーティションおよび鍵へのアクセスと、他のＡＣＲの作成／更新とを実行する権限を有することができる。

【００４７】

ＡＣＲは、ＡＣＲグループすなわちＡＧＰと呼ばれるグループに整理する。ＡＣＲの認証に成功するとＳＳＡシステムがセッションを開放し、このセッションの中でＡＣＲのアクションを実行できる。ＡＣＲとＡＧＰは、方針に従ってパーティションや鍵へのアクセスを制御するためのセキュリティデータ構造である。

【００４８】

ユーザパーティション

ＳＳＡシステムは、ユーザパーティションとも呼ばれる１つ以上の公開パーティションを管理する。このパーティションは記憶装置上に存在し、記憶装置の標準的な読み出し・書き込みコマンドを通じてアクセスできるパーティションである。このパーティションのサイズと装置上でのこのパーティションの存在に関する情報は、好ましくはホストに対して非表示にしない。

【００４９】

ＳＳＡシステムでは、標準的な読み出し・書き込みコマンドまたはＳＳＡコマンドを通じてこのパーティションにアクセスできる。このパーティションへのアクセスは、好ましくは特定のＡＣＲに制限しない。しかし、ＳＳＡシステムの場合、ホスト装置はユーザパーティションへのアクセスを制限できる。読み出し・書き込みアクセスは個別に有効／無効にできる。４通りの組み合わせすべて（例えば、書き込み限定、読み出し限定（書き込み保護）、読み出しおよび書き込み、アクセス不能）が可能である。

【００５０】

ＳＳＡシステムでは、ＡＣＲを使ってユーザパーティションの中にあるファイルに鍵ＩＤを割り振り、そのような鍵ＩＤと関連付けられた鍵を使って個々のファイルを暗号化できる。ユーザパーティションの中にある暗号化ファイルへのアクセスとパーティションへのアクセス権設定は、ＳＳＡコマンドセットを使って行う。前述した機能はファイルの形に組織されていないデータにも当てはまる。

【００５１】

ＳＳＡパーティション

これは、ＳＳＡコマンドでないとアクセスできない非表示（認証されていない者に対して非表示にされた）パーティションである。ＳＳＡシステムは好ましくは、ＡＣＲへのログインによって確立するセッション（後述）の中でアクセスが行われる場合を除き、ホスト装置によるＳＳＡパーティションへのアクセスを許可しない。同様に、ＳＳＡは好ましくは、ＳＳＡパーティションの存在と、サイズと、アクセス権限とに関する情報を、その要求が確立されたセッションの中で発生する場合を除き、提供しない。

【００５２】

パーティションに対するアクセス権はＡＣＲ権限から検索される。ＳＳＡシステムにログインしたＡＣＲは他のＡＣＲとパーティションを共用できる（後述）。パーティションが作成されると、ホストはそのパーティションに参照名またはＩＤ（例えば、図３および４におけるＰ０～Ｐ３）を与える。この参照名は、このパーティションに対する以降の読

み出し・書き込みコマンドで使われる。

【００５３】

記憶装置の分割

好ましくは、装置の使用可能な記憶容量のすべてをユーザパーティションとその時点で構成済みのＳＳＡパーティションとに割り当てる。このため、再分割において既存のパーティションの再構成をともなうことがある。装置容量（全パーティションの合計サイズ）の正味の変化はゼロである。装置メモリ空間におけるパーティションのＩＤはホストシステムによって設定される。

【００５４】

ホストシステムは、既存パーティションのいずれか１つを２つのより小さいパーティションに再分割したり、２つの既存パーティション（隣接する場合とそうでない場合とがある）を１つに併合したりすることができる。分割されたパーティションや併合されたパーティションの中のデータは、ホストの判断で消去するか、あるいは現状のまま残すことができる。

【００５５】

記憶装置の再分割によってデータが（記憶装置の論理アドレス空間の中での消去や移動により）失われるおそれがあるため、ＳＳＡシステムは再分割において厳重な制限を課す。つまり、ルートＡＧＰ（後述）の中にあるＡＣＲにのみ再分割コマンドの発行が許され、これが参照できるパーティションは自身が所有するパーティションのみである。パーティションの中でデータがどのように構成されているかはＳＳＡシステムには分からないから（ＦＡＴまたはその他のファイルシステム構造）、装置の再分割において構成を組み直す責任はホストにある。

【００５６】

ユーザパーティションの再分割によって、ホストＯＳから見たこのパーティションのサイズやその他の属性は変化する。

【００５７】

再分割の後、ホストシステムにはＳＳＡシステムで存在しないパーティションをＡＣＲが参照していないことを確認する責任がある。これらのＡＣＲが適切に削除または更新されないと、不在パーティションに対してこれらのＡＣＲに代わって行われるアクセスの試みはシステムによって検出され、拒否される。削除される鍵や鍵ＩＤについても同様の配慮がなされる。

【００５８】

鍵、鍵ＩＤ、論理的保護

ある特定の非表示パーティションに書き込まれたファイルは公から非表示にされる。しかし、いったん事業体（敵対的な事業体、またはそうでない事業体）が情報を得てこのパーティションにアクセスすると、そのファイルは使用可能となり一目瞭然となる。そのファイルのさらなる安全確保のため、ＳＳＡは非表示パーティションでファイルを暗号化でき、このファイルの復号化に用いる鍵にアクセスするための信用証明は、好ましくはパーティションにアクセスするためのものとは異なるものにする。ファイルはホストによって全面的に制御され、管理されるため、ファイルにＣＥＫを割り振ることには問題がある。これを解決するには、ＳＳＡが了解する何か、すなわち鍵ＩＤにファイルを関連付ける。つまりＳＳＡによって鍵が作成されたら、ホストはその鍵を使って暗号化されるデータに鍵ＩＤを割り振る。鍵が鍵ＩＤと併せてＳＳＡに送られる場合、鍵と鍵ＩＤを互いに関連付けることは容易い。

【００５９】

鍵値と鍵ＩＤは論理的セキュリティを提供する。特定の鍵ＩＤが割り振られたデータはいずれも、その場所にかかわりなく、コンテンツ暗号化鍵（ＣＥＫ）の同じ鍵値で暗号化され、ホストアプリケーションからは一意な参照名すなわち鍵ＩＤが提供される。（ＡＣＲ認証により）非表示パーティションにアクセスし、そのパーティション内にある暗号化ファイルの読み出しまたは書き込みを望む事業体は、そのファイルに割り振られた鍵ＩＤ

にアクセスする必要がある。この鍵ＩＤの鍵に対するアクセスを許諾する場合、ＳＳＡはこの鍵ＩＤと関連付けられたＣＥＫに鍵値をロードし、データを復号化してからホストへ送信するか、あるいはデータを暗号化してからフラッシュメモリ２０に書き込む。一実施形態において、鍵ＩＤと関連付けられたＣＥＫの鍵値がＳＳＡシステムによって無作為に作成され、ＳＳＡシステムによって維持される。ＳＳＡシステムの外でＣＥＫの鍵値を知るか、あるいはアクセスする者はいない。外部から提供され外部で使用するのは参照符すなわち鍵ＩＤのみであり、ＣＥＫの鍵値ではない。鍵値はＳＳＡによって全面的に制御され、好ましくはＳＳＡのみがこれにアクセスできる。代替的に、ＳＳＡシステムに鍵を提供することもできる。

【００６０】

ＳＳＡシステムは、次の暗号モードのいずれか１つ（ユーザにより設定）を用いて鍵ＩＤと関連付けられたデータを保護する（実際に使われる暗号アルゴリズムとＣＥＫにおける鍵値はシステムの管理下にあって、外部には明かされない）。

・ブロックモード：データをブロックに分割し、それぞれのブロックを個別に暗号化する。このモードは一般的に安全性が低いとされ、辞書攻撃を被りやすいが、ユーザはデータブロックのいずれか１つにランダムにアクセスできる。

・連鎖モード：データをブロックに分割し、暗号化の過程で鎖状に繋ぎ合わせる。ブロックはいずれも、次のブロックの暗号化プロセスへの入力として使われる。安全性は高いとされているが、データの読み書きが最初から最後まで順次に行われるため、ユーザにとって容認しがたいオーバーヘッドが発生することがある。

・ハッシュモード：連鎖モードに、データ保全性ベリファイに用いるデータダイジェストの作成を加えたもの。

【００６１】

ＡＣＲとアクセス制御

ＳＳＡは多数のアプリケーションを取り扱うように設計され、システムデータベースの中では、ノードからなるツリーとしてそれぞれのアプリケーションを表現する。ツリーのブランチ間のクロストークをなくすことによりアプリケーション間の相互排除を達成する。

【００６２】

ＳＳＡシステムにアクセスする場合、事業体はシステムのいずれか１つのＡＣＲを通じて接続を確立する必要がある。ＳＳＡシステムは、接続する場合、ユーザが選ぶＡＣＲの規定に従ってログイン手続きを運営する。

【００６３】

ＡＣＲはＳＳＡシステムに至る個々のログイン地点である。ＡＣＲはログイン信用証明と認証方法を保持する。読み出し特権や書き込み特権を含むＳＳＡシステムの中でのログイン権限もこの記録の中にある。これを示す図５には、同じＡＧＰの中にｎ個のＡＣＲがある。これは、ｎ個のＡＣＲのうちの少なくとも種々のＡＣＲが同じ鍵へのアクセス権を共有することを意味する。つまり、ＡＣＲ＃１とＡＣＲ＃ｎは鍵ＩＤ「鍵３」を有する鍵へのアクセス権を共有し、ここでＡＣＲ＃１とＡＣＲ＃ｎはＡＣＲ　ＩＤであって、「鍵３」は鍵の鍵ＩＤであって、この鍵を用いて「鍵３」に関連するデータが暗号化される。複数ファイルまたは複数データ群の暗号化および／または復号化に同じ鍵を使うこともできる。

【００６４】

ＳＳＡシステムは数通りのシステムログインをサポートし、認証アルゴリズムとユーザ信用証明は様々であってもよく、ログインに成功したユーザのシステムにおける特権も様々であってもよい。図５には様々なパスワードログインアルゴリズムと信用証明とが例示されている。ＡＣＲ＃１ではパスワードログインアルゴリズムとパスワードとが、信用証明として指定され、ＡＣＲ＃２ではＰＫＩ（公開鍵基盤）ログインアルゴリズムと公開鍵が信用証明として指定されている。したがって、事業体はログインにおいて有効なＡＣＲＩＤを提示するほか、適切なログインアルゴリズムと信用証明とを提示する必要がある

。

【００６５】

ＳＳＡシステムのＡＣＲにログインした事業体の権限、すなわちＳＳＡコマンドを使用する権利は、ＡＣＲと関連付けられた権限制御記録（ＰＣＲ）の中で設定する。図５のＰＣＲに示すように、ＡＣＲ＃１は「鍵３」と関連付けられたデータに対して読み出し限定権限を許諾し、ＡＣＲ＃２は「鍵５」と関連付けられたデータの読み出し権限と書き込み権限とを許諾する。

【００６６】

読み出しや書き込みに使う鍵等の異なるＡＣＲがシステムで共通の利権・特権を有することがある。このため、共通する部分があるＡＣＲはＡＧＰ、すなわちＡＣＲグループにグループ分けする。ＡＣＲ＃１とＡＣＲ＃ｎはいずれも、鍵ＩＤ「鍵３」を有する鍵へのアクセス権がある。

【００６７】

ＡＧＰとその中にあるＡＣＲは階層状のツリーの中で編制されるため、ＡＣＲは重要データの安全性を保つ安全鍵を作成できるほか、好ましくは自身の鍵ＩＤ／パーティションに対応する他のＡＣＲ項目を作成できる。これらの子ＡＣＲは、その父、すなわち作成元と同じ権限を有するかそれよりも少ない権限を有することになり、父ＡＣＲ自身が作成した鍵の権限が付与される場合がある。言うまでもなく、子ＡＣＲは自身が作成する任意の鍵に対するアクセス権限を取得する。これは図６に例示されている。ＡＧＰ１２０の中にあるＡＣＲはいずれもＡＣＲ１２２によって作成されたものであり、これらのＡＣＲのうちの２つは、「鍵３」と関連付けられたデータへのアクセス権限をＡＣＲ１２２から継承している。

【００６８】

ＡＧＰ

ＳＳＡシステムへのログインにおいて、ＡＧＰとそのＡＧＰの中にあるＡＣＲを指定する。

ＡＧＰはいずれも一意なＩＤ（参照名）を有し、ＳＳＡデータベースにおける該当する項目への索引として使われる。ＡＧＰ名はＡＧＰの作成時にＳＳＡシステムに支給される。ＳＳＡは、支給されるＡＧＰ名がシステムに既に存在する場合に作成動作を拒否する。

【００６９】

以降のセクションで説明するように、アクセス権限や管理権限の委譲に関わる制限事項はＡＧＰを使って管理運営する。完全に独立した事業体、例えば２つの異なるアプリケーションまたは２つの異なるコンピュータユーザによるアクセスの制御運営は、図６の２つのツリーが果たす役割の１つである。ここで大切なり得ることは、２つのアクセスプロセスが、たとえ同時に発生する場合でも、事実上互いに独立する（すなわち、事実上クロストークをなくす）ことである。これは、それぞれのツリーにおけるＡＣＲとＡＧＰの認証、権限、追加作成等が他のツリーにおけるものと無関係であり、かつ他のツリーにおけるものに左右されないことを意味する。このため、ＳＳＡシステムを使用するメモリシステム１０では、複数のアプリケーションを同時に処理できる。また、２つのアプリケーションが互いに自立的に２つの別々のデータ群（例えば、１組の写真と１組の歌）にアクセスすることも可能になる。これは図６に例示されている。図６の上部で、ツリーの中にあるノード（ＡＣＲ）を通じてアクセスするアプリケーションまたはユーザにとって、「鍵３」、「鍵Ｘ」、および「鍵Ｚ」と関連付けられたデータは写真であってもよい。図６の下部で、ツリーのノード（ＡＣＲ）を通じてアクセスするアプリケーションまたはユーザにとって、「鍵５」および「鍵Ｙ」と関連付けられたデータは歌であってもよい。ＡＧＰを作成したＡＣＲは、このＡＧＰにＡＣＲ項目がなく空になっている場合に限りこのＡＧＰを削除できる。

【００７０】

事業体にとってのＳＳＡの入口：アクセス制御記録（ＡＣＲ）

ＳＳＡシステムのＡＣＲは、事業体によるシステムログインのあり方を記述するもので

ある。ＳＳＡシステムにログインする事業体は、これから始まる認証プロセスに該当するＡＣＲを指定する必要がある。図５に示すように、ＡＣＲの中にある権限制御記録（ＰＣＲ）は、ＡＣＲの認証を終えたユーザが実行できる許諾アクションを明らかにするものである。ホスト側事業体はすべてのＡＣＲデータフィールドを提供する。

【００７１】

ＡＣＲへのログインに成功した事業体は、そのＡＣＲのパーティション・鍵アクセス権限やＡＣＡＭ権限（後述）を照会できる。

ＡＣＲ　ＩＤ

ＳＳＡシステムの事業体はログインプロセスを開始するときに、そのログイン方法に該当するＡＣＲ　ＩＤを指定する必要がある（ＡＣＲが作成される場合にホストより支給される）ので、ＳＳＡは正しいアルゴリズムを準備し、すべてのログイン条件が満たされたら正しいＰＣＲを選択する。ＡＣＲ　ＩＤはＡＣＲの作成時にＳＳＡシステムに提供される。

【００７２】

ログイン／認証アルゴリズム

事業体によって使われるログイン手続きと、ユーザのアイデンティティを証明する場合に必要となる信用証明は、認証アルゴリズムによって決まる。手続きなし（信用証明なし）からパスワードに基づく手続き、対称暗号法か非対称暗号法に基づく双方向認証プロトコルまで、ＳＳＡシステムは数通りの標準的なログインアルゴリズムをサポートする。

【００７３】

信用証明

事業体の信用証明はログインアルゴリズムに対応し、ＳＳＡがユーザをベリファイし認証するのに使われる。パスワード認証のためのパスワード／ＰＩＮ番号やＡＥＳ認証のためのＡＥＳ鍵等は信用証明の一例であり得る。信用証明のタイプ／書式（ＰＩＮ、対称鍵等）は予め決まり、認証モードから検索され、ＡＣＲの作成時にＳＳＡシステムに提供される。ＳＳＡシステムはこれら信用証明の設定、配布、管理に関与しないが、例外としてＰＫＩ方式の認証では装置（例えば、フラッシュカード）を使ってＲＳＡ等の鍵対を生成でき、証明書生成のための公開鍵をエクスポートできる。

【００７４】

権限制御記録（ＰＣＲ）

ＰＣＲは、ＳＳＡシステムにログインしＡＣＲの認証プロセスに合格した後の事業体に対する許諾事項を明らかにするものである。権限には、パーティションおよび鍵の作成権限と、パーティションおよび鍵へのアクセス権限と、事業体－ＡＣＲ属性の管理権限の３種類がある。

【００７５】

パーティションへのアクセス

ＰＣＲのこの部分には、ＡＣＲ段階を首尾よく完了した事業体からアクセスできるパーティションのリストが入る（ＳＳＡシステムへ提供されるパーティションのＩＤを使用）。パーティションごとに書き込み限定または読み出し限定にアクセスのタイプが制限される場合があったり、あるいは完全書き込み／読み出しアクセス権が指定される場合もある。図５のＡＣＲ＃１はパーティション＃２にアクセスできてもパーティション＃１にはアクセスできない。ＰＣＲの中で指定される制限はＳＳＡパーティションと公開パーティションとに適用される。

【００７６】

公開パーティションには、ＳＳＡシステムをホストする装置（例えば、フラッシュカード）に対する通常の読み出しおよび書き込みコマンドでアクセスするか、あるいはＳＳＡコマンドでアクセスする。公開パーティションを制限する権限を有するルートＡＣＲ（後述）が作成されると、このルートＡＣＲはその権限を自身の子に渡すことができる。ＡＣＲは、好ましくは通常の読み出しおよび書き込みコマンドによる公開パーティションへのアクセスのみを制限できる。ＳＳＡシステムのＡＣＲは、好ましくはこれが作成されると

きにのみ制限できる。公開パーティションに対する読み出し／書き込み権限をＡＣＲが得た後、好ましくはその権限は剥奪できない。

【００７７】

鍵ＩＤアクセス

ＰＣＲのこの部分には、事業体のログインプロセスによってＡＣＲ方針が満たされた場合に該当する事業体からアクセスできる、鍵ＩＤのリスト（ホストからＳＳＡシステムへの提供）と関連付けられたデータが入る。ＰＣＲに記載されたパーティション内のファイルには指定された鍵ＩＤが割り振られる。デバイス（例えば、フラッシュカード）の論理アドレスに鍵ＩＤは割り振られないため、ある特定のＡＣＲに対して２つ以上のパーティションがある場合、それらのパーティションのいずれかの中にはファイルがある。ＰＣＲの中で指定された鍵ＩＤはそれぞれ異なる１組のアクセス権を有することができる。鍵ＩＤによって指示されるデータへのアクセスは、書き込み限定または読み出し限定に制限される場合があったり、あるいは完全書き込み／読み出しアクセス権が指定される場合もある。

【００７８】

ＡＣＲ属性管理（ＡＣＡＭ）

このセクションではＡＣＲのシステム属性が変更できる場合について説明する。

ＳＳＡシステムで許可され得るＡＣＡＭアクションは次のとおりである。

１．ＡＧＰとＡＣＲの作成／削除／更新

２．パーティションと鍵の作成／削除

３．鍵およびパーティションに対するアクセス権の委譲

父ＡＣＲは、好ましくはＡＣＡＭ権限を編集できない。この場合、好ましくはＡＣＲの削除と再作成が必要となる。また、ＡＣＲによって作成された鍵ＩＤに対するアクセス権限は、好ましくは剥奪できない。

【００７９】

ＡＣＲには他のＡＣＲやＡＧＰを作成する容量があってもよい。ＡＣＲを作成するということは、作成元が所有するＡＣＡＭ権限の一部または全部が作成されたＡＣＲへ委譲されることを意味する場合がある。ＡＣＲを作成する権限を有するということは、次のアクションの権限を有することを意味する。

１．子の信用証明を設定し編集する－作成元ＡＣＲによって一旦設定された認証方法は、好ましくは編集できない。子向けに予め設定された認証アルゴリズムの範囲内で信用証明を変更してもよい。

２．ＡＣＲを削除する。

３．作成権限を子ＡＣＲへ委譲する（よって孫ができる）。

【００８０】

他のＡＣＲを作成する権限を有するＡＣＲは、これが作成するＡＣＲに遮断解除権限を委譲する権限を有する（しかし、ＡＣＲの遮断を解除する権限がない場合もある）。父ＡＣＲは解除ＡＣＲの参照符を子ＡＣＲの中に入れる。

【００８１】

父ＡＣＲは、自身の子ＡＣＲを削除する権限を有する唯一のＡＣＲである。ＡＣＲが作成した下位ＡＣＲを削除すると、この下位ＡＣＲから生まれたすべてのＡＣＲも自動的に削除される。ＡＣＲを削除すると、そのＡＣＲによって作成された鍵ＩＤとパーティションはすべて削除される。

例外として、ＡＣＲが自身の記録を更新できる場合が２つある。

１．作成元ＡＣＲによって設定されたパスワード／ＰＩＮでも、それらを含むＡＣＲによってのみ更新できる。

２．ルートＡＣＲは自分自身と自身が所属するＡＧＰとを削除できる。

【００８２】

鍵・パーティションアクセス権の委譲

ＡＣＲとそのＡＧＰは階層状のツリーの中で構成され、ルートＡＧＰとその中にあるＡ

ＣＲはツリーの最上部に位置する（例えば、図６のルートＡＧＰ１３０および１３２）。ＳＳＡシステムの中には数本のＡＧＰツリーが存在することがあるが、それらは互いに完全に独立している。ＡＧＰの中にあるＡＣＲは、自身の鍵に対するアクセス権限を、同じＡＧＰの中にある全ＡＣＲとそれらによって作成されるこの全ＡＣＲに委譲できる。鍵を作成する権限は、好ましくはその鍵を使用するためのアクセス権限を委譲する権限を含む。

【００８３】

鍵に対する権限は３種類に分かれる。

１．アクセス：鍵に対するアクセス権限、すなわち読み出しと書き込みとを設定する。

２．所有：当然ながら、鍵の所有者はその鍵を作成したＡＣＲである。この所有権は、ある１つのＡＣＲから別のＡＣＲ（同じＡＧＰの中にあるか、あるいは子ＡＧＰの中にあるＡＣＲ）へ委譲できる。鍵の所有権は、鍵を削除する権限のほかに、鍵に対する権限を委譲する権限を提供する。

３．アクセス権委譲：この権限により、ＡＣＲは自身が保持する権利を委譲できる。

ＡＣＲは、自身が作成したパーティションのほかに、自身が所有するアクセス権限の対象となる他のパーティションに対するアクセス権限を委譲できる。

権限を委譲するには、パーティションの名前と鍵ＩＤを指定されたＡＣＲのＰＣＲに追加する。鍵のアクセス権限を委譲するには、鍵ＩＤを使っても、あるいは委譲する側のＡＣＲのすべての作成された鍵がアクセス権限の対象となってもよいことを表明する。

【００８４】

ＡＣＲの遮断と解除

システムによる事業体のＡＣＲ認証プロセスが失敗すると、ＡＣＲの遮断カウンタが増加する場合がある。一定の最大失敗認証数（ＭＡＸ）に達すると、ＳＳＡシステムによってＡＣＲは遮断されることになる。

遮断されたＡＣＲは、この遮断されたＡＣＲから参照する別のＡＣＲによって解除できる。この解除されたＡＣＲに対する参照は、その作成元にたるＡＣＲによって設定される。解除されたＡＣＲは、好ましくは遮断されたＡＣＲの作成元と同じＡＧＰの中にあり、「解除」権限を有する。

システムの中でこれ以外のＡＣＲは遮断されたＡＣＲを解除できない。遮断カウンタがあるＡＣＲでも解除ＡＣＲがなければ、遮断された場合に解除できない。

【００８５】

ルートＡＧＰ－アプリケーションデータベースの作成

ＳＳＡシステムは複数のアプリケーションを処理し、各アプリケーションのデータを分離するように設計されている。アプリケーションデータを識別し、かつ分離する場合にはＡＧＰシステムのツリー構造がメインのツールとして用いられる。ルートＡＧＰはアプリケーションＳＳＡデータベースツリーの先端に位置し、いくぶん異なる挙動ルールに準拠する。ＳＳＡシステムでは数個のルートＡＧＰを構成できる。図６には２つのルートＡＧＰ１３０および１３２が示されている。当然、これよりも少ないＡＧＰやこれよりも多いＡＧＰが使われる場合があり、本発明の範囲内にある。

新規アプリケーションのための装置（例えば、フラッシュカード）の登録および／または装置の新規アプリケーションの信用証明発行は、装置に新たなＡＧＰ／ＡＣＲツリーを追加する過程で行う。

【００８６】

ＳＳＡシステムはルートＡＧＰ（ならびにルートＡＧＰの全ＡＣＲとその権限）を作成する場合に３通りのモードをサポートする。

１．オープンモード：いずれのユーザまたは事業体でも認証なしで、あるいはシステムＡＣＲ（後述）を通じて認証されたユーザ／事業体が、新規ルートＡＧＰを作成できる。オープンモードによるルートＡＧＰの作成は、セキュリティ対策なしですべてのデータ転送がオープンチャネル（発行機関のセキュア環境内）で行われる場合と、システムＡＣＲ認証（Ｏｖｅｒ　Ｔｈｅ　Ａｉｒ（ＯＴＡ）と後発行手順）を通じて確立するセキュアチ

ャネルを通じて行われる場合とがある。
システムＡＣＲが構成されず（オプションとして）、ルートＡＧＰ作成モードをオープンに設定する場合に選べるオプションはオープンチャネルのみである。
２．制御モード：システムＡＣＲを通じて認証された事業体のみが新規ルートＡＧＰを作成できる。システムＡＣＲが構成されなければ、ＳＳＡシステムをこのモードに設定することはできない。
３．ロックモード：ルートＡＧＰの作成は無効になり、さらなるルートＡＧＰをシステムに加えることはできない。
【００８７】
この機能は２つのＳＳＡコマンドで制御する（これらのコマンドはいずれのユーザ／事業体でも認証なしで使用できる）。
１．方法構成コマンド：３通りのルートＡＧＰ作成モードのいずれか１つを使用する形にＳＳＡシステムを構成するために使用する。オプションから制御へ、制御からロックへのモード変更のみが可能である（つまり、ＳＳＡシステムが現在制御モードに構成されている場合、ロックモードにしか変更できない）。
２．方法構成固定コマンド：方法構成コマンドを無効にし、現在選択されている方法で永続的に固定するために使用する。
【００８８】
作成されたルートＡＧＰは特別な初期化モードに入り、ＡＣＲの作成、構成（ルートＡＧＰの作成に適用されたものと同じアクセス制限を使用）が可能になる。ルートＡＧＰ構成プロセスの最後に事業体がこれを明示的に作動モードに切り替えると、既存のＡＣＲは更新できなくなり、ＡＣＲを追加で作成できなくなる。
【００８９】
標準モードに入ったルートＡＧＰを削除するには、そのＡＣＲのうち、ルートＡＧＰの削除する権限が付与されたＡＣＲを通じてシステムにログインしなければならない。特別の初期化モードのほかに、これもルートＡＧＰの例外である。これは好ましくは、次のツリーレベルにあるＡＧＰではなく自身のＡＧＰを削除する権限を有するＡＣＲを含んでもよい唯一のＡＧＰである。
ルートＡＣＲと標準ＡＣＲとの３番目にして最後の違いは、パーティションを作成し削除する権限を有し得るシステム内で唯一のＡＣＲであるということである。
【００９０】
ＳＳＡシステムＡＣＲ
システムＡＣＲは次に記す２つのＳＳＡ操作に使用される。
１．不利な状況の中でセキュアチャネルの保護下でＡＣＲ／ＡＧＰツリーを作成する。
２．ＳＳＡシステムをホストする装置を識別し、認証する。
好ましくはＳＳＡの中でシステムＡＣＲは１つのみであってもよく、いったん設定されたシステムＡＣＲは好ましくは変更できない。システムＡＣＲを作成するときにシステム認証は必要なく、必要なものはＳＳＡコマンドのみである。システムＡＣＲ作成機能は無効にできる（ルートＡＧＰ作成機能と同様）。好ましくは１つのみのシステムＡＣＲが認められるため、システムＡＣＲ作成コマンドはシステムＡＣＲの作成後には作用しない。
【００９１】
システムＡＣＲはその作成プロセスでは機能しない。作成が完了したら、システムＡＣＲが作成され準備が整ったことを伝える専用のコマンドを発行する必要がある。好ましくはこの時点でシステムＡＣＲの更新や差し替えは行えない。
【００９２】
システムＡＣＲはＳＳＡでルートＡＣＲ／ＡＧＰを作成する。システムＡＣＲは、ホストがルートレベルに満足し遮断するまでルートレベルを追加／変更する権限を有する。ルートＡＧＰを遮断すると、基本的にはシステムＡＣＲとのつながりは絶たれ、改竄不能となる。この時点でルートＡＧＰとその中にあるＡＣＲは誰も変更／編集できない。これはＳＳＡコマンドで果たす。ルートＡＧＰ作成を無効にする作用は永続し、元に戻すことは

できない。図７には、システムＡＣＲが関わる前述した機能が示されている。システムＡＣＲを使って３通りのルートＡＧＰが作成されている。図７でシステムＡＣＲをルートＡＧＰに結ぶ点線で示すように、これらのルートＡＧＰが作成された後のある時点で、システムＡＣＲからルートＡＧＰを遮るＳＳＡコマンドがホストから送信され、ルートＡＧＰ作成機能は無効になる。これで３つのルートＡＧＰは改竄不能となる。ルートＡＧＰが遮断される前か後に、３つのルートＡＧＰを使って子ＡＧＰを作ることにより、３つの別々のツリーが形成されている。

【００９３】

前述した機能は、コンテンツの所有者がコンテンツを使ってセキュア製品を構成する場合に優れた柔軟性を提供する。セキュア製品は「発行」する必要がある。発行とは、装置がホストを識別しホストが装置を識別するための識別鍵を出すプロセスである。ホストは装置（例えば、フラッシュカード）を識別することにより、これの秘密を信用できるかどうかを判断できる。一方、装置はホストを識別することにより、ホストが可能な範囲でのみセキュリティ方針を実施することができる（特定のホストコマンドを許諾し実行する）。

【００９４】

複数のアプリケーションに対応するように設計された製品は、様々な識別鍵を有することになる。製品は「前発行」するか（出荷に先立つ製造中に鍵を記憶する）、あるいは「後発行」する（出荷後に新たな鍵を追加する）。後発行の場合、ある種の親鍵または装置レベル鍵をメモリ装置（例えば、メモリカード）に入れる必要があり、この鍵は、装置へのアプリケーションの追加が許される事業体を識別するために使われる。

【００９５】

前述した機能により後発行を有効／無効にするように製品を構成できる。加えて、後発行構成は出荷の後に安全に果たすことができる。装置は、前述した親鍵または装置レベル鍵のほかには鍵のない状態で小売製品として購入され、新たな所有者により、さらなる後発行アプリケーションを有効または無効にするように構成できる。

【００９６】

このようにシステムＡＣＲ機能は前述した目的を達成するための能力を提供する。

・システムＡＣＲがないメモリ装置の場合はアプリケーションを自由に無制限に追加できることになる。

・システムＡＣＲがないメモリ装置はシステムＡＣＲの作成を無効にするように構成でき、これは新規アプリケーションの追加を制御できないことを意味する（新規ルートＡＧＰ作成機能も無効にする場合を除く）。

・システムＡＣＲがあるメモリ装置の場合はシステムＡＣＲ信用証明を使った認証手続きで確立されるセキュアチャネル経由でアプリケーションを追加できる。

・システムＡＣＲがあるメモリ装置は、アプリケーションが追加される前か、あるいは追加された後にアプリケーション追加機能を無効にするように構成できる。

【００９７】

鍵ＩＤリスト

鍵ＩＤは具体的なＡＣＲ要求に従って作成されるが、メモリシステム１０でこれを使用するのはＳＳＡシステムのみである。鍵ＩＤの作成時に作成元ＡＣＲから提供されるか、あるいは作成元ＡＣＲへ提供されるデータは次のとおりである。

１．鍵ＩＤ：このＩＤはホストを通じて事業体から提供され、以降の読み出しアクセスや書き込みアクセスで、鍵と、その鍵を使って暗号化または暗号化されるデータとを参照するために使われる。

２．鍵暗号およびデータ保全モード（後述する前述したブロック、連鎖、およびハッシュモード）

【００９８】

ホストから提供される属性に加えて、ＳＳＡシステムは次のデータを管理する。

１．鍵ＩＤの所有者：所有者にあたるＡＣＲのＩＤ。作成された鍵ＩＤの所有者は作成

元ＡＣＲである。しかし、鍵ＩＤの所有権は別のＡＣＲに譲渡できる。好ましくは、鍵ＩＤの所有権を譲渡し、かつ鍵ＩＤを委譲できるものは鍵ＩＤの所有者のみである。鍵のアクセス権限の委譲とこれらの権利の失効を行えるのは鍵ＩＤの所有者か、または委譲権限を有するその他のＡＣＲである。ＳＳＡシステムは、これらの操作のいずれかが試みられるときに、操作を要求するＡＣＲにその権限が付与されている場合に限り操作を許諾することになる。

２．ＣＥＫ：このＣＥＫの鍵値は、鍵ＩＤが割り振られたコンテンツまたは鍵ＩＤによって指示されるコンテンツの暗号化に使われる。鍵値は、ＳＳＡシステムによって生成される１２８ビットＡＥＳランダム鍵であってもよい。

３．ＭＡＣおよびＩＶ値：連鎖ブロック暗号（ＣＢＣ）符号化アルゴリズムで使われる動的情報（メッセージ認証コードと開始ベクトル）。

【００９９】

図８Ａ～図１６のフローチャートを参照しながらＳＳＡの様々な機能を例示するが、これらの図でステップの左側に記された「Ｈ」はホストによって実行される操作を意味し、「Ｃ」はカードによって実行される操作を意味する。メモリカードを参照しながらＳＳＡ機能を例示するが、物理的形態が異なるメモリ装置にもこれらの機能が当てはまることが理解できる。システムＡＣＲを作成するため、ホストはメモリ装置１０のＳＳＡに向けてシステムＡＣＲ作成コマンドを発行する（ブロック２０２）。装置１０はこれに応じてシステムＡＣＲが既に存在するかどうかをチェックする（ブロック２０４、菱形２０６）。装置１０はこれが既に存在する場合に失敗ステータスを返し、停止する（長円形２０８）。メモリ１０はこれが既に存在しない場合にシステムＡＣＲの作成が許可されるかどうかをチェックし（菱形２１０）、許可されない場合は失敗ステータスを返す（ブロック２１２）。従って、例えば、必要なセキュリティ機能が事前に決まるので、システムＡＣＲが必要とされない場合等、装置発行者がシステムＡＣＲの作成を許可しない場合もある。許可される場合、装置１０はＯＫステータスを返し、ホストからシステムＡＣＲ信用証明が届くのを待つ（ブロック２１４）。ホストはＳＳＡステータスをチェックし、システムＡＣＲの作成が許可されていることを装置１０が伝えているかどうかをチェックする（ブロック２１６と菱形２１８）。作成が許可されないか、あるいはシステムＡＣＲが既に存在する場合、ホストは停止する（長円形２２０）。システムＡＣＲの作成が許可されていることを装置１０が伝える場合、ホストはそのログイン信用証明を設定するＳＳＡコマンドを発行し、装置１０へ送信する（ブロック２２２）。装置１０は受信した信用証明でシステムＡＣＲ記録を更新し、ＯＫステータスを返す（ブロック２２４）。ホストはこのステータス信号に応じて、システムＡＣＲの準備が整っていることを示すＳＳＡコマンドを発行する（ブロック２２６）。これに応じて装置１０はシステムＡＣＲをロックするので、システムＡＣＲの更新や差し替えはできなくなる（ブロック２２８）。これによりシステムＡＣＲの機能と、ホストに対して装置１０を識別するためのアイデンティティとが固定される。

【０１００】

新規ツリー（新規ルートＡＧＰおよびＡＣＲ）の作成手順は、それらの機能が装置でどのように構成されているかによって決まる。図９は、その手順を説明するものである。ホスト２４とメモリシステム１０はいずれもこの手順をたどる。新規ルートＡＧＰの追加が完全に無効になっている場合、新規ルートＡＧＰは追加できない（菱形２４６）。これが有効になっているが、システムＡＣＲが要求される場合、ホストはルートＡＧＰ作成コマンドの発行（ブロック２５４）に先立ちシステムＡＣＲを通じて認証し、セキュアチャネルを確立する（菱形２５０、ブロック２５２）。システムＡＣＲが要求されない場合（菱形２４８）、ホスト２４は認証なしでルートＡＧＰ作成コマンドを発行でき、ブロック２５４へ進む。ホストは、システムＡＣＲが存在する場合、たとえこれが要求されない場合でも、これを使用することがある（フローチャートには示されていない）。装置（例えば、フラッシュカード）は、新規ルートＡＧＰ作成機能が無効になっている場合に新規ルートＡＧＰを作成する試みを拒否し、システムＡＣＲが要求される場合に認証なしで新規ル

ートＡＧＰを作成する試みを拒否する（菱形２４６および２５０）。ブロック２５４で新たに作成されるＡＧＰとＡＣＲは作動モードに切り替わるので、そのＡＧＰの中にあるＡＣＲの更新や変更はできなくなり、ＡＧＰへＡＣＲを追加することもできなくなる（ブロック２５６）。ここでオプションとしてシステムはロックされるので、ルートＡＧＰは追加で作成できなくなる（ブロック２５８）。点線の枠２５８は、このステップがオプションのステップであることを示す表記法である。本願の図のフローチャートにて点線で示された枠はいずれもオプションのステップである。このように、コンテンツの所有者は正当なコンテンツを含む本物のメモリ装置を装う違法な目的に装置１０を利用できないようにすることができる。

【０１０１】

ＡＣＲ（前述したルートＡＧＰの中にあるＡＣＲとは別のＡＣＲ）を作成するには、図１０に示すように、ＡＣＲを作成する権利を有するＡＣＲから開始できる（ブロック２７０）。ホスト２４を通じて入ることを試みる事業体は、入口にあたるＡＣＲのアイデンティティと作成したいがための必要となる属性のすべてを含むＡＣＲとを提供する（ブロック２７２）。ＳＳＡはＡＣＲアイデンティティの一致をチェックし、さらにそのアイデンティティを有するＡＣＲにＡＣＲを作成する権限があるかどうかをチェックする（菱形２７４）。要求が証明される場合、装置１０のＳＳＡはＡＣＲを作成する（ブロック２７６）。

【０１０２】

図１１の２つのＡＧＰは、図１０の方法を使用するセキュリティアプリケーションで役に立つツリーを例示するものである。従って、マーケティングＡＧＰの中でアイデンティティｍ１を有するＡＣＲには、ＡＣＲを作成する権限がある。ＡＣＲ　ｍ１は、鍵ＩＤ「マーケティング情報」と関連付けられたデータと鍵ＩＤ「価格リスト」と関連付けられたデータを鍵を使って読み書きする権限も有する。これにより、図１０の方法を用いて２つのＡＣＲ　ｓ１およびｓ２を含む販売ＡＧＰを作成する。ＡＣＲ　ｓ１およびｓ２には鍵ＩＤ「価格リスト」と関連付けられた価格データにアクセスするための鍵の読み出し権限のみあるが、鍵ＩＤ「マーケティング情報」と関連付けられたデータにアクセスする場合に必要となる鍵の権限はない。このように、ＡＣＲ　ｓ１およびｓ２を有する事業体は、価格データを読み出されてもこれを変更することはできず、さらにマーケティングデータにはアクセスできない。一方、ＡＣＲ　ｍ２にはＡＣＲを作成する権限がなく、鍵ＩＤ「価格リスト」と鍵ＩＤ「マーケティング情報」と関連付けられたデータにアクセスするための鍵の読み出し権限のみを有する。

【０１０３】

従って、アクセス権は前述したやり方で委譲でき、ｍ１は価格データを読み出す権利をｓ１およびｓ２に委譲する。これは特に大規模なマーケティング組織や販売組織が関わる場合に有用である。しかし、販売員が１名～少数であれば図１０の方法を使う必要はない場合がある。代わりに、図１２に示すように、ＡＣＲから同じＡＧＰの下位レベルまたは同じレベルに位置するＡＣＲにアクセス権を委譲できる。事業体はまず、そのＡＧＰのツリーに入るため、ホストを通じてツリーの中のＡＣＲを前述したように指定する（ブロック２８０）。次に、ホストはＡＣＲと委譲する権利を指定する。ＳＳＡはツリーでこのＡＣＲをチェックし、指定された別のＡＣＲに権利を委譲する権限がこのＡＣＲにあるかどうかをチェックする（菱形２８２）。権限があるなら権利は委譲され（ブロック２８４）、そうでないなら停止する。図１３はその結果を示す。この場合、ＡＣＲ　ｍ１には読み出し権限をＡＣＲ　ｓ１に委譲する権限があるため、委譲の後、ｓ１は鍵を使って価格データにアクセスできるようになる。これは、ｍ１が価格データにアクセスするための権利またはそれ以上の権利を有し、さらにそれを委譲する権限を有する場合に果たすことができる。ｍ１は、一実施形態において、委譲の後にそのアクセス権を保持する。好ましくは、時間やアクセス数を制限するなどにより（永続的にではなく）一定の条件のもとでアクセス権を委譲する。

【０１０４】

図１４は、鍵と鍵ＩＤを作成するプロセスを示す。事業体はＡＣＲを通じて認証を受ける（ブロック３０２）。事業体は、ホストによって指定されたＩＤによる鍵の作成を要求する（ブロック３０４）。ＳＳＡは、指定されたＡＣＲにその権限があるかどうかをチェックする（菱形３０６）。例えば、ある特定のパーティションにあるデータにアクセスするために鍵が使われる場合、ＳＳＡはそのパーティションにＡＣＲがアクセスできるかどうかをチェックすることになる。ＡＣＲにその権限がある場合、メモリ装置１０はホストから提供された鍵ＩＤと関連付けられた鍵値を作成し（ブロック３０８）、鍵ＩＤをＡＣＲに記憶し、鍵値をメモリ（コントローラ関連メモリまたはメモリ２０のいずれか）に記憶し、事業体から提供された情報に従って権利と権限を付与し（ブロック３１０）、付与された権利および権限で該当するＡＣＲのＰＣＲを修正する（ブロック３１２）。従って、読み出しおよび書き込み権限、同じＡＧＰの中にある他のＡＣＲまたは下位レベルのＡＣＲに委譲し共有する権利、鍵の所有権を譲渡する権利等、鍵の作成元はすべての権利を有する。

【０１０５】

図１５に示すように、ＡＣＲはＳＳＡシステムの中にある別のＡＣＲの権限（またはＡＣＲの存在そのもの）を変更できる。事業体はこれまでどおりＡＣＲを通じてツリーに入る場合がある。この場合は事業体の認証が行われ、事業体はＡＣＲを指定する（ブロック３３０、３３２）。事業体はターゲットＡＣＲの削除またはターゲットＡＣＲの権限の削除を要求する（ブロック３３４）。指定されたＡＣＲまたはその時点でアクティブなＡＣＲにその権利があるなら（菱形３３６）、ターゲットＡＣＲを削除し、あるいはそのような権限を削除するためにターゲットＡＣＲのＰＣＲを変更する（ブロック３３８）。これが認可されない場合、システムは停止する。

【０１０６】

前述したプロセスの後、ターゲットはプロセスの前にアクセスできたデータにアクセスできなくなる。図１６に示すように、かつて存在したＡＣＲ　ＩＤはもはやＳＳＡに存在しないため、ターゲットＡＣＲに入ることを試みる事業体は認証プロセスの失敗に気づくので、アクセス権は拒否される場合がある（菱形３５２）。ＡＣＲ　ＩＤが削除されていないと仮定した場合、事業体はＡＣＲを指定し（ブロック３５４）、鍵ＩＤおよび／または特定のパーティションのデータを指定し（ブロック３５６）、ＳＳＡはそのようなＡＣＲのＰＣＲに従って鍵ＩＤまたはパーティションアクセス要求が許可されるかどうかをチェックする（菱形３５８）。権限が削除されているか、あるいは失効している場合、要求は再度却下される。そうでない場合、要求は許諾される（ブロック３６０）。

前述したプロセスは、ＡＣＲとそのＰＣＲが別のＡＣＲによって変更された場合であれ、あるいは初めからそのように構成されていた場合であれ、被保護データに対するアクセスが装置（例えば、フラッシュカード）によってどのように管理されるかを説明するものである。

【０１０７】

セッション

ＳＳＡシステムは、同時にログインする複数のユーザを処理するように設計されている。この機能を使用する場合、ＳＳＡによって受信されるコマンドには特定の事業体が対応し、コマンドは、この事業体の認証に用いるＡＣＲに要求された動作を行う権限がある場合に限り実行される。

【０１０８】

複数の事業体はセッションのコンセプトによってサポートされる。セッションは認証プロセスで確立し、ＳＳＡシステムによってセッションｉｄが割り当てられる。セッションｉｄはシステムへのログインに使われたＡＣＲに内部で関連付けられ、事業体へエクスポートされ、それ以降のＳＳＡコマンドで使われる。

【０１０９】

ＳＳＡシステムは、２通りのセッション、すなわちオープンセッションとセキュアセッションとをサポートする。認証プロセスと関連付けられたセッションのタイプはＡＣＲの

中で設定される。ＳＳＡシステムは、認証の施行と同様のやり方でセッション確立を施行する。事業体の権限はＡＣＲで設定されるため、システム設計者は特定の鍵ＩＤに対するアクセスまたは特定のＡＣＲ管理操作（新規ＡＣＲの作成、信用証明の設定等）の実行にセキュアトンネルを関連付けることができる。

【０１１０】

オープンセッション

オープンセッションはセッションｉｄで識別されるセッションであるが、バス暗号化は行われないため、コマンドとデータはいずれも暗号化されずに引き渡される。この動作モードは、好ましくは事業体が脅威モデルに該当せずバス上で傍受を行わない多数のユーザまたは多数の事業体環境に使用される。

【０１１１】

オープンセッションモードではデータ送信が保護されず、ホスト側のアプリケーション間に効率的なファイアウォールは実施されないが、ＳＳＡシステムが認証済みのＡＣＲでアクセスできる情報のみにアクセスを許すことができる。

【０１１２】

オープンセッションはパーティションまたは鍵を保護する必要がある場合にも使用できる。しかし、有効な認証プロセスの後にはホスト側のすべての事業体にアクセスが許諾される。ホストアプリケーションはセッションｉｄさえあれば認証済みＡＣＲの権限を得ることができる。これは図１７Ａに例示されている。線４００より上のステップはホスト２４によって実行されるステップである。ＡＣＲ１の認証（ブロック４０２）を終えた事業体は、メモリ装置１０で鍵ＩＤ　Ｘと関連付けられたファイルへのアクセスを要求する（ブロック４０４、４０６、および４０８）。ＡＣＲ１のＰＣＲがこのアクセスを認める場合、装置１０は要求を許諾する（菱形４１０）。そうでない場合、システムはブロック４０２まで戻る。認証が完了した後、メモリシステム１０はコマンドを発行する事業体を（ＡＣＲ信用証明ではなく）割り当てられたセッションｉｄのみで識別する。オープンセッションでいったんＡＣＲ１がＰＣＲの鍵ＩＤと関連付けられたデータに到達すると、他のどのアプリケーションまたはユーザでも、ホスト２４上の様々なアプリケーションによって共有される正しいセッションｉｄを指定することによって同じデータにアクセスできる。この機能は、一度のみログインし、様々なアプリケーションに対してログインに使われたアカウントに結合されたすべてのデータにアクセスできることがユーザにとって好都合な場合のアプリケーションに有利である。携帯電話機のユーザの場合、記憶されたｅメールにアクセスし、ログインを繰り返すことなくメモリ２０に記憶された音楽を聞くことができる。一方、ＡＣＲ１に該当しないデータにはアクセスできないことになる。このため、ゲームや写真等の同じ携帯電話機のユーザにとって貴重となり得るコンテンツは、別のアカウントＡＣＲ２を通じてアクセスされる。これは、携帯電話機のユーザの電話機を借りる人にアクセスさせたくないデータであるが、携帯電話機のユーザにとって、最初のアカウントＡＣＲ１でアクセスできるデータなら他人がアクセスしてもよい。データへのアクセスを２つの別々のアカウントに分け、ＡＣＲ１へのアクセスをオープンセッションで行うことにより、使い易くなるばかりでなく貴重なデータを保護できる。

【０１１３】

ホストアプリケーション間でのセッションｉｄの共有をさらに簡単にするには、オープンセッションを要求するＡＣＲが、セッションに「０（ゼロ）」ｉｄを割り当てることを具体的に要求する。このように、アプリケーションは所定のセッションｉｄを使用するように設計できる。当然ながら、セッション０を要求するＡＣＲは一度に１つしか認証できない。セッション０を要求する別のＡＣＲを認証する試みは拒否されることになる。

【０１１４】

セキュアセッション

セキュリティ層を追加するため、セッションｉｄは図１７Ｂに示すように使ってもよい。この場合はメモリ１０もアクティブセッションのセッションｉｄを記憶する。図１７Ｂで、例えば鍵ＩＤ　Ｘと関連付けられたファイルにアクセスするには、事業体もセッショ

ンｉｄ、例えばセッションｉｄ「Ａ」を提供する必要があり、その上でファイルへのアクセスが許可されることになる（ブロック４０４、４０６、４１２、および４１４）。このように、要求する事業体は正しいセッションｉｄを知らない限りメモリ１０にアクセスできない。セッションｉｄはセッションが終わった後に削除され、セッションのたびに異なるため、事業体はセッション番号を提供できた場合に限りアクセスできる。

【０１１５】

ＳＳＡシステムは、コマンドが実際に正しい認証済み事業体から届いているかどうかを、セッション番号を使って追跡する。攻撃者がオープンチャネルを使って悪質なコマンドの送信を試みるおそれがある用途や使用がある場合、ホストアプリケーションはセキュアセッション（セキュアチャネル）を使用する。

セキュアチャネルを使用する場合、セッションｉｄとコマンド全体がセキュアチャネル暗号化（セッション）鍵を使って暗号化され、そのセキュリティ水準はホスト側の実施例と同じくらい高くなる。

【０１１６】

セッションの終了

セッションは次に記すシナリオのいずれか１つで終了し、ＡＣＲはログオフされる。

１．事業体が明示的なセッション終了コマンドを発行する。

２．通信タイムアウトが発生する。ある特定の事業体がＡＣＲパラメータの一パラメータとして設定された期間にわたってコマンドを発行しなかった。

３．装置（例えば、フラッシュカード）のリセットおよび／またはパワーサイクルの後にはすべてのオープンセッションが終了する。

【０１１７】

データ保全サービス

ＳＳＡシステムは、ＳＳＡデータベース（ＡＣＲ、ＰＣＲ等を収容）が完全な状態に保たれていることをベリファイする。このほかに、鍵ＩＤ機構による事業体データのデータ保全サービスも提供される。

鍵ＩＤの暗号化アルゴリズムがハッシュモードに設定される場合、ＣＥＫおよびＩＶと併せてハッシュ値がＣＥＫ記録に記憶される。書き込み操作中にはハッシュ値の計算と記憶が行われる。読み出し操作のときにも再度ハッシュ値を計算し、前の書き込み操作中に記憶された値と比較する。事業体が鍵ＩＤにアクセスするたびに追加のデータが古いデータに（暗号的に）連結され、該当するハッシュ値（読み出しまたは書き込みのため）が更新される。

【０１１８】

鍵ＩＤと関連付けられた、または鍵ＩＤによって指示される、データファイルを知るのはホストのみであるため、データ保全機能の各態様はホストが明示的に次のように管理する。

１．鍵ＩＤと関連付けられた、または鍵ＩＤによって指示される、データファイルは最初から最後まで書き込まれるか、または読み出される。ＳＳＡシステムはＣＢＣ暗号方式を使用し、データ全体のハッシュ化メッセージダイジェストを生成するため、ファイルの一部分にアクセスする試みによってファイルは混乱することになる。

２．中間ハッシュ値はＳＳＡシステムによって管理されるため、連続するストリームの中でデータを処理する必要はない（このデータストリームは他の鍵ＩＤのデータストリームでインターリーブでき、複数のセッションにわたって分割できる）。しかし、事業体は、データストリームが再度始まる場合にハッシュ値のリセットをシステムに明示的に指示する必要がある。

３．ホストは読み出し操作が完了すると、読み出されたハッシュを書き込み操作中に計算したハッシュ値と比較することによって有効にすることをＳＳＡシステムに明示的に要求する。

４．ＳＳＡシステムは「ダミー読み出し」操作も提供する。この機能によりデータは暗号化エンジンを通過するが、ホストには送出されないことになる。この機能を利用すれば

、データが実際に装置（例えば、フラッシュカード）から読み出される前に、データが完全な状態に保たれていることをベリファイすることができる。

【０１１９】

乱数生成

外部事業体はＳＳＡシステムの内部乱数生成器を利用でき、乱数はＳＳＡシステムの外で使用できる。このサービスはいずれのホストでも利用でき、認証は必要ない。

【０１２０】

ＲＳＡ鍵対生成

外部ユーザはＳＳＡシステムの内部ＲＳＡ鍵対生成機能を利用でき、鍵対はＳＳＡシステムの外で使用できる。このサービスはいずれのホストでも利用でき、認証は必要ない。

【０１２１】

代替の実施形態

階層アプローチを使う代わりに、図１８に示すデータベースアプローチを使って同様の結果を達成できる。

図１８に示すように、コントローラ１２またはメモリ２０に記憶されたデータベースに入力された事業体の信用証明リスト、認証方法、最大失敗数、遮断解除に必要な最小信用証明数等は、メモリ１０のコントローラ１２によって実行されるデータベース内の方針（鍵・パーティションに対する読み出し、書き込みアクセス、セキュアチャネル要件）に結び付いている。鍵・パーティションアクセスに対する制約事項や制限事項もデータベースに記憶される。ホワイトリストにある可能性がある事業体（例えば、システム管理者）はすべての鍵とパーティションにアクセスできる。ブラックリストにある可能性がある事業体による情報アクセスの試みは阻止される。制限は全域におよぶ場合と鍵および／またはパーティションごとに適用される場合とがある。これは、特定の事業体のみが特定の鍵・パーティションにアクセスでき、特定の事業体はアクセスできないことを意味する。コンテンツのパーティションや、コンテンツの暗号化または復号化に使う鍵にかかわりなく、コンテンツ自体に制約を課すこともできる。したがって、データ（例えば、歌）にアクセスする可能性がある最初の５ホスト装置のみにアクセスを許可したり、あるいはデータ（例えば、映画）にアクセスしたりする事業体は問わず、データの読み出し回数を制限することができる。

認証

パスワード保護

・パスワード保護は、被保護領域へアクセスする場合にパスワードの提示が求められることを意味する。パスワードが１つに限られる場合を除き、それぞれのパスワードには読み出しアクセスや読み出し／書き込みアクセス等、別々の権利を割り振ることができる。

・パスワード保護は、ホストから提供されるパスワードを装置（例えば、フラッシュカード）がベリファイできること、すなわち装置もまた装置によって管理され保護されたメモリ領域にパスワードを記憶することを意味する。

問題と限界

・パスワードはリプレー攻撃を被ることがある。提示のたびに変わらないパスワードは同じ状態で再送できる。つまり、保護の対象となるデータが貴重で、通信バスへのアクセスが容易い場合、パスワードを現状のまま使用するべきではない。

・パスワードによって記憶データへのアクセスは保護できるが、（鍵ではなく）データの保護のためにパスワードを使用するべきではない。

・パスワードに関わるセキュリティ水準を上げるため、親鍵を使ってパスワードを多様化すれば、１つのパスワードがハッキングされてもシステム全体が破られることはない。パスワードの送信にはセッション鍵方式のセキュア通信チャネルを使用できる。

【０１２２】

図１９は、パスワードを使った認証を示すフローチャートである。事業体はアカウントｉｄとパスワードをシステム１０（例えば、フラッシュメモリカード）へ送信する。システムは、パスワードが自身のメモリにあるパスワードに一致するかどうかをチェックする

。一致する場合は認証済みステータスを返す。そうでない場合はそのアカウントのエラーカウンタが増加し、事業体にはアカウントｉｄとパスワードの再入力が求められる。システムはカウンタが一杯になるとアクセス拒否ステータスを返す。

【０１２３】

対称鍵

対称鍵アルゴリズムは、暗号化と復号化の両側で同じ鍵が使われることを意味する。これは、通信に先立ち予め鍵を取り決めておくことを意味する。それぞれの側では相手側の逆のアルゴリズムを実行する。つまり、一方は暗号化アルゴリズムになり、他方は復号化アルゴリズムになる。通信する場合に両側で両方のアルゴリズムを実行する必要はない。

認証

・対称鍵認証は、装置（例えば、フラッシュカード）とホストが同じ鍵を共有し、同じ暗号アルゴリズム（ダイレクトおよびリバース、例えばＤＥＳ、ＤＥＳ－１）を具備することを意味する。

・対称鍵認証は、チャレンジ・レスポンス（リプレー攻撃対策）を意味する。被保護装置が他の装置に対する質問を生成し、両方の装置で回答を計算する。認証を受ける側の装置は回答を送り返し、被保護装置はその回答をチェックして真贋を検査する。そして、認証に応じて権利を付与する。

認証には次のものがある。

・外部認証：装置（例えば、フラッシュカード）が外部を認証する。つまり、装置は特定のホストまたはアプリケーションの信用証明を検査する。

・相互認証：両側で質問を生成する。

・内部認証：ホストアプリケーションが装置（例えば、フラッシュカード）を認証する。つまり、ホストは、装置がそのアプリケーションにとって真正であるかどうかをチェックする。

システム全体のセキュリティ水準を上げるため（１つが破られてもすべてが破られないようにするため）

・対称鍵には通常、親鍵を使った多様化を組み合わせる。

・質問が真正な質問であることを確認するため、相互認証により両側からの質問を使用する。

暗号化

対称鍵暗号法はすこぶる効率的なアルゴリズムで、暗号処理する場合に強力なＣＰＵを必要としないため、暗号化にも使われる。

【０１２４】

通信チャネルを安全に使う場合：

・チャネルの安全を確保する（つまり、全発信データを暗号化し全着信データを復号化する）ために使うセッション鍵を、両方の装置が知らなければならない。このセッション鍵は通常、事前共有秘密対称鍵を使うか、あるいはＰＫＩを使って設定する。

・両方の装置が同じ暗号アルゴリズムを知り、実行しなければならない。

署名

対称鍵を使ってデータに署名することもできる。この場合の署名は暗号化の部分的な結果である。このため、鍵値を露出することなく必要に応じて何度でも署名できる。

【０１２５】

問題と限界

対称アルゴリズムは非常に効率的で安全ではあるが、事前共有秘密を基礎とする。問題は、この秘密を動的に安全に共有することと、（セッション鍵のように）ランダムにすることである。つまり、共有秘密を長期間にわたって安全に保つのは困難であり、多数の人々と共有することはほぼ不可能である。

この作業を促進するために考案されたのが、秘密を共有せずに交換する公開鍵アルゴリズムである。

【０１２６】

非対称認証手続き

非対称鍵に基づく認証では、一連のコマンドを使ってデータを受け渡ししながら、最終的にはセキュアチャネル通信のためのセッション鍵を作る。その基本的プロトコルではＳＳＡシステムに対してユーザを認証する。プロトコルのバリエーションにより、ユーザが使用するＡＣＲをベリファイする相互認証や二因子認証も可能である。

【０１２７】

ＳＳＡの非対称認証プロトコルでは好ましくは、公開鍵基盤（ＰＫＩ）アルゴリズムとＲＳＡアルゴリズムを使用する。これらのアルゴリズムで規定することで、認証プロセスの各当事者に独自のＲＳＡ鍵対を用意することができる。それぞれの対は公開鍵と秘密鍵とからなる。これらの鍵は秘匿の鍵であるためにアイデンティティの証拠を提供することはできない。ＰＫＩ層では信頼された第三者機関が公開鍵に署名する。この信用機関の公開鍵は、互いを認証する当事者間で事前共有され、当事者の公開鍵をベリファイするために使われる。信用が成立すると（両当事者が相手方から提供される公開鍵を信用できると判断したら）、プロトコルによる認証（各当事者が所有する秘密鍵の一致をベリファイする）と鍵の交換が続行する。これは、後述する図２２および２３のチャレンジ・レスポンス機構で果たすことができる。

【０１２８】

署名済みの公開鍵を収容する構造を証明書という。証明書に署名した信用機関を証明機関（ＣＡ）という。認証を受ける側は公開鍵の信憑性を立証する証明書とＲＳＡ鍵対を有する。証明書は、相手方（認証する側）が信用する証明機関によって署名される。認証する側には信用ＣＡの公開鍵の所有が求められる。

【０１２９】

ＳＳＡは証明書連鎖に対応する。これは、識別される側の公開鍵が別のＣＡ、すなわち識別する側が信用するＣＡとは異なるＣＡによって署名されることを意味する。この場合の識別される側は、自分自身の証明書のほかに、その公開鍵に署名したＣＡの証明書を提供する。この第２レベルの証明書さえも相手方によって信用されない（信用ＣＡによって署名されていない）場合、第３レベルの証明書を提供できる。この証明書連鎖アルゴリズムでは、各当事者が公開鍵の認証に必要な証明書の完全なリストを所有する。このことは、図２３および２４に例示されている。この種のＡＣＲによる相互認証に必要な信用証明は、一定の長さを有するＲＳＡ鍵対である。

【０１３０】

ＳＳＡ証明書

ＳＳＡは［Ｘ．５０９］バージョン３デジタル証明書を採用する。［Ｘ．５０９］は汎用規格であり、ここで説明するＳＳＡ証明書プロファイルは証明書の所定フィールドの内容をさらに指定し、制限する。この証明書プロファイルは、証明書連鎖の管理に用いる信頼階層と、ＳＳＡ証明書の検査と、証明書失効リスト（ＣＲＬ）プロファイルも規定する。

証明書は公開情報（内部の公開鍵として）とみなされるため、暗号化されない。しかし、証明書はＲＳＡ署名を含み、このＲＳＡ署名によって公開鍵やその他の情報フィールドが改竄されていないことをベリファイする。

［Ｘ．５０９］はＡＳＮ．１規格を使った各フィールドのフォーマットを定め、ＡＳＮ．１規格はデータ符号化にＤＥＲフォーマットを使用する。

【０１３１】

ＳＳＡ証明書の概要

図２０と図２１とに示されたＳＳＡ証明書管理アーキテクチャの一実施形態は、ホストの無限階層レベルと装置の３階層レベルからなるが、装置で使用する階層レベルは３レベルより多い場合または３レベルより少ない場合がある。

【０１３２】

ホスト証明書階層

装置は、２つの要素、すなわち装置に記憶されたルートＣＡ証明書（ＡＣＲ信用証明と

してＡＣＲの作成時に記憶）と、装置への（その特定のＡＣＲへの）アクセスを試みる事業体から提供される証明書／証明書連鎖とに基づき、ホストを認証する。

【０１３３】

ホスト証明機関は、それぞれのＡＣＲに対してルートＣＡ（ＡＣＲ信用証明の中にある証明書）の役割を果たす。例えば、ある１つのＡＣＲにとってのルートＣＡは「ホスト１ＣＡ（レベル２）証明書」であり、別のＡＣＲにとってのルートＣＡは「ホストルートＣＡ証明書」である。それぞれのＡＣＲに対して、ルートＣＡによって署名された証明書（またはルートＣＡを末端事業体証明書までつなげる証明書連鎖）を保持するすべての事業体が、末端事業体証明書の対応する秘密鍵を有している場合、そのＡＣＲにログインできる。前述したように、証明書は公知であり、秘密にしない。

【０１３４】

ルートＣＡによって発行された証明書（ならびに対応する秘密鍵）の所有者は誰でもそのＡＣＲにログインできるということは、ある特定のＡＣＲに対する認証がそのＡＣＲの信用証明に記憶されたルートＣＡの発行者によって決まることを意味する。換言すると、ルートＣＡの発行者がＡＣＲの認証方式を管理する事業体になる。

【０１３５】

ホストルート証明書

ルート証明書は、ログインを試みる事業体（ホスト）の公開鍵のベリファイを開始するのにＳＳＡが使われるときに使用する信用ＣＡ証明書である。この証明書はＡＣＲの作成時にＡＣＲ信用証明の一部として提供される。これはＰＫＩシステムに対する信用の根元にあたるものであるため、信用された事業体（父ＡＣＲ、または製造／構成信頼環境）から提供されることが前提となる。この証明書をベリファイするＳＳＡは、その公開鍵を使って証明書の署名をベリファイする。ホストルート証明書は暗号化された状態で不揮発性メモリ（図１には示されていない）に記憶され、装置の秘密鍵にアクセスできるものは、好ましくは図１のシステム１０のＣＰＵ１２のみである。

【０１３６】

ホスト証明書連鎖

これらの証明書は認証中にＳＳＡへ提供される。連鎖の処理が完了した後にホストの証明書連鎖を再度集めて装置に記憶することはしない。

【０１３７】

図２０は、多数のホスト証明書連鎖を示す、ホスト証明書レベル階層の概略図である。図２０に示すように、ホスト証明書は多数の証明書連鎖を有することがあり、ここでは３つの証明書連鎖のみが例示されている。

Ａ１．ホストルートＣＡ証明書５０２、ホスト１　ＣＡ（レベル２）証明書５０４、ホスト証明書５０６

Ｂ１．ホストルートＣＡ証明書５０２、ホストｎ　ＣＡ（レベル２）証明書５０８、ホスト１　ＣＡ（レベル３）証明書５１０、ホスト証明書５１２

Ｃ１．ホストルートＣＡ証明書５０２、ホストｎ　ＣＡ（レベル２）証明書５０８、ホスト証明書５１４

【０１３８】

前述した３つの証明書連鎖Ａ１、Ｂ１、およびＣ１は、ホストの公開鍵が真正であることを証明するために使われてもよい３通りのホスト証明書連鎖を例示するものである。図２０と前述した証明書連鎖Ａ１を参照し、ホスト１のＣＡ（レベル２）証明書５０４の公開鍵はホストルートＣＡの秘密鍵によって署名され（すなわち、公開鍵のダイジェストを暗号化）、この公開鍵はホストルートＣＡ証明書５０２にある。したがって、ホストルートＣＡの公開鍵を有する事業体は、前述した証明書連鎖Ａ１の信憑性をベリファイできることになる。この事業体は最初のステップとして、ホストから送信されたホスト１のＣＡ（レベル２）証明書５０４の署名済み公開鍵を、自身が所有するホストルートＣＡの公開鍵を使って復号化し、復号化した署名済み公開鍵を、ホストから送信されたホスト１のＣＡ（レベル２）証明書５０４の署名されていない公開鍵のダイジェストと比較する。２つ

が一致する場合、ホスト１のＣＡ（レベル２）の公開鍵は認証され、事業体は次に、ホストから送信されたホスト証明書５０６の中にあるホスト１のＣＡ（レベル２）の秘密鍵によって署名されたホストの公開鍵を、ホスト１のＣＡ（レベル２）の認証済み公開鍵を用いて復号化することになる。この復号化された署名済みの値が、ホストから送信されたホスト証明書５０６の中にある公開鍵のダイジェストの値に一致する場合、ホストの公開鍵も認証される。証明書連鎖Ｂ１およびＣ１を使った認証も同様に行われる。

【０１３９】

連鎖Ａ１が関わる前述したプロセスから分かるように、ホストから送信され事業体によってベリファイされる最初の公開鍵は、ホストルートＣＡ証明書ではなくホスト１のＣＡ（レベル２）の公開鍵である。このため、ホストが事業体へ送る必要があるものはホスト１のＣＡ（レベル２）証明書５０４とホスト証明書５０６であって、ホスト１のＣＡ（レベル２）証明書は連鎖の中で最初に送信される必要があることになる。前述したように、証明書のベリファイ順序は次のとおりである。ベリファイする側の事業体、すなわちこの場合のメモリ装置１０はまず、連鎖の中で最初の証明書の公開鍵の真性をベリファイし、この場合のものはルートＣＡの下に位置するＣＡの証明書５０４である。この証明書の公開鍵が真正であることをベリファイした後、装置１０は次の証明書のベリファイに進み、この場合のものはホスト証明書５０６である。証明書連鎖が３つ以上の証明書を含む場合のベリファイ順序も同様に、ルート証明書のすぐ下に位置する証明書から始まり、認証の対象となる事業体の証明書で終わる。

【０１４０】

装置証明書階層

ホストは２つの要素、すなわちホストに記憶された装置ルートＣＡと、装置からホストへ提供される（ＡＣＲの作成時に信用証明として装置に提供される）証明書／証明書連鎖とに基づき装置を認証する。ホストによる装置の認証プロセスは、前述した装置によるホスト認証プロセスに類似する。

【０１４１】

装置証明書連鎖

これらの証明書はＡＣＲの鍵対の証明書である。これらの証明書はＡＣＲの作成時にカードに提供される。ＳＳＡはこれらの証明書を個別に記憶し、認証のときにはそれらを１つずつホストに提供する。ＳＳＡはこれらの証明書を使ってホストの認証を受ける。装置は３つの証明書からなる連鎖を処理できるが、証明書数が３以外になる場合がある。証明書の数はＡＣＲによって異なることがある。これはＡＣＲが作成されるときに決まる。装置はホストに向けて証明書連鎖を送信できるが、証明書連鎖データを使用するわけではないので、証明書連鎖を解析する必要はない。

【０１４２】

図２１は、ＳＳＡを使用する記憶装置等の装置で１～ｎ通りの証明書連鎖を示す、装置証明書レベル階層の概略図である。図２１に示されたｎ通りの証明書連鎖は次のとおりである。

Ａ２．装置ルートＣＡ証明書５２０、装置１　ＣＡ（製造業者）証明書５２２、
　　装置証明書５２４

Ｂ２．装置ルートＣＡ証明書５２０、装置ｎ　ＣＡ（製造業者）証明書５２６、
　　装置証明書５２８

【０１４３】

ＳＳＡ装置は、それぞれ独自の装置ＣＡ証明書を有する１～ｎ通りの製造業者によって製造される。したがって、ある特定の装置の装置証明書の公開鍵はその異なる製造業者の秘密鍵によって署名され、製造業者の公開鍵は装置ルートＣＡの秘密鍵によって署名される。装置の公開鍵をベリファイする方法は、前述したホストの公開鍵の場合の方法に類似する。ホストについて前述した連鎖Ａ１のベリファイの場合と同様に、装置ルートＣＡ証明書を送る必要はなく、連鎖の中で送信すべき最初の証明書は装置ｉ　ＣＡ（製造業者）証明書であって、その後に装置証明書が続き、ｉは１～ｎの整数である。

【０１４４】
図２１に示す実施形態において、装置は２つの証明書、つまり装置ｉ　ＣＡ（製造業者）証明書と、その後に自身の装置証明書とを送信する。装置ｉ　ＣＡ（製造業者）証明書は、このような装置を製造し、装置の公開鍵に署名するための秘密鍵を提供する製造業者の証明書である。装置ｉ　ＣＡ（製造業者）証明書を受信したホストは、自身が所有するルートＣＡの公開鍵を使って装置ｉ　ＣＡ（製造業者）公開鍵を復号化し、ベリファイする。ホストはこのベリファイに失敗した場合、プロセスを中断し、認証が失敗したことを装置に伝える。ホストが認証に成功した場合、次の証明書を求める要求を装置へ送信する。そして、装置は自身の装置証明書を送信し、ホストはこれを同様にベリファイする。
【０１４５】
図２２および図２３は、前述したベリファイプロセスをさらに詳しく示すものである。図２２の「ＳＳＭシステム」は、本願明細書で説明するＳＳＡシステムと後述するその他の機能とを実行するソフトウェアモジュールである。ＳＳＭはソフトウェアまたはコンピュータコードとして具現化でき、メモリ２０またはＣＰＵ１２の不揮発性メモリ（図示せず）にデータベースを記憶し、ＲＡＭ　１２ａに読み込まれてＣＰＵ　１２によって実行される。
【０１４６】
図２２に示すように、装置１０のＳＳＭシステム５４２がホストシステム５４０を認証するプロセスには３つの段階がある。最初の公開鍵ベリファイ段階では、ホストシステム５４０がＳＳＭコマンドでホスト証明書連鎖をＳＳＭシステム５４２へ送信する。ＳＳＭシステム５４２は、ホスト証明書５４４の真性とホスト公開鍵５４６の真性を、ＡＣＲ５５０のホストルート証明書５４８にあるルート証明機関公開鍵を用いてベリファイする（ブロック５５２）。ルート証明機関とホストの間に中間証明機関が介在する場合、中間証明書５４９もブロック５５２のベリファイに使われる。ベリファイまたはプロセス（ブロック５５２）が成功したと仮定し、ＳＳＭシステム５４２は第２段階へ進む。
【０１４７】
ＳＳＭシステム５４２は乱数５５４を生成し、これを質問としてホストシステム５４０へ送信する。システム５４０はホストシステムの秘密鍵５４７を使って乱数５５４に署名し（ブロック５５６）、質問に対する回答として署名済みの乱数を送信する。その回答はホスト公開鍵５４６を使って復号化され（ブロック５５８）、乱数５５４と比較される（ブロック５６０）。復号化された回答が乱数５５４に一致したと仮定すると、チャレンジ・レスポンスは成功である。
【０１４８】
第３段階ではホスト公開鍵５４６を使って乱数５６２を暗号化する。この乱数５６２がセッション鍵となる。ホストシステム５４０は、ＳＳＭシステム５４２からの暗号化数５６２を秘密鍵を使って復号化（ブロック５６４）することによってセッション鍵を得ることができる。このセッション鍵により、ホストシステム５４０とＳＳＭシステム５４２との間でセキュア通信を開始できる。図２２に示す一方向非対称認証では、装置１０のＳＳＭシステム５４２によってホストシステム５４０が認証される。図２３は、図２２の一方向認証プロトコルに類似する双方向相互認証プロセスを示すプロトコル図であり、図２３ではＳＳＭシステム５４２もホストシステム５４０によって認証される。
【０１４９】
図２４は、本発明の一実施形態を例示する証明書連鎖５９０の図である。前述したように、ベリファイする場合に提示の必要がある証明書連鎖は多数の証明書を含むことがある。図２４の証明書連鎖は全部で９つの証明書を含み、認証する場合にはこれらの証明書をすべてベリファイすることが必要となる場合がある。背景技術の欄で前に説明したように、既存の証明書ベリファイシステムでは、送信される証明書連鎖に不備があったり、信用証明全体が送信されたり、証明書が特定の順序で送信されないと、受信側は証明書を一通り受信し記憶するまで証明書を解析できない。しかし、連鎖に含まれる証明書の数は事前に分からないため、問題が生じることがある。長さが定かでない証明書連鎖を記憶するた

めに大量の記憶容量を確保する必要になることがある。これはベリファイを行う記憶装置にとって問題になることがある。

【０１５０】

本発明の一実施形態は、証明書連鎖が記憶装置によってベリファイされる順序と同じ順序でホスト装置が証明書連鎖を送信するシステムによってこの問題を軽減できるという認識に基づく。よって、図２４に示すように、証明書の連鎖５９０は、ホストルート証明書のすぐ下に位置する証明書５９０（１）から始まり、ホスト証明書に相当する証明書５９０（９）で終わる。したがって、装置１０はまず、証明書５９０（１）で公開鍵をベリファイし、その後に証明書５９０（２）で公開鍵のベリファイ等を行い、最後に証明書５９０（９）で公開鍵をベリファイする。これで証明書連鎖５９０全体のベリファイプロセスは完了する。ホスト装置が証明書連鎖５９０をベリファイと同じ順序でメモリ装置１０へ送信する場合、メモリ装置１０は証明書が届くたびにベリファイを開始することができ、連鎖５９０に含まれる９つの証明書が一通り届くまで待つ必要はない。

【０１５１】

したがって、ホスト装置は、一実施形態において、メモリ装置１０に対して連鎖５９０の証明書を一度に１つずつ送信する。メモリ装置１０は一度に１つの証明書を記憶することになる。連鎖の中の最後の証明書を除き、ベリファイ済みの証明書はホストから送信される次の証明書で上書きできる。このため、メモリ装置１０には、１つのみの証明書を随時記憶する容量を確保すればよい。

【０１５２】

メモリ装置は、連鎖５９０が一通り届いたことを知る必要がある。このため、好ましくは、最後の証明書５９０（９）には、これが連鎖の中で最後の証明書であることを伝える標識または標示を入れる。これを例示する図２５の表は、ホストからメモリ装置１０へ送信される証明書バッファに先行する制御セクタ内の情報を示す。図２５に示すように、証明書５９０（９）の制御セクタには引数名「最終」フラグがある。メモリ装置１０は、「最終」フラグが設定されているかどうかをチェックして受信した証明書が連鎖における最終証明書であるかどうかを判断することにより、連鎖の中で証明書５９０（９）が最後の証明書であることをベリファイできる。

【０１５３】

代替的な実施形態では、連鎖５９０の証明書を１つずつ送信するのではなく、１つ、２つ、または３つの証明書からなるグループで送信してもよい。当然ながら、グループで使用する証明書の数は異なる場合があったり、あるいは同じになる場合がある。連鎖５９０には５つの連続する証明書列５９１、５９３、５９５、５９７、および５９９がある。それぞれの列は少なくとも１つの証明書を含む。ある１つの証明書の列には、連鎖の中で該当する１列の先行列に隣接する証明書（先頭証明書）と、連鎖の中で該当する１列の後続列に隣接する証明書（終端証明書）と、先頭証明書と終端証明書との間にある全証明書が含まれる。例えば列５９３の中には、全部で３つの証明書５９０（２）、証明書５９０（３）、および証明書５９０（４）がある。メモリ装置１０による５つの証明書の列のベリファイは５９１、５９３、５９５、５９７の順で行われ、５９９で終わる。したがって、５つの列がメモリ装置１０によるベリファイと同じ順序で送信され、受信される場合、ベリファイ済みの列をメモリ装置で記憶する必要はなくなり、最後の列を除く列はいずれも、ホストから到着する次の列で上書きできる。前の実施形態と同様に、連鎖内の最後の証明書には標識、例えばこれが連鎖における最後の証明書であることを伝える特定の値に設定されたフラグを入れるのが望ましい。この実施形態の場合、メモリ装置は５つの列のうち、証明書数が最も多い列の証明書を記憶する十分な容量を確保するだけでよい。よって、ホストが送ろうとする列のうちの最も大きい列を事前にメモリ装置１０に知らせる場合、メモリ装置１０は最も大きい列のための十分な容量を確保するだけでよい。

【０１５４】

好ましくは、ホストによって送信される連鎖の中の各証明書の長さは、その証明書によって証明される公開鍵の長さの４倍以下である。同様に、メモリ装置の公開鍵を証明する

ためにメモリ装置１０からホスト装置へ送信される証明書の長さは好ましくは、その証明書によって証明される公開鍵の長さの４倍以下である。

【０１５５】

図２６のフローチャートは、前述した証明書連鎖ベリファイの実施形態を示すものであり、ここでは簡潔を図るため、各グループ内の証明書数を１と仮定する。図２６に示すように、ホストはカードに向けて連鎖内の証明書を順次送信する。連鎖の中の第１の証明書（前述したように、通常はルート証明書の後続証明書）から始まって、カードは、認証の対象となるホストから証明書連鎖を順次受信する（ブロック６０２）。そして、カードは受信する証明書の各々をベリファイし、証明書のいずれかでベリファイに失敗した場合はプロセスを中止する。カードは、証明書のいずれかでベリファイに失敗した場合、ホストに通知する（ブロック６０４、６０６）。次に、カードは、最後の証明書が受信されベリファイされたかどうかを検出する（菱形６０８）。最終証明書の受信とベリファイとがまだであれば、カードはブロック６０２まで戻り、ホストからの証明書の受信とベリファイを続行する。最終証明書を受信し、ベリファイしたら、カードは証明書ベリファイの後に続く次の段階へ進む（６１０）。図２６とそれ以降の図の内容は例としてメモリカードを参照するが、物理的形態がメモリカードではないメモリ装置にもこれらの内容が当てはまることが理解できる。

【０１５６】

図２７は、カードがホストを認証する場合にホストによって実行されるプロセスを示す。図２７に示すように、ホストは連鎖の中の次の証明書をカードに送信する（ブロック６２０）（通常はルート証明書の後続証明書から始まる。ホストは、認証の失敗を伝える中止通知がカードから届いているかどうかを判断する（菱形６２２）。中止通知が届いているならホストは停止する（ブロック６２４）。中止通知が届いてなければ、ホストは送信された最後の証明書で「最終フラグ」が設定されているかどうかをチェックすることにより、連鎖の最終証明書が送信済みかどうかを確認する。最終証明書が送信済みであれば、ホストは証明書ベリファイの後に続く次の段階へ進む（ブロック６２８）。図２２および２３に示すように、次の段階はチャレンジ・レスポンスであり、その後にセッション鍵の作成が続いてもよい。連鎖の最終証明書が送信済みでなければ、ホストはブロック６２０まで戻り、連鎖内の次の証明書を送信する。

【０１５７】

図２８および図２９は、カードが認証される場合にカードとホストがとる動作を示す。図２８に示すように、カードは開始後、連鎖の中で証明書の送信を求めるホストからの要求を待つ（ブロック６３０、菱形６３２）。ホストから要求が届かなければ、カードは菱形６３２へ戻る。ホストから要求が届く場合、カードは連鎖の中の次の証明書を送信することになり、これは送信すべき最初の証明書から始まる（通常はルート証明書の後続証明書から始まる）（ブロック６３４）。カードは、ホストから失敗通知が届いたかどうかを判断する（菱形６３６）。失敗通知が届いた場合、カードは停止する（ブロック６３７）。失敗通知が届かない場合、カードは最終証明書が送信済みかどうかを判断する（菱形６３８）。最終証明書が送信済みでなければ、カードは菱形６３２まで戻り、連鎖内の次の証明書の送信を求める次の要求をホストから受け取るまで待つ。最終証明書が送信済みであれば、カードは次の段階へ進む（ブロック６３９）。

【０１５８】

図２９は、カードが認証される場合にホストがとる動作を示す。ホストは、連鎖内の次の証明書を求める要求をカードへ送り、これは送信されるべき最初の証明書に対する要求から始まる（ブロック６４０）。ホストは受信するそれぞれの証明書をベリファイし、ベリファイに失敗した場合はプロセスを中止し、カードに通知する（ブロック６４２）。ベリファイに合格した場合、ホストは最終証明書が受信済みでベリファイに成功したかどうかをチェックする（菱形６４４）。最終証明書の受信とベリファイがまだであれば、ホストはブロック６４０まで戻り、連鎖内の次の証明書を求める要求を送る。最終証明書が受信済みでベリファイに成功した場合、ホストは証明書ベリファイの後に続く次の段階へ進

む（ブロック６４６）。

【０１５９】

証明書失効

発行された証明書はその有効期間全体にわたって使われることが予想される。しかし、様々な事情から有効期間の満了に先立ち証明書が無効になる場合がある。名称の変更、対象とＣＡとの関係の変化（例えば、従業員の退職）、対応する秘密鍵の侵害または侵害の疑い等がこれにあたる。このような場合にはＣＡが証明書を無効にする必要がある。

【０１６０】

ＳＳＡにおける証明書の失効には別の方法があり、ＡＣＲはそれぞれ別々の証明書失効制度で構成できる。まず、失効制度をサポートしない形にＡＣＲを構成することができる。この場合の証明書は有効期限まで有効とみなされる。証明書失効リスト（ＣＲＬ）を使うこともできる。さらに別の代案として、後述するようにある特定のアプリケーションに失効制度を限定する、つまりアプリケーション別にしてもよい。ＡＣＲでは、失効値を指定することによって３通りの失効制度のどれが採用されているかを指定する。失効制度なしで作成されたＡＣＲでは、そのＡＣＲの所有者の失効制度を採用できる。メモリ装置証明書の失効は、ＳＳＡセキュリティシステムではなくホストによって執り行われる。ホストルート証明書の失効管理はＡＣＲの所有者が担当し、これはＡＣＲの信用証明を更新することによって果たされる。

【０１６１】

証明書失効リスト（ＣＲＬ）

ＳＳＡシステムで失効制度を使用するには、それぞれのＣＡが証明書失効リスト（ＣＲＬ）と呼ばれる署名済みデータ構造を定期的に発行する。ＣＲＬは失効した証明書を識別するタイムスタンプ付きリストであり、ＣＡ（該当する証明書を発行したＣＡ）によって署名され、一般に公開され自由に利用できる。ＣＲＬの中では、失効した証明書をそれぞれの証明書シリアル番号で識別する。ＣＲＬのサイズは任意なものであって、期限切れ前に失効する証明書の数しだいで決まる。（例えば、ホストのアイデンティティをベリファイするため）証明書を使用する装置は、証明書の署名（ならびに有効性）をチェックするだけでなく、ＣＲＬを通じて受け取ったシリアル番号のリストにこれを照らしてベリファイする。証明書の発行元にあたるＣＡから発行されるＣＲＬでその証明書の識別情報、例えばシリアル番号が見つかる場合、これは、その証明書が失効し、もはや有効でないことを意味する。

【０１６２】

証明書の有効性を検査する目的をＣＲＬで果たすには、ＣＲＬについても、これが真正であることをベリファイする必要がある。ＣＲＬには、その発行元にあたるＣＡの秘密鍵を使って署名し、ＣＡの公開鍵を使って署名済みＣＲＬを復号化することによってこれが真正であることをベリファイする。復号化されたＣＲＬが無署名ＣＲＬのダイジェストに一致する場合、そのＣＲＬに改竄がなく、真正であることを意味する。ＣＲＬのダイジェストを得るためにハッシュアルゴリズムを使って頻繁にＣＲＬのハッシュ計算が行われ、そのダイジェストはＣＡの秘密鍵で暗号化される。ＣＲＬが有効かどうかをベリファイするには、ＣＡの公開鍵を使って署名済みＣＲＬ（すなわち、ハッシュ化・暗号化ＣＲＬ）を復号化して復号化・ハッシュ化ＣＲＬ（すなわち、ＣＲＬのダイジェスト）を得る。そして、これをハッシュ化ＣＲＬと比較する。このため、ベリファイプロセスでは、復号化・ハッシュ化ＣＲＬとの比較のためのＣＲＬのハッシュ計算ステップを頻繁にともなうことがある。

【０１６３】

ＣＲＬ方式の一特徴として、（ＣＲＬを使った）証明書の妥当性のベリファイはＣＲＬの入手と分けて行うことができる。ＣＲＬも証明書の適切な発行元によって署名され、証明書のベリファイと同様に、ＣＲＬの発行元にあたるＣＡの公開鍵を使って前述したようにベリファイされる。メモリ装置は署名がＣＲＬのものであることをベリファイし、さらにＣＲＬの発行元と証明書の発行元との一致をベリファイする。ＣＲＬ方式の別の特徴と

して、ＣＲＬは証明書自体とまったく同じやり方で、具体的には信頼性のないサーバと信頼性のない通信を通じて、配布できる。Ｘ．５０９規格ではＣＲＬとその特徴が詳述されている。

【０１６４】

ＣＲＬのためのＳＳＡ基盤構造

ＳＳＡは、ＣＲＬ方式を使ったホスト失効のための基盤構造を提供する。ＣＲＬ失効制度を採用するＲＳＡ方式ＡＣＲで認証する場合、ホストはＳｅｔ　Ｃｅｒｔｉｆｉｃａｔｅコマンドに対して追加のフィールドとして１つのＣＲＬ（発行元ＣＡによって無効にされた証明書がない場合は空のＣＲＬ）を加える。このフィールドには、証明書の発行元によって署名されたＣＲＬが入る。このフィールドが存在する場合、メモリ装置１０は最初にＳｅｔ　Ｃｅｒｔｉｆｉｃａｔｅコマンドで証明書をベリファイする。ＣＲＬリポジトリの入手とアクセスは全面的にホストが担当する。ＣＲＬが有効であり続ける期間（ＣＲＬ有効期間、すなわちＣＥＴ）もＣＲＬと併せて発行される。現在の時間がこの期間から外れていることがベリファイ中に判明すると、そのＣＲＬには不備があるとみなされ、証明書のベリファイに使うことはできない。その結果、証明書の認証は失敗する。

【０１６５】

従来の証明書ベリファイ方法では、認証する側またはベリファイする側の事業体が、証明書失効リストを所有しているか、あるいはそうでないかにかかわらず、証明機関（ＣＡ）から取り込むことができ、認証のために提示される証明書のシリアル番号をリストに照らしてチェックし、提示された証明書が失効しているかどうかを判断することになっている。認証またはベリファイする側の事業体がメモリ装置の場合、そのメモリ装置自体が使われなかったら、ＣＡから証明書失効リストは取り込まれない。予め装置に記憶された証明書失効リストが時間を経て古くなると、インストールされた日より後に失効した証明書はリストに現れない。その結果、ユーザは失効した証明書を使ってその記憶装置にアクセスできることになる。これは望ましくない。

【０１６６】

一実施形態において、認証を受けようとする事業体が、認証の対象となる証明書と併せて証明書失効リストを、認証する側の事業体、例えばメモリ装置１０に提示するシステムによって前述した問題を解決できる。認証する側の事業体は、受け取った証明書の真偽と証明書失効リストの真偽をベリファイする。認証する側の事業体は、失効リストで証明書の識別情報の有無、例えば証明書のシリアル番号の有無をチェックすることにより、証明書が失効リストに登記されているかどうかをチェックする。

【０１６７】

前述したことを踏まえ、ホスト装置とメモリ装置１０との相互認証に非対称認証方式を使うことができる。メモリ装置１０の認証を受けようとするホスト装置は、証明書連鎖と対応するＣＲＬの両方を提供する必要がある。一方、ホスト装置は予めＣＡに接続してＣＲＬを入手しているため、ホスト装置がメモリ装置１０を認証する場合、メモリ装置は、証明書または証明書連鎖と併せてＣＲＬをホスト装置に提示する必要はない。

【０１６８】

種々の内蔵または独立型ミュージックプレーヤ、ＭＰ３プレーヤ、携帯電話機、個人用携帯情報端末（ＰＤＡ）、ノートブックコンピュータ等、近年コンテンツの再生に使える種々の携帯型装置は増えている。証明機関から証明書失効リストへアクセスするため、そのような装置をワールドワイドウェブに接続することは可能であるが、多数のユーザは通常、ウェブに毎日接続するのではなく、例えば数週間に１度、新たなコンテンツを入手したり契約を更新したりするときに、これを行う。そのようなユーザにとって、証明機関からより頻繁に証明書失効リストを入手するのは面倒な場合がある。そのようなユーザについて、証明書失効リスト、さらに必要であれば被保護コンテンツへアクセスする場合に記憶装置に提示するホスト証明書を、好ましくは記憶装置自体の非保護領域に記憶する。多数の記憶装置（例えば、フラッシュメモリ）で、記憶装置の非保護領域は記憶装置自体によって管理されるのではなくホスト装置によって管理される。これにより、ユーザはより

新しい証明書失効リストを入手するため（ホスト装置を通じて）ウェブに接続する必要がない。ホスト装置は記憶装置の非保護領域からそのような情報を検索し、記憶装置またはメモリ装置に証明書とリストを提示して、記憶装置の被保護コンテンツにアクセスできる。被保護コンテンツにアクセスするための証明書とその対応する証明書失効リストは通常であれば一定の期間にわたって有効であるため、それらが有効である限り、ユーザは最新の証明書または証明書失効リストを入手する必要はない。このため、ユーザは、適度に長い期間にわたって有効な証明書と証明書失効リストを容易く入手でき、最新情報を得るために証明機関に接続する必要はない。

【０１６９】

図３０および図３１のフローチャートには、前述したプロセスが示されている。図３０に示すように、ホスト２４は、認証のためにメモリ装置に提示する証明書に付随するＣＲＬをメモリ装置１０の非保護公開領域から読み出す（ブロック６５２）。ＣＲＬはメモリの非保護領域に記憶されているため、ホストによるＣＲＬの入手より前に認証は必要ない。ＣＲＬはメモリ装置の公開領域に記憶されているため、ＣＲＬの読み出しはホスト装置２４によって管理される。そして、ホストは、ＣＲＬをベリファイの対象となる証明書と併せてメモリ装置へ送信し（ブロック６５４）、メモリ装置１０から失敗通知を受け取らなければ次の段階へ進む（ブロック６５６）。図３１を参照し、メモリ装置はホストからＣＲＬと証明書を受信し（ブロック６５８）、ＣＲＬにおける証明書シリアル番号の有無やその他の点（例えば、ＣＲＬが失効しているかどうか）をチェックする（ブロック６６０）。証明書シリアル番号がＣＲＬで見つかるか、あるいはその他の理由で失敗に終わる場合、メモリ装置はホストに失敗通知を送る（ブロック６６２）。このように同じＣＲＬを異なるホストの認証に使えるため、それぞれのホストはメモリ装置の公開領域に記憶されたＣＲＬを入手する。前述したように、ＣＲＬを使ってベリファイする証明書もまた、ユーザの便宜を図るため、好ましくはメモリ装置１０の非保護領域に、ＣＲＬと併せて、記憶する。しかし、メモリ装置に対して認証する場合に証明書を使えるホストは、証明書の発行を受けたホストのみである。

【０１７０】

図３２に示すようにＣＲＬのフィールドに次回の更新時間が入る場合、装置１０のＳＳＡは、現在の時間をこの時間に照らしてチェックし、現在の時間がこの時間を過ぎているかどうかを確認し、過ぎている場合は認証に失敗する。つまり、ＳＳＡは好ましくは、現在の時間（またはメモリ装置１０でＣＲＬを受信した時間）に照らしてＣＥＴをチェックするばかりでなく次回更新の時間もチェックする。

【０１７１】

前述したように、ＣＲＬに含まれる失効済み証明書の識別情報のリストが長くなると、リストの処理（例えば、ハッシュ計算）と、ホストによって提示される証明書のシリアル番号の検索とに時間を要し、処理と検索が順次に行われる場合は特に時間がかかる。このプロセスを加速するために処理と検索とを同時に行う。また、ＣＲＬの全体を受信した後でないとＣＲＬの処理と検索にかかれない場合にもプロセスに時間がかかる。発明者らは、ＣＲＬの一部分を受信の時点で（その都度）処理し検索すれば、ＣＲＬの最終部分を受信するときにはプロセスは完了間際となり、プロセスが捗ることに気づいた。

【０１７２】

図３３および図３４は、前述した失効制度の特徴を示す。認証する側の事業体（例えば、メモリカード等のメモリ装置）では、認証を受けようとする事業体から証明書とＣＲＬを受信する（ブロック７０２）。暗号化されていないＣＲＬの一部分を処理し（例えば、ハッシュ化し）、それと同時に、提示された証明書の識別情報（例えば、シリアル番号）をそのような部分で検索する。処理された（例えば、ハッシュ化された）ＣＲＬ部分を完全なハッシュ化ＣＲＬに組み立て、認証を受ける側の事業体から受信した部分から復号化されたＣＲＬ部分を組み立てることによって形成される完全な復号化・ハッシュ化ＣＲＬとこれを比較する。一致しないことが比較で明らかになる場合、認証は失敗に終わる。また、認証する側の事業体は、現在の時間に照らしてＣＥＴと次回更新時間の両方をチェッ

クする（ブロック７０６、７０８）。提示された証明書の識別情報がＣＲＬに記載されていることが判明する場合、あるいは現在の時間がＣＥＴの範囲内にない場合、あるいはＣＲＬの次回更新時間が過ぎている場合にも、認証は失敗に終わる（ブロック７１０）。実行に際して、ハッシュ化ＣＲＬ部分と復号化・ハッシュ化ＣＲＬ部分を組み立てるために記憶する場合、大量の記憶容量は必要ない場合がある。

【０１７３】

認証を受けようとする事業体（例えば、ホスト）は、その証明書とＣＲＬを認証する側の事業体へ送信し（ブロック７２２）、次の段階へ進む（ブロック７２４）。これは図３４に示されている。

事業体が認証のために証明書連鎖を提示する場合にも前述したものと同様のプロセスを実施できる。この場合、連鎖の中の各証明書とその対応するＣＲＬにつき前述したプロセスを繰り返すことになる。各々の証明書とそのＣＲＬを受信したらその都度処理でき、証明書連鎖の残りの部分とその対応するＣＲＬの受信を待たずにすむ。

【０１７４】

アイデンティティオブジェクト（ＩＤＯ）

アイデンティティオブジェクトは、フラッシュメモリカード等のメモリ装置１０がＲＳＡ鍵対またはその他の暗号ＩＤを記憶するための被保護オブジェクトである。アイデンティティの署名とベリファイ、データの暗号化と復号化に使う暗号ＩＤであればどのようなタイプのものでもアイデンティティオブジェクトに入れることができる。鍵対の公開鍵が真正であることを証明するＣＡの証明書（または複数のＣＡの証明書連鎖）もアイデンティティオブジェクトに入れる。アイデンティティオブジェクトを使えば、外部事業体や内部カード事業体（すなわち、アイデンティティオブジェクトの所有者と呼ばれる装置自体、内部のアプリケーション、その他）のアイデンティティの証拠を提出できる。したがって、カードは、チャレンジ・レスポンス機構でホストを認証するためにＲＳＡ鍵対またはその他のタイプの暗号ＩＤを使うのではなく、識別情報の証拠としてカードに提示されるデータストリームに署名する。換言すると、アイデンティティオブジェクトはその所有者の暗号ＩＤを収容する。アイデンティティオブジェクトの中の暗号ＩＤにアクセスするにはまず、ホストを認証する必要がある。後述するように、この認証プロセスはＡＣＲによって管理される。ホストの認証に成功したら、アイデンティティオブジェクトの所有者は相手方に対して暗号ＩＤを使って自身のアイデンティティを立証できる。例えば、相手方からホストを通じて提示されるデータには暗号ＩＤ（例えば、公開－秘密鍵対の秘密鍵）を使って署名できる。アイデンティティオブジェクトの署名済みデータと証明書はアイデンティティオブジェクトの所有者に代わって相手方へ提示される。証明書にある公開－秘密鍵の公開鍵が真正であることはＣＡ（すなわち、信用機関）によって証明されるため、相手方はこの公開鍵が真正であると信用できる。そこで相手方は証明書の公開鍵を使って署名済みデータを復号化し、復号化されたデータを相手方によって送信されたデータと比較できる。復号化されたデータが相手方によって送信されたデータに一致する場合、アイデンティティオブジェクトの所有者は真正の秘密鍵にアクセスできる自称するとおりの事業体であることが分かる。

【０１７５】

アイデンティティオブジェクトの第２の用途は、暗号ＩＤ、例えばＲＳＡ鍵自体を使って、ＩＤＯの所有者に指定されたデータを保護することである。このデータをＩＤＯの公開鍵を使って暗号化する。メモリカード等のメモリ装置１０は秘密鍵を使ってデータを復号化する。

【０１７６】

ＩＤＯはどのようなタイプのＡＣＲでも作成できるオブジェクトである。ＡＣＲは、一実施形態において、１つのみのＩＤＯオブジェクトを有していてもよい。データの署名と保護はいずれも、ＡＣＲの認証を受ける事業体に対してＳＳＡシステムから提供されるサービスである。ＩＤＯの保護水準はＡＣＲのログイン認証方式と同じくらい高い。ＩＤＯを有することになるＡＣＲには任意の認証アルゴリズムを選ぶことができる。ＩＤＯ運用

を良好に保護し得るアルゴリズムを評価し決定するのは作成元（ホスト）である。ＩＤＯを有するＡＣＲは、ＩＤＯ公開鍵取得コマンドに応じて証明書連鎖を提供する。

【０１７７】

データ保護にＩＤＯを使用する場合でも、カードから出力される復号化データにはさらなる保護が必要になることがある。そのような場合には、いずれかの認証アルゴリズムによって確立されるセキュアチャネルの使用がホストに推奨される。

ＩＤＯを作成するときには鍵の長さとＰＫＣＳ＃１バージョンを選択する。一実施形態において、ＰＫＣＳ＃１バージョン２．１が定める（指数、係数）表現を公開および秘密鍵に使用する。

ＩＤＯの作成中に盛り込まれるデータは、一実施形態において、選択された長さを有するＲＳＡ鍵対と、公開鍵の信憑性を帰納的に証明する証明書連鎖である。

【０１７８】

ＩＤＯを所有するＡＣＲはユーザデータの署名を許可する。これは２つのＳＳＡコマンドを使って果たす。

・Ｓｅｔ　ｕｓｅｒ　ｄａｔａ：署名の対象となる自由書式のデータバッファを提供する。

・Ｇｅｔ　ＳＳＡ　ｓｉｇｎａｔｕｒｅ：カードはＲＳＡ署名を提供する（ＡＣＲ秘密鍵を使用）。署名の形式とサイズはオブジェクトのタイプに応じてＰＫＣＳ＃１バージョン１．５またはＶ２．１に従い設定される。

【０１７９】

図３５～図３７はＩＤＯを使った操作を示すものであり、ここでメモリ装置１０はフラッシュメモリカードであり、このカードがＩＤＯの所有者である。図３５は、ホストへ送信されるデータに署名する場合にカードによって実行されるプロセスを示す。図３５を参照し、前述したツリー構造のノードに位置するＡＣＲの管理下でホストが認証された後（ブロック８０２）、カードは証明書を求めるホスト要求を待つ（菱形８０４）。要求を受け取ったカードは証明書を送り、菱形８０４へ戻り、次のホスト要求を待つ（ブロック８０６）。カードが所有するＩＤＯの公開鍵を証明するために証明書連鎖を送信する必要がある場合、連鎖の中のすべての証明書がホストへ送信されるまで前述した操作を繰り返す。それぞれの証明書がホストに送信された後、カードはホストから別のコマンドが届くのを待つ（菱形８０８）。所定の期間内にホストからコマンドが届かなければ、カードは菱形８０４へ戻る。ホストからデータとコマンドを受け取ったカードは、そのコマンドをチェックし、データに署名するためのものであるかどうかを確認する（菱形８１０）。データに署名するためのコマンドである場合、カードはＩＤＯの秘密鍵を使ってデータに署名し、署名したデータをホストへ送信し（ブロック８１２）、菱形８０４まで戻る。ホストからのコマンドがホストからのデータに署名するためのものでなければ、カードはＩＤＯの秘密鍵を使って受信データを復号化し（ブロック８１４）、菱形８０４まで戻る。

【０１８０】

図３６は、ホストへ送信されるデータにカードが署名する場合にホストによって実行されるプロセスを示す。図３６を参照すると、ホストはカードへ認証情報を送信する（ブロック８２２）。前述したツリー構造のノードに位置するＡＣＲの制御下で認証に成功したら、ホストは証明書連鎖を求める要求をカードへ送り、連鎖を受け取る（ブロック８２４）。カードの公開鍵のベリファイが終わったら、ホストは署名されるデータをカードへ送信し、カードの秘密鍵で署名されたデータを受信する（ブロック８２６）。

【０１８１】

図３７は、ホストがカードの公開鍵を使ってデータを暗号化し、暗号化したデータをカードへ送信するときにホストによって実行されるプロセスを示す。図３７を参照すると、ホストはカードへ認証情報を送信する（ブロック８６２）。ＡＣＲの管理下で認証に成功したら、ホストはＩＤＯの中にあるカードの公開鍵をベリファイする場合に必要となる証明書連鎖の要求をカードへ送り（ブロック８６４）、さらにデータを求める要求をカードに送る。ＩＤＯの中にあるカードの公開鍵をベリファイした後、ホストはカードのベリフ

ァイ済み公開鍵を使ってカードから届いたデータを暗号化し、カードへ送信する（ブロック８６６、８６８）。

【０１８２】

クエリ

ホストとアプリケーションは、システム操作をの実行する場合に相手方のメモリ装置またはカードについてある種の情報を所有する必要がある。例えば、ホストとアプリケーションは、メモリカードに記憶されたアプリケーションのうち、実行できるアプリケーションがいずれであるかを知る必要がある。ホストにとっての必要情報は公知でない場合があり、これはその情報を所有する権利を有する者とそうでない者があることを意味する。権限を有するユーザと持たないユーザとを区別するには、ホストで使えるクエリを２通り用意する必要がある。

【０１８３】

一般情報クエリ

このクエリはシステム公開情報を無制限に放出する。メモリ装置に記憶される機密情報は２つの部分、すなわち共有部分と非共有部分とからなる。機密情報の一部分には個々の事業体にとっての専有情報が入り、それぞれの事業体は自身の専有情報に限りアクセスが認められ、他の事業体の専有機密情報にはアクセスできない。この種の機密情報は共有されず、機密情報の非共有部位または部分を形成する。

【０１８４】

カードの中にあるアプリケーションの名前とそのライフサイクル状態等、通常であれば公の情報と考えられるものでも、場合によっては機密とみなされることがある。別の例として、公の情報とされるルートＡＣＲ名でもＳＳＡの使用するといった場合によっては機密になることがある。このような場合には、一般情報クエリに応じて情報をすべて認証済みユーザに限って利用させ、認証されていないユーザには利用させないようにするためのオプションをシステムに用意しなければならない。このような情報は機密情報の共有部分を占める。ルートＡＣＲリスト、すなわち装置上に現在存在する全ルートＡＣＲのリストは、機密情報の共有部分の一例となり得る。

【０１８５】

一般情報クエリによる公開情報へアクセスする場合、ホスト／ユーザはＡＣＲにログインする必要がない。このため、ＳＳＡ規格に精通する者であれば誰でも実行可能であり、情報を受け取ることができる。ＳＳＡの規定ではセッション番号なしでこのクエリコマンドが処理される。しかし、機密情報の共有部分へのアクセスを望む事業体は最初に、メモリ装置のデータに対するアクセスを制御する制御構造（例えば、ＡＣＲ）のいずれかを通じて認証を受ける必要がある。認証に成功した事業体は、一般情報クエリを使って機密情報の共有部分にアクセスできるようになる。前述したように、認証プロセスの結果としてアクセスのためのＳＳＡセッション番号またはｉｄが割り当てられる。

【０１８６】

非公開情報クエリ

個々のＡＣＲとそのシステムアクセスおよび資産に関する私的情報は非公開とされ、明確な認証を必要とする。この種の情報クエリで許可を得るには、ＡＣＲのログインと認証（認証がＡＣＲで指定されている場合）が事前に必要になる。このクエリにはＳＳＡセッション番号が必要である。

２種類のクエリを詳述する前に、クエリを実行する現実的な解決策としてインデックスグループの概念を説明することが有益である。

【０１８７】

インデックスグループ

ポテンシャルＳＳＡホストで実行するアプリケーションには、読み出しの対象となるセクタ数を指定することがシステムドライバとホスト上のオペレーティングシステム（ＯＳ）から求められる。これは、ホストアプリケーションがＳＳＡ読み出し操作のたびに読み出しセクタ数を把握する必要があることを意味する。

クエリ操作で供給される情報は、一般的にはこれを要求する側にとって未知の情報であるため、ホストアプリケーションがクエリを発行し、その操作に必要なセクタの量を推測するのは困難である。

【０１８８】

この問題を解決するため、ＳＳＡのクエリ出力バッファは各クエリ要求につき１つのみのセクタ（５１２バイト）からなる。出力情報の一部をなすオブジェクトはインデックスグループと呼ばれるものに編成される。オブジェクトのバイトサイズはオブジェクトのタイプによって異なり、そこから１セクタに収まるオブジェクトの数が明らかになる。これによってオブジェクトのインデックスグループが決まる。オブジェクトのサイズが２０バイトである場合、このオブジェクトのインデックスグループは２５オブジェクトまで収容される。そのようなオブジェクトが全部で５６個ある場合、それらは３つのインデックスグループに編成され、第１のインデックスグループの先頭はオブジェクト「０」（第１のオブジェクト）となり、第２のインデックスグループの先頭はオブジェクト「２５」となり、第３の最終インデックスグループの先頭はオブジェクト５０となる。

【０１８９】

システムクエリ（一般情報クエリ）

このクエリは、装置がサポートするＳＳＡシステムと、ツリー状に構成された現行のシステムと、装置で実行するアプリケーションとについての一般公開情報を提供する。後述するＡＣＲクエリ（非公開クエリ）と同様に、システムクエリは種々のクエリオプションを提供するように構成されている。

・Ｇｅｎｅｒａｌ：サポートされたＳＳＡバージョン

・ＳＳＡ　Ａｐｐｌｉｃａｔｉｏｎｓ：現在装置に存在する全ＳＳＡアプリケーションのリストで、アプリケーションの実行状態を含む。

【０１９０】

前述した情報は公開情報である。ＡＣＲクエリと同様に、ホストがクエリ出力バッファのための読み出しセクタ数を知らずにすませるため、装置からは１セクタが送り返され、ホストが引き続きさらなるインデックスグループを照会できる。インデックスグループ「０」でルートＡＣＲオブジェクトの数が出力バッファサイズの数を超過する場合、ホストは後続のインデックスグループ（「１」）で別のクエリ要求を送ることができる。

【０１９１】

ＡＣＲクエリ（非公開情報クエリ）

ＳＳＡのＡＣＲクエリコマンドは、鍵ＩＤ、アプリケーションＩＤ、パーティション、子ＡＣＲ等、ＡＣＲのシステムリソースに関する情報をＡＣＲユーザに供給するためのものである。そのクエリ情報はログインされたＡＣＲに関するもののみであり、システムツリー上の他のＡＣＲに関するものはない。換言すると、アクセスは、機密情報のうち、該当するＡＣＲの許可のもとでアクセス可能な部分に限られる。

ユーザが照会できるＡＣＲオブジェクトには３通りある。

・パーティション：名前とアクセス権（所有者、読み出し、書き込み）。

・鍵ＩＤとアプリケーションＩＤ：名前とアクセス権（所有者、読み出し、書き込み）。

・子ＡＣＲ：直接の子にあたるＡＣＲのＡＣＲおよびＡＧＰ名。

・ＩＤＯとセキュアデータオブジェクト（後述）：名前とアクセス権（所有者、読み出し、書き込み）。

【０１９２】

ＡＣＲに結び付いたオブジェクトの数は様々に異なる場合があり、情報は５１２バイト、すなわち１セクタを上回ることがある。オブジェクトの数が事前に分からない限り、ユーザはリストすべてを得るために装置内のＳＳＡシステムから読み出される必要があるセクタの数を知ることはできない。そこで前述したシステムクエリの場合と同様に、ＳＳＡシステムによって提供される各オブジェクトリストはインデックスグループに分割される。インデックスグループはセクタに収まるオブジェクトの数であり、例えば装置内のＳＳ

Ａシステムからホストにかけて１セクタで送信できるオブジェクトの数である。これにより、装置内のＳＳＡシステムは要求されたインデックスグループを１セクタで送信できる。ホスト／ユーザは、照会したオブジェクトのバッファ、バッファ内のオブジェクト数を受け取ることになる。バッファが一杯である場合、ユーザは次のオブジェクトインデックスグループを照会できる。

【０１９３】

図３８は、一般情報クエリをともなう操作を示すフローチャートである。図３８を参照すると、事業体から一般情報クエリを受け取ったＳＳＡシステムは（９０２）、その事業体が認証済みかどうかを判断する（菱形９０４）。認証済みである場合には、システムは公開情報と機密情報の共有部分とを事業体に供給する（ブロック９０６）。認証済みでなければ、システムは公開情報のみを事業体に供給する（ブロック９０８）。

【０１９４】

図３９は、非公開情報クエリをともなう操作を示すフローチャートである。図３９を参照すると、事業体から非公開情報クエリを受け取ったＳＳＡシステムは（９２２）、その事業体が認証済みかどうかを判断する（菱形９２４）。認証済みである場合には、システムは事業体に機密情報を供給する（ブロック９２６）。認証済みでない場合には、システムは機密情報に対する事業体のアクセスを拒否する（ブロック（９２８）。

【０１９５】

フィーチャセットエクステンション（ＦＳＥ）

多くの場合、データ処理活動（例えば、ＤＲＭライセンスオブジェクト検査）をカード上のＳＳＡの内部で実行できることは大変有利である。その結果、データ処理タスクのすべてをホストで実行する代替的な解決策に比べてより安全でより効率的なシステムとなり、ホストへの依存度も低くなる。

【０１９６】

ＳＳＡセキュリティシステムは、メモリカードによって記憶され、管理され、保護されるオブジェクトのアクセス、使用、収集を制御する一連の認証アルゴリズムと認可方針とを備える。アクセスを得たホストは、メモリ装置に記憶されたデータに対して処理を行い、メモリ装置に対するアクセスはＳＳＡによって制御される。しかし、データは本質的に用途によって大いに異なるため、装置に記憶されたデータを取り扱うわけではないＳＳＡではデータ形式またはデータ処理は決まっていない。

【０１９７】

本発明の一実施形態は、通常であればホストによって果たされる機能の一部をメモリカードで実行する形にＳＳＡシステムを強化できるという認識に基づく。そこで、ホストのソフトウェア機能のいくつかは、２つの部分、すなわち引き続きホストによって果たされる部分と、カードによって果たされる部分とに分かれる場合がある。こうすることで多くの用途にとってデータ処理の安全性と効率性が向上する。この目的のため、ＦＳＥと呼ばれる機構を加えることによってＳＳＡの能力を高める場合がある。このようにカードによって実行されるＦＳＥのホストアプリケーションを、ここでは内部アプリケーションまたは装置内部アプリケーションと呼ぶ場合がある。

【０１９８】

強化ＳＳＡシステムは、カードの認証およびアクセス制御を提供する基本ＳＳＡコマンド群を、カードアプリケーションの導入により拡張する機構を提供する。カードアプリケーションは、ＳＳＡ以外のサービスを（例えば、ＤＲＭスキーム、ｅコマーストランザクション）を実行することになっている。ＳＳＡフィーチャセットエクステンション（ＦＳＥ）は、独自開発のデータ処理ソフトウェア／ハードウェアモジュールで標準ＳＳＡセキュリティシステムを強化する機構である。ＳＳＡ　ＦＳＥシステムのサービスにより、ホスト装置は前述したクエリで得られる情報のほかに、カードで使用可能なアプリケーションを照会し、特定のアプリケーションを選択し、これと通信できる。前述した一般クエリと非公開クエリをこの目的に使うこともできる。

【０１９９】

ＳＳＡ　ＦＳＥでカード機能群を拡張するには２つの方法を使う。

・サービス提供：認可された事業体が通信パイプと呼ばれる独自のコマンドチャネルを使って内部アプリケーションと直に通信することによって実現する。

・ＳＳＡ標準アクセス制御方針の拡張：内部の被保護データオブジェクト（ＣＥＫ、後述するセキュアデータオブジェクト、すなわちＳＤＯ等）に内部カードアプリケーションを関連付けさせることによって実現する。そのようなオブジェクトにアクセスするときに所定の標準ＳＳＡ方針が満たされる場合は関連付けアプリケーションが起動して、標準ＳＳＡ方針に加えて少なくとも１つの条件を課す。この条件は好ましくは、標準ＳＳＡ方針とは対峙しない。この追加条件も満たされる場合に限りアクセスが許諾される。ＦＳＥの能力をさらに詳述する前に、ＦＳＥの構造的態様と通信パイプとＳＤＯをここで取り上げる。

【０２００】

ＳＳＡモジュールと関連するモジュール

図４０Ａは、ホスト装置２４へ接続されたメモリ装置１０（フラッシュメモリカード等）におけるシステムアーキテクチャ１０００の機能ブロック図であり、本発明の一実施形態を例示するものである。カード２０のメモリ装置にあるソフトウェアモジュールの主要コンポーネントは次のとおりである。

【０２０１】

ＳＳＡトランスポート層１００２

ＳＳＡトランスポート層はカードプロトコルに依拠する。これはカード１０のプロトコル層でホスト側ＳＳＡ要求（コマンド）を処理し、処理したものをＳＳＭ　ＡＰＩに送る。ホスト－カードの同期とＳＳＡコマンドの識別はすべてこのモジュールで行われる。ホスト２４とカード１０との間のＳＳＡデータ転送もトランスポート層がすべて担当する。

【０２０２】

セキュアサービスモジュールコア（ＳＳＭコア）１００４

このモジュールはＳＳＡの実施例の重要部分である。ＳＳＭコアはＳＳＡアーキテクチャを実装する。より具体的に、ＳＳＭコアはＳＳＡツリーと、ＡＣＲシステムと、前述したシステムを構成する全ルールを実行する。ＳＳＭコアモジュールは暗号ライブラリ１０１２を使ってＳＳＡセキュリティと暗号化、復号化、ハッシュ計算等の暗号機能を支援する。

【０２０３】

ＳＳＭコアＡＰＩ１００６

これは、ホストと内部アプリケーションがＳＳＭコアと連絡をとりながらＳＳＡ操作を実行するところの層である。図４０Ａに示すように、ホスト２４と内部装置アプリケーション１０１０はいずれも同じＡＰＩを使用する。

【０２０４】

セキュアアプリケーション管理モジュール（ＳＡＭＭ）１００８

ＳＡＭＭはＳＳＡシステムの一部ではないが、ＳＳＡシステムと連絡をとりながら内部装置アプリケーションを制御するカードの重要モジュールである。

実行する内部装置アプリケーションはいずれもＳＡＭＭによって管理される。

１．アプリケーションライフサイクルの監視と制御

２．アプリケーションの初期化

３．アプリケーション／ホスト／ＳＳＡインターフェイス

【０２０５】

装置内部アプリケーション１０１０

これは、カード側での実行が許可されたアプリケーションである。ＳＡＭＭによって管理され、ＳＳＡシステムにアクセスすることがある。ホスト側アプリケーションと内部アプリケーションとの間の通信パイプはＳＳＭコアから提供される。ＤＲＭアプリケーションや以降で詳述する使い捨てパスワード（ＯＴＰ）アプリケーションは内部実行アプリケーションの一例である。

【０２０６】
装置管理システム（ＤＭＳ）１０１１
これは、カードのシステムおよびアプリケーションファームウェアを更新したり、出荷後（一般的に後発行と呼ばれる）モードでサービスを追加／削除したりするためのプロセスおよびプロトコルを収容するモジュールである。
【０２０７】
図４０Ｂは、ＳＳＭコア１００４の内部ソフトウェアモジュールの機能ブロック図である。図４０Ｂに示すように、コア１００４はＳＳＡコマンド処理部１０２２を含む。処理部１０２２は、ホストまたは装置内部アプリケーション１０１０から発行されたＳＳＡコマンドを解析した後、ＳＳＡ管理部１０２４に引き渡す。ＡＧＰやＡＣＲ等のＳＳＡセキュリティデータ構造や、すべてのＳＳＡのルールと方針はいずれもＳＳＡデータベース１０２６に記憶される。ＳＳＡ管理部１０２４は、データベース１０２６に記憶されたＡＣＲやＡＧＰやその他の制御構造によって制御を実施する。ＩＤＯやセキュアデータオブジェクトをはじめとするその他のオブジェクトもＳＳＡデータベース１０２６に記憶される。ＳＳＡ管理部１０２４は、データベース１０２６に記憶されたＡＣＲやＡＧＰやその他の制御構造に制御を実施する。ＳＳＡが関与しない非セキュア操作はＳＳＡ非セキュア操作モジュール１０２８によって処理される。ＳＳＡアーキテクチャのもとでのセキュア操作はＳＳＡセキュア操作モジュール１０３０によって処理される。モジュール１０３２は、モジュール１０３０を暗号ライブラリ１０１２へ接続するインターフェイスである。１０３４は、モジュール１０２６および１０２８を図１のフラッシュメモリ２０へ接続する層である。
【０２０８】
通信（またはパススルー）パイプ
パススルーパイプオブジェクトは、ＳＳＭコアとＳＡＭＭの制御下で認可されたホスト側事業体と内部アプリケーションとの通信を可能にする。ホストと内部アプリケーションとのデータ転送はＳＥＮＤコマンドとＲＥＣＥＩＶＥコマンドで行われる（後述）。実際のコマンドはアプリケーションによって異なる。パイプを作る事業体（ＡＣＲ）は、パイプ名とチャネルの開通によってつながるアプリケーションのＩＤとを提供することが必要になる。他の被保護オブジェクトと同様に、このＡＣＲがパイプの所有者になり、標準の委譲ルールおよび制限に従って他のＡＣＲに使用権や所有権を委譲できる。
【０２０９】
認証済みの事業体は、そのＡＣＡＭでＣＲＥＡＴＥ＿ＰＩＰＥ権限が設定されている場合にパイプオブジェクトの作成が許可されることになる。内部アプリケーションとの通信は、そのＰＣＲでパイプ書き込み権限またはパイプ読み出し権限が設定されている場合に限り許可される。所有権とアクセス権の委譲は、事業体がパイプの所有者か、あるいはそのＰＣＲでアクセス権委譲が設定されている場合に限り許可される。他のすべての権限と同様に、別のＡＣＲへ所有権を委譲する当初の所有者は、好ましくはこの装置アプリケーションに対するすべての権限から引き離される。
【０２１０】
好ましくは、ある特定のアプリケーションにつき１つのみの通信パイプを作成する。第２のパイプを作成し、接続済みのアプリケーションにそれを接続する試みは、好ましくはＳＳＭシステム１０００によって拒否される。したがって、好ましくは、装置内部アプリケーション１０１０のいずれか１つと通信パイプとの間に１対１の関係がある。しかし、（委譲機構により）複数のＡＣＲが１つの装置内部アプリケーションと通信する場合がある。（別々のアプリケーションに接続された複数パイプの委譲または所有権により）１つのＡＣＲが数個の装置アプリケーションと通信する場合がある。通信パイプ間のクロストークをなくすため、別々のパイプを制御するＡＣＲは、好ましくは全く別個のツリーノードに位置する。
【０２１１】
ホストと特定のアプリケーションとのデータ転送は次のコマンドを使って行う。

・書き込みパススルー：ホストから装置内部アプリケーションへ非定型データバッファを転送する。

・読み出しパススルー：ホストから装置内部アプリケーションへ非定型データバッファを転送し、内部処理が完了したら非定型データバッファをホストに戻す。

【０２１２】

書き込みパススルーコマンドと読み出しパススルーコマンドでは、ホストが通信しようとする相手方の装置内部アプリケーション１００８のＩＤをパラメータとして提供する。事業体の権限をベリファイし、要求される側のアプリケーションにつながるパイプを使用する権限が要求する側の事業体（すなわち、この事業体が使っているセッションを運営するＡＣＲ）にある場合、データバッファを解釈し、コマンドを実行する。

この通信方法により、ホストアプリケーションはＳＳＡ　ＡＣＲセッションチャネルを通じて内部装置アプリケーションにベンダー固有／独自なコマンドを引き渡すことができる。

【０２１３】

セキュアデータオブジェクト（ＳＤＯ）

ＳＤＯは、ＦＳＥと併せて使用できる便利なオブジェクトである。

ＳＤＯは汎用容器として機密情報を安全に記憶する役割を果たす。ＣＥＫオブジェクトと同様に、ＳＤＯはＡＣＲが所有し、アクセス権と所有権はＡＣＲ間で委譲できる。ＳＤＯは所定の規制に従って保護され使用されるデータを収容し、オプションとして、装置内部アプリケーション１００８へ至るリンクを有する。機密データは、好ましくはＳＳＡシステムによって使用されることも解釈されることもなく、オブジェクトの所有者とユーザがこれを使用し、解釈する。換言すると、ＳＳＡシステムは取り扱うデータの情報を認識しない。このため、オブジェクトの中にあるデータの所有者とユーザは、ホストとデータオブジェクトとの間でデータが受け渡しされるときにＳＳＡシステムとの結び付きによって機密情報が失われることをさほど心配せずにすむ。ＳＤＯオブジェクトはホストシステム（または内部アプリケーション）によって作成され、ＣＥＫを作成する場合と同様に、文字列ＩＤが割り当てられる。作成する場合にホストは名前のほかに、ＳＤＯへリンクするアプリケーションのアプリケーションＩＤと、ＳＳＡによって記憶され、保全性ベリファイが行われ、検索されるデータブロックとを提供する。

【０２１４】

ＳＤＯは、ＣＥＫと同様に、好ましくはＳＳＡセッションの中でのみ作成される。このセッションを開放するために使われるＡＣＲがＳＤＯの所有者となり、ＳＤＯを削除する権利や機密データを読み書きする権利を有するほかにも、ＳＤＯの所有権やこれにアクセスする権限を別のＡＣＲ（子ＡＣＲまたは同一ＡＧＰ内のＡＣＲ）に委譲する権利を有する。

【０２１５】

書き込み操作と読み出し操作はＳＤＯの所有者に限定される。書き込み操作は既存のＳＤＯオブジェクトデータを提示されたデータバッファで上書きする。読み出し操作はＳＤＯのデータ記録一式を検索する。

【０２１６】

正式なアクセス権限を有する所有者以外のＡＣＲには、ＳＤＯのアクセス操作が許可される。次の操作が定められている。

・ＳＤＯ　Ｓｅｔ、アプリケーションＩＤの指定：データはこのアプリケーションＩＤを有する内部ＳＳＡアプリケーションによって処理される。アプリケーションはＳＤＯとの関連付けによって起動する。オプションとして、アプリケーションがＳＤＯオブジェクトの書き込みを行う場合がある。

・ＳＤＯ　Ｓｅｔ、アプリケーションＩＤの不在：このオプションは無効であり、不正コマンドエラーを促す。Ｓｅｔコマンドにはカードで実行する内部アプリケーションが必要となる。

・ＳＤＯ　Ｇｅｔ、アプリケーションＩＤの指定：要求はこのアプリケーションＩＤを

有する装置内部アプリケーションによって処理される。アプリケーションはＳＤＯとの関連付けによって起動する。出力は、指定がなくとも、要求する側へ送り返される。オプションとして、アプリケーションがＳＤＯオブジェクトの読み出しを行う場合がある。

・ＳＤＯ　Ｇｅｔ、アプリケーションＩＤの不在：このオプションは無効であり、不正コマンドエラーを促す。Ｇｅｔコマンドにはカードで実行する内部アプリケーションが必要となる。

・ＳＤＯ関連の権限：ＡＣＲにはＳＤＯの所有者になるものと、アクセス権限（Ｓｅｔ、Ｇｅｔ、または両方）を有するのみのものとがある。ＡＣＲには、自身が所有しないＳＤＯに対する自身のアクセス権を別のＡＣＲへ譲渡することが許可される。ＡＣＡＭ権限を有するＡＣＲにはＳＤＯの作成とアクセス権の委譲が明示的に許可される。

【０２１７】

内部ＡＣＲ

内部ＡＣＲはＰＣＲを有するＡＣＲに類似するが、装置１０にとって外部の事業体はこのＡＣＲにログインできない。代替的に、これの管理下にあるオブジェクトか、あるいはこのオブジェクトと関連付けするアプリケーションが呼び出されるときに、図４０ＢのＳＳＡ管理部１０２４が自動的に内部ＡＣＲにログインする。アクセスを試みる事業体はカードまたはメモリ装置にとって内部の事業体であるため、認証の必要はない。ＳＳＡ管理部１０２４は内部通信を可能にするために内部ＡＣＲにセッション鍵を渡すことになる。

【０２１８】

これより使い捨てパスワード生成とデジタル権利管理という２つの例を引いてＦＳＥの能力を例示する。使い捨てパスワード生成の例を説明する前に、二因子認証のテーマを取り上げる。

【０２１９】

ＯＴＰ実施形態

二因子認証（ＤＦＡ）

ＤＦＡは、標準のユーザ信用証明（具体的にはユーザ名とパスワード）に追加の秘密、すなわち「第２の因子」を加えることにより、ウェブサービスサーバ等への私的なログインでセキュリティを高める認証プロトコルである。この第２の秘密は通常、ユーザが所有する物理的で安全なトークンに記憶される。ユーザはログインの過程でログイン信用証明の一部として所有の証拠を提供する必要がある。所有の証明には使い捨てパスワード（ＯＴＰ）がよく使われ、これはセキュアトークンで生成され出力される、１回のログインのみで通用するパスワードである。トークンなしでＯＴＰを計算するのは暗号技術的に不可能であるため、ユーザが正しいＯＴＰを提供できる場合、これをもってトークン所有の十分な証拠とみなされる。ＯＴＰは１回のログインのみで通用し、前のログインから得た古いパスワードは通用しないことになるため、ユーザはログインのときにトークンを所有していなければならない。

【０２２０】

以降のセクションで説明する製品は、ＳＳＡのセキュリティデータ構造と、一連のＯＴＰで次のパスワードを計算するＦＳＥ設計とを利用しながら、フラッシュメモリでそれぞれ別々のパスワード系列（異なるウェブサイトへのログインに使用）を生成する複数の「仮想」セキュアトークンを実行するものである。図４１は、このシステムのブロック図を示す。

【０２２１】

システム一式１０５０は、認証サーバ１０５２と、インターネットサーバ１０５４と、トークン１０５８を有するユーザ１０５６とを備える。最初のステップでは、認証サーバとユーザとの間で共有秘密を取り決める（シード提供とも呼ばれる）。ユーザ１０５６は秘密またはシードの発行を要求し、これをセキュアトークン１０５８に記憶する。次のステップでは、発行された秘密またはシードを特定のウェブサービスサーバに結合する。これを果たしたら認証に取りかかることができる。ユーザはＯＴＰの生成をトークンに指示する。ＯＴＰはユーザ名とパスワードと併せてインターネットサーバ１０５４へ送信され

る。インターネットサーバ１０５４は認証サーバ１０５２にＯＴＰを転送し、ユーザアイデンティティのベリファイを依頼する。認証サーバもＯＴＰを生成するが、これはトークンとの共有秘密から生成されるため、トークンから生成されたＯＴＰに一致することになる。一致が判明する場合、ユーザアイデンティティはベリファイされ、認証サーバがインターネットサーバ１０５４へ肯定応答を返すとユーザログインプロセスは完了することになる。

【０２２２】

ＦＳＥによるＯＴＰ生成には次のような特徴がある。

・ＯＴＰシードは安全な状態で（暗号化されて）カードに記憶される。

・パスワード生成アルゴリズムはカードの内部で実行される。

・装置１０は複数の仮想トークンをエミュレートでき、それぞれの仮想トークンでは異なるシードを記憶し、異なるパスワード生成アルゴリズムを使用できる。

・認証サーバから装置１０へシードを移すセキュアプロトコルは装置１０が提供する。

【０２２３】

図４２は、ＳＳＡのＯＴＰシード提供機能とＯＴＰ生成機能を示すものであり、ここで実線の矢印は所有権またはアクセス権を示し、破線の矢印は関連付けまたはリンクを示している。図４２に示すように、ＳＳＡ　ＦＳＥシステム１１００ではＮ個のアプリケーションＡＣＲ１１０６によってそれぞれ管理される１つ以上の通信パイプ１１０４を通じてソフトウェアプログラムコードＦＳＥ１１０２にアクセスできる。後述する実施形態では１つのみのＦＳＥソフトウェアアプリケーションを例示し、各ＦＳＥアプリケーションにつき１つのみの通信パイプがある。しかし、複数のＦＳＥアプリケーションを使えることが理解できる。図４２には１つのみの通信パイプが例示されているが、複数の通信パイプを使えることが理解できる。そのような変形例はいずれも可能である。図４０Ａ、４０Ｂ、および４２を参照すると、ＦＳＥ１１０２はＯＴＰ提供に用いるアプリケーションであって、図４０Ａの装置内部アプリケーション１０１０の一部をなす場合がある。制御データ構造（ＡＣＲ１１０１、１１０３、１１０６、１１１０）はＳＳＡのセキュリティデータ構造の一部であり、ＳＳＡデータベース１０２６に記憶される。ＩＤＯ１１２０やＳＤＯオブジェクト１１２２等のデータ構造と通信パイプ１１０４もＳＳＡデータベース１０２６に記憶される。

【０２２４】

図４０Ａおよび図４０Ｂを参照すると、ＡＣＲとデータ構造が関わるセキュリティ関連操作（例えば、セッション中のデータ転送、暗号化、復号化、ハッシュ計算等の操作）は、モジュール１０３０がインターフェイス１０３２と暗号ライブラリ１０１２の支援を受けて処理する。ＳＳＭコアＡＰＩ１００６は、ホストと受け渡しするＡＣＲ（外部ＡＣＲ）が関わる操作と、ホストと受け渡ししない内部ＡＣＲが関わる操作を区別しないため、ホストが関わる操作と装置内部アプリケーション１０１０が関わる操作に区別はない。ホスト側事業体によるアクセスと装置内部アプリケーション１０１０によるアクセスは、同じ制御機構によって制御される。このため、ホスト側アプリケーションと装置内部アプリケーション１０１０とでデータ処理を柔軟に区別できる。内部アプリケーション１０１０（例えば、図４２のＦＳＥ１１０２）は内部ＡＣＲ（例えば、図４２のＡＣＲ１１０３）と関連付けし、これの管理のもとで起動する。

【０２２５】

さらに、重要情報へのアクセス、例えばＳＤＯの内容またはそのＳＤＯの内容から検索される情報へのアクセスは、好ましくはＡＣＲやＡＧＰ等のセキュリティデータ構造とＳＳＡのルールと方針とによって管理されるため、外部または内部アプリケーションは、ＳＳＡのルールと方針とに従う限りにおいてその内容または情報にアクセスできる。例えば、２名のユーザがデータを処理するために個々の装置内部アプリケーション１０１０を起動する場合、別々の階層ツリーに位置する内部ＡＣＲを使って２名のユーザによるアクセスが制御されるため、アプリケーション間のクロストークはない。両ユーザはデータ処理する場合に共通の装置内部アプリケーション１０１０にアクセスでき、ＳＤＯの内容また

は情報の所有者の側では、内容または情報制御の喪失を心配せずにすむ。例えば、データを記憶するＳＤＯに対する装置内部アプリケーション１０１０によるアクセスは別々のツリーに位置するＡＣＲによって制御できるため、アプリケーション間のクロストークはない。この制御方法は、前述したデータに対するアクセスをＳＳＡが制御する方法に似ている。これは、データオブジェクトに記憶されたデータのセキュリティを内容の所有者とユーザに提供する。

【０２２６】

図４２を参照すると、ＯＴＰ関連ホストアプリケーションに必要なソフトウェアアプリケーションコードの一部分を、ＦＳＥ１１０２のアプリケーションとしてメモリ装置１０に記憶（メモリカード発行前に予め記憶、またはメモリカード発行後にロード）することは可能である。そのようなコードを実行する場合、ホストはまずＮ個の認証ＡＣＲ１１０６のいずれか１つを通じて認証を受け、パイプ１１０４にアクセスする必要があり、Ｎは正の整数である。ホストは、起動しようとするＯＴＰ関連アプリケーションを識別するためのアプリケーションＩＤを提供する必要もある。認証に成功したら、ＯＴＰ関連アプリケーションと関連付けられたパイプ１１０４を通じてそのようなコードにアクセスし、実行できる。前述したように、パイプ１１０４と、ＯＴＰ関連内部アプリケーション等のアプリケーションとの間には、好ましくは１対１の関係がある。図４２に示すように、複数のＡＣＲ１１０６が共通のパイプ１１０４を制御することがある。１つのＡＣＲで複数のパイプを制御する場合がある。

【０２２７】

図４２には、データ、例えばＯＴＰ生成のためのシードをそれぞれ収容するオブジェクト１１１４と総称するセキュアデータオブジェクトＳＤＯ１、ＳＤＯ２、およびＳＤＯ３が示され、このシードは貴重であって、好ましくは暗号化する。３つのデータオブジェクトとＦＳＥ１１０２との間のリンクまたは関連付け１１０８はこれらのオブジェクトの一属性であり、いずれか１つのオブジェクトにアクセスするときには、アプリケーションＩＤがＳＤＯ属性に一致するＦＳＥ１１０２のアプリケーションが起動し、このアプリケーションは装置のＣＰＵ１２によって実行され、さらなるホストコマンドを受け取る必要はない（図１）。

【０２２８】

図４２を参照すると、ＯＴＰプロセスを制御するためのセキュリティデータ構造（ＡＣＲ１１０１、１１０３、１１０６、および１１１０）とそのＰＣＲは、ユーザがＯＴＰプロセスを開始する前に作成済みである。ユーザは、認証サーバＡＣＲ１１０６のいずれか１つを通じてＯＴＰ装置内部アプリケーション１１０２を起動するためのアクセス権を得る必要がある。ユーザは、Ｎ個のユーザＡＣＲ１１１０のいずれか１つを通じてＯＴＰに対するアクセス権を得る必要もある。ＳＤＯ１１１４はＯＴＰのシード提供過程で作成できる。ＩＤＯ１１１６は、好ましくは作成済みで内部ＡＣＲ１１０３によって制御される。内部ＡＣＲ１１０３は、作成されたＳＤＯ１１１４も制御する。ＳＤＯ１１１４にアクセスするときには、図４０ＢのＳＳＡ管理部１０２４が自動的にＡＣＲ１１０３にログインする。内部ＡＣＲ１１０３にはＦＳＥ１１０２が関連付けられる。破線１１０８に示すように、ＯＴＰのシード提供過程ではＳＤＯ１１１４にＦＳＥを関連付けさせる。関連付けが成立した後、ホストがＳＤＯにアクセスするときには、ホストからさらなる要求がなくとも関連付け１１０８によってＦＳＥ１１０２が起動する。Ｎ個のＡＣＲ１１０６のいずれか１つを通じて通信パイプ１１０４にアクセスするときにも、図４０ＢのＳＳＡ管理部１０２４がＡＣＲ１１０３に自動的にログインする。いずれの場合でも（ＳＤＯ１１１４とパイプ１１０４へのアクセス）、ＳＳＡ管理部はＦＳＥ１１０２にセッション番号を渡し、このセッション番号によって内部ＡＣＲ１１０３に至るチャネルが識別される。

【０２２９】

ＯＴＰ操作は２つの段階、すなわち図４３に示すシード提供段階と図４４に示すＯＴＰ生成段階とを伴う。図４０～図４２も併せて参照することで、この説明に役立つ。図４３はシード提供プロセスを示すプロトコル図である。図４３に示すように、ホスト２４等の

ホストとカードは様々な動作をとる。ＳＳＭコア１００４を含む図４０Ａおよび４０ＢのＳＳＭシステムは、カード側で様々な動作をとる１事業体である。図４２に示すＦＳＥ１１０２もカード側で様々な動作をとる事業体である。

【０２３０】

二因子認証ではユーザがシードの発行を要求し、発行されたシードはセキュアトークンに記憶される。この例のセキュアトークンはメモリ装置またはカードである。ユーザはＳＳＭシステムにアクセスするため、図４２の認証ＡＣＲ１１０６のいずれか１つで認証を受ける（矢印１１２２）。認証に成功したと仮定し（矢印１１２４）、ユーザはシードを要求する（矢印１１２６）。ホストは、シード要求に署名するためのアプリケーション１１０２を選択してシード要求に署名する要求をカードへ送る。起動すべきアプリケーションＩＤをユーザが知らない場合、例えば装置に対する非公開クエリにより、この情報を装置１０から入手できる。そして、ユーザは起動するべきアプリケーションのアプリケーションＩＤを入力し、これによりこのアプリケーションに対応する通信パイプも選択される。パススルーコマンドにより、ユーザから該当する通信パイプを通じてアプリケーションＩＤで指定されたアプリケーションにかけて、ユーザコマンドが転送される（矢印１１２８）。起動したアプリケーションは、図４２のＩＤＯ１１１２等の所定のＩＤＯの公開鍵による署名を要求する。

【０２３１】

ＳＳＭシステムはＩＤＯの公開鍵を用いてシード要求に署名し、署名の完了をアプリケーションに通知する（矢印１１３２）。次に、起動アプリケーションはＩＤＯの証明書連鎖を要求する（矢印１１３４）。これに応じて、ＳＳＭシステムは、ＡＣＲ１１０３の制御下でＩＤＯの証明書連鎖を提供する。起動アプリケーションは通信パイプを通じて署名済みシード要求とＩＤＯの証明書連鎖をＳＳＭシステムへ提供し、ＳＳＭシステムは同じものをホストへ転送する（矢印１１３８）。通信パイプにおける署名済みシード要求とＩＤＯ証明書連鎖の送信は、図４０ＡのＳＡＭＭ１００８とＳＳＭコア１００４との間で確立するコールバック関数によって行われるが、このコールバック関数については以降で詳述する。

【０２３２】

ホストが受け取った署名済みシード要求とＩＤＯ証明書連鎖は、図４１に示す認証サーバ１０５２へ送信される。署名済みシード要求の出所が信用できるトークンであることはカードから提供される証明書連鎖で証明されているため、認証サーバ１０５２には秘密シードをカードに提供する用意がある。そこで認証サーバ１０５２は、ＩＤＯの公開鍵で暗号化されたシードをユーザＡＣＲ情報と併せてホストに送信する。このユーザ情報により、Ｎ個のユーザＡＣＲのうち、これから生成するＯＴＰにユーザがアクセスするためのユーザＡＣＲがいずれであるのかが明らかになる。ホストはアプリケーションＩＤを提供することによってＦＳＥ１１０２でＯＴＰアプリケーションを起動し、これによりこのアプリケーションに対応する通信パイプも選択され、さらにホストはユーザＡＣＲ情報をＳＳＭシステムへ転送する（矢印１１４０）。暗号化されたシードとユーザＡＣＲ情報は通信パイプを通じて選択されたアプリケーションへ転送される（矢印１１４２）。起動したアプリケーションは、ＩＤＯの秘密鍵を使ってシードを復号化する要求をＳＳＭシステムに送る（矢印１１４４）。ＳＳＭシステムはシードを復号化し、復号化の完了を伝える通知をアプリケーションに送る（矢印１１４６）。起動アプリケーションは、セキュアデータオブジェクトを作成し、そのセキュアデータオブジェクトにシードを記憶することを要求する。起動アプリケーションは、使い捨てパスワードを生成するため、そのＳＤＯにＯＴＰアプリケーション（要求するアプリケーションと同じアプリケーションであってもよい）のＩＤを割り振ることも要求する。ＳＳＭシステムはＳＤＯ１１１４のいずれか１つを作成し、そのＳＤＯの中にシードを記憶し、ＯＴＰアプリケーションのＩＤをＳＤＯに割り振り、完了したらアプリケーションに通知を送る（矢印１１５０）。アプリケーションは、ホストから提供されたユーザ情報に基づきＳＤＯ１１１４にアクセスするためのアクセス権を内部ＡＣＲから該当するユーザＡＣＲへ委譲することをＳＳＭシステムに要求す

る（矢印１１５２）。委譲が完了したらＳＳＭシステムはアプリケーションに通知する（矢印１１５４）。アプリケーションは、コールバック関数によりＳＤＯの名前（スロットＩＤ）を通信パイプ経由でＳＳＭシステムへ送信する（矢印１１５６）。ＳＳＭシステムは同じものをホストへ転送する（矢印１１５８）。ホストはＳＤＯの名前をユーザＡＣＲに結合し、このため、ユーザはＳＤＯにアクセスできるようになる。

【０２３３】

今度は図４４のプロトコル図を参照しながらＯＴＰ生成プロセスを説明する。ユーザは使い捨てパスワードを入手するため、アクセス権があるユーザＡＣＲにログインする（矢印１１７２）。認証に成功したと仮定し、ＳＳＭシステムはホストに通知し、ホストは「ｇｅｔ　ＳＤＯ」コマンドをＳＳＭへ送信する（矢印１１７４、１１７６）。前述したように、シードを記憶するＳＤＯにはＯＴＰを生成するアプリケーションが関連付けられている。したがって、これまでのように通信パイプ経由でアプリケーションを選択する代わりに、矢印１１７６のコマンドでアクセスするＳＤＯとＯＴＰ生成アプリケーションとの関連付けによってＯＴＰ生成アプリケーションを起動する（矢印１１７８）。ＯＴＰ生成アプリケーションは、ＳＤＯから内容（すなわち、シード）を読み出すことをＳＳＭシステムに要求する。好ましくは、ＳＳＭはＳＤＯの内容に含まれる情報を認識せず、ＦＳＥの指示に従ってＳＤＯのデータを処理するに過ぎない。シードが暗号化されている場合、ＦＳＥの指示に従い読み出しを行う前にシードを復号化することが必要となる場合がある。ＳＳＭシステムはＳＤＯからシードを読み出し、ＯＴＰ生成アプリケーションへシードを提供する（矢印１１８２）。ＯＴＰ生成アプリケーションはＯＴＰを生成し、これをＳＳＭシステムに提供する（矢印１１８４）。ＯＴＰはＳＳＭによってホストへ転送され（矢印１１８６）、さらにホストから認証サーバ１０５２へＯＴＰが転送され、二因子認証プロセスは完了する。

【０２３４】

コールバック関数

図４０ＡのＳＳＭコア１００４とＳＡＭＭ１００８との間では汎用コールバック関数を確立する。そのような関数には様々な装置内部アプリケーションと通信パイプを登録できる。起動した装置内部アプリケーションはこのコールバック関数を使用することにより、アプリケーションへのホストコマンドの引き渡しに使われたものと同じ通信パイプを使って処理後のデータをＳＳＭシステムへ引き渡すことができる。

【０２３５】

ＤＲＭシステム実施形態

図４５はＤＲＭシステムを示す機能ブロック図であり、このシステムでは通信パイプ１１０４’と、ＦＳＥアプリケーション１１０２’に至るリンク１１０８’を備えるＣＥＫ１１１４’と、ＤＲＭ機能の実行機能を制御する制御構造１１０１’、１１０３’、１１０６’とを使用する。見て分かるように、図４５のアーキテクチャはセキュリティデータ構造として認証サーバＡＣＲとユーザＡＣＲの代わりにライセンスサーバＡＣＲ１１０６’と再生ＡＣＲ１１１０’とを含み、さらにＳＤＯの代わりにＣＥＫ１１１４’を含む点を除き、図４２のものによく似ている。加えて、ＩＤＯは関係しないから図４５で省かれている。ＣＥＫ１１１４’はライセンス提供プロセスの中で作成できる。プロトコル図である図４６はライセンス提供とコンテンツダウンロードのプロセスを示すものであり、ここではライセンスオブジェクトの中で鍵が提供される。ＯＴＰの実施例と同様に、ライセンスの取得を望むユーザはまず、Ｎ個のＡＣＲ１１０６’のいずれか１つとＮ個のＡＣＲ１１１０’のいずれか１つのもとでアクセス権を取得する必要があり、そうすることでメディアプレーヤソフトウェアアプリケーション等のメディアプレーヤでコンテンツを再生できるようになる。

【０２３６】

図４６に示すように、ホストはライセンスサーバＡＣＲ１１０６’による認証を受ける（矢印１２０２）。認証に成功したと仮定し（矢印１２０４）、ライセンスサーバはライセンスファイルをＣＥＫ（鍵ＩＤと鍵値）と併せてホストに提供する。ホストは、カード

上のＳＳＭシステムにアプリケーションＩＤを提供することによって起動すべきアプリケーションも選択する。ホストは、プレーヤ情報（例えば、メディアプレーヤーソフトウェアアプリケーションの情報）も送信する（矢印１２０６）。このプレーヤ情報により、Ｎ個の再生ＡＣＲ１１１０’のうち、プレーヤのアクセス権がある再生ＡＣＲがいずれであるのかが明らかになる。ＳＳＭシステムは、選択されたアプリケーションに対応する通信パイプを通じてライセンスファイルとＣＥＫをＤＲＭアプリケーションへ転送する（矢印１２０８）。起動したアプリケーションは、ライセンスファイルを非表示パーティションに書き込むことをＳＳＭシステムに要求する（矢印１２１０）。ライセンスファイルがそのとおりに書き込まれたら、ＳＳＭシステムはアプリケーションに通知する（矢印１２１２）。ＤＲＭアプリケーションはＣＥＫオブジェクト１１１４’の作成を要求し、ライセンスファイルからその中に鍵値を記憶する。ＤＲＭアプリケーションは、提供された鍵に関連するライセンスをチェックするＤＲＭアプリケーションのＩＤをＣＥＫオブジェクトに割り振ることも要求する（矢印１２１４）。ＳＳＭシステムはこれらのタスクを完了し、その旨をアプリケーションに通知する（矢印１２１６）。アプリケーションは、ホストから送信されたプレーヤ情報に基づきＣＥＫ１１１４’に対するコンテンツの読み出しアクセス権をプレーヤがアクセスできる再生ＡＣＲへ委譲することを要求する（矢印１２１８）。ＳＳＭシステムは委譲を行い、その旨をアプリケーションに通知する（矢印１２２０）。ライセンスの記憶が完了したことを伝えるメッセージがアプリケーションから通信パイプを経由しＳＳＭシステムへ送信され、ＳＳＭシステムはこれをライセンスサーバへ転送する（矢印１２２２および１２２４）。通信パイプ経由のこの操作にはコールバック関数を使用する。この通知を受けたライセンスサーバは、提供されたＣＥＫの鍵値によって暗号化されたコンテンツファイルをカードに提供する。暗号化されたコンテンツはホストによってカードの公開領域に記憶される。暗号化されたコンテンツファイルの記憶にセキュリティ機能は関与しないため、ＳＳＭシステムは記憶に関与しない。

【０２３７】

図４７は、再生操作を示す。ユーザはホストを通じて該当する再生ＡＣＲ（すなわち、前述した矢印１１５２および１１５４で読み出し権を委譲された再生ＡＣＲ）による認証を受ける（矢印１２４２）。認証に成功したと仮定し（矢印１２４４）、ユーザは鍵ＩＤと関連付けられたコンテンツの読み出し要求を送る（矢印１２４６）。要求を受け取ったＳＳＭシステムは、アクセスされているＤＲＭアプリケーションのＩＤがＣＥＫオブジェクトに関連付けられていることに気づき、識別されたＤＲＭアプリケーションを起動する（矢印１２４８）。このＤＲＭアプリケーションは、鍵ＩＤと関連付けられたデータ（すなわち、ライセンス）の読み出しをＳＳＭシステムに要求する（矢印１２５０）。読み出し要求があったデータの情報を認識しないＳＳＭは、ＦＳＥからの要求を処理してデータの読み出しプロセスを実行するに過ぎない。ＳＳＭシステムは非表示パーティションからデータ（すなわち、ライセンス）を読み出し、そのデータをＤＲＭアプリケーションに提供する（矢印１２５２）。ＤＲＭアプリケーションはデータを解釈し、データの中にあるライセンス情報をチェックして、ライセンスが有効かどうかを確認する。ライセンスがなお有効である場合、ＤＲＭアプリケーションはコンテンツの復号化が許可されることをＳＳＭシステムに知らせる（矢印１２５４）。ＳＳＭシステムは要求のあったコンテンツをＣＥＫオブジェクトの鍵値を使って復号化し、復号化されたコンテンツを再生するためにホストに提供する（矢印１２５６）。ライセンスがすでに有効でない場合、コンテンツアクセスの要求は拒否される。

【０２３８】

ライセンスサーバからのライセンスファイルで鍵が提供されない場合のライセンス提供とコンテンツのダウンロードは、図４６に示す場合といくぶん異なる。図４８のプロトコル図はそのような別方式を示す。図４６および図４８で同じステップは同じ数字で識別されている。このため、ホストとＳＳＭシステムはまず初めに認証に取り組む（矢印１２０２、１２０４）。ライセンスサーバはホストにライセンスファイルと鍵ＩＤを提供するが鍵値は提供せず、ホストはそれらを、起動しようとするＤＲＭアプリケーションのアプリ

ケーションＩＤと併せて、ＳＳＭシステムへ転送する。ホストはプレーヤ情報も送信する（矢印１２０６’）。ＳＳＭシステムは、選択されたアプリケーションに対応する通信パイプを通じて選択されたＤＲＭアプリケーションへライセンスファイルと鍵ＩＤを転送する（矢印１２０８）。ＤＲＭアプリケーションは、非表示パーティションへのライセンスファイル書き込みを要求する（矢印１２１０）。ライセンスファイルがそのとおりに書き込まれたら、ＳＳＭシステムはＤＲＭアプリケーションに通知する（矢印１２１２）。ＤＲＭアプリケーションは、鍵値を生成することと、ＣＥＫオブジェクトを作成することと、そこに鍵値を記憶することと、ＣＥＫオブジェクトにＤＲＭアプリケーションのＩＤを割り振ることとをＳＳＭシステムに要求する（矢印１２１４’）。要求に応じたＳＳＭシステムはＤＲＭアプリケーションへ通知を送る（矢印１２１６）。ＤＲＭアプリケーションは、ホストからのプレーヤ情報に基づきＣＥＫオブジェクトに対する読み出しアクセス権を再生ＡＣＲに委譲することをＳＳＭシステムに要求する（矢印１２１８）。これが完了すると、ＳＳＭシステムはその旨をＤＲＭアプリケーションに通知する（矢印１２２０）。ＤＲＭアプリケーションはライセンスが記憶されたことをＳＳＭシステムに通知するが、この通知はコールバック関数により通信パイプ経由で送信される（矢印１２２２）。通知はＳＳＭシステムによってライセンスサーバへ転送される（矢印１２２４）。ライセンスサーバは鍵ＩＤと関連付けられたコンテンツファイルをＳＳＭシステムへ送信する（矢印１２２６）。ＳＳＭシステムは鍵ＩＤによって識別された鍵値でコンテンツファイルを暗号化するが、アプリケーションはこれに一切関与しない。暗号化されカードに記憶されたコンテンツは、図４７のプロトコルを用いて再生できる。

【０２３９】

前述したＯＴＰ実施形態とＤＲＭ実施形態で、ホスト装置は様々なＯＴＰアプリケーションとＤＲＭアプリケーションをＦＳＥ１１０２および１１０２’で選ぶことができる。ユーザは所望の装置内部アプリケーションを選択し、起動できる。しかし、ＳＳＭモジュールとＦＳＥとの全体的関係は常に同じであるため、ユーザとデータの提供者はＳＳＭモジュールとの受け渡しやＦＳＥを起動する場合に標準のプロトコル群を使用することができる。ユーザと提供者は、独自に開発されたものを含む様々な装置内部アプリケーションの詳細に関わる必要はない。

【０２４０】

さらに、図４６および図４８がそうであるように、提供プロトコルはいくぶん異なることがある。図４６の場合、ライセンスオブジェクトは鍵値を収容するが、図４８の場合は鍵値を収容しない。このような違いから、前述したような若干異なるプロトコルが必要となる。しかし、図４７における再生は、ライセンス提供のあり方にかかわりなく同じである。したがって、この違いが問題となるのは通常であればコンテンツの提供者と配布者のみであって、再生段階にしか通常かかわらない消費者には関係ない。このアーキテクチャは、プロトコルのカスタマイズする場合にコンテンツの提供者や配布者に多大な柔軟性を提供しつつ、消費者にとっては扱いやすい状態のままである。当然、３つ以上の提供プロトコル群によって提供されるデータから検索される情報でも、第２のプロトコルを用いてアクセスできる。

【０２４１】

前述した実施形態から提供される別の利点として、ユーザ等の外部事業体と装置内部アプリケーションはいずれもセキュリティデータ構造によって制御されるデータを利用するが、ユーザがアクセスできるものは装置内部アプリケーションによって記憶データから検索される結果のみである。ＯＴＰ実施形態の場合、ホスト装置を通じてユーザが入手できるものはＯＴＰのみであって、シード値は入手できない。ＤＲＭ実施形態の場合、ホスト装置を通じてユーザが入手できるものは再生されたコンテンツのみであって、ライセンスファイルまたは暗号鍵のいずれにもアクセスできない。このため、セキュリティを損なうことなく消費者の便宜を図ることができる。

【０２４２】

ＤＲＭの一実施形態において、装置内部アプリケーションもホストも暗号鍵にアクセス

せず、セキュリティデータ構造のみがこれにアクセスする。別の実施形態において、セキュリティデータ構造以外の事業体も暗号鍵にアクセスできる。鍵が装置内部アプリケーションによって生成され、セキュリティデータ構造によって制御される場合もある。

【０２４３】

装置内部アプリケーションと情報（例えば、ＯＴＰや再生コンテンツ）へのアクセスは同じセキュリティデータ構造によって制御される。これは、制御システムの複雑さとコストを抑える。

装置内部アプリケーションに対するアクセスを制御する内部ＡＣＲから、装置内部アプリケーションを起動することによって得られる情報に対するホストのアクセスを制御するＡＣＲへ、アクセス権を委譲する能力を提供することにより、前述した特徴および機能が実現可能となる。

【０２４４】

アプリケーション別失効制度

セキュリティデータ構造のアクセス制御プロトコルは装置内部アプリケーションの起動時に修正することもできる。例えば、証明書失効プロトコルには、ＣＲＬを使用する標準のプロトコルまたは独自のプロトコルのいずれでもよい。そこで、ＦＳＥを起動することにより、標準のＣＲＬ失効プロトコルをＦＳＥ独自プロトコルに差し替えることができる。

【０２４５】

ＳＳＡはＣＲＬ失効制度をサポートするほか、装置内部アプリケーションとＣＡ、あるいはその他の取消機関との私的通信チャネルを通じて装置の内部アプリケーションからホストを無効にすることができる。内部アプリケーション独自の失効制度はホスト－アプリケーションの関係に限定される。

【０２４６】

アプリケーション別失効制度が構成される場合、ＳＳＡシステムはＣＲＬ（提供される場合）を拒絶することになり、そうでない場合には証明書と独自のアプリケーションデータ（アプリケーション別通信パイプを通じて提供済みのデータ）を用いて証明書が失効済みか否かを判断する。

【０２４７】

前述したように、ＡＣＲでは失効値を指定することによって３通りの失効制度（失効制度なし、標準ＣＲＬ制度、アプリケーション別失効制度）のどれを採用するかを指定する。アプリケーション別失効制度を選ぶ場合、その失効制度を担当する内部アプリケーションＩＤもＡＣＲで指定し、ＣＥＴ／ＡＰＰ＿ＩＤフィールドの値は失効制度を担当する内部アプリケーションＩＤに一致することになる。装置を認証する場合、ＳＳＡシステムは内部アプリケーション独自の制度に準拠する。

【０２４８】

１組のプロトコルを別のものに差し替える代わりに、装置内部アプリケーションを起動する場合、ＳＳＡによって既に施行されているアクセス制御に追加のアクセス条件を設けることもできる。例えば、ＣＥＫの鍵値に対するアクセス権をＦＳＥでより綿密に調べることができる。鍵値のアクセス権がＡＣＲにあると判断したＳＳＡシステムは、ＦＳＥと相談のうえでアクセスを許諾する。これは、コンテンツへのアクセスを制御する場合にコンテンツの所有者に多大な柔軟性を提供する。

【０２４９】

これまで様々な実施形態を参照しながら本発明を説明してきたが、本発明の範囲から逸脱することなく変更や修正を施すことができ、本発明の範囲が専ら添付の特許請求の範囲とその同等物とによって定まるものであることが理解できよう。

【図１】

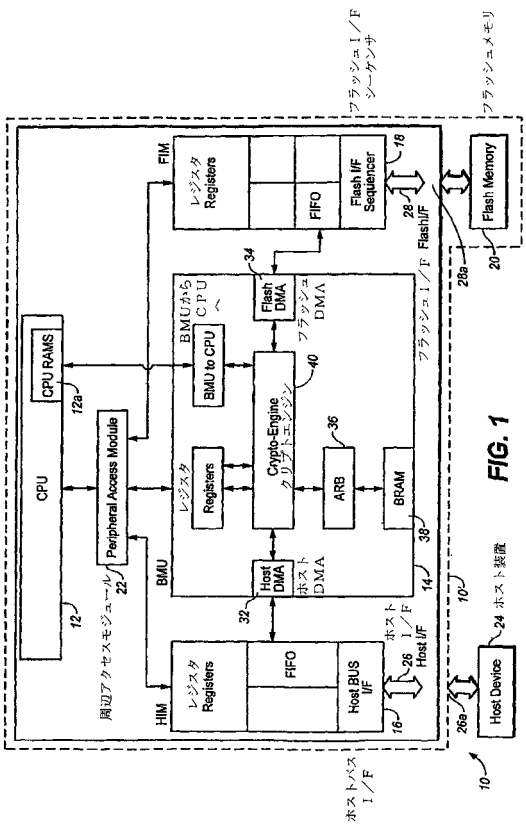


FIG. 1

【図２】

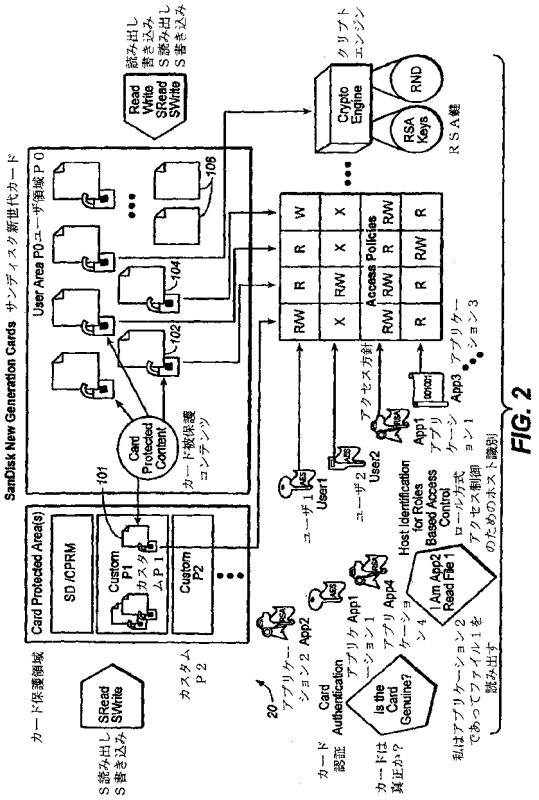


FIG. 2

【図３】

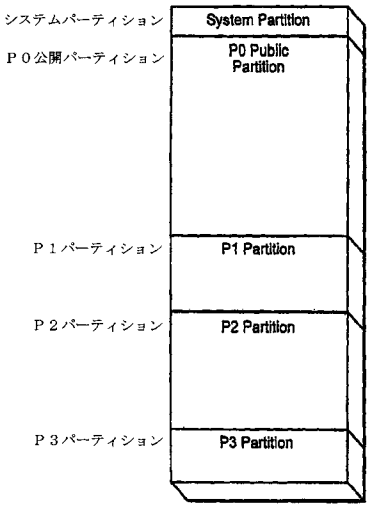


FIG. 3

【図４】

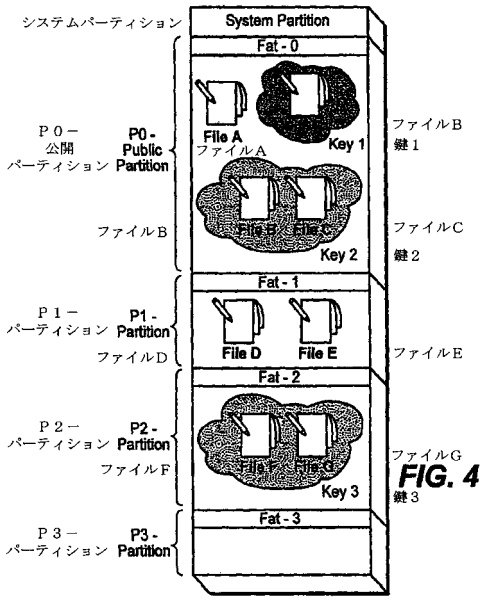


FIG. 4

【図５】

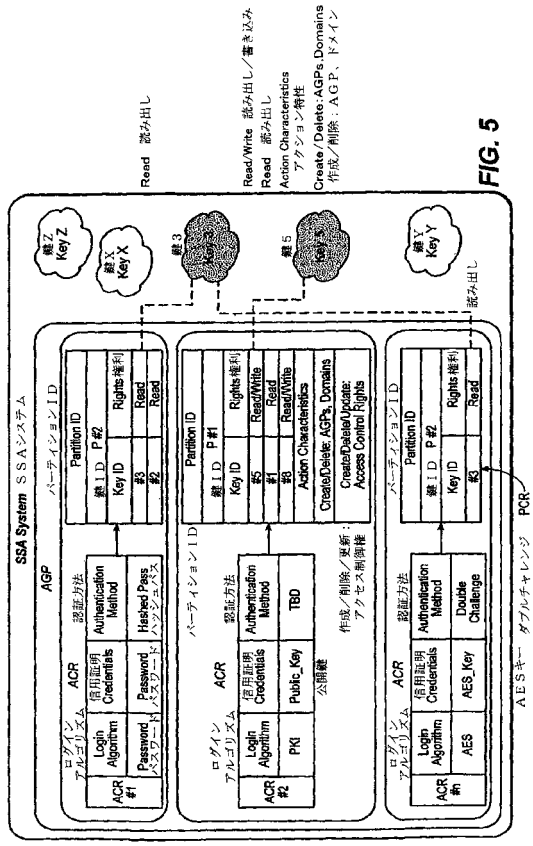


FIG. 5

【図６】

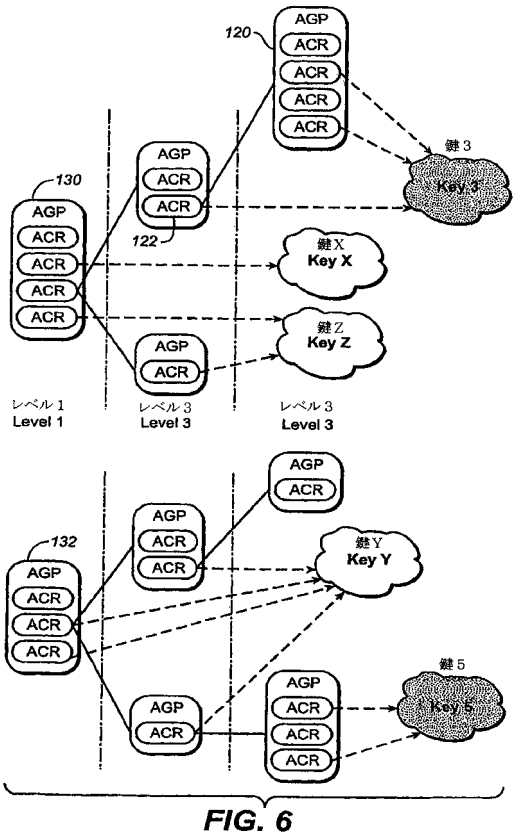


FIG. 6

【図７】

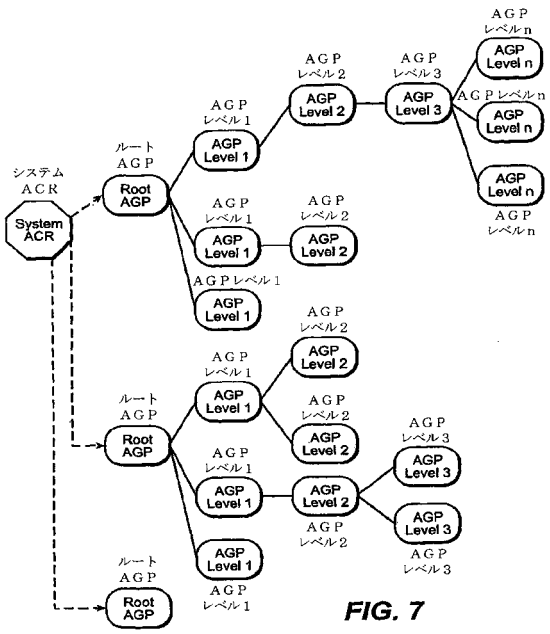


FIG. 7

【図８Ａ】

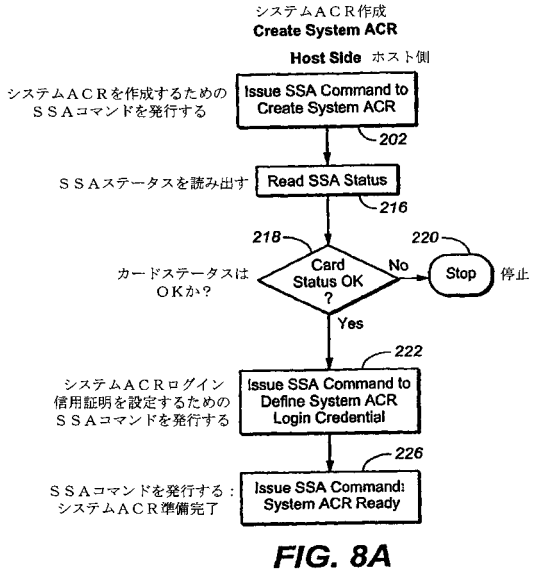


FIG. 8A

【図８Ｂ】

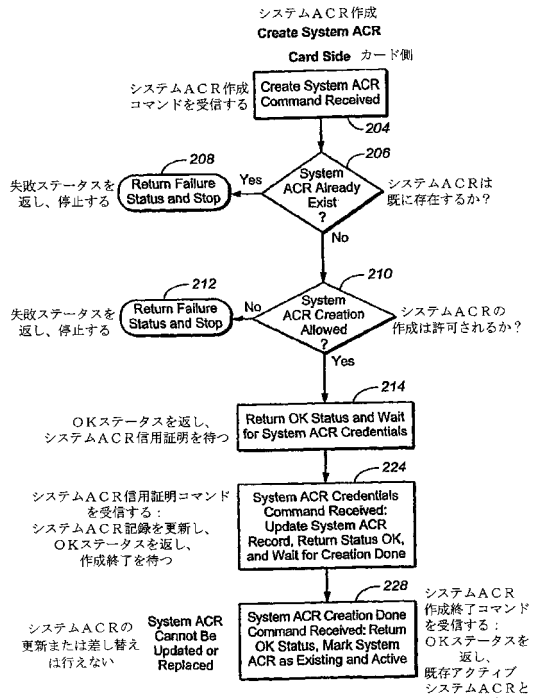


FIG. 8B

【図９】

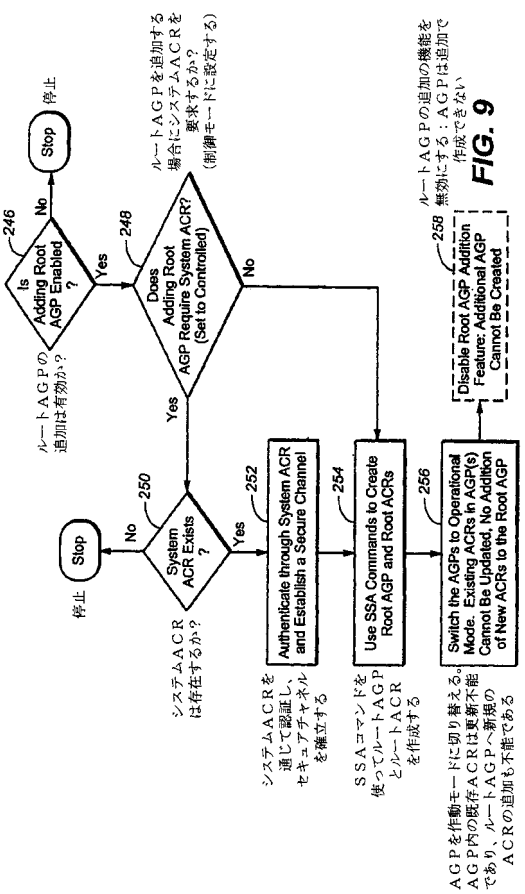


FIG. 9

【図１０】

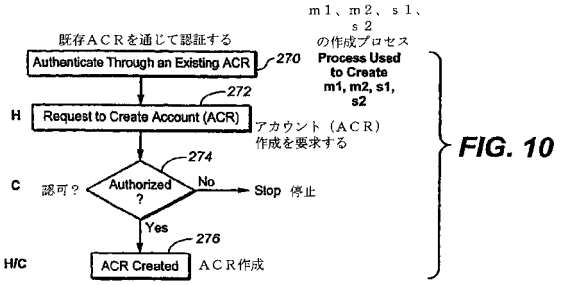


FIG. 10

【図１１】

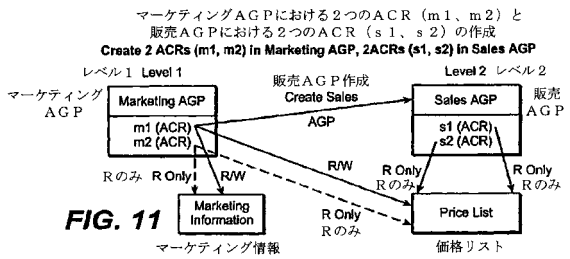


FIG. 11

【図１２】

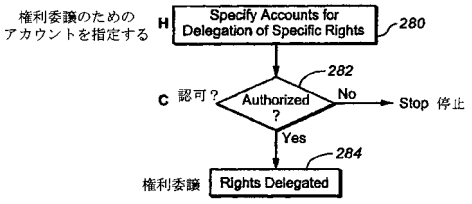


FIG. 12

【図１３】

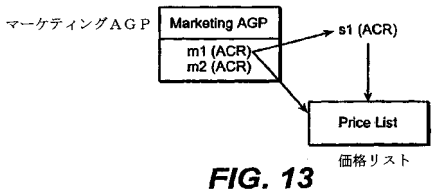


FIG. 13

【図１４】

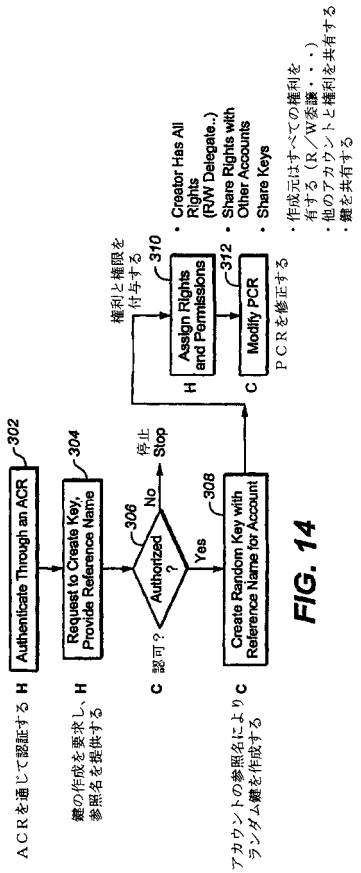


FIG. 14

【図１５】

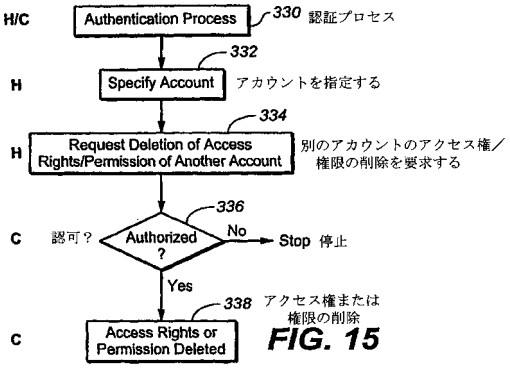


FIG. 15

【図１６】

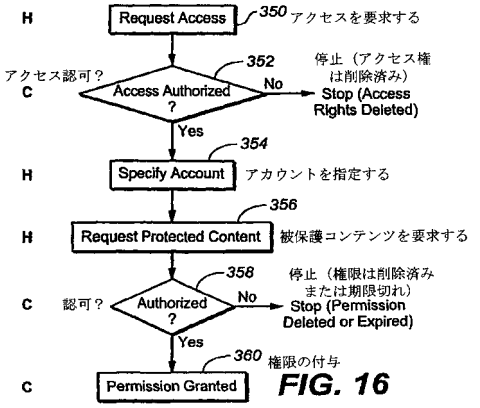


FIG. 16

【図１７Ａ】

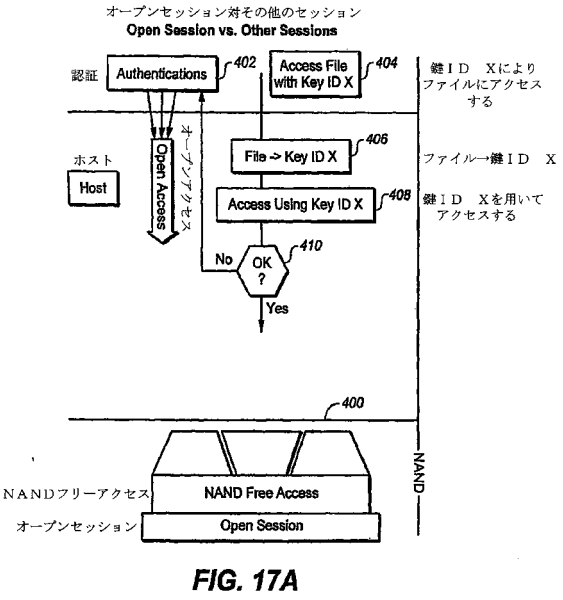


FIG. 17A

【図１７Ｂ】

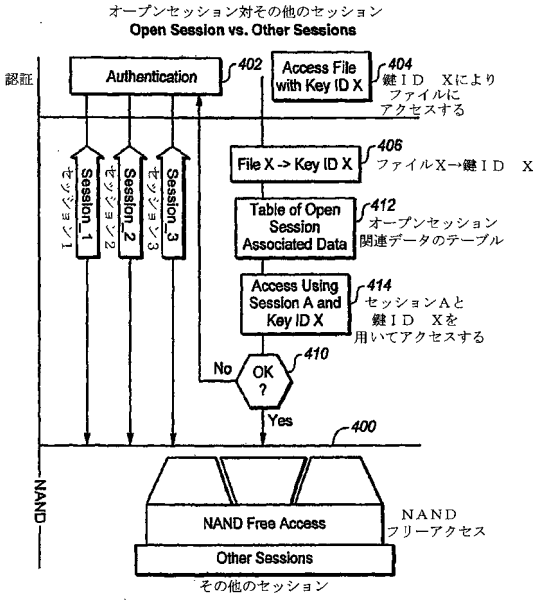


FIG. 17B

【図１８】

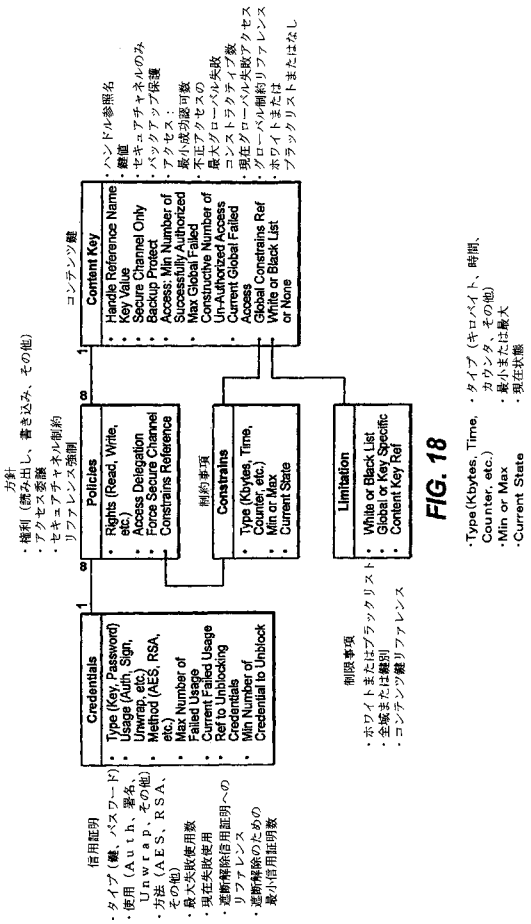


FIG. 18

【図１９】

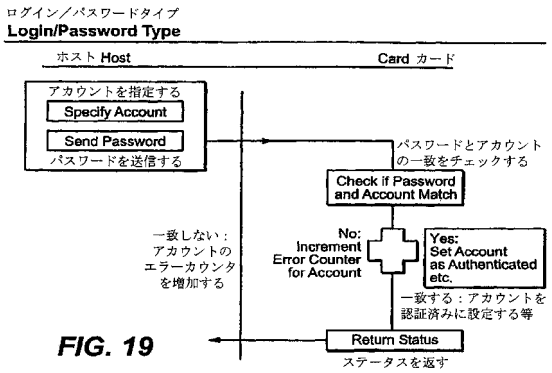


FIG. 19

【図２０】

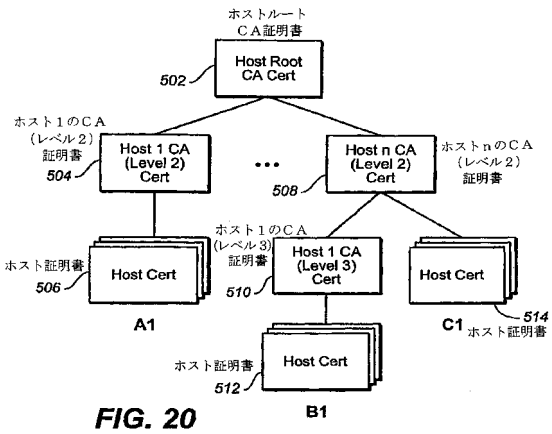


FIG. 20

【図２１】

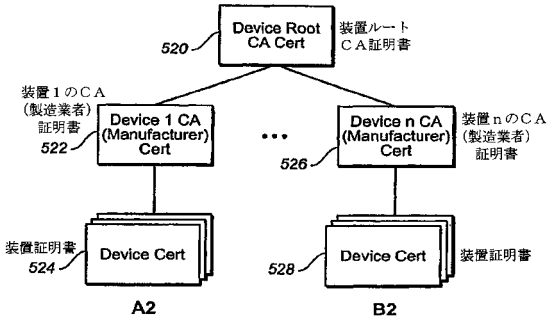
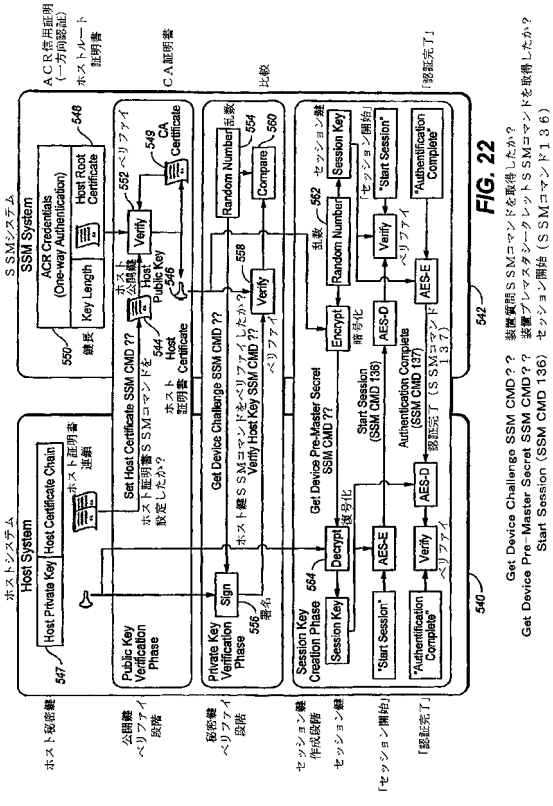
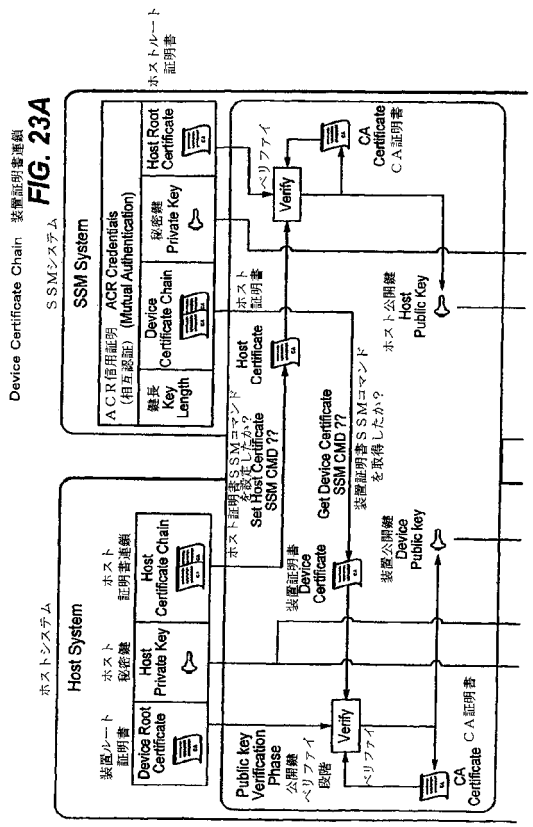


FIG. 21

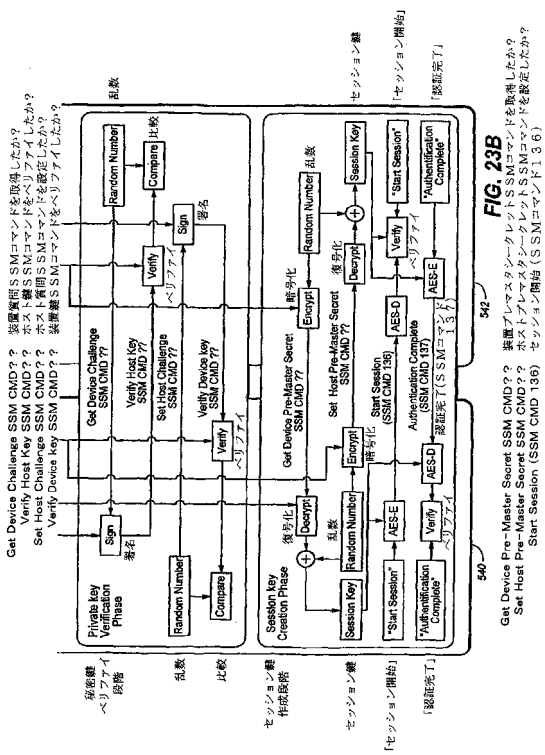
【図２２】



【図２３Ａ】



【図２３Ｂ】



【図２４】

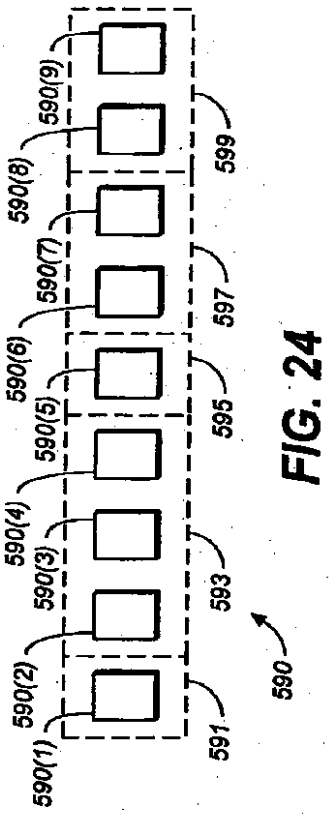


FIG. 24

【図２５】

バイトオフセット	引数長さ	引数名	引数型	注釈
0－1	2	バイト単位の証明書サイズ	整数	バイト単位の証明書鍵の長さ
2	1	「最終」フラグ	離散	このフラグは連鎖における現在の証明書が最終証明書かどうかを指示する

Byte Offset	Arg. Length	Argument Name	Arg. Type	Comments
0-1	2	Certificate Size in Bytes	Integer	Length of Certificate Key in Bytes
2	1	"Is Final" Flag	Discrete	This Flag Indicates if Current Certificate in the Chain is the Last One

FIG. 25

【図２６】

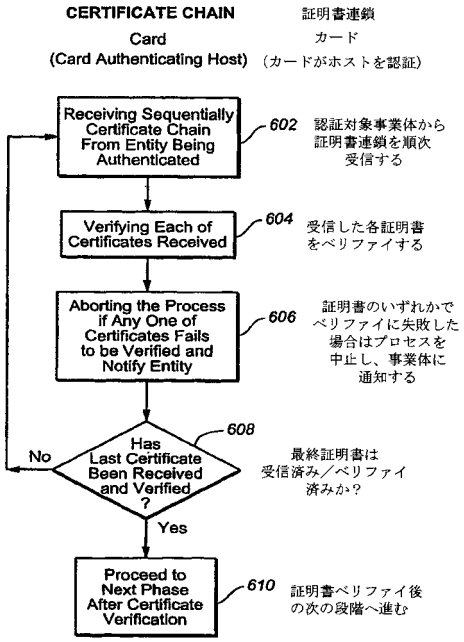


FIG. 26

【図２７】

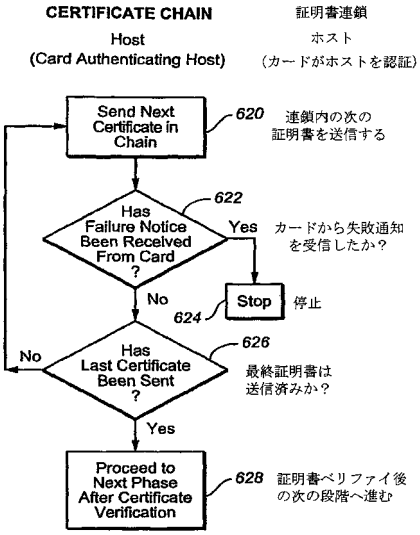


FIG. 27

【図２８】

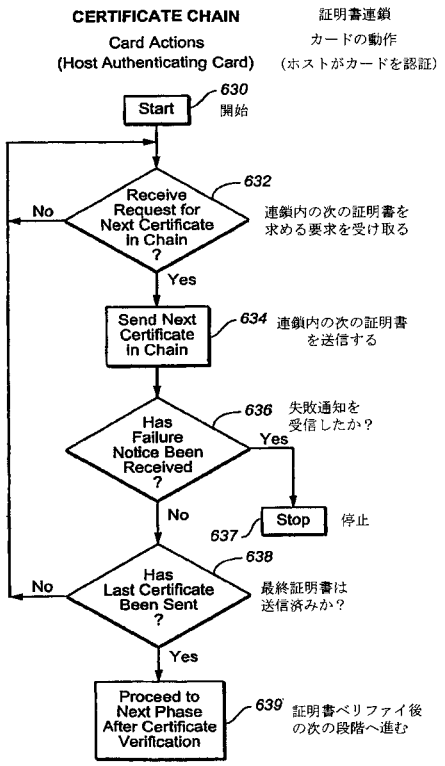


FIG. 28

【図２９】

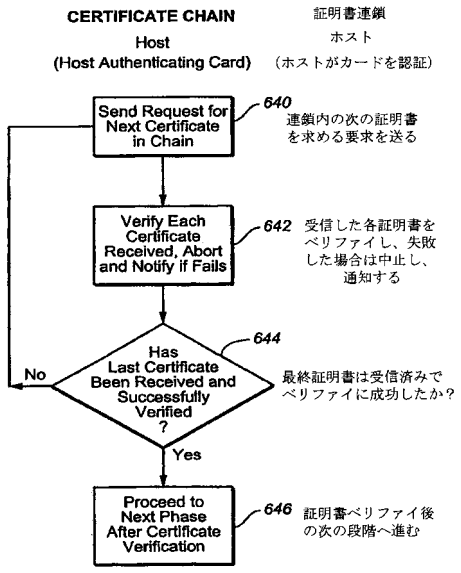


FIG. 29

【図３０】

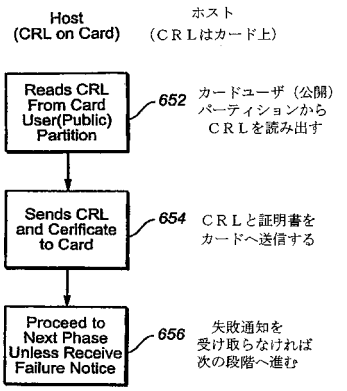


FIG. 30

【図３１】

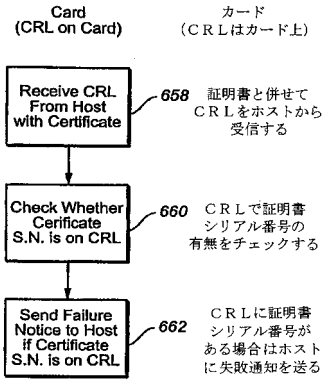


FIG. 31

【図３２】

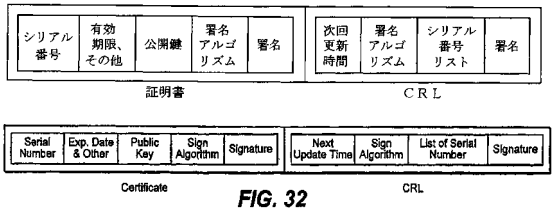


FIG. 32

【図３３】

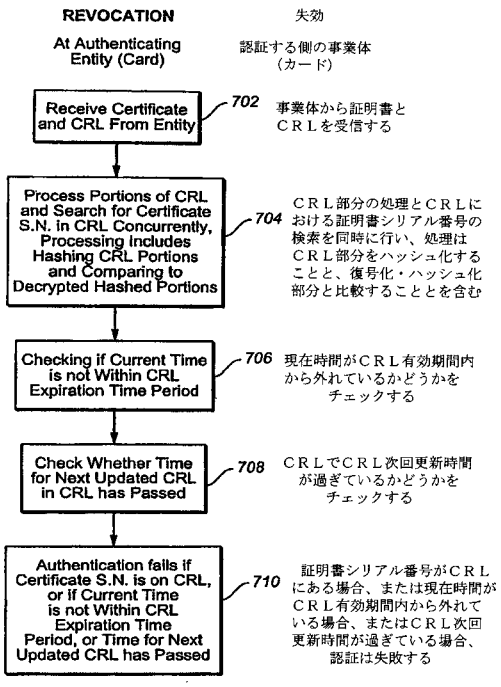


FIG. 33

【図３４】

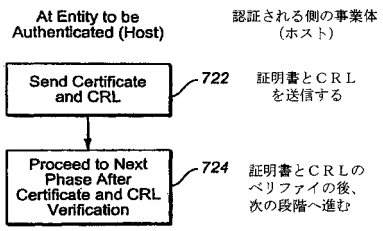


FIG. 34

【図３５】

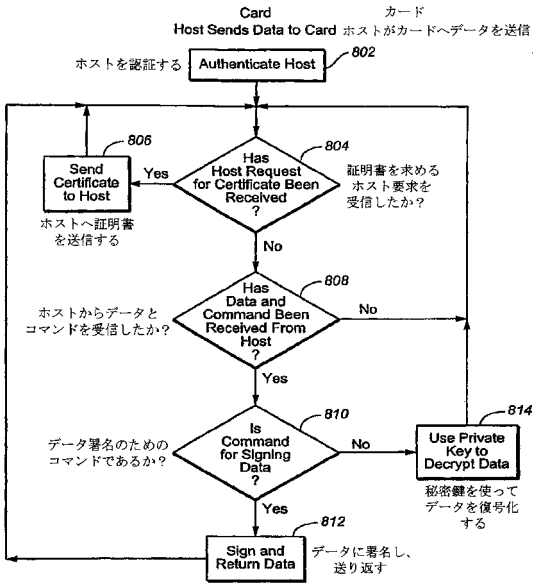


FIG. 35

【図３６】

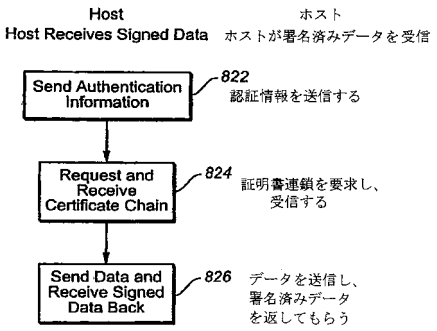


FIG. 36

【図３７】

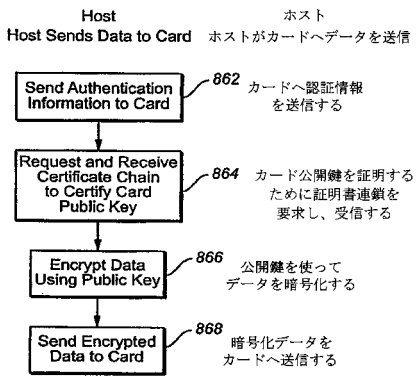


FIG. 37

【図３８】

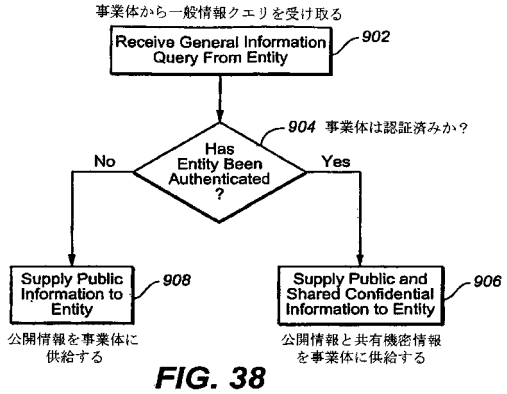


FIG. 38

【図３９】

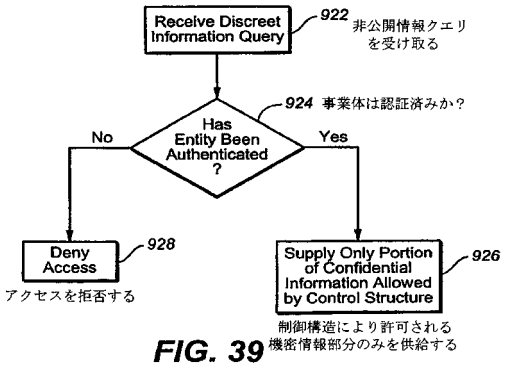


FIG. 39

【図４０Ａ】

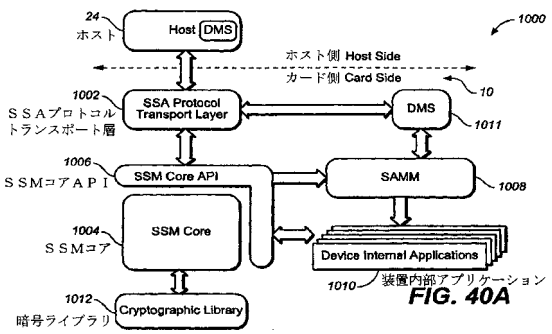


FIG. 40A

【図４０Ｂ】

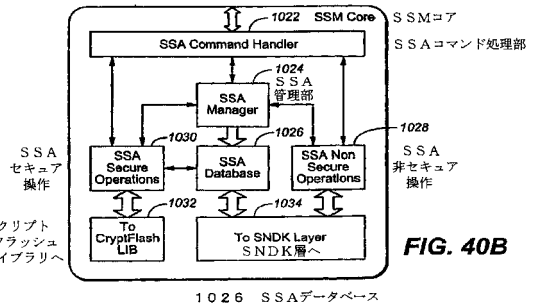


FIG. 40B

【図４１】

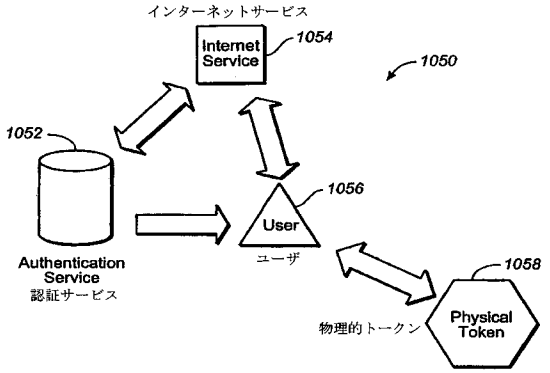
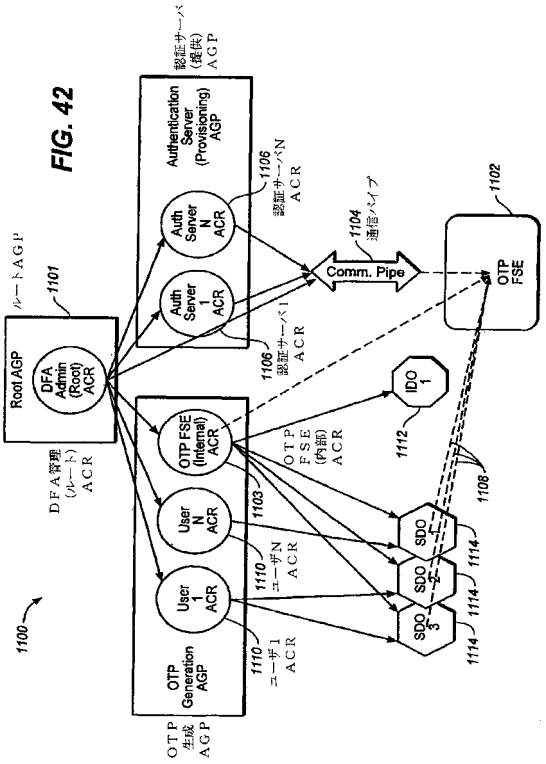


FIG. 41

【図４２】



【図４３】

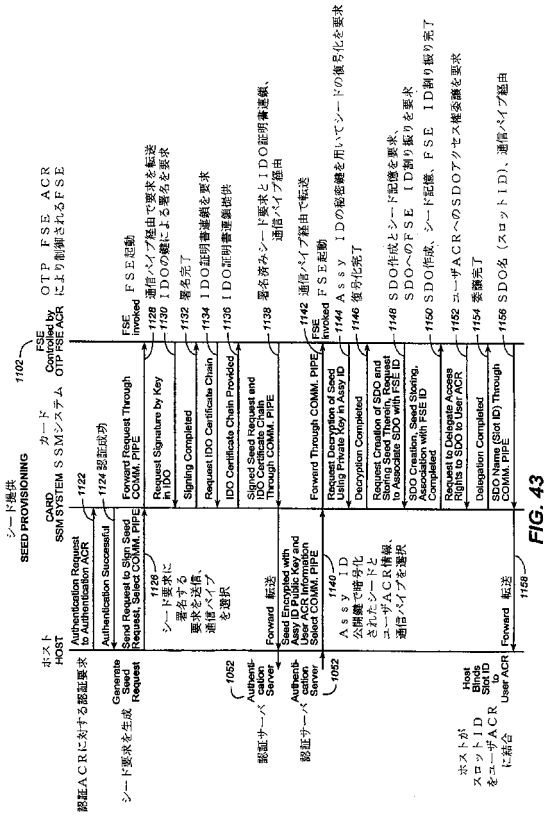


FIG. 43

【図４４】

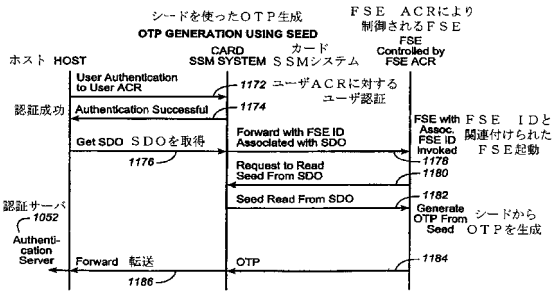


FIG. 44

1178 SDOに割り振られたFSE IDと併せて転送
1180 SDOからのシード読み出しを要求
1182 SDOから読み出されたシード

【図４５】

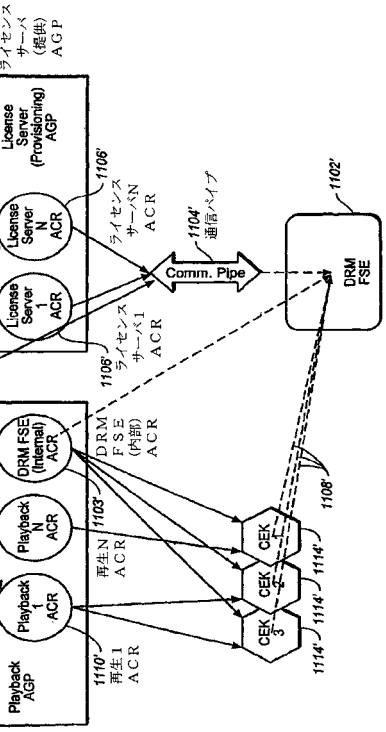


FIG. 45

【図４６】

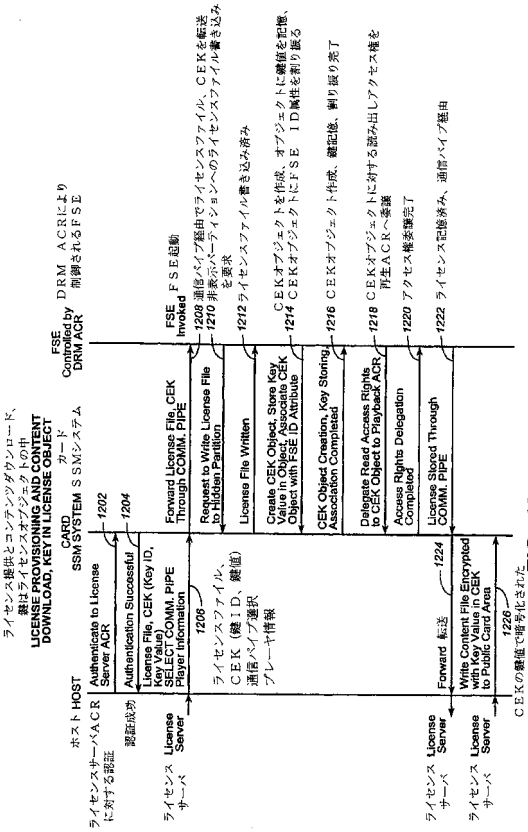


FIG. 46

【図４７】

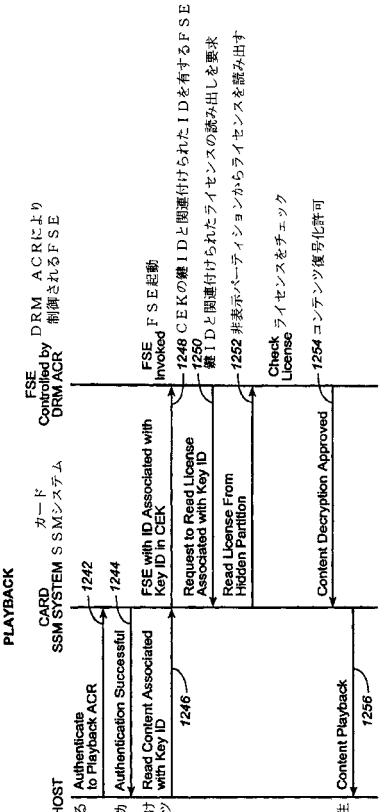


FIG. 47

【図４８】

FIG. 48

【手続補正書】
【提出日】平成21年5月18日(2009.5.18)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
第１の事業体を第２の事業体によって認証する方法であって、
第１の事業体と通信する第２の事業体によって実行されるステップと、
第２の事業体に対して第１の事業体を認証するため、順序付けられるとともにその順序で受信される複数の証明書を第１の事業体から受信するステップと、
受信される順に複数の証明書をベリファイするステップであって、複数の証明書のうちの最初の証明書はルート証明書と照らしてベリファイされる、ステップと、
複数の証明書のうちの最後の証明書がベリファイされたか否かを検出するステップと、
複数の証明書のうちの最後の証明書がベリファイされたならば、その最後の証明書を用いて第２の事業体に対して第１の事業体を認証するステップと、
を含む方法。
【請求項２】
請求項１記載の方法において、
複数の証明書のうちの最後の証明書は、これが最後の証明書であることの指示を収容するメッセージの中で受信され、前記検出するステップは、前記指示をチェックすることによって実行される方法。
【請求項３】
請求項１記載の方法において、
第１の事業体および第２の事業体は、互いに取り外し可能な状態で接続される方法。
【請求項４】
請求項１記載の方法において、
最後の証明書の受信後を除く各証明書の受信後に、複数の証明書のうちの次の証明書を求める要求を第１の事業体へ送信するステップをさらに含む方法。
【請求項５】
請求項４記載の方法において、
各要求に応じて、次の証明書を前記第１の事業体から受信するステップをさらに含む方法。
【請求項６】
請求項１記載の方法において、
第２の事業体はメモリ装置を備え、第１の事業体はホスト装置を備え、前記メモリ装置は取り外し可能な状態で前記ホスト装置へ接続される方法。
【請求項７】
請求項６記載の方法において、
第２の事業体は、メモリカードを備える方法。
【請求項８】
請求項１記載の方法において、
第２の事業体はメモリ装置を備え、前記方法は、複数の証明書のうちの最初の証明書を除き、事前に蓄積された証明書を上書きすることによって、一度に一つずつ複数の証明書をメモリ装置に蓄積するステップをさらに含む方法。
【請求項９】
請求項８記載の方法において、
メモリ装置で複数の証明書のうちのもっとも大きい証明書を蓄積するのに必要なメモリ

空間よりも多くのメモリ空間は割り当てないステップをさらに含む方法。
【請求項１０】
請求項１記載の方法において、
前記第１の事業体は、ホスト装置上で実行されるソフトウェアアプリケーションである方法。
【請求項１１】
請求項１記載の方法において、
前記第１の事業体は、ホスト装置に接続された遠隔サーバ上で実行されるソフトウェアアプリケーションである方法。
【請求項１２】
請求項１記載の方法において、
前記第１の事業体は、ホスト装置に接続された周辺装置上で実行されるソフトウェアアプリケーションである方法。
【請求項１３】
請求項１記載の方法において、
前記第１の事業体は、ホスト装置である方法。
【請求項１４】
請求項１記載の方法において、
前記第２の事業体は、記憶装置である方法。
【請求項１５】
請求項１記載の方法において、
前記第１の事業体は記憶装置であり、前記第２の事業体はホスト装置である方法。
【請求項１６】
請求項１記載の方法において、
第２の証明書から開始する各証明書は、直前に受信した証明書と照らしてベリファイされる方法。
【請求項１７】
請求項１記載の方法において、
第１の事業体に対して第２の事業体を認証するため、第２の複数の証明書を第１の事業体に送信するステップであって、第２の複数の証明書のうちの最後の証明書はこれが最後の証明書であることの指示に沿って送信される、ステップと、
第１の事業体から認証質問を受信するステップと、
前記第１の事業体からの認証質問に応じるステップと、
をさらに含む方法。
【請求項１８】
記憶システムであって、
ルート証明書を蓄積するメモリと、
メモリと通信するコントローラであって、
記憶システムに対して事業体を認証するため、順序付けられるとともにその順序で受信される複数の証明書を事業体から受信し、
受信される順に複数の証明書をベリファイし、複数の証明書のうちの最初の証明書はメモリに蓄積されたルート証明書に照らしてベリファイされ、
複数の証明書のうちの最後の証明書がベリファイされたか否かを検出し、
複数の証明書のうちの最後の証明書がベリファイされたならば、その最後の証明書を用いて記憶システムに対して事業体を認証するように操作されるコントローラと、
を備える記憶システム。
【請求項１９】
請求項１８記載の記憶システムにおいて、
複数の証明書のうちの最後の証明書は、これが最後の証明書であることの指示を収容するメッセージの中で受信され、前記コントローラは、前記指示をチェックすることによっ

て複数の証明書のうちの最後の証明書がベリファイされたか否かを検出するように操作される記憶システム。

【請求項２０】

請求項１８記載の記憶システムにおいて、

事業体および記憶システムは、互いに取り外し可能な状態で接続される記憶システム。

【請求項２１】

請求項１８記載の記憶システムにおいて、

前記コントローラは、最後の証明書の受信後を除く各証明書の受信後に、複数の証明書のうちの次の証明書を求める要求を事業体へ送信するように操作される記憶システム。

【請求項２２】

請求項２１記載の記憶システムにおいて、

各要求に応じて、次の証明書を事業体から受信するように操作される記憶システム。

【請求項２３】

請求項１８記載の記憶システムにおいて、

記憶システムはメモリ装置を備え、事業体はホスト装置を備え、前記メモリ装置は取り外し可能な状態で前記ホスト装置へ接続される記憶システム。

【請求項２４】

請求項２３記載の記憶システムにおいて、

記憶システムは、メモリカードを備える記憶システム。

【請求項２５】

請求項１８記載の記憶システムにおいて、

前記コントローラは、複数の証明書のうちの最初の証明書を除き、事前に蓄積された証明書を上書きすることによって、一度に一つずつ複数の証明書のそれぞれをメモリに蓄積するように操作される記憶システム。

【請求項２６】

請求項２５記載の記憶システムにおいて、

前記コントローラは、メモリで複数の証明書のうちのもっとも大きい証明書を蓄積するのに必要なメモリ空間よりも多くのメモリ空間は割り当てないように操作される記憶システム。

【請求項２７】

請求項１８記載の記憶システムにおいて、

前記コントローラは、

事業体に対して記憶システムを認証するため、第２の複数の証明書を事業体に送信し、第２の複数の証明書のうちの最後の証明書はこれが最後の証明書であることの指示に沿って送信され、

事業体から認証質問を受信し、

前記事業体からの認証質問に応じるように操作される記憶システム。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/015304

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00 H04L29/06

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04L H04N

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 6 513 116 B1 (VALENTE LUIS [US]) 28 January 2003 (2003-01-28) claims 5,6,18; figure 4 paragraphs [0011] - [0013] paragraphs [0046] - [0048] paragraphs [0060] - [0073]	1,11,12 2-10, 13-46
Y	WO 02/096016 A (THOMSON LICENSING SA [FR]; LESENNE LAURENT [FR]; PASQUIER FREDERIC [FR) 28 November 2002 (2002-11-28) page 1, lines 19-26 page 41, line 34 - page 43, line 4	1-46
Y	WO 2006/069311 A (SANDISK CORP [US]; JOGAND-COULUMB FABRICE [US]; HOLTZMAN MICHAEL [US];) 29 June 2006 (2006-06-29) paragraphs [0171] - [0174]; figures 1,2	1-46

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance.

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 March 2008	25/03/2008

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

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/015304

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	LLOYD S ET AL: "Understanding Certification Path Construction" INTERNET CITATION, [Online] September 2002 (2002-09), XP002307946 Retrieved from the Internet: URL:http://www.pkiforum.org/pdfs/Understanding_Path_construction-DS2.pdf> [retrieved on 2004-11-29] pages 1,3; figure 2	1-46
A	DONNAN R A: "TRANSMISSION SYNCHRONIZING METHOD" IBM TECHNICAL DISCLOSURE BULLETIN, IBM CORP. NEW YORK, US, vol. 11, no. 11, April 1969 (1969-04), page 1570, XP000809093 ISSN: 0018-8689 the whole document	1,4
A	EP 1 361 527 A (SONY ERICSSON MOBILE COMM AB [SE]) 12 November 2003 (2003-11-12) paragraphs [0004], [0016], [0027]	1-46
A	US 6 189 097 B1 (TYCKSEN JR FRANK A [US] ET AL) 13 February 2001 (2001-02-13) figures 1,4,9	1-46

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2007/015304

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6513116 B1	28-01-2003	NONE	
WO 02096016 A	28-11-2002	CN 1526217 A	01-09-2004
		DE 60203509 D1	04-05-2005
		DE 60203509 T2	23-02-2006
		EP 1402679 A2	31-03-2004
		ES 2240751 T3	16-10-2005
		FR 2825209 A1	29-11-2002
		JP 2004527188 T	02-09-2004
		MX PA03010564 A	02-03-2004
		US 2004162980 A1	19-08-2004
WO 2006069311 A	29-06-2006	EP 1836642 A2	26-09-2007
		KR 20070087175 A	27-08-2007
EP 1361527 A	12-11-2003	AU 2003229687 A1	11-11-2003
		CN 1653460 A	10-08-2005
		WO 03096238 A1	20-11-2003
		JP 2005524910 T	18-08-2005
		KR 20050026924 A	16-03-2005
US 6189097 B1	13-02-2001	NONE	

フロントページの続き

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

(72)発明者 セラ，ロテム
イスラエル国、６１６４、マーロット、カティフ １７
(72)発明者 ジョガンドークーロン，ファブリス
アメリカ合衆国、９４０７０、カリフォルニア州、サン カルロス、バックランド アベニュー８５５

Ｆターム(参考) 5B285 AA01 BA08 CA02 CA41 CA44 CB47 CB55 CB62 CB72
5J104 AA07 AA08 AA12 AA16 EA05 EA08 EA16 JA21 KA02 LA03
NA02 NA33 NA37 NA38 PA07