【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成24年4月12日(2012.4.12)

【公表番号】特表2009-543210(P2009-543210A)
【公表日】平成21年12月3日(2009.12.3)
【年通号数】公開・登録公報2009-048
【出願番号】特願2009-518355(P2009-518355)
【国際特許分類】
Ｇ０６Ｆ　21/24　　(2006.01)
Ｇ０６Ｆ　12/00　　(2006.01)
Ｇ０６Ｆ　21/20　　(2006.01)
Ｇ０６Ｆ　21/00　　(2006.01)
Ｇ０６Ｋ　19/073　　(2006.01)
Ｈ０４Ｌ　 9/32　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　12/14　　５４０Ｐ
Ｇ０６Ｆ　12/00　　５３７Ｈ
Ｇ０６Ｆ　12/14　　５４０Ｂ
Ｇ０６Ｆ　15/00　　３３０Ｇ
Ｇ０６Ｆ　15/00　　３３０Ｚ
Ｇ０６Ｋ　19/00　　Ｐ
Ｈ０４Ｌ　 9/00　　６７５Ｂ

【誤訳訂正書】
【提出日】平成24年2月24日(2012.2.24)
【誤訳訂正１】
【訂正対象書類名】明細書
【訂正対象項目名】０００７
【訂正方法】変更
【訂正の内容】
【０００７】
用途によっては、メモリカード等のメモリ装置と関連付けられた実体に自身のアイデンティティの証拠を提示することが求められる。このアイデンティティの証拠を容易く入手できないと不都合が生じることがある。この他にも用途によっては、メモリカード等のメモリ装置に記憶されるデータを安全な方法で保護することが必要な場合がある。
【誤訳訂正２】
【訂正対象書類名】明細書
【訂正対象項目名】００１１
【訂正方法】変更
【訂正の内容】
【００１１】
さらに別の実施形態において、メモリシステムの制御データ構造によって実体が認証された後に、アイデンティティオブジェクトの公開鍵と、公開鍵を証明するための少なくとも１つの証明書とを、実体へ提供する。この実施形態の一実用的応用において、アイデンティティオブジェクトの公開鍵によって暗号化された暗号化データを実体から受信する場合、メモリシステムは、アイデンティティオブジェクトの中にある秘密鍵を使って暗号化データを復号化できる。アイデンティティオブジェクトと少なくとも１つの証明書とが不揮発性メモリに記憶され、このメモリはコントローラによって制御される。好ましくは、メモリとコントローラとを筐体で取り囲む。

【誤訳訂正３】
【訂正対象書類名】明細書
【訂正対象項目名】００１４
【訂正方法】変更
【訂正の内容】
【００１４】
【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チェーンを示す図である。
【図２１】多数のデバイス証明書チェーンを示す図である。
【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、証明書チェーンの図である。
【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チェーン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。
【誤訳訂正４】
【訂正対象書類名】明細書
【訂正対象項目名】００１９
【訂正方法】変更
【訂正の内容】
【００１９】
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実体のみとなる。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。
【誤訳訂正５】
【訂正対象書類名】明細書
【訂正対象項目名】００２８
【訂正方法】変更
【訂正の内容】
【００２８】
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。これらの実体は、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実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実体はまず、「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、そのような実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。
【誤訳訂正６】
【訂正対象書類名】明細書
【訂正対象項目名】００２９
【訂正方法】変更
【訂正の内容】

【００２９】
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
実体	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

【誤訳訂正７】
【訂正対象書類名】明細書
【訂正対象項目名】００３３
【訂正方法】変更
【訂正の内容】
【００３３】
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はいずれの実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。
【誤訳訂正８】
【訂正対象書類名】明細書
【訂正対象項目名】００３５
【訂正方法】変更
【訂正の内容】
【００３５】
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、いずれの実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はいずれの実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実体でない限り、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、権限を有する実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。

【誤訳訂正９】
【訂正対象書類名】明細書
【訂正対象項目名】００３７
【訂正方法】変更
【訂正の内容】
【００３７】
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実体であればいずれでもこれにアクセスできる。

【誤訳訂正１０】
【訂正対象書類名】明細書
【訂正対象項目名】００３８
【訂正方法】変更
【訂正の内容】
【００３８】
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、鍵の使用を望む実体は、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。

【誤訳訂正１１】
【訂正対象書類名】明細書
【訂正対象項目名】００５０
【訂正方法】変更
【訂正の内容】
【００５０】
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、いったん実体（敵対的な実体、またはそうでない実体）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。

【誤訳訂正１２】
【訂正対象書類名】明細書
【訂正対象項目名】００５１
【訂正方法】変更
【訂正の内容】

【００５１】
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実体は、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。
【誤訳訂正１３】
【訂正対象書類名】明細書
【訂正対象項目名】００５４
【訂正方法】変更
【訂正の内容】
【００５４】
ＳＳＡシステムにアクセスする場合、実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。
【誤訳訂正１４】
【訂正対象書類名】明細書
【訂正対象項目名】００５６
【訂正方法】変更
【訂正の内容】
【００５６】
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、実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。
【誤訳訂正１５】
【訂正対象書類名】明細書
【訂正対象項目名】００５７
【訂正方法】変更
【訂正の内容】
【００５７】
ＳＳＡシステムのＡＣＲにログインした実体の権限、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。
【誤訳訂正１６】
【訂正対象書類名】明細書

【訂正対象項目名】００６１
【訂正方法】変更
【訂正の内容】
【００６１】
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。完全に独立した実体、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。
【誤訳訂正１７】
【訂正対象書類名】明細書
【訂正対象項目名】００６２
【訂正方法】変更
【訂正の内容】
【００６２】
実体にとってのＳＳＡの入口：アクセス制御記録（ＡＣＲ）
ＳＳＡシステムのＡＣＲは、実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実体は、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。ホスト側実体はすべてのＡＣＲデータフィールドを提供する。
【誤訳訂正１８】
【訂正対象書類名】明細書
【訂正対象項目名】００６３
【訂正方法】変更
【訂正の内容】
【００６３】
ＡＣＲへのログインに成功した実体は、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システムの実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。
【誤訳訂正１９】
【訂正対象書類名】明細書
【訂正対象項目名】００６４

【訂正方法】変更
【訂正の内容】
【００６４】
ログイン／認証アルゴリズム
実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。
【誤訳訂正２０】
【訂正対象書類名】明細書
【訂正対象項目名】００６５
【訂正方法】変更
【訂正の内容】
【００６５】
信用証明
実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。
【誤訳訂正２１】
【訂正対象書類名】明細書
【訂正対象項目名】００６６
【訂正方法】変更
【訂正の内容】
【００６６】
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実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、実体－ＡＣＲ属性の管理権限の３種類がある。
【誤訳訂正２２】
【訂正対象書類名】明細書
【訂正対象項目名】００６７
【訂正方法】変更
【訂正の内容】
【００６７】
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実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。
【誤訳訂正２３】
【訂正対象書類名】明細書
【訂正対象項目名】００６９

【訂正方法】変更
【訂正の内容】
【００６９】
鍵ＩＤアクセス
ＰＣＲのこの部分には、実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実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。
【誤訳訂正２４】
【訂正対象書類名】明細書
【訂正対象項目名】００７６
【訂正方法】変更
【訂正の内容】
【００７６】
ＡＣＲの遮断と解除
システムによる実体の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。
【誤訳訂正２５】
【訂正対象書類名】明細書
【訂正対象項目名】００７８
【訂正方法】変更
【訂正の内容】
【００７８】
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実体でも認証なしで、あるいはシステムＡＣＲ（後述）を通じて認証されたユーザ／実体が、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実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。

【誤訳訂正２６】
【訂正対象書類名】明細書
【訂正対象項目名】００７９
【訂正方法】変更
【訂正の内容】
【００７９】
この機能は２つのＳＳＡコマンドで制御する（これらコマンドはいずれのユーザ／実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。
【誤訳訂正２７】
【訂正対象書類名】明細書
【訂正対象項目名】００８０
【訂正方法】変更
【訂正の内容】
【００８０】
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実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。
【誤訳訂正２８】
【訂正対象書類名】明細書
【訂正対象項目名】００８６
【訂正方法】変更
【訂正の内容】
【００８６】
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実体を識別するために使われる。
【誤訳訂正２９】
【訂正対象書類名】明細書
【訂正対象項目名】００８９
【訂正方法】変更
【訂正の内容】
【００８９】
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はホストを通じて実体から提供され、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、チェーン、およびハッシュモード）

【誤訳訂正３０】
【訂正対象書類名】明細書
【訂正対象項目名】００９３
【訂正方法】変更
【訂正の内容】
【００９３】
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実体は、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）。
【誤訳訂正３１】
【訂正対象書類名】明細書
【訂正対象項目名】００９４
【訂正方法】変更
【訂正の内容】
【００９４】
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を有する実体は、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。
【誤訳訂正３２】
【訂正対象書類名】明細書
【訂正対象項目名】００９５
【訂正方法】変更
【訂正の内容】
【００９５】
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。実体はまず、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。

【誤訳訂正３３】
【訂正対象書類名】明細書
【訂正対象項目名】００９６
【訂正方法】変更
【訂正の内容】
【００９６】
図１４は、鍵と鍵ＩＤを作成するプロセスを示す。実体はＡＣＲを通じて認証を受ける（ブロック３０２）。実体は、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、実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。

【誤訳訂正３４】
【訂正対象書類名】明細書
【訂正対象項目名】００９７
【訂正方法】変更
【訂正の内容】
【００９７】
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。実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。この場合は実体の認証が行われ、実体はＡＣＲを指定する（ブロック３３０、３３２）。実体はターゲット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。

【誤訳訂正３５】
【訂正対象書類名】明細書
【訂正対象項目名】００９８
【訂正方法】変更
【訂正の内容】
【００９８】
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実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、実体は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。

【誤訳訂正３６】
【訂正対象書類名】明細書
【訂正対象項目名】００９９
【訂正方法】変更
【訂正の内容】
【００９９】
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実体が対応し、コマンドは、この実体の認証に用いる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。

【誤訳訂正３７】
【訂正対象書類名】明細書
【訂正対象項目名】０１００
【訂正方法】変更
【訂正の内容】
【０１００】

複数の実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、実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。

【誤訳訂正３８】
【訂正対象書類名】明細書
【訂正対象項目名】０１０１
【訂正方法】変更
【訂正の内容】
【０１０１】

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。実体の権限は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。

【誤訳訂正３９】
【訂正対象書類名】明細書
【訂正対象項目名】０１０２
【訂正方法】変更
【訂正の内容】
【０１０２】
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、好ましくは実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

たは多数の実体環境に使用される。
【誤訳訂正４０】
【訂正対象書類名】明細書
【訂正対象項目名】０１０４
【訂正方法】変更
【訂正の内容】
【０１０４】
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実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）を終えた実体は、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実体を（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。
【誤訳訂正４１】
【訂正対象書類名】明細書
【訂正対象項目名】０１０６
【訂正方法】変更
【訂正の内容】
【０１０６】
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、実体もセッション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、要求する実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、実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。
【誤訳訂正４２】
【訂正対象書類名】明細書
【訂正対象項目名】０１０７
【訂正方法】変更

【訂正の内容】
【０１０７】
ＳＳＡシステムは、コマンドが実際に正しい認証済み実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。
【誤訳訂正４３】
【訂正対象書類名】明細書
【訂正対象項目名】０１０８
【訂正方法】変更
【訂正の内容】
【０１０８】
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．実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。ある特定の実体が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。
【誤訳訂正４４】
【訂正対象書類名】明細書
【訂正対象項目名】０１０９
【訂正方法】変更
【訂正の内容】
【０１０９】
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機構による実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。実体が鍵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。
【誤訳訂正４５】
【訂正対象書類名】明細書
【訂正対象項目名】０１１０
【訂正方法】変更
【訂正の内容】
【０１１０】
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、実体は、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。
【誤訳訂正４６】
【訂正対象書類名】明細書
【訂正対象項目名】０１１１
【訂正方法】変更
【訂正の内容】
【０１１１】
乱数生成
外部実体は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。
【誤訳訂正４７】
【訂正対象書類名】明細書
【訂正対象項目名】０１１３
【訂正方法】変更
【訂正の内容】
【０１１３】
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実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実体（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実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、特定の実体のみが特定の鍵・パーティションにアクセスでき、特定の実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実体は問わず、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。
【誤訳訂正４８】
【訂正対象書類名】明細書
【訂正対象項目名】０１１４
【訂正方法】変更
【訂正の内容】
【０１１４】
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。実体はアカウント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、実体にはアカウント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。
【誤訳訂正４９】
【訂正対象書類名】明細書
【訂正対象項目名】０１２１
【訂正方法】変更
【訂正の内容】
【０１２１】
ＳＳＡは証明書チェーンに対応する。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。この証明書チェーンアルゴリズムでは、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。
【誤訳訂正５０】
【訂正対象書類名】明細書
【訂正対象項目名】０１２２
【訂正方法】変更
【訂正の内容】
【０１２２】
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、証明書チェーン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。
【誤訳訂正５１】
【訂正対象書類名】明細書
【訂正対象項目名】０１２４
【訂正方法】変更
【訂正の内容】
【０１２４】
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）アクセスを試みる実体から提供される証明書／証明書チェーンとに基づき、ホストを認証する。
【誤訳訂正５２】
【訂正対象書類名】明細書
【訂正対象項目名】０１２５
【訂正方法】変更
【訂正の内容】
【０１２５】
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を末端実体証明書までつなげる証明書チェーン）を保持するすべての実体が、末端実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。
【誤訳訂正５３】
【訂正対象書類名】明細書
【訂正対象項目名】０１２６
【訂正方法】変更
【訂正の内容】
【０１２６】
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実体になる。
【誤訳訂正５４】
【訂正対象書類名】明細書
【訂正対象項目名】０１２７
【訂正方法】変更
【訂正の内容】
【０１２７】
ホストルート証明書
ルート証明書は、ログインを試みる実体（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、信用された実体（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。

【誤訳訂正５５】
【訂正対象書類名】明細書
【訂正対象項目名】０１２８
【訂正方法】変更
【訂正の内容】
【０１２８】
ホスト証明書チェーン
これらの証明書は認証中にＳＳＡへ提供される。チェーンの処理が完了した後にホストの証明書チェーンを再度集めて装置に記憶することはしない。

【誤訳訂正５６】
【訂正対象書類名】明細書
【訂正対象項目名】０１２９
【訂正方法】変更
【訂正の内容】
【０１２９】
図２０は、多数のホスト証明書チェーンを示す、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チェーンを有することがあり、ここでは３つの証明書チェーン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

【誤訳訂正５７】
【訂正対象書類名】明細書
【訂正対象項目名】０１３０
【訂正方法】変更
【訂正の内容】
【０１３０】
前述した３つの証明書チェーン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チェーンを例示するものである。図２０と前述した証明書チェーン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の公開鍵を有する実体は、前述した証明書チェーンＡ１の信憑性をベリファイできることになる。この実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、実体は次に、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。証明書チェーンＢ１およびＣ１を使った認証も同様に行われる

。
【誤訳訂正５８】
【訂正対象書類名】明細書
【訂正対象項目名】０１３１
【訂正方法】変更
【訂正の内容】
【０１３１】
チェーン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実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、ホストが実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）証明書はチェーン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実体、すなわちこの場合のメモリ装置１０はまず、チェーン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。証明書チェーンが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、認証の対象となる実体の証明書で終わる。
【誤訳訂正５９】
【訂正対象書類名】明細書
【訂正対象項目名】０１３２
【訂正方法】変更
【訂正の内容】
【０１３２】
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／証明書チェーン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。
【誤訳訂正６０】
【訂正対象書類名】明細書
【訂正対象項目名】０１３３
【訂正方法】変更
【訂正の内容】
【０１３３】
装置証明書チェーン
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チェーンを処理できるが、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チェーンを送信できるが、証明書チェーンデータを使用するわけではないので、証明書チェーンを解析する必要はない。
【誤訳訂正６１】
【訂正対象書類名】明細書
【訂正対象項目名】０１３４
【訂正方法】変更
【訂正の内容】
【０１３４】

図２１は、ＳＳＡを使用する記憶装置等の装置で１～ｎ通りの証明書チェーンを示す、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通りの証明書チェーン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

【誤訳訂正６２】
【訂正対象書類名】明細書
【訂正対象項目名】０１３８
【訂正方法】変更
【訂正の内容】
【０１３８】

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チェーンを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。

【誤訳訂正６３】
【訂正対象書類名】明細書
【訂正対象項目名】０１４１
【訂正方法】変更
【訂正の内容】
【０１４１】

図２４は、本発明の一実施形態を例示する証明書チェーン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チェーンは多数の証明書を含むことがある。図２４の証明書チェーンは全部で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、送信される証明書チェーンに不備があったり、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、チェーン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チェーン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。

【誤訳訂正６４】
【訂正対象書類名】明細書
【訂正対象項目名】０１４２
【訂正方法】変更
【訂正の内容】
【０１４２】

本発明の一実施形態は、証明書チェーン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チェーン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、証明書のチェーン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。これで証明書チェーン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チェーン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、チェーン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。

【誤訳訂正６５】
【訂正対象書類名】明細書
【訂正対象項目名】０１４３
【訂正方法】変更
【訂正の内容】
【０１４３】
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に対してチェーン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。チェーン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。

【誤訳訂正６６】
【訂正対象書類名】明細書
【訂正対象項目名】０１４４
【訂正方法】変更
【訂正の内容】
【０１４４】
メモリ装置は、チェーン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、これがチェーン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チェーン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、チェーンの中で証明書５９０（９）が最後の証明書であることをベリファイできる。

【誤訳訂正６７】
【訂正対象書類名】明細書
【訂正対象項目名】０１４５
【訂正方法】変更
【訂正の内容】
【０１４５】
代替的な実施形態では、チェーン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。チェーン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、チェーンの中で該当する１列の先行列に隣接する証明書（先頭証明書）と、チェーンの中で該当する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、チェーン内の最後の証明書には標識、例えばこれがチェーン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。

【誤訳訂正６８】
【訂正対象書類名】明細書
【訂正対象項目名】０１４６
【訂正方法】変更
【訂正の内容】
【０１４６】
好ましくは、ホストによって送信されるチェーン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。

【誤訳訂正６９】
【訂正対象書類名】明細書
【訂正対象項目名】０１４７
【訂正方法】変更
【訂正の内容】
【０１４７】
図２６のフローチャートは、前述した証明書チェーン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チェーン内の証明書を順次送信する。チェーンの中の第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チェーンを順次受信する（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。

【誤訳訂正７０】
【訂正対象書類名】明細書
【訂正対象項目名】０１４８
【訂正方法】変更
【訂正の内容】
【０１４８】
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、ホストはチェーン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、チェーン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。チェーン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、チェーン内の次の証明書を送信する。
【誤訳訂正７１】
【訂正対象書類名】明細書
【訂正対象項目名】０１４９
【訂正方法】変更
【訂正の内容】
【０１４９】
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、チェーン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、カードはチェーン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、チェーン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）。
【誤訳訂正７２】
【訂正対象書類名】明細書
【訂正対象項目名】０１５０
【訂正方法】変更
【訂正の内容】
【０１５０】
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、チェーン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、チェーン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）。
【誤訳訂正７３】
【訂正対象書類名】明細書
【訂正対象項目名】０１５７
【訂正方法】変更
【訂正の内容】
【０１５７】
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実体が、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実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。
【誤訳訂正７４】
【訂正対象書類名】明細書

【訂正対象項目名】０１５８
【訂正方法】変更
【訂正の内容】
【０１５８】
一実施形態において、認証を受けようとする実体が、認証の対象となる証明書と併せて証明書失効リストを、認証する側の実体、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。認証する側の実体は、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。認証する側の実体は、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。
【誤訳訂正７５】
【訂正対象書類名】明細書
【訂正対象項目名】０１５９
【訂正方法】変更
【訂正の内容】
【０１５９】
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、証明書チェーンと対応する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チェーンと併せてＣＲＬをホスト装置に提示する必要はない。
【誤訳訂正７６】
【訂正対象書類名】明細書
【訂正対象項目名】０１６４
【訂正方法】変更
【訂正の内容】
【０１６４】
図３３および図３４は、前述した失効制度の特徴を示す。認証する側の実体（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実体から証明書と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、認証を受ける側の実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、認証する側の実体は、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。
【誤訳訂正７７】
【訂正対象書類名】明細書
【訂正対象項目名】０１６５
【訂正方法】変更
【訂正の内容】
【０１６５】
認証を受けようとする実体（例えば、ホスト）は、その証明書とＣＲＬを認証する側の実体へ送信し（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。

実体が認証のために証明書チェーンを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、チェーン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、証明書チェーンの残りの部分とその対応するＣＲＬの受信を待たずにすむ。

【誤訳訂正７８】
【訂正対象書類名】明細書
【訂正対象項目名】０１６６
【訂正方法】変更
【訂正の内容】
【０１６６】
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の証明書チェーン）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、外部実体や内部カード実体（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実体であることが分かる。

【誤訳訂正７９】
【訂正対象書類名】明細書
【訂正対象項目名】０１６８
【訂正方法】変更
【訂正の内容】
【０１６８】
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の認証を受ける実体に対して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チェーンを提供する。

【誤訳訂正８０】
【訂正対象書類名】明細書

【訂正対象項目名】０１６９
【訂正方法】変更
【訂正の内容】
【０１６９】
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チェーンである。
【誤訳訂正８１】
【訂正対象書類名】明細書
【訂正対象項目名】０１７１
【訂正方法】変更
【訂正の内容】
【０１７１】
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チェーンを送信する必要がある場合、チェーン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。
【誤訳訂正８２】
【訂正対象書類名】明細書
【訂正対象項目名】０１７２
【訂正方法】変更
【訂正の内容】
【０１７２】
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、ホストは証明書チェーンを求める要求をカードへ送り、チェーンを受け取る（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）。
【誤訳訂正８３】
【訂正対象書類名】明細書
【訂正対象項目名】０１７３

【訂正方法】変更
【訂正の内容】
【０１７３】
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チェーン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）。
【誤訳訂正８４】
【訂正対象書類名】明細書
【訂正対象項目名】０１７５
【訂正方法】変更
【訂正の内容】
【０１７５】
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実体にとっての専有情報が入り、それぞれの実体は自身の専有情報に限りアクセスが認められ、他の実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。
【誤訳訂正８５】
【訂正対象書類名】明細書
【訂正対象項目名】０１７７
【訂正方法】変更
【訂正の内容】
【０１７７】
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実体は最初に、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。認証に成功した実体は、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。
【誤訳訂正８６】
【訂正対象書類名】明細書
【訂正対象項目名】０１８５
【訂正方法】変更
【訂正の内容】
【０１８５】
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、実体から一般情報クエリを受け取ったＳＳＡシステムは（９０２）、その実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実体に供給する（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実体に供給する（ブロック９０８）。
【誤訳訂正８７】
【訂正対象書類名】明細書

【訂正対象項目名】０１８６
【訂正方法】変更
【訂正の内容】
【０１８６】
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、実体から非公開情報クエリを受け取ったＳＳＡシステムは（９２２）、その実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、システムは実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実体のアクセスを拒否する（ブロック（９２８）。
【誤訳訂正８８】
【訂正対象書類名】明細書
【訂正対象項目名】０１９１
【訂正方法】変更
【訂正の内容】
【０１９１】
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：認可された実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。
【誤訳訂正８９】
【訂正対象書類名】明細書
【訂正対象項目名】０２００
【訂正方法】変更
【訂正の内容】
【０２００】
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実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。パイプを作る実体（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。
【誤訳訂正９０】
【訂正対象書類名】明細書
【訂正対象項目名】０２０１
【訂正方法】変更
【訂正の内容】
【０２０１】
認証済みの実体は、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、実体がパイプの所有者か、あるいはそのＰ

ＣＲ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。

【誤訳訂正９１】
【訂正対象書類名】明細書
【訂正対象項目名】０２０４
【訂正方法】変更
【訂正の内容】
【０２０４】
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。実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実体（すなわち、この実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。

【誤訳訂正９２】
【訂正対象書類名】明細書
【訂正対象項目名】０２０９
【訂正方法】変更
【訂正の内容】
【０２０９】
内部ＡＣＲ

内部ＡＣＲはＰＣＲを有するＡＣＲに類似するが、装置１０にとって外部の実体はこの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。アクセスを試みる実体はカードまたはメモリ装置にとって内部の実体であるため、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。

【誤訳訂正９３】
【訂正対象書類名】明細書
【訂正対象項目名】０２１６
【訂正方法】変更
【訂正の内容】
【０２１６】
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。ホスト側実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。

【誤訳訂正９４】
【訂正対象書類名】明細書
【訂正対象項目名】０２２１

【訂正方法】変更
【訂正の内容】
【０２２１】
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実体である。図４２に示すＦＳＥ１１０２もカード側で様々な動作をとる実体である。
【誤訳訂正９５】
【訂正対象書類名】明細書
【訂正対象項目名】０２２３
【訂正方法】変更
【訂正の内容】
【０２２３】
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の証明書チェーンを要求する（矢印１１３４）。これに応じて、ＳＳＭシステムは、ＡＣＲ１１０３の制御下でＩＤＯの証明書チェーンを提供する。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の証明書チェーンを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証明書チェーンの送信は、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。
【誤訳訂正９６】
【訂正対象書類名】明細書
【訂正対象項目名】０２２４
【訂正方法】変更
【訂正の内容】
【０２２４】
ホストが受け取った署名済みシード要求とＩＤＯ証明書チェーンは、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チェーン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。

【誤訳訂正９７】
【訂正対象書類名】明細書
【訂正対象項目名】０２３３
【訂正方法】変更
【訂正の内容】
【０２３３】
前述した実施形態から提供される別の利点として、ユーザ等の外部実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。

【誤訳訂正９８】
【訂正対象書類名】明細書
【訂正対象項目名】０２３４
【訂正方法】変更
【訂正の内容】
【０２３４】
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実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。

【誤訳訂正９９】
【訂正対象書類名】特許請求の範囲
【訂正対象項目名】全文
【訂正方法】変更
【訂正の内容】
【特許請求の範囲】
【請求項１】
不揮発性記憶装置であって、
コントローラと、
秘密鍵と公開鍵とを備える鍵対と、前記鍵対を認証するための証明書とを記憶する不揮発性メモリと、
実体を認証するための前記コントローラによって使用可能な情報と、さらに前記実体が前記コントローラによって認証され次第、前記実体を許可できるかどうかを判断して前記鍵対と証明書とにアクセスするための前記コントローラによって使用可能な情報とを含むアクセス制御構造と、を備え、
前記コントローラは、
前記アクセス制御構造を用いて前記不揮発性記憶装置に対して実体を認証し、
前記実体が成功裏に認証された後、データとコマンドを受信して前記実体からのデータに署名し、

秘密鍵を使用してデータまたは前記データから検索される情報に署名し、
前記証明書と前記データまたは前記データから検索される情報とを前記実体へ送信するように操作される不揮発性記憶装置。
【請求項２】
請求項１記載の不揮発性記憶装置において、
前記不揮発性メモリとコントローラとを囲い込む筐体をさらに備える不揮発性記憶装置。
【請求項３】
請求項２記載の不揮発性記憶装置において、
前記筐体は、カードの形状を有する不揮発性記憶装置。
【請求項４】
請求項１記載の不揮発性記憶装置において、
前記証明書は、証明書チェーンである不揮発性メモリシステム。
【請求項５】
請求項１記載の不揮発性記憶装置において、
前記不揮発性メモリは、フラッシュメモリである不揮発性記憶装置。
【請求項６】
請求項１記載の不揮発性記憶装置において、
前記アクセス制御構造によって、認証済み実体のみがデータにアクセスできる不揮発性記憶装置。
【請求項７】
請求項１記載の不揮発性記憶装置において、
前記コントローラは、前記アクセス制御構造を用いて実体を認証し、公開鍵を証明するために前記証明書を認証済み実体に供給する不揮発性記憶装置。
【請求項８】
実体のアイデンティティの証拠を提供する方法であって、
（ｉ）コントローラと、（ｉｉ）秘密鍵と公開鍵とを備える鍵対と、前記鍵対を認証するための証明書とを記憶する不揮発性メモリと、（ｉｉｉ）実体を認証するための前記コントローラによって使用可能な情報と、さらに前記実体が前記コントローラによって認証され次第、前記実体を許可できるかどうかを判断して前記鍵対と証明書とにアクセスするための前記コントローラによって使用可能な情報とを含むアクセス制御構造とを備える不揮発性記憶装置内で次のステップを実行するステップであって、
前記アクセス制御構造を用いて前記不揮発性記憶装置に対して実体を認証するステップと、
前記実体が成功裏に認証された後、
データとコマンドを受信して前記実体からのデータに署名するステップと、
秘密鍵を使用してデータまたは前記データから検索される情報に署名するステップと、
前記証明書と前記データまたは前記データから検索される情報とを前記実体へ送信するステップと、
を含む方法。
【請求項９】
請求項８記載の方法において、
前記実体が成功裏に認証された後、公開鍵を証明するために前記証明書を実体に供給するステップと、
公開鍵によって暗号化されたデータを受信するステップと、
秘密鍵を用いてデータを復号化するステップと、
をさらに含む方法。
【請求項１０】
請求項８記載の方法において、

前記不揮発性記憶装置は、前記不揮発性メモリとコントローラとを囲い込む筐体を備える方法。
【請求項１１】
請求項１０記載の方法において、
前記筐体は、カードの形状を有する方法。
【請求項１２】
請求項８記載の方法において、
前記証明書は、証明書チェーンである方法。
【請求項１３】
請求項８記載の方法において、
前記不揮発性メモリは、フラッシュメモリである方法。
【請求項１４】
請求項８記載の方法において、
前記アクセス制御構造によって、認証済み実体のみがデータにアクセスできる方法。
【請求項１５】
請求項８記載の方法において、
前記コントローラは、前記アクセス制御構造を用いて実体を認証し、公開鍵を証明するために前記証明書を認証済み実体に供給する方法。
【請求項１６】
請求項１記載の不揮発性記憶装置において、
前記実体は、取り外し可能な状態で記憶装置へ接続されるホスト装置を備える不揮発性記憶装置。
【請求項１７】
請求項８記載の方法において、
前記実体は、取り外し可能な状態で記憶装置へ接続されるホスト装置を備える方法。
【誤訳訂正１００】
【訂正対象書類名】図面
【訂正対象項目名】図２２
【訂正方法】変更
【訂正の内容】

【図２２】

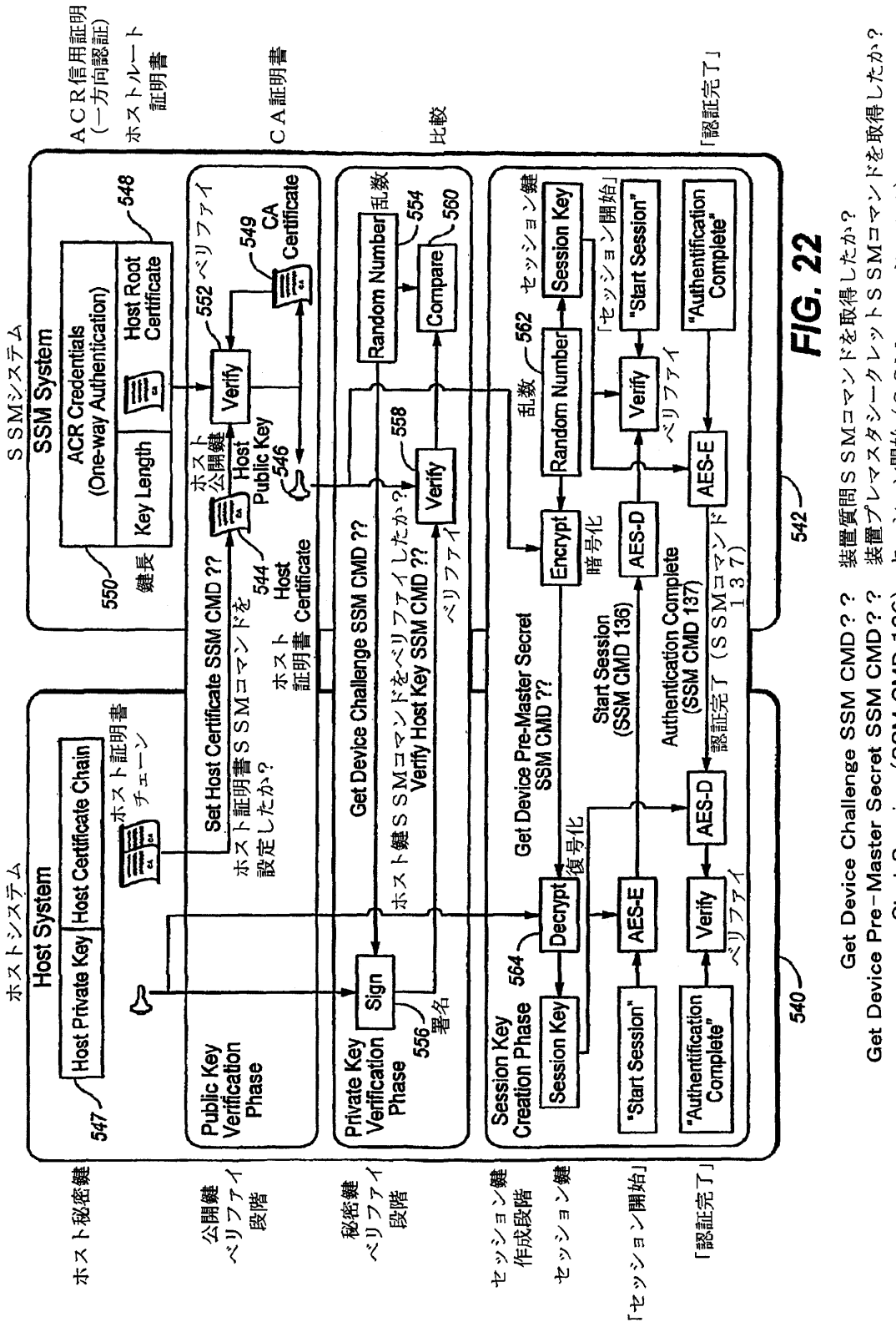
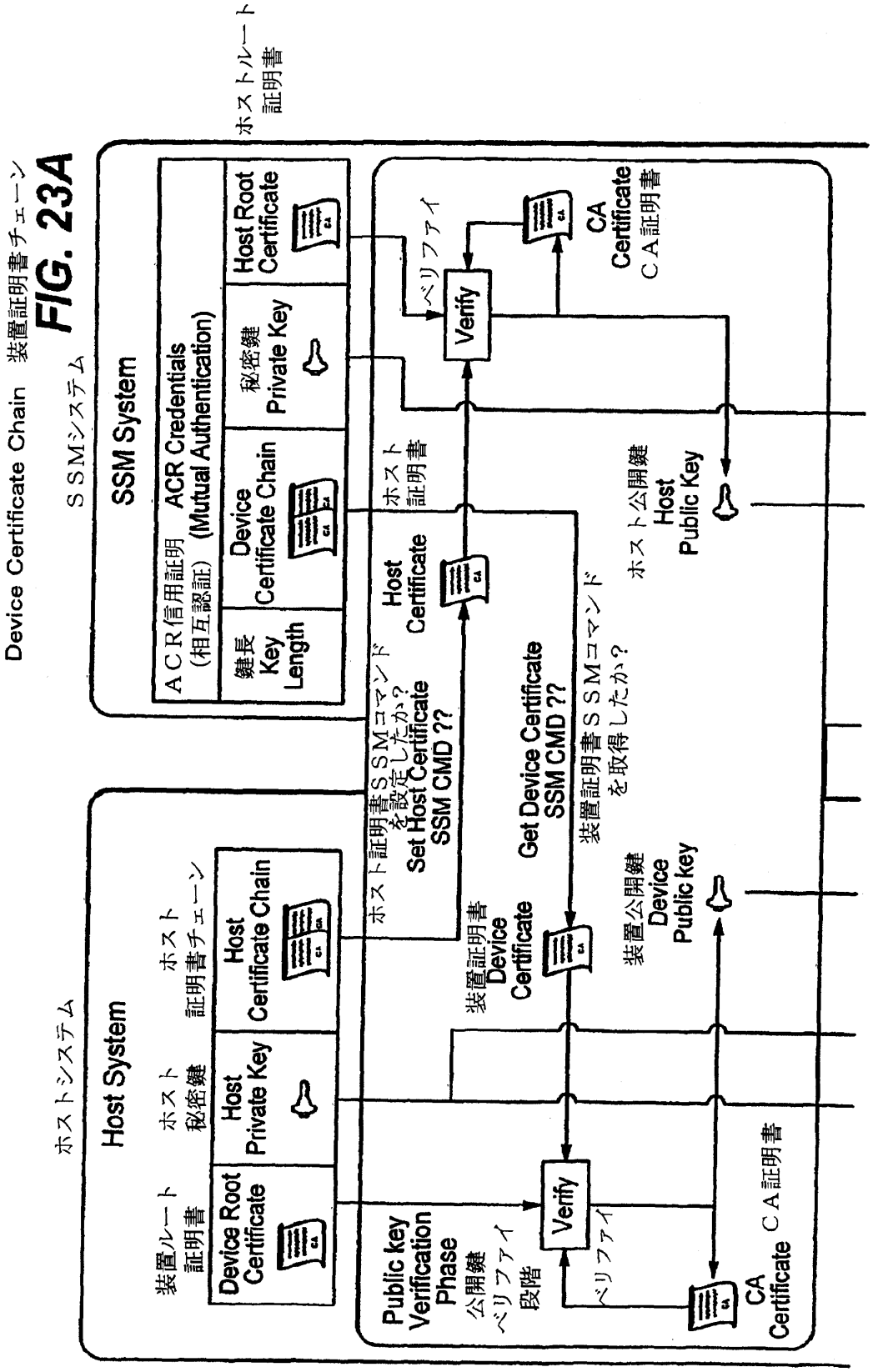


FIG. 22

Get Device Challenge SSM CMD？？　装置質問ＳＳＭコマンドを取得したか？
Get Device Pre-Master Secret SSM CMD？？　装置プレマスタシークレットＳＳＭコマンドを取得したか？
Start Session (SSM CMD 136)　セッション開始（ＳＳＭコマンド１３６）

【誤訳訂正１０１】
【訂正対象書類名】図面
【訂正対象項目名】図２３Ａ
【訂正方法】変更
【訂正の内容】

【図２３Ａ】



【誤訳訂正１０２】
【訂正対象書類名】図面
【訂正対象項目名】図２５
【訂正方法】変更
【訂正の内容】

【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	このフラグはチェーンに 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

【誤訳訂正１０３】
【訂正対象書類名】図面
【訂正対象項目名】図２６
【訂正方法】変更
【訂正の内容】

【図２６】

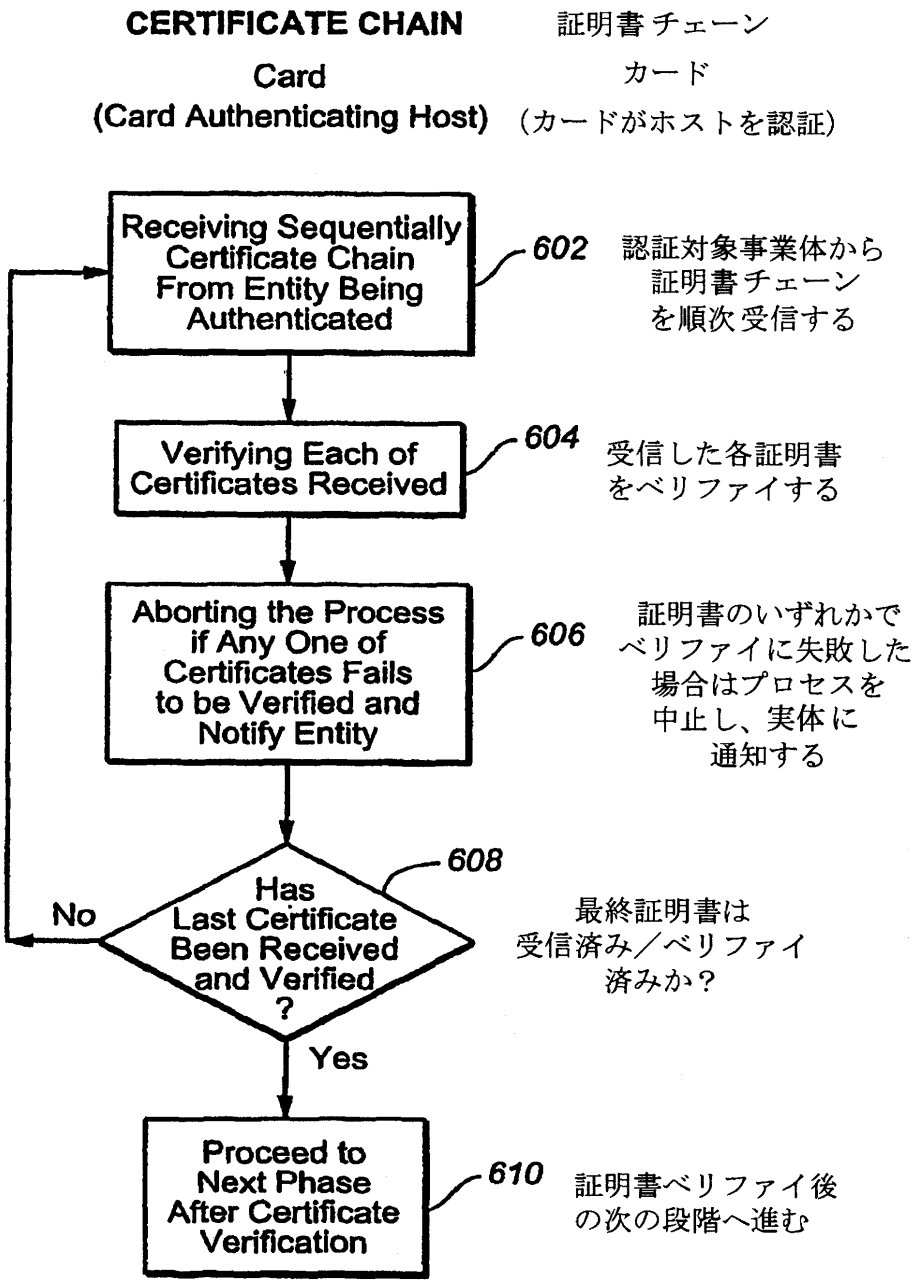


FIG. 26

【誤訳訂正１０４】
【訂正対象書類名】図面
【訂正対象項目名】図２７
【訂正方法】変更
【訂正の内容】

【図２７】

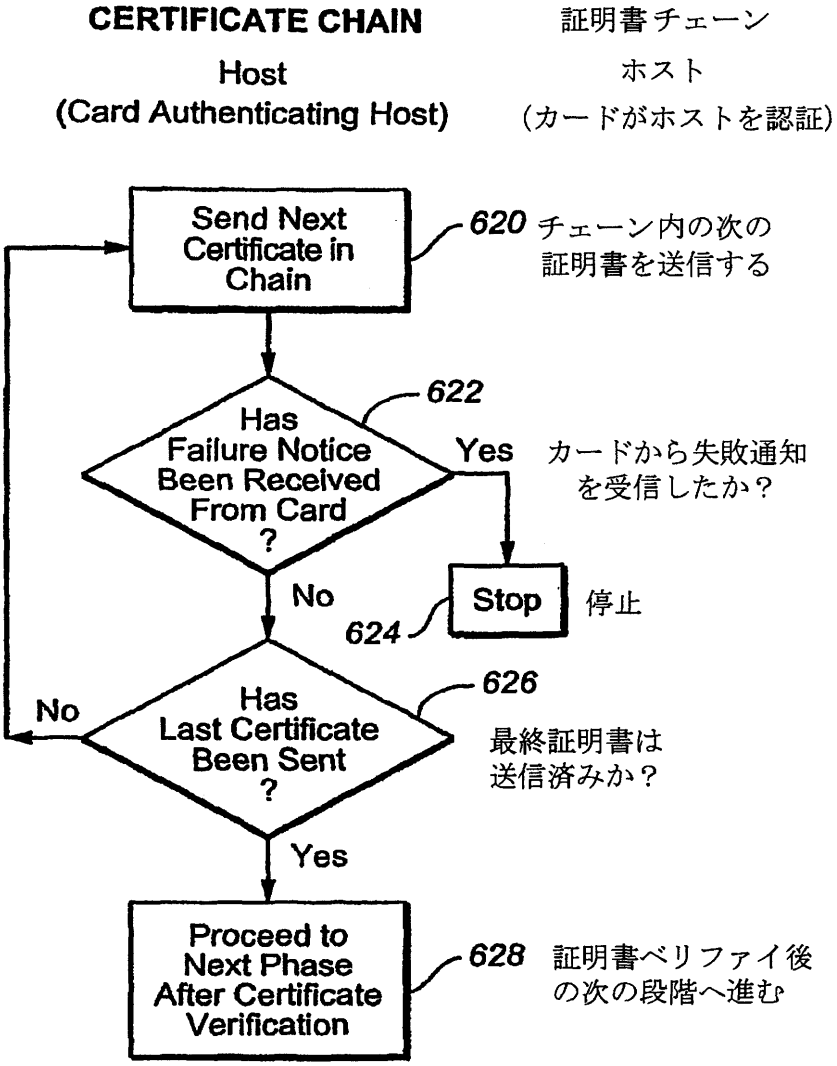


FIG. 27

【誤訳訂正１０５】
【訂正対象書類名】図面
【訂正対象項目名】図２８
【訂正方法】変更
【訂正の内容】

【図２８】

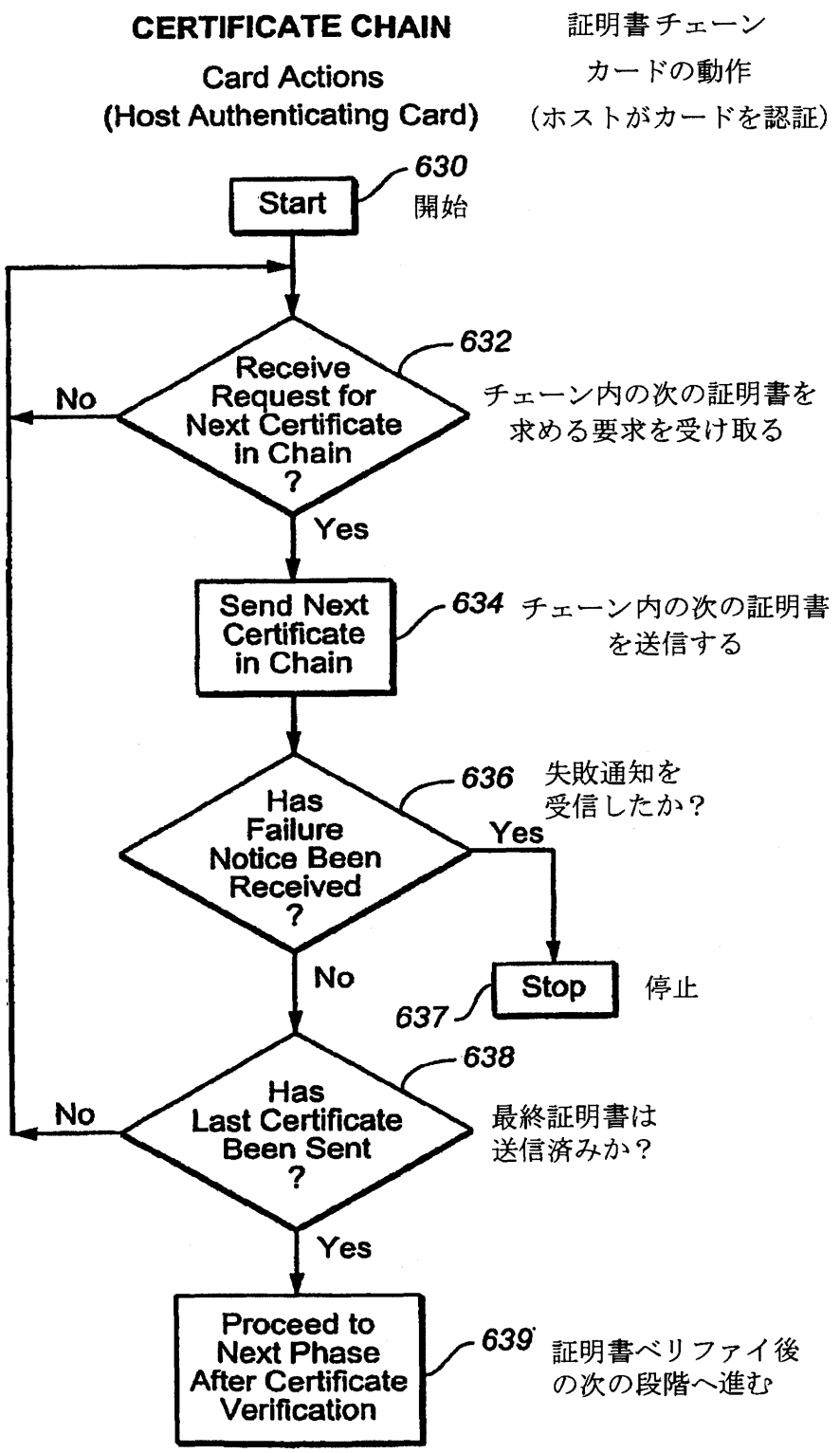


FIG. 28

【誤訳訂正１０６】
【訂正対象書類名】図面
【訂正対象項目名】図２９
【訂正方法】変更
【訂正の内容】

【図２９】

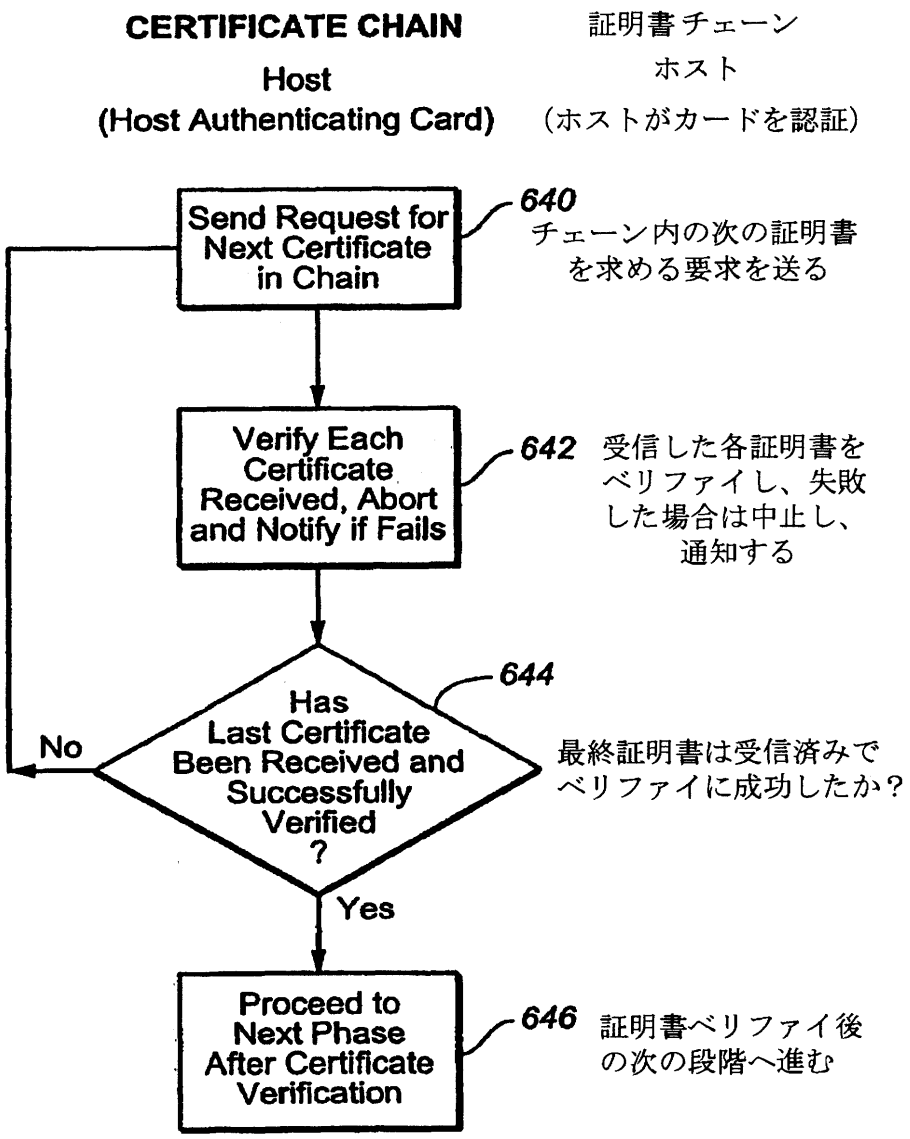


FIG. 29

【誤訳訂正１０７】
【訂正対象書類名】図面
【訂正対象項目名】図３３
【訂正方法】変更
【訂正の内容】

【図３３】

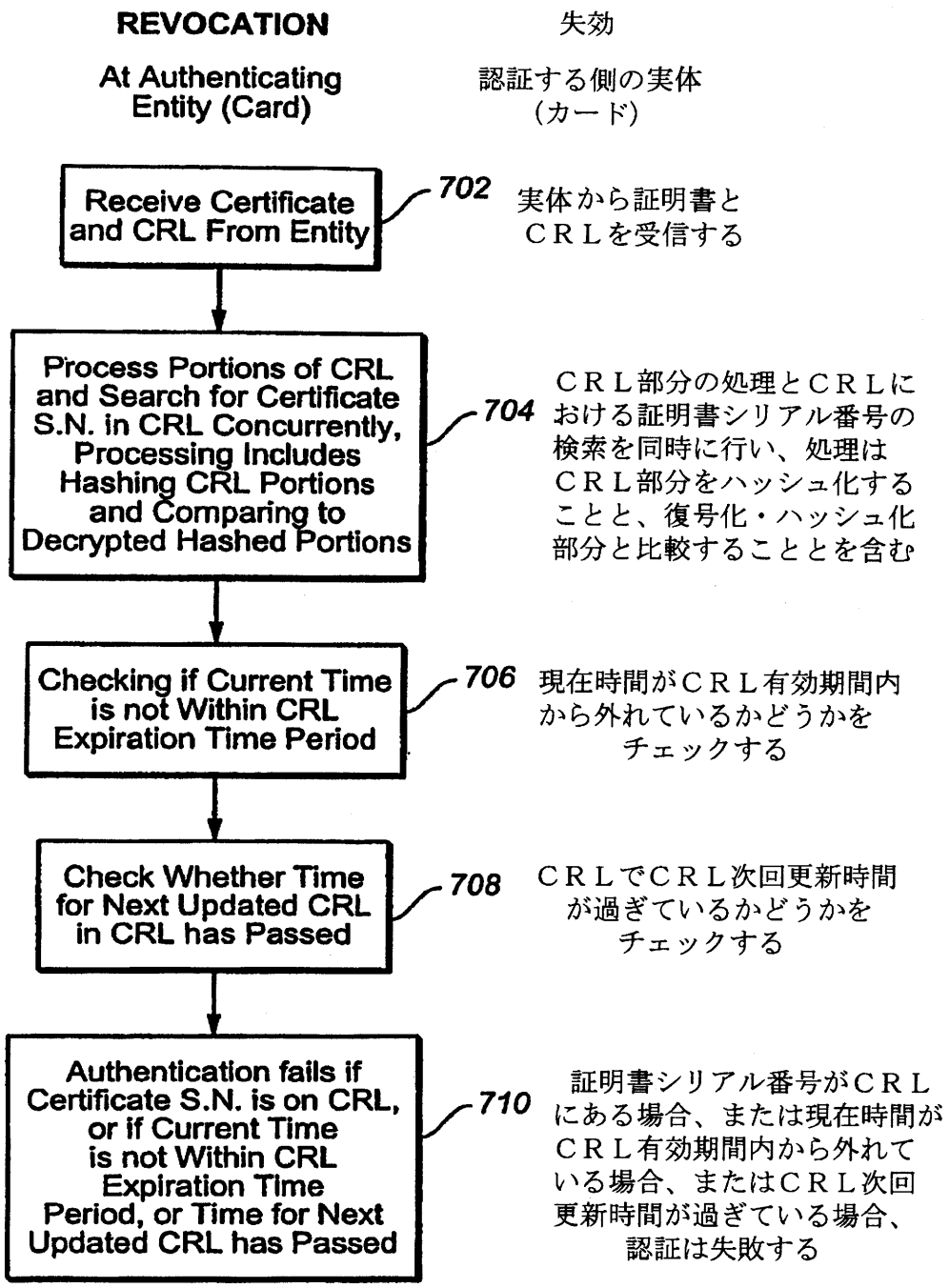


FIG. 33

【誤訳訂正１０８】
【訂正対象書類名】図面
【訂正対象項目名】図３４
【訂正方法】変更
【訂正の内容】

【図３４】

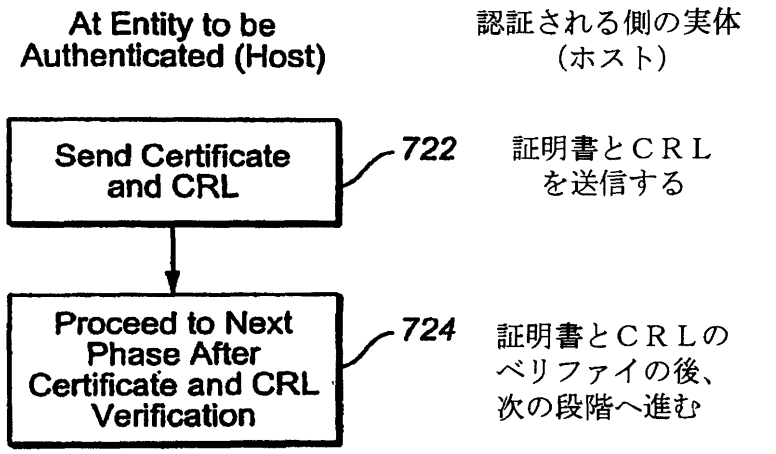


FIG. 34

【誤訳訂正１０９】
【訂正対象書類名】図面
【訂正対象項目名】図３６
【訂正方法】変更
【訂正の内容】
【図３６】

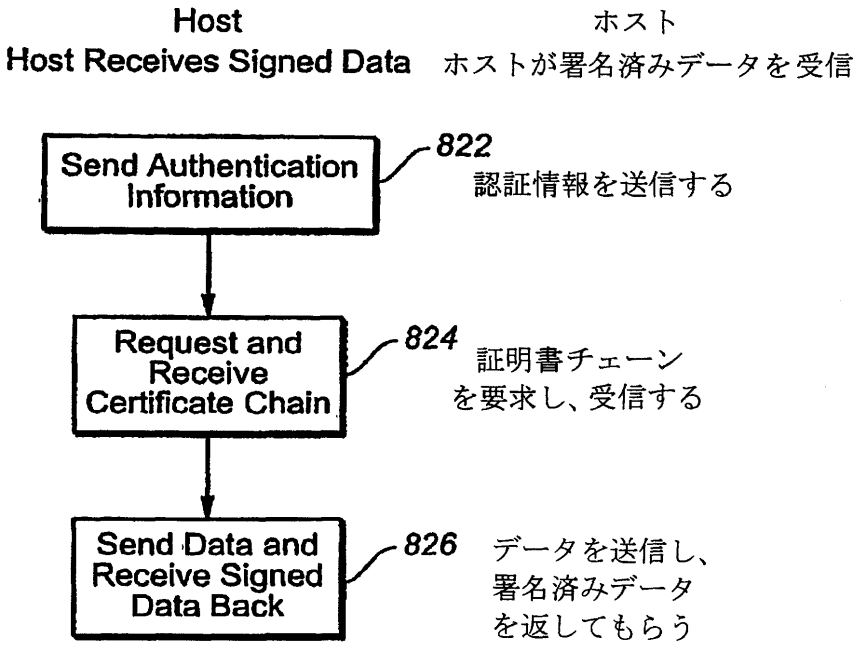


FIG. 36

【誤訳訂正１１０】
【訂正対象書類名】図面
【訂正対象項目名】図３７
【訂正方法】変更
【訂正の内容】
【図３７】

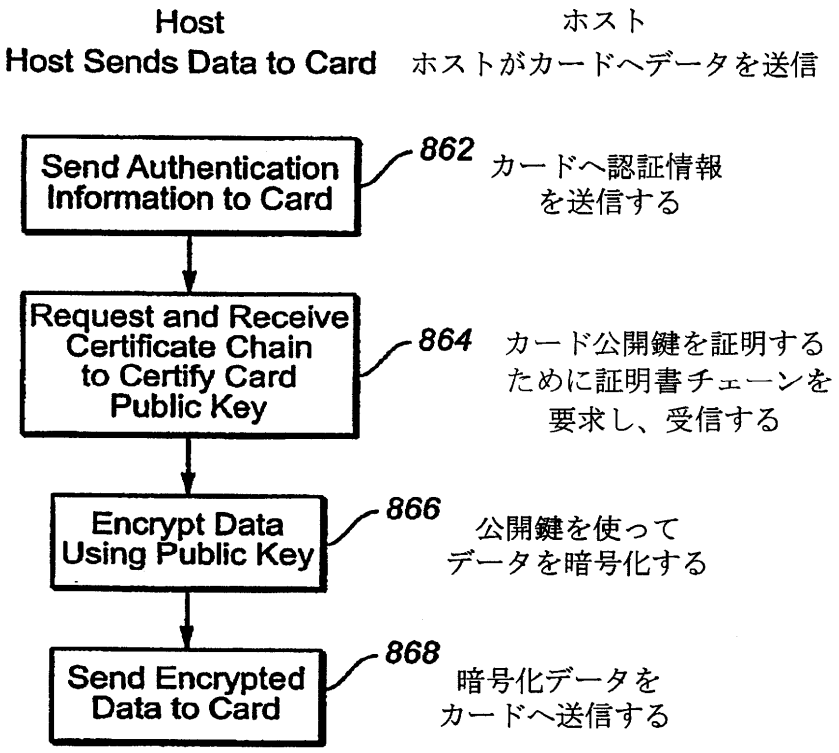


FIG. 37

【誤訳訂正１１１】
【訂正対象書類名】図面
【訂正対象項目名】図３８
【訂正方法】変更
【訂正の内容】

【図３８】

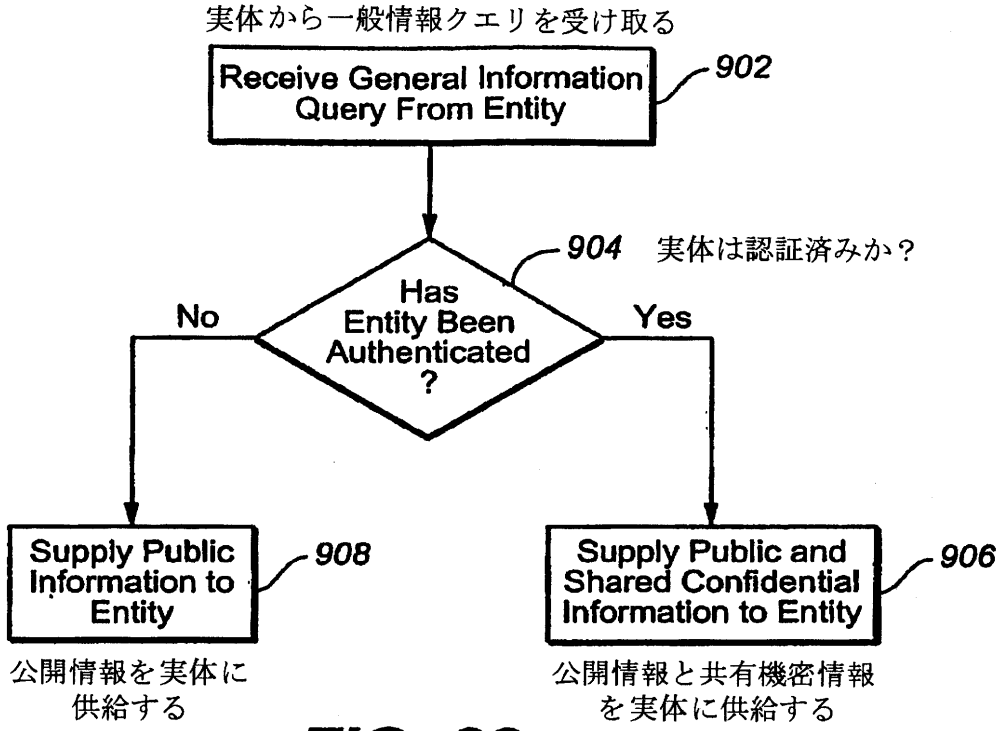


FIG. 38

【誤訳訂正１１２】
【訂正対象書類名】図面
【訂正対象項目名】図３９
【訂正方法】変更
【訂正の内容】

【図３９】

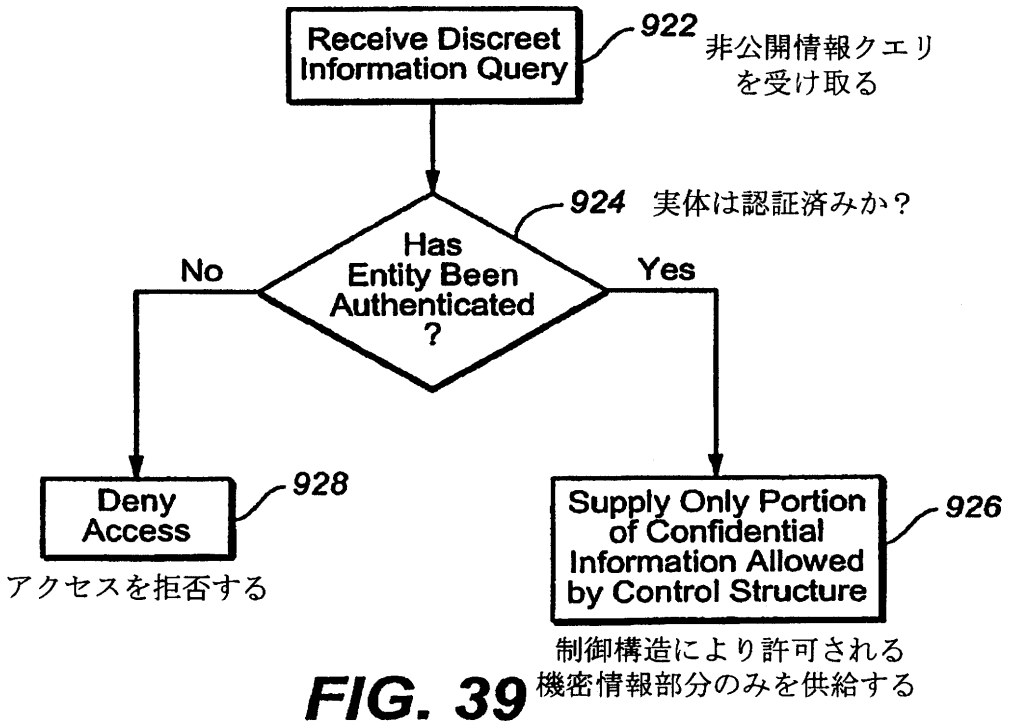


FIG. 39

【誤訳訂正１１３】
【訂正対象書類名】図面
【訂正対象項目名】図４３
【訂正方法】変更
【訂正の内容】

【図４３】

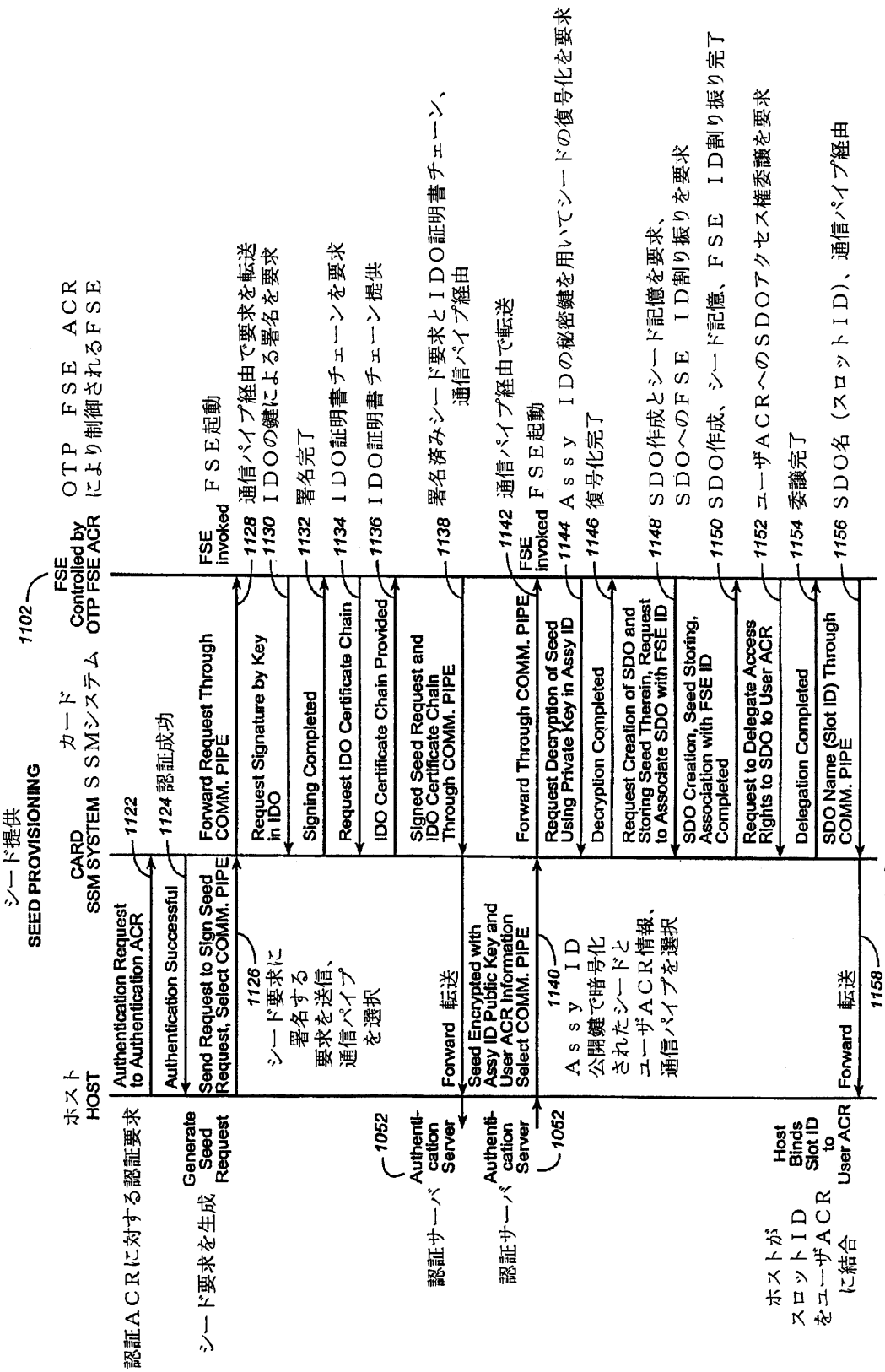

シード提供
SEED PROVISIONING
ホスト
HOST
カード
SSM SYSTEM ＳＳＭシステム
1102
FSE
Controlled by
OTP FSE ACR
OTP FSE ACR
により制御されるFSE
認証ＡＣＲに対する認証要求
Authentication Request to Authentication ACR
1122
Authentication Successful
1124 認証成功
シード要求を生成
Generate Seed Request
Send Request to Sign Seed Request, Select COMM. PIPE
Forward Request Through COMM. PIPE
FSE invoked ＦＳＥ起動
1126 シード要求に署名する要求を送信、通信パイプを選択
Request Signature by Key in IDO
1128 通信パイプ経由で要求を転送
1130 ＩＤＯの鍵による署名を要求
Signing Completed
1132 署名完了
Request IDO Certificate Chain
1134 ＩＤＯ証明書チェーンを要求
IDO Certificate Chain Provided
1136 ＩＤＯ証明書チェーン提供
1052
Authentication Server
認証サーバ
Forward 転送
Signed Seed Request and IDO Certificate Chain Through COMM. PIPE
1138 署名済みシード要求とＩＤＯ証明書チェーン、通信パイプ経由
Authentication Server
認証サーバ
1052
Seed Encrypted with Assy ID Public Key and User ACR Information Select COMM. PIPE
Forward Through COMM. PIPE
1142 通信パイプ経由で転送
FSE invoked ＦＳＥ起動
1140 Ａｓｓｙ ＩＤ公開鍵で暗号化されたシードとユーザＡＣＲ情報、通信パイプを選択
Request Decryption of Seed Using Private Key in Assy ID
1144 Ａｓｓｙ ＩＤの秘密鍵を用いてシードの復号化を要求
Decryption Completed
1146 復号化完了
Request Creation of SDO and Storing Seed Therein, Request to Associate SDO with FSE ID
1148 ＳＤＯ作成とシード記憶を要求、ＳＤＯへのＦＳＥ ＩＤ割り振りを要求
SDO Creation, Seed Storing, Association with FSE ID Completed
1150 ＳＤＯ作成、シード記憶、ＦＳＥ ＩＤ割り振り完了
Request to Delegate Access Rights to SDO to User ACR
1152 ユーザＡＣＲへのＳＤＯアクセス権委譲を要求
Delegation Completed
1154 委譲完了
SDO Name (Slot ID) Through COMM. PIPE
1156 ＳＤＯ名（スロットＩＤ）、通信パイプ経由
ホストがスロットＩＤをユーザＡＣＲに結合
Host Binds Slot ID to User ACR
Forward 転送
1158

FIG. 43