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

特許第3918827号
(P3918827)

(45)発行日　平成19年5月23日(2007.5.23)　(24)登録日　平成19年2月23日(2007.2.23)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330G
G06F 1/00	(2006.01)	G06F	1/00	370E
G06F 21/24	(2006.01)	G06F	12/14	530C
H04L 9/32	(2006.01)	G06F	12/14	560A
		H04L	9/00	673E

請求項の数 11　(全 34 頁)

(21)出願番号　特願2004-117437(P2004-117437)
(22)出願日　平成16年4月13日(2004.4.13)
(65)公開番号　特開2005-235159(P2005-235159A)
(43)公開日　平成17年9月2日(2005.9.2)
審査請求日　平成18年9月29日(2006.9.29)
(31)優先権主張番号　特願2004-12594(P2004-12594)
(32)優先日　平成16年1月21日(2004.1.21)
(33)優先権主張国　日本国(JP)

特許法第30条第1項適用　IEEE TRANSACTIONS ON CONSUMER ELECTRONICS、AUGUST 2003 Vol. 49、P561－566、発行者：IEEE CONSUMER ELECTRONICS SOCIETY、発行日：2003年8月29日

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100100310
弁理士　井上　学
(72)発明者　加藤　崇利
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所システム開発研究所内
(72)発明者　水島　永雅
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所システム開発研究所内

最終頁に続く

(54)【発明の名称】セキュアリモートアクセスシステム

(57)【特許請求の範囲】

【請求項１】

情報処理装置と，

前記情報処理装置に接続される，前記情報処理装置がアクセス可能なストレージデバイスと，からなり，

前記情報処理装置による前記ストレージデバイスへのアクセスを制御するストレージデバイスアクセスシステムであって，

前記ストレージデバイスは，

耐タンパメモリ領域と，

フラッシュメモリ領域と，

前記情報処理装置が前記耐タンパメモリ領域または前記フラッシュメモリ領域にアクセスするために用いられる，インターフェース手段と，を備え，

前記情報処理装置は，

前記ストレージデバイスの前記耐タンパメモリ領域へのアクセスを要求する耐タンパメモリ領域アクセス手段と，

前記ストレージデバイスの前記フラッシュメモリ領域へのアクセスを要求するフラッシュメモリ領域アクセス手段と，

前記耐タンパメモリ領域への前記アクセス要求に応じた，前記耐タンパメモリ領域へのアクセスと，前記フラッシュメモリ領域への前記アクセス要求に応じた，前記フラッシュメモリ領域へのアクセスと，を前記ストレージデバイスの前記インターフェース手段に対

して行うアクセス制御手段と，を備え，
前記情報処理装置の前記アクセス制御手段は，
前記耐タンパメモリ領域アクセス手段による，前記耐タンパメモリ領域への一つのアクセス要求に応じて，前記ストレージデバイスの前記インターフェース手段に対して，前記耐タンパメモリ領域へのアクセスを行い，
前記ストレージデバイスの前記インターフェース手段は，前記アクセス制御手段による，前記耐タンパメモリ領域へのアクセスにおいて，複数のレスポンスを応答し，
前記情報処理装置の前記アクセス制御手段は，競合解決処理として，
前記インターフェース手段から前記複数のレスポンスの最後を受信する前に，前記フラッシュメモリ領域アクセス手段から前記フラッシュメモリ領域へのアクセスを要求された場合に，当該フラッシュメモリ領域へのアクセスの待機処理を行い，
前記インターフェース手段から，前記複数のレスポンスの最後を受信した後に，前記待機処理を行った前記フラッシュメモリ領域へのアクセスを行う
ことを特徴とするストレージデバイスアクセスシステム。
【請求項２】
情報処理装置と，
前記情報処理装置に接続される，前記情報処理装置がアクセス可能なストレージデバイスと，からなり，
前記情報処理装置による前記ストレージデバイスへのアクセスを制御するストレージデバイスアクセスシステムであって，
前記ストレージデバイスは，
耐タンパメモリ領域と，
フラッシュメモリ領域と，
前記情報処理装置が前記耐タンパメモリ領域または前記フラッシュメモリ領域にアクセスするために用いられる，インターフェース手段と，を備え，
前記情報処理装置は，
前記ストレージデバイスの前記耐タンパメモリ領域へのアクセスを要求する耐タンパメモリ領域アクセス手段と，
前記ストレージデバイスの前記フラッシュメモリ領域へのアクセスを要求するフラッシュメモリ領域アクセス手段と，
前記耐タンパメモリ領域への前記アクセス要求に応じた，前記耐タンパメモリ領域へのアクセスと，前記フラッシュメモリ領域への前記アクセス要求に応じた，前記フラッシュメモリ領域へのアクセスと，を前記ストレージデバイスの前記インターフェース手段に対して行うアクセス制御手段と，を備え，
前記情報処理装置の前記アクセス制御手段は，
前記耐タンパメモリ領域アクセス手段による，前記耐タンパメモリ領域への一つのアクセス要求に応じて，前記ストレージデバイスの前記インターフェース手段に対して，複数のレスポンスを受信する前記耐タンパメモリ領域へのアクセスを行い，
前記ストレージデバイスの前記インターフェース手段は，前記アクセス制御手段による，前記耐タンパメモリ領域へのアクセスにおいて，前記複数のレスポンスを応答し，
前記情報処理装置の前記アクセス制御手段は，競合解決処理として，
前記複数のレスポンスを受信し，前記耐タンパメモリ領域への前記アクセスが終了するまでに，前記フラッシュメモリ領域へのアクセス要求の有無を繰り返して調べ，
前記フラッシュメモリ領域への前記アクセス要求が有る場合は，当該フラッシュメモリ領域へのアクセスの待機処理を行い，
前記複数のレスポンスを受信する前記耐タンパメモリ領域への前記アクセスが終了した後に，前記待機処理を行った前記フラッシュメモリ領域へのアクセスを行う
ことを特徴とするストレージデバイスアクセスシステム。
【請求項３】
情報処理装置と，

前記情報処理装置に接続される，前記情報処理装置がアクセス可能なストレージデバイスと，からなり，
前記情報処理装置による前記ストレージデバイスへのアクセスを制御するストレージデバイスアクセスシステムであって，
前記ストレージデバイスは，
耐タンパメモリ領域と，
フラッシュメモリ領域と，
前記情報処理装置が前記耐タンパメモリ領域または前記フラッシュメモリ領域にアクセスするために用いられる，インターフェース手段と，を備え，
前記情報処理装置は，
前記ストレージデバイスの前記耐タンパメモリ領域へのアクセスを要求する耐タンパメモリ領域アクセス手段と，
前記ストレージデバイスの前記フラッシュメモリ領域へのアクセスを要求するフラッシュメモリ領域アクセス手段と，
前記耐タンパメモリ領域への前記アクセス要求に応じた，前記耐タンパメモリ領域へのアクセスと，前記フラッシュメモリ領域への前記アクセス要求に応じた，前記フラッシュメモリ領域へのアクセスと，を前記ストレージデバイスの前記インターフェース手段に対して行うアクセス制御手段と，を備え，
前記情報処理装置の前記アクセス制御手段は，
前記耐タンパメモリ領域アクセス手段による，前記耐タンパメモリ領域への一つのアクセス要求に応じて，前記ストレージデバイスの前記インターフェース手段に対して，前記耐タンパメモリ領域へのアクセスコマンドの発行を伴う前記耐タンパメモリ領域への前記アクセスを，行い，
前記フラッシュメモリ領域アクセス手段による，前記フラッシュメモリ領域への一つのアクセス要求に応じて，前記ストレージデバイスの前記インターフェース手段に対して，前記フラッシュメモリ領域へのアクセスコマンドの発行を行う前記フラッシュメモリ領域への前記アクセスを行い，
前記ストレージデバイスの前記インターフェース手段は，前記アクセス制御手段による，前記耐タンパメモリ領域への前記アクセスにおける一つの前記アクセスコマンドの発行をきっかけとして，複数のレスポンスを応答し，
前記情報処理装置の前記アクセス制御手段は，競合解決処理として，
前記インターフェース手段に対する，前記きっかけとなる，前記耐タンパメモリ領域への前記一つのアクセスコマンドの発行から，前記インターフェース手段から前記複数のレスポンスの最後を受信するまでの間は，前記フラッシュメモリ領域へのアクセスにおける前記フラッシュメモリ領域への前記アクセスコマンドの発行の待機処理を行い，
前記インターフェース手段から，前記複数のレスポンスの最後を受信した後に，前記待機処理を行った前記フラッシュメモリ領域への前記アクセスコマンドの発行を行う
ことを特徴とするストレージデバイスアクセスシステム。

【請求項４】

請求項１または２に記載のストレージデバイスアクセスシステムであって，
前記アクセス制御手段は，
一つの前記耐タンパメモリ領域へのアクセス要求に応じて行う前記耐タンパメモリ領域への前記アクセスにおいて，前記ストレージデバイスの前記インターフェース手段に対して，複数の，前記耐タンパメモリ領域へのアクセスコマンドを発行し，
前記ストレージデバイスの前記インターフェース手段は，前記複数の耐タンパメモリ領域アクセスコマンドの各々に対して，前記複数のレスポンスの各々を応答する
ことを特徴とするストレージデバイスアクセスシステム。

【請求項５】

請求項３に記載のストレージデバイスアクセスシステムであって，
前記アクセス制御手段は，

前記耐タンパメモリ領域への一つのアクセス要求に応じて行う前記耐タンパメモリ領域への前記アクセスにおいて，前記ストレージデバイスの前記インターフェース手段に対して，前記きっかけとなる一つのアクセスコマンドを含む，複数の前記耐タンパメモリ領域へのアクセスコマンドを発行し，
前記ストレージデバイスの前記インターフェース手段は，前記複数の耐タンパメモリ領域アクセスコマンドの各々に対して，前記複数のレスポンスの各々を応答する
ことを特徴とするストレージデバイスアクセスシステム。
【請求項６】
請求項１または２に記載のストレージデバイスアクセスシステムであって，
前記アクセス制御手段は，
前記フラッシュメモリ領域へのアクセスの前記待機処理において，
前記フラッシュメモリ領域への前記アクセス要求に基づくフラッシュメモリ領域アクセスコマンドを，待機用メモリ領域に格納し，
前記前記フラッシュメモリ領域へのアクセスにおいて，前記待機用メモリ領域に格納されている前記フラッシュメモリ領域アクセスコマンドを発行する
ことを特徴とするストレージデバイスアクセスシステム。
【請求項７】
請求項３または５に記載のストレージデバイスアクセスシステムであって，
前記アクセス制御手段は，
前記フラッシュメモリ領域へのアクセスコマンドの前記待機処理において，
待機処理を行う前記フラッシュメモリ領域アクセスコマンドを，待機用メモリ領域に格納し，
前記待機処理を行った前記フラッシュメモリ領域への前記アクセスコマンドの発行において，前記待機用メモリ領域に格納されている前記フラッシュメモリ領域アクセスコマンドを発行する
ことを特徴とするストレージデバイスアクセスシステム。
【請求項８】
請求項１ないし５いずれか一に記載のストレージデバイスアクセスシステムであって，
前記アクセス制御手段は，
一つの前記フラッシュメモリ領域へのアクセス要求に応じて行う前記フラッシュメモリ領域への前記アクセスにおいて，前記フラッシュメモリ領域への，複数のアクセスコマンドを発行し，
前記ストレージデバイスの前記インターフェース手段は，前記複数のフラッシュメモリ領域へのアクセスコマンド各々に対して，レスポンスを応答する
ことを特徴とするストレージデバイスアクセスシステム。
【請求項９】
請求項１ないし８いずれか一に記載のストレージデバイスアクセスシステムであって，
前記情報処理装置は，
CPUとメモリとを備えるクライアント装置と，前記インターフェース手段に接続するストレージデバイス用リーダライタとを備え，
前記メモリには，前記耐タンパメモリ領域アクセス用のソフトウェアと，前記フラッシュメモリ領域アクセス用のソフトウェアとを備え，
前記アクセス制御手段は，
前記CPUが前記耐タンパメモリ領域アクセス用ソフトウェアと前記フラッシュメモリ領域アクセス用ソフトウェアとを実行することにより，
前記ストレージデバイス用リーダライタを介する，前記ストレージデバイスの前記インターフェース手段に対して行う，前記耐タンパメモリ領域へのアクセスと，前記フラッシュメモリ領域へのアクセスと，
前記競合解決処理と，を実行する。
ことを特徴とするストレージデバイスアクセスシステム。

【請求項１０】
請求項６または７に記載のストレージデバイスアクセスシステムであって，
前記アクセス制御手段は，
前記待機用メモリ領域に予め定めた時間を越えて格納されている前記フラッシュメモリ領域アクセスコマンドを破棄する
ことを特徴とするストレージデバイスアクセスシステム。
【請求項１１】
請求項６，７，１０いずれか一に記載のストレージデバイスアクセスシステムであって，
前記待機用メモリ領域は，前記クライアント装置の前記メモリまたは前記ストレージデバイス用リーダライタが備える
ことを特徴とするストレージデバイスアクセスシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、サーバをネットワークを介して安全に遠隔操作することを可能にするセキュアリモートアクセスシステムに関する。特にクライアントを適切にサーバに接続する為の耐タンパデバイスとクライアントもしくは耐タンパデバイス上に記録するプログラム、及びリモートアクセスシステムを動作させるためのネットワーク接続技術に関する。
【背景技術】
【０００２】
近年パーソナルコンピュータ（ＰＣ）やネットワーク機器の低価格化が進み、従業員の大半にＰＣのような業務利用する端末を配布し、業務を行わせるようにしている企業が多数を占めるようになっている。ＰＣが低価格化し、利用が増えると、企業内の機器管理者のメンテナンス作業を行う必要のあるＰＣの数も比例して増える。このメンテナンス作業とは、例えばオペレーティングシステム（ＯＳ）や業務アプリケーションのバージョンアップやバグフィックス、ハードウェア的な障害への対応、ウィルス対策やウィルス駆除などが挙げられる。このようなメンテナンス作業を行う管理コストは非常に大きく、従業員数が増加すると、比例して莫大なものになる。
【０００３】
この管理コストを低減するための一手法として、サーバクライアント方式と呼ばれるシステム運用の方式が取られている。これは、主なプログラムやデータをサーバ側に蓄積し、例えばＴｈｉｎ Ｃｌｉｅｎｔ（シンクライアント）のようなクライアント側に蓄積するデータを低減させたものである。
【０００４】
サーバクライアント方式では、演算処理やデータの蓄積は主にサーバ側で行われるため、シンクライアントのようなクライアント側にて個々にＯＳや業務に利用するアプリケーションのバージョンアップやバグフィックス、ウィルス対策やウィルス駆除などを行う必要性や頻度が減少するため、全体の管理コストを低減できる。
【０００５】
また、近年、ＩＣチップと呼ばれるプロセッサをカード内に内蔵したＩＣカード（別名スマートカード）が、電子認証機能をもつキーデバイスとして注目されている。ＩＣカードとは、主に内部のＩＣカードモジュールに中央演算処理装置（ＣＰＵ）を内蔵しているカードのことを指す。ＩＣカードのメモリにはＲＯＭ、ＥＥＰＲＯＭなどが使用される。ＩＣカードは、カード自身に演算機能を持つため、ホストからの読み書き指示の際、正しいユーザからアクセスが行われたものかどうか自身で判断する機能を持つ。また、ＣＰＵ自体の偽造が困難であるため、耐タンパデバイスであるＩＣカードモジュール（ＩＣカードチップ）の発する情報の改ざんや、不正にＩＣカードモジュール内部にアクセスすることが難しい。このため、高いセキュリティレベルを持つシステムを構築可能である。多くのＩＣカードは、ユーザの登録した個人認証番号（ＰＩＮコード）とカード内部に保持さ

れたＰＩＮコードを照合するなどして、ＩＣカード内の情報を適切にリーダライタ、もしくはホスト出力するか、もしくはしないか等の制御を行うことが可能である。ＩＣカードは内部にＥＥＰＲＯＭやＲＡＭなどの書き換え可能なメモリを持ち、ユーザやカード発行者のアプリケーションや情報を格納することができる。ＩＣカードは、外部から入力される情報に対し、その該当するカード内にしか存在し得ない情報（秘密鍵等）を用いた演算をするなどして、カード外部にカード所有者のみしか知りえない情報もしくは作りえない情報などを出力することでカード所有者を認証させたり、否認防止のための情報を出力したりすることが可能である。

【０００６】

また、フラッシュメモリカードは、不揮発性のメモリモジュールを内蔵したメモリカードでユーザの情報をメモリカード内に記憶することが可能である。フラッシュメモリカードの多くは「第３者からの攻撃に対するハードウェア的な耐久性」（耐タンパ性）を持っていない。耐タンパ性を持たないフラッシュメモリカードは、盗難、紛失時にカードが分解され、カード内のメモリもしくはコントローラを解析されることにより保持している情報が第３者に漏洩する可能性が少なくない。

【０００７】

また、特許文献１に記載されるようにフラッシュメモリインターフェースとＩＣカード機能を持つフラッシュメモリカードが開示されている。このフラッシュメモイリンターフェースとＩＣカード機能を持つフラッシュメモリカードは、その記憶容量の大きさから、パソコンやワークステーションに構築されたユーザの保管文書や設定ファイル等をカード内に保存して持ち歩くために都合がよい。

【０００８】

【特許文献１】特開２００１－２０９７７３号公報

【発明の開示】

【発明が解決しようとする課題】

【０００９】

前述したサーバクライアント方式では、サーバとクライアントの間の認証やデータのやり取りはネットワークを介して行われる。このため、ネットワーク上の一つのクライアントから、サーバへのアクセスを行う際に、サーバ側ではアクセスしてきたクライアントが正しいクライアントであるか否か、またクライアントを利用している利用者が正しい利用者であるか否か等の検証作業を行う必要がある。また、クライアント側でも、アクセスしているサーバが正しいサーバであるか否かを検証せずには自分が欲する業務を行うことができない。もし上記のような検証を行わないとサーバ側に蓄積したデータや、利用者の持つ情報が第３者に漏洩する可能性がある。そこで、ネットワーク上での認証や、業務遂行中の送信情報などの暗号化などのセキュリティを十分に高める必要がある。

【００１０】

本発明の目的は、ＩＣカードに実装されるＩＣチップのような認定された耐タンパデバイスの中に利用者の認証情報を格納し、かつ、大容量のファイルを安全に格納し、持ち歩くことができるフラッシュメモリカードのようなストレージデバイスを認証デバイスとするサーバクライアントシステムによりユーザの利便性を向上させることにある。

【００１１】

また、そのサーバクライアントシステムに使用可能な認証用ストレージデバイスを提供することも本発明の目的である。

【００１２】

本発明の前記並びにその他の目的と新規な特徴は、本明細書の記述および添付図面から明らかになるであろう。

【課題を解決するための手段】

【００１３】

本願において開示される発明のうち代表的なものの概要を説明すれば、下記の通りである。すなわち、上記の目的を達成するために本発明に係るリモートアクセスシステムは、

耐タンパデバイスとストレージとコントローラの機能を実装したストレージデバイスと、前記ストレージデバイスを接続するためのリーダライタと、前記リーダライタと接続するクライアントと、ネットワークを介し前記クライアントから遠隔操作されるサーバとネットワーク上の暗号通信を行うためのゲートウェイを具備し、前記ストレージの中に、前記サーバを遠隔操作するアプリケーションと、前記ネットワーク上の通信を暗号化する暗号化アプリケーションを記録しており、前記ゲートウェイと前記クライアントの暗号通信を行うための認証情報を前記耐タンパデバイス内に格納していることを特徴とする。

【発明の効果】

【００１４】

本発明によれば、認定された耐タンパデバイス搭載したストレージデバイスを利用者に配布し、利用者がストレージデバイスを不特定のクライアントに接続し、ストレージデバイス内の認証情報とアプリケーションを用いてサーバを遠隔操作するサーバクライアントシステムを提供することにより、利用者の使い勝手を向上することが可能で、結果としてシームレスに職場内外での業務遂行機能を利用でき、かつ操作したクライアント内に残る機密情報を低減することにより、ユーザのクライアント利用時のセキュリティ及び利便性を向上させるリモートアクセスシステムを提供できる。

【発明を実施するための最良の形態】

【００１５】

本発明の実施の形態について、添付図面を参照しながら以下詳細に説明する。なお、図面中にて同一の参照番号を付したものは、同一の機能を有する構成要素を示し、説明の便宜上、その詳細な説明は省略する。

【実施例１】

【００１６】

図１から図７を用いて、本発明に係るセキュアリモートアクセスシステムの第１の実施形態を説明する。

【００１７】

図１は、本発明の第１の実施形態を示すリモートアクセスシステムを示す図である。

【００１８】

利用者の使用するサーバ１０００と複数のクライアント（クライアント１００１及びクライアント１００２）は、ネットワークケーブル１００３、１００４及び１００５を介し、ネットワーク１００６に接続されている。ネットワークケーブル１００３、１００４及び１００５とネットワーク１００６は、図示しないネットワークハブやスイッチにて適切に接続され、ネットワークケーブル１００３、１００４、１００５及びネットワーク１００６上の接続された機器へのパケットのルーティングが適切に行われ、正常に通信が可能な状態にある。サーバ１０００は、図示しないディスプレィンターフェースを通してディスプレィ１００７と接続されている。クライアント１００１及び１００２も同様に図示しないディスプレィンターフェースを介してそれぞれディスプレィ１００８及び１００９と接続されている。クライアント１００１及び１００２にはそれぞれユーザインターフェース１０１０及び１０１１が接続されている。ユーザインターフェース１０１０及び１０１１はキーボードやマウス、トラックボール、タッチパネル、タッチパッド、指紋リーダ、生体情報読取装置などにより構成される、クライアント１００１及び１００２の利用者の入力情報をそれぞれクライアント１００１及び１００２に送信する機能を持つ。

【００１９】

リーダライタ１０１２及び１０１３はそれぞれクライアント１００１及び１００２に接続されており、ストレージデバイス１０１４を挿入する機能を持つ。ストレージデバイス１０１４内の後述する端子２０００はリーダライタ１０１２の図示しない端子と接続され、クライアント１００１と通信を行うことができる。ストレージデバイス１０１４は利用者が携帯し持ち歩くことが可能で、クライアント１００１以外の例えばクライアント１００２のような機器においても利用が可能な設計となっている。

【００２０】

ストレージデバイス１０１４は、内部にコントローラ１０１５、耐タンパデバイス１０１６、ストレージ１０１７を実装している。コントローラ１０１５、耐タンパデバイス１０１６、ストレージ１０１７はそれぞれ別の集積回路として実装されているように記載されているが、機能をまとめた１つの集積回路として実装しても良い。耐タンパデバイス１０１６は例えばＩＣカードチップなどのセキュリティ評価団体の定めた基準により認定を受けるかもしくは受けることが可能な水準の耐タンパ性を持つデバイスである。

【００２１】

サーバ１０００内部には、ＣＰＵ１０３０、メモリ１０３１、ストレージ１０３２が実装されている。クライアント１００１には、ＣＰＵ３０００、メモリ３００１、ストレージ３００２、クライアント１００２には、ＣＰＵ１０５０、メモリ１０５１、ストレージ１０５２が実装されている。

【００２２】

ＣＰＵ１０３０上にて実行される情報は、通常ディスプレィ１００７により表示されるが、サーバクライアント型の処理を要求する接続がクライアント１００１よりサーバ１０００に行われ、認証が確立し、サーバ１０００とクライアント１００１の遠隔操作用の暗号通信が確立した場合、クライアント１００１を介してサーバ１０００上でプログラムを実行した処理結果はディスプレィ１００８に表示される。この際、ディスプレィ１００８上に表示される情報は、ディスプレィ１００７に表示される情報と表示方法を同一にしてあり、ユーザは、クライアント１００１とユーザインターフェース１０１０を利用しているのと、サーバ１０００を直接操作しているのと同様に感じ取るため、利用者のユーザビリティを高めることができる。

【００２３】

図２にストレージデバイス１０１４の詳細を示したブロック構成図を示す。ストレージデバイス１０１４は、端子２０００、コントローラ１０１５、耐タンパデバイス１０１６、ストレージ１０１７を実装しており、それぞれが図示するように接続されている。コントローラ１０１５は内部にＣＰＵ２００１、メモリ２００２、不揮発メモリ２００３、インターフェース（Ｉ／Ｆ）２００４、２００５、２００６を持つ。ストレージ１０１７は、フラッシュメモリ、ハードディスク、ＥＥＰＲＯＭ、ＭＲＡＭ、ＭＯ、光ディスク等の不揮発性の記憶媒体である。本実施例においては、ストレージ１０１７がフラッシュメモリであるという前提において説明を行うが、他の種類の記憶媒体であっても良い。

【００２４】

コントローラ１０１５内のＣＰＵ２００１は、不揮発メモリ２００３からメモリ２００２にロードされたアプリケーションを実行し、ストレージ１０１７のファイル管理や耐タンパデバイス１０１６のリセットや制御等の、耐タンパデバイス１０１６及び端子２０００及びストレージ１０１７の間の通信の管理をＩ／Ｆ２００４～２００６を介して行う。

【００２５】

不揮発メモリ２００３は、公開鍵演算プログラム２０５０、共通鍵演算プログラム２０５１及びストレージ１０１７内のファイル管理プログラム２０５２を含む。また、不揮発メモリ２００３は、ハッシュの演算、デジタル署名、証明書の検証、鍵の生成等を行う機能を持っていてもよい。

【００２６】

耐タンパデバイス１０１６は、内部にＣＰＵ２０３０、メモリ２０３１及びストレージ２０３２を含む。コプロセッサ２０３３はＣＰＵ２０３０の演算機能のうち暗号機能などの補完するコプロセッサであるが、ＣＰＵ２０３０の計算速度が高速である場合、実装しなくてもよい。ＣＰＵ２０３０は、ストレージ２０３２からメモリ２０３１にロードされたアプリケーションを実行し、後述する共通鍵による暗復号、非対称鍵による暗復号、ストレージ２０３２内のファイル管理、ハッシュの演算、デジタル署名、証明書の検証、鍵の生成等を行う機能を持つ。耐タンパデバイス１０１６は、電圧変動などの様々な攻撃に対して強い耐性のある、セキュリティ評価団体の定めた基準により認定を受けるかもしくは受けることが可能な水準の耐タンパ性を持つデバイスである。

【００２７】
ストレージ２０３２は、ＥＥＰＲＯＭ、ＭＲＡＭ、フラッシュメモリなどの不揮発性ストレージである。ストレージ２０３２は、内部に秘密鍵２０４０、ＰＩＮ情報２０４１、ログ情報２０４２、証明書２０４３、公開鍵２０４４、ＰＩＮ検証プログラム２０４５、鍵証明書格納プログラム２０４６、公開鍵演算プログラム２０４７、共通鍵演算プログラム２０４８、鍵生成プログラム２０４９等を保存する。保存されたプログラムは、１つでも複数でも良い。ストレージ２０３２内のデータやプログラムは、メモリ２０３１にロードされ、ＣＰＵ２０３０を動作させたり、コントローラ１０１５を経由して耐タンパデバイス１０１６外部に送信される。

【００２８】
秘密鍵２０４０は、利用者の認証や通信路を暗号化するためなどの鍵であり、１つでも複数個でも良い。秘密鍵２０４０は、対応する鍵アルゴリズムの種類によって異なるフォーマットにて記述される。秘密鍵２０４０内の一つの秘密鍵に対応する公開鍵の集まりが公開鍵２０４４であり、対応する証明書の集まりが証明書２０４３である。証明書２０４３は、秘密鍵２０４０に対応する公開鍵２０４４の証明書であり、サーバ１０００や外部の認証局より発行されたものである。また、証明書２０４３は公開鍵２０４４の証明書とそのほかの証明書を発行した証明期間のルート認証局や中間認証局の証明書などその他の認証情報を含む。証明書２０４３のフォーマットは例えば国際電気通信連合（ＩＴＵ）の定めるＸ．５０９の仕様を満たすものである。証明書２０４０内に格納される情報は、公開鍵と公開鍵に対する署名の他に、例えば証明書のバージョン番号、証明書のシリアル番号、利用者の公開鍵の情報、証明書を発行した認証局の情報、証明書の有効期間、氏名や電子メールアドレスなどの利用者の情報及び拡張領域といった項目によって構成される。証明書２０１０はカード内からクライアント１００１及び１００２、サーバ１０００内において、認証情報の検証やデータやセッション鍵等の暗号化に利用される。

【００２９】
ＰＩＮ情報２０４１は、耐タンパデバイス１０１６外部から耐タンパデバイス１０１６内部の情報を出力させたり、演算を行わせたりする利用者の権利を検証するための情報である。ＰＩＮ情報２０４１は、暗証番号（ＰＩＮコード）でも良いし、パスフレーズと呼ばれるような桁数の長い文字列でも良いし、指紋、虹彩、顔形、声紋、静脈などによる生体認証の根拠となる生体認証情報でも良い。

【００３０】
ログ情報２０４２は、耐タンパデバイス１０１６の利用履歴が記録されたもので、ＣＰＵ３０００もしくは２００１もしくは２０３０が動作するたびに追記されたり、耐タンパデバイス１０１６の外部から適切な権利を持つ利用者が追記したり、読み出したりする。ログ情報２０４２は、第３者からの改ざんを防ぐために、ハッシュ値の署名を付加して記録する。

【００３１】
ＰＩＮ検証プログラム２０４５は、ＰＩＮ情報２０４１が耐タンパデバイス１０１６外部から検証用に入力されたＰＩＮ情報と合致するか検証するプログラムである。検証結果が正しければ、耐タンパデバイス１０１６は利用者が内部の情報や演算資源を利用可能な状態にする。ＰＩＮ検証プログラム２０４５は、ストレージ２０３２内にあり、メモリ２０３１にロードされるプログラムやストレージ２０３２上に保存される情報ごとに利用権限を定め、個別に認証を行う。例えば、耐タンパデバイスが通電された後の利用時に一度ＰＩＮ検証プログラムにて正しいと判断された利用者には以降のアクセスにてＰＩＮ検証を求めなかったり、利用のたびにＰＩＮ検証を行ったりできるよう設定することができる。

【００３２】
鍵証明書格納プログラム２０４６は、ストレージ２０３２内に保存されている秘密鍵２０４０や公開鍵２０４４や証明書２０４３を耐タンパストレージ１０１６外部へ出力したり、耐タンパストレージ１０１６外部から内部へ取り込んでストレージ２０３２内に格納

したりする機能を持つ。鍵証明書格納プログラム２０４６を利用するためにはＰＩＮ検証プログラム２０４５による検証が終了する必要がある。ただし、証明書２０４３や公開鍵２０４４を出力するだけであるなら、ＰＩＮ検証プログラム２０４５による検証が不要としても良い。鍵証明書格納プログラム２０４６は、外部へ鍵や証明書を入出力する際に外部のＣＰＵ３０００もしくは２００１もしくは２０３０とセッション鍵を交換し安全な暗号化通信路を設けて鍵や証明書をやり取りする機能を持っている。

【００３３】

公開鍵演算プログラム２０４７及び共通鍵演算プログラム２０４８は、それぞれ前述の公開鍵演算プログラム２０５０及び共通鍵演算プログラム２０５１と同様の機能を持つ。鍵生成プログラム２０４９は、秘密鍵２０４０及び公開鍵２０４４のうちの１つの鍵のペアや対象鍵の秘密鍵（共通鍵）を生成する機能を持つ。作成された公開鍵や共通鍵はストレージ２０３２内に保存されたり、外部に出力される。非対称鍵の秘密鍵は、秘密鍵２０４０内に保存される。

【００３４】

ストレージ１０１７は内部に利用者を識別するための証明書２０１０、利用者がストレージデバイス１０１４を利用して操作を行ったログ情報２０１１、デバイスアクセス用ライブラリ２０１２、デバイス管理用ツール２０１３、デバイスドライバ２０１４、インターフェースハンドラ２０１５、インストーラ２０１６、遠隔操作端末用アプリケーション２０１７、暗号化通信路構築用アプリケーション２０１８、業務アプリケーション２０１９、一時記憶領域２０２０、認証情報のコピー２０２１を記録している。

【００３５】

証明書２０１０は、クライアント１００１やサーバ１０００が利用者やストレージデバイス１０１４を識別する演算を行うために利用する。証明書２０１０のフォーマットは例えばＩＴＵの定めるＸ．５０９の仕様を満たすものなどであればよい。証明書２０１０内には例えば証明書のバージョン番号、証明書のシリアル番号、利用者の公開鍵の情報、証明書を発行した認証局の情報、証明書の有効期間、氏名、電子メールアドレスやストレージデバイス固有の識別番号等の利用者やストレージデバイスの情報、拡張領域といったものが記録されている。証明書２０１０はストレージデバイス１０１４内やクライアント１００１、サーバ１０００内において、認証情報の検証やデータやセッション鍵等の暗号化に利用される。

【００３６】

ログ情報２０１１は、利用者がストレージデバイス１０１４を利用して操作を行った際に、ＣＰＵ２００１もしくはＣＰＵ２０３０もしくはクライアント１００１もしくはサーバ１０００の指示により更新される。ログ情報２０１１は、サーバ１０００上のアプリケーションやクライアント１００１上のアプリケーションより利用されるか、利用者が自分の利用状況を確認するために利用される。ログ情報２０１１は、第３者からの改ざんを防ぐために、ハッシュ値の署名を付加して記録する。

【００３７】

デバイスアクセス用ライブラリ２０１２は、クライアント１００１にて動作する複数のアプリケーションがストレージ１０１７にアクセスする際に利用する、ファイル管理、ハッシュの演算、デジタル署名、証明書の検証、鍵の生成等の機能を利用するための関数群である。通常、後述するインストーラ２０１６によって、クライアント１００１にインストールされて利用するが、直接、デバイスアクセス用ライブラリ２０１２がクライアント１００１上のアプリケーションから利用されても良い。

【００３８】

デバイス管理用ツール２０１３は、ストレージデバイス１０１４を管理するためのツールであり、例えば、利用者の認証番号を変更するツールや閉塞したストレージデバイスを初期化するツールやストレージデバイス上のプログラムやファームウェア、鍵情報、証明書の書き換えツールや、ストレージデバイス１０１４をデバッグする際に必要となるデバッグ用のモニタリングツールや、ストレージデバイスのマニュアルやヘルプファイルや、

遠隔地からサーバの電源を投入するＷａｋｅ ｕｐ ｏｎ ＬＡＮのような機能などを利用しクライアント１００１やサーバ１０００をリモートから電源投入や電源遮断をする電源管理するツールを含む。デバイス管理用ツール２０１３は、後述するインストーラ２０１５によりクライアント１００１にインストールされても良いし、利用者がクライアント１００１へ直接ロードして利用しても良い。

【００３９】

デバイスドライバ２０１４は、ストレージデバイス１０１４の動作に必要な情報をＯＳに提供したり、動作を管理するプログラムであり、後述するインストーラ１０１５によりクライアント１００１にインストールされる。

【００４０】

インターフェースハンドラ２０１５は、デバイスドライバ２０１４を管理するミドルウェアで、クライアント１００１やサーバ１０００上で動作するアプリケーションとデバイスドライバ２０１４を接続させる役割を果たす。

【００４１】

インストーラ２０１６は、ストレージ１０１７上に存在するアプリケーションや情報、ドライバなどをクライアント１００１やサーバ１０００にインストールする際に利用者が利用する。インストーラ２０１６によってインストールされるアプリケーションや情報、ドライバ等は、インストール終了後に削除されても良いが、利用者が別の機器に接続してストレージデバイス１０１４を利用する際のためにストレージデバイス上に保存しておく。

【００４２】

遠隔操作端末用アプリケーション２０１７は、クライアント１００１からサーバ１０００を遠隔操作するために利用する。遠隔操作端末用アプリケーション２０１７は、ターミナルサービスやリモートデスクトップ等といったクライアント１００１やサーバ１０００のＯＳの持つ標準のサービスやアプリケーションでもよい。遠隔操作端末用アプリケーション２０１７は、インストーラ２０１６によってクライアント１００１にインストールされて利用されるか、もしくはストレージデバイス１０１４からクライアント１００１に直接ロードされて利用される。

【００４３】

暗号化通信路構築用アプリケーション２０１８は、クライアント１００１とサーバ１０００との間の通信を暗号化させるために利用される。暗号化通信路構築用アプリケーション２０１８は、サーバ１０００とクライアント１００１の間で秘密鍵を共有させ、その秘密鍵を用いることによりサーバ１０００とクライアント１００１の間に暗号化通信路を成立させる。この秘密鍵の共有に耐タンパデバイス１０１６内の秘密鍵等の秘密情報を用いてもよいし、秘密鍵を共有するプロセス内に耐タンパデバイス１０１６内の秘密情報を用いた認証を用いても良い。

【００４４】

業務アプリケーション２０１９は、利用者がクライアント１００１を利用する際に利用するアプリケーションである。業務アプリケーション２０１９は、例えばサーバ上のウェブベースのアプリケーションを利用するのであれば、ウェブブラウザであり、データベースを利用するのであれば、データベース操作用クライアントである。ストレージ１０１７上の全ての情報が、耐タンパデバイス１０１６内にある秘密鍵２０４０のうちのいくつかの秘密鍵かサーバ１０００もしくはクライアント１００１上に保持する秘密鍵のうちのいくつかによって暗号化されていてもよいし、平文で記録されていてもよい。前者であれば、利用者に提供するセキュリティが向上する。また、コントローラ１０１５や耐タンパデバイス１０１６内において利用者認証が済んでいないとストレージ１０１７にアクセスできないようになっている場合、利用者に提供するセキュリティが向上する。

【００４５】

一時記憶領域２０２０は、業務アプリケーション２０１９等のアプリケーションをクライアント１００１上で実行するときに、アプリケーションの作成する一時ファイルを保存

しておく領域である。業務アプリケーション２０１９やサーバ１０００もしくはクライアント１００１上の業務遂行用アプリケーションは、ビットマップのキャッシュなどの一時記憶ファイルを一時記憶領域２０２０内に作成する。一時記憶領域が暗号化されていない場合、利用者が利用を停止する際には、コントローラ１０１５もしくはクライアント１００１上のＯＳもしくはアプリケーションの指示により一時記憶ファイルは消去される。このことにより、利用者の作成する一時ファイルはストレージデバイス上に記憶され、クライアント１００１内の情報が第３者によって危険にさらされても利用者の利用した情報は安全に保護され、電源を切断したクライアント１００１からの利用者の機密情報やプライバシーを含んだ情報はより漏洩しにくくなる。

【００４６】

図１２にストレージ１０１７上に記録された業務アプリケーション２０１９やクライアント１００１などにインストールされたアプリケーションから一時記憶領域２０２０を利用する際の処理方法をフローチャートにて示した図を示す。図１２のフローチャートに示される処理は、アプリケーションの実行されるＣＰＵ１０３０、もしくは３０００において行われる。例えば、遠隔操作端末用アプリケーション２０１７や業務アプリケーション２０１９は、ＣＰＵ３０００上にて実行され、サーバ１０００上のアプリケーションは、ＣＰＵ１０３０上で実行されることになる。この際、利用者が利用するアプリケーションが起動される（１２０００）と、一時記憶領域２０２０がアプリケーションに定義されているかどうかと利用可能かどうかが調べられる（１２００１）。処理１２００１において未定義もしくは利用不可能の場合一時記憶領域２０２０の領域の定義と利用可能化（１２００２）が行われる。次に、一時記憶領域の容量が十分かなど利用可能かどうかのチェックが行われる（１２００４）。容量不足等の問題が検出された場合は容量不足など問題解決処理が行われ（１２００５）異常状態から復帰できれば（１２００６）処理が継続されるが、出来ない場合は、アプリケーションは異常終了する（１２００７）。次にアプリケーションの処理が開始され（１２００３）、一時記憶領域２０２０への入出力が行われる（１２００８）。アプリケーションの処理が継続されるようであれば、処理１２００４へ戻る。アプリケーションが終了される場合、一時記憶領域２０２０への入出力１２０１０が行われる。処理１２０１０はアプリケーションの利用した情報の消去とその確認作業である。処理１２０１０により利用者の利用した情報が適切に保全されたり、多くの場合は諸居されることにより、利用者の持つプライバシーを含む情報や秘匿情報が保護される。異常が無ければ、アプリケーションは終了する（１２０１１）。

【００４７】

アプリケーションによって、一時記憶領域２０２０の定義方法がいくつか存在する。一つの方法は、アプリケーションが起動される際に、利用者ごとにクライアント１００１上に設けられた利用者のプロファイルに記載されてある一時記憶領域の設定をアプリケーションが読み込むことにより、一時記憶領域２０２０の場所をアプリケーションが特定するやり方である。この際、利用者のプロファイルは、ＯＳもしくはアプリケーションによって定義される利用者の設定情報で、ストレージ３００２もしくは、ストレージ１０１７に記録されている。もう一つの方法は、アプリケーションが起動される際に、利用者に対し、ＯＳもしくはアプリケーションがダイヤログなどの確認手段をディスプレィ１００８上に表示するなどして、利用者に入力を促し、アプリケーションが一時記憶領域の設定を特定することである。この確認手段は多くはアプリケーションの最初の起動時に行われるが、毎起動時に行われても良い。以上のいずれかの方法によりアプリケーションは利用者の利用環境に対応した一時記憶領域の設定を行う。一度利用者が定義した情報は、クライアント上のストレージ３００２もしくはストレージ１０１７上に情報を記録することにより、アプリケーション起動時にアプリケーションが再度利用すればよい。

【００４８】

認証情報のコピー２０２１は、耐タンパデバイス１０１６内にある例えば、証明書２０４３や公開鍵２０４４のような認証情報のコピーである。この認証情報のコピー２０２１は、耐タンパデバイス１０１６内にある公開鍵２０４４や証明書２０４３やＰＩＮ情報２

０４１等のコピーである。

【００４９】

図３に認証情報のコピー２０２１の例を示す。証明書１（５００１）～証明書Ｎ（５００３）は証明書２０４３の一部である。ミドルウェアの認証情報５００４は、サーバ１０００もしくは、クライアント１００１のミドルウェアが認証情報のコピーが改ざんされていないかを検査するハッシュ値と署名やミドルウェアのバージョン情報、認証情報のコピーの作成された時刻情報などのミドルウェアの認証情報が含まれる。

【００５０】

一般的に耐タンパデバイス１０１６、コントローラ１０１５間の通信速度はストレージ１０１７、コントローラ１０１５間の通信速度より遅いことが多い。このため、クライアント１００１上のＯＳもしくはアプリケーションが耐タンパデバイス１０１６内の認証情報をストレージ１０１７にキャッシュもしくはコピーしておくことにより、利用者がストレージデバイスを利用する際に証明書２０４３の読み出しに要する時刻を短縮することができ、ユーザビリティを向上させることができる。認証情報のコピー２０２１は、ストレージデバイス１０１４が利用されるたびの検証されることが望ましく、その際に、認証情報のコピー２０２１の中の、ハッシュ値や耐タンパデバイス１０１６内の秘密鍵による署名や、クライアント１００１上のＯＳもしくはアプリケーションによる署名が利用される。

【００５１】

図４にクライアント１００１の詳細を示したブロック構成図を示す。クライアント１００１は、内部にＣＰＵ３０００、メモリ３００１、ストレージ３００２、インターフェース（Ｉ／Ｆ）３０２０、３０２１、３０２２、３０２３を持つ。ストレージ３００２は、フラッシュメモリ、ハードディスク、ＥＥＰＲＯＭ、ＭＲＡＭ、ＭＯ、光ディスク等の不揮発性の記憶媒体である。

【００５２】

ＣＰＵ３０００は、ストレージ３００２からメモリ３００１にロードされたアプリケーションを実行し、ディスプレィ１００８、ネットワーク１００６、ユーザインターフェース１０１０、リーダライタ１０１２との通信をそれぞれ、Ｉ／Ｆ３０２０、３０２１、３０２２、３０２３を介して行う。

【００５３】

ストレージ３００２は、証明書３０１０、ログ情報３０１１、デバイスアクセス用ライブラリ３０１２、デバイス管理用ツール３０１３、デバイスドライバ３０１４、インターフェースハンドラ３０１５、遠隔操作端末用アプリケーション３０１６、暗号化通信路構築用アプリケーション３０１７、業務アプリケーション３０１８が保存される。

【００５４】

証明書３０１０は、クライアント１００１やサーバ１０００が利用者やストレージデバイス１０１４を識別する演算を行うために利用する。証明書３０１０のフォーマットは例えばＩＴＵの定めるＸ．５０９の仕様を満たすものなどであればよい。

【００５５】

証明書３０１０内には例えば証明書のバージョン番号、証明書のシリアル番号、利用者の公開鍵の情報、証明書を発行した認証局の情報、証明書の有効期間、氏名、電子メールアドレスやストレージデバイス固有の識別番号等の利用者やストレージデバイスの情報、拡張領域といったものが記録されている。証明書３０１０はストレージデバイス１０１４内の証明書２０４３やストレージ１０１７内の証明書２０１０のコピーや独自に利用者が登録した利用者や証明書を証明するルート認証局や中間認証局やストレージデバイス１０１４などの耐タンパデバイスの証明書であり、クライアント１００１、サーバ１０００内において、認証情報の検証やデータやセッション鍵等の暗号化に利用される。

【００５６】

ログ情報３０１１は、利用者がクライアント１００１の操作を行った場合に、ＣＰＵ３０００もしくはサーバ１０００の指示により更新される。ログ情報３０１１は、サーバ１

０００上のアプリケーションやクライアント１００１上のアプリケーションより利用されるか、利用者が自分の利用状況を確認するために利用される。ログ情報３０１１は、第３者からの改ざんを防ぐために、ハッシュ値の署名を付加して記録する。

【００５７】

図５に利用者がクライアント１００１にストレージデバイス１０１４を挿入し、サーバ１０００を利用する際の利用者、ストレージデバイス１０１４、クライアント１００１、サーバ１０００間にて行われる通信の詳細を示した図を示す。利用者はクライアント１００１の利用を開始するまでに利用者の認証情報やクライアント１００１を動作させるためのアプリケーションが保存されたストレージデバイス１０１４をクライアント１００１のリーダライタに接続する。利用者が、クライアント１００１を利用したことがない場合は、利用者はストレージデバイス１０１４内のインストーラ２０１６を利用し、デバイスドライバ２０１４やデバイス管理ツール２０１３や遠隔端末用アプリケーション２０１７のようなサーバ１０００を操作するために必要な情報もしくはアプリケーションをクライアント１００１にインストールする。この際、クライアント１００１によってストレージデバイス１０１４から直接実行できるアプリケーションのインストールを行う必要はない。

【００５８】

利用者は、まずシーケンス４０００に示すようにクライアント１００１に動作確認要求を行う。クライアント１００１はサーバ１０００にサーバ動作確認を行う（４００１）利用者はサーバ１０００の動作を確認できなかった場合は、ストレージデバイス１０１４上のもしくはインストーラ２０１６にてクライアント１００１上に用意された遠隔地からサーバの電源を投入するローカルエリアネットワーク（ＬＡＮ）を利用して機器の電源投入を行うようなＷａｋｅ ｕｐ ｏｎ ＬＡＮのような機能を利用してサーバ１０００の電源投入を行う。この場合、サーバ１０００の、ネットワークに対するＩ／Ｆのみは常時通電されており、ＩＤとパスワードのセットやネットワークボードのＭＡＣアドレス等、何らかの認証情報を利用してサーバ１０００の起動が行われる（４００２、４００３）。この操作によりサーバ１０００は起動される（４００４）。サーバの起動が完了した際、利用者はクライアント１００１にログイン要求を入力する（４００５）。クライアント１００１内に遠隔操作アプリケーション２０１７及び暗号化通信路構築用アプリケーション２０１８がインストールされていない場合、この時点にてクライアント１００１にロードされる（４００６）。次にクライアント１００１からサーバ１０００にログイン要求が行われる（４００７）。サーバ１０００のリモート機器からのログインに対するセキュリティポリシーの設定によるが、ログインに際し、利用者の認証において公開鍵インフラストラクチャ（ＰＫＩ）を用いた認証が必要もしくは可能である場合、サーバ１０００からの認証情報の要求（４００８）、クライアント１００１からの証明書の要求（４００９）、ストレージデバイス１０１４からの証明書の送信（４０１０）、クライアント１００１からの署名の要求（４０１１）が行われる。ストレージデバイス１０１４において署名を行う場合、利用者の認証が必要となる。利用者の認証は、暗証番号、パスワード、パスフレーズ、ワンタイムパスワード、指紋情報などの生体認証情報などにより行われる。

【００５９】

本実施例では、暗証番号を利用した例を示す。ストレージデバイス１０１４からの暗証番号要求（４０１２）が行われた後、クライアント１００１から利用者へ暗証番号要求表示４０１３がディスプレィ１００８などを利用して行われる。利用者が暗証番号をユーザインターフェース１０１０とクライアント１００１を介してストレージデバイス１０１４に送信すると（４０１４、４０１５）、ストレージデバイス１０１４内のＣＰＵ２００１もしくはＣＰＵ２０３０においてサーバ１０００、クライアント１００１から送信された情報に対し、秘密鍵２０４０のうちの一つもしくはいくつかを用いた電子署名が作成される（４０１６）。作成された署名は、クライアントに送信される（４０１７）。クライアント１００１は、証明書２０１０、２０４３などの認証情報と作成された署名の送信を行う（４０１８）。次に、サーバ１０００及びクライアント１００１は、秘密鍵や公開鍵といったお互いの鍵情報と証明書を利用して、秘密共有鍵の鍵交換を行う（４０１９）。こ

の鍵交換４０１９は、遠隔操作端末用アプリケーション２０１７か暗号化通信路構築用アプリケーション２０１８により行われる。シークエンス４０１９において交換された秘密共有鍵を用いて、サーバ１０００及びクライアント１００１は暗号化通信路を構築し、２者の間で通信される情報は暗号化される。暗号化通信路が構築された段階で、ユーザは、サーバ１０００または、クライアント１００１、ストレージデバイス１０１４上に保存されているアプリケーションを起動し、業務遂行をする（４０２０）。

【００６０】

業務遂行中は、ＣＰＵ２００１もしくはＣＰＵ２０３０もしくはサーバ１０００もしくはクライアント１００１は、ログ情報２０１１、２０４２、３０１１に情報を追記し、利用者の業務遂行を適切に監視する。記載されたログ情報は、改ざん防止の処理を施され、ストレージデバイス１０１４やクライアント１００１内に保存されるが、利用者の利用開始時や利用終了時など適切なタイミングでサーバ１０００に送信される。

【００６１】

利用者の利用するサーバ１０００の管理を行う管理者は、ログ情報２０１１、２０４２、３０１１の情報とサーバ１０００に送信される情報を監査し、利用者が管理者が作成したポリシーに違反する利用を行った際に、サーバ１０００もしくはクライアント１００１もしくは、ストレージデバイス１０１４の利用を停止するようなオペレーションを行う。ポリシー違反は、例えば、ログの改ざんや、異常な利用時間、異常な通信量、ネットワーク１００６を介した異常なアクセス、クライアント１００１内に存在する異常なファイルの検出、ファイルやアプリケーションのアップデートの不備などが該当する。サーバ１０００もしくはクライアント１００１もしくは、ストレージデバイス１０１４の利用を停止するようなオペレーションとは、サーバ１０００及びクライアント１００１への利用者のログインの禁止や電源遮断、ストレージデバイス１０１４の閉塞などが該当する。ストレージデバイス１０１４の閉塞とは、ＰＩＮ検証プログラム２０４５の利用する情報を変更し、利用者がストレージデバイス１０１４を利用できないようにすることである。

【００６２】

利用者の業務など、サーバ１０００の利用が終了した場合、利用者は、クライアント１００１に対しサーバ遮断要求を行う（４０２１）。サーバ遮断要求はクライアント１００１からサーバ１０００に送信される（４０２２）。サーバ１０００及びクライアント１００１はセッションの遮断４０２３を行う。サーバ１０００は、利用者の利用情報のログをサーバ１０００上に記憶し（４０２４）、サーバ１０００のサーバ電源遮断を行う。利用者がサーバ遮断要求４０２１を行わなければ、サーバ電源遮断４０２５は行われない。サーバ電源遮断後は、また図５に示すシーケンスで業務遂行が行われる。

【００６３】

図６は、利用者がサーバ１０００及びクライアント１００１及びストレージデバイス１０１４を利用するために管理者が行うストレージデバイス１０１４の初期化操作を説明した図である。図６にて説明される一連の動作は、図５に示した利用者の利用が開始される前もしくは利用者がカードを閉塞もしくは紛失し、利用権限を失った際に行われる。

【００６４】

クライアント６０００は、クライアント１００１と同様にディスプレィやユーザインターフェースやリーダライタを接続されたクライアントで、管理者がストレージデバイス１０１４の書き込みを行うために利用する。

【００６５】

まず、管理者は、利用者の氏名ユーザ番号、電子メールアドレスやストレージデバイス固有の識別番号等をクライアント６０００を通じ、サーバ１０００に登録することにより、サーバ１０００より利用者の認証情報を作成する。利用者の認証情報及び証明書の作成と書き込み要求を行う（６００１）。ここで、ストレージデバイス１０１４は、既にストレージデバイス供給者から鍵証明書格納プログラム２０４６などの各種プログラムが書き込まれている。また、利用者の公開鍵証明書は、ストレージデバイス１０１４もしくはクライアント６０００もしくは管理者が別途生成した秘密鍵に対応する公開鍵を６００１に

て送付することにより得られる。作成された認証情報と公開鍵証明書は、クライアント６０００を経由してストレージデバイスへ書き込まれる（６００２）。次に管理者は、ストレージデバイス１０１４内の認証情報と鍵の利用権をコントロールするための情報を変更する（６００３、６００４）。この操作によってストレージデバイス１０１４は、署名要求や鍵書き換え要求、鍵のエクスポートインポート要求に対する利用権を変更される。利用権の変更は、情報に対するアクセスキーの変更や、暗証番号の変更である。変更されたアクセスキーや暗証番号は、管理者が保管したり、他の耐タンパデバイスに格納したり、利用者に通知する。

【００６６】

次に、管理者は、アプリケーションの書き込み要求を行い、クライアント６０００は、アプリケーションの書き込みを行う。ここで言うアプリケーションとは、デバイスアクセス用ライブラリ２０１２、デバイス管理用ツール２０１３、デバイスドライバ２０１４、インターフェースハンドラ２０１５、インストーラ２０１６、遠隔操作端末用アプリケーション２０１７、暗号化通信路構築用アプリケーション２０１８、業務アプリケーション２０１９などである。

【００６７】

次に、管理者は、サーバ接続試験要求（６００７）を行い、サーバ接続試験が行われる（６００８）。サーバ接続試験６００８は、図５にて示した利用者が行うサーバへの接続や業務遂行のプロセスを管理者が行い、ストレージデバイス１０１４内に記録された情報やアプリケーションの有効性を確認するものである。接続と業務遂行プロセスが正しく行われた場合、ストレージデバイス１０１４は、利用者に送付される。この際、ストレージデバイス１０１４は利用者のＩＤや顔写真や氏名などを印刷されるか、シール針付けするなどされる。また、ストレージデバイス１０１４を管理するための情報に対するアクセスキーや暗証番号もストレージデバイス１０１４を送付するのとは別の封書などの方法で利用者に送付される。

【００６８】

図１１は、本実施例のクライアント１００１上で動作するミドルウェアについて説明した図である。クライアント１００１上で動作する遠隔操作端末用アプリケーション２０１７や暗号化通信路構築用アプリケーション２０１８、業務アプリケーション２０１９のようなアプリケーション１１０００は、図示するように２つの経路を利用してリーダライタ１０１２及びストレージデバイス１０１４にアクセスを行う。カード内のファイルアクセスやファイル管理を行いたい場合は、ファイルアクセス用ＡＰＩ１１００１、ファイルアクセス用ドライバ１１００２、リーダライタ１０１２内のリーダライタファームウェア１１００３を経由し、ストレージデバイス１０１４内のカードＯＳ及びアプリケーション１１００４が呼び出される。また、カード内の耐タンパデバイス２０３２に命令を発するなど、セキュリティ認証にかかわる命令を実行したい場合は、インターフェースハンドラ３０１５、デバイス３０１４、リーダライタ１０１２内のリーダライタファームウェア１１００３を経由し、ストレージデバイス１０１４内のカードＯＳ及びアプリケーション１１００４が呼び出される。この際、ファイルアクセス用ドライバ１１００２、リーダライタファームウェア１１００３、デバイス３０１４は、お互いの命令が同時に発生することが無いように常にストレージデバイス１０１４とリーダライタ１０１２のアクセス状態を監視し、ストレージデバイス１０１４に対して適切なアクセスがなされるように、自身で命令のストックや拒否などの輻輳制御を行う。

【００６９】

図１３は、デバイスドライバ３０１４とファイルアクセス用ドライバ１１００２の行う輻輳制御をフローチャートを用いて説明した図である。ドライバ３０１４及び１１００２は、ＯＳの起動時などに初期化され、処理が開始される（１３０００）。ファイルアクセス用ドライバ１１００２への要求もしくは待機した要求があるかどうかチェックが行われ（１３００１）、要求があった場合、リーダライタを介したカードへのファイルアクセスが行われる（１３００２）。次に、デバイスドライバ３０１４への要求があるかどうかの

チェックが行われる（１３００３）。ある場合は、リーダライタを介したＣＰＵ２０３０へのアクセスが行われる（１３００４）。ファイルアクセス用ドライバ１１００２への要求がこの時点であるかどうかチェックが行われ（１３００５）、要求があった場合、ファイルアクセス用ドライバ１１００２への要求待機処理が行われる。この要求待機処理は、ファイルアクセス用ドライバ１１００２において行われ、要求待機用に作られたメモリ領域に、待機すべき要求がストックされる。ストックされた要求は、次に処理１３００２が実行される際に処理される。ただし、処理１３００２により処理が行われるまでのストックしている時間があらかじめ定めた一定量を超えた場合は、処理１３００５内で、アプリケーションへタイムアウトなど異常を通知し、処理を破棄する。デバイスドライバ３０１４への要求が終了したと認識できるかどうかチェックが行われ（１３００７）処理が完了しない場合は、処理１３００４から再処理が行われる。

【００７０】

また、ＯＳからの終了要求がチェックされ（１３００８）、要求が無い場合は、再び処理１３００１から処理が開始される。上記のようなデバイスドライバ３０１４及びファイルアクセス用ドライバ１１００２による輻輳制御により、リーダライタを介したストレージデバイス１０１４のアクセスは、一般的なストレージデバイスと同様に保たれる。輻輳制御とは、ファイルアクセスに関する命令と、耐タンパデバイスに対する命令との輻輳を制御することで、ファイルアクセス用ドライバ１１００２は、一般的なマスストレージデバイスドライバでも、マスストレージデバイスドライバに接続するアッパーフィルタドライバやローワーフィルタドライバで行ってもよい。また、リーダライタファームウェアに命令を退避させるメモリ領域もしくはバッファを設けて命令を待機させ、輻輳を制御してもよい。

【００７１】

さらに、輻輳制御について詳細に説明する。輻輳制御とは、下記に示すような待機処理もしくは競合解決処理を示す。ここで、輻輳を制御するのは、後述する待機させられたコマンドリストをクライアント上のメモリ領域に作成しソフトウェア的に処理しても良いし、リーダーライタのファームウェアにてソフトウェア的に解決しても良いし、リーダライタ上にバッファを設けてハードウェア的に解決しても良い。

【００７２】

図１４は、デバイスドライバ３０１４とファイルアクセス用ドライバ１１００２における輻輳制御により発せられるコマンドの様子を示すタイムチャートである。ＣＰＵ２０３０へのアクセスのためのコマンド１、コマンド２が順にドライバより発せられるようアプリケーションから指示があったとする。図１４のファイルアクセス用コマンドに示すようにコマンド１がストレージデバイス１０１４に発せられ、そのレスポンス１の応答がある。次にコマンド２がストレージデバイス１０１４に発せられ、そのレスポンス２の応答がある。このコマンドの発行、応答の間にファイルアクセス用コマンド３やコマンド４が発せられたとする。この際、ファイルアクセス用ドライバはコマンド３やコマンド４を待機させられたコマンドリストに格納する。図１３における処理１３００２においてＣＰＵ２０３０へのアクセスのためのコマンドからの入力が無いと判断される場合、待機させられたファイルアクセス用コマンド３が発せられ、そのレスポンス３の応答がある。次に待機させられたファイルアクセス用コマンド４が発せられ、そのレスポンス４の応答がある。全体として、ストレージデバイス１０１４に送受信されるコマンドとレスポンスは、例えば、図１４における「全てのコマンドとレスポンス」に示すように、順にコマンド１、レスポンス１、コマンド２、レスポンス２、コマンド３、レスポンス３、コマンド４、レスポンス４のようになる。

【００７３】

上記のように、本実施形態に示したクライアント１００１は、耐タンパストレージ機能を搭載したストレージデバイス１０１４を挿入しサーバ１０００を遠隔操作する事により、利用者に安全で、使い勝手良く利用できる業務システムを構成することが可能となる。

【００７４】

また、利用者は、利用するクライアント１００１からクライアント１００２に変更したとしても、クライアント１００１を利用するのと同様の操作感覚にて業務遂行を行うことができるため、利用者の使い勝手が向上する。

【００７５】

また、利用者が利用を停止する際には、利用者が利用していた一時記憶ファイルが消去されるため、クライアント１００１内の情報が第３者によって危険にさらされても利用者の利用した情報は安全に保護され、電源を切断したクライアント１００１からの利用者の利用した機密情報やプライバシーを含んだ情報はより漏洩しにくくなることにより、利用者の利便性を向上させる。

【００７６】

また、本実施の形態では、クライアント１００１及びサーバ１０００を別の構成として記載したが、逆にクライアント１００１がサーバ１０００の機能を兼ねたり、サーバ１０００をクライアント１００１の代わりに使用したりすることが可能でもよい。また、サーバ１０００、クライアント１００１、１００２は、ＰＣやＰｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｔｓ（ＰＤＡ）、ワークステーションであるように記載したが、高機能複写機、現金自動支払機（ＡＴＭ）、携帯電話、デジタルスチルカメラ、ビデオカメラ、音楽再生（録音）装置、販売時点商品管理システム、街角端末、Ｉｎｔｅｌｌｉｇｅｎｔ Ｔｒａｎｓｐｏｒｔ Ｓｙｓｔｅｍｓ（ＩＴＳ）用送信機、券売機、決済端末、改札機、自動販売機、入退室管理装置、ゲーム機、公衆電話、注文取り用携帯端末、電子財布、有料放送受信機、医療カード管理装置等として同様である。

【実施例２】

【００７７】

図７から図９用いて、本発明に係るセキュアリモートアクセスシステムの第２の実施形態を説明する。

【００７８】

図７は、本発明の第２の実施形態のリモートアクセスシステムを示す図である。

【００７９】

利用者の使用するサーバ１０００とクライアント１００１、ストレージデバイス１０１４は、第１の実施形態にて説明したものと同様である。ゲートウェイ７０００は、クライアント１００１とサーバ１０００の通信の暗号化と利用者、利用機器認証を行う中継機器である。

【００８０】

ゲートウェイ７０００は、一般的にファイヤーウォール、暗号化ゲートウェイ、バーチャルプライベートネットワーク(ＶＰＮ)ゲートウェイなどと呼ばれる。本実施例では、ゲートウェイ７０００は、ファイヤーウォールと暗号通信機能をインストールされたサーバ機であるとして説明を行うが、例えば、ネットワークルータや無線ＬＡＮアクセスポイント、ネットワークハブ、ブロードバンドルータなどでも良い。ネットワーク７００１は、例えばインターネットや地域ＩＰネットワークのような、公衆回線であり、ネットワーク１００６より通信内容の盗聴や改ざんの危険性の高いネットワークである。クライアント１００１は、ネットワーク７００１越しにサーバ１０００を遠隔操作するため、ゲートウェイ７０００とクライアント１００１の間にて暗号通信と暗号通信を行うための認証を行う。

【００８１】

ゲートウェイ７０００は、ＣＰＵ７００２、メモリ７００３、ストレージ７００４を持ち、動作時にストレージ７００４内に設定された暗号通信及び認証用アプリケーションがメモリ７００３にロードされＣＰＵ７００２にて通信の制御を行う。ゲートウェイ７０００は、認証用サーバ７００５に直接もしくはネットワークを経由して接続している。認証用サーバ７００５は、ゲートウェイ７０００にて暗号通信を行う際の認証情報を蓄積し、ゲートウェイ７０００の問合に対して応答したり、接続されたリーダライタ７００７を介して、ストレージデバイス１０１４の初期化や活性化、個人化などを行う。認証用サーバ

７００５は、内部認証局を持っていても良いし、外部の認証局の証明書リストや証明書リボケーションリストを管理し、ゲートウェイ７０００に通知する役割だけを持っていても良い。

【００８２】

図８に、本実施形態のリモートアクセスシステムを利用する際のストレージデバイス１０１４の初期化と利用者がクライアント１００１にストレージデバイス１０１４を挿入し、サーバ１０００を利用する際の管理者、利用者、ストレージデバイス１０１４、クライアント１００１、ゲートウェイ７０００、サーバ１０００間にて行われる通信の詳細を示した図を示す。

【００８３】

管理者は、ストレージデバイス１０１４を認証サーバ７００５と通信が可能なリーダライタ７００７に挿入する。管理者は、利用者の氏名ユーザ番号、電子メールアドレスやストレージデバイス固有の識別番号等をクライアント１００１を通じ、認証サーバ７００５に登録することにより、認証サーバ７００５より利用者の認証情報を作成する。利用者の認証情報及び証明書の作成と書き込み要求を行う（８００１）。ここで、ストレージデバイス１０１４は、既にストレージデバイス供給者から鍵証明書格納プログラム２０４６などの各種プログラムが書き込まれている。また、利用者の公開鍵証明書は、ストレージデバイス１０１４もしくは認証サーバ７００５もしくは管理者が別途生成した秘密鍵に対応する公開鍵を８００１にて送付することにより得られる。作成された認証情報と公開鍵証明書は、ストレージデバイス１０１４へ書き込まれる。次に管理者は、ストレージデバイス１０１４内の認証情報と鍵の利用権をコントロールするための情報を変更する（８００３、８００４）。この操作によってストレージデバイス１０１４は、署名要求や鍵書き換え要求、鍵のエクスポートインポート要求に対する利用権を変更される。利用権の変更は、情報に対するアクセスキーの変更や、暗証番号の変更である。変更されたアクセスキーや暗証番号は、管理者が保管したり、他の耐タンパデバイスに格納したり、利用者に通知する。

【００８４】

次に、管理者は、アプリケーションの書き込み要求を行い、認証サーバ７００５は、アプリケーションの書き込みを行う。ここで言うアプリケーションとは、デバイスアクセス用ライブラリ２０１２、デバイス管理用ツール２０１３、デバイスドライバ２０１４、インターフェースハンドラ２０１５、インストーラ２０１６、遠隔操作端末用アプリケーション２０１７、暗号化通信路構築用アプリケーション２０１８、業務アプリケーション２０１９などである。

【００８５】

次に、管理者は、サーバ接続試験要求（８００７）を行い、サーバ接続試験が行われる（８００８）。サーバ接続試験８００７は、ストレージデバイス１０１４内に記録された情報やアプリケーションの有効性を確認するものである。接続と業務遂行プロセスが正しく行われた場合、ストレージデバイス１０１４は、利用者に送付される（８００９）。この際、ストレージデバイス１０１４を管理するための情報に対するアクセスキーや暗証番号もストレージデバイス１０１４を送付するのとは別の封書などの方法で利用者に送付される。

【００８６】

次に、利用者はクライアント１００１の利用を開始するまでに利用者の認証情報やクライアント１００１を動作させるためのアプリケーションが保存されたストレージデバイス１０１４をクライアント１００１のリーダライタに接続する。利用者が、クライアント１００１を利用したことがない場合は、利用者はストレージデバイス１０１４内のインストーラ２０１６を利用し、デバイスドライバ２０１４やデバイス管理ツール２０１３や遠隔端末用アプリケーション２０１７のようなサーバ１０００を操作するために必要な情報もしくはアプリケーションをクライアント１００１にインストールする。この際、クライアント１００１によってストレージデバイス１０１４から直接実行できるアプリケーション

のインストールを行う必要はない。

【００８７】

利用者は、まずシーケンス８０１０に示すようにクライアント１００１にゲートウェイ接続要求を行う。クライアント１００１はゲートウェイ７０００にサーバ動作確認を行う（８０１１）ゲートウェイ７０００のリモート機器からのログインに対するセキュリティポリシーの設定によるが、利用者の認証をＰＫＩを用いた認証が必要もしくは可能である場合、ゲートウェイ７０００からの認証情報の要求（８０１２）、クライアント１００１からの証明書の要求（８０１３）、ストレージデバイス１０１４からの証明書の送信（８０１４）、クライアント１００１からの署名の要求（８０１５）が行われる。ストレージデバイス１０１４において署名を行う場合、利用者の認証が必要となる。利用者の認証は、暗証番号、パスワード、パスフレーズ、ワンタイムパスワード、指紋情報などの生体認証情報などにより行われる。本実施例では、暗証番号を利用した例を示す。ストレージデバイス１０１４からの暗証番号要求（８０１６）が行われた後、クライアント１００１から利用者へ暗証番号要求表示（８０１７）がディスプレィ１００８などを利用して行われる。利用者が暗証番号をユーザインターフェース１０１０とクライアント１００１を介してストレージデバイス１０１４に送信すると（８０１８、８０１９）、ストレージデバイス１０１４内のＣＰＵ２００１もしくはＣＰＵ２０３０においてサーバ１０００、クライアント１００１から送信された情報に対し、秘密鍵２０４０のうちの一つもしくはいくつかを用いた電子署名が作成される（８０２０）。作成された署名は、クライアントに送信される（８０２１）。クライアント１００１は、証明書２０１０、２０４３などの認証情報と作成された署名の送信を行う（８０２２）。次に、サーバ１０００及びクライアント１００１は、秘密鍵や公開鍵といったお互いの鍵情報と証明書を利用して、秘密共有鍵の鍵交換を行う（８０２３）。この鍵交換８０２３は、暗号化通信路構築用アプリケーション２０１８により行われる。シークエンス８０２３において交換された秘密共有鍵を用いて、ゲートウェイ７０００及びクライアント１００１は暗号化通信路を構築し、２者の間で通信される情報は暗号化される。

【００８８】

次に、利用者は、シーケンス８０３０に示すようにクライアント１００１に動作確認要求を行う。クライアント１００１はサーバ１０００にサーバ動作確認を行う（８０３１）利用者はサーバ１０００の動作を確認できなかった場合は、ストレージデバイス１０１４もしくはインストーラ２０１６にてクライアント１００１上に用意された遠隔地からサーバの電源を投入するＬＡＮを利用して機器の電源投入を行うようなＷａｋｅ ｕｐ ｏｎ ＬＡＮのような機能を利用してサーバ１０００の電源投入を行う。この場合、サーバ１０００の、ネットワークに対するＩ／Ｆは常時通電されており、ＩＤとパスワードのセットやネットワークボードのＭＡＣアドレス等、何らかの認証情報を利用してサーバ１０００の起動が行われる（８０３２、８０３３）。この操作によりサーバ１０００は起動される（８０３４）。サーバの起動が完了した際、利用者はクライアント１００１にログイン要求を入力する（８０３５）。この操作は、クライアント１００１内の遠隔操作アプリケーション２０１７により行われる。遠隔操作アプリケーションがインストールされていない場合、この時点にてクライアント１００１にロードされる。サーバ１０００のリモート機器からのログインに対するセキュリティポリシーの設定によるが、ログインに際し、利用者の認証をＰＫＩを用いた認証が必要もしくは可能である場合、サーバ１０００からの認証情報の要求などが行われ、８０１２～８０２３と同様の署名の作成と送信がサーバ１０００に対し行われる。利用者は、ゲートウェイ７０００において強固な認証を通過しているので、サーバ１０００がゲートウェイ７０００からの通信を信頼できるとすると、ログイン要求８０３５を行う際のサーバ１０００の認証はＩＤとパスワード認証などの簡便なものでも良い。

【００８９】

暗号化通信路構築とサーバ１０００へのログインが完了した段階で、ユーザは、サーバ１０００または、クライアント１００１、ストレージデバイス１０１４上に保存されてい

るアプリケーションを起動し、業務遂行をする（８０３６）。

【００９０】

業務遂行中は、ＣＰＵ２００１もしくはＣＰＵ２０３０もしくはサーバ１０００もしくはクライアント１００１は、ログ情報２０１１、２０４２、３０１１に情報を追記し、利用者の業務遂行を適切に監視する。記載されたログ情報は、改ざん防止の処理を施され、ストレージデバイス１０１４やクライアント１００１内に保存されるが、利用者の利用開始時や利用終了時など適切なタイミングでサーバ１０００に送信される。

【００９１】

利用者の利用するサーバ１０００の管理を行う管理者は、ログ情報２０１１、２０４２、３０１１の情報とサーバ１０００に送信される情報を監査し、利用者が管理者が作成したポリシーに違反する利用を行った際に、サーバ１０００もしくはクライアント１００１もしくは、ストレージデバイス１０１４の利用を停止するようなオペレーションを行う。ポリシー違反は、例えば、ログの改ざんや、異常な利用時間、異常な通信量、ネットワーク１００６を介した異常なアクセス、クライアント１００１内に存在する異常なファイルの検出、ファイルやアプリケーションのアップデートの不備などが該当する。サーバ１０００もしくはクライアント１００１もしくは、ストレージデバイス１０１４の利用を停止するようなオペレーションとは、サーバ１０００及びクライアント１００１への利用者のログインの禁止や電源遮断、ストレージデバイス１０１４の閉塞などが該当する。ストレージデバイス１０１４の閉塞とは、ＰＩＮ検証プログラム２０４５の利用する情報を変更し、利用者がストレージデバイス１０１４を利用できないようにすることである。利用者の業務など、サーバ１０００の利用が終了した場合、利用者は、クライアント１００１に対しサーバ遮断要求を行う（８０３７）。サーバ遮断要求はクライアント１００１からサーバ１０００に送信される（８０３８）。サーバ１０００及びクライアント１００１はセッションの遮断８０３９を行う。サーバ１０００は、利用者の利用情報のログをサーバ１０００上に記憶し（８０４０）、サーバ１０００のサーバ電源遮断を行う。利用者がサーバ遮断要求８０３７を行わなければ、サーバ電源遮断８０４１は行われない。サーバ電源遮断後は、また８０１０以降のシーケンスで業務遂行が行われる。

【００９２】

図９に、本実施形態のリモートアクセスシステムのネットワーク構成を示したブロック図を示す。図中９０００にて示されたネットワークとネットワークに接続した機器のグループは、利用者が中心的に利用するネットワークと機器のグループである。ネットワークと機器のグループ９０００は、例えば、利用者が常に勤務するオフィスのローカルエリアネットワーク（ＬＡＮ）とＬＡＮに接続された機器である。９０００内には、ユーザの利用可能なサーバ１０００、クライアント１００２、部門サーバ９００１、ＰＣ９００２、ゲートウェイ９００６、７０００、認証サーバ７００５がＬＡＮ９００３を中心に接続されている。また、９０１０にて示されたネットワークとネットワークに接続した機器のグループは、利用者が出張時などに利用する所属外の事業部などのＷＡＮ上のネットワークと機器のグループである。９０１０内には、ユーザの利用可能なクライアント９００８、ゲートウェイ９００７がネットワーク９００５を中心として接続されている。また、ネットワーク７００１のような社外のネットワークにルータ９００４を介してクライアント１００１が接続されている。

【００９３】

ここで、利用者は、ストレージデバイス１０１４を持ち歩くことにより、ＬＡＮ上のクライアント１００２、ＷＡＮ上のクライアント９００８、インターネットを介しＬＡＮ９００３に接続しているクライアント１００１を利用して、ＬＡＮ９００３と接続されたサーバ１０００、部門サーバ９００１、ＰＣ９００２を利用することができる。この際、ＬＡＮ上のクライアント１００２、ＷＡＮ上のクライアント９００８からＬＡＮ９００３と接続されたサーバ１０００、部門サーバ９００１、ＰＣ９００２を利用する際は、ゲートウェイ９００７、９００６では、通信の暗復号を行わず、ゲートウェイ７０００を利用する場合、通信の暗復号を行うようにすれば、利用者の利用手順の簡略化を図りつつ、通信

内容の秘匿が可能である。ここで、部門サーバ９００１とは、ＬＡＮ上に設置されたウェブサーバやメールサーバやリモートログインして演算を行うターミナルサーバなどを示す。ＰＣ９００２は、利用者の所属する部門が共有などで利用している共有リソース管理用ＰＣや出張者用貸し出しＰＣなどを示す。

【００９４】

上記のように、本実施形態に示したクライアント１００１は、耐タンパストレージ機能を搭載したストレージデバイス１０１４を挿入しサーバ１０００、部門サーバ９００１、ＰＣ９００２などを遠隔操作することにより、利用者に安全で、使い勝手良く利用できる業務システムを構成することが可能となる。

【００９５】

また、利用者は、利用するクライアント１００１からクライアント１００２、９００８に変更したとしても、様々な異なる業務執行場所において、クライアント１００１を利用するのと同様の操作感覚にて業務遂行を行うことができるため、利用者の使い勝手が向上する。また、サーバ１０００、クライアント１００１、１００２、９００８は、ＰＣやＰＤＡ、ワークステーションであるように記載したが、高機能複写機、ＡＴＭ、携帯電話、デジタルスチルカメラ、ビデオカメラ、音楽再生（録音）装置、販売時点商品管理システム、街角端末、ＩＴＳ用送信機、券売機、決済端末、改札機、自動販売機、入退室管理装置、ゲーム機、公衆電話、注文取り用携帯端末、電子財布、有料放送受信機、医療カード管理装置等として同様である。

【実施例３】

【００９６】

図１０を用いて、本発明に係るセキュアリモートアクセスシステムの第３の実施形態を説明する。

【００９７】

図１０は、本発明の第３の実施形態を示すリモートアクセスシステムを示す図である。

【００９８】

利用者の使用するサーバ１００００は、サーバ１０００と同等の機能をもつ複数個のサーバ（ＰＣ）の集合体である。サーバ１００００はサーバ１００３２、１００４２、…、１００５２上にある、それぞれＣＰＵ１００３０、１００４０、…、１００５０、メモリ１００３１、１００４１、…、１００５１により動作する。図１０では、利用者は、サーバ１００３２を利用し、ＣＰＵ１００３０上にて実行された情報をディスプレィ１００８に出力させて業務を遂行している。サーバ１００００は、切り替え器１０００４を利用してサーバ１００３２、１００４２、…、１００５２と接続するユーザインターフェース１０００３及びディスプレィ１００００２を選別している。また、サーバ１００００は、制御装置１００００１に接続されている。制御装置１００００１は、ネットワーク１００５に接続しており、サーバ１００００と同様にストレージデバイス１０１４を持つ適切な利用者が利用可能である。ここで、利用者がサーバ１００３２、１００４２、…、１００５２のいずれかを利用しようとした際に、制御装置１００００１は、サーバ１００３２、１００４２、…、１００５２の電源管理、電源のオンオフ、状態のクライアントへの通知を行う。特に、クライアント１００１からのサーバ１００３２、１００４２、…、１００５２への通信が不通になった際は、利用者は、制御装置１００００１にログインし、サーバ１００３２、１００４２、…、１００５２の状態を確認したり、電源をオンオフしたりする。制御装置１００００１内にはハードディスクやフラッシュメモリなどのサーバブート用のストレージが実装してあり、このストレージ上のデータを用いてサーバ１００３２～１００５２がブートアップする。このことにより、利用者のサーバ管理の工数が減少する。

【００９９】

上記のように、本実施形態に示したサーバ１００００及び制御装置１００００１を、耐タンパストレージ機能を搭載したストレージデバイス１０１４を挿入したクライアント１００１より利用することにより、サーバ１００００は、１つの筐体の内部に複数の類似した機能を持つサーバを持つ特長から、管理者のサーバ１００３２、１００４２、…、１００

５２の管理工数を削減することができる。また、利用者が制御装置１００００１を利用することによりサーバの電源管理などが容易に行えるため、利用者の使い勝手が向上する。

【実施例４】

【０１００】

図１、図１５、図１６を用いて、本発明に係るセキュアリモートアクセスシステムの第４の実施例を説明する。本実施形態は、セキュアリモートアクセスシステムを利用する利用者が、多くの人間が使用するような公衆のクライアント機器を介して業務を遂行する場合に有効である。

一般に、公衆のクライアント機器には、ある個人あるいは複数の利用者が使用するためのアプリケーションや個人的な設定情報などが保存されている。本実施形態では、それらアプリケーションや個人設定情報をクライアント機器１００１内部のストレージ３００２にインストールや格納をしないようなセキュアリモートアクセスシステムを提示する。さらに、利用者の操作量を軽減することによって利便性の高いセキュアリモートアクセスシステムを提示する。

【０１０１】

図１５は、本発明の第４の実施例におけるストレージデバイス１０１４の詳細を示したブロック構成図である。本実施例では、第１の実施例におけるストレージデバイス１０１４内部のストレージ１０１７の中に、新たにブートプログラム１５００１とＯＳプログラム１５００２を追加する。ブートプログラム１５００１は、クライアント１００１が起動される際に、そのＢＩＯＳ（Basic Input/Output System）によって最初に実行されるプログラムであり、クライアント１００１用のＯＳを起動させる役割を持つ。ＯＳプログラム１５００２は、前記ブートプログラム１５００１によってストレージデバイス１０１４からクライアント１００１内部のメモリ３００１上に読み込まれ起動されるクライアント１００１用のＯＳのプログラムである。

【０１０２】

利用者の使用するサーバ１０００とクライアント１００１、１００２は、第１の実施例にて説明したものと同様である。

【０１０３】

図１６は、利用者がクライアント１００１に図１５に示したストレージデバイス１０１４を挿入し、サーバ１０００を利用する際の利用者、ストレージデバイス１０１４、クライアント１００１、サーバ１０００間にて行われる通信の詳細を示した図である。利用者はクライアント１００１を起動するまでに利用者の認証情報やクライアント１００１を動作させるためのブートプログラム、ＯＳプログラム、アプリケーション等が保存されたストレージデバイス１０１４をクライアント１００１のリーダライタ１０１２に接続しておく必要がある。また、クライアント１００１のＢＩＯＳは、リーダライタ１０１２を通してブートプログラムを検出するのが、ストレージ３００２を通して検出するのに優先するようにあらかじめ設定されている必要がある。第１の実施例との違いは、利用者がクライアント１００１を利用したことがない場合でも、利用者はデバイスドライバ２０１４やデバイス管理ツール２０１３や遠隔端末用アプリケーション２０１７のようなサーバ１０００を操作するために必要な情報もしくはアプリケーションをクライアント１００１のストレージ３００２にインストールする必要がないことである。

【０１０４】

利用者は、まずシーケンス１６００１に示すようにクライアント１００１の電源を投入する。それによってクライアント１００１のＢＩＯＳが起動し（１６００２）、ストレージデバイス１０１４にブートプログラム１５００１を要求する（１６００３）。ストレージデバイス１０１４は、これに応じてブートプログラム１５００１を送信する（１６００４）。クライアント１００１のＢＩＯＳはブートプログラム１５００１を実行してブート処理を開始する（１６００５）。ブート処理の中では、ブートプログラム１５００１によって、ストレージデバイス１０１４にＯＳプログラム１５００２を要求する（１６００６）。ストレージデバイス１０１４は、これに応じてＯＳプログラム１５００２を送信する

（１６００７）。ＯＳプログラム１５００２は、クライアント１００１内部のメモリ３００１上に読み込まれ、起動される（１６００８）。これ以降、ストレージデバイス１０１４に格納されているアプリケーション、ライブラリ、ドライバ、管理ツール等（２０１２～２０１９）は、このＯＳ上に読み込まれて動作することが可能となる。ＯＳプログラム１５００２にはＯＳ起動直後自動的に特定のアプリケーションを実行するように記述されている。これに従い、クライアント１００１は遠隔操作アプリケーション２０１７及び暗号化通信路構築用アプリケーション２０１８、さらにその実行に必要なライブラリ、ドライバ等をストレージデバイス１０１４に要求する（１６００９）。ストレージデバイス１０１４は、これに応じてそれらのアプリケーションを送信する（１６０１０）。そして、クライアント１００１はそれらのアプリケーションを起動する（１６０１１）。

【０１０５】

それらのアプリケーションのプログラムには、利用者が接続したいサーバのＩＰアドレスがあらかじめ記述されている。クライアント１００１は自動的にそのＩＰアドレスのサーバ１０００に動作確認を行う（１６０１２）。クライアント１００１はサーバ１０００の動作を確認できなかった場合は、Ｗａｋｅ ｏｎ ＬＡＮのような機能を利用してサーバ１０００の電源投入を行う。この場合、サーバ１０００の、ネットワークに対するＩ／Ｆのみは常時通電されており、ＩＤとパスワードのセットやネットワークボードのＭＡＣアドレス等、何らかの認証情報を利用してサーバ１０００の起動が要求される（１６０１３）。これによりサーバ１０００は起動される（１６０１４）。サーバの起動が完了した際、クライアント１００１から自動的にサーバ１００１にログイン要求が行われる（１６０１５）。サーバ１０００のリモート機器からのログインに対するセキュリティポリシーの設定によるが、ログインに際し、利用者の認証において公開鍵インフラストラクチャ（ＰＫＩ）を用いた認証が必要もしくは可能である場合、サーバ１０００からクライアント１００１に認証情報を要求し（１６０１６）、クライアント１００１からストレージデバイス１０１４に証明書を要求し（１６０１７）、ストレージデバイス１０１４からクライアント１００１に証明書を送信し（１６０１８）、クライアント１００１からストレージデバイス１０１４に署名を要求する（１６０１９）。

【０１０６】

ストレージデバイス１０１４において署名を行う場合、利用者の認証が必要となる。利用者の認証は、暗証番号、パスワード、パスフレーズ、ワンタイムパスワード、指紋情報などの生体認証情報などにより行われる。本実施例では、暗証番号を利用した例を示す。ストレージデバイス１０１４からの暗証番号要求（１６０２０）が行われた後、クライアント１００１から利用者へ暗証番号要求表示１６０２１がディスプレィ１００８などを利用して行われる。利用者が暗証番号をユーザインターフェース１０１０とクライアント１００１を介してストレージデバイス１０１４に送信すると（１６０２２、１６０２３）、ストレージデバイス１０１４内のＣＰＵ２００１もしくはＣＰＵ２０３０においてサーバ１０００、クライアント１００１から送信された情報に対し、秘密鍵２０４０のうちの一つもしくはいくつかを用いた電子署名が作成される（１６０２４）。作成された署名は、クライアントに送信される（１６０２５）。クライアント１００１は、証明書２０１０、２０４３などの認証情報と作成された署名の送信を行う（１６０２６）。

【０１０７】

次に、サーバ１０００及びクライアント１００１は、秘密鍵や公開鍵といったお互いの鍵情報と証明書を利用して、秘密共有鍵の鍵交換を行う（１６０２７）。この鍵交換１６０２７は、遠隔操作端末用アプリケーション２０１７か暗号化通信路構築用アプリケーション２０１８により行われる。シーケンス１６０２７において交換された秘密共有鍵を用いて、サーバ１０００及びクライアント１００１は暗号化通信路を構築し、２者の間で通信される情報は暗号化される。暗号化通信路が構築された段階で、利用者は、サーバ１０００、クライアント内のメモリ３００１、またはストレージデバイス１０１４上に格納されているアプリケーションを起動し、業務遂行をする（１６０２８）。

【０１０８】

業務終了後、クライアント１００１は図５のシーケンス４０２１～４０２５のようにサーバ１０００との通信を遮断し、利用者はクライアント１００１の電源を切断してストレージデバイス１０１４をリーダライタ１０１２から抜き取る。これによって、メモリ３００１上の情報も揮発するため、クライアント１００１内部には利用者が使用したアプリケーションや個人情報などが一切残らない。これにより、公衆のクライアントを使用したセキュアリモートアクセスシステムにおいて、利用者のプライバシーが保護される。

【０１０９】

また、クライアント１００１上で動作するＯＳプログラムは利用者自身がストレージデバイス１０１４内に管理しているので、クライアントにインストールされているＯＳに第３者がひそかに設置したコンピュータウイルス等の不正プログラムにより利用者の暗証番号が盗聴されるなどの危険も回避される。これにより、公衆のクライアントを使用したセキュアリモートアクセスシステムにおいて、利用者のセキュリティも保護される。

【０１１０】

また、図１６のように、利用者がクライアント１００１の利用を開始してから業務対象サーバ１０００に接続するまでの間の過程は、ブートプログラム１５００１とＯＳプログラム１５００２によって自動化されているので、利用者の操作は電源投入１６００１と暗証番号送信１６０２２のみである。これにより、利用者にとってのセキュアリモートアクセスシステムの利便性が向上する。

【実施例５】

【０１１１】

第５の実施例は、第４の実施例におけるセキュアリモートアクセスシステムを利用する利用者が、安全であると信用できるクライアントを介して業務を遂行する場合に有効である。

【０１１２】

第４の実施例におけるセキュアリモートアクセスシステムでは、クライアント１００１で動作するＯＳをストレージデバイス１０１４から読み出している。しかし、利用者が公衆クライアント機器のように安全性が保証されないクライアント機器ではなく、自身の所有するＰＣやレンタルオフィスや出張先の管理されたオフィスのＰＣのように安全であると信用できるクライアントを使用する場合には、ＯＳをストレージデバイス１０１４から読み出さずに、クライアント内にインストールされているＯＳを利用してもよい。

【０１１３】

そのため、本実施例のリーダライタ１０１２は起動モードを選択する機能を有する。具体的には、図１７（a）のように機械的なスイッチを搭載している。このスイッチは、第４の実施例におけるブートプログラム１５００１をストレージデバイス１０１４からクライアント１００１に送信可能にしたり、不可能にしたりを切り替えることができる。このスイッチでブートプログラム１５００１を送信可能にすれば、セキュアリモートアクセスシステムは図１６のように（つまり、第４の実施例のように）動作する。

【０１１４】

一方、ブートプログラム１５００１を送信不可能にすれば、ＯＳプログラム１５００２ではなくクライアント内にインストールされているＯＳが起動するため、セキュアリモートアクセスシステムは図５のように（つまり、第１の実施例のように）動作する。図１７（ａ）はその処理を示した図である。利用者は、スイッチ１７０００でブートプログラム１５００１を送信するか送信しないかを選択する。ブートプログラムを送信しないことを選択した場合、ストレージデバイス１０１４からは、クライアント機器へダミーデータ１７００１が送信される。ダミーデータ１７００１がクライアント１００１のメモリ３００１上にロードされると、ＢＩＯＳはストレージデバイス１０１４を通してのＯＳ起動に失敗するため、その代わりにストレージ３００２内のＯＳを起動する。

【０１１５】

なお、該スイッチ等の切替手段を用いて、記憶媒体側（リーダライタ１０１２も含む）からＯＳプログラム１５００２の送信可否を選択してもよい。但し、この場合、ブートプ

ログラムは記憶媒体側からクライアント機器へ送られている。該切替手段を操作し、ＯＳプログラムを送らない設定とした場合、記憶媒体側からクライアント機器へはダミーデータが送信される。ダミーデータを受信したブートプログラムは、ブートプログラムに予め設定されたＯＳプログラムの読み込み先の機器からＯＳプログラムを読み出すこととなる。この場合、ＯＳプログラムの読み込み先の機器としては、クライアント１００１内のストレージ３００２でも、ネットワーク上の計算機上のストレージでも良い。

【０１１６】

また、図１７（ａ）、（ｂ）において記憶媒体側からのブートプログラムの送信が拒否された場合であって、かつ、クライアント機器側のブートプログラムをロードした場合も、上記と同様に、該ブートプログラムの内容によって、自機器あるいは他の機器の記憶装置からＯＳプログラムを読み出すことが可能である。

【０１１７】

このような起動モードを選択するための機械的なスイッチは、ストレージデバイス１０１４に搭載してもよい。一般に、ＰＣ用のディスクデバイスにおいて、ブートプログラムが格納されている領域は最初の論理セクタアドレスで示される領域である。このスイッチでその領域のデータの読み出しを許可するか否かを切り替えることによって、ブートプログラム１５００１の送信を制御できる。結果として、このスイッチで起動モードを選択することができる。図１７（ｂ）はその処理を示した図である。スイッチ１７００２でブートプログラム１５００１を送信するかダミーデータ１７００３を送信するかを選択する。ダミーデータ１７００３がクライアント１００１のメモリ３００１上にロードされると、ＢＩＯＳはストレージデバイス１０１４を通してのＯＳ起動に失敗するため、その代わりにストレージ３００２内のＯＳを起動する。

【０１１８】

起動モードを選択するもう１つの方式としては、ブートプログラム１５００１がクライアント１００１を構成する様々なデバイスを調査することによって、それが安全な端末であると信用できるか否かを判別する方法である。図１７（ｃ）はその処理を示した図である。メモリ３００１上にロードされたブートプログラム１５００１がクライアント１００１を信用できないものと判断したならば、ＯＳプログラム１５００２をメモリ３００１上にロードして起動する。信用できるものと判断したならば、ストレージ３００２内のＯＳを起動する。なお、クライアント１００１内のデバイスを調査する際に、ストレージデバイス１０１４内の耐タンパデバイス１０１６を利用してデバイス認証処理を実行すれば、より信頼性の確証が得られる。この場合、あらかじめ耐タンパデバイス１０１６内のストレージ２０３２内にデバイス認証処理プログラムやデバイス認証処理に必要な鍵や証明書などを格納しておき、ブートプログラム１５００１からの指示によってストレージデバイス１０１４内のＣＰＵ２０３０がデバイス認証処理を実施するのが好ましい。ブートプログラム１５００１がクライアント１００１を構成する様々なデバイスを調査する方法は、例えば、ブートプログラム１５００１がクライアント１００１内にあるかクライアント１００１に接続されているＣＰＵやメモリ、ストレージデバイス、ネットワークカードなどに割り当てられた製造番号やＭＡＣアドレスのように番号と部品に１対１につけられた番号や証明書を調査や検証することである。この番号や証明書は各ＣＰＵやメモリ、ストレージデバイス、ネットワークカードの製造者やクライアントや部品の製造者や管理者などが番号付けを行う。

【０１１９】

図１７（ｃ）において起動モードを選択するもう１つの方法としては、ストレージ３００２内のＯＳが暗号化やパスワードロックがかかった状態であるかどうかを調査してから、ＯＳプログラム１５００２をメモリ３００１上にロードして起動するようにしても良い。この場合、上記したデバイス認証は記憶媒体側のＣＰＵ２０３０が行い、ストレージ３００２内のＯＳが暗号化やパスワードロックがかかった状態であるかどうかの調査はクライアント機器側のＣＰＵ３０００が行うこととなる。

【０１２０】

図１８は、図１７（ｃ）を用いて説明した第５の実施例のＯＳの起動を行う際の動作を説明するためのフローチャートである。

ブートプログラムの起動後（１８０００）、上述した方法により、クライアント１００１に記憶媒体からロードされたブートプログラム１５００１が、デバイス認証に必要な情報を集めてＣＰＵ２０３０に送信して、該ＣＰＵ２０３０でデバイス認証が成功したかどうかが判定される（１８００１）。

判定結果が認証成功(ＹＥＳ)であった場合、ストレージ３００２がパスワードロックなどのロック機能や暗号化機能によってパスワード等の情報の入力無しには内部に格納されているＯＳなどのデータを読み取ることができないようになっているかどうか判定される（１８００２）。

【０１２１】

次にストレージデバイス１０１４から認証情報が取得できるかが判定される（１８００３）。１８００３での判定が失敗した場合（ＮＯ）、利用者からロックや暗号化を解除する情報の入力を促すよう画面表示し、入力をＣＰＵ３０００およびストレージ３００２に送信する（１８００４）。１８００３の判定に成功（ＹＥＳ）した場合もしくは、１８００４の動作を終了した場合、ストレージ３００２は受け取った情報を用いて、例えばパスワードの比較など、内部に格納されている情報に受け取った情報が適合しているかどうか検査を行う（１８００５）。受け取った情報が検査に合格すれば（ＹＥＳ）、利用者はストレージ３００２の正当な利用権を持つことが証明されるので、ストレージ３００２内部に格納されているＯＳプログラム１５００２やその他のデータが利用可能になる。よって、ストレージデバイス３００２を用いてＯＳの起動が行われ（１８００６）、ＯＳの起動は終了する（１８００７）。１８００２の判定が失敗（ＮＯ）だった場合は、ロックや暗号化がされていないということであるため、ストレージデバイス３００２を用いてＯＳの起動が行われ（１８００６）、ＯＳの起動は終了する（１８００７）。１８００５の判定に失敗した（ＮＯ）場合、もしくは、１８００１の判定に失敗した場合（ＮＯ）、ＯＳプログラム１５００２をメモリ３００１上にロードして起動し（１８００８）、ＯＳの起動は終了する（１８００９）。

【０１２２】

なお、図１７（ｃ）において認証の判断結果に基づきＯＳの読込先の切り替えを行う手段は、スイッチのような機械的手段でもよいし、コントローラとバスの組み合わせのようなソフトウェア的手段でもよい。

【０１２３】

以上のように、実施例５に示したストレージデバイス及びリーダライタ及びクライアントを利用することにより、クライアントが信頼できるか否か、または、クライアント内のＯＳやストレージが利用できるか否か等を判定して適切に利用者の利用すべきブートプログラムやＯＳプログラムを選択することができ、利用者のクライアントを利用する際の安全性を高めることができる。また、自動的に起動すべきＯＳを選択したり、認証情報を入力させることにより、利用者の利便性を高めたセキュアリモートアクセスシステムを提供できる。

【図面の簡単な説明】

【０１２４】

【図１】本発明の第１の実施形態のセキュアリモートアクセスシステムを説明するためのブロック構成図。

【図２】本発明の第１の実施形態のストレージデバイスを説明するためのブロック構成図。

【図３】本発明の第１の実施形態の認証情報のコピーの構成を示す図。

【図４】本発明の第１の実施形態のクライアントの詳細を示したブロック構成図

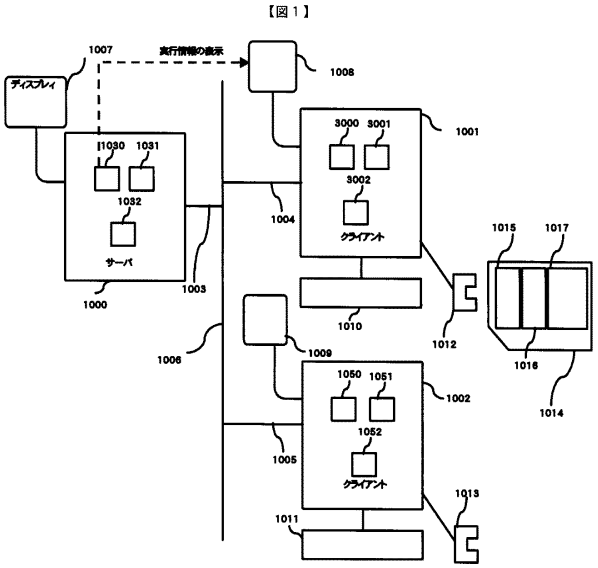
【図５】本発明の第１の実施形態の利用者、ストレージデバイス、クライアント、サーバ間にて行われる通信の詳細を示した図

【図６】本発明の第１の実施形態の管理者が行うストレージデバイスの初期化操作を説明

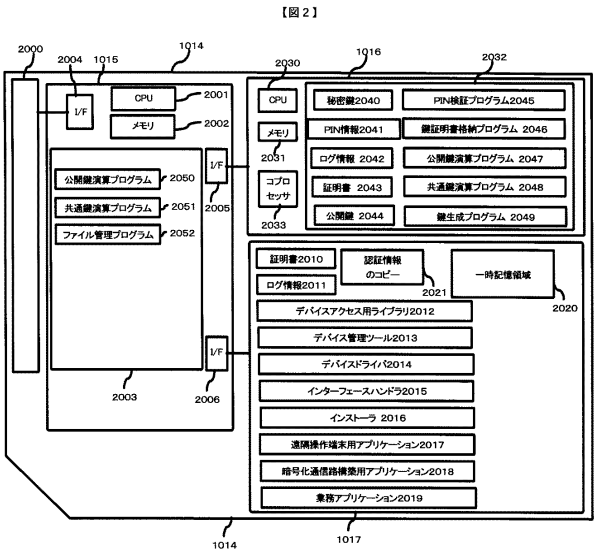
した図
【図７】本発明の第２の実施形態のリモートアクセスシステムを示す図
【図８】本発明の第２の実施形態の利用者、管理者、ストレージデバイス、クライアント、ゲートウェイ、サーバ間にて行われる通信の詳細を示した図
【図９】本発明の第２の実施形態のリモートアクセスシステムのネットワーク構成を示したブロック図
【図１０】本発明の第３の実施形態を示すリモートアクセスシステムを示す図
【図１１】本発明の第１の実施形態のソフトウェア構成を示す図
【図１２】本発明の第１の実施形態のアプリケーションから一時記憶領域を利用する際の処理方法を示すフローチャート
【図１３】本発明の第１の実施形態のドライバにおける輻輳制御を行う際の処理方法を示すフローチャート
【図１４】本発明の第１の実施形態のドライバにおける輻輳制御を示すタイムチャート
【図１５】本発明の第４の実施形態のストレージデバイスを説明するためのブロック構成図
【図１６】本発明の第４の実施形態の利用者、ストレージデバイス、クライアント、サーバ間にて行われる通信の詳細を示した図
【図１７】本発明の第５の実施形態のストレージデバイス、リーダライタ、クライアント間にて行われる処理を示した図
【図１８】本発明の第５の実施形態のＯＳの起動を行う際の動作を説明するためのフローチャート
【符号の説明】
【０１２５】
１０００…サーバ、１００１、１００２…クライアント、１００３、１００４、１００５…ネットワークケーブル、１００６…ネットワーク、１００７、１００８、１００９、１０００２…ディスプレィ、１０１０、１０１１、１０００３…ユーザインターフェース、１０１２、１０１３…リーダライタ、１０１４…ストレージデバイス、１０１５…コントローラ、１０１６…耐タンパデバイス、１０１７、１０３２、１０５２、２０３２、３００２、７００４…ストレージ、１０３０、１０５０、２００１、２０３０、３０００、７００２、１００３０、１００４０、１００５０…ＣＰＵ、１０３１、１０５１、２００２、２０３１、３００１、７００３、１００３１、１００４１、１００５１…メモリ、２０００…端子、２００３…不揮発メモリ２００３、２００４、２００５、２００６、３０２０、３０２１、３０２２、３０２３…インターフェース、２０５０…公開鍵演算プログラム、２０５１…共通鍵演算プログラム、２０５２…ファイル管理プログラム、２０４０…秘密鍵、２０４１…ＰＩＮ情報、２０４２…ログ情報、２０４３…証明書２０４３、２０４４…公開鍵２０４４、２０４５…ＰＩＮ検証プログラム、２０４６…鍵証明書格納プログラム、２０４７…公開鍵演算プログラム、２０４８…共通鍵演算プログラム、２０４９…鍵生成プログラム、５００１…証明書１、５００２…証明書２、５００３…証明書Ｎ、５００４…ミドルウェアの認証情報、３０１０…証明書、３０１１…ログ情報、３０１２…デバイスアクセス用ライブラリ、３０１３…デバイス管理用ツール、３０１４…デバイスドライバ、３０１５…インターフェースハンドラ、３０１６…遠隔操作端末用アプリケーション、３０１７…暗号化通信路構築用アプリケーション、３０１８…業務アプリケーション、７０００…ゲートウェイ、７００１…ネットワーク、７００５…認証用サーバ、７００７…リーダライタ、９００１…部門サーバ、９００２…ＰＣ、９００３…ＬＡＮ、９００４…ルータ、９００５…ネットワーク、９００６、９００７…ゲートウェイ、９００８…クライアント、１００００、１００３２、１００４２、１００５２…サーバ、１０００１…制御装置、１００００４…切り替え器、１１０００…アプリケーション、１１００１…ファイルアクセス用ＡＰＩ、１１００２…ファイルアクセス用ドライバ、１１００３…リーダライタファームウェア、１１００４…カードＯＳ及びアプリケーション、１５００１…ブートプログラム、１５００２…ＯＳプログラム、１７０００、１７００２…スイ

ッチ、１７００１、１７００３…ダミーデータ。

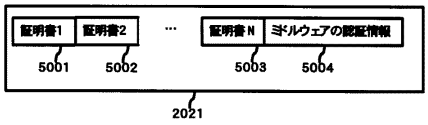
【図１】



【図２】

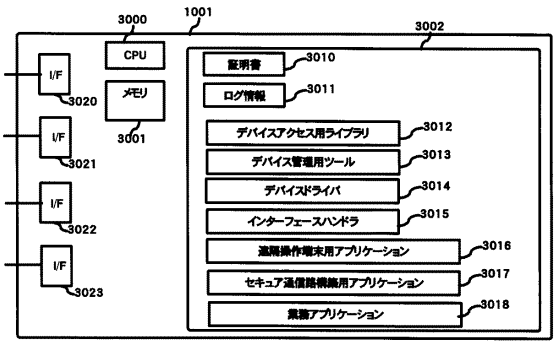


【図３】



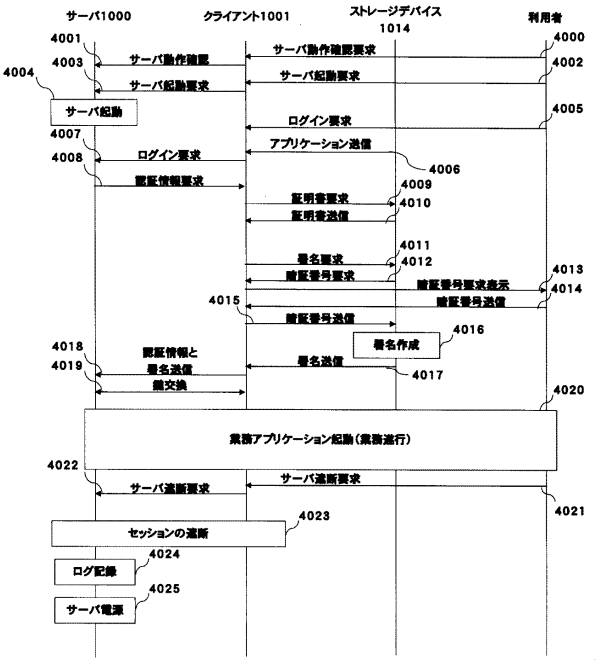
【図４】

【図４】



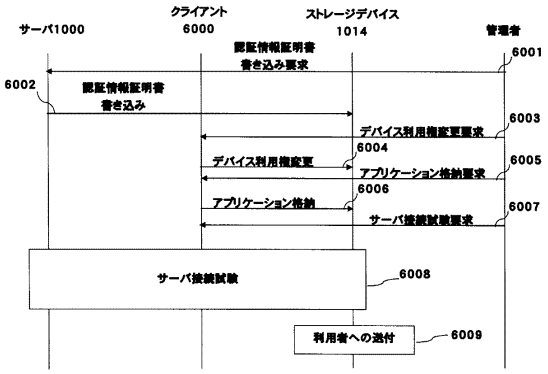
【図５】

【図５】



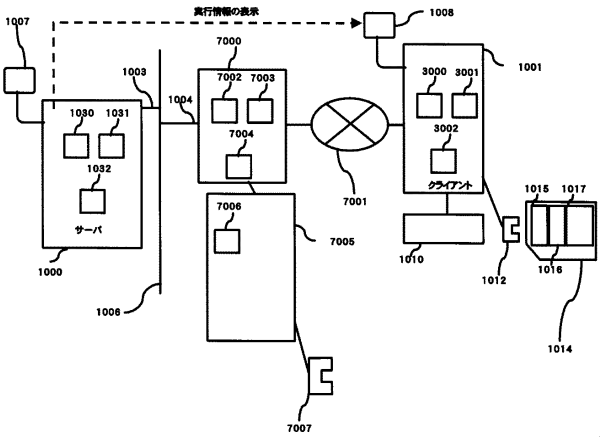
【図６】

【図６】

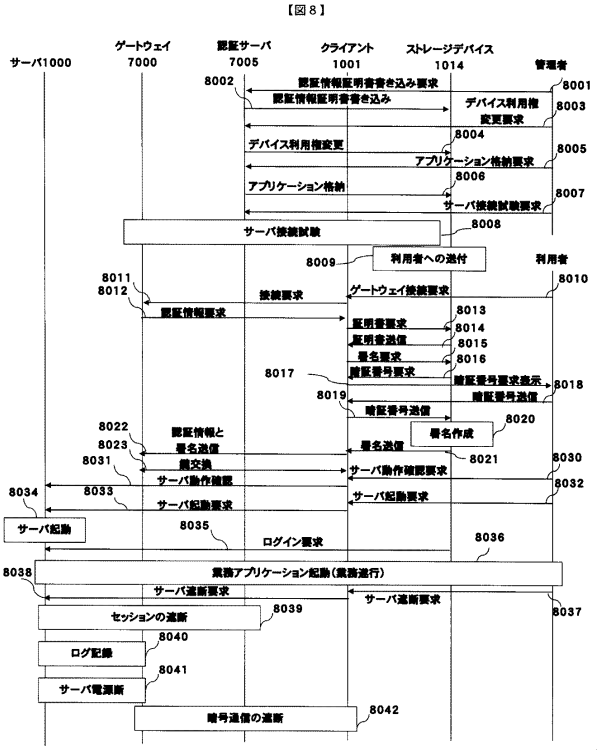


【図７】

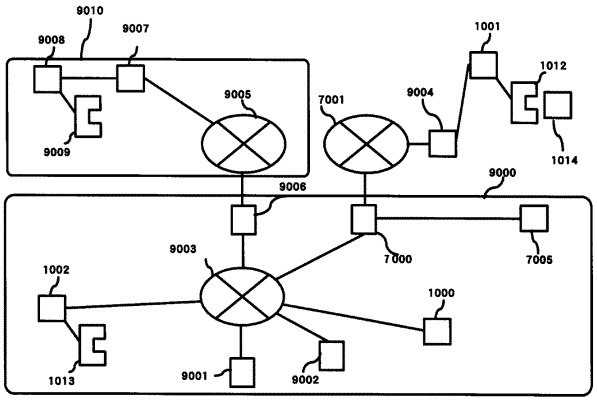
【図７】



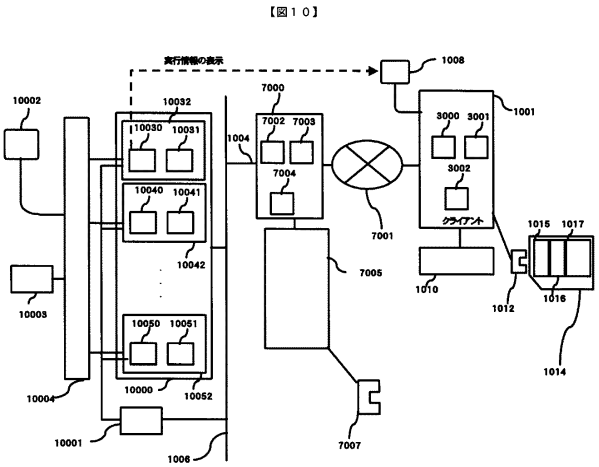
【図８】



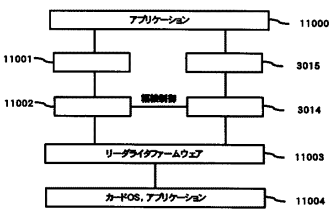
【図９】



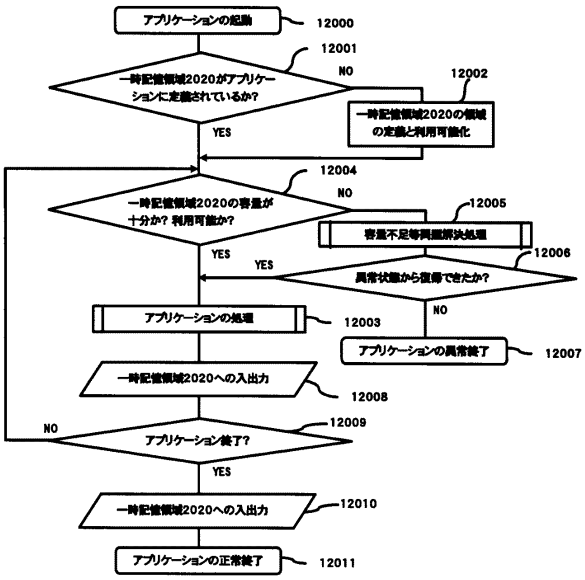
【図１０】



【図１１】

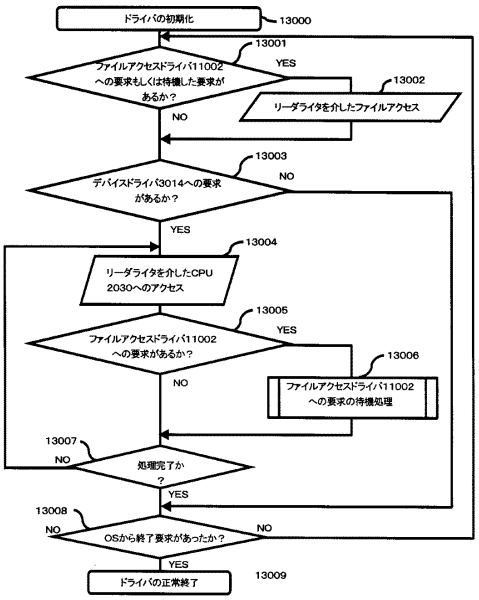


【図１２】



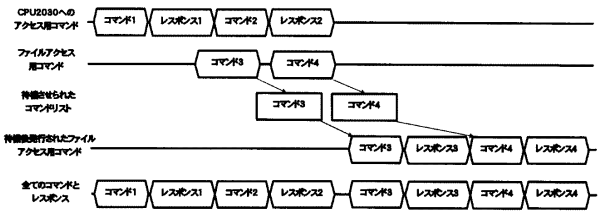
【図１３】

【図１３】



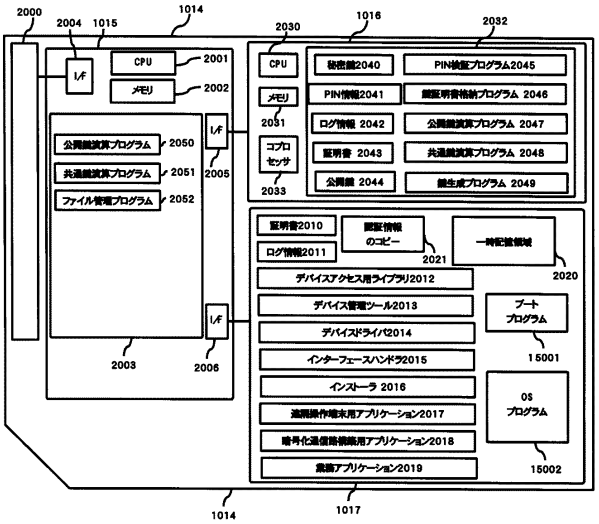
【図１４】

【図１４】



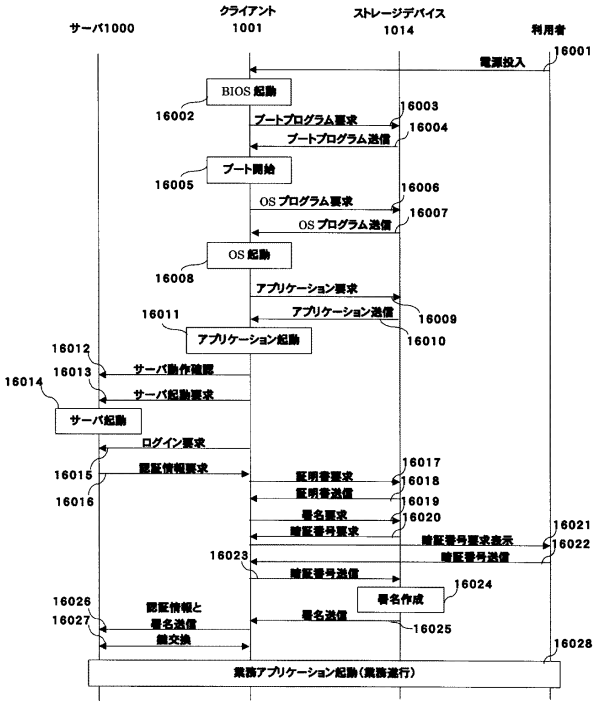
【図１５】

【図１５】



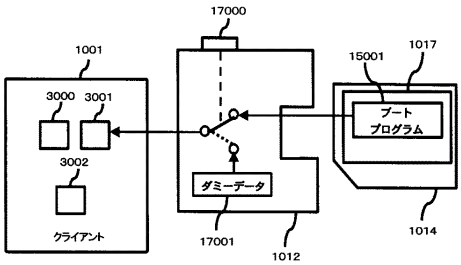
【図１６】

【図１６】

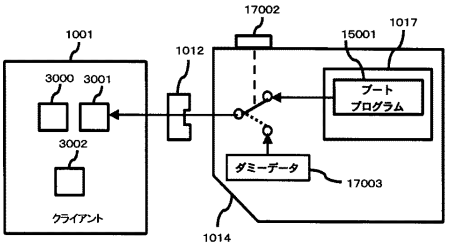


【図１７】

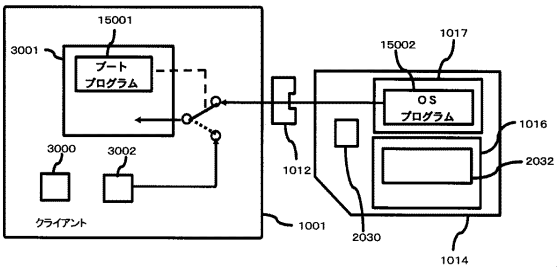
【図１７】（ａ）



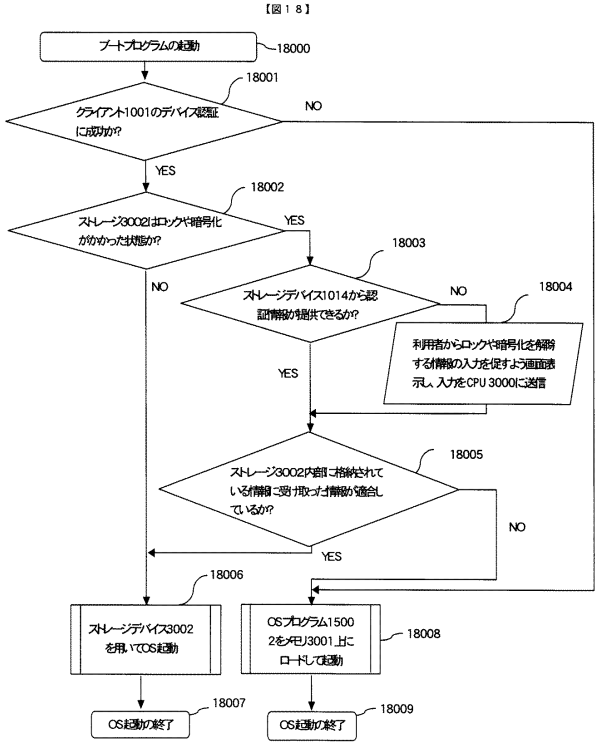
【図１７】（ｂ）



【図１７】（ｃ）



【図１８】


【図１８】
ブートプログラムの起動
18000
18001
クライアント1001のデバイス認証に成功か?
NO
YES
18002
ストレージ3002はロックや暗号化がかかった状態か?
YES
NO
18003
ストレージデバイス1014から認証情報が提供できるか?
NO
18004
利用者からロックや暗号化を解除する情報の入力を促すよう画面表示し、入力をCPU 3000に送信
YES
18005
ストレージ3002内部に格納されている情報に受け取った情報が適合しているか?
NO
YES
18006
ストレージデバイス3002を用いてOS起動
OSプログラム1500 2をメモリ3001上にロードして起動
18008
OS起動が終了
18007
OS起動が終了
18009

フロントページの続き

早期審査対象出願

(72)発明者　常広　隆司
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　萱島　信
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　仲川　和志
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

審査官　石川　正二

(56)参考文献　三宅順、常広隆司、石原晴次，コンテンツ配信・モバイルコマース用のセキュアマルチメディアカード，日立評論　２００１年１０月　増刊号，日本，日立評論社，２００１年１０月　１日，Ｐ９－１４

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｇ０６Ｆ　　１／００
Ｇ０６Ｆ　２１／２４
Ｈ０４Ｌ　　９／３２