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

特許第5531485号
(P5531485)

(45)発行日　平成26年6月25日(2014.6.25)　(24)登録日　平成26年5月9日(2014.5.9)

(51)Int.Cl.		F I		
G06F 21/31	(2013.01)	G06F	21/20	131A
G06F 21/35	(2013.01)	G06F	21/20	135
H04L 9/32	(2006.01)	H04L	9/00	673A

請求項の数 22　(全 28 頁)

(21)出願番号　特願2009-176573(P2009-176573)
(22)出願日　平成21年7月29日(2009.7.29)
(65)公開番号　特開2011-28687(P2011-28687A)
(43)公開日　平成23年2月10日(2011.2.10)
審査請求日　平成24年7月26日(2012.7.26)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100095957
弁理士　亀谷　美明
(74)代理人　100096389
弁理士　金本　哲男
(74)代理人　100101557
弁理士　萩原　康司
(74)代理人　100128587
弁理士　松本　一騎
(72)発明者　宮林　直樹
東京都港区港南１丁目７番１号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】情報処理装置、情報提供サーバ、プログラム、通信システム及びログイン情報提供サーバ

(57)【特許請求の範囲】
【請求項１】
処理部と、通信部と、記憶部とを備え、
前記処理部は、非接触通信に応じて、前記通信部及び前記記憶部と連携して、
(a)アドレス情報を保持するフリー領域とアカウント情報を保持するセキュア領域とを有する記憶装置から前記アドレス情報を取得し、
(b)前記アドレス情報を用いサーバに接続し、
(c)セキュリティサーバに、(i)セキュアな通信路を確立させ、(ii)前記記憶装置から前記アカウント情報を取得させ、(iii)取得した前記アカウント情報を、ユーザの前記アカウント情報を用いた前記サーバへのアクセスを可能とするため、前記サーバに送信させるヽ
処理を行う、
情報処理装置。
【請求項２】
前記非接触通信は、通信カードがカードリーダライターに接触または近接したことに応じて行われる、請求項１に記載の情報処理装置。
【請求項３】
前記処理部は、前記サーバへのアクセスを確認するためのセッション番号を前記サーバに要求する、請求項１に記載の情報処理装置。
【請求項４】

前記記憶装置は、前記情報処理装置とは異なる非接触通信カードに含まれる、請求項１に記載の情報処理装置。
【請求項５】
前記アドレス情報はＵＲＬを含む、請求項１に記載の情報処理装置。
【請求項６】
前記アカウント情報はログイン情報を含む、請求項１に記載の情報処理装置。
【請求項７】
表示装置をさらに備え、
前記処理部は、前記表示装置にログイン画面を表示する、
請求項１に記載の情報処理装置。
【請求項８】
処理部と、通信部と、記憶部とを備える情報処理装置における情報処理方法であって、
前記処理部は、非接触通信に応じて、前記通信部及び前記記憶部と連携して、
(a)アドレス情報を保持するフリー領域とアカウント情報を保持するセキュア領域とを有する第２の記憶部から前記アドレス情報を取得し、
(b)前記アドレス情報を用いサーバに接続し、
(c)セキュリティサーバに、(i)セキュアな通信路を確立させ、(ii)前記第２の記憶部から前記アカウント情報を取得させ、(iii)取得した前記アカウント情報を、ユーザの前記アカウント情報を用いた前記サーバへのアクセスを可能とするため、前記サーバに送信させる、
処理を行う、情報処理方法。
【請求項９】
処理部と、通信部と、記憶部とを備え、
前記処理部は、前記通信部及び前記記憶部と連携し、
(a)アドレス情報を保持するフリー領域とアカウント情報を保持するセキュア領域とを有する記憶装置から前記アドレス情報を取得し当該アドレス情報を用い接続を行う情報処理装置と接続し、
(b)前記記憶装置の前記セキュア領域から前記アカウント情報を取得するセキュリティサーバから前記アカウント情報を取得し、
(c)前記セキュリティサーバから取得した前記アカウント情報を用い、ユーザのアクセスを可能とする、
処理を行う、サーバ。
【請求項１０】
前記記憶部は、前記処理部に、通信カードがカードリーダライターに接触または近接した非接触通信に応じて、前記通信部及び前記記憶部と連携して、前記(a)、(b)、(c)を行う、請求項９に記載のサーバ。
【請求項１１】
前記処理部は、前記サーバへのアクセスを確認するためのセッション番号を前記情報処理装置に送信する、請求項９に記載のサーバ。
【請求項１２】
前記アドレス情報はＵＲＬを含む、請求項９に記載のサーバ。
【請求項１３】
前記アカウント情報はログイン情報を含む、請求項９に記載のサーバ。
【請求項１４】
処理部と、通信部と、記憶部とを備えるサーバにおける情報処理方法であって、
前記処理部は、前記通信部及び前記記憶部と連携し、
(a)アドレス情報を保持するフリー領域とアカウント情報を保持するセキュア領域とを有する記憶装置から前記アドレス情報を取得し当該アドレス情報を用い接続を行う情報処理装置と接続し、
(b)前記記憶装置の前記セキュア領域から前記アカウント情報を取得するセキュリティ

サーバから前記アカウント情報を取得し、
(c)前記セキュリティサーバから取得した前記アカウント情報を用い、ユーザのアクセスを可能とする、
処理を行う、情報処理方法。
【請求項１５】
処理部と、通信部と、第１の記憶装置を備え、
前記処理部は、非接触通信に応じて、前記通信部及び前記第１の記憶装置と連携し、
(a)セキュリティサーバのブラウザを起動させ、
(b)アドレス情報を保持するフリー領域とアカウント情報を保持するセキュア領域とを有する第2の記憶装置から前記アドレス情報を取得し、
(c)前記セキュリティサーバのブラウザを介し、前記取得したアドレス情報を用いてサーバにアクセスし、
(d)前記セキュリティサーバに、(i)セキュアな通信路を確立させ、(ii)ユーザに第１のアクセス先もしくは第２のアクセス先を選択可能とし、(iii)前記第１のアクセス先が選択されたことに応じて、情報処理装置にアクセスさせ、(iv)前記第２のアクセス先が選択されたことに応じて、前記第２の記憶装置の前記セキュア領域にアクセスさせる、
処理を行う、情報処理装置。
【請求項１６】
前記非接触通信は、通信カードがカードリーダライターに接触または近接したことに応じて行われる、請求項１５に記載の情報処理装置。
【請求項１７】
リーダライタを更に備える、請求項１５に記載の情報処理装置。
【請求項１８】
前記処理部は、前記リーダライタに前記アドレス情報を取得する、請求項１７に記載の情報処理装置。
【請求項１９】
前記第2の記憶装置は、前記情報処理装置とは異なる非接触通信カードに含まれる、請求項１８に記載の情報処理装置。
【請求項２０】
前記アドレス情報はＵＲＬを含む、請求項１５に記載の情報処理装置。
【請求項２１】
前記アカウント情報はログイン情報を含む、請求項１５に記載の情報処理装置。
【請求項２２】
処理部と、通信部と、第１の記憶装置とを備える情報処理装置における情報処理方法であって、
前記処理部は、非接触通信に応じて、前記通信部及び前記第１の記憶装置と連携し、
(a)セキュリティサーバのブラウザを起動させ、
(b)アドレス情報を保持するフリー領域とアカウント情報を保持するセキュア領域とを有する第２の記憶装置から前記アドレス情報を取得し、
(c)前記セキュリティサーバのブラウザを介し、前記取得したアドレス情報を用いてサーバにアクセスし、
(d)前記セキュリティサーバに、(i)セキュアな通信路を確立させ、(ii)ユーザに第１のアクセス先もしくは第2のアクセス先を選択可能とし、(iii)前記第１のアクセス先が選択されたことに応じて、情報処理装置にアクセスさせ、(iv)前記第２のアクセス先が選択されたことに応じて、前記第２の記憶装置の前記セキュア領域にアクセスさせる、
処理を行う、情報処理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、情報提供サーバ、プログラム、通信システム及びログイン情

報提供サーバ。
【背景技術】
【０００２】
従来、例えば下記の特許文献１には、通信ネットワーク上の仮想店舗の電子商取引サーバに接続して商品を購入するシステムが記載されている。特許文献１には、クレジットカード機能を有するＩＣカード内の独自番号データを要求して、受信した独自番号を変換して作成した与信可否データを電子商取引サーバへ送信する電子商取引支援サーバを備えたシステムが記載されている。
【０００３】
また、特許文献２には、クレジットカード番号などの情報を加盟店端末からカード発行会社へ転送し、与信依頼をかける仲介システムが記載されている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００２－３６６８６８号公報
【特許文献２】特開２００２－３６６８５９号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、上記従来の技術においては、与信または本人認証はいずれも代行サーバで実施し、その結果を本来の取引先である電子商取引サーバ、加盟店端末へ戻す処理を行っている。この方法では、代行サーバの構成が複雑になり、システムが大規模になるため、システムの構築に多大なコストが必要になるという問題がある。
【０００６】
そこで、本発明は、上記問題に鑑みてなされたものであり、本発明の目的とするところは、　簡素かつセキュアな構成で本人認証を行うことが可能な、新規かつ改良された情報処理装置、情報提供サーバ、プログラム、通信システム及びログイン情報提供サーバを提供することにある。
【課題を解決するための手段】
【０００７】
上記課題を解決するために、本発明のある観点によれば、ネットワークを介して情報提供サーバにアクセスする際に、アクセス先のＵＲＬを前記情報提供サーバへ送信するアクセス先情報送信部と、前記アクセス先のＵＲＬへログインする際に必要なログイン情報を前記情報提供サーバへ提供するログイン情報提供サーバに対して、暗号化された通信路を介して前記ログイン情報を送信するログイン情報送信部と、前記ログイン情報提供サーバによって提供された前記ログイン情報を用いて前記情報提供サーバでログインが実行された前記アクセス先の情報を前記情報提供サーバから受信する受信処理部と、を備える情報処理装置が提供される。
【０００８】
また、前記アクセス先情報送信部は、前記アクセス先のＵＲＬとともに前記ログイン情報提供サーバのＵＲＬを前記情報提供サーバへ送信するものであってもよい。
【０００９】
また、上記課題を解決するために、本発明の別の観点によれば、ネットワークを介して接続された情報処理装置から、前記情報処理装置がアクセスを要求するアクセス先のＵＲＬを取得するアクセス先情報取得部と、前記アクセス先のＵＲＬへログインする際に必要となるログイン情報を、暗号化された通信路を介して前記情報処理装置と通信するログイン情報提供サーバから取得するログイン情報取得部と、前記ログイン情報提供サーバから取得した前記ログイン情報を用いて前記アクセス先のＵＲＬにログインするログイン実行部と、前記アクセス先の情報を前記情報処理装置に送信する情報送信部と、を備える情報提供サーバが提供される。

【００１０】
また、上記課題を解決するために、本発明の別の観点によれば、ネットワークを介して接続された情報処理装置から、前記情報処理装置がアクセスを要求するアクセス先のＵＲＬを取得する手段、前記アクセス先のＵＲＬへログインする際に必要となるログイン情報を、暗号化された通信路を介して前記情報処理装置と通信するログイン情報提供サーバから取得する手段、前記ログイン情報提供サーバから取得した前記ログイン情報を用いて前記アクセス先のＵＲＬにログインする手段、前記アクセス先の情報を前記情報処理装置に送信する手段、としてコンピュータを機能させるためのプログラムが提供される。
【００１１】
また、上記課題を解決するために、本発明の別の観点によれば、ネットワークを介して情報提供サーバにアクセスする際のアクセス先のＵＲＬと、ログイン情報を前記情報提供サーバに提供するログイン情報提供サーバのＵＲＬとを格納したメモリを有する非接触情報通信カードと、前記非接触通信カードと通信を行うことで前記アクセス先のＵＲＬ及び前記ログイン情報提供サーバのＵＲＬを取得するカードリーダライタと、ネットワークを介して情報提供サーバにアクセスする際に、前記カードリーダライタから取得した前記アクセス先のＵＲＬを前記情報提供サーバへ送信するアクセス先情報送信部と、前記アクセス先のＵＲＬへログインする際に必要な前記ログイン情報を、暗号化された通信路を介して前記ログイン情報提供サーバへ送信するログイン情報送信部と、前記ログイン情報提供サーバによって提供された前記ログイン情報を用いて前記情報提供サーバでログインが実行された前記アクセス先の情報を前記情報提供サーバから受信する受信部と、を備える情報処理装置と、ネットワークを介して接続された前記情報処理装置から、前記アクセス先のＵＲＬを取得するアクセス先情報取得部と、前記アクセス先のＵＲＬへログインする際に必要となるログイン情報を、前記ログイン情報提供サーバから取得するログイン情報取得部と、前記ログイン情報提供サーバから取得した前記ログイン情報を用いて前記アクセス先のＵＲＬにログインするログイン実行部と、前記アクセス先の情報を前記情報処理装置に送信する情報送信部と、を備える前記情報提供サーバと、前記情報処理装置から前記ログイン情報を取得し、取得した前記ログイン情報を前記情報提供サーバへ送信する前記ログイン情報提供サーバと、を備える、通信システムが提供される。
【００１２】
また、上記課題を解決するために、本発明の別の観点によれば、ネットワークを介して情報提供サーバにアクセスする際に、アクセス先のＵＲＬを前記情報提供サーバへ送信するアクセス先情報送信部と、前記アクセスを識別するための識別情報を前記情報提供サーバから取得する識別情報取得部と、前記アクセス先のＵＲＬへログインする際に必要なログイン情報を前記情報提供サーバへ提供するログイン情報提供サーバに対して、暗号化された通信路を介して前記ログイン情報とともに前記識別情報を送信するログイン情報送信部と、前記ログイン情報提供サーバによって提供された前記ログイン情報及び前記識別情報を用いて前記情報提供サーバでログインが実行された前記アクセス先の情報を前記情報提供サーバから受信する受信部と、を備える情報処理装置が提供される。
【００１３】
また、上記課題を解決するために、本発明の別の観点によれば、ネットワークを介して情報提供サーバにアクセスする際に、アクセス先のＵＲＬを前記情報提供サーバへ送信する手段、前記アクセスを識別するための識別情報を前記情報提供サーバから取得する手段、前記アクセス先のＵＲＬへログインする際に必要なログイン情報を前記情報提供サーバへ提供するログイン情報提供サーバに対して、暗号化された通信路を介して前記識別情報を含む前記ログイン情報を送信する手段、前記ログイン情報提供サーバによって提供された前記ログイン情報及び前記識別情報を用いて前記情報提供サーバでログインが実行された前記アクセス先の情報を前記情報提供サーバから受信する手段、としてコンピュータを機能させるためのプログラムが提供される。
【００１４】
また、上記課題を解決するために、本発明の別の観点によれば、ネットワークを介して

情報提供サーバにアクセスする際のアクセス先のＵＲＬと、ログイン情報を前記情報提供サーバに提供するログイン情報提供サーバのＵＲＬとを格納したメモリを有する非接触情報通信カードと、前記非接触通信カードと通信を行うことで前記アクセス先のＵＲＬ及び前記ログイン情報提供サーバのＵＲＬを取得するカードリーダライタと、ネットワークを介して情報提供サーバにアクセスする際に、前記カードリーダライタから取得した前記アクセス先のＵＲＬを前記情報提供サーバへ送信するアクセス先情報送信部と、前記アクセスを識別するための識別情報を前記情報提供サーバから取得する識別情報取得部と、前記アクセス先のＵＲＬへログインする際に必要な前記ログイン情報を、前記識別情報とともに、暗号化された通信路を介して前記ログイン情報提供サーバへ送信するログイン情報送信部と、前記ログイン情報提供サーバによって提供された前記ログイン情報及び前記識別情報を用いて前記情報提供サーバでログインが実行された前記アクセス先の情報を前記情報提供サーバから受信する受信部と、を備える情報処理装置と、ネットワークを介して接続された前記情報処理装置から、前記アクセス先のＵＲＬを取得するアクセス先情報取得部と、前記アクセス先のＵＲＬへログインする際に必要となるログイン情報及び前記識別情報を、前記ログイン情報提供サーバから取得するログイン情報取得部と、前記ログイン情報提供サーバから取得した前記ログイン情報及び前記識別情報を用いて前記アクセス先のＵＲＬにログインするログイン実行部と、前記アクセス先の情報を前記情報処理装置に送信する情報送信部と、を備える前記情報提供サーバと、前記情報処理装置から前記ログイン情報及び前記識別情報を取得し、取得した前記ログイン情報及び前記識別情報を前記情報提供サーバへ送信する前記ログイン情報提供サーバと、を備える、通信システムが提供される。

【００１５】

また、上記課題を解決するために、本発明の別の観点によれば、ネットワークを介して情報提供サーバにアクセスする際に、アクセス先のＵＲＬをログイン情報提供サーバへ送信するアクセス先情報送信部と、暗号化された通信路を介して、前記アクセス先のＵＲＬへログインする際に必要なログイン情報を前記ログイン情報提供サーバに送信するログイン情報送信部と、前記ログイン情報提供サーバが前記ログイン情報を用いて情報提供サーバにログインを実行することにより取得した前記アクセス先の情報を前記ログイン情報提供サーバから取得する情報取得部と、を備える情報処理装置が提供される。

【００１６】

また、上記課題を解決するために、本発明の別の観点によれば、ネットワークを介して接続された情報処理装置から、前記情報処理装置がアクセスを要求するアクセス先のＵＲＬを取得するアクセス先情報取得部と、暗号化された通信路を介して、前記アクセス先のＵＲＬにログインする際に必要なログイン情報を前記情報処理装置から受信するログイン情報受信部と、前記ログイン情報を用いて前記アクセス先のＵＲＬにログインするログイン実行部と、ログインした前記アクセス先の情報を前記情報処理装置へ送信するアクセス先情報送信部と、前記情報処理装置との情報の送受信に応じて、前記情報処理装置の記憶媒体に対して情報の書き込みまたは読み出しを実行するローカルアクセス部と、を備えるログイン情報提供サーバが提供される。

【００１７】

また、上記課題を解決するために、本発明の別の観点によれば、ネットワークを介して接続された情報処理装置から、前記情報処理装置がアクセスを要求するアクセス先のＵＲＬを取得する手段、暗号化された通信路を介して、前記アクセス先のＵＲＬにログインする際に必要なログイン情報を前記情報処理装置から受信する手段、前記ログイン情報を用いて前記アクセス先のＵＲＬにログインする手段、ログインした前記アクセス先の情報を前記情報処理装置へ送信する手段、前記情報処理装置との情報の送受信に応じて、前記情報処理装置の記憶媒体に対して情報の書き込みまたは読み出しを実行する手段、としてコンピュータを機能させるためのプログラムが提供される。

【００１８】

また、上記課題を解決するために、本発明の別の観点によれば、ネットワークを介して

情報提供サーバにアクセスする際のアクセス先のＵＲＬと、ログイン情報を前記情報提供サーバに提供するログイン情報提供サーバのＵＲＬとを格納したメモリを有する非接触情報通信カードと、前記非接触通信カードと通信を行うことで前記アクセス先のＵＲＬ及び前記ログイン情報提供サーバのＵＲＬを取得するカードリーダライタと、ネットワークを介して前記情報提供サーバにアクセスする際に、アクセス先のＵＲＬを前記ログイン情報提供サーバへ送信するアクセス先情報送信部と、暗号化された通信路を介して、前記アクセス先のＵＲＬへログインする際に必要なログイン情報を前記ログイン情報提供サーバに送信するログイン情報送信部と、前記ログイン情報提供サーバが前記ログイン情報を用いて情報提供サーバにログインを実行することにより取得した前記アクセス先の情報を前記ログイン情報提供サーバから取得する情報取得部と、を備える情報処理装置と、ネットワークを介して接続された前記情報処理装置から、前記情報処理装置がアクセスを要求するアクセス先のＵＲＬを取得するアクセス先情報取得部と、前記ログイン情報を前記情報処理装置から受信するログイン情報受信部と、前記ログイン情報を用いて前記アクセス先のＵＲＬにログインするログイン実行部と、ログインした前記アクセス先の情報を前記情報処理装置へ送信するアクセス先情報送信部と、前記情報処理装置との情報の送受信に応じて、前記情報処理装置の記憶媒体に対して情報の書き込みまたは読み出しを実行するローカルアクセス部と、を備えるログイン情報提供サーバと、前記ログイン情報提供サーバによるログインを受けて、前記アクセス先の情報を前記ログイン情報提供サーバへ送信する情報提供サーバと、を備える通信システムが提供される。

【発明の効果】

【００１９】

本発明によれば、簡素かつセキュアな構成で本人認証を行うことが可能な情報処理装置、情報提供サーバ、プログラム、通信システム及びログイン情報提供サーバを提供することが可能となる。

【図面の簡単な説明】

【００２０】

【図１】第１の実施形態に係るシステム構成と、情報のやり取りを模式的に示した概念図である。

【図２】本発明の第１の実施形態に係るシステムの構成を示す模式図である。

【図３】第１の実施形態のシステムで行われる処理について説明するためのシーケンス図である。

【図４】図３のステップＳ２８における、ＳＡＭサーバと非接触通信カードとの間のログイン情報取得手順の詳細を示すシーケンス図である。

【図５】第１の実施形態に係るパーソナルコンピュータの構成を示す機能ブロック図である。

【図６】第１の実施形態に係るＷｅｂサーバの構成を示す機能ブロック図である。

【図７】第２の実施形態に係るシステム構成と、情報のやり取りを模式的に示した概念図である。

【図８】第２の実施形態のシステムで行われる処理を示すシーケンス図である。

【図９】ステップＳ８８の処理を示すシーケンス図である。

【図１０】第２の実施形態に係るパーソナルコンピュータの構成を示す機能ブロック図である。

【図１１】第３の実施形態に係るシステム構成と、情報のやり取りを模式的に示した概念図である。

【図１２】第３の実施形態に係るシステム構成と、情報のやり取りを模式的に示した概念図である。

【図１３】第３の実施形態の処理を示すシーケンス図である。

【図１４】図１３のステップＳ１５８のローカルアクセス処理の詳細を示すシーケンス図である。

【図１５】ＳＡＭサーバによるローカルへのアクセス処理（ステップＳ２２８以降）を説

明するためのフローチャートである。
【図１６】第３の実施形態に係るパーソナルコンピュータの構成を示す機能ブロック図である。
【図１７】第３の実施形態に係るＳＡＭサーバの構成を示す機能ブロック図である。
【発明を実施するための形態】
【００２１】
以下に添付図面を参照しながら、本発明の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。
【００２２】
なお、説明は以下の順序で行うものとする。
１．第１の実施の形態（ＳＡＭサーバからログイン情報を取得する構成例）
２．第２の実施の形態（ログインを識別するためのセッション番号を付与する例）
３．第３の実施の形態（ＳＡＭサーバの仮想ウェブ上でアクセス先ＵＲＬに接続する例）
【００２３】
＜１．第１の実施形態＞
図１は、第１の実施形態に係るシステム構成と、情報のやり取りを模式的に示した概念図である。図１の概念図に示すように、本実施形態のシステムは、非接触通信カード１００、カードリーダライタ２００、パーソナルコンピュータ３００、Ｗｅｂサーバ４００、ＳＡＭ（Ｓｅｃｕｒｅ　Ａｐｐｌｉｃａｔｉｏｎ　Ｍｏｄｕｌｅ）サーバ５００を備える。
【００２４】
図１に基づいて、本実施形態の情報のやり取りの概念を説明すると、非接触通信カード１００は、そのメモリ内にフリー領域とセキュア領域を備えている。フリー領域には、ＵＲＬなどの情報が格納され、セキュア領域にはユーザ名、パスワードなどのログイン情報が格納されている。非接触通信カード１００をカードリーダライタ２００に接触または接近させると、パーソナルコンピュータ３００のブラウザが起動し、Ｗｅｂサーバ４００と通信を行うことにより、非接触通信カード１００のフリー領域に格納されていたＵＲＬが開かれる。
【００２５】
Ｗｅｂサーバ４００のＵＲＬが開かれると、ユーザ名、パスワードなどのログイン情報が要求される。Ｗｅｂサーバ４００は、これらのログイン情報をＳＡＭサーバ５００に対して要求する。ＳＡＭサーバ５００は、非接触通信カード１００のセキュア領域の読取り要求を、Ｗｅｂサーバ４００、パーソナルコンピュータ（ＰＣ）３００、カードリーダライタ２００を経由して非接触通信カード１００に要求し、ログイン情報を取得する。そして、ＳＡＭサーバ５００は、取得したログイン情報をＷｅｂサーバ４００に送信する。Ｗｅｂサーバ４００は、受信したログイン情報によりＵＲＬへログインする。これにより、ユーザは、非接触通信カード１００をカードリーダライタ２００と接触または接近させるのみで、Ｗｅｂサーバ４００のＵＲＬにアクセスすることが可能となる。
【００２６】
次に、本実施形態のシステムについて、図２～図４に基づいて詳細に説明する。図２は、本発明の第１の実施形態に係るシステムの構成を示す模式図である。図２に示すように、本実施形態のシステムは、非接触通信カード１００、カードリーダライタ（Ｒ／Ｗ）２００、パーソナルコンピュータ（ＰＣ）３００、ＷＥＢサーバ４００、ＳＡＭ（Ｓｅｃｕｒｅ　Ａｐｐｌｉｃａｔｉｏｎ　Ｍｏｄｕｌｅ）サーバ５００を備える。パーソナルコンピュータ３００、ＷＥＢサーバ４００及びＳＡＭサーバ５００は、インターネット８００を介して相互に通信可能に接続されている。
【００２７】
非接触通信カード１００は、ＲＦ部１０２、ＣＰＵ１０４、メモリ１０６を備える。Ｒ

Ｆ部１０２は、カードリーダライタ２００が発生する１３．５６ＭＨｚ帯の搬送波（ＲＦ信号）から、マンチェスター方式にて重畳されたベースバンド信号を抽出しデータを受信する。また、ＲＦ部１０２は、またこの搬送波に対して自機器のベースバンド信号を重畳させることによってカードリーダライタ２００にデータを送信する。ＣＰＵ１０４は、これら通信制御とカード内のメモリ１０６へのアクセス制御、およびデータの暗号化、復号化処理を行う。メモリ１０６は、サービス毎に領域が分割され、それぞれ書き込み/読み込み可能の属性が設定されている。具体的には、メモリ１０６の領域は、主に、認証および暗号化によるアクセスが必要である領域（以下、セキュア領域という）と、アクセスを制限しない領域（以下、フリー領域という）との２つに属性が決められている。

【００２８】

カードリーダライタ２００は、ＲＦ部２０２、ＣＰＵ２０４を備える。ＲＦ部２０２は、１３．５６ＭＨｚ帯の搬送波を発生させ、送信波へのベースバンド信号の重畳及び受信波からのベースバンド信号の抽出によって、非接触通信カード１００と通信を行う。ＣＰＵ２０４は、パーソナルコンピュータ３００から受信した通信制御コマンドをベースバンド信号化してＲＦ部２０２に送信する。また、ＣＰＵ２０４は、ＲＦ部２０２から受信したベースバンド信号をＰＣ用の通信制御コマンドフォーマットに成形してパーソナルコンピュータ３００へ送信する。

【００２９】

パーソナルコンピュータ３００は、カード制御部３０２、通信部３０４、ユーザインタフェース（ＵＩ）部３０６、ＣＰＵ３０８を備える。カード制御部３０２は、カード制御コマンドを発行し、カードカードリーダライタ２００と送受信を行う。通信部３０４は、ＳＡＭサーバ５００、ＷＥＢサーバ４００等のインターネット８００上のサーバとの通信を行う。ユーザインタフェース部３０６は、キーボード、マウス等によるユーザからの指示入力手段、また、ディスプレイ、音出力などのユーザへの出力手段としての機能を備える。ＣＰＵ３０８は、サーバより得られたｈｔｍｌ情報からＷｅｂブラウザの表示および制御を行う。また、ＣＰＵ３０８は、サーバとの暗号化設定情報から、インターネット通信路の暗号化を行い、ＳＡＭサーバ５００からカードリーダライタ２００への制御信号を変換する。

【００３０】

次に、図３のシーケンス図に基づいて、第１の実施形態のシステムで行われる処理について説明する。先ず、カードの読み込みについて説明する。パーソナルコンピュータ３００は、非接触通信カード１００のフリー領域の情報を読み込むため、読み込み制御信号をカードリーダライタ２００に送信する（ステップＳ１０）。

【００３１】

次に、カードリーダライタ２００は、ポーリングを行う（ステップＳ１２）。ここでは、カードリーダライタ２００は、搬送波を発信してカードの捕捉を行う。非接触通信カード１００のアンテナが搬送波を受信し、その電力によってＣＰＵ１０４が活性化されると、非接触通信カード１００は、固有識別子（ＩＤｍ）、カードの種別（システムコード）を返信する。

【００３２】

（１．２）フリー領域読み込み）

カードの捕捉に成功したカードリーダライタ２００は、非接触通信カード１００のアクセスフリー領域にアクセスする。カードリーダライタ２００は、パーソナルコンピュータ３００のＷＥＢブラウザがインターネットに接続する際の接続先ＵＲＬ（起動ＵＲＬ）と、ＳＡＭ(Ｓｅｃｕｒｅ　Ａｐｐｌｉｃａｔｉｏｎ　Ｍｏｄｕｌｅ)を搭載したＳＡＭサーバ５００のＵＲＬを読み込む（ステップＳ１４）。これにより、ＷＥＢブラウザの接続先ＵＲＬと、ＳＡＭサーバ５００のＵＲＬは、カードリーダライタ２００へ送られ、（ステップＳ１６）、更にパーソナルコンピュータ３００へ送られる（ステップＳ１８）。

【００３３】

２）Ｗｅｂブラウザ起動

パーソナルコンピュータ３００は、Ｗｅｂサーバ４００から受信したｈｔｍｌファイルを表示するＷｅｂブラウザを起動する（ステップＳ２０）。なお、Ｗｅｂブラウザとしては、例えばＩｎｔｅｒｎｅｔ　Ｅｘｐｌｏｒｅｒ、Ｆｉｒｅｆｏｘなどを用いることができる。

【００３４】

３）ｈｔｔｐ＿ｇｅｔ(起動ＵＲＬ、ＳＡＭ＿ＵＲＬ)コマンドの送信

パーソナルコンピュータ３００のＷｅｂブラウザは、ｈｔｔｐ＿ｇｅｔコマンド(起動ＵＲＬ、ＳＡＭサーバ５００のＵＲＬを含む)を送信し（ステップＳ２２）、ｈｔｔｐ＿ｇｅｔコマンドによりＷｅｂサーバ４００のＵＲＬにインターネット８００経由で接続する。パーソナルコンピュータ３００のＷｅｂブラウザは、ＳＡＭサーバ５００のＵＲＬをＷｅｂサーバ４００に渡す。そして、パーソナルコンピュータ３００のＷｅｂブラウザは、ｈｔｔｐ＿ｇｅｔコマンドにより取得したｈｔｔｐフォーマットの受信データを解析し、ログイン画面を表示する。ここで、ｈｔｔｐ＿ｇｅｔコマンドには引数としてＳＡＭサーバ５００のアドレス（ＵＲＬ）を付加する。ｈｔｔｐ＿ｇｅｔコマンドにおける、ＳＡＭサーバのアドレス（ＵＲＬ）の付加は、例えばｈｔｔｐｓ：／／ｗｗｗ．ｓａｍｐｌｅ＿ｗｅｂ＿ｓｅｒｖｅｒ．ｃｏ．ｊｐ／ｓａｍ＿ｌｏｇｉｎ．ｃｇｉ？ＵＲＬ＝ｈｔｔｐｓ：／／ｗｗｗ．ｓａｍ＿ｓｅｒｖｅｒ．ｃｏ．ｊｐなどのようにして行うことができる。

【００３５】

３．１）通信路の暗号化

Ｗｅｂサーバ４００は、パーソナルコンピュータ３００からｈｔｔｐ＿ｇｅｔコマンドを受けると、ＣＧＩを動作させ、ＳＡＭサーバ５００との通信路をＳＳＬ等によって暗号化する（ステップＳ２４）。その後、Ｗｅｂサーバ４００は、パーソナルコンピュータ３００から取得したＳＡＭサーバ５００のＵＲＬを用いてＳＡＭサーバ５００へのアクセスを行う。

【００３６】

３．２）ログイン情報要求

Ｗｅｂサーバ４００は、ＳＡＭサーバ５００へログイン情報要求を行う（ステップＳ２６）。ＳＡＭサーバ５００は、非接触通信カード１００のセキュア領域よりログイン情報（ユーザ名およびパスワード）を取得し（ステップＳ２８）Ｗｅｂサーバ５００にログインを行う。ステップＳ２８の処理は、以下に詳細に説明する。

【００３７】

３．２．１）ログイン情報取得の詳細

図４は、図３のステップＳ２８における、ＳＡＭサーバ５００と非接触通信カード１００との間のログイン情報取得手順の詳細を示すシーケンス図である。

【００３８】

１）セキュアクライアント起動要求

SAMサーバ５００は、Webサーバ４００にパーソナルコンピュータ３００へのセキュリティクライアント要求コマンドを送信する（ステップＳ４０）。

【００３９】

１．１）転送（セキュアクライアント起動要求）

先ず、ＳＡＭサーバ５００は、Ｗｅｂサーバ４００に対して、ｈｔｔｐ＿ｇｅｔコマンドなどを送信することにより、セキュアクライアントの起動要求を出す（ステップＳ４０）。セキュアクライアントは、パーソナルコンピュータ３００が有するプログラムである。Ｗｅｂサーバ４００は、ｈｔｔｐ＿ｇｅｔコマンドで接続しているパーソナルコンピュータ３００に対して、セキュアクライアントの要求コマンドを転送する（ステップＳ４２）。

【００４０】

１．１．１）セキュアクライアント起動

セキュリティクライアントの起動コマンドを取得したパーソナルコンピュータ３００内

部のＣＰＵ３０８は、セキュリティクライアントを起動する（ステップＳ４４）。このクライアントプログラムは、ＳＡＭサーバ５００とパーソナルコンピュータ３００との通信路を暗号化する。また、このクライアントプログラムは、ＳＡＭサーバ５００から受信したカード制御コマンドをカードリーダライタ２００の制御コマンドに変換して非接触通信カード１００のカード制御を行う。これにより、パーソナルコンピュータ３００からＷｅｂサーバ４００を経由してＳＡＭサーバ５００に至る経路が暗号化され、ＳＡＭサーバ５００～パーソナルコンピュータ３００間で送受信されるパケットが暗号化される。従って、非接触通信カード１００に対してどのようなコマンドを送信したのかを隠すことができる。

【００４１】

２）認証要求（公開情報１）

暗号化通信路を確立したＳＡＭサーバ５００は、非接触通信カード１００に対して暗号化の認証を要求するため、パーソナルコンピュータ３００に対して認証要求コマンドを送信する（ステップＳ４６）。このコマンドには乱数Ｎ１および秘密鍵Ａより生成された公開情報（公開鍵）１が含まれる。認証要求は、ＳＡＭサーバ５００～パーソナルコンピュータ３００間で既に暗号化されている伝送路の中で行われる。なお、この時点で非接触通信カード１００は、カードリーダライタ２００と接近または接触した状態にあり、カードリーダライタ２００と通信可能であるものとする。

【００４２】

２．１）転送（認証要求）

ＳＡＭサーバ５００から認証要求コマンドを受信したＷｅｂサーバ４００は、コマンドをそのままパーソナルコンピュータ３００に転送する（ステップＳ４８）。

【００４３】

２．１．１）認証要求（公開情報１）

パーソナルコンピュータ３００は、認証要求コマンドをカードリーダライタ２００用に変換した後、カードリーダライタ２００へ送信する（ステップＳ５０）。

【００４４】

２．１．１．１）認証要求（公開情報１）

カードリーダライタ２００は、認証要求コマンドをＲＦ信号に変換した後、非接触通信カード１００へ送信する（ステップＳ５２）。非接触通信カード１００には、秘密鍵Ａが格納されているので、非接触通信カード１００は、この鍵Ａと乱数Ｎ２より公開情報（公開鍵）２を生成する。公開情報２は、カードリーダライタ２００、パーソナルコンピュータ３００、及びＷｅｂサーバ４００を経由してＳＡＭサーバ５００に返信される。

【００４５】

３）、４）共有鍵生成

非接触通信カード１００とＳＡＭサーバ５００のそれぞれでは、公開情報１，２を送受信して交換したことにより、両者で同一の鍵である共有鍵（秘密鍵）を生成し（ステップＳ５４，Ｓ５６）、共有鍵を共有する。共有鍵を生成した後は、非接触通信カード１００のセキュア領域からの必要な領域の読み出し値は、この共通鍵で暗号化された状態で送信される。なお、ステップＳ４６からステップＳ５６に至る共有鍵の生成は、一般にディフィーヘルマン（Diffie-Hellman）鍵交換と呼ばれる手法により行うことができる。以上のようにしてＳＡＭサーバ５００から非接触通信カード１００に至る暗号化された伝送路が形成され、ＳＡＭサーバ５００と非接触通信カード１００がセキュアに通信できる状態となる。

【００４６】

５）セキュリティ領域読出し（Ｒｅａｄ）要求

ＳＡＭサーバ５００は、非接触通信カード１００のセキュア領域に書き込まれているログイン情報（ユーザ名、パスワード等）を取得するため、暗号化された通信路を用いて、Ｗｅｂサーバ４００を経由して、パーソナルコンピュータ３００へ非接触通信カード１００のセキュア領域の読出し（Ｒｅａｄ）要求を送信する（ステップＳ５８）。セキュア領

域への読出し（Ｒｅａｄ）要求には、非接触通信カード１００のメモリ１０６のアクセスする領域（サービスエリア）の情報が含まれている。

【００４７】

５．１）転送（セキュア領域Read要求）

セキュア領域の読出し（Ｒｅａｄ）要求をＳＡＭサーバ５００から受信したＷｅｂサーバ４００は、コマンドをそのままパーソナルコンピュータ３００に転送する（ステップＳ６０）。

【００４８】

５．１．１）セキュア領域Read要求

パーソナルコンピュータ３００上のセキュリティクライアントは、セキュア領域への読出し（Ｒｅａｄ）要求を受信すると、セキュア領域への読出し（Ｒｅａｄ）要求をカードリーダライタ２００用のコマンドフォーマットに変換し、カードリーダライタ２００へ送信する（ステップＳ６２）。

【００４９】

５．１．１．１）セキュア領域アクセス

セキュア領域への読出し（Ｒｅａｄ）要求を受けたカードリーダライタ２００は、非接触通信カード１００のセキュア領域にアクセスする（ステップＳ６４）。非接触通信カード１００は、セキュア領域に格納されたログイン情報（ユーザ名およびパスワード）を共有鍵で暗号化し、暗号化された伝送路を経由して、ＳＡＭサーバ５００に返信する（ステップＳ６６）。

【００５０】

６）ログイン情報の復号

ＳＡＭサーバ５００は、暗号化された伝送路から非接触通信カード１００のログイン情報を受信すると、共通鍵を用いて暗号化されているログイン情報を復号する（ステップＳ６８）。

【００５１】

以上説明した図４のシーケンスにより、ＳＡＭサーバ５００は、図３のステップＳ２８において、非接触通信カード１００からログイン情報を取得することができる。

【００５２】

ＳＡＭサーバ５００は、復号したログイン情報ををＷｅｂサーバ４００へ送る（図３のステップＳ３０）。Ｗｅｂサーバ４００は、受信した復号されたログイン情報によりログインを行う。これにより、Ｗｅｂサーバ４００へのログインが完了し（ステップＳ３０）、パーソナルコンピュータ３００の画面には、ログイン後の画面が表示される。従って、ユーザは、パーソナルコンピュータ３００のＷｅｂブラウザの画面上で、ログイン画面に入ったことを確かめることができる。

【００５３】

従って、ユーザは、ログイン画面にユーザ名、パスワード等を入力しなくても、非接触通信カード１００のセキュア領域のログイン情報がＳＡＭサーバ５００からＷｅｂサーバ４００へ送信されることから、Ｗｅｂサーバ４００に自動的にログインすることができる。

【００５４】

図５は、第１の実施形態に係るパーソナルコンピュータ３００の構成を示す機能ブロック図である。図５に示すように、パーソナルコンピュータ３００は、アクセス先情報送信部３１０、ログイン情報送信部３１２、受信処理部３１４を備える。各機能ブロックは、パーソナルコンピュータ３００が備えるハードウエア、ＣＰＵ３０８とこれを機能させるためのソフトウェア（プログラム）によって構成されることができる。そのプログラムは、パーソナルコンピュータ３００が備えるハードディスク、またはパーソナルコンピュータ３００の会部から接続されるメモリなどの記録媒体に格納されることができる。

【００５５】

また、図６は、第１の実施形態に係るＷｅｂサーバ４００の構成を示す機能ブロック図

である。図６に示すように、Ｗｅｂサーバ４００は、アクセス先情報取得部４１０、ログイン情報取得部４１２、ログイン実行部４１４、送信処理部４１６を備える。各機能ブロックは、Ｗｅｂサーバ４００が備えるハードウエア、ＣＰＵ４０２とこれを機能させるためのプログラムによって構成されることができる。そのプログラムは、パーソナルコンピュータ３００が備えるハードディスク、またはパーソナルコンピュータ３００の会部から接続されるメモリなどの記録媒体に格納されることができる。

【００５６】

以上説明したように第１の実施形態によれば、暗号化された伝送路からＳＡＭサーバ５００に送られたログイン情報をＳＡＭサーバ５００がＷｅｂサーバ５００に送ってログインする。これにより、ユーザが非接触通信カード１００をカードリーダライタ２００にかざすのみで簡単にログインすることが可能となる。

【００５７】

＜２．第２の実施形態＞

次に、本発明の第２の実施形態について説明する。第２の実施形態は、セッション番号を利用した、ＳＡＭサーバ５００経由のログインに関するものである。

【００５８】

図７は、第２の実施形態に係るシステム構成と、情報のやり取りを模式的に示した概念図である。図７の概念図に示すように、本実施形態のシステムも、非接触通信カード１００、カードリーダライタ２００、パーソナルコンピュータ３００、Ｗｅｂサーバ４００、ＳＡＭ（Ｓｅｃｕｒｅ　Ａｐｐｌｉｃａｔｉｏｎ　Ｍｏｄｕｌｅ）サーバ５００を備える。

【００５９】

図７に基づいて、本実施形態の情報のやり取りの概念を説明すると、非接触通信カード１００は、そのメモリ内にフリー領域とセキュア領域を備えている。フリー領域には、ＵＲＬなどの情報が格納され、セキュア領域にはユーザ名、パスワードなどのログイン情報が格納されている。非接触通信カード１００をカードリーダライタ２００に接触または接近させると、パーソナルコンピュータ３００のブラウザが起動し、Ｗｅｂサーバ４００と通信を行うことにより、非接触通信カード１００のフリー領域に格納されていたＵＲＬが開かれる。

【００６０】

Ｗｅｂサーバ４００のＵＲＬが開かれると、ユーザ名、パスワードなどのログイン情報が要求される。パーソナルコンピュータ３００は、これらのログイン情報をＳＡＭサーバ５００に対して要求する。ＳＡＭサーバ５００は、非接触通信カード１００のセキュア領域の読取り要求を、パーソナルコンピュータ（ＰＣ）３００、カードリーダライタ２００を経由して非接触通信カード１００に要求し、ログイン情報を取得する。そして、ＳＡＭサーバ５００は、取得したログイン情報をＷｅｂサーバ４００に送信する。Ｗｅｂサーバ４００は、受信したログイン情報によりＵＲＬへログインする。これにより、ユーザは、非接触通信カード１００をカードリーダライタ２００と接触または接近させるのみで、Ｗｅｂサーバ４００のＵＲＬにアクセスすることが可能となる。

【００６１】

次に、本実施形態のシステムについて、図８、図９に基づいて詳細に説明する。第２の実施形態に係るシステム構成、及び非接触通信カード１００、カードリーダライタ２００、パーソナルコンピュータ３００、Ｗｅｂサーバ４００、ＳＡＭサーバ５００の構成は、図２と同様である。

【００６２】

図８は、第２の実施形態のシステムで行われる処理を示すシーケンス図である。先ず、パーソナルコンピュータ３００は、非接触通信カードの読み込みを行う（ステップＳ７０～Ｓ７８）。そして、パーソナルコンピュータ３００は、Ｗｅｂブラウザを起動する（ステップＳ８０）。ステップＳ７０～Ｓ８０の処理は、図３のステップＳ１０～Ｓ２０の処理と同様である。

【００６３】
３）ｈｔｔｐ＿ｇｅｔ(起動ＵＲＬ)コマンドの送信
パーソナルコンピュータ３００のＷｅｂブラウザは、ｈｔｔｐ＿ｇｅｔコマンド(起動ＵＲＬを含む)を送信する（ステップＳ８２）。そして。Ｗｅｂブラウザは、ｈｔｔｐ＿ｇｅｔコマンドによりＷｅｂサーバ４００のＵＲＬにインターネット８００経由で接続し、ｈｔｔｐ＿ｇｅｔコマンドにより取得したｈｔｔｐフォーマットの受信データを解析してログイン画面を表示する。
【００６４】
４）ｈｔｔｐｓ＿ｇｅｔ(セッション番号要求)
パーソナルコンピュータ３００は、Ｗｅｂサーバ４００への通信路をＳＳＬで暗号化した後、Ｗｅｂサーバ４００へアクセスを行い、サーバに対してセッション番号の払い出し要求を行う（ステップＳ８４）。ここで、Ｗｅｂサーバ４００が払い出すセッション番号は、乱数などを用いて他ユーザのログイン用セッション番号との区別ができるものとし、また所定の有効期限が過ぎた場合は無効化されるものとする。後述するが、セッション番号は、ユーザによるログインを確認するために使用される番号であり、固有（ユニーク）の番号とされる。
【００６５】
例えば、パーソナルコンピュータ３００は、”ｈｔｔｐｓ：／／ｗｗｗ．ｗｅｂ＿ｓｅｒｖｅｒ．ｃｏ．ｊｐ／ｌｏｇｉｎ．ｈｔｍｌ＋ｇｅｔ＿ｓｅｓｓｉｏｎ＿ｎｕｍｂｅｒ．ｃｇｉ”をｈｔｔｐｓ＿ｇｅｔコマンドで送信する。Ｗｅｂサーバ４００は、実行コード(ｃｇｉスクリプト等)で生成したセッション番号をｈｔｍｌフォーマットで記載し、ｈｔｔｐｓ＿ｇｅｔへ返信する（ステップＳ８５）。
【００６６】
５）ｈｔｔｐｓ＿ｇｅｔ（ＳＡＭ＿ＵＲＬ、ログイン＿ＵＲＬ、セッション番号）
パーソナルコンピュータ３００は、ＳＡＭサーバ５００への通信路をＳＳＬで暗号化した後にアクセスを行い、ＳＡＭサーバ５００に対してＷｅｂサーバ４００へのログイン要求コマンドを送信する（ステップＳ８６）。このとき、要求コマンドにはログイン先のＷｅｂサーバ４００のＵＲＬ、ＳＡＭサーバ５００のＵＲＬ、及びステップＳ８５でＷｅｂサーバ４００から取得したセッション番号情報が引数として付加される。なお、ログイン先のＵＲＬ、ＳＡＭサーバ５００のＵＲＬは、非接触通信カード１００のメモリから読取られたものである。
【００６７】
例えば、パーソナルコンピュータ３００は、”ｈｔｔｐｓ：／／ｗｗｗ．ｓａｍ＿ｓｅｒｖｅｒ．ｃｏ．ｊｐ／ｒｅｍｏｔｅ＿ｌｏｇｉｎ．ｃｇｉ？ＵＲＬ＝ｗｗｗ．ｗｅｂ＿ｓｅｒｖｅｒ．ｃｏ．ｊｐ？ｓｅｓｓｉｏｎ＝ＸＸＸ”をｈｔｔｐｓ＿ｇｅｔコマンドで送信し、ＳＡＭサーバ５００はログイン情報取得用の実行コード(ｃｇｉスクリプト等)を起動する。
５．１）ログイン情報取得
次に、ＳＡＭサーバ５００は、非接触通信カード１００のセキュア領域よりログイン情報を取得する（ステップＳ８８）。ここでの取得方法は、第１の実施形態の図４で説明した処理と同様であるが、ＳＡＭサーバ５００とパーソナルコンピュータ３００との間にはＷｅｂサーバ４００が仲介をしていない。第２の実施形態は、ＳＡＭサーバ５００とパーソナルコンピュータ３００が直接通信する点で第１の実施形態と相違する。
【００６８】
９は、ステップＳ８８の処理を示すシーケンス図である。
【００６９】
１）セキュアクライアント起動要求
先ず、ＳＡＭサーバ５００は、パーソナルコンピュータ３００に対して、ｈｔｔｐ＿ｇｅｔコマンドなどを送信することにより、セキュアクライアントの起動要求を出す（ステップＳ１００）。セキュアクライアントは、パーソナルコンピュータ３００が有するプロ

グラムである。
【００７０】
１．１．１）セキュアクライアント起動
セキュリティクライアントの起動コマンドを取得したパーソナルコンピュータ３００内部のＣＰＵ３０８は、セキュリティクライアントを起動する（ステップＳ１０２）。このクライアントプログラムは、ＳＡＭサーバ５００とパーソナルコンピュータ３００との通信路を暗号化し、またＳＡＭサーバ５００から受信したカード制御コマンドをカードリーダライタ２００の制御コマンドに変換して非接触通信カード１００のカード制御を行うプログラムである。これにより、パーソナルコンピュータ３００からＳＡＭサーバ５００に至る経路が暗号化され、ＳＡＭサーバ５００～パーソナルコンピュータ３００間で送受信されるパケットが暗号化される。従って、非接触通信カード１００に対してどのようなコマンドを送信したのかを隠すことができる。
【００７１】
２）認証要求（公開情報１）
暗号化通信路を確立したＳＡＭサーバ５００は、非接触通信カード１００に対して暗号化の認証を要求するため、パーソナルコンピュータ３００に対して認証要求コマンドを送信する（ステップＳ１０４）。このコマンドには乱数Ｎ１および秘密鍵Ａより生成された公開情報（公開鍵）１が含まれる。認証要求は、ＳＡＭサーバ５００～パーソナルコンピュータ３００間で既に暗号化されている伝送路の中で行われる。なお、この時点で非接触通信カード１００は、カードリーダライタ２００と接近または接触した状態にあり、カードリーダライタ２００と通信可能であるものとする。
【００７２】
２．１）認証要求（公開情報１）
パーソナルコンピュータ３００は、認証要求コマンドをカードリーダライタ２００用に変換した後、カードリーダライタ２００へ送信する（ステップＳ１０６）。
【００７３】
２．１．１）認証要求（公開情報１）
カードリーダライタ２００は、認証要求コマンドをＲＦ信号に変換した後、非接触通信カード１００へ送信する（ステップＳ１０８）。非接触通信カード１００には、秘密鍵Ａが格納されているので、非接触通信カード１００は、この鍵Ａと乱数Ｎ２より公開情報（公開鍵）２を生成する。公開情報２は、カードリーダライタ２００、及びパーソナルコンピュータ３００を経由してＳＡＭサーバ５００に返信される（ステップＳ１０９）。
【００７４】
３）、４）共有鍵生成
非接触通信カード１００とＳＡＭサーバ５００のそれぞれでは、公開情報１，２を送受信して交換したことにより、両者で同一の鍵である共有鍵（秘密鍵）を生成し（ステップＳ１１０，Ｓ１１２）、共有鍵を共有する。共有鍵を生成した後は、非接触通信カード１００のセキュア領域からの必要な領域の読み出し値は、この共通鍵で暗号化された状態で送信される。なお、ステップＳ１０４からステップＳ１１２に至る共有鍵の生成は、第１の実施形態と同様、ディフィーヘルマン（Diffie-Hellman）鍵交換と呼ばれる一般的手法により行うことができる。以上のようにしてＳＡＭサーバ５００から非接触通信カード１００に至る暗号化された伝送路が形成され、ＳＡＭサーバ５００と非接触通信カード１００がセキュアに通信できる状態となる。
【００７５】
５）セキュリティ領域読出し（Ｒｅａｄ）要求
ＳＡＭサーバ５００は、非接触通信カード１００のセキュア領域に書き込まれているログイン情報（ユーザ名、パスワード等）を取得する。このため、ＳＡＭサーバ５００は、暗号化された通信路を用いて、パーソナルコンピュータ３００へ非接触通信カード１００のセキュア領域の読出し（Ｒｅａｄ）要求を送信する（ステップＳ１１４）。セキュア領域への読出し（Ｒｅａｄ）要求には、非接触通信カード１００のメモリ１０６のアクセス

する領域（サービスエリア）の情報が含まれている。
【００７６】
５．１）セキュア領域読出し（Ｒｅａｄ）要求
パーソナルコンピュータ３００上のセキュリティクライアントは、セキュア領域への読出し（Ｒｅａｄ）要求を受信すると、セキュア領域への読出し（Ｒｅａｄ）要求をカードリーダライタ２００用のコマンドフォーマットに変換する。そして、セキュリティクライアントは、変換したコマンドフォーマットをカードリーダライタ２００へ送信する（ステップＳ１１６）。
【００７７】
５．１．１）セキュア領域アクセス
セキュア領域への読出し（Ｒｅａｄ）要求を受けたカードリーダライタ２００は、非接触通信カード１００のセキュア領域にアクセスする（ステップＳ１１８）。非接触通信カード１００は、セキュア領域に格納されたログイン情報（ユーザ名およびパスワード）を共有鍵で暗号化し、暗号化された伝送路を経由して、ＳＡＭサーバ５００に返信する（ステップＳ１２０）。
【００７８】
６）ログイン情報の復号
ＳＡＭサーバ５００は、暗号化された伝送路から非接触通信カード１００のログイン情報を受信すると、共通鍵を用いて暗号化されているログイン情報を復号する（ステップＳ１２２）。
【００７９】
以上説明した図９のシーケンスにより、ＳＡＭサーバ５００は、図８のステップＳ８８において、非接触通信カード１００からログイン情報を取得することができる。
【００８０】
５．２）通信路の暗号化
ログイン情報を取得したＳＡＭサーバ５００は、図８のステップＳ８６で取得したログインＵＲＬで指定されるＷｅｂサーバ４００と接続を行い、ＳＳＬ等の処理で通信路を暗号化する（図８のステップＳ９０）。
【００８１】
５．３）ログイン要求（ログイン情報、セッション番号）
ＳＡＭサーバ５００は、Ｗｅｂサーバ４００へログイン情報（ユーザ名、パスワード、セッション番号等）を含むコマンドを送信する（ステップＳ９２）。Ｗｅｂサーバ４００は、セッション番号を受信することにより、ＳＡＭサーバ５００からのログインが、どのセッションに対するログインであるかを判別することが可能である。Ｗｅｂサーバ４００はログイン情報の真偽をチェックした後、真であればログインを行い、ログイン完了通知をＳＡＭサーバ５００に送信する（ステップＳ９４）。ログイン完了を受信したＳＡＭサーバ５００は、同様にログイン完了通知をパーソナルコンピュータ３００に返信する（ステップＳ９５）。
【００８２】
６．ｈｔｔｐｓ＿ｇｅｔ(ログイン確認、セッション番号)
パーソナルコンピュータ３００は、ログイン完了通知を受信すると、Ｗｅｂサーバ４００にセッション番号を送信し（ステップＳ９６）、ＳＡＭサーバ５００からのログインが完了したことを確認する。例えば、パーソナルコンピュータ３００は、”ｈｔｔｐｓ：／／ｗｗｗ．ｓａｍｐｌｅ＿ｗｅｂ＿ｓｅｒｖｅｒ．ｃｏ．ｊｐ／ｓａｍ＿ｌｏｇｉｎ＿ｃｆｍ．ｃｇｉ？ｓｅｓｓｉｏｎ＝ＹＹＹ”をｈｔｔｐｓ＿ｇｅｔコマンドで送信し、Ｗｅｂサーバ４００はログイン結果を返信する。これにより、パーソナルコンピュータ３００の画面には、ログイン後の画面が表示される。従って、ユーザは、パーソナルコンピュータ３００のＷｅｂブラウザの画面上で、ログイン画面に入ったことを確かめることができる。
【００８３】

図１０は、第２の実施形態に係るパーソナルコンピュータ３００の構成を示す機能ブロック図である。図１０に示すように、パーソナルコンピュータ３００は、アクセス先情報送信部３２０、識別情報取得部３２２、ログイン情報送信部３２４、受信処理部３２６を備える。各機能ブロックは、パーソナルコンピュータ３００が備えるハードウエア、ＣＰＵ３０８とこれを機能させるためのソフトウェア（プログラム）によって構成されることができる。そのプログラムは、パーソナルコンピュータ３００が備えるハードディスク、またはパーソナルコンピュータ３００の会部から接続されるメモリなどの記録媒体に格納されることができる。

【００８４】

以上説明したように第２の実施形態によれば、パーソナルコンピュータ３００のＷｅｂブラウザ上でＷｅｂサーバ４００のＵＲＬを表示する際に、セッション番号を用いることで、Ｗｅｂサーバ４００とＳＡＭサーバ５００を並列動作させることが可能となる。従って、Ｗｅｂサーバ４００とＳＡＭサーバ５００を並列動作させた状態で、セッション番号に基づいてログインしたアクセス先の情報をパーソナルコンピュータ３００に表示させることが可能となる。

【００８５】

＜３．第３の実施形態＞

次に、本発明の第３の実施形態について説明する。第３の実施形態は、セキュア領域をローカル化した仮想ブラウザに関するものである。

【００８６】

図１１及び図１２は、第３の実施形態に係るシステム構成と、情報のやり取りを模式的に示した概念図である。本実施形態のシステムも、非接触通信カード１００、カードリーダライタ２００、パーソナルコンピュータ３００、Ｗｅｂサーバ４００、ＳＡＭ（Ｓｅｃｕｒｅ　Ａｐｐｌｉｃａｔｉｏｎ　Ｍｏｄｕｌｅ）サーバ５００を備える。

【００８７】

図１１及び図１２に基づいて、本実施形態の情報のやり取りの概念を説明すると、非接触通信カード１００は、そのメモリ内にフリー領域とセキュア領域を備えている。フリー領域には、ＵＲＬなどの情報が格納され、セキュア領域にはユーザ名、パスワードなどのログイン情報が格納されている。非接触通信カード１００をカードリーダライタ２００に接触または接近させると、ＳＡＭサーバ５００のブラウザが起動する。更にＳＡＭサーバ５００がＷｅｂサーバ４００と通信を行うことにより、ＳＡＭサーバ５００のブラウザ（仮想ブラウザ）にＷｅｂサーバ４００のＵＲＬが表示された状態でパーソナルコンピュータ３００に表示が行われる。

【００８８】

Ｗｅｂサーバ４００のＵＲＬがユーザ名、パスワードなどのログイン情報を要求する場合は、図１２に示すように、ＳＡＭサーバ５００が暗号化された通信路を介して非接触通信カード１００からログイン情報を取得する。

【００８９】

また、Ｗｅｂサーバ４００がローカルアクセス要求を出した場合、ＳＡＭサーバ５００は、ローカル情報へのアクセスを行う。この際、図１２に示すように、ユーザの選択に応じて、パーソナルコンピュータ３００が備えるハードディスクドライブなどの記憶媒体、または非接触通信カード１００のセキュア領域に対して、ＳＡＭサーバ５００はアクセスし、キャッシュ情報などの書き込みまたは読出しを行う。これにより、ユーザは、非接触通信カード１００をカードリーダライタ２００と接触または接近させるのみで、ＳＡＭサーバ５００上の仮想ブラウザを介してＷｅｂサーバ４００のＵＲＬにアクセスすることが可能となる。

【００９０】

次に、本実施形態のシステムについて、図１３～図１５に基づいて詳細に説明する。第３の実施形態に係るシステム構成、及び非接触通信カード１００、カードリーダライタ２００、パーソナルコンピュータ３００、Ｗｅｂサーバ４００、ＳＡＭサーバ５００の構

成は、図２と同様である。図１３は、第３の実施形態の処理を示すシーケンス図である。

【００９１】

１）非接触通信カード１００の読み込み

先ず、パーソナルコンピュータ３００は、非接触通信カードの読み込みを行う（ステップＳ１３０～Ｓ１３８）。そして、パーソナルコンピュータ３００は、Ｗｅｂブラウザを起動する（ステップＳ１４０）。ステップＳ１３０～Ｓ１３８の処理は、図３のステップＳ１０～Ｓ２０の処理と同様である。

【００９２】

３）仮想ブラウザ起動

パーソナルコンピュータ３００のＷｅｂブラウザは、ＳＡＭサーバ５００の接続先ＵＲＬにインターネット８００経由で接続し、ｈｔｔｐ＿ｇｅｔコマンドによりＳＡＭサーバ５００に仮想ブラウザの起動要求を送信する（ステップＳ１４２）。これにより、ＳＡＭサーバ５００において、Ｗｅｂブラウザ（仮想ブラウザ）が立ち上がる。以後、仮想ブラウザがＷｅｂサーバ４００から受信するｈｔｍｌデータは、基本的にパーソナルコンピュータ３００に転送され、パーソナルコンピュータ３００のＷｅｂブラウザは受信データを解析して画面表示を行なう。従って、図１１に示すように、パーソナルコンピュータ３００の表示画面には、パーソナルコンピュータ３００のＷｅｂブラウザにＳＡＭサーバ５００の仮想ブラウザが表示され、仮想ブラウザ上にＷｅｂサーバ４００のＵＲＬで指定される情報が表示される。

【００９３】

４）Ｗｅｂアクセス要求

パーソナルコンピュータ３００は、ステップＳ１３８でカードより取得した接続先のＵＲＬ情報を付加して、ＳＡＭサーバ５００にＷｅｂアクセスの要求コマンドを送信する（ステップＳ１４４）。

【００９４】

４．１）ｈｔｔｐ＿ｇｅｔ（起動ＵＲＬ）

ＳＡＭサーバ５００は、受信したＵＲＬを含むｈｔｔｐ＿ｇｅｔコマンドをＷｅｂサーバ４００に送信し（ステップＳ１４６）、受信したｈｔｔｐデータをパーソナルコンピュータ３００に転送する。これにより、パーソナルコンピュータ３００の表示画面には、Ｗｅｂサーバ４００のＵＲＬが表示される。

【００９５】

５）ログイン要求

ここで起動先のＷｅｂサーバ４００がログイン画面を表示する場合は、パーソナルコンピュータ３００はＳＡＭサーバ５００にログイン要求コマンドを送信する（ステップＳ１４８）。

【００９６】

５．１）ログイン情報（ユーザ名、パスワード）取得

ＳＡＭサーバ５００は、ログイン要求コマンドを受信すると、ログイン情報を取得する処理を行う（ステップＳ１５０）。ログイン情報は、図９で説明した第２の実施形態と同様な手順によって非接触通信カード１００のセキュア領域から取得される。

【００９７】

５．２）ログイン要求

ＳＡＭサーバ５００は、ステップＳ１５０で取得したログイン情報を用いて、ステップＳ１３０～Ｓ１３８で非接触通信カード１００から読み取ったＵＲＬのＷｅｂサーバ４００にログイン要求を行なう（ステップＳ１５２）。

【００９８】

６）ローカルアクセス要求

Ｗｅｂサーバ４００によっては、ログインの際に、ログイン情報の他に、当該Ｗｅｂサーバ４００へのログイン履歴と、ユーザのパーソナルコンピュータ３００のローカルな記憶媒体に記録されたログイン履歴（Ｃｏｏｋｉｅ内に保存されている）とのマッチングを

行い、ユーザ（ログイン）認証を行なう場合がある。この場合、Ｗｅｂサーバ４００は、ローカル（パーソナルコンピュータ３００）へのアクセス要求を出す（ステップＳ１５６）。また、ユーザは、パーソナルコンピュータ３００のローカルハードディスクドライブ（ＨＤＤ）に保存された「お気に入り（Ｆａｖｏｒｉｔｅ）」の中から表示するＵＲＬを選択することができる。これらの情報は、Ｗｅｂサーバ４００からＳＡＭサーバ５００の仮想ブラウザを経由してパーソナルコンピュータ３００に通知される。なお、ローカルアクセス先は、上述したＣｏｏｋｉｅ、Ｆａｖｏｒｉｔｅに限定されるものではなく、Ｈｉｓｔｏｒｙなどブラウザがパーソナルコンピュータ３００のローカルＨＤＤに保存する全ての情報が対象となり得る。

【００９９】

６．１）ローカルアクセス処理

ＳＡＭサーバ５００は、ローカルアクセス要求を受けると、ローカルアクセス処理を行う（ステップＳ１５８）。ローカル情報の読み書き先は、ハードディスクなどパーソナルコンピュータ３００自体が内包する記憶媒体、または、セキュリティ領域を有する外部の非接触通信カード１０の２つから選択することができる。

【０１００】

図１４は、ステップＳ１５８のローカルアクセス処理の詳細を示すシーケンス図である。

【０１０１】

１）ローカルアクセス要求

先ず、ＳＡＭサーバ５００は、パーソナルコンピュータ３００に対してローカルアクセス要求を出す（ステップＳ１７０）。

【０１０２】

２）ユーザ確認

Ｗｅｂサーバ４００からのローカルアクセス要求を受信したパーソナルコンピュータ３００は、アクセスが可能な保存媒体の一覧（非接触通信カード１００を含む）を作成する。また、ローカルアクセス要求を受信したパーソナルコンピュータ３００は、ユーザに対して「ローカルアクセスの許可または不許可」の確認画面を表示する。「許可」が選択された場合は、アクセス先の候補として「パーソナルコンピュータ３００のローカルのＨＤＤまたは非接触通信カード１００（セキュア領域）」のいずれか一方をユーザに選択させるための画面表示を行う（ステップＳ１７２）。そして、ユーザからのアクセス先選択結果をＳＡＭサーバ５００に送信する。

【０１０３】

図１４に戻って、ステップＳ１７２において、ＨＤＤが選択された場合は、Ｗｅｂサーバ４００が要求するローカル情報へのアクセス先にＨＤＤを設定し、以後の読み書きはＨＤＤに対して行なう。なお、パーソナルコンピュータ３００のローカルアクセス先は、ＨＤＤに限定されるものではなく、フラッシュメモリ（ＮＶＭ）等、パーソナルコンピュータ３００が内包する、またはパーソナルコンピュータ３００に接続される全ての記憶媒体が含まれる。

【０１０４】

４）セキュアクライアント起動要求

一方、ステップＳ１７２で非接触通信カード１００が選択された場合、ＳＡＭサーバ５００は、パーソナルコンピュータ３００に対してセキュアクライアント起動の要求コマンドを送信する（ステップＳ１７６）。

【０１０５】

４．１）セキュアクライアント起動

セキュリティクライアントの起動コマンドを取得したパーソナルコンピュータ３００内部のＣＰＵ３０８は、セキュリティクライアントを起動する（ステップＳ１７８）。このクライアントプログラムは、ＳＡＭサーバ５００とパーソナルコンピュータ３００との通信路を暗号化する。また、クライアントプログラムは、ＳＡＭサーバ５００から受信した

カード制御コマンドをカードリーダライタ２００の制御コマンドに変換して、非接触通信カード１００のカード制御を行う。

【０１０６】

５）認証要求（公開情報１）

暗号化通信路を確立したＳＡＭサーバ５００は、パーソナルコンピュータ３００に対して認証要求コマンドを送信する（ステップＳ１８２）。このコマンドには、乱数Ｎ１および秘密鍵Ａより生成された公開情報１が含まれる。

【０１０７】

５．１）認証要求（公開情報１）

パーソナルコンピュータ３００は、認証要求コマンドをカードリーダライタ２００用に変換した後、カードリーダライタ２００に送信する（ステップＳ１８４）。

【０１０８】

５．１．１）認証要求（公開情報１）

カードリーダライタ２００は、認証要求コマンドをＲＦ信号に変換した後、非接触通信カード１００へ送信する。非接触通信カード１００には秘密鍵Ａが格納されているので、非接触通信カード１００は、この鍵Ａと乱数Ｎ２より公開情報２を生成し、パーソナルコンピュータ３００を経由してＳＡＭサーバ５００に公開情報２を返信する（ステップＳ１８８）。

【０１０９】

６）、７）共有鍵生成

非接触通信カード１００、及びＳＡＭサーバ５００は、送受信した公開情報１，２より両者で同一の鍵である共有鍵を生成する（ステップＳ１９０，Ｓ１９２）。以後、非接触通信カード１００のセキュリティ設定領域が必要な領域の読み出し値は、この共通鍵で暗号化された状態で送信される。第１、第２の実施形態と同様、共有鍵の生成は、一般にディフィーヘルマン（Diffie-Hellman）鍵交換と呼ばれる手法により行うことができる。

【０１１０】

８）Ｗｒｉｔｅ情報の暗号化（共通鍵）

ＳＡＭサーバ５００は、Ｗｅｂサーバ４００からの非接触通信カード１００へのアクセス種別が書き込み（Ｗｒｉｔｅ）であった場合、書き込みデータを共通鍵で暗号化する（ステップＳ１９４）。

【０１１１】

９）セキュリティ領域R/W要求

SAMサーバ５００は、パーソナルコンピュータ３００へセキュリティ領域の読出し（Ｒｅａｄ）または書き込み（Ｗｒｉｔｅ）要求を送信する（ステップＳ１９６）。セキュリティ領域へのＲｅａｄまたは Ｗｒｉｔｅ要求にはアクセスする領域（サービスエリア）の情報が含まれている。

【０１１２】

９．１）セキュア領域Read/Write要求

パーソナルコンピュータ３００上のセキュリティクライアントは、セキュア領域への読出し（Ｒｅａｄ）または書き込み（Ｗｒｉｔｅ）要求をカードリーダライタ２００用のコマンドフォーマットに変換する。セキュリティクライアントは、変換したコマンドフォーマットをカードリーダライタ２００へ送信する（ステップＳ１９８）。

【０１１３】

９．１．１）セキュア領域アクセス

カードリーダライタ２００は、非接触通信カード１００のセキュア領域にアクセスを行う（ステップＳ２００）。セキュア領域へのアクセスは、読出し（Ｒｅａｄ）または書き込み（Ｗｒｉｔｅ）要求に分類される。書き込み（Ｗｒｉｔｅ）情報は共通鍵で復号された後、適切なサービスエリアに書き込みが行われる。また、指定されたサービスエリアから読み出された読出し（Ｒｅａｄ）情報は、共通鍵で暗号化されＳＡＭサーバ５００に返信される（ステップＳ２０２）。

【０１１４】
１０）Ｒｅａｄ情報の復号（共通鍵）
ＳＡＭサーバ５００は、Ｗｅｂサーバ４００からの非接触通信カード１００へのアクセス種別が読出し（Ｒｅａｄ）であった場合、ステップＳ２０２で受信した読出し（Ｒｅａｄ）データを共通鍵で復号する。
【０１１５】
図１５は、図１３及び図１４で説明した処理において、ＳＡＭサーバ５００によるローカルへのアクセス処理（ステップＳ２２８以降）を説明するためのフローチャートである。図１５に基づいて処理を説明すると、ステップＳ２２０では、非接触通信カード１００とカードリーダライタ２００が通信を開始する。次にステップＳ２２２では、パーソナルコンピュータ３００のＷｅｂブラウザが起動し、次のステップＳ２２４ではＷｅｂブラウザ内で仮想ブラウザが起動される。次のステップＳ２２６では、Ｗｅｂブラウザからローカルアクセス要求が出される。
【０１１６】
ステップＳ２２８以降では、ＳＡＭサーバ５００がローカルへのアクセス処理を行う。ステップＳ２２８では、ローカル情報のアクセスがユーザによって許可されたか否かが判定され、アクセスが許可された場合はステップＳ２３０へ進む。ステップＳ２３０では、ユーザによりアクセス先が選択される。一方、ステップＳ２２８でアクセスが不許可の場合は、アクセスが失敗した旨を返信する。
【０１１７】
アクセス先が非接触通信カード１００の場合、ステップＳ２３２へ進み、非接触通信カード１００のセキュア領域を仮想的にローカルのＨＤＤとする。次にステップＳ２３４では、Ｃｏｏｋｉｅ等の情報を非接触通信カード１００に書き込む。ここでの処理は、図１４のステップＳ１９４～Ｓ２０４に対応する。例えば、ユーザがネットカフェ等に設置されたパーソナルコンピュータ３００を使用する場合、個人的情報がパーソナルコンピュータ３００のＨＤＤに書き込まれてしまうのは好ましくない。このため、アクセス先を非接触通信カード１００とすることで、個人的情報をカード１００のセキュア領域に書き込むことができる。この際、非接触通信カード１００とＳＡＭサーバ５００の間には暗号化された伝送路が構築されているため、安全にカード１００に情報を書き込むことが可能である。
【０１１８】
一方、ステップＳ２３０でＨＤＤが選択された場合は、Ｃｏｏｋｉｅ等の情報をパーソナルコンピュータ３００のＨＤＤに書き込む。ここでの処理は、図１４のステップＳ１７４に対応する。ステップＳ２３４，Ｓ２３６の後はステップＳ２３８へ進み、アクセス情報の返信を行う。
【０１１９】
図１６は、第３の実施形態に係るパーソナルコンピュータ３００の構成を示す機能ブロック図である。図１６に示すように、パーソナルコンピュータ３００は、アクセス先情報送信部３３０、ログイン情報送信部３３２、受信処理部３３４を備える。各機能ブロックは、パーソナルコンピュータ３００が備えるハードウエア、ＣＰＵ３０８とこれを機能させるためのソフトウェア（プログラム）によって構成されることができる。そのプログラムは、パーソナルコンピュータ３００が備えるハードディスク、またはパーソナルコンピュータ３００の会部から接続されるメモリなどの記録媒体に格納されることができる。
【０１２０】
図１７は、第３の実施形態に係るＳＡＭサーバ５００の構成を示す機能ブロック図である。図１７に示すように、ＳＡＭサーバ５００は、アクセス先情報取得部５２０、ログイン情報受信部５２２、ログイン実行部５２４、アクセス先情報送信部５２６、ローカルアクセス部５２８を備える。各機能ブロックは、ＳＡＭサーバ５００が備えるハードウエア、ＣＰＵ３０８とこれを機能させるためのソフトウェア（プログラム）によって構成されることができる。そのプログラムは、ＳＡＭサーバ５００が備えるハードディスク、また

はパーソナルコンピュータ３００の会部から接続されるメモリなどの記録媒体に格納されることができる。

【０１２１】

以上のように第３の実施形態では、パーソナルコンピュータ３００は、基本的にＳＡＭサーバ５００上の仮想ブラウザを表示する機能と、ユーザによる選択をＳＡＭサーバ５００に伝える機能を果たしている。つまり、パーソナルコンピュータ３００は、ユーザがＳＡＭサーバ５００の仮想ブラウザを閲覧する際の中継としての役割を果たしている。そして、仮想ブラウザを閲覧している際に、ユーザの個人情報の読み出し、またはクッキー情報等の保存が必要となる場合は、ユーザの選択に応じて、パーソナルコンピュータ３００の記憶媒体、または非接触通信カード１００のセキュア領域にアクセスすることが可能である。

【０１２２】

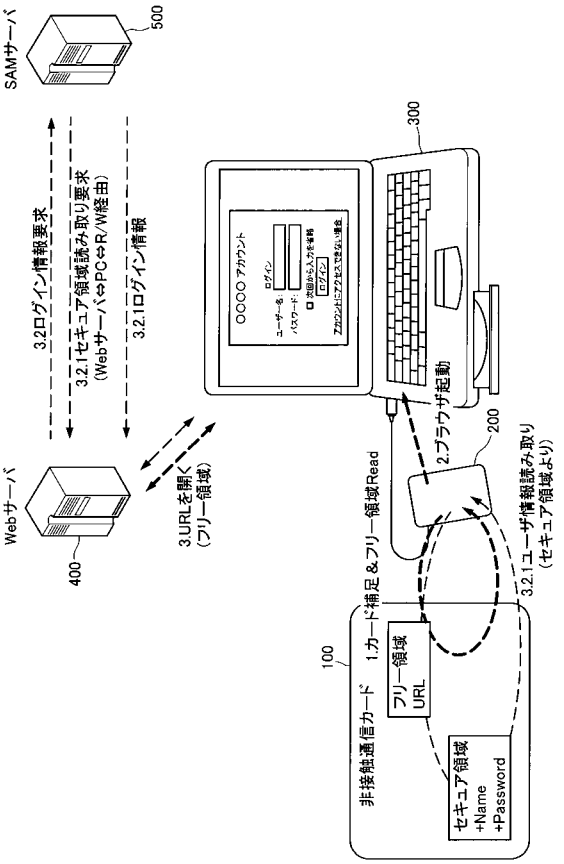
以上、添付図面を参照しながら本発明の好適な実施形態について詳細に説明したが、本発明はかかる例に限定されない。本発明の属する技術の分野における通常の知識を有する者であれば、特許請求の範囲に記載された技術的思想の範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、これらについても、当然に本発明の技術的範囲に属するものと了解される。

【符号の説明】

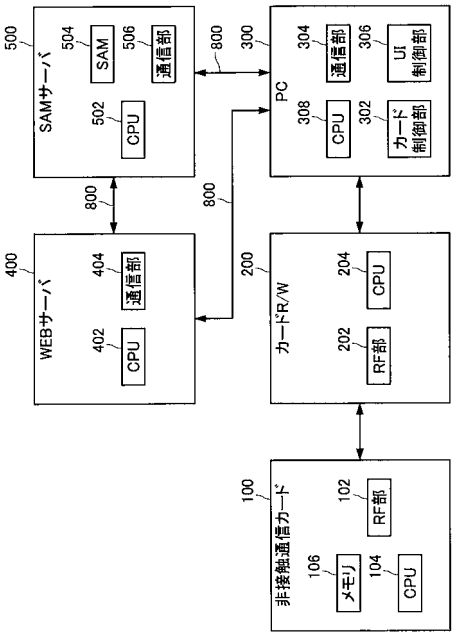
【０１２３】

３１０　アクセス先情報送信部
３１２　ログイン情報送信部
３１４　受信処理部
４１０　アクセス先情報取得部
４１２　ログイン情報取得部
４１４　ログイン実行部
４１６　情報送信部
３２２　識別情報取得部
５２０　アクセス先情報取得部
５２２　ログイン情報受信部
５２４　ログイン実行部
５２６　アクセス先情報送信部
５２８　ローカルアクセス部

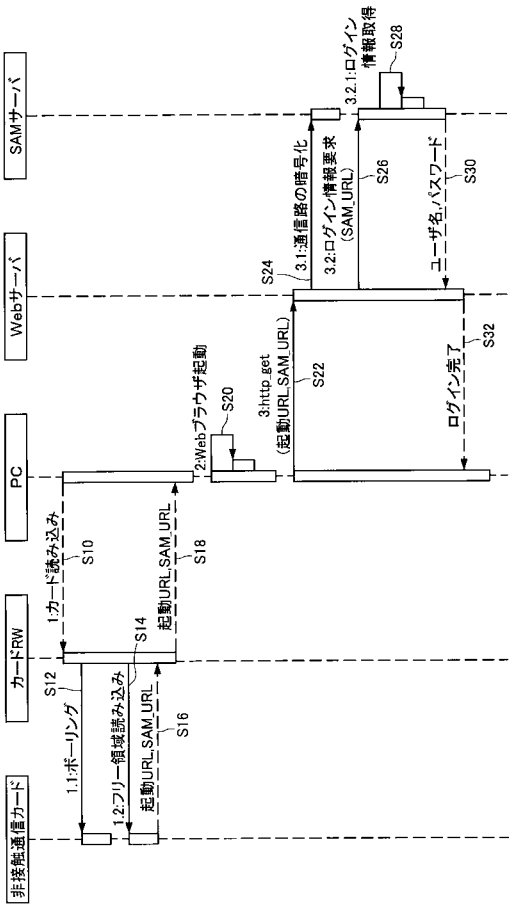
【図１】


SAMサーバ
500
3.2ログイン情報要求
3.2.1セキュア領域読み取り要求
(WebサーバPCR/W経由)
3.2.1ログイン情報
Webサーバ
400
3.URLを開く
(フリー領域)
300
2.ブラウザ起動
200
3.2.1ユーザ情報読み取り
(セキュア領域より)
100
非接触通信カード
1.カード抽足&フリー領域Read
フリー領域
URL
セキュア領域
+Name
+Password

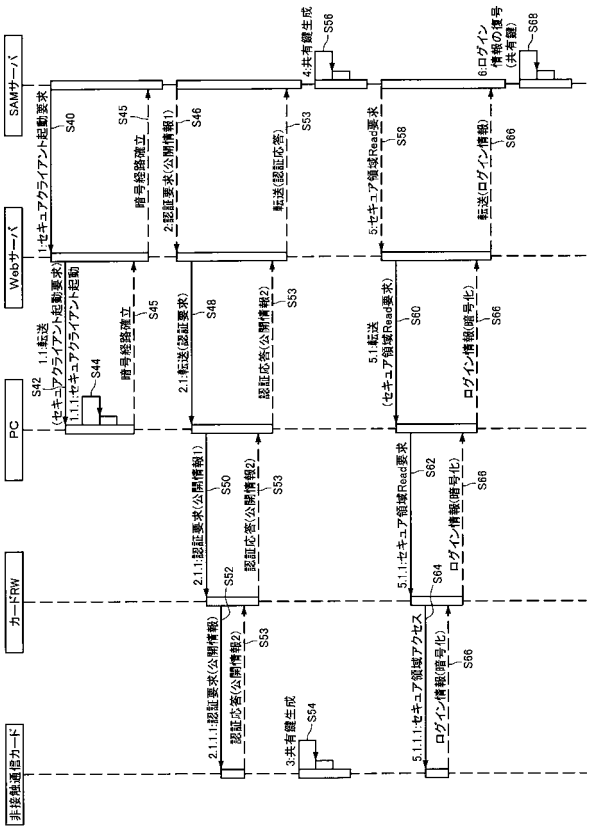
【図２】


500
SAMサーバ
504
SAM
506
通信部
502
CPU
800
300
PC
304
通信部
306
UI
制御部
308
CPU
302
カード
制御部
400
WEBサーバ
404
通信部
402
CPU
200
カードR/W
204
CPU
202
RF部
100
非接触通信カード
106
メモリ
102
RF部
104
CPU

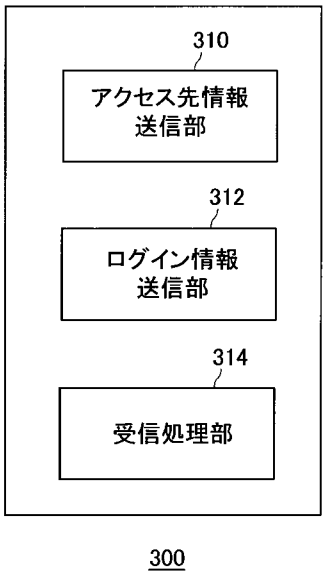
【図３】


非接触通信カード
カードRW
PC
Webサーバ
SAMサーバ
1.1:ポーリング
S12
1.2:フリー領域読み込み
S14
1:カード読み込み
S10
起動URL.SAM_URL
S16
起動URL.SAM_URL
S18
2:Webブラウザ起動
S20
3:http get
(起動URL.SAM_URL)
S22
3.1:通信路の暗号化
S24
3.2:ログイン情報要求
(SAM_URL)
S26
3.2.1:ログイン
情報取得
S28
ユーザ名.パスワード
S30
ログイン完了
S32

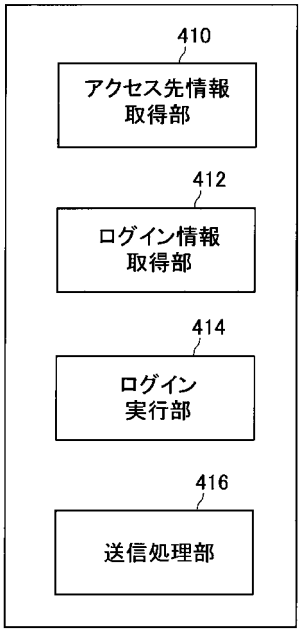
【図４】


非接触通信カード
カードRW
PC
Webサーバ
SAMサーバ
1.1:セキュアクライアント起動要求
S40
1.1.1:セキュアクライアント起動
S42
暗号経路確立
S44
2:認証要求(公開情報1)
S45
2.1:転送(認証要求)
S46
2.1.1:認証要求(公開情報1)
S48
認証応答(公開情報2)
S50
2.1.1.1:認証要求(公開情報2)
S52
認証応答(公開情報2)
S53
3:共有鍵生成
S54
転送(認証応答)
S53
4:共有鍵生成
S56
5:セキュア領域Read要求
S58
5.1:転送
(セキュア領域Read要求)
S60
5.1.1:セキュア領域Read要求
S62
5.1.1.1:セキュア領域アクセス
S64
ログイン情報(暗号化)
S66
ログイン情報(暗号化)
S66
転送(ログイン情報)
S66
6:ログイン
情報の復号
(共有鍵)
S68
ログイン情報(暗号化)
S66

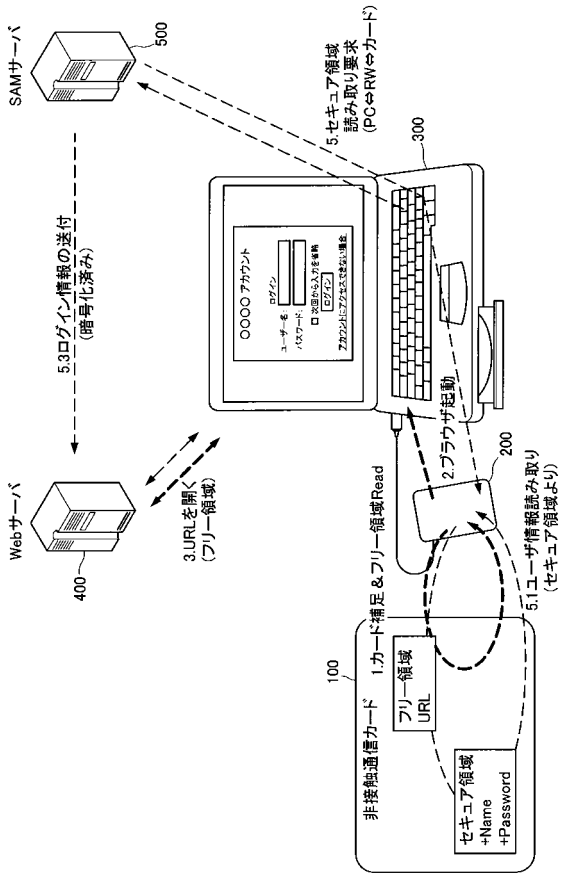
【図５】


310
アクセス先情報
送信部
312
ログイン情報
送信部
314
受信処理部
300

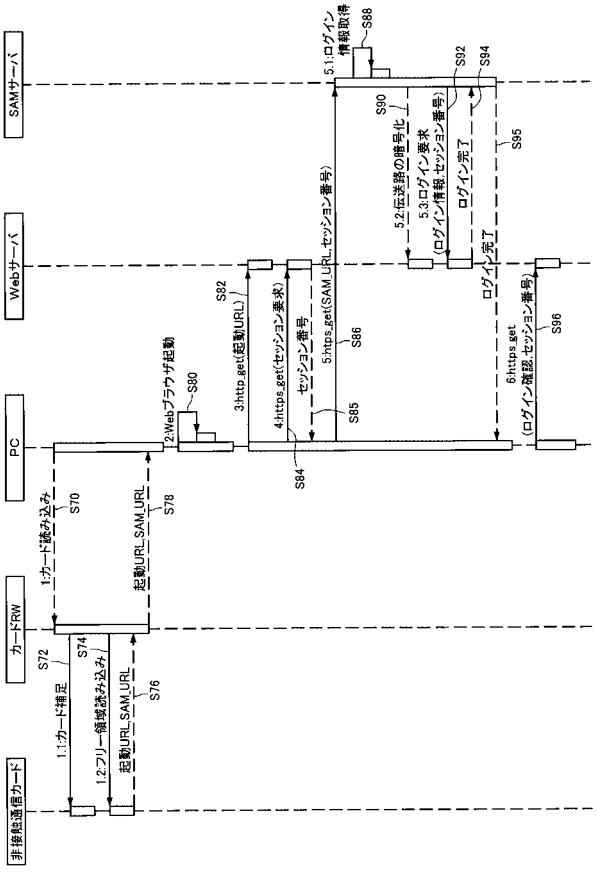
【図６】


410
アクセス先情報
取得部
412
ログイン情報
取得部
414
ログイン
実行部
416
送信処理部
400

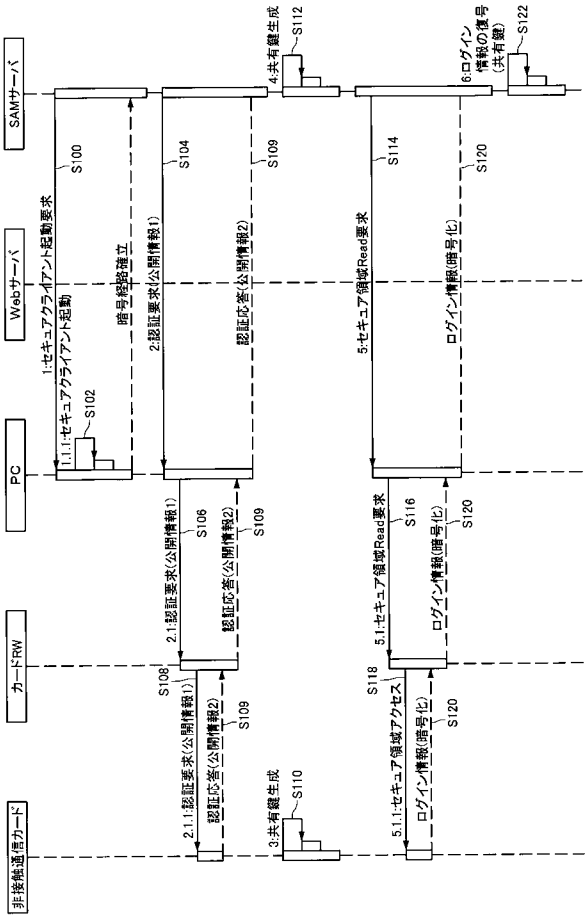
【図７】


SAMサーバ
500
5.セキュア領域
読み取り要求
(PC⇔RW⇔カード)
300
5.0ログイン情報の送付
(暗号化済み)
Webサーバ
400
3.URLを開く
(フリー領域)
2.ブラウザ起動
200
5.1ユーザ情報読み取り
(セキュア領域より)
1.カード補足 &フリー領域Read
100
非接触通信カード
フリー領域
URL
セキュア領域
+Name
+Password

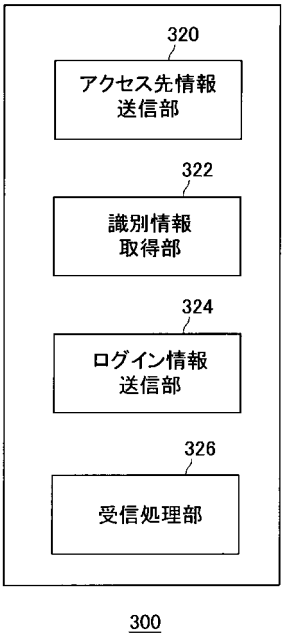
【図８】


SAMサーバ
Webサーバ
PC
カードRW
非接触通信カード
5.1:ログイン
情報取得
S88
S92
S94
S90
5.2:伝送路の暗号化
5.3:ログイン要求
(ログイン情報,セッション番号)
ログイン完了
S95
ログイン完了
S96
6:https.get
(ログイン確認,セッション番号)
S82
3:http.get(起動URL)
4:https.get(セッション要求)
セッション番号
5:https.get(SAM,URL,セッション番号)
S86
S85
S84
2:Webブラウザ起動
S80
1:カード読み込み
S70
起動URL,SAM,URL
S78
S72
1.1:カード補足
S74
1.2:フリー領域読み込み
S76
起動URL,SAM,URL

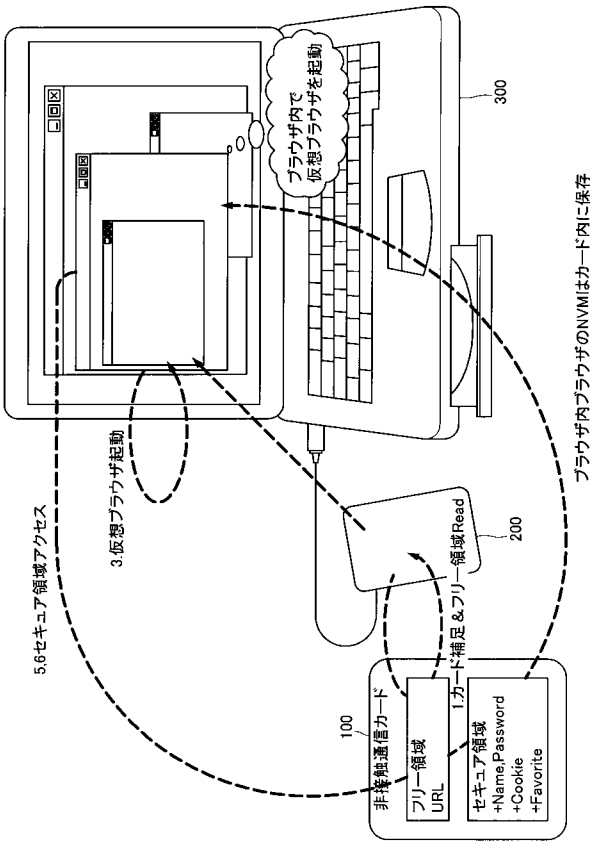
【図９】



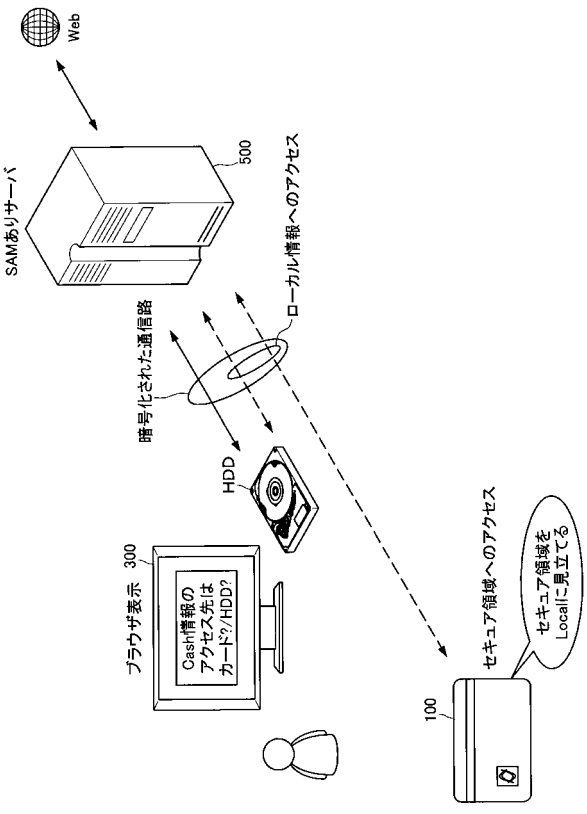
【図１０】



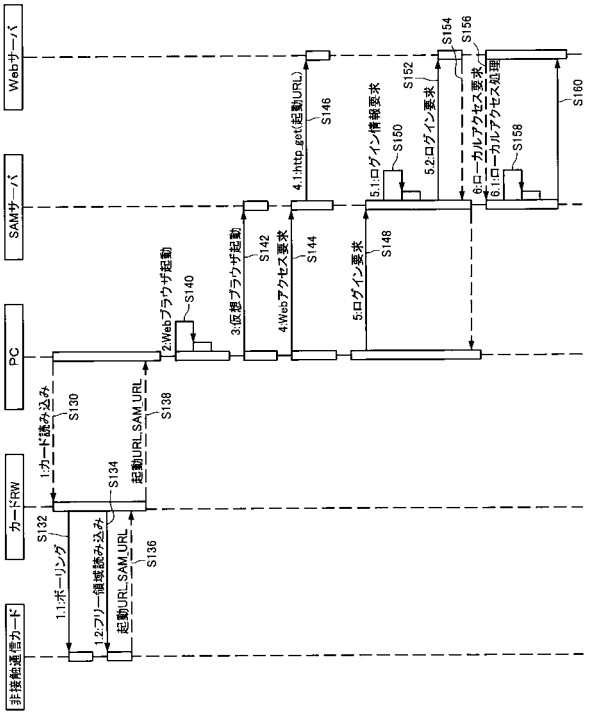
【図１１】



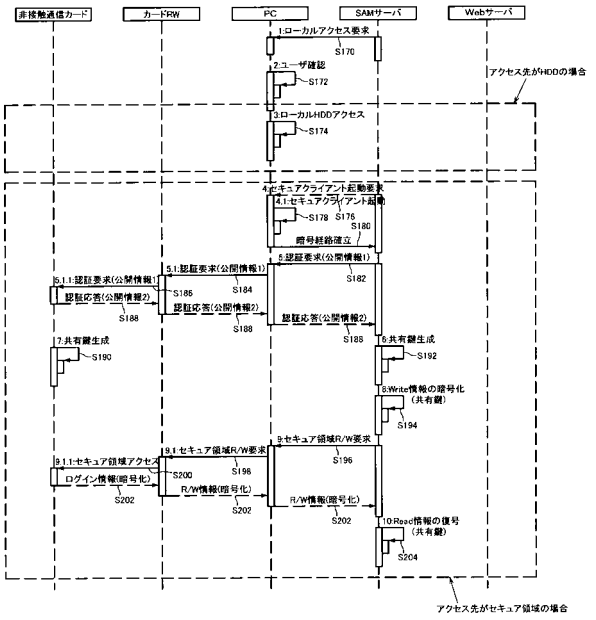
【図１２】



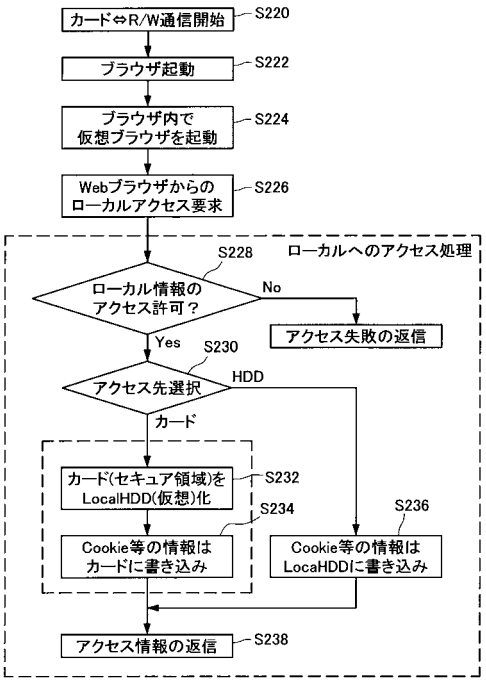
【図１３】



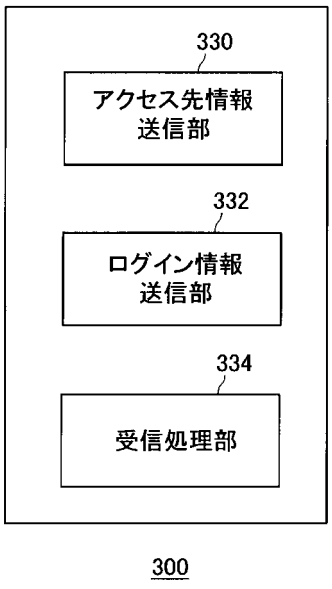
【図１４】



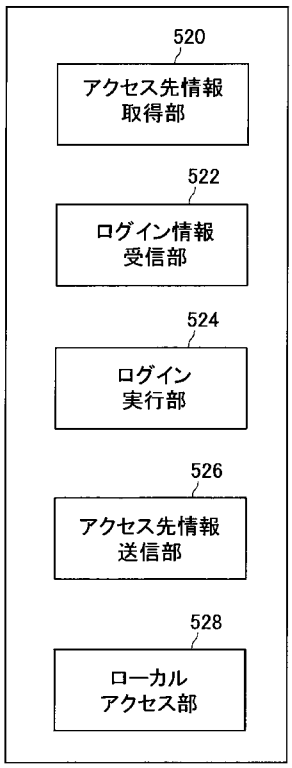
【図１５】



【図１６】



【図１７】


520
アクセス先情報
取得部
522
ログイン情報
受信部
524
ログイン
実行部
526
アクセス先情報
送信部
528
ローカル
アクセス部
500

フロントページの続き

(72)発明者　相馬　功
東京都港区港南１丁目７番１号　ソニー株式会社内
(72)発明者　阿部野　尚
東京都港区港南１丁目７番１号　ソニー株式会社内
(72)発明者　米田　好博
東京都港区港南１丁目７番１号　ソニー株式会社内
(72)発明者　末吉　正弘
東京都港区港南１丁目７番１号　ソニー株式会社内

審査官　平井　誠

(56)参考文献　特開２００８－２２５５７３（ＪＰ，Ａ）
特開２００２－３６６８６８（ＪＰ，Ａ）
特開２００８－２５０９２３（ＪＰ，Ａ）
特開２００９－１１６８００（ＪＰ，Ａ）
特開２００６－１６３５８２（ＪＰ，Ａ）
特開２００２－２４５０１１（ＪＰ，Ａ）
特開２０００－３２２３８３（ＪＰ，Ａ）
国際公開第２００９／００１１９７（WO，Ａ１）
国際公開第２００７／１０７８６８（WO，Ａ１）
欧州特許出願公開第０１５３６３０６（ＥＰ，Ａ１）
英国特許出願公開第０２３９４３２６（ＧＢ，Ａ）
米国特許出願公開第２００８／００７２０６１（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１