(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-234632
(P2004-234632A)
(43)公開日　平成16年8月19日(2004.8.19)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 15/00	G06F 15/00	330G	5B058
G06K 17/00	G06K 17/00	T	5B085
H04L 9/32	H04L 9/00	673A	5J104
	H04L 9/00	673E	

審査請求 有　請求項の数 49　ＯＬ　（全 57 頁）

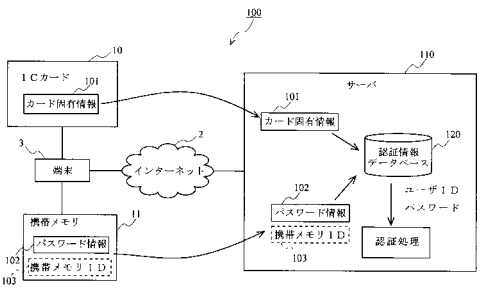
(21)出願番号　特願2003-400367(P2003-400367)
(22)出願日　平成15年11月28日(2003.11.28)
(31)優先権主張番号　特願2003-78(P2003-78)
(32)優先日　平成15年1月6日(2003.1.6)
(33)優先権主張国　日本国(JP)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番３５号
(74)代理人　100096655
弁理士　川井　隆
(74)代理人　100091225
弁理士　仲野　均
(72)発明者　荻野　伸一
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　長谷島　眞時
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】認証システム、認証サーバ、認証方法、認証プログラム、端末、認証要求方法、認証要求プログラム、及び記憶媒体

(57)【要約】
【課題】　２つの記憶媒体を用いてセキュリティと利便性の高い認証システムを提供すること。
【解決手段】　自動ログインシステム１００は、ＩＣカード１０に記憶されているカード固有情報１０１と、携帯メモリ１１に記憶されているパスワード情報１０２を用いてユーザ認証の要求を行い、自動ログインを行うものである。サーバ１１０では、カード固有情報１０１とパスワード情報１０２を用いてユーザＩＤとパスワードを取得し、ユーザ認証を行う。この場合、カード固有情報１０１とパスワード情報１０２が認証要求情報を構成し、ユーザＩＤとパスワードが認証情報を構成している。サーバ１１０は、ユーザ認証が成功した場合、当該ユーザのログイン処理を行い、認証が成功しなかった場合はログイン処理を行わない。
【選択図】　図２０



【特許請求の範囲】
【請求項１】
第１の記憶媒体から前記第１の記憶媒体を識別する第１の識別情報を取得し、第２の記憶媒体から符合情報を取得する端末と、前記端末から前記第１の識別情報、及び前記符合情報を受信して認証処理を行う認証サーバと、から構成された認証システムであって、前記認証サーバで認証処理を行う場合、
前記端末は、前記第１の記憶媒体から前記第１の識別情報を取得し、前記第２の記憶媒体から前記符合情報を取得し、前記取得した第１の識別情報と前記符合情報を前記認証サーバに送信し、
前記認証サーバは、前記端末から前記送信された第１の識別情報と符合情報とを受信し、
前記受信した第１の識別情報と符合情報を用いて認証処理を行うことを特徴とする認証システム。
【請求項２】
第１の記憶媒体から前記第１の記憶媒体を識別する第１の識別情報を取得し、第２の記憶媒体から符合情報を取得する端末から、前記第１の識別情報と前記符合情報を受信して認証を行う認証サーバであって、
前記端末から前記第１の識別情報と前記符合情報を受信する媒体情報受信手段と、
前記受信した第１の識別情報と前記符合情報を用いて認証処理を行う認証手段と、
を具備したことを特徴とする認証サーバ。
【請求項３】
前記第２の記憶媒体は、前記第２の記憶媒体を識別する第２の識別情報を記憶しており、
前記端末から、前記端末が前記第２の記憶媒体から取得した前記第２の識別情報を受信する第２の識別情報受信手段を具備し、
前記認証手段は、前記受信した第２の識別情報と前記符合情報の組合せが、予め登録してある第２の識別情報と符合情報の組合せと一致した場合に認証処理を行うことを特徴とする請求項２に記載の認証サーバ。
【請求項４】
前記認証手段は、前記受信した第１の識別情報が、予め登録してある第１の識別情報と一致した場合に認証処理を行うことを特徴とする請求項２に記載の認証サーバ。
【請求項５】
前記認証手段は、前記受信した第１の識別情報と符合情報の組合せが、予め登録してある第１の識別情報と符合情報の組合せに一致した場合に認証処理を行うことを特徴とする請求項２に記載の認証サーバ。
【請求項６】
前記受信した第１の識別情報から第１の認証情報を検索し、前記受信した符合情報から第２の認証情報を検索する検索手段を具備し、
前記認証手段は、前記検索した第１の認証情報と第２の認証情報を用いて認証処理を行うことを特徴とする請求項２に記載の認証サーバ。
【請求項７】
符合情報を生成して前記端末に送信する符合情報送信手段と、
前記生成した符合情報を、前記第２の識別情報に関連づけて記憶装置に記憶する記憶手段と、
を具備し、
前記検索手段は、前記記憶した符合情報を検索することを特徴とする請求項６に記載の認証サーバ。
【請求項８】
前記符合情報送信手段は、前記端末から受信した符合情報を、前記認証手段で認証処理を行うのに使用した後に新たな符合情報を生成することを特徴とする請求項７に記載の認

証サーバ。
【請求項９】
前記第１の記憶媒体、及び前記第２の記憶媒体のうち少なくとも一方は、ＩＣカード、又は半導体記憶装置により構成された可搬式記憶媒体であることを特徴とする請求項２に記載の認証サーバ。
【請求項１０】
前記端末から新規の第１の識別情報と符合情報を受信し、当該受信した第１の識別情報と前記符合情報に基づいて認証情報を登録する認証情報登録手段を具備し、
前記認証手段は、前記登録した認証情報を用いて認証処理を行うことを特徴とする請求項２に記載の認証サーバ。
【請求項１１】
第１の記憶媒体から前記第１の記憶媒体を識別する第１の識別情報を取得し、第２の記憶媒体から符合情報を取得する端末から、前記第１の識別情報と前記符合情報を受信して認証を行う認証サーバで行う認証方法あって、
前記認証サーバは、媒体情報受信手段と、認証手段と、を具備し、
前記媒体情報受信手段によって、前記端末から前記第１の識別情報と前記符合情報を受信する媒体情報受信ステップと、
前記認証手段によって、前記受信した第１の識別情報と前記符合情報を用いて認証処理を行う認証ステップと、
から構成されたことを特徴とする認証方法。
【請求項１２】
前記第２の記憶媒体は、前記第２の記憶媒体を識別する第２の識別情報を記憶しており、
前記認証サーバは、第２の識別情報受信手段を具備し、
前記第２の識別情報受信手段によって、前記端末から、前記端末が前記第２の記憶媒体から取得した前記第２の識別情報を受信する第２の識別情報受信ステップを有し、
前記認証ステップでは、前記受信した第２の識別情報と前記符合情報の組合せが、予め登録してある第２の識別情報と符合情報の組合せと一致した場合に認証処理を行うことを特徴とする請求項１１に記載の認証方法。
【請求項１３】
前記認証ステップでは、前記受信した第１の識別情報が、予め登録してある第１の識別情報と一致した場合に認証処理を行うことを特徴とする請求項１１に記載の認証方法。
【請求項１４】
前記認証ステップでは、前記受信した第１の識別情報と符合情報の組合せが、予め登録してある第１の識別情報と符合情報の組合せに一致した場合に認証処理を行うことを特徴とする請求項１１に記載の認証方法。
【請求項１５】
前記認証サーバは、検索手段を具備し、
前記検索手段で、前記受信した第１の識別情報から第１の認証情報を検索し、前記受信した符合情報から第２の認証情報を検索する検索ステップを有し、
前記認証ステップでは、前記検索した第１の認証情報と第２の認証情報を用いて認証処理を行うことを特徴とする請求項１１に記載の認証方法。
【請求項１６】
前記認証サーバは、符合情報送信手段と、記憶手段と、を具備し、
前記符合情報送信手段で、符合情報を生成して前記端末に送信する符合情報送信ステップと、
前記記憶手段で、前記生成した符合情報を、前記第２の識別情報に関連づけて記憶装置に記憶する記憶ステップと、
を有し、
前記検索ステップでは、前記記憶した符合情報を検索することを特徴とする請求項１５

に記載の認証方法。
【請求項１７】
前記符合情報送信手段は、前記端末から受信した符合情報を、前記認証手段で認証処理を行うのに使用した後に新たな符合情報を生成することを特徴とする請求項１６に記載の認証方法。
【請求項１８】
前記第１の記憶媒体、及び前記第２の記憶媒体のうち少なくとも一方は、ＩＣカード、又は半導体記憶装置により構成された可搬式記憶媒体であることを特徴とする請求項１１に記載の認証方法。
【請求項１９】
前記認証サーバは、認証情報登録手段を具備し、
前記認証情報登録手段で、前記端末から新規の第１の識別情報と符合情報を受信し、当該受信した第１の識別情報と前記符合情報に基づいて認証情報を登録する認証情報登録ステップを有し、
前記認証ステップでは、前記登録した認証情報を用いて認証処理を行うことを特徴とする請求項１１に記載の認証方法。
【請求項２０】
第１の記憶媒体から前記第１の記憶媒体を識別する第１の識別情報を取得し、第２の記憶媒体から符合情報を取得する端末から、前記第１の識別情報と前記符合情報を受信して認証を行う機能をコンピュータで実現する認証プログラムであって、
前記端末から前記第１の識別情報と前記符合情報を受信する媒体情報受信機能と、
前記受信した第１の識別情報と前記符合情報を用いて認証処理を行う認証機能と、
をコンピュータで実現する認証プログラム。
【請求項２１】
前記第２の記憶媒体は、前記第２の記憶媒体を識別する第２の識別情報を記憶しており、
前記端末から、前記端末が前記第２の記憶媒体から取得した前記第２の識別情報を受信する第２の識別情報受信機能を前記コンピュータで実現し、
前記認証機能は、前記受信した第２の識別情報と前記符合情報の組合せが、予め登録してある第２の識別情報と符合情報の組合せと一致した場合に認証処理を行うことを特徴とする請求項２０に記載の認証プログラム。
【請求項２２】
前記認証機能は、前記受信した第１の識別情報が、予め登録してある第１の識別情報と一致した場合に認証処理を行うことを特徴とする請求項２０に記載の認証プログラム。
【請求項２３】
前記認証機能は、前記受信した第１の識別情報と符合情報の組合せが、予め登録してある第１の識別情報と符合情報の組合せに一致した場合に認証処理を行うことを特徴とする請求項２０に記載の認証プログラム。
【請求項２４】
前記受信した第１の識別情報から第１の認証情報を検索し、前記受信した符合情報から第２の認証情報を検索する検索機能を前記コンピュータで実現し、
前記認証機能は、前記検索した第１の認証情報と第２の認証情報を用いて認証処理を行うことを特徴とする請求項２０に記載の認証プログラム。
【請求項２５】
符合情報を生成して前記端末に送信する符合情報送信機能と、
前記生成した符合情報を、前記第２の識別情報に関連づけて記憶装置に記憶する記憶機能と、
を前記コンピュータで実現し、
前記検索機能は、前記記憶した符合情報を検索することを特徴とする請求項２４に記載の認証プログラム。

【請求項２６】
前記符合情報送信機能は、前記端末から受信した符合情報を、前記認証機能で認証処理を行うのに使用した後に新たな符合情報を生成することを特徴とする請求項２５に記載の認証プログラム。
【請求項２７】
前記第１の記憶媒体、及び前記第２の記憶媒体のうち少なくとも一方は、ＩＣカード、又は半導体記憶装置により構成された可搬式記憶媒体であることを特徴とする請求項２０に記載の認証プログラム。
【請求項２８】
前記端末から新規の第１の識別情報と符合情報を受信し、当該受信した第１の識別情報と前記符合情報に基づいて認証情報を登録する認証情報登録機能を前記コンピュータで実現し、
前記認証機能は、前記登録した認証情報を用いて認証処理を行うことを特徴とする請求項２０に記載の認証プログラム。
【請求項２９】
第１の記憶媒体から前記第１の記憶媒体を識別する第１の識別情報を取得し、第２の記憶媒体から符合情報を取得する端末から、前記第１の識別情報と前記符合情報を受信して認証を行う機能をコンピュータで実現する認証プログラムを記憶したコンピュータが読み取り可能な記憶媒体であって、
前記端末から前記第１の識別情報と前記符合情報を受信する媒体情報受信機能と、
前記受信した第１の識別情報と前記符合情報を用いて認証処理を行う認証機能と、
をコンピュータで実現する認証プログラムを記憶したコンピュータが読み取り可能な記憶媒体。
【請求項３０】
前記第２の記憶媒体は、前記第２の記憶媒体を識別する第２の識別情報を記憶しており、
前記記憶媒体に記憶したコンピュータが読み取り可能な認証プログラムは、前記端末から、前記端末が前記第２の記憶媒体から取得した前記第２の識別情報を受信する第２の識別情報受信機能を前記コンピュータで実現し、
前記認証機能は、前記受信した第２の識別情報と前記符合情報の組合せが、予め登録してある第２の識別情報と符合情報の組合せと一致した場合に認証処理を行うことを特徴とする請求項２９に記載の記憶媒体。
【請求項３１】
前記認証機能は、前記受信した第１の識別情報が、予め登録してある第１の識別情報と一致した場合に認証処理を行うことを特徴とする請求項２９に記載の記憶媒体。
【請求項３２】
前記認証機能は、前記受信した第１の識別情報と符合情報の組合せが、予め登録してある第１の識別情報と符合情報の組合せに一致した場合に認証処理を行うことを特徴とする請求項２９に記載の記憶媒体。
【請求項３３】
前記記憶媒体に記憶したコンピュータが読み取り可能な認証プログラムは、前記受信した第１の識別情報から第１の認証情報を検索し、前記受信した符合情報から第２の認証情報を検索する検索機能を前記コンピュータで実現し、
前記認証機能は、前記検索した第１の認証情報と第２の認証情報を用いて認証処理を行うことを特徴とする請求項２９に記載の記憶媒体。
【請求項３４】
前記記憶媒体に記憶したコンピュータが読み取り可能な認証プログラムは、符合情報を生成して前記端末に送信する符合情報送信機能と、
前記生成した符合情報を、前記第２の識別情報に関連づけて記憶装置に記憶する記憶機能と、

を前記コンピュータで実現し、
前記検索機能は、前記記憶した符合情報を検索することを特徴とする請求項３３に記載の記憶媒体。
【請求項３５】
前記符合情報送信機能は、前記端末から受信した符合情報を、前記認証機能で認証処理を行うのに使用した後に新たな符合情報を生成することを特徴とする請求項３４に記載の記憶媒体。
【請求項３６】
前記第１の記憶媒体、及び前記第２の記憶媒体のうち少なくとも一方は、ＩＣカード、又は半導体記憶装置により構成された可搬式記憶媒体であることを特徴とする請求項２９に記載の記憶媒体。
【請求項３７】
前記記憶媒体に記憶したコンピュータが読み取り可能な認証プログラムは、前記端末から新規の第１の識別情報と符合情報を受信し、当該受信した第１の識別情報と前記符合情報に基づいて認証情報を登録する認証情報登録機能を前記コンピュータで実現し、
前記認証機能は、前記登録した認証情報を用いて認証処理を行うことを特徴とする請求項２９に記載の記憶媒体。
【請求項３８】
請求項２に記載の認証サーバに認証処理の要求を行う端末であって、
第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から符合情報を取得する媒体情報取得手段と、
前記取得した第１の識別情報と符合情報を前記認証サーバに送信する媒体情報送信手段と、
を具備したことを特徴とする端末。
【請求項３９】
請求項３に記載の認証サーバに認証処理を行う端末であって、
第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から当該第２の記憶媒体を識別する第２の識別情報と、符合情報を取得する媒体情報取得手段と、
前記取得した第１の識別情報と第２の識別情報と符合情報を前記認証サーバに送信する媒体情報送信手段と、
を具備したことを特徴とする端末。
【請求項４０】
請求項７に記載の認証サーバに認証処理の要求を行う端末であって、
第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から符合情報を取得する媒体情報取得手段と、
前記取得した第１の識別情報と符合情報を前記認証サーバに送信する媒体情報送信手段と、
前記認証サーバから符合情報を受信する符合情報受信手段と、
前記符合情報受信手段で符合情報を受信した場合に、前記第２の記憶媒体に記憶してある符合情報を前記受信した符合情報で置き換える置き換え手段と、
を具備したことを特徴とする端末。
【請求項４１】
請求項２に記載の認証サーバに認証処理の要求を行う認証要求方法であって、
媒体情報取得手段と、媒体情報送信手段と、を備えたコンピュータにおいて、
前記媒体情報取得手段で、第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から符合情報を取得する媒体情報取得ステップと、
前記媒体情報送信手段で、前記取得した第１の識別情報と符合情報を前記認証サーバに送信する媒体情報送信ステップと、

から構成されたことを特徴とする認証要求方法。
【請求項４２】
請求項３に記載の認証サーバに認証処理の要求を行う認証要求方法であって、
媒体情報取得手段と、媒体情報送信手段と、を備えたコンピュータにおいて、
前記媒体情報取得手段で、第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から当該第２の記憶媒体を識別する第２の識別情報と、符合情報を取得する媒体情報取得ステップと、
前記媒体情報送信手段で、前記取得した第１の識別情報と第２の識別情報と符合情報を前記認証サーバに送信する媒体情報送信ステップと、
から構成されたことを特徴とする認証要求方法。
【請求項４３】
請求項７に記載の認証サーバに認証処理の要求を行う認証要求方法であって、
媒体情報取得手段と、媒体情報送信手段と、符合情報受信手段と、置き換え手段と、を備えたコンピュータにおいて、
前記媒体情報取得手段で、第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から符合情報を取得する情報取得ステップと、
前記媒体情報送信手段で、前記取得した第１の識別情報と符合情報を前記認証サーバに送信する送信ステップと、
前記符合情報受信手段で、前記認証サーバから符合情報を受信する符合情報受信ステップと、
前記置き換え手段において、前記符合情報受信手段で符合情報を受信した場合に、前記第２の記憶媒体に記憶してある符合情報を前記受信した符合情報で置き換える置き換えステップと、
から構成されたことを特徴とする認証要求方法。
【請求項４４】
請求項２に記載の認証サーバに認証処理の要求を行う機能をコンピュータで実現する認証要求プログラムであって、
第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から符合情報を取得する媒体情報取得機能と、
前記取得した第１の識別情報と符合情報を前記認証サーバに送信する媒体情報送信機能と、
をコンピュータで実現する認証要求プログラム。
【請求項４５】
請求項３に記載の認証サーバに認証処理の要求を行う機能をコンピュータで実現する認証要求プログラムであって、
第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から当該第２の記憶媒体を識別する第２の識別情報と、符合情報を取得する媒体情報取得機能と、
前記取得した第１の識別情報と第２の識別情報と符合情報を前記認証サーバに送信する媒体情報送信機能と、
をコンピュータで実現する認証要求プログラム。
【請求項４６】
請求項７に記載の認証サーバに認証処理の要求を行う機能をコンピュータで実現する認証要求プログラムであって、
第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から符合情報を取得する媒体情報取得機能と、
前記取得した第１の識別情報と符合情報を前記認証サーバに送信する媒体情報送信機能と、
前記認証サーバから符合情報を受信する符合情報受信機能と、
前記符合情報受信機能で符合情報を受信した場合に、前記第２の記憶媒体に記憶してあ

る符合情報を前記受信した符合情報で置き換える置き換え機能と、
をコンピュータで実現する認証要求プログラム。
【請求項４７】
請求項２に記載の認証サーバに認証処理の要求を行う機能をコンピュータで実現する認証要求プログラムを記憶したコンピュータが読み取り可能な記憶媒体であって、
第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から符合情報を取得する媒体情報取得機能と、
前記取得した第１の識別情報と符合情報を前記認証サーバに送信する媒体情報送信機能と、
をコンピュータで実現する認証要求プログラムを記憶したコンピュータが読み取り可能な記憶媒体。
【請求項４８】
請求項３に記載の認証サーバに認証処理の要求を行う機能をコンピュータで実現する認証要求プログラムを記憶したコンピュータが読み取り可能な記憶媒体であって、
第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から当該第２の記憶媒体を識別する第２の識別情報と、符合情報を取得する媒体情報取得機能と、
前記取得した第１の識別情報と第２の識別情報と符合情報を前記認証サーバに送信する媒体情報送信機能と、
をコンピュータで実現する認証要求プログラムを記憶したコンピュータが読み取り可能な記憶媒体。
【請求項４９】
請求項７に記載の認証サーバに認証処理の要求を行う機能をコンピュータで実現する認証要求プログラムを記憶したコンピュータが読み取り可能な記憶媒体であって、
第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から符合情報を取得する媒体情報取得機能と、
前記取得した第１の識別情報と符合情報を前記認証サーバに送信する媒体情報送信機能と、
前記認証サーバから符合情報を受信する符合情報受信機能と、
前記符合情報受信機能で符合情報を受信した場合に、前記第２の記憶媒体に記憶してある符合情報を前記受信した符合情報で置き換える置き換え機能と、
をコンピュータで実現する認証要求プログラムを記憶したコンピュータが読み取り可能な記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証システムなどに関し、特に、端末側と認証サーバ側のそれぞれで電子割符を管理し、両者を符合させて認証情報を取得したり、２つの記憶媒体に記憶した認証要求情報を用いて認証要求を行うものなどに関する。
【背景技術】
【０００２】
近年のインターネットの急激な普及により、自宅やオフィスに設置した端末や携帯端末を用いて、インターネット上で提供されているサービスを容易に享受できるようになってきた。
インターネット上で提供されているサービスは、インターネットバンキング、証券取引、オンラインショッピング、情報検索など、多岐に渡っている。
これらサービスを提供するサービスサイトには、パスワードやユーザＩＤなどの認証情報により、ユーザを認証するものがある。
【０００３】
このような認証を要するサイトにログインするためには、ユーザは端末から認証情報を

サーバに送信し、サーバ側で認証用に予め登録してある情報と照合することにより行う。
このため一般に、このようなサイトにログインする場合、ユーザはログイン画面からパスワードやユーザＩＤなどを入力してサーバに送信する。
【０００４】
ところで、パスワードなどによる認証方法は、パスワードが第三者に漏れるなどすると容易になりすましなどを行うことができるため、セキュリティ面で必ずしも十分と言えない場合があった。
そのため、電子割符を用いてユーザを認証する方法も行われている。
電子割符とは、認証情報を所定のロジックに従って複数に分割し（割符化し）、これら分割した全ての電子割符を集めなければ、認証情報を復元できないようにした情報である。
【０００５】
このように、認証情報を２つに割符化して、一方をユーザ側、他方をサーバ側が管理し、認証時にユーザが一方の電子割符をサーバに送信すると、自動ログインサーバは、２つの電子割符を用いて認証情報を復元することができる。
そして、たとえ、ユーザ側の電子割符が第三者に漏れたとしても、この第三者はこの電子割符から認証情報を復元することはできず、そのため、セキュリティの向上を図ることができる。
このような電子割符を用いてセキュリティの向上を図った発明として、例えば、次の技術がある。
【０００６】
【特許文献１】特開２００１－３３１４５０
【０００７】
特許文献１で開示されている技術では、認証情報に基づいてサーバ側で割符を生成し、一方をユーザに渡し、他方をサービスを提供するサービスサイトに渡す。サービスサイトは、ユーザから一方の割符を受け取り、これを既に保持している割符と合成することによってユーザの認証情報を取得し、その認証情報を用いて認証を行う。
【発明の開示】
【発明が解決しようとする課題】
【０００８】
ところが、単に、一方の割符をユーザに渡すだけだと第三者がこの割符を得た場合、これを用いてサーバ認証を受けることが可能となってしまうという問題があった。
そこで、本発明の目的は、ユーザの電子割符が第三者に渡った場合でも、高いセキュリティを実現することができる認証システムや、２つの記憶媒体に記録した情報を用いてユーザ認証を行う認証システムなどを提供することである。
【課題を解決するための手段】
【０００９】
本発明は、前記目的を達成するために、第１の記憶媒体から前記第１の記憶媒体を識別する第１の識別情報を取得し、第２の記憶媒体から符合情報を取得する端末と、前記端末から前記第１の識別情報、及び前記符合情報を受信して認証処理を行う認証サーバと、から構成された認証システムであって、前記認証サーバで認証処理を行う場合、前記端末は、前記第１の記憶媒体から前記第１の識別情報を取得し、前記第２の記憶媒体から前記符合情報を取得し、前記取得した第１の識別情報と前記符合情報を前記認証サーバに送信し、前記認証サーバは、前記端末から前記送信された第１の識別情報と符合情報とを受信し、前記受信した第１の識別情報と符合情報を用いて認証処理を行うことを特徴とする認証システムを提供する（第１の構成）。
また、本発明は、第１の記憶媒体から前記第１の記憶媒体を識別する第１の識別情報を取得し、第２の記憶媒体から符合情報を取得する端末から、前記第１の識別情報と前記符合情報を受信して認証を行う認証サーバであって、前記端末から前記第１の識別情報と前記符合情報を受信する媒体情報受信手段と、前記受信した第１の識別情報と前記符合情報

を用いて認証処理を行う認証手段と、を具備したことを特徴とする認証サーバを提供する（第２の構成）。

第２の構成において、前記第２の記憶媒体は、前記第２の記憶媒体を識別する第２の識別情報を記憶しており、前記端末から、前記端末が前記第２の記憶媒体から取得した前記第２の識別情報を受信する第２の識別情報受信手段を具備し、前記認証手段は、前記受信した第２の識別情報と前記符合情報の組合せが、予め登録してある第２の識別情報と符合情報の組合せと一致した場合に認証処理を行うように構成することもできる（第３の構成）。

第２の構成において、前記認証手段は、前記受信した第１の識別情報が、予め登録してある第１の識別情報と一致した場合に認証処理を行うように構成することもできる（第４の構成）。

第２の構成において、前記認証手段は、前記受信した第１の識別情報と符合情報の組合せが、予め登録してある第１の識別情報と符合情報の組合せに一致した場合に認証処理を行うように構成することもできる（第５の構成）。

第２の構成において、前記受信した第１の識別情報から第１の認証情報を検索し、前記受信した符合情報から第２の認証情報を検索する検索手段を具備し、前記認証手段は、前記検索した第１の認証情報と第２の認証情報を用いて認証処理を行うように構成することもできる（第６の構成）。

第６の構成において、符合情報を生成して前記端末に送信する符合情報送信手段と、前記生成した符合情報を、前記第２の識別情報に関連づけて記憶装置に記憶する記憶手段と、を具備し、前記検索手段は、前記記憶した符合情報を検索するように構成することもできる（第７の構成）。

第７の構成において、前記符合情報送信手段は、前記端末から受信した符合情報を、前記認証手段で認証処理を行うのに使用した後に新たな符合情報を生成するように構成することもできる（第８の構成）。

第２の構成において、前記第１の記憶媒体、及び前記第２の記憶媒体のうち少なくとも一方は、ＩＣカード、又は半導体記憶装置により構成された可搬式記憶媒体であるように構成することもできる（第９の構成）。

第２の構成において、前記端末から新規の第１の識別情報と符合情報を受信し、当該受信した第１の識別情報と前記符合情報に基づいて認証情報を登録する認証情報登録手段を具備し、前記認証手段は、前記登録した認証情報を用いて認証処理を行うように構成することもできる（第１０の構成）。

また、本発明は、前記目的を達成するために、第１の記憶媒体から前記第１の記憶媒体を識別する第１の識別情報を取得し、第２の記憶媒体から符合情報を取得する端末から、前記第１の識別情報と前記符合情報を受信して認証を行う認証サーバで行う認証方法あって、前記認証サーバは、媒体情報受信手段と、認証手段と、を具備し、前記媒体情報受信手段によって、前記端末から前記第１の識別情報と前記符合情報を受信する媒体情報受信ステップと、前記認証手段によって、前記受信した第１の識別情報と前記符合情報を用いて認証処理を行う認証ステップと、から構成されたことを特徴とする認証方法を提供する（第１１の構成）。

第１１の構成において、前記第２の記憶媒体は、前記第２の記憶媒体を識別する第２の識別情報を記憶しており、前記認証サーバは、第２の識別情報受信手段を具備し、前記第２の識別情報受信手段によって、前記端末から、前記端末が前記第２の記憶媒体から取得した前記第２の識別情報を受信する第２の識別情報受信ステップを有し、前記認証ステップでは、前記受信した第２の識別情報と前記符合情報の組合せが、予め登録してある第２の識別情報と符合情報の組合せと一致した場合に認証処理を行うように構成することもできる（第１２の構成）。

第１１の構成において、前記認証ステップでは、前記受信した第１の識別情報が、予め登録してある第１の識別情報と一致した場合に認証処理を行うように構成することもできる（第１３の構成）。

第１１の構成において、前記認証ステップでは、前記受信した第１の識別情報と符合情報の組合せが、予め登録してある第１の識別情報と符合情報の組合せに一致した場合に認証処理を行うように構成することもできる（第１４の構成）。

第１１の構成において、前記認証サーバは、検索手段を具備し、前記検索手段で、前記受信した第１の識別情報から第１の認証情報を検索し、前記受信した符合情報から第２の認証情報を検索する検索ステップを有し、前記認証ステップでは、前記検索した第１の認証情報と第２の認証情報を用いて認証処理を行うように構成することもできる（第１５の構成）。

第１５の構成において、前記認証サーバは、符合情報送信手段と、記憶手段と、を具備し、前記符合情報送信手段で、符合情報を生成して前記端末に送信する符合情報送信ステップと、前記記憶手段で、前記生成した符合情報を、前記第２の識別情報に関連づけて記憶装置に記憶する記憶ステップと、を有し、前記検索ステップでは、前記記憶した符合情報を検索するように構成することもできる（第１６の構成）。

第１６の構成において、前記符合情報送信手段は、前記端末から受信した符合情報を、前記認証手段で認証処理を行うのに使用した後に新たな符合情報を生成するように構成することもできる（第１７の構成）。

第１１の構成において、前記第１の記憶媒体、及び前記第２の記憶媒体のうち少なくとも一方は、ＩＣカード、又は半導体記憶装置により構成された可搬式記憶媒体であるように構成することもできる（第１８の構成）。

第１１の構成において、前記認証サーバは、認証情報登録手段を具備し、前記認証情報登録手段で、前記端末から新規の第１の識別情報と符合情報を受信し、当該受信した第１の識別情報と前記符合情報に基づいて認証情報を登録する認証情報登録ステップを有し、前記認証ステップでは、前記登録した認証情報を用いて認証処理を行うように構成することもできる（第１９の構成）。

また、本発明は、第１の記憶媒体から前記第１の記憶媒体を識別する第１の識別情報を取得し、第２の記憶媒体から符合情報を取得する端末から、前記第１の識別情報と前記符合情報を受信して認証を行う機能をコンピュータで実現する認証プログラムであって、前記端末から前記第１の識別情報と前記符合情報を受信する媒体情報受信機能と、前記受信した第１の識別情報と前記符合情報を用いて認証処理を行う認証機能と、をコンピュータで実現する認証プログラムを提供する（第２０の構成）。

第２０の構成において、前記第２の記憶媒体は、前記第２の記憶媒体を識別する第２の識別情報を記憶しており、前記端末から、前記端末が前記第２の記憶媒体から取得した前記第２の識別情報を受信する第２の識別情報受信機能を前記コンピュータで実現し、前記認証機能は、前記受信した第２の識別情報と前記符合情報の組合せが、予め登録してある第２の識別情報と符合情報の組合せと一致した場合に認証処理を行うように構成することもできる（第２１の構成）。

第２０の構成において、前記認証機能は、前記受信した第１の識別情報が、予め登録してある第１の識別情報と一致した場合に認証処理を行うように構成することもできる（第２２の構成）。

第２０の構成において、前記認証機能は、前記受信した第１の識別情報と符合情報の組合せが、予め登録してある第１の識別情報と符合情報の組合せに一致した場合に認証処理を行うように構成することもできる（第２３の構成）。

第２０の構成において、前記受信した第１の識別情報から第１の認証情報を検索し、前記受信した符合情報から第２の認証情報を検索する検索機能を前記コンピュータで実現し、前記認証機能は、前記検索した第１の認証情報と第２の認証情報を用いて認証処理を行うように構成することもできる（第２４の構成）。

第２４の構成において、符合情報を生成して前記端末に送信する符合情報送信機能と、前記生成した符合情報を、前記第２の識別情報に関連づけて記憶装置に記憶する記憶機能と、を前記コンピュータで実現し、前記検索機能は、前記記憶した符合情報を検索するように構成することもできる（第２５の構成）。

第２５の構成において、前記符合情報送信機能は、前記端末から受信した符合情報を、前記認証機能で認証処理を行うのに使用した後に新たな符合情報を生成するように構成することもできる（第２６の構成）。

第２０の構成において、前記第１の記憶媒体、及び前記第２の記憶媒体のうち少なくとも一方は、ＩＣカード、又は半導体記憶装置により構成された可搬式記憶媒体であるように構成することもできる（第２７の構成）。

第２０の構成において、前記端末から新規の第１の識別情報と符合情報を受信し、当該受信した第１の識別情報と前記符合情報に基づいて認証情報を登録する認証情報登録機能を前記コンピュータで実現し、前記認証機能は、前記登録した認証情報を用いて認証処理を行うように構成することもできる（第２８の構成）。

また、本発明は、第１の記憶媒体から前記第１の記憶媒体を識別する第１の識別情報を取得し、第２の記憶媒体から符合情報を取得する端末から、前記第１の識別情報と前記符合情報を受信して認証を行う機能をコンピュータで実現する認証プログラムを記憶したコンピュータが読み取り可能な記憶媒体であって、前記端末から前記第１の識別情報と前記符合情報を受信する媒体情報受信機能と、前記受信した第１の識別情報と前記符合情報を用いて認証処理を行う認証機能と、をコンピュータで実現する認証プログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する（第２９の構成）。

第２９の構成において、前記第２の記憶媒体は、前記第２の記憶媒体を識別する第２の識別情報を記憶しており、前記記憶媒体に記憶したコンピュータが読み取り可能な認証プログラムは、前記端末から、前記端末が前記第２の記憶媒体から取得した前記第２の識別情報を受信する第２の識別情報受信機能を前記コンピュータで実現し、前記認証機能は、前記受信した第２の識別情報と前記符合情報の組合せが、予め登録してある第２の識別情報と符合情報の組合せと一致した場合に認証処理を行うように構成することもできる（第３０の構成）。

第２９の構成において、前記認証機能は、前記受信した第１の識別情報が、予め登録してある第１の識別情報と一致した場合に認証処理を行うように構成することもできる（第３１の構成）。

第２９の構成において、前記認証機能は、前記受信した第１の識別情報と符合情報の組合せが、予め登録してある第１の識別情報と符合情報の組合せに一致した場合に認証処理を行うように構成することもできる（第３２の構成）。

第２９の構成において、前記記憶媒体に記憶したコンピュータが読み取り可能な認証プログラムは、前記受信した第１の識別情報から第１の認証情報を検索し、前記受信した符合情報から第２の認証情報を検索する検索機能を前記コンピュータで実現し、前記認証機能は、前記検索した第１の認証情報と第２の認証情報を用いて認証処理を行うように構成することもできる（第３３の構成）。

第３３の構成において、前記記憶媒体に記憶したコンピュータが読み取り可能な認証プログラムは、符合情報を生成して前記端末に送信する符合情報送信機能と、前記生成した符合情報を、前記第２の識別情報に関連づけて記憶装置に記憶する記憶機能と、を前記コンピュータで実現し、前記検索機能は、前記記憶した符合情報を検索するように構成することもできる（第３４の構成）。

第３４の構成において、前記符合情報送信機能は、前記端末から受信した符合情報を、前記認証機能で認証処理を行うのに使用した後に新たな符合情報を生成するように構成することもできる（第３５の構成）。

第２９の構成において、前記第１の記憶媒体、及び前記第２の記憶媒体のうち少なくとも一方は、ＩＣカード、又は半導体記憶装置により構成された可搬式記憶媒体であるように構成することもできる（第３６の構成）。

第２９の構成において、前記記憶媒体に記憶したコンピュータが読み取り可能な認証プログラムは、前記端末から新規の第１の識別情報と符合情報を受信し、当該受信した第１の識別情報と前記符合情報に基づいて認証情報を登録する認証情報登録機能を前記コンピュータで実現し、前記認証機能は、前記登録した認証情報を用いて認証処理を行うように

構成することもできる（第３７の構成）。

また、本発明は、請求項２に記載の認証サーバに認証処理の要求を行う端末であって、第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から符合情報を取得する媒体情報取得手段と、前記取得した第１の識別情報と符合情報を前記認証サーバに送信する媒体情報送信手段と、を具備したことを特徴とする端末を提供する（第３８の構成）。

また、本発明は、請求項３に記載の認証サーバに認証処理を行う端末であって、第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から当該第２の記憶媒体を識別する第２の識別情報と、符合情報を取得する媒体情報取得手段と、前記取得した第１の識別情報と第２の識別情報と符合情報を前記認証サーバに送信する媒体情報送信手段と、を具備したことを特徴とする端末を提供する（第３９の構成）。

また、本発明は、請求項７に記載の認証サーバに認証処理の要求を行う端末であって、第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から符合情報を取得する媒体情報取得手段と、前記取得した第１の識別情報と符合情報を前記認証サーバに送信する媒体情報送信手段と、前記認証サーバから符合情報を受信する符合情報受信手段と、前記符合情報受信手段で符合情報を受信した場合に、前記第２の記憶媒体に記憶してある符合情報を前記受信した符合情報で置き換える置き換え手段と、を具備したことを特徴とする端末を提供する（第４０の構成）。

また、本発明は、請求項２に記載の認証サーバに認証処理の要求を行う認証要求方法であって、媒体情報取得手段と、媒体情報送信手段と、を備えたコンピュータにおいて、前記媒体情報取得手段で、第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から符合情報を取得する媒体情報取得ステップと、前記媒体情報送信手段で、前記取得した第１の識別情報と符合情報を前記認証サーバに送信する媒体情報送信ステップと、から構成されたことを特徴とする認証要求方法を提供する（第４１の構成）。

また、本発明は、請求項３に記載の認証サーバに認証処理の要求を行う認証要求方法であって、媒体情報取得手段と、媒体情報送信手段と、を備えたコンピュータにおいて、前記媒体情報取得手段で、第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から当該第２の記憶媒体を識別する第２の識別情報と、符合情報を取得する媒体情報取得ステップと、前記媒体情報送信手段で、前記取得した第１の識別情報と第２の識別情報と符合情報を前記認証サーバに送信する媒体情報送信ステップと、から構成されたことを特徴とする認証要求方法を提供する（第４２の構成）。

また、本発明は、請求項７に記載の認証サーバに認証処理の要求を行う認証要求方法であって、媒体情報取得手段と、媒体情報送信手段と、符合情報受信手段と、置き換え手段と、を備えたコンピュータにおいて、前記媒体情報取得手段で、第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から符合情報を取得する情報取得ステップと、前記媒体情報送信手段で、前記取得した第１の識別情報と符合情報を前記認証サーバに送信する送信ステップと、前記符合情報受信手段で、前記認証サーバから符合情報を受信する符合情報受信ステップと、前記置き換え手段において、前記符合情報受信手段で符合情報を受信した場合に、前記第２の記憶媒体に記憶してある符合情報を前記受信した符合情報で置き換える置き換えステップと、から構成されたことを特徴とする認証要求方法を提供する（第４３の構成）。

また、本発明は、請求項２に記載の認証サーバに認証処理の要求を行う機能をコンピュータで実現する認証要求プログラムであって、第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から符合情報を取得する媒体情報取得機能と、前記取得した第１の識別情報と符合情報を前記認証サーバに送信する媒体情報送信機能と、をコンピュータで実現する認証要求プログラムを提供する（第４４の構成）。

また、本発明は、請求項３に記載の認証サーバに認証処理の要求を行う機能をコンピュ

ータで実現する認証要求プログラムであって、第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から当該第２の記憶媒体を識別する第２の識別情報と、符合情報を取得する媒体情報取得機能と、前記取得した第１の識別情報と第２の識別情報と符合情報を前記認証サーバに送信する媒体情報送信機能と、をコンピュータで実現する認証要求プログラムを提供する（第４５の構成）。

また、本発明は、請求項７に記載の認証サーバに認証処理の要求を行う機能をコンピュータで実現する認証要求プログラムであって、第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から符合情報を取得する媒体情報取得機能と、前記取得した第１の識別情報と符合情報を前記認証サーバに送信する媒体情報送信機能と、前記認証サーバから符合情報を受信する符合情報受信機能と、前記符合情報受信機能で符合情報を受信した場合に、前記第２の記憶媒体に記憶してある符合情報を前記受信した符合情報で置き換える置き換え機能と、をコンピュータで実現する認証要求プログラムを提供する（第４６の構成）。

また、本発明は、請求項２に記載の認証サーバに認証処理の要求を行う機能をコンピュータで実現する認証要求プログラムを記憶したコンピュータが読み取り可能な記憶媒体であって、第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から符合情報を取得する媒体情報取得機能と、前記取得した第１の識別情報と符合情報を前記認証サーバに送信する媒体情報送信機能と、をコンピュータで実現する認証要求プログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する（第４７の構成）。

また、本発明は、請求項３に記載の認証サーバに認証処理の要求を行う機能をコンピュータで実現する認証要求プログラムを記憶したコンピュータが読み取り可能な記憶媒体であって、第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から当該第２の記憶媒体を識別する第２の識別情報と、符合情報を取得する媒体情報取得機能と、前記取得した第１の識別情報と第２の識別情報と符合情報を前記認証サーバに送信する媒体情報送信機能と、をコンピュータで実現する認証要求プログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する（第４８の構成）。

また、本発明は、請求項７に記載の認証サーバに認証処理の要求を行う機能をコンピュータで実現する認証要求プログラムを記憶したコンピュータが読み取り可能な記憶媒体であって、第１の記憶媒体から当該第１の記憶媒体を識別する第１の識別情報を取得し、更に、第２の記憶媒体から符合情報を取得する媒体情報取得機能と、前記取得した第１の識別情報と符合情報を前記認証サーバに送信する媒体情報送信機能と、前記認証サーバから符合情報を受信する符合情報受信機能と、前記符合情報受信機能で符合情報を受信した場合に、前記第２の記憶媒体に記憶してある符合情報を前記受信した符合情報で置き換える置き換え機能と、をコンピュータで実現する認証要求プログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する（第４９の構成）。

【発明の効果】

【００１０】

本発明によれば、電子割符を用いたセキュリティと利便性の高い認証システムや複数の記憶媒体を用いた認証システムを提供することができる。

【発明を実施するための最良の形態】

【００１１】

以下、本発明の好適な実施の形態について、図を参照しながら詳細に説明する。

（１）実施形態の概要

本実施の形態では、パスワードなどの認証に利用する認証情報を含む元データをユーザ割符とサーバ割符の２つの電子割符に分割し、ユーザ割符はユーザ側で管理し、サーバ割符はサーバ側で管理する。

ユーザは、ログインする際に、ユーザ割符をサーバに送信すると共に、サーバ割符とひも付けされたカード固有情報（非接触ＩＣカードから読み取る）をサーバに送信する。

サーバは、カード固有情報を用いてユーザ割符の相手であるサーバ割符を検索し、検索

されたサーバ割符とユーザ割符を用いて元データを復元する。そして、復元された元データを用いてユーザを認証する。

従来の電子割符では、相手方の割符を特定する情報を記憶する識別領域が設けられており、単体の電子割符から相手方の電子割符を特定することができたが、本実施の形態では、以上のように、ユーザ割符と、ユーザ割符の相手方を特定する情報であるサーバ割符特定情報が分離しており、別々にサーバに送信しなければならないため、ユーザ割符が第三者に渡ったとしても、第三者はユーザ割符だけでは認証を受けることができない。

【００１２】

図１は、本実施の形態に係る自動ログインシステムの概要を説明するための概念図である。

ユーザ割符は、可搬式の外部記憶媒体である携帯メモリ１１に格納されており、カード固有情報は、非接触型のＩＣカード１０に格納されている。

本実施の形態では、サーバ５において、カード固有情報とサーバ割符がひも付けされている。

ユーザは、端末３からサーバ５に開設されたサービスサイトにログインする場合、携帯メモリ１１とＩＣカード１０を端末３にセットする。

端末３は、ＩＣカード１０からカード固有情報を読み取り、更に携帯メモリ１１からユーザ割符１１１を読み取り、これらをインターネット２を介してサーバ５に送信する。

【００１３】

サーバ５では、検索部３２がカード固有情報を用いてひも付けされているサーバ割符を検索する。

そして、復元部３３が、検索されたサーバ割符１１５と端末３から受信したユーザ割符１１１を用いて元データを復元する。

認証部３５が、元データに含まれるパスワードと、このパスワードにひも付けされているユーザＩＤ１１９を用いてユーザの認証を行い、ログイン処理を行う。

以上のように、本実施の形態では、非接触型のＩＣカード１０のカード固有情報と、パスワードを用いて単体では無意味なデータである電子割符（ユーザ割符１１１、サーバ割符１１５）を分割して生成し、サーバ割符をサーバ５に記憶させ、ユーザ割符を可搬式の外部記憶媒体である携帯メモリ１１に登録して保有する。

そして、認証時に、ＩＣカード１０のカード固有情報を用いて、サーバ割符１１５とユーザ割符１１１をマッチングし、パスワードを復元することができる。

【００１４】

（２）実施形態の詳細

本実施の形態では、ユーザを認証する際に、「割符」と呼ばれる技術を用いて生成した電子割符を利用する。

割符技術は、保護したい元データをあるロジックを用いて単体では無意味な複数の電子割符（割符情報）に分割し、単体では元データを復元できなくするものである。

まず図２を用いて、割符技術の概念を説明する。

保護対象である元データ１３０があったとする。これを所定のロジックで変換し、複数の電子割符に分割する。ここでは、割符Ａと割符Ｂの２つに分割するものとする。

割符Ａ、Ｂは、それぞれ単体では無意味なデータとなっており、元データを復元するためには、相手方の電子割符を必要とする。一方の電子割符から元データや他方の電子割符を類推することはできない。また、仮に割符Ａ、Ｂの双方を手に入れたとしても、単に割符Ａ、Ｂを合わせただけでは元データを復元できないようになっており、元データを復元するには復元化という先のロジックによる変換の逆変換を行う必要がある。

そこで、図２に示したように、割符Ａ、Ｂの双方を組み合わせて復元化を行うと元データ１３０ａが得られる。元データ１３０と元データ１３０ａは、同じものである。

【００１５】

このように元データを復元するには、割符化された電子割符を全て集めて復元化することが必要である。

そこで、電子割符を生成して別々に管理することにより、高いセキュリティを実現することができる。

なお、全ての電子割符を集めずに、一部の電子割符を集めて元データの一部を復元できるように構成する場合もある。

本実施の形態では、元データとしてユーザの認証に使用するパスワードと、非接触ＩＤカードに固有なカード固有情報を採用する。なお、元データとしてパスワードだけを割符化しても自動ログインシステム１を構成することができるが、業務上の便宜を図るため、カード固有情報もパスワード共に割符化することにした。

【００１６】

図３は、本実施の形態に係る自動ログインシステム１のネットワーク構成の一例を示した図である。

自動ログインシステム１は、サービスサイトが開設されたサーバ５、サービスサイトを利用する端末３、及び端末３とサーバ５をネットワーク接続するためのインターネット２を備えている。

端末３は、例えば、ブラウザを備えたパーソナルコンピュータにより構成され、ユーザは、端末３からサーバ５に開設されたサービスサイト１７をインターネット２を介して利用することができる。

なお、図３では、説明を簡単にするために端末３を一台だけ示しているが、複数の端末３をインターネット２を介して接続可能に配設することができる。

【００１７】

端末３は、周辺機器としてリーダライタ７を備えており、非接触にてＩＣカード１０に対してデータの読み書きを行うことができる。

ＩＣカード１０（第１の可搬式記憶媒体、第１の記憶媒体）は、可搬式の記憶媒体であって、発電及び信号の送受信を行うアンテナと、データやプログラムを格納する記憶部や演算を行う演算部を備えた半導体チップが内蔵されている。そして、ＩＣカード１０をリーダライタ７に接近させると、リーダライタ７が放射している電波によりＩＣカード１０で発電が行われ、半導体チップを駆動するための電力が供給される。

そして、半導体チップを駆動しながら、リーダライタ７とＩＣカード１０の間で電波によりデータを送受信することができる。

これにより、端末３のＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）は、ＩＣカード１０中の半導体チップに対してデータの読み出しや書き込みを行うことができる。

なお、本実施の形態では、ＩＣカード１０を非接触型ＩＣカードとしたが、これを、接触型ＩＣカードや接触型磁気カードとすることもできる。

接触型ＩＣカードは、リーダライタの電極をＩＣカードの接点に接触させ、接触型ＩＣカード内のＩＣチップにたいしてデータの読み書きを行う。

接触型磁気カードは、磁気部にリーダライタの磁気ヘッドを接触させてデータの読み書きを行う。

ところで、ＩＣカード１０として非接触型のＩＣカードを採用した場合、リーダライタ７にかざすだけでデータの読み書きができるので、挿入機構が必要なく、使い勝手がよい。また、機械的な機構や接触部を必要としないので、コストが低減できる他、接点の摩滅や故障によるトラブルを低減することができる。

更に、記憶媒体として非接触型または接触型ＩＣカードを用いると、ユーザは財布やポケットなどに収納することができ、携行性がよい他、磁気カードのように磁気データが劣化する心配がないという利点もある。

【００１８】

ＩＣカード１０に形成されている論理的な構成を図４に示す。

図示しないが、ＩＣカード１０の半導体チップは、内部構成を論理的に分割することにより、複数のアプリケーションソフトで使用することができるようになっている。

本実施の形態では、ＩＣカード１０には、電子マネー用の論理的な領域が形成されてお

り、電子マネーによる決済手段として利用できるようになっている。
電子マネーとは、バリューと呼ばれる交換価値をチャージャと呼ばれる装置によりＩＣカード１０に記憶し、支払いの際に、代金に相当するバリューをＩＣカード１０から差し引くものである。
このように、ＩＣカード１０を電子マネーとして利用すると、プリペイド方式で決済することができる。
なお、ＩＣカード１０が電子マネー機能を有することは、自動ログインに必要な要素ではなく、本実施の形態の自動ログインシステムがアプリケーションと関連させて利用できる例を単に示すためのものである。
また、自動ログインに限らず上記の処理によって得られた認証情報に基づいて、認証を行なった後に、電子マネー機能を利用可能としたり、可搬式記録媒体に格納される情報へのアクセスを可能としたりしても良い。

【００１９】
ＩＣカード１０には、固有のＩＤであるカードＩＤ２５がメモリに改変不能に記憶してある（図４）。カードＩＤ２５は、ＩＣカード１０の表面には表示しておらず（視覚的にわからないようにしてある）、ユーザが容易にわからないように秘匿した状態となったいわゆる密番である。端末３は、リーダライタ７を用いてカードＩＤ２５を読み取ることができる。
ＩＣカード１０には、電子マネーとして利用するための領域２６ａが確保されている。そして、ＩＣカード１０は、電子マネーサービスを受けるための固有の電子マネーＩＤを改変不能に記憶している。

【００２０】
電子マネーＩＤは、ＩＣカード１０の表面に印刷されており、ユーザは、この印刷された電子マネーＩＤを用いて電子マネー事業者に対する問い合わせなどを行えるようになっている。
以下では、ＩＣカード１０に固有なカード固有情報としてカードＩＤ２５と電子マネーＩＤ２６の組み合わせを採用することとする。そして、サーバ５では、カードＩＤ２５と電子マネーＩＤ２６の組み合わせに対してサーバ割符（第１の符合情報）をひも付けすることとし、カード固有情報をサーバ割符を特定するための特定情報として利用する。

【００２１】
なお、本実施の形態では、特定情報としてカード固有情報を用いたが、これは特定情報をカード固有情報に限定するものではなく、サーバ割符とひも付けされた情報であれば他の情報を用いることもできる。例えば、サーバ割符とひも付けされたパスワードやパスフレーズやユーザＩＤなどのユーザ識別情報をＩＣカード１０に記憶し、これを特定情報として利用することもできる。
更に、本実施の形態では、カード固有情報としてカードＩＤ２５と電子マネーＩＤ２６の組み合わせを用いるが、これはカード固有情報の内容を限定するものではない。カード固有情報としては、この他に、カードＩＤ２５単体、電子マネーＩＤ２６単体を用いることもできるし、ＩＣカード１０を利用する他のアプリケーションで使用する固有の情報でもよい。
カード固有情報として電子マネーＩＤ２６を用いると、電子マネーＩＤ２６はＩＣカード１０表面に識別可能に表示してあるため、ユーザからの問い合わせなどに対応する際に便利である。
また、カード固有情報に限らず、カードを所有する個人に固有の個人固有情報をサーバ割符を検索するためのトリガーとしても良い。

【００２２】
図３に戻り、端末３は、携帯メモリ１１に対してデータの読み書きを行う携帯メモリ駆動装置８を備えている。
携帯メモリ駆動装置８は、携帯メモリ１１が着脱可能に構成されており、端末３のＣＰＵは、携帯メモリ駆動装置８に装着された携帯メモリ１１に対してデータの読み書きを行

うことができる。

【００２３】

携帯メモリ１１（第２の可搬式記憶媒体、第２の記憶媒体）は、例えば、読み書き可能なメモリを用いたメモリーカードなど、端末３に着脱可能な不揮発性の可搬式記憶媒体である。

携帯メモリ１１には、固有の携帯メモリ固有情報（携帯メモリＩＤ）が付与されており、端末３は、この携帯メモリ固有情報を読むことはできるが、書き換えることはできないようになっている。

本実施の形態では、認証に用いる元データを割符化したユーザ割符（第２の符合情報）を携帯メモリ１１に格納し、認証時に端末３がユーザ割符を携帯メモリ１１から読み出すようにする。

【００２４】

なお、本実施の形態では、携帯メモリ１１に格納されているユーザ割符を他の携帯メモリ１１にコピーしても利用できないようになっている。

このようにするためには、例えば、携帯メモリ固有情報を復号化鍵としてユーザ割符を暗号化し、他の携帯メモリ固有情報では復号化できないようにしたり、あるいは認証時にユーザ割符と共に携帯メモリ固有情報をサーバ５に送信して、両者が対応するユーザ割符と携帯メモリ固有情報であるかを確認することにより行うことができる。

あるいは、後述するように、携帯メモリ固有情報も元データとして割符化することにより、ユーザ割符を他の携帯メモリ１１にコピーした場合に使用不可となるように構成することもできる。

【００２５】

端末３は、ブラウザを用いて、インターネット２に接続したサーバにアクセスし、これらのサーバに開設されたサービスサイトによるサービスを受けることができる。

ブラウザは、サービスサイトからＨＴＭＬ（Ｈｙｐｅｒｔｅｘｔ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）ファイルやＸＭＬ（Ｅｘｔｅｎｓｉｂｌｅ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）ファイルなどをダウンロードし、これらのファイルに従って画像や音声を再生する他、ユーザが入力した情報（認証に利用するパスワード、アンケートの入力事項など）をサービスサイト側に送信することができる。

【００２６】

そして、端末３のブラウザは、これらのブラウザとしての通常の機能の他に、動作拡張のための補助プログラムをインストールすることができる。

本実施の形態では、端末３で自動ログイン機能を実現するために、サーバ５から後述する補助プログラムをダウンロードし、端末３にインストールする。

この自動ログイン機能により、例えば、ユーザがログイン画面でログインボタンをクリックした場合に、ＩＣカード１０からカード固有情報を読み取ってサーバ５に送信し、更に携帯メモリ１１からユーザ割符を読み取ってサーバ５に送信するなどの機能を発揮することができる。

本実施の形態では、サーバ５から補助プログラムをダウンロードして端末３にインストールするように構成したが、これに限定せず、ユーザがブラウザを購入した際に、予め自動ログイン機能が組み込まれているように構成してもよい。

【００２７】

サーバ５は、予め登録してあるユーザに対してサービスを提供するサーバである。

提供するサービスの種類としては、例えば、銀行取引、有価証券取引、映画や音楽、ゲームなどの娯楽を提供する娯楽提供サイト、ソフトウェアをダウンロード販売するソフト販売サイト、通信販売を行う通信販売サイト、データベースによるデータ検索を行う情報提供サイトなど各種のものがある。

【００２８】

サーバ５は、登録部１３、自動ログイン部１５、サービスサイト１７などの各種機能部や、ユーザ情報データベース１９、サーバ割符データベース２０などの各種データベース

を備えている。
サービスサイト１７は、端末３からの求めに応じて各種のサービスを提供するサービスサイトである。
自動ログイン部１５は、端末３から送信されてきたカード固有情報とユーザ割符を用いてユーザを認証する機能部である。詳細は後述するが、自動ログイン部１５は、端末３から送信されてきたカード固有情報にひも付けされたサーバ割符を検索する。そして、検索されたサーバ割符と端末３から送信されてきたユーザ割符から元データを復元し、元データに含まれるパスワードなどを用いてユーザの認証を行う。
【００２９】
登録部１３は、サービスサイト１７を利用したい新規のユーザを登録する機能部である。登録部１３により登録されたユーザに対して自動ログイン部１５は認証を行う。
ユーザ情報データベース１９は、登録部１３により登録した各ユーザに関する情報を格納したデータベースである。ユーザ情報データベース１９には、ユーザを認証するための認証情報（パスワード、ユーザＩＤ）の他、ユーザが所有するＩＣカード１０に関する情報（カードＩＤ、電子マネーＩＤなど）や、ユーザの個人情報（氏名、年齢、性別、住所、勤務先、趣味など）などが格納されている。
サーバ割符データベース２０は、各ユーザの有するユーザ割符に符合するサーバ割符を格納したデータベースである。サーバ割符データベース２０に格納されたサーバ割符は、ユーザの有するＩＣカードのカード固有情報とひも付けされており、端末３から送信されてきたカード固有情報を用いて検索できるようになっている。
【００３０】
図５は、自動ログイン部１５の機能的な構成を模式的に示したブロック図である。
自動ログイン部１５は、端末アクセス部３１、検索部３２、復元部３３、認証情報生成部３４、認証部３５などを備えている。
端末アクセス部３１（特定情報取得部、第２の符合情報取得部、受信手段）は、端末３とのデータの送受信を行う。より詳細には、アクセスしてきた端末３に対してログイン画面データを送信したり、ログイン画面に応じて端末３から送信されてきたカード固有情報やユーザ割符を受信したりなどする。
なお、端末アクセス部３１は、同一の端末３からカード固有情報とユーザ割符が送信されてきたことを確認する。
自動ログイン部１５は、異なる端末３からカード固有情報とユーザ割符が別々に送信されてきた場合は認証を行わないように構成されており、これによってセキュリティが高められている。
【００３１】
検索部３２（第１の符合情報検索手段、検索手段）は、端末アクセス部３１からカード固有情報を受け取り、このカード固有情報と符合するサーバ割符をサーバ割符データベース２０で検索する。先に述べたように、サーバ割符データベース２０では、サーバ割符がカード固有情報とひも付けされているので、検索部３２は、ログインを要求しているユーザのサーバ割符を検索することができる。
復元部３３（認証情報取得手段）は、検索部３２から検索したサーバ割符を取得し、端末アクセス部３１からユーザ割符を取得し、これらを用いて元データを復元する。本実施の形態では、復元の結果、パスワードとカード固有情報が得られる。
なお、本実施の形態では、元データとしてパスワードとカード固有情報を用いたが、これは元データの内容を限定するものではなく、ユーザを認証するための認証情報を特定できるものであれば、元データとして採用することができる。この例として後ほど携帯メモリ特定情報を元データとする場合について説明する。
【００３２】
認証情報生成部３４（認証情報獲得手段）は、復元部３３から復元したパスワードとカード固有情報を取得し、これらパスワードとカード固有情報の組にひも付けされているユーザＩＤをユーザ情報データベース１９から検索する。

そして、認証情報生成部３４は、パスワードと検索したユーザＩＤから認証情報を生成し、認証部３５に送る。

本実施の形態では、パスワードとユーザＩＤにより認証情報を構成する一方、パスワードを割符化した。このように、認証情報の一部（パスワード）を割符化することによりセキュリティをより高めることができる。

【００３３】

なお、本実施の形態では、ユーザＩＤは、パスワードとカード固有情報の組にひも付けされているとしたが、例えば、パスワード、またはカード固有情報、あるいはカード固有情報を構成するカードＩＤ、電子マネーＩＤのうち何れか一方にひも付けされているように構成してもよい。

認証部３５（認証手段、ログイン手段）は、認証情報生成部３４から認証情報（パスワードとユーザＩＤ）を取得し、これを用いてユーザを認証する。ユーザが認証された場合は、認証部３５はユーザをサービスサイト１７へのログイン処理を行う。一方、ユーザが認証されなかった場合はログイン処理を拒否し、端末３にエラーメッセージを送信する。

【００３４】

図６は、自動ログインシステム１において、ユーザが端末３からサービスサイト１７にログインする手順を説明するためのフローチャートである。

以下の動作は、端末３に搭載したＣＰＵとサーバ５に搭載したＣＰＵが所定のプログラムに従って行うものである。

まず、ユーザがブラウザ上でサービスサイト１７のＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒｓ）を入力するなどし、端末３からサーバ５にアクセスする（ステップ１０５）。

【００３５】

次に、端末アクセス部３１は、自動ログイン機能を端末３で実現する補助プログラムを端末３に送信する（ステップ４０５）。

この補助プログラムは、例えば、ユーザが端末３からサービスサイト１７にアクセスした際に、ＩＣカード１０からカード固有情報を読み込んだり、携帯メモリ１１からユーザ割符を読み込んだり、更に、これら読み込んだカード固有情報とユーザ割符をサーバ５に送信する機能などを端末３に発揮させるものである。　また、後述するように、ユーザが新規にサーバ５に登録する場合は、これを補助する機能を発揮する。

なお、例えば、２回目以降にサーバ５にアクセスする場合のように、端末３に既に補助プログラムがインストールされている場合は、サーバ５はステップ４０５の補助プログラムの送信を行わない。

【００３６】

次に、端末３は、補助プログラムを受信してインストールする。そして、この補助プログラムに従ってリーダライタ７を駆動してＩＣカード１０にアクセスする（ステップ１１０）。なお、リーダライタ７にＩＣカード１０がセットされていない場合は、「ＩＣカードをセットしてください。」などと、ユーザにＩＣカード１０をセットするように促すメッセージを発する。

次に、ＩＣカード１０は、リーダライタ７と非接触で通信を行うことにより、端末３にカード固有情報を送信する（ステップ２０５）。

端末３は、リーダライタ７を介してカード固有情報を取得し、これらをサーバ５に送信する（ステップ１１５）。

サーバ５は、このカード固有情報を受信する（ステップ４１０）。

【００３７】

次に、端末３は、携帯メモリ駆動装置８を駆動して携帯メモリ１１からユーザ割符の読み取りを行う（ステップ１２０）。携帯メモリ１１が携帯メモリ駆動装置８にセットされていない場合は、例えば、「携帯メモリをセットしてください。」などと、ユーザに携帯メモリ１１をセットするように促すメッセージを発する。

次に、携帯メモリ１１は、格納しているユーザ割符を携帯メモリ駆動装置８を介して端

末３に提供する（ステップ３０５）。
端末３は、携帯メモリ１１から取得したユーザ割符をサーバ５に送信する（ステップ１２５）。
次に、サーバ５で端末アクセス部３１がユーザ割符を受信する（ステップ４１５）。
【００３８】
以上の手順では、端末３は、まず、カード固有情報を読み取ってサーバ５に送信し（ステップ１１５）、次いでユーザ割符を読み取ってサーバ５に送信する（ステップ１２５）としたが、これに限定するものではなく、端末３がカード固有情報とユーザ割符の読み取りを行い、これらを一時にサーバ５に送信するように構成してもよい。
あるいは、ユーザ割符をサーバ５に送信した後、カード固有情報をサーバ５に送信するように構成してもよい。
【００３９】
次に、検索部３２が、端末アクセス部３１からカード固有情報を受け取り、サーバ割符データベース２０でユーザのサーバ割符を検索する（ステップ４２０）。
次に、復元部３３が、ユーザ割符を端末アクセス部３１から受け取り、更にサーバ割符を検索部３２から受け取る。そして、復元部３３は、ユーザ割符とサーバ割符から元データ（パスワードとカード固有情報）を復元する（ステップ４２５）。
次に、認証情報生成部３４は、復元部３３から復元したパスワードとカード固有情報を受け取り、これらの情報にひも付けされたユーザＩＤをユーザ情報データベース１９で検索する（ステップ４３０）。
【００４０】
次に、認証部３５が認証情報生成部３４から認証情報（パスワードとユーザＩＤ）を受け取り、ユーザの認証を行う（ステップ４３５）。
ユーザが認証された場合、サーバ５は、ログイン後画面データ（ログイン後に端末３のブラウザ上で表示する画面のデータ）を端末３に送信する（ステップ４４０）。
端末３は、ログイン後画面データを受信し、ブラウザがこれを用いてログイン後画面を表示する（ステップ１３０）。
なお、ユーザが認証されなかった場合は、サーバ５は端末３にエラーメッセージ画面データを送信する。
以上、本実施の形態では、サーバ５がユーザの認証を行うように構成したが、サーバの構成はこれに限定するものではなく、例えば、ユーザの認証を行う専用の認証サーバを設け、認証サーバで認証されたユーザに対してサーバ５がサービスを提供するように構成してもよい。
また、ユーザ割符とサーバ割符とからログインＩＤ及びパスワードを取得するためだけの専用サーバを設け、ユーザがログインを要求している対象サーバへ、専用サーバからログインに必要な情報を提供するように構成しても良い。
【００４１】
図７は、登録部１３の機能的な構成を模式的に示したブロック図である。
登録部１３は、端末アクセス部４１、受信情報処理部４２、割符化部４３、サーバ割符保存部４４などの機能部を備えている。
端末アクセス部４１（登録情報取得手段、第２の符合情報送信手段）は、新規に登録するユーザに対して登録画面データを送信したり、ユーザが登録画面から入力して送信してきた登録情報を受信して処理するほか、生成したユーザ割符を端末３に送信したりなどする。
ユーザが自動ログインサービスを受けるための情報を入力する登録画面には、例えば、認証情報（パスワード、ユーザＩＤなど）を入力する欄、ユーザの個人情報（氏名、年齢、性別、住所、勤務先、趣味など）を入力する欄などが備えられている。このように、登録情報には認証情報が含まれている。
【００４２】
登録に際して端末アクセス部４１が端末３から受信する情報は、ユーザが登録画面に入

力した情報の他に、端末３にセットされており端末３が読み取ったＩＣカード１０のカードＩＤ２５などがある。また、サーバ５側で携帯メモリ固有情報を利用する場合は、携帯メモリ１１から読み取った携帯メモリ固有情報も受信する。

【００４３】

受信情報処理部４２は、端末アクセス部４１から受信情報を受け取り、これを用いてユーザ情報データベース１９に新規登録ユーザのユーザ情報を書き込んで更新すると共に、受信情報に含まれるパスワードとカード固有情報を割符化部４３に送る。

割符化部４３（符合情報生成手段）は、受信情報処理部４２から受け取ったパスワードとカード固有情報を割符化してユーザ割符、及びサーバ割符を生成する。そして、これら生成された電子割符のうち、ユーザ割符は端末アクセス部４１から端末３に送信する。これに対して、端末３は、ユーザ割符を受信して携帯メモリ１１に格納する。

サーバ割符は、サーバ割符保存部４４（対応付け手段、記憶手段）によってサーバ割符データベース２０に格納される。

更にサーバ割符保存部４４は、サーバ割符データベース２０に格納したサーバ割符とユーザ情報データベース１９に格納したカード固有情報（カードＩＤと電子マネーＩＤの組み合わせ）とをひも付けし（対応付けし）、カード固有情報からサーバ割符を検索できるようにする。

【００４４】

図８は、登録部１３が自動ログインシステム１において、ユーザが端末３からサービスサイト１７にユーザ登録する手順を説明するためのフローチャートである。

以下の動作は、端末３に搭載したＣＰＵとサーバ５に搭載したＣＰＵが所定のプログラムに従って行うものである。

まず、端末３からサーバ５にアクセスする（ステップ５０５）。そして、サーバ５から送られてくるトップページなどで新規登録ボタンをクリックするなどして、サーバ５に新規登録したい旨の情報をサーバ５に送信する。

すると、サーバ５では、端末アクセス部４１が登録画面データを端末３に送信する（ステップ８０５）。

【００４５】

次に、端末３では、登録画面データを受信し、ブラウザがこれを用いて入力事項を入力可能に表示する。ユーザは、表示された登録画面にパスワードやユーザＩＤ、その他の情報を入力してサーバ５に送信する（ステップ５１０）。なお、ユーザが既にユーザＩＤを持っている場合は登録画面からこれを入力するが、ユーザがユーザＩＤを持っていない場合は、ユーザが登録することによってユーザＩＤを取得するか、サーバ５側で自動的に設定してもよい。

次に、サーバ５で受信情報処理部４２が端末３から受信した情報を用いてユーザ情報データベース１９を更新し、ユーザ情報を新規に登録する（ステップ８１０）。

次に、登録部１３の端末アクセス部４１は、補助プログラムを端末３に送信する（ステップ８１５）。補助プログラムは、ユーザの登録時においては、端末３でＩＣカード１０からカードＩＤ２５や電子マネーＩＤ２６を読み取ってサーバ５に送信したり、携帯メモリ１１にユーザ割符を書き込んだりなどする。なお、補助プログラムが既にインストールされている場合や、ブラウザに補助プログラムが組み込まれている場合は、このステップを省略することができる。

【００４６】

次に、端末３は、サーバ５から受信した補助プログラムをインストールする。そして、端末３は、補助プログラムに従ってリーダライタ７を駆動し、ＩＣカード１０からカード固有情報の読み取りを開始する（ステップ５１５）。

次に、リーダライタ７にセットされているＩＣカード１０が、非接触にて端末３にカード固有情報を送信する（ステップ６０５）。

次に、端末３は、ＩＣカード１０から読み取ったカード固有情報をサーバ５に送信する（ステップ５２５）。

【００４７】
次に、サーバ５では、端末アクセス部４１がカード固有情報を受信する（ステップ８２０）。
次に、受信情報処理部４２がこれらの情報をユーザ情報データベース１９に格納し、ユーザＩＤとカード固有情報をひも付けする（ステップ８２５）。
次に、割符化部４３が、パスワードとカード固有情報を割符化し、ユーザ割符、及びサーバ割符を生成する（ステップ８３０）。
次に、サーバ割符保存部４４が、生成したサーバ割符をカード固有情報にひも付けし（ステップ８３５）、更にサーバ割符データベース２０に格納する（ステップ８４０）。
次に、端末アクセス部４１が、生成したユーザ割符を割符化部４３から受け取り、端末３に送信する（ステップ８４５）。
【００４８】
端末３は、端末アクセス部４１から送信されてきたユーザ割符を受信する（ステップ５３０）。
次に、端末３は、携帯メモリ駆動装置８を駆動し、受信したユーザ割符を携帯メモリ１１に書き込む（ステップ５３５）。
そして、携帯メモリ１１は、ユーザ割符を記憶する（ステップ７１０）。
次に、端末アクセス部４１は、登録完了通知を端末３に送信する（ステップ８５０）。
端末３は、この登録完了通知を受信し、ブラウザにより登録完了通知が表示される（ステップ５４０）。
【００４９】
図９は、サーバ５のハードウェア的な構成の一例を示した図である。
図９に示したように、サーバ５は、制御装置５１、通信制御装置５２、表示装置５３、入出力装置５４、記憶装置５５、及びこれらの構成要素間でデータや制御信号の送受信を媒介するバスライン５８などから構成されている。
制御装置５１は、ＣＰＵ、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）などから構成されており、ＣＰＵは、所定のプログラムに従って、各種演算処理や、サーバ５全体の制御、インターネット２を介した通信などを行う。
本実施の形態では、自動ログインプログラムに従って、自動ログインの対象となるユーザの登録や、サービスサイト１７にアクセスしてきたユーザを認証して自動ログイン処理を行ったりする。
【００５０】
通信制御装置５２は、インターネット２を介して端末３、３、３…と通信を行う装置である。端末３、３、３…との通信には、例えば、ＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）などのプロトコルが用いられる。
表示装置５３は、例えば、ＣＲＴ（Ｃａｔｈｏｄｅ　Ｒａｙ　Ｔｕｂｅ）やその他の表示装置で構成され、例えば、管理者がサーバ５を維持管理するのに用いる。表示装置５３により、ユーザ情報データベース１９やサーバ割符データベース２０に記憶されたデータを閲覧することができる。
入出力装置５４は、例えば、キーボードやマウスなどの入力装置や、着脱可能な記憶装置を駆動する記憶媒体駆動装置や、プリンタなどの印刷装置から構成されており、サーバ５にコマンドやデータを入力したり、サーバ５からデータを出力したりすることができる。
【００５１】
記憶装置５５は、例えば大容量のハードディスクなどの読み書き可能な記憶装置により構成されている。
記憶装置５５には、自動ログインプログラム５６、ユーザ情報データベース１９、サーバ割符データベース２０などが記憶されている。

自動ログインプログラム５６は、制御装置５１に自動ログイン機能を発揮させるためのプログラムである。

制御装置５１は、自動ログインプログラム５６を読み込んで実行することにより、登録部１３、自動ログイン部１５がソフトウェア的に実現される。

また、記憶装置５５には、図示しないがファイルの入出力など基本的な機能を制御装置５１に発揮させるプログラムであるＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）や、サービスサイト１７を運営するためのプログラムやデータなどが記憶されている。

【００５２】

図１０は、端末３のハードウェア的な構成の一例を示した図である。

本実施の形態では、端末３をパーソナルコンピュータを用いて構成した。

端末３は、制御部６１に、バスライン７２を介して、キーボード６５、マウス６６、表示装置６７、印刷装置６８、通信制御装置６９、入出力Ｉ／Ｆ（インターフェース）７３、リーダライタ７、携帯メモリ駆動装置８、記憶媒体駆動装置７１、記憶装置７５などが接続して構成されている。

【００５３】

制御部６１は、ＣＰＵ６２、ＲＯＭ６３、ＲＡＭ６４などから構成されている。

制御部６１は、ＯＳプログラム７６やブラウザプログラム７７などの各種プログラムに従って動作し、サーバ５との通信の維持、サーバ５の自動ログイン機能へのユーザ登録、ユーザ登録してある場合は、サービスサイト１７への自動ログイン、サービスサイト１７の利用などの各種の情報処理を行ったり、端末３全体の制御などを行う。

【００５４】

ＣＰＵ６２は、制御部６１の中心的なデバイスであって、ＲＯＭ６３や記憶装置７５、または記憶媒体駆動装置７１によって駆動される記憶媒体などからプログラムをロードし、プログラムに従って制御部６１を制御する。ＣＰＵ６２は、後述の補助プログラム７８にしたがって動作することにより、カード固有情報を送信したり（特定情報送信手段）、ユーザ割符を送信したり（第２の符合情報送信手段）、登録情報を送信したり（登録情報送信手段）、登録時にサーバ５から受信したユーザ割符を記憶装置７５に記憶したり（第２の符合情報記憶手段）などする。

ＲＯＭ６３は、ＣＰＵ６２が各種演算や制御を行うための各種プログラム、データ及びパラメータなどを格納したリードオンリーメモリである。

ＲＡＭ６４は、ＣＰＵ６２にワーキングメモリとして使用されるランダムアクセスメモリである。ＣＰＵ６２は、ＲＡＭ６４にプログラムやデータなどを書込んだり消去したりすることができる。本実施の形態では、ＲＡＭ６４には、サーバ５に自動ログイン対象としてユーザ登録したり、サービスサイト１７に自動ログインを行ったり、あるいは、サービスサイト１７を利用するためのエリアが確保可能となっている。

【００５５】

キーボード６５は、カナや英文字などを入力するためのキーや数字を入力するためのテンキー、各種機能キー、カーソルキー及びその他のキーによって構成されている。

キーボート６５は、例えばサーバ５に送信するためのユーザ情報を入力したり、コマンドなど各種プログラムを操作するための情報を入力するのに使用する。　マウス６６は、ＧＵＩ（Ｇｒａｐｈｉｃａｌ　Ｕｓｅｒ　Ｉｎｔｅｒｆａｃｅ）などを用いて端末３を操作する場合に、ＧＵＩ上に表示されたボタンやアイコンなどをマウスでクリックすることにより、所定の情報の入力を行うことができるポインティングデバイスである。

【００５６】

表示装置６７は、例えばＣＲＴディスプレイ、液晶ディスプレイ、プラズマディスプレイなどで構成された情報を画面上に提示するための装置である。

表示装置６７は、キーボード６５やマウス６６の入力結果や、サービスサイト１７が提供する画面、サーバ５の自動ログイン機能にユーザ登録するための登録画面などを表示することができる。

印刷装置６８は、プログラムの実行結果などを紙などの印刷媒体に印刷する装置である

。印刷装置６８は、例えば、インクジェットプリンタ、レーザプリンタ、熱転写プリンタ、ドットプリンタなどの各種プリンタ装置によって構成されている。
通信制御装置６９は、端末３をインターネット２に接続するための装置であって、モデム、ターミナルアダプタその他の装置によって構成されている。
通信制御装置６９は、ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）などを介してインターネット２に接続するように構成することもできる。
通信制御装置６９はＣＰＵ６２によって制御され、所定のプロトコル（ＴＣＰ／ＩＰなど）に従って送受信を行う。

【００５７】

記憶装置７５は、読み書き可能な記憶媒体と、その記憶媒体に対してプログラムやデータを読み書きするための駆動装置によって構成されている。当該記憶媒体として主にハードディスクが使用されるが、その他に、例えば、光磁気ディスク、磁気ディスク、半導体メモリなどの他の読み書き可能な記憶媒体によって構成することも可能である。
記憶装置７５は、ＯＳプログラム７６、ブラウザプログラム７７、補助プログラム７８などの各種プログラムの他、各種データなどを記憶している。

【００５８】

ＯＳプログラム７６は、ファイルの入出力など、端末３を動作させるための基本的なプログラムである。
ブラウザプログラム７７は、サーバ５やその他のＷＷＷ（Ｗｏｒｌｄ Ｗｉｄｅ Ｗｅｂ）サーバに開設されたサービスサイトにアクセスして、これらサービスサイトから送信されてきた画面データを用いて画面を表示装置６７に表示する。また、音声や動画を再生することも可能である。

【００５９】

補助プログラム７８は、サーバ５からダウンロードしてインストールしたものである。
補助プログラム７８は、新規登録用の補助プログラムと自動ログイン用の補助プログラムというように別々のプログラムとして構成してもよいし、両方の機能を持った一つのプログラムとして構成してもよい。
補助プログラム７８は、ユーザ登録の際や自動ログインの際に、ブラウザプログラム７７の機能を補助する機能を発揮させる。具体的には、登録時や自動ログイン時にＩＣカード１０からカード固有情報を読み取ってサーバ５に送信したり、自動ログイン時に携帯メモリ１１からユーザ割符を読み出してサーバ５に送信したり、あるいは登録時にサーバ５から受信したユーザ割符を携帯メモリ１１に書き込んだりなどの機能を発揮させる。
記憶装置７５には、この他に、通信制御装置６９を制御するためのプログラムや、リーダライタ７や携帯メモリ駆動装置８を駆動するためのプログラムなど、各種のプログラムやデータが格納されている。

【００６０】

記憶媒体駆動装置７１は、携帯メモリ１１以外の着脱可能な記憶媒体を駆動してデータの読み書きを行うための駆動装置である。着脱可能な記憶媒体としては、例えば、光磁気ディスク、磁気ディスク、磁気テープ、データをパンチした紙テープ、ＣＤ－ＲＯＭなどがある。なお、ＣＤ－ＲＯＭや紙テープは、読み込みのみ可能である。記憶媒体駆動装置７１を介して記憶媒体にバックアップ用のデータを書き出したり、また記憶媒体からアプリケーションソフトをインストールしたりなどできる。
入出力Ｉ／Ｆ７３は、例えば、シリアルインターフェースやその他の規格のインターフェースにより構成されている。入出力Ｉ／Ｆ７３に当該インターフェースに対応した外部機器を接続することにより、端末３の機能を拡張することができる。このような外部機器として例えば、ハードディスクなどの記憶装置、スピーカ、マイクロフォンなどがある。
リーダライタ７、及び携帯メモリ駆動装置８は、既に説明したので説明を省略する。

【００６１】

以上、サーバ５の自動ログイン機能について説明したが、サーバ５は、従来の方法（ユーザが認証情報を手入力してサーバ５に送信する）によるログイン処理機能も備えている

。

サーバ５へのログイン時に、端末３にＩＣカード１０と携帯メモリ１１がセットされている場合は、自動ログイン処理が行われ、ＩＣカード１０及び携帯メモリ１１がセットされていない場合は、従来方法によるログイン処理が行われる。　このようにサーバ５は、自動ログイン処理と従来のログイン処理の双方の機能を備えることにより、何れのユーザに対しても対応することができる。

以下に、自動ログイン処理を行う場合と、従来の方法によるログイン処理を行う場合について画面遷移図を用いて説明する。

【００６２】

図１１は、自動ログイン処理を行う場合と、従来の方法でログイン処理を行う場合の端末３での画面遷移の一例を示した図である。

まず、自動ログインを行う場合の画面遷移について説明する。

ユーザが端末３にブラウザのＵＲＬ欄にサービスサイト１７のＵＲＬを入力すると、サーバ５からサービスサイト１７のトップ画面データが端末３に送信される。そして、端末３の表示装置６７には、図１１（ａ）に示したトップ画面８１が表示される。

トップ画面８１は、サービスサイト１７にログインするためのログインボタン８５が表示されている。

【００６３】

端末３にＩＣカード１０と携帯メモリ１１がセットしてある場合、ユーザがログインボタン８５をクリックするとＩＣカード１０に格納されているカード固有情報、及び携帯メモリ１１に格納されてるユーザ割符が端末３からサーバ５に送信される。そして、サーバ５は、ユーザの認証処理及びログイン処理を行い、ログイン後の画面データを端末３に送信する。

端末３は、このログイン後の画面データを受信し、これを用いて表示装置６７に図１１（ｃ）に示したログイン後画面８３を表示する。

即ち、自動ログイン処理を行った場合、ユーザはトップ画面８１でログインボタン８５をクリックすると、他に操作することなく、ログイン後画面８３を得ることができる。

【００６４】

次に、従来方法によるログイン処理の画面遷移について説明する。ＩＣカード１０と携帯メモリ１１は何れも端末３にセットされていないものとする。

まず、ブラウザからサービスサイト１７のＵＲＬを入力し、表示装置６７に図１１（ａ）のトップ画面８１を表示する。

ユーザがトップ画面８１上のログインボタン８５をクリックすると、ログインボタン８５がクリックされた旨の情報が端末３からサーバ５に送信される。このとき、端末３にＩＣカード１０と携帯メモリ１１の何れもセットされていない旨の情報が端末３からサーバ５に送信される。そして、これによってサーバ５は、ユーザが従来のログイン処理を希望していると判断し、ログイン画面データを端末３に送信する。

端末３は、このログイン画面データを用いて表示装置６７に図１１（ｂ）に示したログイン画面８２を表示する。

【００６５】

ログイン画面８２は、ユーザＩＤ入力欄８６とパスワード入力欄８７を備えている。ユーザが、キーボード６５などを用いてこれらの欄にユーザＩＤとパスワードを入力した後、送信ボタン８８をクリックすると、ユーザが入力したユーザＩＤとパスワードが端末３からサーバ５に送信される。

サーバ５は、端末３から送信されてきたユーザＩＤとパスワードを受信して、これらを用いて認証処理、ログイン処理を行う。サーバ５は、ログイン処理を行った後、ログイン後の画面データを端末３に送信する。

端末３では、サーバ５から送信されたログイン後の画面データを用いて図１１（ｃ）に示したログイン後画面８３を表示装置６７に表示する。

【００６６】

以上に説明した例では、ＩＣカード１０と携帯メモリ１１の何れも端末３にセットされていない場合、自動的に従来のログイン方法が行われるように構成したが、これに限定せず、例えば、ＩＣカード１０と携帯メモリ１１の一方のみセットされている場合にも、従来のログイン方法を採用するように構成してもよい。　あるいはログインボタン８５をクリックした際にＩＣカード１０と携帯メモリ１１の双方がセットされていなかった場合、ＩＣカード１０と携帯メモリ１１をセットして自動ログインするか、あるいは従来の方法でログインするかユーザに選択させるように構成してもよい。

【００６７】

次に、他の画面構成例について説明する。

図１２は、本実施の形態のサービスサイトのトップページの一例を示した図である。

図に示したように、トップページには、「ユーザＩＤを新規取得」、「ＩＤ入力でログイン」、「カードでログイン」の３つの項目が表示される。これらの項目の何れかをマウスでクリックするなどして選択すると、対応するページにジャンプするようになっている。

「ユーザＩＤを新規取得」は、このサービスサイトに新規に入会する場合や現在のユーザＩＤの他に新たにユーザが欲しい場合に、ユーザＩＤを発行してもらう場合に選択する項目である。この項目を選択すると登録画面にジャンプし、ユーザは新規登録することができると共に、ユーザＩＤの設定またはユーザＩＤを発行することができる。

【００６８】

「ＩＤ入力でログイン」は、従来からの方法でログインする場合に選択する項目である。

この項目を選択すると、ユーザＩＤとパスワードを手入力する従来のログイン画面にジャンプする。

「カードでログイン」は、ＩＣカード１０を用いてログインする場合に選択する項目である。

この項目を選択すると、図１３に示したカードログイン画面にジャンプする。　カードログイン画面では、「カードをカードリーダにセットしてください。」というメッセージによりユーザにＩＣカード１０をリーダライタ７にセットするように促す。これと共にリーダライタ７はポーリングを開始する。

更に、カードログイン画面には、「パソコンに割符の入った携帯メモリをセットしてください。」とのメッセージが表示され、ユーザに携帯メモリ１１を携帯メモリ駆動装置８にセットするように促す。

【００６９】

ユーザが携帯メモリ１１をまだ設定していない場合（即ち、ＩＣカード１０とユーザＩＤとのひも付けは行ってあるが、携帯メモリ１１に格納されたユーザ割符を利用しない場合）、項目「パスワード」に対してパスワードを入力する。パスワードを外部入力することによってＩＣカードでログインするのは、携帯メモリの設定がなされていない場合や、携帯メモリの設定はなされているがメモリカードを利用しない場合等が考えられる。

このように、カードログイン画面ではＩＣカード１０と携帯メモリ１１を用いて全自動で自動ログインすることもできるし、ＩＣカード１０をセットすると共にパスワードを手入力して自動ログインすることもできる。

なお、端末３に既にＩＣカード１０と携帯メモリ１１がセットしてある場合は、カードログイン画面を省略して直に自動ログインが行われる。

端末３にＩＣカード１０か携帯メモリ１１の何れかが既にセットしてある場合は、セットされているものに対するメッセージは表示されない。

【００７０】

図１４は、自動ログインシステムへの登録段階で、ＩＣカード１０のカード固有情報とユーザＩＤをひも付けする際に表示されるひも付け通知画面である。

自動ログインシステムに登録を要求すると、ＩＣカード１０をリーダライタ７にセットするように促す画面が表示される。そして、ユーザがＩＣカード１０をセットすると、リ

ーダライタ７がカード固有情報を読み取り、これがひも付け通知画面に表示される。なお、カードＩＤは密番なので、「＊」印などで表示され、ユーザに認識されないようになっている。

図示しない所定のボタンをクリックすると、カード固有情報がサーバ５に送信され、ユーザＩＤとのひも付けが行われる。

【００７１】

図１５は、カード固有情報とユーザＩＤとのひも付けが完了したときに表示されるひも付け完了画面である。

ひも付け完了画面では、ＩＣカード１０をリーダライタ７にかざすことによりユーザＩＤの入力を代行することができる旨のメッセージが表示されると共に、携帯メモリ１１を設定するとパスワードの入力も自動化できる旨のメッセージも表示される。図示しないが、ひも付け完了画面では、携帯メモリ１１の設定をするか否かを選択する選択ボタンが表示され、携帯メモリ１１の設定を選択すると図１６に示した携帯メモリ設定画面が表示される。

携帯メモリ１１の設定を選択しない場合は、ＩＣカード１０をリーダライタ７にかざすと共に、パスワードを手入力してログインすることになる。

【００７２】

携帯メモリ設定画面では、リーダライタ７に携帯メモリ１１をセットするように促すメッセージの他、ユーザを確認するためのユーザＩＤ入力欄と、電子割符を作成する元となるパスワードを入力するパスワード入力欄が表示される。

ユーザがユーザＩＤとパスワードを入力して、図示しない送信ボタンをクリックすると、これらの情報がサーバ５に送信され、電子割符が生成される。

生成された電子割符のうち、ユーザ割符は端末３に送信されて携帯メモリ１１に書き込まれ、図１７に示した携帯メモリ設定完了画面が表示される。

携帯メモリ設定完了画面では、設定が完了した旨のメッセージと、携帯メモリ１１とＩＣカード１０を組み合わせることにより、パスワードを手入力することなくログインを自動化できる旨のメッセージが表示される。

【００７３】

以上に本実施の形態について説明したが、本実施の形態の自動ログインシステム１により以下のような効果を得ることができる。

（１）割符を用いてユーザを認証することにより以下のような効果が得られる。　認証情報を割符化してあるため、サーバ５へのアタックによりサーバ割符が流出したり、もしくは携帯メモリ１１の紛失によってユーザ割符が流出するようなことがあっても認証情報を復元される危険を回避することができる。従って、自動ログインシステム１は、セキュリティが非常に高いシステムとなっている。

また、ＩＣカード１０が保有する情報で認証情報に関連するものとしては認証に要するデータ（サーバ割符）をひも付けるための番号（カードＩＤ２５、電子マネーＩＤ２６）だけである。このため、ＩＣカード１０を紛失しても他者に悪用されることはない。

更に、２つの割符をそれぞれ別の可搬式媒体に保存する場合、両方が第三者の手に渡ってしまうと、割符が揃い元情報を復元されてしまう可能性があるが、自動ログインシステム１では割符をサーバ５と可搬式媒体（携帯メモリ１１）に保存しているため、第三者が２つの可搬式媒体（ＩＣカード１０と携帯メモリ１１）を同時に手に入れたとしても、元情報を復元することはできない。

【００７４】

（２）自動ログインを行うことにより以下のような効果が得られる。

ＩＣカード１０と携帯メモリ１１を用いて自動ログインを行うため、ユーザＩＤやパスワードを手入力する必要がない。

また、ユーザは、ユーザＩＤやパスワードを記憶する必要がないため、ユーザの利便性が高まる。

更に、パスワードを記憶する必要がないため、パスワードとして大文字、小文字、数字

などを組み合わせた複雑なものを採用することができ、セキュリティを高めることができる。

【００７５】

（３）可搬式記憶媒体として非接触式のＩＣカード１０を採用することにより以下のような効果が得られる。

利用の際にはＩＣカード１０リーダライタ７にかざすだけでよいので使い勝手がよい。

また、ＩＣカード１０とリーダライタ７を物理的に接触させる必要がないので、リーダライタ７及びＩＣカード１０の耐久性が保たれる。

更に、接触式の可搬式記憶媒体（接触式のＩＣカードなど）を用いた場合、屋外で使用する用途では埃・雨水などによる可搬式記憶媒体と端末の接点間の障害が問題点としてあるが、非接触のＩＣカード１０を用いることにより、このような問題を回避することができる。

【００７６】

（変形例１）

先に説明した実施の形態では、パスワードとカード固有情報を割符化してユーザ割符とサーバ割符を生成したが、電子割符を生成する元データとしては、各種のものを利用することができる。

例えば、ユーザＩＤ、パスワード、カードＩＤ２５、電子マネーＩＤ２６、携帯メモリ固有情報の何れか、あるいはこれらの任意の組み合わせを用いることが可能である。

そこで、本変形例では、一例として携帯メモリ固有情報を用いて電子割符を生成する例について図１８のフローチャートを用いて説明する。

ただし、図８と同じステップには、同じステップ番号を付し、携帯メモリ固有情報に関する部分だけ説明する。

【００７７】

まず、端末３は、携帯メモリ駆動装置８を駆動して携帯メモリ１１から携帯メモリ固有情報を読み出す（ステップ５２６）。

これに対し、携帯メモリ１１は、携帯メモリ固有情報を端末３に提供する（ステップ７０５）。

端末３は、携帯メモリ１１から取得した携帯メモリ固有情報をサーバ５に送信する（ステップ５２８）。

【００７８】

サーバ５は、端末３から送信されてきた携帯メモリ固有情報を受信する（ステップ９０３）。

次に、サーバ５では、割符化部４３が乱数を発生させる（ステップ９０５）。乱数を発生させるための基準となる値として例えば、時刻データを用い、乱数がランダムに発生するようにする。

次に、割符化部４３が発生させた乱数をサーバ割符としてサーバ割符データベース２０に保存する（ステップ９１０）。

【００７９】

次に、割符化部４３は、端末３から取得した携帯メモリ固有情報とステップ９０５で発生させた乱数を用いてユーザから取得したパスワードのハッシュを暗号化する（ステップ９１５）。

次に、端末アクセス部４１が、暗号化したパスワードのハッシュをユーザ割符として端末３に送信する（ステップ９２０）。

端末３は、サーバ５からユーザ割符を受信し（ステップ５３０）、携帯メモリ駆動装置８を用いてこれを携帯メモリ１１に書き込む（ステップ５３５）。

そして、携帯メモリ１１は、書き込まれたユーザ割符を記憶する（ステップ７１０）。

以上、携帯メモリ固有情報を用いて電子割符を生成する手順について説明したが、このように電子割符に携帯メモリ固有情報を含めることにより、携帯メモリ１１に保存したユーザ割符を他の携帯メモリ１１へコピーした場合は、そのユーザ割符が無効となるように

設定することかできる。
　このように設定するには、例えば、自動ログインの際に端末３から携帯メモリ固有情報を送信してもらい、電子割符から復元した携帯メモリ固有情報と照合するようにすればよい。
【００８０】
　（変形例２）
　次に、パスワードを手入力する例について説明する。本変形例では、ユーザは、ＩＣカード１０を端末３にセットすると共に、パスワードを手入力する。
　本変形例のサーバ５では、カード固有情報とユーザＩＤがひも付けされている。そのため、ユーザからパスワードを手入力で送信してもらい、更にＩＣカード１０からカード固有情報を送信してもらえば、パスワードとユーザＩＤを用いて認証することができる。
【００８１】
　以下に図１９を用いながら、本変形例の処理手順について説明する。
　まず、端末３からサーバ５にアクセスする（ステップ１１０５）。そして端末３にまだ補助プログラムがインストールされていない場合は、サーバ５は端末３に補助プログラムを送信する（ステップ１２０３）。
　次に、端末３は、補助プログラムの発揮する機能によりＩＣカード１０のカード固有情報の読み取りを開始する（ステップ１１１０）。これに対して、ＩＣカード１０はカード固有情報を端末３に非接触で送信し（ステップ１００５）、端末３は、ＩＣカード１０から受け取ったカード固有情報をサーバ５に送信する（ステップ１１１５）。
【００８２】
　そして、サーバ５は、端末３から送信されてきたカード固有情報を受信する（ステップ１２０５）。
　次に、端末３は、ユーザが入力したパスワードを取得してサーバ５に送信し（ステップ１１２０）、サーバ５は、このパスワードを端末３から受信する（ステップ１２１０）。
　次に、サーバ５は、端末３から受信したカード固有情報にひも付けされたユーザＩＤを検索する（ステップ１２１３）。
【００８３】
　次に、サーバ５は、検索したユーザＩＤと端末３から受信したパスワードを用いてログイン認証を行い、次いでログイン処理を行う（ステップ１２１５）。
　ログイン処理が行われると、サーバ５は、ログイン後画面データを端末３に送信する（ステップ１２２０）。
　端末３では、このログイン後画面データを受信し、表示装置６７に表示する。
【００８４】
　（応用例）
　本実施の形態の自動ログインシステム１を応用して以下のようなサービスを提供することが可能である。
（１）個人情報の共有
　携帯メモリ１１を利用することで、機器間（パーソナルコンピュータ、ＣＥ機器など）での個人情報の共有を行なうことが可能となる。具体的には電子メール、アドレス帳、スケジュール、ブックマーク、個人プロファイルなどが挙げられる。
　ここで、ＣＥ（Ｃｏｎｓｕｍｅｒ　Ｅｌｅｃｔｒｏｎｉｃｓ）機器とは、一般家庭用のテレビやビデオなどのＡＶ機器、もしくは家電のことを指す。
　また、割符の元情報としてＵＲＬ情報を持たせることで、携帯メモリ１１を認識させ、ＩＣカード１０をかざすことで任意のＷｅｂページへアクセスさせることも可能である。
　割符による認証システムを用い、ユーザ割符とサーバ割符が照合しなければプライベートなデータにアクセスできないようにすることで、個人情報の機密性を守ることができる。
【００８５】
（２）ＩＣカード１０、携帯メモリ１１以外の記憶媒体の利用

ＩＣカード１０、携帯メモリ１１については、それぞれ他の可搬式の記憶媒体（携帯電話中のメモリなど）や固定された記憶媒体（パーソナルコンピュータのハードディスクなど）を用途に応じて使い分けることにより、更に利便性を向上させることができる。

（３）ＣＥ機器への応用

本実施の形態では、端末３の一例としてパーソナルコンピュータを用いたが、自動ログインシステム１は、ＣＥ機器（デジタルカメラ、テレビなど）の場合特に有用である。ＣＥ機器は入力インターフェースが貧弱なため、ユーザ割符１１１による認証技術は効果的だと思われる。

（４）会員証への利用

ＩＣカード１０を会員証とする利用も考えられる。この場合には、パスワードによる認証は行なわず、単にＩＣカード１０のカード固有情報がサーバ内の会員として登録してあるユーザＩＤとひも付けられたものかどうか、サーバでチェックすることにより、ＩＣカード１０の持ち主が会員かどうか判断を行なう。

【００８６】

以上、本発明における１実施形態について説明したが、本発明は説明した実施形態に限定されるものではなく、各請求項に記載した範囲において各種の変形を行うことが可能である。

例えば、自動ログインシステム１では、可搬式記憶媒体とし、ＩＣカード１０と携帯メモリ１１を用いたが、これは可搬式記憶媒体をＩＣカード１０と携帯メモリ１１に限定するものではなく、例えば、フレキシブルディスク、光磁気ディスク、他の種類の可搬式記憶媒体を用いてもよい。

更に、端末３としてブラウザを備えたパーソナルコンピュータを用いたが、これに限定するものではなく、端末３としてデジタルテレビなどのネットワーク接続可能な情報家電を用いることもできる。

加えて、ユーザＩＤとカード固有情報とのひも付けを解除する機能をサーバ５に付加することもできる。

また、パスワードの変更を考慮し、電子割符の再発行についても実行可能となっている。

【００８７】

また、本実施の形態は、次の（１）、（２）のように構成することもできる。（１）ユーザを識別するユーザ識別番号と、パスワードを登録するユーザ登録手段と、作成された割符のうち、サーバ（サーバ５）に保有されるサーバ割符（サーバ割符）とひも付けされる秘密の識別情報（カードＩＤ２５）を登録する密番登録手段と、作成された割符のうちユーザによって保有されるユーザ割符（ユーザ割符）をサーバより受信する割符受信手段と、前記割符受信手段において受信された前記ユーザ割符を記憶媒体（携帯メモリ１１）に記録する記録手段とを備え、前記割符は、前記パスワードから作成されることを特徴とする認証処理端末とすることができる。

ここで、前記割符は、前記パスワードと、前記秘密の識別番号とから作成されることを特徴とするように構成することができる。

更に、前記ユーザ割符を記録する記録媒体の識別情報を登録する媒体登録手段を更に備え、前記ユーザ割符は、前記媒体登録手段によって登録された記録媒体に格納されたユーザ割符であるかを認証とするように構成することもできる。

【００８８】

（２）ユーザの識別番号に対応するパスワードと、媒体（ＩＣカード１０）に記録される秘密の識別情報（カードＩＤ２５）とから作成される割符の一方であるユーザ割符（ユーザ割符）を記録媒体（携帯メモリ１１）に、もう一方はサーバ（サーバ５）に記憶されるサーバ割符（サーバ割符）より認証情報を得る情報処理装置において、前記記録媒体に格納される前記ユーザ割符をサーバへ送信する割符送信手段と、前記秘密の識別情報を読み出してサーバへ送信する密番送信手段とを備え、前記サーバへ送られた前記秘密の識別情報にひも付けられた割符であって、サーバに記憶されたサーバ割符と、前記割符送信手段

によって送信された前記割符とから、認証情報を得ることを特徴とする情報処理装置とすることができる。

【００８９】

このような構成では、予め認証情報の少なくとも一部を「割符」として２分割し、サーバと外部記憶媒体に登録する。それぞれのデータは個々では全く無意味なデータとなっている。認証の際には、割符の入った外部記憶媒体とサーバ内の割符とひも付けされた番号を持っている非接触式ＩＣカードを用いることにより認証を行い、ＩＤ・パスワードを手入力することなく自動ログインを可能とする。このようにセキュリティと利便性を両立させたシステムとなっている。また、非接触式ＩＣカードに記憶されている番号を密番とすることによりセキュリティをより高めることができる。

【００９０】

以上に説明したように、本実施の形態は、第１の可搬式記憶媒体から第１の符合情報を特定する特定情報を取得すると共に第２の可搬式記憶媒体から第２の符合情報を取得する端末と、前記端末から前記特定情報と前記第２の符合情報を取得して認証処理を行う認証サーバとから構成された認証システムを提供する。この認証システムでは、前記端末から所定のサービスサイトにログインする際に、前記端末は、前記特定情報と前記第２の符合情報を前記認証サーバに送信し、これに対し、前記認証サーバは、前記端末から受信した前記特定情報を用いて前記第１の符合情報を検索し、前記検索した第１の符合情報と前記端末から取得した前記第２の符合情報を用いて認証情報を取得し、前記取得した認証情報によりユーザが認証された場合に前記所定のサイトへのログイン処理を行う。

また、本実施の形態は、前記目的を達成するために、第１の可搬式記憶媒体から第１の符合情報を特定する特定情報を取得すると共に第２の可搬式記憶媒体から第２の符合情報を取得する端末から、前記特定情報と前記第２の符合情報を取得して認証を行う認証サーバを提供する。この認証サーバは、前記端末から前記特定情報を取得する特定情報取得手段と、前記取得した特定情報を用いて前記第１の符合情報を検索する第１の符合情報検索手段と、前記端末から前記第２の符合情報を取得する第２の符合情報取得手段と、前記検索した第１の符合情報と前記取得した第２の符合情報を用いて認証情報を取得する認証情報取得手段と、前記取得した認証情報を用いて認証を行う認証手段と、を具備している（第１の構成の認証サーバ）。

更に、この認証サーバに、前記認証手段で認証した場合に、前記端末から所定のサイトへのログイン処理を行う認証手段を具備することができる。

また、この認証サーバで扱う前記第１の符合情報と前記第２の符合情報は、前記認証情報の少なくとも一部から成る元データを所定のロジックにより割符化し、何れか一方だけでは前記元データを復元不能に生成した電子割符とすることができる。

この電子割符を用いた場合、前記認証情報取得手段は、前記第１の符合情報と、前記第２の符合情報を用いて、前記元データを復元するように構成することができる。

第１の構成の認証サーバに、更に、端末から認証情報を含んだ登録情報を取得する登録情報取得手段と、前記取得した登録情報に含まれる認証情報を第１の符合情報と第２の符合情報を用いて特定可能となるように、前記第１の符合情報と前記第２の符合情報を生成する符合情報生成手段と、前記端末から前記生成した第１の符合情報を検索するための特定情報を取得し、当該第１の符合情報と前記取得した特定情報を対応付ける対応付け手段と、前記対応付けた前記第１の符合情報を記憶する記憶手段と、前記生成した第２の符合情報を前記端末に送信する第２の符合情報送信手段と、を具備し、自動ログインの対象となるユーザを登録することもできる。

ここで、前記符合情報生成手段は、前記取得した登録情報に含まれる認証情報の少なくとも一部からなる元データを所定のロジックにより割符化することにより、何れか一方だけでは前記元データを復元不能となるように、前記第１の符合情報と前記第２の符合情報を生成するように構成することもできる。

また、本実施の形態は、前記目的を達成するために、第１の可搬式記憶媒体から第１の符合情報を特定する特定情報を取得し、第２の可搬式記憶媒体から第２の符合情報を取得

する端末から、前記特定情報と前記第２の符合情報を取得して認証を行う認証サーバであって、前記端末から認証情報を含んだ登録情報を取得する登録情報取得手段と、前記取得した登録情報に含まれる認証情報を第１の符合情報と第２の符合情報を用いて特定可能となるように、前記第１の符合情報と前記第２の符合情報を生成する符合情報生成手段と、前記端末から前記生成した第１の符合情報を検索するための特定情報を取得し、当該第１の符合情報と前記取得した特定情報を対応付ける対応付け手段と、前記対応付けた前記第１の符合情報を記憶する記憶手段と、前記生成した第２の符合情報を前記端末に送信する第２の符合情報送信手段と、を具備したことを特徴とする認証サーバを提供する（第２の構成の認証サーバ）。

ここで、前記符合情報生成手段は、前記取得した登録情報に含まれる認証情報の少なくとも一部からなる元データを所定のロジックにより割符化することにより、何れか一方だけでは前記元データを復元不能となるように、前記第１の符合情報と前記第２の符合情報を生成するように構成することができる。

また、本実施の形態は、前記目的を達成するために、第１の構成の認証サーバに第１の符合情報を特定する特定情報と第２の符合情報を送信する端末を提供する（第１の構成の端末）。

この端末は、前記特定情報を記憶した第１の可搬式記憶媒体から前記特定情報を取得して前記認証サーバに送信する特定情報送信手段と、第２の可搬式記憶媒体から前記第２の符合情報を取得して前記認証サーバに送信する第２の符合情報送信手段と、を具備するように構成することができる。

また、第１の構成の端末で、前記第１の可搬式記憶媒体、または前記第２の可搬式記憶媒体のうち少なくとも一方は、非接触型または接触型のＩＣカードとすることができる。

更に、前記特定情報の少なくとも一部は、前記ＩＣカード内に秘匿して格納されているように構成することもできる。

更に、本実施の形態は、前記目的を達成するために第２の構成の認証サーバに登録情報と特定情報を送信する端末を提供する（第２の構成の端末）。

ここで、この端末は、認証情報を取得して前記認証サーバに前記認証情報を含んだ登録情報を送信する登録情報送信手段と、第１の可搬式記憶媒体から特定情報を取得して前記認証サーバに送信する特定情報送信手段と、前記認証サーバから、第２の符合情報を受信して第２の可搬式記憶媒体に記憶する第２の符合情報記憶手段と、を具備するように構成することができる。

更に、前記第１の可搬式記憶媒体及び前記第２の可搬式記憶媒体のうち、少なくとも一方は非接触型または接触型のＩＣカードとすることができる。

また、本実施の形態は、前記目的を達成するために、第１の構成の端末に使用する可搬式記憶媒体であって、第２の符合情報を前記端末が読み出し可能に記憶したことを特徴とする可搬式記憶媒体を提供する。

更に、本実施の形態は、前記目的を達成するために、第１の可搬式記憶媒体から第１の符合情報を特定する特定情報を取得し、第２の可搬式記憶媒体から第２の符合情報を取得する端末から、前記特定情報と前記第２の符合情報を取得して認証を行う認証方法を提供する。

ここで、この認証方法は、特定情報取得手段と、第１の符合情報検索手段と、第２の符合情報取得手段と、認証情報取得手段と、認証手段と、を備えたコンピュータにおいて、前記特定情報取得手段で、前記端末から前記特定情報を取得する特定情報取得ステップと、前記第１の符合情報検索手段で、前記取得した特定情報を用いて前記第１の符合情報を検索する第１の符合情報検索ステップと、前記第２の符合情報取得手段で、前記端末から前記第２の符合情報を取得する第２の符合情報取得ステップと、前記認証情報取得手段で、前記検索した第１の符合情報と前記取得した第２の符合情報を用いて認証情報を取得する認証情報取得ステップと、前記認証手段で、前記取得した認証情報を用いて認証を行う認証ステップと、から構成することができる（第１の認証方法）。

ここで、前記コンピュータは、認証手段を具備し、前記認証ステップで認証した場合に

、前記認証手段で、前記端末から所定のサイトへのログイン処理を行うログインステップを備えるように構成することができる。

更に、第１の認証方法における前記第１の符合情報と前記第２の符合情報は、前記認証情報の少なくとも一部から成る元データを所定のロジックにより割符化し、何れか一方だけでは前記元データを復元不能に生成した電子割符であるように構成することができる。

この電子割符を用いた場合、前記認証情報取得ステップは、前記第１の符合情報と、前記第２の符合情報を用いて、前記元データを復元するように構成することができる。

更に、第１の認証方法で、前記コンピュータは、登録情報取得手段と、符合情報生成手段と、対応付け手段と、記憶手段と、第２の符合情報送信手段と、を備え、前記登録情報取得手段で、端末から認証情報を含んだ登録情報を取得する登録情報取得ステップと、前記符合情報生成手段で、前記取得した登録情報に含まれる認証情報を第１の符合情報と第２の符合情報を用いて特定可能となるように、前記第１の符合情報と前記第２の符合情報を生成する符合情報生成ステップと、前記対応付け手段で、前記端末から前記生成した第１の符合情報を検索するための特定情報を取得し、当該第１の符合情報と前記取得した特定情報を対応付ける対応付けステップと、前記記憶手段で、前記対応付けた前記第１の符合情報を記憶する記憶ステップと、前記第２の符合情報送信手段で、前記生成した第２の符合情報を前記端末に送信する第２の符合情報送信ステップと、を行うように構成することもできる。

ここで、前記符合情報生成ステップは、前記取得した登録情報に含まれる認証情報の少なくとも一部からなる元データを所定のロジックにより割符化することにより、何れか一方だけでは前記元データを復元不能となるように、前記第１の符合情報と前記第２の符合情報を生成するように構成することもできる。

また、本実施の形態は、前記目的を達成するために、第１の可搬式記憶媒体から第１の符合情報を特定する特定情報を取得し、第２の可搬式記憶媒体から第２の符合情報を取得する端末から、前記特定情報と前記第２の符合情報を取得して認証を行う認証方法で用いる認証情報登録方法を、

登録情報取得手段と、符合情報生成手段と、対応付け手段と、記憶手段と、第２の符合情報送信手段と、を備えたコンピュータにおいて、前記登録情報取得手段で、前記端末から認証情報を含んだ登録情報を取得する登録情報取得ステップと、前記符合情報生成手段で、前記取得した登録情報に含まれる認証情報を第１の符合情報と第２の符合情報を用いて特定可能となるように、前記第１の符合情報と前記第２の符合情報を生成する符合情報生成ステップと、前記対応付け手段で、前記端末から前記生成した第１の符合情報を検索するための特定情報を取得し、当該第１の符合情報と前記取得した特定情報を対応付ける対応付けステップと、前記記憶手段で、前記対応付けた前記第１の符合情報を記憶する記憶ステップと、前記第２の符合情報送信手段で、前記生成した第２の符合情報を前記端末に送信する第２の符合情報送信ステップと、から構成することができる（第１の認証情報登録方法）。

ここで、前記符合情報生成ステップは、前記取得した登録情報に含まれる認証情報の少なくとも一部からなる元データを所定のロジックにより割符化することにより、何れか一方だけでは前記元データを復元不能となるように、前記第１の符合情報と前記第２の符合情報を生成するように構成することができる。

更に、本実施の形態は、前記目的を達成するために、第１の構成の認証サーバに第１の符合情報を特定する特定情報と第２の符合情報を送信する端末が行う情報送信方法を提供する。ここで、前記端末は、特定情報送信手段と、第２の符合情報送信手段と、を備えており、前記特定情報送信手段で、前記特定情報を記憶した第１の可搬式記憶媒体から前記特定情報を取得して前記認証サーバに送信する特定情報送信ステップと、前記第２の符合情報送信手段で、第２の可搬式記憶媒体から前記第２の符合情報を取得して前記認証サーバに送信する第２の符合情報送信ステップと、から構成することができる（第１の情報送信方法）。

ここで、前記第１の可搬式記憶媒体、または前記第２の可搬式記憶媒体のうち少なくと

も一方は、非接触型または接触型のＩＣカードとすることができる。
また、このＩＣカードを用いる場合、前記特定情報の少なくとも一部は、前記ＩＣカード内に秘匿して格納されているように構成することができる。
また、本実施の形態は、前記目的を達成するために、第２の構成の認証サーバに登録情報と特定情報を送信する端末が行う情報送受信方法を提供する。
ここで、前記端末は、登録情報送信手段と、特定情報送信手段と、第２の符合情報記憶手段と、を備えており、前記登録情報送信手段で、認証情報を取得して前記認証サーバに前記認証情報を含んだ登録情報を送信する登録情報送信ステップと、前記特定情報送信手段で、第１の可搬式記憶媒体から特定情報を取得して前記認証サーバに送信する特定情報送信ステップと、前記第２の符合情報記憶手段で、前記認証サーバから、第２の符合情報を受信して第２の可搬式記憶媒体に記憶する第２の符合情報記憶ステップと、から構成することができる。
また、前記第１の可搬式記憶媒体及び前記第２の可搬式記憶媒体のうち、少なくとも一方は非接触型または接触型のＩＣカードとすることができる。
また、本実施の形態は、前記目的を達成するために、第１の可搬式記憶媒体から第１の符合情報を特定する特定情報を取得し、第２の可搬式記憶媒体から第２の符合情報を取得する端末から、前記特定情報と前記第２の符合情報を取得して認証を行うコンピュータで使用する認証プログラムを提供する。この認証プログラムは、コンピュータで、前記端末から前記特定情報を取得する特定情報取得機能と、前記取得した特定情報を用いて前記第１の符合情報を検索する第１の符合情報検索機能と、前記端末から前記第２の符合情報を取得する第２の符合情報取得機能と、前記検索した第１の符合情報と前記取得した第２の符合情報を用いて認証情報を取得する認証情報取得機能と、前記取得した認証情報を用いて認証を行う認証機能と、を実現させる（第１の構成の認証プログラム）。
更に、本実施の形態は、前記目的を達成するために、第１の可搬式記憶媒体から第１の符合情報を特定する特定情報を取得し、第２の可搬式記憶媒体から第２の符合情報を取得する端末から、前記特定情報と前記第２の符合情報を取得して認証を行うコンピュータで使用する認証プログラムを提供する。
ここで、この認証プログラムは、コンピュータで、前記端末から認証情報を含んだ登録情報を取得する登録情報取得機能と、前記取得した登録情報に含まれる認証情報を第１の符合情報と第２の符合情報を用いて特定可能となるように、前記第１の符合情報と前記第２の符合情報を生成する符合情報生成機能と、前記端末から前記生成した第１の符合情報を検索するための特定情報を取得し、当該第１の符合情報と前記取得した特定情報を対応付ける対応付け機能と、前記対応付けた前記第１の符合情報を記憶する記憶機能と、前記生成した第２の符合情報を前記端末に送信する第２の符合情報送信機能と、を実現させる（第２の構成の認証プログラム）。
また、本実施の形態は、前記目的を達成するために、第１の構成の認証サーバに第１の符合情報を特定する特定情報と第２の符合情報を送信する端末で使用する情報送信プログラムであって、前記特定情報を記憶した第１の可搬式記憶媒体から前記特定情報を取得して前記認証サーバに送信する特定情報送信機能と、第２の可搬式記憶媒体から前記第２の符合情報を取得して前記認証サーバに送信する第２の符合情報送信機能と、をコンピュータに実現させるための情報送信プログラムを提供する。
更に、本実施の形態は、前記目的を達成するために、第２の構成の認証サーバに登録情報と特定情報を送信する端末で使用する情報送受信プログラムであって、認証情報を取得して前記認証サーバに前記認証情報を含んだ登録情報を送信する登録情報送信機能と、第１の可搬式記憶媒体から特定情報を取得して前記認証サーバに送信する特定情報送信機能と、前記認証サーバから、第２の符合情報を受信して第２の可搬式記憶媒体に記憶する第２の符合情報記憶機能と、をコンピュータに実現させるための情報送信プログラムを提供する。
更に、本実施の形態は、前記目的を達成するために、前記第１の構成の認証プログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する。

また、本実施の形態は、前記目的を達成するために、前記第２の構成の認証プログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する。

加えて、本実施の形態は、前記目的を達成するために、前記情報送信プログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する。

また、本実施の形態は、前記目的を達成するために、前記情報送受信プログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する。

また、本実施の形態は、前記目的を達成するために、第１の記憶媒体に記憶された、サーバに格納される第１の符合情報を特定するための特定情報と、第２の記憶媒体に記憶された第２の符合情報とに基づいて、認証を行なう情報処理装置において、前記特定情報と第１の符合情報をひも付けて記憶する記憶手段と、前記第１の記憶媒体に記憶された前記特定情報と前記第２の記憶媒体に記憶された第２の符合情報を受信する受信手段と、前記受信手段で受信した前記特定情報にひも付けられた第１の符合情報を前記記憶手段から検索する検索手段と、前記検索手段で検索した第１の符合情報と、前記受信手段で受信した前記第２の符合情報とを用いて認証情報を得る認証情報獲得手段と、を備えたことを特徴とする情報処理装置を提供する（第１の構成の情報処理装置）。

ここで、第１の構成の情報処理装置において、前記特定情報は、前記第１の記憶媒体を識別する記憶媒体識別番号であるように構成することができる。

また、第１の構成の情報処理装置において、前記特定情報は、認証を要求するユーザを識別するユーザ識別番号であるように構成することができる。

更に、第１の構成の情報処理装置において、前記第１の記憶媒体は、非接触型カードまたは接触型カードであるように構成することができる。ここて、この非接触型カード、接触型カードは、ＩＣカードで構成することもできる。

第１の構成の情報処理装置が、前記認証情報獲得手段において得られた認証情報に基づいて、認証を行なう認証手段を更に備えるように構成することもできる。

加えて、本実施の形態は、前記目的を達成するために、第１の記憶媒体に記憶された、サーバに格納される第１の符合情報を特定するための特定情報と、第２の記憶媒体に記憶された第２の符合情報とに基づいて、認証を行なう情報処理方法であって、記憶手段と、受信手段と、検索手段と、認証情報獲得手段と、を備えたコンピュータにおいて、前記記憶手段で、前記特定情報と第１の符合情報をひも付けて記憶する記憶ステップと、前記受信手段で、前記第１の記憶媒体に記憶された前記特定情報と前記第２の記憶媒体に記憶された第２の符合情報を受信する受信ステップと、前記検索手段で、前記受信手段で受信した前記特定情報にひも付けられた第１の符合情報を前記記憶手段から検索する検索ステップと、前記認証情報獲得手段で、前記検索手段で検索した第１の符合情報と、前記受信手段で受信した前記第２の符合情報とを用いて認証情報を得る認証情報獲得ステップと、から構成されたことを特徴とする情報処理方法を提供する。

また、本実施の形態は、前記目的を達成するために、第１の記憶媒体からサーバに格納される第１の符合情報を特定するための特定情報と、第２の記憶媒体から第２の符合情報とに基づいて、認証を行なう情報処理装置において、前記特定情報と第１の符合情報を紐付けて記憶する記憶手段と、前記第１の記憶媒体から前記特定情報または第２の符合情報を受信する受信手段と、前記受信手段において受信された前記特定情報に対応する第１の符合情報を前記記憶手段から検索する検索手段と、前記検索手段によって検索された第１の符合情報と前記第２の符合情報とから得られる認証情報を得る認証情報獲得手段と、を備えることを特徴とする情報処理装置を提供することもできる（第２の構成の情報処理装置）。

【００９１】

（第２の実施の形態）

以下、本発明の好適な第２の実施の形態について、図を参照しながら詳細に説明する。

（１）第２の実施形態の概要

図２０は、第２の実施の形態に係る自動ログインシステムの概要を説明するための概念図である。

本実施の形態の自動ログインシステム１００は、ＩＣカード１０に記憶されているカード固有情報１０１と、携帯メモリ１１に記憶されているパスワード情報１０２を用いてユーザ認証の要求を行い、自動ログインを行うものである。

サーバ１１０では、カード固有情報１０１とパスワード情報１０２を用いてユーザＩＤとパスワードを取得し、ユーザ認証を行う。この場合、カード固有情報１０１とパスワード情報１０２が認証要求情報を構成し、ユーザＩＤとパスワードが認証情報を構成している。

【００９２】

サーバ１１０は、認証情報を検索するための記憶した認証情報データベース１２０を備えている。

認証情報データベース１２０の論理的な構成は、図２２（ｂ）のようになっており、カード固有情報１０１に携帯メモリＩＤ１０３、パスワード情報１０２、ユーザＩＤ１０６が紐付けられており、更にパスワード情報１０２にはパスワード１０５が紐付けられている。

【００９３】

ユーザは、サーバ１１０に認証要求を行う場合、端末３にＩＣカード１０と携帯メモリ１１をセットし、サーバ１１０にカード固有情報１０１、パスワード情報１０２、及び携帯メモリＩＤ１０３を送信する。

サーバ１１０は、これらの情報を受信し、まず、受信したパスワード情報１０２と携帯メモリＩＤ１０３の組合せが、認証情報データベース１２０で紐付けされているものと一致することを確認し、パスワード情報１０２が認証情報データベース１２０で登録してある携帯メモリに記憶されているものであることを確認する。

【００９４】

次に、サーバ１１０は、認証情報データベース１２０を用いてパスワード情報１０２とカード固有情報１０１の組合せからパスワード１０５を取得し、カード固有情報１０１からユーザＩＤ１０６を取得する。

このように、パスワード情報１０２とカード固有情報１０１の組合せから、ユーザＩＤ１０６を取得することにより、ユーザの使用したＩＣカード１０が予め認証情報データベース１２０に登録したものであることを確認すると共に、ＩＣカード１０と携帯メモリ１１の組合せが予め認証情報データベース１２０に登録したものであることを確認することができる。

また、本実施の形態では、受信したパスワード情報１０２とカード固有情報１０１の組合せからパスワード１０５を取得したが、パスワード情報１０２からパスワード１０５を取得しても良い。

【００９５】

そして、サーバ１１０は、これら取得したユーザＩＤ１０６とパスワード１０５を用いてユーザ認証を行う。

そして、サーバ１１０は、ユーザ認証が成功した場合、当該ユーザのログイン処理を行い、認証が成功しなかった場合はログイン処理を行わない。

【００９６】

なお、パスワード情報１０２は、パスワード１０５と紐付けられた情報であり、認証ごとに生成されて使い捨てで使用される、所謂ワンタイムパスワードである。

サーバ１１０は、ユーザの認証を終えると、新たにパスワード情報１０２を生成して端末３に送信し、端末３は、これを受信して携帯メモリ１１に書き込む。

今回書き込まれたパスワード情報１０２が次回のユーザ認証時に使用される。

【００９７】

（２）第２の実施の形態の詳細

図２１は、第２の実施の形態に係る自動ログインシステム１００のネットワーク構成の一例を示した図である。

自動ログインシステム１００のネットワーク構成は、先に説明した自動ログインシステ

ム１と同じであり、サービスサイトが開設されたサーバ１１０、サービスサイトを利用する端末３、及び端末３とサーバ５をネットワーク接続するためのインターネット２を備えている。

以下では、先に説明した実施の形態と同じ構成要素には同じ符合を付すこととし、重複する説明は簡略化、もしくは省略する。

【００９８】

端末３、リーダライタ７、携帯メモリ駆動装置８、ＩＣカード１０、及び携帯メモリ駆動装置８の構成は、先に説明した実施の形態と同じである。

端末３は、リーダライタ７を介して非接触にてＩＣカード１０に対してデータの読み書きを行うことができ、また、携帯メモリ駆動装置８を介して携帯メモリ１１を駆動し、携帯メモリ１１に対してデータの読み書きを行うことができる。

【００９９】

ＩＣカード１０（図２０）には、このＩＣカード１０に固有なカード固有情報１０１（即ち、他のＩＣカードから当該ＩＣカード１０を識別することができる識別情報）を記憶している。

カード固有情報１０１としては、例えば、カードＩＤ、ＩＣカード１０が備えた電子マネー機能に付与された電子マネーＩＤ、その他のＩＤ情報や、これらの組合せ（例えば、カードＩＤと電子マネーＩＤ）を用いことができる。

【０１００】

また、図示しないが、ＩＣカード１０にはその他のカード情報を記憶しており、カード固有情報１０１とカード情報との組合せをサーバ１１０で確認するように構成するとセキュリティレベルを更に高めることができる。

ここで、ＩＣカード１０は、第１の記憶媒体を構成しており、カード固有情報１０１は、第１の記憶媒体を識別する第１の識別情報を構成している。

【０１０１】

携帯メモリ１１は、サーバ１１０が発行したパスワード情報１０２とこの携帯メモリ１１に固有なＩＤ情報である携帯メモリＩＤ１０３を記憶している（図２０）。

なお、パスワード情報１０２は、後述するように複数のパスワード情報を記憶し、各種の使用形態で用いることが可能である。

ここで、携帯メモリ１１は、第２の記憶媒体を構成し、パスワード情報１０２は、認証情報と関連づけられた符合情報を構成し、携帯メモリＩＤ１０３は、第２の記憶媒体を識別する第２の識別情報を構成している。

【０１０２】

端末３は、リーダライタ７（図２１）と携帯メモリ駆動装置８にセットされたＩＣカード１０と携帯メモリ１１からそれぞれカード固有情報１０１とパスワード情報１０２、及び携帯メモリＩＤ１０３を読み出してサーバ１１０に送信することができる。

【０１０３】

ここで、携帯メモリＩＤ１０３は、携帯メモリ１１がサーバ１１０でこのユーザのものとして登録されているものであることを確認するために必要とされるものであり、ユーザ認証の要求は、カード固有情報１０１とパスワード情報１０２により行われる。

このように、ユーザは、ＩＣカード１０と携帯メモリ１１を端末３にセットしてユーザ認証を要求することができ、入力画面などからユーザＩＤやパスワードを入力するといった作業を行わずにサーバ１１０にログインすることができる。

【０１０４】

サーバ１１０は、登録部１３ａ、自動ログイン部１５ａ、サービスサイト１７ａなどの各種機能部や、認証情報データベース１２０などの各種データベースを備えている。

サーバ１１０は、ユーザの認証処理を行う認証サーバとしての機能を有している。第２の実施の形態では、ユーザの認証処理とサービスの提供をサーバ１１０で行うが、認証処理を行う認証サーバとサービスの提供を行うサービスサーバを別体としてシステムを構成することもできる。この場合、サービスサーバは、認証サーバで認証されたユーザにサー

ビスの提供を行う。

【０１０５】

自動ログイン部１５ａは、端末３から送信されてきたカード固有情報１０１とパスワード情報１０２を用いて認証処理を行い、認証されたユーザに対してはログイン処理を行う。

詳細は後述するが、自動ログイン部１５ａは、カード固有情報１０１とパスワード情報１０２を用いて認証情報データベース１２０に記憶されているユーザＩＤとパスワードを検索し、検索された認証情報を用いてユーザ認証を行う。

【０１０６】

登録部１３ａは、サービスサイト１７ａを利用したい新規のユーザを登録する機能部である。登録部１３ａにより登録されたユーザに対して自動ログイン部１５ａはユーザ認証を行う。

認証情報データベース１２０は、認証情報を検索するための情報やユーザの個人情報などに関するユーザ情報を記憶しているデータベースである。認証情報データベース１２０に関しては、後ほど詳細に説明する。

【０１０７】

図２２（ａ）は、自動ログイン部１５ａの機能的な構成を模式的に示したブロック図である。

自動ログイン部１５ａは、端末アクセス部１３１、パスワード情報確認部１３２、認証情報検索部１３３、認証部１３４、パスワード情報生成部１３５などを備えている。

【０１０８】

端末アクセス部１３１は、端末３とのデータの送受信を行う。

より詳細には、アクセスしてきた端末３に対してログイン画面データを送信したり、ログイン画面に応じて端末３から送信されてきたカード固有情報１０１、パスワード情報１０２、及び携帯メモリＩＤ１０３を受信したり、パスワード情報生成部１３５が生成したパスワード情報を端末３に送信したりする。

端末アクセス部１３１は、媒体情報受信手段を構成している。

【０１０９】

また、端末アクセス部１３１は、同一の端末３からカード固有情報１０１、パスワード情報１０２、及び携帯メモリＩＤ１０３が送信されてきたことを確認するように構成することもできる。

この場合、自動ログイン部１５ａは、異なる端末３からこれらの情報が別々に送信されてきた場合は認証を行わないように構成され、これによってセキュリティが高めることができる。

【０１１０】

パスワード情報確認部１３２は、端末アクセス部１３１からパスワード情報１０２と携帯メモリＩＤ１０３を受け取り、パスワード情報１０２が認証情報データベース１２０に当該ユーザのものとして登録してある携帯メモリ１１から読み出されたものか確認する。これにより、携帯メモリ１１から他の携帯メモリにパスワード情報１０２をコピーして使用することができなくなり、セキュリティレベルを高めることができる。

【０１１１】

また、パスワード情報確認部１３２は、端末アクセス部１３１からカード固有情報１０１を取得して、ユーザが使用したＩＣカード１０が認証情報データベース１２０に当該ユーザのものとして登録されているか否かを確認したり、あるいは、携帯メモリＩＤ１０３とカード固有情報１０１の組、又はパスワード情報１０２と携帯メモリＩＤ１０３の組がパスワード情報１０２で登録された組であるか否かを確認するように構成することもできる。

なお、第２の実施の形態では、これらの確認処理を認証情報検索部１３３で認証情報の検索と共に行う。

【０１１２】

ここで、認証情報データベース１２０の構成について説明する。
図２２（ｂ）は、認証情報データベース１２０に記憶されているあるユーザの認証情報などの論理的な関係を示した図である。
認証情報データベース１２０は、各ユーザごとに、カード固有情報１０１、パスワード情報１０２、携帯メモリＩＤ１０３、パスワード１０５、ユーザＩＤ１０６を関連づけて記憶している。
【０１１３】
図に示したように、カード固有情報１０１は、パスワード情報１０２、携帯メモリＩＤ１０３、ユーザＩＤ１０６のそれぞれと紐付けされており、パスワード情報１０２は、更にパスワード１０５と紐付けされている。
サーバ１１０は、カード固有情報１０１と携帯メモリＩＤ１０３を紐付けて認証情報データベース１２０に記憶することにより、ユーザの使用するＩＣカード１０と携帯メモリ１１の組合せを予め登録することができる。
【０１１４】
そして、これら紐付けされた関係により、カード固有情報１０１からユーザＩＤ１０６を特定し、パスワード情報１０２からパスワード１０５を特定することができる。ユーザ認証は、このユーザＩＤ１０６とパスワード１０５により行われる。
この場合、ユーザＩＤ１０６は、第１の識別情報（カード固有情報１０１）に関連付けられた第１の認証情報を構成し、パスワード１０５は、符合情報（パスワード情報１０２）に関連づけられた第２の認証情報を構成している。
【０１１５】
また、パスワード情報１０２は、毎回認証を行う度に新しいものに更新され、ワンタイムパスワードとして使用される。
このように、パスワード情報１０２を毎回使い捨ての情報とすることでセキュリティレベルを高めることができる。また、第三者に携帯メモリ１１が渡ったとしても、第三者はパスワード１０５を知ることはできない。
【０１１６】
なお、図２２（ｂ）に示した紐付けは、カード固有情報１０１、パスワード情報１０２、携帯メモリＩＤ１０３、パスワード１０５、ユーザＩＤ１０６の関連づけを限定するものではなく、何れか１つから他の情報が導き出せるように紐付けすればよい。
また、カード固有情報１０１とパスワード情報１０２が紐付けられていなくても、カード固有情報１０１からユーザＩＤ１０６が検索でき、パスワード情報１０２からパスワード１０５が検索できれば、ユーザ認証を行うことは可能である
また、図示しないが、認証情報データベース１２０には、これら認証情報の他にユーザの個人情報（氏名、年齢、性別、住所、勤務先、趣味など）なども格納されている。
【０１１７】
図２２（ａ）に戻り、パスワード情報確認部１３２は、端末アクセス部１３１から受け取ったパスワード情報１０２と携帯メモリＩＤ１０３の組合せを認証情報データベース１２０で検索し、紐付けされた同一のパスワード情報１０２と携帯メモリＩＤ１０３（認証情報データベース１２０においては、パスワード情報１０２と携帯メモリＩＤ１０３は、カード固有情報１０１を介して紐付けられている）があるか否かを判断する。
そして、判断結果を認証情報検索部１３３に提供する。
【０１１８】
認証情報検索部１３３は、パスワード情報確認部１３２から確認結果を受け取る。
この確認結果がパスワード情報１０２と携帯メモリＩＤ１０３の組合せが認証情報データベース１２０で確認できたものである場合、パスワード情報確認部１３２は、認証情報の検索を行い、確認結果が、パスワード情報１０２と携帯メモリＩＤ１０３の組合せが認証情報データベース１２０で確認できなかったものである場合、自動ログイン部１５ａは、認証情報の検索を行わずに認証処理を終了する。
【０１１９】

また、パスワード情報確認部１３２で、ＩＣカード１０が登録してあるか否か、あるいは、ＩＣカード１０と携帯メモリ１１の組合せが登録してあるか否かを確認する場合、認証情報検索部１３３は、これらの確認ができた場合に認証情報の検索を行い、確認できなかった場合、自動ログイン部１５ａは、認証処理を終了する。

【０１２０】

認証情報検索部１３３は、認証情報の検索を行う場合、端末アクセス部１３１からカード固有情報１０１とパスワード情報１０２を取得し、これらの組を用いて認証情報データベース１２０からユーザＩＤ１０６とパスワード１０５を検索し、認証部１３４に提供する。

もし、カード固有情報とパスワード情報の組合せが、認証情報データベース１２０で登録したものと異なっている場合は、認証情報を検索することはできない。

【０１２１】

例えば、パスワードがパスワード情報１０２であっても、これと組合せになっているカード固有情報が、カード固有情報１０１と異なるものである場合は、パスワード１０５を検索することはできない。

このように、カード固有情報１０１とパスワード情報１０２の組合せを用いてパスワード１０５とユーザＩＤ１０６を検索することにより、ユーザが使用しているＩＣカード１０と携帯メモリ１１が認証情報データベース１２０で登録してあるものか否かの確認も行うことができる。また、ユーザが使用したＩＣカードがＩＣカード１０であることも確認することができる。

【０１２２】

認証部１３４は、認証情報検索部１３３から認証情報（ユーザＩＤ１０６とパスワード１０５）を取得し、これを用いてユーザを認証する。

図示しないが、サーバ１１０は、認証処理で使用するために、各ユーザのユーザＩＤとパスワードをユーザ毎に関連づけて記憶したデータベースを備えており、認証部１３４は、認証情報検索部１３３が検索したユーザＩＤ１０６とパスワード１０５をこのデータベースに記憶してあるユーザＩＤとパスワードと照合することにより認証処理を行う。

ユーザが認証された場合は、認証部１３４は、ユーザのサービスサイトへのログイン処理を行う。一方、ユーザが認証されなかった場合はログイン処理を拒否し、端末３にエラーメッセージを送信する。

【０１２３】

パスワード情報生成部１３５は、認証部１３４がユーザ認証を終えると、新規のパスワード情報１０２を生成し、これを端末アクセス部１３１を介して端末３に送信すると共に、認証情報データベース１２０に記憶されている使用済みのパスワード情報１０２を、新規のパスワード情報１０２で置き換える。

自動ログイン部１５ａは、次回にユーザ認証を行う場合には、新規のパスワード情報１０２を用いてユーザ認証の要求を受け付ける。

【０１２４】

このように、パスワード情報生成部１３５と端末アクセス部１３１は、符合情報（パスワード情報１０２）を生成して端末３に送信する符合情報送信手段を構成している。

そして、パスワード情報生成部１３５は、生成した符合情報を認証情報データベース１２０（記憶装置）に記憶する記憶手段も構成している。

【０１２５】

一方、端末３は、サーバ１１０から新規のパスワード情報１０２を受信すると、これを用いて携帯メモリ１１に記憶されているパスワード情報１０２（今回のユーザ認証要求に使用したもの）を置き換える。

これにより、次回にユーザ認証を要求する際には、新たらしく発行されたパスワード情報１０２を用いることができる。

このように、端末３は、端末３にカード固有情報１０１やパスワード情報１０２などを送信する媒体情報送信手段を備える他、サーバ１１０から符合情報（パスワード情報１０

２）を受信する符合情報受信手段と、受信したパスワード情報１０２で、現在携帯メモリ１１に記憶されているパスワード情報１０２を置き換える置き換え手段を備えている。

【０１２６】

図２３は、自動ログインシステム１００において、ユーザが端末３からサービスサイト１７ａ（図２１）にログインする手順を説明するためのフローチャートである。

以下の動作は、端末３に搭載したＣＰＵとサーバ１１０に搭載したＣＰＵが所定のプログラムに従って行うものである。

まず、ユーザがブラウザ上でサービスサイト１７ａのＵＲＬを入力するなどし、端末３からサーバ１１０にアクセスする（ステップ２１０５）。

【０１２７】

次に、端末アクセス部１３１は、自動ログイン機能を端末３で実現する補助プログラムを端末３に送信する（ステップ２４０５）。

この補助プログラムは、例えば、ユーザが端末３からサービスサイト１７ａにアクセスした際に、ＩＣカード１０からカード固有情報１０１を読み込んだり、携帯メモリ１１からパスワード情報１０２や携帯メモリＩＤ１０３を読み込んだり、更に、これら読み込んだカード固有情報１０１、パスワード情報１０２、携帯メモリＩＤ１０３をサーバ１１０に送信したり、あるいは、サーバ１１０が発行して送信してきたパスワード情報１０２を受信し、これを用いて携帯メモリ１１に記憶されているパスワード情報１０２を置き換えるなどする機能を端末３に発揮させるものである。

なお、例えば、２回目以降にサーバ１１０にアクセスする場合のように、端末３に既に補助プログラムがインストールされている場合は、サーバ１１０はステップ２４０５の補助プログラムの送信を行わない。

【０１２８】

次に、端末３は、補助プログラムを受信してインストールする。そして、この補助プログラムに従ってリーダライタ７を駆動してＩＣカード１０にアクセスする（ステップ２１１０）。

次に、ＩＣカード１０は、リーダライタ７と非接触で通信を行うことにより、端末３にカード固有情報１０１を送信する（ステップ２２０５）。

端末３は、リーダライタ７を介してカード固有情報１０１を取得し、これをサーバ１１０に送信する（ステップ２１１５）。

サーバ１１０では、端末アクセス部１３１がカード固有情報１０１を受信する（ステップ２４１０）。

【０１２９】

次に、端末３は、携帯メモリ駆動装置８を駆動して携帯メモリ１１からパスワード情報１０２と携帯メモリＩＤ１０３の読み取りを行う（ステップ２１２０）。

これに対し、携帯メモリ１１は、格納しているパスワード情報１０２と携帯メモリＩＤ１０３を携帯メモリ駆動装置８を介して端末３に提供する（ステップ２３０５）。

端末３は、携帯メモリ１１から取得したパスワード情報１０２と携帯メモリＩＤ１０３をサーバ１１０に送信する（ステップ２１２５）。

次に、サーバ１１０では、端末アクセス部１３１がパスワード情報１０２と携帯メモリＩＤ１０３を受信する（ステップ２４１５）。

【０１３０】

なお、端末３がカード固有情報１０１、パスワード情報１０２、及び携帯メモリＩＤ１０３の読み取りを行い、これらを一時にサーバ１１０に送信するように構成してもよい。

あるいは、パスワード情報１０２、携帯メモリＩＤ１０３をサーバ１１０に送信した後、カード固有情報１０１をサーバ１１０に送信するように構成してもよい。

【０１３１】

次に、パスワード情報確認部１３２（図２２）が、端末アクセス部１３１からパスワード情報１０２と携帯メモリＩＤ１０３を受け取り、この組合せを認証情報データベース１２０で検索する。

【０１３２】
そして、認証情報検索部１３３は、認証情報データベース１２０で紐付けされた同一のパスワード情報１０２と携帯メモリＩＤ１０３があることを確認することにより、ユーザが使用している携帯メモリ１１が認証情報データベース１２０で登録されているものであり、更に、その登録されている携帯メモリ１１に設定されているパスワード情報１０２と、端末３から送信されてきたパスワード情報１０２が同一であることを確認する（ステップ２４２０）。
これにより、端末３から送信されてきた情報が、登録された携帯メモリ１１のパスワード情報１０２であることが確認できる。
【０１３３】
なお、このとき、ＩＣカード１０が登録されたものであり、また、ＩＣカード１０と携帯メモリ１１の組合せが登録されたものであることを確認するように構成することもできる。
ＩＣカード１０が登録されたものであるか否かの確認は、例えば、カード固有情報１０１を認証情報データベース１２０で検索してＩＣカード１０が登録されているものか否か確認したり、あるいは、ＩＣカード１０のカード情報を認証情報データベース１２０で記憶しておき、カード固有情報１０１とカード情報の一致を確認することにより行うことができる。
更に、ＩＣカード１０が登録されていなかった場合、カード使用を一定時間ロックするように構成することもできる。
【０１３４】
次に、認証情報検索部１３３が、端末アクセス部１３１からカード固有情報１０１とパスワード情報１０２を受け取り、この組合せを用いて認証情報データベース１２０からユーザＩＤ１０６を検索する（ステップ２４２５）。
なお、カード固有情報１０１だけを用いてもユーザＩＤ１０６を検索することは可能であるが、カード固有情報１０１とパスワード情報１０２の組を用いて検索することにより、ユーザが登録済みの所定のＩＣカード１０と携帯メモリ１１を用いていることを確かめることができる。
次に、認証情報検索部１３３は、パスワード情報１０２を用いて認証情報データベース１２０からパスワード１０５を検索する（ステップ２４３０）。
【０１３５】
次に、認証部１３４が認証情報検索部１３３から検索したユーザＩＤ１０６とパスワード１０５を受け取り、ユーザ認証を行う（ステップ２４３５）。
ユーザが認証された場合、サーバ１１０は、ログイン後画面データ（ログイン後に端末３のブラウザ上で表示する画面のデータ）を端末３に送信する（ステップ２４４０）。
端末３は、ログイン後画面データを受信し、ブラウザがこれを用いてログイン後画面を表示する（ステップ２１３０）。
なお、ユーザが認証されなかった場合は、サーバ１１０は端末３にエラーメッセージ画面データを送信する。
【０１３６】
次に、パスワード情報生成部１３５が新規のパスワード情報１０２を生成し、認証情報データベース１２０に記憶されているパスワード情報１０２をこれで置き換える。
更に、パスワード情報生成部１３５は、生成した新規のパスワード情報１０２を、端末アクセス部１３１を介して端末３に送信する（ステップ２４４５）。
【０１３７】
端末３は、サーバ１１０から送信されてきたパスワード情報１０２を受信し、携帯メモリ駆動装置８を駆動してこれを携帯メモリ１１に書き込む（ステップ２１３５）。
これにより、携帯メモリ１１に記憶してあるパスワード情報１０２は、新規のパスワード情報１０２で更新される（ステップ２３１０）。
なお、新規のパスワード情報１０２の置き換えが失敗した場合、端末３は、これを検知

してサーバ１１０に通知すると共に、置き換えが失敗した旨の通知をユーザに発するように構成することもできる。

【０１３８】

なお、第２の実施の形態では、毎回パスワード情報１０２を更新し使い捨てとしたが、パスワード情報１０２の更新は行わず、毎回同じパスワード情報１０２を使用するように構成することもできる。この場合、パスワード情報１０２の生成や更新といった情報処理は必要なくなる。

【０１３９】

また、第２の実施の形態では、携帯メモリ１１にパスワード情報１０２を記憶し、ユーザ認証は、パスワード情報１０２に関連づけたパスワード１０５を用いるように構成したが、これに限定せず、パスワード１０５を携帯メモリ１１に記憶し、これを用いてユーザ認証を行うように構成することもできる。

また、ステップ２４４５以降の処理をオプションとし、ユーザ又は、サーバ１１０を運営する事業者側が選択できるように構成することもできる。

【０１４０】

以上に説明した認証処理において、パスワード情報不整合対策として、認証に失敗した場合、パスワード情報１０２を認証情報データベース１２０から物理削除し、パスワード情報１０２を再生成するように構成することもできる。

【０１４１】

次に、図２４のフローチャートを用いてユーザをサービスサイト１７ａのユーザとして登録する場合について説明する。

図２４は、登録部１３ａが自動ログインシステム１００において、ユーザが端末３からサービスサイト１７ａのユーザとしてユーザ登録する手順を説明するためのフローチャートである。

以下の動作は、端末３に搭載したＣＰＵとサーバ１１０に搭載したＣＰＵが所定のプログラムに従って行うものである。

【０１４２】

まず、端末３からサーバ１１０にアクセスする（ステップ２５０５）。そして、サーバ１１０から送られてくるトップページなどで新規登録ボタンをクリックするなどして、サーバ１１０に新規登録したい旨の情報をサーバ１１０に送信する。

すると、サーバ１１０では、登録部１３ａが登録画面データを端末３に送信する（ステップ２８０５）。

【０１４３】

次に、端末３では、登録画面データを受信し、ブラウザがこれを用いて入力事項を入力可能に表示する。ユーザは、表示された登録画面にパスワード１０５やユーザＩＤ１０６、その他個人情報などを入力してサーバ１１０に送信する（ステップ２５１０）。

なお、ユーザが既にユーザＩＤ１０６を持っている場合は登録画面からこれを入力するが、ユーザがユーザＩＤ１０６を持っていない場合は、ユーザが登録することによってユーザＩＤ１０６を取得するか、サーバ１１０側で自動的に設定してもよい。

次に、登録部１３ａは、端末３から受信した情報（パスワード１０５、ユーザＩＤ１０６、その他の情報）を用いて認証情報データベース１２０を更新し、ユーザ情報を新規に登録する（ステップ２８１０）。

【０１４４】

次に、登録部１３ａの端末アクセス部４１は、補助プログラムを端末３に送信する（ステップ２８１５）。補助プログラムは、ユーザの登録時においては、端末３でＩＣカード１０からカード固有情報１０１などを読み取ってサーバ１１０に送信したり、携帯メモリ１１から携帯メモリＩＤ１０３を読み取ってサーバ１１０に送信したり、あるいは、サーバ１１０が発行したパスワード情報１０２を携帯メモリ１１に書き込んだりなどする。

なお、補助プログラムが既にインストールされている場合や、ブラウザに補助プログラムが組み込まれている場合は、このステップを省略することができる。

【０１４５】
次に、端末３は、サーバ１１０から受信した補助プログラムをインストールする。そして、端末３は、補助プログラムに従ってリーダライタ７を駆動し、ＩＣカード１０からカード固有情報１０１の読み取りを開始する（ステップ２５１５）。
次に、リーダライタ７にセットされているＩＣカード１０が、非接触にて端末３にカード固有情報１０１を送信する（ステップ２６０５）。
次に、端末３は、ＩＣカード１０から読み取ったカード固有情報をサーバ１１０に送信する（ステップ２５２５）。
【０１４６】
次に、サーバ１１０では、登録部１３ａがカード固有情報１０１を受信する（ステップ２８２０）。
次に、登録部１３ａは、カード固有情報１０１をステップ２８１０で認証情報データベース１２０に記憶したユーザＩＤ１０６と紐付けて認証情報データベース１２０に記憶する（ステップ２８２５）。
そして、登録部１３ａは、端末３に対して携帯メモリＩＤ１０３の送信を要求する（ステップ２８３０）。
【０１４７】
端末３は、この要求を受け、携帯メモリ駆動装置８を駆動して携帯メモリ１１から携帯メモリＩＤ１０３を読み出す（ステップ２５２７）。
これに対し、携帯メモリ１１は、携帯メモリＩＤ１０３を端末３に提供する（ステップ２７０５）。
そして、端末３は、これをサーバ１１０に送信する（ステップ２５２８）。
サーバ１１０では、登録部１３ａが携帯メモリＩＤ１０３を受信する。そして、登録部１３ａは、この携帯メモリＩＤ１０３を、ステップ２８２５で記憶したカード固有情報１０１に紐付けて認証情報データベース１２０に記憶する（ステップ２８４０）。
【０１４８】
次に、登録部１３ａは、パスワード情報１０２を生成し、ステップ２８２５で記憶したカード固有情報１０１に紐付けてパスワード情報１０２を認証情報データベース１２０に記憶する（ステップ２８４３）。
そして、更にステップ２８１０で記憶したパスワード１０５をパスワード情報１０２に紐付けた後、パスワード情報１０２を端末３に送信する（ステップ２８４５）。
【０１４９】
端末３は、サーバ１１０からパスワード情報１０２を受信する（ステップ２５３０）。
次に、端末３は、携帯メモリ駆動装置８を駆動し、受信したパスワード情報１０２を携帯メモリ１１に書き込む（ステップ２５３５）。
そして、携帯メモリ１１は、パスワード情報１０２を記憶する（ステップ２７１０）。
次に、登録部１３ａは、登録完了通知を端末３に送信する（ステップ２８５０）。
端末３は、この登録完了通知を受信し、ブラウザにより登録完了通知が表示される（ステップ２５４０）。
【０１５０】
以上の情報処理により、新規ユーザに関するカード固有情報１０１、パスワード情報１０２、携帯メモリＩＤ１０３、パスワード１０５、ユーザＩＤ１０６を図２２（ｂ）に示したように紐付けすることができ、更に、ユーザの携帯メモリ１１にパスワード情報１０２を記憶させることができる。
このように、登録部１３ａは、第１の識別情報（カード固有情報１０１）と、符合情報（パスワード情報１０２）に基づいて認証情報を登録する認証情報登録手段を構成している。
【０１５１】
携帯メモリ１１には、複数のパスワード情報１０２を記憶することができ、これを利用して、ＩＣカード１０と携帯メモリ１１の様々な利用形態が考えられる。

このような形態としては、例えば、１人のユーザが複数のＩＣカード１０を有する場合や、複数のユーザが１つの携帯メモリ１１を共通利用する場合などがある。

次に、これらの利用形態のいくつかを例示する。

【０１５２】

図２５は、ユーザが単数の場合の利用形態を例示した図である。

図２５（ａ）は、ユーザが一枚のＩＣカード１０と１つの携帯メモリ１１を利用する場合であり、携帯メモリ１１には、ＩＣカード１０のカード固有情報Ａに紐付けされたパスワード情報Ａが記憶されている。

サーバ１１０において、パスワード情報ＡとユーザのユーザＩＤ１は、カード固有情報Ａと紐付けられている。

この場合、ユーザは、ＩＣカード１０と携帯メモリ１１を用いてユーザ認証を受け、サービスサイト１７ａにログインすることができる。

【０１５３】

図２５（ｂ）は、ユーザが２組のＩＣカード１０ａ、携帯メモリ１１ａ、及びＩＣカード１０ｂ、携帯メモリ１１ｂを有する場合である。

携帯メモリ１１ａには、ＩＣカード１０ａのカード固有情報Ａと紐付けされたパスワード情報Ａが記憶されており、また、携帯メモリ１１ｂには、ＩＣカード１０ｂのカード固有情報Ｂと紐付けされたパスワード情報Ｂが記憶されている。

サーバ１１０において、パスワード情報ＡとユーザＩＤ１は、カード固有情報Ａと紐付けられており、また、パスワード情報ＢとユーザＩＤ１は、カード固有情報Ｂと紐付けられている。

【０１５４】

ユーザは、ＩＣカード１０ａと携帯メモリ１１ａの組合せを用いてユーザ認証を受けることができ、また、ＩＣカード１０ｂと携帯メモリ１１ｂの組合せを用いてユーザ認証を受けることができる。

しかし、ＩＣカード１０ａと携帯メモリ１１ｂの組合せ、及びＩＣカード１０ｂと携帯メモリ１１ａの組合せではユーザ認証を受けることはできない。

【０１５５】

このように２組のＩＣカード１０と携帯メモリ１１を有する場合、それぞれの組を別のサービスのユーザ認証に用いるように登録することができる。

例えば、ＩＣカード１０ａと携帯メモリ１１ａの組合せを銀行サービスサイトのユーザ認証用に登録し、ＩＣカード１０ｂと携帯メモリ１１ｂの組合せを通信販売サイトのユーザ認証用に登録するといったような使用方法が可能である。

【０１５６】

図２５（ｃ）は、ユーザが２枚のＩＣカード１０ａ、ＩＣカード１０ｂと１つの携帯メモリ１１を有する場合である。

携帯メモリ１１は、ＩＣカード１０ａのカード固有情報Ａに紐付けされたパスワード情報Ａと、ＩＣカード１０ｂのカード固有情報Ｂに紐付けされたパスワード情報Ｂを記憶している。

【０１５７】

サーバ１１０において、パスワード情報ＡとユーザＩＤ１は、カード固有情報Ａと紐付けられており、また、パスワード情報ＢとユーザＩＤ１は、カード固有情報Ｂと紐付けられている。

ユーザは、ＩＣカード１０ａと携帯メモリ１１の組合せによってユーザ認証を受けることもできるし、あるいはＩＣカード１０ｂと携帯メモリ１１の組合せによってもユーザ認証を受けることもできる。

【０１５８】

このように２枚のＩＣカード１０を用いる場合、それぞれのＩＣカード１０を別のサービスのユーザ認証に用いるように登録することができる。

例えば、ＩＣカード１０ａと携帯メモリ１１の組合せを銀行サービスサイトのユーザ認

証用に登録し、ＩＣカード１０ｂと携帯メモリ１１の組合せを通信販売サイトのユーザ認証用に登録するといったような使用方法が可能である。

この場合、ユーザが保有する携帯メモリは１つでよいので、携帯メモリの管理負担が軽くなる。

【０１５９】

図２６は、ユーザが２人の場合の利用形態を例示した図である。

これは、例えば、家族でユーザ登録する場合などに利用することができる。

図２６（ａ）は、ユーザが個別にＩＣカードと携帯メモリの組を有する場合である。

ユーザＩＤ１を有するユーザは、ＩＣカード１０ａと携帯メモリ１１ａを有し、ＩＣカード１０ａのカード固有情報Ａは携帯メモリ１１ａのパスワード情報Ａと紐付けられている。

【０１６０】

そして、ユーザＩＤ２を有するユーザは、ＩＣカード１０ｂと携帯メモリ１１ｂを有し、ＩＣカード１０ｂのカード固有情報Ｂは携帯メモリ１１ｂのパスワード情報Ｂと紐付けられている。

サーバ１１０において、パスワード情報ＡとユーザＩＤ１は、カード固有情報Ａと紐付けられており、パスワード情報ＢとユーザＩＤ２は、カード固有情報Ｂと紐付けられている。

【０１６１】

図２６（ｂ）は、２人のユーザが１つの携帯メモリを共有する場合である。

ユーザＩＤ１を有するユーザはＩＣカード１０ａを有し、また、ユーザＩＤ２を有するユーザはＩＣカード１０ｂを有している。そして、この２人のユーザは携帯メモリ１１を共有している。

携帯メモリ１１には、ＩＣカード１０ａのカード固有情報Ａと紐付けされたパスワード情報Ａと、ＩＣカード１０ｂのカード固有情報Ｂと紐付けされたパスワード情報Ｂが格納されている。

【０１６２】

サーバ１１０において、パスワード情報ＡとユーザＩＤ１はカード固有情報Ａに紐付けられており、パスワード情報ＢとユーザＩＤ２はカード固有情報Ｂと紐付けられている。

そして、端末３にＩＣカード１０ａと携帯メモリ１１をセットすることにより、ユーザＩＤ１を用いてユーザ認証を受けることができ、また、ＩＣカード１０ｂと携帯メモリ１１をセットすることにより、ユーザＩＤ２を用いてユーザ認証を受けることができる。

【０１６３】

このように携帯メモリを共有する場合、例えば、父親がＩＣカード１０ａを所持し、娘がＩＣカード１０ｂを所持し、父親と娘で携帯メモリ１１を共有するといった利用形態が可能である。この場合、父親はユーザＩＤ１を有し、娘はユーザＩＤ２を有する。

そして、父親はＩＣカード１０ａと携帯メモリ１１を用いて、銀行サービスサイトのユーザとして登録しておき、娘はＩＣカード１０ｂと携帯メモリ１１を用いて通信販売サイトのユーザとして登録しておくといったように別々のサービスのユーザとして登録することができる。

【０１６４】

サーバ１１０は、ＩＣカード１０ａと携帯メモリ１１を用いてユーザ認証要求を受けた場合、これに紐付けされたユーザＩＤ１によりユーザが父親であると識別し、父親に設定されているサービスサイトへログイン処理を行い、ＩＣカード１０ｂと携帯メモリ１１が用いられた場合は同様に娘に設定されているサービスサイトへログイン処理を行う。

【０１６５】

また、ユーザが３人以上存在する場合も、同様にして携帯メモリを共有するように構成することができる。

例えば、各人がＩＣカードを所持し、携帯メモリに各カードのカード固有情報に紐付けされたパスワード情報を記憶しておけばよい。

【０１６６】
先に説明した実施の形態においても、同様に複数のユーザで１つの携帯メモリを共有するように構成することができる。
この場合、各ユーザのユーザ割符を携帯メモリに記憶しておく。また、各人は、それぞれ個別にＩＣカードを所持し、それぞれのカード固有情報と各人のサーバ割符をサーバ５で紐付けておく。
このように構成すると、各ユーザは、自分のＩＣカードと共有に係る携帯メモリを用いてサーバ５にユーザ認証を要求することができる。
【０１６７】
以上に第２の実施の形態について説明したが、第２の実施の形態の自動ログインシステム１００により以下のような効果を得ることができる。
（１）ユーザ認証に必要な情報をＩＣカード１０と携帯メモリ１１の２つに記憶してあるため、ユーザがユーザ認証を要求するためにはこれら２つの記憶媒体を所持することが必要であり、一方が第三者に渡ったとしてもこの第三者はユーザ認証を要求することができない。これによってセキュリティを高めることができる。
（２）これら２つの記憶媒体が、一方がＩＣカード１０、他方が携帯メモリ１１とうように異種の記憶媒体を用いている。このため、これらの記憶媒体の双方を複製するのは困難であり、記憶媒体の複製による不正アクセスを抑止することができる。
【０１６８】
（３）パスワード情報１０２を用いてユーザ認証することにより、パスワード１０５そのものはサーバ１１０で管理することができるため、高いセキュリティレベルを実現することができる。しかも、パスワード情報は、ユーザ認証を行うごと使い捨てるワンタイムパスワードなのでより安全性が高い。
（４）携帯メモリ１１に複数のパスワード情報１０２を記憶することができるため、例えば、携帯メモリ１１を複数のユーザで共有したり、携帯メモリ１１を用いて複数のサービスサイトにログインするなど柔軟な運用を行うことができる。
（５）ユーザは、ＩＣカード１０と携帯メモリ１１を端末３にセットするだけでユーザ認証を要求することができるため、ユーザが認証情報を入力する必要が無く、ユーザの負担を軽減することができる。
【０１６９】
第２の実施の形態により、次のような構成を構築することもできる。
第１の記憶媒体（ＩＣカード１０）と第２の記憶媒体（携帯メモリ１１）を用いた認証方法において、第１の記憶媒体を識別するための第１の識別情報（カード固有情報１０１）を送信し、第２の記憶媒体を識別するための第２の識別情報（携帯メモリＩＤ１０３）と、前記第２の記憶媒体に前記第１の識別情報と関連付けられている符合情報（パスワード情報１０２）と、を送信し、前記符合情報が正しい記憶媒体から提供されたことを確認し、前記第１の識別情報と前記符合情報に基づいて、ユーザの認証を行う認証方法（第１の構成）。
第１の構成において、前記第１の識別情報には、ユーザの認証情報（パスワード１０５とユーザＩＤ１０６の少なくとも一方）が紐付けられているように構成することができる（第２の構成）。
また、前記符合情報には、ユーザの認証情報が紐付けられているように構成することもできる（第３の構成）。
第３の構成において、前記符合情報は、前記ユーザの認証情報に基づいて作成されるように構成することもできる（第４の構成）。
更に、第１の構成において、前記符合情報は、認証されると新たな符合情報が生成されるように構成することもできる（第５の構成）。
加えて、第１の構成において、前記第１の記憶媒体と第２の記憶媒体は、ＩＣカード又は可搬式記憶媒体であるように構成することもできる。
また、端末３で、第１の記憶媒体と第２の記憶媒体を用いた認証方法において、第１の

記憶媒体を識別するための第１の識別情報を送信し、第２の記憶媒体を識別するための第２の識別情報と、前記第２の記憶媒体に前記第１の識別情報と関連付けられている符合情報と、を送信し、前記符合情報が正しい記憶媒体から提供されることが確認されると、前記第１の識別情報と前記符合情報に基づいて、ユーザが認証される認証方法を実現することもがきる。

【０１７０】

なお、第２の実施の形態では、ＩＣカード１０にカード固有情報１０１を記憶し、携帯メモリ１１にパスワード情報１０２を記憶するように構成したが、これとは逆にＩＣカード１０にパスワード情報１０２を記憶し、携帯メモリ１１の携帯メモリＩＤ１０３をユーザＩＤ１０６に紐付けるように構成することもできる。

また、第２の実施の形態では、ＩＣカード１０と携帯メモリ１１と、異種の記憶媒体を用いたが、これに限定せず、２枚のＩＣカード１０、又は２つの携帯メモリ１１を用いてユーザ認証を要求するように構成することもできる。

この場合、一方の記憶媒体のＩＤ情報と、他方の記憶媒体に記憶したパスワード情報１０２を用いてユーザ認証を要求するように構成することができる。

更に、先に説明した実施の形態や第２の実施の形態では、認証対象をユーザとしたが、これは、認証対象をユーザに限定するものではなく、機器の識別番号を認証対象とすることもできる。例えば、近年、ネットワークを介してサービスの提供を利用することのできるＣＥ（ＣＥ：Ｃｏｎｓｕｍｅｒ　Ｅｌｅｃｔｒｏｎｉｃｓ）機器が普及するようになってきており、２つの記憶媒体を用いてＣＥ機器の機器認証を要求するように構成することもできる。この場合、例えば、ＣＥ機器にリーダライタ７や携帯メモリ駆動装置８を備えることができる。

【図面の簡単な説明】

【０１７１】

【図１】本実施の形態に係る自動ログインシステムの概要を説明するための概念図である。

【図２】割符技術の概念を説明するための図である。

【図３】本実施の形態に係る自動ログインシステムのネットワーク構成の一例を示した図である。

【図４】ＩＣカードに形成されている論理的な構成の一例を示した図である。

【図５】自動ログイン部の機能的な構成を模式的に示したブロック図である。

【図６】端末から自動ログインする手順を説明するためのフローチャートである。

【図７】登録部の機能的な構成を模式的に示したブロック図である。

【図８】自動ログインシステムにおける新規登録処理の手順を説明するためのフローチャートである。

【図９】サーバのハードウェア的な構成の一例を示した図である。

【図１０】端末のハードウェア的な構成の一例を示した図である。

【図１１】サービスサイトに接続する際に、端末で表示される画面の画面遷移の一例を示した図である。

【図１２】トップページの一例を示した図である。

【図１３】カードログイン画面の一例を示した図である。

【図１４】ひも付け通知画面の一例を示した図である。

【図１５】ひも付け完了画面の一例を示した図である。

【図１６】携帯メモリ設定画面の一例を示した図である。

【図１７】携帯メモリ設定完了画面の一例を示した図である。

【図１８】携帯メモリ固有情報を用いて電子割符を生成する手順の一例を説明するためのフローチャートである。

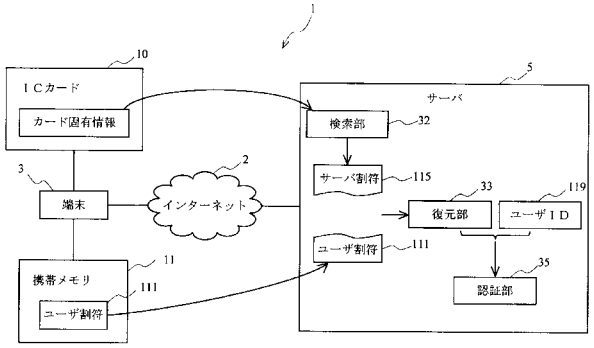
【図１９】パスワードを手入力する場合のログイン処理の手順を説明するためのフローチャートである。

【図２０】第２の実施の形態に係る自動ログインシステムの概要を説明するための概念図

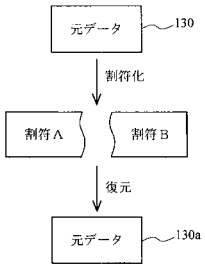
である。
【図２１】第２の実施の形態に係る自動ログインシステムのネットワーク構成の一例を示した図である。
【図２２】（ａ）は、自動ログイン部の機能的な構成を模式的に示したブロック図であり、（ｂ）は、認証情報データベースに記憶されているあるユーザの認証情報の論理的な関係を示した図である。
【図２３】サービスサイトにログインする手順を説明するためのフローチャートである。
【図２４】サービスサイトのユーザとしてユーザ登録する手順を説明するためのフローチャートである。
【図２５】ユーザが単数の場合のＩＣカードと携帯メモリの利用形態を例示した図である。
【図２６】ユーザが複数の場合のＩＣカードと携帯メモリの利用形態を例示した図である。
【符号の説明】
【０１７２】

１	自動ログインシステム	２	インターネット
３	端末	５	サーバ
７	リーダライタ	８	携帯メモリ駆動装置
１０	ＩＣカード	１１	携帯メモリ
１３	登録部	１５	自動ログイン部
１７	サービスサイト	１９	ユーザ情報データベース
２０	サーバ割符データベース	３１	端末アクセス部
３２	検索部	３３	復元部
３４	認証情報生成部	３５	認証部
４１	端末アクセス部	４２	受信情報処理部
４３	割符化部	４４	サーバ割符保存部

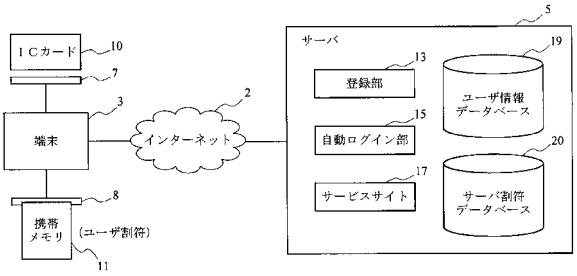
【図１】



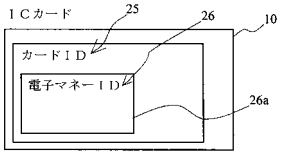
【図２】



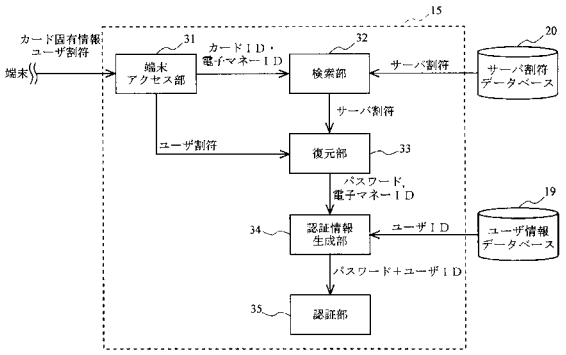
【図３】



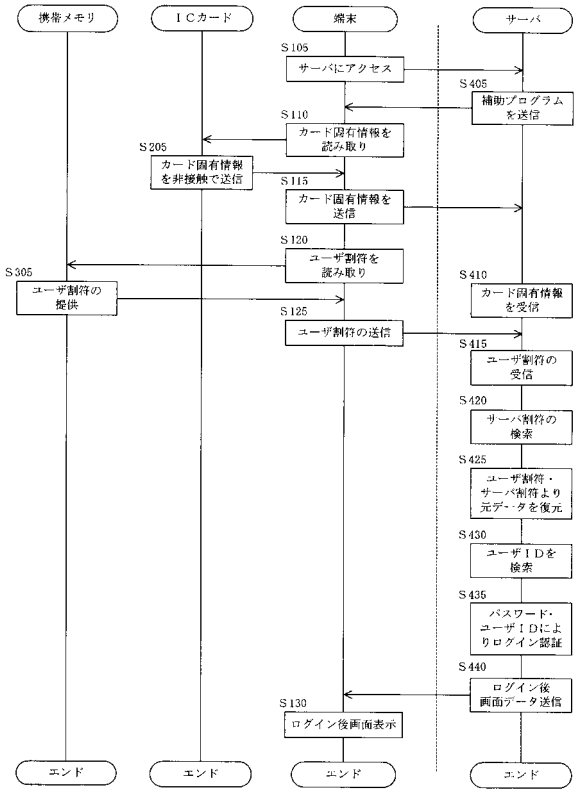
【図４】



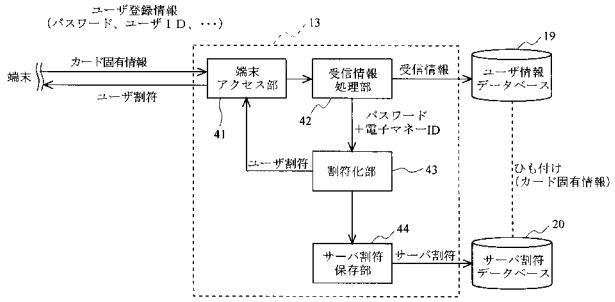
【図５】



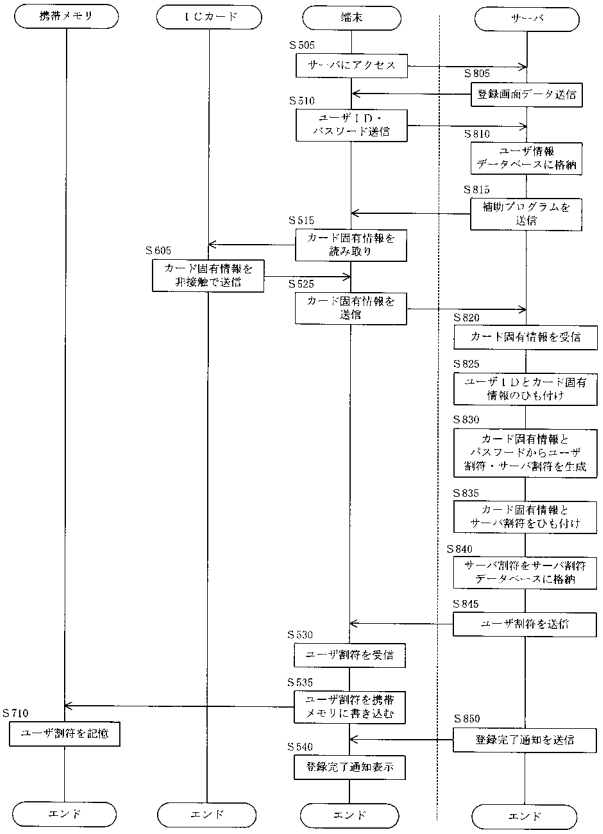
【図６】



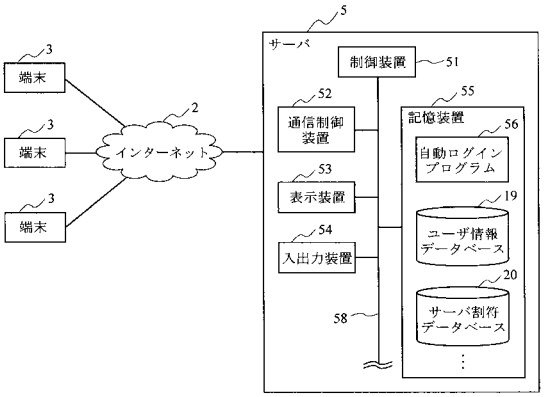
【図７】



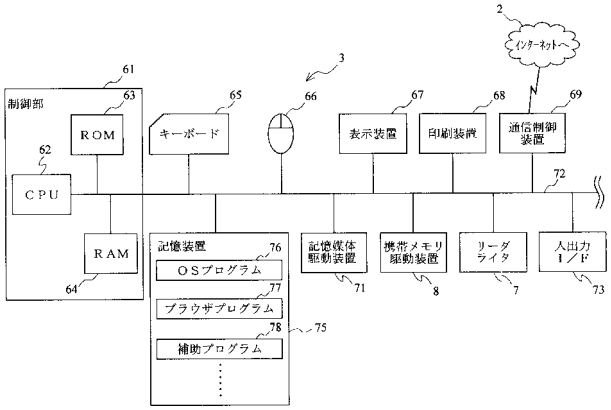
【図８】



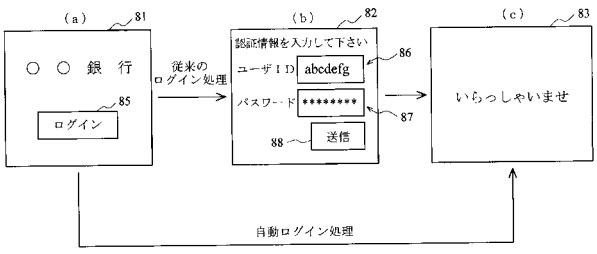
【図９】



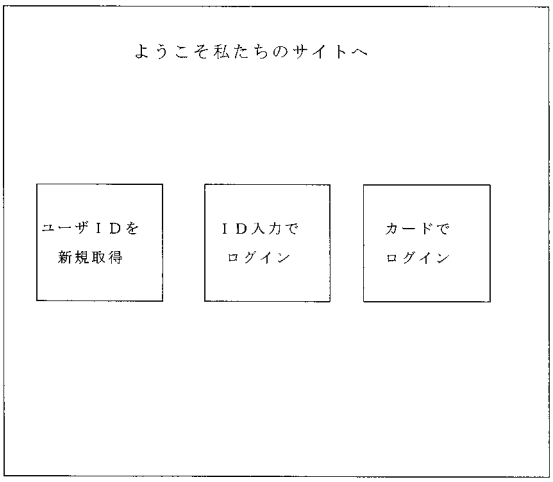
【図１０】



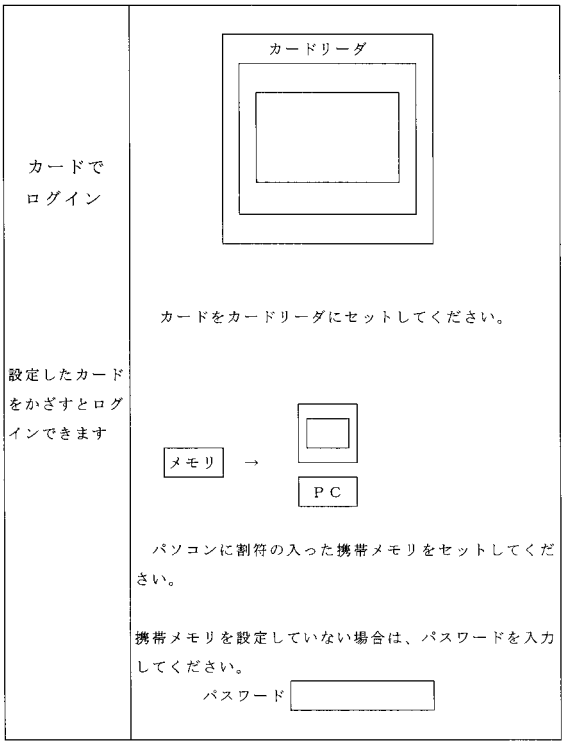
【図１１】



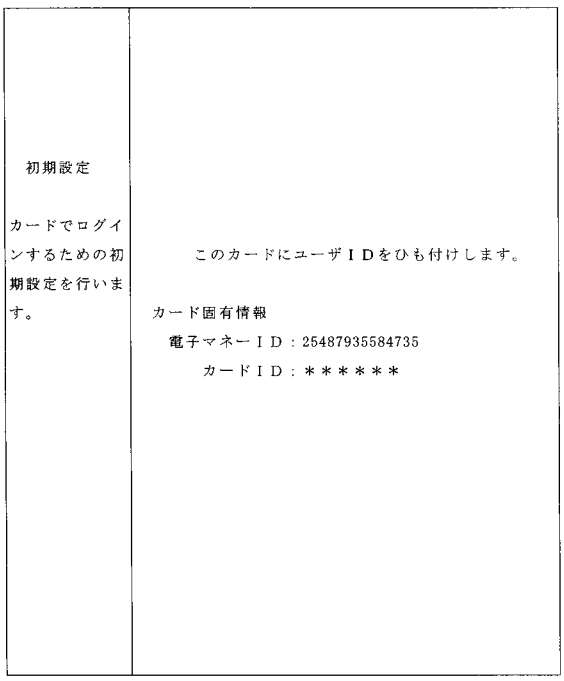
【図１２】



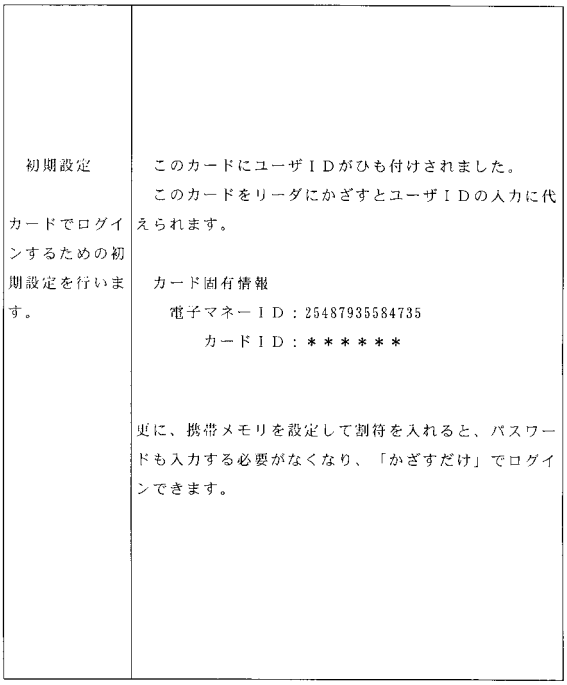
【図１３】



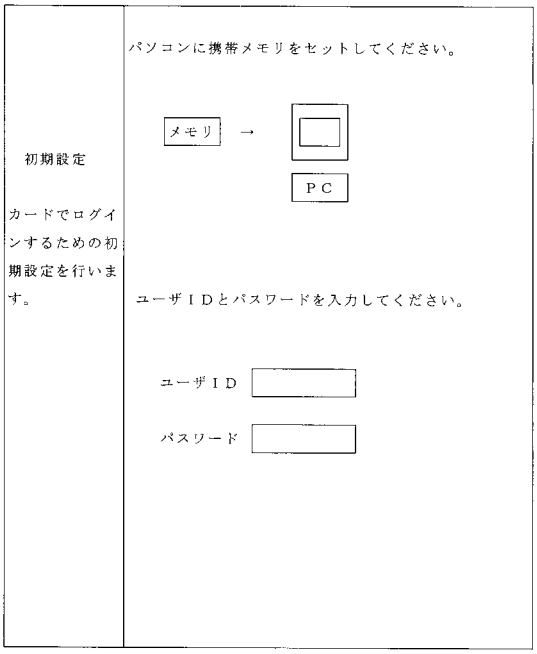
【図１４】



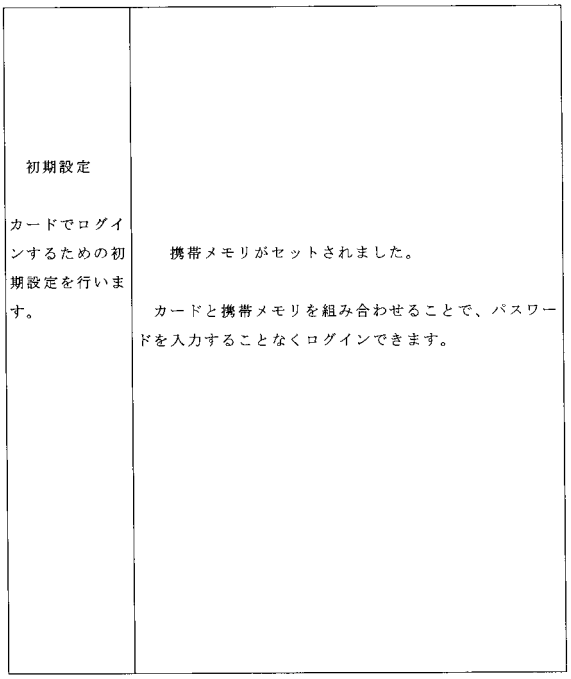
【図１５】



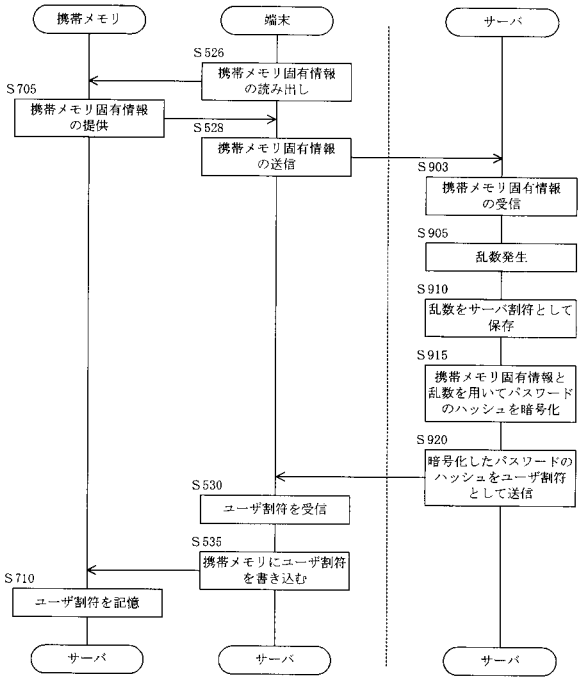
【図１６】



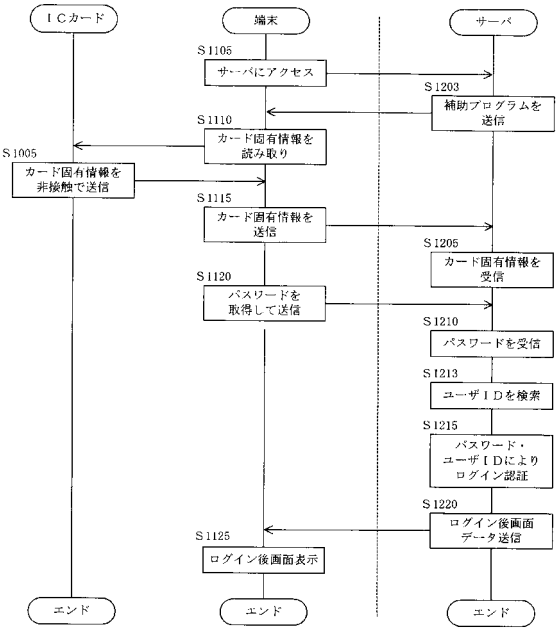
【図１７】



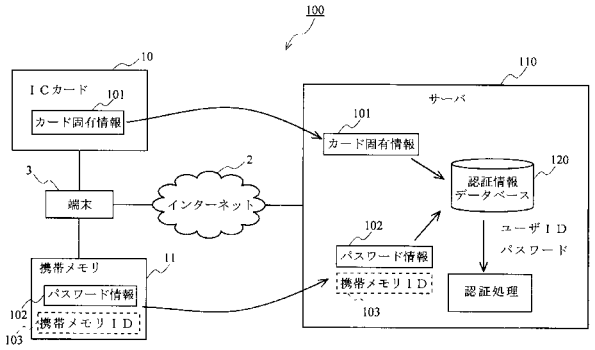
【図１８】



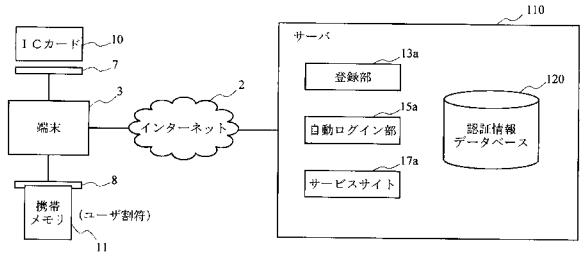
【図１９】



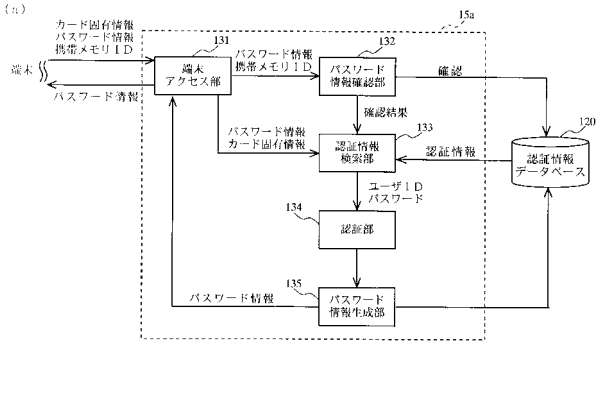
【図２０】

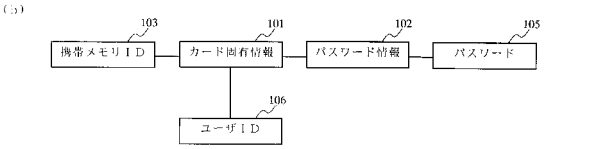


【図２１】

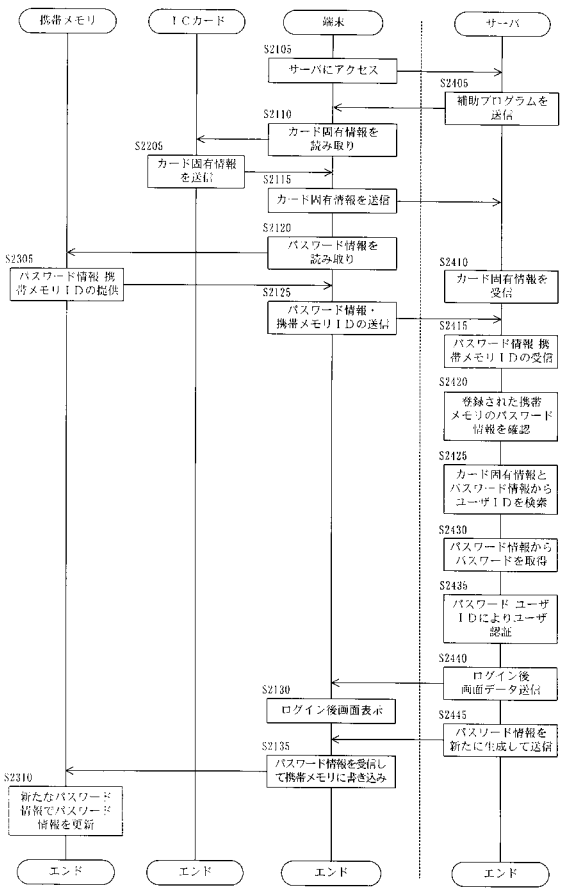


【図２２】

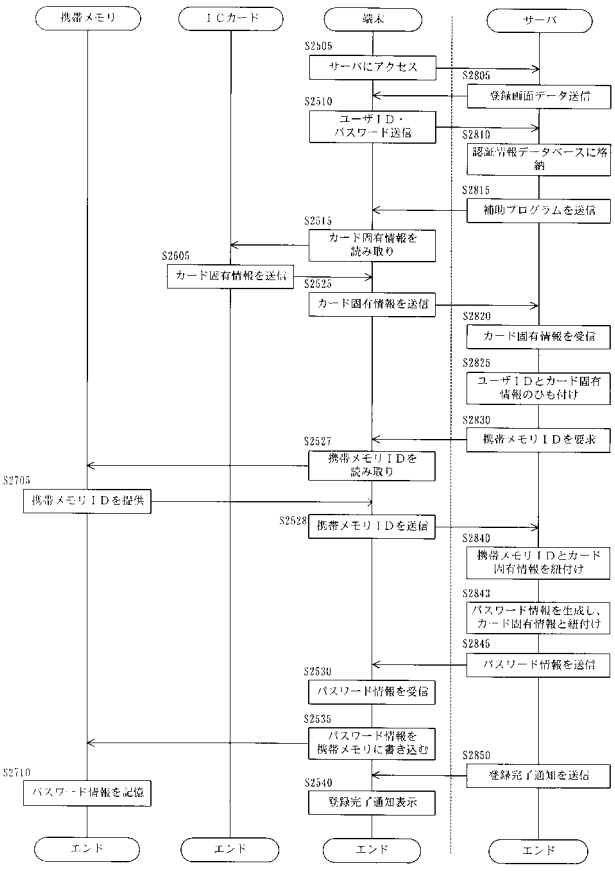




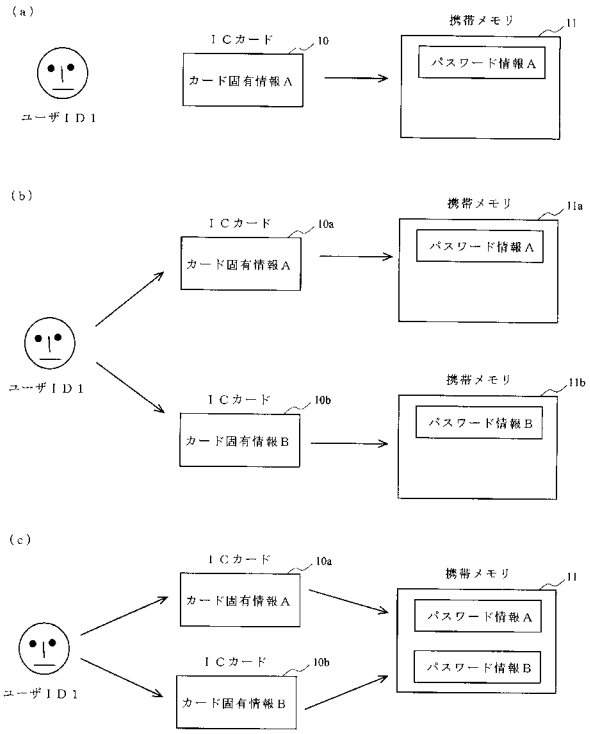
【図２３】



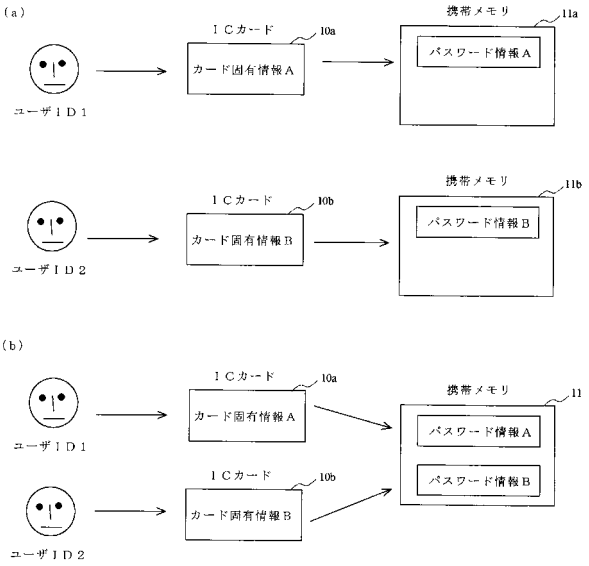
【図２４】



【図２５】


(a)
ユーザＩＤ１
ＩＣカード
10
カード固有情報Ａ
携帯メモリ
11
パスワード情報Ａ
(b)
ユーザＩＤ１
ＩＣカード
10a
カード固有情報Ａ
携帯メモリ
11a
パスワード情報Ａ
ＩＣカード
10b
カード固有情報Ｂ
携帯メモリ
11b
パスワード情報Ｂ
(c)
ユーザＩＤ１
ＩＣカード
10a
カード固有情報Ａ
ＩＣカード
10b
カード固有情報Ｂ
携帯メモリ
11
パスワード情報Ａ
パスワード情報Ｂ

【図２６】


(a)
ユーザＩＤ１
ＩＣカード
10a
カード固有情報Ａ
携帯メモリ
11a
パスワード情報Ａ
ユーザＩＤ２
ＩＣカード
10b
カード固有情報Ｂ
携帯メモリ
11b
パスワード情報Ｂ
(b)
ユーザＩＤ１
ＩＣカード
10a
カード固有情報Ａ
ユーザＩＤ２
ＩＣカード
10b
カード固有情報Ｂ
携帯メモリ
11
パスワード情報Ａ
パスワード情報Ｂ

フロントページの続き

(72)発明者　大橋　春彦
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　山本　浩一
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　村山　麗子
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　布施　篤
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　荒川　真志
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　近藤　秀和
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　岡田　浩
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　三澤　誠一
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　倉崎　俊哉
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　西山　和博
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

Ｆターム(参考)　5B058 CA01　KA02　KA04　KA08
5B085 AE09　AE11
5J104 AA07　AA16　EA03　EA22　KA01　KA02　KA04　KA15　NA05　NA33
NA38　PA07