(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2005-92470
(P2005-92470A)
(43)公開日　平成17年4月7日(2005.4.7)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 15/00	G06F	15/00	330G	5B017
G06F 1/00	G06F	1/00	370E	5B019
G06F 12/14	G06F	12/14	310H	5B035
G06F 15/02	G06F	12/14	320A	5B085
G06F 17/60	G06F	15/02	335G	5J104

審査請求 未請求　請求項の数 21　ＯＬ　（全 16 頁）　最終頁に続く

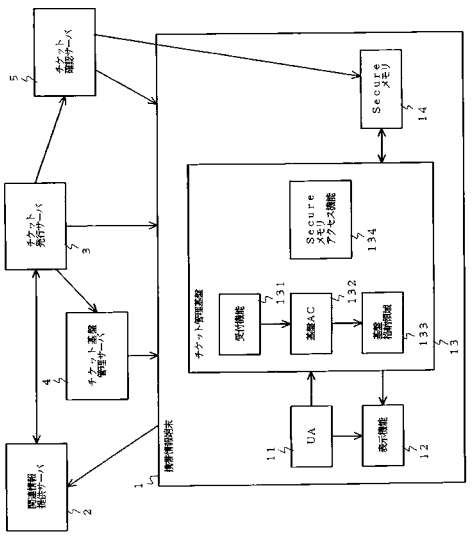
(21)出願番号　特願2003-323835 (P2003-323835)
(22)出願日　平成15年9月17日 (2003.9.17)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100088812
弁理士　▲柳▼川　信
(72)発明者　伊賀　徳寿
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5B017 AA07　BA06　CA14
5B019 FA04　JA10
5B035 AA07　BB09
5B085 AA08　AE00　AE04　BE01
5J104 NA38

(54)【発明の名称】電子情報認証システム、携帯情報端末及びそれらに用いる電子情報認証方法

(57)【要約】
【課題】　高コスト化を招くことなく、端末内の特定の電子情報及びその間連情報に対して強固なセキュリティを施すことが可能な電子情報認証システムを提供する。
【解決手段】　携帯情報端末１のチケット管理基盤１３の基盤格納領域１３３は基盤ＡＣ１３２で許可されたチケット発行サーバ３から渡された関連情報を格納する。基盤格納領域１３３に対してはＵＡ１１と、チケット基盤管理サーバ４と、チケット発行サーバ３とからアクセス可能となっている。セキュリティを考慮しなくてはいけない電子チケットはＳｅｃｕｒｅメモリ１４に格納するが、セキュリティをあまり考慮しなくてもよい場合には基盤格納領域１３３にその電子チケットを置く。
【選択図】　図１



【特許請求の範囲】
【請求項１】
発行サーバから発行された電子情報を携帯情報端末に格納しておき、サービス提供時に前記携帯情報端末に格納された前記電子情報を確認サーバで確認する電子情報認証システムであって、
強固なセキュリティを持ちかつ前記サービス提供時に認証に必要な情報を含む電子情報を格納するメモリと、前記メモリよりも低いセキュリティを持ちかつ前記電子情報の関連情報を格納する格納手段とを前記携帯情報端末に有し、
前記電子情報と前記電子情報の関連情報とを個別に認証することを特徴とする電子情報認証システム。
【請求項２】
前記メモリは、少なくとも耐タンパ性に優れたＩＣカードを含むことを特徴とする請求項１記載の電子情報認証システム。
【請求項３】
少なくとも発行サーバから前記格納手段へのアクセスの認証管理を行う管理サーバを含むことを特徴とする請求項１または請求項２記載の電子情報認証システム。
【請求項４】
前記格納手段へのアクセスの認証管理を行う認証プログラムを前記管理サーバからタウンロードする手段を前記携帯情報端末に含むことを特徴とする請求項３記載の電子情報認証システム。
【請求項５】
前記認証プログラムは、前記格納手段へのアクセス制御情報を含むことを特徴とする請求項４記載の電子情報認証システム。
【請求項６】
前記格納手段へのアクセス制御情報を前記管理サーバから受取る手段を前記携帯情報端末に含むことを特徴とする請求項４記載の電子情報認証システム。
【請求項７】
前記関連情報内に記述された情報を基に前記関連情報より詳細な関連詳細情報を提供する関連情報提供サーバにアクセスする手段を前記携帯情報端末に含むことを特徴とする請求項１から請求項６のいずれか記載の電子情報認証システム。
【請求項８】
発行サーバから発行されかつサービス提供時に確認サーバで確認される電子情報を格納する携帯情報端末であって、
強固なセキュリティを持ちかつ前記サービス提供時に認証に必要な情報を含む電子情報を格納するメモリと、前記メモリよりも低いセキュリティを持ちかつ前記電子情報の関連情報を格納する格納手段とを有し、
前記電子情報と前記電子情報の関連情報とを個別に認証することを特徴とする携帯情報端末。
【請求項９】
前記メモリは、少なくとも耐タンパ性に優れたＩＣカードを含むことを特徴とする請求項８記載の携帯情報端末。
【請求項１０】
少なくとも発行サーバから前記格納手段へのアクセスの認証管理が管理サーバで行われることを特徴とする請求項８または請求項９記載の携帯情報端末。
【請求項１１】
前記格納手段へのアクセスの認証管理を行う認証プログラムを前記管理サーバからタウンロードする手段を含むことを特徴とする請求項１０記載の携帯情報端末。
【請求項１２】
前記認証プログラムは、前記格納手段へのアクセス制御情報を含むことを特徴とする請求項１１記載の携帯情報端末。

【請求項１３】
前記格納手段へのアクセス制御情報を前記管理サーバから受取る手段を含むことを特徴とする請求項１１記載の携帯情報端末。
【請求項１４】
前記関連情報内に記述された情報を基に前記関連情報より詳細な関連詳細情報を提供する関連情報提供サーバにアクセスする手段を含むことを特徴とする請求項８から請求項１３のいずれか記載の携帯情報端末。
【請求項１５】
発行サーバから発行された電子情報を携帯情報端末に格納しておき、サービス提供時に前記携帯情報端末に格納された前記電子情報を確認サーバで確認する電子情報認証方法であって、前記携帯情報端末に設けられかつ強固なセキュリティを持つメモリに前記サービス提供時に認証に必要な情報を含む電子情報を格納し、前記携帯情報端末に設けられかつ前記メモリよりも低いセキュリティを持つ格納手段に前記電子情報の関連情報を格納し、前記電子情報と前記電子情報の関連情報とを個別に認証することを特徴とする電子情報認証方法。
【請求項１６】
前記メモリは、少なくとも耐タンパ性に優れたＩＣカードを含むことを特徴とする請求項１５記載の電子情報認証方法。
【請求項１７】
少なくとも発行サーバから前記格納手段へのアクセスの認証管理を管理サーバで行うことを特徴とする請求項１５または請求項１６記載の電子情報認証方法。
【請求項１８】
前記格納手段へのアクセスの認証管理を行う認証プログラムを前記管理サーバから前記携帯情報端末にタウンロードすることを特徴とする請求項１７記載の電子情報認証方法。
【請求項１９】
前記認証プログラムは、前記格納手段へのアクセス制御情報を含むことを特徴とする請求項１８記載の電子情報認証方法。
【請求項２０】
前記携帯情報端末が、前記格納手段へのアクセス制御情報を前記管理サーバから受取ることを特徴とする請求項１８記載の電子情報認証方法。
【請求項２１】
前記携帯情報端末が、前記関連情報内に記述された情報を基に前記関連情報より詳細な関連詳細情報を提供する関連情報提供サーバにアクセスすることを特徴とする請求項１５から請求項２０のいずれか記載の電子情報認証方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は電子情報認証システム、携帯情報端末及びそれらに用いる電子情報認証方法に関し、特に携帯電話機等の携帯情報端末に保存された電子チケット（入場券等）のセキュリティに関する。
【背景技術】
【０００２】
近年、携帯電話機等の携帯情報端末においては、その多機能化とともに、電子化されたチケット（コンサートチケット、映画チケット、航空券、宿泊券、遊園地や娯楽施設への入場券、住民票等を電子データの形で提供するもの）を格納する機器としても用いられるようになってきている。
【０００３】
携帯情報端末が電子化されたチケットの格納機器として用いられる場合には、それらの情報を必要とする場所、例えばコンサート会場、映画館、遊園地や娯楽施設の入り口等で表示部に表示される電子化されたチケットを提示することで入場が許可されるようになっ

ている。
【０００４】
【特許文献１】特開２００３－１６２６０２号公報
【特許文献２】特開２００２－３２４２５６号公報
【特許文献３】特開２００２－１８９９３３号公報
【特許文献４】特開２００２－１４０７４２号公報
【特許文献５】特開２００２－８３３３３号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
上述した従来の携帯情報端末では、電子化されたチケットを管理する場合、より強固なセキュリティが要求されるチケットの格納場所として、耐タンパ性に優れたＩＣ（集積回路）カード等の強固なセキュリティを持つメモリ（Ｓｅｃｕｒｅメモリ）が挙げられるが、このＳｅｃｕｒｅメモリを用いると高コスト化を招いてしまう。
【０００６】
また、電子化されたチケットの関連情報は、チケット本来の情報（データ）よりはるかに大容量なメモリが要求されることが想定される。よって、その関連情報はセキュリティレベルが比較的低いと思われるため、Ｓｅｃｕｒｅメモリよりも通常のメモリを格納場所とした方が好ましい。但し、ある一定のアクセス制限は必要と考えられる。
【０００７】
電子化されたチケットの関連情報に関しては、上記の特許文献１～５の場合、Ｓｅｃｕｒｅメモリに置く、あるいは通常メモリにアクセス制限を施さないで格納する例が提案されているが、これらの例では悪意を持つものから関連情報を削除されたり、改ざんされる恐れがある。
【０００８】
そこで、本発明の目的は上記の問題点を解消し、高コスト化を招くことなく、端末内の特定の電子情報及びその間連情報に対して強固なセキュリティを施すことができる電子情報認証システム、携帯情報端末及びそれらに用いる電子情報認証方法を提供することにある。
【課題を解決するための手段】
【０００９】
本発明による電子情報認証システムは、発行サーバから発行された電子情報を携帯情報端末に格納しておき、サービス提供時に前記携帯情報端末に格納された前記電子情報を確認サーバで確認する電子情報認証システムであって、
強固なセキュリティを持ちかつ前記サービス提供時に認証に必要な情報を含む電子情報を格納するメモリと、前記メモリよりも低いセキュリティを持ちかつ前記電子情報の関連情報を格納する格納手段とを前記携帯情報端末に備え、
前記電子情報と前記電子情報の関連情報とを個別に認証している。
【００１０】
本発明による携帯情報端末は、発行サーバから発行されかつサービス提供時に確認サーバで確認される電子情報を格納する携帯情報端末であって、
強固なセキュリティを持ちかつ前記サービス提供時に認証に必要な情報を含む電子情報を格納するメモリと、前記メモリよりも低いセキュリティを持ちかつ前記電子情報の関連情報を格納する格納手段とを備え、
前記電子情報と前記電子情報の関連情報とを個別に認証している。
【００１１】
本発明による電子情報認証方法は、発行サーバから発行された電子情報を携帯情報端末に格納しておき、サービス提供時に前記携帯情報端末に格納された前記電子情報を確認サーバで確認する電子情報認証方法であって、前記携帯情報端末に設けられかつ強固なセキュリティを持つメモリに前記サービス提供時に認証に必要な情報を含む電子情報を格納し

、前記携帯情報端末に設けられかつ前記メモリよりも低いセキュリティを持つ格納手段に前記電子情報の関連情報を格納し、前記電子情報と前記電子情報の関連情報とを個別に認証している。

【００１２】

すなわち、本発明の電子情報認証システムは、例えば電子チケット等の特定の電子情報の格納において、入場時の認証に必要な情報を含む電子チケットを高価で耐タンパ性に優れたＩＣ（集積回路）カード等の強固なセキュリティを持つメモリ（以下、Ｓｅｃｕｒｅメモリとする）に格納し、その電子チケットの関連情報を携帯情報端末（携帯電話機を含む）のチケット管理基盤の基盤格納領域に格納することを特徴としている。

【００１３】

本発明の電子情報認証システムでは、基盤格納領域への格納を行うことで、このチケット管理基盤の提供者からアクセス権を得られないと格納することができなくし、さらに確認／参照するができなくしている。

【００１４】

チケット提供者は、電子チケットを格納するＳｅｃｕｒｅメモリとの認証と、その電子チケットの関連情報を格納するチケット管理基盤の基盤格納領域の認証との合わせて２回の認証が必要となる。

【００１５】

したがって、本発明の電子情報認証システムでは、高コスト化を招くことなく、端末内の特定の電子情報及びその間連情報に対して強固なセキュリティを施すことが可能となる。

【発明の効果】

【００１６】

本発明は、以下に述べるような構成及び動作とすることで、高コスト化を招くことなく、端末内の特定の電子情報及びその間連情報に対して強固なセキュリティを施すことができるという効果が得られる。

【発明を実施するための最良の形態】

【００１７】

次に、本発明の実施例について図面を参照して説明する。図１は本発明の一実施例による電子情報認証システムの構成を示すブロック図である。以下、図１を参照して本発明の一実施例による電子情報認証システムでの電子チケット（コンサートチケット、映画チケット、航空券、宿泊券、遊園地や娯楽施設への入場券、住民票等を電子データの形で提供するもの）等の電子情報の認証について説明する。図１には利用者が電子チケットを獲得した後に使用する例を示している。

【００１８】

図１を参照すると、本発明の一実施例による電子情報認証システムは、少なくとも携帯電話機やＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）等の携帯情報端末１と、関連情報提供サーバ２と、チケット発行サーバ３と、チケット基盤管理サーバ４と、チケット確認サーバ５とから構成されている。

【００１９】

携帯情報端末１は、少なくともＵＡ（Ｕｓｅｒ　Ａｇｅｎｔ）１１と、表示機能１２と、チケット管理基盤１３と、強固なセキュリティを持つメモリ（以下、Ｓｅｃｕｒｅメモリとする）１４とから構成されている。

【００２０】

ＵＡ１１は利用者の命令にしたがってチケット管理基盤１３を操作し、関連情報の表示を依頼することが可能な機能を有している。表示機能１２はＵＡ１１あるいはチケット管理基盤１３からの命令によって関連情報の表示を行う機能を有している。この時、関連情報提供サーバ２のアドレスが渡された場合には、関連情報提供サーバ２にアクセスし、必要な表示情報を獲得する。また、関連情報自身を表示することも可能である。

【００２１】

チケット管理基盤１３は、少なくとも受付機能１３１と、基盤ＡＣ（Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ）１３２と、基盤格納領域１３３と、Ｓｅｃｕｒｅメモリアクセス機能１３４とから構成されている。

【００２２】

受付機能１３１はチケット発行サーバ３からの電子チケット及び関連情報の設定を処理する機能、チケット基盤管理サーバ４からのチケット発行サーバ３及びチケット確認サーバ５のアクセス制御情報の設定を処理する機能、チケット確認サーバ５からのチケット確認を処理する機能を有している。

【００２３】

基盤ＡＣ１３２はチケット発行サーバ３のアクセスコントロール情報を管理する機能を有している。このアクセスコントロール情報は、チケット基盤管理サーバ４から通知される。また、チケット発行サーバ３から基盤格納領域１３３へのアクセス要求があった場合、そのアクセスコントロール情報を基にアクセス制御を行っている。

【００２４】

基盤格納領域１３３は基盤ＡＣ１３２で許可されたチケット発行サーバ３から渡された関連情報を格納する機能を有している。基盤格納領域１３３にアクセス可能なものはＵＡ１１と、チケット基盤管理サーバ４と、チケット発行サーバ３とが考えられる。セキュリティを考慮しなくてはいけない電子チケットは、Ｓｅｃｕｒｅメモリ１４に格納するが、セキュリティをあまり考慮しなくてもよい場合には基盤格納領域１３３にその電子チケットを置くことができる。

【００２５】

Ｓｅｃｕｒｅメモリアクセス機能１３４は、Ｓｅｃｕｒｅメモリ１４へのアクセス機能を有している。Ｓｅｃｕｒｅメモリ１４は耐タンパ性に優れたＩＣ（集積回路）カード等のメモリである。このメモリは携帯情報端末１内に内蔵されていてもよいし、携帯情報端末１に着脱可能なものでもよい。

【００２６】

関連情報提供サーバ２はチケット発行サーバ３で提供する電子チケットに関連付けられた関連情報よりも詳細な関連情報を提供するサーバである。関連情報に関連情報提供サーバ２のアドレスが記述されていた場合、携帯情報端末１はそのアドレスの関連情報提供サーバ２にアクセスし、より詳細な関連情報を獲得することができる。

【００２７】

チケット発行サーバ３はＳｅｃｕｒｅメモリ１４に格納する電子チケットと、基盤格納領域１３２に格納する関連情報とを提供可能なサーバである。チケット基盤管理サーバ４は携帯情報端末１がチケット管理基盤１３の機能を有効にする処理と、チケット発行サーバ３がチケット管理基盤１３にアクセス可能とする処理とを実行することができる機能を有するサーバである。

【００２８】

チケット確認サーバ５は利用者が電子チケットを使用してあるサービスを利用する場合に、電子チケットの存在を確認する機能を有している。尚、関連情報提供サーバ２、チケット発行サーバ３、チケット確認サーバ５は同一サーバ上で実現してもよい。

【００２９】

図２は図１のチケット発行サーバ３が携帯情報端末１のチケット管理基盤１３を利用したサービスを行いたい場合の処理を示すシーケンスチャートであり、図３は図１の携帯情報端末１のチケット管理基盤１３に対してチケット発行サーバ３とチケット確認サーバ５とがアクセス可能となるように設定する手順を示すシーケンスチャートである。

【００３０】

図４は図１の携帯情報端末１に対してチケット発行サーバ３が電子チケット及び関連情報を設定する手順を示すシーケンスチャートであり、図５は利用者が関連情報を参照する場合の手順を示すシーケンスチャートであり、図６は利用者が獲得したい電子チケットを使用して対応したサービスを受けたい場合の手順を示すシーケンスチャートである。

【００３１】
これら図１～図６を参照して本発明の一実施例による電子情報認証システムの動作について説明する。ここで、本発明の一実施例による電子情報認証システムの動作としては、（１）チケット管理基盤１３へのアクセス依頼、（２）チケット管理基盤１３へのチケット発行サーバ３のアクセス設定、（３）電子チケット及び関連情報の獲得、（４）関連情報の使用、（５）電子チケットの使用という処理に大きく分けることができる。
【００３２】
まず、（１）チケット管理基盤１３へのアクセス依頼について述べる。チケット発行サーバ３は携帯情報端末１のチケット管理基盤１３を利用したい旨をチケット基盤管理サーバ４に通知する（図２のａ１）。この場合、チケット発行サーバ３及びチケット基盤管理サーバ４は必要であれば、相互認証を行う。
【００３３】
その後、チケット発行サーバ３はチケット基盤管理サーバ４が一意に識別可能な識別情報、及び携帯情報端末１との相互認証に必要な認証情報を獲得する（図２のａ２）。
【００３４】
チケット発行サーバ３が獲得した識別情報及び認証情報は、チケット確認サーバ５に渡される（図２のａ３）。本実施例ではチケット発行サーバ３からチケット確認サーバ５に識別情報及び認証情報を渡しているが、チケット確認サーバ５はチケット基盤管理サーバ４から直接もらっても良い。
【００３５】
また、これら識別情報及び認証情報は携帯情報端末１への通知時に使用されるが、チケット発行サーバ３が持つものと、チケット確認サーバ５がもつものとは同じでもよいし、別のものでもよい。別のものである場合、チケット基盤管理サーバ４はチケット発行サーバ３用の識別情報及び認証情報と、チケット確認サーバ５用の識別情報及び認証情報とを携帯情報端末１の基盤ＡＣ１３２に設定する必要がある。
【００３６】
チケット発行サーバ３が発行する電子チケットに関連した情報である詳細な関連情報（以下、関連詳細情報とする）を利用者に提供したい場合、チケット発行サーバ３は関連情報提供サーバ２に関連詳細情報の作成を依頼する（図２のａ４）。この関連詳細情報は携帯情報端末１の基盤格納領域１３２に設定する関連情報よりももっと詳細な情報である。
【００３７】
または、関連情報提供サーバ２がチケット発行サーバ３の発行する電子チケットに対して関連詳細情報、あるいは別の関連情報をユーザに提供したい場合、関連情報提供サーバ２は自サーバのアドレスを含む関連情報の提供を行いたい旨をチケット発行サーバ３に通知する（図２のａ５）。
【００３８】
これらの処理をすべて終えることによって、チケット発行サーバ３は電子チケットを利用者に提供することが可能となる。また、チケット発行サーバ３は必要に応じて、関連情報をも用意する。
【００３９】
この関連情報には、少なくとも、表示情報（携帯情報端末１の表示機能１２で表示する情報）、確証情報（Ｓｅｃｕｒｅメモリ１４に確かに電子チケットを格納したという情報）、関連詳細情報（関連情報提供サーバ２のアドレス）、識別情報（本関連情報をアクセス可能なサーバを一意に識別可能な識別情報）、アクセスコントロール（識別情報で一意に識別されるサーバに対するデフォルトのＲｅａｄ権限、Ｗｒｉｔｅ権限情報）が含まれている。
【００４０】
次に、（２）チケット管理基盤１３へのチケット発行サーバ３のアクセス設定について述べる。携帯情報端末１の利用者がチケット基盤管理サーバ４が設置されている場所へ行き、赤外線経由、あるいは無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）経由で

チケット管理基盤サーバ４と通信する、あるいは携帯情報端末１が携帯電話網（図示せず）を利用可能であれば、その携帯電話網を利用してチケット管理基盤サーバ４と通信することを想定している。

【００４１】

まず、チケット管理基盤サーバ４と携帯情報端末１のチケット管理基盤１３とは相互認証を行い、互いが正しいものであることを確認する（図３のｂ１）。その後、チケット基盤管理サーバ４は携帯情報端末１のチケット管理基盤１３にアクセス制御情報の設定を依頼する（図３のｂ２）。チケット基盤管理サーバ４との通信は受付機能１３１が行い、アクセス制御情報は基盤ＡＣ１３２へと格納される。

【００４２】

この時のアクセス制御情報は、少なくとも、識別情報（チケット管理基盤１３にアクセスするサーバを一意に識別可能な識別情報、例えばチケット発行サーバ３の識別情報、チケット確認サーバ５の識別情報）、認証情報（識別情報で一意に識別されるサーバとの認証時に使用される情報）、アクセスコントロール（識別情報で一意に識別されるサーバに対するデフォルトのＲｅａｄ権限、Ｗｒｉｔｅ権限情報）という内容を持つ。

【００４３】

チケット発行サーバ３とチケット確認サーバ５とが別の識別情報と認証情報とを持つ場合には、それぞれのサーバについて、上記の処理（ｂ２の処理）でアクセス制御情報を設定する必要がある。

【００４４】

続いて、（３）チケット及び関連情報の獲得について述べる。この場合には、チケット発行サーバ３が携帯情報端末１のチケット管理基盤１３の受付機能１３１との通信を行う。

【００４５】

チケット発行サーバ３と携帯情報端末１のチケット管理基盤１３とは相互認証を行う（図４のｃ１）。この場合、チケット発行サーバ３は自サーバを識別可能な識別情報をチケット管理基盤１３に渡す。チケット管理基盤１３は基盤ＡＣ１３２からチケット発行サーバ３の識別情報と一致するアクセス制御情報をサーチし、そのアクセス制御情報の認証情報とチケット発行サーバ３が持っている認証情報とを使用して相互認証を行う。

【００４６】

その後、チケット発行サーバ３はチケット管理基盤１３へ関連情報の設定を依頼する（図４のｃ２）。携帯情報端末１ではチケット管理基盤１３内の基盤ＡＣ１３２を通して、その関連情報を基盤格納領域１３３へ格納する。

【００４７】

この時、基盤ＡＣ１３２は上記の処理（ｃ１の処理）でサーチしたアクセス制御情報内のアクセスコントロールからチケット発行サーバ２のアクセス権を調べ、Ｗｒｉｔｅ権限をもつサーバであることを確認してから基盤格納領域４３３へアクセスする。

【００４８】

チケット発行サーバ３はチケット管理基盤１３へＳｅｃｕｒｅメモリ１４との間で相互認証を依頼する（図４のｃ３）。この認証処理を行うために、チケット発行サーバ３は予めＳｅｃｕｒｅメモリ１４に関連する認証情報を保持しておく必要がある。この認証処理では、チケット発行サーバ３がチケット管理基盤１３に認証に必要な情報を渡しておく。例えば、チケット発行サーバ３はチャレンジ・レスポンスデータ等をチケット管理基盤１３に渡しておく。

【００４９】

チケット管理基盤１３はＳｅｃｕｒｅメモリアクセス機能１３４を通してＳｅｃｕｒｅメモリ１４との間で相互認証処理を行う（図４のｃ４）。その後に、チケット発行サーバ３はチケット管理基盤１３へＳｅｃｕｒｅメモリ１４へ電子チケットの設定の依頼を行う（図４のｃ５）。チケット管理基盤１３はＳｅｃｕｒｅメモリアクセス機能１３４を通してＳｅｃｕｒｅメモリ１４に電子チケットの設定を行う（図４のｃ６）。

【００５０】
また、（４）関連情報の使用について述べる。利用者が関連情報を参照する場合、利用者は携帯情報端末１のＵＡ１１をＧＵＩ（Ｇｒａｐｈｉｃａｌ Ｕｓｅｒ Ｉｎｔｅｒｆａｃｅ）画面等を操作してある電子チケットの関連情報を獲得することをチケット管理基盤１３に通知する（図５のｄ１）。
【００５１】
この場合、チケット管理基盤１３はその獲得依頼を受付機能１３１で受取り、基盤ＡＣ１３２を通して、基盤格納領域１３３内の利用者が指定する関連情報を検索する。この時のアクセスコントロールは、関連情報のアクセスコントロールにしたがう。もし、ＵＡ１１についてのアクセスコントロールが設定されていない場合には、上記のｂ２の処理で設定されたアクセス制御情報内のアクセスコントロールが適用される。
【００５２】
チケット管理基盤１３は関連情報内の表示情報を表示機能１２に渡す（図５のｄ２）。表示機能１２は受取った表示情報を表示する（図５のｄ４）。この場合、表示機能１２は表示情報、あるいは関連詳細情報を携帯情報端末１のディスプレイ（図示せず）に表示する。
【００５３】
もし、表示情報が関連情報提供サーバ２のアドレスであれば、表示機能１２は関連情報提供サーバ２との通信を開始し、関連詳細情報を獲得する。その後、表示機能１２は受取った表示情報を表示する（図５のｄ４）。この場合も、表示機能１２は表示情報、あるいは関連詳細情報を携帯情報端末１のディスプレイに表示する。
【００５４】
さらに、（５）電子チケットの使用について述べる。利用者が獲得したい電子チケットを使用して対応したサービスを受けたい場合、チケット確認サーバ５はチケット管理基盤１３へＳｅｃｕｒｅメモリ１４との間で相互認証を依頼する（図６のｅ１）。チケット管理基盤１３はＳｅｃｕｒｅメモリアクセス機能１３４を通してＳｅｃｕｒｅメモリ１４との間で相互認証処理を行う（図６のｅ２）。これらの処理はチケット確認サーバ５が携帯情報端末１に装着されているＳｅｃｕｒｅメモリ１４への相互認証処理である。これらの処理は上述したｃ３の処理及びｃ４の処理と同じである。
【００５５】
その後に、チケット確認サーバ５はチケット管理基盤１３へＳｅｃｕｒｅメモリ１４に設定された電子チケットの確認の依頼を行う（図６のｅ３）。チケット管理基盤１３はＳｅｃｕｒｅメモリアクセス機能１３４を通してＳｅｃｕｒｅメモリ１４に設定された電子チケットの確認を行う（図６のｅ４）。これらの処理は上述したｃ５の処理及びｃ６の処理とほぼ同じである。
【００５６】
Ｓｅｃｕｒｅメモリ１４が携帯情報端末１から分離されている状態の場合、チケット確認サーバ５はＳｅｃｕｒｅメモリ１４との間で相互認証を行い（図６のｅ５）、Ｓｅｃｕｒｅメモリ１４に設定された電子チケットの確認を行う（図６のｅ６）。
【００５７】
このように、本実施例では、電子チケットと関連情報とをそれぞれ別に認証することによって、チケット発行業者が関連情報を提供する、あるいはチケット発行者とは別の業者が関連情報を提供する、または関連情報を参照して別の関連業者が新たな関連情報を格納することをそれぞれ安全に行うことができる。
【００５８】
つまり、本実施例では、チケット基盤管理サーバ４で認められた業者（サーバ）のみがチケット管理基盤１３にアクセス可能であり、悪質な業者（サーバ）から基盤格納領域１３３及び関連情報を守ることができる。
【００５９】
また、本実施例では、チケット発行業者が新たに現れても、携帯情報端末１内のチケッ

ト管理基盤１３にその業者についてのアクセス制御情報を容易に追加可能である。これは、携帯情報端末１がその都度、チケット基盤管理サーバ４と通信を行うことで可能となる。

【００６０】

利用者はチケット基盤管理サーバ４が設定されている場所、または店舗に行けば、いつでも通信可能となる。この場合、本実施例では、携帯情報端末１が携帯電話網を利用することが可能であれば、リモートに存在するチケット基盤管理サーバ４への通信も可能である。

【００６１】

さらに、本実施例では、電子チケットの関連情報をＳｅｃｕｒｅメモリ１４よりも安価なメモリに格納可能であり、大容量の関連情報を扱うことが可能となる。つまり、Ｓｅｃｕｒｅメモリ１４には電子チケットを使用する場合の必要最低限の情報のみを格納すればよい。

【００６２】

さらにまた、本実施例では、関連情報内に関連情報提供サーバ２のアドレスを記述可能としているので、携帯情報端末１から関連情報提供サーバ２へのアクセスが可能であり、より多くの、そしてより詳細な関連情報を利用者に提供することが可能となる。

【００６３】

本実施例では、関連情報毎に、その関連情報にアクセスを許可する各種サーバ及びアプリケーションに関してアクセスコントロール情報を含んでいるので、各種サーバ及び携帯情報端末１内のアプリケーションがある１つの関連情報を利用する場合、各種サーバ及びアプリケーションについてアクセス制御が可能となる。

【００６４】

図７は本発明の他の実施例による電子情報認証システムの構成を示すブロック図である。図７において、本発明の他の実施例による電子情報認証システムは携帯情報端末６内にダウンロード機能６１及び設定ＡＰ（アプリケーションプログラム）６２を追加した以外は図１に示す本発明の一実施例による電子情報認証システムと同様の構成となっており、同一構成要素には同一符号を付してある。また、同一構成要素の動作は本発明の一実施例と同様である。

【００６５】

ダウンロード機能６１は設定ＡＰ６２をチケット基盤管理サーバ４からダウンロード可能とする機能を有している。これによって、チケット基盤管理サーバ４は設定ＡＰ６２を管理する機能、及び携帯情報端末６のダウンロード機能６１と連携して設定ＡＰ６２を送出す機能を有している。

【００６６】

設定ＡＰ６２は上述した本発明の一実施例においてチケット基盤管理サーバ４が行っていたアクセス制御情報の設定を、チケット基盤管理サーバ４の代わりに実行することが可能な機能を有している。本実施例による手順においては、アクセス制御情報を設定する手順が、上述した本発明の一実施例による手順とは異なる。

【００６７】

図８は本発明の他の実施例におけるアクセス制御情報の設定手順を示すシーケンスチャートである。これら図７及び図８を参照して本発明の他の実施例におけるアクセス制御情報の設定手順について説明する。

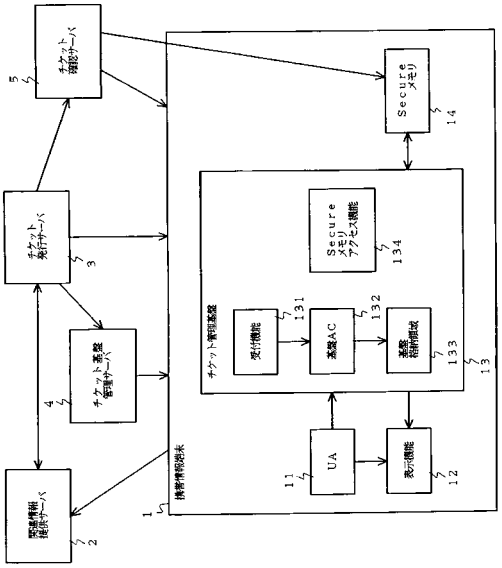
【００６８】

チケット基盤管理サーバ４は携帯情報端末６のダウンロード機能６１との間で相互認証を行う（図８のｆ１）。ダウンロード機能６１はチケット基盤管理サーバ４からアクセス制御情報を含む設定ＡＰ６２をダウンロードする（図８のｆ２）。ダウンロード機能６１はダウンロードした設定ＡＰ６２を起動する（図８のｆ３）。この起動はダウンロード機能６１が行わない場合、利用者が携帯情報端末６に対して設定ＡＰ６２への起動要求を行っても良い。

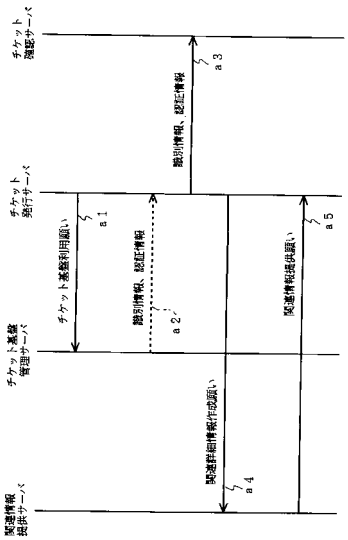
【００６９】
設定ＡＰ６２は自身に含まれているアクセス制御情報をチケット管理基盤１３に渡す。チケット管理基盤１３はそのアクセス制御情報を受付機能１３１を経由して基盤ＡＣ１３２へ設定する（図８のｆ４）。あるいは、チケット管理基盤１３は基盤ＡＣ１３２を直接呼出して設定してもよい。
【００７０】
この時、設定ＡＰ６２とチケット管理基盤１３との間の相互認証は、上記のｆ１の処理において、信頼することができるチケット基盤管理サーバ４からダウンロードしたので、ダウンロードした設定ＡＰ４６も信頼することができるので、不要となる。
【００７１】
このように、本実施例では、利用者がアクセス制御情報、電子チケット、及びその関連情報を携帯情報端末６に設定し、あるいは携帯情報端末６内のメモリをそれら情報に使用可能とさせるということを承諾したうえで、設定ＡＰ６２をダウンロードすることで、上述した本発明の一実施例よりも、利用者にとっては、より承諾／契約したことを明確にすることが可能である。
【００７２】
図９は本発明の別の実施例におけるアクセス制御情報の設定手順を示すシーケンスチャートである。本発明の別の実施例による電子情報認証システムは上記の本発明の他の実施例による電子情報認証システムと同様の構成となっている。尚、図９のｇ１～ｇ３の処理は上述したｆ１～ｆ３０の処理と同じであるので、その説明は省略する。
【００７３】
チケット管理サーバ４は携帯情報端末６にダウンロードされた設定ＡＰ６２と通信する機能を有している。携帯情報端末６にダウンロードされた設定ＡＰ６２はチケット管理サーバ４と通信する機能を有している。
【００７４】
本実施例では、必要であれば、チケット管理基盤サーバ４と設定ＡＰ６２を介したチケット管理基盤１３との間の相互認証を行う（図９のｇ４，ｇ５）。その後、チケット基盤管理サーバ４は設定ＡＰ６２との通信を開始し、アクセス制御情報を設定ＡＰ６２に送信してその設定依頼を行う（図９のｇ６）。
【００７５】
設定ＡＰ６２はチケット基盤管理サーバ４から受取ったアクセス制御情報をチケット管理基盤１３に渡す。チケット管理基盤１３ではそのアクセス制御情報を受付機能１３１を通して基盤ＡＣ１３２に設定する（図９のｇ７）。
【００７６】
上述した本発明の他の実施例では、設定ＡＰ６２にアクセス制御情報を埋め込んでいるため、アクセス制御情報が異なれば、その異なる数だけ設定ＡＰ６２を用意する必要ある。
【００７７】
これに対し、本実施例では、アクセス制御情報をチケット基盤管理サーバ４と通信して受取る手順となっているため、複数の設定ＡＰ６２を用意する必要がない。これによって、本実施例では、チケット基盤管理サーバ４が設定ＡＰ６２を１種類用意しておけばよく、より柔軟なアクセス制御情報の設定が可能となる。
【産業上の利用可能性】
【００７８】
本発明は、上述したような電子チケットの認証以外に、電子チケット以外にも、住民票等の個人認証情報、プリペイドカード等の金額情報、招待状等の入場券、その他、様々な電子データに置換可能な電子情報に対する認証に用いることが可能である。
【図面の簡単な説明】
【００７９】
【図１】本発明の一実施例による電子情報認証システムの構成を示すブロック図である。

【図２】図１のチケット発行サーバが携帯情報端末１のチケット管理基盤を利用したサービスを行いたい場合の処理を示すシーケンスチャートである。
【図３】図１の携帯情報端末のチケット管理基盤に対してチケット発行サーバとチケット確認サーバとがアクセス可能となるように設定する手順を示すシーケンスチャートである。
【図４】図１の携帯情報端末に対してチケット発行サーバが電子チケット及び関連情報を設定する手順を示すシーケンスチャートである。
【図５】利用者が関連情報を参照する場合の手順を示すシーケンスチャートである。
【図６】利用者が獲得したい電子チケットを使用して対応したサービスを受けたい場合の手順を示すシーケンスチャートである。
【図７】本発明の他の実施例による電子情報認証システムの構成を示すブロック図である。
【図８】本発明の他の実施例におけるアクセス制御情報の設定手順を示すシーケンスチャートである。
【図９】本発明の別の実施例におけるアクセス制御情報の設定手順を示すシーケンスチャートである。
【符号の説明】
【００８０】
１，６　携帯情報端末
２　関連情報提供サーバ
３　チケット発行サーバ
４　チケット基盤管理サーバ
５　チケット確認サーバ
１１　ＵＡ
１２　表示機能
１３　チケット管理基盤
１４　Ｓｅｃｕｒｅメモリ
６１　ダウンロード機能
６２　設定ＡＰ
１３１　受付機能
１３２　基盤ＡＣ
１３３　基盤格納領域
１３４　Ｓｅｃｕｒｅメモリアクセス機能

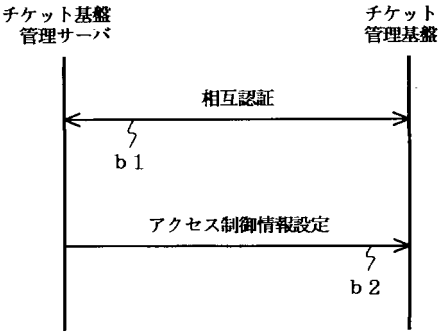
【図１】


チケット認証サーバ
5
Secure メモリ
14
チケット発行サーバ
3
Secure メモリアクセス機能
134
チケット管理基盤
受付機能
131
基盤AC
132
基盤構成機能
133
13
チケット基盤管理サーバ
4
携帯情報端末
1
UA
11
表示機能
12
関連情報提供サーバ
2

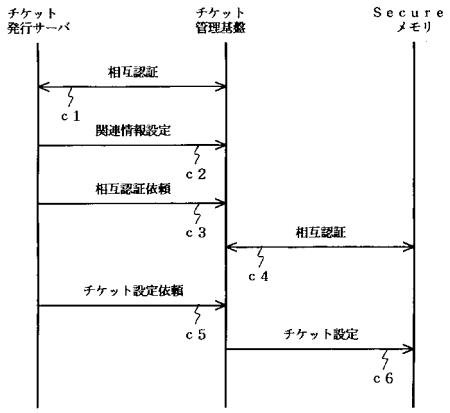
【図２】


チケット認証サーバ
a 3
識別情報、認証情報
チケット発行サーバ
a 1
チケット基盤利用届い
識別情報、認証情報
a 2
a 5
関連情報提供届い
チケット基盤管理サーバ
関連詳細情報作成届い
a 4
関連情報提供サーバ

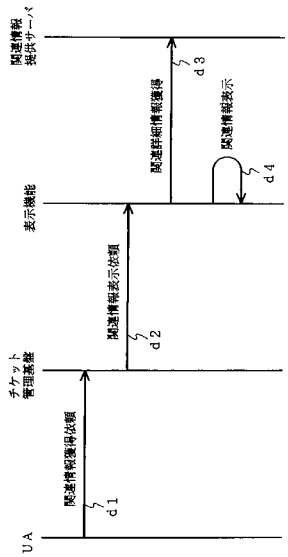
【図３】


チケット基盤管理サーバ
チケット管理基盤
相互認証
b 1
アクセス制御情報設定
b 2

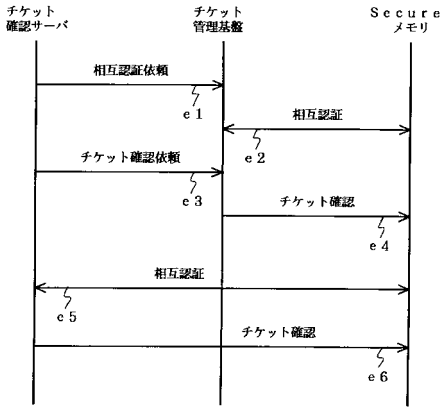
【図４】


チケット発行サーバ
チケット管理基盤
Secure メモリ
相互認証
c 1
関連情報設定
c 2
相互認証依頼
c 3
相互認証
c 4
チケット設定依頼
c 5
チケット設定
c 6

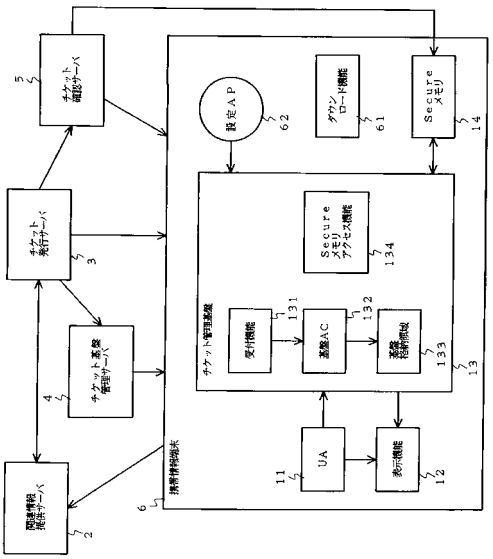
【図５】


関連情報提供サーバ
表示機能
チケット管理基盤
UA
関連情報取得依頼
d1
関連情報表示依頼
d2
関連詳細情報取得
d3
関連情報表示
d4

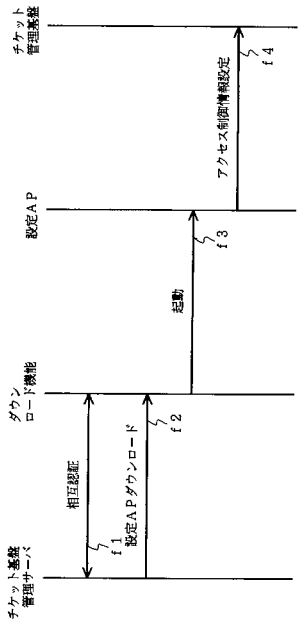
【図６】


チケット確認サーバ
チケット管理基盤
Secure メモリ
相互認証依頼
e1
相互認証
e2
チケット確認依頼
e3
チケット確認
e4
相互認証
e5
チケット確認
e6

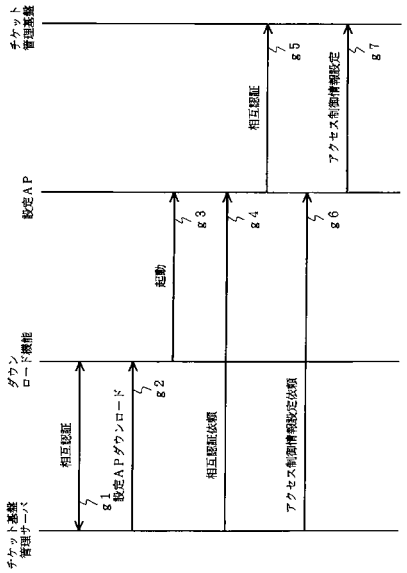
【図７】


チケット確認サーバ
チケット発行サーバ
チケット基盤管理サーバ
関連情報提供サーバ
携帯情報端末
設定AP
ダウンロード機能
Secure メモリ
Secure メモリアクセス機能
チケット管理基盤
受付機能
基盤AC
基盤情報領域
UA
表示機能

【図８】


チケット管理基盤
設定AP
ダウンロード機能
チケット基盤管理サーバ
アクセス制御情報設定
f4
起動
f3
相互認証
f1
設定APダウンロード
f2

【図９】


チケット管理基盤
設定ＡＰ
ダウンロード機能
チケット基盤管理サーバ
相互認証
ｇ１
設定ＡＰダウンロード
ｇ２
起動
ｇ３
ｇ４
相互認証
ｇ５
アクセス制御情報設定
ｇ６
ｇ７
相互認証依頼
アクセス制御情報設定依頼

フロントページの続き

(51)Int.Cl.[7]	FI		テーマコード（参考）
Ｇ０６Ｋ 19/073	Ｇ０６Ｆ 15/02	３４０Ｚ	
Ｇ０９Ｃ 1/00	Ｇ０６Ｆ 15/02	３６０Ｚ	
Ｈ０４Ｌ 9/10	Ｇ０６Ｆ 17/60	１４０	
	Ｇ０６Ｆ 17/60	５０６	
	Ｇ０６Ｆ 17/60	５１０	
	Ｇ０６Ｆ 17/60	５１２	
	Ｇ０９Ｃ 1/00	６６０Ｃ	
	Ｇ０６Ｋ 19/00	Ｐ	
	Ｈ０４Ｌ 9/00	６２１Ｚ	