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

特許第3791131号

(P3791131)

(45)発行日　平成18年6月28日(2006.6.28)　(24)登録日　平成18年4月14日(2006.4.14)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675D
G09C	1/00	(2006.01)	G09C	1/00	640C
G06K	17/00	(2006.01)	H04L	9/00	675C
G07B	5/00	(2006.01)	G06K	17/00	T
G07F	7/12	(2006.01)	G07B	5/00	Z

請求項の数 58　(全 64 頁)　最終頁に続く

(21)出願番号　特願平9-188064
(22)出願日　平成9年7月14日(1997.7.14)
(65)公開番号　特開平11-31204
(43)公開日　平成11年2月2日(1999.2.2)
審査請求日　平成13年10月25日(2001.10.25)

(73)特許権者　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目１７番２２号
(74)代理人　100086531
弁理士　澤田　俊夫
(72)発明者　寺尾　太郎
神奈川県足柄上郡中井町境４３０　グリーンテクなかい　富士ゼロックス株式会社内
(72)発明者　亀井　光久
神奈川県足柄上郡中井町境４３０　グリーンテクなかい　富士ゼロックス株式会社内
(72)発明者　中津山　恒
神奈川県足柄上郡中井町境４３０　グリーンテクなかい　富士ゼロックス株式会社内

最終頁に続く

(54)【発明の名称】電子チケットシステム

(57)【特許請求の範囲】

【請求項１】

チケット発行装置、検証装置、証明装置からなる電子チケットシステムであって、上記チケット発行装置は、指定されたチケット仕様ごとに用意された少なくともチケット公開情報とチケット秘密情報を保持するチケット特徴情報保持手段と、証明装置固有情報を保持する証明装置固有情報保持手段と、少なくともチケット秘密情報と証明装置固有情報とに対して予め定められたチケット生成用演算を実行した実行結果から、デジタル情報であるチケットを作成するチケット発行手段とからなり、上記検証装置は、対話証明で用いられる値を生成する認証情報生成手段と、上記証明装置がチケット秘密情報を算出できたか否かを検証する対話検証手段とからなり、上記証明装置は、当該証明装置の証明装置固有情報を保持する証明装置固有情報保持手段と、デジタル情報であるチケットを保持するチケット保持手段と、少なくとも証明装置固有情報とチケットとに対して予め定められた証明情報生成用演算を実行した実行結果から証明情報を生成してチケット秘密情報に関する知識の証明を行なえる対話証明手段とからなり、

さらに、上記チケット秘密情報、上記証明装置固有情報および上記チケットが対応する場合に、上記検証装置の上記対話検証手段が、上記証明装置が上記チケット秘密情報を算出できたと検証するように、上記チケット生成用演算と上記証明情報生成用演算とを選定したことを特徴とする電子チケットシステム。

【請求項２】

請求項１の電子チケットシステムであって、上記チケット発行装置は、チケット特徴情

報を作成できるチケット特徴情報作成手段を備えたことを特徴とする電子チケットシステム。

【請求項３】

請求項１または２記載の電子チケットシステムであって、上記チケット発行装置は、証明装置識別情報を証明装置固有情報と関連づけて保持する証明装置識別情報保持手段を備えたことを特徴とする電子チケットシステム。

【請求項４】

請求項１、２または３記載の電子チケットシステムであって、チケット特徴情報は少なくともチケット公開情報とチケット秘密情報からなることを特徴とする電子チケットシステム。

【請求項５】

請求項４記載の電子チケットシステムであって、チケット公開情報が有限アーベル群であり、チケット秘密情報がその零化域であることを特徴とする電子チケットシステム。

【請求項６】

請求項４記載の電子チケットシステムであって、チケット秘密情報が整数であり、チケット公開情報が有限群とその元とその元の位数とその元の秘密情報倍であることを特徴とする電子チケットシステム。

【請求項７】

請求項１～６のいずれかに記載の電子チケットシステムであって、証明装置は可変な内部状態を保持する内部状態保持手段を備えたことを特徴とする電子チケットシステム。

【請求項８】

請求項７記載の電子チケットシステムであって、上記証明装置の内部状態保持手段が保持する可変な内部状態の少なくとも一部は外部から書き換え不能であることを特徴とする電子チケットシステム。

【請求項９】

請求項８記載の電子チケットシステムであって、上記証明装置は初期化が行なわれた内部状態を示す情報を保持するチケットカウント手段を備えたことを特徴とする電子チケットシステム。

【請求項１０】

請求項７、８、または９記載の電子チケットシステムであって、対話検証および対話証明の過程で少なくとも１度の秘密情報に関する知識の証明の観点から冗長な情報伝達を行なうことを特徴とする電子チケットシステム。

【請求項１１】

請求項９記載の電子チケットシステムであって、少なくとも１度は証明装置の内部情報から得られる情報を上記証明装置から上記検証装置に伝達することを特徴とする電子チケットシステム。

【請求項１２】

請求項１１記載の電子チケットシステムであって、少なくとも１度は、外部から書き換え不能な上記証明装置の内部情報から得られる情報を上記証明装置から上記検証装置に伝達することを特徴とする電子チケットシステム。

【請求項１３】

請求項８または９記載の電子チケットシステムであって、上記証明装置の内部状態保持手段はチケットの有効性を示す内部状態をチケットと関連づけて外部から書き換え不能な形で保持し、上記チケットの有効性を示す内部状態が特定の値であるときには、対応するチケットが無効であるものとして、対話証明時に伝達する情報として正しくないものを伝達することを特徴とする電子チケットシステム。

【請求項１４】

請求項１３記載の電子チケットシステムであって、上記検証装置は少なくとも１度、上記証明装置に情報を伝達し、上記証明装置は、上記検証装置から伝達される情報にしたがって、チケットと関連付けられた、チケットの有効性を示す内部状態を変更して、有効な

チケットの無効化あるいは無効となったチケットの有効化を行なうことを特徴とする電子チケットシステム。

【請求項１５】

請求項８または９記載の電子チケットシステムであって、上記証明装置の内部状態保持手段は、チケットのカウンタとして機能する内部状態をチケットと関連づけ、外部から書き換え不能な形で保持し、対話証明の過程でチケットのカウンタとして機能する内部状態を用いて演算を行ない、演算結果が所定の値であるときには、対応するチケットが無効であるものとして、対話証明時に伝達する情報として正しくないものを伝達することを特徴とする電子チケットシステム。

【請求項１６】

請求項１５の電子チケットシステムであって、上記検証装置は少なくとも１度、上記証明装置に情報を伝達し、上記証明装置は、上記検証装置から伝達される情報にしたがって、チケットと関連付けられた、チケットのカウンタとして機能する内部状態を設定することを特徴とする電子チケットシステム。

【請求項１７】

請求項１～１６のいずれかに記載の電子チケットシステムであって、上記証明装置は複数の対話検証手続きを実行可能な証明手順実行部を備え、チケット特徴情報の一部を用いて、適切な証明手順を選択し、対話証明を実行することを特徴とする電子チケットシステム。

【請求項１８】

請求項１～１６のいずれかに記載の電子チケットシステムであって、上記証明装置は対話検証手続きの少なくとも一部のステップを記述したプログラムを実行可能な証明手順実行部を備え、チケット特徴情報の一部からプログラムを抽出し、対話証明を実行することを特徴とする電子チケットシステム。

【請求項１９】

請求項１～１８のいずれかに記載の電子チケットシステムであって、上記検証装置は、対話検証手続きにおいて、上記検証装置および上記証明装置間で通信された情報、あるいはその一部、あるいはそれらに所定の演算を施して生成した情報を保存することを特徴とする電子チケットシステム。

【請求項２０】

請求項１～１９のいずれかに記載の電子チケットシステムであって、上記検証装置は対話検証手続きにおいて上記証明装置に伝達した情報の生成に利用した情報と、上記証明装置が上記情報に演算を施して応答した情報の組を保存することを特徴とする電子チケットシステム。

【請求項２１】

請求項１～２０のいずれかに記載の電子チケットシステムであって、上記検証装置は、上記検証装置の固有情報を保持する検証装置固有情報保持手段と、チケットを保持するチケット保持手段を備え、対話検証においてチケットからの情報を利用することを特徴とする電子チケットシステム。

【請求項２２】

請求項１～２１のいずれかに記載の電子チケットシステムであって、上記証明装置は、認証情報とチケット公開情報とチケットとチケット付加情報と証明装置固有情報とより所定の方法で証明情報を計算することを特徴とする電子チケットシステム。

【請求項２３】

請求項２２の電子チケットシステムであって、チケットの秘密情報がＤであり、チケットの公開情報が（ｎ，Ｅ）であり、λ（ｎ）が法ｎの下で位数が最大となる数の位数であり、ＥＤ≡１　ｍｏｄ　λ（ｎ）であり、チケットの付加情報がＬであり、証明装置固有情報が秘密の一方向性関数d_U（Ｌ，ｎ）であり、チケットがｔ：＝Ｄ－d_U（Ｌ，ｎ）で与えられているとき、上記証明装置は、認証情報Ｃに対して、証明情報ＲをＣの法ｎでのｔによる冪乗と、Ｃの法ｎでの一方向性関数値d_U（Ｌ，ｎ）を指数とする冪乗との法

ｎでの積$C^{t}C^{dU(L,n)}$ ｍｏｄ ｎとして証明情報を計算することを特徴とする電子チケットシステム。

【請求項２４】

請求項２２記載の電子チケットシステムであって、チケットの秘密情報がＤであり、チケットの公開情報が（ｎ，Ｅ）であり、ＥＤ≡１ ｍｏｄ λ（ｎ）であり、チケットの付加情報がＬであり、証明装置固有情報が秘密の値d_Uであり、ｆ（d_U，Ｌ，ｎ）を一方向性関数として、チケットがｔ：＝Ｄ－ｆ（d_U，Ｌ，ｎ）で与えられているとき、上記証明装置は、認証情報Ｃに対して、証明情報ＲをＣの法ｎでのｔによる冪乗と、Ｃの法ｎでの一方向性関数値ｆ（d_U，Ｌ，ｎ）を指数とする冪乗との法ｎでの積$C^{t}C^{f(dU,L,n)}$ ｍｏｄ ｎとして証明情報を計算することを特徴とする電子チケットシステム。

【請求項２５】

請求項２２記載の電子チケットシステムであって、チケットの秘密情報がｘであり、ｐが素数であり、Ｇが離散対数問題が困難な有限群であり、ｇが有限群Ｇの位数ｐの元であり、チケットの公開情報が（ｐ，Ｇ，ｇ，ｙ）であり、$y=g^{x}$であり、チケットの付加情報がＬであり、証明装置固有情報が秘密の一方向性関数d_U（Ｌ，ｙ）であり、チケットがｔ：＝ｘ－d_U（Ｌ，ｙ）で与えられているとき、上記証明装置は、認証情報Ｃに対して、証明情報ＲをＣのｔを指数とする冪乗と、Ｃの一方向性関数値d_U（Ｌ，ｙ）を指数とする冪乗との積$C^{t}C^{dU(L,y)}$として証明情報を計算することを特徴とする電子チケットシステム。

【請求項２６】

請求項２２記載の電子チケットシステムであって、チケットの秘密情報がｘであり、チケットの公開情報が（ｐ，Ｇ，ｇ，ｙ）であり、$y=g^{x}$であり、チケットの付加情報がＬであり、証明装置固有情報が秘密の値d_Uであり、ｆ（d_U，Ｌ，ｙ）を一方向性関数として、チケットがｔ：＝ｘ－ｆ（d_U，Ｌ，ｙ）で与えられているとき、上記証明装置は、認証情報Ｃに対して、証明情報ＲをＣのｔを指数とする冪乗と、Ｃの一方向性関数値ｆ（d_U，Ｌ，ｙ）を指数とする冪乗との積$C^{t}C^{f(dU,L,y)}$として証明情報を計算することを特徴とする電子チケットシステム。

【請求項２７】

請求項２２記載の電子チケットシステムであって、上記検証装置は、認証情報と証明情報とチケット公開情報とより証明情報が正しいかどうかを判定し、証明情報が正しい場合は、証明情報に埋め込まれた情報を導出することを特徴とする電子チケットシステム。

【請求項２８】

請求項２７記載の電子チケットシステムであって、上記検証装置は、認証情報Ｃと証明情報Ｒとチケット公開情報（ｎ，Ｅ）との場合、証明情報Ｒを法ｎでＥ乗したものをＣと比較し、あるビット列Ｍがあって、R^{E} ｍｏｄ ｎ＝Ｃ｜｜Ｍ（ＣとＭとのビット連結）となっていれば証明情報は正しいと判定し、証明情報が正しい場合はＭを証明情報に埋め込まれた情報として導出することを特徴とする電子チケットシステム。

【請求項２９】

請求項２７記載の電子チケットシステムであって、上記検証装置は、認証情報Ｃと証明情報Ｒとチケット公開情報（ｎ，Ｅ）との場合、Ｉを予め与えた限界として、あるＭ＜Ｉに対して、証明情報Ｒを法ｎでE^{M}乗したものとＣとが等しければ証明情報は正しいと判定し、証明情報が正しい場合はＭを証明情報に埋め込まれた情報として導出することを特徴とする電子チケットシステム。

【請求項３０】

請求項２２記載の電子チケットシステムであって、上記証明装置は、チケットとチケット付加情報と証明装置固有情報とより所定の方法でチケット秘密情報を計算し、認証情報に対して、前記チケット秘密情報を用いた計算を施すことによって証明情報を生成することを特徴とする電子チケットシステム。

【請求項３１】

請求項３０記載の電子チケットシステムであって、チケットの秘密情報がＤであり、チケットの付加情報がＬであり、証明装置固有情報がある暗号系の復号鍵d_Uであり、証明装置固有情報に対応する暗号化をE_Uとして、上記証明装置は、チケットがｔ：＝E_U（Ｄ｜｜Ｌ）で与えられているとき、チケットｔをd_Uによって復号してチケット秘密情報Ｄとチケット付加情報Ｌを計算することを特徴とする電子チケットシステム。

【請求項３２】

請求項３０記載の電子チケットシステムであって、チケットの秘密情報がＤであり、チケットの付加情報がＬであり、証明装置固有情報がある暗号系の復号鍵d_Uであり、証明装置固有情報に対応する暗号化をE_Uとし、ｈ（Ｌ）を一方向性関数として、上記証明装置は、チケットがｔ：＝E_U（Ｄ｜｜ｈ（Ｌ））で与えられているとき、チケットｔをd_Uによって復号してチケット秘密情報Ｄを計算し、チケット付加情報Ｌの一方向性関数値ｈ（Ｌ）を計算することにより、Ｌの完全性を検証することを特徴とする電子チケットシステム。

【請求項３３】

請求項３０記載の電子チケットシステムであって、チケットの秘密情報がＤであり、チケットの付加情報がＬであり、証明装置固有情報がある暗号系の復号鍵d_Uであり、証明装置固有情報に対応する暗号化をE_Uとし、ｈ（Ｌ）を一方向性関数として、チケットがｔ：＝（E_U（Ｄ）、ｈ（d_U｜｜Ｄ｜｜Ｌ））で与えられているとき、上記証明装置はチケットｔの第１成分をd_Uによって復号してチケット秘密情報Ｄを計算し、チケットｔの第２成分と一方向性関数値ｈ（d_U｜｜Ｄ｜｜Ｌ）とを比較することによってチケット付加情報Ｌの完全性を検証することを特徴とする電子チケットシステム。

【請求項３４】

請求項２７～２９のいずれかに記載の電子チケットシステムであって、上記証明装置は、出力情報保持手段を持ち、前記チケット秘密情報を用いた計算を施す際に、出力情報保持手段に保持された出力情報と認証情報より証明情報を計算することを特徴とする電子チケットシステム。

【請求項３５】

請求項３４記載の電子チケットシステムであって、上記証明装置は、出力情報保持手段を持ち、チケットの秘密情報をＤとし、出力情報保持手段に保持された出力情報をＭとし、認証情報をＣとすると、証明情報を

【数１】

$$C^{D^M} \bmod n$$

として計算することを特徴とする電子チケットシステム。

【請求項３６】

請求項３４記載の電子チケットシステムであって、上記証明装置は、出力情報保持手段を持ち、前記チケット秘密情報を用いた計算を施す前に、出力情報保持手段に保持された出力情報を用いて認証情報を更新することを特徴とする電子チケットシステム。

【請求項３７】

請求項３６記載の電子チケットシステムであって、上記証明装置は、出力情報保持手段を持ち、出力情報保持手段に保持された出力情報をＭとし、認証情報をＣとすると、認証情報をＣ｜｜Ｍに更新することを特徴とする電子チケットシステム。

【請求項３８】

請求項２２記載の電子チケットシステムであって、上記証明装置は、第２の認証情報生成手段を持ち、第２の認証情報と第２の証明情報とチケット付加情報とより第２の証明情報が正しいかどうかを判定し、第２の証明情報が正しい場合、上記証明装置の内部状態を更新することを特徴とする電子チケットシステム。

【請求項３９】

請求項３８記載の電子チケットシステムであって、チケット付加情報Ｌは少なくとも上記検証装置を検証するための情報ν｜｜εの一部を含み、εとλ（ν）は互いに素として

、上記証明装置は、第２の認証情報χと第２の証明情報ρが
【数２】
$$\chi = \rho^{\varepsilon} \bmod \nu$$
を満たすときに第２の証明情報が正しいと判定することを特徴とする電子チケットシステム。
【請求項４０】
請求項３８記載の電子チケットシステムであって、チケット付加情報Ｌは少なくともηの一部を含み、上記証明装置は、第２の認証情報g^{s}と第２の証明情報ρが
【数３】
$$\rho = \eta^{s} \bmod p$$
を満たすときに第２の証明情報が正しいと判定することを特徴とする電子チケットシステム。
【請求項４１】
請求項３８記載の電子チケットシステムであって、上記証明装置は、入力情報保持手段を持ち、第２の証明情報が正しい場合は、第２の証明情報に埋め込まれた入力情報を導出し、入力情報保持手段に保持することを特徴とする電子チケットシステム。
【請求項４２】
請求項４１記載の電子チケットシステムであって、チケット付加情報Ｌは少なくともν||εの一部を含み、εとλ（ν）は互いに素として、上記証明装置は、第２の認証情報χと第２の証明情報ρがあるビット列μに対して、
【数４】
$$\chi \| \mu = \rho^{\varepsilon} \bmod \nu$$
を満たすときに第２の証明情報が正しいと判定し、μを第２の証明情報に埋め込まれた入力情報として入力情報保持手段に保持することを特徴とする電子チケットシステム。
【請求項４３】
請求項４１記載の電子チケットシステムであって、チケット付加情報Ｌは少なくともν||εの一部を含み、上記証明装置は、第２の認証情報χと第２の証明情報ρがＩを予め与えた限界として、あるμ＜Ｉに対して、
【数５】
$$\chi = \rho^{\varepsilon^{\mu}} \bmod \nu$$
を満たすときに第２の証明情報が正しいと判定し、μを第２の証明情報に埋め込まれた入力情報として入力情報保持手段に保持することを特徴とする電子チケットシステム。
【請求項４４】
請求項２２記載の電子チケットシステムであって、上記証明装置は、入力情報保持手段を持ち、入力情報保持手段に保持された入力情報に基づいて内部状態保持手段に保持された内部状態を更新することを特徴とする電子チケットシステム。
【請求項４５】
請求項２２記載の電子チケットシステムであって、上記証明装置は、認証情報とチケット付加情報とに基づいて、証明情報を正しく生成するか否かを判定することを特徴とする電子チケットシステム。
【請求項４６】
請求項２２記載の電子チケットシステムであって、上記証明装置は、内部状態とチケット付加情報とに基づいて、証明情報を正しく生成するか否かを判定することを特徴とする電子チケットシステム。
【請求項４７】
請求項２２記載の電子チケットシステムであって、上記証明装置は、内部状態とチケット付加情報とに基づいて、出力情報を計算し、出力情報保持手段に保持することを特徴とする電子チケットシステム。

【請求項４８】
請求項２２記載の電子チケットシステムであって、上記検証装置は、第２の認証情報と特権を表す秘密情報とより第２の証明情報を生成することを特徴とする電子チケットシステム。
【請求項４９】
請求項４８記載の電子チケットシステムであって、特権を表す秘密情報をδとして、対応する公開情報を（ν，ε）として、εδ≡１　ｍｏｄ　λ（ν）が満たされるとき、上記検証装置は、第２の認証情報χより第２の証明情報ρを
【数６】

$$\rho := \chi^{\delta} \bmod \nu$$

として生成することを特徴とする電子チケットシステム。
【請求項５０】
請求項４８記載の電子チケットシステムであって、特権を表す秘密情報をξとして、対応する公開情報を（ｐ，ｇ，ｑ，η）として、
【数７】

$$\eta = g^{\xi} \bmod p$$

が満たされるとき、上記検証装置は、第２の認証情報χより第２の証明情報ρを
【数８】

$$\rho := \chi^{\xi} \bmod p$$

として生成することを特徴とする電子チケットシステム。
【請求項５１】
請求項４８、４９または５０記載の電子チケットシステムであって、上記検証装置は、入力情報保持手段を持ち、前記特権を表す秘密情報を用いた計算を施す際に、入力情報保持手段に保持された入力情報と第２の認証情報をより第２の証明情報を計算することを特徴とする電子チケットシステム。
【請求項５２】
請求項５１記載の電子チケットシステムであって、特権を表す秘密情報をδとして、対応する公開情報を（ν、ε）として、εδ≡　１　ｍｏｄ　λ（ν）が満たされるとき、上記検証装置は、入力情報保持手段に保持された入力情報μと　第２の認証情報χより第２の証明情報ρを
【数９】

$$\rho := \chi^{\delta^{\mu}} \bmod \nu$$

として生成することを特徴とする電子チケットシステム。
【請求項５３】
請求項４８、４９または５０記載の電子チケットシステムであって、上記検証装置は、入力情報保持手段を持ち、前記特権を表す秘密情報を用いた計算を施す前に、入力情報保持手段に保持された入力情報を用いて第２の認証情報を更新することを特徴とする電子チケットシステム。
【請求項５４】
請求項５３記載の電子チケットシステムであって、上記検証装置は、入力情報保持手段を持ち、入力情報保持手段に保持された入力情報をμとし、第２の認証情報をχとすると、第２の認証情報をχ｜｜μに更新することを特徴とする電子チケットシステム。
【請求項５５】
権利を表象するデジタル情報からなるチケットを発行する電子チケット発行装置であって、デジタル情報であるチケットを保持するチケット保持手段と、少なくとも証明装置固有情報とチケットとに対して予め定められた証明情報生成用演算を実行した実行結果から

証明情報を生成してチケット秘密情報に関する知識の証明を行なえる対話証明手段とを具備する証明装置と、対話証明で用いられる値を生成する認証情報生成手段と、上記証明装置がチケット秘密情報を算出できたか否かを検証する対話検証手段とを具備する上記検証装置とともに用いられる、上記電子チケット発行装置において、

少なくともチケット秘密情報を保持するチケット特徴情報保持手段と、

チケット利用者固有情報を保持するチケット利用者固有情報保持手段と、

少なくとも上記チケット秘密情報および上記チケット利用者固有情報に対して予め定められたチケット生成用演算を実行した実行結果から、チケットを作成するチケット発行手段とからなり、

さらに、上記チケット秘密情報、上記証明装置固有情報および上記チケットが対応する場合に、上記検証装置の上記対話検証手段が、上記証明装置が上記チケット秘密情報を算出できたと検証するように、上記チケット生成用演算と上記証明情報生成用演算とを選定したことを特徴とする電子チケット発行装置。

【請求項５６】

権利を表象するデジタル情報からなるチケットを用いて上記権利を有することを証明する電子チケット証明装置であって、指定されたチケット仕様ごとに用意された少なくともチケット公開情報とチケット秘密情報を保持するチケット特徴情報保持手段と、証明装置固有情報を保持する証明装置固有情報保持手段と、少なくともチケット秘密情報と証明装置固有情報とに対して予め定められたチケット生成用演算を実行した実行結果から、デジタル情報であるチケットを作成するチケット発行手段とを具備するチケット発行装置と、対話証明で用いられる値を生成する認証情報生成手段と、上記証明装置がチケット秘密情報を算出できたか否かを検証する対話検証手段とを具備する検証装置とともに用いられる上記電子チケット証明装置において、

チケット利用者固有情報を保持するチケット利用者固有情報保持手段と、

少なくともチケット秘密情報と上記チケット利用者固有情報とから生成されたデジタル情報からなるチケットを保持するチケット保持手段と、

少なくとも上記チケット利用者固有情報と上記チケットとに対して予め定められた証明情報生成用演算を実行した実行結果から、上記チケット秘密情報なしには生成できない証明情報を生成する証明手段とを有し、

さらに、上記チケット秘密情報、上記証明装置固有情報および上記チケットが対応する場合に、上記検証装置の上記対話検証手段が、上記証明装置が上記チケット秘密情報を算出できたと検証するように、上記チケット生成用演算と上記証明情報生成用演算とを選定したことを特徴とする証明装置。

【請求項５７】

権利を表象するデジタル情報からなるチケットを用いて電子チケット証明装置により生成された証明情報を検証して上記電子チケット証明装置の担持者が上記権利を有することを検証する電子チケット検証装置であって、指定されたチケット仕様ごとに用意された少なくともチケット公開情報とチケット秘密情報を保持するチケット特徴情報保持手段と、証明装置固有情報を保持する証明装置固有情報保持手段と、少なくともチケット秘密情報と証明装置固有情報とに対して予め定められたチケット生成用演算を実行した実行結果から、デジタル情報であるチケットを作成するチケット発行手段とを具備するチケット発行装置と、当該証明装置の証明装置固有情報を保持する証明装置固有情報保持手段と、デジタル情報であるチケットを保持するチケット保持手段と、少なくとも証明装置固有情報とチケットとに対して予め定められた証明情報生成用演算を実行した実行結果から証明情報を生成してチケット秘密情報に関する知識の証明を行なえる対話証明手段とを具備するチケット証明装置とともに用いられる上記電子チケット検証装置において、

認証用の情報を生成する手段と、

少なくともチケット秘密情報とチケット証明装置の固有情報とから生成されたデジタル情報からなるチケットと、上記チケット証明装置の固有情報とに基づいて生成された証明情報が、上記チケット秘密情報に関連して生成されていることを検証する手段とを有し、

さらに、上記チケット秘密情報、上記証明装置固有情報および上記チケットが対応する場合に、上記検証装置の上記対話検証手段が、上記証明装置が上記チケット秘密情報を算出できたと検証するように、上記チケット生成用演算と上記証明情報生成用演算とを選定したことを特徴とする電子チケット検証装置。

【請求項５８】

検証装置および証明装置を用いて行う権利証明方法において、

当該権利証明方法は、指定されたチケット仕様ごとに準備されたチケット秘密情報と証明装置固有情報とに対して予め定められたチケット生成用演算を実行した実行結果としてチケット発行装置により生成されたデジタル情報であるチケットを用い、

上記証明装置は、上記チケットと、自ら保有する証明装置固有情報とに対して予め定められた証明情報生成用演算を実行した実行結果から証明情報を生成し、

上記検証装置は、上記証明情報が上記チケット秘密情報に関連して生成されたことを検証して上記チケットに関連する権利の存在を証明し、

さらに、上記チケット秘密情報、上記証明装置固有情報および上記チケットが対応する場合に、上記検証装置が、上記証明装置が上記チケット秘密情報を算出できたと検証するように、上記チケット生成用演算と上記証明情報生成用演算とを選定した権利証明方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、チケットやカードの作成、発行および利用の技術に関する。

【０００２】

【従来の技術】

乗車券、通行券、入場券、指定券、予約券、回数券、定期券、商品券、プリペイドカード、ポイントカード、会員証、通行証、許可証などは、それを保持する者（以下では利用者と呼ぶ）がそれに応じた各々の権利を保持することを証明する。ここでは、これらをまとめてチケットと呼ぶ。一般にチケットは、利用者に権利を与える者もしくはその代理人（以下ではまとめて発行者と呼ぶ）が発行して、利用者が保持管理する。従来、チケットは、紙やプラスティックなどへ印刷やエンボス加工などの処理を施すことで実現されていた。

【０００３】

このようなチケットをここでは紙チケットと呼ぶ。近年では、発行者が、利用者に与えた権利を特定できて、正しいチケットであることを検証できる、という機能を持つ電子チケットを実現する試みがなされている。電子情報は、作成が容易であり、通信回線を通して送信できるという特長を持つ。しかしながら、完全なコピーを簡単に作れるので、電子チケットを実現するには、偽造と複製による不正利用への対策が必要である。電子署名により偽造は防止できるが、複製の防止は困難である。

このため、複製による不正利用を防止することが、電子チケットの実現にあたっての最大の課題となっている。

【０００４】

従来、電子チケットは、チケットの利用時に正当な利用者か確認する第１の従来技術、発行者以外の者にチケットを複写する機会を与えない第２の従来技術、検証時の通信を公開できるように第２の従来技術を修正した第３の従来技術の、３つの方法で実現されてきた。

【０００５】

以下、各従来技術について順次説明する。

【０００６】

第１の従来技術は、チケットの利用時に正当な利用者か確認する方法である。この方法では、正当な利用者であるかを確認するために必要な情報（利用者特定情報）と、与えた権利とを対応づける情報をチケットとして発行して、利用者が記録管理する。発行者以外の者が勝手にチケットを偽造できないようにするためには、発行者がチケットに電子署名を

施す。電子署名のないチケットは、偽造されたものと判断される。

【０００７】

不正に複写したチケットの利用を防止するため、利用者は、チケットを利用する時に、チケットとともに、自分が利用者特定情報に適合する正当な利用者であることを示す。利用者特定情報に適合していれば、対応する権利の行使が認められ、適合していなければ拒否される。利用者特定情報には、身元、顔写真などの身体的特徴、パスワードなどの知識の所有、などが利用できる。身元を利用する場合には、身分証明書などを提示させて確認した身元を利用できる。顔写真などの身体的特徴の場合には、利用者はそれを提示する。パスワードの場合には、そのパスワードを利用者が入力する。

【０００８】

第２の従来技術は、発行者以外の者にチケットを複写する機会を与えない方法である。この方法では、利用者特定情報を用いる必要がないので、匿名性を持ったチケットを実現できる。しかし、不正にチケットを複写した場合に、その複写したチケットの不正利用を防止する方法がないので、チケットの複写を直接防止する必要がある。このため、利用者が保持管理しているチケットを複写できないようにする機構と、発行時や検証時の通信からチケットが漏洩しない機構の両方を必要とする。前者の達成のため、利用者は、発行者以外の者が自由に内容を変更できない装置を所持して、その装置の中にチケットを記録する方法をとっている。後者の達成のため、盗聴できない通信方法をとっている。

【０００９】

この従来技術の一例が、特開平８－１４７５００号公報で開示されている。この方法では，利用者が携帯するチケット格納装置に、チケット発行者がチケットの内容に電子署名を加えたチケットを閉じ込めることで、電子チケットを実現している。電子署名をしているので偽造は困難である。チケット格納装置からチケットを取り出すのに特別な命令を必要とすることで、チケットを複写されることを防止している。この方法によれば、チケット発行者毎に異なる署名鍵を利用できるので、複数のチケット発行者が発行した複数のチケットを、単一の格納装置に格納できる。また、利用者に関する情報を知らなくても、チケットの署名の正当性を確認するだけで検証が可能である。

【００１０】

第３の従来技術は、検証時の通信を公開できるように第２の従来技術を修正した方法である。

【００１１】

この方法では、チケットを秘密情報として利用者の所持する装置（証明器）に複写できないように記録するのは第２の従来技術と同じであるが、検証の方法が異なる。まず、検証を行う検証器は、証明器に乱数などの繰り返し利用されない値（チャレンジ）を送る。証明器は、チケットである秘密情報を利用した演算をチャレンジに対して施して、得られた値（レスポンス）を検証器に送り返す。検証器は、秘密情報とチャレンジを利用してレスポンスが演算されたことを確認することで、利用者の正当性を認証する。チャレンジとレスポンスから秘密情報を求めることを計算量的に困難とすることで、検証器と証明器との通信を秘匿する必要がなくなる。

【００１２】

セキュリティ施設へのアクセス制御のための認証に目的が限定されているが、第３の従来技術と同様の機能を提供する方法が、特公平６－５２５１８号公報で開示されている。この方法では、第３の従来技術に加えて、検証者が利用者に対応する証明器の秘密情報を管理しなくてもよいという特徴を持つ。利用者は、第３の従来技術における証明器に相当する携帯用物体を携帯している。認証を行う通信では、認証を行う施設（検証器）は、利用者もしくは携帯用物体から識別番号を受け取り、この識別番号から携帯用物体に固有のシークレット・コードと呼ばれる秘密情報を計算する。この秘密情報を利用したチャレンジ・レスポンスを行って利用者を認証するので、検証器は秘密情報を保持管理する必要がない。

【００１３】

【従来の技術の問題点】
現在紙チケットが果たしている役割を電子チケットが担うには、発行者が、利用者に与えた権利を特定できて、正しいチケットであることを検証できる、という機能だけでは不十分である。当事者間で争いが生じた時には第三者による調停が必要である。このため、紙チケットが果たしていた、権利を証明する機能が、電子チケットにも必要になる。
【００１４】
したがって、電子チケットには、次の３点の機能が必須である。第１点は、正当な権利を持たないものが、不当にチケットを利用することを防止する機能である。第２点は、利用者が自分の保持するチケットの正当性を確認できる機能である。第３点は、チケットに与えられた権利内容を第三者に証明する機能である。ただし、第３の機能は第２の機能を包含しているので、第１と第３の機能が実現されれば、チケットに必須の機能が満たされる。さらに、第４点として、利用者の匿名性を保証する機能が要請されることもある。
【００１５】
第１の従来技術では、利用する利用者特定情報に応じて、いくつかの機能が失われる。
【００１６】
利用者特定情報に利用者の身元を利用する方法では、発行時と検証時に利用者の身元が明らかになる。利用者特定情報に顔写真などの身体的特徴を利用する方法では直接身元が特定される訳ではないが、人物を特定するという意味で匿名性が失われている。いずれの方法にしても匿名性が失われるので、匿名性を有するチケット（第４の機能）が実現できない。
【００１７】
さらに、通信回線を利用した遠隔的な環境で身分を安全に証明する方法は実現されていないので、このような環境では第１の機能を提供できない。
【００１８】
第１の従来技術において、利用者特定情報にパスワードを利用する方法では、匿名性の問題は軽減されるが、パスワードを記憶する負荷を利用者にあたえる。また、利用者が故意にパスワードを漏洩させることを防止できないので、不正利用の危険が増し、チケットに必要な第１の機能が達成されていない。
【００１９】
第２の従来技術では、利用者が保管しているチケットを複写できなくするのに加えて、発行者がチケットの正当性を検証している時の通信の内容も機密にしている。これより２つの問題が生じる。第１の問題は、発行者以外の者はチケットを複写できないので、チケットの正当性を第三者に証明することが困難になることである。これは、チケットに必要な機能の第３が達成されていないことを示す。第２の問題は、チケットの発行時と検証時の通信の内容も機密に行うので、チケットの発行時と検証時にプライバシーなどの利用者の権利が侵害されていないことを証明できないことである。
【００２０】
特開平８－１４７５００号公報に開示された方法は第２の従来技術の一例であるから、上述の問題を有する。
【００２１】
第３の従来技術は、認証のために利用されるものであり、正当なチケットを保持しているか否か以外に情報を伝達しない。このため、有効期限などを示すことができず、単純なチケットしか表現できない。また、チケットを証明器に送信する方法が、第３の従来技術と同様に機密通信で行う必要があり、不当に利用者の情報を開示して利用者の権利を侵害していないことを証明できない。
【００２２】
特公平６－５２５１８号公報に開示されている方法は第３の従来技術の一例であるから、上述の問題を有する。
【００２３】
これまでに述べたように、従来の技術はいずれも、チケットに必要な第１の機能である不

正利用を防止する機能を実現するために、第２および第３の機能である第三者に対するチケットの内容証明の機能や、第４の機能である利用者の匿名性を、犠牲にしている点に問題があった。

【００２４】

【解決しようとする課題】

そこで本発明は、上記の問題を解決するために、第１の機能として、偽造や複製などによる不正利用が非常に難しく、第２および第３の機能として、チケットの内容を第三者に証明できて、第４の機能として、チケットの利用時に利用者の匿名性が維持されるチケットの作成・発行・利用システムを実現することを課題とする。

【００２５】

【課題を解決するための手段】

本発明に係わる電子チケットシステムは、以下のチケット発行装置とチケット証明装置とチケット検証装置とからなる。チケットを発行するチケット発行装置は、チケットの特徴情報を保持する手段と、証明装置の固有情報を保持する手段と、チケットの特徴情報と証明装置の固有情報からチケットを計算する手段とを持つ。チケット証明装置は、チケット保持手段と、チケット検索手段と、固有情報保持手段と、内部状態保持手段と、証明手順実行手段と、検証装置との通信手段とを持つ。チケット検証装置は、検証手順実行手段と、証明装置との通信手段とをを持つ。

【００２６】

チケット発行装置は、チケットの特徴情報と証明器の固有情報とからチケットを発行する。証明装置は、チケット発行装置が発行したチケットを保持する。また、検証装置と通信手段を介して接続し、保持するチケットに対応する証明手順を実行することによって対話を行ない、証明を成功させることによってチケットの利用がなされる。証明手順実行手段は手順の実行において、検証装置から送信されたチケット識別子に対応するチケットを、検索手段を用いて検索し、対応するチケットが存在する場合には、そのチケットを用いて証明手順を実行する。証明手順の実行にあたっては固有情報保持手段に保持された固有情報と内部状態保持手段に保持された内部情報を用いることができる。チケットの利用では、証明装置は特徴情報から決定されるチケットの有効性の証明と、チケットに対応する情報の更新や伝達が行なわれる。検証装置は、証明装置と通信手段を介して接続し、検証手順を実行することによって対話を行ない、対話の結果によって証明装置が有効なチケットを保持していることを検証する。チケットの検証では、検証装置は特徴情報から決定されるチケットの有効性の検証と、証明装置の保持するチケットに対応する情報の更新指示や獲得を行う。

【００２７】

【発明の実施の態様】

以下、本発明の詳細をつぎの順に説明する。

【００２８】
［１．実施例全体の概要］
（図１、図２、図３、図１２、図２８、図２９）
図１は本発明の電子チケットシステムの構成図である。図１において、この発明の電子チケットシステムは、チケット作成・発行装置１、チケット証明装置２、およびチケット検証装置３を含んで構成されている。チケット作成・発行装置１はチケット作成手段４およびチケット発行手段５を有している。チケット作成手段４は、チケット作成依頼者（チケットを受け取って対価を享受する者や、その代理人）のチケット作成依頼に基づいて、所定のサービスや物に対応するチケットの仕様を作成する。チケット発行手段５は、チケット発行依頼者（チケットを示してサービス等の提供を受けたい者またはその代理人）のチケット発行依頼に基づいて、チケット識別子と証明器識別子とチケット仕様識別子とチケット付加情報を入力として、対応するチケットを発行する。
【００２９】
チケット証明装置２は、チケット発行手段５の発行したチケットを保持し、チケット検証装置３と通信を行ないチケットの保有を証明する。チケット検証装置３は、チケット作成手段４の作成したチケット識別子とチケット検証手順を保持し、チケット証明装置２と通信を行ないチケットの検証を行なう。なお、以下では、チケット作成・発行装置１、チケット証明装置２およびチケット検証装置３をそれぞれチケット作成・発行器、チケット証明器およびチケット検証器または単に作成・発行器、証明器および検証器と呼ぶことがある。
【００３０】
図２および図３はチケット作成・発行装置１の構成を全体として示している。また、図１２はチケット証明装置２およびチケット検証装置３の構成を全体として示している。なお、図２および図３はほぼ同一の構成を示している。ただし、図２が一般的な公開暗号系を認証に用いる例を説明するのに対して、図３はＲＳＡ公開暗号系を認証に用いる例を説明している。
【００３１】
図２において、チケット作成・発行装置１は、チケット作成部（手段）４、チケット発行部（手段）５、チケット原型データベース６および証明器固有情報データベース７を有している。図３においては、さらに、チケット仕様データベース８が設けられている。チケット作成・発行装置１の詳細（動作）については第３の実施例および第４の実施例を参照して後述する。
【００３２】
図１２において、チケット検証装置３は、検証手順実行部１１１および通信部１１２を有しており、また、チケット証明装置２は、チケット保持部１２１、チケット検索部１２２

、固有情報保持部１２３、内部状態保持部１２４、証明手順実行部１２５および通信部１２６を有している。

【００３３】

図２９はチケット証明装置２の証明手順実行部１２５の詳細な構成を示しており、また、図２８はチケット検証装置３の検証手順実行部１１１の詳細な構成を示している。図２８および図２９に示すように、本実施例では、証明装置２の証明手順実行部１２５は、送信部２９１、受信部２９２、第１の演算部２９３、第２の演算部２９４、正当性検証部２９５、認証情報生成部２９６、認証情報保持部２９７、第２の認証情報保持部２９８、情報保持部２９９、出力情報保持部２９１０、入力情報保持部２９１１、制御部２９１２とから構成されている。

【００３４】

検証装置３の検証手順実行部１１１は、送信部２８１、受信部２８２、第１の演算部２８３、第２の演算部２８４、正当性検証部２８５、認証情報生成部２８６、認証情報保持部２８７、チケット識別子保持部２８８、情報保持部２８９、出力情報保持部２８１０、入力情報保持部２８１１、出力部２８１２、入力部２８１３、利用証拠情報保持部２８１４とから構成される。

【００３５】

以下の例示において各手順実行部を構成する手段の中から必要なものを用いて証明手順・検証手順を実行するものとする。

【００３６】

［２．第１の実施例］

まず本発明の第１の実施例について説明する。

［２．１．認証手法］

チケットはチケットの特徴情報と証明器２の固有情報とからチケット発行装置によって算出される。チケットの特徴情報がＲＳＡ公開鍵暗号系における公開情報と秘密情報、つまり、ｐ，ｑを相異なる奇素数とし、

【００３７】

【数１０】

$n=pq$、$\lambda(n)=lcm(p-1, q-1)$、

（ここでｌｃｍは最小公倍数を表す）

【００３８】

【数１１】

$ED \equiv 1 \mod \lambda(n)$

が満たされるとき、（ｎ，Ｅ）を公開情報とし、Ｄを対応する秘密情報とする場合について、実現できるチケットの証明方法について詳述する。

【００３９】

チケットはチケット特徴情報Ｄと証明器固有情報d_Uとチケット付加情報Ｌより計算されるデータであり、証明器２が（Ｃ，ｎ，ｔ，Ｌ）に対して証明器固有情報d_Uを用いて$\tau(C, n, t, L)=C^D \mod n$が計算できるように構成する。

【００４０】

例えば、d_Uをある暗号系の復号鍵とし、E_Uをd_Uに対応する暗号化とし、Ｈを一方向性関数としたとき、

【００４１】

【数１２】

$t := (E_U(D), H(d_U||D||L))$

のように定めることができる。（ここで｜｜はビット列の連結である。）

チケットを（１）として定義すると、チケットを用いた秘密の特徴情報Ｄによる符号化$C^D \mod n$は、入力（Ｃ，ｎ，ｔ，Ｌ）に対して証明装置の固有情報d_Uによって$E_U(D)$を復号して証明装置中でＤを回復し、その値を用いて一方向性関数の値をチケットと比較することによってＬの値の正当性を確認し、回復されたＤの値を用いて証明装置内

でC^D ｍｏｄ ｎを計算するようにすれば良い。
【００４２】
また、d_Uを一方向性関数として、
【００４３】
【数１２】
ｔ：＝Ｄ－d_U（Ｌ、ｎ）
と定めることもできる。
【００４４】
チケットを上式として定義すると、入力（Ｃ，ｎ，ｔ，Ｌ）に対してＤによる符号化C^D ｍｏｄ ｎは、$C^tC^{dU(L,n)}$ ｍｏｄ ｎを計算することによって行なうこともできる。このチケットにおいては、Ｌの値の完全性もＤの値も証明器２の秘密計算を行なう部分ではチケットｔもしくは公開情報Ｅを入力しない限り確認できず、また、チケットｔを証明器２の秘密計算を行なう部分に入力せずに秘密情報に対応する符号化が計算できるという特徴がある。
【００４５】
証明器２の固有情報d_Uと（Ｃ，ｎ，ｔ，Ｌ）に対してC^D ｍｏｄ ｎを計算する手段の少なくとも一部は耐タンパー性を有する容器に保護することが望ましい。
【００４６】
なお、以下の証明手順の例示において図１９におけるステップ１９４以外は全てに共通する。したがって、ステップ１９４の詳細な手順（Ｐｒｏｖｅｒで示す）を重点的に説明する。
【００４７】
［２．２．簡単な対話プロトコル］
（証明器２が時計を持つ定期券型のチケット、図１３、図１９、図２０）
以下、検証器３と証明器２との対話の簡単な例をあげて説明する。以下の例では証明器２の内部情報として現在時刻を持つものとする。なお、以下では、検証手順と証明手順とをまとめて対話プロトコルと呼ぶことにする。
【００４８】
簡単な対話の例における検証器３の構成を図１２および図２８に示し、手順を図１３に従って説明する。証明器２の構成を図１２および図２９に示し、手順を図１９に従って説明する。
【００４９】
検証器３は、認証情報生成部２８６でチャレンジＣを生成して、認証情報保持部２８７に記録する（ステップ１３１）。このＣは、過去に利用した値を再び利用しないことが求められる。特にＣは乱数であることが望ましい。認証情報保持部２８７に記録されたＣと、識別子保持部２８８に保持されている検証しようとするチケットの識別子ｎとをまとめて、送信部２８１より証明器２へ送信する（ステップ１３２）。
【００５０】
証明器２は、検証器３から送信された（Ｃ，ｎ）を受信部２９２で受信して、情報保持部２９９に記録する（ステップ１９１）。チケット探索部１２２は受信したｎに対応するチケットをチケット保持部１２１から探して、チケットを持っているかを判定する（ステップ１９２）。ただし、１種類のチケットしか扱わないような本発明の適用場面では、ｎに対応するチケットを探す手順は不要になり、チケットを持っているかを判定するだけである。この場合には、ステップ１３２において検証器３から（Ｃ，ｎ）を送る必要はなくなり、Ｃだけ送れば十分である。さらにチケットを持っていることが保証されている場合には、持っているかの判定の手順（ステップ１９２）およびステップ１９７も不要になる。ステップ１９２の判定の結果として対応するチケットを持たない場合には、レスポンスＲにチケットを持たないことを意味する値（この場合は０）を設定して、情報保持部２９９に記録する（ステップ１９７）。ステップ１９２の判定の結果として対応するチケットを持つ場合には、チケットｔ、証明器２の手順$Prover_S$、チケット付加情報Ｌを制御

部２９１２内にセットする（ステップ１９３）。

【００５１】

ステップ１９３が実行されたら、ステップ１９４を実施する。この対話の例におけるステップ１９４の詳細な手順を図２０に従って説明する。内部状態保持部１２４の第２の内部状態保持部から読み出したその時の時刻ｔｉｍｅと、Ｌに記述されている有効期限とを比較して、チケットがその時点で有効であるか判定する（ステップ２０１）。この判定には、有効期限として終了時刻のみを記述している場合には、ｔｉｍｅがその終了時刻に達していれば無効であり、達していなければ有効であると判定できる。有効期限として開始時刻および終了時刻を記述している場合には、ｔｉｍｅがその開始時刻と終了時刻の間になければ無効であり、間にあれば有効であると判定できる。チケットを有効であると判定した場合には、第１の演算部２９３においてＲを、$R := C^{D} \mod n$のように計算して、情報保持部２９９に記録する（ステップ２０２）。特にＲのこの計算を、証明器２の中の第１の演算部２９３ですべて計算してもよいが、チケットｔがｔ＝Ｄ－d_U（Ｌ，ｎ）のように構成されている場合には、$C^{D} \mod n$の計算は$C^{t}C^{dU(L,n)} \mod n$のようにも計算できるので、$C^{t} \mod n$を証明器２の外で計算して、証明器２の中の第１の演算部２９３で計算した$C^{dU(L,n)} \mod n$とを証明器２の外で掛け合わせても計算できる。証明器２の計算速度が遅い場合には、このような方法も有効になる。

【００５２】

ステップ２０１においてチケットを無効であると判定した場合には、必要であるならばチケットをチケット保持部１２１から削除して（ステップ２０３）、Ｒにチケットが有効期間でなかったことを意味する値（この例では１）を設定して、情報保持部２９９に記録する（ステップ２０４）。ここまでがこの対話の例におけるステップ１９４の詳細な手順である。

【００５３】

ステップ１９４が実行されたら、ステップ１９３でセットされたｔ、$Prover_S$、Ｌを制御部２９１２から解除する（ステップ１９５）。ステップ１９５もしくはステップ１９７が実行されたら、Ｒを送信部２９１より検証器３へ送信する（ステップ１９６）。

【００５４】

検証器３は、受信部２８２において証明器２から送信されたＲを受信して、情報保持部２８９に記録する（ステップ１３３）。$R := R^{E} \mod n$を第１の演算部２８３で計算して、その計算結果が認証情報保持部２８７で記録しているＣと一致するかを、正当性検証部２８５で判定する（ステップ１３４）。一致すると判定された場合は証明器２が有効なチケットを持っていることを示すので、「有効」を意味する出力を出力部２８１２より出力する。一致しないと判定された場合は証明器２が有効なチケットを持っていることが示されなかったので、「無効」意味する出力を出力部２８１２より出力する。

【００５５】

以上が対話の簡単な例である。

【００５６】

対話手順を簡略に記述すると、以下のとおりである。

【００５７】

【表１】

検証器
公開情報: (n, E)
出力: ’有効’ もしくは ’無効’

$C :=$ **rand**
send (C, n)
receive R
$R := R^E \bmod n$
if $C = R$
  output ’有効’
else
  output ’無効’

Prover
if $time < L$
  $R := C^D \bmod n$
else
  $R := 1$

【００５８】
［２．３．第１の対話プロトコル］
（検証器３が時計を持つ定期券型のチケット、図１４、図１９、図２１）
検証器３と証明器２との種々の対話の方式を以下順次列挙して説明する。先に説明した構成の基に、検証の手順と証明の手順を変更することにより、異なる機能性を持つチケットを同一の構成によって実現できる。
【００５９】
まず、第１の対話プロトコルについて説明する。第１の対話プロトコルでは、検証器３の認証情報は単なる乱数ではなく、証明器２の証明情報生成の条件が、送信された認証情報とチケット発行時に固定された情報Ｌとの関係に依存するものである。
【００６０】
例えば、検証器３が現在時刻を表現する情報を発行する手段を持ち、時間情報を認証情報に埋め込み、Ｌを有効期限を表現する情報とすると、証明器２に時計機能を保持することなく時間制限型のチケットを実現できる。Ｌのビット長を｜｜Ｌ｜｜で表す。
【００６１】
第１の対話プロトコルの検証器３の手順を図１４に、証明器２の手順を図１９にそれぞれ従って説明する。
【００６２】
検証器３は、認証情報生成部２８６で乱数ｒを生成して（ステップ１４１）、さらに、ｒとその時の時刻ｔｉｍｅとを結合してチャレンジＣを生成して、認証情報保持部２８７に記録する（ステップ１４２）。例えば、ｒとｔｉｍｅの結合は、Ｃ：＝ｒ｜｜ｔｉｍｅのように実現すればよい。識別子保持部２８８に記録されている検証しようとするチケットの識別子ｎとＣとを合わせて、送信部２８１より証明器２へ送信する（ステップ１４３）。
【００６３】
証明器２の処理の流れはステップ１９３までは最初の対話例と同じである。証明器２は、

検証器３から送信された（Ｃ，ｎ）を受信部２９２で受信して、情報保持部２９９に記録する（ステップ１９１）。チケット探索部１２２が受信したｎに対応するチケットをチケット保持部１２１から探して、チケットを持っているかを判定する（ステップ１９２）。対応するチケットを持たない場合には、レスポンスＲに０を設定して、情報保持部２９９に記録する（ステップ１９７）。対応するチケットを持つ場合には、チケットｔ、証明器２の手順$Ｐｒｏｖｅｒ_{S}$、チケット付加情報Ｌをセットする（ステップ１９３）。

【００６４】

ステップ１９３が実行されたら、ステップ１９４を実施する。第１の対話プロトコルにおけるステップ１９４の詳細な手順を図２１に示す。Ｃからｔｉｍｅを抽出する（ステップ２１１）。この抽出には、Ｃから決められた長さの下位の桁を取り出せばよい。

【００６５】

例えば、Ｃが２進数表現されていて、ｔｉｍｅの長さを｜｜Ｌ｜｜ビットと表現するならば、ｔｉｍｅ：＝Ｃ　ｍｏｄ　$2^{||L||}$によって取り出すことができる。ステップ２１１でｔｉｍｅを取り出したら、Ｌに記述されている制限事項である有効期限と比較してチケットがその時点で有効であるかを判定する（ステップ２１２）。この判定は、最初の対話例のステップ２０１で説明した方法と同様である。ステップ２１２の結果としてチケットが有効であると判定した場合には、証明器２はＲとして、$Ｒ：＝Ｃ^{Ｄ}$　ｍｏｄ　ｎを第１の演算部２９３で計算して、情報保持部２９９に記録する（ステップ２１３）。ステップ２１２の結果としてチケットが無効であると判定した場合には、必要ならばチケット保持部１２１からチケットを削除して、Ｒにチケットが有効期間でなかったことを意味する値（この場合では１）を設定して、情報保持部２９９に記録する（ステップ２１４）。ここまでが第１の対話プロトコルにおけるステップ１９４の詳細な手順である。

【００６６】

ステップ１９４が実行されたら、ステップ１９３でセットされたｔ、$Ｐｒｏｖｅｒ_{S}$、Ｌを解除する（ステップ１９５）。ステップ１９５もしくはステップ１９７が実行されたら、送信部２９１から検証器３へＲを送信する（ステップ１９６）。

【００６７】

検証器３は、証明器２から送信されたＲを受信部２８２に受信して、情報保持部２８９に記録する（ステップ１４４）。$Ｒ：＝Ｒ^{Ｅ}$　ｍｏｄ　ｎを第１の演算部２８３で計算して、この演算結果が認証情報保持部２８７に記録されているＣと一致するかを、正当性検証部２８５で判定する（ステップ１４５）。一致する場合は証明器２が有効なチケットを持っていることが示されたので、「有効」を意味する出力を出力部２８１２から出力する。一致しない場合は証明器２が有効なチケットを持つことが示されなかったので、「無効」を意味する出力を出力部２８１２から出力する。

【００６８】

以上が第１の対話プロトコルである。証明器２が時計を持たなくても、最初の対話例と同じ機能を実現している。本プロトコルを、検証器が「有効」を出力したらゲートを開け、「無効」を出力したら、ゲートを閉ざすように適用することで、有効期限付きの通行証や定期券の機能を実現できる。

【００６９】

以上の対話手順を簡略に記述すると、以下のとおりである。

【００７０】

【表２】

検証器
公開情報: (n, E)
出力: ’有効’ もしくは ’無効’

$C := \mathbf{rand}||\mathbf{time}$
send (C, n)
receive R
$R := R^E \bmod n$
if $C = R$
  output ’有効’
else
  output ’無効’

Prover
if $C \bmod 2^{||L||} < L$
  $R := C^D \bmod n$
else
  $R := 1$

【００７１】
［２．４．第２の対話プロトコル］
（メンバーズカード型のチケット、図１５、図１９、図２２）
第２の対話プロトコルでは、証明手順において、証明器２が送信する証明情報は、認証情報にチケット発行時に関係付けられた固定的な情報Ｌを添加したものを、チケットの特徴情報に基づいて符号化したものとする。また、検証手順において、証明情報が認証情報に対応することの検証と付加的に得られる情報Ｌの導出を行なう。
【００７２】
このプロトコルでは証明器２から検証器３に対して、チケット発行時に関係付けられた定数が伝達される。
【００７３】
第２の対話プロトコルの、検証器３の手順を図１５に従って説明し、証明器２の手順を図１９に従って説明する。
【００７４】
検証器３はチャレンジＣを認証情報生成部２８６で生成して、認証情報保持部２８７に記録する（ステップ１５１）。検証しようとするチケットの識別子ｎと生成したＣを合わせて、送信部２８１より証明器２へ送信する（ステップ１５２）。
【００７５】
証明器２の処理の流れは、最初の対話例とステップ１９３まで同じである。証明器２は、検証器３から送信された（Ｃ，ｎ）を受信部２９２で受信して、情報保持部２９９に記録する（ステップ１９１）。チケット探索部１２２は受信したｎに対応するチケットをチケット保持部１２１から探して、チケットを持っているかどうかを判定する（ステップ１９２）。判定の結果として対応するチケットを持たない場合には、レスポンスＲに０を設定して、情報保持部２９９に記録する（ステップ１９７）。判定の結果として対応するチケットを持つ場合には、チケットｔ、証明器２の手順Prover_S、チケット付加情報Ｌをセットする（ステップ１９３）。

【００７６】
ステップ１９３が実行されたら、ステップ１９４を実行する。第２の対話プロトコルにおけるステップ１９４の手順の詳細な手順を図２２に従って説明する。Ｌから取り出した、検証器３に送出するメッセージＭと、Ｃとを結合して、情報保持部２９９に記録する（ステップ２２１）。ＣとＭの結合の方法は、Ｃ：＝Ｃ｜｜Ｍによって実現できる。結合したＣを使って、第１の演算部２８３においてＲ：＝C^{D} ｍｏｄ ｎを計算して、情報保持部２９９に記録する（ステップ２２２）。ここまでが、第２の対話プロトコルにおけるステップ１９４の詳細な手順である。

【００７７】
ステップ１９４が実行されたら、ステップ１９３でセットされたｔ、$Ｐｒｏｖｅｒ_{S}$、Ｌを解除する（ステップ１９５）。ステップ１９５もしくはステップ１９７が実行されたら、Ｒを送信部２９１より検証器３へ送信する（ステップ１９６）。

【００７８】
検証器３は、証明器２から送信されたＲを受信部２８２で受信して、情報保持部２８９に記録する（ステップ１５３）。Ｒ：＝R^{E} ｍｏｄ ｎを第１の演算部２８３で計算して（ステップ１５４）、この計算されたＲの上位の桁が、認証情報保持部２８７に記録されているＣと一致することを、正当性検証部２８５で判定する（ステップ１５５）。一致していればＲの下位の桁よりＭを取り出して（ステップ１５６）、出力部２８１２より出力する。一致していなければ証明器２が有効なチケットを持つことが示されなかったので、「無効」を意味する出力を出力部２８１２より出力する。

【００７９】
以上が第２の対話プロトコルである。本プロトコルによると、証明器２はチケットを持つことを証明すると同時に、改竄を検知できるようにメッセージを検証器３へ伝達できる。例えば、メッセージを会員番号として本プロトコルを適用することで、会員であることを証明すると同時に、会員番号を伝達する会員証が実現される。

【００８０】
【表３】

検証器
公開情報: (n, E)
出力: $M\ (=L)$ もしくは ’無効’

$C :=$ **rand**
send (C, n)
receive R
$R := R^{E} \bmod n$
if $R = C||M$
  output M
else
  output ’無効’

Prover
$M := L$
$R := (C||M)^{D} \bmod n$

【００８１】

［２．５．第３の対話プロトコル］
（使い捨ての回数券型のチケット、図１６、図１９、図２３）
第３の対話プロトコルでは、チケットに対して証明器２が可変な内部状態を持ち、チケット利用において検証器３が内部状態の更新を行なう。内部状態の更新を行ないうる検証器３は、それを証明する秘密の特徴情報を持つ。この特徴情報を持つ検証器３を特権を持つ検証器３と呼ぶ。
【００８２】
また、その特徴情報を持たない検証器３との対話においては、内部状態の更新を回避してチケットの有効性を検証することができる。
【００８３】
例えば、証明器２が持つ内部状態を度数情報とする。検証器３側で把握することなく、特権を持つ検証器３との対話の回数を制限する機構を実現する。
【００８４】
検証器３の特権を保証する特徴情報を（δ，ν）として、検証器３の特徴情報に対応する公開情報を（ε，ν）とする。ただし、εδ≡１　ｍｏｄ　λ（ν）である。利用するチケット補助情報Ｌには、検証器３の特徴情報の公開情報（ν，ε）と、内部状態であるカウンタの上限値ｉが含まれている。例えば、Ｌ：＝ν｜｜ε｜｜ｉのように構成しておき、それぞれの情報の長さが決めれれていれば、Ｌからそれぞれの情報を取り出すことができる。第３の対話プロトコルの検証器３の手順を図１６に従って説明し、証明器２の手順を図１９に従って説明する。
【００８５】
検証器３は、認証情報生成部２８６でチャレンジＣを生成して、認証情報保持部２８７に記録する（ステップ１６１）。検証しようとするチケットの識別子ｎと生成したＣを、まとめて送信部２８１より証明器２へ送信する（ステップ１６２）。
【００８６】
証明器２の処理の流れはステップ１９３までは最初の対話例と同じである。証明器２は、検証器３から送信された（Ｃ，ｎ）を受信部２９２で受信して、情報保持部２９９に記録する（ステップ１９１）。チケット探索部１２２は受信したｎに対応するチケットをチケット保持部１２１から探して、チケットを持っているかどうかを判定する（ステップ１９２）。対応するチケットを持たない場合には、レスポンスＲに０を設定して、情報保持部２９９に記録する（ステップ１９７）。対応するチケットを持つ場合には、チケットｔ、証明器２の手順Prover_S、チケット付加情報Ｌをセットする（ステップ１９３）。Prover_Sのセットによって、Ｌよりｉとνとεを取り出す。
【００８７】
ステップ１９３が実行されたら、ステップ１９４を実行する。第３の対話プロトコルにおけるステップ１９４の詳細な手順を図２３に示す。認証情報生成部２９６でチャレンジχを生成して、第２の認証情報保持部２９８に記録する（ステップ２３１）。χは、これまで示した最初の対話例におけるＣの生成と同じ方法で生成できる。生成したχを送信部２９１から検証器３へ送信する（ステップ２３２）。
【００８８】
検証器３は、χを受信部２８２で受信して、情報保持部２８９に記録する（ステップ１６３）。ただし、χとして０を受信した場合は、証明器２がチケットを持っていなくて、Ｒとして０を送ったことを意味するので、「無効」を意味する出力を出力部２８１２から出力して、対話プロトコルを終了する。第２の演算部２８４においてレスポンスρを、
【００８９】
【数１４】

$$\rho := \chi^{\delta} \bmod \nu$$

により計算する（ステップ１６４）。計算したρを送信部２８１より証明器２へ送信する（ステップ１６５）。

【００９０】
証明器２は、ρを受信部２９２で受信して、情報保持部２９９に記録する（ステップ２３３）。第２の演算部２９４で
【００９１】
【数１５】

$$\rho := \rho^{\varepsilon} \bmod \nu$$

を計算する。第２の認証情報保持部２９８に記録されているχとρが、一致するか判定する（ステップ２３４）。判定の結果として一致しない場合には、メッセージＭに１を設定して、情報保持部２９９に記録する（ステップ２３９）。判定の結果として一致する場合には、Ｍに０を設定して、情報保持部２９９に記録して（ステップ２３５）、内部状態保持部１２４の第２の内部状態保持部に確保されているカウンタi_nの値をインクリメントする（ステップ２３６）。ステップ２３６もしくはステップ２３９が実行されたら、i_nの値をＬより得られた上限値ｉと比較する（ステップ２３７）。ステップ２３７の比較の結果として、i_nの値がｉ以下の場合は、第１の演算部２９３でＲ：＝（Ｃ｜｜Ｍ）^{D}　ｍｏｄ　ｎを計算して、情報保持部２９９に記録する（ステップ２３８）。ステップ２３７の比較の結果として、カウンタi_nがｉよりも大きい場合は、内部状態保持部１２４よりi_nの記憶領域を開放して（ステップ２３１０）、チケット保持部１２１からｔを削除して（ステップ２３１１）、Ｒの値を１に設定して情報保持部２９９に記録する（ステップ２３１２）。ここまでが、第３の対話プロトコルにおけるステップ１９４の詳細な手順である。
【００９２】
なお、上の説明ではi_nが初期値０に設定された後は、検証に成功する度にインクリメントしてｉと大小を比較しているが、i_nの初期値をｉに設定して、検証に成功するたびにデクリメントして負の値になるか判定する方法でも同様のことが実現できる。
【００９３】
ステップ１９４が実行されたら、ステップ１９３でセットされたｔ、Prover_S、Ｌを解除する（ステップ１９５）。ステップ１９５もしくはステップ１９７が実行されたら、送信部２９１から検証器３へＲを送信する（ステップ１９６）。
【００９４】
検証器３は、証明器２から送信されたＲを受信部２８２に受信して、情報保持部２８９に記録する（ステップ１６６）。Ｒ：＝Ｒ^{E}　ｍｏｄ　ｎを第１の演算部２８３で計算する（ステップ１６７）。この計算結果の上位の桁が、認証情報保持部２８７に記録されているＣと一致するかを、正当性検証部２８５で判定する（ステップ１６８）。一致する場合は証明器２が有効なチケットを持っていることが示されたので、Ｒの下位の桁より取り出したＭを、証明器２から受け取った情報として取り出して（ステップ１６９）、出力部２８１２から出力する。一致しない場合は証明器２が有効なチケットを持つことが示されなかったので、「無効」を意味する出力を出力部２８１２から出力する。
【００９５】
以上が第３の対話プロトコルである。特権を持つ検証器３は決められた回数だけ、チケットの検証ができる。また、特権を持たない検証器３でも、レスポンスρとして適当な値を返すことで、チケットの有効性を検証できる。例えば、検証器３の出力が０の時だけサービスを提供して、それ以外の値の時に提供しないように本プロトコルを適用すると、回数券の機能を実現できる。
【００９６】
【表４】

検証器
公開情報: (n, E)
出力: $M \in \{0$(有効: 対特権検証器), 1(有効: 対一般の検証器)$\}$ もしくは '無効'
特権を保証する特徴情報: (δ, ν), ただし $\varepsilon\delta \equiv 1 \bmod \lambda(\nu)$

rand C
send (C, n)
receive χ
$\rho := \chi^{\delta} \bmod \nu$
send ρ
receive R
$R := R^{E} \bmod n$
if $R = C||M$
  output M
else
  output '無効'

Prover
$\nu||\varepsilon||i := L$
rand χ
send χ
receive ρ
$\rho := \rho^{\varepsilon} \bmod \nu$
if $\rho = \chi$
  $i_n := i_n + 1$
  $M := 0$
else
  $M := 1$
if $i_n \leq i$
  $R := (C||M)^{D} \bmod n$
else
  free i_n
  delete t
  $R := 1$

【００９７】
［２．６．第４の対話プロトコル］
（再充填可能な回数券型のチケット、図１６、図１９、図２４）
第４の対話プロトコルでは、第３の対話プロトコルにおけると同様にレスポンスの生成回数を制限する機構を実現する。本対話プロトコルでは、さらに、特権的な検証者は消費さ

れた利用回数を充当することができる。

【００９８】

このプロトコルでは検証器３から証明器２に対して、検証器３が特権的であることと検証器３の１ビットの指示（対応する内部状態に対しての２通りの更新指示の選択：度数の消費と度数の充填）が伝達される。

【００９９】

これによってチケットの発行をチケット作成・発行装置が一度行なえば、そのチケットが無効になった場合、チケット作成・発行装置による新たなチケット発行によらず、特権を持つ検証者と対話を行なうことによって有効性を回復する。

【０１００】

検証器３の特権を保証する特徴情報の（δ，ν）および公開情報の（ε，ν）、チケット補助情報Ｌは第３の対話プロトコルと同じである。第４の対話プロトコルの検証器３の手順を図１６に従って説明し、証明器２の手順を図１９に従って説明する。ただし、対話プロトコルに先立って、度数の消費を実行するのか、度数の充填を実行するのかを、検証器３の入力部２８１３より入力されて、入力情報保持部２８１１に記録されているとする。

【０１０１】

検証器３は認証情報生成部２８６でチャレンジＣを生成して、認証情報保持部２８７に記録する（ステップ１６１）。検証しようとするチケットの識別子ｎと生成したＣを、まとめて送信部２８１より証明器２へ送信する（ステップ１６２）。

【０１０２】

証明器２は、検証器３から送信された（Ｃ，ｎ）を受信部２９２で受信して、情報保持部２９９に記録する（ステップ１９１）。チケット探索部１２２は受信したｎに対応するチケットをチケット保持部１２１から探して、チケットを持っているかどうかを判定する（ステップ１９２）。対応するチケットを持たない場合には、レスポンスＲに０を設定して、情報保持部２９９に記録する（ステップ１９７）。対応するチケットを持つ場合には、チケットｔ、証明器２の手順Prover_S、チケット付加情報Ｌをセットする（ステップ１９３）。

【０１０３】

ステップ１９３が実行されたら、ステップ１９４を実行する。第４の対話プロトコルにおけるステップ１９４の詳細な手順を図２４に従って説明する。認証情報生成部２９６でチャレンジχを生成して、第２の認証情報保持部２９８に記録する（ステップ２４１）。生成したχを送信部２９１から検証器３へ送信する（ステップ２４２）。

【０１０４】

検証器３は、χを受信部２８２で受信して、情報保持部２８９に記録する（ステップ１６３）。χとして０を受信した場合は、証明器２がチケットを持っていなくて、Ｒとして０を送ったことを意味するので、「無効」を意味する出力を出力部２８１２から出力して、対話プロトコルを終了する。次に、レスポンスρを計算する（ステップ１６４）。まず、第２の演算部２８４においてレスポンスρを、

【０１０５】

【数１６】

$$\rho := \chi^{\delta} \bmod \nu$$

にように計算する。チケットの度数の充填を行いたい場合にはさらに、第２の演算部２８４において、

【０１０６】

【数１７】

$$\rho := \rho^{\delta} \bmod \nu$$

を計算する。ステップ１６４におけるρの計算は、チケットの度数の消費を行いたい場合にはμ：＝１として、チケットの度数の充填を行いたい場合にはμ：＝２として、

【０１０７】
【数１８】

$$\rho := \chi^{\delta\mu} \bmod \nu$$

を計算しても同様である。ステップ１６４で計算したρを送信部２８１より証明器２へ送信する（ステップ１６５）。
【０１０８】
証明器２は、ρを受信部２９２で受信して、情報保持部２９９に記録する（ステップ２４３）。第２の演算部２９４で
【０１０９】
【数１９】

$$\rho := \rho^{\varepsilon} \bmod \nu$$

を計算して、第２の認証情報保持部２９８に記録されているχとρが、一致するか判定する（ステップ２４４）。ステップ２４４の判定の結果が一致する場合には、Ｍに０を設定して情報保持部２９９に記録して、内部状態保持部１２４に確保されているカウンタi_nの値をインクリメントする（ステップ２４５）。ステップ２４４の判定の結果が一致しない場合には、第２の演算部２９４で
【０１１０】
【数２０】

$$\rho := \rho^{\varepsilon} \bmod \nu$$

を計算して、第２の認証情報保持部２９８に記録されているχとρが、一致するか判定する（ステップ２４８）。ステップ２４８の判定の結果が一致する場合には、Ｍに０を設定して情報保持部２９９に記録して、内部状態保持部１２４の第２の内部状態保持部に確保されているカウンタi_nの値を０に設定する（ステップ２４９）。ステップ２４８の判定の結果が一致しない場合には、メッセージＭに１を設定して、情報保持部２９９に記録する（ステップ２４１１）。ステップ２４５もしくはステップ２４９、ステップ２４１１が実行されたら、i_nの値をＬより得られた上限値ｉと比較する（ステップ２４７）。ステップ２４７の比較の結果として、i_nの値がｉ以下の場合は、第１の演算部２９３でＲ：＝（Ｃ｜｜Ｍ）^{D} ｍｏｄ ｎを計算して、情報保持部２９９に記録する（ステップ２４８）。ステップ２４７の比較の結果として、カウンタi_nがｉよりも大きい場合は、Ｒの値を１に設定して情報保持部２９９に記録する（ステップ２４１０）。ここまでが第４の対話プロトコルにおけるステップ１９４の詳細な手順である。
【０１１１】
ステップ１９４が実行されたら、ステップ１９３でセットされたｔ、Prover_S、Ｌを解除する（ステップ１９５）。ステップ１９５もしくはステップ１９７が実行されたら、送信部２９１から検証器３へＲを送信する（ステップ１９６）。
【０１１２】
検証器３は、証明器２から送信されたＲを受信部２８２に受信して、情報保持部２８９に記録する（ステップ１６６）。Ｒ：＝Ｒ^{E} ｍｏｄ ｎを第１の演算部２８３で計算する（ステップ１６７）。この計算結果の上位の桁が、認証情報保持部２８７に記録されているＣと一致するかを、正当性検証部２８５で判定する（ステップ１６８）。一致する場合は証明器２が有効なチケットを持っていることが示されたので、Ｒの下位の桁より取り出したＭを、証明器２から受け取った情報として取り出して（ステップ１６９）、出力部２８１２から出力する。一致しない場合は証明器２が有効なチケットを持つことが示されなかったので、「無効」を意味する出力を出力部２８１２から出力する。
【０１１３】
以上が第４の対話プロトコルである。第４の対話プロトコルと同様の機能を提供する変形例として、i_nの初期値をｉに設定して、ステップ２４５でインクリメントの変わりにデ

クリメントして、ステップ２４６で負の値になるか判定する方法も実現できる。この変形例では、ステップ２４９の度数の充填時にi_nをｉに設定する。さらに別の変形例として、ステップ２４９の度数の充填時にi_nにｉを加える方法もある。

【０１１４】

【表５】

検証器公開情報: (n, E)
入力: $\mu \in \{1$(回数の消費指示)$, 2$(回数の充填指示)$\}$
出力: $M \in \{0$(有効: 対特権検証器)$, 1$(有効: 対一般の検証器)$\}$ もしくは '無効'
特権保証特徴情報: (δ, ν)

$C :=$ **rand**
send (C, n)
receive χ
$\rho := \chi^{\delta^{\mu}} \bmod \nu$
send ρ
receive R
$R := R^E \bmod n$
if $R = C||M$
  output M
else
  output '無効'

Prover
$\nu||\varepsilon||i := L$
$\chi :=$ **rand**
send χ
receive ρ
$\rho := \rho^{\varepsilon} \bmod \nu$
if $\rho = \chi$
  $i_n := i_n + 1$
  $M := 0$
else
  $\rho := \rho^{\varepsilon} \bmod \nu$
  if $\rho = \chi$
    $i_n := 0$
    $M := 0$
  else
    $M := 1$
if $i_n \leq i$
  $R := (C||M)^D \bmod n$
else
  $R := 1$

【０１１５】
［２．７．第５の対話プロトコル］
（スタンプカード型チケット、図１７、図１９、図２５）
第５の対話プロトコルでは、特権を持つ検証者に対して生成したレスポンスの回数が、チケット発行時に割り付けられたある一定回数に達する都度、そのことを検証者に通知する機構を実現する。
【０１１６】
また、一般的な検証者に対してもチケットの有効性を確認することが可能である。
【０１１７】
検証器３の特権を保証する特徴情報の（δ，ν）および公開情報の（ε，ν）、チケット補助情報Ｌは第３の対話プロトコルと同じである。ただし、Ｌに含まれるｉは、達すると通知を行うべき一定回数を意味している。第５の対話プロトコルの検証器３の手順を図１７に従って説明し、証明器２の手順を図１９に従って説明する。
【０１１８】
検証器３は、認証情報生成部２８６でチャレンジＣを生成して、認証情報保持部２８７に記録する（ステップ１７１）。検証しようとするチケットの識別子ｎと生成したＣを、まとめて送信部２８１より証明器２へ送信する（ステップ１７２）。
【０１１９】
証明器２は、検証器３から送信された（Ｃ，ｎ）を受信部２９２で受信して、情報保持部２９９に記録する（ステップ１９１）。チケット探索部１２２は受信したｎに対応するチケットをチケット保持部１２１から探して、チケットを持っているかどうかを判定する（ステップ１９２）。対応するチケットを持たない場合には、レスポンスＲに０を設定して、情報保持部２９９に記録する（ステップ１９７）。対応するチケットを持つ場合には、チケットｔ、証明器２の手順Prover_S、チケット付加情報Ｌをセットする（ステップ１９３）。
【０１２０】
ステップ１９３が実行されたら、ステップ１９４を実行する。第５の対話プロトコルにおけるステップ１９４の詳細な手順を図２５に示す。認証情報生成部２９６でチャレンジχを生成して、第２の認証情報保持部２９８に記録する（ステップ２５１）。生成したχを送信部２９１から検証器３へ送信する（ステップ２５２）。
【０１２１】
検証器３は、χを受信部２８２で受信して、情報保持部２８９に記録する（ステップ１７３）。χとして０を受信した場合は、証明器２がチケットを持っていなくて、Ｒとして０を送ったことを意味するので、「無効」を意味する出力を出力部２８１２から出力して、対話プロトコルを終了する。第２の演算部２８４においてレスポンスρを、
【０１２２】
【数２１】

$$\rho := \chi^{\delta} \bmod \nu$$

にように計算する（ステップ１７４）。計算したρを送信部２８１より証明器２へ送信する（ステップ１７５）。
【０１２３】
証明器２は、ρを受信部２９２で受信して、情報保持部２９９に記録する（ステップ２５３）。第２の演算部２９４で
【０１２４】
【数２２】

$$\rho := \rho^{\varepsilon} \bmod \nu$$

を計算して、第２の認証情報保持部２９８に記録されているχとρが、一致するか判定する（ステップ２５４）。ステップ２５４の判定の結果が一致する場合には、内部状態保持

部１２４の第２の内部状態保持部に確保されているカウンタi_nの値をインクリメントする（ステップ２５５）。ステップ２５４の判定の結果が一致しない場合もしくはステップ２５５が実行されたら、内部状態保持部１２４に確保されているi_nの値とＬより得られた上限値ｉとを比較する（ステップ２５６）。ステップ２５６の比較の結果として、i_nとｉが等しくない場合は、第１の演算部２９３でＲ：＝C^D　ｍｏｄ　ｎを計算して、情報保持部２９９に記録する（ステップ２５７）。ステップ２５６の比較の結果として、i_nとｉが等しい場合は、i_nを０に設定して（ステップ２５８）、第１の演算部２９３で

【０１２５】

【数２３】

$$R := C^{D^2} \bmod n$$

を計算して、情報保持部２９９に記録する（ステップ２５１０）。ここまでが第５の対話プロトコルにおけるステップ１９４の詳細な手順である。

【０１２６】

ステップ１９４が実行されたら、ステップ１９３でセットされたｔ、$Prover_S$、Ｌを解除する（ステップ１９５）。ステップ１９５もしくはステップ１９７が実行されたら、送信部２９１から検証器３へＲを送信する（ステップ１９６）。

【０１２７】

検証器３は、証明器２から送信されたＲを受信部２８２に受信して、情報保持部２８９に記録する（ステップ１７６）。Ｒ：＝R^E　ｍｏｄ　ｎを第１の演算部２８３で計算して情報保持部２９９に記録するとともに、この計算結果が、認証情報保持部２８７に記録されているＣと一致するかを、正当性検証部２８５で判定する（ステップ１７７）。一致する場合は、０を出力部２８１２から出力する。一致しない場合は、Ｒ：＝R^E　ｍｏｄ　ｎを第１の演算部２８３でさらに計算して情報保持部２９９に記録するとともに、この計算結果が、認証情報保持部２８７に記録されているＣと一致するかを、正当性検証部２８５で判定する（ステップ１７８）。ステップ１７８の結果が一致する場合は、証明器２のチケットが規定の度数に達したことを示すので、１を出力部２８１２から出力する。ステップ１７８の結果が一致しない場合は、「無効」を意味する出力を出力部２８１２から出力する。

【０１２８】

以上が第５の対話プロトコルである。一定回数の利用があった場合に景品を授与するためのポイント・カードとして、本プロトコルを適用できる。

【０１２９】

【表６】

検証器
公開情報: (n, E)
出力: $M \in \{1(\text{有効}), 2(\text{レスポンス生成が一定の回数 } i \text{ に達した})\}$ **もしくは '無効'**
特権保証特徴情報: (δ, ν)

$C := \mathbf{rand}$
send (C, n)
receive χ
$\rho := \chi^{\delta} \bmod \nu$
send ρ
receive R
$R := R^{E} \bmod n$
if $C = R$
  output 1
else
  $R := R^{E} \bmod n$
  if $C = R$
    output 2
  else
    output '無効'

Prover
$\nu \| \varepsilon \| i := L$
$\chi := \mathbf{rand}$
send χ
receive ρ
$\rho := \rho^{\varepsilon} \bmod \nu$
if $\rho = \chi$
  $i_n := i_n + 1$
else
if $i_n = i$
  $R := C^{D^2} \bmod n$
  $i_n := 0$
else
  $R := C^{D} \bmod n$

【０１３０】
［２．８．第６の対話プロトコル］
（使い捨てのプリペイドカード型チケット、図１８、図１９、図２６）
この発明における第６の対話プロトコルでは、特権を持つ検証者に対しては、チケットに関係付けられた記憶領域中に保持される値を指定値だけ減少することができる。また、内部状態の更新がチケット発行時に定められた限界を越えるとそれを検証器３に通知する。
【０１３１】
一般的な検証者に対してもチケットの有効性の検証と記憶領域中に保持された値を伝達することができる。

【０１３２】
この対話プロトコルでは、検証器３から可変な指示情報が伝達され、証明器２からもチケットに対応する可変な状態情報が伝達される。
【０１３３】
検証器３の特権を保証する特徴情報の（δ，ν）および公開情報の（ε，ν）、チケット補助情報Ｌは第３の対話プロトコルと同じである。ただし、Ｌには特にｉは含む必要がない。第６の対話プロトコルの検証器３の手順を図１８に、証明器２の手順を図１９にそれぞれ従って説明する。
【０１３４】
検証器３は、認証情報生成部２８６でチャレンジＣを生成して、認証情報保持部２８７に記録する（ステップ１８１）。検証しようとするチケットの識別子ｎと生成したＣを、まとめて送信部２８１より証明器２へ送信する（ステップ１８２）。
【０１３５】
証明器２は、検証器３から送信された（Ｃ，ｎ）を受信部２９２で受信して、情報保持部２９９に記録する（ステップ１９１）。チケット探索部１２２は受信したｎに対応するチケットをチケット保持部１２１から探して、チケットを持っているかどうかを判定する（ステップ１９２）。対応するチケットを持たない場合には、レスポンスＲに０を設定して、情報保持部２９９に記録する（ステップ１９７）。対応するチケットを持つ場合には、チケットｔ、証明器２の手順Prover_S、チケット付加情報Ｌをセットする（ステップ１９３）。
【０１３６】
ステップ１９３が実行されたら、ステップ１９４を実行する。第６の対話プロトコルにおけるステップ１９４の詳細な手順を図２６に従って説明する。認証情報生成部２９６でチャレンジχを生成して、第２の認証情報保持部２９８に記録する（ステップ２６１）。生成したχを送信部２９１から検証器３へ送信する（ステップ２６２）。
【０１３７】
検証器３は、χを受信部２８２で受信して、情報保持部２８９に記録する（ステップ１８３）。χとして０を受信した場合は、証明器２がチケットを持っていなくて、Ｒとして０を送ったことを意味するので、「無効」を意味する出力を出力部２８１２から出力して、対話プロトコルを終了する。入力部２８１３より入力されて入力情報保持部２８１１に予め記録されていたメッセージμを使って、第２の演算部２８４において
【０１３８】
【数２４】

$$\rho := (\chi \,||\, \mu)^{\delta} \bmod \nu$$

を計算する（ステップ１８４）。計算したレスポンスρを送信部２８１より証明器２へ送信する（ステップ１８５）。
【０１３９】
証明器２は、ρを受信部２９２で受信して、情報保持部２９９に記録する（ステップ２６３）。第２の演算部２９４で
【０１４０】
【数２５】

$$\rho := \rho^{\varepsilon} \bmod \nu$$

を計算して、情報保持部２９９に記録する（ステップ２６４）。第２の認証情報保持部２９８に記録されているχと計算したρの上位の桁とが、一致するか判定する（ステップ２６５）。ステップ２６５の判定の結果が一致しない場合には、内部状態保持部１２４の内部状態保持部に確保されているカウンタi_nの値を利用して、メッセージとしてＭ：＝１||i_nを設定して、情報保持部２９９に記録する（ステップ２６１３）。ステップ２６５の判定の結果が一致する場合には、ρの下位の桁からμを取り出して、i_nの値をi_n：

＝i_n－μのように減算する（ステップ２６５）。Ｍ：＝０｜｜i_nを設定して、情報保持部２９９に記録する（ステップ２６７）。i_nが０より小さいか判定する（ステップ２６８）。０より小さい場合には、内部状態保持部１２４からi_nを解放して（ステップ２６１１）、チケット保持部１２１からｔを削除する（ステップ２６１２）。いずれの場合でも、第１の演算部２９３でＲ：＝（Ｃ｜｜Ｍ）^{D} ｍｏｄ ｎを計算して、情報保持部２９９に記録する（ステップ２６９）。ここまでが第６の対話プロトコルにおけるステップ１９４の詳細な手順である。

【０１４１】

ステップ１９４が実行されたら、ステップ１９３でセットされたｔ、$Prover_S$、Ｌを解除する（ステップ１９５）。ステップ１９５もしくはステップ１９７が実行されたら、送信部２９１から検証器３へＲを送信する（ステップ１９６）。

【０１４２】

検証器３は、証明器２から送信されたＲを受信部２８２に受信して、情報保持部２８９に記録する（ステップ１８６）。Ｒ：＝R^E ｍｏｄ ｎを第１の演算部２８３で計算して情報保持部２９９に記録する（ステップ１８７）。この計算結果の上位の桁が、認証情報保持部２８７に記録されているＣと一致するかを、正当性検証部２８５で判定する（ステップ１８８）。一致する場合は、Ｒの下位の桁からＭを取り出して（ステップ１８９）、出力部２８１２から出力する。一致しない場合は、「無効」を意味する出力を出力部２８１２から出力する。

【０１４３】

以上が第６の対話プロトコルである。検証器３の出力が「無効」以外の値の時は、出力の最上位のビットによってカウンタの減算の実行の有無を確認できて、その下の桁でカウンタi_nの値を確認できる。特権のない検証器３でも、レスポンスρに適当な値（例えば１）を送ることで、カウンタの値を変更せずに、カウンタの値を調べられる。例えば、チケットを初期化する時にカウンタi_nを決められた値に設定して、サービスを利用する度に、対価をカウンタから減算するように本プロトコルを適用することで、プリペイドカードの機能を提供できる。

【０１４４】

【表７】

検証器
公開情報: (n, E)
入力: μ **(減少度数)**
出力: M **もしくは** '**無効**'
特権保証特徴情報: (δ, ν)

$C :=$ **rand**
send (C, n)
receive χ
$\rho := (\chi||\mu)^{\delta} \bmod \nu$
send ρ
receive R
$R := R^{E} \bmod n$
if $R = C||M$
  output M
else
  output '**無効**'

Prover
$\chi :=$ **rand**
send χ
receive ρ
$\rho := \rho^{\varepsilon} \bmod \nu$
if $\rho = \chi||\mu$
  $i_n := i_n - \mu$
  $M := 0||i_n$
  if $i_n < 0$
    free i_n
    delete t
else
  $M := 1||i_n$
$R := (C||M)^{D} \bmod n$

【０１４５】
［２．９．第７の対話プロトコル］
（再充填可能なプリペイドカード型のチケット、図１８、図１９、図２７）
この発明における第７の対話プロトコルは、第６の対話プロトコルの変形であって、特権を持つ検証者に対しては、チケットに関係付けられた記憶領域中に保持された値を指定して増減することができる。
【０１４６】
第６の対話プロトコルと同様に、一般的な検証者に対してもチケットの有効性と対応する内部状態を検証することができる。
【０１４７】

この対話プロトコルでは、検証器３から可変な指示情報が伝達され、証明器２からもチケットに対応する可変な状態情報が伝達される。

【０１４８】

検証器３の特権を保証する特徴情報の（δ，ν）および公開情報の（ε，ν）、チケット補助情報Ｌは第６の対話プロトコルと同じである。第７の対話プロトコルの検証器３の手順を図１８に、証明器２の手順を図１９にそれぞれ従って説明する。

【０１４９】

検証器３は、認証情報生成部２８６でチャレンジＣを生成して、認証情報保持部２８７に記録する（ステップ１８１）。検証しようとするチケットの識別子ｎと生成したＣを、まとめて送信部２８１より証明器２へ送信する（ステップ１８２）。

【０１５０】

証明器２は、検証器３から送信された（Ｃ，ｎ）を受信部２９２で受信して、情報保持部２９９に記録する（ステップ１９１）。チケット探索部１２２は受信したｎに対応するチケットをチケット保持部１２１から探して、チケットを持っているかどうかを判定する（ステップ１９２）。対応するチケットを持たない場合には、レスポンスＲに０を設定して、情報保持部２９９に記録する（ステップ１９７）。対応するチケットを持つ場合には、チケットｔ、証明器２の手順Prover_S、チケット付加情報Ｌをセットする（ステップ１９３）。

【０１５１】

ステップ１９３が実行されたら、ステップ１９４を実行する。第７の対話プロトコルにおけるステップ１９４の詳細な手順を図２７に従って説明する。認証情報生成部２９６でチャレンジχを生成して、第２の認証情報保持部２９８に記録する（ステップ２７１）。生成したχを送信部２９１から検証器３へ送信する（ステップ２７２）。

【０１５２】

検証器３は、χを受信部２８２で受信して、情報保持部２８９に記録する（ステップ１８３）。χとして０を受信した場合は、証明器２がチケットを持っていなくて、Ｒとして０を送ったことを意味するので、「無効」を意味する出力を出力部２８１２から出力して、対話プロトコルを終了する。入力部２８１３より入力されて入力情報保持部２８１１に予め記録されていたメッセージμを使って、第２の演算部２８４において

【０１５３】

【数２６】

$$\rho := (\chi \,||\, \mu)^{\delta} \bmod \nu$$

を計算する（ステップ１８４）。計算したレスポンスρを送信部２８１より証明器２へ送信する（ステップ１８５）。

【０１５４】

証明器２は、ρを受信部２９２で受信して、情報保持部２９９に記録する（ステップ２７３）。第２の演算部２９４で

【０１５５】

【数２７】

$$\rho := \rho^{\varepsilon} \bmod \nu$$

を計算して、情報保持部２９９に記録する（ステップ２７４）。第２の認証情報保持部２９８に記録されているχと計算したρの上位の桁とが、一致するか判定する（ステップ２７５）。ステップ２７５の判定の結果が一致しない場合には、内部状態保持部１２４の第２の内部状態保持部に確保されているカウンタi_nの値を利用して、メッセージとしてＭ：＝１｜｜i_nを設定して、情報保持部２９９に記録する（ステップ２７１２）。ステップ２７５の判定の結果が一致する場合には、ρの下位の桁からμを取り出して、i_nの値を$i_n := i_n - \mu$のように減算する（ステップ２７５）。Ｍ：＝０｜｜i_nを設定して、情報保持部２９９に記録する（ステップ２７７）。i_nが０より小さいか判定する（ステ

ップ２７８）。０より小さい場合には、i_nを０に設定する（ステップ２７１１）。いずれの場合でも、第１の演算部２９３でＲ：＝（Ｃ｜｜Ｍ）^{D} ｍｏｄ ｎを計算して、情報保持部２９９に記録する（ステップ２７９）。ここまでが第７の対話プロトコルにおけるステップ１９４の詳細な手順である。

【０１５６】

ステップ１９４が実行されたら、ステップ１９３でセットされたｔ、$Ｐｒｏｖｅｒ_S$、Ｌを解除する（ステップ１９５）。ステップ１９５もしくはステップ１９７が実行されたら、送信部２９１から検証器３へＲを送信する（ステップ１９６）。

【０１５７】

検証器３は、証明器２から送信されたＲを受信部２８２に受信して、情報保持部２８９に記録する（ステップ１８６）。Ｒ：＝$Ｒ^E$ ｍｏｄ ｎを第１の演算部２８３で計算して情報保持部２９９に記録する（ステップ１８７）。この計算結果の上位の桁が、認証情報保持部２８７に記録されているＣと一致するかを、正当性検証部２８５で判定する（ステップ１８８）。一致する場合は、Ｒの下位の桁からＭを取り出して（ステップ１８９）、出力部２８１２から出力する。一致しない場合は、「無効」を意味する出力を出力部２８１２から出力する。

【０１５８】

以上が第７の対話プロトコルである。

【０１５９】

【表８】

検証器
公開情報: (n, E)
入力: μ
出力: M もしくは ' 無効'
特権保証特徴情報: (δ, ν)

$C :=$ **rand**
send (C, n)
receive χ
$\rho := (\chi||\mu)^{\delta} \bmod \nu$
send ρ
receive R
$R := R^{E} \bmod n$
if $R = C||M$
  output M
else
  output ' 無効'

Prover
$\nu||\varepsilon := L$
$\chi :=$ **rand**
send χ
receive ρ
$\rho := \rho^{\varepsilon} \bmod \nu$
if $\rho = \chi||\mu$
  $i_n := i_n - \mu$
  $M := 0||i_n$
  if $i_n < 0$
    $i_n := 0$
else
  $M := 1||i_n$
$R := (C||M)^{D} \bmod n$

【０１６０】
［２．１０．第８の対話プロトコル］
（回数券型チケット－無効化・払い戻し処理、図１６、図１９、図２４）
この発明における第８の対話プロトコルでは、チケットに対して有効か無効かを表すフラグが証明器２の内部状態として対応し、特権のある検証者がチケットを無効化することが可能である。
【０１６１】
検証器３の特権を保証する特徴情報の（δ，ν）および公開情報の（ε，ν）、チケット補助情報Ｌは第３の対話プロトコルと同じである。第８の対話プロトコルの検証器３の手順を図１６に、証明器２の手順を図１９にそれぞれ従って説明する。ただし、対話プロト

コルに先立って、検証を実行するのか、チケットの無効化を実行するのかを、検証器３の入力部２８１３より入力されて、入力情報保持部２８１１に記録されているとする。

【０１６２】

検証器３は、認証情報生成部２８６でチャレンジＣを生成して、認証情報保持部２８７に記録する（ステップ１６１）。検証しようとするチケットの識別子ｎと生成したＣを、まとめて送信部２８１より証明器２へ送信する（ステップ１６２）。

【０１６３】

証明器２は、検証器３から送信された（Ｃ，ｎ）を受信部２９２で受信して、情報保持部２９９に記録する（ステップ１９１）。チケット探索部１２２は受信したｎに対応するチケットをチケット保持部１２１から探して、チケットを持っているかどうかを判定する（ステップ１９２）。対応するチケットを持たない場合には、レスポンスＲに０を設定して、情報保持部２９９に記録する（ステップ１９７）。対応するチケットを持つ場合には、チケットｔ、証明器２の手順Prover_S、チケット付加情報Ｌをセットする（ステップ１９３）。

【０１６４】

ステップ１９３が実行されたら、ステップ１９４を実行する。第８の対話プロトコルにおけるステップ１９４の詳細な手順を図２４に従って説明する。認証情報生成部２９６でチャレンジχを生成して、第２の認証情報保持部２９８に記録する（ステップ２４１）。生成したχを送信部２９１から検証器３へ送信する（ステップ２４２）。

【０１６５】

検証器３は、χを受信部２８２で受信して、情報保持部２８９に記録する（ステップ１６３）。χとして０を受信した場合は、証明器２がチケットを持っていなくて、Ｒとして０を送ったことを意味するので、「無効」を意味する出力を出力部２８１２から出力して、対話プロトコルを終了する。あらかじめ、通常の検証を行う場合にはμ：＝１として、チケットを無効化する場合にはμ：＝２として、μの値を入力部２８１３より与えて入力情報保持部２８１１に記録しておき、第２の演算部２８４において、

【０１６６】

【数２８】

$$\rho := \chi^{\delta\mu} \bmod \nu$$

としてレスポンスρを計算する（ステップ１６４）。計算したρを送信部２８１より証明器２へ送信する（ステップ１６５）。

【０１６７】

証明器２は、ρを受信部２９２で受信して、情報保持部２９９に記録する（ステップ２４３）。第２の演算部２９４で

【０１６８】

【数２９】

$$\rho := \rho^{\varepsilon} \bmod \nu$$

を計算して、第２の認証情報保持部２９８に記録されているχとρが、一致するか判定する（ステップ２４４）。ステップ２４４の判定の結果が一致する場合にはステップ２４５の代わりに、Ｍに０を設定して情報保持部２９９に記録する。ステップ２４４の判定の結果が一致しない場合には、第２の演算部２９４で

【０１６９】

【数３０】

$$\rho := \rho^{\varepsilon} \bmod \nu$$

を計算して、第２の認証情報保持部２９８に記録されているχとρが、一致するか判定する（ステップ２４８）。ステップ２４８の判定の結果が一致する場合にはステップ２４９の代わりに、内部状態保持部１２４の第２の内部状態保持部に確保されているカウンタｉ

$_n$の値を０以外の値（例えば１）に設定する。ステップ２４８の判定の結果が一致しない場合には、メッセージＭに１を設定して、情報保持部２９９に記録する（ステップ２４１１）。いずれの場合においても次にステップ２４７の代わりに、i_nの値が０であるか確認する。i_nの値が０の場合は、第１の演算部２９３で$R:=(C||M)^D \bmod n$を計算して、情報保持部２９９に記録する（ステップ２４８）。i_nが０でない場合は、Ｒの値を１に設定して情報保持部２９９に記録する（ステップ２４１０）。ここまでが第８の対話プロトコルにおけるステップ１９４の詳細な手順である。

【０１７０】

ステップ１９４が実行されたら、ステップ１９３でセットされたｔ、$Prover_S$、Ｌを解除する（ステップ１９５）。ステップ１９５もしくはステップ１９７が実行されたら、送信部２９１から検証器３へＲを送信する（ステップ１９６）。

【０１７１】

検証器３は、証明器２から送信されたＲを受信部２８２に受信して、情報保持部２８９に記録する（ステップ１６６）。$R:=R^E \bmod n$を第１の演算部２８３で計算する（ステップ１６７）。この計算結果の上位の桁が、認証情報保持部２８７に記録されているＣと一致するかを、正当性検証部２８５で判定する（ステップ１６８）。一致する場合は証明器２が有効なチケットを持っていることが示されたので、Ｒの下位の桁より取り出したＭを、証明器２から受け取った情報として取り出して（ステップ１６９）、出力部２８１２から出力する。一致しない場合は、現対話で無効にした場合も含めて、証明器２が有効なチケットを持つことが示されなかったので、「無効」を意味する出力を出力部２８１２から出力する。

【０１７２】

以上が第８の対話プロトコルである。カウンタi_nの値が１に設定されると、Ｄを利用したレスポンスを送信できなくなるので、チケットの無効化となる。一度利用したら無効になるチケットや、チケットの払い戻しなどでチケットを無効にする必要がある場合に、本プロトコルが適用できる。

【０１７３】

【表９】

検証器
公開情報: (n, E)
入力: μ **(1: 通常, 2: チケットの無効化)**
出力: M **もしくは '無効'**
特権保証特徴情報: (ν, δ)
$C :=$ **rand**
send (C, n)
receive χ
$\rho := \chi^{\delta^{\mu}} \bmod \nu$
send ρ
receive R
$R := R^{E} \bmod n$
if $R = C||M$
  output M
else
  output '無効'

Prover
$\nu||\varepsilon := L$
$\chi :=$ **rand**
send χ
receive ρ
$\rho := \rho^{\varepsilon} \bmod \nu$
if $\rho = \chi$
  $M := 0$
else
  $\rho := \rho^{\varepsilon} \bmod \nu$
  if $\rho = \chi$
    $i_n := 1$
  else
    $M := 1$
if $i_n = 0$
  $R := (C||M)^{D} \bmod n$
else
  $R := 1$
  free i_n

【０１７４】
［２．１１．第９の対話プロトコル］
（チケット利用の証拠の生成、図１８）
この発明における第９の対話プロトコルでは、特権を有する検証者は、証明器２に対して行なった検証の証拠を残すことができる。

【０１７５】
本対話プロトコルでは検証器３の認証情報生成部がｒを保持し、また一方向性関数Ｈを施すことによってチャレンジＣを生成することと、（ｒ，Ｒ）を利用証拠情報保持部に蓄積することが特徴であり、証明気側の手順には依存しない。したがって、すでに述べた第１ないし第８のプロトコル全てに適用できる。
【０１７６】
検証器３の特権を保証する特徴情報の（δ，ν）は、第６の対話プロトコルと同じである。第９の対話プロトコルを、図１８の検証器３の手順に適用した例を示す。ただし、対話プロトコルに先立って、検証器３から証明器２へ伝えるメッセージμが、検証器３の入力部２８１３より入力されて、入力情報保持部２８１１に記録されているとする。
【０１７７】
認証情報生成部２８６において、乱数ｒを生成し、それをＣ：＝Ｈ（ｒ）のように一方向性関数に通してチャレンジＣを生成し、認証情報保持部２８７に記録する（ステップ１８１）。検証しようとするチケットの識別子ｎと生成したＣを、まとめて送信部２８１より証明器２へ送信する（ステップ１８２）。
【０１７８】
証明器２から送られてきたχを、受信部２８２で受信して、情報保持部２８９に記録する（ステップ１８３）。χとして０を受信した場合は、証明器２がチケットを持っていなくて、Ｒとして０を送ったことを意味するので、「無効」を意味する出力を出力部２８１２から出力して、対話プロトコルを終了する。第２の演算部２８４においてレスポンスρを、
【０１７９】
【数３１】

$$\rho := (\chi \,||\, \mu)^{\delta} \bmod \nu$$

にように計算する（ステップ１８４）。計算したρを送信部２８１より証明器２へ送信する（ステップ１８５）。
【０１８０】
証明器２から送信されたレスポンスＲを受信部２８２に受信して、情報保持部２８９に記録する（ステップ１８６）。R^{E} ｍｏｄ ｎを第１の演算部２８３で計算する（ステップ１８７）。この計算結果の上位の桁が、認証情報保持部２８７に記録されているＣと一致するかを、正当性検証部２８５で判定する（ステップ１８８）。ステップ１８８で一致した場合は、ステップ１８１で生成した乱数ｒと、ステップ１８６で情報保持部２８９に記録したＲとを組にして、利用証拠情報保持部２８１４に記録する。さらに、Ｒの下位の桁より取り出したＭを、証明器２から受け取った情報として取り出して（ステップ１８９）、出力部２８１２から出力する。ステップ１８８で一致しなかった場合は、「無効」を意味する出力を出力部２８１２から出力する。
【０１８１】
以上が第９の対話プロトコルを、図１８の検証器３の手順に適用した例である。
【０１８２】
商品券や宝くじのように、利用者と代理人（加盟店）がチケットの対価交換を済ませ、代理人がチケットの管理者に対価交換済みのチケットを送付ないしは報告するという形態のチケットの実現を想定する。チケット検証がチケットの譲渡に相当するので、その証拠を残すことができれば、代理人とチケットの管理者との間に強い信頼関係を仮定せずにチケットの譲渡が実現できる。
【０１８３】
利用証拠情報保持部２８１４に記録される情報は，本実施例のように，検証器３と証明器２のあいだで通信された情報であってもよいし，それらの情報の一部であってもよい。まら，その情報に一方向性ハッシュ関数などの所定の演算を施したもの，あるいは上記のものの組み合わせであってもよい。

【０１８４】
【表１０】

公開情報: (n, E)
検証器を特権化する情報: (ν, δ)
入力: μ
出力: M または **invalid**

検証器
$r :=$ **rand**
$C := H(r)$
send (C, n)
receive χ
$\rho := (\chi || \mu)^{\delta} \bmod \nu$
send ρ
receive R
if $R^E \bmod n = C || M$
  output M
  store (r, R)
else
  output invalid

【０１８５】
［２．１２．第１０の対話プロトコル］
（センター管理型のプリペイドカード型チケット、図１８、図１９、図２７）
この発明における第１０の対話プロトコルでは、証明器２はセンターが操作可能な度数保持手段を持ち、第９の検証プロトコルにおける、特権を有する検証者とのチケット検証に伴い度数を減じ、減じた度数情報の証拠が検証器３に保持される。
【０１８６】
検証器３の検証手順は第９のプロトコルと同じである。以下は証明器２のプロトコルを説明する。
【０１８７】
検証器３の特権を保証する特徴情報の（δ，ν）および公開情報の（ε，ν）、チケット補助情報Ｌは第６の対話プロトコルと同じである。第１０の対話プロトコルの検証器３の手順は第９の対話プロトコルと同じである。検証器３の手順を図１８に、証明器２の手順を図１９にそれぞれ従って説明する。
【０１８８】
認証情報生成部２８６において、乱数ｒを生成しそれを一方向性関数に通してチャレンジＣを生成し、認証情報保持部２８７に記録する（ステップ１８１）。検証しようとするチケットの識別子ｎと生成したＣを、まとめて送信部２８１より証明器２へ送信する（ステップ１８２）。
【０１８９】
証明器２は、検証器３から送信された（Ｃ，ｎ）を受信部２９２で受信して、情報保持部２９９に記録する（ステップ１９１）。チケット探索部１２２は受信したｎに対応するチケットをチケット保持部１２１から探して、チケットを持っているかどうかを判定する（ステップ１９２）。対応するチケットを持たない場合には、レスポンスＲに０を設定して

、情報保持部２９９に記録する（ステップ１９７）。対応するチケットを持つ場合には、チケットｔ、証明器２の手順$Prover_S$、チケット付加情報Ｌをセットする（ステップ１９３）。

【０１９０】

ステップ１９３が実行されたら、ステップ１９４を実行する。第１０の対話プロトコルにおけるステップ１９４の詳細な手順は図２７の変形である。認証情報生成部２９６でチャレンジχを生成して、第２の認証情報保持部２９８に記録する（ステップ２７１）。生成したχを送信部２９１から検証器３へ送信する（ステップ２７２）。

【０１９１】

検証器３は、χを受信部２８２で受信して、情報保持部２８９に記録する（ステップ１８３）。χとして０を受信した場合は、証明器２がチケットを持っていなくて、Ｒとして０を送ったことを意味するので、「無効」を意味する出力を出力部２８１２から出力して、対話プロトコルを終了する。入力部２８１３より入力されて入力情報保持部２８１１に予め記録されていたメッセージμを使って、第２の演算部２８４において

【０１９２】

【数３２】

$$\rho := (\chi \| \mu)^{\delta} \bmod \nu$$

を計算する（ステップ１８４）。計算したレスポンスρを送信部２８１より証明器２へ送信する（ステップ１８５）。

【０１９３】

証明器２は、ρを受信部２９２で受信して、情報保持部２９９に記録する（ステップ２７３）。第２の演算部２９４で

【０１９４】

【数３３】

$$\rho := \rho^{\varepsilon} \bmod \nu$$

を計算して、情報保持部２９９に記録する（ステップ２７４）。第２の認証情報保持部２９８に記録されているχと計算したρの上位の桁とが、一致するか判定する（ステップ２７５）。ステップ２７５の判定の結果が一致しない場合には、メッセージとしてＭ：＝１｜｜i_nを設定して、情報保持部２９９に記録する（ステップ２７１２）。ステップ２７５の判定の結果が一致する場合には、ステップ２７６とステップ２７７の代わりに、ρの下位の桁からμを取り出して、入力情報保持部２９１１に記録して、Ｍに０を設定して、情報保持部２９９に記録する。ステップ２７８の代わりとして、内部状態保持部１２４の第１の内部状態保持部に記録されているｊが、取り出したμ以上であるか判定する。ｊがμ以上である場合には、ステップ２７１１の代わりに、ｊ：＝ｊ－μとしてｊの値を変更して、Ｍ：＝Ｍ｜｜μとしてＭの値を変更する。ｊがμより小さい場合には、ｊの値を０に変更して、Ｍ：＝Ｍ｜｜ｊとしてＭの値を変更する。いずれの場合でも、第１の演算部２９３でＲ：＝（Ｃ｜｜Ｍ）^{D} ｍｏｄ ｎを計算して、情報保持部２９９に記録する（ステップ２７１０）。ここまでが第１０の対話プロトコルにおけるステップ１９４の詳細な手順である。

【０１９５】

ステップ１９４が実行されたら、ステップ１９３でセットされたｔ、$Prover_S$、Ｌを解除する（ステップ１９５）。ステップ１９５もしくはステップ１９７が実行されたら、送信部２９１から検証器３へＲを送信する（ステップ１９６）。

【０１９６】

検証器３は、証明器２から送信されたレスポンスＲを受信部２８２に受信して、情報保持部２８９に記録する（ステップ１８６）。R^{E} ｍｏｄ ｎを第１の演算部２８３で計算する（ステップ１８７）。この計算結果の上位の桁が、認証情報保持部２８７に記録されているＣと一致するかを、正当性検証部２８５で判定する（ステップ１８８）。ステップ

１８８で一致した場合は、ステップ１８１で生成した乱数ｒと、ステップ１８６で情報保持部２８９に記録したＲとを組にして、利用証拠情報保持部２８１４に記録する。さらに、Ｒの下位の桁より取り出したＭを、証明器２から受け取った情報として取り出して（ステップ１８９）、出力部２８１２から出力する。ステップ１８８で一致しなかった場合は、「無効」を意味する出力を出力部２８１２から出力する。

【０１９７】

以上が第１０の対話プロトコルである。第７の対話プロトコルでは、チケット毎に独立のカウンタi_nからメッセージμの値だけ減算していた。本プロトコルは、チケットとは独立の内部状態を減算しているところが異なる。第７のプロトコルは、チケット一つが独立のプリペイドカードに適用できるのに対して、本プロトコルは、共通のプリペイドカードによって、複数のチケットから構成されるサービスを提供できる。例えば、施設内で飲食と娯楽は別のチケットの団体が提供して、利用するときにはそれぞれ別のチケットを必要とするが、それぞれの利用に応じて、あらかじめ購入した一つのプリペイドカードから対価を減じることができる。

【０１９８】

【表１１】

Prover
$f||\nu||\varepsilon := L$
if f
  $\chi :=$ **rand**
  send χ
  receive ρ
  if $\rho^{\varepsilon} \bmod \nu = \chi||\mu$
    $M := 0$
    if $\mu \leq j$
      $j := j - \mu$
      $M := M||\mu$
    else
      $M := M||j$
      $j := 0$
  else
    $M := 1||j$
$R := (C||M)^{D} \bmod n$

【０１９９】

［２．１３．第１１の対話プロトコル］

（複数の対話プロトコルを実装）

この発明における第１１の対話プロトコルでは、証明器２は予め決められた複数の証明手順を行なえる。証明器２には複数の証明手順を実行可能な証明手順実行部があり、予め決められた証明手順のいずれかを選択して実行する。手順の選択はチケット付加情報Ｌの一部を用いて行なえる。

【０２００】

［２．１４．第１２の対話プロトコル］

（チケット付加情報を用いた証明手順の付与、図１９、図３１）

この発明における第１２の対話プロトコルでは、証明器２に証明手順を与えることができる。

【０２０１】

証明器２に制御手段があり、Ｌに証明手順の一部を与えることによって証明手順を与えることができる。

【０２０２】

証明手順の与えかたは、手順を記述する記述言語を利用して完全に自由な記述を許す方法も可能である。しかし、ある程度の汎用性のある固定の手順を用意しておき、その各ブロックの手順を記述言語でＬに記述してもよい。後者の方法は、比較的小さい情報量で表現できる利点を持っている。

【０２０３】

第１２の対話プロトコルの証明器２の手順を図１９および図３１に従って説明する。Ｌの中に、検証器３の検証の実行の有無ｆ、検証器３の検証に必要な公開情報（ν，ε）、証明手順の命令群$P_?$が含まれている。また、命令群$P_?$には、何もしないという命令も記述できるとする。例えば、Ｌが（ｆ，ν，ε，P_0，P_1，P_2，P_3，P_4，P_5）のように構成されているとする。

【０２０４】

受信部２９２で検証器３から（Ｃ，ｎ）を受信して（ステップ１９１）、情報保持部２９９に記録する。チケット探索部１２２は受信したｎに対応するチケットをチケット保持部１２１から探して、チケットを持っているかどうかを判定する（ステップ１９２）。対応するチケットを持たない場合には、レスポンスＲに０を設定して、情報保持部２９９に記録する（ステップ１９７）。対応するチケットを持つ場合には、チケットｔ、証明器２の手順$Prover_S$、チケット付加情報Ｌをセットする（ステップ１９３）。第１２の対話プロトコルでは、$Prover_S$のセットにおいて、Ｌから（ｆ，ν，ε，P_0，P_1，P_2，P_3，P_4，P_5）を取り出して記録する。

【０２０５】

ステップ１９３が実行されたら、ステップ１９４を実行する。第１の対話プロトコルにおけるステップ１９４の詳細な手順を図３１に示す。ｆが真であるか判定する（ステップ３１０１）。ｆが正しければ、ステップ３１０２からステップ３１０９までを実行する。

【０２０６】

認証情報生成部２９６で乱数χを生成して、第２の認証情報保持部２９８に記録する（ステップ３１０２）。送信部２９１より検証部２へχを送信する（ステップ３１０３）。検証部２から送信されたρを受信部２９２で受信して、情報保持部２９９に記録する（ステップ３１０４）。

【０２０７】

【数３４】

$$\rho^{\varepsilon} \bmod \nu$$

を計算して上位の桁が、χと等しいか比較する（ステップ３１０５）。ステップ３１０５の結果が等しい場合には、ステップ３１０６とステップ３１０７を実行する。Ｍに０を設定して情報記録部２９９に記録する（ステップ３１０６）。P_0の命令もしくは命令群を実行する（ステップ３１０７）。ステップ３１０５の結果が等しくない場合には、ステップ３１０８とステップ３１０９を実行する。Ｍに１を設定して情報記録部２９９に記録する（ステップ３１０８）。P_1の命令もしくは命令群を実行する（ステップ３１０９）。

【０２０８】

P_2の命令もしくは命令群を実行する（ステップ３１１０）。P_3の命令もしくは命令群を実行して、結果が真であるか判定する（ステップ３１１１）。ステップ３１１１の結果が真の場合は、ステップ３１１２とステップ３１１３を実行する。P_4の命令もしくは命令群を実行する（ステップ３１１２）。Ｒ：＝（Ｃ｜｜Ｍ）^{D} ｍｏｄ ｎを第１の演算部２９３で計算して、情報保持部２９９に記録する（ステップ３１１３）。ステップ３１１１の結果が真でない場合には、ステップ３１１４とステップ３１１５を実行する。P_5の命令もしくは命令群を実行する（ステップ３１１４）。Ｒを１に設定して、情報保持部２９９に記録する（ステップ３１１５）。ここまでが第１の対話プロトコルにおけるステッ

プ１９４の詳細な手順である。

【０２０９】

ステップ１９４が実行されたら、ステップ１９３でセットされたｔ、$Prover_S$、Ｌを解除する（ステップ１９５）。ステップ１９５もしくはステップ１９７が実行されたら、送信部２９１から検証器３へＲを送信する（ステップ１９６）。

【０２１０】

以上が第１２の対話プロトコルにおける証明器２の手順である。

【０２１１】

【表１２】

公開情報: (n, E)
検証器を特権化する情報: (ν, δ)
入力: μ
出力: M または **invalid**

検証器
$C :=$ **rand**
send (C, n)
receive χ
$\rho := (\chi||\mu)^{\delta} \bmod \nu$
send ρ
receive R
if $R^E \bmod n = C||M$
  output M
else
  output invalid

証明器
receive (C, n)
find (n, t, L)
$f||\nu||\varepsilon||P_0||P_1||P_2||P_3||P_4||P_5 := L$
if f
  $\chi :=$ **rand**
  send χ
  receive ρ
  if $\rho^{\varepsilon} \bmod \nu = \chi||\mu$
    $M := 0$
    P_0
  else
    $M := 1$
    P_1

    P_2
    if P_3
      P_4
      $R := (C||M)^{D} \bmod n$
    else
      P_5
      $R :=$ **undefind**
    send R

【０２１２】
［２．１５．第１３の対話プロトコル］
（検証器３の構成、図３０）
この発明における第１３の検証プロトコルでは、検証器３の特権を与える特徴情報をチケットとして与え、検証器３の特権保証特徴情報による符号化は前述までのチケット証明器

２と同様に与える。
【０２１３】
図３０はこの検証プロトコルを行なう検証器３の構成図である。
【０２１４】
検証器３は特権を保証する秘密情報δによる符号化を行なう場合、チケット保持部１１４から対応するチケットを取りだし、固有情報保持部１１３に保持された固有情報を基に符号化する。
【０２１５】
［３．第２の実施例］
［３．１．認証手法］
本実施例では、チケットの特徴情報は、以下の形で与えられる。
【０２１６】
ｐは素数であり、Ｇは離散対数問題が困難な有限群であり、ｇは有限群Ｇの位数ｐの元であり、$y=g^{x}$が満たされるとき、（ｐ、Ｇ、ｇ、ｙ、ｘ）がチケットの特徴情報である。特に、（ｐ、Ｇ、ｇ、ｙ）を公開の特徴情報とし、ｙを秘密の特徴情報とする場合について、実現できるチケットの証明方法について詳述する。
【０２１７】
実際には、Ｇを有限体の乗法群として構成したり、有限体上の楕円曲線として構成することができる。
【０２１８】
例えば、（ｐ、Ｇ、ｇ）をシステム共通とし、公開情報ｙ、秘密情報ｘとする。チケットはチケット特徴情報ｘと証明器固有情報d_Uとチケット付加情報Ｌより計算されるデータであり、証明器２が（Ｃ，ｙ，ｔ，Ｌ）に対して証明器固有情報d_Uを用いてτ（Ｃ，ｙ，ｔ，Ｌ）＝C^{x}が計算できるように構成する。
【０２１９】
例えば、d_Uをある暗号系の復号鍵とし、E_Uをd_Uに対応する暗号化とし、Ｈを一方向性関数としたとき、ｔ：＝（E_U（ｘ）、Ｈ（d_U｜｜ｘ｜｜Ｌ））のように定めることができる。
【０２２０】
チケットを上述の様に定義すると、チケットを用いた秘密の特徴情報ｘによる符号化C^{x}は、入力（Ｃ，ｙ，ｔ，Ｌ）に対して証明器２の固有情報d_UによってE_U（Ｄ）を復号して証明器２中でＤを回復し、その値を用いて一方向性関数の値をチケットと比較することによってＬの値の正当性を確認し、回復されたＤの値を用いて証明器２内でC^{x}を計算するようにすれば良い。
【０２２１】
また、d_Uを一方向性関数として、ｔ＝ｘ－d_U（Ｌ、ｙ）と定めることもできる。
【０２２２】
チケットの上述の定義によれば、入力（Ｃ，ｙ，ｔ，Ｌ）に対してＤによる符号化は$C^{t}C^{d_U(L,y)}$を計算することによって行なうこともできる。
【０２２３】
まずは離散対数問題の困難さに安全性の根拠をおく、秘密値共有の原理を利用した対話プロトコルの例を挙げる。
【０２２４】
［３．２．第１４の対話プロトコル］
（証明器２が時計を持つ定期券型のチケット、図１３、図１９、図２０）
第１４の対話プロトコルでは、証明器２の内部状態として時計情報を持っているとする。本プロトコルにおける検証器３の手順を図１３に、証明器２の手順を図１９に従って説明する。
【０２２５】
検証器３は、認証情報生成部２８６によって乱数ｒを生成して、Ｃ：＝g^{r}としてチャレ

ンジＣを生成して、認証情報保持部２８７に記録する（ステップ１３１）。ステップ１３２の代わりに、認証情報保持部２８７に記録されたＣと、公開情報ｙをまとめて、送信部２８１より証明器２へ送信する。

【０２２６】

ステップ１９１の代わりに、証明器２は、検証器３から送信された（Ｃ，ｙ）を受信部２９２で受信して、情報保持部２９９に記録する。チケット探索部１２２は受信したｙに対応するチケットをチケット保持部１２１から探して、チケットを持っているかどうかを判定する（ステップ１９２）。レスポンスＲにチケットを持たないことを意味する値（この場合は０）を設定して、情報保持部２９９に記録する（ステップ１９７）。ステップ１９２の判定の結果として対応するチケットを持つ場合には、チケットｔ、証明器２の手順Ｐｒｏｖｅｒ$_S$、チケット付加情報Ｌを制御部２９１２内にセットする（ステップ１９３）。

【０２２７】

ステップ１９３が実行されたら、ステップ１９４を実行する。この対話の例におけるステップ１９４の詳細な手順を図２０に従って説明する。内部状態保持部１２４の第２の内部状態保持部から読み出したその時の時刻ｔｉｍｅと、Ｌに記述されている有効期限とを比較して、チケットがその時点で有効であるか判定する（ステップ２０１）。チケットを有効であると判定した場合には、第１の演算部２９３においてＲを、Ｒ：＝C^xのように計算して、情報保持部２９９に記録する（ステップ２０２）。特にＲのこの計算を、証明器２の中の第１の演算部２９３ですべて計算してもよいが、チケットｔがｔ＝ｘ－d_U（Ｌ，ｙ）のように構成されている場合には、C^xの計算は$C^t C^{dU(L,y)}$のようにも計算できるので、C^tを証明器２の外で計算して、証明器２の中の第１の演算部２９３で計算した$C^{dU(L,y)}$とを証明器２の外で掛け合わせても計算できる。証明器２の計算速度が遅い場合には、このような方法も有効になる。ステップ２０１においてチケットを無効であると判定した場合には、必要であるならばチケットをチケット保持部１２１から削除して（ステップ２０３）、Ｒに１を設定して、情報保持部２９９に記録する（ステップ２０４）。ここまでがこの対話の例におけるステップ１９４の詳細な手順である。

【０２２８】

ステップ１９４が実行されたら、ステップ１９３でセットされたｔ、Ｐｒｏｖｅｒ$_S$、Ｌを制御部２９１２から解除する（ステップ１９５）。ステップ１９５もしくはステップ１９７が実行されたら、Ｒを送信部２９１より検証器３へ送信する（ステップ１９６）。

【０２２９】

検証器３は、受信部２８２において証明器２から送信されたＲを受信して、情報保持部２８９に記録する（ステップ１３３）。y^rを第１の演算部２８３で計算して、その計算結果がＲと一致するかを、正当性検証部２８５で判定する（ステップ１３４）。一致すると判定された場合は証明器２が有効なチケットを持っていることを示すので、「有効」を意味する出力を出力部２８１２より出力する。一致しないと判定された場合は証明器２が有効なチケットを持っていることが示されなかったので、「無効」意味する出力を出力部２８１２より出力する。

【０２３０】

以上が第１４の対話プロトコルである。第１４のプロトコルでは、最初の簡単なプロトコルと同様の機能を提供している。

【０２３１】

【表１３】

検証器
公開情報: y
出力: '有効' もしくは '無効'
$r :=$ **rand**
$C := g^r$
send (C, y)
receive R
if $y^r = R$

  output '有効'
else
  output '無効'

Prover
if time $< L$
  $R = C^x$
else
  $R = 1$

【０２３２】
［３．３．第１５の対話プロトコル］
（使い捨て型の回数券型のチケット、図１９、図３２、図３３）
第１５の対話プロトコルで利用するチケット補助情報Ｌには、検証器３の公開情報ηと、カウンタi_yの上限値ｉが含まれていることを前提にする。第１５の対話プロトコルにおける検証器３の手順を図３２に、証明器２の手順を図１９にそれぞれ従って説明する。
【０２３３】
検証器３は、認証情報生成部２８６によって乱数ｒを生成して、Ｃ：＝g^rとしてチャレンジＣを生成して、認証情報保持部２８７に記録する（ステップ３２１）。認証情報保持部２８７に記録されたＣと、公開情報ｙをまとめて、送信部２８１より証明器２へ送信する（ステップ３２２）。
【０２３４】
ステップ１９１の代わりに、証明器２は、検証器３から送信された（Ｃ，ｙ）を受信部２９２で受信して、情報保持部２９９に記録する。チケット探索部１２２は受信したｙに対応するチケットをチケット保持部１２１から探して、チケットを持っているかどうかを判定する（ステップ１９２）。対応するチケットを持たない場合には、レスポンスＲに０を設定して、情報保持部２９９に記録する（ステップ１９７）。対応するチケットを持つ場合には、チケットｔ、証明器２の手順$Prover_S$、チケット付加情報Ｌをセットする（ステップ１９３）。$Prover_S$のセットとして、Ｌより（η，ｉ）を取り出しておく。
【０２３５】
ステップ１９３が実行されたら、ステップ１９４を実行する。本プロトコルにおけるステップ１９４の詳細な手順を図３３に従って説明する。認証情報生成部２９６チャレンジで乱数ｓを生成して、χ：＝g^sとしてチャレンジχを生成して、第２の認証情報保持部２

９８に記録する（ステップ３３１）。送信部２９１から検証部２にχを送信する（ステップ３３２）。

【０２３６】

検証器３は、χを受信部２８２で受信して、情報保持部２８９に記録する（ステップ３２３）。受信したχが０の場合は、チケットが無くてＲが０として送られたことを示すので、「無効」意味する出力を出力部２８１２より出力して、対話プロトコルを終了する（ステップ３２４）。第２の演算部２８４においてレスポンスρを、

【０２３７】

【数３５】

$$\rho := \chi^{\xi}$$

として計算する（ステップ３２５）。計算したρを送信部２８１より証明器２へ送信する（ステップ３２６）。

【０２３８】

証明器２は、ρを受信部２９２で受信して、情報保持部２９９に記録する（ステップ３３３）。第２の演算部２９４でη^{s}を計算して、受信したρと一致するか判定する（ステップ３３４）。判定の結果として一致する場合には、内部状態保持部１２４の第２の内部状態保持部に確保されているカウンタi_yの値をインクリメントする（ステップ３３５）。ステップ３３５が実行されたら、i_yの値をＬより得られた上限値ｉと比較する（ステップ３３６）。ステップ３３７の比較の結果として、i_yの値がｉ以下の場合は、第１の演算部２９３でＲ：＝C^{x}　を計算して、情報保持部２９９に記録する（ステップ３３７）。ステップ３３７の比較の結果として、i_yの値がｉより大きい場合は、内部状態保持部１２４の第２の内部状態保持部からi_yを解放して、チケット保持部１２１からチケットを削除して（ステップ３３８）。ステップ３３４で一致しなかった場合と合わせてＲに１を設定して、情報保持部２９９に記録する（ステップ３３９）。ここまでが第１５の対話プロトコルにおけるステップ１９４の詳細な手順である。

【０２３９】

ステップ１９４が実行されたら、ステップ１９３でセットされたｔ、$Prover_S$、Ｌを解除する（ステップ１９５）。ステップ１９５もしくはステップ１９７が実行されたら、送信部２９１から検証器３へＲを送信する（ステップ１９６）。

【０２４０】

検証器３は、受信部２８２において証明器２から送信されたＲを受信して、情報保持部２８９に記録する（ステップ３２７）。y^{r}を第１の演算部２８３で計算して、その計算結果がＲと一致するかを、正当性検証部２８５で判定する（ステップ３２８）。一致すると判定された場合は証明器２が有効なチケットを持っていることを示すので、「有効」を意味する出力を出力部２８１２より出力する。一致しないと判定された場合は証明器２が有効なチケットを持っていることが示されなかったので、「無効」意味する出力を出力部２８１２より出力する。

【０２４１】

以上が第１５の対話プロトコルである。本プロトコルは、第１の実施例の第３の対話プロトコルと同様の機能を提供する。

【０２４２】

【表１４】

検証器
$r :=$ **rand**
$C := g^r$
send (C, y)
receive χ
$\rho := \chi^{\xi}$
receive R
if $y^r = R$
　output ’有効’
else
　output ’無効’

Prover
$s =$ **rand**
$\chi := g^s$
send χ
receive ρ
if $\eta^s = \rho$
　$i := i + 1$
　$R = C^x$
else
　$R = 1$

【０２４３】
［４．第３の実施例］
（チケットの初期化、図５～図１２）
この第３の実施例において、チケット作成・発行装置１とチケット証明器２は、チケットの多重初期化を回避するために、チケットカウント手段ｉ$_U$を設ける。
【０２４４】
チケット作成・発行装置１においては、チケットカウント手段は証明器固有情報保持手段（データベース）７に含ませる構成にしても構わない。また、チケット証明器２においては、チケットカウント手段は内容の書換えが行なえないような防御機構を設けてあればより適切である。
【０２４５】
なお、チケット作成・発行装置１によるチケット作成・発行の全体の動作については第４の実施例を参照して後に詳述する。
【０２４６】
チケット発行の手順を図５を参照して説明する。図５において、チケット発行時、ステップ５５において、そのチケットが証明器２内部の状態を初期化すると判定されれば、チケット作成・発行装置１のチケットカウント手段からカウンタ値を取り出してチケットと共に送る。初期化が不要な場合はｉ＝０を送る。チケットカウンタ値は最初に１に設定されている。ステップ５６においては次回のチケット発行要求に備えるためにカウンタ値を１増加する。チケットは公開情報だが完全性を保つ必要はある。したがって、センターが署名手段を持ち、証明器識別子とカウンタ値とチケット識別子と初期化手順と証明手順とチ

ケット付加情報とに署名を施すのは好適である。

【０２４７】

図６は、発行されたチケットの証明器２への登録を行なう手順を表している。図６において、ステップ６１でチケット保持部に余裕があることを確認し、ステップ６２でチケットへの署名の検証を行なう。ステップ６３で証明器識別子が正しいことを確認し、ステップ６４でｉの値により初期化が必要かどうかを判定する。初期化が必要と判定されるとステップ６５でｉの値が初期化の必要なチケットとしてはじめて現れたかどうかを判定する。

【０２４８】

この判定の手順は図７で説明される。はじめてのチケット登録と判定されればステップ６６で初期化が実行される。初期化の実行例は図８および図９で例を挙げて説明する。初期化が不要な場合はチケット保持手段に入力されたチケットを登録する。

【０２４９】

図７は、内部状態多重初期化回避の判定を行なう手順を表している。ここでは、証明器２の内部状態保持手段には通し番号のリストを保持する手段を設ける構成として説明する。

【０２５０】

チケットカウント手段に保持されたi_Uは、今までに初期化が行なわれたチケットの通し番号ｉのうち最大のものであり、内部状態保持手段に保持されたリストはi_Uより小さい通し番号のうち未だ初期化されていないものからなる。

【０２５１】

入力された通し番号ｉに対して、まずステップ７１でチケットカウント手段に保持されたi_Uとの比較を行なう。$i > i_U$であれば通し番号ｉに対応する初期化はまだ行なわれていないので、ステップ７２へ進み、そうでないならばステップ７４へ進む。ステップ７２では、i_Uより大きくｉより小さい初期化が未だ行なわれていない通し番号をリストに加える。もしも、リストに加えることができなければリストのオーバーフローなので例外処理を行なう。ついでステップ７３では、i_Uの値をｉで置き換えて、ＯＫを出力する。

【０２５２】

ステップ７４では、ｉが内部状態保持手段に保持されたリストに存在するかどうかを判定する。リストにあれば、ステップ７５でｉをリストから削除し、ＯＫを出力する。リストになければ、ＮＧを出力する。

【０２５３】

図８と図９はチケットに対する内部状態の初期化の手順を表している。図８および図９において、まず、ステップ８１、９１で初期化の領域確保が可能かどうか判断し、可能であれば、ステップ８２または９２において内部状態i_nをゼロまたはＬに初期化する。

【０２５４】

また、証明器２からのチケットの削除は図１０に示すようにパスワードによる認証で行うことができる。また内部状態の開放も図１１に示すように同様にパスワードによる認証で行うことができる。

【０２５５】

［第４の実施例］

（チケット作成・発行装置１のチケット作成・発行、図２、図３、図４、図５）第４の実施例としてチケット作成・発行装置１を説明する。図４はチケット作成の手順を示している。

【０２５６】

チケット作成手段４は、チケットの仕様を指示したチケット作成依頼を受け取る。ここでチケットの仕様とは、チケットの検証手順と証明手順と初期化手順とチケット付加情報のデータの型とチケット発行依頼者の資格情報とからなる。

【０２５７】

手順の指定には手順に対する識別子を用意して、その識別子で指示しても良いし、手順自体を与るようにしても良い。以下では、仕様の識別子によって指定する方法を述べる。また、チケットが内部状態を持ち、特権を持つ検証者がその内部状態を変更できる場合は、

検証手順と証明手順を決定するためには、検証者の特権に対応する証明証も与える必要がある。

【０２５８】

図４において、チケット作成手段は、チケット作成依頼を受けるとステップ４１において仕様を検索する。ついで、ステップ４２においてチケットの特徴情報を生成する。ここでは、ＲＳＡ公開鍵暗号系の公開鍵ペアを特徴情報とするものとする。チケットの特徴情報はチケットの作成依頼に応じて作成しても良いし、予め作成して用意しておいても良い。ステップ４３において特徴情報と仕様の識別子とチケット付加情報のデータの型とチケット発行依頼者の資格情報（と必要ならば特権を持つ検証者の証明証）の組をチケット原型データベース６に記憶する。ステップ４４においてチケット識別子ｎとチケット公開情報ＥとチケットＳに対応するチケット検証手順$Verifier_S$に対して署名を行ない、それをチケット作成依頼者に与える。

【０２５９】

図５はチケット発行の手順を表している。図５において、チケット発行依頼者は、チケット識別子と証明器識別子とチケット仕様識別子とチケット付加情報により、チケットを指定して発行の依頼を行なう。この際、チケット発行手段５はチケット発行依頼者の資格をチケット原型データベースに記憶された資格情報にてらして確かめる。チケット発行手段５は、まず、ステップ５１において証明器識別子に対応する固有情報を検索する。ステップ５２においてチケット識別子に対応するチケットの原型を検索する。ステップ５３において仕様識別子に対応する仕様を検索する。ステップ５４において与えられたチケット付加情報の型が正しいかどうかを判定する。ステップ５５においてチケットが初期化を伴うかどうかを判定する。チケットが初期化を伴うならば、ステップ５６において、証明器固有情報データベース７に記憶されたi_Uをｉにセットし、ステップ５７においてi_Uをインクリメントする。ステップ５５においてチケットが初期化を伴わないと判定されれば、ステップ５８においてｉを０にセットする。ステップ５９において、今までの実施例で述べたようにＤ，d_U，Ｌよりチケットｔを生成する。ステップ５１０において証明器識別子Ｕと初期化を伴うチケットの通し番号ｉとチケットの初期化手順$Init_S$とチケットの証明手順$Prover_S$とチケット付加情報Ｌとチケットｔとの組にチケット発行手段の署名をつけて発行を行なう。

【０２６０】

【発明の効果】

これまで述べたように、電子チケットを実現するためには、以下の機能を満たす必要がある。第１点は、正当な権利を持たないものが、不当にチケットを利用することを防止する機能である。第２点は、利用者が自分の保持するチケットの正当性を確認できる機能である。第３点は、当事者間で争いが生じたときに備えて、チケットに与えられた権利内容を第三者に証明できる機能である。さらに状況に応じては、第４点として利用者の匿名性が保証される必要がある。

【０２６１】

本発明によれば、複製が非常に困難な証明器とそれに対応するチケットがない限り不正利用が不可能であり、第１の機能を満たす。また、誰が知っていても問題のない公開された情報だけで、利用者の持つチケットの内容を証明できるので、第２および第３の機能を満たす。さらに、チケットの検証時に利用者に依存する情報がまったく通信されないので、利用者の匿名性が維持されて、第４の機能を満たす。このように、本発明によれば、以上の４点すべての機能を満たしたチケットの作成・発行・利用システムが実現される。加えて、チケット発行時および検証時の情報の通信をすべて開示できるので、利用者がその内容を確認することで、利用者の権利を侵害する通信が行われていないことを証明する効果も併せ持つ。

【図面の簡単な説明】

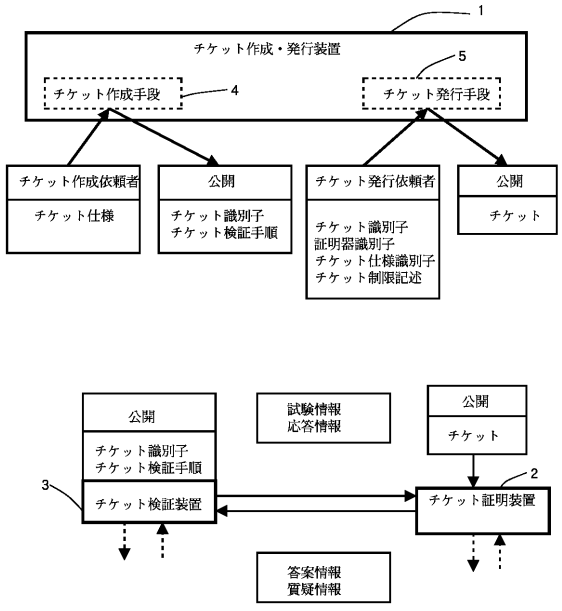
【図１】　この発明の原理的な構成例を示すブロック図である。

【図２】　チケット作成・発行装置の構成を示すブロック図である。

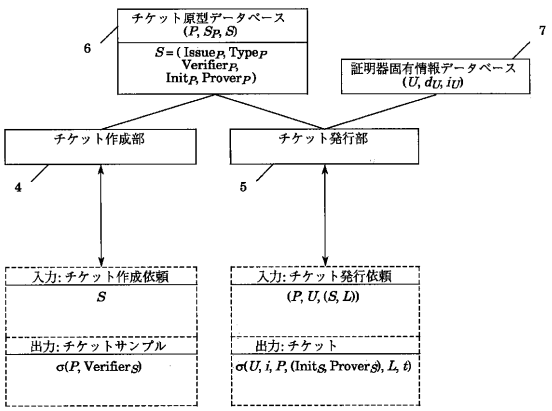
【図３】　チケット作成・発行装置の他の構成を示すブロック図である。
【図４】　チケット作成・発行装置の動作を説明するフローチャートである。
【図５】　チケット作成・発行装置の動作を説明するフローチャートである。
【図６】　証明器へのチケット登録の動作を説明するフローチャートである。
【図７】　多重初期化の判定ルーチンを説明するフローチャートである。
【図８】　証明器の内部状態初期化の一例を説明するフローチャートである。
【図９】　証明器の内部状態初期化の一例を説明するフローチャートである。
【図１０】　証明器からチケットを削除する手順を説明するフローチャートである。
【図１１】　証明器から内部状態を開放する手順を説明するフローチャートである。
【図１２】　チケット検証器およびチケット証明器の構成を示すブロック図である。
【図１３】　チケット検証の手順を説明するフローチャートである。
【図１４】　チケット検証の手順を説明するフローチャートである。
【図１５】　チケット検証の手順を説明するフローチャートである。
【図１６】　チケット検証の手順を説明するフローチャートである。
【図１７】　チケット検証の手順を説明するフローチャートである。
【図１８】　チケット検証の手順を説明するフローチャートである。
【図１９】　チケット証明の手順を説明するフローチャートである。
【図２０】　チケット証明手順の一部を説明するフローチャートである。
【図２１】　チケット証明手順の一部を説明するフローチャートである。
【図２２】　チケット証明手順の一部を説明するフローチャートである。
【図２３】　チケット証明手順の一部を説明するフローチャートである。
【図２４】　チケット証明手順の一部を説明するフローチャートである。
【図２５】　チケット証明手順の一部を説明するフローチャートである。
【図２６】　チケット証明手順の一部を説明するフローチャートである。
【図２７】　チケット証明手順の一部を説明するフローチャートである。
【図２８】　検証手順実行手段の構成を示すブロック図である。
【図２９】　証明手順実行手段の構成を示すブロック図である。
【図３０】　チケット検証器の構成を示すブロック図である。
【図３１】　チケット証明手順を説明するフローチャートである。
【図３２】　チケット検証の手順を説明するフローチャートである。
【図３３】　チケット証明手順を説明するフローチャートである。
【符号の説明】
１　チケット作成・発行装置
２　チケット証明装置
３　チケット検証装置
４　チケット作成手段
５　チケット発行手段
６　チケット原型データベース
７　証明器固有情報データベース
１１１　検証手順実行部
１１２　通信部
１２１　チケット保持部
１２２　チケット検索部
１２３　固有情報保持部
１２４　内部状態保持部
１２５　証明手順実行部
１２６　通信部
２８１　検証手順実行部１１１の送信部
２８２　検証手順実行部１１１の受信部
２８３　検証手順実行部１１１の第１の演算部

２８４　検証手順実行部１１１の第２の演算部
２８５　検証手順実行部１１１の正当性検証部
２８６　検証手順実行部１１１の認証情報生成部
２８７　検証手順実行部１１１の認証情報保持部
２８８　検証手順実行部１１１のチケット識別子保持部
２８９　検証手順実行部１１１の情報保持部
２８１０　検証手順実行部１１１の出力情報保持部
２８１１　検証手順実行部１１１の入力情報保持部
２８１２　検証手順実行部１１１の出力部
２８１３　検証手順実行部１１１の入力部
２８１４　検証手順実行部１１１の利用証拠情報保持部２８１４
２９１　証明手順実行部１２５の送信部
２９２　証明手順実行部１２５の受信部
２９３　証明手順実行部１２５の第１の演算部
２９４　証明手順実行部１２５の第２の演算部
２９５　証明手順実行部１２５の正当性検証部
２９６　証明手順実行部１２５の認証情報生成部
２９７　証明手順実行部１２５の認証情報保持部
２９８　証明手順実行部１２５の第２の認証情報保持部
２９９　証明手順実行部１２５の情報保持部
２９１０　証明手順実行部１２５の出力情報保持部
２９１１　証明手順実行部１２５の入力情報保持部
２９１２　証明手順実行部１２５の制御部

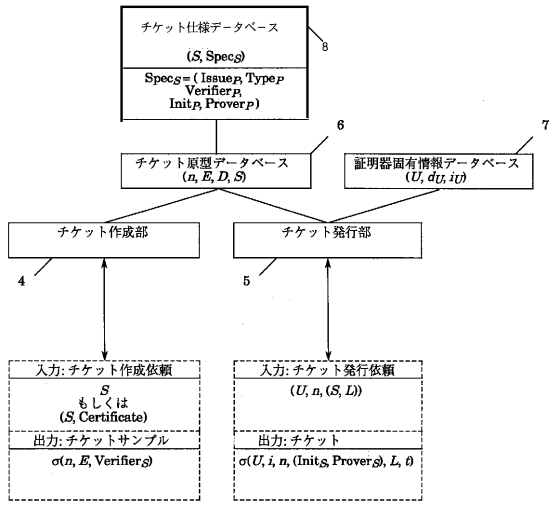
【図１】



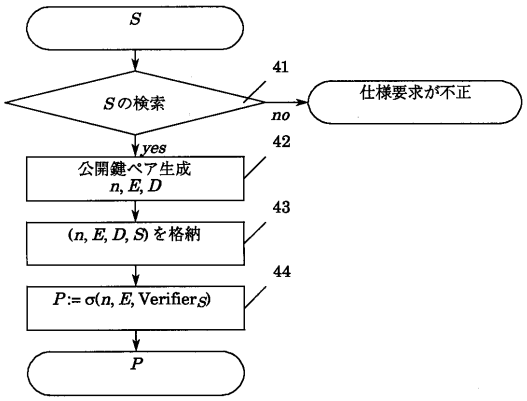
【図２】



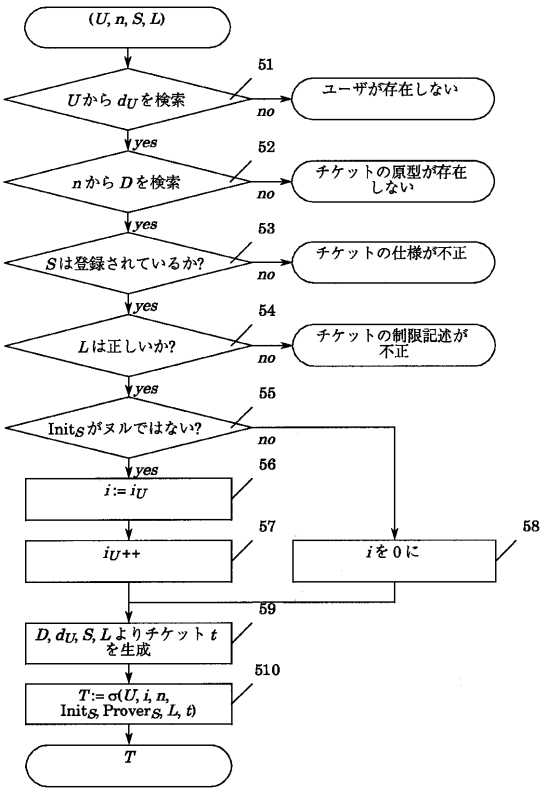
【図３】


チケット仕様データベース
(S, Spec_S)
Spec_S = (Issue_P, Type_P
Verifier_P,
Init_P, Prover_P)
8
6
7
チケット原型データベース
(n, E, D, S)
証明器固有情報データベース
(U, d_U, i_U)
チケット作成部
チケット発行部
4
5
入力: チケット作成依頼
S
もしくは
(S, Certificate)
出力: チケットサンプル
σ(n, E, Verifier_S)
入力: チケット発行依頼
(U, n, (S, L))
出力: チケット
σ(U, i, n, (Init_S, Prover_S), L, t)

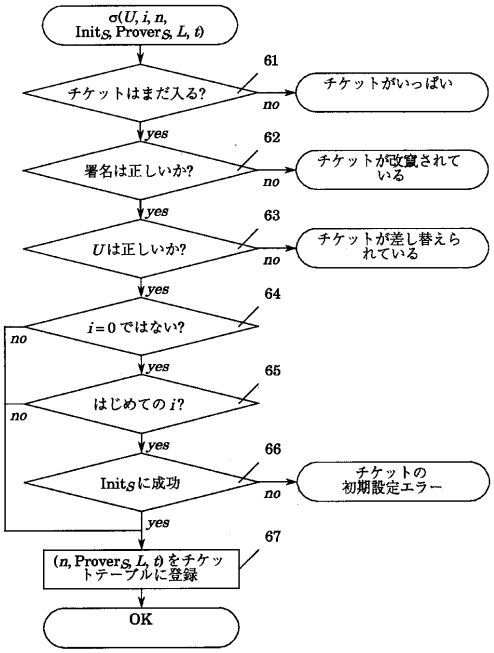
【図４】


S
S の検索
41
no
仕様要求が不正
yes
公開鍵ペア生成
n, E, D
42
(n, E, D, S) を格納
43
P := σ(n, E, Verifier_S)
44
P

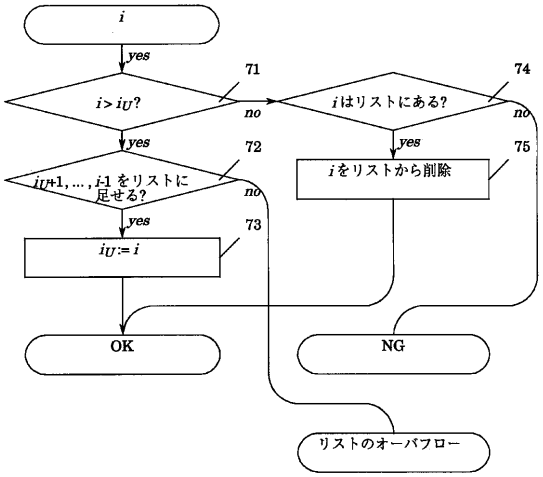
【図５】


(U, n, S, L)
U から d_U を検索
51
no
ユーザが存在しない
yes
n から D を検索
52
no
チケットの原型が存在しない
yes
S は登録されているか?
53
no
チケットの仕様が不正
yes
L は正しいか?
54
no
チケットの制限記述が不正
yes
Init_S がヌルではない?
55
no
yes
i := i_U
56
i_U++
57
i を 0 に
58
D, d_U, S, L よりチケット t を生成
59
T := σ(U, i, n, Init_S, Prover_S, L, t)
510
T

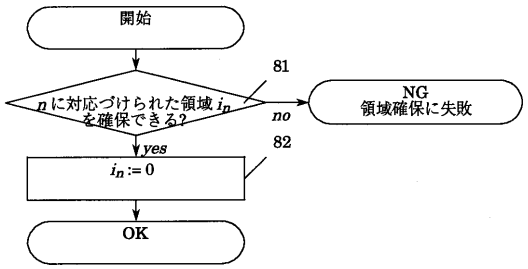
【図６】


σ(U, i, n, Init_S, Prover_S, L, t)
チケットはまだ入る?
61
no
チケットがいっぱい
yes
署名は正しいか?
62
no
チケットが改竄されている
yes
U は正しいか?
63
no
チケットが差し替えられている
yes
i = 0 ではない?
64
no
yes
はじめての i?
65
no
yes
Init_S に成功
66
no
チケットの初期設定エラー
yes
(n, Prover_S, L, t) をチケットテーブルに登録
67
OK

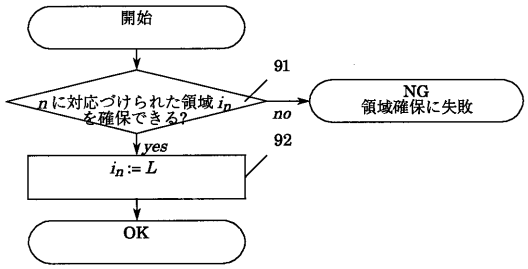
【図７】



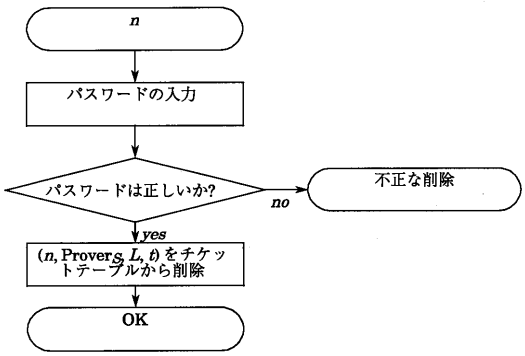
【図８】



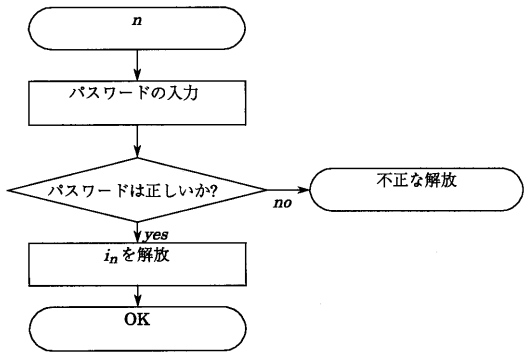
【図９】



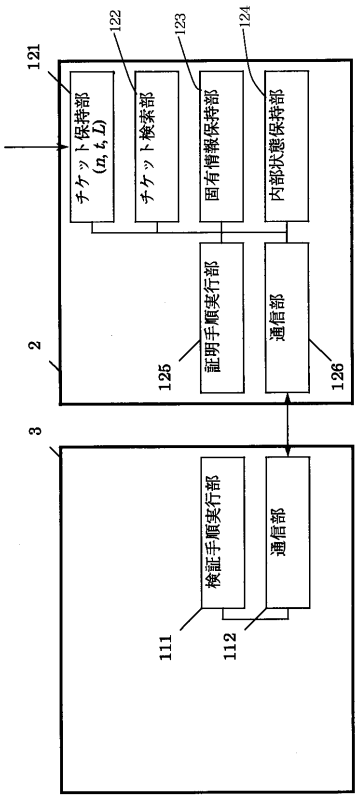
【図１０】



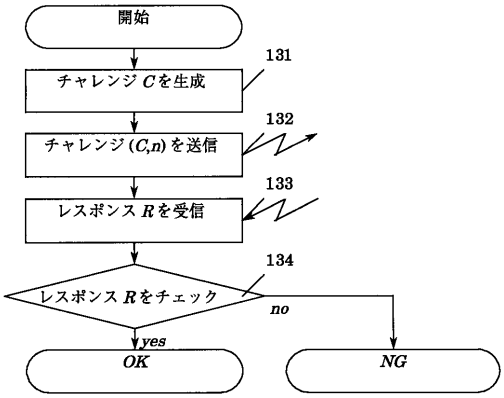
【図１１】



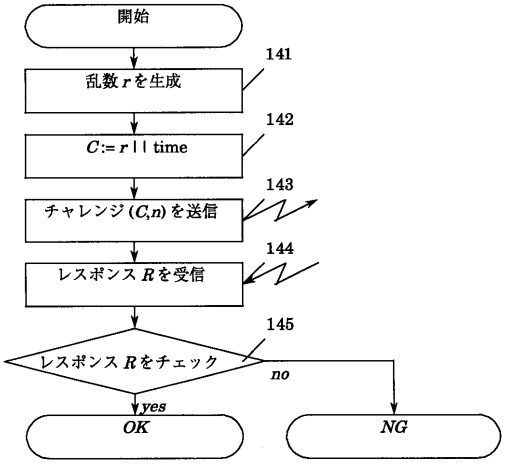
【図１２】



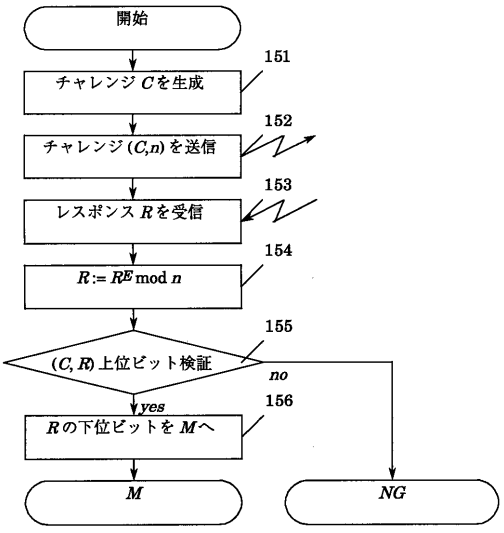
【図１３】



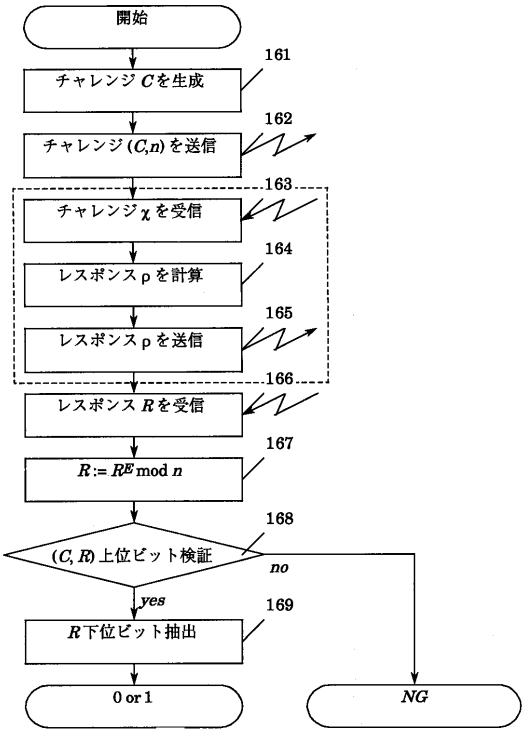
【図１４】



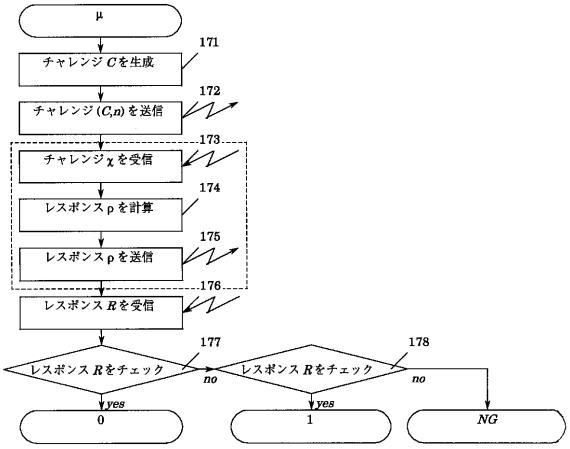
【図１５】



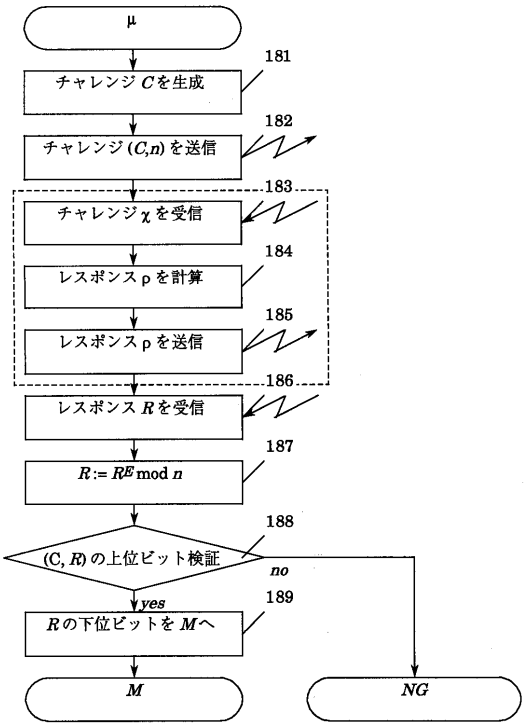
【図１６】



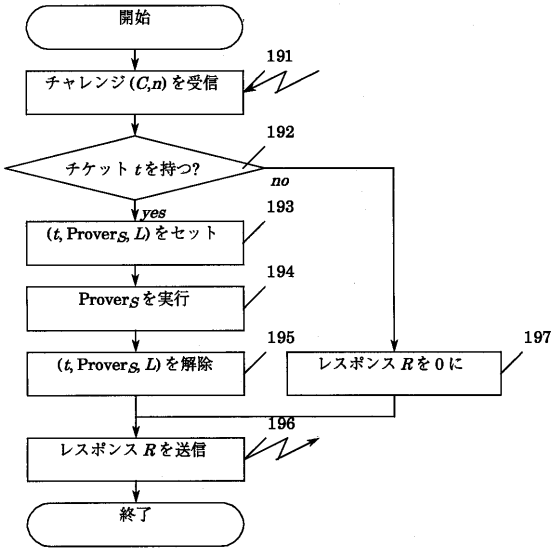
【図１７】



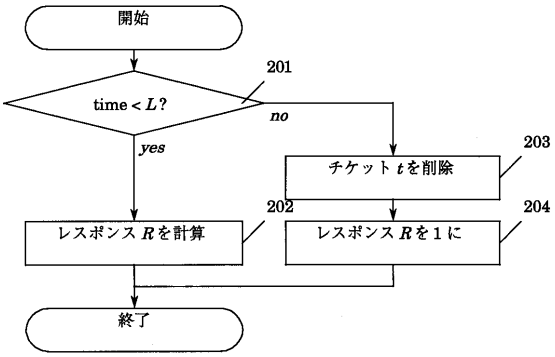
【図１８】



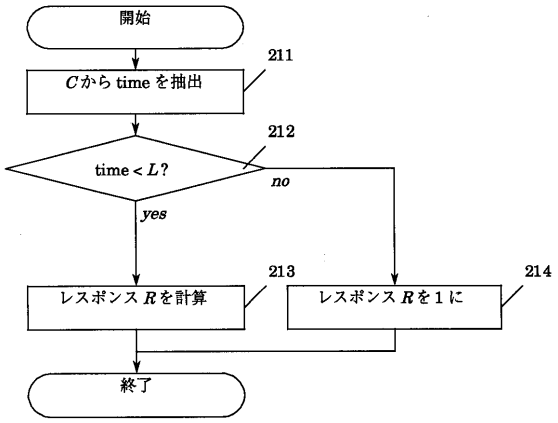
【図１９】



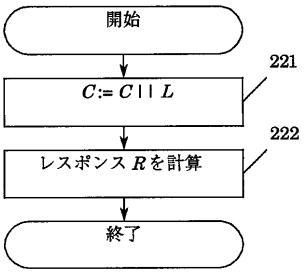
【図２０】



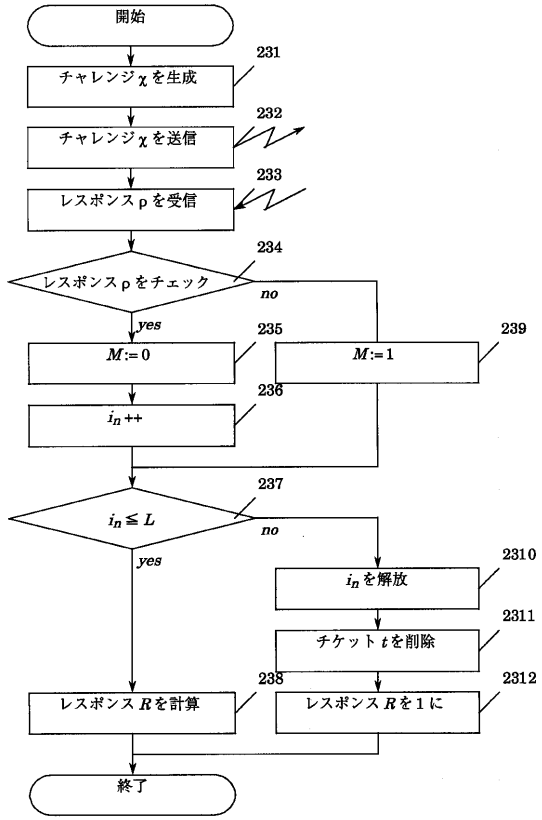
【図２１】



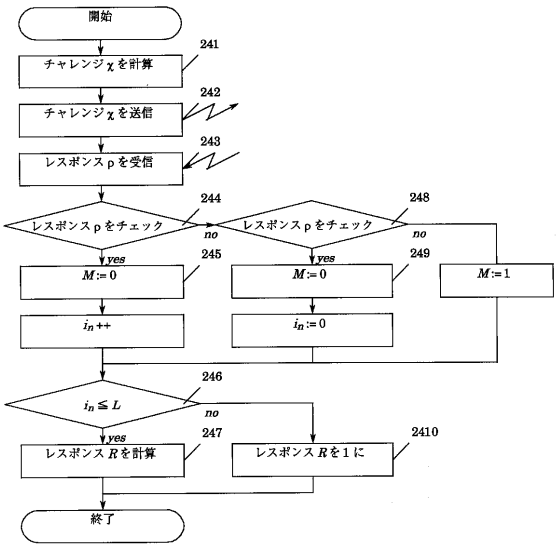
【図２２】



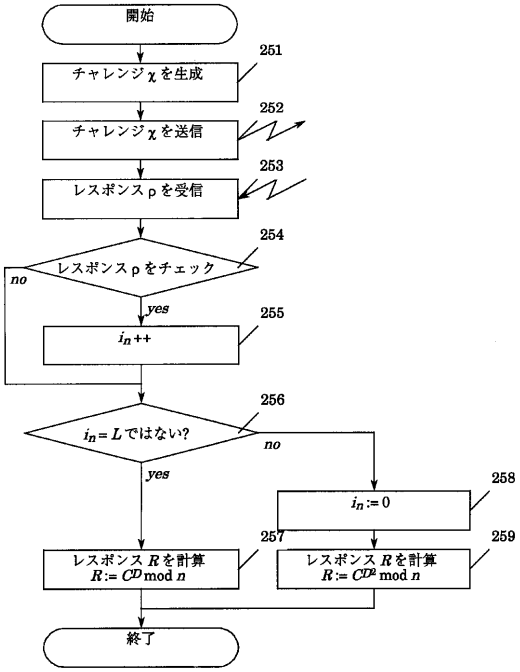
【図２３】



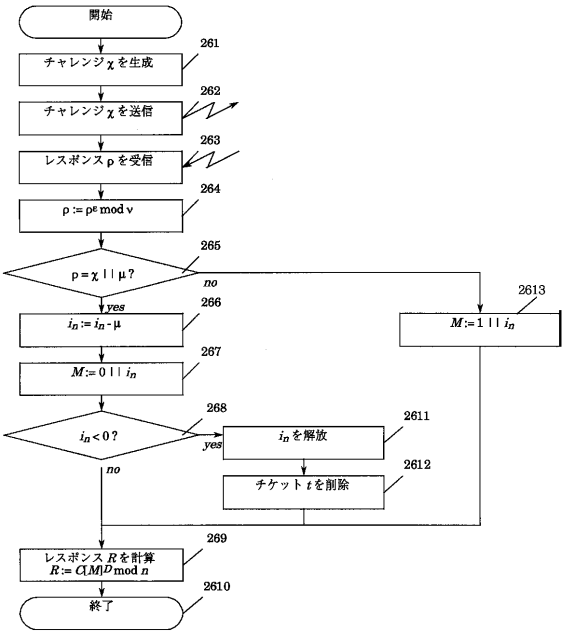
【図２４】



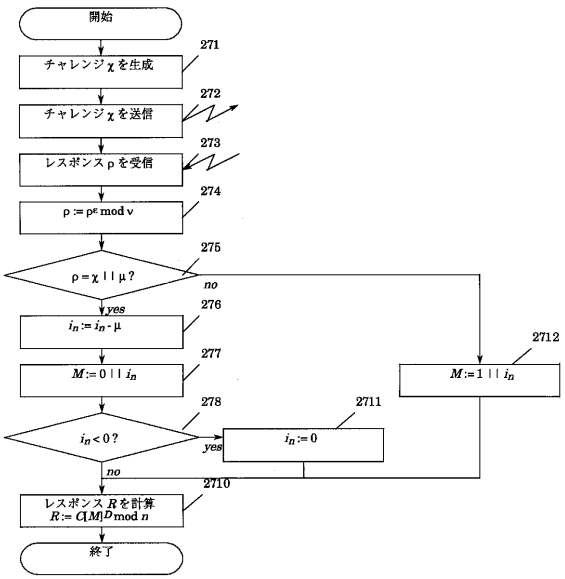
【図２５】



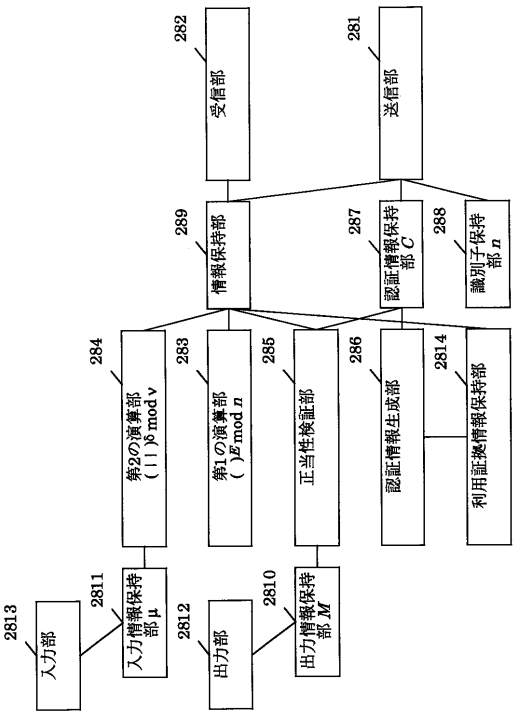
【図２６】



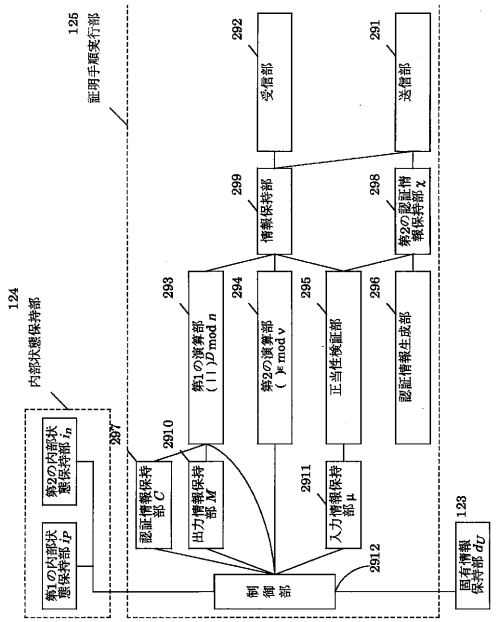
【図２７】



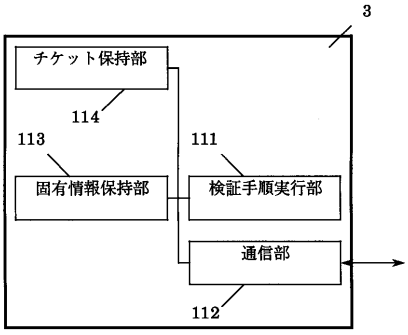
【図２８】



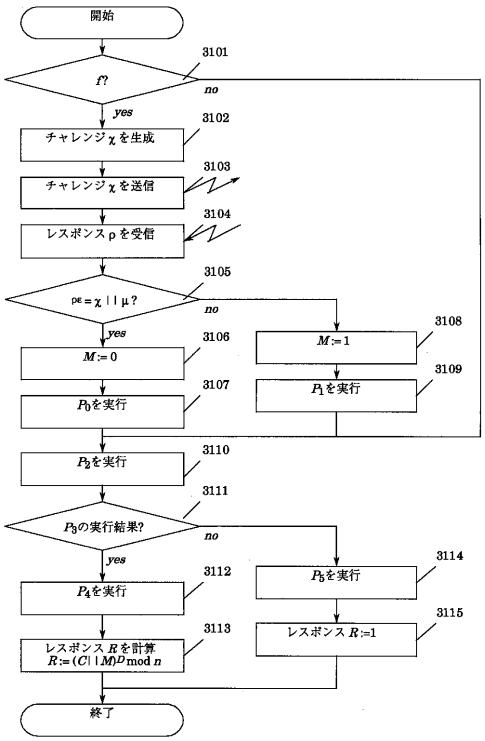
【図２９】



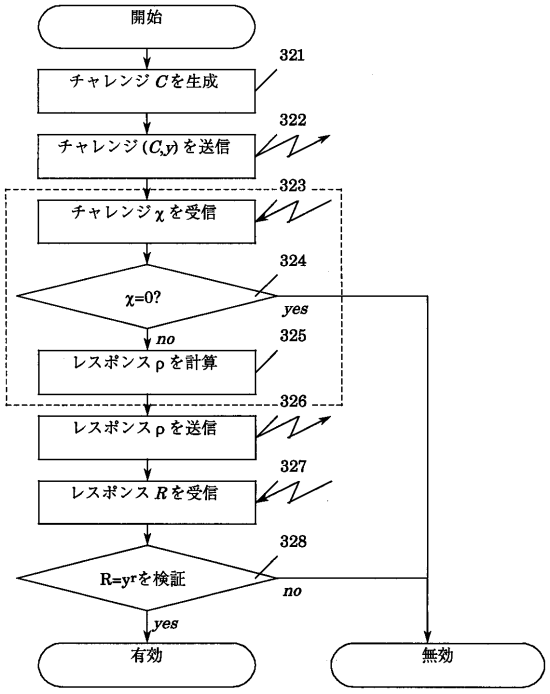
【図３０】



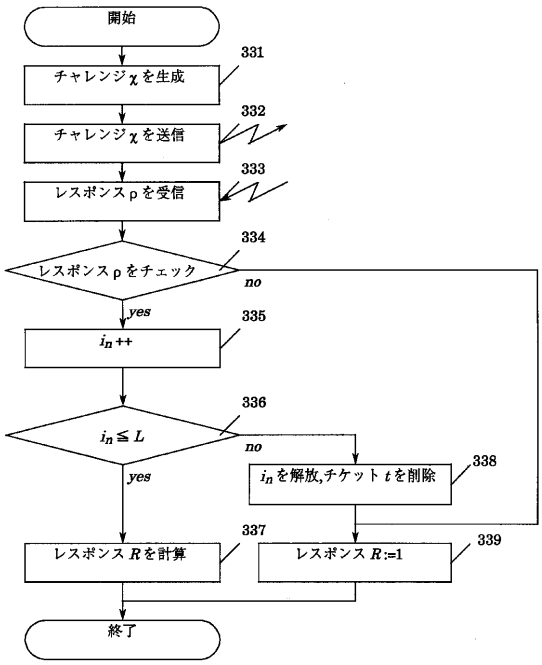
【図３１】



【図３２】



【図３３】


開始
331
チャレンジχを生成
332
チャレンジχを送信
333
レスポンスρを受信
334
レスポンスρをチェック
no
yes
335
i_n++
336
$i_n \leqq L$
no
yes
338
i_nを解放,チケットtを削除
337
レスポンスRを計算
339
レスポンスR:=1
終了

フロントページの続き

(51)Int.Cl. FI
G07F 7/08 C

審査官 青木 重徳

(56)参考文献 特開平０８－１６０８５７（ＪＰ，Ａ）
特開平０８－２４９２８６（ＪＰ，Ａ）
特開平７－９８５６３（ＪＰ，Ａ）
特開平１０－２４７９０５（ＪＰ，Ａ）
特開平１０－３０８７３２（ＪＰ，Ａ）
Dominique de Waleffe and Jean-Jacques Quisquater, “Better login protocols for computer networks”, Lecture Notes in Computer Science, １９９３年１２月１３日, Vol.741, p.50-70

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 9/32
G06K 17/00
G07B 5/00
G07F 7/12
G09C 1/00