(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3613936号
(P3613936)
(45)発行日　平成17年1月26日(2005.1.26)　(24)登録日　平成16年11月12日(2004.11.12)

(51)Int.Cl.[7]	F I		
H04L 9/32	H04L	9/00	675B
G06F 9/06	G06F	9/06	550A
G06F 12/14	G06F	12/14	320A
G09C 1/00	G09C	1/00	640B
	G09C	1/00	640E

請求項の数 62　(全 49 頁)

(21)出願番号　特願平9-181025
(22)出願日　平成9年7月7日(1997.7.7)
(65)公開番号　特開平11-27257
(43)公開日　平成11年1月29日(1999.1.29)
審査請求日　平成11年6月29日(1999.6.29)

前置審査

(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
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100101801
弁理士　山田　英治
(72)発明者　筧　るみ子
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　京嶋　仁樹
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】アクセス資格認証装置

(57)【特許請求の範囲】
【請求項１】
ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証装置において、
認証用データを記憶する第１の記憶手段と、
ユーザの固有情報を記憶する第２の記憶手段と、
上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、証明用補助情報を生成するために予め定められた第１の所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、
上記第１の記憶手段に保持されている上記認証用データと、上記第２の記憶手段に保持されている上記ユーザの固有情報とに証明データを生成するために予め定められた第２の所定の計算を実行して証明データを生成する証明データ生成手段と、
上記証明データが上記ユーザの固有情報に基づいて生成されていることを検証する証明データ検証手段であって、上記証明データ生成手段によって生成された証明データと、上記第３の記憶手段に保持されている上記証明用補助情報とに検証用に予め定められた第３の所定の計算を実行する演算手段を有し、上記演算手段の計算結果を使用して検証を行なうものとを有し、
上記証明用補助情報を生成するために予め定められた第１の所定の計算と、上記証明データを生成するために予め定められた第２の所定の計算と、上記検証用に予め定められた第３の所定の計算とを、上記ユーザの固有情報、上記アクセス資格の特徴情報および上記

証明用補助情報が対応する場合に上記証明データ検証手段が上記証明データを正当なものと検証するように選定したことを特徴とするアクセス資格認証装置。

【請求項２】

少なくとも、上記第２の記憶手段と、上記証明データ生成手段とが、内部のデータ及び処理手続を外部から観測することを困難ならしめる防御手段中に保持されていることを特徴とする請求項１記載のアクセス資格認証装置。

【請求項３】

少なくとも、上記第２の記憶手段と、上記証明データ生成手段とが、ＩＣカードなどの携帯可能な小型演算装置として構成されていることを特徴とする請求項１記載のアクセス資格認証装置。

【請求項４】

上記第３の記憶手段に記憶される上記証明用補助情報が、上記アクセス資格認証の特徴情報および上記ユーザの固有情報から作成されることを特徴とする請求項１乃至３記載のアクセス資格認証装置。

【請求項５】

上記第３の記憶手段に記憶される上記証明用補助情報が、上記アクセス資格認証の特徴情報と、上記ユーザの固有情報と、上記アクセス資格認証の特徴情報に対応する公開情報とから作成されることを特徴とする請求項１乃至３記載のアクセス資格認証装置。

【請求項６】

上記第３の記憶手段に記憶される上記証明用補助情報ｔが、上記ユーザの固有情報ｅを、非衝突性関数の入力として計算した値と、上記アクセス資格認証の特徴情報とから作成されることを特徴とする請求項１乃至３記載のアクセス資格認証装置。

【請求項７】

上記第３の記憶手段に記憶される上記証明用補助情報ｔが、上記ユーザの固有情報ｅと、上記アクセス資格認証の特徴情報に対応する公開情報とを、非衝突性関数の入力として計算した値と、上記アクセス資格認証の特徴情報とから作成されることを特徴とする請求項１乃至３記載のアクセス資格認証装置。

【請求項８】

第２の認証用データを記憶する第４の記憶手段を有し、上記証明データ検証手段が持つ上記演算手段が、上記第４の記憶手段に記憶されている上記第２の認証用データを使用して演算を行なうことを特徴とする請求項１乃至７記載のアクセス資格認証装置。

【請求項９】

認証用素データを記憶する第５の記憶手段と、乱数生成手段が生成した乱数を記憶する第６の記憶手段とを備え、上記乱数生成手段は生成した乱数を上記第６の記憶手段に書き込むと共に、上記第５の記憶手段に記憶されている上記認証用素データに上記乱数を用いた乱数効果を施した後、上記認証用データとして上記第１の記憶手段に書き込むことを特徴とする請求項１乃至８記載のアクセス資格認証装置。

【請求項１０】

認証用素データを記憶する第５の記憶手段と、上記乱数生成手段が生成した乱数を記憶する第６の記憶手段とを備え、上記乱数生成手段は生成した乱数を上記第６の記憶手段に書き込むと共に、上記第５の記憶手段に記憶されている上記認証用素データに上記乱数を用いた乱数効果を施した値と、上記第４の記憶手段に記憶されている上記第２の認証用データもしくは上記第２の認証用データに対して上記乱数を用いた乱数効果を施した値の組とを、上記認証用データとして上記第１の記憶手段に書き込むことを特徴とする請求項１乃至８記載のアクセス資格認証装置。

【請求項１１】

上記証明データ検証手段は、上記第６の記憶手段に記憶されている上記乱数による乱数効果を、上記証明データ生成手段によって生成された上記証明データから除去することを特徴とする請求項９または１０記載のアクセス資格認証装置。

【請求項１２】

上記アクセス資格認証の特徴情報が暗号化関数の暗号化鍵であり、上記証明データ検証手段が乱数生成手段を備え、上記乱数生成手段は生成した乱数を上記認証用データとして上記第１の記憶手段に書き込み、上記演算手段による演算結果が、上記乱数である認証用データを上記アクセス資格認証の特徴情報である暗号化鍵で暗号化したものであることを検証することを特徴とする請求項１乃至または１１記載のアクセス資格認証装置。

【請求項１３】

上記アクセス資格認証の特徴情報が暗号関数における復号鍵であり、上記認証用データが適当なデータを上記復号鍵に対応する暗号化鍵を用いて暗号化したものであり、上記証明データ検証手段は、上記演算手段による演算結果が、上記認証用データを正しく復号したものであることを検証することを特徴とする請求項１乃至１１記載のアクセス資格認証装置。

【請求項１４】

上記暗号化関数が非対称鍵暗号関数であり、上記アクセス資格認証の特徴情報が鍵の一方であることを特徴とする請求項１２または１３記載のアクセス資格認証装置。

【請求項１５】

上記暗号化関数が公開鍵暗号関数であり、上記アクセス資格認証の特徴情報が秘密鍵であることを特徴とする請求項１４記載のアクセス資格認証装置。

【請求項１６】

上記暗号化関数が対称鍵暗号関数であり、上記アクセス資格認証の特徴情報が共通秘密鍵であることを特徴とする請求項１２または１３記載のアクセス資格認証装置。

【請求項１７】

上記暗号化関数が法ｎのもとでのＲＳＡ公開鍵暗号であり、上記アクセス資格認証の特徴情報が秘密鍵Ｄであり、上記秘密鍵Ｄに対応する公開鍵がＥであるとき、上記証明データ検証手段は、上記演算手段で、上記第５の記憶手段に記憶されている上記認証用データＣを上記法ｎのもとで上記証明用補助情報ｔでべき乗したものと、上記証明データ生成手段によって生成された上記証明データＲとの積を、上記法ｎのもとで上記公開鍵Ｅでべき乗し、その結果と、上記第５の記憶手段に記憶されている上記認証用データＣとが、上記法ｎのもとで合同であることを検証することを特徴とする請求項１２記載のアクセス資格認証装置。

【請求項１８】

上記暗号化関数が所定の法と指数のもとでのべき乗剰余演算であり、アクセス資格認証の特徴情報が該暗号化関数の復号鍵であるとき、上記第１の記憶手段に記憶される認証用データがデータＫを上記暗号化関数によって暗号化したものであり、上記証明データ検証手段は、上記演算手段で，上記法のもとで、上記第５の記憶手段に記憶されている認証用データＣを上記証明用補助情報ｔでべき乗したものと、上記証明データ生成手段によって生成された上記証明データＲの積を計算し、その結果と、上記Ｋとが上記法のもとで合同であることを検証することを特徴とする請求項１３記載のアクセス資格認証装置。

【請求項１９】

上記第２の認証用データが適当なデータを上記復号鍵に対応する暗号化鍵を用いて暗号化したものであり、上記証明データ検証手段は、上記演算手段で演算した結果が、アクセス資格認証の特徴情報である上記暗号鍵に対応する復号鍵によって、上記第２の認証用データを正しく復号したものであることを認証することを特徴とする請求項８、１０または１１記載のアクセス資格認証装置。

【請求項２０】

上記暗号関数が法ｐ，正整数ａ上での公開鍵暗合であり、アクセス資格認証の特徴情報が秘密鍵Ｘであり、秘密鍵Ｘに対応する公開鍵がＹであり（$Y = a^{X} \mod p$）、ｕが上記ａを法ｐのもとで適当な乱数ｚを指数としてべき乗した値であり、Ｃが、上記Ｙを法ｐのもとで上記乱数ｚを指数としてべき乗した数と、データＫとの間に所定の演算を施したものであるとき、上記第１の記憶手段に認証用データとしてｕが記憶され、上記第４の記憶手段にはＣが記憶され、上記証明データ検証手段は、上記演算手段で，法ｐのもとで

、上記ｕを証明用補助情報ｔでべき乗した値と，上記証明データ生成手段によって生成された証明データＲと、を乗じた値Ｒ’を生成し、上記第４の記憶手段に記憶されているＣと上記Ｒ’に所定の演算を施し，その結果と、上記Ｋとが法ｐのもとで合同であることを検証することを特徴とする請求項１３または１９記載のアクセス資格認証装置。

【請求項２１】

上記暗号化関数が法ｐ、正整数ａのもとでの公開鍵暗号であり、アクセス資格認証の特徴情報が一方の鍵Ｘであり、鍵Ｘに対応する公開鍵がＹであり（$Y = a^X \mod p$）、ｕが上記ａを法ｐのもとで適当な乱数ｚを指数としてべき乗した値であり、Ｃが、上記Ｙを法ｐのもとで上記乱数ｚを指数としてべき乗した数と、データＫとの積である時（$C = Y^z K \mod p$）、上記第５の記憶手段に認証用素データとしてｕが記憶され、上記第４の記憶手段にはＣが記憶され、上記第１の記憶手段に認証用データとしてｕとＣの組が記憶され、上記証明データ検証手段は、上記演算手段で，法ｐのもとで、上記証明データ生成手段によって生成された証明データＲを、上記ｕを証明用補助情報でｔ乗した値で割った値を計算し、その結果と、上記Ｒ’と、上記Ｋとが法ｐのもとで合同であることを検証することを特徴とする請求項１３または１９記載のアクセス資格認証装置。

【請求項２２】

上記第３の記憶手段に記憶される証明用補助情報ｔが、アクセス資格認証の特徴情報から、上記ユーザの固有情報ｅを減じたデータであり、上記証明データ生成手段は、上記ｅと、上記第１の記憶手段に書き込まれた認証用データＣとから、上記アクセス資格認証の特徴情報に対応する法数のもとでＣのｅ乗を計算することを特徴とする請求項１７乃至２１記載のアクセス資格認証装置。

【請求項２３】

上記第３の記憶手段に記憶される証明用補助情報ｔが、アクセス資格認証の特徴情報から、上記ユーザの固有情報ｅと、上記アクセス資格認証の特徴情報に対応する公開情報とに所定の演算を施して生成した正整数ｆを減じたデータであり、上記証明データ生成手段は、上記ｅと、上記第１の記憶手段に書き込まれた認証用データＣとから、上記アクセス資格認証の特徴情報に対応する法数のもとでＣのｆ乗を計算することを特徴とする請求項１７乃至２１記載のアクセス資格認証装置。

【請求項２４】

少なくとも上記第１の記憶手段と、上記第２の記憶手段と、上記証明データ生成手段とから構成される証明データ生成装置と、

少なくとも上記証明データ検証手段を有し、さらに上記第３の記憶手段と、認証用データを記憶する第７の記憶手段と、証明データを記憶する第８の記憶手段を備えた証明データ検証装置とが、

互いに通信することによりユーザのアクセス資格を認証するアクセス資格認証装置において、

上記証明データ検証装置は、上記第７の記憶手段に記憶されている認証用データを上記証明データ生成装置の上記第１の記憶手段に書き出し、

上記証明データ生成装置は、上記証明データ生成手段によって上記第１の記憶手段に書き込まれた上記認証用データをもとに生成した証明データを、上記証明データ検証装置中の上記第８の記憶手段に書き出し、

上記証明データ検証装置は上記第８の記憶手段に書き込まれた上記証明データを用いてユーザのアクセス資格を認証することを特徴する請求項１乃至２３記載のアクセス資格認証装置。

【請求項２５】

ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証装置において、

認証用データを記憶する第１の記憶手段と、

ユーザの固有情報を記憶する第２の記憶手段と、

上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、証明用補助情報を生成

するために予め定められた第１の所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、
上記第１の記憶手段に保持されている上記認証用データと、上記第３の記憶手段に保持されている上記証明用補助情報とに証明データを生成するために予め定められた第２の所定の計算を実行して証明データを生成する証明データ生成手段と、
上記証明データが上記証明用補助情報に基づいて生成されていることを検証する証明データ検証手段であって、上記証明データ生成手段によって生成された証明データと、上記第２の記憶手段に保持されている上記ユーザの固有情報とに検証用に予め定められた第３の所定の計算を実行する演算手段を有し、該演算手段の計算結果を使用して検証を行なう、上記証明データ検証手段とを有し、
　上記証明用補助情報を生成するために予め定められた第１の所定の計算と、上記証明データを生成するために予め定められた第２の所定の計算と、上記検証用に予め定められた第３の所定の計算とを、上記ユーザの固有情報、上記アクセス資格の特徴情報および上記証明用補助情報が対応する場合に上記証明データ検証手段が上記証明データを正当なものと検証するように選定したことを特徴とするアクセス資格認証装置。
【請求項２６】
上記第３の記憶手段に記憶される上記証明用補助情報が、上記アクセス資格認証の特徴情報および上記ユーザの固有情報から作成されることを特徴とする請求項２５記載のアクセス資格認証装置。
【請求項２７】
上記第３の記憶手段に記憶される上記証明用補助情報が、上記アクセス資格認証の特徴情報と、上記ユーザの固有情報と、上記アクセス資格認証の特徴情報に対応する公開情報とから作成されることを特徴とする請求項２５のアクセス資格認証装置。
【請求項２８】
上記第３の記憶手段に記憶される上記証明用補助情報ｔが、上記ユーザの固有情報ｅを、非衝突性関数の入力として計算した値と、上記アクセス資格認証の特徴情報とから作成されることを特徴とする請求項２５記載のアクセス資格認証装置。
【請求項２９】
上記第３の記憶手段に記憶される上記証明用補助情報ｔが、上記ユーザの固有情報ｅと、上記アクセス資格認証の特徴情報に対応する公開情報とを、非衝突性関数の入力として計算した値と、上記アクセス資格認証の特徴情報とから作成されることを特徴とする請求項２５記載のアクセス資格認証装置。
【請求項３０】
第２の認証用データを記憶する第４の記憶手段を有し、
上記証明データ検証手段が持つ演算手段が、さらに上記第４の記憶手段に記憶されている上記第２の認証用データを使用して演算を行なうことを特徴とする請求項２５乃至２９記載のアクセス資格認証装置。
【請求項３１】
認証用素データを記憶する第５の記憶手段と、乱数生成手段が生成した乱数を記憶する第６の記憶手段とを備え、上記乱数生成手段は生成した乱数を上記第６の記憶手段に書き込むと共に、上記第５の記憶手段に記憶されている上記認証用素データに上記乱数を用いた乱数効果を施した後、上記認証用データとして上記第１の記憶手段に書き込むことを特徴とする請求項２５乃至３０記載のアクセス資格認証装置。
【請求項３２】
認証用素データを記憶する第５の記憶手段と、上記乱数生成手段が生成した乱数を記憶する第６の記憶手段とを備え、上記乱数生成手段は生成した乱数を上記第６の記憶手段に書き込むと共に、上記第５の記憶手段に記憶されている認証用素データに上記乱数を用いた乱数効果を施した値と、上記第４の記憶手段に記憶されている上記第２の認証用データもしくは上記第２の認証用データに対して上記乱数を用いた乱数効果を施した値の組とを、上記認証用データとして上記第１の記憶手段に書き込むことを特徴とする請求項２５乃至

３１記載のアクセス資格認証装置。
【請求項３３】
上記証明データ検証手段は、上記第６の記憶手段に記憶されている乱数による乱数効果を、上記証明データ生成手段によって生成された上記証明データから除去することを特徴とする請求項３１または３２記載のアクセス資格認証装置。
【請求項３４】
上記アクセス資格認証の特徴情報が暗号化関数の暗号化鍵であり、上記証明データ検証手段が乱数生成手段を備え、上記乱数生成手段は生成した乱数を上記認証用データとして上記第１の記憶手段に書き込み、上記演算手段による演算結果が、上記乱数である認証用データを上記アクセス資格認証の特徴情報である暗号化鍵で暗号化したものであることを検証することを特徴とする請求項２５乃至３３記載のアクセス資格認証装置。
【請求項３５】
上記アクセス資格認証の特徴情報が暗号関数における復号鍵であり、上記認証用データが適当なデータを上記復号鍵に対応する暗号化鍵を用いて暗号化したものであり、上記証明データ検証手段は、上記演算手段による演算結果が、上記認証用データを正しく復号したものであることを検証することを特徴とする請求項２５乃至３３記載のアクセス資格認証装置。
【請求項３６】
上記暗号化関数が非対称鍵暗号関数であり、上記アクセス資格認証の特徴情報が鍵の一方であることを特徴とする請求項３４または３５記載のアクセス資格認証装置。
【請求項３７】
上記暗号化関数が公開鍵暗号関数であり、上記アクセス資格認証の特徴情報が秘密鍵であることを特徴とする請求項３６記載のアクセス資格認証装置。
【請求項３８】
上記暗号化関数が対称鍵暗号関数であり、上記アクセス資格認証の特徴情報が共通秘密鍵であることを特徴とする請求項３４または３５記載のアクセス資格認証装置。
【請求項３９】
上記第２の認証用データが適当なデータを上記復号鍵に対応する暗号化鍵を用いて暗号化したものであり、上記証明データ検証手段は、上記演算手段で演算した結果が、アクセス資格認証の特徴情報である上記暗号鍵に対応する復号鍵によって、上記第２の認証用データを正しく復号したものであることを認証することを特徴とする請求項３０、３２または３３記載のアクセス資格認証装置。
【請求項４０】
上記暗号化関数が法ｎのもとでのＲＳＡ公開鍵暗号であり、アクセス資格認証の特徴情報が秘密鍵Ｄであり、秘密鍵Ｄに対応する公開鍵がＥであるとき、上記証明データ検証手段は、上記演算手段で、上記第５の記憶手段に記憶されている認証用データＣを法ｎのもとで上記ユーザの固有情報ｅに所定の演算を施して生成した正整数ｆでべき乗した値Ｃ’を計算し、上記Ｃ’と上記公開鍵Ｅと上記証明データ生成手段によって生成された証明データＲとの積を，法ｎのもとで上記公開鍵Ｅ乗を行い，その結果と、上記第５の記憶手段に記憶されている認証用データＣとが、法ｎのもとで合同であること（$R^{E}C'^{E}$　ｍｏｄ　ｎ＝Ｃ　ｍｏｄ　ｎ）を検証することを特徴とする請求項３４記載のアクセス資格認証装置。
【請求項４１】
上記暗号化関数が法ｎのもとでのＲＳＡ公開鍵暗号であり、所定の法と指数のもとでの巾乗剰余演算であり，アクセス資格認証の特徴情報が該暗号化関数の復号鍵であるとき、上記第１の記憶手段に記憶される認証用データがデータＫを上記暗号化関数によって暗号化したものであり、上記証明データ検証手段は、上記演算手段で、上記法のもとで、上記第５の記憶手段に記憶されている認証用データＣを、上記ユーザの固有情報ｅに所定の演算を施して生成した正整数ｆでべき乗したものと、上記証明データ生成手段によって生成された証明データＲの積を計算し，その結果と、上記Ｋとが法ｎのもとで合同であることを

検証することを特徴とする請求項３５記載のアクセス資格認証装置。
【請求項４２】
上記暗号化関数が法ｐ、正整数ａ上での公開鍵暗号であり、アクセス資格認証の特徴情報が一方の鍵Ｘであり、鍵Ｘに対応する公開鍵がＹであり（$Y = a^X \mod p$）、ｕが上記ａを法ｐのもとで適当な乱数ｚを指数としてべき乗した値であり、Ｃが、上記Ｙを法ｐのもとで上記乱数ｚを指数としてべき乗した数と、データＫとの間に所定の演算を施したものであるとき、上記第１の記憶手段に認証用データとしてｕが記憶され、上記第４の記憶手段にはＣが記憶され、上記証明データ検証手段は、上記演算手段で，法ｐのもとで、上記ｕを上記ユーザの固有情報ｅに所定の演算を施して生成した正整数ｆでべき乗した値と、上記証明データ生成手段によって生成された証明データＲとを乗じた値Ｒ’を生成し、上記第４の記憶手段に記憶されているＣと上記Ｒ’に所定の演算を施し，その結果と、上記Ｋとが法ｐのもとで合同であることを検証することを特徴とする請求項３５または３９記載のアクセス資格認証装置。
【請求項４３】
上記暗号化関数が法ｐ、正整数ａのもとでの公開鍵暗号であり、アクセス資格認証の特徴情報が一方の鍵Ｘであり、鍵Ｘに対応する公開鍵がＹであり（$Y = a^X \mod p$）、ｕが上記ａを法ｐのもとで適当な乱数ｚを指数としてべき乗した値であり、Ｃが、上記Ｙを法ｐのもとで上記乱数ｚを指数としてべき乗した数と、データＫとの積である時（$C = Y^z K \mod p$）、上記第５の記憶手段に認証用素データとしてｕが記憶され、上記第４の記憶手段にはＣが記憶され、上記第１の記憶手段に認証用データとしてｕとＣの組が記憶され、上記証明データ検証手段は、上記演算手段で，法ｐのもとで、上記証明データ生成手段によって生成された証明データＲを、上記ｕを上記ユーザの固有情報ｅに所定の演算を施して生成した正整数ｆでべき乗した値で割った値を計算し、その結果と，上記Ｒ’と、上記Ｋとが法ｐのもとで合同であることを検証することを特徴とする請求項３５または３９記載のアクセス資格認証装置。
【請求項４４】
上記証明データ生成手段は、上記ｅと、上記第３の記憶手段に記憶される証明用補助情報ｔと上記第１の記憶手段に書き込まれた認証用データＣとから、上記アクセス資格認証の特徴情報に対応する法数のもとでＣのｔ乗を計算することを特徴とする請求項３９、４０または４３記載のアクセス資格認証装置。
【請求項４５】
少なくとも上記第１の記憶手段と、上記第３の記憶手段と、上記証明データ生成手段とから構成される証明データ生成装置と、
少なくとも上記証明データ検証手段を有し、さらに上記第２の記憶手段と、認証用データを記憶する第７の記憶手段と、証明データを記憶する第８の記憶手段を備えた証明データ検証装置とが、
互いに通信することによりユーザのアクセス資格を認証するアクセス資格認証装置において、
上記証明データ検証装置は、上記第７の記憶手段に記憶されている上記認証用データを上記証明データ生成装置の上記第１の記憶手段に書き出し、
上記証明データ生成装置は、上記証明データ生成手段によって上記第１の記憶手段に書き込まれた上記認証用データをもとに生成した証明データを、上記証明データ検証装置中の上記第８の記憶手段に書き出し、
上記証明データ検証装置は上記第８の記憶手段に書き込まれた上記証明データを用いてユーザのアクセス資格を認証することを特徴する請求項２５乃至４４記載のアクセス資格認証装置。
【請求項４６】
上記証明データ検証手段は、暗号化されたデータである上記認証用データあるいは上記認証用素データに対応する平文データを記憶する第９の記憶手段と、比較手段とを有し、上記比較手段は、上記証明データ生成手段が生成した上記証明データに所定の演算を施した

結果と、上記第９の記憶手段に記憶されている平文データを比較し、両者が一致した場合に限り、上記証明データが正当であると判断することを特徴とする請求項１乃至４５記載のアクセス資格認証装置。

【請求項４７】

上記証明データ検証手段は、データの冗長性を検証する冗長性検証手段を有し、上記証明データ生成手段が生成した上記証明データの値、もしくは上記証明データを用いて演算を行った結果得られた値が、冗長性検証手段によって特定の冗長性を持つことが確認されることによって、上記証明データが正当であると判断することを特徴とする請求項１乃至４５記載のアクセス資格認証装置。

【請求項４８】

上記証明データ検証手段は、暗号化されたデータである上記認証用データあるいは上記認証用素データに対応する平文データに所定の一方向性関数を施した結果を記憶する第１０の記憶手段と、上記一方向性関数を実行する一方向関数値生成手段と、上記比較手段とを有し、一方向関数値生成手段は、上記データ生成手段が生成した上記証明データに所定の演算を施した後、一方向関数を施し、上記比較手段は、上記一方向関数を施した結果と、上記第１０の記憶手段に記憶されているデータを比較し、両者が一致した場合に限り、上記証明データが正当であると判断することを特徴とする請求項１乃至４５記載のアクセス資格認証装置。

【請求項４９】

上記証明データ検証手段は、プログラム実行手段を含み、上記認証用データあるいは上記認証用素データは、プログラムを暗号化して得られるデータであり、上記証明データ検証手段が、証明データ生成手段が生成した上記証明データに所定の演算を施した値を、プログラムの一部もしくは全部としてプログラム実行手段に引き渡すことにより、証明データ生成手段が、暗号化されたプログラムである上記認証用データあるいは認証用素データを正しく復号した場合、すなわち、暗号化されたプログラムが正しく復号された場合に限り、プログラム実行手段が正しい動作を行うことを特徴とする請求項１乃至３２記載のアクセス資格認証装置。

【請求項５０】

上記証明データ検証手段は、さらに、プログラム実行手段と、プログラム記憶手段と、プログラム復号手段とを含み、プログラム記憶手段に記憶されているプログラムは、その一部あるいは全部が暗号化されたものであり、上記認証用データあるいは認証用素データは、上記暗号化されたプログラムを復号するための復号鍵を別途暗号化して得られるデータであり、上記証明データ検証手段は、上記証明データ生成手段が生成した上記証明データを上記プログラム復号手段に引き渡し、上記プログラム復号手段は、上記証明データ生成手段が生成した証明データと、上記証明用補助情報とに所定の演算を施した結果得られた値を復号鍵として、上記プログラム記憶手段に記憶されたプログラムの一部もしくは全部を復号し、上記プログラム実行手段が復号されたプログラムを実行することにより、上記証明データ生成手段が上記認証用データあるいは認証用素データを正しく復号した場合、すなわち、暗号化されたプログラムを復号するために復号鍵が正しく復号された場合に限り、プログラム実行手段が正しい動作を行うことを特徴とする請求項１乃至４５記載のアクセス資格認証装置。

【請求項５１】

ユーザのアクセス資格を認証するアクセス資格認証装置において、

認証用データを記憶する第１の記憶手段と、

ユーザの固有情報を記憶する第２の記憶手段と、

上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、証明用補助情報を生成するために予め定められた第１の所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、

上記第１の記憶手段に記憶されている上記認証用データと、上記第２の記憶手段に記憶されている上記ユーザの固有情報と、上記第３の記憶手段に記憶されている上記証明用補助

情報とから、上記証明用補助情報と上記ユーザの固有情報との組が、上記アクセス資格認証の特徴情報に対して正しく対応するものであることを所定の演算手段による、検証用に予め定められた第３の所定の計算により検証する検証手段とを有し、

上記証明用補助情報を生成するために予め定められた第１の所定の計算と、上記検証用に予め定められた第３の所定の計算とを、上記ユーザの固有情報、上記アクセス資格の特徴情報および上記証明用補助情報が対応する場合に上記検証手段が上記証明用補助情報と上記ユーザの固有情報との組が正当なものと検証するように選定したことを特徴とするアクセス資格認証装置。

【請求項５２】

上記第３の記憶手段に記憶される上記証明用補助情報が、上記アクセス資格認証の特徴情報および上記ユーザの固有情報から作成されることを特徴とする請求項５１記載のアクセス資格認証装置。

【請求項５３】

上記第３の記憶手段に記憶される上記証明用補助情報が、上記アクセス資格認証の特徴情報と、上記ユーザの固有情報と、上記アクセス資格認証の特徴情報に対応する公開情報とから作成されることを特徴とする請求項５１記載のアクセス資格認証装置。

【請求項５４】

上記第３の記憶手段に記憶される上記証明用補助情報ｔが、上記ユーザの固有情報ｅを、非衝突性関数の入力として計算した値と、上記アクセス資格認証の特徴情報とから作成されることを特徴とする請求項５１記載のアクセス資格認証装置。

【請求項５５】

上記第３の記憶手段に記憶される上記証明用補助情報ｔが、上記ユーザの固有情報ｅと、上記アクセス資格認証の特徴情報に対応する公開情報とを、非衝突性関数の入力として計算した値と、上記アクセス資格認証の特徴情報とから作成されることを特徴とする請求項５２記載のアクセス資格認証装置。

【請求項５６】

第２の認証用データを記憶する第４の記憶手段を有し、

上記所定の演算手段が、さらに上記第４の記憶手段に記憶されている上記第２の認証用データを使用して演算を行なうことを特徴とする請求項５１記載のアクセス資格認証装置。

【請求項５７】

第１の記憶手段、第２の記憶手段、第３の記憶手段、証明データ生成手段および証明データ検証手段を用いユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証方法において、

上記第１の記憶手段に認証用データを記憶する第１の記憶ステップと、

上記第２の記憶手段にユーザの固有情報を記憶する第２の記憶ステップと、

上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、証明用補助情報を生成するために予め定められた第１の所定の計算を実行した実行結果である証明用補助情報を上記第３の記憶手段に記憶する第３の記憶ステップと、

上記第１の記憶手段に保持されている上記認証用データと、上記第２の記憶手段に保持されている上記ユーザの固有情報とに、上記証明データ生成手段により、証明データを生成するために予め定められた第２の所定の計算を実行して証明データを生成する証明データ生成ステップと、

上記証明データ生成手段によって生成された証明データと、上記第３の記憶手段に保持されている上記証明用補助情報とに、上記証明データ検証手段の演算手段により、検証用に予め定められた第３の所定の計算を実行し、上記証明データが上記ユーザの固有情報に基づいて生成されていることを検証するステップとを有し、

上記証明用補助情報を生成するために予め定められた第１の所定の計算と、上記証明データを生成するために予め定められた第２の所定の計算と、上記検証用に予め定められた第３の所定の計算とを、上記ユーザの固有情報、上記アクセス資格の特徴情報および上記

証明用補助情報が対応する場合に上記証明データ検証装手段が上記証明データを正当なものと検証するように選定したことを特徴とするアクセス資格認証方法。

【請求項５８】

第１の記憶手段、第２の記憶手段、第３の記憶手段、証明データ生成手段および証明データ検証手段を用いユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証方法において、

上記第１の記憶手段に認証用データを記憶する第１の記憶ステップと、

上記第２の記憶手段にユーザの固有情報を記憶する第２の記憶ステップと、

上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、証明用補助情報を生成するために予め定められた第１の所定の計算を実行した実行結果である証明用補助情報を、上記第３の記憶手段に記憶する第３の記憶ステップと、

上記第１の記憶手段に保持されている上記認証用データと、上記第３の記憶手段に保持されている上記証明用補助情報とに、上記証明データ生成手段により、証明データを生成するために予め定められた第２の所定の計算を実行して証明データを生成する証明データ生成ステップと、

上記証明データ生成手段によって生成された証明データと、上記第２の記憶手段に保持されている上記ユーザの固有情報とに、上記証明データ検証手段の演算手段により、検証用に予め定められた第３の所定の計算を実行し、上記証明データが上記証明用補助情報に基づいて生成されていることを検証する証明データ検証ステップとを有し、

上記証明用補助情報を生成するために予め定められた第１の所定の計算と、上記証明データを生成するために予め定められた第２の所定の計算と、上記検証用に予め定められた第３の所定の計算とを、上記ユーザの固有情報、上記アクセス資格の特徴情報および上記証明用補助情報が対応する場合に上記証明データ検証装手段が上記証明データを正当なものと検証するように選定したことを特徴とするアクセス資格認証方法。

【請求項５９】

第１の記憶手段、第２の記憶手段、第３の記憶手段および演算手段を用いユーザのアクセス資格を認証するアクセス資格認証方法において、

第１の記憶手段に認証用データを記憶する第１の記憶ステップと、

第２の記憶手段にユーザの固有情報を記憶する第２の記憶ステップと、

上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、証明用補助情報を生成するために予め定められた第１の所定の計算を実行した実行結果である証明用補助情報を、上記第３の記憶手段に記憶する第３の記憶ステップと、

上記第１の記憶手段に記憶されている上記認証用データと、上記第２の記憶手段に記憶されている上記ユーザの固有情報と、上記第３の記憶手段に記憶されている上記証明用補助情報とから、上記証明用補助情報と上記ユーザの固有情報との組が、上記アクセス資格認証の特徴情報に対して正しく対応するものであることを所定の演算手段よる、検証用に予め定められた第３の所定の計算により検証する検証ステップとを有し、

上記証明用補助情報を生成するために予め定められた第１の所定の計算と、上記検証用に予め定められた第３の所定の計算とを、上記ユーザの固有情報、上記アクセス資格の特徴情報および上記証明用補助情報が対応する場合に上記検証手段が上記証明用補助情報と上記ユーザの固有情報との組が正当なものと検証するように選定したことを特徴とするアクセス資格認証方法。

【請求項６０】

第１の記憶手段、第２の記憶手段、第３の記憶手段、証明データ生成手段および証明データ検証手段を用いユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証用コンピュータプログラムを記録した記録媒体において、

上記第１の記憶手段に認証用データを記憶する第１の記憶ステップと、

上記第２の記憶手段にユーザの固有情報を記憶する第２の記憶ステップと、

上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、証明用補助情報を生成するために予め定められた第１の所定の計算を実行した実行結果である証明用補助情報を上記第３の記憶手段に記憶する第３の記憶ステップと、
上記第１の記憶手段に保持されている上記認証用データと、上記第２の記憶手段に保持されている上記ユーザの固有情報とに、上記証明データ生成手段により、証明データを生成するために予め定められた第２の所定の計算を実行して証明データを生成する証明データ生成ステップと、
上記証明データ生成手段によって生成された証明データと、上記第３の記憶手段に保持されている上記証明用補助情報とに、上記検証手段の演算手段により、検証用に予め定められた第３の所定の計算を実行し、上記証明データが上記ユーザの固有情報に基づいて生成されていることを検証するステップとをコンピュータに実行させるために用いられ、
さらに、上記証明用補助情報を生成するために予め定められた第１の所定の計算と、上記証明データを生成するために予め定められた第２の所定の計算と、上記検証用に予め定められた第３の所定の計算とを、上記ユーザの固有情報、上記アクセス資格の特徴情報および上記証明用補助情報が対応する場合に上記証明データ検証装手段が上記証明データを正当なものと検証するように選定したコンピュータプログラムをコンピュータに読み出し可能に記録したことを特徴とするアクセス資格認証用コンピュータプログラムを記録した記録媒体。

【請求項６１】

第１の記憶手段、第２の記憶手段、第３の記憶手段、証明データ生成手段および証明データ検証手段を用いユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証用コンピュータプログラムを記録した記録媒体において、
上記第１の記憶手段に認証用データを記憶する第１の記憶ステップと、
上記第２の記憶手段にユーザの固有情報を記憶する第２の記憶ステップと、
上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、証明用補助情報を生成するために予め定められた第１の所定の計算を実行した実行結果である証明用補助情報を、上記第３の記憶手段に記憶する第３の記憶ステップと、
上記第１の記憶手段に保持されている上記認証用データと、上記第３の記憶手段に保持されている上記証明用補助情報とに、上記証明データ生成手段により、証明データを生成するために予め定められた第２の所定の計算を実行して証明データを生成する証明データ生成ステップと、
上記証明データ生成手段によって生成された証明データと、上記第２の記憶手段に保持されている上記ユーザの固有情報とに、上記証明データ検証手段の演算手段により、検証用に予め定められた第３の所定の計算を実行し、上記証明データが上記証明用補助情報に基づいて生成されていることを検証する証明データ検証ステップとをコンピュータに実行させるために用いられ、
さらに、上記証明用補助情報を生成するために予め定められた第１の所定の計算と、上記証明データを生成するために予め定められた第２の所定の計算と、上記検証用に予め定められた第３の所定の計算とを、上記ユーザの固有情報、上記アクセス資格の特徴情報および上記証明用補助情報が対応する場合に上記証明データ検証装手段が上記証明データを正当なものと検証するように選定したコンピュータプログラムをコンピュータに読み出し可能に記録したことを特徴とするアクセス資格認証用コンピュータプログラムを記録した記録媒体。

【請求項６２】

第１の記憶手段、第２の記憶手段、第３の記憶手段および演算手段を用いユーザのアクセス資格を認証するアクセス資格認証用コンピュータプログラムを記録した記録媒体において、
第１の記憶手段に認証用データを記憶する第１の記憶ステップと、
第２の記憶手段にユーザの固有情報を記憶する第２の記憶ステップと、

上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、証明用補助情報を生成するために予め定められた第１の所定の計算を実行した実行結果である証明用補助情報を、上記第３の記憶手段に記憶する第３の記憶ステップと、
上記第１の記憶手段に記憶されている上記認証用データと、上記第２の記憶手段に記憶されている上記ユーザの固有情報と、上記第３の記憶手段に記憶されている上記証明用補助情報とから、上記証明用補助情報と上記ユーザの固有情報との組が、上記アクセス資格認証の特徴情報に対して正しく対応するものであることを所定の演算手段による、検証用に予め定められた第３の所定の計算により検証する検証ステップとをコンピュータに実行させるために用いられ、
さらに、上記証明用補助情報を生成するために予め定められた第１の所定の計算と、上記検証用に予め定められた第３の所定の計算とを、上記ユーザの固有情報、上記アクセス資格の特徴情報および上記証明用補助情報が対応する場合に上記検証手段が上記証明用補助情報と上記ユーザの固有情報との組が正当なものと検証するように選定したコンピュータプログラムをコンピュータに読み出し可能に記録したことを特徴とするアクセス資格認証用コンピュータプログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明はユーザのアクセス資格を認証するアクセス資格認証装置に関する。

【０００２】

【従来技術】

本発明と同分野に属する先行技術としてプログラムの実行制御技術が知られている。プログラム実行制御技術は、
▲１▼アプリケーションプログラム中にユーザ認証のためのルーチンを埋め込み、
▲２▼該ルーチンはアプリケーションの実行を試みているユーザが正規の認証用の鍵を保有していることを検査し、
▲３▼前記認証用の鍵の存在が確認された場合に限りプログラムを続行し、それ以外の場合にはプログラムの実行を停止する
技術である。

【０００３】

当技術を利用することにより、認証鍵を保有する正規のユーザにのみアプリケーションプログラムの実行を可能ならしめることが出来る。当技術はソフトウェア頒布事業において実用化されており、製品として、例えばＲａｉｎｂｏｗ Ｔｅｃｈｎｏｌｏｇｉｅｓ，Ｉｎｃ．社のＳｅｎｔｉｎｅｌＳｕｐｅｒＰｒｏ（商標）や、Ａｌａｄｄｉｎ Ｋｎｏｗｌｅｄｇｅ Ｓｙｓｔｅｍｓ Ｌｔｄ．社のＨＡＳＰ（商標）等がある。

【０００４】

以下にプログラム実行制御技術について、より詳細に説明する。

【０００５】

▲１▼ソフトウェアの実行を行うユーザはユーザ識別情報として認証鍵を保有する。認証鍵は暗号化のための鍵であり、ソフトウェアの利用を許可する者、例えばソフトウェアベンダがユーザに配布する。認証鍵は複製を防ぐためにハードウェア中のメモリ等に厳重に封入され、郵便等の物理的手段を用いてユーザに配送される。
▲２▼ユーザは認証鍵を内蔵したハードウェアを指定された方法で所有のパソコン・ワークステーションに装着する。ハードウェアは、例えばプリンタポートに装着される。
▲３▼ユーザがアプリケーションプログラムを起動し、プログラムの実行が前記ユーザ認証ルーチンに及ぶと、プログラムはユーザの認証鍵を内蔵したハードウェアと通信する。通信の結果に基づいてプログラムは認証鍵を識別し、正しい認証鍵の存在が確認されると次のステップへ実行を移す。通信が失敗し認証鍵の存在が確認できない場合は、プログラムは自らを停止し以降の実行ができないようにする。

【０００６】

アクセス資格認証ルーチンによる認証鍵の識別は、例えば、次のようなプロトコルに従って行われる。
▲１▼アクセス資格認証ルーチンは適当な数を生成し鍵内蔵ハードウェアに送信する。
▲２▼鍵内蔵ハードウェアは内蔵する認証鍵を用いて送られた数を暗号化し、前記認証ルーチンに返信する。
▲３▼認証ルーチンは、返信された数が予め予想された数、即ちハードウェアに送信した数を正しい認証鍵で暗号化して得られる数であるか否かを判定する。
▲４▼返信された数が予想された数と一致する場合にはプログラムの実行を続行し、一致しない場合には停止する。
【０００７】
この際、アプリケーションプログラムと認証鍵内蔵ハードウェア間の通信は、たとえ同じアプリケーションプログラム中の同じ箇所において同じハードウェアとの間で交換されるものであろうとも、実行のたびに異ならなければならない。さもなければ、正常な実行過程における通信内容を一度記録し、以後プログラムを実行する度に記録した通りにアプリケーションプログラムへの返信を行うことにより、正しい認証鍵を保有しないユーザでもプログラムを実行することが可能となってしまう。このような通信内容の再現によるアプリケーションプログラムの不正実行をリプレイアタック（ｒｅｐｌａｙ　ａｔｔａｃｋ）と呼ぶ。
【０００８】
リプレイアタックを防ぐために、通常、鍵内蔵ハードウェアに送られる数は通信の度に新たに生成される乱数を用いる。
【０００９】
［従来技術の問題点］
従来技術の問題点は、アプリケーションプログラムを作成する際に、プログラム作成者がユーザが持つ認証鍵を予め想定した上で、該認証鍵に基づいてプログラムの保護処理を行わなければならないという性質に由来する。
【００１０】
つまり、プログラム作成者は、鍵内蔵ハードウェアからの正しい返信をプログラム作成時に予測して、正しい返信を受けた場合にのみプログラムが正常に実行されるようにプログラムの作成を行わなければならない。
【００１１】
上記特徴を有する従来技術の利用形態は基本的に２通りとなるが、いずれの場合も以下に述べる問題を有する。
▲１▼第一の方法ではユーザの認証鍵をユーザ毎に異なるように用意する。即ち、ユーザ甲には認証鍵甲、ユーザ乙には認証鍵乙というように、ユーザ毎に異なる認証鍵を一つずつ用意する。
【００１２】
この場合、プログラム作成者は、プログラム中の認証ルーチンをユーザ毎に適切に変えてプログラムを作成する必要がある。つまり、ユーザ毎に認証鍵が異なるので、プログラム中の認証ルーチンは該プログラムを利用するユーザ固有の認証鍵を識別するように作成されなければならず、プログラム作成者は利用ユーザの数だけ異なるプログラムを作成する必要がある。
【００１３】
対象となるユーザが多数の場合、プログラムをユーザ毎に個別化する作業はプログラム作成者にとって耐えがたい労力を要求し、管理しなければならないユーザ認証鍵のリストも膨大なものとなる。
【００１４】
▲２▼第二の方法では、プログラム作成者はアプリケーション毎にそれぞれ異なる認証鍵を用意する。即ち、アプリケーション甲には認証鍵甲、アプリケーション乙には認証鍵乙というように、アプリケーション毎に異なる認証鍵を一つずつ用意し、固有の認証鍵を識

別するように各アプリケーションプログラムを作成する。
【００１５】
この方法では、第一の方法の場合のようにユーザ毎にプログラムを個別的に作成する必要は無くなるが、逆に、ユーザは利用するアプリケーションの数だけ認証鍵を保持しなければならないこととなる。
【００１６】
この制約はプログラム作成者及びユーザそれぞれに以下のような問題を惹起する。
【００１７】
前述のように、認証鍵はハードウェアに厳重に封入した状態でユーザに配布する必要がある。従って、プログラム自身はネットワークを介して簡便に配布することができるのと対照的に、認証鍵を内蔵するハードウェアの配布は郵便等の物理手段に頼らざるを得ない。この制限は、コスト、時間、梱包の手間いずれをとっても、プログラム作成者とって大きな負担となる。
【００１８】
プログラム作成者は、ユーザの要求に応えるべく、アプリケーション毎に異なるハードウェアを一定個数ストックしておかなければならず、在庫管理のコストを必要とする。
【００１９】
また、ユーザは利用するアプリケーションを変更する度にハードウェアを交換しなければならないという煩雑さに甘んじなければならない。
【００２０】
ユーザがあるアプリケーションを使いたいとしても、認証鍵が封入されたハードウェアが届くまで待たねばならず、即座に利用できないという点での不便さも生ずる。
【００２１】
この負担を軽減するため、ハードウェア中に複数の認証鍵を予め封入しておき、新しいアプリケーションの利用をユーザに許可する度に、ハードウェア中の未使用の認証鍵を利用可能とするためのパスワードをユーザに教えるといった方法が用いられる。しかしながら、この方法を用いたとしても、前記の問題点は原理的に解決されないことは明らかである。実際、商品化に際しては、上記問題点に起因する不便さを緩和するために、ハードウェアは連接して複数結合することが可能となるように設計される。
【００２２】
このように、上記二つのいずれの方法をとったとしても、プログラム作成者及びユーザの利便に問題が存在する。
【００２３】
なお、実行制御の外的な特質を考えると、メールのプライバシー保護やファイルや計算機資源のアクセス制御、その他一般のデジタルコンテンツアクセス制御にも適用可能であると想像できる。しかしながら、従来技術をこれらの分野に適用しようとしても、前記の問題点により不可能である。
【００２４】
【発明が解決しようとする課題】
本発明は、以上の事情を考慮してなされたものであり、ユーザ側及びアプリケーション作成者等のプロテクト側の双方に生ずる、多数の認証鍵等の固有情報を取り扱うことによって派生する不具合を解消し、プログラムの実行制御、デジタルコンテンツ（静止画・動画・音声等）のアクセス権保護、メールのプライバシー保護、ファイルや計算機資源のアクセス制御等を行う際に、ユーザのアクセス資格を簡易に認証する事ができるようにした、アクセス資格認証装置を提供することを目的とする。
【００２５】
【課題を解決する手段】
本発明の第１の側面によれば、上述の目的を達成するために、ユーザの権限を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証装置に、認証用データを記憶する第１の記憶手段と、ユーザの固

有情報を記憶する第２の記憶手段と、上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、上記第１の記憶手段に保持されている認証用データと、上記第２の記憶手段に保持されている上記ユーザの固有情報とに所定の演算を施して証明データを生成する証明データ生成手段と、上記証明データが上記ユーザの固有情報に基づいて生成されていることを検証する証明データ検証手段であって、上記証明データ生成手段によって生成された証明データと、上記第３の記憶手段に保持されている上記証明用補助情報とに所定の演算を施す演算手段を有し、該演算手段の演算結果を使用して検証を行なうものとを設けるようにしている。

【００２６】

この構成においては、証明用補助情報（アクセスチケット）を導入することにより、アクセス資格認証の特徴情報とユーザ固有情報とを独立させることができ、したがってプロテクト側もユーザ側も、１つの固有情報を準備しておくだけですむ。また、ユーザはアクセスチケットを受け取る必要がないので、たとえば、ユーザへのアプリケーションプログラム配布の際、配布するプログラムにアクセスチケットを添付しておき、証明データ検証装置が検証時に使用するといった検証方法が可能になる。

【００２７】

また、本発明の第２の側面によれば、ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証装置に、認証用データを記憶する第１の記憶手段と、ユーザの固有情報を記憶する第２の記憶手段と、上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、上記第１の記憶手段に保持されている認証用データと、上記第３の記憶手段に保持されている上記証明用補助情報とに所定の演算を施して証明データを生成する証明データ生成手段と、上記証明データが上記証明用補助情報に基づいて生成されていることを検証する証明データ検証手段であって，上記証明データ生成手段によって生成された証明データと、上記第２の記憶手段に保持されている上記ユーザの固有情報とに所定の演算を施す演算手段を有し、該演算手段の演算結果を使用して、検証を行なうものとを設けている。

【００２８】

この構成においても、アクセス資格認証の特徴情報とユーザ固有情報とを独立させることができ、したがってプロテクト側もユーザ側も、１つの固有情報を準備しておくだけですむ。さらに、証明データ検証装置側でユーザ固有情報に関連する計算を行っているので、ユーザ側ではアクセスチケットに関連する計算を行うだけでよい。たとえば、検証装置が専用のハードウエアにより耐タンパー特性を持つよう構成されており、ユーザの固有情報を保持しているような場合、ユーザはアクセスチケットを持っているだけで、安全に認証を行うことができる。

【００２９】

また、本発明の第３の側面によれば、上述の目的を達成するために、ユーザのアクセス資格を認証するアクセス資格認証装置に、認証用データを記憶する第１の記憶手段と、ユーザの固有情報を記憶する第２の記憶手段と、上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、上記認証用データと、上記ユーザの固有情報と、上記証明用補助情報とから、上記証明用補助情報と上記ユーザの固有情報との組が、上記アクセス資格認証の特徴情報に対して正しく対応するものであることを検証する検証手段とを設けるようにしている。

【００３０】

この構成においても、アクセス資格認証の特徴情報とユーザ固有情報とを独立させることができ、したがってプロテクト側もユーザ側も、１つの固有情報を準備しておくだけですむ。さらに、すべての計算を検証装置で行うため、ユーザは自分の固有情報とアクセスチケットを持ち歩くだけで、認証を行うことが可能となる。たとえば、アプリケーションプ

ログラムが専用装置上に構成されているような場合、ユーザは自分の固有情報とアクセスチケットとをＩＣカードに封入しておく。該専用装置はＩＣカードを挿入するためのスロットを備えており、ユーザは該スロットにＩＣカードを挿入することで認証を行うことができる。

【００３１】

【発明の実施の形態】

以下本発明について詳細に説明する。

［全体の構成］

具体的な個別の実施例を述べる前に、本発明の実施態様の概要を以下に述べる。

まず、本発明を、ユーザのＰＣあるいはワークステーション上で動作するアプリケーションプログラムの実行制御に用いる場合について述べる。図１、図２および図３に３つの実施態様の構成を示す。

【００３２】

図１は、第１の実施態様を全体として示している。第１の実施態様では、アクセスチケット（証明用補助情報）を証明データ検証時に用いるようにしている。図１において、プログラム実行制御装置（ユーザ認証装置）は、証明データ検証装置１０および証明データ生成装置１１を含んで構成されている。証明データ検証装置１０は検証手段１３を具備し、また認証用データ１４を保持している。また、証明データ検証装置１０は、アクセスチケット生成装置１２からアクセスチケット（証明用補助情報）１５を受領するようになっている。証明データ生成装置１１は、証明データ生成手段１６を具備しており、またユーザ固有情報１７を保持している。

【００３３】

証明データ検証装置１０は認証用データ１４を証明データ生成装置１１に送出する。証明データ生成装置１１の証明データ生成手段１６は、受け取った認証用データと、保持しているユーザ固有情報（ユーザを識別するための固有情報）１７とから証明データ１８を生成し、この証明データ１８を証明データ検証装置１０に返す。証明データ検証装置１０の検証手段１３は、認証データ１４、アクセスチケット１５を用いて証明データ１８を検証する。検証が成功すればプログラムの実行が許容される。

【００３４】

図２は、第２の実施態様を示している。この第２の実施態様では、アクセスチケットを証明データ生成時に用い、他方、ユーザ固有情報を証明データ検証時に用いるようにしている。図２において、図１と対応する箇所には対応する符号を付し詳細な説明を省略する。

【００３５】

図３は、第３の実施態様を示している。この第３の実施態様では、ユーザ固有情報およびアクセスチケットの双方を直接検証するようにしている。この実施態様では証明データを生成しない。図２において図１と対応する箇所には対応する符号を付して詳細な説明を省略する。

【００３６】

以下、各実施態様について詳細に説明する。

【００３７】

図１、図２および図３の各実施態様において、ユーザを識別するための固有情報（ユーザ固有情報１７）をユーザがコピーして配布することができると、正当な利用権をもたないユーザにもアプリケーションプログラムの使用を許すこととなる。そこで、ユーザ固有情報１７はその正当な保持者であるユーザであってもこれを窃取することができないように、該計算機に装着され、耐タンパー特性を有するハードウェア（ＩＣカード、ボードなど）を併用することが可能である。この際、ＩＣカードのような携帯性のあるハードウェアを用いれば、ユーザが複数のＰＣあるいはワークステーション上で作業をする場合に便利である。

【００３８】

図１の実施態様では、証明データ生成装置１１はユーザが用いる計算機上の証明用プログ

ラムとして実現することができる。この際、証明データ１８を生成するためにユーザ固有情報１７を用いるため、上記理由により、前記プログラムの少なくとも一部はＩＣカード等の防御手段によって保護される必要がある。

【００３９】

証明データ検証装置１０は該ユーザが利用するアプリケーションプログラムの一部として構成される。即ち、ユーザが該アプリケーションプログラムをＰＣあるいはワークステーション上で起動すると、該アプリケーションプログラム中にプログラムとして記述された証明データ検証装置１０が起動されて認証が行われ、正しく認証された時に限って該アプリケーションプログラムの実行を可能とする。これらの実施態様では証明データ生成装置１１と通信してユーザ認証を行い、通信が正しく終了した場合に限って該アプリケーションプログラムの実行を可能とする。

【００４０】

ユーザが、証明データ検証装置１０が埋めこまれた前記アプリケーションプログラムを利用するためには、ユーザ本人宛に発行され、前記アプリケーションプログラムに対応する証明用補助情報（アクセスチケット１５）を取得する必要がある。アクセスチケット１５は、前記ＰＣあるいはワークステーション上に置く構成にしてもよいし、ユーザ固有情報１７がＩＣカードに封入されている場合には、このＩＣカード中においてもよい。

【００４１】

証明データ生成装置１１（ＰＣあるいはワークステーション上のプログラムとＩＣカードによって構成される）は、ユーザ固有情報１７に基づいて計算を行い、その計算に基づいて証明データ検証装置１０と通信を行う。

【００４２】

通信の結果、証明データ検証装置１０による認証が成功するのは、ユーザ固有情報１７と、アクセスチケット１５と、証明データ検証装置１０が検証するアクセス資格認証の特徴情報の三つが正しく対応している場合に限られる。

【００４３】

ユーザ固有情報１７あるいはアクセスチケット１５の一方が欠けていた場合には、認証は成功しない。

【００４４】

図１の実施形態の場合、ユーザはアクセスチケットを受け取る必要がない。たとえば、ユーザへのアプリケーションプログラム配布の際、配布するプログラムにアクセスチケットを添付しておき、証明データ検証装置が検証時に使用するといった検証方法が可能になる。

【００４５】

図２の実施態様では、証明データ生成装置１１はユーザが用いる計算機上の証明用プログラムとして実現することができる。

【００４６】

証明データ検証装置１０は該ユーザが利用するアプリケーションプログラムの一部として構成される。即ち、ユーザが該アプリケーションプログラムをＰＣあるいはワークステーション上で起動すると、該アプリケーションプログラム中にプログラムとして記述された証明データ検証装置１０が起動されて認証が行われ、正しく認証された時に限って該アプリケーションプログラムの実行を可能とする。これらの実施態様では証明データ生成装置１１と通信してユーザ認証を行い、通信が正しく終了した場合に限って該アプリケーションプログラムの実行を可能とする。この通信の際、ユーザ固有情報１７を送信することがあるが、前記理由によりユーザ固有情報が外部に漏洩すると問題があるため、安全に検証装置１０に送る必要がある。

【００４７】

ユーザが、証明データ検証装置１０が埋めこまれた前記アプリケーションプログラムを利用するためには、アクセスチケット１５を取得する必要がある。アクセスチケット１５は、前記ＰＣあるいはワークステーション上に置く構成にしてもよいし、ユーザ固有情報１

７がＩＣカードに封入されている場合には、このＩＣカード中においてもよい。
【００４８】
証明データ生成装置１１は、アクセスチケット１５に基づいて計算を行い、その計算に基づいて証明データ検証装置１０と通信を行う。
【００４９】
通信の結果、証明データ検証装置１０による認証が成功するのは、この場合も、ユーザ固有情報１７と、アクセスチケット１５と、証明データ検証装置１０が検証するアクセス資格認証の特徴情報の三つが正しく対応している場合に限られる。
【００５０】
ユーザ固有情報１７あるいはアクセスチケット１５の一方が欠けていた場合には、認証は成功しない。
【００５１】
図２の実施形態では、ユーザ側ではアクセスチケットに関連する計算を行うだけでよい。たとえば、証明データ検証装置１０が専用のハードウエアにより耐タンパー特性を持つよう構成されており、ユーザの固有情報を保持しているような場合、ユーザはアクセスチケットを持っているだけで、安全に認証を行うことができる。
【００５２】
図３の実施態様では、検証装置１０（正確には証明データ検証装置１０ではないが、便宜上、符号１０を用いて参照する）は該ユーザが利用するアプリケーションプログラムの一部として構成される。即ち、ユーザが該アプリケーションプログラムをＰＣあるいはワークステーション上で起動すると、該アプリケーションプログラム中にプログラムとして記述された検証装置１０が起動されて認証が行われ、正しく認証された時に限って該アプリケーションプログラムの実行を可能とする。検証装置１０は、ユーザ固有情報１７とアクセスチケット１５とを取得して認証を行う。この際、前記理由により、ユーザの固有情報が外部に漏洩しないよう保護する必要がある。
【００５３】
一連の動作の結果、検証装置１０による認証が成功するのは、この場合も、ユーザ固有情報１７と、アクセスチケット１５と、検証装置１０が検証するアクセス資格認証の特徴情報の三つが正しく対応している場合に限られる。
【００５４】
ユーザ固有情報１７あるいはアクセスチケット１５の一方が欠けていた場合には、認証は成功しない。
【００５５】
図３の実施形態では、すべての計算を検証装置１０で行うため、ユーザは自分の固有情報とアクセスチケットを持ち歩くだけで、認証を行うことが可能となる。たとえば、アプリケーションプログラムが専用装置上に構成されているような場合、ユーザは自分の固有情報とアクセスチケットとをＩＣカードに封入しておく。該専用装置はＩＣカードを挿入するためのスロットを備えており、ユーザは該スロットにＩＣカードを挿入することで認証を行うことができる。
【００５６】
以上説明したように、各実施態様において、アクセスチケット１５は特定のユーザ宛に発行される。即ち、アクセスチケット１５の生成に際して、特定のユーザのユーザ固有情報１７が使用される。アクセスチケット１５の生成時に使用されるユーザ固有情報１７と、そのアクセスチケット１５を使用するユーザのユーザ固有情報１７とが一致していない場合、やはり、認証は成功しない。
【００５７】
また、アクセスチケットは、特定のアクセス資格認証の特徴情報に基づいて生成され、証明データ検証装置（図３の構成では検証装置）１０はこのアクセス資格認証の特徴情報を認証するように構成される。従って、アクセスチケット１５の生成のもととなった特徴情報と、アプリケーションプログラムに埋めこまれている証明データ検証装置１０が認証し

ようとする特徴情報とが互いに対応していなかった場合にも、認証は成功しない。

【００５８】

また、アプリケーションプログラムがネットワークによって結合された別の計算機上で実行され、実行結果がネットワークを介してユーザが用いる計算機に通信されるものとしてもよい。この場合、いわゆるサーバ・クライアントモデルに基づく構成となる。先に述べた、ユーザのＰＣあるいはワークステーション上で実行されるアプリケーションプログラムの実行制御の場合では、証明データ生成装置１１と証明データ検証装置１０との通信がいわゆるプロセス間通信として実行されるのに対し、サーバ・クライアント・モデルに従った場合、証明データ生成装置１１と証明データ検証装置１０との通信はＴＣＰ／ＩＰ（トランスミッション・コントロール・プロトコル／インターネット・プロトコル）などのネットワークプロトコルに従った通信として実行される。

【００５９】

また、アプリケーションプログラムが専用装置上に構成されている場合にも、本発明を適用することが可能である。例えば、証明データ生成装置１１が存在する構成では、ユーザの固有情報だけでなく証明データ生成装置１１全体もＩＣカード内に実装し、取得したアクセスチケット１５もＩＣカードに登録するものとする。証明データ検証装置１０は前記専用装置上に実装されるが、該専用装置はＩＣカードを挿入するためのスロットを備え、ユーザは該スロットに所有するＩＣカードを挿入することで認証を行う。

【００６０】

このような専用装置による構成は、銀行のＡＴＭ機や、ゲームセンターにおけるゲーム機などに適用することができる。

【００６１】

ユーザによるアクセスチケット１５の取得に関しては、アクセスチケット１５を発行する共通のセンターが、ユーザからの発行依頼に応じて生成して配布する方法と、アプリケーションプログラムの作成者が、アクセスチケット発行プログラムやアクセスチケット生成装置１２の助けを借りて個別に生成する方法がある。

このような場合、アクセスチケット生成装置１２は、チケット発行者によって管理され、アクセスチケットはこれら正当な権利者等によって、ユーザの環境とは別個に作成され、配布される。

【００６２】

生成されたアクセスチケット１５は、フロッピーディスク等の可搬型記憶媒体を介してユーザに配送されるものとしてもよいが、アクセスチケット１５が十分な安全性を備えていることから、電子メールなどを用いてネットワークを介して配送されるように構成してもよい。

【００６３】

アクセスチケット１５の安全性とは、以下の二つの性質である。

【００６４】

１）アクセスチケットはいわゆる記名式である。即ち、アクセスチケットが発行されたユーザ本人（正確には、アクセスチケット生成時に用いられたユーザ固有情報の保持者）だけが該アクセスチケットを用いて証明データ生成装置を正しく作動させることができる。従って、悪意の第三者が、他のユーザのアクセスチケットを不正に手に入れたとしても、この第三者がアクセスチケットの発行先である正規のユーザのユーザ固有情報を手に入れないかぎり、このアクセスチケットを利用することは不可能である。

【００６５】

２）アクセスチケットはさらに厳密な安全性を保持している。即ち、悪意の第三者が任意個数のアクセスチケットを集めて、いかなる解析を行ったとしても、得られた情報をもとに別のアクセスチケットを偽造したり、証明データ生成装置の動作を模倣して認証を成立させるような装置を構成することは不可能である。

【００６６】

以下では、より具体的な構成について実施例に即して説明する。

【００６７】
［実施例１］
実施例１では、ＲＳＡ（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｅｌｍａｎ）暗号を用いて認証を行うものであり、また、アクセスチケットを証明データ検証装置１０で利用する点に特徴がある。
【００６８】
本実施例の全体の構成を図１に、証明データ検証装置１０の構成を図４に示し、証明データ生成装置の構成を図６に示す。また、本実施例の証明データ検証装置１０の動作を図８に示し、証明データ生成装置１１の動作を図１８に示す。
【００６９】
図４において、証明データ検証装置１０は、アクセスチケット公開鍵記憶部１０１、乱数生成部１０２、乱数記憶部１０３、検証用演算部１０４、乱数効果除去部１０５、実行手段１０６、乱数効果付与部１０７、認証用素データ記憶部１０８、認証用データ記憶部１０９、受信データ記憶部１１０およびアクセスチケット記憶部１１１を含んで構成されている。証明データ検証装置１０の各部の動作およびデータの流れが図１０に示すとおりである。動作の詳細については後に詳述する。
【００７０】
図６において、証明データ生成装置１１は、受信データ記憶部１２１、ユーザ固有情報記憶部１２２、指数生成部１２３および証明データ生成部１２４を含んで構成されている。証明データ生成装置１１の各部の動作およびデータの流れは図１８に示すとおりである。動作の詳細については後に詳述する。
【００７１】
つぎに、本実施例における認証の詳細を説明する。
【００７２】
本発明における実施例１では、アクセス資格認証の特徴情報Ｄと、Ｄに対応する公開情報ＥおよびｎはＲＳＡ法数、すなわち、十分大きな二つの素数ｐ，ｑの積であり、式１－１を満たす。
【００７３】
【数１】
（１－１）　　ｎ＝ｐｑ
φ（ｎ）をｎのオイラー数であり、式１－２によって計算される。
【００７４】
【数２】
（１－２）　　φ（ｎ）＝（ｐ－１）（ｑ－１）
アクセス資格認証の特徴情報Ｄは、法数ｎのもとでのＲＳＡ秘密鍵であり、式１－３を満たす。
【００７５】
【数３】
（１－３）　　ｇｃｄ（Ｄ，φ（ｎ））＝１
ここで、ｇｃｄ（ｘ，ｙ）は、二数ｘ、ｙの最大公約数を表す。式１－３によって表現される性質は、式１－４を満たす数Ｅが存在することを保証する。
【００７６】
【数４】
（１－４）　　ＥＤ　ｍｏｄ　φ（ｎ）＝１
Ｄをアクセスチケット秘密鍵、Ｅをアクセスチケット公開鍵と呼ぶ。
【００７７】
アクセスチケットｔは、アクセスチケット秘密鍵Ｄ、ユーザの固有情報ｅ、法数ｎを用い、以下の式１－５に基づいて生成される。
【００７８】

【数５】
（１－５）　　ｔ＝Ｄ－Ｆ（ｅ，ｎ）
ユーザの固有情報ｅは、ユーザ毎に異なる数であり、ユーザを識別するために用いられる。関数Ｆは関数値が衝突しにくい関数であり、例えば、一方向ハッシュ関数ｈを利用して、式１－６あるいは式１－７のように定めることができる。
【００７９】
【数６】
（１－６）　　Ｆ（ｘ，ｙ）＝ｈ（ｘ｜ｙ）
【００８０】
【数７】
（１－７）　　Ｆ（ｘ，ｙ，ｚ，ｕ，ｗ）＝ｈ（ｘ｜ｙ｜ｚ｜ｕ｜ｗ）
ここで、ｘ｜ｙはｘとｙとのビットの連結であることを表す。
【００８１】
一方向ハッシュ関数とは、ｈ（ｘ）＝ｈ（ｙ）を満たす相異なるｘ、ｙを算出することが著しく困難であるという性質をもつ関数である。一方向ハッシュ関数の例として、ＲＳＡ　Ｄａｔａ　Ｓｅｃｕｒｉｔｙ　Ｉｎｃ．によるＭＤ２、ＭＤ４、ＭＤ５、米国連邦政府による規格ＳＨＳ（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ｓｔａｎｄａｒｄ）が知られている。
【００８２】
上記の説明中に現れた数において、ｔ、Ｅ、ｎは公開可能であり、残りのＤ、ｅ、ｐ、ｑ、φ（ｎ）および関数Ｆはチケットを作成する権利を有するもの以外には秘密である必要がある。
【００８３】
また、以下では、暗号化されるデータＫを検証用データ、証明データ生成装置１１が証明のために生成するデータＲを証明用データとよぶ。また、証明データ生成装置１１が証明データを生成するために、検証装置１０から受け取るデータ、及び、検証装置が復号された値を検証するために用いるデータを認証用データと呼ぶ。
【００８４】
以下に本実施例の動作を示す。
【００８５】
１．ユーザが、アクセス資格認証装置による認証を必要とするデジタルコンテンツにアクセスすることによって、証明データ検証装置１０が起動される。
【００８６】
証明データ検証装置１０がユーザのＰＣあるいはワークステーション上で動作するアプリケーションプログラムの一部として構成されている場合、ユーザがキーボードあるいはマウスなどの指示装置を用いた通常の方法で、アプリケーションプログラムを起動する。アプリケーションプログラムの実行が証明データ検証装置１０を構成しているプログラムに到達することにより、証明データ検証装置１０が起動される。
【００８７】
証明データ検証装置１０がネットワークで結ばれた他のＰＣあるいはワークステーション（サーバと呼ぶ）上に構成されている場合、ユーザは自分のＰＣあるいはワークステーション上の通信プログラムを起動し、該通信プログラムが所定の手続きに従って前記サーバに通信の開設要求を行うことにより、前記サーバ上の証明データ検証装置１０が起動される。例えば、ユーザの通信プログラムがサーバと通信する際にＴＣＰ／ＩＰ（トランスミッション・プロトコル／インターネット・プロトコル）と呼ばれる手続きに従うとすると、証明データ検証装置１０をサーバの特定のポートに予め対応づけておき、更に、ユーザの通信プログラムが該ポートを指定してＴＣＰ接続要求をサーバに要求するように設定しておくことにより、サーバ上のデーモン（ｉｎｅｔｄ）がＴＣＰ接続要求に応じて証明データ検証装置を起動することが可能となる。このような実現方法は、インターネットなどのネットワークにおいて広く利用されているものである。
【００８８】

証明データ検証装置１０を専用目的の装置とすることも可能である。例えば、証明データ検証装置をＩＣカード・リーダ・ライター内のＲＯＭに焼きつけられたプログラムとして構成し、証明データ生成装置１０をＩＣカードのマイクロコントローラーに実装されたプログラムとすることができる。この場合、ユーザがＩＣカードをリーダ・ライターに挿入することにより、証明データ検証装置１０が起動される。

【００８９】

２．証明データ検証装置１０は、認証用データＣと、アクセスチケット公開鍵記憶部１０１に記憶されている法数ｎとを、証明データ生成装置１１中の受信データ記憶部１２１に書き込む。認証用素データ記憶部１０８には、認証用素データとしてＣ’が記憶されている。ここで、検証用データを適当なデータＫとする時、認証用素データＣ’は、データＫに対して式１－８を満たす。

【００９０】

【数８】

（１－８）　　$C' = K^{E} \mod n$

ここで、データＫを証明データ検証装置１０に保持せず、代わりに、その暗号化の結果であるＣ’のみを保持するように証明データ検証装置１０を構成すれば、証明データ検証装置１０からデータＫが漏洩する危険を回避することができる。

【００９１】

認証用データＣは、証明データ検証装置１０により、乱数生成部１０２で乱数ｒを生成し、ｒと、アクセスチケット公開鍵記憶部１０１から取得したＥ、ｎと、認証用素データ記憶部１０８から取得したＣ’とを用い、乱数効果付与部１０７で式１－９の計算を行うことで生成される。生成された認証用データＣは、証明データ生成装置１１中の受信データ記憶部１２１に書き込まれるとともに、証明データ検証装置１０の認証用データ記憶部１０９にも記憶される。また、生成した乱数ｒは、乱数記憶部１０３に記憶される。

【００９２】

【数９】

（１－９）　　$C = r^{E} C' \mod n$

このように、認証用データに乱数効果を加え、証明データ生成装置１１が返す証明データを検証する際に乱数効果を除去するように構成することにより、いわゆるリプレイアタックを防止することができる。これは、以下の実施例においても、同様である。

【００９３】

３．証明データ生成装置１１中の指数生成部１２３は、ユーザ固有情報記憶部１２２に記憶されているユーザの固有情報ｅと、アクセスチケット公開鍵記憶部１０１に記憶されている法数ｎとを取得し、式１－１０の計算を実行する。

【００９４】

【数１０】

（１－１０）　　$F(e, n)$

【００９５】

４．証明データ生成装置１１中の証明データ生成部１２４は、指数生成部１２３で生成されたデータを用いて、式１－１１の計算を実行しＲを得る。

【００９６】

【数１１】

（１－１１）　　$R = C^{F(e, n)} \mod n$

【００９７】

５．証明データ生成装置はＲを証明データ検証装置の受信データ記憶部に返送する。

【００９８】

６．証明データ検証装置１０中の検証用演算部１０４は、アクセスチケット記憶部１１１に記憶されているアクセスチケットｔを取得し、受信データ記憶部１１０に書き込まれた法数ｎのもとで式１－１２を実行し、Ｓを得る。

【００９９】

【数１２】
（１－１２）　　$S = RC^{t} \mod n$
【０１００】
７．証明データ検証装置１０中の乱数効果除去部１０５は、乱数記憶部１０３から先に生成した乱数ｒを取り出し、式１－１３の計算を行う。
【０１０１】
【数１３】
（１－１３）　　$K' = r^{-1} S \mod n$
【０１０２】
８．証明データ生成装置１１において用いられるアクセスチケットｔとユーザの固有情報ｅの組み合わせが正しい場合に限り、計算の結果得られたＫ’と検証用データＫが一致し、正しく検証が行われる。
【０１０３】
９．計算されたＫ’は、証明データ検証装置１０中の実行手段に引き渡されるが、実行手段はＫ’＝Ｋが成立する場合に限り正規の処理を実行する。
【０１０４】
以下、証明データ検証装置１０において、ＫとＫ’が同一であることを検証する方法について、いくつかの例を記す。
【０１０５】
［１］検証用データと復号結果を直接比較する構成例
証明データ検証装置１０は予め検証用データＫを記憶しておく。証明データ検証装置１０中の比較部は、この検証用データＫと、認証用データを復号したデータＫ’とを直接比較し、Ｋ’＝Ｋが成立する場合に限り正規の処理を実行し、成立しない場合には処理を中止するなどのエラー処理を実行する。
【０１０６】
この構成例では、検証すべき検証用データＫそのものが装置中に現れるという安全上の弱点がある。例えば、証明データ検証装置１０がユーザのＰＣあるいはワークステーション上で動作するプログラムとして構成されている場合、プログラムを解析してＫを窃取することは、困難であっても、必ずしも不可能ではない。Ｋの値がユーザの知るところとなると、証明データ生成装置１１の動作を模倣する装置を構成することが可能となり、なりすましによる不正アクセスが可能となる。
【０１０７】
［２］一方向性関数を用いた構成例
上記の欠点を改善するため、証明データ検証装置１０が記憶している検証のためのデータを、検証用データＫそのものではなく、Ｋに前述の一方向ハッシュ関数ｈを施して得られるデータｈ（Ｋ）とする。一方向ハッシュ関数の性質から、証明データ記憶手段に記憶されるデータｙから、ｙ＝ｈ（ｘ）を満たすｘを算出することは著しく困難である。
【０１０８】
証明データ検証装置１０は、入力データに対し一方向ハッシュ関数を施した結果を返す変換部を有する。比較部は、認証用データを復号したデータＫ’をハッシュ関数の入力として得られる出力ｈ（Ｋ’）と、記憶されているデータ（＝ｈ（Ｋ））とを比較する。
【０１０９】
この方法例では、検証用データＫがプログラム中に現れることがなく、また、証明データ記憶手段に記憶されたｈ（Ｋ）からＫを計算することも著しく困難であることから、上記［１］の例よりは安全であるといえる。
【０１１０】
しかしながら、比較部はプログラム中では条件文として構成されており、証明データ検証装置がプログラムで、分析・改竄が容易であるような構成の場合には、該条件文をスキップするようにプログラムを改竄することが可能である点で、なお弱点を有している。
【０１１１】

［３］復号された値が、特定のデータを復号するための復号鍵である構成例
検証のために記憶されているデータが、暗号化されたデータであり、認証用データを復号したデータＫ’は、この暗号化されたデータを復号するための鍵である。
【０１１２】
証明データ検証装置１０は、データＫ’の値を、検証のために記憶されているデータを暗号化するのに用いた暗号の復号鍵として用いて復号し、その結果、暗号化されたデータが復号できた場合のみ、プログラムの実行を可能とする。
【０１１３】
この構成でも、検証装置中に復号鍵そのものは現れないため、安全度は高くなっている。
【０１１４】
［４］復号された値が特定の冗長性を満たすことを確認する構成例
証明データ検証装置１０が冗長性検証手段をもち、証明データ検証装置１０は、認証用データを復号したデータＫ’の値を、冗長性検証手段に送る。冗長性検証手段が、そのデータが特定の冗長性を満たすことを確認した場合のみ、プログラムの実行を可能とする。
【０１１５】
冗長性の例としては、復号されたデータがある特定のパターンを繰り返していることや、特定の位置のデータが特定の条件を満たすこと、あるいは、データが特定の言語として意味があること、等があげられる。
【０１１６】
［５］プログラムコード自体を暗号化する構成例
証明データ検証装置１０が保持するプログラムのコードの一部或は全部を暗号化したデータを認証用データとして、認証用データ記憶手段に保持する。即ち、認証用データを復号したデータＫ’はプログラムのコードの一部或は全部となる。
【０１１７】
実行手段はデータＫ’を、プログラム中の予め定められた位置に埋め込み、その後、埋め込んだプログラムを実行する。証明データ生成装置１１が正しいデータを返信した場合、即ち、Ｋ’がコードを正しく復号したものである場合に限ってプログラムは実行可能となる。
【０１１８】
実行手段は復号されたコードを本来のプログラムに埋め込んだファイルを生成した後、そのファイルを起動してもよいが、プログラムがメモリ上に展開されている状態で、復号したコードをメモリ上のプログラムに埋め込んだのち起動する方法が、安全上は望ましい。
【０１１９】
この構成例では、プログラムの実行に不可欠なコードの一部或は全部が暗号化されているため、実行手段がユーザのＰＣあるいはワークステーション上で動作するアプリケーションプログラムとして構成されているような比較的安全性の低い場合でも、不正実行を防止することができる。
【０１２０】
［６］復号された値がプログラムの復号鍵である構成例
証明データ検証装置１０がプログラムのコードの一部或は全部を暗号化したデータを保持しており、認証用データを復号したデータＫ’が、暗号化したプログラムコードを復号するために必要な復号鍵となっているものである。この構成によると、暗号化するコードのサイズに関わらず、データＫ’のサイズを一定の小さい値に抑えることが可能となり、通信のオーバヘッドを減少させることができる。
【０１２１】
証明データ検証装置１０はデータＫ’を用いて、記憶している暗号化されたプログラムコードを復号する。実行部は、復号されたコードを、プログラム中の予め定められた位置に埋め込み、その後、埋め込んだプログラムを実行する。証明データ生成装置が正しいデータを返信していた場合、即ち、Ｋ’によってコードが正しく復号されていた場合に限ってプログラムは実行可能となる。

【０１２２】
［実施例２］
つぎに本発明の実施例２について説明する。この実施例２においては、ＥｌＧａｍａｌ暗号を用いて認証を行い、また、アクセスチケットを証明データ検証装置１０で利用する点に特徴がある。
【０１２３】
本実施例の構成は、実施例１と同様である。すなわち、本実施例の全体の構成を図１に示す。また、本実施例の証明データ検証装置１０の構成を図４に示し、証明データ生成装置１１の構成を図６に示す。
【０１２４】
本実施例の証明データ検証装置１０の動作を図９に示し、証明データ生成装置１１の動作を図１９に示す。これらの動作については詳述する前に、本実施例の認証の詳細について説明する。
【０１２５】
本発明における実施例２では、アクセス資格認証の特徴情報Ｘは、法数ｐ（ｐは十分大きな素数）のもとでのＥｌＧａｍａｌ暗号の秘密鍵であり、Ｙが対応する公開鍵である。即ち、式２－１を満たす。
【０１２６】
【数１４】
（２－１）　　$Y = a^{X} \mod p$
ここで、ａは位数ｐの有限体の乗法群の生成元、即ち、式２－２及び２－３を満たす。
【０１２７】
【数１５】
（２－２）　　$a \neq 0$
（２－３）　　$\min\{X > 0 \mid a^{X} = 1 \mod p\} = p - 1$
次に、ユーザを識別するために、ユーザ毎に異なる数であるユーザ固有情報ｅを定める。アクセスチケットｔは次の式２－４に基づいて生成される。
【０１２８】
【数１６】
（２－４）　　$t = X - F(e, p)$
関数Ｆは、実施例１と同様である。
【０１２９】
つぎに本実施例の動作について詳述する。
【０１３０】
１．ユーザがアクセスすることによって、証明データ検証装置１０が起動される。
【０１３１】
証明データ検証装置１０の実現方法として、ユーザのＰＣやワークステーション上で動作するアプリケーションプログラム、ユーザのＰＣやワークステーションとネットワークを介して接続されたサーバ上のサーバプログラム、あるいは、ＩＣカード・リーダ・ライターのような専用の装置のいずれも可能であることは、第一の実施例の場合と変わらない。これは、以降の実施例においても同様である。
【０１３２】
２．証明データ検証装置１０は、認証用データｕ’と、アクセスチケット公開鍵記憶部１０１に記憶されている法数ｐとを、証明データ生成装置１１中の受信データ記憶部１２１に書き込む。認証用素データ記憶部１０８には、認証用素データとしてｕが記憶され、認証用データ記憶部１０９には認証用データＣおよびｕ’が記憶されている。
【０１３３】
ｕは、上記ａを法ｐのもとで適当な乱数ｚを指数としてべき乗した数であり、即ち、式２－５を満たす。
【０１３４】

【数１７】
（２－５）　　$u = a^{z} \mod p$
ここで、検証用データを適当なデータＫとする時、Ｃは、アクセスチケット公開鍵Ｙを、法ｐのもとで、上記乱数ｚを指数としてべき乗した数と、検証用データＫとの積であり、式２－６を満たす。
【０１３５】
【数１８】
（２－６）　　$C = Y^{z} K \mod p$
証明データ検証装置１０は、乱数生成部１０２によって、乱数ｒをアクセスチケット公開鍵記憶部１０１に保持されている法数ｐより１引いた値（ｐ－１）と互いに素になるように生成し、乱数記憶部１０３に記録する。
【０１３６】
次いで、乱数効果付与部１０７は、認証用素データ記憶部１０８に記憶されているデータｕを取得して、式２－７により認証用データｕ’を計算する。
【０１３７】
【数１９】
（２－７）　　$u' = u^{r} \mod p$
【０１３８】
３．証明データ生成装置１１中の指数生成部１２３は、ユーザ固有情報記憶部１２２に記憶されているユーザの固有情報ｅと、受信データ記憶部１２１に記憶されている法数ｐを取得し、式２－８の計算を実行する。
【０１３９】
【数２０】
（２－８）　　Ｆ（ｅ，ｐ）
【０１４０】
４．証明データ生成装置１１中の証明データ生成部１２４は、指数生成部１２３で生成されたデータを用いて、式２－９の計算を実行しＲを得る。
【０１４１】
【数２１】
（２－９）　　$R = u'^{F(e,p)} \mod p$
【０１４２】
５．証明データ生成装置１２４は、Ｒを証明データ検証装置１０の受信データ記憶部１１０に返送する。
【０１４３】
６．証明データ検証装置１０中の検証用演算部１０４は、アクセスチケット公開鍵記憶部１０１から法数ｐ、認証用データ記憶部１０９から認証用素データｕ’、および、アクセスチケット記憶部１１１からアクセスチケットｔを取得して、式２－１０の計算を行う。
【０１４４】
【数２２】
（２－１０）　　$S = u'^{t} \mod p$
【０１４５】
７．更に、証明データ検証装置１０中の検証用演算部１０４は、受信データ記憶部１１０に記憶された証明データＲを取得し、式２－１１の計算を行い、Ｒ’を得る。
【０１４６】
【数２３】
（２－１１）　　$R' = SR \mod p$
【０１４７】
８．証明データ検証装置１０中の乱数効果除去部１０５は、乱数記憶部１０３から先に生成した乱数ｒを取り出し、まず式２－１２の計算を行う。
【０１４８】

【数２４】
（２－１２）　　$v = R'^{A} \mod p$
ただし$A = (r^{-1} \mod (p-1))$
次いで、計算の結果得られたｖと、認証用データ記憶部１０９に記憶されているＣを用いて、式２－１３の計算を行う。
【０１４９】
【数２５】
（２－１３）　　$K' = C \cdot v^{-1} \mod p$
【０１５０】
９．証明データ検証装置１０において用いられるアクセスチケットｔとユーザの固有情報ｅの組み合わせが正しい場合に限り、計算の結果得られたＫ’と検証用データＫが一致し、正しく検証が行われる。
【０１５１】
［実施例３］
つぎに本発明の実施例３について説明する。本実施例は実施例２を変形したものである。本実施例では、ＥｌＧａｍａｌ公開鍵暗号の構成方法、アクセスチケットｔ、及び認証用素データｕ，認証用データＣの生成方法とそれぞれの満たすべき性質は、実施例２と同様である。
【０１５２】
本実施例の全体の構成を図１に示し、証明データ検証装置１０の構成を図４に示し、証明データ生成装置１１の構成を図６に示す。また、本実施例の検証装置の動作を図１０に、証明データ生成装置の動作を図１９に示す。
【０１５３】
以下、本実施例の動作について説明する。
【０１５４】
１．ユーザがアクセスすることによって、証明データ検証装置１０が起動される。
【０１５５】
２．証明データ検証装置１０は、認証用データｕ’と、アクセスチケット公開鍵記憶部１０１に記憶されている法数ｐとを、証明データ生成装置１１中の受信データ記憶部１２１に書き込む。認証用素データ記憶部１０８には、認証用素データとしてｕが記憶され、認証用データ記憶部１０９には認証用データＣが記憶されている。
【０１５６】
証明データ検証装置１０は、乱数生成部１０２によって、乱数ｒを生成し、乱数記憶部１０３に記録する。
【０１５７】
次いで、乱数効果付与部１０７は、認証用素データ記憶部１０８に記憶されているデータｕを取得して、式３－１により認証用データｕ’を計算する。
【０１５８】
【数２６】
（３－１）　　$u' = u \cdot a^{r} \mod p$
【０１５９】
３．証明データ生成装置１１中の指数生成部１２３は、ユーザ固有情報記憶部１２２に記憶されているユーザの固有情報ｅと、受信データ記憶部１２１に記憶されている法数ｐを取得し、式３－２の計算を実行する。
【０１６０】
【数２７】
（３－２）　　$F(e, p)$
【０１６１】
４．証明データ生成装置１１中の証明データ生成部１２４は、指数生成部１２３で生成されたデータを用いて、式３－３の計算を実行しＲを得る。

【０１６２】
【数２８】
（３－３）　　$R = u'^{F(e,p)} \mod p$
【０１６３】
５．証明データ生成装置１１は、Ｒを証明データ検証装置１の受信データ記憶部１１０に返送する。
【０１６４】
６．証明データ検証装置１０中の検証用演算部１０４は、アクセスチケット公開鍵記憶部１０１から法数ｐ、認証用素データ記憶部１０９から認証用データｕ’、および、アクセスチケット記憶部１１１からアクセスチケットｔを取得して、式３－４の計算を行う。
【０１６５】
【数２９】
（３－４）　　$S = u'^{t} \mod p$
【０１６６】
７．更に、証明データ検証装置１０中の検証用演算部１０４は、受信データ記憶部１１０に記憶された証明データＲを取得し、式３－５の計算を行い、Ｒ’を得る。
【０１６７】
【数３０】
（３－５）　　$R' = SR \mod p$
【０１６８】
８．証明データ検証装置１０中の乱数効果除去部１０５は、乱数記憶部１０３から先に生成した乱数ｒを取り出し、まず式３－６の計算を行う。
【０１６９】
【数３１】
（３－６）　　$v = Y^{-r} \cdot R' \mod p$
次いで、計算の結果得られたｖと、認証用データ記憶部１０９に記憶されているＣを用いて、式３－７の計算を行う。
【０１７０】
【数３２】
（３－７）　　$K' = C \cdot v^{-1} \mod p$
【０１７１】
９．証明データ検証装置１０において用いられるアクセスチケットｔとユーザの固有情報ｅの組み合わせが正しい場合に限り、計算の結果得られたＫ’と検証用データＫが一致し、正しく検証が行われる。
【０１７２】
［実施例４］
つぎに本発明の実施例４について説明する。本実施例も実施例２の変更例である。本実施例では、ＥｌＧａｍａｌ公開鍵暗号の構成方法、アクセスチケットｔ、及び認証用素データｕ、認証用データＣの生成方法とそれぞれの満たすべき性質は、実施例２と同様である。
【０１７３】
本実施例の全体の構成を図１に示す、証明データ検証装置１０の構成を図４に示し、証明データ生成装置１１の構成を図６に示す。また、本実施例の証明データ検証装置１０の動作を図１１に示し、証明データ生成装置１１の動作を図２０に示す。
【０１７４】
以下、本実施例の動作について説明する。
【０１７５】
１．ユーザがアクセスすることによって、証明データ検証装置１０が起動される。
【０１７６】
２．証明データ検証装置１０は、認証用データｕ’、Ｃ’と、アクセスチケット公開鍵記

憶部１０１に記憶されている法数ｐとを、証明データ生成装置１１中の受信データ記憶部１２１に書き込む。認証用素データ記憶部１０８には、認証用素データとしてｕおよびＣが記憶されている。

【０１７７】

証明データ検証装置１０は、乱数生成部１０２によって、乱数ｒをアクセスチケット公開鍵記憶部１０１に保持されている法数ｐより１引いた値（ｐ－１）と互いに素になるように生成し、乱数記憶部１０３に記録する。

【０１７８】

次いで、乱数効果付与部１０７は、認証用素データ記憶部１０８に記憶されているデータｕを取得して、式４－１の計算により認証用データｕ’を計算する。

【０１７９】

【数３３】

（４－１）　　$u' = u^{r} \mod p$

さらに乱数効果付与部１０７は、認証用素データ記憶部１０８に記憶されているデータＣを取得して、式４－２の計算を行う。

【０１８０】

【数３４】

（４－２）　　$C' = C^{r} \mod p$

【０１８１】

３．証明データ生成装置１１中の指数生成部１２３は、ユーザ固有情報記憶部１２２に記憶されているユーザの固有情報ｅと、受信データ記憶部１２１に記憶されている法数ｐを取得し、式４－３の計算を実行する。

【０１８２】

【数３５】

（４－３）　　Ｆ（ｅ，ｐ）

【０１８３】

４．証明データ生成装置１１中の証明データ生成部１２４は、指数生成部１２３で生成されたデータを用いて、式４－４の計算を実行しＲを得る。

【０１８４】

【数３６】

（４－４）　　$R = C' u'^{-F(e,p)} \mod p$

【０１８５】

５．証明データ生成装置１１は、Ｒを証明データ検証装置１０の受信データ記憶部１１０に返送する。

【０１８６】

６．証明データ検証装置１０中の検証用演算部１０４は、アクセスチケット公開鍵記憶部１０１から法数ｐ、認証用データ記憶部１０９から認証用データｕ’、および、アクセスチケット記憶部１１１からアクセスチケットｔを取得して、式４－５の計算を行う。

【０１８７】

【数３７】

（４－５）　　$S = u'^{t} \mod p$

【０１８８】

７．更に、証明データ検証装置１０中の検証用演算部１０４は、受信データ記憶部１１０に記憶された証明データＲを取得し、式４－６の計算を行い、Ｒ’を得る。

【０１８９】

【数３８】

（４－６）　　$R' = S^{-1} R \mod p$

【０１９０】

８．証明データ検証装置１０中の乱数効果除去部１０５は、乱数記憶部１０３から先に生成した乱数ｒを取り出し、式４－７の計算を行う。

【０１９１】
【数３９】
（４－７）　　$K' = R'^{A} \mod p$
ただし$A = (r^{-1} \mod (p-1))$
【０１９２】
９．証明データ検証装置１０において用いられるアクセスチケットｔとユーザの固有情報ｅの組み合わせが正しい場合に限り、計算の結果得られたＫ’と検証用データＫが一致し、正しく検証が行われる。
【０１９３】
［実施例５］
つぎに本発明の実施例５について説明する。本実施例も実施例２の変更例である。本実施例では、ＥｌＧａｍａｌ公開鍵暗号の構成方法、アクセスチケットｔ、及び認証用素データｕ、認証用データＣの生成方法とそれぞれの満たすべき性質は、実施例２と同様である。
【０１９４】
本実施例の全体の構成を図１に示す。また、証明データ検証装置１０の構成を図４に示し、証明データ生成装置１１の構成を図６に示す。また、本実施例の証明データ検証装置１０の動作を図１２に示し、証明データ生成装置１１の動作を図２１に示す。
【０１９５】
以下、本実施例の動作について説明する。
【０１９６】
１．ユーザがアクセスすることによって、証明データ検証装置１０が起動される。
【０１９７】
２．証明データ検証装置１０は、認証用データｕ’，Ｃと、アクセスチケット公開鍵記憶部１０１に記憶されている法数ｐとを、証明データ生成装置１１中の受信データ記憶部１２１に書き込む。認証用素データ記憶部１０８には、認証用素データとしてｕが記憶され、認証用データ記憶部１０９には認証用データＣおよびｕ’が記憶されている。
【０１９８】
証明データ検証装置１０は、乱数生成部１０２によって、乱数ｒを生成し、乱数記憶部１０３に記録する。
【０１９９】
次いで、乱数効果付与部１０７は、認証用素データ記憶部１０８に記憶されているデータｕを取得して、式５－１により認証用データｕ’を計算する。
【０２００】
【数４０】
（５－１）　　$u' = u \cdot a^{r} \mod p$
【０２０１】
３．証明データ生成装置１１中の指数生成部１２３は、ユーザ固有情報記憶部１２２に記憶されているユーザの固有情報ｅと、受信データ記憶部１２１に記憶されている法数ｐを取得し、式５－２の計算を実行する。
【０２０２】
【数４１】
（５－２）　　$F(e, p)$
【０２０３】
４．証明データ生成装置１１中の証明データ生成部１２４は、指数生成部１２３で生成されたデータを用いて、式５－３の計算を実行しＲを得る。
【０２０４】
【数４２】
（５－３）　　$R = C \cdot u'^{-F(e,p)} \mod p$
【０２０５】

５．証明データ生成装置１１は、Ｒを証明データ検証装置１０の受信データ記憶部１１０に返送する。

【０２０６】

６．証明データ検証装置１０中の検証用演算部１０４は、アクセスチケット公開鍵記憶部１０１から法数ｐ、認証用データ記憶部１０９から認証用データｕ’、および、アクセスチケット記憶部１１１からアクセスチケットｔを取得して、式５－４の計算を行う。

【０２０７】

【数４３】

（５－４）　　$S = u'^{t} \mod p$

【０２０８】

７．更に、証明データ検証装置１０中の検証用演算部１０４は、受信データ記憶部１１０に記憶された証明データＲを取得し、式５－５の計算を行い、Ｒ’を得る。

【０２０９】

【数４４】

（５－５）　　$R' = S^{-1} R \mod p$

【０２１０】

８．証明データ検証装置１０中の乱数効果除去部１０５は、乱数記憶部１０３から先に生成した乱数ｒを取り出し、式５－６の計算を行う。

【０２１１】

【数４５】

（５－６）　　$K' = Y^{r} \cdot R' \mod p$

【０２１２】

９．証明データ検証装置１０において用いられるアクセスチケットｔとユーザの固有情報ｅの組み合わせが正しい場合に限り、計算の結果得られたＫ’と検証用データＫが一致し、正しく検証が行われる。

【０２１３】

［実施例６］

つぎに本発明の実施例６について説明する。本実施例においては、認証にＲＳＡ暗号を用い、また、アクセスチケットを証明データ生成時に用い、ユーザ固有情報を証明データ検証時に用いている。

【０２１４】

本発明における実施例６では、アクセス資格認証の特徴情報Ｄと、Ｄに対応する公開情報Ｅおよびｎ、関数Ｆ、ユーザの固有情報ｅは、実施例１と同様に与えられる。実施例１と同様に、Ｄをアクセスチケット秘密鍵、Ｅをアクセスチケット公開鍵と呼ぶ。

【０２１５】

本実施例の全体の構成を図２に示す。また、証明データ検証装置１０の構成を図５に示し、証明データ生成装置１１の構成を図７に示す。また、本実施例の証明データ検証装置１０の動作を図１３に示し、証明データ生成装置１１の動作を図２２に示す。

【０２１６】

図５において、証明データ検証装置１０は、アクセスチケット公開鍵記憶部１０１、乱数生成部１０２、乱数記憶部１０３、検証用演算部１０４、乱数効果除去部１０５、実行手段１０６、乱数効果付与部１０７、認証用素データ記憶部１０８、認証用データ記憶部１０９、受信データ記憶部１１０、ユーザ固有情報記憶部１１２および指数生成部１１３を含んで構成されている。

【０２１７】

図７において、証明データ生成装置１１は、受信データ記憶部１２１、ユーザ固有情報記憶部１２２、証明データ生成部１２４およびアクセスチケット記憶部１２５を含んで構成されている。

【０２１８】

なお、アクセスチケットｔは、アクセスチケット秘密鍵Ｄ、ユーザの固有情報ｅ、法数ｎ

を用い、以下の式６－１に基づいて生成される。

【０２１９】

【数４６】

（６－１）　　ｔ＝Ｄ－Ｆ（ｅ，ｎ）

つぎに本実施例の動作について説明する。

【０２２０】

１．ユーザがアクセスすることによって、証明データ検証装置１０が起動される。

【０２２１】

２．証明データ検証装置１０は、認証用データＣと、アクセスチケット公開鍵記憶部１０１に記憶されている法数ｎとを、証明データ生成装置１１中の受信データ記憶部１２１に書き込む。認証用素データ記憶部１０８には、認証用素データとしてＣ’が記憶されている。ここで、検証用データを適当なデータＫとする時、認証用素データＣ’は、データＫに対して式６－２を満たす。

【０２２２】

【数４７】

（６－２）　　$C' = K^{E} \mod n$

証明データ検証装置１０の乱数生成部１０２は乱数ｒを生成し乱数記憶部１０３に保持する。認証用データＣは、乱数記憶部１０３の乱数ｒと、アクセスチケット公開鍵記憶部１０１から取得したＥ、ｎと、認証用素データ記憶部１０８から取得したＣ’とを用い、乱数効果付与部１０７で式６－３の計算を行うことで生成される。生成された認証用データＣは、証明データ生成装置１１中の受信データ記憶部１２１に書き込まれるとともに、証明データ検証装置１１の認証用データ記憶部１０９にも記憶される。

【０２２３】

【数４８】

（６－３）　　$C = r^{E} C' \mod n$

【０２２４】

３．証明データ生成装置１１中の証明データ生成部１２４は、アクセスチケット記憶部１２５に記憶されているアクセスチケットｔを取得し、受信データ記憶部１２１に書き込まれた法数ｎのもとで式の計算を実行しＲを得る。

【０２２５】

【数４９】

（６－４）　　$R = C^{t} \mod n$

【０２２６】

４．証明データ生成装置１１はＲを証明データ検証装置１０の受信データ記憶部１１０に返送する。

【０２２７】

５．証明データ検証装置１０中の指数生成部１１３は、ユーザ固有情報記憶部１１２に記憶されているユーザの固有情報ｅと、アクセスチケット公開鍵記憶部１０１に記憶されている法数ｎとを取得し、式６－５の計算を実行する。

【０２２８】

【数５０】

（６－５）　　Ｆ（ｅ，ｎ）

【０２２９】

６．証明データ検証装置１０中の検証用演算部１０４は、指数生成部１１３で生成されたデータを用いて、式６－６の計算を行い、Ｓを得る。

【０２３０】

【数５１】

（６－６）　　$S = R C^{F(e,n)} \mod n$

【０２３１】

７．証明データ検証装置１０中の乱数効果除去部１０５は、乱数記憶部１０３から先に生

成した乱数ｒを取り出し、式６－７の計算を行う。

【０２３２】

【数５２】

（６－７）　　Ｋ’＝ｒ$^{-1}$Ｓ　ｍｏｄ　ｎ

【０２３３】

８．証明データ生成装置１１において用いられるアクセスチケットｔとユーザの固有情報ｅの組み合わせが正しい場合に限り、計算の結果得られたＫ’と検証用データＫが一致し、正しく検証が行われる。

【０２３４】

［実施例７］

つぎに本発明の実施例７について説明する。本実施例においては、認証にＥｌＧａｍａｌ暗号を用いている。また実施例６と同様に証明データ生成時にアクセスチケットを用い、証明データ検証時にユーザ固有情報を用いている。

【０２３５】

本実施例では、ＥｌＧａｍａｌ公開鍵暗号の構成方法、アクセスチケットｔ、及び認証用素データｕ，認証用データＣの生成方法とそれぞれの満たすべき性質は、実施例２と同様である。

【０２３６】

本実施例の全体の構成を図２に示す。また、証明データ検証装置１０の構成を図５に示し、証明データ生成装置１１の構成を図７に示す。また、本実施例の証明データ検証装置１０の動作を図１４に示し、証明データ生成装置１１の動作を図２３に示す。

【０２３７】

以下、本実施例の動作について説明する。

【０２３８】

１．ユーザがアクセスすることによって、証明データ検証装置１０が起動される。

【０２３９】

２．証明データ検証装置１０は、認証用データｕ’と、アクセスチケット公開鍵記憶部１０１に記憶されている法数ｐとを、証明データ生成装置１１中の受信データ記憶部１２１に書き込む。認証用素データ記憶部１０８には、認証用素データとしてｕが記憶され、認証用データ記憶部１０９には認証用データＣが記憶されている。

【０２４０】

証明データ検証装置１０は、乱数生成部１０２によって、乱数ｒを生成し、乱数記憶部１０３に記録する。

【０２４１】

次いで、乱数効果付与部１０７は、認証用素データ記憶部１０７に記憶されているデータｕを取得して、式７－１により認証用データｕ’を計算する。

【０２４２】

【数５３】

（７－１）　　ｕ’＝ｕ^{r}　ｍｏｄ　ｐ

【０２４３】

３．証明データ生成装置１１中の証明データ生成部１２４は、アクセスチケット記憶部１２５に記憶されているアクセスチケットｔを取得し、受信データ記憶部１２１に書き込まれた法数ｐのもとで式７－２の計算を実行しＲを得る。

【０２４４】

【数５４】

（７－２）　　Ｒ＝ｕ’^{t}　ｍｏｄ　ｐ

【０２４５】

４．証明データ生成装置１１は、Ｒを証明データ検証装置１０の受信データ記憶部１１０に返送する。

【０２４６】

５．証明データ検証装置１０中の指数生成部１１３は、ユーザ固有情報記憶部１１２に記憶されているユーザの固有情報ｅと、アクセスチケット公開鍵記憶部
１０１に記憶されている法数ｐを取得し、式７－３の計算を実行する。
【０２４７】
【数５５】
（７－３）　　Ｆ（ｅ，ｐ）
【０２４８】
６．証明データ検証装置１０中の検証用演算部１０４は、アクセスチケット公開鍵記憶部１０１から法数ｐ、認証用素データ記憶部１０８から認証用素データｕを取得して、式７－４の計算を行う。
【０２４９】
【数５６】
（７－４）　　$S=u'^{F(e,p)} \mod p$
【０２５０】
７．更に、証明データ検証装置１０中の検証用演算部１０４は、受信データ記憶部１１０に記憶された証明データＲを取得し、式７－５の計算を行い、Ｒ’を得る。
【０２５１】
【数５７】
（７－５）　　$R'=SR \mod p$
【０２５２】
８．証明データ検証装置１０中の乱数効果除去部１０５は、乱数記憶部１０３から先に生成した乱数ｒを取り出し、まず式７－６の計算を行う。
【０２５３】
【数５８】
（７－６）　　$v=R'^{A} \mod p$
ただし$A=(r^{-1} \mod (p-1))$
次いで、計算の結果得られたｖと、認証用データ記憶部に記憶されているＣを用いて、式７－７の計算を行う。
【０２５４】
【数５９】
（７－７）　　$K'=C \cdot v^{-1} \mod p$
【０２５５】
９．証明データ検証装置１０において用いられるアクセスチケットｔとユーザの固有情報ｅの組み合わせが正しい場合に限り、計算の結果得られたＫ’と検証用データＫが一致し、正しく検証が行われる。
【０２５６】
［実施例８］
つぎに本発明の実施例８について説明する。本実施例は実施例７の変更例である。
【０２５７】
実施例では、ＥｌＧａｍａｌ公開鍵暗号の構成方法、アクセスチケットｔ、及び認証用素データｕ、証用データＣの生成方法とそれぞれの満たすべき性質は、実施例２と同様である。
【０２５８】
本実施例の全体の構成を図２に示す。証明データ検証装置１０の構成を図５に示し、証明データ生成装置１１の構成を図７に示す。また、本実施例の証明データ検証装置１０の動作を図１５に示し、証明データ生成装置１１の動作を図２３に示す。
【０２５９】
以下、本実施例の動作について説明する。
【０２６０】
１．ユーザがアクセスすることによって、証明データ検証装置１０が起動される。

【０２６１】
２．証明データ検証装置１０は、認証用データｕ’と、アクセスチケット公開鍵記憶部１０１に記憶されている法数ｐとを、証明データ生成装置１１中の受信データ記憶部１２１に書き込む。認証用素データ記憶部１０８には、認証用素データとしてｕが記憶され、認証用データ記憶部１０９には認証用データＣが記憶されている。
【０２６２】
証明データ検証装置１０は、乱数生成部１０２によって、乱数ｒを生成し、乱数記憶部１０３に記録する。
【０２６３】
次いで、乱数効果付与部１０７は、認証用素データ記憶部１０８に記憶されているデータｕを取得して、式８－１により認証用データｕ’を計算する。
【０２６４】
【数６０】
（８－１）　　$u' = u \cdot a^{r} \mod p$
【０２６５】
３．証明データ生成装置１１中の証明データ生成部１２４は、アクセスチケット記憶部２５に記憶されているアクセスチケットｔを取得し、受信データ記憶部１２１に書き込まれた法数ｐのもとで式８－２の計算を実行しＲを得る。
【０２６６】
【数６１】
（８－２）　　$R = u'^{t} \mod p$
【０２６７】
４．証明データ生成装置１１は、Ｒを証明データ検証装置１０の受信データ記憶部１１０に返送する。
【０２６８】
５．証明データ検証装置１０中の指数生成部１１３は、ユーザ固有情報記憶部１１２に記憶されているユーザの固有情報ｅと、アクセスチケット公開鍵記憶部１０１に記憶されている法数ｐを取得し、式８－３の計算を実行する。
【０２６９】
【数６２】
（８－３）　　Ｆ（ｅ，ｐ）
【０２７０】
６．証明データ検証装置１０中の検証用演算部１０４は、アクセスチケット公開鍵記憶部１０１から法数ｐ、認証用データ記憶部１０９から認証用データｕ’を取得して、式８－４の計算を行う。
【０２７１】
【数６３】
（８－４）　　$S = u'^{F(e,\,p)} \mod p$
【０２７２】
７．更に、証明データ検証装置１０中の検証用演算部１０４は、受信データ記憶部１１０に記憶された証明データＲを取得し、式８－５の計算を行い、Ｒ’を得る。
【０２７３】
【数６４】
（８－５）　　$R' = SR \mod p$
【０２７４】
８．証明データ検証装置１０中の乱数効果除去部１０５は、乱数記憶部１０３から先に生成した乱数ｒを取り出し、まず式８－６の計算を行う。
【０２７５】
【数６５】
（８－６）　　$v = Y^{-r} \cdot R' \mod p$

次いで、計算の結果得られたｖと、認証用データ記憶部１０９に記憶されているＣを用いて、式８－７の計算を行う。

【０２７６】

【数６６】

（８－７）　　$K' = C \cdot v^{-1} \mod p$

【０２７７】

９．証明データ検証装置１０において用いられるアクセスチケットｔとユーザの固有情報ｅの組み合わせが正しい場合に限り、計算の結果得られたＫ’と検証用データＫが一致し、正しく検証が行われる。

【０２７８】

［実施例９］

つぎに本発明の実施例９について説明する。本実施例も実施例７の変更例である。本実施例でも、ＥｌＧａｍａｌ公開鍵暗号の構成方法、アクセスチケットｔ、及び認証用素データｕ，認証用データＣの生成方法とそれぞれの満たすべき性質は、実施例２と同様である。

【０２７９】

本実施例の全体の構成を図２に示す。また証明データ検証装置１０の構成を図５に示し、証明データ生成装置１１の構成を図７に示す。また、本実施例の証明データ検証装置１０の動作を図１６に示し、証明データ生成装置１１の動作を図２４に示す。

【０２８０】

以下、本実施例の動作について説明する。

【０２８１】

１．ユーザがアクセスすることによって、証明データ検証装置１０が起動される。

【０２８２】

２．証明データ検証装置１０は、認証用データｕ’、Ｃ’と、アクセスチケット公開鍵記憶部１０１に記憶されている法数ｐとを、証明データ生成装置１１中の受信データ記憶部１２１に書き込む。認証用素データ記憶部１０８には、認証用素データとしてｕおよびＣが記憶されている。

【０２８３】

証明データ検証装置１０は、乱数生成部１０２によって、乱数ｒをアクセスチケット公開鍵記憶部１０１に保持されている法数ｐより１引いた値（ｐ－１）と互いに素になるように生成し、乱数記憶部１０３に記録する。

【０２８４】

次いで、乱数効果付与部１０７は、認証用素データ記憶部１０８に記憶されているデータｕを取得して、式９－１の計算により認証用データｕ’を計算する。

【０２８５】

【数６７】

（９－１）　　$u' = u^{r} \mod p$

さらに乱数効果付与部１０７は、認証用素データ記憶部１０８に記憶されているデータＣを取得して、式９－２の計算を行う。

【０２８６】

【数６８】

（９－２）　　$C' = C^{r} \mod p$

【０２８７】

３．証明データ生成装置１１中の証明データ生成部１２４は、アクセスチケット記憶部１２５に記憶されているアクセスチケットｔを取得し、受信データ記憶部１２１に書き込まれた法数ｐのもとで式９－３の計算を実行しＲを得る。

【０２８８】

【数６９】

（９－３）　　$R = C' \cdot u'^{-t} \mod p$

【０２８９】
４．証明データ生成装置１１は、Ｒを証明データ検証装置１０の受信データ記憶部１１０に返送する。
【０２９０】
５．証明データ検証装置１０中の指数生成部１１３は、ユーザ固有情報記憶部１１２に記憶されているユーザの固有情報ｅと、アクセスチケット公開鍵記憶部１０１に記憶されている法数ｐを取得し、式９－４の計算を実行する。
【０２９１】
【数７０】
（９－４）　　Ｆ（ｅ，ｐ）
【０２９２】
６．証明データ検証装置１０中の検証用演算部１０４は、アクセスチケット公開鍵記憶部１０１から法数ｐ、認証用データ記憶部１０９から認証用データｕ’を取得して、式９－５の計算を行う。
【０２９３】
【数７１】
（９－５）　　$S=u'^{F(e,p)} \mod p$
【０２９４】
７．更に、証明データ検証装置１０中の検証用演算部１０４は、受信データ記憶部１１０に記憶された証明データＲを取得し、式９－６の計算を行い、Ｒ’を得る。
【０２９５】
【数７２】
（９－６）　　$R'=S^{-1}R \mod p$
【０２９６】
８．証明データ検証装置１０中の乱数効果除去部１０５は、乱数記憶部１０３から先に生成した乱数ｒを取り出し、式９－７の計算を行う。
【０２９７】
【数７３】
（９－７）　　$K'=R'^{A} \mod p$
ただし$A=(r^{-1} \mod (p-1))$
【０２９８】
９．証明データ検証装置１０において用いられるアクセスチケットｔとユーザの固有情報ｅの組み合わせが正しい場合に限り、計算の結果得られたＫ’と検証用データＫが一致し、正しく検証が行われる。
【０２９９】
［実施例１０］
つぎに本発明の実施例１０について説明する。本実施例も実施例７の変更例である。本実施例でも、ＥｌＧａｍａｌ公開鍵暗号の構成方法、アクセスチケットｔ、及び認証用素データｕ，認証用データＣの生成方法とそれぞれの満たすべき性質は、実施例２と同様である。
【０３００】
本実施例の全体の構成を図２に示す。また証明データ検証装置１０の構成を図５に示し、証明データ生成装置１１の構成を図７に示す。また、本実施例の証明データ検証装置１０の動作を図１７に示し、証明データ生成装置１１の動作を図２５に示す。
【０３０１】
以下、本実施例の動作について説明する。
【０３０２】
１．ユーザがアクセスすることによって、証明データ検証装置１０が起動される。
【０３０３】
２．証明データ検証装置１０は、認証用データｕ’，Ｃと、アクセスチケット公開鍵記憶

部１０１に記憶されている法数ｐとを、証明データ生成装置１１中の受信データ記憶部１２１に書き込む。認証用素データ記憶部１０８には、認証用素データとしてｕが記憶され、認証用データ記憶部１０９には認証用データＣが記憶されている。

【０３０４】

証明データ検証装置１０は、乱数生成部１０２によって、乱数ｒを生成し、乱数記憶部１０３に記録する。

【０３０５】

次いで、乱数効果付与部１０７は、認証用素データ記憶部１０８に記憶されているデータｕを取得して、式１０－１により認証用データｕ’を計算する。

【０３０６】

【数７４】

（１０－１）　$u' = u \cdot a^{r} \mod p$

【０３０７】

３．証明データ生成装置１１中の証明データ生成部１２４は、アクセスチケット記憶部１２５に記憶されているアクセスチケットｔを取得し、受信データ記憶部１２１に書き込まれた法数ｐのもとで式１０－２の計算を実行しＲを得る。

【０３０８】

【数７５】

（１０－２）　$R = C \cdot u'^{-t} \mod p$

【０３０９】

４．証明データ生成装置１１は、Ｒを証明データ検証装置１０の受信データ記憶部１１０に返送する。

【０３１０】

５．証明データ検証装置１０中の指数生成部１１３は、ユーザ固有情報記憶部１１２に記憶されているユーザの固有情報ｅと、アクセスチケット公開鍵記憶部１０１に記憶されている法数ｐを取得し、式１０－３の計算を実行する。

【０３１１】

【数７６】

（１０－３）　Ｆ（ｅ，ｐ）

【０３１２】

６．証明データ検証装置１０中の検証用演算部１０４は、アクセスチケット公開鍵記憶部１０１から法数ｐ、認証用データ記憶部１０９から認証用データｕ’を取得して、式１０－４の計算を行う。

【０３１３】

【数７７】

（１０－４）　$R = u'^{F(e,p)} \mod p$

【０３１４】

７．更に、証明データ検証装置１０中の検証用演算部１０４は、受信データ記憶部１１０に記憶された証明データＲを取得し、式１０－５の計算を行い、Ｒ’を得る。

【０３１５】

【数７８】

（１０－５）　$R' = S^{-1} R \mod p$

【０３１６】

８．証明データ検証装置１０中の乱数効果除去部１０５は、乱数記憶部１０３から先に生成した乱数ｒを取り出し、式１０－６の計算を行う。

【０３１７】

【数７９】

（１０－６）　$K' = Y^{r} \cdot R' \mod p$

【０３１８】

９．証明データ検証装置１０において用いられるアクセスチケットｔとユーザの固有情報

ｅの組み合わせが正しい場合に限り、計算の結果得られたＫ’と検証用データＫが一致し、正しく検証が行われる。

【０３１９】

［実施例１１］

つぎに本発明の実施例１１について説明する。本実施例においては、証明データを生成せずに、アクセスチケットを利用してユーザを認証するものである。

【０３２０】

本実施例の構成を図３に示す。また、本実施例の検証装置の構成例を図２６に示し、その動作を図２７に示す。

【０３２１】

図２６において、検証装置１０は、アクセスチケット公開暗号鍵記憶部１０１、検証演算部１０４、実行部１０６、認証用データ記憶部１０９および指数演算部１１３を含んで構成されている。この検証装置１０にはアクセスチケット記憶部１１１およびユーザ固有情報記憶部１１２からアクセスチケットおよびユーザ固有情報がそれぞれ入力される。

【０３２２】

以下、本実施例を詳細に説明する。

【０３２３】

本発明における実施例１１では、アクセス資格認証の特徴情報Ｄと、Ｄに対応する公開情報Ｅおよびｎ、ユーザの固有情報ｅは、実施例１と同様に与えられる。実施例１と同様に、Ｄをアクセスチケット秘密鍵、Ｅをアクセスチケット公開鍵と呼ぶ。

【０３２４】

アクセスチケットｔは、アクセス資格認証の特徴情報Ｄおよびユーザの固有情報ｅとを組み合わせて生成される。アクセスチケットの生成は、他の実施例と同様に、関数Ｆ、法数ｎを用い、式１１－１に基づいて行われる。

【０３２５】

【数８０】

（１１－１）　　ｔ＝Ｄ－Ｆ（ｅ，ｎ）

また、式１１－２のように生成してもよい。

【０３２６】

【数８１】

（１１－２）　　ｔ＝Ｅｎｃｒｙｐｔ（Ｄ，ｅ）

ここで、Ｅｎｃｒｙｐｔ（ｘ，ｙ）は、ｘをｙで暗号化することを意味する。この場合、ユーザの固有情報ｅは、慣用暗号の秘密鍵であり、アクセスチケットｔは、アクセス資格認証の特徴情報Ｄをユーザの固有情報ｅで暗号化したものになる。また、ｅを公開鍵暗号の秘密鍵とし、公開鍵をｄとして、式１１－３のように、ｘをｄで暗号化してもよい。

【０３２７】

【数８２】

（１１－３）　　ｔ＝Ｅｎｃｒｙｐｔ（Ｄ，ｄ）

つぎに本実施例の動作について詳述する。

【０３２８】

１．ユーザがアクセスすることによって、検証装置１０が起動される。

【０３２９】

２．検証装置１０の認証用データ記憶部１０９には、認証用データとしてＣが記憶されている。ここで、検証用データを適当なデータＫとする時、認証用データＣは、データＫに対して式１１－４を満たす。

【０３３０】

【数８３】

（１１－４）　　$C=K^{E} \mod n$

【０３３１】

３．アクセスチケットが式１１－１に基づいて計算されている場合、検証装置１０の指数

生成部１１３は、ユーザ固有情報記憶部１１２に記憶されているユーザの固有情報ｅと、アクセスチケット公開鍵記憶部１０１に記憶されている法数ｎとを取得し、式１１－５の計算を実行する。

【０３３２】

【数８４】

（１１－５）　Ｆ（ｅ，ｎ）

【０３３３】

４．検証装置１０の検証用演算部１０４は、指数生成部１１３で生成されたデータを用いて、式１１－６の計算を行い、Ｓを得る。

【０３３４】

【数８５】

（１１－６）　$S = C^{F(e,n)} \mod n$

【０３３５】

５．更に、検証装置１０の検証用演算部１０４は、アクセスチケット記憶部１１１に記憶されているアクセスチケットｔを取得し、アクセスチケット公開鍵記憶部１０１に記憶されている法数ｎのもとで式１１－７の計算を実行しＫ’を得る。

【０３３６】

【数８６】

（１１－７）　$K' = SC^{t} \mod n$

【０３３７】

６．検証装置１０に与えられるアクセスチケットｔとユーザの固有情報ｅの組み合わせが正しい場合に限り、計算の結果得られたＫ’と検証用データＫが一致し、正しく検証が行われる。

【０３３８】

また、アクセスチケットが式１１－２または式１１－３に基づいている場合は、上記３、４、５のステップを実行せず、つぎの３’、４’のステップを実行する。

【０３３９】

３’．検証装置１０の検証用演算部１０４は、式１１－８を実行する。ここで、Ｄｅｃｒｙｐｔ（ｘ，ｙ）は、ｘを鍵ｙで復号することを意味する。

【０３４０】

【数８７】

（１１－８）　Ｄｅｃｒｙｐｔ（ｔ，ｅ）

【０３４１】

４’．更に、検証装置１０の検証用演算部１０４は、式１１－９の計算を行い、Ｋ’を得る。

【０３４２】

【数８８】

（１１－９）　$K' = C^{Decrypt(t,e)} \mod n$

【０３４３】

【０３４４】

【発明の効果】

以上の説明から明らかなように，本発明によれば、証明用補助情報（アクセスチケット）を導入することにより、アクセス資格認証の特徴情報とユーザ固有情報とを独立させることができ、したがってプロテクト側もユーザ側も、１つの固有情報を準備しておくだけですむ。アクセスチケットは、特定のユーザの固有情報とアクセス資格認証の特徴情報とに基づいて計算されるデータであり、また、ユーザ固有情報を知らずに、アクセスチケットからアクセス資格認証の特徴情報を計算することは困難である。そして、ユーザ固有情報とアクセスチケットとの正しい組み合わせ、すなわち、ユーザ固有情報と該ユーザ固有情報に基づいて計算されたアクセスチケットの組み合わせが入力された場合に限って、正しい証明用データが計算される。したがってユーザはあらかじめ固有情報を保持し、プログ

ラム作成者等のプロテクト者はユーザが所持する固有情報とは独立にアクセス資格認証の特徴情報を用意し、アクセスチケットをユーザの固有情報とアプリケーションプログラムの作成等に使用したアクセス資格認証の特徴情報とに応じて作成し、配布することにより、実行制御等のユーザのアクセス資格の認証を行うことができる。

【図面の簡単な説明】

【図１】本発明の実施例１、２、３、４、および５における全体の構成を示す図である。

【図２】本発明の実施例６、７、８、９、および１０における全体の構成を示す図である。

【図３】本発明の実施例１１における全体の構成を示す図である。

【図４】上述実施例１、２、３、４、および５における証明データ検証装置の構成を示す図である。

【図５】上述実施例６、７、８、９、および１０における証明データ検証装置の構成を示す図である。

【図６】上述実施例１、２、３、４、および５における証明データ生成装置の構成を示す図である。

【図７】上述実施例６、７、８、９、および１０における証明データ生成装置の構成を示す図である。

【図８】上述実施例１における証明データ検証装置の動作を示す図である。

【図９】上述実施例２における証明データ検証装置の動作を示す図である。

【図１０】上述実施例３における証明データ検証装置の動作を示す図である。

【図１１】上述実施例４における証明データ検証装置の動作を示す図である。

【図１２】上述実施例５における証明データ検証装置の動作を示す図である。

【図１３】上述実施例６における証明データ検証装置の動作を示す図である。

【図１４】上述実施例７における証明データ検証装置の動作を示す図である。

【図１５】上述実施例８における証明データ検証装置の動作を示す図である。

【図１６】上述実施例９における証明データ検証装置の動作を示す図である。

【図１７】上述実施例１０における証明データ検証装置の動作を示す図である。

【図１８】上述実施例１における証明データ生成装置の動作を示す図である。

【図１９】上述実施例２、および３における証明データ生成装置の動作を示す図である。

【図２０】上述実施例４における証明データ生成装置の動作を示す図である。

【図２１】上述実施例５における証明データ生成装置の動作を示す図である。

【図２２】上述実施例６における証明データ生成装置の動作を示す図である。

【図２３】上述実施例７、および８における証明データ生成装置の動作を示す図である。

【図２４】上述実施例９における証明データ生成装置の動作を示す図である。

【図２５】上述実施例１０における証明データ生成装置の動作を示す図である。

【図２６】上述実施例１１における検証装置の構成を示す図である。

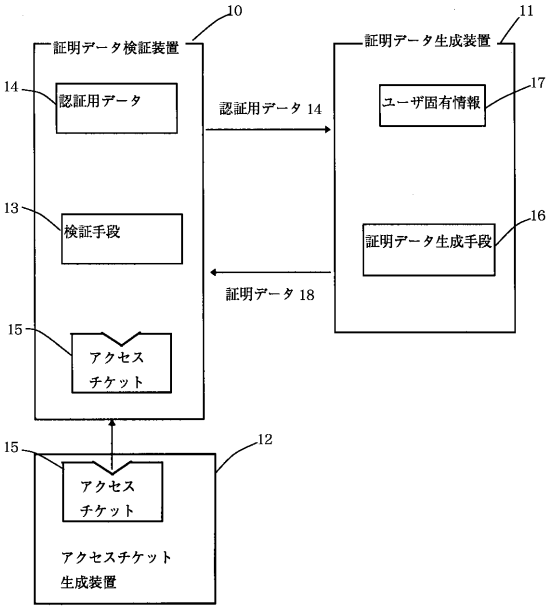
【図２７】上述実施例１１における検証装置の動作を示す図である。

【符号の説明】

１０　証明データ検証装置（検証装置）
１１　証明データ生成装置
１２　アクセスチケット生成装置
１３　検証手段
１４　証明用データ
１５　アクセスチケット
１６　証明データ生成手段
１７　ユーザ固有情報
１０１　アクセスチケット公開鍵記憶部
１０２　乱数生成部
１０３　乱数記憶部
１０４　検証用演算部

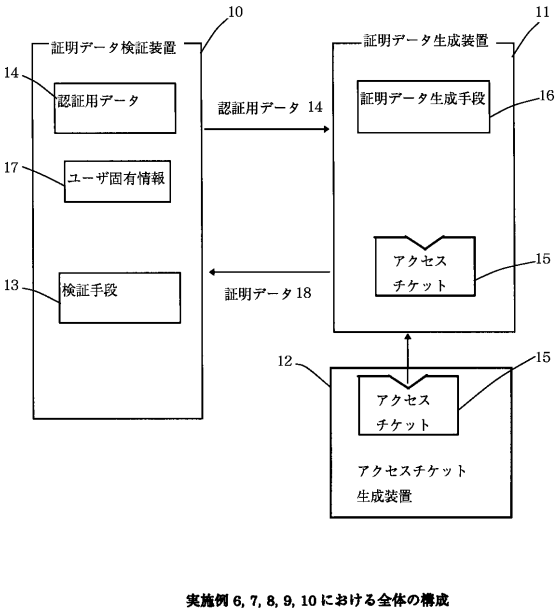
１０５　乱数効果除去部
１０６　実行手段
１０７　乱数効果付与部
１０８　認証用素データ記憶部
１０９　認証用データ記憶部
１１０　受信データ記憶部
１１１　アクセスチケット記憶部
１１２　ユーザ固有情報記憶部
１１３　指数生成部
１２１　受信データ記憶部
１２２　ユーザ固有情報記憶部
１２３　指数生成部
１２４　証明データ生成部
１２５　アクセスチケット記憶部

【図１】



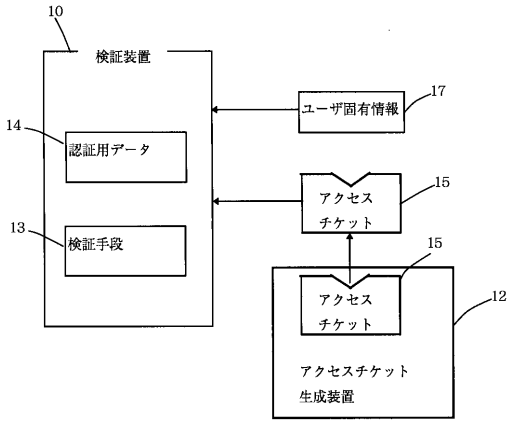
実施例 1, 2, 3, 4, 5 における全体の構成

【図２】



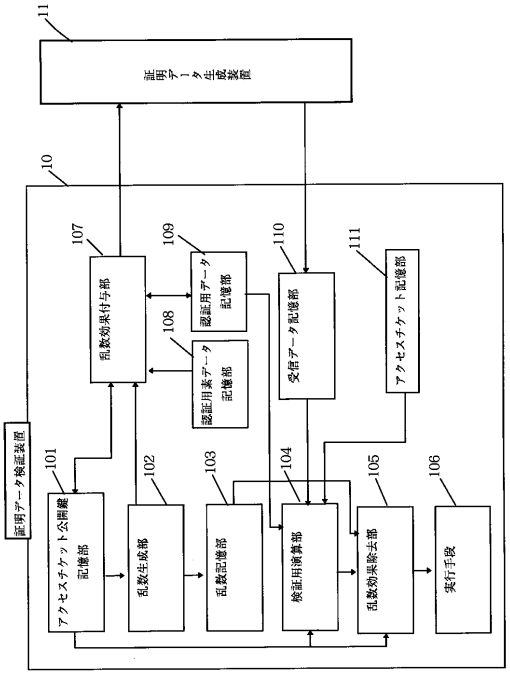
実施例 6, 7, 8, 9, 10 における全体の構成

【図３】



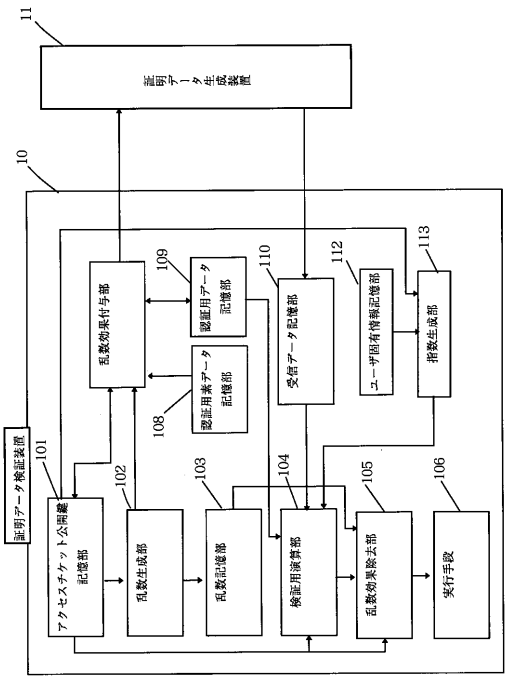
実施例 11 における全体の構成

【図４】



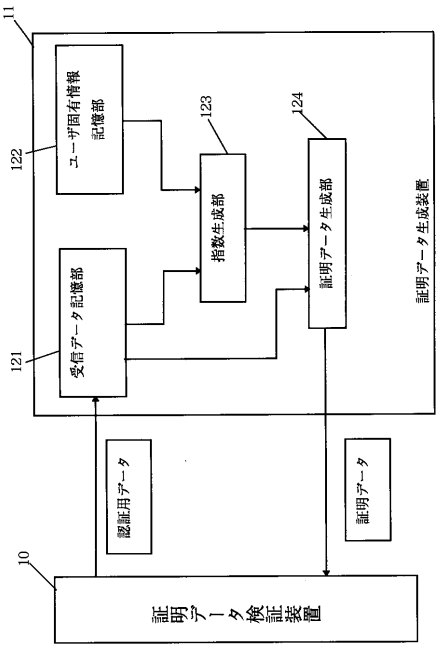
実施例 1, 2, 3, 4, 5 における検証装置の構成

【図５】



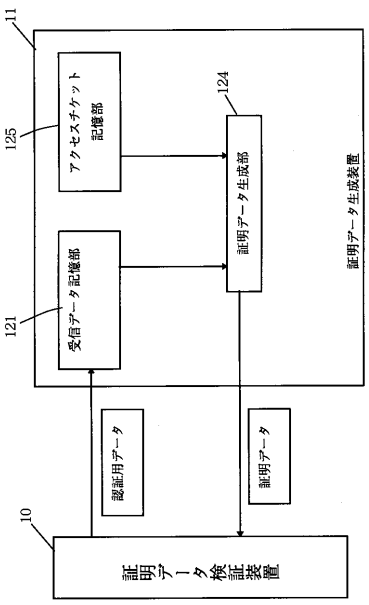
実施例 6, 7, 8, 9, 10 における検証装置の構成

【図６】



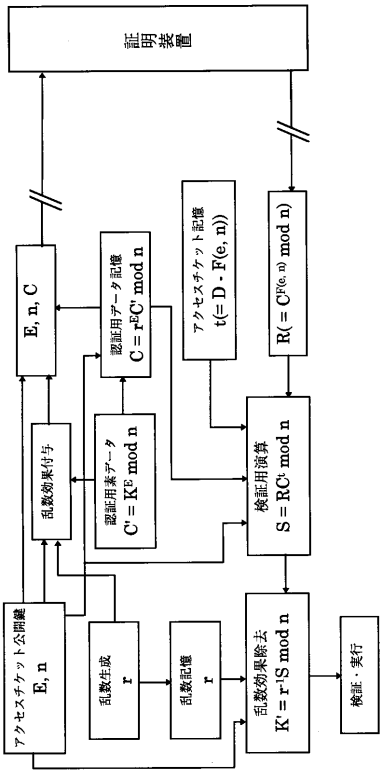
実施例1、2、3、4、5の証明装置の構成

【図７】



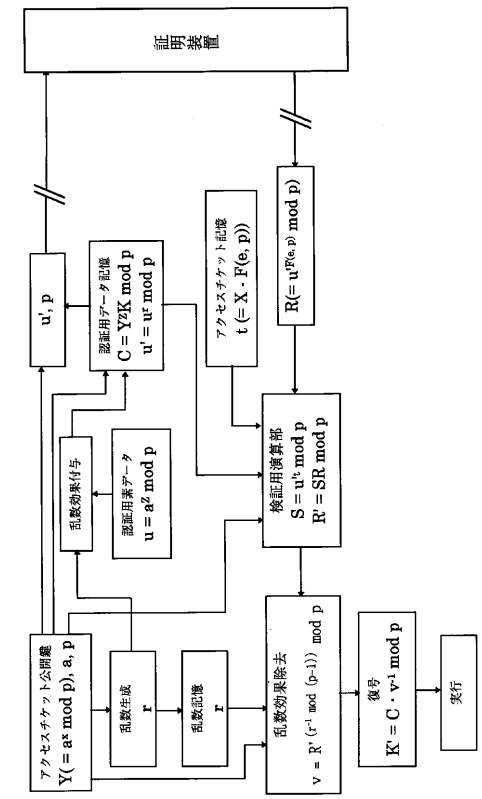
実施例 6, 7, 8, 9, 10 の証明装置の構成

【図８】



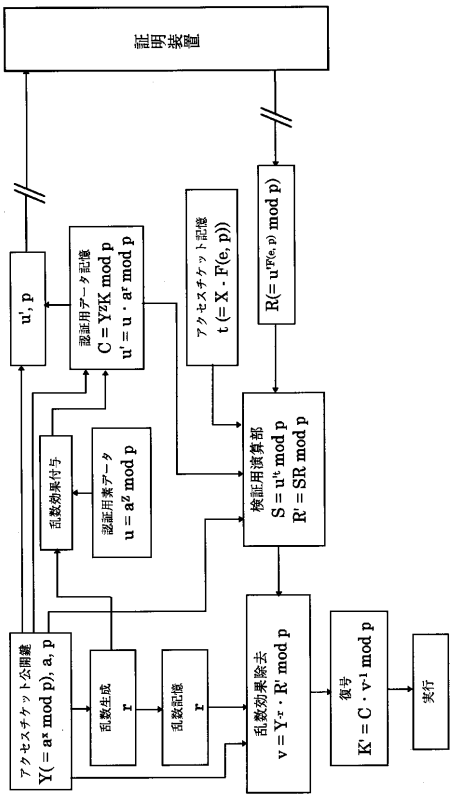
実施例 1 における検証装置の動作

【図９】



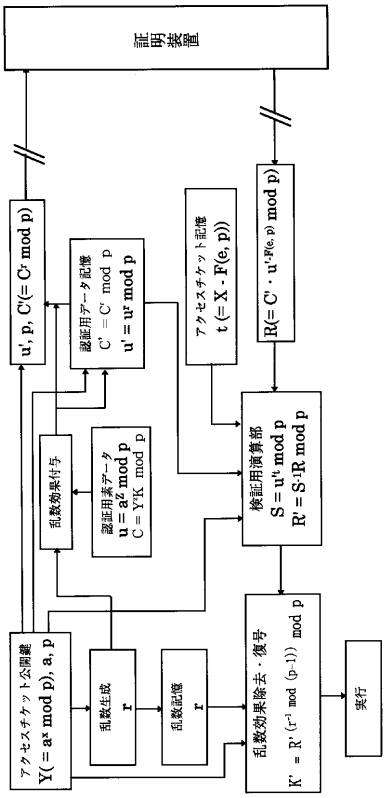
実施例 2 における検証装置の動作

【図１０】



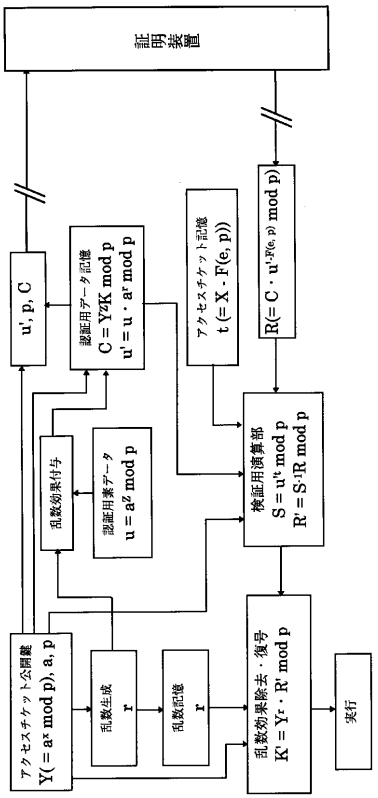
実施例 3 における検証装置の動作

【図１１】



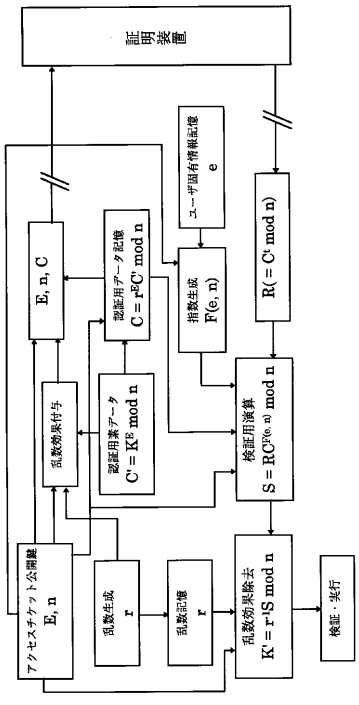
実施例４における検証装置の動作

【図１２】



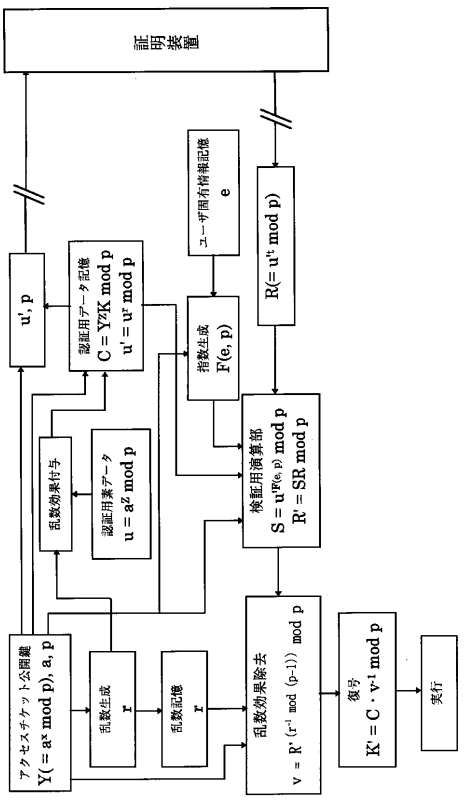
実施例５における検証装置の動作

【図１３】



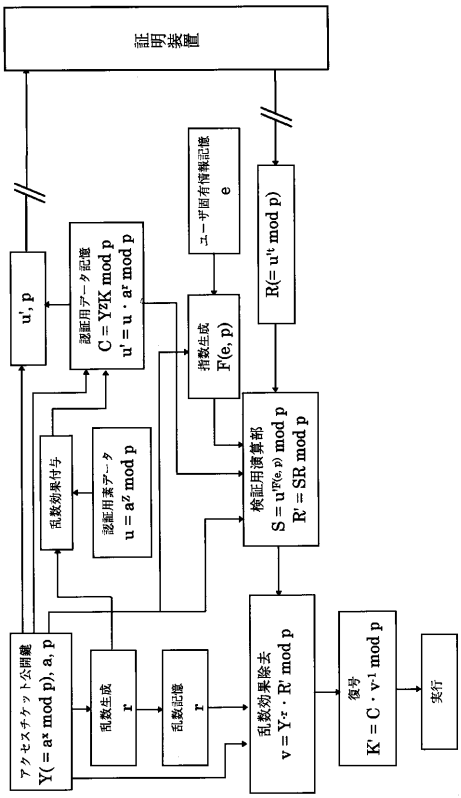
実施例６における検証装置の動作

【図１４】



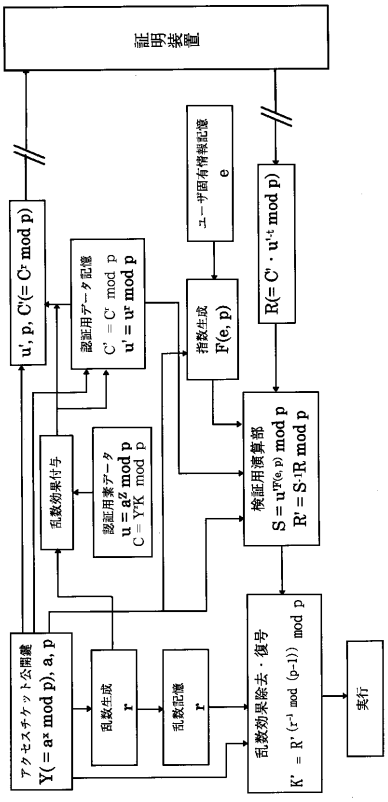
実施例７における検証装置の動作

【図１５】



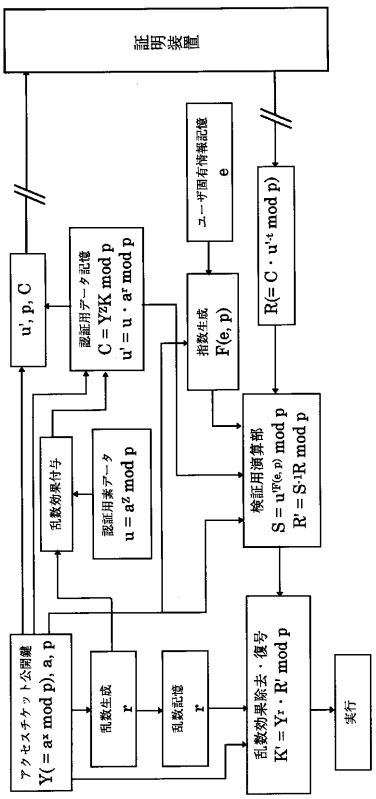
実施例８における検証装置の動作

【図１６】



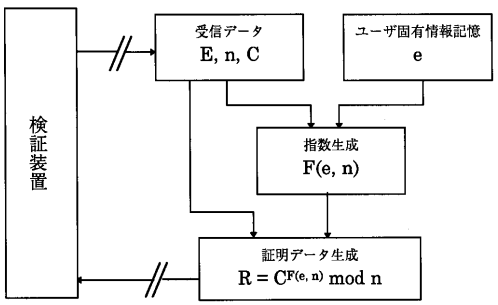
実施例９における検証装置の動作

【図１７】



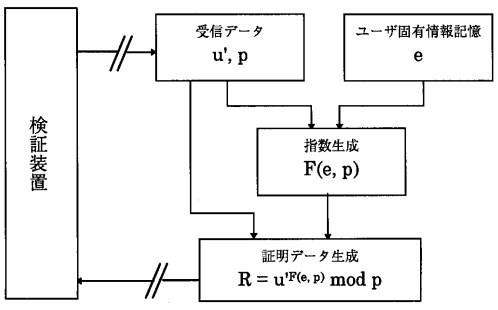
実施例１０における検証装置の動作

【図１８】



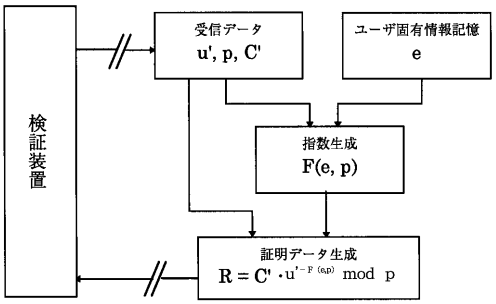
実施例１における証明装置の動作

【図１９】



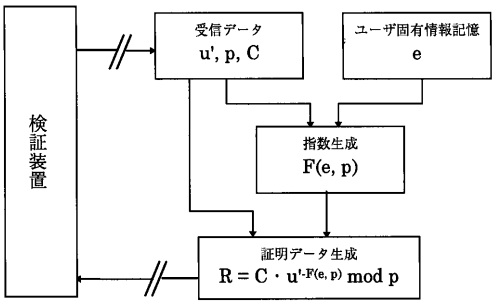
実施例２、３における証明装置の動作

【図２０】



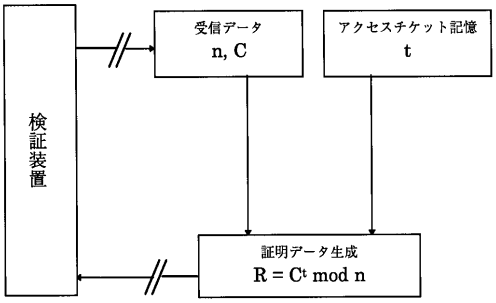
実施例４における証明装置の動作

【図２１】



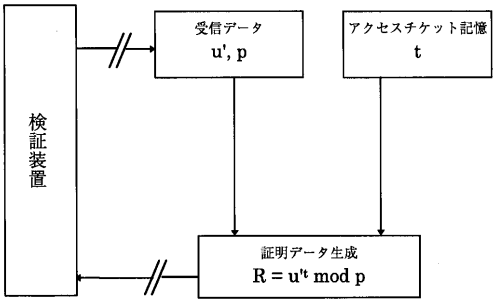
実施例５における証明装置の動作

【図２２】



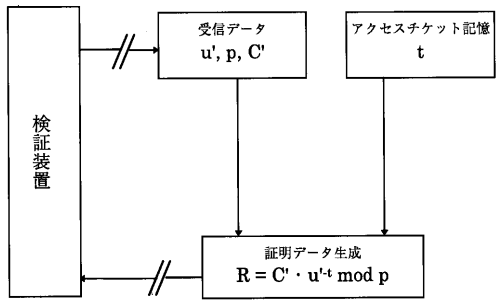
実施例６における証明装置の動作

【図２３】



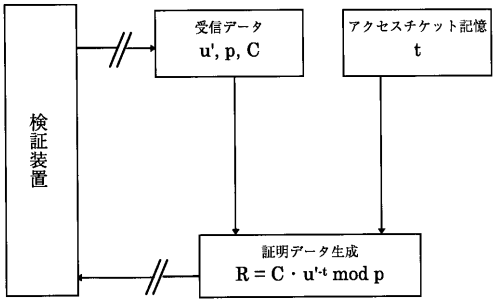
実施例７、８における証明装置の動作

【図２４】



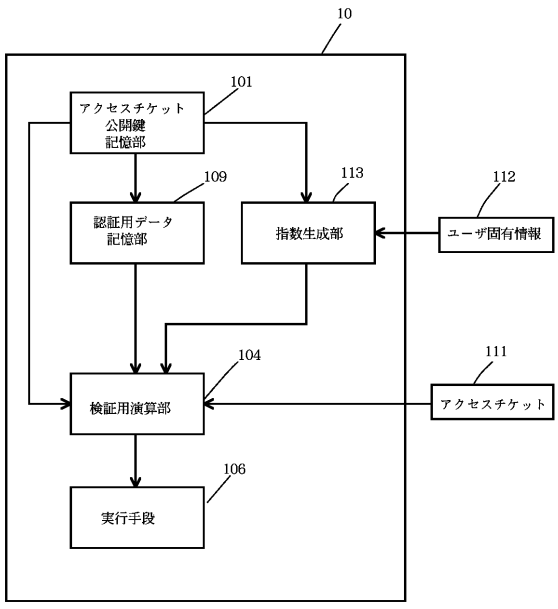
実施例９における証明装置の動作

【図２５】

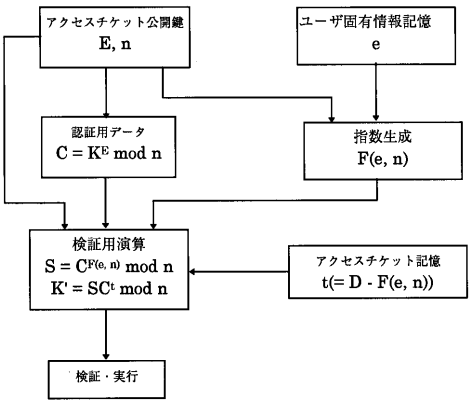


実施例１０における証明装置の動作

【図２６】



【図２７】



実施例11における検証装置の動作

フロントページの続き

審査官　青木　重徳

(56)参考文献　特開平０７－２８１５９５（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
申吉浩，小島俊一，“デジタル著作権流通の為のアクセス制御スキーム”，電子情報通信学会技術研究報告（ＩＳＥＣ９７－２０），日本，社団法人電子情報通信学会，１９９７年　7月１８日，Ｖｏｌ．９７，Ｎｏ．１８１，ｐ．６５－７１

(58)調査した分野(Int.Cl.[7]，ＤＢ名)

H04L 9/32
G06F 9/06 550
G06F 12/14 320
G09C 1/00 640