(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2010-4288
(P2010-4288A)
(43)公開日　平成22年1月7日(2010.1.7)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601D	5J104
		H04L	9/00	601E	

審査請求 未請求　請求項の数 10　ＯＬ　（全 18 頁）

(21)出願番号　特願2008-160839 (P2008-160839)
(22)出願日　平成20年6月19日 (2008.6.19)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100121706
弁理士　中尾　直樹
(74)代理人　100066153
弁理士　草野　卓
(74)代理人　100128705
弁理士　中村　幸雄
(72)発明者　知加良　盛
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5J104 AA16　EA23　EA26　PA07

(54)【発明の名称】秘密情報送信システム、秘密情報送信方法、秘密情報管理サーバ、暗号装置、秘密情報送信プログラム

(57)【要約】
【課題】本発明は、ＩＤベース暗号において利用するマスターシークレットと秘密情報を管理する秘密情報管理サーバが、ＩＤベース暗号を利用して、秘密情報を暗号装置に送信する秘密情報送信システムを提供することを目的とする。
【解決手段】本発明の秘密情報送信システムは、ＩＤベース暗号において利用するマスターシークレットと秘密情報を管理する秘密情報管理サーバが、秘密情報管理サーバに通信ネットワークを介して接続している暗号装置に秘密情報を送信する。暗号装置は、秘密情報管理サーバのＩＤ情報に基づき共通鍵ｋを生成し、リクエスト情報を第二の共通鍵ｋによって暗号化する。秘密情報管理サーバは、秘密情報管理サーバのＩＤ情報に基づき共通鍵ｋを生成し、リクエスト情報を復号する。リクエスト情報から得た第一の共通鍵r_{com}を用いて、レスポンス情報を暗号化する。
【選択図】図２

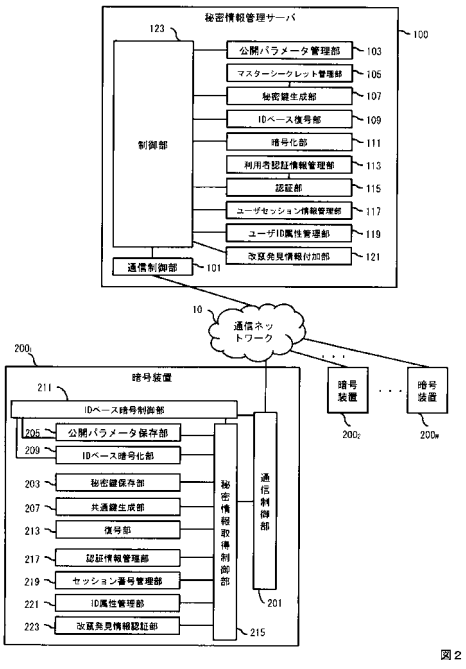

図２

【特許請求の範囲】
【請求項１】
ＩＤベース暗号において利用するマスターシークレットと秘密情報を管理する秘密情報管理サーバが、該秘密情報管理サーバに通信ネットワークを介して接続している暗号装置に該秘密情報を送信する秘密情報送信システムにおいて、
該暗号装置は、該秘密情報管理サーバの公開パラメータを保存する公開パラメータ保存部と、
第一の共通鍵r_{com}を生成する共通鍵生成部と、
乱数を生成し、該乱数と該公開パラメータと該秘密情報管理サーバのＩＤ情報に基づき第二の共通鍵ｋ及び補助鍵ｃを生成し、該秘密情報の種別を特定する秘密情報要求種別と該第一の共通鍵r_{com}を含むリクエスト情報を該第二の共通鍵ｋによって暗号化するＩＤベース暗号化部と、
該秘密情報管理サーバに暗号化された該リクエスト情報及び該補助鍵ｃを送信し、該秘密情報管理サーバから該秘密情報を含む暗号化されたレスポンス情報を受信する通信制御部と、
暗号化された該レスポンス情報を該第一の共通鍵r_{com}を用いて復号する復号部を有し、
該秘密情報管理サーバは、該公開パラメータを管理する公開パラメータ管理部と、
該マスターシークレットと該秘密情報管理サーバのＩＤ情報に基づき秘密鍵TA_{scr}を生成する秘密鍵生成部と、
該秘密鍵TA_{scr}と該補助鍵ｃに基づき該第二の共通鍵ｋを生成し、該第二の共通鍵ｋによって暗号化された該リクエスト情報を復号するＩＤベース復号部と、
該リクエスト情報から得た該第一の共通鍵r_{com}を用いて、該レスポンス情報を暗号化する暗号化部と、
該暗号装置から暗号化された該リクエスト情報及び該補助鍵ｃを受信し、該暗号装置に暗号化された該レスポンス情報を送信する通信制御部を有する、
ことを特徴とする秘密情報送信システム。
【請求項２】
請求項１記載の秘密情報送信システムであって、
該秘密情報が該暗号装置間のＩＤ情報に基づく暗号処理において利用するＩＤベース暗号の復号鍵を生成するために用いる秘密鍵USR_{scr}又はＩＤ情報に基づく署名処理において利用するＩＤベース署名用の署名鍵を生成するために用いる秘密鍵USR'_{scr}であり、
該秘密情報管理サーバの該秘密鍵生成部は、該マスターシークレットと該暗号装置の利用者のＩＤ情報に基づき該秘密鍵USR_{scr}又はUSR'_{scr}を生成する、
ことを特徴とする秘密情報送信システム。
【請求項３】
請求項１または２記載の秘密情報送信システムであって、
時刻情報を用いたセッション番号を管理するセッション番号管理部を有し、
該ＩＤベース暗号化部は、乱数を生成し、該乱数と該公開パラメータと該秘密情報管理サーバのＩＤ情報と該セッション番号に基づき第二の共通鍵ｋ及び補助鍵ｃを生成し、該第一の共通鍵r_{com}と該秘密情報を特定する秘密情報要求種別を含むリクエスト情報を該第二の共通鍵ｋによって暗号化し、
該暗号装置の該通信制御部は、該秘密情報管理サーバに暗号化された該リクエスト情報、該補助鍵ｃ及び該セッション番号を送信し、該秘密情報管理サーバから該秘密情報を含む暗号化されたレスポンス情報及び該セッション番号を受信し、
該秘密情報管理サーバは、利用者のＩＤ情報と該セッション番号を管理するユーザセッション情報管理部を有し、
該秘密鍵生成部は、該マスターシークレットと該秘密情報管理サーバのＩＤ情報と該セッション番号に基づき秘密鍵TA_{scr}を生成し、

該秘密情報管理サーバの該通信制御部は、該暗号装置から暗号化された該リクエスト情報、該補助鍵ｃ及び該セッション番号を受信し、該暗号装置に暗号化された該レスポンス情報及び該セッション番号を送信する、

ことを特徴とする秘密情報送信システム。

【請求項４】

請求項１から３の何れかに記載の秘密情報送信システムであって、

該暗号装置は、予め該秘密情報管理サーバに登録している該利用者の認証情報を管理する認証情報管理部を有し、

該リクエスト情報は該認証情報を含み、

該秘密情報管理サーバは、利用者の認証情報を管理する利用者認証情報管理部と、

該リクエスト情報に含まれる該認証情報と利用者認証情報管理部で管理される認証情報に基づき認証を行う認証部を有する、

ことを特徴とする秘密情報送信システム。

【請求項５】

請求項１から４の何れかに記載の秘密情報送信システムであって、

該秘密鍵生成部は、該マスターシークレットとは異なる他のマスターシークレットと該秘密情報管理サーバのＩＤ情報に基づいて秘密鍵管理サーバの署名鍵ＴＡ’$_{scr}$を生成し、又は、該秘密鍵生成部は、該マスターシークレットと該秘密情報管理サーバのＩＤ情報に予め定められた署名用の識別子を付加した情報に基づいて秘密鍵管理サーバの署名鍵ＴＡ”$_{scr}$を生成し、

該秘密情報管理サーバは、該署名鍵ＴＡ’$_{scr}$と暗号化されたレスポンス情報を含む情報と該公開パラメータに基づき、又は、ＴＡ”$_{scr}$と暗号化されたレスポンス情報を含む情報と該公開パラメータに基づき、署名を生成し、暗号化されたレスポンス情報を含む情報に署名を付加する改竄発見情報付加部を有し、

該秘密情報管理サーバの該通信制御部は、該暗号装置に暗号化された該レスポンス情報を含む情報に署名を付加した情報を送信する、

該暗号装置の該通信制御部は、該秘密情報管理サーバから暗号化された該レスポンス情報を含む情報に署名を付加した情報を受信し、

該暗号装置は、暗号化された該レスポンス情報を含む情報と該署名と該公開パラメータと該秘密情報管理サーバのＩＤ情報に基づいて、又は、暗号化された該レスポンス情報を含む情報と該署名と該公開パラメータと該秘密情報管理サーバのＩＤ情報に予め定められた署名用の識別子を付加した情報に基づいて、署名の検証を行う改竄発見情報認証部を有する、

ことを特徴とする秘密情報送信システム。

【請求項６】

ＩＤベース暗号において利用するマスターシークレットと秘密情報を管理する秘密情報管理サーバが、該秘密情報管理サーバに通信ネットワークを介して接続している暗号装置に該秘密情報を送信する秘密情報送信方法において、

該暗号装置は、乱数を生成し、該乱数と公開バラメータ保存部に保存されている公開パラメータと該秘密情報管理サーバのＩＤ情報に基づき第二の共通鍵ｋ及び補助鍵ｃを生成し、該秘密情報の種別を特定する秘密情報要求種別と共通鍵生成部で生成される第一の共通鍵ｒ$_{com}$を含むリクエスト情報を該第二の共通鍵ｋによって暗号化するＩＤベース暗号化ステップと、

該暗号装置は、暗号化された該リクエスト情報及び該補助鍵ｃを該通信ネットワークを介して該秘密情報管理サーバへ送信するステップと、

該秘密情報管理サーバは、暗号化された該リクエスト情報及び該補助鍵ｃを受信するステップと、

該秘密情報管理サーバは、該マスターシークレットと該秘密情報管理サーバのＩＤ情報に基づき秘密鍵ＴＡ$_{scr}$を生成する秘密鍵生成ステップと、

該秘密情報管理サーバは、該秘密鍵ＴＡ$_{scr}$と該補助鍵ｃに基づき該第二の共通鍵

ｋを生成し、該第二の共通鍵ｋによって暗号化された該リクエスト情報を復号するＩＤベース復号ステップと、

該秘密情報管理サーバは、該リクエスト情報から得た該第一の共通鍵r_{com}を用いて、該秘密情報を含むレスポンス情報を暗号化する暗号化ステップと、

該秘密情報管理サーバは、暗号化された該レスポンス情報を該通信ネットワークを介して該暗号装置へ送信するステップと、

該暗号装置は、暗号化された該レスポンス情報を受信するステップと、

該暗号装置は、該レスポンス情報を該第一の共通鍵r_{com}を用いて復号する復号ステップと、

を有する秘密情報送信方法。

【請求項７】

請求項６記載の秘密情報送信方法であって、

該秘密情報が該暗号装置間のＩＤベース情報に基づく暗号処理において利用するＩＤベース暗号の復号鍵を生成するために用いる秘密鍵USR_{scr}又はＩＤ情報に基づく署名処理において利用するＩＤベース署名のＩＤベース署名用署名鍵を生成するために用いる秘密鍵USR'_{scr}であり、

該マスターシークレットと該暗号装置の利用者のＩＤ情報に基づき該秘密鍵USR'_{scr}又はUSR'_{scr}を生成する暗号装置間秘密鍵生成ステップを有する

ことを特徴とする秘密情報送信方法。

【請求項８】

通信ネットワークを介して暗号装置と接続しているＩＤベース暗号において利用するマスターシークレットと秘密情報を管理する秘密情報管理サーバであって、

該秘密情報管理サーバの公開パラメータを管理する公開パラメータ管理部と、

該マスターシークレットと該秘密情報管理サーバのＩＤ情報に基づき秘密鍵TA_{scr}を生成する秘密鍵生成部と、

該秘密鍵TA_{scr}と補助鍵ｃから第二の共通鍵ｋを生成し、該暗号装置で該第二の共通鍵ｋによって暗号化されたリクエスト情報（秘密情報の種別を特定する秘密情報要求種別と該暗号装置で生成した第一の共通鍵r_{com}を含む）を復号するＩＤベース復号部と、

該リクエスト情報から得た該第一の共通鍵r_{com}を用いて、該秘密情報を含むレスポンス情報を暗号化する暗号化部と、

該暗号装置から暗号化された該リクエスト情報及び該補助鍵ｃを受信し、該暗号装置に暗号化された該レスポンス情報を送信する通信制御部と、

を有する秘密情報管理サーバ。

【請求項９】

ＩＤベース暗号において利用するマスターシークレットと秘密情報を管理する秘密情報管理サーバに通信ネットワークを介して接続している暗号装置であって、

該秘密情報管理サーバの公開パラメータを保存する公開パラメータ保存部と、

第一の共通鍵r_{com}を生成する共通鍵生成部と、

乱数を生成し、該乱数と該公開パラメータと該秘密情報管理サーバのＩＤ情報に基づき第二の共通鍵ｋ及び補助鍵ｃを生成し、該秘密情報の種別を特定する秘密情報要求種別と該第一の共通鍵r_{com}を含むリクエスト情報を該第二の共通鍵ｋによって暗号化するＩＤベース暗号化部と、

該秘密情報管理サーバに暗号化された該リクエスト情報及び該補助鍵ｃを送信し、該秘密情報管理サーバから該秘密情報を含む暗号化されたレスポンス情報を受信する通信制御部と、

暗号化された該レスポンス情報を該第一の共通鍵r_{com}を用いて復号する復号部と、

を有する暗号装置。

【請求項１０】

請求項６または７に記載された方法をコンピュータに実行させるための秘密情報送信プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ＩＤベース暗号において利用するマスターシークレットと秘密情報を管理するサーバから通信ネットワークを介して暗号装置に秘密情報を送信することを目的とした秘密情報送信システム、秘密情報送信方法、秘密情報管理サーバ、暗号装置、秘密情報送信プログラムに関する。

【背景技術】

【０００２】

ＩＤ情報に基づく暗号技術（以下「ＩＤベース暗号」という）が提案されている（非特許文献１、非特許文献２）。図１を用いてＩＤベース暗号について説明する。秘密情報管理サーバ１００は、ペアリング演算に利用できる楕円曲線を決定し、楕円曲線上のベースポイントである楕円点Ｐを決定する。秘密情報管理サーバは、ベースポイントＰに対してマスターシークレットｓを用いて楕円スカラー倍（楕円曲線上のｓ倍算）を行った楕円曲線上の点ｓ・Ｐを計算する。秘密情報管理サーバ１００は、公開パラメータとして、Ｐとｓ・Ｐを公開する。暗号装置２００_{2}から暗号装置２００_{1}へ送信する情報を暗号化する場合、暗号装置２００_{2}は、乱数r_{id}を生成し、この乱数r_{id}と暗号装置２００_{1}の利用者のＩＤ情報を楕円曲線上の点に変換した情報$ＩＤ_{２００１}$からペアリング演算ｅ（）を利用して、鍵ｋを生成する。

【０００３】

$$k=e(r_{id}\cdot ID_{2001},s\cdot P)$$

なお、ペアリング演算は、以下の性質を持つ。なお、ここでは“ａ・Ｐ”は楕円曲線上の点Ｐのａ倍算を行った結果であることを示す。“ａ・Ｐ”の情報から、演算の元情報となっているａ及びＰが直接分かるわけではない。また、演算子“^”は、“ａ^ｂ”でａをｂでべき乗することを表す演算子である。

【０００４】

e(P,Q+R) = e(P,Q)e(P,R)
e(P+Q,R) = e(P,R)e(Q,R)
e(P,Q+Q) = e(P,Q)e(P,Q) = e(P,Q)^2
e(P+P,Q) = e(P,Q)e(P,Q) = e(P,Q)^2

楕円スカラー倍：（楕円曲線上の点のｎ倍算）は以下のように表される。

【０００５】

P+P+・・・+P=nP
e(a・P,b・Q)=e(b・P,a・Q)

さらに以下のような性質が得られ、暗号、署名プロトコルで利用される。

【０００６】

e(P,nQ) = e(P,Q)^n
e(nP,Q) = e(P,Q)^n
e(aP,bQ) = e(P,Q)^ab
e(P,-Q) = e(P,Q)^(-1)
e(P,Q)e(P,-Q) = 1

この鍵ｋを用いて、暗号化した情報をＥＲＥＱとする。ＥＲＥＱとr_{id}・Ｐを暗号装置２００_{1}へ送信する。暗号装置２００_{1}は、秘密情報管理サーバ１００へ秘密鍵ｓ・$ＩＤ_{２００１}$を要求し、取得する。暗号装置２００_{1}は、秘密鍵ｓ・$ＩＤ_{２００１}$とr_{id}・Ｐからペアリング演算ｅ（）を利用して、鍵ｋを生成する。

【０００７】

$$k=e(s\cdot ID_{2001},\ r_{id}\cdot P)$$

この鍵ｋを使用して暗号化された情報ＥＲＥＱを復号する。$s\cdot ID_{2001}$は暗号装置２００

$_1$以外はしらないため、暗号装置間の通信を盗聴等したとしても、鍵ｋを得ることはできない。

【０００８】

ここで、秘密情報管理サーバ１００から暗号装置２００$_1$への秘密鍵ｓ・ＩＤ$_{2001}$の配送はＨＴＴＰＳにて行うことが提案されている（非特許文献３）。ＨＴＴＰＳについては、非特許文献４に詳しく説明されている。

【非特許文献１】笠原正雄、境隆一著、「暗号　ネットワーク社会の安全を守る鍵」、共立出版、２００２、p.81-101

【非特許文献２】Identity-based encryption from the Weil pairing, D.Boneh and M. Franklin, Advances in Cryptology 0 CRYTPO’01,volume 2139 of LNCS, pages 213-229 .Springer, 2001.

【非特許文献３】IETF Internet Draft,draft-ietf-simime-ibearch-03.txt,September 2007

【非特許文献４】Eric Rescorlal著、「マスタリングＴＣＰ／ＩＰ　ＳＳＬ／ＴＬＳ編」、オーム社、p.337-359

【発明の開示】

【発明が解決しようとする課題】

【０００９】

非特許文献４に記載されているようにＨＴＴＰＳによる暗号化は、暗号装置が秘密情報管理サーバへの接続を確立し、ＳＳＬ接続をネゴシエートし、その後ＳＳＬアプリケーション用のデータ通信路を通じてＨＴＴＰデータを転送するという手順を踏むため、暗号化のためのオーバヘッドは大きい。また、暗号装置の増加に伴い、秘密情報管理サーバの暗号化、復号処理負荷が増大する。さらに、ＨＴＴＰＳでは、プロキシとの連動性が悪く、ファイアウォールの管理者のポリシーとの整合性を取るために、ユーザはファイアウォールの設定状況に合わせることを余儀なくされる。インターネットプロバイダでの運用規約や設定の条件が悪い場合は、最悪ファイアウォールを通過できず、鍵の取得ができない場合もある。ユーザの設定や運用不備により、全てのサーバ証明書を受け入れるような設定がされている場合やＣＡ（認証局）の証明書が不適切に設定されている場合には、man-in-the-middleプロキシにより、攻撃者から秘密鍵の送信情報を盗み見られてしまうなどの問題がある。

【００１０】

本発明は、ＩＤベース暗号において利用するマスターシークレットと秘密情報を管理する秘密情報管理サーバが、ＩＤベース暗号を利用して、秘密情報を暗号装置に送信する秘密情報送信システム、秘密情報送信方法、秘密情報管理サーバ、暗号装置、秘密情報送信プログラム、記録媒体を提供することを目的とする。

【課題を解決するための手段】

【００１１】

請求項１記載の秘密情報送信システムは、ＩＤベース暗号において利用するマスターシークレットと秘密情報を管理する秘密情報管理サーバが、秘密情報管理サーバに通信ネットワークを介して接続している暗号装置に秘密情報を送信する。暗号装置は、秘密情報管理サーバの公開パラメータを保存する公開パラメータ保存部と、第一の共通鍵r_{com}を生成する共通鍵生成部と、乱数を生成し、乱数と公開パラメータと秘密情報管理サーバのＩＤ情報に基づき第二の共通鍵ｋ及び補助鍵ｃを生成し、秘密情報の種別を特定する秘密情報要求種別と第一の共通鍵r_{com}を含むリクエスト情報を第二の共通鍵ｋによって暗号化するＩＤベース暗号化部と、秘密情報管理サーバに暗号化されたリクエスト情報及び補助鍵ｃを送信し、秘密情報管理サーバから秘密情報を含む暗号化されたレスポンス情報を受信する通信制御部と、暗号化されたレスポンス情報を第一の共通鍵r_{com}を用いて復号する復号部を有する。秘密情報管理サーバは、公開パラメータを管理する公開パラメータ管理部と、マスターシークレットと秘密情報管理サーバのＩＤ情報に基づき秘密鍵TA_{scr}を生成する秘密鍵生成部と、秘密鍵TA_{scr}と補助鍵ｃに基づき第二の共通鍵

ｋを生成し、第二の共通鍵ｋによって暗号化されたリクエスト情報を復号するＩＤベース復号部と、リクエスト情報から得た第一の共通鍵r_{com}を用いて、レスポンス情報を暗号化する暗号化部と、暗号装置から暗号化されたリクエスト情報及び補助鍵ｃを受信し、暗号装置に暗号化されたレスポンス情報を送信する通信制御部を有する。

【００１２】

請求項６記載の秘密情報送信方法は、ＩＤベース暗号において利用するマスターシークレットと秘密情報を管理する秘密情報管理サーバが、秘密情報管理サーバに通信ネットワークを介して接続している暗号装置に秘密情報を送信する。暗号装置は、乱数を生成し、乱数と公開パラメータ保存部に保存されている公開パラメータと秘密情報管理サーバのＩＤ情報に基づき第二の共通鍵ｋ及び補助鍵ｃを生成し、秘密情報の種別を特定する秘密情報要求種別と共通鍵生成部で生成される第一の共通鍵r_{com}を含むリクエスト情報を第二の共通鍵ｋによって暗号化する。暗号装置は、暗号化されたリクエスト情報及び補助鍵ｃを通信ネットワークを介して秘密情報管理サーバへ送信する。秘密情報管理サーバは、暗号化されたリクエスト情報及び補助鍵ｃを受信する。秘密情報管理サーバは、マスターシークレットと秘密情報管理サーバのＩＤ情報に基づき秘密鍵TA_{scr}を生成する。秘密情報管理サーバは、秘密鍵TA_{scr}と補助鍵ｃに基づき第二の共通鍵ｋを生成し、第二の共通鍵ｋによって暗号化されたリクエスト情報を復号する。秘密情報管理サーバは、リクエスト情報から得た第一の共通鍵r_{com}を用いて、秘密情報を含むレスポンス情報を暗号化する。秘密情報管理サーバは、暗号化されたレスポンス情報を通信ネットワークを介して暗号装置へ送信する。暗号装置は、暗号化されたレスポンス情報を受信する。暗号装置は、レスポンス情報を第一の共通鍵r_{com}を用いて復号する。

【発明の効果】

【００１３】

ＳＳＬ接続のネゴシエート等を行わず、暗号化データを送信できるＩＤベース暗号を利用するため、暗号化のためのオーバヘッドが低減できる。ユーザの設定状況やプロバイダの運用ポリシーに依存していたセキュリティ機能設定のミスやファイアウォールの配置などネットワーク構成の制限を回避することができ、中間者攻撃を防ぐことができる。

【発明を実施するための最良の形態】

【００１４】

ここで、本発明の実施例について述べる。

【実施例】

【００１５】

システムの全体構成は従来技術と同様であるため、図１を用いて、本実施例の秘密情報送信システムの全体構成を説明する。秘密情報送信システムは、ＩＤベース暗号において利用するマスターシークレットと秘密情報を管理する秘密情報管理サーバ１００と、秘密情報管理サーバ１００に通信ネットワーク１０を介して接続している暗号装置２００を有する。

【００１６】

図２は、本実施例の秘密情報管理サーバ１００と暗号装置200_1の構成例を示す図である。なお、他の暗号装置200_2、・・・、200_Nも同様の構成を有する。

【００１７】

秘密情報管理サーバ１００は、通信制御部１０１、公開パラメータ管理部１０３、マスターシークレット管理部１０５、秘密鍵生成部１０７、ＩＤベース復号部１０９、暗号化部１１１、利用者認証情報管理部１１３、認証部１１５、ユーザセッション情報管理部１１７、ユーザＩＤ属性管理部１１９、改竄発見情報付加部１２１、制御部１２３を有する。

【００１８】

暗号装置200_1は、通信制御部２０１、秘密鍵保存部２０３、公開パラメータ保存部２０５、共通鍵生成部２０７、ＩＤベース暗号化部２０９、ＩＤベース暗号制御部２１１、復号部２１３、秘密情報取得制御部２１５、認証情報管理部２１７、セッション番号管

理部２１９、ＩＤ属性管理部２２１、改竄発見情報認証部２２３を有する。図３は、これら構成要素の機能を示す。なお、図４のように、秘密情報管理サーバ１００からマスターシークレット管理部１０５、秘密鍵生成部１０７を取り出し新たに通信制御部１４１を加えた秘密鍵生成サーバ１４０を設け、利用者認証情報管理部１１３、認証部１１５を取り出し新たに通信制御部１３１を加えた認証サーバ１３０を設け、秘密情報管理サーバ１００と秘密鍵生成サーバ１４０と認証サーバ１３０を専用に設けられた通信ネットワーク１１で接続してもよい。また、公開パラメータ管理部１０３、マスターシークレット管理部１０５、利用者認証情報管理部１１３、ユーザセッション情報管理部１１７、ユーザＩＤ属性管理部１１９、認証情報管理部２１７、セッション番号管理部２１９、ＩＤ属性管理部２２１は、管理する情報を記録する記録部を有してもよい。また、本発明において、「管理する」とは、情報を生成すること、他の端末や入力装置から情報を取得すること、情報を記録、保存、更新、削除すること等を意味する。

【００１９】

図５は、暗号装置２００$_1$と秘密情報管理サーバ１００との間の処理の流れを、図６（Ａ）は、メッセージ認証コードを利用した場合の処理の流れの詳細を、図６（Ｂ）は、ＩＤベース署名を利用した場合の他のマスターシークレットを用いる処理の流れの詳細を、図６（Ｃ）は、ＩＤベース署名を利用した場合の署名用の識別子を用いる処理の流れを、図７は、図６で用いられるＩＤベース暗号の処理手順の概略（ここでは、例としてBoneh-Franklin方式（非特許文献２）を用いる）を、図８は、図６で用いられるデータの定義を、図９は、図６で用いられる関数の機能を示す。

なお、本実施例の秘密情報送信システムの利用者はシステム管理者に利用登録申請を行い、システム管理者はＩＤ情報や認証情報を秘密情報管理サーバ１００へ登録する。ＩＤ情報や認証情報は住民基本台帳などのＩＤや公的証明書であっても良いが、本実施例では、ユーザＩＤとユーザパスワードとする。また、登録したＩＤ情報及び認証情報を利用者に返送する。利用者とシステム管理者との情報のやり取りは、従来の封書による郵便などオフライン、ネットワークを利用したオンラインを問わず安全な方法を前提とする。また、利用者は暗号装置にシステム管理者から取得したＩＤ情報及び認証情報を設定する。

【００２０】

暗号装置２００$_2$の利用者は、暗号装置２００$_1$の利用者のＩＤ情報（例えば「user1@example.com」とする）と属性情報（例えば有効期限と役職「date=2007/07/08;role=manager」とする）と乱数と公開パラメータに基づき共通鍵ｋ’及び補助鍵ｃ’を生成する。生成した共通鍵ｋ’によってデータを暗号化する。暗号化したデータは、通信ネットワーク１０を介して暗号装置２００$_1$に送信される（ｓ２００）。図１０（ｅ）は、暗号装置２００$_2$から送信されるデータ例を示す。

【００２１】

本発明の主眼の一つは、秘密情報管理サーバ１００が、ＩＤベース暗号において利用するマスターシークレットと秘密情報を管理すること利用して、ＩＤベース暗号を用いて秘密情報を暗号装置に送信することである。以下、説明する。

【００２２】

暗号装置２００$_1$は、秘密鍵ｋ’が秘密鍵保存部２０３に保存されているか確認する（ｓ２０１）。例えば、暗号化データを受信した暗号装置２００$_1$では、暗号化データを復号するため、ＩＤベース暗号制御部２１１へ暗号化データが渡され秘密鍵の取得処理を行う。まず、暗号化されたデータの暗号に用いた利用者のＩＤ情報と属性情報を合わせたもの（「user1@example.com.date=2007/07/08;role=manager」）を取得し、この情報を元に秘密情報取得制御部２１５に秘密鍵取得を要求する。秘密情報取得制御部２１５は、秘密鍵保存部２０３に秘密鍵ｋ’が保存されているか確認する。保存されている場合には、ＩＤベース暗号制御部２１１にその秘密鍵ｋ’を返す。保存されていない場合には、セッション番号管理部２１９に問合せる。図１１（ａ）は、セッション番号管理部２１９で管理されるデータ例を示す。

【００２３】

暗号装置２００$_1$は、セッション番号管理部２１９で管理される時刻情報を用いたセッション番号（例えば「2007/07/08/09：10：11：123」とする）を生成し（ｓ２０２）、保存する。この情報を秘密情報取得制御部２１５を介してＩＤベース暗号化部２０９へ渡す。

【００２４】

ＩＤベース暗号化部２０９は、乱数を生成し、乱数と公開パラメータと秘密情報管理サーバ１００のＩＤ情報とセッション番号に基づき第二の共通鍵ｋ及び補助鍵ｃを生成し、第一の共通鍵r_{com}と秘密情報を特定する秘密情報要求種別、認証情報、属性情報を含むリクエスト情報を第二の共通鍵ｋによって暗号化する（ｓ２０３）。図１０（ａ）は、リクエスト情報のデータ例を示す。例えば、ＩＤベース暗号化部２０９は、セッション番号と秘密情報管理サーバ１００のＩＤ情報（例えば「http://pkg.example.com/」とする）を結合した情報$TA_{sessionID}$（「http://pkg.example.com/2007/07/08/09：10：11：123」）を生成し、楕円曲線上の点TA_{pub}に変換する。さらに、ＩＤベース暗号化部２０９は、乱数r_{id}を生成し、公開パラメータ保存部２０５に保存されている公開パラメータＰ，ｓ・Ｐを取得する。これらの情報に基づき第二の共通鍵ｋ及び補助鍵ｃを生成する。

【００２５】

$$k=H((e(TA_{pub},s\cdot P)\hat{}r_{id}))$$

$$c=r_{id}\cdot P$$

なお、Ｈ（ ）はハッシュ関数である。本実施例では、第二の共通鍵ｋを使った共通鍵暗号方式としてＣａｍｅｌｌｉａを想定しているが、ＡＥＳ等他の共通鍵暗号方式であってもよい。共通鍵生成部２０７で生成された第一の共通鍵r_{com}と、要求する秘密情報を特定する秘密情報要求種別（例えば「ＫＥＭ－ｋｅｙ：鍵共有に用いる暗号鍵」とする）と、暗号装置２００$_1$の利用者の認証情報（例えば「ユーザＩＤ、ユーザパスワード」とする）と、ＩＤ属性管理部にて管理される属性情報（例えば、有効期限と役職「date=2007/07/08;role=manager」とする）を含むリクエスト情報を第二の共通鍵ｋによって暗号化する。ここで、第一の共通鍵r_{com}は、対応するセッション番号とともにセッション番号管理部２１９へ保存される。本実施例では、第一の共通鍵r_{com}を使った共通鍵暗号方式としてＣａｍｅｌｌｉａを想定しているが、ＡＥＳ等他の共通鍵暗号方式であってもよい。また、認証情報は、予め秘密情報管理サーバに登録している認証情報と同一であり、認証情報管理部２１７で管理される。図１１（ｂ）は、認証情報管理部２１７で管理されるデータ例を示す。秘密情報要求種別とは、要求する秘密情報を特定するための種別であり、秘密鍵以外であってもよい。属性情報とは、ＩＤ情報に付加される情報、例えば、有効期限、役職、権限等の情報であり、ＩＤ属性管理部で管理される。

【００２６】

通信制御部２０１は、暗号化されたリクエスト情報、補助鍵ｃ及び情報$TA_{sessionID}$含む情報REQ_{msg}を通信ネットワーク１０を介して、秘密情報管理サーバ１００へ送信する（ｓ２０４）。図１０（ｂ）は、情報REQ_{msg}のデータ例を示す。

【００２７】

秘密情報管理サーバの通信制御部１０１は、通信ネットワークを介して情報REQ_{msg}受信する（ｓ１０１）。秘密鍵生成部１０７は、マスターシークレット管理部１０５で管理されるマスターシークレットｓと情報$TA_{sessionID}$に基づき秘密鍵TA_{scr}を生成する（ｓ１０２）。なお、この秘密鍵TA_{scr}は、時刻情報を用いたセッション番号を利用せずに生成する場合には、予め生成しておいてもよい。例えば、秘密情報管理サーバ１００の制御部１２３は、情報REQ_{msg}から、補助鍵ｃと情報$TA_{sessionID}$を取り出し、秘密鍵生成部１０７に情報$TA_{sessionID}$を渡し、対応する秘密鍵TA_{scr}を要求する。秘密鍵生成部１０７は、マスターシークレット管理部１０５で管理されるマスターシークレットｓと情報$TA_{sessionID}$を楕円曲線上の点に変換したTA_{pub}から秘密鍵TA_{scr}を生成し、制御部１２３へ渡す。

【００２８】

$TA_{scr}=s\cdot TA_{pub}$

制御部１２３は、補助鍵ｃと秘密鍵TA_{scr}をＩＤ復号部１０９へ渡す。ＩＤベース復号部１０９は、秘密鍵TA_{scr}と補助鍵ｃから第二の共通鍵ｋを生成し、第二の共通鍵ｋによって暗号化されたリクエスト情報を復号する（ｓ１０３）。例えば、ＩＤベース復号部１０９は、秘密鍵TA_{scr}と補助鍵ｃに基づき第二の共通鍵ｋを生成する。

【００２９】

$H(e(TA_{scr}, c))$

$= H(e(s\cdot TA_{pub}, r_{id}\cdot P)) = H((e(TA_{pub}, s\cdot P)\hat{}r_{id})) = k$

この第二の共通鍵ｋによって、Ｃａｍｅｌｌｉａで暗号化されたリクエスト情報を復号し、第一の共通鍵r_{com}と秘密情報を特定する秘密情報要求種別、認証情報、属性情報を取得する。なお、復号できない場合には、エラーメッセージを暗号装置200_1に返す。

【００３０】

認証部１１５では、リクエスト情報に含まれる認証情報と利用者認証情報管理部１１３で管理される認証情報に基づき認証を行う（ｓ１０４）。図１１（ｄ）は、利用者認証情報管理部１１３で管理される認証情報のデータ例を示す。なお、利用者認証情報管理部１１３には、秘密情報管理情報管理サーバを利用する利用者毎の認証情報が登録されている。

認証が失敗した場合には、エラーメッセージを暗号装置200_1に返す。

【００３１】

秘密情報管理サーバ１００は、利用者のＩＤ情報、セッション番号とユーザセッション情報管理部１１７で管理される利用者のＩＤ情報、セッション番号に基づきセッション番号が正しいか確認する（ｓ１０５）。図１１（ｃ）は、ユーザセッション情報管理部１１７で管理されるデータ例を示す。取得したセッション番号がユーザセッション情報管理部１１９で管理されるセッション番号と比較し、最新のものでない場合には、リプレイアタックまたは２重要求送信と判断し、エラーメッセージを暗号装置200_1に返す。このように時刻情報を用いたセッション番号を利用することで、リプレイアタックを防ぐことができるという効果がある。なお、このような効果が得られるのは、秘密情報管理サーバ１００が、マスターシークレットｓを管理し、秘密情報管理サーバ１００自身で秘密情報管理サーバの秘密鍵TA_{SCR}を生成し、ＩＤベース復号のための共通鍵ｋを生成することができるため、暗号装置200_1は、時刻情報を用いたセッション番号を含む情報$TA_{sessionID}$に基づき、ユニークな共通鍵ｋを生成し、ＩＤベース暗号化を行うことができるからである。

【００３２】

秘密情報管理サーバ１００は、リクエスト情報に含まれるＩＤ属性とユーザＩＤ属性管理部１１９で管理される利用者のＩＤ情報と属性情報の条件に基づきリクエスト情報に含まれるＩＤ属性が条件を満たすか確認する（ｓ１０６）。図１１（ｅ）は、ユーザＩＤ属性管理部で管理されるデータの例を示す。ユーザＩＤ属性管理部１１９で管理される属性情報の条件とは、ＩＤ情報の有効期限、権限、役職等がある。取得したＩＤ属性がユーザＩＤ属性管理部１１９で管理される属性情報に定まる条件を満たさない場合には、エラーメッセージを暗号装置200_1に返す。属性情報を用いることで、利用者毎に取得できる秘密情報を設定すること等ができるという効果がある。

【００３３】

秘密情報管理サーバ１００の秘密鍵生成部１０７は、マスターシークレットｓと暗号装置の利用者のＩＤ情報に基づきＩＤベース暗号の復号鍵を生成するために用いる秘密鍵USR_{scr}を生成する（ｓ１０７）。なお、この秘密鍵USR_{scr}は、予め生成しておいてもよい。例えば、取得した認証情報に含まれるユーザＩＤと属性情報を結合した情報$IDATR_{user}$に基づき、秘密情報要求種別（本実施例では、ＫＥＭ－ｋｅｙ：鍵共有のための復号鍵とする）に従い、秘密鍵USR_{scr}を生成する。例えば、秘密鍵生成部１０７は、マスターシークレットｓと情報$IDATR_{user}$を楕円曲線上の点に変換したUSR_{pub}から秘密鍵USR_{scr}を生成する。

【００３４】

$USR_{scr}=s\cdot USR_{pub}$

秘密情報管理サーバ１００は、暗号化部１１１において、リクエスト情報から得た第一の共通鍵r_{com}を用いて、秘密鍵USR_{scr}を含むレスポンス情報を暗号化する（ｓ１０８）。レスポンス情報には、情報$IDATR_{user}$を含んでもよい。図１０（ｃ）は、レスポンス情報のデータ例を示す。

【００３５】

秘密情報管理サーバ１００は、改竄発見情報付加部１２１において暗号化されたレスポンス情報にセッション情報を付加し、これらをまとめた情報ｍに対する改竄を発見するために用いる改竄発見情報を付加する（ｓ１０９）。例えば、情報ｍに対する改竄発見情報としてメッセージ認証コードを付加する。また、改竄発見情報として、メッセージ認証コードに代えて、例えば、秘密情報管理サーバのＩＤベース署名を付加してもよい。なお、暗号装置間のＩＤ情報に基づく署名処理に関しては、例えば、Florian Hess. Efficient Identity Based Signature Schemes Based on Pairings. SAC 2002, LNCS 2595, pp.310-324, 2003.Springer-Verlag,2003に詳しく述べられている。図６（Ａ）は、メッセージ認証コードを利用した場合の処理の流れの詳細を、図６（Ｂ）は、ＩＤベース署名を利用した場合の他のマスターシークレットを用いる処理の流れの詳細を、図６（Ｃ）は、ＩＤベース署名を利用した場合の署名用の識別子を用いる処理の流れを示す。図１２は、図６（Ｂ）、（Ｃ）に用いられるＩＤベース署名の処理手順の概略を示す。この場合、改竄発見情報付加部１２１は、署名鍵と暗号化されたレスポンス情報にセッション番号を付加した情報ｍと公開パラメータに基づき、署名（Ｖ，Ｓ）を生成し、情報ｍに付加する。ここで、署名鍵は、第二の共通鍵ｋを生成する際に用いた秘密鍵TA_{scr}でもよいが、鍵の強度を高めるために新たに以下の２つ方法によって生成することもできる。一つ目は、秘密鍵生成部１０７は、マスターシークレットｓとは異なるマスターシークレット管理部で管理される他のマスターシークレットｓ’と情報$TA_{sessionID}$を楕円曲線上の点に変換したTA_{pub}から署名鍵TA'_{scr}を生成する方法である。この場合、公開パラメータにＰ’ｓ＝ｓ’・Ｐを加える。

【００３６】

$TA'_{scr}=s'\cdot TA_{pub}$

二つ目は、秘密鍵生成部１０７は、マスターシークレットｓと情報$TA_{sessionID}$に予め定めた署名用の識別子を付加した情報$TA'_{sessionID}$を楕円曲線上の点に変換したTA'_{pub}から署名鍵TA''_{scr}を生成する方法である。

【００３７】

$TA''_{scr}=s\cdot TA'_{pub}$

改竄発見情報付加部１２１は、暗号化されたレスポンス情報にセッション番号を付加した情報ｍに対して署名（Ｖ，Ｓ）を生成し、情報ｍに署名（Ｖ，Ｓ）を付加した情報RES_{msg}を生成する。なお、署名（Ｖ、Ｓ）は以下のように表される。ここで、Ｈ’（）は、Ｈ（）とは異なるハッシュ関数を、ｍ‖ｒは、ｍとｒを連結することを意味する。

【００３８】

$V=H'(m\|r)$

$r=e(P1,P)^{k}$

ただし、Ｐ１は任意の秘密情報管理サーバ１００の公開パラメータの楕円曲線上の点であり、ｋは乱数である。

【００３９】

$S=V\cdot TA_{X}+k\cdot P1$

但し、署名鍵TA_{X}には、上述のTA_{scr}、TA'_{scr}、TA''_{scr}の何れかを用いる。通信制御部１０１は、通信ネットワーク１０を介して、暗号化装置200_{1}に、暗号化されたレスポンス情報にセッション番号を付加した情報ｍに対して改竄発見情報を生成し、情報ｍに改竄発見情報を付加した情報RES_{msg}を送信する（ｓ１１０）。

【００４０】

秘密情報管理サーバ１００は、ユーザセッション情報管理部１１７で管理されているユーザセッション情報を更新する（ｓ１１１）。図１０（ｄ）は、情報REQ_{msg}のデータ例を示す。

【００４１】

暗号装置200_1の通信制御部２０１は、通信ネットワーク１０を介して情報RES_{msg}を受信する（ｓ２０５）。

【００４２】

暗号装置200_1は、改竄発見情報認証部２２３において、秘密情報管理サーバから暗号装置へ送られる改竄発見情報を認証する（ｓ２０６）。例えば、メッセージ認証コードや署名（Ｖ，Ｓ）を確認し、改竄等が行われていないか確認する。改竄等が行われていることが確認された場合には、エラーメッセージを生成する。署名（Ｖ，Ｓ）を付加した場合について説明する。改竄発見情報認証部２２３は、署名鍵TA_Xに、上述のTA_{scr}を用いた場合には、情報ｍ、署名（Ｖ，Ｓ）、秘密情報管理サーバの公開パラメータ、情報$TA_{sessionID}$を楕円曲線上の点に変換したTA_{pub}に基づいて、署名検証を行う。

【００４３】

$$W=e(S,P)\cdot e(TA_{pub},-s\cdot P)\wedge V$$
$$V'=H'(m\|W)$$

署名鍵TA_Xに、上述のTA'_{scr}を用いた場合には、情報ｍ、署名（Ｖ，Ｓ）、秘密情報管理サーバのＰ’ｓを含む公開パラメータ、情報$TA_{sessionID}$を楕円曲線上の点に変換したTA_{pub}に基づいて、署名検証を行う。

【００４４】

$$W=e(S,P)\cdot e(TA_{pub}-s''\cdot P)\wedge V$$
$$V'=H'(m\|W)$$

署名鍵TA_Xに、上述のTA''_{scr}を用いた場合には、情報ｍ、署名（Ｖ，Ｓ）、秘密情報管理サーバの公開パラメータ、情報$TA_{sessionID}$に予め定められた署名用識別子を付加した情報$TA'_{sessionID}$を楕円曲線上の点に変換したTA'_{pub}に基づいて、署名検証を行う。

【００４５】

$$W=e(S,P)\cdot e(TA'_{pub},-s\cdot P)\wedge V$$
$$V'=H'(m\|W)$$

署名ＶとＶ’が一致する場合には、認証は成功したことを意味し、一致しない場合には、情報ｍに何らかの変更や破損等があったことを意味する。各暗号装置は、署名用の公開パラメータを発行している秘密情報管理サーバのＩＤ情報を取得することができる。そのため、署名鍵発行の処理が悪意のあるものによって操作されていなければ、暗号装置がリクエスト情報をＩＤベース暗号する際に使用した秘密情報管理サーバのＩＤ情報と署名用の公開パラメータのみで、秘密情報管理サーバから返送されてくるレスポンス情報の署名を検証できる。よって、ＰＫＩ（Public Key Infrastructure）のように署名用の公開鍵証明書を取得し、さらにその証明書を検証する処理が必要ないという有利な効果がある。

暗号装置200_1は、暗号化されたレスポンス情報に付加されたセッション番号とセッション番号管理部２１９に保存したセッション番号が同一か確認する（ｓ２０７）。セッション番号管理部２１９に該当するセッション番号がない場合には、エラーメッセージを生成する。

【００４６】

復号部２１３において、暗号化されたレスポンス情報を第一の共通鍵r_{com}を用いて復号する（ｓ２０８）。例えば、セッション番号管理部２１９に保存した第一の共通鍵r_{com}と暗号化されたレスポンス情報を、復号部２１３へ入力し、復号し、秘密情報（秘密鍵USR_{scr}）や情報$IDATR_{user}$を取得する。秘密情報管理サーバ１００は、利用者の認証情報にて、利用者はセッション番号に対応した第一の共通鍵r_{com}で暗号化されたレスポンス情報が復号できることでそれぞれ認証を行うため、公開鍵証明書を用いたＨＴＴＰＳによる相互認証のように、利用者は、秘密鍵と公開鍵のペアを作成し、

公開鍵を認証局に登録してクライアント証明書を事前に入手しておく必要がなく、手続を簡略化できるという効果がある。

【００４７】

暗号装置２００$_1$は、エラーメッセージを生成した場合や秘密情報管理サーバ１００からエラーメッセージを受信した場合には、暗号装置２００$_1$のディスプレイやプリンタ等の出力部からエラーメッセージを表示し利用者に知らせる（ｓ２０９）。

【００４８】

暗号装置２００$_1$は、取得した秘密鍵ＵＳＲ$_{scr}$と補助鍵ｃ’を用いて、共通鍵ｋ’を生成し、暗号装置２００$_2$から送信されてきた暗号化データを復号することができる（ｓ２１０）。

【００４９】

本実施例において、暗号装置２００$_1$と暗号装置２００$_2$間の暗号処理はＩＤベース暗号を用いている。この場合、暗号装置２００$_1$と秘密情報管理サーバ間の秘密情報をやりとりする際にＨＴＴＰＳを利用すると、ＨＴＴＰＳとＩＤベース暗号の二つの暗号方式を利用するため、暗号化のためのリソースの消費が大きいのに比べ、暗号装置間、暗号装置と秘密鍵管理サーバ間のいずれの暗号方式もＩＤベース暗号となるため、ＳＳＬ暗号化のためのリソースの消費など、暗号化のためのリソース消費を低減できるという効果がある。さらに、秘密情報管理サーバから暗号装置に秘密情報を送信する際に、秘密情報に対して署名を付加する場合に、ＩＤベース署名を利用することによって、リソースの消費を抑えることができる。ただし、本発明は、暗号装置間の暗号方式をＩＤベース暗号に限定するものではなく、他の暗号方式を用いてもよい。

【００５０】

本実施例において、ＩＤベース暗号方式として、Ｂｏｎｅｈ－Ｆｒａｎｋｌｉｎ方式を用いているが、このＩＤベース暗号方式に限定するものではない。本実施例において、暗号装置２００$_2$から２００$_1$へＩＤベース暗号を利用して暗号化データを送信する際に利用するＩＤベース暗号の復号鍵ｋ’を生成するために用いる秘密鍵ＵＳＲ$_{scr}$を秘密情報管理サーバ１００から暗号装置２００$_1$へ送信しているが、暗号装置２００$_1$から２００$_2$へＩＤベース署名を利用して、データを送信する際に利用するＩＤベース署名用署名鍵を生成するために用いる秘密鍵ＵＳＲ’$_{scr}$を秘密情報管理サーバ１００から暗号装置２００$_1$へ送信する場合であっても本発明を利用することができる。また、利用者間の署名方式は、ＩＤベース署名に限定するものではなく、他の署名方式であってもよい。

【００５１】

なお、認証情報に基づき認証を行う必要がない場合には、秘密情報管理サーバ１００には、利用者認証情報管理部１１３及び認証部１１４を設けなくともよく、暗号装置２００には、認証情報管理部２１７を設けなくともよい。また、リクエスト情報には、認証情報を含まなくてもよい。

【００５２】

また、セッション番号による管理を必要としない場合には、秘密情報管理サーバ１００には、ユーザセッション情報管理部１１７を設けなくともよく、暗号装置２００には、セッション番号管理部２１９を設けなくともよい。この場合、ＩＤベース暗号化部２０９では、乱数を生成し、乱数と公開パラメータと秘密情報管理サーバのＩＤ情報に基づき第二の共通鍵ｋ及び補助鍵ｃを生成し、秘密情報の種別を特定する秘密情報要求種別と第一の共通鍵ｒ$_{com}$を含むリクエスト情報を第二の共通鍵ｋによって暗号化する。また、秘密鍵生成部１０７では、マスターシークレットと秘密情報管理サーバのＩＤ情報に基づき第二の共通鍵ｋを生成する。また、セッション情報の確認（ｓ１０５）、セッション情報の更新（ｓ１１１）、セッション番号確認（ｓ２０７）等は行わなくてもよい。

【００５３】

さらに、ＩＤ情報に付加された属性情報により利用者毎に取得できる秘密情報を設定する必要がない場合には、秘密情報管理サーバ１００には、ユーザＩＤ属性管理部１１７を設けなくともよく、暗号装置２００には、ＩＤ属性管理部２２１を設けなくともよい。ま

た、リクエスト情報には、属性情報を含まなくてもよい。
【００５４】
本実施例において、秘密情報は、秘密鍵としているが、他の秘密情報であってもよい。この発明において、秘密情報管理サーバ及び暗号装置は、コンピュータにより機能させてもよい。その場合は、各過程をコンピュータにより実行させるためのプログラムを、ＣＤ－ＲＯＭ、磁気ディスク、半導体記憶装置などの記録媒体からインストールし、あるいは通信回線を通じてダウンロードして、そのコンピュータにそのプログラムを実行させればよい。
【図面の簡単な説明】
【００５５】
【図１】実施例の秘密情報送信システムの全体構成を示す図である。
【図２】実施例の秘密情報管理サーバ１００と暗号装置２００_{1}の構成例を示す図である。
【図３】構成要素の機能を示す図である。
【図４】秘密鍵生成サーバ１４０と認証サーバ１３０を設けた秘密情報管理サーバ１００の構成例を示す図である。
【図５】暗号装置２００_{1}と秘密情報管理サーバ１００との間の処理の流れを示す図である。
【図６（Ａ）】（Ａ）は、メッセージ認証コードを利用した処理の流れの詳細を示す図である。
【図６（Ｂ）】（Ｂ）は、署名を利用した他のマスターシークレットを用いる処理の流れの詳細を示す図である。
【図６（Ｃ）】（Ｃ）は、署名を利用した署名用の識別子を用いる処理の流れの詳細を示す図である。
【図７】図６で用いられるＩＤベース暗号の処理手順の概略を示す図である。
【図８】図６で用いられるデータの定義を示す図である。
【図９】図６で用いられる関数の機能を示す図である。
【図１０】（ａ）は、リクエスト情報のデータ例を、（ｂ）は、情報$ＲＥＱ_{ｍｓｇ}$のデータ例を、（ｃ）は、レスポンス情報のデータ例を、情報ＲＥＱｍｓｇのデータ例を、（ｅ）は、暗号装置２００_{2}から送信されるデータの例を示す。
【図１１】（ａ）は、セッション番号管理部２１９で管理されるデータ例を、（ｂ）は、認証情報管理部２１７で管理されるデータ例を、（ｃ）は、ユーザセッション情報管理部１１７で管理されるデータの例を（ｄ）は、利用者認証情報管理部１１３で管理される認証情報のデータ例を、（ｅ）は、ユーザＩＤ属性管理部で管理されるデータの例を示す。
【図１２】図６（Ｂ）、（Ｃ）で用いられるＩＤベース署名の処理手順の概略を示す図である。
【符号の説明】
【００５６】
１００　秘密情報管理サーバ　　１０１　通信制御部
１０３　公開パラメータ管理部　　１０５　マスターシークレット管理部
１０７　秘密鍵生成部　　１０９　ＩＤベース復号部
１１１　暗号化部　　１１３　利用者認証情報管理部
１１５　認証部　　１１７　ユーザセッション情報管理部
１１９　ユーザＩＤ属性管理部　　１２１　改竄発見情報付加部
１２３　制御部　　１０　通信ネットワーク
２００　暗号装置　　２０１　通信制御部
２０３　秘密鍵保存部　　２０５　公開パラメータ保存部
２０７　共通鍵生成部　　２０９　復号部
２１１　ＩＤベース暗号制御部　　２１３　復号部
２１５　秘密情報取得制御部　　２１７　認証情報管理部

２１９　セッション番号管理部　　２２１　ＩＤ属性管理部
２２３　　改竄発見情報認証部

【図１】

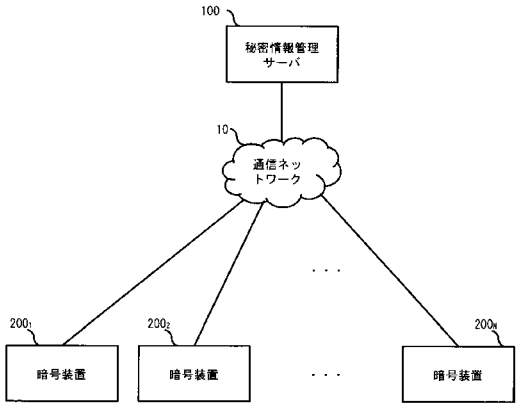

図１

【図２】

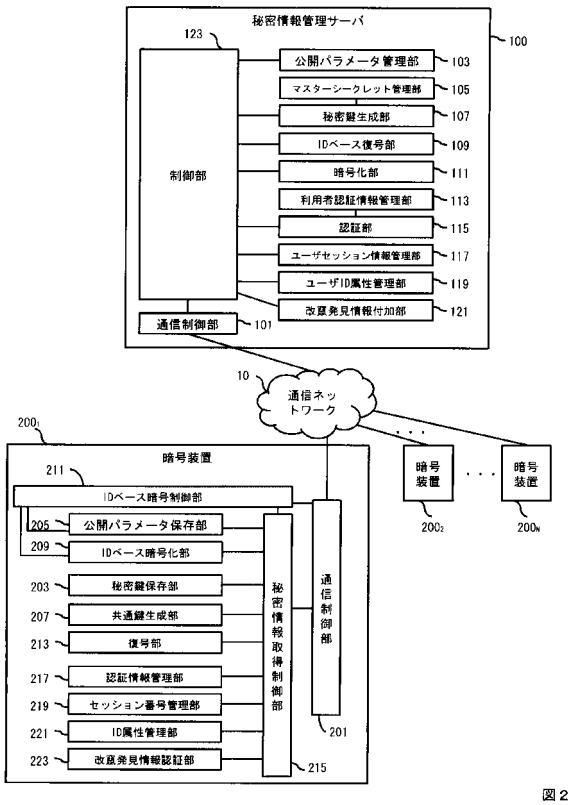

図２

【図３】

符号	システム構成	符号	機能部	役割説明
10	通信ネットワーク	10	通信ネットワーク	インターネットなど秘密情報管理サーバと暗号装置をつなぐネットワーク
100	秘密情報管理サーバ	101	通信制御部	暗号装置、通信ネットワークとの通信を制御する
		103	公開パラメータ管理部	公開パラメータを管理する
		105	マスターシークレット管理部	マスターシークレットを管理する
		107	秘密鍵生成部	マスターシークレットと秘密鍵を要求する利用者のID情報に基づき秘密鍵を生成する
		109	ID復号部	暗号鍵とマスターシークレットとID情報に基づき第二の共通鍵を生成し、その第二の共通鍵によって、暗号化されたリクエスト情報を復号する
		111	暗号化部	リクエスト情報に含まれる第一の共通鍵を用いてレスポンス情報を暗号化する
		113	利用者認証情報管理部	秘密情報管理サーバに登録されている利用者の認証情報を管理する
		115	認証部	リクエスト情報に含まれる認証情報と利用者認証情報管理部で管理される認証情報に基づき認証を行う
		117	ユーザセッション情報管理部	利用者のID情報毎にセッション番号を管理する
		119	ユーザID属性管理部	利用者のID情報毎の属性情報の条件を管理する
		121	改竄発見情報付加部	暗号化されたレスポンス情報に対して改竄発見情報を付加する
200	暗号装置	123	制御部	各処理を制御する
		201	通信制御部	秘密情報管理サーバや他の暗号装置、通信ネットワークとの通信を制御する
		203	秘密鍵取得部	秘密鍵を保存する
		205	公開パラメータ保存部	秘密情報管理サーバの公開パラメータを保存する
		207	共通鍵生成部	秘密情報管理サーバで秘密情報の暗号化を行う際に利用する第一の共通鍵を生成する
		209	ID ベース鍵生成部	生成した乱数と公開パラメータと秘密情報管理サーバのID情報に基づき第二の共通鍵を生成し、その第二の共通鍵によって、リクエスト情報を暗号化する
		211	ID ベース鍵号解読部	IDベース暗号処理を制御する
		213	復号部	暗号化されたレスポンス情報を第一の共通鍵を用いて復号する
		215	秘密情報取得制御部	秘密情報の取得処理を制御する
		217	認証情報管理部	秘密情報管理サーバに登録している利用者の認証情報を管理する
		219	セッション番号管理部	利用情報を用いたセッション番号を管理する
		221	ID属性管理部	利用者のID情報に付加された属性情報を管理する
		223	改竄発見情報認証部	改竄発見情報を認証する

図3

【図４】

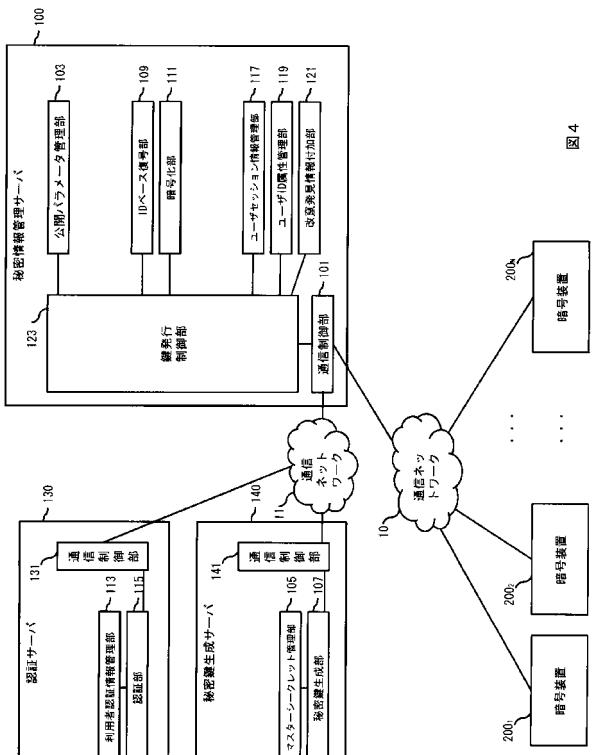

図4

【図５】

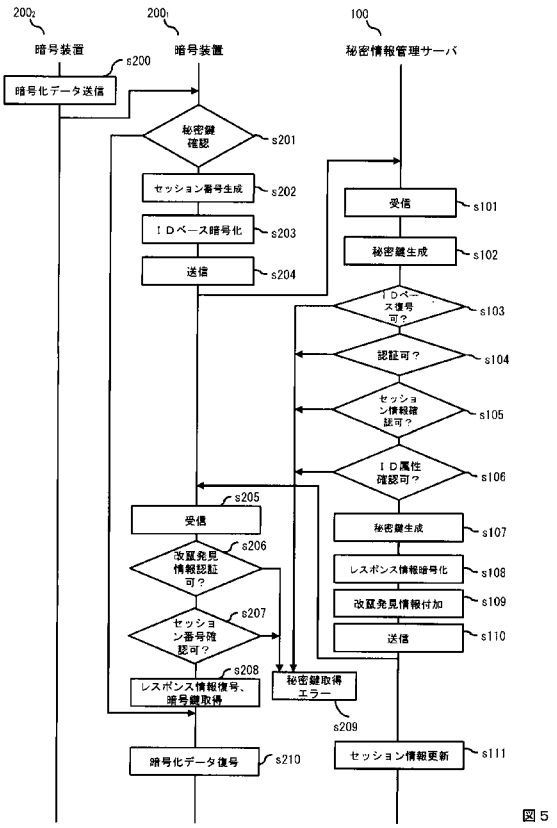

図5

【図６（Ａ）】

[秘密情報管理サーバへのユーザ登録]
　ID_{user}
　PWD_{user}
[秘密情報管理サーバのシステム設定]
　ID_{PK}=pkg.example.com
　Pベースポイント
　master-乱数生成 s
　P_{pub}=s・P
　TA_{pub}=[P,P_{pub}]
[暗号装置から秘密情報管理サーバへの秘密鍵要求]
s202)　sessionNo=Date.HH.MM.SS.msec
s203-1)　$TA_{sessionID}$=ID_{TA} ‖ sessionNo
s203-2)　TA_{pair}=MapToPoint($TA_{sessionID}$)
s203-3)　[k_{enc},c]=IDEnc(TA_{pub}, TA_{pair})
s203-4)　r_{user}=Random()
s203-5)　REQ_{body}=[KEM-Key,ID_{user},PWD_{user},ATR_{user},r_{User}]
s203-6)　$EREQ_{body}$ =ReqEnc(REQ_{body},k_{enc})
s203-7)　REQ_{mac}=[$TA_{sessionID}$,c,$EREQ_{body}$]
s204)　Send()
[秘密情報管理サーバへのシステム設定]
s101)　Receive()
s102-1)　[$TA_{sessionID}$,c,$EREQ_{body}$]= REQ_{msg}
s102-2)　TA_{key}=KeyGen(s,$TA_{sessionID}$)
s102-3)　k_{dec}=IDDec(TA_{key},c)
s103-1)　REQ_{body}=ReqDec($EREQ_{body}$,k_{dec})
s103-2)　[KEM-Key,ID_{user},PWD_{user},ATR_{user},r_{User}] =REQ_{body}
s104)　Auth(ID_{user},PWD_{user})
s105-1)　ID_{TA} | sessionNo= $TA_{sessionID}$
s105-2)　CHK1USERSession(ID_{user},sessionNo)
s106)　CHKATR(ID_{user},ATR_{user})
s107-1)　$IDATR_{user}$=ID_{user} ‖ ATR_{user}
s107-2)　USR_{ref}=KeyGen(s,$IDATR_{user}$)
s108-1)　KEY_{body}=[$IDATR_{user}$,USR_{ref}]
s108-2)　$EKEY_{body}$=ResEnc(KEY_{body},r_{User})
s109-1)　RES_{body}=[sessionNo,$EKEY_{body}$]
s109-2)　RES_{mac}=MAC(RES_{body})
s109-3)　RES_{msg}=[RES_{body},RES_{mac}]
s110)　Send()
s111)　UpdateUserSession()
[暗号装置における秘密鍵復号]
s205)　Receive()
s206-1)　[RES_{body},RES_{mac}]= RES_{msg}
s206-2)　CHKMAC(RES_{body},RES_{mac})
s207-1)　[sessionNo,$EKEY_{body}$]= RES_{body}
s207-2)　CHKSession(sessionNo)
s208-1)　KEY_{body}=ResDec($EKEY_{body}$,r_{User})
s208-2)　[$IDATR_{user}$,USR_{ref}]= KEY_{body}

図６（Ａ）

【図６（Ｂ）】

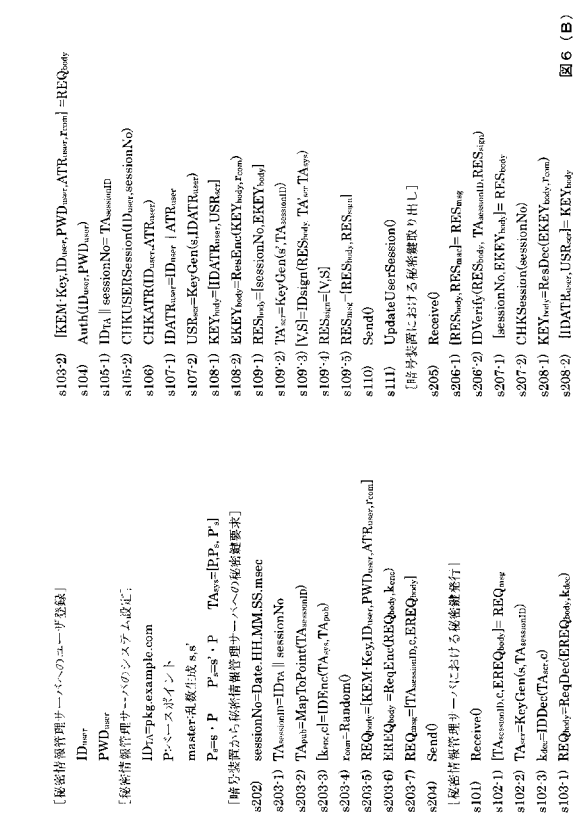

図６（Ｂ）

【図６（Ｃ）】

図６（Ｃ）

【図７】

処理	処理内容
IDから公開鍵の計算：MapToPoint()	ユーザのID文字列ID_{user}を、TA_{sys}パラメータの楕円曲線上の点ID_{pub}に変換する。（TAの公開ID $TA_{sessionID}$はTA_{pub}に変換） ID_{pub}＝MapToPoint(TA_{sys},ID_{user})
秘密鍵生成：KeyGen()	IDから楕円曲線上の点に変換された公開鍵を、楕円スカラー倍（マスターシークレット：s倍）する。 $ID_{sec}=s*ID_{pub}$
IDベース暗号による鍵生成：IDEnc()	乱数r_{id}を生成し、公開鍵ID_{pub}、TAのシステムパラメータP_sとを用いペアリング演算e(,)を行い、その結果を乱数r_{id}でべき乗する。H()でハッシュ値を計算し、暗号用の共通鍵とする。TAのシステムパラメータをr_{id}で楕円スカラー倍し、復号用の鍵cとする。 [P,P_s]:=TA_{sys} r_{id}=Random() k_{enc}=H((e(ID_{pub},P_s)^r_{id})) c=r_{id}・P return(k_{enc},c)
IDベース暗号による復号鍵の計算：IDDec()	受信したcと自身の秘密鍵ID_{sec}により、ペアリング演算e(,)を行い、その結果をH()でハッシュ値を計算し、復号用の共通鍵k_{dec}とする。ペアリング演算の性質により、e(ID_{sec},P_s)は、e(ID_{pub},P_s)^r_{id}となり、k_{dec}はk_{enc}と同じになる。 k_{dec}=H(e(ID_{sec},c))

図7

【図８】

データ型	定義説明
[A,B]	AとBの組
$INFO_{auth}$	認証情報
ID_{user}	ユーザID
ID_{pub}	利用者の公開鍵
PWD_{user}	ユーザパスワード
ATR_{user}	属性情報
$IDATR_{user}$	ユーザIDと属性情報を結合したもの
USR_{ser}	利用者の秘密鍵
sessionNo	セッション番号
r_{com}	第一の共通鍵用乱数
r_{id}	IBE用乱数
k_{enc}	IDEnc()で生成されるIDベース暗号鍵
c	IDEnc()で生成されるIDベース暗号鍵k_{enc}と対の鍵
REQ_{body}	秘密鍵要求本文情報
$EREQ_{body}$	暗号化された秘密鍵要求本文情報
REQ_{msg}	秘密情報管理サーバに送信する暗号化された秘密鍵要求文
P	公開パラメータ1（ベースポイント：楕円曲線上の点）
s	マスターシークレット（整数）
P_s	公開パラメータ2（マスターシークレット倍されたベースポイント）
ID_{TA}	秘密情報管理サーバのID情報
$TA_{sessionID}$	秘密情報管理サーバのID情報とセッション番号を結合したもの
TA_{sys}	秘密情報管理サーバの公開パラメータ（公開パラメータP,Psの組）
TA_{pub}	秘密情報管理サーバの公開鍵
TA_{ser}	秘密情報管理サーバの秘密鍵
k_{dec}	IDDec()で生成されるIDベース暗号鍵
KEY_{body}	秘密情報管理サーバが生成した利用者の秘密鍵本文
$EKEY_{body}$	暗号化された利用者の秘密鍵本文
RES_{body}	セッション番号と$EKEY_{body}$を結合したもの
RES_{mac}	RES_{body}のMAC（メッセージ認証コード）
RES_{msg}	RES_{body}とRES_{mac}を結合したものであってユーザに返す応報メッセージ
RES_{sign}	RES_{body}の署名である
sign	署名用の識別子

図8

【図９】

関数名	機能
Random()	乱数生成
e(P,Q)	ペアリング演算 楕円曲線上の双線形写像
H()	ハッシュ関数
KeyGen(s,ID_{pub})	秘密鍵の生成 ID_{sec}=s・ID_{pub}
MapToPoint(TA_{sys},ID_{user})	文字列を楕円曲線上の点へ変換
IDEnc(TA_{sys},ID_{pub})	ID ベース暗号を用いてランダムに変わる鍵を生成 (Boneh-Franklin の方式で行う) [P,P_s]:=TA_{sys} r_{id}=Random() k_{enc}=e(ID_{pub},P_s)^r_{id} c=r_{id}・P return (k_{enc},c)
IDDec(ID_{sec},c)	ID ベース暗号を用いて鍵を復元する k_{dec}=e(ID_{sec},c) Return k_{dec}
ReqEnc(REQ_{body},k_{enc})	要求メッセージの共通鍵方式による暗号化 Camellia,AES 等の共通鍵暗号を利用する
ReqDec()	要求メッセージの共通鍵方式による復号 Camellia,AES 等の共通鍵暗号で暗号化したメッセージを復号する
ResEnc()	応答メッセージの共通鍵方式を用いた暗号化 Camellia,AES 等の共通鍵暗号を利用する
ResDec()	応答メッセージの共通鍵方式を用いた復号 Camellia,AES 等の共通鍵暗号で暗号化したメッセージを復号する
Auth()	ユーザの認証 ID,パスワードなど、認証方式・認証情報に合わせたユーザ認証を行う。
CHKSession()	セッション情報の確認
CHKUSERSession()	ユーザのセッション情報の確認
UpdateUserSession()	ユーザのセッション情報の更新
CHKATR()	属性の確認
MAC(msg,key)	メッセージ認証コードの生成
CHKMAC()	メッセージ認証コードの確認（検証）
IDSign()	メッセージに対して署名を生成する
IDVerify()	署名検証を行う

図９

【図１０】

(a)リクエスト情報

秘密情報要求種別		KEM-key
認証情報	ユーザＩＤ	user1@example.com
	ユーザパスワード	WQvPwBMQ+7G
属性情報(ATR_{user})		date=2007/07/08:role=manager
共通鍵(r_{com})		626d027839ea0a13(octet string)

(b)情報ＲＥＱｍｓｇ

秘密情報管理サーバのＩＤ情報(ID_{TA})	http://pkg.example.com
セッション番号(SessionNo)	2007/07/08/09:10:11:123
補助鍵(c)	8df2a494492276aa(octet string)
暗号化されたリクエスト情報 ($EREQ_{body}$)	b7210eafc2e9adac32ab7aac2249693dfb f83724c2cc0736ee31c8029(octet string)

(c)レスポンス情報

情報 $IDATR_{user}$	user1@example.com.date=2007/07/08:role=manager
秘密鍵(USR_{sec})	b06869cbcac0d83afb8d0ef7cbb8324f0d7882 e5d0762fc5b7210eaf(octet string)

(d)情報ＲＥＳｍｓｇ

セッション番号(sessionNo)	2007/07/08/09:10:11:123
暗号化されたレスポンス情報 ($EKEY_{body}$)	8bac1ab66410435cb7181f95b16a b97c92b341c0e2b28483be52c74d 4b30de61(octet string)
MAC:メッセージ認証コード(RES_{mac})	cbb8324f0d7882e5(octet string)

(e)暗号装置２００$_2$から送信される暗号化データ

暗号装置２００$_1$の ID 情報 (ID_{user})	user1@example.com
属性情報	date=2007/07/08:role=manager
補助鍵 c'	839eac2e9adac(octet string)
暗号化データ	41c0e2b8483be528bac1ab66410 469cbea(octet string)

図１０

【図１１】

(a)セッション番号管理部２１９で管理されるデータ

セッション番号	2007/07/08/09:10:11:123
第一の共通鍵(r_{com})	626d027839ea0a13(octet string)
状態	鍵要求中

(b)認証情報管理部２１７で管理されるデータ

ユーザＩＤ	user1@example.com
ユーザパスワード	WQvPwBMQ+7G

(c)ユーザセッション情報管理部１１７で管理されるデータ

ユーザID	セッション番号	共通鍵	状態
user1@example.com	2007/07/08/09:10:11:123	626d027839ea0a13	発行中
user2@example.com	2007/07/06/05:04:03:210	9df4ece5826be95f	発行済
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・
user5@example.com	2007/07/08/09:08:07:654	55b4ba2db6dcd8c8	未発行
user6@example.com	2007/07/06/05:06:07:890	6410435cb7181f95	未発行

(d)利用者認証情報管理部１１３で管理されるデータ

ユーザID	ユーザパスワード
user1@example.com	WQvPwBMQ+7G
user2@example.com	JjXKl6oTLx7f
・ ・ ・	・ ・ ・
user5@example.com	2Pes2Q7LTFs3
user6@example.com	OqETUXx7Jdbx

(e)ユーザID属性管理部１１９

ユーザID	属性情報の条件
user1@example.com	notBefore=2007/6/1:notAfter=2008/3/31:role=manager
user2@example.com	notBefore=2007/6/1:notAfter=2008/3/31
・ ・ ・	・ ・ ・
user5@example.com	notBefore=2007/7/1:notAfter=2008/1/31
user6@example.com	notBefore=2007/7/1:notAfter=2008/1/31

図１１

【図１２】

処理	処理内容
IDから公開鍵の計算: MapToPoint()	署名者のID文字列ID_{user}を、TA_{sys}パラメータの楕円曲線上の点ID_{pub}に変換する。(TAの公開ID $TA_{sessionID}$はTA_{pub}に変換) ID_{pub}＝MapToPoint(TA_{sys},ID_{user})
秘密鍵生成: KeyGen()	IDに対応する楕円曲線上の点を、秘密情報管理サーバのマスターシークレットsの 楕円スカラー倍し、署名鍵ID_{sec}を生成する。 ID_{sec}=s・ID_{pub}
IDベース署名: IDsign(m,ID_{sec},TA_{sys})	署名対象のメッセージmに対して、署名鍵ID_{sec}、TA公開情報TA_{sys}を用いて署名情報(V, S)を生成する。署名対象のメッセージ(m)、署名情報(V, S)と署名者のID文字列ID_{user}を署名検証者に送信する。 [P,Ps] := TA_{sys} m = 署名対象メッセージ k = Random() P1 = 任意のTA_{sys}パラメータの楕円曲線上の点 r = e(P1,P)^k V = H(m‖r) S = V・ID_{sec}+k・P1 return (S,V)
IDベース署名検証: IDVerify(m,V,S,ID_{pub},TA_{sys})	署名検証者は、受け取ったm、V,S,ID_{user}とTA_{sys}、さらにID_{user}から変換したID_{pub}とを用いて署名検証を行う。 [P,Ps] := TA_{sys} W = e(S,P)・e(ID_{pub},−Ps)^V V'=H(m‖W) return(V==V') V==V'となるのは、V==H(m ‖ r)になるときのみであるため、V==V'であれば、認証成功であり、V!=V'であれば、認証失敗である。以下、式の展開を行う。 e(S,P) = e(V・s・ID_{pub},P)・(k・P1,P) ={e(ID_{pub},P)^(V・s)}{e(P,P1)^k} e(ID_{pub},−Ps)^V = e(ID_{pub},P)^−(V・s) W = e(S,P)・e(ID_{pub},−Ps)^V = e(P1,P)^k = r

図12