(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2012 年 1 月 26 日(26.01.2012)

PCT

(10) 国際公開番号
WO 2012/011575 A1

(51) 国際特許分類:
H04L 9/08 (2006.01)

(21) 国際出願番号: PCT/JP2011/066716

(22) 国際出願日: 2011 年 7 月 22 日(22.07.2011)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2010-166401 2010 年 7 月 23 日(23.07.2010) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電信電話株式会社(NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町二丁目３番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 小林 鉄太郎(KOBAYASHI, Tetsutaro) [JP/JP]; 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP). 竹内 格(TAKEUCHI, Kaku) [JP/JP]; 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP). 知加良 盛(CHIKARA, Sakae) [JP/JP]; 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP).

(74) 代理人: 中尾 直樹, 外(NAKAO, Naoki et al.); 〒1600022 東京都新宿区新宿三丁目１番２２号 新宿ＮＳＯビル４階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

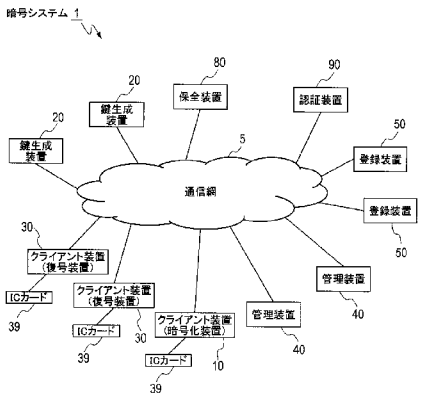
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI

[続葉有]

(54) **Title**: CRYPTOSYSTEM, CRYPTOGRAPHIC COMMUNICATION METHOD, ENCRYPTION DEVICE, KEY-GENERATING DEVICE, DECRYPTION DEVICE, CONTENT SERVER DEVICE, PROGRAM, AND RECORDING MEDIUM

(54) 発明の名称 : 暗号システム、暗号通信方法、暗号化装置、鍵生成装置、復号装置、コンテンツサーバ装置、プログラム、記憶媒体

[図1]



1 Cryptosystem
5 Communication Network
10 Client Device (Encryption Device)
20 Key-Generating Device
30 Client Device (Decryption Device)
39 IC Card
40 Management Device
50 Registration Device
80 Maintenance Device
90 Authentication Device

(57) **Abstract**: Disclosed is a cryptographic communication technique that depends on a function cipher and that can be operated flexibly. A conversion rule information pair is prescribed ahead of time, said pair being the pair of: attribute conversion rule information that stipulates conversion rules for converting attribute assignment information to attribute information used in a function encryption algorithm; and logical formula conversion rule information that stipulates conversion rules for converting logical formula assignment information to logical information used in the function encryption algorithm. Using one of the sets of conversion rule information contained in the conversion rule information pair, first attribute information or first logical information is obtained from input information. This information is used in encryption processing. In decryption processing, decryption processing of encrypted information is performed using a decryption key produced using second attribute information or second logical information obtained from user information using the other set of conversion rule information.

(57) 要約: 柔軟に運用可能であって関数暗号に依拠する暗号通信技術を提供する。属性指定情報を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している属性用変換規則情報と論理式指定情報を関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している論理式用変換規則情報とのペアである変換規則情報ペアが予め定められている。この変換規則情報ペアに含まれる一方の変換規則情報を用いて入力情報から第１属性情報または第１論理情報が得られる。この情報が暗号化処理に用いられる。復号処理では、他方の変換規則情報を用いて利用者情報から得られた第２属性情報または第２論理情報を用いて作られた復号鍵を使って、暗号情報の復号処理が行われる。

WO 2012/011575 A1

(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ：

暗号システム、暗号通信方法、暗号化装置、鍵生成装置、復号装置、コンテンツサーバ装置、プログラム、記憶媒体

技術分野

[0001] 本発明は、暗号通信技術に関し、より詳しくは、関数暗号に依拠する暗号通信技術に関する。

背景技術

[0002] これまで暗号技術として、例えば共通鍵暗号、公開鍵暗号などが知られている。

[0003] 共通鍵暗号は、メッセージの送信者が共通鍵でメッセージを暗号化して暗号化メッセージを求め、受信者が送信者と同じ共通鍵を使って暗号化メッセージを復号してメッセージを得る方式である。このため、送信者と受信者との間で安全に共通鍵を所有する手続きが必要になる。

[0004] 公開鍵暗号は、（１）受信者が一意の公開鍵とそれに対応する一意の秘密鍵を用意し、（２）送信者は受信者の公開鍵でメッセージを暗号化して暗号化メッセージを求め、（３）受信者がその秘密鍵で暗号化メッセージを復号してメッセージを得る方式である。このため、送信者がメッセージを暗号化する前に受信者の公開鍵を入手する必要がある。つまり、受信者が公開鍵を生成しないと暗号化できない。

[0005] また、近年、述語暗号が提案されている。述語暗号は、送信者による暗号化の過程で暗号メッセージに或る情報Ｘが組み込まれ、当該情報Ｘと特定の関係を満たす情報Ｙを持つ受信者が、暗号メッセージの復号や、メッセージを知ることなくメッセージに関する情報を取得することができる方式である。送信者は、暗号化の際に、必ずしも受信者の持つ情報Ｙを知っている必要はない。また、送信者は、必ずしも、暗号化する前に受信者を特定している必要もない。送信者は、自由に、能動的に、主導権を持って、情報Ｘを決め

ることができる。講学的に、情報Ｘは属性Ｉ（変数）として、情報Ｙは述語ｆ（命題関数、ブール関数）として表される。復号に際し、情報Ｘと情報Ｙとが満たすべき特定の関係は、例えばｆ（Ｉ）＝Trueである。

先行技術文献

非特許文献

[0006] 非特許文献1：ＮＴＴ情報流通プラットフォーム研究所情報セキュリティプロジェクト、“ＮＴＴの暗号要素技術”、インターネット〈URL: http://info.isl.ntt.co.jp/crypt/camellia/technology.html〉［平成２２年７月１５日検索］

非特許文献2：J. Katz, A. Sahai and B. Waters, "Predicate Encryption Supporting Disjunction, Polynomial Equations, and Inner Products", EUROCRYPT 2008, 146-162.

発明の概要

発明が解決しようとする課題

[0007] 本発明は、柔軟に運用可能な、関数暗号に依拠する暗号通信技術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

[0008] 第１の観点による本発明の概要は次のとおりである。

関数暗号を用いる暗号システムは、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含む。

そして、各鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められている。

また、属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に

変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められている。

また、属性用変換規則情報と論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている。

暗号化装置は、変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる属性用変換規則情報と論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じてポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得処理と、第１属性情報または第１論理情報と、鍵生成装置の公開鍵とを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化処理を行う。

鍵生成装置は、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得処理と、第２属性情報または第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、暗号情報の復号に用いる復号鍵を生成する鍵生成処理を行う。

復号装置は、復号鍵を用いて、関数暗号アルゴリズムに則り、暗号情報に対する復号処理を行う。

[0009] あるいは、第１の観点による本発明の概要は次のとおりである。

関数暗号を用いる暗号システムは、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含む。

そして、各鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め

定められている。

また、属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められている。

また、属性用変換規則情報と論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている。

暗号化装置は、変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる属性用変換規則情報と論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じてポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得処理と、第１属性情報または第１論理情報と、鍵生成装置の公開鍵とを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化処理を行う。

復号装置は、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得処理と、鍵生成装置から送られた復号鍵を用いて、関数暗号アルゴリズムに則り、暗号情報に対する復号処理を行う。

鍵生成装置は、第２属性情報または第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、暗号情報の復号に用いる復号鍵を生成する鍵生成処理を行う。

[0010] あるいは、第１の観点による本発明の概要は次のとおりである。

関数暗号を用いる暗号システムは、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含む。

そして、各鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められている。

また、属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められている。

また、属性用変換規則情報と論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている。

暗号化装置は、変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる属性用変換規則情報と論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じてポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得処理と、第１属性情報または第１論理情報と、鍵生成装置の公開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号情報を求める暗号化処理を行う。

鍵生成装置は、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理

情報取得処理と、第２属性情報または第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、暗号情報の復号に用いる復号鍵を生成する鍵生成処理を行う。

復号装置は、復号鍵を用いて、関数暗号アルゴリズムに則り、暗号情報に対する復号処理を行う。

[0011] あるいは、第１の観点による本発明の概要は次のとおりである。

関数暗号を用いる暗号システムは、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含む。

そして、各鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められている。

また、属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められている。

また、属性用変換規則情報と論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている。

暗号化装置は、変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる属性用変換規則情報と論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じてポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得処理と、第１属性情報または第１論理情報と、鍵生成装置の公開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号情報を求める暗号化

処理を行う。

復号装置は、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得処理と、鍵生成装置から送られた復号鍵を用いて、関数暗号アルゴリズムに則り、暗号情報に対する復号処理を行う。

鍵生成装置は、第２属性情報または第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、暗号情報の復号に用いる復号鍵を生成する鍵生成処理を行う。

[0012] 第２の観点による本発明の概要は次のとおりである。

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、複数の復号装置とを含み、関数暗号を用いる暗号システムにおいて、各鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、属性用変換規則情報と論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている。

そして、暗号化装置は、変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる属性用変換規則情報と論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じてポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得処理

と、第１属性情報または第１論理情報と、鍵生成装置の公開鍵とを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化処理を行う。

また、鍵生成装置は、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得処理と、第２属性情報または第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、暗号情報の復号に用いる復号鍵を生成する鍵生成処理を行う。

また、復号装置は、復号鍵を用いて、関数暗号アルゴリズムに則り、暗号情報に対する復号処理を行う。そして、この復号装置は、暗号情報を別の復号装置に転送する転送処理も行う。転送する暗号情報は、暗号化装置から送られたものであってもよいし、別の復号装置から転送されたものであってもよい。暗号システムに含まれる復号装置のうち少なくとも一部の復号装置が転送処理を行う機能を持つが、全ての復号装置がこの転送機能を持つことは要求されない。転送された暗号情報を受信した復号装置は、必要に応じて鍵生成装置に復号鍵を生成して貰い、上記復号処理を行う。

[0013] あるいは、第２の観点による本発明の概要は次のとおりである。

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、複数の復号装置とを含み、関数暗号を用いる暗号システムにおいて、各鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められてお

り、属性用変換規則情報と論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている。

そして、暗号化装置は、変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる属性用変換規則情報と論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じてポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得処理と、第１属性情報または第１論理情報と、鍵生成装置の公開鍵とを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化処理を行う。

また、復号装置は、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得処理と、鍵生成装置から送られた復号鍵を用いて、関数暗号アルゴリズムに則り、暗号情報に対する復号処理を行う。

また、鍵生成装置は、第２属性情報または第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、暗号情報の復号に用いる復号鍵を生成する鍵生成処理を行う。

上述の復号装置は、暗号情報を別の復号装置に転送する転送処理も行う。転送する暗号情報は、暗号化装置から送られたものであってもよいし、別の復号装置から転送されたものであってもよい。暗号システムに含まれる復号装置のうち少なくとも一部の復号装置が転送処理を行う機能を持つが、全ての復号装置がこの転送機能を持つことは要求されない。転送された暗号情報を受信した復号装置は、必要に応じて鍵生成装置に復号鍵を生成して貰い、上記復号処理を行う。

[0014] あるいは、第２の観点による本発明の概要は次のとおりである。

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、複数の復号装置とを含み、関数暗号を用いる暗号システムにおいて、各鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、属性用変換規則情報と論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている。

そして、暗号化装置は、変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる属性用変換規則情報と論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じてポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得処理と、第１属性情報または第１論理情報と、鍵生成装置の公開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号情報を求める暗号化処理を行う。

また、鍵生成装置は、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得処理と、第２属性情報または第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、暗号情報の復号に用いる復号鍵を生成する鍵生成処理を行う。

また、復号装置は、復号鍵を用いて、関数暗号アルゴリズムに則り、暗号

情報に対する復号処理を行う。そして、この復号装置は、暗号情報を別の復号装置に転送する転送処理も行う。転送する暗号情報は、暗号化装置から送られたものであってもよいし、別の復号装置から転送されたものであってもよい。暗号システムに含まれる復号装置のうち少なくとも一部の復号装置が転送処理を行う機能を持つが、全ての復号装置がこの転送機能を持つことは要求されない。転送された暗号情報を受信した復号装置は、必要に応じて鍵生成装置に復号鍵を生成して貰い、上記復号処理を行う。

[0015] あるいは、第２の観点による本発明の概要は次のとおりである。

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、複数の復号装置とを含み、関数暗号を用いる暗号システムにおいて、各鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、属性用変換規則情報と論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている。

そして、暗号化装置は、変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる属性用変換規則情報と論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じてポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得処理と、第１属性情報または第１論理情報と、鍵生成装置の公開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号情報を求める暗号化処理を行う。

また、復号装置は、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得処理と、鍵生成装置から送られた復号鍵を用いて、関数暗号アルゴリズムに則り、暗号情報に対する復号処理を行う。

また、鍵生成装置は、第２属性情報または第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、暗号情報の復号に用いる復号鍵を生成する鍵生成処理を行う。

上述の復号装置は、暗号情報を別の復号装置に転送する転送処理も行う。転送する暗号情報は、暗号化装置から送られたものであってもよいし、別の復号装置から転送されたものであってもよい。暗号システムに含まれる復号装置のうち少なくとも一部の復号装置が転送処理を行う機能を持つが、全ての復号装置がこの転送機能を持つことは要求されない。転送された暗号情報を受信した復号装置は、必要に応じて鍵生成装置に復号鍵を生成して貰い、上記復号処理を行う。

[0016] 第３の観点による本発明の概要は次のとおりである。

関数暗号を用いる暗号システムは、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含む。

そして、各鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められている。

また、属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められて

いる。

また、属性用変換規則情報と論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている。

暗号化装置は、変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる属性用変換規則情報と論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じてポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得処理と、第１属性情報または第１論理情報と、鍵生成装置の公開鍵と、コンテンツとを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報と、当該共通鍵で当該コンテンツを暗号化した暗号化コンテンツとを求める暗号化処理を行う。

コンテンツサーバ装置は、各暗号化装置から送られた暗号情報および暗号化コンテンツを記憶する処理と、復号装置からの要求に応じて暗号化コンテンツとこれに対応する暗号情報を当該復号装置に送信する送信処理を行う。

鍵生成装置は、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得処理と、第２属性情報または第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、暗号情報の復号に用いる復号鍵を生成する鍵生成処理を行う。

復号装置は、コンテンツサーバ装置に対する暗号化コンテンツの取得要求処理と、復号鍵を用いて、関数暗号アルゴリズムに則り、コンテンツサーバ装置から取得した暗号情報に対する復号処理と、この復号処理で得られた共通鍵を用いて、コンテンツサーバ装置から取得した暗号化コンテンツを復号するコンテンツ取得処理と、暗号化コンテンツから復号されたコンテンツを

表示する処理を行う。

[0017] あるいは、第３の観点による本発明の概要は次のとおりである。

関数暗号を用いる暗号システムは、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含む。

そして、各鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められている。

また、属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められている。

また、属性用変換規則情報と論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている。

暗号化装置は、変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる属性用変換規則情報と論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じてポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得処理と、第１属性情報または第１論理情報と、鍵生成装置の公開鍵と、コンテンツとを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報と、当該共通鍵で当該コンテンツを暗号化した暗号化コンテンツとを求める暗号化処理を行う。

コンテンツサーバ装置は、各暗号化装置から送られた暗号情報および暗号化コンテンツを記憶する処理と、復号装置からの要求に応じて暗号化コンテ

ンツとこれに対応する暗号情報を当該復号装置に送信する送信処理を行う。

復号装置は、コンテンツサーバ装置に対する暗号化コンテンツの取得要求処理と、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得処理と、復号鍵を用いて、関数暗号アルゴリズムに則り、コンテンツサーバ装置から取得した暗号情報に対する復号処理と、この復号処理で得られた共通鍵を用いて、コンテンツサーバ装置から取得した暗号化コンテンツを復号するコンテンツ取得処理と、暗号化コンテンツから復号されたコンテンツを表示する処理を行う。

鍵生成装置は、第２属性情報または第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、暗号情報の復号に用いる復号鍵を生成する鍵生成処理を行う。

[0018] あるいは、第３の観点による本発明の概要は次のとおりである。

関数暗号を用いる暗号システムは、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含む。

そして、各鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められている。

また、属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められている。

また、属性用変換規則情報と論理式用変換規則情報のうちいずれであるか

を特定するためのポリシー情報が予め定められている。

暗号化装置は、変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる属性用変換規則情報と論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じてポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得処理と、第１属性情報または第１論理情報と、鍵生成装置の公開鍵と、コンテンツとを用いて、関数暗号アルゴリズムに則り、当該コンテンツを暗号化した暗号化コンテンツを求める暗号化処理を行う。

コンテンツサーバ装置は、各暗号化装置から送られた暗号化コンテンツを記憶する処理と、復号装置からの要求に応じて暗号化コンテンツを当該復号装置に送信する送信処理を行う。

鍵生成装置は、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得処理と、第２属性情報または第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、暗号化コンテンツの復号に用いる復号鍵を生成する鍵生成処理を行う。

復号装置は、コンテンツサーバ装置に対する暗号化コンテンツの取得要求処理と、復号鍵を用いて、関数暗号アルゴリズムに則り、コンテンツサーバ装置から取得した暗号化コンテンツを復号する復号処理と、暗号化コンテンツから復号されたコンテンツを表示する処理を行う。

[0019] あるいは、第３の観点による本発明の概要は次のとおりである。

関数暗号を用いる暗号システムは、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含む。

そして、各鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められている。

また、属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められている。

また、属性用変換規則情報と論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている。

暗号化装置は、変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる属性用変換規則情報と論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じてポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得処理と、第１属性情報または第１論理情報と、鍵生成装置の公開鍵と、コンテンツとを用いて、関数暗号アルゴリズムに則り、当該コンテンツを暗号化した暗号化コンテンツを求める暗号化処理を行う。

コンテンツサーバ装置は、各暗号化装置から送られた暗号化コンテンツを記憶する処理と、復号装置からの要求に応じて暗号化コンテンツを当該復号装置に送信する送信処理を行う。

復号装置は、コンテンツサーバ装置に対する暗号化コンテンツの取得要求処理と、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報

取得処理と、復号鍵を用いて、関数暗号アルゴリズムに則り、コンテンツサーバ装置から取得した暗号化コンテンツを復号する復号処理と、暗号化コンテンツから復号されたコンテンツを表示する処理を行う。

鍵生成装置は、第２属性情報または第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、暗号化コンテンツの復号に用いる復号鍵を生成する鍵生成処理を行う。

発明の効果

[0020] 本発明に拠れば、変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる属性用変換規則情報と論理式用変換規則情報のうち、暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報または論理情報を得ることから、関数暗号に依拠する暗号通信を柔軟に運用できる。

図面の簡単な説明

[0021] [図1]第１の観点による各実施形態に関る暗号システムの構成図。

[図2]第１の観点による各実施形態に関る暗号通信方法の処理手順を示す図（その１）。

[図3]第１の観点による各実施形態に関る暗号通信方法の処理手順を示す図（その２）。

[図4]第１の観点による各実施形態に関る暗号通信方法の処理手順を示す図（その３）。

[図5]第１の観点による第１実施形態に関る暗号化装置の機能ブロック図。

[図6]第１の観点による第１実施形態に関る暗号化処理の処理手順の詳細を示す図。

[図7]第１の観点による第１実施形態に関る復号装置の機能ブロック図。

[図8]第１の観点による第１実施形態に関る復号処理の処理手順の詳細を示す図。

[図9]第１の観点による第１実施形態に関る鍵生成装置の機能ブロック図。

[図10]第１の観点による第１実施形態に関る鍵生成処理の処理手順の詳細を示す図。

[図11]入力情報または利用者情報からポリシーに対応するスキーマを用いて、属性情報または述語情報を得ることを図解した図。

[図12]属性指定情報から属性用スキーマを用いて、属性情報を得ることを図解した図。

[図13]述語指定情報から述語用スキーマを用いて、述語情報を得ることを図解した図。

[図14]ポリシーの例を示す図。

[図15]復号鍵テーブルの例を示す図。

[図16]認証テーブルの例を示す図。

[図17]利用者情報テーブルの例を示す図。

[図18]第１の観点による第２実施形態に関る復号装置の機能ブロック図。

[図19]第１の観点による第２実施形態に関る復号処理の処理手順の詳細を示す図。

[図20]第１の観点による第２実施形態に関る鍵生成装置の機能ブロック図。

[図21]第１の観点による第２実施形態に関る鍵生成処理の処理手順の詳細を示す図。

[図22]第１の観点による第３実施形態に関る暗号化装置の機能ブロック図。

[図23]第１の観点による第３実施形態に関る暗号化処理の処理手順の詳細を示す図。

[図24]第１の観点による第３実施形態に関る復号装置の機能ブロック図。

[図25]第１の観点による第３実施形態に関る復号処理の処理手順の詳細を示す図。

[図26]第１の観点による第４実施形態に関る復号装置の機能ブロック図。

[図27]第１の観点による第４実施形態に関る復号処理の処理手順の詳細を示す図。

[図28]第２の観点による各実施形態に関る暗号システムの構成図。

[図29]第２の観点による各実施形態に関る暗号通信方法の処理手順を示す図（その１）。

[図30]第２の観点による各実施形態に関る暗号通信方法の処理手順を示す図（その２）。

[図31]第２の観点による各実施形態に関る暗号通信方法の処理手順を示す図（その３）。

[図32]第２の観点による各実施形態に関る暗号通信方法の処理手順を示す図（その４）。

[図33]第２の観点による第１実施形態に関る暗号化装置の機能ブロック図。

[図34]第２の観点による第１実施形態に関る暗号化処理の処理手順の詳細を示す図。

[図35]第２の観点による第１実施形態に関る第１の復号装置の機能ブロック図。

[図36]第２の観点による第１実施形態に関る第１の復号処理の処理手順の詳細を示す図。

[図37]第２の観点による第１実施形態に関る第２の復号装置の機能ブロック図。

[図38]第２の観点による第１実施形態に関る第２の復号処理の処理手順の詳細を示す図。

[図39]第２の観点による第１実施形態に関る鍵生成装置の機能ブロック図。

[図40]第２の観点による第１実施形態に関る鍵生成処理の処理手順（第１の復号装置に対応）の詳細を示す図。

[図41]第２の観点による第１実施形態に関る鍵生成処理の処理手順（第２の復号装置に対応）の詳細を示す図。

[図42]第２の観点による第２実施形態に関る第１の復号装置の機能ブロック図。

[図43]第２の観点による第２実施形態に関る第１の復号処理の処理手順の詳細を示す図。

[図44]第２の観点による第２実施形態に関る第２の復号装置の機能ブロック図。

[図45]第２の観点による第２実施形態に関る第２の復号処理の処理手順の詳細を示す図。

[図46]第２の観点による第２実施形態に関る鍵生成装置の機能ブロック図。

[図47]第２の観点による第２実施形態に関る鍵生成処理の処理手順（第１の復号装置に対応）の詳細を示す図。

[図48]第２の観点による第２実施形態に関る鍵生成処理の処理手順（第２の復号装置に対応）の詳細を示す図。

[図49]第２の観点による第３実施形態に関る暗号化装置の機能ブロック図。

[図50]第２の観点による第３実施形態に関る暗号化処理の処理手順の詳細を示す図。

[図51]第２の観点による第３実施形態に関る第１の復号装置の機能ブロック図。

[図52]第２の観点による第３実施形態に関る第１の復号処理の処理手順の詳細を示す図。

[図53]第２の観点による第３実施形態に関る第２の復号装置の機能ブロック図。

[図54]第２の観点による第３実施形態に関る第２の復号処理の処理手順の詳細を示す図。

[図55]第２の観点による第４実施形態に関る第１の復号装置の機能ブロック図。

[図56]第２の観点による第４実施形態に関る第１の復号処理の処理手順の詳細を示す図。

[図57]第２の観点による第４実施形態に関る第２の復号装置の機能ブロック図。

[図58]第２の観点による第４実施形態に関る第２の復号処理の処理手順の詳細を示す図。

[図59]電子メールシステムやインスタントメッセージングシステムとして実施される場合における、送受信されるデータの構成の例を示す図。

[図60]第３の観点による各実施形態に関る暗号システムの構成図。

[図61]第３の観点による各実施形態に関る暗号通信方法の処理手順を示す図（その１）。

[図62]第３の観点による各実施形態に関る暗号通信方法の処理手順を示す図（その２）。

[図63]第３の観点による各実施形態に関る暗号通信方法の処理手順を示す図（その３）。

[図64]第３の観点による各実施形態に関る暗号通信方法の処理手順を示す図（その４）。

[図65]第３の観点による第１実施形態に関る暗号化装置の機能ブロック図。

[図66]第３の観点による第１実施形態に関る暗号化処理の処理手順の詳細を示す図。

[図67]第３の観点による第１実施形態に関るコンテンツサーバ装置の機能ブロック図。

[図68]第３の観点による第１実施形態に関る復号装置の機能ブロック図。

[図69]第３の観点による第１実施形態に関る復号処理の処理手順の詳細を示す図。

[図70]第３の観点による第１実施形態に関る鍵生成装置の機能ブロック図。

[図71]第３の観点による第１実施形態に関る鍵生成処理の処理手順の詳細を示す図。

[図72]第３の観点による第２実施形態に関る復号装置の機能ブロック図。

[図73]第３の観点による第２実施形態に関る復号処理の処理手順の詳細を示す図。

[図74]第３の観点による第２実施形態に関る鍵生成装置の機能ブロック図。

[図75]第３の観点による第２実施形態に関る鍵生成処理の処理手順の詳細を示す図。

[図76]第３の観点による第３実施形態に関る暗号化装置の機能ブロック図。

[図77]第３の観点による第３実施形態に関る暗号化処理の処理手順の詳細を示す図。

[図78]第３の観点による第３実施形態に関る復号装置の機能ブロック図。

[図79]第３の観点による第３実施形態に関る復号処理の処理手順の詳細を示す図。

[図80]第３の観点による第４実施形態に関る復号装置の機能ブロック図。

[図81]第３の観点による第４実施形態に関る復号処理の処理手順の詳細を示す図。

[図82]コンテンツ配信システムとして実施される場合における、送受信されるデータの構成の例を示す図。

[図83]命題変数PR0(1),PR0(2)と命題変数PR0(3)の否定¬PR0(3)と論理記号∧, ∨とを含む標準形論理式PR0(1)∧PR0(2)∨¬PR0(3)を表現する木構造データを例示する図。

[図84]命題変数PR0(1),PR0(2),PR0(3),PR0(6),PR0(7)と命題変数PR0(4),PR0(5)の否定¬PR0(4),¬PR0(5)と論理記号∧, ∨とを含む標準形論理式PR0(1)∧PR0(2)∨PR0(2)∧PR0(3)∨PR0(1)∧PR0(3)∨¬PR0(4)∨(¬PR0(5)∧PR0(6))∧PR0(7)を表現する木構造データを例示する図。

発明を実施するための形態

[0022] ＜関数暗号の概要＞

近年、関数暗号と呼ばれるＩＤベース暗号の拡張暗号が話題となっている。関数暗号は下記の４つのアルゴリズム(Setup,KeyGen,Enc,Dec)から構成される。プロトコルの概略は下記のとおりである。

《プロトコルFE》

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

・Setup(1^λ)→(pk,sk)：セットアップアルゴリズム

セキュリティパラメータ1^λを入力とし、公開パラメータpkとマスター鍵skを出力する確率的多項式時間アルゴリズム

・KeyGen(sk,i)→sk_i：鍵生成アルゴリズム

マスター鍵skと鍵識別子iを入力とし、当該鍵識別子iに対応する秘密鍵sk_iを出力する確率的多項式時間アルゴリズム

・Enc(pk,j,x)→c_j：暗号化アルゴリズム

公開パラメータpkと受信者識別子jと暗号化対象の情報（平文）xを入力とし、暗号文c_jを出力する確率的多項式時間アルゴリズム

・Dec(pk,sk_i,c_j)→y：復号アルゴリズム

公開パラメータpkと秘密鍵sk_iと暗号文c_jを入力とし、平文yを出力する確率的多項式時間アルゴリズム

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

[0023] 関数暗号では、ＩＤベース暗号の正当性が拡張されており、暗号文の受信者は鍵識別子iを持つ秘密鍵と受信者識別子jを持つ暗号文から平文xに関する何らかの関数$f_{i,j}(x)$を評価することができるようになっている。即ち、或る関数$f_{i,j}(x)$が存在し$\forall i$，$\forall j$，$\forall x \in \{0,1\}^{poly(\lambda)}$に対して式（Ａ）で表される確率Prがλに関して圧倒的（１との差が無視しうる）であるとき、その関数暗号(Setup,KeyGen,Enc,Dec)は正当であると云う。なお、poly(λ)はλで決まる多項式長を表している。

[数1]

$$\Pr\left[y = f_{i,j}(x) \;\middle|\; \begin{array}{c} (pk, sk) \leftarrow Setup(1^{\lambda}) \\ sk_i \leftarrow KeyGen(sk, i) \\ c_j \leftarrow Enc(pk, j, x) \\ y \leftarrow Dec(pk, sk_i, c_j) \end{array} \right] \qquad \cdots(A)$$

[0024] 特に、或る関係Ｒ(・,・)が存在し、式（Ｂ）で表されるタイプの関数$f_{i,j}(x)$を持つ関数暗号は様々な暗号を包含している（⊥は正常に復号できなかったことを表す記号である）。

[数2]

$$f_{i,j}(x) = \begin{cases} x & (R(i,j) : True) \\ \perp & (R(i,j) : False) \end{cases} \qquad \cdots(B)$$

[0025] 例えばＩＤベース暗号は式（Ｃ）で表される関数$f_{i,j}(x)$を持つ関数暗号と定義することができる。

[数3]

$$f_{i,j}(x)=\begin{cases} x & (i=j) \\ \perp & (i\neq j) \end{cases} \qquad \cdots(C)$$

[0026] より高度な関係Ｒ(・,・)を持つ様々な関数暗号が研究されている。このタイプの関数暗号のうち最も汎用性の高いものは属性ベース暗号(attribute-based encryption, ABE)あるいは述語暗号(predicate encryption, PE)等と呼ばれ、よく研究されている。2010年に岡本龍明らは多項式サイズの述語および述語変数の集合に対応し、標準的な暗号学的仮定の下で適応的識別子攻撃に対してＣＣＡ安全が証明できる比較的実用的なこのタイプの関数暗号を提案した（参考文献Ｒ１参照）。

（参考文献Ｒ１）Tatsuaki Okamoto and Katsuyuki Takashima, "Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption," In: Advances in Cryptology -- CRYPTO 2010, Lecture Notes in Computer Science, Volume 6223, 191-208, Springer-Verlag, 2010, Full paper: http://eprint.iacr.org/2010/563/

[0027] 鍵識別子iを述語、受信者識別子jを述語変数のインスタンスとして式（Ｄ）で表される関係Ｒ(・,・)を持つ関数暗号は鍵ポリシー関数暗号と呼ばれる。このとき、暗号文が平文xだけでなく述語変数のインスタンスjも秘匿する事を属性秘匿と云う。

[数4]

$$R(i,j)=\begin{cases} True & (\text{受信者識別子}\ j\ \text{が述語}\ i\ \text{を充足する}) \\ False & (\text{受信者識別子}\ j\ \text{が述語}\ i\ \text{を充足しない}) \end{cases} \qquad \cdots(D)$$

[0028] 鍵識別子iを述語変数、受信者識別子jを述語のインスタンスとして式（Ｅ）で表される関係Ｒ(・,・)を持つ関数暗号は暗号文ポリシー関数暗号と呼ばれる。このとき、暗号文が平文xだけでなく述語jも秘匿する事を述語秘匿と云う。

[数5]

$$R(i,j)=\begin{cases} True & (\text{鍵識別子}\ i\ \text{が述語}\ j\ \text{を充足する}) \\ False & (\text{鍵識別子}\ i\ \text{が述語}\ j\ \text{を充足しない}) \end{cases} \quad \cdots(E)$$

[0029] 属性秘匿を持つ鍵ポリシー関数暗号あるいは述語秘匿を持つ暗号文ポリシー関数暗号を述語暗号と呼ばれる（参考文献Ｒ２参照）。

（参考文献Ｒ２）Tatsuaki Okamoto and Katsuyuki Takashima, "Hierarchical Predicate Encryption for Inner-Products," ASIACRYPT 2009: pp.214-231, 2009.

[0030] ＜閾値ゲート＞

関数暗号における閾値ゲートの構成は、N個の分散情報のうち任意のt個が与えられれば秘密を復元できるが、任意のt-1個以下の分散情報が与えられても秘密を復元できない閾値秘密分散方式、即ちt-out-of-N秘密分散方式を用いて実現される。t-out-of-N秘密分散については参考文献Ｒ３などを参照されたい。t-out-of-N秘密分散方式を用いた閾値ゲートはt-out-of-N閾値ゲートと呼ばれる。t-out-of-N閾値ゲートは入力のN個の条件式のうちt個以上の条件が成立すると真を出力し、それ以外は偽を出力するゲート構造を有する。t-out-of-N閾値ゲートの（出力の）否定は（全入力の）否定の(N-t+1)-out-of-N閾値ゲートと等価である。

（参考文献Ｒ３）A. Shamir, "How to Share a Secret", Communications of the ACM, November 1979, Volume 22, Number 11, pp.612-613.

[0031] ＜秘密鍵検証可能関数暗号＞

関数暗号のうち、秘密鍵sk_iが鍵識別子iに対して正しく作られていることが納得できるものは、秘密鍵検証可能関数暗号と呼ばれる。鍵生成手続きが正しく行われたことを証明する非対話零知識証明（参考文献Ｒ４参照）を秘密鍵に付加することによって、秘密鍵検証可能関数暗号を構成することができる。秘密鍵検証可能関数暗号を用いれば秘密鍵sk_iが鍵識別子iに対して正しく作られていることが納得できる。

（参考文献Ｒ４）Jens Groth and Amit Sahai, "Efficient Non-interactive

Proof Systems for Bilinear Groups,"Advances in Cryptology - EUROCRYPT 2008, LNCS 4965, pp.415-432, March 2010.

[0032] ＜暗号文公開検証可能関数暗号＞

関数暗号のうち、暗号文に対してKeyGenアルゴリズムから得られる如何なる鍵を持たなくとも、暗号文が正しく作られていることが納得できるものは暗号文公開検証可能関数暗号と呼ばれる。暗号化手続きが正しく行われたことを証明する非対話零知識証明（上記参考文献Ｒ４参照）を暗号文に付加することによって、暗号文公開検証可能関数暗号を構成することができる。暗号文公開検証可能関数暗号を用いれば暗号文に対して復号可能などの鍵を使っても同じ結果が得られることが納得できる。

[0033] ＜電子署名＞

電子署名とは次の３つのアルゴリズム$(KeyGen_{\Sigma},Sign_{\Sigma},Verify_{\Sigma})$のことである。プロトコルの概略は下記のとおりである。

《プロトコルES》

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

・$KeyGen_{\Sigma}(1^{\lambda})\rightarrow(sk_{\Sigma},pk_{\Sigma})$：鍵生成アルゴリズム

セキュリティパラメータ1^{λ}を入力とし、電子署名検証用公開鍵pk_{Σ}と電子署名用秘密鍵sk_{Σ}を出力する確率的多項式時間アルゴリズム

・$Sign_{\Sigma}(sk_{\Sigma},m)\rightarrow\sigma$：署名アルゴリズム

電子署名用秘密鍵sk_{Σ}と署名対象情報mを入力とし、署名σを出力する確率的多項式時間アルゴリズム

・$Verify_{\Sigma}(pk_{\Sigma},m,\sigma)\rightarrow0/1$：署名検証アルゴリズム

電子署名検証用公開鍵pk_{Σ}と署名対象情報mと署名σを入力とし、検証結果(拒絶(0)または受理(1))を出力する確率的多項式時間アルゴリズム

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

[0034] なお、適当な暗号学的仮定の下、適応的選択文書攻撃に対して存在的偽造不可が証明可能な電子署名方式が提案されている（例えば、RSA-PSS（参考文献Ｒ５参照））。

（参考文献Ｒ５）藤岡淳、暗号アルゴリズム評価報告書RSA-PSS、日本電信電話株式会社、2001年

[0035] 次に、関数暗号について概説する。説明に先立ち記号等を定義する。

〔定義〕

行列：「行列」とは演算が定義された集合の元を矩形に並べたものを表す。環の元を要素とするものだけではなく、群の元を要素とするものも「行列」と表現する。

$(\cdot)^{T}$：$(\cdot)^{T}$は・の転置行列を表す。

$(\cdot)^{-1}$：$(\cdot)^{-1}$は・の逆行列を表す。

∧：∧は論理積（ＡＮＤ）を表す論理記号である。

∨：∨は論理和（ＯＲ）を表す論理記号である。

¬：¬は否定（ＮＯＴ）を表す論理記号である。

命題変数：命題変数は命題の「真」,「偽」（"false","true"）を要素とする集合｛真，偽｝上の変数である。命題変数及び命題変数の否定を総称してリテラル（literal）と呼ぶ。

論理式：論理式とは数理論理学における命題を表す形式的文法を有する式を意味する。具体的には「真」及び「偽」は論理式であり、命題変数は論理式であり、論理式の否定は論理式であり、論理式と論理式との論理積は論理式であり、論理式と論理式との論理和は論理式である。

Ｚ：Ｚは整数集合を表す。

sec：secはセキュリティパラメータ（$sec \in Z$, $sec>0$）を表す。

0^{*}：0^{*}は*個の0からなる列を表す。

1^{*}：1^{*}は*個の１からなる列を表す。

[0036] F_q：F_qは位数qの有限体を表す。位数qは１以上の整数であり、例えば、素数や素数のべき乗値を位数qとする。すなわち、有限体F_qの例は素体やそれを基礎体とした拡大体である。なお、有限体F_qが素体である場合の演算は、例えば、位数qを法とする剰余演算によって容易に構成できる。また、有限体F_qが拡大体である場合の演算は、例えば、既約多項式を法とする剰余演算によって

容易に構成できる。有限体F_qの具体的な構成方法は、例えば、参考文献１「ISO/IEC 18033-2: Information technology - Security techniques - Encryption algorithms - Part 2: Asymmetric ciphers」に開示されている。

0_F：0_Fは有限体F_qの加法単位元を表す。

1_F：1_Fは有限体F_qの乗法単位元を表す。

$\delta(i,j)$：$\delta(i,j)$はクロネッカーのデルタ関数を表す。i=jの場合に$\delta(i,j)=1_F$を満たし、i≠jの場合に$\delta(i,j)=0_F$を満たす。

[0037] E：Eは有限体F_q上で定義された楕円曲線を表す。Eはアフィン（affine）座標版のWeierstrass方程式

$$y^2+a_1\cdot x\cdot y+a_3\cdot y=x^3+a_2\cdot x^2+a_4\cdot x+a_6$$

（ただし、$a_1,a_2,a_3,a_4,a_6\in F_q$）を満たす$x,y\in F_q$からなる点(x,y)の集合に無限遠点と呼ばれる特別な点Ｏを付加したもので定義される。楕円曲線Ｅ上の任意の２点に対して楕円加算と呼ばれる二項演算＋及び楕円曲線E上の任意の１点に対して楕円逆元と呼ばれる単項演算－がそれぞれ定義できる。また、楕円曲線E上の有理点からなる有限集合が楕円加算に関して群をなすこと、楕円加算を用いて楕円スカラー倍算と呼ばれる演算が定義できること、及びコンピュータ上での楕円加算などの楕円演算の具体的な演算方法はよく知られている（例えば、参考文献１、参考文献２「RFC 5091: Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems」、参考文献３「イアン・Ｆ・ブラケ、ガディエル・セロッシ、ナイジェル・Ｐ・スマート＝著、「楕円曲線暗号」、出版＝ピアソン・エデュケーション、ISBN4-89471-431-0」等参照）。

また、楕円曲線E上の有理点からなる有限集合は位数p(p≧1)の部分群を持つ。例えば、楕円曲線E上の有理点からなる有限集合の要素数を＃Eとし、pを＃Eを割り切る大きい素数とした場合、楕円曲線Eのp等分点からなる有限集合E[p]は、楕円曲線E上の有理点からなる有限集合の部分群を構成する。なお、楕円曲線Eのp等分点とは、楕円曲線E上の点Aのうち、楕円曲線E上での楕円スカラー倍算値p・Aがp・A＝Ｏを満たす点を意味する。

[0038] G_1, G_2, G_T：G_1, G_2, G_Tは位数qの巡回群を表す。巡回群G_1, G_2の具体例は、楕円曲線Eのp等分点からなる有限集合E[p]やその部分群である。$G_1=G_2$であってもよいし$G_1\neq G_2$であってもよい。また、巡回群G_Tの具体例は、有限体F_qを基礎体とする拡大体を構成する有限集合である。その一例は、有限体F_qの代数閉包における１のｐ乗根からなる有限集合である。巡回群G_1, G_2, G_Tの位数と有限体F_qの位数とを同一とすることで安全性が向上する。

なお、本形態では、巡回群G_1, G_2上で定義された演算を加法的に表現し、巡回群G_T上で定義された演算を乗法的に表現する。すなわち、$\chi\in F_q$及び$\Omega\in G_1$に対する$\chi\cdot\Omega\in G_1$は、$\Omega\in G_1$に対して巡回群G_1で定義された演算をχ回施すことを意味し、Ω_1, $\Omega_2\in G_1$に対する$\Omega_1+\Omega_2\in G_1$は、$\Omega_1\in G_1$と$\Omega_2\in G_1$とを被演算子として巡回群G_1で定義された演算を行うことを意味する。同様に、$\chi\in F_q$及び$\Omega\in G_2$に対する$\chi\cdot\Omega\in G_2$は、$\Omega\in G_2$に対して巡回群G_2で定義された演算をχ回施すことを意味し、Ω_1, $\Omega_2\in G_2$に対する$\Omega_1+\Omega_2\in G_2$は、$\Omega_1\in G_2$と$\Omega_2\in G_2$とを被演算子として巡回群G_2で定義された演算を行うことを意味する。一方、$\chi\in F_q$及び$\Omega\in G_T$に対する$\Omega^{\chi}\in G_T$は、$\Omega\in G_T$に対して巡回群G_Tで定義された演算をχ回施すことを意味し、$\Omega_1, \Omega_2\in G_T$に対する$\Omega_1\cdot\Omega_2\in G_T$は、$\Omega_1\in G_T$と$\Omega_2\in G_T$とを被演算子として巡回群$G_T$で定義された演算を行うことを意味する。

[0039] Ψ：Ψは1以上の整数を表す。

ϕ：ϕは0以上Ψ以下の整数$\phi=0,\ldots,\Psi$を表す。

λ：λは1以上Ψ以下の整数$\lambda=1,\ldots,\Psi$を表す。

$n(\phi)$：$n(\phi)$は1以上の整数を表す。

$\zeta(\phi)$：$\zeta(\phi)$は0以上の整数を表す。

$G_1^{n(\phi)+\zeta(\phi)}$：$G_1^{n(\phi)+\zeta(\phi)}$は$n(\phi)+\zeta(\phi)$個の巡回群$G_1$の直積を表す。

$G_2^{n(\phi)+\zeta(\phi)}$：$G_2^{n(\phi)+\zeta(\phi)}$は$n(\phi)+\zeta(\phi)$個の巡回群$G_2$の直積を表す。

g_1, g_2, g_T：g_1, g_2, g_Tは巡回群G, G_1, G_2, G_Tの生成元を表す。

$V(\phi)$：$V(\phi)$は$n(\phi)+\zeta(\phi)$個の巡回群G_1の直積からなる$n(\phi)+\zeta(\phi)$次元のベクトル空間を表す。

$V^*(\phi)$：$V^*(\phi)$は$n(\phi)+\zeta(\phi)$個の巡回群G_2の直積からなる$n(\phi)+\zeta(\phi)$次

元のベクトル空間を表す。

[0040] e_ϕ：e_ϕは直積$G_1^{n(\phi)+\zeta(\phi)}$と直積$G_2^{n(\phi)+\zeta(\phi)}$との直積$G_1^{n(\phi)+\zeta(\phi)}\times G_2^{n(\phi)+\zeta(\phi)}$を巡回群$G_T$に写す非退化な双線形写像（bilinear map）を表す。双線形写像e_ϕは、巡回群G_1の$n(\phi)+\zeta(\phi)$個の元$\gamma_\beta(\beta=1,...,n(\phi)+\zeta(\phi))$と巡回群$G_2$の$n(\phi)+\zeta(\phi)$個の元$\gamma_\beta^*(\beta=1,...,n(\phi)+\zeta(\phi))$とを入力とし、巡回群$G_T$の１個の元を出力する。

$$e_\phi : G_1^{n(\phi)+\zeta(\phi)}\times G_2^{n(\phi)+\zeta(\phi)}\rightarrow G_T \qquad \cdots(1)$$

[0041] 双線形写像e_ϕは以下の性質を満たす。

［双線形性］すべての$\Gamma_1\in G_1^{n(\phi)+\zeta(\phi)}$，$\Gamma_2\in G_2^{n(\phi)+\zeta(\phi)}$及び$\nu$，$\kappa\in F_q$について以下の関係を満たす。

$$e_\phi(\nu\cdot\Gamma_1,\kappa\cdot\Gamma_2)=e_\phi(\Gamma_1,\Gamma_2)^{\nu\cdot\kappa} \qquad \cdots(2)$$

［非退化性］すべての$\Gamma_1\in G_1^{n(\phi)+\zeta(\phi)}$，$\Gamma_2\in G_2^{n(\phi)+\zeta(\phi)}$を巡回群$G_T$の単位元に写す写像ではない。

［計算可能性］あらゆる

$$\Gamma_1\in G_1^{n(\phi)+\zeta(\phi)},\ \Gamma_2\in G_2^{n(\phi)+\zeta(\phi)} \qquad \cdots(3)$$

について$e_\phi(\Gamma_1,\Gamma_2)$を効率的に計算するアルゴリズムが存在する。

[0042] 本形態では、巡回群G_1と巡回群G_2との直積$G_1\times G_2$を巡回群G_Tに写す非退化な双線形写像

$$Pair:G_1\times G_2\rightarrow G_T \qquad \cdots(4)$$

を用いて双線形写像e_ϕを構成する。本形態の双線形写像e_ϕは、巡回群G_1の$n(\phi)+\zeta(\phi)$個の元$\gamma_\beta(\beta=1,...,n(\phi)+\zeta(\phi))$からなる$n(\phi)+\zeta(\phi)$次元ベクトル$(\gamma_1,...,\gamma_{n(\phi)+\zeta(\phi)})$と、巡回群$G_2$の$n(\phi)+\zeta(\phi)$個の元$\gamma_\beta^*(\beta=1,...,n(\phi)+\zeta(\phi))$からなる$n(\phi)+\zeta(\phi)$次元ベクトル$(\gamma_1^*,...,\gamma_{n(\phi)+\zeta(\phi)}^*)$との入力に対し、巡回群$G_T$の１個の元を出力する。

$$e_\phi : \Pi_{\beta=1}^{n(\phi)+\zeta(\phi)}Pair(\gamma_\beta,\ \gamma_\beta^*) \qquad \cdots(5)$$

[0043] なお、双線形写像Pairは、巡回群G_1の１個の元と巡回群G_2の１個の元との組を入力とし、巡回群G_Tの１個の元を出力する。双線形写像Pairは、以下の性質を満たす。

［双線形性］すべての$\Omega_1 \in G_1$，$\Omega_2 \in G_2$及びν，$\kappa \in F_q$について以下の関係を満たす。

$$Pair(\nu \cdot \Omega_1, \kappa \cdot \Omega_2) = Pair(\Omega_1, \Omega_2)^{\nu \cdot \kappa} \quad \cdots(6)$$

［非退化性］すべての

$$\Omega_1 \in G_1, \ \Omega_2 \in G_2 \quad \cdots(7)$$

を巡回群G_Tの単位元に写す写像ではない。

［計算可能性］あらゆる$\Omega_1 \in G_1$，$\Omega_2 \in G_2$について$Pair(\Omega_1, \Omega_2)$を効率的に計算するアルゴリズムが存在する。

双線形写像Pairの具体例は、Weilペアリングや Tateペアリングなどのペアリング演算を行うための関数である（例えば、参考文献４「Alfred. J. Menezes, ELLIPTIC CURVE PUBLIC KEY CRYPTOSYSTEMS, KLUWER ACADEMIC PUBLISHERS, ISBN0-7923-9368-6, pp. 61-81」等参照）。また、楕円曲線Eの種類に応じ、Tateペアリングなどのペアリング演算を行うための関数と所定の関数phiを組み合わせた変更ペアリング関数$e(\Omega_1, phi(\Omega_2))$（$\Omega_1 \in G_1$，$\Omega_2 \in G_2$）を双線形写像Pairとして用いてもよい（例えば、参考文献２等参照）。また、ペアリング演算をコンピュータ上で行うためのアルゴリズムとしては、周知のMiller のアルゴリズム（参考文献５「V. S. Miller, “Short Programs for functions on Curves,” 1986, インターネット<http://crypto.stanford.edu/miller/miller.pdf>」などが存在する。また、ペアリング演算を効率的に行うための楕円曲線や巡回群の構成方法はよく知られている（例えば、参考文献２、参考文献６「A. Miyaji, M. Nakabayashi, S.Takano, ”New explicit conditions of elliptic curve Traces for FR-Reduction,” IEICE Trans. Fundamentals, vol. E84-A, no05, pp. 1234-1243, May 2001」、参考文献７「P.S.L.M. Barreto, B. Lynn, M. Scott, ”Constructing elliptic curves with prescribed embedding degrees,” Proc. SCN ’2002, LNCS 2576, pp.257-267, Springer-Verlag. 2003」、参考文献８「R. Dupont, A. Enge, F. Morain, ”Building curves with arbitrary small MOV degree over finite prime fields,” http://eprint.iacr.org/2002/094/」等参照）。

[0044] $a_i(\phi)(i=1,...,n(\phi)+\zeta(\phi))$：$a_i(\phi)$は巡回群$G_1$の$n(\phi)+\zeta(\phi)$個の元を要素とする$n(\phi)+\zeta(\phi)$次元の基底ベクトルを表す。基底ベクトル$a_i(\phi)$の一例は、$\kappa_1 \cdot g_1 \in G_1$をi次元目の要素とし、残りの$n(\phi)+\zeta(\phi)-1$個の要素を巡回群$G_1$の単位元（加法的に「0」と表現）とする$n(\phi)+\zeta(\phi)$次元の基底ベクトルである。この場合、$n(\phi)+\zeta(\phi)$次元の基底ベクトル$a_i(\phi)(i=1,...,n(\phi)+\zeta(\phi))$の各要素をそれぞれ列挙して表現すると、以下のようになる。

$$a_1(\phi)=(\kappa_1 \cdot g_1,0,0,...,0)$$
$$a_2(\phi)=(0,\kappa_1 \cdot g_1,0,...,0) \quad \cdots(8)$$
$$...$$
$$a_{n(\phi)+\zeta(\phi)}(\phi)=(0,0,0,...,\kappa_1 \cdot g_1)$$

ここで、κ_1は加法単位元0_F以外の有限体F_qの元からなる定数であり、$\kappa_1 \in F_q$の具体例は$\kappa_1=1_F$である。基底ベクトル$a_i(\phi)$は直交基底であり、巡回群G_1の$n(\phi)+\zeta(\phi)$個の元を要素とするすべての$n(\phi)+\zeta(\phi)$次元ベクトルは、$n(\phi)+\zeta(\phi)$次元の基底ベクトル$a_i(\phi)(i=1,...,n(\phi)+\zeta(\phi))$の線形和によって表される。すなわち、$n(\phi)+\zeta(\phi)$次元の基底ベクトル$a_i(\phi)$は前述のベクトル空間$V(\phi)$を張る。

[0045] $a_i^*(\phi)(i=1,...,n(\phi)+\zeta(\phi))$：巡回群$G_2$の$n(\phi)+\zeta(\phi)$個の元を要素とする$n(\phi)+\zeta(\phi)$次元の基底ベクトルを表す。基底ベクトル$a_i^*(\phi)$の一例は、$\kappa_2 \cdot g_2 \in G_2$をi次元目の要素とし、残りの$n(\phi)+\zeta(\phi)-1$個の要素を巡回群$G_2$の単位元（加法的に「0」と表現）とする$n(\phi)+\zeta(\phi)$次元の基底ベクトルである。この場合、基底ベクトル$a_i^*(\phi)(i=1,...,n(\phi)+\zeta(\phi))$の各要素をそれぞれ列挙して表現すると、以下のようになる。

$$a_1^*(\phi)=(\kappa_2 \cdot g_2,0,0,...,0)$$
$$a_2^*(\phi)=(0,\kappa_2 \cdot g_2,0,...,0) \quad \cdots(9)$$
$$...$$
$$a_{n(\phi)+\zeta(\phi)}^*(\phi)=(0,0,0,...,\kappa_2 \cdot g_2)$$

ここで、κ_2は加法単位元0_F以外の有限体F_qの元からなる定数であり、$\kappa_2 \in F_q$の具体例は$\kappa_2=1_F$である。基底ベクトル$a_i^*(\phi)$は直交基底であり、巡回群G_2のn

(φ)+ζ(φ)個の元を要素とするすべてのn(φ)+ζ(φ)次元ベクトルは、n(φ)+ζ(φ)次元の基底ベクトル$a_i^*(\phi)$(i=1,...,n(φ)+ζ(φ))の線形和によって表される。すなわち、n(φ)+ζ(φ)次元の基底ベクトル$a_i^*(\phi)$は前述のベクトル空間V*(φ)を張る。

なお、基底ベクトル$a_i(\phi)$と基底ベクトル$a_i^*(\phi)$とは、0_Fを除く有限体F_qの元$\tau=\kappa_1\cdot\kappa_2$について

$$e_\phi(a_i(\phi),\ a_j^*(\phi))=g_T^{\tau\cdot\delta(i,j)} \qquad \cdots(10)$$

を満たす。すなわち、i=jの場合には、式(5)(6)の関係から、

$$e_\phi(a_i(\phi),\ a_j^*(\phi))=\mathrm{Pair}(\kappa_1\cdot g_1,\kappa_2\cdot g_2)\cdot\mathrm{Pair}(0,\ 0)\cdot\ldots\cdot\mathrm{Pair}(0,\ 0)$$

$$=\mathrm{Pair}(g_1,\ g_2)^{\kappa1\cdot\kappa2}\cdot\mathrm{Pair}(g_1,\ g_2)^{0\cdot0}\cdot\ldots\cdot\mathrm{Pair}(g_1,\ g_2)^{0\cdot0}$$

$$=\mathrm{Pair}(g_1,\ g_2)^{\kappa1\cdot\kappa2}=g_T^{\tau}$$

を満たす。なお、上付き添え字κ1, κ2はそれぞれκ_1, κ_2を表す。一方、i≠jの場合には、$e_\phi(a_i(\phi),\ a_j^*(\phi))=\Pi_{i=1}^{n(\phi)+\zeta(\phi)}\mathrm{Pair}(a_i(\phi),\ a_j^*(\phi))$の右辺は、$\mathrm{Pair}(\kappa_1\cdot g_1,\kappa_2\cdot g_2)$を含まず、$\mathrm{Pair}(\kappa_1\cdot g_1,0)$と $\mathrm{Pair}(0,\kappa_2\cdot g_2)$とPair(0,0)との積になる。さらに、式(6)の関係から$\mathrm{Pair}(g_1,\ 0)=\mathrm{Pair}(0,\ g_2)=\mathrm{Pair}(g_1,\ g_2)^0$を満たす。そのため、i≠jの場合には、

$$e_\phi(a_i(\phi),\ a_j^*(\phi))=e_\phi(g_1,\ g_2)^0=g_T^0$$

を満たす。

特に、$\tau=\kappa_1\cdot\kappa_2=1_F$である場合（例えば、$\kappa_1=\kappa_2=1_F$の場合）、

$$e(a_i(\phi),\ a_j^*(\phi))=g_T^{\delta(i,j)} \qquad \cdots(11)$$

を満たす。ここで、$g_T^0=1$は巡回群G_Tの単位元であり、$g_T^1=g_T$は巡回群G_Tの生成元である。この場合、基底ベクトル$a_i(\phi)$と基底ベクトル$a_i^*(\phi)$とは双対正規直交基底であり、ベクトル空間V(φ)とベクトル空間V*(φ)とは、双線形写像を構成可能な双対ベクトル空間〔双対ペアリングベクトル空間（DPVS:Dual Paring Vector space)〕である。

[0046] A(φ)：基底ベクトル$a_i(\phi)$(i=1,...,n(φ)+ζ(φ))を要素とするn(φ)+ζ(φ)行n(φ)+ζ(φ)列の行列を表す。例えば、基底ベクトル$a_i(\phi)$(i=1,...,n(

ϕ)+ζ(ϕ))が式(8)によって表現される場合、行列A(ϕ)は、

[数6]

$$A(\psi)=\begin{pmatrix} a_1(\psi) \\ a_2(\psi) \\ \vdots \\ a_{n(\psi)+\zeta(\psi)}(\psi) \end{pmatrix}=\begin{pmatrix} \kappa_1\cdot g_1 & 0 & \cdots & 0 \\ 0 & \kappa_1\cdot g_1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \kappa_1\cdot g_1 \end{pmatrix} \quad \cdots(12)$$

となる。

[0047] A*(ϕ)：基底ベクトル$a_i^*(\phi)$(i=1,...,n(ϕ)+ζ(ϕ))を要素とするn(ϕ)+ζ(ϕ)行n(ϕ)+ζ(ϕ)列の行列を表す。例えば、基底ベクトル$a_i^*(\phi)$(i=1,...,n(ϕ)+ζ(ϕ))が式(9)によって表現される場合、行列A*(ϕ)は、

[数7]

$$A^*(\psi)=\begin{pmatrix} a_1^*(\psi) \\ a_2^*(\psi) \\ \vdots \\ a_{n(\psi)+\zeta(\psi)}^*(\psi) \end{pmatrix}=\begin{pmatrix} \kappa_2\cdot g_2 & 0 & \cdots & 0 \\ 0 & \kappa_2\cdot g_2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \kappa_2\cdot g_2 \end{pmatrix} \quad \cdots(13)$$

となる。

[0048] X(ϕ)：X(ϕ)は有限体F_qの元を要素とするn(ϕ)+ζ(ϕ)行n(ϕ)+ζ(ϕ)列の行列を表す。行列X(ϕ)は基底ベクトル$a_i(\phi)$の座標変換に用いられる。行列X(ϕ)のi行j列(i=1,...,n(ϕ)+ζ(ϕ),j=1,...,n(ϕ)+ζ(ϕ))の要素を$\chi_{i,j}(\phi)\in F_q$とすると、行列X(ϕ)は、

[数8]

$$X(\psi)=\begin{pmatrix} \chi_{1,1}(\psi) & \chi_{1,2}(\psi) & \cdots & \chi_{1,n(\psi)+\zeta(\psi)}(\psi) \\ \chi_{2,1}(\psi) & \chi_{2,2}(\psi) & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n(\psi)+\zeta(\psi),1}(\psi) & \chi_{n(\psi)+\zeta(\psi),2}(\psi) & \cdots & \chi_{n(\psi)+\zeta(\psi),n(\psi)+\zeta(\psi)}(\psi) \end{pmatrix} \quad \cdots(14)$$

となる。なお、行列X(ϕ)の各要素$\chi_{i,j}(\phi)$を変換係数と呼ぶ。

[0049] X*(ϕ)：X*(ϕ)と行列X(ϕ)とはX*(ϕ)=$\tau'\cdot(X(\phi)^{-1})^T$の関係を満たす。ただし、$\tau'\in F_q$は有限体$F_q$に属する任意の定数であり、例えば、$\tau'=1_F$である。X*($\phi$)は基底ベクトル$a_i^*(\phi)$の座標変換に用いられる。行列X*($\phi$)のi行j列の

要素を$\chi_{i,j}^{*}(\psi)\in F_q$とすると、行列$X^{*}(\psi)$は、

[数9]

$$X^{*}(\psi)=\begin{pmatrix} \chi_{1,1}^{*}(\psi) & \chi_{1,2}^{*}(\psi) & \cdots & \chi_{1,n(\psi)+\zeta(\psi)}^{*}(\psi) \\ \chi_{2,1}^{*}(\psi) & \chi_{2,2}^{*}(\psi) & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n(\psi)+\zeta(\psi),1}^{*}(\psi) & \chi_{n(\psi)+\zeta(\psi),2}^{*} & \cdots & \chi_{n(\psi)+\zeta(\psi),n(\psi)+\zeta(\psi)}^{*} \end{pmatrix} \quad \cdots(15)$$

となる。なお、行列$X^{*}(\psi)$の各要素$\chi_{i,j}^{*}(\psi)$を変換係数と呼ぶ。

この場合、$n(\psi)+\zeta(\psi)$行$n(\psi)+\zeta(\psi)$列の単位行列を$I(\psi)$とすると$X(\psi)\cdot(X^{*}(\psi))^{T}=\tau'\cdot I(\psi)$を満たす。すなわち、単位行列

[数10]

$$I(\psi)=\begin{pmatrix} 1_F & 0_F & \cdots & 0_F \\ 0_F & 1_F & & \vdots \\ \vdots & & \ddots & 0_F \\ 0_F & 0_F & \cdots & 1_F \end{pmatrix} \quad \cdots(16)$$

に対し、

[数11]

$$\begin{pmatrix} \chi_{1,1}(\psi) & \chi_{1,2}(\psi) & \cdots & \chi_{1,n(\psi)+\zeta(\psi)}(\psi) \\ \chi_{2,1}(\psi) & \chi_{2,2}(\psi) & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n(\psi)+\zeta(\psi),1}(\psi) & \chi_{n(\psi)+\zeta(\psi),2}(\psi) & \cdots & \chi_{n(\psi)+\zeta(\psi),n(\psi)+\zeta}(\psi) \end{pmatrix}$$
$$\times\begin{pmatrix} \chi_{1,1}^{*}(\psi) & \chi_{2,1}^{*}(\psi) & \cdots & \chi_{n(\psi)+\zeta(\psi),1}^{*}(\psi) \\ \chi_{1,2}^{*}(\psi) & \chi_{2,2}^{*}(\psi) & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{1,n(\psi)+\zeta(\psi)}^{*}(\psi) & \chi_{2,n(\psi)+\zeta(\psi)}^{*}(\psi) & \cdots & \chi_{n(\psi)+\zeta(\psi),n(\psi)+\zeta(\psi)}^{*}(\psi) \end{pmatrix}$$
$$=\tau'\cdot\begin{pmatrix} 1_F & 0_F & \cdots & 0_F \\ 0_F & 1_F & & \vdots \\ \vdots & & \ddots & 0_F \\ 0_F & 0_F & \cdots & 1_F \end{pmatrix} \quad \cdots(17)$$

を満たす。ここで、$n(\psi)+\zeta(\psi)$次元ベクトル

$$\chi_{i}^{\rightarrow}(\psi)=(\chi_{i,1}(\psi),\ldots,\chi_{i,n(\psi)+\zeta(\psi)}(\psi)) \quad \cdots(18)$$

$$\chi_{j}^{\rightarrow *}(\psi)=(\chi_{j,1}^{*}(\psi),\ldots,\chi_{j,n(\psi)+\zeta(\psi)}^{*}(\psi)) \quad \cdots(19)$$

を定義する。すると、式(17)の関係から、$n(\psi)+\zeta(\psi)$次元ベクトル$\chi_{i}^{\rightarrow}(\psi)$

と$\chi_j^{\rightarrow *}(\phi)$との内積は、

$$\chi_i^{\rightarrow}(\phi)\cdot\chi_j^{\rightarrow *}(\phi)=\tau'\cdot\delta(i,j) \qquad \cdots(20)$$

となる。

[0050] $b_i(\phi)$：$b_i(\phi)$は巡回群G_1の$n(\phi)+\zeta(\phi)$個の元を要素とする$n(\phi)+\zeta(\phi)$次元の基底ベクトルを表す。$b_i(\phi)$は行列$X(\phi)$を用いて基底ベクトル$a_i(\phi)$ ($i=1,\ldots,n(\phi)+\zeta(\phi)$)を座標変換することで得られる。具体的には、基底ベクトル$b_i(\phi)$は、

$$b_i(\phi)=\Sigma_{j=1}^{n(\phi)+\zeta(\phi)}\chi_{i,j}(\phi)\cdot a_j(\phi) \qquad \cdots(21)$$

の演算によって得られる。例えば、基底ベクトル$a_j(\phi)$($j=1,\ldots,n(\phi)+\zeta(\phi)$)が式(8)によって表現される場合、基底ベクトル$b_i(\phi)$の各要素をそれぞれ列挙して表現すると、以下のようになる。

$$b_i(\phi)=(\chi_{i,1}(\phi)\cdot\kappa_1\cdot g_1,\ \chi_{i,2}(\phi)\cdot\kappa_1\cdot g_1,$$
$$\ldots,\ \chi_{i,n(\phi)+\zeta(\phi)}(\phi)\cdot\kappa_1\cdot g_1) \qquad \cdots(22)$$

巡回群G_1の$n(\phi)+\zeta(\phi)$個の元を要素とするすべての$n(\phi)+\zeta(\phi)$次元ベクトルは、$n(\phi)+\zeta(\phi)$次元の基底ベクトル$b_i(\phi)$($i=1,\ldots,n(\phi)+\zeta(\phi)$)の線形和によって表される。すなわち、$n(\phi)+\zeta(\phi)$次元の基底ベクトル$b_i(\phi)$は前述のベクトル空間$V(\phi)$を張る。

[0051] $b_i^*(\phi)$：$b_i^*(\phi)$は巡回群G_2の$n(\phi)+\zeta(\phi)$個の元を要素とする$n(\phi)+\zeta(\phi)$次元の基底ベクトルを表す。$b_i^*(\phi)$は行列$X^*(\phi)$を用いて基底ベクトル$a_i^*(\phi)$ ($i=1,\ldots,n(\phi)+\zeta(\phi)$)を座標変換することで得られる。具体的には、基底ベクトル$b_i^*(\phi)$は、

$$b_i^*(\phi)=\Sigma_{j=1}^{n(\phi)+\zeta(\phi)}\chi_{i,j}^*(\phi)\cdot a_j^*(\phi) \qquad \cdots(23)$$

の演算によって得られる。例えば、基底ベクトル$a_j^*(\phi)$ ($j=1,\ldots,n(\phi)+\zeta(\phi)$)が式(9)によって表現される場合、基底ベクトル$b_i^*(\phi)$の各要素をそれぞれ列挙して表現すると、以下のようになる。

$$b_i^*(\phi)=(\chi_{i,1}^*(\phi)\cdot\kappa_2\cdot g_2\ ,\ \chi_{i,2}^*(\phi)\cdot\kappa_2\cdot g_2,$$
$$\ldots,\ \chi_{i,n(\phi)+\zeta(\phi)}^*(\phi)\cdot\kappa_2\cdot g_2) \qquad \cdots(24)$$

となる。巡回群G_2の$n(\phi)+\zeta(\phi)$個の元を要素とするすべての$n(\phi)+\zeta(\phi)$次

元ベクトルは、$n(\psi)+\zeta(\psi)$次元の基底ベクトル$b_i^*(\psi)$($i=1,\ldots,n(\psi)+\zeta(\psi)$)の線形和によって表される。すなわち、$n(\psi)+\zeta(\psi)$次元の基底ベクトル$b_i^*(\psi)$は前述のベクトル空間$V^*(\psi)$を張る。

なお、基底ベクトル$b_i(\psi)$と基底ベクトル$b_i^*(\psi)$とは、0_Fを除く有限体F_qの元$\tau=\kappa_1\cdot\kappa_2$について

$$e_\phi(b_i(\psi),\ b_j^*(\psi))=g_T^{\tau\cdot\tau'\cdot\delta(i,j)} \quad \cdots(25)$$

を満たす。すなわち、式(5)(20)(22)(24)の関係から、

[数12]

$$e_\psi(b_i(\psi),b_j^*(\psi))=\prod_{\beta=1}^{n(\psi)+\zeta(\psi)}\mathrm{Pair}(\chi_{i,\beta}(\psi)\cdot\kappa_1\cdot g_1,\chi_{j,\beta}^*(\psi)\cdot\kappa_2\cdot g_2)$$
$$=\mathrm{Pair}(g_1,g_2)^{\kappa_1\cdot\kappa_2\cdot\vec{\chi_i}(\psi)\cdot\vec{\chi_j}^*(\psi)}$$
$$=\mathrm{Pair}(g_1,g_2)^{\tau\tau'\cdot\delta(i,j)}=g_T^{\tau\cdot\tau'\cdot\delta(i,j)}$$

を満たす。特に$\tau=\kappa_1\cdot\kappa_2=1_F$（例えば、$\kappa_1=\kappa_2=1_F$）及び$\tau'=1_F$である場合、

$$e_\phi(b_i(\psi),\ b_j^*(\psi))=g_T^{\delta(i,j)} \quad \cdots(26)$$

を満たす。この場合、基底ベクトル$b_i(\psi)$と基底ベクトル$b_i^*(\psi)$とは、双対ペアリングベクトル空間（ベクトル空間$V(\psi)$とベクトル空間$V^*(\psi)$）の双対正規直交基底である。

なお、式(25)の関係を満たすのであれば、式(8)(9)で例示したもの以外の基底ベクトル$a_i(\psi)$及び$a_i^*(\psi)$や、式(21)(23)で例示したもの以外の基底ベクトル$b_i(\psi)$及び$b_i^*(\psi)$を用いてもよい。

[0052] $B(\psi)$：$B(\psi)$は基底ベクトル$b_i(\psi)$（$i=1,\ldots,n(\psi)+\zeta(\psi)$）を要素とする$n(\psi)+\zeta(\psi)$行$n(\psi)+\zeta(\psi)$列の行列である。$B(\psi)=X(\psi)\cdot A(\psi)$を満たす。例えば、基底ベクトル$b_i(\psi)$が式(22)によって表現される場合、行列$B(\psi)$は

、

[数13]

$$B(\psi)=\begin{pmatrix} b_1(\psi) \\ b_2(\psi) \\ \vdots \\ b_{n(\psi)+\zeta(\psi)}(\psi) \end{pmatrix} \quad \cdots(27)$$
$$=\begin{pmatrix} \chi_{1,1}(\psi)\cdot\kappa_1\cdot g_1 & \cdots & \chi_{1,n(\psi)+\zeta(\psi)}(\psi)\cdot\kappa_1\cdot g_1 \\ \vdots & \ddots & \vdots \\ \chi_{n(\psi)+\zeta(\psi),1}(\psi)\cdot\kappa_1\cdot g_1 & \cdots & \chi_{n(\psi)+\zeta(\psi),n(\psi)+\zeta(\psi)}\cdot\kappa_1\cdot g_1 \end{pmatrix}$$

となる。

[0053] $B^*(\phi)$：$B^*(\phi)$は基底ベクトル$b_i^*(\phi)$（$i=1,\ldots,n(\phi)+\zeta(\phi)$）を要素とする$n(\phi)+\zeta(\phi)$行$n(\phi)+\zeta(\phi)$列の行列を表す。$B^*(\phi)=X^*(\phi)\cdot A^*(\phi)$を満たす。例えば、基底ベクトル$b_i^*(\phi)$（$i=1,\ldots,n(\phi)+\zeta(\phi)$）が式(24)によって表現される場合、行列$B^*(\phi)$は、

[数14]

$$B^*(\psi)=\begin{pmatrix} b_1^*(\psi) \\ b_2^*(\psi) \\ \vdots \\ b_{n(\psi)+\zeta(\psi)}^*(\psi) \end{pmatrix}$$
$$=\begin{pmatrix} \chi_{1,1}^*(\psi)\cdot\kappa_2\cdot g_2 & \cdots & \chi_{1,n(\psi)+\zeta(\psi)}^*(\psi)\cdot\kappa_2\cdot g_2 \\ \vdots & \ddots & \vdots \\ \chi_{n(\psi)+\zeta(\psi),1}^*(\psi)\cdot\kappa_2\cdot g_2 & \cdots & \chi_{n(\psi)+\zeta(\psi),n(\psi)+\zeta(\psi)}^*(\psi)\cdot\kappa_2\cdot g_2 \end{pmatrix}$$

$\cdots(28)$

となる。

[0054] $v(\lambda)^{\rightarrow}$：$v(\lambda)^{\rightarrow}$は有限体F_qの元を要素とする$n(\lambda)$次元ベクトルを表す。

$$v(\lambda)^{\rightarrow}=(v_1(\lambda),\ldots,v_{n(\lambda)}(\lambda))\in F_q^{n(\lambda)} \quad \cdots(29)$$

$v_\mu(\lambda)$：$v_\mu(\lambda)$は$n(\lambda)$次元ベクトル$v(\lambda)^{\rightarrow}$のμ（$\mu=1,\ldots,n(\lambda)$）番目の要素を表す。

$w(\lambda)^{\rightarrow}$：$w(\lambda)^{\rightarrow}$は有限体F_qの元を要素とする$n(\lambda)$次元ベクトルを表す。

$$w(\lambda)^{\rightarrow}=(w_1(\lambda),\ldots,w_{n(\lambda)}(\lambda))\in F_q^{n(\lambda)} \quad \cdots(30)$$

$w_\mu(\lambda)$：$w_\mu(\lambda)$は$n(\lambda)$次元ベクトル$w(\lambda)^{\rightarrow}$のμ（$\mu=1,\ldots,n(\lambda)$）番目の要

素を表す。

Enc：Encは共通鍵暗号方式の暗号化処理を示す共通鍵暗号関数を表す。

$Enc_K(M)$：$Enc_K(M)$は、共通鍵Kを用い、共通鍵暗号関数Encに従って平文Mを暗号化して得られた暗号文を表す。

Dec：Decは、共通鍵暗号方式の復号処理を示す共通鍵復号関数を表す。

$Dec_K(C)$：$Dec_K(C)$は、共通鍵Kを用い、共通鍵復号関数Decに従って暗号文Cを復号して得られた復号結果を表す。

[0055] 〔関数暗号方式〕

次に、関数暗号方式の基本的な構成について説明する。

関数暗号方式とは、第１情報と第２情報との組み合わせによって定まる論理式の真理値が「真」となる場合に暗号文が復号される方式である。「第１情報」と「第２情報」の一方が暗号文に埋め込まれ、他方が鍵情報に埋め込まれる。例えば、「”Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products,” with Amit Sahai and Brent Waters One of 4 papers from Eurocrypt 2008 invited to the Journal of Cryptology」（参考文献９）に開示された述語暗号方式は関数暗号方式の一種である。

[0056] これ以外にも様々な公知の関数暗号方式が存在するが、以下では未公開の新たな関数暗号方式を説明する。以下に説明する新たな関数暗号方式では秘密情報に応じた値が所定の論理式に応じた態様で階層的に秘密分散される。所定の論理式は、第１情報と第２情報との組み合わせによって真理値が定まる命題変数を含み、必要に応じてさらに論理記号∧，∨，¬の何れか又はすべてを含む。そして、各命題変数の真理値が特定されることで定まる当該所定の論理式の真理値が「真」となる場合に秘密情報に応じた値が復元され、それに基づいて暗号文が復号される。

[0057] ＜論理式と階層的な秘密分散との関係＞

上述した所定の論理式と階層的な秘密分散との関係を説明する。

秘密分散とは、しきい値K_t($K_t \geqq 1$)個以上のシェア情報が得られた場合にの

み秘密情報が復元されるように、秘密情報をN(N≧2)個のシェア情報に分散することである。K_t=Nを満たす秘密分散の方式（SSS: Secret Sharing Scheme）をN-out-of-N分散方式（或いは「N-out-of-Nしきい値分散方式」）といい、K_t＜Nを満たす秘密分散の方式をK_t-out-of-N分散方式（或いは「K_t-out-of-Nしきい値分散方式」）という（例えば、参考文献１０「黒沢馨、尾形わかは、“現代暗号の基礎数理（電子情報通信レクチャーシリーズ)”、コロナ社 、２００４年３月、p.116-119」、参考文献１１「A. Shamir, "How to Share a Secret", Communications of the ACM, November 1979, Volume 22, Number 11, pp.612-613.」等参照）。

[0058] N-out-of-N分散方式は、すべてのシェア情報share(1),...,share(N)が与えられれば秘密情報SEを復元できるが、任意のN-1個のシェア情報share(ϕ_1),...,share(ϕ_{N-1})が与えられても秘密情報SEの情報はまったく得られない方式である。以下に、その一例を示す。

・SH_1,...,SH_{N-1}をランダムに選択する。

・SH_N=SE-(SH_1+...+SH_{N-1})の計算を行う。

・SH_1,...,SH_Nを各シェア情報share(1),...,share(N)とする。

・すべてのシェア情報share(1),...,share(N)が与えられれば、

SE=share(1)+...+share(N) …(31)

の復元処理によって秘密情報SEの復元が可能である。

[0059] K_t-out-of-N分散方式は、任意の相違なるK_t個のシェア情報share(ϕ_1),...,share(ϕ_{Kt})が与えられれば秘密情報SEを復元できるが、任意のK_t-1個のシェア情報share(ϕ_1),...,share(ϕ_{Kt-1})が与えられても秘密情報SEの情報はまったく得られない方式である。なお、添え字のKtはK_tを表す。以下にK_t-out-of-N分散方式の一例を示す。

[0060] ・f(0)=SEを満たすK_t-1次の多項式$f(x)=\xi_0+\xi_1\cdot x+\xi_2\cdot x^2+...+\xi_{Kt-1}\cdot x^{Kt-1}$をランダムに選ぶ。すなわち、$\xi_0$=SEとし、$\xi_1$,..., ξ_{Kt-1}をランダムに選ぶ。シェア情報をshare(ρ)=(ρ, f(ρ)) (ρ=1,...,N) とする。なお、(ρ, f(ρ))はρ及びf(ρ)の値をそれぞれ抽出可能な情報であり、例えばρとf(ρ)

とのビット結合値である。

[0061] ・任意の相違なるK_t個のシェア情報share(ϕ_1),...,share(ϕ_{Kt})((ϕ_1,...,ϕ_{Kt})⊂(1,...,N))が得られた場合、例えば、ラグランジェ(Lagrange)の補間公式を用い、以下のような復元処理によって秘密情報SEの復元が可能である。

$$SE=f(0)=LA_1 \cdot f(\phi_1)+...+ LA_{Kt} \cdot f(\phi_{Kt}) \quad \cdots(32)$$

[数15]

$$LA_\rho(x)=\frac{(x-\phi_1)\cdots\overset{\rho}{\vee}\cdots(x-\phi_{K_t})}{(\phi_\rho-\phi_1)\cdots\overset{\rho}{\vee}\cdots(\phi_\rho-\phi_{K_t})}\in F_q \quad \cdots(33)$$

なお、「$\cdots\overset{\rho}{\vee}\cdots$」は先頭からρ番目の被演算子〔分母の要素($\phi_\rho-\phi_\rho$)、分子の要素($x-\phi_\rho$)〕が存在しないことを意味する。すなわち、式(33)の分母は、

$$(\phi_\rho-\phi_1)\cdot...\cdot(\phi_\rho-\phi_{\rho-1})\cdot(\phi_\rho-\phi_{\rho+1})\cdot...\cdot(\phi_\rho-\phi_{Kt})$$

であり、式(33)の分子は、

$$(x-\phi_1)\cdot...\cdot(x-\phi_{\rho-1})\cdot(x-\phi_{\rho+1})\cdot...\cdot(x-\phi_{Kt})$$

である。

[0062] 上述した各秘密分散は体上でも実行可能である。また、これらを拡張して秘密情報SEに応じた値をシェア情報shareに秘密分散することもできる。秘密情報SEに応じた値とは秘密情報SEそのものや秘密情報SEの関数値であり、シェア情報shareに応じた値とはシェア情報shareそのものやシェア情報の関数値である。例えば、有限体F_qの元である秘密情報SE∈F_qに応じた巡回群G_Tの元g_T^{SE}∈G_Tを秘密情報SEの各シェア情報share(1),share(2)に応じた巡回群G_Tの元$g_T^{share(1)}$,$g_T^{share(2)}$∈G_Tに秘密分散することもできる。また、上述した秘密情報SEはシェア情報shareの線形結合となる(式(31)(32))。このように秘密情報SEがシェア情報shareの線形結合となる秘密分散方式を線形秘密分散方式と呼ぶ。

[0063] 上述した所定の論理式は、秘密情報を階層的に秘密分散して得られる木構造データによって表現できる。すなわち、ド・モルガンの法則により、上述

した所定の論理式はリテラルからなる論理式、又は、論理記号∧，∨の少なくとも一部とリテラルとからなる論理式（これらを「標準形論理式」と呼ぶことにする）によって表現でき、この標準形論理式は秘密情報を階層的に秘密分散して得られる木構造データによって表現できる。

[0064] 標準形論理式を表現する木構造データは複数のノードを含み、少なくとも一部のノードは１個以上の子ノードの親ノードとされ、親ノードの１つはルートノードとされ、子ノードの少なくとも一部は葉ノードとされる。ルートノードの親ノードや、葉ノードの子ノードは存在しない。ルートノードには秘密情報に応じた値が対応し、各親ノードの子ノードには当該親ノードに対応する値を秘密分散したシェア情報に応じた値が対応する。各ノードでの秘密分散形態（秘密分散方式やしきい値）は標準形論理式に応じて定まる。また、各葉ノードには標準形論理式を構成する各リテラルが対応し、当該各リテラルの真理値は第１情報と第２情報との組み合わせによって定まる。

[0065] ここで、真理値が真となったリテラルに対応する葉ノードに対応するシェア情報に応じた値は得られるが、真理値が偽となったリテラルに対応する葉ノードに対応するシェア情報に応じた値は得られないものとする。また、上述した秘密分散の性質により、親ノードに対応するシェア情報に応じた値（その親ノードがルートノードであれば秘密情報に応じた値）は、その子ノードに対応するシェア情報に応じた値が当該親ノードに対応するしきい値以上の個数だけ得られた場合にのみ復元される。そのため、どの葉ノードに対応するリテラルの真理値が真になったのかと木構造データの構成（各ノードでの秘密分散の形態を含む）とに応じ、最終的にルートノードに対応する秘密情報に応じた値が復元できるか否かが定まる。そして、各葉ノードに対応する各リテラルの真理値が標準形論理式の真理値を真にする場合にのみ最終的にルートノードに対応する秘密情報に応じた値が復元できるように木構造データが構成されている場合、このような木構造データは標準形論理式を表現する。このような標準形論理式を表現する木構造データは容易に設定できる。以下に具体例を示す。

[0066] 図８３は、命題変数PRO(1),PRO(2)と命題変数PRO(3)の否定¬PRO(3)と論理記号∧，∨とを含む標準形論理式PRO(1)∧PRO(2)∨¬PRO(3)を表現する木構造データを例示する図である。図８３に例示する木構造データは複数のノード$N_1,...,N_5$を含む。ノードN_1はノードN_2,N_5の親ノードとされ、ノードN_2はノードN_3,N_4の親ノードとされ、親ノードの１つノードN_1がルートノードとされ、子ノードの一部であるノードN_3,N_4,N_5が葉ノードとされる。ノードN_1には秘密情報SEに応じた値が対応し、ノードN_1の子ノードN_2,N_5には、秘密情報SEに応じた値が1-out-of-2分散方式で秘密分散された各シェア情報SE,SEに応じた値がそれぞれ対応する。ノードN_2の子ノードN_3,N_4には、シェア情報SEに応じた値が2-out-of-2分散方式で秘密分散された各シェア情報SE-SH_1,SH_1に応じた値がそれぞれ対応する。すなわち、葉ノードN_3にはシェア情報share(1)=SE-SH_1に応じた値が対応し、葉ノードN_4にはシェア情報share(2)=SH_1に応じた値が対応し、葉ノードN_5にはシェア情報share(3)=SEに応じた値が対応する。また、葉ノードN_3,N_4,N_5には標準形論理式PRO(1)∧PRO(2)∨¬PRO(3)を構成する各リテラルPRO(1),PRO(2),¬PRO(3)がそれぞれ対応し、当該各リテラルPRO(1),PRO(2),¬PRO(3)の真理値は第１情報と第２情報との組み合わせによって定まる。ここで、真理値が真となったリテラルに対応する葉ノードに対応するシェア情報に応じた値は得られるが、真理値が偽となったリテラルに対応する葉ノードに対応するシェア情報に応じた値は得られない。この場合、第１情報と第２情報との組み合わせが標準形論理式PRO(1)∧PRO(2)∨¬PRO(3)の真理値を真にする場合にのみ秘密情報SEに応じた値が復元される。

[0067] 図８４は、命題変数PRO(1),PRO(2),PRO(3),PRO(6),PRO(7)と命題変数PRO(4),PRO(5)の否定¬PRO(4),¬PRO(5)と論理記号∧，∨とを含む標準形論理式PRO(1)∧PRO(2)∨PRO(2)∧PRO(3)∨PRO(1)∧PRO(3)∨¬PRO(4)∨(¬PRO(5)∧PRO(6))∧PRO(7)を表現する木構造データを例示する図である。

図８４に例示する木構造データは複数のノード$N_1,...,N_{11}$を含む。ノードN_1はノードN_2,N_6,N_7の親ノードとされ、ノードN_2はノードN_3,N_4,N_5の親ノードとされ、ノードN_7はノードN_8,N_{11}の親ノードとされ、ノードN_8はノードN_9,N_{10}の親ノ

ードとされ、親ノードの１つであるノードN_1がルートノードとされ、ノードN_3,N_4,N_5,N_6,N_9,N_{10},N_{11}が葉ノードとされる。ノードN_1には秘密情報SEに応じた値が対応し、ノードN_1の子ノードN_2,N_6,N_7には、秘密情報SEに応じた値が1-out-of-3分散方式で秘密分散された各シェア情報SE,SE,SEに応じた値がそれぞれ対応する。ノードN_2の子ノードN_3,N_4,N_5には、シェア情報SEに応じた値が2-out-of-3分散方式で秘密分散された各シェア情報(1,f(1)),(2,f(2)),(3,f(3))に応じた値がそれぞれ対応する。ノードN_7の子ノードN_8,N_{11}には、シェア情報SEに応じた値が2-out-of-2分散方式で秘密分散された各シェア情報SH_4,SE-SH_4に応じた値がそれぞれ対応する。ノードN_8の子ノードN_9,N_{10}には、シェア情報SH_4に応じた値が1-out-of-2分散方式で秘密分散された各シェア情報SH_4,SH_4に応じた値がそれぞれ対応する。すなわち、葉ノードN_3にはシェア情報share(1)=(1,f(1))に応じた値が対応し、葉ノードN_4にはシェア情報share(2)=(2,f(2))に応じた値が対応し、葉ノードN_5にはシェア情報share(3)=(3,f(3))に応じた値が対応し、葉ノードN_6にはシェア情報share(4)=SEに応じた値が対応し、葉ノードN_9にはシェア情報share(5)=SH_4に応じた値が対応し、葉ノードN_{10}にはシェア情報share(6)=SH_4に応じた値が対応し、葉ノードN_{11}にはシェア情報share(7)=SE-SH_4に応じた値が対応する。また、葉ノードであるノードN_3,N_4,N_5,N_6,N_9,N_{10},N_{11}には標準形論理式PRO(1)∧PRO(2)∨PRO(2)∧PRO(3)∨PRO(1)∧PRO(3)∨¬PRO(4)∨(¬PRO(5)∧PRO(6))∧PRO(7)を構成する各リテラルPRO(1),PRO(2),PRO(2),PRO(3),PRO(1),PRO(3),¬PRO(4),¬PRO(5),PRO(6),PRO(7)がそれぞれ対応し、各リテラルPRO(1),PRO(2),PRO(2),PRO(3),PRO(1),PRO(3),¬PRO(4),¬PRO(5),PRO(6),PRO(7)の真理値は第１情報と第２情報との組み合わせによって定まる。ここで、真理値が真となったリテラルに対応する葉ノードに対応するシェア情報に応じた値は得られるが、真理値が偽となったリテラルに対応する葉ノードに対応するシェア情報に応じた値は得られない。この場合、第１情報と第２情報との組み合わせが標準形論理式PRO(1),∧PRO(2),∨PRO(2),∧PRO(3),∨PRO(1),∧PRO(3),∨¬PRO(4),∨(¬PRO(5),∧PRO(6),)∧PRO(7)の真理値を真にする場合にのみ秘密情報SEに応じた値が復元される。

[0068] ＜アクセス構造＞

上述のように秘密情報を階層的に秘密分散して得られる木構造データによって所定の論理式を表現した場合、第１情報と第２情報との組み合わせに対して得られる葉ノードでのシェア情報に応じた値から秘密情報に応じた値を復元できるか否かによって、第１情報と第２情報との組み合わせによって定まる論理式の真理値が「真」となるか「偽」となるかを判定できる。以下、第１情報と第２情報との組み合わせによって定まる論理式の真理値が「真」となる場合に第１情報と第２情報との組み合わせを受け入れ、「偽」となる場合に第１情報と第２情報との組み合わせを拒絶する仕組みをアクセス構造と呼ぶ。

[0069] 上述のように所定の論理式を表現した木構造データの葉ノードの総数をΨとし、各葉ノードに対応する識別子をλ=1,...,Ψとする。各葉ノードに対応するn(λ)次元ベクトルv(λ)→の集合$\{v(\lambda)^{\rightarrow}\}_{\lambda=1,\ldots,\Psi}$を第１情報とし、n(λ)次元ベクトルw(λ)→の集合$\{w(\lambda)^{\rightarrow}\}_{\lambda=1,\ldots,\Psi}$を第２情報とする。また、上述した木構造データをラベル付き行列LMT(MT,LAB)として実装する。

[0070] ラベル付き行列LMT(MT,LAB)は、Ψ行COL列（COL≧1）の行列

[数16]

$$MT=\begin{pmatrix} mt_{1,1} & \cdots & mt_{1,COL} \\ \vdots & \ddots & \vdots \\ mt_{\Psi,1} & \cdots & mt_{\Psi,COL} \end{pmatrix} \qquad \cdots(34)$$

と、行列MTの各行λ=1,...,Ψに対応付けられたラベルLAB(λ)とを含む。

[0071] 行列MTの各要素$mt_{\lambda,col}$（col=1,...,COL）は次の２つの要件を満たす。第１に、上述のように所定の論理式を表現した木構造データのルートノードに秘密情報SE∈F_qに応じた値が対応する場合、予め定められた有限体F_qの元を要素とするCOL次元ベクトル

$$GV^{\rightarrow}=(gv_1,\ldots,gv_{COL})\in F_q^{COL} \qquad \cdots(35)$$

と、秘密情報SEに応じた有限体F_qの元を要素とするCOL次元ベクトル

$$CV^{\rightarrow}=(cv_1,\ldots,cv_{COL})\in F_q^{COL} \qquad \cdots(36)$$

とに対して

$$SE=GV^{\rightarrow}\cdot(CV^{\rightarrow})^{T} \quad \cdots(37)$$

が成立する。COL次元ベクトル$GV^{\rightarrow}$の具体例は、

$$GV^{\rightarrow}=(1_F,\ldots,1_F)\in F_q^{COL} \quad \cdots(38)$$

であるが、$GV^{\rightarrow}=(1_F,0_F,\ldots,0_F)\in F_q^{COL}$などのその他のCOL次元ベクトルであってもよい。第２に、識別子λに対応する葉ノードにシェア情報$share(\lambda)\in F_q$に応じた値が対応する場合、

$$(share(1),\ldots,share(\Psi))^{T}=MT\cdot(CV^{\rightarrow})^{T} \quad \cdots(39)$$

が成立する。上述のように所定の論理式を表現した木構造データが定まれば、これら２つの要件を満たす行列MTを選択することは容易である。また、秘密情報SEやシェア情報share(λ)が変数であったとしても、これら２つの要件を満たす行列MTを選択することは容易である。すなわち、行列MTを定めた後で秘密情報SEやシェア情報share(λ)の値が定められてもよい。

[0072] また、行列MTの各行$\lambda=1,\ldots,\Psi$に対応付けられたラベルLAB(λ)は、識別子λに対応する葉ノードに対応するリテラル（PRO(λ)又は¬PRO(λ)）に対応する。ここで、命題変数PRO(λ)の真理値が「真」であることと第１情報$VSET1=\{\lambda,v(\lambda)^{\rightarrow}|\lambda=1,\ldots,\Psi\}$が含む$v(\lambda)^{\rightarrow}$と第２情報$VSET2=\{\lambda,w(\lambda)^{\rightarrow}|\lambda=1,\ldots,\Psi\}$が含む$w(\lambda)^{\rightarrow}$との内積$v(\lambda)^{\rightarrow}\cdot w(\lambda)^{\rightarrow}$が０となることとが等価であると扱い、命題変数PRO(λ)の真理値が「偽」であることと内積$v(\lambda)^{\rightarrow}\cdot w(\lambda)^{\rightarrow}$が０とならないこととが等価であると扱う。そして、PRO(λ)に対応するラベルLAB(λ)が$v(\lambda)^{\rightarrow}$を表し、¬PRO(λ)に対応するラベルLAB(λ)が$\neg v(\lambda)^{\rightarrow}$を表すものとする。なお、$\neg v(\lambda)^{\rightarrow}$は$v(\lambda)^{\rightarrow}$の否定を表す論理式であり、$\neg v(\lambda)^{\rightarrow}$から$v(\lambda)^{\rightarrow}$の特定が可能である。また、LAB(λ)が$v(\lambda)^{\rightarrow}$を表すことを「$LAB(\lambda)=v(\lambda)^{\rightarrow}$」と表記し、LAB(λ)が$\neg v(\lambda)^{\rightarrow}$を表すことを「$LAB(\lambda)=\neg v(\lambda)^{\rightarrow}$」と表記する。また、LAB(λ)（$\lambda=1,\ldots,\Psi$）の集合$\{LAB(\lambda)\}_{\lambda=1,\ldots,\Psi}$をLABと表記する。

[0073] さらに、Ψ次元ベクトル

$$TFV^{\rightarrow}=(tfv(1),\ldots,tfv(\Psi)) \quad \cdots(40)$$

を定義する。要素tfv(λ)は、内積v(λ)→・w(λ)→が０のときにtfv(λ)=１となり、０以外のときにtfv(λ)=0となる。

tfv(λ)=1　(PRO(λ)が真)　if　v(λ)→・w(λ)→=0　…(41)

tfv(λ)=0　(PRO(λ)が偽)　if　v(λ)→・w(λ)→≠0　…(42)

[0074] さらに、論理式

{(LAB(λ)=v(λ)→)∧(tfv(λ)=1)}∨{(LAB(λ)=¬v(λ)→)∧(tfv(λ)=0)}　…(43)

の真理値が「真」になるときLIT(λ)=1と表記し「偽」になるときLIT(λ)=0と表記する。すなわち、識別子λに対応する葉ノードに対応するリテラルの真理値が「真」になるときLIT(λ)=1と表記し「偽」になるときLIT(λ)=0と表記する。すると、行列MTが含む行ベクトルのうちLIT(λ)=1となる行ベクトル$mt_{\lambda}^{\rightarrow}=(mt_{\lambda,1},...,mt_{\lambda,COL})$のみからなる部分行列$MT_{TFV}$は以下のように表記できる。

$$MT_{TFV}=(MT)_{LIT(\lambda)=1} \quad \cdots(44)$$

[0075] 上述した秘密分散方式が線形秘密分散方式である場合、識別子λに対応するシェア情報share(λ)に応じた値から秘密情報SEに応じた値が復元できることと、識別子λに対応する行ベクトル$mt_{\lambda}^{\rightarrow}$で張られるベクトル空間にCOL次元ベクトルGV→が属することとは等価である。すなわち、識別子λに対応する行ベクトル$mt_{\lambda}^{\rightarrow}$で張られるベクトル空間にCOL次元ベクトルGV→が属するか否かを判定することで、識別子λに対応するシェア情報share(λ)に応じた値から秘密情報SEに応じた値が復元できるか否かが判定できる。なお、行ベクトル$mt_{\lambda}^{\rightarrow}$で張られるベクトル空間とは、行ベクトル$mt_{\lambda}^{\rightarrow}$の線形結合で表すことができるベクトル空間を意味する。

[0076] ここで、上述の部分行列MT_{TFV}の各行ベクトル$mt_{\lambda}^{\rightarrow}$で張られるベクトル空間span<$MT_{TFV}$>にCOL次元ベクトルGV→が属する場合に第１情報と第２情報との組み合わせが受け入れられ、そうでない場合に第１情報と第２情報との組み合わせが拒絶されることにする。これにより、上述のアクセス構造が具体化される。なお、上述したようにラベル付き行列LMT(MT,LAB)が第１情報に対応する

場合、アクセス構造が第１情報と第２情報との組み合わせを受け入れることを「アクセス構造が第２情報を受け入れる」といい、アクセス構造が第１情報と第２情報との組み合わせを受け入れないことを「アクセス構造が第２情報を拒絶する」という。

受け入れ　if　$GV^{\rightarrow}\in span\langle MT_{TFV}\rangle$

拒絶　　if　$\neg(GV^{\rightarrow}\in span\langle MT_{TFV}\rangle)$

また、$GV^{\rightarrow}\in span\langle MT_{TFV}\rangle$の場合、

$$SE=\Sigma_{\mu\in SET}const(\mu)\cdot share(\mu) \qquad \cdots(45)$$

$$\{const(\mu)\in F_q|\ \mu\in SET\},SET\subseteq\{1,...,\lambda|LIT(\lambda)=1\}$$

を満たす係数$const(\mu)$が存在し、このような係数$const(\mu)$は行列MTのサイズの多項式時間で求めることができる。

[0077] ＜アクセス構造を用いた関数暗号方式の基本構成＞

以下では、アクセス構造を用いた関数暗号方式によって鍵カプセル化メカニズムKEM (Key Encapsulation Mechanisms)を構成する場合の基本構成を例示する。この構成は$Setup(1^{sec}, (\Psi;n(1),...,n(\Psi)))$, $GenKey(PK,MSK,LMT(MT,LAB))$, $Enc(PK,M,\{\lambda,v(\lambda)^{\rightarrow}|\lambda=1,...,\Psi\})(v_1(\lambda)=1_F)$, $Dec(PK,SKS,C)$を含む。また、第２情報$VSET2=\{\lambda,w(\lambda)^{\rightarrow}|\lambda=1,...,\Psi\}$の1番目の要素$w_1(\lambda)$が$1_F$とされる。

[0078] [$Setup(1^{sec}, (\Psi;n(1),...,n(\Psi)))$：セットアップ]

ー入力：$1^{sec}, (\Psi;n(1),...,n(\Psi))$

ー出力：マスター鍵情報MSK, 公開パラメータPK

Setupでは各$\phi=0,...,\Psi$について以下の処理が実行される。

(Setup-1) 1^{sec}を入力としてセキュリティパラメータsecでの位数q、楕円曲線E、巡回群G_1, G_2, G_T、双線形写像$e_\phi(\phi=0,...,\Psi)$が生成される（$param=(q, E, G_1, G_2, G_T, e_\phi)$）。

(Setup-2) $\tau'\in F_q$が選択され、$X^*(\phi)=\tau'\cdot(X(\phi)^{-1})^T$を満たす行列$X(\phi)$, $X^*(\phi)$が選択される。

(Setup-3) 基底ベクトル$a_i(\phi)$ $(i=1,...,n(\phi)+\zeta(\phi))$が式(21)に従って

座標変換され、$n(\phi)+\zeta(\phi)$次元の基底ベクトル$b_i(\phi)$ $(i=1,...,n(\phi)+\zeta(\phi))$が生成される。基底ベクトル$b_i(\phi)$ $(i=1,...,n(\phi)+\zeta(\phi))$を要素とする$n(\phi)+\zeta(\phi)$行$n(\phi)+\zeta(\phi)$列の行列$B(\phi)$が生成される。

(Setup-4) 基底ベクトル$a_i^*(\phi)$ $(i=1,...,n(\phi)+\zeta(\phi))$が式(23)に従って座標変換され、$n(\phi)+\zeta(\phi)$次元の基底ベクトル$b_i^*(\phi)$ $(i=1,...,n(\phi)+\zeta(\phi))$が生成される。基底ベクトル$b_i^*(\phi)$ $(i=1,...,n(\phi)+\zeta(\phi))$を要素とする$n(\phi)+\zeta(\phi)$行$n(\phi)+\zeta(\phi)$列の行列$B^*(\phi)$が生成される。

(Setup-5) $B^*(\phi)\hat{}$の集合$\{B^*(\phi)\hat{}\}_{\phi=0,...,\Psi}$をマスター鍵情報$MSK=\{B^*(\phi)\hat{}\}_{\phi=0,...,\Psi}$とする。また、$B(\phi)\hat{}$の集合$\{B(\phi)\hat{}\}_{\phi=0,...,\Psi}$と$1^{sec}$とparamとを公開パラメータPKとする。ただし、$B^*(\phi)\hat{}$は行列$B^*(\phi)$又はその部分行列であり、$B(\phi)\hat{}$は行列$B(\phi)$又はその部分行列である。また、集合$\{B^*(\phi)\hat{}\}_{\phi=0,...,\Psi}$は、少なくとも、$b_1^*(0), b_1^*(\lambda)\cdots, b_{n(\lambda)}^*(\lambda)$ $(\lambda=1,...,\Psi)$を含む。また、集合$\{B(\phi)\hat{}\}_{\phi=0,...,\Psi}$は、少なくとも、$b_1(0), b_1(\lambda),\cdots, b_{n(\lambda)}(\lambda)$ $(\lambda=1,...,\Psi)$を含む。以下に一例を示す。

・$n(0)+\zeta(0)\geqq 5$, $\zeta(\lambda)=3\cdot n(\lambda)$

・$B(0)\hat{}=(b_1(0)\ b_3(0)\ b_5(0))^T$

・$B(\lambda)\hat{}=(b_1(\lambda)\cdots b_{n(\lambda)}(\lambda)\ b_{3\cdot n(\lambda)+1}(\lambda)\cdots\ b_{4\cdot n(\lambda)}(\lambda))^T$ $(\lambda=1,...,\Psi)$

・$B^*(0)\hat{}=(b_1^*(0)\ b_3^*(0)\ b_4^*(0))^T$

・$B^*(\lambda)\hat{}=(b_1^*(\lambda)\cdots\ b_{n(\lambda)}^*(\lambda)\ b_{2\cdot n(\lambda)+1}^*(\lambda)\cdots\ b_{3\cdot n(\lambda)}^*(\lambda))^T$ $(\lambda=1,...,\Psi)$

[0079] [GenKey(PK,MSK,LMT(MT,LAB)):鍵情報生成]

ー入力:公開パラメータPK, マスター鍵情報MSK, 第1情報$VSET1=\{\lambda, v(\lambda)\rightarrow|\lambda=1,...,\Psi\}$に対応するラベル付き行列LMT(MT,LAB)

ー出力:鍵情報SKS

(GenKey-1) 式(35)-(39)を満たす秘密情報SEに対して以下の処理が実行される。

$$D^*(0)=-SE\cdot b_1^*(0)+\Sigma_{\iota=2}^{I}coef_\iota(0)\cdot b_\iota^*(0) \qquad \cdots(46)$$

ただし、Iは2以上n(0)+ζ(0)以下の定数である。$coef_\iota(0)\in F_q$は定数又は乱数である

。「乱数」とは真性乱数や擬似乱数を意味する。以下にD*(0)の一例を示す。なお、式(47)の$coef_4(0)$は乱数である。

$$D^*(0)=-SE\cdot b_1^*(0)+b_3^*(0)+coef_4(0)\cdot b_4^*(0) \quad \cdots(47)$$

(GenKey-2) 式(35)-(39)を満たすshare(λ)(λ=1,...,Ψ)に対して以下の処理が実行される。

LAB(λ)=v(λ)→となるλに対して

$$D^*(\lambda)=(share(\lambda)+coef(\lambda)\cdot v_1(\lambda))\cdot b_1^*(\lambda)+\Sigma_{\iota=2}^{n(\lambda)}coef(\lambda)\cdot v_\iota(\lambda)\cdot b_\iota^*(\lambda)+\Sigma_{\iota=n(\lambda)+1}^{n(\lambda)+\zeta(\lambda)}coef_\iota(\lambda)\cdot b_\iota^*(\lambda) \quad \cdots(48)$$

が生成され、

LAB(λ)=¬v(λ)→となるλに対して

$$D^*(\lambda)=share(\lambda)\cdot\Sigma_{\iota=1}^{n(\lambda)}v_\iota(\lambda)\cdot b_\iota^*(\lambda)+\Sigma_{\iota=n(\lambda)+1}^{n(\lambda)+\zeta(\lambda)}coef_\iota(\lambda)\cdot b_\iota^*(\lambda) \quad \cdots(49)$$

が生成される。ただしcoef(λ),$coef_\iota(\lambda)\in F_q$は定数又は乱数である。以下に一例を示す。

LAB(λ)=v(λ)→となるλに対して

$$D^*(\lambda)=(share(\lambda)+coef(\lambda)\cdot v_1(\lambda))\cdot b_1^*(\lambda)+\Sigma_{\iota=2}^{n(\lambda)}coef(\lambda)\cdot v_\iota(\lambda)\cdot b_\iota^*(\lambda)+\Sigma_{\iota=2\cdot n(\lambda)+1}^{3\cdot n(\lambda)}coef_\iota(\lambda)\cdot b_\iota^*(\lambda) \quad \cdots(50)$$

が生成され、

LAB(λ)=¬v(λ)→となるλに対して

$$D^*(\lambda)=share(\lambda)\cdot\Sigma_{\iota=1}^{n(\lambda)}v_\iota(\lambda)\cdot b_\iota^*(\lambda)+\Sigma_{\iota=2\cdot n(\lambda)+1}^{3\cdot n(\lambda)}coef_\iota(\lambda)\cdot b_\iota^*(\lambda) \quad \cdots(51)$$

が生成される。なお、式(50)(51)のcoef(λ)及び$coef_\iota(\lambda)$は乱数である。

(GenKey-3) 鍵情報

$$SKS=(LMT(MT,LAB),D^*(0),D^*(1),...,D(\Psi)) \quad \cdots(52)$$

生成される。

[0080] [Enc(PK,M,VSET2)：暗号化]

－入力：公開パラメータPK，平文M，第２情報VSET2={λ,w(λ)→|λ=1,...,Ψ}($w_1(\lambda)=1_F$)

－出力：暗号文C

(Enc-1) 以下の処理によって共通鍵Kの暗号文C(φ)(φ=0,...,Ψ)が生成される。

$$C(0)=\upsilon\cdot b_1(0)+\Sigma_{\iota=2}^{I}\upsilon_\iota(0)\cdot b_\iota(0) \quad \cdots(53)$$

$$C(\lambda)=\upsilon\cdot\Sigma_{\iota=1}^{n(\lambda)}w_\iota(\lambda)\cdot b_\iota(\lambda)+\Sigma_{\iota=n(\lambda)+1}^{n(\lambda)+\zeta(\lambda)}\upsilon_\iota(\lambda)\cdot b_\iota(\lambda) \quad \cdots(54)$$

ただし、$\upsilon,\upsilon_\iota(\phi)\in F_q(\phi=0,...,\Psi)$は定数又は乱数であり、

$$(coef_2(0),...,coef_I(0))\cdot(\upsilon_2(0),...,\upsilon_I(0))=\upsilon' \quad \cdots(55)$$

$$coef_\iota(\lambda)\cdot\upsilon_\iota(\lambda)=0_F\ (\iota=n(\lambda)+1,...,n(\lambda)+\zeta(\lambda)) \quad \cdots(56)$$

を満たす。υ'の例は$\upsilon_2(0),...,\upsilon_I(0)$の何れか１個である。例えば、$\upsilon,\upsilon_3(0),\upsilon_5(0),\upsilon_{3\cdot n(\lambda)+1}(\lambda),...,\upsilon_{4\cdot n(\lambda)}(\lambda)$が乱数であり、$\zeta(\lambda)=3\cdot n(\lambda)$、I=5であり、

$$(\upsilon_2(0),...,\upsilon_I(0))=(0_F,\upsilon_3(0),0_F,\upsilon_5(0))$$

$$\upsilon'=\upsilon_3(0)$$

$$(\upsilon_{n(\lambda)+1}(\lambda),...,\upsilon_{3\cdot n(\lambda)}(\lambda))=(0_F,...,0_F)$$

である。

(Enc-2) 共通鍵

$$K=g_T^{\tau\cdot\tau'\cdot\upsilon'}\in G_T \quad \cdots(57)$$

が生成される。例えば、$\tau=\tau'=1_F$の場合、

$$K=g_T^{\upsilon'}\in G_T \quad \cdots(58)$$

である。

(Enc-3) 共通鍵Kを用いて平文Mの暗号文

$$C(\Psi+1)=Enc_K(M) \quad \cdots(59)$$

が生成される。なお、共通鍵暗号方式Encは、例えば共通鍵Kを用いて暗号化

可能に構成されたカメリア（Camellia）（登録商標）やAESや共通鍵と平文との排他的論理和などでよいが、その他の簡単な例として以下のように$Enc_K(M)$を生成してもよい。ただし、式(60)の例では$M \in G_T$とされる。

$$C(\Psi+1)=g_T^{v'} \cdot M \qquad \cdots(60)$$

(Enc-4) 暗号文

$$C=(VSET2, C(0), \{C(\lambda)\}_{(\lambda, w(\lambda)\rightarrow)\in VSET2}, C(\Psi+1)) \qquad \cdots(61)$$

が生成される。ただし、下付き添え字の「$w(\lambda)\rightarrow$」は「$w(\lambda)^{\rightarrow}$」を表す。

[0081] [Dec(PK,SKS,C)：復号]

－入力：公開パラメータPK，鍵情報SKS，暗号文C

－出力：平文M'

(Dec-1) $\lambda=1,\ldots,\Psi$について、鍵情報SKSが含むラベル付き行列LMT(MT,LAB)の各ラベルLAB(λ)であるn(λ)次元ベクトル$v(\lambda)^{\rightarrow}$と暗号文CのVSET2が含むn(λ)次元ベクトル$w(\lambda)^{\rightarrow}$との内積$v(\lambda)^{\rightarrow} \cdot w(\lambda)^{\rightarrow}$が0となるか否かが判定され、これによって$GV^{\rightarrow} \in span\langle MT_{TFV}\rangle$であるか否かが判定される。$GV^{\rightarrow} \in span\langle MT_{TFV}\rangle$でなければ暗号文Cが拒絶され、$GV^{\rightarrow} \in span\langle MT_{TFV}\rangle$であれば暗号文Cが受け入れられる。

(Dec-2) 暗号文Cが受け入れられると、$SET \subseteq \{1,\ldots,\lambda \mid LIT(\lambda)=1\}$と式(45)を満たす係数const($\mu$)($\mu \in SET$)とが計算される。

(Dec-3) 共通鍵

[数17]

$$K = e_0(C(0), D^*(0)) \cdot \prod_{\mu \in SET \wedge LAB(\mu)=v(\mu)^{\rightarrow}} e_\mu(C(\mu), D^*(\mu))^{const(\mu)} \cdot \prod_{\mu \in SET \wedge LAB(\mu)=\neg v(\mu)^{\rightarrow}} e_\mu(C(\mu), D^*(\mu))^{const(\mu)/(v(\mu)^{\rightarrow} \cdot w(\mu)^{\rightarrow})} \qquad \cdots(62)$$

が生成される。ここで、式(6)(25)(55)から、

[数18]

$$
\begin{aligned}
&e_0(C(0), D^*(0)) \\
&= e_0(\upsilon \cdot b_1(0) + \sum_{\iota=2}^{I} \upsilon_\iota(0) \cdot b_\iota(0), -SE \cdot b_1^*(0) + \sum_{\iota=2}^{I} coef_\iota(0) \cdot b_\iota^*(0)) \\
&= e_0(\upsilon \cdot b_1(0), -SE \cdot b_1^*(0)) \cdot \prod_{\iota=2}^{I} e_0(\upsilon_\iota(0) \cdot b_\iota(0), coef_\iota(0) \cdot b_\iota^*(0))) \\
&= e_0(b_1(0), b_1^*(0))^{-SE \cdot \upsilon} \cdot \prod_{\iota=2}^{I} e_0(b_\iota(0), b_\iota^*(0))^{\upsilon_\iota(0) \cdot coef_\iota(0)}) \\
&= g_T^{\tau \cdot \tau' \cdot \delta(1,1) \cdot (-SE \cdot \upsilon)} \cdot \prod_{\iota=2}^{I} g_T^{\tau \cdot \tau' \cdot \delta(\iota,\iota) \cdot \upsilon_\iota(0) \cdot coef_\iota(0)} \\
&= g_T^{\tau \cdot \tau' \cdot (-SE \cdot \upsilon + \upsilon')}
\end{aligned}
\qquad \cdots (63)
$$

を満たす。また、式(6)(25)(41)(48)(54)(56)及び$w_1(\lambda)=1_F$から

[数19]

$$
\begin{aligned}
&\prod_{\mu \in SET \wedge LAB(\mu)=v(\mu)^{\rightarrow}} e_\mu(C(\mu), D^*(\mu))^{const(\mu)} \\
&= \prod_{\mu \in SET \wedge LAB(\mu)=v(\mu)^{\rightarrow}} e_\mu(\upsilon \cdot \sum_{\iota=1}^{n(\mu)} w_\iota(\mu) \cdot b_\iota(\mu) + \sum_{\iota=n(\mu)+1}^{n(\mu)+\zeta(\mu)} \upsilon_\iota(\mu) \cdot b_\iota(\mu), \\
&share(\mu) \cdot b_1^*(\mu) + \sum_{\iota=1}^{n(\mu)} coef(\mu) \cdot v_\iota(\mu) \cdot b_\iota^*(\mu) \\
&+ \sum_{\iota=n(\mu)+1}^{n(\mu)+\zeta(\mu)} coef_\iota(\mu) \cdot b_\iota^*(\mu))^{const(\mu)} \\
&= \prod_{\mu \in SET \wedge LAB(\mu)=v(\mu)^{\rightarrow}} \left\{ \begin{array}{l} e_\mu(\upsilon \cdot \sum_{\iota=1}^{n(\mu)} w_\iota(\mu) \cdot b_\iota(\mu), share(\mu) \cdot b_1^*(\mu)) \\ \cdot e_\mu(\upsilon \cdot \sum_{\iota=1}^{n(\mu)} w_\iota(\mu) \cdot b_\iota(\mu), \sum_{\iota=1}^{n(\mu)} cocf(\mu) \cdot v_\iota(\mu) \cdot b_\iota^*(\mu)) \end{array} \right\}^{const(\mu)} \\
&= \prod_{\mu \in SET \wedge LAB(\mu)=v(\mu)^{\rightarrow}} \left(g_T^{\tau \cdot \tau' \cdot \upsilon \cdot share(\mu)} \cdot \prod_{\iota=1}^{n(\mu)} g_T^{\tau \cdot \tau' \cdot \upsilon \cdot coef(\mu) \cdot w_\iota(\mu) \cdot v_\iota(\mu)} \right)^{const(\mu)} \\
&= \prod_{\mu \in SET \wedge LAB(\mu)=v(\mu)^{\rightarrow}} g_T^{\tau \cdot \tau' \cdot \upsilon \cdot const(\mu) \cdot share(\mu)}
\end{aligned}
\qquad \cdots (64)
$$

を満たす。また、式(6)(25)(42)(49)(54)(56)から

[数20]

$$\prod_{\mu\in SET\wedge LAB(\mu)=\neg v(\mu)^{\rightarrow}} e_{\mu}(C(\mu),D^{*}(\mu))^{const(\mu)/(v(\mu)^{\rightarrow}\cdot w(\mu)^{\rightarrow})}$$

$$= \prod_{\mu\in SET\wedge LAB(\mu)=\neg v(\mu)^{\rightarrow}} e_{\mu}(\upsilon\cdot\sum_{\iota=1}^{n(\mu)} w_{\iota}(\mu)\cdot b_{\iota}(\mu)+\sum_{\iota=n(\mu)+1}^{n(\mu)+\zeta(\mu)}\upsilon_{\iota}(\mu)\cdot b_{\iota}(\mu),$$

$$share(\mu)\cdot\sum_{\iota=1}^{n(\mu)} v_{\iota}(\mu)\cdot b_{\iota}^{*}(\mu)+\sum_{\iota=n(\mu)+1}^{n(\mu)+\zeta(\mu)} coef_{\iota}(\mu)\cdot b_{\iota}^{*}(\mu))^{const(\mu)/(v(\mu)^{\rightarrow}\cdot w(\mu)^{\rightarrow})}$$

$$= \prod_{\mu\in SET\wedge LAB(\mu)=\neg v(\mu)^{\rightarrow}} \left\{\prod_{\iota=1}^{n(\mu)} e_{\mu}\left(b_{\iota}(\mu),b_{\iota}^{*}(\mu)\right)^{\upsilon\cdot share(\mu)\cdot w_{\iota}(\mu)\cdot v_{\iota}(\mu)}\right\}^{const(\mu)/(v(\mu)^{\rightarrow}\cdot w(\mu)^{\rightarrow})}$$

$$= \prod_{\mu\in SET\wedge LAB(\mu)=\neg v(\mu)^{\rightarrow}} \left\{\prod_{\iota=1}^{n(\mu)} g_{T}^{\tau\cdot\tau'\cdot\upsilon\cdot share(\mu)\cdot w_{\iota}(\mu)\cdot v_{\iota}(\mu)}\right\}^{const(\mu)/(v(\mu)^{\rightarrow}\cdot w(\mu)^{\rightarrow})}$$

$$= \prod_{\mu\in SET\wedge LAB(\mu)=\neg v(\mu)^{\rightarrow}} \left\{g_{T}^{\tau\cdot\tau'\cdot\upsilon\cdot share(\mu)\cdot v(\mu)^{\rightarrow}\cdot w(\mu)^{\rightarrow}}\right\}^{const(\mu)/(v(\mu)^{\rightarrow}\cdot w(\mu)^{\rightarrow})}$$

$$= \prod_{\mu\in SET\wedge LAB(\mu)=\neg v(\mu)^{\rightarrow}} g_{T}^{\tau\cdot\tau'\cdot\upsilon\cdot const(\mu)\cdot share(\mu)} \quad \cdots(65)$$

を満たす。よって、式(45)(63)-(65)から

[数21]

$$K = g_{T}^{\tau\cdot\tau'\cdot(-SE\cdot\upsilon+\upsilon')}\cdot \prod_{\mu\in SET\wedge LAB(\mu)=v(\mu)^{\rightarrow}} g_{T}^{\tau\cdot\tau'\cdot\upsilon\cdot const(\mu)\cdot share(\mu)}$$

$$\cdot \prod_{\mu\in SET\wedge LAB(\mu)=\neg v(\mu)^{\rightarrow}} g_{T}^{\tau\cdot\tau'\cdot\upsilon\cdot const(\mu)\cdot share(\mu)}$$

$$= g_{T}^{\tau\cdot\tau'\cdot(-SE\cdot\upsilon+\upsilon')}\cdot g_{T}^{\tau\cdot\tau'\cdot\upsilon\cdot SE} = g_{T}^{\tau\cdot\tau'\cdot\upsilon'} \quad \cdots(66)$$

を満たす。例えば、$\tau=\tau'=1_{F}$の場合、

$$K=g_{T}^{\upsilon'}\in G_{T} \quad \cdots(67)$$

を満たす。

(Dec-4) 共通鍵Kを用いて平文

$$M'=Dec_{K}(C(\Psi+1))=Dec_{K}(C(\Psi+1)) \quad \cdots(68)$$

が生成される。例えば、式(60)に例示した共通鍵暗号方式の場合、

$$M'=C(\Psi+1)/K \quad \cdots(69)$$

によって平文M'が生成される。

[0082] なお、g_{T}をG_{T}の生成元とする代わりにg_{T}^{τ}や$g_{T}^{\tau'}$や$g_{T}^{\tau\cdot\tau'}$をG_{T}の生成元と扱っ

てもよい。また、鍵情報SKSのλと暗号文のλとを対応関係を特定する写像を用いてC(λ)とD*(λ)との組み合わせを特定し、［Dec(PK,SKS,C)：復号］の処理が実行されてもよい。また、第２情報VSET2={λ,w(λ)→|λ=1,...,Ψ}の1番目の要素$w_1(\lambda)$が1_Fとされるだけではなく、第１情報VSET1={λ,v(λ)→|λ=1,...,Ψ}のn(λ)番目の要素$v_{n(\lambda)}(\lambda)$が1_Fとされてもよい。また、要素$w_1(\lambda)$が1_Fでない場合にはw(λ)→の代わりにw(λ)→/$w_1(\lambda)$を用いてもよく、要素$v_{n(\lambda)}(\lambda)$が1_Fでない場合にはv(λ)→の代わりにv(λ)→/$v_{n(\lambda)}(\lambda)$を用いてもよい。また、第１情報VSET1={λ,v(λ)→|λ=1,...,Ψ}の代わりに第２情報VSET2={λ,w(λ)→|λ=1,...,Ψ}が用いられ、第２情報VSET2={λ,w(λ)→|λ=1,...,Ψ}の代わりに第１情報VSET1={λ,v(λ)→|λ=1,...,Ψ}が用いられてもよい。この場合には第１情報VSET1={λ,v(λ)→|λ=1,...,Ψ}の1番目の要素$v_1(\lambda)$が1_Fとされる。

[0083] 次に、関数暗号の一形態である述語暗号の一例として内積を用いた述語暗号について説明する。なお、数式の番号は本節で改めて付け直している。また、説明の都合、上述の説明で用いた文言や記号と同じ文言や記号であっても意味が異なる場合があるので注意されたい。述語暗号は1-out-of-1分散方式を用いた関数暗号に相当する。

[0084] 〔定義〕

行列：「行列」とは演算が定義された集合の元を矩形に並べたものを表す。環の元を要素とするものだけではなく、群の元を要素とするものも「行列」と表現する。

$(\cdot)^T$：$(\cdot)^T$は・の転置行列を表す。

$(\cdot)^{-1}$：$(\cdot)^{-1}$は・の逆行列を表す。

∧：∧は論理積を表す。

∨：∨は論理和を表す。

Ｚ：Ｚは整数集合を表す。

ｋ：ｋはセキュリティパラメータ（$k\in Z, k>0$）を表す。

$\{0,1\}^*$：$\{0,1\}^*$は任意ビット長のバイナリ系列を表す。その一例は、整数0

及び1からなる系列である。しかし、{0,1}*は整数0及び1からなる系列に限定されない。{0,1}*は位数2の有限体又はその拡大体と同義である。

{0,1}$^{\zeta}$：{0,1}$^{\zeta}$はビット長ζ（$\zeta\in Z$, $\zeta>0$）のバイナリ系列を表す。その一例は、整数0及び1からなる系列である。しかし、{0,1}$^{\zeta}$は整数0及び1からなる系列に限定されない。{0,1}$^{\zeta}$は位数2の有限体（$\zeta=1$の場合）又はそれをζ次拡大した拡大体（$\zeta>1$の場合）と同義である。

(+):(+)はバイナリ系列間の排他的論理和演算子を表す。例えば、10110011(+)11100001=01010010を満たす。

[0085] F_q：F_qは位数qの有限体を表す。位数qは１以上の整数であり、例えば、素数や素数のべき乗値を位数qとする。すなわち、有限体F_qの例は素体やそれを基礎体とした拡大体である。なお、有限体F_qが素体である場合の演算は、例えば、位数qを法とする剰余演算によって容易に構成できる。また、有限体F_qが拡大体である場合の演算は、例えば、既約多項式を法とする剰余演算によって容易に構成できる。有限体F_qの具体的な構成方法は、例えば、参考文献１「ISO/IEC 18033-2: Information technology - Security techniques - Encryption algorithms - Part 2: Asymmetric ciphers」に開示されている。

[0086] 0_F：0_Fは有限体F_qの加法単位元を表す。

1_F：1_Fは有限体F_qの乗法単位元を表す。

$\delta(i,j)$：$\delta(i,j)$はクロネッカーのデルタ関数を表す。i=jの場合に$\delta(i,j)=1_F$を満たし、i≠jの場合に$\delta(i,j)=0_F$を満たす。

[0087] E：Eは有限体F_q上で定義された楕円曲線を表す。Eはアフィン（affine）座標版のWeierstrass方程式

$$y^2+a_1\cdot x\cdot y+a_3\cdot y=x^3+a_2\cdot x^2+a_4\cdot x+a_6 \qquad \cdots(1)$$

（ただし、$a_1, a_2, a_3, a_4, a_6\in F_q$）を満たすx,y$\in F_q$からなる点(x,y)の集合に無限遠点と呼ばれる特別な点Ｏを付加したもので定義される。楕円曲線E上の任意の２点に対して楕円加算と呼ばれる二項演算＋及び楕円曲線E上の任意の１点に対して楕円逆元と呼ばれる単項演算－がそれぞれ定義できる。また、楕円曲線E上の有理点からなる有限集合が楕円加算に関して群をなすこと、楕円加

算を用いて楕円スカラー倍算と呼ばれる演算が定義できること、及びコンピュータ上での楕円加算などの楕円演算の具体的な演算方法はよく知られている（例えば、参考文献１、参考文献２「RFC 5091: Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems」、参考文献３「イアン・Ｆ・ブラケ、ガディエル・セロッシ、ナイジェル・Ｐ・スマート＝著、「楕円曲線暗号」、出版＝ピアソン・エデュケーション、ISBN4-89471-431-0」等参照）。

また、楕円曲線E上の有理点からなる有限集合は位数p(p≧1)の部分群を持つ。例えば、楕円曲線E上の有理点からなる有限集合の要素数を＃Eとし、pを＃Eを割り切る大きい素数とした場合、楕円曲線Eのp等分点からなる有限集合E[p]は、楕円曲線E上の有理点からなる有限集合の部分群を構成する。なお、楕円曲線Eのp等分点とは、楕円曲線E上の点Aのうち、楕円曲線E上での楕円スカラー倍算値p・Aがp・A＝Ｏを満たす点を意味する。

[0088] G_1, G_2, G_T：G_1, G_2,G_Tは位数qの巡回群を表す。巡回群G_1, G_2の具体例は、楕円曲線Eのp等分点からなる有限集合E[p]やその部分群である。$G_1=G_2$であってもよいし$G_1\neq G_2$であってもよい。また、巡回群G_Tの具体例は、有限体F_qを基礎体とする拡大体を構成する有限集合である。その一例は、有限体F_qの代数閉包における１のｐ乗根からなる有限集合である。

[0089] なお、本形態では、巡回群G_1, G_2上で定義された演算を加法的に表現し、巡回群G_T上で定義された演算を乗法的に表現する。すなわち、$\chi\in F_q$及び$\Omega\in G_1$に対する$\chi\cdot\Omega\in G_1$は、$\Omega\in G_1$に対して巡回群G_1で定義された演算をχ回施すことを意味し、Ω_1, $\Omega_2\in G_1$に対する$\Omega_1+\Omega_2\in G_1$は、$\Omega_1\in G_1$と$\Omega_2\in G_1$とを被演算子として巡回群G_1で定義された演算を行うことを意味する。同様に、$\chi\in F_q$及び$\Omega\in G_2$に対する$\chi\cdot\Omega\in G_2$は、$\Omega\in G_2$に対して巡回群G_2で定義された演算をχ回施すことを意味し、Ω_1, $\Omega_2\in G_2$に対する$\Omega_1+\Omega_2\in G_2$は、$\Omega_1\in G_2$と$\Omega_2\in G_2$とを被演算子として巡回群G_2で定義された演算を行うことを意味する。一方、$\chi\in F_q$及び$\Omega\in G_T$に対する$\Omega^{\chi}\in G_T$は、$\Omega\in G_T$に対して巡回群G_Tで定義された演算をχ回施すことを意味し、$\Omega_1,\Omega_2\in G_T$に対する$\Omega_1\cdot\Omega_2\in G_T$は、$\Omega_1\in G_T$と

$\Omega_2 \in G_T$とを被演算子として巡回群G_Tで定義された演算を行うことを意味する。

[0090] G_1^{n+1}：G_1^{n+1}はn+1(n≧1)個の巡回群G_1の直積を表す。

G_2^{n+1}：G_2^{n+1}はn+1個の巡回群G_2の直積を表す。

g_1, g_2, g_T：g_1, g_2, g_Tは巡回群G_1, G_2, G_Tの生成元を表す。

V：Vはn+1個の巡回群G_1の直積からなるn+1次元のベクトル空間を表す。

V*：V*はn+1個の巡回群G_2の直積からなるn+1次元のベクトル空間を表す。

[0091] e：eは直積G_1^{n+1}と直積G_2^{n+1}との直積$G_1^{n+1} \times G_2^{n+1}$を巡回群$G_T$に写す非退化な双線形写像（bilinear map）を計算するための関数（「双線形関数」と呼ぶ）を表す。双線形関数eは、巡回群G_1のn+1個の元γ_L(L=1,...,n+1)(n≧1)と巡回群G_2のn+1個の元γ_L*(L=1,...,n+1)とを入力とし、巡回群G_Tの１個の元を出力する。

$$e : G_1^{n+1} \times G_2^{n+1} \rightarrow G_T \qquad \cdots(2)$$

[0092] 双線形関数eは以下の性質を満たす。

［双線形性］すべての$\Gamma_1 \in G_1^{n+1}$, $\Gamma_2 \in G_2^{n+1}$及びν, $\kappa \in F_q$について以下の関係を満たす。

$$e(\nu \cdot \Gamma_1, \kappa \cdot \Gamma_2) = e(\Gamma_1, \Gamma_2)^{\nu \cdot \kappa} \qquad \cdots(3)$$

［非退化性］すべての

$$\Gamma_1 \in G_1^{n+1}, \ \Gamma_2 \in G_2^{n+1} \qquad \cdots(4)$$

を巡回群G_Tの単位元に写す関数ではない。

［計算可能性］あらゆる$\Gamma_1 \in G_1^{n+1}$, $\Gamma_2 \in G_2^{n+1}$についてe(Γ_1, Γ_2)を効率的に計算するアルゴリズムが存在する。

[0093] 本形態では、巡回群G_1と巡回群G_2との直積$G_1 \times G_2$を巡回群G_Tに写す非退化な双線形写像を計算するための関数

$$Pair : G_1 \times G_2 \rightarrow G_T \qquad \cdots(5)$$

を用いて双線形関数eを構成する。本形態の双線形関数eは、巡回群G_1のn+1個の元γ_L(L=1,...,n+1)からなるn+1次元ベクトル(γ_1,...,γ_{n+1})と、巡回群G_2のn+1個の元γ_L*(L=1,...,n+1)からなるn+1次元ベクトル(γ_1*,...,γ_{n+1}*)との入力に対し、巡回群G_Tの１個の元

$$e=\Pi_{L=1}^{n+1} \mathrm{Pair}(\gamma_L, \gamma_L^*) \quad \cdots(6)$$

を出力する関数である。

なお、双線形関数Pairは、巡回群G_1の１個の元と巡回群G_2の１個の元との組を入力とし、巡回群G_Tの１個の元を出力する関数であり、以下の性質を満たす。

［双線形性］すべての$\Omega_1 \in G_1$, $\Omega_2 \in G_2$及びν, $\kappa \in F_q$について以下の関係を満たす。

$$\mathrm{Pair}(\nu \cdot \Omega_1, \kappa \cdot \Omega_2)=\mathrm{Pair}(\Omega_1, \Omega_2)^{\nu \cdot \kappa} \quad \cdots(7)$$

［非退化性］すべての

$$\Omega_1 \in G_1, \ \Omega_2 \in G_2 \quad \cdots(8)$$

を巡回群G_Tの単位元に写す関数ではない。

［計算可能性］あらゆる$\Omega_1 \in G_1$, $\Omega_2 \in G_2$についてPair(Ω_1, Ω_2)を効率的に計算するアルゴリズムが存在する。

[0094] なお、双線形関数Pairの具体例は、Weilペアリングや Tateペアリングなどのペアリング演算を行うための関数である（例えば、参考文献４「Alfred. J. Menezes, ELLIPTIC CURVE PUBLIC KEY CRYPTOSYSTEMS, KLUWER ACADEMIC PUBLISHERS, ISBN0-7923-9368-6, pp.61-81」等参照）。また、楕円曲線Eの種類に応じ、Tateペアリングなどのペアリング演算を行うための関数と所定の関数phiを組み合わせた変更ペアリング関数e(Ω_1, phi(Ω_2))（$\Omega_1 \in G_1$, $\Omega_2 \in G_2$）を双線形関数Pairとして用いてもよい（例えば、参考文献２等参照）。また、ペアリング演算をコンピュータ上で行うためのアルゴリズムとしては、周知のMiller のアルゴリズム（参考文献５「V. S. Miller, “Short Programs for functions on Curves,” 1986, インターネット＜http://crypto.stanford.edu/miller/miller.pdf＞」などが存在する。また、ペアリング演算を効率的に行うための楕円曲線や巡回群の構成方法はよく知られている（例えば、参考文献２、参考文献６「A. Miyaji, M. Nakabayashi, S.Takano, ”New explicit conditions of elliptic curve Traces for FR-Reduction,” IEICE Trans. Fundamentals, vol. E84-A, no.05, pp. 1234-1243, May 2001」、

参考文献７「P.S.L.M. Barreto, B. Lynn, M. Scott, "Constructing elliptic curves with prescribed embedding degrees," Proc. SCN '2002, LNCS 2576, pp.257-267, Springer-Verlag. 2003」、参考文献８「R. Dupont, A. Enge, F. Morain, "Building curves with arbitrary small MOV degree over finite prime fields," http://eprint.iacr.org/2002/094/」等参照）。

[0095] $a_i(i=1,...,n+1)$：巡回群G_1のn+1個の元を要素とするn+1次元の基底ベクトルを表す。基底ベクトルa_iの一例は、$\kappa_1 \cdot g_1 \in G_1$をi次元目の要素とし、残りのn個の要素を巡回群$G_1$の単位元（加法的に「0」と表現）とするn+1次元の基底ベクトルである。この場合、n+1次元の基底ベクトル$a_i(i=1,...,n+1)$の各要素をそれぞれ列挙して表現すると、以下のようになる。

$$a_1=(\kappa_1 \cdot g_1,0,0,...,0)$$
$$a_2=(0,\kappa_1 \cdot g_1,0,...,0) \quad \cdots(9)$$
$$...$$
$$a_{n+1}=(0,0,0,...,\kappa_1 \cdot g_1)$$

ここで、κ_1は加法単位元0_F以外の有限体F_qの元からなる定数であり、$\kappa_1 \in F_q$の具体例は$\kappa_1=1_F$である。基底ベクトルa_iは直交基底であり、巡回群G_1のn+1個の元を要素とするすべてのn+1次元ベクトルは、n+1次元の基底ベクトル$a_i(i=1,...,n+1)$の線形和によって表される。すなわち、n+1次元の基底ベクトルa_iは前述のベクトル空間Vを張る。

[0096] $a_i^*(i=1,...,n+1)$：a_i^*は巡回群G_2のn+1個の元を要素とするn+1次元の基底ベクトルを表す。基底ベクトルa_i^*の一例は、$\kappa_2 \cdot g_2 \in G_2$をi次元目の要素とし、残りのn個の要素を巡回群$G_2$の単位元（加法的に「0」と表現）とするn+1次元の基底ベクトルである。この場合、基底ベクトル$a_i^*(i=1,...,n+1)$の各要素をそれぞれ列挙して表現すると、以下のようになる。

$$a_1^*=(\kappa_2 \cdot g_2,0,0,...,0)$$
$$a_2^*=(0,\kappa_2 \cdot g_2,0,...,0) \quad \cdots(10)$$
$$...$$
$$a_{n+1}^*=(0,0,0,...,\kappa_2 \cdot g_2)$$

ここで、κ_2は加法単位元0_F以外の有限体F_qの元からなる定数であり、$\kappa_2 \in F_q$の具体例は$\kappa_2=1_F$である。基底ベクトルa_i^*は直交基底であり、巡回群G_2のn+1個の元を要素とするすべてのn+1次元ベクトルは、n+1次元の基底ベクトルa_i^*(i=1,...,n+1)の線形和によって表される。すなわち、n+1次元の基底ベクトルa_i^*は前述のベクトル空間V^*を張る。

[0097] なお、基底ベクトルa_iと基底ベクトルa_i^*とは、0_Fを除く有限体F_qの元$\tau=\kappa_1 \cdot \kappa_2$について

$$e(a_i, a_j^*)=g_T^{\tau \cdot \delta(i,j)} \quad \cdots(11)$$

を満たす。すなわち、i=jの場合には、式(6)(7)の関係から、

$$e(a_i, a_j^*)= Pair(\kappa_1 \cdot g_1, \kappa_2 \cdot g_2) \cdot Pair(0, 0) \cdot \ldots \cdot Pair(0, 0)$$
$$= Pair(g_1, g_2)^{\kappa 1 \cdot \kappa 2} \cdot Pair(g_1, g_2)^{0 \cdot 0} \cdot \ldots \cdot Pair(g_1, g_2)^{0 \cdot 0}$$
$$= Pair(g_1, g_2)^{\kappa 1 \cdot \kappa 2}=g_T^{\tau}$$

を満たす。一方、i≠jの場合には、$e(a_i, a_j^*)$は、$Pair(\kappa_1 \cdot g_1, \kappa_2 \cdot g_2)$を含まず、$Pair(\kappa_1 \cdot g_1, 0)$と $Pair(0, \kappa_2 \cdot g_2)$と$Pair(0,0)$との積になる。さらに、式(7)の関係から$Pair(g_1, 0)=Pair(0, g_2)=Pair(g_1, g_2)^0$を満たす。そのため、i≠jの場合には、

$$e(a_i, a_j^*)=e(g_1, g_2)^0=g_T^0$$

を満たす。

特に、$\tau=\kappa_1 \cdot \kappa_2=1_F$である場合（例えば、$\kappa_1=\kappa_2=1_F$の場合）、

$$e(a_i, a_j^*)=g_T^{\delta(i,j)} \quad \cdots(12)$$

を満たす。ここで、$g_T^0=1$は巡回群G_Tの単位元であり、$g_T^1=g_T$は巡回群G_Tの生成元である。この場合、基底ベクトルa_iと基底ベクトルa_i^*とは双対正規直交基底であり、ベクトル空間Vとベクトル空間V^*とは、双線形写像を構成可能な双対ベクトル空間〔双対ペアリングベクトル空間（DPVS:Dual Paring Vector space)〕である。

[0098] A：Aは基底ベクトルa_i(i=1,...,n+1)を要素とするn+1行n+1列の行列を表す。例えば、基底ベクトルa_i(i=1,...,n+1)が式(9)によって表現される場合、行列Aは、

[数22]

$$A=\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{n+1} \end{pmatrix}=\begin{pmatrix} \kappa_1\cdot g_1 & 0 & \cdots & 0 \\ 0 & \kappa_1\cdot g_1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \kappa_1\cdot g_1 \end{pmatrix} \quad \cdots(13)$$

となる。

[0099] A*：A*は基底ベクトルa_i^*(i=1,...,n+1)を要素とするn+1行n+1列の行列を表す。例えば、基底ベクトルa_i^*(i=1,...,n+1)が式(10)によって表現される場合、行列A*は、

[数23]

$$A^*=\begin{pmatrix} a_1^* \\ a_2^* \\ \vdots \\ a_{n+1}^* \end{pmatrix}=\begin{pmatrix} \kappa_2\cdot g_2 & 0 & \cdots & 0 \\ 0 & \kappa_2\cdot g_2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \kappa_2\cdot g_2 \end{pmatrix} \quad \cdots(14)$$

となる。

[0100] X：Xは有限体F_qの元を要素とするn+1行n+1列の行列を表す。行列Xは基底ベクトルa_iの座標変換に用いられる。行列Xのi行j列(i=1,...,n+1,j=1,...,n+1)の要素を$\chi_{i,j}\in F_q$とすると、行列Xは、

[数24]

$$X=\begin{pmatrix} \chi_{1,1} & \chi_{1,2} & \cdots & \chi_{1,n+1} \\ \chi_{2,1} & \chi_{2,2} & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n+1,1} & \chi_{n+1,2} & \cdots & \chi_{n+1,n+1} \end{pmatrix} \quad \cdots(15)$$

となる。なお、行列Xの各要素$\chi_{i,j}$を変換係数と呼ぶ。

[0101] X*：X*は行列Xの逆行列の転置行列$X^*=(X^{-1})^T$を表す。行列X*は基底ベクトルa_i^*の座標変換に用いられる。行列X*のi行j列の要素を$\chi_{i,j}^*\in F_q$とすると、行列X*は、

[数25]

$$X^{*}=\begin{pmatrix} \chi_{1,1}^{*} & \chi_{1,2}^{*} & \cdots & \chi_{1,n+1}^{*} \\ \chi_{2,1}^{*} & \chi_{2,2}^{*} & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n+1,1}^{*} & \chi_{n+1,2}^{*} & \cdots & \chi_{n+1,n+1}^{*} \end{pmatrix} \quad \cdots(16)$$

となる。なお、行列X*の各要素$\chi_{i,j}^{*}$を変換係数と呼ぶ。

この場合、n+1行n+1列の単位行列をIとすると$X\cdot(X^{*})^{T}=I$を満たす。すなわち、単位行列

[数26]

$$I=\begin{pmatrix} 1_F & 0_F & \cdots & 0_F \\ 0_F & 1_F & & \vdots \\ \vdots & & \ddots & 0_F \\ 0_F & 0_F & \cdots & 1_F \end{pmatrix} \quad \cdots(17)$$

に対し、

[数27]

$$\begin{pmatrix} \chi_{1,1} & \chi_{1,2} & \cdots & \chi_{1,n+1} \\ \chi_{2,1} & \chi_{2,2} & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n+1,1} & \chi_{n+1,2} & \cdots & \chi_{n+1,n+1} \end{pmatrix}\cdot\begin{pmatrix} \chi_{1,1}^{*} & \chi_{2,1}^{*} & \cdots & \chi_{n+1,1}^{*} \\ \chi_{1,2}^{*} & \chi_{2,2}^{*} & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{1,n+1}^{*} & \chi_{2,n+1}^{*} & \cdots & \chi_{n+1,n+1}^{*} \end{pmatrix} \quad \cdots(18)$$

$$=\begin{pmatrix} 1_F & 0_F & \cdots & 0_F \\ 0_F & 1_F & & \vdots \\ \vdots & & \ddots & 0_F \\ 0_F & 0_F & \cdots & 1_F \end{pmatrix}$$

を満たす。ここで、n+1次元ベクトル

$$\chi_{i}^{\rightarrow}=(\chi_{i,1},\ldots,\chi_{i,n+1}) \quad \cdots(19)$$

$$\chi_{j}^{\rightarrow *}=(\chi_{j,1}^{*},\ldots,\chi_{j,n+1}^{*}) \quad \cdots(20)$$

を定義する。すると、式(18)の関係から、n+1次元ベクトル$\chi_{i}^{\rightarrow}$と$\chi_{j}^{\rightarrow *}$との内積は、

$$\chi_{i}^{\rightarrow}\cdot\chi_{j}^{\rightarrow *}=\delta(i,j) \quad \cdots(21)\text{となる。}$$

[0102] b_i：b_iは巡回群G_1のn+1個の元を要素とするn+1次元の基底ベクトルを表す。

基底ベクトルb_iは行列Xを用いて基底ベクトルa_i(i=1,...,n+1)を座標変換することで得られる。具体的には、基底ベクトルb_iは、

$$b_i=\Sigma_{j=1}^{n+1}\chi_{i,j}\cdot a_j \quad \cdots(22)$$

の演算によって得られる。例えば、基底ベクトルa_j(j=1,...,n+1)が式(9)によって表現される場合、基底ベクトルb_iの各要素をそれぞれ列挙して表現すると、以下のようになる。

$$b_i=(\chi_{i,1}\cdot\kappa_1\cdot g_1\ ,\chi_{i,2}\cdot\kappa_1\cdot g_1\ ,...,\chi_{i,n+1}\cdot\kappa_1\cdot g_1) \quad \cdots(23)$$

巡回群G_1のn+1個の元を要素とするすべてのn+1次元ベクトルは、n+1次元の基底ベクトルb_i(i=1,...,n+1)の線形和によって表される。すなわち、n+1次元の基底ベクトルb_iは前述のベクトル空間Vを張る。

[0103] b_i^*：b_i^*は巡回群G_2のn+1個の元を要素とするn+1次元の基底ベクトルを表す。行列X^*を用いて基底ベクトルa_i^*(i=1,...,n+1)を座標変換することで得られる。具体的には、基底ベクトルb_i^*は、

$$b_i^*=\Sigma_{j=1}^{n+1}\chi_{i,j}^*\cdot a_j^* \quad \cdots(24)$$

の演算によって得られる。例えば、基底ベクトルa_j^*(j=1,...,n+1)が式(10)によって表現される場合、基底ベクトルb_i^*の各要素をそれぞれ列挙して表現すると、以下のようになる。

$$b_i^*=(\chi_{i,1}^*\cdot\kappa_2\cdot g_2\ ,\chi_{i,2}^*\cdot\kappa_2\cdot g_2\ ,...,\chi_{i,n+1}^*\cdot\kappa_2\cdot g_2) \quad \cdots(25)$$

となる。巡回群G_2のn+1個の元を要素とするすべてのn+1次元ベクトルは、n+1次元の基底ベクトルb_i^*(i=1,...,n+1)の線形和によって表される。すなわち、n+1次元の基底ベクトルb_i^*は前述のベクトル空間V^*を張る。

[0104] なお、基底ベクトルb_iと基底ベクトルb_i^*とは、0_Fを除く有限体F_qの元$\tau=\kappa_1\cdot\kappa_2$について

$$e(b_i,\ b_j^*)=g_T^{\tau\cdot\delta(i,j)} \quad \cdots(26)$$

を満たす。すなわち、式(6)(21)(23)(25)の関係から、

[数28]

$$
\begin{aligned}
e(b_i, b_j^*) &= \prod_{L=1}^{n+1} \mathrm{Pair}(\chi_{i,L} \cdot \kappa_1 \cdot g_1, \chi_{j,L}^* \cdot \kappa_2 \cdot g_2) \\
&= \mathrm{Pair}(\chi_{i,1} \cdot \kappa_1 \cdot g_1, \chi_{j,1}^* \cdot \kappa_2 \cdot g_2) \cdot \ldots \cdot (\chi_{i,n} \cdot \kappa_1 \cdot g_1, \chi_{j,n}^* \cdot \kappa_2 \cdot g_2) \\
&\quad \times \mathrm{Pair}(\chi_{j,n+1} \cdot \kappa_1 \cdot g_1, \chi_{j,n+1}^* \cdot \kappa_2 \cdot g_2) \\
&= \mathrm{Pair}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_{i,1} \cdot \chi_{j,1}^*} \cdot \ldots \cdot \mathrm{Pair}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_{i,2} \cdot \chi_{j,2}^*} \\
&\quad \times \mathrm{Pair}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_{i,n+1} \cdot \chi_{j,n+1}^*} \\
&= \mathrm{Pair}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 (\chi_{i,1} \cdot \chi_{j,1}^* + \chi_{i,2} \cdot \chi_{j,2}^* + \ldots + \chi_{i,n+1} \cdot \chi_{j,n+1}^*)} \\
&= \mathrm{Pair}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \vec{\chi_i} \cdot \vec{\chi_j}^*} \\
&= \mathrm{Pair}(g_1, g_2)^{\tau \cdot \delta(i,j)} = g_T^{\tau \cdot \delta(i,j)}
\end{aligned}
$$

を満たす。特に、$\tau = \kappa_1 \cdot \kappa_2 = 1_F$である場合（例えば、$\kappa_1 = \kappa_2 = 1_F$の場合）、

$$e(b_i, b_j^*) = g_T^{\delta(i,j)} \qquad \cdots(27)$$

を満たす。この場合、基底ベクトルb_iと基底ベクトルb_i^*とは、双対ペアリングベクトル空間（ベクトル空間Vとベクトル空間V*）の双対正規直交基底である。

なお、式(26)の関係を満たすのであれば、式(9)(10)で例示したもの以外の基底ベクトルa_i及びa_i^*や、式(22)(24)で例示したもの以外の基底ベクトルb_i及びb_i^*を用いてもよい。

[0105] B：Bは基底ベクトルb_i(i=1,...,n+1)を要素とするn+1行n+1列の行列を表す。B=X・Aを満たす。例えば、基底ベクトルb_iが式(23)によって表現される場合、行列Bは、

[数29]

$$
\begin{aligned}
B &= \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_{n+1} \end{pmatrix} \\
&= \begin{pmatrix} \chi_{1,1} \cdot \kappa_1 \cdot g_1 & \chi_{1,2} \cdot \kappa_1 \cdot g_1 & \cdots & \chi_{1,n+1} \cdot \kappa_1 \cdot g_1 \\ \chi_{2,1} \cdot \kappa_1 \cdot g_1 & \chi_{2,2} \cdot \kappa_1 \cdot g_1 & & \vdots \\ \vdots & & \ddots & \chi_{n,n+1} \cdot \kappa_1 \cdot g_1 \\ \chi_{n+1,1} \cdot \kappa_1 \cdot g_1 & \cdots & \chi_{n+1,n} \cdot \kappa_1 \cdot g_1 & \chi_{n+1,n+1} \cdot \kappa_1 \cdot g_1 \end{pmatrix}
\end{aligned}
\qquad \cdots(28)
$$

となる。

[0106] B*：B*は基底ベクトルb_i^*(i=1,...,n+1)を要素とするn+1行n+1列の行列を表す。B*=X*・A*を満たす。例えば、基底ベクトルb_i^*(i=1,...,n+1)が式(25)によって表現される場合、行列B*は、

[数30]

$$\mathbf{B}^* = \begin{pmatrix} \mathbf{b}_1^* \\ \mathbf{b}_2^* \\ \vdots \\ \mathbf{b}_{n+1}^* \end{pmatrix} = \begin{pmatrix} \chi_{1,1}^* \cdot \kappa_2 \cdot \mathbf{g}_2 & \chi_{1,2}^* \cdot \kappa_2 \cdot \mathbf{g}_2 & \cdots & \chi_{1,n+1}^* \cdot \kappa_2 \cdot \mathbf{g}_2 \\ \chi_{2,1}^* \cdot \kappa_2 \cdot \mathbf{g}_2 & \chi_{2,2}^* \cdot \kappa_2 \cdot \mathbf{g}_2 & & \vdots \\ \vdots & & \ddots & \chi_{n,n+1}^* \cdot \kappa_2 \cdot \mathbf{g}_2 \\ \chi_{n+1,1}^* \cdot \kappa_2 \cdot \mathbf{g}_2 & \cdots & \chi_{n+1,n}^* \cdot \kappa_2 \cdot \mathbf{g}_2 & \chi_{n+1,n+1}^* \cdot \kappa_2 \cdot \mathbf{g}_2 \end{pmatrix} \quad \cdots(29)$$

となる。

[0107] $\vec{w}$：$\vec{w}$は有限体F_qの元を要素とするn次元ベクトルを表す。

$$\vec{w}=(w_1,\ldots,w_n)\in F_q^n \quad \cdots(30)$$

w_μ：w_μはn次元ベクトルのμ(μ=1,...,n)番目の要素を表す。

$\vec{v}$：$\vec{v}$は有限体F_qの元を要素とするn次元ベクトルを表す。

$$\vec{v}=(v_1,\ldots,v_n)\in F_q^n \quad \cdots(31)$$

v_μ：v_μはn次元ベクトルのμ(μ=1,...,n)番目の要素を表す。

[0108] 衝突困難な関数：「衝突困難な関数」とは、十分大きなセキュリティパラメータkに対して以下の条件を満たす関数h、又は、それとみなせる関数を表す。

$$Pr[A(h)=(x,y)|h(x)=h(y)\wedge x\neq y]<\varepsilon(k) \quad \cdots(32)$$

ただし、Pr[・]は事象[・]の確率であり、A(h)は関数hに対してh(x)=h(y)を満たす値x,y（x≠y）を算出する確率的多項式時間アルゴリズムであり、ε(k)はセキュリティパラメータkについての多項式である。衝突困難な関数の例は、参考文献１に開示された「cryptographic hash function」などのハッシュ関数である。

[0109] 単射関数：「単射関数」とは、値域に属する元が何れもその定義域のただ一つの元の像として表される関数、又は、それとみなせる関数を表す。単射関数の例は、参考文献１に開示された「KDF(Key Derivation Function)」などのハッシュ関数である。

[0110] 擬似的なランダム関数：「擬似的なランダム関数」とは、任意の確率的多項式時間アルゴリズムが集合Φ_ζとその部分集合ϕ_ζとを区別できない場合における、当該部分集合ϕ_ζに属する関数、又は、それとみなせる関数を表す。ただし、集合Φ_ζは集合$\{0,1\}^\zeta$の元を集合$\{0,1\}^\zeta$の元へ写すすべての関数の集合である。擬似的なランダム関数の例は、上述のようなハッシュ関数である。

[0111] H_1：H_1は２つのバイナリ系列（ω_1, ω_2）$\in\{0,1\}^k\times\{0,1\}^*$を入力とし、有限体$F_q$の２つの元（$\phi_1, \phi_2$）$\in F_q\times F_q$を出力する衝突困難な関数を表す。

$$H_1 : \{0,1\}^k\times\{0,1\}^*\rightarrow F_q\times F_q \quad \cdots(33)$$

このような関数H_1の例は、ω_1とω_2とのビット連結値$\omega_1||\omega_2$を入力とし、参考文献１に開示された「cryptographic hash function」などのハッシュ関数と、「バイナリ系列から整数への変換関数（Octet string/integer conversion）」と、「バイナリ系列から有限体の元への変換関数（Octet string and integer/finite field conversion）」との演算を行い、有限体F_qの２つの元（ϕ_1, ϕ_2）$\in F_q\times F_q$を出力する関数である。なお、関数H_1は、擬似的なランダム関数であることが望ましい。

[0112] H_2：H_2は巡回群G_Tの元とバイナリ系列（ξ, ω_2）$\in G_T\times\{0,1\}^*$を入力とし、有限体F_qの１つの元$\phi\in F_q$を出力する衝突困難な関数を表す。

$$H_2 : G_T\times\{0,1\}^*\rightarrow F_q \quad \cdots(34)$$

このような関数H_2の例は、巡回群G_Tの元$\xi\in G_T$とバイナリ系列$\omega_2\in\{0,1\}^*$とを入力とし、巡回群G_Tの元$\xi\in G_T$を参考文献１に開示された「有限体の元からバイナリ系列への変換関数（Octet string and integer/finite field conversion）」に入力してバイナリ系列を求め、そのバイナリ系列とバイナリ系列$\omega_2\in\{0,1\}^*$とのビット連結値に対して参考文献１に開示された「cryptograph

ic hash function」などのハッシュ関数演算を行い、さらに「バイナリ系列から有限体の元への変換関数（Octet string and integer/finite field conversion）」の演算を行い、有限体F_qの１つの元$\psi \in F_q$を出力する関数である。なお、安全性の観点から、関数H_2は擬似的なランダム関数であることがより望ましい。

[0113] R:Rは１つの巡回群G_Tの元$\xi \in G_T$を入力とし、１つのバイナリ系列$\omega \in \{0,1\}^k$を出力する単射関数を表す。

$$R : G_T \rightarrow \{0,1\}^k \quad \cdots(35)$$

このような単射関数Rの例は、巡回群G_Tの元$\xi \in G_T$を入力とし、参考文献１に開示された「有限体の元からバイナリ系列への変換関数（Octet string and integer/finite field conversion）」と、参考文献１に開示された「KDF(Key Derivation Function)」などのハッシュ関数との演算を行い、１つのバイナリ系列$\omega \in \{0,1\}^k$を出力する関数である。なお、安全性の観点から、関数Rは衝突困難な関数であることが望ましく、擬似的なランダム関数であることがより望ましい。

[0114] Enc：Encは共通鍵暗号方式の暗号化処理を示す共通鍵暗号関数を表す。共通鍵暗号方式の具体例は、カメリア（Camellia（登録商標））やAESなどである。

$Enc_k(M)$：$Enc_k(M)$は、共通鍵Kを用い、共通鍵暗号関数Encに従って平文Mを暗号化して得られた暗号文を表す。

Dec：Decは、共通鍵暗号方式の復号処理を示す共通鍵復号関数を表す。

$Dec_k(C)$：$Dec_k(C)$は、共通鍵Kを用い、共通鍵復号関数Decに従って暗号文Cを復号して得られた復号結果を表す。

[0115] 〔内積述語暗号〕

次に、内積述語暗号の基本的な構成について説明する。

[0116] ＜述語暗号＞

述語暗号（「関数暗号」と呼ぶ場合もある）とは、「属性情報」と呼ばれる情報と「述語情報」と呼ばれる情報との組み合わせが所定の論理式を「真

」にする場合に暗号文が復号できる方式である。「属性情報」と「述語情報」の一方が暗号文に埋め込まれ、他方が鍵情報に埋め込まれる。従来の述語暗号の構成は、例えば、参考文献９「"Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products," with Amit Sahai and Brent Waters One of 4 papers from Eurocrypt 2008 invited to the Journal of Cryptology」等に開示されている。

[0117] ＜内積述語暗号＞

内積述語暗号は、属性情報や述語情報としてベクトルを用い、それらの内積が０となる場合に暗号文が復号される述語暗号である。内積述語暗号では、内積が０となることと論理式が「真」となることとが等価である。

[0118] ［論理式と多項式との関係］

内積述語暗号では、論理和や論理積からなる論理式を多項式で表現する。

まず、「xがη_1である」という命題１と「xがη_2である」という命題２との論理和 $(x=\eta_1)\vee(x=\eta_2)$を

$$(x-\eta_1)\cdot(x-\eta_2) \qquad \cdots(36)$$

という多項式で表現する。すると、各真理値と式(36)の関数値との関係は以下のようになる。

[表1]

命題１ $(x=\eta_1)$	命題２ $(x=\eta_2)$	論理和 $(x=\eta_1)\vee(x=\eta_2)$	関数値 $(x-\eta_1)\cdot(x-\eta_2)$
真	真	真	0
真	偽	真	0
偽	真	真	0
偽	偽	偽	その他

[0119] ［表1］から分かるように、論理和$(x=\eta_1)\vee(x=\eta_2)$が真である場合、式(36)の関数値は0になり、論理和$(x=\eta_1)\vee(x=\eta_2)$が偽である場合、式(36)の関数値は0以外の値となる。すなわち、論理和$(x=\eta_1)\vee(x=\eta_2)$が真であることと、式(36)の関数値が0となることとは等価である。よって、論理和は式(36)で表現できる。

[0120] また、「xがη_1である」という命題１と「xがη_2である」という命題２との

論理積 $(x=\eta_1)\wedge(x=\eta_2)$ を

$$\iota_1\cdot(x-\eta_1)+\iota_2\cdot(x-\eta_2) \qquad \cdots(37)$$

という多項式で表現する。ただし、ι_1及びι_2は乱数である。すると、真理値と式(37)の関数値とは以下の関係となる。

[表2]

命題1 $(x=\eta_1)$	命題2 $(x=\eta_2)$	論理積 $(x=\eta_1)\wedge(x=\eta_2)$	関数値 $\iota_1\cdot(x-\eta_1)+\iota_2\cdot(x-\eta_2)$
真	真	真	0
真	偽	偽	その他
偽	真	偽	その他
偽	偽	偽	その他

[0121] [表２]から分かるように、論理積 $(x=\eta_1)\wedge(x=\eta_2)$ が真である場合、式(37)の関数値は0になり、論理積$(x=\eta_1)\wedge(x=\eta_2)$が偽である場合、式(37)の関数値は0以外の値となる。すなわち、論理積 $(x=\eta_1)\wedge(x=\eta_2)$ が真であることと、式(37)の関数値が0となることとは等価である。よって、論理積は式(37)で表現できる。

[0122] 以上のように、式(36)と式(37)とを用いることで論理和や論理積からなる論理式を多項式f(x)で表現できる。例えば、論理式$\{(x=\eta_1)\vee(x=\eta_2)\vee(x=\eta_3)\}\wedge(x=\eta_4)\wedge(x=\eta_5)$は、多項式

$$f(x)=\iota_1\cdot\{(x-\eta_1)\cdot(x-\eta_2)\cdot(x-\eta_3)\}+\iota_2\cdot(x-\eta_4)+\iota_3\cdot(x-\eta_5) \qquad \cdots(38)$$

で表現できる。

なお、式(36) では、１つの不定元xを用いて論理和を表現したが、複数の不定元を用いて論理和を表現することも可能である。例えば、２つの不定元x_0及びx_1を用い、「x_0がη_0である」という命題１と「x_1がη_1である」という命題２との論理和 $(x_0=\eta_0)\vee(x_1=\eta_1)$ を

$$(x_0-\eta_0)\cdot(x_1-\eta_1)$$

という多項式で表現することも可能であり、３つ以上の不定元を用い、論理和を多項式で表現することも可能である。

[0123] また、式(37) では、１つの不定元xを用いて論理積を表現したが、複数の

不定元を用いて論理積を表現することも可能である。例えば、また、「x_0がη_0である」という命題１と「x_1がη_1である」という命題２との論理積（$x_0=\eta_0$）$\wedge(x_1=\eta_1)$を

$$\iota_0\cdot(x_0-\eta_0)+\iota_1\cdot(x_1-\eta_1)$$

という多項式で表現することも可能であり、３つ以上の不定元を用い、論理積を多項式で表現することも可能である。

[0124] 論理和及び／又は論理積を含む論理式をH(H≧1)種類の不定元$x_0,\ldots,x_{H-1}$を用いて表現した多項式を$f(x_0,\ldots,x_{H-1})$と表現する。また、各不定元$x_0,\ldots,x_{H-1}$に対応する命題を「x_hがη_hである」とする。ただし、η_h（h=0,...H-1）は命題ごとに定まる定数である。この場合、当該論理式を示す多項式$f(x_0,\ldots,x_{H-1})$は、不定元x_hと定数η_hとの差をとる多項式によって当該不定元x_hが当該定数η_hであるという命題を表現し、命題をそれぞれ表現する多項式の積によって当該命題の論理和を表現し、命題又は命題の論理和をそれぞれ表現する多項式の線形和によって当該命題又は命題の論理和の論理積を表現し、それによって論理式を表現した多項式となる。例えば、５つの不定元$x_0,\ldots,x_4$を用い、論理式$\{(x_0=\eta_0)\vee(x_1=\eta_1)\vee(x_2=\eta_2)\}\wedge(x_3=\eta_3)\wedge(x_4=\eta_4)$を多項式で表現すると、

$f(x_0,\ldots,x_4)=\iota_0\cdot\{(x_0-\eta_0)\cdot(x_1-\eta_1)\cdot(x_2-\eta_2)\}+\iota_1\cdot(x_3=\eta_3)+\iota_2\cdot(x_4=\eta_4)$

となる。

[0125] ［多項式と内積の関係］

論理式を示す多項式$f(x_0,\ldots,x_{H-1})$は、２つのn次元ベクトルの内積で表現できる。すなわち、多項式$f(x_0,\ldots,x_{H-1})$は、当該多項式$f(x_0,\ldots,x_{H-1})$の各項の不定元成分を各要素とするベクトル

$$\vec{v}=(v_{1,\ldots,}v_n)$$

と、当該多項式$f(x_0,\ldots,x_{H-1})$の各項の係数成分を各要素とするベクトル

$$\vec{w}=(w_{1,\ldots,}w_n)$$

との内積

$$f(x_0,\ldots,x_{H-1})=\vec{w}\cdot\vec{v}$$

に等しい。すなわち、論理式を示す多項式$f(x_0,...,x_{H-1})$が0であるか否かと、多項式$f(x_0,...,x_{H-1})$の各項の不定元成分を各要素とするベクトル$v^{\rightarrow}$と、多項式$f(x_0,...,x_{H-1})$の各項の係数成分を各要素とするベクトル$w^{\rightarrow}$との内積が0であるか否かとは等価である。

$$f(x_0,...,x_{H-1})=0 \quad \longleftrightarrow \quad w^{\rightarrow}\cdot v^{\rightarrow}=0$$

[0126] 例えば、１つの不定元xで表現された多項式$f(x)=\theta_0\cdot x^0+\theta_1\cdot x+...+\theta_{n-1}\cdot x^{n-1}$は、２つのn次元ベクトル

$$w^{\rightarrow}=(w_1,...,w_n)=(\theta_0,...,\theta_{n-1}) \qquad \cdots(39)$$

$$v^{\rightarrow}=(v_1,...,v_n)=(x^0,...,x^{n-1}) \qquad \cdots(40)$$

の内積

$$f(x)= w^{\rightarrow}\cdot v^{\rightarrow} \qquad \cdots(41)$$

で表現できる。すなわち、論理式を示す多項式f(x)が0であるか否かと、式(41)の内積が0であるか否かとは等価である。

$$f(x)=0 \quad \longleftrightarrow \quad w^{\rightarrow}\cdot v^{\rightarrow}=0 \qquad \cdots(42)$$

また、多項式$f(x_0,...,x_{H-1})$の各項の不定元成分を各要素とするベクトルを

$$w^{\rightarrow}=(w_1,...,w_n)$$

とし、多項式$f(x_0,...,x_{H-1})$の各項の係数成分を各要素とするベクトル

$$v^{\rightarrow}=(v_1,...,v_n)$$

としても、論理式を示す多項式$f(x_0,...,x_{H-1})$が0であるか否かと、ベクトル$w^{\rightarrow}$とベクトル$v^{\rightarrow}$との内積が0であるか否かとは等価である。

例えば、式(39)(40)の代わりに

$$w^{\rightarrow}=(w_1,...,w_n)=(x^0,...,x^n) \qquad \cdots(43)$$

$$v^{\rightarrow}=(v_1,...,v_n)=(\theta_0,...,\theta_{n-1}) \qquad \cdots(44)$$

としても、論理式を示す多項式f(x)が0であるか否かと、式(41)の内積が0であるか否かとは等価である。

[0127] 内積述語暗号では、ベクトル$v^{\rightarrow}=(v_1,...,v_n)$及び$w^{\rightarrow}=(w_1,...,w_n)$の何れか一方を属性情報とし、他方を述語情報とし、属性情報と述語情報の一方が暗号文に埋め込まれ、他方が鍵情報に埋め込まれる。例えば、n次元ベクトル$(\theta_0,...,\theta$

$_{n-1}$)が述語情報とされ、n次元ベクトル($x^0,\ldots,x^{n-1}$)が属性情報とされ、属性情報と述語情報の一方が暗号文に埋め込まれ、他方が鍵情報に埋め込まれる。なお、以下では、鍵情報に埋め込まれるn次元ベクトルを$\vec{w}=(w_1,\ldots,w_n)$とし、暗号文に埋め込まれるn次元ベクトルを$\vec{v}=(v_1,\ldots,v_n)$とする。例えば、

述語情報：$\vec{w}=(w_1,\ldots,w_n)=(\theta_0,\ldots,\theta_{n-1})$

属性情報：$\vec{v}=(v_1,\ldots,v_n)=(x^0,\ldots,x^{n-1})$

であるか、

述語情報：$\vec{v}=(v_1,\ldots,v_n)=(\theta_0,\ldots,\theta_{n-1})$

属性情報：$\vec{w}=(w_1,\ldots,w_n)=(x^0,\ldots,x^{n-1})$

である。

[0128] ［内積述語暗号の基本構成］

以下では、内積述語暗号を用いて鍵カプセル化メカニズムKEM (Key Encapsulation Mechanisms)を構成する場合の基本構成を例示する。この構成はSetup(1^k), GenKey(MSK,$\vec{w}$), Enc(PA,$\vec{v}$), Dec(SKw,C_2)を含む。

[0129] 《Setup(1^k)：セットアップ》

－入力：セキュリティパラメータk

－出力：マスター鍵情報MSK, 公開パラメータPK

Setup(1^k)の一例では、まず、セキュリティパラメータkをnとして、n+1次元の基底ベクトルa_i(i=1,...,n+1)を要素とするn+1行n+1列の行列Aと、基底ベクトルa_i^*(i=1,...,n+1)を要素とするn+1行n+1列の行列A*と、座標変換のためのn+1行n+1列の行列X, X*とが選択される。次に、式(22)に従って座標変換されたn+1次元の基底ベクトルb_i(i=1,...,n+1)が算出され、式(24)に従って座標変換されたn+1次元の基底ベクトルb_i^*(i=1,...,n+1)が算出される。そして、基底ベクトルb_i^*(i=1,...,n+1)を要素とするn+1行n+1列の行列B*がマスター鍵情報MSKとして出力され、ベクトル空間V, V*、基底ベクトルb_i(i=1,...,n+1)を要素とするn+1行n+1列の行列B、セキュリティパラメータk、有限体F_q、楕円曲線E、巡回群G_1, G_2,G_T、生成元g_1, g_2, g_T、双線形関数eなどが公開パラメータPKとして出力される。

[0130] 《GenKey(MSK,$w^{\rightarrow}$)：鍵情報生成》

－入力：マスター鍵情報MSK，ベクトル$w^{\rightarrow}$

－出力：ベクトル$w^{\rightarrow}$に対応する鍵情報D^*

GenKey(MSK,$w^{\rightarrow}$)の一例では、まず、有限体F_qから元$\alpha \in F_q$が選択される。そして、マスター鍵情報MSKである行列B^*を用い、ベクトル$w^{\rightarrow}$に対応する鍵情報

$$D^*=\alpha \cdot (\Sigma_{\mu=1}^{n} w_\mu \cdot b_\mu^*)+b_{n+1}^* \in G_2^{n+1} \quad \cdots(45)$$

が生成され、出力される。なお、巡回群G_2上での離散対数問題の求解が困難である場合、鍵情報D^*から$w_\mu \cdot b_\mu^*$やb_{n+1}^*の成分を分離抽出することは困難である。

[0131] 《Enc(PA,$v^{\rightarrow}$)：暗号化》

－入力：公開パラメータPK，ベクトル$v^{\rightarrow}$

－出力：暗号文C_2，共通鍵K

Enc(PA,$v^{\rightarrow}$)の一例では、まず、共通鍵Kと有限体F_qの元である乱数υ_1とが生成される。そして、行列Bなどの公開パラメータPKと、共通鍵Kを含む値に対応する有限体F_qの元υ_2と、ベクトル$v^{\rightarrow}$と、乱数υ_1とを用い、暗号文

$$C_2=\upsilon_1 \cdot (\Sigma_{\mu=1}^{n} v_\mu \cdot b_\mu)+\upsilon_2 \cdot b_{n+1} \in G_1^{n+1} \quad \cdots(46)$$

が生成される。そして、暗号文C_2と共通鍵Kとが出力される。共通鍵Kの一例は$K=g_T^{\tau \cdot \upsilon 2} \in G_T$である。ここで、添え字の$\upsilon 2$は$\upsilon_2$を意味する。また、前述のように$\tau$の一例は$\tau=1_F$である。なお、巡回群$G_1$上での離散対数問題の求解が困難である場合、暗号文$C_2$から$v_\mu \cdot b_\mu$や$\upsilon_2 \cdot b_{n+1}$の成分を分離抽出することは困難である。

[0132] 《Dec(SKw,C_2)：復号・鍵共有》

－入力：ベクトル$w^{\rightarrow}$に対応する鍵情報D_1^*，暗号文C_2

－出力：共通鍵K

Dec(SKw,C_2)の一例では、まず、暗号文C_2と鍵情報D_1^*とが式(2)の双線形関数eに入力される。すると、式(3)(26)の性質から、

[数31]

$$\begin{aligned} e(C_2,D^*) &= e(\upsilon_1\cdot(\textstyle\sum_{\mu=1}^{n} v_\mu\cdot b_\mu)+\upsilon_2\cdot b_{n+1},\alpha\cdot(\textstyle\sum_{\mu=1}^{n} w_\mu\cdot b_\mu^{\,*})+b_{n+1}^{\,*}) \\ &= e(\upsilon_1\cdot v_1\cdot b_1,\alpha\cdot w_1\cdot b_1^{\,*})\cdot\ldots\cdot e(\upsilon_1\cdot v_n\cdot b_n,\alpha\cdot w_n\cdot b_n^{\,*}) \\ &\quad\times e(\upsilon_2\cdot b_{n+1},b_{n+1}^{\,*}) \\ &= e(b_1,b_1^{\,*})^{\upsilon_1\cdot v_1\cdot\alpha\cdot w_1}\cdot\ldots\cdot e(b_n,b_n^{\,*})^{\upsilon_1\cdot v_n\cdot\alpha\cdot w_n}\cdot e(b_{n+1},b_{n+1}^{\,*})^{\upsilon_2} \\ &= g_T^{\tau\cdot\upsilon_1\cdot v_1\cdot\alpha\cdot w_1}\cdot\ldots\cdot g_T^{\tau\cdot\upsilon_1\cdot v_n\cdot\alpha\cdot w_n}\cdot g_T^{\tau\cdot\upsilon_2} \\ &= g_T^{\tau\cdot\upsilon_1\cdot\alpha\cdot\vec{v}\cdot\vec{w}}\cdot g_T^{\tau\cdot\upsilon_2} \end{aligned} \quad \cdots(47)$$

を満たす。

ここで、内積$\vec{w}\cdot\vec{v}=0$であれば、式(47)は、

[数32]

$$\begin{aligned} e(C_2,D^*) &= g_T^{\tau\cdot\upsilon_1\cdot\alpha\cdot 0}\cdot g_T^{\tau\cdot\upsilon_2} \\ &= g_T^{\tau\cdot\upsilon_2} \end{aligned} \quad \cdots(48)$$

と変形できる。この結果から共通鍵Kが生成され出力される。共通鍵Kの一例は$K=g_T^{\tau\cdot\upsilon 2}\in G_T$である。

[0133] ここではn+1次元の基底ベクトルを用いてアルゴリズムを構成する例を示したが、次元はn+1に限定されず、Ξを２以上の所定の整数としてn+Ξ次元の基底ベクトル$b_i^*(i=1,\ldots,n+\Xi)$を用いてアルゴリズムを構成してもよい。このとき、例えば式(45)に替えて式(49)を、式(46)に替えて式(50)を用いることができる。ここでυ_ιは定数や変数（乱数など）などである。

$$D^*=\alpha\cdot(\Sigma_{\mu=1}^{n} w_\mu\cdot b_\mu^*)+\Sigma_{\iota=n+1}^{n+\Xi}\upsilon_\iota\cdot b_\iota^*\in G_2^{n+\Xi} \quad \cdots(49)$$

$$C_2=\upsilon_1\cdot(\Sigma_{\mu=1}^{n} v_\mu\cdot b_\mu)+\Sigma_{\iota=2}^{\Xi+1}\upsilon_\iota\cdot b_{\iota+n-1}\in G_1^{n+\Xi} \quad \cdots(50)$$

[0134] なお、式(45)は、

$$D^*=\alpha\cdot(\Sigma_{\mu=1}^{n} w_\mu\cdot b_\mu^*)+\upsilon_{n+1}\cdot b_{n+1}^*\in G_2^{n+1}$$

であってもよい。さらに、入力情報を入れ換えて、つまり、式(45)にてwをvに置換し式(46)にてvをwに置換してもよい。

[0135] 次に、第１の観点から、柔軟に運用可能な、関数暗号（関数暗号の一例として述語暗号を採用する）に依拠する暗号通信技術に関する実施形態を説明する。なお、数式の番号は本節で改めて付け直している。

[0136] 〔第１の観点による第１実施形態〕

図１から図１７を参照して、第１の観点による本発明の第１実施形態を説明する。

[0137] 暗号システム１は、図１に示すように、複数のクライアント装置１０、３０と、一つまたは複数の鍵生成装置２０と、一つまたは複数のユーザ情報管理装置４０（以下、管理装置と言う）、変換規則情報ペア管理装置５０（以下、登録装置と言う）、一つまたは複数の保全装置８０、一つまたは複数の認証装置９０を含んでいる。これらの各装置は、例えばインターネットである通信網５を介して相互に通信可能とされている。

[0138] クライアント装置は、処理目的に応じて、暗号化装置として、あるいは復号装置として機能する。そこで、クライアント装置を機能の観点から、暗号化装置１０または復号装置３０と呼称する。なお、暗号システム１は、暗号化装置としてのみ機能するクライアント装置および／または復号装置としてのみ機能するクライアント装置を含んでもよい。

[0139] 暗号システム１では述語暗号を用いた暗号化と復号が行われる。第１の観点による本発明では、使用する述語暗号アルゴリズムに限定は無く、例えば上記非特許文献２に開示される述語暗号アルゴリズムを用いることが許される。第１の観点による第１実施形態では、ＫＥＭ(Key Encapsulation Mechanisms)タイプの述語暗号アルゴリズムを用いた例を示す。

[0140] 暗号システム１における暗号通信方法を、図２、３、４、６、８、１０を参照しながら叙述する。各装置の機能構成については、図５、７、９を参照されたい。

[0141] 《準備プロセス》

鍵生成装置２０のパラメータ生成部（図示せず）が、述語暗号アルゴリズムで用いられる秘密鍵とエントリを生成する（ステップＳ１）。エントリには、述語暗号アルゴリズムで用いられる公開パラメータ（図面では公開Ｐと略記される）、鍵生成装置２０のアドレス、鍵生成装置２０が使用可能なポリシーリスト、鍵生成装置２０が使用可能なスキーマリストが含まれる。

[0142] 公開パラメータは、例えば位数ｑの巡回群G_1，G_2，G_Tの生成元g_1，g_2，g_T、非退化性を持つ双線形写像ｅ：$G_1 \times G_2 \to G_T$（但し、$e(g_1, g_2)=g_T$）、位数ｑ、（ｎ＋１）次元のベクトル空間Ｖの直交基底Ｂを含む。秘密鍵は、双対ベクトル空間Ｖ*の直交基底Ｂ*を含む。代数構造を有限体F_qとする場合、ｑは素数または素数の冪乗値である。双線形写像ｅは例えばTateペアリングやWeilペアリングである。

[0143] 直交基底Ｂおよび直交基底Ｂ*について説明を加える。（ｎ＋１）次元のベクトル空間Ｖの任意の元が、式（１）のように巡回群G_1の（ｎ＋１）次元直積G_1^{n+1}の元として表されるとする。（ｎ＋１）次元のベクトル空間Ｖの任意の元は、（ｎ＋１）次元のベクトル空間Ｖの標準基底Ａを用いて式（２）のように表すこともできる。ただし、a_iは（ｎ＋１）次元直積G_1^{n+1}の元、z_iは（ｎ＋１）次元直積F_q^{n+1}の元とする。また、１は加法単位元とする。

[数33]

$$V:(g_1^{z_1},\cdots,g_1^{z_{n+1}})\in G_1^{n+1} \qquad (1)$$

$$V:z_1a_1+\cdots+z_{n+1}a_{n+1} \qquad (2)$$

$$A=(a_1,\cdots,a_{n+1})=\begin{pmatrix} g_1 & 1 & \cdots & 1 \\ 1 & g_1 & & \vdots \\ \vdots & & \ddots & 1 \\ 1 & \cdots & 1 & g_1 \end{pmatrix}, \quad a_i\in G_1^{n+1}$$

$$z_i\in F_q^{n+1}$$

[0144] 直交基底Ｂは、式（３）のように、標準基底Ａに（ｎ＋１）次正方行列Ｘを作用させたものとして得られる。記号Ｔは転置を表す。なお、行列Ｘは秘密鍵と同様に秘密とされる。

[数34]

$$B = X \cdot A \qquad (3)$$

$$B = {}^{T}(b_1, \cdots, b_{n+1})$$

$$X = {}^{T}(x_1, \cdots, x_{n+1}) = \left(\chi_{ij}\right)_{(n+1)\times(n+1)}, \quad \chi_{ij} \in F_q$$

$$x_i = (\chi_{i1}, \cdots, \chi_{i(n+1)})$$

$$b_i = \sum_{j=1}^{n+1} \chi_{ij} a_j = (g_1^{x_{i1}}, \cdots, g_1^{x_{i(n+1)}})$$

[0145] 同様に、ベクトル空間Ｖと双対な双対ベクトル空間Ｖ*の任意の元が、式（４）のように巡回群G_2の（ｎ＋１）次元直積G_2^{n+1}の元として表されるとする。双対ベクトル空間Ｖ*の任意の元は、双対ベクトル空間Ｖ*の標準基底Ａ*を用いて式（５）のように表すこともできる。ただし、a_i*は（ｎ＋１）次元直積G_2^{n+1}の元、y_i*は（ｎ＋１）次元直積F_q^{n+1}の元とする。また、１は加法単位元とする。

[数35]

$$V^* : (g_2^{y_1}, \cdots, g_2^{y_{n+1}}) \in G_2^{n+1} \qquad (4)$$

$$V^* : y_1 a_1^* + \cdots + y_{n+1} a_{n+1}^* \qquad (5)$$

$$A^* = \left(a_1^*, \cdots, a_{n+1}^*\right) = \begin{pmatrix} g_2 & 1 & \cdots & 1 \\ 1 & g_2 & & \vdots \\ \vdots & & \ddots & 1 \\ 1 & \cdots & 1 & g_2 \end{pmatrix}, \quad a_i^* \in G_2^{n+1}$$

$$y_i \in F_q^{n+1}$$

[0146] 直交基底Ｂ*は、式（６）のように、標準基底Ａ*に（ｎ＋１）次正方行列${}^{T}(X^{-1})$を作用させたものとして得られる。記号Ｅは単位行列を表す。

[数36]

$$B^* = {}^T(X^{-1}) \cdot A^* \qquad (6)$$

$$B^* = {}^T(b_1^*, \cdots, b_{n+1}^*)$$

$$b_i^* = \left(g_2{}^{x_{i1}^*}, \cdots, g_2{}^{x_{i(n+1)}^*} \right)$$

$$X \cdot {}^T(X^*) = E, \quad X^* = {}^T(X^{-1})$$

[0147] 次に、スキーマリストについて説明を加える。属性を指定する情報（属性指定情報；つまり、例えば名前、生年月日などの属性を具体的に一意に特定する情報であり、属性値ともいう）を述語暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（属性用変換規則情報；属性用スキーマともいう）と、

述語（論理式）を指定する情報（述語（論理式）指定情報；つまり、例えば年齢、権限などの属性に関する条件を論理式などで具体的に設定する情報であり、命題関数ともいう）を当該述語暗号アルゴリズムに用いられる述語情報（論理情報）に変換するための変換規則を規定している情報（述語（論理式）用変換規則情報；述語（論理式）用スキーマともいう）とのペアである変換規則情報ペアをスキーマペアと呼ぶ（図１１－図１３参照）。一つまたは複数のスキーマペアの集合体（データリスト）がスキーマリストである。各々の鍵生成装置２０はスキーマリストを自由に定めてよい。スキーマリストに含まれる各スキーマの各データ項目は、例えばＸＭＬ(eXtensible Markup Language)やＡＳＮ．１(Abstract Notation Number One)で記述される。

[0148] 図１２に示す属性用スキーマの例について説明を加える。ユーザの属性指定情報（属性値）は、属性名およびデータ型に対応付けられている。図１２に示す例では、例えば、属性名‘email1’にデータ型‘文字列’が設定されており、属性名‘email1’およびデータ型‘文字列’に属性値‘XXX@XXX.ntt.co.jp’が対応付けられている。

[0149] 属性用スキーマは、要素番号に属性名と型変換関数を対応付けた変換規則を規定している。図１２に示す例では、例えば、要素番号‘１’に属性名‘

血液型’と型変換関数が対応付けられている。要素番号‘１’に対応する型変換関数は、属性値の血液型がＯ型であれば０に、属性値の血液型がA型であれば１に、属性値の血液型がB型であれば２に、属性値の血液型がAB型であれば３に変換することを規定している。また、要素番号‘２’および‘３’に属性名‘生年月日’と型変換関数が対応付けられている。要素番号‘２’および‘３’に対応する型変換関数は、要素番号２に対して属性値の生年月日の年を入力とするHash関数の値に、要素番号３に対して属性値の生年月日の月日を入力とするHash関数の値に変換することを規定している。

[0150] 図１２に示すユーザの属性指定情報（属性値）の例に図１２に示す属性用スキーマの例を適用した結果が、図１２に示す属性情報（ベクトル情報）の例として示されている。属性用スキーマの要素番号をベクトルの要素番号と見なして型変換関数の出力値を並べることにより、この属性情報をベクトルと考えることができる。なお、一般的に、関数暗号によると、暗号化の際に複数の属性情報を指定できる。例えば、属性用スキーマを複数の属性指定情報に適用することによって、複数の属性情報を得ることができる。あるいは、複数の属性用スキーマを一つの属性指定情報に適用することによって、複数の属性情報を得てもよい。

[0151] なお、型変換関数の出力値は、この説明では整数値やHash関数の出力値として例示されたが、実際には述語暗号アルゴリズムに依拠し例えば有限体F_qの元である。

[0152] 図１３に示す述語用スキーマの例について説明を加える。述語指定情報として属性に関する条件を表す論理式が与えられる。図１３に示す例では、例えば、属性名‘名前’の属性値を‘田中太郎’とし、属性名‘年齢’の属性値を‘２０歳以上’とする述語指定情報‘名前=田中太郎かつ年齢=20歳以上’が与えられている。

[0153] 述語用スキーマは、要素番号に属性名と型変換関数を対応付けた変換規則を規定している。図１３に示す例では、例えば、要素番号‘１’に属性名‘血液型’と型変換関数が対応付けられている。要素番号‘１’に対応する型

変換関数は、属性値の血液型がＯ型であればＯに、属性値の血液型がA型であれば１に、属性値の血液型がB型であれば２に、属性値の血液型がAB型であれば３に変換することを規定している。また、要素番号‘2’および‘3’に属性名‘生年月日’と型変換関数が対応付けられている。要素番号‘2’および‘3’に対応する型変換関数は、要素番号２に対して属性値の生年月日の年を入力とするHash関数の値に、要素番号３に対して属性値の生年月日の月日を入力とするHash関数の値に変換することを規定している。

[0154] 図１３に示す述語指定情報の例に図１３に示す述語用スキーマの例を適用した結果が、図１３に示す述語情報（ベクトル情報）の例として示されている。具体的には、この例では、述語用スキーマを述語指定情報に適用することにより要素番号に応じた変数を持つ多変数多項式ｆが得られ、この多変数多項式ｆをベクトル情報に変換することにより、述語情報（ベクトル情報）が得られる。図１３に示す述語指定情報の例に則して説明する。述語指定情報‘名前=田中太郎かつ年齢=20歳以上’に述語用スキーマを適用することにより、要素番号‘０’に対応した型変換関数の出力値‘Hash(田中太郎)’および要素番号‘２３’に対応した型変換関数の出力値‘１’が得られる。そして、要素番号‘０’に対応した型変換関数の出力値‘Hash(田中太郎)’を零点とする要素番号‘０’に対応した変数X_0の１次式と、要素番号‘２３’に対応した型変換関数の出力値‘１’を零点とする要素番号‘２３’に対応した変数X_{23}の１次式との線形結合により、多変数多項式$f=r_1(X_0-H(田中太郎))+r_2(X_{23}-1)$が得られる。ここで$r_1$と$r_2$は乱数である。さらに、この多変数多項式ｆを展開して各項の係数を並べることにより、多変数多項式ｆがベクトル情報に変換され、図１３に示す述語情報（ベクトル情報）の例が得られる。なお、一般的に、関数暗号によると、暗号化の際に複数の述語情報を指定できる。例えば、述語用スキーマを複数の述語指定情報に適用することによって、複数の述語情報を得ることができる。あるいは、複数の述語用スキーマを一つの述語指定情報に適用することによって、複数の述語情報を得てもよい。

[0155] なお、型変換関数の出力値は、この説明では整数値やHash関数の出力値として例示されたが、実際には述語暗号アルゴリズムに依拠し例えば有限体F_qの元である。

[0156] また、スキーマペアを構成する両スキーマの間では、属性名と型変換関数との組み合わせ、入力となる属性値のデータ型などが統一されていることが求められる。

[0157] 次にポリシーリストについて図１４を参照して説明を加える。属性用スキーマと述語用スキーマのうちいずれであるかを特定するための情報をポリシー情報（以下、ポリシーと言う）と呼ぶ。このポリシーを記述したデータリストがポリシーリストである。鍵生成装置２０が属性用スキーマと述語用スキーマの両方を使用する場合には、ポリシーとして２種類のタイプが用意される。それはCipher_Text_PolicyとKey_Policyである。鍵生成装置２０が属性用スキーマのみを使用する場合には、ポリシーとして１種類のタイプが用意される。それは、Key_Policyである。鍵生成装置２０が述語用スキーマのみを使用する場合には、ポリシーとして１種類のタイプが用意される。それは、Cipher_Text_Policyである。ポリシーは、例えばＸＭＬ(eXtensible Markup Language)やASN.1(Abstract Notation Number One)で記述される。鍵生成装置２０は、ポリシーの特定対象が、属性用スキーマのみ、あるいは、述語用スキーマのみ、あるいは、属性用スキーマおよび述語用スキーマであることを自由に定めてよい。一般的に関数暗号によると、上述のように、複数の異なる属性用スキーマを一つの属性指定情報に適用することによって、複数の属性情報を得ることができるので、このような場合は、ポリシーとして複数の属性用スキーマを指定しておく。複数の異なる述語用スキーマを一つの述語指定情報に適用することによって、複数の述語情報を得ることができるので、このような場合は、ポリシーとして複数の述語用スキーマを指定しておく。

[0158] ステップＳ１の処理に続いて、鍵生成装置２０の送信部はエントリを認証装置９０に送信し、認証装置９０の受信部がエントリを受信する（ステップ

Ｓ２）。認証装置９０の署名付与部（図示せず）がエントリに対して例えば従来的な手法で電子署名を付与して（ステップＳ３）、認証装置９０の送信部が署名付きエントリを鍵生成装置２０に送信し、鍵生成装置２０の受信部が署名付きエントリを受信する（ステップＳ４）。そして、鍵生成装置２０の送信部が署名付きエントリを保全装置８０に送信し、保全装置８０の受信部が署名付きエントリを受信する（ステップＳ５）。

[0159] 保全装置８０の送信部は鍵生成装置２０を特定する情報（例えばアドレス）を含む検索クエリを登録装置５０に送信し、登録装置５０の受信部が検索クエリを受信する（ステップＳ６）。登録装置５０の検索部（図示せず）は、鍵生成装置２０に関する登録内容（エントリ）を検索し（ステップＳ７）、登録装置５０の送信部が登録の有無や登録内容を含む検索結果を保全装置８０に送信し、保全装置８０の受信部が検索結果を受信する（ステップＳ８）。

[0160] 保全装置８０の検査部（図示せず）は、ステップＳ５の処理で受信した署名付きエントリと、ステップＳ８の処理で受信した検索結果を比較し、重複の有無を検査する（ステップＳ９）。重複の無いことを確認できた場合、保全装置８０の送信部は、署名付きエントリを登録装置５０に送信し、登録装置５０の受信部が、署名付きエントリを受信する（ステップＳ１０）。登録装置５０の登録部（図示せず）は、署名付きエントリを鍵生成装置２０と対応付けて登録装置５０の記憶部に記憶する（ステップＳ１１）。登録装置５０の送信部は登録結果を保全装置８０に送信し、保全装置の受信部が登録結果を受信する（ステップＳ１２）。保全装置８０の送信部は、登録結果を鍵生成装置２０に送信し、鍵生成装置２０は登録結果を受信する（ステップＳ１３）。

[0161] 複数の鍵生成装置２０が存在する場合、各鍵生成装置２０が独自に、ステップＳ１からステップＳ１３の各処理を行う。例えば、公開パラメータと秘密鍵は鍵生成装置ごとに定められる。但し、このことは、各鍵生成装置が共通の公開パラメータと秘密鍵を持つことを妨げるものではない。また、各鍵

生成装置が同じ登録装置５０にエントリを登録してもよいし、各鍵生成装置が異なる登録装置５０にエントリを登録してもよい。

[0162] 予め、秘密鍵、エントリ、登録装置５０へのエントリ登録などが設定されている場合には、ステップＳ１からステップＳ１３の各処理を省略することが許される。

[0163] また、認証装置９０と保全装置８０は同じハードウェアエンティティであってもよい。なお、エントリ登録に認証を要求しない場合や、登録装置５０に登録されるエントリの一意性が確保されている場合などでは、暗号システム１が保全装置８０および／または認証装置９０を備えないシステム構成も許容される。

[0164] これで《準備プロセス》は終了する。

[0165] 《暗号化プロセス》

暗号化装置１０の送信部１４は、図示しない制御部の制御を受けて、検索クエリを登録装置５０に送信し、登録装置５０の受信部が検索クエリを受信する（ステップＳ１４）。登録装置５０の検索部は、登録装置５０の記憶部に登録されているエントリの一部または全部を検索して任意の一つのエントリを選び（ステップＳ１５）、登録装置５０の送信部は検索結果のエントリを暗号化装置１０に送信し、暗号化装置１０の受信部はエントリを受信する（ステップＳ１６）。このエントリには、鍵生成装置のアドレス、この鍵生成装置の公開パラメータ、この鍵生成装置が使用可能なポリシーリスト、この鍵生成装置が使用可能なスキーマリストが含まれている。受信したエントリは、暗号化装置１０のメモリ１１に記憶される。

[0166] なお、各鍵生成装置２０の公開パラメータ、スキーマリスト、ポリシーリスト、アドレスを予め暗号化装置１０が所有している場合には、ステップＳ１４－Ｓ１６の処理は省略される。つまり、暗号システム１が登録装置５０を含まない形態も許容されることに注意しなければならない。

[0167] 暗号化装置１０の第１述語論理情報取得部１２が、メモリ１１から入力情報とポリシーとスキーマを読み込み、属性情報（以下、第１属性情報と言う

）または述語情報（以下、第１述語情報と言う）を求める（ステップＳ１７ａ）。この処理の詳細について説明を加える（図１２、図１３参照）。

[0168] まず、スキーマリストに複数のスキーマペアが記述されている場合、用途などに応じて一つのスキーマペアが選択される。暗号化装置１０の利用者によってスキーマペアが選択されてその指示情報が入力される場合や、所定の規則に従い、第１述語論理情報取得部１２がスキーマペアを選択してもよい。

[0169] そして、入力情報が属性指定情報または述語指定情報のいずれであるかに応じてポリシーと共にいずれか一方のスキーマを選択する。暗号化装置１０の利用者によってポリシーといずれか一方のスキーマが選択されてその指示情報が入力される場合や、所定の規則に従い、第１述語論理情報取得部１２がポリシーといずれか一方のスキーマを選択する場合のいずれであってもよい。なお、鍵生成装置２０のポリシーが１種類のタイプのみ用意されている場合には、そのポリシーに従ってスキーマペアのうちの一方のスキーマが選択される。もし、選択されたスキーマが入力情報の種類に対応していない場合には、スキーマリストからスキーマペアを再選択するか、登録装置５０からエントリの提供を再度受ければよい。

[0170] 入力情報は、暗号化装置１０の利用者によって入力された情報または、例えばＩＣカード３９のような記憶媒体から暗号化装置１０の取得部（図示せず）が取得した情報でもよい。

[0171] そして、第１述語論理情報取得部１２が、ポリシーに従ってスキーマペアの中から選択されたスキーマを用いて入力情報から第１属性情報または第１述語情報を得る。ポリシーがKey_Policyであり選択されたスキーマが属性用スキーマである場合には第１属性情報が得られる。ポリシーがCipher_Text_Policyであり選択されたスキーマが述語用スキーマである場合には第１述語情報が得られる。第１属性情報と第１述語情報は、第１の観点による第１実施形態では、有限体F_qの元を成分とする一つ又は複数のベクトル情報とされる（図１１－１３参照）。この際、スキーマを用いて入力情報から必要な属性

値の抽出や整列化が行われる。

[0172] 次に、暗号化装置１０の暗号化部１３が、第１属性情報ｖ＝（v_1，…，v_n）または第１述語情報ｗ＝（w_1，…，w_n）と、メモリ１１からの公開パラメータに含まれる直交基底Ｂ（実質的な公開鍵）と平文Ｍを用いて、共通鍵Ｋと暗号情報C_1と暗号文C_2を求める（ステップＳ１７ｂ、Ｓ１７ｃ）。これらの処理の詳細について説明を加える。ただし、第１の観点による第１実施形態が共通鍵Ｋの配送に特化した実施形態である場合には暗号文C_2の生成は不要である。

[0173] まず、第１暗号化部１３ａが、述語暗号アルゴリズムに則り、有限体F_qの元である乱数ｒ、ρを生成して、式（７）のように共通鍵Ｋを設定し、式（８）に従って暗号情報C_1を求める（ステップＳ１７ｂ）。Ｈは例えばハッシュ関数である。この例では第１属性情報ｖを用いているが、第１述語情報を用いる場合は式（８）においてｖをｗに置き換えればよい。また、この例では、暗号情報C_1は共通鍵Ｋの生成に用いる情報ρに対応する情報であるが、暗号情報C_1を共通鍵Ｋに対応する情報としてもよい。

[数37]

$$K = H(g_T{}^{\rho}) \qquad (7)$$

$$C_1 = r\sum_{i=1}^{n} v_i b_i + \rho b_{n+1} \qquad (8)$$

[0174] 次に、第２暗号化部１３ｂが、共通鍵Ｋと平文Ｍを用いて、式（９）に従って暗号文C_2を求める（ステップＳ１７ｃ）。共通鍵を用いた暗号化方法Enc_Kは周知の方法でよく、例えば上記非特許文献１に開示される方法である。既述のとおり、第１の観点による第１実施形態が共通鍵Ｋの配送に特化した実施形態である場合には、ステップＳ１７ｃの処理は省略される。つまり、暗号化装置１０は、第２暗号化部１３ｂの機能を持つとしても、ステップＳ１７ｃの処理を行わない。

[数38]

$$C_2 = Enc_K(M) \qquad (9)$$

[0175] 次に、暗号化装置１０の送信部１４は、制御部による制御を受けて、暗号情報C_1と、（必要に応じて）暗号文C_2と、メモリ１１からのスキーマペア、ポリシー、公開パラメータ、鍵生成装置のアドレスを纏めた暗号メッセージを生成する（ステップＳ１７ｄ）。そして暗号化装置１０の送信部１４は、暗号メッセージを復号装置３０に送信し、復号装置３０の受信部が暗号メッセージを受信する（ステップＳ１８）。

[0176] これで《暗号化プロセス》は終了する。

[0177] 《復号プロセス》

復号装置３０の送信部３４は、図示しない制御部の制御を受けて、暗号メッセージに含まれる鍵生成装置のアドレスを含む検索クエリを登録装置５０に送信し、登録装置５０の受信部が検索クエリを受信する（ステップＳ１９）。登録装置５０の検索部は、アドレスで指定された鍵生成装置のエントリを検索してそれを選び（ステップＳ２０）、登録装置５０の送信部は検索結果のエントリを復号装置３０に送信し、復号装置３０の受信部はエントリを受信する（ステップＳ２１）。このエントリには、鍵生成装置のアドレス、この鍵生成装置の公開パラメータ、この鍵生成装置が使用可能なポリシーリスト、この鍵生成装置が使用可能なスキーマリストが含まれている。受信したエントリは、復号装置３０のメモリ３１に記憶される。

[0178] なお、各鍵生成装置２０の公開パラメータ、スキーマリスト、ポリシーリスト、アドレスを予め復号装置３０が所有している場合には、ステップＳ１９－Ｓ２１の処理は省略される。この場合、復号装置３０は、暗号メッセージに含まれるアドレスに対応する鍵生成装置のエントリを自身のメモリ３１から検索してこれを取得する。

[0179] 復号装置３０の検証部（図示せず）は、制御部の制御を受けて、暗号メッセージに含まれるスキーマペアとポリシーが、登録装置５０から取得したエントリに含まれるポリシーリストとスキーマリストに含まれるか否かを検証する（ステップＳ２２ａ）。この検証に失敗した場合、復号処理の失敗として処理を終了する（ステップＳ２２ｇ）。

[0180] この検証に成功した場合、復号装置３０の取得部３２が、例えばＩＣカード３９のような記憶媒体から、当該復号装置３０の利用者に対応する属性指定情報または述語指定情報を読み取る（ステップＳ２２ｆ）。属性指定情報または述語指定情報のいずれを読み取るかは、暗号メッセージに含まれるポリシーによって決まる。つまり、読み取られる情報は、このポリシーで特定される一方のスキーマとペアになっている他方のスキーマを特定するポリシーの内容に対応する指定情報である。もしポリシーがCipher_Text_Policyである場合、取得部３２は記憶媒体から属性指定情報を読み取る。もしポリシーがKey_Policyである場合、取得部３２は記憶媒体から述語指定情報を読み取る。以下、読み取られた指定情報を利用者情報と呼ぶ。また、復号装置３０の取得部３２が、後述する鍵生成装置２０における処理《利用者情報取得プロセス》と同様に、管理装置４０から、当該復号装置３０の利用者に対応する属性指定情報または述語指定情報を読み取ることも許容される。なお、第１の観点による第１実施形態では、ステップＳ２２ｆの処理は任意に行われる。例えば、予め復号装置３０が利用者に対応する属性指定情報と述語指定情報を所有している場合、ポリシーに従って属性指定情報または述語指定情報のいずれかが利用者情報となる。

[0181] 次に、復号装置３０の検証部が、暗号メッセージに含まれる暗号情報を復号するために使用する復号鍵を持っているか否かを検証する（ステップＳ２２ｂ）。

[0182] 復号装置３０はメモリ３１に復号鍵テーブルを記憶している。復号鍵テーブルでは、例えば図１５に示すように、鍵生成装置の識別子に対して、公開パラメータと、スキーマペアと、復号鍵の対象と、述語指定情報と、復号鍵とが対応付けられている。そこで、検証部は、暗号メッセージに含まれるアドレスによって判別する鍵生成装置の識別子、公開パラメータと、スキーマペアと、復号鍵の対象（但し、復号鍵の対象は、暗号メッセージに含まれるポリシーで特定される一方のスキーマとペアになっている他方のスキーマを特定するポリシーの内容に対応する）に対応する復号鍵の有無を検証する。

もし復号鍵が存在すれば、ステップＳ２９の処理を行う。もし復号鍵が存在しなければ、ステップＳ２３の処理を行う。

[0183] ここで《復号プロセス》の説明を中断し、《鍵生成プロセス》の説明をする。

[0184] 上述のように復号鍵が存在しない場合、復号装置３０の送信部３４は、制御部による制御を受けて、メモリ３１からの公開パラメータ、ポリシー、スキーマペア、（もし在れば）利用者情報、認証情報を纏めた鍵要求メッセージを生成する。認証情報は、例えば利用者のＩＤとパスワードを含む。そして、復号装置３０の送信部３４は、メモリ３１からのアドレスを持つ鍵生成装置に鍵要求メッセージを送信し、この鍵生成装置２０の受信部が、鍵要求メッセージを受信する（ステップＳ２３）。受信した鍵要求メッセージは、鍵生成装置２０のメモリ２１に記憶される。

[0185] 鍵生成装置２０の検証部（図示せず）は、制御部の制御を受けて、鍵要求メッセージに含まれるスキーマペアとポリシーが、当該鍵生成装置２０が所有するエントリ（例えばステップＳ１で生成されたエントリである）に含まれるポリシーリストとスキーマリストに含まれるか否か、および、鍵要求メッセージに含まれる公開パラメータが当該鍵生成装置２０の公開パラメータであるか否かを検証する（ステップＳ２４ａ）。この検証に失敗した場合、鍵生成処理の失敗として処理を終了する（ステップＳ２４ｇ）。なお、ステップＳ２４ａの処理では、鍵要求メッセージに認証情報が含まれるならば、鍵要求メッセージに含まれる認証情報の検証も行われる。鍵生成装置２０は、メモリ２１に認証テーブルを記憶している。認証テーブルでは、例えば図１６に示すように、利用者のＩＤに対してパスワードが対応付けられている。そこで、検証部は、鍵要求メッセージに含まれる利用者のＩＤとパスワードと認証テーブルに含まれる利用者のＩＤとパスワードとの整合性を検証する。この検証に失敗した場合も、ステップＳ２４ｇの処理が行われる。

[0186] この検証に成功した場合、鍵生成装置２０の検証部が、鍵要求メッセージに利用者情報が含まれているか否かを検証する（ステップＳ２４ｂ）。鍵要

求メッセージに利用者情報が含まれていればステップＳ２４ｃの処理を行い、鍵要求メッセージに利用者情報が含まれていなければステップＳ２５の処理を行う。なお、必ず鍵要求メッセージに利用者情報が含まれる方法を採用する場合には、ステップＳ２４ｂの処理および後述する《利用者情報取得プロセス》は不要である。

[0187] ここで《鍵生成プロセス》の説明を中断し、《利用者情報取得プロセス》の説明をする。

[0188] 鍵生成装置２０の送信部は、鍵要求メッセージに含まれるポリシーと（もし在れば）認証情報を含むリクエストを管理装置４０に送信し、管理装置４０がリクエストを受信する（ステップＳ２５）。受信したリクエストは、管理装置４０のメモリに記憶される。

[0189] 管理装置４０はメモリに認証テーブルを記憶している。この認証テーブルでは、上述の認証テーブルと同様に、利用者のＩＤに対してパスワードが対応付けられている（図１６参照）。そこで、管理装置４０の検証部（図示せず）は、リクエストに含まれる利用者のＩＤとパスワードと認証テーブルに含まれる利用者のＩＤとパスワードとの整合性を検証する。

[0190] この検証に成功すると、管理装置４０の検索部（図示せず）がリクエストに含まれるポリシーに従って、メモリに記憶されている利用者情報テーブルから属性指定情報または述語指定情報を検索する（ステップＳ２６）。利用者情報テーブルは、例えば利用者のＩＤとこれに対応付けられた属性名および属性指定情報で構成される第１テーブルと、利用者のＩＤとこれに対応付けられた述語指定情報で構成される第２テーブルとを含んでいる（図１７参照）。属性指定情報または述語指定情報のいずれを読み取るかは、リクエストに含まれるポリシーによって決まる。つまり、読み取られる情報は、このポリシーで特定される一方のスキーマとペアになっている他方のスキーマを特定するポリシーの内容に対応する指定情報である。もしポリシーがCipher_Text_Policyである場合、検索部は第１テーブルからリクエストに含まれる利用者のＩＤに対応する属性指定情報を取得する。もしポリシーがKey_Policy

である場合、検索部は第２テーブルからリクエストに含まれる利用者のＩＤに対応する述語指定情報を取得する。読み取られた指定情報を利用者情報と呼ぶ。

[0191] 管理装置４０の送信部は、制御部による制御を受けて、検索結果の利用者情報を鍵生成装置２０に送信し、鍵生成装置２０の受信部が利用者情報を受信する（ステップＳ２７）。受信した利用者情報は、鍵生成装置２０のメモリ２１に記憶される。

[0192] 以上で《利用者情報取得プロセス》を終了し、再び《鍵生成プロセス》の説明に戻る。

[0193] 利用者情報を既に所有している場合、あるいは、利用者情報取得プロセスによって利用者情報を受信した場合（ステップＳ２７）、鍵生成装置２０の第２述語論理情報取得部２３は、メモリ２１からポリシーと、スキーマペアと、公開パラメータと、利用者情報を読み込み、利用者情報から、属性情報（第２属性情報と言う）または述語情報（第２述語情報と言う）を得る（ステップＳ２４ｃ）。この処理において利用者情報に適用されるスキーマは、ポリシーで特定される一方のスキーマとペアになっている他方のスキーマである。ポリシーがCipher_Text_Policyである場合、Cipher_Text_Policyで特定される一方のスキーマ（述語用スキーマ）とペアになっている他方のスキーマ（属性用スキーマ）を用いて、利用者情報（属性指定情報）から第２属性情報を得る。ポリシーがKey_Policyである場合、Key_Policyで特定される一方のスキーマ（属性用スキーマ）とペアになっている他方のスキーマ（述語用スキーマ）を用いて、利用者情報（述語指定情報）から第２述語情報を得る。このように、この処理で用いられるスキーマは、ステップＳ１７ａで用いられたスキーマとペアになっているスキーマであることに注意しなければならない。第２属性情報と第２述語情報は、第１の観点による第１実施形態では、有限体F_qの元を成分とする一つ又は複数のベクトル情報とされる（図１１－１３参照）。この際、スキーマを用いて入力情報から必要な属性値の抽出や整列化が行われる。

[0194] 次に、鍵生成装置２０の鍵生成部２５が、述語暗号アルゴリズムに則り、公開パラメータのｑに基づき有限体F_qの元である乱数αを生成して、メモリ２１からの第２属性情報$v_{(p)}=(v_{(p)1}, \cdots, v_{(p)n})$または第２述語情報$w_{(p)}=(w_{(p)1}, \cdots, w_{(p)n})$と、当該鍵生成装置の秘密鍵Ｂ*を用いて、式（１０）に従って復号鍵Ｒを求める（ステップＳ２４ｄ）。暗号化処理で用いられた入力情報が属性指定情報である場合に対応して、この例では第２述語情報$w_{(p)}$を用いているが、入力情報が述語指定情報である場合には、第２属性情報$v_{(p)}$が対応するので、式（１０）において$w_{(p)}$を$v_{(p)}$に置き換えればよい。

[数39]

$$R=\alpha\sum_{i=1}^{n}w_{(p)i}b_i^*+b_{n+1}^* \qquad (10)$$

[0195] 次に、鍵生成装置２０の送信部２４は、制御部による制御を受けて、復号鍵Ｒを復号装置３０に送信し、復号装置３０の受信部が復号鍵Ｒを受信する（ステップＳ２８）。受信した復号鍵Ｒは、復号装置３０のメモリ３１に記憶される。

[0196] 以上で《鍵生成プロセス》を終了し、再び《復号プロセス》の説明に戻る。

[0197] 復号鍵を既に所有している場合、あるいは、鍵生成プロセスによって復号鍵を受信した場合（ステップＳ２８）、復号装置３０の復号部３３が、メモリ３１から公開パラメータと復号鍵Ｒと暗号情報C_1と（必要に応じて）暗号文C_2を読み込んで、共通鍵Ｋと（必要に応じて）平文Ｍを求める（ステップＳ２９）。

[0198] このステップＳ２９の処理の詳細について説明を加える。第１復号部３３ａは、メモリ３１から公開パラメータと暗号情報C_1と復号鍵Ｒを読み込み、述語暗号アルゴリズムに則り、$e(C_1, R)$を求める。この演算結果は式（１１）に示すように、入力情報が属性指定情報である場合、双線形性に基づき暗号情報C_1と復号鍵Ｒから取り出された第１属性情報ｖと第２述語情報$w_{(p)}$の標準内積の結果に依存する。入力情報が述語指定情報である場合、式（１１

）においてｖをｖ$_{(\rho)}$に、ｗ$_{(\rho)}$をｗに置き換えればよく、演算結果は双線形性に基づき暗号情報Ｃ$_1$と復号鍵Ｒから取り出された第１述語情報ｗと第２属性情報ｖ$_{(\rho)}$の標準内積の結果に依存する。但し、ｅ（ｂ$_i$，ｂ$_i^*$)は式（１２）のように定義される。δ$_{ij}$は、クロネッカーのデルタ記号である。

[数40]

$$e(C_1,R)=e(r\sum_{i=1}^{n}v_ib_i,R)\cdot e(\rho b_{n+1},R)$$
$$=\prod_{i=1}^{n}e(b_i,b_i^*)^{r\alpha v_iw_{(\rho)i}}\cdot e(b_{n+1},b_{n+1}^*)^{\rho}$$
$$=g_T{}^{r\alpha\sum_{i=1}^{n}v_iw_{(\rho)i}}\cdot g_T{}^{\rho}$$
$$=g_T{}^{r\alpha\vec{v}\cdot\vec{w}_{(\rho)}}\cdot g_T{}^{\rho} \qquad (11)$$

$$e(b_i,b_j^*)=\prod_{j=1}^{n+1}e(g_1^{\chi_{ij}},g_2^{\chi_{ij}^*})$$
$$=g_T{}^{\sum_{j=1}^{n+1}\chi_{ij}\chi_{ij}^*}$$
$$=g_T{}^{x_i\cdot{}^Tx_j^*}$$
$$=g_T{}^{\delta_{ij}} \qquad (12)$$

[0199] 従って、第１属性情報ｖと第２述語情報ｗ$_{(\rho)}$の標準内積が０（あるいは第１述語情報ｗと第２属性情報ｖ$_{(\rho)}$の標準内積が０）の場合、式（１１）の演算結果ｇ$_T{}^{\rho}$が得られる。この演算結果ｇ$_T{}^{\rho}$が得られた場合、復号装置３０の第１復号部３３ａは、式（７）に従って“正しい”共通鍵Ｋを得る（ステップＳ２２ｃ）。もし第１属性情報ｖと第２述語情報ｗ$_{(\rho)}$の標準内積が０（あるいは第１述語情報ｗと第２属性情報ｖ$_{(\rho)}$の標準内積が０）ではない場合、第１復号部３３ａは、式（７）に従って“正しくない”値を得る。この例では、ハッシュ関数Ｈはシステムに共通とするか公開パラメータに含まれるとする。この例では、暗号情報Ｃ$_1$が共通鍵Ｋの生成に用いる情報ρに対応する情報であるが、暗号情報Ｃ$_1$を共通鍵Ｋに対応する情報とする場合には、式（１１）の演算結果が共通鍵Ｋ（あるいは正しくない値）となる。つまり、復号装置３０の正当な利用者は、第１属性情報ｖとの標準内積が０となる第２述語情報

$w_{(p)}$を与える述語指示情報、あるいは、第１述語情報ｗとの標準内積が０となる第２属性情報$v_{(p)}$を与える属性指示情報を持つ。

[0200] 次に、第２復号部３３ｂが、共通鍵Ｋと暗号文C_2を用いて、式（１３）に従って平文Ｍを求める（ステップＳ２２ｄ）。共通鍵を用いた復号方法Dec_Kは暗号化方法Enc_Kに対応する。既述のとおり、第１の観点による第１実施形態が共通鍵Ｋの配送に特化した実施形態である場合には、ステップＳ２２ｄの処理は省略される。つまり、復号装置３０は、第２復号部３３ｂの機能を持つとしても、ステップＳ２２ｄの処理を行わない。

[数41]

$$M = Dec_K(C_2) \qquad (13)$$

[0201] もし、式（１１）に従った演算結果が正しくない値である場合には、式（１３）によっては正しい平文Ｍを得ることができない。

[0202] なお、復号装置３０は、復号鍵Ｒを復号鍵テーブルに記憶してもよい。また、共通鍵Ｋを復号鍵テーブルに付加して記憶してもよい。

[0203] これで《復号プロセス》は終了する。

[0204] 〔第１の観点による第２実施形態〕

第１の観点による第２実施形態では、第１の観点による第１実施形態と異なり、復号装置３０が第２属性情報または第２述語情報を生成する。この差異に伴い、第１の観点による第２実施形態は、いくつかの事項で第１の観点による第１実施形態と異なる。そこで、第１の観点による第１実施形態と重複する部分については重複説明を省略し（同一の構成要素に同じ参照番号を割り当てる）、図１８－図２１を参照しながら第１の観点による第１実施形態と異なる部分を説明する。

[0205] ステップＳ１からステップＳ２２ｂまでの処理は、第１の観点による第１実施形態と同じである。

[0206] ステップＳ２２ｂの処理で復号鍵を所有していない場合、復号装置３０の第２述語論理情報取得部３５が、メモリ３１からポリシーと、スキーマペアと、公開パラメータと、利用者情報を読み込み、利用者情報から、属性情報

（第２属性情報と言う）または述語情報（第２述語情報と言う）を得る（ステップＳ２３ｇ）。この処理において利用者情報に適用されるスキーマは、ポリシーで特定される一方のスキーマとペアになっている他方のスキーマである。ポリシーがCipher_Text_Policyである場合、Cipher_Text_Policyで特定される一方のスキーマ（述語用スキーマ）とペアになっている他方のスキーマ（属性用スキーマ）を用いて、利用者情報（属性指定情報）から第２属性情報を得る。ポリシーがKey_Policyである場合、Key_Policyで特定される一方のスキーマ（属性用スキーマ）とペアになっている他方のスキーマ（述語用スキーマ）を用いて、利用者情報（述語指定情報）から第２述語情報を得る。このように、この処理で用いられるスキーマは、ステップＳ１７ａで用いられたスキーマとペアになっているスキーマであることに注意しなければならない。第２属性情報と第２述語情報は、第１の観点による第２実施形態では、有限体F_qの元を成分とする一つ又は複数のベクトル情報とされる（図１１－１３参照）。

[0207] ステップＳ２３ｇの処理の後、ステップＳ２３の処理が行われる。ただし、この処理では、復号装置３０の送信部３４が、制御部による制御を受けて、メモリ３１からの公開パラメータ、ポリシー、スキーマペア、認証情報、第２属性情報または第２述語情報を纏めた鍵要求メッセージを生成する。そして、復号装置３０の送信部３４は、メモリ３１からのアドレスを持つ鍵生成装置に鍵要求メッセージを送信し、この鍵生成装置２０の受信部が、鍵要求メッセージを受信する。

[0208] そして、ステップＳ２４ａの処理で検証に成功した場合、ステップＳ２４ｄの処理が行われる。鍵生成装置２０は復号装置３０から第２属性情報または第２述語情報を受信しているため、第１の観点による第１実施形態と異なり、この情報を生成するための機能と処理が不要である。

[0209] そして、ステップＳ２４ｄの処理の後のステップＳ２８とステップＳ２９の各処理は、第１の観点による第１実施形態と同じである。

[0210] 〔第１の観点による第３実施形態〕

第１の観点による第３実施形態では、第１の観点による第１実施形態と異なり、暗号化装置１０の暗号化部１３が、第１属性情報ｖ＝(v_1，…，v_n)または第１述語情報ｗ＝(w_1，…，w_n)と、メモリ１１からの公開パラメータに含まれる公開鍵と平文Ｍを用いて、暗号情報C_1を求める。つまり、第１の観点による第３実施形態では、例えば上記非特許文献２に示す述語暗号アルゴリズムが用いられる。この差異に伴い、第１の観点による第３実施形態は、いくつかの事項で第１の観点による第１実施形態と異なる。そこで、第１の観点による第１実施形態と重複する部分については重複説明を省略し（同一の構成要素に同じ参照番号を割り当てる）、図２２－図２５を参照しながら第１の観点による第１実施形態と異なる部分を説明する。

[0211] ステップＳ１からステップＳ１７ａまでの処理は、第１の観点による第１実施形態と同じである。但し、公開パラメータなどの情報は第１の観点による第３実施形態の述語暗号アルゴリズムに必要な情報とされる。具体的な情報については、例えば上記非特許文献２などを参考されたい。

[0212] ステップＳ１７aの処理に続くステップＳ１７ｂ１の処理では、暗号化装置１０の暗号化部１３が、述語暗号アルゴリズムに則り、第１属性情報ｖ＝(v_1，…，v_n)または第１述語情報ｗ＝(w_1，…，w_n)と、メモリ１１からの公開パラメータに含まれる公開鍵と平文Ｍを用いて、暗号情報C_1を求める（ステップＳ１７ｂ１）。

[0213] 次に、ステップＳ１７ｂ１の処理の後、ステップＳ１７ｄの処理が行われる。但し、この処理では、暗号化装置１０の送信部１４が、制御部による制御を受けて、暗号情報C_1と、メモリ１１からのスキーマペア、ポリシー、公開パラメータ、鍵生成装置のアドレスを纏めた暗号メッセージを生成する（ステップＳ１７ｄ）。

[0214] ステップＳ１７ｄの処理に続くステップＳ１８からステップＳ２８までの処理は、第１の観点による第１実施形態と同じである。

[0215] ステップＳ２８の処理に続くステップＳ２２ｃ１の処理では、復号装置３０の復号部３３が、述語暗号アルゴリズムに則り、メモリ３１から公開パラ

メータと復号鍵Ｒと暗号情報C_1を読み込んで、平文Ｍを求める（ステップＳ２２ｃ１）。

[0216] 〔第１の観点による第４実施形態〕

第１の観点による第４実施形態は、第１の観点による第２実施形態と第１の観点による第３実施形態の組み合わせ形態に相当する。つまり、第１の観点による第４実施形態は、第１の観点による第１実施形態と異なり、（１）復号装置３０が第２属性情報または第２述語情報を生成する、（２）暗号化装置１０の暗号化部１３が、第１属性情報ｖ＝(v_1，…，v_n)または第１述語情報ｗ＝(w_1，…，w_n)と、メモリ１１からの公開パラメータに含まれる公開鍵と平文Ｍを用いて、暗号情報C_1を求める。この差異に伴い、第１の観点による第４実施形態は、いくつかの事項で第１の観点による第１実施形態と異なる。そこで、第１の観点による第１実施形態と重複する部分については重複説明を省略し（同一の構成要素に同じ参照番号を割り当てる）、図２６と図２７も参照して第１の観点による第１実施形態と異なる部分を説明する。

[0217] ステップＳ１からステップＳ１７ａまでの処理は、第１の観点による第１実施形態と同じである。但し、公開パラメータなどの情報は第１の観点による第４実施形態の述語暗号アルゴリズムに必要な情報とされる。具体的な情報については、例えば上記非特許文献２などを参考されたい。

[0218] ステップＳ１７aの処理に続くステップＳ１７ｂ１の処理では、暗号化装置１０の暗号化部１３が、述語暗号アルゴリズムに則り、第１属性情報ｖ＝(v_1，…，v_n)または第１述語情報ｗ＝(w_1，…，w_n)と、メモリ１１からの公開パラメータに含まれる公開鍵と平文Ｍを用いて、暗号情報C_1を求める（ステップＳ１７ｂ１）。

[0219] 次に、ステップＳ１７ｂ１の処理の後、ステップＳ１７ｄの処理が行われる。但し、この処理では、暗号化装置１０の送信部１４が、制御部による制御を受けて、暗号情報C_1と、メモリ１１からのスキーマペア、ポリシー、公開パラメータ、鍵生成装置のアドレスを纏めた暗号メッセージを生成する（ステップＳ１７ｄ）。

[0220] ステップＳ１７ｄの処理に続くステップＳ１８からステップＳ２２ｂの処理までは、第１の観点による第１実施形態と同じである。

[0221] ステップＳ２２ｂの処理で復号鍵を所有していない場合、復号装置３０の第２述語論理情報取得部３５が、メモリ３１からポリシーと、スキーマペアと、公開パラメータと、利用者情報を読み込み、利用者情報から、属性情報（第２属性情報と言う）または述語情報（第２述語情報と言う）を得る（ステップＳ２３ｇ）。この処理において利用者情報に適用されるスキーマは、ポリシーで特定される一方のスキーマとペアになっている他方のスキーマである。ポリシーがCipher_Text_Policyである場合、Cipher_Text_Policyで特定される一方のスキーマ（述語用スキーマ）とペアになっている他方のスキーマ（属性用スキーマ）を用いて、利用者情報（属性指定情報）から第２属性情報を得る。ポリシーがKey_Policyである場合、Key_Policyで特定される一方のスキーマ（属性用スキーマ）とペアになっている他方のスキーマ（述語用スキーマ）を用いて、利用者情報（述語指定情報）から第２述語情報を得る。このように、この処理で用いられるスキーマは、ステップＳ１７ａで用いられたスキーマとペアになっているスキーマであることに注意しなければならない。第２属性情報と第２述語情報は、第１の観点による第４実施形態では、有限体F_qの元を成分とする一つ又は複数のベクトル情報とされる（図１１－１３参照）。

[0222] ステップＳ２３ｇの処理の後、ステップＳ２３の処理が行われる。ただし、この処理では、復号装置３０の送信部３４が、制御部による制御を受けて、メモリ３１からの公開パラメータ、ポリシー、スキーマペア、認証情報、第２属性情報または第２述語情報を纏めた鍵要求メッセージを生成する。そして、復号装置３０の送信部３４は、メモリ３１からのアドレスを持つ鍵生成装置に鍵要求メッセージを送信し、この鍵生成装置２０の受信部が、鍵要求メッセージを受信する。

[0223] そして、ステップＳ２４ａの処理で検証に成功した場合、ステップＳ２４ｄの処理が行われる。鍵生成装置２０は、復号装置３０から第２属性情報ま

たは第２述語情報を受信しているため、この情報を生成するための機能と処理が不要である。

[0224] そして、ステップＳ２４ｄの処理の後のステップＳ２８の処理は、第１の観点による第１実施形態と同じである。

[0225] ステップＳ２８の処理に続くステップＳ２２ｃ１の処理では、復号装置３０の復号部３３が、述語暗号アルゴリズムに則り、メモリ３１から公開パラメータと復号鍵Ｒと暗号情報C_1を読み込んで、平文Ｍを求める（ステップＳ２２ｃ１）。

[0226] 次に、上述の第１の観点による暗号通信技術に留意しつつ、第２の観点から、柔軟に運用可能であって述語暗号で暗号化された暗号情報を流通させることが可能な、述語暗号に依拠する暗号通信技術に関する実施形態を説明する。この技術によると、復号装置が転送機能を持っているため、述語暗号で暗号化された暗号情報を流通させることができる。

[0227] 第２の観点による暗号通信技術の説明は上述の第１の観点による暗号通信技術の説明と実質的に重複する部分を多く含むが、第１の観点による暗号通信技術の説明を参照しなくてもよいように、できるだけ重複説明と重複図面を省略せずに第２の観点による暗号通信技術を説明する。このため、数式の番号、機能部を表す参照番号、ステップを表す参照番号なども両者で重複するが、文脈から混乱の虞は無いであろう。

[0228] 〔第２の観点による第１実施形態〕

図２８から図４１を参照して第２の観点による本発明の第１実施形態を説明する。

[0229] 第２の観点による暗号システム１は、図２８に示すように、複数のクライアント装置１０、３０－１、３０－２と、一つまたは複数の鍵生成装置２０と、一つまたは複数のユーザ情報管理装置４０（以下、管理装置と言う）、変換規則情報ペア管理装置５０（以下、登録装置と言う）、一つまたは複数の保全装置８０、一つまたは複数の認証装置９０を含んでいる。これらの各装置は、例えばインターネットである通信網５を介して相互に通信可能とさ

れている。

[0230] クライアント装置は、処理目的に応じて、暗号化装置として、あるいは復号装置として機能する。そこで、クライアント装置を機能の観点から、暗号化装置１０または復号装置と呼称する。復号装置は、後述する暗号メッセージの授受について暗号化装置１０との関係で当事者である第１の復号装置３０－１と、当事者ではない第２の復号装置３０－２に類別される。なお、第２の観点による暗号システム１は、暗号化装置としてのみ機能するクライアント装置および／または復号装置としてのみ機能するクライアント装置を含んでもよい。

[0231] 第２の観点による暗号システム１では述語暗号を用いた暗号化と復号が行われる。第２の観点による本発明では、使用する述語暗号アルゴリズムに限定は無く、例えば上記非特許文献２に開示される述語暗号アルゴリズムを用いることが許される。第２の観点による第１実施形態では、ＫＥＭ(Key Encapsulation Mechanisms)タイプの述語暗号アルゴリズムを用いた例を示す。

[0232] 第２の観点による暗号システム１における暗号通信方法を、図２９、３０、３１、３２、３４、３６、３８、４０、４１を参照しながら叙述する。各装置の機能構成については、図３３、３５、３７、３９を参照されたい。

[0233] 《準備プロセス》

第１の観点による発明の第１実施形態における《準備プロセス》の説明の全てをここに援用し、重複説明を省略する。なお、この《準備プロセス》の説明に対応する図として図２９を、スキーマペアについては図１１－１３を、ポリシーリストについては図１４を参照されたい。これで《準備プロセス》は終了する。

[0234] 《暗号化プロセス》

暗号化装置１０の送信部１４は、図示しない制御部の制御を受けて、検索クエリを登録装置５０に送信し、登録装置５０の受信部が検索クエリを受信する（ステップＳ１４）。登録装置５０の検索部は、登録装置５０の記憶部に登録されているエントリの一部または全部を検索して一つのエントリを選

び（ステップＳ１５）、登録装置５０の送信部は検索結果のエントリを暗号化装置１０に送信し、暗号化装置１０の受信部はエントリを受信する（ステップＳ１６）。このエントリには、鍵生成装置のアドレス、この鍵生成装置の公開パラメータ、この鍵生成装置が使用可能なポリシーリスト、この鍵生成装置が使用可能なスキーマリストが含まれている。受信したエントリは、暗号化装置１０のメモリ１１に記憶される。

[0235] なお、各鍵生成装置２０の公開パラメータ、スキーマリスト、ポリシーリスト、アドレスを予め暗号化装置１０が所有している場合には、ステップＳ１４－Ｓ１６の処理は省略される。つまり、暗号システム１が登録装置５０を含まない形態も許容されることに注意しなければならない。

[0236] 暗号化装置１０の第１述語論理情報取得部１２が、メモリ１１から入力情報とポリシーとスキーマを読み込み、属性情報（以下、第１属性情報と言う）または述語情報（以下、第１述語情報と言う）を求める（ステップＳ１７ａ）。この処理の詳細について説明を加える（図１２、図１３参照）。

[0237] まず、スキーマリストに複数のスキーマペアが記述されている場合、用途などに応じて一つのスキーマペアが選択される。暗号化装置１０の利用者によってスキーマペアが選択されてその指示情報が入力される場合や、所定の規則に従い、第１述語論理情報取得部１２がスキーマペアを選択してもよい。

[0238] そして、入力情報が属性指定情報または述語指定情報のいずれであるかに応じてポリシーと共にいずれか一方のスキーマを選択する。暗号化装置１０の利用者によってポリシーといずれか一方のスキーマが選択されてその指示情報が入力される場合や、所定の規則に従い、第１述語論理情報取得部１２がポリシーといずれか一方のスキーマを選択する場合のいずれであってもよい。なお、鍵生成装置２０のポリシーが１種類のタイプのみ用意されている場合には、そのポリシーに従ってスキーマペアのうちの一方のスキーマが選択される。もし、選択されたスキーマが入力情報の種類に対応していない場合には、スキーマリストからスキーマペアを再選択するか、登録装置５０か

らエントリの提供を再度受ければよい。

[0239] 入力情報は、暗号化装置１０の利用者によって入力された情報または、例えばＩＣカード３９のような記憶媒体から暗号化装置１０の取得部（図示せず）が取得した情報でもよい。

[0240] そして、第１述語論理情報取得部１２が、ポリシーに従ってスキーマペアの中から選択されたスキーマを用いて入力情報から第１属性情報または第１述語情報を得る。ポリシーがKey_Policyであり選択されたスキーマが属性用スキーマである場合には第１属性情報が得られる。ポリシーがCipher_Text_Policyであり選択されたスキーマが述語用スキーマである場合には第１述語情報が得られる。第１属性情報と第１述語情報は、第２の観点による第１実施形態では、有限体F_qの元を成分とする一つ又は複数のベクトル情報とされる（図１１－１３参照）。この際、スキーマを用いて入力情報から必要な属性値の抽出や整列化が行われる。

[0241] 次に、暗号化装置１０の暗号化部１３が、第１属性情報$v=(v_1, \cdots, v_n)$または第１述語情報$w=(w_1, \cdots, w_n)$と、メモリ１１からの公開パラメータに含まれる直交基底Ｂ（実質的な公開鍵）と平文Ｍを用いて、共通鍵Ｋと暗号情報C_1と暗号文C_2を求める（ステップＳ１７ｂ、Ｓ１７ｃ）。これらの処理の詳細について説明を加える。ただし、第２の観点による第１実施形態が共通鍵Ｋの配送に特化した実施形態である場合には暗号文C_2の生成は不要である。

[0242] まず、第１暗号化部１３ａが、述語暗号アルゴリズムに則り、有限体F_qの元である乱数ｒ、ρを生成して、上記式（７）のように共通鍵Ｋを設定し、上記式（８）に従って暗号情報C_1を求める（ステップＳ１７ｂ）。Ｈは例えばハッシュ関数である。この例では第１属性情報ｖを用いているが、第１述語情報を用いる場合は上記式（８）においてｖをｗに置き換えればよい。また、この例では、暗号情報C_1は共通鍵Ｋの生成に用いる情報ρに対応する情報であるが、暗号情報C_1を共通鍵Ｋに対応する情報としてもよい。

[0243] 次に、第２暗号化部１３ｂが、共通鍵Ｋと平文Ｍを用いて、上記式（９）

に従って暗号文C_2を求める（ステップＳ１７ｃ）。共通鍵を用いた暗号化方法Enc_Kは周知の方法でよく、例えば上記非特許文献１に開示される方法である。既述のとおり、第２の観点による第１実施形態が共通鍵Ｋの配送に特化した実施形態である場合には、ステップＳ１７ｃの処理は省略される。つまり、暗号化装置１０は、第２暗号化部１３ｂの機能を持つとしても、ステップＳ１７ｃの処理を行わない。

[0244] 次に、暗号化装置１０の送信部１４は、制御部による制御を受けて、暗号情報C_1と、（必要に応じて）暗号文C_2と、メモリ１１からのスキーマペア、ポリシー、公開パラメータ、鍵生成装置のアドレスを纏めた暗号メッセージを生成する（ステップＳ１７ｄ）。そして暗号化装置１０の送信部１４は、暗号メッセージを第１の復号装置３０－１に送信し、第１の復号装置３０－１の受信部が暗号メッセージを受信する（ステップＳ１８）。なお、暗号化装置１０が複数の第１の復号装置３０－１に対して暗号メッセージを送信することが許容される。

[0245] これで《暗号化プロセス》は終了する。

[0246] 《第１の復号プロセス》

第１の復号装置３０－１の送信部３４は、図示しない制御部の制御を受けて、暗号メッセージに含まれる鍵生成装置のアドレスを含む検索クエリを登録装置５０に送信し、登録装置５０の受信部が検索クエリを受信する（ステップＳ１９）。登録装置５０の検索部は、アドレスで指定された鍵生成装置のエントリを検索してそれを選び（ステップＳ２０）、登録装置５０の送信部は検索結果のエントリを第１の復号装置３０－１に送信し、第１の復号装置３０－１の受信部はエントリを受信する（ステップＳ２１）。このエントリには、鍵生成装置のアドレス、この鍵生成装置の公開パラメータ、この鍵生成装置が使用可能なポリシーリスト、この鍵生成装置が使用可能なスキーマリストが含まれている。受信したエントリは、第１の復号装置３０－１のメモリ３１に記憶される。

[0247] なお、各鍵生成装置２０の公開パラメータ、スキーマリスト、ポリシーリ

スト、アドレスを予め第１の復号装置３０－１が所有している場合には、ステップＳ１９－Ｓ２１の処理は省略される。この場合、第１の復号装置３０－１は、暗号メッセージに含まれるアドレスに対応する鍵生成装置のエントリを自身のメモリ３１から検索してこれを取得する。

[0248] 第１の復号装置３０－１の検証部（図示せず）は、制御部の制御を受けて、暗号メッセージに含まれるスキーマペアとポリシーが、登録装置５０から取得したエントリに含まれるポリシーリストとスキーマリストに含まれるか否かを検証する（ステップＳ２２ａ）。この検証に失敗した場合、復号処理の失敗として処理を終了する（ステップＳ２２ｇ）。

[0249] この検証に成功した場合、第１の復号装置３０－１の取得部３２が、例えばＩＣカード３９のような記憶媒体から、当該第１の復号装置３０－１の利用者に対応する属性指定情報または述語指定情報を読み取る（ステップＳ２２ｆ）。属性指定情報または述語指定情報のいずれを読み取るかは、暗号メッセージに含まれるポリシーによって決まる。つまり、読み取られる情報は、このポリシーで特定される一方のスキーマとペアになっている他方のスキーマを特定するポリシーの内容に対応する指定情報である。もしポリシーがCipher_Text_Policyである場合、取得部３２は記憶媒体から属性指定情報を読み取る。もしポリシーがKey_Policyである場合、取得部３２は記憶媒体から述語指定情報を読み取る。以下、読み取られた指定情報を利用者情報と呼ぶ。また、第１の復号装置３０－１の取得部３２が、後述する鍵生成装置２０における処理《利用者情報取得プロセス》と同様に、管理装置４０から、当該第１の復号装置３０－１の利用者に対応する属性指定情報または述語指定情報を読み取ることも許容される。なお、第２の観点による第１実施形態では、ステップＳ２２ｆの処理は任意に行われる。例えば、予め第１の復号装置３０－１が利用者に対応する属性指定情報と述語指定情報を所有している場合、ポリシーに従って属性指定情報または述語指定情報のいずれかが利用者情報となる。

[0250] 次に、第１の復号装置３０－１の検証部が、暗号メッセージに含まれる暗

号情報を復号するために使用する復号鍵を持っているか否かを検証する（ステップＳ２２ｂ）。

[0251] 第１の復号装置３０－１はメモリ３１に復号鍵テーブルを記憶している。復号鍵テーブルでは、例えば図１５に示すように、鍵生成装置の識別子に対して、公開パラメータと、スキーマペアと、復号鍵の対象と、述語指定情報と、復号鍵とが対応付けられている。そこで、検証部は、暗号メッセージに含まれるアドレスによって判別する鍵生成装置の識別子、公開パラメータと、スキーマペアと、復号鍵の対象（但し、これは、暗号メッセージに含まれるポリシーで特定される一方のスキーマとペアになっている他方のスキーマを特定するポリシーの内容に対応する）に対応する復号鍵の有無を検証する。もし復号鍵が存在すれば、ステップＳ２９の処理を行う。もし復号鍵が存在しなければ、ステップＳ２３の処理を行う。

[0252] ここで《復号プロセス》の説明を中断し、《鍵生成プロセス》の説明をする。

[0253] 上述のように復号鍵が存在しない場合、第１の復号装置３０－１の送信部３４は、制御部による制御を受けて、メモリ３１からの公開パラメータ、ポリシー、スキーマペア、（もし在れば）利用者情報、認証情報を纏めた鍵要求メッセージを生成する。認証情報は、例えば利用者のＩＤとパスワードを含む。そして、第１の復号装置３０－１の送信部３４は、メモリ３１からのアドレスを持つ鍵生成装置に鍵要求メッセージを送信し、この鍵生成装置２０の受信部が、鍵要求メッセージを受信する（ステップＳ２３）。受信した鍵要求メッセージは、鍵生成装置２０のメモリ２１に記憶される。

[0254] 鍵生成装置２０の検証部（図示せず）は、制御部の制御を受けて、鍵要求メッセージに含まれるスキーマペアとポリシーが、当該鍵生成装置２０が所有するエントリ（例えばステップＳ１で生成されたエントリである）に含まれるポリシーリストとスキーマリストに含まれるか否か、および、鍵要求メッセージに含まれる公開パラメータが当該鍵生成装置２０の公開パラメータであるか否かを検証する（ステップＳ２４ａ）。この検証に失敗した場合、

鍵生成処理の失敗として処理を終了する（ステップＳ２４ｇ）。なお、ステップＳ２４ａの処理では、鍵要求メッセージに認証情報が含まれるならば、鍵要求メッセージに含まれる認証情報の検証も行われる。鍵生成装置２０は、メモリ２１に認証テーブルを記憶している。認証テーブルでは、例えば図１６に示すように、利用者のＩＤに対してパスワードが対応付けられている。そこで、検証部は、鍵要求メッセージに含まれる利用者のＩＤとパスワードと認証テーブルに含まれる利用者のＩＤとパスワードとの整合性を検証する。この検証に失敗した場合も、ステップＳ２４ｇの処理が行われる。

[0255] この検証に成功した場合、鍵生成装置２０の検証部が、鍵要求メッセージに利用者情報が含まれているか否かを検証する（ステップＳ２４ｂ）。鍵要求メッセージに利用者情報が含まれていればステップＳ２４ｃの処理を行い、鍵要求メッセージに利用者情報が含まれていなければステップＳ２５の処理を行う。なお、必ず鍵要求メッセージに利用者情報が含まれる方法を採用する場合には、ステップＳ２４ｂの処理および後述する《利用者情報取得プロセス》は不要である。

[0256] ここで《鍵生成プロセス》の説明を中断し、《利用者情報取得プロセス》の説明をする。

[0257] 鍵生成装置２０の送信部は、鍵要求メッセージに含まれるポリシーと（もし在れば）認証情報を含むリクエストを管理装置４０に送信し、管理装置４０がリクエストを受信する（ステップＳ２５）。受信したリクエストは、管理装置４０のメモリに記憶される。

[0258] 管理装置４０はメモリに認証テーブルを記憶している。この認証テーブルでは、上述の認証テーブルと同様に、利用者のＩＤに対してパスワードが対応付けられている（図１６参照）。そこで、管理装置４０の検証部（図示せず）は、リクエストに含まれる利用者のＩＤとパスワードと認証テーブルに含まれる利用者のＩＤとパスワードとの整合性を検証する。

[0259] この検証に成功すると、管理装置４０の検索部（図示せず）がリクエストに含まれるポリシーに従って、メモリに記憶されている利用者情報テーブル

から属性指定情報または述語指定情報を検索する（ステップＳ２６）。利用者情報テーブルは、例えば利用者のＩＤとこれに対応付けられた属性名および属性指定情報で構成される第１テーブルと、利用者のＩＤとこれに対応付けられた述語指定情報で構成される第２テーブルとを含んでいる（図１７参照）。属性指定情報または述語指定情報のいずれを読み取るかは、リクエストに含まれるポリシーによって決まる。つまり、読み取られる情報は、このポリシーで特定される一方のスキーマとペアになっている他方のスキーマを特定するポリシーの内容に対応する指定情報である。もしポリシーがCipher_Text_Policyである場合、検索部は第１テーブルからリクエストに含まれる利用者のＩＤに対応する属性指定情報を取得する。もしポリシーがKey_Policyである場合、検索部は第２テーブルからリクエストに含まれる利用者のＩＤに対応する述語指定情報を取得する。読み取られた指定情報を利用者情報と呼ぶ。

[0260] 管理装置４０の送信部は、制御部による制御を受けて、検索結果の利用者情報を鍵生成装置２０に送信し、鍵生成装置２０の受信部が利用者情報を受信する（ステップＳ２７）。受信した利用者情報は、鍵生成装置２０のメモリ２１に記憶される。

[0261] 以上で《利用者情報取得プロセス》を終了し、再び《鍵生成プロセス》の説明に戻る。

[0262] 利用者情報を既に所有している場合、あるいは、利用者情報取得プロセスによって利用者情報を受信した場合（ステップＳ２７）、鍵生成装置２０の第２述語論理情報取得部２３は、メモリ２１からポリシーと、スキーマペアと、公開パラメータと、利用者情報を読み込み、利用者情報から、属性情報（第２属性情報と言う）または述語情報（第２述語情報と言う）を得る（ステップＳ２４ｃ）。この処理において利用者情報に適用されるスキーマは、ポリシーで特定される一方のスキーマとペアになっている他方のスキーマである。ポリシーがCipher_Text_Policyである場合、Cipher_Text_Policyで特定される一方のスキーマ（述語用スキーマ）とペアになっている他方のスキ

ーマ（属性用スキーマ）を用いて、利用者情報（属性指定情報）から第２属性情報を得る。ポリシーがKey_Policyである場合、Key_Policyで特定される一方のスキーマ（属性用スキーマ）とペアになっている他方のスキーマ（述語用スキーマ）を用いて、利用者情報（述語指定情報）から第２述語情報を得る。このように、この処理で用いられるスキーマは、ステップＳ１７ａで用いられたスキーマとペアになっているスキーマであることに注意しなければならない。第２属性情報と第２述語情報は、第２の観点による第１実施形態では、有限体F_qの元を成分とする一つ又は複数のベクトル情報とされる（図１１－１３参照）。この際、スキーマを用いて入力情報から必要な属性値の抽出や整列化が行われる。

[0263] 次に、鍵生成装置２０の鍵生成部２５が、述語暗号アルゴリズムに則り、公開パラメータのｑに基づき有限体F_qの元である乱数αを生成して、メモリ２１からの第２属性情報$v_{(p)}=(v_{(p)1}, \cdots, v_{(p)n})$または第２述語情報$w_{(p)}=(w_{(p)1}, \cdots, w_{(p)n})$と、当該鍵生成装置の秘密鍵Ｂ*を用いて、上記式（１０）に従って復号鍵Ｒを求める（ステップＳ２４ｄ）。暗号化処理で用いられた入力情報が属性指定情報である場合に対応して、この例では第２述語情報$w_{(p)}$を用いているが、入力情報が述語指定情報である場合には、第２属性情報$v_{(p)}$が対応するので、上記式（１０）において$w_{(p)}$を$v_{(p)}$に置き換えればよい。

[0264] 次に、鍵生成装置２０の送信部２４は、制御部による制御を受けて、復号鍵Ｒを第１の復号装置３０－１に送信し、第１の復号装置３０－１の受信部が復号鍵Ｒを受信する（ステップＳ２８）。受信した復号鍵Ｒは、第１の復号装置３０－１のメモリ３１に記憶される。

[0265] 以上で《鍵生成プロセス》を終了し、再び《復号プロセス》の説明に戻る。

[0266] 復号鍵を既に所有している場合、あるいは、鍵生成プロセスによって復号鍵を受信した場合（ステップＳ２８）、第１の復号装置３０－１の復号部３３が、メモリ３１から公開パラメータと復号鍵Ｒと暗号情報C_1と（必要に応じて）暗号文C_2を読み込んで、共通鍵Ｋと（必要に応じて）平文Ｍを求める

（ステップＳ２９）。

[0267] このステップＳ２９の処理の詳細について説明を加える。第１復号部３３ａは、メモリ３１から公開パラメータと暗号情報C_1と復号鍵Ｒを読み込み、述語暗号アルゴリズムに則り、ｅ(C_1, Ｒ)を求める。この演算結果は上記式（１１）に示すように、入力情報が属性指定情報である場合、双線形性に基づき暗号情報C_1と復号鍵Ｒから取り出された第１属性情報ｖと第２述語情報$w_{(p)}$の標準内積の結果に依存する。入力情報が述語指定情報である場合、上記式（１１）においてｖを$v_{(p)}$に、$w_{(p)}$をｗに置き換えればよく、演算結果は双線形性に基づき暗号情報C_1と復号鍵Ｒから取り出された第１述語情報ｗと第２属性情報$v_{(p)}$の標準内積の結果に依存する。但し、ｅ(b_i, b_i^*)は上記式（１２）のように定義される。δ_{ij}は、クロネッカーのデルタ記号である。

[0268] 従って、第１属性情報ｖと第２述語情報$w_{(p)}$の標準内積が０（あるいは第１述語情報ｗと第２属性情報$v_{(p)}$の標準内積が０）の場合、上記式（１１）の演算結果g_T^{ρ}が得られる。この演算結果g_T^{ρ}が得られた場合、第１の復号装置３０－１の第１復号部３３ａは、上記式（７）に従って“正しい”共通鍵Ｋを得る（ステップＳ２２ｃ）。もし第１属性情報ｖと第２述語情報$w_{(p)}$の標準内積が０（あるいは第１述語情報ｗと第２属性情報$v_{(p)}$の標準内積が０）ではない場合、第１復号部３３ａは、上記式（７）に従って“正しくない”値を得る。この例では、ハッシュ関数Ｈはシステムに共通とするか公開パラメータに含まれるとする。この例では、暗号情報C_1が共通鍵Ｋの生成に用いる情報ρに対応する情報であるが、暗号情報C_1を共通鍵Ｋに対応する情報とする場合には、上記式（１１）の演算結果が共通鍵Ｋ（あるいは正しくない値）となる。つまり、第１の復号装置３０－１の正当な利用者は、第１属性情報ｖとの標準内積が０となる第２述語情報$w_{(p)}$を与える述語指示情報、あるいは、第１述語情報ｗとの標準内積が０となる第２属性情報$v_{(p)}$を与える属性指示情報を持つ。

[0269] 次に、第２復号部３３ｂが、共通鍵Ｋと暗号文C_2を用いて、上記式（１３）に従って平文Ｍを求める（ステップＳ２２ｄ）。共通鍵を用いた復号方法D

ec_Kは暗号化方法Enc_Kに対応する。既述のとおり、第２の観点による第１実施形態が共通鍵Ｋの配送に特化した実施形態である場合には、ステップＳ２２ｄの処理は省略される。つまり、第１の復号装置３０－１は、第２復号部３３ｂの機能を持つとしても、ステップＳ２２ｄの処理を行わない。

[0270] もし、上記式（１１）に従った演算結果が正しくない値である場合には、上記式（１３）によっては正しい平文Ｍを得ることができない。

[0271] なお、第１の復号装置３０－１は、復号鍵Ｒを復号鍵テーブルに記憶してもよい。また、共通鍵Ｋを復号鍵テーブルに付加して記憶してもよい。

[0272] これで《第１の復号プロセス》は終了する。

[0273] 《転送プロセス》

第１の復号装置３０－１の転送部３７は、暗号化装置１０から受信した暗号メッセージを第２の復号装置３０－２に転送し、第２の復号装置３０－２の受信部が暗号メッセージを受信する（ステップ３０）。転送先の復号装置は、第２の復号装置（暗号メッセージの授受について暗号化装置と当事者の関係にない復号装置）に限らず、他の第１の復号装置（暗号メッセージの授受について暗号化装置と当事者の関係にある復号装置）であってもよい。また、ステップＳ３０の処理は、説明の都合、ステップＳ２９の処理に続く処理として説明するが、第１の復号装置３０－１が暗号化装置１０から暗号メッセージを受信した以降であれば何時でもよい。

[0274] これで《転送プロセス》は終了する。

[0275] 第２の復号装置３０－２による第２の復号プロセス（鍵生成プロセスと必要に応じて利用者情報取得プロセスを含む）について説明する。この一連の処理は、第１の復号プロセスと実質的に同じである。また、第２の復号装置３０－２の機能構成は、転送部３７を必ずしも持たなくてよいという点を除いて、第１の復号装置３０－１と同じであるから、共通する機能構成要素については同一の参照番号を割り当てている。

[0276] 《第２の復号プロセス》

第２の復号装置３０－２の送信部３４は、図示しない制御部の制御を受け

て、暗号メッセージに含まれる鍵生成装置のアドレスを含む検索クエリを登録装置５０に送信し、登録装置５０の受信部が検索クエリを受信する（ステップＳ３１）。登録装置５０の検索部は、アドレスで指定された鍵生成装置のエントリを検索してそれを選び（ステップＳ３２）、登録装置５０の送信部は検索結果のエントリを第２の復号装置３０－２に送信し、第２の復号装置３０－２の受信部はエントリを受信する（ステップＳ３３）。このエントリには、鍵生成装置のアドレス、この鍵生成装置の公開パラメータ、この鍵生成装置が使用可能なポリシーリスト、この鍵生成装置が使用可能なスキーマリストが含まれている。受信したエントリは、第２の復号装置３０－２のメモリ３１に記憶される。

[0277] なお、各鍵生成装置２０の公開パラメータ、スキーマリスト、ポリシーリスト、アドレスを予め第２の復号装置３０－２が所有している場合には、ステップＳ３１－Ｓ３３の処理は省略される。この場合、第２の復号装置３０－２は、暗号メッセージに含まれるアドレスに対応する鍵生成装置のエントリを自身のメモリ３１から検索してこれを取得する。

[0278] 第２の復号装置３０－２の検証部（図示せず）は、制御部の制御を受けて、暗号メッセージに含まれるスキーマペアとポリシーが、登録装置５０から取得したエントリに含まれるポリシーリストとスキーマリストに含まれるか否かを検証する（ステップＳ３４ａ）。この検証に失敗した場合、復号処理の失敗として処理を終了する（ステップＳ３４ｇ）。

[0279] この検証に成功した場合、第２の復号装置３０－２の取得部３２が、例えばＩＣカード３９のような記憶媒体から、当該第２の復号装置３０－２の利用者に対応する属性指定情報または述語指定情報を読み取る（ステップＳ３４ｆ）。属性指定情報または述語指定情報のいずれを読み取るかは、暗号メッセージに含まれるポリシーによって決まる。つまり、読み取られる情報は、このポリシーで特定される一方のスキーマとペアになっている他方のスキーマを特定するポリシーの内容に対応する指定情報である。もしポリシーがCipher_Text_Policyである場合、取得部３２は記憶媒体から属性指定情報を読

み取る。もしポリシーがKey_Policyである場合、取得部３２は記憶媒体から述語指定情報を読み取る。以下、読み取られた指定情報を利用者情報と呼ぶ。また、第２の復号装置３０－２の取得部３２が、後述する鍵生成装置２０における処理《利用者情報取得プロセス》と同様に、管理装置４０から、当該第２の復号装置３０－２の利用者に対応する属性指定情報または述語指定情報を読み取ることも許容される。なお、第２の観点による第１実施形態では、ステップＳ３４ｆの処理は任意に行われる。例えば、予め第２の復号装置３０－２が利用者に対応する属性指定情報と述語指定情報を所有している場合、ポリシーに従って属性指定情報または述語指定情報のいずれかが利用者情報となる。

[0280] 次に、第２の復号装置３０－２の検証部が、暗号メッセージに含まれる暗号情報を復号するために使用する復号鍵を持っているか否かを検証する（ステップＳ３４ｂ）。

[0281] 第２の復号装置３０－２はメモリ３１に復号鍵テーブルを記憶している。復号鍵テーブルでは、例えば図１５に示すように、鍵生成装置の識別子に対して、公開パラメータと、スキーマペアと、復号鍵の対象と、述語指定情報と、復号鍵とが対応付けられている。そこで、検証部は、暗号メッセージに含まれるアドレスによって判別する鍵生成装置の識別子、公開パラメータと、スキーマペアと、復号鍵の対象（但し、これは、暗号メッセージに含まれるポリシーで特定される一方のスキーマとペアになっている他方のスキーマを特定するポリシーの内容に対応する）に対応する復号鍵の有無を検証する。もし復号鍵が存在すれば、ステップＳ４１の処理を行う。もし復号鍵が存在しなければ、ステップＳ３５の処理を行う。

[0282] ここで《復号プロセス》の説明を中断し、《鍵生成プロセス》の説明をする。

[0283] 上述のように復号鍵が存在しない場合、第２の復号装置３０－２の送信部３４は、制御部による制御を受けて、メモリ３１からの公開パラメータ、ポリシー、スキーマペア、（もし在れば）利用者情報、認証情報を纏めた鍵要

求メッセージを生成する。認証情報は、例えば利用者のＩＤとパスワードを含む。そして、第２の復号装置３０－２の送信部３４は、メモリ３１からのアドレスを持つ鍵生成装置に鍵要求メッセージを送信し、この鍵生成装置２０の受信部が、鍵要求メッセージを受信する（ステップＳ３５）。受信した鍵要求メッセージは、鍵生成装置２０のメモリ２１に記憶される。この鍵生成装置２０は、第１の復号装置３０－１の相手方の鍵生成装置２０と同じである必要はない。

[0284] 鍵生成装置２０の検証部（図示せず）は、制御部の制御を受けて、鍵要求メッセージに含まれるスキーマペアとポリシーが、当該鍵生成装置２０が所有するエントリ（例えばステップＳ１で生成されたエントリである）に含まれるポリシーリストとスキーマリストに含まれるか否か、および、鍵要求メッセージに含まれる公開パラメータが当該鍵生成装置２０の公開パラメータであるか否かを検証する（ステップＳ３６ａ）。この検証に失敗した場合、鍵生成処理の失敗として処理を終了する（ステップＳ３６ｇ）。なお、ステップＳ３６ａの処理では、鍵要求メッセージに認証情報が含まれるならば、鍵要求メッセージに含まれる認証情報の検証も行われる。鍵生成装置２０は、メモリ２１に認証テーブルを記憶している。認証テーブルでは、例えば図１６に示すように、利用者のＩＤに対してパスワードが対応付けられている。そこで、検証部は、鍵要求メッセージに含まれる利用者のＩＤとパスワードと認証テーブルに含まれる利用者のＩＤとパスワードとの整合性を検証する。この検証に失敗した場合も、ステップＳ３６ｇの処理が行われる。

[0285] この検証に成功した場合、鍵生成装置２０の検証部が、鍵要求メッセージに利用者情報が含まれているか否かを検証する（ステップＳ３６ｂ）。鍵要求メッセージに利用者情報が含まれていればステップＳ３６ｃの処理を行い、鍵要求メッセージに利用者情報が含まれていなければステップＳ３７の処理を行う。なお、必ず鍵要求メッセージに利用者情報が含まれる方法を採用する場合には、ステップＳ３６ｂの処理および後述する《利用者情報取得プロセス》は不要である。

[0286] ここで《鍵生成プロセス》の説明を中断し、《利用者情報取得プロセス》の説明をする。

[0287] 鍵生成装置２０の送信部は、鍵要求メッセージに含まれるポリシーと（もし在れば）認証情報を含むリクエストを管理装置４０に送信し、管理装置４０がリクエストを受信する（ステップＳ３７）。受信したリクエストは、管理装置４０のメモリに記憶される。

[0288] 管理装置４０はメモリに認証テーブルを記憶している。この認証テーブルでは、上述の認証テーブルと同様に、利用者のＩＤに対してパスワードが対応付けられている（図１６参照）。そこで、管理装置４０の検証部（図示せず）は、リクエストに含まれる利用者のＩＤとパスワードと認証テーブルに含まれる利用者のＩＤとパスワードとの整合性を検証する。

[0289] この検証に成功すると、管理装置４０の検索部（図示せず）がリクエストに含まれるポリシーに従って、メモリに記憶されている利用者情報テーブルから属性指定情報または述語指定情報を検索する（ステップＳ３８）。利用者情報テーブルは、例えば利用者のＩＤとこれに対応付けられた属性名および属性指定情報で構成される第１テーブルと、利用者のＩＤとこれに対応付けられた述語指定情報で構成される第２テーブルとを含んでいる（図１７参照）。属性指定情報または述語指定情報のいずれを読み取るかは、リクエストに含まれるポリシーによって決まる。つまり、読み取られる情報は、このポリシーで特定される一方のスキーマとペアになっている他方のスキーマを特定するポリシーの内容に対応する指定情報である。もしポリシーがCipher_Text_Policyである場合、検索部は第１テーブルからリクエストに含まれる利用者のＩＤに対応する属性指定情報を取得する。もしポリシーがKey_Policyである場合、検索部は第２テーブルからリクエストに含まれる利用者のＩＤに対応する述語指定情報を取得する。読み取られた指定情報を利用者情報と呼ぶ。

[0290] 管理装置４０の送信部は、制御部による制御を受けて、検索結果の利用者情報を鍵生成装置２０に送信し、鍵生成装置２０の受信部が利用者情報を受

信する（ステップＳ３９）。受信した利用者情報は、鍵生成装置２０のメモリ２１に記憶される。

[0291] 以上で《利用者情報取得プロセス》を終了し、再び《鍵生成プロセス》の説明に戻る。

[0292] 利用者情報を既に所有している場合、あるいは、利用者情報取得プロセスによって利用者情報を受信した場合（ステップＳ３９）、鍵生成装置２０の第２述語論理情報取得部２３は、メモリ２１からポリシーと、スキーマペアと、公開パラメータと、利用者情報を読み込み、利用者情報から、属性情報（第２属性情報と言う）または述語情報（第２述語情報と言う）を得る（ステップＳ３６ｃ）。一般的に、第１の復号装置３０－１の利用者と第２の復号装置３０－２の利用者は異なるので、この処理で得られる第２属性情報または第２述語情報は、ステップＳ２４ｃの処理で得られる第２属性情報または第２述語情報と同じになる保証はない。この処理において利用者情報に適用されるスキーマは、ポリシーで特定される一方のスキーマとペアになっている他方のスキーマである。ポリシーがCipher_Text_Policyである場合、Cipher_Text_Policyで特定される一方のスキーマ（述語用スキーマ）とペアになっている他方のスキーマ（属性用スキーマ）を用いて、利用者情報（属性指定情報）から第２属性情報を得る。ポリシーがKey_Policyである場合、Key_Policyで特定される一方のスキーマ（属性用スキーマ）とペアになっている他方のスキーマ（述語用スキーマ）を用いて、利用者情報（述語指定情報）から第２述語情報を得る。このように、この処理で用いられるスキーマは、ステップＳ１７ａで用いられたスキーマとペアになっているスキーマであることに注意しなければならない。第２属性情報と第２述語情報は、第２の観点による第１実施形態では、有限体F_qの元を成分とする一つ又は複数のベクトル情報とされる（図１１－１３参照）。この際、スキーマを用いて入力情報から必要な属性値の抽出や整列化が行われる。

[0293] 次に、鍵生成装置２０の鍵生成部２５が、述語暗号アルゴリズムに則り、公開パラメータのｑに基づき有限体F_qの元である乱数εを生成して、メモリ

２１からの第２属性情報ｖ’$_{(p)}$＝（ｖ’$_{(p)1}$，…，ｖ’$_{(p)n}$）または第２述語情報ｗ’$_{(p)}$＝（ｗ’$_{(p)1}$，…，ｗ’$_{(p)n}$）と、当該鍵生成装置の秘密鍵Ｂ＊を用いて、式（１４）に従って復号鍵Ｒ’を求める（ステップＳ３６ｄ）。暗号化処理で用いられた入力情報が属性指定情報である場合に対応して、この例では第２述語情報ｗ’$_{(p)}$を用いているが、入力情報が述語指定情報である場合には、第２属性情報ｖ’$_{(p)}$が対応するので、式（１４）においてｗ’$_{(p)}$をｖ’$_{(p)}$に置き換えればよい。

[数42]

$$R' = \varepsilon \sum_{i=1}^{n} w'_{(p)i} b_i^* + b_{n+1}^* \qquad (14)$$

[0294] 次に、鍵生成装置２０の送信部２４は、制御部による制御を受けて、復号鍵Ｒ’を第２の復号装置３０－２に送信し、第２の復号装置３０－２の受信部が復号鍵Ｒを受信する（ステップＳ４０）。受信した復号鍵Ｒは、第２の復号装置３０－２のメモリ３１に記憶される。

[0295] 以上で《鍵生成プロセス》を終了し、再び《復号プロセス》の説明に戻る。

[0296] 復号鍵を既に所有している場合、あるいは、鍵生成プロセスによって復号鍵を受信した場合（ステップＳ４０）、第２の復号装置３０－２の復号部３３が、メモリ３１から公開パラメータと復号鍵Ｒ’と暗号情報C_1と（必要に応じて）暗号文C_2を読み込んで、共通鍵Ｋと（必要に応じて）平文Ｍを求める（ステップＳ４１）。

[0297] このステップＳ４１の処理の詳細について説明を加える。第１復号部３３ａは、メモリ３１から公開パラメータと暗号情報C_1と復号鍵Ｒ’を読み込み、述語暗号アルゴリズムに則り、ｅ（C_1，Ｒ’）を求める。この演算結果は式（１５）に示すように、入力情報が属性指定情報である場合、双線形性に基づき暗号情報C_1と復号鍵Ｒ’から取り出された第１属性情報ｖと第２述語情報ｗ’$_{(p)}$の標準内積の結果に依存する。入力情報が述語指定情報である場合、式（１５）においてｖをｖ’$_{(p)}$に、ｗ’$_{(p)}$をｗに置き換えればよく、演算結果は双線形

性に基づき暗号情報C_1と復号鍵R'から取り出された第１述語情報ｗと第２属性情報$v'_{(\rho)}$の標準内積の結果に依存する。但し、$e(b_i, b_i^*)$は上記式（１２）のように定義される。

[数43]

$$e(C_1,R') = e(r\sum_{i=1}^{n} v_i b_i, R')\cdot e(\rho b_{n+1}, R')$$
$$= \prod_{i=1}^{n} e(b_i, b_i^*)^{r\alpha v_i w'_{(\rho)i}} \cdot e(b_{n+1}, b_{n+1}^*)^{\rho}$$
$$= g_T{}^{r\alpha \sum_{i=1}^{n} v_i w'_{(\rho)i}} \cdot g_T{}^{\rho}$$
$$= g_T{}^{r\alpha v\cdot w'_{(\rho)}} \cdot g_T{}^{\rho} \qquad (15)$$

[0298] 従って、第１属性情報ｖと第２述語情報$w'_{(\rho)}$の標準内積が０（あるいは第１述語情報ｗと第２属性情報$v'_{(\rho)}$の標準内積が０）の場合、式（１５）の演算結果$g_T{}^{\rho}$が得られる。この演算結果$g_T{}^{\rho}$が得られた場合、第２の復号装置３０－２の第１復号部３３ａは、上記式（７）に従って“正しい”共通鍵Ｋを得る（ステップＳ３４ｃ）。もし第１属性情報ｖと第２述語情報$w'_{(\rho)}$の標準内積が０（あるいは第１述語情報ｗと第２属性情報$v'_{(\rho)}$の標準内積が０）ではない場合、第１復号部３３ａは、上記式（７）に従って“正しくない”値を得る。この例では、ハッシュ関数Ｈはシステムに共通とするか公開パラメータに含まれるとする。この例では、暗号情報C_1が共通鍵Ｋの生成に用いる情報ρに対応する情報であるが、暗号情報C_1を共通鍵Ｋに対応する情報とする場合には、式（１５）の演算結果が共通鍵Ｋ（あるいは正しくない値）となる。つまり、第２の復号装置３０－２の正当な利用者は、第１属性情報ｖとの標準内積が０となる第２述語情報$w'_{(\rho)}$を与える述語指示情報、あるいは、第１述語情報ｗとの標準内積が０となる第２属性情報$v'_{(\rho)}$を与える属性指示情報を持つ。

[0299] 次に、第２復号部３３ｂが、共通鍵Ｋと暗号文C_2を用いて、上記式（１３）に従って平文Ｍを求める（ステップＳ３４ｄ）。共通鍵を用いた復号方法Dec_Kは暗号化方法Enc_Kに対応する。既述のとおり、第２の観点による第１実施

形態が共通鍵Ｋの配送に特化した実施形態である場合には、ステップＳ３４ｄの処理は省略される。つまり、第２の復号装置３０－２は、第２復号部３３ｂの機能を持つとしても、ステップＳ３４ｄの処理を行わない。

[0300] もし、式（１５）に従った演算結果が正しくない値である場合には、上記式（１３）によっては正しい平文Ｍを得ることができない。

[0301] なお、第２の復号装置３０－２は、復号鍵Ｒを復号鍵テーブルに記憶してもよい。また、共通鍵Ｋを復号鍵テーブルに付加して記憶してもよい。

[0302] これで《第２の復号プロセス》は終了する。

[0303] 第２の復号装置３０－２が転送部３７を持つ場合には、第２の復号装置３０－２は、第１の復号装置３０－１から受信した暗号メッセージを別の第２の復号装置（暗号メッセージの授受について暗号化装置と当事者の関係にない復号装置）に転送してもよいし、第１の復号装置（暗号メッセージの授受について暗号化装置と当事者の関係にある復号装置）に転送してもよい。この転送処理は、第２の復号装置３０－２が第１の復号装置３０－１から暗号メッセージを受信した以降であれば何時でもよい。

[0304] 〔第２の観点による第２実施形態〕

第２の観点による第２実施形態では、第２の観点による第１実施形態と異なり、第１の復号装置３０－１と第２の復号装置３０－２が第２属性情報または第２述語情報を生成する。この差異に伴い、第２の観点による第２実施形態は、いくつかの事項で第２の観点による第１実施形態と異なる。そこで、第２の観点による第１実施形態と重複する部分については重複説明を省略し（同一の構成要素に同じ参照番号を割り当てる）、図４２－図４８を参照しながら第１実施形態と異なる部分を説明する。

[0305] ステップＳ１からステップＳ２２ｂまでの処理は、第２の観点による第１実施形態と同じである。

[0306] ステップＳ２２ｂの処理で復号鍵を所有していない場合、第１の復号装置３０－１の第２述語論理情報取得部３５が、メモリ３１からポリシーと、スキーマペアと、公開パラメータと、利用者情報を読み込み、利用者情報から

、属性情報（第２属性情報と言う）または述語情報（第２述語情報と言う）を得る（ステップＳ２３ｇ）。この処理において利用者情報に適用されるスキーマは、ポリシーで特定される一方のスキーマとペアになっている他方のスキーマである。ポリシーがCipher_Text_Policyである場合、Cipher_Text_Policyで特定される一方のスキーマ（述語用スキーマ）とペアになっている他方のスキーマ（属性用スキーマ）を用いて、利用者情報（属性指定情報）から第２属性情報を得る。ポリシーがKey_Policyである場合、Key_Policyで特定される一方のスキーマ（属性用スキーマ）とペアになっている他方のスキーマ（述語用スキーマ）を用いて、利用者情報（述語指定情報）から第２述語情報を得る。このように、この処理で用いられるスキーマは、ステップＳ１７ａで用いられたスキーマとペアになっているスキーマであることに注意しなければならない。第２属性情報と第２述語情報は、第２の観点による第２実施形態では、有限体F_qの元を成分とする一つ又は複数のベクトル情報とされる（図１１－１３参照）。

[0307] ステップＳ２３ｇの処理の後、ステップＳ２３の処理が行われる。ただし、この処理では、第１の復号装置３０－１の送信部３４が、制御部による制御を受けて、メモリ３１からの公開パラメータ、ポリシー、スキーマペア、認証情報、第２属性情報または第２述語情報を纏めた鍵要求メッセージを生成する。そして、第１の復号装置３０－１の送信部３４は、メモリ３１からのアドレスを持つ鍵生成装置に鍵要求メッセージを送信し、この鍵生成装置２０の受信部が、鍵要求メッセージを受信する。

[0308] そして、ステップＳ２４ａの処理で検証に成功した場合、ステップＳ２４ｄの処理が行われる。鍵生成装置２０は第１の復号装置３０－１から第２属性情報または第２述語情報を受信しているため、第２の観点による第１実施形態と異なり、この情報を生成するための機能と処理が不要である。

[0309] そして、ステップＳ２４ｄの処理の後のステップＳ２８からステップＳ３４ａまでの各処理は、第２の観点による第１実施形態と同じである。

[0310] ステップＳ３４ｂの処理で復号鍵を所有していない場合、第２の復号装置

３０－２の第２述語論理情報取得部３５が、メモリ３１からポリシーと、スキーマペアと、公開パラメータと、利用者情報を読み込み、利用者情報から、属性情報（第２属性情報と言う）または述語情報（第２述語情報と言う）を得る（ステップＳ３５ｇ）。この処理において利用者情報に適用されるスキーマは、ポリシーで特定される一方のスキーマとペアになっている他方のスキーマである。ポリシーがCipher_Text_Policyである場合、Cipher_Text_Policyで特定される一方のスキーマ（述語用スキーマ）とペアになっている他方のスキーマ（属性用スキーマ）を用いて、利用者情報（属性指定情報）から第２属性情報を得る。ポリシーがKey_Policyである場合、Key_Policyで特定される一方のスキーマ（属性用スキーマ）とペアになっている他方のスキーマ（述語用スキーマ）を用いて、利用者情報（述語指定情報）から第２述語情報を得る。このように、この処理で用いられるスキーマは、ステップＳ１７ａで用いられたスキーマとペアになっているスキーマであることに注意しなければならない。第２属性情報と第２述語情報は、第２の観点による第２実施形態では、有限体F_qの元を成分とする一つ又は複数のベクトル情報とされる（図１１－１３参照）。

[0311] ステップＳ３５ｇの処理の後、ステップＳ３５の処理が行われる。ただし、この処理では、第２の復号装置３０－２の送信部３４が、制御部による制御を受けて、メモリ３１からの公開パラメータ、ポリシー、スキーマペア、認証情報、第２属性情報または第２述語情報を纏めた鍵要求メッセージを生成する。そして、第２の復号装置３０－２の送信部３４は、メモリ３１からのアドレスを持つ鍵生成装置に鍵要求メッセージを送信し、この鍵生成装置２０の受信部が、鍵要求メッセージを受信する。

[0312] そして、ステップＳ３６ａの処理で検証に成功した場合、ステップＳ３６ｄの処理が行われる。鍵生成装置２０は第２の復号装置３０－２から第２属性情報または第２述語情報を受信しているため、第２の観点による第１実施形態と異なり、この情報を生成するための機能と処理が不要である。

[0313] そして、ステップＳ３６ｄの処理の後のステップＳ４０とステップＳ４１

の各処理は、第２の観点による第１実施形態と同じである。

[0314] 〔第２の観点による第３実施形態〕

第２の観点による第３実施形態では、第２の観点による第１実施形態と異なり、暗号化装置１０の暗号化部１３が、第１属性情報ｖ＝(v_1，…，v_n)または第１述語情報ｗ＝(w_1，…，w_n)と、メモリ１１からの公開パラメータに含まれる公開鍵と平文Ｍを用いて、暗号情報C_1を求める。つまり、第２の観点による第３実施形態では、例えば上記非特許文献２に示す述語暗号アルゴリズムが用いられる。この差異に伴い、第２の観点による第３実施形態は、いくつかの事項で第２の観点による第１実施形態と異なる。そこで、第２の観点による第１実施形態と重複する部分については重複説明を省略し（同一の構成要素に同じ参照番号を割り当てる）、図４９－図５４を参照しながら第２の観点による第１実施形態と異なる部分を説明する。

[0315] ステップＳ１からステップＳ１７ａまでの処理は、第２の観点による第１実施形態と同じである。但し、公開パラメータなどの情報は第２の観点による第３実施形態の述語暗号アルゴリズムに必要な情報とされる。具体的な情報については、例えば上記非特許文献２などを参考されたい。

[0316] ステップＳ１７aの処理に続くステップＳ１７ｂ１の処理では、暗号化装置１０の暗号化部１３が、述語暗号アルゴリズムに則り、第１属性情報ｖ＝(v_1，…，v_n)または第１述語情報ｗ＝(w_1，…，w_n)と、メモリ１１からの公開パラメータに含まれる公開鍵と平文Ｍを用いて、暗号情報C_1を求める（ステップＳ１７ｂ１）。

[0317] 次に、ステップＳ１７ｂ１の処理の後、ステップＳ１７ｄの処理が行われる。但し、この処理では、暗号化装置１０の送信部１４が、制御部による制御を受けて、暗号情報C_1と、メモリ１１からのスキーマペア、ポリシー、公開パラメータ、鍵生成装置のアドレスを纏めた暗号メッセージを生成する（ステップＳ１７ｄ）。

[0318] ステップＳ１７ｄの処理に続くステップＳ１８からステップＳ２８までの処理は、第２の観点による第１実施形態と同じである。

[0319] ステップＳ２８の処理に続くステップＳ２２ｃ１の処理では、第１の復号装置３０－１の復号部３３が、述語暗号アルゴリズムに則り、メモリ３１から公開パラメータと復号鍵Ｒと暗号情報C_1を読み込んで、平文Ｍを求める（ステップＳ２２ｃ１）。

[0320] ステップＳ２２ｃ１の処理に続くステップＳ３０からステップＳ４０までの処理は、第２の観点による第１実施形態と同じである。

[0321] ステップＳ４０の処理に続くステップＳ３４ｃ１の処理では、第２の復号装置３０－２の復号部３３が、述語暗号アルゴリズムに則り、メモリ３１から公開パラメータと復号鍵Ｒと暗号情報C_1を読み込んで、平文Ｍを求める（ステップＳ３４ｃ１）。

[0322] 〔第２の観点による第４実施形態〕

第２の観点による第４実施形態は、第２の観点による第２実施形態と第２の観点による第３実施形態の組み合わせ形態に相当する。つまり、第２の観点による第４実施形態は、第２の観点による第１実施形態と異なり、（１）第１の復号装置３０－１と第２の復号装置３０－２が第２属性情報または第２述語情報を生成する、（２）暗号化装置１０の暗号化部１３が、第１属性情報$v=(v_1, \cdots, v_n)$または第１述語情報$w=(w_1, \cdots, w_n)$と、メモリ１１からの公開パラメータに含まれる公開鍵と平文Ｍを用いて、暗号情報C_1を求める。この差異に伴い、第２の観点による第４実施形態は、いくつかの事項で第２の観点による第１実施形態と異なる。そこで、第２の観点による第１実施形態と重複する部分については重複説明を省略し（同一の構成要素に同じ参照番号を割り当てる）、図５５から図５８も参照して第１実施形態と異なる部分を説明する。

[0323] ステップＳ１からステップＳ１７ａまでの処理は、第２の観点による第１実施形態と同じである。但し、公開パラメータなどの情報は第２の観点による第４実施形態の述語暗号アルゴリズムに必要な情報とされる。具体的な情報については、例えば上記非特許文献２などを参考されたい。

[0324] ステップＳ１７aの処理に続くステップＳ１７ｂ１の処理では、暗号化装置

１０の暗号化部１３が、述語暗号アルゴリズムに則り、第１属性情報ｖ＝(v_1, …, v_n)または第１述語情報ｗ＝(w_1, …, w_n)と、メモリ１１からの公開パラメータに含まれる公開鍵と平文Ｍを用いて、暗号情報C_1を求める（ステップＳ１７ｂ１）。

[0325] 次に、ステップＳ１７ｂ１の処理の後、ステップＳ１７ｄの処理が行われる。但し、この処理では、暗号化装置１０の送信部１４が、制御部による制御を受けて、暗号情報C_1と、メモリ１１からのスキーマペア、ポリシー、公開パラメータ、鍵生成装置のアドレスを纏めた暗号メッセージを生成する（ステップＳ１７ｄ）。

[0326] ステップＳ１７ｄの処理に続くステップＳ１８からステップＳ２２ｂの処理までは、第２の観点による第１実施形態と同じである。

[0327] ステップＳ２２ｂの処理で復号鍵を所有していない場合、第１の復号装置３０－１の第２述語論理情報取得部３５が、メモリ３１からポリシーと、スキーマペアと、公開パラメータと、利用者情報を読み込み、利用者情報から、属性情報（第２属性情報と言う）または述語情報（第２述語情報と言う）を得る（ステップＳ２３ｇ）。この処理において利用者情報に適用されるスキーマは、ポリシーで特定される一方のスキーマとペアになっている他方のスキーマである。ポリシーがCipher_Text_Policyである場合、Cipher_Text_Policyで特定される一方のスキーマ（述語用スキーマ）とペアになっている他方のスキーマ（属性用スキーマ）を用いて、利用者情報（属性指定情報）から第２属性情報を得る。ポリシーがKey_Policyである場合、Key_Policyで特定される一方のスキーマ（属性用スキーマ）とペアになっている他方のスキーマ（述語用スキーマ）を用いて、利用者情報（述語指定情報）から第２述語情報を得る。このように、この処理で用いられるスキーマは、ステップＳ１７ａで用いられたスキーマとペアになっているスキーマであることに注意しなければならない。第２属性情報と第２述語情報は、第２の観点による第４実施形態では、有限体F_qの元を成分とする一つ又は複数のベクトル情報とされる（図１１－１３参照）。

[0328] ステップＳ２３ｇの処理の後、ステップＳ２３の処理が行われる。ただし、この処理では、第１の復号装置３０－１の送信部３４が、制御部による制御を受けて、メモリ３１からの公開パラメータ、ポリシー、スキーマペア、認証情報、第２属性情報または第２述語情報を纏めた鍵要求メッセージを生成する。そして、第１の復号装置３０－１の送信部３４は、メモリ３１からのアドレスを持つ鍵生成装置に鍵要求メッセージを送信し、この鍵生成装置２０の受信部が、鍵要求メッセージを受信する。

[0329] そして、ステップＳ２４ａの処理で検証に成功した場合、ステップＳ２４ｄの処理が行われる。鍵生成装置２０は、第１の復号装置３０－１から第２属性情報または第２述語情報を受信しているため、この情報を生成するための機能と処理が不要である。

[0330] そして、ステップＳ２４ｄの処理の後のステップＳ２８の処理は、第２の観点による第１実施形態と同じである。

[0331] ステップＳ２８の処理に続くステップＳ２２ｃ１の処理では、第１の復号装置３０－１の復号部３３が、述語暗号アルゴリズムに則り、メモリ３１から公開パラメータと復号鍵Ｒと暗号情報C_1を読み込んで、平文Ｍを求める（ステップＳ２２ｃ１）。

[0332] そして、ステップＳ２２ｃ１の処理の後のステップＳ３０からステップＳ３４ａまでの各処理は、第２の観点による第１実施形態と同じである。

[0333] ステップＳ３４ｂの処理で復号鍵を所有していない場合、第２の復号装置３０－２の第２述語論理情報取得部３５が、メモリ３１からポリシーと、スキーマペアと、公開パラメータと、利用者情報を読み込み、利用者情報から、属性情報（第２属性情報と言う）または述語情報（第２述語情報と言う）を得る（ステップＳ３５ｇ）。この処理において利用者情報に適用されるスキーマは、ポリシーで特定される一方のスキーマとペアになっている他方のスキーマである。ポリシーがCipher_Text_Policyである場合、Cipher_Text_Policyで特定される一方のスキーマ（述語用スキーマ）とペアになっている他方のスキーマ（属性用スキーマ）を用いて、利用者情報（属性指定情報）か

ら第２属性情報を得る。ポリシーがKey_Policyである場合、Key_Policyで特定される一方のスキーマ（属性用スキーマ）とペアになっている他方のスキーマ（述語用スキーマ）を用いて、利用者情報（述語指定情報）から第２述語情報を得る。このように、この処理で用いられるスキーマは、ステップＳ１７ａで用いられたスキーマとペアになっているスキーマであることに注意しなければならない。第２属性情報と第２述語情報は、第２の観点による第４実施形態では、有限体F_qの元を成分とする一つ又は複数のベクトル情報とされる（図１１－１３参照）。

[0334] ステップＳ３５ｇの処理の後、ステップＳ３５の処理が行われる。ただし、この処理では、第２の復号装置３０－２の送信部３４が、制御部による制御を受けて、メモリ３１からの公開パラメータ、ポリシー、スキーマペア、認証情報、第２属性情報または第２述語情報を纏めた鍵要求メッセージを生成する。そして、第２の復号装置３０－２の送信部３４は、メモリ３１からのアドレスを持つ鍵生成装置に鍵要求メッセージを送信し、この鍵生成装置２０の受信部が、鍵要求メッセージを受信する。

[0335] そして、ステップＳ３６ａの処理で検証に成功した場合、ステップＳ３６ｄの処理が行われる。鍵生成装置２０は第２の復号装置３０－２から第２属性情報または第２述語情報を受信しているため、第１実施形態と異なり、この情報を生成するための機能と処理が不要である。

[0336] そして、ステップＳ３６ｄの処理の後のステップＳ４０の処理は、第２の観点による第１実施形態と同じである。

[0337] ステップＳ４０の処理に続くステップＳ３４ｃ１の処理では、第２の復号装置３０－２の復号部３３が、述語暗号アルゴリズムに則り、メモリ３１から公開パラメータと復号鍵Ｒと暗号情報C_1を読み込んで、平文Ｍを求める（ステップＳ３４ｃ１）。

[0338] 第２の観点による上述の各実施形態は、例えば電子メールシステムやインスタントメッセージングシステムとして実施される。図５９に、送受信されるデータの構成を例示する。メッセージ全体の基本的なフォーマットは例え

ばＳ／ＭＩＭＥ（Secure Multipurpose Internet Mail Extensions）に従うが、暗号メッセージ開始位置マーカから暗号メッセージ終了位置マーカまでのデータはＸＭＬ（eXtensible Markup Language）などで適切なデータ構成が与えられる。

[0339] 暗号メッセージ開始位置マーカから暗号メッセージ終了位置マーカまでが述語暗号に関する一連のデータを示す。

[0340] アルゴリズム識別子ブロックには、共通鍵の暗号化に使用した述語暗号アルゴリズムとメッセージペイロードの暗号化に使用した共通鍵暗号アルゴリズムを特定するための情報が指定される。このように、アルゴリズムを表す識別子やアルゴリズムのバージョンなどを指定できる（PE/VersionX+Camellia［Camelliaは登録商標］など）。

[0341] デジタル署名ブロックにはデジタル署名が記述される。署名アルゴリズムは既存の方式を使用できる。この項目は運用形態に応じて省略可能である。

[0342] 公開パラメータ情報ブロックには、使用した公開情報パラメータを特定する情報が指定される。公開情報パラメータを特定する識別子、もしくは公開情報パラメータのデータそのものを指定することもできる。

[0343] ポリシーフィールドには、使用したポリシーを特定する識別子が指定される。

[0344] スキーマフィールドには、使用したスキーマを特定する識別子が指定されるか、もしくはスキーマのデータが記述される。

[0345] 暗号情報フィールドにはメッセージペイロード（平文）の暗号化に使用した共通鍵を述語暗号で暗号化したデータ（暗号情報）が指定される。

[0346] 暗号文フィールドにはメッセージペイロード（平文）を暗号化して作成したデータ（暗号文）が記述される。

[0347] 属性フィールド／述語フィールドにはポリシーフィールドに対応して暗号化に使用した属性／述語を表す文字列表現を指定することができる。これらの項目は運用形態に応じては省略可能である。

[0348] 添付フィールドには例えばＲＳＡ暗号化した添付ファイルなどを添付する

ことができる。この項目は運用形態に応じて省略可能である。

[0349] また、例えばインストタントメッセージングに伴うセキュアな通信の場合には、共通鍵を暗号化した暗号情報を再送する必要はない。インスタントメッセージングでは通常、最初のインスタントメッセージで適切な共通鍵を取得できたならば、後続のインスタントメッセージの復号に用いるために共通鍵を受信者が保存しておいてもよい。このように後続のインスタントメッセージを送信者から受信者に送信する際には、暗号文は送るが、公開パラメータ情報、ポリシー、スキーマ、暗号情報を送らないようにしてもよい。同様に、使用される暗号アルゴリズムを変更しない運用の場合には、後続のインスタントメッセージ内の暗号アルゴリズム識別子を省略してもよい。

[0350] 述語暗号は、暗号化に際して、受信者に依存する情報に拘束されない方式であるから、送信者（装置）は、未知の受信者（装置）に対しても暗号メッセージを送信することができる。換言すると、送信者は、複数の受信者（装置）が存在する場合であっても暗号化処理を１回しか行わない（公開鍵暗号方式では、Ｎ回の暗号化処理が必要である）。このため、送信者（装置）は、低い処理コストで暗号メッセージを同報送信することができる。

[0351] また、受信者（装置）が第三者（装置）に暗号メッセージを転送する際、暗号化装置から受信した暗号メッセージをそのまま第三者（装置）に転送することができる。公開鍵暗号方式では、受信者（装置）が一旦、暗号メッセージを復号し、第三者（装置）の公開鍵を用いて暗号化し、この暗号化された暗号メッセージを送信する処理が必要であり、処理コストの負担が大きい。しかし、上述の各実施形態では、暗号化装置から受信した暗号メッセージをそのまま第三者（装置）に転送するから、低い処理コストで暗号メッセージを転送することができる。

[0352] 次に、上述の第１の観点による暗号通信技術に留意しつつ、第３の観点から、柔軟に運用可能であって述語暗号で暗号化されたコンテンツ（暗号化コンテンツ）を配信することが可能な、述語暗号に依拠する暗号通信技術に関する実施形態を説明する。この技術によると、述語暗号で暗号化されたコン

テンツ（暗号化コンテンツ）がコンテンツサーバ装置に蓄えられ、復号装置からの要求に応じて暗号化コンテンツを送信することによって、暗号化コンテンツを配信することができる。

[0353] 第３の観点による暗号通信技術の説明は上述の第１の観点による暗号通信技術の説明と実質的に重複する部分を多く含むが、第１の観点による暗号通信技術の説明を参照しなくてもよいように、できるだけ重複説明と重複図面を省略せずに第３の観点による暗号通信技術を説明する。このため、数式の番号、機能部を表す参照番号、ステップを表す参照番号なども両者で重複するが、文脈から混乱の虞は無いであろう。

[0354] 〔第３の観点による第１実施形態〕

図６０から図７１を参照して第３の観点による本発明の第１実施形態を説明する。

[0355] 第３の観点による暗号システム１は、図６０に示すように、複数のクライアント装置１０、３０と、一つまたは複数の鍵生成装置２０と、一つまたは複数のコンテンツサーバ装置６０と、一つまたは複数のユーザ情報管理装置４０（以下、管理装置と言う）、変換規則情報ペア管理装置５０（以下、登録装置と言う）、一つまたは複数の保全装置８０、一つまたは複数の認証装置９０を含んでいる。これらの各装置は、例えばインターネットである通信網５を介して相互に通信可能とされている。

[0356] クライアント装置は、処理目的に応じて、コンテンツを暗号化して暗号化コンテンツを生成する暗号化装置として、あるいは暗号化コンテンツを復号する復号装置として機能する。そこで、クライアント装置を機能の観点から、暗号化装置１０または復号装置３０と呼称する。なお、第３の観点による暗号システム１は、暗号化装置としてのみ機能するクライアント装置および／または復号装置としてのみ機能するクライアント装置を含んでもよい。

[0357] 第３の観点による暗号システム１では述語暗号を用いた暗号化と復号が行われる。第３の観点による本発明では、使用する述語暗号アルゴリズムに限定は無く、例えば上記非特許文献２に開示される述語暗号アルゴリズムを用

いることが許される。第３の観点による第１実施形態では、ＫＥＭ(Key Encapsulation Mechanisms)タイプの述語暗号アルゴリズムを用いた例を示す。

[0358] 暗号システム１における暗号通信方法を、図６１、６２、６３、６４、６６、６９、７１を参照しながら叙述する。各装置の機能構成については、図６５、６７、６８、７０を参照されたい。

[0359] 《準備プロセス》

第１の観点による発明の第１実施形態における《準備プロセス》の説明の全てをここに援用し、重複説明を省略する。なお、この《準備プロセス》の説明に対応する図として図６１を、スキーマペアについては図１１－１３を、ポリシーリストについては図１４を参照されたい。これで《準備プロセス》は終了する。

[0360] 《暗号化プロセス》

暗号化装置１０の送信部１４は、図示しない制御部の制御を受けて、検索クエリを登録装置５０に送信し、登録装置５０の受信部が検索クエリを受信する（ステップＳ１４）。登録装置５０の検索部は、登録装置５０の記憶部に登録されているエントリの一部または全部を検索して一つのエントリを選び（ステップＳ１５）、登録装置５０の送信部は検索結果のエントリを暗号化装置１０に送信し、暗号化装置１０の受信部はエントリを受信する（ステップＳ１６）。このエントリには、鍵生成装置のアドレス、この鍵生成装置の公開パラメータ、この鍵生成装置が使用可能なポリシーリスト、この鍵生成装置が使用可能なスキーマリストが含まれている。受信したエントリは、暗号化装置１０のメモリ１１に記憶される。

[0361] なお、各鍵生成装置２０の公開パラメータ、スキーマリスト、ポリシーリスト、アドレスを予め暗号化装置１０が所有している場合には、ステップＳ１４－Ｓ１６の処理は省略される。つまり、暗号システム１が登録装置５０を含まない形態も許容されることに注意しなければならない。

[0362] 暗号化装置１０の第１述語論理情報取得部１２が、メモリ１１から入力情報とポリシーとスキーマを読み込み、属性情報（以下、第１属性情報と言う

）または述語情報（以下、第１述語情報と言う）を求める（ステップＳ１７ａ）。この処理の詳細について説明を加える（図１２、図１３参照）。

[0363] まず、スキーマリストに複数のスキーマペアが記述されている場合、用途などに応じて一つのスキーマペアが選択される。暗号化装置１０の利用者によってスキーマペアが選択されてその指示情報が入力される場合や、所定の規則に従い、第１述語論理情報取得部１２がスキーマペアを選択してもよい。

[0364] そして、入力情報が属性指定情報または述語指定情報のいずれであるかに応じてポリシーと共にいずれか一方のスキーマを選択する。暗号化装置１０の利用者によってポリシーといずれか一方のスキーマが選択されてその指示情報が入力される場合や、所定の規則に従い、第１述語論理情報取得部１２がポリシーといずれか一方のスキーマを選択する場合のいずれであってもよい。なお、鍵生成装置２０のポリシーが１種類のタイプのみ用意されている場合には、そのポリシーに従ってスキーマペアのうちの一方のスキーマが選択される。もし、選択されたスキーマが入力情報の種類に対応していない場合には、スキーマリストからスキーマペアを再選択するか、登録装置５０からエントリの提供を再度受ければよい。

[0365] 入力情報は、暗号化装置１０の利用者によって入力された情報または、例えばＩＣカード３９のような記憶媒体から暗号化装置１０の取得部（図示せず）が取得した情報でもよい。

[0366] そして、第１述語論理情報取得部１２が、ポリシーに従ってスキーマペアの中から選択されたスキーマを用いて入力情報から第１属性情報または第１述語情報を得る。ポリシーがKey_Policyであり選択されたスキーマが属性用スキーマである場合には第１属性情報が得られる。ポリシーがCipher_Text_Policyであり選択されたスキーマが述語用スキーマである場合には第１述語情報が得られる。第１属性情報と第１述語情報は、第３の観点による第１実施形態では、有限体F_qの元を成分とする一つ又は複数のベクトル情報とされる（図１１－１３参照）。この際、スキーマを用いて入力情報から必要な属性

値の抽出や整列化が行われる。

[0367] 次に、暗号化装置１０の暗号化部１３が、第１属性情報ｖ＝(v_1, …, v_n)または第１述語情報ｗ＝(w_1, …, w_n)と、メモリ１１からの公開パラメータに含まれる直交基底Ｂ（実質的な公開鍵）とコンテンツＭを用いて、共通鍵Ｋと暗号情報C_1と暗号化コンテンツC_2を求める（ステップＳ１７ｂ、Ｓ１７ｃ）。これらの処理の詳細について説明を加える。

[0368] まず、第１暗号化部１３ａが、述語暗号アルゴリズムに則り、有限体F_qの元である乱数ｒ、ρを生成して、上記式（７）のように共通鍵Ｋを設定し、上記式（８）に従って暗号情報C_1を求める（ステップＳ１７ｂ）。Ｈは例えばハッシュ関数である。この例では第１属性情報ｖを用いているが、第１述語情報を用いる場合は上記式（８）においてｖをｗに置き換えればよい。また、この例では、暗号情報C_1は共通鍵Ｋの生成に用いる情報ρに対応する情報であるが、暗号情報C_1を共通鍵Ｋに対応する情報としてもよい。

[0369] 次に、第２暗号化部１３ｂが、共通鍵Ｋとコンテンツ Ｍを用いて、上記式（９）に従って暗号化コンテンツC_2を求める（ステップＳ１７ｃ）。共通鍵を用いた暗号化方法Enc_Kは周知の方法でよく、例えば上記非特許文献１に開示される方法である。

[0370] 次に、暗号化装置１０の送信部１４は、制御部による制御を受けて、暗号情報C_1と、暗号化コンテンツC_2と、メモリ１１からのスキーマペア、ポリシー、公開パラメータ、鍵生成装置のアドレスを纏めた暗号メッセージを生成する（ステップＳ１７ｄ）。そして暗号化装置１０の送信部１４は、暗号メッセージをコンテンツサーバ装置６０に送信し、コンテンツサーバ装置６０の受信部が暗号メッセージを受信する（ステップＳ１８）。暗号化コンテンツのアップロードは例えばＦＴＰ(File Transfer Protocol)やＷｅｂＤＡＶ(Distributed Authoring and Versioning protocol for the WWW)などの周知の方式を利
用して行われる。

[0371] これで《暗号化プロセス》は終了する。

[0372] 《コンテンツ配信プロセス》

コンテンツサーバ装置６０は、図示しない制御部の制御の下、そのメモリ６１に各暗号化装置１０から送られた暗号メッセージを記憶する。これによって、暗号メッセージに含まれる暗号情報と暗号化コンテンツがコンテンツサーバ装置６０に登録される。コンテンツサーバ装置６０にどのような暗号化コンテンツが登録されているかは、例えばＷｅｂページ上で公開される。

[0373] 上記Ｗｅｂページは、例えばインターネットプロトコルに従い、復号装置３０のブラウザ部３８によって、復号装置３０のディスプレイ（図示せず）に表示される。復号装置３０の利用者は、所望の暗号化コンテンツを選択する入力操作を行う。復号装置３０のブラウザ部３８は、利用者が入力した情報に基づき、選択された暗号化コンテンツをコンテンツサーバ装置６０から取得するための取得要求を復号装置３０の復号部３３（以下、中継部という）に伝える（ステップＳ１９）。そして、復号装置３０の中継部３３はこの取得要求をコンテンツサーバ装置６０に送信し、コンテンツサーバ装置６０の受信部はこの取得要求を受信する（ステップＳ２０）。このように、ブラウザ部３８とコンテンツサーバ装置６０との例えばＨＴＴＰ(Hiper Text Transfer Protocol)に従ったやりとりは中継部３３を経由して行われる（例えばWWWブラウザのプロキシ設定を使用することが許される）。コンテンツサーバ装置６０の検索部６２は、取得要求で指定された暗号化コンテンツを含む暗号メッセージを検索してそれを選び（ステップＳ２１）、検索部６２からの指示に基づき、コンテンツサーバ装置６０の送信部６４は暗号メッセージを復号装置３０に送信し、復号装置３０の受信部は暗号メッセージを受信する（ステップＳ２２）。

[0374] これで《コンテンツ配信プロセス》は終了する。

[0375] 《復号プロセス》

復号装置３０の送信部３４は、図示しない制御部の制御を受けて、暗号メッセージに含まれる鍵生成装置のアドレスを含む検索クエリを登録装置５０に送信し、登録装置５０の受信部が検索クエリを受信する（ステップＳ２３

）。登録装置５０の検索部は、アドレスで指定された鍵生成装置のエントリを検索してそれを選び（ステップＳ２４）、登録装置５０の送信部は検索結果のエントリを復号装置３０に送信し、復号装置３０の受信部はエントリを受信する（ステップＳ２５）。このエントリには、鍵生成装置のアドレス、この鍵生成装置の公開パラメータ、この鍵生成装置が使用可能なポリシーリスト、この鍵生成装置が使用可能なスキーマリストが含まれている。受信したエントリは、復号装置３０のメモリ３１に記憶される。

[0376] なお、各鍵生成装置２０の公開パラメータ、スキーマリスト、ポリシーリスト、アドレスを予め復号装置３０が所有している場合には、ステップＳ１９－Ｓ２１の処理は省略される。この場合、復号装置３０は、暗号メッセージに含まれるアドレスに対応する鍵生成装置のエントリを自身のメモリ３１から検索してこれを取得する。

[0377] 復号装置３０の検証部（図示せず）は、制御部の制御を受けて、暗号メッセージに含まれるスキーマペアとポリシーが、登録装置５０から取得したエントリに含まれるポリシーリストとスキーマリストに含まれるか否かを検証する（ステップＳ２６ａ）。この検証に失敗した場合、復号処理の失敗として処理を終了する（ステップＳ２６ｇ）。

[0378] この検証に成功した場合、復号装置３０の取得部３２が、例えばＩＣカード３９のような記憶媒体から、当該復号装置３０の利用者に対応する属性指定情報または述語指定情報を読み取る（ステップＳ２６ｆ）。属性指定情報または述語指定情報のいずれを読み取るかは、暗号メッセージに含まれるポリシーによって決まる。つまり、読み取られる情報は、このポリシーで特定される一方のスキーマとペアになっている他方のスキーマを特定するポリシーの内容に対応する指定情報である。もしポリシーがCipher_Text_Policyである場合、取得部３２は記憶媒体から属性指定情報を読み取る。もしポリシーがKey_Policyである場合、取得部３２は記憶媒体から述語指定情報を読み取る。以下、読み取られた指定情報を利用者情報と呼ぶ。また、復号装置３０の取得部３２が、後述する鍵生成装置２０における処理《利用者情報取得

プロセス》と同様に、管理装置４０から、当該復号装置３０の利用者に対応する属性指定情報または述語指定情報を読み取ることも許容される。なお、第３の観点による第１実施形態では、ステップＳ２６ｆの処理は任意に行われる。例えば、予め復号装置３０が利用者に対応する属性指定情報と述語指定情報を所有している場合、ポリシーに従って属性指定情報または述語指定情報のいずれかが利用者情報となる。

[0379] 次に、復号装置３０の検証部が、暗号メッセージに含まれる暗号情報を復号するために使用する復号鍵を持っているか否かを検証する（ステップＳ２６ｂ）。

[0380] 復号装置３０はメモリ３１に復号鍵テーブルを記憶している。復号鍵テーブルでは、例えば図１５に示すように、鍵生成装置の識別子に対して、公開パラメータと、スキーマペアと、復号鍵の対象と、述語指定情報と、復号鍵とが対応付けられている。そこで、検証部は、暗号メッセージに含まれるアドレスによって判別する鍵生成装置の識別子、公開パラメータと、スキーマペアと、復号鍵の対象（但し、これは、暗号メッセージに含まれるポリシーで特定される一方のスキーマとペアになっている他方のスキーマを特定するポリシーの内容に対応する）に対応する復号鍵の有無を検証する。もし復号鍵が存在すれば、ステップＳ３３の処理を行う。もし復号鍵が存在しなければ、ステップＳ２７の処理を行う。

[0381] ここで《復号プロセス》の説明を中断し、《鍵生成プロセス》の説明をする。

[0382] 上述のように復号鍵が存在しない場合、復号装置３０の送信部３４は、制御部による制御を受けて、メモリ３１からの公開パラメータ、ポリシー、スキーマペア、（もし在れば）利用者情報、認証情報を纏めた鍵要求メッセージを生成する。認証情報は、例えば利用者のＩＤとパスワードを含む。そして、復号装置３０の送信部３４は、メモリ３１からのアドレスを持つ鍵生成装置に鍵要求メッセージを送信し、この鍵生成装置２０の受信部が、鍵要求メッセージを受信する（ステップＳ２７）。受信した鍵要求メッセージは、

鍵生成装置２０のメモリ２１に記憶される。

[0383] 鍵生成装置２０の検証部（図示せず）は、制御部の制御を受けて、鍵要求メッセージに含まれるスキーマペアとポリシーが、当該鍵生成装置２０が所有するエントリ（例えばステップＳ１で生成されたエントリである）に含まれるポリシーリストとスキーマリストに含まれるか否か、および、鍵要求メッセージに含まれる公開パラメータが当該鍵生成装置２０の公開パラメータであるか否かを検証する（ステップＳ２８ａ）。この検証に失敗した場合、鍵生成処理の失敗として処理を終了する（ステップＳ２８ｇ）。なお、ステップＳ２８ａの処理では、鍵要求メッセージに認証情報が含まれるならば、鍵要求メッセージに含まれる認証情報の検証も行われる。鍵生成装置２０は、メモリ２１に認証テーブルを記憶している。認証テーブルでは、例えば図１６に示すように、利用者のＩＤに対してパスワードが対応付けられている。そこで、検証部は、鍵要求メッセージに含まれる利用者のＩＤとパスワードと認証テーブルに含まれる利用者のＩＤとパスワードとの整合性を検証する。この検証に失敗した場合も、ステップＳ２８ｇの処理が行われる。

[0384] この検証に成功した場合、鍵生成装置２０の検証部が、鍵要求メッセージに利用者情報が含まれているか否かを検証する（ステップＳ２８ｂ）。鍵要求メッセージに利用者情報が含まれていればステップＳ２８ｃの処理を行い、鍵要求メッセージに利用者情報が含まれていなければステップＳ２９の処理を行う。なお、必ず鍵要求メッセージに利用者情報が含まれる方法を採用する場合には、ステップＳ２８ｂの処理および後述する《利用者情報取得プロセス》は不要である。

[0385] ここで《鍵生成プロセス》の説明を中断し、《利用者情報取得プロセス》の説明をする。

[0386] 鍵生成装置２０の送信部は、鍵要求メッセージに含まれるポリシーと（もし在れば）認証情報を含むリクエストを管理装置４０に送信し、管理装置４０がリクエストを受信する（ステップＳ２９）。受信したリクエストは、管理装置４０のメモリに記憶される。

[0387] 管理装置４０はメモリに認証テーブルを記憶している。この認証テーブルでは、上述の認証テーブルと同様に、利用者のＩＤに対してパスワードが対応付けられている（図１６参照）。そこで、管理装置４０の検証部（図示せず）は、リクエストに含まれる利用者のＩＤとパスワードと認証テーブルに含まれる利用者のＩＤとパスワードとの整合性を検証する。

[0388] この検証に成功すると、管理装置４０の検索部（図示せず）がリクエストに含まれるポリシーに従って、メモリに記憶されている利用者情報テーブルから属性指定情報または述語指定情報を検索する（ステップＳ３０）。利用者情報テーブルは、例えば利用者のＩＤとこれに対応付けられた属性名および属性指定情報で構成される第１テーブルと、利用者のＩＤとこれに対応付けられた述語指定情報で構成される第２テーブルとを含んでいる（図１７参照）。属性指定情報または述語指定情報のいずれを読み取るかは、リクエストに含まれるポリシーによって決まる。つまり、読み取られる情報は、このポリシーで特定される一方のスキーマとペアになっている他方のスキーマを特定するポリシーの内容に対応する指定情報である。もしポリシーがCipher_Text_Policyである場合、検索部は第１テーブルからリクエストに含まれる利用者のＩＤに対応する属性指定情報を取得する。もしポリシーがKey_Policyである場合、検索部は第２テーブルからリクエストに含まれる利用者のＩＤに対応する述語指定情報を取得する。読み取られた指定情報を利用者情報と呼ぶ。

[0389] 管理装置４０の送信部は、制御部による制御を受けて、検索結果の利用者情報を鍵生成装置２０に送信し、鍵生成装置２０の受信部が利用者情報を受信する（ステップＳ３１）。受信した利用者情報は、鍵生成装置２０のメモリ２１に記憶される。

[0390] 以上で《利用者情報取得プロセス》を終了し、再び《鍵生成プロセス》の説明に戻る。

[0391] 利用者情報を既に所有している場合、あるいは、利用者情報取得プロセスによって利用者情報を受信した場合（ステップＳ３１）、鍵生成装置２０の

第２述語論理情報取得部２３は、メモリ２１からポリシーと、スキーマペアと、公開パラメータと、利用者情報を読み込み、利用者情報から、属性情報（第２属性情報と言う）または述語情報（第２述語情報と言う）を得る（ステップＳ２８ｃ）。この処理において利用者情報に適用されるスキーマは、ポリシーで特定される一方のスキーマとペアになっている他方のスキーマである。ポリシーがCipher_Text_Policyである場合、Cipher_Text_Policyで特定される一方のスキーマ（述語用スキーマ）とペアになっている他方のスキーマ（属性用スキーマ）を用いて、利用者情報（属性指定情報）から第２属性情報を得る。ポリシーがKey_Policyである場合、Key_Policyで特定される一方のスキーマ（属性用スキーマ）とペアになっている他方のスキーマ（述語用スキーマ）を用いて、利用者情報（述語指定情報）から第２述語情報を得る。このように、この処理で用いられるスキーマは、ステップＳ１７ａで用いられたスキーマとペアになっているスキーマであることに注意しなければならない。第２属性情報と第２述語情報は、第３の観点による第１実施形態では、有限体F_qの元を成分とす

る一つ又は複数のベクトル情報とされる（図１１－１３参照）。この際、スキーマを用いて入力情報から必要な属性値の抽出や整列化が行われる。

[0392] 次に、鍵生成装置２０の鍵生成部２５が、述語暗号アルゴリズムに則り、公開パラメータのｑに基づき有限体F_qの元である乱数αを生成して、メモリ２１からの第２属性情報$v_{(p)}=(v_{(p)1}, \cdots, v_{(p)n})$または第２述語情報$w_{(p)}=(w_{(p)1}, \cdots, w_{(p)n})$と、当該鍵生成装置の秘密鍵Ｂ*を用いて、上記式（１０）に従って復号鍵Ｒを求める（ステップＳ２８ｄ）。暗号化処理で用いられた入力情報が属性指定情報である場合に対応して、この例では第２述語情報$w_{(p)}$を用いているが、入力情報が述語指定情報である場合には、第２属性情報$v_{(p)}$が対応するので、上記式（１０）において$w_{(p)}$を$v_{(p)}$に置き換えればよい。

[0393] 次に、鍵生成装置２０の送信部２４は、制御部による制御を受けて、復号鍵Ｒを復号装置３０に送信し、復号装置３０の受信部が復号鍵Ｒを受信する（ステップＳ３２）。受信した復号鍵Ｒは、復号装置３０のメモリ３１に記

憶される。

[0394] 以上で《鍵生成プロセス》を終了し、再び《復号プロセス》の説明に戻る。

[0395] 復号鍵を既に所有している場合、あるいは、鍵生成プロセスによって復号鍵を受信した場合（ステップＳ３２）、復号装置３０の中継部３３が、メモリ３１から公開パラメータと復号鍵Ｒと暗号情報C_1と（必要に応じて）暗号化コンテンツC_2を読み込んで、共通鍵Ｋとコンテンツ Ｍを求める（ステップＳ３３）。

[0396] このステップＳ３３の処理の詳細について説明を加える。中継部３３は、復号処理を担う第１復号部３３ａと第２復号部３３ｂを含む。

[0397] 第１復号部３３ａは、メモリ３１から公開パラメータと暗号情報C_1と復号鍵Ｒを読み込み、述語暗号アルゴリズムに則り、ｅ（C_1, Ｒ）を求める。この演算結果は上記式（１１）に示すように、入力情報が属性指定情報である場合、双線形性に基づき暗号情報C_1と復号鍵Ｒから取り出された第１属性情報ｖと第２述語情報$w_{(p)}$の標準内積の結果に依存する。入力情報が述語指定情報である場合、上記式（１１）においてｖを$v_{(p)}$に、$w_{(p)}$をｗに置き換えればよく、演算結果は双線形性に基づき暗号情報C_1と復号鍵Ｒから取り出された第１述語情報ｗと第２属性情報$v_{(p)}$の標準内積の結果に依存する。但し、ｅ（b_i, b_i^*）は上記式（１２）のように定義される。δ_{ij}は、クロネッカーのデルタ記号である。

[0398] 従って、第１属性情報ｖと第２述語情報$w_{(p)}$の標準内積が０（あるいは第１述語情報ｗと第２属性情報$v_{(p)}$の標準内積が０）の場合、上記式（１１）の演算結果g_T^{ρ}が得られる。この演算結果g_T^{ρ}が得られた場合、復号装置３０の第１復号部３３ａは、上記式（７）に従って“正しい”共通鍵Ｋを得る（ステップＳ２６ｃ）。もし第１属性情報ｖと第２述語情報$w_{(p)}$の標準内積が０（あるいは第１述語情報ｗと第２属性情報$v_{(p)}$の標準内積が０）ではない場合、第１復号部３３ａは、上記式（７）に従って“正しくない”値を得る。この例では、ハッシュ関数Ｈはシステムに共通とするか公開パラメータに含まれ

るとする。この例では、暗号情報C_1が共通鍵Ｋの生成に用いる情報ρに対応する情報

であるが、暗号情報C_1を共通鍵Ｋに対応する情報とする場合には、上記式（１１）の演算結果が共通鍵Ｋ（あるいは正しくない値）となる。つまり、復号装置３０の正当な利用者は、第１属性情報ｖとの標準内積が０となる第２述語情報$w_{(\rho)}$を与える述語指示情報、あるいは、第１述語情報ｗとの標準内積が０となる第２属性情報$v_{(\rho)}$を与える属性指示情報を持つ。

[0399] 次に、第２復号部３３ｂが、共通鍵Ｋと暗号化コンテンツC_2を用いて、上記式（１３）に従ってコンテンツＭを求める（ステップＳ２６ｄ）。共通鍵を用いた復号方法Dec_Kは暗号化方法Enc_Kに対応する。

[0400] もし、上記式（１１）に従った演算結果が正しくない値である場合には、上記式（１３）によっては正しいコンテンツＭを得ることができない。

[0401] なお、復号装置３０は、復号鍵Ｒを復号鍵テーブルに記憶してもよい。また、共通鍵Ｋを復号鍵テーブルに付加して記憶してもよい。

[0402] 暗号化コンテンツを復号して得られたコンテンツＭは、中継部３３からブラウザ部３８に伝えられ（ステップＳ３４）、ブラウザ部３８によって、復号装置３０のディスプレイに表示される（ステップＳ３５）。

[0403] これで《復号プロセス》は終了する。

[0404] 〔第３の観点による第２実施形態〕

第３の観点による第２実施形態では、第３の観点による第１実施形態と異なり、復号装置３０が第２属性情報または第２述語情報を生成する。この差異に伴い、第３の観点による第２実施形態は、いくつかの事項で第３の観点による第１実施形態と異なる。そこで、第３の観点による第１実施形態と重複する部分については重複説明を省略し（同一の構成要素に同じ参照番号を割り当てる）、図７２－図７５を参照しながら第３の観点による第１実施形態と異なる部分を説明する。

[0405] ステップＳ１からステップＳ２６ｂまでの処理は、第３の観点による第１実施形態と同じである。

ステップＳ２６ｂの処理で復号鍵を所有していない場合、復号装置３０の第２述語論理情報取得部３５が、メモリ３１からポリシーと、スキーマペアと、公開パラメータと、利用者情報を読み込み、利用者情報から、属性情報（第２属性情報と言う）または述語情報（第２述語情報と言う）を得る（ステップＳ２７ｇ）。この処理において利用者情報に適用されるスキーマは、ポリシーで特定される一方のスキーマとペアになっている他方のスキーマである。ポリシーがCipher_Text_Policyである場合、Cipher_Text_Policyで特定される一方のスキーマ（述語用スキーマ）とペアになっている他方のスキーマ（属性用スキーマ）を用いて、利用者情報（属性指定情報）から第２属性情報を得る。ポリシーがKey_Policyである場合、Key_Policyで特定される一方のスキーマ（属性用スキーマ）とペアになっている他方のスキーマ（述語用スキーマ）を用いて、利用者情報（述語指定情報）から第２述語情報を得る。このように、この処理で用いられるスキーマは、ステップＳ１７ａで用いられたスキーマとペアになっているスキーマであることに注意しなければならない。第２属性情報と第２述語情報は、第３の観点による第２実施形態では、有限体F_qの元を成分とする一つ又は複数のベクトル情報とされる（図１１－１３参照）。

[0406] ステップＳ２７ｇの処理の後、ステップＳ２７の処理が行われる。ただし、この処理では、復号装置３０の送信部３４が、制御部による制御を受けて、メモリ３１からの公開パラメータ、ポリシー、スキーマペア、認証情報、第２属性情報または第２述語情報を纏めた鍵要求メッセージを生成する。そして、復号装置３０の送信部３４は、メモリ３１からのアドレスを持つ鍵生成装置に鍵要求メッセージを送信し、この鍵生成装置２０の受信部が、鍵要求メッセージを受信する。

[0407] そして、ステップＳ２８ａの処理で検証に成功した場合、ステップＳ２８ｄの処理が行われる。鍵生成装置２０は復号装置３０から第２属性情報または第２述語情報を受信しているため、第３の観点による第１実施形態と異なり、この情報を生成するための機能と処理が不要である。

[0408] そして、ステップＳ２８ｄの処理の後のステップＳ３２からステップＳ３５までの各処理は、第３の観点による第１実施形態と同じである。

[0409] 〔第３の観点による第３実施形態〕

第３の観点による第３実施形態では、第３の観点による第１実施形態と異なり、暗号化装置１０の暗号化部１３が、第１属性情報ｖ＝(v_1，…，v_n)または第１述語情報ｗ＝(w_1，…，w_n)と、メモリ１１からの公開パラメータに含まれる公開鍵とコンテンツＭを用いて、暗号化コンテンツC_1を求める。つまり、第３の観点による第３実施形態では、例えば上記非特許文献２に示す述語暗号アルゴリズムが用いられる。この差異に伴い、第３の観点による第３実施形態は、いくつかの事項で第３の観点による第１実施形態と異なる。そこで、第３の観点による第１実施形態と重複する部分については重複説明を省略し（同一の構成要素に同じ参照番号を割り当てる）、図７６－図７９を参照しながら第３の観点による第１実施形態と異なる部分を説明する。

[0410] ステップＳ１からステップＳ１７ａまでの処理は、第３の観点による第１実施形態と同じである。但し、公開パラメータなどの情報は第３の観点による第３実施形態の述語暗号アルゴリズムに必要な情報とされる。具体的な情報については、例えば上記非特許文献２などを参考されたい。

[0411] ステップＳ１７aの処理に続くステップＳ１７ｂ１の処理では、暗号化装置１０の暗号化部１３が、述語暗号アルゴリズムに則り、第１属性情報ｖ＝(v_1，…，v_n)または第１述語情報ｗ＝(w_1，…，w_n)と、メモリ１１からの公開パラメータに含まれる公開鍵とコンテンツＭを用いて、暗号化コンテンツC_1を求める（ステップＳ１７ｂ１）。

[0412] 次に、ステップＳ１７ｂ１の処理の後、ステップＳ１７ｄの処理が行われる。但し、この処理では、暗号化装置１０の送信部１４が、制御部による制御を受けて、暗号化コンテンツC_1と、メモリ１１からのスキーマペア、ポリシー、公開パラメータ、鍵生成装置のアドレスを纏めた暗号メッセージを生成する（ステップＳ１７ｄ）。

[0413] ステップＳ１７ｄの処理に続くステップＳ１８からステップＳ３２までの

処理は、第３の観点による第１実施形態と同じである。

[0414] ステップＳ３２の処理に続くステップＳ２６ｃ１の処理では、復号装置３０の中継部３３に含まれる復号部３３ｃが、述語暗号アルゴリズムに則り、メモリ３１から公開パラメータと復号鍵Ｒと暗号化コンテンツC_1を読み込んで、コンテンツＭを求める（ステップＳ２６ｃ１）。

[0415] ステップＳ２６ｃ１の処理に続くステップＳ３４とステップＳ３５の各処理は、第３の観点による第１実施形態と同じである。

[0416] 〔第３の観点による第４実施形態〕

第３の観点による第４実施形態は、第３の観点による第２実施形態と第３の観点による第３実施形態の組み合わせ形態に相当する。つまり、第３の観点による第４実施形態は、第３の観点による第１実施形態と異なり、（１）復号装置３０が第２属性情報または第２述語情報を生成する、（２）暗号化装置１０の暗号化部１３が、第１属性情報ｖ＝(v_1，…，v_n)または第１述語情報ｗ＝(w_1，…，w_n)と、メモリ１１からの公開パラメータに含まれる公開鍵とコンテンツＭを用いて、暗号化コンテンツC_1を求める。この差異に伴い、第３の観点による第４実施形態は、いくつかの事項で第３の観点による第１実施形態と異なる。そこで、第３の観点による第１実施形態と重複する部分については重複説明を省略し（同一の構成要素に同じ参照番号を割り当てる）、図８０と図８１も参照して第３の観点による第１実施形態と異なる部分を説明する。

[0417] ステップＳ１からステップＳ１７ａまでの処理は、第３の観点による第１実施形態と同じである。但し、公開パラメータなどの情報は第３の観点による第４実施形態の述語暗号アルゴリズムに必要な情報とされる。具体的な情報については、例えば上記非特許文献２などを参考されたい。

[0418] ステップＳ１７aの処理に続くステップＳ１７ｂ１の処理では、暗号化装置１０の暗号化部１３が、述語暗号アルゴリズムに則り、第１属性情報ｖ＝(v_1，…，v_n)または第１述語情報ｗ＝(w_1，…，w_n)と、メモリ１１からの公開パラメータに含まれる公開鍵とコンテンツＭを用いて、暗号化コンテンツC_1

を求める（ステップＳ１７ｂ１）。

[0419] 次に、ステップＳ１７ｂ１の処理の後、ステップＳ１７ｄの処理が行われる。但し、この処理では、暗号化装置１０の送信部１４が、制御部による制御を受けて、暗号化コンテンツC_1と、メモリ１１からのスキーマペア、ポリシー、公開パラメータ、鍵生成装置のアドレスを纏めた暗号メッセージを生成する（ステップＳ１７ｄ）。

[0420] ステップＳ１７ｄの処理に続くステップＳ１８からステップＳ２６ｂの処理までは、第３の観点による第１実施形態と同じである。

[0421] ステップＳ２６ｂの処理で復号鍵を所有していない場合、復号装置３０の第２述語論理情報取得部３５が、メモリ３１からポリシーと、スキーマペアと、公開パラメータと、利用者情報を読み込み、利用者情報から、属性情報（第２属性情報と言う）または述語情報（第２述語情報と言う）を得る（ステップＳ２７ｇ）。この処理において利用者情報に適用されるスキーマは、ポリシーで特定される一方のスキーマとペアになっている他方のスキーマである。ポリシーがCipher_Text_Policyである場合、Cipher_Text_Policyで特定される一方のスキーマ（述語用スキーマ）とペアになっている他方のスキーマ（属性用スキーマ）を用いて、利用者情報（属性指定情報）から第２属性情報を得る。ポリシーがKey_Policyである場合、Key_Policyで特定される一方のスキーマ（属性用スキーマ）とペアになっている他方のスキーマ（述語用スキーマ）を用いて、利用者情報（述語指定情報）から第２述語情報を得る。このように、この処理で用いられるスキーマは、ステップＳ１７ａで用いられたスキーマとペアになっているスキーマであることに注意しなければならない。第２属性情報と第２述語情報は、第３の観点による第４実施形態では、有限体F_qの元を成分とする一つ又は複数のベクトル情報とされる（図１１－１３参照）。

[0422] ステップＳ２７ｇの処理の後、ステップＳ２７の処理が行われる。ただし、この処理では、復号装置３０の送信部３４が、制御部による制御を受けて、メモリ３１からの公開パラメータ、ポリシー、スキーマペア、認証情報、

第２属性情報または第２述語情報を纏めた鍵要求メッセージを生成する。そして、復号装置３０の送信部３４は、メモリ３１からのアドレスを持つ鍵生成装置に鍵要求メッセージを送信し、この鍵生成装置２０の受信部が、鍵要求メッセージを受信する。

[0423] そして、ステップＳ２８ａの処理で検証に成功した場合、ステップＳ２８ｄの処理が行われる。鍵生成装置２０は、復号装置３０から第２属性情報または第２述語情報を受信しているため、この情報を生成するための機能と処理が不要である。

[0424] そして、ステップＳ２８ｄの処理の後のステップＳ３２の処理は、第３の観点による第１実施形態と同じである。

[0425] ステップＳ３２の処理に続くステップＳ２６ｃ１の処理では、復号装置３０の復号部３３が、述語暗号アルゴリズムに則り、メモリ３１から公開パラメータと復号鍵Ｒと暗号化コンテンツC_1を読み込んで、コンテンツＭを求める（ステップＳ２６ｃ１）。

[0426] ステップＳ２６ｃ１の処理に続くステップＳ３４とステップＳ３５の各処理は、第３の観点による第１実施形態と同じである。

[0427] 第３の観点による上述の各実施形態から明らかなように、中継部が暗号化コンテンツの復号を行う。このため、復号処理を例えばＷＷＷサーバやＷＷＷブラウザの通常のプロトコルから切り離して実施でき、既存のＷＷＷシステムを流用することが容易になる。また、利用者が暗号化コンテンツの復号処理を行うための操作をせずとも、中継部が復号処理を行うので、利用者の利便性が高い。

[0428] 第３の観点による上述の各実施形態では、コンテンツサーバ装置６０と復号装置３０との間の通信路にキャッシュサーバ装置等が設置される運用も許容される（この場合、暗号化コンテンツがキャッシュされる）。

[0429] また、クライアント端末装置を通信網５に常時接続させない運用での利便性を考慮して、中継部が復号前の暗号化コンテンツをキャッシュしてもよい。

[0430] また、WWWブラウザへの復号済みコンテンツのキャッシュを回避するため、キャッシュを無効とさせるＨＴＴＰキャッシュコントロールヘッダをＷＷＷブラウザへのレスポンスに付与させてもよい。

[0431] 複数の利用者が同じクライアント端末装置を使用するようなケースを考慮して、中継部が認証機能を持つシステム構成を採用してもよい。この場合には、WWWブラウザに対してＨＴＴＰのBasic認証やDigest認証を利用し、また、認証のための認証情報（ユーザＩＤ／パスワード）のテーブル等および認証情報の追加・変更・削除に関する管理機能を中継部に追加してもよい。

[0432] 第３の観点による上述の各実施形態は、コンテンツ配信システムとして好適に実施される。述語暗号は、暗号化に際して受信者に依存する情報に拘束されない方式であるから、不特定の者が閲覧する可能性のあるコンテンツのアクセス制御として好適である。

[0433] 図８２に、送受信されるデータの構成を例示する。メッセージ全体の基本的なフォーマットは例えばＳ／ＭＩＭＥ（Secure Multipurpose Internet Mail Extensions）に従うが、暗号メッセージ開始位置マーカから暗号メッセージ終了位置マーカまでのデータはＸＭＬ（eXtensible Markup Language）などで適切なデータ構成が与えられる。

[0434] 暗号化コンテンツに関するデータを暗号ブロックとする。以下、暗号ブロックの構成要素を示す。

[0435] アルゴリズム識別子ブロックには、共通鍵の暗号化に使用した述語暗号アルゴリズムとコンテンツの暗号化に使用した共通鍵暗号アルゴリズムを特定するための情報が指定される。このように、アルゴリズムを表す識別子やアルゴリズムのバージョンなどを指定できる（PE/VersionX+Camellia［Camelliaは登録商標］など）。

[0436] デジタル署名ブロックにはデジタル署名が記述される。署名アルゴリズムは既存の方式を使用できる。この項目は運用形態に応じて省略可能である。

[0437] 公開パラメータ情報ブロックには、使用した公開情報パラメータを特定する情報が指定される。公開情報パラメータを特定する識別子、もしくは公開

情報パラメータのデータそのものを指定することもできる。

[0438] ポリシーフィールドには、使用したポリシーを特定する識別子が指定される。

[0439] スキーマフィールドには、使用したスキーマを特定する識別子が指定されるか、もしくはスキーマのデータが記述される。

[0440] 暗号情報フィールドにはコンテンツの暗号化に使用した共通鍵を述語暗号で暗号化したデータ（暗号情報）が指定される。

[0441] コンテンツファイル名、コンテンツタイプ、コンテンツファイルサイズには、それぞれ、コンテンツのファイル名、コンテンツのデータタイプ（例：text/htmlなど）、コンテンツのファイルサイズが記述される。

[0442] 属性フィールド／述語フィールドにはポリシーフィールドに対応して暗号化に使用した属性／述語を表す文字列表現を指定することができる。これらの項目は運用形態に応じては省略可能である。

[0443] 暗号データにはコンテンツを暗号化して生成した暗号化コンテンツが記述される。

[0444] コンテンツの基本的なデータ構成はＨＴＭＬ(Hyper Text Markup Language)で記述され、暗号ブロックはＨＴＭＬ内部のコメント文で指定される。

[0445] 暗号ブロックはＸＭＬ(eXtensible Markup Language)などで適切なデータ構成が与えられる。

[0446] ブラウザなどで直接閲覧しようとした場合には、コメント文は表示されず、残りのＨＴＭＬの文章が表示されるので、残りのＨＴＭＬ部分には暗号化コンテンツであることを示すメッセージや、復号に失敗した場合のエラーメッセージなどを記述してもよい。

[0447] 上述の説明では、代数構造Ｓを有限体としたが、有限環（整数剰余環）でもよい。述語暗号アルゴリズムが例えば内積を用いる述語暗号アルゴリズムである場合、第１、第２属性情報ならびに第１、第２述語情報は、Ｓの元を成分とするベクトルとされる。

[0448] また、代数構造Ｓの体系に応じて、公開鍵ＢはＳ上の加群Ｖの元の集合で

あり、秘密鍵Ｂ*は、加群Ｖの双対加群Ｖ*の元の集合であり、復号鍵Ｒは、双対加群Ｖ*の元とされる。なお、代数構造Ｓが有限体である場合、有限体上の加群Ｖは、いわゆる有限体上のベクトル空間のことである。このとき、暗号化部は、公開鍵Ｂの元に対して第１属性情報の成分を係数とするスカラー倍を行う演算または公開鍵Ｂの元に対して第１述語情報の成分を係数とするスカラー倍を行う演算を含む演算を行うことで暗号情報を求める。そして、鍵生成部は、秘密鍵Ｂ*の元に対して第２述語情報の成分を係数とするスカラー倍を行う演算または秘密鍵Ｂ*の元に対して第２属性情報の成分を係数とするスカラー倍を行う演算を含む演算を行うことで復号鍵Ｒを求める。

[0449] 暗号システムに含まれるハードウェアエンティティ（クライアント装置、鍵生成装置、登録装置、管理装置、保全装置、認証装置、コンテンツサーバ装置）は、キーボードなどが接続可能な入力部、液晶ディスプレイなどが接続可能な出力部、ハードウェアエンティティの外部に通信可能な通信装置（例えば通信ケーブル）が接続可能な通信部、ＣＰＵ（Central Processing Unit）〔キャッシュメモリやレジスタなどを備えていてもよい。〕、メモリであるＲＡＭやＲＯＭ、ハードディスクである外部記憶装置並びにこれらの入力部、出力部、通信部、ＣＰＵ、ＲＡＭ、ＲＯＭ、外部記憶装置の間のデータのやり取りが可能なように接続するバスを有している。また必要に応じて、ハードウェアエンティティに、ＣＤ－ＲＯＭなどの記憶媒体を読み書きできる装置（ドライブ）などを設けるとしてもよい。このようなハードウェア資源を備えた物理的実体としては、汎用コンピュータなどがある。

[0450] ハードウェアエンティティの外部記憶装置には、上述の機能を実現するために必要となるプログラムおよびこのプログラムの処理において必要となるデータなどが記憶されている（外部記憶装置に限らず、例えばプログラムを読み出し専用記憶装置であるＲＯＭに記憶させておくなどでもよい。）。また、これらのプログラムの処理によって得られるデータなどは、ＲＡＭや外部記憶装置などに適宜に記憶される。上述の説明では、演算結果やその格納領域のアドレスなどを記憶するＲＡＭやレジスタなどの記憶装置を単に「メ

モリ」とした。

[0451] ハードウェアエンティティでは、外部記憶装置〔あるいはＲＯＭなど〕に記憶された各プログラムとこの各プログラムの処理に必要なデータが必要に応じてメモリに読み込まれて、適宜にＣＰＵで解釈実行・処理される。その結果、ＣＰＵが所定の機能（例えば、暗号化部、復号部、鍵生成部、第１述語論理情報取得部、第２述語論理情報取得部、制御部など）を実現する。

[0452] 各実施形態で説明したハードウェアエンティティの細部においては、整数論における数値計算処理が必要となる場合があるが、整数論における数値計算処理自体は、周知技術と同様にして達成されるので、その演算処理方法などの詳細な説明は省略した（この点の技術水準を示す整数論における数値計算処理が可能なソフトウェアとしては、例えばＰＡＲＩ／ＧＰ、ＫＡＮＴ／ＫＡＳＨなどが挙げられる。ＰＡＲＩ／ＧＰについては、例えばインターネット〈URL: http://pari.math.u-bordeaux.fr/〉［平成２１年４月１４日検索］を参照のこと。ＫＡＮＴ／ＫＡＳＨについては、例えばインターネット〈URL: http://www.math.tu-berlin.de/algebra/〉［平成２１年４月１４日検索］を参照のこと。）。また、この点に関する文献として、参考文献Ａを挙げることができる。

（参考文献Ａ） H. Cohen, "A Course in Computational Algebraic Number Theory", GTM 138, Springer-Verlag, 1993.

[0453] 本発明は上述の実施形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲で適宜変更が可能である。また、上記実施形態において説明した処理は、記載の順に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されるとしてもよい。

[0454] また、上記実施形態において説明したハードウェアエンティティにおける処理機能をコンピュータによって実現する場合、ハードウェアエンティティが有すべき機能の処理内容はプログラムによって記述される。そして、このプログラムをコンピュータで実行することにより、上記ハードウェアエンテ

ィティにおける処理機能がコンピュータ上で実現される。

[0455] この処理内容を記述したプログラムは、コンピュータで読み取り可能な記憶媒体に記憶しておくことができる。コンピュータで読み取り可能な記憶媒体としては、例えば、磁気記憶装置、光ディスク、光磁気記憶媒体、半導体メモリ等どのようなものでもよい。具体的には、例えば、磁気記憶装置として、ハードディスク装置、フレキシブルディスク、磁気テープ等を、光ディスクとして、ＤＶＤ（Digital Versatile Disc）、ＤＶＤ－ＲＡＭ（Random Access Memory）、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）、ＣＤ－Ｒ（Recordable）／ＲＷ（ReWritable）等を、光磁気記憶媒体として、ＭＯ（Magneto-Optical disc）等を、半導体メモリとしてＥＥＰ－ＲＯＭ（Electronically Erasable and Programmable-Read Only Memory）等を用いることができる。

[0456] また、このプログラムの流通は、例えば、そのプログラムを記憶したＤＶＤ、ＣＤ－ＲＯＭ等の可搬型記憶媒体を販売、譲渡、貸与等することによって行う。さらに、このプログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータにそのプログラムを転送することにより、このプログラムを流通させる構成としてもよい。

[0457] このようなプログラムを実行するコンピュータは、例えば、まず、可搬型記憶媒体に記憶されたプログラムもしくはサーバコンピュータから転送されたプログラムを、一旦、自己の記憶装置に格納する。そして、処理の実行時、このコンピュータは、自己の記憶媒体に格納されたプログラムを読み取り、読み取ったプログラムに従った処理を実行する。また、このプログラムの別の実行形態として、コンピュータが可搬型記憶媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することとしてもよく、さらに、このコンピュータにサーバコンピュータからプログラムが転送されるたびに、逐次、受け取ったプログラムに従った処理を実行することとしてもよい。また、サーバコンピュータから、このコンピュータへのプログラムの転

送は行わず、その実行指示と結果取得のみによって処理機能を実現する、いわゆるＡＳＰ（Application Service Provider）型のサービスによって、上述の処理を実行する構成としてもよい。なお、本形態におけるプログラムには、電子計算機による処理の用に供する情報であってプログラムに準ずるもの（コンピュータに対する直接の指令ではないがコンピュータの処理を規定する性質を有するデータ等）を含むものとする。

[0458] また、この形態では、コンピュータ上で所定のプログラムを実行させることにより、ハードウェアエンティティを構成することとしたが、これらの処理内容の少なくとも一部をハードウェア的に実現することとしてもよい。

[0459] なお、図面に記載した氏名などの情報は、架空のものであり、実際の人物とは全く関係ない。

[0460] ＜総括＞

第１の観点から本発明を総括すると、下記のとおりである。

[0461] ［アイテム１］

関数暗号を用いる暗号システムであって、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵とを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化部とを含み、

上記鍵生成装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成部とを含み、

上記復号装置は、

上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号部を含む、

暗号システム。

[0462] ［アイテム２］

関数暗号を用いる暗号システムであって、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵とを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化部とを含み、

上記復号装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記鍵生成装置から送られた復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号部を含み、

上記鍵生成装置は、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成部とを含む、

暗号システム。

[0463] ［アイテム３］

関数暗号を用いる暗号システムであって、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理

情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号情報を求める暗号化部とを含み、

上記鍵生成装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成部とを含み、

上記復号装置は、

上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号部を含む、

暗号システム。

[0464] ［アイテム４］

関数暗号を用いる暗号システムであって、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と

言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号情報を求める暗号化部とを含み、

上記復号装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記鍵生成装置から送られた復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号部を含み、

上記鍵生成装置は、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成部とを含む、

暗号システム。

[0465] ［アイテム５］

アイテム１またはアイテム２に記載の暗号システムにおいて、

上記暗号化装置の上記暗号化部は、上記共通鍵で平文を暗号化した暗号文も求め、

上記復号装置の上記復号部は、上記復号処理で得られた上記共通鍵を用いる上記暗号文の第２復号処理、または、上記復号処理で得られた上記共通鍵の生成に用いる上記情報から生成された共通鍵を用いる上記暗号文の第２復号処理も行う、

暗号システム。

[0466] ［アイテム６］

アイテム１からアイテム５のいずれかに記載の暗号システムにおいて、

上記利用者に対応する上記属性指定情報および／または上記論理式指定情報は記憶媒体に記憶されており、

上記復号装置は、当該復号装置の利用者に対応する上記属性指定情報または上記論理式指定情報を上記記憶媒体から取得するユーザ情報取得部を含む、

暗号システム。

[0467] ［アイテム７］

アイテム１またはアイテム３に記載の暗号システムにおいて、

上記鍵生成装置が用いる、上記復号装置の利用者に対応する上記属性指定情報または上記論理式指定情報は、上記復号装置から取得した情報である、

暗号システム。

[0468] ［アイテム８］

アイテム１からアイテム６のいずれかに記載の暗号システムにおいて、

上記暗号システムは、一つまたは複数のユーザ情報管理装置をさらに含み、

各上記ユーザ情報管理装置は、上記利用者に対応する上記属性指定情報および／または上記論理式指定情報を記憶する記憶部を含み、

上記鍵生成装置は、上記復号装置の利用者に対応する上記属性指定情報または上記論理式指定情報を上記ユーザ情報管理装置から取得するユーザ情報取得部を含む、

暗号システム。

[0469] ［アイテム９］

アイテム１からアイテム８のいずれかに記載の暗号システムにおいて、

各上記鍵生成装置につき一つまたは複数の上記変換規則情報ペアが予め定められており、

上記暗号システムは、一つまたは複数の変換規則情報ペア管理装置をさらに含み、

各上記変換規則情報ペア管理装置は、各上記鍵生成装置に対応する各上記変換規則情報ペアを記憶する記憶部を含み、

上記暗号化装置は、上記変換規則情報ペア管理装置から上記変換規則情報ペアを取得する変換規則情報ペア取得部を含み、

上記復号装置は、上記変換規則情報ペア管理装置から上記変換規則情報ペアを取得する変換規則情報ペア取得部を含む、

暗号システム。

[0470] ［アイテム１０］

アイテム１からアイテム８のいずれかに記載の暗号システムにおいて、

各上記鍵生成装置につき一つまたは複数の上記変換規則情報ペアが予め定められており、

各上記鍵生成装置は、当該鍵生成装置に対応する各上記変換規則情報ペアを記憶する記憶部をさらに含み、

各上記暗号化装置は、少なくとも一つ以上の上記鍵生成装置に対応す

る各上記変換規則情報ペアを記憶する記憶部をさらに含み、

各上記復号装置は、少なくとも一つ以上の上記鍵生成装置に対応する各上記変換規則情報ペアを記憶する記憶部をさらに含む、

暗号システム。

[0471] ［アイテム１１］

アイテム１からアイテム１０のいずれかに記載の暗号システムにおいて、

上記ポリシー情報の特定対象が上記属性用変換規則情報のみ、あるいは、上記論理式用変換規則情報のみ、あるいは、上記属性用変換規則情報および上記論理式用変換規則情報であることが、上記鍵生成装置ごとに予め定められている、

暗号システム。

[0472] ［アイテム１２］

アイテム１からアイテム１１のいずれかに記載の暗号システムにおいて、

代数構造Ｋを有限環または有限体として、

上記第１、第２属性情報ならびに上記第１、第２論理情報は、上記Ｋの元を成分とするベクトルであり、

上記復号部の上記復号処理では、上記暗号情報と上記復号鍵を入力とし、上記第１論理情報と上記第２属性情報との標準内積または上記第１属性情報と上記第２論理情報との標準内積の結果に依存する演算が行われる、

暗号システム。

[0473] ［アイテム１３］

アイテム１２に記載の暗号システムにおいて、

上記公開鍵は、Ｋ上の加群Ｖの元の集合であり、

上記秘密鍵は、上記加群Ｖの双対加群Ｖ*の元の集合であり、

上記復号鍵は、上記双対加群Ｖ*の元であり、

上記暗号化部は、上記公開鍵の元に対して上記第１属性情報の成分を

係数とするスカラー倍を行う演算または上記公開鍵の元に対して上記第１論理情報の成分を係数とするスカラー倍を行う演算を含む演算を行うことで上記暗号情報を求め、

上記鍵生成部は、上記秘密鍵の元に対して上記第２論理情報の成分を係数とするスカラー倍を行う演算または上記秘密鍵の元に対して上記第２属性情報の成分を係数とするスカラー倍を行う演算を含む演算を行うことで上記復号鍵を求め、

上記復号部の上記復号処理に用いられる上記演算は、双線形性を有し、上記演算の結果が、双線形性に基づき上記暗号情報と上記復号鍵から取り出された上記第１論理情報と上記第２属性情報あるいは上記第１属性情報と上記第２論理情報の標準内積の結果に依存するように構成されている、

暗号システム。

[0474] ［アイテム１４］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペア

の中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵とを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化ステップと、

上記鍵生成装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成ステップと、

上記復号装置の復号部が、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと

を有する暗号通信方法。

[0475] ［アイテム１５］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴ

リズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵とを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化ステップと、

上記復号装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成ステップと、

上記復号装置の復号部が、上記復号鍵を用いて、関数暗号アルゴリズ

ムに則り、上記暗号情報に対する復号処理を行う復号ステップと

を有する暗号通信方法。

[0476] ［アイテム１６］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号情報を求める暗号化ステップと、

上記鍵生成装置の第２命題論理情報取得部が、上記ポリシー情報で特

定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成ステップと、

上記復号装置の復号部が、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと

を有する暗号通信方法。

[0477] ［アイテム１７］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性

指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号情報を求める暗号化ステップと、

上記復号装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成ステップと、

上記復号装置の復号部が、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと

を有する暗号通信方法。

[0478] ［アイテム１８］

アイテム１４またはアイテム１５に記載の暗号通信方法において、

上記暗号化ステップは、上記暗号化部が上記共通鍵で平文を暗号化した暗号文も求める暗号文生成ステップを含み、

上記復号ステップは、上記復号部が、上記復号処理で得られた上記共通鍵を用いる上記暗号文の第２復号処理、または、上記復号処理で得られた上記共通鍵の生成に用いる上記情報から生成された共通鍵を用いる上記暗号文の第２復号処理を行う第２復号ステップを含む、

暗号通信方法。

[0479] ［アイテム１９］

アイテム１４からアイテム１８のいずれかに記載の暗号通信方法において、

上記復号装置の取得部が、上記利用者に対応する上記属性指定情報および／または上記論理式指定情報を記憶する記憶媒体から、当該復号装置の利用者に対応する上記属性指定情報または上記論理式指定情報を取得する取得ステップ

を有する暗号通信方法。

[0480] ［アイテム２０］

アイテム１４またはアイテム１６に記載の暗号通信方法において、

上記復号装置の送信部が、当該復号装置の利用者に対応する上記属性指定情報または上記論理式指定情報を上記鍵生成装置に送信するユーザ情報送信ステップと、

上記鍵生成装置の受信部が、上記復号装置から上記利用者に対応する上記属性指定情報または上記論理式指定情報を受信するユーザ情報受信ステップと

を有する暗号通信方法。

[0481] ［アイテム２１］

アイテム１４からアイテム１８のいずれかに記載の暗号通信方法において、

上記暗号システムは、上記利用者に対応する上記属性指定情報および／または上記論理式指定情報を記憶する記憶部を備える、一つまたは複数のユーザ情報管理装置を含んでおり、

上記鍵生成装置のユーザ情報取得部が、上記復号装置の利用者に対応する上記属性指定情報または上記論理式指定情報を上記ユーザ情報管理装置から取得するユーザ情報取得ステップと

を有する暗号通信方法。

[0482] ［アイテム２２］

アイテム１４からアイテム２１のいずれかに記載の暗号通信方法にお

いて、

各上記鍵生成装置につき一つまたは複数の上記変換規則情報ペアが予め定められており、

上記暗号システムは、各上記鍵生成装置に対応する各上記変換規則情報ペアを記憶する記憶部を備える、一つまたは複数の変換規則情報ペア管理装置を含んでおり、

上記暗号化装置の変換規則情報ペア取得部が、上記変換規則情報ペア管理装置から上記変換規則情報ペアを取得する変換規則情報ペア取得ステップと、

上記復号装置の変換規則情報ペア取得部が、上記変換規則情報ペア管理装置から上記変換規則情報ペアを取得する変換規則情報ペア取得ステップと

を有する暗号通信方法。

[0483] ［アイテム２３］

アイテム１４からアイテム２２のいずれかに記載の暗号通信方法において、

上記ポリシー情報の特定対象が上記属性用変換規則情報のみ、あるいは、上記論理式用変換規則情報のみ、あるいは、上記属性用変換規則情報および上記論理式用変換規則情報であることが、上記鍵生成装置ごとに予め定められている、

暗号通信方法。

[0484] ［アイテム２４］

アイテム１４からアイテム２３のいずれかに記載の暗号通信方法において、

代数構造Ｋを有限環または有限体として、

上記第１、第２属性情報ならびに上記第１、第２論理情報は、上記Ｋの元を成分とするベクトルであり、

上記復号ステップでは、上記復号部が、上記暗号情報と上記復号鍵を

入力とし、上記第１論理情報と上記第２属性情報との標準内積または上記第１属性情報と上記第２論理情報との標準内積の結果に依存する演算を行う、暗号通信方法。

[0485] ［アイテム２５］

アイテム２４に記載の暗号通信方法において、

上記公開鍵は、Ｋ上の加群Ｖの元の集合であり、

上記秘密鍵は、上記加群Ｖの双対加群Ｖ*の元の集合であり、

上記復号鍵は、上記双対加群Ｖ*の元であり、

上記暗号化ステップでは、上記暗号化部が、上記公開鍵の元に対して上記第１属性情報の成分を係数とするスカラー倍を行う演算または上記公開鍵の元に対して上記第１論理情報の成分を係数とするスカラー倍を行う演算を含む演算を行うことで上記暗号情報を求め、

上記鍵生成ステップでは、上記鍵生成部が、上記秘密鍵の元に対して上記第２論理情報の成分を係数とするスカラー倍を行う演算または上記秘密鍵の元に対して上記第２属性情報の成分を係数とするスカラー倍を行う演算を含む演算を行うことで上記復号鍵を求め、

上記復号部の上記復号処理に用いられる上記演算は、双線形性を有し、上記演算の結果が、双線形性に基づき上記暗号情報と上記復号鍵から取り出された上記第１論理情報と上記第２属性情報あるいは上記第１属性情報と上記第２論理情報の標準内積の結果に依存するように構成されている、

暗号通信方法。

[0486] ［アイテム２６］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以

下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおける暗号化装置であって、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵とを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化部と

を含む暗号化装置。

[0487] ［アイテム２７］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおける暗号化装置であって、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号情報を求める暗号化部と

を含む暗号化装置。

[0488] ［アイテム２８］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおける鍵生成装置であって、

上記ポリシー情報で特定される一方の変換規則情報とペアになってい

る他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成部とを含む鍵生成装置。

[0489] ［アイテム２９］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおける鍵生成装置であって、

上記ポリシー情報で特定される一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から生成された属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成部を含む鍵生成装置。

[0490] ［アイテム３０］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおける復号装置であって、

上記鍵生成装置が生成した復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号化装置が生成した暗号情報に対する復号処理を行う復号部

を含む復号装置。

[0491] ［アイテム３１］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれである

かを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおける復号装置であって、

上記ポリシー情報で特定される一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記鍵生成装置が生成した復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号化装置が生成した暗号情報に対する復号処理を行う復号部を含む復号装置。

[0492] ［アイテム３２］

アイテム２６またはアイテム２７に記載の暗号化装置としてコンピュータを機能させるためのプログラム。

[0493] ［アイテム３３］

アイテム２８またはアイテム２９に記載の鍵生成装置としてコンピュータを機能させるためのプログラム。

[0494] ［アイテム３４］

アイテム３０またはアイテム３１に記載の復号装置としてコンピュータを機能させるためのプログラム。

[0495] ［アイテム３５］

アイテム３２に記載のプログラム、アイテム３３に記載のプログラム、アイテム３４に記載のプログラムのうち少なくともいずれかを格納したコンピュータ読み取り可能な記憶媒体。

[0496] 第２の観点から本発明を総括すると、下記のとおりである。なお、アイテム番号をリセットして、１から順番にアイテム番号を割り当てる。

[0497] ［アイテム１］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、複数の復号装置とを含み、関数暗号を用いる暗号システムにおけ

る暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵とを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化ステップと、

上記暗号化装置の送信部が、上記暗号情報を第１の復号装置に送信する暗号情報送信ステップと、

上記第１の復号装置の受信部が、上記暗号化装置から上記暗号情報を受信する暗号情報受信ステップと、

上記鍵生成装置の第２命題論理情報取得部が、上記ポリシー情報で特

定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記第１の復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる第１の復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記第１の復号鍵を上記第１の復号装置に送信する復号鍵送信ステップと、

上記第１の復号装置の受信部が、上記鍵生成装置から上記第１の復号鍵を受信する復号鍵受信ステップと、

上記第１の復号装置の復号部が、上記第１の復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと、

上記第１の復号装置の転送部が、上記暗号情報を当該第１の復号装置以外の第２の復号装置に転送する転送ステップと、

上記第２の復号装置の受信部が、上記暗号情報を上記第１の復号装置から受信する受信ステップと、

上記鍵生成装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記第２の復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第３属性情報と言う）または論理情報（以下、第３論理情報と言う）を得る第３命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第３属性情報または上記第３論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる第２の復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記第２の復号鍵を上記第２の復号装置に送信する復号鍵送信ステップと、

上記第２の復号装置の受信部が、上記鍵生成装置から上記第２の復号鍵を受信する復号鍵受信ステップと、

上記第２の復号装置の復号部が、上記第２の復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと

を有する暗号通信方法。

[0498] ［アイテム２］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、複数の復号装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵とを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化ステップと、

上記暗号化装置の送信部が、上記暗号情報を第１の復号装置に送信する暗号情報送信ステップと、

上記第１の復号装置の受信部が、上記暗号化装置から上記暗号情報を受信する暗号情報受信ステップと、

上記第１の復号装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該第１の復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記第１の復号装置の送信部が、上記第２属性情報または上記第２論理情報を上記鍵生成装置に送信する論理情報送信ステップと、

上記鍵生成装置の受信部が、上記第１の復号装置から上記第２属性情報または上記第２論理情報を受信する論理情報受信ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる第１の復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記第１の復号鍵を上記第１の復号装置に送信する復号鍵送信ステップと、

上記第１の復号装置の受信部が、上記鍵生成装置から上記第１の復号鍵を受信する復号鍵受信ステップと、

上記第１の復号装置の復号部が、上記第１の復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと、

上記第１の復号装置の転送部が、上記暗号情報を当該第１の復号装置

以外の第２の復号装置に転送する転送ステップと、

上記第２の復号装置の受信部が、上記暗号情報を上記第１の復号装置から受信する受信ステップと、

上記第２の復号装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該第２の復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第３属性情報と言う）または論理情報（以下、第３論理情報と言う）を得る第３命題論理情報取得ステップと、

上記第２の復号装置の送信部が、上記第３属性情報または上記第３論理情報を上記鍵生成装置に送信する論理情報送信ステップと、

上記鍵生成装置の受信部が、上記第２の復号装置から上記第３属性情報または上記第３論理情報を受信する論理情報受信ステップと、

上記鍵生成装置の鍵生成部が、上記第３属性情報または上記第３論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる第２の復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記第２の復号鍵を上記第２の復号装置に送信する復号鍵送信ステップと、

上記第２の復号装置の受信部が、上記鍵生成装置から上記第２の復号鍵を受信する復号鍵受信ステップと、

上記第２の復号装置の復号部が、上記第２の復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと、

を有する暗号通信方法。

[0499] ［アイテム３］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、複数の復号装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め

定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号情報を求める暗号化ステップと、

上記暗号化装置の送信部が、上記暗号情報を第１の復号装置に送信する暗号情報送信ステップと、

上記第１の復号装置の受信部が、上記暗号化装置から上記暗号情報を受信する暗号情報受信ステップと、

上記鍵生成装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記第１の復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以

下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる第１の復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記第１の復号鍵を上記第１の復号装置に送信する復号鍵送信ステップと、

上記第１の復号装置の受信部が、上記鍵生成装置から上記第１の復号鍵を受信する復号鍵受信ステップと、

上記第１の復号装置の復号部が、上記第１の復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと、

上記第１の復号装置の転送部が、上記暗号情報を当該第１の復号装置以外の第２の復号装置に転送する転送ステップと、

上記第２の復号装置の受信部が、上記暗号情報を上記第１の復号装置から受信する受信ステップと、

上記鍵生成装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記第２の復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第３属性情報と言う）または論理情報（以下、第３論理情報と言う）を得る第３命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第３属性情報または上記第３論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる第２の復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記第２の復号鍵を上記第２の復号装置に送信する復号鍵送信ステップと、

上記第２の復号装置の受信部が、上記鍵生成装置から上記第２の復号鍵を受信する復号鍵受信ステップと、

上記第２の復号装置の復号部が、上記第２の復号鍵を用いて、関数暗

号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと

を有する暗号通信方法。

[0500] ［アイテム４］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、複数の復号装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号情報を求める暗号化ステップと、

上記暗号化装置の送信部が、上記暗号情報を第１の復号装置に送信する暗号情報送信ステップと、

上記第１の復号装置の受信部が、上記暗号化装置から上記暗号情報を受信する暗号情報受信ステップと、

上記第１の復号装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該第１の復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記第１の復号装置の送信部が、上記第２属性情報または上記第２論理情報を上記鍵生成装置に送信する論理情報送信ステップと、

上記鍵生成装置の受信部が、上記第１の復号装置から上記第２属性情報または上記第２論理情報を受信する論理情報受信ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる第１の復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記第１の復号鍵を上記第１の復号装置に送信する復号鍵送信ステップと、

上記第１の復号装置の受信部が、上記鍵生成装置から上記第１の復号鍵を受信する復号鍵受信ステップと、

上記第１の復号装置の復号部が、上記第１の復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと、

上記第１の復号装置の転送部が、上記暗号情報を当該第１の復号装置以外の第２の復号装置に転送する転送ステップと、

上記第２の復号装置の受信部が、上記暗号情報を上記第１の復号装置から受信する受信ステップと、

上記第２の復号装置の第２命題論理情報取得部が、上記ポリシー情報

で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該第２の復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第３属性情報と言う）または論理情報（以下、第３論理情報と言う）を得る第３命題論理情報取得ステップと、

上記第２の復号装置の送信部が、上記第３属性情報または上記第３論理情報を上記鍵生成装置に送信する論理情報送信ステップと、

上記鍵生成装置の受信部が、上記第２の復号装置から上記第３属性情報または上記第３論理情報を受信する論理情報受信ステップと、

上記鍵生成装置の鍵生成部が、上記第３属性情報または上記第３論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる第２の復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記第２の復号鍵を上記第２の復号装置に送信する復号鍵送信ステップと、

上記第２の復号装置の受信部が、上記鍵生成装置から上記第２の復号鍵を受信する復号鍵受信ステップと、

上記第２の復号装置の復号部が、上記第２の復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと、

を有する暗号通信方法。

[0501] ［アイテム５］

アイテム１またはアイテム２に記載の暗号通信方法において、

上記暗号化ステップは、上記暗号化部が上記共通鍵で平文を暗号化した暗号文も求める暗号文生成ステップを含み、

上記復号ステップは、上記復号部が、上記復号処理で得られた上記共通鍵を用いる上記暗号文の第２復号処理、または、上記復号処理で得られた上記共通鍵の生成に用いる上記情報から生成された共通鍵を用いる上記暗号文の第２復号処理を行う第２復号ステップを含む、

暗号通信方法。

[0502] ［アイテム６］

アイテム１からアイテム５のいずれかに記載の暗号通信方法において、

上記復号装置の取得部が、上記利用者に対応する上記属性指定情報および／または上記論理式指定情報を記憶する記憶媒体から、当該復号装置の利用者に対応する上記属性指定情報または上記論理式指定情報を取得する取得ステップ

を有する暗号通信方法。

[0503] ［アイテム７］

アイテム１またはアイテム３に記載の暗号通信方法において、

上記復号装置の送信部が、当該復号装置の利用者に対応する上記属性指定情報または上記論理式指定情報を上記鍵生成装置に送信するユーザ情報送信ステップと、

上記鍵生成装置の受信部が、上記復号装置から上記利用者に対応する上記属性指定情報または上記論理式指定情報を受信するユーザ情報受信ステップと

を有する暗号通信方法。

[0504] ［アイテム８］

アイテム１からアイテム６のいずれかに記載の暗号通信方法において、

上記暗号システムは、上記利用者に対応する上記属性指定情報および／または上記論理式指定情報を記憶する記憶部を備える、一つまたは複数のユーザ情報管理装置を含んでおり、

上記鍵生成装置のユーザ情報取得部が、上記復号装置の利用者に対応する上記属性指定情報または上記論理式指定情報を上記ユーザ情報管理装置から取得するユーザ情報取得ステップと

を有する暗号通信方法。

[0505] ［アイテム９］

アイテム１からアイテム８のいずれかに記載の暗号通信方法において、

各上記鍵生成装置につき一つまたは複数の上記変換規則情報ペアが予め定められており、

上記暗号システムは、各上記鍵生成装置に対応する各上記変換規則情報ペアを記憶する記憶部を備える、一つまたは複数の変換規則情報ペア管理装置を含んでおり、

上記暗号化装置の変換規則情報ペア取得部が、上記変換規則情報ペア管理装置から上記変換規則情報ペアを取得する変換規則情報ペア取得ステップと、

上記復号装置の変換規則情報ペア取得部が、上記変換規則情報ペア管理装置から上記変換規則情報ペアを取得する変換規則情報ペア取得ステップと

を有する暗号通信方法。

[0506] ［アイテム１０］

アイテム１からアイテム９のいずれかに記載の暗号通信方法において、

上記ポリシー情報の特定対象が上記属性用変換規則情報のみ、あるいは、上記論理式用変換規則情報のみ、あるいは、上記属性用変換規則情報および上記論理式用変換規則情報であることが、上記鍵生成装置ごとに予め定められている、

暗号通信方法。

[0507] ［アイテム１１］

アイテム１からアイテム１０のいずれかに記載の暗号通信方法において、

代数構造Ｋを有限環または有限体として、

上記第１、第２属性情報ならびに上記第１、第２論理情報は、上記Ｋの元を成分とするベクトルであり、

上記復号ステップでは、上記復号部が、上記暗号情報と上記復号鍵を入力とし、上記第１論理情報と上記第２属性情報との標準内積または上記第１属性情報と上記第２論理情報との標準内積の結果に依存する演算を行う、暗号通信方法。

[0508] ［アイテム１２］

アイテム１１に記載の暗号通信方法において、

上記公開鍵は、Ｋ上の加群Ｖの元の集合であり、

上記秘密鍵は、上記加群Ｖの双対加群Ｖ*の元の集合であり、

上記復号鍵は、上記双対加群Ｖ*の元であり、

上記暗号化ステップでは、上記暗号化部が、上記公開鍵の元に対して上記第１属性情報の成分を係数とするスカラー倍を行う演算または上記公開鍵の元に対して上記第１論理情報の成分を係数とするスカラー倍を行う演算を含む演算を行うことで上記暗号情報を求め、

上記鍵生成ステップでは、上記鍵生成部が、上記秘密鍵の元に対して上記第２論理情報の成分を係数とするスカラー倍を行う演算または上記秘密鍵の元に対して上記第２属性情報の成分を係数とするスカラー倍を行う演算を含む演算を行うことで上記復号鍵を求め、

上記復号部の上記復号処理に用いられる上記演算は、双線形性を有し、上記演算の結果が、双線形性に基づき上記暗号情報と上記復号鍵から取り出された上記第１論理情報と上記第２属性情報あるいは上記第１属性情報と上記第２論理情報の標準内積の結果に依存するように構成されている、

暗号通信方法。

[0509] ［アイテム１３］

関数暗号を用いる暗号システムであって、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵とを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化部とを含み、

上記鍵生成装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成部とを含み

、

上記復号装置は、

上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号部と、

上記暗号情報を当該復号装置以外の一つ以上の復号装置に転送する転送部とを含む、

暗号システム。

[0510] ［アイテム１４］

関数暗号を用いる暗号システムであって、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理

情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵とを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化部とを含み、

上記復号装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記鍵生成装置から送られた復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号部と、

上記暗号情報を当該復号装置以外の一つ以上の復号装置に転送する転送部とを含み、

上記鍵生成装置は、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成部とを含む、

暗号システム。

[0511] ［アイテム１５］

関数暗号を用いる暗号システムであって、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報

（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号情報を求める暗号化部とを含み、

上記鍵生成装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成部とを含み、

上記復号装置は、

上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対す

る復号処理を行う復号部と、

上記暗号情報を当該復号装置以外の一つ以上の復号装置に転送する転送部とを含む、

暗号システム。

[0512] ［アイテム１６］

関数暗号を用いる暗号システムであって、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号

情報を求める暗号化部とを含み、

上記復号装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記鍵生成装置から送られた復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号部と、

上記暗号情報を当該復号装置以外の一つ以上の復号装置に転送する転送部とを含み、

上記鍵生成装置は、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成部とを含む、

暗号システム。

[0513] ［アイテム１７］

アイテム１３またはアイテム１４に記載の暗号システムにおいて、

上記暗号化装置の上記暗号化部は、上記共通鍵で平文を暗号化した暗号文も求め、

上記復号装置の上記復号部は、上記復号処理で得られた上記共通鍵を用いる上記暗号文の第２復号処理、または、上記復号処理で得られた上記共通鍵の生成に用いる上記情報から生成された共通鍵を用いる上記暗号文の第２復号処理も行う、

暗号システム。

[0514] ［アイテム１８］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおける復号装置であって、

上記鍵生成装置が生成した復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号化装置が生成した暗号情報に対する復号処理を行う復号部と、

上記暗号情報を当該復号装置以外の一つ以上の復号装置に転送する転送部と

を含む復号装置。

[0515] ［アイテム１９］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおける復号装置であって、

上記ポリシー情報で特定される一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記鍵生成装置が生成した復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号化装置が生成した暗号情報に対する復号処理を行う復号部と、

上記暗号情報を当該復号装置以外の一つ以上の復号装置に転送する転送部と

を含む復号装置。

[0516] ［アイテム２０］

アイテム１８またはアイテム１９に記載の復号装置としてコンピュータを機能させるためのプログラム。

[0517] ［アイテム２１］

アイテム２０に記載のプログラムを格納したコンピュータ読み取り可能な記憶媒体。

[0518] 第３の観点から本発明を総括すると、下記のとおりである。なお、アイテム番号をリセットして、１から順番にアイテム番号を割り当てる。

[0519] ［アイテム１］

関数暗号を用いる暗号システムであって、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、コンテンツとを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報と、当該共通鍵で当該コンテンツを暗号化した暗号化コンテンツとを求める暗号化部とを含み、

上記コンテンツサーバ装置は、

各上記暗号化装置から送られた上記暗号情報および上記暗号化コンテンツを記憶する記憶部と、

上記復号装置からの要求に応じて上記暗号化コンテンツとこれに対応する上記暗号情報を当該復号装置に送信する送信部とを含み、

上記鍵生成装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになってい

る他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成部とを含み、

上記復号装置は、

ブラウザ部と中継部とを含み、

上記ブラウザ部は、上記コンテンツサーバ装置に対する上記暗号化コンテンツの取得要求処理を行い、上記暗号化コンテンツから復号されたコンテンツを表示し、

上記中継部は、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信し、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号情報に対する復号処理と、当該復号処理で得られた上記共通鍵を用いて、上記コンテンツサーバ装置から取得した上記暗号化コンテンツを復号するコンテンツ取得処理を行う、

暗号システム。

[0520] ［アイテム２］

関数暗号を用いる暗号システムであって、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変

換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、コンテンツとを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報と、当該共通鍵で当該コンテンツを暗号化した暗号化コンテンツとを求める暗号化部とを含み、

上記コンテンツサーバ装置は、

各上記暗号化装置から送られた上記暗号情報および上記暗号化コンテンツを記憶する記憶部と、

上記復号装置からの要求に応じて上記暗号化コンテンツとこれに対応する上記暗号情報を当該復号装置に送信する送信部とを含み、

上記復号装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、ブラウザ部と、中継部とを含み、

上記ブラウザ部は、上記コンテンツサーバ装置に対する上記暗号化コンテンツの取得要求処理を行い、上記暗号化コンテンツから復号されたコンテンツを表示し、

上記中継部は、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信し、上記鍵生成装置から送られた復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号情報に対する復号処理と、当該復号処理で得られた上記共通鍵を用いて、上記コンテンツサーバ装置から取得した上記暗号化コンテンツを復号するコンテンツ取得処理を行い、

上記鍵生成装置は、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成部とを含む、

暗号システム。

[0521] ［アイテム３］

関数暗号を用いる暗号システムであって、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれで

あるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、コンテンツとを用いて、関数暗号アルゴリズムに則り、当該コンテンツを暗号化した暗号化コンテンツを求める暗号化部とを含み、

上記コンテンツサーバ装置は、

各上記暗号化装置から送られた上記暗号化コンテンツを記憶する記憶部と、

上記復号装置からの要求に応じて上記暗号化コンテンツを当該復号装置に送信する送信部とを含み、

上記鍵生成装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号化コンテンツの復号に用いる復号鍵を生成する鍵生成部とを含み、

上記復号装置は、

ブラウザ部と中継部とを含み、

上記ブラウザ部は、上記コンテンツサーバ装置に対する上記暗号化コンテ

ンツの取得要求処理を行い、上記暗号化コンテンツから復号されたコンテンツを表示し、

上記中継部は、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信し、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号化コンテンツに対する復号処理を行う、

暗号システム。

[0522] ［アイテム４］

関数暗号を用いる暗号システムであって、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理

情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、コンテンツとを用いて、関数暗号アルゴリズムに則り、当該コンテンツを暗号化した暗号化コンテンツを求める暗号化部とを含み、

上記コンテンツサーバ装置は、

各上記暗号化装置から送られた上記暗号化コンテンツを記憶する記憶部と、

上記復号装置からの要求に応じて上記暗号化コンテンツを当該復号装置に送信する送信部とを含み、

上記復号装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、ブラウザ部と、中継部とを含み、

上記ブラウザ部は、上記コンテンツサーバ装置に対する上記暗号化コンテンツの取得要求処理を行い、上記暗号化コンテンツから復号されたコンテンツを表示し、

上記中継部は、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信し、上記鍵生成装置から送られた復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号化コンテンツに対する復号処理を行い、

上記鍵生成装置は、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号化コンテンツの復号に用いる復号鍵を生成する鍵生成部とを含む、

暗号システム。

[0523] ［アイテム５］

アイテム１からアイテム４のいずれかに記載の暗号システムにおいて、

上記利用者に対応する上記属性指定情報および／または上記論理式指定情報は記憶媒体に記憶されており、

上記復号装置は、当該復号装置の利用者に対応する上記属性指定情報または上記論理式指定情報を上記記憶媒体から取得するユーザ情報取得部を含む、

暗号システム。

[0524] ［アイテム６］

アイテム１またはアイテム３に記載の暗号システムにおいて、

上記鍵生成装置が用いる、上記復号装置の利用者に対応する上記属性指定情報または上記論理式指定情報は、上記復号装置から取得した情報である、

暗号システム。

[0525] ［アイテム７］

アイテム１からアイテム６のいずれかに記載の暗号システムにおいて、

上記暗号システムは、一つまたは複数のユーザ情報管理装置をさらに含み、

各上記ユーザ情報管理装置は、上記利用者に対応する上記属性指定情報および／または上記論理式指定情報を記憶する記憶部を含み、

上記鍵生成装置は、上記復号装置の利用者に対応する上記属性指定情報または上記論理式指定情報を上記ユーザ情報管理装置から取得するユーザ情報取得部を含む、

暗号システム。

[0526] ［アイテム８］

アイテム１からアイテム７のいずれかに記載の暗号システムにおいて、

各上記鍵生成装置につき一つまたは複数の上記変換規則情報ペアが予め定められており、

上記暗号システムは、一つまたは複数の変換規則情報ペア管理装置をさらに含み、

各上記変換規則情報ペア管理装置は、各上記鍵生成装置に対応する各上記変換規則情報ペアを記憶する記憶部を含み、

上記暗号化装置は、上記変換規則情報ペア管理装置から上記変換規則情報ペアを取得する変換規則情報ペア取得部を含み、

上記復号装置は、上記変換規則情報ペア管理装置から上記変換規則情報ペアを取得する変換規則情報ペア取得部を含む、

暗号システム。

[0527] ［アイテム９］

アイテム１からアイテム７のいずれかに記載の暗号システムにおいて、

各上記鍵生成装置につき一つまたは複数の上記変換規則情報ペアが予め定められており、

各上記鍵生成装置は、当該鍵生成装置に対応する各上記変換規則情報ペアを記憶する記憶部をさらに含み、

各上記暗号化装置は、少なくとも一つ以上の上記鍵生成装置に対応する各上記変換規則情報ペアを記憶する記憶部をさらに含み、

各上記復号装置は、少なくとも一つ以上の上記鍵生成装置に対応する各上記変換規則情報ペアを記憶する記憶部をさらに含む、

暗号システム。

[0528] ［アイテム１０］

アイテム１からアイテム９のいずれかに記載の暗号システムにおいて、

上記ポリシー情報の特定対象が上記属性用変換規則情報のみ、あるいは、上記論理式用変換規則情報のみ、あるいは、上記属性用変換規則情報お

よび上記論理式用変換規則情報であることが、上記鍵生成装置ごとに予め定められている、

暗号システム。

[0529] ［アイテム１１］

アイテム１からアイテム１０のいずれかに記載の暗号システムにおいて、

代数構造Ｋを有限環または有限体として、

上記第１、第２属性情報ならびに上記第１、第２論理情報は、上記Ｋの元を成分とするベクトルであり、

上記復号部の上記復号処理では、上記第１論理情報と上記第２属性情報との標準内積または上記第１属性情報と上記第２論理情報との標準内積の結果に依存する演算が行われる、

暗号システム。

[0530] ［アイテム１２］

アイテム１１に記載の暗号システムにおいて、

上記公開鍵は、Ｋ上の加群Ｖの元の集合であり、

上記秘密鍵は、上記加群Ｖの双対加群Ｖ*の元の集合であり、

上記復号鍵は、上記双対加群Ｖ*の元であり、

上記暗号化部は、上記公開鍵の元に対して上記第１属性情報の成分を係数とするスカラー倍を行う演算または上記公開鍵の元に対して上記第１論理情報の成分を係数とするスカラー倍を行う演算を含む演算を行うことで上記暗号情報を求め、

上記鍵生成部は、上記秘密鍵の元に対して上記第２論理情報の成分を係数とするスカラー倍を行う演算または上記秘密鍵の元に対して上記第２属性情報の成分を係数とするスカラー倍を行う演算を含む演算を行うことで上記復号鍵を求め、

上記復号部の上記復号処理に用いられる上記演算は、双線形性を有し、上記演算の結果が、双線形性に基づき上記暗号情報または上記暗号化コン

テンツと上記復号鍵から取り出された上記第１論理情報と上記第２属性情報あるいは上記第１属性情報と上記第２論理情報の標準内積の結果に依存するように構成されている、

暗号システム。

[0531] ［アイテム１３］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理

情報と、上記鍵生成装置の公開鍵と、コンテンツとを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報と、当該共通鍵で当該コンテンツを暗号化した暗号化コンテンツとを求める暗号化ステップと、

上記暗号化装置の送信部が、上記暗号化コンテンツとこれに対応する上記暗号情報を上記コンテンツサーバ装置に送信する送信ステップと、

上記コンテンツサーバ装置の記憶部が、各上記暗号化装置から送られた上記暗号情報と上記暗号化コンテンツを記憶する記憶ステップと、

上記復号装置のブラウザ部が、上記コンテンツサーバ装置に対する上記暗号化コンテンツの取得要求処理を行う取得要求処理ステップと、

上記復号装置の中継部が、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信する送信ステップと、

上記コンテンツサーバ装置の送信部が、上記復号装置からの要求に応じて上記暗号化コンテンツとこれに対応する上記暗号情報を当該復号装置に送信する送信ステップと、

上記復号装置の受信部が、上記コンテンツサーバ装置から上記暗号化コンテンツと上記暗号情報を受信する受信ステップと、

上記鍵生成装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記復号鍵を上記復号装置に送信する復号鍵送信ステップと、

上記復号装置の受信部が、上記鍵生成装置から上記復号鍵を受信する

復号鍵受信ステップと、

上記復号装置の中継部が、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号情報に対する復号処理と、当該復号処理で得られた上記共通鍵を用いて、上記コンテンツサーバ装置から取得した上記暗号化コンテンツを復号するコンテンツ取得処理を行う復号ステップと、

上記復号装置のブラウザ部が、上記暗号化コンテンツから復号されたコンテンツを表示する表示ステップと

を有する暗号通信方法。

[0532] ［アイテム１４］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性

指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、コンテンツとを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報と、当該共通鍵で当該コンテンツを暗号化した暗号化コンテンツとを求める暗号化ステップと、

上記暗号化装置の送信部が、上記暗号化コンテンツとこれに対応する上記暗号情報を上記コンテンツサーバ装置に送信する送信ステップと、

上記コンテンツサーバ装置の記憶部が、各上記暗号化装置から送られた上記暗号情報および上記暗号化コンテンツを記憶する記憶ステップと、

上記復号装置のブラウザ部が、上記コンテンツサーバ装置に対する上記暗号化コンテンツの取得要求処理を行う取得要求処理ステップと、

上記復号装置の中継部が、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信する送信ステップと、

上記コンテンツサーバ装置の送信部が、上記復号装置からの要求に応じて上記暗号化コンテンツとこれに対応する上記暗号情報を当該復号装置に送信する送信ステップと、

上記復号装置の受信部が、上記コンテンツサーバ装置から上記暗号化コンテンツと上記暗号情報を受信する受信ステップと、

上記復号装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記復号装置の送信部が、上記第２属性情報または上記第２論理情報

を上記鍵生成装置に送信する論理情報送信ステップと、

上記鍵生成装置の受信部が、上記復号装置から上記第２属性情報または上記第２論理情報を受信する論理情報受信ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記復号鍵を上記復号装置に送信する復号鍵送信ステップと、

上記復号装置の受信部が、上記鍵生成装置から上記復号鍵を受信する復号鍵受信ステップと、

上記復号装置の中継部が、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号情報に対する復号処理と、当該復号処理で得られた上記共通鍵を用いて、上記コンテンツサーバ装置から取得した上記暗号化コンテンツを復号するコンテンツ取得処理を行う復号ステップと、

上記復号装置のブラウザ部が、上記暗号化コンテンツから復号されたコンテンツを表示する表示ステップと

を有する暗号通信方法。

[0533] ［アイテム１５］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理

式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、コンテンツとを用いて、関数暗号アルゴリズムに則り、当該コンテンツを暗号化した暗号化コンテンツを求める暗号化ステップと、

上記暗号化装置の送信部が、上記暗号化コンテンツを上記コンテンツサーバ装置に送信する送信ステップと、

上記コンテンツサーバ装置の記憶部が、各上記暗号化装置から送られた上記暗号化コンテンツを記憶する記憶ステップと、

上記復号装置のブラウザ部が、上記コンテンツサーバ装置に対する上記暗号化コンテンツの取得要求処理を行う取得要求処理ステップと、

上記復号装置の中継部が、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信する送信ステップと、

上記コンテンツサーバ装置の送信部が、上記復号装置からの要求に応じて上記暗号化コンテンツを当該復号装置に送信する送信ステップと、

上記復号装置の受信部が、上記コンテンツサーバ装置から上記暗号化

コンテンツを受信する受信ステップと、

上記鍵生成装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号化コンテンツの復号に用いる復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記復号鍵を上記復号装置に送信する復号鍵送信ステップと、

上記復号装置の受信部が、上記鍵生成装置から上記復号鍵を受信する復号鍵受信ステップと、

上記復号装置の中継部が、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号化コンテンツに対する復号処理を行う復号ステップと、

上記復号装置のブラウザ部が、上記暗号化コンテンツから復号されたコンテンツを表示する表示ステップと

を有する暗号通信方法。

[0534] ［アイテム１６］

少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報

（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、コンテンツとを用いて、関数暗号アルゴリズムに則り、当該コンテンツを暗号化した暗号化コンテンツを求める暗号化ステップと、

上記暗号化装置の送信部が、上記暗号化コンテンツを上記コンテンツサーバ装置に送信する送信ステップと、

上記コンテンツサーバ装置の記憶部が、各上記暗号化装置から送られた上記暗号化コンテンツを記憶する記憶ステップと、

上記復号装置のブラウザ部が、上記コンテンツサーバ装置に対する上記暗号化コンテンツの取得要求処理を行う取得要求処理ステップと、

上記復号装置の中継部が、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信する送信ステップと、

上記コンテンツサーバ装置の送信部が、上記復号装置からの要求に応じて上記暗号化コンテンツを当該復号装置に送信する送信ステップと、

上記復号装置の受信部が、上記コンテンツサーバ装置から上記暗号化コンテンツを受信する受信ステップと、

上記復号装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記復号装置の送信部が、上記第２属性情報または上記第２論理情報を上記鍵生成装置に送信する論理情報送信ステップと、

上記鍵生成装置の受信部が、上記復号装置から上記第２属性情報または上記第２論理情報を受信する論理情報受信ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号化コンテンツの復号に用いる復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記復号鍵を上記復号装置に送信する復号鍵送信ステップと、

上記復号装置の受信部が、上記鍵生成装置から上記復号鍵を受信する復号鍵受信ステップと、

上記復号装置の中継部が、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号化コンテンツに対する復号処理を行う復号ステップと、

上記復号装置のブラウザ部が、上記暗号化コンテンツから復号されたコンテンツを表示する表示ステップと

を有する暗号通信方法。

[0535] ［アイテム１７］

少なくとも、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報と、当該共通鍵でコンテンツを暗号化した暗号化コンテンツとを求める、一つまたは複数の暗号

化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、上記暗号化コンテンツと上記暗号情報を記憶している一つまたは複数のコンテンツサーバ装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおける復号装置であって、

ブラウザ部と中継部とを含み、

上記ブラウザ部は、上記コンテンツサーバ装置に対する上記暗号化コンテンツの取得要求処理を行い、上記暗号化コンテンツから復号されたコンテンツを表示し、

上記中継部は、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信し、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号情報に対する復号処理と、当該復号処理で得られた上記共通鍵を用いて、上記コンテンツサーバ装置から取得した上記暗号化コンテンツを復号するコンテンツ取得処理を行う、

復号装置。

[0536] ［アイテム１８］

少なくとも、関数暗号アルゴリズムに則り、コンテンツを暗号化した暗号化コンテンツを求める、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、上記暗号化コンテンツを

記憶している一つまたは複数のコンテンツサーバ装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおける復号装置であって、

ブラウザ部と中継部とを含み、

上記ブラウザ部は、上記コンテンツサーバ装置に対する上記暗号化コンテンツの取得要求処理を行い、上記暗号化コンテンツから復号されたコンテンツを表示し、

上記中継部は、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信し、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号化コンテンツに対する復号処理を行う、

復号装置。

[0537] ［アイテム１９］

少なくとも、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報と、当該共通鍵でコンテンツを暗号化した暗号化コンテンツとを求める一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定め

られており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおけるコンテンツサーバ装置であって、

各上記暗号化装置から送られた上記暗号情報および上記暗号化コンテンツを記憶する記憶部と、

上記復号装置からの要求に応じて上記暗号化コンテンツとこれに対応する上記暗号情報を当該復号装置に送信する送信部と

を含むコンテンツサーバ装置。

[0538] ［アイテム２０］

少なくとも、関数暗号アルゴリズムに則り、コンテンツを暗号化した暗号化コンテンツを求める一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおけるコンテンツサーバ装置であって、

各上記暗号化装置から送られた上記暗号化コンテンツを記憶する記憶部と、

上記復号装置からの要求に応じて上記暗号化コンテンツを当該復号装置に送信する送信部と

を含むコンテンツサーバ装置。

[0539] ［アイテム２１］

アイテム１７またはアイテム１８に記載の復号装置としてコンピュータを機能させるためのプログラム。

[0540] ［アイテム２２］

アイテム１９またはアイテム２０に記載のコンテンツサーバ装置としてコンピュータを機能させるためのプログラム。

[0541] ［アイテム２３］

アイテム２１に記載のプログラムおよび／またはアイテム２２に記載のプログラムを格納したコンピュータ読み取り可能な記憶媒体。

請求の範囲

［請求項1］ 関数暗号を用いる暗号システムであって、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵とを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化部とを含み、

上記鍵生成装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成部とを含み、

上記復号装置は、

上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号部を含む、

暗号システム。

［請求項2］ 関数暗号を用いる暗号システムであって、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペア

に含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵とを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化部とを含み、

上記復号装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記鍵生成装置から送られた復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号部を含み、

上記鍵生成装置は、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成部とを含む、

暗号システム。

［請求項3］ 関数暗号を用いる暗号システムであって、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号情報を求める暗号化部とを含み、

上記鍵生成装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生

成部とを含み、

上記復号装置は、

上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号部を含む、

暗号システム。

[請求項4] 関数暗号を用いる暗号システムであって、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公

開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号情報を求める暗号化部とを含み、

上記復号装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記鍵生成装置から送られた復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号部を含み、

上記鍵生成装置は、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成部とを含む、

暗号システム。

［請求項5］ 請求項１に記載の暗号システムにおいて、

上記暗号化装置の上記暗号化部は、上記共通鍵で平文を暗号化した暗号文も求め、

上記復号装置の上記復号部は、上記復号処理で得られた上記共通鍵を用いる上記暗号文の第２復号処理、または、上記復号処理で得られた上記共通鍵の生成に用いる上記情報から生成された共通鍵を用いる上記暗号文の第２復号処理も行う、

暗号システム。

［請求項6］ 請求項２に記載の暗号システムにおいて、

上記暗号化装置の上記暗号化部は、上記共通鍵で平文を暗号化した暗号文も求め、

上記復号装置の上記復号部は、上記復号処理で得られた上記共通鍵を用いる上記暗号文の第２復号処理、または、上記復号処理で得

られた上記共通鍵の生成に用いる上記情報から生成された共通鍵を用いる上記暗号文の第２復号処理も行う、暗号システム。

[請求項7] 請求項１から請求項６のいずれかに記載の暗号システムにおいて、

上記暗号システムは、複数の上記復号装置を含み、

複数の上記復号装置のうち少なくとも一つの上記復号装置は、当該復号装置以外の一つ以上の復号装置に上記暗号情報を転送する転送部をさらに含む

暗号システム。

[請求項8] 関数暗号を用いる暗号システムであって、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報

のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、コンテンツとを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報と、当該共通鍵で当該コンテンツを暗号化した暗号化コンテンツとを求める暗号化部とを含み、

上記コンテンツサーバ装置は、

各上記暗号化装置から送られた上記暗号情報および上記暗号化コンテンツを記憶する記憶部と、

上記復号装置からの要求に応じて上記暗号化コンテンツとこれに対応する上記暗号情報を当該復号装置に送信する送信部とを含み、

上記鍵生成装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成部とを含み、

上記復号装置は、

ブラウザ部と中継部とを含み、

上記ブラウザ部は、上記コンテンツサーバ装置に対する上記暗号化コンテンツの取得要求処理を行い、上記暗号化コンテンツから復号されたコンテンツを表示し、

上記中継部は、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信し、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号情報に対する復号処理と、当該復号処理で得られた上記共通鍵を用いて、上記コンテンツサーバ装置から取得した上記暗号化コンテンツを復号するコンテンツ取得処理を行う、

暗号システム。

[請求項9] 関数暗号を用いる暗号システムであって、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、

第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、コンテンツとを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報と、当該共通鍵で当該コンテンツを暗号化した暗号化コンテンツとを求める暗号化部とを含み、

上記コンテンツサーバ装置は、

各上記暗号化装置から送られた上記暗号情報および上記暗号化コンテンツを記憶する記憶部と、

上記復号装置からの要求に応じて上記暗号化コンテンツとこれに対応する上記暗号情報を当該復号装置に送信する送信部とを含み、

上記復号装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、ブラウザ部と、中継部とを含み、

上記ブラウザ部は、上記コンテンツサーバ装置に対する上記暗号化コンテンツの取得要求処理を行い、上記暗号化コンテンツから復号されたコンテンツを表示し、

上記中継部は、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信し、上記鍵生成装置から送られた復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号情報に対する復号処理と、当該復号処理で得られた上記共通鍵を用いて、上記コンテンツサーバ装置から取得した上記暗号化コンテンツを復号するコンテンツ取得処理を行い、

上記鍵生成装置は、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成部とを含む、

暗号システム。

［請求項10］ 関数暗号を用いる暗号システムであって、少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公

開鍵と、コンテンツとを用いて、関数暗号アルゴリズムに則り、当該コンテンツを暗号化した暗号化コンテンツを求める暗号化部とを含み、

上記コンテンツサーバ装置は、

各上記暗号化装置から送られた上記暗号化コンテンツを記憶する記憶部と、

上記復号装置からの要求に応じて上記暗号化コンテンツを当該復号装置に送信する送信部とを含み、

上記鍵生成装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号化コンテンツの復号に用いる復号鍵を生成する鍵生成部とを含み、

上記復号装置は、

ブラウザ部と中継部とを含み、

上記ブラウザ部は、上記コンテンツサーバ装置に対する上記暗号化コンテンツの取得要求処理を行い、上記暗号化コンテンツから復号されたコンテンツを表示し、

上記中継部は、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信し、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号化コンテンツに対する復号処理を行う、

暗号システム。

［請求項11］ 関数暗号を用いる暗号システムであって、少なくとも、一つま

たは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置は、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、コンテンツとを用いて、関数暗号アルゴリズムに則り、当該コンテンツを暗号化した暗号化コンテンツを求める暗号化部とを含み、

上記コンテンツサーバ装置は、

各上記暗号化装置から送られた上記暗号化コンテンツを記憶する記

憶部と、

上記復号装置からの要求に応じて上記暗号化コンテンツを当該復号装置に送信する送信部とを含み、

上記復号装置は、

上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、ブラウザ部と、中継部とを含み、

上記ブラウザ部は、上記コンテンツサーバ装置に対する上記暗号化コンテンツの取得要求処理を行い、上記暗号化コンテンツから復号されたコンテンツを表示し、

上記中継部は、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信し、上記鍵生成装置から送られた復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号化コンテンツに対する復号処理を行い、

上記鍵生成装置は、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号化コンテンツの復号に用いる復号鍵を生成する鍵生成部とを含む、

暗号システム。

［請求項12］ 少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定

している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵とを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化ステップと、

上記鍵生成装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成ステップと、

上記復号装置の復号部が、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと

を有する暗号通信方法。

[請求項13] 少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵とを用いて、関数暗号アルゴ

リズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化ステップと、

上記復号装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成ステップと、

上記復号装置の復号部が、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと

を有する暗号通信方法。

［請求項14］ 少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちい

ずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号情報を求める暗号化ステップと、

上記鍵生成装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成ステップと、

上記復号装置の復号部が、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと

を有する暗号通信方法。

［請求項15］ 少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、関数暗号を用

いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号情報を求める暗号化ステップと、

上記復号装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）ま

たは論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成ステップと、

上記復号装置の復号部が、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと

を有する暗号通信方法。

［請求項16］ 少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、複数の復号装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則

情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵とを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化ステップと、

上記暗号化装置の送信部が、上記暗号情報を第１の復号装置に送信する暗号情報送信ステップと、

上記第１の復号装置の受信部が、上記暗号化装置から上記暗号情報を受信する暗号情報受信ステップと、

上記鍵生成装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記第１の復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる第１の復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記第１の復号鍵を上記第１の復号装置に送信する復号鍵送信ステップと、

上記第１の復号装置の受信部が、上記鍵生成装置から上記第１の復号鍵を受信する復号鍵受信ステップと、

上記第１の復号装置の復号部が、上記第１の復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと、

上記第１の復号装置の転送部が、上記暗号情報を当該第１の復

号装置以外の第２の復号装置に転送する転送ステップと、

上記第２の復号装置の受信部が、上記暗号情報を上記第１の復号装置から受信する受信ステップと、

上記鍵生成装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記第２の復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第３属性情報と言う）または論理情報（以下、第３論理情報と言う）を得る第３命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第３属性情報または上記第３論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる第２の復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記第２の復号鍵を上記第２の復号装置に送信する復号鍵送信ステップと、

上記第２の復号装置の受信部が、上記鍵生成装置から上記第２の復号鍵を受信する復号鍵受信ステップと、

上記第２の復号装置の復号部が、上記第２の復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと

を有する暗号通信方法。

［請求項17］ 少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、複数の復号装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定す

る情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵とを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化ステップと、

上記暗号化装置の送信部が、上記暗号情報を第１の復号装置に送信する暗号情報送信ステップと、

上記第１の復号装置の受信部が、上記暗号化装置から上記暗号情報を受信する暗号情報受信ステップと、

上記第１の復号装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該第１の復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記第１の復号装置の送信部が、上記第２属性情報または上記第２論理情報を上記鍵生成装置に送信する論理情報送信ステップと、

上記鍵生成装置の受信部が、上記第１の復号装置から上記第２属性情報または上記第２論理情報を受信する論理情報受信ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる第１の復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記第１の復号鍵を上記第１の復号装置に送信する復号鍵送信ステップと、

上記第１の復号装置の受信部が、上記鍵生成装置から上記第１の復号鍵を受信する復号鍵受信ステップと、

上記第１の復号装置の復号部が、上記第１の復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと、

上記第１の復号装置の転送部が、上記暗号情報を当該第１の復号装置以外の第２の復号装置に転送する転送ステップと、

上記第２の復号装置の受信部が、上記暗号情報を上記第１の復号装置から受信する受信ステップと、

上記第２の復号装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該第２の復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第３属性情報と言う）または論理情報（以下、第３論理情報と言う）を得る第３命題論理情報取得ステップと、

上記第２の復号装置の送信部が、上記第３属性情報または上記第３論理情報を上記鍵生成装置に送信する論理情報送信ステップと、

上記鍵生成装置の受信部が、上記第２の復号装置から上記第３

属性情報または上記第３論理情報を受信する論理情報受信ステップと、

上記鍵生成装置の鍵生成部が、上記第３属性情報または上記第３論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる第２の復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記第２の復号鍵を上記第２の復号装置に送信する復号鍵送信ステップと、

上記第２の復号装置の受信部が、上記鍵生成装置から上記第２の復号鍵を受信する復号鍵受信ステップと、

上記第２の復号装置の復号部が、上記第２の復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと、

を有する暗号通信方法。

［請求項18］ 少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、複数の復号装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情

報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号情報を求める暗号化ステップと、

上記暗号化装置の送信部が、上記暗号情報を第１の復号装置に送信する暗号情報送信ステップと、

上記第１の復号装置の受信部が、上記暗号化装置から上記暗号情報を受信する暗号情報受信ステップと、

上記鍵生成装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記第１の復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる第１の復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記第１の復号鍵を上記第１の復号装置に送信する復号鍵送信ステップと、

上記第１の復号装置の受信部が、上記鍵生成装置から上記第１の復号鍵を受信する復号鍵受信ステップと、

上記第１の復号装置の復号部が、上記第１の復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと、

上記第１の復号装置の転送部が、上記暗号情報を当該第１の復号装置以外の第２の復号装置に転送する転送ステップと、

上記第２の復号装置の受信部が、上記暗号情報を上記第１の復号装置から受信する受信ステップと、

上記鍵生成装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記第２の復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第３属性情報と言う）または論理情報（以下、第３論理情報と言う）を得る第３命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第３属性情報または上記第３論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる第２の復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記第２の復号鍵を上記第２の復号装置に送信する復号鍵送信ステップと、

上記第２の復号装置の受信部が、上記鍵生成装置から上記第２の復号鍵を受信する復号鍵受信ステップと、

上記第２の復号装置の復号部が、上記第２の復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと

を有する暗号通信方法。

［請求項19］ 少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、複数の復号装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵

が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号情報を求める暗号化ステップと、

上記暗号化装置の送信部が、上記暗号情報を第１の復号装置に送信する暗号情報送信ステップと、

上記第１の復号装置の受信部が、上記暗号化装置から上記暗号情報を受信する暗号情報受信ステップと、

上記第１の復号装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方

の変換規則情報を用いて、当該第１の復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記第１の復号装置の送信部が、上記第２属性情報または上記第２論理情報を上記鍵生成装置に送信する論理情報送信ステップと、

上記鍵生成装置の受信部が、上記第１の復号装置から上記第２属性情報または上記第２論理情報を受信する論理情報受信ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる第１の復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記第１の復号鍵を上記第１の復号装置に送信する復号鍵送信ステップと、

上記第１の復号装置の受信部が、上記鍵生成装置から上記第１の復号鍵を受信する復号鍵受信ステップと、

上記第１の復号装置の復号部が、上記第１の復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと、

上記第１の復号装置の転送部が、上記暗号情報を当該第１の復号装置以外の第２の復号装置に転送する転送ステップと、

上記第２の復号装置の受信部が、上記暗号情報を上記第１の復号装置から受信する受信ステップと、

上記第２の復号装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該第２の復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第３属性情報と言う）または論理情報（以下、第３論理情報と言う）を得る第３

命題論理情報取得ステップと、

上記第２の復号装置の送信部が、上記第３属性情報または上記第３論理情報を上記鍵生成装置に送信する論理情報送信ステップと、

上記鍵生成装置の受信部が、上記第２の復号装置から上記第３属性情報または上記第３論理情報を受信する論理情報受信ステップと、

上記鍵生成装置の鍵生成部が、上記第３属性情報または上記第３論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる第２の復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記第２の復号鍵を上記第２の復号装置に送信する復号鍵送信ステップと、

上記第２の復号装置の受信部が、上記鍵生成装置から上記第２の復号鍵を受信する復号鍵受信ステップと、

上記第２の復号装置の復号部が、上記第２の復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号情報に対する復号処理を行う復号ステップと、

を有する暗号通信方法。

［請求項20］ 少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報

（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、コンテンツとを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報と、当該共通鍵で当該コンテンツを暗号化した暗号化コンテンツとを求める暗号化ステップと、

上記暗号化装置の送信部が、上記暗号化コンテンツとこれに対応する上記暗号情報を上記コンテンツサーバ装置に送信する送信ステップと、

上記コンテンツサーバ装置の記憶部が、各上記暗号化装置から送られた上記暗号情報と上記暗号化コンテンツを記憶する記憶ステップと、

上記復号装置のブラウザ部が、上記コンテンツサーバ装置に対する上記暗号化コンテンツの取得要求処理を行う取得要求処理ステップと、

上記復号装置の中継部が、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信する送信ステップと、

上記コンテンツサーバ装置の送信部が、上記復号装置からの要求に応じて上記暗号化コンテンツとこれに対応する上記暗号情報を当該復号装置に送信する送信ステップと、

上記復号装置の受信部が、上記コンテンツサーバ装置から上記暗号化コンテンツと上記暗号情報を受信する受信ステップと、

上記鍵生成装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記復号鍵を上記復号装置に送信する復号鍵送信ステップと、

上記復号装置の受信部が、上記鍵生成装置から上記復号鍵を受信する復号鍵受信ステップと、

上記復号装置の中継部が、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号情報に対する復号処理と、当該復号処理で得られた上記共通鍵を用いて、上記コンテンツサーバ装置から取得した上記暗号化コンテンツを復号するコンテンツ取得処理を行う復号ステップと、

上記復号装置のブラウザ部が、上記暗号化コンテンツから復号されたコンテンツを表示する表示ステップと

を有する暗号通信方法。

［請求項21］ 少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコ

ンテンツサーバ装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、コンテンツとを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報と、当該共通鍵で当該コンテンツを暗号化した暗号化コンテンツとを求める暗号化ステップと、

上記暗号化装置の送信部が、上記暗号化コンテンツとこれに対応する上記暗号情報を上記コンテンツサーバ装置に送信する送信ステ

ップと、

上記コンテンツサーバ装置の記憶部が、各上記暗号化装置から送られた上記暗号情報および上記暗号化コンテンツを記憶する記憶ステップと、

上記復号装置のブラウザ部が、上記コンテンツサーバ装置に対する上記暗号化コンテンツの取得要求処理を行う取得要求処理ステップと、

上記復号装置の中継部が、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信する送信ステップと、

上記コンテンツサーバ装置の送信部が、上記復号装置からの要求に応じて上記暗号化コンテンツとこれに対応する上記暗号情報を当該復号装置に送信する送信ステップと、

上記復号装置の受信部が、上記コンテンツサーバ装置から上記暗号化コンテンツと上記暗号情報を受信する受信ステップと、

上記復号装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記復号装置の送信部が、上記第２属性情報または上記第２論理情報を上記鍵生成装置に送信する論理情報送信ステップと、

上記鍵生成装置の受信部が、上記復号装置から上記第２属性情報または上記第２論理情報を受信する論理情報受信ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号情報の復号に用いる復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記復号鍵を上記復号装置に送信

する復号鍵送信ステップと、

上記復号装置の受信部が、上記鍵生成装置から上記復号鍵を受信する復号鍵受信ステップと、

上記復号装置の中継部が、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号情報に対する復号処理と、当該復号処理で得られた上記共通鍵を用いて、上記コンテンツサーバ装置から取得した上記暗号化コンテンツを復号するコンテンツ取得処理を行う復号ステップと、

上記復号装置のブラウザ部が、上記暗号化コンテンツから復号されたコンテンツを表示する表示ステップと

を有する暗号通信方法。

[請求項22] 少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属

性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、コンテンツとを用いて、関す暗号アルゴリズムに則り、当該コンテンツを暗号化した暗号化コンテンツを求める暗号化ステップと、

上記暗号化装置の送信部が、上記暗号化コンテンツを上記コンテンツサーバ装置に送信する送信ステップと、

上記コンテンツサーバ装置の記憶部が、各上記暗号化装置から送られた上記暗号化コンテンツを記憶する記憶ステップと、

上記復号装置のブラウザ部が、上記コンテンツサーバ装置に対する上記暗号化コンテンツの取得要求処理を行う取得要求処理ステップと、

上記復号装置の中継部が、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信する送信ステップと、

上記コンテンツサーバ装置の送信部が、上記復号装置からの要求に応じて上記暗号化コンテンツを当該復号装置に送信する送信ステップと、

上記復号装置の受信部が、上記コンテンツサーバ装置から上記暗号化コンテンツを受信する受信ステップと、

上記鍵生成装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）

または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号化コンテンツの復号に用いる復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記復号鍵を上記復号装置に送信する復号鍵送信ステップと、

上記復号装置の受信部が、上記鍵生成装置から上記復号鍵を受信する復号鍵受信ステップと、

上記復号装置の中継部が、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号化コンテンツに対する復号処理を行う復号ステップと、

上記復号装置のブラウザ部が、上記暗号化コンテンツから復号されたコンテンツを表示する表示ステップと

を有する暗号通信方法。

［請求項23］ 少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含み、関数暗号を用いる暗号システムにおける暗号通信方法であって、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められており、

上記暗号化装置の第１命題論理情報取得部が、上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得ステップと、

上記暗号化装置の暗号化部が、上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、コンテンツとを用いて、関数暗号アルゴリズムに則り、当該コンテンツを暗号化した暗号化コンテンツを求める暗号化ステップと、

上記暗号化装置の送信部が、上記暗号化コンテンツを上記コンテンツサーバ装置に送信する送信ステップと、

上記コンテンツサーバ装置の記憶部が、各上記暗号化装置から送られた上記暗号化コンテンツを記憶する記憶ステップと、

上記復号装置のブラウザ部が、上記コンテンツサーバ装置に対する上記暗号化コンテンツの取得要求処理を行う取得要求処理ステップと、

上記復号装置の中継部が、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信する送信ステップと、

上記コンテンツサーバ装置の送信部が、上記復号装置からの要求に応じて上記暗号化コンテンツを当該復号装置に送信する送信ステップと、

上記復号装置の受信部が、上記コンテンツサーバ装置から上記暗号化コンテンツを受信する受信ステップと、

上記復号装置の第２命題論理情報取得部が、上記ポリシー情報で特定される上記一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得ステップと、

上記復号装置の送信部が、上記第２属性情報または上記第２論理情報を上記鍵生成装置に送信する論理情報送信ステップと、

上記鍵生成装置の受信部が、上記復号装置から上記第２属性情報または上記第２論理情報を受信する論理情報受信ステップと、

上記鍵生成装置の鍵生成部が、上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、上記暗号化コンテンツの復号に用いる復号鍵を生成する鍵生成ステップと、

上記鍵生成装置の送信部が、上記復号鍵を上記復号装置に送信する復号鍵送信ステップと、

上記復号装置の受信部が、上記鍵生成装置から上記復号鍵を受信する復号鍵受信ステップと、

上記復号装置の中継部が、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号化コンテンツに対する復号処理を行う復号ステップと、

上記復号装置のブラウザ部が、上記暗号化コンテンツから復号されたコンテンツを表示する表示ステップと

を有する暗号通信方法。

［請求項24］ 少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アル

ゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおける暗号化装置であって、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵とを用いて、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報とを求める暗号化部と

を含む暗号化装置。

［請求項25］ 少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情

報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおける暗号化装置であって、

上記変換規則情報ペアの中から選択された一つの変換規則情報ペアに含まれる上記属性用変換規則情報と上記論理式用変換規則情報のうち、当該暗号化装置の入力情報が属性指定情報または論理式指定情報のいずれであるかに応じて上記ポリシー情報と共に選択されたいずれか一方の変換規則情報を用いて、当該入力情報から属性情報（以下、第１属性情報と言う）または論理情報（以下、第１論理情報と言う）を得る第１命題論理情報取得部と、

上記第１属性情報または上記第１論理情報と、上記鍵生成装置の公開鍵と、平文とを用いて、関数暗号アルゴリズムに則り、当該平文に対応する暗号情報を求める暗号化部と

を含む暗号化装置。

［請求項26］ 少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペア

が予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおける鍵生成装置であって、

上記ポリシー情報で特定される一方の変換規則情報とペアになっている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記第２属性情報または上記第２論理情報と、当該鍵生成装置の秘密鍵とを用いて、暗号情報の復号に用いる復号鍵を生成する鍵生成部と

を含む鍵生成装置。

［請求項27］ 少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおける鍵生成装置であって、

上記ポリシー情報で特定される一方の変換規則情報とペアにな

っている他方の変換規則情報を用いて、上記復号装置の利用者に対応する属性指定情報または論理式指定情報から生成された属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）と、当該鍵生成装置の秘密鍵とを用いて、暗号情報の復号に用いる復号鍵を生成する鍵生成部

を含む鍵生成装置。

［請求項28］ 少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおける復号装置であって、

上記鍵生成装置が生成した復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号化装置が生成した暗号情報に対する復号処理を行う復号部

を含む復号装置。

［請求項29］ 少なくとも、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおける復号装置であって、

上記ポリシー情報で特定される一方の変換規則情報とペアになっている他方の変換規則情報を用いて、当該復号装置の利用者に対応する属性指定情報または論理式指定情報から、属性情報（以下、第２属性情報と言う）または論理情報（以下、第２論理情報と言う）を得る第２命題論理情報取得部と、

上記鍵生成装置が生成した復号鍵を用いて、関数暗号アルゴリズムに則り、上記暗号化装置が生成した暗号情報に対する復号処理を行う復号部

を含む復号装置。

[請求項30] 請求項２８または請求項２９に記載の復号装置において、

上記暗号システムが複数の復号装置を含む場合に、

当該復号装置以外の一つ以上の復号装置に上記暗号情報を転送する転送部をさらに含む復号装置。

[請求項31] 少なくとも、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報と、当該共通鍵でコンテンツを暗号化した暗号化コンテンツとを求める、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、上記暗号化コンテンツと上記暗号情報を記

憶している一つまたは複数のコンテンツサーバ装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおける復号装置であって、

ブラウザ部と中継部とを含み、

上記ブラウザ部は、上記コンテンツサーバ装置に対する上記暗号化コンテンツの取得要求処理を行い、上記暗号化コンテンツから復号されたコンテンツを表示し、

上記中継部は、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信し、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号情報に対する復号処理と、当該復号処理で得られた上記共通鍵を用いて、上記コンテンツサーバ装置から取得した上記暗号化コンテンツを復号するコンテンツ取得処理を行う、

復号装置。

［請求項32］ 少なくとも、関数暗号アルゴリズムに則り、コンテンツを暗号化した暗号化コンテンツを求める、一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、上記暗号化コンテンツを記憶している一つまたは複数のコンテンツサーバ

装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおける復号装置であって、

ブラウザ部と中継部とを含み、

上記ブラウザ部は、上記コンテンツサーバ装置に対する上記暗号化コンテンツの取得要求処理を行い、上記暗号化コンテンツから復号されたコンテンツを表示し、

上記中継部は、上記ブラウザ部からの上記取得要求を上記コンテンツサーバ装置へ送信し、上記復号鍵を用いて、関数暗号アルゴリズムに則り、上記コンテンツサーバ装置から取得した上記暗号化コンテンツに対する復号処理を行う、

復号装置。

［請求項33］ 少なくとも、関数暗号アルゴリズムに則り、共通鍵と、当該共通鍵または当該共通鍵の生成に用いる情報に対応する暗号情報と、当該共通鍵でコンテンツを暗号化した暗号化コンテンツとを求める一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおけるコンテンツサーバ装置であって、

各上記暗号化装置から送られた上記暗号情報および上記暗号化コンテンツを記憶する記憶部と、

上記復号装置からの要求に応じて上記暗号化コンテンツとこれに対応する上記暗号情報を当該復号装置に送信する送信部と

を含むコンテンツサーバ装置。

［請求項34］ 少なくとも、関数暗号アルゴリズムに則り、コンテンツを暗号化した暗号化コンテンツを求める一つまたは複数の暗号化装置と、一つまたは複数の鍵生成装置と、一つまたは複数の復号装置と、一つまたは複数のコンテンツサーバ装置とを含み、

各上記鍵生成装置につき秘密鍵とこの秘密鍵に対応する公開鍵が予め定められており、

属性を指定する情報（以下、属性指定情報と言う）を関数暗号アルゴリズムに用いられる属性情報に変換するための変換規則を規定している情報（以下、属性用変換規則情報と言う）と論理式を指定する情報（以下、論理式指定情報と言う）を当該関数暗号アルゴリズムに用いられる論理情報に変換するための変換規則を規定している情報（以

下、論理式用変換規則情報と言う）とのペアである変換規則情報ペアが予め一つまたは複数定められており、

上記属性用変換規則情報と上記論理式用変換規則情報のうちいずれであるかを特定するためのポリシー情報が予め定められている、関数暗号を用いる暗号システムにおけるコンテンツサーバ装置であって、

各上記暗号化装置から送られた上記暗号化コンテンツを記憶する記憶部と、

上記復号装置からの要求に応じて上記暗号化コンテンツを当該復号装置に送信する送信部と

を含むコンテンツサーバ装置。

[請求項35] 請求項２４または請求項２５に記載の暗号化装置としてコンピュータを機能させるためのプログラム。

[請求項36] 請求項２６または請求項２７に記載の鍵生成装置としてコンピュータを機能させるためのプログラム。

[請求項37] 請求項２８、２９、３１、３２のいずれかに記載の復号装置としてコンピュータを機能させるためのプログラム。

[請求項38] 請求項３３または請求項３４に記載のコンテンツサーバ装置としてコンピュータを機能させるためのプログラム。

[請求項39] 請求項３５に記載のプログラム、請求項３６に記載のプログラム、請求項３７に記載のプログラム、請求項３８に記載のプログラム、のうち少なくともいずれかを格納したコンピュータ読み取り可能な記憶媒体。

[図1]

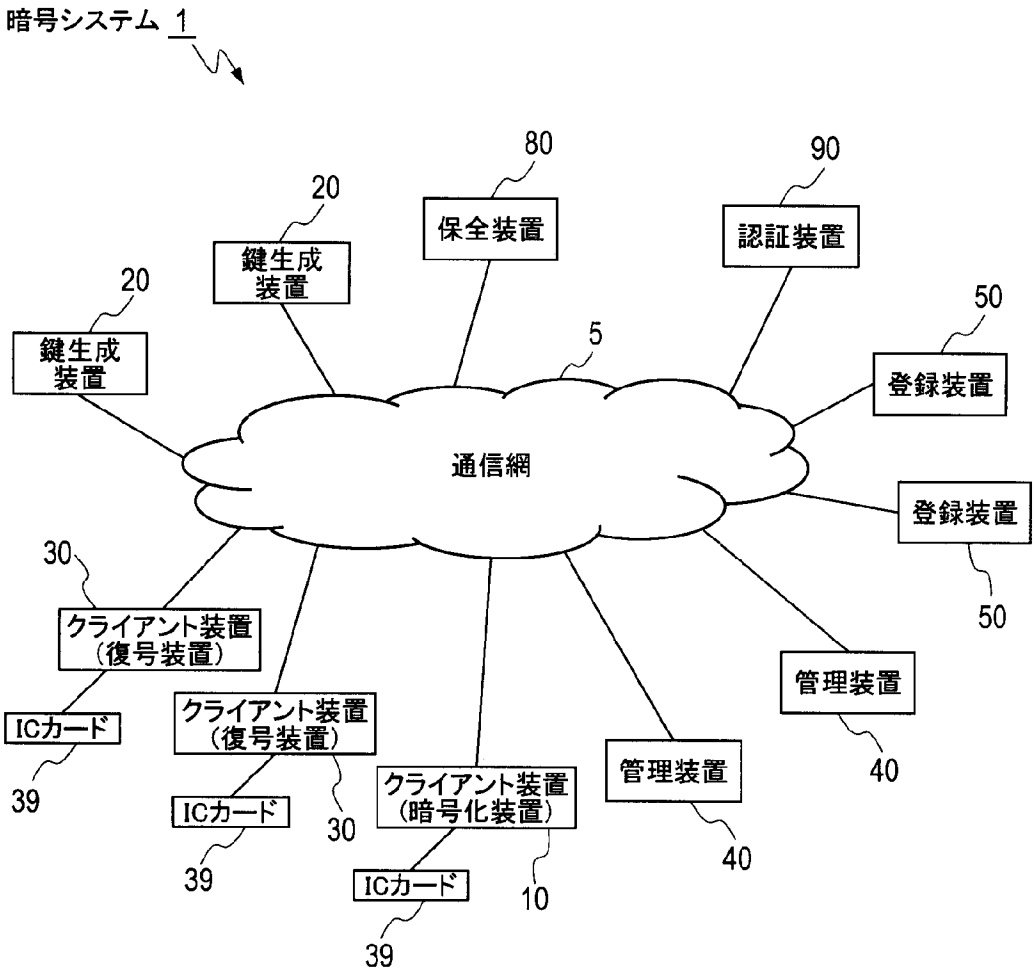

暗号システム 1
80
保全装置
90
認証装置
20
鍵生成装置
20
鍵生成装置
5
通信網
50
登録装置
登録装置
50
30
クライアント装置（復号装置）
ICカード
39
クライアント装置（復号装置）
ICカード
39
30
クライアント装置（暗号化装置）
ICカード
39
10
管理装置
40
管理装置
40

図1

[図2]

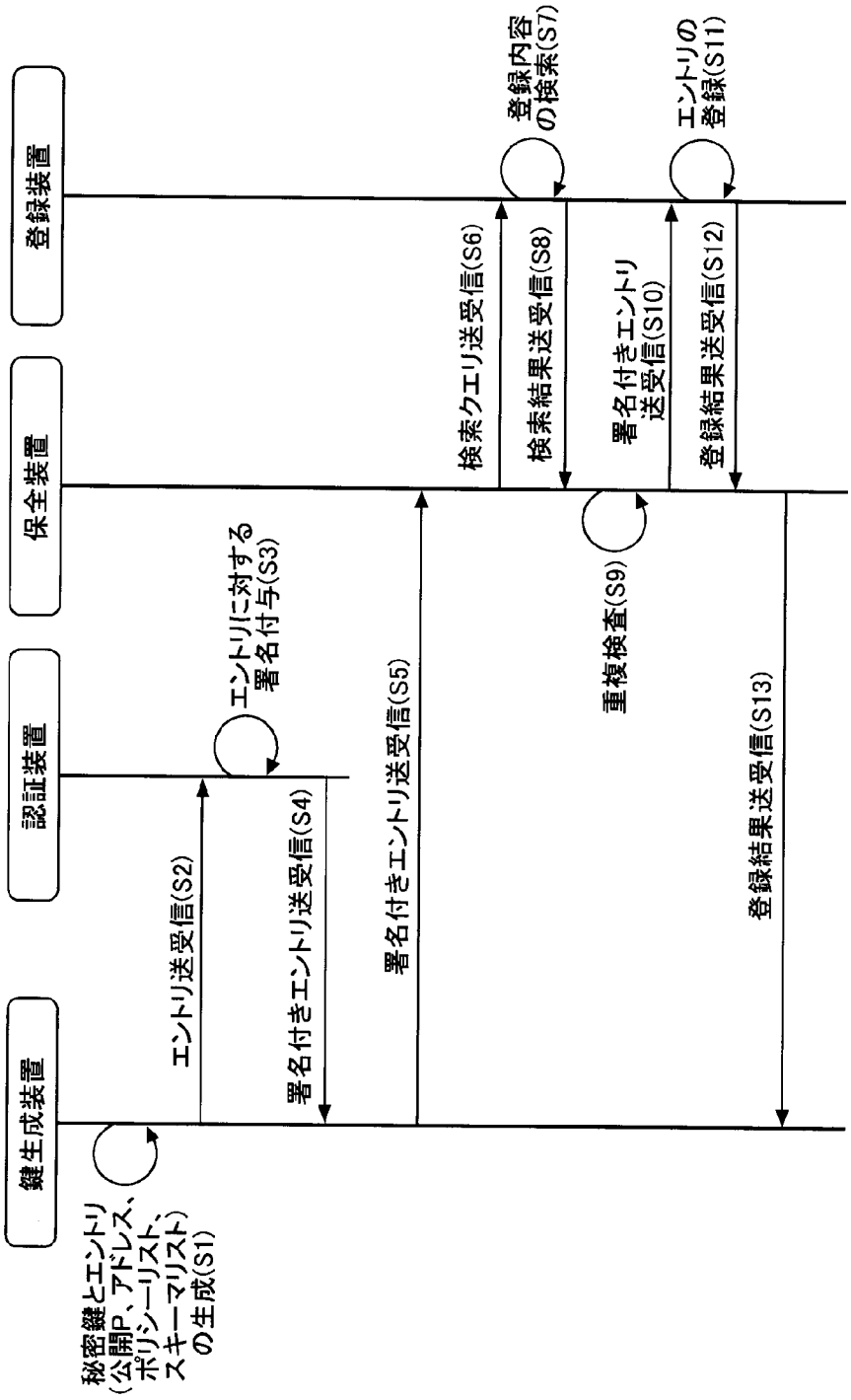

鍵生成装置
認証装置
保全装置
登録装置
秘密鍵とエントリ（公開P、アドレス、ポリシーリスト、スキーマリスト）の生成(S1)
エントリ送受信(S2)
エントリに対する署名付与(S3)
署名付きエントリ送受信(S4)
署名付きエントリ送受信(S5)
検索クエリ送受信(S6)
登録内容の検索(S7)
検索結果送受信(S8)
重複検査(S9)
署名付きエントリ送受信(S10)
エントリの登録(S11)
登録結果送受信(S12)
登録結果送受信(S13)

図2

[図3]

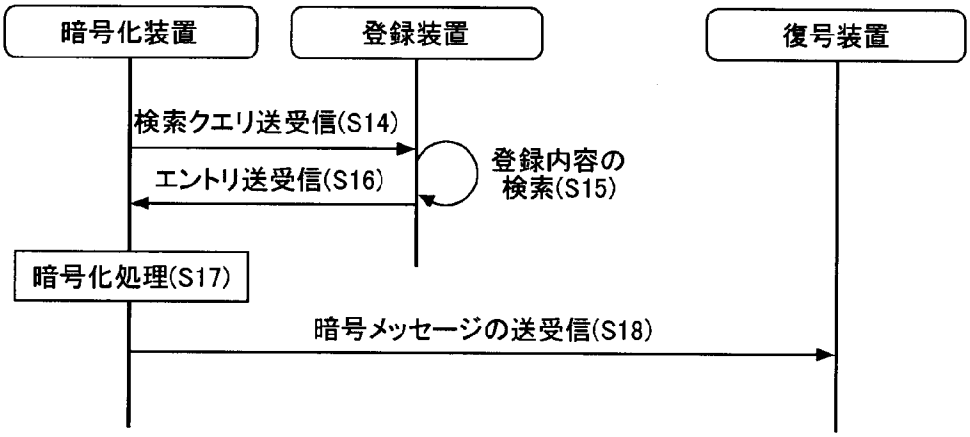

暗号化装置
登録装置
復号装置
検索クエリ送受信(S14)
登録内容の
検索(S15)
エントリ送受信(S16)
暗号化処理(S17)
暗号メッセージの送受信(S18)

図3

[図4]

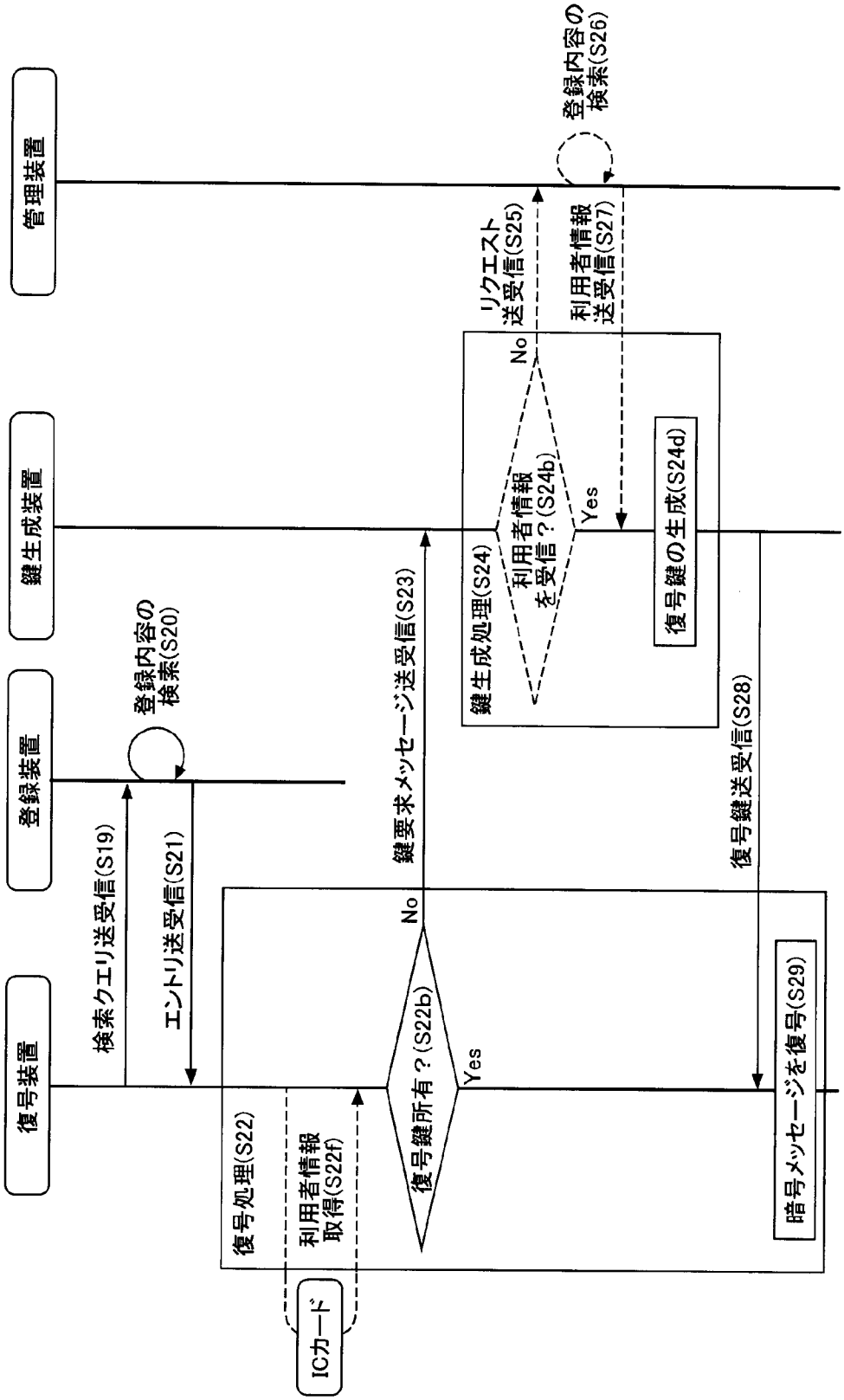

管理装置
鍵生成装置
登録装置
復号装置
登録内容の検索(S26)
リクエスト送受信(S25)
利用者情報送受信(S27)
No
Yes
鍵生成処理(S24)
利用者情報を受信？(S24b)
復号鍵の生成(S24d)
登録内容の検索(S20)
検索クエリ送受信(S19)
エントリ送受信(S21)
鍵要求メッセージ送受信(S23)
復号鍵送受信(S28)
No
Yes
復号処理(S22)
利用者情報取得(S22f)
復号鍵所有？(S22b)
暗号メッセージを復号(S29)
ICカード

図4

[図5]

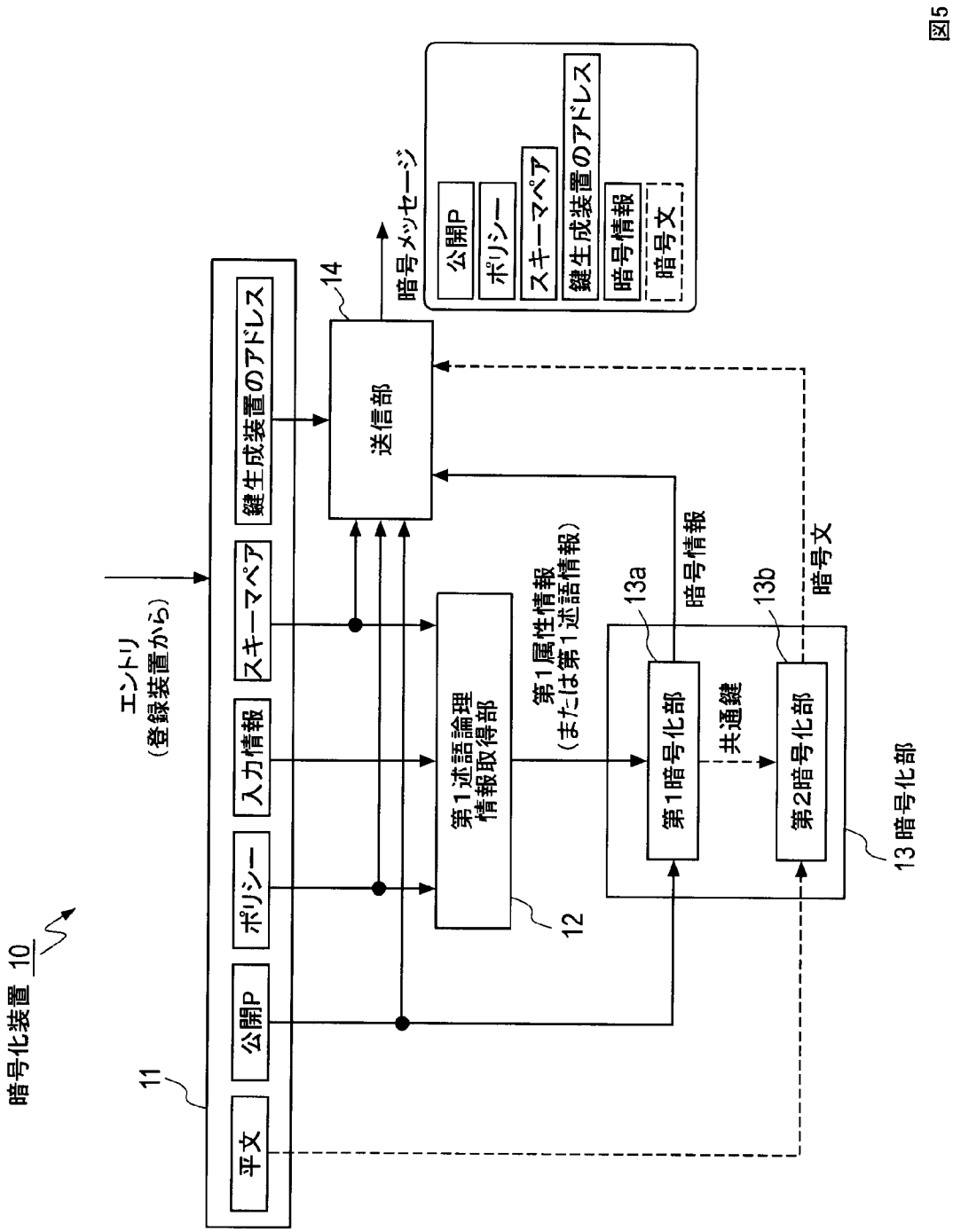

暗号化装置 10
11
平文
公開P
ポリシー
入力情報
スキーマペア
鍵生成装置のアドレス
エントリ
(登録装置から)
第1述語論理
情報取得部
12
第1属性情報
(または第1述語情報)
13 暗号化部
13a
第1暗号化部
共通鍵
13b
第2暗号化部
暗号情報
暗号文
送信部
14
暗号メッセージ
公開P
ポリシー
スキーマペア
鍵生成装置のアドレス
暗号情報
暗号文

図5

[図6]

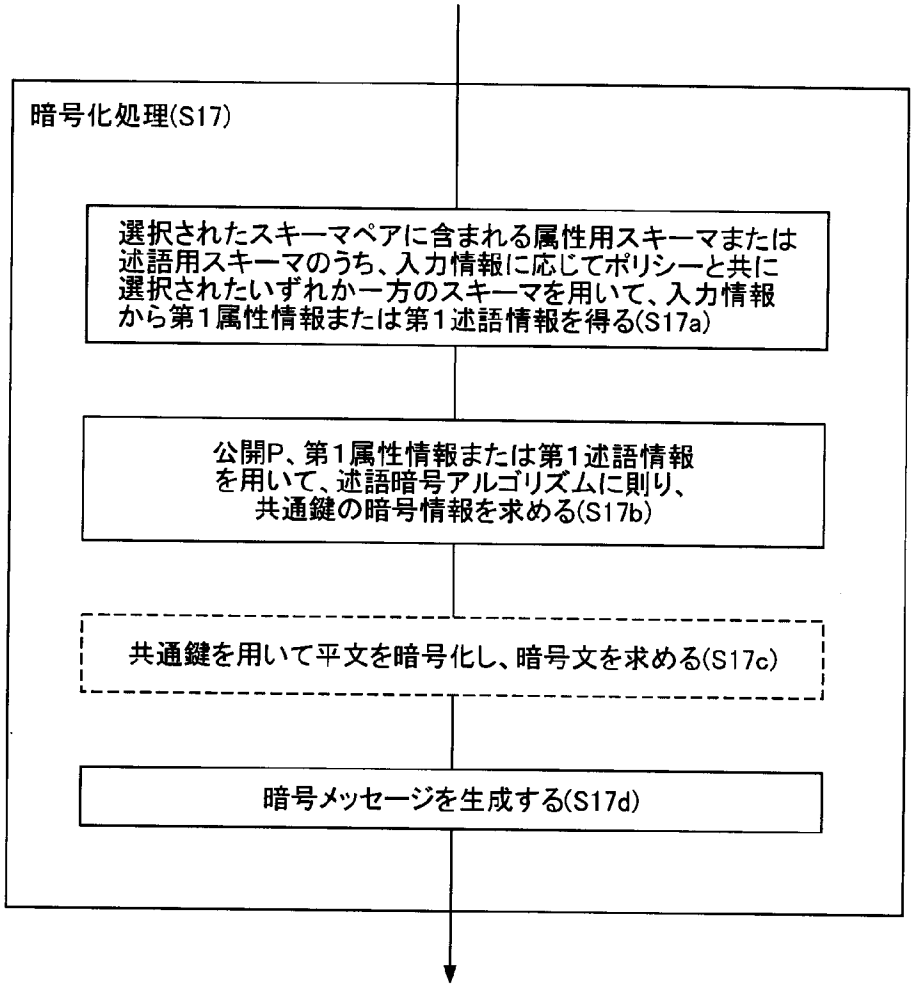

暗号化処理(S17)
選択されたスキーマペアに含まれる属性用スキーマまたは述語用スキーマのうち、入力情報に応じてポリシーと共に選択されたいずれか一方のスキーマを用いて、入力情報から第1属性情報または第1述語情報を得る(S17a)
公開P、第1属性情報または第1述語情報を用いて、述語暗号アルゴリズムに則り、共通鍵の暗号情報を求める(S17b)
共通鍵を用いて平文を暗号化し、暗号文を求める(S17c)
暗号メッセージを生成する(S17d)

図6

[図7]

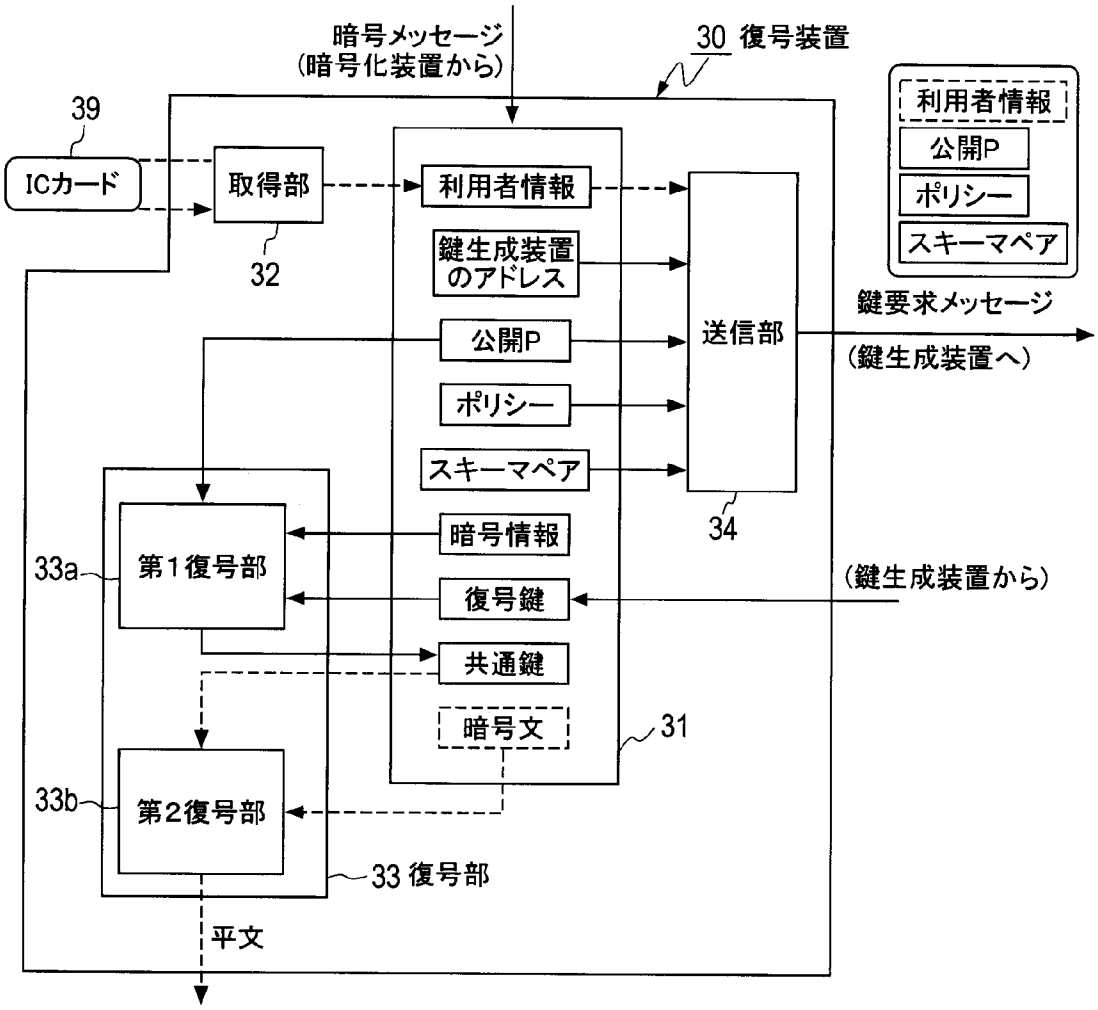

暗号メッセージ
(暗号化装置から)
30 復号装置
39
ICカード
取得部
32
利用者情報
鍵生成装置のアドレス
公開P
ポリシー
スキーマペア
送信部
34
利用者情報
公開P
ポリシー
スキーマペア
鍵要求メッセージ
(鍵生成装置へ)
暗号情報
復号鍵
(鍵生成装置から)
共通鍵
暗号文
31
33a
第1復号部
33b
第2復号部
33 復号部
平文

図7

[図8]

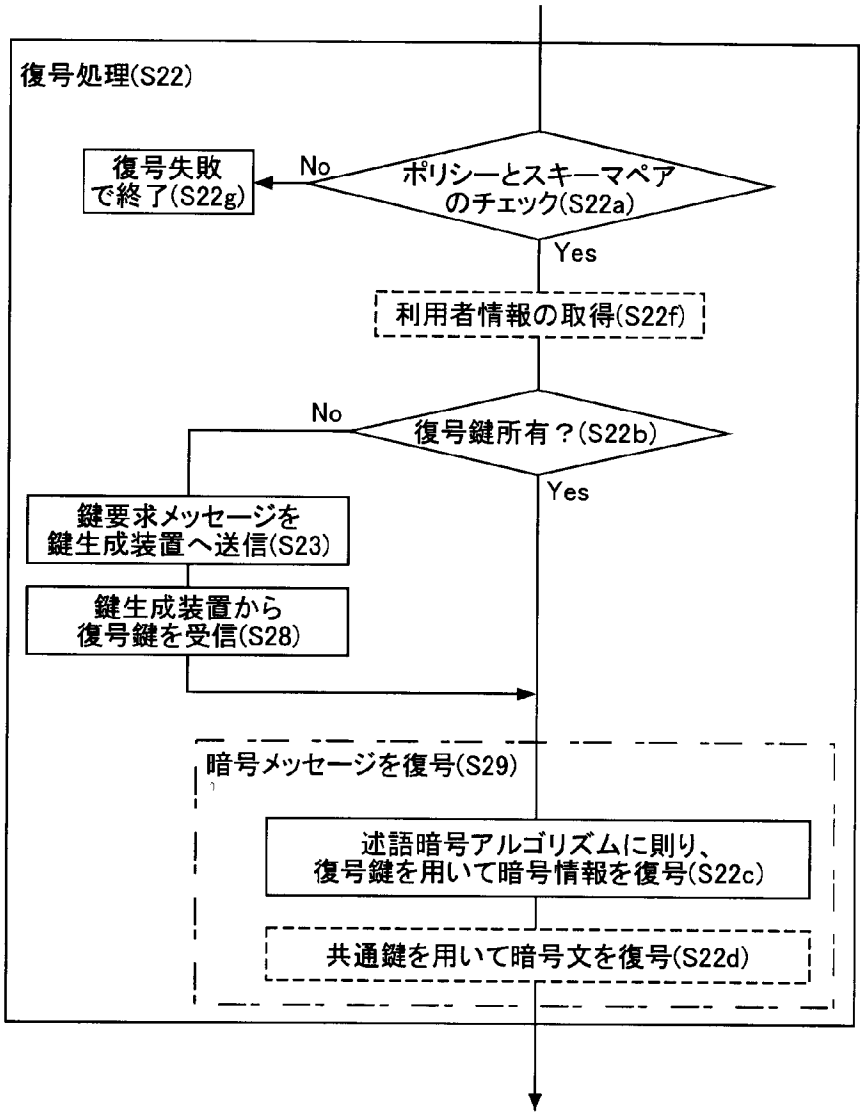

復号処理(S22)
ポリシーとスキーマペアのチェック(S22a)
No
復号失敗で終了(S22g)
Yes
利用者情報の取得(S22f)
復号鍵所有？(S22b)
No
Yes
鍵要求メッセージを鍵生成装置へ送信(S23)
鍵生成装置から復号鍵を受信(S28)
暗号メッセージを復号(S29)
述語暗号アルゴリズムに則り、復号鍵を用いて暗号情報を復号(S22c)
共通鍵を用いて暗号文を復号(S22d)

図8

[図9]

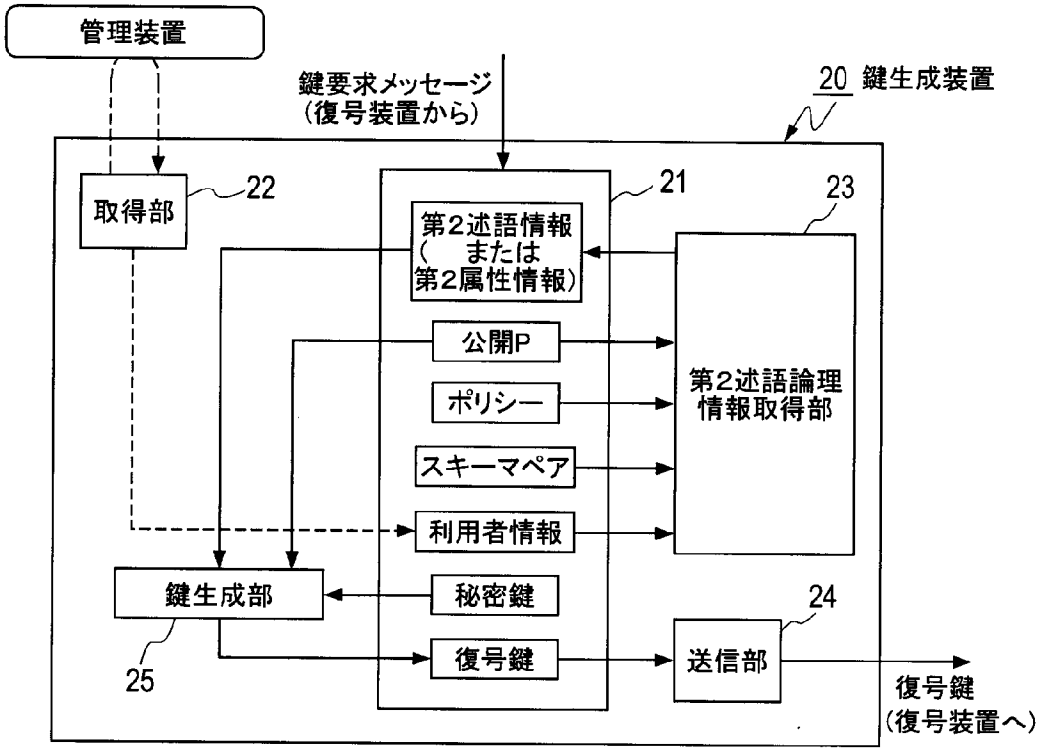

管理装置
鍵要求メッセージ
(復号装置から)
20 鍵生成装置
取得部
22
21
23
第2述語情報
(または
第2属性情報)
公開P
ポリシー
スキーマペア
利用者情報
第2述語論理
情報取得部
鍵生成部
秘密鍵
24
復号鍵
送信部
25
復号鍵
(復号装置へ)

図9

[図10]

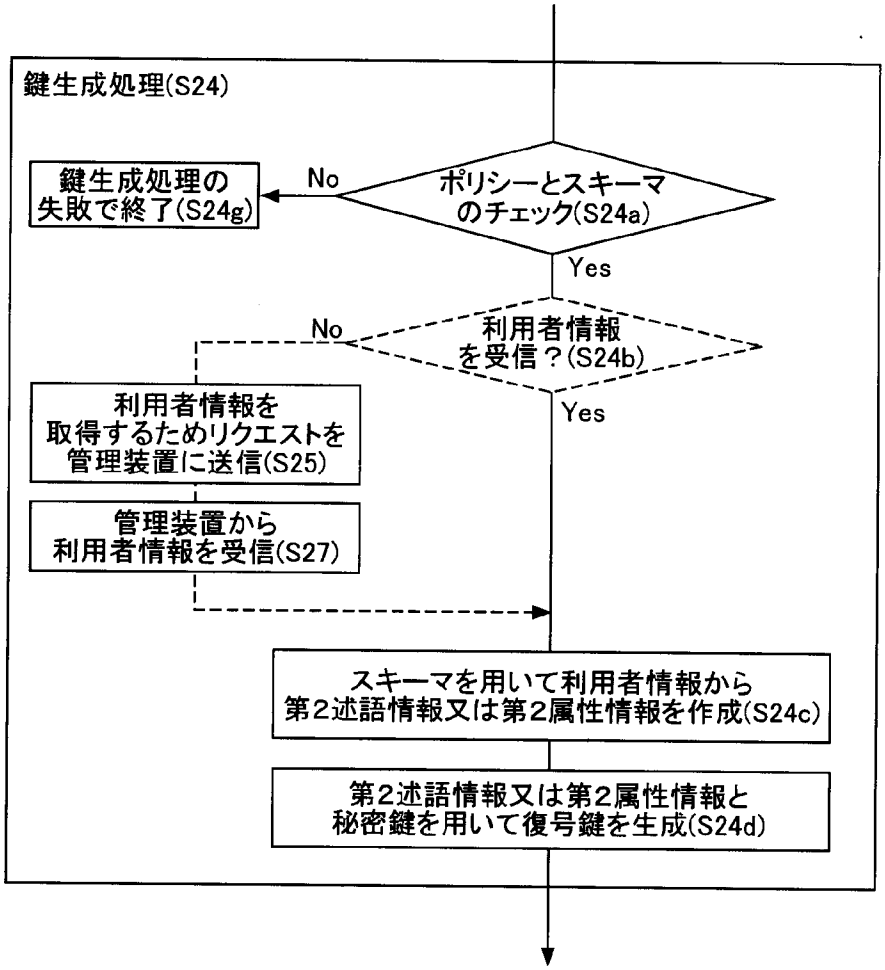

鍵生成処理(S24)
ポリシーとスキーマのチェック(S24a)
No
鍵生成処理の失敗で終了(S24g)
Yes
利用者情報を受信？(S24b)
No
Yes
利用者情報を取得するためリクエストを管理装置に送信(S25)
管理装置から利用者情報を受信(S27)
スキーマを用いて利用者情報から第2述語情報又は第2属性情報を作成(S24c)
第2述語情報又は第2属性情報と秘密鍵を用いて復号鍵を生成(S24d)

図10

[図11]

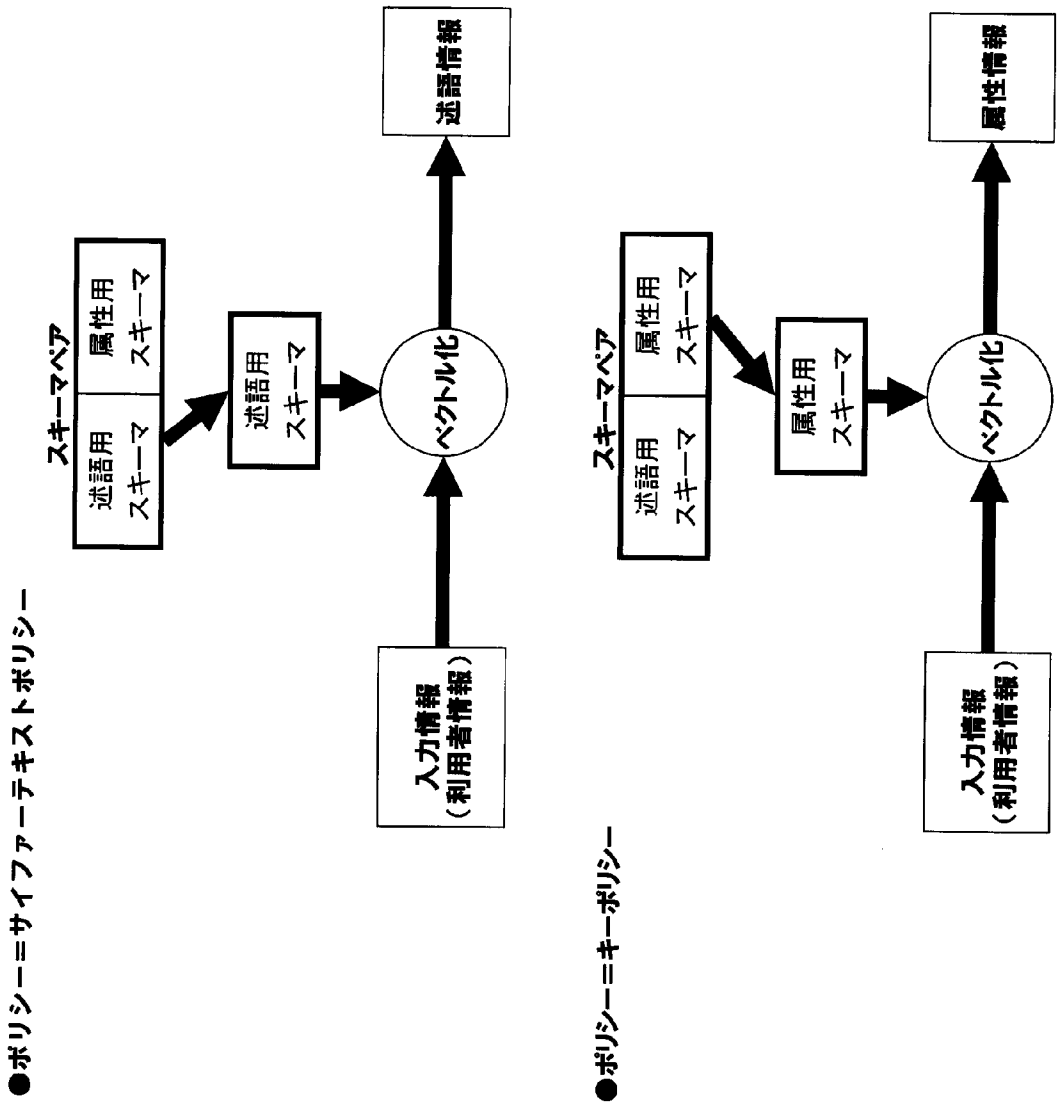

●ポリシー＝サイファーテキストポリシー
スキーマペア
述語用スキーマ
属性用スキーマ
述語用スキーマ
ベクトル化
述語情報
入力情報（利用者情報）
●ポリシー＝キーポリシー
スキーマペア
述語用スキーマ
属性用スキーマ
属性用スキーマ
ベクトル化
属性情報
入力情報（利用者情報）

図11

[図12]

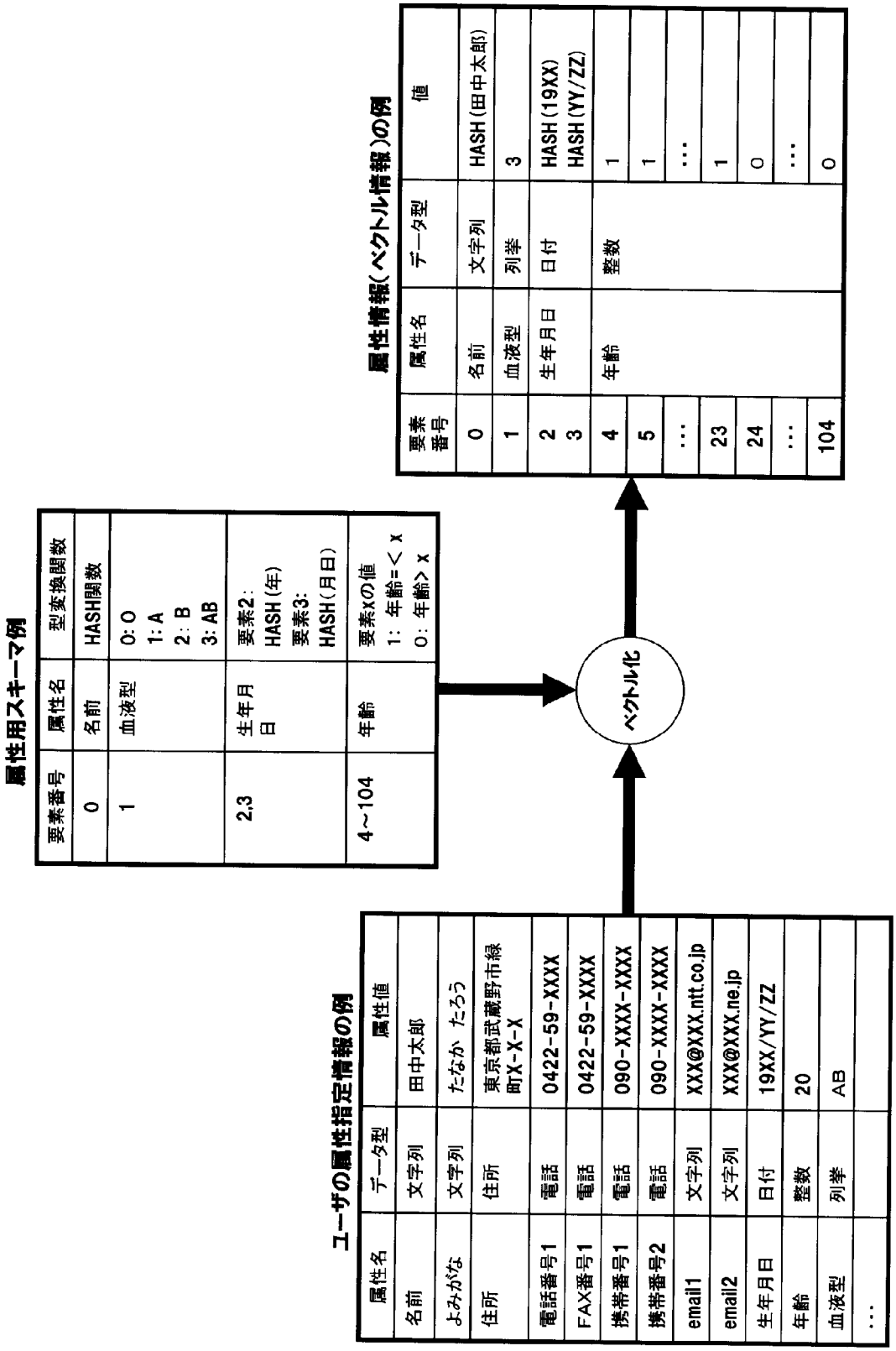

属性用スキーマ例
要素番号
属性名
型変換関数
0
名前
HASH関数
1
血液型
0: O
1: A
2: B
3: AB
2,3
生年月日
要素2:
HASH(年)
要素3:
HASH(月日)
4~104
年齢
要素xの値
1: 年齢=< x
0: 年齢> x
ベクトル化
ユーザの属性指定情報の例
属性名
データ型
属性値
名前
文字列
田中太郎
よみがな
文字列
たなか たろう
住所
住所
東京都武蔵野市緑町X-X-X
電話番号1
電話
0422-59-XXXX
FAX番号1
電話
0422-59-XXXX
携帯番号1
電話
090-XXXX-XXXX
携帯番号2
電話
090-XXXX-XXXX
email1
文字列
XXX@XXX.ntt.co.jp
email2
文字列
XXX@XXX.ne.jp
生年月日
日付
19XX/YY/ZZ
年齢
整数
20
血液型
列挙
AB
...
属性情報(ベクトル情報)の例
要素番号
属性名
データ型
値
0
名前
文字列
HASH(田中太郎)
1
血液型
列挙
3
2
3
生年月日
日付
HASH(19XX)
HASH(YY/ZZ)
4
年齢
整数
1
5
1
...
...
23
1
24
0
...
...
104
0

図12

[図13]

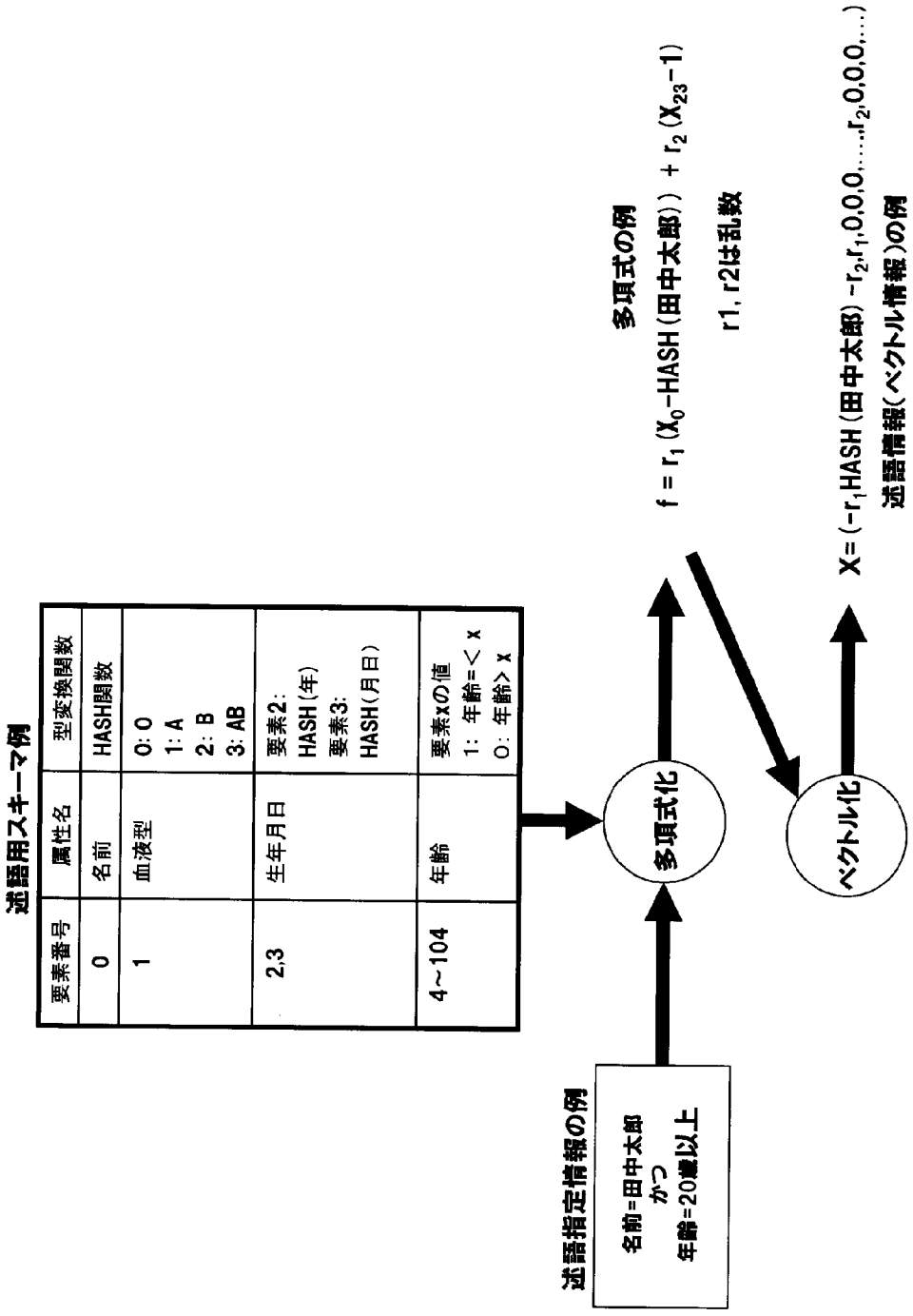

述語用スキーマ例
要素番号
属性名
型変換関数
0
名前
HASH関数
1
血液型
0: O
1: A
2: B
3: AB
2,3
生年月日
要素2:
HASH(年)
要素3:
HASH(月日)
4~104
年齢
要素xの値
1: 年齢=< x
0: 年齢> x
述語指定情報の例
名前=田中太郎
かつ
年齢=20歳以上
多項式化
ベクトル化
多項式の例
f = r1 (X0-HASH(田中太郎)) + r2 (X23-1)
r1, r2は乱数
X= (-r1HASH(田中太郎) -r2,r1,0,0,0,....,r2,0,0,0,...)
述語情報(ベクトル情報)の例

図13

[図14]

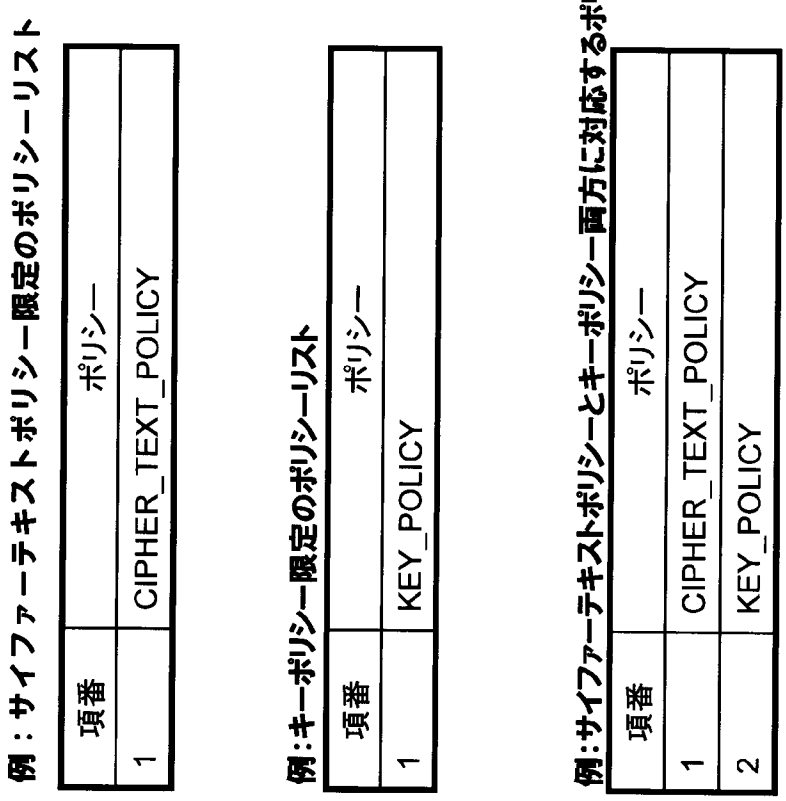

例：サイファーテキストポリシー限定のポリシーリスト
項番
ポリシー
1
CIPHER_TEXT_POLICY
例:キーポリシー限定のポリシーリスト
項番
ポリシー
1
KEY_POLICY
例:サイファーテキストポリシーとキーポリシー両方に対応するポリシーリスト
項番
ポリシー
1
CIPHER_TEXT_POLICY
2
KEY_POLICY

図14

[図15]

鍵生成装置の識別子	公開パラメータ	スキーマペア	復号鍵の対象	述語指定情報	復号鍵
鍵生成装置20－1	公開パラメータ1	スキーマペア1			復号鍵1
鍵生成装置20－2	公開パラメータ2	スキーマペア2			復号鍵2
…	…	…			…
鍵生成装置20－N	公開パラメータN	スキーマペアN			復号鍵N

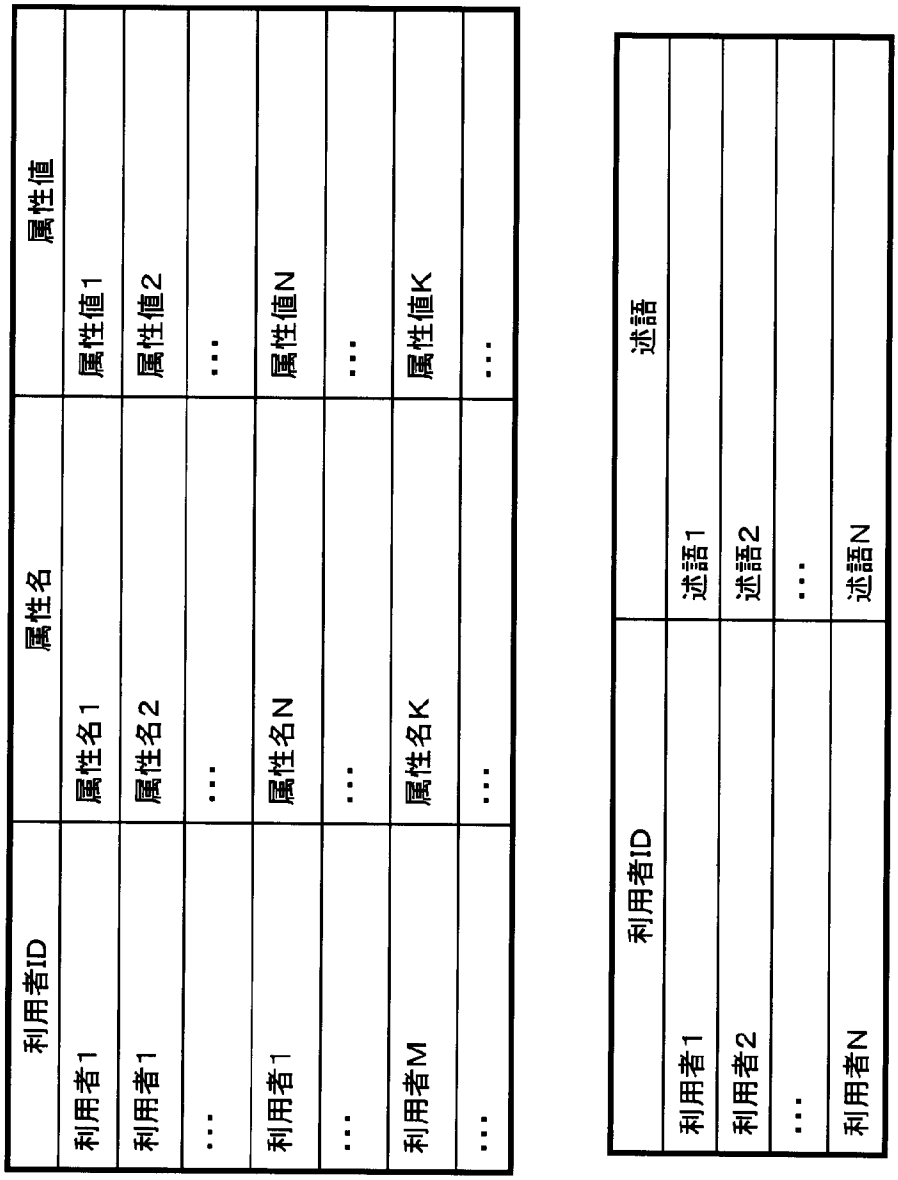
図15

[図16]

図16

ユーザID	パスワード
ユーザ1	パスワード1
ユーザ2	パスワード2
…	…
ユーザN	パスワードN

[図17]



利用者ID	属性名	属性値
利用者1	属性名1	属性値1
利用者1	属性名2	属性値2
...	...	...
利用者1	属性名N	属性値N
...	...	...
利用者M	属性名K	属性値K
...	...	...

利用者ID	述語
利用者1	述語1
利用者2	述語2
...	...
利用者N	述語N

図17

[図18]

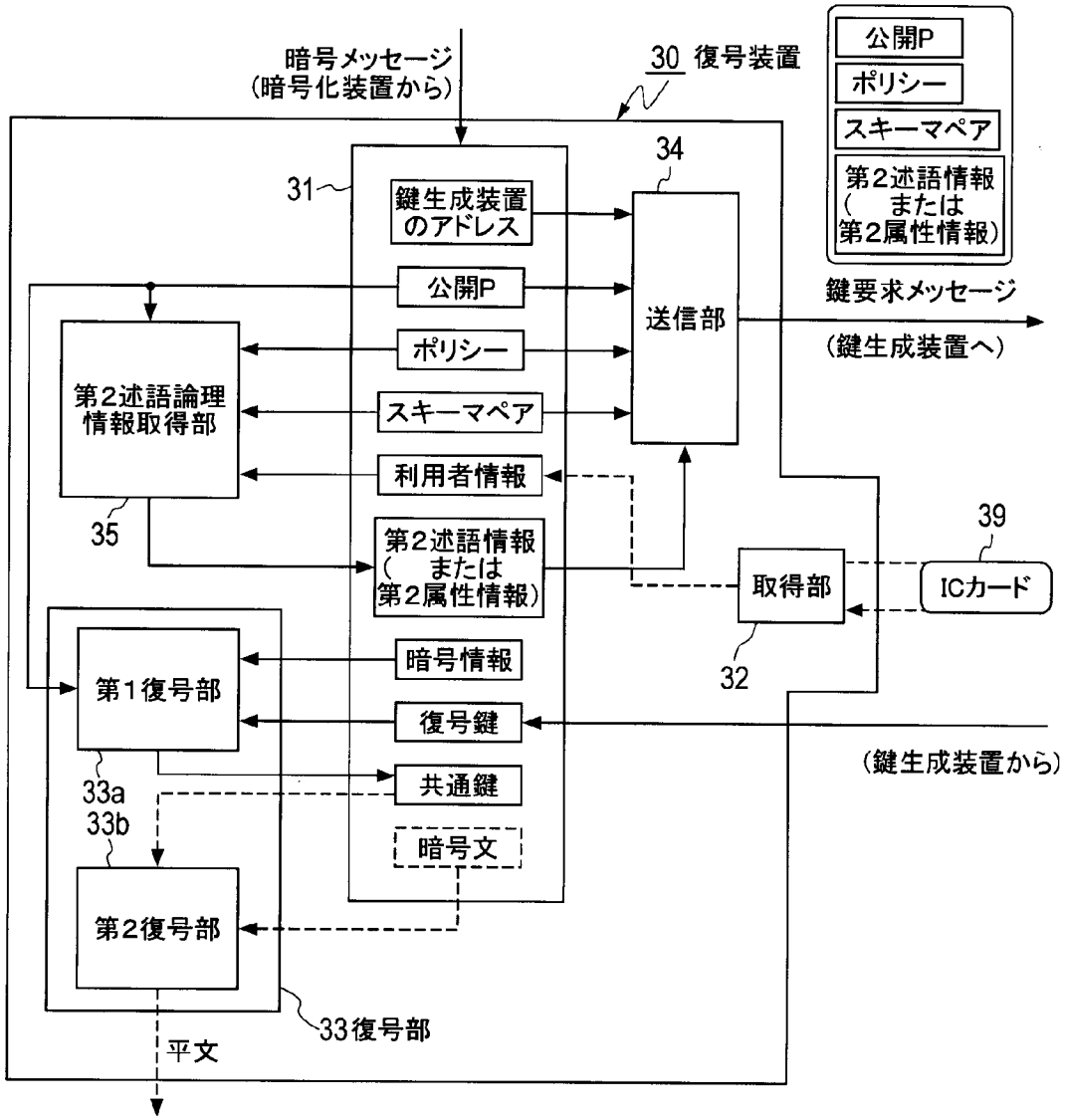

暗号メッセージ
(暗号化装置から)
30 復号装置
公開P
ポリシー
スキーマペア
第2述語情報
(または
第2属性情報)
鍵要求メッセージ
(鍵生成装置へ)
31
鍵生成装置
のアドレス
34
送信部
公開P
ポリシー
スキーマペア
利用者情報
第2述語論理
情報取得部
35
第2述語情報
(または
第2属性情報)
39
取得部
ICカード
32
暗号情報
復号鍵
(鍵生成装置から)
第1復号部
33a
33b
共通鍵
暗号文
第2復号部
33復号部
平文

図18

[図19]

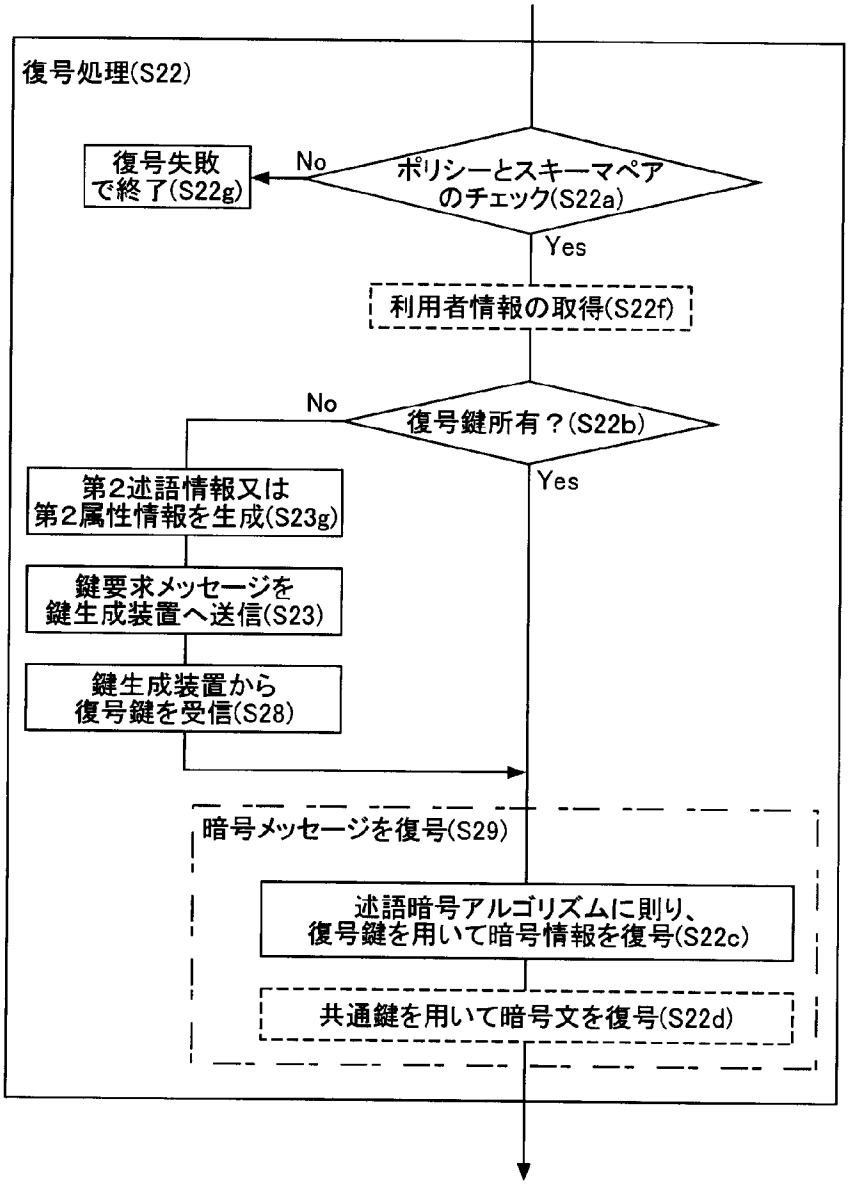

復号処理(S22)
ポリシーとスキーマペア のチェック(S22a)
No
復号失敗 で終了(S22g)
Yes
利用者情報の取得(S22f)
復号鍵所有？(S22b)
No
Yes
第2述語情報又は 第2属性情報を生成(S23g)
鍵要求メッセージを 鍵生成装置へ送信(S23)
鍵生成装置から 復号鍵を受信(S28)
暗号メッセージを復号(S29)
述語暗号アルゴリズムに則り、 復号鍵を用いて暗号情報を復号(S22c)
共通鍵を用いて暗号文を復号(S22d)

図19

[図20]

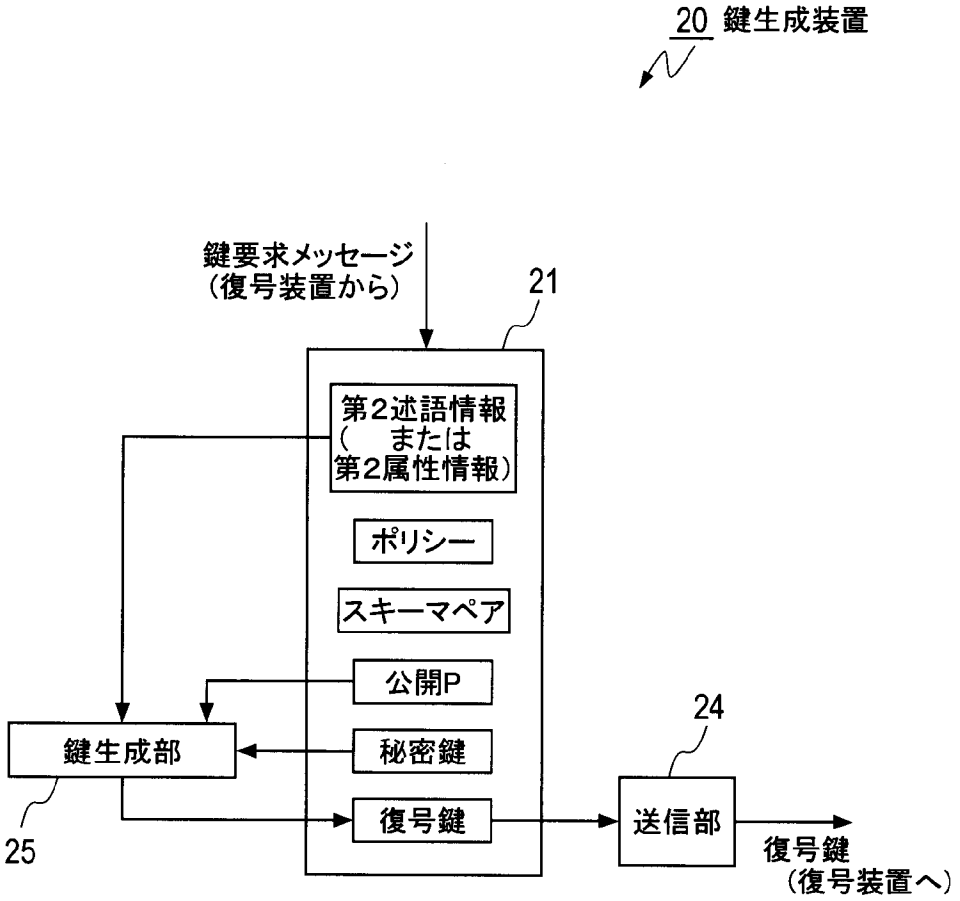

20 鍵生成装置
鍵要求メッセージ
(復号装置から)
21
第2述語情報
(または
第2属性情報)
ポリシー
スキーマペア
公開P
秘密鍵
復号鍵
鍵生成部
25
24
送信部
復号鍵
(復号装置へ)

図20

[図21]

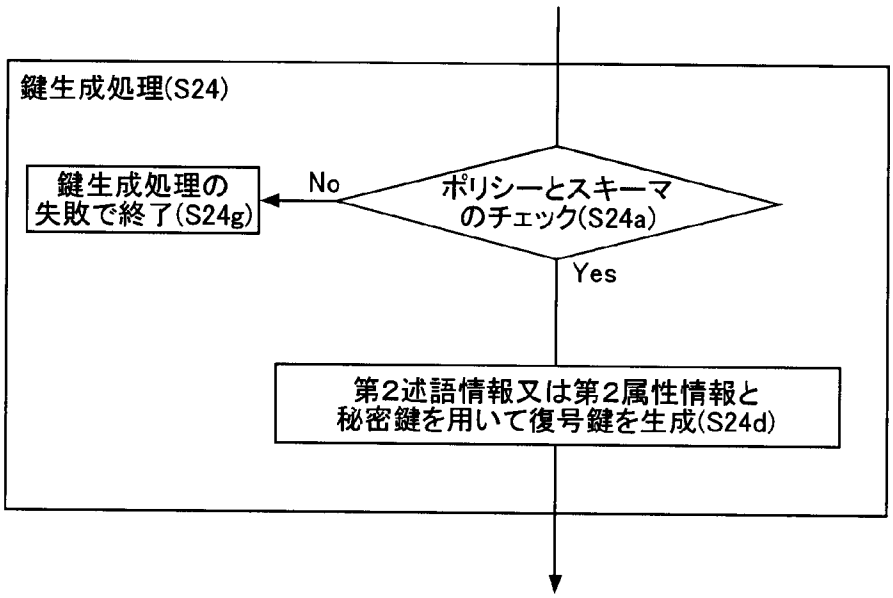

鍵生成処理(S24)
鍵生成処理の
失敗で終了(S24g)
No
ポリシーとスキーマ
のチェック(S24a)
Yes
第2述語情報又は第2属性情報と
秘密鍵を用いて復号鍵を生成(S24d)

図21

[図22]

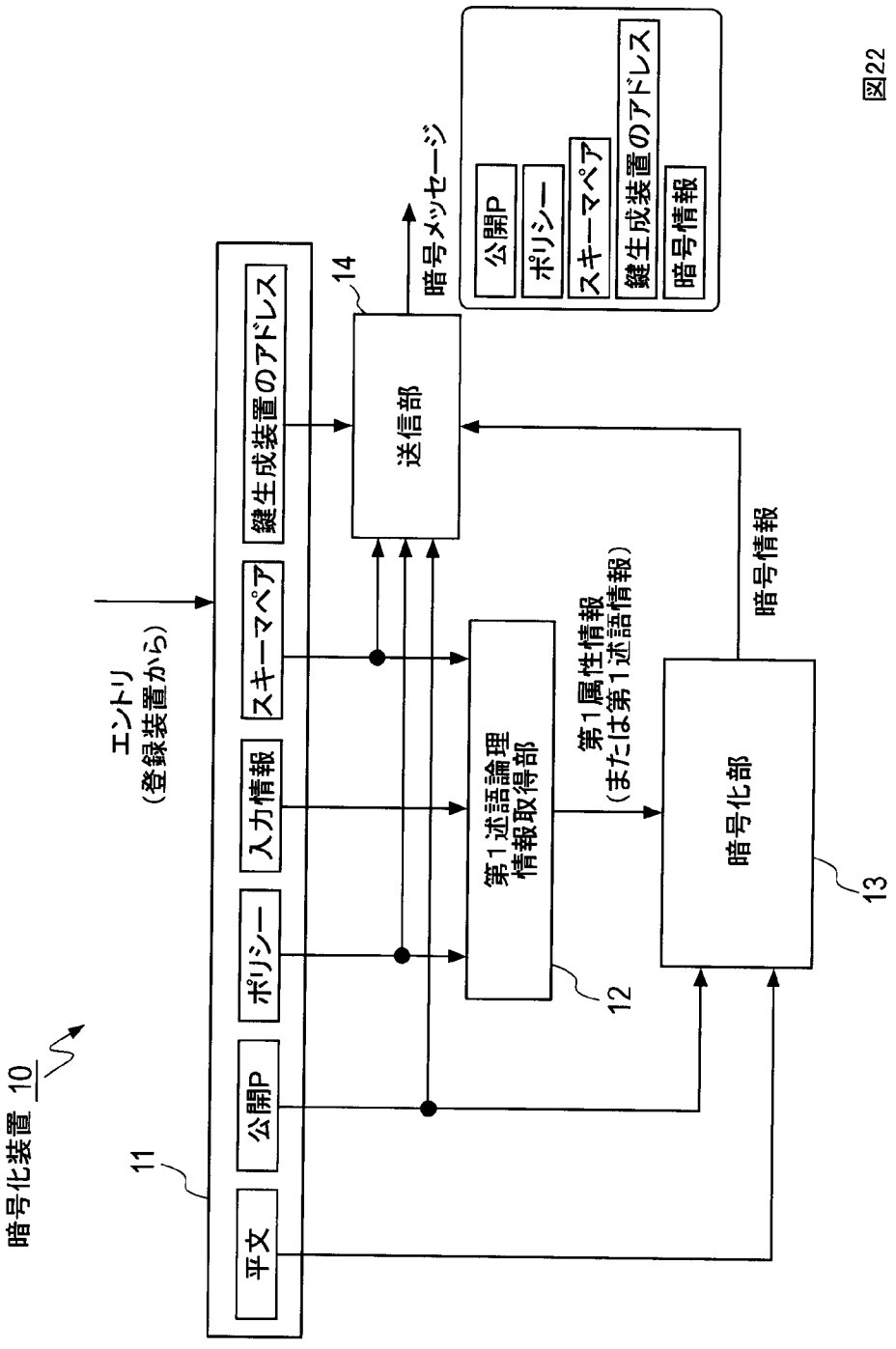

暗号化装置 10
11
平文
公開P
ポリシー
入力情報
スキーマペア
鍵生成装置のアドレス
エントリ
(登録装置から)
第1述語論理
情報取得部
12
第1属性情報
(または第1述語情報)
暗号化部
13
暗号情報
送信部
14
暗号メッセージ
公開P
ポリシー
スキーマペア
鍵生成装置のアドレス
暗号情報

図22

[図23]

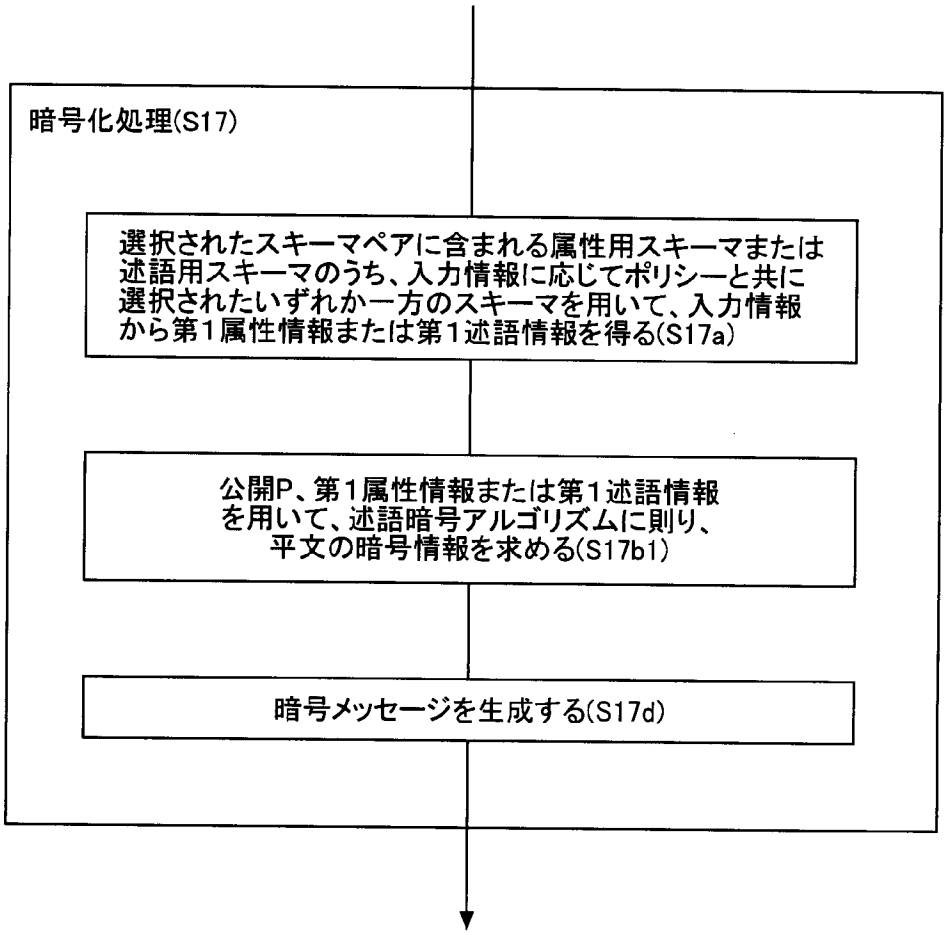

暗号化処理(S17)
選択されたスキーマペアに含まれる属性用スキーマまたは述語用スキーマのうち、入力情報に応じてポリシーと共に選択されたいずれか一方のスキーマを用いて、入力情報から第1属性情報または第1述語情報を得る(S17a)
公開P、第1属性情報または第1述語情報を用いて、述語暗号アルゴリズムに則り、平文の暗号情報を求める(S17b1)
暗号メッセージを生成する(S17d)

図23

[図24]

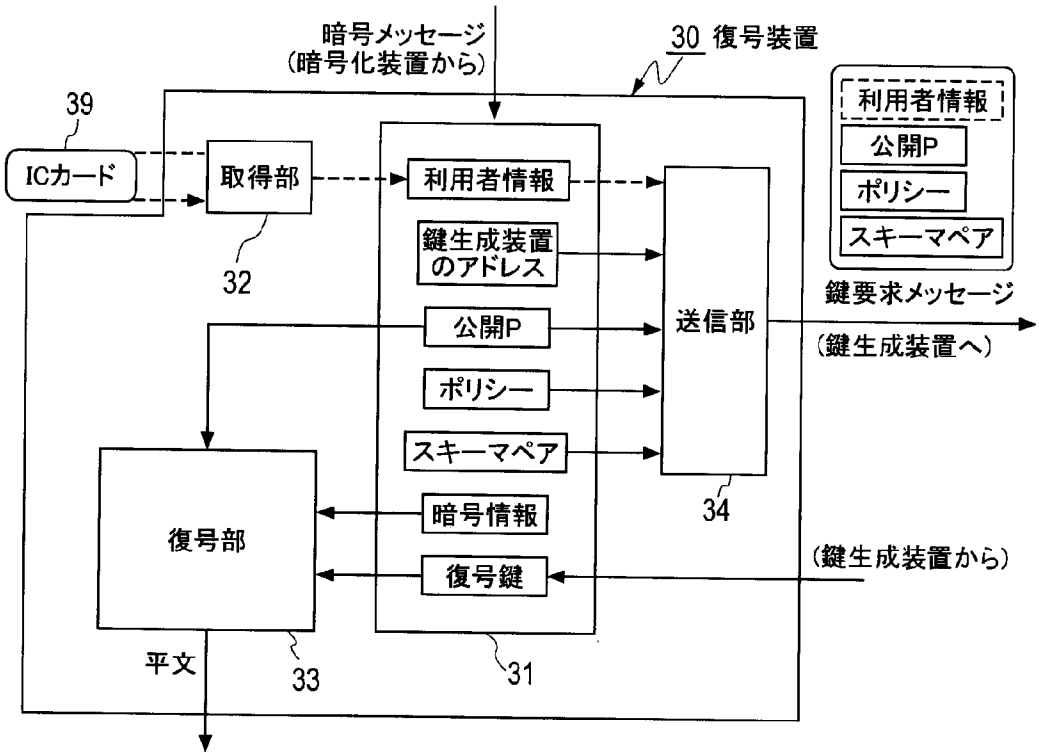

暗号メッセージ
(暗号化装置から)
30 復号装置
39
ICカード
取得部
32
利用者情報
鍵生成装置
のアドレス
公開P
ポリシー
スキーマペア
送信部
34
利用者情報
公開P
ポリシー
スキーマペア
鍵要求メッセージ
(鍵生成装置へ)
復号部
暗号情報
復号鍵
(鍵生成装置から)
平文
33
31

図24

[図25]

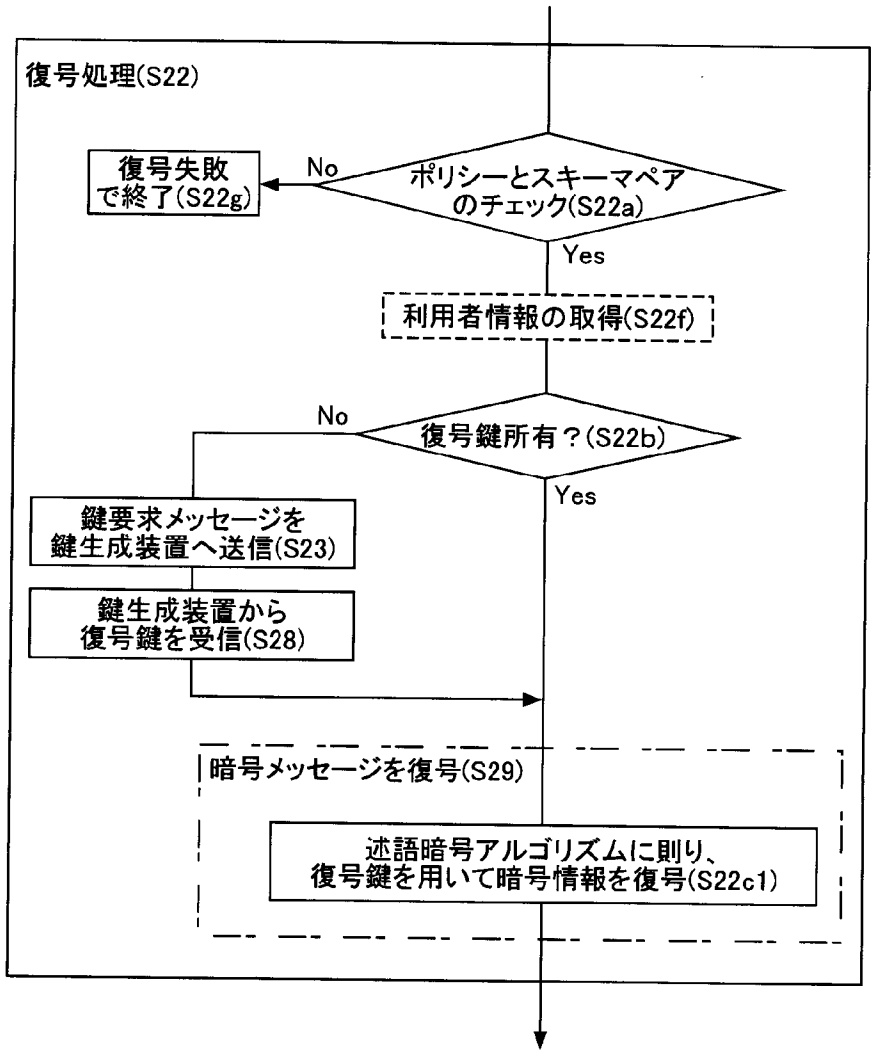

復号処理(S22)
ポリシーとスキーマペア のチェック(S22a)
No
復号失敗 で終了(S22g)
Yes
利用者情報の取得(S22f)
復号鍵所有？(S22b)
No
Yes
鍵要求メッセージを 鍵生成装置へ送信(S23)
鍵生成装置から 復号鍵を受信(S28)
暗号メッセージを復号(S29)
述語暗号アルゴリズムに則り、 復号鍵を用いて暗号情報を復号(S22c1)

図25

[図26]

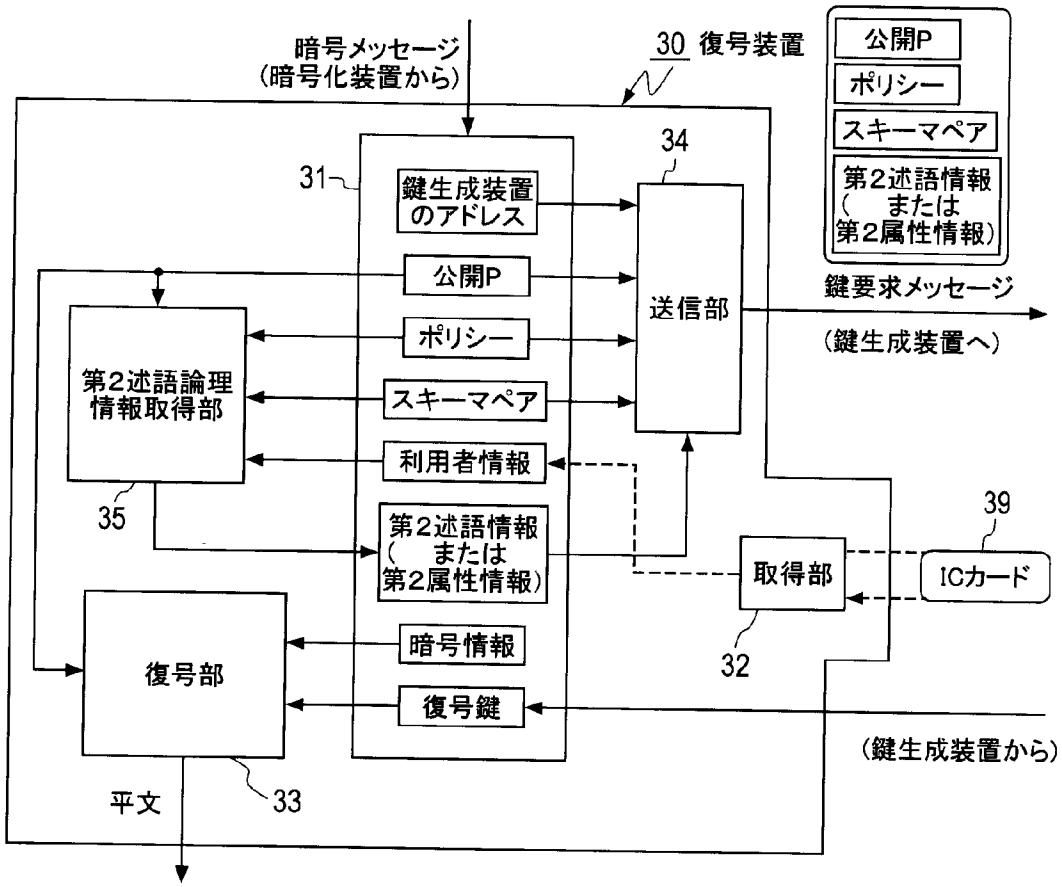

暗号メッセージ
(暗号化装置から)
30 復号装置
公開P
ポリシー
スキーマペア
第2述語情報
(または
第2属性情報)
34
31
鍵生成装置
のアドレス
公開P
ポリシー
スキーマペア
利用者情報
送信部
鍵要求メッセージ
(鍵生成装置へ)
第2述語論理
情報取得部
35
第2述語情報
(または
第2属性情報)
39
取得部
ICカード
32
暗号情報
復号鍵
復号部
(鍵生成装置から)
平文
33

図26

[図27]

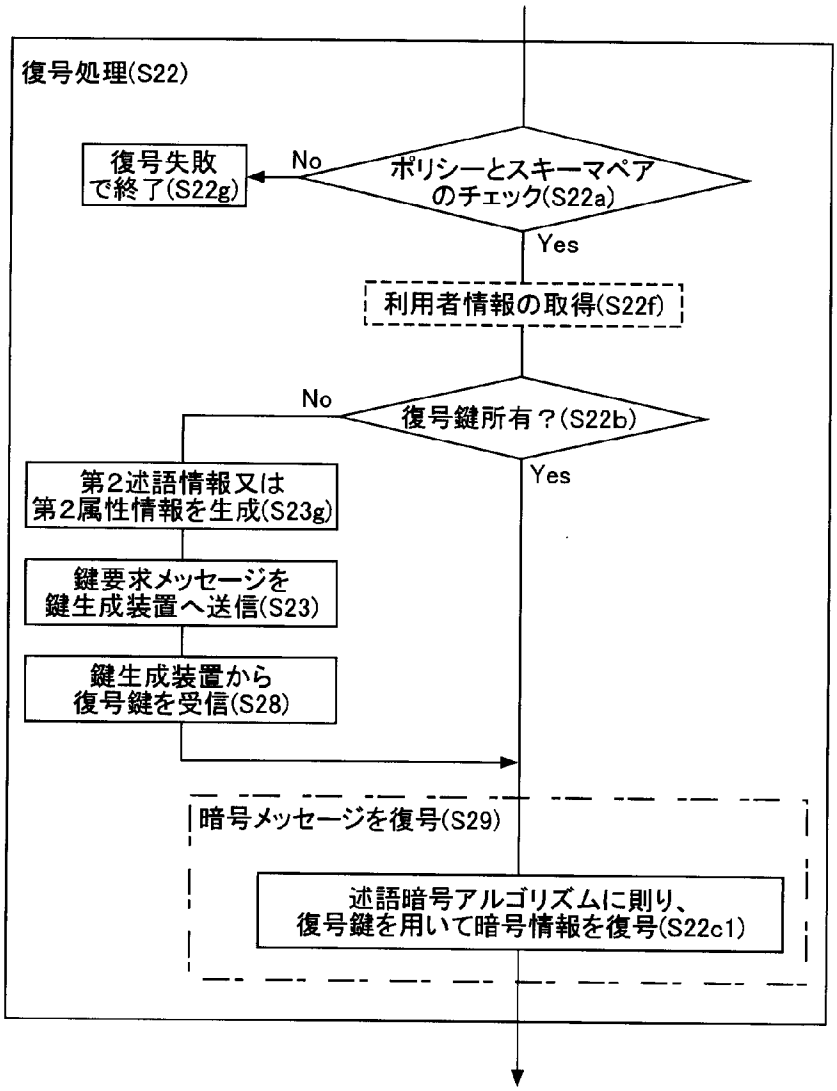

復号処理(S22)
ポリシーとスキーマペアのチェック(S22a)
No
復号失敗で終了(S22g)
Yes
利用者情報の取得(S22f)
復号鍵所有？(S22b)
No
Yes
第2述語情報又は第2属性情報を生成(S23g)
鍵要求メッセージを鍵生成装置へ送信(S23)
鍵生成装置から復号鍵を受信(S28)
暗号メッセージを復号(S29)
述語暗号アルゴリズムに則り、復号鍵を用いて暗号情報を復号(S22c1)

図27

[図28]

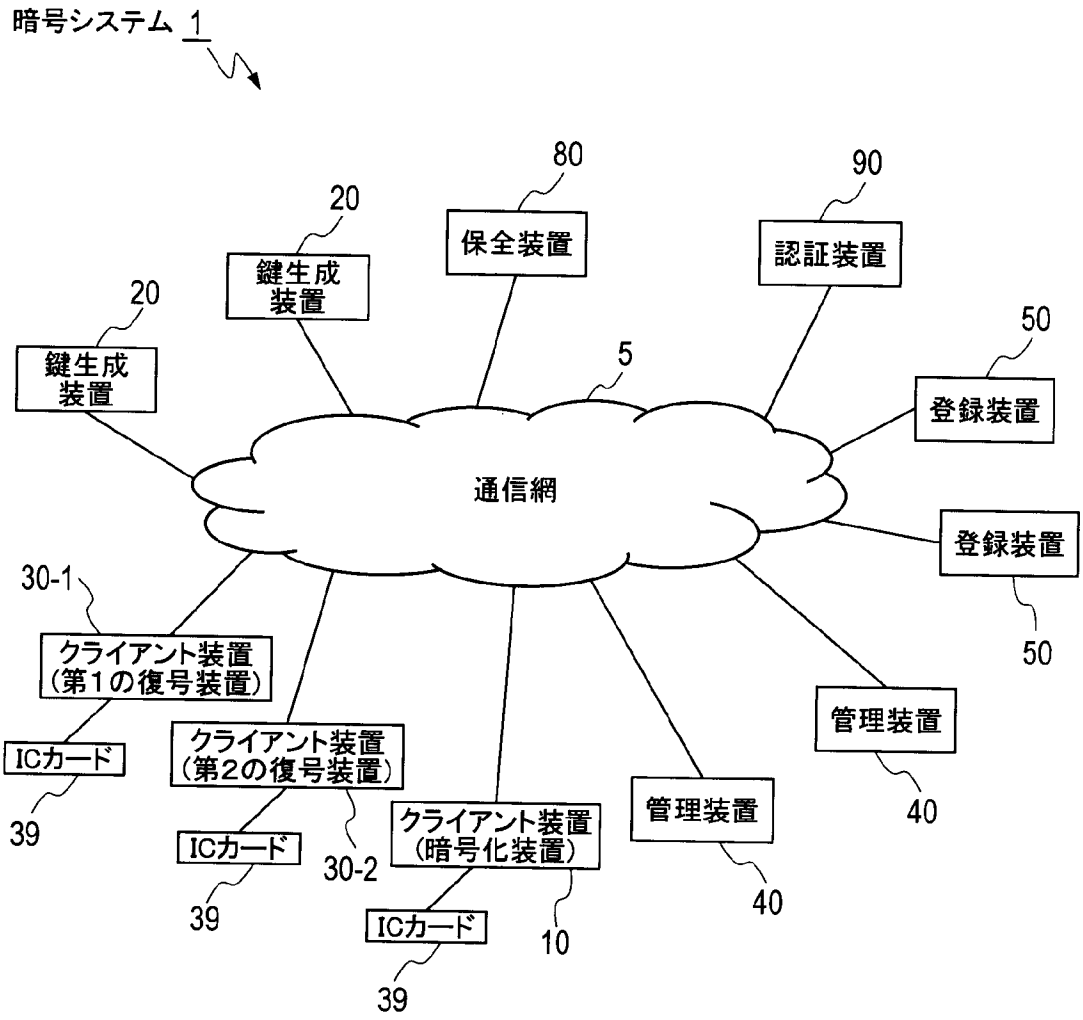

暗号システム 1
80
保全装置
90
認証装置
20
鍵生成装置
20
鍵生成装置
5
通信網
50
登録装置
登録装置
50
30-1
クライアント装置（第1の復号装置）
ICカード
39
クライアント装置（第2の復号装置）
30-2
ICカード
39
クライアント装置（暗号化装置）
ICカード
39
10
管理装置
40
管理装置
40

図28

[図29]

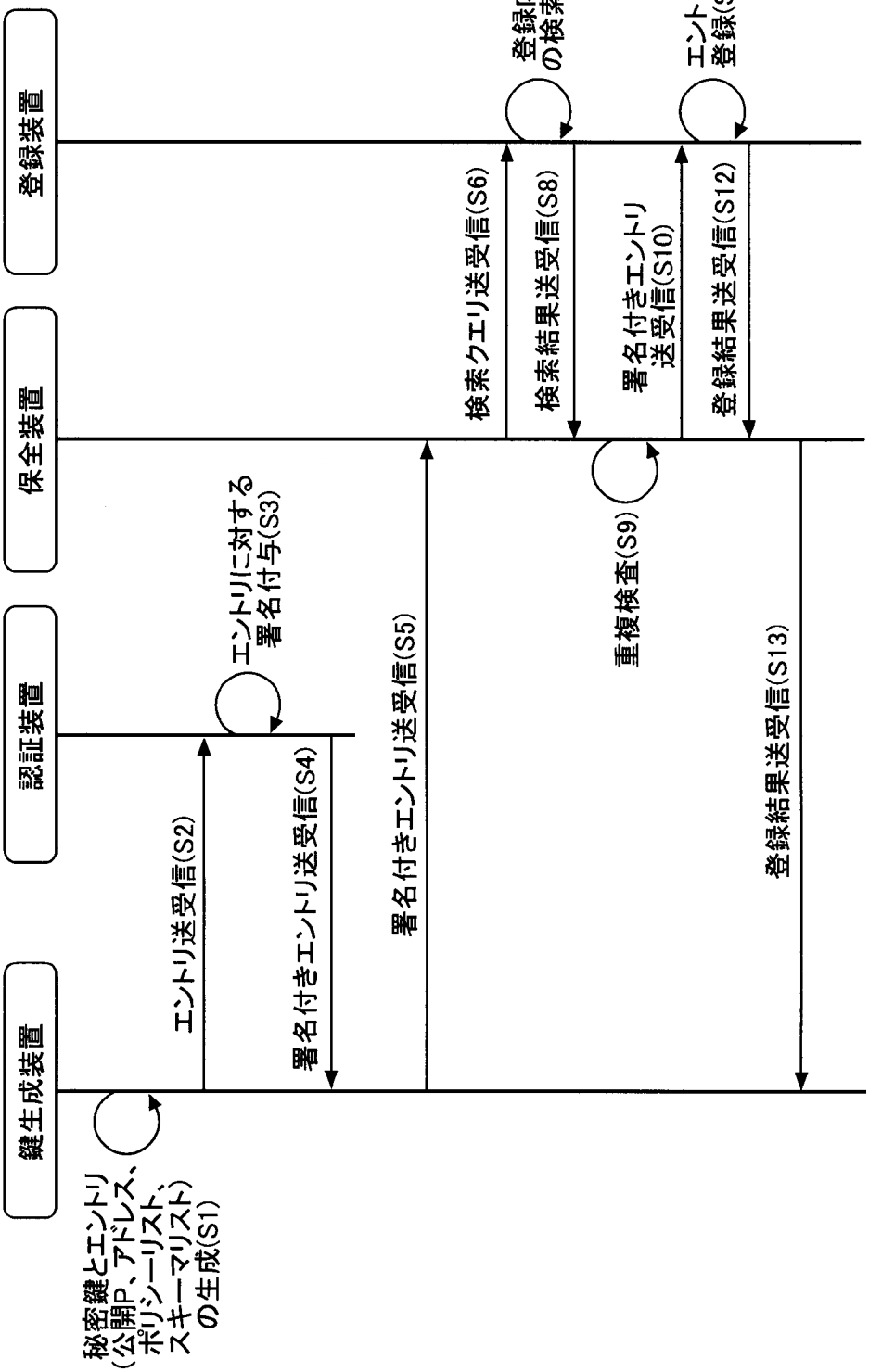

鍵生成装置
認証装置
保全装置
登録装置
秘密鍵とエントリ
(公開P、アドレス、
ポリシーリスト、
スキーマリスト)
の生成(S1)
エントリ送受信(S2)
エントリに対する
署名付与(S3)
署名付きエントリ送受信(S4)
署名付きエントリ送受信(S5)
検索クエリ送受信(S6)
登録内容
の検索(S7)
検索結果送受信(S8)
重複検査(S9)
署名付きエントリ
送受信(S10)
エントリの
登録(S11)
登録結果送受信(S12)
登録結果送受信(S13)

図29

[図30]

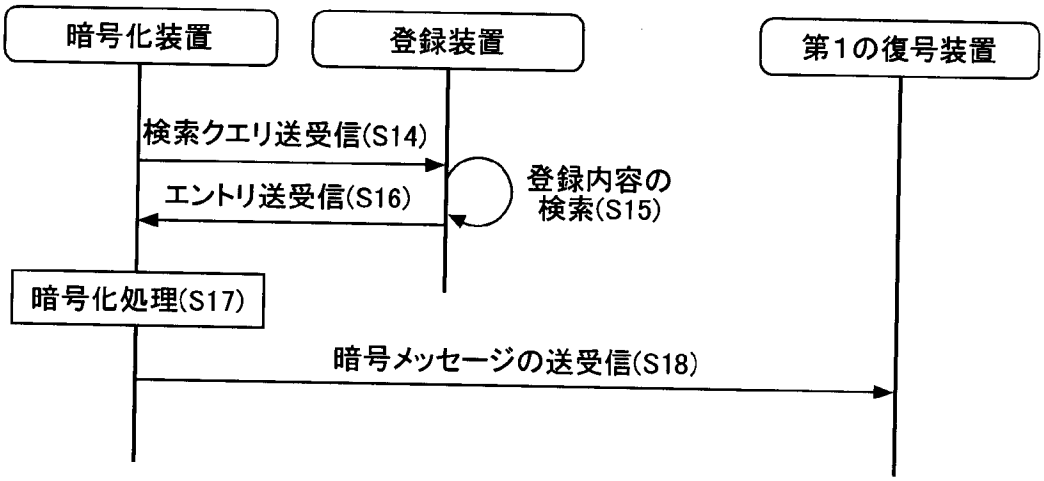

暗号化装置
登録装置
第1の復号装置
検索クエリ送受信(S14)
登録内容の
検索(S15)
エントリ送受信(S16)
暗号化処理(S17)
暗号メッセージの送受信(S18)

図30

[図31]

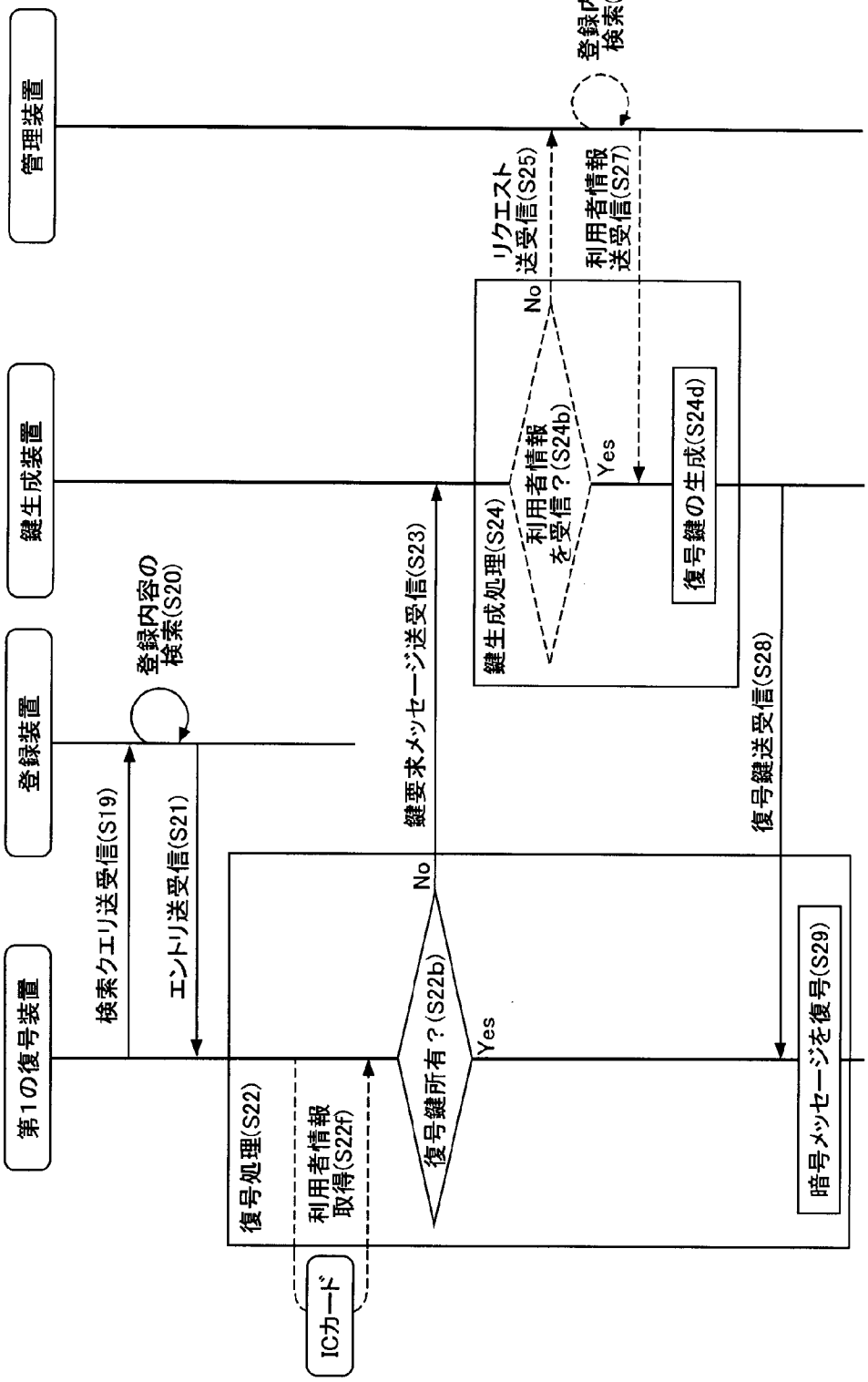

管理装置
鍵生成装置
登録装置
第1の復号装置
登録内容の検索(S26)
リクエスト送受信(S25)
利用者情報送受信(S27)
No
Yes
鍵生成処理(S24)
利用者情報を受信？(S24b)
復号鍵の生成(S24d)
登録内容の検索(S20)
検索クエリ送受信(S19)
エントリ送受信(S21)
鍵要求メッセージ送受信(S23)
復号鍵送受信(S28)
No
Yes
復号処理(S22)
利用者情報取得(S22f)
復号鍵所有？(S22b)
暗号メッセージを復号(S29)
ICカード

図31

[図32]

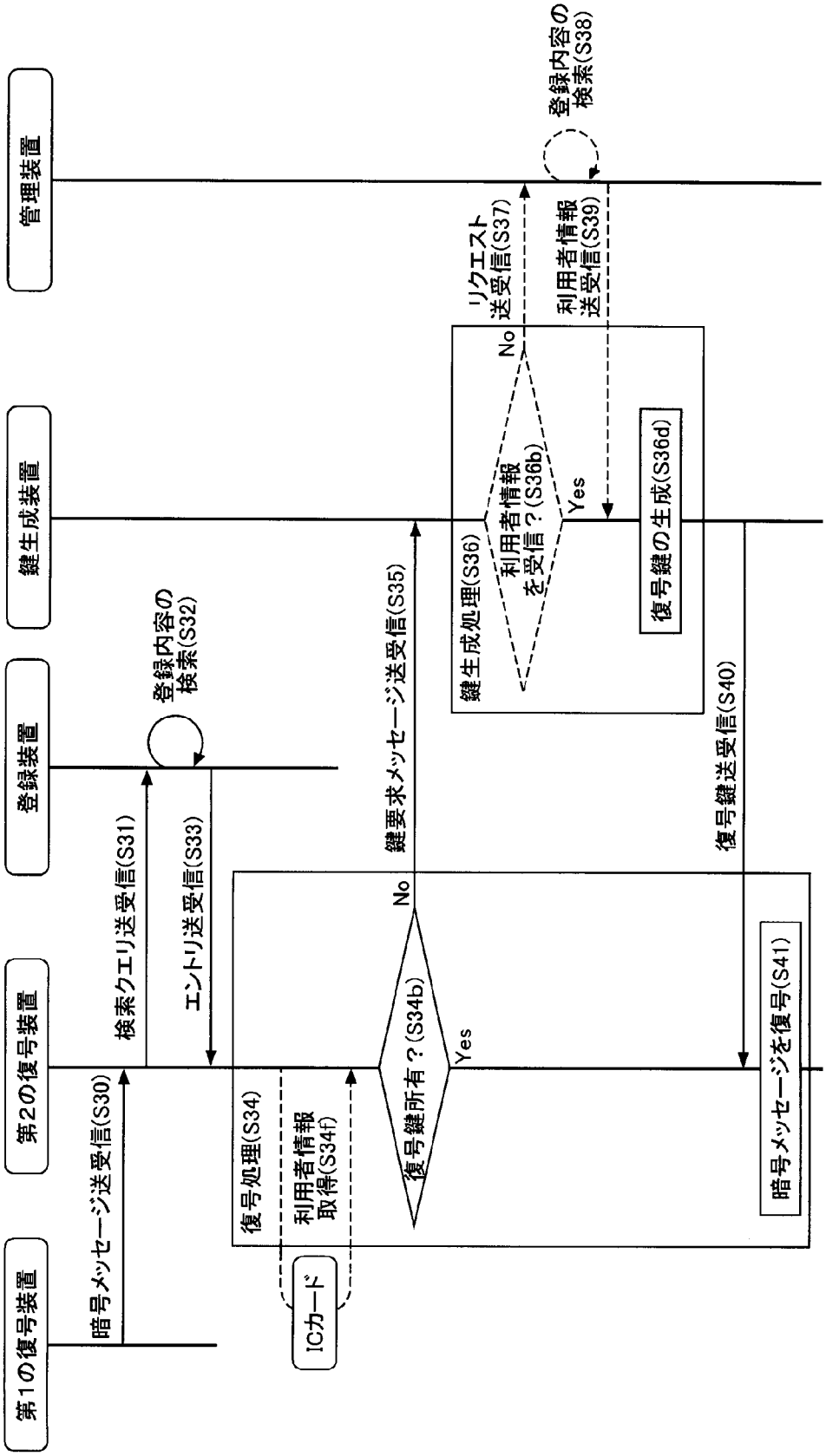

管理装置
鍵生成装置
登録装置
第2の復号装置
第1の復号装置
登録内容の検索(S38)
リクエスト送受信(S37)
利用者情報送受信(S39)
No
Yes
鍵生成処理(S36)
利用者情報を受信？(S36b)
復号鍵の生成(S36d)
登録内容の検索(S32)
検索クエリ送受信(S31)
エントリ送受信(S33)
鍵要求メッセージ送受信(S35)
復号鍵送受信(S40)
暗号メッセージ送受信(S30)
復号処理(S34)
利用者情報取得(S34f)
ICカード
No
Yes
復号鍵所有？(S34b)
暗号メッセージを復号(S41)

図32

[図33]

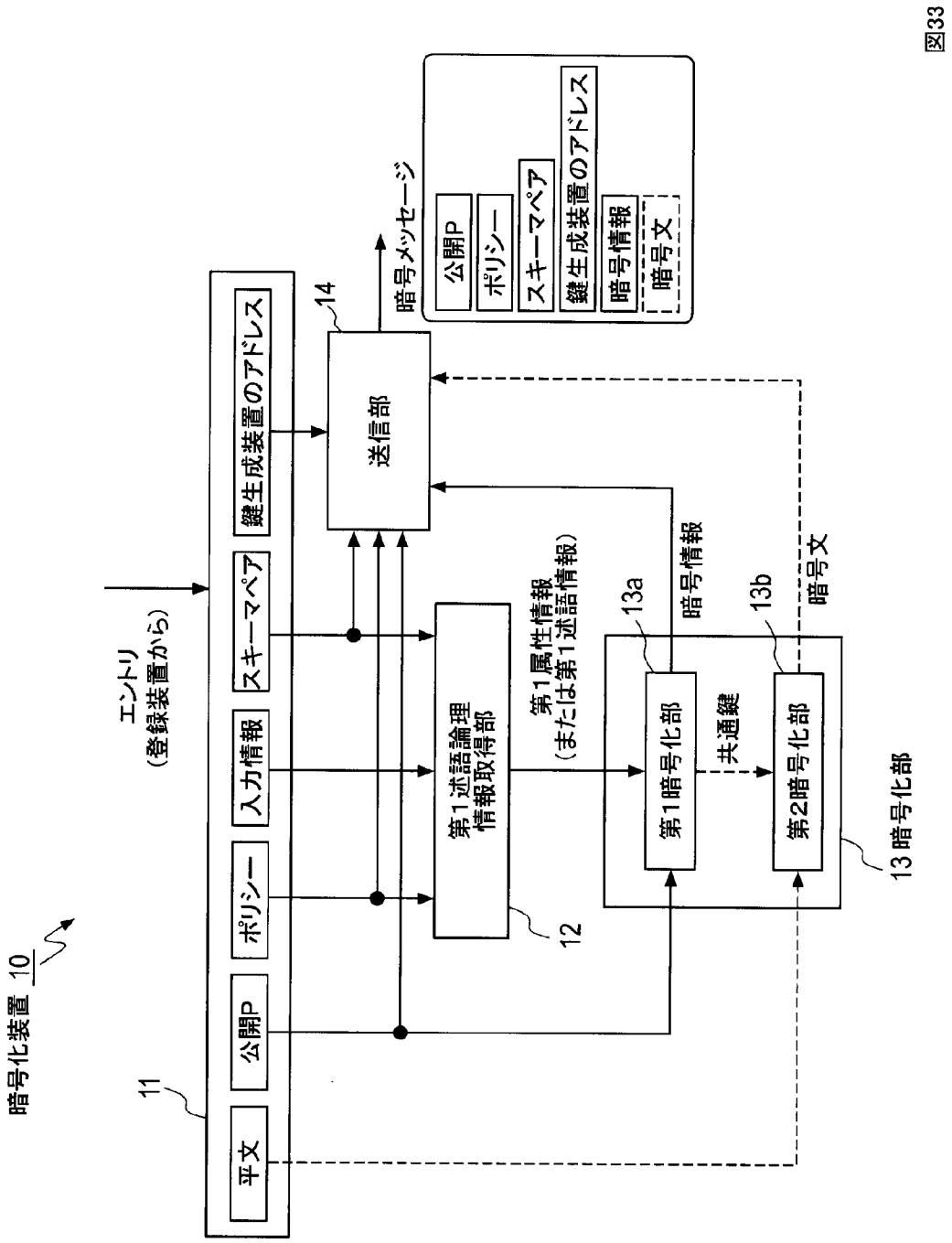

暗号化装置 10
11
平文
公開P
ポリシー
入力情報
スキーマペア
鍵生成装置のアドレス
エントリ
(登録装置から)
第1述語論理
情報取得部
12
第1属性情報
(または第1述語情報)
13a
第1暗号化部
暗号情報
共通鍵
13b
第2暗号化部
暗号文
13 暗号化部
送信部
14
暗号メッセージ
公開P
ポリシー
スキーマペア
鍵生成装置のアドレス
暗号情報
暗号文

図33

[図34]

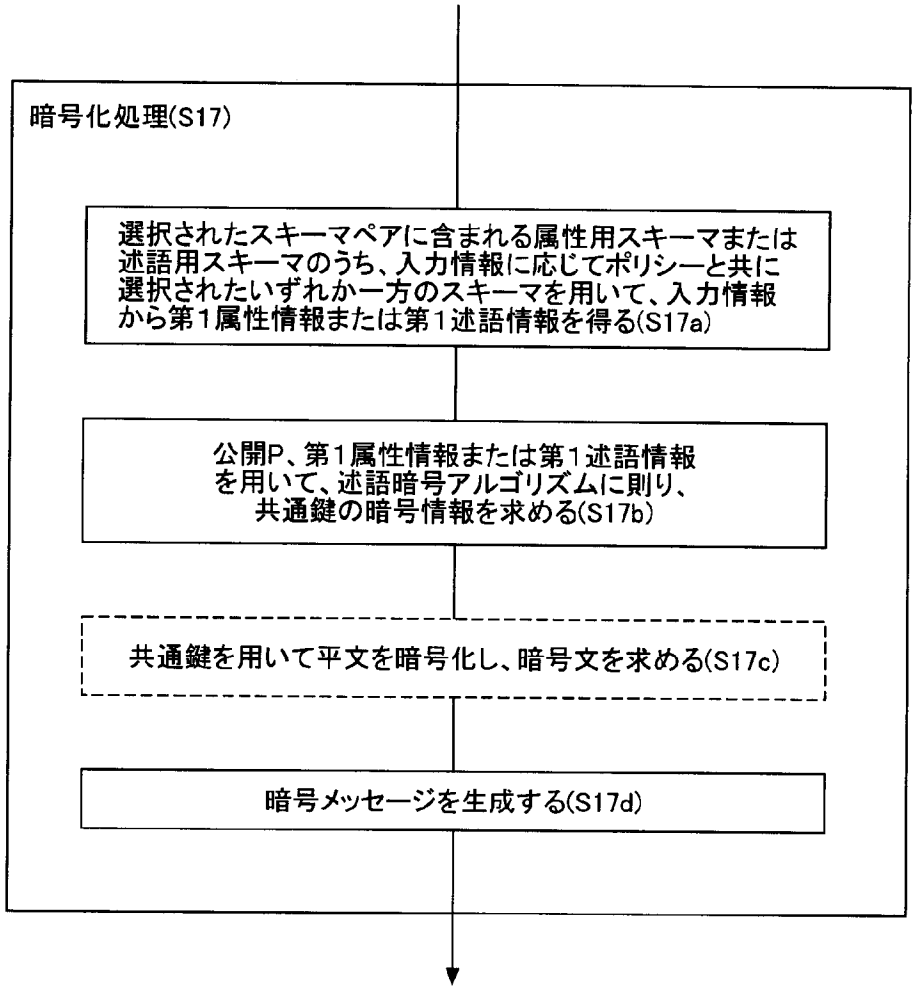

暗号化処理(S17)
選択されたスキーマペアに含まれる属性用スキーマまたは述語用スキーマのうち、入力情報に応じてポリシーと共に選択されたいずれか一方のスキーマを用いて、入力情報から第1属性情報または第1述語情報を得る(S17a)
公開P、第1属性情報または第1述語情報を用いて、述語暗号アルゴリズムに則り、共通鍵の暗号情報を求める(S17b)
共通鍵を用いて平文を暗号化し、暗号文を求める(S17c)
暗号メッセージを生成する(S17d)

図34

[図35]

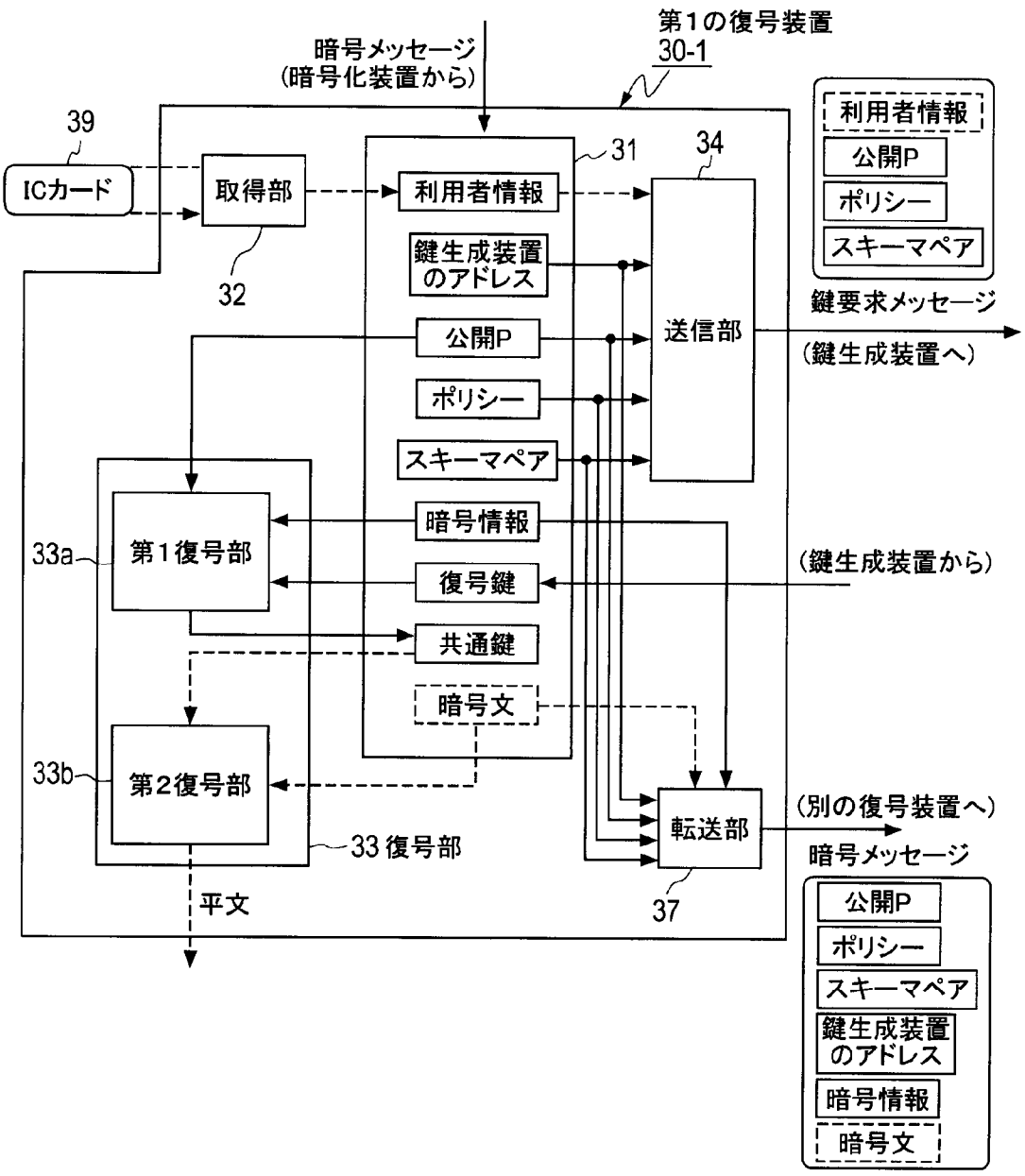

第1の復号装置
30-1
暗号メッセージ
(暗号化装置から)
39
ICカード
取得部
32
31
34
利用者情報
鍵生成装置のアドレス
公開P
ポリシー
スキーマペア
送信部
利用者情報
公開P
ポリシー
スキーマペア
鍵要求メッセージ
(鍵生成装置へ)
暗号情報
復号鍵
共通鍵
暗号文
(鍵生成装置から)
33a
第1復号部
33b
第2復号部
33 復号部
平文
転送部
37
(別の復号装置へ)
暗号メッセージ
公開P
ポリシー
スキーマペア
鍵生成装置のアドレス
暗号情報
暗号文

図35

[図36]

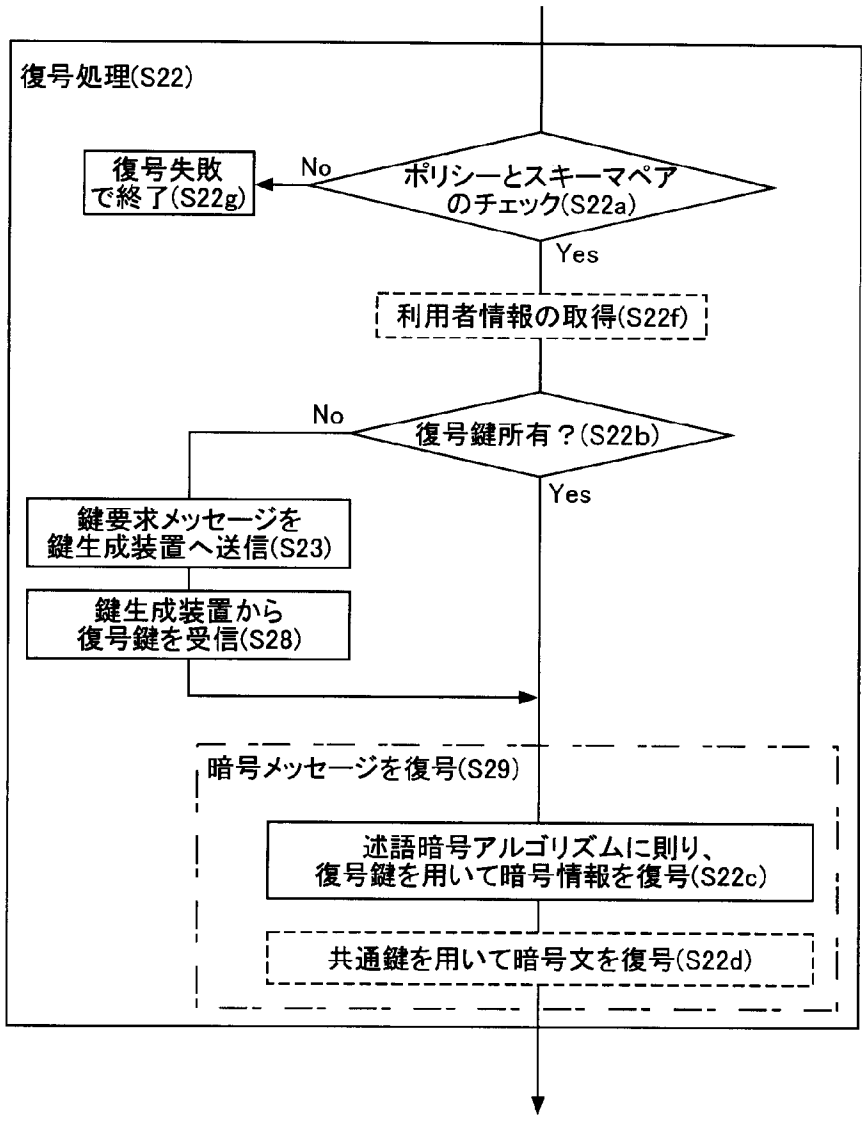

復号処理(S22)
ポリシーとスキーマペアのチェック(S22a)
No
復号失敗で終了(S22g)
Yes
利用者情報の取得(S22f)
復号鍵所有？(S22b)
No
Yes
鍵要求メッセージを鍵生成装置へ送信(S23)
鍵生成装置から復号鍵を受信(S28)
暗号メッセージを復号(S29)
述語暗号アルゴリズムに則り、復号鍵を用いて暗号情報を復号(S22c)
共通鍵を用いて暗号文を復号(S22d)

図36

[図37]

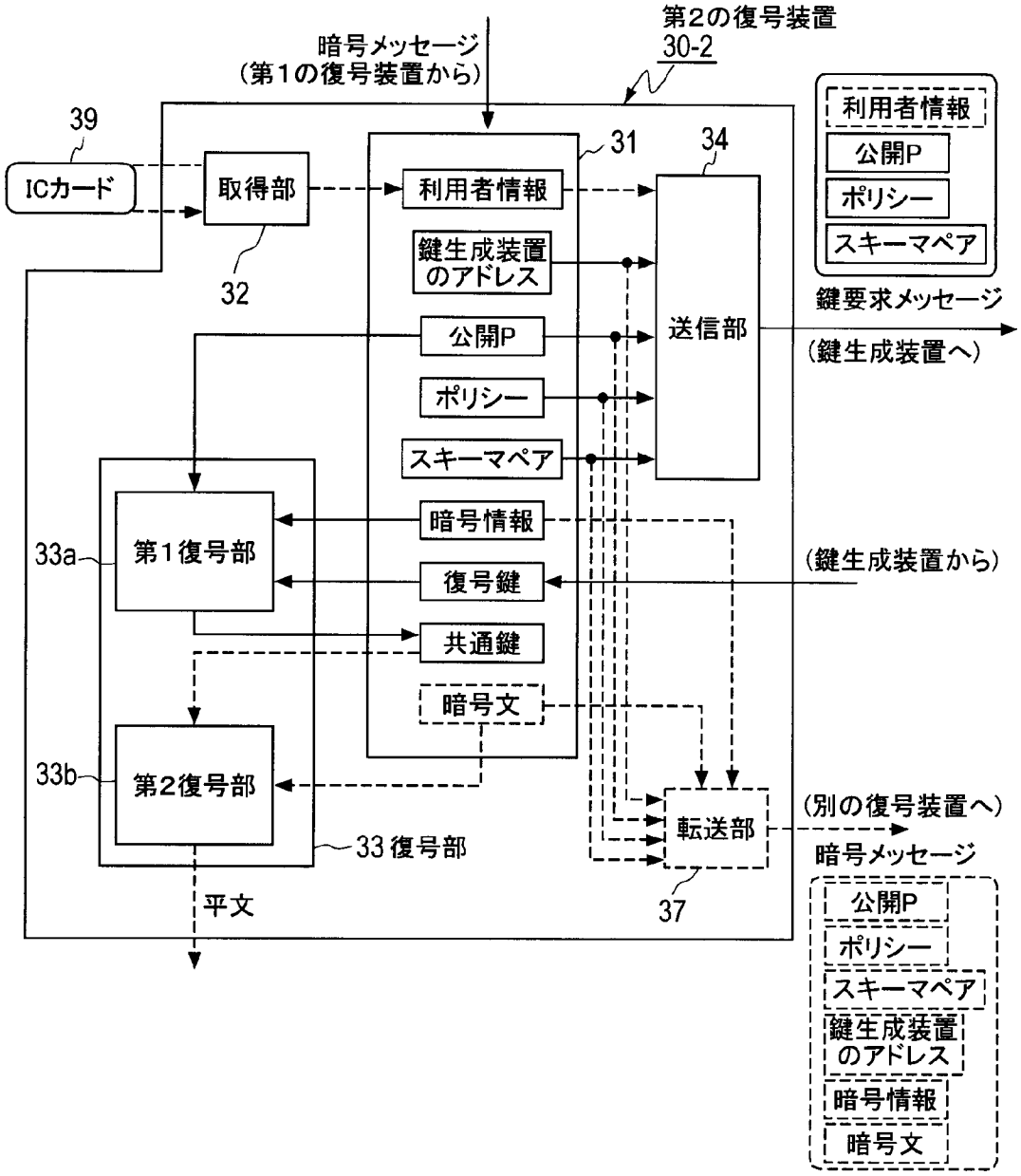

第2の復号装置
30-2
暗号メッセージ
(第1の復号装置から)
39
ICカード
取得部
32
31
34
利用者情報
鍵生成装置のアドレス
公開P
ポリシー
スキーマペア
送信部
利用者情報
公開P
ポリシー
スキーマペア
鍵要求メッセージ
(鍵生成装置へ)
暗号情報
復号鍵
共通鍵
暗号文
(鍵生成装置から)
33a
第1復号部
33b
第2復号部
33 復号部
平文
転送部
37
(別の復号装置へ)
暗号メッセージ
公開P
ポリシー
スキーマペア
鍵生成装置のアドレス
暗号情報
暗号文

図37

[図38]

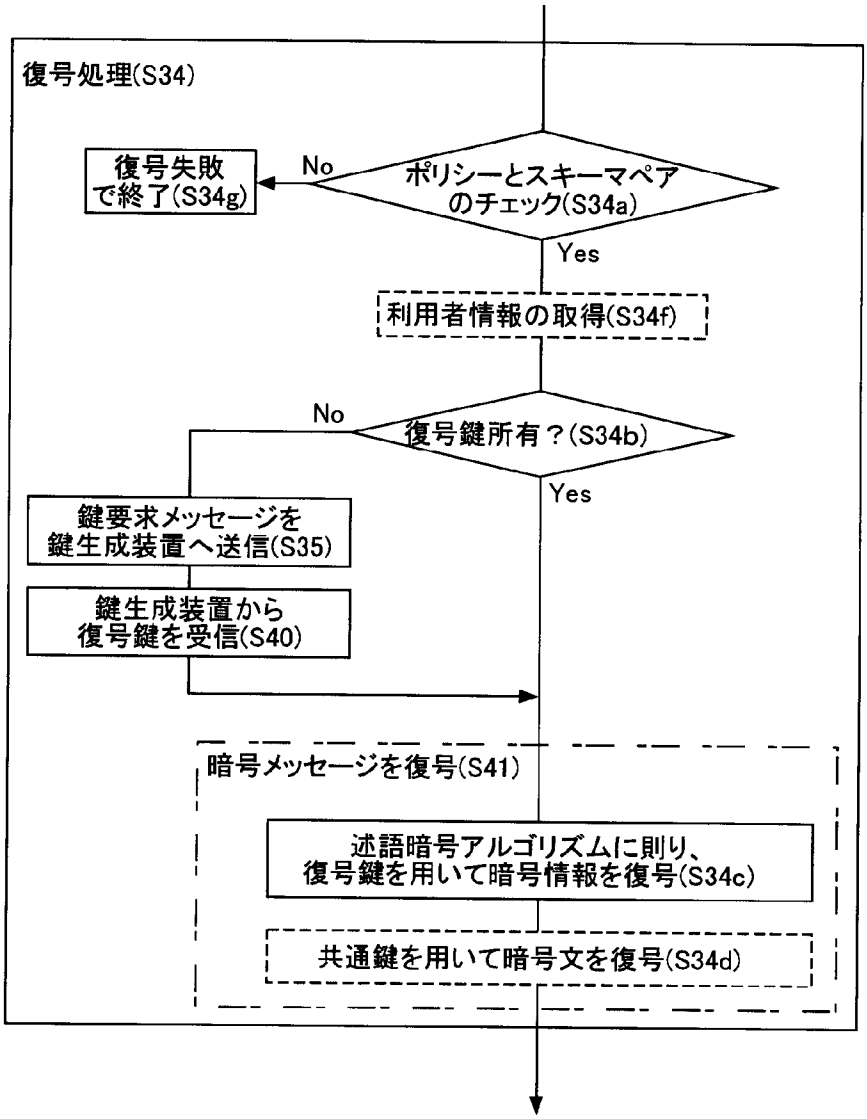

復号処理(S34)
ポリシーとスキーマペアのチェック(S34a)
No
復号失敗で終了(S34g)
Yes
利用者情報の取得(S34f)
復号鍵所有？(S34b)
No
Yes
鍵要求メッセージを鍵生成装置へ送信(S35)
鍵生成装置から復号鍵を受信(S40)
暗号メッセージを復号(S41)
述語暗号アルゴリズムに則り、復号鍵を用いて暗号情報を復号(S34c)
共通鍵を用いて暗号文を復号(S34d)

図38

[図39]

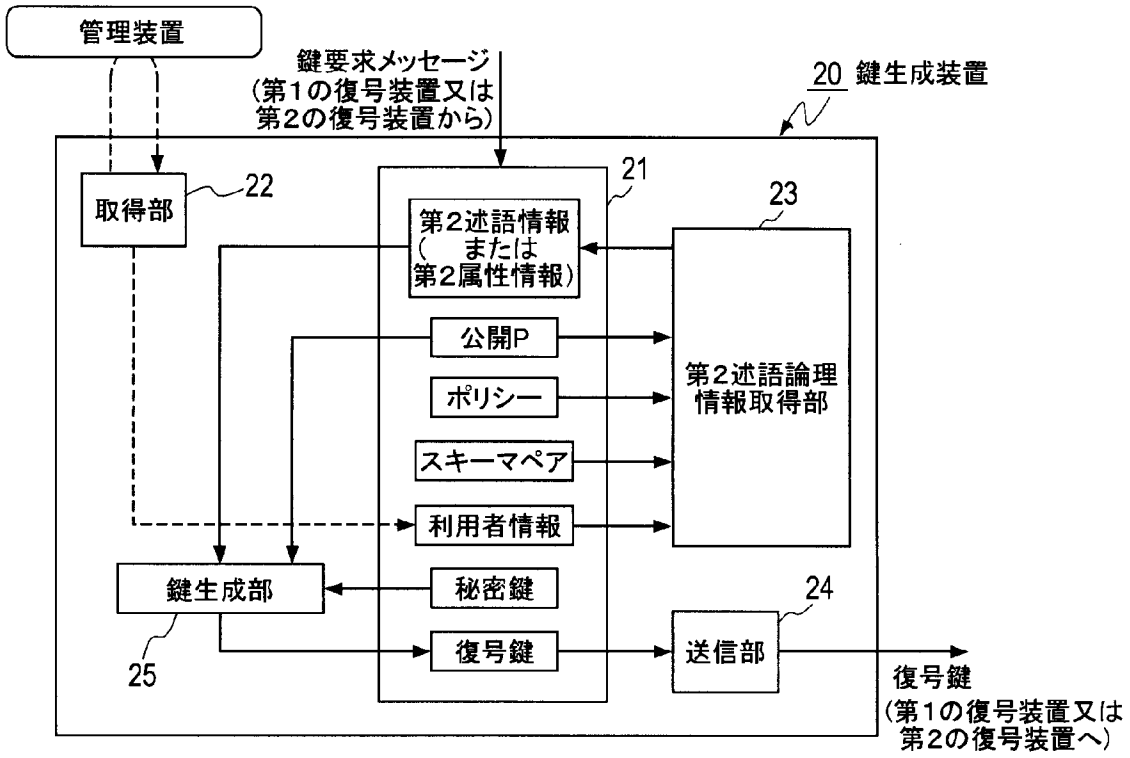

管理装置
鍵要求メッセージ
(第1の復号装置又は
第2の復号装置から)
20 鍵生成装置
取得部
22
21
23
第2述語情報
(または
第2属性情報)
公開P
ポリシー
スキーマペア
利用者情報
第2述語論理
情報取得部
鍵生成部
秘密鍵
24
復号鍵
送信部
25
復号鍵
(第1の復号装置又は
第2の復号装置へ)

図39

[図40]

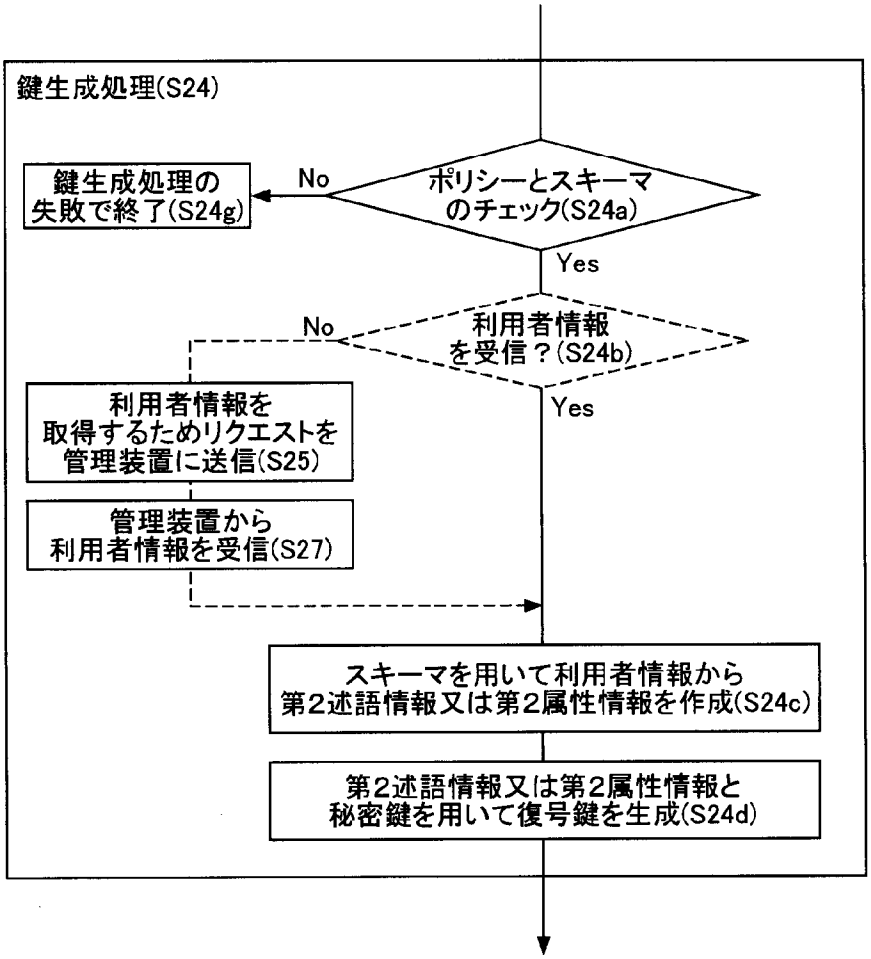

鍵生成処理(S24)
鍵生成処理の
失敗で終了(S24g)
No
ポリシーとスキーマ
のチェック(S24a)
Yes
No
利用者情報
を受信？(S24b)
Yes
利用者情報を
取得するためリクエストを
管理装置に送信(S25)
管理装置から
利用者情報を受信(S27)
スキーマを用いて利用者情報から
第2述語情報又は第2属性情報を作成(S24c)
第2述語情報又は第2属性情報と
秘密鍵を用いて復号鍵を生成(S24d)

図40

[図41]

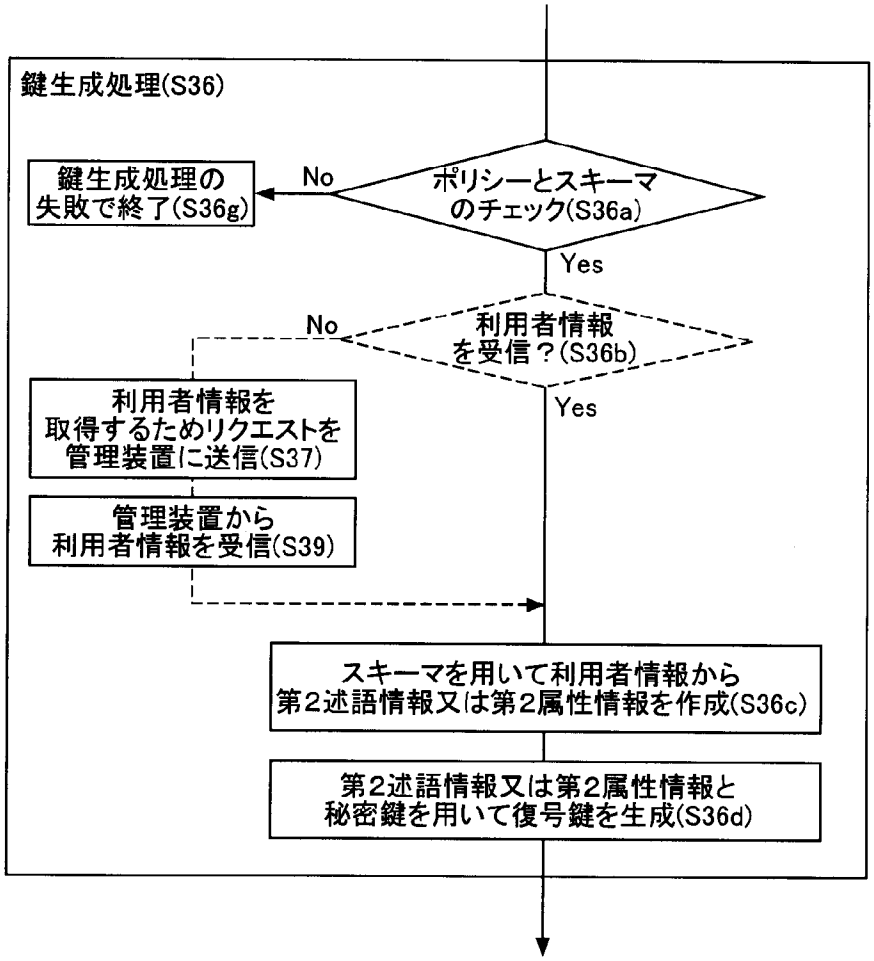

鍵生成処理(S36)
鍵生成処理の
失敗で終了(S36g)
No
ポリシーとスキーマ
のチェック(S36a)
Yes
No
利用者情報
を受信？(S36b)
Yes
利用者情報を
取得するためリクエストを
管理装置に送信(S37)
管理装置から
利用者情報を受信(S39)
スキーマを用いて利用者情報から
第2述語情報又は第2属性情報を作成(S36c)
第2述語情報又は第2属性情報と
秘密鍵を用いて復号鍵を生成(S36d)

図41

[図42]

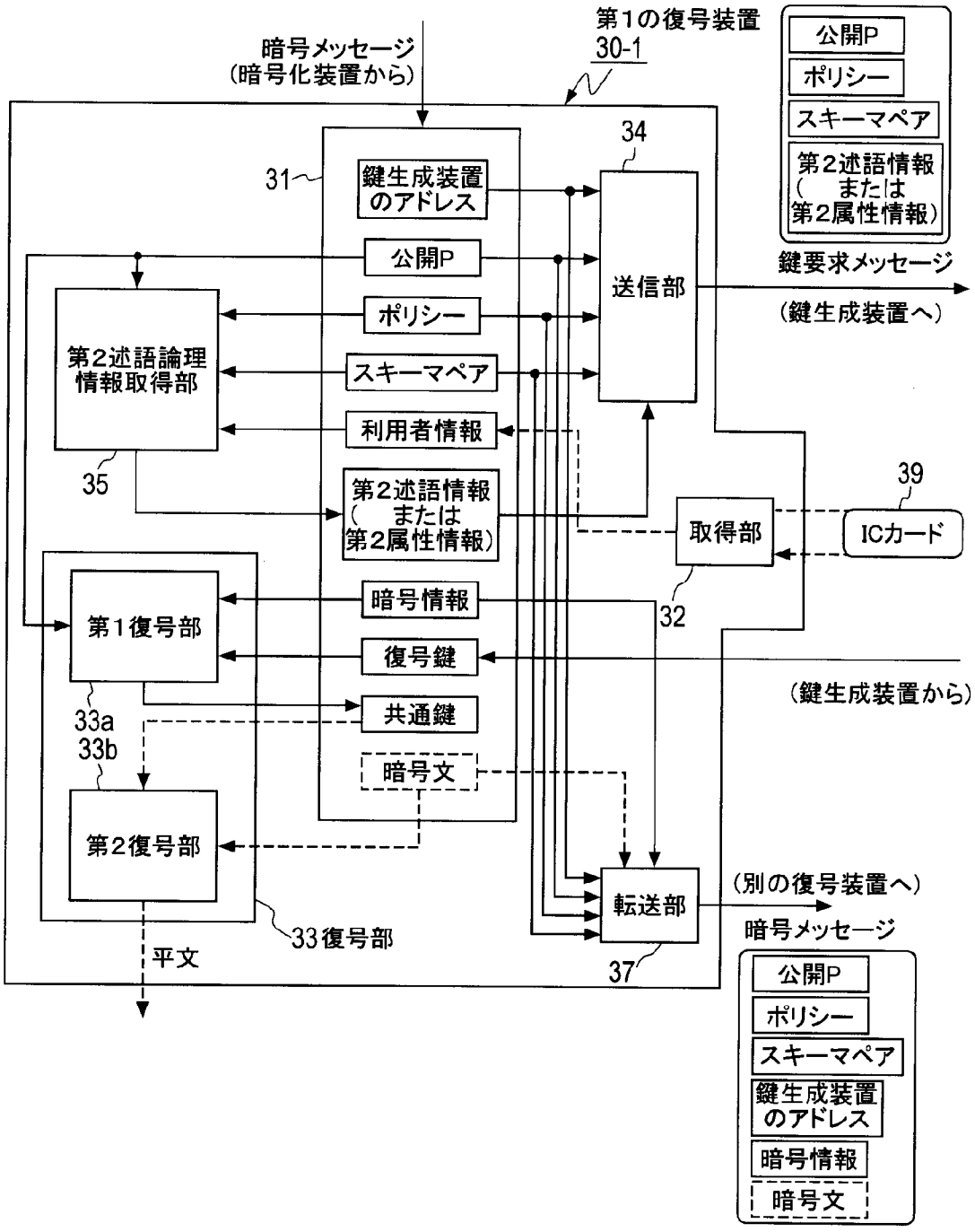

第1の復号装置
30-1
暗号メッセージ
(暗号化装置から)
公開P
ポリシー
スキーマペア
第2述語情報
(または
第2属性情報)
31
鍵生成装置
のアドレス
34
公開P
ポリシー
スキーマペア
利用者情報
送信部
鍵要求メッセージ
(鍵生成装置へ)
第2述語論理
情報取得部
35
第2述語情報
(または
第2属性情報)
39
取得部
ICカード
32
暗号情報
復号鍵
(鍵生成装置から)
第1復号部
33a
33b
共通鍵
暗号文
第2復号部
転送部
(別の復号装置へ)
暗号メッセージ
33復号部
平文
37
公開P
ポリシー
スキーマペア
鍵生成装置
のアドレス
暗号情報
暗号文

図42

[図43]

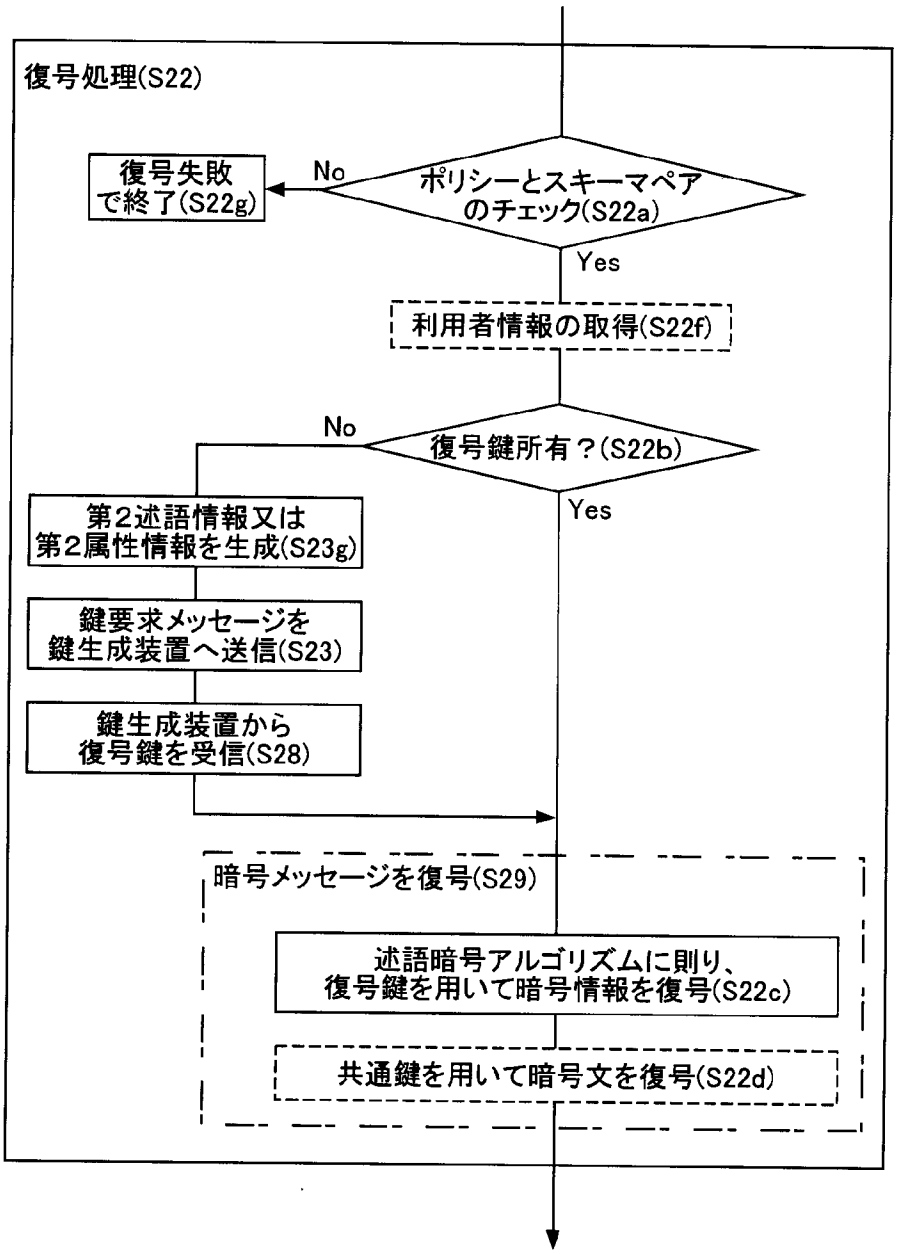

復号処理(S22)
ポリシーとスキーマペアのチェック(S22a)
No
復号失敗で終了(S22g)
Yes
利用者情報の取得(S22f)
復号鍵所有？(S22b)
No
Yes
第2述語情報又は第2属性情報を生成(S23g)
鍵要求メッセージを鍵生成装置へ送信(S23)
鍵生成装置から復号鍵を受信(S28)
暗号メッセージを復号(S29)
述語暗号アルゴリズムに則り、復号鍵を用いて暗号情報を復号(S22c)
共通鍵を用いて暗号文を復号(S22d)

図43

[図44]

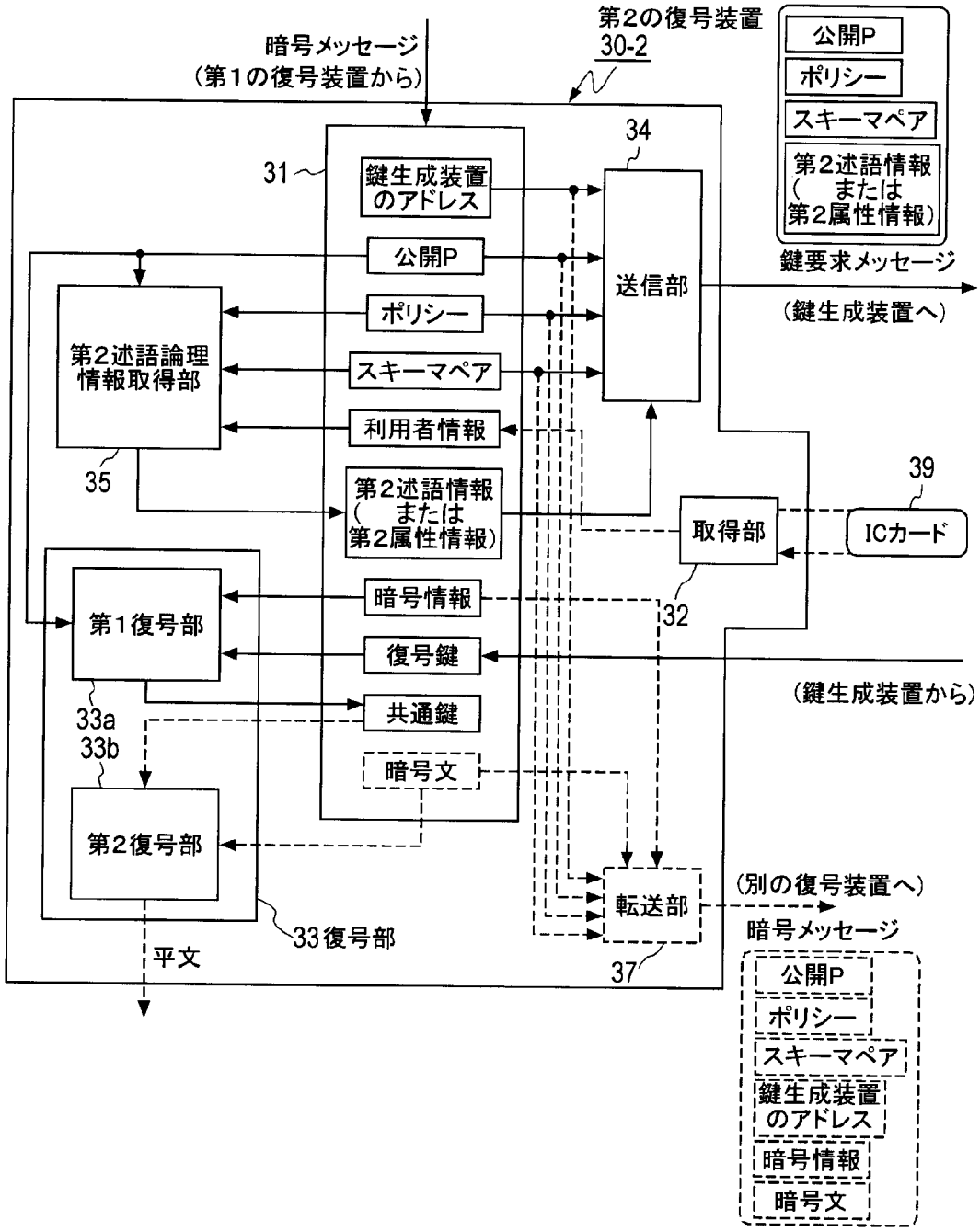

暗号メッセージ
(第1の復号装置から)
第2の復号装置
30-2
公開P
ポリシー
スキーマペア
第2述語情報
(または
第2属性情報)
鍵要求メッセージ
(鍵生成装置へ)
31
鍵生成装置
のアドレス
公開P
ポリシー
スキーマペア
利用者情報
第2述語情報
(または
第2属性情報)
暗号情報
復号鍵
共通鍵
暗号文
34
送信部
第2述語論理
情報取得部
35
39
取得部
ICカード
32
(鍵生成装置から)
第1復号部
33a
33b
第2復号部
33復号部
平文
転送部
37
(別の復号装置へ)
暗号メッセージ
公開P
ポリシー
スキーマペア
鍵生成装置
のアドレス
暗号情報
暗号文

図44

[図45]

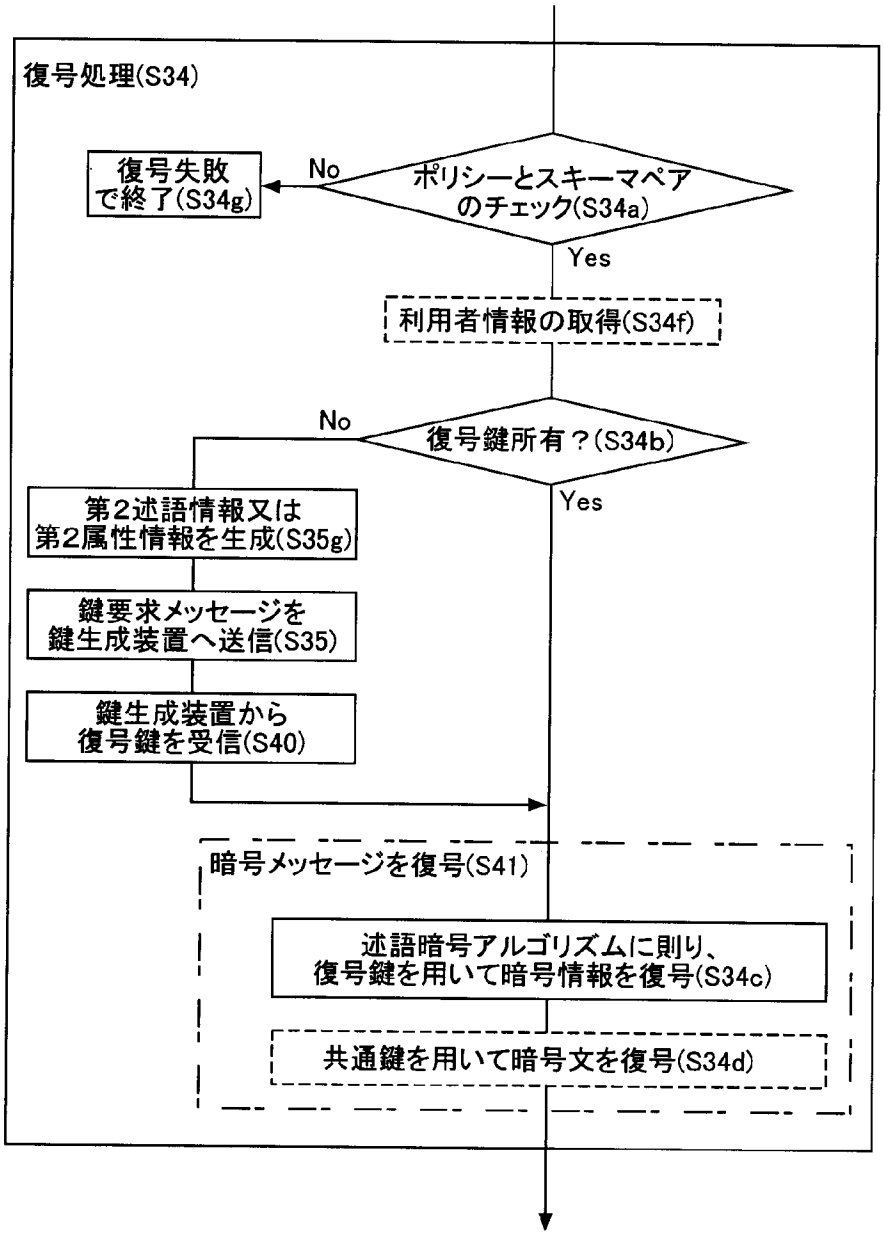

復号処理(S34)
ポリシーとスキーマペアのチェック(S34a)
No
復号失敗で終了(S34g)
Yes
利用者情報の取得(S34f)
復号鍵所有？(S34b)
No
Yes
第2述語情報又は第2属性情報を生成(S35g)
鍵要求メッセージを鍵生成装置へ送信(S35)
鍵生成装置から復号鍵を受信(S40)
暗号メッセージを復号(S41)
述語暗号アルゴリズムに則り、復号鍵を用いて暗号情報を復号(S34c)
共通鍵を用いて暗号文を復号(S34d)

図45

[図46]

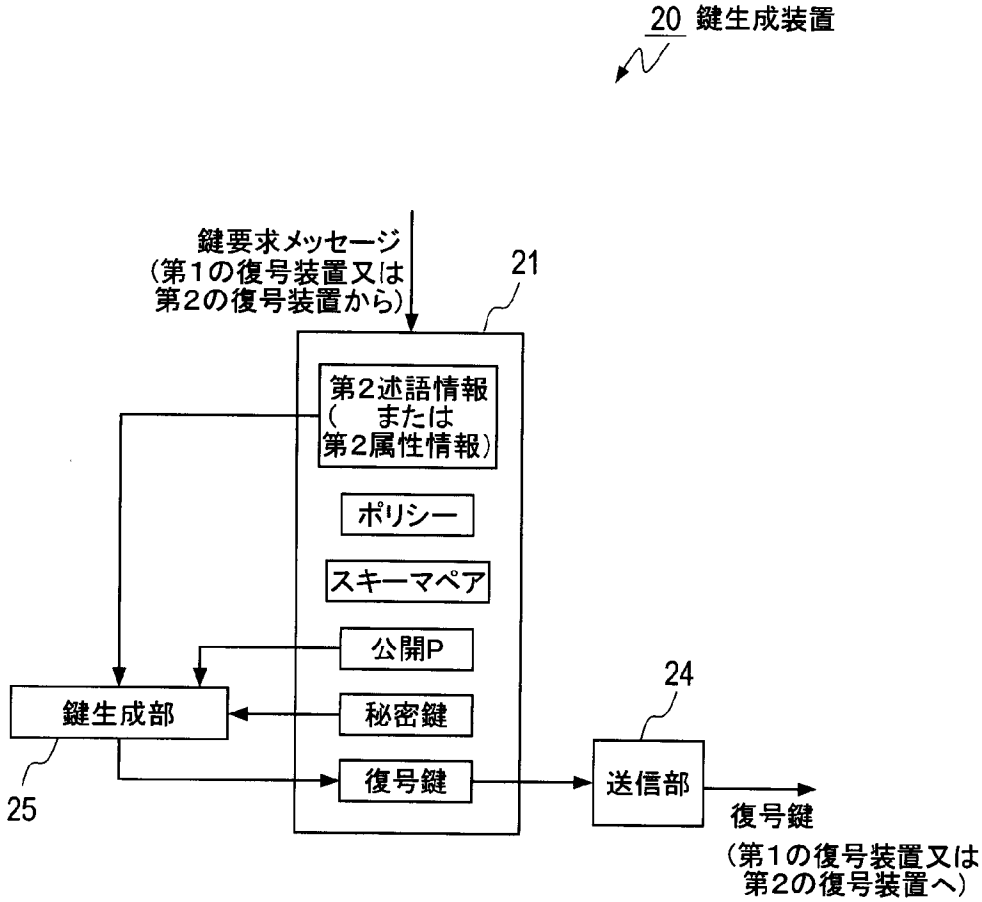

20 鍵生成装置
鍵要求メッセージ
(第1の復号装置又は
第2の復号装置から)
21
第2述語情報
(または
第2属性情報)
ポリシー
スキーマペア
公開P
秘密鍵
復号鍵
鍵生成部
25
24
送信部
復号鍵
(第1の復号装置又は
第2の復号装置へ)

図46

[図47]

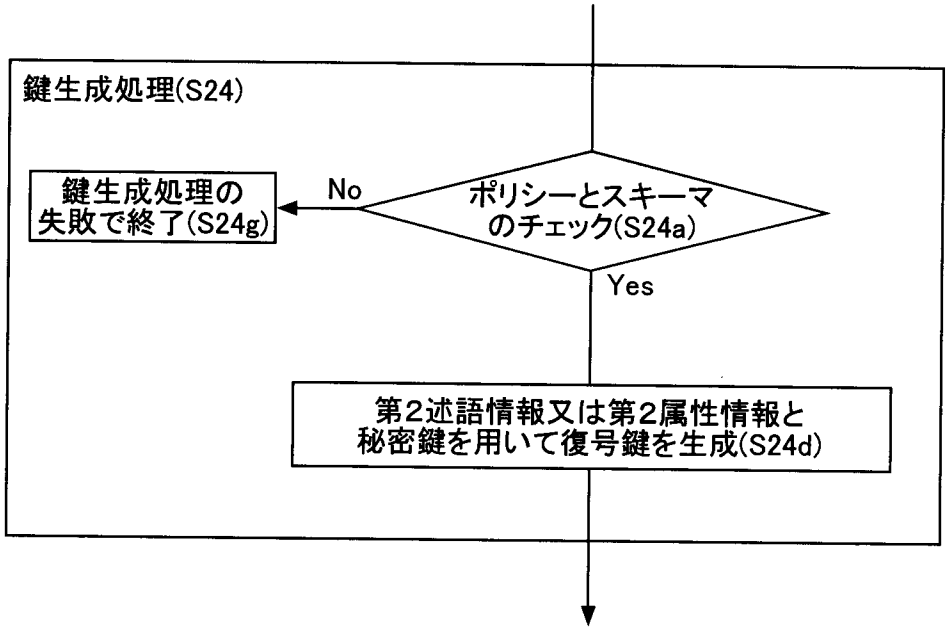

鍵生成処理(S24)
鍵生成処理の
失敗で終了(S24g)
No
ポリシーとスキーマ
のチェック(S24a)
Yes
第2述語情報又は第2属性情報と
秘密鍵を用いて復号鍵を生成(S24d)

図47

[図48]

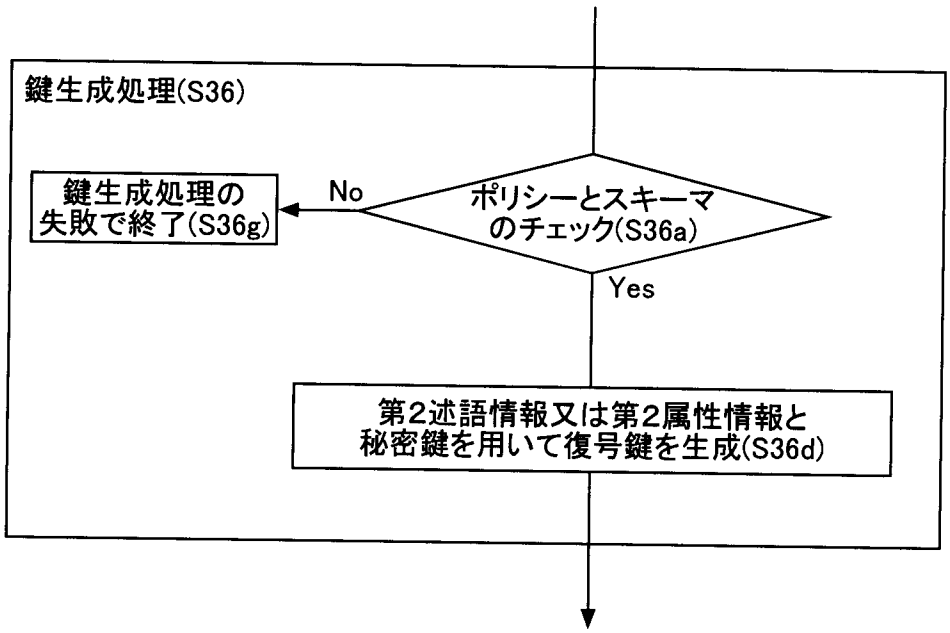

鍵生成処理(S36)
鍵生成処理の
失敗で終了(S36g)
No
ポリシーとスキーマ
のチェック(S36a)
Yes
第2述語情報又は第2属性情報と
秘密鍵を用いて復号鍵を生成(S36d)

図48

[図49]

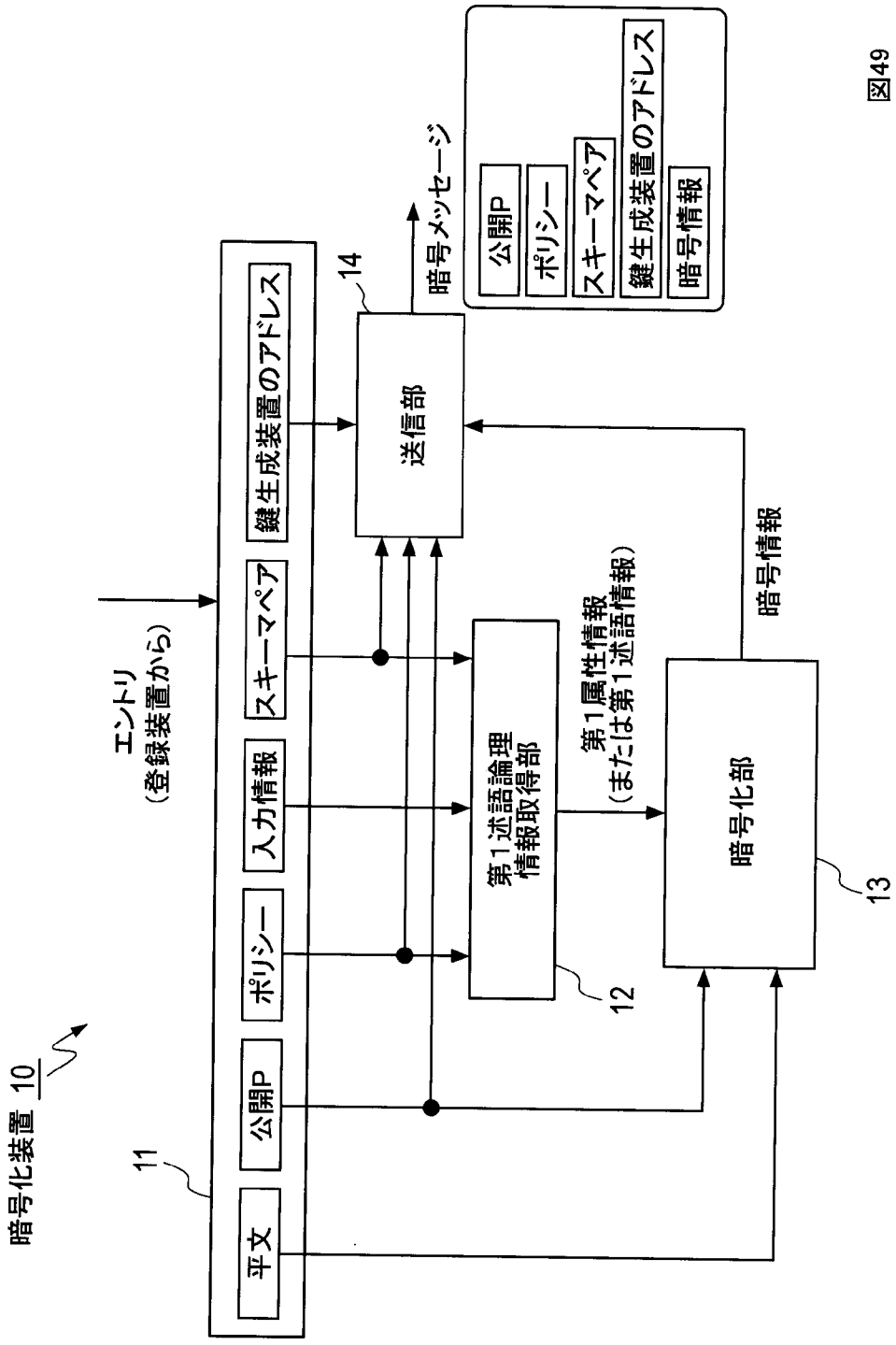

暗号化装置 10
11
平文
公開P
ポリシー
入力情報
スキーマペア
鍵生成装置のアドレス
エントリ
(登録装置から)
第1述語論理
情報取得部
12
第1属性情報
(または第1述語情報)
暗号化部
13
暗号情報
送信部
14
暗号メッセージ
公開P
ポリシー
スキーマペア
鍵生成装置のアドレス
暗号情報

図49

[図50]

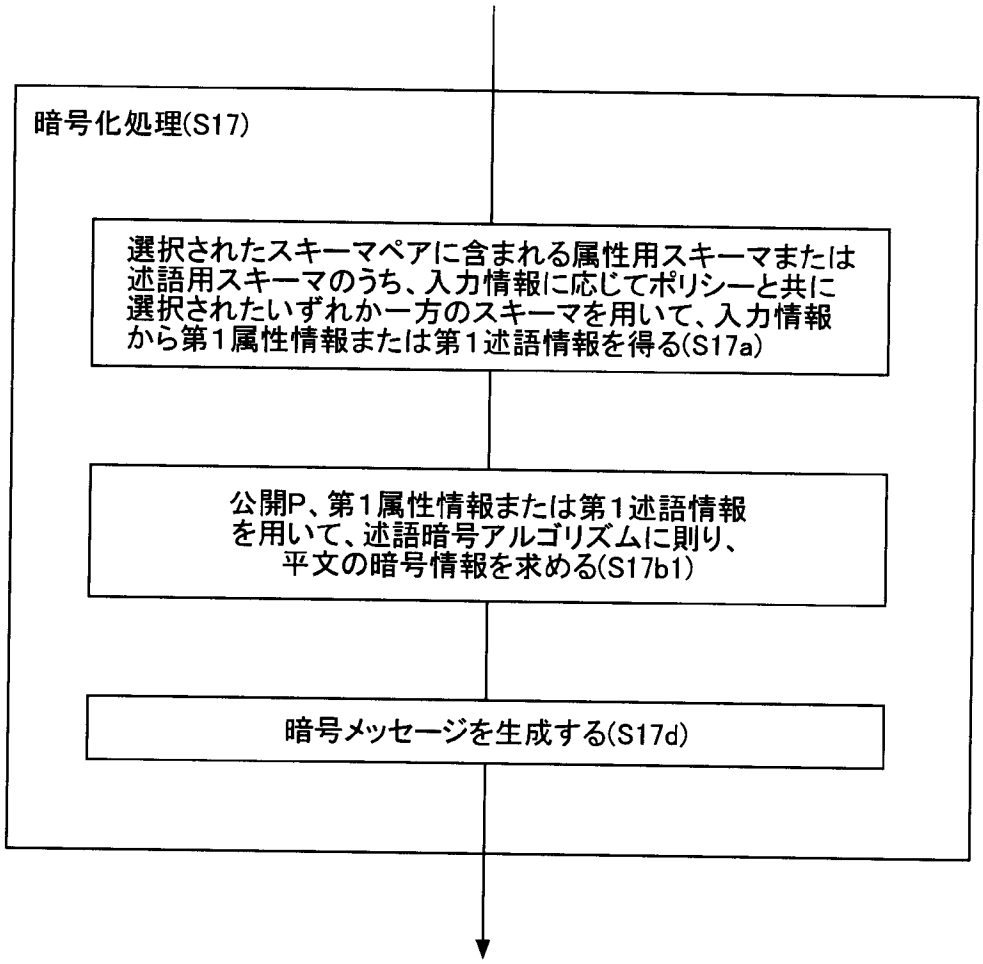

暗号化処理(S17)
選択されたスキーマペアに含まれる属性用スキーマまたは述語用スキーマのうち、入力情報に応じてポリシーと共に選択されたいずれか一方のスキーマを用いて、入力情報から第1属性情報または第1述語情報を得る(S17a)
公開P、第1属性情報または第1述語情報を用いて、述語暗号アルゴリズムに則り、平文の暗号情報を求める(S17b1)
暗号メッセージを生成する(S17d)

図50

[図51]

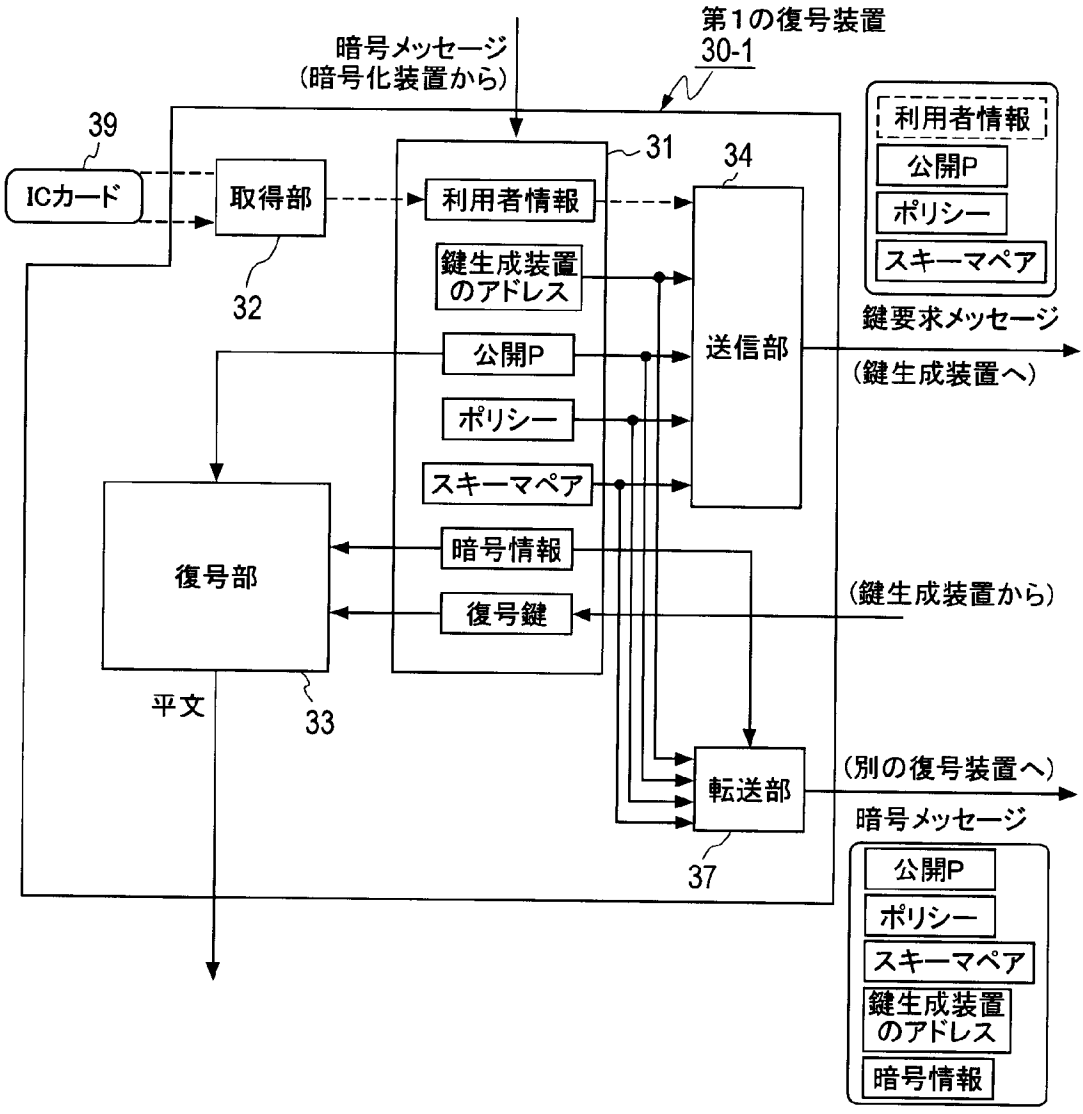

第1の復号装置
30-1
暗号メッセージ
(暗号化装置から)
39
ICカード
取得部
32
31
34
利用者情報
鍵生成装置のアドレス
公開P
ポリシー
スキーマペア
送信部
利用者情報
公開P
ポリシー
スキーマペア
鍵要求メッセージ
(鍵生成装置へ)
復号部
暗号情報
復号鍵
(鍵生成装置から)
平文
33
転送部
37
(別の復号装置へ)
暗号メッセージ
公開P
ポリシー
スキーマペア
鍵生成装置のアドレス
暗号情報

図51

[図52]

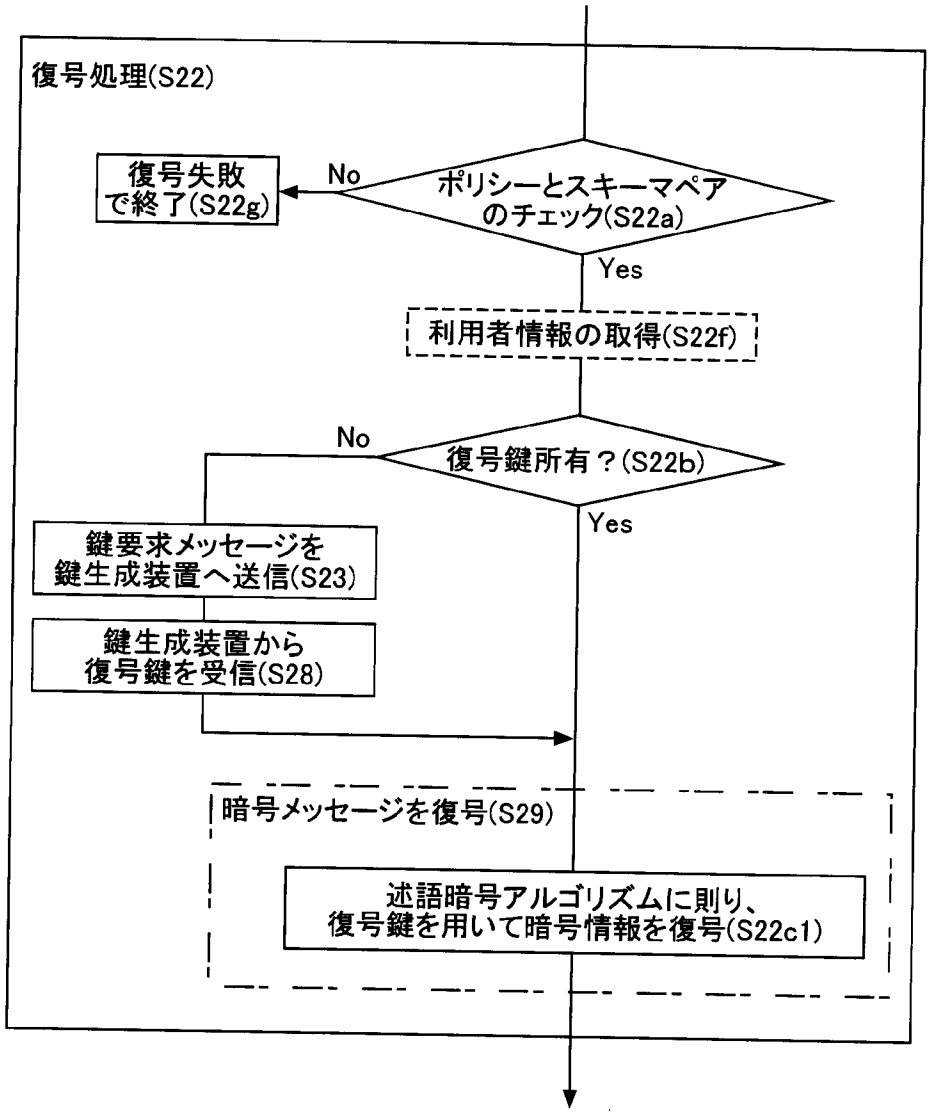

復号処理(S22)
復号失敗
で終了(S22g)
No
ポリシーとスキーマペア
のチェック(S22a)
Yes
利用者情報の取得(S22f)
No
復号鍵所有？(S22b)
Yes
鍵要求メッセージを
鍵生成装置へ送信(S23)
鍵生成装置から
復号鍵を受信(S28)
暗号メッセージを復号(S29)
述語暗号アルゴリズムに則り、
復号鍵を用いて暗号情報を復号(S22c1)

図52

[図53]

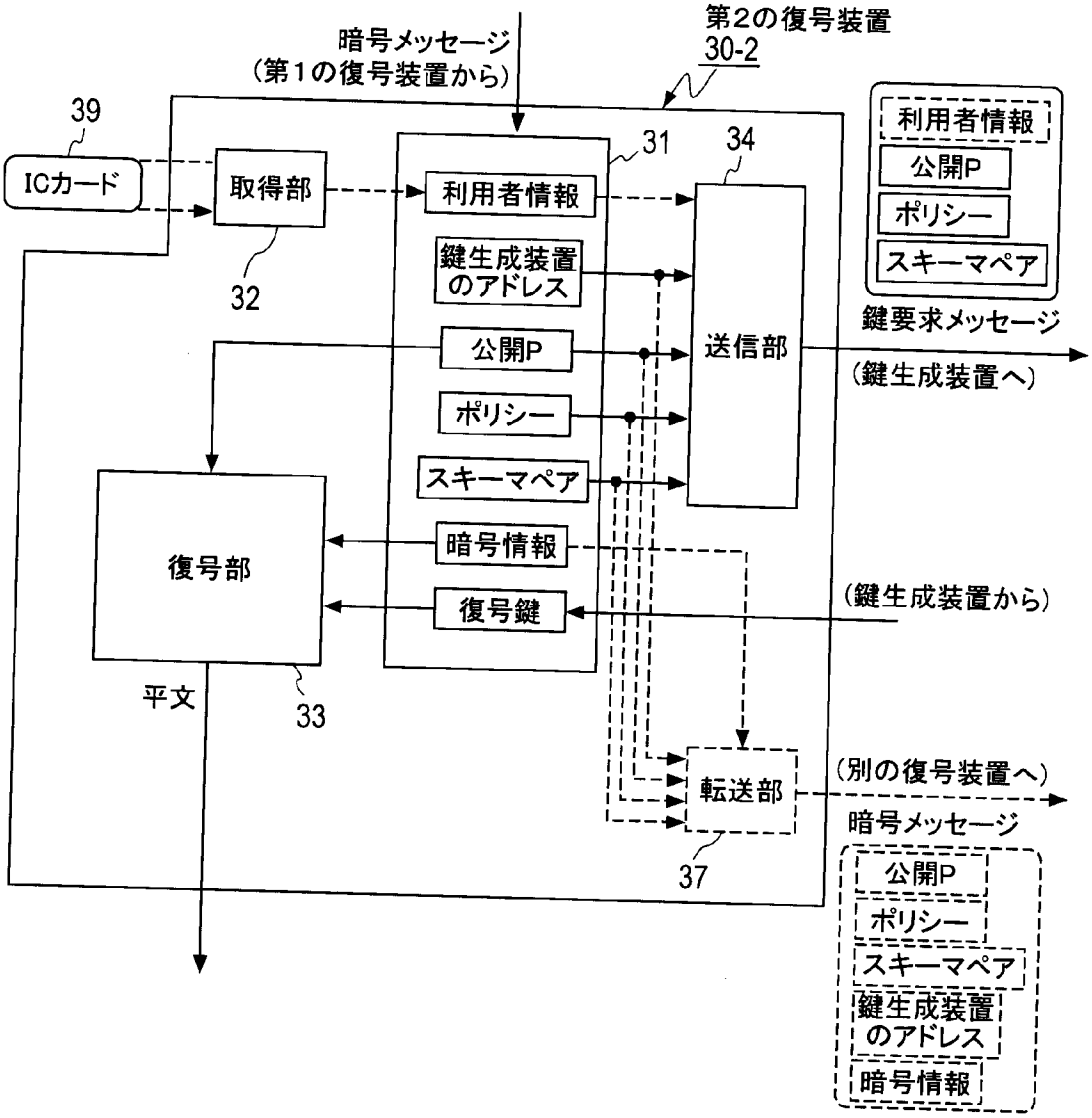

暗号メッセージ
(第1の復号装置から)
第2の復号装置
30-2
39
ICカード
取得部
32
31
34
利用者情報
鍵生成装置のアドレス
公開P
ポリシー
スキーマペア
送信部
利用者情報
公開P
ポリシー
スキーマペア
鍵要求メッセージ
(鍵生成装置へ)
復号部
暗号情報
復号鍵
(鍵生成装置から)
平文
33
転送部
37
(別の復号装置へ)
暗号メッセージ
公開P
ポリシー
スキーマペア
鍵生成装置のアドレス
暗号情報

図53

[図54]

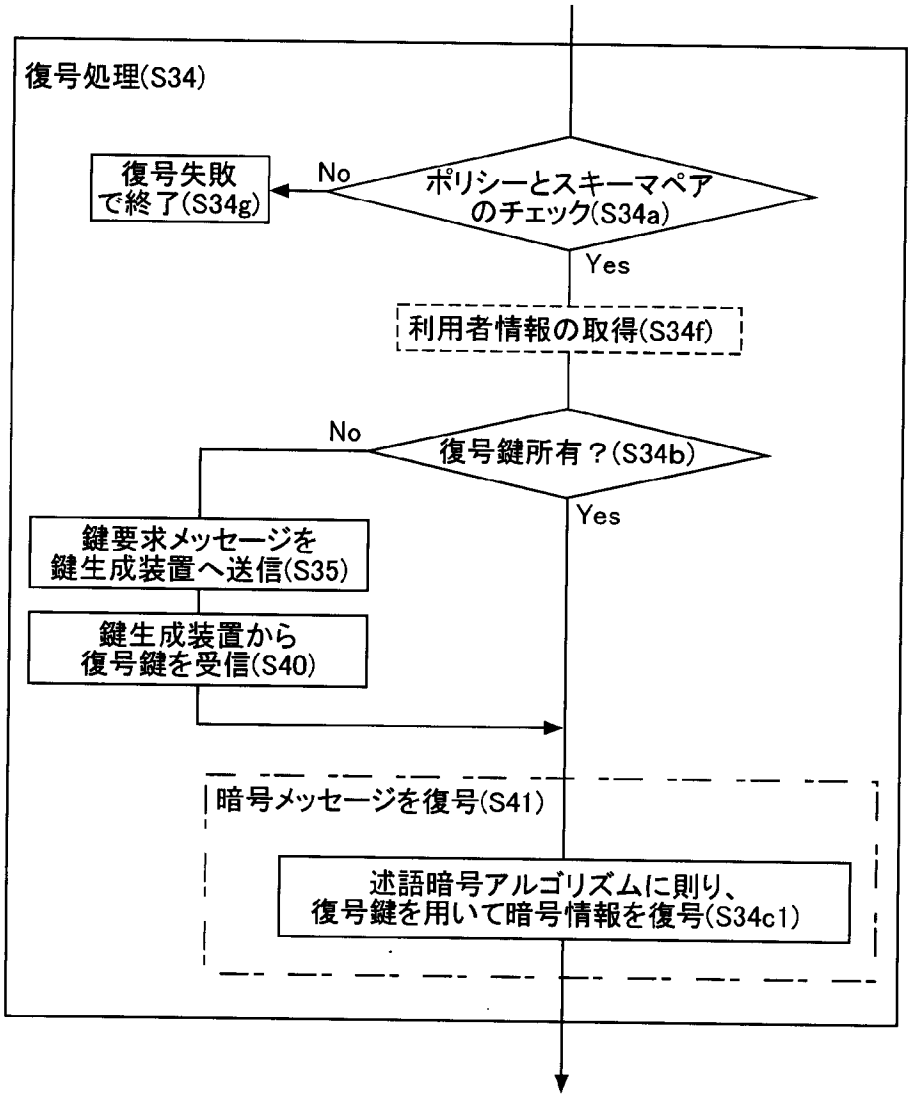

復号処理(S34)
ポリシーとスキーマペアのチェック(S34a)
No
復号失敗で終了(S34g)
Yes
利用者情報の取得(S34f)
復号鍵所有？(S34b)
No
Yes
鍵要求メッセージを鍵生成装置へ送信(S35)
鍵生成装置から復号鍵を受信(S40)
暗号メッセージを復号(S41)
述語暗号アルゴリズムに則り、復号鍵を用いて暗号情報を復号(S34c1)

図54

[図55]

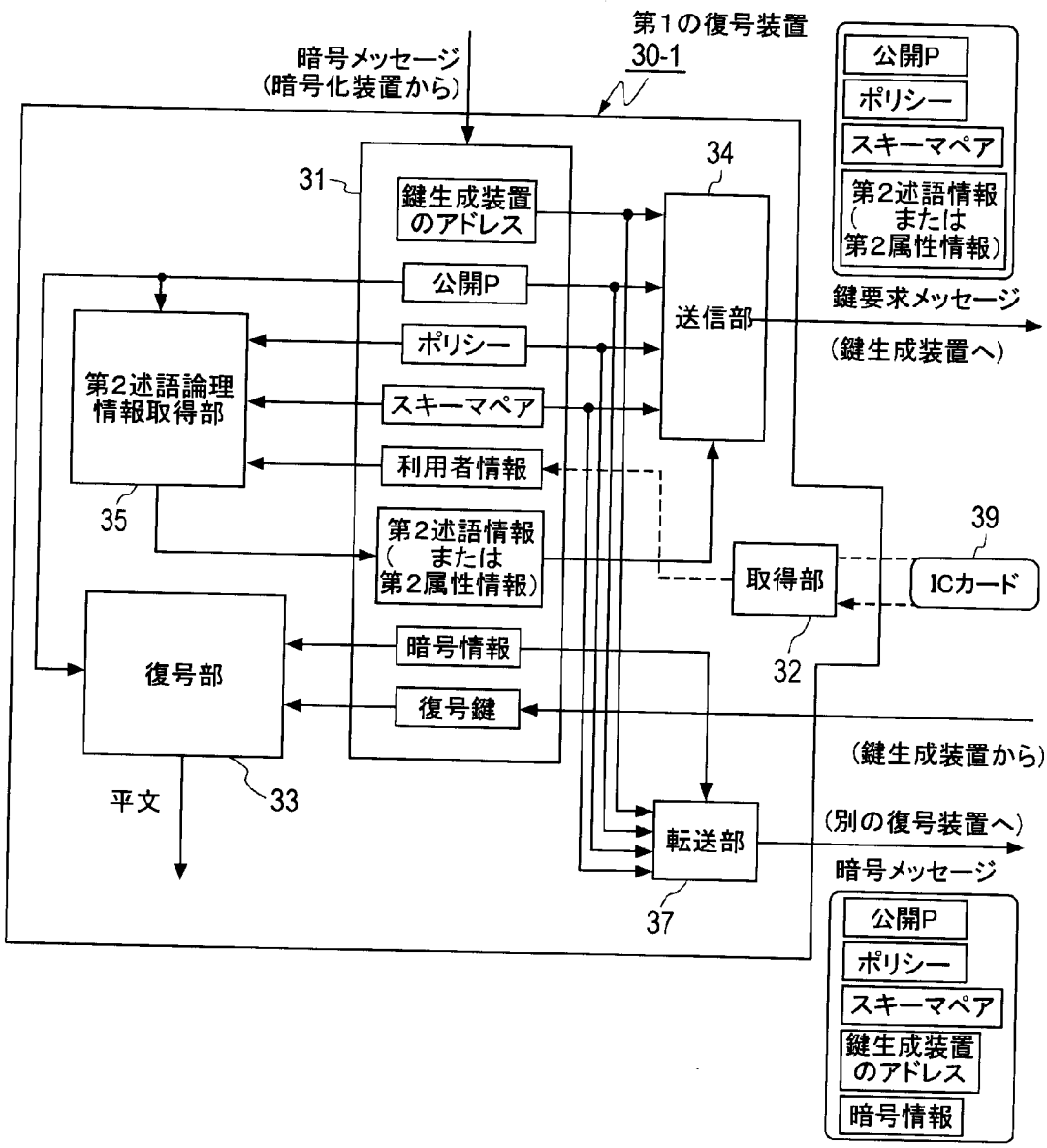

第1の復号装置
30-1
暗号メッセージ
(暗号化装置から)
31
鍵生成装置
のアドレス
公開P
ポリシー
スキーマペア
利用者情報
第2述語情報
(または
第2属性情報)
暗号情報
復号鍵
34
送信部
公開P
ポリシー
スキーマペア
第2述語情報
(または
第2属性情報)
鍵要求メッセージ
(鍵生成装置へ)
第2述語論理
情報取得部
35
取得部
39
ICカード
32
復号部
平文
33
(鍵生成装置から)
転送部
37
(別の復号装置へ)
暗号メッセージ
公開P
ポリシー
スキーマペア
鍵生成装置
のアドレス
暗号情報

図55

[図56]

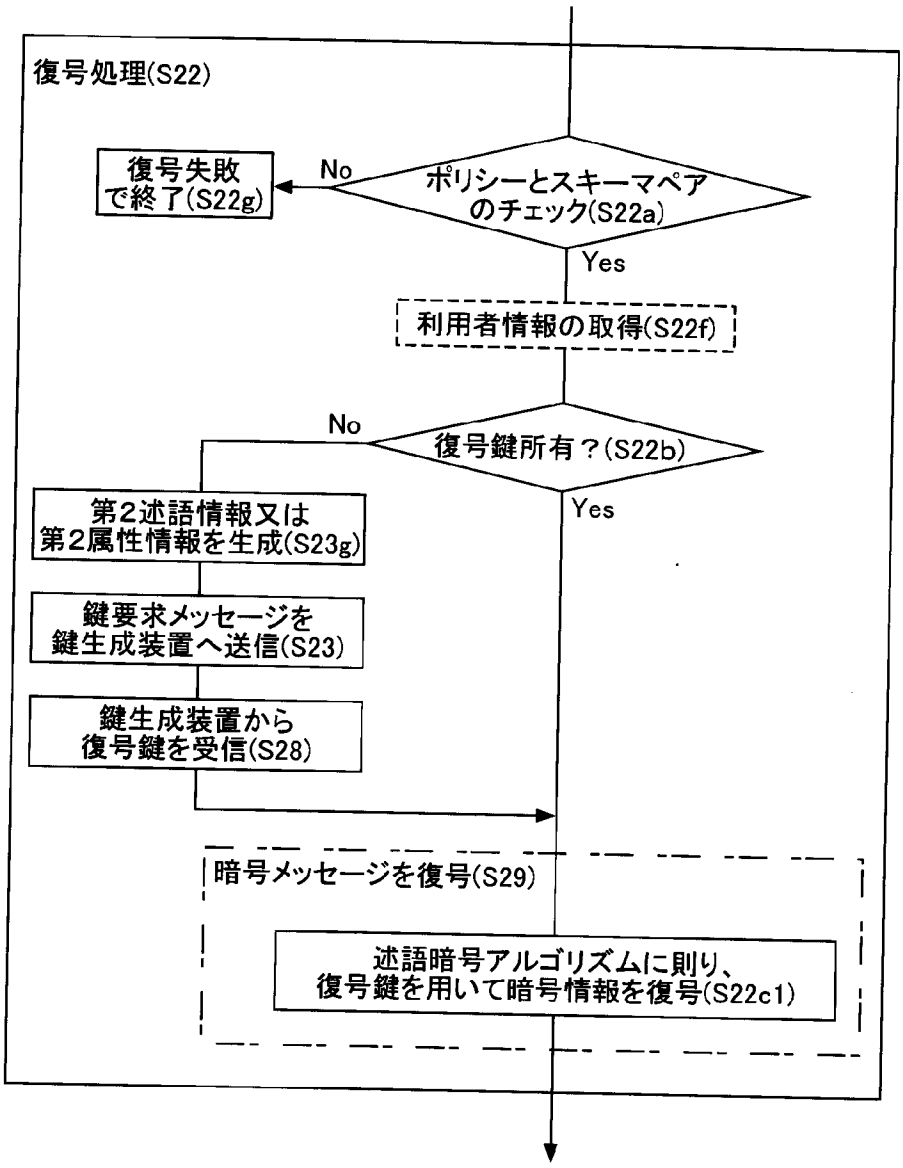

復号処理(S22)
ポリシーとスキーマペアのチェック(S22a)
No
復号失敗で終了(S22g)
Yes
利用者情報の取得(S22f)
復号鍵所有？(S22b)
No
Yes
第2述語情報又は第2属性情報を生成(S23g)
鍵要求メッセージを鍵生成装置へ送信(S23)
鍵生成装置から復号鍵を受信(S28)
暗号メッセージを復号(S29)
述語暗号アルゴリズムに則り、復号鍵を用いて暗号情報を復号(S22c1)

図56

[図57]

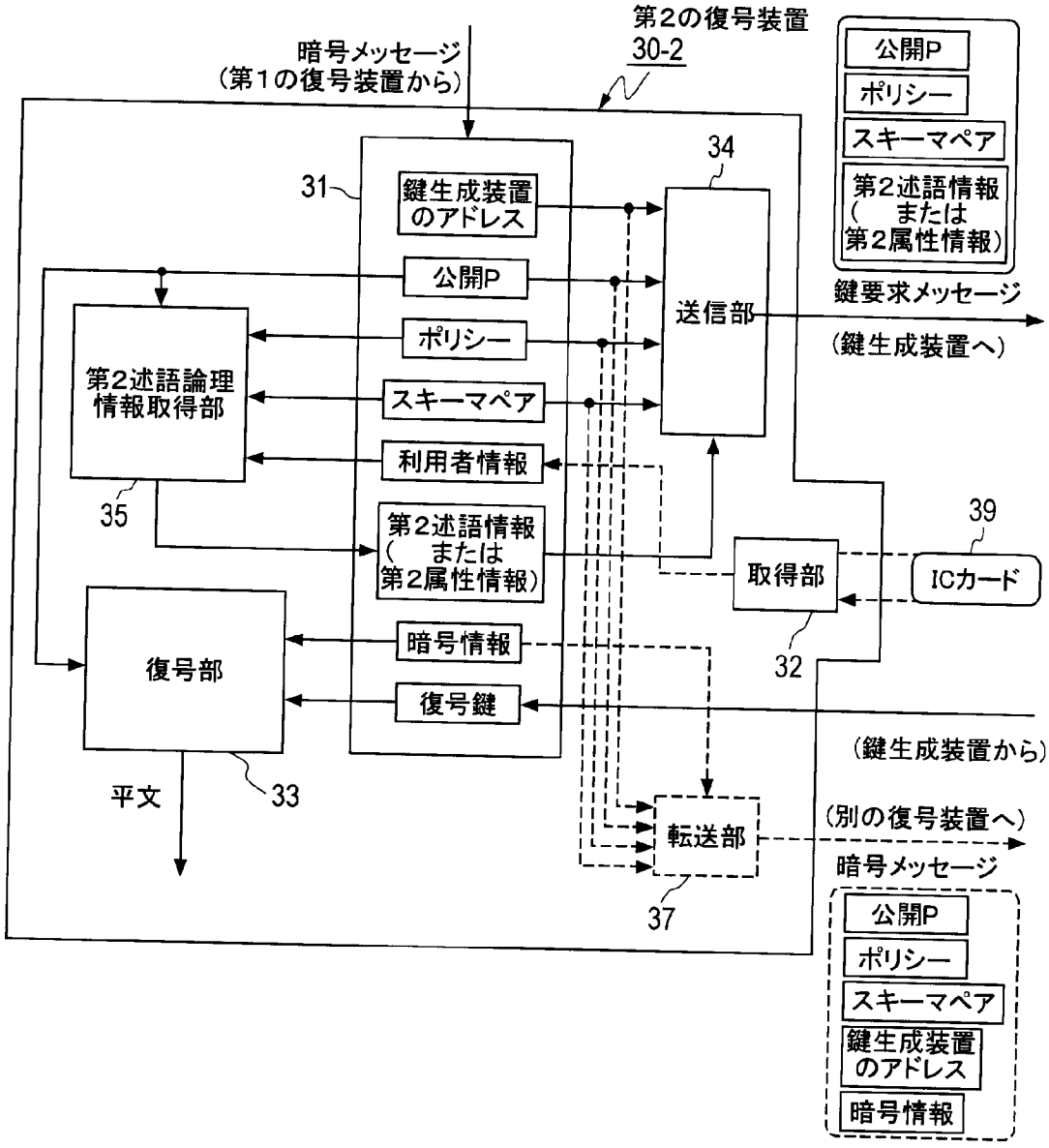

第2の復号装置
30-2
暗号メッセージ
(第1の復号装置から)
公開P
ポリシー
スキーマペア
第2述語情報
(または
第2属性情報)
31
鍵生成装置
のアドレス
34
公開P
ポリシー
スキーマペア
利用者情報
第2述語情報
(または
第2属性情報)
送信部
鍵要求メッセージ
(鍵生成装置へ)
第2述語論理
情報取得部
35
39
取得部
ICカード
32
暗号情報
復号鍵
復号部
(鍵生成装置から)
平文
33
転送部
(別の復号装置へ)
暗号メッセージ
37
公開P
ポリシー
スキーマペア
鍵生成装置
のアドレス
暗号情報

図57

[図58]

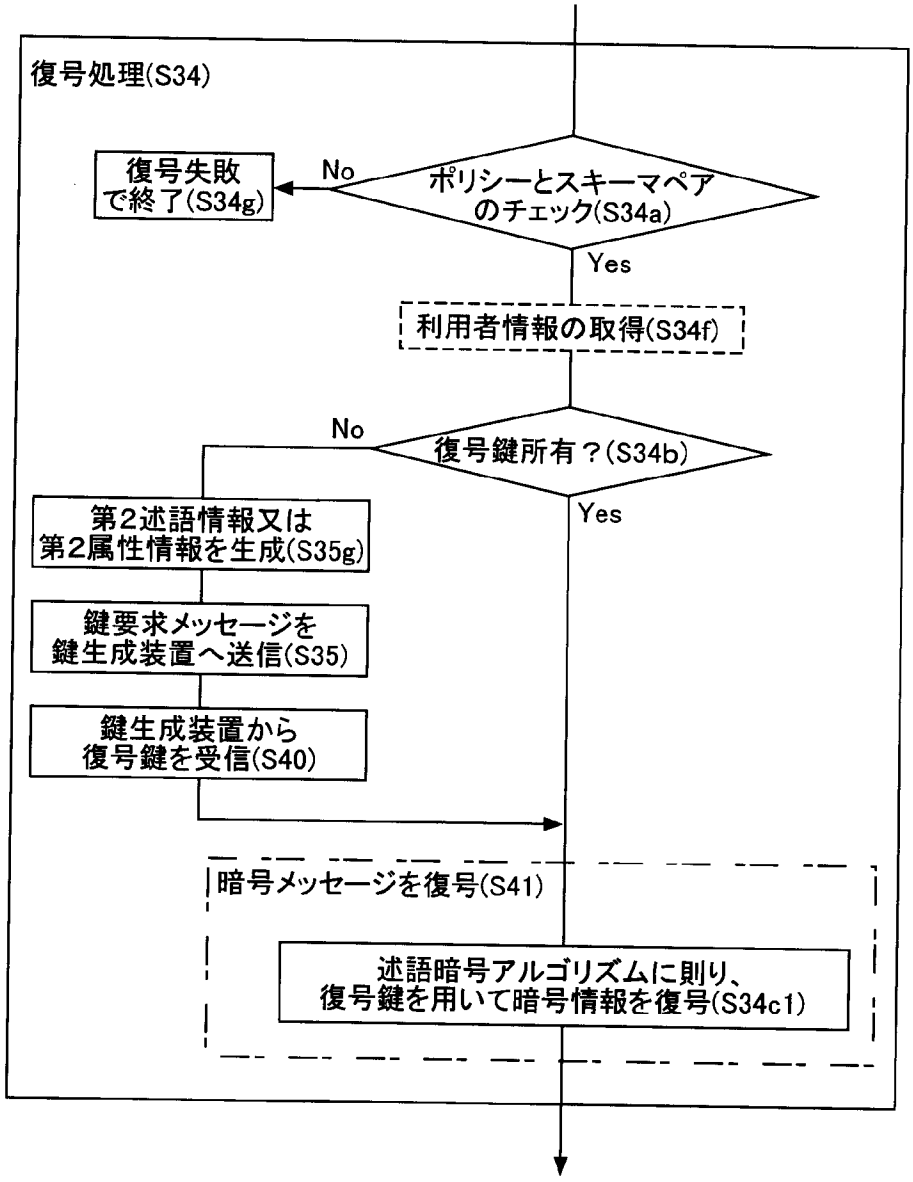

復号処理(S34)
ポリシーとスキーマペアのチェック(S34a)
No
復号失敗で終了(S34g)
Yes
利用者情報の取得(S34f)
復号鍵所有？(S34b)
No
Yes
第2述語情報又は第2属性情報を生成(S35g)
鍵要求メッセージを鍵生成装置へ送信(S35)
鍵生成装置から復号鍵を受信(S40)
暗号メッセージを復号(S41)
述語暗号アルゴリズムに則り、復号鍵を用いて暗号情報を復号(S34c1)

図58

[図59]

S／MIMEメールヘッダ From: ALICE TO:BOB SUBJECT:～ SENT:～
暗号メッセージ開始位置マーカ
アルゴリズム識別子ブロック ・共通鍵に対する述語暗号アルゴリズム ・メッセージペイロードに対する共通鍵暗号アルゴリズム
デジタル署名ブロック
公開パラメータ情報ブロック
ポリシーフィールド
スキーマフィールド
暗号情報フィールド
暗号文フィールド
属性フィールド
述語フィールド
暗号メッセージ終了位置マーカ
添付フィールド（例：RSA暗号化添付）

図59

[図60]

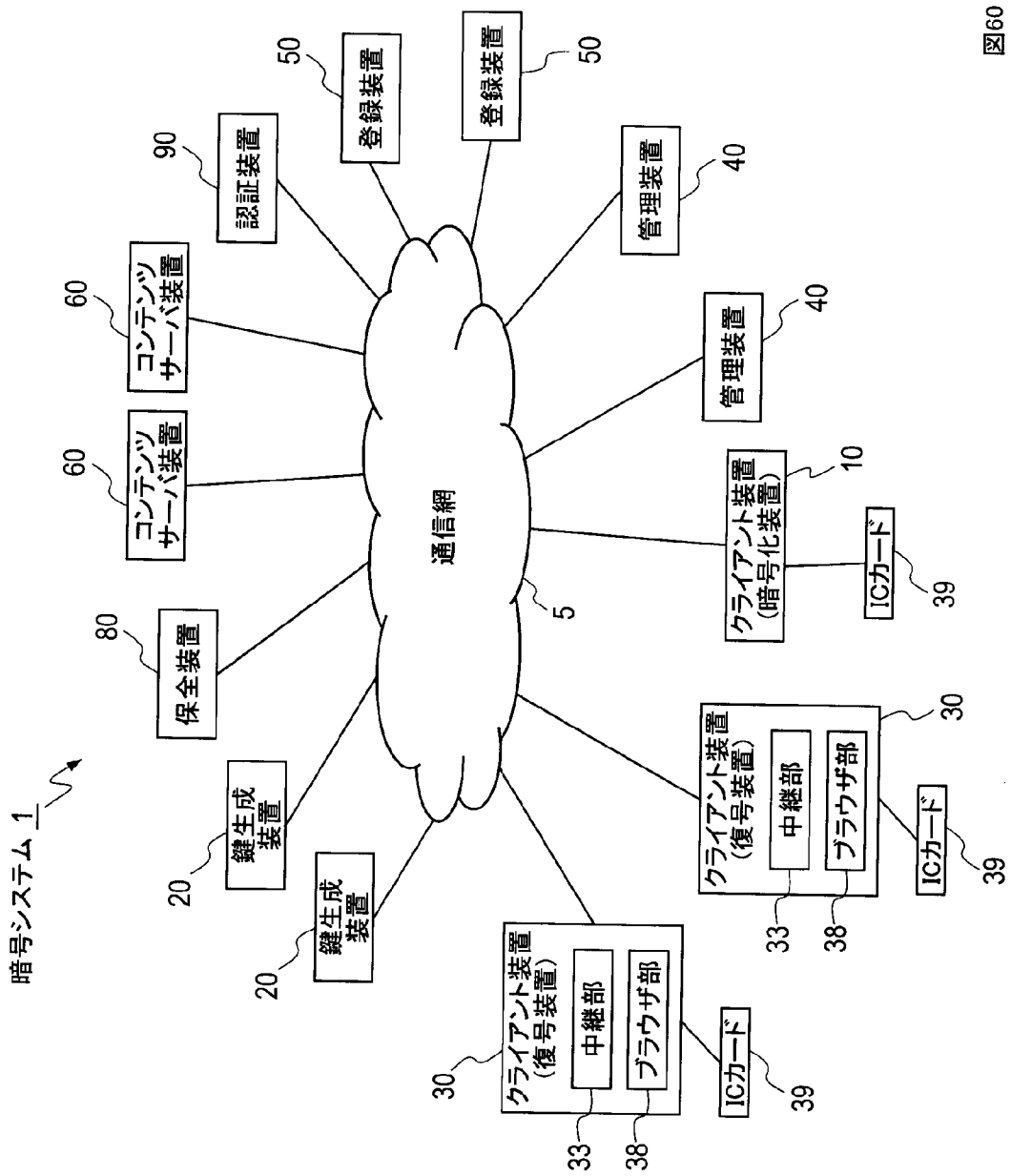

暗号システム 1
通信網
5
鍵生成装置
20
保全装置
80
コンテンツサーバ装置
60
コンテンツサーバ装置
60
認証装置
90
登録装置
50
登録装置
50
管理装置
40
管理装置
40
クライアント装置(暗号化装置)
10
ICカード
39
クライアント装置(復号装置)
30
中継部
33
ブラウザ部
38
ICカード
39
鍵生成装置
20
クライアント装置(復号装置)
30
中継部
33
ブラウザ部
38
ICカード
39

図60

[図61]

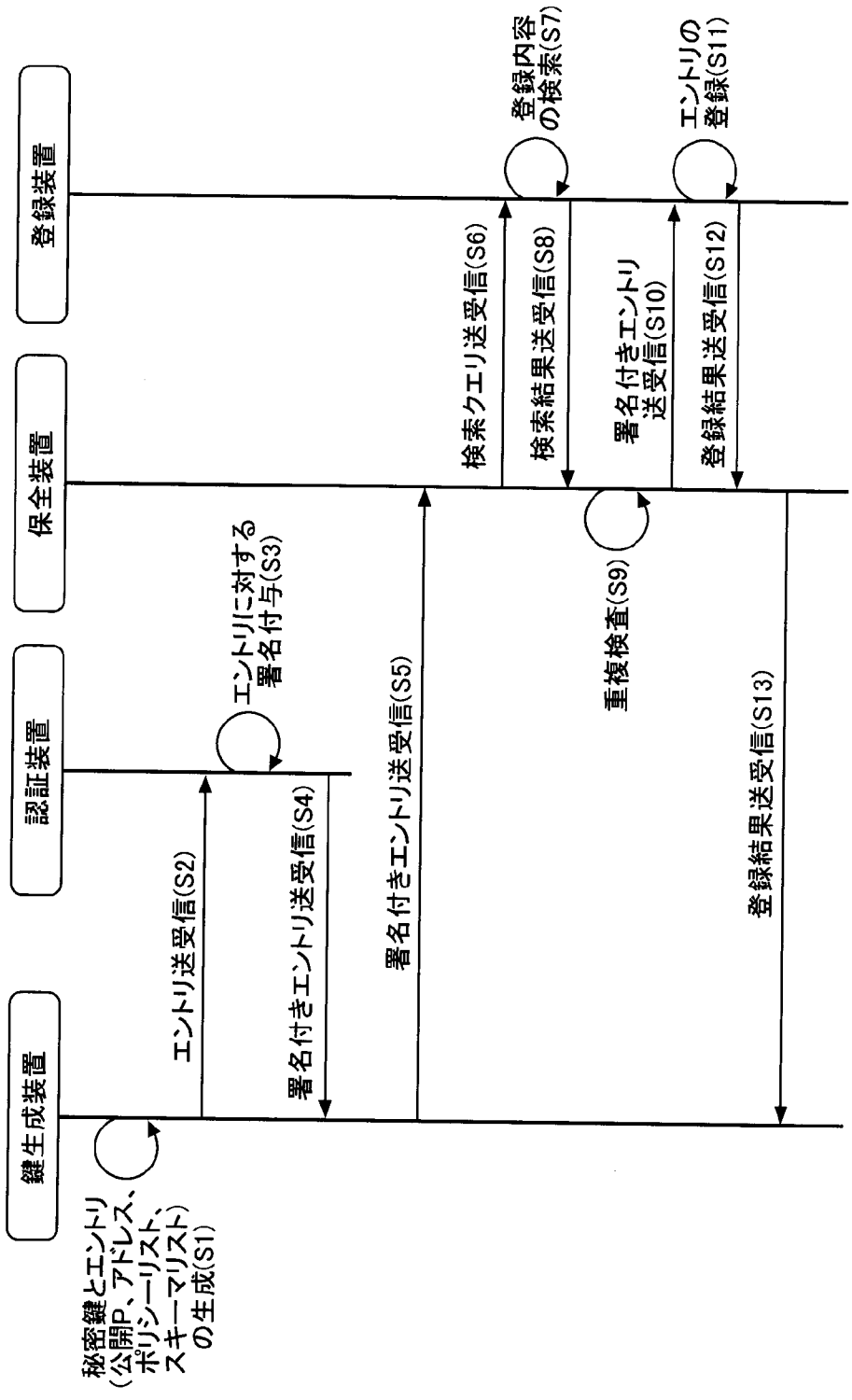

鍵生成装置
認証装置
保全装置
登録装置
秘密鍵とエントリ(公開P、アドレス、ポリシーリスト、スキーマリスト)の生成(S1)
エントリ送受信(S2)
エントリに対する署名付与(S3)
署名付きエントリ送受信(S4)
署名付きエントリ送受信(S5)
検索クエリ送受信(S6)
登録内容の検索(S7)
検索結果送受信(S8)
重複検査(S9)
署名付きエントリ送受信(S10)
エントリの登録(S11)
登録結果送受信(S12)
登録結果送受信(S13)

図61

[図62]

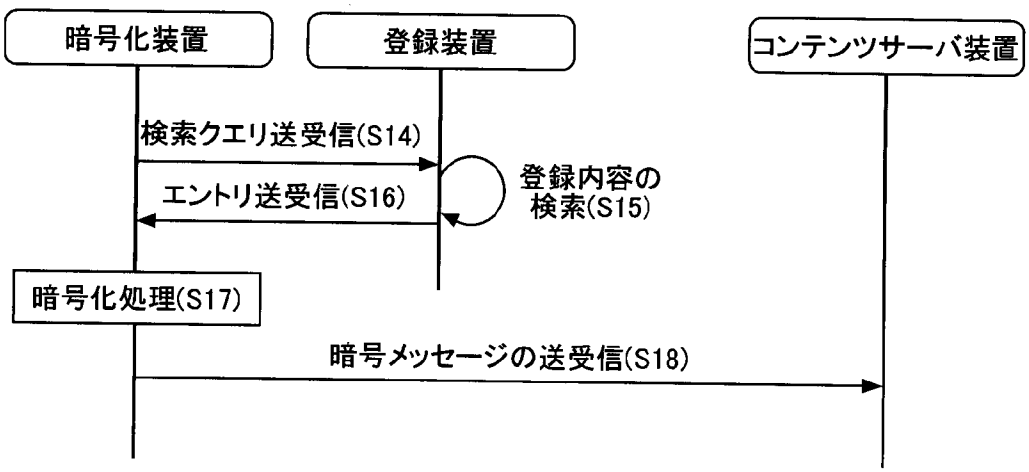


図62

[図63]

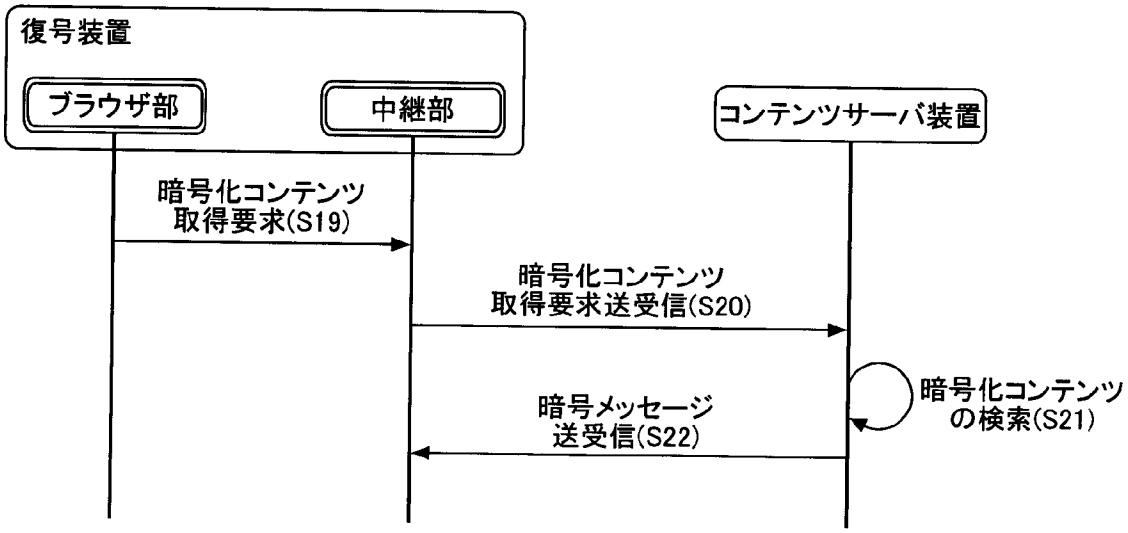


図63

[図64]

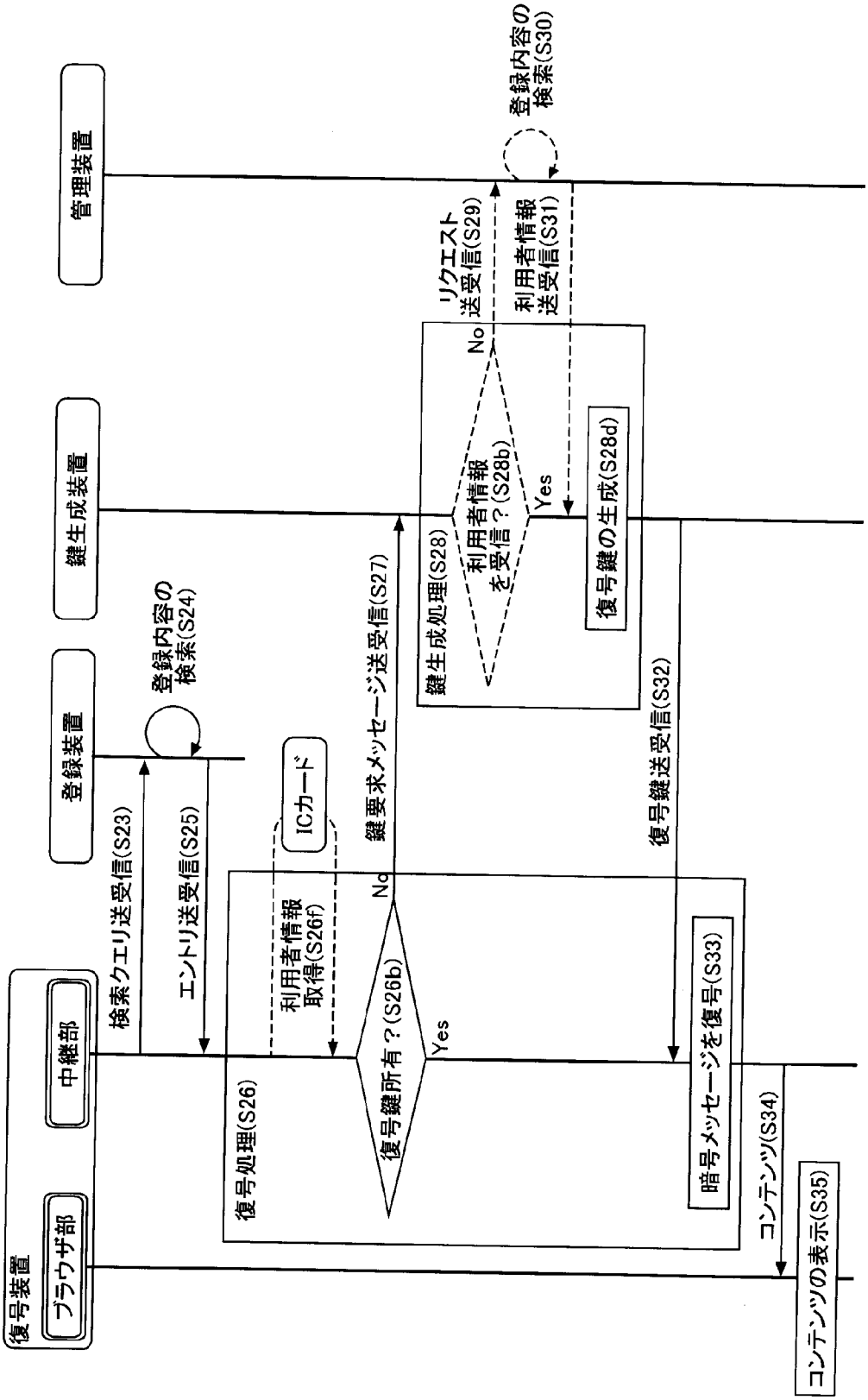

復号装置
ブラウザ部
中継部
登録装置
鍵生成装置
管理装置
検索クエリ送受信(S23)
エントリ送受信(S25)
登録内容の検索(S24)
ICカード
利用者情報取得(S26f)
復号処理(S26)
鍵要求メッセージ送受信(S27)
復号鍵所有？(S26b)
No
Yes
鍵生成処理(S28)
利用者情報を受信？(S28b)
No
Yes
リクエスト送受信(S29)
登録内容の検索(S30)
利用者情報送受信(S31)
復号鍵の生成(S28d)
復号鍵送受信(S32)
暗号メッセージを復号(S33)
コンテンツ(S34)
コンテンツの表示(S35)

図64

[図65]

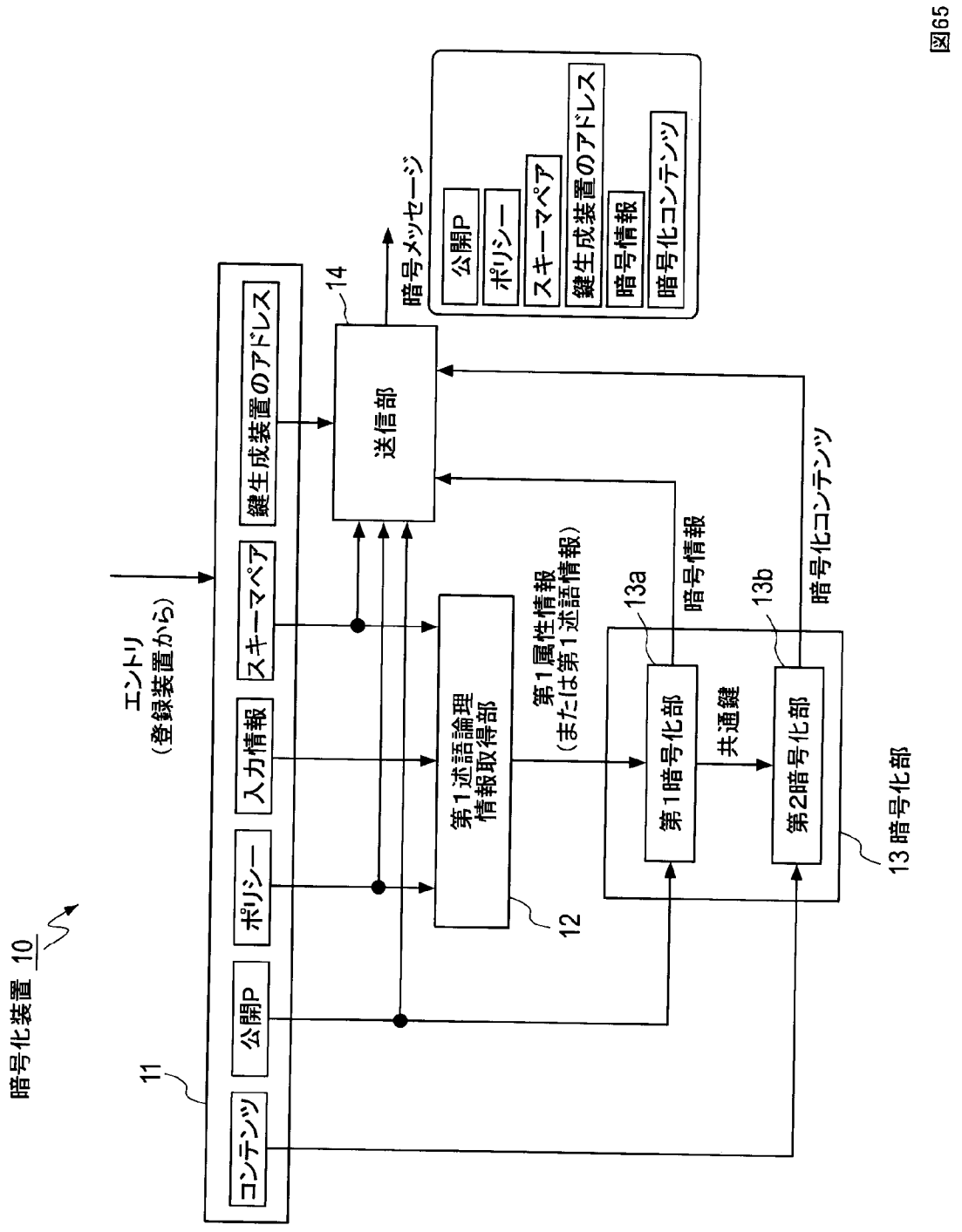

暗号化装置 10
11
エントリ
(登録装置から)
コンテンツ
公開P
ポリシー
入力情報
スキーマペア
鍵生成装置のアドレス
第1述語論理
情報取得部
12
第1属性情報
(または第1述語情報)
送信部
14
暗号メッセージ
公開P
ポリシー
スキーマペア
鍵生成装置のアドレス
暗号情報
暗号化コンテンツ
13a
第1暗号化部
暗号情報
共通鍵
13b
第2暗号化部
暗号化コンテンツ
13 暗号化部

図65

[図66]

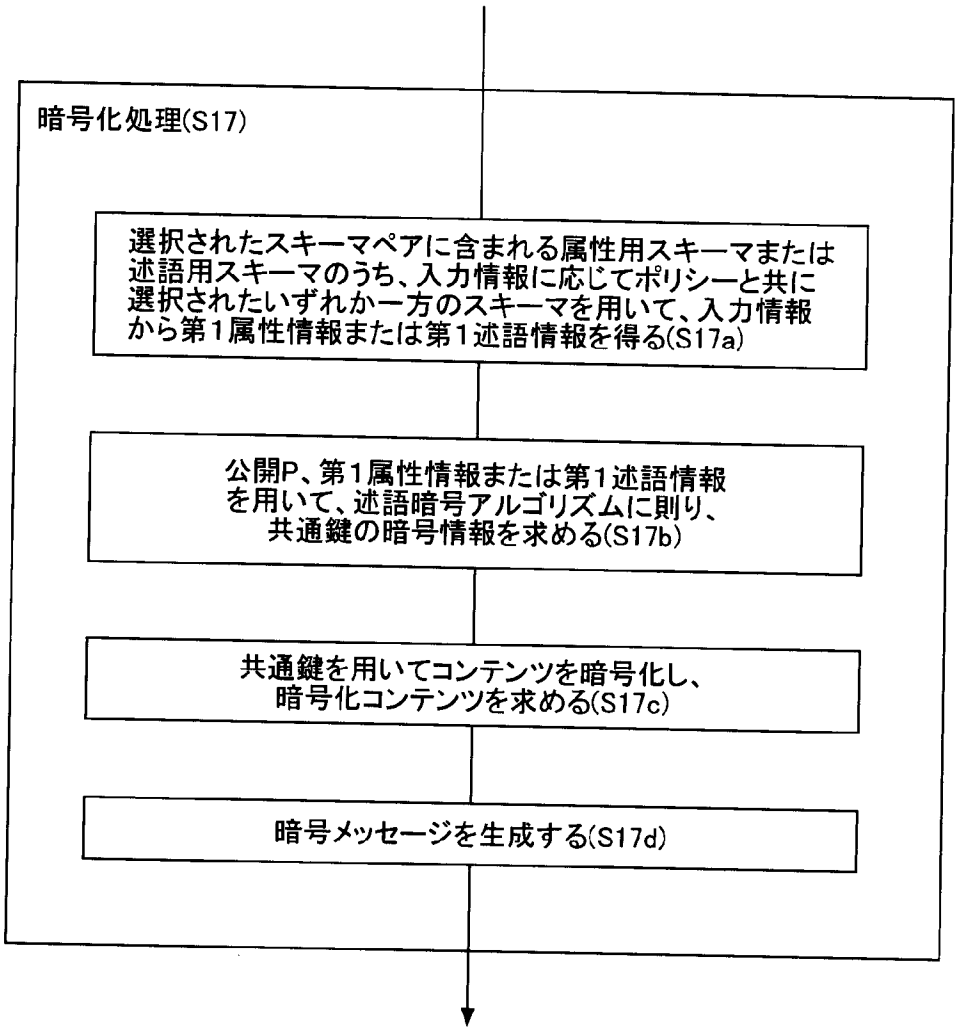

暗号化処理(S17)
選択されたスキーマペアに含まれる属性用スキーマまたは述語用スキーマのうち、入力情報に応じてポリシーと共に選択されたいずれか一方のスキーマを用いて、入力情報から第1属性情報または第1述語情報を得る(S17a)
公開P、第1属性情報または第1述語情報を用いて、述語暗号アルゴリズムに則り、共通鍵の暗号情報を求める(S17b)
共通鍵を用いてコンテンツを暗号化し、暗号化コンテンツを求める(S17c)
暗号メッセージを生成する(S17d)

図66

[図67]

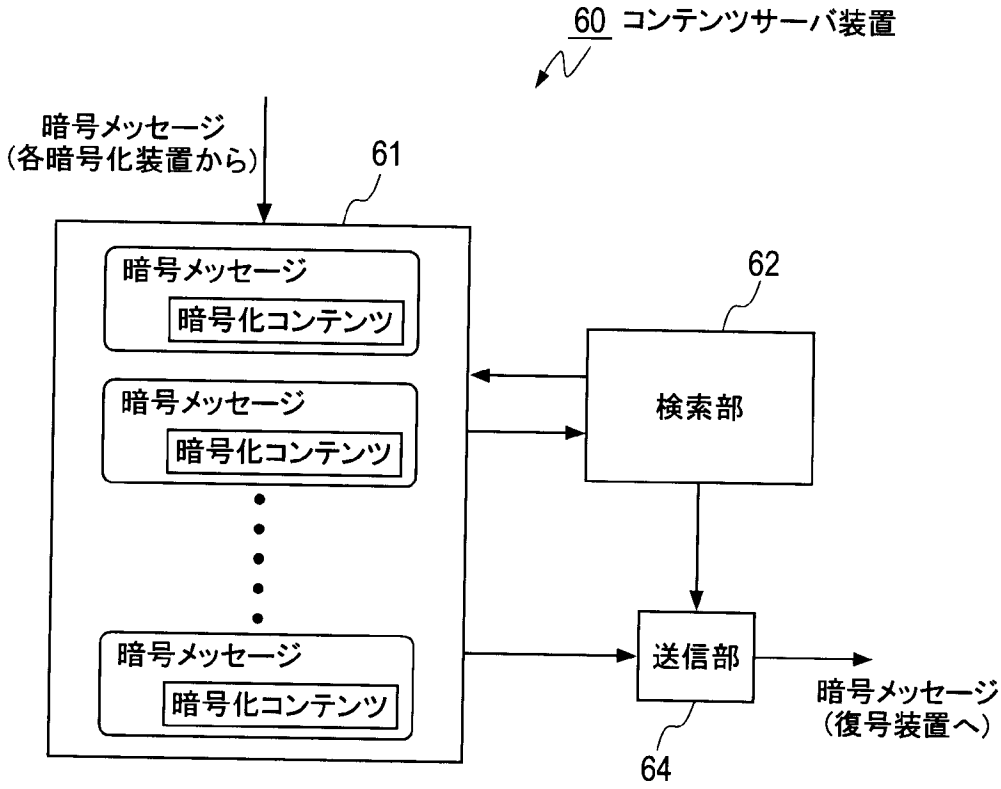

60 コンテンツサーバ装置
暗号メッセージ
(各暗号化装置から)
61
暗号メッセージ
暗号化コンテンツ
暗号メッセージ
暗号化コンテンツ
暗号メッセージ
暗号化コンテンツ
62
検索部
送信部
暗号メッセージ
(復号装置へ)
64

図67

[図68]

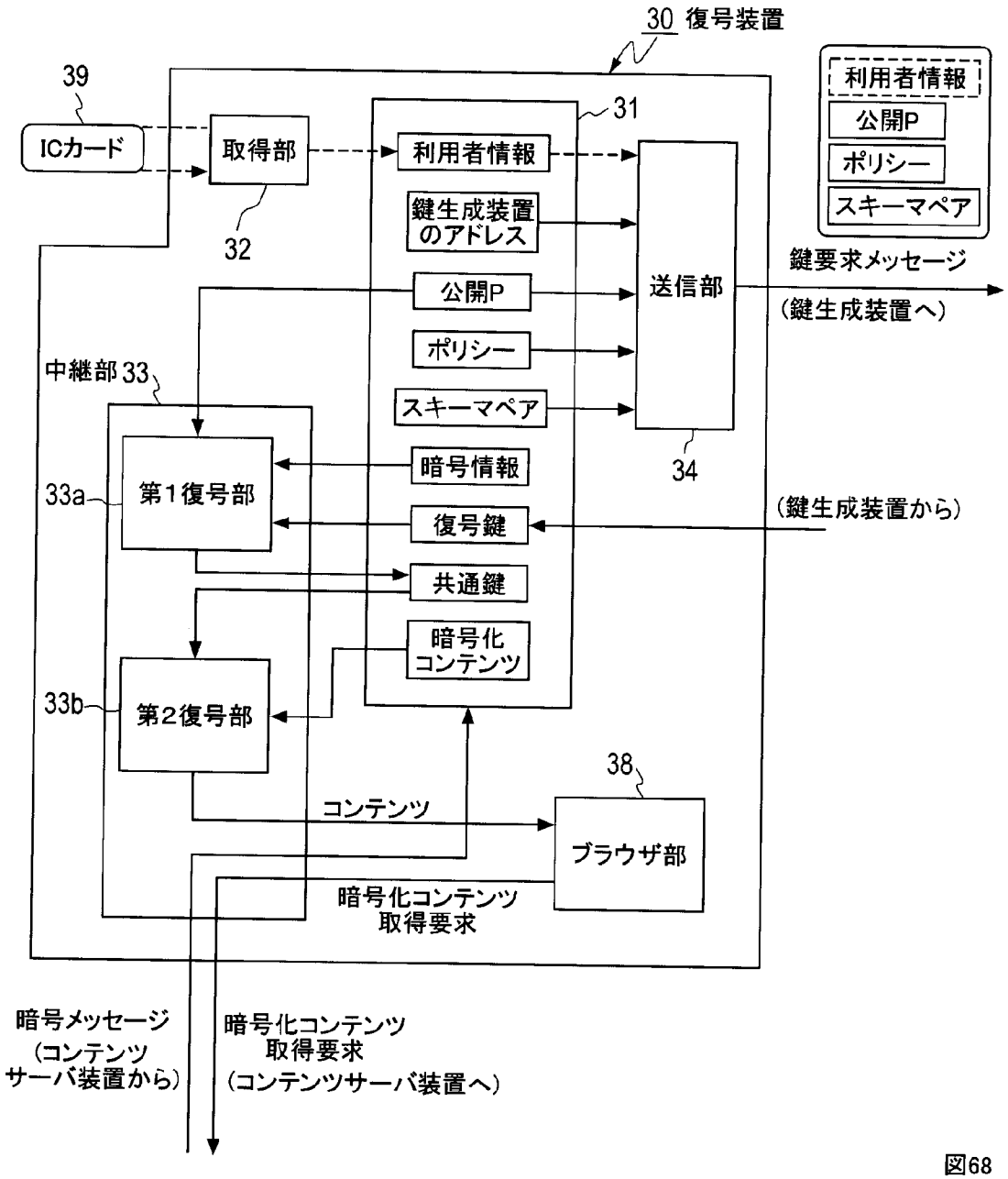

30 復号装置
39
ICカード
取得部
32
31
利用者情報
鍵生成装置のアドレス
公開P
ポリシー
スキーマペア
送信部
34
利用者情報
公開P
ポリシー
スキーマペア
鍵要求メッセージ
(鍵生成装置へ)
中継部 33
33a
第1復号部
33b
第2復号部
暗号情報
復号鍵
共通鍵
暗号化コンテンツ
(鍵生成装置から)
38
コンテンツ
ブラウザ部
暗号化コンテンツ取得要求
暗号メッセージ
(コンテンツサーバ装置から)
暗号化コンテンツ取得要求
(コンテンツサーバ装置へ)

図68

[図69]

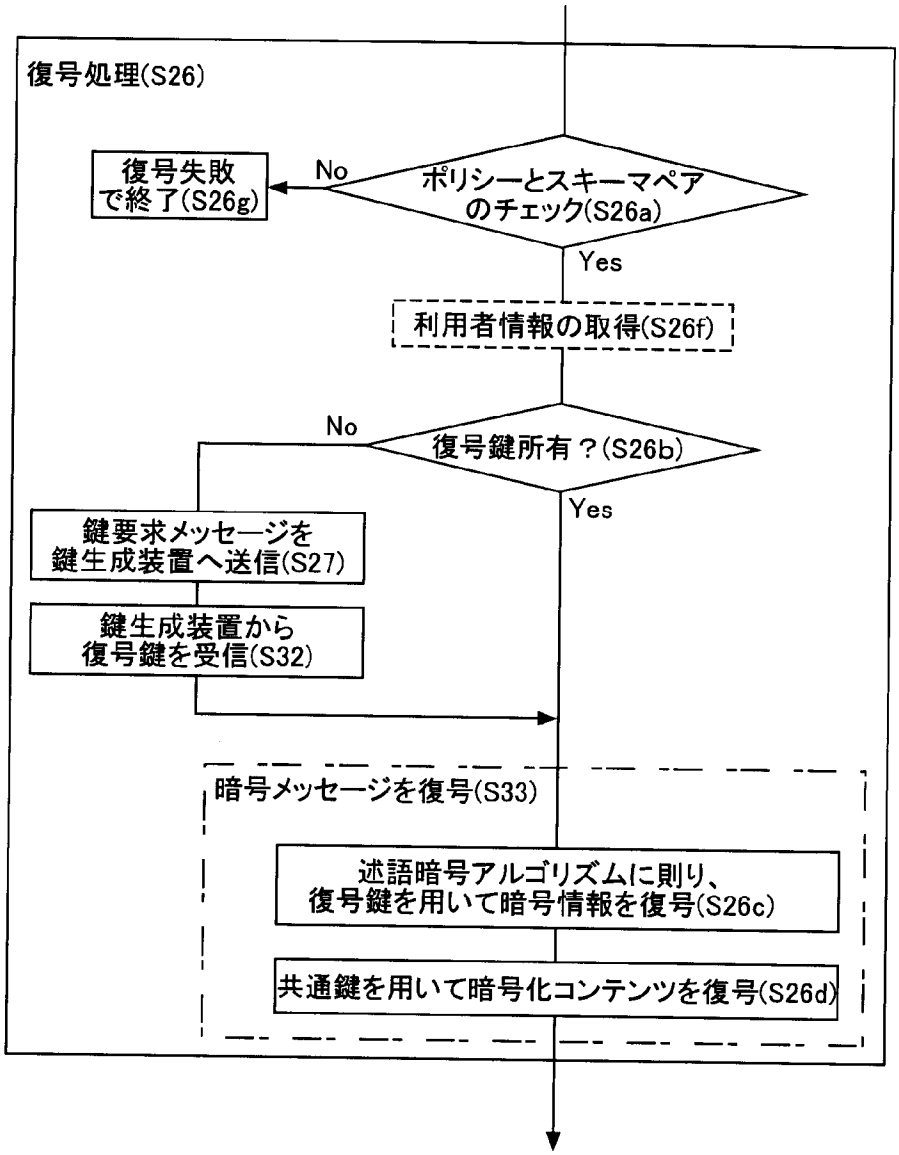

復号処理(S26)
ポリシーとスキーマペアのチェック(S26a)
No
復号失敗で終了(S26g)
Yes
利用者情報の取得(S26f)
復号鍵所有？(S26b)
No
Yes
鍵要求メッセージを鍵生成装置へ送信(S27)
鍵生成装置から復号鍵を受信(S32)
暗号メッセージを復号(S33)
述語暗号アルゴリズムに則り、復号鍵を用いて暗号情報を復号(S26c)
共通鍵を用いて暗号化コンテンツを復号(S26d)

図69

[図70]

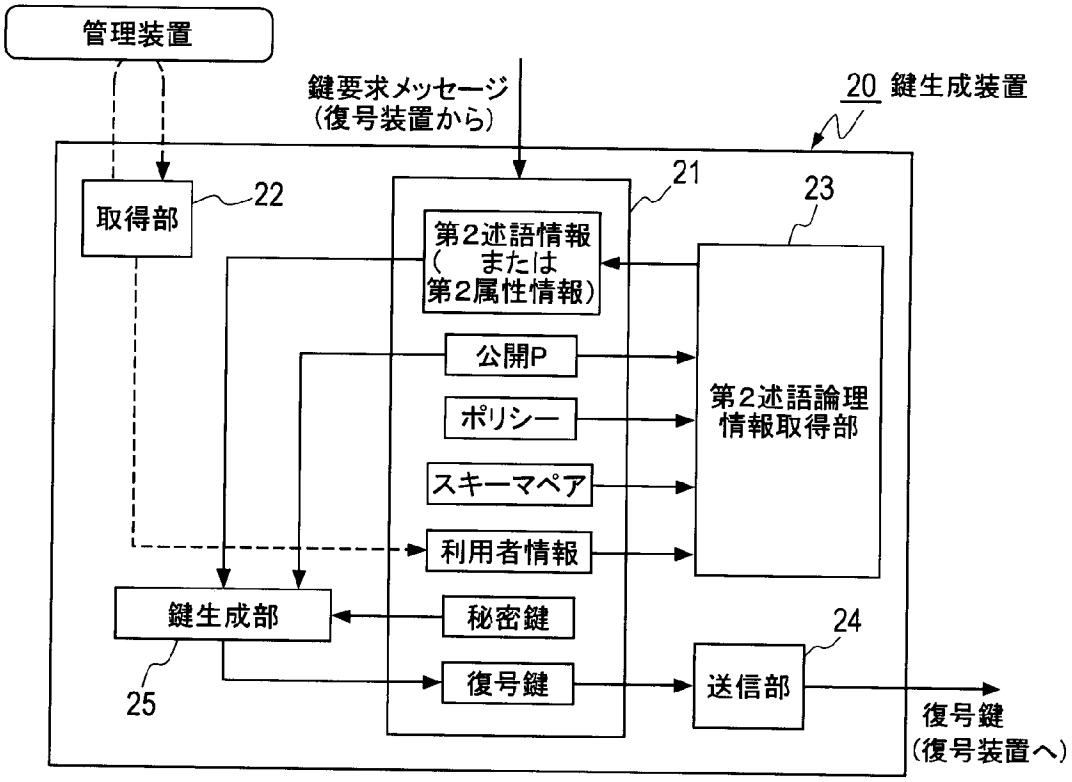

管理装置
鍵要求メッセージ
(復号装置から)
20 鍵生成装置
取得部
22
21
23
第2述語情報
(または
第2属性情報)
公開P
ポリシー
スキーマペア
利用者情報
第2述語論理
情報取得部
鍵生成部
秘密鍵
24
25
復号鍵
送信部
復号鍵
(復号装置へ)

図70

[図71]

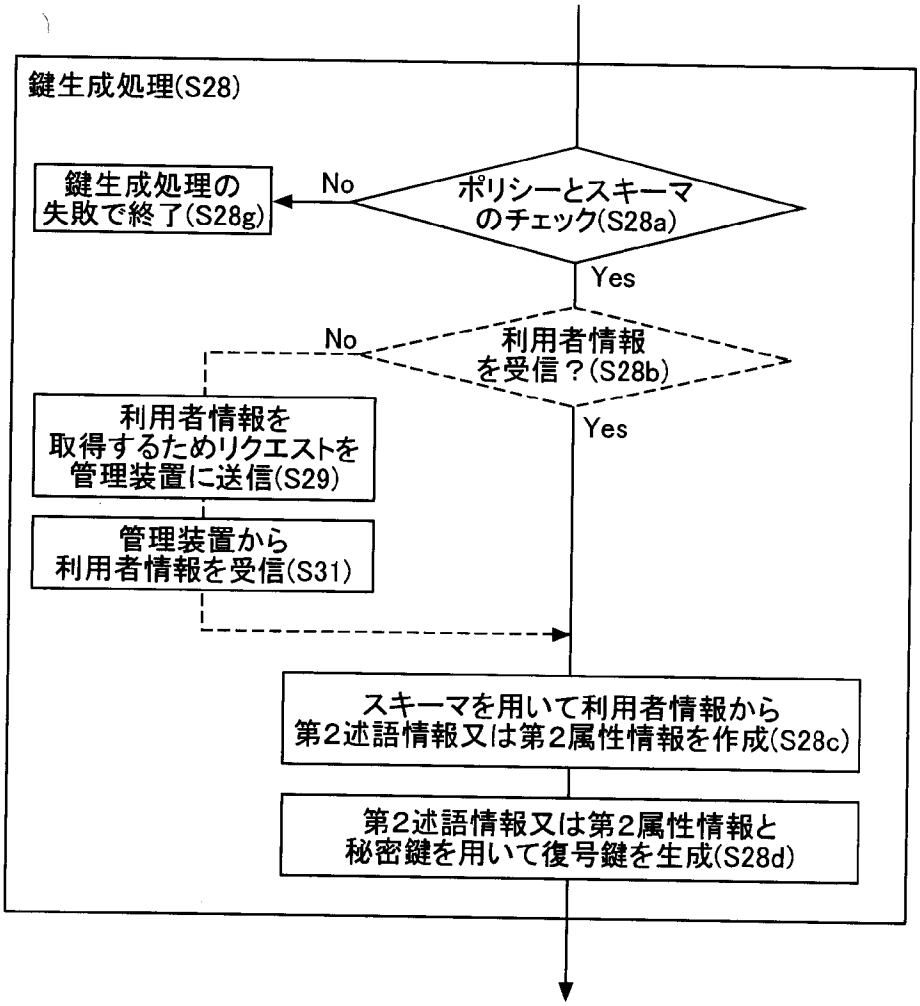

鍵生成処理(S28)
ポリシーとスキーマのチェック(S28a)
No
鍵生成処理の失敗で終了(S28g)
Yes
利用者情報を受信？(S28b)
No
Yes
利用者情報を取得するためリクエストを管理装置に送信(S29)
管理装置から利用者情報を受信(S31)
スキーマを用いて利用者情報から第2述語情報又は第2属性情報を作成(S28c)
第2述語情報又は第2属性情報と秘密鍵を用いて復号鍵を生成(S28d)

図71

[図72]

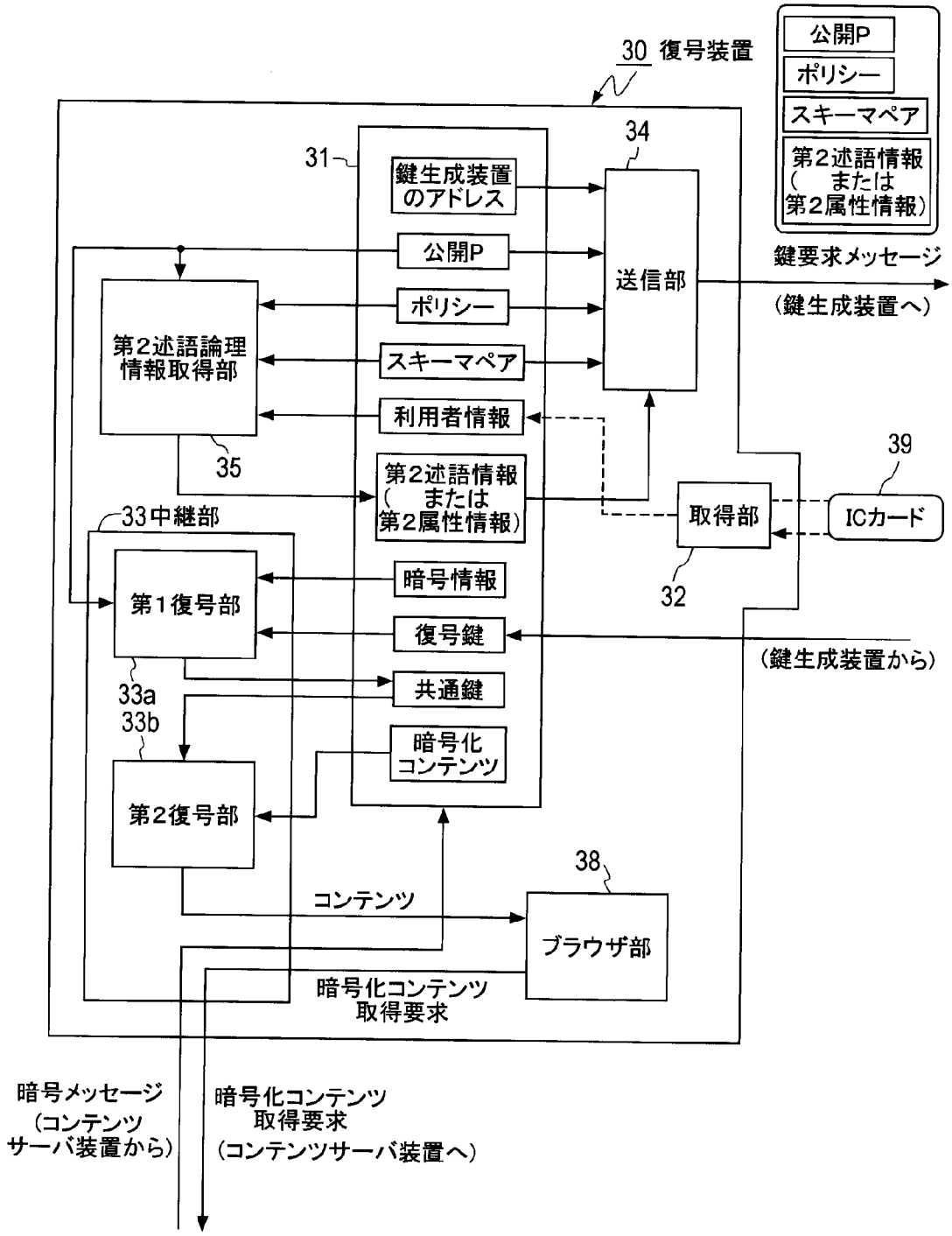

30 復号装置
公開P
ポリシー
スキーマペア
第2述語情報
(または
第2属性情報)
31
鍵生成装置
のアドレス
34
公開P
ポリシー
スキーマペア
利用者情報
送信部
鍵要求メッセージ
(鍵生成装置へ)
第2述語論理
情報取得部
35
第2述語情報
(または
第2属性情報)
39
ICカード
取得部
32
33中継部
第1復号部
暗号情報
復号鍵
(鍵生成装置から)
33a
33b
共通鍵
暗号化
コンテンツ
第2復号部
38
コンテンツ
ブラウザ部
暗号化コンテンツ
取得要求
暗号メッセージ
(コンテンツ
サーバ装置から)
暗号化コンテンツ
取得要求
(コンテンツサーバ装置へ)

図72

[図73]

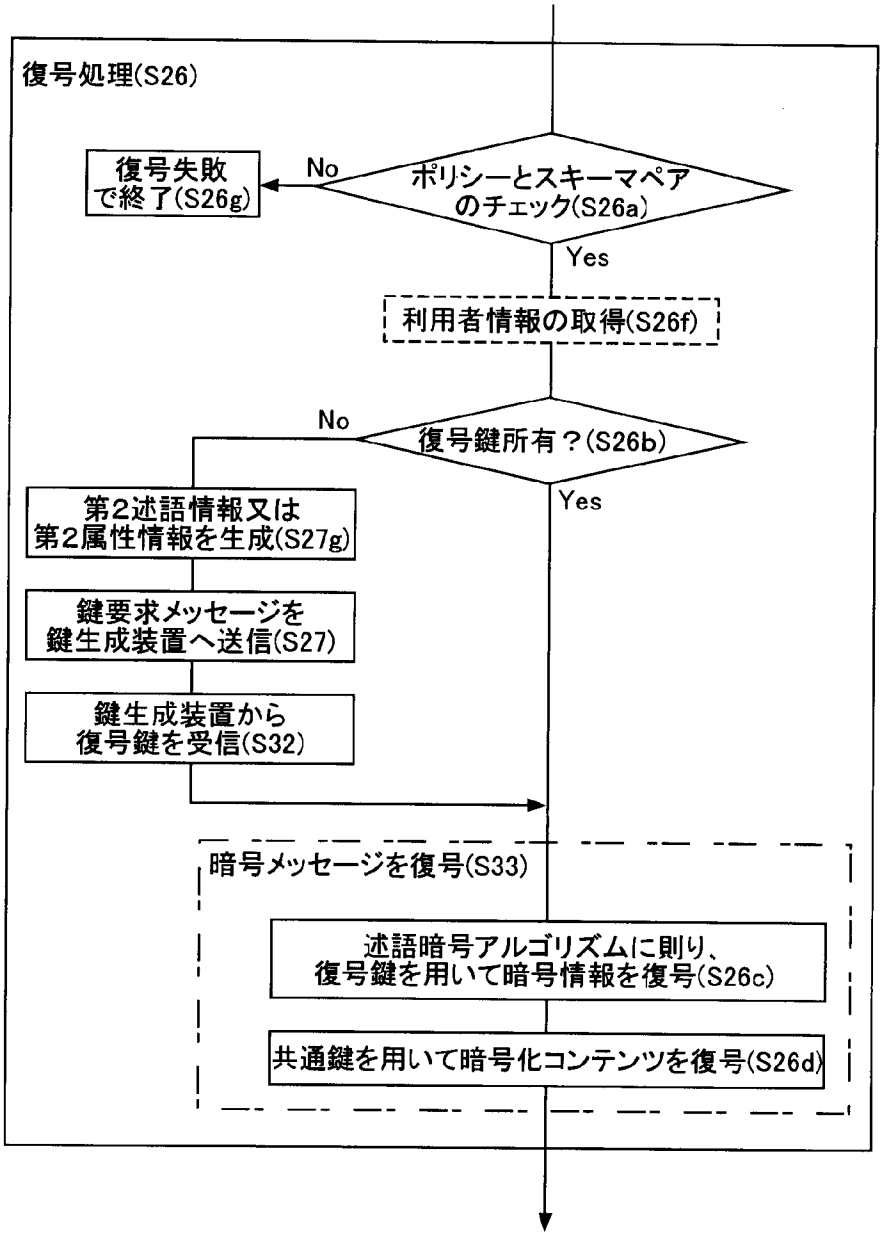

復号処理(S26)
ポリシーとスキーマペアのチェック(S26a)
No
復号失敗で終了(S26g)
Yes
利用者情報の取得(S26f)
復号鍵所有？(S26b)
No
Yes
第2述語情報又は第2属性情報を生成(S27g)
鍵要求メッセージを鍵生成装置へ送信(S27)
鍵生成装置から復号鍵を受信(S32)
暗号メッセージを復号(S33)
述語暗号アルゴリズムに則り、復号鍵を用いて暗号情報を復号(S26c)
共通鍵を用いて暗号化コンテンツを復号(S26d)

図73

[図74]

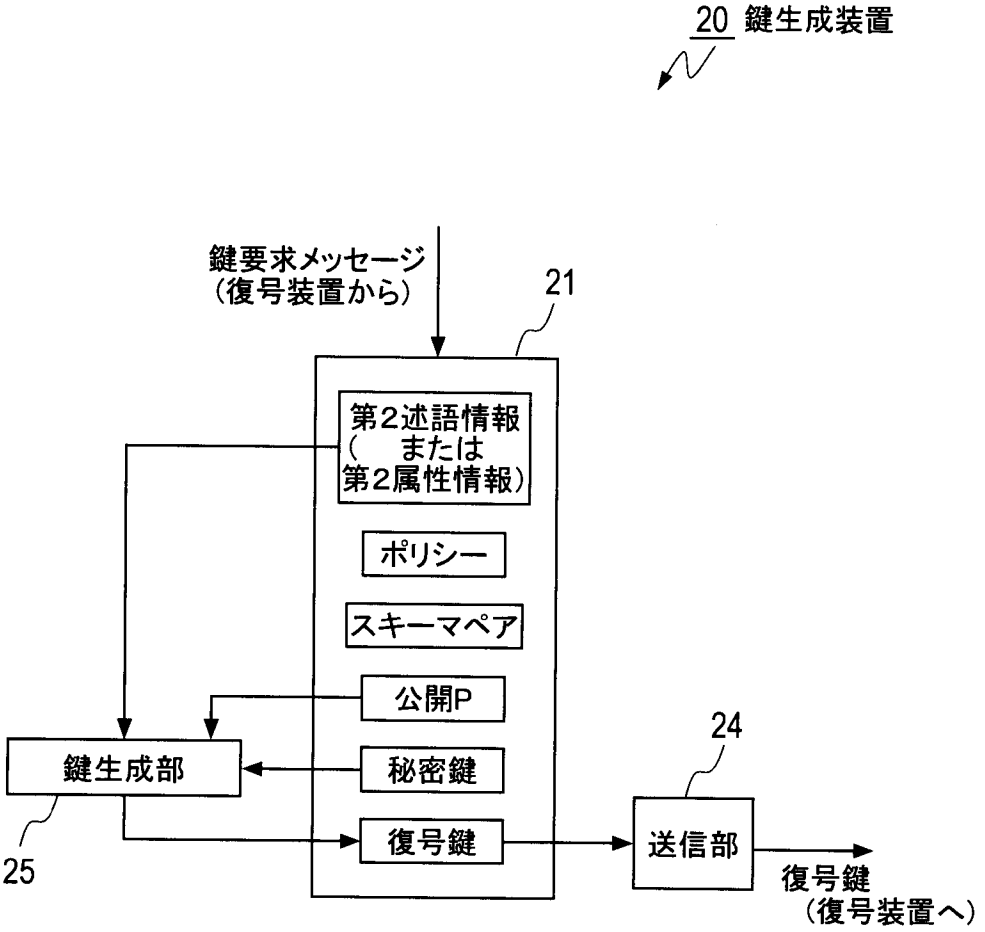

20 鍵生成装置
鍵要求メッセージ
(復号装置から)
21
第2述語情報
(または
第2属性情報)
ポリシー
スキーマペア
公開P
秘密鍵
復号鍵
鍵生成部
25
24
送信部
復号鍵
(復号装置へ)

図74

[図75]

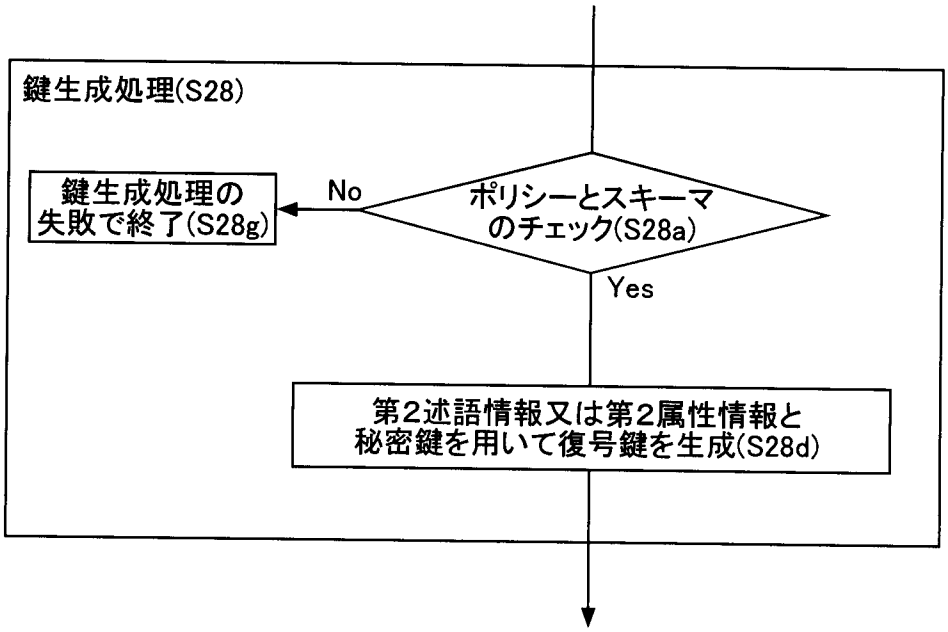

鍵生成処理(S28)
鍵生成処理の
失敗で終了(S28g)
No
ポリシーとスキーマ
のチェック(S28a)
Yes
第2述語情報又は第2属性情報と
秘密鍵を用いて復号鍵を生成(S28d)

図75

[図76]

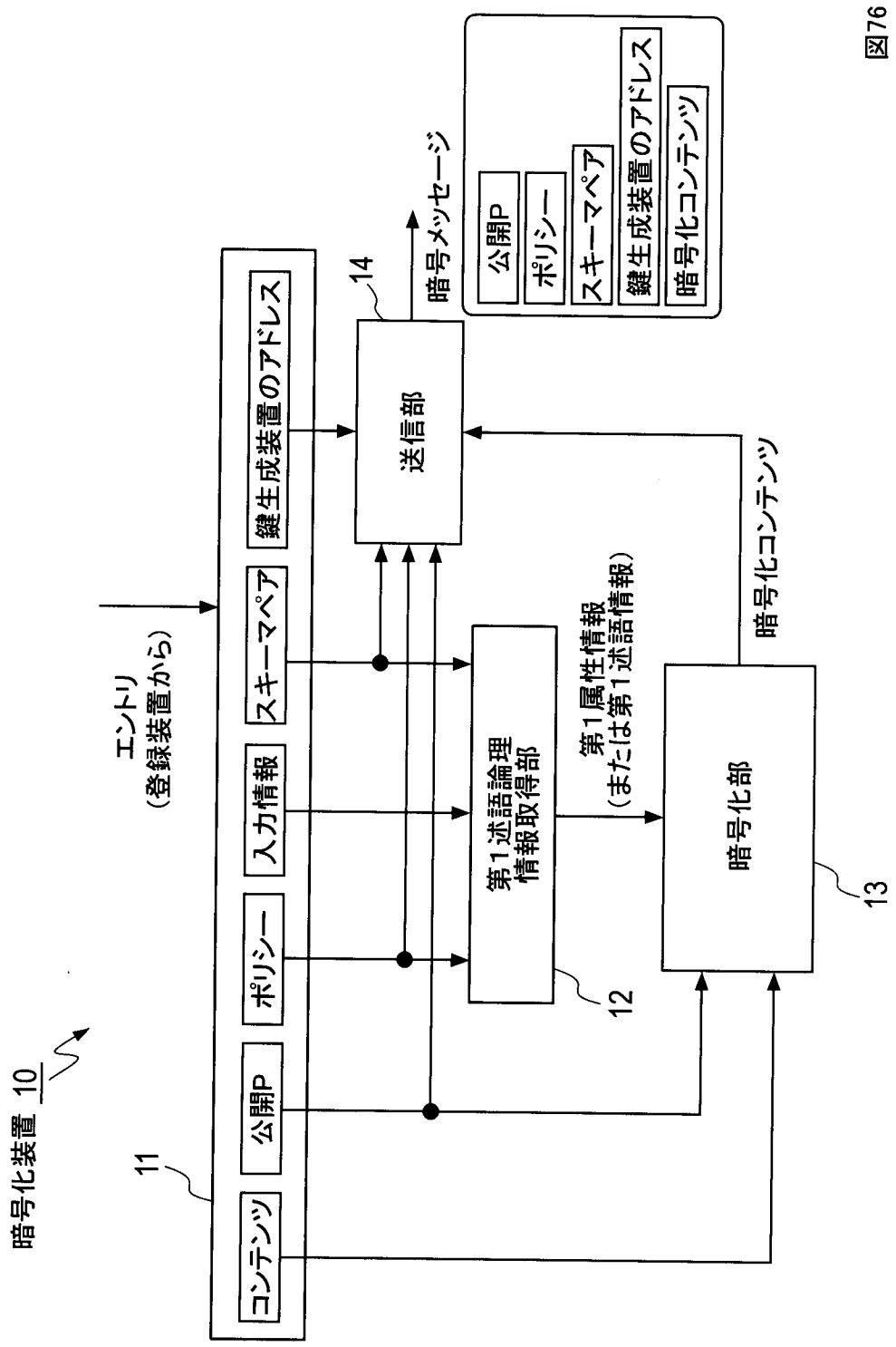

暗号化装置 10
11
コンテンツ
公開P
ポリシー
入力情報
スキーマペア
鍵生成装置のアドレス
エントリ
(登録装置から)
第1述語論理
情報取得部
12
第1属性情報
(または第1述語情報)
暗号化部
13
暗号化コンテンツ
送信部
14
暗号メッセージ
公開P
ポリシー
スキーマペア
鍵生成装置のアドレス
暗号化コンテンツ

図76

[図77]

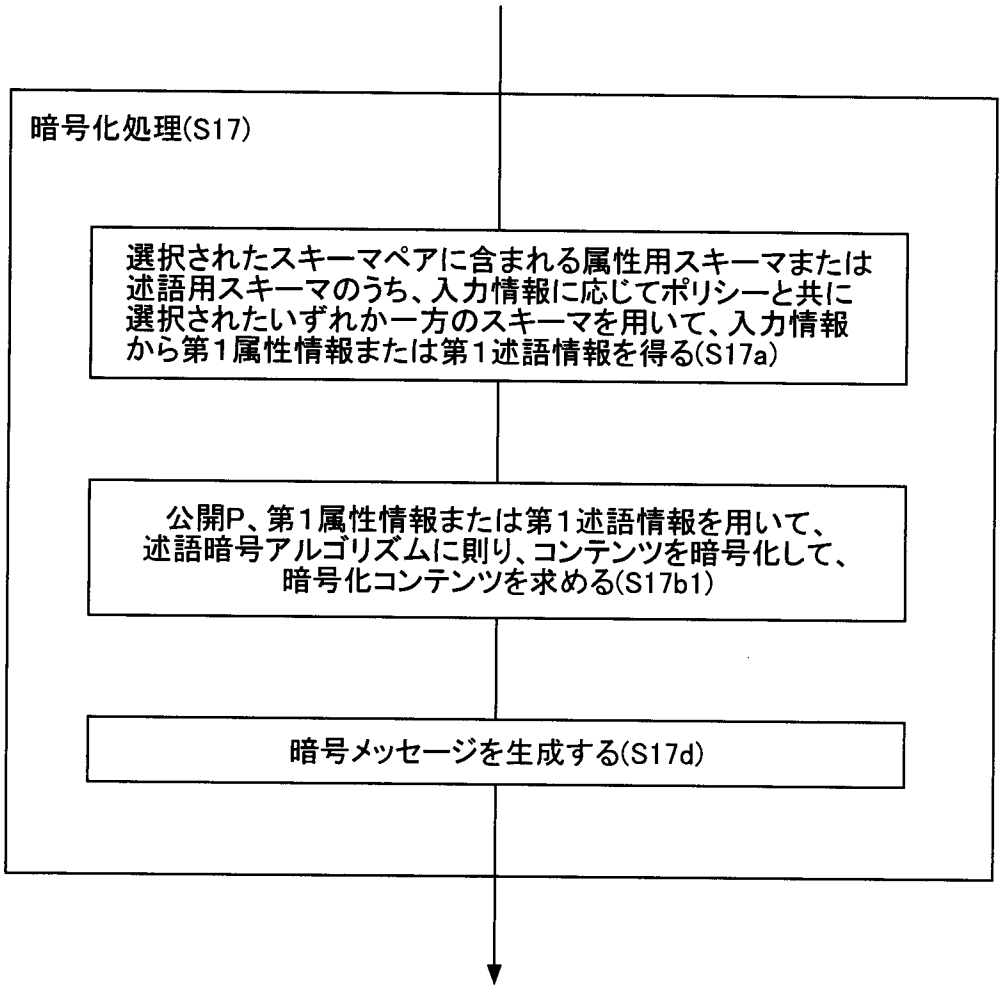

暗号化処理(S17)
選択されたスキーマペアに含まれる属性用スキーマまたは述語用スキーマのうち、入力情報に応じてポリシーと共に選択されたいずれか一方のスキーマを用いて、入力情報から第1属性情報または第1述語情報を得る(S17a)
公開P、第1属性情報または第1述語情報を用いて、述語暗号アルゴリズムに則り、コンテンツを暗号化して、暗号化コンテンツを求める(S17b1)
暗号メッセージを生成する(S17d)

図77

[図78]

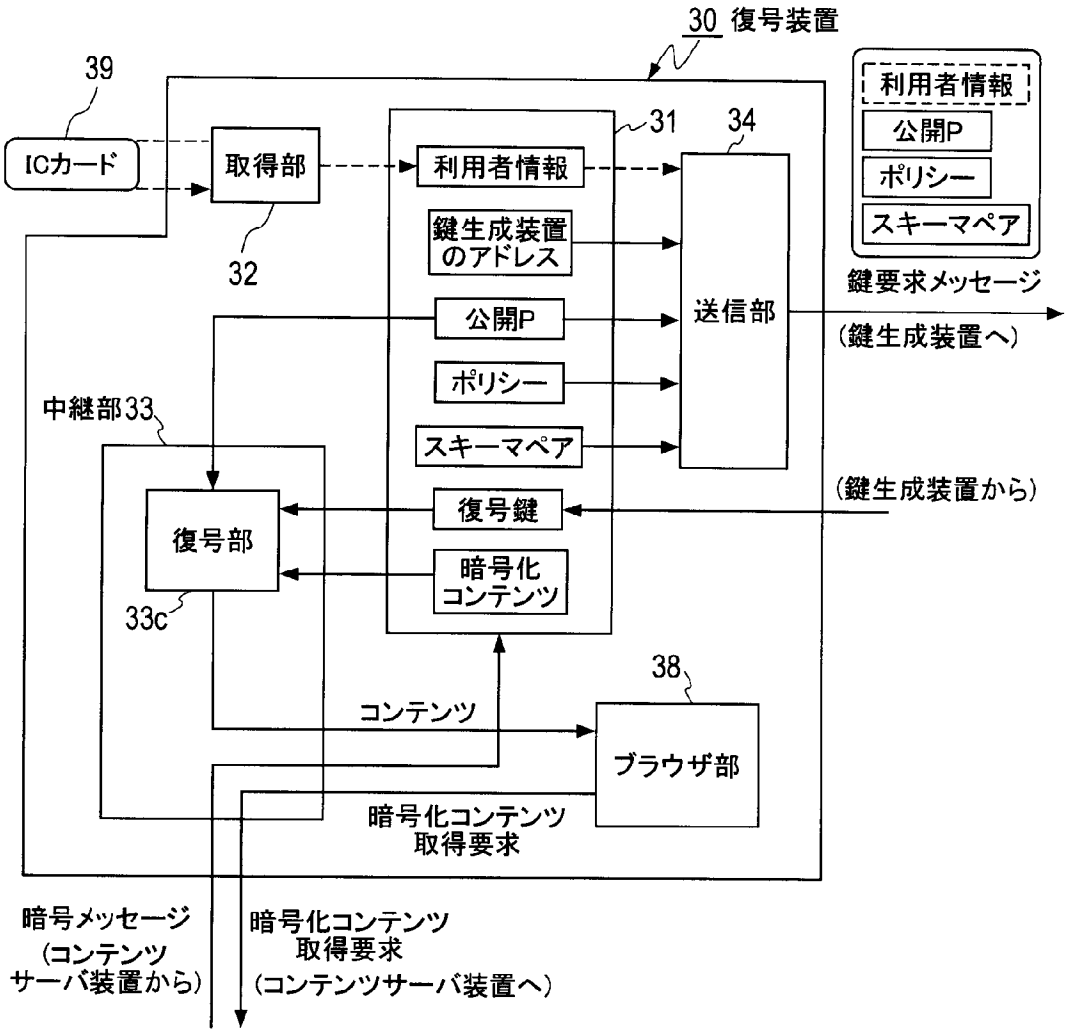

30 復号装置
39
ICカード
取得部
32
利用者情報
31
34
鍵生成装置のアドレス
公開P
ポリシー
スキーマペア
送信部
利用者情報
公開P
ポリシー
スキーマペア
鍵要求メッセージ
(鍵生成装置へ)
(鍵生成装置から)
中継部33
復号鍵
復号部
暗号化コンテンツ
33c
38
コンテンツ
ブラウザ部
暗号化コンテンツ取得要求
暗号メッセージ
(コンテンツサーバ装置から)
暗号化コンテンツ取得要求
(コンテンツサーバ装置へ)

図78

[図79]

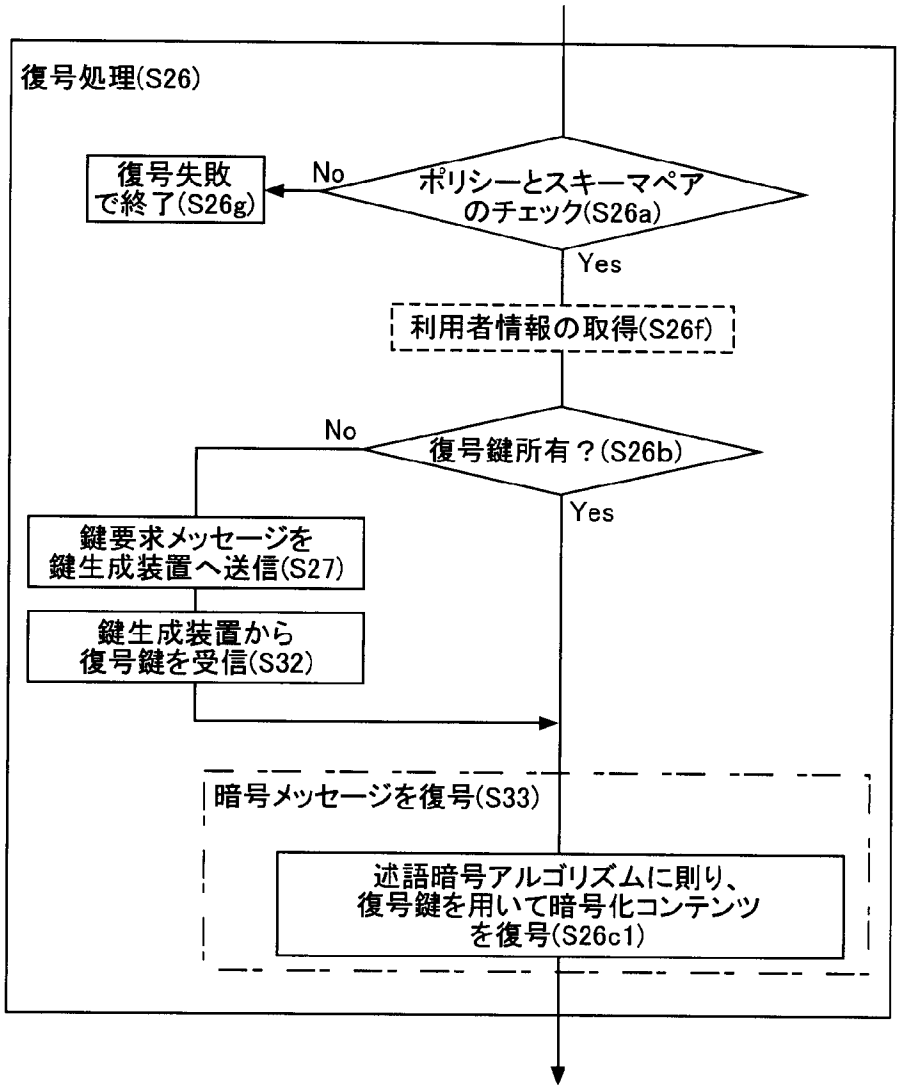

復号処理(S26)
ポリシーとスキーマペア
のチェック(S26a)
No
復号失敗
で終了(S26g)
Yes
利用者情報の取得(S26f)
復号鍵所有？(S26b)
No
Yes
鍵要求メッセージを
鍵生成装置へ送信(S27)
鍵生成装置から
復号鍵を受信(S32)
暗号メッセージを復号(S33)
述語暗号アルゴリズムに則り、
復号鍵を用いて暗号化コンテンツ
を復号(S26c1)

図79

[図80]

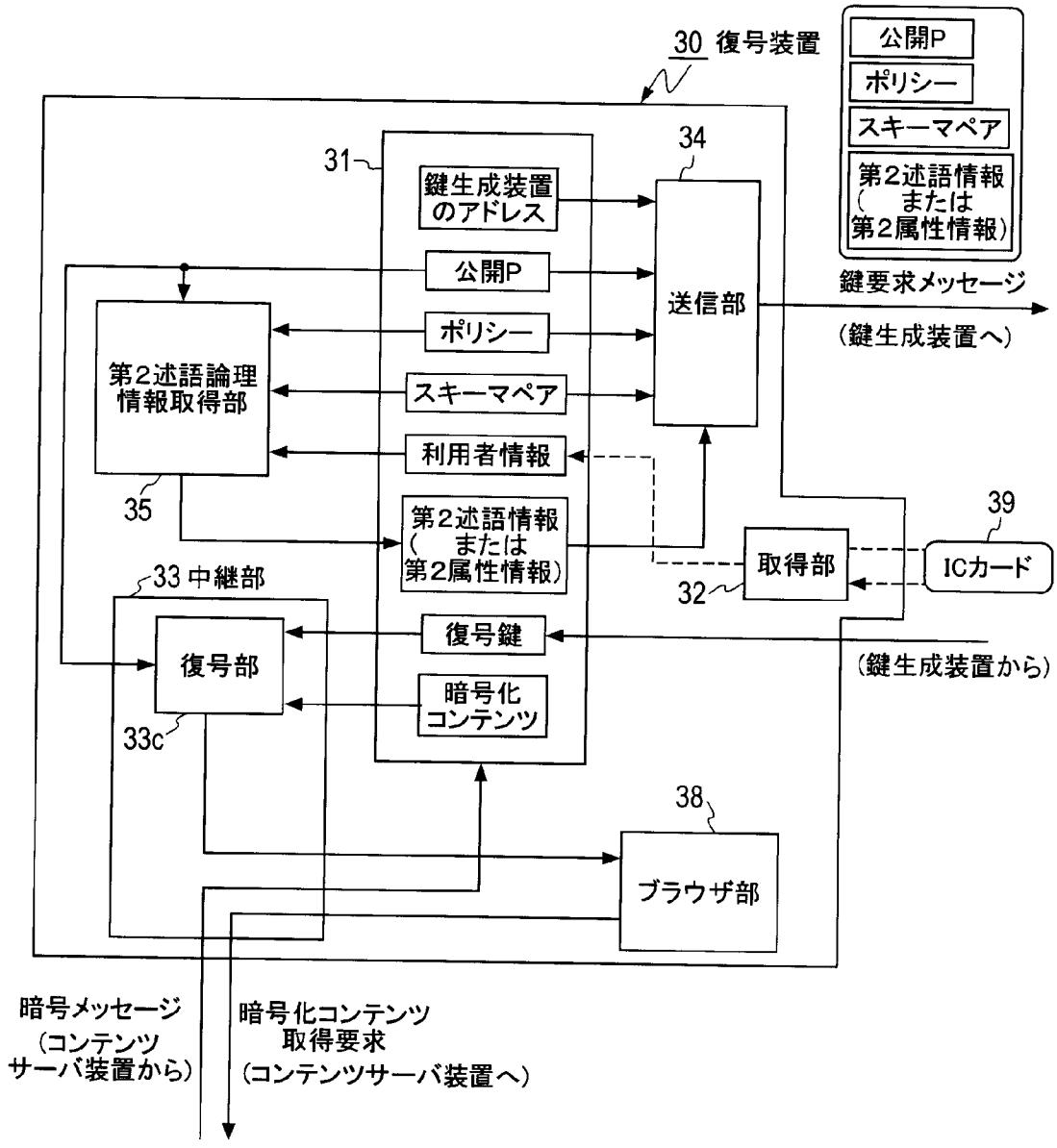

30 復号装置
公開P
ポリシー
スキーマペア
第2述語情報
(または
第2属性情報)
31
鍵生成装置
のアドレス
34
公開P
ポリシー
スキーマペア
利用者情報
送信部
鍵要求メッセージ
(鍵生成装置へ)
第2述語論理
情報取得部
35
第2述語情報
(または
第2属性情報)
39
ICカード
取得部
32
33 中継部
復号鍵
(鍵生成装置から)
復号部
暗号化
コンテンツ
33c
38
ブラウザ部
暗号メッセージ
(コンテンツ
サーバ装置から)
暗号化コンテンツ
取得要求
(コンテンツサーバ装置へ)

図80

[図81]

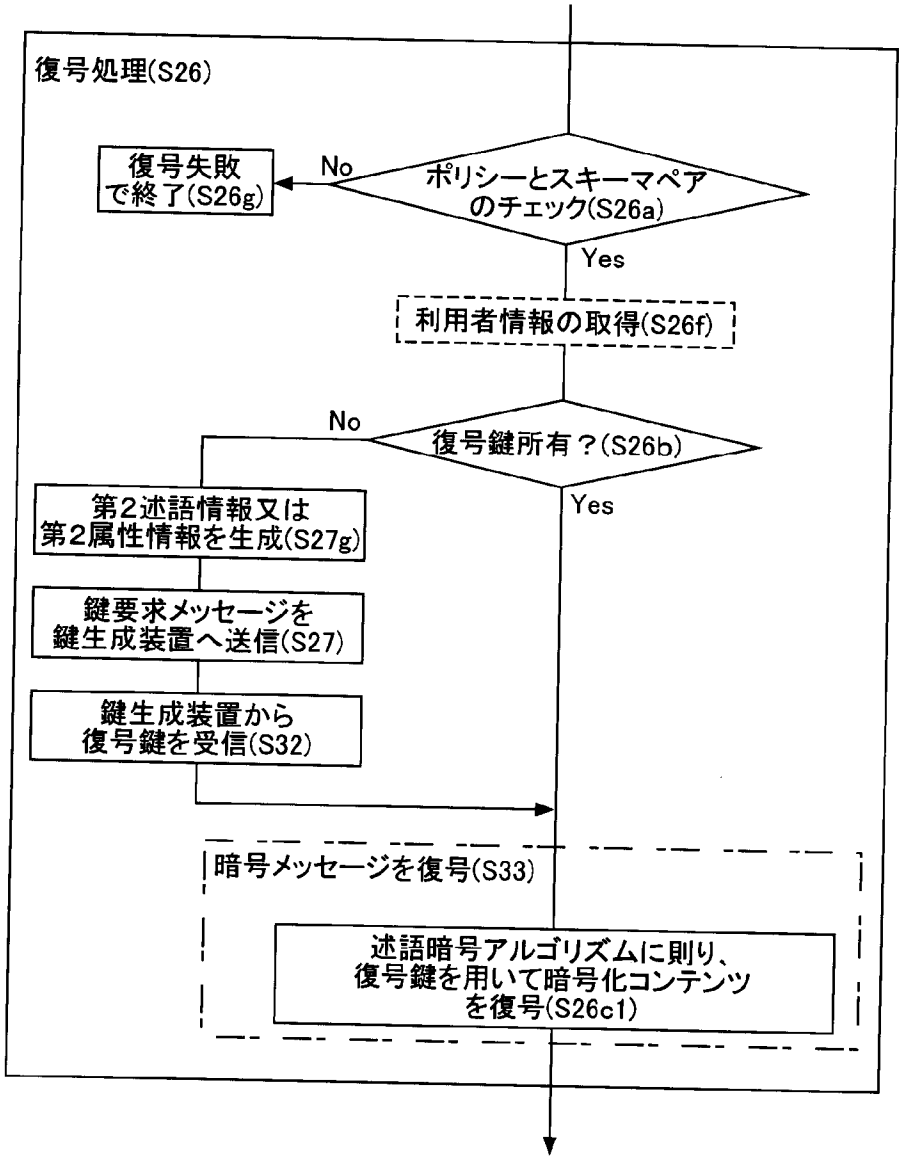

復号処理(S26)
ポリシーとスキーマペアのチェック(S26a)
No
復号失敗で終了(S26g)
Yes
利用者情報の取得(S26f)
復号鍵所有？(S26b)
No
Yes
第2述語情報又は第2属性情報を生成(S27g)
鍵要求メッセージを鍵生成装置へ送信(S27)
鍵生成装置から復号鍵を受信(S32)
暗号メッセージを復号(S33)
述語暗号アルゴリズムに則り、復号鍵を用いて暗号化コンテンツを復号(S26c1)

図81

[図82]

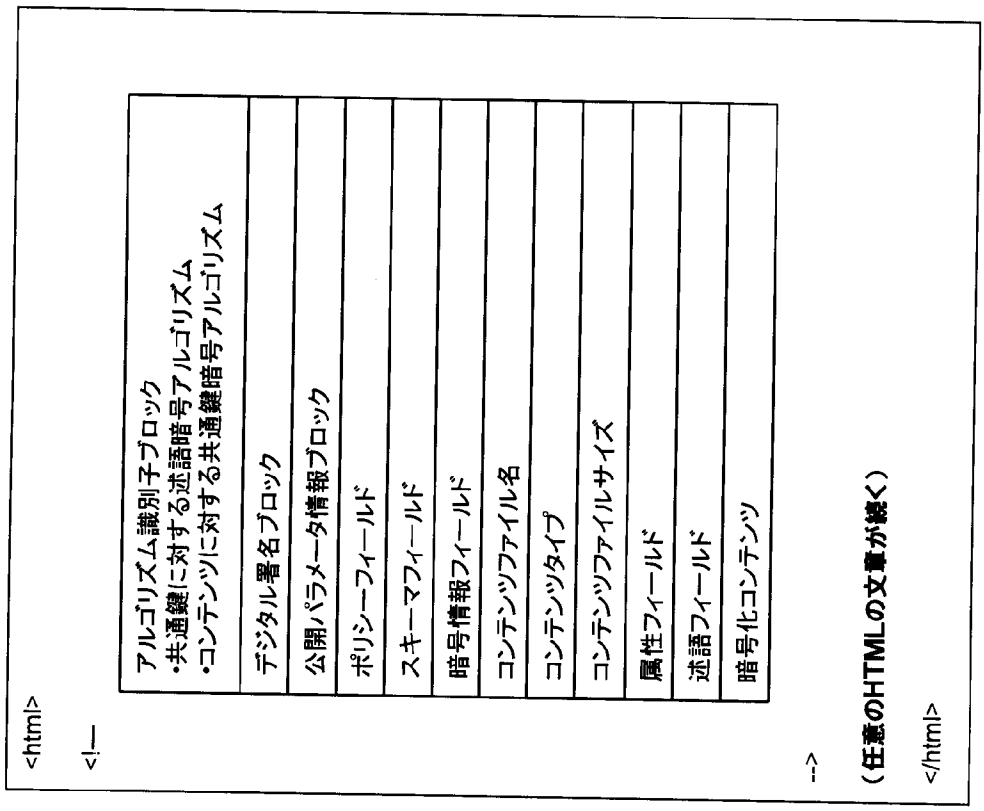

<html>
<!—
アルゴリズム識別子ブロック
•共通鍵に対する述語暗号アルゴリズム
•コンテンツに対する共通鍵暗号アルゴリズム
デジタル署名ブロック
公開パラメータ情報ブロック
ポリシーフィールド
スキーマフィールド
暗号情報フィールド
コンテンツファイル名
コンテンツタイプ
コンテンツファイルサイズ
属性フィールド
述語フィールド
暗号化コンテンツ
-->
（任意のHTMLの文章が続く）
</html>

図82

[図83]

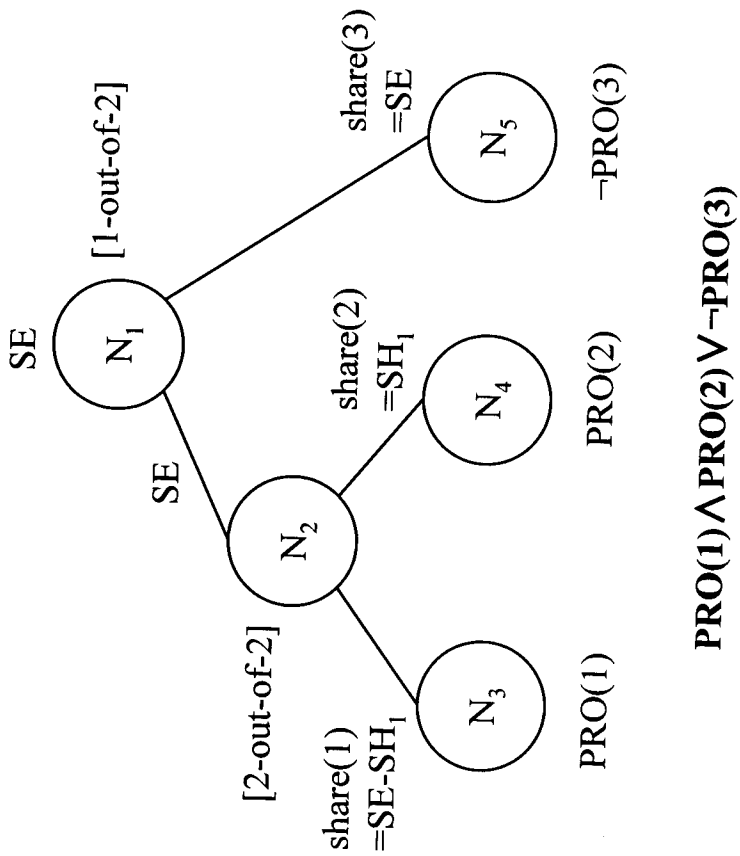

SE
N1
[1-out-of-2]
share(3)
=SE
N5
¬PRO(3)
SE
N2
share(2)
=SH1
N4
PRO(2)
[2-out-of-2]
share(1)
=SE-SH1
N3
PRO(1)
PRO(1)∧PRO(2)∨¬PRO(3)

図83

[図84]

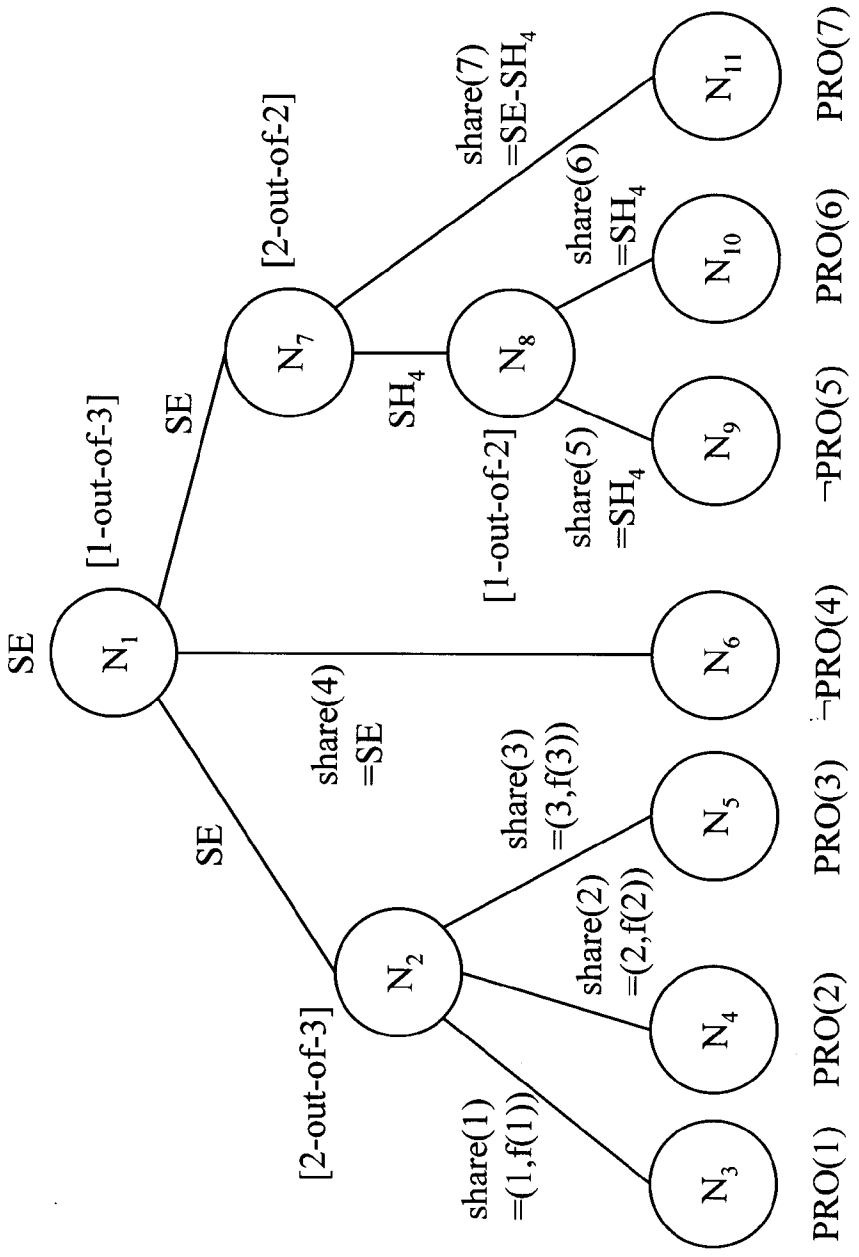

SE
N1
[1-out-of-3]
SE
SE
[2-out-of-3]
N2
share(1)
=(1,f(1))
share(2)
=(2,f(2))
share(3)
=(3,f(3))
share(4)
=SE
N3
N4
N5
N6
N7
[2-out-of-2]
SH4
N8
[1-out-of-2]
share(5)
=SH4
share(6)
=SH4
share(7)
=SE-SH4
N9
N10
N11
PRO(1)
PRO(2)
PRO(3)
¬PRO(4)
¬PRO(5)
PRO(6)
PRO(7)
PRO(1)∧PRO(2)∨PRO(2)∧PRO(3)∨PRO(1)∧PRO(3)
∨¬PRO(4)∨(¬PRO(5)∨PRO(6))∧PRO(7)

図84

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/066716

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2011
Kokai Jitsuyo Shinan Koho	1971-2011	Toroku Jitsuyo Shinan Koho	1994-2011

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580(JDreamII), functional encryption, attribute-based encryption

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2009/0080658 A1 (Brent Waters, et al.), 26 March 2009 (26.03.2009), all pages (Family: none)	1-39
A	Katz, J., et al., Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products, Cryptology ePrint Archive, Report 2007/404, 2008.07.07, p.1-29, 4 Our Main Construction	1-39
A	Attrapadung, N., et al., Dual-Policy Attribute Based Encryption, Lecture Notes in Computer Science, Vol.5536, 2009, p.168-185, 1 Introduction, 4 Dual-Policy ABE Scheme, 6 Single-Policy Modes of DP-ABE	1-39

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 13 September, 2011 (13.09.11)	Date of mailing of the international search report 20 September, 2011 (20.09.11)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/066716

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Lewko, A., et al., Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption, Cryptology ePrint Archive, Report 2010/110, 2010.03.29, p.1-56, 2 Fully Secure Attribute-Based Encryption, 3 Fully Secure Predicate Encryption	1-39
P,A	Boneh, D., et al., Functional Encryption: Definitions and Challenges, Cryptology ePrint Archive, Report 2010/543, 2011.01.04, p.1-23, all pages	1-39

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１１／０６６７１６

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１１年
日本国実用新案登録公報	１９９６－２０１１年
日本国登録実用新案公報	１９９４－２０１１年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JSTPlus/JMEDPlus/JST7580(JDreamII) functional encryption, attribute-based encryption

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	US 2009/0080658 A1 (Brent Waters, et al.) 2009.03.26, 全頁を参照（ファミリーなし）	1-39
A	Katz, J., et al., Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products, Cryptology ePrint Archive, Report 2007/404, 2008.07.07, p.1-29, 4 Our Main Construction	1-39

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１３．０９．２０１１	２０．０９．２０１１

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　９３６４
中里　裕正
電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	Attrapadung, N., et al., Dual-Policy Attribute Based Encryption, Lecture Notes in Computer Science, Vol.5536, 2009, p.168-185, 1 Introduction, 4 Dual-Policy ABE Scheme, 6 Single-Policy Modes of DP-ABE	1-39
A	Lewko, A., et al., Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption, Cryptology ePrint Archive, Report 2010/110, 2010.03.29, p.1-56, 2 Fully Secure Attribute-Based Encryption, 3 Fully Secure Predicate Encryption	1-39
P, A	Boneh, D., et al., Functional Encryption: Definitions and Challenges, Cryptology ePrint Archive, Report 2010/543, 2011.01.04, p.1-23, 全頁を参照	1-39