(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
2006 年12 月28 日 (28.12.2006)

PCT

(10) 国際公開番号
WO 2006/137250 A1

(51) 国際特許分類:
H04L 9/32 (2006.01) *G06Q 10/00* (2006.01)
G06F 21/20 (2006.01) *G06Q 50/00* (2006.01)
G06F 21/24 (2006.01)

(21) 国際出願番号: PCT/JP2006/310909

(22) 国際出願日: 2006 年5 月31 日 (31.05.2006)

(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2005-183560 2005 年6 月23 日 (23.06.2005) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目７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): 米澤 祥子 (YONEZAWA, Shoko) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP). 佐古 和恵 (SAKO, Kazue) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP).

(74) 代理人: 宮崎 昭夫, 外(MIYAZAKI, Teruo et al.); 〒1070052 東京都港区赤坂１丁目９番２０号 第１６興和ビル８階 Tokyo (JP).

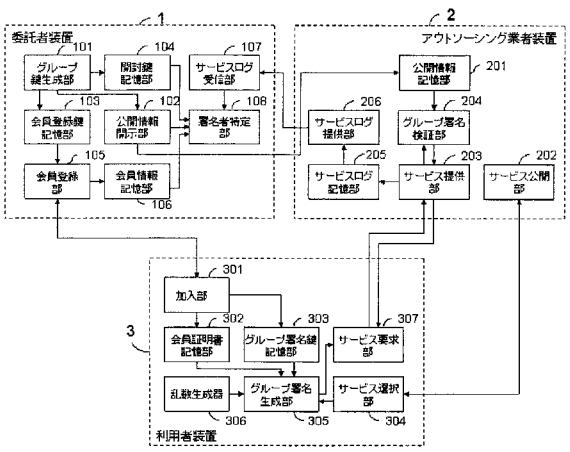
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI,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

[続葉有]

(54) **Title:** SERVICE PROVIDING SYSTEM, OUTSOURCING BUSINESS DEVICE, SERVICE PROVIDING METHOD, AND PROGRAM

(54) 発明の名称: サービス提供システム、アウトソーシング業者装置、サービス提供方法およびプログラム



1... CLIENT DEVICE
101. GROUP KEY CREATION UNIT
102. PUBLIC INFORMATION DISCLOSURE UNIT
103. MEMBER REGISTRATION KEY STORAGE UNIT
104. OPENING KEY STORAGE UNIT
105. MEMBER REGISTRATION UNIT
106. MEMBER INFORMATION STORAGE UNIT
107. SERVICE LOG RECEPTION UNIT
108. SIGNER SPECIFICATION UNIT
2... OUTSOURCING BUSINESS DEVICE
201. PUBLIC INFORMATION STORAGE UNIT
202. SERVICE PUBLIC UNIT
203. SERVICE PROVIDING UNIT
204. GROUP SIGNATURE VERIFICATION UNIT
205. SERVICE LOG STORAGE UNIT
206. SERVICE LOG PROVIDING UNIT
3... USER DEVICE
301. SUBSCRIPTION UNIT
302. MEMBER CERTIFICATION STORAGE UNIT
303. GROUP SIGNATURE KEY STORAGE UNIT
304. SERVICE SELECTION UNIT
305. GROUP SIGNATURE CREATION UNIT
306. RANDOM NUMBER CREATOR
307. SERVICE REQUEST UNIT

(57) Abstract: A client is enabled to receive member services, at the time of asking an outsourcing business for the services, while keeping the member information secret from the outsourcing business, and without any communication with the user. At the time of using the services, a user device (3) transmits group signature data to an outsourcing business device (2). The outsourcing business device (2) verifies the group signature data by using the public information of a client device (1). When the verification is satisfied to confirm that the user device (3) is a member of the client device (1), the outsourcing business device (2) provides services for the user device (3).

(57) 要約: 委託者が、会員向けサービスをアウトソーシング業者に委託する際に、委託者の管理する会員情報をアウトソーシング業者に秘匿し、かつ利用者が委託者と通信せずにサービスを受けられるようにする。サービスを利用する際、利用者装置３は、アウトソーシング業者装置２にグループ署名データを送信する。アウトソーシング業者装置２は、委託者装置１の公開情報を用いてグループ署名データを検証する。検証を通過し、利用者装置３が確かに委託者装置１の会員であることが確認できたら、アウトソーシング業者装置２は、利用者装置３にサービスを提供する。

WO 2006/137250 A1

KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。