

(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



(10) 国際公開番号

WO 2012/063783 A1

PCT

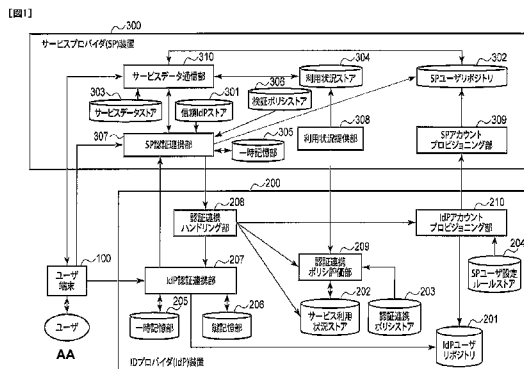
(43) 国際公開日
2012 年 5 月 18 日(18.05.2012)

- (51) 国際特許分類:
G06F 21/20 (2006.01) H04L 9/32 (2006.01)
- (21) 国際出願番号: PCT/JP2011/075611
- (22) 国際出願日: 2011 年 11 月 7 日(07.11.2011)
- (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 2010-250903 2010 年 11 月 9 日(09.11.2010) JP
- (71) 出願人 (米国を除く全ての指定国について): 株式会社 東芝 (KABUSHIKI KAISHA TOSHIBA) [JP/JP]; 〒1058001 東京都港区芝浦一丁目 1 番 1 号 Tokyo (JP). 東芝ソリューション株式会社 (TOSHIBA SOLUTIONS CORPORATION) [JP/JP]; 〒1056691 東京都港区芝浦一丁目 1 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): 西澤 実 (NISHIZAWA, Minoru) [JP/JP]. 田中 誠一郎 (TANAKA, Seiichiro) [JP/JP]. 池田 竜朗 (IKEDA, Tatsuro) [JP/JP].
- (74) 代理人: 蔵田 昌俊, 外 (KURATA, Masatoshi et al.); 〒1050001 東京都港区虎ノ門 1 丁目 1 2 番 9 号 鈴榮特許総合事務所内 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, 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, QA, RO, RS, RU, RW, 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.

[続葉有]

(54) Title: AUTHENTICATION COLLABORATION SYSTEM AND ID PROVIDER DEVICE

(54) 発明の名称: 認証連携システム及び ID プロバイダ装置



- 100 User terminal
200 ID provider (IdP) device
201 IdP user repository
202 Service usage status store
203 Authentication collaboration policy store
204 SP user settings rule store
205 Key storage unit
206 Key storage unit
207 IdP authentication collaboration unit
208 Authentication collaboration handling unit
209 Authentication collaboration policy evaluation unit
210 IdP account provisioning unit
300 Service provider (SP) device
301 Trusted IdP store
302 SP user repository
303 Service data store
304 Usage status store
306 Verification policy store
307 SP authentication collaboration unit
308 Usage status provision unit
309 SP account provisioning unit
310 Service data communication unit
AA User

(57) Abstract: According to the embodiment of the present invention, policy storage means of an ID provider device stores a plurality of policy information units indicating affiliations and positions of users for which transmission of service data is permitted. The ID provider device, upon success of login processing, transmits a policy evaluation request including the user ID used in the login processing and the service provider ID within an authentication collaboration request. The ID provider device reads policy information from the policy storage means on the basis of the policy evaluation request. Transmission permission assessment means of the ID provider device assesses whether or not to permit transmission of the service data depending upon whether or not the affiliation and the position within user attribute information comply with the affiliations and positions indicated in the policy information.

(57) 要約: 実施形態によれば、前記 ID プロバイダ装置のポリシー記憶手段は、前記サービスプロバイダ ID 毎に、サービスデータの送信が許可されるユーザの所属及び役職を示す複数のポリシー情報を記憶する。前記 ID プロバイダ装置は、前記ログイン処理が成功したとき、当該ログイン処理に用いたユーザ ID と前記認証連携要求内のサービスプロバイダ ID とを含むポリシー評価要求を送出する。前記 ID プロバイダ装置は、ポリシー評価要求に基づいて前記ポリシー記憶手段からポリシー情報を読み出す。前記 ID プロバイダ装置の送信許可判定手段は、ポリシー情報に示される所属及び役職に対しユーザ属性情報内の所属及び役職が適合するかどうかに応じて、前記サービスデータの送信を許可するかどうかを判定する。



(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, RW, 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 (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))