

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2005 年 8 月 4 日 (04.08.2005)

PCT

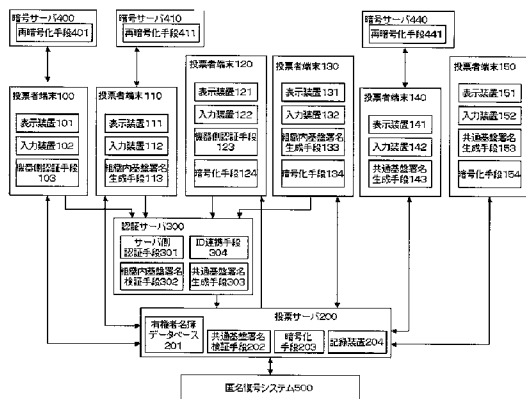
(10) 国際公開番号
WO 2005/071878 A1

- (51) 国際特許分類⁷: H04L 9/08, 9/32, (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 7-1 Tokyo (JP).
- (21) 国際出願番号: PCT/JP2005/000532
- (22) 国際出願日: 2005 年 1 月 18 日 (18.01.2005) (72) 発明者; および
- (25) 国際出願の言語: 日本語 (75) 発明者/出願人 (米国についてのみ): 森 健吾 (MORI, Kengo) [JP/JP]; 〒1088001 東京都港区芝五丁目 7-1 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 7-1 日本電気株式会社内 Tokyo (JP).
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2004-016894 2004 年 1 月 26 日 (26.01.2004) JP

/ 続葉有 /

(54) Title: ANONYMOUS ELECTRONIC VOTING SYSTEM AND ANONYMOUS ELECTRONIC VOTING METHOD

(54) 発明の名称: 匿名電子投票システム及び匿名電子投票方法



(57) Abstract: An encrypted candidate name corresponding to a candidate selected from a combination list of a candidate name transmitted from a voting server (200) by voter terminals (100, 110, 140) and an encrypted candidate name, is transmitted to an encryption server (400) via a network. The encrypted candidate name is re-encrypted into encrypted voting data by the encryption server (400) and the data is returned to the voter terminals (100, 110, 140). Among them, a valid encrypted voting data list is created so that voting is performed in the voting server (200) via the network and an anonymous decoding system (500) decrypts the encrypted voting data.

- 400 ENCRYPTION SERVER
401 RE-ENCRYPTION MEANS
410 ENCRYPTION SERVER
411 RE-ENCRYPTION MEANS
440 ENCRYPTION SERVER
441 RE-ENCRYPTION MEANS
100 VOTER TERMINAL
101 DISPLAY DEVICE
102 INPUT DEVICE
103 DEVICE SIDE AUTHENTICATION MEANS
110 VOTER TERMINAL
111 DISPLAY DEVICE
112 INPUT DEVICE
113 IN-ORGANIZATION SUBSTRATE SIGNATURE CREATION MEANS
120 VOTER TERMINAL
121 DISPLAY DEVICE
122 INPUT DEVICE
123 DEVICE SIDE AUTHENTICATION MEANS
124 ENCRYPTION MEANS
130 VOTER TERMINAL
131 DISPLAY DEVICE
132 INPUT DEVICE
133 IN-ORGANIZATION SUBSTRATE SIGNATURE CREATION MEANS
134 ENCRYPTION MEANS
140 VOTER TERMINAL
141 DISPLAY DEVICE
142 INPUT DEVICE
143 COMMON SUBSTRATE SIGNATURE CREATION MEANS
150 VOTER TERMINAL
151 DISPLAY DEVICE
152 INPUT DEVICE
153 COMMON SUBSTRATE SIGNATURE CREATION MEANS
154 ENCRYPTION MEANS
300 AUTHENTICATION SERVER
301 SERVER SIDE AUTHENTICATION MEANS
304 ID LINKAGE MEANS
302 IN-ORGANIZATION SUBSTRATE SIGNATURE VERIFICATION MEANS
303 COMMON SUBSTRATE SIGNATURE CREATION MEANS
200 VOTING SERVER
201 VOTER LIST DATABASE
202 COMMON SUBSTRATE SIGNATURE VERIFICATION MEANS
203 ENCRYPTION MEANS
204 RECORDING DEVICE
500 ANONYMOUS DECRYPTION SYSTEM

/ 続葉有 /

WO 2005/071878 A1



(74) 代理人: 稲垣 清, 外(INAGAKI, Kiyoshi et al.); 〒1010042 東京都千代田区神田東松下町3 7 林道ビル 5 階 扶桑特許事務所内 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, 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, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, 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, 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, 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。

(57) 要約:

投票者端末 (1 0 0, 1 1 0, 1 4 0) により投票サーバ (2 0 0) から送信された候補者名と暗号化候補者名との組み合わせリストの中から選択した候補者に対応する暗号化候補者名をネットワーク経由で暗号サーバ (4 0 0) へ送信し、暗号化サーバ (4 0 0) により該暗号化候補者名を再度暗号化した暗号化投票データを返信された投票者端末 (1 0 0, 1 1 0, 1 4 0) は、このうち有効な暗号化投票データリストを作成してネットワーク経由で投票サーバ (2 0 0) に投票を行い、匿名復号システム (5 0 0) により暗号化投票データの復号を行う。