

(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 4 月 12 日(12.04.2012)

PCT

(10) 国際公開番号
WO 2012/046303 A1

- (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/JP2010/067472
- (22) 国際出願日: 2010 年 10 月 5 日(05.10.2010)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人 (米国を除く全ての指定国について): 株式会社シー・エス・イー (Computer Systems Engineering Co., Ltd.) [JP/JP]; 〒1500044 東京都渋谷区円山町 2 3 番 2 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): 玉井 成知 (TAMAI Shigetomo) [JP/JP]; 〒1500044 東京都渋谷区円山町 2 3 番 2 号 株式会社シー・エス・イー内 Tokyo (JP). 高野 透 (TAKANO Toru) [JP/JP]; 〒1500044 東京都渋谷区円山町 2 3 番 2 号 株式会社シー・エス・イー内 Tokyo (JP).

小林 剛 (KOBAYASHI Tsuyoshi) [JP/JP]; 〒1500044 東京都渋谷区円山町 2 3 番 2 号 株式会社シー・エス・イー内 Tokyo (JP).

(74) 代理人: 辻居 幸一, 外 (TSUJII Koichi et al.); 〒1008355 東京都千代田区丸の内 3 丁目 3 番 1 号 新東京ビル 中村合同特許法律事務所 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.

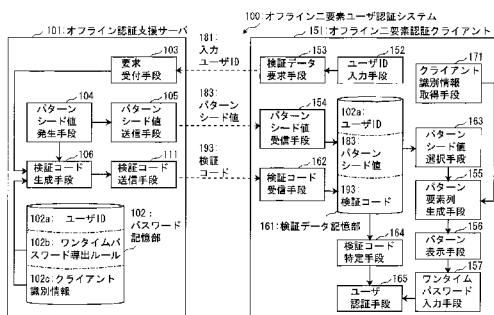
[続葉有]

(54) Title: OFFLINE TWO-FACTOR USER AUTHENTICATION SYSTEM, METHOD THEREFOR THEREOF, AND PROGRAM THEREFOR THEREOF

(54) 発明の名称: オフライン二要素ユーザ認証システム、その方法、およびそのプログラム

[図2]

FIG. 2



- 100 OFFLINE TWO-FACTOR USER AUTHENTICATION SYSTEM
- 101 OFFLINE AUTHENTICATION ASSISTANCE SERVER
- 102 PASSWORD STORAGE UNIT
- 102a USER ID
- 102b ONE-TIME PASSWORD DERIVATION RULE
- 102c CLIENT IDENTIFICATION INFORMATION
- 103 REQUEST RECEIVING MEANS
- 104 PATTERN SEED VALUE GENERATION MEANS
- 105 PATTERN SEED VALUE TRANSMISSION MEANS
- 106 VERIFICATION CODE GENERATION MEANS
- 111 VERIFICATION CODE TRANSMISSION MEANS
- 151 OFFLINE TWO-FACTOR AUTHENTICATION CLIENT
- 152 USER ID INPUT MEANS
- 153 VERIFICATION DATA REQUEST MEANS
- 154 PATTERN SEED VALUE RECEIVING MEANS
- 155 PATTERN REQUEST STRING GENERATION MEANS
- 156 PATTERN DISPLAY MEANS
- 157 ONE-TIME PASSWORD INPUT MEANS
- 161 VERIFICATION DATA STORAGE MEANS UNIT
- 162 VERIFICATION CODE RECEIVING MEANS
- 163 PATTERN SEED VALUE SELECTION MEANS
- 164 VERIFICATION CODE SPECIFYING MEANS
- 165 USER AUTHENTICATION MEANS
- 171 CLIENT IDENTIFICATION INFORMATION ACQUISITION MEANS
- 181 INPUT USER ID
- 183 PATTERN SEED VALUE
- 193 VERIFICATION CODE

(57) Abstract: The present invention realizes implements matrix authentication for offline two-factor authentication, reducing the risk of authentication information leakage. A two-factor user authentication system using uses as a password a derivation rule for generating a one-time password by applying the derivation rule to an element factor included at a specific position in a presentation pattern included in a presentation pattern, and further using the password to authenticate identification information of a client used by a user. wherein Wwithin an offline authentication client, authentication is carried out by: storing on the client a plurality of pattern seed values which are values that combined with client identification information uniquely determine a presentation pattern, and a plurality of verification codes respectively corresponding to the plurality of pattern seed values; generating a presentation pattern on the basis of the client identification information, and one selected pattern seed value; and verifying an inputted one-time password on the basis of a corresponding verification code.

(57) 要約:

[続葉有]