(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 8 月 23 日(23.08.2012)

WIPO | PCT

(10) 国際公開番号
WO 2012/111714 A1

(51) 国際特許分類:
H04L 9/08 (2006.01) *H04L 9/14* (2006.01)
G09C 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2012/053547

(22) 国際出願日: 2012 年 2 月 15 日(15.02.2012)

(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 2011-030813 2011 年 2 月 16 日(16.02.2011) 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): 吉田 琢也 **(YOSHIDA, Takuya)** [JP/JP]. 岡田 光司 **(OKADA, Koji)** [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１２番９号 鈴榮特許綜合事務所内 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.

(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,

[続葉有]

(54) **Title**: FILE SERVER DEVICE AND FILE SERVER SYSTEM

(54) 発明の名称 : ファイルサーバ装置およびファイルサーバシステム

[図1]

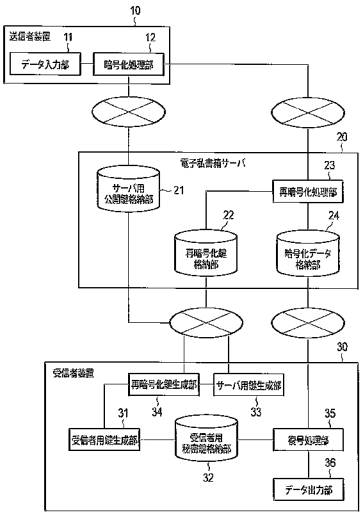

FIG. 1:
10 TRANSMITTER DEVICE
11 DATA INPUT UNIT
12 ENCRYPTION PROCESSING UNIT
20 ELECTRONIC PRIVATE MAILBOX SERVER
21 SERVER-USE PUBLIC KEY STORAGE UNIT
22 RE-ENCRYPTION KEY STORAGE UNIT
23 RE-ENCRYPTION PROCESSING UNIT
24 ENCRYPTED DATA STORAGE UNIT
30 RECEIVER DEVICE
31 RECEIVER-USE KEY GENERATING UNIT
32 RECEIVER-USE PRIVATE KEY STORAGE UNIT
33 SERVER-USE KEY GENERATING UNIT
34 RE-ENCRYPTION KEY GENERATING UNIT
35 DECODING PROCESSING UNIT
36 DATA OUTPUT UNIT

(57) Abstract: From a transmission device, a receiving means receives server-use encrypted data obtained by encrypting data using a server-use public key. A re-encryption key storage means stores a re-encryption key used for re-encrypting server-use encrypted data into receiver-use encrypted data obtained by encrypting the data using a receiver-use public key different from the server-use public key. A re-encryption means uses the re-encryption key stored in the re-encryption key storage means to re-encrypt the received server-use encrypted data into receiver-use encrypted data. A transmission means transmits the re-encrypted receiver-use encrypted data to the receiver device.

(57) 要約: 受信手段は、サーバ用公開鍵を用いてデータを暗号化することによって得られるサーバ用暗号化データを送信者装置から受信する。再暗号化鍵格納手段は、サーバ用暗号化データを、サーバ用公開鍵とは異なる受信者用公開鍵を用いてデータを暗号化することによって得られる受信者用暗号化データに再暗号化するために用いられる再暗号化鍵を格納する。再暗号化手段は、再暗号化鍵格納手段に格納されている再暗号化鍵を用いて、受信されたサーバ用暗号化データを受信者用暗号化データに再暗号化する。送信手段は、再暗号化された受信者用暗号化データを受信者装置に送信する。

WO 2012/111714 A1

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)）