

(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
2013年5月16日(16.05.2013)



(10) 国際公開番号

WO 2013/069505 A1

- (51) 国際特許分類:
H04L 9/14 (2006.01) G09C 1/00 (2006.01)
- (21) 国際出願番号: PCT/JP2012/078028
- (22) 国際出願日: 2012年10月30日(30.10.2012)
- (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 2011-245618 2011年11月9日(09.11.2011) JP
- (71) 出願人: 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: 総田 佑樹 (KASEDA, Yuki); 〒1056691 東京都港区芝浦一丁目1番1号 東芝ソリューション株式会社 技術企画部 知的財産担当内 Tokyo (JP). 吉田 琢也 (YOSHIDA, Takuya); 〒1056691 東京都港区芝浦一丁目1番1号 東芝ソリューション株式会社 技術企画部 知的財産

担当内 Tokyo (JP). 藤井 吉弘 (FUJII, Yoshihiro); 〒1056691 東京都港区芝浦一丁目1番1号 東芝ソリューション株式会社 技術企画部 知的財産担当内 Tokyo (JP). 阿部 真吾 (ABE, Shingo); 〒1056691 東京都港区芝浦一丁目1番1号 東芝ソリューション株式会社 技術企画部 知的財産担当内 Tokyo (JP). 山田 正隆 (YAMADA, Masataka); 〒1056691 東京都港区芝浦一丁目1番1号 東芝ソリューション株式会社 技術企画部 知的財産担当内 Tokyo (JP).

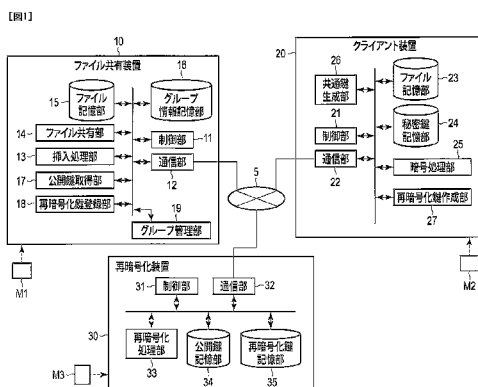
- (74) 代理人: 蔵田 昌俊, 外 (KURATA, Masatoshi et al.); 〒1050001 東京都港区虎ノ門1丁目12番9号 鈴榮特許総合事務所内 Tokyo (JP).

- (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, BN, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL,

[続葉有]

(54) Title: RE-ENCRYPTION SYSTEM, RE-ENCRYPTION DEVICE, AND PROGRAM

(54) 発明の名称: 再暗号化システム、再暗号化装置及びプログラム



- 10... FILE-SHARING DEVICE
11, 21, 31... CONTROL UNIT
12, 22, 32... COMMUNICATION UNIT
13... INSERTION PROCESSING UNIT
14... FILE-SHARING UNIT
15, 23... FILE STORAGE UNIT
16... GROUP INFORMATION STORAGE UNIT
17... PUBLIC KEY ACQUISITION UNIT
18... RE-ENCRYPTION KEY REGISTRATION UNIT
19... GROUP MANAGEMENT UNIT
20... CLIENT DEVICE
24... PRIVATE KEY STORAGE UNIT
25... CRYPTOGRAPHIC PROCESSING UNIT
26... PUBLIC KEY GENERATION UNIT
27... RE-ENCRYPTION KEY GENERATION UNIT
30... RE-ENCRYPTION DEVICE
33... RE-ENCRYPTION PROCESSING UNIT
34... PUBLIC KEY STORAGE UNIT
35... RE-ENCRYPTION KEY STORAGE UNIT

(57) Abstract: An embodiment of this re-encryption system is equipped with a file-sharing device and a re-encryption device. Upon receiving a file request from a client device, the file-sharing device obtains a first encrypted file on the basis of a file name contained in the file request, and transmits a re-encryption request, which includes the first encrypted file, to the re-encryption device. The re-encryption device re-encrypts the first encrypted file in the re-encryption request into a second encrypted file on the basis of a re-encryption key, and transmits the second encrypted file to the file-sharing device. The file-sharing device transmits the second encrypted file to the client device. The client device decrypts the second encrypted file received from the file-sharing device on the basis of a private key that corresponds to a public key of the member in order to obtain the file.

(57) 要約: 実施形態の再暗号化システムは、ファイル共有装置及び再暗号化装置を備えている。前記ファイル共有装置は、ファイル要求を前記クライアント装置から受けると、前記ファイル要求内のファイル名に基づいて第1暗号化ファイルを取得し、前記第1暗号化ファイルを含む再暗号化要求を前記再暗号化装置に送信する。前記再暗号化装置は、前記再暗号化鍵に基づいて前記再暗号化要求内の第1暗号化ファイルを前記第2暗号化ファイルに再暗号化し、前記第2暗号化ファイルを前記ファイル共有装置に送信する。前記ファイル共有装置は、当該第2暗号化ファイルを前記クライアント装置に送信する。前記クライアント装置は、前記ファイル共有装置から受けた第2暗号化ファイルを前記メンバの公開鍵に対応する秘密鍵に基づいて復号することにより、前記ファイルを得る。



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, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, 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))