(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 2012/111713 A1

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

(21) 国際出願番号: PCT/JP2012/053546

(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 2011-032078 2011 年 2 月 17 日(17.02.2011) 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]. 藤井 吉弘 **(FUJII, Yoshihiro)** [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, 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).

[続葉有]

(54) **Title**: KEY MANAGEMENT SYSTEM

(54) 発明の名称 : 鍵管理システム

[図1]

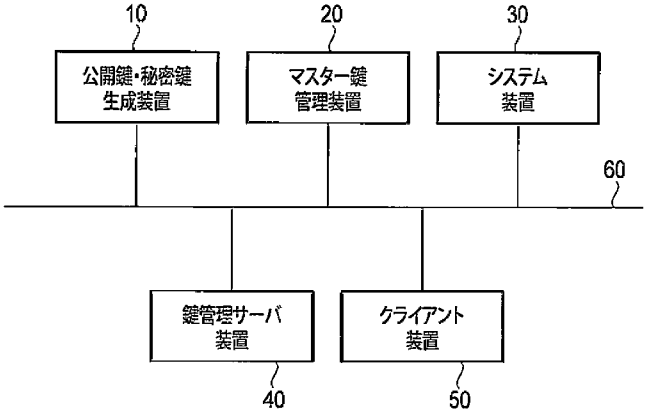

FIG. 1:
10 PUBLIC KEY / PRIVATE KEY GENERATION DEVICE
20 MASTER KEY MANAGEMENT DEVICE
30 SYSTEM DEVICE
40 KEY MANAGEMENT SERVER DEVICE
50 CLIENT DEVICE

(57) **Abstract**: A master key management device includes a re-encryption key generation means which, using a first private key and a third public key stored in a first storage means, generates a re-encryption key used to re-encrypt a second private key, which is encrypted with a first public key stored in a second storage means, into a second private key encrypted with the third public key. A key management server device includes: a receiving means which, in a state in which the master key management device and the key management server device are connected, receives from said master key management device a re-encryption key generated by the re-encryption key generation means; and a third storage means for storing the re-encryption key received by the receiving means. The connection between the master key management device and the key management server device is cut after the re-encryption key is stored in the third storage means.

(57) 要約: マスター鍵管理装置は、第１の記憶手段に記憶されている第１の秘密鍵および３の公開鍵を用いて、第２の記憶手段に記憶されている第１の公開鍵で暗号化された第２の秘密鍵を第３の公開鍵で暗号化された第２の秘密鍵に再暗号化するために用いられる再暗号化鍵を生成する再暗号化鍵生成手段を含む。鍵管理サーバ装置は、マスター鍵管理装置と鍵管理サーバ装置とが接続された状態で再暗号化鍵生成手段によって生成された再暗号化鍵を当該マスター鍵管理装置から受信する受信手段と、受信手段によって受信された再暗号化鍵を記憶する第３の記憶手段とを含む。マスター鍵管理装置と鍵管理サーバ装置との接続は、再暗号化鍵が第３の記憶手段に記憶された後に切断される。

WO 2012/111713 A1