(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
2007 年1 月4 日 (04.01.2007)

PCT

(10) 国際公開番号
WO 2007/001075 A1

(51) 国際特許分類:
*H04L 9/06* (2006.01) *H04L 9/14* (2006.01)

(21) 国際出願番号: PCT/JP2006/313186

(22) 国際出願日: 2006 年6 月27 日 (27.06.2006)

(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2005-190803 2005 年6 月29 日 (29.06.2005) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社エヌクリプト (N-CRYPT, INC.) [JP/JP]; 〒5128044 三重県四日市市中村町２２９３番地１ Mie (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 中村 貴利 (NAKAMURA, Takatoshi) [JP/JP]; 〒5128044 三重県四日市市中村町２２９３番地１ 株式会社エヌクリプト内 Mie (JP).

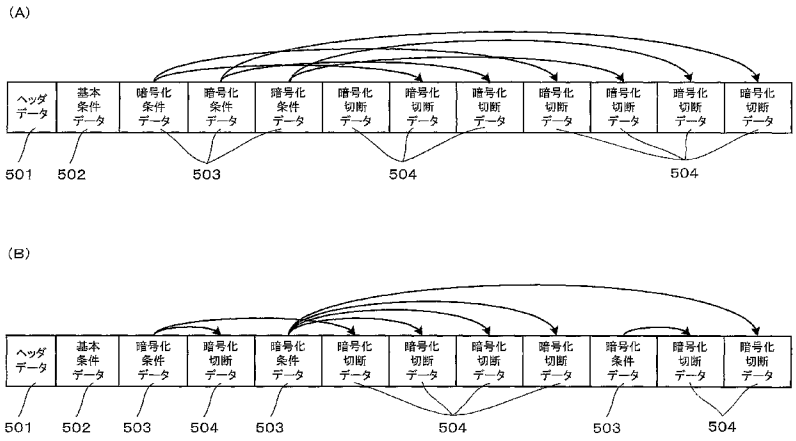
(74) 代理人: 鈴木 正剛, 外 (SUZUKI, Seigoh et al.); 〒1050014 東京都港区芝二丁目２９番１０号 パシフィックシティ芝ビル６階 Tokyo (JP).

(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, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH,

[続葉有]

(54) **Title:** ENCRYPTION DEVICE, ENCRYPTION METHOD, DECRYPTION DEVICE, DECRYPTION METHOD, AND DATA STRUCTURE

(54) **発明の名称:** 暗号化処理装置、暗号化方法、復号化処理装置、復号化方法、及びデータ構造




(57) **Abstract:** It is possible to perform encryption by setting various decryption conditions. Encrypted data obtained by encryption data to be processed includes header data (501), basic condition data (502), encrypted condition data (503), and encrypted cut data (504). The basic condition data (502) contains data on the condition for allowing or inhibiting decryption of the encrypted condition data (503). In the decryption device, only the encrypted condition data which is allowed to be decrypted by the basic condition data (502) is decrypted into condition data. The condition data contains data on the condition for allowing or inhibiting decryption of the encrypted cut data. In the decryption device, only the encrypted cut data (504) allowed to be decrypted by the condition data (503) is decrypted.

(57) 要約: 復号化の条件を多様に設定して暗号化を行えるようにする。 処理対象データを暗号化して得られる暗号化データは、ヘッダデータ５０１、基本条件データ５０２、暗号化条件データ５０３、暗号化切断データ５０４を有する。基本条件データ５０２は、暗号化条件データ５０３の復号化を許容又は禁止するための条件についてのデータを含んで

[続葉有]

WO 2007/001075 A1

PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SY, 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, 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, LV, 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。

いる。復号化処理装置では、基本条件データ５０２で復号化が認められた暗号化条件データのみが復号化されて条件データとされる。条件データは、暗号化切断データの復号化を許容又は禁止するための条件についてのデータを含んでいる。復号化処理装置では、条件データ５０３で復号化が認められた暗号化切断データ５０４のみが復号化される。