

(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
2016年3月31日(31.03.2016)



(10) 国際公開番号

WO 2016/047110 A1

- (51) 国際特許分類:
H04L 9/36 (2006.01) H04L 9/10 (2006.01)
G06F 21/56 (2013.01)
- (21) 国際出願番号: PCT/JP2015/004742
- (22) 国際出願日: 2015年9月17日(17.09.2015)
- (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 2014-195179 2014年9月25日(25.09.2014) JP
- (71) 出願人: 日本電気株式会社(NEC CORPORATION)
[JP/JP]; 〒1088001 東京都港区芝五丁目7番1号
Tokyo (JP).
- (72) 発明者: 山根 匡人(YAMANE, Masato); 〒1088001
東京都港区芝五丁目7番1号日本電気株式会
社内 Tokyo (JP). 芦野 佑樹(ASHINO, Yuki); 〒
1088001 東京都港区芝五丁目7番1号日本電
気株式会社内 Tokyo (JP). 渡部 正文(WATANABE,
Masafumi); 〒1088001 東京都港区芝五丁目7番1
号日本電気株式会社内 Tokyo (JP).
- (74) 代理人: 下坂 直樹(SHIMOSAKA, Naoki); 〒
1088001 東京都港区芝五丁目7番1号日本電
気株式会社内 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,
IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR,
LS, 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, SA, 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, ST, 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, KM,
ML, MR, NE, SN, TD, TG).

[続葉有]

(54) Title: ANALYSIS SYSTEM, ANALYSIS DEVICE, ANALYSIS METHOD, AND RECORDING MEDIUM HAVING ANALYSIS PROGRAM RECORDED THEREIN

(54) 発明の名称: 解析システム、解析装置、解析方法、及び、解析プログラムが記録された記録媒体

[図17]

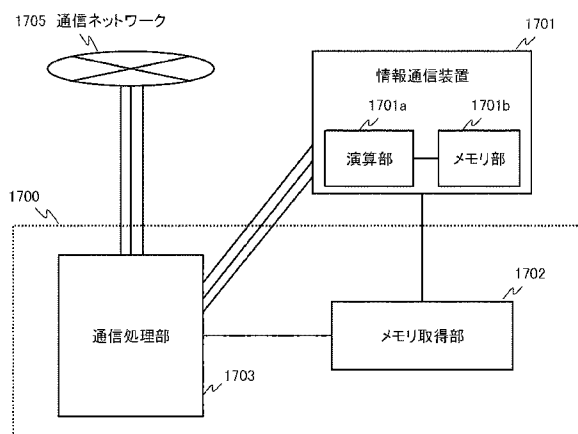


FIG. 17:
1701 Information communications device
1701a Calculation unit
1701b Memory unit
1702 Memory acquisition unit
1703 Communications processing unit
1705 Communications network

(57) Abstract: An analysis system that obtains data including an encryption key relating to encrypted communications executed between an information communications device and a communications network, from a memory space held by the information communications device. The analysis system comprises: a memory acquisition unit capable of obtaining at least part of the data held in the memory unit, from the information communications device having a calculation unit and a memory unit; and a communications processing unit that determines whether or not key data is held in the memory unit, on the basis of communications data sent and received between the information communications device and the communications network in accordance with an encrypted communications protocol, and instructions the memory acquisition unit to obtain data held in the memory unit, on the basis of the determination results, said key data including the encryption key used in encryption processing in the encrypted communications protocol.

(57) 要約: 情報通信装置と、通信ネットワークとの間で実行される暗号通信に関する暗号鍵を含むデータを、当該情報通信装置が保持するメモリ空間から取得する。解析システムは、演算部とメモリ部とを有する情報通信装置から、上記メモリ部に保持されたデータの少なくとも一部を取得可能なメモリ取得部と、上記情報通信

装置と、通信ネットワークとの間で暗号通信プロトコルに従って送受信される通信データに基づいて、当該暗号通信プロトコルにおける暗号処理に用いられる暗号鍵を含む鍵データが上記メモリ部に保持されているか否かを判定し、当該判定した結果に基づいて、上記メモリ取得部に対して上記メモリ部に保持されたデータの取得を指示する通信処理部と、を備える。

添付公開書類:

— 国際調査報告 (条約第 21 条(3))