

(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)



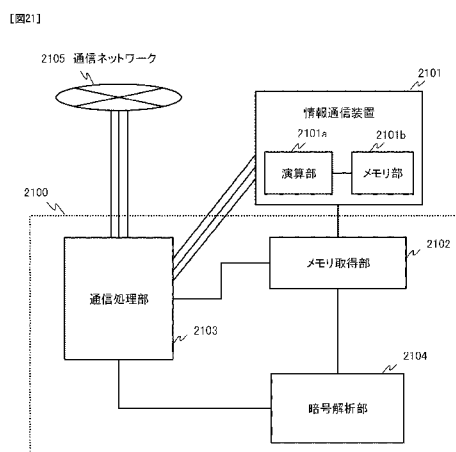
(10) 国際公開番号

WO 2016/047111 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/JP2015/004744
- (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 2014-195178 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).
- 添付公開書類:
— 国際調査報告 (条約第21条(3))

(54) Title: ANALYSIS SYSTEM, ANALYSIS DEVICE, ANALYSIS METHOD, AND STORAGE 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憶媒体



2101... INFORMATION COMMUNICATIONS DEVICE
2101a... CALCULATION UNIT
2101b... MEMORY UNIT
2102... MEMORY ACQUISITION UNIT
2103... COMMUNICATIONS PROCESSING UNIT
2104... ENCRYPTION ANALYSIS UNIT
2105... COMMUNICATIONS NETWORK

(57) Abstract: In order to execute specific processing in accordance with communications data sent and received between an analysis-target device and a communications network, using an encrypted communications protocol, this analysis system comprises: a memory acquisition unit that obtains data held in a memory unit, from an information communications device having a calculation unit and the memory unit; a communications processing unit that instructs the memory acquisition unit to obtain data held in the memory unit, if a determination has been made that key data is held in the memory unit, said key data including an encryption key used in a prescribed encrypted communications protocol used between the information communications device and the communications network; and an encryption analysis unit that extracts correct key data capable of deciphering the communications data, from among candidates for the key data extracted on the basis of data that exhibits characteristics of the key data from among the data held in the memory unit. The communications processing unit executes specific processing in accordance with the deciphered communications data.

(57) 要約: 解析対象装置と、通信ネットワークとの間で暗号通信プロトコルを用いて送受信される通信データに応じて、特定の処理を実行する。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を取得するメモリ取得部と、上記情報通信装置と、通信ネットワークとの間で用いられる特定の暗号通信プロトコルにおいて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と判定した場合に、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、当該メモリ部に保持されたデータから上記鍵データの特徴を表すデータに基づいて抽出した上記鍵データの候補の中から、通信データを解読可能な正しい鍵データを抽出する暗号解析部と、を備え、上記通信処理部は、解読された上記通信データに応じた特定の処理を実行する。

WO 2016/047111 A1