

(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
2021年12月9日(09.12.2021)



(10) 国際公開番号

WO 2021/245944 A1

- (51) 国際特許分類:
G06F 21/55 (2013.01) *G06F 21/56* (2013.01)
- (21) 国際出願番号: PCT/JP2020/022422
- (22) 国際出願日: 2020年6月5日(05.06.2020)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人: 富士通株式会社 (FUJITSU LIMITED)
[JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP).
- (72) 発明者: 乾 真季 (INUI, Maki); 〒2118588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 藤島 由紀 (FUJISHIMA, Yuki); 〒2118588 神奈川県

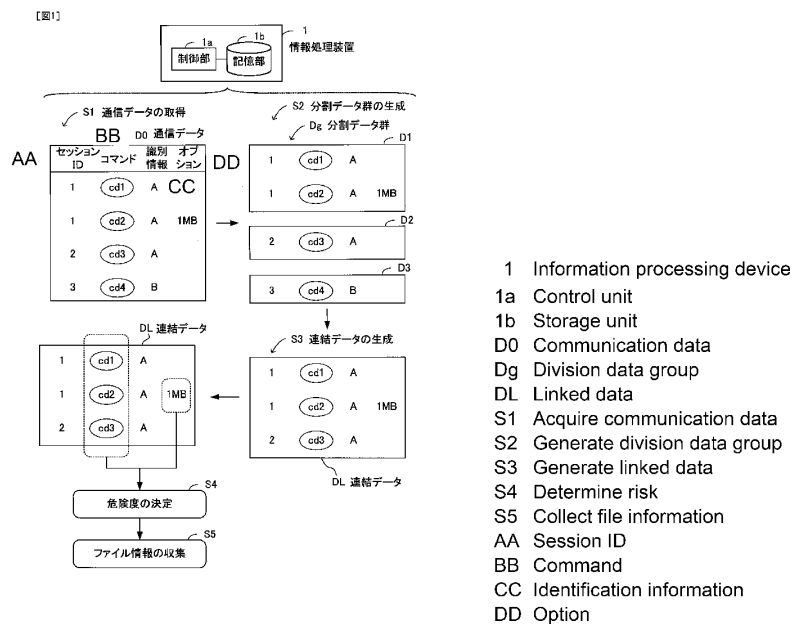
川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 及川 孝徳 (OIKAWA, Takanori); 〒2118588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP).

(74) 代理人: 特許業務法人扶桑国際特許事務所 (FUSO INTERNATIONAL PATENT FIRM); 〒1920082 東京都八王子市東町9番8号 八王子東町センタービル5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, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,

(54) Title: INFORMATION PROCESSING PROGRAM, INFORMATION PROCESSING METHOD, AND INFORMATION PROCESSING DEVICE

(54) 発明の名称: 情報処理プログラム、情報処理方法および情報処理装置



(57) Abstract: In the present invention, data corresponding to risk of communication is efficiently extracted. A control unit (11) determines risk levels of false session data (dp) and division session data (d3), and collects file information from between the false session data (dp) and the division session data (d3). In this case, since a file is not included in the division session data (d3) but a file is included in the false session data (dp), the file information is collected from the file included in the false session data (dp). In addition, an a.exe file is included in the false session data (dp), and the a.exe file

[続葉有]

HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH,
KN, KP, KR, KW, 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,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, 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))

is associated with a schtasks command having a risk level of 3. Therefore, the control unit (11) collects, from the a.exe file, meta-information, a file hash value, and a file body as the file information.

(57) 要約: 通信の危険度に応じたデータを効率よく抽出する。制御部(11)は、疑似セッションデータ(d p)および分割セッションデータ(d 3)の危険度レベルを決定し、疑似セッションデータ(d p)および分割セッションデータ(d 3)のうちからファイル情報を収集する。この場合、分割セッションデータ(d 3)にはファイルは含まれず、疑似セッションデータ(d p)にはファイルが含まれているため、疑似セッションデータ(d p)に含まれるファイルからファイル情報が収集される。また、疑似セッションデータ(d p)には、a.exeファイルが含まれており、また、a.exeファイルは、危険度レベルが3のschtasksコマンドに紐づけられている。このため、制御部(11)は、a.exeファイルからメタ情報、ファイルハッシュ値およびファイル本体をファイル情報として収集する。