(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
2005 年5 月26 日 (26.05.2005)

PCT

(10) 国際公開番号
WO 2005/048114 A1

(51) 国際特許分類[7]: G06F 12/14, 13/00, 15/00

(21) 国際出願番号: PCT/JP2004/009860

(22) 国際出願日: 2004 年7 月9 日 (09.07.2004)

(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 2003-387212
2003 年11 月17 日 (17.11.2003) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社インテリジェントウェイブ (INTELLIGENT WAVE INC.) [JP/JP]; 〒1040033 東京都中央区新川一丁目２１番２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): 青木修 (AOKI, Osamu) [JP/JP]; 〒1660004 東京都杉並区阿佐ヶ谷南１−１２−５ クリオレミントンハウス阿佐ヶ谷１４０３ Tokyo (JP). 白杉政晴 (SHIRASUGI, Masaharu) [JP/JP]; 〒1350043 東京都江東区塩浜１丁目４番３３−１７２９号 Tokyo (JP). 小出研一 (KOIDE, Kenichi) [JP/JP]; 〒1340085 東京都江戸川区南葛西２−１５−５ 第二アライハイツ２０３ Tokyo (JP). 河野裕晃 (KAWANO, Hiroaki) [JP/JP]; 〒2610003 千葉県千葉市美浜区高浜５−２１−６ Chiba (JP).

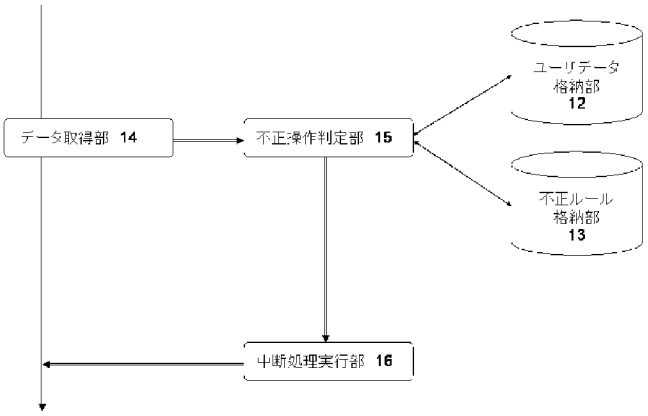
(74) 代理人: 土生哲也 (HABU, Tetsuya); 〒1020084 東京都千代田区二番町４番地５ 住友不動産麹町ビル２号館 土生特許事務所 Tokyo (JP).

(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,

[続葉有]

(54) Title: INVALIDITY MONITORING PROGRAM, INVALIDITY MONITORING METHOD, AND INVALIDITY MONITORING SYSTEM

(54) 発明の名称: 不正監視プログラム、不正監視の方法及び不正監視システム



12...USER DATA STORAGE UNIT
14...DATA ACQUISITION UNIT
15...INVALID OPERATION DETERMINATION UNIT
13...INVALIDITY RULE STORAGE UNIT
16...INTERRUPTION PROCESSING EXECUTION UNIT

(57) Abstract: For use in monitoring invalid data that causes a computer to execute an invalid operation there is provided, an invalidity monitoring program that can monitor input/output data sent to and received from not only a network but also an externally connected device and that allows a user to set a variety of invalidity determination rules and apply an efficient rule. A data acquisition unit (14) acquires input/output data, flowing on a network or an externally connected bus, and the ID of an operator. An invalid operation determination unit (15) determines whether an operation is invalid by acquiring attribute information on a user, corresponding to the ID, from a user data storage unit (12), by referencing a rule, corresponding to the attribute information, from the rules stored in an invalidity rule storage unit (13) and defined for the respective user attributes and, in addition, by referencing a rule that generally determines an operation as invalid regardless of the attributes stored in the invalidity rule storage unit (13). If it is found that the operation is invalid, an interruption processing execution unit (16) stops the processing to be executed by the operation.

[続葉有]

WO 2005/048114 A1

DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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, IT, LU, 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。

(57) 要約:

コンピュータに不正な操作を実行させる不正データの監視において、ネットワークのみでなく外部接続デバイスとの間の入出力データの監視が可能であり、かつ不正判定のための多様なルール設定と効率的なルールの適用が可能な不正監視プログラムを提供する。

データ取得部１４は、ネットワーク又は外部接続バスを流れる入出力データと操作者のＩＤを取得する。不正操作判定部１５においては、ユーザデータ格納部１２から当該ＩＤに対応するユーザの属性情報を取得して、不正ルール格納部１３に格納されたユーザの属性毎に定められたルールから当該属性情報に対応するルールを参照し、さらに不正ルール格納部１３に格納された属性に関わらず一般的に不正と判定すべきルールを参照して、不正の判定を行う。不正な操作であると判定されると、中断処理実行部１６において当該操作により実行される処理を停止させる。