

(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
2013年5月16日(16.05.2013)



(10) 国際公開番号
WO 2013/069758 A1

- (51) 国際特許分類:
G06F 21/56 (2013.01)
- (21) 国際出願番号: PCT/JP2012/079084
- (22) 国際出願日: 2012年11月9日(09.11.2012)
- (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 2011-246193 2011年11月10日(10.11.2011) JP
- (71) 出願人(米国を除く全ての指定国について): 株式会社セキュアブレイン(SECUREBRAIN CORPORATION) [JP/JP]; 〒1020083 東京都千代田区麹町2-6-7 麹町RKビル Tokyo (JP).
- (72) 発明者: および
- (71) 出願人(米国についてのみ): 山村 元昭(YAMAMURA, Motoaki) [JP/JP]; 〒1020083 東京都千代田区麹町2-6-7 麹町RKビル 株式

会社セキュアブレイン内 Tokyo (JP). 西田 雅太(NISHIDA, Masata) [JP/JP]; 〒1138654 東京都千代田区麹町2-6-7 麹町RKビル 株式会社セキュアブレイン内 Tokyo (JP).

(74) 代理人: 新保 斉(SHIMBO Itsuki); 〒1010065 東京都千代田区西神田2丁目5番9号 HIビル4階 Tokyo (JP).

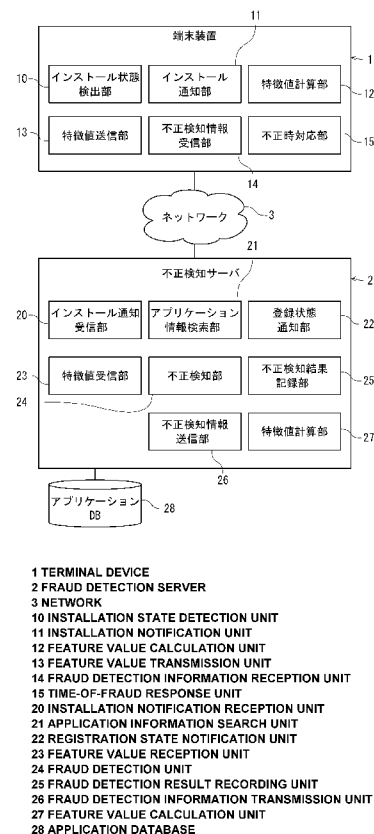
(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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.

[続葉有]

(54) Title: UNAUTHORIZED APPLICATION DETECTION SYSTEM AND METHOD

(54) 発明の名称: 不正アプリケーション検知システム及び、方法

【図1】



(57) Abstract: [Problem] The objective of the present invention is to provide technology for detecting unauthorized operability of an application upon a terminal device using a low load as well as to increase accuracy of detection; in particular, to provide technology capable of performing detection even regarding an application which has been deleted upon the terminal device. [Solution] A change in the installation state of an application in a terminal device is detected, upon which information for the installed application is reported to a fraud detection server device so as to be recorded. In addition, a predetermined feature value based on an application file or component files configuring a package of the application is reported to the fraud detection server device. The feature value is associated with the unauthorized operability of the application so as to be registered in an application database, whereupon if unauthorized operability of the application is detected, fraud detection information is transmitted to the terminal device. When the fraud detection information is received, predetermined response processing is performed upon the terminal device.

(57) 要約: 【課題】端末装置上でのアプリケーションの不正動作性を低負荷で検知すると共に、検知精度を高める技術を提供することを目的とする。特に、端末装置上で削除されたアプリケーションについても検知することのできる技術を提供すること。【解決手段】端末装置におけるアプリケーションのインストール状態が変化したことを検出して該インストールされたアプリケーション情報を、不正検知サーバ装置に通知して記録すると共に、アプリケーションファイル、又は当該アプリケーションのパッケージを構成する要素ファイルに基づく所定の特徴値を不正検知サーバ装置に通知する。特徴値と、当該アプリケーションの不正動作性とは関連付けてアプリケーションデータベースに登録し、当該アプリケーションの不正動作性が検知された場合に不正検知情報を該端末装置に送信する。不正検知情報の受信時には、端末装置上で所定の対応処理を行う。



(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, 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, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告 (条約第 21 条(3))