

(43) 国際公開日
2015 年 8 月 20 日(20.08.2015)



(10) 国際公開番号

WO 2015/121923 A1

- (51) 国際特許分類:
G06F 21/55 (2013.01)

(21) 国際出願番号: PCT/JP2014/053179

(22) 国際出願日: 2014 年 2 月 12 日(12.02.2014)

(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: 三菱電機株式会社(MITSUBISHI ELECTRIC CORPORATION) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目 7 番 3 号 Tokyo (JP). 三菱電機インフォメーションネットワーク株式会社(MITSUBISHI ELECTRIC INFORMATION NETWORK CORPORATION) [JP/JP]; 〒1080023 東京都港区芝浦四丁目 6 番 8 号 Tokyo (JP).

(72) 発明者: 砂田 英之(SUNADA, Hideyuki); 〒1008310 東京都千代田区丸の内二丁目 7 番 3 号 三菱電機株式会社内 Tokyo (JP). 長田 康志(NAGATA, Yasushi); 〒1080023 東京都港区芝浦四丁目 6 番 8 号 三菱電機インフォメーションネットワーク株式会社内 Tokyo (JP).

(74) 代理人: 溝井 章司, 外(MIZOI, Shoji et al.); 〒2470056 神奈川県鎌倉市大船二丁目 1 7 番 1 〇

号 N T A 大船ビル 3 階 溝井国際特許事務所 Kanagawa (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, 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, 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, SZ, TZ, UG, ZM, ZW), ユーロパ (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).

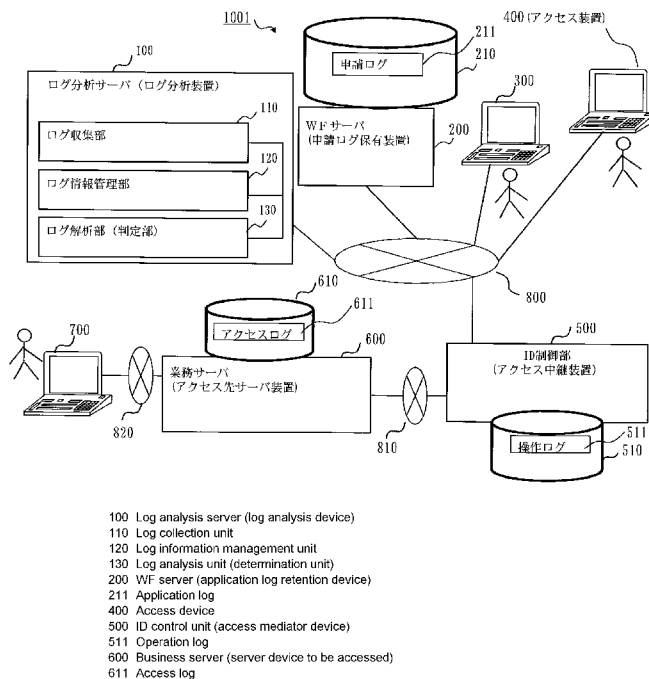
添付公開書類:
— 国際調査報告 (条約第 21 条(3))

添付公開書類:

— 國際調查報告（條約第 21 條(3)）

(54) Title: LOG ANALYSIS DEVICE, UNAUTHORIZED ACCESS AUDITING SYSTEM, LOG ANALYSIS PROGRAM, AND LOG ANALYSIS METHOD

(54) 発明の名称：ログ分析装置、不正アクセス監査システム、ログ分析プログラム及びログ分析方法



(57) Abstract: A log collection unit (110) of a log analysis server (100) collects an application log (211) from a WF server (200), which retains the application log (211) therein, further collects an operation log (511) from an ID control unit (500), through which an operator terminal (400) accesses a business server (600) and which enters operation records in the operation log (511), with each operation record indicating the state of an access to the business server (600), and further collects an access log (611) from the business server (600), which enters access records in the access log (611), with each access record indicating the state of an access to the business server (600). On the basis of the application log (211), the operation log (511), and the access log (611) collected by the log collection unit (110), a log analysis unit (130) determines whether the access state logged in each access record is authorized.

(57) 要約: ログ分析サーバ100のログ収集部110は、WFサーバ200の申請ログ211をWFサーバ200から収集し、運用者端末400から業務サーバ600へアクセスを中継すると共に業務サーバ600へのアクセス状態を操作レコードとして操作ログ511に記録するID制御部500から操作ログ511を収集し、アクセスされたアクセス状態をアクセスレコードとしてアクセスログ611に記録する業務サーバ600からアクセスログ611を収集

する。ログ分析部 130 は、ログ収集部 110 が収集した申請ログ 211、操作ログ 511、及びアクセスログ 611 に基づいて、アクセスレコードとして記録されたアクセス状態が正規のアクセスかどうかを判定する。

WO 2015/121923 A1