

(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
2015 年 10 月 8 日(08.10.2015)



(10) 国際公開番号

WO 2015/151667 A1

- (51) 国際特許分類:
G06F 21/55 (2013.01) H04L 12/70 (2013.01)
G06Q 50/10 (2012.01)
- (21) 国際出願番号: PCT/JP2015/055613
- (22) 国際出願日: 2015 年 2 月 26 日(26.02.2015)
- (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 2014-074606 2014 年 3 月 31 日(31.03.2014) JP
- (71) 出願人: 株式会社ラック(LAC CO., LTD.) [JP/JP];
〒1020093 東京都千代田区平河町 2 丁目 1 6 番
1 号 平河町森タワー Tokyo (JP).
- (72) 発明者: 土屋 和英(TSUCHIYA Kazuhide); 〒
1020093 東京都千代田区平河町 2 丁目 1 6 番 1
号 平河町森タワー 株式会社ラック内 Tokyo
(JP). 阿部 正道(ABE Masamichi); 〒1020093 東京
都千代田区平河町 2 丁目 1 6 番 1 号 平河町森

タワー 株式会社ラック内 Tokyo (JP). 影山 徹
哉(KAGEYAMA Tetsuya); 〒1020093 東京都千代田
区平河町 2 丁目 1 6 番 1 号 平河町森タワー
株式会社ラック内 Tokyo (JP). 川口 洋
(KAWAGUCHI Hiroshi); 〒1020093 東京都千代田
区平河町 2 丁目 1 6 番 1 号 平河町森タワー
株式会社ラック内 Tokyo (JP). 鷺尾 浩之(WASH-
IO Hiroyuki); 〒1020093 東京都千代田区平河町 2
丁目 1 6 番 1 号 平河町森タワー 株式会
社ラック内 Tokyo (JP). 馬着 篤(UMAKI Atsushi); 〒
1020093 東京都千代田区平河町 2 丁目 1 6 番 1
号 平河町森タワー 株式会社ラック内 Tokyo
(JP). 塩出 一平(SHIODE Ipppei); 〒1020093 東京
都千代田区平河町 2 丁目 1 6 番 1 号 平河町森タ
ワー 株式会社ラック内 Tokyo (JP). 木村 雅弘
(KIMURA Masahiro); 〒1020093 東京都千代田区平
河町 2 丁目 1 6 番 1 号 平河町森タワー 株式
会社ラック内 Tokyo (JP). 藤本 博史(FUJIMOTO
Hiroshi); 〒1020093 東京都千代田区平河町 2 丁目
1 6 番 1 号 平河町森タワー 株式会社ラック
内 Tokyo (JP). 武智 洋(TAKECHI Hiroshi); 〒

[続葉有]

(54) Title: LOG ANALYSIS SYSTEM

(54) 発明の名称 : ログ分析システム

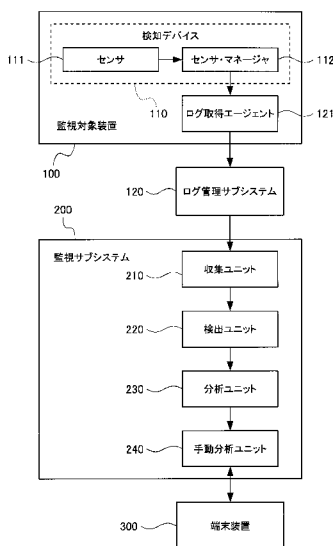


FIG. 1:
100 Device to be monitored
110 Detection device
111 Sensor
112 Sensor manager
120 Log management sub-system
121 Log acquisition agent
200 Monitoring sub-system
210 Collection unit
220 Detection unit
230 Analysis unit
240 Manual analysis unit
300 Terminal device

(57) Abstract: In the present invention, a processing device of a log analysis system is provided with: a first processing unit that normalizes a detection log acquired by an acquisition device and outputs the results divided into preset monitoring units; a second processing unit that adds common information based on preset rules to the detection logs for each monitoring unit output from the first processing unit, aligns the information granularity on the basis of the contents of the detection logs and the common information, and outputs the results as analysis unit information; a third processing unit that accumulates on the basis of preset rules the analysis unit information output from the second processing unit and uses the result as a candidate for an event to be detected, determines on the basis of preset rules whether or not the candidate for an event to be detected is a process to be detected having a specific nature, and outputs the candidate for an event to be detected and the determination results; and a fourth processing unit that outputs in a preset output format the candidate for an event to be detected and the determination results, both of which were output from the third processing unit.

(57) 要約: ログ分析システムの処理装置は、取得装置により取得された検知ログを正規化し、予め設定された監視対象単位ごとに振り分けて出力する第1処理ユニットと、前記第1処理ユニットから出力された前記監視対象単位ごとの検知ログに対して、予め設定された規則に基づく共通情報を付加し、当該検知ログの内容および当該共通情報に基づいて情報粒度を揃え、分析単位情報として出力する第2処理ユニットと、前記第2処理ユニットから出力された前記分析単位情報を、予め設定された規則に基づいて集積して検出対象の事象の候補とし、予め設定された規則に基づいて当該検出対象の事象の候補が特定の性質を有する検知対象処理かどうかを判断し、当該検出対象の事象の候補および判断結果を出力する第3処理ユニットと、前記第3処理ユニットから出力された前記検出対象の事象の候補および前記判断結果を、予め設定された出力形式で出力する第4処理ユニットとを備える。



1020093 東京都千代田区平河町 2 丁目 1 6 番 1
号 平河町森タワー 株式会社ラック内 Tokyo
(JP).

(74) 代理人: 棚井 澄雄, 外(TANAI Sumio et al.); 〒
1006620 東京都千代田区丸の内一丁目 9 番 2 号
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, 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))