

TITLE

DEVICE FOR OUTPUTTING INFORMATION FOR INSPECTION AND FOR ANALYZING SYSTEM TENDENCY THROUGH ANALYSIS AND TRANSLATION OF COMPUTER OPERATION LOG

TECHNICAL FIELD

[0001] The invention relates to a technical device which analyzes and translates the log information outputted by a computer device when it is used, translates the operation or operating record of the computer device as an object into a report of plain nature language for outputting and providing improvement proposal.

BACKGROUND

[0002] The computer device has the function of recording the log file which includes the operations of all software in the operating system (OS) of the computer device. However, the information of recording all operation within the OS becomes large and complicated, which is difficult to be interpreted by human.

[0003] In addition, it is required to rapidly perform the analysis for the monitoring of the person information protection law or the cause of information leakage by carrying out information illegally.

[0004] Although the log which records various operations of the computer could be outputted by the OS or its operating software, as illustrated in the above [0002] paragraph, the information is large, complicated and difficult for people to interpret. Therefore, a technology for analyzing and translating the log file is required.

[0005] An improvement information is needed to analyze the stored log file, discover the improvement, and obtain the optimized method. Specifically, a technology is needed to

visualize the information of the file with access right but has not been accessed, the file has never been accessed by anyone, and the access-accumulated server. The technology could also perform the statistical analysis for the past information.

[0006] Regarding the prior art of the patent references 1~4, the communication traffic could be reduced by determining and extracting necessary log. It is still unavailable to further analyze the log so that everyone could easily understand which operation is performed in which method by who and when. Therefore, the information of the log file which is outputted by the computer cannot be utilized efficiently.

[0007] The technology can analyze the computer log file, translate its content into understandable nature language for people, and improve the current technology and application.

THE PRIOR ART

[0008] Patent Reference

Patent Reference 1: JP 2011-191823

Patent Reference 2: JP 2011-113443

Patent Reference 3: JP 2005-227846

Patent Reference 4: JP 2014-16758

SUMMARY OF THE INVENTION

THE PROBLEM TO BE SOLVED

[0009] Recently, regarding the events or accidents of the computer system, from the points of view of incident management or security management of the point of view of the developing Internet of Things (IoT), the necessity about analyzing the information which is needed by operations has increased for communication between objects efficiently and accurately.

[0010] However, although the computer system, the personal computer (smartphone, tablet, wearable device), the machine (industrial machine, general machine, vehicle), or other devices (appliances, furniture, architecture) are connected as IoT, all of the operations are recorded along the time axis mechanically with the status of the log information outputted by the type of machine. Therefore, the information amount is large, and the information which is meaningless for analyzing or tracking is even recorded. It becomes difficult to find out effective information.

[0011] As a result, it is very difficult to master a series of facts of operations, and large storage resource is also needed.

THE METHOD FOR SOLVING THE PROBLEM

[0012] The invention is utilized to realize the following procedure.

[0013] A mapping processing device is provided to determine the input from the service log, the application log, the system log, the monitoring log information and the event log data which are outputted by the computer system, the personal computer (smartphone, tablet, wearable device), the machine (industrial machine, general machine, vehicle), or other devices (furniture, architecture). The necessary items of the log information are extracted based on each user, server and object.

[0014] The arrangement of items after the output of the mapping processing of each user, server and object is linked to the combination pattern of n operation results which are predetermined at the rule master. The symbol of operation which are actually generated is tracked.

[0015] From the tracking result of each summary outputted by the pass 1 processing device, the identical operation of the constant time is compressed into one, and the output of the pass 1 processing device is organized into the type which is more readable.

[0016] For example, when read and write are generated at a short time, because read

does not mean much, it will be organized to a single write.

[0017] A series of processing results of the mapping processing device, the pre-pass processing device, the pass 1 processing device, the pass 2 processing device and the pass 3 processing device are inspected to perform the report, so that the event management or the security management could be performed efficiently and accurately. By utilizing the pass 4 processing device which translates the code or the binary data into the natural language, the pass 5 processing device, the pass 6 processing device and the pass 7 processing device which output the improvement information from the log information, further utilization for the log could be obtained.

THE EFFECT OF THE PRESENT INVENTION

[0018] The professional knowledge of user is not needed for the log information translation device and the log information analysis of the computer device of the invention. The log is easy to read for control the original operations, and the storage resource could be greatly reduced. The code or the binary data corresponding to the large amount of outputted detail could be translated into the natural language to perform the tendency analysis.

BRIEF DESCRIPTION OF DRAWINGS

[0019] FIG.1 is an overall composition schematic according to an embodiment of the invention.

[0020] FIG.2 is the schematic of mapping process.

[0021] FIG.3 is the schematic of the pre-pass 1.

[0022] FIG.4 is the schematic of the pass 1.

[0023] FIG.5 is the schematic of the pass 2.

[0024] FIG.6 is the schematic of the pass 3.

[0025] FIG.7 is the schematic of the pass 4.

[0026] FIG.8 is the schematic of the pass 5.

[0027] FIG.9 is the schematic of the pass 6.

[0028] FIG.10 is the schematic of the pass 7.

DETAILED DESCRIPTION

[0029] Embodiments

[0030] FIG.1 is an overall composition schematic according to an embodiment of the invention which accumulates the 111 log information outputted by the computer, compresses the accumulated log information, and translates the log information into the nature language which can be understood by human.

[0031] When the file 107X of the 104 server α is operated by the 101 user A, the file 108Y and the file 109Z of the 105 server β is operated by the 101 user A, the file 108Y and the file 109Z of the 105 server β is operated by the 102 user B, and the file 110W of the 106 server γ is operated by the 103 user C, the operating state of the computer is respectively outputted as the 111 log information by the computer 104 server α , the 105 server β and the 106 server γ .

[0032] The 113 translation server periodically accumulates the outputted log information by utilizing the internet, and combines into the 114 accumulation log information.

[0033] The overall composition schematic includes the 114 accumulation log information which is accumulated and read, the 116 mapping processing device performing translation with necessary data, the 117 pre-pass 1 processing device which performs the classification of the log pattern, the 118 pass 1 processing device which reorganizes the log, the 119 pass 2 processing device and the 120 pass 3 processing device which reorganize the translation so that the data amount is reduced from one in 1000th to one in 2000th through the 116 mapping processing device and the 120 pass 3 processing device, the 121 pass 4 processing device which performs translation to be the understandable nature language, the

122 pass 5 processing device which performs the evaluation of the access right of the user, the 123 pass 6 processing device which performs the output of improvement proposal information, and the 124 pass 7 processing device which outputs the loading statistical information of the server.

[0034] The names of each software and each device of the invention are illustrated below in association with the specific names by the inventor and the applicant.

[0035] Date And Time: The Date, clock, minute and second for the user to access the file.

[0036] User: The person who accesses the file, or the function having the account.

[0037] Object: The events related to the operation.

The accessed file or directory when the file is accessed.

[0038] Detail: The events related to the operation, which is the additional event of the data and time, the user and the object.

When the file access is AccessValue, the IP address of the object. When the file access is AccessValue, the session information and the IP address of the object.

[0039] AccessValue: The information of operation which determines the output of the symbol or the binary data.

[0040] Operation: The information of the file determined by the OS and the application program (such as logon, logoff, write, read).

[0041] Summary Table: Utilizing the combination of the user, server and object to be the table of the key, and storing the actual memory address.

[0042] Summary No: The unique address of the memory which is given by the summary.

[0043] Skip: Whether the determination information of each row of the log information outputted by the OS is needed or not.

[0044] Log Information: Including the operation records which are outputted by the

computer system, the personal computer, the smart phone, the tablet, the wearable device, the industrial machine, the general machine, the vehicle, the electronic device, the medical machine, the furniture, the architecture, or including the operation records of the application program log, the service log, the system log, the event log, the monitor log, the command information, the digital data.

[0045] Log Information Table: The information needed for analyzing the log information is converted to the analysis format and expanded on the table of the memory status.

[0046] System Log: Recording information of the initiation or end of the computer, logon or logoff of the manager, re-initiation, the obstacle of the hardware, the error generated by the kernel, the initiation or end of the server software, Daemon or the permanent program.

[0047] Access Control List: Recording the information of the access right for each person through the setting of the certification process system.

[0048] Control Information: The information of the operation, the summary, the Skip.

[0049] Event Log: Recording various events generated by the system when the composition changes or the obstacle occurs.

[0050] Monitoring Log: Recording the operation content based on the time sequence which is executed by the operator, the developer, and the user of the system.

[0051] Rule Master: Recording the rule of analyzing and determining the operations of each row of the log information based on the time sequence, and recording the required time for analysis on the rule which is called the Constant time.

[0052] Constant Time: The time recorded in the rule master which varies with each rule. It is the seconds required for each rule of the time definition of the security value at the rule master and the separation master for reorganizing the same operation when the various log information is analyzed by the inventor and the operations are performed during the n seconds.

[0053] Mechanical Language: The information which cannot be understood by human under the output status of the computer.

[0054] FIG.2 is the schematic of 116 mapping processing device of the present invention.

[0055] The 111 log information is accumulated by the network, outputted by the computer, and organized to become the 114 accumulation log information. The 114 accumulation log information is read with the analysis content to extract the items of the data and time, the user, the server, the object, and the detail content. The information setting region of the 211 operation, the 212 summary No, the 213 Skip could be confirmed. In addition, the items are extracted and expanded on the memory to search the 202 detail of the 201 operation master based on the search key of the 210 detail and set up the corresponding 203 operation on the 211 operation.

[0056] The information item which is required for analysis is selected from the object of the 114 accumulation log information. In the embodiment, the log information of the file server is made by utilizing each item of the 206 date and time, the 207 user, the 208 server, the 209 object and the 210 detail. The analysis of the file operation stored in the file server by the user is provided as the example.

[0057] When the analysis object is the power-saving car or industrial machine, the object is the data and time, the consumed energy during a constant time, the status of the energy-consuming machine (such as the spin number), the moving distance of the external environment (such as the temperature and the humidity), and the operating number.

[0058] Each item of the read 206 data and time, the 207 user, the 208 server, the 209 object and the 210 detail is setup in each item of the 204 log information table of the memory. The 210 detail is utilized to match the 202 detail of the 201 operation master, setup the matched 203 operation on the 211 operation and confirm the memory region of the 212 summary No. The default value of “FALSE” is set up at the 213 Skip item to conform the

memory region which could store the 214 number.

[0059] “FALUS” means that the information of each row of the 204 log information table is very important and will not be skipped.

[0060] In addition, when the 210 detail of the 201 operation master does not exist, it will not be the processing object, and the “TRUE” value is set up on the 204 log information table. The information registered on the 201 operation master is the information group which is composed by the information of the past experience and actual performance of the present invention.

[0061] Actually, when the file is erased by the computer, the read process is executed for the disk device. Afterwards, the file is erased by writing information into the disk device. As such, the human operation is not consistent with the computer operation. Therefore, it is important to analyze the actual operation of people.

[0062] FIG.3 is the schematic of the 117 pre-pass 1 processing device of the invention.

[0063] The overall combined 301 summary table is made from the 207 user, the 208 server and the 209 object on the 204 log information table. The symbol of the sequence No. is provided for each row of the 301 summary table on the memory.

[0064] The 207 user, the 208 server and the 209 object on the 204 log information table are matched to the 303 user, the 304 server and the 305 object of the 301 summary table of the identical object. The 302 summary No allocated at the 301 summary table is setup on the 212 summary No. item of the 204 log information table.

[0065] When there is no identical combination for matching the 207 user, the 208 server and the 209 object on the 204 log information table and the 303 user, the 304 server and the 305 object of the 301 summary table, the symbol of the sequence number is provided on the 302 summary No. and is set up. The combination of the 207 user, the 208 server and the 209 object is set up at the 303 user, the 304 server and the 305 object. The 301 summary table of

the total combination is made on the memory.

[0066] After the 301 summary table of the total combination is made, the 207 user, the 208 server and the 209 object on the 204 log information table are matched to the 303 user, the 304 server and the 305 object of the 301 summary table of the identical object. The 302 summary No. allocated at the 301 summary table is setup on the 212 summary No. item of the 204 log information table.

[0067] FIG.4 is the schematic of the pass 1 processing device of the invention.

[0068] The processing is started by the 204 log information table which is expanded on the memory.

[0069] The 212 summary No. is utilized to track the identical user, server and object through the rows. The emergence pattern of the 210 detail is mapped to the 401 rule master. When the emergence pattern is matched, and the 213 Skip of each row of the 204 log information table which is matched except the 404 basic sequence is updated to be "TRUE".

[0070] The processing is started by the 204 log information table which is expanded on the memory.

[0071] Because the 213 Skip of the 205 Seq# "1" is "FALSE", it becomes the processing object.

[0072] Because the 210 detail is "\$%#097", there is the same information 402ID "1" on the 404 basic sequence of the 401 rule master. Therefore, it is memorized.

[0073] When the same data "①" of the 212 summary No. is investigated, the same data "①" of the 212 summary No. of the 205 Seq# "2" could be investigated. Because the data of the 210 detail of the 205 Seq# "2" is "\$%#257445y7nc09yw983", it is the same data when comparing with the 406 sequence 1 of the 402ID "1". There is no data at the 407 sequence 2 of the 402ID "1", and the 405 constant time is "3", and the difference of 206 date and time is "0". Therefore, the 211 operation of the 205 Seq# "1" is determined to be read,

and the 211 operation becomes “read”.

[0074] When the 213 Skip is setup to be the stats of “FALSE”, the 213 Skip of the 205 Seq# “2” is set to be “TRUE”.

[0075] Afterwards, the pointer is incremented by 1. Because the 213 Skip of the 205 Seq# “2” is “TRUE”, it will not be the processing object, and the pointer is incremented by 1.

[0076] Because the 213 Skip of the 205 Seq# “3” is “FALSE”, it becomes the processing object.

[0077] Because the 210 detail is “\$%#38a2”eh48w”, there is the same information 402ID “2” on the 404 basic sequence of the 401 rule master. Therefore, it is memorized.

[0078] In the embodiment, when the same data “②” of the 212 summary No. is investigated, because there is merely the data “②” on the 212 summary No. of the 204 log information table of FIG.4, the 213 Skip is setup to be “FALSE” and the pointer is incremented by one.

[0079] Afterwards, because the 213 Skip of the 205 Seq# “4” is “FALSE”, it becomes the processing object.

[0080] Because the 210 detail is “\$%#257445y7nc09yw983” and there is no identical information at the 404 basic sequence of the 401 rule master, the 213 Skip is setup to be “FALSE” and the pointer is incremented by one.

[0081] Afterwards, because the 213 Skip of the 205 Seq# “5” is “TRUE”, it will not become the processing object and the pointer is incremented by one.

[0082] Afterwards, because the 213 Skip of the 205 Seq# “6” is “FALSE”, it becomes the processing object.

[0083] Because the 210 detail is “\$%#257445y7nc09yw983” and there is no identical information at the 404 basic sequence of the 401 rule master, the 213 Skip is setup

to be “FALSE” and the pointer is incremented by one.

[0084] Because the 213 Skip of the 205 Seq# “7” is “FALSE”, it becomes the processing object.

[0085] Because the 210 detail is “\$ % # 0 9 7”, there is the same information 402ID “1” on the 404 basic sequence of the 401 rule master. Therefore, it is memorized.

[0086] When the same data “①” of the 212 summary No. is investigated, the same data “①” of the 212 summary No. of the 205 Seq# “8” could be investigated. Because the data of the 210 detail of the 205 Seq# “8” is “\$ % # 2 5 7 4 4 5 y 7 n c o 9 y w 9 8 3”, it is the same data when comparing with the 406 sequence 1 of the 402ID “1”. There is no data at the 407 sequence 2 of the 402ID “1”, and the 405 constant time is “3”, and the difference of 206 date and time is “1”. Therefore, the 211 operation of the 205 Seq# “7” is determined to be read, and the 211 operation becomes “read”.

[0087] The 213 Skip is setup to be “FALSE”, the 213 Skip of the 205 Seq# “8” is setup to be “TRUE”, and the pointer is incremented by one.

[0088] Afterwards, the pointer is incremented by one. Because the 213 Skip of the 205 Seq# “8” is “TRUE”, it will not become the processing object and the pointer is incremented by one. Because the data is ended, the processing finishes and the next processing will be executed.

[0089] FIG.5 is the schematic of the pass 2 processing device of the invention.

[0090] The object is the content of “FALSE” of the 204 log information table expanded on the memory. The counting number is setup based on the 211 operation and the 212 summary No. with the same 214 counting number and the data of the same 211 operation and 212 summary No. of the constant duration before and after the organization according to the 501 separation master.

[0091] The processing starts by the 204 log information table expanded on the memory.

[0092] Because the 213 Skip of the 205 Seq# "1" is "FALSE", the 211 operation is "read".

[0093] Therefore, when the 502 operation of the 501 separation master is investigated, because there is "read" and the 503 separation is "2" for the investigation before and after the 2 seconds, the pointer of the 211 operation "read", the 212 summary No. "①" and the 205 Seq# "1" are memorized. The match processing pointer is incremented by 1.

[0094] Because the 213 Skip of the 205 Seq# "2" is "TRUE", it will not become the processing object, and the match processing pointer is incremented by 1.

[0095] Although the 213 Skip of the 205 Seq# "3" is "FALSE", the 211 operation is not matched with the 212 summary No., it will not become the processing object, and the match processing pointer is incremented by 1.

[0096] Although the 213 Skip of the 205 Seq# "4" is "FALSE" "FALSE", the 211 operation is not matched with the 212 summary No., it will not become the processing object, and the match processing pointer is incremented by 1.

[0097] Because the 213 Skip of the 205 Seq# "5" is "TRUE", it will not become the processing object, and the match processing pointer is incremented by 1.

[0098] Although the 213 Skip of the 205 Seq# "6" is "FALSE" "FALSE", the 211 operation is not matched with the 212 summary No., it will not become the processing object, and the match processing pointer is incremented by 1.

[0099] Because the 213 Skip of the 205 Seq# "7" is "FALSE" and the 212 summary No. is "①" and the 211 operation is "read", the 214 count of the initial value 1 of the 205 Seq# "1" is added by 1 to be 2 at the above memorized pointer. the match processing object is incremented by 1.

[00100] Because the 213 Skip of the 205 Seq# "8" is "TRUE", it will not become the processing object, and the match processing pointer is incremented by 1.

[00101] Because all data of the 204 log information table has be processed, the pointer is

incremented by 1 to process the second 205 Seq# "2".

[00102] Because the 213 Skip is "TRUE", there is no operation and the pointer is incremented by 1.

[00103] Because the 213 Skip of the 205 Seq# "3" is "FALSE", the 211 operation is "read".

[00104] Therefore, when the 502 operation of the 501 separation master is investigated, because there is "read" and the 503 separation is "2", in order to investigate the period before and after 2 seconds, the pointer of the 211 operation "read", the 212 summary No. "②" and the 205 Seq# "3" is memorized. The match processing pointer is staggered before the 2 second. In the embodiment, 2 second before the 206 date and time becomes the initial data of the 204 log information table.

[00105] Although the 213 Skip of the 205 Seq# "1" is "TRUE", the 211 operation is not matched with the 212 summary No, it will not become the processing object, and the match processing pointer is incremented by 1.

[00106] Because the 213 Skip of the 205 Seq# "2" is "TRUE", it will not become the processing object, and the match processing pointer is incremented by 1.

[00107] Because the 205 Seq# "3" is the currently-processing data, the match processing pointer is incremented by 1.

[00108] Although the 213 Skip of the 205 Seq# "4" is "FALSE", the 211 operation is not matched with the 212 summary No, it will not become the processing object, and the match processing pointer is incremented by 1.

[00109] Because the 213 Skip of the 205 Seq# "5" is "TRUE", it will not become the processing object, and the match processing pointer is incremented by 1.

[00110] Although the 213 Skip of the 205 Seq# "6" is "FALSE" "FALSE", the 211 operation is not matched with the 212 summary No, it will not become the processing object, and the match processing pointer is incremented by 1.

[00111] Although the 213 Skip of the 205 Seq# "7" is "FALSE" "FALSE", the 211 operation is not matched with the 212 summary No, it will not become the processing object, and the match processing pointer is incremented by 1.

[00112] Because the 213 Skip of the 205 Seq# "8" is "TRUE", it will not become the processing object, and the match processing pointer is incremented by 1.

[00113] Although all data of the 204 log information table has been processed, there is no identical 211 operation "read" and 212 summary No. "②", the 214 counting number of the 205 Seq# "3" is setup to be 1.

[00114] Because the pointer is incremented by 1 and the 213 Skip of the fourth 205 Seq# "4" is "FALSE", the 211 operation is "write".

[00115] Therefore, when the 502 operation of the 501 separation master is investigated, because there is "write" and the 503 separation is "2", in order to investigate before and after 2 seconds, the pointer of the 211 operation "write" and the 212 summary No. "①" and the 205 Seq# "4" is memorized. The match processing pointer is staggered before the 2 seconds. In the embodiment, 2 seconds before the 206 date and time becomes the initial data of the 204 log information table.

[00116] Although the 213 Skip of the 205 Seq# "1" is "FALSE", the 211 operation is not matched with the 212 summary No, it will not become the processing object, and the match processing pointer is incremented by 1.

[00117] Because the 213 Skip of the 205 Seq# "2" is "TRUE", it will not become the processing object, and the match processing pointer is incremented by 1.

[00118] Although the 213 Skip of the 205 Seq# "3" is "FALSE", the 211 operation is not matched with the 212 summary No, it will not become the processing object, and the match processing pointer is incremented by 1.

[00119] Because the 205 Seq# "4" is the currently-processing data, the match processing

pointer is incremented by 1.

[00120] Because the 213 Skip of the 205 Seq# "5" is "TRUE", it will not become the processing object, and the match processing pointer is incremented by 1.

[00121] Although the 213 Skip of the 205 Seq# "6" is "FALSE", the 211 operation is not matched with the 212 summary No, it will not become the processing object, and the match processing pointer is incremented by 1.

[00122] Although the 213 Skip of the 205 Seq# "7" is "FALSE", the 211 operation is not matched with the 212 summary No, it will not become the processing object, and the match processing pointer is incremented by 1.

[00123] Because the 213 Skip of the 205 Seq# "8" is "TRUE", it will not become the processing object, and the match processing pointer is incremented by 1.

[00124] Although all data of the 204 log information table has been processed, there is no identical 211 operation "write" and 212 summary No. "① ", the 214 counting number of the 205 Seq# "4" is setup to be 1.

[00125] Because the pointer is incremented by 1 and the 213 Skip of the fifth 205 Seq# "5" is "TRUE", it will not become the processing object.

[00126] Because the pointer is incremented by 1 and the 213 Skip of the sixth 205 Seq# "6" is "FALSE", the 211 operation is "write".

[00127] Therefore, when the 502 operation of the 501 separation master is investigated, because there is "write" and the 503 separation is "2", in order to investigate before and after 2 seconds, the pointer of the 211 operation "write" and the 212 summary No. "③ " and the 205 Seq# "6" is memorized. The match processing pointer is staggered before the 2 seconds. In the embodiment, 2 seconds before the 206 date and time becomes the initial data of the 204 log information table.

[00128] Although the 213 Skip of the 205 Seq# "1" is "FALSE", the 211 operation is not

matched with the 212 summary No, it will not become the processing object, and the match processing pointer is incremented by 1.

[00129] Because the 213 Skip of the 205 Seq# "2" is "TRUE", it will not become the processing object, and the match processing pointer is incremented by 1.

[00130] Although the 213 Skip of the 205 Seq# "3" is "FALSE", the 211 operation is not matched with the 212 summary No, it will not become the processing object, and the match processing pointer is incremented by 1.

[00131] Although the 213 Skip of the 205 Seq# "4" is "FALSE", the 211 operation is not matched with the 212 summary No, it will not become the processing object, and the match processing pointer is incremented by 1.

[00132] Because the 213 Skip of the 205 Seq# "5" is "TRUE", it will not become the processing object, and the match processing pointer is incremented by 1.

[00133] Because the 205 Seq# "6" is the currently-processing data, the match processing pointer is incremented by 1.

[00134] Although the 213 Skip of the 205 Seq# "7" is "FALSE", the 211 operation is not matched with the 212 summary No, it will not become the processing object, and the match processing pointer is incremented by 1.

[00135] Because the 213 Skip of the 205 Seq# "8" is "TRUE", it will not become the processing object, and the match processing pointer is incremented by 1.

[00136] Although all data of the 204 log information table has been processed, there is no identical 211 operation "write" and 212 summary No. "③", the 214 counting number of the 205 Seq# "6" is setup to be 1.

[00137] Because the pointer is incremented by 1 and the 213 Skip of the 205 Seq# "7" is "TRUE", it will not become the processing object, and the pointer is incremented by 1.

[00138] Because the pointer is incremented by 1 and the 213 Skip of the 205 Seq# "8" is

"TRUE", it will not become the processing object. When the pointer is incremented by 1, because all data has been processed, next process will be executed.

[00139] By repeating the processing disclosed by the embodiment, the 214 counting number will become the status of the 204 log information table which is disclosed on the following paragraph.

[00140] FIG.6 is the schematic of the pass 3 processing device of the invention.

[00141] The computer is operated based on several activities of the command from the user. When the file is deleted, the computer reads the index information at the disk and performs the operation of deleting the index information. Several operations must be organized to merely record the actual activity of people. The 211 operation is inspected according to each 212 summary No. of the 204 log information table based on the 601 operation master in order to confirm the actual activity of people.

[00142] The process is initiated by the 204 log information table which is expanded at the memory of the FIG.6. Because the 213 Skip of the 205 Seq# "1" is "FALSE" and the 212 summary No. is "①", the 211 operation is "read" initially. Therefore, the 211 operation "read" and the 212 summary No. "①" and the pointer are memorized, and the pointer is incremented by 1.

[00143] Because the 213 Skip of the 205 Seq# "2" is "TRUE", the pointer is incremented by 1.

[00144] Because the 212 summary No. of the 205 Seq# "3" is "②", the pointer is incremented by 1.

[00145] Because the 212 summary No. of the 205 Seq# "4" is "①", the 211 operation is "write", when investigating whether or not the combination of "read" and "write" is matched with the pattern of 601 operation master, because the 603 slave operation 1 and 604 slave operation 2 of the row of the 602 basic operation "write" is matched together with the "read"

and "write", the "write" is recorded.

[00146] The pointer is incremented by 1.

[00147] Because the 213 Skip of the 205 Seq# "5" is "TRUE", the pointer is incremented by 1.

[00148] Because the 212 summary No. of the 205 Seq# "6" is "③", the pointer is incremented by 1.

[00149] Because the 213 Skip of the 205 Seq# "7" is "TRUE", the pointer is incremented by 1.

[00150] Because the 213 Skip of the 205 Seq# "7" is "TRUE", the pointer is incremented by 1. Because the data is ended, the combination of the 205 Seq# "1" and 205 Seq# "4" is determined to be "write" by the 601 operation master, and the 213 Skip of the 205 Seq# "1" of the 204 log information table (1) is changed to be "TRUE".

[00151] Afterwards, the process disclosed at the initial of the embodiment is repeated, which becomes the status of the 204 log file table at the lower-portion of FIG.6.

[00152] The processing is initiated at the 204 log file table at the lower-portion of FIG.6.

[00153] Only the 213 Skip is "FALSE". The 206 data and time, the 207 user, the 208 server, the 209 object and the 214 counting number are the data output of the 124 access log.

[00154] Accordingly, the 111 log information could be compressed from one in 1000th to one in 2000th. All process is executed at the memory, and the processing speed is extremely fast.

[00155] FIG.7 is the schematic of the pass 4 processing device of the invention.

[00156] The activities of user are translated into natural language by utilizing the 701 dictionary master based on the 612 user through the 124 access log which is the file from the output of the pass 3. By translating into natural language, the report which is readable for people could be accomplished automatically such as the system monitoring evidence, the

attendance management, the daily report and the weekly report. Any data outputted by the machine could be converted into the natural language by changing the 701 dictionary master.

[00157] The embodiment is illustrated by regarding the 612 user of the 124 access log as the center.

[00158] The first row of the 124 access log is read, and the 701 dictionary master is searched by utilizing the 615 operation "logon" of the 612 user "A" as the searching key. Because the 702 operation 1 has "logon" and the 705 date is "0" and the 706 new line is "0", the data portion and the new line code of the 611 date and time are outputted on the 126 natural language report file.

[00159] Afterwards, the time of the 611 date and time is outputted. The matched information is applied on the portion which is surrounded by the "{}" of the 704 article matched with the 701 dictionary master.

[00160] In the embodiment, the 702 operation 1 of the 701 dictionary master is applied to the 612 user corresponding to the "{user}" and applied to the 613 server corresponding to the "{server}" of the 704 article of "logon", and it is outputted on the 126 natural language report file.

[00161] When the next identical 612 user and the 615 operation are "logoff", the comma "、" and the new line code are written. The logoff process is executed based on the dictionary master.

[00162] However, because the 615 operation of next identical 612 user is "read", the "read" of the 702 operation 1 of the 701 dictionary master is searched.

[00163] Because there are two examples at the 701 dictionary master and the "write" is a continual pattern, the 211 operation searches the object of "write" under the conditions that the identical 612 user on the 124 access log is "A" and the 613 server is "α" and the 614 object is "X".

[00164] The data of the 611 date and time is "2015/06/24 20 : 39 : 49", which is matched with "2015/06.24 20 : 59 : 05".

[00165] Therefore, the 702 operation 1 of the 701 dictionary master is "read", the 703 operation 2 is the 614 object applied for the "{object}" of the 704 article of "write". The time of the 124 access log, the 704 article, the punctuation, the new line code are outputted at the 126 natural language report file.

[00166] Afterwards, the pointer is staggered to the next position of "2015/06/24 20 : 37 : 46" of the 611 date and time. When the activity of the 612 user "A" is followed, the new pattern is at the 611 data and time "2015/06/24 21 : 05 : 49" and the 611 data and time "2015/06/24 21 : 05 : 58". The 702 operation 1 and the 703 operation 2 of the 701 dictionary master are matched with the "write" pattern. Therefore, the 614 object is applied for the "{object}" of the 704 article, and the 704 article, the punctuation, the new line code are outputted at the 126 natural language report file.

[00167] Afterwards, the pointer is staggered to the next position of "2015/06/24 21 : 05 : 49" of the 611 date and time. When the activity of the 612 user "A" is followed, the new pattern is at the 611 data and time "2015/06/24 21 : 10 : 55", and the 702 operation 1 of the 701 dictionary master is matched to the pattern of logoff.

[00168] Therefore, the 612 user corresponding to the "{article}" of the 704 article and the 613 server corresponding to the "{server}" are applied. The 704 article, the punctuation, the new line code are outputted at the 126 natural language report file.

[00169] The output as the 126 natural language report is readable content for people. Therefore, the first logon and the last logoff could be applied for the attendance table of "on YY year MM month DD day, HH hour MM minute on work, HH hour MM minute off work".

[00170] FIG.8 is the schematic of the pass 5 processing device of the invention.

[00171] In the embodiment, the searching key is the 803 user of the 801 user sort and the information such as the server, object, right, application duration, certification date and time which are available and predetermined for each user to use the electronic certification work flow. The suitability of the access right of the 805 object is confirmed, and the confirmation content is written into the 821 warning of the 127 warning report.

[00172] It could be understood that the 802 date and time "2015/06/21 10 : 35 : 40" and the 804 server "α" and the 805 object "X" are read from the 806 operation by the 803 user "A" with the 801 access log (user sort) which is sorted and outputted from the 125 access log by the 612 user.

[00173] The searching key is the 803 user, the 804 server and the 805 object of the 801 access log (user sort) so that the 812 user, the 813 server and the 814 object of the 811 access control list are matched. It could be known that the 812 user "A" is the 813 server "α" and the access right of the 814 object "X" is canceled to be 2015/06/20 from the 818 canceling date, which is obtained from the information of the 816 application period, the 817 certification date and the 818 canceling date.

[00174] However, actually, the 803 user "A" reads the object "X" of the server "α" from operation at the 802 date and time "2015/06/21 10 : 35 : 40".

[00175] It could be estimated from the event that :

[00176] The manager misunderstands the setting of the access right.

[00177] Someone operates the access right illegally.

[00178] Abnormal error occurs on the access management system.

[00179] Illegal Access occurs such as the hacking.

[00180] Therefore, on the 127 warning report, the "read right canceling completed" and the warning information are outputted at the 802 date and time, the 803 user, the 804 server, the 805 object, the 806 operation and the 821 warning.

[00181] When the inconsistency occurs, it could be shown the "read" right and the actual warning of violating the rights.

[00182] FIG.9 is the schematic of the pass 6 processing device of the invention.

[00183] In the embodiment, the past access resume is accumulated. The accumulated access records are utilized to compare the actual access status of the file according to the pointing information predetermined by the user. When there is a file not accessed by anyone over a constant period, the alarm report will be outputted, or the file is automatically canceled or is automatically backed up at the storage.

[00184] The searching key is the 904 server and the 905 object of the 901 access log (server sort) of the 125 access log which is sorted and outputted by the 613 server. The 914 final access date of the row of the 912 object and the identical 911 server is set up to be the date of the 902 date and time. The 915 monitoring date is set up to be the processing date, and 916 passing day is updated to be the days by the current date subtracting the final access date.

[00185] When the 916 passing day exceeds the days of the pointing information which is predetermined by the manager, the warning report is outputted. The file of the 905 object is automatically canceled or backed up at the storage through the indication of the manager.

[00186] In the embodiment, the days which exceed the 816 application period of the 811 access control list becomes the days of the pointing information. The 916 passing day of the 128 access resume is the data of "536" which becomes the object.

[00187] FIG.10 is the schematic of the pass 7 processing device of the invention.

[00188] In the embodiment, the access frequency of the files of the server is calculated during a constant period such as half year, a quarter or a year. As such, the 1005 ratio 1 or the processing amount from the access is calculated, and the report considering the loading diversity of each server in the future is outputted.

[00189] The searching key is the year and month portion of the 206 date and time, the 207 user, the 208 server, the 209 object, the 211 operation of the 125 access log. The appearing numbers of the 207 server, the 208 object, the 206 date and time, the date portion of the 205 date and time, and the 210 operation of the 125 access log are calculated on the 1004 counting number which is consistent with the 129 operation improvement information, and they are added on the 1004 counting number.

[00190] After all rows of the 203 log information table have been processed, the value of the 1004 counting number is utilized to calculate the statistical information of the access ratio by the unit such as month and quarter.

[00191] In the embodiment, the percentage ratio is determined by the 1004 counting number with the unit of month and the 1004 counting number of all servers. The information is setup based on the object unit at the 1005 ratio 1, and it is setup based on the server unit at the 1006 ratio 2.

[00192] Accordingly, the access frequency of the actual operation of people could be obtained.

[00193] Because each item of the 902 statistical information could be changed arbitrarily, all statistical information could be analyzed such as the utilizing frequency of the communication lines and the communication fee of the communication line.

[00194] The processing content and the improvement of programming could be accomplished by utilizing the loading analysis of each access content.

AVAILABLE APPLICATIONS FOR THE INDUSTRY

[00195] Currently, corresponding to the popularized computer and the increasing computer crime, the law becomes severe such as the electronic calculator usage cheating crime and the business hinder crime of the illegal electromagnetic record composition crime, the electromagnetic record damage crime, and the electronic calculator damage crime.

However, the risk management system could be fulfilled by strengthening the monitoring and the monitor system and importing the system to know when and who did what by anyone. In addition, it is needed to analyze the operation record which is outputted from the computer device of inhibiting the crime, translate into natural language, and analyze the log and the operation content in order to provide improvement from the analyzed content and obtain the optimized technology. A technical device is provided to cancel the file which has the access right but has not been accessed, cancel the file which has not been accessed by anyone, perform the loading diversity of the server which is mainly-accessed, improve the performance, re-evaluate the safety control, and provide the support information of accumulating and analyzing the past information.

What is claimed is:

1. A mapping processing device, equipped with the following function, comprising:

reading an accumulation log information outputted by a computer device group
5 which has become an object;

in order to analyze the read accumulation log information according to a time
sequence, extracting a date and time, a user, a server, an object and a
detail from the accumulation log information, attaching a control
information which is needed for translation, and arranging on a log
10 information table at the memory.

2. A pass 1 processing device, equipped with the following function, comprising:

from a log information which is arranged on the log information table of the
memory, expanding the user, the server, the object as a summary at
15 other memory regions which are different from the log information
table, utilizing the expanded summary to make the row of same user,
same server and same object of a plurality of rows which cover the log
information as the only assembly, linking the assembly with a rule
master, when it is matched with the rule master, translating into an
20 operation which is visible and readable for people according to the
conversion rule and aggregation of computer operation defined on the
rule master.

3. A pass 2 processing device, equipped with the following function, comprising:

25 by utilizing the date and time of an operation record from the log information
table translated by the pass 1 processing device, determining the
operation record generated at a constant time, calculating and
organizing the same operation in the constant time, converting the

operation record of the rows into the operation record of one row, and
selecting useful operation record, and

a pass 3 processing device, equipped with the following function, comprising:

by utilizing the pass 2 processing device, scanning the selected log information
table according to the time sequence, providing priority on the operation
generated at the constant time before and after the specific operation for
the row of the same user, the same server and the same object.

4. A pass 4 processing device, equipped with the following function,
comprising:

extracting information for translation into natural language from the log
information table translated by the pass 3 processing device, providing
a report about translating information outputted by the machine into the
natural language by referring the dictionary master so that any natural
language speaker could understand, compositing the readable report of
weekly report, daily report, attendance management, system monitoring
symbol for people with a fixed pattern which is made automatically with
a predetermined report format, so that any data outputted by machine
could be converted into the natural language.

5. A pass 5 processing device, equipped with the following function,
comprising:

inspecting whether or not the user, the object and the operation outputted at the
log information table is consistent with content of the right defined by
the access control list outputted by the electronic certification work
flow, when the inspected content is qualified, performing certification
of legitimacy of the right, when the inspected content is not qualified,
outputting a warning of violating the right; and

a pass 6 processing device, equipped with the following function, comprising:

defining user of right at the access control list, when the object file is not operated during the application period, executing the warning for the effectiveness of the right of the user.

6. A pass 7 processing device, equipped with the following function,
5 comprising:

regarding the log information table translated by the pass 2 processing device as an input, providing information about loading diversity based on the operating number of people for the server and the object unit.