What is claimed is:

1. A log analysis system configured to analyze detection logs detected in a monitoring target system, the log analysis system comprising:

an acquisition device configured to detect detection target processes performed in the monitoring target system, and to acquire detection logs of the detection target processes; and

at least one processor device configured to process the detection logs acquired by the acquisition device, the at least one processor device being configured to sort the detection logs into detection target processes having a specific quality, and into detection target processes not having the specific quality;

the at least one processor device comprising:

a first processor unit configured to normalize the detection logs acquired by the acquisition device, the first processor unit being configured to allocate the detection logs as normalized into predefined monitoring target units, and to output the detection logs as normalized and allocated for the respective monitoring target units;

a second processor unit configured to append common information based on a predefined rule to each of the detection logs for a respective one of the monitoring target units, which have been output from the first processor unit, the second processor unit being configured to make information granularities uniform over the monitoring target units, based on the contents of the detection logs and the common information, to output analysis unit information;

a third processor unit configured to integrate the analysis unit information output from the second processor unit and set detection target event candidates, based on a first predefined rule, the third processor unit being configured to determine whether or not the detection target event candidates are detection target processes having the specific quality, based on a second predefined rule, and the third processor unit being configured to output the detection target event candidates and the determination results; and

a fourth processor unit configured to output the detection target event candidates and the determination results output from the third unit in a predefined output format.

2. The log analysis system according to claim 1, wherein the first processor unit of

the processor device comprises a combination of process unit blocks which are componentized separately for individual processing for performing normalization and allocation of the detection logs.

3. The log analysis system according to claim 2, wherein the first processor unit of the processor device is configured to specify types and processing order of the process unit blocks that are included in the first processor unit, based on a rule which has been set according to a type of the acquisition device.

4. The log analysis system according to any one of claims 1 to 3, wherein the second processor unit of the processor device comprises a combination of process unit blocks componentized separately for individual processing for appending common information to the detection logs and making information granularities uniform.

5. The log analysis system according to claim 4, wherein the second processor unit of the processor device is configured to specify types and processing order of the process unit blocks that are included in the second processor unit, based on a rule which has been set according to a type of the monitoring target unit.

6. The log analysis system according to any one of claims 1 to 5, wherein the third processor unit of the processor device comprises:

a classification unit configured to classify the analysis unit information output from the second processor unit into an analysis unit information which is to be subject to a correlation analysis and into another analysis unit information which is not to be subject to the correlation analysis;

an integration unit configured to integrate the analysis unit information which is to be subject to the correlation analysis, and configured to set detection target event candidates; and

an analysis unit configured to perform determination processing including analysis of correlation of the analysis unit information with respect to the detection target event candidates, and to determine whether or not the detection target even candidates are detection target processes having the specific quality.

7. The log analysis system according to claim 6, wherein the analysis unit included in

the third processor unit of the processor device comprises a combination of the process unit blocks componentized separately for individual processing for determination processing including the correlation analysis based on determination conditions set for determining whether or not detection target event candidates are detection target processes having the specific quality.

8. The log analysis system according to any one of claims 1 to 7, wherein the second processor unit of the processor device comprises a process for making information granularities of the detection logs, the process comprising:

setting multiple detection logs aggregated based on a predefined aggregation condition as one piece of analysis unit information in case that the detection log is acquired from the monitoring target system when the detection log undergoes one detection target process; and

setting one detection log as one piece of the analysis unit information in case that the detection log is a detection log acquired from the monitoring target system when the detection log is subject to multiple detection target processes.

Claims:

1. An information analysis system comprising:

a first processor unit configured to append common information to analysis target information generated by events; the processor unit being configured to make information granularities uniform based on the contents of the analysis target information and the common information to output analysis unit information; and

a second processor unit configured to integrate the analysis unit information output from the first processor unit to generate detection target event candidates, the second processor unit being configured to determine whether or not the events have at least one specific quality, the events having generated the analysis target information specified by the detection target event candidates.

2. An information analysis method performed by one or more computers, the method comprising:

appending common information to analysis target information generated by events;

making information granularities uniform based on the contents of the analysis target information and the common information to output analysis unit information;

integrating the analysis unit information into detection target event candidates; and

determining whether or not the events have at least one specific quality, the events having generated the analysis target information specified by the detection target event candidates.

3. A computer program product comprising one or more computer programs embodied on a non-transitory computer readable medium, the one or more computer programs comprising codes for:

appending common information based on a first predefined rule to analysis target information generated by events;

making information granularities uniform based on the contents of the analysis target information and the common information to output analysis unit information;

integrating the analysis unit information into detection target event candidates; and

determining whether or not the events have at least one specific quality, the events having generated the analysis target information specified by the detection target event candidates.

4. An information analysis system comprising:

a first processor unit configured to append common information to analysis target information generated by events; the processor unit being configured to make information granularities uniform by selectively conducting a process for grouping the analysis target information based on the contents of the analysis target information and the common information to output analysis unit information; and

a second processor unit configured to analyze the analysis unit information output from the first processor unit.

5. An information analysis method performed by one or more computers, the method comprising:

appending common information to analysis target information generated by events;

making information granularities uniform by selectively conducting a process for grouping the analysis target information based on the contents of the analysis target information and the common information to output analysis unit information; and

analyzing the analysis unit information.

6. A computer program product comprising one or more computer programs embodied on a non-transitory computer readable medium, the one or more computer programs comprising codes for:

appending common information based on a first predefined rule to analysis target information generated by events;

making information granularities uniform by selectively conducting a process for grouping the analysis target information based on the contents of the analysis target information and the common information to output analysis unit information; and

analyzing the analysis unit information.