

What is claimed is:

1. A terminal device comprising:

5 a file generation unit which acquires logs among a plurality of logs output from a security sensor monitoring the logs at all times and outputting the logs monitored at all times and generates a file including the acquired logs;

a file transmission unit which transmits the file generated by the file generation unit to a file analysis device that performs file analysis in a case where a condition that information of the logs included in one or a plurality of the files to be analyzed once be
10 equal to or less than an upper limit value of an allowable amount of data is satisfied;

a notification control unit which receives a notification of an analysis result of the file transmitted from the file analysis device;

a file condition determination unit which determines whether or not the condition that the information of the logs to be scheduled to be included in one or the
15 plurality of files to be analyzed once be equal to or less than the upper limit value of the allowable amount of data is satisfied; and

a log reduction unit which reduces the amount of data of the logs included in the file in a case where the file condition determination unit determines that the condition is not satisfied,

20 wherein, in a case where the file condition determination unit determines that the condition is not satisfied, the log reduction unit reduces the amount of data of the logs included in the file, the file generation unit generates the file using the information of the logs satisfying the condition, and the file transmission unit transmits the file to the file analysis device.

2. The terminal device according to claim 1, wherein

the log reduction unit displays a period including a date and time when the logs are generated, and satisfying the condition with respect to the information of the logs included in the period, and changes the period so that the condition is satisfied in a case
5 where the condition is not satisfied when the displayed period is changed by a user's operation, and

the file generation unit generates the file using the information of the logs included in the period satisfying the condition.

10 3. The terminal device according to claim 2,

wherein one or two or more sensors are designated by user's operation, and the information of the logs scheduled to be included in the file includes information of the logs which is detected by the designated sensors.

15 4. The terminal device according to any one of claims 1 to 3, further comprising:

an analysis request availability determination unit which determines whether or not a request for analyzing the file is able to be made on the basis of content of a contract related to an analysis service for the file and usage conditions of the service.

20

5. A file analysis device comprising:

a reception unit which receives one or a plurality of files to be analyzed once which are transmitted from a terminal device, the file including logs among a plurality of logs output from a security sensor monitoring the logs at all times and outputting the logs
25 monitored at all times;

a file inspection unit which determines whether or not the file received by the reception unit satisfies an inspection condition that information of the logs included in one or the plurality of files to be analyzed once be equal to or less than an upper limit value of an allowable amount of data;

5 a file analysis unit which analyzes the information of the logs included in one or the plurality of files to be analyzed once for which the file inspection unit determines that the inspection condition is satisfied; and

a notification unit which transmits a notification of a result of analysis of the file which is performed by the file analysis unit to the terminal device.

10

6. The file analysis device according to claim 5, further comprising:

a management unit which manages charging information related to the analysis performed by the file analysis unit,

wherein the charging information includes information of an amount of money

15 according to the number of times analysis is performed, and

the information of an amount of money according to the number of times analysis is performed is information of a charged amount of money according to the number of times analysis is performed or information indicating that the information is free when the number of times analysis is performed is equal to or less than a

20 predetermined number of times.

7. A file analysis system comprising:

a terminal device; and

a file analysis device,

25 wherein the terminal device includes

a file generation unit which acquires logs among a plurality of logs output from a security sensor monitoring the logs at all times and outputting the logs monitored at all times and generates a file including the acquired logs,

a file transmission unit which transmits the file generated by the file generation
5 unit to the file analysis device,

a notification control unit which receives a notification of an analysis result of the file transmitted from the file analysis device,

a file condition determination unit which determines whether or not the condition that the information of the logs to be scheduled to be included in one or the
10 plurality of files to be analyzed once be equal to or less than an upper limit value of an allowable amount of data is satisfied; and

a log reduction unit which reduces the amount of data of the logs included in the file in a case where the file condition determination unit determines that the condition is not satisfied,

15 in a case where the file condition determination unit determines that the condition is not satisfied, the log reduction unit reduces the amount of data of the logs included in the file, the file generation unit generates the file using the information of the logs satisfying the condition, and the file transmission unit transmits the file to the file analysis device, and

20 the file analysis device includes

a reception unit which receives the file transmitted from the terminal device,

a file inspection unit which determines whether or not the file received by the reception unit satisfies a predetermined inspection condition,

a file analysis unit which analyzes the file for which the file inspection unit
25 determines that the inspection condition is satisfied, and

a notification unit which transmits a notification of a result of analysis of the file which is performed by the file analysis unit to the terminal device.

8. A file analysis method comprising:

5 causing a terminal device to acquire logs among a plurality of logs output from a security sensor monitoring the logs at all times and outputting the logs monitored at all times, determine whether or not a condition that information of the logs to be scheduled to be included in one or a plurality of files to be analyzed once be equal to or less than an upper limit value of an allowable amount of data is satisfied, and reduce the amount of
10 data of the logs included in the file in a case where it is determined that the condition is not satisfied to thereby generate the file using the information of the logs satisfying the condition, and to transmit the file to a file analysis device;

causing the file analysis device to receive the file transmitted from the terminal device, determine whether or not the received file satisfies a predetermined inspection
15 condition, analyze the file determined to satisfy the inspection condition, and transmit a notification of an analysis result of the file to the terminal device; and

causing the terminal device to receive the notification of the analysis result of the file which is transmitted from the file analysis device.

20 9. A program causing a computer to perform functions comprising:

a function of acquiring logs among a plurality of logs output from a security sensor monitoring the logs at all times and outputting the logs monitored at all times;

a function of determining whether or not a condition that information of the logs to be scheduled to be included in one or a plurality of files to be analyzed once be equal
25 to or less than an upper limit value of an allowable amount of data is satisfied;

a function of reducing the amount of data of the logs included in the file in a case where it is determined that the condition is not satisfied to thereby generate the file using the information of the logs satisfying the condition;

- 5 a function of transmitting the generated file to a file analysis device performing file analysis in a case where the condition that the information of the logs included in one or the plurality of files to be analyzed once be equal to or less than the upper limit value of the allowable amount of data is satisfied; and

a function of receiving a notification of an analysis result of the file which is transmitted from the file analysis device.