

[DESCRIPTION]

[TITLE OF INVENTION]

TERMINAL DEVICE, FILE ANALYSIS DEVICE, FILE ANALYSIS SYSTEM, FILE
ANALYSIS METHOD, AND PROGRAM

5 [Technical Field]

[0001]

The present invention relates to a terminal device, a file analysis device, a file
analysis system, a file analysis method, and a program.

Priority is claimed on Japanese Patent Application No. 2018-180718, filed
10 September 26, 2018, the content of which is incorporated herein by reference.

[Background Art]

[0002]

Log analysis systems that acquire and analyze a log generated in a system to be
analyzed have become known (see, for example, Patent Literature 1). The log is, for
15 example, a log related to security.

In such log analysis systems, a sensor for security monitors and detects a log
generated in the system to be analyzed. Such monitoring is performed at all times.
Further, in the log analysis system, the system to be analyzed transmits a log detected by
the sensor to a log analysis device through a network. Further, in the log analysis
20 system, the log analysis device analyzes a log transmitted from the system to be
analyzed.

[0003]

However, in order to operate such a log analysis system, it is necessary to
perform setting for transmitting a log detected by the sensor to the log analysis device.
25 Examples of the setting include setting for arranging an environment of a sensor and

setting for arranging an environment of a network.

For this reason, in order to operate the log analysis system, it may take time and burden to perform such environment setting. Further, in order to operate the log analysis system, it is necessary to change a sensor environment and a network environment, but it may be difficult to obtain permission for such a change depending on an organization having a system to be analyzed, or the like.

[Citation List]

[Patent Literature]

[0004]

10 [Patent Literature 1]

Japanese Patent No. 5640166

[Summary of Invention]

[Technical Issues]

[0005]

15 As described above, in the related art, an initial burden for setting the log analysis system to be in an operable state was heavy.

[0006]

Embodiments of the present invention provide a terminal device, a file analysis device, a file analysis system, a file analysis method, and a program which are capable of easily performing log analysis in view of such circumstances.

20

[Solution to Issues]

[0007]

According to some aspects of the present invention, a 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

25

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 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 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, in which 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.

[0008]

According to some aspects of the present invention, in the terminal device, the log reduction unit may display 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 where the condition is not satisfied when the displayed period is changed by a user's operation, and the file generation unit may generate the file using the information of the logs included in the period satisfying the condition.

According to some aspects of the present invention, in the terminal device, one

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

According to some aspects of the present invention, the terminal device may
5 further include 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.
[0009]

According to some aspects of the present invention, a file analysis device
10 includes 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 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
15 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, 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
20 performed by the file analysis unit to the terminal device.

According to some aspects of the present invention, the file analysis device may further include a management unit which manages charging information related to the analysis performed by the file analysis unit, in which the charging information includes information of an amount of money according to the number of times analysis is
25 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 predetermined number of times.

5 [0010]

According to some aspects of the present invention, a file analysis system includes a terminal device and a file analysis device, in which 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
10 times and generates a file including the acquired logs, a file transmission unit which transmits the file generated by the file generation 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
15 to be 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 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, in a case
20 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 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
25 received by the reception unit satisfies a predetermined inspection condition, a file

analysis unit which analyzes the file 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.

5 [0011]

According to some aspects of the present invention, a file analysis method includes 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
10 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 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
15 to receive the file transmitted from the terminal device, determine whether or not the received file satisfies a predetermined inspection 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 [0012]

According to some aspects of the present invention, a program causes a computer to realize functions including 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
25 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, 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, a function of transmitting
5 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.

10 [Advantageous Effects of Invention]

[0013]

According to the above-described file analysis system, file analysis device, terminal device, file analysis method, and program, it is possible to easily perform log analysis.

15 [Brief Description of Drawings]

[0014]

Fig. 1 is a diagram showing a schematic configuration example of a file analysis system according to an embodiment of the present invention.

Fig. 2 is a diagram showing a schematic configuration example of a terminal
20 device according to the embodiment of the present invention.

Fig. 3 is a diagram showing a schematic configuration example of a file according to the embodiment of the present invention.

Fig. 4 is a diagram showing an example of information representing a file analysis result according to the embodiment of the present invention.

25 Fig. 5 is a diagram showing another example of information representing a file

analysis result according to the embodiment of the present invention.

Fig. 6 is a diagram showing an example of information representing the range of a log capable of being subjected to file analysis according to the embodiment of the present invention.

5 Fig. 7 is a diagram showing an example of contract information according to the embodiment of the present invention.

Fig. 8 is a diagram showing an example of a procedure of processing performed in the terminal device according to the embodiment of the present invention.

10 Fig. 9 is a diagram showing an example of a procedure of processing performed in the terminal device according to the embodiment of the present invention.

Fig. 10 is a diagram showing an example of a procedure of processing performed in the terminal device according to the embodiment of the present invention.

Fig. 11 is a diagram showing an example of a procedure of processing performed in the terminal device according to the embodiment of the present invention.

15 Fig. 12 is a diagram showing an example of a procedure of processing performed in a file analysis device according to the embodiment of the present invention.

Fig. 13 is a diagram showing an example of a procedure of processing performed in the file analysis device according to the embodiment of the present invention.

20 Fig. 14 is a diagram showing an example of a procedure of processing performed in the file analysis device according to the embodiment of the present invention.

Fig. 15 is a diagram showing an example of a hardware configuration of an information processing device according to the embodiment of the present invention.

25 [Description of Embodiments]

[0015]

An embodiment of the present invention will be described in detail with reference to the accompanying drawings.

[0016]

5 [File analysis system]

Fig. 1 is a diagram showing a schematic configuration example of a file analysis system 1 according to an embodiment of the present invention. Meanwhile, a configuration of functional blocks shown in Fig. 1 is an example, and other configurations may be used.

10 The file analysis system 1 includes an analysis unit 11, a plurality of terminal portions 21 to 23, and a network 31.

The terminal portions 21 to 23 and the analysis unit 11 are communicatively connected to each other through a network 31.

[0017]

15 Here, the terminal portions 21 to 23 are managed by different management subjects. The management subjects may be organizations such as companies or schools or may be individual persons. In a case where a management subject is an organization, a person belonging to the organization manages the terminal portions 21 to 23. Further, in a case where the management subject is an individual person, the individual person
20 manages the terminal portions 21 to 23. In the present embodiment, a person managing each of the terminal portions 21 to 23 may also be referred to as a user.

Meanwhile, two or more terminal portions among the plurality of terminal portions 21 to 23 may be managed by the same management subject. The two or more terminal portions may be some of the plurality of terminal portions 21 to 23 or may be all
25 of the plurality of terminal portions.

[0018]

The number of terminal portions 21 to 23 may be any number of 1 or greater.

In the present embodiment, for convenience of description, the configurations and operations of the plurality of terminal portions 21 to 23 are the same except that

5 management subjects of the respective terminal portions 21 to 23 may be different from each other. For this reason, in the present embodiment, one terminal portion 21 will be representatively described.

Meanwhile, a mode in which the configurations or operations of the terminal portions 21 to 23 are different may be used.

10 [0019]

In the present embodiment, the analysis unit 11 performs the same operation on each of the plurality of terminal portions 21 to 23 except that the management subjects of the respective terminal portions 21 to 23 are different from each other.

Meanwhile, a configuration in which the analysis unit 11 performs a different
15 operation on each of the plurality of terminal portions 21 to 23 may be used.

[0020]

In the present embodiment, the analysis unit 11 is common to the plurality of terminal portions 21 to 23. Meanwhile, the file analysis system 1 may include a plurality of analysis units 11. In this case, the plurality of analysis units 11 share the
20 plurality of terminal portions 21 to 23 and perform operations.

Here, the analysis unit 11 may be regarded as, for example, a device or a system. In addition, the terminal portion 21 may be regarded as, for example, a device or a system.

[0021]

25 The network 31 may be any network. The network 31 may be, for example,

the Internet or may be a dedicated network.

Meanwhile, communication between each of the terminal portions 21 to 23 and the analysis unit 11 may be, for example, wired communication, wireless communication, or a combination of wired communication and wireless communication.

5 [0022]

[Outline of terminal portion]

The terminal portion 21 will be representatively described.

The terminal portion 21 includes a log detection device 51, a log management device 52, and a terminal device 53. The log management device 52 includes a storage
10 unit 151.

In the example of Fig. 1, a configuration in which each of the log detection device 51, the log management device 52, and the terminal device 53 is connected to the network 31 is shown, but this is not limiting.

[0023]

15 The log detection device 51 detects a predetermined log. In the present embodiment, the log detection device 51 monitors a predetermined target at all times to detect a target log. In the present embodiment, the log is a log related to security (security log) and is, for example, a log which is target for communication through the network 31.

20 The log detection device 51 may be configured using, for example, a sensor that detects a predetermined log. In the present embodiment, the log detection device 51 detects a log related to communication performed by the terminal device 53. The log detection device 51 outputs the detected log. In the present embodiment, the log detection device 51 transmits the detected log to the log management device 52.

25 Meanwhile, in the present embodiment, the log detection device 51 does not

store a detected log. In another example, the log detection device 51 may include a storage unit that stores a detected log.

[0024]

The log management device 52 stores a log detected by the log detection device 51 in the storage unit 151 and manages the stored log.

Here, the log management device 52 may store logs detected by the log detection device 51 in the storage unit 151 for each predetermined group. The predetermined group may be, for example, a group of logs of which the detection times are included in a predetermined period. For example, the predetermined group may be generated as a file. For example, the predetermined period may be a period in units of days.

For example, the log management device 52 may be configured using a log management server device that stores and manages a log.

For example, the log detection device 51 or the log management device 52 may use a syslog which is a communication protocol for recording a log of a computer system.

[0025]

The terminal device 53 is configured using, for example, an information processing device operated by a user. The information processing device is, for example, a computer. The computer may be, for example, a desktop computer, a notebook computer, a mobile phone computer, a smartphone computer, or the like.

The terminal device 53 generates a predetermined file including at least some of logs stored in the storage unit 151 of the log management device 52 on the basis of the logs stored in the storage unit 151 of the log management device 52. The terminal device 53 transmits the generated file to the analysis unit 11 through the network 31.

In addition, the terminal device 53 receives an email transmitted from the analysis unit 11 through the network 31.

In addition, the terminal device 53 acquires information of a web page which is provided by the analysis unit 11.

5 [0026]

[Outline of file analysis unit]

The analysis unit 11 includes a file analysis device 41, a Web server device 42, and a mail server device 43.

In the example of Fig. 1, a configuration in which each of the file analysis
10 device 41, the Web server device 42, and the mail server device 43 is connected to the network 31 is shown, but this is not limiting.

[0027]

The file analysis device 41 includes a storage unit 111, a communication unit
112, a file inspection unit 113, a file analysis unit 114, a notification unit 115, and a
15 management unit 116.

The communication unit 112 includes a reception unit 121.

The file inspection unit 113 includes a decoding unit 131 and a decompression
unit 132.

Meanwhile, although the terms "compression" and "decompression" are used in
20 the description of this embodiment, a term such as "extension" may be used instead of "decompression."

[0028]

An outline of operations performed in the file analysis device 41 will be
described.

25 The storage unit 111 stores various types of information.

The communication unit 112 performs communication of information. In the present embodiment, the communication unit 112 performs communication through the network 31.

The reception unit 121 receives a file transmitted to the analysis unit 11 from the terminal device 53 through the network 31. The reception unit 121 outputs the received file to the file inspection unit 113. In the present embodiment, the terminal device 53 transmits the file to the file analysis device 41.

[0029]

The file inspection unit 113 inputs the file which is output from the reception unit 121. The file inspection unit 113 performs inspection for determining whether or not the input file satisfies predetermined conditions (for convenience of description, also referred to as "inspection conditions"). In a case where the file inspection unit 113 determines that the input file satisfies the inspection conditions, the file is output to the file analysis unit 114. On the other hand, in a case where the file inspection unit 113 determines that the input file does not satisfy the inspection conditions, predetermined information (for convenience of description, also referred to as "inspection error information") is output to the notification unit 115.

In the present embodiment, the storage unit 111 stores information for specifying inspection conditions. The file inspection unit 113 acquires inspection conditions on the basis of the information.

[0030]

Here, in the present embodiment, regarding a file which is transmitted from the terminal device 53 to the file analysis device 41, information of the file is compressed and is then encoded.

In the file inspection unit 113, an input file is in an encoded state, and the

decoding unit 131 decodes the file. Further, in the file inspection unit 113, information of the decoded file is compressed, and the decompression unit 132 decompresses the information. Thereby, the compressed and encoded file is converted into a file before compression and encoding (for convenience of description, also referred to as an "original file"). The file inspection unit 113 performs predetermined inspection on the obtained original file. In a case where the file inspection unit 113 determines that the inspection conditions are satisfied, such an original file is output to the file analysis unit 114.

[0031]

10 As the inspection conditions, any conditions may be used.

The inspection conditions may include, for example, a condition that the amount of data of logs included in a file to be analyzed once be equal to or less than a predetermined upper limit value, a condition that the size of a file to be analyzed once be equal to or less than a predetermined upper limit value, or both conditions.

15 The inspection conditions may include, for example, a condition that a file to be analyzed do not contain a computer virus. Meanwhile, whether or not a file to be analyzed contains a computer virus may be determined using, for example, anti-virus software. The inspection conditions may include, for example, a condition that a file to be analyzed be a file in a predetermined format.

20 The inspection conditions may include, for example, a condition that a file to be analyzed include predetermined information. The predetermined information may be, for example, information indicating that the file is transmitted from a legitimate terminal device 53.

[0032]

25 The file analysis unit 114 inputs a file which is output from the file inspection

unit 113. The file analysis unit 114 performs analysis on the input file on the basis of predetermined conditions (for convenience of description, also referred to as "analysis conditions"). The file analysis unit 114 outputs predetermined information regarding a result obtained by performing analysis on the input file (for convenience of description, also referred to as "analysis result information") to the notification unit 115.

In the present embodiment, the storage unit 111 stores information for specifying analysis conditions. The file analysis unit 114 acquires analysis conditions on the basis of the information.

[0033]

10 As the analysis conditions, any conditions may be used.

As the analysis conditions, for example, a condition for determining whether or not a log included in a file to be analyzed has a problem may be used. The problem may be, for example, a computer virus or may be something else.

As the analysis conditions, for example, "a condition that it is determined that a log has a problem in a case where information for identifying a transmission source included in the log, information for identifying a transmission destination included in the log, or other information included in the log coincides with predetermined information" may be used. As the analysis conditions, for example, a condition described in a black list in which conditions of logs determined to have a problem are listed may be used. In addition, a condition for determining that a log has a problem may be referred to as, for example, a "rule."

Meanwhile, in a case where logs of a plurality of types may be included in a file to be analyzed, for example, the file analysis unit 114 determines the type of each of the logs. In this case, information of each of the logs includes information for specifying the type of log. As another example, such a type of log may be determined by the file

inspection unit 113 instead of the file analysis unit 114.

[0034]

In a case where inspection error information is input from the file inspection unit 113, the notification unit 115 notifies the terminal device 53 of predetermined
5 information based on the inspection error information. As the predetermined information, information for notifying the terminal device 53 of information regarding an inspection error may be used, or any information may be used.

Further, in a case where analysis result information is input from the file analysis unit 114, the notification unit 115 notifies the terminal device 53 of predetermined
10 information based on the analysis result information. As the predetermined information, information for notifying the terminal device 53 of information regarding an analysis result may be used, or any information may be used.

[0035]

Here, any method may be used as a method of notifying the terminal device 53
15 of information by the notification unit 115.

In the present embodiment, in a case where information of which the terminal device 53 is to be notified is generated, the notification unit 115 creates an email addressed to the terminal device 53 and transmits the created email to the mail server device 43. In this case, the notification unit 115 includes information of an access
20 destination that can be accessed by the terminal device 53 in the email. The information may be, for example, a Uniform Resource Locator (URL).

The notification unit 115 generates a web page corresponding to information of the access destination included in the email and transmits information of the generated web page to the Web server device 42. The notification unit 115 includes information
25 of which the terminal device 53 is to be notified in the web page.

[0036]

The mail server device 43 receives an email transmitted from the notification unit 115. The mail server device 43 transmits the received email to an address of the email. In the present embodiment, an email addressed to the terminal device 53 is
5 transmitted to the terminal device 53 through the network 31 from the mail server device 43.

The Web server device 42 receives information of a web page transmitted from the notification unit 115. The Web server device 42 provides the web page so that it can be viewed, on the basis of the received information. In the present embodiment, the
10 Web server device 42 provides the web page to the terminal device 53 so that it can be viewed, in response to access from the terminal device 53.

[0037]

The management unit 116 performs various types of management on the terminal device 53.

15 In the present embodiment, in the analysis unit 11, there may be a case where information of the terminal device 53 is unknown and a case where information of the terminal device 53 is known.

In the present embodiment, in a case where a contract related to a file analysis service is made between a management subject of the terminal device 53 and a
20 management subject providing the file analysis service by the analysis unit 11, information of the terminal device 53 is set in the analysis unit 11 with respect to the contract. The information may be stored in, for example, the storage unit 111. The information may include, for example, information for specifying the terminal device 53. The information may include an address of an email of the terminal device 53.

25 On the other hand, in the present embodiment, in a case where such a contract is

not made, information of the terminal device 53 is unknown to the analysis unit 11.

[0038]

Here, examples of the information of the terminal device 53 which is set with respect to the contract may include information for specifying the range of file analysis in which a service can be received, information regarding a charge required to receive a service (for convenience of description, also referred to as "charging information"), and the like.

The range of file analysis in which a service can be received may be set using, for example, one or more of the amount of data, the number of times, a period, and the like. The range of file analysis in which a service can be received may be specified using, for example, one or more of an upper limit value for the sum of the amount of data of all logs to be analyzed for a predetermined period, an upper limit value for the amount of data of logs to be analyzed once, an upper limit value of the number of times a file analysis service can be received in a predetermined period, and the like.

[0039]

As an example, a service may be charged at a fixed amount.

As another example, a service may be charged on a metered basis. In this case, the management unit 116 stores information for determining a charge to be charged in the storage unit 111 and manages the information with respect to a service provided to the terminal device 53. The information may be, for example, one or more pieces of information among the sum of the amount of data of logs on which a file analysis service has been performed in a predetermined period, the number of times a file analysis service is received in a predetermined period, and the like. For example, an amount of money according to the amount of data using file analysis or the number of times may be charged. In addition, for example, a service provided free of charge up to a

predetermined amount of data using file analysis or a service provided free of charge up to a predetermined number of times file analysis is used may be performed.

In addition, the management unit 116 may store information for specifying a charge charged at the present point in time with respect to the terminal device 53 in the storage unit 111 and may manage the information.

[0040]

As a specific example, the management unit 116 manages charging information regarding file analysis performed by the file analysis unit 114. The charging information includes information of an amount of money according to the number of times file analysis is performed. The information of an amount of money according to the number times of file analysis is performed is, for example, information of a charged amount of money according to the number of times of file analysis is performed or information indicating that the information is free of charge when the number of times file analysis is performed is equal to or less than a predetermined number of times.

Meanwhile, although a specific example of charging according to the number of times file analysis is performed has been described here, the same is true for charging according to the amount of data of file analysis, and the like.

[0041]

[Details of Terminal Device]

Fig. 2 is a diagram showing a schematic configuration example of the terminal device 53 according to the embodiment of the present invention. Meanwhile, a configuration of functional blocks shown in Fig. 2 is an example, and other configurations may be used. The terminal device 53 includes an input unit 211, an output unit 212, an operation unit 213, a display unit 214, a communication unit 215, a storage unit 216, and a control unit 217.

The control unit 217 includes a log acquisition unit 231, a file condition acquisition unit 232, a file condition determination unit 233, a log reduction unit 234, a file generation unit 235, a compression unit 236, an encoding unit 237, a notification control unit 238, and an analysis request availability determination unit 239.

5 [0042]

The input unit 211 inputs information which is output from an external device.

The output unit 212 outputs information to an external device.

Here, the external device may be any device. The external device may be, for example, a portable recording medium. The external device may be, for example, a
10 printing device.

The operation unit 213 inputs information corresponding to an operation performed by a user. The operation unit 213 may include, for example, a keyboard, a mouse, or the like.

The display unit 214 includes a screen and outputs information to the screen.

15 Thereby, the information is displayed on the screen.

[0043]

The communication unit 215 performs communication through the network 31. In the present embodiment, the terminal device 53 is connected to be capable of communicating with the network 31 by the communication unit 215.

20 Meanwhile, the terminal device 53 may be connected to the network 31 through the log detection device 51. In this case, the communication unit 215 outputs a signal to be transmitted to the network 31 through the log detection device 51. In this case, the log detection device 51 inputs a signal which is output from the communication unit 215 and outputs the input signal to the network 31. Further, in this case, the communication
25 unit 215 inputs a signal through the log detection device 51 from the network 31. In

this case, the log detection device 51 inputs a signal from the network 31 and outputs the input signal to the communication unit 215.

[0044]

The storage unit 216 stores various information.

5 The control unit 217 performs various control in the terminal device 53.

[0045]

The log acquisition unit 231 acquires a log. In the present embodiment, the log acquisition unit 231 acquires a predetermined log from logs stored in the log management device 52.

10 The file condition acquisition unit 232 acquires conditions of a file (for convenience of description, also referred to as "file conditions").

In the present embodiment, the storage unit 216 stores information for specifying file conditions. The file condition acquisition unit 232 acquires file conditions on the basis of the information.

15 The file condition determination unit 233 determines whether or not the file conditions have been satisfied with respect to a file to be determined, on the basis of the file conditions acquired by the file condition acquisition unit 232.

[0046]

Here, in the present embodiment, the file conditions include a condition of an upper limit value of an allowable amount of data with respect to information of logs included in a file to be analyzed at least once.

Meanwhile, in a case where the number of files to be analyzed once is one, an upper limit value of an allowable amount of data is an upper limit value of an allowable amount of data with respect to information of logs included in one file.

25 Further, in a case where the number of files to be analyzed once is two or more,

an upper limit value of an allowable amount of data is an upper limit value of an allowable amount of data with respect to the sum of information of logs included in the predetermined number of files.

[0047]

5 The log reduction unit 234 has a function of performing a process of reducing logs which are unnecessary as objects to be analyzed (for convenience of description, also referred to as "unnecessary logs") (for convenience of description, also referred to as an "unnecessary log reduction process") and a function of performing a process of reducing logs to be analyzed by reducing the range of logs to be analyzed (for
10 convenience of description, also referred to as a "log range") (for convenience of description, also referred to as a "log range reduction process"). Thereby, the log reduction unit 234 reduces the amount of data of logs to be analyzed. Meanwhile, in the present embodiment, when the amount of data of logs included in a file is increased, the size of the file is increased or the number of files is increased.

15 In the present embodiment, the log reduction unit 234 performs an unnecessary log reduction process at all times when a file to be analyzed is generated.

 Further, in the present embodiment, the log reduction unit 234 performs a log range reduction process in a case where the amount of data exceeds an upper limit value of an allowable amount of data with respect to information of logs scheduled to be
20 included in a file to be analyzed once.

[0048]

 Meanwhile, as another configuration example, the log reduction unit 234 may not perform an unnecessary log reduction process in a case where the amount of data is equal to or less than an upper limit value of an allowable amount of data with respect to
25 information of logs scheduled to be included in a file to be analyzed once. In addition,

the log reduction unit 234 may perform an unnecessary log reduction process in a case where the amount of data exceeds an upper limit value of an allowable amount of data with respect to information of logs scheduled to be included in a file to be analyzed once. In this case, the log reduction unit 234 performs a log range reduction process in a case
5 where the amount of data exceeds an upper limit value of an allowable amount of data with respect to information of logs scheduled to be included in a file to be analyzed once even after an unnecessary log reduction process is performed.

[0049]

The file generation unit 235 generates a file including information of logs
10 scheduled to be included in a file to be analyzed once by using the information. Regarding the information, for example, the information may not be reduced by the log reduction unit 234 or may be reduced by the log reduction unit 234.

Meanwhile, as an example, the file generation unit 235 may use a group of logs (for example, a group configured as a file) for each predetermined period which is stored
15 in the storage unit 151 of the log management device 52 as a generated file by the file generation unit 235. In this case, the file generation unit 235 may change a format or the like with respect to a group of logs (for example, a group configured as a file) for each predetermined period which are stored in the storage unit 151 of the log management device 52.

20 As another example, the file generation unit 235 may generate a file using a group of logs obtained by reducing logs from the group of logs (for example, a group configured as a file) for each predetermined period which is stored in the storage unit 151 of the log management device 52.

[0050]

25 The compression unit 236 compresses the file generated by the file generation

unit 235.

The encoding unit 237 encodes the file compressed by the compression unit 236.

The control unit 217 transmits the file encoded by the encoding unit 237 to the file analysis device 41 through the network 31 by the communication unit 215.

5 [0051]

Here, information encoded by the encoding unit 237 in the terminal device 53 is returned to the original information through decoding performed by the decoding unit 131 in the file analysis device 41.

In addition, information compressed by the compression unit 236 in the terminal
10 device 53 is returned to the original information through decompression performed by the decompression unit 132 in the file analysis device 41.

[0052]

The notification control unit 238 performs a process for receiving contents of a notification given by the notification unit 115 of the file analysis device 41.

15 In the present embodiment, the notification control unit 238 receives an email by the communication unit 215, the email being transmitted to the terminal device 53 through the network 31 from the mail server device 43. In addition, the notification control unit 238 accesses a Web page which is an access destination written in the received email to acquire information of the Web page provided by the Web server device
20 42. This access may be performed in response to, for example, an operation of the operation unit 213 which is performed by a user.

[0053]

The analysis request availability determination unit 239 determines whether or not a request for file analysis can be made to the file analysis device 41 from the terminal
25 device 53 on the basis of predetermined conditions (for convenience of description,

referred to as "analysis request conditions"). As the analysis request conditions, any conditions may be used, or conditions related to, for example, one or more of the amount of data, the number of times, a period, and the like may be used.

[0054]

5 Here, in the present embodiment, the analysis request availability determination unit 239 performs such determination in a case where a contract related to a file analysis service is made between a management subject of the terminal device 53 and a management subject providing the file analysis service by the analysis unit 11. The analysis request availability determination unit 239 determines whether or not a request
10 for file analysis can be made to the file analysis device 41 from the terminal device 53, on the basis of the contents of the contract and the usage conditions of the service in the terminal device 53.

For example, the storage unit 216 stores information for specifying the terminal device 53 for which a contract has been made, information for specifying the contents of
15 the contract, and information for specifying the usage conditions of a service in the terminal device 53. The information for specifying the terminal device 53 may include, for example, an address of an email of the terminal device 53.

When seen from a management subject providing a file analysis service by the analysis unit 11, a management subject of the terminal device 53 for which a contract
20 related to the service has been made is a customer. Management subjects of the plurality of terminal portions 21 to 23 may be different customers.

[0055]

[File]

Fig. 3 is a diagram showing a schematic configuration example of a file 1011
25 according to the embodiment of the present invention.

The file 1011 includes a header and a plurality of pieces of log information.

The log information may include one or more pieces of information among, for example, the date and time of occurrence or the like, a signature, information for identifying a transmission source, information for identifying a transmission destination, an error code, and the like. As the information for identifying a transmission source and the information for identifying a transmission destination, for example, an Internet Protocol (IP) address may be used. These pieces of information may be included in, for example, the header.

In addition, the header may include, for example, an address of an email of the terminal device 53.

[0056]

Meanwhile, in the example of Fig. 3, a configuration example in which a plurality of pieces of log information are distinctively included in the file 1011 has been described. However, as another example, one group of log information may be regarded as being included in the file 1011.

Further, in a case where a plurality of files 1011 serves as a group of objects to be analyzed once, for example, information for specifying such a group may be included in a header of each of the files 1011.

[0057]

Fig. 4 is a diagram showing an example of information representing a file analysis result according to the embodiment of the present invention.

Fig. 4 shows an example of a display content 2011 displayed on a screen by the display unit 214 of the terminal device 53 on the basis of a Web page provided by the Web server device 42.

In the example of Fig. 4, character information of "No problem has been

detected" is displayed as "a result of file analysis" in the display content 2011. That is, as a result of file analysis, a case where no problem has been detected is shown.

Meanwhile, the display content 2011 in such a case may be any of other contents.

[0058]

5 Fig. 5 is a diagram showing another example of information representing a file analysis result according to the embodiment of the present invention.

Fig. 5 shows an example of a display content 2111 displayed on a screen by the display unit 214 of the terminal device 53 on the basis of a Web page provided by the Web server device 42. In the example of Fig. 5, character information of "the following
10 problem has been detected" is displayed as "a result of file analysis" in the display content 2111. That is, as a result of file analysis, a case where a problem has been detected is shown. In this case, the contents of such a display may be regarded as a warning (alert). Meanwhile, the display content 2111 in such a case may be any of other contents.

15 Meanwhile, the "problem" in the result of file analysis may be referred to as, for example, "incident", "abnormality", or the like.

[0059]

[Reduction in Logs To Be Analyzed: Unnecessary Log Reduction Process]

The log reduction unit 234 reduces logs to be analyzed by reducing unnecessary
20 logs among logs acquired by the log acquisition unit 231.

In the present embodiment, information for specifying logs that are not required to be analyzed is stored in the storage unit 216 in the terminal device 53.

[0060]

Here, logs that are not required to be analyzed may be determined arbitrarily.

25 As an example, logs that are not required to be analyzed may be determined

using a list including information for specifying one or more logs that are not required to be analyzed. The list may be referred to as a white list. The log reduction unit 234 reduces logs that are not required to be analyzed from objects to be analyzed among logs acquired by the log acquisition unit 231 on the basis of the contents of the list.

5 [0061]

[Reduction in Logs To Be Analyzed: Log Range Reduction Process]

In the present embodiment, file conditions include an upper limit value of the amount of data of logs that can be analyzed at least once.

In the present embodiment, in the terminal device 53, the file condition
10 determination unit 233 determines whether or not the sum of the amount of data of logs serving as candidates for objects to be analyzed once is equal to or less than a predetermined upper limit value by using the logs as logs to be determined.

As a result, in a case where the sum of the amount of data of the logs exceeds the predetermined upper limit value, the log reduction unit 234 reduces logs serving as
15 candidates for objects to be analyzed once by reducing some of the logs from the candidates.

[0062]

Meanwhile, in the present embodiment, the log reduction unit 234 deletes some of the logs serving as candidates for objects to be analyzed from the candidates, but some
20 of the logs are stored in the storage unit 151 of the log management device 52.

Further, in the present embodiment, a case where both an unnecessary log reduction process and a log range reduction process are performed has been described, but any one of the unnecessary log reduction process and the log range reduction process may be performed independently of the other one.

25 [0063]

Fig. 6 is a diagram showing an example of information representing the range of a log capable of being subjected to file analysis according to the embodiment of the present invention.

Fig. 6 shows an example of a display content 2211 displayed on a screen by the display unit 214 of the terminal device 53 in order to present the range of logs that can be analyzed once. The example of Fig. 6 shows that file analysis can be performed when a period is "2018/7/10 13:00 to 2018/7/12 15:45" and a sensor is a "sensor A".

[0064]

Here, the period indicates a period in which the date and time when a log is generated should be included. The "2018/7/10 13:00 to 2018/7/12 15:45" shown in Fig. 6 indicates a period from 13:00 on July 10, 2018 to 15:45 on July 12, 2018.

In the example of Fig. 6, the period is a group of continuous periods, but two or more discrete groups of periods may be used.

In general, when the range of a period is shortened from the range of a certain period, the total amount of data of logs is also decreased.

[0065]

The sensor indicates a sensor that detects logs. The "sensor A" shown in Fig. 6 indicates, for example, a sensor of the log detection device 51.

Meanwhile, as the sensor, for example, one sensor may be designated, or two or more sensors may be designated. In general, when the number of sensors is decreased from a certain number of sensors, the total amount of data of logs is also decreased.

[0066]

In the present embodiment, in the terminal device 53, the file condition acquisition unit 232, the file condition determination unit 233, and the log reduction unit 234 automatically execute respective processes even when any explicit instruction is not

given from a user. Thereby, in the terminal device 53, logs to be analyzed are automatically reduced before a file to be subjected to file analysis is generated. In addition, the display content 2211 shown in Fig. 6 is displayed to the user. That is, the range of logs that can be analyzed in terms of the amount of data is presented to the user as a recommended range of logs.

[0067]

Here, in the terminal device 53, for example, conditions of the range of logs to be displayed in the early stage are set. The conditions may be any conditions.

Information for specifying the conditions is stored in the storage unit 216.

For example, regarding the conditions, a point in time of termination may be determined with respect to a period from the start to the termination. As an example, the point in time of termination may be set on the basis of a rule which is set at a point in time when a process of displaying the range of logs in the early stage (that is, at the present point in time) is performed or a rule which is set at a point in time by a predetermined time before the point in time. In this case, the log reduction unit 234 can set a log at the set point in time of termination as the latest log and can extract logs having a predetermined amount of data as objects to be analyzed by going back to an older log (at the point in time of start) from the log.

In addition, for example, regarding the conditions, predetermined one or more sensors may be determined with respect to the sensor. As an example, the predetermined sensor may be set on the basis of a rule that the sensor is set to be the "sensor A" which is determined in advance.

[0068]

In addition, the terminal device 53 may change a portion or the entirety of the range of logs by the control unit 217 in response to an operation of the operation unit 213

which is performed by the user.

In this case, in the control unit 217, the change performed by the user's operation is approved in a case where the file condition determination unit 233 determines that the range of logs which is changed by the user's operation is within the range of logs that can be analyzed once.

[0069]

On the other hand, in the control unit 217, logs are reduced by the log reduction unit 234 in a case where the file condition determination unit 233 determines that the range of logs which is changed by the user's operation exceeds the range of logs that can be analyzed once. In this case, the log reduction unit 234 does not perform change with respect to, for example, a location changed by the user's operation. That is, the user's change is preferentially performed. Further, in the control unit 217, the range of logs which is obtained as a result of the reduction in logs is displayed on the screen of the display unit 214.

Meanwhile, in a case where the file conditions are not satisfied when any change is not made to a location changed by the user's operation, the control unit 217 may display information indicating an error on the screen of the display unit 214.

[0070]

With such a configuration, for example, an appropriate range of logs is presented by the terminal device 53 even when the range of logs that can be analyzed once is not ascertained, so that the user can use such a range of logs.

In addition, for example, even when a user changes the range of logs which is presented by the terminal device 53 to an impossible range of logs in response to the user's desire, a new range of logs is presented due to the range of logs being adjusted again by the terminal device 53, which leads to an extreme convenience.

[0071]

The display content 2211 shown in Fig. 6 includes a predetermined button 2221 indicating "uploading".

The user can press the button 2221 (for example, clicking using a mouse, or the like) on a screen by operating the operation unit 213 of the terminal device 53. When the button 2221 is pressed, the range of logs displayed at that point in time is adopted, so that a file including logs in the range is generated, and the generated file is transmitted to the file analysis device 41 through the network 31 from the terminal device 53.

[0072]

Meanwhile, in the present embodiment, a "period " and a "sensor" are used as parameters for determining the range of logs, but other parameters may be used.

[0073]

[Content of Contract]

Fig. 7 is a diagram showing an example of contract information 3011 according to the embodiment of the present invention.

In the example of Fig. 7, the contract information 3011 includes identification information of a customer and contents of a contract which are associated with each other. The contents of a contract include, for example, the number of times, a capacity, a period, and the like.

Meanwhile, in the example of Fig. 7, the contract information 3011 includes contents of a contract of a customer and conditions of usage related to the contents of the contract. As another example, contents of a contract of a customer and conditions of usage related to the contents of the contract may be managed separately.

[0074]

The identification information of the customer may be, for example, number

information. In the present embodiment, the terminal device 53 of each of customers is identified by identification information of the customer. In the example of Fig. 7, information such as "001", "002", and "003" is used as the identification information.

[0075]

5 The number of times indicates a maximum number of times a file analysis service can be received, with respect to the terminal device 53 of each of the customers. In the example of Fig. 7, information such as "2/10" is used as the number of times. For example, "2/10" indicates that a maximum number of times is 10 and two times thereof have already been performed

10 The capacity indicates a total capacity of the amount of data with which a file analysis service can be received, with respect to the terminal device 53 of each of the customers. In the example of Fig. 7, information such as "300/1000" is used as the capacity. For example, "300/1000" indicates that a maximum capacity is 1000 Gbytes and a service of 300 Gbytes has already been performed. The period indicates a period
15 in which a file analysis service can be received, with respect to a terminal device 53 of each of the customers. In the example of Fig. 7, information such as "2018/1/1 to 2018/12/31" is used as the period. For example, "2018/1/1 to 2018/12/31" indicates that a period from January 1, 2018 to December 31, 2018 is an effective period.

[0076]

20 In the present embodiment, in the file analysis device 41, the management unit 116 manages the contract information 3011. For example, the contract information 3011 is stored in the storage unit 111.

 Further, in the present embodiment, in the terminal device 53, information corresponding to the customer of the terminal device 53 in the contract information 3011
25 is stored in the storage unit 216. That is, in the file analysis device 41, information

regarding a plurality of customers is managed, but information regarding the customer is managed in the terminal device 53 of each of the customers.

[0077]

[Access to File Analysis Device from Terminal Device]

5 A method of accessing the file analysis device 41 from the terminal device 53 is not particularly limited.

As an example, the terminal device 53 accesses a Web page which can be viewed by a management subject providing a file analysis service by the analysis unit 11. The Web page may be provided by, for example, the Web server device 42.

10 The terminal device 53 may access the Web page in response to, for example, an operation of the operation unit 213 which is performed by the user.

Further, for example, in a case where a contract for receiving a file analysis service is made, the terminal device 53 may be accessed by the file analysis device 41. In this case, in the file analysis device 41, information for specifying the terminal device 53 is stored in the storage unit 111, and the management unit 116 accesses the terminal

15 device 53 on the basis of the information.

[0078]

In the file analysis service, the terminal device 53 and the file analysis device 41 may execute a process on demand. For example, a process for satisfying a request made

20 by the terminal device 53 may be executed by the file analysis device 41 in response to the request.

[0079]

[Dedicated Tool for File Analysis]

The terminal device 53 may include a dedicated tool for receiving a file analysis

25 service (for convenience of description, also referred to as a "dedicated tool"). The

dedicated tool may be software. The software may be a program.

In the terminal device 53, the software may be stored in, for example, the storage unit 216. Further, in the terminal device 53, a process is performed on the basis of contents of the software.

5 [0080]

The dedicated tool is distributed to a management subject of the terminal device 53, for example, by a management subject providing a file analysis service by the analysis unit 11. For example, the dedicated tool may be stored in a recording medium and distributed or may be transmitted (downloaded) to the terminal device 53 through the
10 network 31 from the file analysis device 41 or the like. In the terminal device 53, for example, a program which is the dedicated tool is installed so as to be usable.

For example, the dedicated tool may be distributed free of charge or may be distributed for a fee.

In addition, for example, the dedicated tool may be distributed to a person who
15 has made a contract for receiving a file analysis service or may be distributed to any person even when the person has not made such a contract.

[0081]

In the terminal device 53, the file analysis device 41 may be accessed using a function of a dedicated tool in a case where the dedicated tool is included. A destination
20 of the access may be a predetermined Web page.

Further, in the terminal device 53, in a case where a dedicated tool is included, communication from the file analysis device 41 to the terminal device 53 may be communication using an email or communication using a Web push notification.

[0082]

25 In the example of Fig. 2, the function of the file condition acquisition unit 232

and the function of the file condition determination unit 233 in the terminal device 53 may be included in functions realized by, for example, a dedicated tool. In this case, for example, in a state where the dedicated tool is not included in the terminal device 53, the function of the file condition acquisition unit 232 and the function of the file condition
5 determination unit 233 may not be provided in the terminal device 53.

In this case, in the terminal device 53, for example, when the same process as these functions is performed, the process is performed in response to an operation of the operation unit 213 which is performed by the user. That is, the same process as these functions is performed by the user's manual operation.

10 [0083]

Similarly, in the example of Fig. 2, the function of the log reduction unit 234 in the terminal device 53 may be included in, for example, functions realized by a dedicated tool. In this case, for example, in a state where a dedicated tool is not provided in the terminal device 53, the function of the log reduction unit 234 may not be provided in the
15 terminal device 53.

In this case, in the terminal device 53, for example, when the same process as the function is performed, the process is performed in response to an operation of the operation unit 213 which is performed by the user. That is, the same process as the function is performed by the user's manual operation.

20 [0084]

In addition, similarly, in the example of Fig. 2, one or more of the function of the compression unit 236, the function of the encoding unit 237, the function of the analysis request availability determination unit 239, and the function of the file generation unit 235 in the terminal device 53 may be included in, for example, functions
25 realized by a dedicated tool. In this case, for example, in a state where a dedicated tool

is not provided in the terminal device 53, a corresponding function may not be provided in the terminal device 53.

In this case, in the terminal device 53, for example, when the same process as the function is performed, the process is performed in response to an operation of the operation unit 213 which is performed by the user. That is, the same process as the function is performed by the user's manual operation.

[0085]

In addition, a dedicated tool may realize other functions.

Here, in a case where information to be referred to by the dedicated tool in order to realize a predetermined function is stored in the storage unit 216 or the like and managed, the information may be automatically updated in response to, for example, a request from the file analysis device 41 or the like. The information may be, for example, information of a white list. The information in the terminal device 53 may be periodically updated, for example, or automatically updated when there is a change in the information being the source of the information. Thereby, the information is shared between the terminal device 53 and the file analysis device 41 so as to be maintained to be the same information, and is maintained to be up-to-date information. Updating of the information may be performed by, for example, a dedicated tool.

[0086]

The dedicated tool may have a function of performing compression in a peculiar format as the function of the compression unit 236. In this case, the file analysis device 41 has a function of performing decompression in a format suitable for the format as the function of the decompression unit 132. In the file analysis system 1, such a peculiar format is used, and thus it is possible to reduce a security risk.

As an example, the dedicated tool may write predetermined information in a

header or the like capable of being read out even when a compressed file is not decompressed when the file is compressed in a peculiar format. In this case, in the file analysis device 41, in a case where the file inspection unit 113 determines that the predetermined information included in the compressed file is information which is determined in advance, the compressed file is regarded as being safe. The predetermined information may be any information, and for example, is information indicating that the information has been compressed by the dedicated tool.

[0087]

Similarly, the dedicated tool may have a function of performing encoding in a peculiar format as the function of the encoding unit 237. In this case, the file analysis device 41 has a function of performing decoding in a format suitable for the format as the function of the decoding unit 131. In the file analysis system 1, such a peculiar format is used and thus it is possible to reduce a security risk.

[0088]

Similarly, the dedicated tool may have a function of generating a file in a peculiar format as the function of the file generation unit 235. In this case, in the file analysis device 41, the file inspection unit 113 inspects whether or not such a peculiar format has been used. In this case, in the file analysis device 41, such a peculiar format is used, and thus it is possible to reduce a security risk.

[0089]

As the dedicated tool, for example, tools having a plurality of different functions, such as a tool having a function of determining file conditions, a tool having a function of reducing logs, a tool having a function of performing compression, and a tool having a function of performing encoding, may be provided separately, or a tool having a combination of two or more of these tools may be provided.

In addition, as the dedicated tool, a tool having both a compression function and a decompression function may be provided. In addition, as the dedicated tool, a tool having both an encoding function and a decoding function may be provided.

[0090]

5 In the file analysis system 1, a file to be analyzed is generated by a dedicated tool in the terminal device 53, so that, for example, it becomes easy to secure a state where the file to be transmitted from the terminal device 53 to the file analysis device 41 satisfies predetermined inspection conditions. That is, it is easier to adapt to the predetermined inspection conditions in a case where a file is generated by a dedicated
10 tool provided exclusively than in a case where a file is generated in response to any operation performed by the user. That is, a configuration in which a file satisfying the predetermined inspection conditions is generated by a dedicated tool is adopted, and thus it is possible to omit file inspection to be performed by the file inspection unit 113 in the file analysis device 41 or reduce a burden required for the file inspection. Thereby, it is
15 possible to simplify file inspection to be performed by the file inspection unit 113 in the file analysis device 41.

[0091]

Here, an example in which control using the display content 2211 shown in Fig. 6 is performed by a dedicated tool will be described.

20 It is assumed that a frame using a dedicated tool is displayed on the screen of the display unit 214 in the terminal device 53. In this case, an icon of information to be analyzed is dragged and dropped onto the frame in response to an operation of the operation unit 213 which is performed by the user. The icon may be, for example, an icon indicating a log file of a security sensor.

25 Then, the dedicated tool reads logs to be analyzed and deletes a row

(unnecessary log) which is unnecessary for analysis from the logs on the basis of a white list. In addition, the dedicated tool cuts out a log retroactively from a log on the latest date and time as necessary so that a log to be analyzed falls within a predetermined size and does not become oversized. In this case, the dedicated tool calculates the range of the date and time of a log and displays the calculated range on the screen of the display unit 214. The user confirms displayed contents (in the example of Fig. 6, the display content 2211) and performs an operation of pressing the button 2221 for uploading. Accordingly, the dedicated tool compresses a file including the log to be analyzed in a peculiar format and transmits the compressed file to the file analysis device 41. The file analysis device 41 performs inspection and analysis on the received file and gives a notification.

In this manner, it is possible to transmit a file of which the size is limited to the file analysis device 41 using the dedicated tool through the user's simple operation.

For example, the dedicated tool may be in a form of being used by uploading or processing a file on a browser.

[0092]

[Process Performed in File Analysis System]

Fig. 8 is a diagram showing an example of a procedure of processing performed in the terminal device 53 according to the embodiment of the present invention.

In the example of Fig. 8, a case where the terminal device 53 uses a file analysis service on the basis of a manual operation performed by a user is shown.

In the present example, a case where the functions of the file condition acquisition unit 232, the file condition determination unit 233, and the log reduction unit 234 are turned off (invalidated) or a case where the functions are not provided in the terminal device 53 is shown.

[0093]

(Step S1)

In the terminal device 53, the operation unit 213 receives and acquires contents of an operation performed by the user. In addition, the processing proceeds to the

5 process of step S2. In the present example, the operation is an operation for using a file analysis service.

[0094]

(Step S2)

In the terminal device 53, the file generation unit 235 generates a file to be
10 subjected to file analysis on the basis of the acquired contents of the operation. In addition, the processing proceeds to the process of step S3.

Here, in the terminal device 53, either one or both of compression performed by the compression unit 236 and encoding performed by the encoding unit 237 may be performed with respect to the generated file.

15 [0095]

(Step S3)

In the terminal device 53, the control unit 217 transmits the generated file to the file analysis device 41 through the network 31 by the communication unit 215. In addition, the processing proceeds to the process of step S4.

20 Thereby, the file analysis device 41 performs processing of inspection and analysis on the file received from the terminal device 53 and gives a notification to the terminal device 53.

Meanwhile, the terminal device 53 may transmit the file in response to, for example, the reception of the user's predetermined operation by the operation unit 213.

25 [0096]

(Step S4)

In the terminal device 53, the notification control unit 238 receives the notification given from the file analysis device 41. Thereafter, in the terminal device 53, the notification control unit 238 displays contents of the received notification on the screen of the display unit 214. In addition, the processing in this flow is terminated. Thereby, the user can ascertain the contents of the notification, that is, can ascertain a result of the file analysis.

[0097]

Fig. 9 is a diagram showing an example of a procedure of processing performed in the terminal device 53 according to the embodiment of the present invention.

In the example of Fig. 9, a case where the terminal device 53 uses a file analysis service on the basis of a predetermined rule (for convenience of description, also referred to as a "file generation rule") is shown. The file generation rule is stored in, for example, the storage unit 216. The file generation rule is a rule for generating a file, and for example, one or more rules of a timing when a file is generated, the range of logs included in the file, and the like may be included.

In the present example, a case where the functions of the file condition acquisition unit 232, the file condition determination unit 233, and the log reduction unit 234 are turned off (invalidated) or a case the functions are not provided in the terminal device 53 is shown.

[0098]

(Step S21)

In the terminal device 53, the file generation unit 235 reads out and acquires a file generation rule. In addition, the processing proceeds to the process of step S22.

[0099]

(Step S22)

In the terminal device 53, the file generation unit 235 generates a file to be subjected to file analysis on the basis of contents of the acquired file generation rule. In addition, the processing proceeds to the process of step S23.

5 Here, in the terminal device 53, either one or both of compression performed by the compression unit 236 and encoding performed by the encoding unit 237 may be performed with respect to the generated file.

[0100]

(Step S23)

10 In the terminal device 53, the control unit 217 transmits the generated file to the file analysis device 41 through the network 31 by the communication unit 215. In addition, the processing proceeds to the process of step S24.

Thereby, the file analysis device 41 performs processing of inspection and analysis on the file received from the terminal device 53 and gives a notification to the
15 terminal device 53.

[0101]

(Step S24)

In the terminal device 53, the notification control unit 238 receives the notification given from the file analysis device 41. Thereafter, in the terminal device
20 53, the notification control unit 238 displays contents of the received notification on the screen of the display unit 214. In addition, the processing in this flow is terminated. Thereby, the user can ascertain the contents of the notification, that is, can ascertain a result of the file analysis.

[0102]

25 Fig. 10 is a diagram showing an example of a procedure of processing

performed in the terminal device 53 according to the embodiment of the present invention.

In the example of Fig. 10, the terminal device 53 generates a file appropriate for predetermined file conditions. Meanwhile, any processes may be used as processes

5 before and after the file generation.

In the present example, a case where the functions of the file condition acquisition unit 232, the file condition determination unit 233, and the log reduction unit 234 are provided in the terminal device 53 and turned on (validated) is shown.

[0103]

10 (Step S41)

In the terminal device 53, the file generation unit 235 generates a file on the basis of logs acquired by the log acquisition unit 231. In addition, the processing proceeds to the process of step S42. In the present example, the file is a file which is temporarily generated to determine whether or not the file is appropriate for file

15 conditions.

[0104]

(Step S42)

In the terminal device 53, the file condition acquisition unit 232 acquires file conditions. In addition, the processing proceeds to the process of step S43.

20 [0105]

(Step S43)

In the terminal device 53, the file condition determination unit 233 determines whether or not the generated file satisfies the file conditions.

As a result, in the terminal device 53, in a case where the file condition
25 determination unit 233 determines that the generated file satisfies the file conditions (step

S43: YES), the processing in this flow is terminated. In this case, the generated file is decided to be a candidate for an object to be analyzed, and the range of logs corresponding thereto is presented to the user (for example, the example of Fig. 6).

When the range of the logs is approved by the user, the file is decided to be an object to
5 be analyzed.

On the other hand, in the terminal device 53, in a case where the file condition determination unit 233 determines that the generated file does not satisfy the file conditions (step S43: NO), the processing proceeds to the process of step S44.

[0106]

10 (Step S44)

In the terminal device 53, the log reduction unit 234 reduces logs included in the file. In addition, the processing proceeds to the process of step S41.

Meanwhile, in the present example, a case where a process of determining whether or not a file generated again after the reduction in logs satisfies file conditions is
15 performed is shown, but the processing in this flow may be terminated after the process of step S44 in a configuration in which logs are reduced so that a generated file satisfies file conditions.

[0107]

Fig. 11 is a diagram showing an example of a procedure of processing

20 performed in the terminal device 53 according to the embodiment of the present invention.

In the example of Fig. 11, the terminal device 53 determines whether or not a request for file analysis can be made. Meanwhile, the processing in this flow may be performed at any timing when a process for receiving a file analysis service is performed
25 in the terminal device 53.

In the present example, a case where the analysis request availability determination unit 239 is included in the terminal device 53 and turned on (validated) is shown. Meanwhile, in a case where the analysis request availability determination unit 239 is turned off (invalidated) or in a case where the analysis request availability determination unit 239 is not included in the terminal device 53, the processing in this flow is not performed.

[0108]

(Step S61)

In the terminal device 53, the analysis request availability determination unit 239 determines whether or not a request for file analysis can be made. In this case, the analysis request availability determination unit 239 may determine whether or not a request for file analysis can be made on the basis of, for example, the same information as the contract information 3011. The information may be stored in, for example, the storage unit 216 and managed by the analysis request availability determination unit 239.

As a result, in the terminal device 53, in a case where the analysis request availability determination unit 239 determines that a request for file analysis can be made (step S61: YES), the processing in this flow is terminated. On the other hand, in the terminal device 53, in a case where the analysis request availability determination unit 239 determines that a request for file analysis cannot be made (step S61: NO), the processing proceeds to the process of step S62.

[0109]

(Step S62)

In the terminal device 53, the analysis request availability determination unit 239 stops the process for receiving a file analysis service. In this case, the analysis request availability determination unit 239 may display the stopping of the process on the

screen of the display unit 214. In addition, the processing in this flow is terminated.

Meanwhile, thereafter, a process for receiving a file analysis service may be performed again in the terminal device 53.

[0110]

5 Fig. 12 is a diagram showing an example of a procedure of processing performed in the file analysis device 41 according to the embodiment of the present invention.

[0111]

(Step S101)

10 In the file analysis device 41, an analysis target file transmitted from the terminal device 53 is received by the reception unit 121. In addition, the processing proceeds to the process of step S102.

[0112]

(Step S102)

15 In the file analysis device 41, the file inspection unit 113 determines whether or not the received file satisfies predetermined inspection conditions.

As a result, in the file analysis device 41, in a case where the file inspection unit 113 determines that the received file satisfies predetermined inspection conditions (step S102: YES), the processing proceeds to the process of step S103.

20 On the other hand, in the file analysis device 41, in a case where the file inspection unit 113 determines that the received file does not satisfy predetermined inspection conditions (step S102: NO), the processing proceeds to the process of step S104.

[0113]

25 (Step S103)

In the file analysis device 41, the file analysis unit 114 analyzes an inspected file on the basis of analysis conditions. In addition, the processing proceeds to the process of step S104.

[0114]

5 (Step S104)

In the file analysis device 41, the notification unit 115 gives a notification to the terminal device 53.

Here, in a case where the file inspection unit 113 determines that a file does satisfy inspection conditions, the notification unit 115 notifies the terminal device 53 of
10 information indicating that the file does satisfy the inspection conditions.

Further, in a case where the file analysis unit 114 determines that the file has no problem, the notification unit 115 notifies the terminal device 53 of information indicating that the file has no problem.

Further, in a case where the file analysis unit 114 determines that the file has a
15 problem, the notification unit 115 notifies the terminal device 53 of information indicating that the file has a problem.

[0115]

<Modification Example>

A modification example will be described with reference to Fig. 13.

20 Fig. 13 is a diagram showing an example of a procedure of processing performed in the file analysis device 41 according to the embodiment of the present invention.

In the present example, a case where the file analysis unit 114 has a function of determining whether or not a file satisfies file conditions and a function of reducing logs
25 included in the file in the file analysis device 41 is shown.

In the present example, information for specifying file conditions is stored in the storage unit 111.

In the present example, it is particularly effective in a case where the functions of the file condition acquisition unit 232, the file condition determination unit 233, and the log reduction unit 234 are turned off (invalidated) in the terminal device 53 or a case where the functions are not provided in the terminal device 53. Meanwhile, the processing in this flow may be applied in a case where the functions of the file condition acquisition unit 232, the file condition determination unit 233, and the log reduction unit 234 are not provided in the terminal device 53 and turned on (validated).

10 In the present example, it is assumed that the contents of the inspection conditions do not include the contents of the file conditions. Meanwhile, the contents of the inspection conditions may include a portion of the contents of the file conditions.

[0116]

(Step S121)

15 In the file analysis device 41, an analysis target file transmitted from the terminal device 53 is received by the reception unit 121. In addition, the processing proceeds to the process of step S122.

[0117]

(Step S122)

20 In the file analysis device 41, the file inspection unit 113 determines whether or not the received file satisfies predetermined inspection conditions.

As a result, in the file analysis device 41, in a case where the file inspection unit 113 determines that the received file satisfies predetermined inspection conditions (step S122: YES), the processing proceeds to the process of step S123.

25 On the other hand, in the file analysis device 41, in a case where the file

inspection unit 113 determines that the received file does not satisfy predetermined inspection conditions (step S122: NO), the processing proceeds to the process of step S126.

[0118]

5 (Step S123)

In the file analysis device 41, the file analysis unit 114 acquires file conditions. Thereafter, in the file analysis device 41, the file analysis unit 114 determines whether or not an inspected file satisfies the file conditions.

As a result, in the file analysis device 41, in a case where the file analysis unit
10 114 determines that the inspected file satisfies the file conditions (step S123: YES), the processing proceeds to the process of step S125. In this case, the file becomes an analysis target.

On the other hand, in the file analysis device 41, in a case where the file analysis unit 114 determines that the inspected file does not satisfy the file conditions (step S123:
15 NO), the processing proceeds to the process of step S124.

[0119]

(Step S124)

In the file analysis device 41, the file analysis unit 114 reduces logs included in the inspected file. In addition, the processing proceeds to the process of step S125. In
20 this case, a file including logs after the reduction becomes an analysis target.

Meanwhile, in the present example, the file analysis unit 114 reduces logs so that the file including logs after the reduction satisfies the file conditions.

[0120]

(Step S125)

25 In the file analysis device 41, the file analysis unit 114 analyzes the file to be

analyzed on the basis of analysis conditions. In addition, the processing proceeds to the process of step S126.

[0121]

(Step S126)

5 In the file analysis device 41, the notification unit 115 gives a notification to the terminal device 53.

Here, in a case where the file inspection unit 113 determines that a file does not satisfy inspection conditions, the notification unit 115 notifies the terminal device 53 of information indicating that the file does not satisfy the inspection conditions.

10 Further, in a case where the file analysis unit 114 determines that the file has no problem, the notification unit 115 notifies the terminal device 53 of information indicating that the file has no problem.

Further, in a case where the file analysis unit 114 determines that the file has a problem, the notification unit 115 notifies the terminal device 53 of information
15 indicating that the file has a problem.

Further, in a case where the file analysis unit 114 reduces logs, the notification unit 115 notifies the terminal device 53 of information indicating that the logs have been reduced. The information may include, for example, either one or both of information for specifying the reduced logs and information for specifying logs that have not been
20 reduced. Thereby, in a case where logs to be analyzed have been reduced by the file analysis device 41, the user of the terminal device 53 can ascertain the reduction in logs.

[0122]

Here, the file condition determination process and the log reduction process in the file analysis device 41 may be the same as, for example, a file condition
25 determination process and a log reduction process in the terminal device 53. That is, in

the present example, even when the file condition determination process and the log reduction process are not performed in the terminal device 53, the file condition determination process and the log reduction process are performed in the file analysis device 41.

5 Meanwhile, in a case where there are file conditions used in the file analysis device 41 and file conditions used in the terminal device 53, for example, these file conditions may be the same or may be partially or entirely different from each other.
[0123]

 Further, in the present example, a case where the file analysis unit 114 performs
10 a file condition determination process and a log reduction process in the file analysis device 41 has been described. However, as another example, the file inspection unit 113 may perform a file condition determination process and a log reduction process instead of the file analysis unit 114. In this case, contents of inspection conditions may include a portion or the entirety of contents of file conditions. In a case where the
15 contents of the inspection conditions include the entirety of the contents of the file conditions, only the inspection conditions may be determined, and the file conditions are not required to be determined.
[0124]

<Modification Example>

20 A modification example will be described with reference to Fig. 14.

 Fig. 14 is a diagram showing an example of a procedure of processing performed in the file analysis device 41 according to the embodiment of the present invention.

 In the present example, the file analysis device 41 recommends the terminal
25 device 53 to use a file analysis service at a predetermined timing (for convenience of

description, also referred to as an "analysis recommendation timing"). The analysis recommendation timing may be any timing, or may be, for example, a regular timing.

In the present example, information for specifying the analysis recommendation timing is stored in the storage unit 111.

5 [0125]

(Step S141)

In the file analysis device 41, the management unit 116 determines whether or not the analysis recommendation timing has arrived. In this case, the management unit 116 may refer to, for example, information of a timepiece function (not shown) provided
10 inside or outside the file analysis device 41.

As a result, in the file analysis device 41, in a case where the management unit 116 determines that the analysis recommendation timing has arrived (step S141: YES), the processing proceeds to the process of step S142.

On the other hand, in the file analysis device 41, in a case where the
15 management unit 116 determines that the analysis recommendation timing has not arrived (step S141: NO), the processing in this flow is terminated.

[0126]

(Step S142)

In the file analysis device 41, the management unit 116 notifies the terminal
20 device 53 of information indicating that the analysis recommendation timing has arrived by the notification unit 115. In addition, the processing in this flow is terminated.

Meanwhile, the processing in this flow may be performed, for example, at fixed time intervals.

25 In addition, any method may be used as a method of giving a notification to the

terminal device 53 by the notification unit 115.

[0127]

Here, in the terminal device 53, in a case where the file analysis device 41 recommends (notifies) that the analysis recommendation timing has arrived, information
5 indicating that the analysis recommendation timing has arrived may be displayed on the screen of the display unit 214. In this case, the user can ascertain that the analysis recommendation timing has arrived.

Further, in the terminal device 53, in a case where the file analysis device 41 recommends (notifies) that the analysis recommendation timing has arrived, a process for
10 receiving a file analysis service (for example, the processing in the flow shown in Fig. 9) may be automatically performed without the user's operation, as another example.

[0128]

Fig. 15 is a diagram showing an example of a hardware configuration of an information processing device 4001 according to the embodiment of the present
15 invention.

The information processing device 4001 having a hardware configuration as shown in Fig. 15 may be used as the terminal device 53, the file analysis device 41, or the like in the present embodiment.

[0129]

20 In the example of Fig. 15, the information processing device 4001 includes a processor 4011, an operation unit 4012, a display unit 4013, a storage device 4014, a memory 4015, an input and output interface 4016, a network interface 4017, and a bus 4021 for connecting these components to each other.

[0130]

25 The processor 4011 is constituted by a central processing unit (CPU) or the like,

and executes a program to execute a process specified in the program.

The operation unit 4012 includes one or more input devices of a keyboard, a mouse, and the like, and receives an operation performed by a user (person).

The display unit 4013 includes a screen, and displays and outputs information to
5 the screen.

[0131]

The storage device 4014, which is a non-volatile storage unit, is constituted by, for example, a hard disk or the like, and stores information.

The memory 4015, which is a volatile storage unit, is constituted by a random
10 access memory (RAM) or the like, and temporarily stores information. As the RAM, for example, a dynamic random access memory (DRAM) may be used.

The storage device 4014 or the memory 4015 may store, for example, information of programs executed by the processor 4011.

[0132]

15 The input and output interface 4016 is an interface which is connected to an external recording medium and the like.

The network interface 4017 is an interface which is connected to an external network.

[0133]

20 Here, the information processing device 4001 may include one processor or may include two or more processors as the processor 4011. As an example, the information processing device 4001 includes a plurality of CPUs each of which executes a process, and the plurality of CPUs may realize the entire process in cooperation.

[0134]

25 [Conclusion of Embodiment]

As described above, in the file analysis system 1 according to the present embodiment, the terminal device 53 transmits a file including logs to be analyzed to the file analysis device 41, so that it is possible to receive a notification of a result obtained by analyzing the logs by the file analysis device 41. For this reason, in the file analysis system 1 according to the present embodiment, even when initial settings for setting a system analyzing logs to be in an operable state are not performed, it is possible to easily analyze the logs and to easily realize a log analysis service.

[0135]

For example, even when sensor setting and network settings are not performed, the user of the terminal device 53 transmits a file including logs of a security sensor from the terminal device 53 to the file analysis device 41, and thus it is possible to evaluate or confirm the accuracy of analysis of a monitoring function.

In general, a security sensor monitors logs at all times. However, in the file analysis system 1 according to the present embodiment, a file including logs desired to be analyzed may be transmitted from the terminal device 53 to the file analysis device 41, and it is possible to easily attempt a file analysis service.

[0136]

Further, in the file analysis system 1 according to the present embodiment, for example, the terminal device 53 can also receive a file analysis service only in a period in which a security risk is increased.

For example, in the terminal device 53, when a large-scale new virus is generated, it is possible to receive a file analysis service for logs in the past predetermined period from that time. The predetermined period may be a period such as the past two weeks. Further, in the terminal device 53, as an opportunity for receiving the service, for example, the service may be received in response to an

operation performed by the user, the service may be received on the basis of a rule related to the generation of a new virus which is set in advance, or the service may be received in response to a request given from the file analysis device 41.

[0137]

5 In the file analysis system 1 according to the present embodiment, in the terminal device 53, logs are reduced by the log reduction unit 234, so that the amount of data of logs included in a file transmitted from the terminal device 53 to the file analysis device 41 is reduced. Thereby, in the file analysis system 1 according to the present embodiment, for example, logs which are not required to be subjected to file analysis are
10 excluded in the terminal device 53, and thus it is possible to achieve an improvement in the efficiency of a file analysis service. Further, in the file analysis system 1 according to the present embodiment, for example, in a case where conditions of an upper limit value are imposed on the amount of data of logs included in a file to be analyzed, the logs are reduced in the terminal device 53 so that the conditions are satisfied, and thus it is
15 possible to smoothly perform a file analysis service.

[0138]

 In general, in the security sensor, since a data size of a log file is large, it is likely to take a long time to analyze the log file or conditions for restricting the capacity of analysis are not likely to be satisfied. However, in the file analysis system 1
20 according to the present embodiment, such problems can be solved. In the file analysis system 1 according to the present embodiment, for example, a burden on a file analysis service is reduced by restricting the amount of data of logs that can be analyzed, and thus it is possible to reduce a charge for a file analysis service to a low cost.

[0139]

25 Further, in the file analysis system 1 according to the present embodiment, for

example, a dedicated tool for receiving a file analysis service is used in the terminal device 53, so that it is possible to simplify an operation performed by the user of the terminal device 53. In addition, the dedicated tool is used, and thus it is possible to improve, for example, security.

5 Further, in the file analysis system 1 according to the present embodiment, on-demand communication is used between the terminal device 53 and the file analysis device 41, and thus it is possible to achieve, for example, a reduction in costs.

[0140]

[Type of Log]

10 In the present embodiment, a case where logs of a security sensor are used as logs to be subjected to file analysis has been described. Examples of the logs of the security sensor include a firewall (FW), a new generation firewall (NGFW), an intrusion prevention system (IPS), an intrusion detection system (IDS), a unified threat management (UTM), a Web application firewall (WAF), and the like.

15 [0141]

As an example, a device detecting a log may be a device of an invasion prevention system (IPS) that prevents illegal invasion in a computer network. For example, the device may detect a log likely to be related to illegality.

As another example, a device detecting a log may be a device of a firewall (FW) obstructing communication that should not be passed. For example, the device may
20 detect both a log likely to be related to illegality and a log which is not related to illegality.

Meanwhile, in general, comparing an IPS and a firewall with each other, there is a log for a signal having passed in the firewall, and thus the amount of data is easily
25 increased, and it can be said that the density of logs likely to have a problem is higher in

the IPS.

[0142]

As the logs to be subjected to file analysis, other logs can also be used.

Examples of other logs include an authentication log, an error log, a terminal scanning

5 log, a communication log, a program operating log, an application operation log, and the like.

Examples of the authentication log include logs such as Active Directory, Berkeley internet name domain (BIND), and domain name system (DNS).

Examples of the error log include a log such as WinEvt.

10 Examples of the terminal scanning log include logs such as anti-virus and an endpoint detection and response (EDR).

Examples of the communication log include logs such as Proxy, mail, File access, and database (DB) access.

15 Examples of the program operating log include logs such as a boot log and dmesg.

Examples of the application operation log include logs such as an event log and a specific log.

[0143]

20 In the present embodiment, a case where a log is used as an object to be subjected to file analysis has been described, but information other than a log can also be used as an object to be subjected to file analysis.

Examples of the information other than a log include information for setting an operating system (OS).

25 Examples of the information for setting an OS include registry information, and the like.

In addition, for example, a Web browsing history, an operation history, or a login history may be used.

[0144]

In the present embodiment, a case where logs of one type are detected by one
5 log detection device 51 has been described, but a configuration in which two or more log detection devices are included and logs of two or more types are detected may be used.

Meanwhile, for example, the log detection device may be provided outside the terminal device 53 or may be provided as an internal function of the terminal device 53.

[0145]

10 The log management device 52 may store information of logs detected by a plurality of log detection devices in the storage unit 151 and manage the stored information.

For example, information of logs of a plurality of different types may be stored and the like in a mixed form in time order. For example, information for identifying a
15 sensor that detects logs is added to the logs. The logs can be distinguished on the basis of the information. Thereby, information of logs of a predetermined type can be extracted from information in which the information of the logs of the plurality of different types are mixed.

[0146]

20 In the terminal device 53, for example, logs of one type may be included in a file to be analyzed, or logs of two or more types may be included in the file.

In the file analysis device 41, for example, file inspection of the file inspection unit 113 may be performed for each type of logs or may be performed collectively for logs of two or more types.

25 In the file analysis device 41, for example, file analysis of the file analysis unit

114 may be performed for each type of logs or may be performed collectively for logs of two or more types.

[0147]

<Configuration Example>

5 As a configuration example, a terminal device (in the present embodiment, the terminal device 53) includes a file generation unit (in the present embodiment, the file generation unit 235) which acquires logs among a plurality of logs output from a security sensor (in the present embodiment, the sensor of the log detection device 51) monitoring logs at all times and outputting the logs monitored at all times and generates a file
10 including the acquired logs, a file transmission unit (in the present embodiment, the communication unit 215) which transmits the file generated by the file generation unit to a file analysis device (in the present embodiment, the file analysis device 41), and a notification control unit (in the present embodiment, the notification control unit 238) which receives a notification of an analysis result of the file transmitted from the file
15 analysis device.

 As the configuration example, the terminal device includes an unnecessary log reduction unit (in the present embodiment, the function of the log reduction unit 234) which reduces the amount of data of logs included in a file by reducing unnecessary logs from the logs included in the file on the basis of information for specifying unnecessary
20 logs not required to be analyzed.

 As the configuration example, the terminal device includes a log range reduction unit (in the present embodiment, the function of the log reduction unit 234) which sets the amount of data of logs included in a file to be equal to or less than a predetermined upper limit value by reducing the range of the logs included in the file.

25 As the configuration example, the terminal device includes an analysis request

availability determination unit (in the present embodiment, the analysis request availability determination unit 239) which determines whether or not a request for file analysis can be made.

[0148]

5 As the configuration example, the file analysis device (in the present embodiment, the file analysis device 41) includes a reception unit (in the present embodiment, the reception unit 121) which receives a file transmitted from a terminal device (in the present embodiment, the terminal device 53), a file analysis unit (in the present embodiment, the file analysis unit 114) which analyzes the file received by the
10 reception unit, and a notification unit (in the present embodiment, the notification unit 115) which transmits a notification of a result obtained by analyzing the file by the file analysis unit to the terminal device. The file includes logs among a plurality of logs output from a security sensor (in the present embodiment, the sensor of the log detection device 51) monitoring logs at all times and outputting the logs monitored at all times.

15 As the configuration example, the file analysis device includes a management unit (in the present embodiment, the management unit 116) which manages charging information regarding analysis performed by the file analysis unit. The charging information includes information of an amount of money according to the number of times analysis is performed. The information of an amount of money based on the
20 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 of charge when the number of times analysis is performed is equal to or less than a predetermined number of times.

[0149]

25 Meanwhile, the present invention may be implemented in various modes, for

example, a device such as a terminal device or a file analysis device, a system such as a file analysis system, a method such as a file analysis method, a program, and a recording medium having a program recorded thereon. The recording medium may be, for example, a transitory recording medium.

5 [0150]

As described above, a process can be performed by recording (storing) a program for realizing the functions of the devices (for example, the terminal device 53, the file analysis device 41, and the like) according to the embodiment in a computer-readable recording medium (storage medium) and causing a computer system to read and
10 execute the program recorded in the recording medium.

Meanwhile, the "computer system" mentioned herein may be a system including hardware such as an operating system or peripheral equipment.

In addition, the "computer-readable recording medium" refers to a writable non-volatile memory such as a flexible disc, a magneto-optical disc, a read only memory
15 (ROM), or a flash memory, a portable medium such as a digital versatile disc (DVD), or a storage device such as a hard disk built into the computer system.

Further, the "computer-readable recording medium" may also include a medium holding a program for a fixed period of time, for example, a server in a case where the program is transmitted through a network such as the Internet or through a
20 communication line such as a telephone line, or a volatile memory inside the computer system serving as a client.

In addition, the above-described program may be transmitted to another computer system from a computer system in which the program is stored in a storage device or the like through a transmission medium or transmission waves in the
25 transmission medium. Here, the "transmission medium" transmitting the program refers

to a medium having a function of transmitting information, for example, a network (communication network) such as the Internet or a communication line (communication wire) such as a telephone line.

In addition, the above-described program may be a program for realizing some
 5 of the above-described functions. Further, the above-described program may be a so-called differential file (differential program) that can realize the above-described functions in combination with a program recorded in the computer system in advance.
 [0151]

Meanwhile, the present invention has been described using an embodiment, but
 10 a technical range of the present invention is not limited to the above-described embodiment. It will be apparent to those skilled in the art that various modifications and alternative embodiments can be adopted without departing from the spirit and scope of the present invention.

[Reference Signs List]

15 [0152]

1 File analysis system

11 Analysis unit

21 to 23 Terminal portion

31 Network

20 41 File analysis device

42 Web server device

43 Mail server device

51 Log detection device

52 Log management device

25 53 Terminal device

	111, 151, 216 Storage unit
	112, 215 Communication unit
	113 File inspection unit
	114 File analysis unit
5	115 Notification unit
	116 Management unit
	121 Reception unit
	131 Decoding unit
	132 Decompression unit
10	211 Input unit
	212 Output unit
	213, 4012 Operation unit
	214, 4013 Display unit
	217 Control unit
15	231 Log acquisition unit
	232 File condition acquisition unit
	233 File condition determination unit
	234 Log reduction unit
	235 File generation unit
20	236 Compression unit
	237 Encoding unit
	238 Notification control unit
	239 ANALYSIS REQUEST AVAILABILITY determination unit
	1011 File
25	2011, 2111, 2211 Display content

2221 Button

3011 Contract information

4001 Information processing device

4011 Processor

5

4014 Storage device

4015 Memory

4016 Input and output interface

4017 Network interface

4021 Bus

10

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.