

[DESCRIPTION]

[TITLE OF INVENTION]

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

5 [Technical Field]

[0001]

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

Priority is claimed on Japanese Patent Application No. 2018-180914, filed
10 September 26, 2018, the content of which is incorporated herein by reference.

[Background Art]

[0002]

For example, analysis systems performing an analysis of a security log for
organizations of a plurality of different customers using analysis devices are known.

15 In such an analysis system, as a rule used in an automatic analysis of a security
log, a rule for detecting characteristics of a harmful log or the like is generated and used.
In addition, as such a rule, a rule common to organizations of a plurality of different
customers is frequently used.

[0003]

20 However, in such a common rule, for example, in a case in which a name of a
non-harmful device in a specific organization accidentally coincides with a name of a
harmful server or the like, error in determination (for convenience of description, also
referred to as “erroneous detection”) for a log of the specific organization may occur. In
other words, erroneous detection of determining a non-harmful device to be harmful may
25 occur.

At that time, for example, there are cases in which it is necessary to generate a customized rule for such a specific organization for which erroneous detection occurs.

[0004]

In addition, in Patent Literature 1, a web access monitoring method in a
5 computer system in which a centralized management server used for managing client
computers is provided within an in-house network is disclosed (see Patent literature 1).
In the web access monitoring method, the centralized management server sets a
monitoring rule including a warning condition for unnecessary or inappropriate web
access for business or education and a processing form at the time of warning.

10 [Citation List]

[Patent Literature]

[0005]

[Patent Literature 1]

PCT International Publication No. WO 2007/069338

15 [Summary of Invention]

[Technical Issues]

[0006]

However, there are cases in which it is not efficient to take only a
countermeasure of generating a customized rule like in a conventional case when
20 erroneous detection occurs in a specific organization among organizations of a plurality
of different customers.

[0007]

In view of such circumstances, an embodiment of the present invention provides
an analysis device, a terminal device, an analysis system, an analysis method, and a
25 program capable of efficiently handling a case in which erroneous detection occurs in a

specific organization among organizations of a plurality of different customers.

[Solution to Issues]

[0008]

According to an aspect of the present invention, an analysis device includes: an
5 acquisition unit that acquires target information relating to a first terminal device; an
analysis executing unit that determines whether or not the target information acquired by
the acquisition unit satisfies a first condition; a notification unit that notifies the first
terminal device of first information in a case in which it is determined by the analysis
executing unit that the target information satisfies the first condition; an information
10 accepting unit that accepts second information from the first terminal device for the first
information notified by the notification unit; and a notification prohibiting unit that
prohibits notification of the first information to the first terminal device in a case in
which the second information is accepted from the first terminal device for the first
information, and the notification prohibiting unit stops the notification of the first
15 information according to the first condition for the first terminal device for a
predetermined period and resumes the notification of the first information according to
the first condition after the predetermined period elapses.

According to another aspect of the present invention, an analysis device
includes: an acquisition unit that acquires target information relating to a first terminal
20 device; an analysis executing unit that determines whether or not the target information
acquired by the acquisition unit satisfies a first condition; a notification unit that notifies
the first terminal device of first information in a case in which it is determined by the
analysis executing unit that the target information satisfies the first condition; an
information accepting unit that accepts second information from the first terminal device
25 for the first information notified by the notification unit; a notification prohibiting unit

that prohibits notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first information; and a management unit that manages a status of the notification of the first information according to the first condition, the status at least includes a status of being prohibited, and a search for the first information can be performed using the status of the notification.

According to still another aspect of the present invention, an analysis device includes: an acquisition unit that acquires target information relating to a first terminal device; an analysis executing unit that determines whether or not the target information acquired by the acquisition unit satisfies a first condition; a notification unit that notifies the first terminal device of first information in a case in which it is determined by the analysis executing unit that the target information satisfies the first condition; an information accepting unit that accepts second information from the first terminal device for the first information notified by the notification unit; and a notification prohibiting unit that prohibits notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first information, and the notification prohibiting unit prohibits notification of the first information for the first terminal device on the basis of a second condition for specifying the prohibition of the notification of the first information for the first terminal device.

According to an additional aspect of the present invention, an analysis device includes: an acquisition unit that acquires target information relating to a first terminal device; an analysis executing unit that determines whether or not the target information acquired by the acquisition unit satisfies a first condition; a notification unit that notifies the first terminal device of first information in a case in which it is determined by the analysis executing unit that the target information satisfies the first condition; an

information accepting unit that accepts second information from the first terminal device for the first information notified by the notification unit; and a notification prohibiting unit that prohibits notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first information, and the target information is a log relating to security.

According to some aspects of the present invention, in the analysis device, the first condition is a rule for detecting a problem, the first information is information of an alert corresponding to the problem, and the second information is information for instructing that there is an error in the alert.

According to some aspects of the present invention, the analysis device further includes a change unit that changes the first condition. According to one aspect of the present invention, there is provided a terminal device including: a notification reception control unit that receives notification of first information relating to security notified from an analysis device in a case in which it is determined by the analysis device that target information relating to the terminal device having a detection device setting a log relating to security as target information, detecting the target information relating to the terminal device, and transmitting the target information to the analysis device satisfies a first condition; an instruction accepting unit that accepts a predetermined instruction relating to the security for the first information received by the notification reception control unit; and an instruction transmission control unit that transmits second information including an instruction for prohibiting notification of the first information relating to the security for the terminal device to the analysis device in a case in which the instruction is accepted for the first information.

According to some aspects of the present invention, in the terminal device, the first condition is a rule for detecting a problem, the first information is information of an

alert corresponding to the problem, and the second information is information for instructing that there is an error in the alert.

[0009]

According to some aspects of the present invention, an analysis system includes:

5 a first terminal device; and an analysis device, the analysis device includes: an acquisition unit that acquires target information relating to a first terminal device; an analysis executing unit that determines whether or not the target information acquired by the acquisition unit satisfies a first condition; a notification unit that notifies the first terminal device of first information in a case in which it is determined by the analysis
10 executing unit that the target information satisfies the first condition; an information accepting unit that accepts second information from the first terminal device for the first information notified by the notification unit; and a notification prohibiting unit that prohibits notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first
15 information, and the first terminal device includes: a notification reception control unit that receives notification of the first information notified from the analysis device; an instruction accepting unit that accepts a predetermined instruction for the first information received by the notification reception control unit; and an instruction transmission control unit that transmits the second information to the analysis device in a
20 case in which the instruction is accepted for the first information, and the notification prohibiting unit stops the notification of the first information according to the first condition for the first terminal device for a predetermined period and resumes the notification of the first information according to the first condition after the predetermined period elapses.

25 According to some aspects of the present invention, an analysis system includes:

a first terminal device; and an analysis device, the analysis device includes: an acquisition unit that acquires target information relating to a first terminal device; an analysis executing unit that determines whether or not the target information acquired by the acquisition unit satisfies a first condition; a notification unit that notifies the first terminal device of first information in a case in which it is determined by the analysis executing unit that the target information satisfies the first condition; an information accepting unit that accepts second information from the first terminal device for the first information notified by the notification unit; a notification prohibiting unit that prohibits notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first information; and a management unit that manages a status of the notification of the first information according to the first condition, and the first terminal device includes: a notification reception control unit that receives notification of the first information notified from the analysis device; an instruction accepting unit that accepts a predetermined instruction for the first information received by the notification reception control unit; and an instruction transmission control unit that transmits the second information to the analysis device in a case in which the instruction is accepted for the first information, the status at least includes a status of being prohibited, and a search for the first information can be performed using the status of the notification.

20 According to some aspects of the present invention, an analysis system includes: a first terminal device; and an analysis device, the analysis device includes: an acquisition unit that acquires target information relating to a first terminal device; an analysis executing unit that determines whether or not the target information acquired by the acquisition unit satisfies a first condition; a notification unit that notifies the first terminal device of first information in a case in which it is determined by the analysis

executing unit that the target information satisfies the first condition; an information accepting unit that accepts second information from the first terminal device for the first information notified by the notification unit; and a notification prohibiting unit that prohibits notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first information, the first terminal device includes: a notification reception control unit that receives notification of the first information notified from the analysis device; an instruction accepting unit that accepts a predetermined instruction for the first information received by the notification reception control unit; and an instruction transmission control unit that transmits the second information to the analysis device in a case in which the instruction is accepted for the first information, and the notification prohibiting unit prohibits notification of the first information for the first terminal device on the basis of a second condition for specifying the prohibition of the notification of the first information for the first terminal device.

According to some aspects of the present invention, an analysis system includes: a first terminal device; and an analysis device, the analysis device includes: an acquisition unit that acquires target information relating to a first terminal device; an analysis executing unit that determines whether or not the target information acquired by the acquisition unit satisfies a first condition; a notification unit that notifies the first terminal device of first information in a case in which it is determined by the analysis executing unit that the target information satisfies the first condition; an information accepting unit that accepts second information from the first terminal device for the first information notified by the notification unit; and a notification prohibiting unit that prohibits notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first

information, the first terminal device includes: a notification reception control unit that receives notification of the first information notified from the analysis device; an instruction accepting unit that accepts a predetermined instruction for the first information received by the notification reception control unit; and an instruction transmission control unit that transmits the second information to the analysis device in a case in which the instruction is accepted for the first information, and the target information is a log relating to security.

According to some aspects of the present invention, in the analysis system, the first condition is a rule for detecting a problem, the first information is information of an alert corresponding to the problem, and the second information is information for instructing that there is an error in the alert.

According to some aspects of the present invention, in the analysis system, the analysis device further includes a change unit that changes the first condition.

[0010]

According to some aspects of the present invention, an analysis method in an analysis system includes a first terminal device and an analysis device, the analysis method including: acquiring target information relating to a first terminal device, determining whether or not the acquired target information satisfies a first condition, and notifying the first terminal device of first information in a case in which it is determined that the target information satisfies the first condition by using the analysis device; receiving notification of the first information notified from the analysis device and transmitting second information to the analysis device in a case in which a predetermined instruction is accepted for the received first information by using the first terminal device; prohibiting the notification of the first information for the first terminal device in a case in which the second information is accepted from the first terminal device by using

the analysis device; and stopping the notification of the first information according to the first condition for the first terminal device for a predetermined period as the prohibition of the notification and resuming the notification of the first information according to the first condition after the predetermined period elapses by using the analysis device.

5 According to some aspects of the present invention, an analysis method in an analysis system includes a first terminal device and an analysis device, the analysis method including: acquiring target information relating to a first terminal device, determining whether or not the acquired target information satisfies a first condition, and notifying the first terminal device of first information in a case in which it is determined
10 that the target information satisfies the first condition by using the analysis device; receiving notification of the first information notified from the analysis device and transmitting second information to the analysis device in a case in which a predetermined instruction is accepted for the received first information by using the first terminal device; prohibiting the notification of the first information for the first terminal device in
15 a case in which the second information is accepted from the first terminal device by using the analysis device; and managing a status of the notification of the first information according to the first condition by using the analysis device, the status at least includes a status of being prohibited, and a search for the first information can be performed using the status of the notification.

20 According to some aspects of the present invention, an analysis method in an analysis system includes a first terminal device and an analysis device, the analysis method including: acquiring target information relating to a first terminal device, determining whether or not the acquired target information satisfies a first condition, and notifying the first terminal device of first information in a case in which it is determined
25 that the target information satisfies the first condition by using the analysis device;

receiving notification of the first information notified from the analysis device and transmitting second information to the analysis device in a case in which a predetermined instruction is accepted for the received first information by using the first terminal device; prohibiting the notification of the first information for the first terminal device in
5 a case in which the second information is accepted from the first terminal device by using the analysis device; and prohibiting notification of the first information for the first terminal device on the basis of a second condition for specifying the prohibition of the notification of the first information for the first terminal device as prohibition of the notification by using the analysis device.

10 According to some aspects of the present invention, an analysis method in an analysis system includes a first terminal device and an analysis device, the analysis method including: acquiring target information relating to a first terminal device, determining whether or not the acquired target information satisfies a first condition, and notifying the first terminal device of first information in a case in which it is determined
15 that the target information satisfies the first condition by using the analysis device; receiving notification of the first information notified from the analysis device and transmitting second information to the analysis device in a case in which a predetermined instruction is accepted for the received first information by using the first terminal device; and prohibiting the notification of the first information for the first terminal
20 device in a case in which the second information is accepted from the first terminal device by using the analysis device, and the target information is a log relating to security.

 According to some aspects of the present invention, in the analysis method, the first condition is a rule for detecting a problem, the first information is information of an
25 alert corresponding to the problem, and the second information is information for

instructing that there is an error in the alert.

According to some aspects of the present invention, in the analysis method, the analysis device changes the first condition.

[0011]

5 According to some aspects of the present invention, a program causes a computer configuring an analysis device to realize: a function of acquiring target information relating to a first terminal device; a function of determining whether or not the acquired target information satisfies a first condition; a function of notifying the first terminal device of first information in a case in which it is determined that the target
10 information satisfies the first condition; a function of accepting second information from the first terminal device for the notified first information; and a function of prohibiting notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first information, and the function of prohibiting notification stops the notification of the first information
15 according to the first condition for the first terminal device for a predetermined period and resumes the notification of the first information according to the first condition after the predetermined period elapses. According to one aspect of the present invention, there is provided a program causing a computer configuring an analysis device to realize: a function of acquiring target information relating to a first terminal device; a function of
20 determining whether or not the acquired target information satisfies a first condition; a function of notifying the first terminal device of first information in a case in which it is determined that the target information satisfies the first condition; a function of accepting second information from the first terminal device for the notified first information; a function of prohibiting notification of the first information to the first terminal device in a
25 case in which the second information is accepted from the first terminal device for the

first information; and a function of managing a status of the notification of the first information according to the first condition, the status at least includes a status of being prohibited, and a search for the first information can be performed using the status of the notification.

5 According to some aspects of the present invention, a program causes a computer configuring an analysis device to realize: a function of acquiring target information relating to a first terminal device; a function of determining whether or not the acquired target information satisfies a first condition; a function of notifying the first terminal device of first information in a case in which it is determined that the target
10 information satisfies the first condition; a function of accepting second information from the first terminal device for the notified first information; and a function of prohibiting notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first information, and the function of prohibiting notification prohibits notification of the first information
15 for the first terminal device on the basis of a second condition for specifying the prohibition of the notification of the first information for the first terminal device.

 According to some aspects of the present invention, a program causes a computer configuring an analysis device to realize: a function of acquiring target information relating to a first terminal device; a function of determining whether or not
20 the acquired target information satisfies a first condition; a function of notifying the first terminal device of first information in a case in which it is determined that the target information satisfies the first condition; a function of accepting second information from the first terminal device for the notified first information; and a function of prohibiting notification of the first information to the first terminal device in a case in which the
25 second information is accepted from the first terminal device for the first information,

and the target information is a log relating to security.

According to some aspects of the present invention, in the program, the first condition is a rule for detecting a problem, the first information is information of an alert corresponding to the problem, and the second information is information for instructing
5 that there is an error in the alert.

According to some aspects of the present invention, the program, further causes the computer to realize a function of changing the first condition.

According to some aspects of the present invention, a program causes a computer configuring a terminal device having a detection device setting a log relating to
10 security as target information, detecting the target information relating to the terminal device, and transmitting the target information to an analysis device to realize: a function of receiving notification of first information relating to security notified from the analysis device in a case in which it is determined by the analysis device that the target information relating to the terminal device satisfies a first condition; a function of
15 accepting a predetermined instruction relating to the security for the received first information; and a function of transmitting second information including an instruction for prohibiting notification of the first information relating to the security for the terminal device to the analysis device in a case in which the instruction is accepted for the first information.

20 According to some aspects of the present invention, in the program, the first condition is a rule for detecting a problem, the first information is information of an alert corresponding to the problem, and the second information is information for instructing that there is an error in the alert.

[Advantageous Effects of Invention]

25 [0012]

According to the analysis device, the terminal device, the analysis system, the analysis method, and the program described above, a case in which erroneous detection occurs in a specific organization among organizations of a plurality of different customers can be efficiently handled.

5 [Brief Description of Drawings]

[0013]

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

Fig. 2 is a diagram illustrating a schematic configuration example of a terminal
10 device according to one embodiment of the present invention.

Fig. 3 is a diagram illustrating one example of display details of an alert list according to one embodiment of the present invention.

Fig. 4 is a diagram illustrating one example of alert detailed display details according to one embodiment of the present invention.

15 Fig. 5 is a diagram illustrating one example of display details of an alert search according to one embodiment of the present invention.

Fig. 6 is a diagram illustrating one example of the sequence of a process performed by a terminal device according to one embodiment of the present invention.

Fig. 7 is a diagram illustrating one example of the sequence of a process
20 performed by an analysis device according to one embodiment of the present invention.

Fig. 8 is a diagram illustrating one example of the sequence of a process performed by an analysis device according to one embodiment of the present invention.

Fig. 9 is a diagram illustrating one example of the sequence of a process performed by an analysis device according to one embodiment of the present invention.

25 Fig. 10 is a diagram illustrating one example of the hardware configuration of an

information processing device according to one embodiment of the present invention.

[Description of Embodiments]

[0014]

Embodiments of the present invention will be described with reference to the
5 drawings

[0015]

[Analysis system]

Fig. 1 is a diagram illustrating a schematic configuration example of an analysis
system 1 according to one embodiment of the present invention. In addition, the
10 configuration of functional blocks illustrated in Fig. 1 is one example, and another
configuration may be used.

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

The terminal units 21 to 23 and the analysis unit 11 are communicatively
15 connected through the network 31.

[0016]

Here, the terminals 21 to 23 are managed by different management entities.
For example, a management entity may be an organization such as a company or a school
or an individual. In a case in which the management entity is an organization, a person
20 belonging to the organization manages the terminal units 21 to 23. In addition, in a case
in which the management entity is an individual, a person corresponding to the individual
manages the terminal units 21 to 23. In this embodiment, a person managing the
terminal units 21 to 23 may be referred to as a user.

In addition, two or more terminal units among a plurality of the terminal units
25 21 to 23 may be managed by the same management entity. The two or more terminal

units may be some or all of the plurality of the terminal units 21 to 23.

[0017]

The number of terminal units 21 to 23 may be an arbitrary number equal to or larger than one.

5 In this embodiment, for convenience of description, the configurations and the operations of the plurality of terminal units 21 to 23 are similar to one another except that the management entities of the terminal units 21 to 23 may be different from one another. For this reason, in this embodiment, one terminal unit 21 will be representatively described.

10 In addition, a form in which the configurations or the operations of the terminal units 21 to 23 are different from one another may be used.

[0018]

In this embodiment, the analysis unit 11 performs a similar operation for the plurality of terminal units 21 to 23 except that the management entities of the terminal
15 units 21 to 23 may be different from one another.

In addition, the analysis unit 11 may be configured to perform different operations for the plurality of terminal units 21 to 23.

[0019]

In this embodiment, the analysis unit 11 is common to the plurality of terminal
20 units 21 to 23. In addition, the analysis system 1 may include a plurality of analysis units 11. In such a case, the plurality of analysis units 11 perform an operation commonly with the plurality of terminal units 21 to 23.

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

[0020]

The network 31 may be an arbitrary network. The network 31, for example, may be the Internet or a dedicated network. In addition, for example, communication between the terminal units 21 to 23 and the analysis unit 11 may be wired

5 communication or wireless communication or may combine both wired communication and wireless communication.

[0021]

[Overview of terminal unit]

The terminal unit 21 will be representatively described.

10 The terminal unit 21 includes a log detecting device 51 and a terminal device 52.

In the example illustrated in Fig. 1, although a configuration in which the log detecting device 51 and the terminal device 52 are connected to the network 31 is illustrated, the configuration is not limited thereto.

[0022]

15 The log detecting device 51 detects information that is a detection target (for convenience of description, also referred to as “target information”). In this embodiment, the target information is a predetermined log. In this embodiment, the log detecting device 51 monitors a predetermined target all the time and detects a log of the target. In this embodiment, the log is a log relating to security (a security log) and, for
20 example, is a log having a communication through the network 31 as a target.

The log detecting device 51, for example, may be configured using a sensor detecting a predetermined log. In this embodiment, the log detecting device 51 detects a log relating to communication performed by the terminal device 52. The log detecting device 51 outputs the detected log. In this embodiment, the log detecting device 51
25 transmits the detected log to the analysis unit 11. The transmission of a log, for

example, may be performed for each predetermined unit of logs. The unit may be a group for each predetermined period. The predetermined period, for example, may be one day or the like.

In addition, in this embodiment, the log detecting device 51 does not store
5 detected logs. As another example, the log detecting device 51 may include a storage unit that stores detected logs.

[0023]

The terminal device 52, for example, is configured using an information
processing device operated by a user. The information processing device, for example,
10 is a computer. For example, the computer may be a desktop computer, a laptop computer, a cellular phone computer, a smartphone computer, or the like.

The terminal device 52 receives an electronic mail transmitted from the analysis unit 11 through the network 31.

In addition, the terminal device 52 acquires information of a web page provided
15 by the analysis unit 11. In addition, the terminal device 52 transmits information to the analysis unit 11 through the network 31. In this embodiment, for example, the terminal device 52 transmits information relating to erroneous detection (misdetection) for a result of an analysis performed by the analysis unit 11 to the analysis unit 11.

[0024]

20 [Overview of analysis unit]

The analysis unit 11 includes an analysis device 41, a web server device 42, and a mail server device 43.

In the example illustrated in Fig. 1, although a configuration in which the analysis device 41, the web server device 42, and the mail server device 43 are connected
25 to the network 31 is illustrated, the configuration is not limited thereto.

[0025]

The analysis device 41 includes a storage unit 111, an acquisition unit 112, an analysis executing unit 113, a notification unit 114, an erroneous detection control unit 115, and a management unit 116.

5 The acquisition unit 112 includes a reception unit 131.

The management unit 116 includes a search processing unit 151.

[0026]

An overview of an operation performed by the analysis device 41 will be illustrated.

10 The storage unit 111 stores various kinds of information.

The acquisition unit 112 receives a log transmitted from the log detecting device 51 to the analysis unit 11 through the network 31 using the reception unit 131. Then, the acquisition unit 112 acquires the received log. In this embodiment, the acquisition unit 112 collects various logs by acquiring various logs. The acquisition unit 112
15 outputs the received log to the analysis executing unit 113. In this embodiment, the log detecting device 51 transmits the log addressed to the analysis device 41.

[0027]

Here, the log detecting device 51 may compress information of a log and transmit compressed information of the log to the analysis device 41. In such a case, in
20 the analysis device 41, the analysis executing unit 113 decompresses the received information and acquires information of the original log. In addition, instead of “decompression”, this may be referred to as “expansion” or the like.

Furthermore, the log detecting device 51 may encrypt information that is a transmission target and transmit encrypted information to the analysis device 41. In
25 such a case, in the analysis device 41, the analysis executing unit 113 acquires original

information by decoding the received information.

[0028]

The analysis executing unit 113 receives a log output from the acquisition unit 112 as an input. The analysis executing unit 113 analyzes an input log on the basis of a
5 predetermined condition (for convenience of description, also referred to as an “analysis condition”). The analysis executing unit 113 outputs predetermined information (for convenience of description, also referred to as “analysis result information”) relating to a result of an analysis of an input log to the notification unit 114.

In this embodiment, the storage unit 111 stores information used for specifying
10 an analysis condition. The analysis executing unit 113 acquires the analysis condition on the basis of the information.

[0029]

As the analysis condition, an arbitrary condition may be used.

As the analysis condition, for example, a condition used for determining whether
15 or not there is a problem in a log that is an analysis target may be used. For example, the problem may be a computer virus or any other event.

As the analysis condition, for example, “a condition for determining that there is a problem in a case in which one or more of information used for identifying a transmission source included in the log, information used for identifying a transmission
20 destination included in the log, and other information included in the log coincide with predetermined information” may be used. As the analysis condition, for example, a condition described in a black list in which conditions of logs for determining that there is a problem are listed may be used.

[0030]

25 In addition, a condition for determining that there is a problem, for example,

may be referred to as a “rule”, and, for convenience of description, it will be referred to as a “detection rule” in description in this embodiment. The detection rule, for example, may be understood as a condition for detecting a problem on the basis of a log. In other words, in a case in which it is determined that a status corresponding to a specific

5 detection rule has occurred for a specific log, it is determined that a problem associated with the detection rule has occurred. One or more detection rules are generated, and a plurality of different detection rules are generated and used in this embodiment.

In this case, in each detection rule, information for specifying a rule used for determining correspondence/non-correspondence to the detection rule is included. In

10 addition, information identifying a problem regarded to have occurred in the case of correspondence to the detection rule is associated with each detection rule.

Furthermore, also information identifying a problem regarded to have occurred in the case of correspondence to a specific detection rule may be perceived to be included in the detection rule.

15 In addition, alert details to be notified in a case in which a problem has occurred are associated with each problem.

[0031]

In this way, a detection rule, a problem, and an alert (alert details) are associated with one another in this embodiment. In this embodiment, for example, such

20 association information is stored in the storage unit 111 and is managed by the management unit 116.

In addition, for example, a problem and alert details may be configured as common information. In other words, in a case in which a problem is presented in alert details, the problem can be notified using the alert details.

25 [0032]

In addition, in this embodiment, for convenience of description, a case in which each detection rule is initially generated as a detection rule common to all the terminal devices 52 will be illustrated. As another example, for each detection rule, one or more terminal devices 52 to which the detection rule is applied may be initially set. Such
5 setting details may be regarded to be included in the detection rule.

As specific examples of the detection rule, “a detection rule of determining that a problem called information communication from a suspicious transmission source has occurred in a case in which, for a received signal, identification information of a device that is a transmission source of the received signal coincides with predetermined
10 identification information”, “a detection rule of determining that a problem of information communication to a suspicious transmission destination has occurred in a case in which, for a transmitted signal, identification information of a device that is a transmission destination of the transmitted signal coincides with predetermined identification information”, and the like may be used.

15 [0033]

Here, in this embodiment, when a detection rule is satisfied, there is a case in which an alert corresponding to the detection rule is notified and there is a case in which an alert corresponding to the detection rule is not notified. In this embodiment, for each detection rule, a rule defining whether or not an alert is to be notified when the detection
20 rule is satisfied (in this embodiment, for convenience of description, also referred to as an “alert rule”) is used.

In this embodiment, an alert rule is associated with a detection rule. In an alert rule, information for identifying a terminal device 52 to which an alert is to be notified when a detection rule associated with the alert rule is satisfied or information for
25 identifying a terminal device 52 to which an alert is not notified when a detection rule

associated with the alert rule is satisfied is included. In an alert rule, for example, it is initially set to notify an alert to all the terminal devices 52 when a detection rule associated with the alert rule is satisfied.

[0034]

5 In addition, as another example, an alert rule may be provided for each terminal device 52. In such a case, in an alert rule of each terminal device 52, information for specifying a detection rule for notifying an alert to the terminal devices 52 or information for specifying a detection rule for not notifying an alert to the terminal device 52 is included.

10 [0035]

Here, in this embodiment, by combining a detection rule and an alert rule, for example, a case in which a predetermined problem is detected, and an alert is notified to the terminal device 52 and a case in which a predetermined problem is detected, and an alert is not notified can be specified.

15 As a form in which an alert is not notified, for example, a form in which notification of an alert is stopped for a predetermined period may be included or an aspect in which notification of an alert is permanently stopped may be included.

As another example, a rule in which a detection rule and an alert rule are integrated may be used.

20 [0036]

In this embodiment, in a case in which a certain detection rule is satisfied, on the basis of an alert rule corresponding to the detection rule, the analysis executing unit 113 outputs analysis result information to the notification unit 114 in a case in which an alert is to be notified and does not output analysis result information to the notification unit

25 114 in a case in which an alert is not to be notified.

In addition, in this embodiment, although a case in which whether or not notification of an alert is performed is controlled by the analysis executing unit 113 is illustrated, as another example, a configuration in which analysis result information is output from the analysis executing unit 113 to the notification unit 114, and the

5 notification unit 114 controls whether or not notification of an alert is performed on the basis of details of an alert rule may be used.

[0037]

In addition, in a case in which logs of a plurality of types are included in logs that are analysis targets, for example, the analysis executing unit 113 determines the

10 types of logs. In this case, information of each log includes information used for specifying a type of log.

[0038]

In addition, for example, a configuration in which a sensor of the log detecting device 51 transmits information of an alert together with a detection result of a log to the

15 analysis device 41 may be used.

In such a case, in the analysis device 41, the analysis executing unit 113, for example, determines whether or not the information of the alert added to the detection result of the log is correct. In this case, for example, a condition for determining whether or not information of an alert added to a detection result of a log is correct is

20 used as an analysis condition.

Generally, in a sensor of the log detecting device 51, there are also many cases in which accuracy of an alert notified from the sensor that notifies an alert is not high. The alert, for example, may include a name of a signature.

[0039]

25 In this embodiment, together with a condition for determining a log having a

problem, one or more among a name of an alert (for convenience of description, also referred to as an “alert name”), a degree of importance, and the like may be stored in a detection rule while being associated therewith. For example, the alert corresponds to an occurring problem.

- 5 The alert name represents the name of an alert. For example, the alert name is set in advance for each type of alert.

Information used for specifying each type of details of an alert may be added to each alert.

- The degree of importance represents a degree of importance of an alert. The
10 degree of importance may be represented using arbitrary levels. In this embodiment, the degree of importance is represented using three levels.

[0040]

- In a case in which analysis result information is input from the analysis
executing unit 113, the notification unit 114 notifies the terminal device 52 of
15 predetermined information based on the analysis result information. As the
predetermined information, information used for notifying the terminal device 52 of
information relating to an analysis result is used, and arbitrary information may be used.

[0041]

- Here, as a technique for notifying the terminal device 52 of information from the
20 notification unit 114, an arbitrary technique may be used.

- In this embodiment, in a case in which information to be notified to the terminal
device 52 is generated, the notification unit 114 generates an electronic mail addressed to
the terminal device 52 and transmits the generated electronic mail to the mail server
device 43. In this case, the notification unit 114 includes information of an access
25 destination, which can be accessed from the terminal device 52, in the electronic mail.

For example, the information may be a uniform resource locator (URL).

The notification unit 114 generates a web page corresponding to information of an access destination included in an electronic mail and transmits information of the generated web page to the web server device 42. The notification unit 114 includes
5 information to be notified to the terminal device 52 in the web page.

[0042]

The mail server device 43 receives an electronic mail transmitted from the notification unit 114. The mail server device 43 transmits the received electronic mail to the destination of the electronic mail. In this embodiment, an electronic mail having
10 the terminal device 52 as a destination is transmitted from the mail server device 43 to the terminal device 52 through the network 31.

The web server device 42 receives information of a web page transmitted from the notification unit 114. The web server device 42 provides the web page to be readable on the basis of the received information. In this embodiment, the web server
15 device 42 provides the web page to be readable for the terminal device 52 in accordance with an access from the terminal device 52.

[0043]

The erroneous detection control unit 115 performs control relating to erroneous detection for a result of an analysis performed by the analysis executing unit 113.

20 The erroneous detection control unit 115, for example, performs a process of receiving a notification of erroneous detection from the terminal device 52 for each alert, a process of stopping notification of an alert according to a detection rule corresponding to an alert for the terminal device 52 that is a notification source in a case in which a notification of erroneous detection is received from the terminal device 52 for each alert,
25 a process of resuming a notification of an alert according to the detection rule for a

notification source, and the like.

In this embodiment, the error detection control unit 115 controls stopping of the notification of the alert or resuming of the notification of the alert by rewriting details of an alert rule corresponding to the detection rule.

5 [0044]

The management unit 116 performs various kinds of management for the terminal device 52.

In the management unit 116, for example, the search processing unit 151 performs a process of information searching. The search processing unit 151 may
10 perform a process of executing a search performed in the terminal device 52 instead of the terminal device 52 or a process of assisting a search performed in the terminal device 52. The search processing unit 151, for example, performs a process of searching using information stored in the storage unit 111.

In addition, for example, the management unit 116 changes a detection rule and
15 the like stored in the storage unit 111 by rewriting them. In such rewriting, for example, new registration, overwriting, and erasing may be included.

[0045]

In this embodiment, a case in which information of the terminal device 52 is known in the analysis unit 11 is illustrated.

20 In this embodiment, in a case in which, between a management entity of the terminal device 52 and a management entity providing an analysis service using the analysis unit 11, a contract relating to the service is concluded, information of the terminal device 52 relating to the contract is set in the analysis unit 11. For example, the information may be stored in the storage unit 111. For example, the information
25 may include information for identifying the terminal device 52. The information may

include an address of an electronic mail of the terminal device 52.

[0046]

Here, the information of the terminal device 52 set in regards to a contract, for example, may be information for specifying an analysis range in which a service can be received, information relating to a charge required for receiving a service (for
5 convenience of description, also referred to as “billing information”), or the like.

An analysis range in which a service can be received, for example, may be set using one or more among a data amount, the number of times, a period, and the like.

The management unit 116 may manage the information for specifying a charge
10 that is billed at the current time point to the terminal device 52 by storing it in the storage unit 111.

In addition, when seen from a management entity providing an analyzing service by the analysis unit 11, the management entity of a terminal device 52 for which a contract relating to the service is concluded becomes a customer. Management entities
15 of a plurality of terminal units 21 to 23 may be customers different from one another.

[0047]

[Details of terminal device]

Fig. 2 is a diagram illustrating a schematic configuration example of the terminal device 52 according to one embodiment of the present invention. In addition, the
20 configuration of functional blocks illustrated in Fig. 2 is one example, and any other configuration may be used.

The terminal device 52 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.

25 The control unit 217 includes a notification reception control unit 231, an

instruction transmission control unit 232, and a search control unit 233.

[0048]

The input unit 211 receives information output from an external device as an input.

5 The output unit 212 outputs information to an external device.

Here, the external device may be an arbitrary device. The external device, for example, may be a recording medium that can be carried. For example, the external device may be a printer device.

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

The display unit 214 includes a screen and outputs information to the screen. Accordingly, the information is displayed on the screen.

The communication unit 215 performs communication through a network 31.

15 The storage unit 216 stores various kinds of information.

The control unit 217 performs various kinds of control in the terminal device 52.

[0049]

The notification reception control unit 231 performs a process for receiving details of a notification performed by the notification unit 114 of the analysis device 41.

20 In this embodiment, the notification reception control unit 231 receives an electronic mail transmitted with being addressed to the terminal device 52 through the network 31 from the mail server device 43 using the communication unit 215. In addition, the notification reception control unit 231 acquires information of a web page provided by the web server device 42 by accessing the web page that is an access
25 destination described in the received electronic mail. For example, this access may be

performed in accordance with an operation on the operation unit 213 that is performed by a user.

[0050]

The notification reception control unit 231 displays information of an acquired
5 electronic mail or information of an acquired web page on the screen of the display unit 214.

For example, details of a notification of an analysis result of a log includes information for notifying determination of an occurrence of a problem as a result of the analysis of the log. Such a notification serves as a notification of an alert (warning).

10 In addition, a “problem” in an analysis result, for example, may be referred to as an “incident”, an “abnormality”, or the like.

[0051]

The instruction transmission control unit 232 transmits an instruction according to an operation on the operation unit 213 that is performed by a user to the analysis
15 device 41 using the communication unit 215.

In this embodiment, a user can perform an operation for performing a predetermined instruction on a web page displayed on the screen of the display unit 214.

In this embodiment, an instruction for a notification of erroneous detection (misdetection) for detection determining an occurrence of a problem in an analysis result
20 of a log is used as such an instruction.

[0052]

The search control unit 233 performs a process of various searches for details of a notification of an analysis result.

For example, the search control unit 233 may receive a result of the process of a
25 search performed by the search processing unit 151 of the analysis device 41 and perform

presentation or the like of the result. In addition, the search control unit 233 may performs the process of a search, for example, by being assisted by the search processing unit 151 of the analysis device 41. In addition, the search control unit 233 may perform the process of a search, for example, independently from the analysis device 41.

5 [0053]

[Alert list]

Fig. 3 is a diagram illustrating one example of display details 2011 of an alert list according to one embodiment of the present invention.

The display details 2011 represent a list of alerts. The display details 2011 are
10 displayed on the screen of the display unit 214 in the terminal device 52. For example, the display details 2011 may be different for each terminal device 52. In the example illustrated in Fig. 3, the list of alerts is a list of alerts performed in the past.

[0054]

The display details 2011, for example, are based on information provided for the
15 terminal device 52 from the analysis device 41.

As one example, the display details 2011 may be generated on the analysis device 41 side and be provided for the terminal device 52 from the analysis device 41.

As another example, the display details 2011 may be generated on the basis of information stored in the storage unit 216 in the terminal device 52 after the information
20 provided for the terminal device 52 from the analysis device 41 is stored in the storage unit 216. In addition, the display details 2011 may include other information.

[0055]

In the example illustrated in Fig. 3, date and time, an alert name, a degree of importance, and a status are displayed in association with one another. In addition, a
25 display color of information may be changed in accordance with one or more of the

degree of importance, the status, and the like.

[0056]

The date and time represent a date and time at which an alert has occurred. In the example illustrated in Fig. 3, for example, “2018/1/2” represents January 2, 2018, and the others are similarly represented.

In the example illustrated in Fig. 3, there are “suspicious transmission”, “suspicious reception”, and the like as alert names. In addition, such alert names are examples for convenience of description, and arbitrary names may be used as alert names.

As degrees of importance, there are three degrees of importance including “high”, “intermediate”, and “low” in order of highest to lowest degree in the example illustrated in Fig. 3.

A status represents a status at which an alert is handled. In this embodiment, statuses including “no handling”, “under investigation”, “handled”, “on pending”, “on handling”, “prohibition”, and the like are used as statuses. In addition, arbitrary statuses may be used as the statuses.

[0057]

“No handling” represents that an alert has not been handled yet.

“Under investigation” represents an alert being in the middle of an investigation.

“Handled” represents that an alert has been handled. In other words, it represents that a problem relating to the alert has been resolved.

“On pending” represents that handling of an alert is on pending.

“On handling” represents that an alert is in the middle of handling.

“Prohibition” represents that a notification of an alert is prohibited for the alert.

In this embodiment, for an alert, in a case in which an erroneous detection in the terminal

device 52 is indicated, a status “prohibition” is set in the analysis device 41. For example, such a setting is performed in accordance with an alert rule.

In addition, each word representing a status of an alert may be represented using another arbitrary word.

5 [0058]

Here, a date and time of an alert, an alert name, and a degree of importance are, for example, determined by the analysis executing unit 113 of the analysis device 41, and analysis result information including such information is output from the analysis executing unit 113 to the notification unit 114. The notification unit 114 includes a date
10 and time of an alert, an alert name, and a degree of importance in details notified to the terminal device 52 on the basis of the analysis result information.

In addition, for example, the status of an alert is set in accordance with an operation on the operation unit 213 that is performed by a user in the terminal device 52. The set status of an alert is notified from the terminal device 52 to the notification unit
15 114 of the analysis device 41 and is managed by the management unit 116. The management unit 116, for example, performs management by storing information in which an alert and a status are associated with each other in the storage unit 111 on the basis of information received from the terminal device 52 by the notification unit 114.

[0059]

20 Here, in this embodiment, although a case in which information of an alert having “prohibition” as its status is also displayed in the alert list is illustrated, as another example, a form in which information of an alert having “prohibition” at its status is not displayed may be used.

[0060]

25 Fig. 4 is a diagram illustrating one example of alert detailed display details 2111

according to one embodiment of the present invention.

The display details 2111 represents details of an alert. The display details 2111 are displayed on the screen of the display unit 214 in the terminal device 52. For example, the display details 2111 may be different for each terminal device 52.

5 [0061]

For example, the display details 2111 are based on information provided from the analysis device 41 for the terminal device 52.

As one example, the display details 2111 may be generated on the analysis device 41 side and be provided from the analysis device 41 for the terminal device 52.

10 As another example, after information provided from the analysis device 41 for the terminal device 52 is stored in the storage unit 216, the display details 2111 may be generated using the information stored in the storage unit 216 in the terminal device 52. In addition, the display details 2111 may include other information.

[0062]

15 As details of an alert, for example, in a case in which one alert in the list of alerts is instructed by a user, details of the alert are represented for the instructed alert.

In the example illustrated in Fig. 4, a frame of an attribute area 2121, a frame of a handling status area 2122, and a frame of a details area 2123 are displayed on one screen. In addition, names of such areas, an arrangement, and the like may be arbitrary.

20 [0063]

Information for one alert is displayed on the screen of alert details.

Attributes of one alert that is a display target are represented in the attribute area 2121. In the example illustrated in Fig. 4, a date and time, an alert name, a degree of importance, and a status are represented in the attribute area 2121. In addition, the

25 display color of information may be changed in accordance with one or more of a degree

of importance, a status, and the like.

In the handling status area 2122, information for which an arbitrary handling status can be selected from a plurality of handling statuses is represented.

In the details area 2123, detailed information for an alert, a log causing an alert
5 to be generated, and the like are represented.

[0064]

In the example illustrated in Fig. 4, as handling statuses that can be selected, there are “no handling”, “under investigation”, “handled”, “on pending”, “on handling”, “erroneous detection”, and “non target”. In each handling status, a button switched
10 between a selected state and an unselected state is displayed. The button, for example, is switched between a black state that is a selected state and a white state that is an unselected state in accordance with an operation on the operation unit 213 that is performed by a user. For example, the button may be a radio button.

[0065]

15 Here, “no handling”, “under investigation”, “on handling”, “on pending”, and “on handling” are the same as those described with reference to Fig. 3.

“Erroneous detection” is an item for accepting an instruction for a notification of an erroneous detection for the displayed alert from the terminal device 52 to the analysis device 41.

20 “Non-target” is an item for accepting an instruction for a notification of a non-detection target for the displayed alert from the terminal device 52 to the analysis device 41.

In addition, in this embodiment, a status “prohibition” is automatically set in the analysis device 41 for an alert for which “erroneous detection” is selected. For this
25 reason, in this embodiment, a user cannot select a status “prohibition”. As another

example, in the terminal device 52, a configuration in which a user can select a status “prohibition” may be used.

In addition, in this embodiment, a status “prohibition” is automatically set by the analysis device 41 for the alert in which “non target” is selected.

5 In this embodiment, although “erroneous detection” and “non-target” have similar points, they are provided as being different. In addition, “non-target” may not be provided.

[0066]

 In the display details 2111 illustrated in Fig. 4, a user selects a handling status
10 that is appropriate for a displayed alert among handling statuses that can be selected by operating the operation unit 213.

In addition, in this embodiment, although “no handling” is selected in the handling status area 2122 in an initial default state, another handling status may be selected.

15 A button 2131 of determination is also displayed in the handling status area 2122. When the button 2131 is pressed on the basis of an operation on the operation unit 213 that is performed by a user, information for identifying a selected handling status is transmitted by the instruction transmission control unit 232 from the terminal device 52 to the analysis device 41.

20 [0067]

In this case, the terminal device 52 transmits information for identifying an alert and information for identifying a handling status selected by the user for the alert to the analysis device 41.

 In the analysis device 41, the notification unit 114 receives the information
25 transmitted from the terminal device 52, and the management unit 116 manages the

received information.

[0068]

<Selection of “erroneous detection”>

In a case in which information received from the terminal device 52 indicates
5 “erroneous detection”, in the analysis device 41, the erroneous detection control unit 115
stops the notification of an alert according to a detection rule generating the alert relating
to the erroneous detection for a constant period. The constant period may be an
arbitrary period and, for example, may be one month or the like.

In this embodiment, in the analysis device 41, such stopping of the notification
10 of the alert is performed for the terminal device 52 for which “erroneous detection” has
been selected by the user and is not performed for the other terminal devices. In other
words, even for the same detection rule, the notification of an alert according to the
detection rule is stopped only for the terminal device 52 for which the detection rule
becomes erroneous detection.

15 [0069]

In this embodiment, “erroneous detection” can be selected for each alert for each
customer. For example, for a certain detection rule, in a case in which erroneous
detection occurs only in the organization of a specific customer, the erroneous detection
may be set only for the organization of the specific customer. In the organization of the
20 specific customer, when “erroneous detection” is selected once for a certain alert,
notification of an alert based on the same detection rule can be prevented for the constant
period.

[0070]

In addition, in this embodiment, although such stopping of the notification of an
25 alert is temporarily performed, as another example, such stopping of the notification of

an alert may be permanently performed, in other words, the detection rule may be permanently set to be invalid for the corresponding terminal device 52. A technique for invalidating a detection rule is arbitrary. As the technique for invalidating a detection rule, for example, the management unit 116 may manage information representing that each detection rule is valid or invalid for each terminal device 52. In this embodiment, for example, information of an alert rule is used as the information.

[0071]

In the analysis device 41, the erroneous detection control unit 115 stores information specifying whether a notification of an alert according to a detection rule stored in the storage unit 111 is valid or invalid for each terminal device 52 in the storage unit 111. In this embodiment, the information is included in an alert rule and, for example, may be information of a flag. In addition, in the analysis device 41, the erroneous detection control unit 115 stores information for specifying a period for a notification of an alert that is invalid and is stopped for the constant period in the alert rule stored in the storage unit 111.

Furthermore, in this embodiment, a state in which a notification of an alert is invalid is also referred to as an “prohibition state”.

[0072]

In the analysis device 41, the erroneous detection control unit 115 determines whether or not the period has elapsed for a notification of an alert that is invalid and is stopped for the constant period on the basis of information stored in the storage unit 111. For example, the erroneous detection control unit 115 performs such determination at constant time intervals.

Then, in the analysis device 41, in a case in which it is determined that there is a notification of an alert of which a stop period indicating invalidity has elapsed, the

erroneous detection control unit 115 validates the notification of the alert again and applies the notification of the alert again to the terminal device 52 to which the application has been stopped.

[0073]

5 Here, as a detection rule applied when the notification of an alert corresponding to the detection rule for which erroneous detection has been indicated is resumed, for example, the same detection rule as that before the notification of the alert stopped is used.

 As another example, as a detection rule applied when the notification of an alert
10 corresponding to the detection rule for which erroneous detection has been indicated is resumed, a detection rule that is changed such that the detection rule before the notification of the alert is stopped is improved may be used. For example, such a change of a detection rule may be manually performed on the basis of a thought of a person such as an analyst on the analysis device 41 side may be performed using
15 artificial intelligence (AI) such as machine learning or the like, or may be automatically performed in the analysis device 41 on the basis of a change rule set in advance. For example, in a case in which “erroneous detection” is selected in the terminal device 52, the erroneous detection control unit 115 may notify a predetermined person of an indication thereof. Such a notification may be performed using an arbitrary technique,
20 and, for example, one or more techniques among a screen display, a speech output, printing on a sheet, transmission of an electronic mail, and the like may be used.

[0074]

 In a case in which machine learning is used as AI, for example, technologies such as logistic regression, a Bayesian filter, a support vector machine (SVM), deep
25 learning, and the like may be used.

A functional unit (in this embodiment, for convenience of description, also referred to as a “rule processing unit”) performing a process or changing a detection rule may be provided in the analysis device 41 or another device

For example, the rule processing unit acquires a result of learning using AI by
5 combining data and customer information on the basis of the data in which a detection rule that has been determined to cause as an erroneous detection and results of changes of the detection rule performed by an analyst are acquired in a large quantity. Then, the rule processing unit may automatically perform a process of changing the detection rule that is similar to that performed by the analyst using such the result of such learning.

10 For example, the detection rule that has been changed by AI may be checked by an analyst.

For example, the rule processing unit may check a detection rule that has been newly generated or changed by an analyst using AI.

[0075]

15 In addition, as one example of an erroneous detection, there are cases in which, although an attack against the terminal device 52 is correctly detected on the basis of the detection rule by the analysis device 41, a tool that is a target aimed by the attack is not used in a customer environment such as the terminal device 52 or the like. In other words, there are cases in which an attack to the weakness of a tool that is not used in a
20 customer environment comes to the terminal device 52 in the customer environment. In such cases, for example, the analysis device 41 may automatically finalize selection of an “erroneous detection” for the generated alert. Here, in the customer environment, terminal devices 52 are included, and devices other than the terminal devices 52 such as the server device and the like are included.

25 Alternatively, in a case in which the analysis device 41 correctly detects an

attack for the terminal device 52 on the basis of a detection rule, and a tool that is a target aimed by the attack is not used in a customer environment such as the terminal device 52 and the like, in a case in which information of an alert is notified to the terminal device 52, an indication of recommendation of selection of an “erroneous detection” and a
5 reason for recommending the selection of the “erroneous detection” may be notified to the terminal device 52. In such a case, in the terminal device 52, a user views the details of such a notification and determines whether or not “erroneous detection” is selected.

Here, as the case in which the analysis device 41 correctly detects an attack on
10 the basis of a detection rule, and a tool that is a target aimed by the attack is not used in a customer environment such as the terminal device 52 and the like, for example, there is a case in which, when a SQL server is not used in a customer environment, an attack of a SQL injection is performed, and an SQL injection alert is transmitted from the log detecting device 51 to the analysis device 41.

15 [0076]

<Selection of “non-target”>

In the analysis device 41, in a case in which information received from the terminal device 52 indicates “non-target”, the erroneous detection control unit 115 stops the notification of an alert according to a detection rule generating the alert relating to the
20 non-target.

In this embodiment, in the analysis device 41, such stopping of the notification of an alert is performed for the terminal device 52 in which “non-target” is selected and is not performed for the other terminal devices. In other words, even for the same detection rule, the notification of the alert is stopped for the terminal device 52 for which
25 the notification of an alert according to the detection rule is a non-target.

In the analysis device 41, the erroneous detection control unit 115 may store information for identifying a non-target or not in the storage unit 111 for each terminal device 52 for the detection rule stored in the storage unit 111. As the information, for example, information of an alert rule may be used.

5 [0077]

In addition, in a case in which the analysis device 41 correctly detects an attack on the basis of a detection rule, and a tool that is a target aimed by the attack is not used in a customer environment such as the terminal device 52 and the like, for example, the analysis device 41, for example, may automatically finalize the selection of “non-target”
10 for the generated alert.

Alternatively, in a case in which information of an alert is notified to the terminal device 52, the analysis device 41 may notify the terminal device 52 of an indication of recommendation of “non-target” and a reason for recommending “non-target”. In such a case, in the terminal device 52, a user views the details of such a
15 notification and determines whether or not “non-target” is selected.

[0078]

In addition, in a case in which the analysis device 41 correctly detects an attack on the basis of a detection rule, and a tool that is a target aimed by the attack is not used in a customer environment such as the terminal device 52 and the like, when “erroneous
20 detection” is selected by a user in the terminal device 52, the analysis device 41, for example, may automatically finalize the selection of “non-target” for the generated alert.

In such a configuration, in the analysis device 41, the management unit 116 manages information for identifying whether or not the tool is used in the terminal device 52 by storing it in the storage unit 111. Then, the analysis device 41 determines whether or
25 not the designation of “erroneous detection” according to the user is to be changed to

“non-target” on the basis of the information for identifying whether or not the tool is used and the detection rule that has generated the alert for the terminal device 52 in which the alert has been generated and performs a change in a predetermined case.

In addition, as another example, in a case in which “erroneous detection” is
5 designated to a certain alert by the user using the terminal device 52, and it is determined (judged) by the analysis device 41 or a person such as an analyst or the like that there is a likelihood that it corresponds to “non-target”, a configuration in which, after it is checked by the analysis device 41 for the user whether “erroneous detection” is to be changed to “non-target”, a change is performed in accordance with a permission of the user may be
10 used.

[0079]

In addition, in this embodiment, although “erroneous detection” and “non-target” are provided, for example, both “erroneous detection” and “non-target” may be configured to stop notification of an alert according to a detection rule. For example,
15 only a period in which the notification of an alert is stopped may be different between “erroneous detection” and “non-target”. As one example, a period in which a notification of an alert according to “erroneous detection” is stopped may have a finite value (for example, one month or the like), and a period in which a notification of an alert according to “non-target” is stopped may be permanent.

20 [0080]

Here, in this embodiment, although a case in which information of an alert for a log having “prohibition” as its status is also displayed in the alert details is illustrated, as another example, a form in which information of an alert having “prohibition” as its status is not displayed may be used.

25 [0081]

Fig. 5 is a diagram illustrating one example of display details 2211 of an alert search according to one embodiment of the present invention.

The display details 2211 are details of a screen for performing a search for an alert. The display details 2211 are displayed on the screen of the display unit 214 in the terminal device 52. For example, the display details 2211 may be different for each terminal device 52.

[0082]

The display details 2211, for example, are based on information provided from the analysis device 41 for the terminal device 52.

As one example, the display details 2211 may be generated on the analysis device 41 side and are provided from the analysis device 41 for the terminal device 52. As another example, the display details 2211 may be generated on the basis of information stored in the storage unit 216 of the terminal device 52 after information provided from the analysis device 41 for the terminal device 52 is stored in the storage unit 216. In addition, the display details 2211 may include other information.

[0083]

In the example illustrated in Fig. 5, a range of a date and time, a range of a degree of importance, a type of sensor, and a range of a handling status can be selected as search conditions.

[0084]

The range of a date and time is identified using a start time point and an end time point. For example, as each of the start time point and the end time point, a year/month/date is designated. In the example illustrated in Fig. 5, a range of “April 1, 2018 to May 1, 2018” is designated.

A degree of importance is designated using three levels of high, intermediate,

low in order of highest to lowest level. A plurality of different degrees of importance may be designated.

The type of sensor is designated using a name or the like of an individual sensor. A plurality of different sensors may be designated.

5 A handling status is designated from among a plurality of items. Two or more other items may be designated. In the example illustrated in Fig. 5, as handling statuses, there are “no handling”, “under investigation”, “on handling”, “on pending”, “handling”, “erroneous detection”, “prohibition”, and “non-target”.

[0085]

10 In the terminal device 52, search conditions are set on an alert search screen in accordance with an operation on the operation unit 213 performed by the user.

A button 2221 of a search is also displayed in the display details 2211. On the basis of an operation on the operation unit 213 that is performed by a user, when the button 2221 is pressed, information for specifying selected search conditions is

15 transmitted from the terminal device 52 to the analysis device 41.

In this embodiment, in the terminal device 52, the search control unit 233 performs the whole control for a search for an alert.

[0086]

The analysis device 41 receives information for specifying search conditions
20 transmitted from the terminal device 52. In the analysis device 41, the management unit 116 searches for an alert matching the search conditions by referring to the information relating to alerts stored in the storage unit 111 on the basis of the search conditions identified by the information received by the search processing unit 151. Then, the management unit 116 generates information representing a result of the search using the
25 search processing unit 151, and the information is notified to the terminal device 52 using

the notification unit 114. In this embodiment, at the time of searching for an alert, the management unit 116 may determine a status “prohibition”, a status “non-target”, or the like by referring to the details of an alert rule using the search processing unit 151.

[0087]

5 [Communication between terminal device and analysis device]

In this embodiment, in the service of a log analysis, the terminal device 52 and the analysis device 41 may execute the process in an on-demand manner. For example, in response to a request generated from the terminal device 52, a process for satisfying the request may be executed by the analysis device 41.

10 [0088]

[Dedicated tool]

In this embodiment, a dedicated tool (for convenience of description, also referred to as a “dedicated tool”) may be used in the terminal device 52. In other words, some or all of the functions of the terminal device 52 may be configured using a
15 dedicated tool. For example, the dedicated tool may be software such as a program or the like.

For example, in the terminal device 52, one or more functions of the notification reception control unit 231, the instruction transmission control unit 232, and the search control unit 233 may be configured as functions of a dedicated tool. For example, the
20 dedicated tool may be distributed for a fee or for free by the management entity or the like of the analysis unit 11. For example, the management tool is installed in the terminal device 52 and exhibits functions.

[0089]

[Process performed in analysis system]

25 Fig. 6 is a diagram illustrating one example of the sequence of a process

performed by the terminal device 52 according to one embodiment of the present invention.

In the example illustrated in Fig. 6, a handling status is selected in a case in which a notification of an alert is received in the terminal device 52.

5 [0090]

(Step S1)

In the terminal device 52, the notification reception control unit 231 receives a notification of an alert transmitted from the analysis device 41. Then, the process proceeds to the process of Step S2.

10 [0091]

(Step S2)

In the terminal device 52, the notification reception control unit 231 displays the received notification of the alert. In this example, in the terminal device 52, after the display details 2011 of the alert list are displayed, the alert detailed display details 2111
15 are displayed in accordance with a user's operation. Then, the process proceeds to the process of Step S3.

[0092]

(Step S3)

In the terminal device 52, the instruction transmission control unit 232
20 determines whether or not there has been a user's operation of selecting a handling status. In the example illustrated in Fig. 4, the operation is pressing of a button 2131 of determination in a state in which a handling status is designated.

As a result, in the terminal device 52, in a case in which it is determined by the instruction transmission control unit 232 that there has been a user's operation of
25 selecting a handling status (Step S3: Yes), the process proceeds to the process of Step S4.

On the other hand, in the terminal device 52, in a case in which it is determined by the instruction transmission control unit 232 that there has not been a user's operation of selecting a handling status (Step S3: No), the process of this flow ends.

[0093]

5 (Step S4)

In the terminal device 52, the instruction transmission control unit 232 transmits information for specifying an instruction for selecting a handling status received in accordance with an operation performed by a user to the analysis device 41. Then, the process of this flow ends.

10 [0094]

Fig. 7 is a diagram illustrating one example of the sequence of a process performed by the analysis device 41 according to one embodiment of the present invention.

In the example illustrated in Fig. 7, the analysis device 41 performs an analysis
15 of a log.

[0095]

(Step S21)

In the analysis device 41, the acquisition unit 112 receives and acquires a log transmitted from the log detecting device 51 using the reception unit 131. In this
20 embodiment, such reception of a log is constantly performed. Then, the process proceeds to the process of Step S22.

[0096]

(Step S22)

In the analysis device 41, the analysis executing unit 113 performs an analysis of
25 the received log on the basis of analysis conditions. For example, the analysis

executing unit 113 determines a log that matches a predetermined detection rule as a log having a problem. Then, the process proceeds to the process of Step S23.

[0097]

(Step S23)

5 In the analysis device 41, the notification unit 114 notifies the terminal device 52 of information of a result of the analysis performed by the analysis executing unit 113. Then, the process of this flow ends.

 In addition, in this embodiment, an alert requiring a notification is notified from the notification unit 114 to the terminal device 52 on the basis of an alert rule, and an
10 alert not requiring a notification is not notified from the notification unit 114 to the terminal device 52.

[0098]

 Fig. 8 is a diagram illustrating one example of the sequence of a process performed by the analysis device 41 according to one embodiment of the present
15 invention.

 In the example illustrated in Fig. 8, the analysis device 41 performs a process relating to selection of “erroneous detection”. In addition, in this embodiment, also the process relating to selection of “non-target” may be similar to the process relating to selection of “erroneous detection”.

20 [0099]

(Step S41)

 In the analysis device 41, the management unit 116 receives a notification of selection of “erroneous detection” for the alert in the terminal device 52. Then, the process proceeds to the process of Step S42.

25 [0100]

(Step S42)

In the analysis device 41, the erroneous detection control unit 115 stops the notification of an alert according to a detection rule generating the alert for which “erroneous detection” is selected in a notification source that is the terminal device 52 in which “erroneous detection” is selected. In this example, a stop period of the alert is assumed to have been set. Then, the process proceeds to the process of Step S43.

In this embodiment, for example, for the terminal device 52 in which “erroneous detection” is selected among detection rules common to a plurality of terminal devices 52, the notification of an alert according to the detection rule is stopped.

10 [0101]

(Step S43)

In the analysis device 41, the erroneous detection control unit 115 determines whether or not the stop period has elapsed for the notification of the alert that is being stopped.

15 As a result, in the analysis device 41, in a case in which the erroneous detection control unit 115 determines that the stop period has elapsed for the notification of the alert that is being stopped (Step S43: Yes), the process proceeds to the process of Step S44.

20 On the other hand, in the analysis device 41, in a case in which the erroneous detection control unit 115 determines that the stop period has not elapsed for the notification of the alert that is being stopped (Step S43: No), the process of Step S43 is repeatedly performed.

[0102]

(Step S44)

25 In the analysis device 41, in a case in which it is determined that the stop period

has elapsed for the notification of the alert that is being stopped, the erroneous detection control unit 115 resumes the notification of the alert for the corresponding terminal device 52. Then, the process of this flow ends.

[0103]

5 Fig. 9 is a diagram illustrating one example of the sequence of a process performed by the analysis device 41 according to one embodiment of the present invention.

 In the example illustrated in Fig. 9, the analysis device 41 performs a process of changing a detection rule.

10 In this embodiment, a case in which the management unit 116 can change a detection rule stored in the storage unit 111 in the analysis device 41 in accordance with an instruction from an analyst or the like is illustrated. In addition, as another example, a configuration in which changing of a detection rule stored in the storage unit 111 of the analysis device 41 is performed by an access from a device other than the analysis device
15 41 may be used.

[0104]

(Step S61)

 In the analysis device 41, the management unit 116 determines whether or not an instruction for changing a corresponding detection rule has been received for the alert for
20 which a notification of selection of “erroneous detection” has been received from the terminal device 52. In this example, the instruction, for example, may be an instruction that is given to the analysis device 41 by a person such as an analyst or the like or may be an instruction that is automatically given by a device such as the analysis device 41 or the like 41.

25 As a result, in the analysis device 41, in a case in which the management unit

116 determines that an instruction for changing the detection rule has been received (Step S61: Yes), the process proceeds to the process of Step S62.

On the other hand, in the analysis device 41, in a case in which the management unit 116 determines that an instruction for changing the detection rule has not been
5 received (Step S61: No), the process of this flow ends.

[0105]

(Step S62)

In the analysis device 41, the management unit 116 changes the corresponding detection rule in accordance with the received instruction. Then, the process of this
10 flow ends.

[0106]

Here, in this embodiment, a detection rule that generates an alert for which “erroneous detection” is indicated by a certain terminal device 52 may be commonly changed for a plurality of terminal devices including terminal devices other than the
15 terminal device 52. The plurality of terminal devices, for example, may be all or some of terminal devices to which the detection rule before change is applied.

In addition, as another example, a detection rule that generates an alert for which “erroneous detection” has been indicated by a certain terminal device 52 may be changed only for the terminal device 52.

20 [0107]

[Alert, detection rule, and status]

In this embodiment, an alert and a detection rule have been described to have one-to-one correspondence. In addition, a detection rule, an alert, and an alert rule have been described to have one-to-one-to-one correspondence. In this case, on the basis of
25 the correspondence between an alert and an alert rule and the correspondence between

the alert and a detection rule, correspondence between the detection rule and a status of validity/invalidity of a notification (details of the alert rule) is identified. Similarly, on the basis of the correspondence between a detection rule and an alert rule and the correspondence between the detection rule and an alert, correspondence between the alert and a status of validity/invalidity of a notification (details of the alert rule) is identified. In the analysis system 1 according to this embodiment, by managing the correspondence among a detection rule, an alert, and an alert rule, the status of validity/invalidity of the notification of an alert corresponding to the detection rule is managed.

[0108]

As another example, a plurality of different detection rules and one alert may be associated with each other. In such a case, in the analysis system 1, in order to manage a status selected for an alert, information for identifying correspondence between the alert and the status is managed. For example, each alert is identified on the basis of identification information attached to each alert. For example, in a case in which “erroneous detection” is selected for a certain alert, for example, the notification of the alert may be caused to be in the “prohibition” state for the detection rule that has generated the alert at that time. In other words, although there may be a plurality of detection rules for generating the alert at that time, for example, one detection rule that has generated the alert among them may be caused to be in the “prohibition” state. In addition, also for “non-target”, the process may be performed similar to that of the case of “erroneous detection”.

[0109]

[One example of configuration of information processing device]

Fig. 10 is a diagram illustrating one example of the hardware configuration of an information processing device 4001 according to one embodiment of the present

invention.

As the terminal device 52, the analysis device 41, or the like according to this embodiment, the information processing device 4001 having a hardware configuration as illustrated in Fig. 10 may be used.

5 [0110]

In the example illustrated in Fig. 10, 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/output interface 4016, and a network interface 4017 and a bus 4021 connecting these.

10 [0111]

The processor 4011 is composed of a central processing unit (CPU) or the like and executes a process defined in a certain program by executing the program.

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

15 The display unit 4013 includes a screen and outputs information to the screen for display.

[0112]

The storage device 4014 is a nonvolatile storage unit and, for example, is composed of a hard disk and the like, and stores information.

20 The memory 4015 is a volatile storage unit, is composed of a random access memory (RAM) and 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, for example, may store information of a program executed by the processor 4011.

25 [0113]

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

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

5 [0114]

Here, the information processing device 4001 may include one processor or two or more processors as the processor 4011. As one example, the information processing device 4001 may include a plurality of CPUs and realize all the processes using the plurality of CPUs in association with one another together with executing each process
10 using each CPU.

[0115]

[Summary of embodiment]

As above, the analysis system 1 according to this embodiment can efficiently handle a case in which an erroneous detection has occurred in a specific organization
15 among organizations of a plurality of different customers. In the analysis system 1 according to this embodiment, a user using the terminal device 52 can prohibit continuation of an erroneous detection by performing a simple operation.

For example, a designer of a detection rule can acquire information of feedback relating to an erroneous detection given from a user. Then, the designer of a detection
20 rule can review the detection rule, for example, during a period in which the notification of an alert according to the detection rule is prohibited. For example, the designer of a detection rule may manually generate an improved detection rule on the basis of the information that has been fed back. For example, the designer of a detection rule may generate an improved detection rule using a machine learning device by causing the
25 machine learning device to learn the information that has been fed back through machine

learning. In this way, for example, the number of erroneous detections is reduced.

In the analysis system 1 according to this embodiment, a customized rule may not be necessarily generated for each customer. In addition, also in the analysis system 1 according to this embodiment, a customized rule may be generated for each customer.

5 [0116]

Furthermore, in the analysis system 1 according to this embodiment, a search for a prohibited alert can be performed. In this way, the analysis system 1 according to this embodiment can perceive the number of times, a frequency, a trend, and the like of prohibition of unnecessary notification.

10 For example, the number of times of preventing notification of an unnecessary alert can be checked by using the number of prohibited alerts.

For example, in a case in which there is no prohibited alert or in a case in which the number of prohibited alerts is small like being equal to or smaller than one per month or the like, it can be checked that the number of attacking communications causing
15 generation of alerts is decreased or the number of alerts of “erroneous detection” is decreased in accordance with improvement of the detection rule or the like.

[0117]

In this embodiment, a system that monitors logs of devices of each of a plurality of customers is configured as below.

20 In other words, in the system, logs of each customer are acquired, and it is determined whether or not the logs of the customer satisfy a predetermined condition.

In the system, in a case in which it is determined that the logs of the customer satisfy the predetermined condition, predetermined information is transmitted to the customer. The predetermined information enables reception of a predetermined instruction from the

25 customer. Then, in the system, in a case in which the predetermined instruction is

received from the customer, the notification of the predetermined information is invalidated (a status of being prohibited) for the customer. In addition, the system may be referred to as not only the analysis system 1 but also a monitoring system or the like. [0118]

5 <Configuration Example>

As one configuration example, an analysis device (the analysis device 41 in this embodiment) includes: an acquisition unit (the function of the acquisition unit 112 in this embodiment) that acquires target information (a log in this embodiment) relating to a first terminal device (the terminal device 52 in this embodiment); an analysis executing unit
10 (the function of the analysis executing unit 113 in this embodiment) that determines whether or not the target information acquired by the acquisition unit satisfies a first condition (a detection rule in this embodiment); a notification unit (the function of the notification unit 114 in this embodiment) that notifies the first terminal device of first information (information of an alert in this embodiment) in a case in which it is
15 determined by the analysis executing unit that the target information satisfies the first condition; an information accepting unit (the function of the notification unit 114 in this embodiment) that accepts second information (information of “erroneous detection” or information of “non-target” in this embodiment) from the first terminal device for the first information notified by the notification unit; and a notification prohibiting unit (the
20 function of the erroneous detection control unit 115 in this embodiment) that prohibits notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first information. [0119]

As one configuration example, in the analysis device, the first condition is a rule
25 for detecting a problem, the first information is information of an alert corresponding to

the problem, and the second information is information for instructing that there is an error in the alert.

As one configuration example, in the analysis device, the notification prohibiting unit stops the notification of the first information according to the first condition (may be the same as that before stop or be changed in this embodiment) for the first terminal device for a predetermined period and resumes the notification of the first information according to the first condition after the predetermined period elapses.

As one configuration example, the analysis device includes a change unit (the management unit 116 in this embodiment) that changes the first condition.

As one configuration example, the analysis device includes a management unit (the management unit 116 in this embodiment) that manages a status of the notification of the first information according to the first condition, the status at least includes a status of being prohibited, and a search for the first information can be performed using the status of the notification.

As one configuration example, in the analysis device, the notification prohibiting unit prohibits notification of the first information for the first terminal device on the basis of a second condition (an alert rule in this embodiment) for specifying the prohibition of the notification of the first information for the first terminal device.

As one example, in the analysis device, the target information is a log relating to security.

[0120]

As one configuration example, a terminal device (the terminal device 52 in this embodiment) includes: a notification reception control unit (the function of the notification reception control unit 231 in this embodiment) that receives notification of first information notified from an analysis device in a case in which it is determined by

an analysis device that the target information relating to the terminal device satisfies a first condition; an instruction accepting unit (the function of the operation unit 213 and the function of the instruction transmission control unit 232 in this embodiment) that accepts a predetermined instruction (an instruction for selecting “erroneous detection” or
5 an instruction for selecting “non-target” in this embodiment) for the first information received by the notification reception control unit; and an instruction transmission control unit (the function of the instruction transmission control unit 232 in this embodiment) that transmits second information including an instruction for prohibiting notification of the first information for the terminal device to the analysis device in a case in which the
10 instruction is accepted for the first information.

[0121]

In addition, the present invention may be performed in various forms including a device such as a terminal device, an analysis device, or the like, a system such as an analysis system or the like, a method such as an analysis method or the like, a program, a
15 recording medium having a program recorded thereon, and the like. As the recording medium, for example, a temporary recording medium may be used.

[0122]

[Type of log]

In this embodiment, a case in which logs of a security sensor are used as logs
20 that are analysis targets has been illustrated. As logs of the security sensor, for example, there are logs of a firewall (FW), a new generation firewall (NGFW), an intrusion prevention system (IPS), an intrusion detection system (IDS), unified threat management (UTM), a web application firewall (WAF), and the like.

[0123]

25 As one example, a device that detects logs may be a device of an intrusion

prevention system (IPS) that prevents unauthorized intrusion in a computer network.
For example, the device may detect logs having a likelihood of an unauthorized relation.

As another example, a device that detects logs may be a device of a firewall (FW) that blocks communication that should not be passed. For example, the device
5 may detect both a log having a likelihood of an unauthorized relation and a log having no unauthorized relation.

Generally, when the IPS and the firewall are compared with each other, in the firewall, there are also logs relating to signals that have passed through it, and thus the amount of data may be easily increased, and the IPS has a high density of logs having a
10 likelihood of having problems.

[0124]

As a log that is an analysis target, other logs may be used. As other logs, for example, there are an authentication log, an error log, a terminal scan log, a communication log, a program operating log, and application operating log, and the like.

15 As the authentication log, for example, there are logs of an active directory, a Berkeley Internet name domain (BIND), a domain name system (DNS), and the like.

As the error log, for example, there are logs of WinEvt and the like.

As the terminal scan log, there are logs of an antivirus, an endpoint detection and response (EDR), and the like.

20 As the communication log, there are logs of a proxy, a mail, a file access, a database (DB) access, and the like.

As the program operating log, for example, there are logs such as a boot log, dmesg, and the like. As the application operating log, for example, there are logs such as an event log, an inherent log, and the like.

25 [0125]

In this embodiment, although a case in which a log is used as an analysis target has been illustrated, information other than a log may be used as an analysis target.

As the information other than a log, for example, there is information of a settings of an operating system (OS).

5 As the information of settings of an OS, for example, there are information of a registry and the like.

In addition, for example, a history of reading a web, a history of operations, a login history, or the like may be used.

[0126]

10 In this embodiment, although a case in which one type of log is detected by one log detecting device 51 has been illustrated, a configuration in which two or more log detecting devices are provided, and two or more types of log are detected may be used.

In addition, the log detecting device, for example, may be provided outside the terminal device 52 or may be provided as an internal function of the terminal device 52.

15 [0127]

For example, information of a plurality of different types of logs may be stored in a form in which they are mixed in order of time or the like. For example, information for specifying a sensor that has detected each log is added to the log. The logs can be distinguished on the basis of the information. Accordingly, information of a

20 predetermined type of log can be extracted from information in which information of a plurality of different types of logs is mixed.

[0128]

In the analysis device 41, an analysis of logs that is performed by the analysis executing unit 113, for example, may be performed for each type of log or may be

25 performed for two or more types of logs altogether.

[0129]

As above, by recording (storing) a program for realizing the function of each device according to embodiments (for example, the terminal device 52, the analysis device 41, or the like) in a computer-readable recording medium (storage medium) and
5 causing a computer system to read and execute the program recorded on this recording medium, the process can be performed.

In addition, a “computer system” described here includes an operating system and hardware such as peripheral devices.

In addition, a “computer-readable recording medium” represents a writable
10 nonvolatile memory such as a flexible disk, a magneto-optical disc, a read only memory (ROM), or a flash memory, a portable medium such as a digital versatile disc (DVD), or a storage device such as a hard disk that is built into a computer system or the like.

Furthermore, a “computer-readable recording medium” includes a server in a case in which a program is transmitted through a network such as the Internet or a
15 communication line such as a telephone line or a device that stores a program for a predetermined time such as a volatile memory (for example, a DRAM) disposed inside a computer system that serves as a client.

In addition, the program described above may be transmitted from a computer system storing this program in a storage device or the like to another computer system
20 through a transmission medium or a transmission wave in a transmission medium.

Here, the “transmission medium” transmitting a program represents a medium having an information transmitting function such as a network (communication network) including the Internet and the like or a communication line (communication wire) including a telephone line.

25 The program described above may be used for realizing a part of the functions

described above. In addition, the program described above may be a program realizing the functions described above by being combined with a program recorded in the computer system in advance, a so-called a differential file (differential program).

[0130]

5 In addition, although the present invention has been described using embodiments, the technical scope of the present invention is not limited to the embodiments described above. It is apparent to persons skilled in the art that various changes and employment of a substituent form can be performed without departing from the spirit and the scope of the present invention.

10 [Reference Signs List]

[0131]

	1 analysis system
	11 analysis unit
	21 to 23 terminal unit
15	31 network
	41 analysis device
	42 web server device
	43 mail server device
	51 log detecting device
20	52 terminal device
	111, 216 storage unit
	112 acquisition unit
	113 analysis executing unit
	114 notification unit
25	115 erroneous detection control unit

	116 management unit
	131 reception unit
	151 search processing unit
	211 input unit
5	212 output unit
	213, 4012 operation unit
	214, 4013 display unit
	215 communication unit
	217 control unit
10	231 notification reception control unit
	232 instruction transmission control unit
	233 search control unit
	2011, 2111, 2211 display details
	2121 attribute area
15	2122 handling status area
	2123 details area
	2131, 2221 button
	4001 information processing device
	4011 processor
20	4014 storage device
	4015 memory
	4016 input/output interface
	4017 network interface

Claims

1. An analysis device comprising:

an acquisition unit that acquires target information relating to a first terminal device;

an analysis executing unit that determines whether or not the target information acquired by the acquisition unit satisfies a first condition;

a notification unit that notifies the first terminal device of first information in a case in which it is determined by the analysis executing unit that the target information satisfies the first condition;

an information accepting unit that accepts second information from the first terminal device for the first information notified by the notification unit; and

a notification prohibiting unit that prohibits notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first information,

wherein the notification prohibiting unit stops the notification of the first information according to the first condition for the first terminal device for a predetermined period and resumes the notification of the first information according to the first condition after the predetermined period elapses.

2. An analysis device comprising:

an acquisition unit that acquires target information relating to a first terminal device;

an analysis executing unit that determines whether or not the target information acquired by the acquisition unit satisfies a first condition;

a notification unit that notifies the first terminal device of first information in a case in which it is determined by the analysis executing unit that the target information satisfies the first condition;

an information accepting unit that accepts second information from the first terminal device for the first information notified by the notification unit;

a notification prohibiting unit that prohibits notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first information; and

a management unit that manages a status of the notification of the first information according to the first condition,

wherein the status includes at least a status of being prohibited, and

wherein a search for the first information can be performed using the status of the notification.

3. An analysis device comprising:

an acquisition unit that acquires target information relating to a first terminal device;

an analysis executing unit that determines whether or not the target information acquired by the acquisition unit satisfies a first condition;

a notification unit that notifies the first terminal device of first information in a case in which it is determined by the analysis executing unit that the target information satisfies the first condition;

an information accepting unit that accepts second information from the first terminal device for the first information notified by the notification unit; and

a notification prohibiting unit that prohibits notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first information,

wherein the notification prohibiting unit prohibits notification of the first information for the first terminal device on the basis of a second condition for specifying the prohibition

of the notification of the first information for the first terminal device.

4. An analysis device comprising:

an acquisition unit that acquires target information relating to a first terminal device;

an analysis executing unit that determines whether or not the target information acquired by the acquisition unit satisfies a first condition;

a notification unit that notifies the first terminal device of first information in a case in which it is determined by the analysis executing unit that the target information satisfies the first condition;

an information accepting unit that accepts second information from the first terminal device for the first information notified by the notification unit; and

a notification prohibiting unit that prohibits notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first information,

wherein the target information is a log relating to security.

5. The analysis device according to any one of claims 1 to 4,

wherein the first condition is a rule for detecting a problem,

wherein the first information is information of an alert corresponding to the problem,
and

wherein the second information is information for instructing that there is an error in the alert.

6. The analysis device according to any one of claims 1 to 5, further comprising a change unit that changes the first condition.

7. A terminal device comprising:

a notification reception control unit that receives notification of first information relating to security notified from an analysis device in a case in which it is determined by the analysis device that target information relating to the terminal device having a detection device setting a log relating to security as target information, detecting the target information relating to the terminal device, and transmitting the target information to the analysis device satisfies a first condition;

an instruction accepting unit that accepts a predetermined instruction relating to the security for the first information received by the notification reception control unit; and

an instruction transmission control unit that transmits second information including an instruction for prohibiting notification of the first information relating to the security for the terminal device to the analysis device in a case in which the instruction is accepted for the first information.

8. The terminal device according to claim 7,

wherein the first condition is a rule for detecting a problem,

wherein the first information is information of an alert corresponding to the problem,

and

wherein the second information is information for instructing that there is an error in the alert.

9. An analysis system comprising:

a first terminal device; and

an analysis device,

wherein the analysis device includes:

an acquisition unit that acquires target information relating to a first terminal device;

an analysis executing unit that determines whether or not the target information acquired by the acquisition unit satisfies a first condition;

a notification unit that notifies the first terminal device of first information in a case in which it is determined by the analysis executing unit that the target information satisfies the first condition;

an information accepting unit that accepts second information from the first terminal device for the first information notified by the notification unit; and

a notification prohibiting unit that prohibits notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first information,

wherein the first terminal device includes:

a notification reception control unit that receives notification of the first information notified from the analysis device;

an instruction accepting unit that accepts a predetermined instruction for the first information received by the notification reception control unit; and

an instruction transmission control unit that transmits the second information to the analysis device in a case in which the instruction is accepted for the first information, and

wherein the notification prohibiting unit stops the notification of the first information according to the first condition for the first terminal device for a predetermined period and resumes the notification of the first information according to the first condition after the predetermined period elapses.

10. An analysis system comprising:

a first terminal device; and

an analysis device,

wherein the analysis device includes:

an acquisition unit that acquires target information relating to a first terminal device;

an analysis executing unit that determines whether or not the target information acquired by the acquisition unit satisfies a first condition;

a notification unit that notifies the first terminal device of first information in a case in which it is determined by the analysis executing unit that the target information satisfies the first condition;

an information accepting unit that accepts second information from the first terminal device for the first information notified by the notification unit;

a notification prohibiting unit that prohibits notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first information; and

a management unit that manages a status of the notification of the first information according to the first condition,

wherein the first terminal device includes:

a notification reception control unit that receives notification of the first information notified from the analysis device;

an instruction accepting unit that accepts a predetermined instruction for the first information received by the notification reception control unit; and

an instruction transmission control unit that transmits the second information to the analysis device in a case in which the instruction is accepted for the first information,

wherein the status at least includes a status of being prohibited, and

wherein a search for the first information can be performed using the status of the

notification.

11. An analysis system comprising:

a first terminal device; and

an analysis device,

wherein the analysis device includes:

an acquisition unit that acquires target information relating to a first terminal device;

an analysis executing unit that determines whether or not the target information acquired by the acquisition unit satisfies a first condition;

a notification unit that notifies the first terminal device of first information in a case in which it is determined by the analysis executing unit that the target information satisfies the first condition;

an information accepting unit that accepts second information from the first terminal device for the first information notified by the notification unit; and

a notification prohibiting unit that prohibits notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first information,

wherein the first terminal device includes:

a notification reception control unit that receives notification of the first information notified from the analysis device;

an instruction accepting unit that accepts a predetermined instruction for the first information received by the notification reception control unit; and

an instruction transmission control unit that transmits the second information to the analysis device in a case in which the instruction is accepted for the first information, and

wherein the notification prohibiting unit prohibits notification of the first information

for the first terminal device on the basis of a second condition for specifying the prohibition of the notification of the first information for the first terminal device.

12. An analysis system comprising:

a first terminal device; and

an analysis device,

wherein the analysis device includes:

an acquisition unit that acquires target information relating to a first terminal device;

an analysis executing unit that determines whether or not the target information acquired by the acquisition unit satisfies a first condition;

a notification unit that notifies the first terminal device of first information in a case in which it is determined by the analysis executing unit that the target information satisfies the first condition;

an information accepting unit that accepts second information from the first terminal device for the first information notified by the notification unit; and

a notification prohibiting unit that prohibits notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first information,

wherein the first terminal device includes:

a notification reception control unit that receives notification of the first information notified from the analysis device;

an instruction accepting unit that accepts a predetermined instruction for the first information received by the notification reception control unit; and

an instruction transmission control unit that transmits the second information to the analysis device in a case in which the instruction is accepted for the first information, and

wherein the target information is a log relating to security.

13. The analysis system according to any one of claims 9 to 12,
 wherein the first condition is a rule for detecting a problem,
 wherein the first information is information of an alert corresponding to the problem,
 and
 wherein the second information is information for instructing that there is an error in
 the alert.

14. The analysis system according to any one of claims 9 to 13, wherein the analysis
 device further includes a change unit that changes the first condition.

15. An analysis method in an analysis system including a first terminal device and an
 analysis device, the analysis method comprising:

Acquiring, by using the analysis device, target information relating to a first terminal
 device, determining, by using the analysis device, whether or not the acquired target
 information satisfies a first condition, and notifying, by using the analysis device, the first
 terminal device of first information in a case in which it is determined that the target
 information satisfies the first condition;

receiving, by using the first terminal device, notification of the first information
 notified from the analysis device and transmitting second information to the analysis device
 in a case in which a predetermined instruction is accepted for the received first information;

prohibiting, by using the analysis device, the notification of the first information for
 the first terminal device in a case in which the second information is accepted from the first
 terminal device; and

stopping, by using the analysis device, the notification of the first information according to the first condition for the first terminal device for a predetermined period as the prohibition of the notification and resuming, by using the analysis device, the notification of the first information according to the first condition after the predetermined period elapses.

16. An analysis method in an analysis system including a first terminal device and an analysis device, the analysis method comprising:

acquiring, by using the analysis device, target information relating to a first terminal device, determining whether or not the acquired target information satisfies a first condition, and notifying the first terminal device of first information in a case in which it is determined that the target information satisfies the first condition;

receiving, by using the first terminal device, notification of the first information notified from the analysis device and transmitting, by using the first terminal device, second information to the analysis device in a case in which a predetermined instruction is accepted for the received first information;

prohibiting, by using the analysis device, the notification of the first information for the first terminal device in a case in which the second information is accepted from the first terminal device; and

managing, by using the analysis device, a status of the notification of the first information according to the first condition,

wherein the status at least includes a status of being prohibited, and

wherein a search for the first information can be performed using the status of the notification.

17. An analysis method in an analysis system including a first terminal device and an

analysis device, the analysis method comprising:

acquiring, by using the analysis device, target information relating to a first terminal device, determining whether or not the acquired target information satisfies a first condition, and notifying, by using the analysis device, the first terminal device of first information in a case in which it is determined that the target information satisfies the first condition;

receiving, by using the first terminal device, notification of the first information notified from the analysis device and transmitting second information to the analysis device in a case in which a predetermined instruction is accepted for the received first information;

prohibiting, by using the analysis device, the notification of the first information for the first terminal device in a case in which the second information is accepted from the first terminal device; and

prohibiting, by using the analysis device, notification of the first information for the first terminal device on the basis of a second condition for specifying the prohibition of the notification of the first information for the first terminal device as prohibition of the notification.

18. An analysis method in an analysis system including a first terminal device and an analysis device, the analysis method comprising:

acquiring, by using the analysis device, target information relating to a first terminal device, determining, by using the analysis device, whether or not the acquired target information satisfies a first condition, and notifying, by using the analysis device, the first terminal device of first information in a case in which it is determined that the target information satisfies the first condition;

receiving, by using the first terminal device, notification of the first information notified from the analysis device and transmitting second information to the analysis device

in a case in which a predetermined instruction is accepted for the received first information;
and

prohibiting, by using the analysis device, the notification of the first information for the first terminal device in a case in which the second information is accepted from the first terminal device,

wherein the target information is a log relating to security.

19. The analysis method according to any one of claims 15 to 18,
wherein the first condition is a rule for detecting a problem,
wherein the first information is information of an alert corresponding to the problem,
and

wherein the second information is information for instructing that there is an error in the alert.

20. The analysis method according to any one of claims 15 to 19, wherein the analysis device changes the first condition.

21. A program causing a computer configuring an analysis device to perform:
a function of acquiring target information relating to a first terminal device;
a function of determining whether or not the acquired target information satisfies a first condition;

a function of notifying the first terminal device of first information in a case in which it is determined that the target information satisfies the first condition;

a function of accepting second information from the first terminal device for the notified first information; and

a function of prohibiting notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first information,

wherein the function of prohibiting notification stops the notification of the first information according to the first condition for the first terminal device for a predetermined period and resumes the notification of the first information according to the first condition after the predetermined period elapses.

22. A program causing a computer configuring an analysis device to perform:

a function of acquiring target information relating to a first terminal device;

a function of determining whether or not the acquired target information satisfies a first condition;

a function of notifying the first terminal device of first information in a case in which it is determined that the target information satisfies the first condition;

a function of accepting second information from the first terminal device for the notified first information;

a function of prohibiting notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first information; and

a function of managing a status of the notification of the first information according to the first condition,

wherein the status at least includes a status of being prohibited, and

wherein a search for the first information can be performed using the status of the notification.

23. A program causing a computer configuring an analysis device to perform:

- a function of acquiring target information relating to a first terminal device;
- a function of determining whether or not the acquired target information satisfies a first condition;
- a function of notifying the first terminal device of first information in a case in which it is determined that the target information satisfies the first condition;
- a function of accepting second information from the first terminal device for the notified first information; and
- a function of prohibiting notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for the first information,

wherein the function of prohibiting notification prohibits notification of the first information for the first terminal device on the basis of a second condition for specifying the prohibition of the notification of the first information for the first terminal device.

24. A program causing a computer configuring an analysis device to perform:

- a function of acquiring target information relating to a first terminal device;
- a function of determining whether or not the acquired target information satisfies a first condition;
- a function of notifying the first terminal device of first information in a case in which it is determined that the target information satisfies the first condition;
- a function of accepting second information from the first terminal device for the notified first information; and
- a function of prohibiting notification of the first information to the first terminal device in a case in which the second information is accepted from the first terminal device for

the first information,

wherein the target information is a log relating to security.

25. The program according to any one of claims 21 to 24,

wherein the first condition is a rule for detecting a problem,

wherein the first information is information of an alert corresponding to the problem,

and

wherein the second information is information for instructing that there is an error in the alert.

26. The program according to any one of claims 21 to 25, further causing the computer to perform a function of changing the first condition.

27. A program causing a computer configuring a terminal device having a detection device setting a log relating to security as target information, detecting the target information relating to the terminal device, and transmitting the target information to an analysis device to perform:

a function of receiving notification of first information relating to security notified from the analysis device in a case in which it is determined by the analysis device that the target information relating to the terminal device satisfies a first condition;

a function of accepting a predetermined instruction relating to the security for the received first information; and

a function of transmitting second information including an instruction for prohibiting notification of the first information relating to the security for the terminal device to the analysis device in a case in which the instruction is accepted for the first information.

28. The program according to claim 27,
wherein the first condition is a rule for detecting a problem,
wherein the first information is information of an alert corresponding to the problem,
and
wherein the second information is information for instructing that there is an error in
the alert.