

## 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.