

necessary to reduce the time needed to take countermeasures against the vulnerability.

The technique disclosed in the above-mentioned Patent Literature 1 stores, in a database, countermeasures taken against vulnerabilities of a terminal in association with a keyword indicating the type of vulnerabilities. Specifically, the technique disclosed in Patent Literature 1 is a technique that stores, in a database, countermeasures against vulnerabilities which have been actually taken in a terminal, and it is not a technique that reduces the time needed to take countermeasures against vulnerabilities.

10 [0006]

An object of the present disclosure is to solve the above-described problem, and to provide a technique capable of reducing the time needed to take countermeasures against vulnerabilities.

Solution to Problem

15 [0007]

According to a first aspect of the present disclosure, a security risk management system includes a server, and an agent unit included in a terminal, wherein the server transmits vulnerability information to the agent unit before a release date and time of the vulnerability information, the agent unit investigates presence or absence of vulnerabilities in the terminal based on information regarding a method for vulnerability investigation contained in the vulnerability information, and transmits vulnerability investigation results containing the investigation results to the server before the release date and time of the vulnerability information, and the server presents the vulnerability information and the vulnerability investigation results on or after the release date and time of the vulnerability information.

[0008]

According to a second aspect of the present disclosure, a server includes a communication unit configured to transmit, to an agent unit included in a terminal, vulnerability information before a release date and time of the vulnerability information, and receives, from the agent unit, vulnerability investigation results containing investigation results regarding presence or absence of vulnerabilities in the terminal investigated by the agent unit based on information regarding a method for vulnerability investigation contained in the vulnerability information before the release date and time of the vulnerability information,

35

and a presentation unit configured to present the vulnerability information and the vulnerability investigation results on or after the release date and time of the vulnerability information.

[0009]

5 According to a third aspect of the present disclosure, a control method is a control method of a server, including a transmission step of transmitting, to an agent unit included in a terminal, vulnerability information before a release date and time of the vulnerability information, a step of receiving, from the agent unit, vulnerability investigation results containing investigation results regarding
10 presence or absence of vulnerabilities in the terminal investigated by the agent unit based on information regarding a method for vulnerability investigation contained in the vulnerability information before the release date and time of the vulnerability information, and a presentation step of presenting the vulnerability information and the vulnerability investigation results on or after the release date
15 and time of the vulnerability information.

[0010]

 According to a fourth aspect of the present disclosure, a non-transitory computer readable medium is a non-transitory computer readable medium storing a program causing a computer to execute a transmission step of transmitting, to an
20 agent unit included in a terminal, vulnerability information before a release date and time of the vulnerability information, a step of receiving, from the agent unit, vulnerability investigation results containing investigation results regarding presence or absence of vulnerabilities in the terminal investigated by the agent unit based on information regarding a method for vulnerability investigation contained
25 in the vulnerability information before a release date and time of the vulnerability information, and a presentation step of presenting the vulnerability information and the vulnerability investigation results on or after the release date and time of the vulnerability information.

[0011]

30 According to a fifth aspect of the present disclosure, a non-transitory computer readable medium is a non-transitory computer readable medium storing a program causing a computer to execute a receiving step of receiving, from a server, vulnerability information before a release date and time of the vulnerability information, an investigation step of investigating presence or absence of
35 vulnerabilities in a terminal based on information regarding a method for

vulnerability investigation contained in the vulnerability information before a release date and time of the vulnerability information, and a step of transmitting, to the server, vulnerability investigation results containing investigation results in the investigation step before the release date and time of the vulnerability information.

Advantageous Effects of Invention

[0012]

According to the exemplary aspects of the present disclosure, it is possible to reduce the time needed to take countermeasures against vulnerabilities.

Brief Description of Drawings

[0013]

Fig. 1 is a view showing a configuration example of a security system according to a first embodiment.

Fig. 2 is a block diagram showing a block configuration example of a vulnerability information distribution system and a security risk management system according to the first embodiment.

Fig. 3 is a view showing a configuration example of the hardware configuration of a computer that implements the vulnerability information distribution system, a server and a terminal according to the first embodiment.

Fig. 4 is a flowchart showing an operation example that receives vulnerability information from a vulnerability information transmission system, creates vulnerability information data, and transmits the vulnerability information data to a server in the vulnerability information distribution system according to the first embodiment.

Fig. 5 is a view showing an example of vulnerability information data according to the first embodiment.

Fig. 6 is a flowchart showing an operation example that receives vulnerability information data from a vulnerability information distribution system and transmits the vulnerability information data to an agent unit in the server according to the first embodiment.

Fig. 7 is a flowchart showing an operation example that receives vulnerability information data from a server, investigates the presence or absence of vulnerabilities of a corresponding terminal, and transmits vulnerability

presentation is to display the information on a screen of the corresponding terminal 330.

[0028]

Note that the common key storage unit 214 in the vulnerability information distribution system 210, the common key storage unit 318 in the server 310, and the common key storage unit 325 in the agent unit 320 share a common key, and store the shared common key.

[0029]

(1-1-7) Hardware Configuration

Fig. 3 shows a configuration example of the hardware configuration of a computer 400 for implementing the vulnerability information distribution system 210 according to the first embodiment. Referring to Fig. 3, the vulnerability information distribution system 210 according to the first embodiment can be implemented by the computer 400. The computer 400 includes a processor 401, a memory 402, a storage 403, an input/output interface (input/output I/F) 404, a communication interface (communication I/F) 405 and the like. The processor 401, the memory 402, the storage 403, the input/output interface 404 and the communication interface 405 are connected through a data transmission line for transmitting and receiving data to and from one another.

[0030]

The processor 401 is a processing unit such as CPU (Central Processing Unit) or GPU (Graphics Processing Unit). The memory 402 is a memory such as RAM (Random Access Memory) or ROM (Read Only Memory). The storage 403 is a storage device such as HDD (Hard Disk Drive), SSD (Solid State Drive) or memory card. Alternatively, the storage 403 may be a memory such as RAM or ROM.

[0031]

The storage 403 stores a program for implementing the function of each processing unit (the vulnerability information receiving unit 211, the vulnerability information data creation unit 212, the vulnerability information data encryption unit 213, the vulnerability information data transmitting unit 216 etc.) included in the vulnerability information distribution system 210. The processor 401 executes each program and thereby implements the function of each processing unit. The processor 401 may execute each program after reading the program

(1-2-3) The operation of the agent unit 320 that receives vulnerability information data from the server 310, investigates the presence or absence of vulnerabilities in the corresponding terminal 330, and transmits vulnerability investigation results indicating results of the investigation to the server 310 is described with reference to Fig. 7.

[0045]

Referring to Fig. 7, in the agent unit 320, the vulnerability information data receiving unit 321 receives the vulnerability information data transmitted from the server 310 (S301). The vulnerability information data receiving unit 321 stores the received vulnerability information data into the vulnerability information data storage unit 322 (S302). The vulnerability investigation unit 323 reads the vulnerability information data from the vulnerability information data storage unit 322 (S303). When 0, which indicates "unreleased", is set to the release flag of the read vulnerability information data (Yes in S304), the vulnerability investigation unit 323 transmits the vulnerability information data to the vulnerability information data decryption unit 324. The vulnerability information data decryption unit 324 reads a common key for decryption from the common key storage unit 325, decrypts the information about the method for investigation in the vulnerability information data by using the read common key (S305), and sends the decrypted vulnerability information data back to the vulnerability investigation unit 323. The vulnerability investigation unit 323 investigates the presence or absence of vulnerabilities in the corresponding terminal 330 based on the information about the method for investigation in the vulnerability information data decrypted by the vulnerability information data decryption unit 324 (S306). On the other hand, when 1, which indicates "released", is set to the release flag of the read vulnerability information data (No in S304), because the information about the method for investigation in the read vulnerability information data is not decrypted, the vulnerability investigation unit 323 investigates the presence or absence of vulnerabilities in the corresponding terminal 330 based on the information about the method for investigation (S306). The vulnerability investigation unit 323 creates vulnerability investigation results indicating investigation results regarding the presence or absence of vulnerabilities in the corresponding terminal 330 (S307).

[0046]

a communication unit configured to transmit, to an agent unit included in a terminal, vulnerability information before a release date and time of the vulnerability information, and receives, from the agent unit, vulnerability investigation results containing investigation results regarding presence or absence of vulnerabilities in the terminal investigated by the agent unit based on information regarding a method for vulnerability investigation contained in the vulnerability information before the release date and time of the vulnerability information, and

a presentation unit configured to present the vulnerability information and the vulnerability investigation results on or after the release date and time of the vulnerability information.

(Supplementary Note 9)

The server according to Supplementary Note 8, wherein the communication unit transmits the vulnerability information to the agent unit before a release date and time of the vulnerability information, the vulnerability information containing encrypted information regarding a method for vulnerability investigation.

(Supplementary Note 10)

The server according to Supplementary Note 8 or 9, further comprising:

a vulnerability information storage unit configured to store the vulnerability information before a release date and time of the vulnerability information, the vulnerability information containing encrypted information regarding an overview of vulnerabilities, a method for investigation and a method for countermeasures, wherein

the communication unit transmits the vulnerability information to the agent unit before the release date and time of the vulnerability information, the vulnerability information containing the encrypted information regarding an overview of vulnerabilities, a method for investigation and a method for countermeasures.

(Supplementary Note 11)

The server according to Supplementary Note 10, further comprising:

a release date and time checking unit, wherein

a release flag to which a value indicating whether the vulnerability information is unreleased or released is set is added to the vulnerability information,

a transmission step of transmitting, to an agent unit included in a terminal, vulnerability information before a release date and time of the vulnerability information;

5 a step of receiving, from the agent unit, vulnerability investigation results containing investigation results regarding presence or absence of vulnerabilities in the terminal investigated by the agent unit based on information regarding a method for vulnerability investigation contained in the vulnerability information before the release date and time of the vulnerability information; and

10 a presentation step of presenting the vulnerability information and the vulnerability investigation results on or after the release date and time of the vulnerability information.

(Supplementary Note 14)

The control method according to Supplementary Note 13, wherein the transmission step transmits the vulnerability information to the agent unit before a
15 release date and time of the vulnerability information, the vulnerability information containing encrypted information regarding a method for vulnerability investigation.

(Supplementary Note 15)

20 The control method according to Supplementary Note 13 or 14, further comprising:

a step of storing, into a vulnerability information storage unit, the vulnerability information before a release date and time of the vulnerability information, the vulnerability information containing encrypted information regarding an overview of vulnerabilities, a method for investigation and a method
25 for countermeasures, wherein

the transmission step transmits the vulnerability information to the agent unit before the release date and time of the vulnerability information, the vulnerability information containing the encrypted information regarding an overview of vulnerabilities, a method for investigation and a method for
30 countermeasures.

(Supplementary Note 16)

The control method according to Supplementary Note 15, wherein

CLAIMS

1. A security risk management system comprising:
a server; and
5 an agent unit included in a terminal, wherein
the server transmits vulnerability information to the agent unit before a
release date and time of the vulnerability information,
the agent unit investigates presence or absence of vulnerabilities in the
terminal based on information regarding a method for vulnerability investigation
10 contained in the vulnerability information, and transmits vulnerability
investigation results containing the investigation results to the server before the
release date and time of the vulnerability information, and
the server presents the vulnerability information and the vulnerability
investigation results on or after the release date and time of the vulnerability
15 information.
2. The security risk management system according to Claim 1, wherein
the server transmits the vulnerability information to the agent unit before a
release date and time of the vulnerability information, the vulnerability
20 information containing encrypted information regarding a method for vulnerability
investigation, and
the agent unit decrypts the information regarding a method for
vulnerability investigation contained in the vulnerability information, and
investigates presence or absence of vulnerabilities in the terminal based on the
25 decrypted information regarding a method for vulnerability investigation before
the release date and time of the vulnerability information.
3. The security risk management system according to Claim 1 or 2,
wherein
30 the server stores the vulnerability information before a release date and
time of the vulnerability information, the vulnerability information containing
encrypted information regarding an overview of vulnerabilities, a method for
investigation and a method for countermeasures, and transmits the vulnerability
information to the agent unit before the release date and time of the vulnerability

information, the vulnerability information containing the encrypted information regarding an overview of vulnerabilities, a method for investigation and a method for countermeasures, and

the agent unit stores the vulnerability information before the release date and time of the vulnerability information, the vulnerability information containing the encrypted information regarding an overview of vulnerabilities, a method for investigation and a method for countermeasures.

4. The security risk management system according to Claim 3, wherein a release flag to which a value indicating whether the vulnerability information is unreleased or released is set is added to the vulnerability information,

the server reads the vulnerability information to which the release flag to which a value indicating "unreleased" is set is added from among the stored vulnerability information, and

when a release date and time contained in the read vulnerability information is before a current date and time, the server decrypts the information regarding an overview of vulnerabilities, a method for investigation and a method for countermeasures contained in the read vulnerability information, sets a value indicating "released" to the release flag added to the read vulnerability information, and stores the read vulnerability information again.

5. The security risk management system according to Claim 4, wherein a vulnerability information ID for identifying the vulnerability information is further added to the vulnerability information,

the vulnerability investigation results contain a vulnerability information ID for identifying the vulnerability information related to investigated vulnerabilities, a terminal ID for identifying the terminal, and investigation results indicating presence or absence of vulnerabilities in the terminal,

the server stores the vulnerability investigation results, reads the vulnerability information to which the release flag to which a value indicating "released" is set is added from among the stored vulnerability information, reads the vulnerability investigation results containing the vulnerability information ID matching with the read vulnerability information and containing investigation

results indicating presence of vulnerabilities in the terminal from among the stored vulnerability investigation results, and presents an overview and a method for countermeasures contained in the read vulnerability information and presents the terminal ID contained in the read vulnerability investigation results.

5

6. The security risk management system according to Claim 3, wherein a release flag to which a value indicating whether the vulnerability information is unreleased or released is set is added to the vulnerability information,

10 the agent unit reads the vulnerability information to which the release flag to which a value indicating "unreleased" is set is added from among the stored vulnerability information, and

when a release date and time contained in the read vulnerability information is before a current date and time, the agent unit decrypts the
15 information regarding an overview of vulnerabilities, a method for investigation and a method for countermeasures contained in the read vulnerability information, sets a value indicating "released" to the release flag added to the read vulnerability information, and stores the read vulnerability information again.

20 7. A server comprising:

a communication unit configured to transmit, to an agent unit included in a terminal, vulnerability information before a release date and time of the vulnerability information, and receives, from the agent unit, vulnerability investigation results containing investigation results regarding presence or absence
25 of vulnerabilities in the terminal investigated by the agent unit based on information regarding a method for vulnerability investigation contained in the vulnerability information before the release date and time of the vulnerability information, and

a presentation unit configured to present the vulnerability information and
30 the vulnerability investigation results on or after the release date and time of the vulnerability information.

8. A control method of a server, comprising:

a transmission step of transmitting, to an agent unit included in a terminal, vulnerability information before a release date and time of the vulnerability information;

5 a step of receiving, from the agent unit, vulnerability investigation results containing investigation results regarding presence or absence of vulnerabilities in the terminal investigated by the agent unit based on information regarding a method for vulnerability investigation contained in the vulnerability information before the release date and time of the vulnerability information; and

10 a presentation step of presenting the vulnerability information and the vulnerability investigation results on or after the release date and time of the vulnerability information.

9. A non-transitory computer readable medium storing a program causing a
15 computer to execute:

a transmission step of transmitting, to an agent unit included in a terminal, vulnerability information before a release date and time of the vulnerability information;

a step of receiving, from the agent unit, vulnerability investigation results
20 containing investigation results regarding presence or absence of vulnerabilities in the terminal investigated by the agent unit based on information regarding a method for vulnerability investigation contained in the vulnerability information before a release date and time of the vulnerability information; and

a presentation step of presenting the vulnerability information and the
25 vulnerability investigation results on or after the release date and time of the vulnerability information.

10. A non-transitory computer readable medium storing a program causing
a computer to execute:

30 a receiving step of receiving, from a server, vulnerability information before a release date and time of the vulnerability information;

an investigation step of investigating presence or absence of vulnerabilities in a terminal based on information regarding a method for vulnerability investigation

contained in the vulnerability information before a release date and time of the vulnerability information; and

- a step of transmitting, to the server, vulnerability investigation results containing investigation results in the investigation step before the release date
- 5 and time of the vulnerability information.