US 20250265354A1

(19) **United States**

(12) **Patent Application Publication**

WADA et al.

(10) **Pub. No.: US 2025/0265354 A1**

(43) **Pub. Date: Aug. 21, 2025**

(54) **INFORMATION PROCESSING SYSTEM, INFORMATION PROCESSING METHOD, AND COMPUTER PROGRAM PRODUCT**

(71) Applicant: **KABUSHIKI KAISHA TOSHIBA**, Tokyo (JP)

(72) Inventors: **Hiroho WADA**, Yokohama Kanagawa (JP); **Tatsuya UEHARA**, Kawasaki Kanagawa (JP); **Jun KANAI**, Inagi Tokyo (JP); **Yurie SHINKE**, Kawasaki Kanagawa (JP); **Ryuiti KOIKE**, Kawasaki Kanagawa (JP); **Hayeong SHIN**, Ota Tokyo (JP); **Yuto MASHIMA**, Yokohama Kanagawa (JP)

(73) Assignee: **KABUSHIKI KAISHA TOSHIBA**, Tokyo (JP)

(21) Appl. No.: **19/051,309**

(22) Filed: **Feb. 12, 2025**

(30) **Foreign Application Priority Data**

Feb. 19, 2024 (JP) 2024-022603

Publication Classification

(51) **Int. Cl.**
G06F 21/57 (2013.01)

(52) **U.S. Cl.**
CPC *G06F 21/577* (2013.01); *G06F 2221/033* (2013.01)

(57) **ABSTRACT**

According to an embodiment, an information processing system includes one or more hardware processors. The one or more hardware processors are configured to: identify a threat type capable of being countered by installed software being security countermeasure software installed in a target system, from among security countermeasure software with a reported vulnerability; calculate a first risk value when a countermeasure is taken by the installed software for a threat of the identified threat type; calculate a second risk value when no countermeasure is taken by the installed software for the threat of the identified threat type; and output damage potential information including risk value change information representing a change in the second risk value with respect to the first risk value.

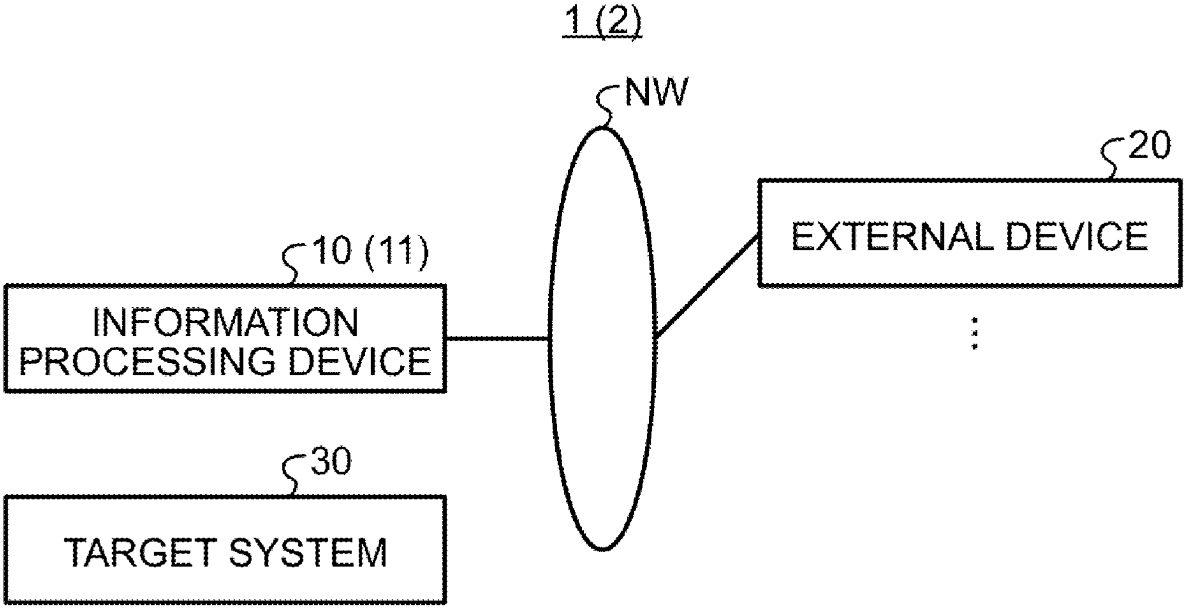


FIG.1

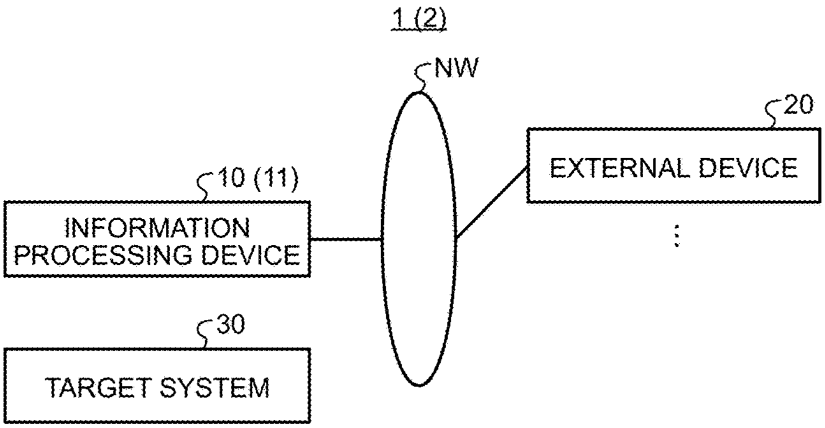

1 (2)
NW
20
EXTERNAL DEVICE
⋮
10 (11)
INFORMATION PROCESSING DEVICE
30
TARGET SYSTEM

FIG.2

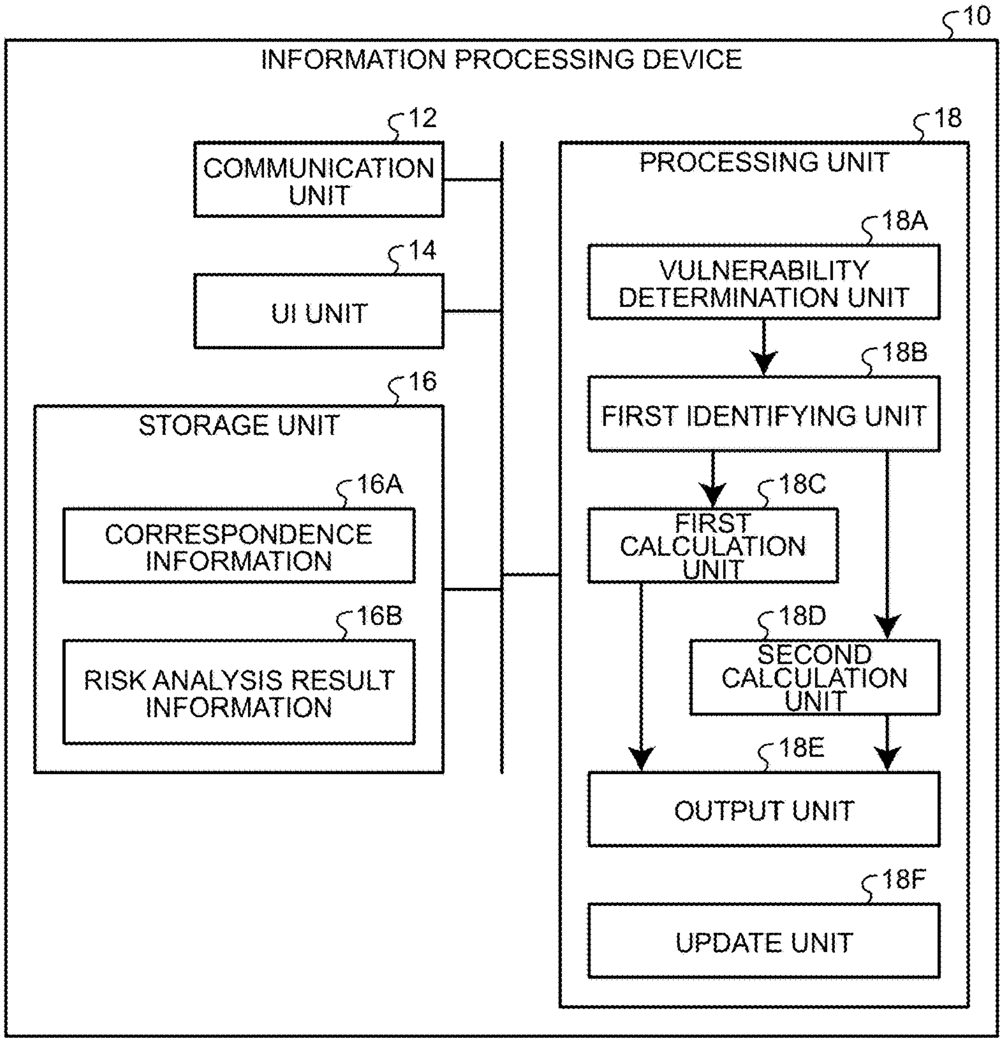
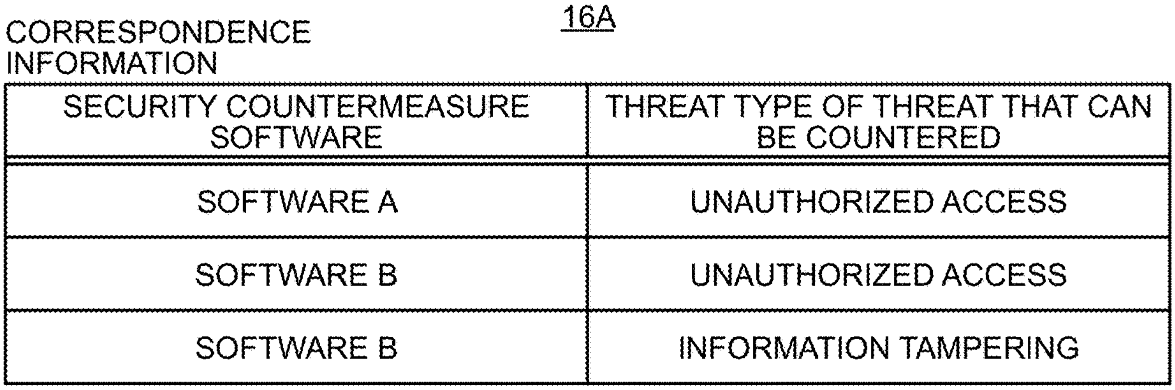

10
INFORMATION PROCESSING DEVICE
12
COMMUNICATION UNIT
14
UI UNIT
16
STORAGE UNIT
16A
CORRESPONDENCE INFORMATION
16B
RISK ANALYSIS RESULT INFORMATION
18
PROCESSING UNIT
18A
VULNERABILITY DETERMINATION UNIT
18B
FIRST IDENTIFYING UNIT
18C
FIRST CALCULATION UNIT
18D
SECOND CALCULATION UNIT
18E
OUTPUT UNIT
18F
UPDATE UNIT

FIG.3



16A

CORRESPONDENCE INFORMATION

SECURITY COUNTERMEASURE SOFTWARE	THREAT TYPE OF THREAT THAT CAN BE COUNTERED
SOFTWARE A	UNAUTHORIZED ACCESS
SOFTWARE B	UNAUTHORIZED ACCESS
SOFTWARE B	INFORMATION TAMPERING

FIG.4

16B

RISK ANALYSIS RESULT INFORMATION

ITEM NUMBER	ASSET TYPE	TARGET DEVICE	EVALUATION INDEX				THREAT TYPE	DESCRIPTION	COUNTERMEASURE								COUNTERMEASURE LEVEL
			THREAT LEVEL	VULNERABILITY LEVEL	IMPORTANCE OF ASSET	RISK VALUE			DEFENSE				DETECTION/DAMAGE ASCERTAINMENT		BUSINESS CONTINUITY		EACH THREAT
									INTRUSION/DIFFUSION STAGE		PURPOSE ACCOMPLISHMENT STAGE						
1	INFORMATION SYSTEM ASSET	CONTROL SERVER	2	2	3	B	UNAUTHORIZED ACCESS	INTRUDE DEVICE VIA NETWORK AND EXECUTE ATTACK	FW								2
									ONE-WAY GATEWAY								
									PROXY SERVER								
									WAF								
									AUTHENTICATION OF COMMUNICATION PARTNER	○							
2			3	2		A	INFORMATION TAMPERING	TAMPER WITH INFORMATION STORED IN DEVICE	AUTHORITY MANAGEMENT	○					DATA BACKUP	○	2
									ACCESS CONTROL								
									DATA SIGNATURE								
3			3	1		B	MALWARE INFECTION	INFECT AND ACTIVATE MALWARE ON DEVICE TO BE ATTACKED	ANTIVIRUS	○			DEVICE ANOMALITY DETECTION				3
									PROCESS STARTUP AUTHORITY BY WHITELIST	○			DEVICE FATE MONITORING				
									PATCH APPLICATION				LOG COLLECTION /ANALYSIS				
...																	

FIG.5

40

DAMAGE POTENTIAL INFORMATION					
DATE AND TIME	VULNERABILITY	SOFTWARE NAME	THREAT TYPE	RISK VALUE CHANGE INFORMATION	INFORMATION ON PRESENCE OR ABSENCE OF DAMAGE POTENTIAL
X YEAR X MONTH X DAY	CVE-XXX	SOFTWARE A	UNAUTHORIZED ACCESS	B→A	PRESENCE OF DAMAGE POTENTIAL

FIG.6

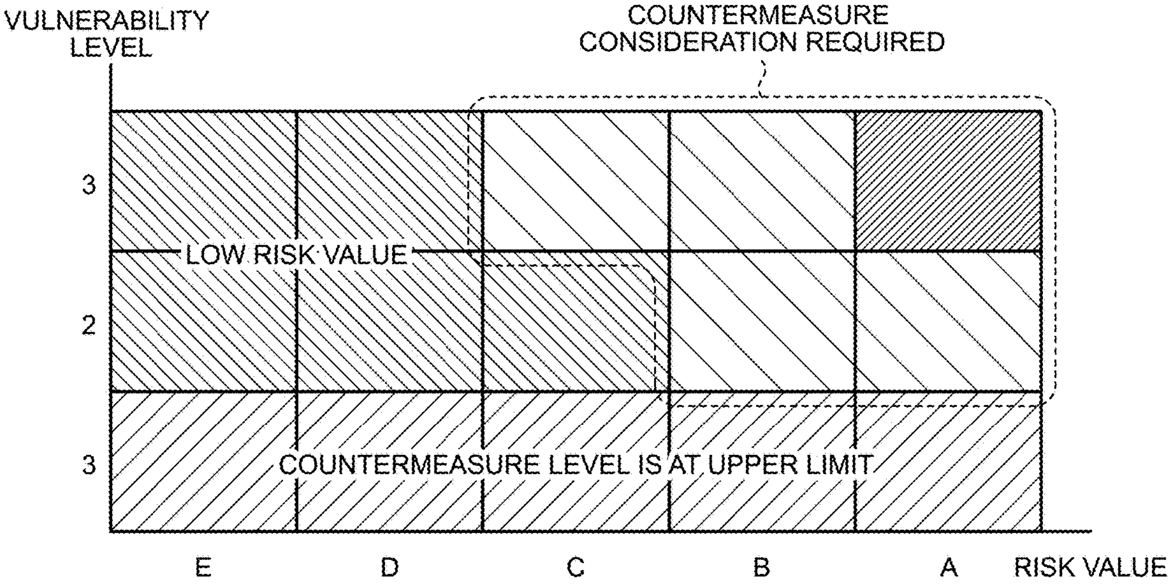


FIG.7

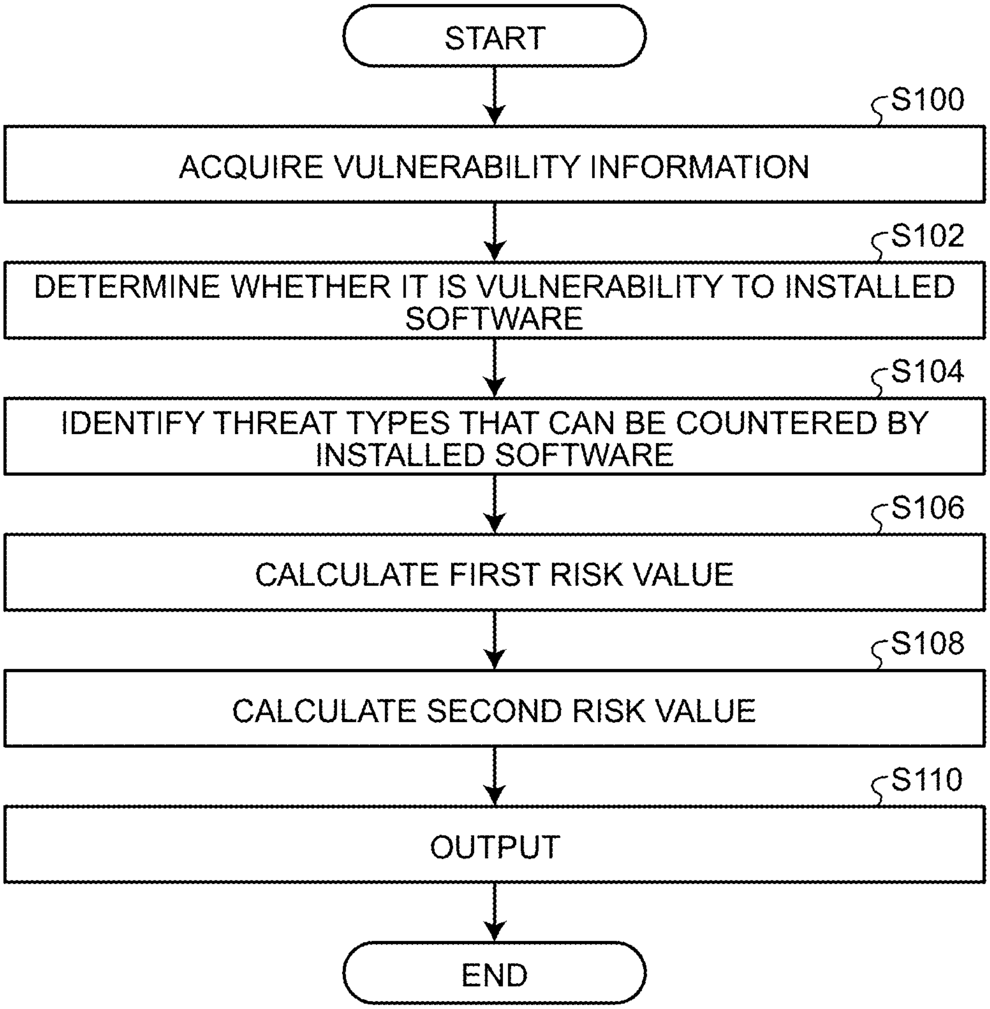

START
S100
ACQUIRE VULNERABILITY INFORMATION
S102
DETERMINE WHETHER IT IS VULNERABILITY TO INSTALLED SOFTWARE
S104
IDENTIFY THREAT TYPES THAT CAN BE COUNTERED BY INSTALLED SOFTWARE
S106
CALCULATE FIRST RISK VALUE
S108
CALCULATE SECOND RISK VALUE
S110
OUTPUT
END

FIG.8

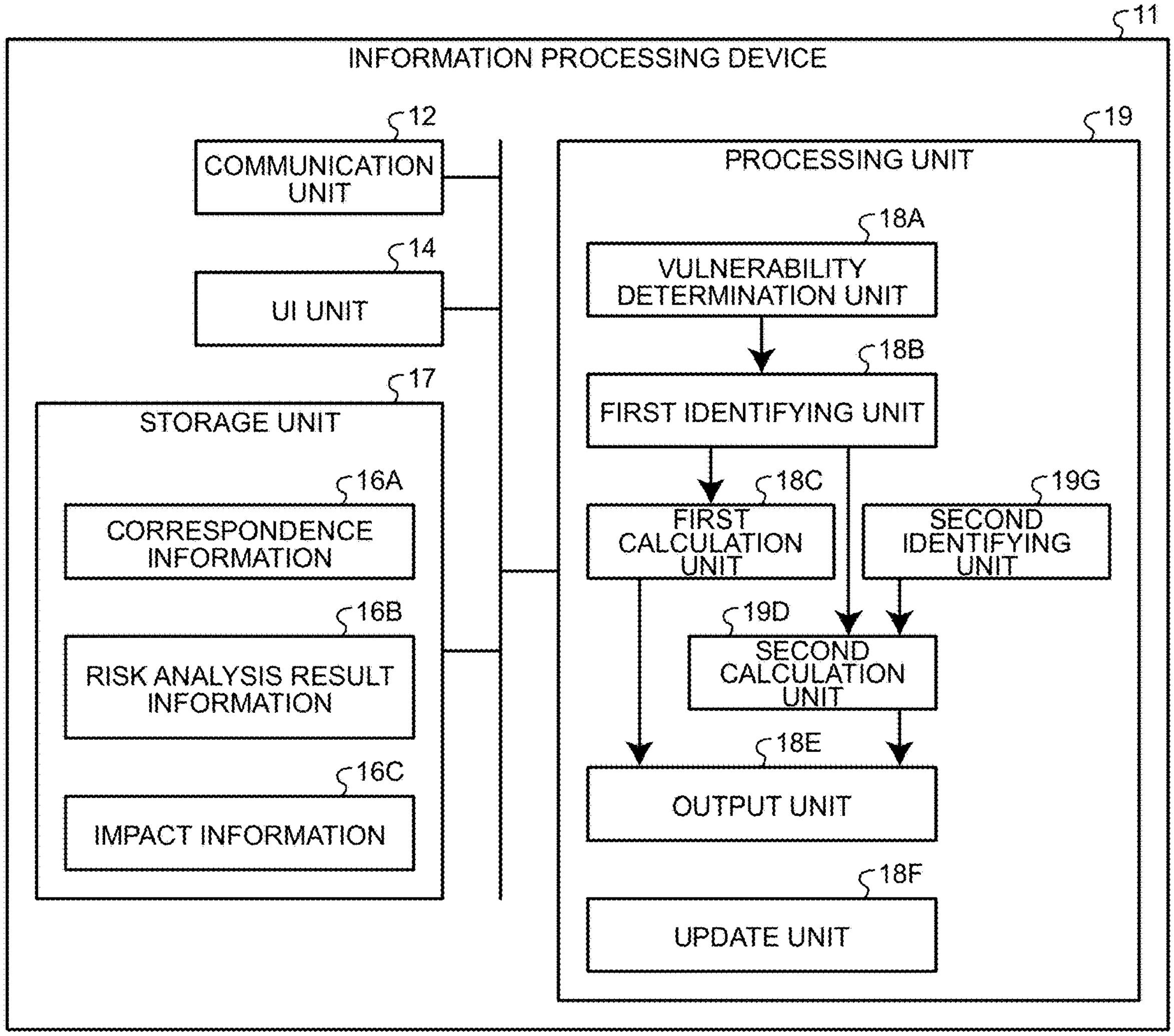
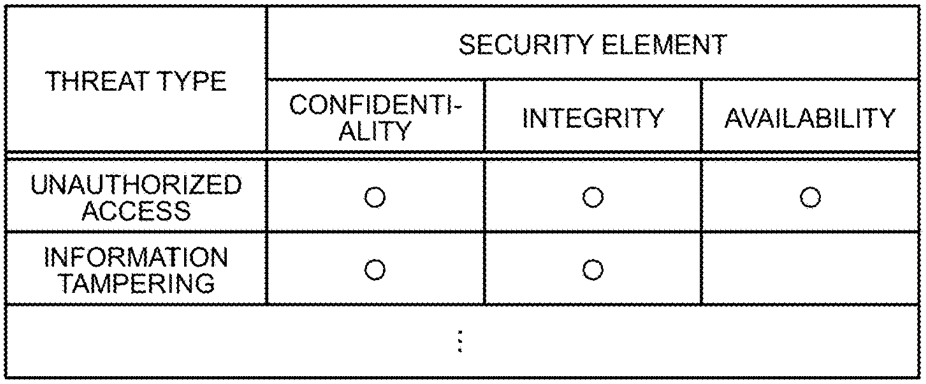


FIG.9

16C

IMPACT INFORMATION



THREAT TYPE	SECURITY ELEMENT		
	CONFIDENTI-ALITY	INTEGRITY	AVAILABILITY
UNAUTHORIZED ACCESS	○	○	○
INFORMATION TAMPERING	○	○	
⋮			

FIG.10

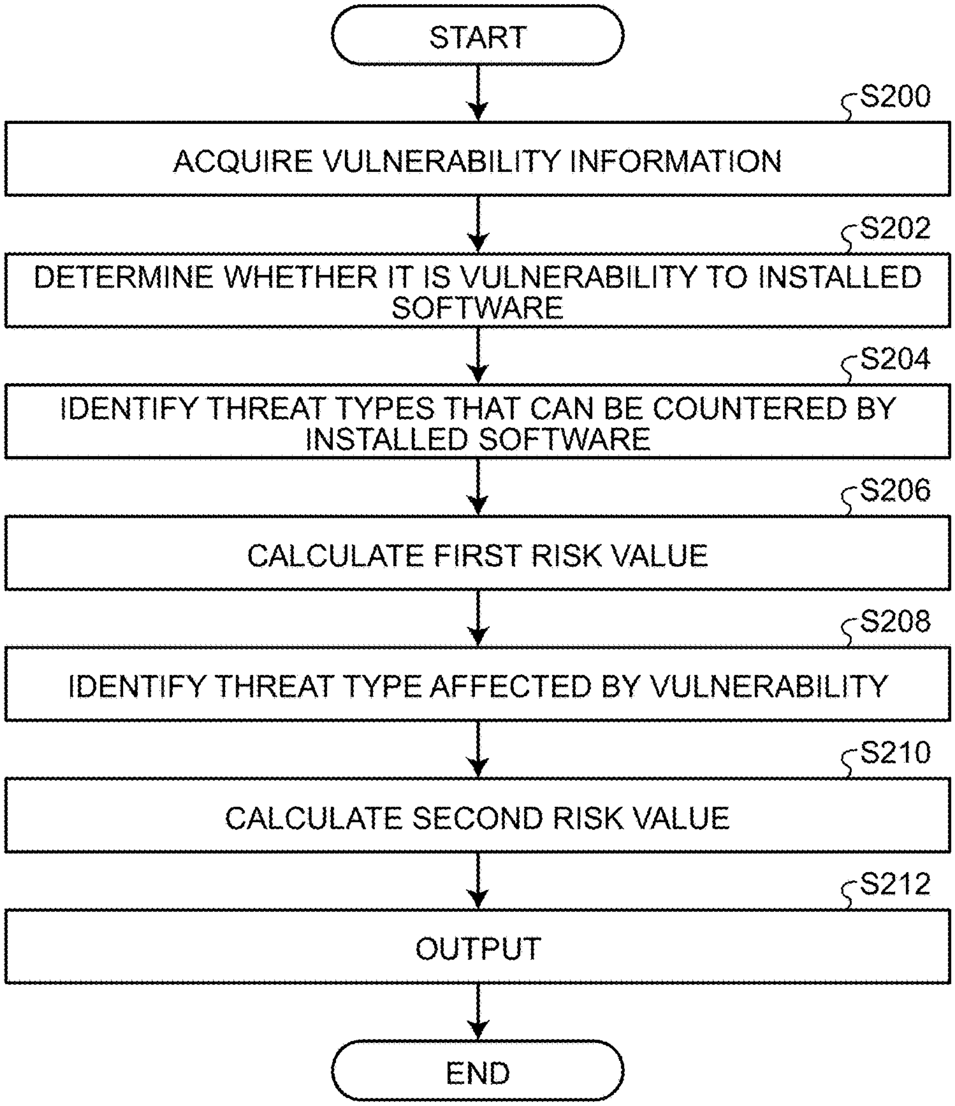
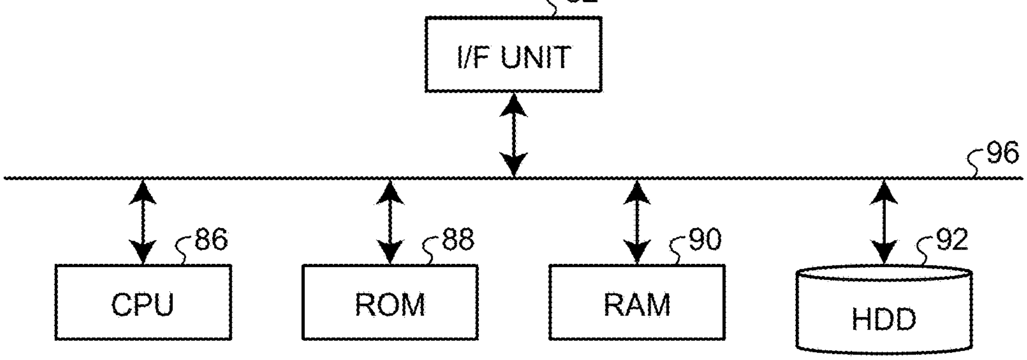

START
S200
ACQUIRE VULNERABILITY INFORMATION
S202
DETERMINE WHETHER IT IS VULNERABILITY TO INSTALLED SOFTWARE
S204
IDENTIFY THREAT TYPES THAT CAN BE COUNTERED BY INSTALLED SOFTWARE
S206
CALCULATE FIRST RISK VALUE
S208
IDENTIFY THREAT TYPE AFFECTED BY VULNERABILITY
S210
CALCULATE SECOND RISK VALUE
S212
OUTPUT
END

FIG.11


82
I/F UNIT
96
86
CPU
88
ROM
90
RAM
92
HDD

INFORMATION PROCESSING SYSTEM, INFORMATION PROCESSING METHOD, AND COMPUTER PROGRAM PRODUCT

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is based upon and claims the benefit of priority from Japanese Patent Application No. 2024-022603, filed on Feb. 19, 2024; the entire contents of which are incorporated herein by reference.

FIELD

[0002] Embodiments described herein relate generally to an information processing system, an information processing method, and a computer program product.

BACKGROUND

[0003] Numerous new software vulnerabilities have been reported, and systems are known to diagnose vulnerability risks to software on the basis of vulnerability information published by vendors and the like.

[0004] Vulnerabilities in security countermeasure software affect not only the software itself, but also a target system countered by the security countermeasure software. However, in the related art, even when vulnerabilities are found in security countermeasure software, evaluating the risk of the target system countered by the software has been difficult. That is, in the related art, evaluating the risk to the target system due to vulnerabilities in the security countermeasure software has been difficult.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] FIG. **1** is a schematic diagram of an information processing system of an embodiment;

[0006] FIG. **2** is a block diagram of the functional configuration of an information processing device;

[0007] FIG. **3** is a schematic diagram of a data structure of correspondence information;

[0008] FIG. **4** is a schematic diagram of a data structure of risk analysis result information;

[0009] FIG. **5** is a schematic of a display screen;

[0010] FIG. **6** is an explanatory diagram of countermeasure levels;

[0011] FIG. **7** is a flowchart of an information processing flow;

[0012] FIG. **8** is a block diagram of a functional configuration of the information processing device;

[0013] FIG. **9** is a schematic diagram of a data structure of impact information;

[0014] FIG. **10** is a flowchart of an information processing flow; and

[0015] FIG. **11** is a hardware configuration diagram.

DETAILED DESCRIPTION

[0016] According to an embodiment, an information processing system includes one or more hardware processors. The one or more hardware processors are configured to: identify a threat type capable of being countered by installed software being security countermeasure software installed in a target system, from among security countermeasure software with a reported vulnerability; calculate a first risk value when a countermeasure is taken by the installed software for a threat of the identified threat type; calculate a second risk value when no countermeasure is taken by the installed software for the threat of the identified threat type; and output damage potential information including risk value change information representing a change in the second risk value with respect to the first risk value.

[0017] Exemplary embodiments of an information processing system, an information processing method, and an information processing program will be explained in detail below with reference to the accompanying drawings.

First Embodiment

[0018] FIG. **1** is a schematic diagram illustrating an example of an information processing system **1** of the present embodiment.

[0019] The information processing system **1** includes an information processing device **10** and one or more external devices **20**. The information processing device **10** and the external device **20** are communicatively connected via a network NW or the like.

[0020] The information processing system **1** is a system for evaluating risks due to vulnerabilities in a target system **30**.

[0021] The target system **30** is a system for which the risk due to the vulnerability is evaluated. The target system **30** includes one or more computers. One or more pieces of security countermeasure software have been introduced in the target system **30**. The target system **30** may also have one or more pieces of security countermeasure software scheduled to be introduced. The introduction implies installation. The present embodiment explains an example in which one or more pieces of security countermeasure software have been installed in the target system **30**.

[0022] The external device **20** is a dedicated or general-purpose computer. The external device **20** is a device that provides vulnerability information to the information processing device **10** or the like, and receives damage potential information of the target system **30** from the information processing device **10**. The damage potential information will be explained below.

[0023] The vulnerability information is information representing vulnerabilities published by vendors being manufacturers or suppliers of software and hardware. The vulnerability information includes publicly available information on vulnerabilities published by the vendors. In the present embodiment, the vulnerability information includes at least information on vulnerabilities included in security countermeasure software.

[0024] Specifically, for example, the vulnerability information includes one or more of the following item information: evaluation criteria including conformance conditions for the vulnerability and risk values for each of the conformance conditions; the range of possible impacts of the vulnerability on a system device; and countermeasures to address the vulnerability. The conformance condition represents the risk value for the version of software such as security countermeasure software in the form of (conformance condition/risk value), for example, (Software_A10.1 or earlier/4.5 (high)). That is, the conformance condition includes information on the security countermeasure software with a reported vulnerability. The range of possible impacts is expressed, for example, as “arbitrary code execution” or “possibility of information leakage or tampering”. That is, the range of possible impacts includes the threat type of a threat. The range of possible impacts may also include an information security element representing at least one of confidentiality, integrity, and availability affected by the threat of the threat type. The countermeasure is expressed, for example, as "apply patch_001" or "change settings_001 to 100".

[0025] Whenever new vulnerability information is published by a vendor or the like, the external device **20** transmits the vulnerability information to the information processing device **10**. For example, the external device **20** acquires new vulnerability information from vulnerability databases such as common vulnerabilities and exposures (CVE), national vulnerability database (NVD), Japan vulnerability notes (JVN) iPedia, or the like, and transmits the acquired vulnerability information to the information processing device **10**. The information processing device **10** may directly acquire the vulnerability information from these vulnerability databases.

[0026] The information processing device **10** is an information processing device for evaluating a risk to the target system **30** due to vulnerabilities in security countermeasure software on the basis of the vulnerability information. The information processing device **10** is a dedicated or general-purpose computer.

[0027] FIG. **2** is a block diagram illustrating an example of the functional configuration of the information processing device **10**.

[0028] The information processing device **10** includes a communication unit **12**, a user interface (UI) unit **14**, a storage unit **16**, and a processing unit **18**. The communication unit **12**, the UI unit **14**, the storage unit **16**, and the processing unit **18** are connected via a bus or the like to be able to exchange data or signals.

[0029] At least one of the UI unit **14** and the storage unit **16** may be communicatively connected to the processing unit **18** via the network NW. That is, at least one of the UI unit **14** and the storage unit **16** may be provided in an external information processing device connected to the information processing device **10** via the network NW. In addition, at least one of the functional units to be explained below, which are included in the processing unit **18**, may be provided in the external information processing device. The external information processing device is, for example, an external server, the external device **20**, or the like.

[0030] The communication unit **12** communicates with the external information processing device such as the external device **20** via the network NW. The UI unit **14** has a function of receiving operation input from a user and a function of outputting various types of information. For example, the UI unit **14** includes a display and an input unit. The display displays various types of information. The display is, for example, a known electro-luminescence (EL) display, a liquid crystal display (LCD), a projection device, or the like. The input unit receives various instructions from the user. The input unit is, for example, a keyboard, a mouse, a touch panel, a microphone, or the like. The UI unit **14** may be configured as a touch panel with an input mechanism and an output mechanism. The UI unit **14** may further include a speaker that outputs audio.

[0031] The storage unit **16** stores various types of data. The storage unit **16** is, for example, a semiconductor memory element such as a random access memory (RAM) and a flash memory, a hard disk, an optical disk, or the like. The storage unit **16** may be a storage device provided outside the information processing device **10**. The storage unit **16** may be a storage medium. Specifically, the storage medium may be one in which computer programs and various information are downloaded and stored or temporarily stored via a local area network (LAN), the Internet, or the like. The storage unit **16** may include a plurality of storage media.

[0032] In the present embodiment, the storage unit **16** stores correspondence information **16**A and risk analysis result information **16**B. The storage unit **16** stores the correspondence information **16**A in advance. The correspondence information **16**A may be in a form that is updated by the processing unit **18** to be explained below. The risk analysis result information **16**B may be stored in the storage unit **16** in advance, or may be generated and updated by the processing unit **18** to be explained below, or the like. Details of the correspondence information **16**A and the risk analysis result information **16**B will be explained below.

[0033] The processing unit **18** includes a vulnerability determination unit **18**A, a first identifying unit **18**B, a first calculation unit **18**C, a second calculation unit **18**D, an output unit **18**E, and an update unit **18**F.

[0034] At least one of the vulnerability determination unit **18**A, the first identifying unit **18**B, the first calculation unit **18**C, the second calculation unit **18**D, the output unit **18**E, and the update unit **18**F is implemented by one or more processors, for example. For example, each of the above units may be implemented by causing a processor such as a central processing unit (CPU) to execute a computer program, that is, by software. Each of the above units may also be implemented by a processor such as a dedicated integrated circuit (IC), that is, by hardware. Each of the above units may be implemented using a combination of software and hardware. When a plurality of processors are used, each processor may implement one of the units or two or more of the units.

[0035] As explained above, at least one of these functional units included in the processing unit **18** may be provided in an information processing device outside the information processing device **10**. The processing unit **18** may be configured without at least one of the vulnerability determination unit **18**A and the update unit **18**F.

[0036] The vulnerability determination unit **18**A determines whether a vulnerability represented by newly reported vulnerability information is a vulnerability to installed software being the security countermeasure software installed in the target system **30**.

[0037] The vulnerability determination unit **18**A acquires vulnerability information by receiving new vulnerability information from the information processing device **10**. The vulnerability determination unit **18**A may acquire vulnerability information from vulnerability databases such as CVE, NVD, and JVN iPedia.

[0038] Subsequently, the vulnerability determination unit **18**A determines whether the vulnerability indicated in the acquired new vulnerability information is a vulnerability to the security countermeasure software installed in the target system **30**. For example, the vulnerability determination unit **18**A reads list information of security countermeasure software that has been or is scheduled to be installed in the target system **30** from the storage unit **16** or the like. Subsequently, the vulnerability determination unit **18**A determines whether the vulnerability indicated in the vulnerability information is a vulnerability to the security countermeasure software that has been or is scheduled to be installed in the target system **30** by using, for example, a common platform enumeration (CPE) listed in the Known Affected Software Configurations column of NVD.

[0039] The vulnerability determination unit **18**A outputs, to the first identifying unit **18**B, information representing the security countermeasure software installed in the target system **30** and having a reported vulnerability, the vulnerability being determined on the basis of the new vulnerability information. That is, the vulnerability determination unit **18**A selects information on the security countermeasure software installed in the target system **30** from many reports of vulnerability information, and outputs the selected information to the first identifying unit **18**B.

[0040] The first identifying unit **18**B identifies a threat type that can be countered by the installed software being the security countermeasure software installed in the target system **30**, out of the security countermeasure software with a reported vulnerability.

[0041] First, the first identifying unit **18**B identifies the installed software, which is the security countermeasure software installed in the target system **30**, out of the security countermeasure software with a reported vulnerability.

[0042] For example, the first identifying unit **18**B receives, from the vulnerability determination unit **18**A, the vulnerability information and information on the installed software installed in the target system **30** and having a vulnerability. The information on the installed software is, for example, identification information of installed software being security countermeasure software that has been installed or is scheduled to be installed in the target system **30**. In this case, the first identifying unit **18**B reads the information on the installed software received from the vulnerability determination unit **18**A to identify the installed software determined by the vulnerability determination unit **18**A to be vulnerable to the installed software in the target system **30**.

[0043] The processing unit **18** may be configured without the vulnerability determination unit **18**A. In this case, the first identifying unit **18**B may identify the installed software in the target system **30** and having a vulnerability by performing the determination process in the same manner as the vulnerability determination unit **18**A by means of the new vulnerability information acquired from the external device **20**, an external vulnerability database, or the like. That is, in this case, the first identifying unit **18**B may identify the installed software in the target system **30** and having a vulnerability from the known affected software configurations column of CVE or NVD, JVN iPedia, or the like.

[0044] The first identifying unit **18**B may also identify, as installed software, security countermeasure software that is registered in the correspondence information **16**A to be explained below, out of the security countermeasure software having a vulnerability indicated in the acquired vulnerability information.

[0045] Subsequently, the first identifying unit **18**B identifies a threat type that can be countered by the installed software in the target system **30** and having a reported vulnerability. The first identifying unit **18**B identifies the threat type by using the correspondence information **16**A.

[0046] FIG. **3** is a schematic diagram of an example of the data structure of the correspondence information **16**A. In the present embodiment, the following explanation is given on the assumption that the correspondence information **16**A for each target system **30** is stored in the storage unit **16** in advance.

[0047] The correspondence information **16**A is a database in which the identification information of the security countermeasure software installed in the target system **30** is associated with the threat types of threats that can be countered by the security countermeasure software identified by the identification information. In the correspondence information **16**A, identification information of security countermeasure software scheduled to be installed in the target system **30** may be further registered. That is, in the correspondence information **16**A, the threat type of a threat to be defended in the target system **30** and the identification information of the security countermeasure software that has been installed or is scheduled to be installed in order to counter the threat of the threat type are registered in association with each other. The data format of the correspondence information **16**A is not limited to a database.

[0048] The correspondence information **16**A may be stored in the storage unit **16** in advance. The correspondence information **16**A may be generated by a user's operating instruction on the UI unit **14**, or may be generated in advance by the processing unit **18**, the external device **20**, or the like, and stored in the storage unit **16** in advance. The threat types of threats that can be countered by the security countermeasure software identified by the identification information registered in the correspondence information **16**A may be set arbitrarily by the user, or may be set in the correspondence information **16**A in any way by the processing unit **18**, the external device **20**, or the like. For example, the processing unit **18** and the external device **20** may register threat types in the correspondence information **16**A by acquiring information from any edition of the Security Risk Analysis Guide for Control Systems published by the Information-technology Promotion Agency (IPA). Specifically, for example, as the threats (attack methods) in the Security Risk Analysis Guide for Control Systems, Second Edition: unauthorized access, physical intrusion, unauthorized operation, negligent operation, connection of unauthorized media or device, illegal execution of processes, malware infection, information theft, information tampering, information destruction, illegal transmission, functional stop, high-load attacks, theft, and information theft by disassembly at the time of theft or disposal, a threat type of a threat that can be countered by the security countermeasure software installed in the target system **30** may be registered in the correspondence information **16**A by being selected from these threat types by the user or the processing unit **18**.

[0049] One or more threat types may be registered in the correspondence information **16**A for one security countermeasure software. For example, as illustrated in FIG. **3**, software B being the security countermeasure software may be able to counter threats of both threat types of unauthorized access and information tampering.

[0050] As illustrated in FIG. **3**, a plurality of types of security countermeasure software may have been installed or be scheduled to be installed in one target system **30**.

[0051] The first identifying unit **18**B reads the threat type associated with the identification information of the installed software, which is the security countermeasure software installed in the target system **30** out of the security countermeasure software with vulnerabilities indicated in the vulnerability information, from the correspondence information **16**A. Through this reading process, the first identifying unit **18**B identifies the threat types of threats that can be countered by the installed software.

[0052] Return to FIG. **2** to continue the explanation.

[0053] The first calculation unit **18**C calculates a first risk value, which is a risk value for the threats of the threat types identified by the first identifying unit **18**B, when countermeasures have been taken by the installed software. The case where countermeasures have been taken by the installed software means a case where countermeasures against the threats of the threat types identified by the first identifying unit **18**B are considered to have been taken by the installed software with a reported vulnerability.

[0054] For example, the first calculation unit **18**C calculates the first risk value on the basis of the risk analysis result information **16**B.

[0055] FIG. **4** is a schematic diagram of an example of the data structure of the risk analysis result information **16**B.

[0056] The risk analysis result information **16**B is information representing the result of risk analysis comparing the risk values before and after countermeasures against the threats of the threat types identified by the first identifying unit **18**B, when countermeasures have been taken by the installed software.

[0057] For the risk analysis, any analysis method having a property that the risk values before and after the countermeasure by the installed software can be compared may be used. Specific examples of the risk analysis include analysis methods in accordance with the "Security Risk Analysis Guide for Control Systems" published by the IPA. The risk analysis result information **16**B illustrated in FIG. **4** shows an example of the result of risk analysis according to the above guide published by the IPA.

[0058] For example, in the "Security Risk Analysis Guide for Control Systems" published by the IPA, a risk analysis procedure includes the following steps: Step 1: List the assets on the system; Step 2: Examine the importance of the assets and the threat level for each threat; Step 3: Examine the countermeasure implementation status and the countermeasure level (vulnerability level); and Step 4: Mechanically calculate the risk value for each threat based on the importance of the assets, the threat level, and the countermeasure level.

[0059] Therefore, for example, in the risk analysis, the device names of devices included in the target system **30** are listed in the columns of target devices, and the threat level and vulnerability level for each importance and threat type of the listed devices are registered in the risk analysis result information **16**B. Subsequently, by registering the presence or absence of countermeasures for each device and threat type (mark "O" in FIG. **4** indicates that countermeasures are present), the number of countermeasures taken and the countermeasure level corresponding to the threat level are registered in the risk analysis result information **16**B for each device and threat type. The higher the value of the countermeasure level, the more countermeasures are taken. The higher the value of the countermeasure level, the lower the vulnerability level is registered in the risk analysis result information **16**B. Subsequently, based on the registered threat level, vulnerability level, and importance of assets, risk values are mechanically determined for each device and threat type and registered in the risk analysis result information **16**B.

[0060] The risk value determined for each threat type by the risk analysis may be expressed as an alphabet or a numerical value. When the risk value is expressed as an alphabet, the closer the risk value is to A, the higher the risk is, and the closer the risk value is to Z, the lower the risk is. Specifically, for example, the risk value may be expressed on a five-step rating from A to E, with A being the highest risk. On the other hand, when the risk value is expressed as a numerical value, the higher the risk value is, the higher the risk is, and the lower the risk value is, the lower the risk is. Specifically, for example, the risk value may be expressed on a five-step rating from **5** to **1**, with **5** being the highest risk. In the present embodiment, the following explanation is given on the assumption that a risk value expressed on a five-step rating from A to E, with A being the highest risk, is registered for each threat type in the risk analysis result information **16**B.

[0061] When the risk analysis result information **16**B is stored in advance in the storage unit **16**, the first calculation unit **18**C calculates the first risk value by using the risk analysis result information **16**B.

[0062] For example, it is assumed that the above risk analysis is performed in advance by an external device such as the processing unit **18** or the external device **20** and that the risk analysis result information **16**B representing the result of the risk analysis is stored in the storage unit **16** in advance.

[0063] In this case, the first calculation unit **18**C calculates the first risk value by using the risk analysis result information **16**B. For example, the first calculation unit **18**C acquires, from the risk analysis result information **16**B, the risk values in the risk analysis result information **16**B associated with the threat types of threats that can be countered by the installed software, the threat types being identified by the first identifying unit **18**B. Through this acquisition process, the first calculation unit **18**C calculates the read risk value as the first risk value for the threat of the threat type when the countermeasures have been taken by the installed software. In the present embodiment, the following explanation is continuously given on the assumption that the first calculation unit **18**C calculates any of the risk values from A to E, which are expressed by a five-step rating of the alphabet, as the first risk value.

[0064] Return to FIG. **2** to continue the explanation.

[0065] The second calculation unit **18**D calculates a second risk value for the threat type identified by the first identifying unit **18**B, which represents the risk value for the threat when no countermeasures have been taken by the installed software. The case where no countermeasures have been taken by the installed software means a case where no countermeasures against the threats of the threat types identified by the first identifying unit **18**B are considered to have been taken by the installed software with a reported vulnerability.

[0066] The second calculation unit **18**D calculates the second risk value by using the same analysis method as the first calculation unit **18**C. Therefore, when the first calculation unit **18**C calculates the first risk value on the basis of the risk analysis result information **16**B, the second calculation unit **18**D calculates the second risk value by using the risk analysis method used to generate the risk analysis result information **16**B.

[0067] For example, it is assumed that the risk analysis result information **16**B used by the first calculation unit **18**C to calculate the first risk value is based on an analysis method in accordance with the "Security Risk Analysis Guide for Control Systems" published by the IPA. In this case, the second calculation unit **18**D calculates the second risk value, which is the risk value for the threat of the threat type identified by the first identifying unit **18**B, in accordance with the "Security Risk Analysis Guide for Control Systems" when no countermeasures have been taken by the installed software.

[0068] In the process of risk analysis, the second calculation unit **18**D uses information regarding whether the security countermeasure software against the threat has been installed. However, even though the security countermeasure software has actually been installed in the target system **30**, the risk analysis is performed assuming that the security countermeasure software has not been installed in the target system **30**. This allows the second calculation unit **18**D to calculate the second risk value being the risk value for the threat of the threat type identified by the first identifying unit **18**B, for which no countermeasure has been taken by the installed software.

[0069] For example, in the "Security Risk Analysis Guide for Control Systems" published by the IPA, the risk analysis procedure is to mechanically calculate the risk value for each threat by performing the above steps 1 to 4 in order. Therefore, the second calculation unit **18**D can calculate the second risk value, which is the risk value when no countermeasures are taken against threats, by performing a risk analysis by assuming that a countermeasure implementation status by the security countermeasure software with a reported vulnerability is not present in Step 3: Examine the countermeasure implementation status and the countermeasure level (vulnerability level).

[0070] When the risk analysis was performed in the past by the first calculation unit **18**C, the second calculation unit **18**D, or the like, the second calculation unit **18**D may perform the risk analysis from the first step 1 of the risk analysis procedure including steps 1 to 4, or from a necessary part in the middle of step 2 or later. For example, it is assumed that the risk analysis is performed in accordance with the "Security Risk Analysis Guide for Control Systems" published by the IPA and the risk analysis result information **16**B has already been generated by the processing unit **18** or the like. In this case, the second calculation unit **18**D may skip the steps 1 and 2 of the risk analysis procedure including the steps 1 to 4 and perform the risk analysis starting from the step 3. This can reduce the processing time required for the second calculation unit **18**D to perform the risk analysis and calculate the second risk value.

[0071] In the present embodiment, the following explanation is continuously given on the assumption that the second calculation unit **18**D calculates, as the second risk value, any of the risk values from A to E, expressed as a five-step rating in the alphabet, like the first calculation unit **18**C.

[0072] The risk analysis result information **16**B may not be stored in advance in the storage unit **16**.

[0073] In such a case, the first calculation unit **18**C may calculate the first risk value by performing the risk analysis explained above. In detail, the first calculation unit **18**C may calculate the first risk value by a risk analysis using any analysis method having a property that the risk values before and after the countermeasures by the installed software can be compared. Specifically, for example, the first calculation unit **18**C may calculate the first risk value by using the analysis method explained above in accordance with the "Security Risk Analysis Guide for Control Systems" published by the IPA.

[0074] The first calculation unit **18**C may also generate the risk analysis result information **16**B by the above risk analysis and store the generated risk analysis result information **16**B in the storage unit **16**. Subsequently, for the next and subsequent calculations of the first risk value, the first calculation unit **18**C may calculate the first risk value in the same process as explained above by using the risk analysis result information **16**B stored in the storage unit **16**.

[0075] In this case, the second calculation unit **18**D may calculate the second risk value by using the same analysis method as the first calculation unit **18**C. For example, it is assumed that the first calculation unit **18**C calculates the first risk value by risk analysis using the analysis method in accordance with the "Security Risk Analysis Guide for Control Systems" published by the IPA. In this case, the second calculation unit **18**D may calculate the second risk value in the same manner as above by a risk analysis using an analysis method in accordance with the "Security Risk Analysis Guide for Control Systems" published by the IPA.

[0076] In the processing unit **18**, when the risk analysis result information **16**B is not stored in the storage unit **16**, the first calculation unit **18**C and the second calculation unit **18**D may calculate the first risk value and the second risk value, respectively, in the same manner as above by using the same risk analysis method when a vulnerability is reported for the first time. Subsequently, when calculating risk values based on the acquisition of vulnerability information for the second and subsequent times, the first calculation unit **18**C and the second calculation unit **18**D may calculate the first risk value and the second risk value, respectively, by the above method by using the risk analysis result information **16**B generated by the initial risk analysis.

[0077] The second calculation unit **18**D may also update the risk analysis result information **16**B stored in the storage unit **16**, by using the analysis result of the risk analysis performed when calculating the second risk value.

[0078] For example, it is assumed that the second calculation unit **18**D calculates the second risk value by risk analysis using an analysis method in accordance with the "Security Risk Analysis Guide for Control Systems" published by the IPA. In this case, the second calculation unit **18**D may reflect, in the risk analysis result information **16**B, information representing a change in the risk value when no countermeasures have been taken by the installed software. Specifically, for example, it is assumed that the second calculation unit **18**D calculates the second risk value on the basis of certain vulnerability information, which considers no countermeasures against threats of any threat type by software A being the installed software in the target system **30**. In this case, the second calculation unit **18**D may perform a process of setting the countermeasures corresponding to the threat type of the threat in the risk analysis result information **16**B to none (that is, remove "O" from the countermeasure column), and register a newly calculated value in a corresponding countermeasure level. Subsequently, the second calculation unit **18**D may calculate the second risk value by using the newly calculated value of the countermeasure level.

[0079] Subsequently, when the second risk value is calculated next time or later, that is, when the second risk value based on new vulnerability information is calculated, the second calculation unit **18**D may calculate the second risk value by using the previously updated risk analysis result information **16**B. That is, the second calculation unit **18**D may calculate the second risk value based on the analysis result of the previous risk analysis.

[0080] Specifically, for example, it is assumed that by reflecting the analysis result from the previous calculation of the second risk value, the countermeasures corresponding to the threat type of the threat that can be countered by the software A being the installed software in the target system **30** is set to none in the risk analysis result information **16**B (that is, remove "O" from the countermeasure column), and the newly calculated value of the countermeasure level is registered as the corresponding countermeasure level. Subsequently, it is assumed that the second calculation unit **18**D calculates the second risk value by using the value of the countermeasure level. In this case, when the second risk value is next calculated, the second calculation unit **18**D may newly calculate a second risk value based on the analysis result reflected in the previous analysis, that is, the analysis result of the previous risk analysis in which it was deemed that no countermeasures against the threat have been taken by the software A.

[0081] More specifically, for example, it is assumed that the installed software in the target system **30** is software G, software H, and software I. In addition, it is assumed that these installed software are able to counter unauthorized access.

[0082] It is assumed that the software G, the software H, and the software I are used as countermeasures (three marks "O" are registered) for "one-way gateway", "WAF", and "authentication of communication partners", respectively, in response to the threat type "unauthorized access" in the risk analysis result information **16**B.

[0083] Subsequently, it is assumed that vulnerable installed software represented by vulnerability information acquired for the first time is the software G. In this case, when the second risk value is calculated based on the vulnerability information acquired for the first time, for example, the second calculation unit **18**D performs a risk analysis as no countermeasures by the "one-way gateway" using the software G. In this case, since "O" indicating the presence of countermeasures registered in the "one-way gateway" by the software G is removed, the number of "O"s indicating the presence of countermeasures against "unauthorized access" is 2. Therefore, the second calculation unit **18**D calculates, for example, a risk value "C" as the second risk value from a countermeasure level corresponding to the number of countermeasures.

[0084] Subsequently, it is assumed that the vulnerable installed software represented by the vulnerability information acquired for the second time is the software H. In this case, when the second risk value is calculated based on the vulnerability information acquired for the second time, for example, the second calculation unit **18**D performs a risk analysis as no countermeasure by the "WAF" using the software H. In this case, since "O" indicating the presence of countermeasures registered in the "WAF" by the software H is further removed, the number of "O"s indicating the presence of countermeasures against "unauthorized access" is 0. Therefore, the second calculation unit **18**D calculates a risk value "B", which is increased from the risk value "C", as the second risk value from a countermeasure level corresponding to the number of countermeasures.

[0085] On the other hand, when the second calculation unit **18**D calculates the second risk value in the same manner without using the previously updated risk analysis result information **16**B, the second risk value calculated on the basis of the vulnerability information acquired for the second time above is the risk value "C" with no change from the first time.

[0086] Therefore, in this way, when the second risk value is calculated next time or later, that is, when the second risk value based on new vulnerability information is calculated, the second calculation unit **18**D can calculate the second risk value by using the previously updated risk analysis result information **16**B, thereby calculating the second risk value based on the analysis result of the previous risk analysis.

[0087] The first calculation unit **18**C may calculate the first risk value in the same manner as above by using the risk analysis result information **16**B updated by the second calculation unit **18**D.

[0088] Therefore, in this case, the second calculation unit **18**D updates the risk analysis result information **16**B by using the analysis result of the risk analysis, so that when risk values (the first risk value and the second risk value) are calculated the next time or later, the first calculation unit **18**C and the second calculation unit **18**D can calculate the risk values based on the analysis result of the previous risk analysis.

[0089] The output unit **18**E will be explained below.

[0090] The output unit **18**E outputs the damage potential information.

[0091] The damage potential information is information representing a potential damage to the target system **30** caused by the vulnerability of the installed software.

[0092] The damage potential information includes at least risk value change information. The risk value change information represents a change in the second risk value with respect to the first risk value. That is, the risk value change information is information representing a change in risk value from the presence of countermeasures against the threats of the threat types that can be countered by the installed software to the absence of the countermeasures against the threats. For example, it is assumed that the first risk value calculated by the first calculation unit **18**C is "B" and the second risk value calculated by the second calculation unit **18**D is "A". In this case, the output unit **18**E outputs damage potential information including information representing a change from the first risk value "B" to the second risk value "A" as the risk value change information.

[0093] The damage potential information may further include threat types of threats having damage potential according to the risk value change information. That is, the output unit **18**E may output damage potential information including the risk value change information on the threat type of the threat that can be countered by the installed software and the threat type.

[0094] The damage potential information may further include information on the presence or absence of damage potential. The information on the presence or absence of damage potential is information representing the presence of damage potential or absence of damage potential. The output unit **18**E may generate and output information on the presence or absence of damage potential that represents the presence of damage potential when the change in risk value represented by the risk value change information represents an increase in risk and represents the absence of damage potential when the change represents no change or a decrease in risk. For example, it is assumed that the change in risk value represented by the risk value change information is a change representing an increase in risk from the first risk value "B" to the second risk value "A". In this case, the output unit **18**E may generate information on the presence or absence of damage potential that represents the presence of damage potential, and output damage potential information further including the information on the presence or absence of damage potential.

[0095] The output unit **18**E outputs the damage potential information to at least one of the storage unit **16**, the UI unit **14**, and an external device such as the external device **20**. That is, outputting the damage potential represents at least one of storage in the storage unit **16**, display on the UI unit **14**, and transmission to the external device.

[0096] For example, the output unit **18**E stores the damage potential information in the storage unit **16**. The output unit **18**E stores the damage potential information in the storage unit **16**, which enables the analysis result to be stored and used for a trend analysis and other data applications.

[0097] The output unit **18**E also transmits the damage potential information to an external information processing device such as an external device via the communication unit **12**. The output unit **18**E transmits the damage potential information to the external information processing device, so that the information processing device receiving the damage potential information can use the information for a trend analysis and other data applications.

[0098] The output unit **18**E also displays the damage potential information on the UI unit **14**.

[0099] FIG. **5** is a schematic diagram of an example of a display screen **40** displayed in the UI unit **14**.

[0100] For example, the output unit **18**E displays the display screen **40** representing the damage potential information on the UI unit **14**. As illustrated in FIG. **5**, for example, the display screen **40** including damage potential information including the threat type, the risk value change information, the information on the presence or absence of damage potential, and the like is displayed on the UI unit **14**. The output unit **18**E may output the damage potential information further including the date and time when the comparison between the first and second risk values was conducted, the CVE number, and the software name of the installed software.

[0101] By outputting the damage potential information, the output unit **18**E can enable to easily identify whether the security risk of the target system **30** changes due to the vulnerability of the installed software with a reported vulnerability and what kind of damage (threat) the target system **30** may be subjected to.

[0102] The output unit **18**E may output the damage potential information further including at least one of the following: the risk value change information, the countermeasure level calculated from the vulnerability level, and information representing whether the security risk for the threat has changed.

[0103] In detail, the output unit **18**E assumes a risk analysis using an analysis method in accordance with the "Security Risk Analysis Guide for Control Systems" published by the IPA, and determines whether the security risk of the target system **30** changes due to a change in the countermeasure level and what kind of damage (threat) may occur.

[0104] The countermeasure level is information calculated from the risk value and the vulnerability level, and is represented, for example, by a matrix illustrated in FIG. **6**. FIG. **6** is an explanatory diagram illustrating an example of a countermeasure level.

[0105] The output unit **18**E compares a first countermeasure level calculated from the first risk value and the vulnerability level calculated by the first calculation unit **18**C with a second countermeasure level calculated from the second risk value and the vulnerability level calculated by the second calculation unit **18**D. The first countermeasure level and the second countermeasure level are examples of countermeasure levels.

[0106] Subsequently, when a change from the first countermeasure level calculated from the first risk value, which is the case with countermeasures, to the second countermeasure level calculated from the second risk value, which is the case without countermeasures, represents a change to a higher risk countermeasure level, the output unit **18**E determines that the security risk for the threat has changed. Specifically, when the change from the first countermeasure level to the second countermeasure level is from a lower risk "countermeasure level is at upper limit" to a higher risk "countermeasure consideration required" or from a lower risk "low risk value" to a higher risk "countermeasure consideration required", the output unit **18**E determines that the security risk for the threat has changed. Subsequently, the output unit **18**E outputs the damage potential information further including at least one of the countermeasure level and information representing whether the security risk for the threat has changed. In this case, the output unit **18**E can further provide the comparison result of security risk changes considering a countermeasure priority determined from the countermeasure level.

[0107] The output unit **18**E may further output a threat type to be output by referring to information in the Description column on the NVD vulnerability information page or the assumed impact column on the JVN iPedia vulnerability information page. This process allows the output unit **18**E to output more detailed information for threat types.

[0108] Return to FIG. **2** to continue the explanation.

[0109] The update unit **18**F updates the correspondence information **16**A. In detail, the update unit **18**F updates the correspondence information **16**A to be information representing the latest state of the target system **30**. The update unit **18**F may update the correspondence information **16**A in response to user's instructions to operate the UI unit **14** in at least one of the following cases: when new security countermeasure software is installed in the target system **30**, when new security countermeasure software is scheduled to be installed in the target system **30**, when the security countermeasure software installed in the target system **30** is uninstalled, and when a change occurs in the threat type of a threat that can be countered by the security countermeasure software.

[0110] The update unit **18**F updates the correspondence information **16**A to be information representing the latest state of the target system **30**. The processing unit **18** may be configured without the update unit **18**F.

[0111] An example of an information processing flow to be performed by the information processing device **10** of the present embodiment will be explained.

[0112] FIG. **7** is a flowchart illustrating an example of an information processing flow to be performed by the information processing device **10** of the present embodiment.

[0113] The vulnerability determination unit **18**A acquires newly reported vulnerability information (step S**100**). Subsequently, the vulnerability determination unit **18**A determines whether a vulnerability represented by the vulnerability information acquired at step S**100** is a vulnerability to the installed software being the security countermeasure software installed in the target system **30** (step S**102**). The vulnerability determination unit **18**A outputs, to the first identifying unit **18**B, information representing the security countermeasure software installed in the target system **30** and having a reported vulnerability, the vulnerability being determined on the basis of the new vulnerability information.

[0114] The first identifying unit **18**B identifies threat types that can be countered by the installed software, which is the security countermeasure software installed in the target system **30**, out of the security countermeasure software with a reported vulnerability (step S**104**). For example, the first identifying unit **18**B receives, from the vulnerability determination unit **18**A, the vulnerability information and information on the installed software installed in the target system **30** and having a vulnerability. The first identifying unit **18**B reads the information on the installed software received from the vulnerability determination unit **18**A to identify the installed software determined by the vulnerability determination unit **18**A to be vulnerable to the installed software in the target system **30**. Subsequently, the first identifying unit **18**B identifies the threat types that can be countered by the identified installed software with a reported vulnerability.

[0115] The first calculation unit **18**C calculates the first risk value, which is a risk value for the threat of the threat type identified at step S**104**, when countermeasures have been taken by the installed software (step S**106**). For example, the first calculation unit **18**C calculates the first risk value on the basis of the threat type identified at step S**104** and the risk analysis result information **16**B.

[0116] The second calculation unit **18**D calculates the second risk value, which is a risk value for the threat of the threat type identified at step S**104** when no countermeasures have been taken by the installed software (step S**108**). The second calculation unit **18**D calculates the second risk value by using the same analysis method as the analysis method performed at step S**106** by the second calculation unit **19**C.

[0117] The output unit **18**E outputs the damage potential information including at least the risk value change information representing a change in the second risk value calculated at step S**108** with respect to the first risk value calculated at step S**106** (step S**110**). Subsequently, the routine is terminated.

[0118] As explained above, the information processing system **1** of the present embodiment includes the first identifying unit **18**B, the first calculation unit **18**C, the second calculation unit **18**D, and the output unit **18**E. The first identifying unit **18**B identifies the threat types that can be countered by the installed software, which is the security countermeasure software installed in the target system **30**, out of the security countermeasure software with a reported vulnerability. The first calculation unit **18**C calculates the first risk value for the threat of the identified threat type when countermeasures have been taken by the installed software. The second calculation unit **18**D calculates the second risk value for the threat of the identified threat type when no countermeasures have been taken by the installed software. The output unit **18**E outputs damage potential information including risk value change information representing a change in the second risk value with respect to the first risk value.

[0119] Here, vulnerabilities in security countermeasure software affect not only the software itself, but also the target system **30** countered by the security countermeasure software. However, in the related art, even when vulnerabilities are found in security countermeasure software, evaluating the risk of the target system **30** countered by the software has been difficult. That is, in the related art, evaluating the risk to the target system **30** due to the vulnerability of the security countermeasure software has been difficult.

[0120] On the other hand, the information processing system **1** of the present embodiment identifies threat types that can be countered by the installed software in the target system **30** out of the security countermeasure software with a reported vulnerability, and outputs the damage potential information including the risk value change information representing a change in the first risk value when countermeasures have been taken by the installed software against the threats of the identified threat types and the second risk value when no countermeasures have been taken by the installed software.

[0121] Therefore, when a new vulnerability in the security countermeasure software is reported, the information processing system **1** of the present embodiment can output damage potential information being information that can identify whether the risk of the target system **30** increases.

[0122] Consequently, the information processing system **1** of the present embodiment can evaluate risks to the target system **30** due to vulnerabilities in the security countermeasure software.

Second Embodiment

[0123] The present embodiment will explain a form in which the second risk value is calculated for a plurality of types of threats that can be countered by installed software, considering an impact on information security elements explained in vulnerability information and assuming that countermeasures are taken against some types of threats.

[0124] In the present embodiment, the same functional components as in the above embodiment are given the same codes and detailed explanations thereof will be omitted.

[0125] FIG. **1** is a schematic diagram illustrating an example of the configuration of an information processing system **2** of the present embodiment. The information processing system **2** has the same configuration as the information processing system **1** of the above embodiment, except that an information processing device **11** is provided instead of the information processing device **10**.

[0126] FIG. **8** is a block diagram illustrating an example of the functional configuration of the information processing device **11** of the present embodiment.

[0127] The information processing device **11** includes the communication unit **12**, the UI unit **14**, a storage unit **17**, and a processing unit **19**. The communication unit **12**, the UI unit **14**, the storage unit **17**, and the processing unit **19** are connected via a bus or the like to be able to exchange data or signals.

[0128] The information processing device **11** is the same as the information processing device **10** of the above embodiment, except that the storage unit **17** and the processing unit **19** are provided instead of the storage unit **16** and the processing unit **18**.

[0129] The storage unit **17** further stores impact information **16**C, in addition to the correspondence information **16**A and the risk analysis result information **16**B. Details of the impact information **16**C will be explained below.

[0130] The processing unit **19** includes the vulnerability determination unit **18**A, the first identifying unit **18**B, the first calculation unit **18**C, a second calculation unit **19**D, the output unit **18**E, the update unit **18**F, and a second identifying unit **19**G.

[0131] At least one of the vulnerability determination unit **18**A, the first identifying unit **18**B, the first calculation unit **18**C, the second calculation unit **19**D, the output unit **18**E, the update unit **18**F, and the second identifying unit **19**G is implemented by one or more processors, for example. For example, each of the units may be implemented by causing a processor such as a CPU to execute a computer program, that is, by software. Each of the units may be implemented by a processor such as a dedicated IC, that is, hardware. Each of the above units may be implemented using a combination of software and hardware. When a plurality of processors are used, each processor may implement one of the units or two or more of the units. In addition, at least one of the functional units provided in the processing unit **19** may be provided in an external information processing device that is communicatively connected to the information processing device **11** via the network NW. The impact information **16**C may be configured to be stored in the external information processing device that is communicatively connected to the information processing device **11** via the network NW.

[0132] The processing unit **19** is the same as the processing unit **18** of the above embodiment, except that the second calculation unit **19**D is provided instead of the second calculation unit **18**D and the second identifying unit **19**G is further provided.

[0133] On the basis of the vulnerability information and the impact information **16**C, the second identifying unit **19**G identifies, among threats that can be countered by the installed software, the threat types of threats that are affected by the vulnerability represented by the vulnerability information. The vulnerability information used by the second identifying unit **19**G for identifying is the vulnerability information acquired by the vulnerability determination unit **18**A.

[0134] As explained above, the vulnerability information defines the threat type of a threat having a vulnerability and an information security element representing at least one of confidentiality, integrity, and availability affected by the threat of the threat type. Therefore, the second identifying unit **19**G first identifies, on the basis of the vulnerability information, an element affected by a newly reported vulnerability among the three information security elements: confidentiality, integrity, and availability.

[0135] In detail, the second identifying unit **19**G identifies the element affected by the vulnerability among the above three information security elements by acquiring information by referring to a common vulnerability scoring system (CVSS), for example. The second identifying unit **19**G may also identify the elements affected by the vulnerability by acquiring or setting information in other ways. For example, the second identifying unit **19**G may refer to the CVSS Severity column of the NVD vulnerability information page, and identify the vulnerability as having an impact on the relevant element when it is rated high or low out of high, low, or none for each of the above three information security elements. When the vulnerability is rated as either full or partial, out of full, partial, or none for each of the above three information security elements, the vulnerability may be identified as having an impact on the relevant element.

[0136] FIG. **9** is a schematic diagram of an example of the data structure of the impact information **16**C. The impact information **16**C is information defining the presence or absence of an impact on information security elements for each threat type. In other words, the impact information **16**C is information representing which of the three information security elements is affected by the threat type. In FIG. **9**, "O" means that the threat of a corresponding threat type affects a corresponding information security element. A blank space means that no information security element is affected.

[0137] The impact information **16**C may be generated in advance by a user's instruction to the UI unit **14** and stored in the storage unit **17**. The impact information **16**C may be mechanically generated and stored in the storage unit **17** in advance. That is, the processing unit **19** may generate the impact information **16**C in advance and store the generated impact information **16**C in the storage unit **17**. The correspondence between threat types and information security elements in the impact information **16**C may be arbitrarily set by a user who operates the UI unit **14** or the like, may be mechanically set, or may be set in any way. It may also be set up so that a plurality of information security elements are affected for one threat type.

[0138] On the basis of the vulnerability information and the impact information **16**C, the second identifying unit **19**G identifies the threat types affected by the vulnerability represented by the vulnerability information among the threat types of threats that can be countered by the installed software.

[0139] For example, it is assumed that the second identifying unit **19**G identifies a vulnerability in the element "availability" being one of the three information security elements, from the vulnerability information. It is assumed that two threat types that can be countered by the installed software and identified by the first identifying unit **18**B are unauthorized access and information tampering. As illustrated in FIG. **9**, the impact information **16**C indicates that unauthorized access affects three elements: confidentiality, integrity, and availability, while information tampering affects two elements: confidentiality and integrity. In this case, the second identifying unit **19**G identifies, from the impact information **16**C, the threat type "unauthorized access" that affects the element "availability" identified as being vulnerable. The second identifying unit **19**G identifies threat types other than those identified as having an impact on the vulnerability as threat types having no impact on the vulnerability.

[0140] Subsequently, the second identifying unit **19**G notifies the second calculation unit **19**D of the threat types that are affected by the vulnerability and those that are not affected by the vulnerability.

[0141] When a plurality of threat types are identified by the first identifying unit **18**B, the second calculation unit

19D calculates the second risk value when the threat of the threat type identified by the second identifying unit **19**G that is affected by the vulnerability is assumed to have no countermeasure and the threat of the threat type identified by the second identifying unit **19**G that is not affected by the vulnerability is assumed to have countermeasure, among the threat types.

[0142] An example of an information processing flow to be performed by the information processing device **11** of the present embodiment will be explained.

[0143] FIG. **10** is a flowchart illustrating an example of an information processing flow to be performed by the information processing device **11** of the present embodiment.

[0144] The information processing device **11** performs processes of step S**200**, S**202**, S**204**, and S**206** in the same manner as the processes of step S**100**, S**102**, S**104**, and step S**106** (see FIG. **7**) performed by the information processing device **10**.

[0145] In detail, the vulnerability determination unit **18**A of the information processing device **11** acquires newly reported vulnerability information (step S**200**). Subsequently, the vulnerability determination unit **18**A determines whether a vulnerability represented by the vulnerability information acquired at step S**200** is a vulnerability to the installed software (step S**202**). The first identifying unit **18**B identifies a threat type that can be countered by the installed software, which has been determined to be a vulnerability to the installed software at step S**202** (step S**204**). The second calculation unit **18**D calculates the first risk value, which is a risk value for the threat of the threat type identified at step S**204**, when the countermeasure by the installed software is taken (step S**206**).

[0146] On the basis of the vulnerability information acquired at step S**200** and the impact information **16**C, the second identifying unit **19**G identifies a threat type affected by the vulnerability represented by the vulnerability information among the threat types of threats that can be countered by the installed software (step S**208**).

[0147] The second calculation unit **18**D calculates the second risk value when the threat of the threat type identified at step S**208** that is affected by the vulnerability is assumed to have no countermeasure and threats of other threat types that are not affected by the vulnerability are assumed to have countermeasure, among the threat types identified at step S**204** (step S**210**).

[0148] The output unit **18**E outputs the damage potential information including at least the risk value change information representing a change in the second risk value calculated at step S**210** with respect to the first risk value calculated at step S**206** (step S**212**). Subsequently, the routine is terminated.

[0149] As explained above, in the information processing system **2** of the present embodiment, on the basis of the threat type of a threat having a vulnerability, vulnerability information defining an information security element representing at least one of confidentiality, integrity, and availability affected by the threat of the threat type, and the impact information **16**C, the second identifying unit **19**G identifies, among threat types of threats that can be countered by installed software, a threat type affected by a vulnerability represented by the vulnerability information. Subsequently, the second calculation unit **19**D calculates the second risk value when the threat of the threat type identified by the second identifying unit **19**G that is affected by the vulnerability is assumed to have no countermeasure and the threat of the threat type identified by the second identifying unit **19**G that is not affected by the vulnerability is assumed to have countermeasure, among the threat types identified by the first identifying unit **18**B.

[0150] In this way, in the present embodiment, the second calculation unit **19**D calculates the second risk value when the threats of threat types having an impact on the vulnerability identified by the second identifying unit **19**G are assumed to have no countermeasures and the threat types of threat types having no impact on the vulnerability are assumed to have countermeasures, in consideration of an impact on confidentiality, integrity, and availability being the three information security elements explained in the vulnerability information.

[0151] Therefore, in addition to the effects of the above embodiment, the information processing system **2** of the present embodiment can provide damage potential information narrowed down to threat types that truly affect the target system **30**.

[0152] An example of the hardware configuration of the information processing device **10** and the information processing device **11** of the above embodiment will be explained.

[0153] FIG. **11** is a diagram illustrating an example of the hardware configuration of the information processing device **10** and the information processing device **11** of the above embodiment.

[0154] The information processing device **10** and the information processing device **11** each include a control device such as a CPU **86**, storage devices such as a read only memory (ROM) **88**, a random access memory (RAM) **90**, and a hard disk drive (HDD) **92**, an I/F unit **82** being an interface with various devices, and a bus **96** connecting various parts, and have a hardware configuration using a normal computer.

[0155] In the information processing device **10** and the information processing device **11**, each of the above parts is implemented on a computer by the CPU **86** reading computer programs from the ROM **88** onto the RAM **90** and executing the read computer programs.

[0156] The computer programs for executing the above processes performed by the information processing device **10** and the information processing device **11** may be stored in the HDD **92**. The computer programs for performing the above processes performed by the information processing device **10** and the information processing device **11** may be pre-embedded in the ROM **88** and provided.

[0157] The computer programs for performing the above processes, which are executed by the information processing device **10** and the information processing device **11**, may be stored on a computer-readable storage medium, such as a CD-ROM, a CD-R, a memory card, a digital versatile disc (DVD), and a flexible disk (FD), in an installable or executable file format, and provided as a computer program product. The computer programs for performing the above processes, which are executed by the information processing device **10** and the information processing device **11**, may be stored on a computer connected to a network such as the Internet and be downloaded over the network so as to be provided. The computer programs for performing the above processes, which are executed by the information processing device **10** and the information processing device **11**, may be provided or distributed over the network such as the Internet.

[0158] While certain embodiments have been described, these embodiments have been presented by way of example only, and are not intended to limit the scope of the inventions. Indeed, the novel embodiments described herein may be embodied in a variety of other forms; furthermore, various omissions, substitutions and changes in the form of the embodiments described herein may be made without departing from the spirit of the inventions. The accompanying claims and their equivalents are intended to cover such forms or modifications as would fall within the scope and spirit of the inventions.

What is claimed is:

1. An information processing system comprising one or more hardware processors configured to:

identify a threat type capable of being countered by installed software being security countermeasure software installed in a target system, from among security countermeasure software with a reported vulnerability;

calculate a first risk value when a countermeasure is taken by the installed software for a threat of the identified threat type;

calculate a second risk value when no countermeasure is taken by the installed software for the threat of the identified threat type; and

output damage potential information including risk value change information representing a change in the second risk value with respect to the first risk value.

2. The system according to claim **1**, wherein the one or more hardware processors are configured to output the damage potential information further including the threat type of the threat having damage potential according to the risk value change information.

3. The system according to claim **1**, wherein the one or more hardware processors are configured to output the damage potential information further including information on presence or absence of damage potential that represents presence of damage potential when a change in a risk value represented by the risk value change information represents an increase in risk and absence of damage potential when the change represents no change or a decrease in risk.

4. The system according to claim **1**, wherein

the one or more hardware processors are configured to:

calculate the first risk value by a risk analysis comparing risk values before and after the countermeasure by the installed software for the threat of the identified threat type; and

calculate the second risk value by the risk analysis when no countermeasure is taken by the installed software for the threat of the identified threat type.

5. The system according to claim **1**, wherein the one or more hardware processors are configured to calculate the first risk value based on risk analysis result information obtained by comparing risk values before and after the countermeasure against the threat when the countermeasure is taken by the installed software.

6. The system according to claim **5**, wherein the one or more hardware processors are configured to update the risk analysis result information by using an analysis result of a risk analysis for calculating the second risk value.

7. The system according to claim **1**, wherein the one or more hardware processors are further configured to determine whether a vulnerability represented by newly reported vulnerability information is a vulnerability to the installed software being the security countermeasure software installed in the target system, and

the one or more hardware processors are configured to identify the installed software for which it is determined that the vulnerability is to the installed software in the target system, and the threat type capable of being countered by the installed software.

8. The system according to claim **1**, wherein the one or more hardware processors are configured to identify the threat type capable of being countered by the installed software, based on correspondence information that associates the installed software in the target system with a threat type of a threat capable of being countered by the installed software.

9. The system according to claim **8**, wherein the one or more hardware processors are further configured to update the correspondence information.

10. The system according to claim **1**, wherein the one or more hardware processors are configured to output the damage potential information further including a countermeasure level calculated from the risk value change information and a vulnerability level.

11. The system according to claim **1**, wherein the one or more hardware processors are configured to display the damage potential information on a display.

12. The system according to claim **1**, wherein the one or more hardware processors are further configured to identify a threat type affected by a vulnerability represented by vulnerability information among threat types of threats capable of being countered by the installed software, based on the vulnerability information and impact information, the vulnerability information defining a threat type of a threat having a vulnerability and an information security element representing at least one of confidentiality, integrity, and availability affected by the threat of the threat type, the impact information defining presence or absence of an impact on the information security element for each threat type, and

the one or more hardware processors are configured to calculate the second risk value when no countermeasure is taken for a threat of the threat type identified as affected by the threat, and countermeasure is taken for a threat of the threat type identified as not affected by the vulnerability, among a plurality of threat types identified as capable of being countered by the installed software.

13. An information processing method performed by an information processing device, the information processing method comprising:

identifying a threat type capable of being countered by installed software being security countermeasure software installed in a target system, from among security countermeasure software with a reported vulnerability;

calculating a first risk value when a countermeasure is taken by the installed software for a threat of the identified threat type;

calculating a second risk value when no countermeasure is taken by the installed software for the threat of the identified threat type; and

outputting damage potential information including risk value change information representing a change in the second risk value with respect to the first risk value.

14. A computer program product having a non-transitory computer readable medium including programmed instructions, wherein the programmed instructions, when executed by a computer, cause the computer to execute:

identifying a threat type capable of being countered by installed software being security countermeasure software installed in a target system, from among security countermeasure software with a reported vulnerability;

calculating a first risk value when a countermeasure is taken by the installed software for a threat of the identified threat type;

calculating a second risk value when no countermeasure is taken by the installed software for the threat of the identified threat type; and

outputting damage potential information including risk value change information representing a change in the second risk value with respect to the first risk value.

* * * * *