[0008]

PTL 1: Japanese Translation of PCT International Application Publication No. JP-T-2009-539182

PTL 2: U.S. Patent No. 8131012

PTL 3: Japanese Unexamined Patent Application Publication No. 2013-003929

[Summary of Invention]

[Technical Problem]

[0009]

In the techniques disclosed in NPL 1 and PTL 1, an operator of a monitoring system needs to set a monitoring rule by hand. However, setting of a lot of monitoring rules by hand is work requiring many worker-hours for an operator of a monitoring system. In addition, setting of an appropriate monitoring rule is difficult work for an operator without expert knowledge about a monitoring system.

[0010]

In order for the technique disclosed in PTL 2 to appropriately determine whether or not a given situation is an abnormal circumstance, input of a large amount of learning data is needed. In the technique disclosed in PTL 2, a person needs to generate a large amount of learning data by hand. Generating of a large amount of learning data by hand is troublesome work for an operator of a monitoring system.

[0011]

The technique disclosed in PTL 3 cannot generate a monitoring rule depending on an environment to be monitored.

[0012]

~~It is an object~~ Embodiments of the present invention ~~to~~ support work of an operator of a monitoring system to set a monitoring rule depending on an

environment to be monitored.

[Solution to Problem]

[0013]

~~A first aspect of the present invention is an information processing system including: an environment expression extracting unit which extracts environment expressions from incident information, which includes the environment expressions which are expressions expressing environments to be monitored and action expressions which are expressions expressing actions performed in the environments, and is information expressing a certain incident by the expressions; an action expression extracting unit which extracts the action expressions from the incident information; and an information collecting unit which generates information in which the extracted action expressions are associated with the environment expressions expressing the environments when the actions expressed by the action expressions have been performed among the extracted environment expressions, conducts a search with respect to the generated information, with the action expressions as a key, and calculates, on the basis of the search, frequency at which the environment expressions have been extracted.~~

According to a first aspect of the present invention, there is provided an information processing system comprising circuitry configured to: extract environment expressions from incident information, which describes an incident in which what abnormal action was performed in what environment, and which includes the environment expressions expressing the environments to be monitored and action expressions expressing actions performed in the environments; extract the action expressions from the incident information; generate information in which the extracted action expressions are associated with the environment expressions expressing the environments when the actions expressed by the action expressions have been performed among the extracted environment expressions, conduct a search with respect to the generated information, with the action expressions as a key, and calculate, on the basis of the search, frequency at which the environment expressions have been extracted; store

the action expressions and the associated environment expressions; refer to the stored expressions, and, when the frequency at which the environment expressions associated with a specific action expression among the stored action expressions have been extracted is higher than a predetermined threshold value, associate the specific action expression with the environment expressions having high frequency of extraction and outputs the associated expressions; and generate a monitoring rule for monitoring occurrence of an abnormal circumstance, on the basis of the outputted environment expressions and action expression, the monitoring rule having a conditional clause in which the environments expressed by the environment expressions are satisfied and the action expressed by the action expression is detected.

[0014]

~~A second aspect of the present invention is an information processing method by a computer, including: extracting environment expressions from incident information, which includes the environment expressions which are expressions expressing environments to be monitored and action expressions which are expressions expressing actions performed in the environments, and is information expressing a certain incident by the expressions; extracting the action expressions from the incident information; and generating information in which the extracted~~

~~action expressions are associated with the environment expressions expressing the environments when the actions expressed by the action expressions have been performed among the extracted environment expressions, conducting a search with respect to the generated information, with the action expressions as a key, and calculating, on the basis of the search, frequency at which the environment expressions have been extracted.~~

According to a second aspect of the present invention, there is provided an information processing method executed by a computer, comprising processes of: extracting environment expressions from incident information, which describes an incident in which what abnormal action was performed in what environment, and which includes the environment expressions expressing the environments to be monitored and action expressions expressing actions performed in the environments extracting the action expressions from the incident information; generating information in which the extracted action expressions are associated with the environment expressions expressing the environments when the actions expressed by the action expressions have been performed among the extracted environment expressions, conducting a search with respect to the generated information, with the action expressions as a key, and calculating, on the basis of the search, frequency at which the environment expressions have been extracted; storing the action expressions and the associated environment expressions; referring to the stored expressions, and, when the frequency at which the environment expressions associated with a specific action expression among the stored action expressions have been extracted is higher than a predetermined threshold value, associates the specific action expression with the environment expressions having high frequency of extraction and outputs the associated expressions; and generating a monitoring rule for monitoring occurrence of an abnormal circumstance, on the basis of the outputted environment expressions and action expression, the monitoring rule having a conditional clause in which the environments expressed by the environment expressions are satisfied and the action expressed by the action expression is detected.

[0015]

~~A third aspect of the present invention is a program which makes a computer~~

~~execute: processing of extracting environment expressions from incident information, which includes the environment expressions which are expressions expressing environments to be monitored and action expressions which are expressions expressing actions performed in the environments, and is information expressing a certain incident by the expressions; processing of extracting the action expressions from the incident information; and processing of generating information in which the extracted action expressions are associated with the environment expressions expressing the environments when the actions expressed by the action expressions have been performed among the extracted environment expressions, conducting a search with respect to the generated information, with the action expressions as a key, and calculating, on the basis of the search, frequency at which the environment expressions have been extracted.~~

According to a third aspect of the present invention, there is provided a non-transitory computer-readable storage medium storing a program which causes a computer to execute processing for: extracting environment expressions from incident information, which describes an incident in which what abnormal action was performed in what environment, and which includes the environment expressions expressing the environments to be monitored and action expressions expressing actions performed in the environments ; extracting the action expressions from the incident information; and generating information in which the extracted action expressions are associated with the environment expressions expressing the environments when the actions expressed by the action expressions have been performed among the extracted environment expressions, conducting a search with respect to the generated information, with the action expressions as a key, and calculating, on the basis of the search, frequency at which the environment expressions have been extracted; storing the action expressions and the associated environment expressions; referring to the stored expressions, and, when the frequency at which the environment expressions associated with a specific action expression among the stored action expressions have been extracted is higher than a predetermined threshold value, associates the specific action expression with the

environment expressions having high frequency of extraction and outputs the associated expressions; and generating a monitoring rule for monitoring occurrence of an abnormal circumstance, on the basis of the outputted environment expressions and action expression, the monitoring rule having a conditional clause in which the environments expressed by the environment expressions are satisfied and the action expressed by the action expression is detected.

[0016]

~~The object~~Embodiments of the present invention ~~is~~are achieved by a computer-readable storage medium storing the above-described program.

[Advantageous Effects of Invention]

[0017]

According to embodiments of the present invention, work of an operator of a monitoring system to set a monitoring rule depending on an environment to be monitored can be supported.

[Brief Description of Drawings]

[0018]

Fig. 1 is a block diagram illustrating a configuration of an information processing system 1000 in a first exemplary embodiment of the present invention.

Fig. 2 is a diagram illustrating an example of information which a first storing unit 210 in the first exemplary embodiment of the present invention stores.

Fig. 3 is a diagram illustrating an example of a configuration of hardware capable of achieving the information processing system 1000 in the first exemplary embodiment of the present invention.

Fig. 4 is a flow chart illustrating an operation of the information processing system 1000 in the first exemplary embodiment of the present invention.

Fig. 5 is a flow chart illustrating the operation of the information processing system 1000 in the first exemplary embodiment of the present invention.

Fig. 6 is a block diagram illustrating a configuration of an information processing system 2000 in a second exemplary embodiment of the present invention.

Fig. 7 is a flow chart illustrating an operation of the information processing system 2000 in the second exemplary embodiment of the present invention.

Fig. 8 is an example of information which a second storing unit 220 in the second exemplary embodiment of the present invention stores.

CLAIMS

~~[Claim 1]~~

1. An information processing system comprising circuitry configured to:

~~an environment expression extracting means which~~ extract~~s~~ environment expressions from incident information, which describes an incident in which what abnormal action was performed in what environment, and which includes

the environment expressions ~~which are expressions~~ expressing the environments to be monitored and

action expressions ~~which are expressions~~ expressing actions performed in the environments

~~, and is information expressing a certain incident by the expressions~~;

~~an action expression extracting means which~~ extract~~s~~ the action expressions from the incident information; ~~and~~

~~an information collecting means which~~ generate~~s~~ information in which the extracted action expressions are associated with the environment expressions expressing the environments when the actions expressed by the action expressions have been performed among the extracted environment expressions, conduct~~s~~ a search with respect to the generated information, with the action expressions as a key, and calculate~~s~~, on the basis of the search, frequency at which the environment expressions have been extracted~~.~~;

~~[Claim 2]~~

~~The information processing system according to claim 1, wherein~~

~~the incident information is text information describing an incident in which what abnormal action was performed in what environment,~~

~~the information processing system further comprises a first storing means which~~ store~~s~~ the action expressions and the associated environment expressions ~~associated by the information collecting means, and~~;

~~the information processing system further comprises an outputting~~

means which refers to the first storing means the stored expressions, and, when the frequency at which the environment expressions associated with a specific action expression among the stored action expressions which the first storing means stores have been extracted is higher than a predetermined threshold value, associates the specific action expression with the environment expressions having high frequency of extraction and outputs the associated expressions.; and

generate a monitoring rule for monitoring occurrence of an abnormal circumstance, on the basis of the outputted environment expressions and action expression, the monitoring rule having a conditional clause in which the environments expressed by the environment expressions are satisfied and the action expressed by the action expression is detected.

[Claim 3]

2. The information processing system according to claim 21, the circuitry further configured to wherein the outputting means further

in the outputting, outputs information indicating that the actions expressed by the action expressions are abnormal actions in the environments expressed by the environment expressions.

[Claim 4]

The information processing system according to claim 2 or 3, further comprising:

a monitoring rule generating means which generates a monitoring rule for monitoring occurrence of an abnormal circumstance, on the basis of the outputted environment expressions and action expression, wherein

the monitoring rule generating means generates a monitoring rule having a conditional clause in which the environments expressed by the environment expressions are satisfied and the action expressed by the action expression is detected.

[Claim 5]

3. The information processing system according to any one of claims 1 to 4 or 2, wherein the information collecting means the circuitry further configured to

associates an action expression with an environment expression

extracted from the same incident information.

~~[Claim 6]~~

4. The information processing system according to any one of claims 1 to ~~4~~3, ~~wherein the information collecting means~~ the circuitry further configured to

associate~~s~~ an action expression with an environment expression extracted from the same sentence included in the incident information.

~~[Claim 7]~~

5. The information processing system according to any one of claims 1 to ~~6~~4, ~~wherein,~~the circuitry further configured to

for an action expression having frequency of extraction exceeding a predetermined threshold value, ~~the outputting means~~ in the outputting, output~~s~~ the action expression and an environment expression associated with the action expression.

~~[Claim 8]~~

6. The information processing system according to any one of claims 1 to ~~7~~5, ~~further comprising:~~ the circuitry further configured to

~~a typical expression storing means which~~ associate~~s~~ a plurality of expressions expressing the same or similar actions or environments with a typical expression which is a typical expression of the plurality of expressions, and store~~s~~ the associated expressions; and

~~an expression unifying means which~~ refer~~s~~ to the stored typical expression ~~storing means~~, on the basis of the environment expressions or the action expressions, to replace the environment expressions or the action expressions with the typical expression.

~~[Claim 9]~~

7. An information processing method executed by a computer, comprising processes of:

extracting environment expressions from incident information, which describes an incident in which what abnormal action was performed

in what environment, and which includes

the environment expressions ~~which are expressions~~ expressing the environments to be monitored and

action expressions ~~which are expressions~~ expressing actions performed in the environments

~~, and is information expressing a certain incident by the expressions;~~

extracting the action expressions from the incident information; ~~and~~

generating information in which the extracted action expressions are associated with the environment expressions expressing the environments when the actions expressed by the action expressions have been performed among the extracted environment expressions, conducting a search with respect to the generated information, with the action expressions as a key, and calculating, on the basis of the search, frequency at which the environment expressions have been extracted~~.~~;

storing the action expressions and the associated environment expressions;

referring to the stored expressions, and, when the frequency at which the environment expressions associated with a specific action expression among the stored action expressions have been extracted is higher than a predetermined threshold value, associates the specific action expression with the environment expressions having high frequency of extraction and outputs the associated expressions; and

generating a monitoring rule for monitoring occurrence of an abnormal circumstance, on the basis of the outputted environment expressions and action expression, the monitoring rule having a conditional clause in which the environments expressed by the environment expressions are satisfied and the action expressed by the action expression is detected.

~~[Claim 10]~~

8. A non-transitory computer-readable storage medium storing a program which causes a computer to execute processing for:

~~processing of~~ extracting environment expressions from incident information, which describes an incident in which what abnormal action was performed in what environment, and which includes

the environment expressions ~~which are expressions~~

expressing the environments to be monitored and action expressions ~~which are expressions~~ expressing actions performed in the environments ~~, and is information expressing a certain incident by the expressions~~;

~~processing of~~ extracting the action expressions from the incident information; and

~~processing of~~ generating information in which the extracted action expressions are associated with the environment expressions expressing the environments when the actions expressed by the action expressions have been performed among the extracted environment expressions, conducting a search with respect to the generated information, with the action expressions as a key, and calculating, on the basis of the search, frequency at which the environment expressions have been extracted~~.~~;

storing the action expressions and the associated environment expressions;

referring to the stored expressions, and, when the frequency at which the environment expressions associated with a specific action expression among the stored action expressions have been extracted is higher than a predetermined threshold value, associates the specific action expression with the environment expressions having high frequency of extraction and outputs the associated expressions; and

generating a monitoring rule for monitoring occurrence of an abnormal circumstance, on the basis of the outputted environment expressions and action expression, the monitoring rule having a conditional clause in which the environments expressed by the environment expressions are satisfied and the action expressed by the action expression is detected.