

CLAIMS

1. A non-transitory computer-readable recording medium storing a control program causing a computer to execute processing, the processing comprising:

displaying a rule node, a first node related to an access destination which is allowed and a second node related to an information range which is provided to the access destination;

when transmission of information about a cyber attack is performed based on a transmission request of the information about the cyber attack event to a transmission destination from a terminal, performing, in a case where the transmission destination is included in the access destination provided by the first node coupled to the rule node corresponding to the terminal, a mask processing on information belonging to an information category provided by the second node coupled to the rule node corresponding to the terminal; and

providing the information about the cyber attack event after the mask processing is performed to the transmission destination.

2. The non-transitory computer-readable recording medium according to claim 1, wherein

a plurality of nodes are allowed to be registered as the access destination in association with the first node.

3. The non-transitory computer-readable recording medium according to claim 1, wherein

in a case where a plurality of nodes are registered as the information category in association with the second node, the mask processing is performed on all of the information belonging to a plurality of information categories indicated by the plurality of nodes as the information category, and the information about the cyber attack event is provided after the mask processing to the transmission node.

4. The non-transitory computer-readable recording medium according to claim 1, wherein

the mask processing is processing of anonymizing the information included in the information category.

5. A control method, comprising:

displaying, by a computer, a rule node, a first node related to an access destination which is allowed and a second node related to an information range which is provided to the access destination;

when transmission of information about a cyber attack event is performed based on a transmission request of the information about the cyber attack event to a transmission destination from a terminal, performing, in a case where the transmission destination is included in the access destination provided by the first node coupled to the rule node corresponding to the terminal, a mask processing on information belonging to an information category provided by the second node coupled to the rule node corresponding to the terminal; and

providing the information about the cyber attack event after the mask processing is performed to the transmission destination.

6. The control method according to claim 5, wherein

a plurality of nodes are allowed to be registered as the access destination in association with the first node.

7. The control method according to claim 5, further comprising:

performing, in a case where a plurality of nodes are registered as the information category in association with the second node, the mask processing on all of the plurality of nodes as the information category; and

providing the information about the cyber attack event after mask processing to the transmission node.

8. The control method according to claim 5, wherein the mask processing is processing of anonymizing the information included in the information category.

9. An information processing device, comprising:
a memory that stores a control program; and
a processor that performs a processing based on the control program, wherein the processing includes:
displaying a rule node, a first node related to an access destination which is allowed and a second node related to an information range which is provided to the access destination;

when transmission of information about a cyber attack event is performed based on a transmission request of the information about the cyber attack event to a transmission destination from a terminal, performing, in a case where the transmission destination is included in the access destination provided by the first node coupled to the rule node corresponding to the terminal, a mask processing on information belonging to an information category provided by the second node coupled to the rule node corresponding to the terminal; and
providing the information about the cyber attack event after the mask processing is performed to the transmission destination.

10. The information processing device according to claim 9, wherein a plurality of nodes are allowed to be registered as the access destination in association with the first node.

11. The information processing device according to claim 9, wherein in a case where a plurality of nodes are registered each as the fifth node in association with the second node, control is performed to execute the processing in common on all the information belonging to a plurality of

information categories indicated by the plurality of nodes, and to provide information after processing to the third node.

12. The information processing device according to claim 9, wherein the mask processing is processing of anonymizing the information included in the information category.