

CLAIMS

1. A non-transitory computer readable recording medium storing a computer executable program that, when executed, causes a computer to perform a cyber attack analysis support process, the cyber attack analysis support process comprising:

when information of a first cyber attack event including information of malware is registered as a result of a detection of the malware within an information processing system to be monitored, searching for past cyber attack events by referring to a storage storing information on the past cyber attack events, comparing first child elements of first elements of the first cyber attack event and past child elements of past elements of each of the past cyber attack events, counting a number of child elements in which the first child element and the past child element match with each other and determining the past cyber attack event having the number of child elements which is equal to or more than a specific number as a second cyber attack event having a similarity relationship with the first cyber attack event; and

displaying information of the second cyber attack event and the registered information of the first cyber attack event on a display circuit by associating a second child element of a second element of the second cyber attack event which matches the first child element with the first child element.

2. The non-transitory computer readable recording medium according to claim 1, the cyber attack analysis support process further comprising:

displaying information indicating the number of child elements on the display circuit .

3. The non-transitory computer readable recording medium according to claim 1, wherein the displaying the information is performed in such a manner that the second child element which matches the first child element and the first child element are coupled by a coupling line on the on the display circuit.

4. The non-transitory computer readable recording medium according to claim 1, wherein the first elements, the past elements and the second element include at least one of a cyber attack activity, an attacker and an attack method.

5. The non-transitory computer readable recording medium according to claim 4, wherein the first child elements, the past child elements and the second child element include, when the first elements, the past elements and the second element include the attacker, include at least one of an IP address, a mail address and an account of a social network service regarding the attacker.

6. The non-transitory computer readable recording medium according to claim 3, wherein a display of the first cyber attack event is a display of at least one of information on a pattern of a first cyber attack regarding the first cyber attack event, information on an attack base of an attacker, and information on a target to be attacked.

7. A cyber attack analysis support method comprising:

searching, by a computer, when information of a first cyber attack event including information of malware is registered as a result of a detection of the malware within an information processing system to be monitored, for past cyber attack events by referring to a storage storing information on the past cyber attack events, comparing first child elements of first elements of the first cyber attack event and past child elements of past elements of each of the past cyber attack events, counting a number of child elements in which the first child element and the past child element match with each other and determining the past cyber attack event having the number of child elements which is equal to or more than a specific number as a second cyber attack event having a similarity relationship with the first cyber attack event; and

displaying information of the searched second cyber attack event and the registered information of the first cyber attack event on a display circuit by associating a second child element of a second element of the second cyber attack event which matches the first child element with the first child element.

8. The cyber attack analysis support method according to claim 7, further comprising:

displaying information indicating the number of child elements on the display circuit.

9. The cyber attack analysis support method according to claim 7, wherein the displaying the information is performed in such a manner that the second child element which matches the first child element and the first child element are coupled by a coupling line on the on the display circuit.

10. The cyber attack analysis support method according to claim 8, wherein the first elements, the past elements and the second element include at least one of a cyber attack activity, an attacker and an attack method.

11. The cyber attack analysis support method according to claim 10, wherein the first child elements, the past child elements and the second child element include, when the first elements, the past elements and the second element include the attacker, include at least one of an IP address, a mail address and an account of a social network service regarding the attacker.

12. The cyber attack analysis support method according to claim 9, wherein a display of the first cyber attack event is a display of at least one of information on a pattern of a first cyber attack regarding the first cyber attack event, information on an attack base of an attacker, and information on a target to be attacked.

13. A cyber attack analysis support system comprising:
a memory that stores a computer executable program; and
a processor that executes a process based on the computer executable program,

wherein the process includes:

searching for past cyber attack events by referring to a storage storing information on the past cyber attack events, when information of a first cyber attack event including information of malware is registered as a result of a detection of the malware within an information processing system to be monitored, comparing first child elements of first elements of the first cyber attack event and past child elements of past elements of each of the past cyber attack events, counting a number of child elements in which the first child element and the past child element match with each other and determining the past cyber attack event having the number of child elements which is equal to or more than a specific number as a second cyber attack event having a similarity relationship with the first cyber attack event; and

displaying information of the second cyber attack event and the registered information of the first cyber attack event on a display circuit by associating a second child element of a second element of the second cyber attack event which matches the first child element with the first child element.

14. The cyber attack analysis support system according to claim 13, the process further comprising:

displaying information indicating the number of child elements on the display circuit.

15. The cyber attack analysis support system according to claim 13, wherein the displaying the information is performed in such a manner that the

second child element which matches the first child element and the first child element are coupled by a coupling line on the on the display circuit.

16. The cyber attack analysis support system according to claim 13, wherein the first elements, the past elements and the second element include at least one of a cyber attack activity, an attacker and an attack method.

17. The cyber attack analysis support system according to claim 16, wherein the first child elements, the past child elements and the second child element include, when the first elements, the past elements and the second element include the attacker, include at least one of an IP address, a mail address and an account of a social network service regarding the attacker.

18. The cyber attack analysis support system according to claim 15, wherein a display of the first cyber attack event is a display of at least one of information on a pattern of a first cyber attack regarding the first cyber attack event, information on an attack base of an attacker, and information on a target to be attacked.