[Document Name] DESCRIPTION

[Title of Invention] ANALYSIS SYSTEM, ANALYSIS METHOD, AND STORAGE MEDIUM

[Technical Field]

[0001]

The present invention relates to a technology of analyzing cryptographic communication executed by an information communication apparatus and the like.

[Background Art]

[0002]

There is a demand for a technology of analyzing communication processing executed by an information processing apparatus (such as a computer) that is connected to a communication network (hereinafter simply referred to as an "information communication apparatus"), in recent years.

[0003]

For example, such analysis of communication processing is used for analysis of behavior of an information communication apparatus during development and operation stages, or analysis of behavior of a communication processing program executed on an information communication apparatus.

[0004]

There is a particular demand in recent years for a technology for analyzing a content of improper communication processing caused by an improper computer program (a computer program includes various types of software programs, and may be hereinafter simply referred to as a "program"), such as a virus, that is executed on an information communication apparatus.

CLAIMS:

1. An analysis system comprising:

memory acquisition means capable of acquiring at least part of data stored in a memory unit in an information communication apparatus including a computing unit and the memory unit; and

communication processing means for

determining whether key data including an encryption key used for encryption processing in a cryptographic communication protocol are stored in the memory unit, based on communication data transmitted and received in accordance with the cryptographic communication protocol between the information communication apparatus and a communication network, and

instructing the memory acquisition means to acquire data stored in the memory unit, based on the determination result.

2. The analysis system according to Claim 1, wherein

the communication processing means determines that the key data are stored in the memory unit when, based on a result of analyzing the communication data, determining that a specific condition with regard to the cryptographic communication protocol is satisfied, and

instructs the memory acquisition means to acquire data stored in the memory unit when determining that the key data are stored in the memory unit.

3. The analysis system according to Claim 2, wherein

the communication processing means, being arranged between the information communication apparatus and the communication network,

suspends communication between the information communication apparatus and the communication network when determining that the key data are stored in the memory unit, and

instructs the memory acquisition means to acquire data stored in the memory unit,

resumes communication between the information communication apparatus and the communication network after receiving notification

representing completion of acquisition of data stored in the memory unit from the memory acquisition means.

4. The analysis system according to Claim 3, wherein

the communication processing means resumes communication between the information communication apparatus and the communication network when a predetermined time elapses after instructing the memory acquisition means to acquire data stored in the memory unit.

5. The analysis system according to any one of Claim 2 to Claim 4, wherein the communication processing means

includes a key data acquisition policy including information by which whether at least the specific condition related to the key data is satisfied or not can be determined for each of one or more of the cryptographic communication protocols, and

instructs the memory acquisition means to acquire data stored in the memory unit, when, as a result of analyzing the communication data, determining that the specific condition is satisfied based on the key data acquisition policy.

6. The analysis system according to Claim 5, wherein

the key data acquisition policy includes information by which a timing at which the key data are shared, in the cryptographic communication protocol, between the information communication apparatus and other information communication apparatus communicably connected to the information communication apparatus through the communication network, can be determined, and

the communication processing means determines that the specific condition is satisfied when, as a result of analyzing the communication data, determining arrival of the timing at which the key data are shared , based on the key data acquisition policy.

7. The analysis system according to Claim 5, wherein the key data acquisition

policy includes information by which execution of a specific procedure related to sharing of the key data, in the cryptographic communication protocol, between the information communication apparatus and other information communication apparatus communicably connected to the information communication apparatus through the communication network, can be determined, and

the communication processing means determines that the specific condition is satisfied when, as a result of analyzing the communication data, determining that the specific procedure is executed, based on the key data acquisition policy.

8. The analysis system according to Claim 7, wherein

the communication processing means determines that the specific condition is satisfied when, as a result of analyzing information in an unencrypted part of the communication data, determining that the specific procedure is executed, based on the key data acquisition policy.

9. An analysis method comprising, by an information processing apparatus:

determining whether key data including an encryption key used for encryption processing in a cryptographic communication protocol are stored in a memory unit, based on communication data transmitted and received in accordance with the cryptographic communication protocol between an information communication apparatus including a computing unit and the memory unit, and a communication network; and

acquiring at least part of data stored in the memory unit, based on the determination result.

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

processing of determining whether key data including an encryption key used for encryption processing in a cryptographic communication protocol are stored in a memory unit, based on communication data transmitted and received in accordance with the cryptographic communication protocol between an information communication apparatus including a computing unit and the memory

unit, and a communication network; and

processing of acquiring at least part of data stored in the memory unit, based on the determination result.