

[DESCRIPTION]

[Title of Invention]

COMMUNICATION DESTINATION DETERMINATION DEVICE,
COMMUNICATION DESTINATION DETERMINATION METHOD,
5 AND RECORDING MEDIUM

[Technical Field]

[0001]

The present invention relates to a communication
destination determination device and the like which are useful for
10 securing security.

[Background Art]

[0002]

A server such as a web server and a mail server receives a
request and the like for acquiring a mail from a plurality of
15 communication destinations (communication devices) via a
communication network such as an intranet or the Internet.

[0003]

For example, Patent Literature 1 and Patent Literature 2
disclose devices that manage a server capable of processing a
20 request signal received via a communication network, respectively.
The technologies disclosed in Patent Literature 1 and Patent
Literature 2 will be respectively described.

[0004]

The managing device disclosed in Patent Literature 1
25 generates a request category log in which the number of request
signals received via the communication network are classified
based on predetermined time intervals and types of the requests.
The managing device further generates, in accordance with
predetermined time interval, a system log in which a resource

usage amount in the server managing the requests are recorded. The managing device calculates a usage amount of resources required for processing the requests every request on the basis of the generated request category log and the generated system log.

5 [0005]

The request limiting device disclosed in Patent Literature 2 can limit a request having high possibility of reducing processing loads according to the state of the loads in the server. The request limiting device classifies requests into a plurality of request patterns, and calculates loads when performing request-based processing every classified request pattern. For a certain request, the request limiting device specifies a request pattern to which the request belongs, and determines whether or not to limit the certain request on the basis of loads when processing a request belonging to the specified request pattern.

15 [0006]

In the case of constructing the above-described server in the aforementioned example, it is not only necessary to secure high security in the server, but also reduce risk of a threat (an unauthorized program) from a malicious communication destination via the communication network. For example, Patent Literature 3 discloses a vulnerability diagnosis conducting apparatus capable of diagnosing vulnerability of a host device.

20 [0007]

In the case of performing a process for diagnosing vulnerability of the host device, the vulnerability diagnosis conducting apparatus has history information indicating a time at which the process has been performed. In the case of diagnosing vulnerability of a certain host device, the vulnerability diagnosis

25

conducting apparatus estimates a time required for diagnosing vulnerability of the certain host device on the basis of the history information and generates a schedule for diagnosing the certain host device on the basis of the estimated time.

5 [Citation List]

[Patent Literature]

[0008]

PTL 1: International Publication No. WO 2008/007669

PTL 2: Japanese Laid-open Patent Publication No.
10 2007-328417

PTL 3: Japanese Laid-open Patent Publication No.
2009-237807

[Summary of Invention]

[Technical Problem]

15 [0009]

Attack method of malicious communication destination to a device increases. As a consequence, for example, even though vulnerability of the server is efficiently diagnosed using the vulnerability diagnosis conducting apparatus disclosed in Patent
20 Literature 3, the apparatus cannot always diagnose all types of vulnerability. The reason for this is because the apparatus is not always able to detect the communication destination that attacks according to various attack methods.

[0010]

25 Therefore, one of main objects of the present invention is to provide a communication destination determination device and the like capable of detecting a suspicious communication destination as a threat.

[Solution to Problem]

[0011]

In order to achieve the above-described object, as an aspect of the present invention, a communication destination
5 determination device including:

signal transmission means for transmitting a second signal in response to a first signal to a communication destination when the first signal is received from the communication destination via a communication network; and

10 communication destination determination means for determining whether or not the communication destination is suspicious as a threat on a basis of whether or not a third signal transmitted from the communication destination is received within a certain time period after a timing of transmission of the second
15 signal.

[0012]

In addition, as another aspect of the present invention, a communication destination determination method including:

transmitting a second signal in response to a first signal to a
20 communication destination when the first signal is received from the communication destination via a communication network; and

determining whether or not the communication destination is suspicious as a threat on a basis of whether or not a third signal transmitted from the communication destination is received within
25 a certain time period after a timing of transmission of the second signal.

[0013]

Furthermore, the object is also realized by an associated communication destination determination program, and

a computer-readable recording medium which records the program.

[Advantageous Effects of Invention]

[0014]

In accordance with the communication destination
5 determination device and the like according to the present
invention, it is possible to detect a suspicious communication
destination as a threat.

[Brief Description of Drawings]

[0015]

10 [Fig. 1] Fig. 1 is a block diagram illustrating a
configuration of a communication destination determination
device according to a first example embodiment of the present
invention.

[Fig. 2] Fig. 2 is a flowchart illustrating the flow of
15 processing in the communication destination determination device
according to the first example embodiment.

[Fig. 3] Fig. 3 is a diagram illustrating an example of a
request signal.

[Fig. 4] Fig. 4 is a diagram illustrating an example of a
20 response signal (the second signal).

[Fig. 5] Fig. 5 is a block diagram illustrating a
configuration of a communication destination determination
device according to a second example embodiment of the present
invention.

25 [Fig. 6] Fig. 6 is a flowchart illustrating the flow of
processing in the communication destination determination device
according to the second example embodiment.

[Fig. 7] Fig. 7 is a diagram conceptually illustrating an
example of signal information.

[Fig. 8] Fig. 8 is a diagram conceptually illustrating an example of communication history information.

[Fig. 9] Fig. 9 is a block diagram illustrating a configuration of a communication destination determination
5 device according to a third example embodiment of the present invention.

[Fig. 10] Fig. 10 is a flowchart illustrating the flow of processing in the communication destination determination device according to the third example embodiment.

10 [Fig. 11] Fig. 11 is a diagram conceptually illustrating an example of communication history information.

[Fig. 12] Fig. 12 is a diagram conceptually illustrating an example of communication history information.

15 [Fig. 13] Fig. 13 is a diagram conceptually illustrating an example of communication history information.

[Fig. 14] Fig. 14 is a diagram conceptually illustrating an example of communication history information.

[Fig. 15] Fig. 15 is a diagram conceptually illustrating an example of communication history information.

20 [Fig. 16] Fig. 16 is a block diagram schematically illustrating a hardware configuration of a calculation processing device capable of realizing the communication destination determination device according to each example embodiment of the present invention.

25 [Description of Embodiments]

[0016]

Next, example embodiments embodying the present invention will be described in detail with reference to the drawings.

[0017]

<First example embodiment>

With reference to Fig. 1, configuration of a communication destination determination device 101 according to a first example embodiment of the present invention will be described in detail. Fig. 1 is a block diagram illustrating the configuration of the communication destination determination device 101 according to the first example embodiment of the present invention.

[0018]

The communication destination determination device 101 according to the first example embodiment has a signal transmission unit (signal transmitter) 102 and a communication destination determination unit (communication destination determiner) 103.

[0019]

The communication destination determination device 101 can perform communication connection with a communication destination (a communication device) 104 via a communication network.

[0020]

Hereinafter, processing in the communication destination determination device will be described; however, for the purpose of convenience, information transmitted/received via the communication network is assumed to be processed in accordance with HTTP. The HTTP indicates an abbreviation for Hypertext_Transfer_Protocol. The information transmitted/received via the communication network may not be processed in accordance with the HTTP and may be processed according to another communication protocols.

[0021]

With reference to Fig. 2, the processing in the communication destination determination device 101 according to the first example embodiment will be described in detail. Fig. 2 is a flowchart illustrating the flow of the processing in the communication destination determination device 101 according to the first example embodiment.

[0022]

The communication destination 104 transmits a request signal (hereinafter, also referred to as a “first signal”) to the communication destination determination device 101 via the communication network. The request signal, for example, is a signal for requiring a certain file. In the case of a HTTP request, the request signal, for example, is a signal including a request illustrated in an example 1 to an example 3.

[0023]

Example 1: GET / HTTP/1.1 (a request signal for requiring a file in a directory “/”, which is described in HTTP version 1.1)

Example 2: GET /rom-0 HTTP/1.1 (a request signal for requiring a file “rom-0” in the directory “/”, which is described in the HTTP version 1.1)

Example 3: GET /nnnn/nnn/nn.php HTTP/1.1 (a request signal for requiring a file “nn.php” in a directory “/nnnn/nnn”, which is described in the HTTP version 1.1)

[0024]

With reference to Fig. 3, the request signal (the first signal) will be described in more detail. Fig. 3 is a diagram illustrating an example of the request signal.

[0025]

For example, the request signal may have a header (“Accept:” to “Keep-Alive”) including information and the like indicating that an address (an item of “Host” in Fig. 3) indicating a communication destination is “www.xxx.zzz”, in addition to the requests illustrated in the example 1 to the example 3. The header, for example, may include information and the like indicating that an operating system of the communication destination is “OS_10”. Since the request signal illustrated in the example 3 conforms to the HTTP, a detailed description for each item in Fig. 3 will be omitted.

[0026]

Referring to Fig. 2, the signal transmission unit 102 receives the first signal (the request signal) transmitted by the communication destination 104 (step S101). The signal transmission unit 102 transmits a response signal (hereinafter, also referred to as a “second signal”) in response to the received the first signal to the communication destination 104 (step S102).

[0027]

In the case of the HTTP version 1.1, the response signal is a signal as illustrated in an example of Fig. 4, and for example, is a signal including a response of “200_OK” indicating normal completion of processing for the received request signal. Fig. 4 is a diagram illustrating an example of the response signal (the second signal). The response signal may include a header (“Date:” to “text/html”) in which a date and the like has been described, information (a message body) to respond the request signal, and the like, in addition to the response of “200_OK”. Since the response signal exemplified in Fig. 4 conforms to the HTTP, a detailed description for each item in Fig. 4 will be

omitted. The response signal transmitted by the signal transmission unit 102 may not be always a signal indicating normal completion of processing for the request signal.

[0028]

5 Referring to Fig. 2, after step S102, the communication destination determination unit 103 determines whether or not the communication destination 104 is suspicious as a threat on the basis of whether or not it is possible to receive a third signal from the communication destination 104 within a certain period time
10 after the timing of transmission of the second signal (the response signal) to the communication destination 104 (step S103). When the third signal is received within the certain period time after the timing of transmission of the response signal to the communication destination 104, the communication destination determination unit
15 103 determines that the communication destination 104 is suspicious as a threat. When the third signal is not received within the certain period time after the timing of transmission of the response signal to the communication destination 104, the communication destination determination unit 103 determines that
20 the communication destination 104 is less likely to pose a threat in relation to the second signal.

[0029]

In step S103, the third signal, for example, is a request signal. In this case, the third signal may be a signal for requiring
25 the same file as that of the first signal or a signal for requiring a different file.

[0030]

In step S103, the certain period time, for example, is 30 minutes. In this case, the communication destination

determination unit 103 determines whether or not the communication destination 104 is suspicious as a threat on the basis of whether or not the third signal is received from the communication destination 104 within 30 minutes after the timing of transmission of the second signal (the response signal) to the communication destination 104. When the third signal is received within 30 minutes after the timing of transmission of the response signal to the communication destination 104, the communication destination determination unit 103 determines that the communication destination 104 is suspicious as a threat. When the third signal is not received within the certain period time after the timing of transmission of the response signal to the communication destination 104, the communication destination determination unit 103 determines that the communication destination 104 is less likely to pose a threat in relation to the second signal.

[0031]

The communication destination determination unit 103 may output information (for example, an address) about a suspicious communication destination 104 with a threat to a display device (not illustrated), an external device (not illustrated) and the like.

[0032]

A manager, who monitors communication performed via the communication network, for example, can specify a communication destination that is less likely to pose a threat by referring to the information displayed on the display device.

[0033]

Next, effects for the communication destination determination device 101 according to the first example

embodiment will be described.

[0034]

According to the communication destination determination device 101, it is possible to detect a suspicious communication destination as a threat. The reason for this will be described in detail.

[0035]

A signal transmitted/received via the communication network is largely classified into a suspicious signal as a threat and a less suspicious signal as a threat. The inventor of the present application has found a tendency that when the first signal is received from a certain communication destination, it is possible to determine whether or not the certain communication destination is suspicious as a threat on the basis of whether or not the certain communication destination transmits the third signal within a predetermined time period with respect to the second signal transmitted in response to the first signal. This determination method will be described in detail below.

[0036]

For the convenience of description, it is assumed that the certain communication destination transmits the first signal to the server via the communication network.

[0037]

The inventor of the present application has found that the certain communication destination can be largely classified into a first communication device, which transmits the third signal to the server within the predetermined time period in response to the reception of the second signal in the certain communication destination in response to the first signal, and a second

communication device which does not transmit the third signal to the server regardless of the reception of the second signal. Furthermore, in such a case, the inventor of the present application has found a tendency (a characteristic) that the first
5 communication device is suspicious as a threat and the second communication device is less likely to pose a threat. As a consequence, the inventor of the present application has found a tendency that it is possible to determine whether or not the certain communication destination is suspicious as a threat on the basis of
10 whether or not the third signal is received within the predetermined time period after the second signal in response to the first signal is transmitted.

[0038]

As described above, the communication destination
15 determination device 101 according to the present example embodiment determines whether a communication destination is suspicious as a threat by using the tendency, so that it is possible to detect a suspicious communication destination as a threat in accordance with the communication destination determination
20 device 101 according to the present example embodiment.

[0039]

In contrast, since the vulnerability diagnosis conducting apparatus disclosed in Patent Literature 3 does not use the tendency as described above, it is not always possible to detect a
25 suspicious communication destination as a threat.

[0040]

That is, in accordance with the communication destination determination device 101 according to the first example embodiment, it is possible to detect a suspicious communication

destination as a threat.

[0041]

The communication destination determination device 101 starts processing in response to the reception of the first signal transmitted by the communication destination 104; however, for
5 example, it may be possible to employ a mode in which a fourth signal is transmitted to the communication destination 104 and the communication destination 104 transmits the first signal in response to the fourth signal. Furthermore, in the
10 aforementioned example, the communication destination determination device 101 transmits the second signal and further receives the third signal; however, it is not always necessary to allow one device to perform the process for transmitting the second signal and the process for receiving the third signal.
15 When the communication determination device 101 is provided in a plural number, it may be determined whether a certain communication determination device transmits the second signal and a communication determination device different from the certain communication determination device receives the third
20 signal.

[0042]

Moreover, the aforementioned function can also be performed using a proxy scanner (hereinafter, also referred to as a “second communication destination”) that searches for an IP
25 address indicating a proxy server capable of performing communication connection with the communication network. In this case, a transmission destination of the second signal from the communication destination determination device 101 does not always need to be a communication destination having transmitted

the first signal. A description will be provided for a process mode in which the aforementioned function is performed using the proxy server.

[0043]

5 The proxy scanner transmits a fifth signal to a specific device. The specific device receives the fifth signal transmitted by the proxy scanner, and transmits a sixth signal to the server in response to the received fifth signal. The server receives the sixth signal transmitted by the specific device, and transmits a
10 seventh signal in response to the received sixth signal to the specific device. The specific device receives the seventh signal transmitted by the server, and transmits an eighth signal to the proxy scanner in response to the received seventh signal. The proxy scanner receives the eighth signal transmitted by the
15 specific device. The proxy scanner determines whether or not the specific device has a proxy function on the basis of whether or not the fifth signal and the sixth signal coincide with each other, the seventh signal and the eighth signal coincide with each other, and the eighth signal is a signal in response to the fifth signal. In
20 this processing, when the specific device is the communication destination determination device 101, the communication destination determination device 101 transmits the sixth signal to the server in response to the fifth signal transmitted by the proxy scanner, and determines whether or not the server is suspicious as
25 a threat on the basis of whether or not the seventh signal transmitted by the server in response to the sixth signal is received within a predetermined period time from the timing of transmission of the sixth signal.

[0044]

The aforementioned example has described the flow of the processing in which the communication destination determination device 101 determines whether or not a communication destination having transmitted the first signal is suspicious as a threat with
5 reference to an example in which the communication destination transmits the third signal; however, only one communication destination is not always provided. For example, as will be described later in a third example embodiment, the communication destination determination device 101 may determine whether or
10 not a communication destination is suspicious as a threat on the basis of a port and the like through which a signal (the first signal or the third signal) is received.

[0045]

<Second example embodiment>

15 Next, a second example embodiment of the present invention based on the aforementioned first example embodiment will be described.

[0046]

In the following description, characteristics according to
20 the present example embodiment will be mainly described, and the same reference numerals are given to configuration similar to those of the aforementioned first example embodiment and a redundant description will be omitted.

[0047]

25 With reference to Fig. 5, configuration of a communication destination determination device 208 according to the second example embodiment of the present invention will be described in detail. Fig. 5 is a block diagram illustrating the configuration of the communication destination determination device 208 according

to the second example embodiment of the present invention.

[0048]

The communication destination determination device 208 according to the second example embodiment has the signal
5 transmission unit (signal transmitter) 102, the communication destination determination unit (communication destination determiner) 103, a history specifying unit (history specifier) 205, a signal selection unit (signal selector) 206, and a history update unit (history updater) 207. The communication destination
10 determination device 208 can refer to, update, or store signal information 209, which will be described later with reference to Fig. 7, and communication history information 210 which will be described later with reference to Fig. 8.

[0049]

15 The communication destination determination device 208 can perform communication connection with the communication destination (a communication device) 104 via the communication network.

[0050]

20 With reference to Fig. 7, the signal information 209 will be described. Fig. 7 is a diagram conceptually illustrating an example of the signal information 209.

[0051]

When the request signal (the first signal) is received from
25 the communication destination 104, the signal information 209 includes the response signal (the second signal) effective for the received request signal. As illustrated in Fig. 7, the signal information 209 may be information in which the response signal and signal identifier capable of identifying the response signal are

associated with each other.

[0052]

In the signal information 209 exemplified in Fig. 7, a signal identifier “R1” is associated with a response signal
5 “200_OK_Its_works!”. This indicates that a signal identifier indicating the response signal “200_OK_Its_works!” is “R1” and “200_OK_Its_works!” can be transmitted as a response signal effective for a request signal. Furthermore, in the signal information 209 exemplified in Fig. 7, a signal identifier “R2” is
10 associated with a response signal “400_Not_Found”. This indicates that a signal identifier indicating the response signal “404_Not_Found” is “R2” and “404_Not_Found” can be transmitted as a response signal effective for a request signal.

[0053]

15 The signal information 209 may include many response signals, or items different from those (the signal identifier and the response signal) exemplified in Fig. 7. That is, the signal information 209 is not limited to the aforementioned example.

[0054]

20 Next, with reference to Fig. 8, the communication history information 210 will be described. Fig. 8 is a diagram conceptually illustrating an example of the communication history information 210.

[0055]

25 The communication history information 210 includes a response signal transmitted to the communication destination 104 in response to a received request signal. As illustrated in Fig. 8, the communication history information 210 may be information in which the response signal and a signal identifier capable of

identifying the response signal are associated with each other.

[0056]

In the communication history information 210 exemplified in Fig. 8, the signal identifier “R1” is associated with the response
5 signal “200_OK._Its_works!”. This represents a history that the signal identifier indicating the response signal “200_OK._Its_works!” is “R1” and the signal transmission unit 102 has transmitted the response signal “200_OK._Its_works!” in response to the request signal (the first signal).

10 [0057]

The communication history information 210 may include many response signals, or items different from those exemplified in Fig. 8. That is, the communication history information 210 is not limited to the aforementioned example.

15 [0058]

Next, with reference to Fig. 6, the processing in the communication destination determination device 208 according to the second example embodiment will be described in detail. Fig. 6 is a flowchart illustrating the flow of the processing in the
20 communication destination determination device 208 according to the second example embodiment.

[0059]

The signal transmission unit 102 receives the first signal transmitted by the communication destination 104 (step S101).

25 [0060]

The history specifying unit 205 reads the response signal included in the communication history information 210 (step S201). That is, in step S201, the history specifying unit 205 reads the response signal (the second signal), which has been transmitted to

the communication destination 104, from the communication history information 210.

[0061]

The signal selection unit 206 selects one response signal, which is different from the response signal read by the history specifying unit 205, from the response signals included in the signal information 209 (step S202). That is, in step S202, the signal selection unit 206 selects a response signal, which has not been transmitted to the communication destination 104, from response signals effective as a response for a request signal. When the communication history information 210 includes no response signals, it is sufficient if the signal selection unit 206 selects one response signal from the response signals included in the signal information 209. Alternatively, when the history specifying unit 205 includes no response signals, the signal selection unit 206 may select a predetermined response signal with respect to a received request signal from the response signals included in the signal information 209. For example, when it is known that many (or few) response signals transmitted in response to the request signal are biased to a specific response signal, the specific response signal may be set as the predetermined response signal.

[0062]

The signal transmission unit 102 transmits the response signal (that is, the aforementioned second signal) selected by the signal selection unit 206 to the communication destination 104 (step S102).

[0063]

The history update unit 207 updates the communication

history information 210 by adding the response signal, which is transmitted by the signal transmission unit 102, to the communication history information 210 (step S203).

[0064]

5 The processing may be performed in sequence of step S103 and step S203.

[0065]

Next, effects for the communication destination determination device 208 according to the second example
10 embodiment will be described.

[0066]

According to the communication destination determination device 208, it is possible to detect the communication destination 104 that is suspicious as a threat. The reason for this is because
15 the configuration of the communication destination determination device 208 include the configuration of the communication destination determination device 101 according to the first example embodiment.

[0067]

20 In accordance with the communication destination determination device 208 according to the present example embodiment, it is possible to efficiently detect a suspicious communication destination 104 as a threat. The reason for this is because the communication destination determination device 208
25 can search for a specific response signal serving as a trigger by which the communication destination 104 transmits a request signal. When a response signal received in response to the request signal is the specific response signal, it is highly probable that a suspicious communication destination 104 as a threat will

transmit the request signal by employing the response signal as a trigger. However, since the specific response signal is not clear, it is necessary to find out a specific response signal according to the communication destination 104 in order to more reliably detect
5 a suspicious communication destination as a threat. When the request signal is received from the communication destination 104, the signal selection unit 206 selects a response signal different from the response signals included in the communication history information 210 from transmittable response signals included in
10 the signal information 209. Since the signal transmission unit 102 transmits the response signal selected by the signal selection unit 206, it is highly probable to efficiently find out a specific response signal.

[0068]

15 That is, in accordance with the communication destination determination device 208 according to the present example embodiment, it is possible to efficiently detect a suspicious communication destination as a threat.

[0069]

20 In the aforementioned processing, the communication destination determination device 208 transmits the response signal different from the response signals included in the communication history information 210 to the communication destination 104; however, in the case of transmitting each response signal included
25 in the signal information 209, it may be possible to employ a configuration for ending the process for transmitting the response signal.

[0070]

Furthermore, the communication destination determination

device 208 may be provided in a plural number. In this case, the plurality of communication destination determination devices 208 may employ a configuration for referring to one communication history information 210. For example, when the communication destination determination device 208 are provided in a plural number and each communication destination determination device 208 refers to one communication history information 210, it is possible to more efficiently detect a suspicious communication destination as a threat. The reason for this is because, when the communication destination 104 transmits a request signal to the plurality of communication destination determination devices 208 in a short period, each communication destination determination device 208 can share the communication history information 210 and transmit response signals, which are different from one another, to a communication destination.

[0071]

<Third example embodiment>

Next, a third example embodiment of the present invention will be described.

[0072]

In the following description, characteristics according to the present example embodiment will be mainly described, and the same reference numerals are given to elements similar to those of the aforementioned second example embodiment and a redundant description will be omitted.

[0073]

With reference to Fig. 9, configuration of a communication destination determination device 311 according to the third example embodiment of the present invention will be described in

detail. Fig. 9 is a block diagram illustrating the configuration of the communication destination determination device 311 according to the third example embodiment of the present invention.

[0074]

5 The communication destination determination device 311 according to the third example embodiment has the signal transmission unit (signal transmitter) 102, the communication destination determination unit (communication destination determiner) 103, a history specifying unit (history specifier) 305,
10 the signal selection unit (signal selector) 206, a history update unit (history updater) 307, and a communication history information storage unit (communication history information storage) 310. The communication destination determination device 311 can refer to the signal information 209 as described
15 with reference to Fig. 7.

[0075]

 The communication destination determination device 311 can perform communication connection with the communication destination (a communication device) 104 via the communication
20 network.

[0076]

 Next, with reference to Fig. 10, processing in the communication destination determination device 311 according to the third example embodiment will be described in detail. Fig.
25 10 is a flowchart illustrating the flow of the processing in the communication destination determination device 311 according to the third example embodiment. The third example embodiment is different from the second example embodiment in terms of processing and the like for communication history information

stored in the communication history information storage unit 310 for example, as compared with the second example embodiment.

[0077]

The signal transmission unit 102 receives the first signal
5 transmitted by the communication destination 104 (step S101).

[0078]

The history specifying unit 305 reads a transmitted response signal on the basis of the communication history information, which is stored in the communication history information storage
10 unit 310 and will be described with reference to Fig. 11 to Fig. 15 (step S301). The processing for step S301 will be described later with reference to Fig. 11 to Fig. 15.

[0079]

The signal selection unit 206 selects one response signal,
15 which is different from the response signal read by the history specifying unit 305, from the response signals included in the signal information 209 (step S202). That is, in step S202, the signal selection unit 206 selects a non-transmitted response signal from response signals effective as a response for a request signal.
20 When the communication history information storage unit 310 includes no response signals for a received request signal, it is sufficient if the signal selection unit 206 selects one response signal from the response signals included in the signal information 209.

25 [0080]

The signal transmission unit 102 transmits the response signal (that is, the aforementioned second signal) selected by the signal selection unit 206 to the communication destination 104 (step S102).

[0081]

The history update unit 307 updates the communication history information in the communication history information storage unit 310 by adding the response signal, that is transmitted
5 by the signal transmission unit 102, to the communication history information storage unit 310 (step S303). The process for step S303 will be described later with reference to Fig. 11 to Fig. 15.

[0082]

The processing may be performed in sequence of step S103
10 and step S303. Furthermore, the processing of step S103 may be a determination process which will be described later with reference to Fig. 11 to Fig. 15.

[0083]

Next, with reference to each diagram illustrated in Fig. 11
15 to Fig. 15, the processes of step S301 and step S303 in the communication destination determination device 311, the communication history information stored in the communication history information storage unit 310, and effects obtained by the processes will be described.

20 [0084]

Firstly, with reference to Fig. 11, communication history information 312 stored in the communication history information storage unit 310, the processing illustrated in step S301 (Fig. 10) and step S303 (Fig. 10), and effects obtained in the case of the
25 communication history information 312 will be described. Fig. 11 is a diagram conceptually illustrating an example of the communication history information 312.

[0085]

The communication history information 312 will be

described.

[0086]

The communication history information 312 is information in which a response signal transmitted to a certain communication destination, a communication destination identifier capable of identifying the certain communication destination, and a signal identifier capable of identifying the response signal are associated with one another. The communication history information 312 may not always include the signal identifier.

10 [0087]

In the communication history information 312 exemplified in Fig. 11, a signal identifier “R1”, a communication destination identifier “10. 11. 12. 13”, and a response signal “200_OK._its_works!” are associated with one another. This represents a history that the signal identifier indicating the response signal “200_OK._Its_works!” is “R1” and the signal transmission unit 102 has transmitted the response signal “200_OK._Its_works!” to a communication destination indicated by the communication destination identifier “10. 11. 12. 13” in response to the request signal (the first signal).

20

[0088]

The process of step S303 regarding the communication history information 312 will be described.

[0089]

25 The history update unit 307, for example, specifies a communication destination identifier indicating a communication destination on the basis of the request signal (the first signal) exemplified in Fig. 3. The history update unit 307 generates information in which the specified communication destination

identifier, the response signal, which has been transmitted to the communication destination from the signal transmission unit 102, and the signal identifier, which indicates the response signal, are associated with one another, and adds the generated information to
5 the communication history information storage unit 310 as the communication history information 312.

[0090]

The process of step S301 regarding the communication history information 312 will be described.

10 [0091]

On the basis of the request signal (the first signal) exemplified in Fig. 3, the history specifying unit 305 specifies a communication destination identifier indicating a communication destination. The history specifying unit 305 specifies a response
15 signal associated with the specified communication destination identifier in the communication history information 312 stored in the communication history information storage unit 310.

[0092]

A description will be provided for effects obtained by the
20 communication destination determination device 311 according to the present example embodiment when the communication history information is the communication history information 312. In accordance with the communication destination determination device 311 according to the present example embodiment, it is
25 possible to more quickly detect a suspicious communication destination as a threat. The reason for this is because the communication destination determination device 311 can search for a specific response signal serving as a trigger, by which the communication destination 104 transmits a request signal, on the

basis of the communication destination identifier. As described above, when a response signal received in response to a request signal is the specific response signal, it is highly probable that a suspicious communication destination 104 as a threat will transmit
5 a request signal by employing the response signal as a trigger. However, since the specific response signal depends on the communication destination 104, it is necessary to find out the specific response signal depending on the communication destination 104 in order to quickly detect a suspicious
10 communication destination as a threat. When a request signal is received from a certain communication destination, the signal selection unit 206 selects a response signal, which is different from a response signal transmitted to the certain communication destination, from transmittable response signals included in the
15 signal information 209. Since the signal transmission unit 102 transmits the response signal selected by the signal selection unit 206, it is highly probable to find out the specific response signal.
[0093]

Next, with reference to Fig. 12, communication history
20 information 313 stored in the communication history information storage unit 310, the processing illustrated in step S301 (Fig. 10) and step S303 (Fig. 10), and effects obtained in the case of the communication history information 313 will be described. Fig. 12 is a diagram conceptually illustrating an example of the
25 communication history information 313.

[0094]

The communication history information 313 will be described.

[0095]

The communication history information 313 is information in which a response signal transmitted to a certain communication destination, an information identifier capable of identifying information requested by a request signal transmitted by the certain communication destination, and a signal identifier capable of identifying the response signal are associated with one another. The communication history information 313 may not always include the signal identifier.

[0096]

In the communication history information 313 exemplified in Fig. 12, a signal identifier “R1”, an information identifier “xp.php”, and a response signal “200_OK._its_works!” are associated with one another. This represents a history that the signal identifier indicating the response signal “200_OK._Its_works!” is “R1” and the signal transmission unit 102 has transmitted the response signal “200_OK._Its_works!” in response to the request signal (the first signal) requiring information indicated by the information identifier “xp.php”.

[0097]

The processing of step S303 regarding the communication history information 313 will be described.

[0098]

On the basis of the request signal (the first signal) exemplified in Fig. 3, the history update unit 307 specifies an information identifier required by the request signal. The history update unit 307 generates information in which the specified information identifier, the response signal, which has been transmitted to the communication destination from the signal transmission unit 102, and the signal identifier, which indicates

the response signal, are associated with one another, and adds the generated information to the communication history information storage unit 310 as the communication history information 313.

[0099]

5 The processing of step S301 regarding the communication history information 312 will be described.

[0100]

 The history specifying unit 305 specifies an information identifier capable of identifying information requested by the request signal on the basis of the request signal (the first signal) exemplified in Fig. 3. The history specifying unit 305 specifies a response signal associated with the specified information identifier in the communication history information 312 stored in the communication history information storage unit 310.

15 [0101]

 The processing described with reference to Fig. 12 may be assumed to be a process mode in which the communication destination determination device 311 has the signal transmission unit 102 and the communication destination determination unit 103. In this case, when the first signal requiring certain information is received from a first communication destination via a communication network, the signal transmission unit 102 transmits the second signal in response to the first signal to the first communication destination. When the third signal requiring the certain information is received from a second communication destination within a certain time period after the timing of transmission of the second signal, the communication destination determination unit 103 determines that at least one of the first communication destination and the second communication

destination is suspicious as a threat.

[0102]

A description will be provided for effects obtained by the communication destination determination device 311 according to the present example embodiment when the communication history information is the communication history information 313. In accordance with the communication destination determination device 311 according to the present example embodiment, for example, even when a communication destination changes a communication destination identifier such as an IP address and then transmits a request signal, it is possible to efficiently detect a suspicious communication destination as a threat. The reason for this is because the communication destination determination device 311 searches for a specific response signal on the basis of information required by the request signal. The IP indicates an abbreviation for Internet_Protocol.

[0103]

The reason for obtaining the aforementioned effects will be described in more detail. The communication destination 104 does not always transmit a request signal by using a communication destination identifier such as one IP address. In other words, it is probable that the communication destination 104 will transmit the request signal by using a plurality of IP addresses. In this case, the communication destination determination device 311 according to the present example embodiment does not select a response signal on the basis of the communication destination identifier, but selects a response signal on the basis of information required by the request signal. Consequently, in accordance with the communication destination determination device 311 according

to the present example embodiment, for example, even when an IP address is changed, it is possible to efficiently search for a specific response signal on the basis of the requested information. That is, for example, even though there are a plurality of
5 communication destinations, when the communication destinations perform a process for requiring specific information, it is possible to efficiently detect a suspicious communication destination as a threat in accordance with the communication destination determination device 311 according to the present example
10 embodiment.

[0104]

Next, with reference to Fig. 13, communication history information 314 stored in the communication history information storage unit 310, the processing illustrated in step S301 (Fig. 10)
15 and step S303 (Fig. 10), and effects obtained in the case of the communication history information 314 will be described. Fig. 13 is a diagram conceptually illustrating an example of the communication history information 314.

[0105]

20 The communication history information 314 will be described.

[0106]

The communication history information 314 is information in which a response signal transmitted to a certain communication destination, a port identifier (for example, a port number) via
25 which a request signal transmitted by the certain communication destination is received, and a signal identifier capable of identifying the response signal are associated with one another. The communication history information 314 may not always

include the signal identifier.

[0107]

In the communication history information 314 exemplified in Fig. 13, a signal identifier “R1”, a port identifier “80”, and a response signal “200_OK._its_works!” are associated with one another. This represents a history that the signal identifier indicating the response signal “200_OK._Its_works!” is “R1” and the signal transmission unit 102 has transmitted the response signal “200_OK._Its_works!” to the communication destination 104 in response to the request signal (the first signal) received via the port identifier “80”.

[0108]

The processing of step S303 regarding the communication history information 314 will be described.

15 [0109]

The history update unit 307 specifies a port identifier via which the request signal (the first signal) exemplified in Fig. 3 is received. The history update unit 307 generates information in which the specified port identifier, the response signal, which has been transmitted to the communication destination from the signal transmission unit 102, and the signal identifier, which indicates the response signal, are associated with one another, and adds the generated information to the communication history information storage unit 310 as the communication history information 314.

25 [0110]

The processing of step S301 regarding the communication history information 314 will be described.

[0111]

The history specifying unit 305 specifies a port identifier

via which the request signal (the first signal) is received. The history specifying unit 305 specifies a response signal associated with the specified port identifier in the communication history information 314 stored in the communication history information storage unit 310.

[0112]

The processing described with reference to Fig. 13 may be assumed to be a process mode in which the communication destination determination device 311 has the signal transmission unit 102 and the communication destination determination unit 103. In this case, when the first signal is received from a first communication destination via a port through which communication connection with the communication network is performed, the signal transmission unit 102 transmits the second signal in response to the first signal to the first communication destination. When the third signal is received from a second communication destination via the port within a certain time period after the timing of transmission of the second signal, the communication destination determination unit 103 determines that at least one of the first communication destination and the second communication destination is suspicious as a threat.

[0113]

A description will be provided for effects obtained by the communication destination determination device 311 according to the present example embodiment when the communication history information is the communication history information 314. In accordance with the communication destination determination device 311 according to the present example embodiment, it is possible to efficiently detect a suspicious communication

destination as a threat. The reason for this is as follows. For example, even though the communication destination 104 requires various types of information by using a plurality of IP addresses, when port identifiers of the communication destination, which
5 transmits the request signal, are equal to each other, it is possible to select a non-transmitted response signal on the basis of the port identifiers. That is, for example, even though there are a plurality of communication destinations, when the communication destinations perform a process for transmitting a request to a port
10 indicated by a specific port identifier, it is possible to efficiently detect a suspicious communication destination as a threat on the basis of the port identifier in accordance with the communication destination determination device 311 according to the present example embodiment.

15 [0114]

Next, with reference to Fig. 14, communication history information 315 stored in the communication history information storage unit 310, the processing illustrated in step S301 (Fig. 10) and step S303 (Fig. 10), and effects obtained in the case of the
20 communication history information 315 will be described. Fig. 14 is a diagram conceptually illustrating an example of the communication history information 315.

[0115]

The communication history information 315 will be
25 described.

[0116]

The communication history information 315 is information in which a response signal transmitted to a certain communication destination, a device identifier (for example, an AS number)

capable of identifying a device via which the certain communication destination transmits a request signal, and a signal identifier capable of identifying the response signal are associated with one another. The AS indicates an abbreviation for Autonomous_System. The communication history information 315 may not always include the signal identifier.

[0117]

In the communication history information 315 exemplified in Fig. 14, a signal identifier “R1”, a device identifier “1234”, and a response signal “200_OK._its_works!” are associated with one another. This represents a history that the signal identifier indicating the response signal “200_OK._Its_works!” is “R1” and the signal transmission unit 102 has transmitted the response signal “200_OK._Its_works!” to a communication destination in response to the request signal (the first signal) received via the device identifier “1234”.

[0118]

The processing of step S303 regarding the communication history information 315 will be described.

[0119]

The history update unit 307 specifies a device identifier (an AS number) via which a communication destination indicated by a communication destination identifier transmits a request signal on the basis of the communication destination identifier included in the request signal (the first signal) exemplified in Fig. 3. The method for specifying the AS number (the device identifier) based on the communication destination identifier will not be described. The history update unit 307 generates information in which the specified device identifier, the response signal, which has been

transmitted to the communication destination from the signal transmission unit 102, and the signal identifier, which indicates the response signal, are associated with one another, and adds the generated information to the communication history information storage unit 310 as the communication history information 315.

[0120]

The processing of step S301 regarding the communication history information 315 will be described.

[0121]

The history specifying unit 305 specifies the AS number via which the communication destination indicated by the communication destination identifier transmits a request signal on the basis of the communication destination identifier included in the request signal (the first signal). The history specifying unit 305 specifies a response signal associated with the specified device identifier in the communication history information 315 stored in the communication history information storage unit 310.

[0122]

The processing described with reference to Fig. 14 may be assumed to be a process mode in which the communication destination determination device 311 has the signal transmission unit 102 and the communication destination determination unit 103. In this case, when the first signal is received from a first communication destination via the communication network, the signal transmission unit 102 transmits the second signal in response to the first signal to the first communication destination. When the third signal is received from a second communication destination within a certain time period after the timing of transmission of the second signal, the communication destination

determination unit 103 specifies a first device via which communication with the first communication destination is performed and a second device via which communication with the second communication destination is performed. When the specified first device and the specified second device coincide with each other, the communication destination determination unit 103 determines that at least one of the first communication destination and the second communication destination is suspicious as a threat.

10 [0123]

A description will be provided for effects obtained by the communication destination determination device 311 according to the present example embodiment when the communication history information is the communication history information 315. In accordance with the communication destination determination device 311 according to the present example embodiment, it is possible to efficiently detect a suspicious communication destination as a threat. The reason for this is as follows. For example, when a communication destination transmits a request signal via a specific device, it is possible to select a non-transmitted response signal on the basis of a device identifier indicating the specific device. That is, for example, even though there are a plurality of communication destinations, when the communication destinations perform a process for transmitting a request via a device indicated by a specific device identifier, it is possible to efficiently detect a suspicious communication destination as a threat on the basis of the device identifier in accordance with the communication destination determination device 311 according to the present example embodiment.

[0124]

Next, with reference to Fig. 15, communication history information 316 stored in the communication history information storage unit 310, the processing illustrated in step S301 (Fig. 10) and step S303 (Fig. 10), and effects obtained in the case of the communication history information 316 will be described. Fig. 14 is a diagram conceptually illustrating an example of the communication history information 316.

[0125]

The communication history information 316 will be described.

[0126]

The communication history information 316 is information in which a response signal transmitted to a certain communication destination, a time zone in which a request signal is received from the certain communication destination, and a signal identifier capable of identifying the response signal are associated with one another. The communication history information 316 may not always include the signal identifier.

[0127]

In the communication history information 316 exemplified in Fig. 15, a signal identifier “R1”, a time zone “10:00 to 11:00”, and a response signal “200_OK._its_works!” are associated with one another. This represents a history that the signal identifier indicating the response signal “200_OK._Its_works!” is “R1” and the signal transmission unit 102 has transmitted the response signal “200_OK._Its_works!” to the communication destination 104 in response to the request signal (the first signal) received in the time zone “10:00 to 11:00”.

[0128]

The processing of step S303 regarding the communication history information 316 will be described.

[0129]

5 The history update unit 307 calculates a time zone including a time at which the request signal (the first signal) exemplified in Fig. 3 is received. The time zone, for example, is a time zone in which one day (that is, 24 hours) is divided every hour. The time zone needs not to be decided in advance, and for example, may be
10 calculated on the basis of a time at which a request is received. The history update unit 307 generates information in which the calculated time zone, the response signal, which has been transmitted to the communication destination from the signal transmission unit 102, and the signal identifier, which indicates
15 the response signal, are associated with one another, and adds the generated information to the communication history information storage unit 310 as the communication history information 316.

[0130]

 The processing of step S301 regarding the communication
20 history information 316 will be described.

[0131]

 The history specifying unit 305 calculates a time zone including a time at which the request signal (the first signal) is received. The history specifying unit 305 specifies a response
25 signal associated with the calculated time zone in the communication history information 312 stored in the communication history information storage unit 310.

[0132]

A description will be provided for effects obtained by the

communication destination determination device 311 according to the present example embodiment in the case of the communication history information 316. In accordance with the communication destination determination device 311 according to the present example embodiment, it is possible to efficiently detect a suspicious communication destination 104 as a threat. The reason for this is as follows. For example, when the communication destination transmits a request signal in a specific time zone, it is possible to select a non-transmitted response signal on the basis of the time zone. That is, for example, even though there are a plurality of communication destinations, when the communication destinations perform a process for transmitting a request signal in the specific time zone, it is possible to efficiently detect a suspicious communication destination as a threat on the basis of the time zone in accordance with the communication destination determination device 311 according to the present example embodiment.

[0133]

The communication history information may be information obtained by combining at least two of the communication history information illustrated in Fig. 11 to Fig. 15 with one another.

[0134]

According to the communication destination determination device 311, it is further possible to detect a further suspicious communication destination 104 as a threat, in addition to the aforementioned effects. The reason for this is because the configuration of the communication destination determination device 311 include the configuration of the communication destination determination device 311 according to the first

example embodiment.

[0135]

(Hardware Configuration Example)

A configuration example of hardware resources that realize
5 the communication destination determination device according to
each example embodiment of the present invention will be
described. However, the communication destination
determination device may be realized using physically or
functionally at least two calculation processing devices. Further,
10 the communication destination determination device may be
realized as a dedicated apparatus.

[0136]

Fig. 16 is a block diagram schematically illustrating a
hardware configuration of a calculation processing device capable
15 of realizing the communication destination determination device
according to the first to third example embodiments of the present
invention. A calculation processing device 20 includes a central
processing unit (CPU) 21, a memory 22, a disk 23, a non-transitory
recording medium 24, a communication interface (hereinafter,
20 expressed as. "communication I/F") 27 and a display 28. The
calculation processing device 20 may connect an input device 25
and an output device 26. The calculation processing device 20
can execute transmission/reception of information to/from another
calculation processing device and a communication apparatus via
25 the communication I/F 27.

[0137]

The non-transitory recording medium 24 is, for example, a
computer-readable Compact Disc, Digital Versatile Disc. The
non-transitory recording medium 24 may be Universal Serial Bus

(USB) memory, Solid State Drive or the like. The non-transitory recording medium 24 allows a related program to be holdable and portable without power supply. The non-transitory recording medium 24 is not limited to the above-described media. Further, a related program can be carried via a communication network by way of the communication I/F 27 instead of the non-transitory recording medium 24.

[0138]

In other words, the CPU 21 copies, on the memory 22, a software program (a computer program: hereinafter, referred to simply as a “program”) stored by the disk 23 when executing the program and executes arithmetic processing. The CPU 21 reads data necessary for program execution from the memory 22. When display is needed, the CPU 21 displays an output result on the display 28. When a program is input from the outside, the CPU 21 reads the program from the input device 25. The CPU 21 interprets and executes an communication destination determination program (Fig. 2, Fig. 6, or Fig. 10) present on the memory 22 corresponding to a function (processing) indicated by each unit illustrated in Fig. 1, Fig. 5, or Fig. 9 described above. The CPU 21 sequentially executes the processing described in each example embodiment of the present invention.

[0139]

In other words, in such a case, it is conceivable that the present invention can also be made using the communication destination determination program. Further, it is conceivable that the present invention can also be made using a computer-readable, non-transitory recording medium storing the communication destination determination program.

[0140]

The present invention has been described using the above-described example embodiments as example cases. However, the present invention is not limited to the
 5 above-described example embodiments. In other words, the present invention is applicable with various aspects that can be understood by those skilled in the art without departing from the scope of the present invention.

[0141]

10 This application is based upon and claims the benefit of priority from Japanese patent application No. 2015-178305, filed on September 10, 2015, the disclosure of which is incorporated herein in its entirety.

15 [Reference signs List]

[0142]

	101	communication destination determination device
	102	signal transmission unit
	103	communication destination determination unit
20	104	communication destination
	205	history specifying unit
	206	signal selection unit
	207	history update unit
	208	communication destination determination device
25	209	signal information
	210	communication history information
	305	history specifying unit
	307	history update unit
	310	communication history information storage unit

	311	communication destination determination device
	312	communication history information
	313	communication history information
	314	communication history information
5	315	communication history information
	316	communication history information
	20	calculation processing device
	21	CPU
	22	memory
10	23	disk
	24	non-transitory recording medium
	25	input device
	26	output device
	27	communication IF
15	28	display

[Document Name] CLAIMS

[Claim 1]

A communication destination determination device comprising:

5 signal transmission means for transmitting a second signal in response to a first signal to a communication destination when the first signal is received from the communication destination via a communication network; and

10 communication destination determination means for determining whether or not the communication destination is suspicious as a threat on a basis of whether or not a third signal transmitted from the communication destination is received within a certain time period after a timing of transmission of the second signal.

15 [Claim 2]

The communication destination determination device according to claim 1, further comprising:

20 history specifying means for reading a signal from communication history information including the second signal transmitted to the communication destination when the first signal is received from the communication destination;

25 signal selection means for selecting a signal different from the signal read by the history specifying means from signal information including a signal transmittable to the communication destination; and

 history update means for adding the second signal transmitted by the signal transmission means to the communication history information, wherein

 the signal transmission means transmits the signal selected

by the signal selection means to the communication destination as the second signal.

[Claim 3]

The communication destination determination device
5 according to claim 2, further comprising:

history information storage means capable of storing the communication history information including communication information in which a communication destination identifier, which is able to identify the communication destination, and the
10 second signal, which has been transmitted to the communication destination, are associated with each other, wherein,

when a fourth signal is received from a certain communication destination, the history specifying means specifies a signal associated with a communication destination identifier
15 indicating the certain communication destination in the communication history information,

the signal selection means selects a signal different from the signal specified by the history specifying means from the signal information, and

20 the history update means generates communication information in which a communication destination identifier, which has been transmitted by the signal transmission means and indicates the communication destination, and the second signal, which has been transmitted by the signal transmission means, are
25 associated with each other, and adds the generated communication information to the communication history information.

[Claim 4]

The communication destination determination device according to claim 2, further comprising:

history information storage means capable of storing the communication history information including communication information in which a time zone, in which the first signal has been received, and the second signal, which has been transmitted
5 with respect to the first signal, are associated with each other, wherein,

when a fourth signal is received in a certain time zone, the history specifying means specifies a signal associated with the certain time zone in the communication history information,

10 the signal selection means selects a signal different from the signal specified by the history specifying means from the signal information, and

the history update means generates communication information in which the certain time zone, and the second signal,
15 which has been transmitted by the signal transmission means, are associated with each other, and adds the generated communication information to the communication history information.

[Claim 5]

The communication destination determination device
20 according to claim 2, further comprising:

history information storage means capable of storing the communication history information including communication information in which a time zone, in which the first signal has been received from the communication destination, a
25 communication destination identifier, which is able to identify the communication destination, and the second signal, which has been transmitted in response to the first signal, are associated with each other, wherein,

when a fourth signal is received from a communication

destination indicated by a certain communication destination identifier in a certain time zone, the history specifying means specifies a signal associated with the certain communication destination identifier and the certain time zone in the communication history information,

the signal selection means selects a signal different from the signal specified by the history specifying means from the signal information, and

the history update means generates communication information in which the certain communication destination identifier, the certain time zone, and the second signal, which has been transmitted by the signal transmission means, are associated with each other, and adds the generated communication information to the communication history information.

[Claim 6]

A communication destination determination device comprising:

signal transmission means for transmitting a second signal in response to a first signal requiring certain information to a first communication destination when the first signal is received from the first communication destination via a communication network; and

communication destination determination means for determining that at least one of the first communication destination and a second communication destination is suspicious as a threat when a third signal requiring the certain information is received from the second communication destination within a certain time period after a timing of transmission of the second signal.

[Claim 7]

The communication destination determination device according to claim 6, further comprising:

history specifying means for reading a signal from
5 communication history information including the second signal transmitted when the first signal is received;

signal selection means for selecting a signal different from the signal read by the history specifying means from signal information including a signal in response to the first signal; and

10 history update means for adding the second signal transmitted by the signal transmission means to the communication history information, wherein

the signal transmission means transmits the signal selected by the signal selection means as the second signal.

15 [Claim 8]

The communication destination determination device according to claim 7, further comprising:

history information storage means capable of storing the communication history information including communication
20 information in which an information identifier, which is able to identify the certain information requested by the first signal, and the second signal, which has been transmitted in response to the first signal, are associated with each other, wherein,

when a fourth signal requiring information indicated by a
25 specific information identifier is received, the history specifying means specifies a signal associated with the specific information identifier in the communication history information,

the signal selection means selects a signal different from the signal specified by the history specifying means from the

signal information, and

the history update means generates communication information in which the specific information identifier and the second signal, which has been transmitted by the signal
5 transmission means, are associated with each other, and adds the generated communication information to the communication history information.

[Claim 9]

A communication destination determination comprising:

10 signal transmission means for transmitting a second signal in response to a first signal to a first communication destination when the first signal is received from the first communication destination via a port through which communication connection with a communication network is performed; and

15 communication destination determination means for determining that at least one of the first communication destination and a second communication destination is suspicious as a threat when a third signal is received from the second communication destination via the port within a certain time
20 period after a timing of transmission of the second signal.

[Claim 10]

The communication destination determination device according to claim 9, further comprising:

history specifying means for reading a signal from
25 communication history information including the second signal transmitted when the first signal is received;

signal selection means for selecting a signal different from the signal read by the history specifying means from signal information including a signal in response to the first signal; and

history update means for adding the second signal transmitted by the signal transmission means to the communication history information, wherein

the signal transmission means transmits the signal selected
5 by the signal selection means as the second signal.

[Claim 11]

The communication destination determination device according to claim 10, further comprising:

history information storage means capable of storing the
10 communication history information including communication information in which a port identifier, which is able to identify the port via which the first signal is received, and the second signal, which has been transmitted in response to the first signal, are associated with each other, wherein,

15 when a fourth signal is received via a port indicated by a certain port identifier, the history specifying means specifies a signal associated with the certain port identifier in the communication history information,

the signal selection means selects a signal different from
20 the signal specified by the history specifying means from the signal information, and

the history update means generates communication information in which the certain port identifier and the second signal, which has been transmitted by the signal transmission means, are associated with each other, and adds the generated
25 communication information to the communication history information.

[Claim 12]

A communication destination determination comprising:

signal transmission means for transmitting a second signal in response to a first signal to a first communication destination when the first signal is received from the first communication destination via a communication network; and

5 communication destination determination means for specifying a first device via which communication with the first communication destination is performed and a second device via which communication with a second communication destination is performed when a third signal is received from the second
10 communication destination within a certain time period after a timing of transmission of the second signal, and determines that at least one of the first communication destination and the second communication destination is suspicious as a threat when the first device and the second device coincide with each other.

15 [Claim 13]

The communication destination determination device according to claim 12, further comprising:

history specifying means for reading a signal from communication history information including the second signal
20 transmitted when the first signal is received;

signal selection means for selecting a signal different from the signal read by the history specifying means from signal information including a signal in response to the first signal; and

history update means for adding the second signal
25 transmitted by the signal transmission means to the communication history information, wherein

the signal transmission means transmits the signal selected by the signal selection means as the second signal.

[Claim 14]

The communication destination determination device according to claim 13, further comprising:

history information storage means capable of storing the communication history information including communication
5 information in which a device identifier, which is able to identify the first device via which communication with the first communication destination is performed, and the second signal, which has been transmitted to the first communication destination, are associated with each other, wherein

10 the history specifying means specifies a signal associated with a certain device identifier indicating a device via which communication with a third communication destination having received a fourth signal is performed in the communication history information,

15 the signal selection means selects a signal different from the signal specified by the history specifying means from the signal information, and

the history update means generates communication information in which the certain device identifier and the second
20 signal, which has been transmitted by the signal transmission means, are associated with each other, and adds the generated communication information to the communication history information.

[Claim 15]

25 The communication destination determination device according to any one of claim 2 to claim 5, claim 7, claim 8, claim 10, claim 11, claim 13, or claim 14, wherein

the signal transmission means does not transmit the second signal when the signal selection means determines that the signal

different from the signal specified by the history specifying means is not included in the signal information.

[Claim 16]

A communication destination determination method
5 comprising:

transmitting a second signal in response to a first signal to a communication destination when the first signal is received from the communication destination via a communication network; and

determining whether or not the communication destination
10 is suspicious as a threat on a basis of whether or not a third signal transmitted from the communication destination is received within a certain time period after a timing of transmission of the second signal.

[Claim 17]

15 A recoding medium storing a communication destination determination program recorded therein, the program making a computer achieve:

a signal transmission function for transmitting a second signal in response to a first signal to a communication destination
20 when the first signal is received from the communication destination via a communication network; and

a communication destination determination function for determining whether or not the communication destination is suspicious as a threat on a basis of whether or not a third signal
25 transmitted from the communication destination is received within a certain time period after a timing of transmission of the second signal.