

CLAIMS

1. An information processing device comprising:
 - an access log collection unit that collects access logs when a client terminal requests a content from a web server;
 - a database in which a malicious URL is registered in advance; ~~and~~
 - a falsification detection unit that collates a connection destination URL corresponding to a connection destination of the client terminal with the database and detects falsification of the content if the connection destination URL matches the malicious URL, and
 - an access verification unit that, if the connection destination URL matches the malicious URL, makes a direct request of an access source URL extracted from the access log to the web server and compares the access source URL with the connection destination URL at a time of the direct request being made,
 - wherein the falsification detection unit detects falsification of the content when the access source URL and the connection destination URL at the time of the direct request being made match each other based on a comparison by the access verification unit.

2. The information processing device according to claim 1, comprising a log extraction unit that extracts, from the access logs collected by the access log collection unit, an access log in which an access source URL corresponding to a request destination of the content and the connection destination URL do not match each other.

3. The information processing device according to claim 1, comprising a falsification notification unit that, if the falsification is detected, notifies occurrence of the falsification to an administrator of the web server corresponding to the content in which the falsification is detected.

~~4. The information processing device according to claim 1, comprising an access verification unit that, if the connection destination URL matches the malicious URL, makes a direct request of an access source URL extracted from the access log to the web server and compares the access source URL with the connection destination URL at a time of the direct request being made, wherein~~
~~the falsification detection unit detects~~
~~falsification of the content when the access source URL and the connection destination URL at the time of the direct request being made match each other based on a comparison~~

~~by the access verification unit.~~

~~54.~~ The information processing device according to claim 1, wherein

an unclassified URL that does not match a URL registered in the database is extracted from the access logs collected,

a benign URL is registered in advance together with the malicious URL in the database, and

the information processing device comprises a URL analysis unit that analyzes whether the unclassified URL is a malicious URL and registers the unclassified URL as the benign URL or the malicious URL.

~~65.~~ The information processing device according to claim 1, wherein

a benign URL is registered in advance together with the malicious URL in the database, and

the falsification detection unit detects falsification of the content if an access source URL matches the benign URL, whereas the connection destination URL matches the malicious URL, and a URL category shifts from benign to malicious.

~~76.~~ An information processing method comprising:

a step of collecting access logs when a client terminal requests a content from a web server;

a step of registering a malicious URL in database in advance; and

a step of collating a connection destination URL corresponding to a connection destination of the client terminal with the database and detecting falsification of the content if the connection destination URL matches the malicious URL,

wherein if the connection destination URL matches the malicious URL, a direct request of an access source URL extracted from the access log to the web server is made and the access source URL is compared with the connection destination URL at a time of the direct request being made, and

wherein falsification of the content is detected when the access source URL and the connection destination URL at the time of the direct request being made match each other based on a comparison.

87. A computer-readable storage medium storing a program for causing a computer to execute processing comprising:

collecting access logs when a client terminal requests a content from a web server;

registering a malicious URL in database in advance;

and

collating a connection destination URL corresponding to a connection destination of the client terminal with the database and detecting falsification of the content if the connection destination URL matches the malicious URL,

wherein if the connection destination URL matches the malicious URL, a direct request of an access source URL extracted from the access log to the web server is made and the access source URL is compared with the connection destination URL at a time of the direct request being made,
and

wherein falsification of the content is detected when the access source URL and the connection destination URL at the time of the direct request being made match each other based on a comparison.