CLAIMS:

1. A file leak detection method, characterized by comprising:

acquiring a file operation event on a terminal device, wherein the file operation event is an event for performing a specified operation on a target file;

extracting, from the file operation event, a file path of the target file which the file operation event involves;

searching for file content of the target file in accordance with the file path, and performing a mapping process on the file content of the target file to obtain a file fingerprint of the target file, wherein the file fingerprint uniquely identifies the file content of the target file;

determining whether the target file belongs to specified file libraries in accordance with the file path and the file fingerprint, wherein the specified file libraries are used for dynamically maintaining business files that need to be protected; and

determining that a file in the specified file libraries is being leaked, if the target file belongs to the specified file libraries.

2. The method according to claim 1, characterized in that the determining whether the target file belongs to specified file libraries in accordance with the file path and the file fingerprint comprises:

determining whether the file path is contained in an index information library; wherein the index information library stores a file path and a file fingerprint of at least one file in the specified file libraries;

determining that the target file belongs to the specified file libraries, if the file path is contained in the index information library;

determining whether the file fingerprint is contained in the index information library, if the file path is not contained in the index information library; and

determining that the target file belongs to the specified file libraries, if the file fingerprint is contained in the index information library.

3. The method according to claim 2, characterized in that in a case wherein the file fingerprint is not contained in the index information library, the method further comprises:

determining whether the target file originates from preset file hosting platforms in accordance with whether a preset field is contained in the file path;

determining a first file library which is a file warehouse of an item to which the target file belongs, if the target file originates from the preset file hosting platforms;

determining whether the first file library belongs to the specified file libraries; and

determining that the target file belongs to the specified file libraries, if the first file library belongs to the specified file libraries.

4. The method according to claim 3, characterized in that in a case of determining that the first file library does not belong to the specified file libraries, the method further comprises:

determining whether a same-level file, a parent file of which is the same as that of the target file, originates from the preset file hosting platforms, in accordance with whether the preset field is contained in a same-level path which is a path of the same-level file;

determining a second file library which is a file warehouse of an item to which the same-level file

belongs, if the same-level file originates from the preset file hosting platforms;

determining whether the second file library belongs to the specified file libraries; and

determining that the target file belongs to the specified file libraries, if the second file library belongs to the specified file libraries.

5. The method according to claim 4, characterized in that in a case of determining that the second file library does not belong to the specified file libraries, the method further comprises:

determining whether at least one level of parent file of the target file originates from the preset file hosting platforms, in accordance with whether the preset field is contained in a parent path which is a path of the parent file;

determining a third file library which is a file warehouse of an item to which the parent file originating from the preset file hosting platforms belongs, if any level of the parent file originates from the preset file hosting platforms;

determining whether the third file library belongs to the specified file libraries; and

determining that the target file belongs to the specified file libraries, if the third file library belongs to the specified file libraries.

6. The method according to any one of claims 3 to 5, characterized in that the method further comprises:

adding the file path and the file fingerprint into the index information library, in a case of determining that the target file belongs to the specified file libraries.

7. The method according to any one of claims 1 to 5, characterized in that the method further comprises:

transmitting alarm information to a server, wherein the alarm information is used for indicating that a file in the specified file libraries is being leaked, in a case of determining that a file in the specified file libraries is being leaked.

8. The method according to any one of claims 1 to 5, characterized in that the method further comprises:

transmitting attribute information of the file operation event to a server, in a case of determining that a file in the specified file libraries is being leaked;

wherein the attribute information of the file operation event comprises at least one of identification information of the terminal device, identification information of the target file, and account information for logging in the terminal device.

9. The method according to any one of claims 1 to 5, characterized in that the method further comprises:

preventing the file operation event from being performed, in a case of determining that a file in the specified file libraries is being leaked.

10. A file leak detection apparatus, characterized by comprising:

a detecting unit configured to acquire a file operation event on a terminal device, wherein the file operation event is an event for performing a specified operation on a target file;

an extracting unit configured to extract, from the file operation event, a file path of the target file which the file operation event involves;

an acquiring unit configured to search for file content of the target file in accordance with the file path, and perform a mapping process on the file content of the target file to obtain a file fingerprint of the target file, wherein the file fingerprint uniquely identifies the file content of the target file;

a determining unit configured to determine whether the target file belongs to specified file libraries in accordance with the file path and the file fingerprint, wherein the specified file libraries are used for dynamically maintaining business files that need to be protected; and

a processing unit configured to determine that a file in the specified file libraries is being leaked, if the target file belongs to the specified file libraries.

11. An electronic device, characterized by comprising: a memory configured to store a computer program and a processor configured to, when executes the computer program, cause the electronic device to implement the file leak detection method according to any one of claims 1 to 9.

12. A computer-readable storage medium characterized by having stored thereon a computer program which, when executed by a computing device, causes the computing device to implement the file leak detection method according to any one of claims 1 to 9.