

[CLAIMS]

[Claim 1]

An access management system that manages access to an electronic file stored in a file sharing server, the access management system comprising:

a file access information receiving unit that receives, from a user device, file identification information identifying the electronic file to be accessed by the user device;

a restriction information receiving unit that receives restriction information indicating a restriction imposed by the file sharing server on access, by the user device, to the electronic file that is identified by the file identification information received by the file access information receiving unit and is stored in the file sharing server; and

an access control information transmitting unit that transmits, to the user device, access control information that is for controlling access to the electronic file in the user device and corresponds to the restriction information.

[Claim 2]

The access management system according to Claim 1, wherein

the restriction information includes information indicating a user whose access to the electronic file is permitted or prohibited by the file sharing server,

the file access information receiving unit receives, from the user device, the file identification information and user identification information identifying a user of the user device, and

the access control information transmitting unit transmits the access control information to the user device when it is determined, based on the user identification information and the restriction information, that the user of the user device is accessible to the electronic file stored in the file sharing server.

[Claim 3]

The access management system according to Claim 2, wherein

the file sharing server stores therein an encrypted electronic file,

the access management system further comprises a key information storage unit that stores therein, in association with each other, the file identification information and a file decryption key required for decryption of the encrypted electronic file, and

the access control information transmitting unit transmits, to the user device, the file decryption key stored in the key information storage unit when it is determined that the user of the user device is accessible to the electronic file stored in the file sharing server.

[Claim 4]

The access management system according to Claim 2 or 3, wherein  
the restriction information includes information indicating operation on the electronic file that is permitted or prohibited by the file sharing server for a user to perform, and  
the access control information transmitting unit generates, based on the restriction information, information indicating operation on the electronic file that the user of the user device should be permitted to perform or prohibited from performing and transmits the information to the user device when it is determined that the user of the user device is accessible to the electronic file stored in the file sharing server.

[Claim 5]

The access management system according to Claim 4, wherein  
the operation includes at least one of: operation of viewing the electronic file; operation of editing the electronic file; operation of printing the electronic file; operation of saving the electronic file, operation of copying data included in the electronic file; and operation of capturing a display screen of the electronic file.

[Claim 6]

The access management system according to any one of Claims 1 to 5, wherein the user device transmits, to the access management system, the file identification information when opening the electronic file downloaded from the file sharing server.

[Claim 7]

The access management system according to Claim 6, wherein  
the file identification information is embedded in the electronic file, and  
the user device transmits, to the access management system, the file identification information embedded in the electronic file downloaded from the file sharing server.

[Claim 8]

The access management system according to any one of Claims 1 to 7, further comprising a restriction specifying information storage unit that stores therein, in association with each other: restriction specifying information for specifying a restriction imposed on access to the electronic file imposed by the file sharing server; and the file identification information, wherein

the restriction information receiving unit receives the restriction information from the file sharing server based on the restriction specifying information stored in the restriction specifying information storage unit in association with the file identification information received by the file access information receiving unit.

[Claim 9]

The access management system according to Claim 8, further comprising:

a monitoring unit that monitors an electronic file stored in a predetermined folder in the file sharing server;

a file processing unit that: acquires a newly stored electronic file from the file sharing server when the monitoring unit determines that the electronic file is newly stored in the predetermined folder in the file sharing server; and embeds, in the electronic file, file identification information identifying the electronic file;

a file storage control unit that causes the file sharing server to store therein an electronic file in which the file identification information is embedded; and

a restriction specifying information storage control unit that causes the restriction specifying information storage unit to store therein, in association with each other: information identifying an electronic file that is stored in the file sharing server and in which the file identification information is embedded; and the file identification information.

[Claim 10]

The access management system according to Claim 9, wherein

when an electronic file is newly stored in the predetermined folder in the file sharing server, the file processing unit encrypts the electronic file, and embeds the file identification information in the encrypted electronic file, and

the restriction specifying information storage unit stores therein, in association with each other, the restriction specifying information, the file identification information, and a file decryption key required for decryption of the encrypted electronic file.

[Claim 11]

The access management system according to Claim 10, further comprising a data converting unit that:

acquires, from the file sharing server, the encrypted electronic file stored in the file sharing server;

decrypts the encrypted electronic file by using the file decryption key;

converts the decrypted electronic file into data for display; and

transmits the data for display to the file sharing server.

[Claim 12]

The access management system according to any one of Claims 1 to 7, wherein

the restriction information receiving unit receives from the file sharing server the restriction information indicating a restriction imposed by the file sharing server on access to the electronic file that is identified by the file identification information stored in the file sharing server.

[Claim 13]

A file access system comprising:  
the access management system according to any one of Claims 1 to 12; and  
the user device.

[Claim 14]

The file access system according to Claim 13, wherein the user device has:  
an encrypting unit that encrypts an electronic file by including file identification information identifying the electronic file to be encrypted;  
a file storage control unit that causes the file sharing server to store therein the encrypted electronic file; and  
a storage control unit that causes the access management system to store therein, in association with each other: restriction specifying information for specifying a restriction imposed by the file sharing server on access to the encrypted electronic file stored in the file sharing server; the file identification information; and a file decryption key required for decryption of the encrypted electronic file.

[Claim 15]

A program for causing a computer to function as the access management system according to any one of Claims 1 to 12.

[Claim 16]

An encrypting apparatus comprising:  
an encrypting unit that encrypts an electronic file by including file identification information identifying the electronic file to be encrypted;  
a file storage control unit that causes a file sharing server to store therein the encrypted electronic file; and  
a storage control unit that causes an external server to store therein, in association with each other: restriction specifying information for specifying a restriction imposed by the file sharing server on access to the encrypted electronic file stored in the file sharing server; the file identification information; and a file decryption key required for decryption of the encrypted electronic file.

[Claim 17]

An encrypting apparatus comprising:  
an encrypting unit that encrypts an electronic file by including file identification information identifying the electronic file to be encrypted;  
a file storage control unit that causes a file sharing server to store therein the encrypted electronic file; and  
a storage control unit that causes an external server to store therein, in association with each other: restriction specifying information for the external server to receive from the file

sharing server a restriction information indicating a restriction imposed by the file sharing server on access to the encrypted electronic file stored in the file sharing server; the file identification information; and a file decryption key required for decryption of the encrypted electronic file.

[Claim 18]

A program for causing a computer to function as the encrypting apparatus according to Claim 16 or 17.