

[Document Name] SPECIFICATION

[Title of Invention] ACCESS CONTROL APPARATUS, CONTROL METHOD,
AND NON-TRANSITORY COMPUTER READABLE MEDIUM~~PROGRAM~~

[Technical Field]

5 [0001]

The present invention relates to data sharing.

[Background Art]

[0002]

10 Data sharing has been performed by storing data in a storage apparatus accessible from a plurality of terminals. As one of storage apparatuses for use in such data sharing, a blockchain storage achieved by using a blockchain technique is known. For example, Patent Document 1 discloses sharing information pertaining to an event that has occurred in a terminal by storing the information in a blockchain storage.

15 [Related Document]

[Patent Document]

[0003]

[Patent Document 1] Japanese Patent Application Publication No. 2018-081464

[Disclosure of the Invention]

20 [Technical Problem]

[0004]

A blockchain storage has an advantage that it is difficult to tamper stored data. On the other hand, since it is also difficult to delete stored data from a blockchain storage, once data (e.g., personal information) that the owner may desire to delete later is stored in the blockchain storage, it may be difficult to handle the data when the owner desires to delete the data.

25 [0005]

The present invention has been made in view of the above-described problem, and one of objects of the present invention is to provide a technique for utilizing a blockchain storage, while enabling data deletion.

30 [~~Solution to Problem~~Summary]

[0006]

An access control apparatus according to a first aspect of the present invention-disclosure includes 1) a request acquisition unit that acquires a request for access to data stored in a

35

first storage apparatus, 2) a privilege information acquisition unit that acquires, from a second storage apparatus in which privilege information representing access privilege pertaining to access to the first storage apparatus is stored, the privilege information, 3) a privilege determination unit that determines whether the access is within a range of the access privilege of a target entity being a subject of the request, by using the privilege information of the target entity, and 4) an access execution unit that executes the access, when the access is determined to be within a range of the access privilege of the target entity. The second storage apparatus is a blockchain storage.

[0007]

A control method according to a second aspect of the present invention-disclosure is executed by a computer. The control method includes 1) a request acquisition step of acquiring a request for access to data stored in a first storage apparatus, 2) a privilege information acquisition step of acquiring, from a second storage apparatus in which privilege information representing access privilege pertaining to access to the first storage apparatus is stored, the privilege information, 3) a privilege determination step of determining whether the access is within a range of the access privilege of a target entity being a subject of the request, by using the privilege information of the target entity, and 4) an access execution step of executing the access, when the access is determined to be within a range of the access privilege of the target entity. The second storage apparatus is a blockchain storage.

[0008]

A non-transitory computer readable medium storing a program according to a third aspect of the present invention-disclosure causes a computer to execute the control method according to the ~~present invention~~second aspect.

[Advantageous Effects of Invention]

[0009]

The present invention provides a technique for utilizing a blockchain storage, while enabling data deletion.

[Brief Description of the Drawings]

[0010]

[Fig. 1] Fig. 1 is a diagram conceptually illustrating an operation of an access control apparatus according to an example embodiment 1.

[Fig. 2] Fig. 2 is a block diagram illustrating a functional configuration of

Therefore, the requested access is determined to be within the range of the access privilege of the insurance company C. Then, the access execution unit 2080 reads, from the partial area 32 of the user 110, a face image of the user 110.

[0067]

5 The access control apparatus 2000 collates a face image acquired from the store terminal 120 (face image acquired by capturing the user 110 at the store S) with a face image acquired from the partial area 32 (determines whether the face images indicate a same person). When the face images are determined to indicate a same person, personal information stored in the partial area 32 can be
10 said to be legitimate personal information of the user 110. In view of the above, the access control apparatus 2000 acquires personal information of the user 110 from the partial area 32 of the user 110, and provides the personal information to the store terminal 120. On the other hand, when the face images are determined not to indicate a same person, the access control apparatus 2000 transmits, to the
15 store terminal 120, an error notification that authentication has failed. Note that, an existing method can be used as a method of determining whether two face images indicate a same person. For example, the access control apparatus 2000 computes a similarity between two face images, and compares the similarity with a predetermined threshold value. In a case where the similarity is equal to or
20 more than the predetermined threshold value, the two face images are determined to indicate a same person, and in a case where the similarity is less than the predetermined threshold value, the two face images are determined not to indicate a same person.

[0068]

25 When personal information of the user 110 is acquired from the access control apparatus 2000, the store terminal 120 determines whether personal information provided from the user 110 matches the personal information provided from the access control apparatus 2000 (i.e., personal information read from the partial area 32 of the user 110). When these pieces of information
30 match each other, the store terminal 120 determines that the personal information provided from the user 110 at the store S is legitimate. Specifically, it is possible to confirm that the user 110 who visited the store S of the insurance company S is a person himself or herself.

[0069]

from the first storage apparatus.

11. The control method according to any one of supplementary notes 7 to 10, in which

a partial storage area is allocated for each user in the first storage

5 apparatus, and

the privilege information representing access privilege of an entity with respect to the partial storage area is stored in the second storage apparatus in association with a combination of identification information of the entity, and identification information of the partial storage area.

10 12. The control method according to supplementary note 11, in which

authentication information and personal information of a first user are stored in the partial storage area of the first user,

the control method further including, in the access execution step, storing confirmation information representing a result of confirmation in the partial
15 storage area, when authentication of the first user is successful, and it is confirmed that the personal information of the first user is legitimate.

13. A program causing a computer to execute the control method according to any one of supplementary notes 7 to 12.

[Reference signs List]

20 [0093]

10 Target entity

20 Request

30 First storage apparatus

32 Partial area

25 40 Second storage apparatus, blockchain storage

70 Privilege information

100 Table

102 Entity identification information

104 Object identification information

30 110 User

120 Store terminal

1000 Computer

1020 Bus

1040 Processor

[Document Name] CLAIMS

[Claim 1]

An access control apparatus comprising:

5 a request acquisition unit that acquires a request for access to data stored in a first storage apparatus;

a privilege information acquisition unit that acquires, from a second storage apparatus in which privilege information representing access privilege pertaining to access to the first storage apparatus is stored, the privilege information;

10 a privilege determination unit that determines whether the access is within a range of the access privilege of a target entity being a subject of the request, by using the privilege information of the target entity; and

an access execution unit that executes the access, when the access is determined to be within a range of the access privilege of the target entity,

15 wherein

the second storage apparatus is a blockchain storage.

[Claim 2]

The access control apparatus according to claim 1, wherein

20 authentication information of a user is stored in the first storage apparatus,

the access indicated by the request includes reading of the authentication information of a user,

25 the request includes authentication information of a user to be authenticated, and

the access execution unit performs authentication of the user to be authenticated by comparing the authentication information included in the request with the authentication information read by access to the first storage apparatus.

30

[Claim 3]

The access control apparatus according to claim 2, wherein

the authentication information is biometric information.

[Claim 4]

The access control apparatus according to claim 2 or 3, wherein
the access execution unit outputs a notification representing a result of
the authentication, and

5 the notification does not include authentication information acquired
from the first storage apparatus.

[Claim 5]

10 The access control apparatus according to any one of claims 1 to 4,
wherein

a partial storage area is allocated for each user in the first storage
apparatus, and

15 the privilege information representing access privilege of an entity with
respect to the partial storage area is stored in the second storage apparatus in
association with a combination of identification information of the entity and
identification information of the partial storage area.

[Claim 6]

20 The access control apparatus according to claim 5, wherein
authentication information and personal information of a first user are
stored in the partial storage area of the first user, and

25 the access execution unit stores confirmation information representing a
result of confirmation in the partial storage area, when authentication of the first
user is successful, and it is confirmed that the personal information of the first
user is legitimate.

[Claim 7]

30 A control method to be executed by a computer, the method comprising:
a request acquisition step of acquiring a request for access to data stored
in a first storage apparatus;

a privilege information acquisition step of acquiring, from a second
storage apparatus in which privilege information representing access privilege
pertaining to access to the first storage apparatus is stored, the privilege
information;

a privilege determination step of determining whether the access is within a range of the access privilege of a target entity being a subject of the request, by using the privilege information of the target entity; and

an access execution step of executing the access, when the access is
5 determined to be within a range of the access privilege of the target entity, wherein

the second storage apparatus is a blockchain storage.

[Claim 8]

10 The control method according to claim 7, wherein

authentication information of a user is stored in the first storage
apparatus,

the access indicated by the request includes reading of the authentication
information of a user, and

15 the request includes authentication information of a user to be
authenticated,

the control method further including, in the access execution step,
performing authentication of the user to be authenticated by comparing the
authentication information included in the request with the authentication
20 information read by access to the first storage apparatus.

[Claim 9]

The control method according to claim 8, wherein

the authentication information is biometric information.

25

[Claim 10]

The control method according to claim 8 or 9, further comprising,

in the access execution step, outputting a notification representing a
result of the authentication, wherein

30 the notification does not include authentication information acquired
from the first storage apparatus.

[Claim 11]

The control method according to any one of claims 7 to 10, wherein

a partial storage area is allocated for each user in the first storage apparatus, and

the privilege information representing access privilege of an entity with respect to the partial storage area is stored in the second storage apparatus in
5 association with a combination of identification information of the entity, and identification information of the partial storage area.

[Claim 12]

The control method according to claim 11, wherein
10 authentication information and personal information of a first user are stored in the partial storage area of the first user,

the control method further including, in the access execution step, storing confirmation information representing a result of confirmation in the partial storage area, when authentication of the first user is successful, and it is
15 confirmed that the personal information of the first user is legitimate.

[Claim 13]

A non-transitory computer readable medium storing a program causing a computer to execute the control method according to any one of claims 7 to 12.

[Title of Invention] ACCESS CONTROL APPARATUS, CONTROL METHOD,
AND NON-TRANSITORY COMPUTER READABLE MEDIUM~~PROGRAM~~

[Document Name] ABSTRACT

An access control apparatus (2000) acquires a request (20) for access to
5 data stored in a first storage apparatus 30. The access control apparatus (2000)
acquires privilege information (70) from a blockchain storage (40). The
privilege information (70) represents access privilege pertaining to access to the
first storage apparatus (30). The access control apparatus (2000) determines
whether requested access is within a range of the access privilege of a target
10 entity (10) being a subject of the request (20), by using the privilege information
(70) of the target entity (10). When it is determined that the access is within
the range of the access privilege of the target entity (10), the access control
apparatus (2000) executes the access.

15 [FIG .1]