[CLAIMS]

1. A first management system for managing an IoT device that can be connected to a network, the first management system comprising:

managing device identification information for identifying the IoT device, device user identification information for identifying a user in the IoT device, and a setting in the IoT device for a user identified by the device user identification information; and

mapping the device identification information, the device user identification information, and the setting to each other, wherein

in a second system independent of the first management system and not managing the IoT device, user identification information for identifying a user and a password corresponding to the user identification information are managed,

the first management system comprising a first acquisition unit that acquires the device identification information, the user identification information, and the password from a terminal apparatus that has acquired the device identification information from the IoT device;

a first requesting unit that requests a server of the second system capable of authenticating a user based on the user identification information and the password for first authentication by using the user identification information

and the password acquired by the first acquisition unit;

a second acquisition unit that acquires the device user identification information, the user identification information, and the password from the terminal apparatus;

a second requesting unit that requests the server of the second system for second authentication by using the user identification information and the password acquired by the second acquisition unit;

a management unit that maps the user identification information, the device identification information, and the device user identification information to each other and manages the information accordingly, when the first authentication is provided and when the second authentication is provided; wherein

a total number of items of the user identification information that can be acquired by the first acquisition unit and the second acquisition unit is larger than a total number of items of the device user identification information that can be acquired by the second acquisition unit.

2. A management method comprising:

managing, by a first management system managing an IoT device connected to a network, device identification information for identifying the IoT device, device user identification information for identifying a user in the IoT

device, and a setting in the IoT device for a user identified by the device user identification information,

mapping, by the first management system, the device identification information, the device user identification information, and the setting to each other;

managing, by a second management system independent of the first management system and not managing the IoT device, user identification information for identifying a user and a password corresponding to the user identification information,

acquiring, by the first management system comprising a first acquisition unit, the device identification information, the user identification information, and the password from a terminal apparatus that has acquired the device identification information from the IoT device;

requesting, by a first requesting unit, a server of the second management system capable of authenticating a user based on the user identification information and the password for first authentication, wherein the user identification information and the password is acquired by the first acquisition unit;

acquiring, by a second acquisition unit, the device user identification information, the user identification information, and the password from the terminal apparatus;

requesting, by a second requesting unit, the server of the second management system for second authentication,

wherein the user identification information and the password is acquired by the second acquisition unit;

mapping and managing, by a management unit, when the first authentication is provided and when the second authentication is provided, the user identification information, the device identification information, and the device user identification information to each other; wherein

a total number of items of the user identification information that can be acquired by the first acquisition unit and the second acquisition unit is larger than a total number of items of the device user identification information that can be acquired by the second acquisition unit.