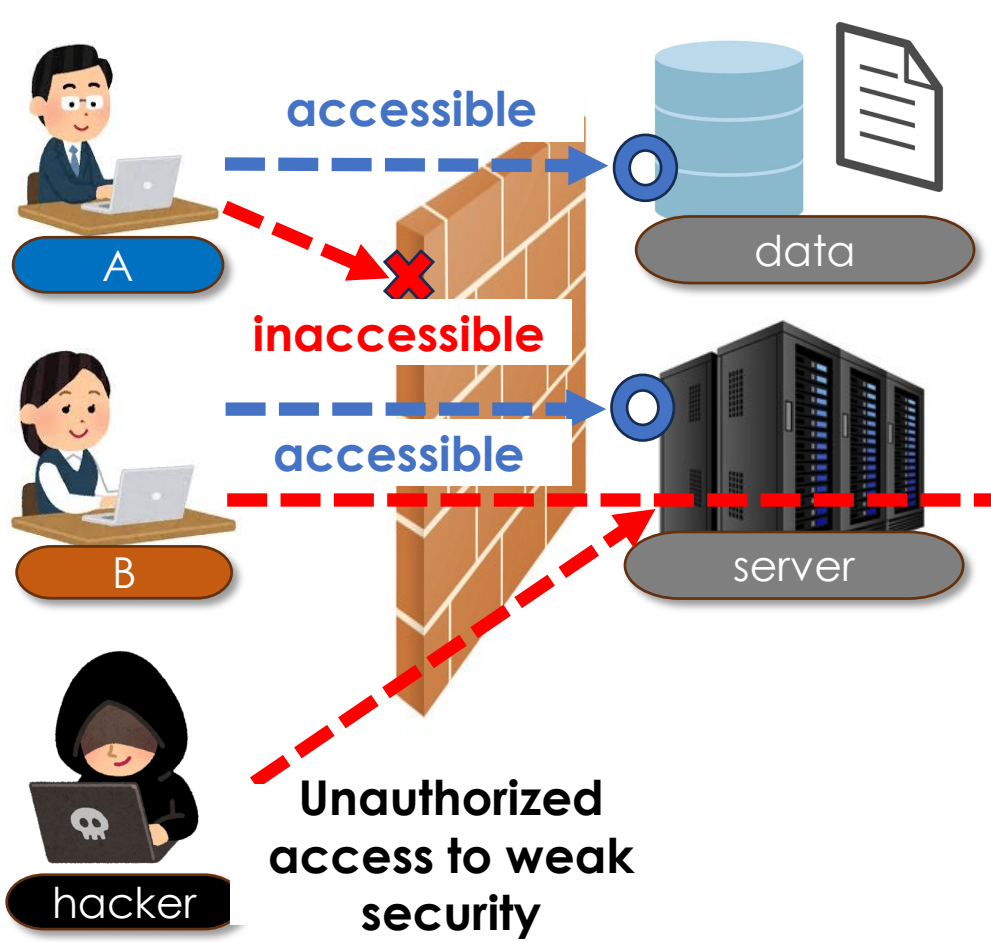
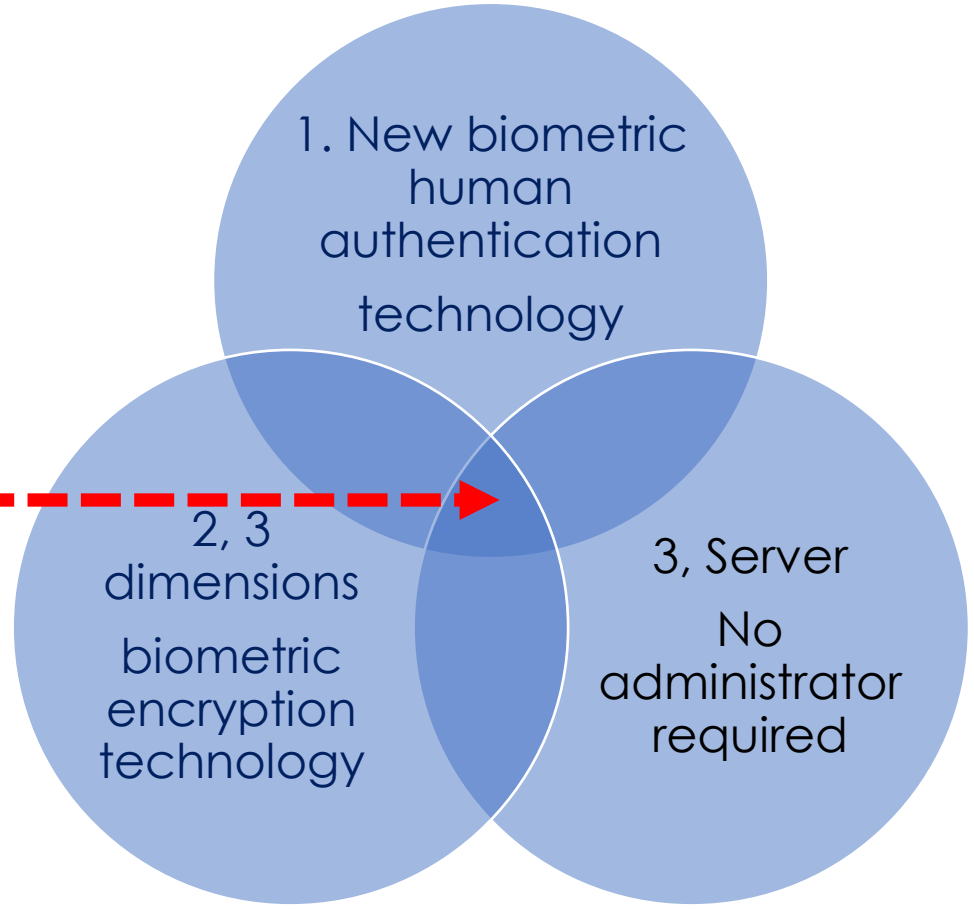
# 3D biometric cryptographic security

| Common access management | 3D biometric cryptography management |
|---|---|

**Protect your data with the "3D biometrics method" even if there is unauthorized access!**



# 1， New biometric authentication method

## Zero hacking risk for ID and password authentication

biometrics enhanced Personal authentication method

Safety equivalent to face-to-face

**Combined use of each method possible**

**ID password**

80% of hacking causes

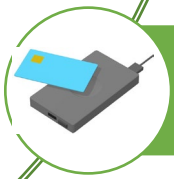
Forget
stolen
lose


Fingerprint authentication


Vein authentication

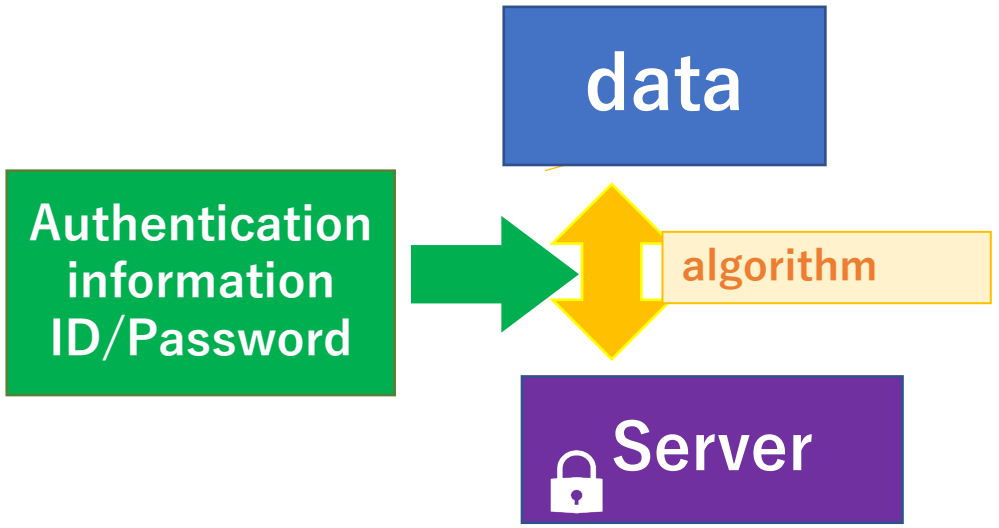

face authentication


voice authentication


IC card authentication

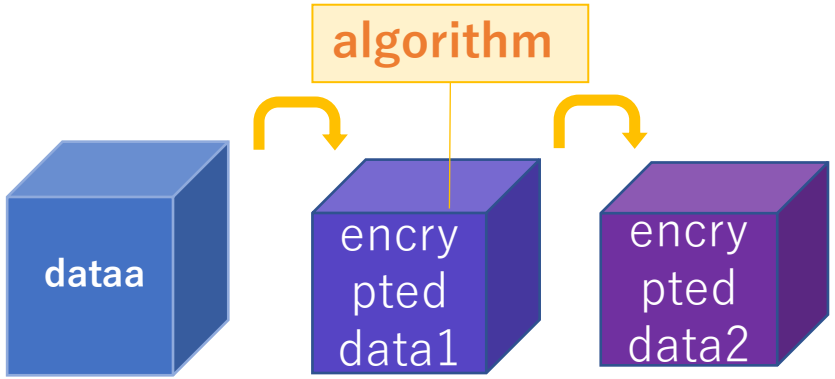
# 2， 3D biometric cryptography technology

## Common encryption




Authentication and encryption are performed by separate programs, each with its own strengths. Firewalls, blockchain, and other security systems are adamant that hackers can penetrate them.

## 3D biometric cryptography




A mechanism that protects data by integrating authentication and encryption

.1. Algorithm final processing encryption is unpredictable, it is impossible to decryption the code.

2. It is impossible to identify "Personal authentication information 1" and "Personal authentication information 2" are This information is only for the certifier's PC.

3. Even if someone other than the certifier takes out the data, the information becomes garbage, Block information leaks.

# 3， No server administrator required

## Common access management method

server administrator

server

administrator

If data is taken out, information will be leaked

ID password
Central management
Have a master key that allows access to the data.

Smartphone

## 3D biometric cryptography management method

No server administrator

server

administrator

Even if the data is taken out, it will be trash.

Engaged only in system operation; no master key

Smartphone