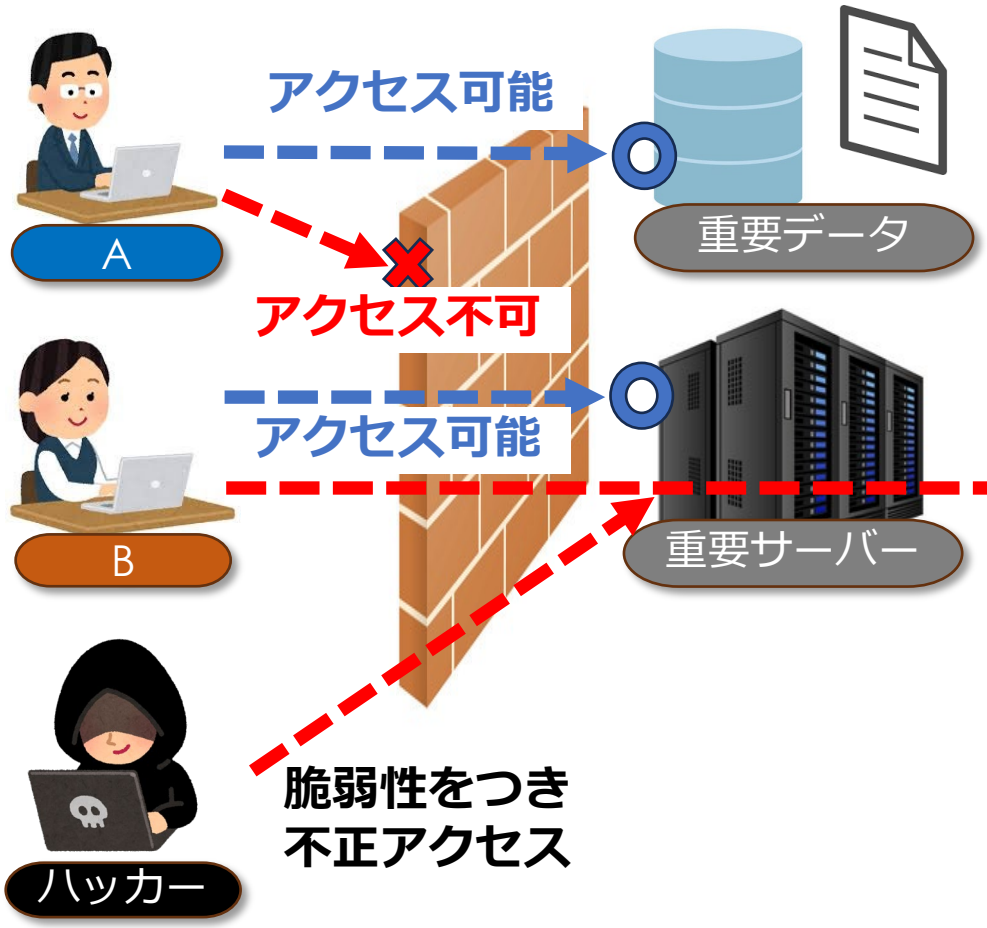
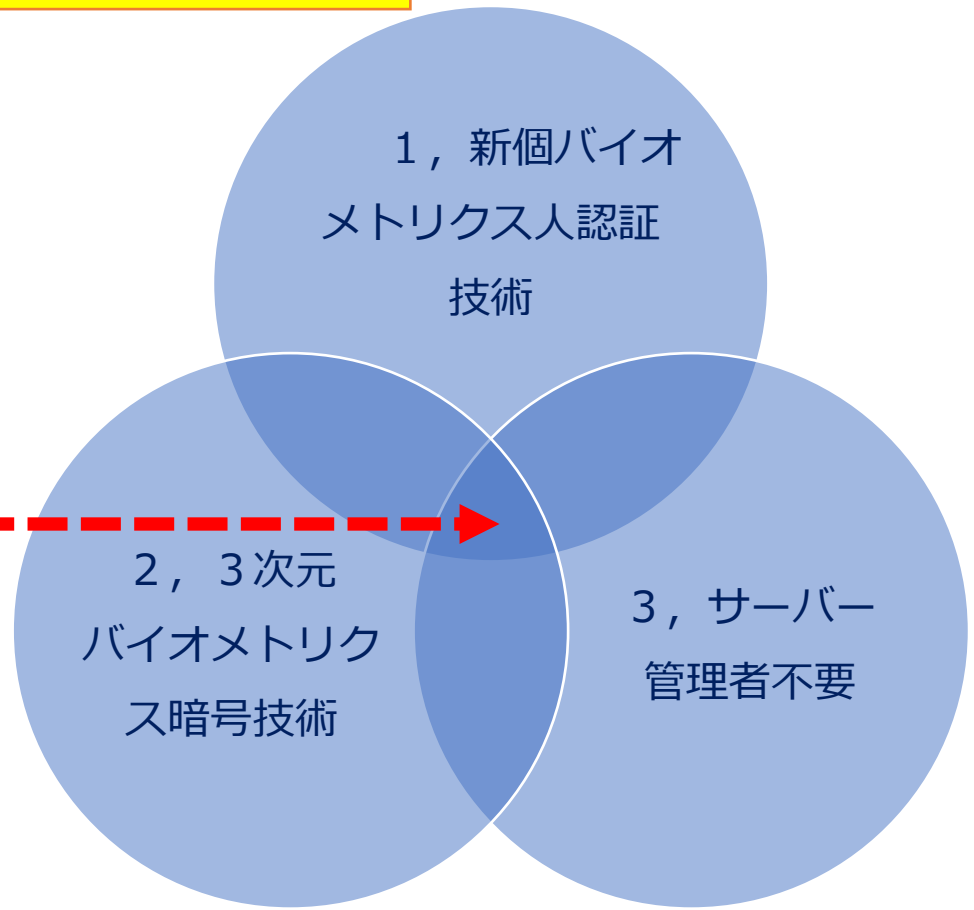
３次元バイオメトリクス暗号セキュリティ

一般的なアクセス管理

３次元バイオメトリクス暗号管理

不正アクセスがあっても「３次元バイオメトリクス方式」でデータを守る！





1，新・バイオメトリクス認証方式

ID,パスワード認証のハッキングリスクがゼロになる

バイオメトリクス
強化された
個人生体認証方式

フェーストゥフェース
と同等な安全性

各方式の複合使用可能

ID
パスワード

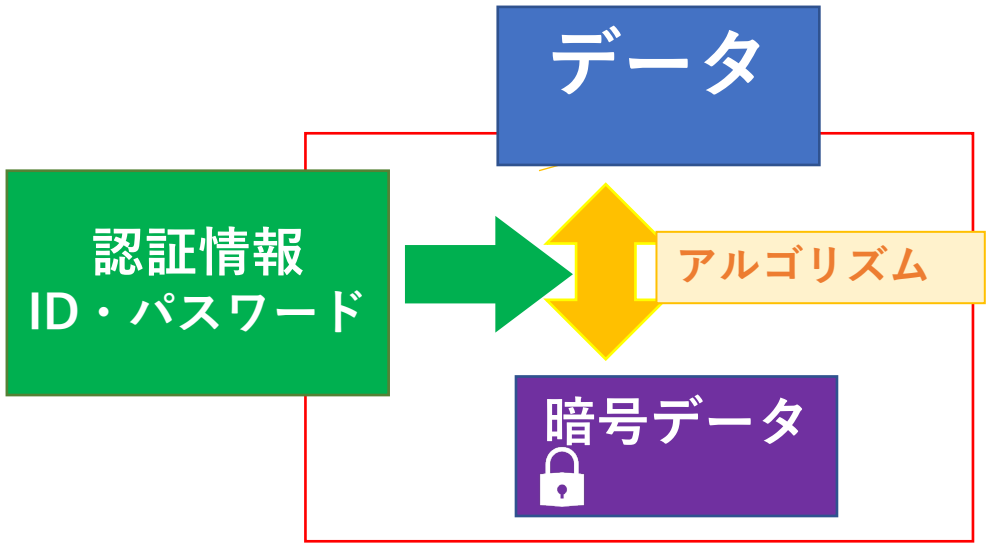
ハッキング
原因の80%

忘れる
盗まれる
紛失する

- 指紋認証
- 静脈認証
- 顔認証
- 音声認証
- ICカード認証

2，３次元バイオメトリクス暗号技術

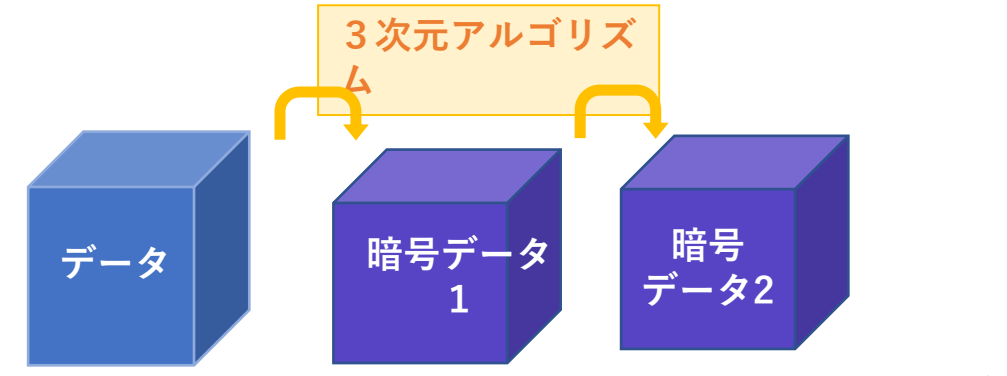
一般的な暗号



認証と暗号化はそれぞれのプログラムで行われ、それぞれに強度を追求している。

ファイアウォール、ブロックチェーンなどのセキュリティはハッカーが侵入可能である事を断言している。

三次元バイオメトリクス暗号



SONAYA３次元暗号技術とは？

認証と暗号化を一体化させてデータを保護する仕組み。

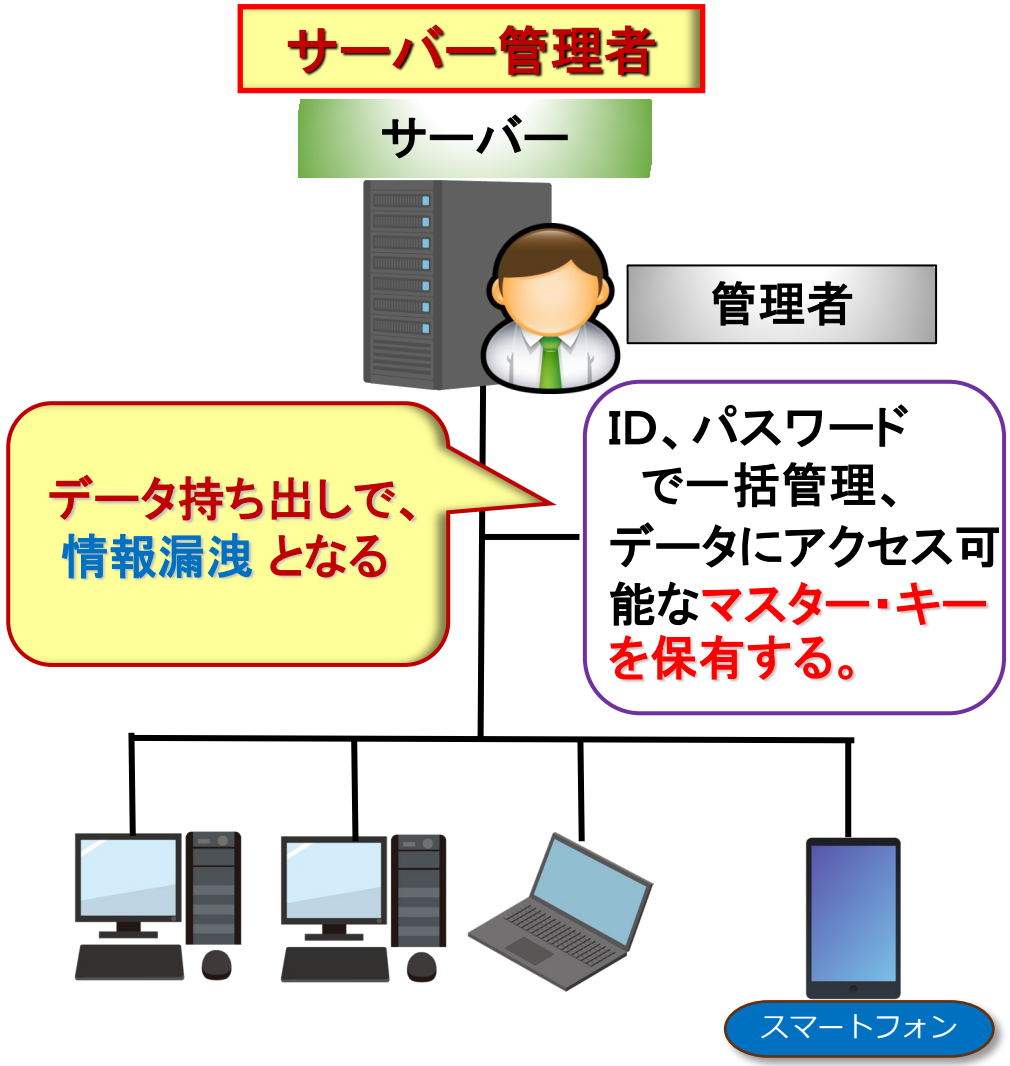
1，最終処理暗号が予測不可能なアルゴリズムで、暗号解読不可能です。

2，さらに原因の特定も不可能です。
「個人認証情報１」と「個人認証情報２」は認証者本人PCだけの情報になります。

3，認証者本人以外がデータを持ち出しても、情報がゴミ になるので、
情報漏洩をブロックします。

3，サーバー管理者不要

一般的なアクセス管理



３次元バイオメトリクスで管理