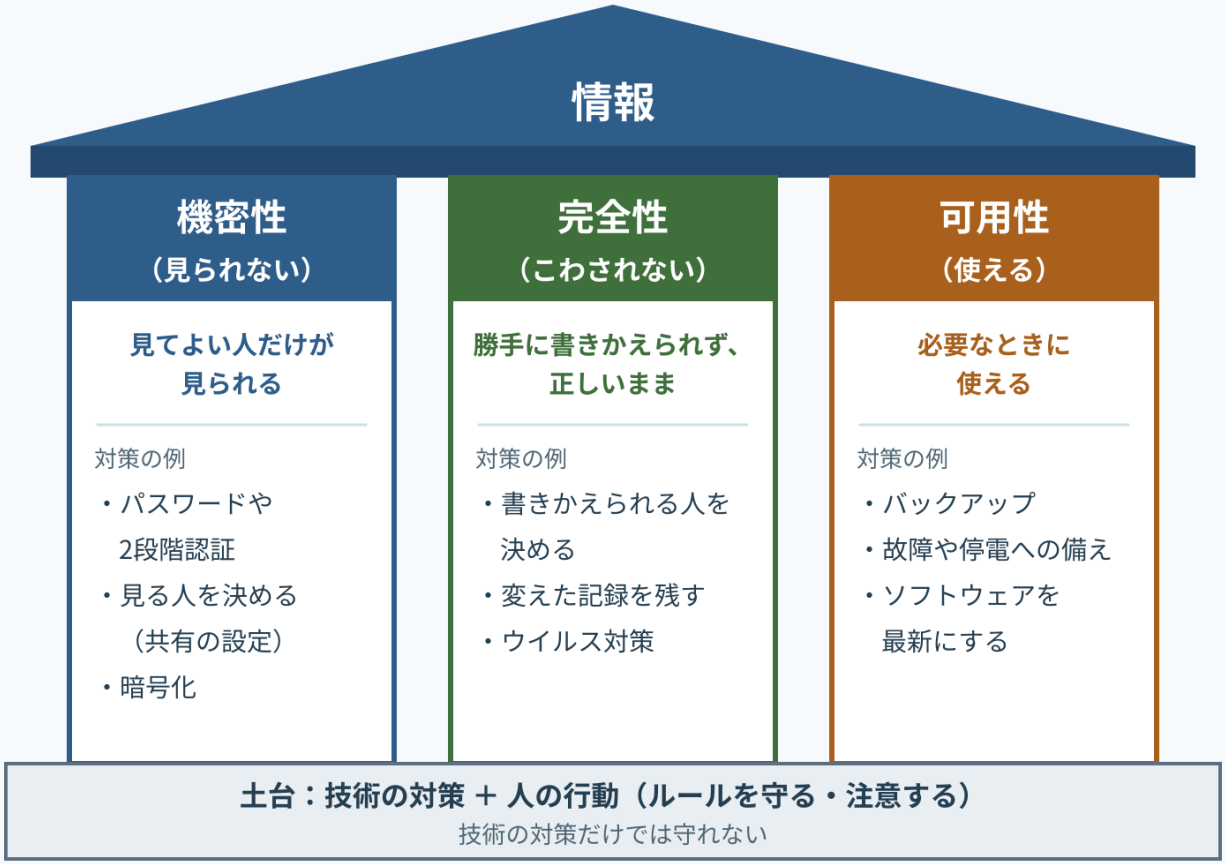
情報セキュリティの3つの柱

情報を守るとは、何を守ることなのだろう



AI AIサービスでも同じ

機密性
入力した情報が、
ほかの人への答えに
使われて見られないか

完全性
不正な操作で、AIの
動きや答えが勝手に
変えられないか

可用性
不正な操作でAIが
止まらないか。止まった
ときに困らないか

自分でできること

- 推測されにくいパスワード
- 共有する相手を確かめる
- 大切なデータはバックアップ
- AIに個人の情報を入力しない

※ 対策は例。学校や家庭のきまりに合わせて行う。