ハッシュ関数のしくみ

データの「指紋」をつくる一方向のしくみ

文章やファイルから、決まった長さの「指紋」のような
値をつくるのがハッシュ関数。元のデータには戻せないのが特ちょう。

1 ハッシュってなに？

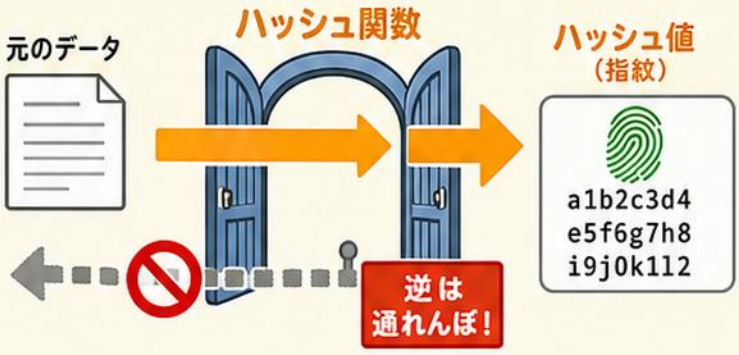
どんな長さの入力でも、決まった長さの
文字列（指紋）に変える計算。

- 入力 → 決まった長さの値
- 同じ入力なら必ず同じ結果
- ちがう入力はたいていちがう結果

2 戻せない（一方向）

指紋からその人を完全に作り直せないのと
同じで、結果から元のデータは戻せない。

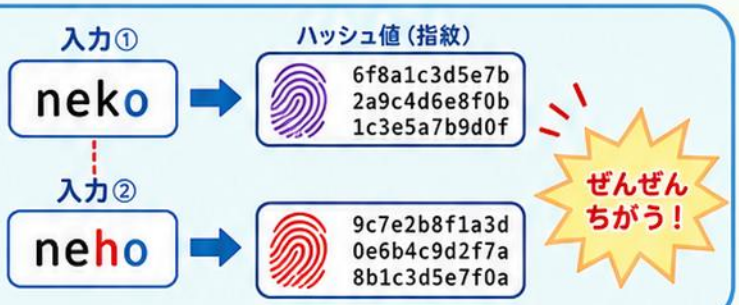
- 結果から元データは戻せない
- 暗号化とはちがう
- 暗号化は戻せる／ハッシュは戻せない



3 少し変えると大きく変わる

入力を１文字変えただけで、結果は
まったくちがう値になる（なだれ効果）。

- １文字変えても結果は別物
- だから改ざんを見つけられる



4 どこで使う？

身のまわりの安全やデータ管理を支えている。

- ファイルがこわれていないか確認
- パスワードの保管（そのまま保存しない）
- データの目印（ID）づくり

★大切なポイント！

ハッシュ＝戻せない

「データの指紋」