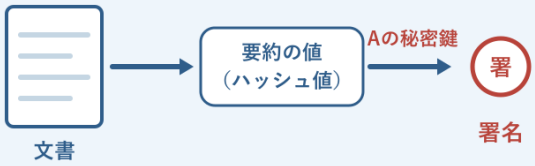
デジタル署名とデジタル証明書

受け取った文書が、本人から届き、書きかえられていないことを、どう確かめるのだろう

送る人（A）

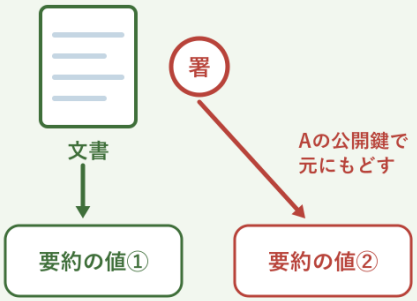


1 文書から、要約の値（ハッシュ値）をつくる
2 要約の値を、Aだけが持つ秘密鍵で暗号化する
→ これが「デジタル署名」
3 文書と署名を一緒に送る

要約の値（ハッシュ値）：文書から計算した短い値。
文書が1文字でも変わると、まったく別の値になる。

送る

受け取る人（B）



①と②が同じ？

同じなら：
・Aが送ったもの（なりすましでない）
・途中で書きかえられていない

Aの公開鍵で元にもどせるのは、Aの秘密鍵で
暗号化したものだけ。だから、Aが署名したと分かる。

でも、その公開鍵は本当にAのもの？ → デジタル証明書

信頼できる第三者（認証局）が、「この公開鍵はAのものです」と証明したもの。
たとえると、印鑑（署名）と、それが本人の印鑑だと示す印鑑登録証明書（証明書）の関係。
Webの暗号化通信（https）でも、サーバーが本物かをデジタル証明書で確かめている。

※ 模式図。署名のしくみは考え方を単純にして示した。