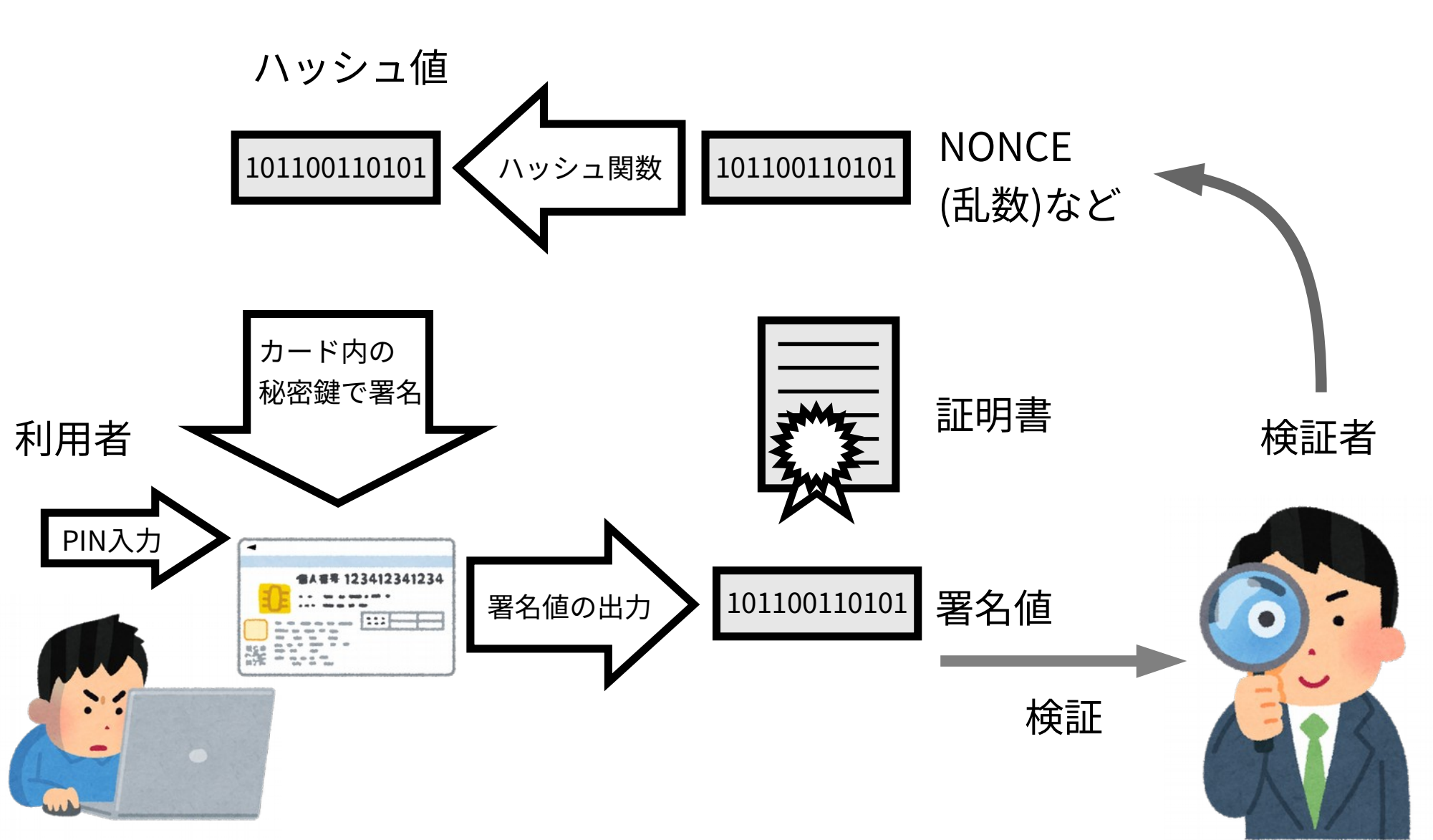
ハッシュ値
101100110101
ハッシュ関数
101100110101
NONCE
(乱数)など
カード内の
秘密鍵で署名
利用者
証明書
検証者
PIN入力
署名値の出力
101100110101
署名値
検証