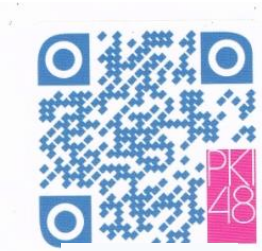


PKIを教えよう！

2016年10月26日

政本　廣志
JNSA 電子署名WG

PKIは普及しているか

高い

証明書が、
運用コストが、

少ない

アプリが、
利用者が、

難しい

技術者にも、
一般の人にも。

⇒ 若いうちから
教えよう！

学生 訂正 2人 に聞きました！
「PKIって知ってますか？」

- 大学生：1
  - ⇒　知ってる。国連平和維持活動。
    - ⇒　残念、それはPKO。
- 高校生：1
  - ⇒　知らない。それ入試に出るの？
    - ⇒　出ません、たぶん。

※かなり脚色しています。

これからの教科書(一案)

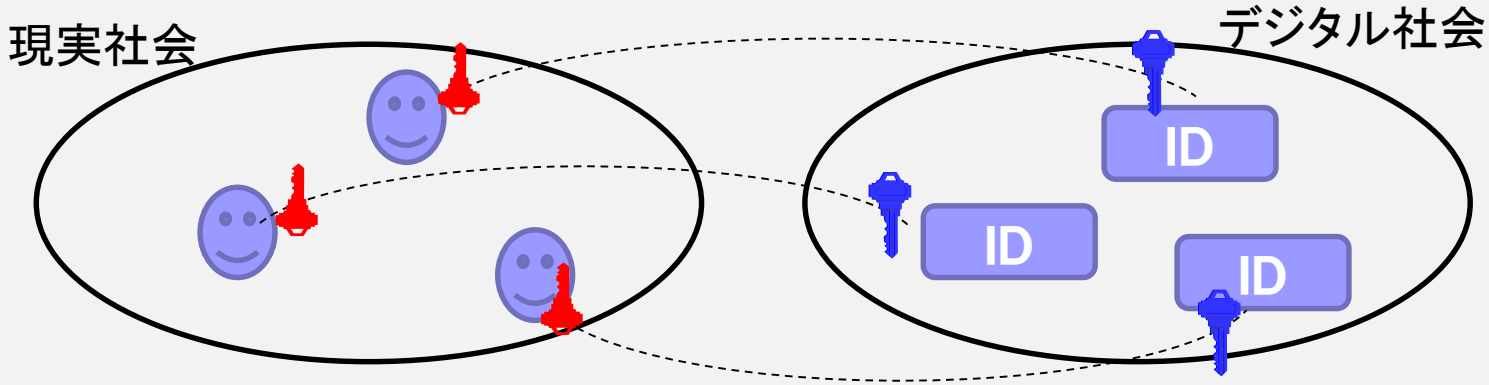
※一部正確でないかもしれませんが、
ネタですのでご容赦ください。

大学(文系)編

『社会学概論』 第5章　PKI

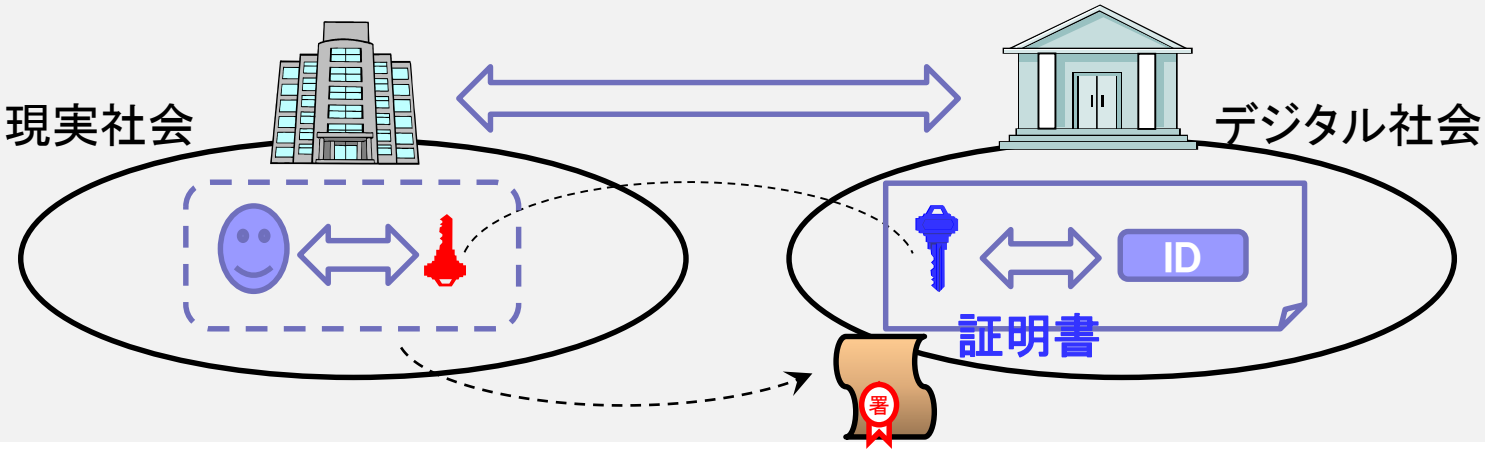
5.1 PKI(PublicKeyInfrastructure)

PKIは、現実社会(のある集団)のエンティティとデジタル社会のIDを、一対の情報(鍵対と呼ぶ)で対応付け、デジタル社会における認証と識別、さらにそのエンティティが生成する情報(署名)に対する保証を与える基盤である。例えば、大学生と学籍番号、市民とそのID、サーバとurlなどである。



『社会学概論』 つづき

この関係を担保するには各々と鍵情報の結びつきを保証する社会的な仕組み(登録、発行、失効など)、それを行使して生成された情報(署名)が有効であるとする法整備や、他の集団との相互運用性を実現する仕組みまで必要である。欧州では包括的に整備するためeIDASという仕組み作りが始まっている。



高校編

『情報A』 第3章　暗号とPKI

3.1 共通鍵暗号と公開鍵暗号

・・・

3.2 PKI(公開鍵暗号基盤)

公開鍵方式に基づいて暗号や署名を行っても、鍵の持ち主が誰か、その証明書は有効かということが分からなければ、意味がありません。

持ち主を登録する仕組み、証明書を発行する仕組み、有効性を確認する仕組みなどを組み合わせることで、社会で使える基盤(PKI)となります。・・・

中学校編

『公民』 第4章　社会の信頼の仕組み

　紙の書類が中心の実社会では、契約などの信頼性を高めるために、『実印』と『印鑑登録』という制度があります。・・・

　同様に、電子社会でも他人のなりすましや電子データの偽造などを防止する仕組みが必要です。それがPKI(公開鍵暗号基盤)と呼ばれる仕組みです。実印の代わりに本人だけが持つ情報をICカードなどに入れ、それを持つことの証明書を発行してもらいます。・・・

小学校編

『生活』 ６．ネットのあんぜんとしんらい

　スマートフォンやパソコンで他の人とやり取りしたり、調べごとをする子もいるでしょう。遠くの人とやり取りできるのは便利ですが、本当にその人でしょうか。言っていることにウソはないでしょうか。

　それを確認できるようにするのが『ピーケーアイ』です。ネットの安全を守るために、様々な仕組みが作られています。・・・

おまけ

えほん

・・・（ry

　もう、かみのじだいではないですね
というおはなしでした。