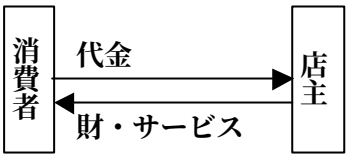
情報法学入門第１１回

ネット上の情報変換

１．非対面取引

近代法は対面取引が前提



料金請求のミス、代金のミス等をどう防ぐか？

２．本人の確認

注文者、業者が存在するかの確認

電子書類の製作者が本人であるかの確認→確認方法のひとつとして「暗号化」

公開鍵←→非公開鍵

公開鍵

データをやり取りする人間に鍵を渡しておく

→手間がかかる、信用できる人間としか取引できない

非公開鍵

ハッシュ関数でペアの鍵を作る

デジタル署名

＊　認証機関（CA）を利用

→CA が信頼できる機関であることが必要

公的な認可や、公共の機関が CA になるのも有効

認証機関同士の認証も必要

ただし、政府が公開鍵を保持する（重大犯罪の盗聴用に）とすると

他の個人のプライバシーが脅かされる恐れがある

しかし、政府機関と確実に電子的なやりとりをするには必要だという点も

日本、欧州諸国はこの 暗号鍵寄託制度 に批判的な声が多い

ＯＥＣＤ暗号製作ガイドライン

ＥＵとアメリカ（暗号産業の寡占を目指している）が対立

アメリカの暗号があふれたら・・・国内の機密情報は？

暗号の強さ→暗号の桁数が長いほど破られにくい
用途に応じて暗号の桁数を調整する

多種多様な暗号方式があるほうが望ましい