【金融業務における暗号技術の応用と国際標準化】(担当:岩下直行)

[授業の目的・概要]

DES 暗号の開発に始まる現代暗号の進化には，金融業界という巨大なユーザーの存在があった．本授業では，1970 年代に始まる銀行の巨大情報ネットワーク化と，そこで利用された暗号がムーアの法則に伴う暗号技術の危殆化の経験を経て，どのように進化を遂げたかを述べる． また，そうした技術の一つの応用事例として，仮想通貨とブロックチェーン技術を取り上げる．

[授業の目標]

暗号技術がそのユーザーである金融業界とともに進化してきた歴史を学ぶとともに，今後も発生するであろう暗号危殆化に対処していく能力を養成する． また，仮想通貨などの新しい応用事例の実態と，その原理を学ぶ．

[知識単位]

暗号危殆化，国際標準の役割, OAuth 認証，ブロックチェーン技術，仮想通貨, ICO

[講義計画]

第 1 回 金融業務における暗号技術の応用の経緯

DES 暗号の開発と金融業界における応用事例，国際標準との関わり

DES 暗号の危殆化と金融業界の対応, 3DES 標準化と AES コンファレンス

2010 年, 2 回目の暗号危機と金融業界の対応

FinTech の発展と金融オープン API を巡る議論

第 2 回 ビットコインと暗号技術

ビットコインの誕生前史，ブロックチェーン技術の原理と課題

ビットコインがもたらしたもの，仮想通貨ブームと相場急騰の背景

ブロックチェーン技術, DLT とその応用事例

ICO を巡る動きと各国規制当局の動向

[履修条件・受講条件]

特に事前知識は仮定しないが，下記があるとより理解が深まる．

- 共通鍵暗号・公開鍵暗号に関する基礎的な知識
- 暗号的ハッシュ関数に関する基礎的な知識

[授業外における学習]

演習課題(教育システムで提示)

テキストの予習及び演習課題(教育システムで提示)

テキストの予習(教育システムで提示)

[参考文献]

1. 今井秀樹,『暗号のおはなし』, 日本規格協会, 2003 年

2. ドン＆アレックス・タプスコット,『ブロックチェーン・レボリューション』, ダイヤモンド社, 2016 年