「ブロックチェーンと暗号技術」

■日程：2022 年 8 月 31 日・9 月 1 日 10:00～17:00
■担当：有田 正剛, 土井 洋, 大塚 玲（情報セキュリティ大学院大学教授）
■開講形態：情報セキュリティ大学院大学での開講のみとする

1. 演習のねらい
本講義では、基盤となる暗号技術を学んだ上で、ブロックチェーンの原理と実践について学ぶ。基盤暗号技術として、自律分散型のシステムにとって重要な、マルチパーティプロトコルとゼロ知識証明技術について学ぶ。その上で、ブロックチェーンの原理と安全性の考え方について学び、演習を通して理解を深める。

2. 達成目標
- マルチパーティプロトコルの観点からブロックチェーンを理解する。
- ゼロ知識証明技術によってブロックチェーンにプライバシーをもたらす方法を学ぶ。
- ブロックチェーンの原理と安全性の考え方について理論と実践双方から理解する。

3. 前提条件
ブロック暗号、ハッシュ関数、公開鍵暗号、デジタル署名等の暗号理論の基礎知識を仮定する。

4. 授業計画
- 第１・２時限：（担当　土井教授）マルチパーティプロトコルについて講義形式で学ぶ。
- 第３・４時限：（担当　有田教授）ゼロ知識証明技術について講義形式で学ぶ。
- 第５～８時限：（担当　大塚教授）ブロックチェーンについて講義と演習を組み合わせて学ぶ。

5. 教科書
特に指定しない。

6. 参考書
特に指定しない。

7. 受講申請について
受講希望者は、Basic SecCap受講申請期間内に、「Basic SecCap履修登録システム」にて受講申請すること。

8. 成績評価および成績の報告について
成績評価（修了／不合格）は以下の 3 点により行う
- 講義の受講状況

- 演習への参加状況
- 課題レポートの評価
  課題レポートの提出期限と形式は講義中に指定する。

また、成績は終了後、速やかに各所属校の SecCap 担当窓口に報告する。

9. その他
災害障害保険及び賠償責任保険に加入している必要がある。詳細は所属校の担当窓口に問い合わせること。

10. 問い合わせ先
情報セキュリティ大学院大学 SecCap 担当(iisec@seccap.jp)

【5 月 12 日追加：「3. 前提条件」について】
下のようなキーワードを受講者が理解しているとの前提で担当者は授業を進めます。
各キーワードが授業内で掘り下げて解説されることはありませんので、必要に応じて自身で予習してください。

キーワード：
NP 言語，対話証明，行列，ベクトル空間，線型結合，線形従属，楕円曲線上のペアリング，暗号学的ハッシュ関数，デジタル署名，存在的偽造不可能性（EUF-CMA)，Chernoff 限界，マルコフ過程

以上