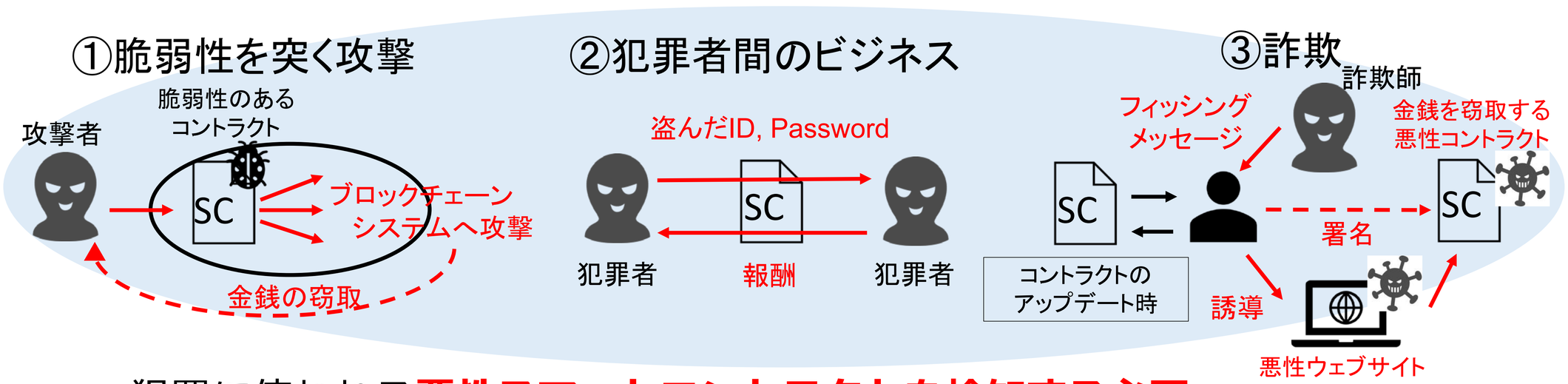
松浦研究室

暗号と情報セキュリティ

情報・エレクトロニクス系部門

情報理工学系研究科　電子情報学専攻
http://kmlab.iis.u-tokyo.ac.jp/

- 悪性スマートコントラクト
  ブロックチェーン上のアプリケーションとして働くコンピュータプログラムである**スマートコントラクトを利用した犯罪が近年増加**



⇒ 犯罪に使われる**悪性スマートコントラクトを検知する必要**

【従来の分類モデル [1] と問題点】

既存の悪性スマートコントラクトの分類は２種類

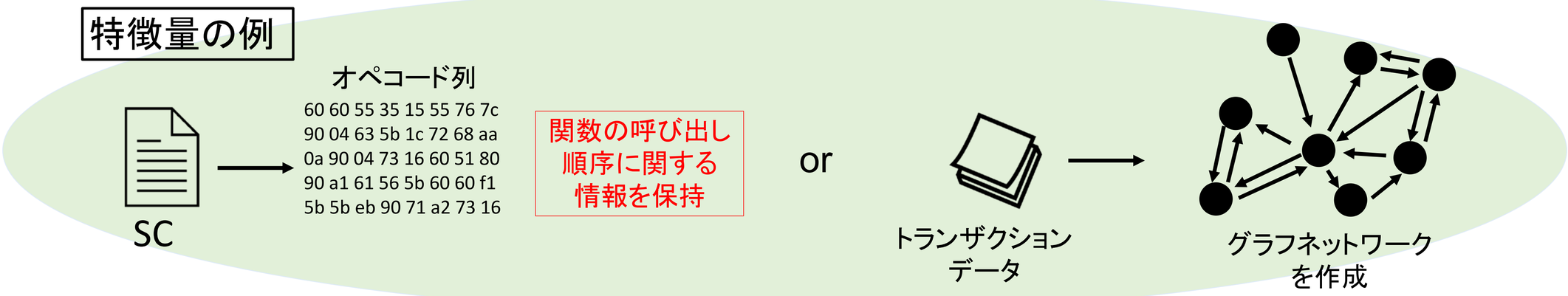
①Vulnerable Smart Contract　… 脆弱性のあるコントラクト ②Criminal Smart Contract　　… 犯罪者の取引を促進させるコントラクト

⇒ 詐欺に関わるコントラクトに対応する分類がない

⇒ 悪性スマートコントラクト全体の包括的な検知が困難

詐欺を促進させるコントラクト（Fraudulent Smart Contract）を分類モデルに追加
⇒ Fraudulent Smart Contract の検知手法の構築を目指す [2]

- Fraudulent Smart Contract 検知の展望
  コード or トランザクションを基にした特徴量を作成 ⇒ **機械学習により検知**



[1] M.Ndiaye, and P. Konate “Cryptocurrency Crime: Behaviors of Malicious Smart Contracts in Blockchain.” *2021 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2021.pp.1-8
[2] 五十嵐太一ほか．“スマートコントラクトにおけるセキュリティに関する調査”．2023年暗号と情報セキュリティシンポジウム（SCIS2023），3C-1，2023年1月．