会津大学大学院コンピュータ理工学研究科
情報セキュリティクラスター（ARC-Security）

メンバー

リーダー
中村 章人
（教授）

サブリーダー
蘇 春華
（上級准教授）

可知 靖之
（上級准教授）

クラスターの概要

本クラスターは、当初クラウドコンピューティングを主な研究領域としていましたが、2017年からは情報セキュリティを中心とした研究に取り組んでいます。

従来型ICTシステムのセキュリティ対策に加えて、最近は、新しい応用領域であるIoT/IIoT、サイバーフィジカルシステム（CPS）、人工知能（AI）などに関するセキュリティの研究に取り組んでいます。また、利用者（人）を騙すタイプのサイバー攻撃を防止する技術も対象にしています。

さらに、ソフトウェア開発者やシステムエンジニアが高品質で信頼性の高いプロダクトを構築できるように、セキュリティテストを支援する研究も推進しています。

キーワード：サイバー攻撃対策、脆弱性管理、フィッシング対策、セイフWebブラウジング、侵入検知、システムテスト、アクセス制御、認証、軽量暗号、ポスト量子暗号、ブロックチェーン、非代替性トークン、プライバシー保護

ミッション

研究

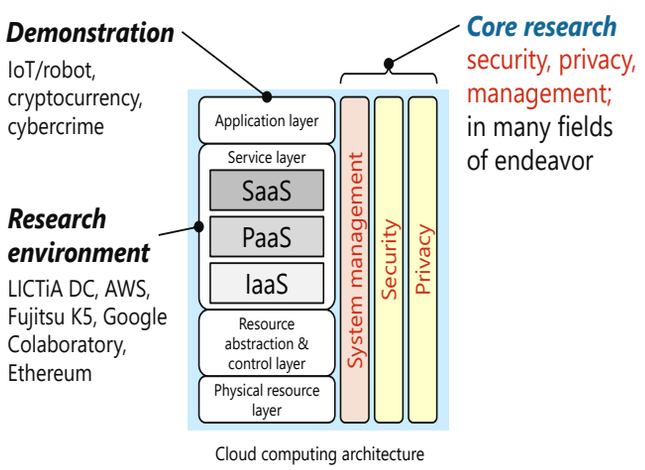
- 情報セキュリティ、オンラインプライバシ、クラウドコンピューティング、IoT/CPS、AIにまたがる最先端の研究

教育

- 学内外でのICTプロフェッショナル人材の育成（特にセキュリティ人材）

社会貢献

- 産学官連携による社会ニーズへの対応、産業の振興



メンバ・関係者

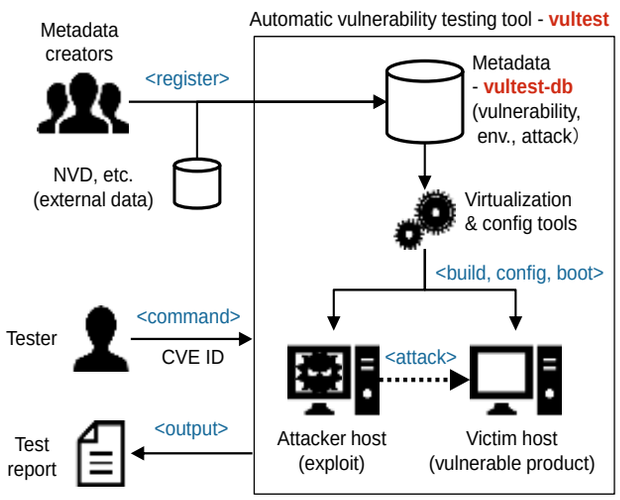
- 岩瀬 次郎（理事）
- 屋代 眞（特任教授）
- 阿部 泰裕（上級准教授）
- 畠 圭佑（准教授）
- 九州大学、デンマーク工科大学、
  國立東華大学、福島県警察本部、他

教育・人材育成の活動

- サイバー攻撃対策演習講座【プロ向け】
- リーダー養成講座【企業向け】
- リテラシー・モラル講義【一般向け、小中高教員向け】
- サイバー防犯ボランティア【本学学生】

会津大学大学院コンピュータ理工学研究科
情報セキュリティクラスター（ARC-Security）

最近の研究テーマ

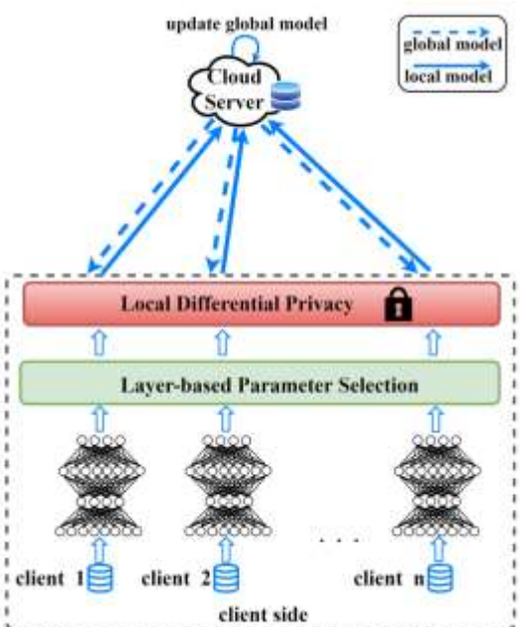


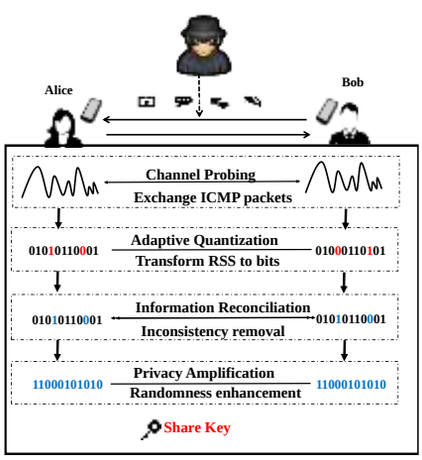
ソフトウェア脆弱性の再現・テストの自動化

- コマンド一発でテストの全プロセスを自動実行
- 指定した脆弱性を再現する標的ホストを仮想環境に自動構築、OSや関連ソフトのインストールや設定はツールにおまかせ、攻撃を実行してレポート
- オープンソースで公開中
  ：GitHub uoanlab/vultest
- ユースケース：ソフトウェア開発者のデバッグ支援、システム管理者の攻撃影響評価、トレーニングにおける攻撃の原因や影響の学習支援

プライバシーを保護した連合学習

- パーソナルデータを一か所に集めない分散型の機械学習方式
- データをクラウドにアップロードせずエッジ側で学習、複数のローカルモデルをクラウドで統合（連合学習）、データやモデルを暗号化したまま計算（準同型暗号）
- ユースケース：スマートシティ





IoTのための暗号鍵管理

- IoTデバイス同士の通信に用いる暗号鍵を自動生成
- 無線チャネルの信号特性をそれぞれ0/1の列に量子化し、調整を経て、ランダム性を加えて共通鍵を生成
- ユースケース：スマートホーム、自動運転、遠隔医療

ブロックチェーンによるIoT認証

- つながるクルマの計算資源の割当問題を定式化、機械学習とブロックチェーンの組合せで解決
- ブロックチェーンの性能を維持しつつ、資源割当を最適化