

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）

概要

本クラスター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、最近では、新しい応用領域であるIoT/IoT、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、セーフ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ー、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

実用化の可能性

○ プライバシーを保護する機械学習方式
データをクラウドにアップロードせずエッジ側で学習し、データやモデルを暗号化したまま計算できるので、分散型AIを安全にクラウドで統合できます。

（ヘルスケアシステムなどでの利用）

○ ソフトウェア脆弱性テストの自動化
指定した脆弱性を再現するホストの構築から攻撃の試行までを仮想環境で自動実行できます。（ソフトウェア開発、セキュリティ診断などに利用）

研究概要図

