IoTセキュリティ研究センター

Research Center for IoT Security

IoTやセキュリティに関わる基準策定、人材育成に取り組み IoTを基盤としたスマート社会の実現に貢献する

あらゆる「機器＝モノ（Things）」がインターネットに接続可能なIoT（Internet of Things）が進展する現代、社会基盤としてIoTを安全に活用していく上で、いかにセキュリティを保持するかが重大な社会課題となっています。IoTとセキュリティに関する研究やセキュリティリテラシーの醸成を通じてこうした課題を解決し、安全・安心なスマート社会の実現に貢献することを目指し、2020年8月、IoTセキュリティ研究センターは設立しました。

本センターでは、主に三つのプロジェクトを推進しています。一つは、IoTセキュリティに対応した技術者の育成です。セキュアな通信技術やソフトウェアの開発技法などに関するスキルセットを定め、大学教員である研究メンバーの教育ツールや授業コンテンツなど大学の持つ教育シーズを活用し、機器やシステムの開発に携わる技術者に教育カリキュラムを提供します。そのために企業と連携してコンソーシアムを組織し、カリキュラムの充実を図っていきます。

二つ目は、IoTセキュリティ技術に関する基準の検討・構築です。2019年4月に経済産業省が「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」を策定したことに伴い、各産業分野でこれに則ったセキュリティ基準の構築が急務となっています。本プロジェクトでは、産業分野ごとに必要となるセキュリティ基準を検討し、産学間での共通認識を構築するとと

もに、各業界のCPSFへの対応を支援します。三つ目は、ブロックチェーン技術に関する基準の検討です。暗号技術を使って複数のコンピュータで情報を共有するブロックチェーン技術は、仮想通貨（暗号資産）の運用に用いられるなど、次代の経済活動の基盤技術になると期待されていますが、いまだ安全性が十分確立されているとはいえません。本プロジェクトでは、IoTセキュリティの視点からブロックチェーン技術に関するガイドラインの策定に役立ちたいと考えています。

本センターの特長は、セキュリティやIoT関連技術を専門とする研究者を中心に理工学や法学の研究者も参画し、学際的に研究するところにあります。目標は幅広い分野の専門家にネットワークを広げ、IoTやセキュリティに関するあらゆる知見が集積する拠点となること。今後、産官学公が連携してサイバー攻撃の対策やサイバー犯罪の抑止にも貢献し、セキュアなIoTシステムを実現するための研究に取り組んでいきます。

〈IoTセキュリティ研究コンソーシアム〉

本コンソーシアムは、コンソーシアム会員が研究者との研究交流を行うため
具体的な研究活動の拠点として本コンソーシアム内に以下の研究会（分科会）を設置することを目標としています。

IoTセキュリティ技術基準の検討研究会

産業システムのIoT化に関しては経済産業省が2019年4月にサイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）を策定し、これに沿ったセキュリティ基準を産業分野別に策定していくことを求めていますが、国際的技術基準との相互関係は必ずしも明らかではないため、業界別に整理していく必要があるはずです。本センターでは産業システム分野別に対するセキュリティ基準策定について検討、その実現に必要となる各種技術の研究開発、各分野のCPSF対応を支援していきます。

IoTセキュリティの確保に資する要素技術の開発研究会

本センターの各研究者が有するIoTセキュリティの確保に資する要素技術の開発技術をベースとして、以下のようなサブテーマを想定しています。

- IoT向けのセキュアなオペレーティングシステムの設計と実装
- IoT向けのアドホックネットワークのセキュアプロトコル設計
- 複製不可能デバイスを用いた認証基盤の産業システム応用
- 形式仕様記述およびメモリ安全なプログラミング言語を用いた組み込み向けセキュア開発技法
- ブロックチェーンを利用したIoT向け証跡管理とその分析
- ユーザブルセキュリティ確保のためのIoT向け生体認証技術の開発

IoTセキュリティに対応した人材育成研究会

各産業分野において、従来から機器やシステムの開発に携わってきた技術者に対し、インターネット接続を行う際のセキュリティ対策に関するノウハウが十分教育されておらず、実装上の脆弱性を排除しきれない例が報告されています。そのような技術者に対してリカレント教育を行う際に必要なセキュアな通信技術やセキュアソフトウェア開発技法、プライバシー保護開発技法などに関するスキルセットを定め、教育カリキュラムを策定の検討をします。

その他コンソーシアムの目的達成に必要な研究会

各コンソーシアム会員企業自身が抱えるIoT開発技術やそれに伴うセキュリティ開発技術などの課題に対し、応えるべく産業システムセキュリティ基準について検討する。また、IoTとセキュリティのスムーズな融合を図るため、IoT開発技術の適正化を行うことも大きな検討課題としています。

コンソーシアム入会年会費

法人会員：1法人あたり100,000円（民間企業・営利団体）
個人会員：1人あたり　10,000円（コンソーシアムの目的に賛同する個人）
賛助会員：無料（行政機関・非営利団体・公益を目的とする法人等・立命館大学院生）
※入会ご希望の方はBKCリサーチオフィス内、IoTセキュリティ研究コンソーシアム事務局までご連絡ください。

主な研究テーマ

- 産業システム分野別に対するセキュリティ基準の策定
- IoT向けのセキュアなオペレーティングシステムの設計と実装
- IoT向けのアドホックネットワークのセキュアプロトコル設計
- 複製不可能デバイスを用いた認証基盤の産業システム応用
- 形式仕様記述およびメモリ安全なプログラミング言語を用いた組み込み向けセキュア開発技法
- ブロックチェーンを利用したIoT向け証跡管理とその分析
- ユーザブルセキュリティ確保のためのIoT向け生体認証技術の開発
- 企業の技術者に対してセキュアソフトウェア開発技法、プライバシー保護開発技法などに関するスキルセットを定め、教育カリキュラムを策定
- 知見を生かした再利用可能なセキュリティ啓蒙コンテンツの開発、及びその積極的な公開

センター長：上原 哲太郎（情報理工学部 教授）
主な研究拠点：びわこ・くさつキャンパス　サイバーセキュリティ研究室（上原研究室）
お問い合わせ：立命館大学 研究部 BKCリサーチオフィス　TEL：077-561-2802　FAX：077-561-2811　✉：liaisonb@st.ritsumei.ac.jp
http://www.ritsumei.ac.jp/research/center/iot-security/