個人研究

スマート社会

安全なネットワークやシステムの構築

ネットショッピングをはじめとしたWebサービスや、自動車、工場などの様々なシステムにおいて、情報セキュリティの脅威が高まっています。
これらに対抗するために、ネットワーク、クラウドやブロックチェーンのセキュリティ技術や、暗号理論・方式など幅広く研究しています。

KEYWORDS　情報セキュリティ、ネットワークセキュリティ、暗号技術

RESEARCHER

コンピュータサイエンス学部 准教授　布田裕一

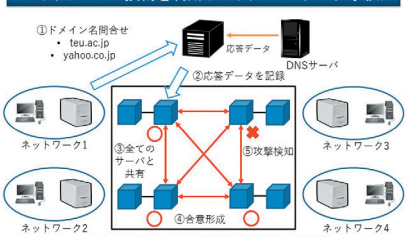
学会発表・論文・著書・社会活動

[1] “Formalization of Definitions and Theorems Related to an Elliptic Curve over a Finite Prime Field by Using Mizar”, Formal Mathematics for Mathematicians, Journal of Automated Reasoning, Vol. 50, No. 2, Springer, 161-172, 2012.
[2] “Suitable Symbolic Models for Cryptographic Verification of Secure Protocols in ProVerif”, The International Symposium on Information Theory and Its Applications (ISITA) 2018, 2018.
[3] “形式的安全性検証ツールを用いた暗号教育の実践とそのe-Learning教材化の課題について”, 日本ソフトウェア科学会, コンピュータソフトウェア, Vol. 37, No. 1, 99-113, 2020.

01｜ネットワークとブロックチェーンの融合

インターネットの通信では、ネットワークの関連情報を取得しながら、データを送信しています。ネットワークに不正な情報が流れてしまうと、クレジットカードのデータや個人データが攻撃者に送られてしまい不正に使用される可能性があります。そこで、ブロックチェーンの基盤とする分散ネットワークや、情報の信頼性を向上させる合意形成を使用し、ネットワークの攻撃を検知します。具体的には、DNSサーバからの応答データをブロックチェーンとして各サーバ間で共有し、合意形成を用いて、DNSキャッシュポイズニング攻撃を検知します。
この他に、DDoS攻撃の対策や、工場などの制御システムの攻撃検知も研究しています。

ブロックチェーン技術を利用したネットワークの攻撃検知



ブロックチェーンとして共有したDNSサーバからの応答データの合意形成の結果により、攻撃を検知

02｜暗号方式やアルゴリズムの設計

インターネットで使用される暗号通信SSL/TLSでは、公開鍵暗号やディジタル署名を用いていますが、多くのメモリや処理時間が必要となります。
そこで、メモリ量や処理時間を軽減するアルゴリズムを研究しています。特に、最近、注目されている格子暗号のアルゴリズムに取り組んでいます。
この他に、ブロックチェーンなどで使用する暗号方式やプロトコルの安全性評価を実施しています。

格子暗号のアルゴリズム評価