教員名	宮本大輔 准教授	研究場所	本郷　工学部1号館 柏2 情報基盤センター	研究分野	サイバー セキュリティ

当研究室は、サイバーセキュリティの研究室です。サイバー脅威の技術的要因、人的要因、組織的要因の特徴を捉えたセキュリティ研究開発を行い、誰もが安心して利用できるサイバー社会を目指します。

ウェブサイト:https://www.iplove.net
連絡先:daisu-mi@nc.u-tokyo.ac.jp

研究室の概要

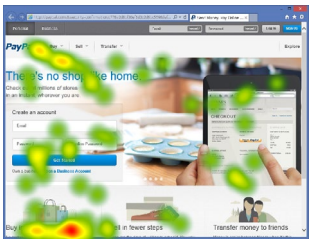
インターネットが社会基盤となり、サイバー社会は我々の暮らしと密接に連携しています。一方で、この社会基盤に対するサイバー脅威も増大しています。全てのサイバー脅威の解決は幻想に過ぎず、我々はリスクの回避・受容を考えながら、サイバー社会のセキュリティを向上させる実践的な研究を行っています。

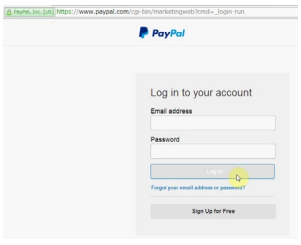
当研究室では、技術的要因、人的要因、そして組織的要因の 3 つの観点からサイバーセキュリティの研究に取り組んでいます。「技術的要因」では、マルウェア対策、ハニーポット技術、DoS/DDoS 対策、トラフィック解析、サイバーレンジ技術を研究しています。「人的要因」では、フィッシングサイト対策、標的型メール対策、セキュリティにおける状況認識、意思決定理論を研究しています。「組織的要因」では、インシデント対応と組織連携、自動脅威分析、セキュリティ教育、国際標準化活動などに取り組んでいます。これらのキーワードだけではなく、サイバー空間を構成する全ての要素を研究対象としています。

主な研究テーマ

1. フィッシング対策技術

フィッシングとは、正規のメールやウェブサイトを偽装することで、エンドユーザを騙し、個人情報を搾取するサイバー脅威です。メール本文やコンテンツは巧妙に偽装されており判別が難しく、ユーザはセキュリティ情報を見つけ出し判断する必要があります。ユーザがどのように意思決定をするかを、ユーザの視線情報から分析する提案を行うなど、ユーザの行動に着目した研究を行っています。

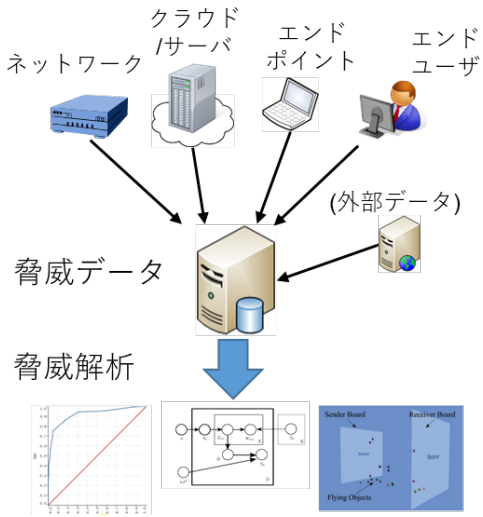




左図はコンテンツに着目しセキュリティ情報を閲覧していないユーザの視線移動の様子です。右図はユーザの視線を追跡し、ユーザがセキュリティ情報を確認するまで、個人情報の入力を受け付けないようにするブラウザ拡張の開発事例です。

2. マルチレイヤ脅威対策

ユーザの行動だけでなく、マルウェアや不正アクセスなどサイバー脅威のデータを多層的に収集し、攻撃の予兆を早期に発見することが求められています。研究室は機械学習によるサイバー脅威データ解析に早くから取り組んでおり、現在は実践的な対策システムの開発を課題としています。この課題を解決するには、ネットワーク基盤技術やシステム運用を理解する能力、サイバー脅威データの解析能力、そして、有効性あるセキュリティ対策を行う能力が重要です。このため、国内・国外の研究者と連携し、問題解決に取り組んでいます。



上図はサイバー脅威データを俯瞰的に収集し、解析を目指す概念を説明しています。システムとしてはデータ解析基盤の開発、探索的データ解析、教育コンテンツの開発、演習プログラムの設計を行っています。