[2023]九州大学情報統括本部年報 : 2023年度

出版情報：九州大学情報統括本部年報. 2023, pp.1-, 2024-09-01. Information Infrastructure Initiative, Kyushu University
バージョン：
権利関係：

第 5 章　情報システムセキュリティ研究部門

5.1　活動概要

サイバー攻撃から情報システムや情報資産を守るために、サイバー攻撃の検出手法や防御手法、情報システムをセキュアにする設計・構築手法からセキュアな運用手法に関する研究開発を推進する。

5.2　構成員

《部門長》 教　授　　小　出　　洋

5.3　各員活動概要

5.3.1　小出　洋

研究内容

1. Moving Target Defense　(MTD) に関する研究
   Target Defense（MTD）は情報システムにおけるさまざまなパラメータ（例えば OS、システムコール番号、実行可能バイナリのマジックナンバー、ネットワーク識別子）を変化させ、攻撃を困難にする近年注目されている手法である。本研究では、特定のアプリケーションや特定の情報システムに向いた MTD の開発と評価、ある MTD を情報システムに適用したときの平均攻撃成功時間間隔などの MTD のサイバー攻撃に対する防御性を評価する方法に関する考察、ひとつの情報システムに複数の異なる MTD を適用した場合の防御性を評価する方法について研究を行っている。

2. 脅威トレースに関する研究
   APT 攻撃に利用されるマルウェアに代表される脅威が情報システムに侵入したときの活動を予測し、脅威が行う攻撃を阻止したり、情報漏洩を防いだりするには何が必要かを明らかにし、情報システムの設計や運用に資することを目的として脅威トレースの提案、実装、評価を行っている。脅威トレースはマルウェアとそれが動作する情報システムと攻撃に使われるマルウェアを抽象度の高いモデルで表現し、その挙動をシミュレーションすることで解析している。

3. Web アプリケーションのための攻撃検知システムに関する研究
   Web アプリケーションを作成する際には、Web アプリケーション・フレームワークが必ず利用される。サイバー攻撃の検知やサイバー攻撃からシステムを防御するための機能は Web アプリケーション・フレームワークが備えるべき機能といえるが、実際は Web アプリケーション・ファイヤーウォールやセキュリティアプライアンス等の別のシステムになっていることが多い。サイバー攻撃からの防御のための機能を Web アプリケーション・フレームに組み込んだ場合、Web アプリケーション内部の情報や Web アプリケーションの特徴にあわせた攻撃検知とすることができる。Web アプリケーションの特徴に合わせた攻撃検知や攻撃をハニーポットに誘導する機能を Web アプリケーション・フレームワークに実装して評価する研究を行っている。

所属学会名

ACM、ソフトウェア科学会、電気情報通信学会、情報処理学会

研究プロジェクト

サイバー攻撃が困難な情報システムを構築するためのフレームワーク
2021.04 ～ 2025.03　代表者：小出　洋、九州大学

研究実績

- **原著論文**

1. Yuki Funaoka, Hiroshi Koide、Improved Vulnerability Handling Framework to Automatically Fix Vulnerable Web Applications.、CANDARW、2023.12
2. Xiaojuan Cai, Hiroshi Koide、New Perspectives on Data Exfiltration Detection for Advanced Persistent Threats Based on Ensemble Deep Learning Tree.、WEBIST、2023.11
3. Yutaka Yamaguchi, Dirceu Cavendish, Hiroshi Koide、Electric Vehicle Authentication and Secure Metering in Smart Grids、Proc. 17th International Conference on Emerging Security Information, Systems and Technologies, SECUREWARE 2023、2023.09

研究資金

- **科学研究費補助金**

  2021 年度～ 2024 年度、基盤研究 (C)、代表、サイバー攻撃が困難な情報システムを構築するためのフレームワーク

- **共同研究、受託研究**

1. 2023.12 ～ 2024.03、代表、研究開発コンサルティング
2. 2023.06 ～ 2024.03、代表、情報システムを攻撃から防御するための Moving Target Defense に関する研究

- **寄付金**

  2023 年度、セキュアスカイテクノロジー、寄付金「ProSec-IT/SECKUN 事業

教育活動

- **担当授業科目**

2023 年度・春学期　　サイバーセキュリティ基礎論 .
2023 年度・春学期　　サイバーセキュリティ基礎論 .
2023 年度・春学期　　暗号と情報セキュリティ特論 .
2023 年度・春学期　　【ｻｲﾊﾞｰ】暗号と情報セキュリティ特論 .
2023 年度・春学期　　暗号と情報セキュリティ特論 .

2023 年度・通年	情報システムセキュリティ演習Ⅰ.
2023 年度・通年	情報システムセキュリティ演習Ⅱ.
2023 年度・通年	情報システムセキュリティ演習.
2023 年度・通年	セキュリティエンジニアリング演習.
2023 年度・通年	セキュリティエンジニアリング演習.
2023 年度・通年	【通年】情報理工学研究Ⅰ.
2023 年度・通年	【通年】情報理工学演習.
2023 年度・通年	【通年】情報理工学講究.
2023 年度・前期	情報理工学読解.
2023 年度・前期	情報理工学論述Ⅰ.
2023 年度・前期	情報理工学論議Ⅰ.
2023 年度・通年	Cyber Security Exercise for Information Systems I.
2023 年度・通年	Cyber Security Exercise for Information Systems II.
2023 年度・通年	Security Engineering Exercise.
2023 年度・秋学期	通信工学通論Ⅰ.
2023 年度・冬学期	通信工学通論Ⅱ.
2023 年度・秋学期	コンピュータシステム通論Ⅰ.
2023 年度・冬学期	コンピュータシステム通論Ⅱ.
2023 年度・秋学期	コンピュータシステム通論 A.
2023 年度・冬学期	コンピュータシステム通論 B.
2023 年度・後期	（後期）コンピュータシステム通論.
2023 年度・後期	情報理工学論述Ⅱ.
2023 年度・後期	情報理工学論議Ⅱ.
2023 年度・通年	Scientific English Presentation I.
2023 年度・通年	Scientific English Presentation II.
2023 年度・通年	Advanced Project Management I.
2023 年度・通年	Advanced Project Management II.
2023 年度・通年	先端プロジェクト管理技法.
2023 年度・通年	Scientific English Presentation.
2023 年度・通年	Intellectual Property Management.
2023 年度・通年	Advanced Project Management Technique.
2023 年度・通年	情報ネットワーク特別講究.
2023 年度・通年	Advanced Research in Networking Technologies and Application.
2023 年度・通年	情報理工学特別研究Ⅰ.
2023 年度・通年	情報理工学特別研究Ⅱ.
2023 年度・通年	情報理工学特別演習.
2023 年度・通年	Advanced Research in Information Science and Technology I.
2023 年度・通年	Advanced Research in Information Science and Technology II.
2023 年度・通年	Advanced Seminar in Information Science and Technology.
2023 年度・通年	情報ネットワーク特別講究.