准教授
吉岡 克成
ヨシオカ カツナリ

大学院環境情報研究院　社会環境と情報部門
工学部　電子情報工学科　情報工学コース
大学院環境情報学府　情報メディア環境学専攻　情報メディア学コース
理工学部　数物・電子情報系学科　情報工学教育プログラム
yoshioka@ynu.ac.jp
http://www.ynu-irc.ynu.ac.jp/yoshioka.html

工学
電気電子工学

通信・ネットワーク工学

情報システムセキュリティ
ネットワークセキュリティ
マルウェア対策
トラヒック解析
IoT セキュリティ

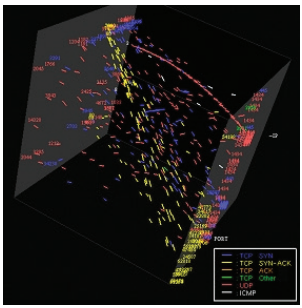
[研究概要]

インターネットに代表される情報通信ネットワークで実際に発生している様々な脅威の観測、詳細分析を行い、そのメカニズムを明らかにし、対策を導出することで、安心・安全な情報社会を実現することを目指し、研究を行っています。

そのため、国内外の研究機関と協力し、不正アクセスやウイルス検体等の実データ収集・共有を進め(独立行政法人情報通信研究機構とのデータ共有を進めています)、ネットワーク攻撃やウイルスの解析を行っています。

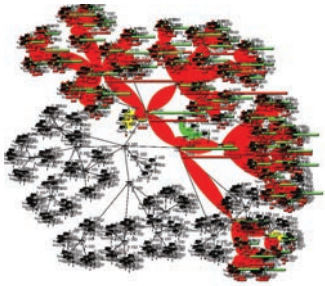
[アドバンテージ]

前職にて広域ネットワークモニタリングおよびマルウェア解析を行う最先端分析システム構築に関する国家プロジェクトに中心メンバとして関わり、トラヒック分析、ネットワーク攻撃検知、マルウェア解析技術に精通しています。



[事例紹介]

・マルウェアを実際に実行してその挙動を解析するマルウェア動的解析システムの構築
・大規模ネットワークモニタリングおよびマルウェア解析システムの構築



■ 相談に応じられるテーマ

マルウェア解析・対策全般
ネットワーク監視・侵入検知技術

■ 主な所属学会

電子情報通信学会
情報処理学会

■ 主な論文

Akira Yokoyama, Kou Ishii, Rui Tanabe, Yin Minn Papa, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Daisuke Inoue, Michael Brengel, Michael Backes, Christian Rossow, "SANDPRINT: Fingerprinting Malware Sandboxes to Provide Intelligence for Sandbox Evasion," Proc. Research in Attacks, Intrusions, and Defenses (RAID16), Lecture Notes in Computer Science, 2016.

Arman Noroozian, Maciej Korczynski, Carlos Hernandez Ganan, Daisuke Makita, Katsunari Yoshioka, Michel van Eeten, "Who Gets the Boot? Analyzing Victimization by DDoS-as-a-Service," Proc. Research in Attacks, Intrusions, and Defenses (RAID16), Lecture Notes in Computer Science, 2016.

Yosuke Kikuchi, Hiroshi Mori, Hiroki Nakano, Katsunari Yoshioka, Tsutomu Matsumoto, Michel van Eeten, "Evaluating Malware Mitigation by Android Market Operators," 9th USENIX Workshop on Cyber Security Experimentation and Test (USENIX CSET 2016), 2016.

Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, and Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, "IoTPOT: Analysing the Rise of IoT Compromises," 9th USENIX Workshop on Offensive Technologies (USENIX WOOT 2015), 2015.

Lukas Kramer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, Christian Rossow, "AmpPot: Monitoring and Defending Amplification DDoS Attacks," Proc. Research in Attacks, Intrusions, and Defenses (RAID15), Lecture Notes in Computer Science, Vol. 9404, pp. 615-636, 2015.