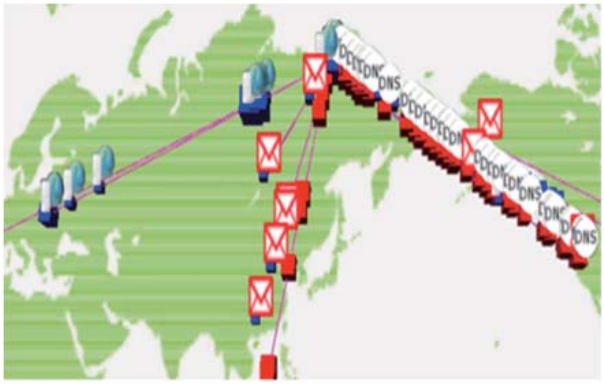
UNIT 7

情報・物理セキュリティ

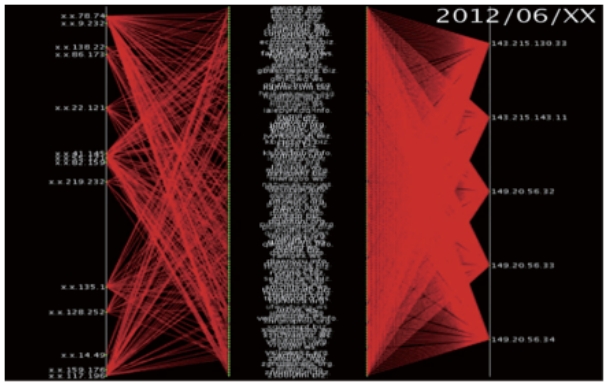
Research unit: Information and Physical Security

ネットワーク観測とマルウェア解析の融合による大規模サイバー攻撃の観測・分析・対策

最先端マルウェア対策技術、暗号技術、ソフトウェア・ハードウェア技術、システム技術、セキュリティ・エコノミクス等を駆使してITの進歩の一歩先を行くサイバーセキュリティ技術の研究を実施します。



A variety of important malware, including large scale P2P botnets, financial malware targeting domestic banks, and DDoS malware, are continuously monitored by our sandboxes that can now analyze 50 different malware samples in parallel.



Analysis of large-scale DNS cache server traffic enables us to find unusual use of domain names that may be caused by malicious online activities. Combined with the black domains obtained from the malware sandbox analysis, we identify malware infected hosts.

ユニット・メンバー

主任研究者　松本勉教授、Christopher Kruegel 上席特別教授（カルフォルニア大学サンタバーバラ校、米国）、中尾康二IAS客員教授（KDDI株式会社）

共同研究者　吉岡克成准教授、四方順司准教授、徐浩源教授、志村俊也講師

連携研究者　Engin Kirda IAS連携教授（ノースイースタン大学、米国）、William Robertson IAS連携助教（ノースイースタン大学、米国）
岩村誠IAS客員研究員（日本電信電話株式会社）、針生剛男IAS客員研究員（日本電信電話株式会社）、八木毅IAS客員研究員（日本電信電話株式会社）
秋山満昭IAS客員研究員（日本電信電話株式会社）、島成佳IAS客員研究員（NEC クラウドシステム研究所）、渡部正文IAS客員研究員（NEC クラウドシステム研究所）
角丸貴洋IAS客員研究員（NEC クラウドシステム研究所）、寺田真敏IAS客員研究員（株式会社日立製作所横浜研究所）
Michel van Eeten IAS連携教授（デルフト工科大学、オランダ）、武部達明 IAS客員研究員（KPMGコンサルティング株式会社）（予定）
山本大IAS客員研究員（株式会社富士通研究所）（予定）、川北将IAS客員研究員（日本電気株式会社）（予定）

研究協力者　Christian Rossow IAS招聘准教授（ザールラント大学、ドイツ）、Stevens Le Blond IAS招聘助教（マックス・プランク研究所、ドイツ）（予定）

松本勉

1986年3月東京大学大学院工学系研究科電子工学専攻博士課程修了，工学博士．同年4月横浜国立大学講師．2001年4月より同大学院環境情報研究院教授．ネットワーク・ソフトウェア・ハードウェアセキュリティ，暗号，耐タンパー技術，生体認証，人工物メトリクス等の「情報・物理セキュリティ」の研究教育に1981年より従事．1982年にオープンな学術的暗号研究を目指した「明るい暗号研究会」を4名で創設．2005年-2010年国際暗号学会IACR理事．1994年第32回電子情報通信学会業績賞，2006年第5回ドコモ・モバイル・サイエンス賞，2008年第4回情報セキュリティ文化賞，2010年文部科学大臣表彰・科学技術賞（研究部門）受賞．

主な研究プログラム

- 大規模サイバー攻撃の検知・分析・即応
- 標的型攻撃に対する実効性の高い対策
- 産業および電力制御システムセキュリティ
- 車載ネットワークセキュリティの解析と強化
- 組込みシステム向け耐タンパーソフトウェアの構成
- 人工物メトリクスとバイオメトリクス
- 暗号モジュールのフォールト攻撃の解析
- 情報理論的暗号理論
- 時間制御暗号理論

横浜国立大学 先端科学高等研究院
Institute of Advanced Sciences, Yokohama National University

Institute of Advanced Sciences Yokohama National University

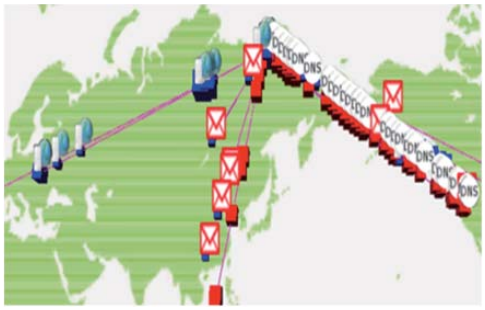
UNIT 7

Research Unit:

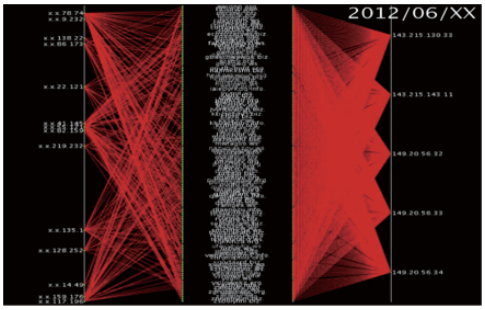
Information and Physical Security

Observation, analysis, and measure for information and physical security techniques by uniting network observation and malware analysis

This research unit conducts research on one-step-ahead information and physical security techniques, developing and implementing cutting-edge malware countermeasures, cryptography, software and hardware technologies, system technologies, security economics, etc.



A variety of important malware, including large scale P2P botnets, financial malware targeting domestic banks, and DDoS malware, are continuously monitored by our sandboxes that can now analyze 50 different malware samples in parallel.



Analysis of large-scale DNS cache server traffic enables us to find unusual use of domain names that may be caused by malicious online activities. Combined with the black domains obtained from the malware sandbox analysis, we identify malware infected hosts.

Unit Member

Principal Investigator

Professor **Tsutomu MATSUMOTO,** Distinguished YNU Professor **Christopher KRUGEL** (University of California, Santa Barbara, USA)
IAS Visiting Professor **Koji NAKAO** (KDDI CORPORATION)

Collaborating Investigator

Associate Professor **Katsunari YOSHIOKA,** Associate Professor **Junji SHIKATA,** Professor **Haoyuan XU,** Lecturer **Toshiya SHIMURA**

Adjunct Investigator

IAS Adjunct Professor **Engin KIRDA** (Northeastern University, USA), IAS Adjunct Assistant Professor **William ROBERTSON** (Northeastern University, USA)
IAS Visiting Researcher **Makoto IWAMURA** (NIPPON TELEGRAPH AND TELEPHONE CORPORATION)
IAS Visiting Researcher **Takeo HARIU** (NIPPON TELEGRAPH AND TELEPHONE CORPORATION)
IAS Visiting Researcher **Takeshi YAGI** (NIPPON TELEGRAPH AND TELEPHONE CORPORATION)
IAS Visiting Researcher **Mitsuaki AKIYAMA** (NIPPON TELEGRAPH AND TELEPHONE CORPORATION)
IAS Visiting Researcher **Shigeyoshi SHIMA** (NEC Corporation), IAS Visiting Researcher **Masafumi WATANABE** (NEC Corporation)
IAS Visiting Researcher **Takahiro KAKUMARU** (NEC Corporation), IAS Visiting Researcher **Masato TERADA** (Hitachi, Ltd.)
IAS Adjunct Professor **Michel van Eeten** (Delft University of Technology, The Netherlands), IAS Visiting Researcher **Tatsuaki TAKEBE** (KPMG Consulting Co., Ltd.)(Planned)
IAS Visiting Researcher **Dai YAMAMOTO** (Fujitsu Laboratories Ltd.)(Planned), IAS Visiting Researcher **Masaru KAWAKITA** (NEC Corporation)(Planned)

Visitor etc.

IAS Visiting Associate Professor **Christian Rossow** (Saarland University, Germany)
IAS Visiting Assistant Professor **Stevens Le Blond** (Max Planck Institutes, Germany) (Planned)

Tsutomu MATSUMOTO

Tsutomu Matsumoto is a professor of the Graduate School of Environment and Information Sciences, Yokohama National University and directing the Research Center for Information and Physical Security. He received Doctor of Engineering from the University of Tokyo in 1986. Starting from Cryptography in the early 80's, he has opened up the field of security measuring for logical and physical security mechanisms. Currently he is interested in research and education of Embedded Security Systems such as Smartcards, Network Appliances, Mobile Terminals, In-vehicle Networks, Biometrics, and Artifact-metrics. He is serving as a program officer of the JSPS Research Center for Science Systems, the chair of Japanese National Body for ISO/TC68 (Financial Services), and a core member of the Cryptography Research and Evaluation Committees (CRYPTREC). He was a director of the International Association for Cryptologic Research (IACR) and the chair of the IEICE Technical Committee on Information Security and served as an associate member of the Science Council of Japan (SCJ). He received the IEICE Achievement Award, the DoCoMo Mobile Science Award, the Culture of Information Security Award, the MEXT Prize for Science and Technology, and the Fuji Sankei Business Eye Award.

Research Program

- Detection, Analysis, and Response of Large-scale Cyber Attacks
- Countermeasures for Advanced Persistent Threats
- Industrial and Power Control Systems Security
- In-Vehicle Network Security Analysis and Enhancement
- Tamper-Resistant Software for Embedded Systems
- Artifact-metrics and Biometrics
- Analysis of Fault Injection Attacks to Cryptographic Modules
- Information-Theoretic Cryptography
- Timed Release Cryptography

横浜国立大学 先端科学高等研究院
Institute of Advanced Sciences, Yokohama National University

Institute of Advanced Sciences Yokohama National University