

Associate Professor	Daisuke Miyamoto	Laboratory Location	Faculty of Engineering Bldg.1 (Hongo) / ITC (Kashiwa2)	Research Area	Cybersecurity
---------------------	------------------	---------------------	--	---------------	---------------

Laboratory for cybersecurity. We study on cybersecurity with three perspectives of technical, human, and organizational factors and aim at secure cyber society for everyone.

Website: <https://www.iplove.net>

Email: [daisu-mi@nc.u-tokyo.ac.jp](mailto:daisu-mi@nc.u-tokyo.ac.jp)

**Research overview**

Internet became the social infrastructure and cyber society is closely linked to our everyday life. At the same time, cyber threats to the infrastructure are also increasing. There is no silver bullet to solve all threats, and hence, we are conducting practical research to improve security while thinking about risk avoidance and acceptance.

We are working on cybersecurity research from three perspectives of technical, human, and organizational factors. As for technical factors, we study such research topics that anti-malware, honeypot, DoS/DDoS mitigation, traffic analysis, and cyber range technologies. As for human factors, we study countermeasures against phishing and targeted email, and security aspects for situation awareness and decision theory. As for organizational factors, our activities involve incident response and collaboration, automated threat analysis, security education, and international standardization. Our research interests are not limited to the above keywords but are comprised of all elements in cyberspaces.

**Research topics**

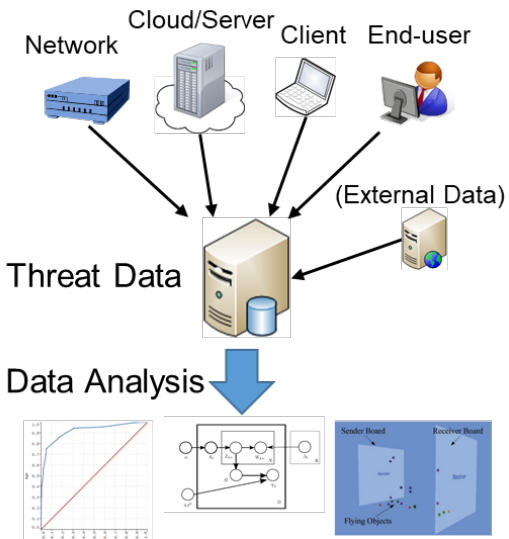
1. Countermeasures against Phishing Attacks

Phishing is a scam to deceive end users into disclosing their personal information by mimicking email and websites. Their content is designed to be look-alike the legitimate ones, and hence, users have to find security information regardless of the content. We try to recognize users' internal intention by their observable behavior and provide effective

protection for users who are going to be victims. The left-side figure shows eye movement of a user who focused on web content rather than security information. The right-side figure indicates our developed browser's extension which deactivates web forms until the user checked security information.

2. Multi-layer Threat Analysis

As well as users' behavior, we perform multi-layer threat observation and find anomaly to prevent our assets from being compromised. We have been leveraging machine learning for cybersecurity research, and our current challenge is a practical adaptation to mitigate cyber risks. It should be addressed such capabilities of understanding system components, analysis of cyber threat data, and implementing effective security actions. We are developing solutions with collaboration among researchers around the world.



The figure illustrates the concept of observing multilayer threats and explorative analysis with regard to the threat landscape. Our research interests involve data analysis, and cyber defense, and development of educational materials.

