4.日仏情報学連携拠点
"JFLI, Japanese-French laboratory for Informatics"

②	Next-Generation Internet: the EU-JST Project Necoma and the ANR Project Doctor 次世代インターネット：日本(JST)とEUの共同研究開発プロジェクトNECOMAおよびフランス国立研究機構(ANR)のDOCTORプロジェクト
NAME 名前	Pr. Phong Nguyen フォングエン教授
AFFILIATION 所属	Inria/JFLI-CNRS/U-Tokyo
TITLE 役職	Senior researcher
CONTACT 連絡先	http://www.di.ens.fr/~pnguyen/page_contact.htm
TITLE OF INVENTION OR SPECIALITY 発明の名称もしくは専門	
EXPLANATION 説明	NECOMA addresses the aspect of data collection, leveraging past and current work on the topic with the goal to expand these existing mechanisms and orient them towards threat data analysis. Second, it addresses threat data analysis not only from the perspective of understanding attackers and vulnerabilities, but also from the point of view of the target and victim, needing to protect itself in real-time and in the most efficient manner possible; this will be achieved through the development of metrics that allow to measure the impact of attacks on the protected infrastructure or endpoint. Third, it aims to develop and demonstrate new cyberdefense mechanisms that leverage these metrics for deployment and evaluation.These three aspects will be analyzed both from an infrastructure perspective (networks and largecomputing infrastructures) and endpoints (smartphones and browsers). The results of the NECOMA project will be showcased in demonstrators that will highlight the innovations of the project and prepare exploitation. Project DOCTOR Network operators are usually reluctant to adopt new networking stacks and functionalities because of the huge initial investment costs required and the important technical breakthrough needed to perform the migration from the traditional IP to new stacks in a single step. For example, with Information-Centric Networking (ICN), a novel promising networking paradigm that allows adapting networks to current content-centric usage patterns. The DOCTOR project advocates the use of virtualized network equipment (NFV), enabling the co-existence of IP and ICN stacks and the progressive migration of traffic from one stack to the other. This also raises two main challenges that will be addressed by the DOCTOR project: (1) the efficient deployment of emerging networks functions or protocols in a virtualized networking environment; (2) the monitoring and security of virtually deployed networking architectures, including the detection of attacks and their mitigation with appropriate counter-measures. NECOMAプロジェクト(Nippon-European Cyberdefense-Oriented Multilayer threat Analysis) では、欧州委員会 FP7 プログラム (Seventh Framework Programme) と総務省 戦略的国際連携型研究開発推進事業の日欧ICT 協調課題である「サイバー脅威に対する回復性強化のためのサイバーセキュリティ」に取り組んでいます（平成25年度～27年度）。 本プロジェクトでは、インターネットセキュリティに関する最先端の技術を有する奈良先端大、IIJ技術研究所、国立情報学研究所、慶應義塾大学および東京大学からなる日本側コンソーシアムと、ウイルス解析技術やサイバー事故対策の研究において実績を有するフランスIMT (Institut Mines-Télécom), 6cure SAS, スペイン Atos S.A., ポーランド NASK (Research and Academic Computer Network), ギリシャ FORTH-ICS (Foundation for Research and Technology Hellas - Institute of Computer Science) からなる欧州側コンソーシアムが4つの研究課題について国際共同研究を行っています。 NECOMA プロジェクトでは、これまでの不正コードの解析やネットワーク観測に関する研究成果や、クラウド等に対する新たな脅威の動向をふまえ、それらの知見をサイバー防御に応用します。データ獲得、解析、サイバー防御の各段階を連接し、それらをまたがる制御を行うことにより、DDoSやボットネット、フィッシング に対するサイバー防御の自動化を提案し実証実験をおこないます。さらに最新の脅威はマルウェアに加えてクラウド、Web、DNS等の様々な通信基盤を悪用することから、これらに対する横断的解析とコントロールに関する研究を実施します。
MERITS 利点	
PERFORMANCE 性能	
APPLICABLE FIELDS 応用分野	
FIGURES/DIAGRAMS 図表等	
Figure caption 図の説明	

③	Next-Generation Cryptography: Quantum-safe Cryptography, Lightweight Cryptography and Homomorphic Encryption 次世代暗号：量子計算でも破れない暗号(Quantum-safe Cryptography)、軽量暗号(Lightweight Cryptography)、準同型暗号(Homomorphic Encryption)
NAME 名前	Phong Nguyen フォングエン
AFFILIATION 所属	Inria/JFLI-CNRS/U-Tokyo
TITLE 役職	Senior researcher
CONTACT 連絡先	
TITLE OF INVENTION OR SPECIALITY 発明の名称もしくは専門	
EXPLANATION 説明	We present trends in cryptography: quantum-safe cryptography, lightweight cryptography and homomorphic encryption. Quantum-safe cryptography is cryptography resistant to quantum computers: public-key cryptography currently deployed is not. The NIST has recently announced an international competition for quantum-safe public-key standards. Lightweight cryptography proposes cryptographic tools for the Internet of Things. Homomorphic encryption targets cloud computing and big data, by allowing computations on encrypted data.
MERITS 利点	
PERFORMANCE 性能	
APPLICABLE FIELDS 応用分野	
FIGURES/DIAGRAMS 図表等	
Figure caption 図の説明	