第１回目　サイバーセキュリティー研究会　２年目のテーマとその概要
実施日：２０１８年5月３１日（木）
発表者：井上大介氏　NICT(情報通信機構サイバーセキュリティー研究室室長)

まず最初に研究会事務局である MIGA より２年目の研究会テーマとしてキャパシティービルディングモデル (Capacity Maturing Model) とセキュリティー人材の育成を取り上げた。前者は欧米の大学研究機関や NIST、ENISA などの政府機関のフレームワークを取り込んだ汎用的なモデルガイドラインで、サイバーセキュリティー政策の施行や運営上の成果などの一元的分析・評価として注目されている。セキュリティー人材の育成は、インフラ防護、企業運営、研究開発、国家防衛や犯罪対策など政策の幅広い部分において必要不可欠となっている。特にサイバーセキュリティーはインターネット技術に特有な継続的発達に起因しているため、データ解析や攻撃検知などの防止能力は技術面・政策面双方において高度なレベルで要求される。

MIGA から３０分ほど説明を行った後、NICT 井上室長に NICT におけるセキュリティー研究活動についての発表を行っていただいた。発表内容は以下の通り。

NICT におけるセキュリティー研究事業の紹介
（以下研究プログラム）
事故分析ネットワークシステム（NICTER）
DAEDALUS（Darknet など悪意ネットワークに対する警告通知プログラム）
NIRVANA/NIRVANA 改（ネットワーク分析システム）
WarpDrive（アクティブ型攻撃対応プログラム）
STARDUST（偽的ネットワーク増幅拡散プログラム）

また日本のサイバーセキュリティの現状における問題にも触れた。以下のような見解が上がった。

- 欧米では学会と産業界との研究・事業投資による相互関係が蜜（例えば大学研究者が研究目的として個人事業を立ち上げ業界投資する）であるのに対して、日本では業界からの一方通行かもしくは皆無に等しい。
- デジタル社会においてサイバー攻撃は日常的で攻撃は常に起こりうるものという共通認識があるのに対して、日本では攻撃させない・指一本触れさせないという潔癖感が根強いている。
- ２０２０年東京オリンピックに向けた ICT インフラ整備・防護や IoT 対応など国としての包括的対策が以前として不明。

発表後の参加者の意見など

日本国内における法的制約について

- 電気通信事業法により受信データの再活用などを目的とした採取や収集は原則として禁止されているため、１ユーザー又は民間事業がサイバー攻撃の検知先を見抜いたり攻撃の特徴を分析するといったことは事実上不可能。許可なく行うと刑法で罰せられてしまう。NICT に法的な例外措置が設けられ、近年国会にて承認されたのは特筆すべき事項で非常に羨ましい。
- 受信データの利用・活用に関する制約は、日本国内において自己防衛など能動的な攻撃分析や検知などができない要因となっている。このためサイバー攻撃を受ける国内企業の多くはデータ解析や情報収集、組織内外への報告などの面において事故対応の全面的なまずさを露呈している。
- セキュリティーにおける専門知識や実践はインターネットによる広がりと発達から常に継続的なアップデートが必要とされる。日本のセキュリティー観は従来の情報処理やシステムエンジニアに対する固定観点から未だに抜け切れておらず多様性や先見に乏しい。これは情報処理資格と現実とのギャップから見ても明らかである。
- 日本ではセキュリティ技術の人材が育ちにくい土壌を形成している。過去に干された人材が再生するべく新しく立ち上がった土壌に戻るというケースは殆ど見られない。
- NTT では国内による法的制約から、データ研究は欧米など海外に事業所を建てて行っている。国産企業でありながら日本にはないセキュリティー観を吸収できるのは、地元の同業他社団体や ISAC などと提携しながらネットワークを形成し、現地におけるデータ送受信やサイバー攻撃対応などの情報収集に務めているからである。