情報通信研究機構（NICT）の研究開発成果が社会に還元された事例
（セキュリティ・インシデント分析技術）

情報通信研究機構（NICT）の研究者による研究

【研究内容】

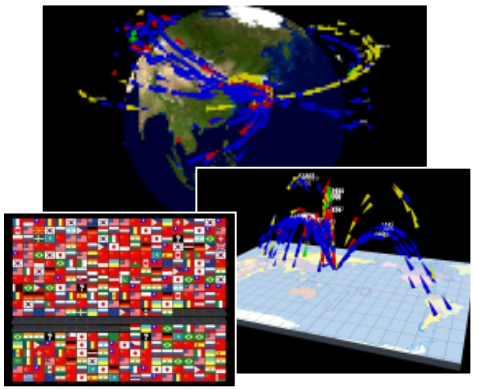
社会的影響の大きいサイバー攻撃によるインシデント（セキュリティ事故）をリアルタイムに検知・分析し、現状のインターネット環境および今後のネットワーク環境の安全・安全を実現するネットワークセキュリティ技術の研究開発。

インシデント分析センター
nicter

【研究成果】

◆大規模※1なインターネット観測とマルウェア※2の完全自動解析※3を行い、サイバー攻撃とそれを引き起こしているマルウェアの特定を可能とするインシデント分析センター「*nicter*」を開発。

◆サイバー攻撃のリアルタイムの「見える化（可視化）」を行い、少ない人的コストでの早期検知、高精度分析、実効的な対策を実現。



インシデントの「見える化」

【社会への適用】

◆Telecom-ISAC　Japan及び関連セキュリティベンダーとの連携を通して、攻撃・インシデント情報の共有と社会への情報展開を進める。また、ITU-T及びISO/IECなどの国際標準化活用にも寄与。

◆学術的にも日本のネットワークセキュリティ分野を牽引し、中心的存在。

◆今後は、次世代インターネットIPv6やホームネットワークなどのセキュリティ確保の研究開発を進めるとともに、日本全国規模のネットワーク観測網の構築を目指す。

※1　国内最大、国際的にも最大級のIPアドレス観測規模。
※2　マルウェア・・・コンピュータウィルスに代表される悪意をもったソフトウェアの総称。
※3　自動解析・・・従来は、マルウェアの個々の解析を専門家の知識・経験により実施していた。