発達障害の特性別評価法（MSPA）の社会実装

京都大学　大学院人間・環境学研究科　教授　**船曳　康子**

科学研究費助成事業（科研費）

テーラーメイド型支援に向けた広汎性発達障害の行動・認知特性でのサブタイプ分け（2007–2008　特別研究員奨励費）

発達障害の特性分布の掌握と多特性複合の客観的指標の開発（2010–2013　若手研究（B））

・厚生労働省科学研究費（障害者対策総合研究事業：精神障害分野）「発達障害者の特性別適応評価用チャートの開発」（2009–2011）
・科学技術振興機構　社会技術研究開発センター（RISTEX）：「発達障害者の特性別評価法（MSPA）の医療・教育・社会現場への普及と活用」(2014–2017)

発達障害とは、先天的な脳機能の特性により偏った言動が出てしまうなど、社会生活上の困難を伴う状態である。病気とは異なり、周囲の理解やサポートにより支障を軽減することが可能であり、早期の支援が重要となる。しかしながら、発達障害には自閉スペクトラム症、注意欠如・多動症、学習障害など様々なタイプがあるのみならず、その発現も個人差が大きく、支援の前提となる障害の評価を適正に行うことが困難という課題があった。

こうした背景から、発達障害者の認知機能についての基礎研究や評価手法の検討を積み重ね、その成果を医療や教育の現場で実装するため、発達障害者の持つ生活困難度（要支援度）を認知・行動特性別に多面的に評価し、一目で分かりやすく図示した評価法MSPA（Multi-dimensional Scale for PDD and ADHD）を作成した。

さらに、教育関係者との協働によるMSPAを活用してもらうためのマニュアル作りや、医療機関や学会への提案・働きかけなどにも取り組んだ。こうした活動の結果、2016年4月1日よりMSPAが保険収載となった。今後、医療・教育・自治体等の機関における発達障害者への支援において大きく貢献することが期待される。

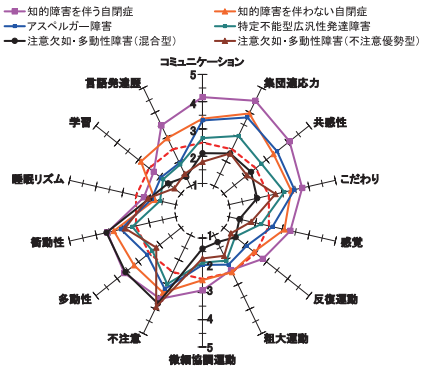

図１　診断（旧）ごとの平均値
・どの診断でも不注意の困りが多い
・発達障害の下位分類は類縁である可能性を示唆

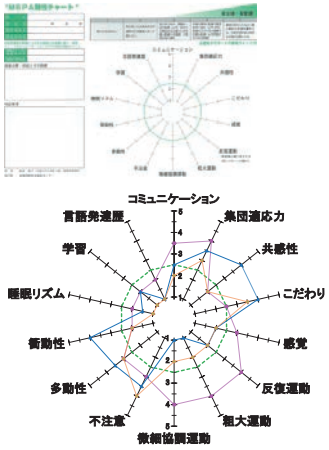

図２　MSPAの完成（上図：イメージ図）
下図は自閉スペクトラム症の３例で、同じ診断でも特性は種々であることを示す

マルウェア分析技術を活用した新たなセキュリティ脅威の発見

横浜国立大学　大学院環境情報研究院　先端科学高等研究院　准教授　**吉岡　克成**
［お問い合わせ先］　TEL：045–339–3690　E-MAIL：yoshioka@ynu.ac.jp

科学研究費助成事業（科研費）

マルウェア対策導出の自動化に関する研究（2010–2011　若手研究（B））

実効性の高い標的型攻撃対策に関する研究（2012–2014　若手研究（A））

総務省「国際連携によるサイバー攻撃予知・即応技術の研究開発」（2011–2015）
NICT「Web媒介型攻撃対策技術の実用化に向けた研究開発」（2016–2018）

インターネットの普及に加え、IoTなどサイバー空間と実空間の一体化が急速に進展しつつある。そのような環境の中で、個人や組織を狙ったサイバー攻撃の脅威は極めて深刻なものとなっている。

サイバー攻撃に対抗するためには、マルウェア（不正プログラム）の振る舞いを観測・分析し、これを検知・遮断・駆除する技術が不可欠である。このため、様々なマルウェアを効率的に分析する技術と、それに基づくサイバー攻撃の検知等を行う対策技術の研究を実施した。

●マルウェアからの攻撃を高精度で検知・分類するツールは情報通信研究機構（NICT）が運用する対サイバー攻撃アラートシステム「DAEDALUS」（ダイダロス）に導入されたほか、NICTより技術移転を受けたクルウィットにより「SiteVisor」として商用化されており、我が国発のセキュリティ技術の普及に貢献している。

●大規模サービス妨害攻撃を早期検知し，アラートを発行するシステムを構築し、国内のインターネットサービスプロバイダや企業等に情報提供することで、インターネットの安定運用に貢献している。

●PCやスマートフォンだけでなく、家電や重要施設の機器に感染する新たなマルウェア（IoTマルウェア）の脅威を世界に先駆けて発見し、詳細な情報収集、分析を行い、世界20か国、50以上の組織に情報提供を行い、対策に貢献している。

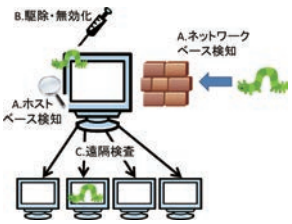

図１　科学研究費により実施したマルウェア分析・対策導出技術の概要

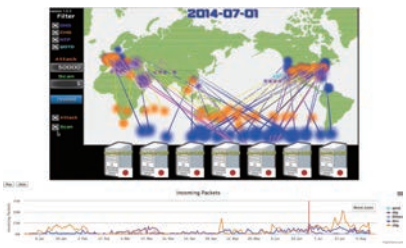

図２　大規模サービス妨害攻撃の早期検知

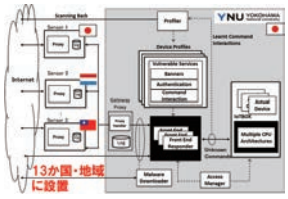

図３　IoT機器へのサイバー攻撃の観測機構

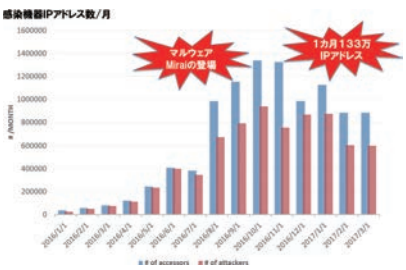

図４　IoT機器の大量マルウェア感染の発見