NICT サイバー研究所の役割

NICT サイバーセキュリティ研究所

急増かつ巧妙化するサイバー攻撃から我が国を守るため、NICT の中立性を最大限に活用し、産学との緊密な連携によりサイバーセキュリティ研究開発の世界的中核拠点を目指す

サイバーセキュリティ研究室

- サイバー攻撃という社会課題の解決に資する、より能動的・網羅的なサイバー攻撃観測・分析・蓄積・共有技術の研究開発
- サイバーセキュリティの研究開発を加速し、サイバー演習等にも活用できるセキュリティ・テストベッド技術の研究開発

セキュリティ基盤研究室

- 新たな機能を備えた機能性暗号技術や軽量暗号・認証技術の研究開発 及び暗号技術の安全性評価
- パーソナルデータの利活用に貢献するためのプライバシー保護技術の研究開発

ナショナルサイバートレーニングセンター

サイバーセキュリティ技術を生かし、実践的サイバー防御演習（CYDER）の開発・実施

（国立研究開発法人情報通信研究機構　サイバーセキュリティ研究所　Web ページより）

公的研究機関として総務省所管の国立研究開発法人である NICT（情報通信研究機構 :National Institute of Information and Communications Technology）は、電磁波や、AI、未来 ICT などの様々な研究をする組織が分かれて存在していますが、その一つに有名なサイバーセキュリティ研究所があります。
その中でも、サイバーセキュリティ研究室では、無差別型攻撃や標的型攻撃など多様化したサイバー攻撃の情報を大量に集約・分析し、サイバー攻撃対策の自動化を目指す技術の研究開発を行っています。
サイバーセキュリティ研究室 が行っている NICTER プロジェクトは、インターネット上で起こる大規模攻撃への迅速な対応を目指したサイバー攻撃の観測、分析、対策のシステムを用いて、ダークネットや各種ハニーポットによるサイバー攻撃の大規模観測や、その原因であるマルウェア等の分析を実施しています。
NICTER（Network Incident analysis Center for Tactical Emergency Response）は、マクロ解析としてのサイバー攻撃観測を行うネットワーク観測・分析システムから得られた現象と、ミクロ解析としてのマルウェア検体収集からマルウェア自動解析システムから得られる原因を、相関分析システムへつなぎ、それらの結果から対策システムでインシデントアラートを発行することにより、政府・官公庁、インターネットプロバイダのみならず、一般ユーザに情報提供をしています。
そして、NICTER による観測・分析結果の一部は、nicterWeb 上で一般公開しており、地図上にグラフィカルな動きで、どの国からどれくらい攻撃を受けているのかなど、一目瞭然にサイバーアタックの状況がわかります。
NICTER プロジェクトでは、企業や組織に割り当てられているものの、実際には使われていない IP アドレス群であるダークネットを利用して、怪しい通信を観測しています。ダークネットへの通信は、使われていない IP アドレスなので、正常な通信が届くことはほぼないため、マルウェアによる通信や、調査目的の通信である可能性が極めて高いので、パケットの送信元の情報やポート番号、その内容などを分析してサイバー攻撃の兆候や、傾向などが把握できます。
NICTER で構築した大規模ダークネット観測網を活用した対サイバー攻撃アラートシステムの DAEDALUS (Direct Alert Environment for Darknet And Livenet Unified Security) は 、NICTER のセンサを設置可能な大学等の組織には、無償提供しています。
NICTER 観測レポートからは、年間総観測パケット数の統計などサイバー攻撃が年々激しくなっていることがわかります。