3.13　サイバー攻撃対策総合研究センター

センター長（兼務）　　今瀬　真

【センター概要】

近年、APT（Advanced Persistent Threat）による攻撃*等の巧妙化・高度化する新たなサイバー攻撃の脅威が社会問題化しており、その対応が国家的な喫緊の課題となっている。本対策において、NICTが国内外で主導的な役割を果たすべく、平成25年4月からサイバー攻撃対策総合研究センターの活動を本格化させ、情報セキュリティに関連する研究所の横断的な連携を強化しつつ、テストベッドネットワークを活用した実践的な対策研究を加速化する。これにより、現状、解析自体が困難なAPTによる攻撃等の新たなサイバー攻撃への対応基盤を確立し、我が国の情報セキュリティ確保のための総合的な対策手法の導出を目指す。

*APTによる攻撃とは、特定の相手にねらいを定め、その相手に適合した方法・手段を適宜用いて侵入・潜伏し、数か月から数年にわたって継続するサイバー攻撃のこと。

目的・目標

◆ 国内の英知を結集したサイバーセキュリティ研究開発拠点を構築
- ✓ 産学から、マルウェア解析技術、サイバーインテリジェンス等の各分野のトップクラスの人材を集積し、先鋭的な研究集団を組織

◆ 新たなサイバー攻撃への実践的かつ根本的な対策技術を確立
- ✓ 単なる学術研究ではなく、今まさに生じている攻撃を、実ネットワークへの影響を最小限にしつつ、根本的解決を目指す

◆ 研究開発成果の速やかな社会展開を実施
- ✓ 世界をリードする日本発の技術を開発し、官公庁・重要インフラ等への社会実装、技術移転による製品・サービス化を目指す

◆ 欧米、アジア地域とのサイバーセキュリティ国際連携を推進
- ✓ 諸外国との連携による観測網の広域化、情勢分析能力・判断能力の強化を目指す

サイバー攻撃対策総合研究センターでは、具体的に以下に示すような研究開発を実施している。

① サイバー防御戦術研究室
　NICTERで培った基盤技術群を活用し、APTによる攻撃等に対する能動的かつ根本的な防御技術を確立・実現

② サイバー攻撃検証研究室
　StarBEDとその基盤技術群を活用し、攻撃・防御の検証用模擬環境を用いたAPTによる攻撃等の実践的検証を実現

【主な記事】

サイバー攻撃対策総合研究センターにおける平成26年度の主なトピックスを以下に示す。なお、詳細については、それぞれの研究室の報告を参照いただきたい。

（1） サイバー防御戦術研究室

- サイバー攻撃統合分析プラットフォーム「NIRVANA改」について、複数種のアラートの横断的な分析を実現する相関分析エンジンのプロトタイプを開発するとともに、Interop Tokyo 2014において国内外のセキュリティ関連企業複数社と連携して、多様なセキュリティアプライアンス群からのアラート集約の実証実験を実施
- 膨大なライブネットのリアルタイム分析を可能にするライブネット高速分析基盤の開発を進め、大容量オンメモリ処理によりNICTのライブネットにおいて20万パケット毎秒のリアルタイム処理性能を実証
- NIRVANA改をベースに、サイバー模擬攻防戦“CTF”（Capture The Flag）をリアルタイムに視覚化す

る専用エンジン“NIRVANA 改 SECCON カスタム Mk-II”を開発し、日本最大規模の CTF 大会である SECCON CTF 2014 決勝戦に導入

(2) サイバー攻撃検証研究室

- 企業内システム利用者のマウス及びキーボード入力を記録し、その再現を可能とするシステム「Puppet Master」を開発
- 安価な PC 群を利用してソフトウェアにより広帯域ネットワークトラフィックのリアルタイム解析とその内容を保存するシステム「SF-TAP」を開発
- Hardening や CYDER、SecCap などのサイバー人材育成プログラムへの技術や知見の協力、演習環境の提供