3.12　サイバー攻撃対策総合研究センター

研究センター長　　今瀬　真

【センター概要】

近年、APT（Advanced Persistent Threat）による攻撃(注)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。

（注）APT による攻撃とは、特定の相手に狙いを定め、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 25 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されたい。

（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」のプロトタイプを開発し、Interop Tokyo 2013 へ出展
- 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プロトタイプを開発し、NICT において実証
- アンチウイルスソフト（ホストベースの侵入検知）とライブネット分析（ネットワークベースの侵入検知）を協働させる NIDS-HIDS 連携システムを構築
- サイバー攻撃検証研究室と共同で、StarBED 上に組織内ネットワークを簡易的に模擬した模擬ネットワーク環境を構築し、標的型攻撃の一連の流れを実際に再現する模擬攻防実験を実施
- NIRVANA 改をベースに、サイバー攻撃の対処能力の強化を目的とした競技 CTF の攻防戦をリアルタイムに可視化する専用エンジン「NIRVANA 改 SECCON カスタム」を開発し、SECCON 2013 の決勝戦の可視化を実施

(2) サイバー攻撃検証研究室

- サイバー防御戦術研究室と連携し、組織内で一般的に動作していると考えられる Web サーバ、Proxy サーバ等の要素とそのトポロジを検討し、実際に仮想ノードを利用して典型的な組織ネットワークを再現し、いくつかのマルウェアを動作させ、その挙動を解析
- StarBED でのネットワーク実験環境の運用ノウハウを活かしつつ、サイバーセキュリティ実験にも対応するためのモジュールの検討を行い、それらモジュール群の接続のための通信プロトコルの設計及ライブラリを構築
- IT-Keys、Hardening One Remix、CYDER 等のサイバー演習への協力、演習環境の提供