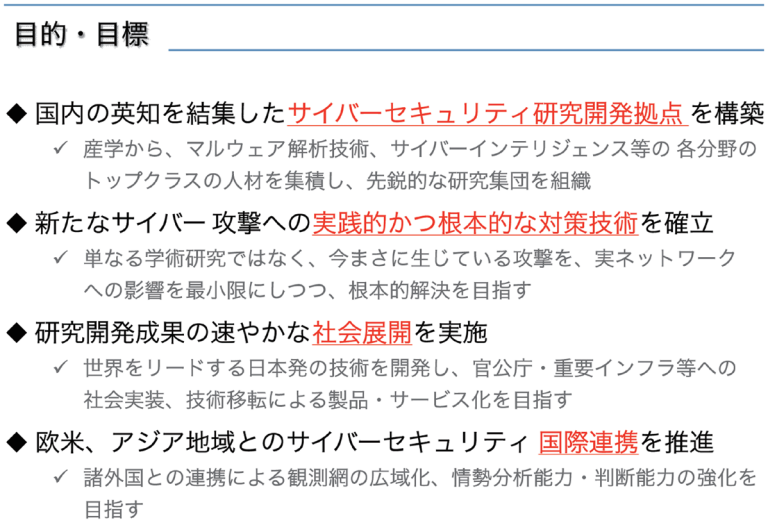
3.13　サイバー攻撃対策総合研究センター

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[*1]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。



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27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、国産アンチウイルスソフトからの情報を収集するエンドホスト連携機能や、ファイヤーウォール、スイッチ、ルータ、OpenFlowスイッチ等に対する自動防御機能を開発し民間企業への技術移転を開始。Interop Tokyo 2015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）大会をリアルタイムに視覚化する専用エンジン“AMATERAS[*2]”を開発し、2015年に日本初の女性限定のCTF大会である「攻殻CTF」に導入。さらに、SECCON CTF 2015にも、Attack&Defense専用に「AMATERAS」をバージョ

ンアップし導入。

(2)　サイバー攻撃検証研究室

・サイバーレンジ環境を構築するためのミドルウェア Alfons と Windows 上で利用者の挙動を摸倣する Puppet Master の連携を可能とし、SDN 技術を用いて、任意の場所のトラフィック情報監視機構を開発。統合的な実験環境構築を可能にした。
・PC 群利用のソフトウェアで、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」を用い、DNS/HTTP の解析エンジンを開発。プライバシ情報の取得状態を可視化。
・サイバー人材育成プログラムの技術として、環境に存在する利用者を摸倣するための Web クローラ、メール模擬システムを構築。環境のリアリティを向上。

*1 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。
*2 Advanced Multi-Actor Tactical Exercise Real-time Analysis System: Prototype Version 0