公益財団法人 セコム科学技術振興財団

（平成 23 年度～平成 27 年度）

次世代ネットワークにおける持続的標的型攻撃の検出手法の開発

Development of Detection Methods for Advanced Persistent Attacks on the Future Network

2016 年 6 月

研究代表者

国立情報学研究所　教授　高倉 弘喜

National Institute of Informatics, Professor, Hiroki Takakura

サイバー攻撃は日々巧妙化し、従来からの対策技術では、攻撃を防御するだけでなく攻撃による侵入に気づくことも難しくなった。また、IoT など新たなインターネット技術の応用が広がりつつある中、パソコンやサーバを想定したサイバー攻撃対策では十分とは言えなくもなった。さらに、組織内に接続される情報機器も爆発的に増大することを考えると、従来のようにすべての通信を一元監視することは非現実的になると考えられる。

この問題を解決するため、異種多様な機器が接続される次世代ネットワーク環境において、隠密裏に活動するサイバー攻撃の存在を察知する技術、その察知をトリガーとしてサイバー攻撃の被害状況を把握する技術、さらに被害拡大を抑えつつ運用を継続する技術が必須になる。また、様々な機器が相互認証しあうことで、異常な挙動を示す機器を炙り出す技術も必要になる。

本研究では、これらの課題を以下の方法で解決することを試みた。

- 次世代ネットワークとして HEMS(Home Energy Management System)を題材とした、不正通信検知アルゴリズム
- マルウェアによる通信挙動の解析によるマルウェア分類アルゴリズム
- 次世代ネットワークで標準になると想定される自動 IP アドレス設定環境における情報機器追跡システム(例、SLAAC, StateLess Address AutoConfiguration)
- 平常時のネットワークの状況を把握し、不要な区間の通信を遮断もしくは監視することで異変察知と被害拡大抑制を可能とするネットワーク構築支援システム
- 必要最小限の秘密情報の相互開示による機器間の相互認証プロトコル

これらの技術の大部分については、研究室や大学規模での実データによる性能評価は完了している。今後、大規模な学術ネットワークでの運用実験によって、その有効性を検証し、引き続き改良を続けていく。