日欧協調によるマルチレイヤ脅威分析およびサイバー防御の研究開発（13802170）

NECOMA: Nippon-European Cyberdefense-Oriented Multilayer threat Analysis

研究代表者

門林雄基　奈良先端科学技術大学院大学　情報科学研究科

Youki Kadobayashi　Graduate School of Information Science, Nara Institute of Science and Technology

研究分担者

櫨山寛章 †　岡田和也 †　長健二郎 ††　Romain Fontugne††　福田健介 †††　Saran Tarnoi†††

加藤朗 ‡　関谷勇司 ‡‡　宮本大輔 ‡‡　田崎創 ‡‡　石原知洋 ‡‡　飯村卓司 ‡‡

Hiroaki Hazeyama†　Kazuya Okada†　Kenjiro Cho††　Romain Fontugne††　Kensuke Fukuda†††

Saran Tarnoi†††　Akira Kato‡　Yuji Sekiya‡‡　Daisuke Miyamoto‡‡　Hajime Tazaki‡‡

Tomohiro Ishihara‡‡　Takuji Iimura‡‡

†奈良先端科学技術大学院大学　††株式会社インターネットイニシアティブ技術研究所

†††国立情報学研究所　‡慶應義塾大学　‡‡東京大学

†Nara Institute of Science and Technology　††IIJ Innovation Institute

†††National Institute of Informatics　‡Keio University　‡‡The University of Tokyo

研究期間　平成 25 年度～平成 27 年度

概要

本研究開発では、これまでの攻撃コードの解析やネットワーク観測に関する研究成果や、クラウド等に対する新たな脅威の動向をふまえ、それらの知見をサイバー防御に応用した。脅威データ獲得、解析、サイバー防御の各段階を連接し、それらをまたがる制御を行うことにより、DDoS やボットネット、フィッシングに対するサイバー防御の自動化を提案し実証実験を行った。さらに最新の脅威はマルウェアに加えてクラウド、Web、DNS 等の様々な通信基盤を悪用することから、これらに対する横断的解析と制御に関する研究を実施した。

１．まえがき

昨今、サイバー攻撃は、インターネットインフラ自体を揺るがすほど大規模になってきている。これらの攻撃をネットワークインフラである ISP（Internet Service Provider）、IXP（Internet eXchange Point）のみで防御、抑制することが困難となってきている。また、昨今のサイバー攻撃は広範囲にわたって発生し、単一組織のみで攻撃を防ぐことは容易ではない。

そこで本研究開発では、インターネットインフラを支える ISP や IXP とエンドポイントにあたる家庭、事業者間での協調によるサイバー防御体制の実現を目標とする。インフラとエンドポイントがそれぞれ自律的にサイバー攻撃に対する情報提供と共有を行うことで、インターネットインフラ全体に渡るサイバー攻撃の抑制、緩和を図る。そのためには、インフラ、エンドポイントからの情報収集、サイバー脅威の検知、脅威情報の共有、防御・緩和手法の連携が必要不可欠である。

NECOMA は、以下に示す 3 項目を目標とした。

1. 実用的なサイバー脅威の知識管理を行う手法を開発する。少なくとも 3 つ以上の新たな指標を定義し、インターネット上の脅威の状態を測定し、サイバー防御機構の高度化に用いる。
2. 高度なサイバー防御機構を開発する。少なくとも 3 つ以上の新しいメカニズムを開発し、事例実験を通じて実証を行う。
3. 脅威情報からその情報に基づいた対応までの情報流通のパイプラインを完成させる。ICT インフラの回復性を向上させるため、サイバー脅威から対策までの橋渡しを行う。

これらの目標を達成することにより、我々はプライバシー保護、スマートフォンセキュリティ、新世代のネットワークにおけるセキュリティ、セキュリティポリシー、そして回復性ある防御機構に対して大きな影響を与えることを目指した。また、NECOMA の研究開発を通じて日欧の研究開発のつながりをより強固なものにすることに大きく貢献することを目指し、研究開発を行った。

NECOMA では、著者らが所属する日本側 5 組織に欧州の IMT（フランス）、FORTH（ギリシャ）、ATOS（スペイン）、NASK/CERT-Polska（ポーランド）、6cure（フランス）の 5 組織を加えた合計 10 組織の体制で研究開発を遂行した。

２．研究開発内容及び成果

NECOMA では、4 つの研究開発課題を設定し組織間で連携しつつ研究開発に取り組んだ。

課題 1：サイバー脅威の多階層的な観測に関する研究では、ネットワークインフラからエンドポイントにいたる多種多様なデータ収集を行った。この過程で、大規模データ蓄積／解析基盤である MATATABI（図１）を実装し、3 年間で総計 24 テラバイトに登るデータを収集した。

課題 2：サイバー攻撃に対する回復性あるデータ解析では、課題 1 により収集されたサイバー脅威データを活用した脅威検知・解析手法の研究開発を行った。解析では、sFlow/netFlow といったネットワークバックボーントラフィック、未使用 IP アドレスに対する通信を観測したダークネットトラフィックデータ、Domain Name System (DNS) サーバに対する問い合わせ記録、SPAM メール等を利用した各種解析・検知を行った。合計 16 種類のデータ解析手法の提案と実装、評価を行った。

課題 3：サイバー防御に関する研究では、攻撃検知結果を元にしてインフラ、エンドポイントにて攻撃を防御、緩和する方式の研究開発を行った。インフラにおける防御では、MPLS, SDN を活用したキャリア通信網、企業ネットワークおよび IX における DDoS 緩和機構、クラウド環境

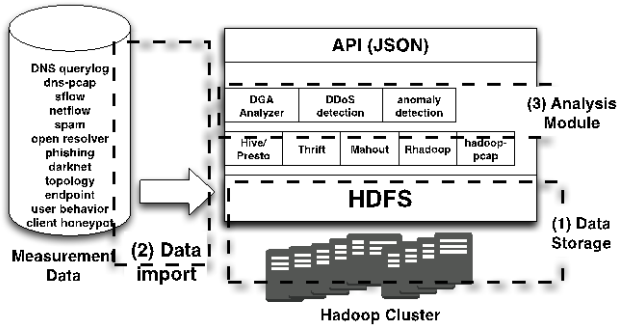

図 1 MATATABI の概要

における防御機構を開発した。エンドポイントでは、個人端末におけるフィッシング対策、OpenFlow と無線アクセスポイントを用いてスマートフォン防御機構を開発した。

課題 4：実証実験では、課題 1、課題 2 および課題 3 の研究開発成果を統合した複数の事例を作成し、実験を行った。各事例では、防御機構だけに留まらずデータ収集（課題 1）、解析・検知（課題 2）、共有（課題 3）、防御（課題 3）間の連携（パイプライン）を取り込んだものとなっている。本課題の成果は報告書としてまとめるとともに、デモビデオを作成し合計 9 件のビデオを YouTube (http://www.necoma-project.eu/videos/) 上で公開した。課題 4 では本プロジェクトの目標であるサイバーセキュリティのパイプラインを課題 1 から課題 3 の成果を元に複数構築し、研究開発成果の有用性を十分に示した。

３．今後の研究開発成果の展開及び波及効果創出への取り組み

NECOMA では、本研究開発で得られた成果の内 17 件が通信事業者をはじめとする産業界で応用可能と考えている（成果物 5.6 に記載 : http://www.necoma-project.eu/publications）。課題 1、2 で開発した大規模データ解析基盤（MATATABI）は、本プロジェクトの参加組織内で導入に向けて動いており、実用段階にあると考える。また、SDN/MPLS を利用した各種 DDoS 防御技術は、通信事業者、IX での導入が期待できる。

成果展開にむけて、研究開発期間中の 2015 年 1 月と 2016 年 3 月に日本のセキュリティに関わる企業、研究所、専門機関の関係者を招いたリエゾン会合を開催した。各会合には、総務省のサイバーセキュリティ関連の委託事業である ACTIVE, CYDER, PRACTICE からもご参加いただいた。会合では、欧州側パートナーを国内の専門家に紹介し、研究開発成果の発表、および参加者との議論を行った。

さらに、産業界に研究開発成果を還元することを目的として、2014 年 6 月と 2015 年 6 月に千葉県の幕張メッセにて開催された国内最大規模の情報通信技術の展示会である INTEROP Tokyo において、課題 3 で開発した SDN IX のプロタイプを提供し動態展示を行った。また、課題 1 から課題 3 にて開発したソフトウェアのソースコード 7 件を GitHub（https://github.com/necoma）にて公開した。これによりプロジェクト外部の技術者や研究者が自由に開発成果を活用可能となっている。

４．むすび

NECOMA では、3 年間にわたり日欧の参加組織間で綿密に連携しプロジェクトを遂行し目標を達成した。また、研究開発過程で合計 8 名の研究者・学生が日欧双方の研究機関に数ヶ月滞在し人材交流も実施した。今後は、プロジェクトを通して得られた欧州組織との関係を維持し、共同での研究開発プロジェクトや互いの人材交流を継続する。

【誌上発表リスト】

[1] Johan Mazel, Pedro Casas, Romain Fontugne, Kensuke Fukuda, and Philippe Owezarski, "Hunting Attacks in the Dark: Clustering and Correlation Analysis for Unsupervised Anomaly Detection", International Journal of Network Management pp283-305 vol.25 issue 5 Wiley (2015 年 5 月)

[2] Kriangkrai Limthong, Kensuke Fukuda, Yusheng Ji, Shigeki Yamada. "Unsupervised learning model for real-time anomaly detection in computer networks", IEICE Transactions on Information and Systems pp2084-2094 vol.E97-D no.8 IEICE 2014（2014 年 8 月）

[3] Sirikarn Pukkawanna, Hiroaki Hazeyama and Youki Kadobayashi, and Suguru Yamaguchi. "Detecting Anomalies in Massive Traffic Streams based on S-transform Analysis of Summarized Traffic Entropies", IEICE Transactions on Information and Systems March 2015（2015 年 3 月）

【国際標準提案リスト】

[1] ITU-T, Study Group 17, Question 4: X.cogent, Design considerations for improved end-user perception of trustworthiness indicators, Daisuke Miyamoto, Youki Kadobayashi, 提案: April 2015, 修正: March 2016.

[2] ITU-T, Study Group 17, Question 4: X.metric, Metrics for Evaluating Threat and Resilience in Cyberspace, Daisuke Miyamoto, Youki Kadobayashi, 提案: March 2016.

[3] IETF MILE Working Group, Internet Draft: MILE Implementation Report. Chris Inacio, Daisuke Miyamoto, 提案:July 2014, 修正: November 2014, March 2015, October 2015.

【参加国際標準会議リスト】

[1] ITU-T Study Group 17、ジュネーブ（スイス）、2015 年 4 月、2016 年 3 月

[2] IETF 94、横浜（日本）、2015 年 11 月

[3] IETF 93、プラハ（チェコ）、2015 年 7 月

【受賞リスト】

[1] Jianxing Chen, Romain Fontugne, Akira Kato, Kensuke Fukuda, Best paper award, In Proceedings of AINTEC2014, “Clustering Spam Campaigns with Fuzzy Clustering”, 2014 年 11 月 26 日

【報道掲載リスト】

[1] 「SDN ソフトウェアスイッチ Lagopus が Interop Tokyo 2015 の ShowNet の中核に採用」、日本電信電話株式会社　プレスリリース、 2015 年 6 月 8 日

[2] SDN Software Switch "Lagopus" Showcased in ShowNet at Interop Tokyo 2015, CNN Money, 2015 年 6 月 16 日

[3] “Droid malware cloak outwits Google Bouncer and friend”, The Register, 2014 年 5 月 13 日

【本研究開発課題を掲載したホームページ】

[1] 日本側：http://www.necoma-project.jp/

[2] 欧州側：http://www.necoma-project.eu/