FP7-ICT-2013-EU-JAPAN
ICT-2013.10.1(c): Cybersecurity for improved resilience against cyber threats

SEVENTH FRAMEWORK PROGRAMME

Ministry of Internal Affairs and Communications

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)

研究代表者：門林 雄基 (奈良先端科学技術大学院大学)

代理発表：関谷 勇司 (東京大学)

研究分担者

櫨山 寛章 (奈良先端科学技術大学院大学)
岡田 和也 (奈良先端科学技術大学院大学)
長 健二朗 (株式会社インターネットイニシアティブ技術研究所)
福田 健介 (国立情報学研究所)
加藤 朗 (慶應義塾大学)

関谷 勇司 (東京大学)
宮本 大輔 (東京大学)
田崎 創 (東京大学)
石原 知洋 (東京大学)
飯村卓司 (東京大学)

2016年10月4日

研究開発内容

収集

課題1：サイバー脅威の多階層的な観測に関する研究

1) **サイバー攻撃のデータを多階層から観測するシステムの設計**
   サイバー攻撃のデータをインフラ・エンドポイントの多階層から観測し、収集・変換及び共有を行った。
2) **ネットワークインフラにおけるサイバー攻撃データ収集**
   サイバー攻撃の全容を解明するため、攻撃トラフィックの傾向を示すフロー統計情報、DNSサーバログ、ダークネットや早期検知システムなどから攻撃関連のデータを収集した。
3) **エンドポイントにおけるサイバー攻撃データ収集**
   マルウェアの挙動やフィッシングのような悪性ウェブサイトに引き寄せられるエンドユーザの傾向を分析し、攻撃関連データを収集した。

解析

課題2：回復性を指向した脅威分析

1) **データ集約及び分析アルゴリズムの開発**
   サイバー攻撃のパターンや傾向を抽出し、インシデントを解明するためのデータ解析を行った。
2) **自動的なレーティング及び分類アルゴリズムの開発**
   収集されたデータを基に解析を行い、サイバー脅威の検出・分類を行った。
3) **データ解析基盤の設計及び開発**
   サイバー脅威の解析や、関連するデータとの相関性を解析する基盤を設計した。

防御

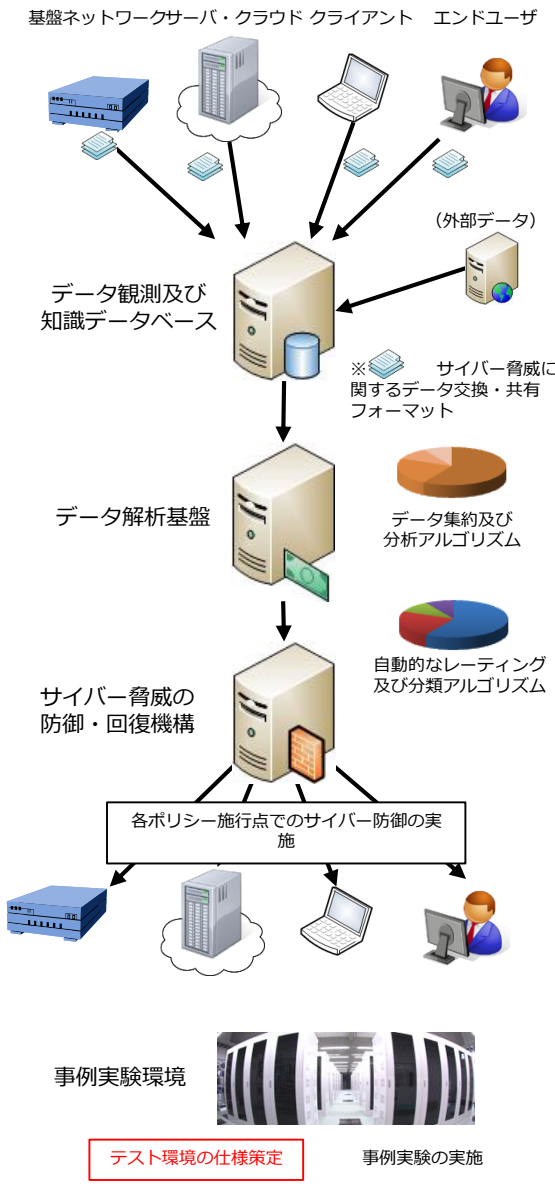
課題3：サイバー防御に関する研究

1) **既存のポリシー施行点に関する調査**
   サイバー攻撃に対する回復性ある防御機構を構築する場所について、その能力と特性を明らかにした。
2) **サイバー脅威情報交換に関する研究**
   サイバー防御のために適した脅威情報共有のためのデータフォーマットと API を構築した。
3) **ネットワークインフラにおける回復機構の開発**
   SDN 技術を用いてサイバー脅威に対するネットワークインフラにおける回復機構を開発した。
4) **エンドポイントにおける回復機構の開発**
   エンドポイントに適したサイバー脅威の防御機構を開発した

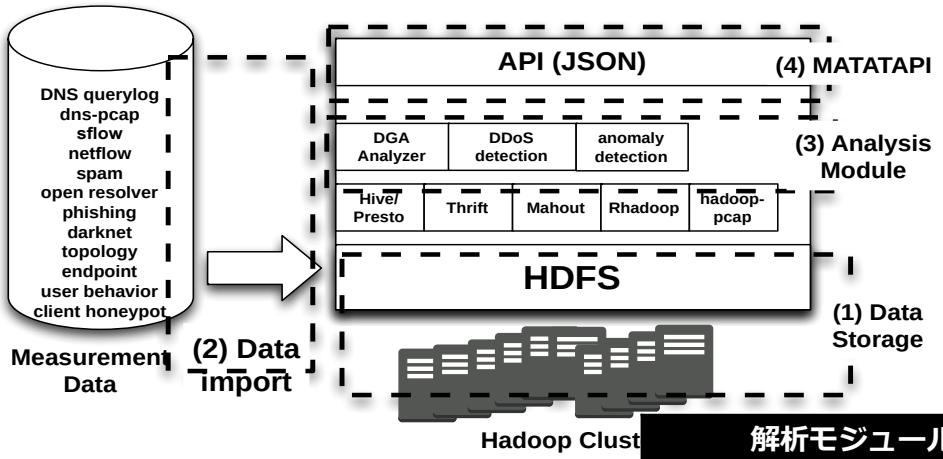
検証

課題4：事例実験

1) **サイバー防御技術のテスト環境の構築**
   様々なサイバー脅威をテスト環境上で再現しサイバー防御機構の回復力を検証した。
2) **テスト環境における事例実験の実施と評価**
   実環境やテスト環境を用いてサイバー脅威を検知し防御できることを検証した。



NECOMAプロジェクトにおけるビッグデータ基盤 MATATABI



- 多様かつ膨大なデータを並列処理(Hadoop)
- ボットネット、DDoSなど多岐にわたる脅威を効率的に検知

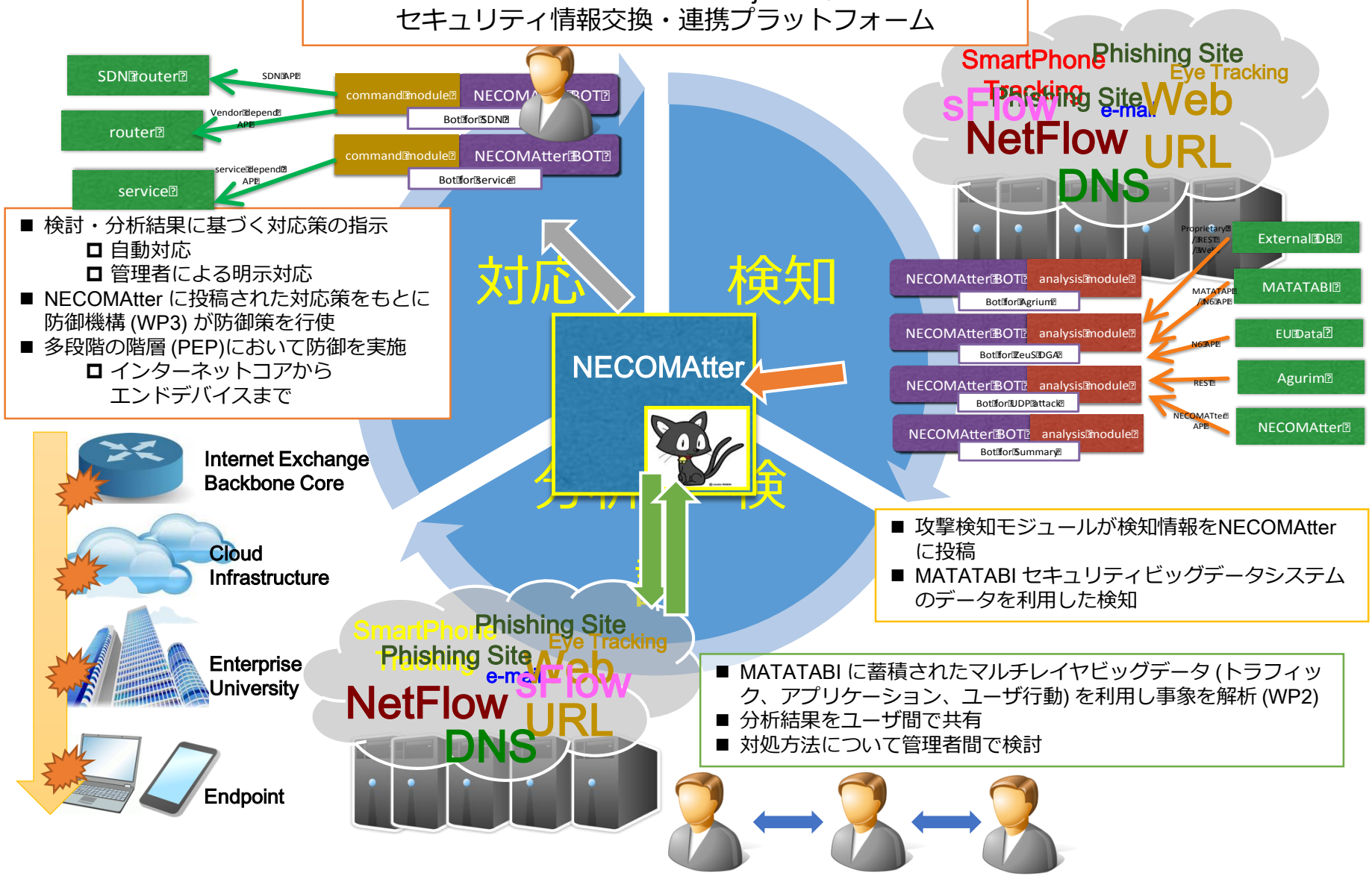
- 簡潔な記述、膨大なプログラミングは不要
- 日本側コンソーシアムで開発
- 欧州側コンソーシアムでも採用

解析モジュール名	データセット	解析頻度	行数
ZeuS DGA detector	DNS pcap, netflow	daily	25
UDP fragmentation detector	sFlow	daily	48
Phishing likelihood calculator	Phishing URLs, Phishing content	1-shot	–
NTP amplifier detector	netflow, sFlow	daily	143
NTP amplifier detector	sFlow	daily	24
DNS amplifier detector	sFlow, open resolver	daily	37
Anomalous heavy-hitter detector	netflow, sFlow	daily	106
DNS anomaly detection	DNS pcap, domain list	daily	57
SSL scan detector	sFlow	1-shot	36
DNS failure graph analysis	DNS pcap	daily	159

Hajime Tazaki, Kazuya Okada, Yuji Sekiya, Youki Kadobayashi. MATATABI: Multi-layer Threat Analysis Platform with Hadoop. In Proceedings of BADGERS 2014, Wroclaw, Poland. September, 2014.

セキュリティ情報交換・連携プラットフォーム NECOMAtter

NECOMAtter は NECOMA Project が開発した
セキュリティ情報交換・連携プラットフォーム



- 検討・分析結果に基づく対応策の指示
  - 自動対応
  - 管理者による明示対応
- NECOMAtter に投稿された対応策をもとに防御機構 (WP3) が防御策を行使
- 多段階の階層 (PEP)において防御を実施
  - インターネットコアから エンドデバイスまで

- 攻撃検知モジュールが検知情報をNECOMAtter に投稿
- MATATABI セキュリティビッグデータシステムのデータを利用した検知

- MATATABI に蓄積されたマルチレイヤビッグデータ (トラフィック、アプリケーション、ユーザ行動) を利用し事象を解析 (WP2)
- 分析結果をユーザ間で共有
- 対処方法について管理者間で検討

成果の公開・広報

- 欧州各国への成果発信
  - 英国大使館 UK-Japan Cybersecurity Researcher Workshop（2014年5月）
  - オランダ大使館 サイバーセキュリティ訪問団（2015年3月）
- ENISA （欧州情報セキュリティ庁）との連携
  - ENISA Report “Actionable Information for Security Incident Response” にてNECOMAプロジェクトの取り組みに言及ENISA Report “Standards and tools for exchange and processing of actionable information” の編纂に参画
- 招待講演
  - 特別講演, 2014年10月. The 5th APT Cybersecurity Forum (CSF-5), Ulaanbaatar, Mongolia, May 2014.
  - International Workshop on Traffic Analysis and Characterization, Nicosia, Cyprus, August 2014.
  - Cybersecurity Data Mining Competition and Workshop, Kuala Lumpur, Malaysia, Nov 2014.
  - 情報処理学会 コンピュータセキュリティシンポジウム

- NECOMA Business Meeting （リエゾン会合）
  - 研究者と事業者の意見交換を実施
    - 研究成果を展示
    - 研究成果をサービスとして展開
  - 参加者
    - セキュリティ専門機関
    - サービス事業者
    - セキュリティベンダー
    - 日欧産業協力センター

NECOMA business meeting, Jan 21, 2015