インターネット上の攻撃を多角的にどのように検出して防御するか?

インターネットトラフィックの異常検出

どんな研究？

インターネット上で生じる異常イベントを多種多様なデータから早期に検出し，その影響を最小限にするための研究をしています.

何がわかる？

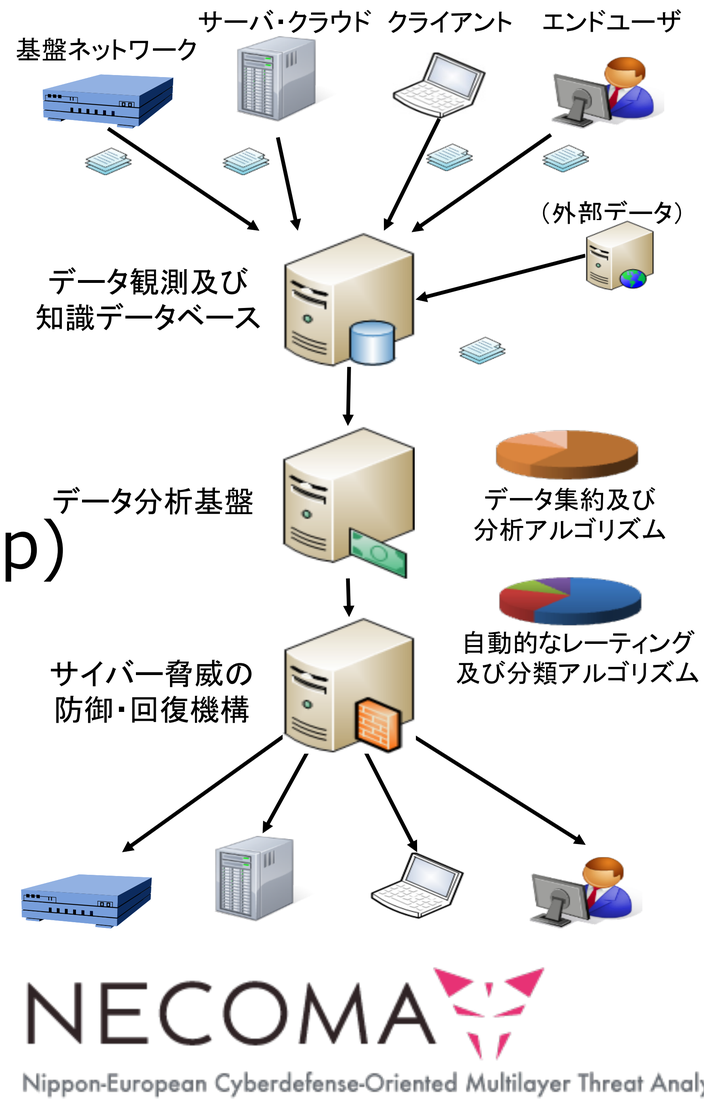
インターネットトラフィックをリアルタイムにモニタリングすることで，各種異常を引き起こす原因(攻撃，故障，誤設定等)を見つけだし，ネットワークの防御を可能とします.

はじめに

- インターネットでの攻撃は大規模分散かつ巧妙化
- インターネットインフラへの脅威も増大(400Gbpsを超えるDDoS攻撃(2014))
- 異常・攻撃の早期発見と防御が不可欠
  - 多地点・多種のデータ収集・解析の重要性
  - 組織間協調や連携の必要性

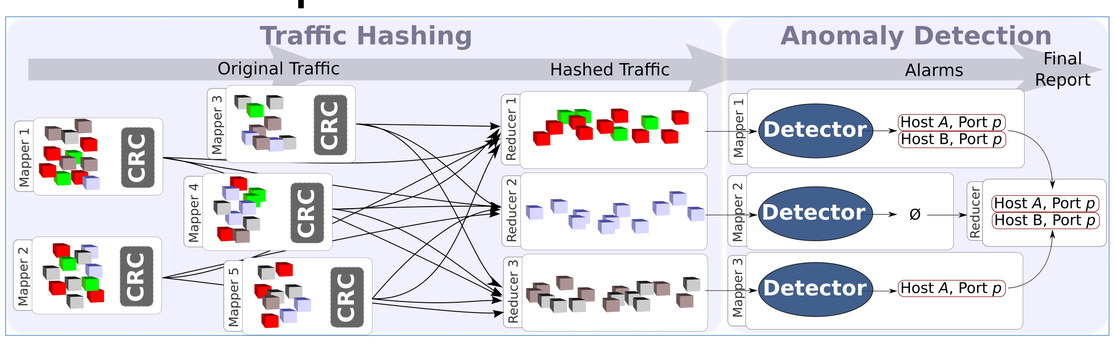
日欧協調によるマルチレイヤ脅威分析およびサイバー防御の研究 (総務省&FP7)

- マルチレイヤでのデータ収集
  - 基盤ネットワーク: 複数backbone traffic
  - サーバ・クラウド: DNS, firewall, cloud
  - クライアント: honeypot, dakrnet
  - エンドユーザ: phishing, spam
- データ分析基盤
  - ハッシュを用いたMapReduce異常検出基盤 (hashdoop)
  - 異常検出器の組み合わせによる性能向上 (mawilab)
  - 複数データセットからの関連イベントの抽出
- サイバー脅威の防御・回復機構
  - SDNによるDDoS防御
  - 知的なファイアーウォール



NECOMA
Nippon-European Cyberdefense-Oriented Multilayer Threat Analysis
http://www.necoma-project.jp

Hashdoop



Detection of spam domains

Domain names	
www.akivcsgree.jp	www.yrjtohjmbga.jp
mail.gtasomgree.jp	www.bsyhdjaskwheatmixi.jp
yrtwetwamixi.jp	www.lkjaysaddlebrowngree.jp
mayonnaisembga.jp	ns1.djbngree.jp

連絡先：福田健介／ 国立情報学研究所 アーキテクチャ科学研究系
TEL：03-4212-2514 FAX：03-4212-2120 Email：kensuke@nii.ac.jp