MWS 2013 意見交換会（2013/06/12）

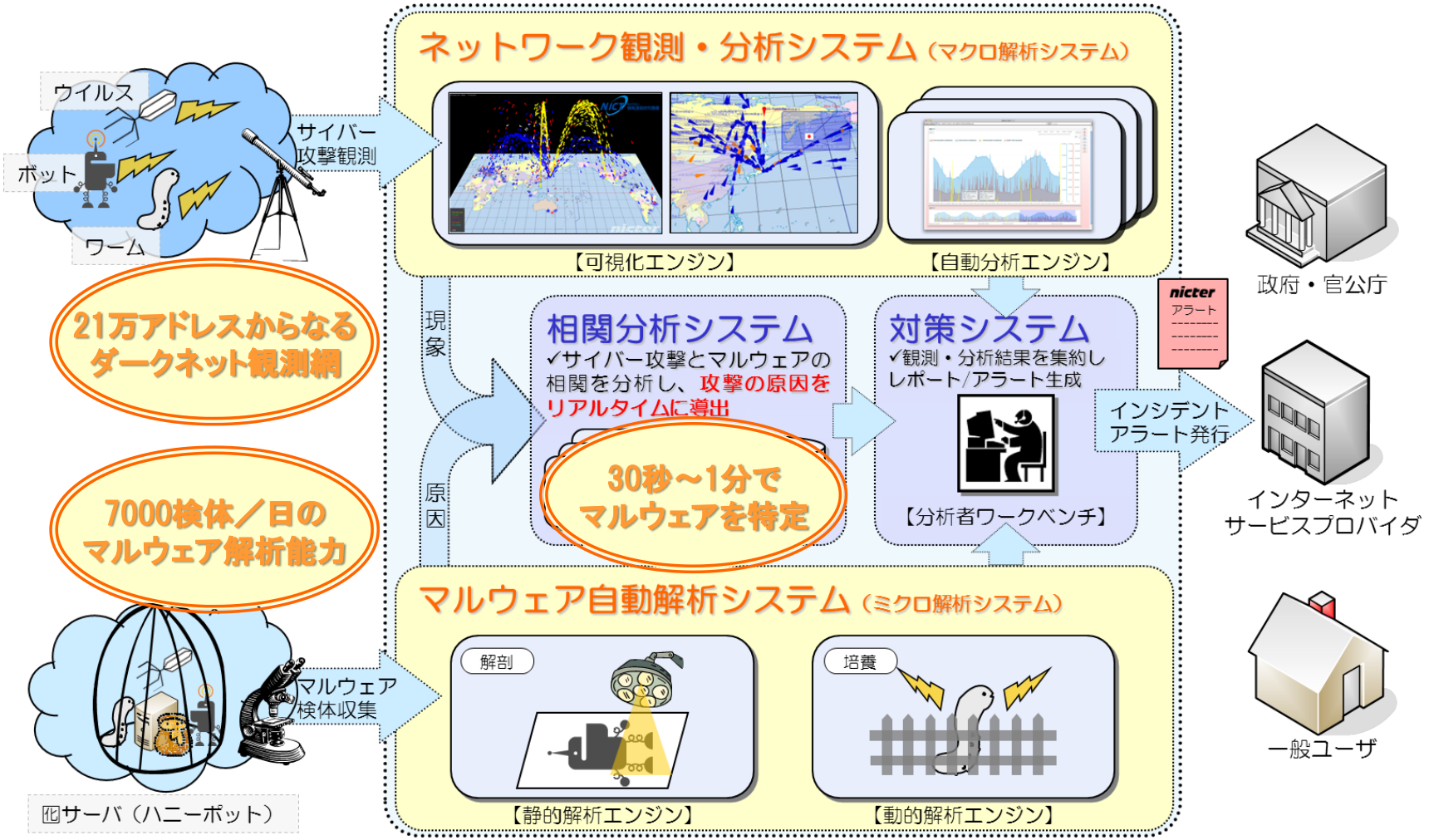
nicter darknet 2013

情報通信研究機構
ネットワークセキュリティ研究所
サイバーセキュリティ研究室

笠間　貴弘

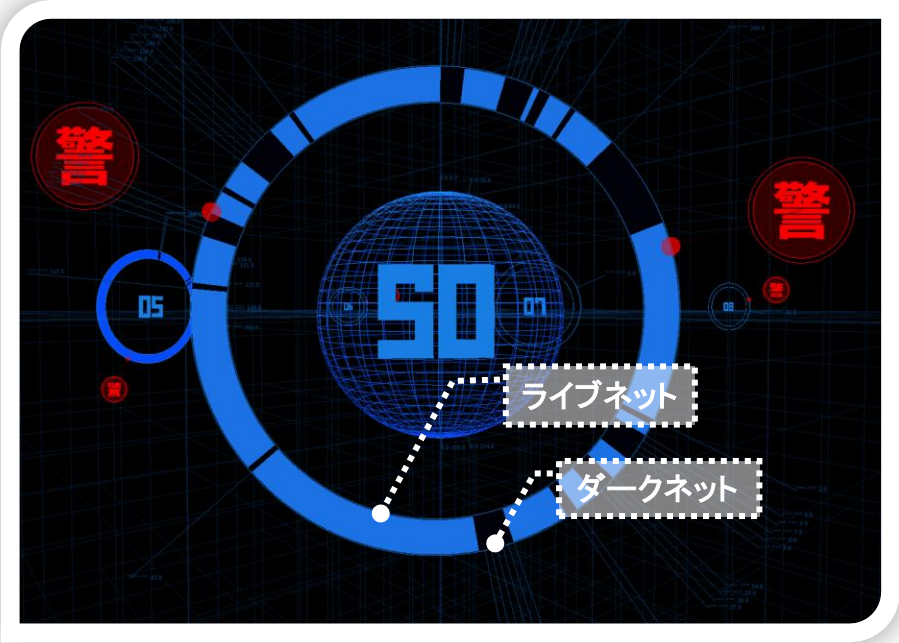
NICTER

Network Incident analysis Center for Tactical Emergency Response



MWS 2013 Datasets

- nicter Darknet 2013
  - nicterで収集したダークネットトラフィックデータ
  - 観測対象はある1組織 (/16) のダークネット (/20)
  - 2011年4月1日～2013年3月31日の2年間分＋α
  - PCAP形式のファイルを NONSTOP(機能制限版)上で 提供



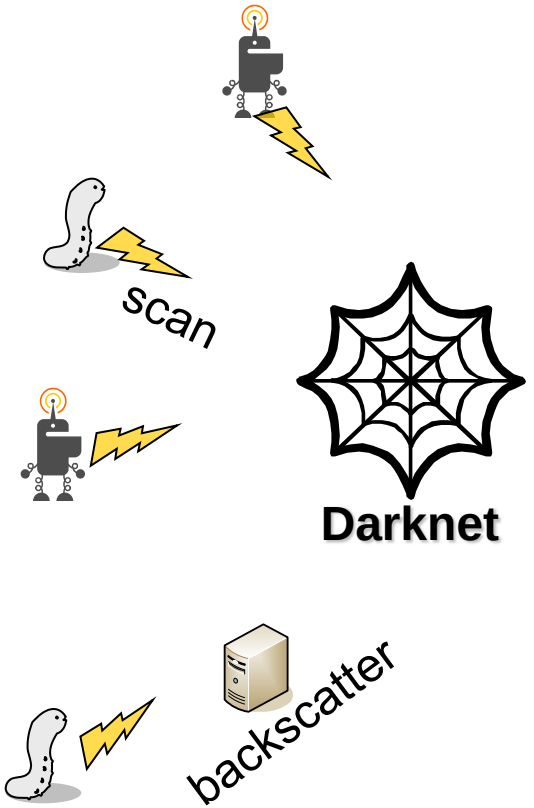
ダークネットとは

- 実ホストが存在しない未使用IPアドレス（ブロック）

- ダークネットに届くパケットは
  - マルウェア（リモートエクスプロイト型）によるスキャン
  - マルウェア本体の感染行為（主にUDP）
  - DDoS攻撃の跳ね返り（バックスキャッタ）
  - 設定ミス

  などが原因。

- インターネット上で広範囲に影響を与える攻撃の把握に役立つ。



NONSTOP

NICTER Open Network Security Test-Out Platform

- nicterで収集したサイバーセキュリティ情報（ダークネットトラフィック, マルウェア検体, etc.）を遠隔から安全に利用するための分析基盤

- 利用に必要なもの
  - ICカード（nicter Darknet 2013の利用申請後に送付されます）
  - ICカードリーダ（各自でご用意ください）
  - SSHクライアント等のソフトウェア

- できること
  - NONSTOP上のVM（Linux, Windows）の利用
  - nicterの各種データリソースへのアクセス
  - ローカルマシン－VM間でのファイル転送

- 他にも・・・
  - データリソース
    - リアルタイムのダークネットトラフィックデータ
    - マルウェア検体
    - ミクロ解析システムの解析結果
    - スパムメール（ダブルバウンスメール）
    - etc.
  - 設備
    - IDA Proなどの解析ツールをVM内に標準用意
    - WebサーバによるVM管理等のためのインターフェイス提供
    - 利用者間の知識共有やトラブルシューティングのために、NONSTOP内にWikiサーバを用意

- 参考文献
  - 竹久, 井上, 衛藤, 吉岡, 笠間, 中里, 中尾, “サイバーセキュリティ情報遠隔分析基盤NONSTOP,” ICSS研究会@長岡, 2013年6月

NICTERにおける
ダークネットトラフィック分析

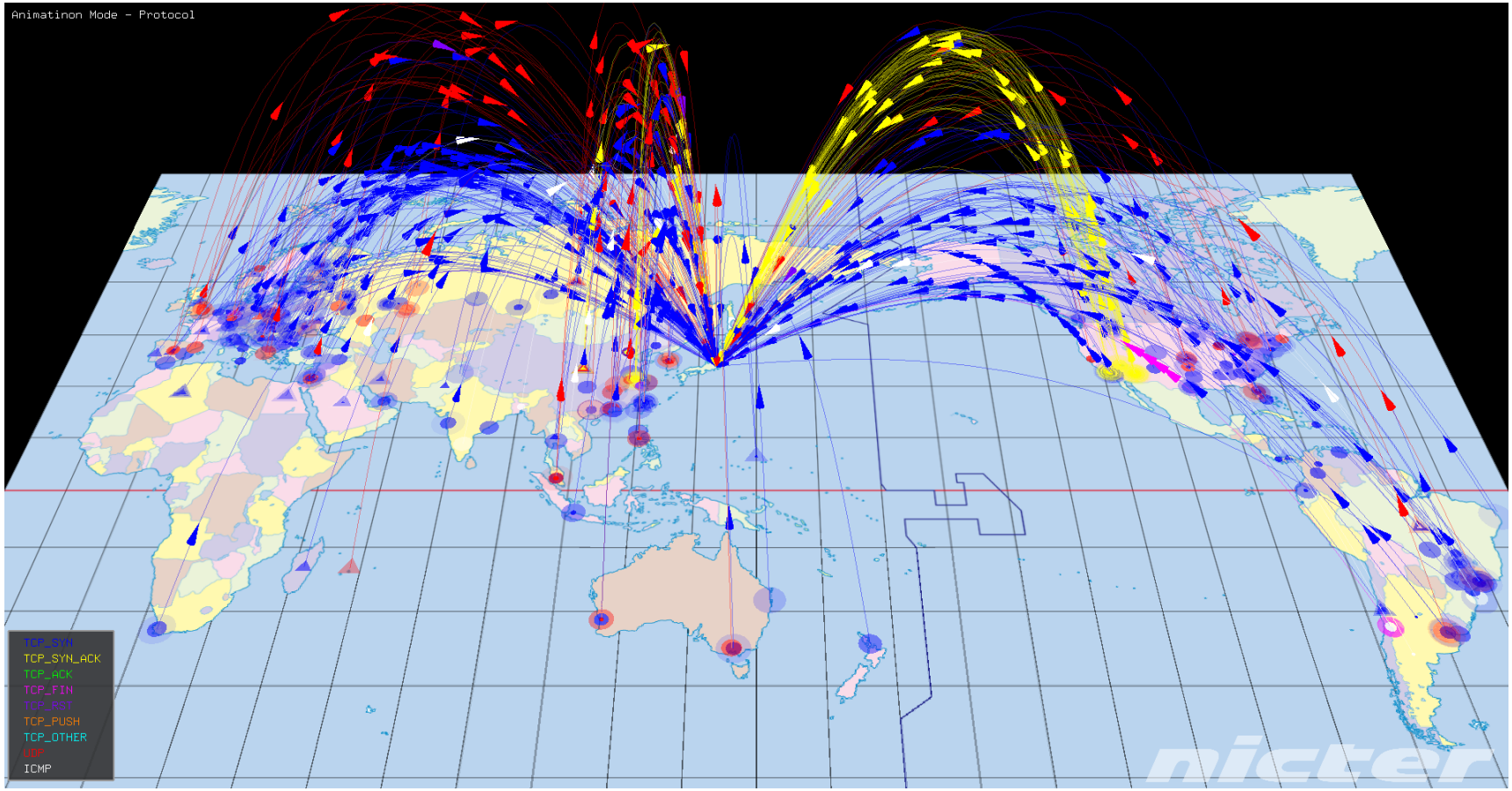
～可視化・分析エンジン～

独立行政法人
情報通信研究機構
National Institute of Information and Communications Technology

NICTER

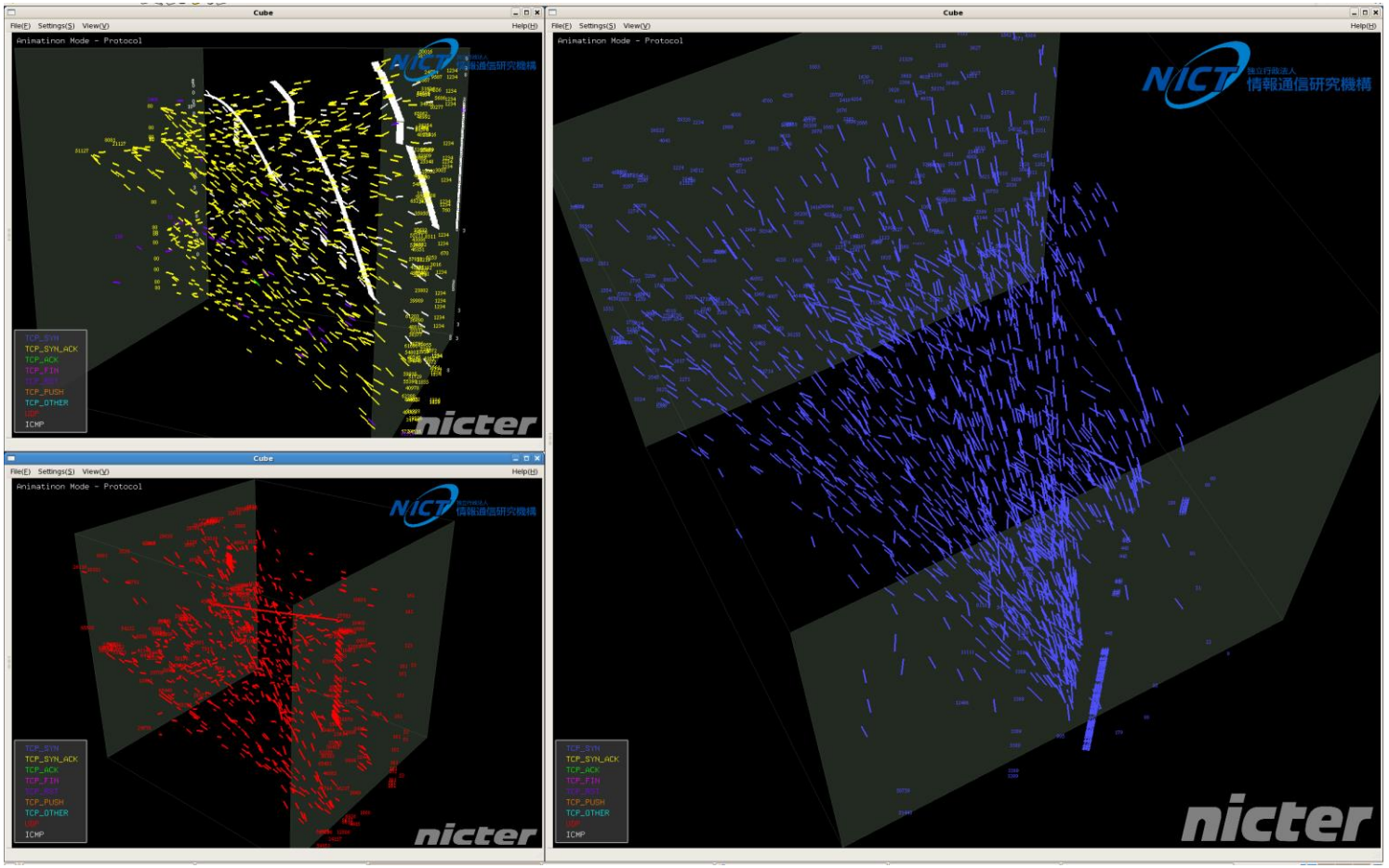
Atlas: *Geographical Traffic Visualization*

- 攻撃元の地理的分布を俯瞰（色: プロトコルやTCPフラグ, 高度: 宛先ポート番号）



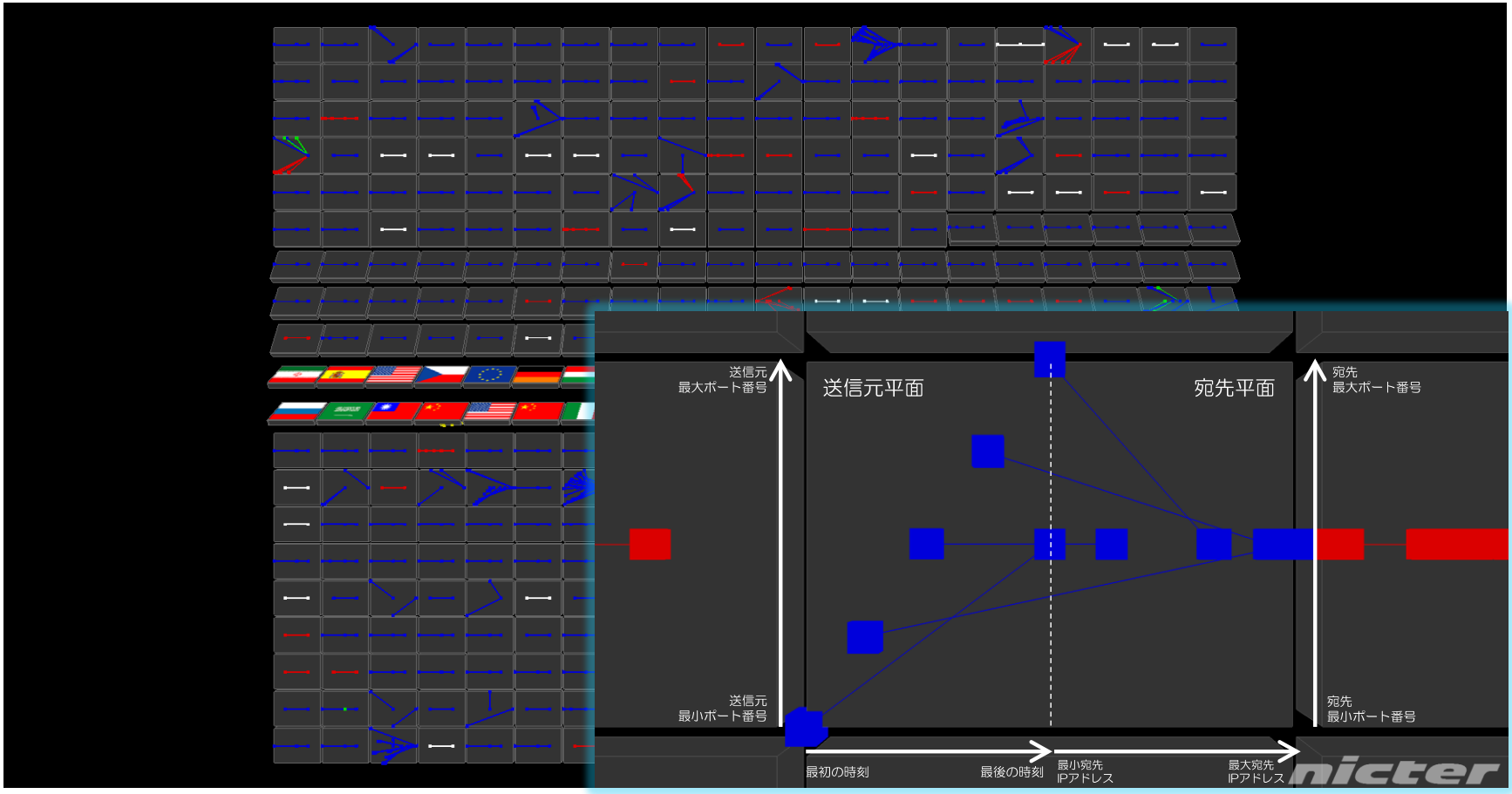
Cube: *3D Traffic Visualization*

- 全体的なスキャン傾向を把握（画像はプロトコル毎に可視化）



Tiles: *Host-based Behavioral Analysis Engine*

- 1ホストの30秒間の挙動を表現（自動的にクラスタリング）

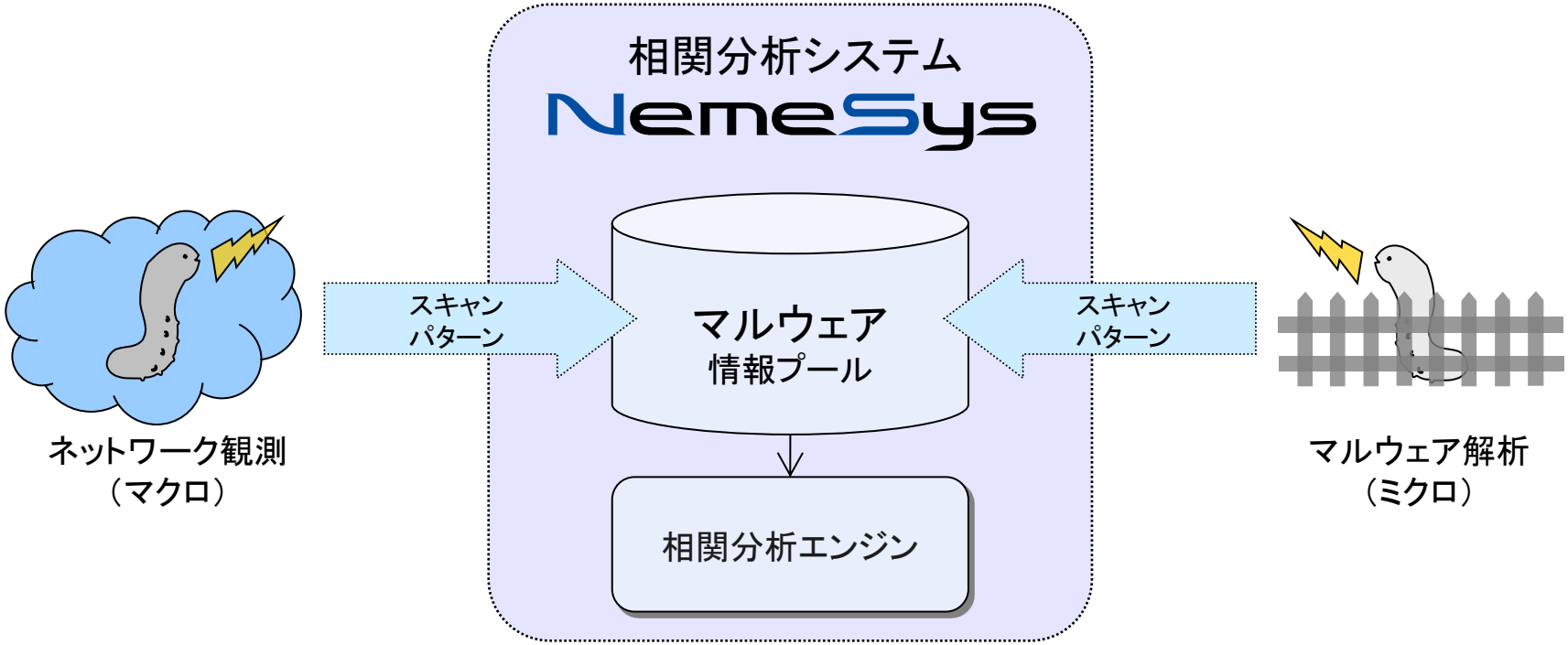


NemeSys

network and malware enchaining system

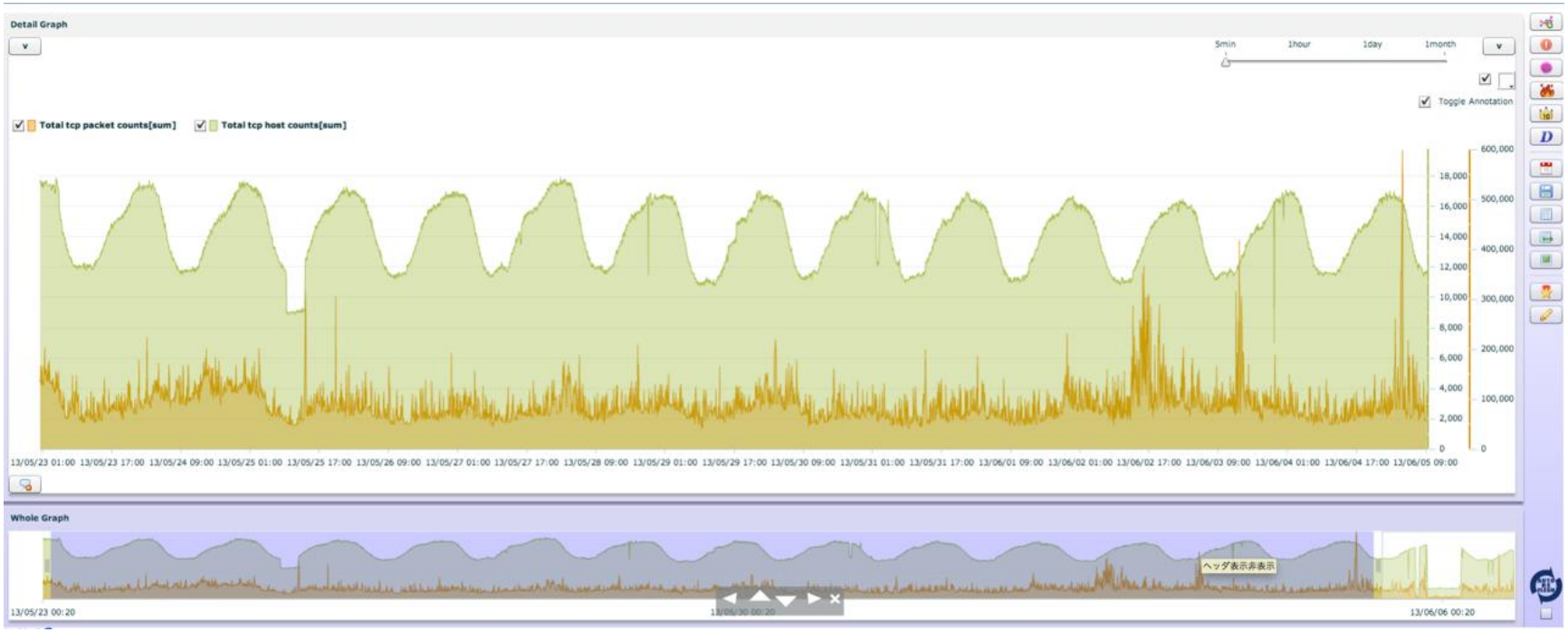
- 目的

  マクロ解析システムにおいて観測されたスキャンと
  ミクロ解析システムにおけるマルウェアのスキャンの
  相関を調べることで、**現象**と**原因**を関連付ける



他

- CPD（Change Point Detector）
  - 変化点検出エンジンを用いたインシデント検知エンジン
- Stats
  - 長期的な統計表示による傾向把握
- etc.



NICTERにおける
ダークネットトラフィック分析

～大規模感染マルウェア出現の予兆～

独立行政法人
情報通信研究機構
National Institute of Information and Communications Technology

NICTER

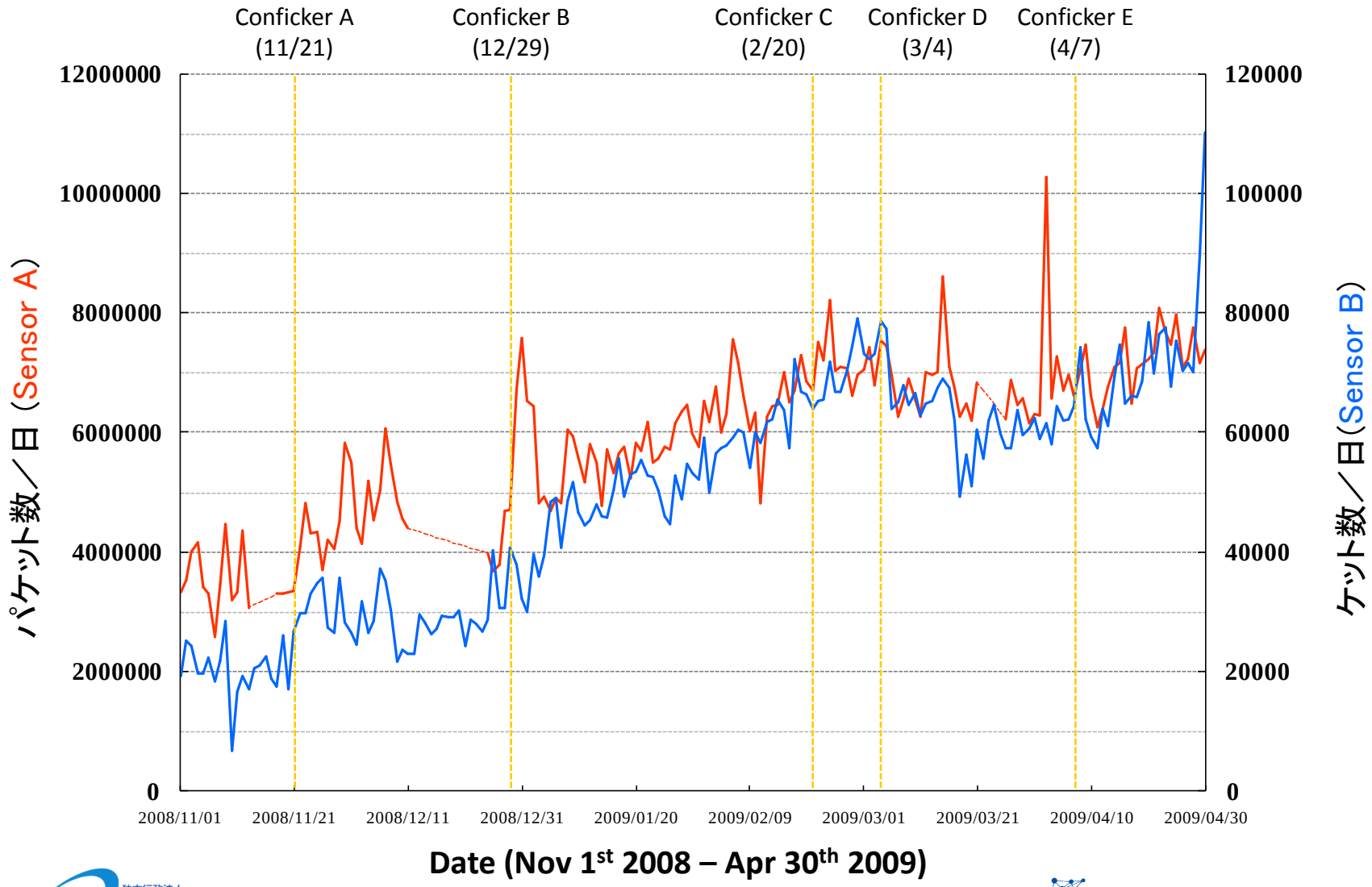
観測事例：Conficker

【時系列】

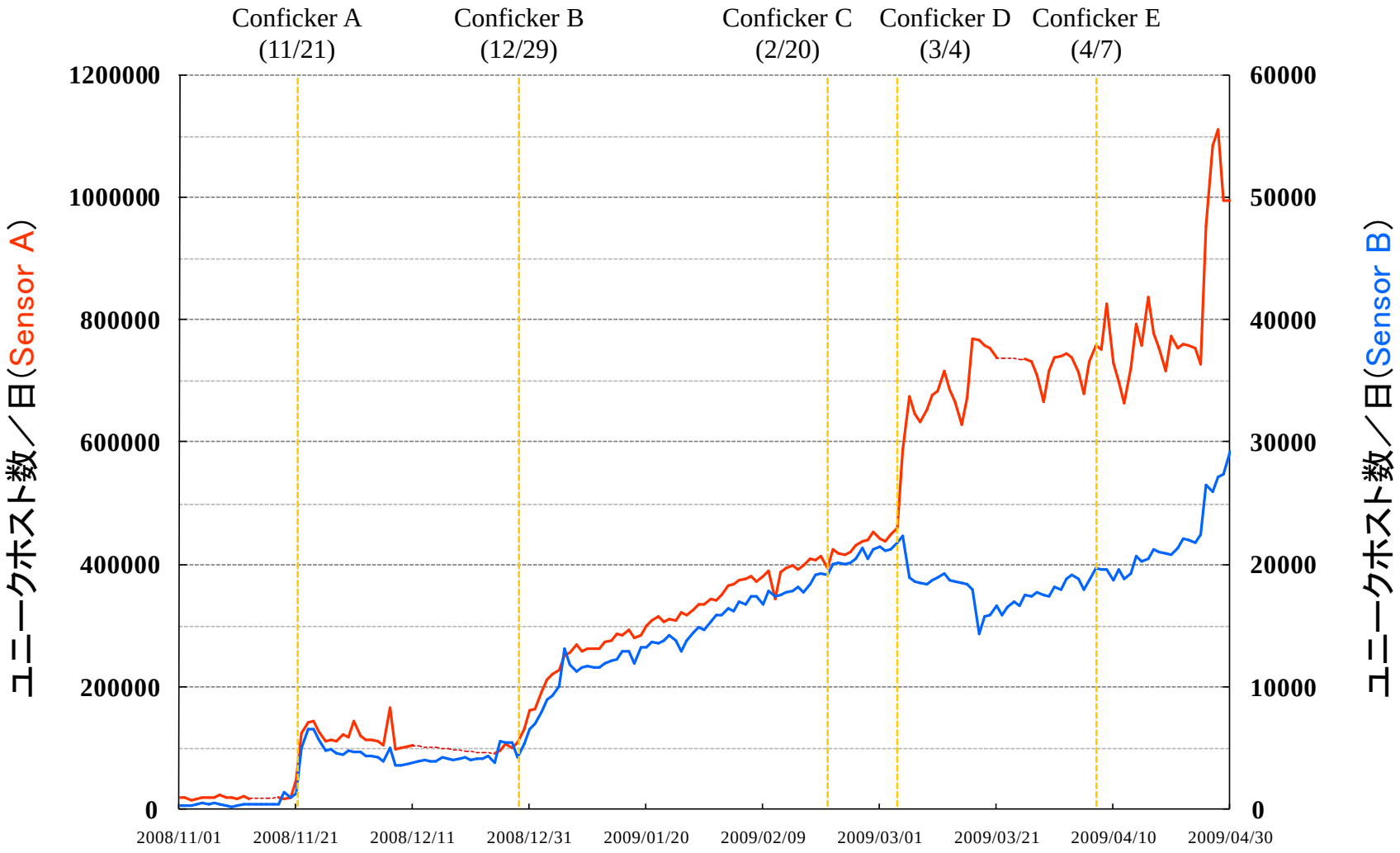
- 2008/10/24
  - MS08-067
    - Server サービスの脆弱性により、リモートでコードが実行される

- 2008/11/21: Conficker.A
- 2008/12/29: Conficker.B
- 2009/02/20: Conficker.C
- 2009/03/04: Conficker.D
- 2009/04/07: Conficker.E

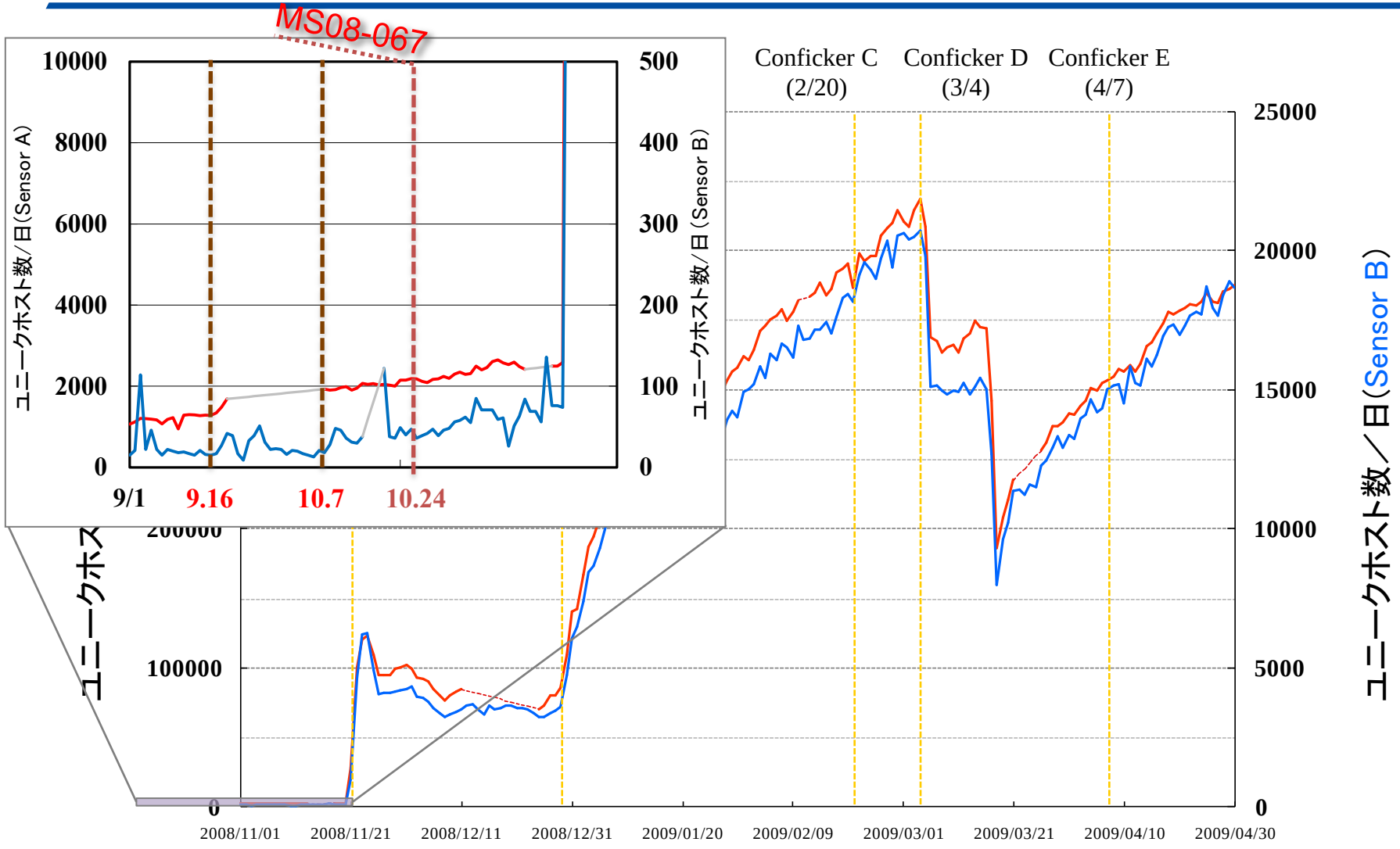
ダークネット観測結果（パケット数）



ダークネット観測結果（ユニークホスト数）



ダークネット観測結果（ユニークホスト数 on 445/tcp）



Date (Nov 1st 2008 – Apr 30th 2009)

観測事例：Morto

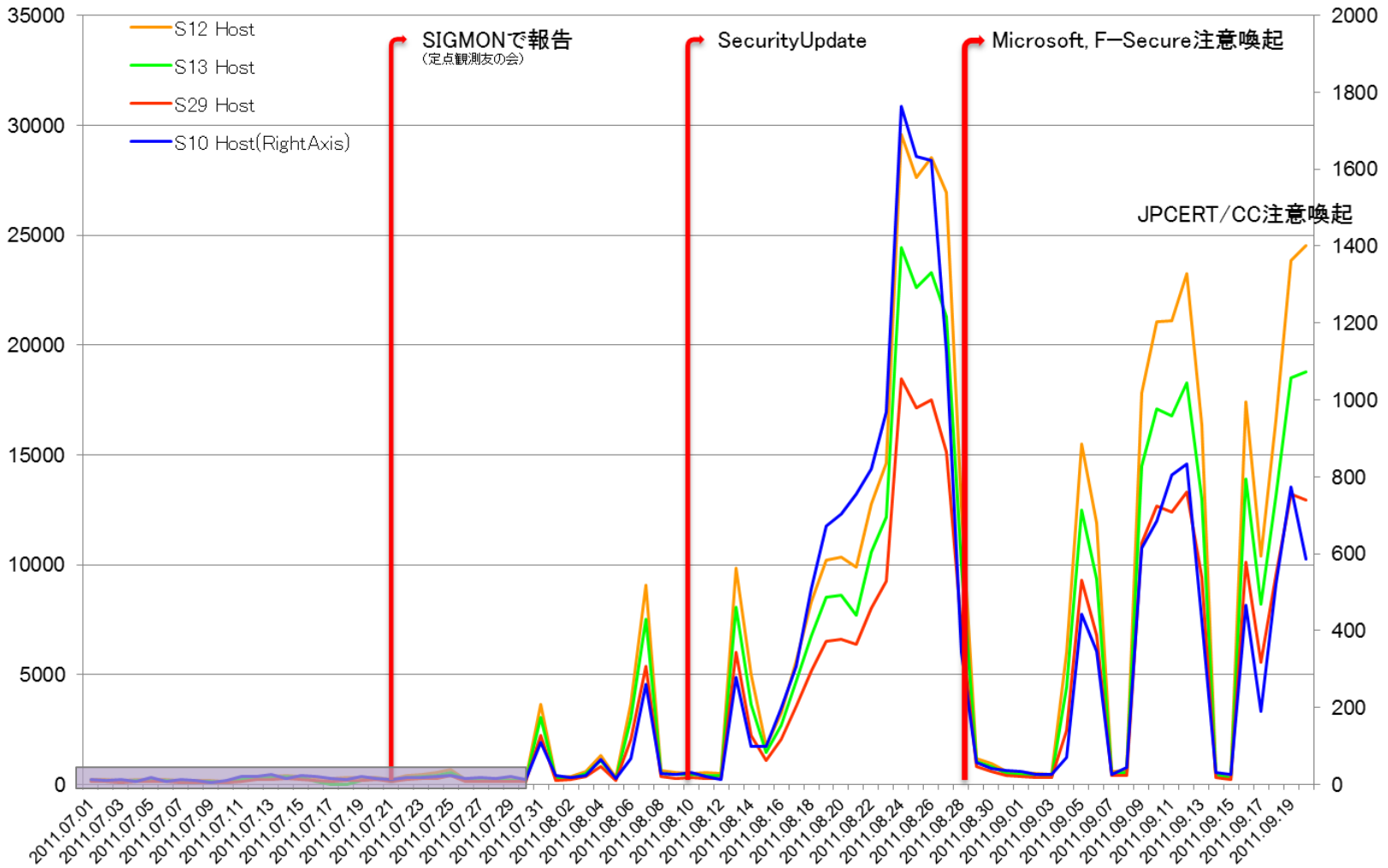
【時系列】

- 2011/08/10
  - MS11-061
    - リモート デスクトップ Web アクセスの脆弱性により、特権が昇格される
  - MS11-065
    - リモート デスクトップ プロトコルの脆弱性によりサービス拒否が発生する

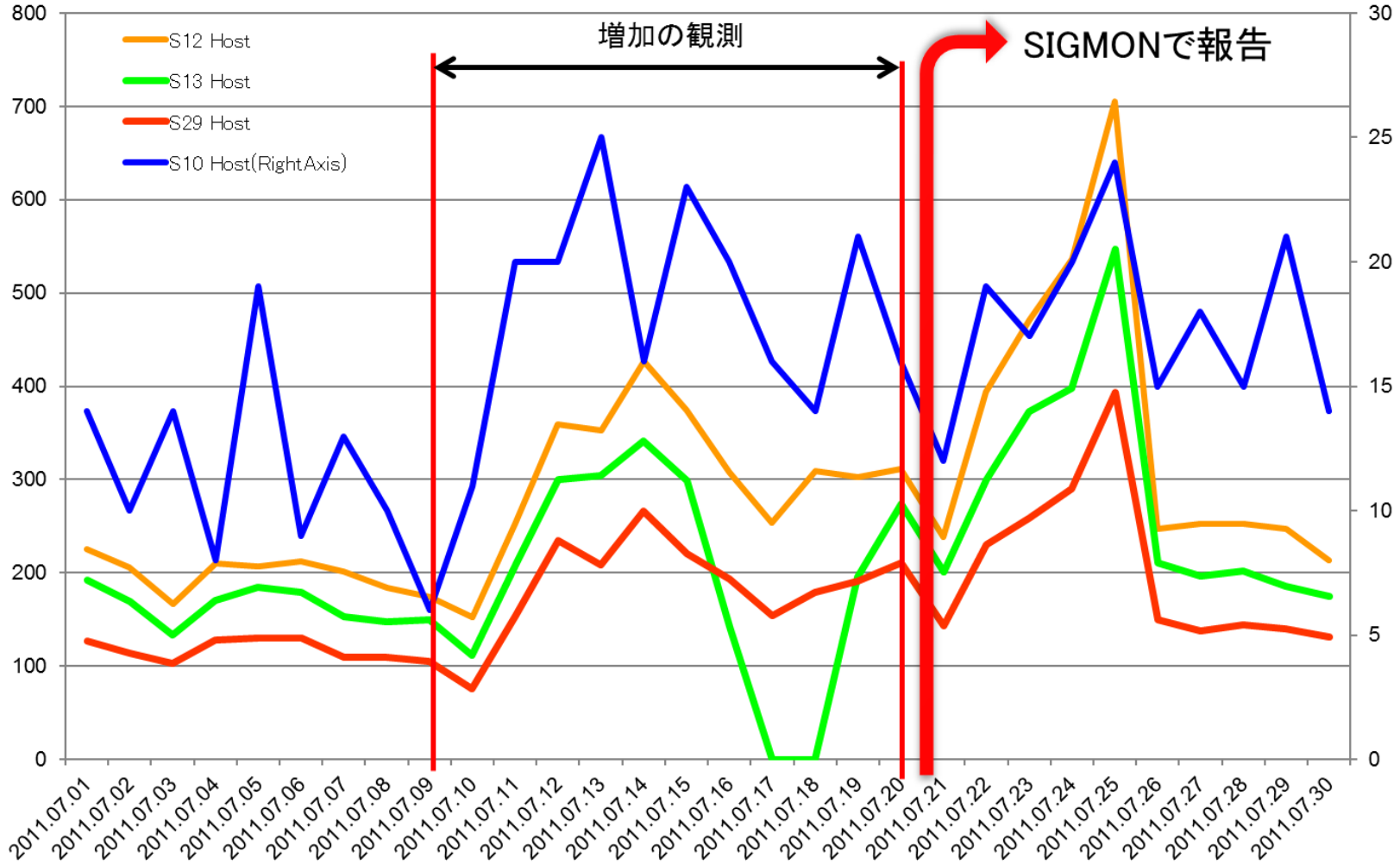
- 2011/08/28
  - Microsoft（Mortoワーム）
    - Mortoの注意喚起、及びウイルス定義作成
  - F-Secure
    - Mortoの注意喚起

- 2011/09/07
  - JPCERT/CCからの注意喚起
    - http://www.jpcert.or.jp/at/2011/at110024.html

ダークネット観測結果（ユニークホスト数 on 3389/tcp）



ダークネット観測結果（ユニークホスト数 on 3389/tcp）



予兆検出(オペレータ視点)の流れ

- 一例
  - ユニークホスト数の増加（全体、プロトコル別、宛先ポート別）
    - Stats（統計グラフ）
    - Cube
  - 現象が継続するか観察
    - ボットの活動由来だと急増して急降下するケースが多い
  - スキャンパターンの確認
    - Tiles
    - Chronos（Tilesの長期間版）
    - ミクロ解析システムとの比較
  - 関連情報の収集
    - 脆弱性情報
    - 他組織の観測傾向
  - 情報共有（連携組織など）

NICTERにおける
ダークネットトラフィック分析

～他～

サイバーセキュリティ研究室の取り組み

- 可視化・分析ツール
  - 攻撃元の地理的分布（Atlas）
  - 全体の攻撃傾向（Cube）
  - 個々の攻撃元の攻撃パターン（Tiles、Chronos）
  - 統計情報（Stats）
  - 変化点検出（CPD）
  - マルウェア動的解析結果との突合（Nemesys）
  - ダークネット観測ベースのアラートシステム（DAEDALUS）

- 研究課題（一例）
  - 機械学習を応用したインシデント予測
  - バックスキャッタ分析・対策応用
  - 他のサイバー攻撃観測情報との突合（マルチモーダル分析）
    - スパムメール、ドライブ・バイ・ダウンロード攻撃、ハニーポット、etc.
  - 新たな能動的ダークネット観測網
  - ダークネット観測網災害応用技術（ACTIVATE）

nicter Darknet 2013 を利用した
論文投稿をよろしくお願いします！！