NICTER Darknet 2014

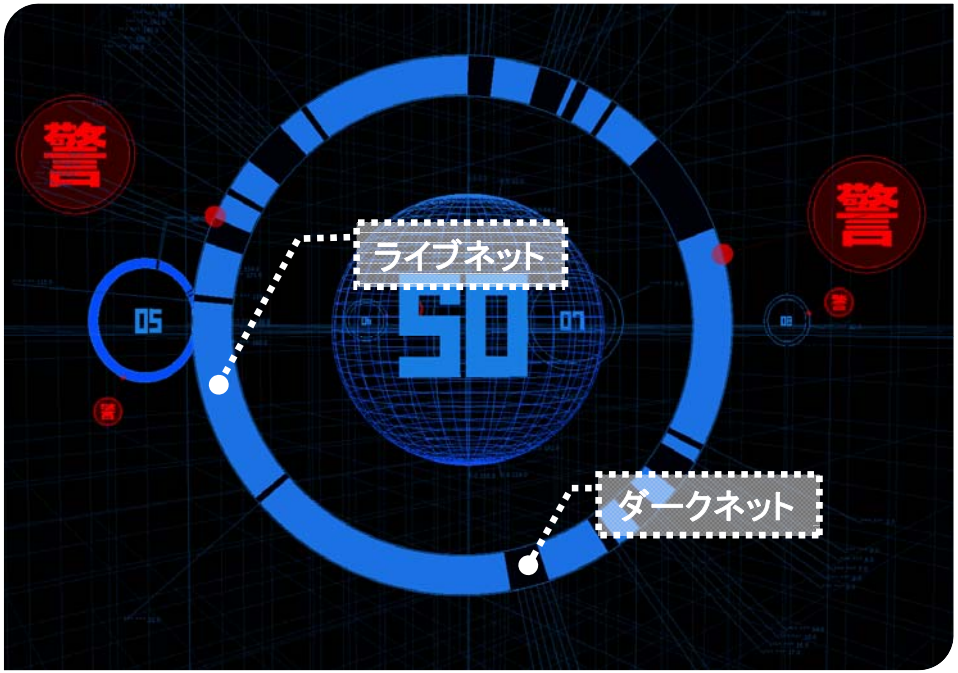
独立行政法人 情報通信研究機構（NICT）
笠間貴弘　　神薗雅紀

NICT

NICTER
Network Incident analysis Center for Tactical Emergency Response

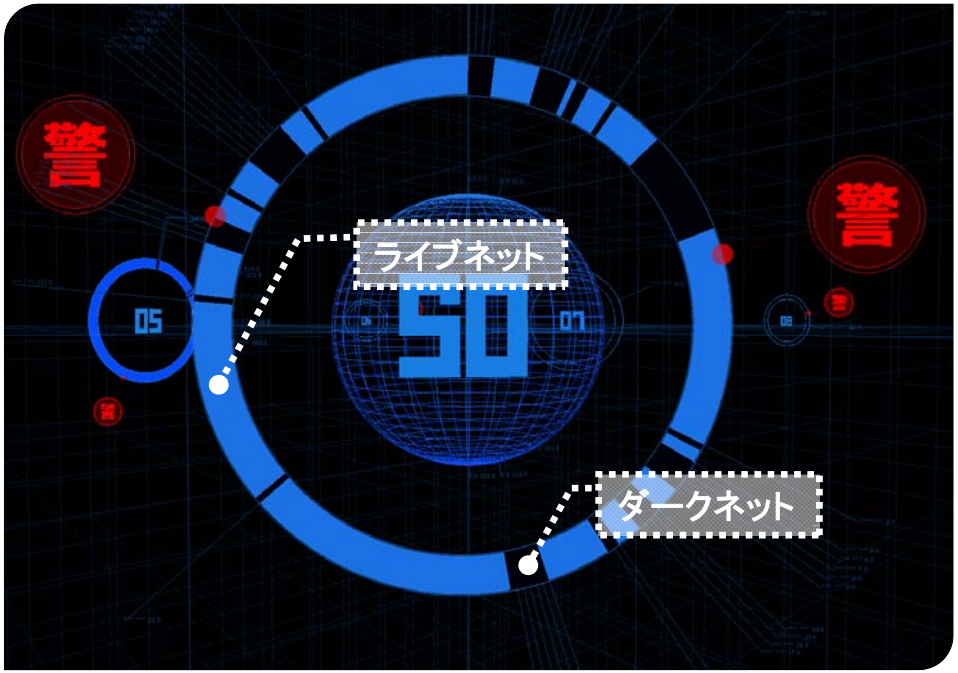
NICTER Darknet 2014

- NICTER Darknet 2014
  - ダークネット（未使用IPアドレス）宛てのトラフィックデータ
  - 観測対象はある/20の連続したダークネット
  - 2011年4月1日～2014年3月31日の3年間分＋α
  - NONSTOPを利用して提供（pcap＋DB(予定)）



Network Incident analysis Center for Tactical Emergency Response

- データの注意点
  - ダークネットからは応答を返していないため、インターネットからダークネットへの片方向の通信データしか含まれていない
  - センサ設置場所を秘匿する目的で、宛先IPアドレスの第１および第２オクテットは適当な値に置換している



NICTER Darknet 2013 利用実績

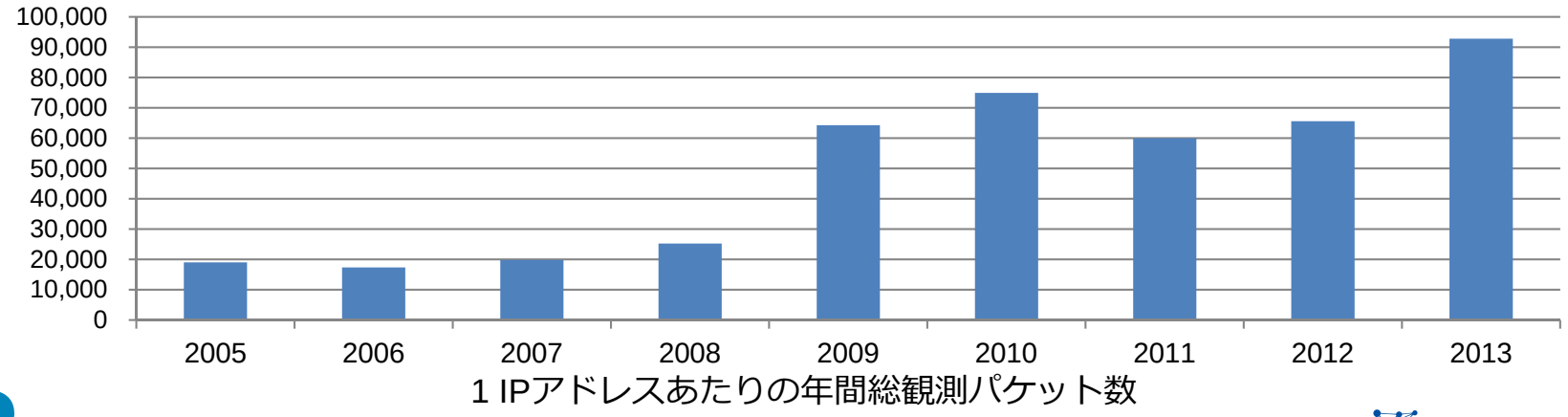
- インターネット観測システムへの観測点検出攻撃を考慮した動的観測手法の一検討
- 通信源ホストの分類を利用したダークネット通信解析
- ライブネットにおける不正通信の早期検知手法
- ダークネットモニタリングによるDNSトラフィック分析
- NONSTOPデータを用いたマルウェアの時系列分析
- ダークネットトラフィックデータの解析によるサブネットの脆弱性判定に関する研究

Q：ダークネットで見える攻撃は
減少している？

いいえ。
むしろ増加しています！

NICTERダークネット観測統計

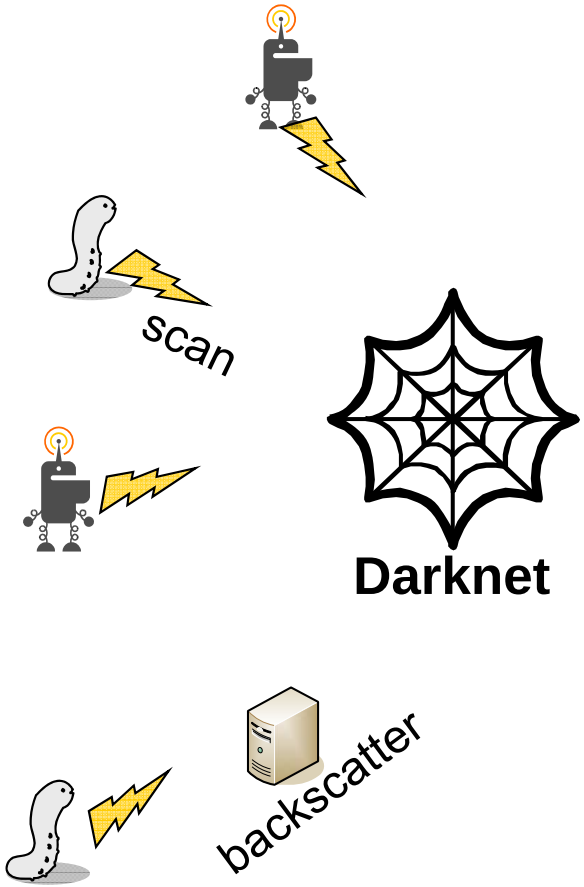
年	年間 総観測パケット数	観測IPアドレス数	1 IPアドレス当たりの 年間総観測パケット数
2005	約 3.1億	約1.6万	約1.9万
2006	約 8.1億	約10万	約1.7万
2007	約19.9億	約10万	約2.0万
2008	約22.9億	約12万	約2.5万
2009	約35.7億	約12万	約6.4万
2010	約56.5億	約12万	約7.5万
2011	約45.4億	約12万	約6.0万
2012	約77.9億	約19万	約6.6万
2013	約128.8億	約21万	約9.3万



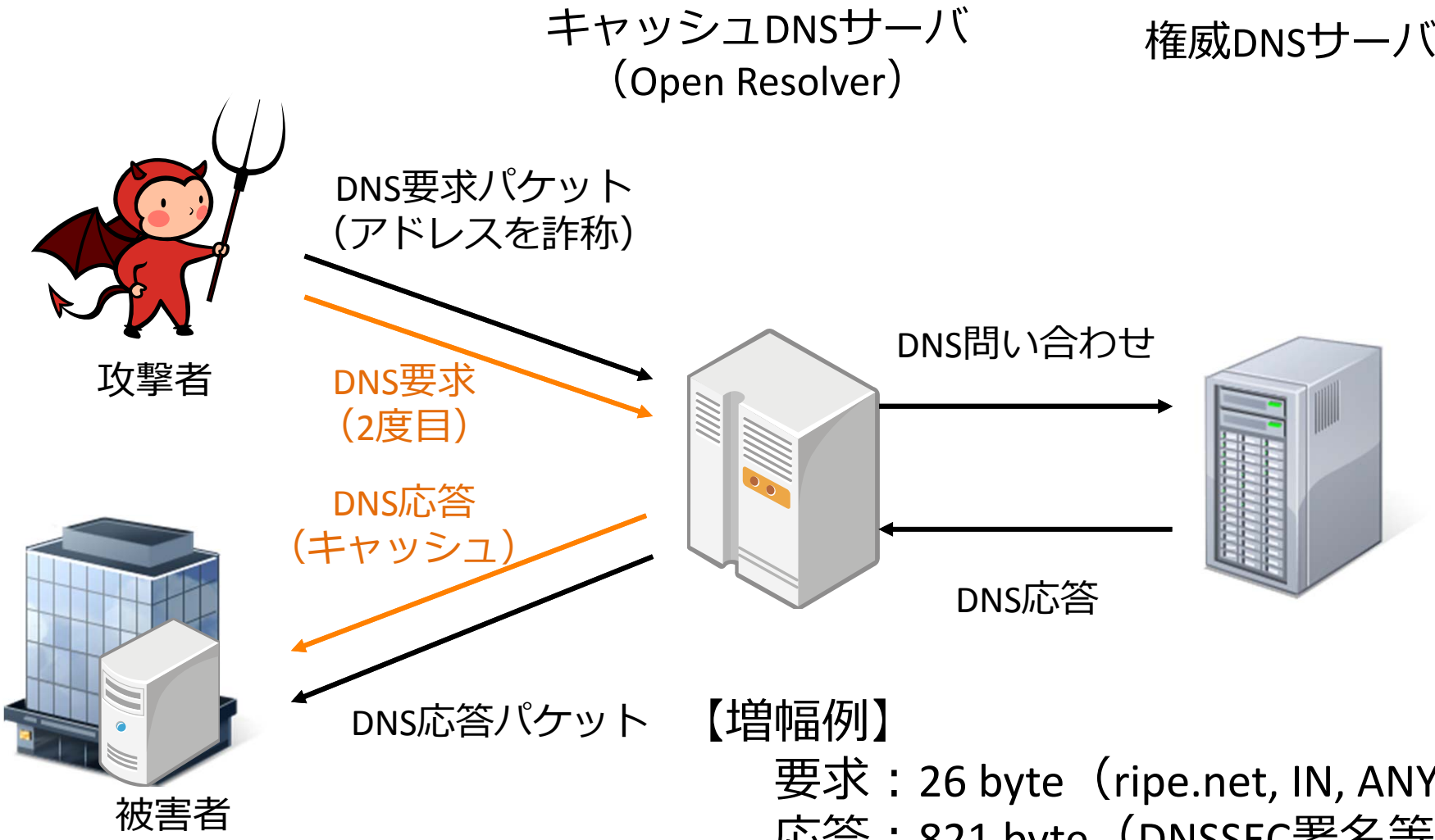
Network Incident analysis Center for Tactical Emergency Response

ダークネットで何が見えているのか？

- **マルウェアによるスキャン**
  - ✓ ワーム型マルウェアの探索活動
  - ✓ マルウェア感染の大局的傾向
  - ✓ 感染爆発の前兆
- **DDoS攻撃の跳ね返り**
  - ✓ 送信元IPアドレス偽装されたSYN Flood
  - ✓ 被攻撃サーバからの応答（SYN-ACK）
  - ✓ DDoS攻撃の早期検知（1パケット目から）
- **設定ミス**
  - ✓ 組織内ダークネット
- **リフレクション攻撃の準備活動** 新
  - ✓ DNS Open Resolver探索
  - ✓ NTP探索 etc.



DNS amp攻撃の概要



【増幅例】

要求：26 byte（ripe.net, IN, ANY）

応答：821 byte（DNSSEC署名等含む）

増幅率：**約32倍**

DNS amp攻撃とダークネット

Open Resolverを攻撃に利用するためには、

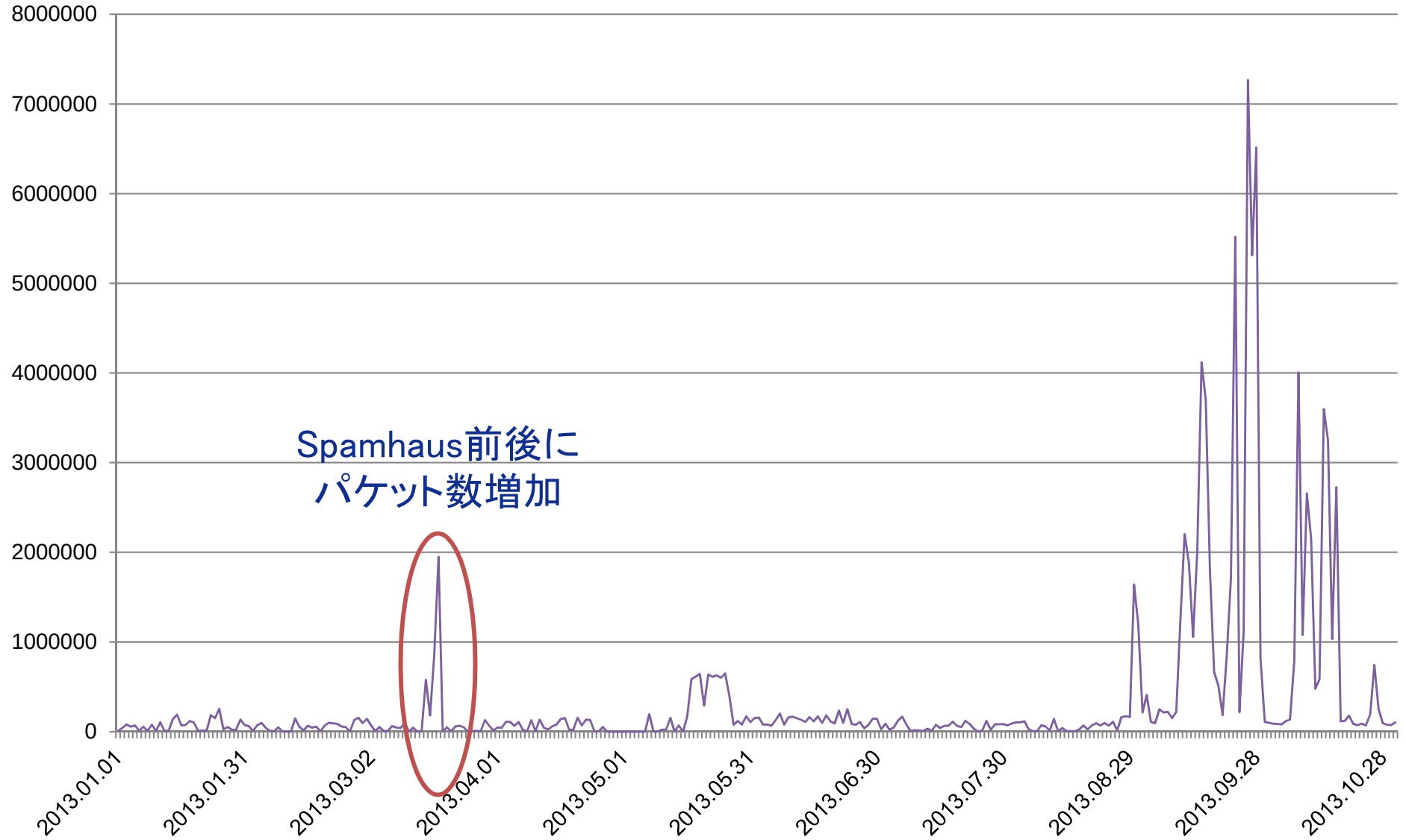
Open Resolverを探す必要があります。

Open Resolver探索のスキャンが来る！

（宛先53/UDP）

パケット数（宛先53/UDP）

- 2013年1月～10月(/16センサ) -

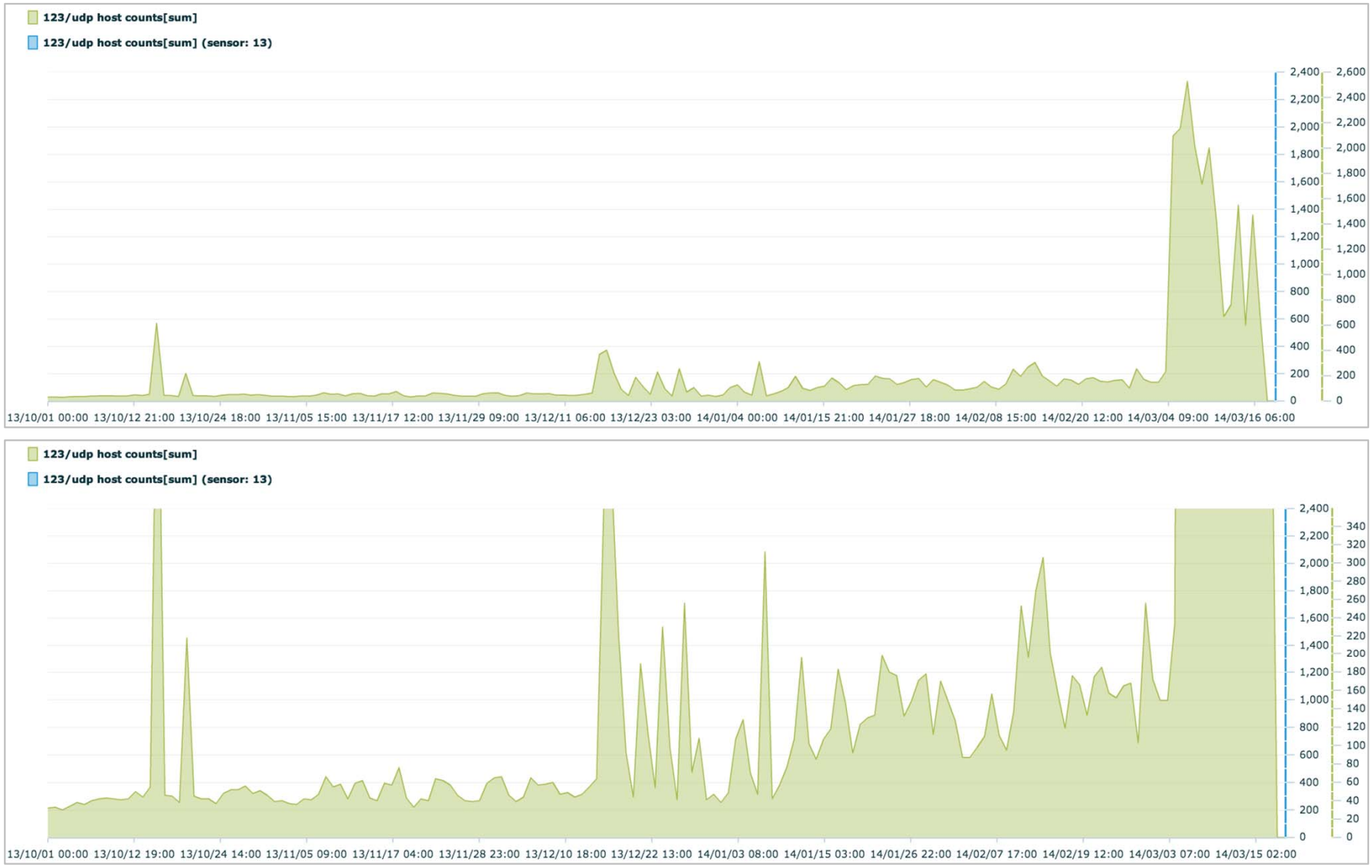


NICT

NICTER
Network Incident analysis Center for Tactical Emergency Response

ユニークホスト数（宛先123/UDP）

- 2013年10月～2014年03月 -



ダークネット関連研究

- A. Dainotti, K. Benson, A. King, K. Claffy, M, Kallitsis, E. Glatz, and X. Dimitropoulos, “Estimating internet address space usage through passive measurements,” ACM SIGCOMM 2014
  - IPアドレス空間の利用推定手法

- A. Dainotti, R. Amman, E. Aben, K. Claffy, “Extracting Benefit from Harm: Using Malware Pollution to Analyze the Impact of Political and Geophysical Events on the Internet,” ACM SIGCOMM 2012
  - 震災等によるネットワーク障害を検知
  - Awarded as one of top-three papers in ACM SIGCOMM Computer Communication Review in 2012

- Christian Rossow, “Amplification Hell: Revisiting Network Protocols for DDoS Abuse,” NDSS 2014
  - DRDoS (Distributed Reflective Denial of Service)に利用されるプロトコルの洗い出しと実際の攻撃の観測

- 牧田大佑, 吉岡克成, 松本勉, 中里純二, 島村隼平, 井上大介, “DNSアンプ攻撃の早期対策を目的としたDBSハニーポットとダークネットの突合分析,” SCIS2014（SCIS論文賞受賞）
  - DNSハニーポットとダークネットデータの突合分析

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

MWS2014 意見交換会(2014-05-19)

NONSTOP

NICTER Open Network Security Test-Out Platform

MWS Editionについて

独立行政法人 情報通信研究機構
サイバー攻撃対策総合研究センター
サイバー防御戦術研究室
招へい専門員
竹久　達也

CYREC
サイバー攻撃対策総合研究センター

- 背景

　NICTERは，多数の開発者，分析者，研究協力者により，開発・運営されており，開発者，分析者，研究協力者らユーザの研究開発をさらに促進するために，外部から安全にインシデント分析が行えるシステムへのニーズが高まっている．

NICT（小金井）に行かないと
NICTERのサイバーセキュリティ情報を活用した研究開発が出来ない．

外部からのアクセスを適切に制御しながら
ユーザの利便性も考慮した
遠隔インシデント分析環境が欲しい！

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

NONSTOPって？

nicter open network security test-out platform

NICTER内で保有する
サイバーセキュリティ情報(NICTERリソース)を
外部から扱うことが出来るようにした、

Virtual Private Server(VPS) サービス

VPSサービス ＋ NICTERリソース

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

NICTERリソースって？

- ダークネットトラフィックデータ（PCAPファイル）
- リアルタイムダークネットトラフィックデータ
- マルウエア検体
- マルウエア検体のミクロ解析結果
- ミクロ・マクロ相関分析結果
- SPAMメール　．．．

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

NONSTOP(MWS Edition)では,

- ダークネットトラフィックデータ（PCAPファイル）
- ~~リアルタイムダークネットトラフィックデータ~~
- ~~マルウエア検体~~
- ~~マルウエア検体のミクロ解析結果~~
- ~~ミクロ・マクロ相関分析結果~~
- ~~SPAMメール　．．．~~

- リモートログイン（OpenSSH改造）
  - ICカードによる認証
  - ターミナルログイン禁止
  - 転送速度制限(<10Mbps)
  - ポートフォワード制限
    80(HTTP),3389(RDP)

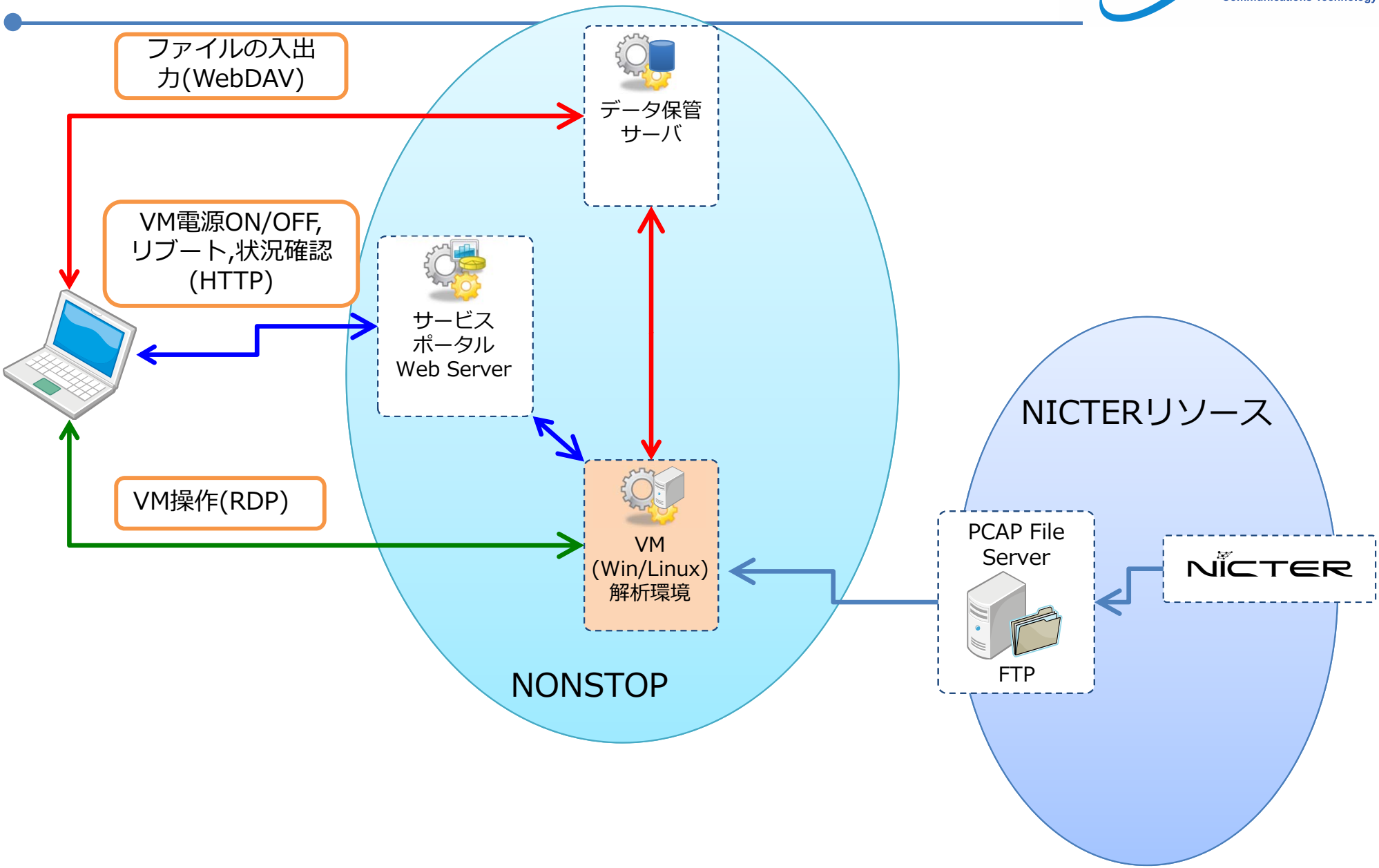
- NONSTOPポータル(web)
  - ユーザ管理，VM管理
- NONSTOP Wiki
  - オンラインマニュアル、FAQなど
- ファイル転送
  - WebDAV経由のファイル転送（Read/Write）
  - ファイルフィルタリング
    （Hash比較，種別，圧縮・暗号，サイズなど）
  - ファイル入出力監視，複製

- 分析VM
  - OS

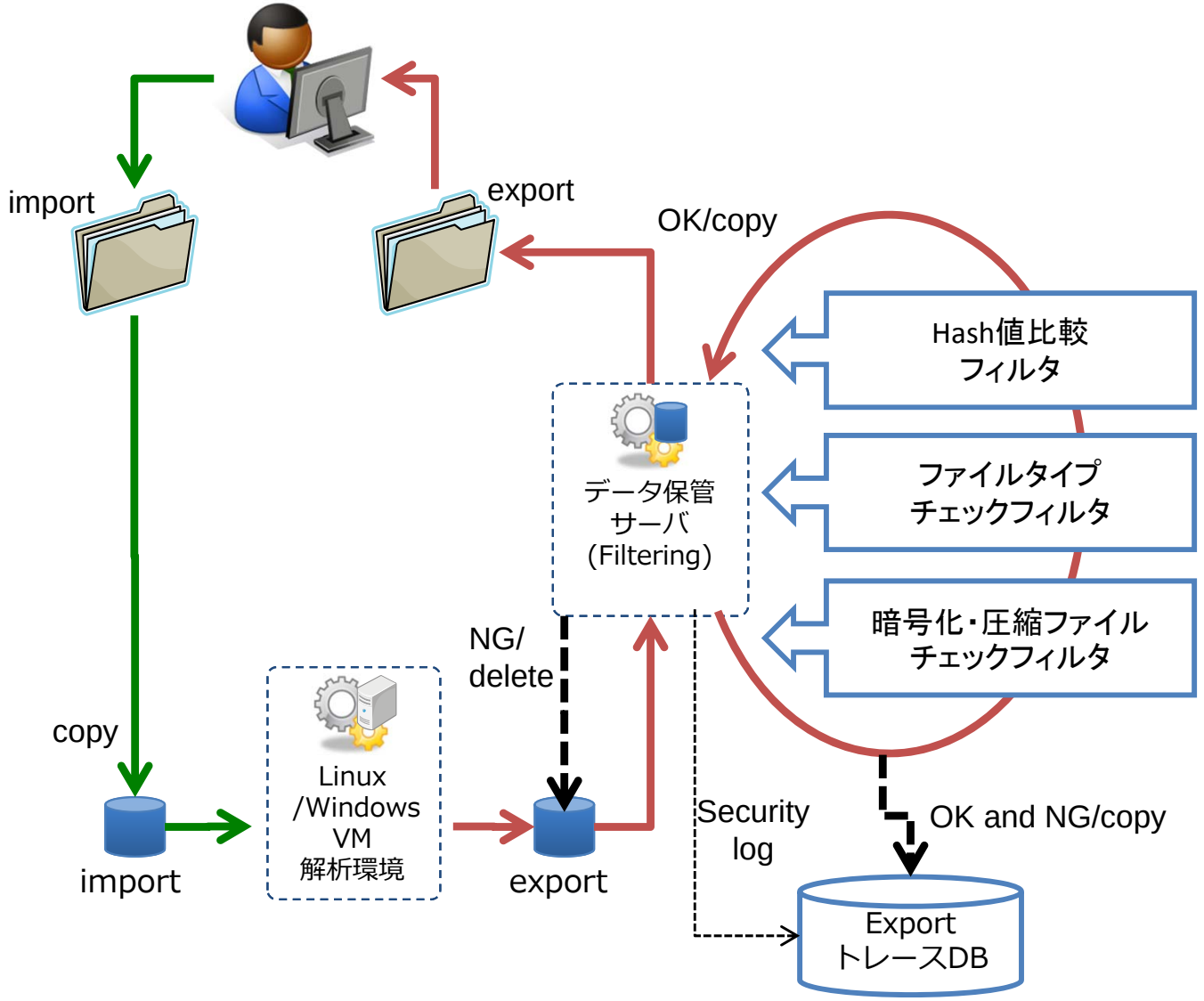
    CentOS5.x, 6.x

  - NIC
    - NIC A:VM間通信のマスク
    - ~~NIC B:ダークネットパケット受信用NIC（着信IPは匿名化）~~

Operation


ファイルの入出力(WebDAV)
VM電源ON/OFF, リブート,状況確認 (HTTP)
VM操作(RDP)
データ保管サーバ
サービスポータル Web Server
VM (Win/Linux) 解析環境
NONSTOP
NICTERリソース
PCAP File Server
FTP
NICTER

VMから解析結果の取得，ユーザ側からのデータ転送



100MBまで

Access Count(2013/06 ～ 2014/05)