NICTER Darknet 2016

国立研究開発法人 情報通信研究機構
サイバー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 Darknet 2016

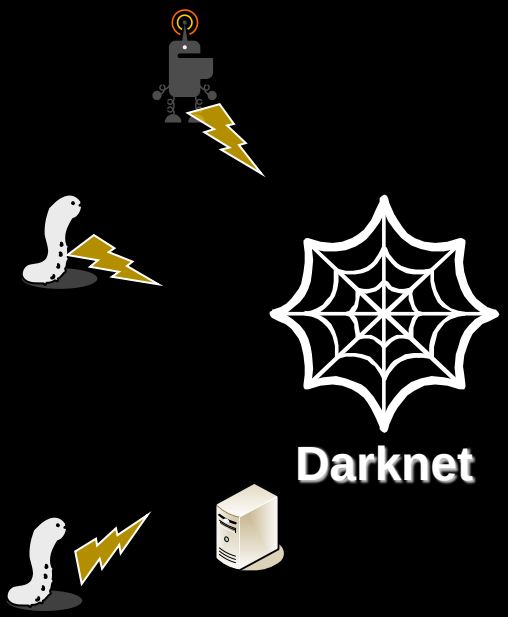
- /20のダークネット宛てのトラフィックデータ
- 観測期間は2011年4月1日～の５年間＋α
- NONSTOPを通じて提供（pcap+DB）

NICTER
Network Incident analysis Center for Tactical Emergency Response

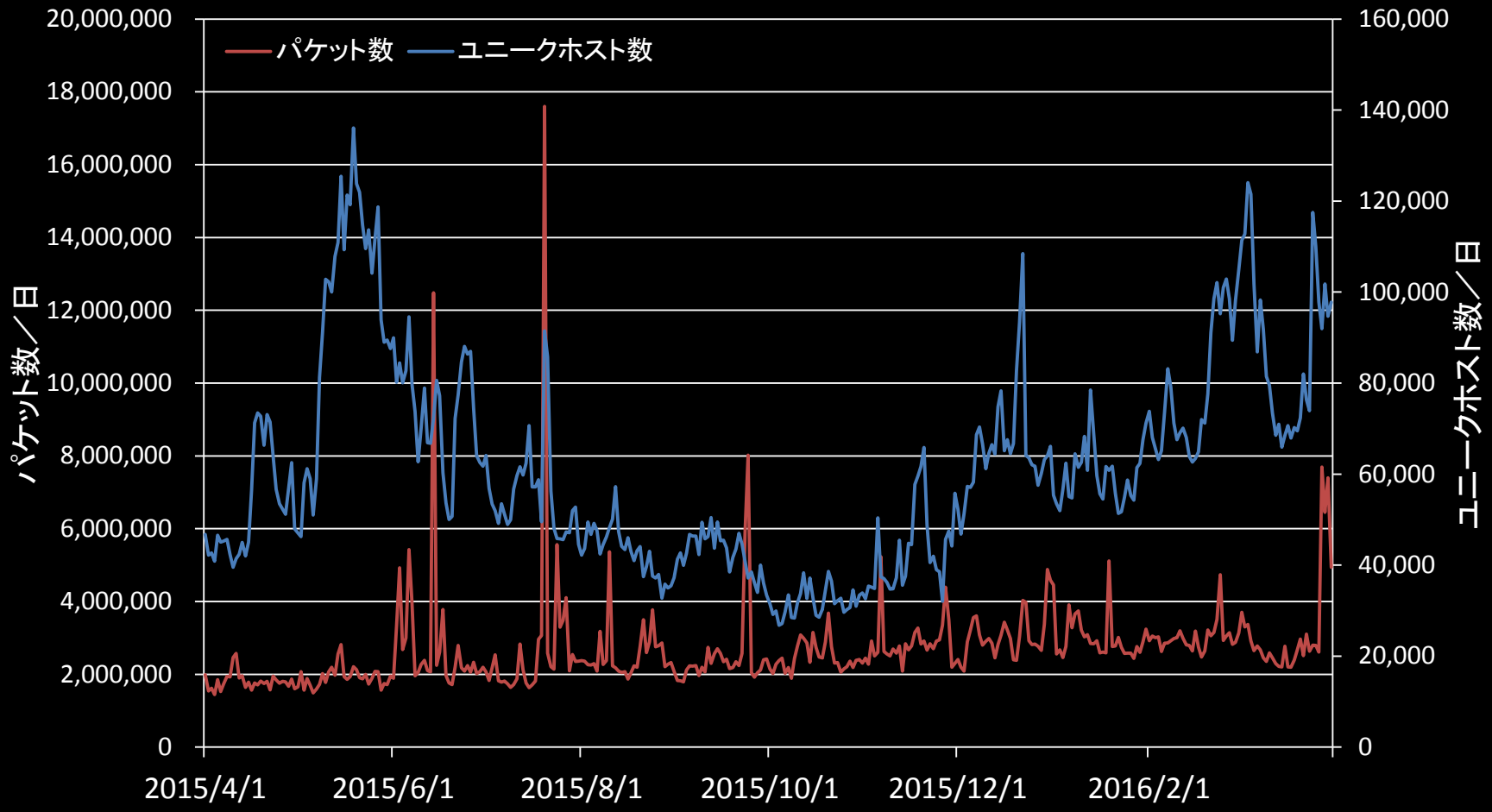
ダークネットで何が見えているのか？

- ダークネット = 未使用IPアドレス
  - ➢通常はダークネットにはトラフィックは届かない

- 実際はたくさん飛んできます
  - マルウェアによるスキャン活動
  - DDoS攻撃の跳ね返り
  - リフレクション攻撃の準備活動
  - 設定ミス
  - etc.

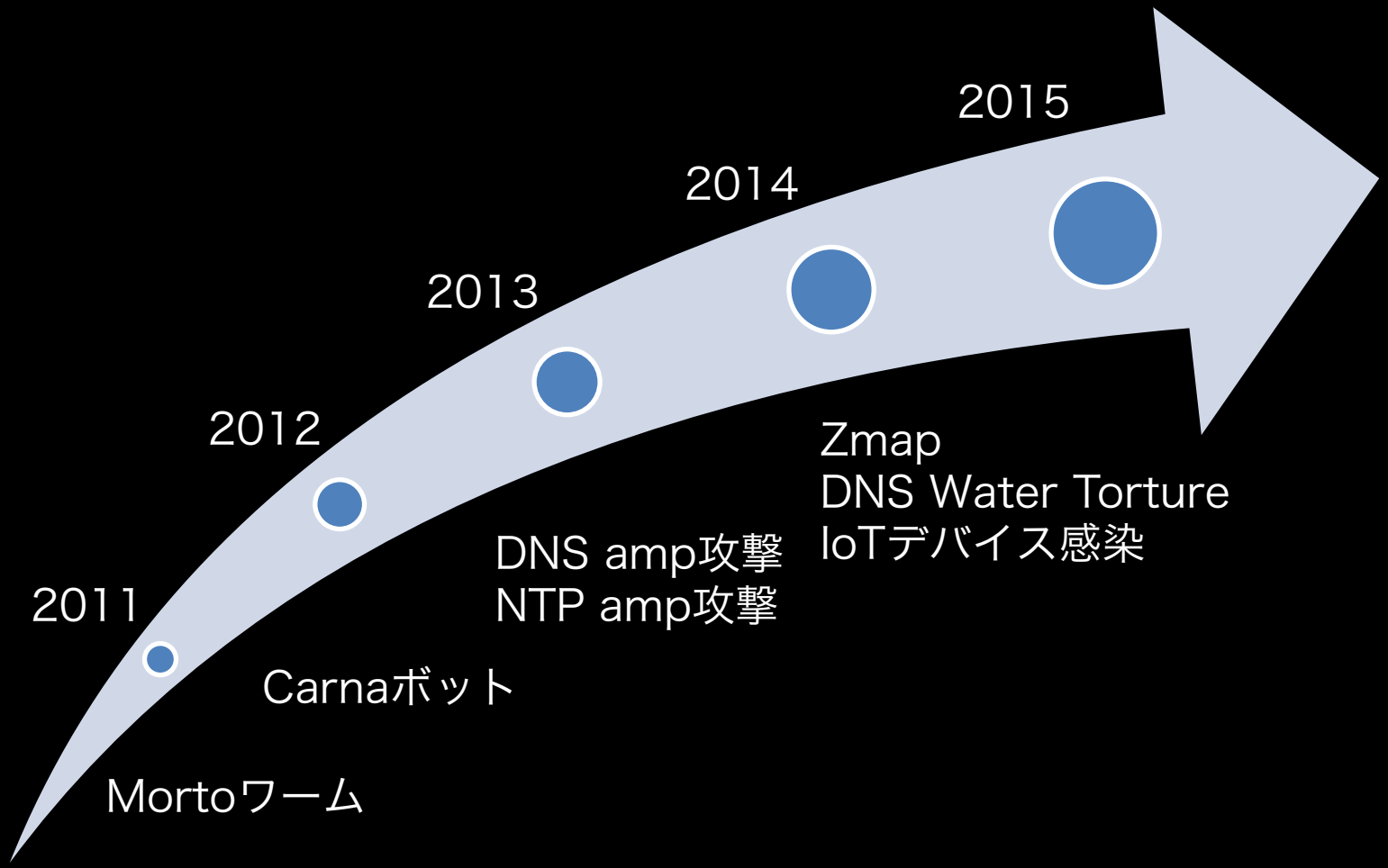


2015/04/01～2016/03/31の観測統計



NICTER
Network Incident analysis Center for Tactical Emergency Response

ここ数年の観測トピック

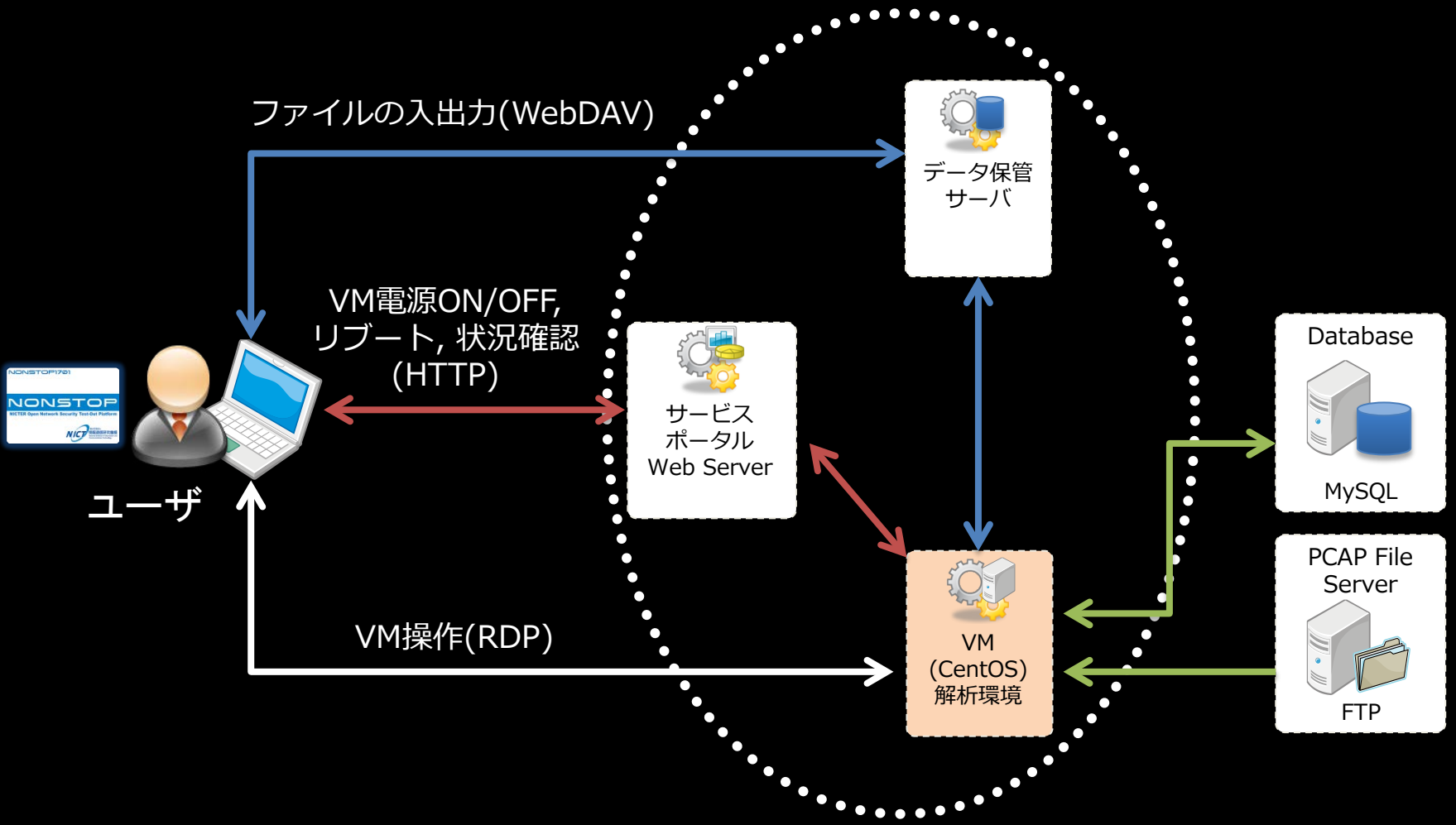


NONSTOPって？

- NICTERが持つサイバーセキュリティ情報（ダークネットトラフィック等）を遠隔から安全に利用してもらうための分析環境

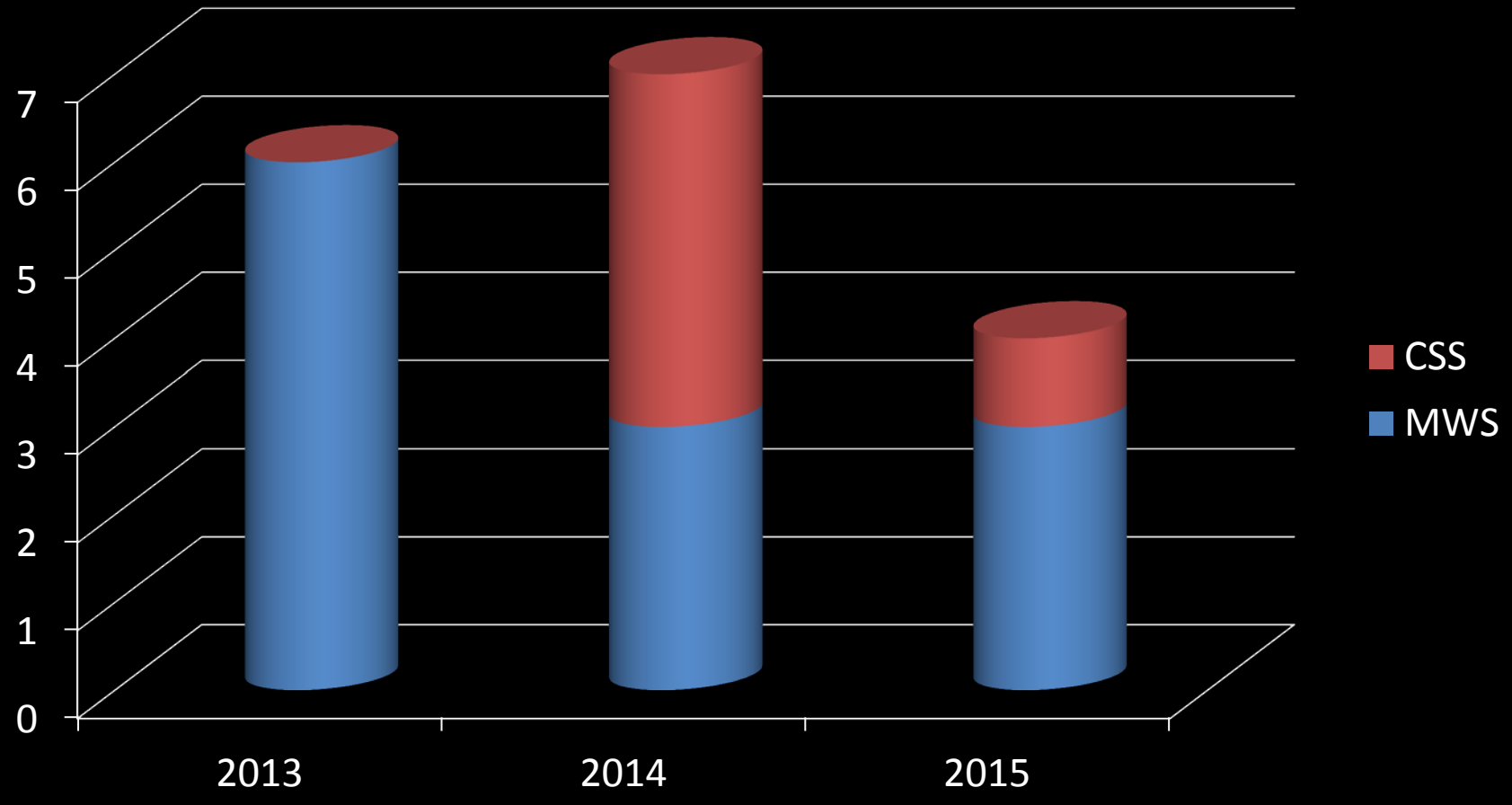
NICTER
Network Incident analysis Center for Tactical Emergency Response

NONSTOPって？



NICTER
Network Incident analysis Center for Tactical Emergency Response

NICTER Darknet 2013～2015利用実績



NICTER
Network Incident analysis Center for Tactical Emergency Response

ダークネットトラフィックを用いた関連研究

- [IMC12] A. Dainotti, et al.,
  “Analysis of a “/0” Stealth Scan from a Botnet”
- [IMC13] J. Czyz, et al.,
  “Understanding IPv6 Internet Background Radiation”
- [SIGCOMM14] A. Dainotti, et al.,
  “Estimating Internet Address Space Usage Through Passive Measurements”
- [NDSS14] C. Rossow,
  “Amplification Hell: Revisiting Network Protocols for DDoS Abuse”
- [Usenix Sec14] Z. Durumeric, et al.,
  “An Internet-Wide View of Internet Wide Scanning”
- [RAID15] L. Krämer, et al.,
  “AmpPot: Monitoring and Defending Against Amplification DDoS Attacks”
- [USENIX WOOT15] Y. M. Papa, et al.,
  “IoTPOT: Analysing the Rise of IoT Compromises”
- [GLOBECOM15] Y. Haga, et al.,
  “Increasing the Darkness of Darknet Traffic”