NICTER Dataset 2019

笠間　貴弘

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　研究マネージャー

National Institute of Information and Communications Technology

Network Incident analysis Center for Tactical Emergency Response

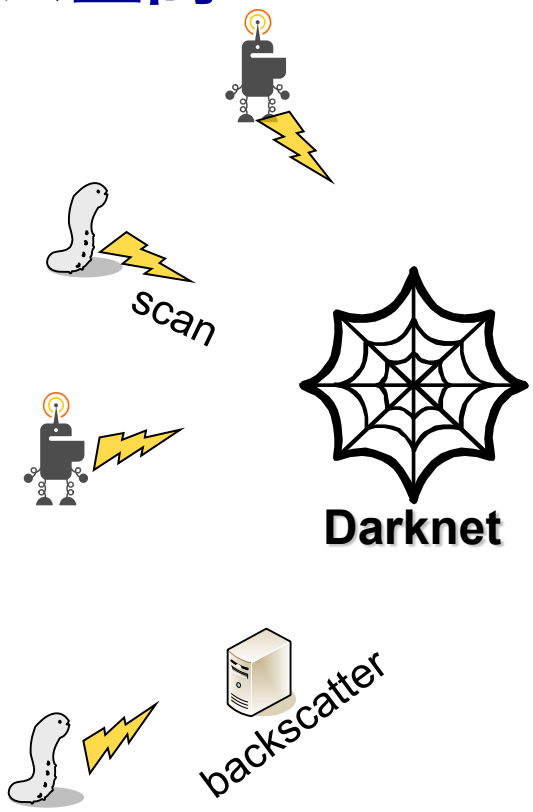
NICTER Dataset 2019

- **ダークネットトラフィックデータ**
  - ✓/20(約4千アドレス)のダークネットトラフィック
  - ✓観測期間は2011年4月1日から現在まで8年間以上
  - ✓NONSTOP上で提供（pcap+DB）

- **スパムメールデータ**
  - ✓NICTのメールサーバに届いたダブルバウンスメール
  - ✓観測期間は2015年1月1日から現在まで3年間以上
  - ✓NONSTOP上で提供（メールファイル）

ダークネット観測とは？

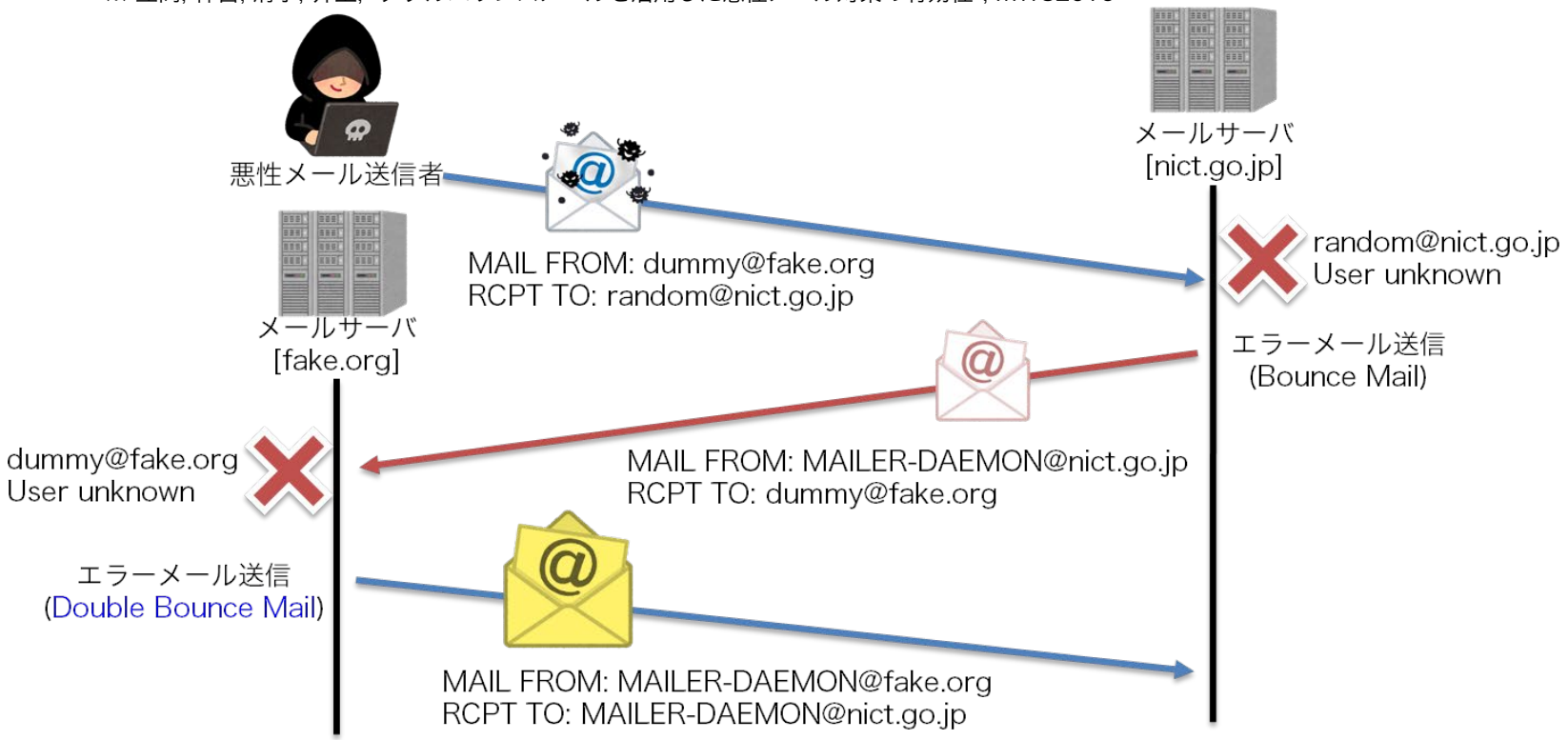
- **ダークネット：未使用のIPアドレス空間**
  - ✓正常な通信は “基本的に” 届かない
- **実際は大量の通信が届く**
  - ✓ マルウェアによるスキャン
  - ✓ DDoS攻撃の跳ね返り
  - ✓ リフレクション攻撃の準備活動
  - ✓ etc.
- **ダークネットの観測によって パンデミックの兆候が分かる**
  - ✓ パンデミック：マルウェアの大量感染



ダブルバウンスメールとは？

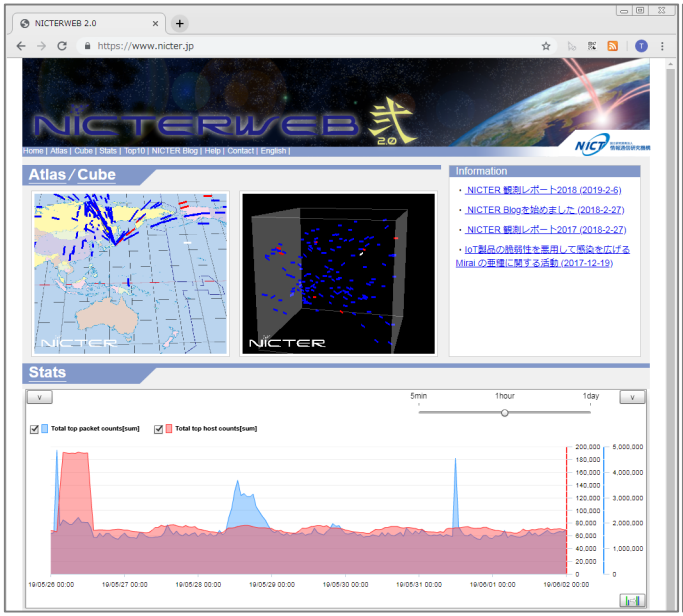
- **エラーメールの一種**
  - 主に送信元/宛先アドレスが存在しない場合に発生する
  - ほぼ全て悪性メール（宛先ランダム+送信元詐称）

※ 笠間, 神宮, 清水, 井上, “ダブルバウンスメールを活用した悪性メール対策の有効性”, MWS2016



観測結果の一般公開

- NICTERWEB (http://www.nicter.jp/)
- NICTER Blog (http://blog.nicter.jp)
- NICTER 観測レポート (http://www.nict.go.jp/cyber/report.html)



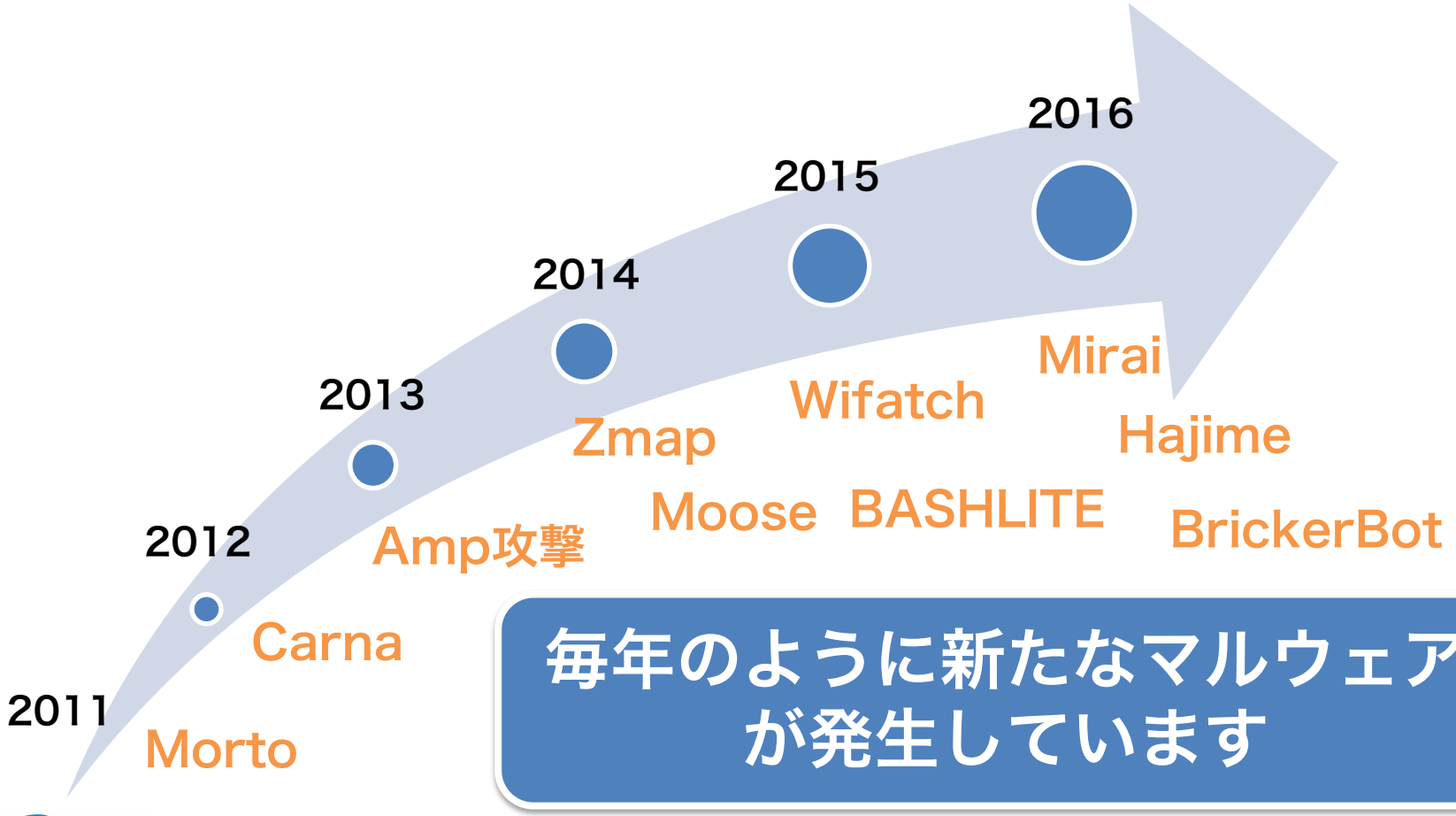
よくある誤解（その１）

- ワームとか古いし今時スキャンとか飛んでこないでしょ

10年間観測し続けていますが
基本的にずっと増加傾向です

よくある誤解（その２）

- スキャンしてるのなんて昔のConfickerだけでしょ



よくある誤解（その３）

- ダークネット使った研究とか枯れ果ててるでしょ

USENIX Sec'14

he 23rd USENIX Security Symposium, August 2014.

An Internet-Wide View of Internet-Wide Scanning

chael Bailey J. Alex Halderman

SIGCOMM'14

Estimating Internet Address Space Usage through I Measurements

USENIX WOOT'15

IoTPOT: Analysing the Rise of IoT Compromises

Yin [illegible]ki[†1], Katsunari Yoshioka[†1], Tsutomu Matsumoto[†1],
Kasama[†2], Christian Rossow[†3]
[†1]Gradua d Information Sciences/Institute of Advanced Sciences

NDSS'14

Amplification Hell: Revisiting Network Protocols for DDoS Abuse

Christian Rossow

NDSS'17

lberto Dainotti, Karyn Benson, Alistair King, kc claffy

Michael Kallitsis
Merit Network, Inc.
Ann Arbor, Michigan, USA

Eduard Glatz, Xenofontas Dimitropoulos
ETH Zurich

Internet-scale Probing of CPS: Inference, Characterization and Orchestration Analysis

Claude Fachkha[1,2], Elias Bou-Harb[3], Anastasis K

[1]New York University (N
[2]University
[3]Florida Atlan
[4]Georgia Institut

***Abstract*—Although the security of Cyber-Physical Systems (CPS) has been recently receiving significant attention from the research community, undoubtedly, there still exists a substantial lack of a comprehensive and a holistic understanding of attackers' malicious strategies, aims and intentions. To this end, this paper uniquely exploits passive monitoring and analysis of a newly deployed network telescope IP address space in a first attempt ever to build broad notions of real CPS maliciousness. Specifically, we approac**

IMC'15

Leveraging Internet Background Radiation for Opportunistic Network Analysis

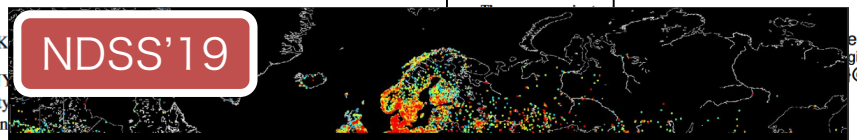
erto Dainotti[†], kc claffy[†], Alex C. Snoeren[⋆], Michael Kallitsis[‡]
gineering, UC San Diego [†]CAIDA, UC San Diego ‡Merit Network, Inc.
@caida.org, snoeren@cs.ucsd.edu, mgkallit@umich.edu

ic sent to unused regions
le insight into malicious
ore the utility of this traf-
ation (IBR), for a differ-
-wide measurements. We
larknets, carefully decon-
acterizing them along di-
easurements. Intuitively,

unused regions of the address space, known as Internet Background Radiation (IBR), to address this challenge.

Monitoring unused portions of the IPv4 address space reveals that IBR is of considerable volume, incessant, and originates from a variety of services [41, 48]. This unsolicited traffic is caused by scanning (e.g., searching for hosts running a vulnerable service), misconfigurations (e.g., a typo in the IP address for a mail server), backscatter (responses to packets with forged source IP addresses, including spoofed DoS attack), bugs, etc. Historically, researchers

NDSS'19



Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai

Orçun Çetin*,‡, Carlos Gañán*, Lisette Altena*, Takahiro Kasama***, Daisuke Inoue***, Kazuki Tamiya**, Ying Tie**, Katsunari Yoshioka** and Michel van Eeten*

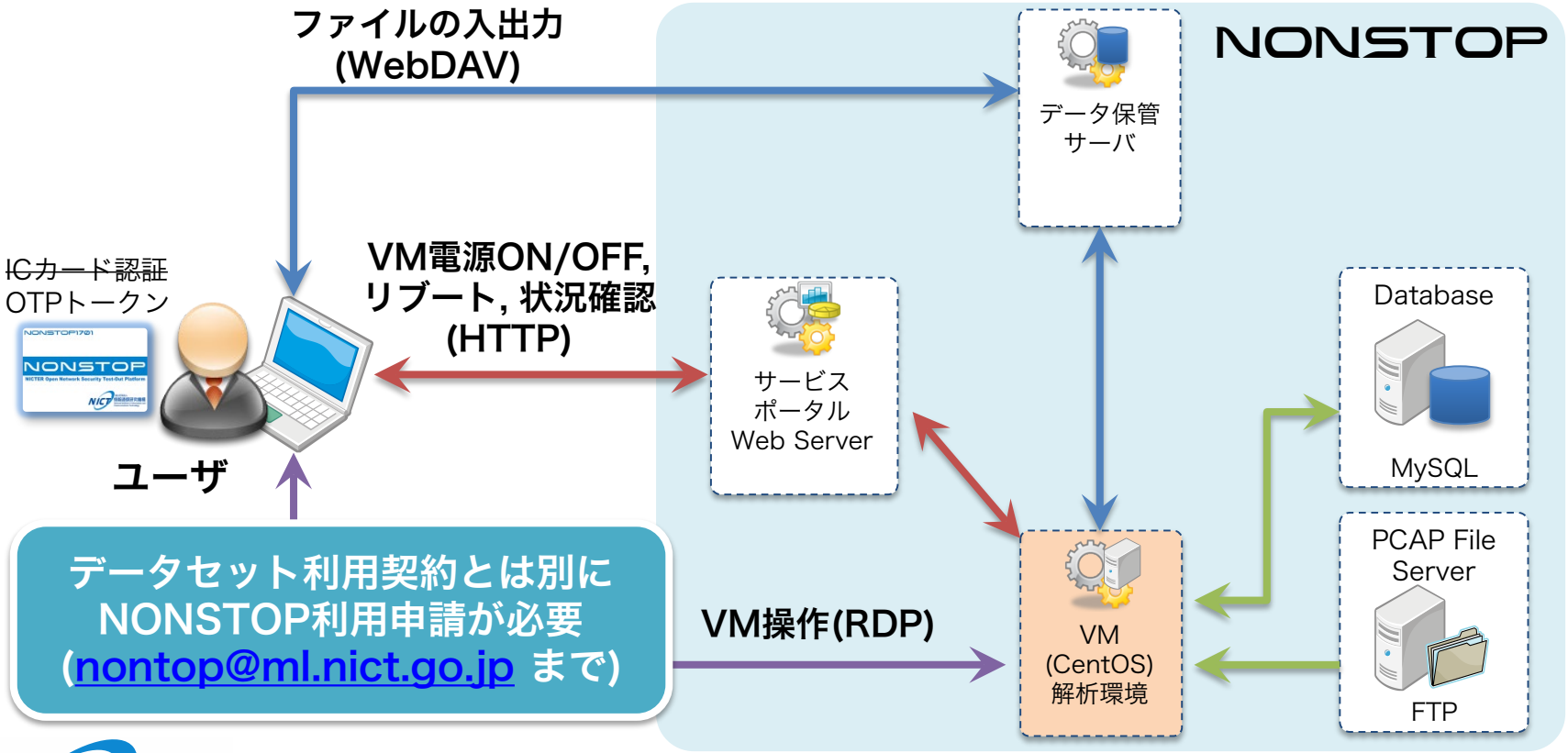
ダークネットデータを使った論文は
難関国際会議も含めて多数発表されています

NICT

ER
Emergency Response

NONSTOPって？

- NICTが持つサイバーセキュリティ情報を
  遠隔から安全に利用してもらうための環境



National Institute of Information and Communications Technology

Network Incident analysis Center for Tactical Emergency Response

NICTER Dataset まとめ

- **今年度提供するデータは２種類：**
  - ダークネットトラフィック
  - スパムメールデータ（要望があれば）
- **データセットはNONSTOP上で提供：**
  - データにアクセスできるVM環境をユーザ毎に用意
  - 利用申請は nonstop@ml.nict.go.jp まで
- **メリット：**
  - リアルタイムかつ継続的な長期間のデータセット提供
  - 加工されていない生データなので用途は自由