
NICTER Dataset 2018

注：本資料はほぼ2017年版と同じです

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 主任研究員
ナショナルサイバートレーニングセンター サイバートレーニング研究室(兼務)

NICTER Dataset 2018

● 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7年間以上
- ✓ NONSTOP上で提供 (pcap+DB)

● スпам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**

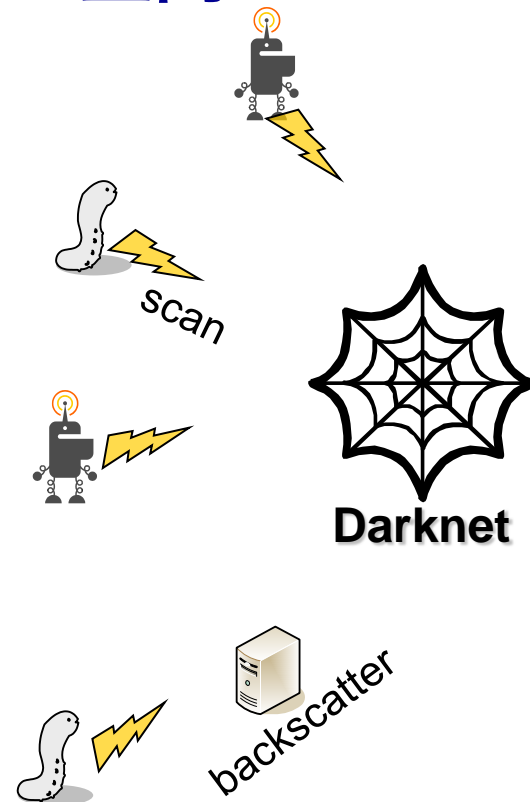
- ✓ 正常な通信は“基本的に”届かない

- **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

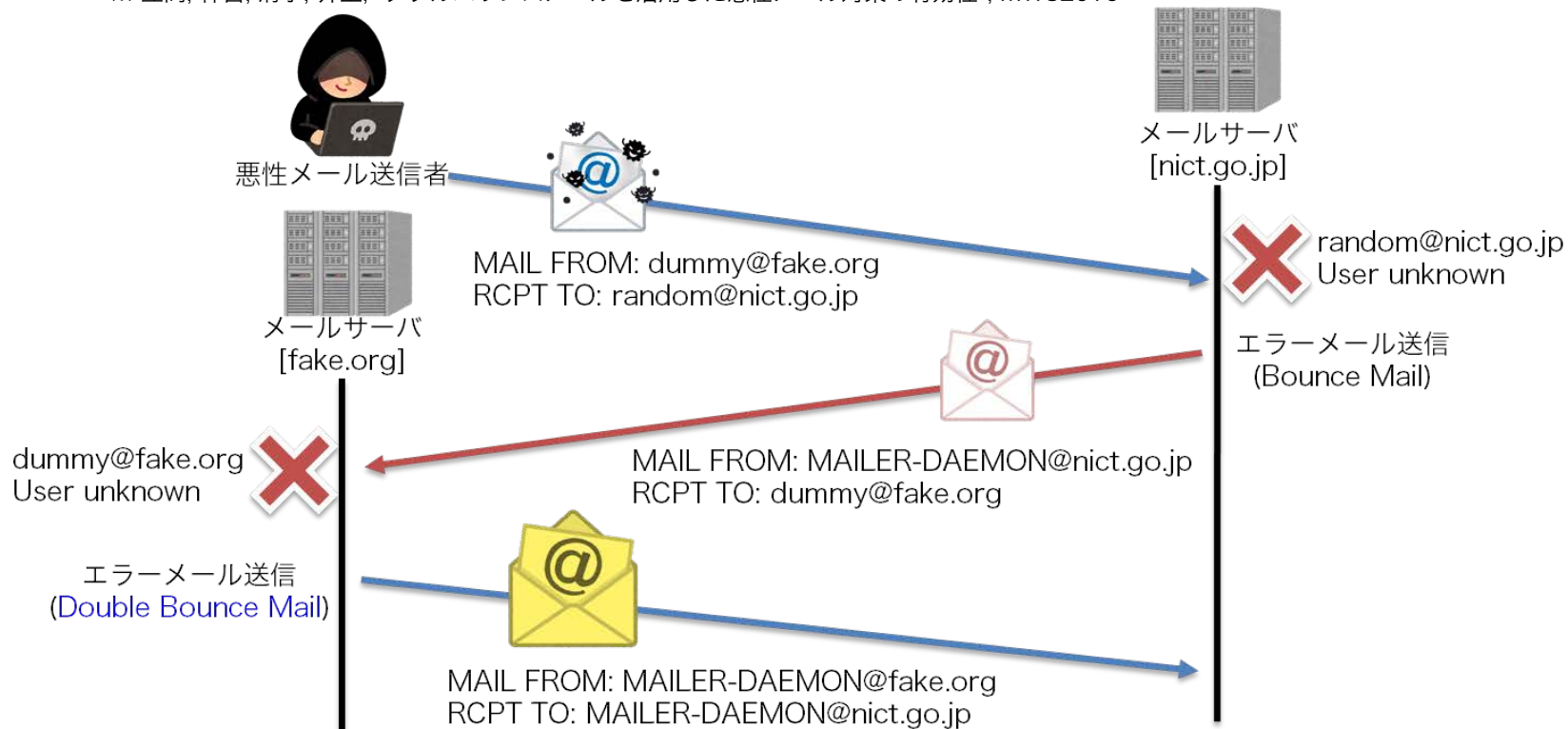


ダブルバウンスメールとは？

● 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



@2018年5月30日 MWS2018意見交換会

よくある誤解（その1）

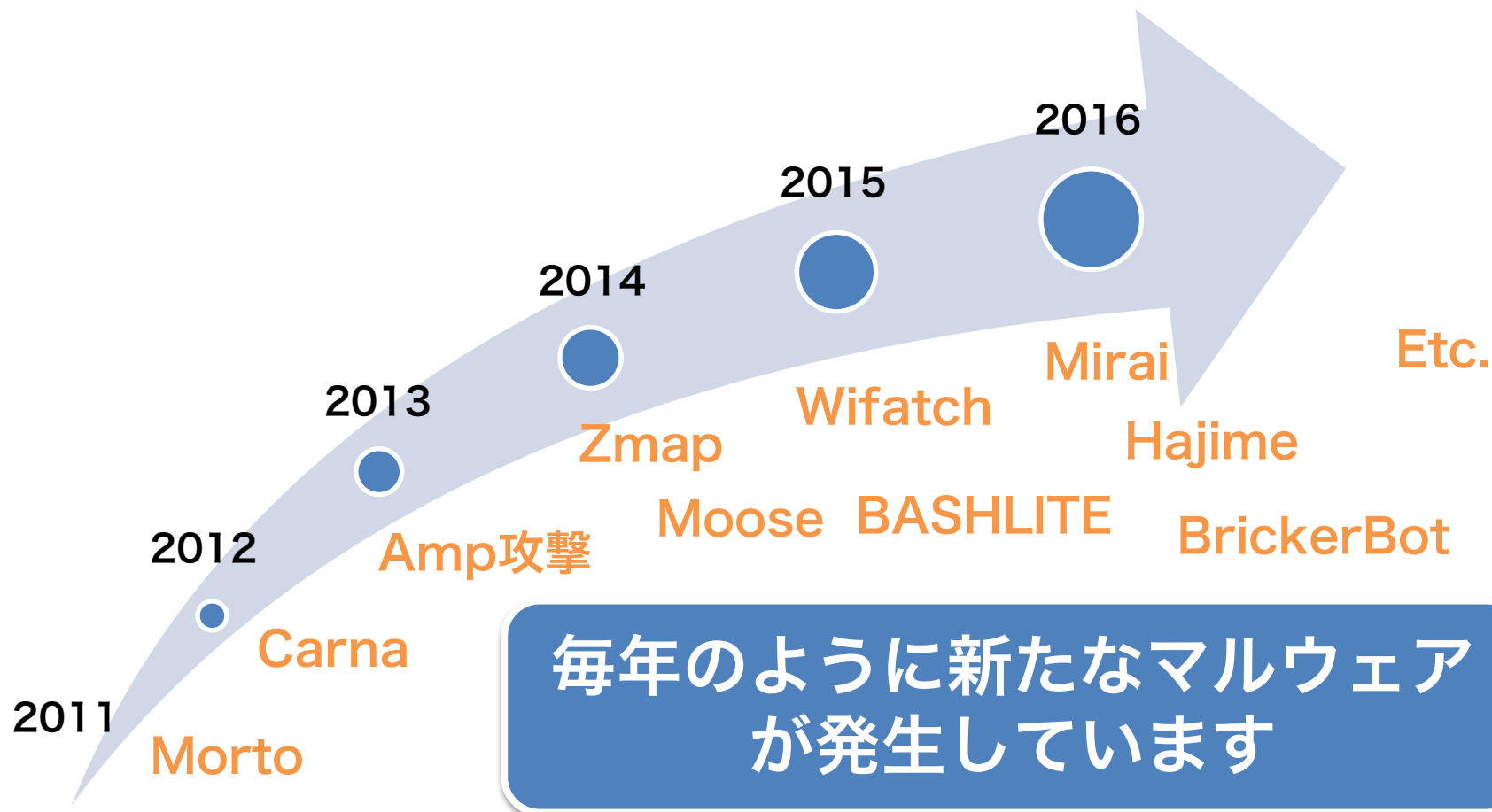
- ワームとか古いし今時スキャンとか飛んでこないでしょ

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



@2018年5月30日 MWS2018意見交換会

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 The 23rd USENIX Security Symposium, August 2014.

USENIX WOOT'15

SIGCOMM'14

NDSS'14

NDSS'17

IMC'15

An Internet-Wide View of Internet-Wide Scanning
Zakir Durumeric, Michael Bailey, J. Alex Halderman
University of Michigan, University of Michigan, University of Michigan

IoTPOT: Analysing the Rise of IoT Compromises
Yin Minn Pa Pa^{†1}, Shogo Suzuki^{†1}, Katsunari Yoshioka^{†1}, Tsutomu Matsumoto^{†1}, Takahiro Kasama^{†2}, Christian Rossow^{†3}
^{†1}Graduate School of Information Sciences/Institute of Advanced Sciences, ^{†2}Osaka National University, Japan, ^{†3}Rubicon Cyber Security, The Netherlands

Estimating Internet Address Space Usage through Measurements
Alberto Dainotti, Michael Kallitsis, Eduard Glatz, Xenofontas Dimitropoulos
University of Michigan, USA, Merit Network, Inc., ETH Zurich, ETH Zurich, Switzerland
{alberto.dainotti, kallitsis}@umich.edu, {kallitsis, eduard.glatz, xenofontas.dimitropoulos}@tik.ee.ethz.ch

Amplification Hell: Revisiting Network Protocols for DDoS Abuse
Christian Rossow
VU University Amsterdam, The Netherlands, Horst Görtz Institute for IT-Security, Ruhr University Bochum, Germany
{firstname.lastname}@rub.de

Internet-scale Probing of CPS: Inference, Characterization and...
Karyn Benson^{*†}, Alberto Dainotti[†], kc claffy[†], Alex C. Snoeren^{*}, Michael Kallitsis^{*}

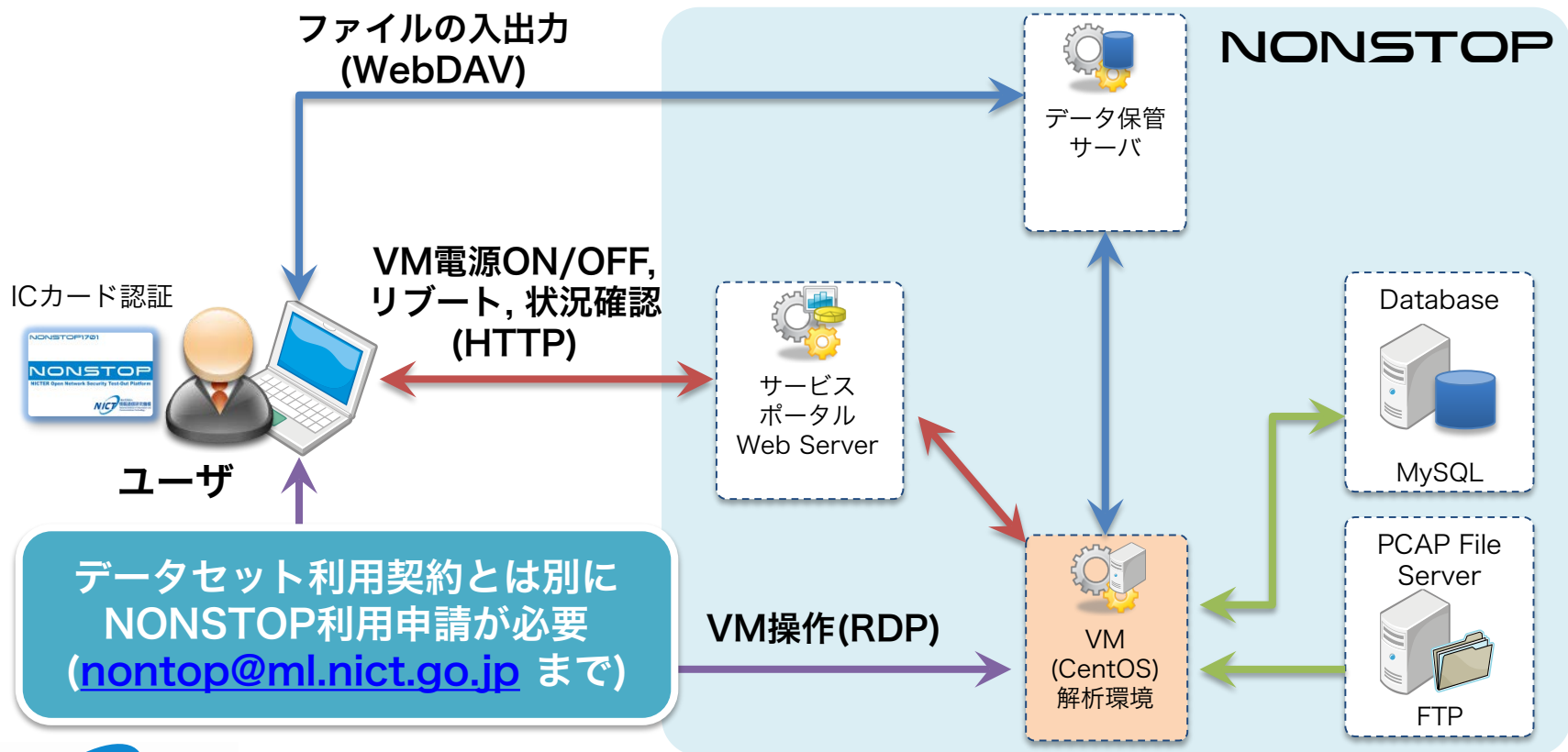
Leveraging Internet Background Radiation for Opportunistic Network Analysis
Karyn Benson^{*†}, Alberto Dainotti[†], kc claffy[†], Alex C. Snoeren^{*}, Michael Kallitsis^{*}

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

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 approach this problem by inferring, investigating, characterizing, and reporting large-scale probing activities that these systems have been undergoing large-scale transformations with the infusion of new "smart" cyber-based technologies to improve their efficiency and reliability. These transitions are being driven by continual advances and cost-

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



@2018年5月30日 MWS2018意見交換会

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памメールデータ
- 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