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)

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

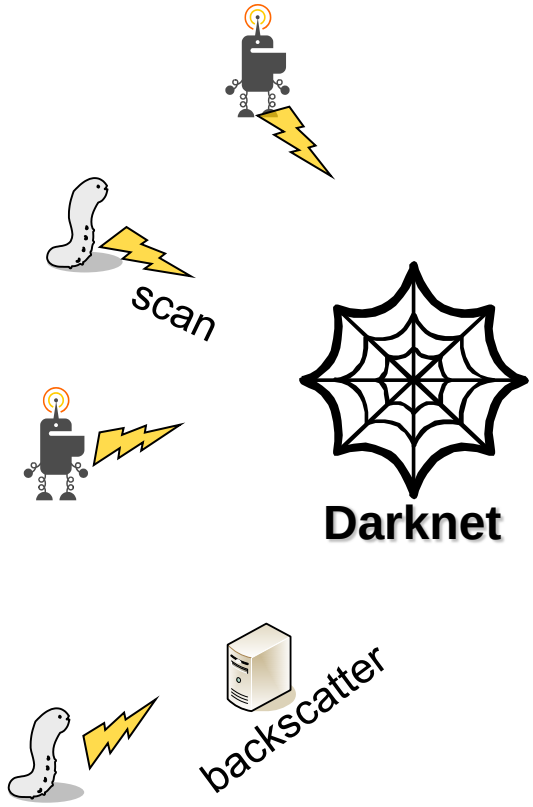
NICTER Dataset 2018

- **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？

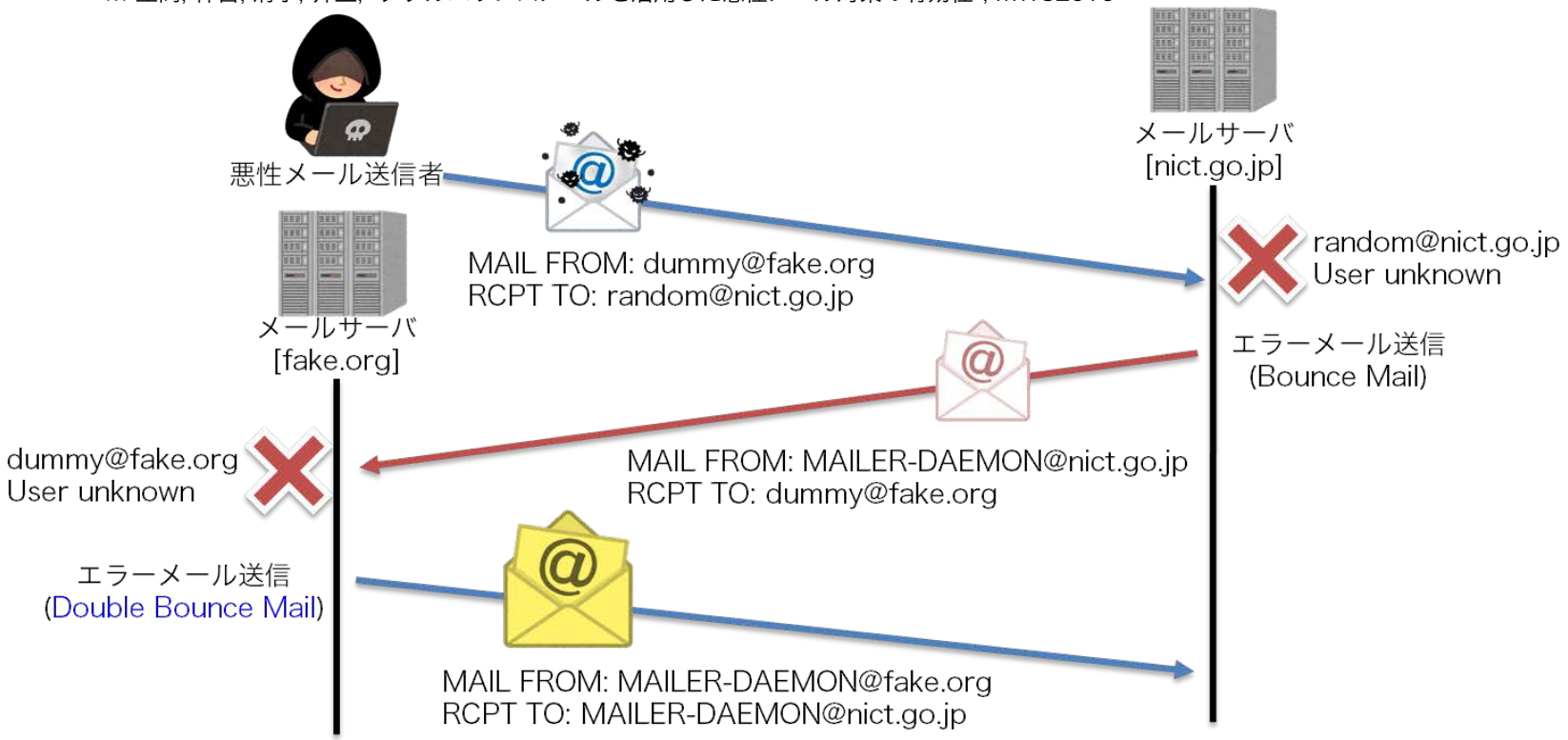
- **ダークネット：未使用のIPアドレス空間**
  - ✓正常な通信は “基本的に” 届かない
- **実際は大量の通信が届く**
  - ✓ マルウェアによるスキャン
  - ✓ DDoS攻撃の跳ね返り
  - ✓ リフレクション攻撃の準備活動
  - ✓ etc.
- **ダークネットの観測によって パンデミックの兆候が分かる**
  - ✓ パンデミック：マルウェアの大量感染



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



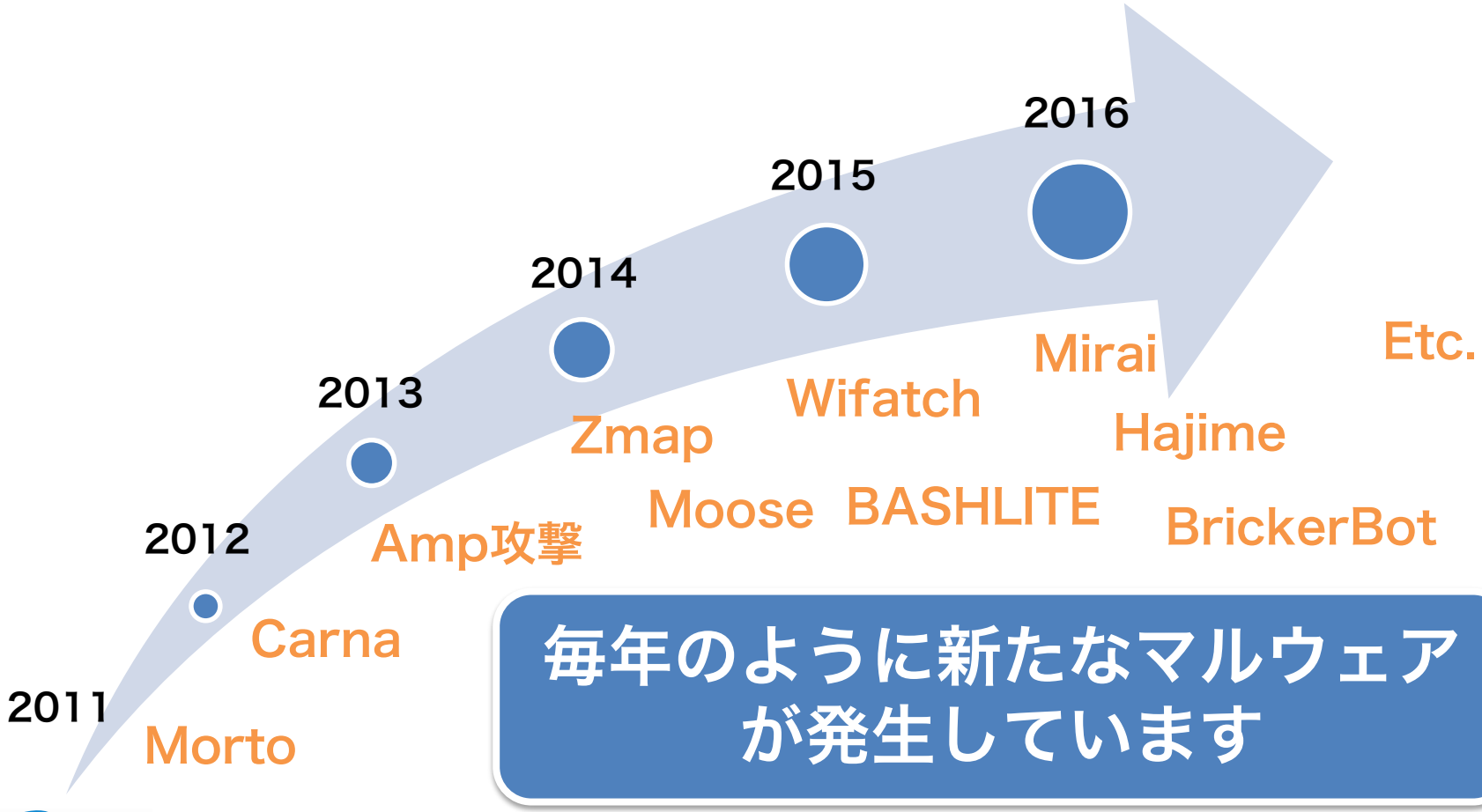
よくある誤解（その１）

- 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

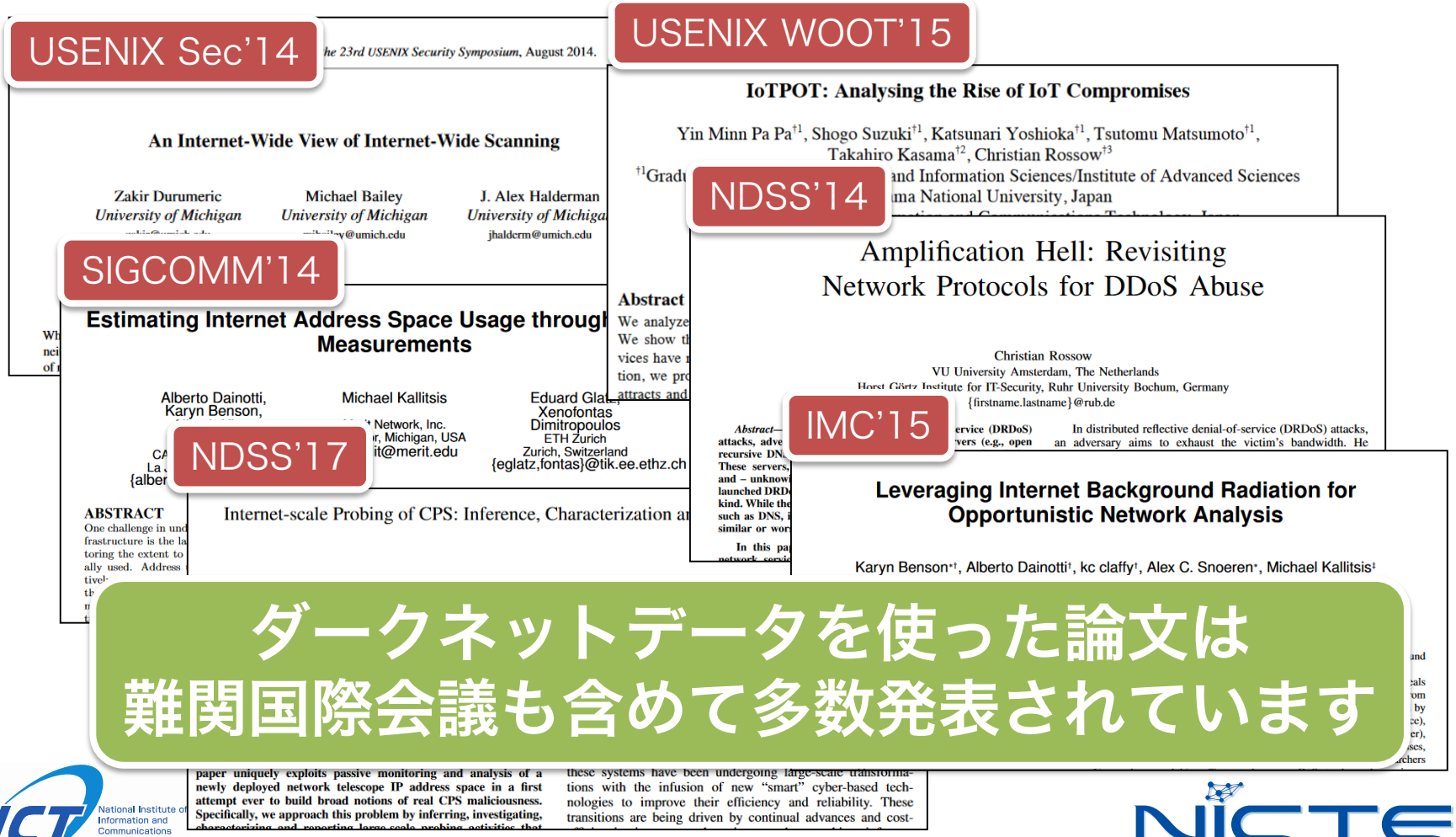
よくある誤解（その２）

- 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）

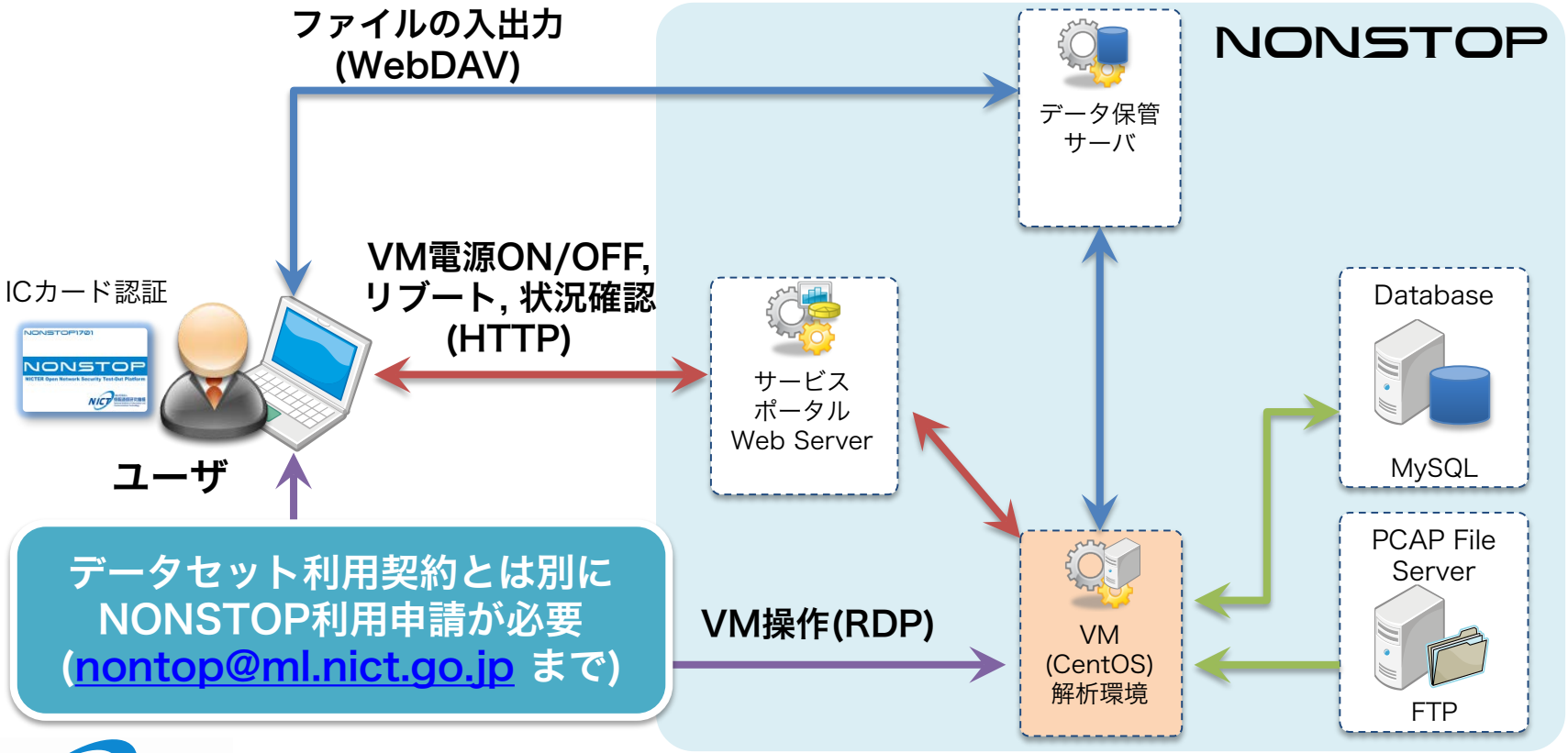
- ダークネット使った研究とか枯れ果ててるでしょ



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

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



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
- **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