NICTER Dataset 2017

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

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

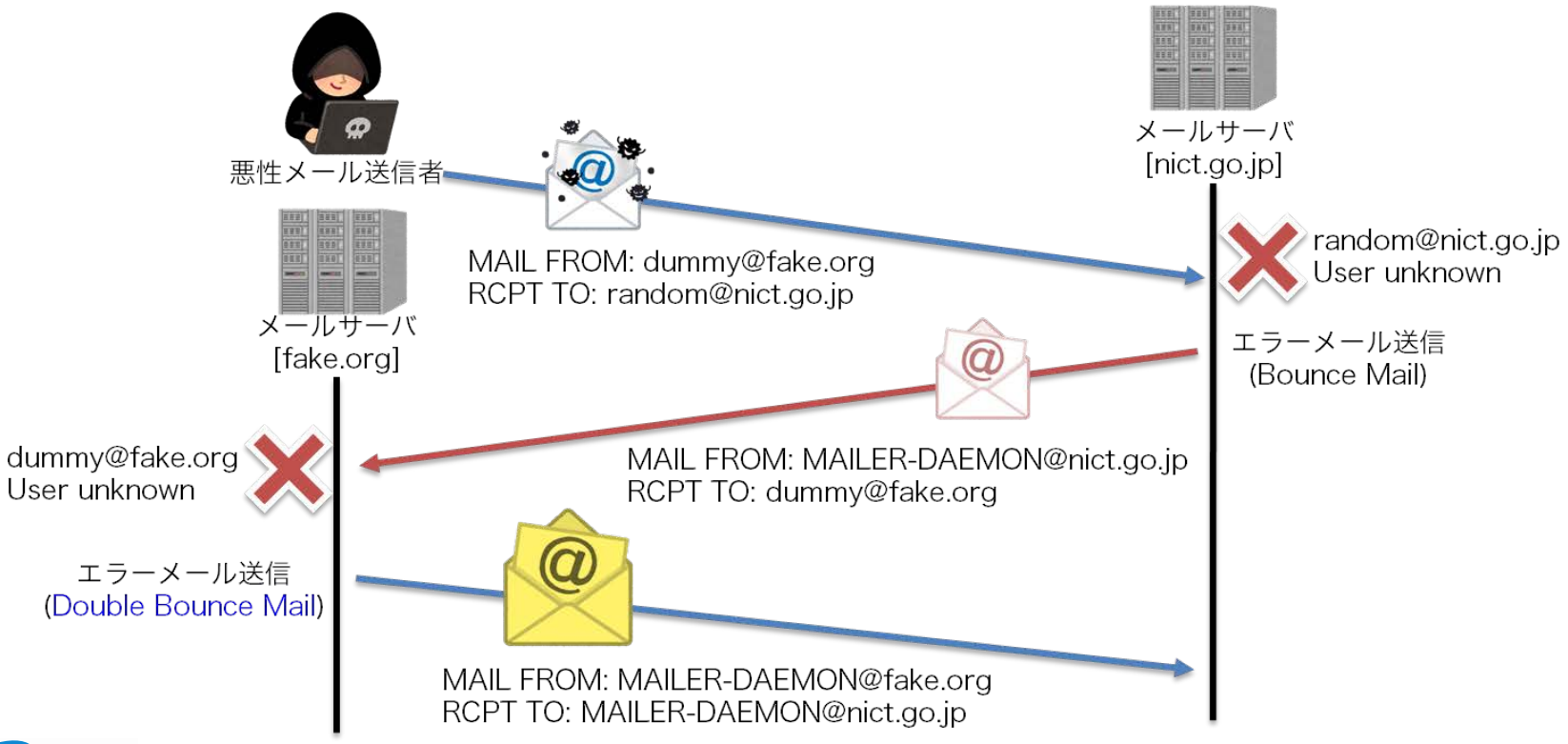
Darknet → Dataset

- **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6年間以上
  - NONSTOP上で提供（pcap+DB）

- **スパムメールデータ (New!)**
  - 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2年間以上
  - NONSTOP上で提供（メールファイル）

ダブルバウンスメールとは？

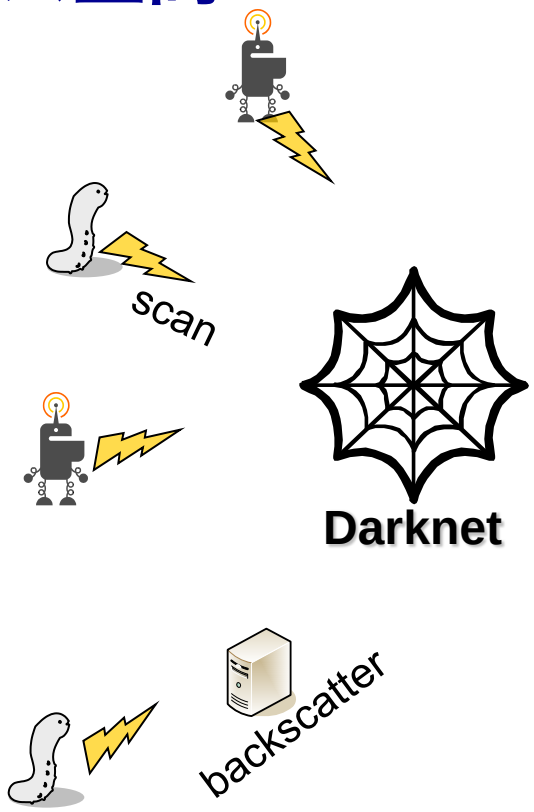
- **エラーメールの一種**
  - 主に送信元/宛先アドレスが存在しない場合に発生する
  - ほぼ全て悪性メール（宛先ランダム+送信元詐称）



※ 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
(MWS2016 ベストプラクティカル研究賞　受賞)

ダークネット観測とは？

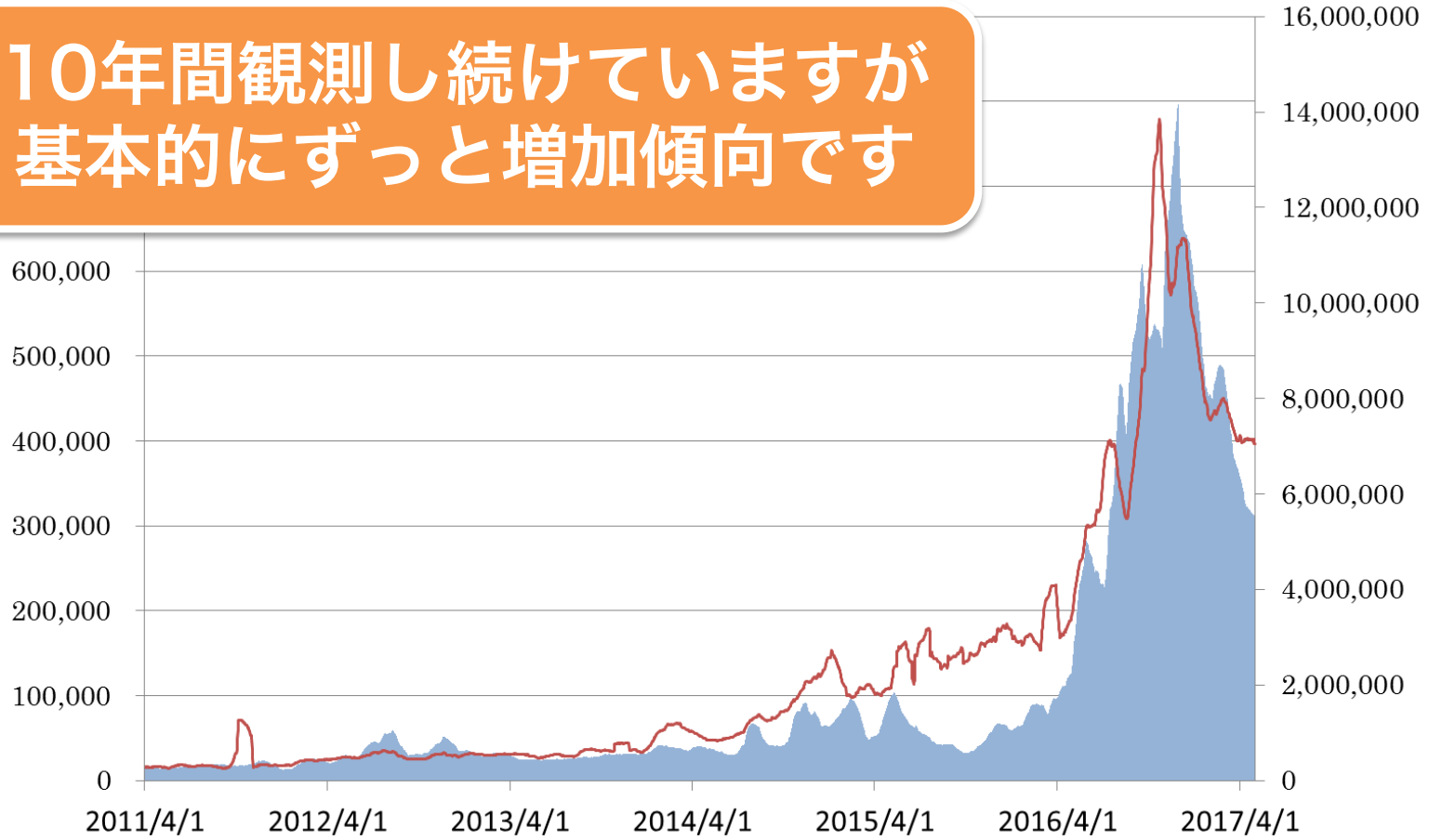
- **ダークネット：未使用のIPアドレス空間**
  - ✓正常な通信は “基本的に” 届かない
- **実際は大量の通信が届く**
  - ✓ マルウェアによるスキャン
  - ✓ DDoS攻撃の跳ね返り
  - ✓ リフレクション攻撃の準備活動
  - ✓ etc.
- **ダークネットの観測によって パンデミックの兆候が分かる**
  - ✓ パンデミック：マルウェアの大量感染



よくある誤解（その１）

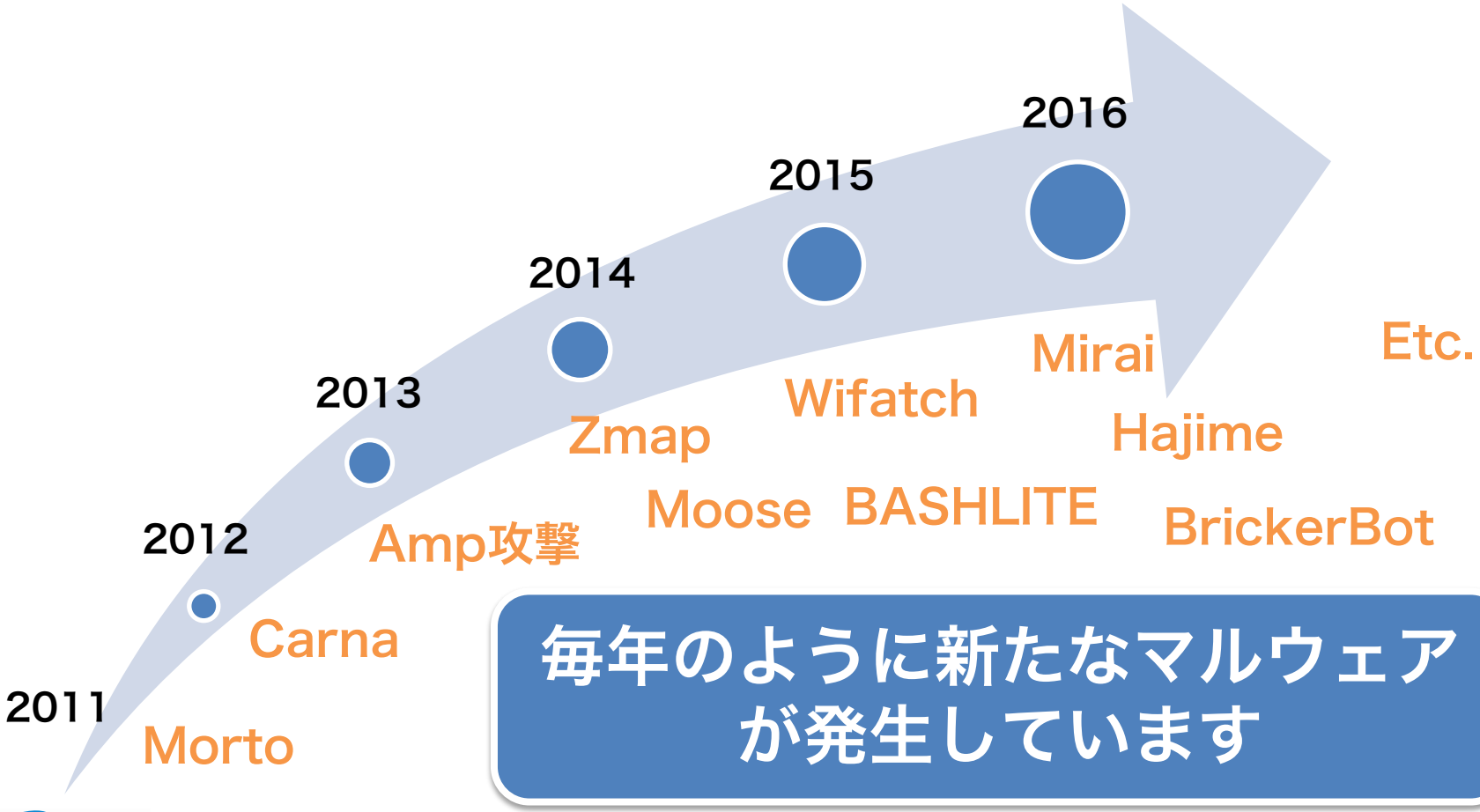
- ワームとか古いし今時スキャンとか飛んでこないでしょ

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



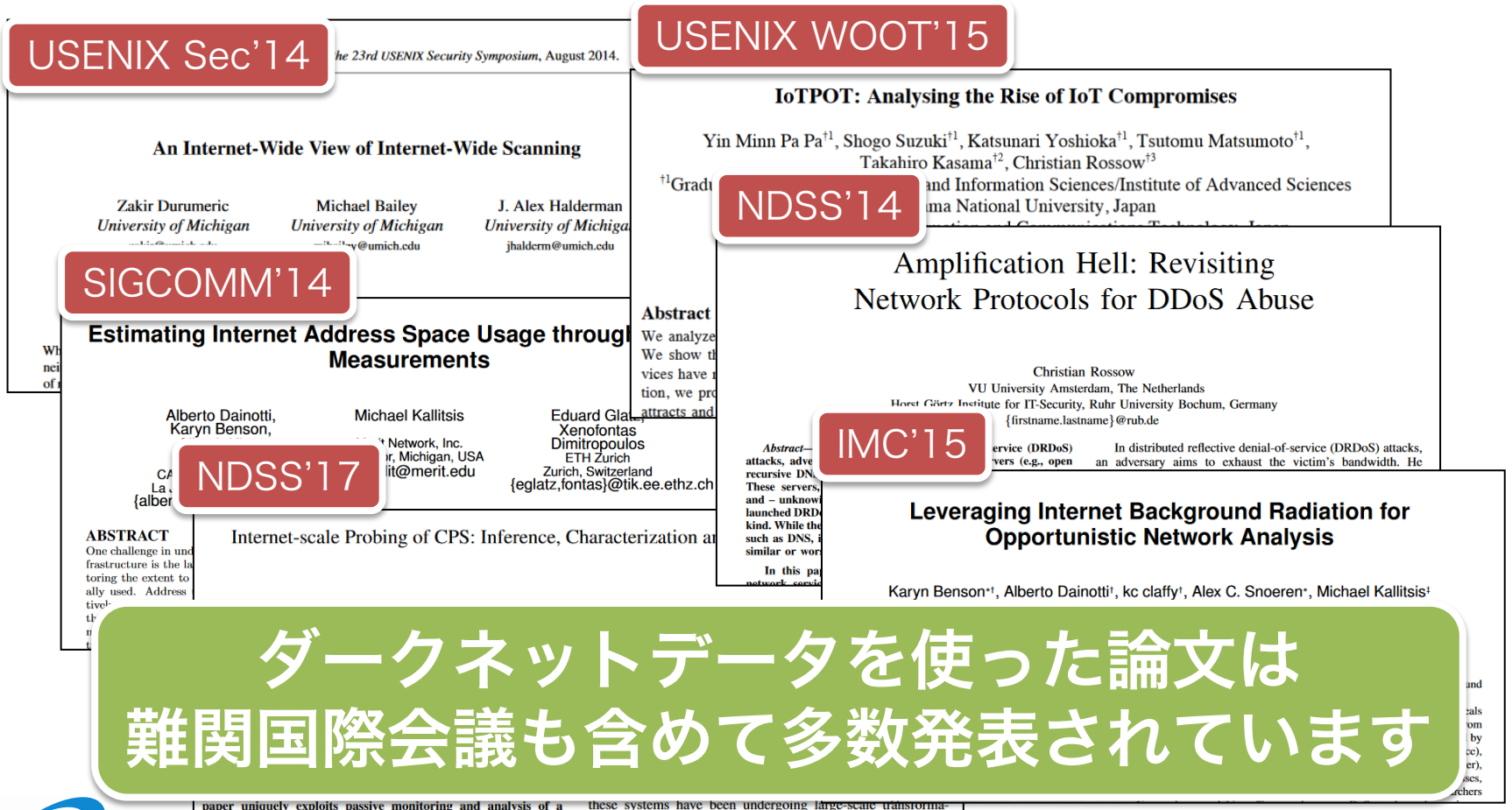
よくある誤解（その２）

- 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）

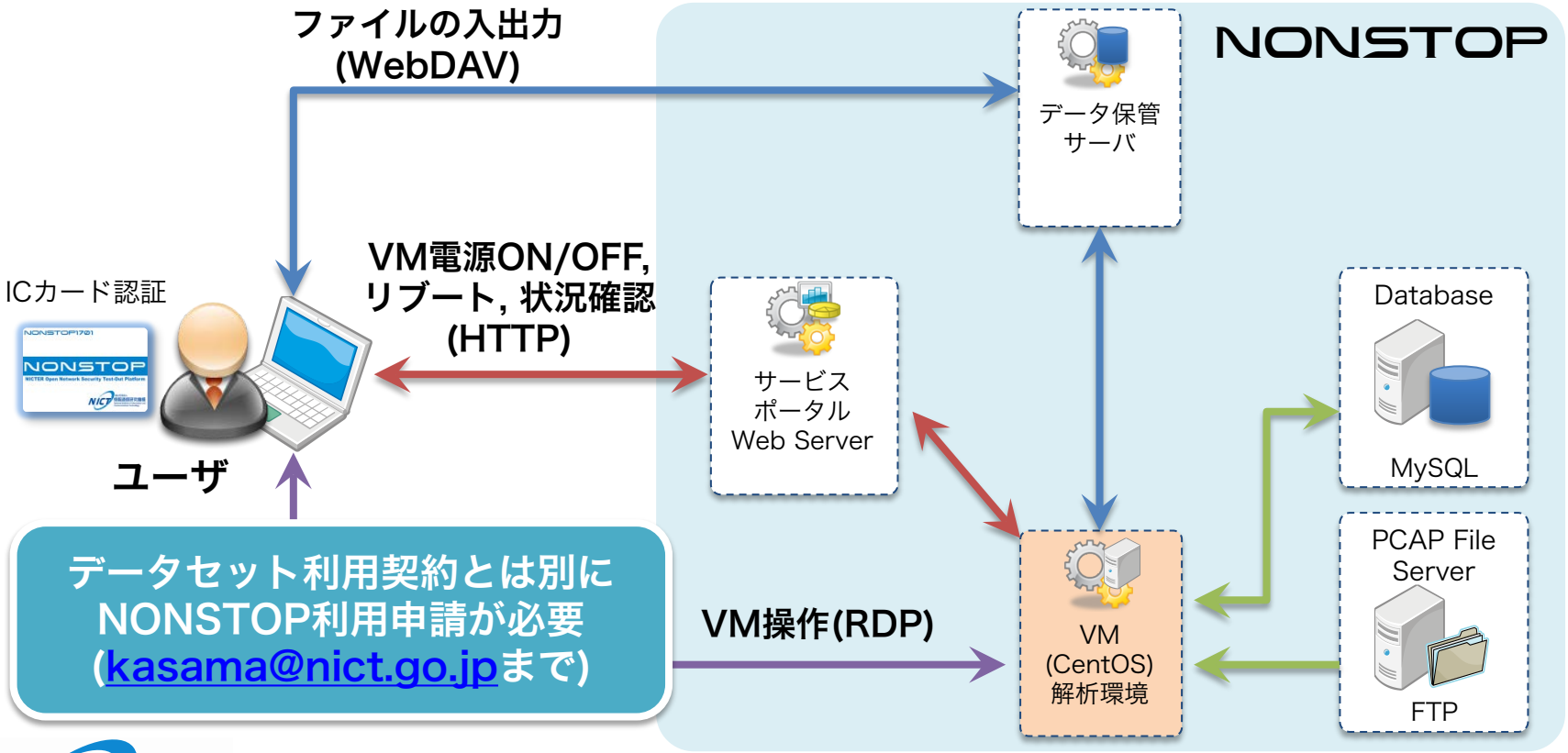
- ダークネット使った研究とか枯れ果ててるでしょ



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？

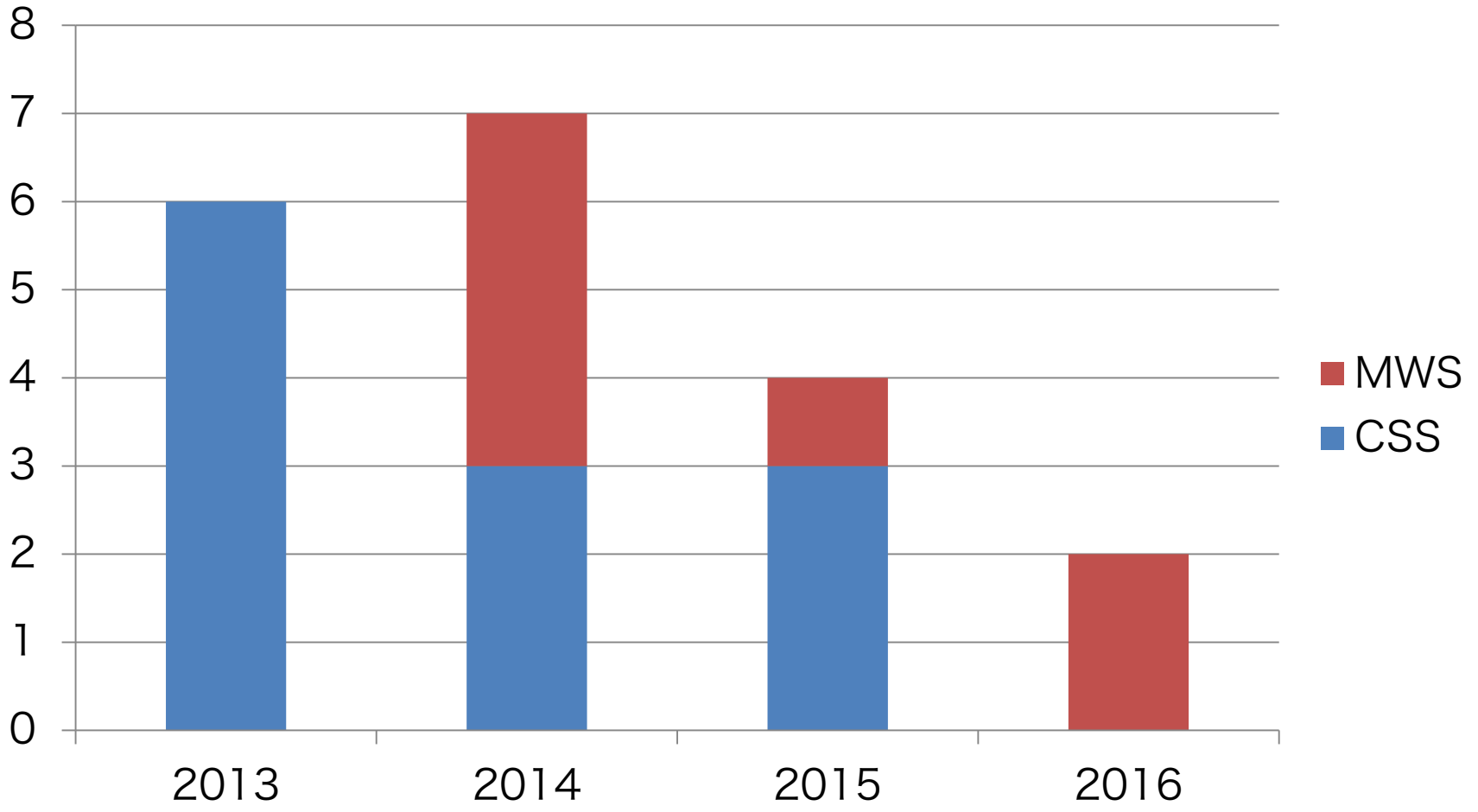
- NICTが持つサイバーセキュリティ情報を
  遠隔から安全に利用してもらうための環境



National Institute of Information and Communications Technology

Network Incident analysis Center for Tactical Emergency Response

NICTER Darknet 利用実績



※MWSのデータセット契約枠としては0件

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NICT笠間(kasama@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
- *需要(実績)が無いなら(いずれ)供給は止まります*
  - *積極的な論文投稿を期待しています！*