NICTER Dataset 2022

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
副室長

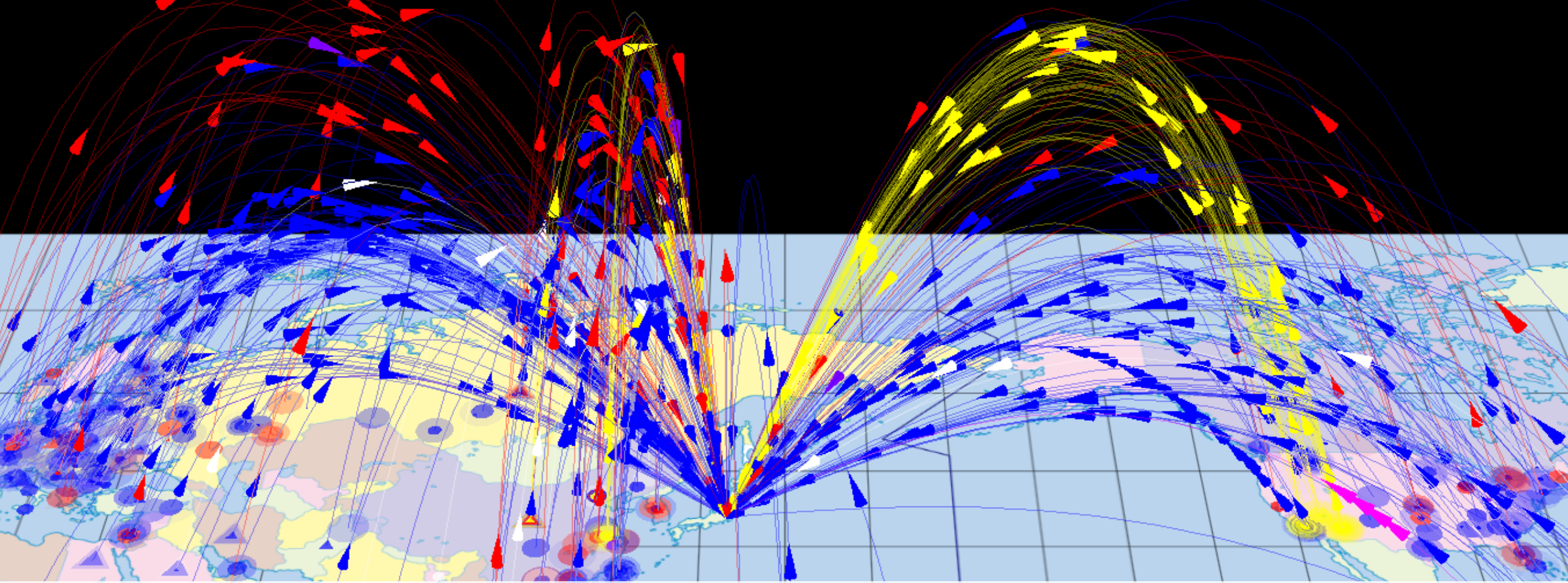
NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

NICTER Dataset 2022

- 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
  - ✓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
  - ✓NONSTOP上で提供（メールファイル）

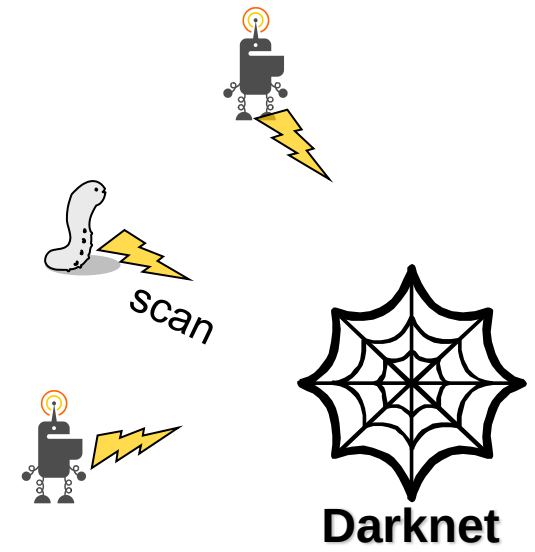


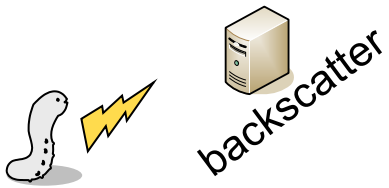
NICTER

- サイバー攻撃リアルタイム大規模観測・分析システム
- 国内外で30万の未使用IPアドレス“**ダークネット**”を観測
- 無差別型サイバー攻撃の大局的な傾向把握に有効

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





NICTER Dataset は 2022年で10周年を迎えました

National Institute of Information and Communications Technology

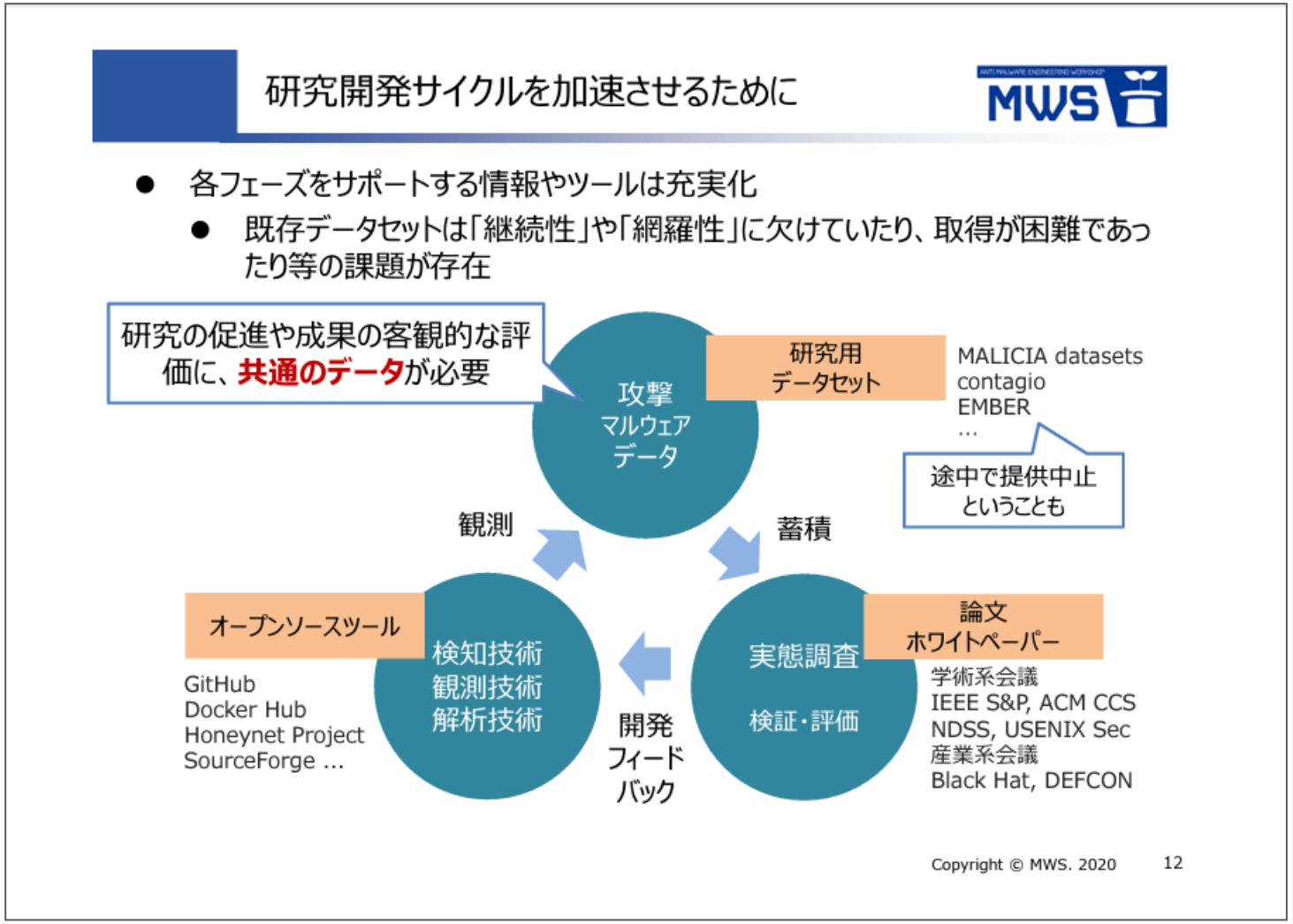
NICTER Network Incident analysis Center for Tactical Emergency Response

MWS Dataset 15年間の変遷

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
CCC DATAset (CCC)															
MARS for MWS (NICT)															
D3M (NTT研)															
IIJ MITF DATAset (IIJ)															
PRACTICE Dataset (Ncom)															
PRACTICE (AmpPot) Dataset (横浜国大)															
FFRI Dataset (FFRI)															
NICTER Dataset (NICT)															
BOS (日立)															
NCD in MWS Cup (MWS)															
MWS Cup Dataset (MWS)															
Soliton Dataset (ソリトン)															
Augma Dataset (nao_sec)															

10年間(12年分)
同じ形式のデータを提供し続けているのは
NICTER Dataset だけ

「継続」の重要性と難しさ(NICTERは今年で18年目)



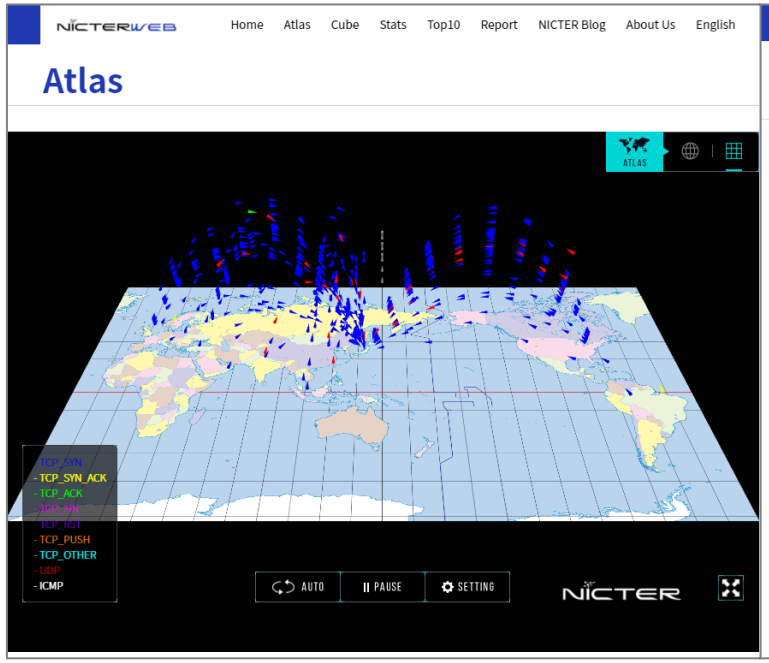
[出典] 寺田真敏, 他: マルウェア対策のための研究用データセット MWS Datasets ～コミュニティへの貢献とその課題～, 情報処理学会, Vol.2020-IFAT-139 No.8, 2020年7月.発表資料

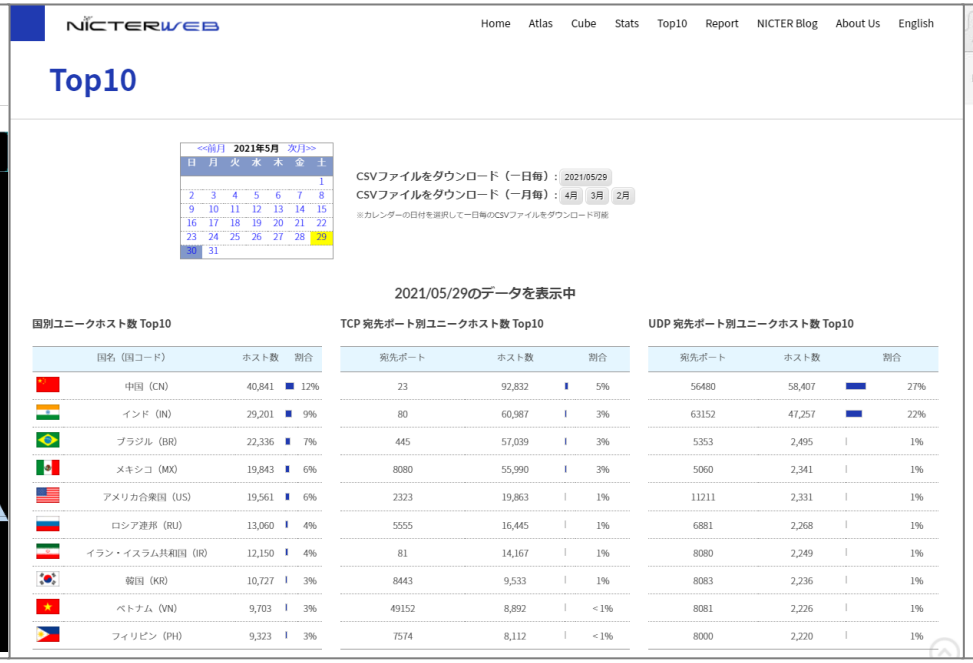
@2022年7月12日 MWS2022 プレミーティング

NICT National Institute of Information and Communications Technology
NICTER Network Incident analysis Center for Tactical Emergency Response

観測結果や分析結果は一般公開もしています

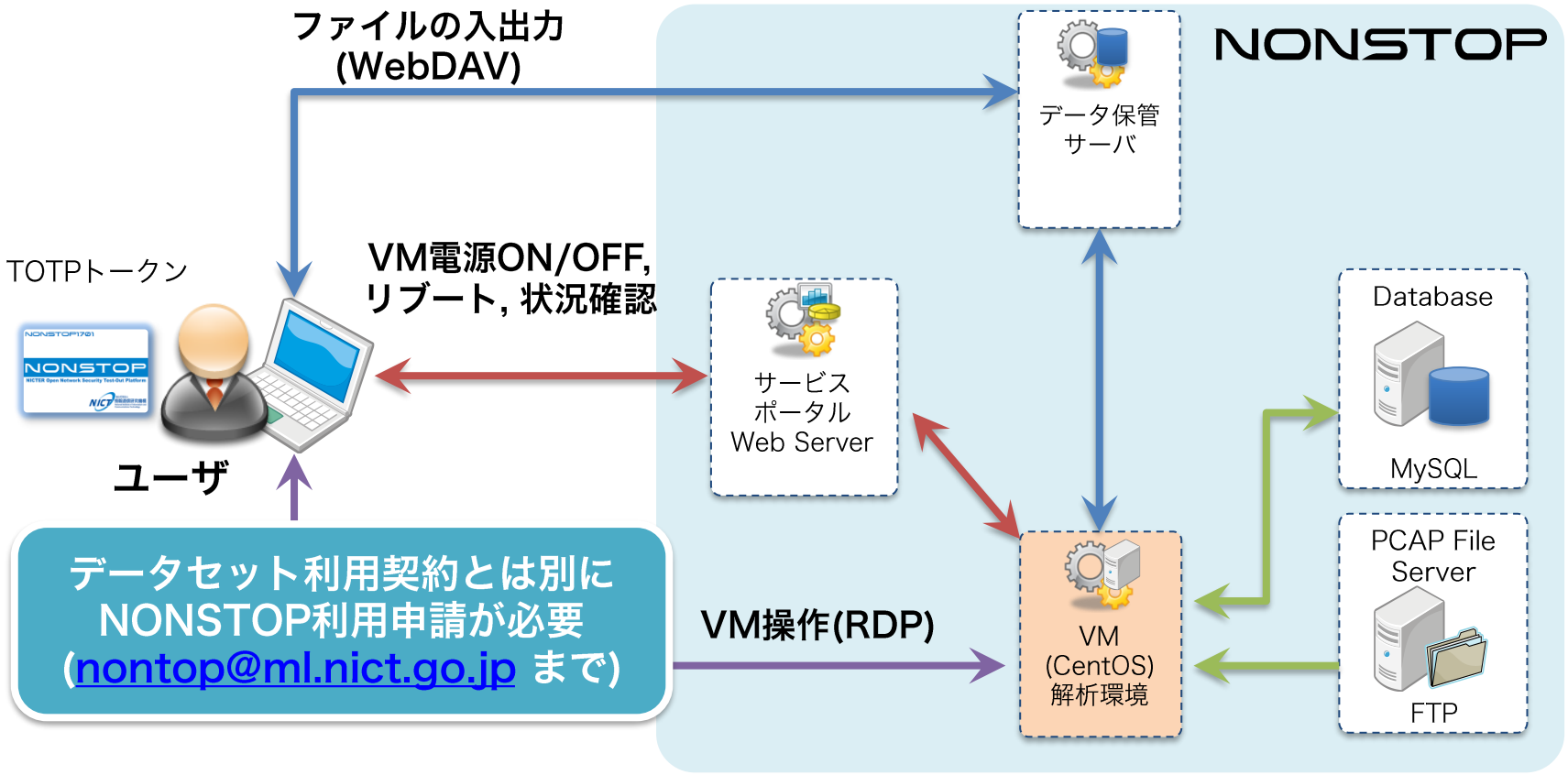
- NICTERWEB (http://www.nicter.jp/)
- NICTER Blog (http://blog.nicter.jp)
- NICTER 観測レポート 2016~2021





NICTERデータセットはNONSTOP上で提供

- 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



まとめ

- **データセットに興味があり利用したい方は**
  - MWS Dataset 利用のための覚書のやり取りを終えた後に
  - nonstop@ml.nict.go.jp に利用希望の連絡をしてください

- **昨年度利用していて継続利用を希望される方も**
  - データセット利用(NICTとMWSとの契約)は1年間ですので毎年継続の申請が必要です
  - 継続利用希望の連絡が無い場合は、NONSTOPのVMを停止しています

- **NICTは引き続きDatasetの最長記録を更新していきます**
  - 利用者がゼロになったら役目は終わり