
NICTER Dataset

2022

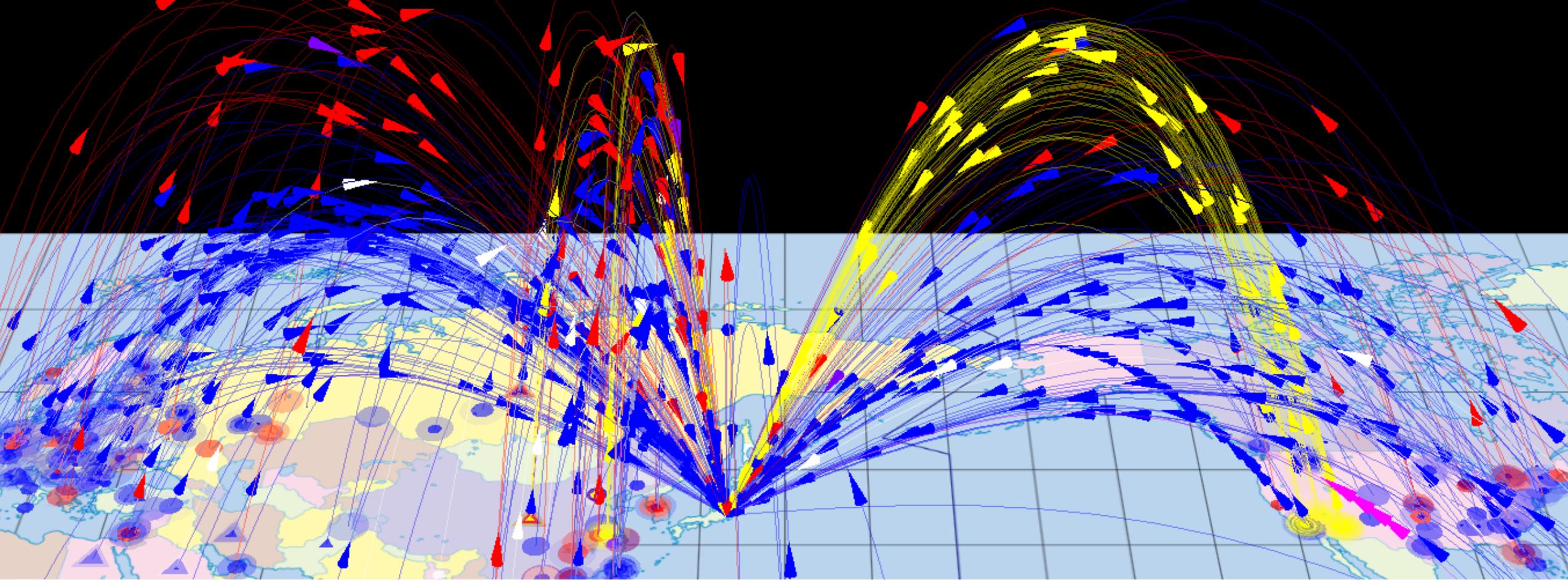
笠間 貴弘

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

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
 - ✓ 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

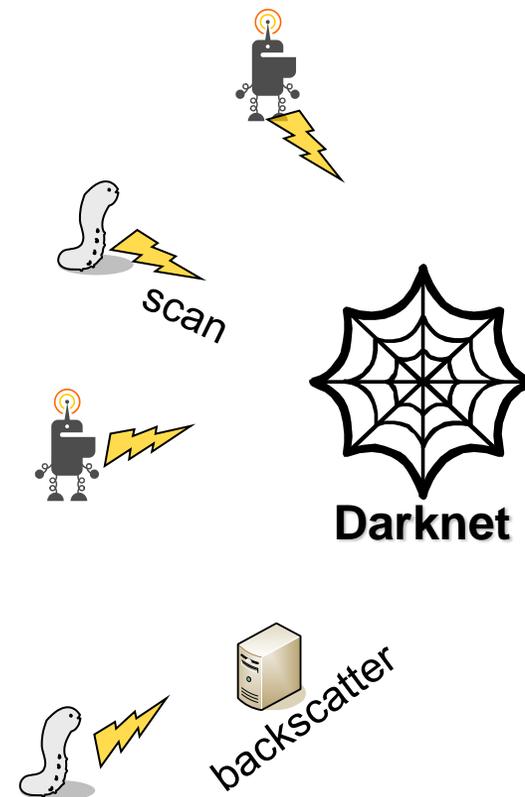
- ✓ 正常な通信は“基本的に”届かない

- 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

<p>MWS 2013 意見交換会 (2013/06/12)</p> <p>nicter darknet 2013</p> <p>情報通信研究機構 ネットワークセキュリティ研究所 サイバーセキュリティ研究室</p> <p>笠間 貴弘</p>  	<p>NICTER Darknet 2014</p> <p>独立行政法人 情報通信研究機構 (NICT)</p> <p>笠間貴弘 神園雅紀</p>  	<p>MWS意見交換会 1</p> <p>NICTER DARKNET DATASET データ解析のノウハウ</p> <p>早稲田大学 森達哉 研究室 芳賀夢久, 笹生憲</p> <p>2015/05/13 MWS意見交換会</p> <p>NICTER Darknet 2016</p> <p>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</p> <p>笠間 貴弘</p>	
<p>NICTER Dataset 2017</p> <p>笠間 貴弘</p> <p>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</p>  	<p>NICTER Dataset 2018</p> <p>注：本資料はほぼ2017年版と同じです</p> <p>笠間 貴弘</p> <p>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)</p>  	<p>NICTER Dataset 2019</p> <p>笠間 貴弘</p> <p>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</p>  	<p>NICTER Dataset 2020</p> <p>笠間 貴弘</p> <p>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</p>  
<p>NICTER Dataset 2021</p> <p>笠間 貴弘</p> <p>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</p>  			

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)	Orange	Orange	Orange	Orange	Orange	Orange	Light Blue								
MARS for MWS (NICT)	Orange														
D3M (NTT研)	Light Blue														
IIJ MITF DATASet (IIJ)	Light Blue														
PRACTICE Dataset (Ncom)	Light Blue														
PRACTICE (AmpPot) Dataset (横浜国大)	Light Blue														
FFRI Dataset (FFRI)	Light Blue														
NICTER Dataset (NICT)	Light Blue														
BOS (日立)	Light Blue														
NCD in MWS Cup (MWS)	Light Blue														
MWS Cup Dataset (MWS)	Light Blue														
Soliton Dataset (ソリトン)	Light Blue														
Augma Dataset (nao_sec)	Light Blue														

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

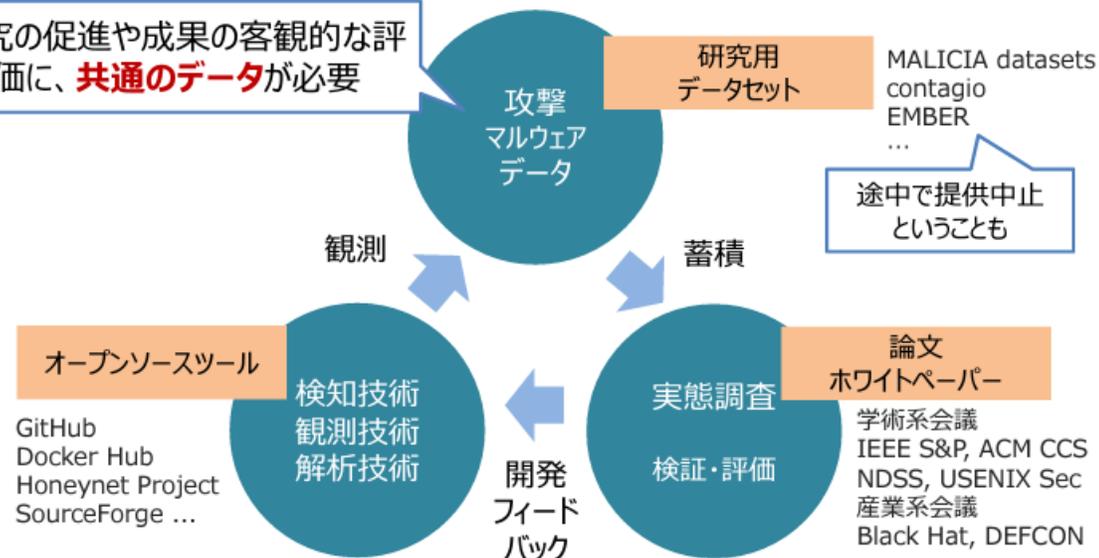
「継続」の重要性と難しさ (NICTERは今年で18年目)

研究開発サイクルを加速させるために



- 各フェーズをサポートする情報やツールは充実化
 - 既存データセットは「継続性」や「網羅性」に欠けていたり、取得が困難であったり等の課題が存在

研究の促進や成果の客観的な評価に、**共通のデータ**が必要



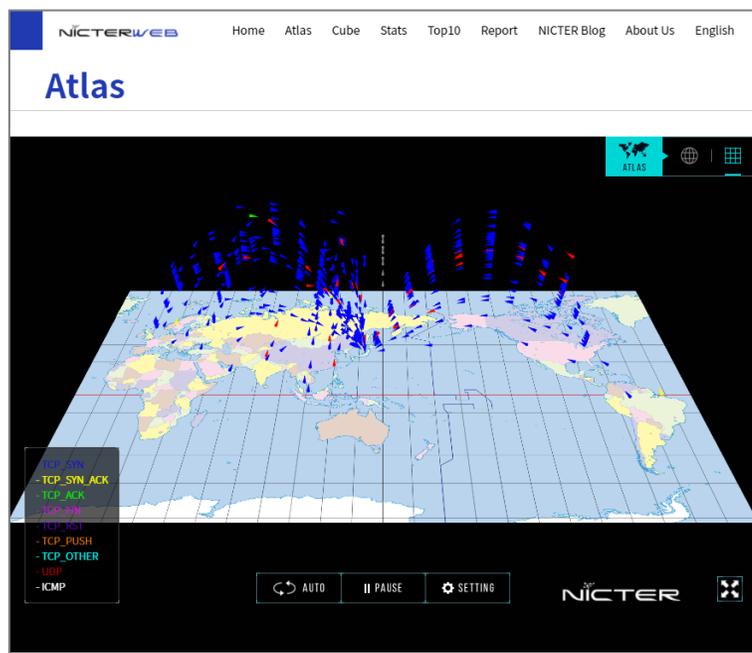
Copyright © MWS. 2020 12

[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

観測結果や分析結果は一般公開もしています

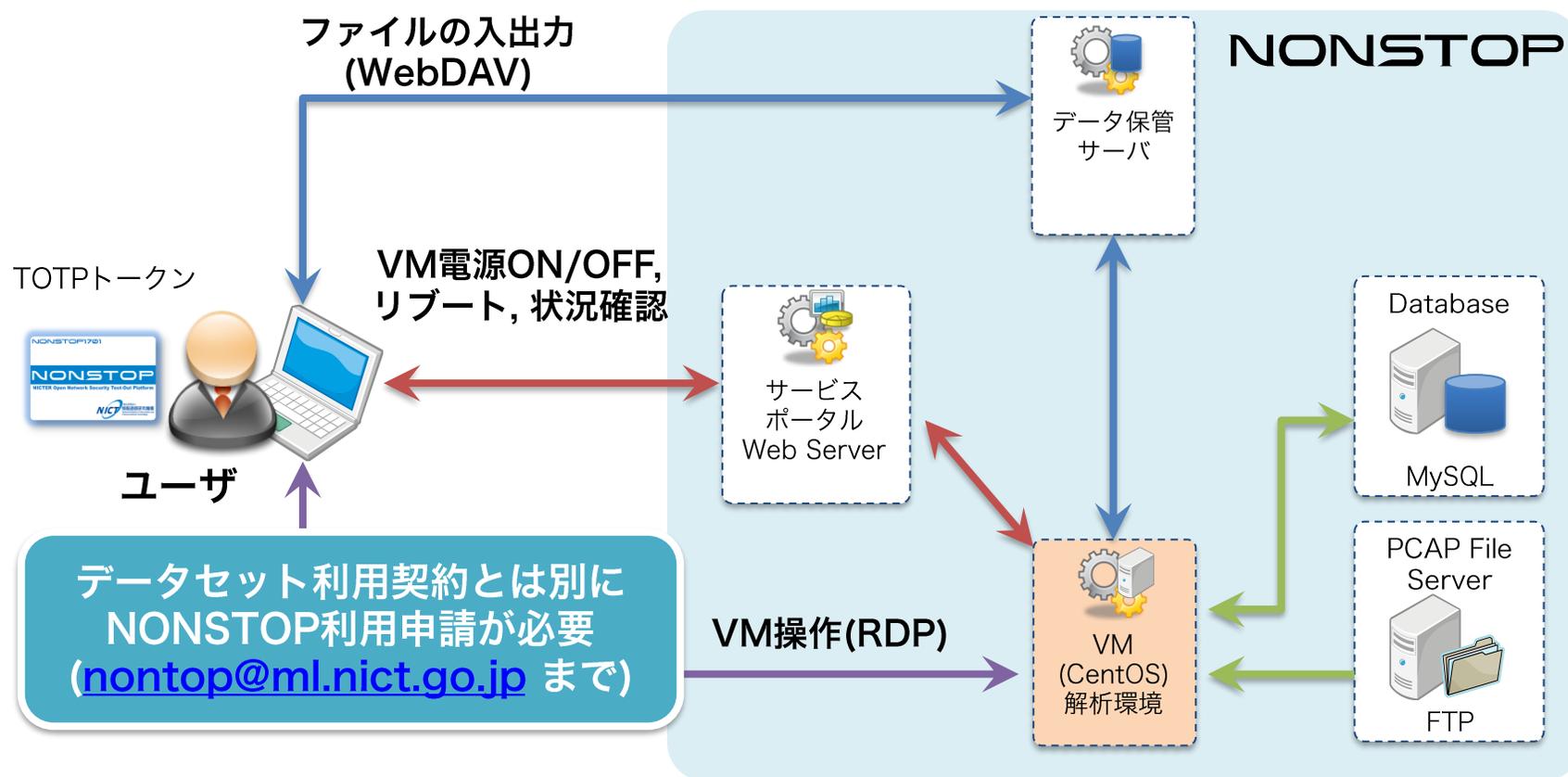
- NICTERWEB (<http://www.nicter.jp/>)
- NICTER Blog (<http://blog.nicter.jp>)
- NICTER 観測レポート 2016~2021



The NICTER Blog interface shows a header with the NICTER Blog logo and navigation links. The main content area features two articles. The first article is titled "サイバー脅威情報集約システム EXIST" and is dated 2019-03-15. The second article is titled "継続する 5555/TCP ポート宛攻撃通信と ADB が有効化された脆弱な Android エミュレータについて" and is dated 2018-10-22. The third article is titled "80/TCP 宛通信の増加" and is dated 2018-06-21.

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