
NICTER Dataset 2020

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 研究マネージャー

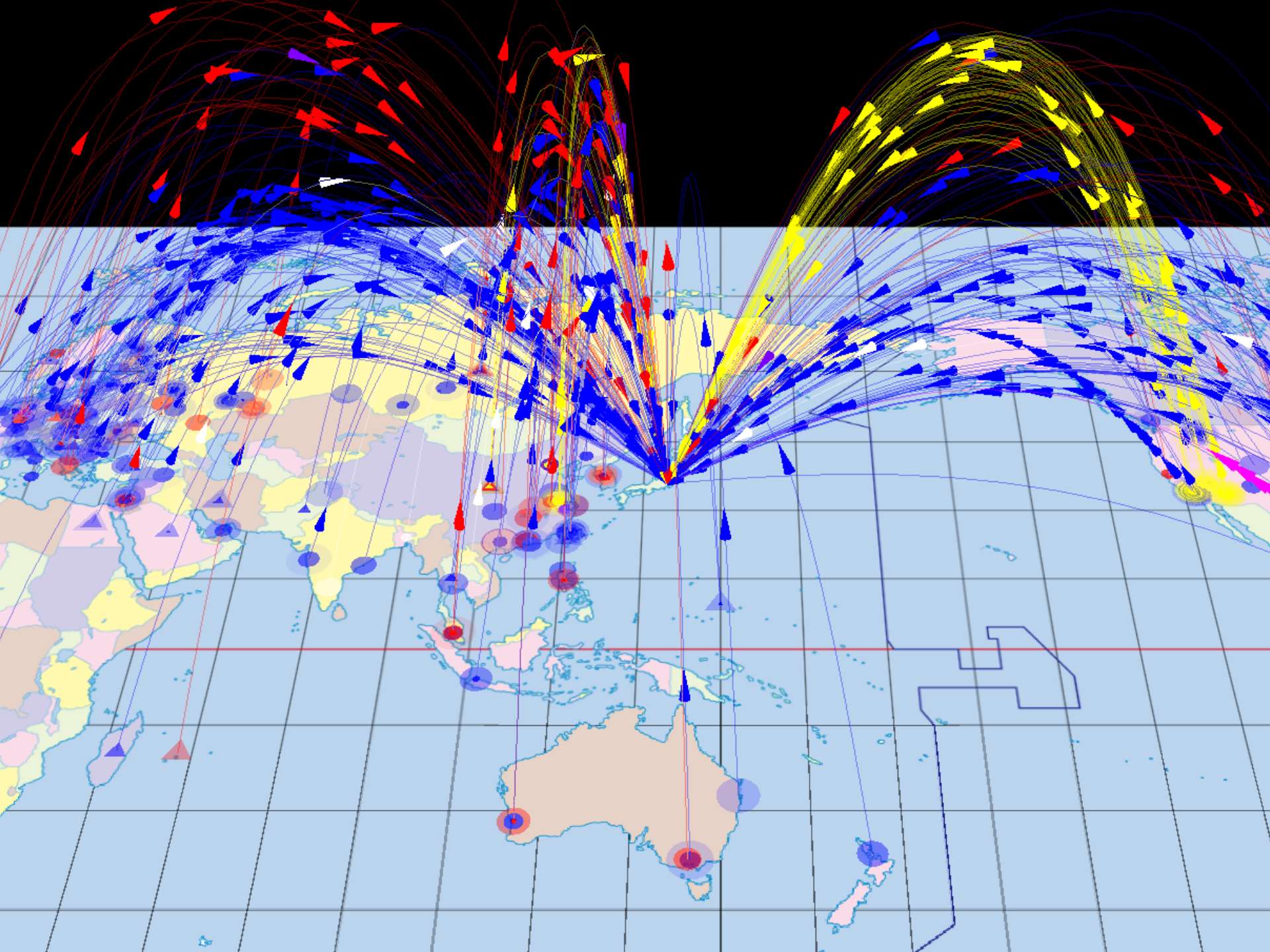
NICTER Dataset 2020

● 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9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5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**

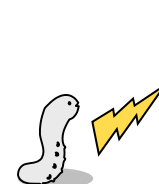
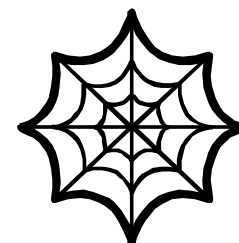
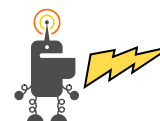
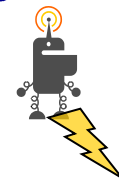
- ✓ 正常な通信は“基本的に”届かない

- **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.

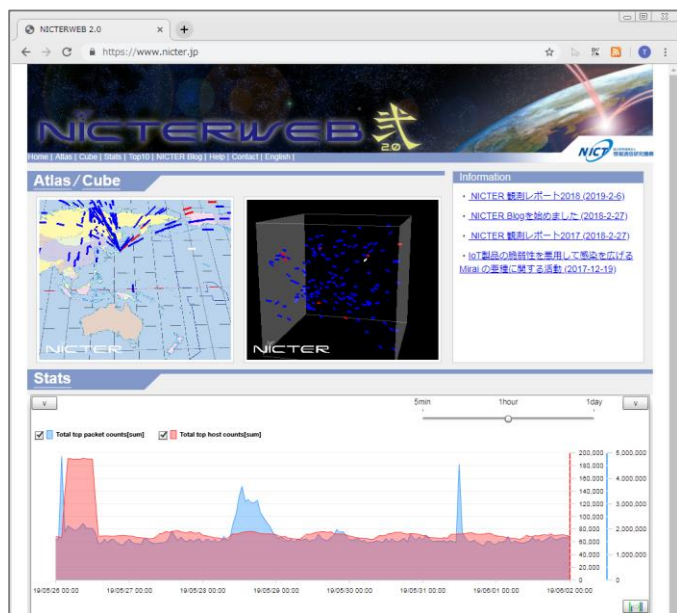
- **ダークネットの観測によって
パンデミックの兆候が分かる**

- ✓ パンデミック：マルウェアの大量感染



観測結果の一般公開

- **NICTERWEB** (<http://www.nicter.jp/>)
- **NICTER Blog** (<http://blog.nicter.jp>)
- **NICTER 観測レポート** (<http://www.nict.go.jp/cyber/report.html>)



よくある誤解（その1）

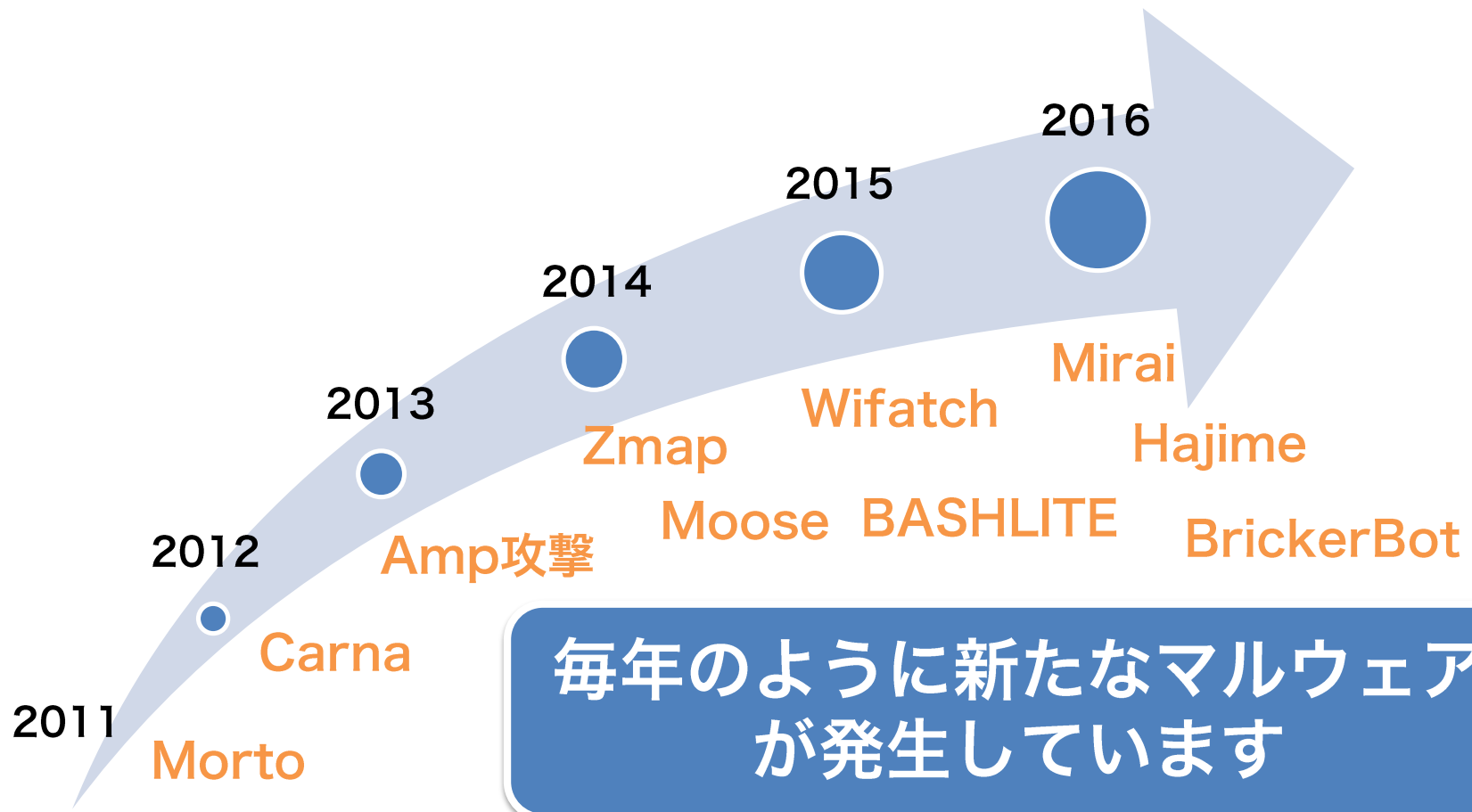
- ワームとか古いし今時スキャンとか飛んでこないでしょ

10年間以上基本的に増加し続けています



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



毎年のように新たなマルウェア
が発生しています

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.

An Internet-Wide View of Internet-Wide Scanning

SIGCOMM'14

Michael Bailey, J. Alex Halderman

Estimating Internet Address Space Usage through Measurements

NDSS'17

Alberto Dainotti, Karyn Benson, Alistair King, kc claffy, Michael Kallitsis, Merit Network, Inc., Ann Arbor, Michigan, USA, Eduard Glatz, Xenofontas Dimitropoulos, ETH Zurich

Internet-scale Probing of CPS: Inference, Characterization and Orchestration Analysis

Claude Fachkha^{1,2}, Elias Bou-Harb³, Anastasis K

¹New York University (NYU)

²University of

³Florida Atlantic

⁴Georgia Institute of Technology

Abstract—Although the security of Cyber-Physical Systems (CPS) has been recently receiving significant attention from the research community, undoubtedly, there still exists a substantial lack of a comprehensive and a holistic understanding of attackers' malicious strategies, aims and intentions. To this end, this 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 characterizing and re

USENIX WOOT'15

IoT POT: Analysing the Rise of IoT Compromises

Yip...¹, Katsunari Yoshioka¹, Tsutomu Matsumoto¹, Kasama², Christian Rossow^{1,3}
¹Graduate School of Information Sciences/Institute of Advanced Sciences

NDSS'14

Amplification Hell: Revisiting Network Protocols for DDoS Abuse

IMC'15

Christian Rossow
Amsterdam, The Netherlands

Leveraging Internet Background Radiation for Opportunistic Network Analysis

Abstract—In distributed attacks, adversaries sequentially resolve recursive DNS

NDSS'19

Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai

Orçun Çetin**, Carlos Gafán*, Lisette Altena*, Takahiro Kasama***, Daisuke Inoue***, Kazuki Tamiya**, Ying Tie**, Katsunari Yoshioka** and Michel van Eeten*

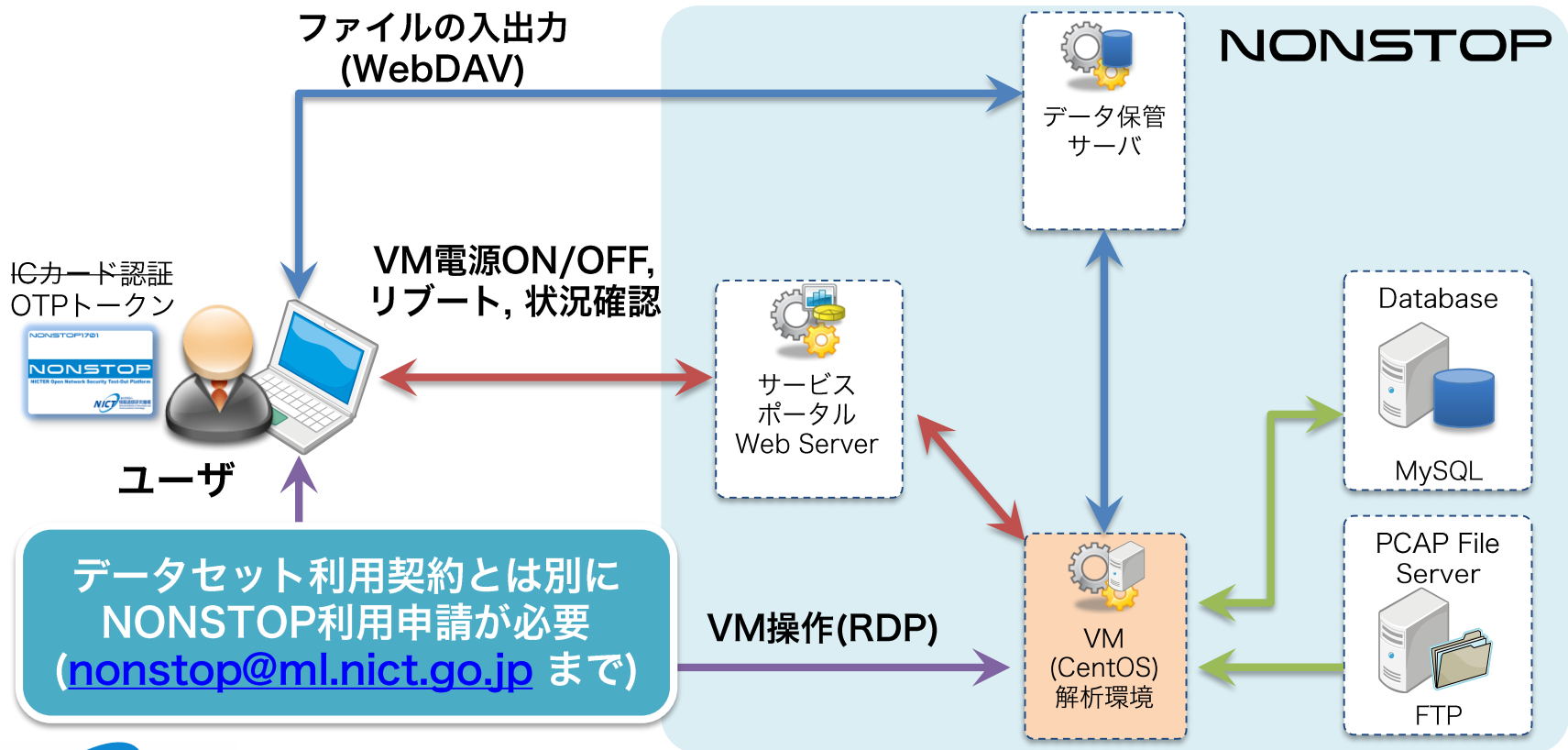
Alberto Dainotti¹, kc claffy¹, Alex C. Snoeren², Michael Kallitsis⁴, Engineering, UC San Diego, CAIDA, UC San Diego, Merit Network, Inc., @caida.org, snoeren@cs.ucsd.edu, mgkallit@umich.edu

unused regions of the address space, known as Internet Background Radiation (IBR), to address this challenge. Monitoring unused portions of the IPv4 address space reveals that IBR is of considerable volume, incessant, and originates from a variety of services [41,48]. This unsolicited traffic is caused by scanning (e.g., searching for hosts running a vulnerable service), misconfigurations (e.g., a typo in the IP address for a mail server), backscatter (responses to packets with forged source IP addresses, including spoofed DoS attack), bugs, etc. Historically, researchers

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



@2020年6月8日 MWS2020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（要望があれば）
- 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