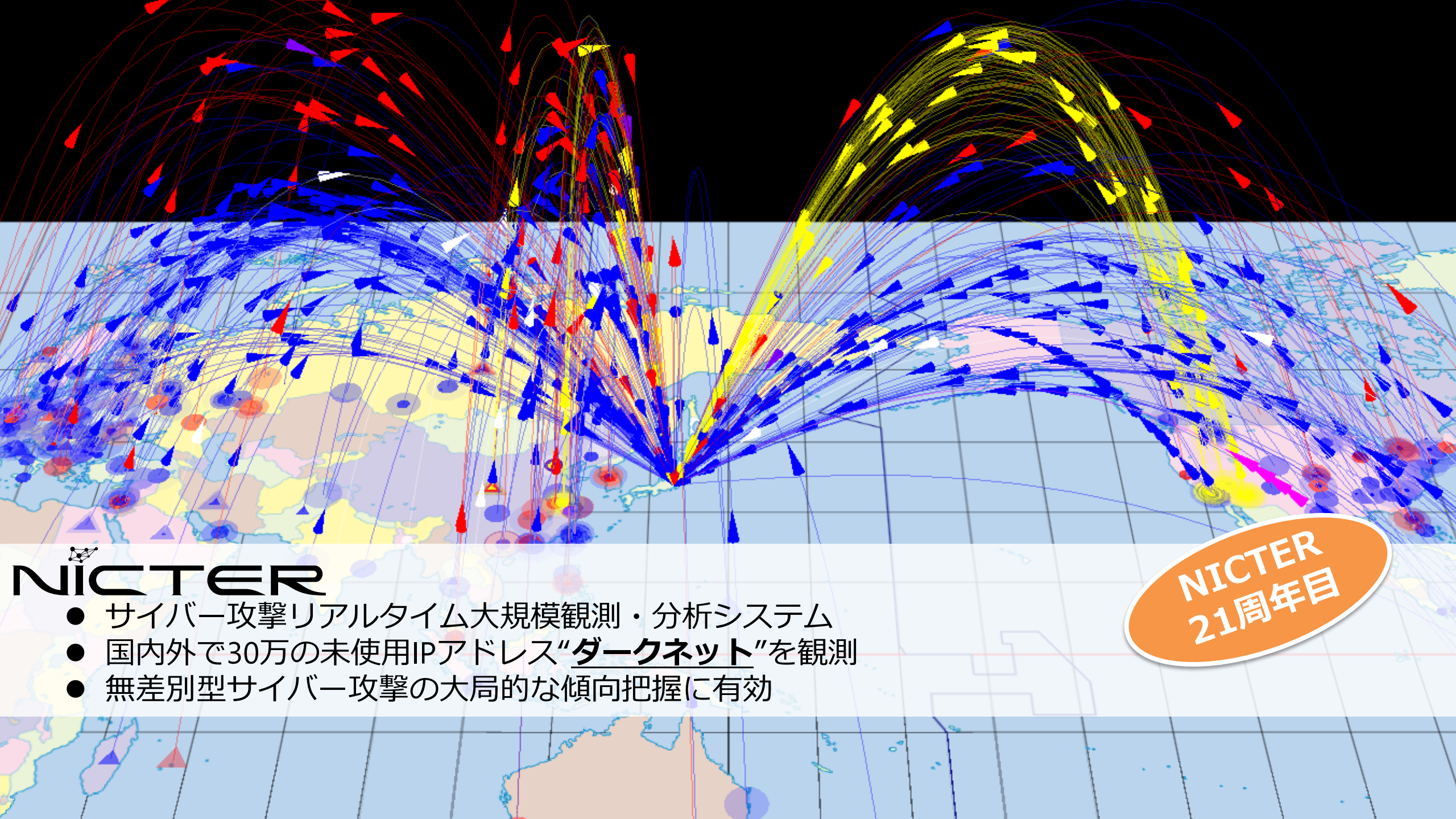
NICTER Dataset 2026

@MWS2026 プレミーティング（2026/7/3）

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



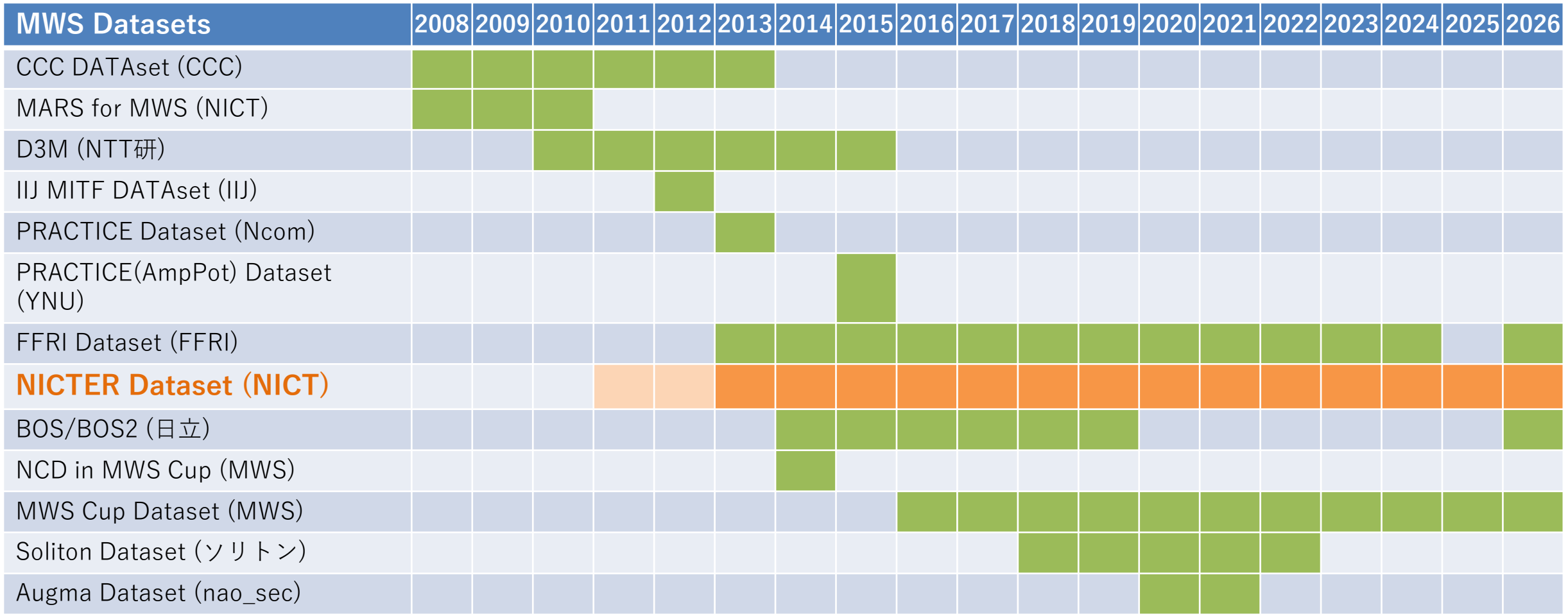
NICTER

- 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

NICTER
21周年目

MWS Datasets 変遷

- NICTER Dataset は2013年から継続提供されている唯一のデータセット

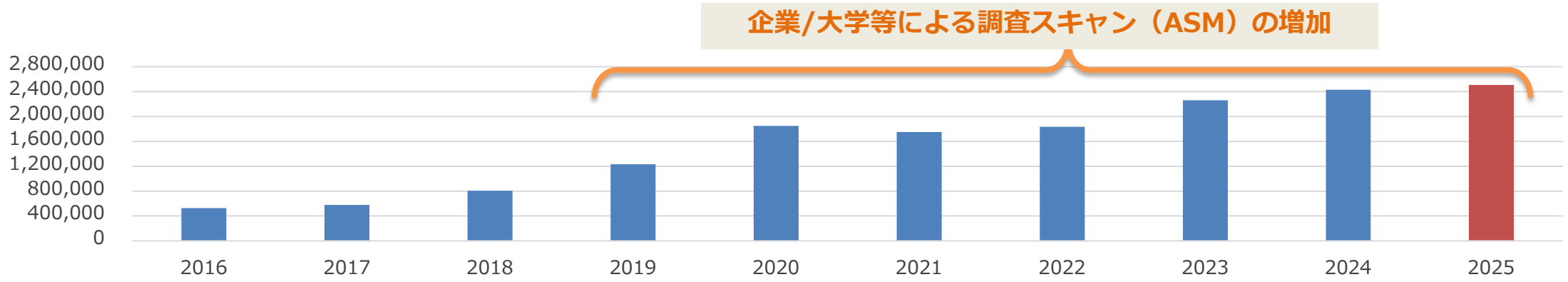


- **未使用のグローバルIPv4アドレス宛てに届くトラフィックデータ**
  - ✓/20（約4,000アドレス）の未使用アドレス（ダークネット）を観測
  - ✓宛先IPアドレスの第1・第2オクテットを適当な値に置換
  - ✓Pcapファイル（一ヶ月分）で30～40GB程度

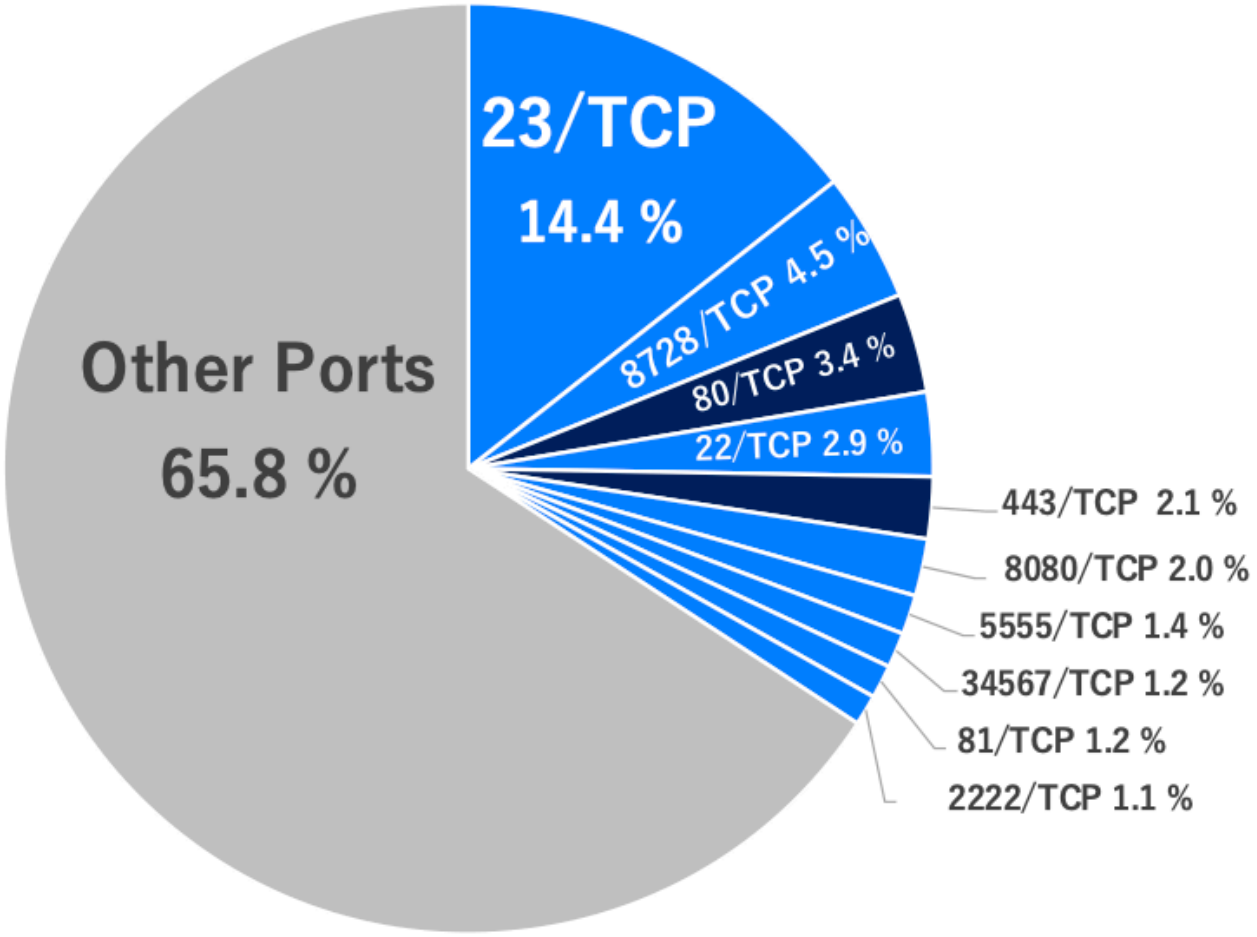
- **ネットワーク経由での様々な悪性通信が含まれるデータセット**
  - ✓マルウェア感染危機によるスキャン活動
  - ✓DDoS攻撃の跳ね返り
  - ✓リフレクタの探索活動
  - ✓研究組織やセキュリティ企業による調査スキャン

NICTERダークネット観測統計（過去10年）

年	年間総観測パケット数	ダークネットIPアドレス数	1 IPアドレス当たりの年間総観測パケット数
2016	約1,440億	274,872	527,888
2017	約1,559億	253,086	578,750
2018	約2,169億	273,292	806,877
2019	約3,756億	309,769	1,231,331
2020	約5,705億	307,985	1,849,817
2021	約5,180億	289,946	1,747,685
2022	約5,226億	288,042	1,833,012
2023	約6,197億	289,686	2,260,132
2024	約6,862億	284,445	2,427,977
2025	**約7,010億**	**284.305**	**2,504,679**



スキャンパケットの宛先ポート割合（2025年）



Dest. Port	Target Service
23/TCP	Telnet (Router, Web Camera)
8728/TCP	MikroTik RouterOS API
80/TCP	HTTP (Web Server)
22/TCP	SSH (Server, Router)
443/TCP	HTTPS (Web Server)
8080/TCP	HTTP (Web Console)
5555/TCP	ADB (Android)
34567/TCP	Xiongmai DVR API
81/TCP	HTTP (Web Console)
2222/TCP	Telnet (Router, Web Camera)

Distribution of Packets by Destination Port (Excluding Internet Scanners)

Source: NICTER Report 2025
https://csl.nict.go.jp/report/NICTER_report_2025.pdf

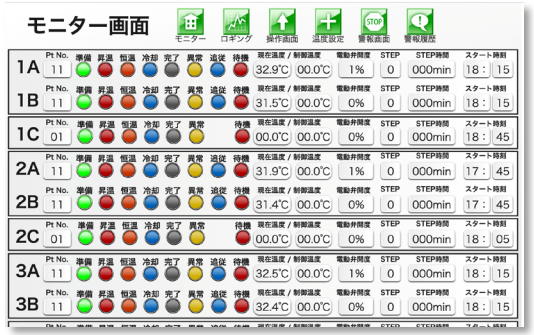
国内のマルウェア感染機器

- 2016年：**IoTマルウェア Mirai** 登場

- 国内の特徴的な感染機器
  - ✓ 2017～18年：ホームルータ製品
  - ✓ 2019年　　：Android OS搭載製品
  - ✓ 2020年　　：中国製 DVR 製品
  - ✓ 2021年～　：韓国製 **DVR 製品**
  - ✓ 2023年～　：モバイル回線で繋がる製品
  - ✓ 2025年～　：家庭用Wi-Fiルータ（レジプロ化）

- 感染後のマルウェア動作
  - ✓ 感染拡大のためのネットワークスキャン
  - ✓ C2指令によるDDoS攻撃、etc.

国交省の河川監視カメラの感染
(2023年)



産業用LTEルータの感染
(2023年)

工事現場サイネージ機器の感染
(2019年)

DVR(韓国製OEM) の感染
(2021年)

調査スキャン組織の特定と追跡

- 感染機器や攻撃傾向の分析においてセキュリティ企業や大学等によるスキャンはノイズとなるため、調査スキャン実施組織の特定と追跡（Ethics対応確認）を実施

IEEE Access

Received 6 January 2025, accepted 10 March 2025, date of publication 17 March 2025, date of current version 24 March 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3551691

RESEARCH ARTICLE

Please Stop Knocking on My Door: An Empirical Study on Opt-Out of Internet-Wide Scanning

TAKAHIRO KASAMA, YUKIKO ENDO, MASAKI KUBO, AND DAISUKE INOUE

National Institute of Information and Communications Technology, Koganei 184-8795, Japan

Corresponding author: Takahiro Kasama (kasama@nict.go.jp)

ABSTRACT Internet-wide scanning is prevalent due to the availability and widespread adoption of high-speed scanning tools, e.g., ZMap and Masscan, which can be used to perform Internet census tasks. However, benign scanning traffic can create undesirable noise for network administrators or researchers monitoring network traffic for security-related events. To mitigate the negative effects, previous studies have proposed best practices to guide ethical and well-regulated Internet-wide scans. In this paper, we are the first to shed light on the practicality of these best practices, with a primary focus on opt-out practices. By analyzing large-scale darknet traffic, we identify 46 scan organizations, including some that have not been reported in previous studies. We found that nearly 70% of the scanners we considered to be for survey purposes did not reveal their identity. In addition, we demonstrated that among scanners with identifiable identities, approximately 50% did not implement effective opt-out measures, which suggests that the effectiveness of opt-out practices is limited. Furthermore, only seven scanners confirmed that an opt-out request was sent from a legitimate administrator, indicating a challenge in terms of verifying the authenticity of opt-out requests. Based on these findings and reactions from scanning organizations, we revisit best practices for scanning organizations and recipients to facilitate effective and sustainable Internet-wide scanning practices.

INDEX TERMS Internet-wide scan, darknet monitoring, ethics.

https://ieeexplore.ieee.org/document/10928993

Peak Defense: Building Adaptive Systems for Modern Threats

THE CONFERENCE | REGISTRATION | PROGRAM | SPONSORSHIP | ATTENDEE COMMS

June 17, 2026 14:20-14:55

Attack or Noise?: Tracking and Evaluating the Impact of Internet-Wide Survey Scanners

TLP:CLEAR

Yukiko Endo (NICT, JP), Masato Jingu (NICT, JP), Masaki Kubo (NICT, JP)

Yukiko Endo

***Yukiko Endo** is a Senior Technical Researcher at the Cyber Threat Analysis Office, National Institute of Information and Communications Technology (NICT) in Japan, where she actively works on darknet monitoring, internet-wide scanning analysis, and threat intelligence research. Before joining NICT, she worked in both Japan and Germany on research and product development in the field of Identity and Access Management. Her broader interests include IoT security, Internet-wide measurement, and the collection and analysis of threat intelligence data.*

Masato Jingu

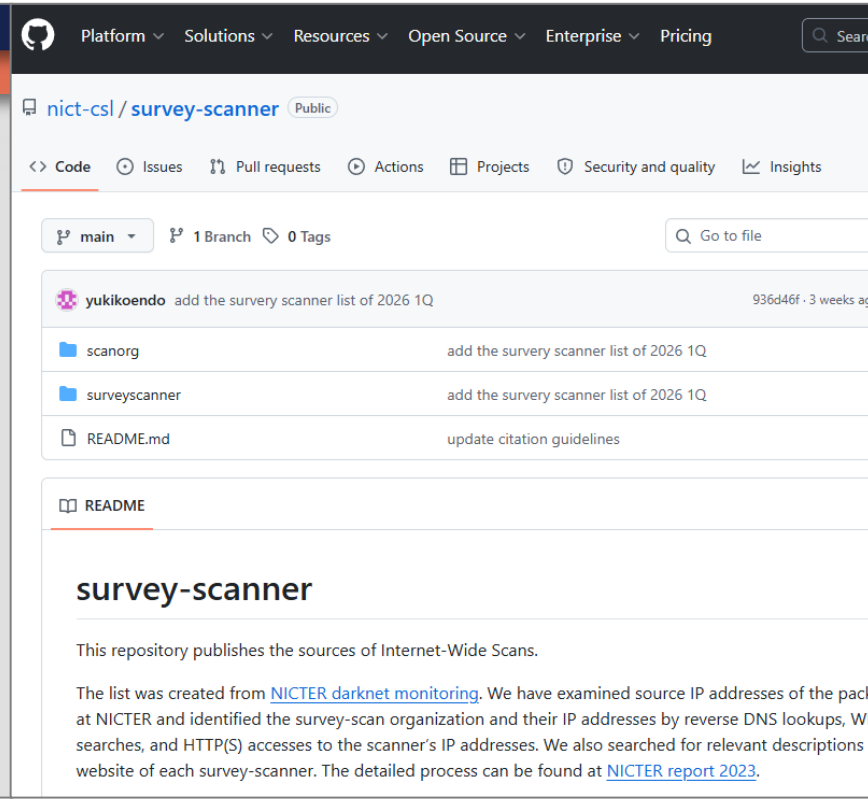
***Masato Jingu** is an analyst at the Cyber Threat Analysis Office of the National Institute of Information and Communications Technology (NICT). He also serves as a member of NICT-CSIRT, where he is primarily responsible for the analysis of a livenet. Prior to joining NICT, he held positions in the private sector, where he was engaged in cybersecurity incident response as well as research and development activities.*

Masaki Kubo

***Masaki Kubo** serves as Director of the Cyber Threat Analysis Office at NICT. His responsibilities extend to both the internal security operation and a darknet monitoring research project known as 'NICTER'. Prior to joining NICT, He was a manager of JPCERT coordination center, focusing on the analysis and coordination of vulnerabilities and advocating for a secure coding initiative.*

Security teams routinely waste time investigating benign scans from services such as Censys, Shodan, ZoomEye, and other survey-scanners. However, there has been no comprehensive, openly available source that identifies which organizations are scanning

https://www.first.org/conference/2026/program



Platform | Solutions | Resources | Open Source | Enterprise | Pricing

nict-csl / survey-scanner Public

Code | Issues | Pull requests | Actions | Projects | Security and quality | Insights

main | 1 Branch | 0 Tags | Go to file

yukikoendo add the survey scanner list of 2026 1Q 936d46f · 3 weeks ag

scanorg	add the survey scanner list of 2026 1Q
surveyscanner	add the survey scanner list of 2026 1Q
README.md	update citation guidelines

README

survey-scanner

This repository publishes the sources of Internet-Wide Scans.

The list was created from NICTER darknet monitoring. We have examined source IP addresses of the pacl at NICTER and identified the survey-scan organization and their IP addresses by reverse DNS lookups, W searches, and HTTP(S) accesses to the scanner's IP addresses. We also searched for relevant descriptions website of each survey-scanner. The detailed process can be found at NICTER report 2023.

https://github.com/nict-csl/survey-scanner

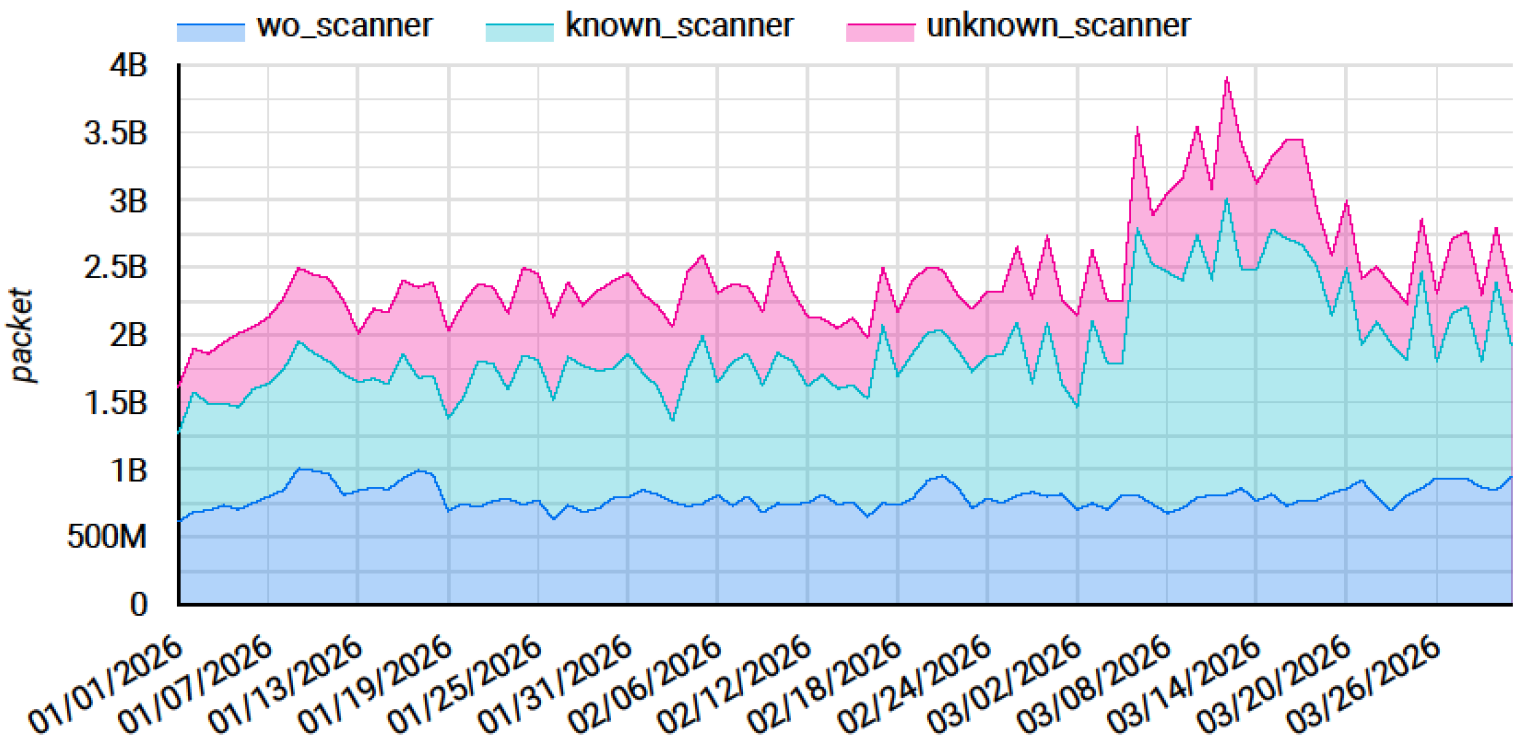
調査スキャンの割合（推定含む）

Jan. 1–Mar. 31
observation period

221.5B
observed packets

83
identified organizations

67.7%
scanner-attributed traffic



Scan by Unknown Scanner

Scan by Identified Scanner

Scan by Bot

Survey scanning accounted for more than two thirds of observed darknet traffic during 2026 Q1.

調査スキャンの実施組織（2026 Q1で83組織特定）

scanner name	type
Modat	Threat Intelligence service
Palo Alto Networks (Cortex-Xpanse)	Threat Intelligence service
Censys	Threat Intelligence service
Shadowserver	Threat Intelligence service
Stretchoid	-
NOKIA (Deepfield)	DDoS Detection service
driftnet (internet-measurement.com)	Threat Intelligence service
Shodan	Threat Intelligence service
Onyphe	Threat Intelligence service
VisionHeight	Threat Intelligence service
Academy for Internet Research	-
CriminalIP	Threat Intelligence service
The Recyber Project	-
bitsight	Security evaluation service
NETSCOUT (Arbor)	Threat Intelligence service
ICT-ISAC	Survey and warning
Binaryedge	Threat Intelligence service
F6	Threat Intelligence service
ipip	Threat Intelligence service
Rapid7 (Project Sonar)	Threat Intelligence service
Qrator (Qrator.Radar)	Threat Intelligence service
A Recorded Future (Securitytrails)	Threat Intelligence service
Ruhr University Bochum	Research
GROUP-IB	Attack Surface Management service
bufferover.run	TLS certificate information service
Limes Security (Alpha Strike Labs)	Threat Intelligence service
SBA Research	-
Edgewatch	Threat Intelligence service
UpGuard (CyberResilience)	Research
BarkScan	Threat Intelligence service
Yokohama National University	Research
FR Cert	Survey and warning
Intrinsec	Threat Intelligence service
Adscore	Traffic Detection service
Georgia Institute of Technology	Research
Max Planck Institute	Research
DomainTools	Threat Intelligence service
Infrawatch	Threat Intelligence service
FH Muenster	Research
Cybergreen	Threat Intelligence service
The Technical University of Munich (TUM)	Research
Leakix	Threat Intelligence service
University of Cambridge	Research
ipinfo	IP address information service
CYPEX	Threat Intelligence service
University of California, San Diego	Research
Esslingen University of Applied Sciences (Project Patchwatch)	Research
Technical University of Denmark (Digital Ghost Ships)	Research
University of Twente (Internet Transparency research project)	Research
internet.survey	-
CyberCube	Cyber risk quantification service
ANT lab	Research
A10	DDoS Protection service
Cyber OK	Attack Surface Management service
Politecnico di Milano	Research
TU Dresden	Research
Stanford University	Research
University of Maryland	Research
GDNplus	Internet Market Research
ProbeTheNet	Research
ENTELIJAN	AI Threat Intelligence service
ESET	End point security product
pocnroll	Research
Root Evidence	Attack Surface Management service
internettl	-
Cymru	Threat Intelligence service
Halo Security	Attack Surface Management service
CAIDA	Research
Open Port Stats	-
DE-CIX	Internet Service provider/Research
Microsoft (Bing Crawler)	Web crawl bot
research-scanner.com	-
Research knoq	-
OnlyScans	Threat hunting
BigDataCloud.com	IP address geolocation service
Apple (Applebot)	Web crawl bot
Zern	Threat Intelligence service
University of California, Berkeley	Research
The Internet Archive	Web crawl bot
Facebook (FacebookBot)	Web crawl bot
RWTH Aachen University	Research
semrush	Web crawl bot
dataforseo	Web crawl bot

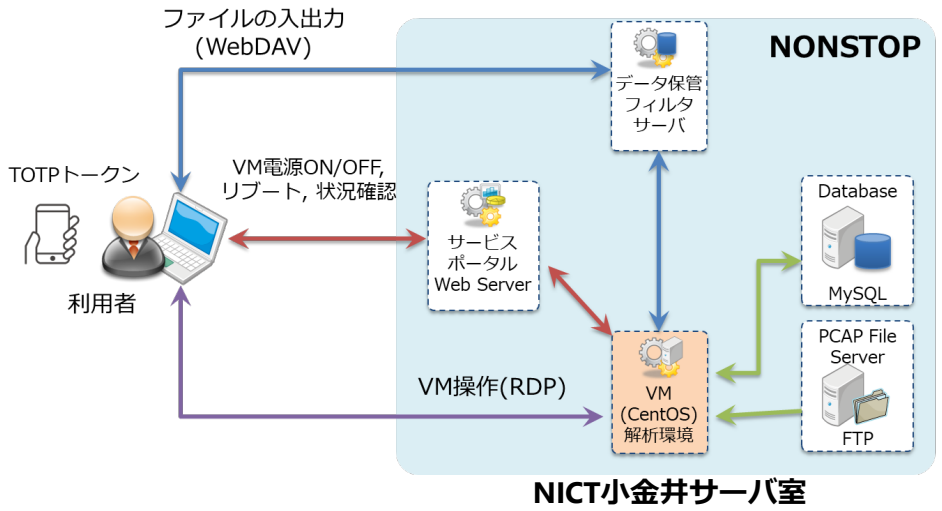
Security Intelligence and Measurement Services
Research Organizations
Gray Scanners / Unknown Objectives
web crawlers

Red = 9 newly observed organization in 2026 Q1.
Sorted by packet volume.

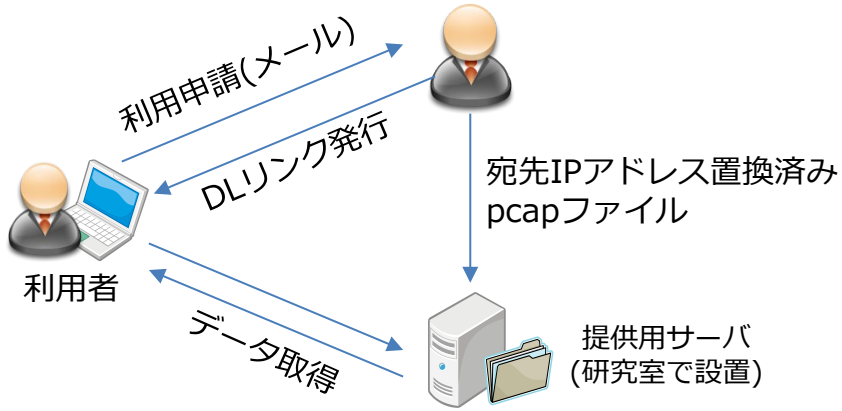
Note: Subsequent analyses exclude 6 web crawlers and focus on 77 survey-scanner organizations.

【重要】NICTER Dataset 提供方法の変更

- NONSTOPという独自VPS環境上でのデータ提供を行っていましたが、今年度は**ファイル（Pcap形式）をDL可能な提供方法に変更**します。
  - ✓提供データはPcapファイルのみ、期間は2026/1/1～2026/6/30（更新無し）
- DLリンクを個別に発行しますので**利用希望者はメールで申請が必要**
  - ✓ nicter-dataset@ml.nict.go.jp まで代表者からご連絡ください。



2025年まで：NONSTOP上でのみデータにアクセス可能



2026年：利用希望者にDLリンクを発行しファイル提供

NICTER Dataset 2026 の ご活用をぜひ検討ください

✉ *nicter-dataset@ml.nict.go.jp*

CSL HP
https://csl.nict.go.jp/en

NICTERWEB
https://www.nicter.jp/en/

国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology