NICTER Dataset 2025

笠間 貴弘

国立研究開発法人情報通信研究機構

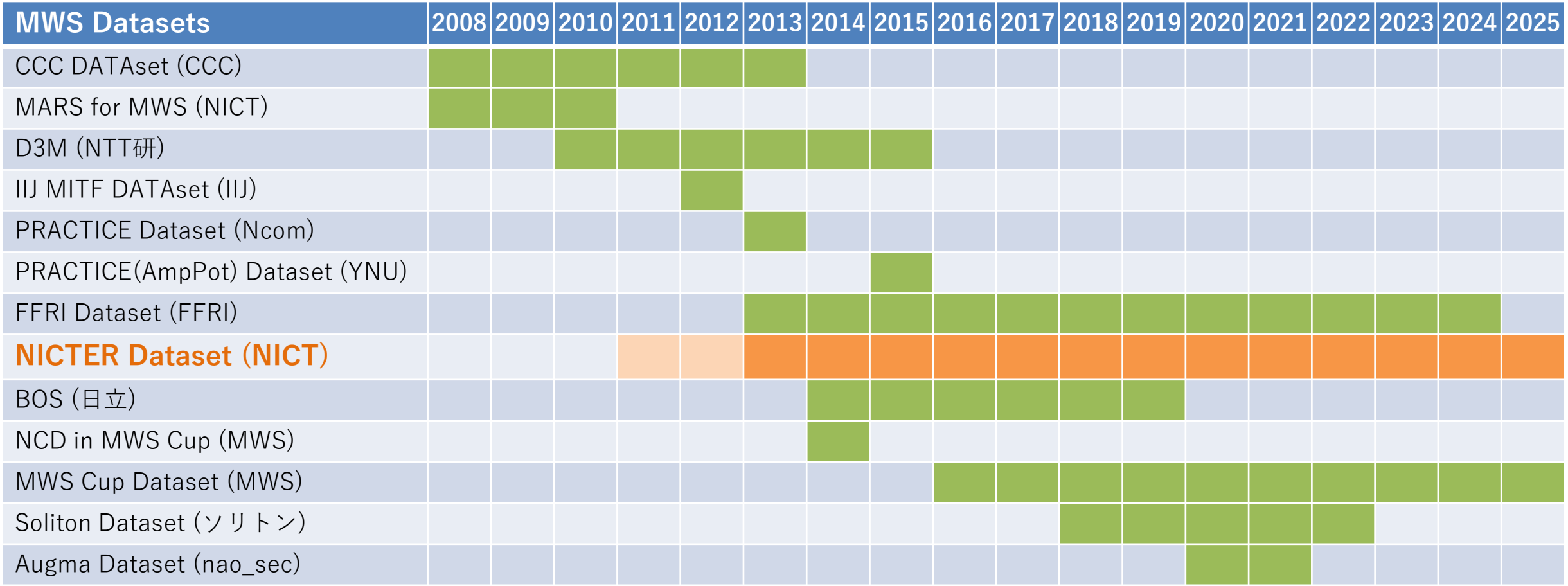
サイバーセキュリティ研究所

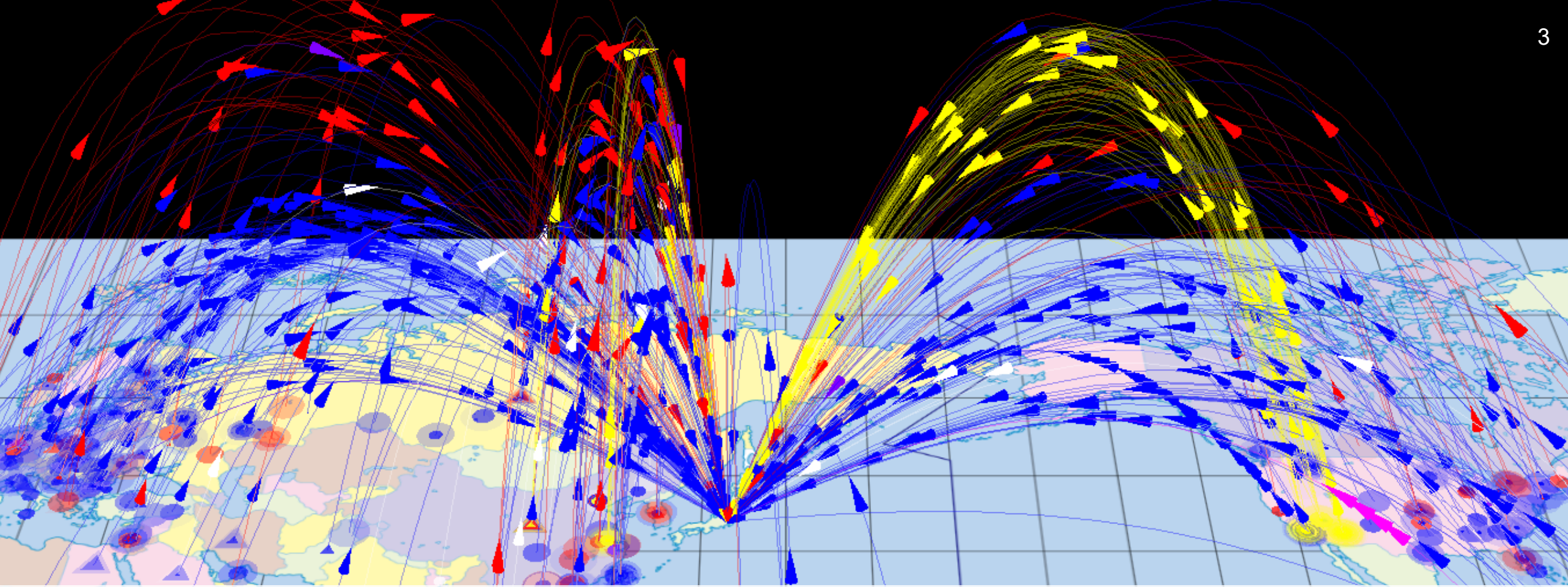
サイバーセキュリティ研究室　室長

NICT National Institute of Information and Communications Technology

CYBERSECURITY Laboratory

祝！最長データセット(新規データ有)達成!!





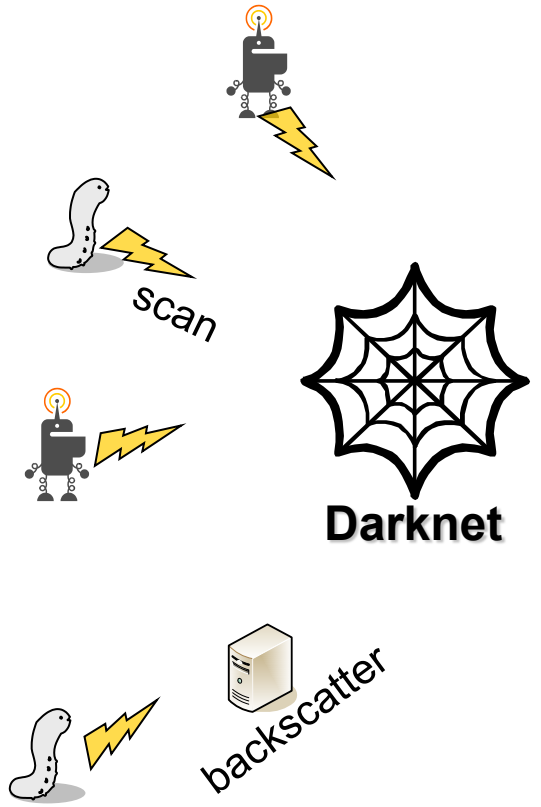
NICTER

- 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 Dataset 2025

- **未使用のIPアドレス宛に届いた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
  - ✓観測は期間は2011年1月1日から現在(約6TB)
  - ✓独自システムのVM内からアクセス可能(pcap+DB)

- **様々な悪性通信が含まれるデータセット**
  - ✓マルウェア感染機器によるスキャン
  - ✓DDoS攻撃の跳ね返り
  - ✓最近は研究組織や企業による調査スキャンも多数
  - ✓etc.



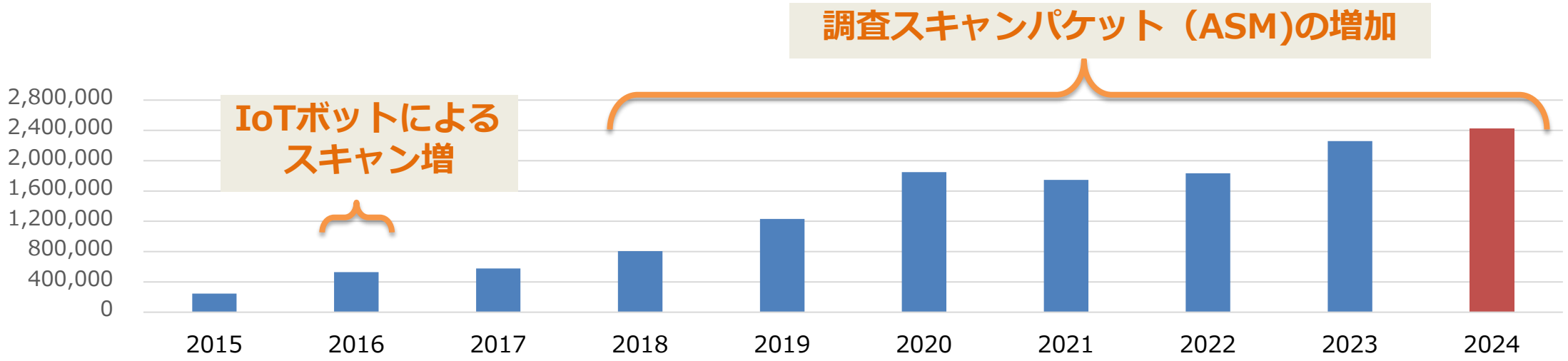
NICTERダークネット観測統計（過去10年）

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
2015	約632億	270,973	245,540
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**

1アドレスあたり

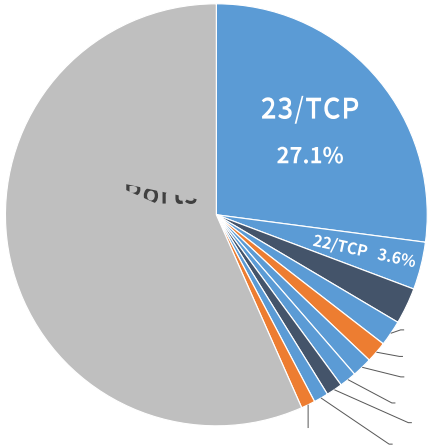
13秒に1回

攻撃関連通信受信

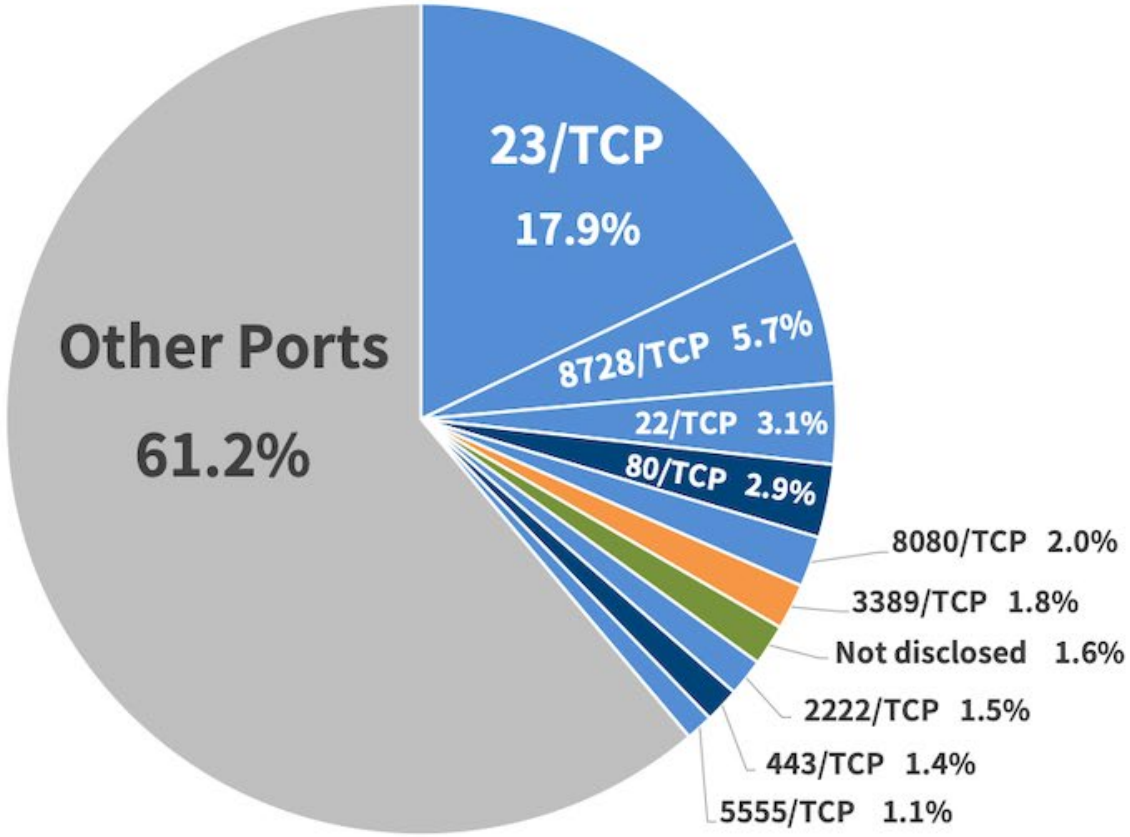


感染機器の分布（2024年）

- NICTER 観測レポート 2024：宛先ポート番号別パケット数分布 -



2023



宛先ポート	攻撃対象
23/TCP	Telnet （ルータ，Webカメラ等）
8728/TCP	MikroTik RouterOS API
22/TCP	SSH（サーバ，ルータ等）
80/TCP	HTTP（Webサーバ）
8080/TCP	HTTP（Web管理画面）
3389/TCP	Remote Desktop
Not disclosed	-
2222/TCP	SSH（IoT機器）
443/TCP	HTTPS （Webサーバ）
5555/TCP	ADB （Android）

宛先ポート別パケット数の割合
（調査スキャンを除く）

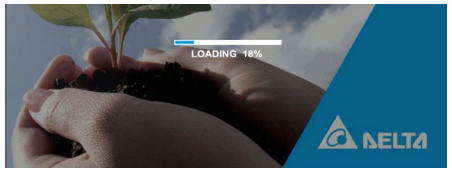
出典：NICTER観測レポート2024
https://csl.nict.go.jp/report/NICTER_report_2024.pdf

IoTボットの感染活動

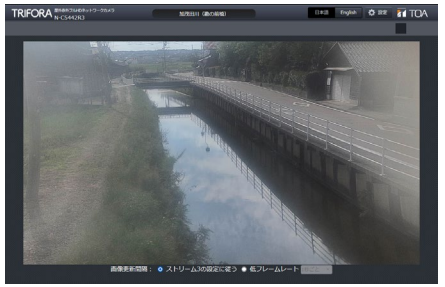
- **2016年：Miraiボット**
  - ✓ IoT機器に感染し大規模なDDoS攻撃を実行

- **NICTで観測した特徴的な感染機器**
  - ✓ 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年末～：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**

ソーラーパネル



河川の監視カメラ



PLC（制御システム）

ボットに感染した産業用LTEルータに
接続されていた機器の管理画面（2024年）

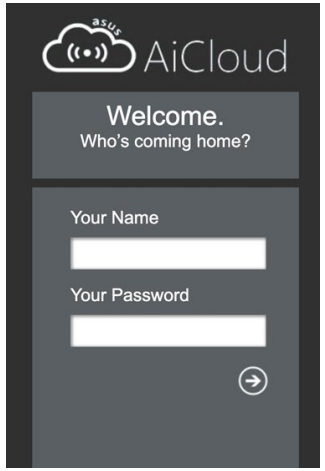
- **感染後に観測された動作**
  - ✓ 感染拡大のためのネットワークスキャン、指令によるDDoS攻撃等

ASUS製Wi-Fiルータ(AiCloud機能)の脆弱性悪用

- **AiCloud: ASUSルータに搭載されているクラウドストレージ機能**
  - ✓ LAN or USBに接続されたストレージをパーソナルクラウドとして利用できるサービス
- **証明書インストール機能に認証無しでコマンド実行の脆弱性が存在(CVE-2025-2492)**
  - ✓ NICTER(+実機ハニーポット)により**世界規模で3000台規模の被害**を観測
  - ✓ ASUSより修正ファームウェアとアドバイザリが公開済みのため、速やかな更新を推奨

実機ハニーポットによって観測した悪用パターン

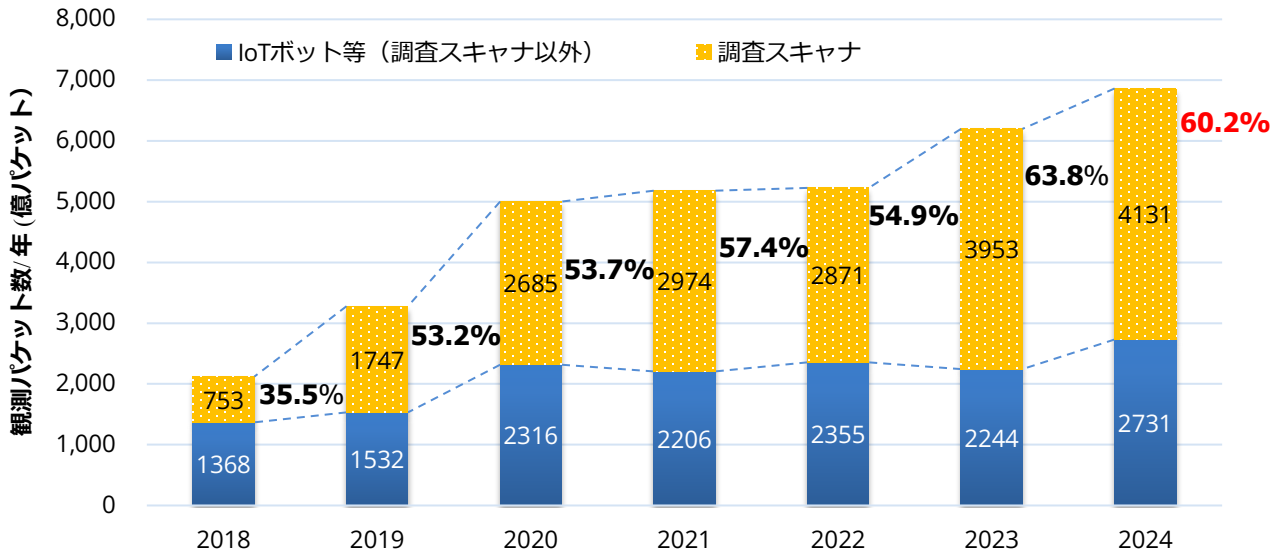
	脆弱なAiCloud バージョン	実際に観測した攻撃活動	悪用された独自メソッド
パターン1	2.0.2.28以下	✓ バックドア（Telnetなど）の有効化 ✓ ファイアーウォールの操作 ✓ Hostファイルの操作 ✓ /etc/passwd の操作 ✓ マルウェアへの感染	•APPLYAPP
パターン2	2.0.2.36以下	✓ マルウェアへの感染	•SETROOTCERTIFICATE •APPLYAPP
パターン3	2.0.2.12以下	✓ マルウェアへの感染	•SETROOTCERTIFICATE



Attack Surface Management (ASM) の台頭

● 2018年以降、IPv4全域をスキャンするパケットの観測数が増加

- ✓ **セキュリティリサーチの一般化，商業化**
  - OSSツール（Zmapやmasscan）による高速スキャン実施の技術的容易性の向上
  - Shodan(2009)，Censys(2015)の成功により同様のスキャンプラットフォームが台頭
- ✓ **大規模脆弱性の頻発，対応スピードの高速化**
  - Miraiボット(2016)，WannaCry(2017)
  - 脆弱性公表から悪用までの期間短縮
- ✓ **ASMの定着、市場カテゴリ化**
  - 複数のベンダがASMを提唱、商品化



素性特定が可能な調査スキャン実施組織リスト

● 2024年に特定した組織：79組織

1	Censys	アメリカ
2	Palo Alto Networks (Cortex-Xpanse)	アメリカ
3	Stretchoid	不明
4	The Recyber Project	不明
5	Shadowserver	アメリカ
6	CriminalIP	アメリカ
7	driftnet (internet-measurement.com)	アメリカ
8	Academy for Internet Research	不明
9	Inspici	アメリカ
10	Shodan	アメリカ
11	internettl	不明
12	Onyphe	フランス
13	bitsight	アメリカ
14	一般社団法人ICT-ISAC	日本
15	GROUP-IB	シンガポール
16	Binaryedge	アメリカ
17	NETSCOUT (Arbor)	アメリカ
18	bufferover.run	不明
19	Rapid7 (Project Sonar)	アメリカ
20	ScanOpticon	不明
21	Qrator (Qrator.Radar)	チェコ
22	ipip	中国
23	Limes Security (Alpha Strike Labs)	ドイツ
24	Open Port Stats	不明
25	Adscore	UAE
26	UpGuard (CyberResilience)	アメリカ
27	FR Cert	フランス
28	横浜国立大学	日本
29	Intrinsec	フランス
30	スタンフォード大学	アメリカ
31	Leakix	ベルギー
32	トゥヴェンテ大学 (Internet Transparency research project)	オランダ
33	Cybergreen	アメリカ
34	ミュンヘン工科大学 (TUM)	ドイツ
35	ミュンスター工科大学	ドイツ
36	ipinfo	アメリカ
37	ケンブリッジ大学	イギリス
38	カリフォルニア大学サンディエゴ校	アメリカ
39	netsecscan	不明
40	GDNplus	不明
41	マックスプランク研究所	ドイツ
42	internet.survey	不明
43	Crowd Strike (Reposify)	アメリカ
44	ミシガン大学	アメリカ
45	ミラノ工科大学	イタリア
46	Edgewatch	スペイン
47	The Internet Archive	アメリカ
48	ANT lab	アメリカ
49	エスリンゲン大学 (Project Patchwatch)	ドイツ
50	ルール大学ボーフム	ドイツ
51	ESET	スロバキア
52	コロラド大学	アメリカ
53	CAIDA	アメリカ
54	research-scanner.com	不明
55	Research knoq	不明
56	NOKIA (Deepfield)	フィンランド
57	SBA Research	オーストリア
58	ジョージア工科大学	アメリカ
59	Facebook (FacebookBot)	アメリカ
60	THESEUS	オランダ
61	semrush	アメリカ
62	dataforseo	エストニア
63	Apple (Applebot)	アメリカ
64	Common Crawl	アメリカ
65	Ahrefs (AhrefsBot)	シンガポール
66	Net Systems Research	不明
67	Sogou (Sogouspider)	中国
68	DE-CIX	ドイツ
69	SI6 Networks	アルゼンチン
70	ドレスデン工科大学	ドイツ
71	FOI Internet Scanning Project	スウェーデン
72	ByteDance (Bytespider)	中国
73	アーヘン工科大学	ドイツ
74	Winnti Scanner	不明
75	WebMeUp (BlexBot)	キプロス
76	Cyble (ODIN)	インド
77	フリーステート大学 (UFS)	南アフリカ
78	ブラウンシュヴァイク工科大学 (IAS Lab)	ドイツ
79	NICT（NOTICE）	日本

```
==========================================================================
_____   ________________
___  | / /_  ___/__  __ \  Passive.
__   |/ /_____ \__  / / /  Realtime.
_  /|  / ____/ /_  /_/ /   Unfiltered.
/_/ |_/  /____/ /_____/    From the Darknet.
==========================================================================
NICTER Stream Detector v1.0
(C) 2025 National Institute of Infomation and Communications Technology.
==========================================================================
```

No.	Last Seen[l] v	Src IPaddr[s]	ORG	CC	Scanner[a]	Count[c]	pps[p] v	Proto	Portset	JA4T tag	JA4T
1	2025/06/03 09:40:11	185.91.127.81	Tube-Hosting	DE	--	14106	305	S	S:20947		138_65535_2-1-3-1-1-4_1460_8:2304..
2	2025/06/03 09:40:11	113.249.159.56	China Telecom	CN	--	255	8	S	S:456,S:2217..	Nmap:236	132_1024_2_1460_0:14, 138_1024_2_1460_0:54..
3	2025/06/03 09:40:11	207.90.244.17	Cogent Communic	US	Shodan	540	15	S	S:51,S:85,S:131..		100_56307_2_1460_0:1, 12_20932_2_1240_0:1..
4	2025/06/03 09:40:11	199.45.154.190	Censys-arin-03	US	Censys	386	8	S,U	S:21,S:22,S:25..		115_42340_2-4-8-1-3_1460_10:5..
5	2025/06/03 09:40:11	71.136.67.9	Beijing Guanghu	CN	--	414	10	I	I:8		
6	2025/06/03 09:40:11	138.197.15.182	Digital Ocean	US	--	95	5	S	S:8888	Modified ZMap:90	102_65535_2_1460_0:16, 131_65535_2_1460_0:14..
7	2025/06/03 09:40:11	159.89.52.125	Digital Ocean	US	--	69	2	S	S:5903		116_65535_2-4-8-1-3_1460_7:1..
8	2025/06/03 09:40:11	124.44.72.125	NTT-ME Corporat	JP	--	8	0	S	S:23		138_54176_2_1414_0:3, 131_54176_2_1414_0:1..
9	2025/06/03 09:40:11	120.61.233.37	BSNL	IN	--	16	1	S	S:23		13_1765_0_00_00:3, 102_1765_0_00_00:1..
10	2025/06/03 09:40:11	167.94.145.30	Censys-arin-02	US	Censys	389	9	S	S:21,S:23,S:25..		102_42340_2-4-8-1-3_1460_10:81..
11	2025/06/03 09:40:11	83.222.191.130	SS-Net	BG	--	11804	257	S	S:13,S:80,S:81..	masscan:11804	13_1024_0_00_00:1283, 29_1024_0_00_00:781..
12	2025/06/03 09:40:11	115.231.78.10	China Telecom	CN	--	2484	55	S,U	S:11,S:21,S:22..		29_29200_2_1460_0:639, 100_29200_2_1460_0:556..
13	2025/06/03 09:40:11	190.73.86.239	Cantv	VE	--	6	0	S	S:23		12_29200_2-4-8-1-3_1240_5:1..
14	2025/06/03 09:40:11	15.235.227.163	OVHcloud	CA	--	6390	136	S	S:23		29_65535_2-1-3-1-1-4_1460_8:489..
15	2025/06/03 09:40:11	179.43.191.98	Private Layer	PA	--	3897	88	S	S:37777	Zmap:3897	101_65535_0_00_00:68, 138_65535_0_00_00:589..
16	2025/06/03 09:40:11	64.62.197.68	Hurricane Elect	US	Shadowserver	953	37	S,U	S:3000,U:523	Zmap:864	12_65535_0_00_00:81, 100_65535_0_00_00:47..
17	2025/06/03 09:40:11	13.89.125.29	Microsoft Azure	US	--	7923	154	S	S:443	Zmap:7923	13_65535_0_00_00:7310, 115_65535_0_00_00:613
18	2025/06/03 09:40:11	65.49.1.177	Hurricane Elect	US	--	515	31	S	S:8030	Zmap:515	29_65535_0_00_00:26, 108_65535_0_00_00:27..
19	2025/06/03 09:40:11	88.218.193.55	Detai Prosperou	DE	--	135	3	S	S:21,S:22,S:23..		138_64240_2_1460_0:28, 29_64240_2_1460_0:15..
20	2025/06/03 09:40:11	74.82.47.19	Hurricane Elect	US	Shadowserver	151	34	S	S:33060	Zmap:151	102_65535_0_00_00:31, 13_65535_0_00_00:21..
21	2025/06/03 09:40:11	134.122.68.196	Digital Ocean	US	--	25	0	S	S:80,S:443,S:8001..	Modified Nmap:25	102_1025_2_1460_0:7, 100_1025_2_1460_0:1..
22	2025/06/03 09:40:11	46.173.209.136	Garant-Park-Int	RU	--	8	0	S	S:80	masscan:8	29_1024_0_00_00:1, 12_1024_0_00_00:1..
23	2025/06/03 09:40:11	88.218.193.30	Detai Prosperou	DE	--	151	2	S	S:21,S:22,S:23..		138_64240_2_1460_0:19, 62_64240_2_1460_0:1..
24	2025/06/03 09:40:11	179.43.186.240	Private Layer	PA	--	378	9	S	S:1111,S:2222..	masscan:378	131_1024_0_00_00:48, 138_1024_0_00_00:60..
25	2025/06/03 09:40:11	152.32.207.229	Ucloud Informat	HK	--	11	1	S	S:81,S:554,S:1024..		102_29200_2-4-8-1-3_1412_7:1..
26	2025/06/03 09:40:11	167.94.138.154	Censys	US	Censys	344	10	S,U	S:2,S:21,S:25..		102_42340_2-4-8-1-3_1460_10:46..
27	2025/06/03 09:40:11	198.235.24.246	Google Virtual	US	Palo Alto Netwo	300	12	S	S:61337	Modified ZMap:273	108_65535_2_1460_0:26, 131_65535_2_1460_0:24..
28	2025/06/03 09:40:11	83.222.191.42	[illegible]Net	BG	--	4378	105	S	S:24001,S:24002..	masscan:4378	132_1024_0_00_00:162, 131_1024_0_00_00:489..
29	[illegible]	167.94.14[illegible]	Censys-arin-02	US	Censys	[illegible]	[illegible]	[illegible]	S:[illegible],S:1900..		[illegible]
30	[illegible]	220.134.1[illegible]	[illegible]hwa Teleco	TW	[illegible]	[illegible]	0	[illegible]	[illegible]	[illegible]	29_29[illegible], 102_29692_0_00_00:1..
31	2025/06/03 09:40:11	176.123.5.196	Alexhost	MD	--	217	29	R	R:1094,R:1628		102_0_0_00_00:217
32	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	131_65535_0_00_00:562, 102_65535_0_00_00:821..
33	[illegible]	[illegible]	[illegible]	NL	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	62_65535_0_00_00:18, 13_65535_0_00_00:372..
34	2025/06/03 09:40:11	205.210.31.202	Google Virtual	US	Palo Alto Netwo	255	3	S	S:6667	Modified ZMap:237	100_65535_2_1460_0:13, 108_65535_2_1460_0:20..
35	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
36	2025/06/03 09:40:11	147.185.132.85	Google Virtual	US	Palo Alto Netwo	[illegible]	9	S	S:5800	[illegible]	131_1024_2_1460_0:34, 101_1024_2_1460_0:2..
37	[illegible]	[illegible]	[illegible]	PA	[illegible]	[illegible]	[illegible]	S	S:83..	[illegible]	29_65535_0_00_00:224, 108_65535_0_00_00:250..
38	[illegible]	[illegible]	[illegible]	GB	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	13_14600_2_1460_0:10, 108_14600_2_1460_0:9..
39	2025/06/03 09:40:11	51.68.109.53	OVHcloud	FR	--	343	36	SA	SA:280,SA:479..		12_17520_0_00_00:39, 29_17520_0_00_00:44..
40	2025/06/03 09:40:11	71.6.135.131	CariNet	US	Shodan	318	10	S,U	S:13,S:17,S:19..		13_8574_2_1460_0:1, 29_5183_2_1460_0:1..
41	2025/06/03 09:40:11	189.127.165.34	Ecxon Datacente	BR	--	6890	129	SA	SA:1040,SA:1063..		102_875_2-1-1-4-1-3_1400_4:6890
42	2025/06/03 09:40:11	167.94.138.136	Censys	US	Censys	266	4	S,U	S:21,S:22,S:25..		102_42340_2-4-8-1-3_1460_10:34..
43	2025/06/03 09:40:11	186.94.57.126	Cantv	VE	--	9	0	S	S:23		138_29200_2-4-8-1-3_1460_5:4..
44	2025/06/03 09:40:11	193.163.125.253	Driftnet	GB	driftnet (inter	85	1	S,U	S:21,S:80,S:110..	Hajime:83	29_14600_2_1460_0:8, 100_14600_2_1460_0:3..
45	2025/06/03 09:40:11	196.251.85.74	Sovy Cloud Serv	SC	--	238	8	S	S:80,S:443	Modified Nmap:238	113_1025_2_1460_0:6, 108_1025_2_1460_0:58..
46	2025/06/03 09:40:11	20.15.224.135	Microsoft Azure	US	--	6212	149	S	S:873	Zmap:6212	102_65535_0_00_00:6212
47	[illegible]	[illegible]	Google Virtual	US	Palo Alto Netwo	[illegible]	[illegible]	S	[illegible]	[illegible]	[illegible]

NSD: NICTER Stream Detector

- ダークネットトラフィックをストリーム処理によりリアルタイムに分析
- スキャン元アドレスの素性や組織、スキャンの特徴などを自動判別
- Mirai判定、JA4Tタグ、独自ルールによる調査スキャナの自動判別

ダークネットトラフィックデータの活用は様々

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

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.

Spoki: Unveiling a New Wave of Scanners through a Reactive Network Telescope

Raphael Hiesgen, *HAW Hamburg*; Marcin Nawrocki, *Freie Universität Berlin*; Alistair King, *Kentik*; Alberto Dainotti, *CAIDA, UC San Diego, Georgia Institute of Technology*; Thomas C. Schmidt, *HAW Hamburg*; Matthias Wählisch, *Freie Universität Berlin*

The Age of DDoScovery: An Empirical Comparison of Industry and Academic DDoS Assessments

Raphael Hiesgen, HAW Hamburg, Hamburg, Germany; Marcin Nawrocki, NETSCOUT, Westford, MA, USA; Marinho Barcellos, U of Waikato, Hamilton, New Zealand; Daniel Kopp, DE-CIX, Frankfurt am Main, Germany; Oliver Hohlfeld, University of Kassel, Kassel, Germany; Echo Chan, Akamai/Hong Kong PolyU, Hong Kong, China; Christian Doerr, Hasso Plattner Institute, Potsdam, Germany; Christian Rossow, CISPA, Saarbrücken, Germany; Mattijs Jonker, University of Twente; Ricky Mok, CAIDA/UC San Diego

DarkSim: A Similarity-Based Time Series Analytic Framework for Darknet Traffic

Max Gao, CAIDA/UC San Diego, San Diego, CA, United States, magao@ucsd.edu; Ricky Mok, CAIDA/UC San Diego, San Diego, CA, United States, cskpmok@caida.org; Eric Li, UC San Diego, San Diego, CA, United States, jul108@ucsd.edu; Shubham Kulkarni, UC San Diego, San Diego, CA, United States, skulkarn@ucsd.edu

Have you SYN me? Characterizing Ten Years of Internet Scanning

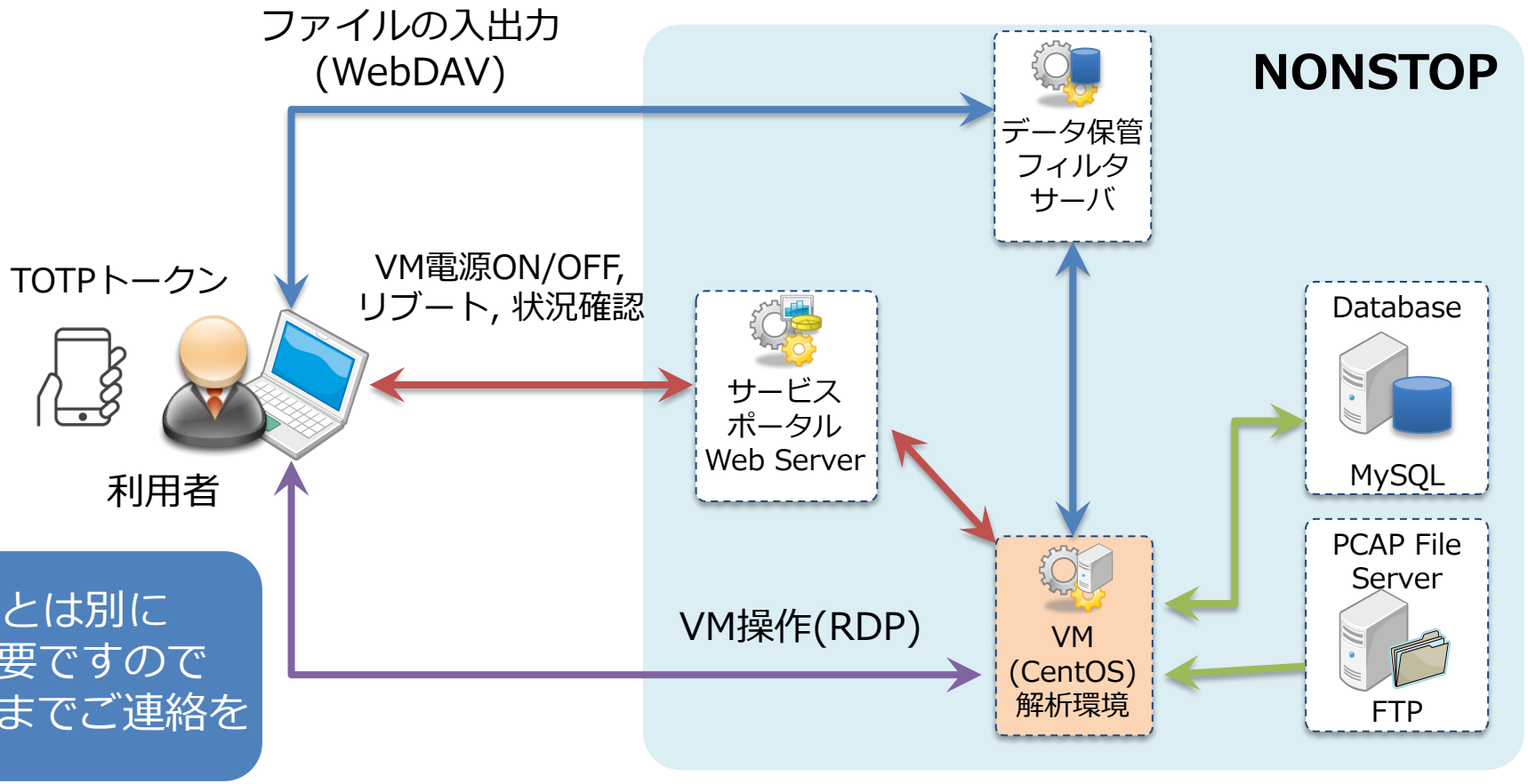
Harm Griffioen, Delft University of Technology, Delft, The Netherlands; Georgios Koursiounis, Delft University of Technology, Delft, The Netherlands; Georgios Smaragdakis, Delft University of Technology, Delft, The Netherlands; Christian Doerr, Hasso Plattner Institute, Potsdam, Germany

Can Public IP Blocklists Explain Internet Radiation?

Simone Cossaro, University of Trieste, simone.cossaro@studenti.units.it; Damiano Ravalico, University of Trieste, damiano.ravalico@phd.units.it; Rodolfo Vieira Valentim, University of Turin, rodolfo.valentim@unito.it; Martino Trevisan, University of Trieste, martino.trevisan@dia.units.it; Idilio Drago, University of Turin, idilio.drago@unito.it

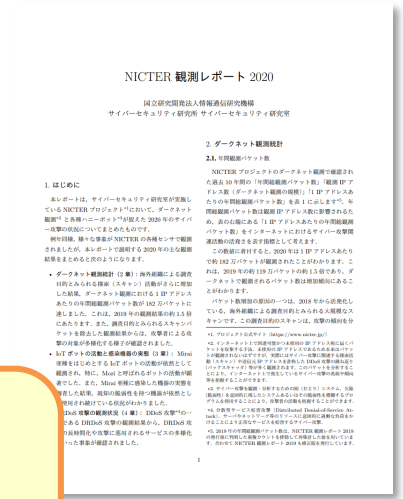
NICTER DatasetはNONSTOP上で提供

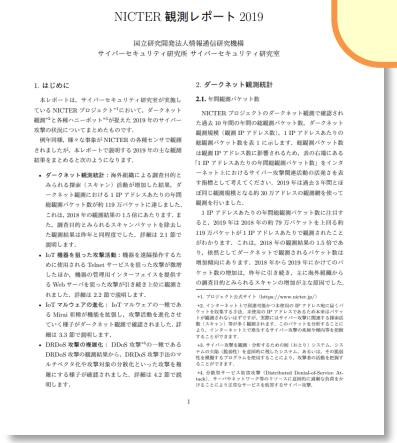
- セキュリティ研究情報を遠隔から安全に利用してもらうための環境

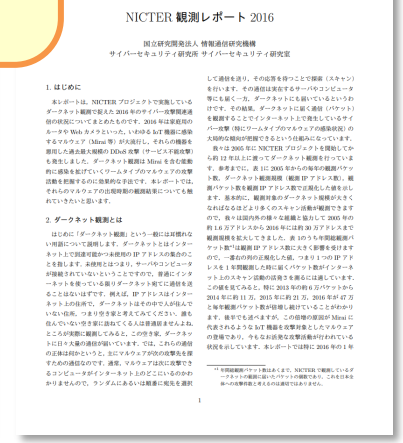


データセット利用契約とは別に
NONSTOP利用申請が必要ですので
nontop@ml.nict.go.jp までご連絡を

NICTER 観測レポート（毎年2月頃発行）







NICTERWEBで公開中
(https://nicter.jp)

宣伝 NICTサイバーセキュリティ研究室の採用情報

- **サイバーセキュリティ研究室では人材を絶賛募集中**
  - ✓研究員：７名、研究技術員：８名、RA：４名

- **様々なキャリアパス**
  - ✓企業からの転職
  - ✓博士新卒採用
  - ✓修士卒採用後に博士課程進学
  - ✓RAから研究員/技術員

- **興味がある人はぜひ**

https://csri.nict.go.jp/careers.html

まとめ

- **NICTER Dataset は提供13年目(15年間のデータ)に突入**
  - ✓ご利用に興味のある方はMWS Dataset利用のための契約締結後に、NICT 笠間(nonstop@ml.nict.go.jp) までご連絡ください
  - ✓2024年度に利用していた方も継続利用を希望される場合はご連絡ください(連絡が無い場合はどこかのタイミングでアカウントを停止します)

- **MWS Dataset 提供期間 ≒ NICTER Dataset提供期間**
  - ✓大規模データ観測は継続することが重要（短期的に集めるのは比較的容易）
  - ✓独自のデータを持っていることは大きなアドバンテージ