Institute of Advanced Sciences
Yokohama National University

YNU YOKOHAMA National University

資料７－１
※一部非公開資料※

IoT機器へのサイバー攻撃の観測と対策について

吉岡　克成

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　教授

本日のトピック

１） IoT機器を狙う脆弱性攻撃

・ハニーポットによるゼロデイ攻撃の早期検出に向けて

・クラウドボットネットについて

２） IoT機器の中での攻撃者vs攻撃者の攻防とその影響

３） 組織内のIoT機器の状況について(大学での調査)

IoTPOT（2015～），Xポット（2020～）

IoT機器へのサイバー攻撃を観測するIoTハニーポット

攻撃元機器
（マルウェア
感染済）

攻撃者が用意
したサーバ

IoT
ハニーポット

解析システム
（サンドボックス）

捕獲後15分以内に
動的解析！

Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, and Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, "IoTPOT: Analysing the Rise of IoT Compromises," 9th USENIX Workshop on Offensive Technologies (USENIX WOOT 2015), 2015.
Yin Minn Pa Pa, Suzuki Shogo, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow "IoTPOT: A Novel Honeypot for Revealing Current IoT Threats," Journal of Information Processing, Vol. 57, No. 4, 2016.
Seiya Kato, Rui Tanabe, Katsunari Yoshioka, Tsutomu Matsumoto, "Adaptive Observation of Emerging Cyber Attacks targeting Various IoT Devices," IFIP/IEEE International Symposium on Integrated Network Management (IM), 2021.

参考：IoTハニーポットに関わる統計

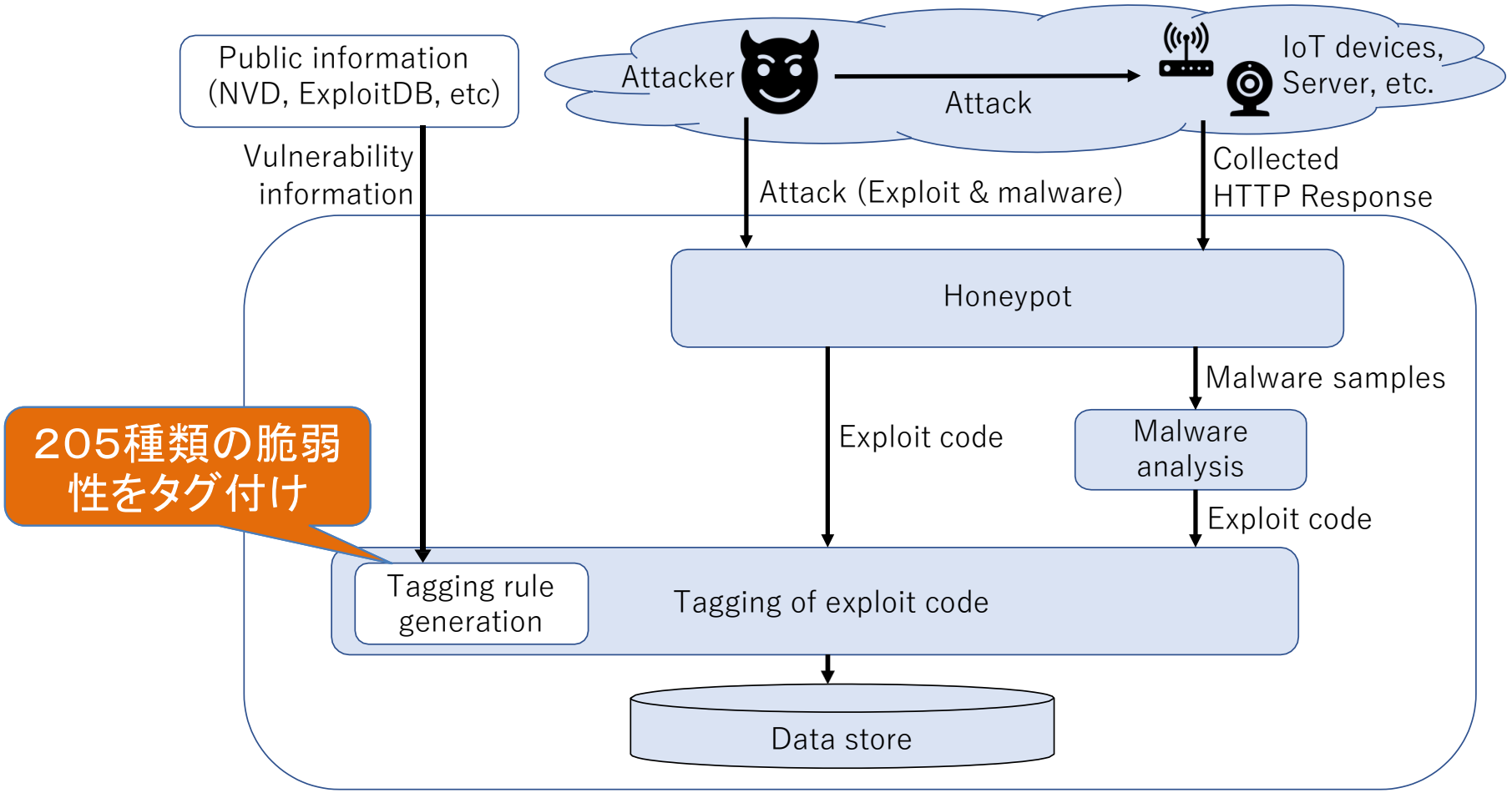
運用年数：	9年間
累計収集検体数（重複あり）：	40,392,220検体‡
累計収集検体数（ハッシュ値ベース）：	367,950検体‡
マルウェアDL URL：	418,621 件‡
検体等提供組織数：	255 組織・個人
検体等提供先国数：	47か国・地域
学術論文引用件数†：	766件†

‡ 2017/11～2024/4/28 現在での集計
† 関連論文3件の参照件数（Google Scholarによる集計, 2024/4/28現在）

参考：https://sec.ynu.codes/iot

悪用された脆弱性の判定

公開脆弱性DBを参照し、観測された攻撃とマッチングすることで、自動で攻撃対象となった脆弱性を判別、タグ付け



九鬼琉, 植田岳洋, 佐々木貴之, 吉岡克成, 松本勉, “ハニーポットで観測されたサイバー攻撃の対象機器及び脆弱性の自動推定手法の提案,” 情報処理学会コンピュータセキュリティ研究会, 2022.

機器の脆弱性を狙う攻撃の増加

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

増加

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(2017年8種類検知→2020年63種類検知)

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.

参考：特定された脆弱性一覧（2020時点）

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	Mirai	Oracle	Oracle WebLogic Server		○		1
	CVE-2019-7276	2019-01-31	2019-11-12	Mirai	Optergy	Optergy 2.3.0a	○			3
	CVE-2019-10655	2019-03-30	2019-03-31	Mirai	Grandstream	GAC2500; GVC3202; GXV3275-40; GXP2200 *	○			3
	CVE-2018-20841	2019-06-11	2019-01-14	Mirai	HooToo	HT-TM05&HT-05 routers		○		1
	Sar2HTML 3.2.1 RCE	2019-08-02	2019-08-02	Mirai	Sar2HTML	Sar2html 3.2.1	○			3
	CVE-2020-9054	2020-02-18	2020-02-24	Mirai	Zyxel	Zyxel NAS and Firewall	◐	◐		6
	Netlink GPON Router 1.0.11 RCE	2020-03-18	2020-03-18	Mirai	Netlink GPON	Netlink GPON Router 1.0.11	○			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

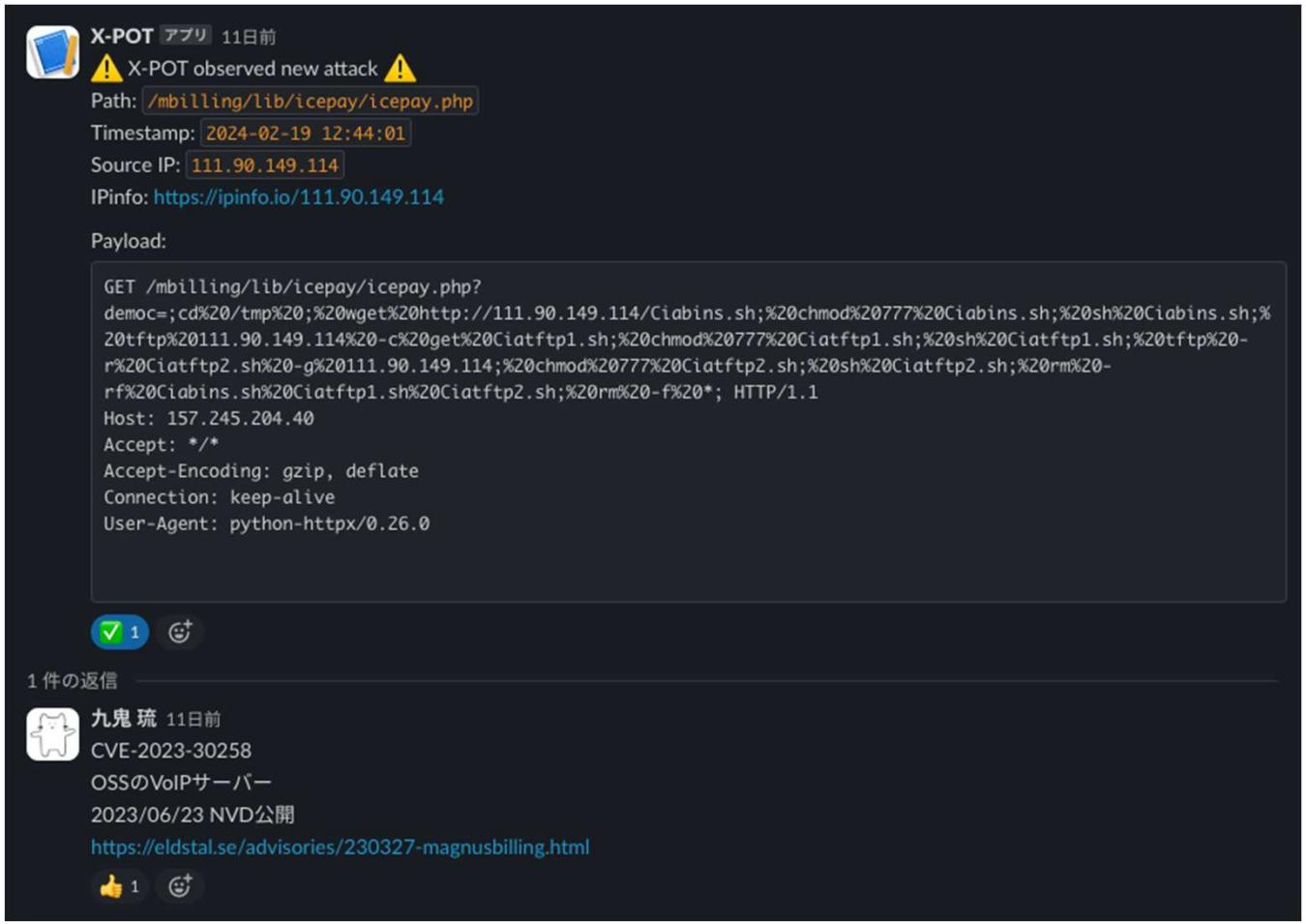
参考：特定された脆弱性一覧（2020時点）

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

未知の攻撃の早期警戒アラート

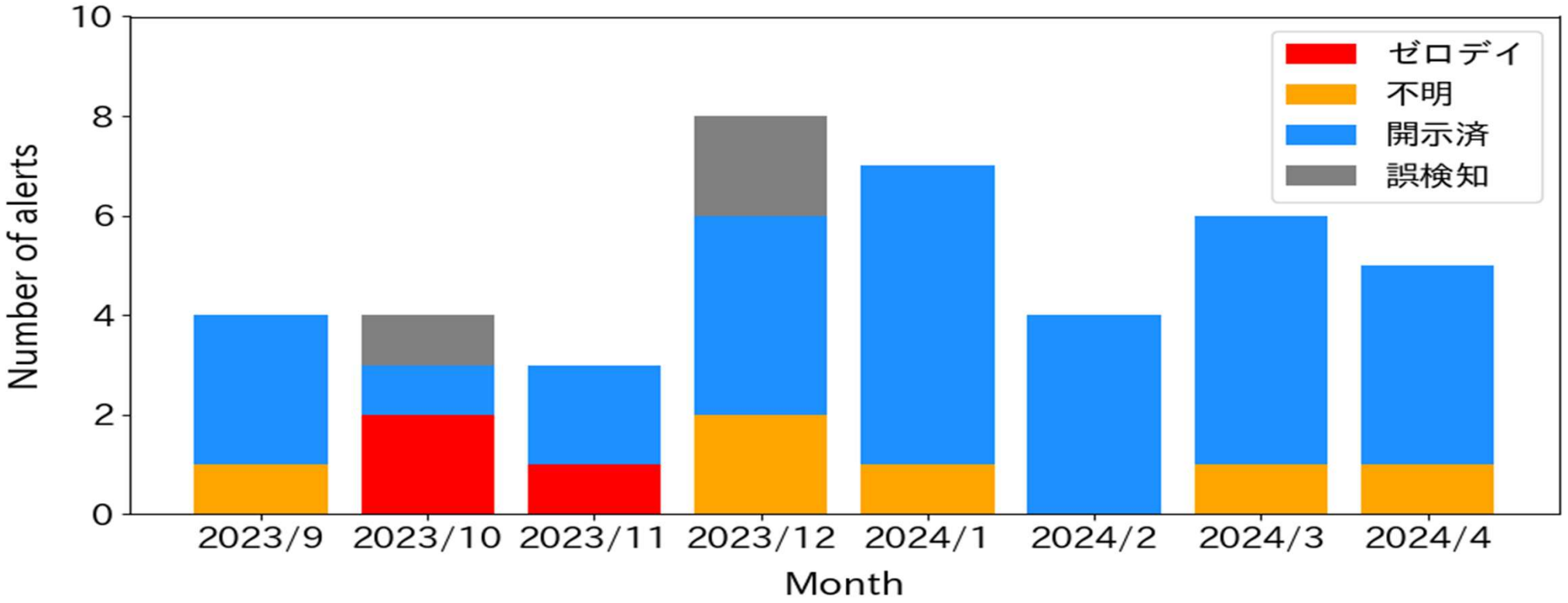
タグ付けされていない（=未知の）攻撃が観測された際にアラートを発行



アラートを精査し、ゼロデイ攻撃の疑いがあるケースは国内の観測機関が集まる定点観測友の会[1]で情報共有

[1]https://blogs.jpcert.or.jp/ja/2021/09/sigmon72.html

月次アラート数・内訳



ゼロデイ：ゼロデイ攻撃だったことが現時点で確定しているもの．アラート時点では不明だったが、事後調査によりゼロデイであることが判明したものも含む

不明：現在も対象機器・脆弱性が特定できていないもの。ゼロデイ攻撃の疑いあり

開示済：観測時点で既に脆弱性情報が開示済だったもの。X-POTでは初観測であったため、タグ付けルールを追加

誤検知：同一脆弱性に対する攻撃を既に観測・タグ付け済にも関わらずアラートが出たもの。ランダムなパスへのアクセスを除外するなどの対策を実施後、減少

非公開

ハニーポットで観測した攻撃のCVE登録

※非公開※

事例：太陽光発電施設の遠隔監視機器(国産)を狙った攻撃について

非公開

※非公開※

事例：太陽光発電施設の遠隔監視機器(国産)を狙った攻撃について

非公開

※非公開※

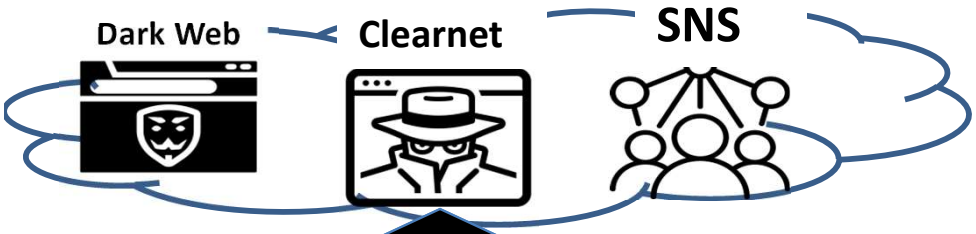
事例：太陽光発電施設の遠隔監視機器(国産)を狙った攻撃について

非公開

※非公開※

脅威アクタ観測との突合

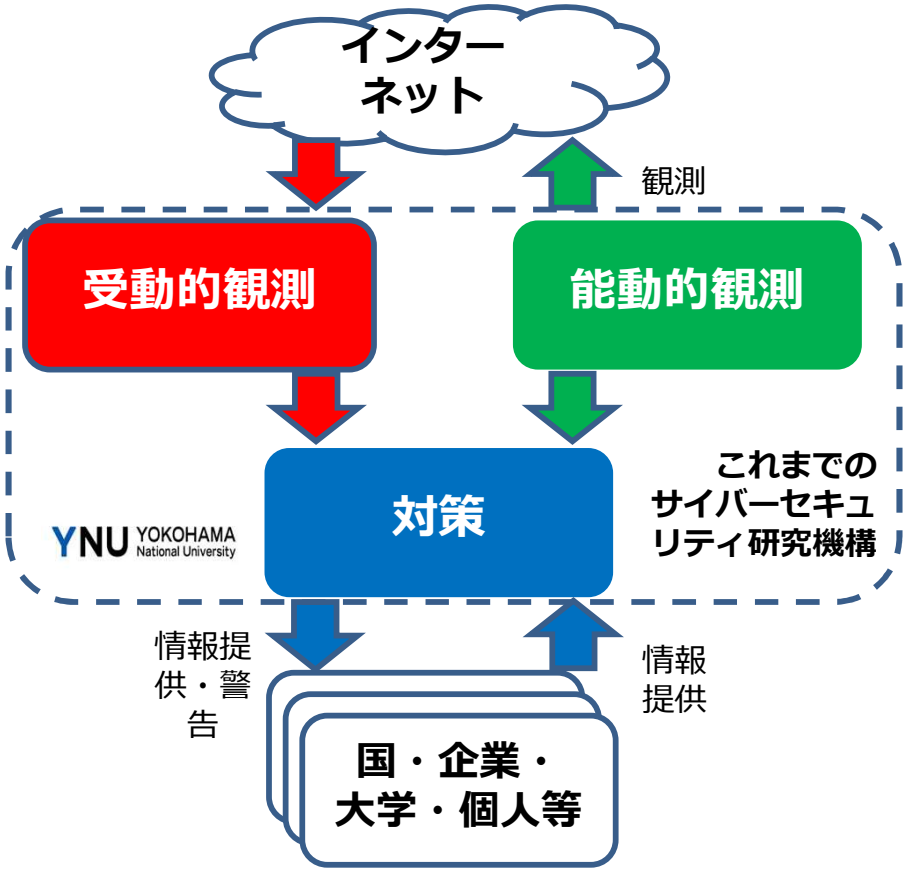
横浜国大サイバー攻撃エコシステム観測網



観測

- 脅威アクタ観測
- 仮想通貨観測
- リークデータ観測

相関分析



（新たに）
攻撃の背景となる活動を観測（構築中）

（従来通り）
サイバー攻撃と攻撃対象そのものを観測

非公開

脅威アクタの活動状況

※非公開※

非公開

当該機器の探索

※非公開※

事例：太陽光発電施設の遠隔監視機器(国産)を狙った攻撃について

非公開

※非公開※

本日のトピック

１） IoT機器を狙う脆弱性攻撃

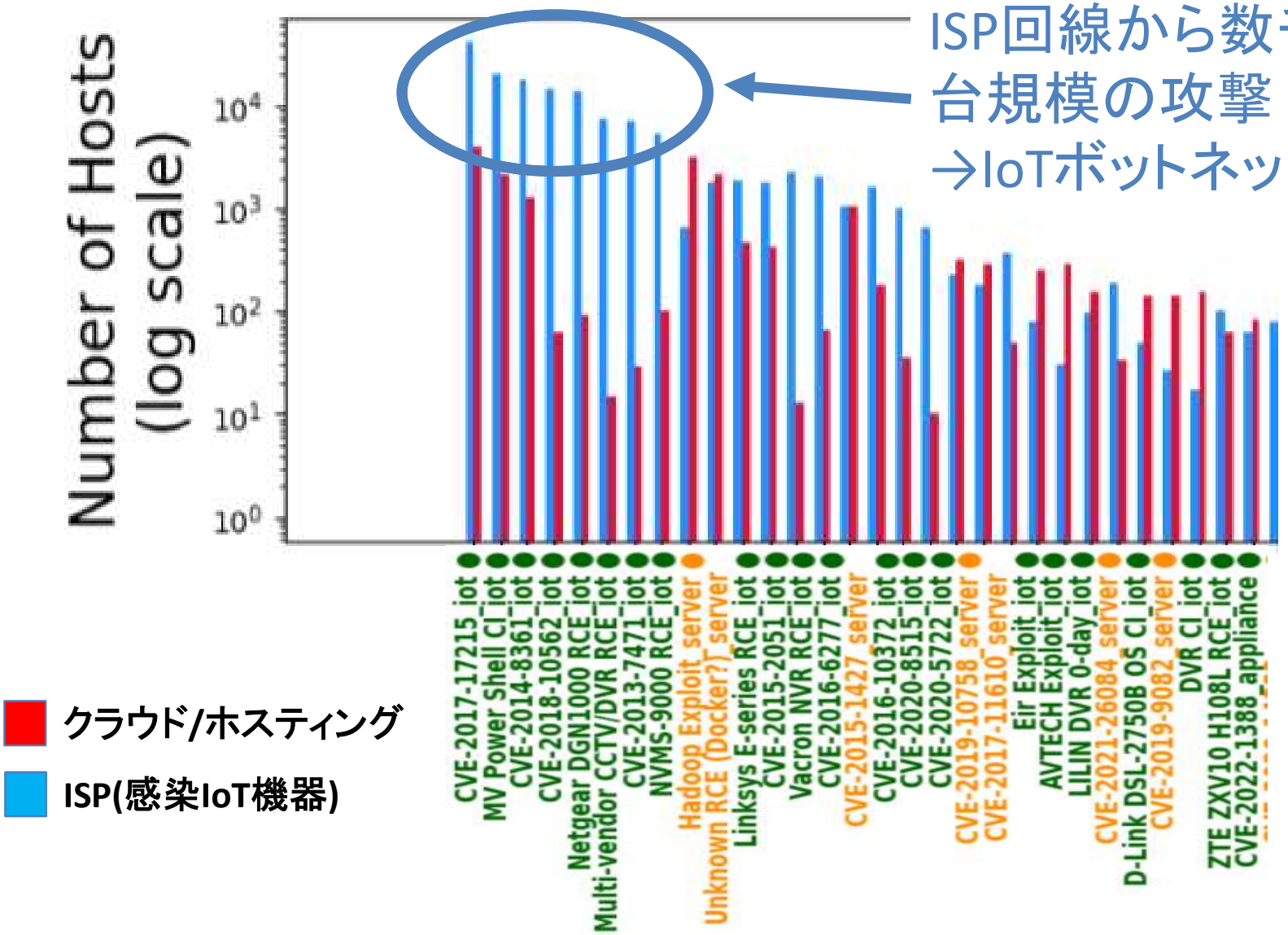
・ハニーポットによるゼロデイ攻撃の早期検出に向けて

・クラウドボットネットについて

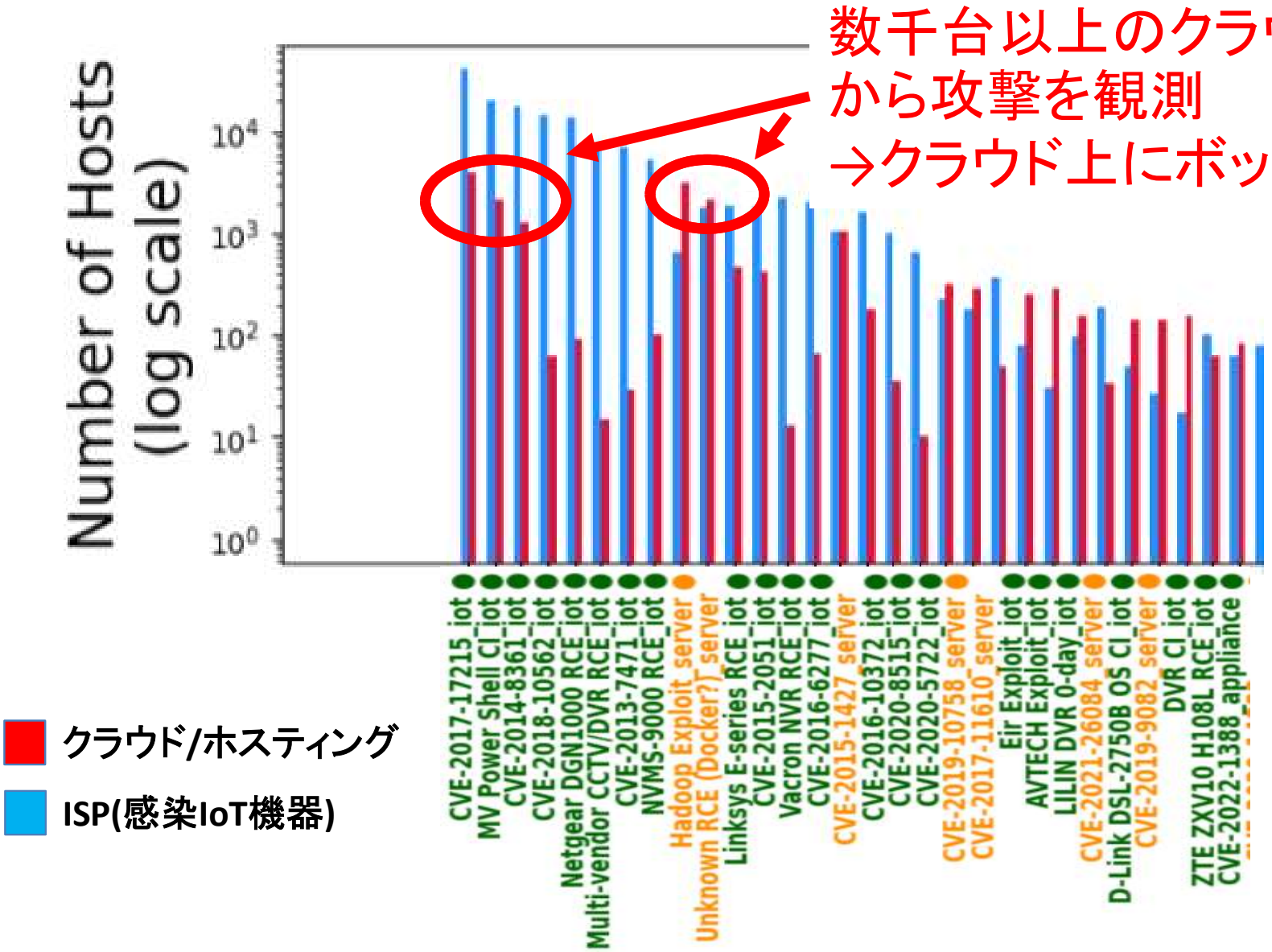
２） IoT機器の中での攻撃者vs攻撃者の攻防とその影響

３） 組織内のIoT機器の状況について(大学での調査)

脆弱性攻撃の送信元は？


ISP回線から数千～数万
台規模の攻撃
→IoTボットネットの活動
Number of Hosts
(log scale)
10^4
10^3
10^2
10^1
10^0
CVE-2017-17215_iot
MV Power Shell CI_iot
CVE-2014-8361_iot
CVE-2018-10562_iot
Netgear DGN1000 RCE_iot
Multi-vendor CCTV/DVR RCE_iot
CVE-2013-7471_iot
NVMS-9000 RCE_iot
Hadoop Exploit server
Unknown RCE (Docker?)_server
Linksys E-series RCE_iot
CVE-2015-2051_iot
Vacron NVR RCE_iot
CVE-2016-6277_iot
CVE-2015-1427_server
CVE-2016-10372_iot
CVE-2020-8515_iot
CVE-2020-5722_iot
CVE-2019-10758_server
CVE-2017-11610_server
Eir Exploit_iot
AVTECH Exploit_iot
LILIN DVR 0-day_iot
CVE-2021-26084_server
D-Link DSL-2750B OS CI_iot
CVE-2019-9082_server
DVR CI_iot
ZTE ZXV10 H108L RCE_iot
CVE-2022-1388_appliance
クラウド/ホスティング
ISP(感染IoT機器)

脆弱性攻撃の送信元は？


数千台以上のクラウドサーバから攻撃を観測
→クラウド上にボットネット？
Number of Hosts (log scale)
10^0
10^1
10^2
10^3
10^4
CVE-2017-17215_iot
MV Power Shell CI_iot
CVE-2014-8361_iot
CVE-2018-10562_iot
Netgear DGN1000 RCE_iot
Multi-vendor CCTV/DVR RCE_iot
CVE-2013-7471_iot
NVMS-9000 RCE_iot
Hadoop Exploit_server
Unknown RCE (Docker?)_server
Linksys E-series RCE_iot
CVE-2015-2051_iot
Vacron NVR RCE_iot
CVE-2016-6277_iot
CVE-2015-1427_server
CVE-2016-10372_iot
CVE-2020-8515_iot
CVE-2020-5722_iot
CVE-2019-10758_server
CVE-2017-11610_server
Eir Exploit_iot
AVTECH Exploit_iot
LILIN DVR 0-day_iot
CVE-2021-26084_server
D-Link DSL-2750B OS CI_iot
CVE-2019-9082_server
DVR CI_iot
ZTE ZXV10 H108L RCE_iot
CVE-2022-1388_appliance
クラウド/ホスティング
ISP(感染IoT機器)

クラウドボットネットの実態調査

クラウド/ホスティングネットワーク上の多数の攻撃ホストから攻撃発生

- 考えられる要因仮説

1. クラウドボットネットによる攻撃 (= 同時に多数の攻撃ホストが存在している)
2. 攻撃ホストの頻繁な入れ替わりやIPアドレスの変更 (= 同時に存在する攻撃ホストは少数だが多数のIPアドレスが観測)

非公開

クラウドボットネットの実態調査①

※非公開※

非公開

クラウドボットネットの実態調査①

※非公開※

非公開

Cloudflare Names OVH and Hetzner as Origins of DDOS Attack

※非公開※

非公開

クラウドボットネットの実態調査①

※非公開※

非公開

クラウドボットネットの実態調査②
（別の事例）

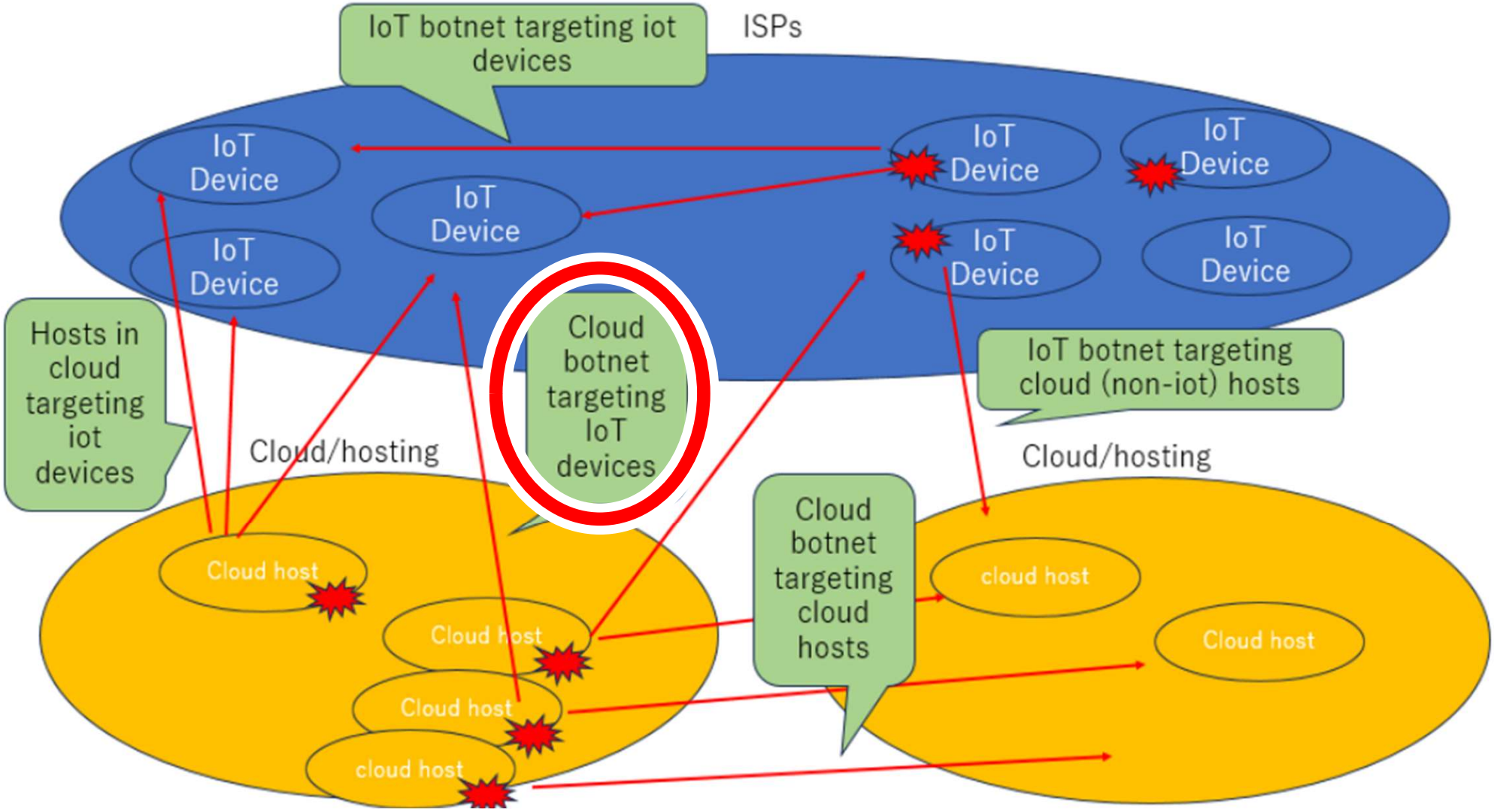
※非公開※

非公開

クラウドボットネットの実態調査②

※非公開※

クラウドボットネットの実態調査



クラウドボットネットはIoT機器とクラウドホストの両方を狙って攻撃
→クラウドとIoTで攻撃がクロスオーバーしている

本日のトピック

１） IoT機器を狙う脆弱性攻撃

・ハニーポットによるゼロデイ攻撃の早期検出に向けて

・クラウドボットネットについて

２） IoT機器の中での攻撃者vs攻撃者の攻防とその影響

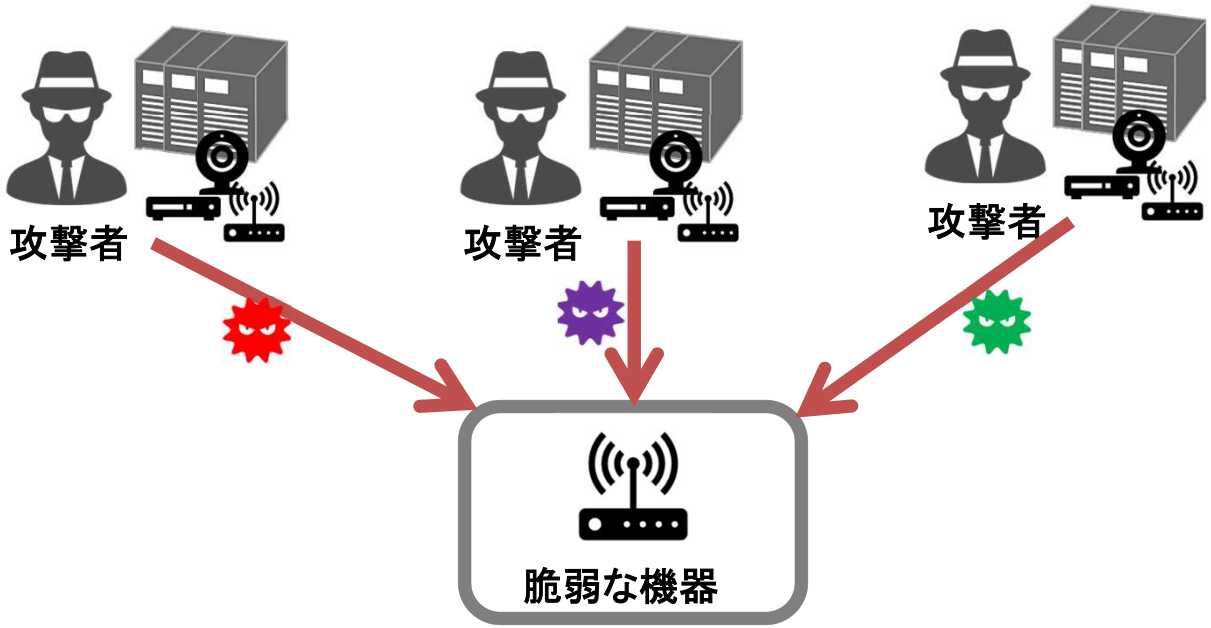
３） 組織内のIoT機器の状況について(大学での調査)

質問：脆弱なIoT機器には実際に何が起こる？

疑問：1時間に何百回も様々なマルウェアや攻撃者から攻撃を受けるが、沢山の種類のマルウェアに多重感染するのか？

疑問： 侵入時に他のマルウェアを止めたり、侵入口(例：Telnet)を閉じるマルウェアが知られているが、最終的にはどのマルウェアが勝つ？

結局、脆弱なIoT機器に何が起こるのか、わかっていない



IoTマルウェア活動の長期観測システム

■12種類の脆弱なIoT機器を用意

■ホストベースの監視機構を組み込み、プロセスやポート待ち受け、通信を監視

■マルウェアダウンロードは自動許可

■マルウェアから外部への通信をダミーサーバに転送し、行われた通信を手動で解析．C&Cサーバへの通信を特定、外部への通信を随時許可

■スキャン、エクスプロイト、DoSはダミーに転送

■各機器を**数十日間**連続で観測する実験を**約半年間**に渡り実施

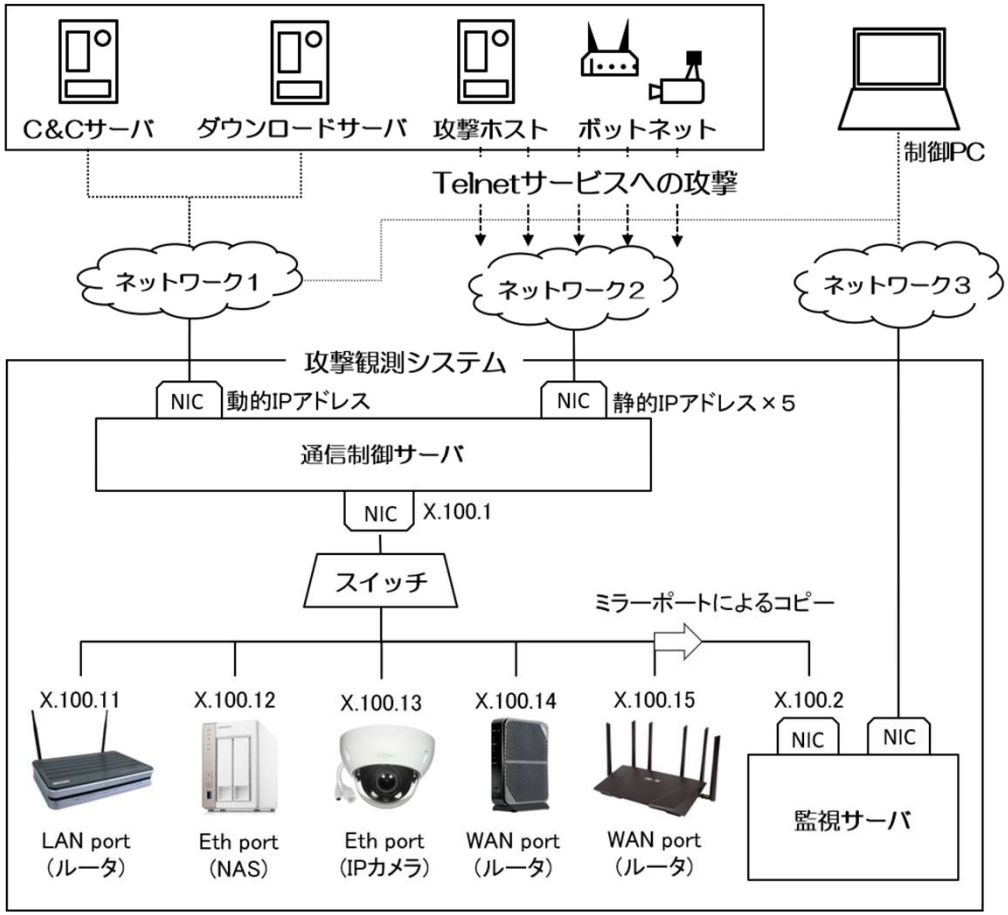
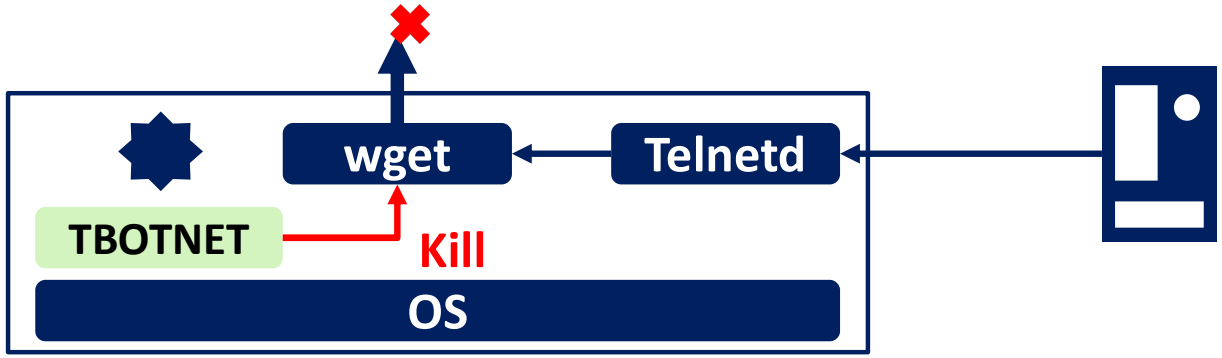


図3：攻撃観測システムのネットワーク構成

Device ID		1	2	3	4	5	6	7	8	9	10	11	12
Device Information	Vendor	Billion	QNAP	Dahua	ZyXEL	ASUS	ZTE	D-Link	opengear	Ubiquiti	Synology	Hikvision	NETGEAR
	Category	Router	NAS	IP Camera	Router	Router	Router	Router	Router	Access Point	NAS	IP Camera	Router
	CPU	mips	x86-64	armv5l	mips	armv7l	mips	mips	armv7l	mips	armv8l	armv5l	mips

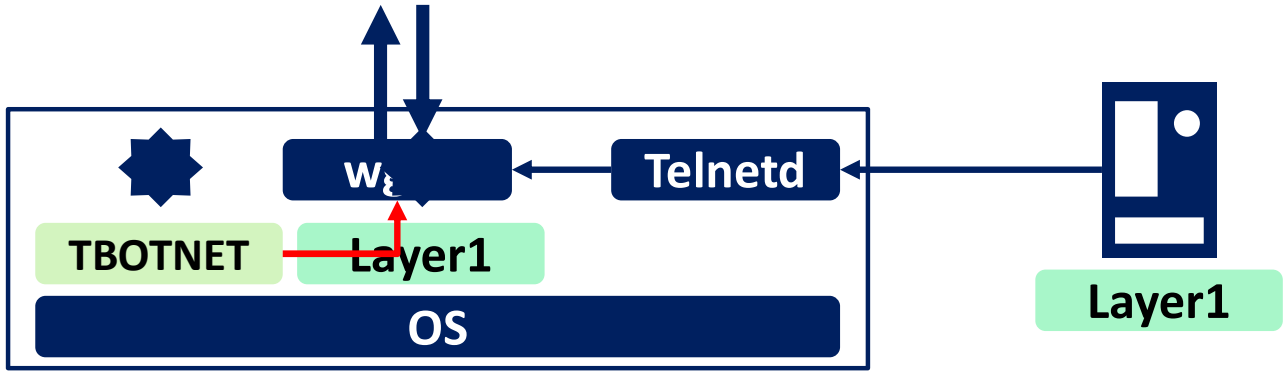
事例1：QNAP NASを巡る攻防

ボットネット「TBOTNET」は侵入後、他の侵入者が行うファイル転送コマンドのKill
を続けることで、他のマルウェアの感染を妨害し、約10日間QNAPを占有した



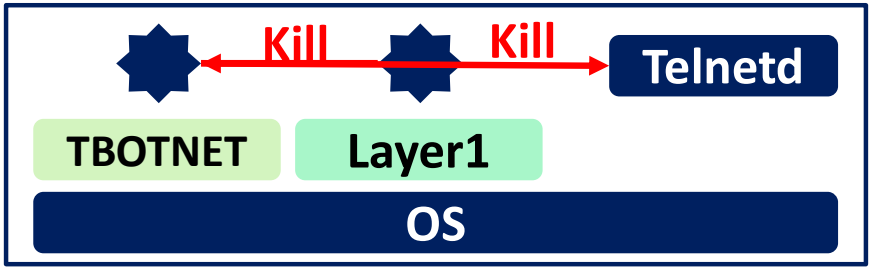
事例1：QNAP NASを巡る攻防

観測14日目、別のボットネットLayer1が、偶然マルウェアファイル転送と感染に成功.



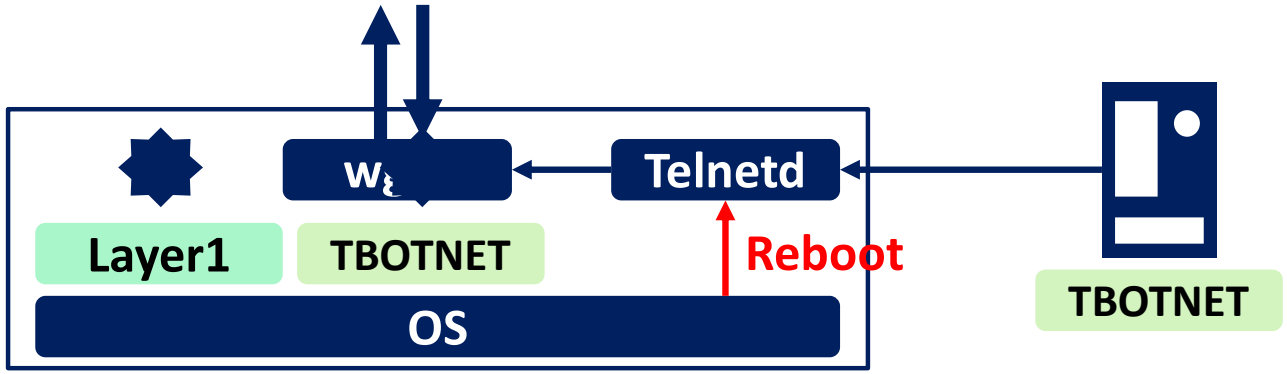
事例1：QNAP NASを巡る攻防

ボットネットLayer1は、TBOTNETをkillし、機器の権限を奪取．さらに、侵入口であるTelnetdのプロセスもkillし、機器の独占支配に成功した(と思われた).



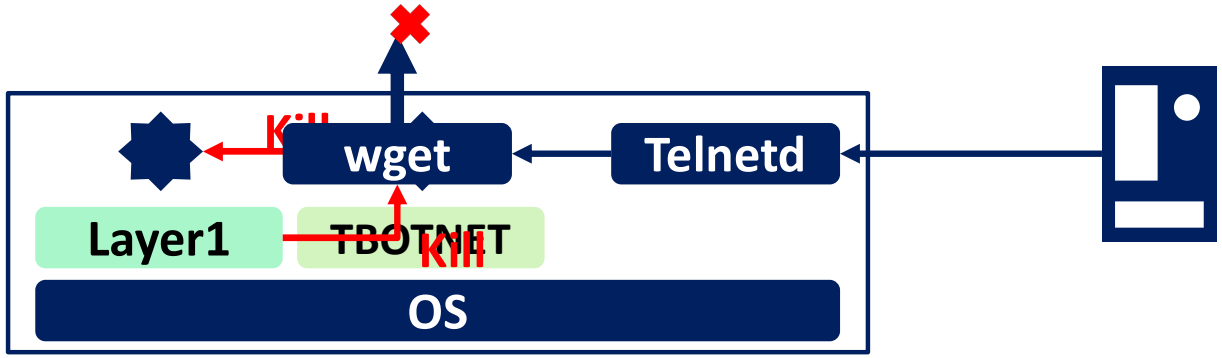
事例1：QNAP NASを巡る攻防

ところがQNAPのサービス管理機能により、Layer1が停止させたTelnetdが再起動し、その隙にTBOTNETが再び侵入



事例1：QNAP NASを巡る攻防

今度は逆にTBOTNETがLayer1をkillし、さらにファイル転送コマンドのkillによる独占を再開



- この「14日目の攻防」は3分間の出来事だった
- 隙を見せるとすぐに他の攻撃者に侵入される状況であり、IoT機器を巡り、攻撃者vs攻撃者の攻防が激化している
- 機器が自動でTelnetを再起動しなければ、Layer1が機器を独占していた．その場合、Telnetは停止され、NOTICE等の広域スキャンで発見が出来なかったはずである．(TBOTNETに感染しているとTelnetは動作し続けるため、広域スキャンにより検知可能)

→攻撃者同士の攻防がNOTICEの観測結果に影響し得る

このような攻防は頻繁に起きている

非公開

※非公開※

非公開

各ボットネットが有する攻防能力

※非公開※

調査のまとめ

IoT機器の中では複数の攻撃者が機器を**奪い合っている**

外部の攻撃ホストとマルウェアの両方で**機器を独占**しようという振る舞い観測された。

後続の侵入を防ぐ

- ファイアウォールの変更
- Telnetサービスの停止
- セッションの切断
- ファイル転送コマンドの停止

既存の感染機器を奪う

- 他マルウェアプロセスの停止
- ファイルの削除
- 機器の再起動

機器を奪い返す

- 報告された認証情報の記憶
- 継続的な機器への攻撃

セキュリティの甘いIoT機器への侵入者の主な相手は**「防御者」ではなく「他の攻撃者」**であり、それを認識している攻撃者は、他の攻撃者を排除して機器を占有する戦略を採っている

→この状況を理解した上で観測を行うことでより適切な状況把握が可能

本日のトピック

１） IoT機器を狙う脆弱性攻撃

・ハニーポットによるゼロデイ攻撃の早期検出に向けて

・クラウドボットネットについて

２） IoT機器の中での攻撃者vs攻撃者の攻防とその影響

３） 組織内のIoT機器の状況について(大学での調査)

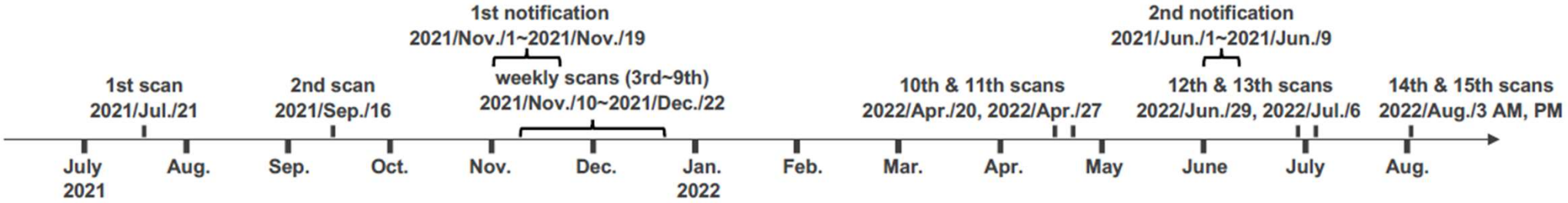
横浜国大における脆弱IoT機器調査

•横浜国大はクラスB(65,535アドレス)ネットワークを所持．FWにより外部からのTCPセッション確立は不可能．サーバ公開には申請が必要となっている．

•一方、附属小中学校など多数の部局、関連組織が利用しており、学生等の持ち込みデバイスも多いため、境界防御は不十分．ゼロトラストセキュリティの観点でも学内の機器のセキュリティを確保する必要がある．

•そこで、横浜国大が所持するクラスB(65,535)ネットワークをスキャンし、IoT機器で動作することが多いTelnet, FTPに特化した調査を行った．

•学内で**Telnet/FTPが動作するIoT機器を185件**検出した．これらの機器の所有者(正確には機器が検知されたIPアドレスの利用者)に注意喚起を行い、機器の使用状況や利用者の意識、メーカの対応を調査した．（下記は調査スケジュール）



発見された機器の台数(カッコ内は機器種類数)

Device Type	Telnet or FTP	Telnet	FTP
Smart card reader	53 (2)	53 (2)	53 (2)
Printer/Multi-function printer	38 (27)	21 (16)	36 (25)
Electric current monitor	13 (2)	13 (2)	11 (1)
Display controller	11 (1)	0 (0)	11 (1)
NAS	11 (10)	1 (1)	10 (10)
Announcement broadcast system	8 (1)	0 (0)	8 (1)
Data logger	6 (2)	0 (0)	6 (2)
Earthquake early warning system	6 (2)	6 (2)	0 (0)
L2 switch	5 (2)	5 (2)	0 (0)
Wireless LAN access point	4 (2)	4 (2)	0 (0)
UPS	4 (2)	4 (2)	1 (1)
Wireless LAN controller	3 (1)	0 (0)	3 (1)
Energy monitor	3 (1)	0 (0)	3 (1)
Router	3 (1)	3 (1)	0 (0)
Network adapter for printer	2 (2)	2 (2)	2 (2)
Web camera	2 (2)	1 (1)	2 (2)
Black and white printer	2 (1)	0 (0)	2 (1)
Paperless recorder	1 (1)	0 (0)	1 (1)
HPLC controller*	1 (1)	1 (1)	0 (0)
Web conferencing system	1 (1)	1 (1)	0 (0)
Power supply Control	1 (1)	1 (1)	0 (0)
Backup storage	1 (1)	0 (0)	1 (1)
Total (IoT devices identified model No.)	179 (66)	116 (36)	150 (52)

* High-Performance Liquid Chromatography (HPLC) controller

学内の多数の機器でTelnetとFTPが動作

スマートカードリーダ、プリンタ、複合機、電流計、ディスプレイコントローラ、NAS、データロガー、地震速報システム、L2スイッチ、UPS、エネルギーモニター、など多様な機器が発見された

注：型番まで判明した179台に関する結果

Takayuki Sasaki, Takaya Noma, Yudai Morii, Toshiya Shimura, Michel van Eeten, Katsunari Yoshioka, and Tsutomu Matsumoto, "Who Left the Door Open? Investigating the Causes of Exposed IoT Devices in an Academic Network," Proc. 45th IEEE Symposium on Security and Privacy (IEEE S&P 2024), 2024.

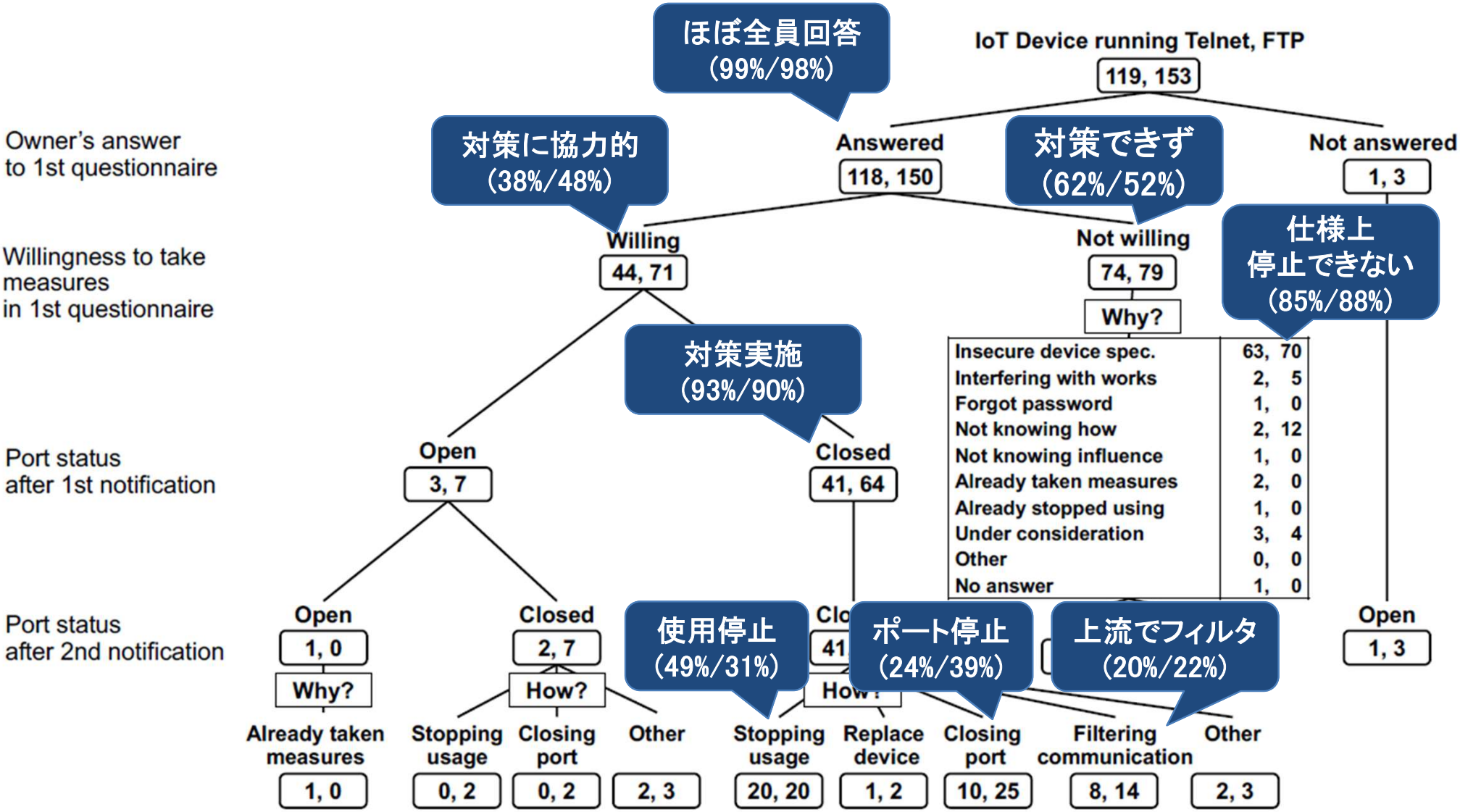
機器の所有者(利用者)はTelnet/FTPについて認識していない

Default setting	Owner's awareness of each device			
	Telnet		FTP	
	Unaware	Aware	Unaware	Aware
Enabled by default	42	1	61	8
Disabled by default	2	1	13	3

Telnet/FTPがデフォルトで動作しているにもかかわらず、その動作を認識していない所有者(利用者)が圧倒的に多い

Takayuki Sasaki, Takaya Noma, Yudai Morii, Toshiya Shimura, Michel van Eeten, Katsunari Yoshioka, and Tsutomu Matsumoto, "Who Left the Door Open? Investigating the Causes of Exposed IoT Devices in an Academic Network," Proc. 45th IEEE Symposium on Security and Privacy (IEEE S&P 2024), 2024.

機器の所有者(利用者)による対応状況



Takayuki Sasaki, Takaya Noma, Yudai Morii, Toshiya Shimura, Michel van Eeten, Katsunari Yoshioka, and Tsutomu Matsumoto, "Who Left the Door Open? Investigating the Causes of Exposed IoT Devices in an Academic Network," Proc. 45th IEEE Symposium on Security and Privacy (IEEE S&P 2024), 2024.

機器の説明書の分析

TABLE 9. DESCRIPTIONS OF THE PURPOSE OF TELNET/FTP IN IOT DEVICE MANUALS

Purpose of services	Telnet	FTP
Mentioned in manuals	10	36
Not mentioned in manuals	5	3
No description*	15	10
Total models	30	49

* No description of the service at all.

Telnetが動作する機器のうち、用途がマニュアルに明記されているのは30機種中10機種のみ、5機種は用途が明記されておらず、15機種は全く説明がなかった.

FTPについても、49機種中、全く説明がない機器が10機種あった

これらの機器では所有者はサービスのリスクも把握できず、対策も採れない

機器メーカへの質問の結果

Telnet: #Total device models = 22 , #Manufacturers = 10

Question #Subject models(Manuf.)*	Manufacturers' answers	#Mo (#Manu
Q1. Usage of Telnet 22 (10)	For management	16 (8)
	Don't know the purpose of Telnet	5 (1)
	Don't know Telnet service itself	1 (1)
Q2. Default enabled 20 (10)	Enabled by default	21 (9)
	Don't know	1 (1)
Q3. Login credentials (10)	Disclosed in answer	16 (6)
	Don't know	1 (1)
	Not disclosed to owners	5 (3)
Q4. Security measures 22 (10)	Not deployed	21 (9)
	Don't know	1 (1)

管理用

不明！？

Telnetの使用目的は？

不明！？

デフォルトで動作

デフォルト設定は？

不明！？

(機器の所有者なので)ログイン情報を下さい

(所有者なのに)非開示

対策なし

不正侵入時の対策は？

まとめ

- 学内でTelnet/FTPが動作する機器を185件発見
- 大部分のユーザは機器で動作するTelnet/FTPを認識せず
- 機器のマニュアルにはTelnet/FTPの記載がないか、リスクの記載がない場合が多く、利用者は対応しようがない
- Telnetを管理目的で使っている場合が多いが、中にはTelnetが動作していることを認識していないメーカもある
- Telnetを利用者に知らせずに管理目的で利用しており、要求してもパスワードを開示しないメーカがある

メーカのセキュリティ対策には改善の余地があり、特にユーザへの適切な情報提供が不足している.

全体のまとめ

- IoT機器の脆弱性を狙う攻撃が活性化
- ハニーポットによるゼロデイ攻撃検知は有効であり、ハッカーフォーラム等を含め関連情報を充実化することで迅速な対応につながる
- 攻撃者はIoT機器とクラウドの両方を標的/リソースと見ている
- IoT機器を狙う攻撃者同士の争いが激化し、観測結果に影響を与えている可能性があるため、この状況を適切に把握する必要がある
- 組織内のIoT機器の現状は、インターネットに直接接続された機器よりも深刻．メーカの意識改善と利用者とのリスクコミュニケーションの改善が必要
- マニュアルはベストのコミュニケーションツールとは言い難い．AI等も活用し、インタラクティブでバリアフリーなコミュニケーションが実現できないか？

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2:本研究は、国立研究開発法人情報通信研究機構（NICT）の委託研究（JPJ012368C05201および採択番号08101）により得られた成果を含みます。