JNSA標準化部会セミナー
「IoTセキュリティ標準化の動向を知る」

中尾　康二
JNSA　副会長、標準化部会長
NICT 主管研究員
横浜国大　客員教授

NICTERによるサイバー脅威観測

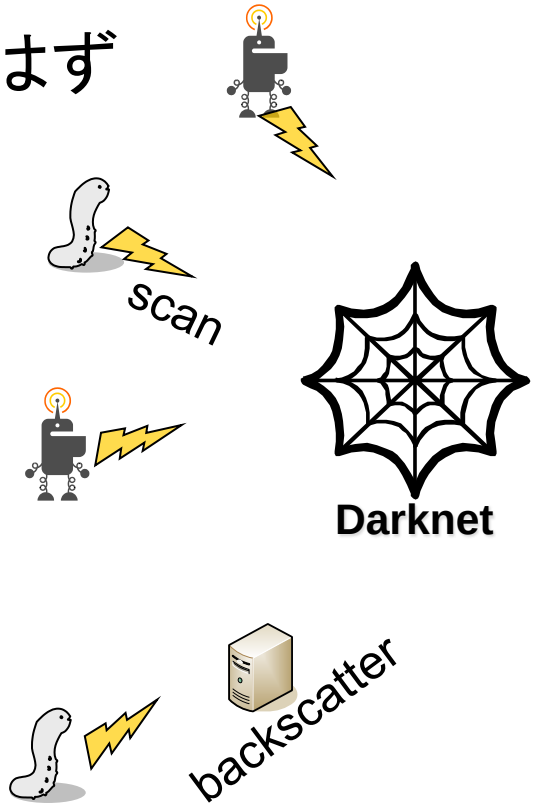
ダークネットとは

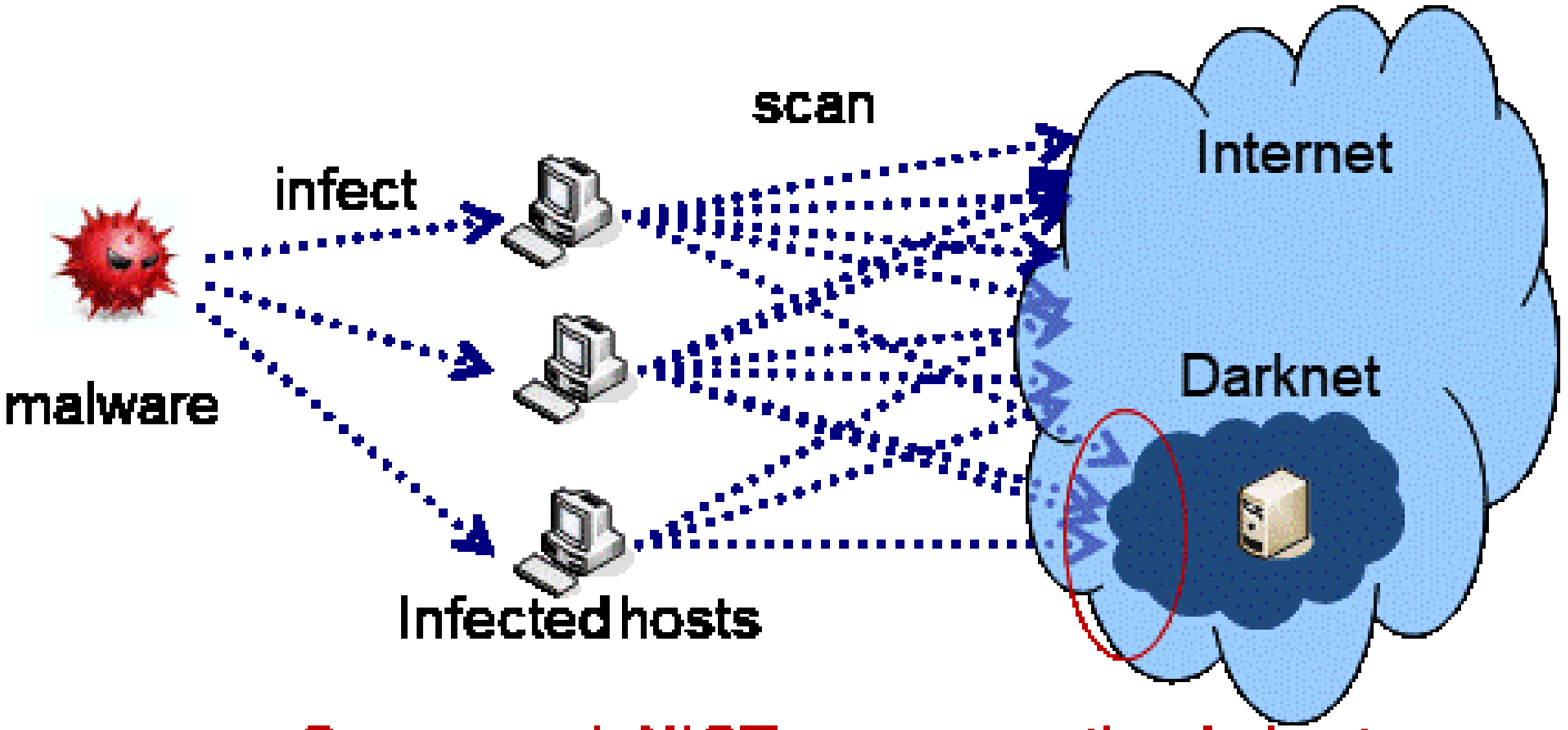
- **Darknet**:　未使用IPアドレス空間

- **理論的には**:　未使用のため、理論的にはパケットは来ないはず
- **実際は**:　実際は到達している

- 到達パケットには：
  - Scans by malwares （マルウェアによるスキャン）
  - Backscatter (reflection of DDoS attack)（Dosの跳ね返り）
  - Miss configurations　etc. （ご設定等）

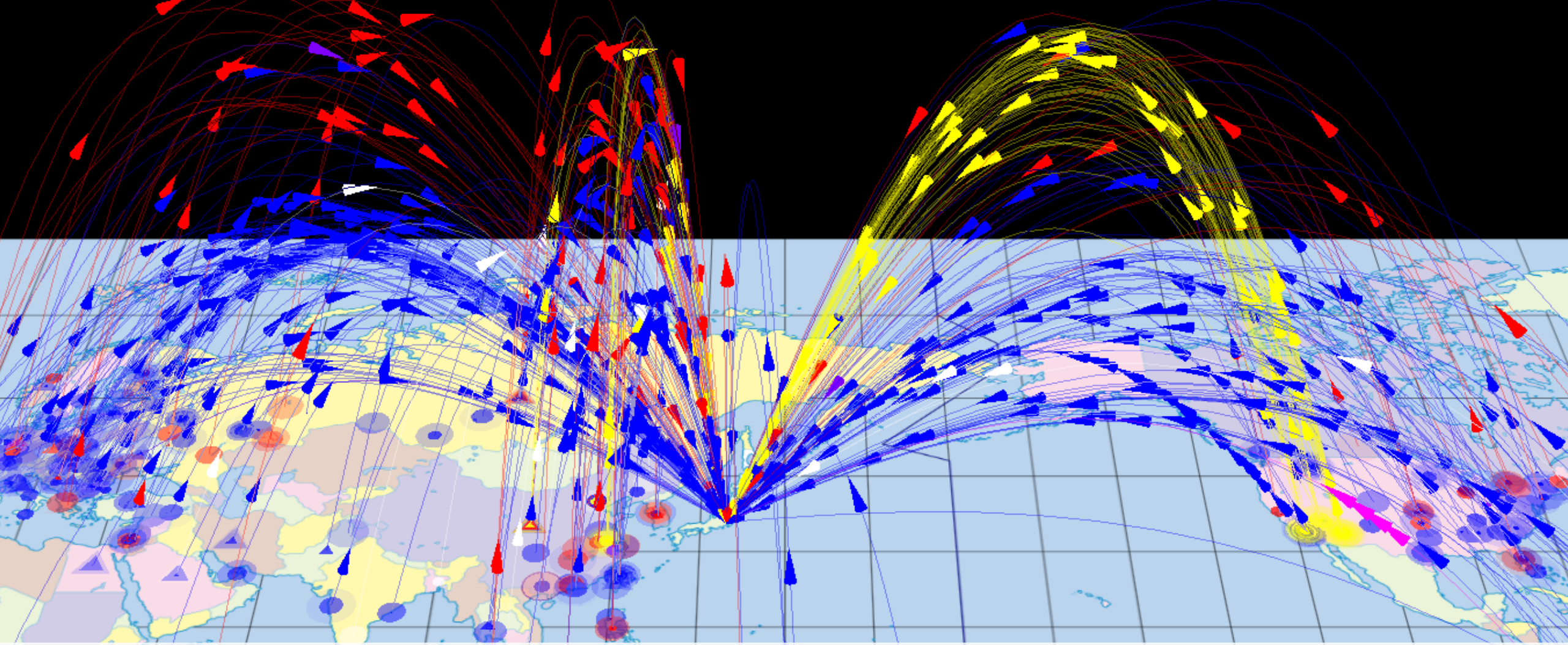
- ダークネットを用いることで、マルウェア感染状況の
  大きなトレンドを把握できる





Scans reach NICT sensors on the darknet

ＮＩＣＴのダークネット観測に到達するスキャンのイメージ

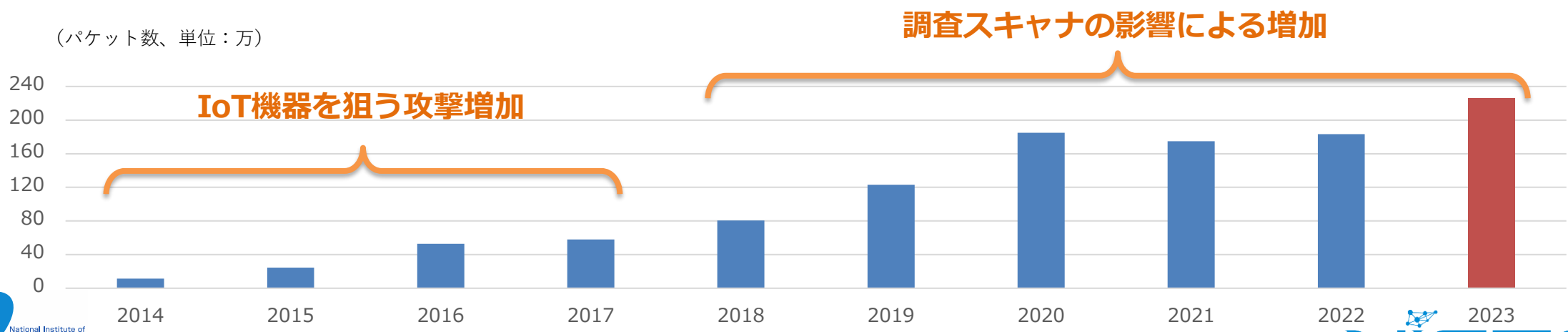


NICTER

- 無差別サイバー攻撃に対抗するための統合セキュリティ・システム
- 大規模なダークネット監視、自動マルウェア解析、およびそれらの相関関係の導出

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
2014	約241.0億	212,878	115,335
2015	約631.6億	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**

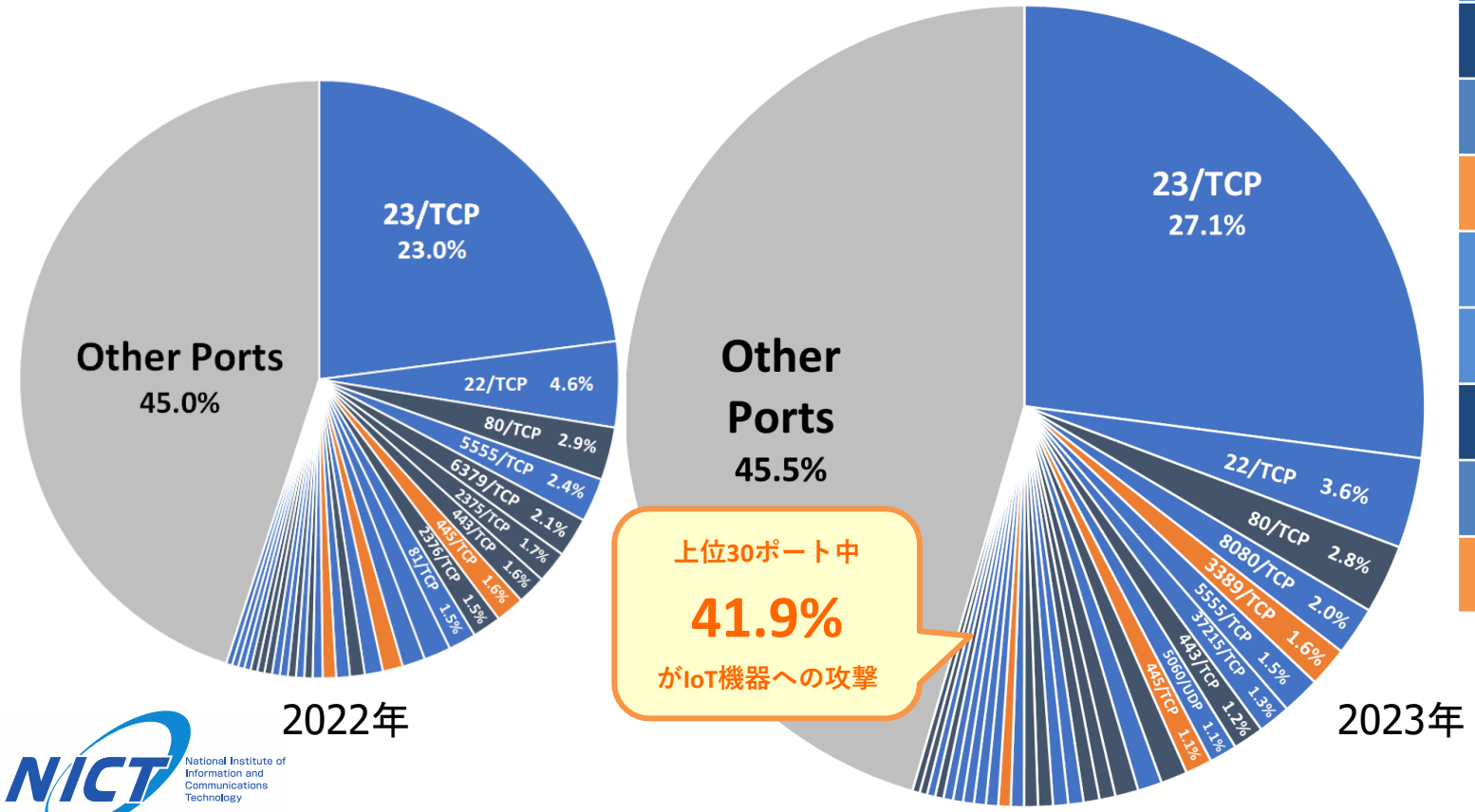


1 IPアドレス当たりの年間総観測パケット数

宛先ポート番号別パケット数分布（2023年）

2023年の特徴

- 上位30ポート中 **41.9%がIoT機器への攻撃**
- **23/TCP**（Telnet）宛ての増加傾向が2022年から継続
- IoT機器固有のサービスのポート番号宛てが増加



ポート番号	主な攻撃対象
23/TCP	Telnet （ルータ，Webカメラ等）
22/TCP	SSH（サーバ，ルータ等）
80/TCP	HTTP（Web管理画面）
8080/TCP	HTTP（ホームルータ、DVR等）
3389/TCP	Windows Remote Desktop
5555/TCP	ADB（Android Debug Bridge）
37215/TCP	HTTP（ホームルータ）
443/TCP	HTTPS (Web管理画面等)
5060/UDP	SIP (PBX, ルータ等)
445/TCP	Microsoft-DS（SMB等）

宛先ポート番号別パケット数分布
（調査目的のスキャンパケットを除く）

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

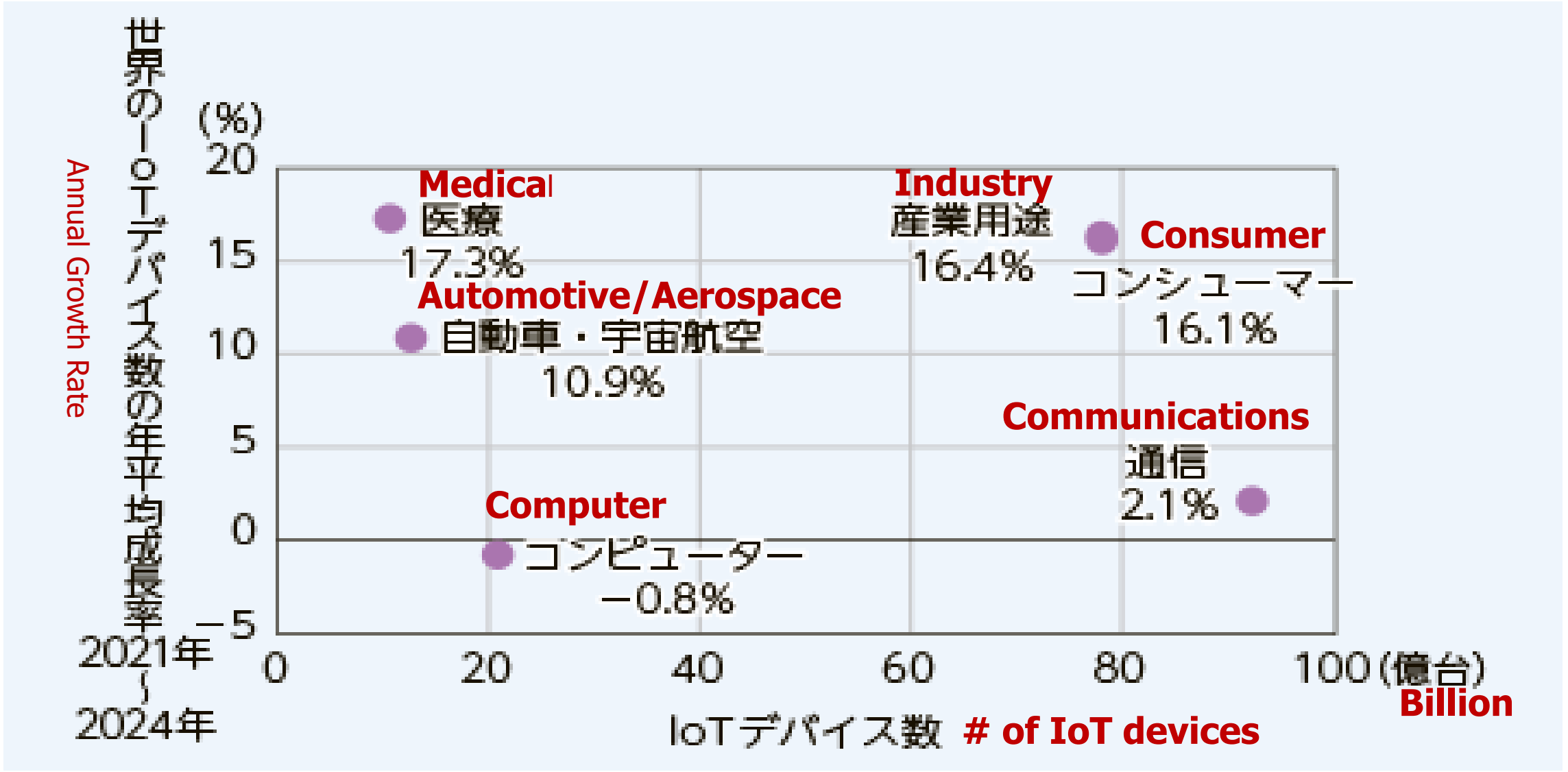
2023's Infected Device in JP: LTE Router (2023年の感染機器：LETルーター)

- **Rooster Series (Sundenshi Co.,Ltd.)　（ルーターシリーズ）**
  - ✓LTE router
  - ✓liveness monitoring
  - ✓automatic recovery
  - ✓remote maintenance
  - ✓**Infected via management Web IF with default ID/Password**
    （デフォルトのID/パスワードで管理ウェブIF経由で感染）

- **HWL-2511-SS (HYTEC INTER Co., Ltd.)　（台湾製）**
  - ✓LTE router for small industrial system
  - ✓**Infected via management Web IF with no ID/Password**
    （ID/パスワード無しで管理ウェブIF経由で感染）

IoT時代　サイバーフィジカルの世界・・・

Global IoT Device Count and Growth Rate Forecast by Sector/Industry
(分野・産業別の世界のIoTデバイス数及び成長率予測)



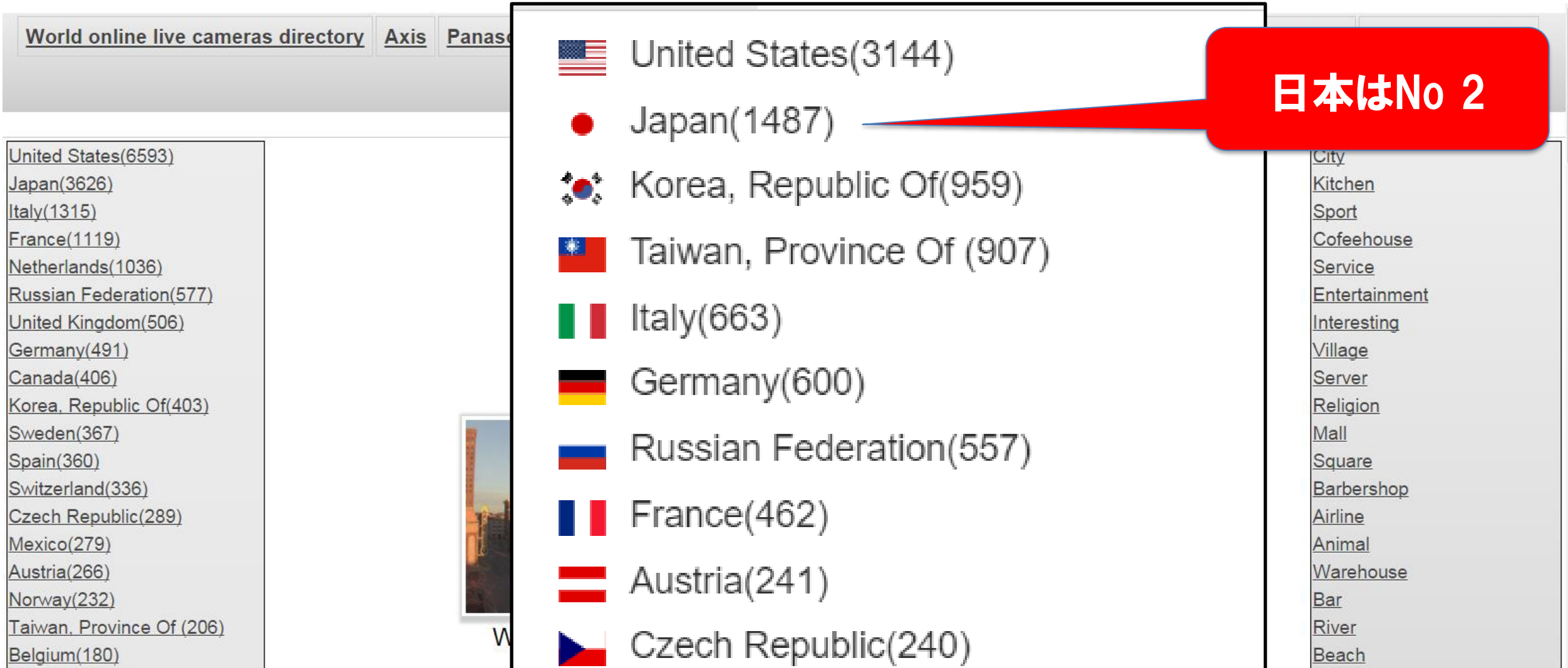
出典： 総務省情報通信白書　令和4年　IoTデバイスの急速な普及

IPカメラの場合

ネットワークカメラ画像無断公開サイト：Insecam
https://www.insecam.org/

ネットワークカメラ画像が漏れている

http://insecam.org/



公開されているNWカメラ画像（日本）

Live camera in Tokyo, Japan

Live camera in Tokyo, Japan

Live camera in Tokyo, Japan

IoTの脅威

Cyber attacks in IoT on the rise

Thingbots: The Future of Botnets in the Internet of Things

February 20, 2016 | By Paul Sabanal

The Internet of Things (IoT
upon us. Everything from
home appliances, watches
even children's toys are be
connected online. It is proj
that by the year 2020, ther
more 25 billion devices

T Home Router Botnet Leveraged in
Large DDoS Attack

Is your refri spam-sendi

ing botnet?

Ars unravels the report that hackers have commandeered 100,000 smart devices.

by Dan Goodin - Jan 18, 2014 5:25am JST

Internet of Things security concerns pr boost in IoT services

by

News roundup: As Internet of Things concerns become
erprise reality, one vendor is quick to offer IoT
s to combat the risks. Plus: 1% of users create
the risk; Target pays up; Apple devices
erly secured in the enterprise.

RISK ASSESSMENT / SECURITY & HACKTIVISM

"Internet of Things" is the new Windows XP —malware's favorite target

Botnet & DDoS

Targeted Facilities

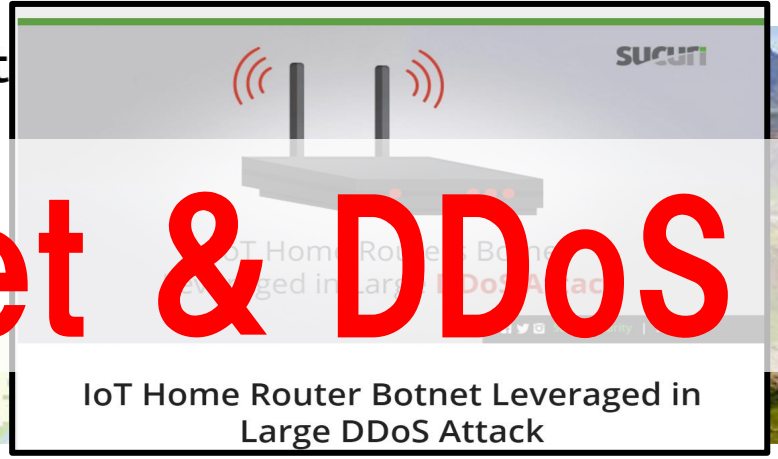
Insecure Cameras

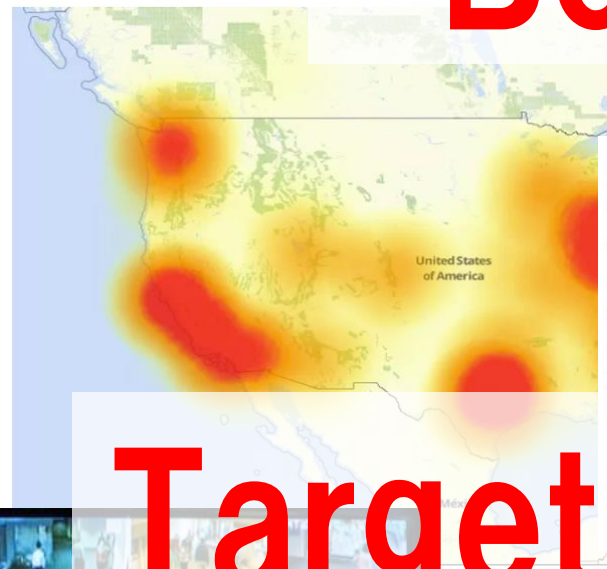
How an army of vulnerable gadget
web today

Malware known as Mirai is targeting the smart home

By Nick Statt | @nickstatt | Oct 21, 2016, 4:55pm EDT

SHARE



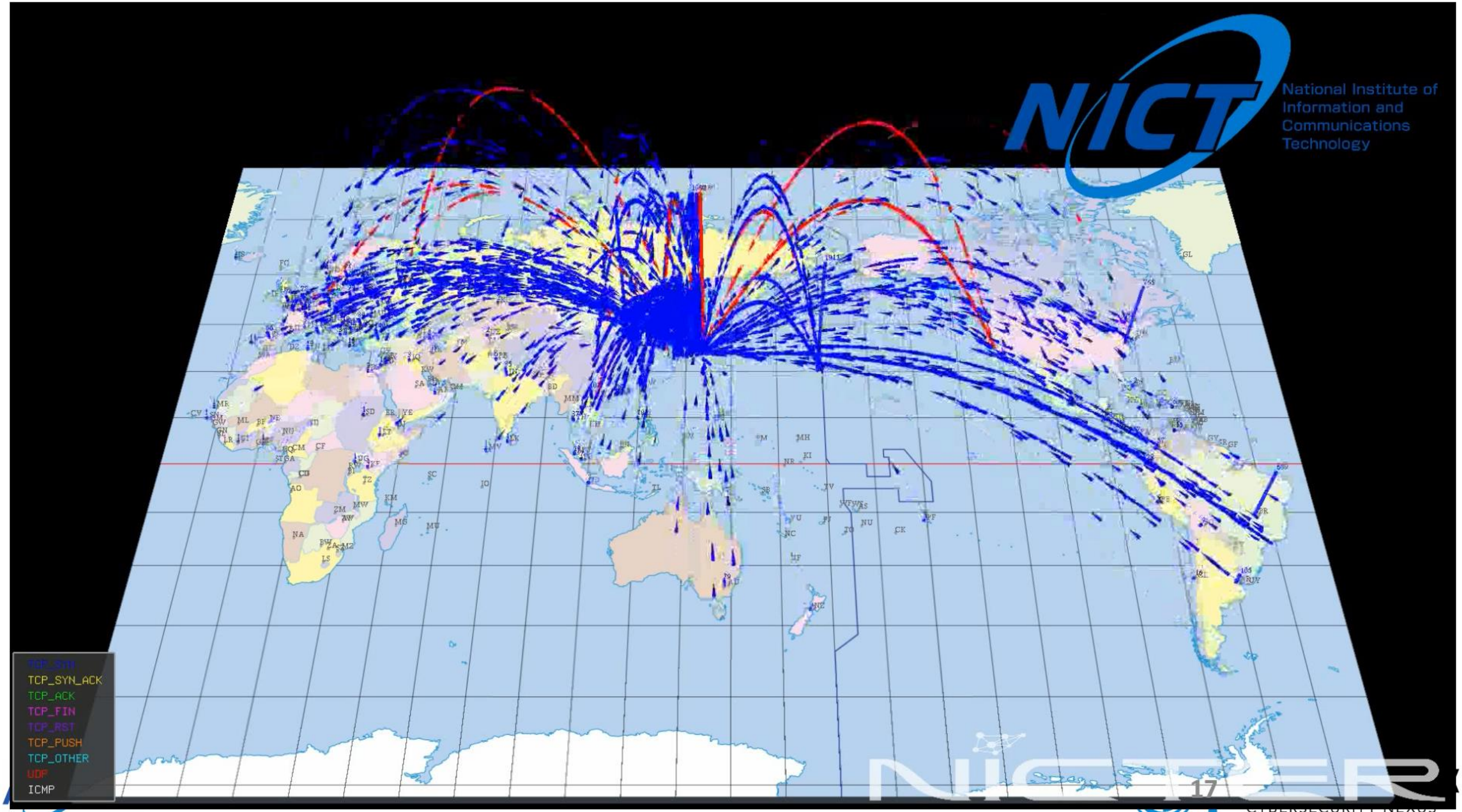


21 KrebsOnSecurity Hit With Record DDoS

SEP 16

On Tuesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual distributed denial-of-service (DDoS) attack designed to knock the site offline. The attack did not succeed thanks to the hard work of the engineers at **Akamai**, the company that protects my site from such digital sieges. But according to Akamai, it was nearly double the size of the largest attack they'd seen previously, and was among the biggest assaults the Internet has ever witnessed.

Industrial Control Systems


TCP_SYN
TCP_SYN_ACK
TCP_ACK
TCP_FIN
TCP_RST
TCP_PUSH
TCP_OTHER
UDP
ICMP

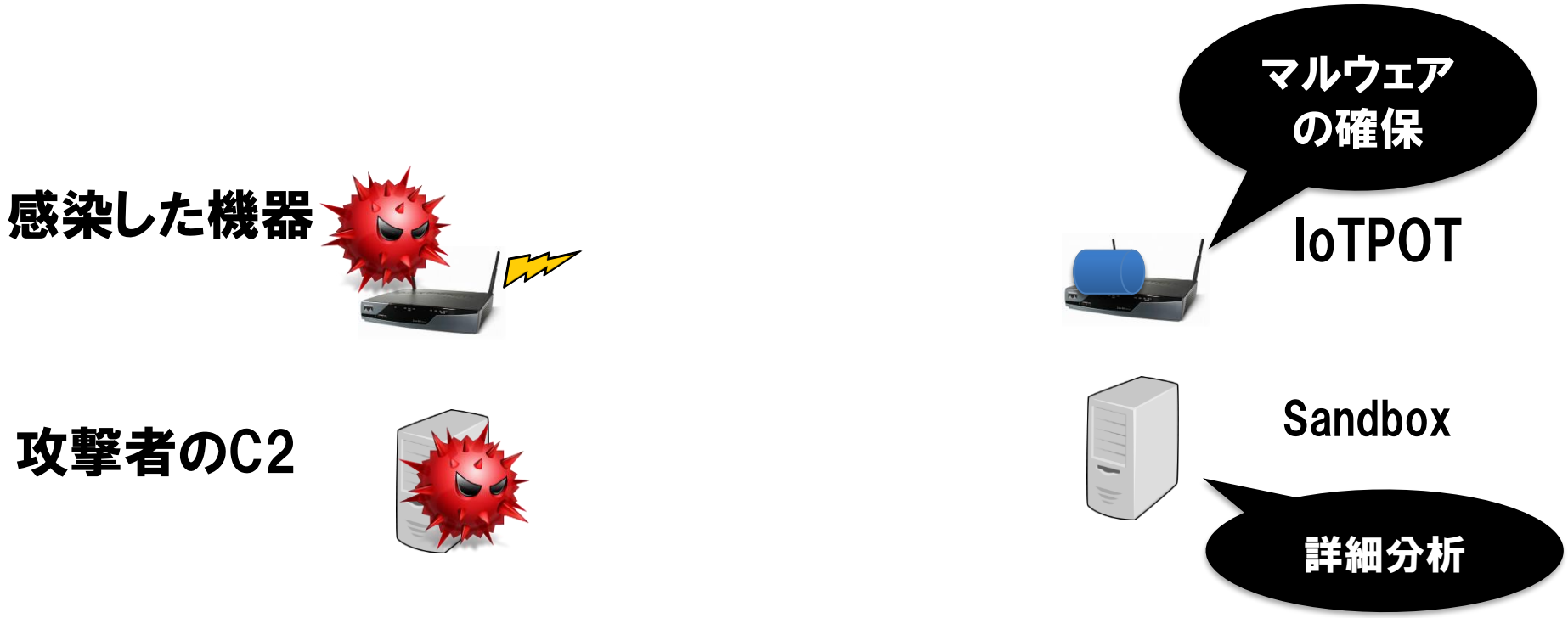
ROUTE CAUSES OF THE MASS-INFECTION（大量感染の原因）

Telnet

最近は、機器のぜい弱性をつく攻撃にシフトしてきている。

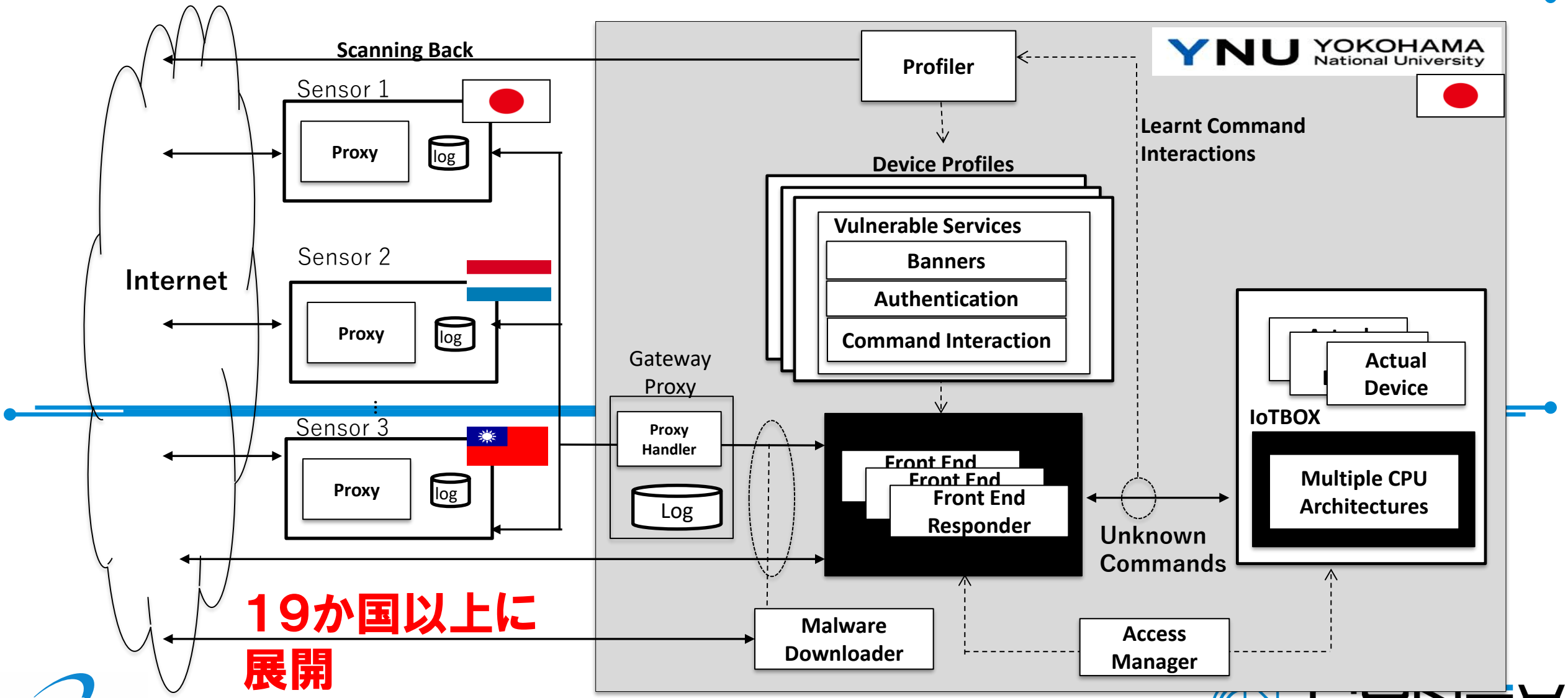
IoTPOT = IoT Honeypot

おとりシステム（ハニーポット）を使って脆弱なIoT機器をエミュレートし、攻撃を深く監視



Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, "IoTPOT: Analysing the Rise of IoT Compromises," USENIX WOOT 2015

IoTPoTのシステム体系



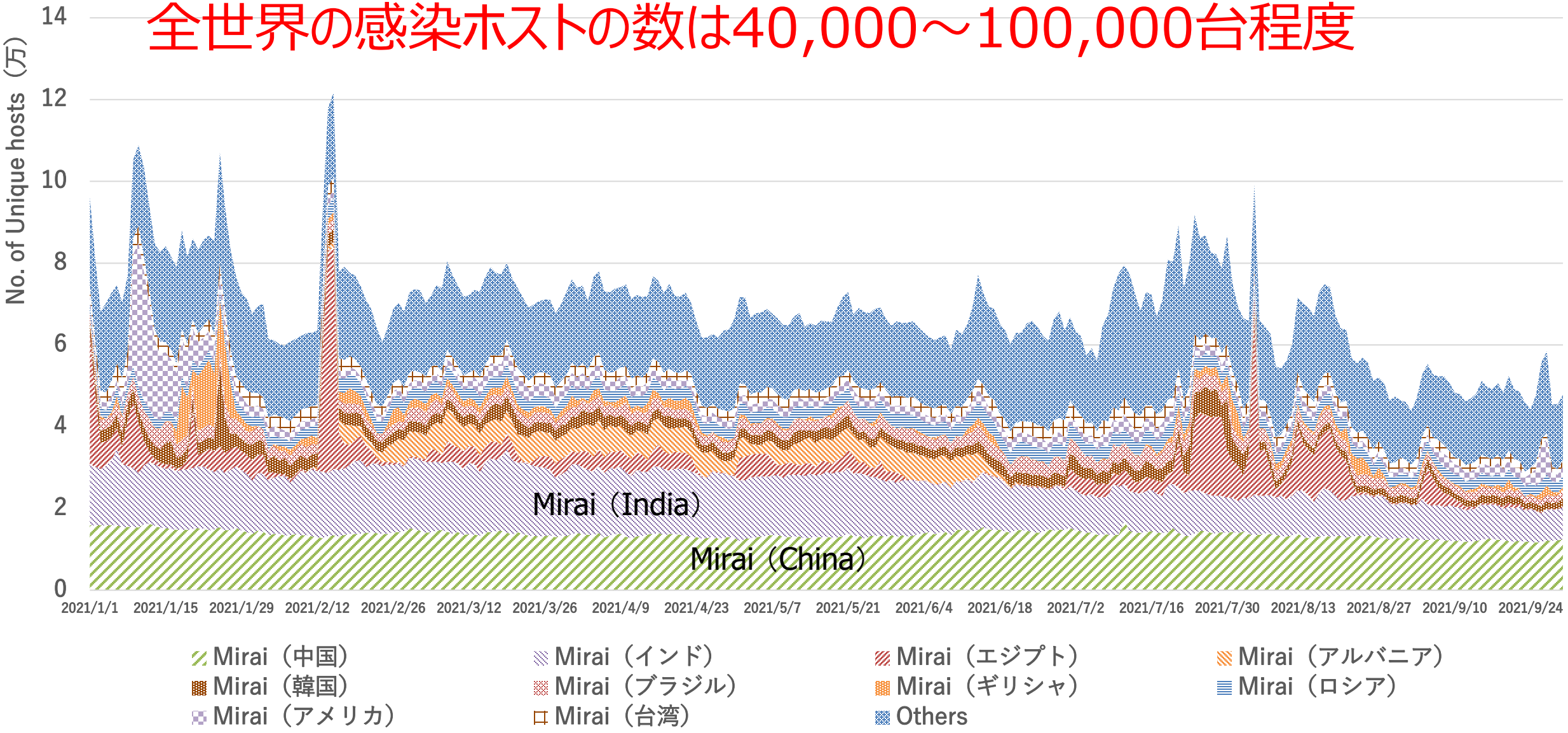
2016年の観測では

- IoTマルウェア「Mirai」がアウトブレーク
- 23/tcp、2323/tcpのdstポートが標的
- 6か月の観測で、60万台以上、500機種以上のIoT機器から攻撃
- 218か国からの攻撃、特にアジア圏からの攻撃が多い
- ベトナム、中国、ブラジルが最も感染しているとみられた
- Miraiのソースが公開ー公開後、感染活動が活性化
- Miraiがパンドラの箱を開けた
  - ✓ 多くの機器（ボットとして）操れる
  - ✓ システムに世界規模でダメージを与えられる
  - ✓ 攻撃者への気づきを誘発

IoTマルウェア： Mirai

- telnetサービスを使って500,000以上のIoT機器に感染 （2016年）
- 特徴は
  - 23/TCP，2323/TCPへスキャン
  - 辞書攻撃
  - スキャン先IPアドレスとTCPシーケンス番号が同一
  - 送信先，windowサイズ，送信ポートはランダム（多分）
- 2016年9月にAnna-senpaiと名乗る人物がHackforumsにソースコードを公開（その後GitHubにも公開）
- Anna-senpai：アニメ：「下ネタという概念が存在しない退屈な世界」（2015年7月より9月まで放送（東京MX等））

Miraiによる攻撃のトレンド（現在）



その後、IoTを用いた攻撃の多様化

- IoTマルウェア「Mirai」をベースとした亜種が急増
- Dstポートは、もはや23、2323だけではない－多様化
- モバイルルーターを狙った攻撃　（SSHを介した）
- マイクロコントローラのSDKの脆弱性を狙った攻撃
- 頻繁に使われるポートは10倍以上の種類に増加

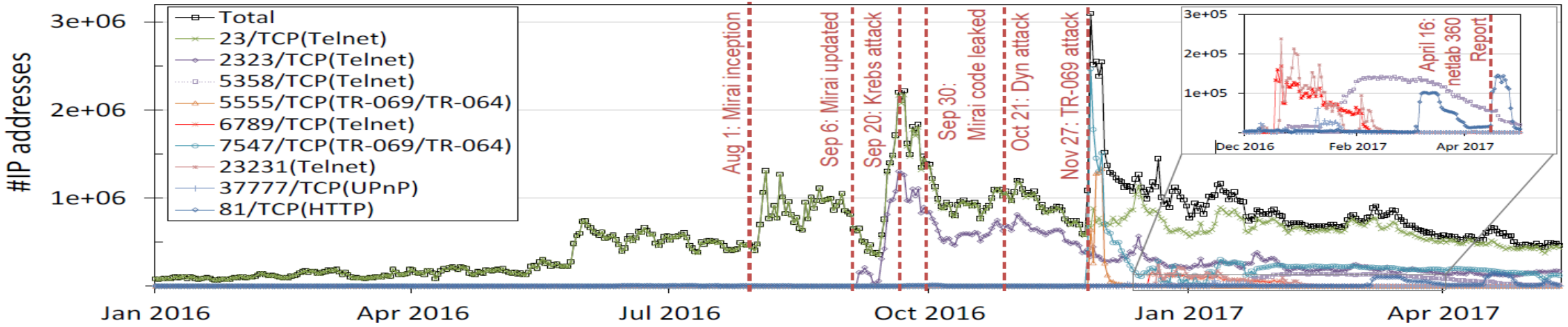
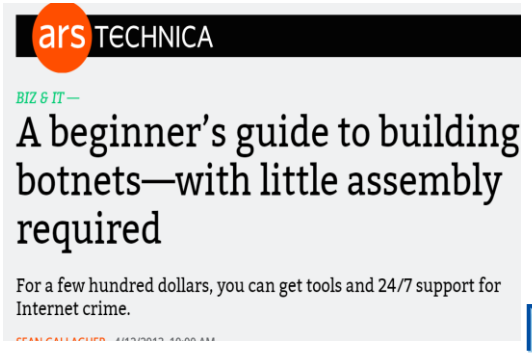


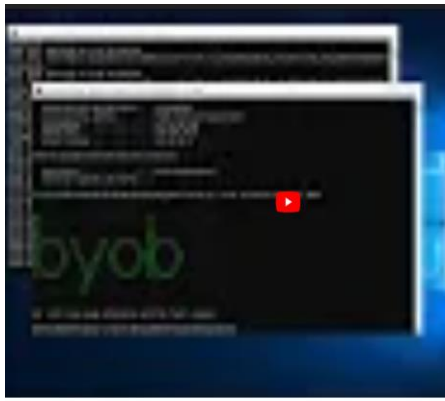
Figure 2: Number of scanning hosts captured via darknet

攻撃の一般化、高度化

- 攻撃基盤（インフラ）となるマルウェアDLサーバ、C2サーバは
  クラウドを使っていることが多いことが判明
- 50検体での分析では、1週間程度でインフラは使えない状況となる
- C2サーバ等のブラックリストを作成しても、有効性に乏しい
- 調査によると、攻撃者用のチュートリアル等が多い
  （BYOB：Build Your Own Botnet）
- 継続感染性をもつIoTマルウェア（VPNFILTER等）が発生

How to Turn a Router Into Part of a Botnet (Livestream)





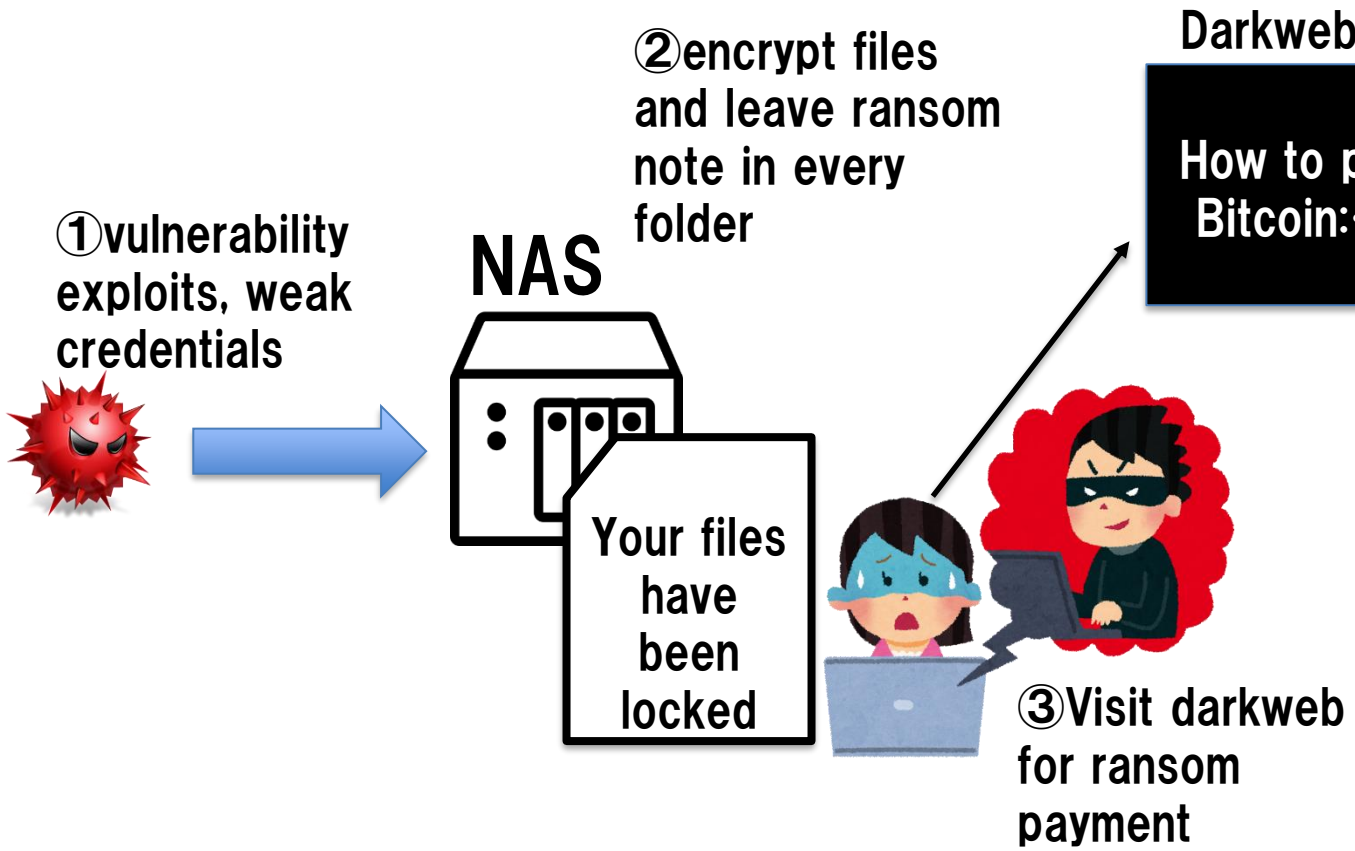
BYOB (Build Your Own Botnet) Test/Demo

持続感染性を保有する “VPNFILTER”の登場

https://blog.talosintelligence.com/2018/05/VPNFilter.html

IoTランサム攻撃

ベアメタルNAS（Network Attached Storage）ハニーポットを開発し、ランサム攻撃を観測した



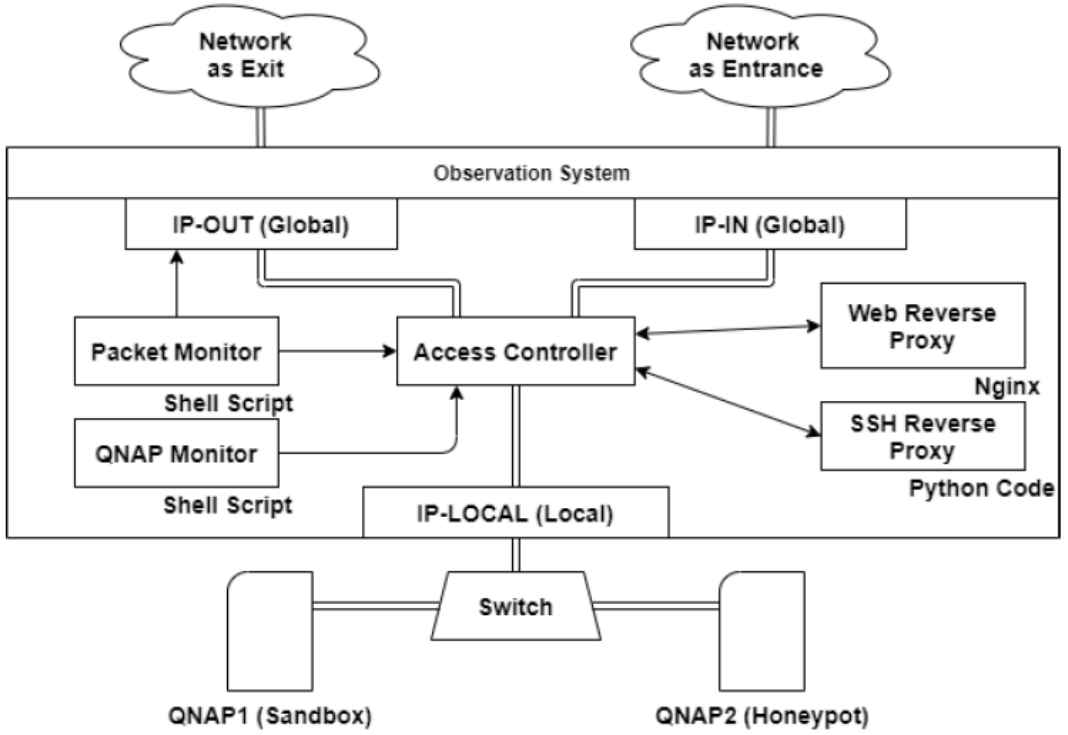


Fig. 1. Structure of SPOT

Ransom notes（ランサムノート）

ダークウェブの支払いの説明サイト

ランサムの支払いのために、どのように暗号資産を使うかの解説

IoT脅威の要約

- 安全性の低いIoTデバイスは、すでに何年も前から悪用されている。攻撃者は、IoT産業における多様性と複雑なサプライチェーンに起因するこの基本的な安全性の低さを認識しており、IoTを使ったこの攻撃傾向は今後も続くと思われる。
- 攻撃者の視点に立つと、IoT機器を構成するモジュールのぜい弱性や機器等の使用方法の問題により、攻撃者にとっては侵入しやすく、悪用しやすい攻撃対象となっているのが現状。
- IoTデバイスへのサイバー攻撃は、サイバー犯罪ビジネスの一部となっており、そして今後もその傾向は継続すると思われる。

IoTセキュリティ対策

１）ぜい弱なIoT機器、感染したIoT機器の探索とその対応

現在使用されているIoT機器のぜい弱な点（弱いID/PW等の使用等）やIoTマルウェアによる感染を受けているIoT機器を探索・把握し、それらに機器に対するセキュリティ対策を講じる方法

２） IoT機器のサイバーセキュリティラベリングによるIoT機器の健全化

これから販売され市場にでてくるIoT機器のセキュリティ・プライバシーを確保するため、IoT機器のセキュリティ・プライバシーを保証する仕組み（IoT機器のサイバーセキュリティラベリング）を構築する方法

特に、後者については、国際標準化とも強く関係し、英国、ドイツ、シンガポール、米国などで当該の仕組みが活発に議論されており、日本においても、経済産業省において「IoTセキュリティ適合性評価制度」のための検討が開始され、国際標準化活動に沿った形で制度設計がほぼ完成している段階

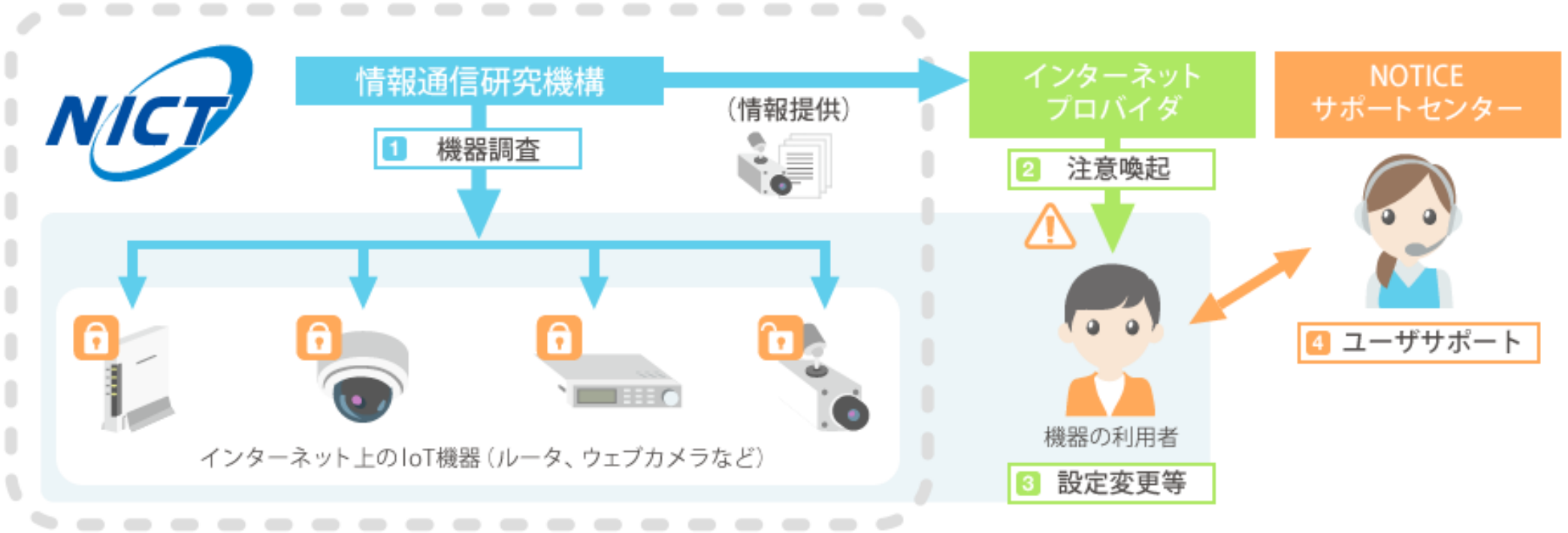
ぜい弱なIoT機器、感染したIoT機器の探索とその対応

－　IoTセキュリティのためのNOTICEとNICTER　総務省施策　－

NOTICE
National Operation Towards IoT Clean Environment

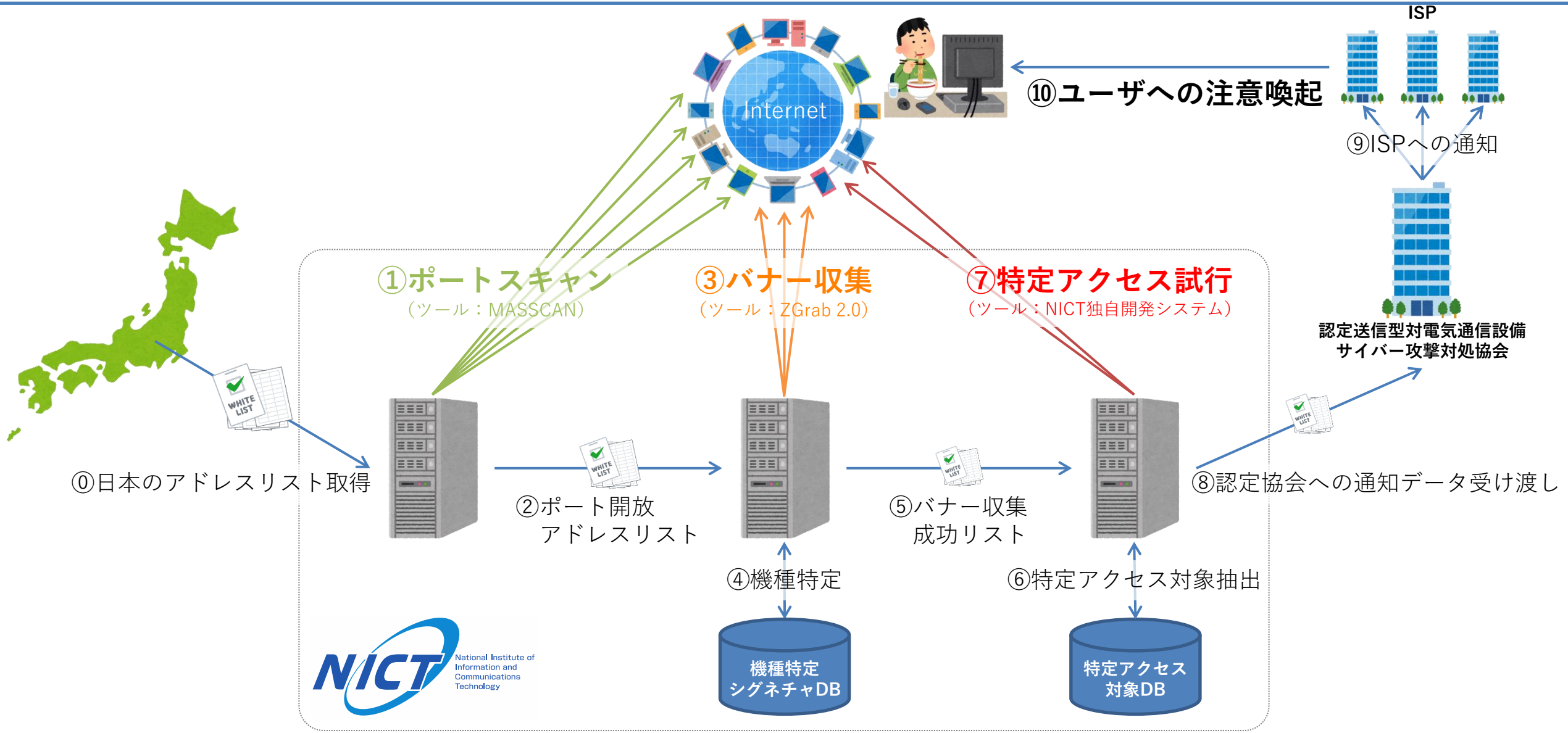
NOTICE

- **NOTICE: National Operation Towards IoT Clean Environment**
- 総務省、NICT、ISPが連携し、サイバー攻撃に悪用されるおそれのある機器の調査及び当該機器の利用者への注意喚起を行う取組



https://notice.go.jp/

NICTによるIoT機器調査の技術詳細



能動的対策と受動的対策

能動的対策

パスワード設定等に
不備があるIoT機器

能動的観測

NOTICE
National Operation Towards IoT Clean Environment

通知

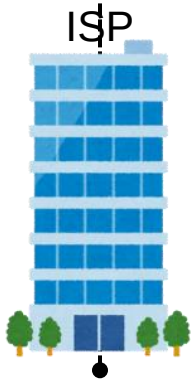
受動的対策

感染IoT機器

受動的観測

NICTER

通知



ISP

NOTICE　10月期の観測分析結果（概要）

https://notice.go.jp/status

- **IoT機器観測状況　：　IoT機器観測総数　　月1.25億件**
- **容易に推測可能なID･パスワードであるIoT機器　：　月15,794件**（ルータ等　57.83%、ネットワークカメラ等　8.97%、その他機種　3.33%、　機種不明　29.87%）＜容易に推測可能なIDやパスワードを使用しているため、攻撃者によって管理権限を乗っ取られたり、サイバー攻撃に加担させられる危険性がある機器＞
- **ファームウェアに高リスク脆弱性を有するIoT機器：　月4891件**　＜第三者に不正利用される危険性があるファームウェア脆弱性を有するIoT機器＞
- **マルウェア感染　IoT機器検知数：　最大990件/日**　＜ Miraiに既に感染していると推定されるIoT機器。サイバー攻撃に加担させられている可能性がある＞

METI
Ministry of Economy, Trade and Industry

IoT機器のサイバーセキュリティラベリングによるIoT機器の健全化

－ 日本におけるIoT機器の認証制度の設計 －

Ministry of Economy, Trade and Industry of Japan

（経済産業省）

NICT National Institute of Information and Communications Technology

本セミナーの構成

講演とパネル：講演の部

講演１：IoT製品に対するセキュリティ適合性評価制度の紹介

木本 達也 氏　（経済産業省）

講演２：ISO/IEC JTC1/SC41の動向

河合 和哉 氏（産業技術総合研究所)

講演３： ISO/IEC JTC1/SC27の動向

中尾康二　（情報通信研究機構）

講演４： IETFでも議論されるConstrained IoTデバイスのファームウェア
アップデート

髙山 献 氏（セコム株式会社）

講演とパネル：パネルの部

パネリスト：

- 木本 達也 氏　（経済産業省）
- 荻野　司 氏（一般社団法人 重要生活機器連携セキュリティ協議会　代表理事）
- 髙山 献 氏（セコム株式会社）
- 松本　泰　（JNSAフェロー）

モデレータ：中尾康二

内容：パネルの前の講演内容、及びパネルの中でもIoTに関する多くの知見をお持ちの専門家からご発表をいただき、IoTのセキュリティに関する現状や標準化の課題を見据えた上で、今後のIoTセキュリティの強化に向けた活動の方向性やIoTに関わる国際標準化の活用に関するビジョン（方法論等）につき意見交換を行う。

Approach to global standardization of IoT security

ISO/IEC JTC1/SC27
27400, 27402 (FDIS), and 27404 (WD)

US – CTIA
IoT Cybersecurity Certification,
SP 800-213(NIST)
IoT Device Cybersecurity Guidance for the Federal Government

Common parts
- Terminologies
- Reference Architecture
- Use Cases
- Certification Framework

- Risk Analysis
- Security/Privacy Controls

UK – IASME IoT Cyber Scheme, etc
EU – ETSI, Cyber Security for Consumer IoT: Baseline Req. EN 303 645
EU – ENISA Cybersecurity Certification - EUCC Candidate Scheme

Japan – CPSF (METI), Device Requirements (MIC), IoT device Certification Scheme (under study), etc.