資料37－3

Institute of Advanced Sciences
Yokohama National University

YNU YOKOHAMA National University

IoTにおけるサイバー攻撃の動向とその対策に向けて

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　准教授
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　招聘専門員

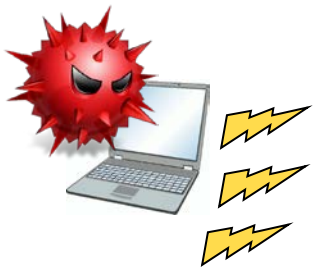
IPネットワーク設備委員会（2018.3.30）

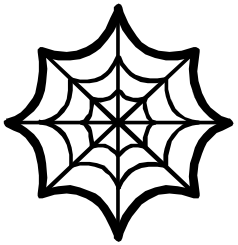
ご説明の流れ

- **マルウェア感染したIoT機器からのサイバー攻撃の観測状況**
- **感染が疑われるIoT機器について**
- **サイバー攻撃により乗っ取られるリスクが大きい機器について**
- **IoT機器への対策について**

参考：ダークネットによる攻撃の観測

ダークネット：パソコンや機器等のエンドホストが接続されていない未使用のIPアドレス帯





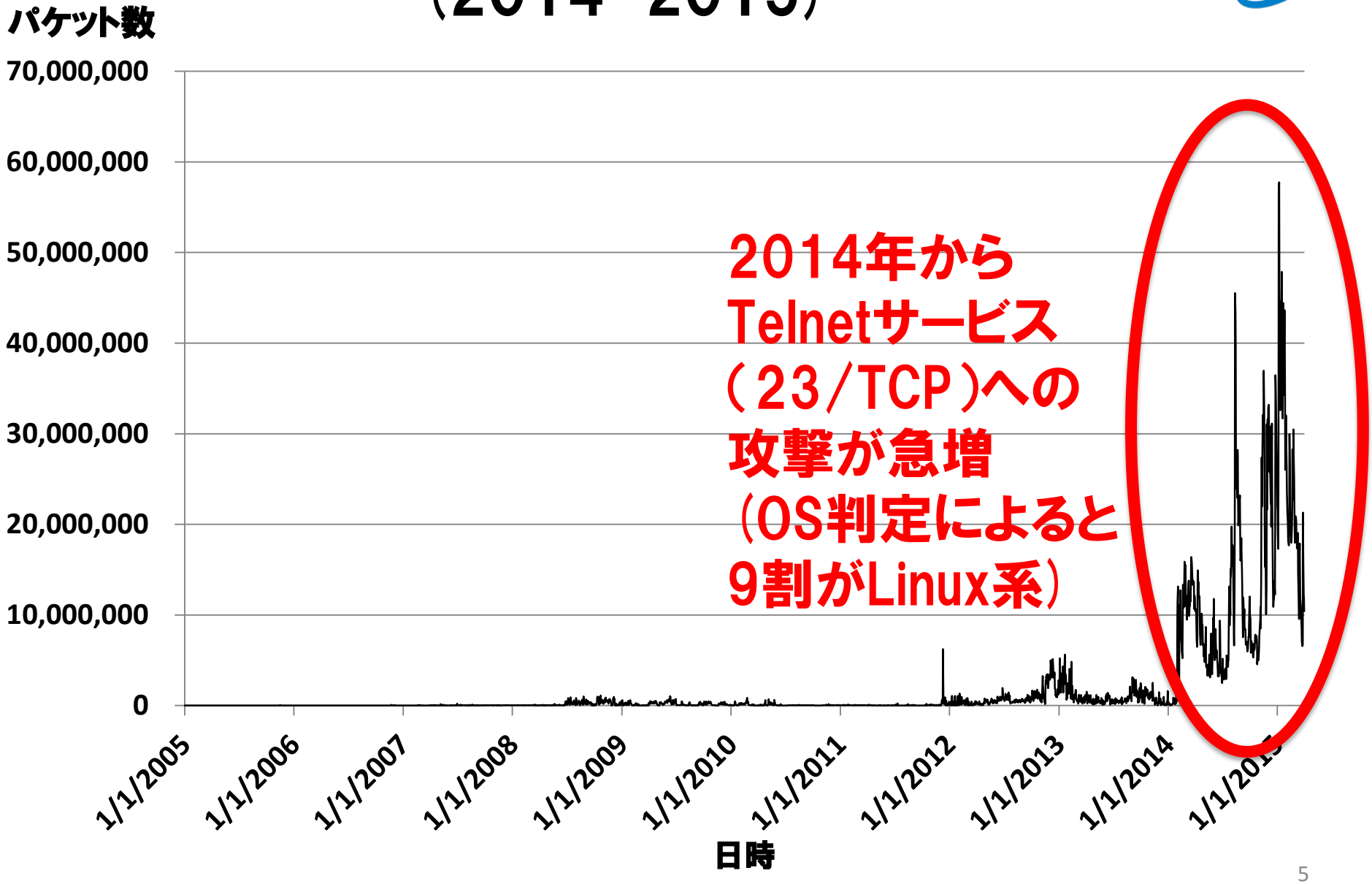
ダークネット

- マルウェア（不正プログラム）に感染して外部に無作為に攻撃を行っているパソコン、デバイスからの攻撃の観測に有効
- 全ポート観測が可能であるため**様々なネットワークサービスへの攻撃**の概況を観測するのに適している

参考：ハニーポットによる攻撃の観測とマルウェアの捕獲・詳細分析

ハニーポット：脆弱な機器を模擬したおとりシステム．攻撃を受けつつ観測を行うため、観測されたアクセスが調査ではなく**攻撃であることが確定的**に判別できる．マルウェア捕獲し、詳細分析が可能．
（一方、観測対象でないサービスへの攻撃は観測できない）

Telnetを狙ったIoT機器への攻撃の勃興 (2014-2015)



情報通信研究機構NICTERにおける2005年から10年間の観測結果(23/tcpのみ)

Telnetを狙ったIoT機器への攻撃の勃興 (2014-2015)

パケット数

TCP 宛先ポート別パケット数 Top 10

宛先ポート	パケット数	割合
23	2,699,639	45%
22	461,738	8%
[illegible]	[illegible]	6%
1433	208,460	3%
[illegible]	[illegible]	3%
[illegible]	[illegible]	3%
8080	145,657	2%
[illegible]	[illegible]	2%
9200	116,255	2%
25	94,901	2%

観測される攻撃パケットの約4～5割がTelnet狙い

TCP 宛先ポート別パケット数 Top 10

宛先ポート	パケット数	割合
23	11,727,894	65%
1433	791,485	4%
22	559,059	3%
3389	247,547	1%
80	247,159	1%
8080	184,132	1%
443	147,434	1%
3306	128,382	1%
4028	116,029	1%
54628	78,378	0%

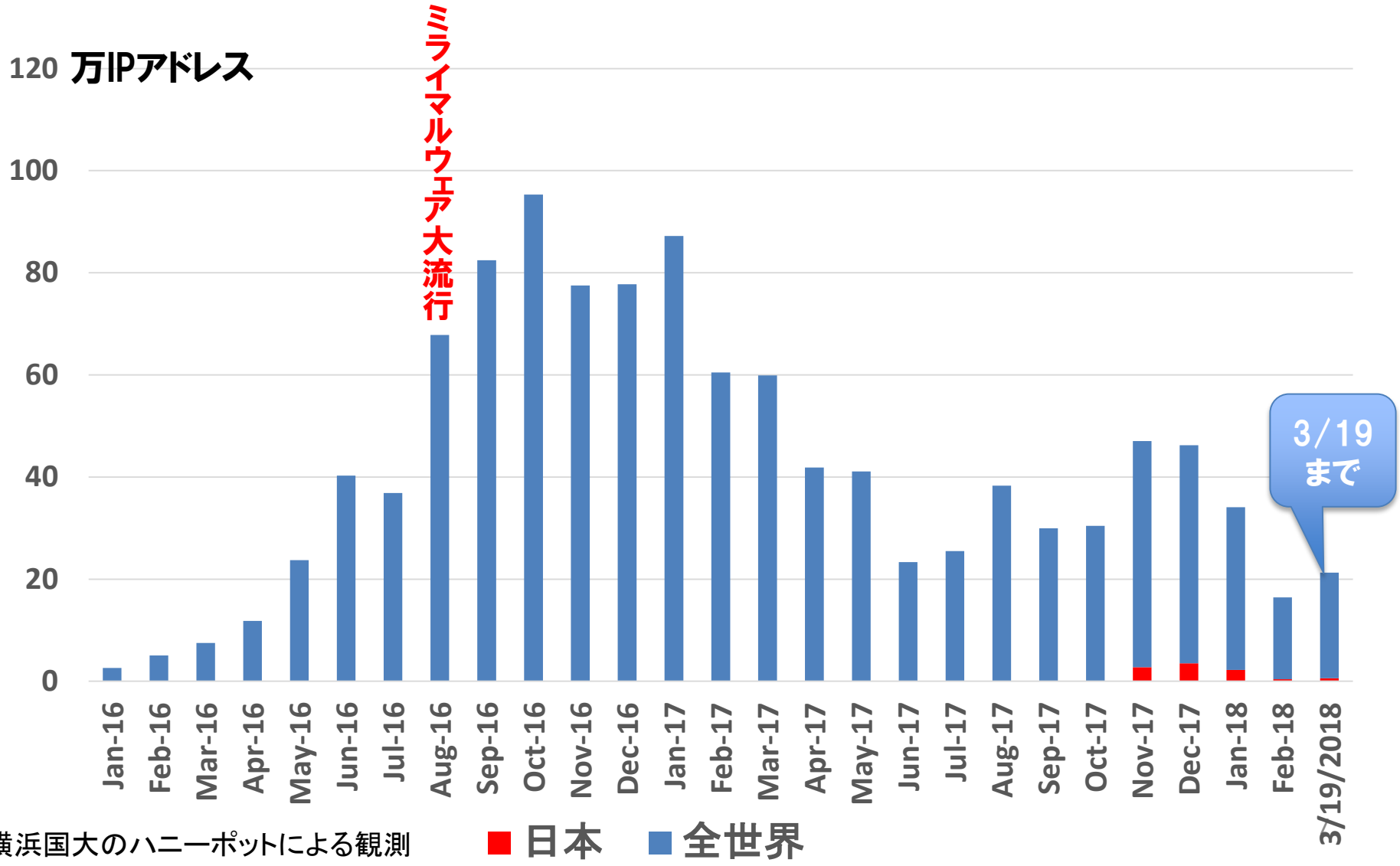
7 6 5 4 3 2 1

1/1/2005 1/1/2006 1/1/2007 1/1/2008 1/1/2009

日時

情報通信研究機構NICTERにおける2005年から10年間の観測結果 (23/tcpのみ)

Telnetを狙った攻撃の全盛と ミライマルウェアの大流行（2016-2017前半）



横浜国大のハニーポットによる観測

攻撃の多様化（2017-現在）

- Telnet以外のサービスの脆弱性やデフォルトポート以外で動作するTelnetが次々に標的に.
- **攻撃の多様化により国内機器の大量感染**事例が発生.

横浜国立大学、NICT、ドイツ・ザールラント大学、オランダ・デルフト工科大学共同研究成果

攻撃の多様化（2017-現在）

2018/03/25のデータを表示中

TCP 宛先ポート別ユニークホスト数 Top 10

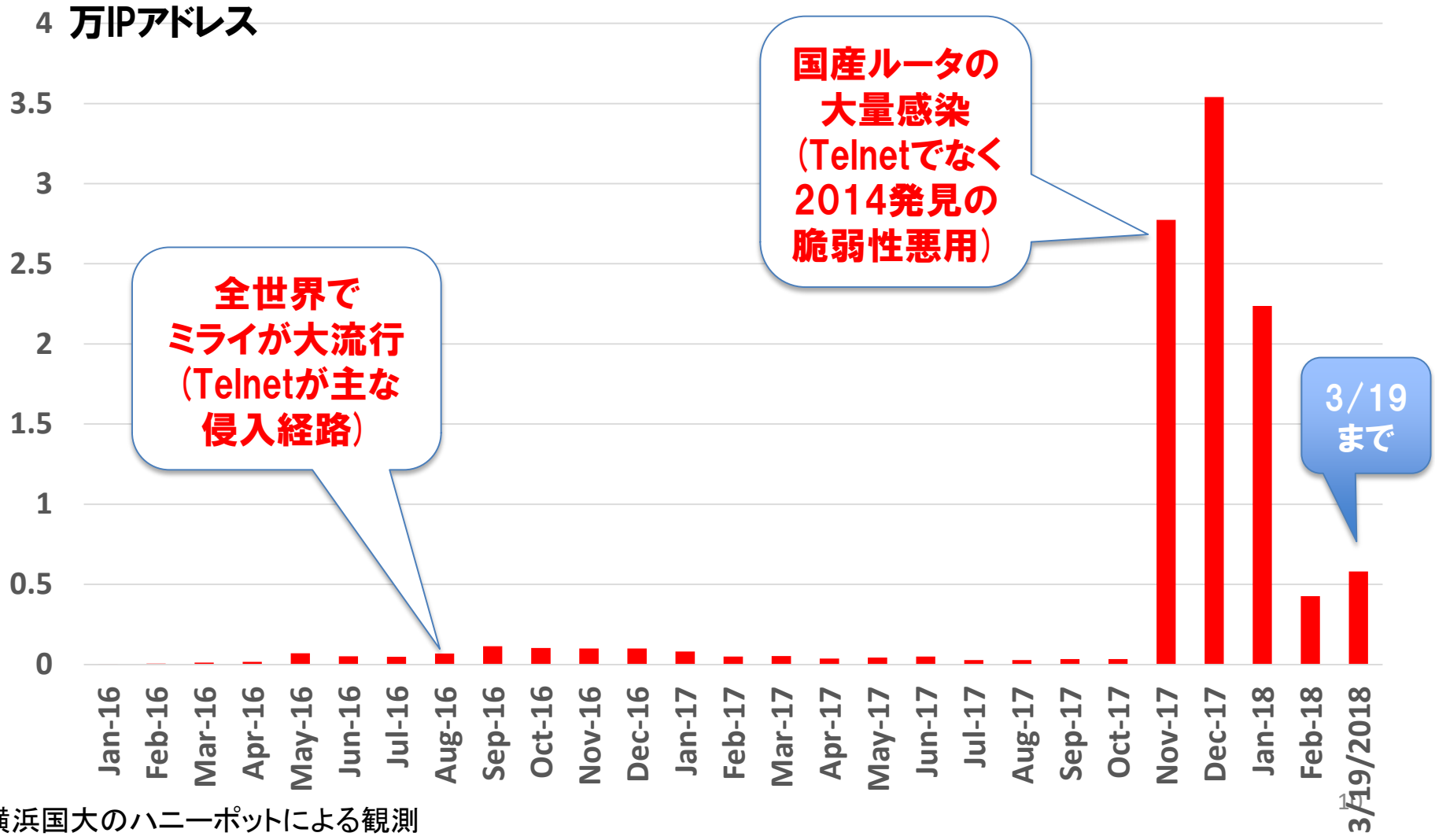
宛先ポート	ホスト数	割合
23	518,142	23%
8291	339,314	15%
445	106,734	5%
2323	21,074	1%
81	10,655	< 1%
80	10,245	< 1%
5555	8,824	< 1%
3389	8,392	< 1%
443	7,883	< 1%
1433	5,957	< 1%

Telnetの占有率が低下

- Telnet以外のサービスの脆弱性
  動作するTelnetが次々に標的
- 攻撃の多様化により国内機器

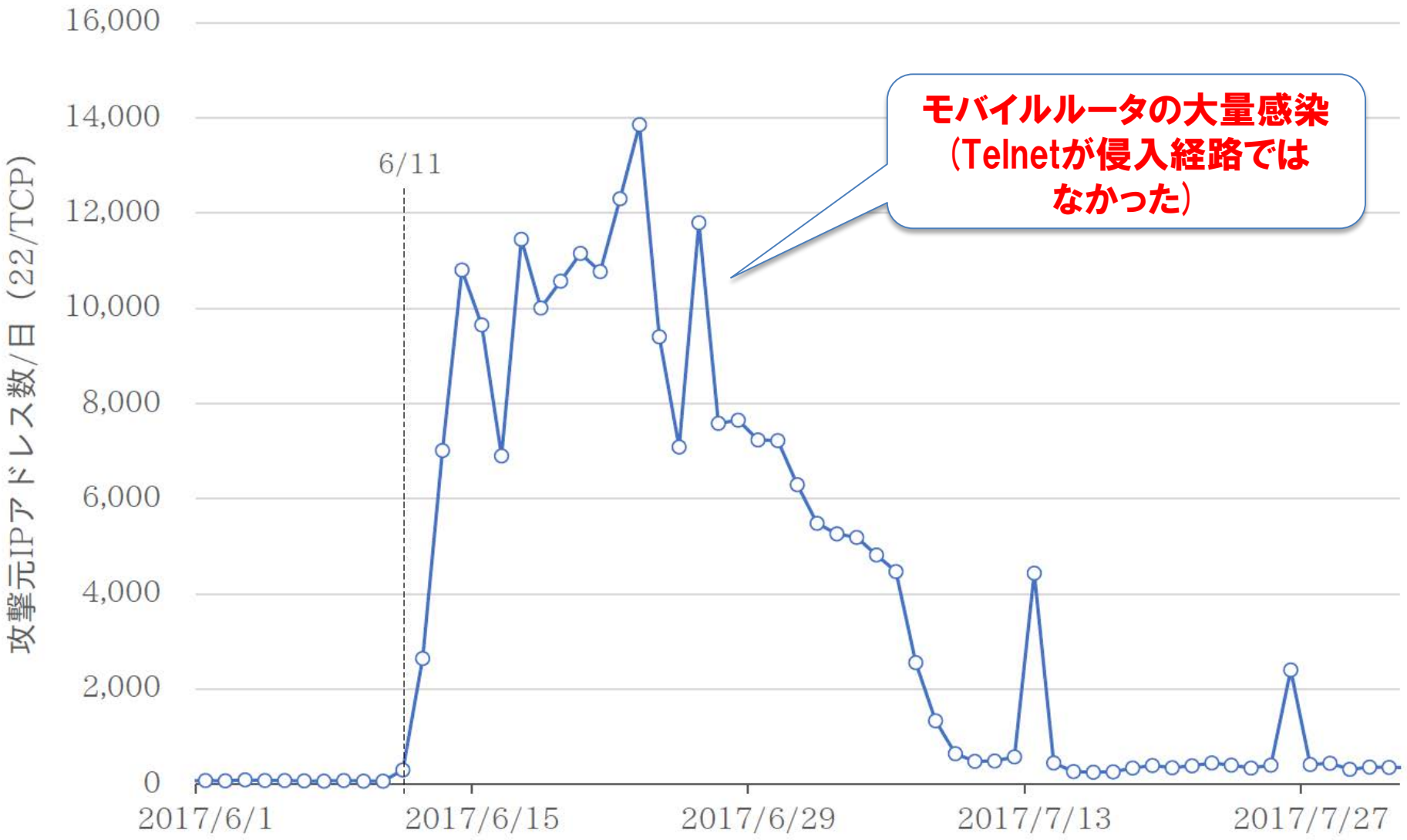
横浜国立大学、NICT、ドイツ・ザールラント大学、オランダ・デルフト工科大学共同研究成果

攻撃の多様化による国内感染機器の急増（2017-現在）



横浜国大のハニーポットによる観測

国内感染機器が急増した事例（2017/6-7）



「NICTER観測レポート2017」より

管理画面（WebUI）を経由した攻撃の観測

機器名	メーカ国/地域	認証方法	ID/Password	観測期間	観測日数
IPカメラA	日本	ベーシック認証 ダイジェスト認証	xxx/xxx	2016/12/16～2017/8/16	244日
IPカメラB	台湾	ベーシック認証	xxx/xxx	2016/11/30～2017/8/16	260日
ルータC	台湾	ベーシック認証	xxx/xxx	2016/11/30～2017/3/8 2017/4/12～2017/8/16	226日
ルータD	台湾	ベーシック認証	xxx/xxx	2016/12/16～2017/2/5 2017/2/23～2017/3/3 2017/4/12～2017/5/3	83日
ルータE	台湾	フォーム認証	xxx/xxx	2016/12/16～2017/1/27 2017/2/22～2017/3/7 2017/4/12～2017/7/17	154日
ポケットルータF	日本	フォーム認証	xxx/xxx	2016/11/30～2016/11/30 2016/12/5～2017/3/1	88日
ポケットルータG	アメリカ	フォーム認証	xxx/xxx	2016/12/16～2017/8/16	244日
プリンタH	アメリカ	なし	なし	2016/11/30～2017/3/1 2017/6/24～2017/8/16	146日
放送受信機I	ドイツ	なし	なし	2016/12/9～2017/2/11 2017/2/22～2017/3/1 2017/6/24～2017/7/26	106日

各機器に10IPを割り当てた。外部からアクセス可能なように、ルータでは**ファイヤーウォール**を**無効**にし、ログイン認証がある機器は**初期パスワード**から**変更しない**。なお、ルータCでは非公式のカスタムファームウェアを使用した。

横浜国大のハニーポットによる観測

※ポケットルーター：持ち運びが容易でルータとして機能する機器

管理画面（WebUI）を経由した攻撃の観測

機器名	リクエスト ホスト数	ログイン試行 ホスト数	ログイン成功 ホスト数	特定機器へのアクセスホスト数
IPカメラA	8695	222	26	25
IPカメラB	10426	239	19	12
ルータC	6661	298	103	79
ルータD	3359	105	51	38
ルータE	5469	8	8	11
ポケットルータF	2769	0	0	0
ポケットルータG	8724	36	6	12
プリンタH	3876			0
放送受信機I	3299			17

横浜国大のハニーポットによる観測

観測した攻撃内容と推定される目的

機器名	リクエストホスト数	特定機器へのアクセスホスト数	情報搾取			設定変更				
			設定情報自動取得	映像	保存データリスト	VPNサーバ	VPNクライアント	FW有効化	DDNS	DNS
IPカメラA	8695	25		25						
IPカメラB	10426	12	11	1						
ルータC	6661	79	25			17	5	2	4	(2)
ルータD	3359	38	9			7			2	(2)
ルータE	5469	11						1		2
ポケットルータF	2769	0								
ポケットルータG	8724	12			4					
プリンタH	3876	0								
放送受信機I	3299	17								

踏み台独占

覗き見 情報漏えい

偵察・情報収集

踏み台化

情報漏えい

情報漏えい 悪性サイト等への誘導

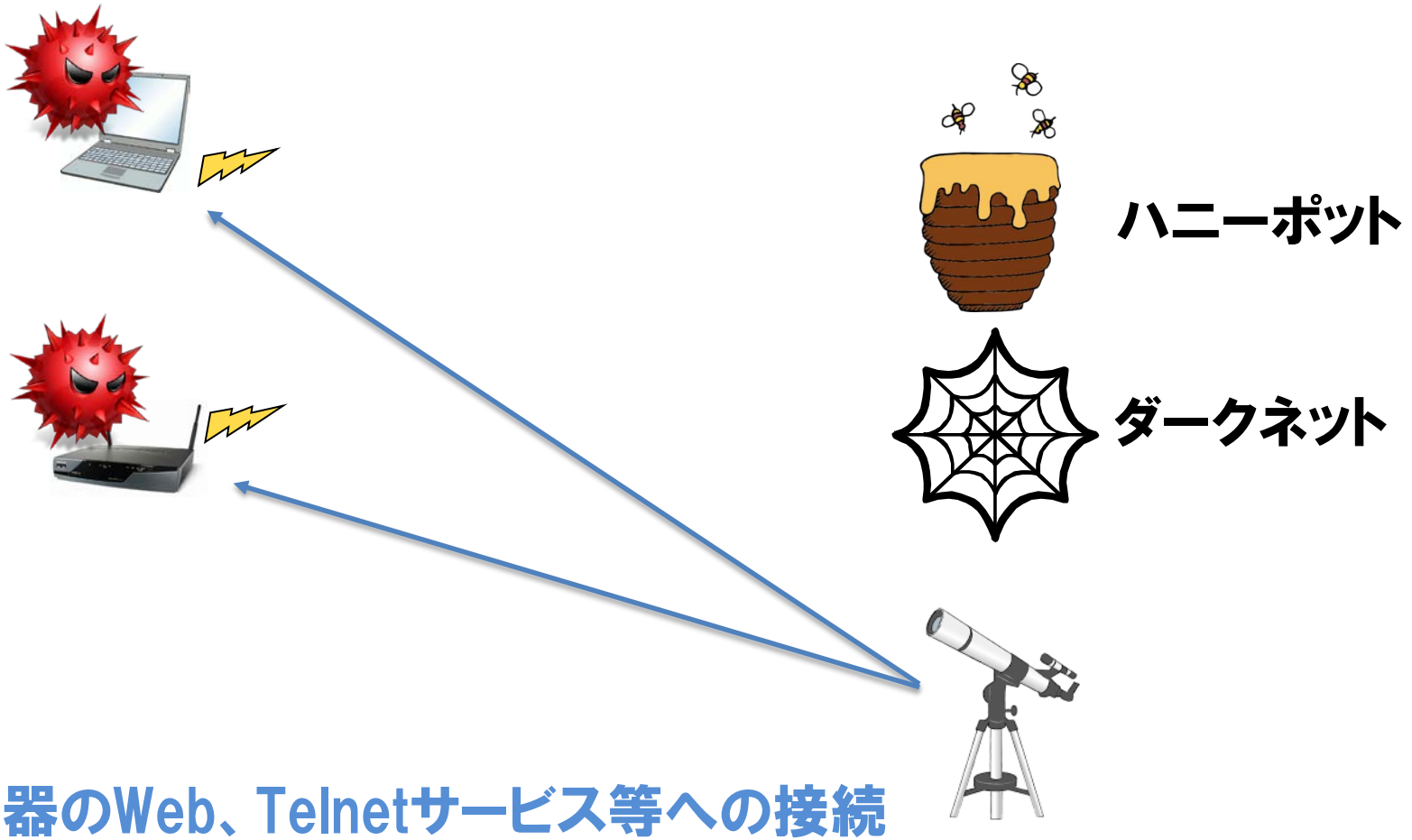
※設定情報自動取得:自動化された特定の流れで設定情報を取得する攻撃を行うホスト数
FW有効化:ファイヤーウォールの有効化を行うホスト数
DDNS:動的に割り当てられるIPアドレスとそのホスト名の対応を、登録管理する仕組みであるDynamic Domain Name Systemの設定変更を行うホスト数

横浜国大のハニーポットによる観測

ご説明の流れ

- マルウェア感染したIoT機器からのサイバー攻撃の観測状況
- **感染が疑われるIoT機器について**
- **サイバー攻撃により乗っ取られるリスクが大きい機器について**
- **IoT機器への対策について**

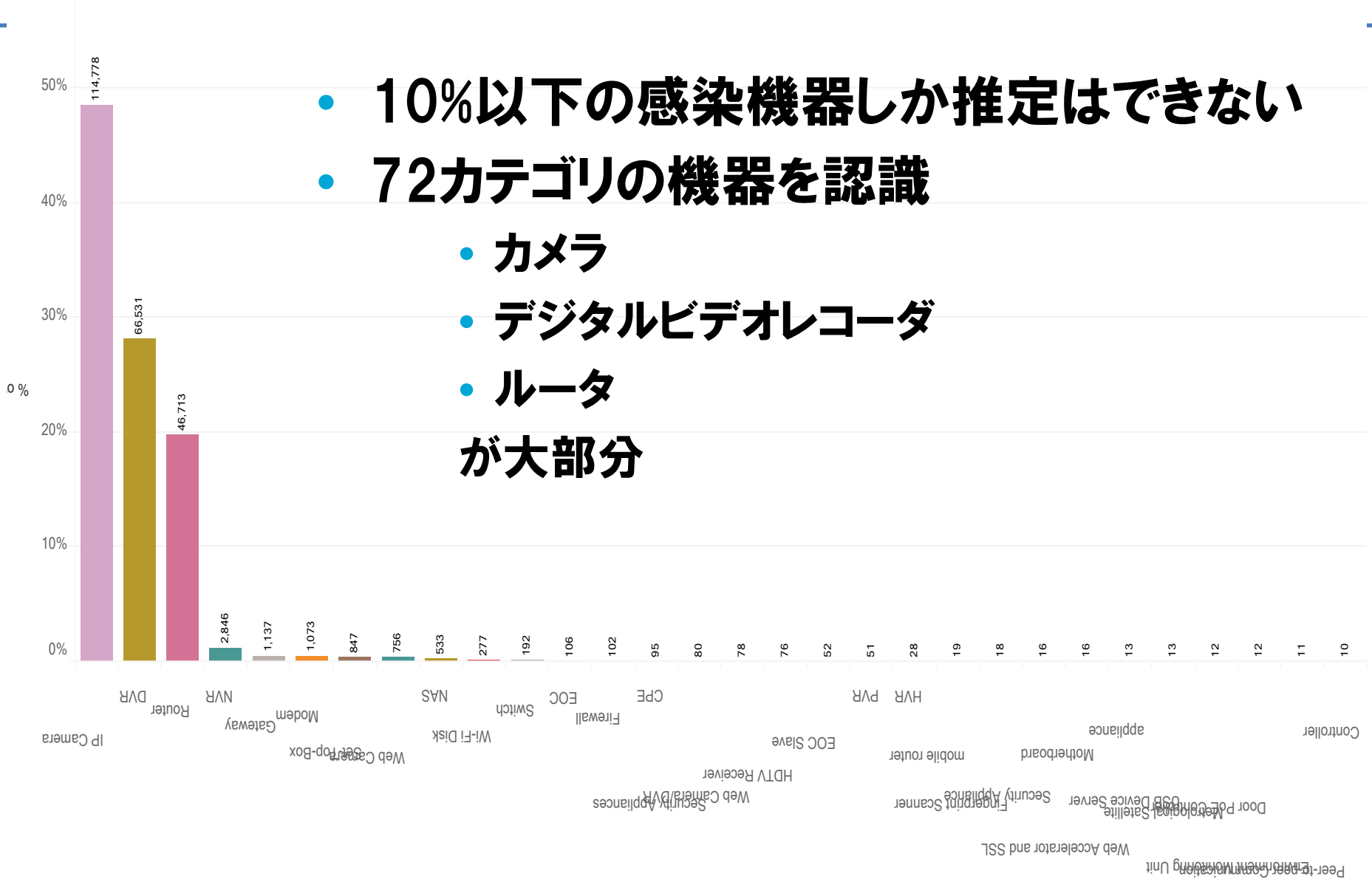
参考：スキャンによる攻撃元機器の推定



攻撃元機器のWeb、Telnetサービス等への接続

→特徴的な応答から機器を推定

ハニーポットで観測された感染機器の種類



- 10%以下の感染機器しか推定はできない
- 72カテゴリの機器を認識
  - カメラ
  - デジタルビデオレコーダ
  - ルータ

  が大部分

感染機器の種別

- 監視カメラ等
  - IP カメラ
  - デジタルビデオレコーダ
- ネットワーク機器
  - ルータ・ゲートウェイ
  - モデム、ブリッジ
  - 無線ルータ
  - ネットワークストレージ
  - セキュリティアプライアンス
- 電話関連機器
  - VoIPゲートウェイ
  - IP電話
  - GSMルータ
  - アナログ電話アダプタ
- インフラ
  - 電力制御システム
  - LEDディスプレイ制御システム
  - 医療機器(MRI)
  - 指紋スキャナ
- 制御システム
  - ソリッドステートレコーダ
  - インターネット接続モジュール
  - センサ監視装置
  - ビル制御システム
- 家庭・個人向け
  - Webカメラ、ビデオレコーダ
  - ホームオートメーションGW
  - 太陽光発電管理システム
  - 電力需要監視システム
- 放送関連機器
  - 映像配信システム
  - デジタル音声レコーダ
  - ビデオエンコーダ/デコーダ
  - セットトップボックス・アンテナ
- その他
  - ポンプ
  - 火災報知システム
  - 大容量記憶装置

海外製品が多い．国産製品でもファームウェアは海外で開発されているケースが多い．

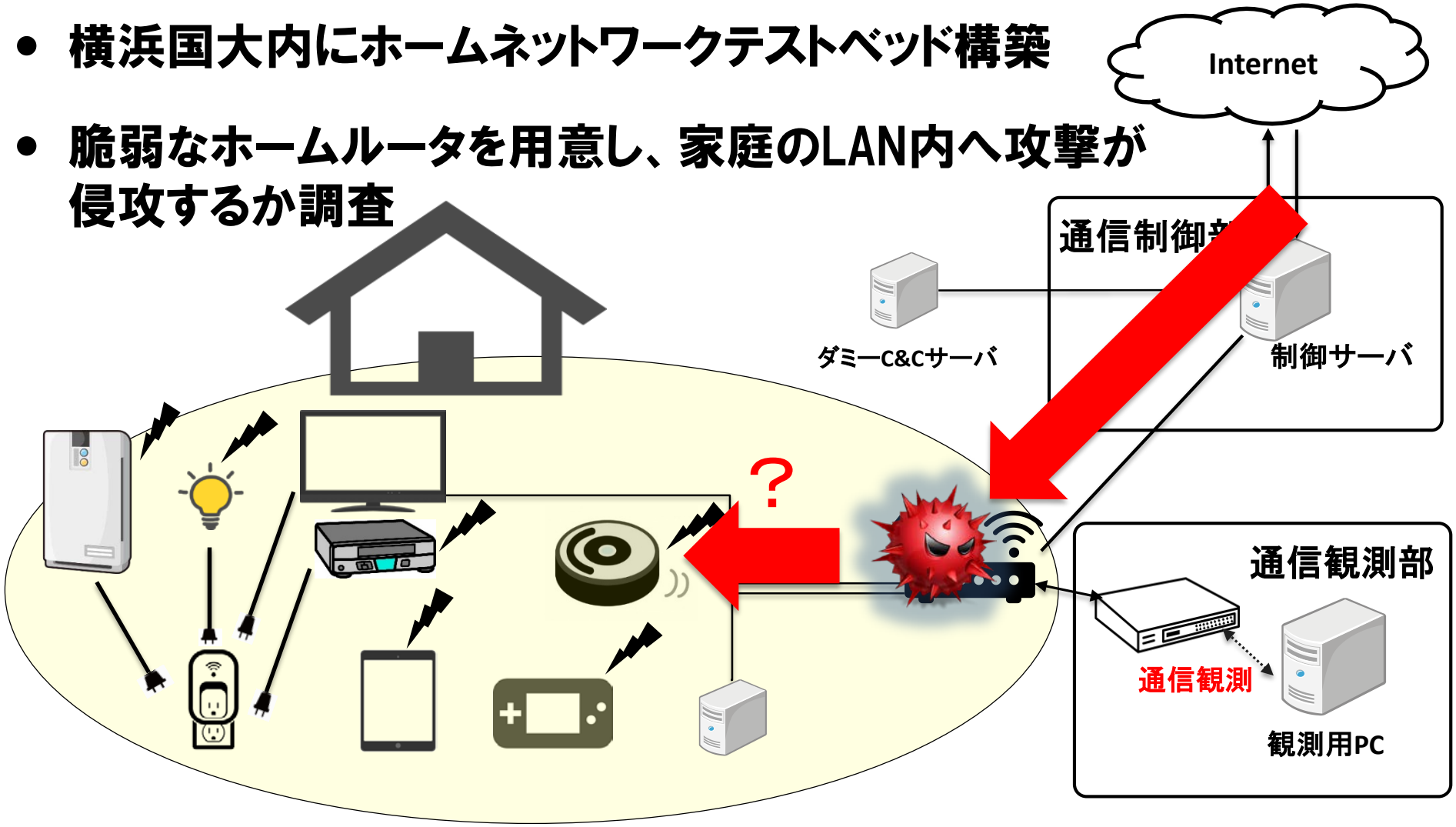
デバイスはWebおよびTelnetの応答から判断しています．

ご説明の流れ

- マルウェア感染したIoT機器からのサイバー攻撃の観測状況
- 感染が疑われるIoT機器について
- **サイバー攻撃により乗っ取られるリスクが大きい機器について**
- **IoT機器への対策について**

参考：ホームネットワークテストベッドによる実攻撃の引き込み実験

- 横浜国大内にホームネットワークテストベッド構築
- 脆弱なホームルータを用意し、家庭のLAN内へ攻撃が侵攻するか調査



横浜国大とBBSS社の共同研究成果

参考：ホームネットワークテストベッドによる実攻撃の引き込み実験

横浜国大とBBSS社の共同研究成果

家庭内（LAN側）への攻撃の調査

- 2016/12/20～2017/11/30の期間でIoTハニーポットで収集した6859検体（MIPS：3000検体，MIPSEL:3859検体）でLAN側への攻撃を行うものが存在するか調査

CPU	総数	LAN側へ攻撃
MIPS	3000検体	90検体（3%）
MIPSEL	3859検体	199検体（5%）

- LAN側へ攻撃を行う検体は全体の3～5％程度だった
- 脆弱なホームルータを設置し、1週間に渡り観測（ルータは数分で感染するため15分おきに再起動）したが、LAN側への攻撃は観測されなかった

→現在はグローバルIPアドレスを有する機器へのインターネット側からの直接的攻撃が主流と考えられる．ただし、UPnPによりルータにポートフォーワード設定する機器（見守りカメラなどで多い）は、外部から直接アクセス可能であるため、要注意．

ご説明の流れ

- マルウェア感染したIoT機器からのサイバー攻撃の観測状況
- 感染が疑われるIoT機器について
- サイバー攻撃により乗っ取られるリスクが大きい機器について
- **IoT機器への対策について**

IoT機器への（機能面での）対策案

＜観測されている現状＞

- Telnetのように多数の機器に共通する問題だけでなく、攻撃が多様化し機器に特有の脆弱性への攻撃が多くなっている.
- インターネット側からの攻撃が主流である.
- 既知の古い脆弱性が最近になって悪用される例がある
- 機器の管理画面（WebUI）の認証の不備（パスワード未設定やデフォルト設定）を突かれる場合がある

＜（製造者視点での）対策＞

- インターネット側からアクセス可能なネットワークサービスについては特に脆弱性検査を徹底する.
- 製品が使用する組込みOS、OSS（オープンソースソフトウェア）、ライブラリの脆弱性情報を把握し、製品への影響を迅速に把握する
- 新規に発見される脆弱性に対応するためのセキュリティアップデートと、アップデートを徹底させる仕組み（強制アップデートやユーザへの通知手段の確保、ユーザフレンドリな更新インターフェイス）
- 管理画面（WebUI）は不用意にインターネット側からアクセスできる仕様にしない．インターネット側からのアクセスが必要な機器については、ユーザによるパスワード設定を促す仕組みを導入する（管理者パスワード設定をしないと機器が使用開始できないようにする、など）