IoTにおけるサイバー攻撃の最新動向とその対策

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

第14回デジタル・フォレンジック・コミュニティ2017 in TOKYO(2017.12.11)

2016年1月～6月の6ヶ月で横浜国大に攻撃をしてきたマルウェア感染IoT機器

約60万台‡

‡IPアドレスによる区別

500種類以上†

† WebおよびTelnetの応答による判断

デバイスはWebおよびTelnetの応答から判断しています。

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
  - 駐車管理システム
  - LEDディスプレイ制御システム

デバイスはWebおよびTelnetの応答から判断しています。

- 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
  - ヒートポンプ
  - 火災報知システム
  - ディスク型記憶装置
  - 医療機器(MRI)
  - 指紋スキャナ

デバイス大量感染の元凶は…

Telnet

Telnetとは

1983年にRFC 854で規定された通信規約。

IPネットワークにおいて、遠隔地にあるサーバを端末から操作できるようにする仮想端末ソフトウェア（プログラム）、またはそれを可能にするプロトコルのことを指す。（省略）

現在では、認証も含めすべての通信を暗号化せずに平文のまま送信するというTelnetプロトコルの仕様はセキュリティ上問題とされ、Telnetによるリモートログインを受け付けているサーバは少なく、リモート通信方法としての利用は推奨できない。

https://ja.wikipedia.org/wiki/Telnet

しかも多くは
デフォルト／弱いパスワードで

```
[shogo@www9058up ~]$ telnet x.x.243.13
Trying x.x.243.13...
Connected to x.x.243.13.
Escape character is '^]'.

[redacted]i.3.0.dm800s
[redacted]e.login: root
Password:12345
```

リモートログイン成功

```
BusyBox v1.1.2 (2007.05.09-01:19+0000) Built-
in shell (ash)
Enter 'help' for a list of built-in commands.
```

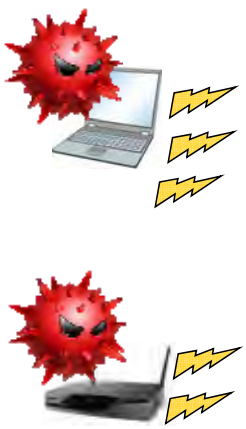
攻撃の観測：いくつかのアプローチ

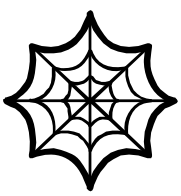
- 受動 (passive) 型：
  観測用ネットワークで攻撃が来るのをまつ
  - ダークネットモニタリング
  - ハニーポット

- 能動 (active) 型：
  インターネット上の攻撃ホスト情報・脆弱性等を自ら探索する
  - Web、Telnet、 FTP等へのアクセスによる機器、システムの判定
  - バックドアポート等の確認

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





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

ダークネットへのTelnet攻撃の急増

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

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

日時

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%

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

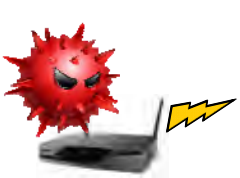
より詳細に攻撃を分析するために

ダークネットは、大量のアドレスを広範囲に観測できる反面、
攻撃の最初の通信（パケット）のみ観測可能であるため、
攻撃の詳細手順やマルウェア本体を分析するには観測方法を工夫する必要がある

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

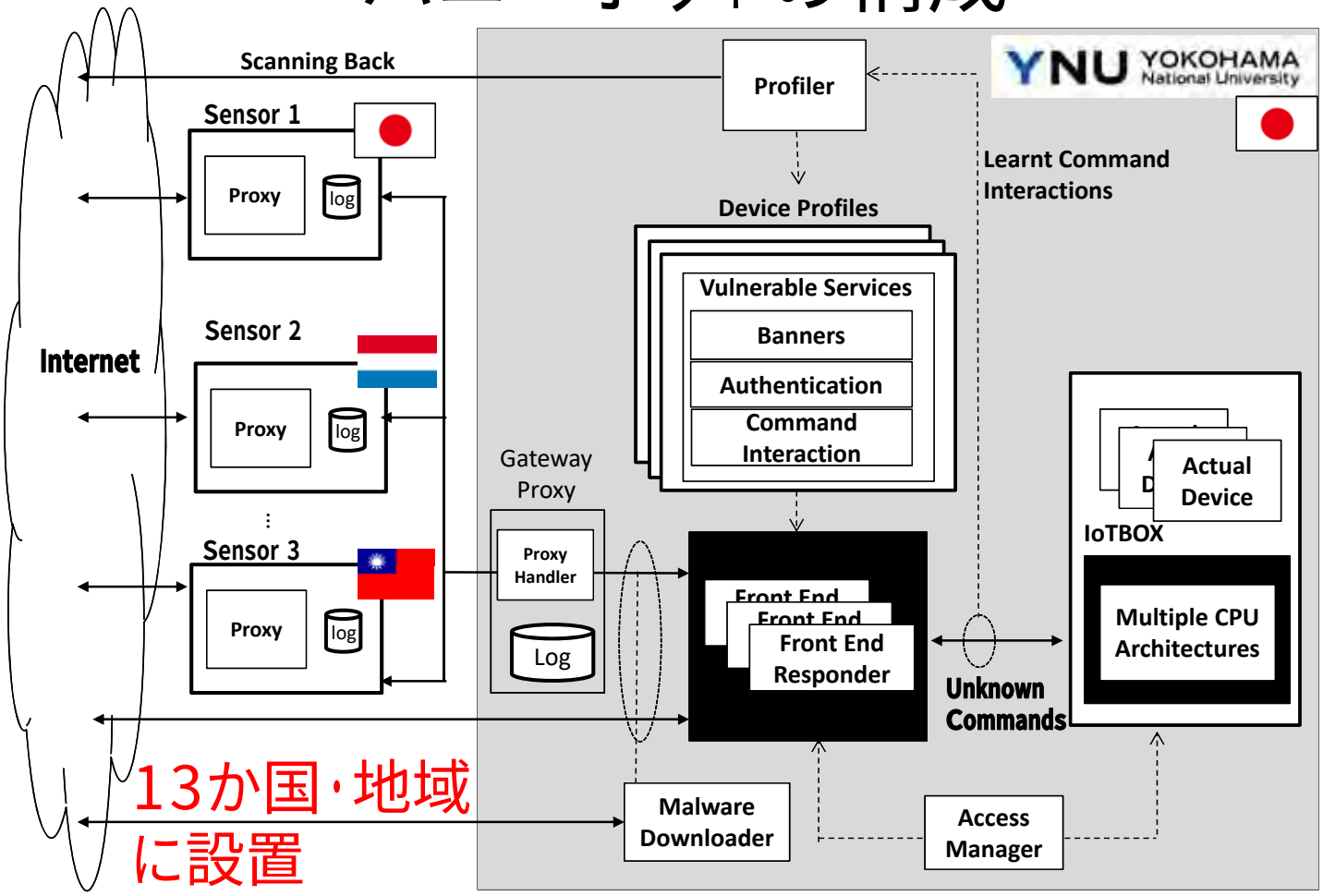
脆弱な機器を模擬した囮システム（ハニーポット）により攻撃元と通信を行い、攻撃の観測・マルウェア捕獲し、詳細解析を行う

攻撃元機器
（マルウェア
感染済）



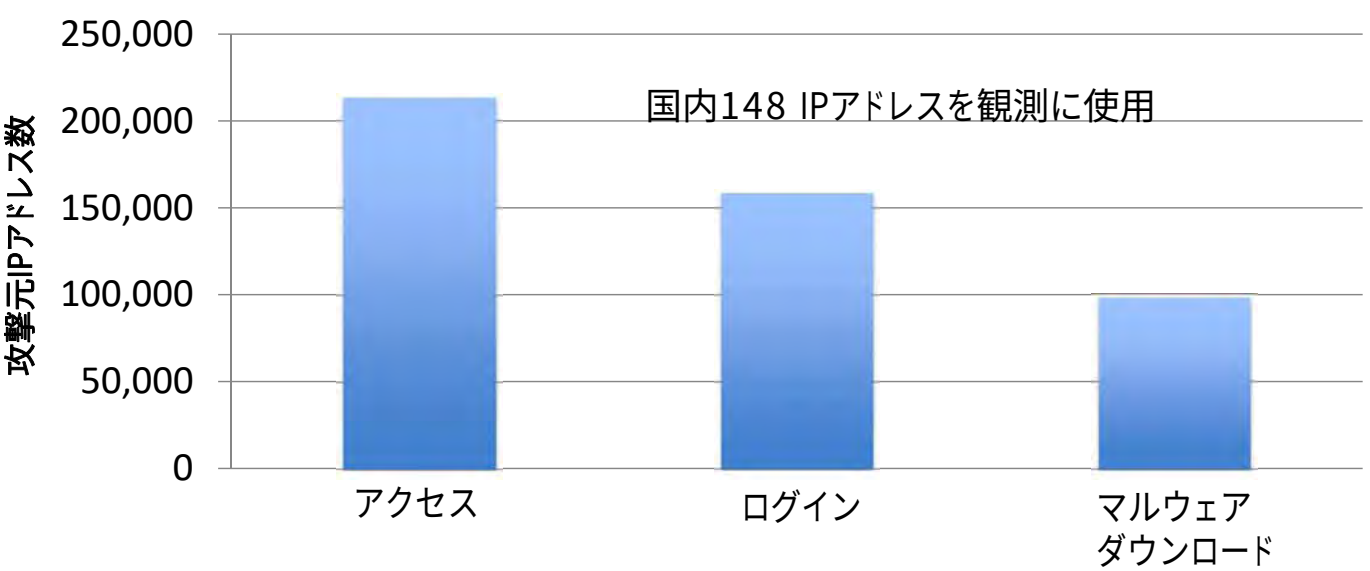
攻撃者が用意
したサーバ

ハニーポットの構成



観測結果 (2015)

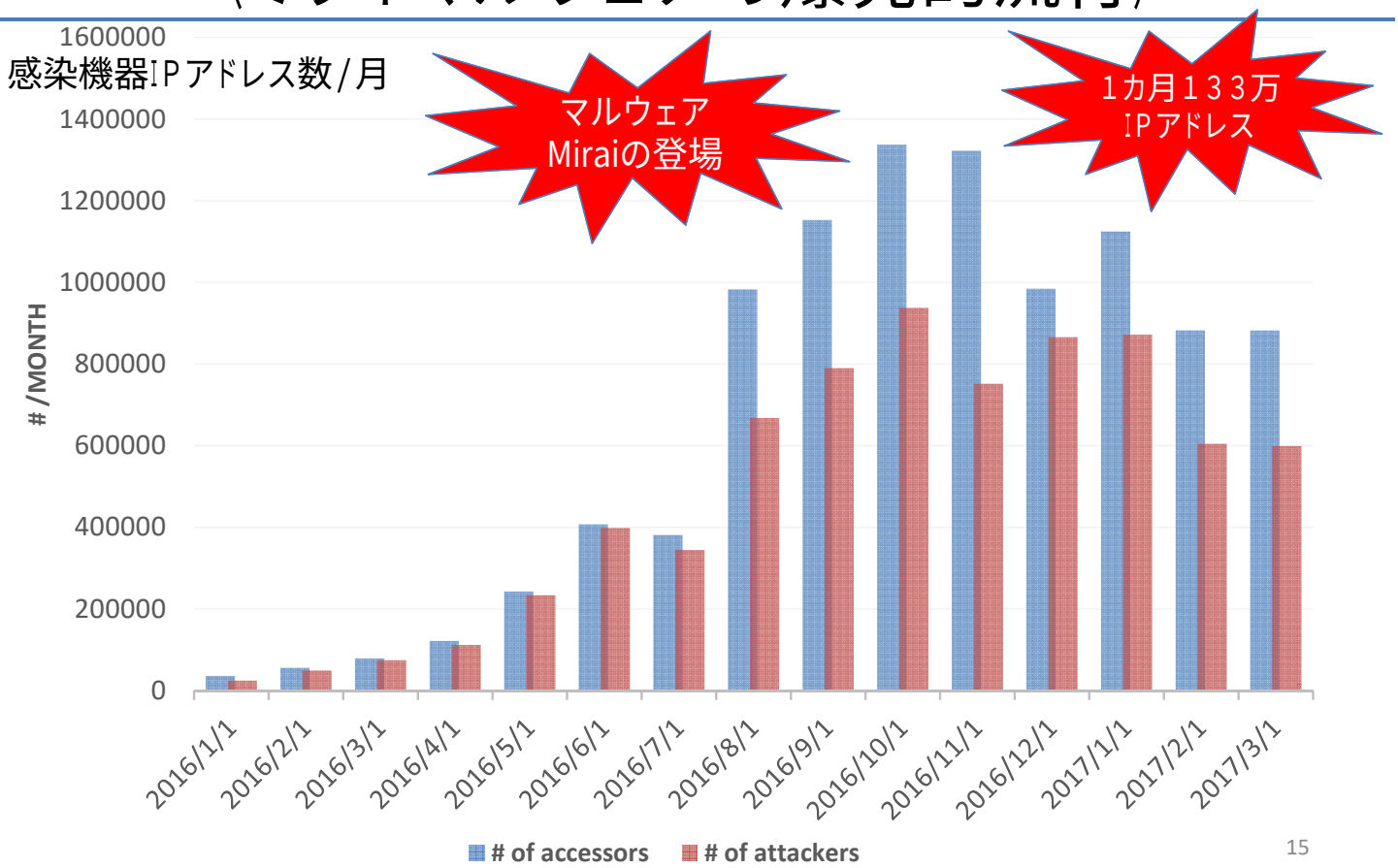
観測期間：2015/4/1～2015/7/31 (122日)



約15万アドレスから不正ログインを検出し、90万回のマルウェアダウンロード試行を観測

11種類のCPUアーキテクチャ向けマルウェアを捕獲

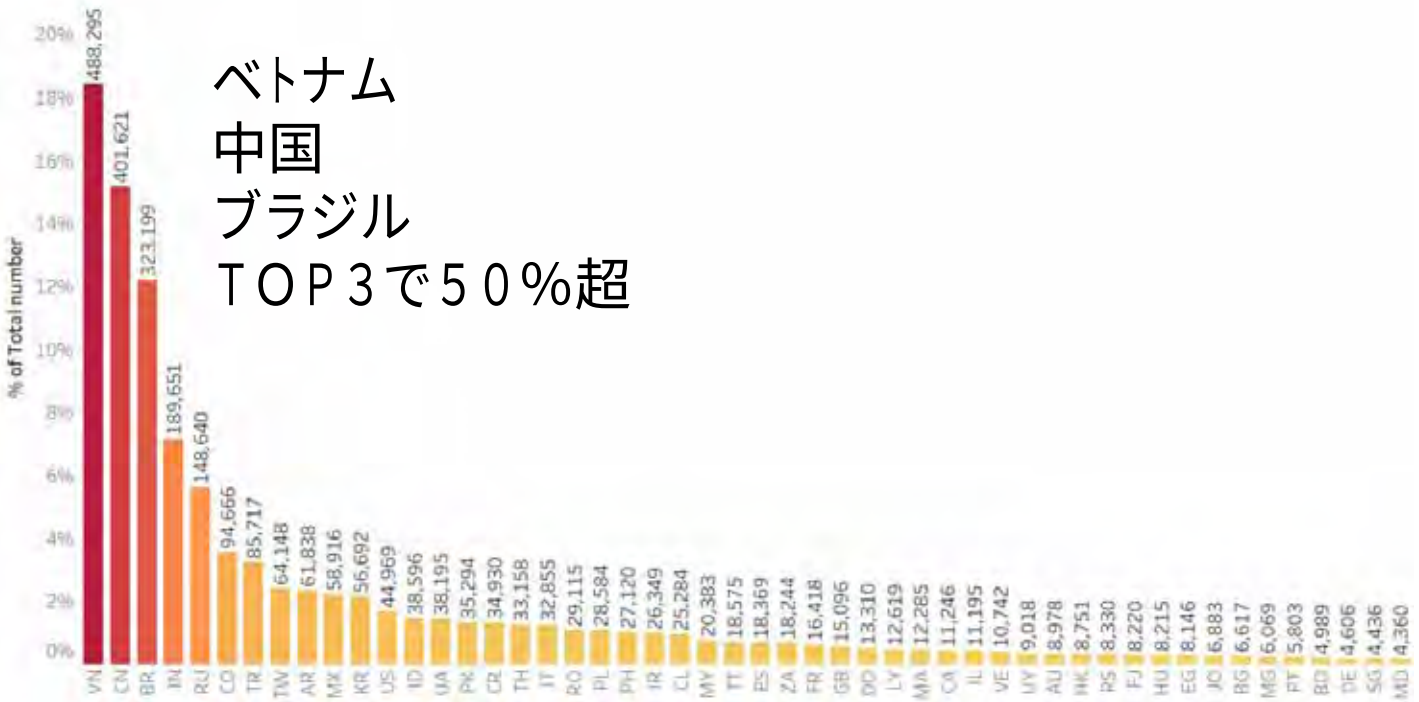
2016後半に攻撃が急増
(ミライマルウェアの爆発的流行)



世界的に広がる感染

- 218か国
  からの攻撃を観測
- 特にアジアと南米
  の感染が多い

国別感染機器台数（IPアドレス）



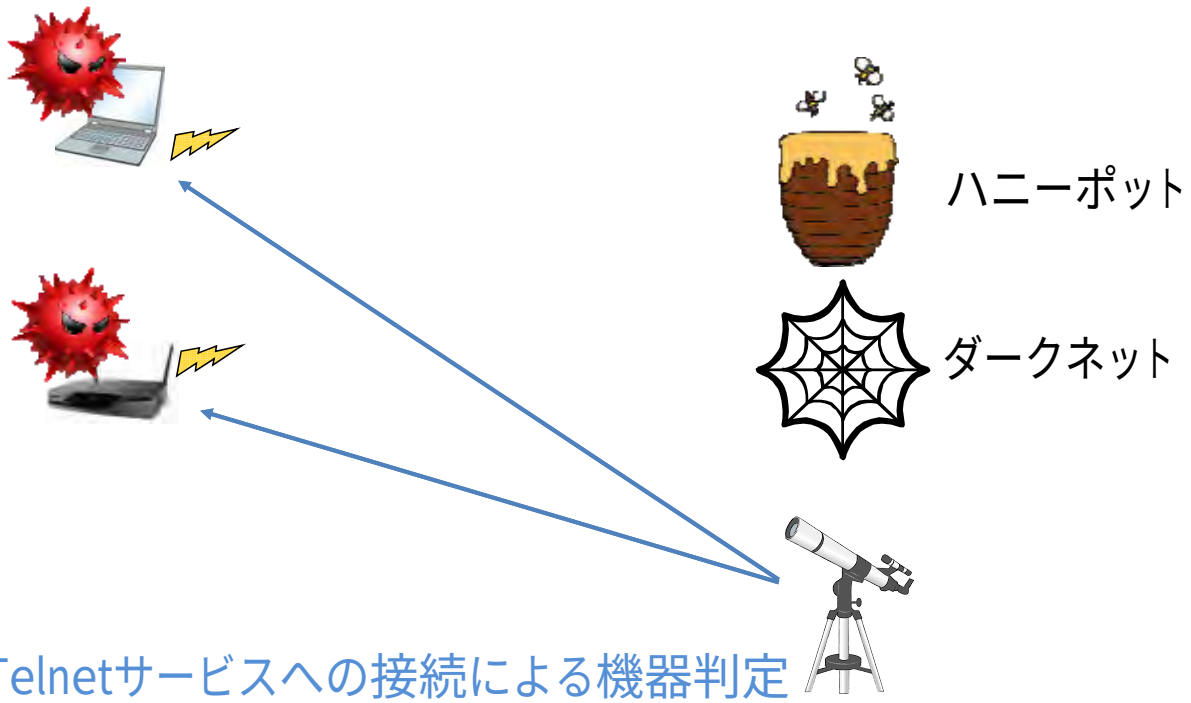
ベトナム
中国
ブラジル
ＴＯＰ３で５０％超

攻撃の観測：いくつかのアプローチ

- 受動（passive）型：
  観測用ネットワークで攻撃が来るのをまつ
  – ダークネットモニタリング
  – ハニーポット

- 能動（active）型：
  インターネット上の攻撃ホスト情報・脆弱性等を自ら探索する
  – Web、Telnet、FTP等へのアクセスによる機器、システムの判定
  – バックドアポート等の確認

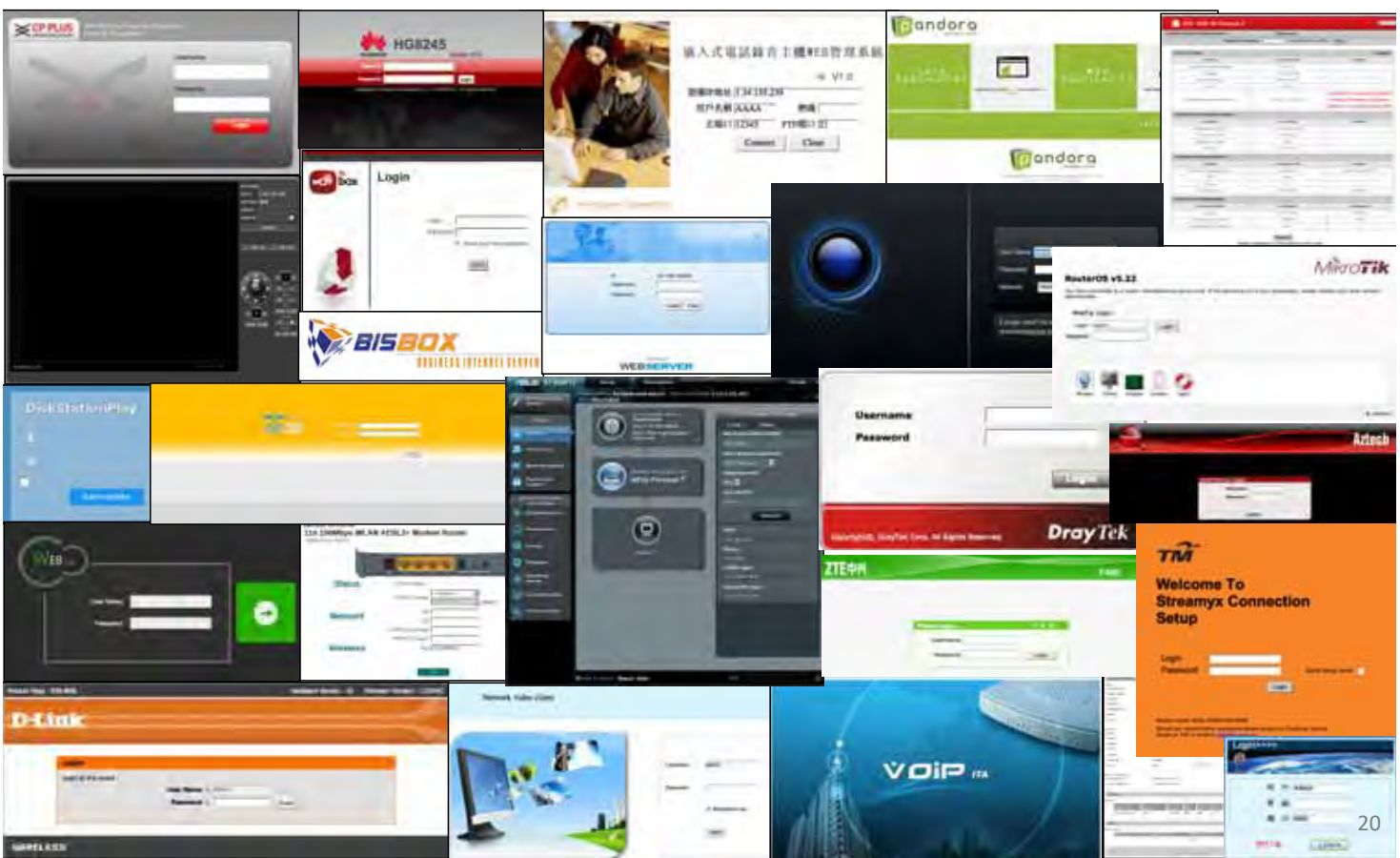
攻撃元機器の判定



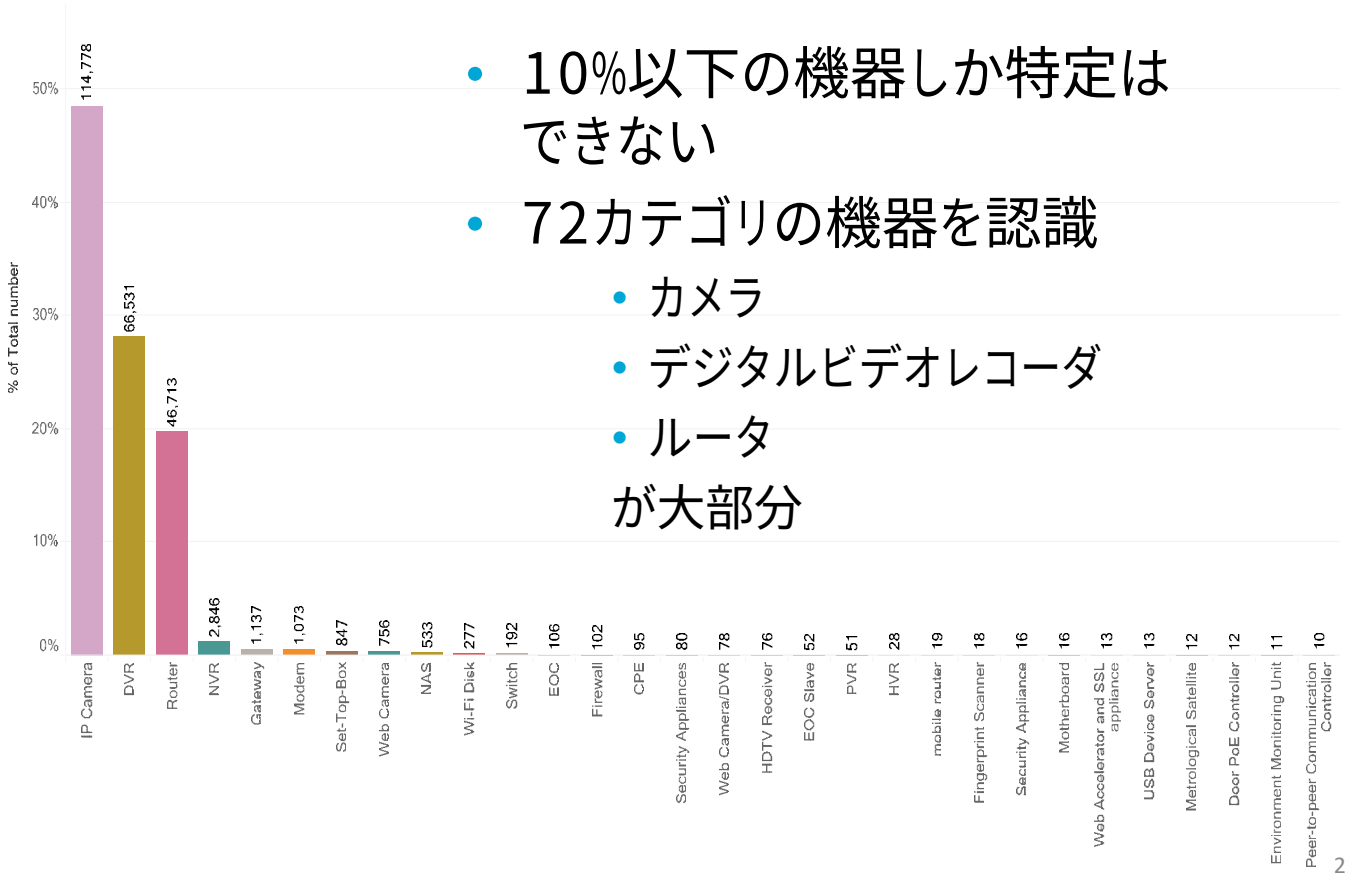
Web、Telnetサービスへの接続による機器判定

→IoT機器であることを確認

攻撃元（感染）機器のWebインターフェイスの例



ハニーポットで観測された感染機器の種類

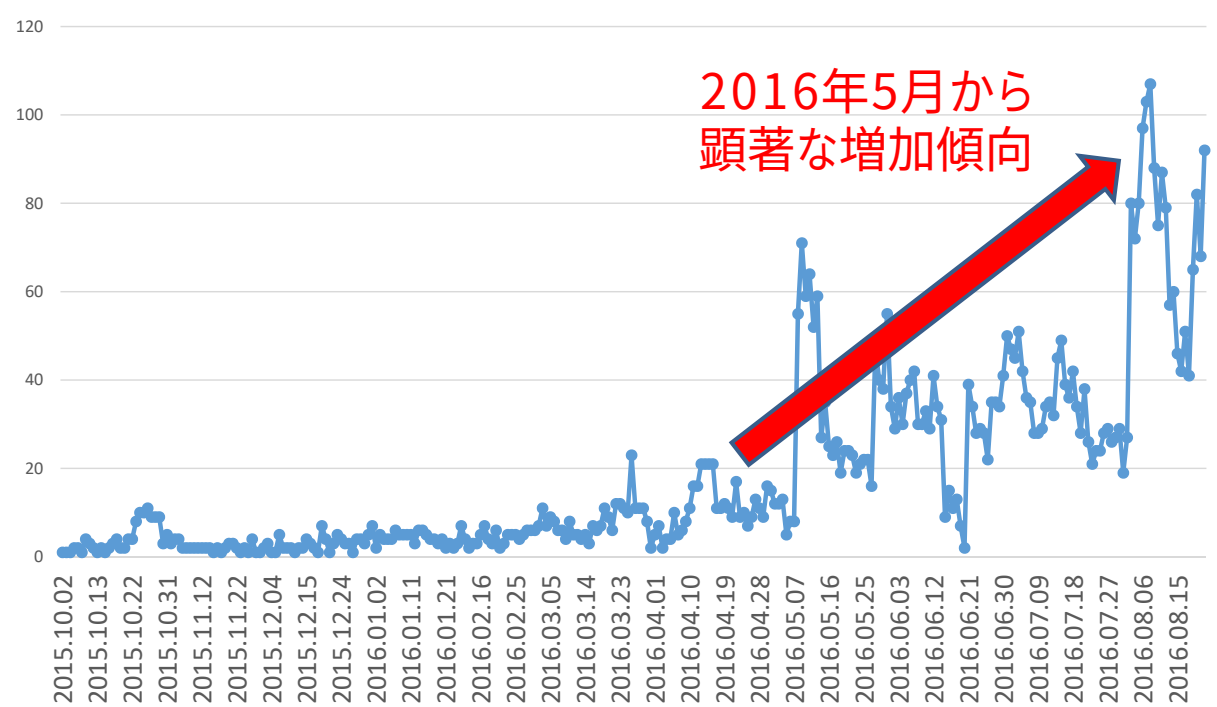


- 10%以下の機器しか特定はできない
- 72カテゴリの機器を認識
  - カメラ
  - デジタルビデオレコーダ
  - ルータ

  が大部分

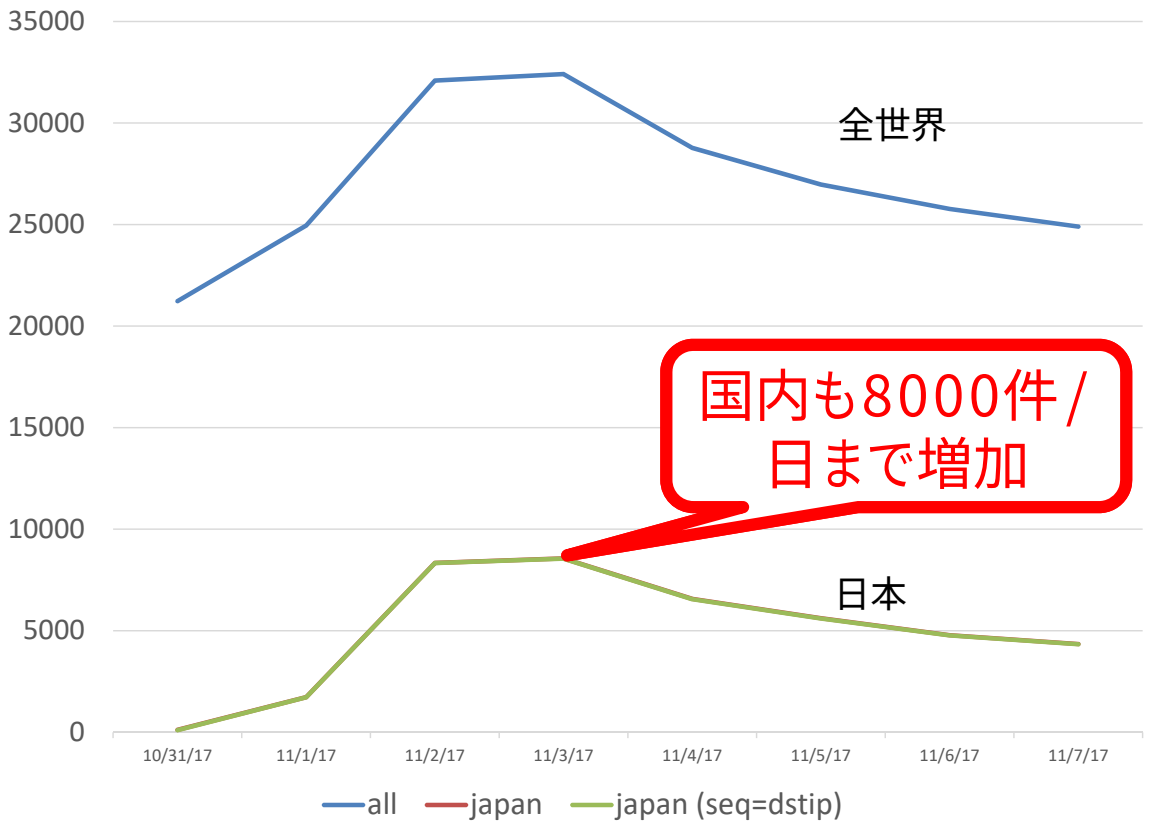
日本国内 感染機器台数 (日ごとにカウント)

IPアドレス/日

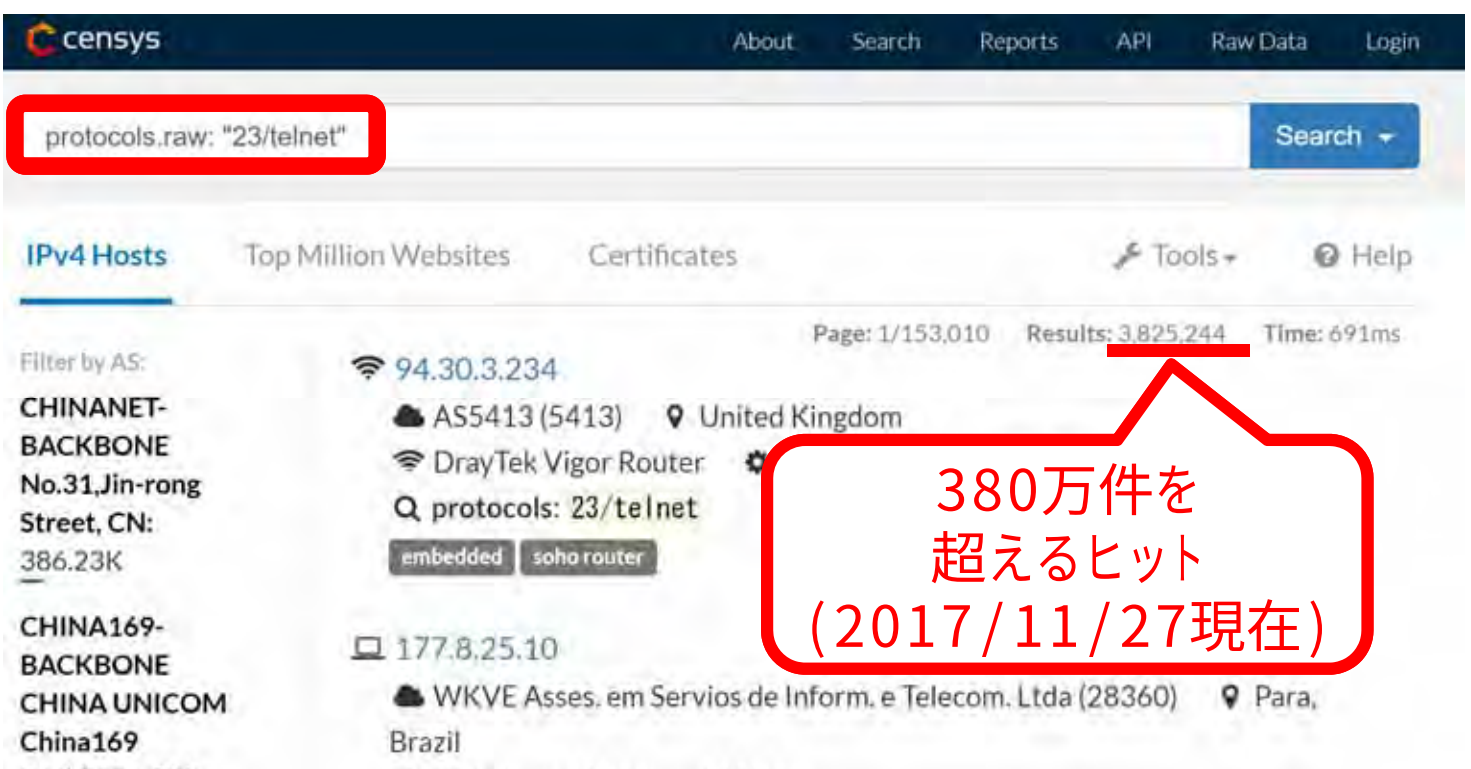


最近の国内感染機器の急増(2017年11月)

IPアドレス/日



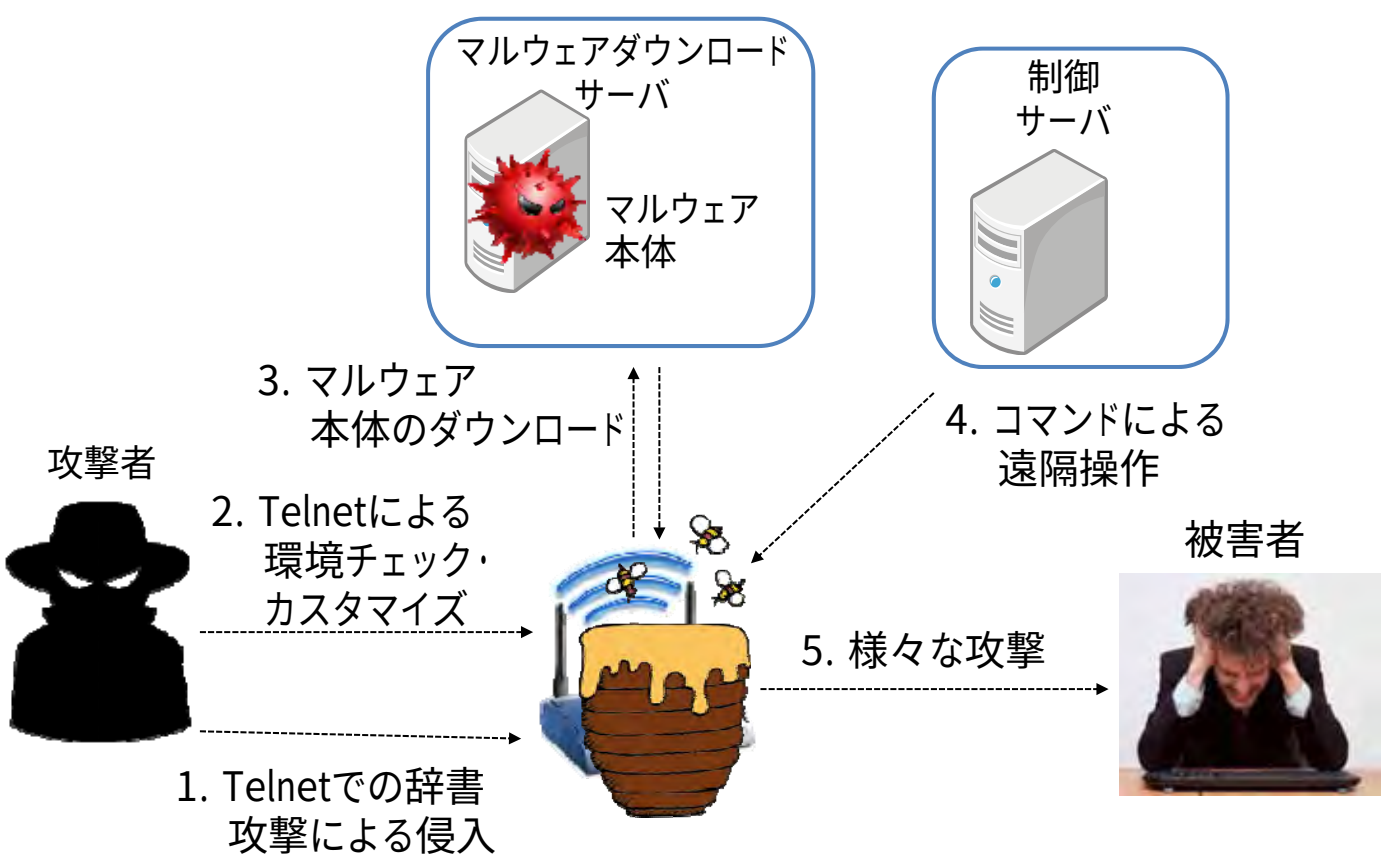
世界中の機器をスキャンした結果を公開しているサイトCensys（ミシガン大学）



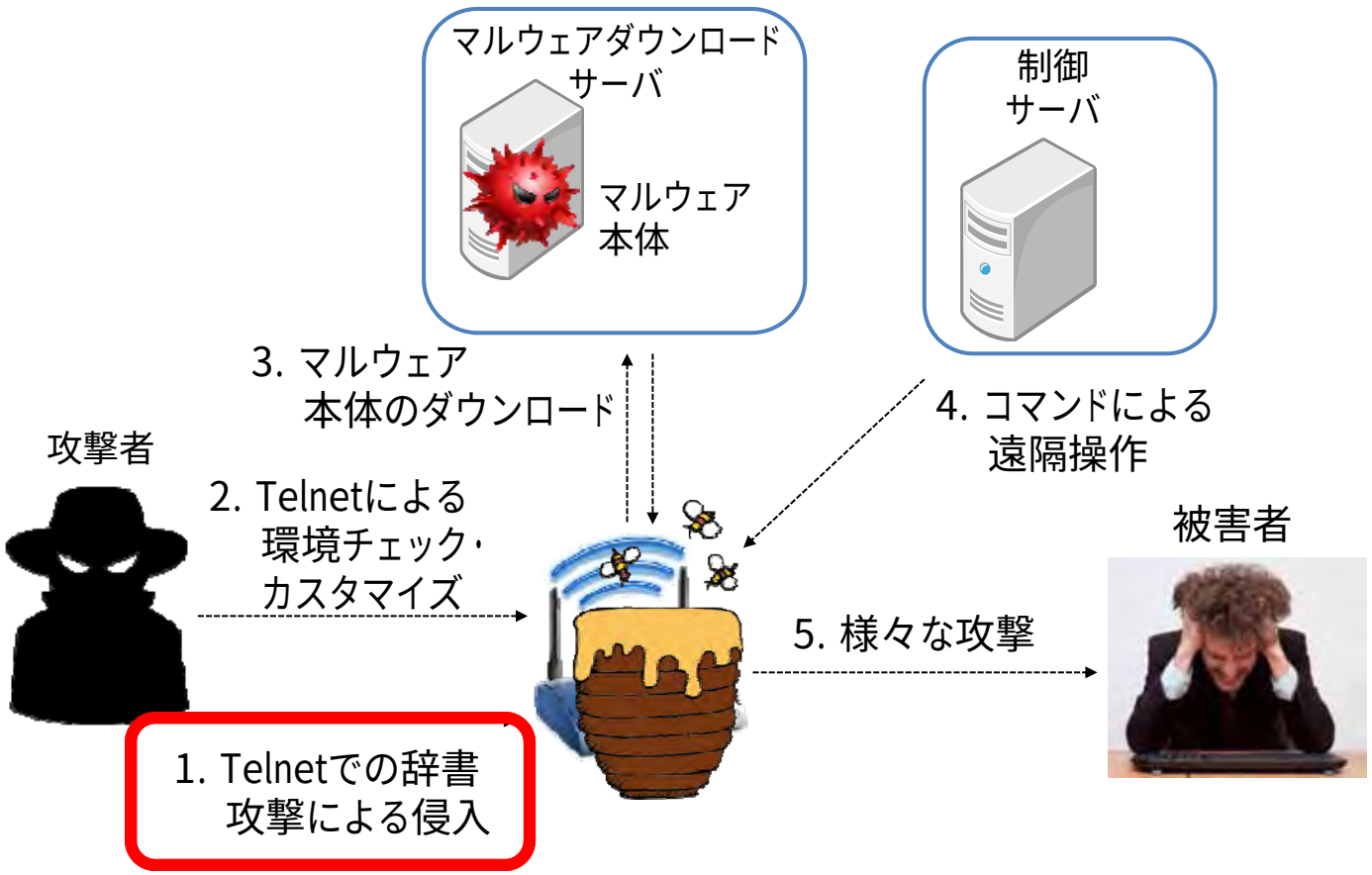
ミライ (Mirai) のその先 (1)

侵入方法の多様化

Telnetベースのマルウェア感染の流れ



Telnetベースのマルウェア感染の流れ



観測開始当初見られた辞書攻撃は6パターン

固定順序型攻撃パターン1

```
root/r
root/a    n
root/1
root/1    5
root/1    56
root/1
root/p    word
root/d    mbox
```

順序変更型攻撃パターン1

```
root/    511
root/    456
root/    45
root/    t
…
```

順序変更型攻撃パターン2

```
root/    t
root/    nin
root/    45
root/    456
admi    oot
…
```

固定順序型攻撃パターン2

```
guest/    st
guest/    45
admin
root/r
root/a    in
root/
root/1
root/1    56
root/1
root/p    word
root/d    mbox
root/v    y
```

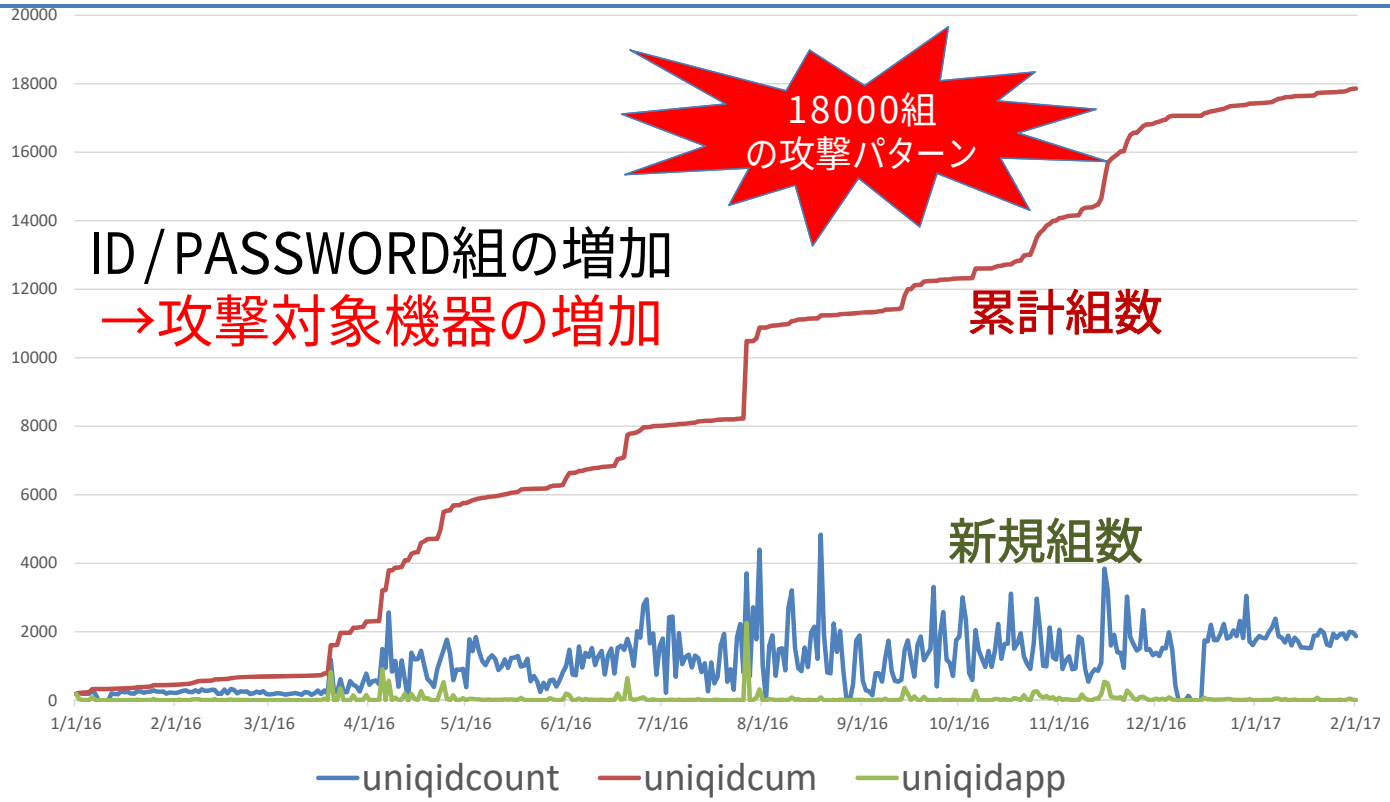
固定順序攻撃パターン3

```
admin/    nin
admin/    729
admin/    f6h3
admin/    yporra
admin/    297
admin/    m0r
admin/    4
root/12
```

順序変更型攻撃パターン3

```
root/    t
root/    r
root/    nin
root/    r
….
```

攻撃に利用されるID/PASSWORD組の増加



ネットワークカメラ
“のぞき見”
の観測

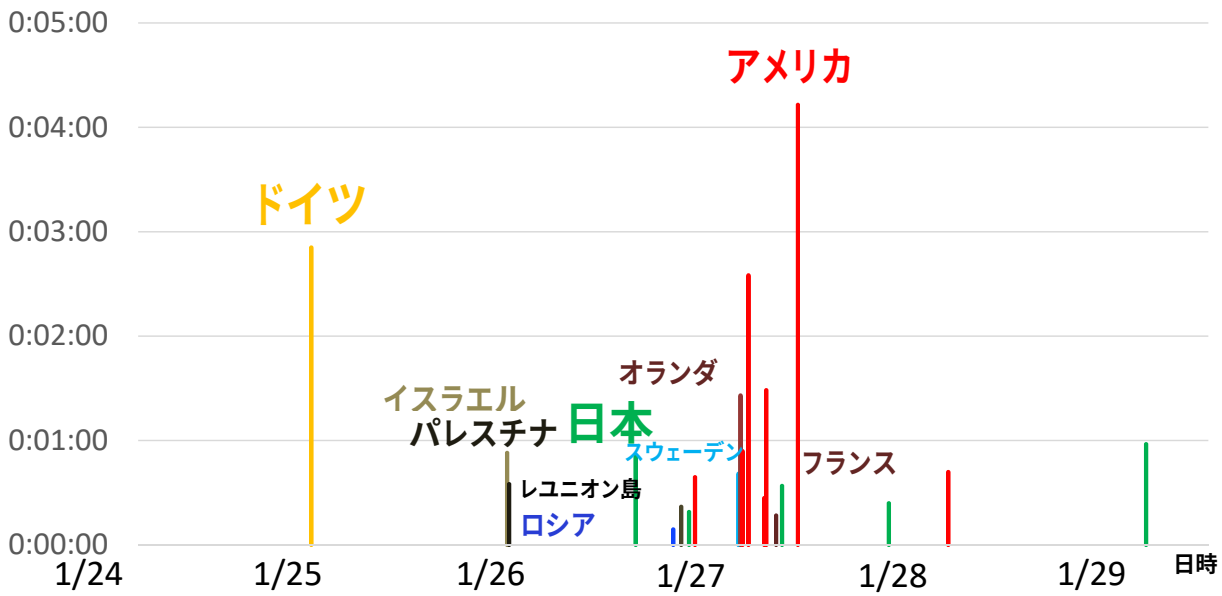
ネットワークカメラ画像無断公開サイト Insecam (ロシア)

おとりカメラの映像 (大学サーバ室)

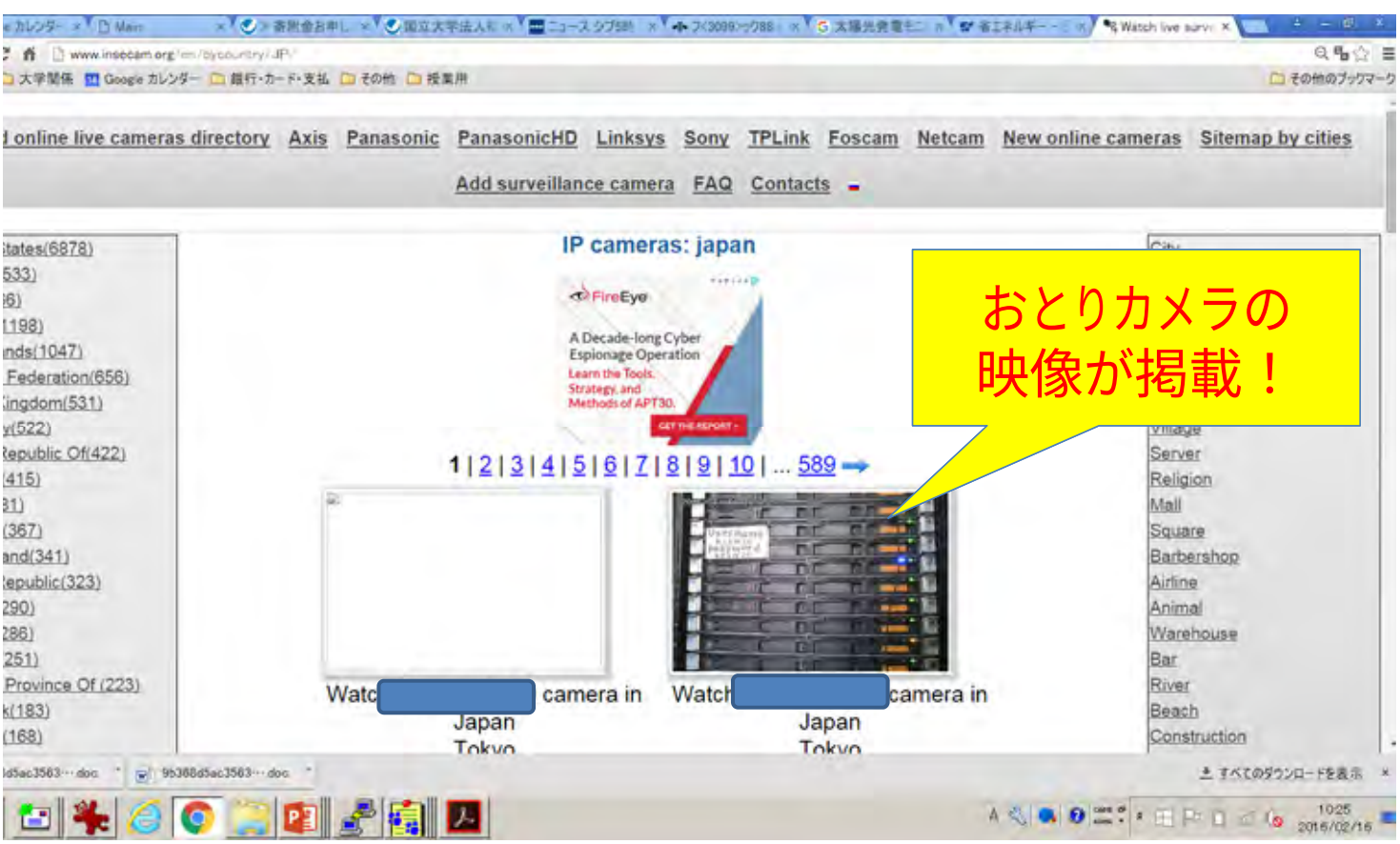
おとりカメラの“のぞき見”

1）観測開始後、5日目にドイツから最初のアクセス（のぞき見）
2）その後多様な国からアクセス（のぞき見）が観測・最長で4分超
3）**映像内のID/パスワード**を利用したアクセスも検知
　→プログラムではなく人間が実際に映像を目視確認している

のぞき見の継続時間

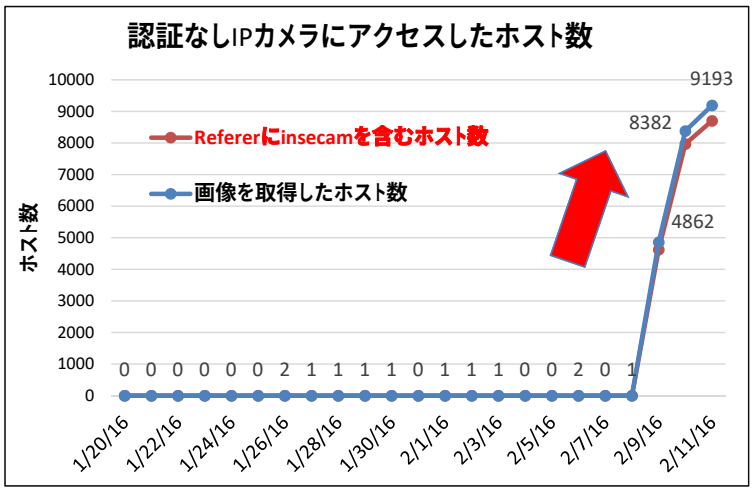


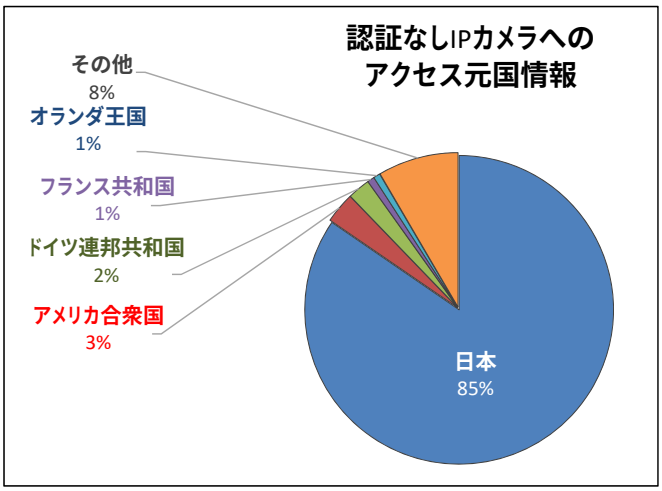
無断でIPカメラ映像を公開する WebサイトInsecam（ロシア）



おとりカメラへのアクセス（Insecam掲載後）

- Insecam掲載（2/9）後にアクセスが急増（数千倍のアクセス頻度、9,163ホストからアクセスを観測）
- 8割以上が日本からのアクセス

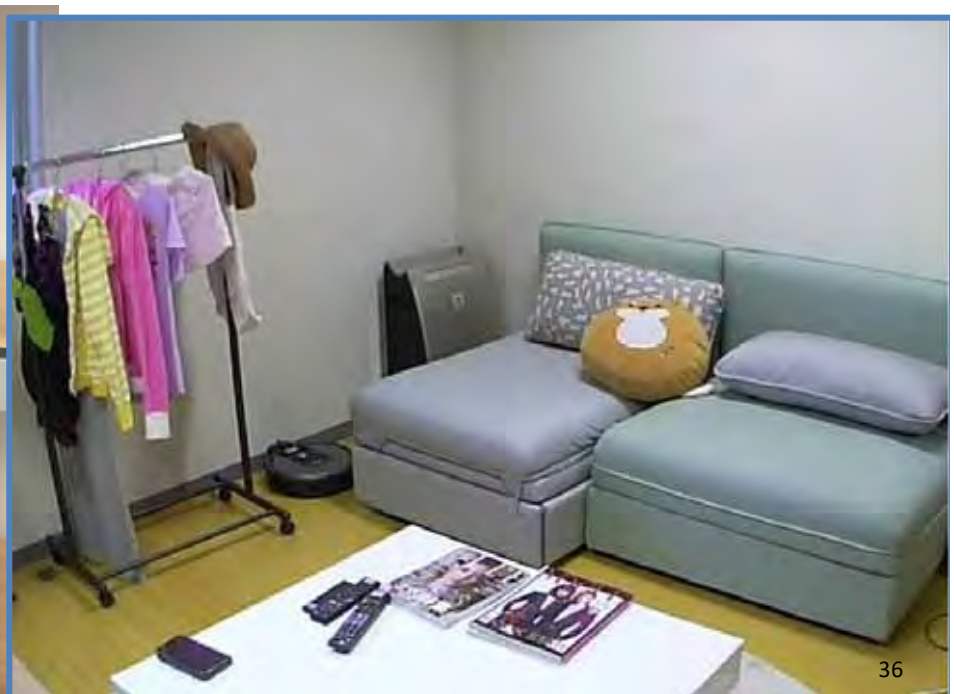




Insecamへの掲載が設定不備カメラ問題を助長し、一日４０００件以上の“のぞき見”が発生

カメラ操作を伴う長期的のぞき見の観測

- NHKとの共同調査（囮カメラを6台設置し囮カメラを監視するためのカメラも3台設置、認証有と無を用意）



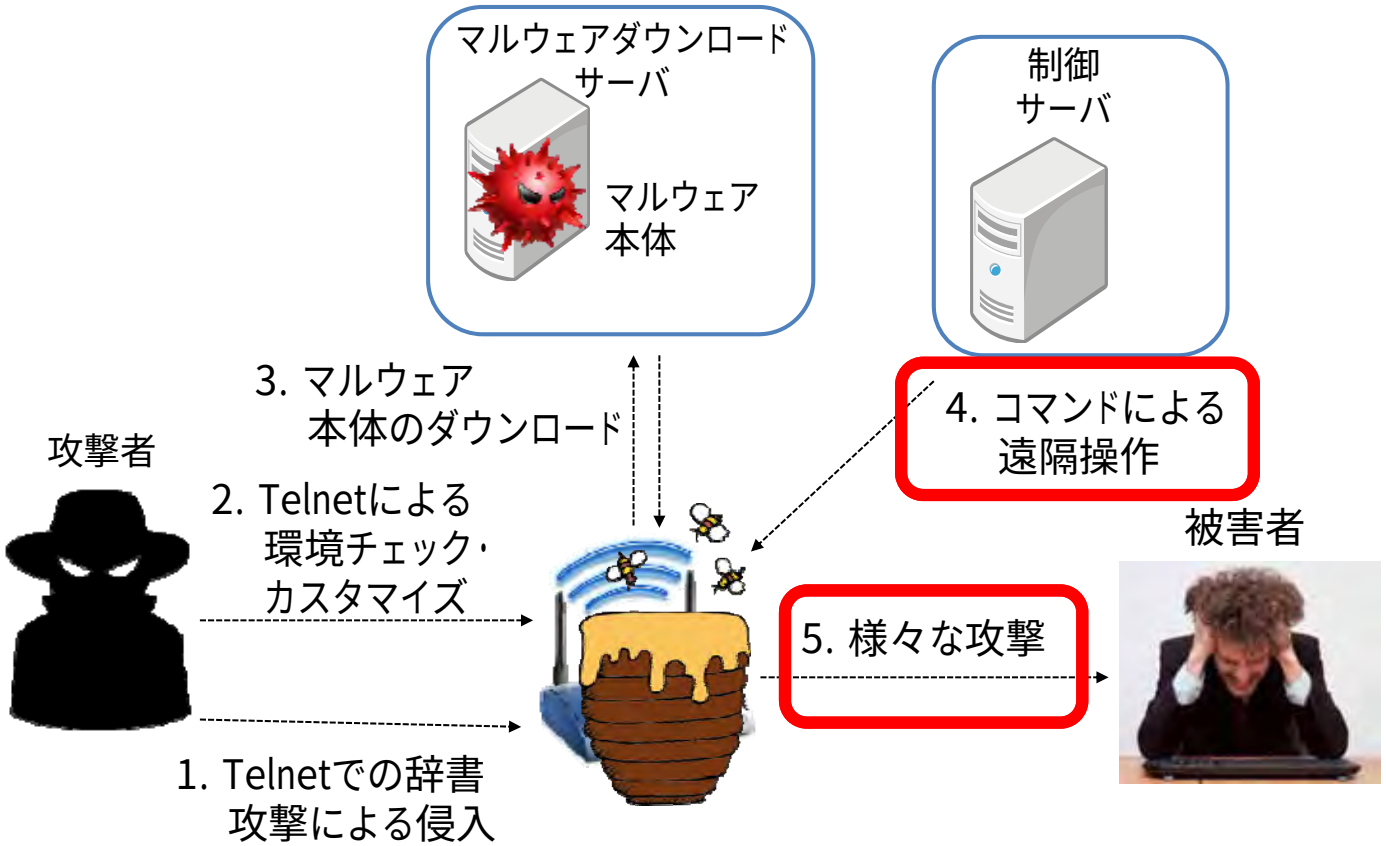
カメラ操作を伴う長期的のぞき見

部屋を隅から隅まで覗いている

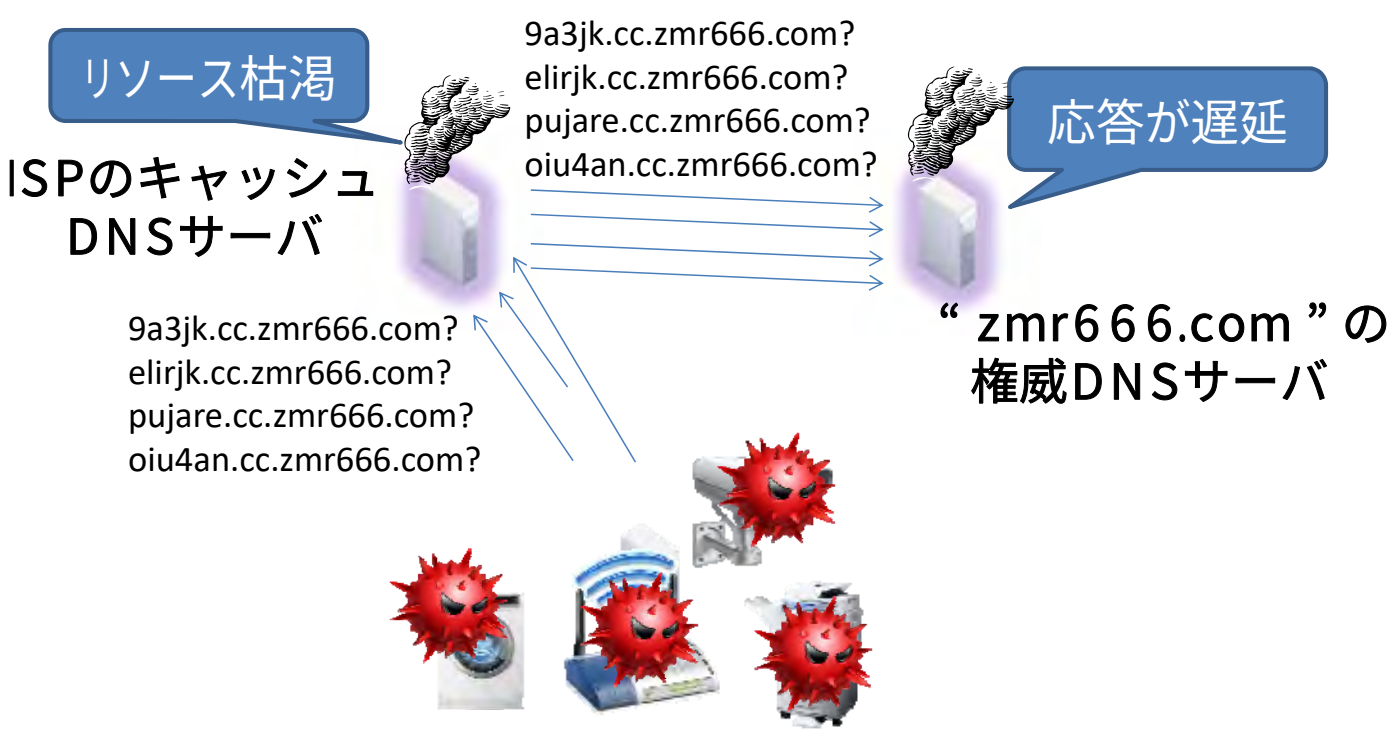
ミライ (Mirai) のその先 (2)

攻撃規模の巨大化

Telnetベースのマルウェア感染の流れ

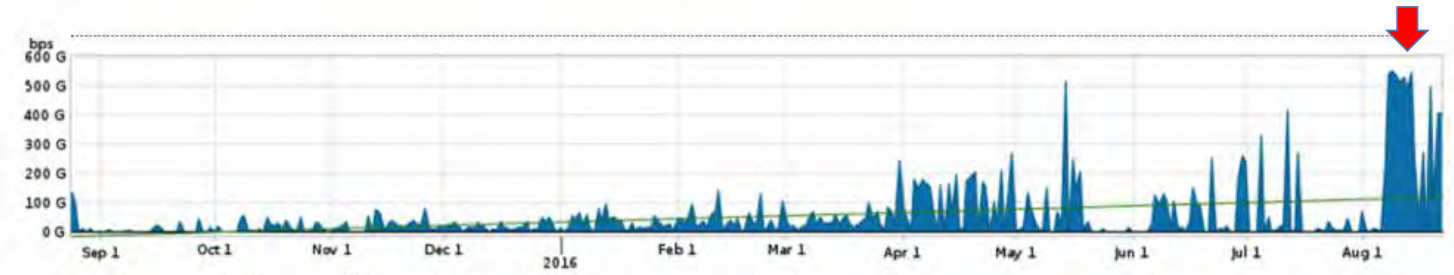


サービス妨害攻撃への加担

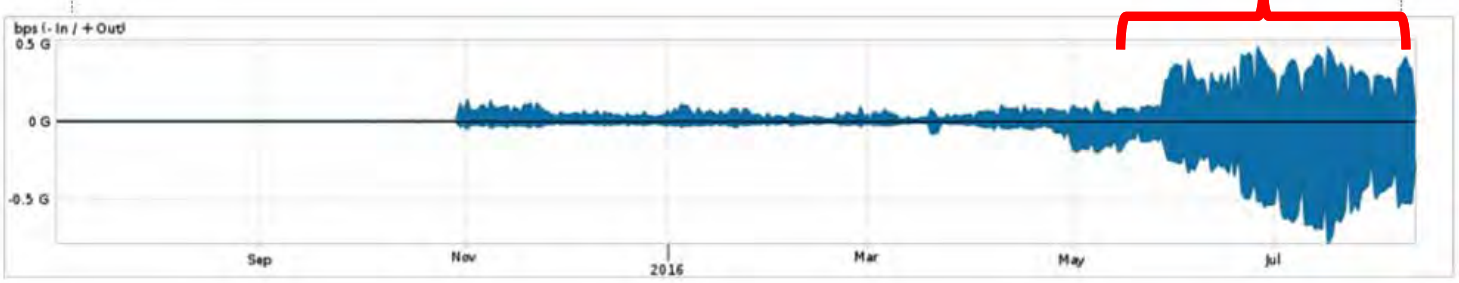


リオ五輪の時期に500Gbps規模の超大規模サービス妨害攻撃が頻発

Tokyo Olympics, what to expect.



Telnet通信の急増(感染機器の増加＝攻撃準備)

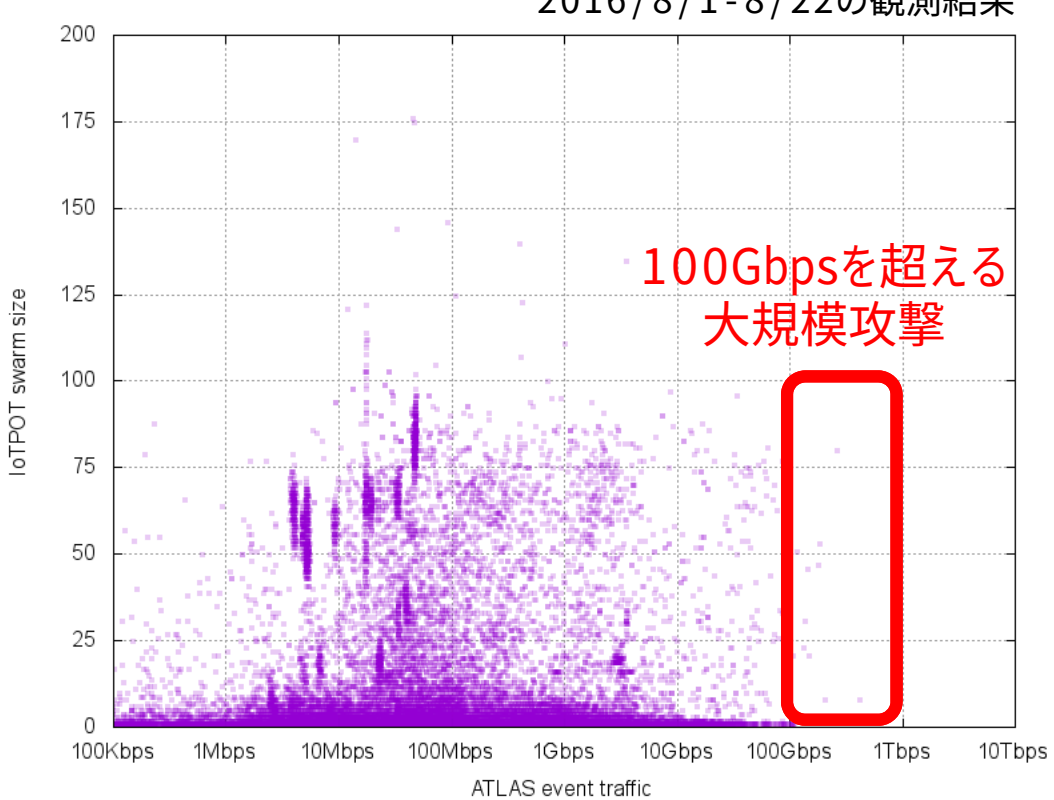


本データは米国Arbor Networks社から提供を受けたものです

ARBOR NETWORKS

横浜国大で観測した感染機器のうち
サービス妨害攻撃に加担していた台数

2016/8/1-8/22の観測結果



Arbor Networksが観測したサービス妨害攻撃の規模

本データはArbor Networks社と横浜国大の産学連携活動の成果であり、
Arbor Networks ASERT Japanの分析結果です。

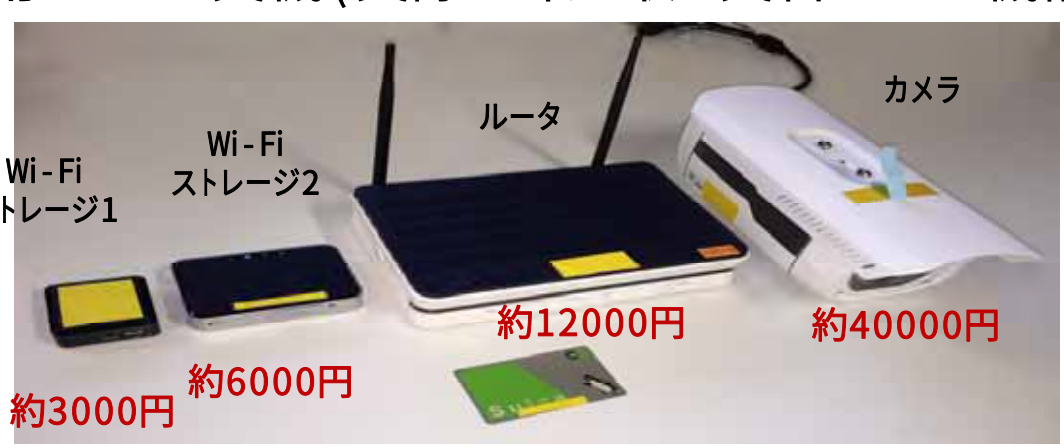
攻撃はどこまで大きくなるのか？

理論的上限値を試算

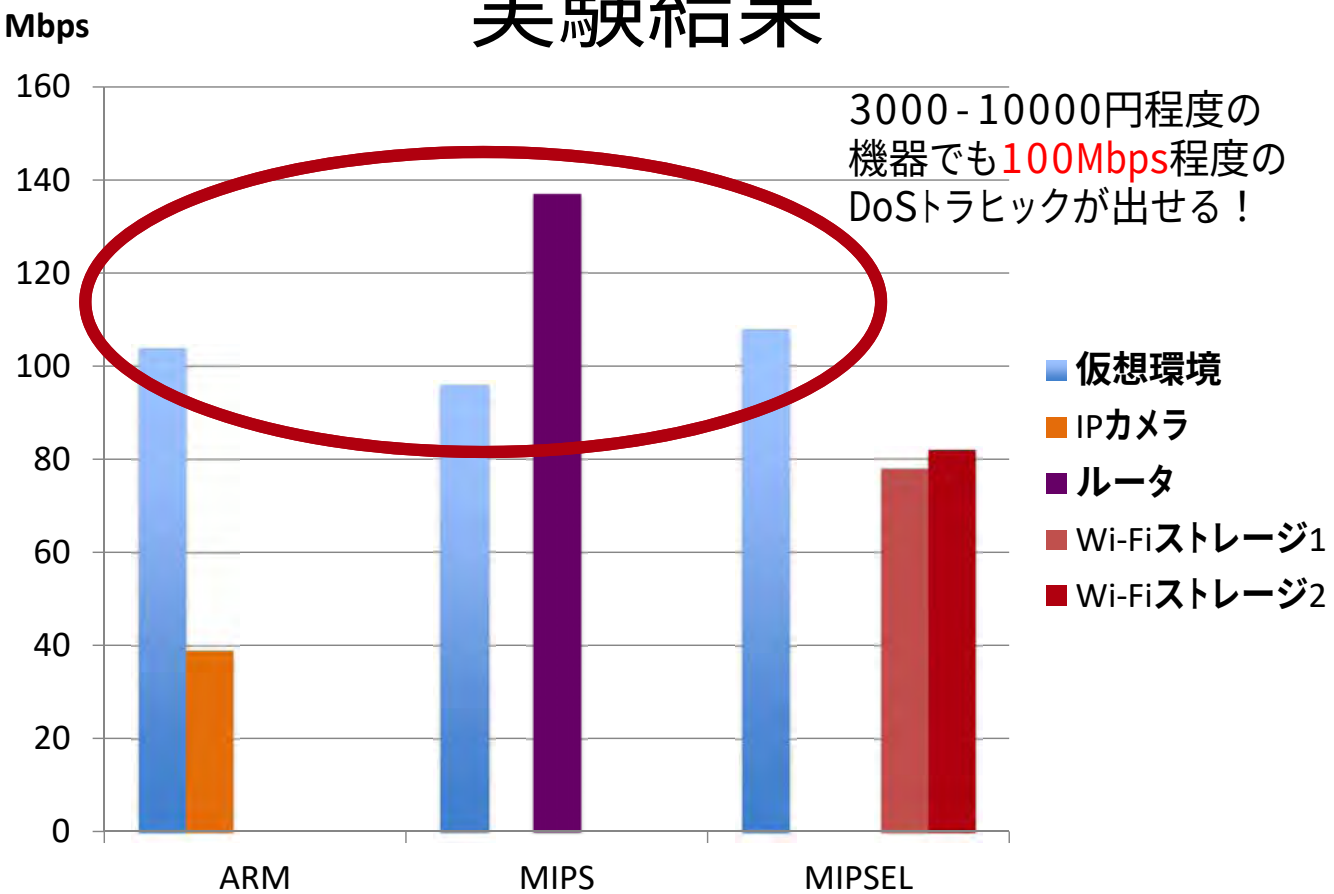
- １台あたり、どのくらいの出力が出る？
  （アップリンクの上限値も考慮）
- 攻撃者は何台くらい同時に操れる？

各機器のDoS出力測定実験

- 使用するマルウェア検体
  - IoTハニーポットにより収集した、同種のマルウェア(bashlite)でarm、mips、mipsel上にて動作する検体2組 計6種
- 使用したIoT実機(実際に乗っ取り実害のある機器群)



実験結果

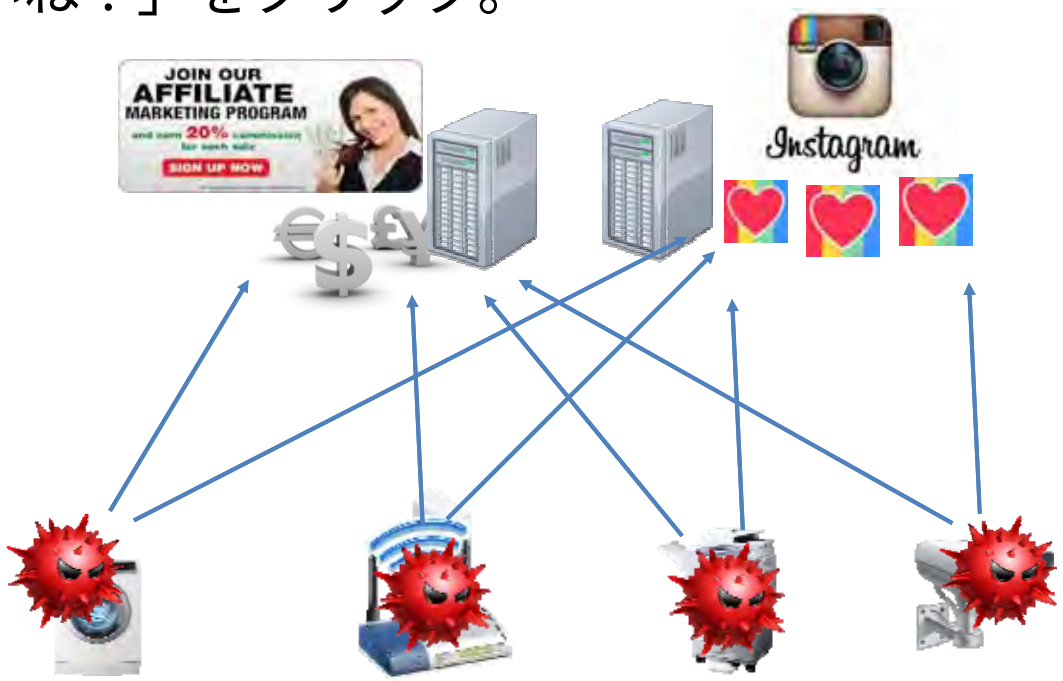


ミライ (Mirai) のその先 (3)

目的の多様化

観測事例1：不正クリック

アフィリエイトサイト（広告サイト）にクリックを装ってアクセスし対価を得る。インスタグラムで「いいね！」をクリック。



感染機器

観測事例2：
有料ネット放送の認証情報の盗取

セットトップボックス（有料TV放送受信装置）から認証情報を盗取

特定の機器（セットトップボックス）を狙った攻撃であることに注意

観測事例3：機器を故障させるIoTマルウェア

2017年1月より、ストレージ内のファイルをランダム値に書き換え、機器の破壊を試みるマルウェアBrickerbotを11か国から60件観測
2017年8月に活動再開し、ハニーポット機器4台を故障させた

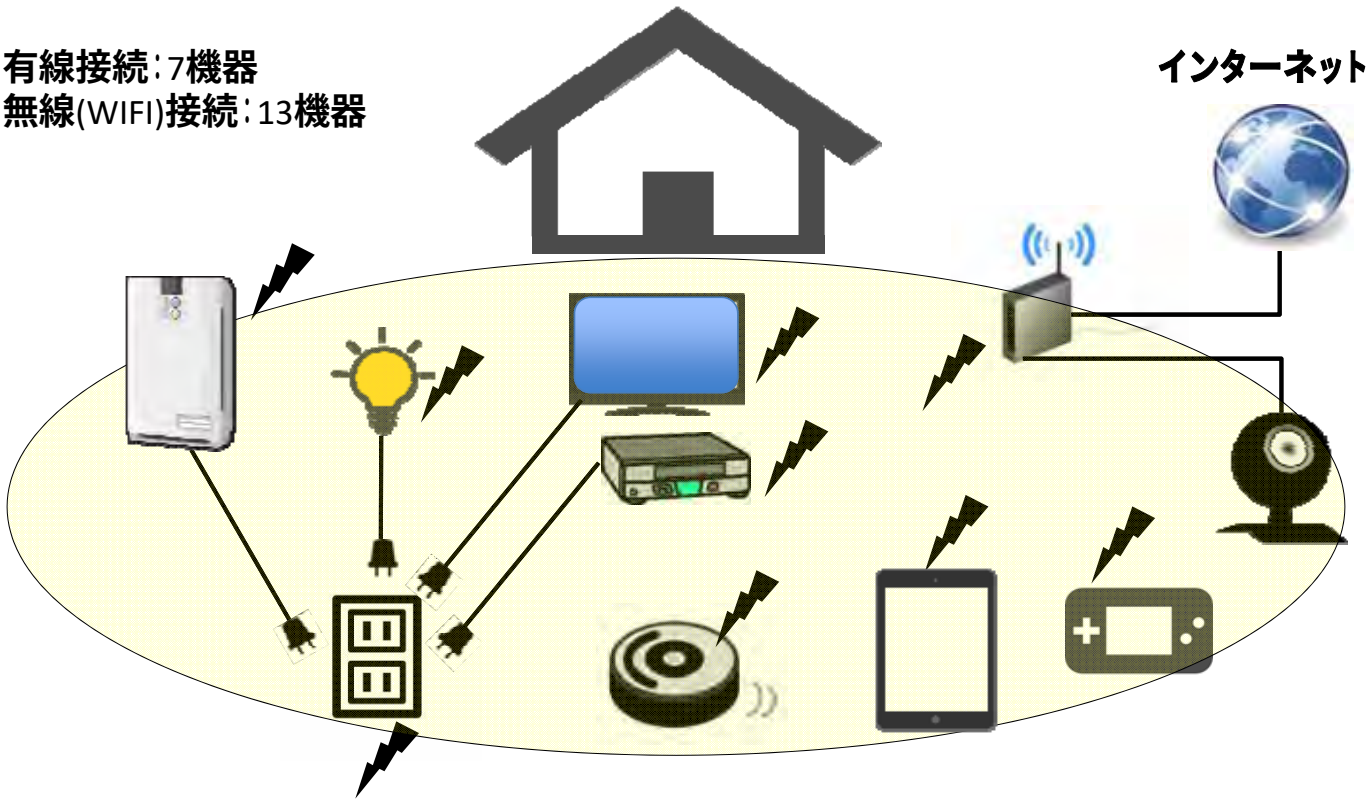
```
dd if=/dev/urandom of=/dev/hdb1 &
dd if=/dev/urandom of=/dev/root &
dd if=/dev/urandom of=/dev/ram0 &
dd if=/dev/urandom of=/dev/mmcblk0 &
dd if=/dev/urandom of=/dev/mmcblk0p1 &
cat /dev/urandom >/dev/sda &
cat /dev/urandom >/dev/sda1 &
cat /dev/urandom >/dev/sda2 &
cat /dev/urandom >/dev/sda3 &
cat /dev/urandom >/dev/sda4 &
```


横浜国立大学・BBSS
IoTサイバーセキュリティ
共同研究プロジェクト

YNU YOKOHAMA National University
BBSS

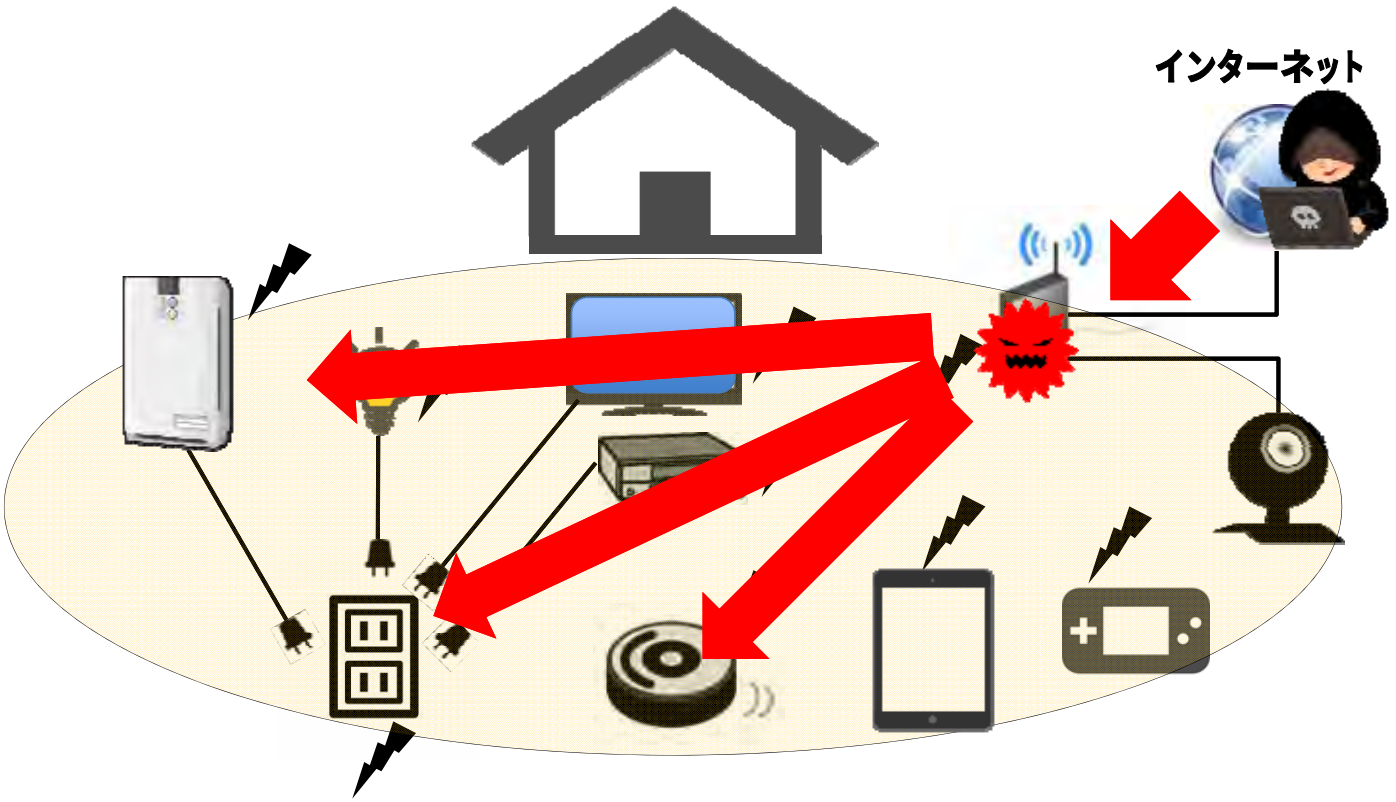
コネクテッドホーム試験室

有線接続：7機器
無線(WIFI)接続：13機器



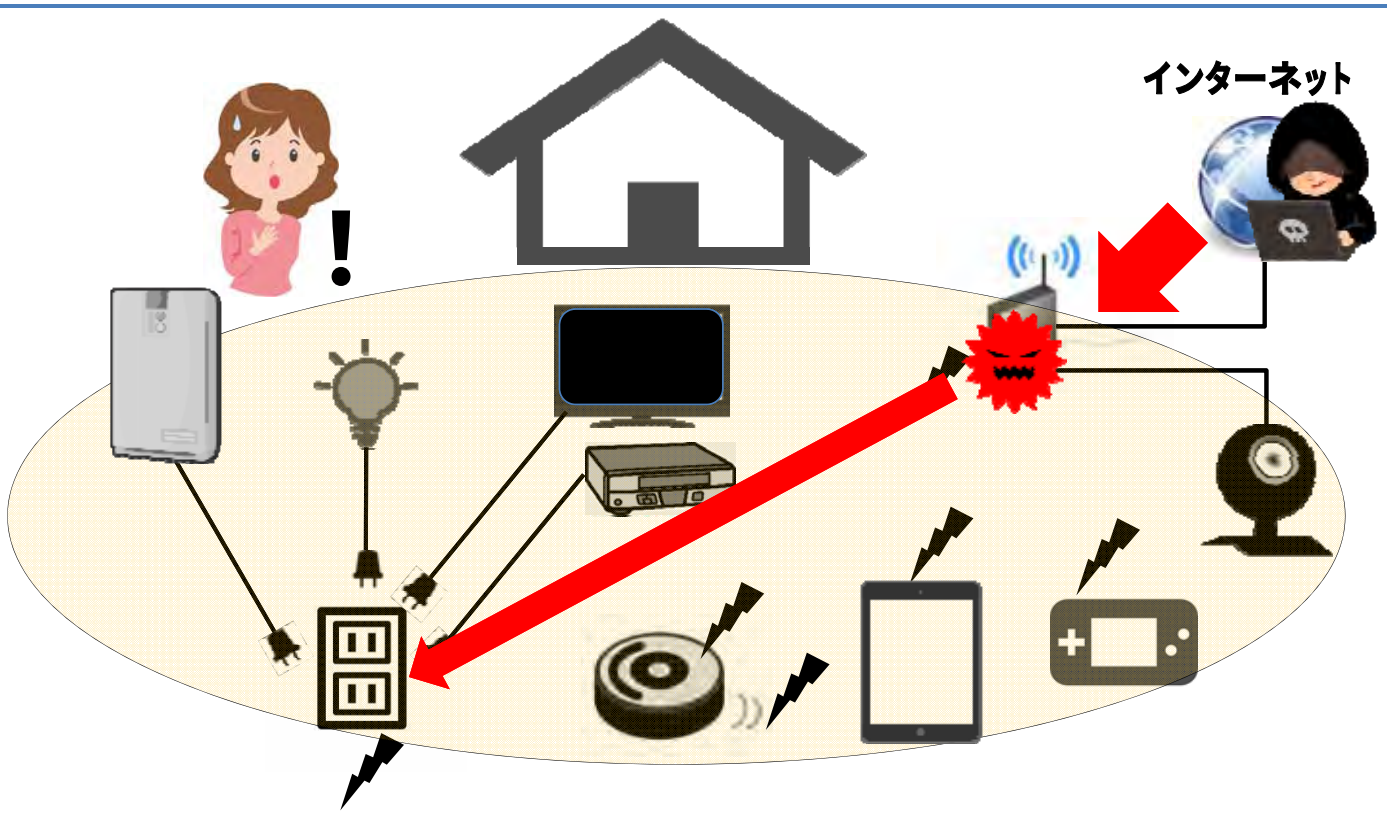
コネクテッドホーム試験室

インターネットから家庭への攻撃の観測



ルータを乗っ取った後に家庭内にさらに侵入するマルウェアも確認

疑似攻撃事例：
マルウェアによる機器の不正操作

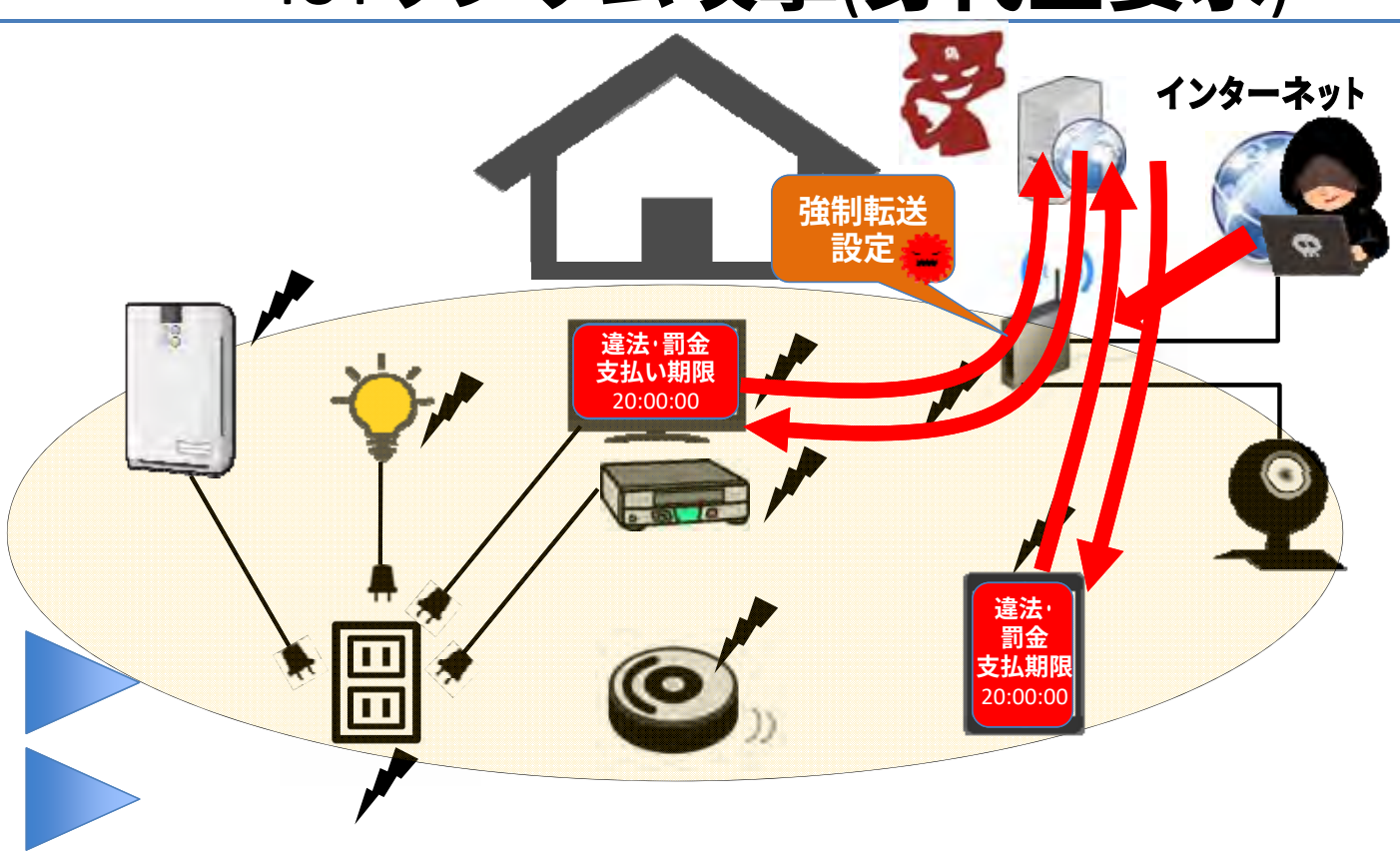


疑似攻撃事例：
マルウェアによる機器の不正操作

製品名	アプリケーション層プロトコル	ペイロードの可読性	操作機能	攻撃耐性
学習リモコン	独自プロトコル	あり，意味解釈も容易（ASCIIコードで記載）	TV電源ON/OFF	✕
			TV音量調整	✕
			TVチャンネル変更	✕
			エアコンON/OFF	✕
ロボット掃除機	MQTT	なし（SSLで暗号化）	掃除開始	○
			掃除一時中止	○
			掃除停止	○
スマート電源プラグ	独自プロトコル	なし（バイナリデータ）	電源ON	✕
			電源OFF	✕

「○」は機器に不正操作の攻撃を実施した際に、機器が動作しなかったことを意味する。（不正操作が失敗）
「✕」は機器に不正操作の攻撃を実施した際に、機器が動作したことを意味する。（不正操作が成功）

疑似攻撃事例：
IoTランサム攻撃(身代金要求)

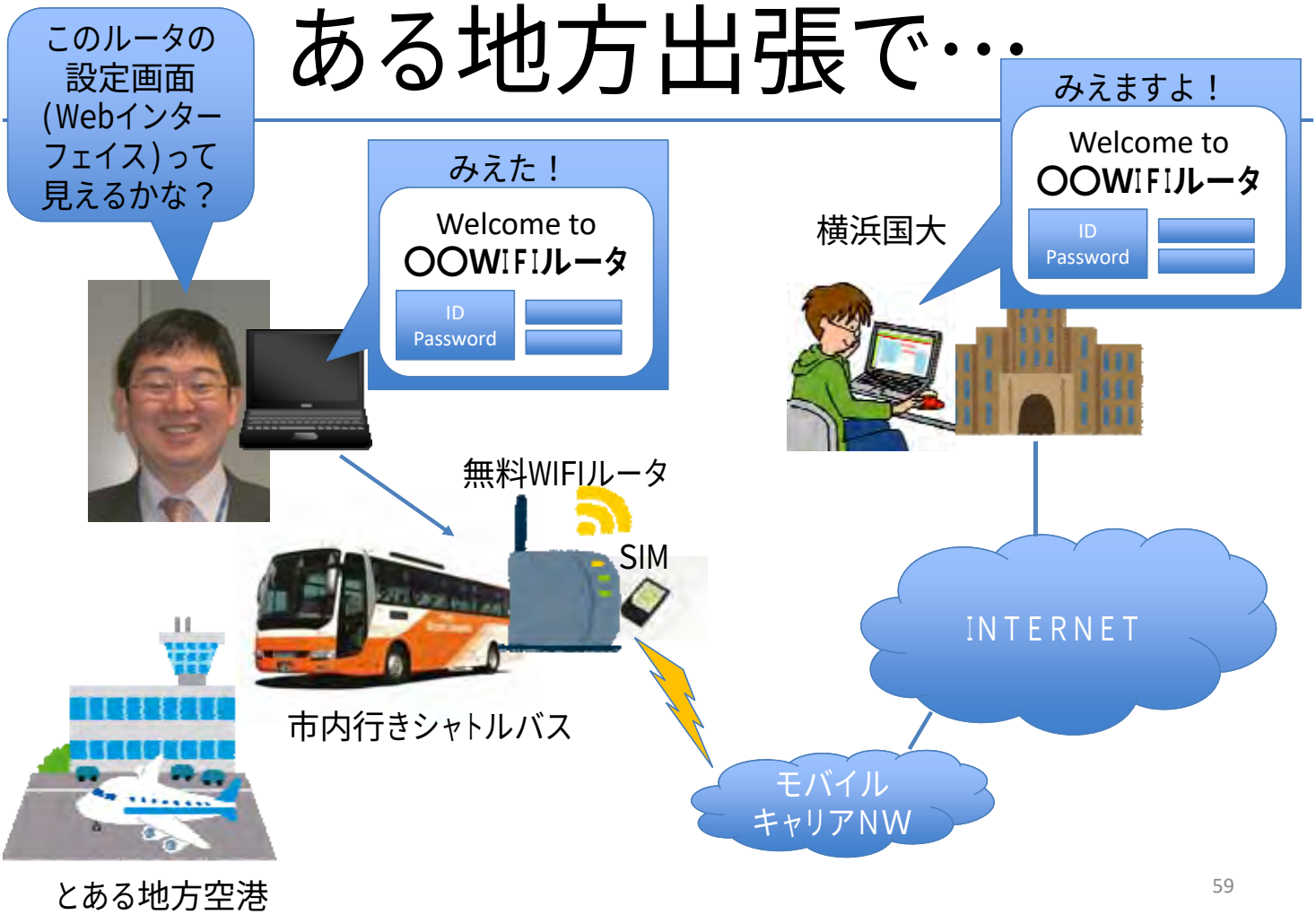


ここまでのまとめ

- IoT機器の大量マルウェア感染が深刻化
- 今後の脅威に関する予想（一部既に発生）
  - 侵入方法の多様化
    - Telnet以外も攻撃
  - 攻撃規模の巨大化
    - 1T強のDDoSが上限とは言い切れない
  - 目的の多様化
    - 攻撃の収益化（Monetization）がポイント
    - 収益につながらない攻撃（機器破壊など）もある

重要IOTシステムのアクセス制御不備問題

ある地方出張で…



ある地方出張で…

この空港シャトルバスのWIFIルータは
1）設定画面に世界中からアクセス可能
2）設定画面からルータ型番特定可能
3）ルータ型番からオンラインマニュアル取得可能
4）オンラインマニュアルにはデフォルトID／PASS記載
→世界中から設定変更される恐れあり
→キャッシュDNS設定を変えられたら乗客のアクセス先が漏えい、
フィッシングも可能（ダークホテルならぬ、ダークバス？）

インターネット側からＷｅｂインターフェイスにアクセス可能な機器等の調査

国内アドレスレンジにおいて

1）ミシガン大学のCensysを利用した調査

2）独自の探索による調査

を実施し、インターネット側からWebインターフェイスにアクセス可能な機器やシステムを特定

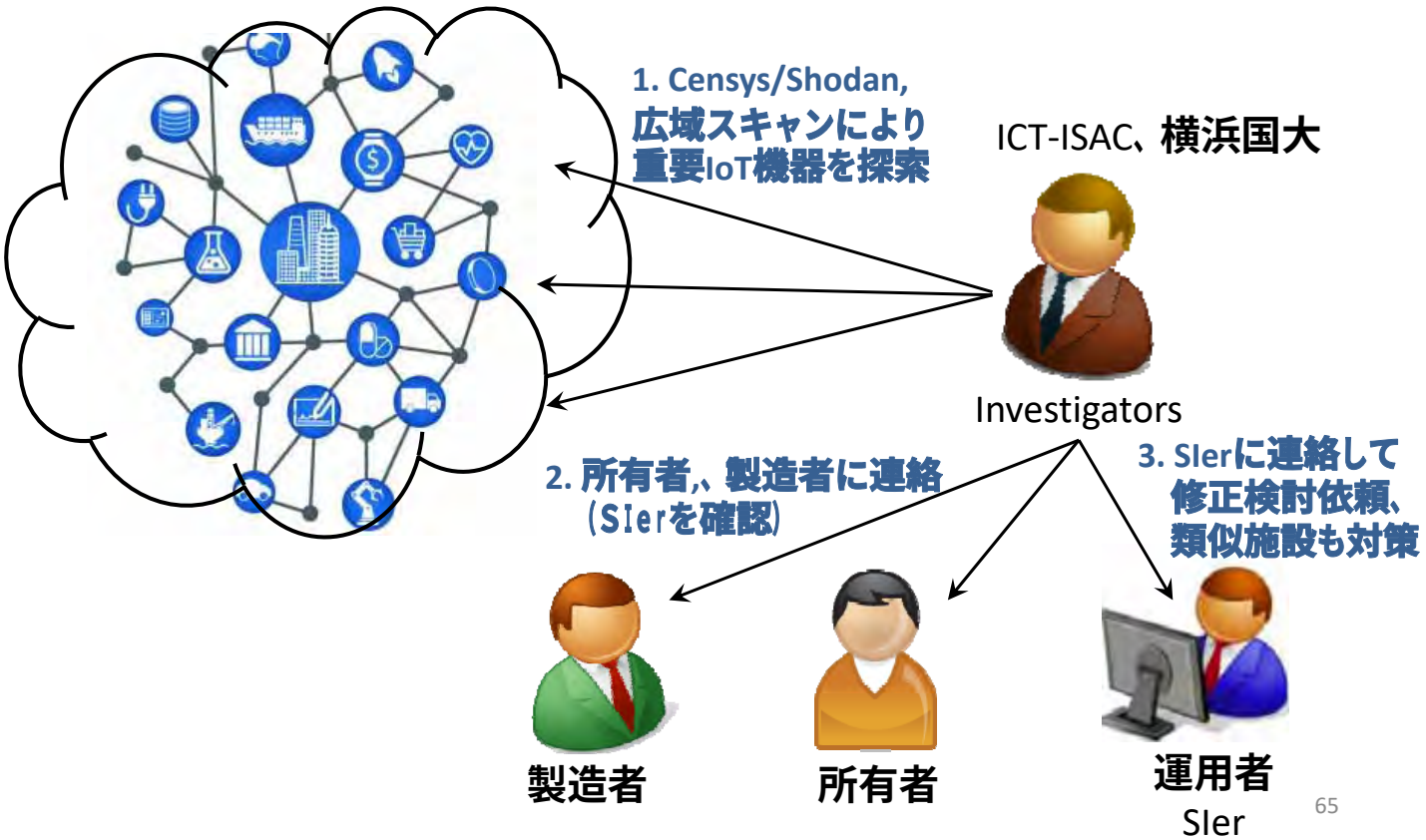
調査の結果わかったこと

多くの末端IoT機器のWebインターフェイス（設定、操作画面）に以下の問題が存在

- デフォルトでグローバルからアクセス可能
- 認証が弱い（ユーザ名固定、パスワード空間が狭い）、またはそもそも認証が要らない
- デフォルトID／ＰＡＳＳが調査可能
  （意図して公開しているのでなければ、デフォルトのままの可能性も十分考えられる）

クラウド側のインターフェイスが簡単に探索できるようになっており、サービス妨害攻撃の対象となる恐れがある

総務省 重要IoT機器の調査



対策について

デバイス大量感染の元凶はTelnet

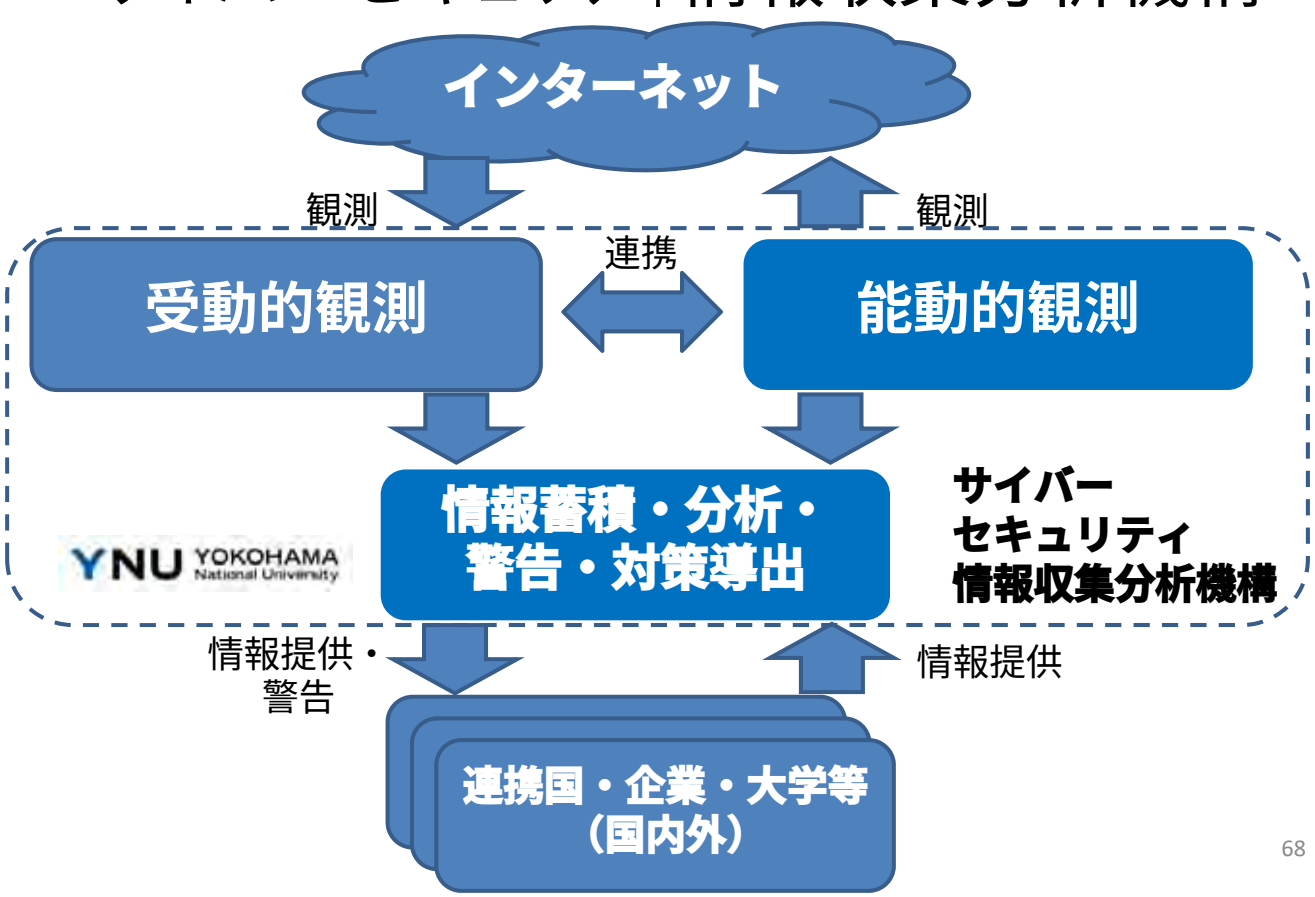
多様なはずのIoTデバイスが
Telnetという共通のセキュリティ問題を
共有してしまっている

＜現状のギャップ＞
・製造者側・利用者側は認識していない

・攻撃者側は認識している
(ネットワーク攻撃の5割以上がTelnet)

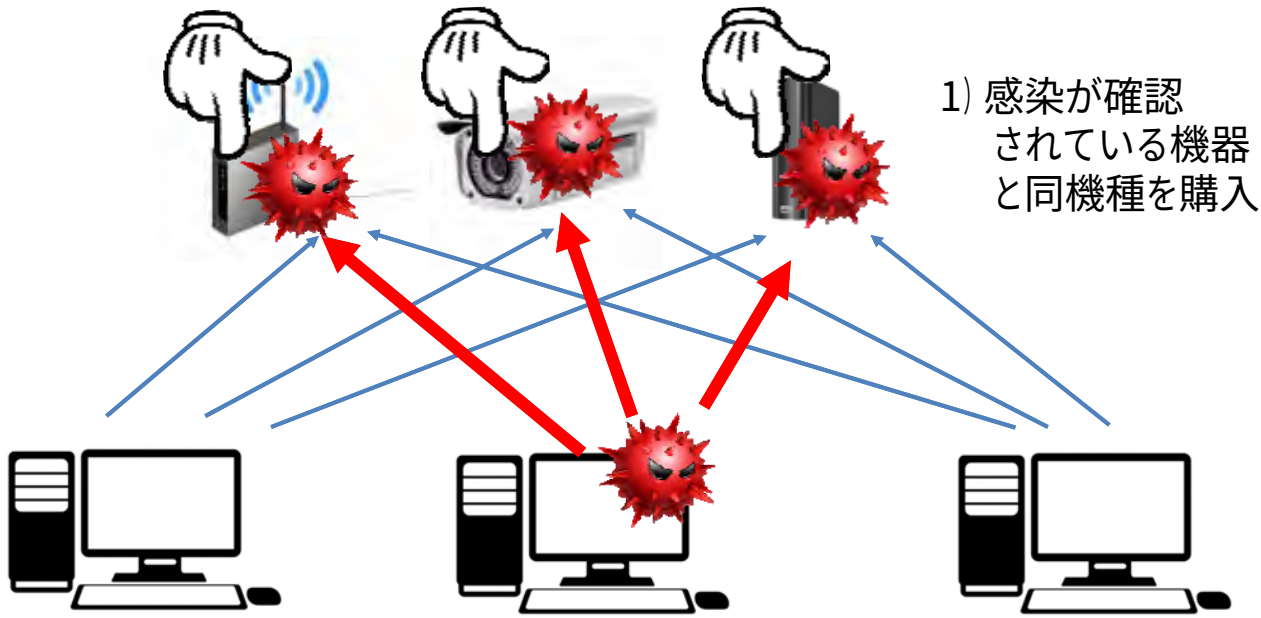
**脆弱機器・感染状況・脅威の変遷の
正確な把握・情報提供が必要**

能動的観測と受動的観測を融合させた サイバーセキュリティ情報収集分析機構



IoTマルウェア駆除実験

4) 電源切、コマンドによるシステムリブート、工場出荷状態に戻す、など**操作**を実施



1) 感染が確認されている機器と同機種を購入

2) 通常使用時のファイルシステム、プロセスを記録

3) 実IoTマルウェアで攻撃、感染の確認（C2通信など）

5) 感染前と比較して感染状態が修復されているか確認

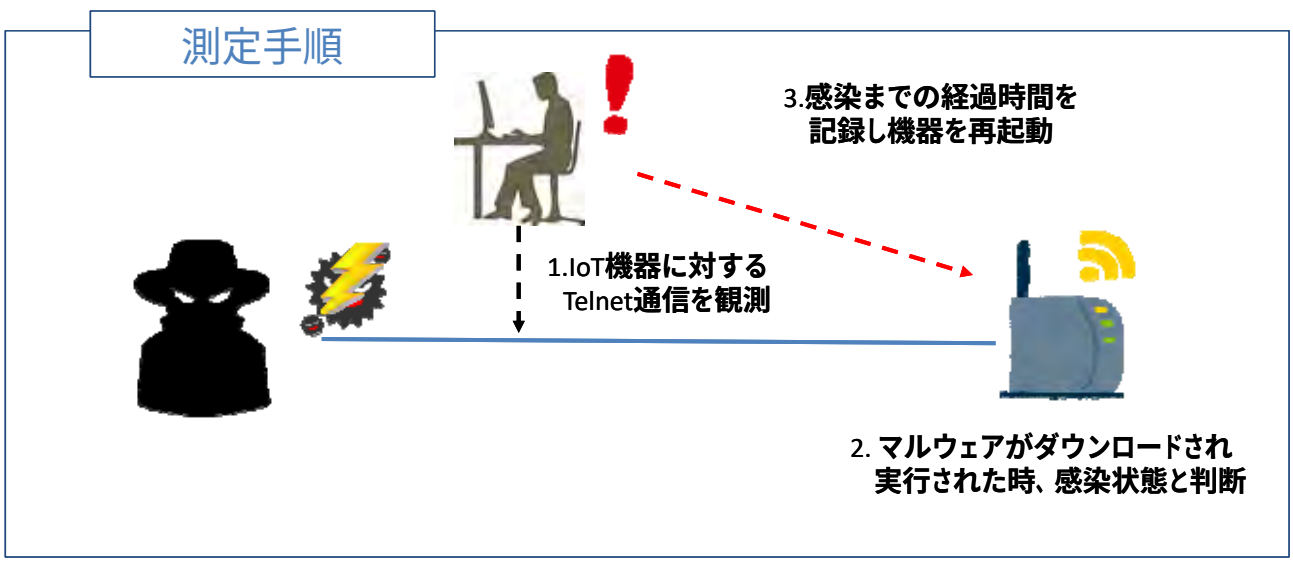
駆除実験結果

機器	種類	電源再起動による マルウェアの挙動
A	IP Camera	プロセス・バイナリともに消滅
B	プリンター	プロセスのみ消滅 バイナリは残る
C	ルータ	プロセス・バイナリともに消滅
D	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅
E	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅
F	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅
G	衛星放送受信機	プロセス・バイナリともに消滅

いずれの機器でも主電源による再起動と
工場出荷状態の復元の操作によりマルウェア駆除が可能
特に主電源による再起動では機器設定を
初期状態に戻すことなく駆除が可能であった

駆除後の再感染時間の測定

- マルウェア駆除後、感染原因を改善しなければ容易に再感染する恐れがある
- そこで駆除実験後、各機器をインターネットに接続し再びマルウェアに感染するまでの時間を観測した



感染時間観測結果

	1回目	2回目	3回目	平均
IPカメラA	48時間経過しても感染せず	← Telnet認証に3回失敗すると30分ログイン不可となる機器の機能による影響だと考えられる		
プリンターB	15分24秒	16分40秒	24分57秒	19分0秒
ルータC	38秒	3分55秒	58秒	1分50秒
Wi-Fiストレージ D	30分1秒	8分14秒	5分30秒	14分35秒
Wi-Fiストレージ E	18分59秒	73分3秒	49分25秒	47分9秒
Wi-Fiストレージ F	8分	57分49秒	47分22秒	37分47秒
衛星放送受信機G	1分46秒	5分59秒	9分	5分35秒

IPカメラAを除く6種類の機器では最短で38秒、最長でも73分で感染した
また、3回の測定の平均をとるとすべて1時間以内であり対策を講じていない機器では短時間で感染してしまうことがわかった

ファイルシステムによる差異

機器	種類	電源再起動による マルウェアの挙動	ファイルシステム
A	IP Camera	プロセス・バイナリともに消滅	不明
B	プリンター	プロセスのみ消滅 バイナリは残る	UBIFS （※読み書き可能）
C	ルータ	プロセス・バイナリともに消滅	squashfs （※読み取り専用）
D	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅	squashfs （※読み取り専用）
E	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅	squashfs （※読み取り専用）
F	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅	squashfs （※読み取り専用）
G	衛星放送受信機	プロセス・バイナリともに消滅	cramfs （※読み取り専用）

読み取り専用ファイルシステムでは、
調査対象のマルウェア(Mirai等)は再起動で消滅

永続感染マルウェアの可能性

読み書き可能ファイルシステムのため、
通常のＰＣマルウェアと同様に永続感染可能

機器	種類		
A	IP Camera	プロセス・バイ[illegible]もに消滅	不明
B	プリンター	プロセスのみ消滅 バイナリは残る	UBIFS （※読み書き可能）
C	ルータ	プロセス・バイナリともに消滅	squashfs （※読み取り専用）
D	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅	squashfs （※読み取り専用）
E	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅	squashfs （※読み取り専用）
F	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅	squashfs （※読み取り専用）
G	衛星放送受信機		

偽ファームウェアへの更新が容易に可能、
永続感染マルウェア発生の恐れ

紹介事例からわかること

機器個別の対策は技術的に容易

Telnetを出荷前・設置前・使用前に止める
ID/PASSWORD設定を徹底
脆弱性修正とファームウェア更新

対策の徹底は困難（運用の問題）

製造者・設置者・利用者が多様な分野・地域に分散
個体数が多い、販売後追跡が困難
強制ファームウェア更新が不可能、寿命が長い
攻撃を助長する恐れのある行き過ぎた情報共有
（Shodan、Insecamなど）

IoTのセキュリティ向上（国内向け）

状況把握（定常的に実施）

- サイバー攻撃観測網（ハニーポット等）による感染機器把握
- 能動的観測機構（日本版Shodan/Censys）による機器状況の把握
- 機器情報、脆弱性情報の集約（メーカ、運用者、研究者窓口）

緊急性高

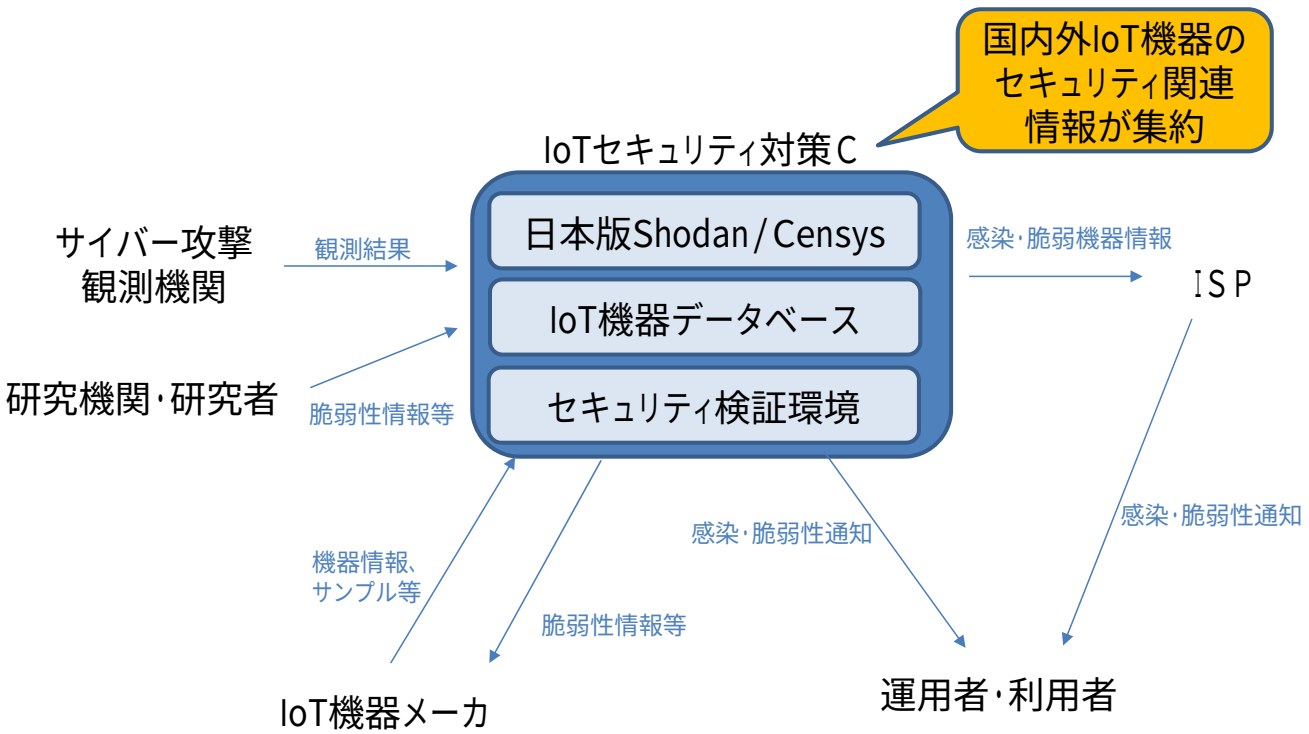
短期的対策

- ISPによる通知、ブロック、切り離しなど
- メーカ、運用者、所持者への情報提供、対策の促し

中長期的対策

- ガイドライン・認証制度（検証環境構築）
- セキュアなプラットフォーム（セキュリティバイデザイン）
- IoTセキュリティゲートウェイ

IoTのセキュリティ向上（国内向け）



まとめ

- IoT機器の大量感染が深刻化しており、マルウェア感染した機器を悪用した大規模サービス妨害攻撃が顕在化している
- 大規模マルウェア感染だけでなく、設定画面のアクセス制御などもずさんな機器が多い
- 実施の容易なグローバルからの攻撃だけでなく、ローカルからのIoT水飲み場攻撃（標的型攻撃）に悪用される恐れもある
- IoT特有の産業構造（多様な製造者）や実情（膨大な機器、管理不可能性、長寿命）から上記の傾向がメーカの自助努力のみで現状が自然回復（改善）するとは考えにくい
- マルウェア感染や、脆弱性を有するIoT機器の現状を正確に把握し、実効的な対策を行うための体制づくりが急務

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

謝辞1：本研究の一部は総務省委託研究「国際連携による
サイバー攻撃予知・即応技術の研究開発(H23-H27)」の
成果として得られたものです。
謝辞2：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-H30)」の支援を受けて行われたものです。