(ISC)² Secure Events

SECURE TOKYO 2017

Cyber Attack in IoT on the rise
- さらに増えているIoTへの攻撃の現状 -

中尾　康二

NICT 主管研究員

横浜国大　客員教授

内閣官房　NISC　サイバーセキュリティ補佐官

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
be more 25 billion devices

Home Router Botnet Leveraged in
Large DDoS Attack

Is your refrigerator really part of a massive
spam-sending 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 conce
boost in IoT services

by

News roundup: As Internet of Things conce
rise reality, one vendor is quick to
to combat the risks. Plus: 1% of use
e risk; Target pays up; Apple devic
ly secured in the enterprise.

(ISC) Secure Events

RISK ASSESSMENT / SECURITY & HACKTIVISM

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

IoT機器の
大量マルウェア感染
が既に発生している

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

感染機器の種別の例

- 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
  - 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
  - LCDディスプレイ制御シス



- 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

- 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
  - 指紋スキャナ



デバイスはWebおよびTelnetの応答から判断しています.

大量感染の根本原因は？

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。

やはり、多くの機器で”Telnet”が動いています

```
B[redacted]5328 Broadband Router
```

```
ope[redacted]i.3.0.dm800se
```

```
Net[redacted]r login:
```

```
TL-[redacted]40N login:
```

```
[redacted]20-VoIP-AG login:
```

```
BC[redacted]328 xDSL Router
```

```
B[redacted]5328 ADSL Router
```

```
Router [redacted] User Access Verification
```

```
[redacted]800se.login:
```

```
[redacted]dvs.login:
```

```
adv[redacted]s login:
```

```
[redacted]vision login:
```

```
[redacted]x00 login:
```

```
Air[redacted]v2 login:
```

インターネット上の任意のホストからアクセス可能なTelnetサービスのバナーの例

しかも多くは
デフォルト/弱いパスワードで

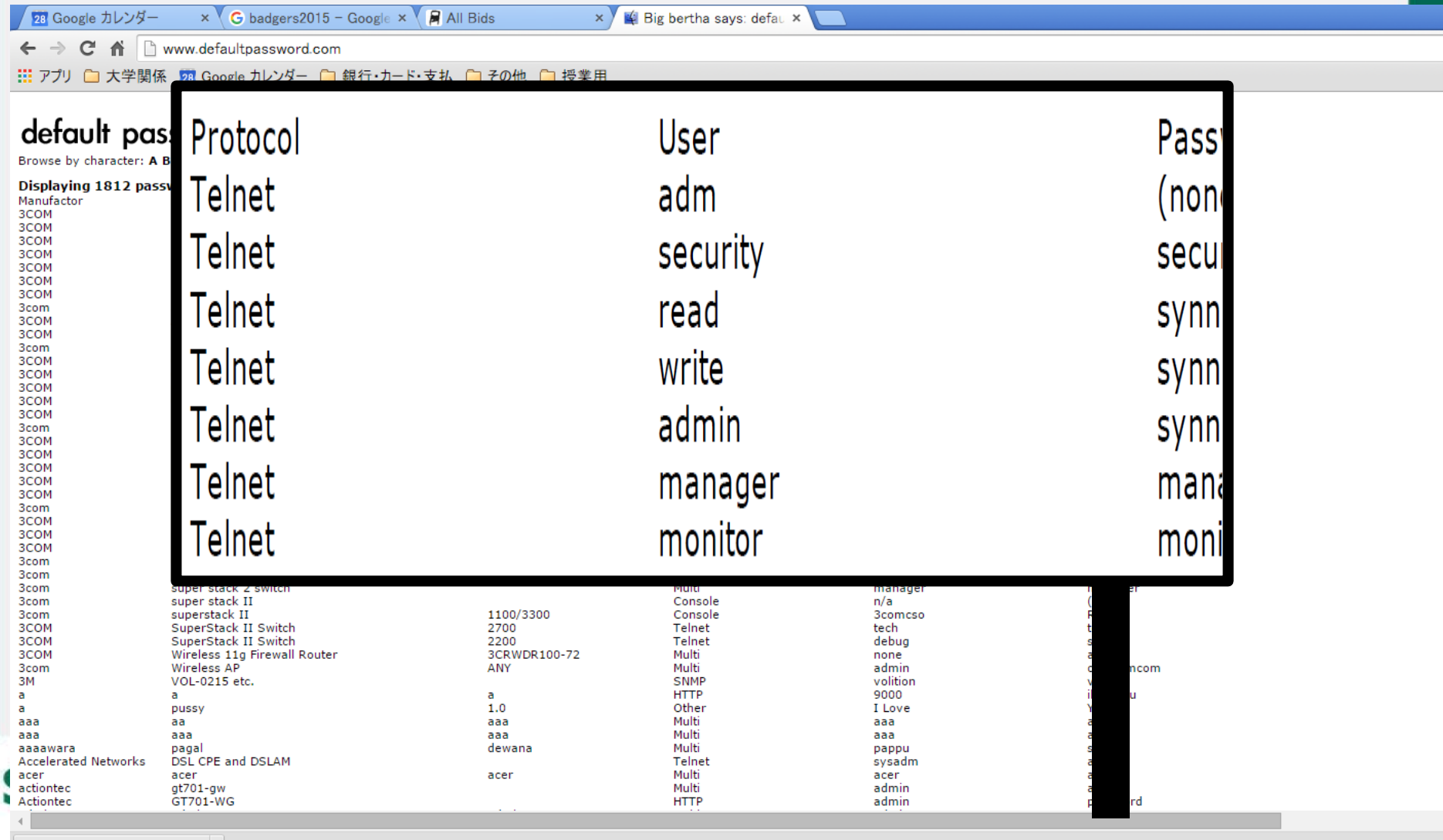
```
[shogo@www9058up ~]$ telnet x.x.243.13
Trying x.x.243.13...
Connected to x.x.243.13.
Escape character is '^]'.

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

リモートログイン成功

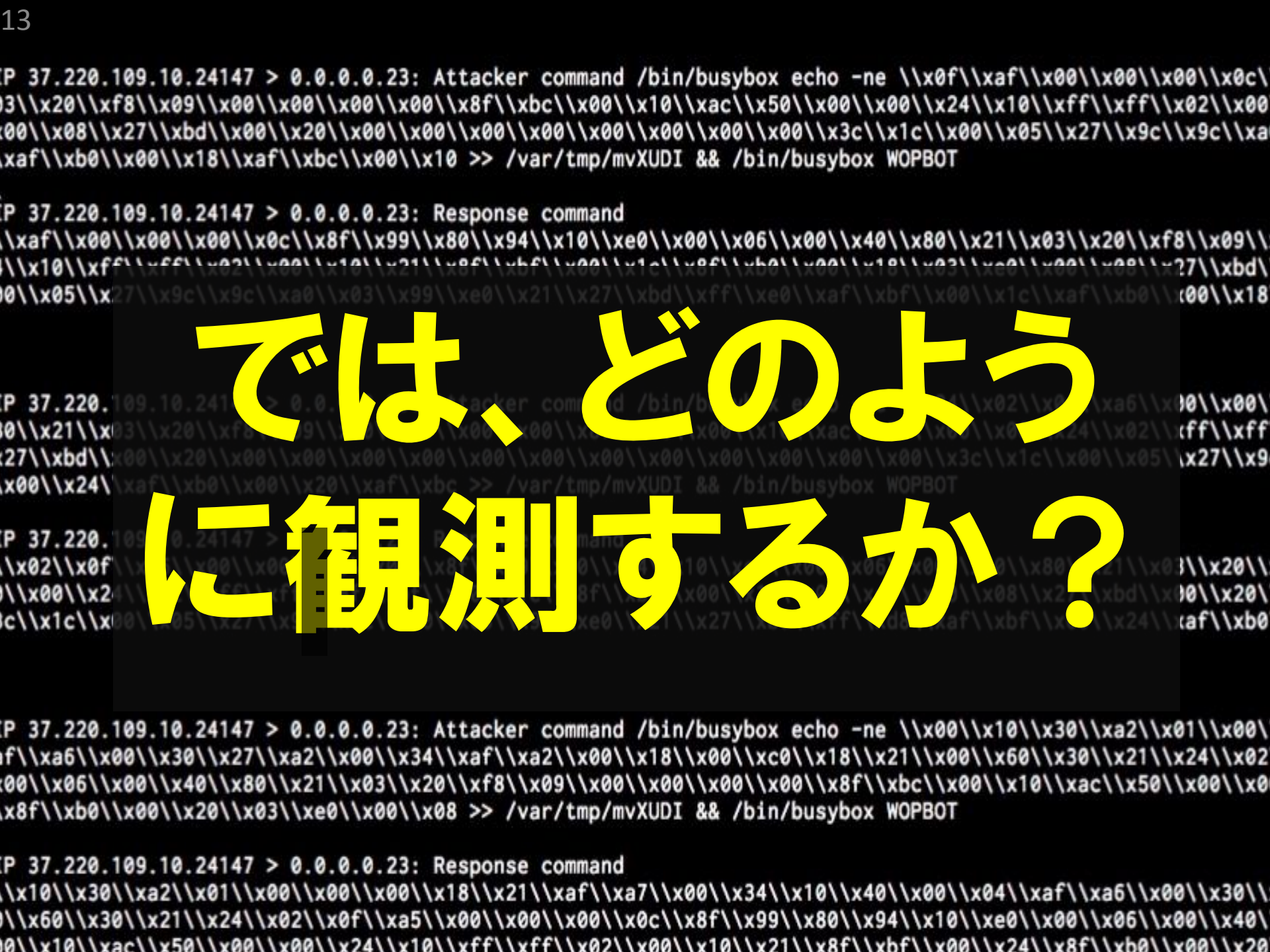
```
BusyBox v1.1.2 (2007.05.09-01:19+0000) Built-
in shell (ash)
Enter 'help' for a list of built-in commands.
```

“default” “password” “list”などで検索すると



なぜIoT 機器が感染？？

- **24/7** オンライン
- **AV**がない
- 弱い/デフォルトの**ID/PW**の使用
- グローバル **IP** を持ち、インターネットへの接続を開いている



では、どのように観測するか？

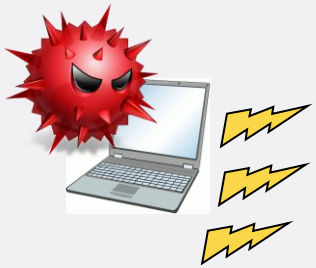
攻撃の観測のための2つのアプローチ

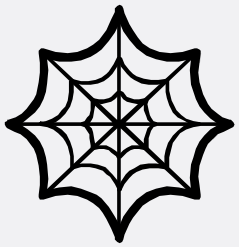
» （これまでの）受動（passive）型：
観測用ネットワークで攻撃が来るのを待つ
- ダークネットモニタリング
- ハニーポット

» 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

受動型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

ダークネットで何が見えているのか？

●マルウェアによるスキャン

- ✓ ワーム型マルウェアの探索活動
- ✓ マルウェア感染の大局的傾向
- ✓ 感染爆発の前兆

●DDoS攻撃の跳ね返り

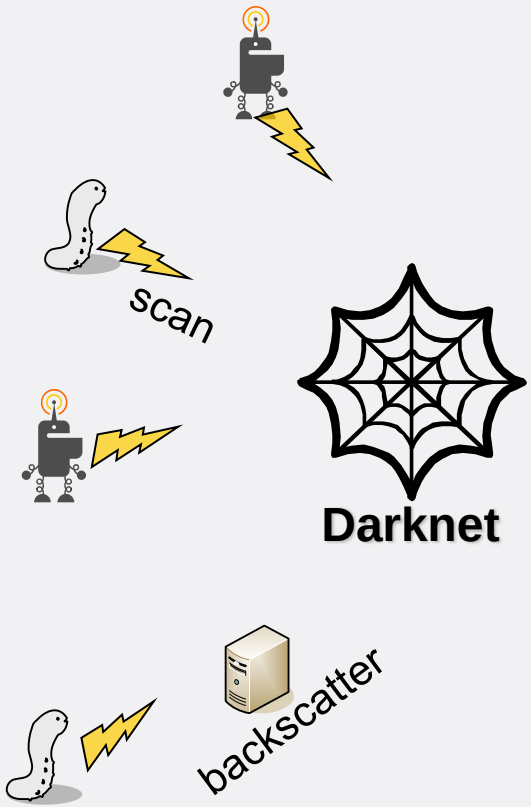
- ✓ 送信元IPアドレス偽装されたSYN Flood
- ✓ 被攻撃サーバからの応答（SYN-ACK）
- ✓ DDoS攻撃の早期検知（1パケット目から）

●リフレクション攻撃の準備活動

- ✓ DNS Open Resolver探索
- ✓ NTP探索　　etc.

●設定ミス

- ✓ 組織内ダークネット

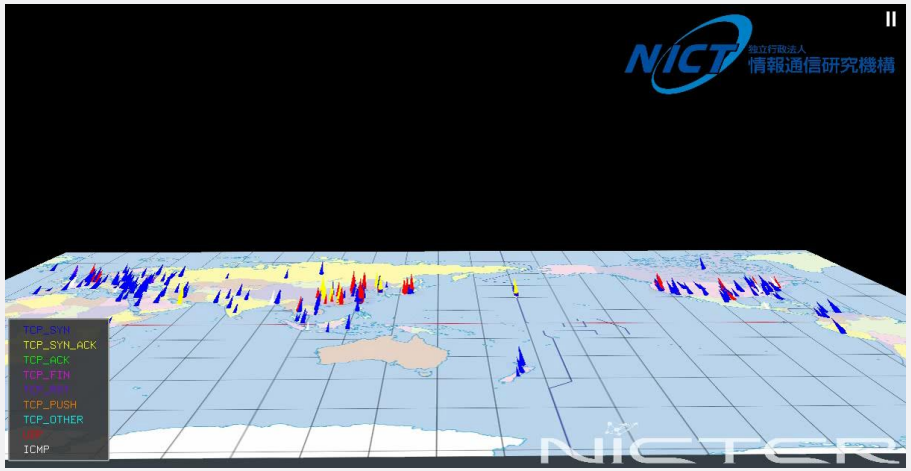


nicter-Atlas（ダークネット観測システム）によるスキャンの現状把握

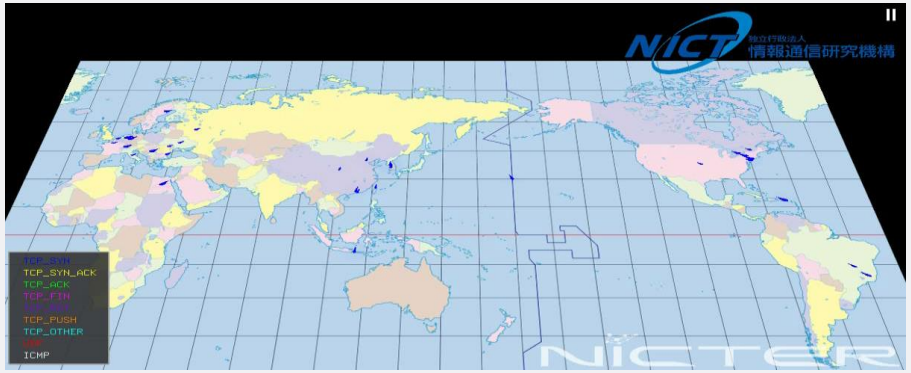
最近は, “Port 23 (telenet)へのスキャン” が増えている!!

- ダークネットに来るパケットを実時間で捕捉。
- 可視化におけるパケット色は、プロトコルタイプを表現。

- **UDP**
- **TCP SYN**
- **TCP SYN/ACK**
- **TCP Other**
- **ICMP**

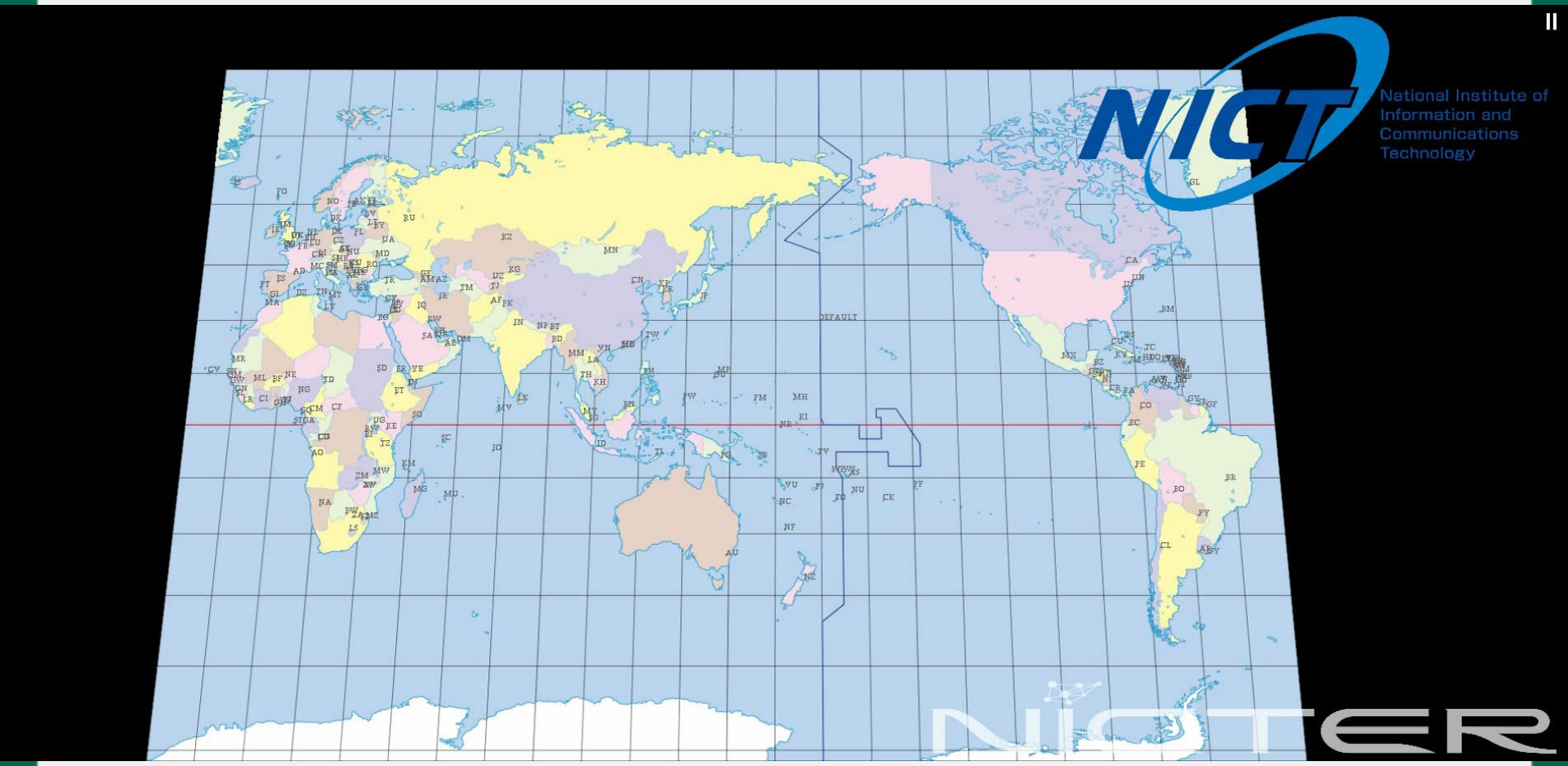


Atlas All view



Atlas only port23

IoT攻撃に関連するポート群へのスキャン（ポート23へのスキャンを含む）



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%
443	[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

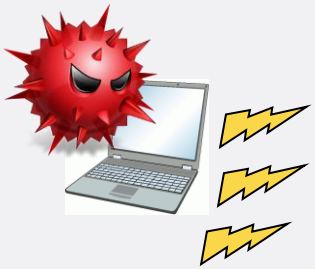
1/1/2005 1/1/2006 1/1/2007 1/1/2008 1/1/2009

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）

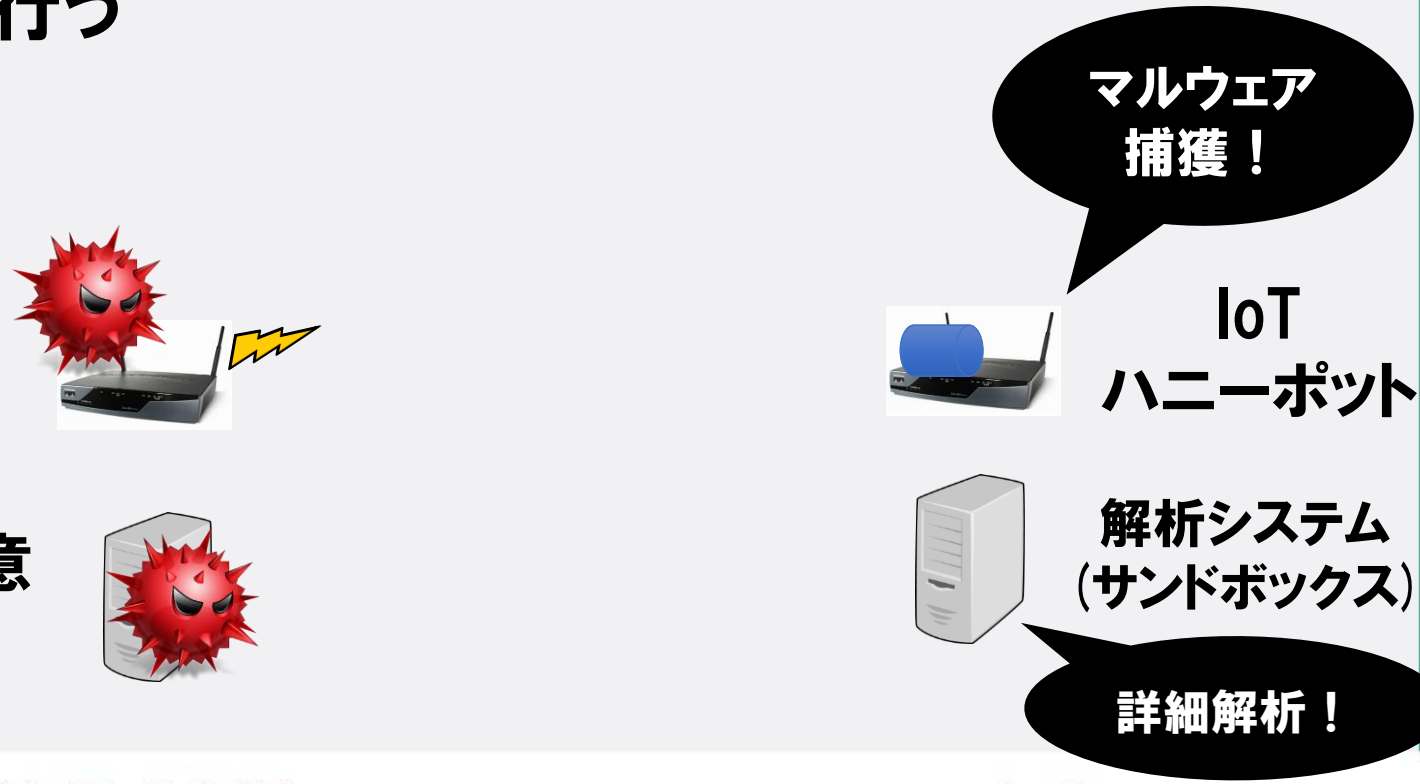
より詳細に攻撃を分析するために

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）のみの観測であるため、
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

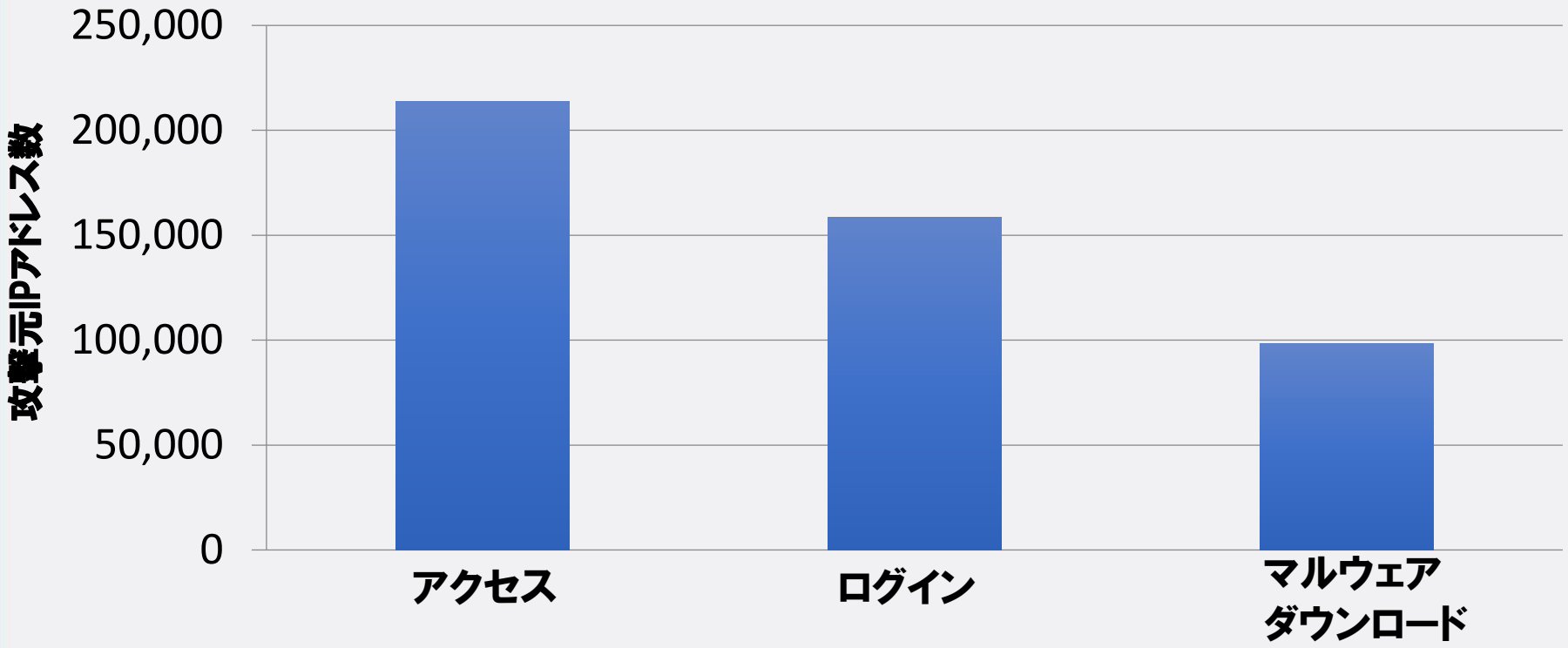
脆弱な機器を模擬した**囮システム（ハニーポット）**により攻撃元と通信を行い、攻撃の観測・マルウェア捕獲し、詳細解析を行う



ハニーポットでの観測結果

観測期間：2015/4/1～2015/7/31（122日）

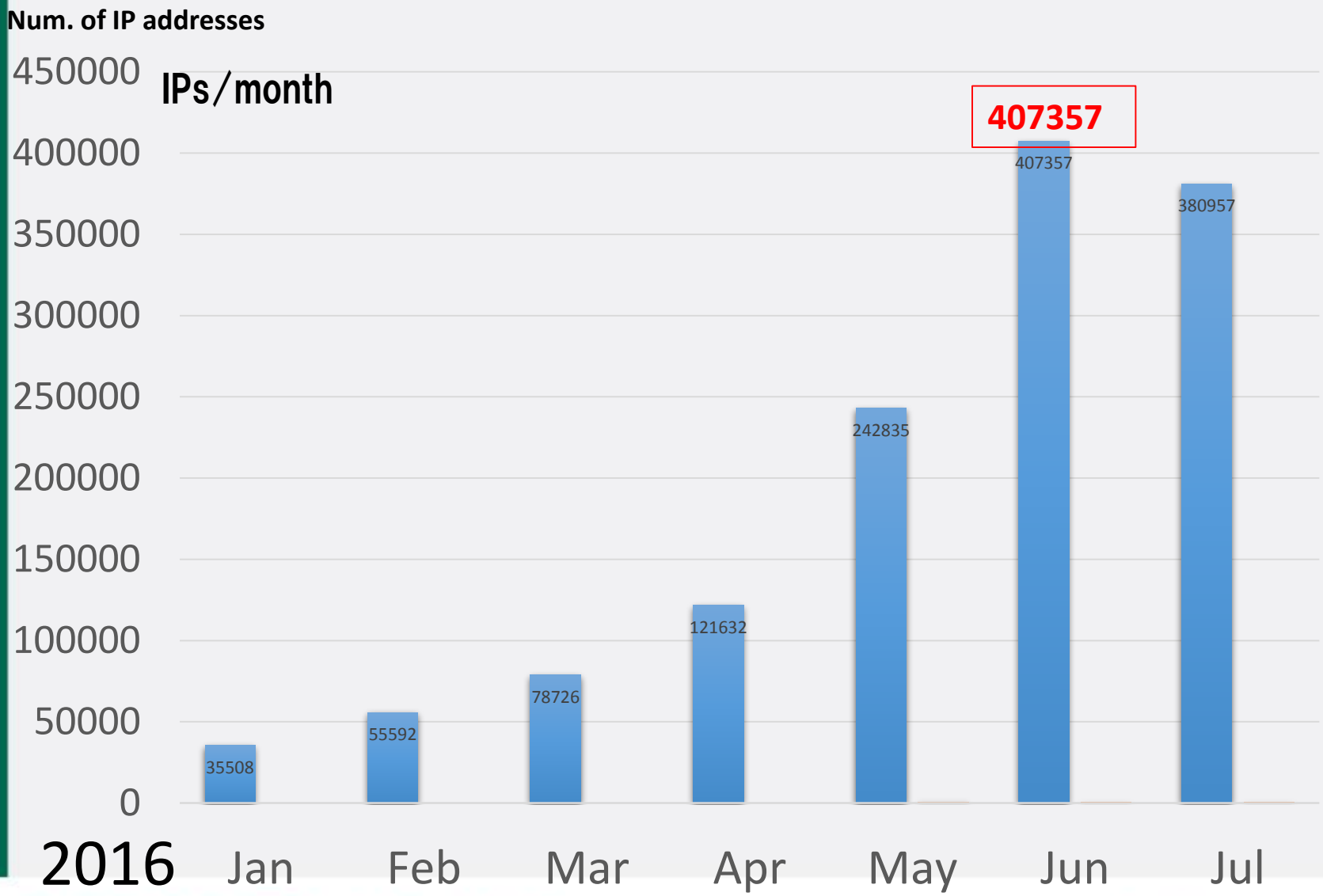
国内148 IPアドレスを観測に使用



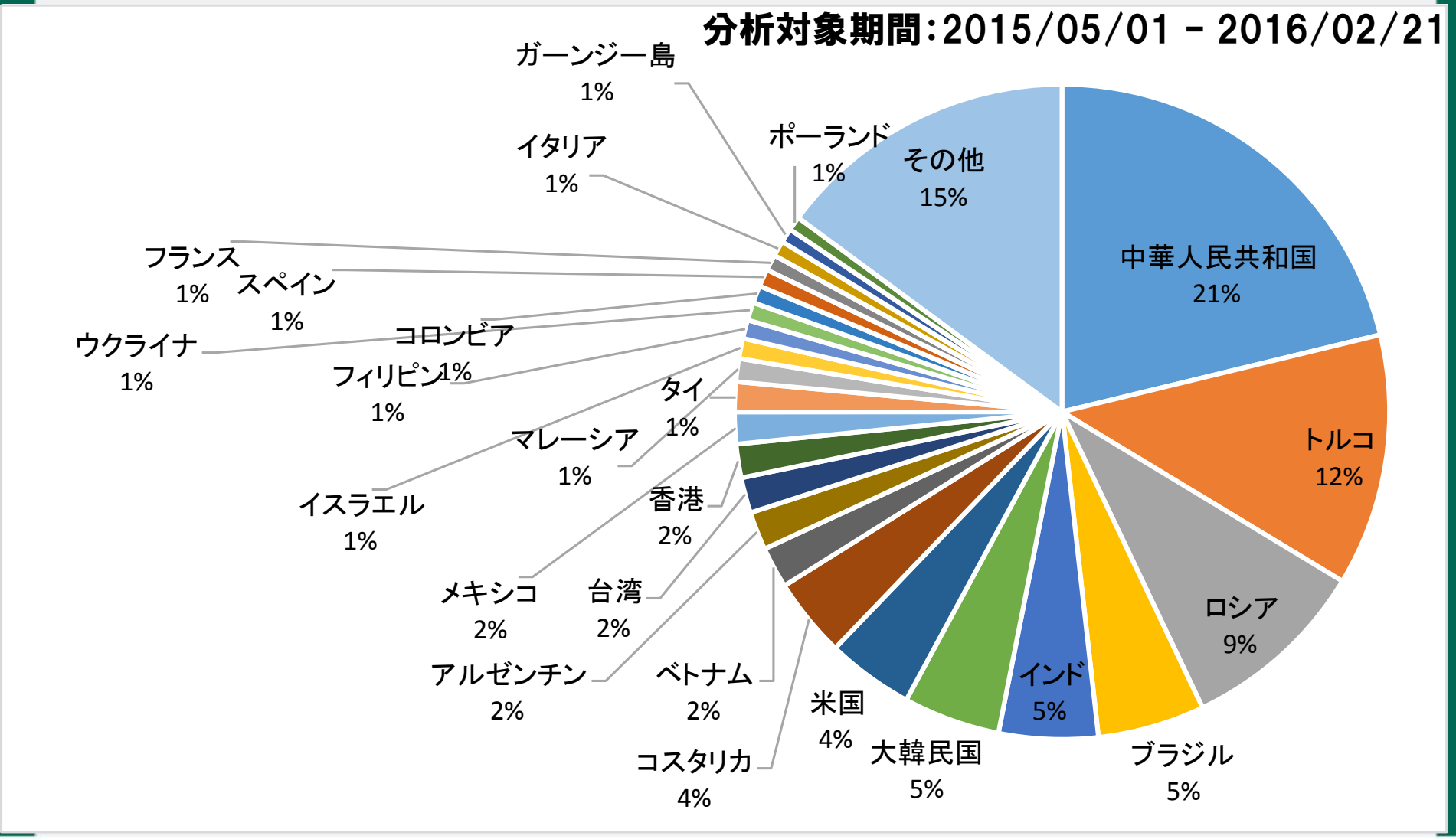
約15万アドレスから不正ログインを検出し、90万回のマルウェアダウンロード試行を観測

11種類のCPUアーキテクチャ向けマルウェアを捕獲

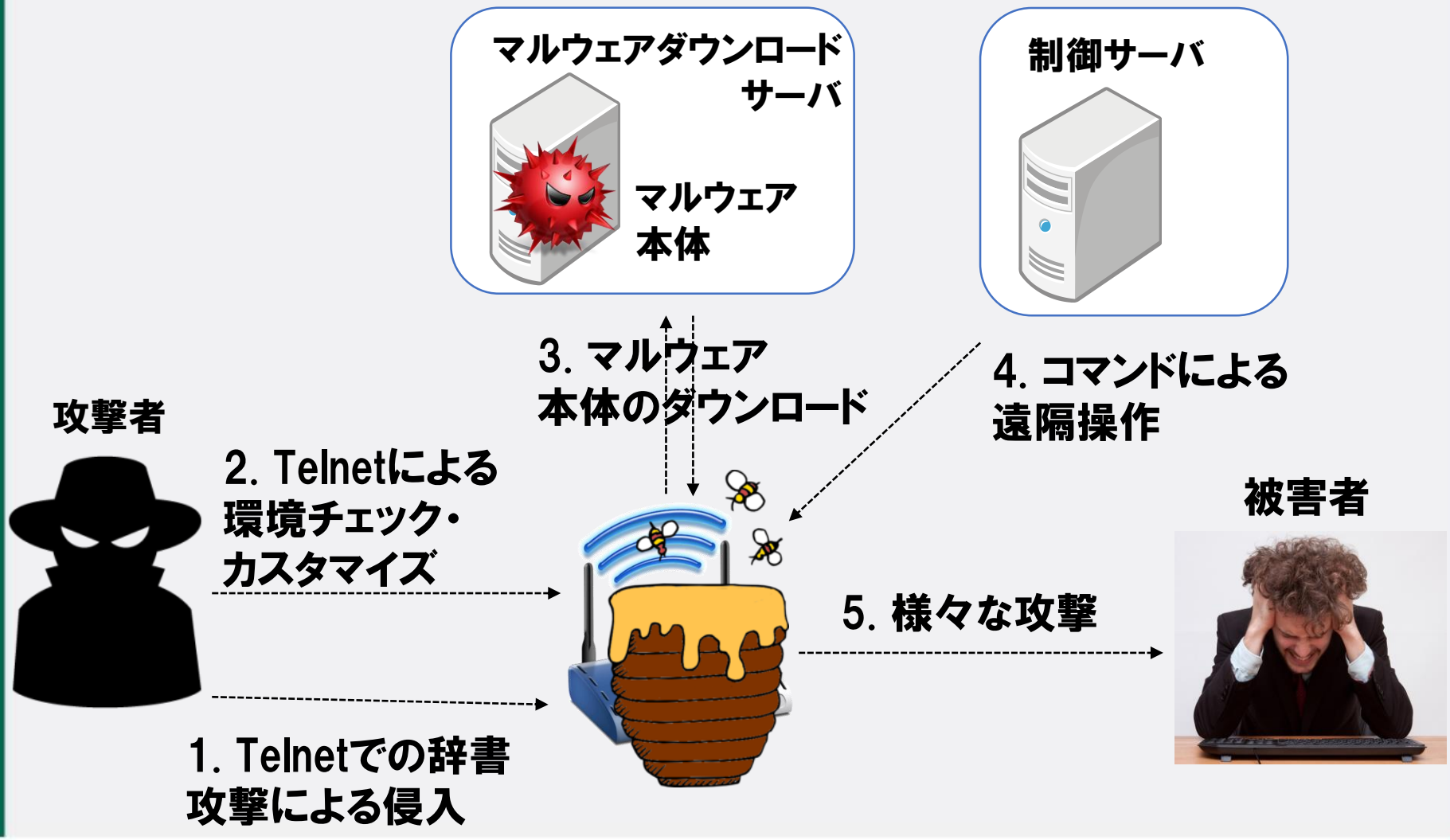
2016年はさらに攻撃が増加



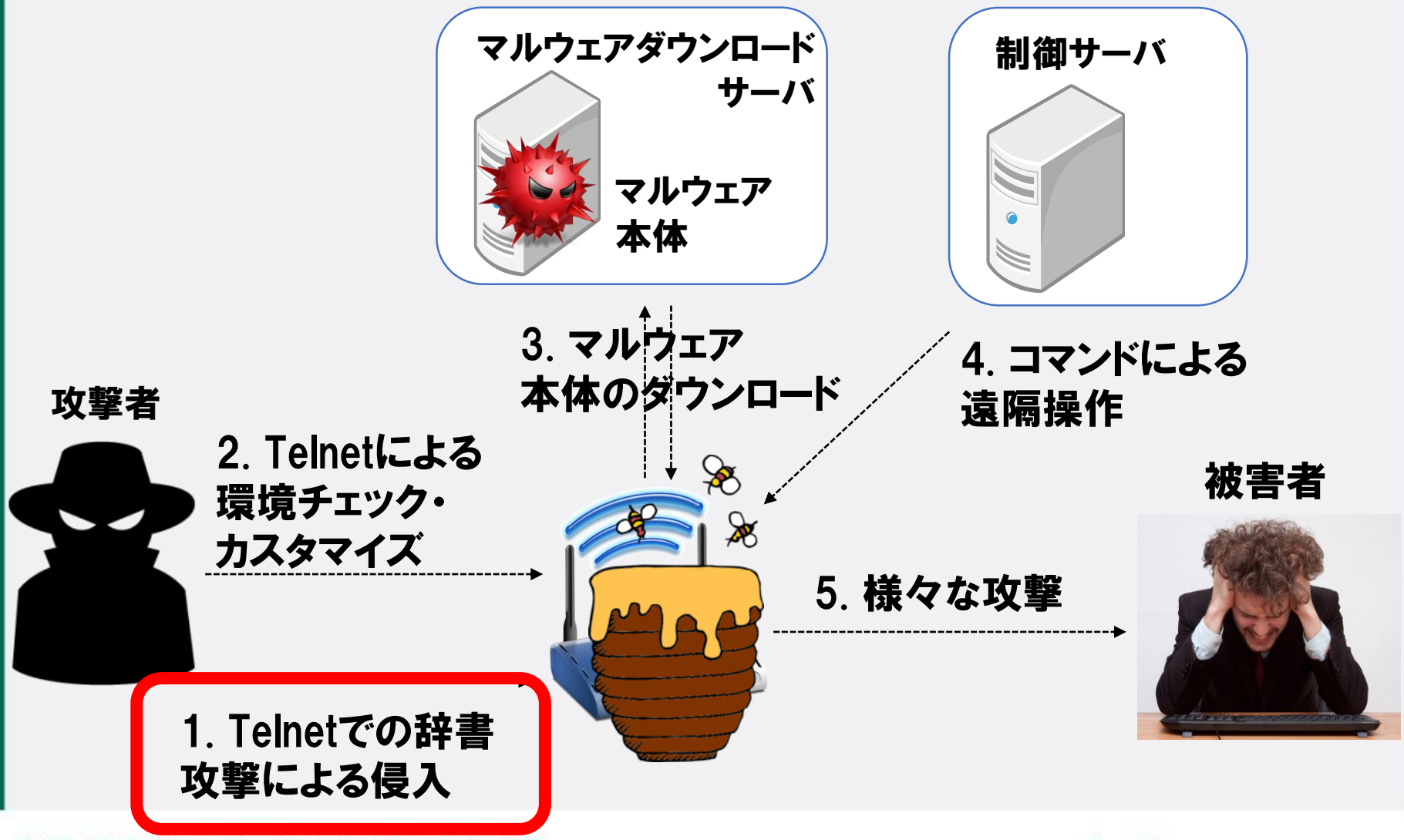
国別の感染状況


分析対象期間:2015/05/01 - 2016/02/21
中華人民共和国 21%
トルコ 12%
ロシア 9%
ブラジル 5%
インド 5%
大韓民国 5%
米国 4%
コスタリカ 4%
ベトナム 2%
アルゼンチン 2%
メキシコ 2%
台湾 2%
香港 2%
イスラエル 1%
マレーシア 1%
タイ 1%
フィリピン 1%
コロンビア 1%
ウクライナ 1%
フランス 1%
スペイン 1%
イタリア 1%
ガーンジー島 1%
ポーランド 1%
その他 15%

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 in
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/a in
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

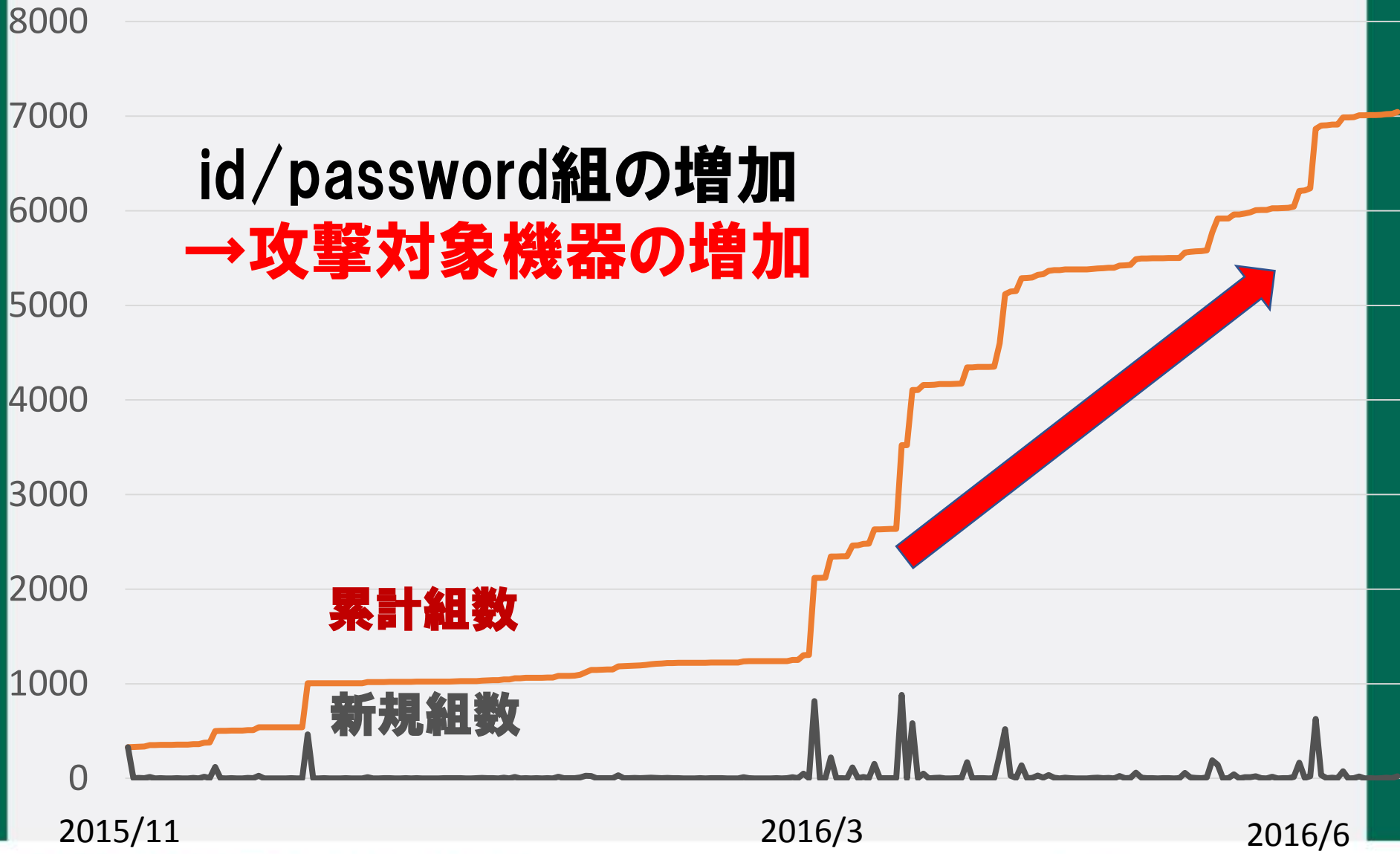
固定順序攻撃パターン3

admin/a in
admin/ 729
admin/ f6h3
admin/ yporra
admin/ 297
admin/ m0r
admin/ 4
root/12

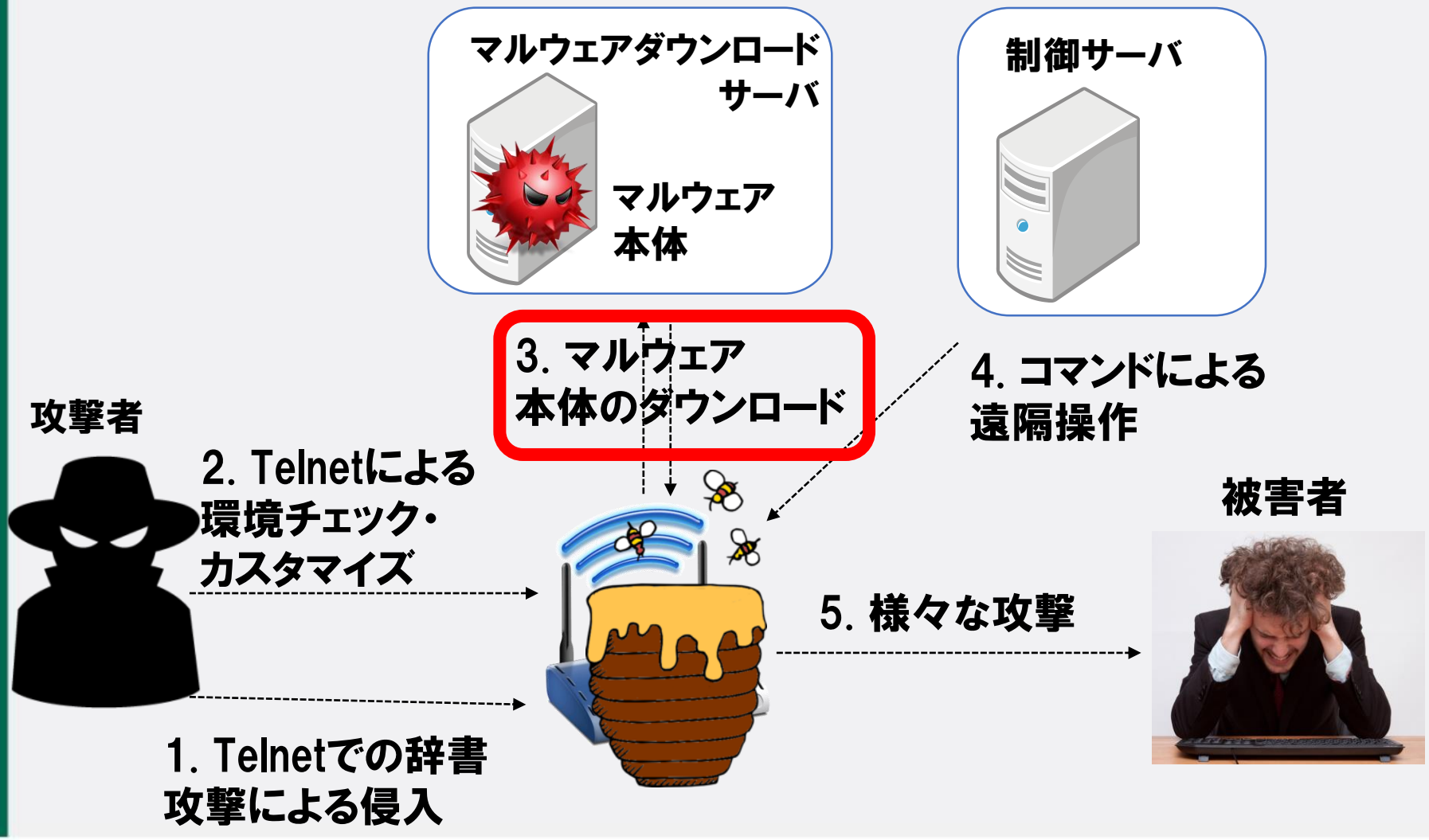
順序変更型攻撃パターン3

root/ t
root/ r
root/a in
root/ r
….

攻撃に利用されるid/password組の増加



Telnetベースのマルウェア感染の流れ



マルウェアのバイナリーDLの例

```
cat m68k > busybox; rm m68k; cp busybox systemr; rm busybox; ./systemr && sleep 1
cat mips > busybox; rm mips; cp busybox systemr; rm busybox; ./systemr && sleep 1
cat mipsel > busybox; rm mipsel; cp busybox systemr; rm busybox; ./systemr && sleep
t arm > busybox; rm arm; cp busybox systemr; rm busybox; ./systemr && sleep 1
cat arm7 > busybox; rm arm7; cp busybox arm7; rm busybox; ./arm7 && sleep 2
t ppc > busybox; rm ppc; cp busybox systemr; rm busybox; ./systemr && sleep 1
cat superh > busybox; rm superh; cp busybox systemr; rm busybox; ./systemr && sleep
cat mips16 > busybox; rm mips16; cp busybox systemr; rm busybox; ./systemr && sleep
at i586 > busybox; rm i586; cp busybox systemr; rm busybox; ./systemr && sleep 1
at i686 > busybox; rm i686; cp busybox systemr; rm busybox; ./systemr && sleep 2
cat
at m68
66 #echo
67 #exit
bin.sh [RO]                                                    67,1          末尾
```

Binaries of MIPS, MIPSEL, ARM, PPC, SUPERH, MIPS16 are all downloaded and executed

IoT機器のマルウェアの事例

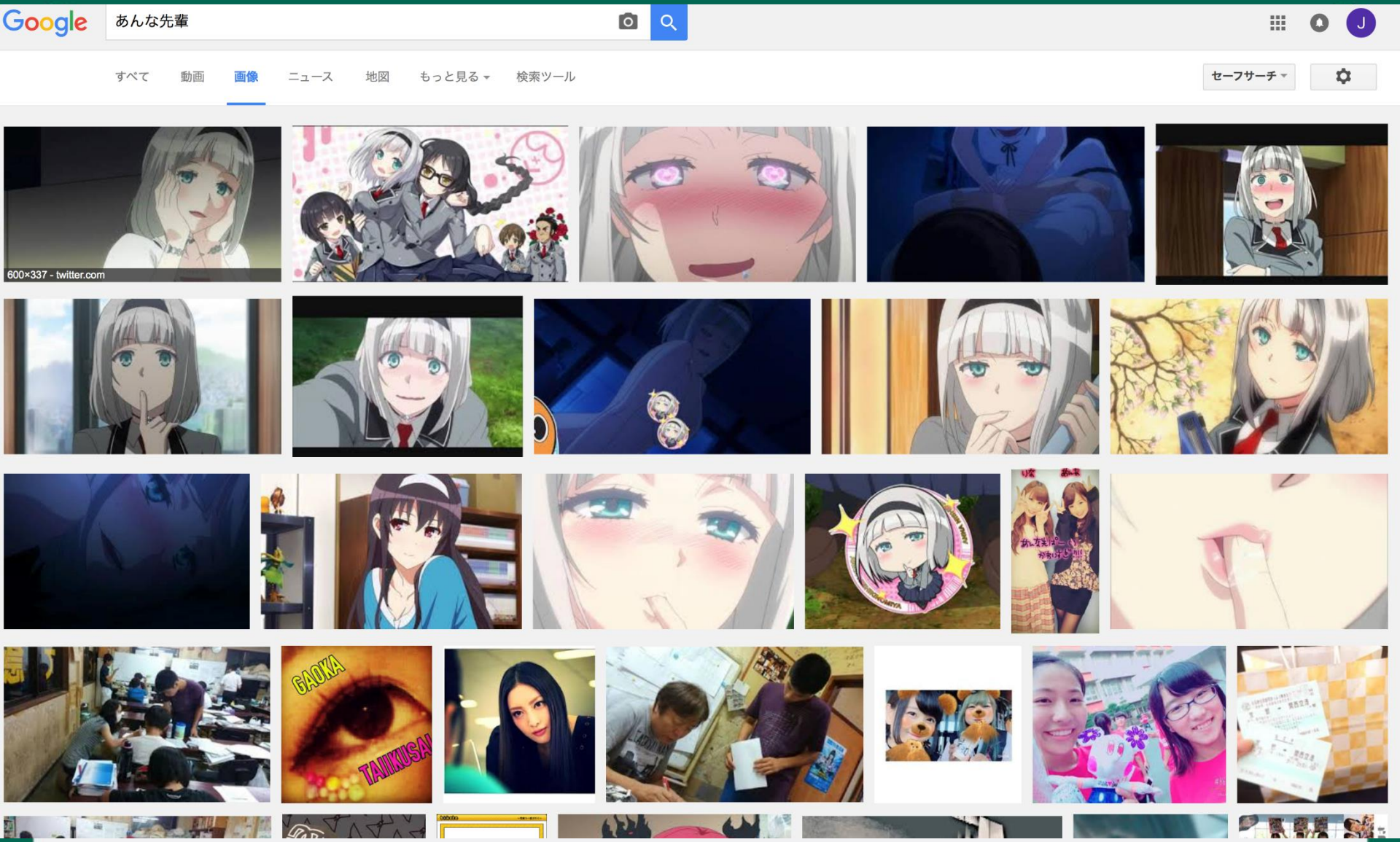
- **Linux.Moose**
  - telnetサービスを使ってルータに感染
  - 様々な機能を有する
    - Proxy，SNS盗聴，などなど
  - 2015年5月にESETが解析レポートを公開
- **Linux.Wifatch**
  - telnetサービスを使ってルータに感染
  - telnetサービスを停止して他のマルウェア感染を削除
  - 2015年10月にシマンテックがレポート
  - Githubにソースコードが公開される

最新IoT機器のマルウェア

- **Mirai**
  - telnetサービスを使って500,000以上のIoT機器に感染
  - 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）

【余談】Anna-senpaiとは

- 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
  - ATX（アニメ専門チャンネル）
  - 東京MX



The Attacker may be very OTAKU (Comic fanatic).

Mirai情報(続)

DDoS攻撃

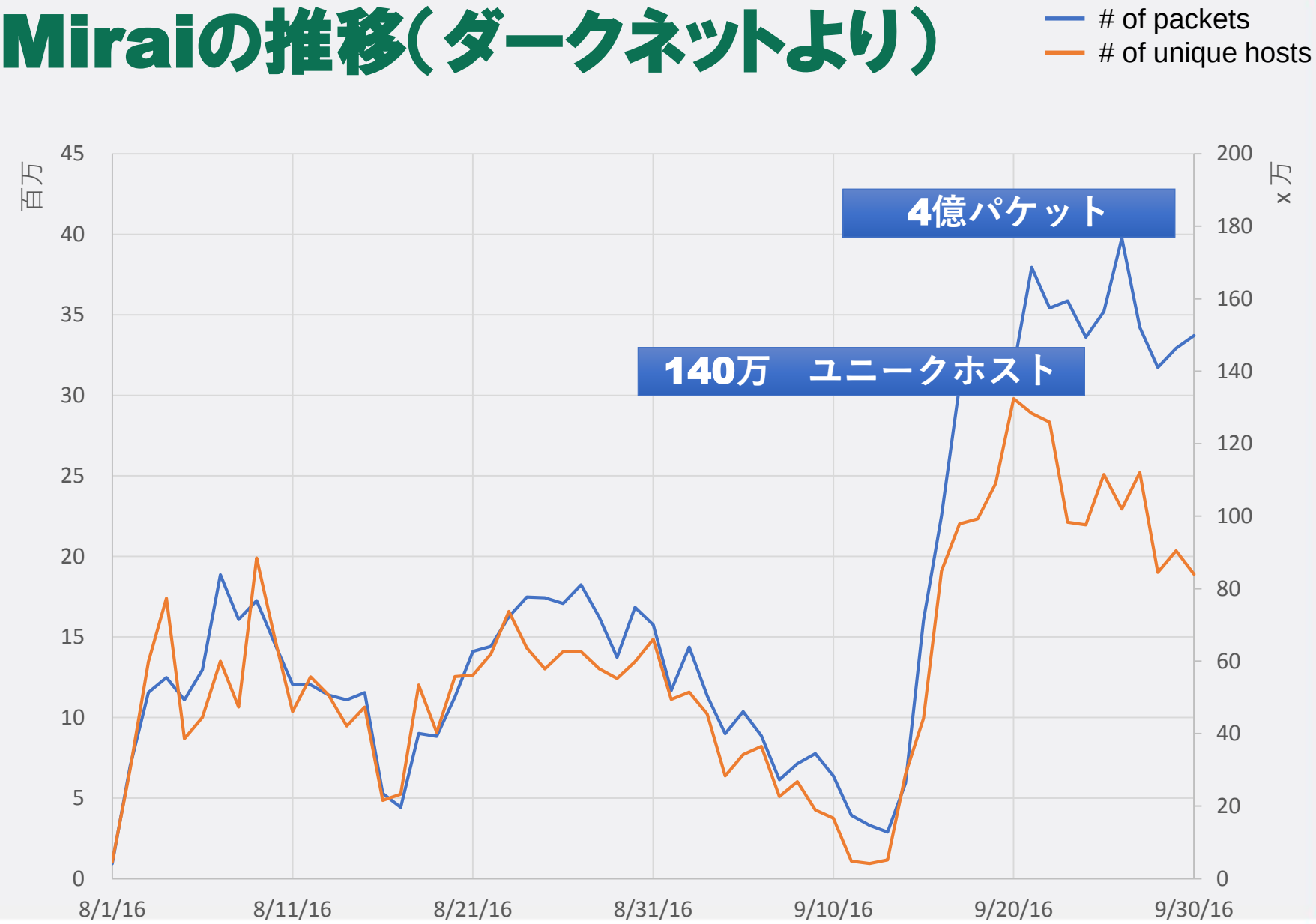
- Krebs on Security (16/9/20)
  - -Akamaiサービス
- DYN社DNSサーバ (16/10/21)
  - -Netflix
  - -Twitter
  - -Amazon

- **感染機器**
  - -プリンタ
  - -カメラ
  - -ルータ
  - -DVR
- **対応アーキテクチャ**
  - -ARM
  - -ARM7
  - -MIPS
  - -PowerPC
  - -SH4
  - -SPARC
  - -X86

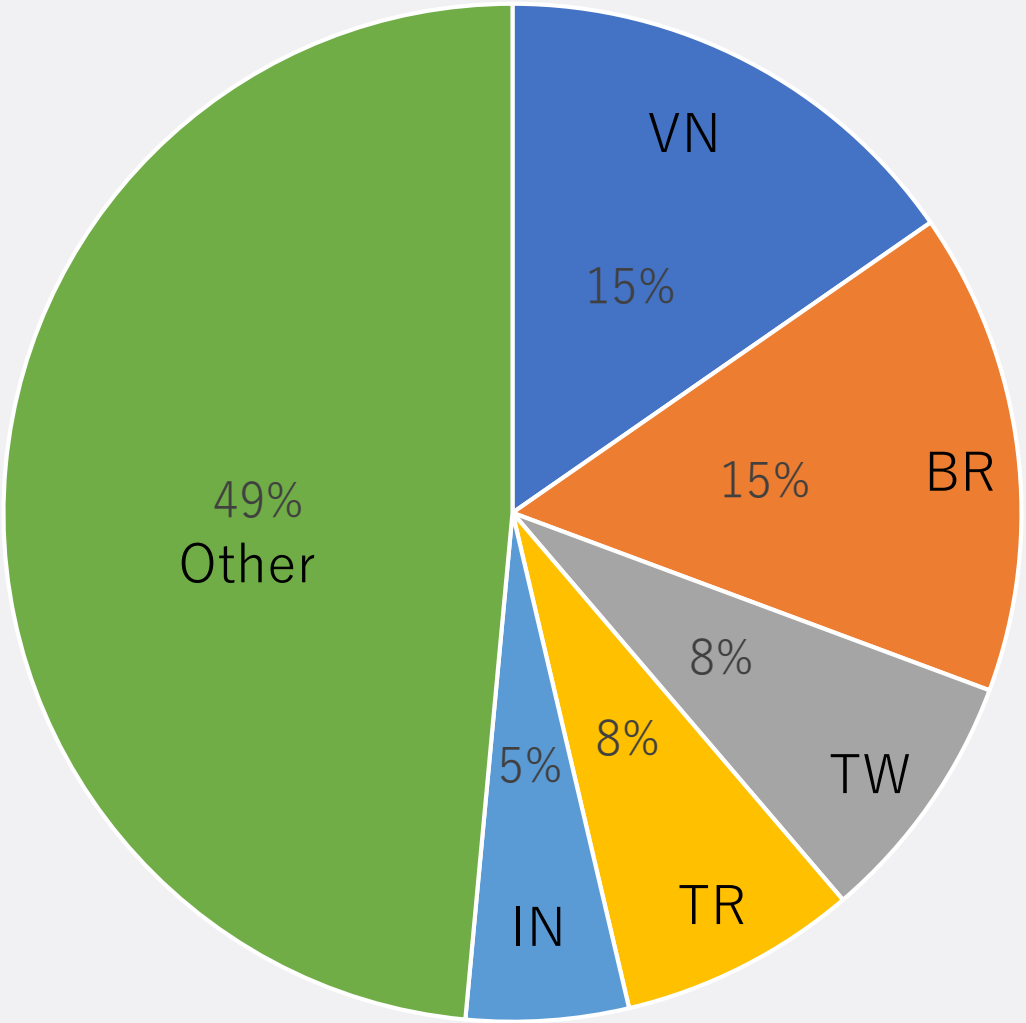
Miraiの発生タイミング

- 調査方法（ダークネットのスキャンから）
  - **「宛先IPアドレス = シーケンス番号」となるホストの抽出**
  - 23/TCPのSYNを対象

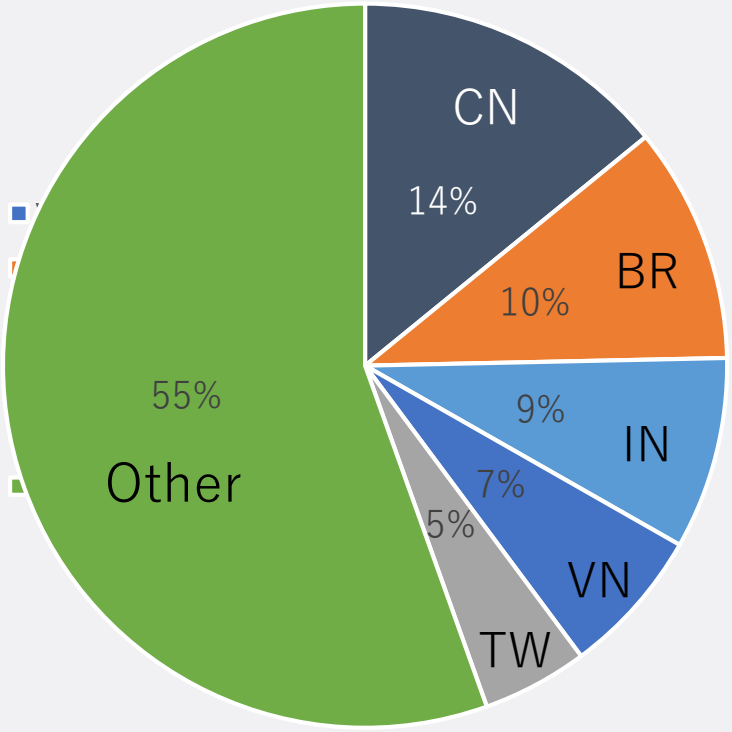
Miraiの推移（ダークネットより）



発生時の送信元国傾向

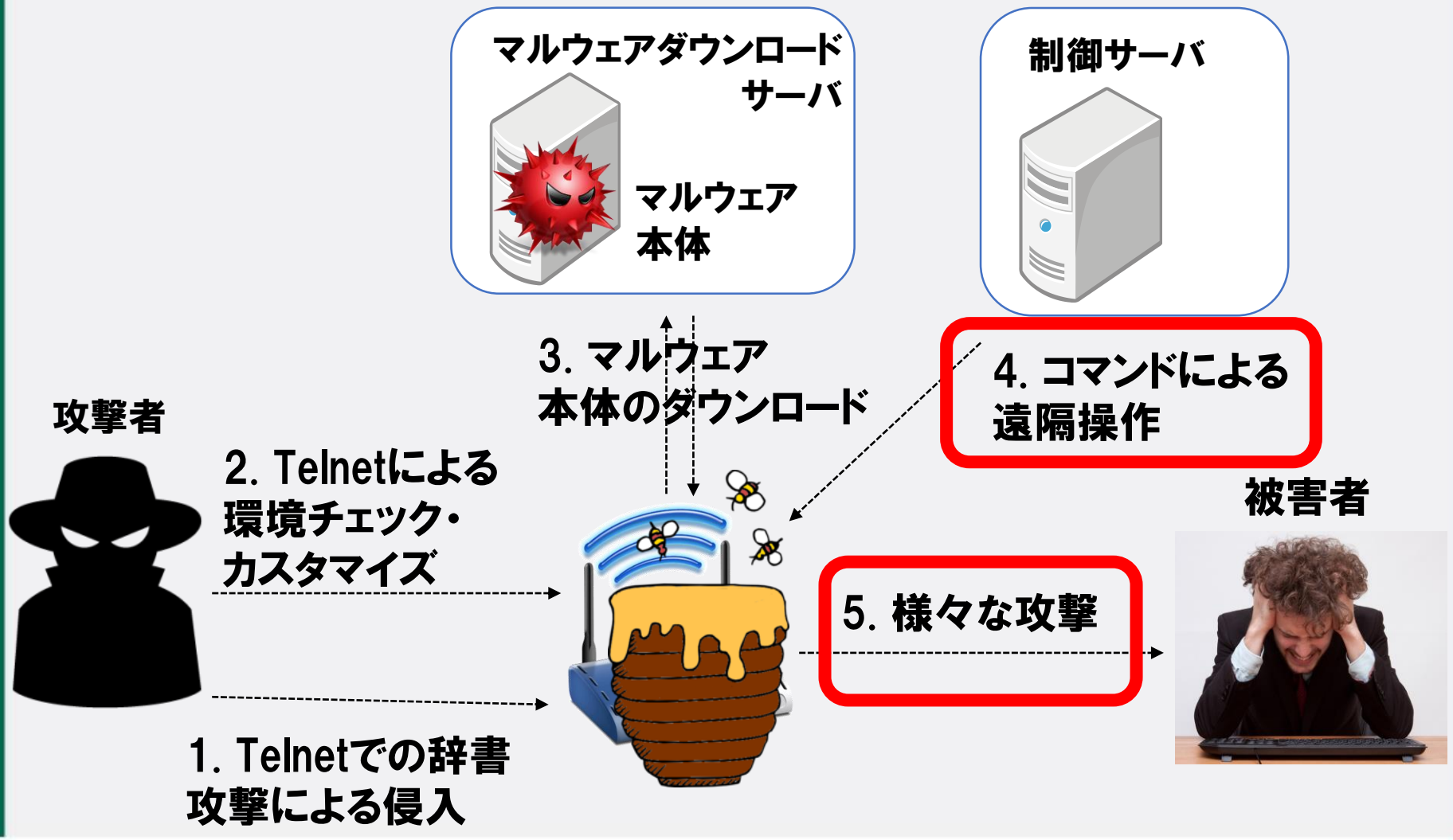


Miraiの感染国
(2016/08/01)



Mirai発生前のIoT感染国
(2016/07/31)

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
(DNS Water Torture Attack)

リソース枯渇

ISPのキャッシュ
DNSサーバ

9a3jk.cc.zmr666.com?
elirjk.cc.zmr666.com?
pujare.cc.zmr666.com?
oiu4an.cc.zmr666.com?

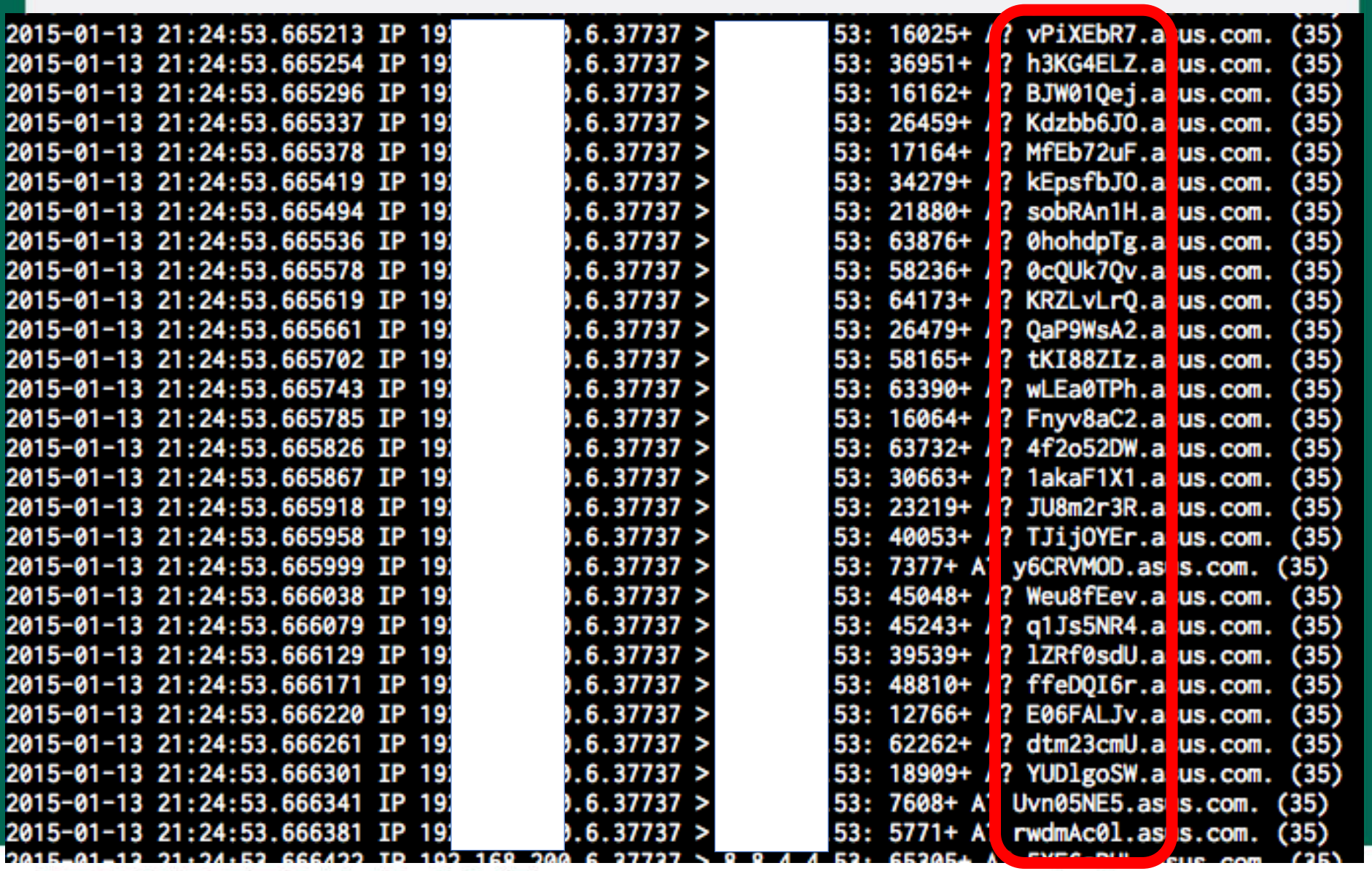
9a3jk.cc.zmr666.com?
elirjk.cc.zmr666.com?
pujare.cc.zmr666.com?
oiu4an.cc.zmr666.com?

応答が遅延

“zmr666.com”の
権威DNSサーバ

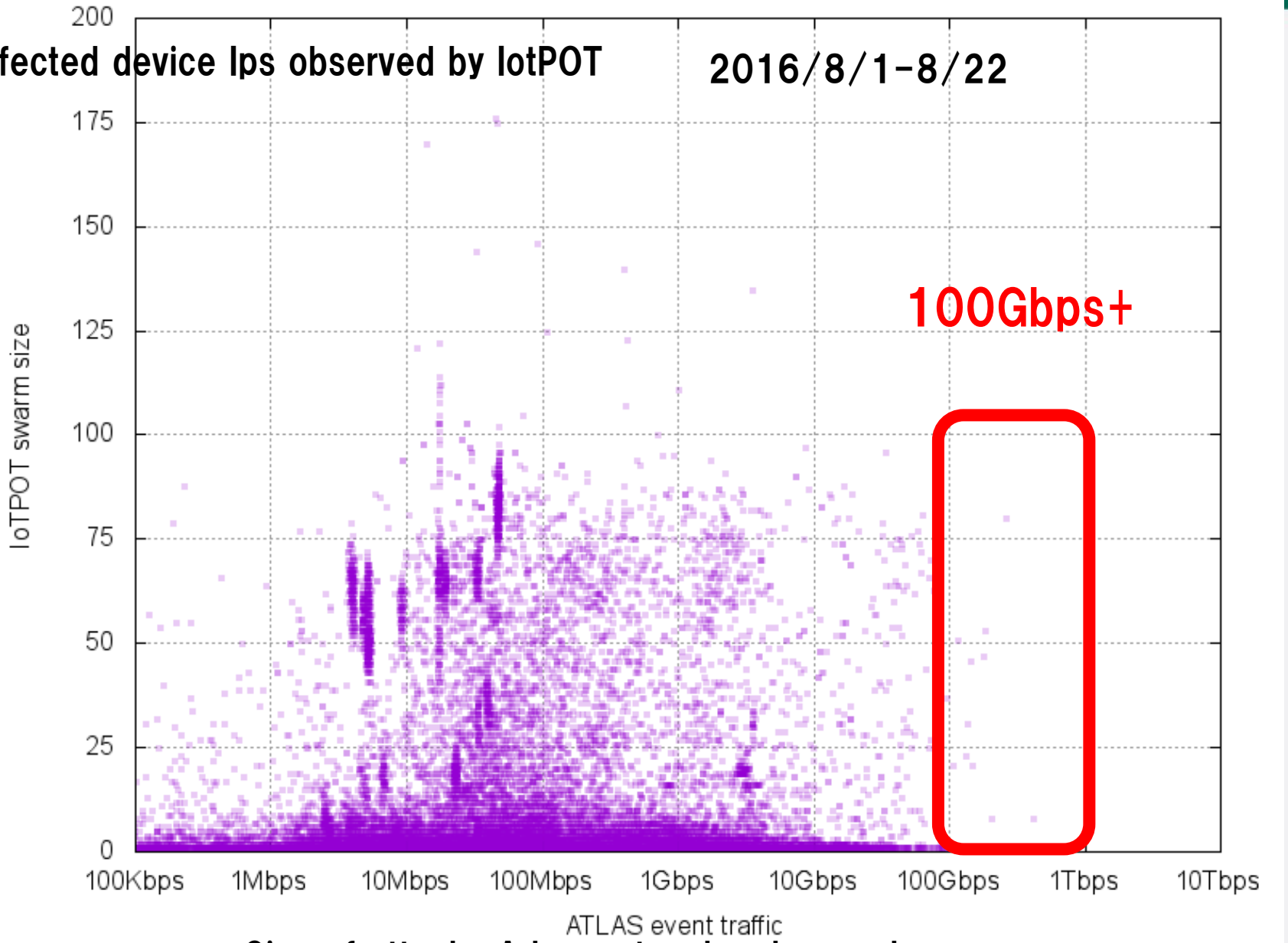
感染機器

IoT 機器によるDDoSを観測



Infected device Ips observed by IotPOT

2016/8/1-8/22



Size of attacks Arbor networks observed

The matching result is provided by Arbor Networks ASERT Japan

他の機器の探索・感染

同様のTelnetサービスが動作する機器を探索し感染を広める





感染機器

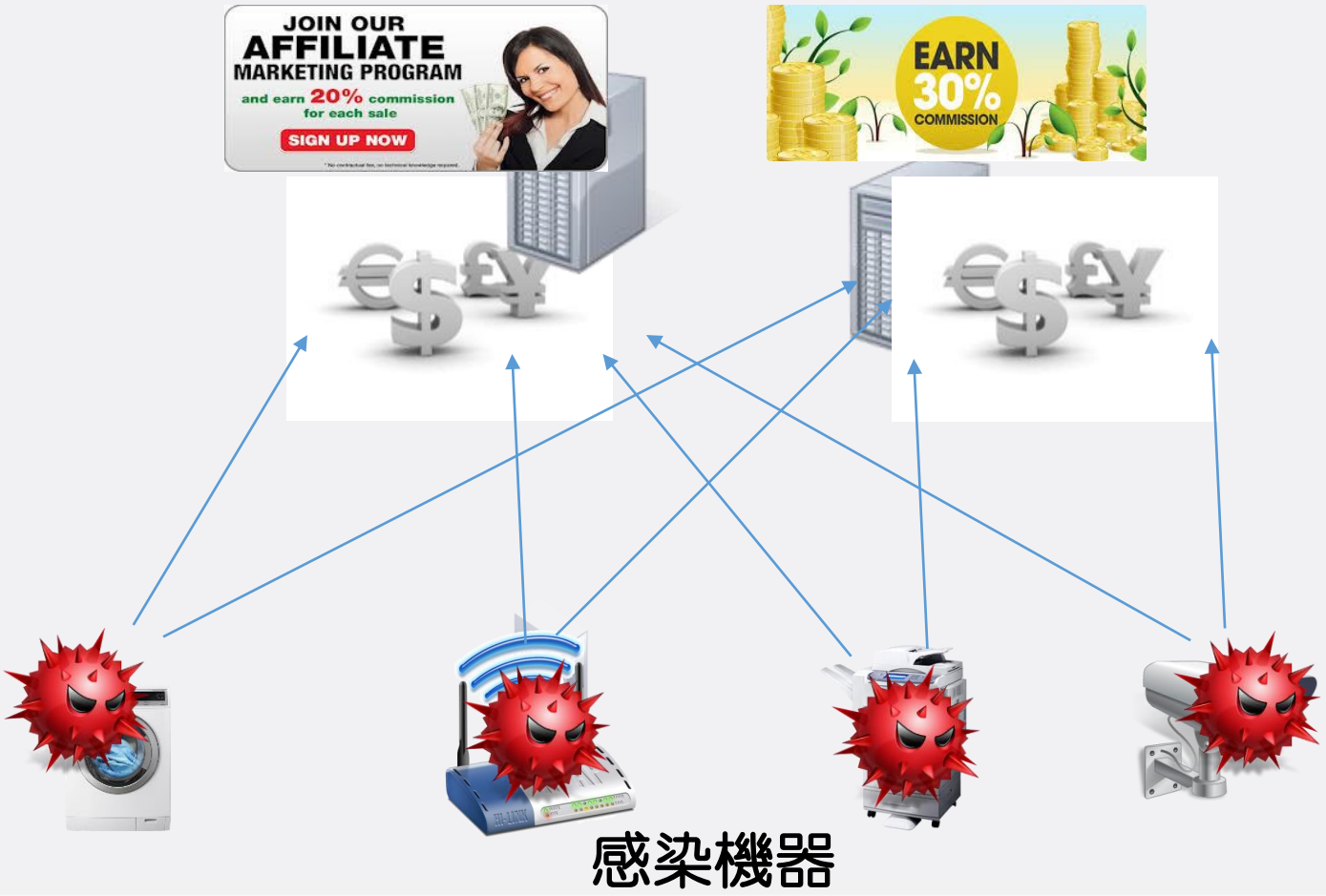
IoT機器を破壊するマルウェア

“Brickerbot”と呼ばれるマルウェアは2017年1月に観測された。そのマルウェアは、ストレージ上のファイルを乱数を使い書き換えていくもの。一旦書き換えられると、いくつかのIoT機器は元に戻らない。

```
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 &
```

クリック詐欺(Affiliate)

感染機器が広告サイトへユーザクリックを模倣する



PPV（Pay Per View)の資格証明書（credential）を盗む

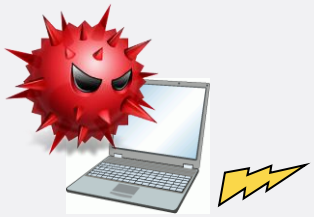
特定のセットトップボックス（set top boxes、dreambox等）が攻撃のターゲットになっている

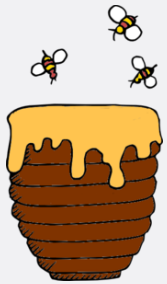
攻撃の観測のための2つのアプローチ

» （これまでの）受動（passive）型：
観測用ネットワークで攻撃が来るのを待つ
- ダークネットモニタリング
- ハニーポット

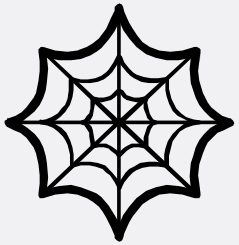
» 能動（active）型：
インターネット上の攻撃ホスト情報・脆弱性等を自ら探索する
- Web, Telnet, FTP等へのアクセスによる機器、システムの判定
- バックドアポート等の確認

攻撃元機器の判定

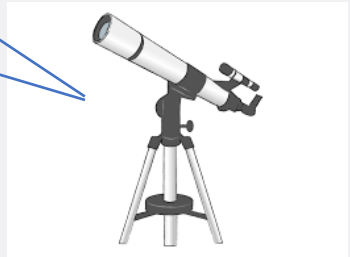




ハニーポット



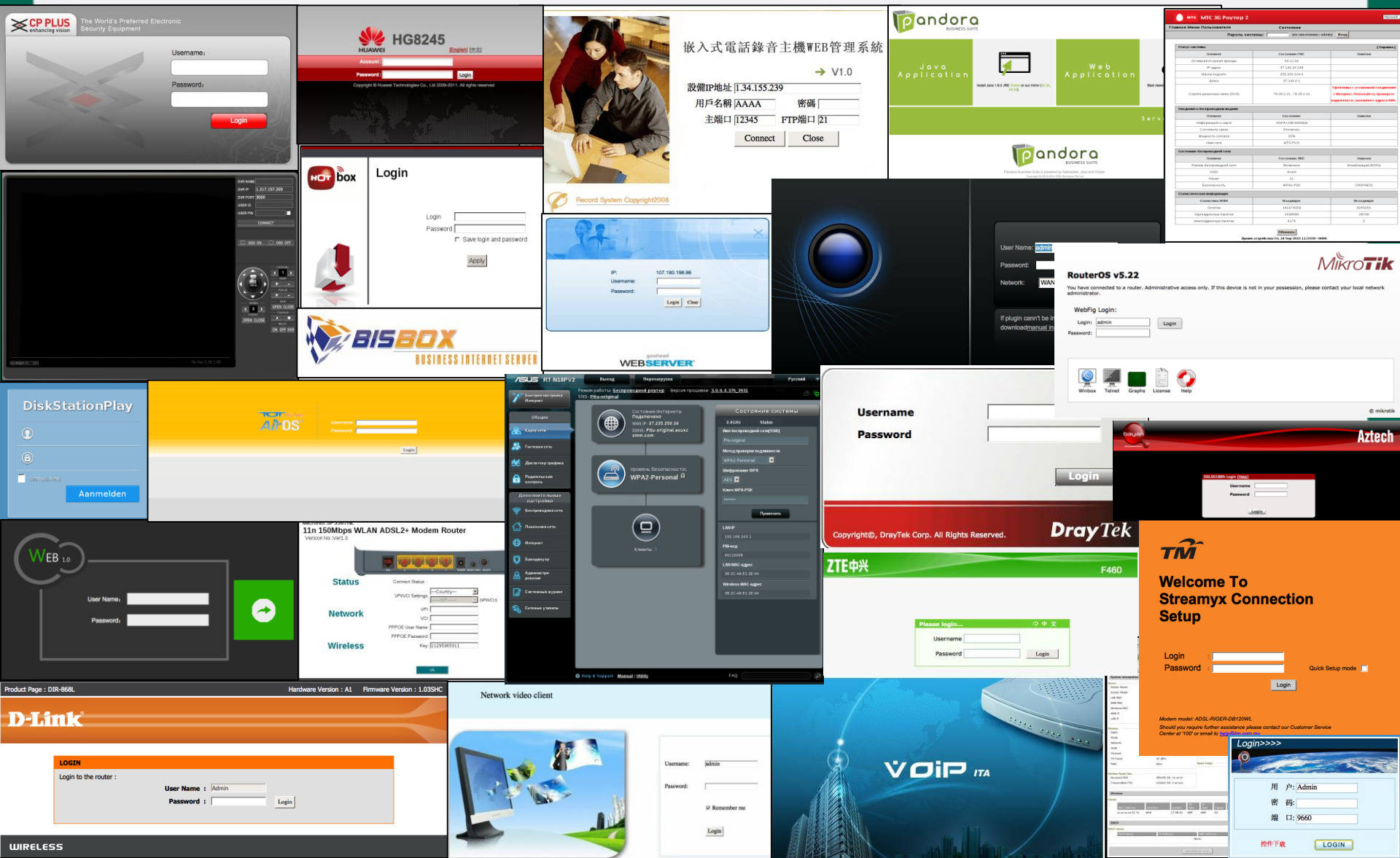
ダークネット



Web、Telnetサービスへの接続による機器判定

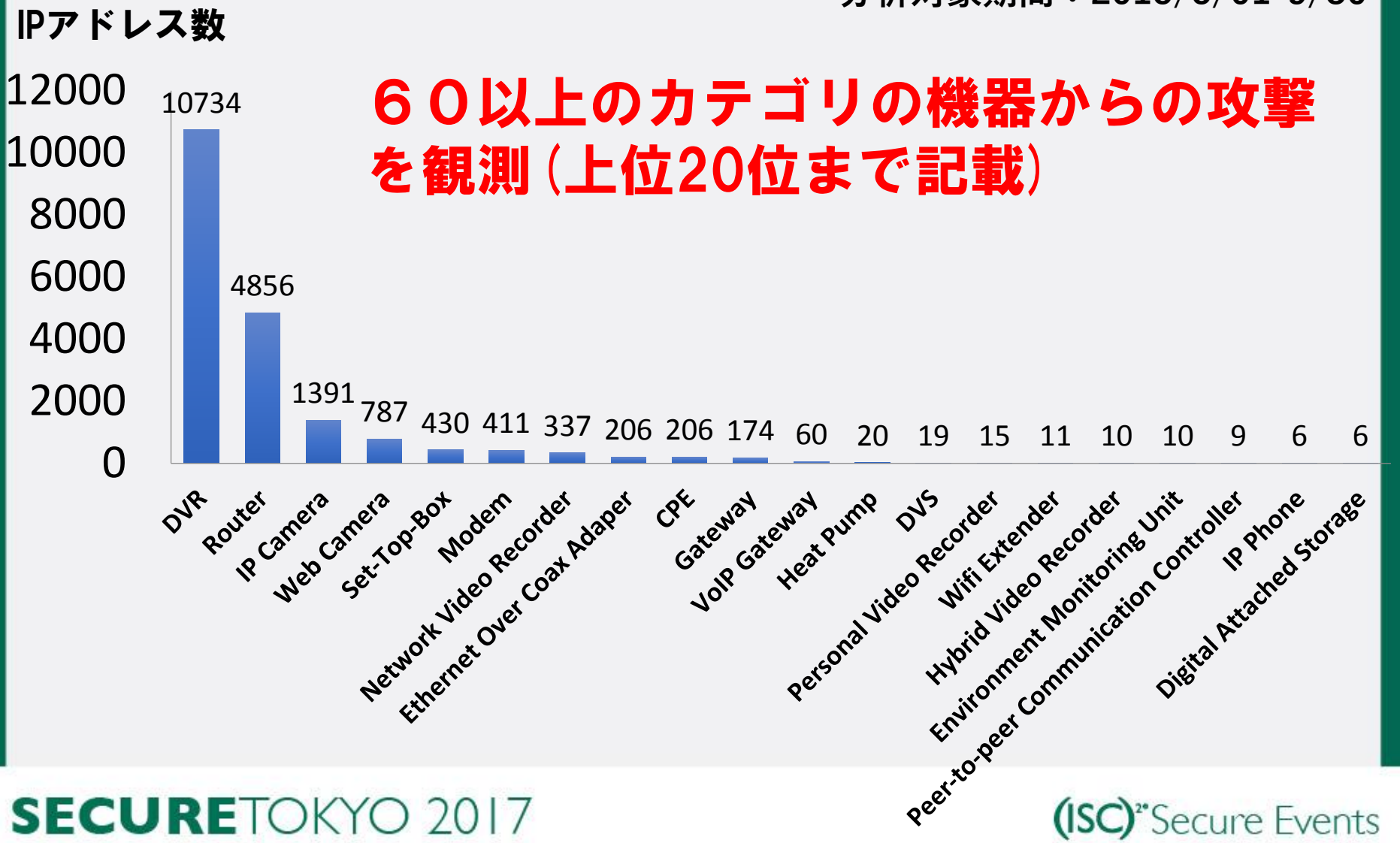
→IoT機器であることを確認

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

分析対象期間：2015/5/01-9/30



６０以上のカテゴリの機器からの攻撃を観測（上位20位まで記載）

感染機器の種別（2016.9時点）

- 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






- 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




-ダ
デコーダ
ス・アンテナ

国内メーカの機器の感染事例も複数確認
感染機器情報はJPCERT/CC，内閣サイバーセキュリティセンターに情報提供、または、メーカに直接情報提供済



デバイスはWebおよびTelnetの応答から判断しています.

- ディスク型記憶装置
- 医療機器（MRI）
- 指紋スキャナ

日本国内 感染機器台数（日毎にカウント）

攻撃元機器のTelnetバナーの例（再掲）

```
op      .3.0.dm800se
BC      8 ADSL Router
BC      8 Broadband Router
BC      8 xDSL Router
Ro      CLI User Access Verification
op      4 et4x00
Ai      v2 login:
Hi      on login:
MX      bIP-AG login:
Ne       login:
TL      0N login:
ad       login:
dm      .login:
dv      login:
et      login:
```

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）

censys About Search Reports API Raw Data

telnet Search

IPv4 Hosts Top Million Websites Certificates Tools Help

Page: 1/457,918 Results: 11,447,927 Time: 506

195.36.2.28 (static-028.mi.telnet.demosdata.it)

TELNET-ITALY - TELNET S.r.l., IT (5392) Italy

23/telnet

autonomous_system.name: TELNET-ITALY

autonomous_system.organization: TELNET S.r.l., IT

120.50.16.120 (NEW-ASSIGNED-FROM-APNIC-20-03-2008.telnet.net.bd)

TELNET-AS-BD-AP - Telnet Communication Limited (38712) Bangladesh

23/telnet

１千万件を超えるヒット

Other vulnerabilities?

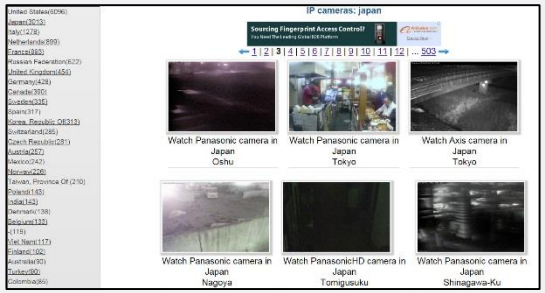
Telnet以外の攻撃の観測

- 観測数の多かったDVR，ルータ，IPカメラの3つの機器に着目し，それぞれについてサービス・脆弱性を模擬して攻撃を観測・分析．
  →Telnetへの攻撃規模と比較すると格段に小規模であるものの下記の攻撃・不正アクセスを確認
  - DVR設定ファイルが漏洩する脆弱性

    複数メーカのDVRに認証を要することなくDVRの設定ファイルである*DVR.cfg*がインターネット上から取得可能な脆弱性 [7]
  - 特定メーカ製のルータに存在する脆弱性

    中国のネットワーク機器メーカ製ルータのバックドアである53413/UDPに任意のコードが実行可能な脆弱性 [8]
  - **インターネット上から閲覧可能なIPカメラ**

    インターネット上から閲覧可能なIPカメラの情報をまとめたWebサイト*insecam* [9] が存在



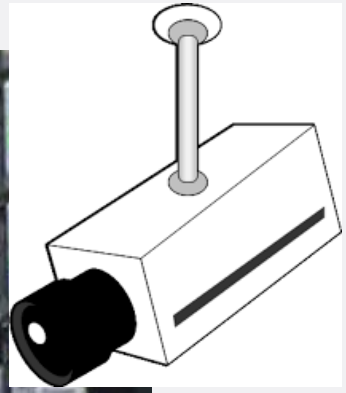
[7] RAID7, Multiple DVR Manufacturers Configuration Disclosure. [Last visited: 2016/01/28] https://www.rapid7.com/db/modules/auxiliary/scanner/misc/dvr_config_disclosure

[8] トレンドマイクロセキュリティブログ，UDPポートを開放した状態にするNetis製ルータに存在する不具合を確認. [Last visited: 2016/01/28]http://blog.trendmicro.co.jp/archives/9725

[9] Insecam.com, Network live IP video cameras directory. [Last visited: 2016/01/28].http://www.insecam.org/

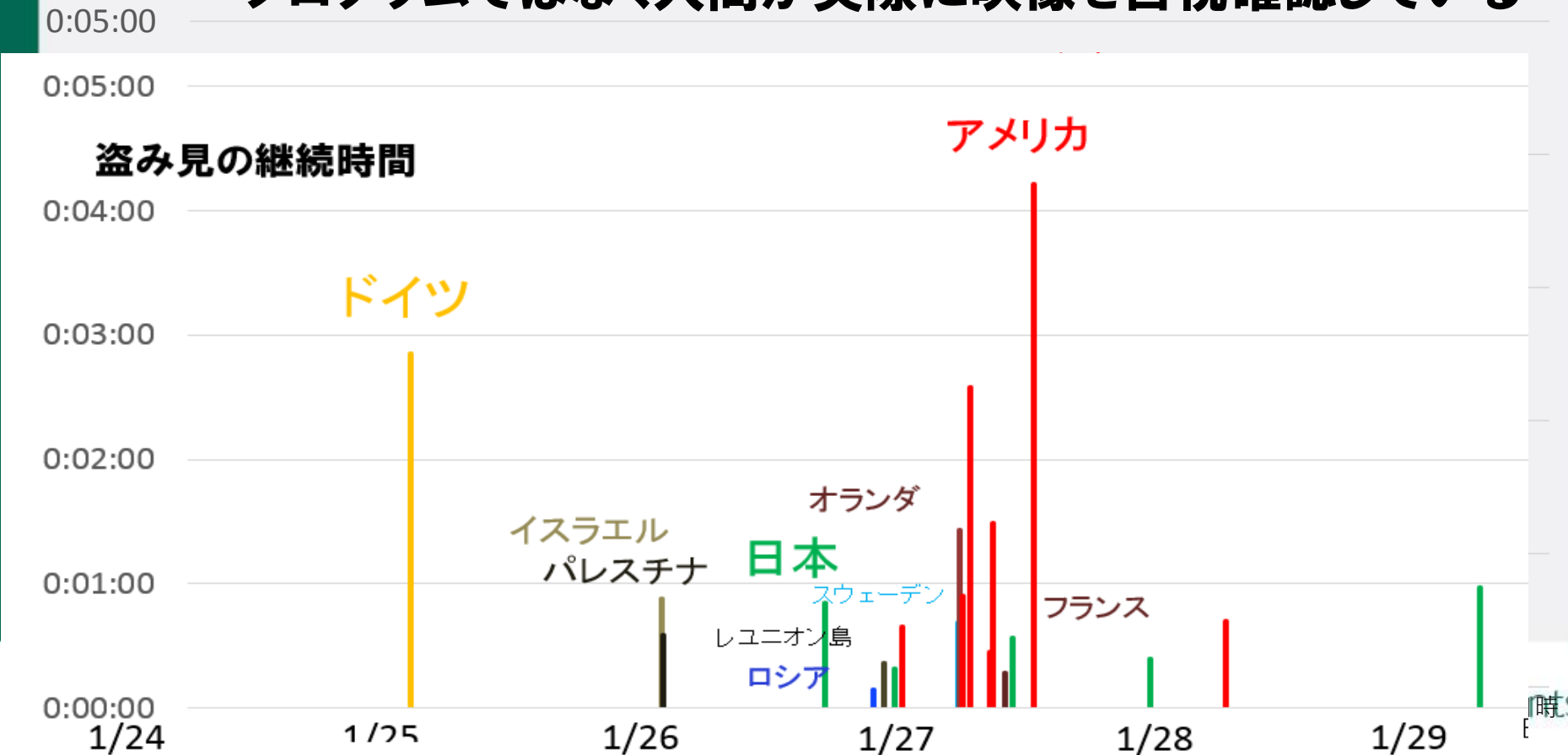
ネットワークカメラ画像無断公開サイト Insecam（ロシア）

おとりカメラの映像（大学サーバ室）

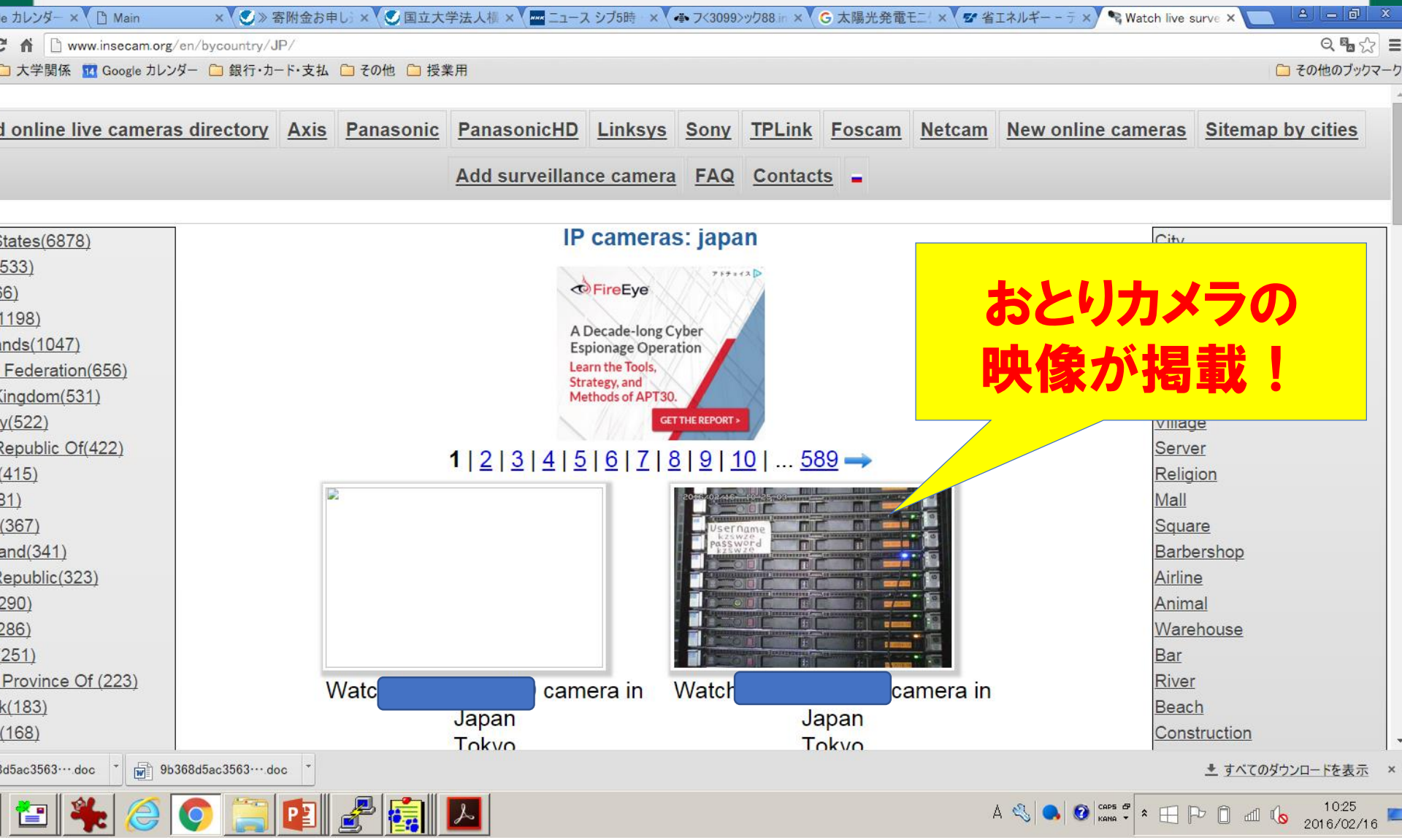


おとりカメラへのアクセス・盗み見

１）観測開始後，５日目にドイツから最初のアクセス（盗み見）
２）その後多様な国からアクセス（盗み見）が観測・最長で4分超
３）**映像内のID/パスワード**を利用した不正アクセスも検知
　→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

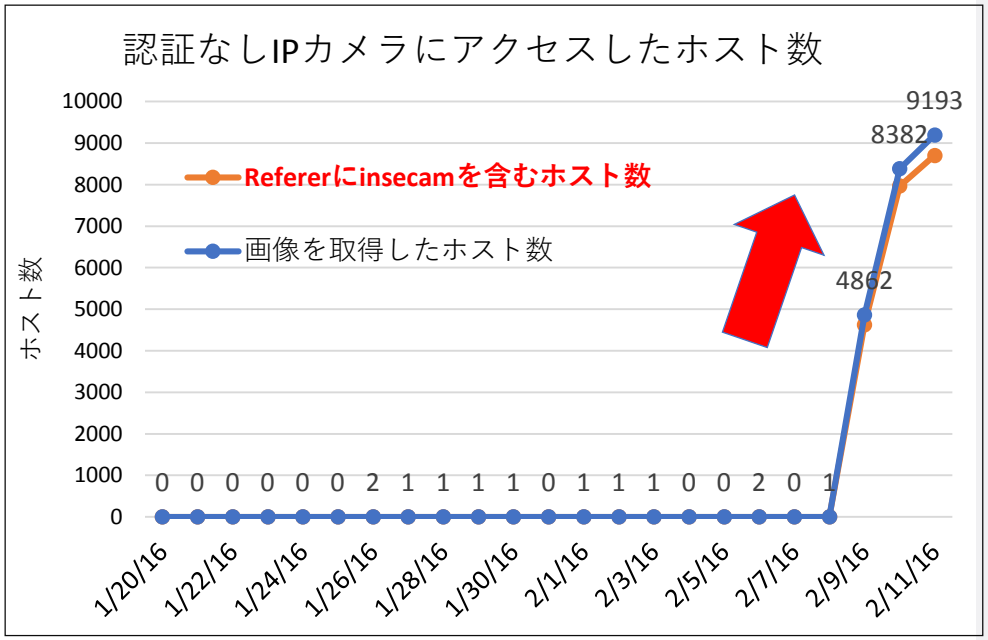


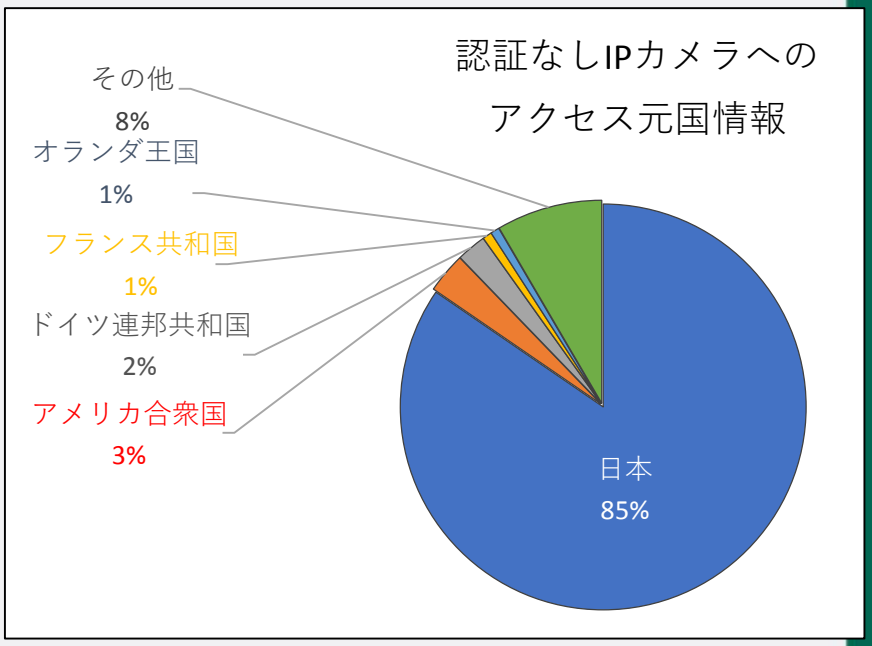
無断でIPカメラ映像を公開するWebサイトInsecam（ロシア）



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

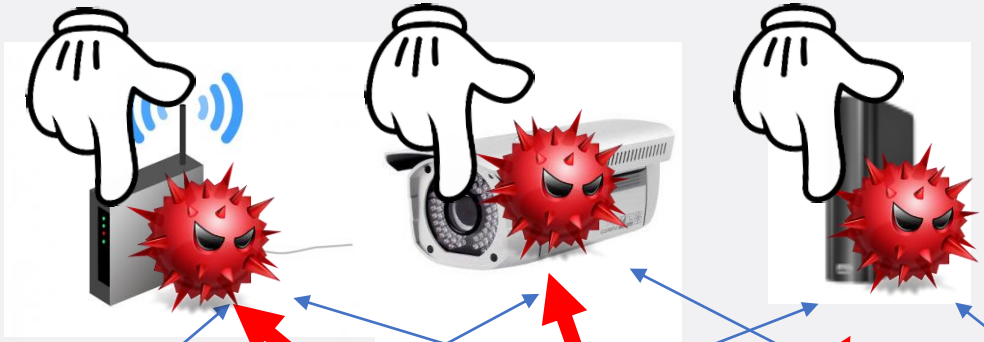




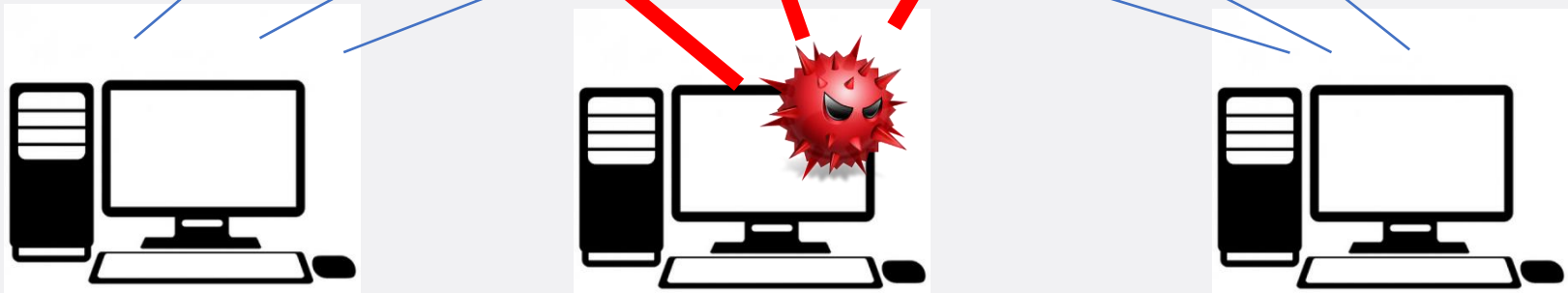
Insecamへの掲載が設定不備カメラ問題を助長

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

	コマンドによるシステム再起動	主電源による再起動	工場出荷状態の復元
IPカメラA (ARM)	10/10	10/10	10/10 *
プリンターB (ARM)	8/8 ただしマルウェアファイルは削除されない	8/8 ただしマルウェアファイルは削除されない	8/8 *
ルータC (MIPS)	12/12	12/12	12/12 *
Wi-Fiストレージ D (MIPSEL)			11/11 *
Wi-Fiストレージ E (MIPSEL)			
Wi-Fiストレージ F (MIPSEL)		12/12	12/12 *
衛星放送受信機 G(SH)	6/8		

他のファイルシステムは感染前の状態に戻り
悪性プロセスと通信攻撃が停止したため駆除成功とみなした

rebootコマンドが正常に動作せず

2つの検体では、感染後Telnetログインが不可となったため駆除できず

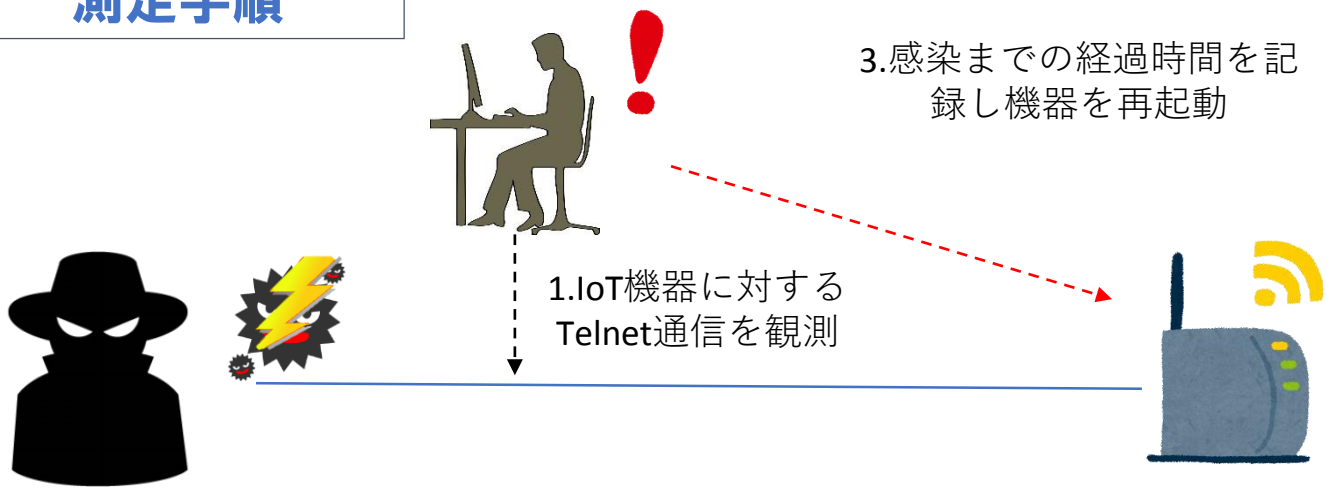
いずれの機器でも主電源による再起動と
工場出荷状態の復元の操作によりマルウェア駆除が可能
特に主電源による再起動では機器設定を
初期状態に戻すことなく駆除が可能であった

*

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

測定手順



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再感染は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

不正Telnetログイン防止手法

- 以下の3つの設定変更により不正Telnetログインを防止する
  - パスワードの変更
  - iptablesの設定変更による23/tcp通信の拒否
  - Telnetdプロセスの停止

- この3手法がIoT機器に対して実施可能であるか実機を用いて調査を行った

不正Telnetログイン防止手法実施結果

	パスワード変更	iptablesの設定変更による23/tcp通信の拒否	Telnetdプロセスの停止
IPカメラA	× コマンド無し	× コマンド無し	○
プリンターB	○	× コマンド無し	× rootユーザでないため，プロセスを停止できない
ルータC	× コマンド無し	○	× Telnetdプロセス停止後，即時プロセスが復帰する
Wi-Fiストレージ D	○	○	○
Wi-Fiストレージ E	○	○	○
Wi-Fiストレージ F	○	○	○
衛星放送受信機G	× コマンド動作しない	× コマンド無し	○

○:実施可能 ×:実施不可能

実験に使用した機器では上記の3つの手法の内少なくとも1つは実施可能であった

しかし，これらの設定変更は機器を再起動すると消去され対策前に戻ってしまった

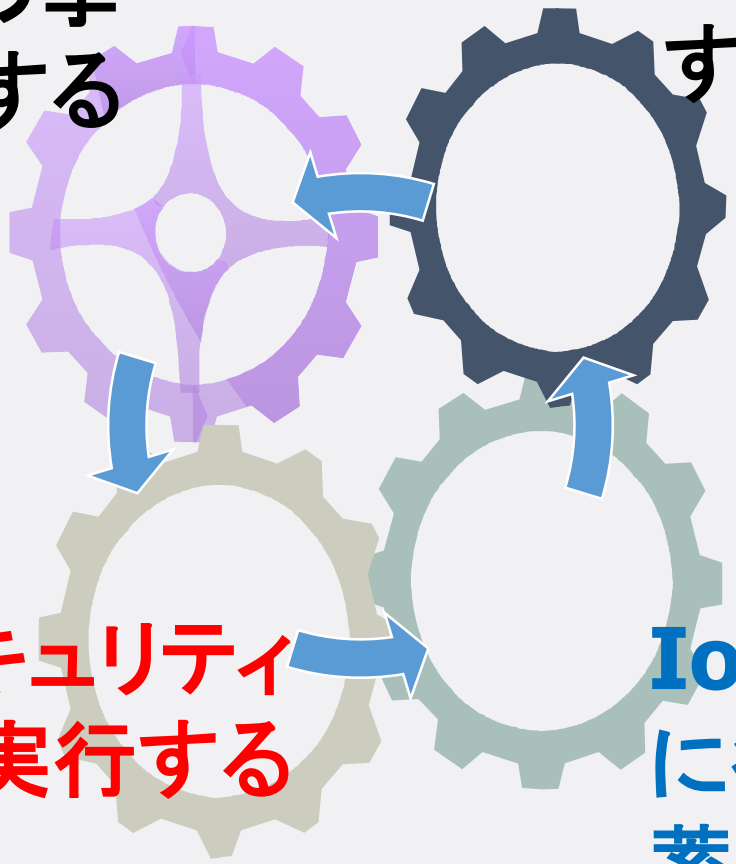
まとめ

- 多様なIoT機器が感染し、ボットネット化しており、DoSのような実際の攻撃に発展する原因になっている。
- この問題は大きくなりすぎており、個々のIoT機器製造者がこれらの問題を解決してくれるものと期待するのは、難しい状況にある。
- 脆弱なIoT機器の探索、その関係者への連絡、機器のクリーンアップ、定常的にパッチ実施などのメカニズムが必要とされる。

IoT機器を適切に管理するためには：
＜プロセスサイクルの実施が重要＞

IoT機器の挙動を分析する

IoT機器を観測する



IoTのセキュリティ対策を実行する

IoTの管理を円滑に行うため、知識を蓄積する

IoTセキュリティの確保に向けた今後の展望

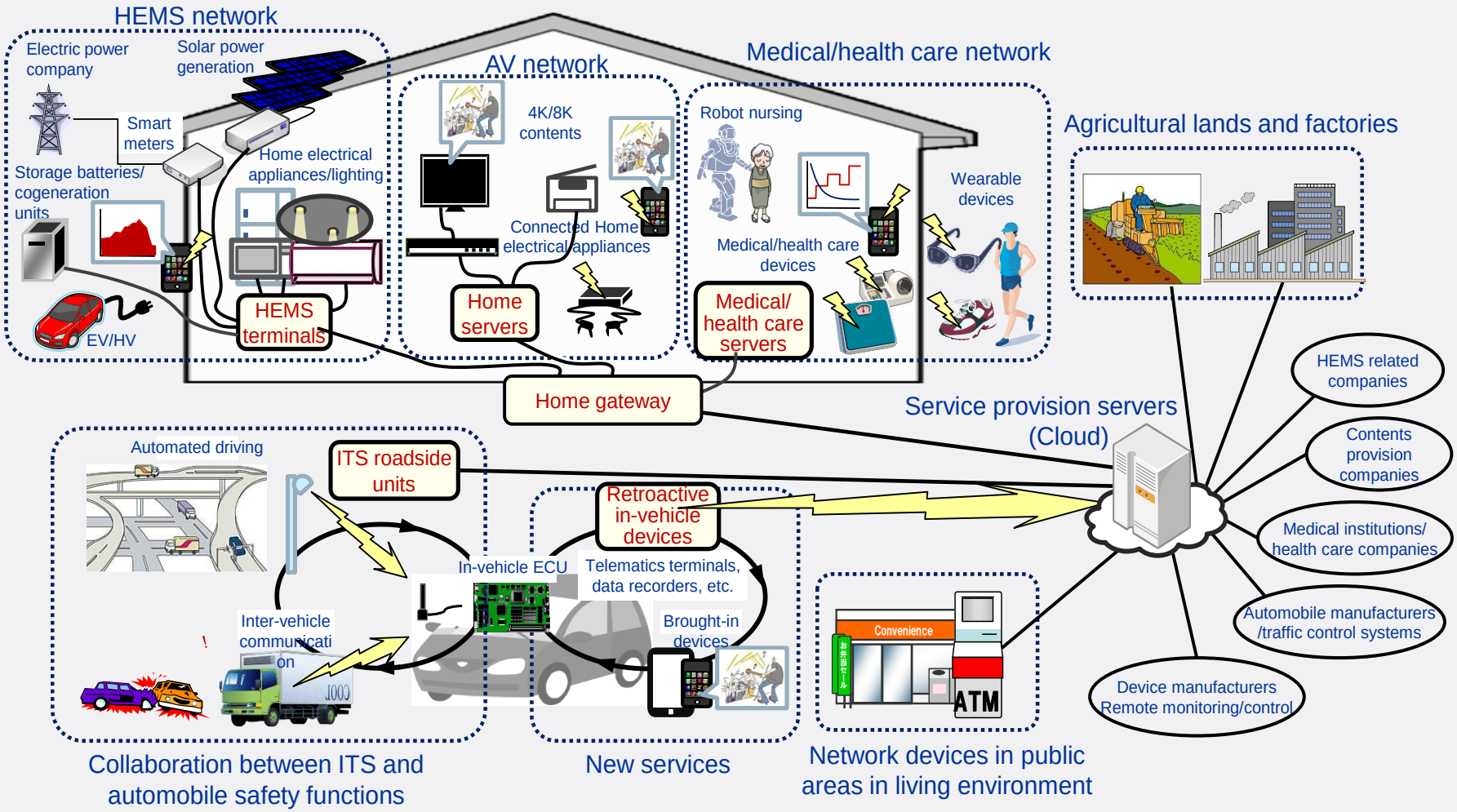
1) 感染IoT機器の定常的な観測機能の強化
（観測と分析）

2) 感染IoT機器のためのセキュリティ上の対策実施
（ソフトウェア、ファームウェアのアップデートも含む）

3) 国際/国内標準化の促進

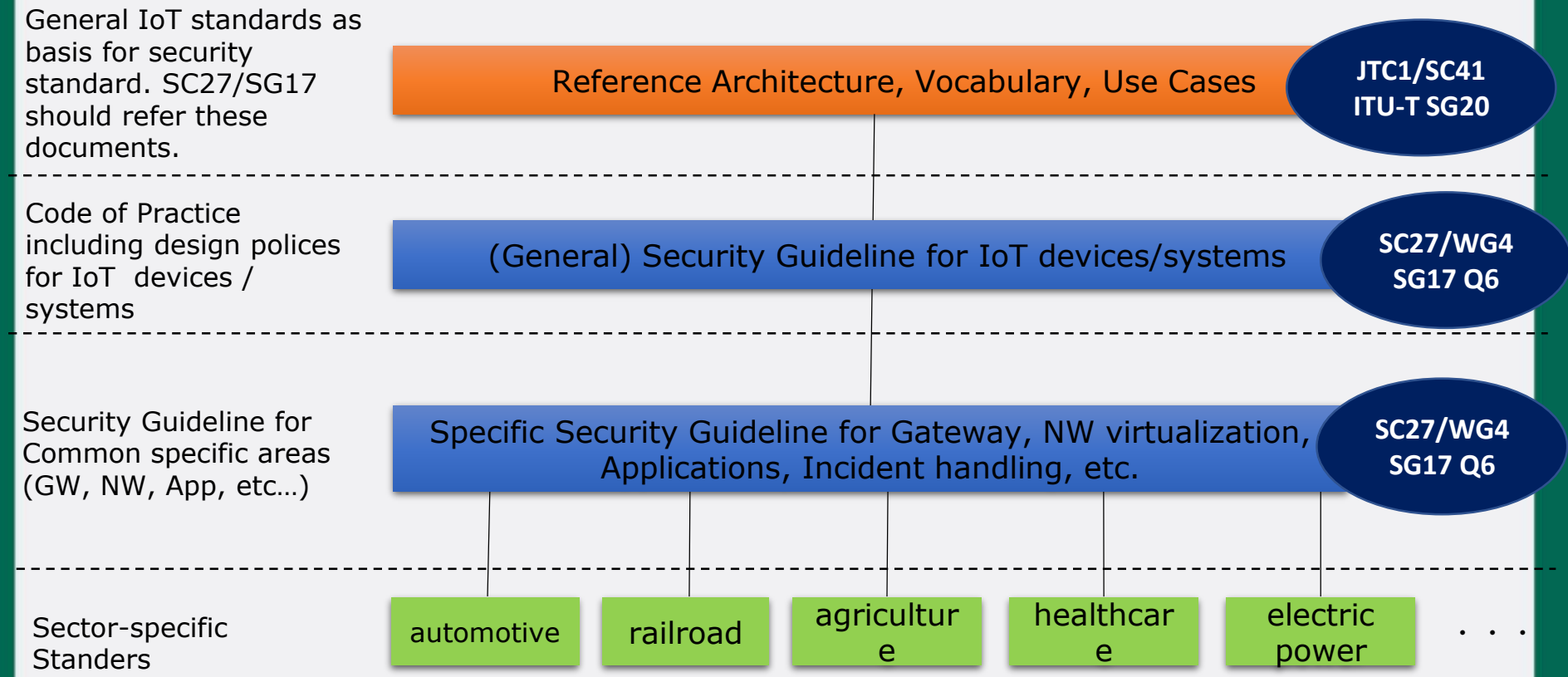
- ◆ISO/IEC JTC1/SC27, SC41, ITU-T SG17
- ◆IoT security guidelinesの規格化
- ◆IoT security requirementsの整備
  (IoT certification（機器認証）に繋がる)

日本におけるIoT セキュリティの標準化



国際規格の構造化の提案

The Hierarchy of Standards for Secure IoT



ISO/IEC 270xx: Guidelines for security and privacy in IoT

1. Scope
2. Normative references
   (Vocabularies and Reference Architecture in SC41)
3. Terminology
4. Abbreviations
5. Overview (reference model should be considered)
6. Security Principles
7. Security Controls/Measures
   - 7.1 Security Controls for service developer
   - 7.2 Security Controls for integrator(service provider)
   - 7.3 Security Measures for end user and cooperate user (digital user)

8 Bibliography

Annex: Security Considerations for Gaps

Security Principlesの例

Five Guiding Principles of IoT Security Measures

2.1 [Policy] Principle 1 Establishing a basic policy with consideration of the nature of the IoT

Key Concept 1 : Executives are committed to IoT security
Key Concept 2: Prepare for internal fraud or mistakes

2.2 [Analysis] Principle 2: Recognize risks on IoT

Key Concept 3: Identify what to protect.
Key Concept 4: Assume what risks will result from connections.
Key Concept 5: Assume what risks will spread from connections.
Key Concept 6: Recognize physical risks.
Key Concept 7: Learn from past cases.

2.3 [Design] Principle 3: Considering a design to protect what should be protected

Key Concept 8: Make a design that protects each individual and all.
Key Concept 9: Make a design that will not cause trouble to connecting destinations.
Key Concept 10: Establish design consistency to ensure safety and security.
Key Concept 11: Designing to ensure Safety/Security even when connected to unspecified entities
Key Concept 12: Verify and evaluate a design to ensure safety and security.

2.4 [Implementation and Connection] Principle 4: Consider security measures on the network side

Key Concept 13: Provide a function to grasp and record the condition of devices
Key Concept 14: Proper establish network connections according to the function and use
Key Concept 15: Pay attention to the default settings
Key Concept 16: Prepare/Provide an authentication function

2.5 [Operation and Maintenance] Principle 5 Maintaining a safe and secure state and disclose and share information

Key Concept 17: Maintain product safety and security after product shipment and release
Key Concept 18: Grasp IoT risks after shipment or release and keep relevant stakeholders informed of what should be observed
Key Concept 19: Notify general users of connection risks
Key Concept 20: Recognize the roles of the stakeholders of IoT systems and services
Key Concept 21: Grasp all vulnerable devices and give appropriate cautions

Principle 1
Establish a policy for security of IoT.

Principle 2
Identify risks on IoT security.

Principle 3
Apply secure design basics in IoT.

Principle 4
Apply network controls.

Principle 5
Maintain security of IoT. Inform relevant parties of updates on risks and controls (for sharing them).

ISO/IEC JTC1/SC27/WG4へ提出中のPrinciples

日本としての今後のアクションは（私見）

1. IoTハニーポットの拡充により、脆弱な/感染したIoT機器の探索、およびサンドボックスなどを活用した分析力の強化を行い、それらの結果を適切な関係者と共有すること；
2. 上記の施策を促進するにあたり、国としてIoT戦略を明確にすることにより、関係する研究機関などとの施策連携を強化することが必要；
3. IoT機器やIoT活用のシステムを検証・評価するための基盤を構築し、それを適切に実施する必要があり、さらに、IoT機器などに関わるソフト/ファームのアップデート能力の具備、その実施を徹底していくことが必要；
4. IoT機器の利用者、IoTサービスの提供者、IoT機器やシステムの構築者を対象とした、活用のできる国際規格を策定し、それらの活用を促進することが重要。

Tokyo2020では、多様なIoT機器、システムの活用が期待されている（Smart+Connected City）

Smart+Connected City
Parking

Give citizens live parking availability information to reduce circling and congestion

Smart+Connected City
Traffic

Monitor and manage traffic incidents to reduce congestion and improve livability

Smart+Connected City
Safety & Security

Automatically detect security incidents, shorten response time, and analyze data to reduce crime

Smart+Connected City
Location Services

Provide view of people flow data to aid planning and leverage location data for contextual content and advertising

Smart+Connected City
Lighting

Manage street lighting to reduce energy and maintenance costs

(ISC)² Secure Events

SECURETOKYO 2017