

ネットワーク観測からわかる IoTのサイバーセキュリティ実情

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

JNSA IoTセキュリティセミナー (2016/10/26)

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

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

- 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。

多くの機器で動いています

B[redacted]328 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]328 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:

ope[redacted]4 et4x00

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 '^]'.

```

```

i.3.0.dm800s
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.

```

デフォルトパスワードはWeb等でも簡単に手に入れます

The screenshot shows a web browser window with the URL www.defaultpassword.com. The page displays a list of default passwords for various protocols and manufacturers. A black box highlights a specific section of the list.

Protocol	User	Pass
Telnet	adm	(non
Telnet	security	secu
Telnet	read	synn
Telnet	write	synn
Telnet	admin	synn
Telnet	manager	mana
Telnet	monitor	moni

The background list includes entries for manufacturers like 3COM, SuperStack II, Wireless 11g Firewall Router, and Actiontec, with their respective protocols, users, and passwords.


```
P 37.220.109.10.24147 > 0.0.0.0.23: Attacker command /bin/busybox echo -ne \\x0f\\xaf\\x00\\x00\\x00\\x0c\\x3\\x20\\xf8\\x09\\x00\\x00\\x00\\x00\\x8f\\xbc\\x00\\x10\\xac\\x50\\x00\\x00\\x24\\x10\\xff\\xff\\x02\\x00\\x00\\x08\\x27\\xbd\\x00\\x20\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x3c\\x1c\\x00\\x05\\x27\\x9c\\x9c\\xaf\\xb0\\x00\\x18\\xaf\\xbc\\x00\\x10 >> /var/tmp/mvXUDI && /bin/busybox WOPBOT
```

```
P 37.220.109.10.24147 > 0.0.0.0.23: Response command \\xaf\\x00\\x00\\x00\\x0c\\x8f\\x99\\x80\\x94\\x10\\xe0\\x00\\x06\\x00\\x40\\x80\\x21\\x03\\x20\\xf8\\x09\\x00\\x10\\xff\\xff\\x02\\x00\\x10\\x21\\x8f\\xbf\\x00\\x1c\\x8f\\xb0\\x00\\x18\\x03\\xe0\\x00\\x08\\x27\\xbd\\x00\\x05\\x27\\x9c\\x9c\\xa0\\x03\\x99\\xe0\\x21\\x27\\xbd\\xff\\xe0\\xaf\\xbf\\x00\\x1c\\xaf\\xb0\\x00\\x18
```

攻擊觀測技術

```
P 37.220.109.10.24147 > 0.0.0.0.23: Response command \\x02\\x0f\\xa6\\x00\\x00\\x00\\x0c\\x8f\\x99\\x80\\x94\\x10\\xe0\\x00\\x06\\x00\\x40\\x80\\x21\\x03\\x20\\x00\\x24\\x02\\xff\\xff\\x8f\\xbf\\x00\\x1c\\x8f\\xb0\\x00\\x18\\x03\\xe0\\x00\\x08\\x27\\xbd\\x00\\x20\\xc\\x1c\\x00\\x05\\x27\\x9c\\x9c\\x40\\x03\\x99\\xe0\\x21\\x27\\xbd\\xff\\xd8\\xaf\\xbf\\x00\\x24\\xaf\\xb0
```

```
P 37.220.109.10.24147 > 0.0.0.0.23: Attacker command /bin/busybox echo -ne \\x00\\x10\\x30\\xa2\\x01\\x00\\f\\xa6\\x00\\x30\\x27\\xa2\\x00\\x34\\xaf\\xa2\\x00\\x18\\x00\\xc0\\x18\\x21\\x00\\x60\\x30\\x21\\x24\\x02\\x00\\x06\\x00\\x40\\x80\\x21\\x03\\x20\\xf8\\x09\\x00\\x00\\x00\\x00\\x00\\x8f\\xbc\\x00\\x10\\xac\\x50\\x00\\x0x8f\\xb0\\x00\\x20\\x03\\xe0\\x00\\x08 >> /var/tmp/mvXUDI && /bin/busybox WOPBOT
```

```
P 37.220.109.10.24147 > 0.0.0.0.23: Response command \\x10\\x30\\xa2\\x01\\x00\\x00\\x00\\x18\\x21\\xaf\\xa7\\x00\\x34\\x10\\x40\\x00\\x04\\xaf\\xa6\\x00\\x30\\x00\\x60\\x30\\x21\\x24\\x02\\x0f\\xa5\\x00\\x00\\x00\\x0c\\x8f\\x99\\x80\\x94\\x10\\xe0\\x00\\x06\\x00\\x40\\x00\\x10\\xac\\x50\\x00\\x00\\x24\\x10\\xff\\xff\\x02\\x00\\x10\\x21\\x8f\\xbf\\x00\\x24\\x8f\\xb0\\x00\\x20
```

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

7 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%
80	318,071	6%
1433	208,460	3%
3389	179,372	3%
32	155,518	3%
8080	145,657	2%
443	124,800	2%
9200	116,255	2%
25	94,901	2%

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%

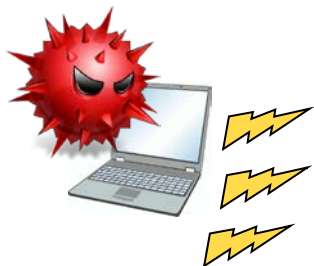
観測される
攻撃パケットの
約4~5割が
Telnet狙い

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

日時

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**罠システム (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



IoT
ハニーポット

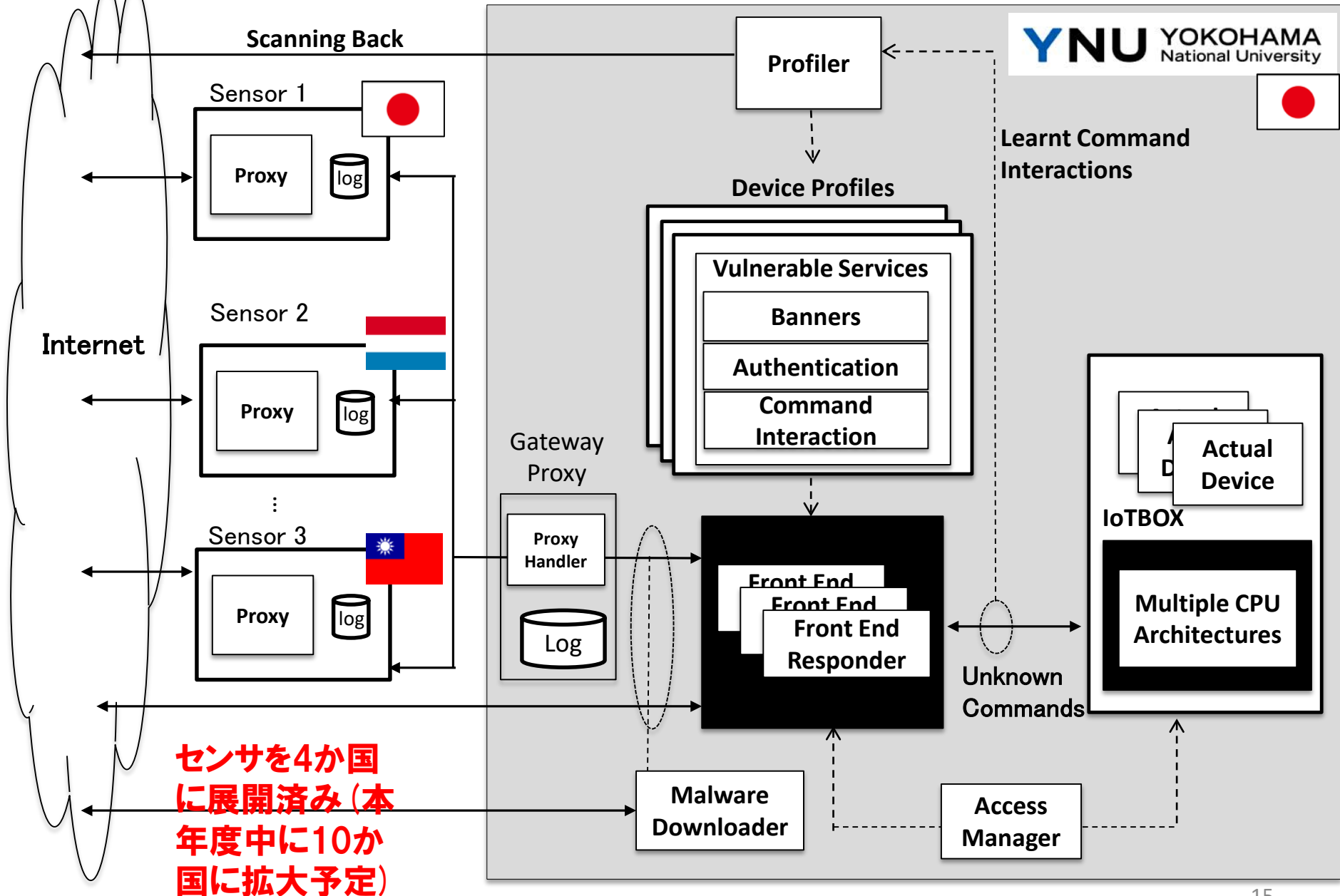


解析システム
(サンドボックス)

マルウェア
捕獲!

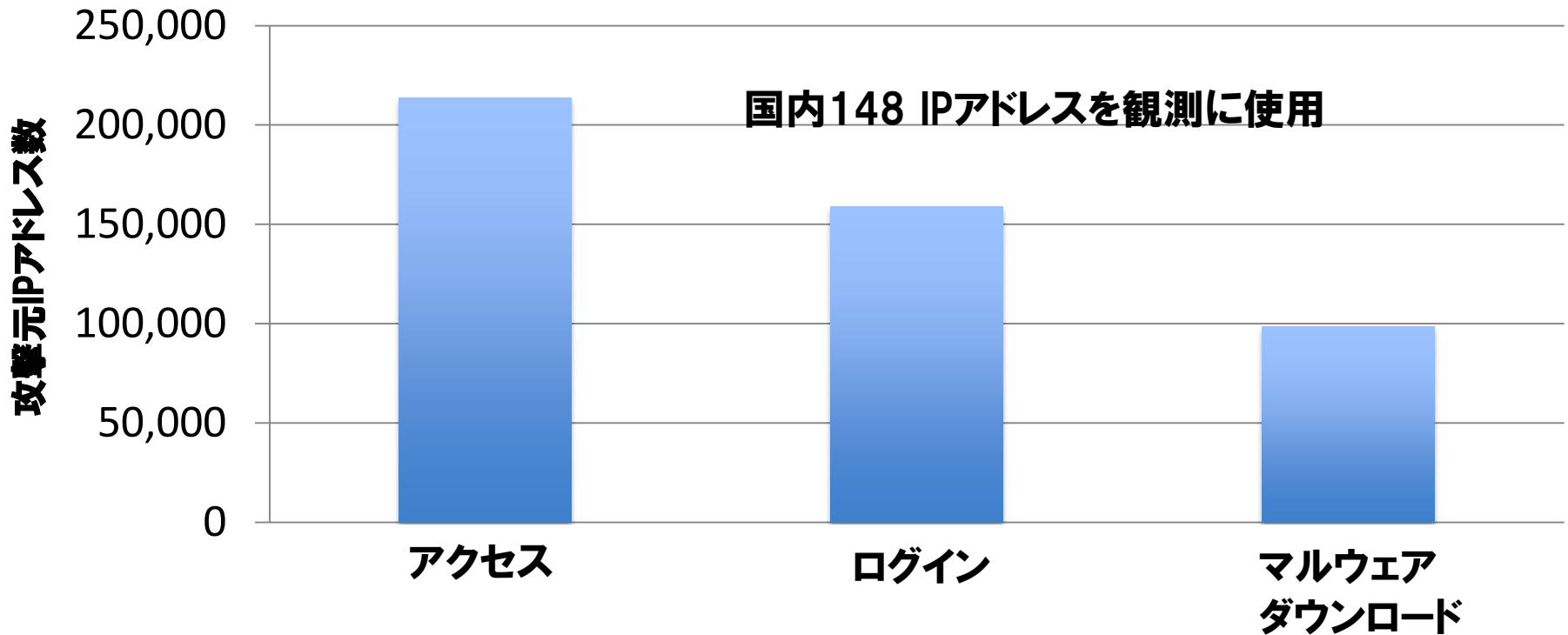
詳細解析!

ハニーポットの構成



観測結果 (昨年)

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

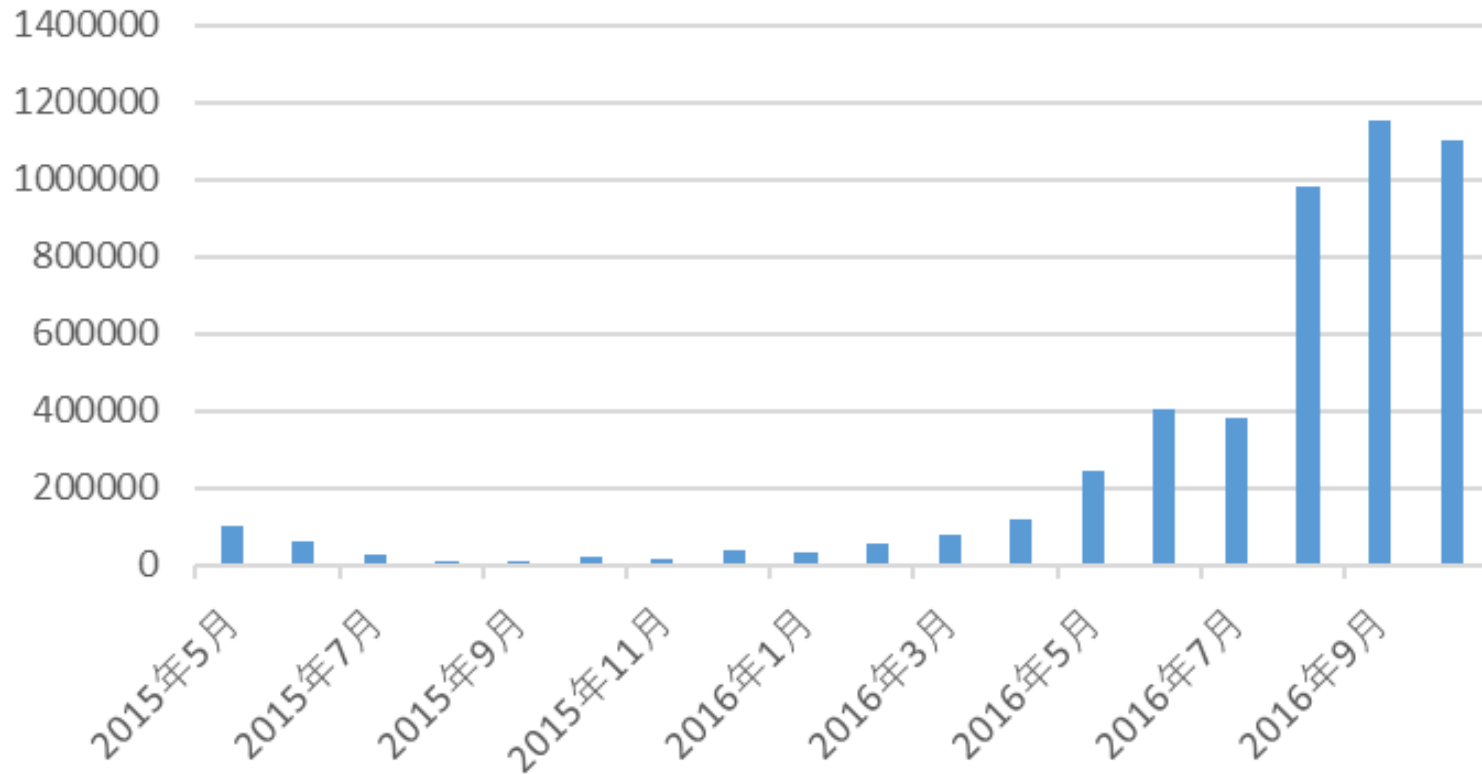
11種類のCPUアーキテクチャ向けマルウェアを捕獲

感染台数の増加 (全世界統計)

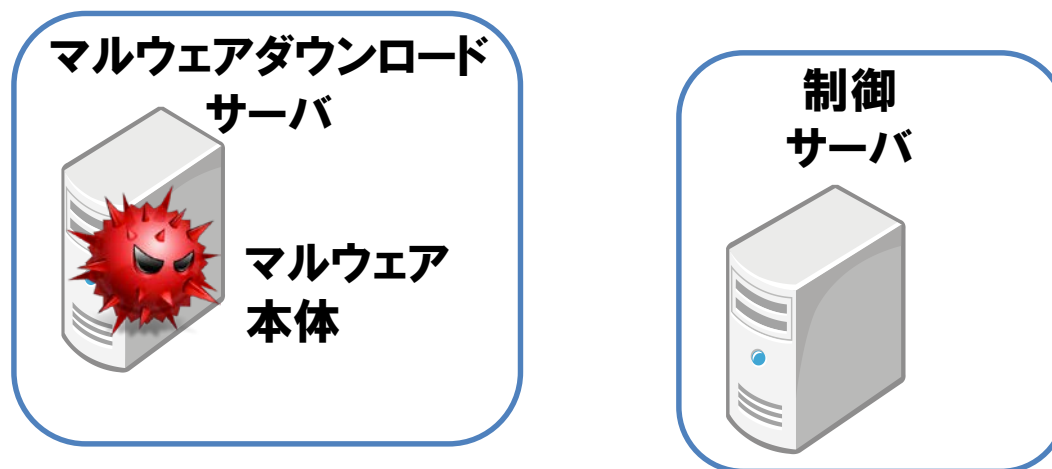
IPアドレス数

感染機器IPアドレス数/月

グラフ タイトル



Telnetベースのマルウェア感染の流れ



攻撃者

2. Telnetによる
環境チェック・
カスタマイズ

3. マルウェア
本体のダウンロード

4. コマンドによる
遠隔操作

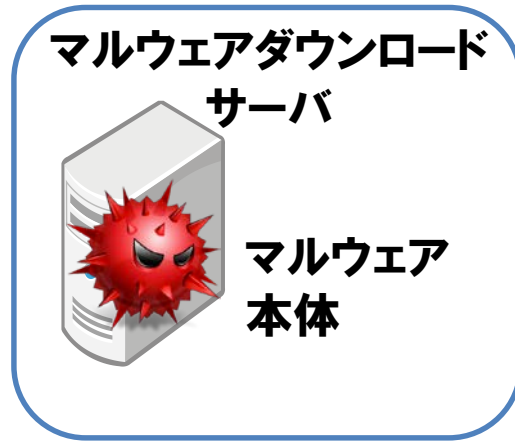
被害者

5. 様々な攻撃

1. Telnetでの辞書
攻撃による侵入



Telnetベースのマルウェア感染の流れ



攻撃者

2. Telnetによる
環境チェック・
カスタマイズ

3. マルウェア
本体のダウンロード

4. コマンドによる
遠隔操作

被害者

5. 様々な攻撃

1. Telnetでの辞書
攻撃による侵入



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/ro[redacted]  
root/admin  
root/1[redacted]  
root/1[redacted]5  
root/1[redacted]56  
root/1[redacted]  
root/password  
root/d[redacted]mbox
```

順序変更型攻撃パターン2

```
root/[redacted]  
root/admin  
root/[redacted]45  
root/[redacted]456  
admin[redacted]oot  
...
```

固定順序攻撃パターン3

```
admin/[redacted]min  
admin/[redacted]729  
admin/[redacted]6h3  
admin/[redacted]yporra  
admin/[redacted]297  
admin/[redacted]m0r  
admin/[redacted]4  
root/12[redacted]
```

順序変更型攻撃パターン1

```
root/[redacted]511  
root/[redacted]456  
root/[redacted]45  
root/[redacted]  
...
```

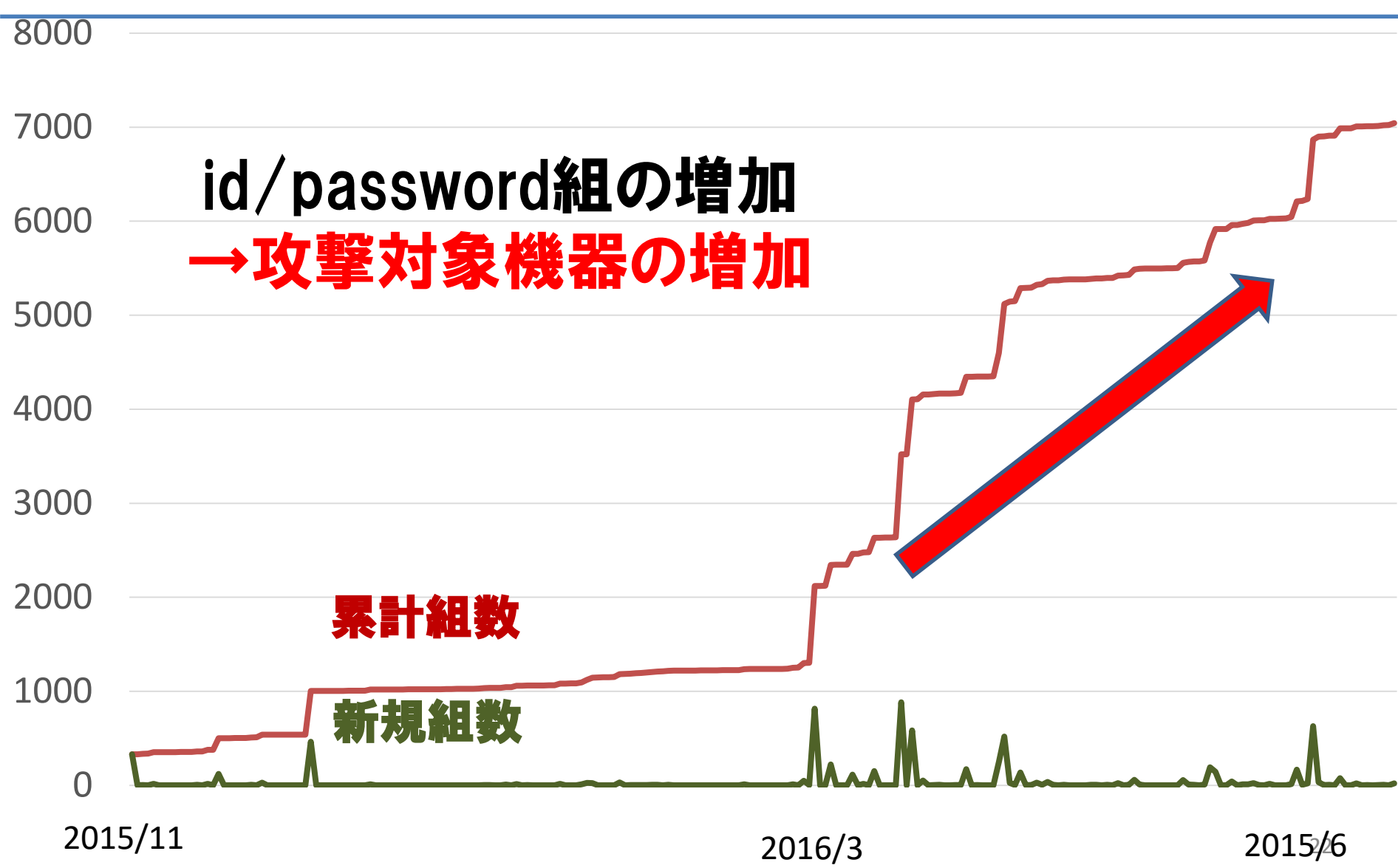
固定順序型攻撃パターン2

```
guest/[redacted]st  
guest/[redacted]45  
admin[redacted]  
root/ro[redacted]  
root/admin  
root/[redacted]  
root/1[redacted]  
root/1[redacted]56  
root/1[redacted]  
root/password  
root/d[redacted]mbox  
root/v[redacted]y
```

順序変更型攻撃パターン3

```
root/[redacted]  
root/[redacted]  
root/admin  
root/[redacted]  
....
```

攻撃に利用されるid/password組の増加



id/password組の増加
→ 攻撃対象機器の増加

累計組数

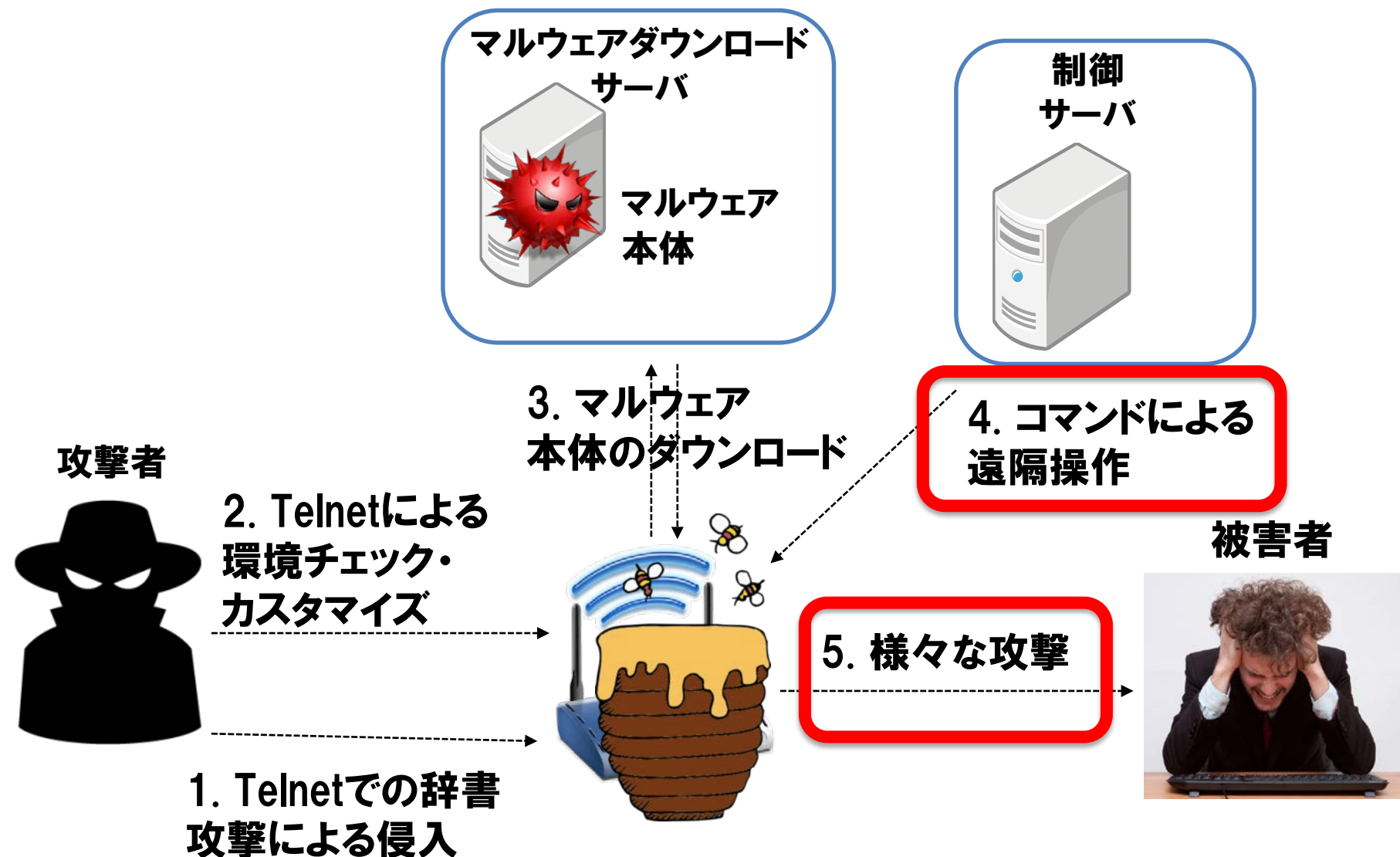
新規組数

2015/11

2016/3

2015/6

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

他の機器の探索・感染

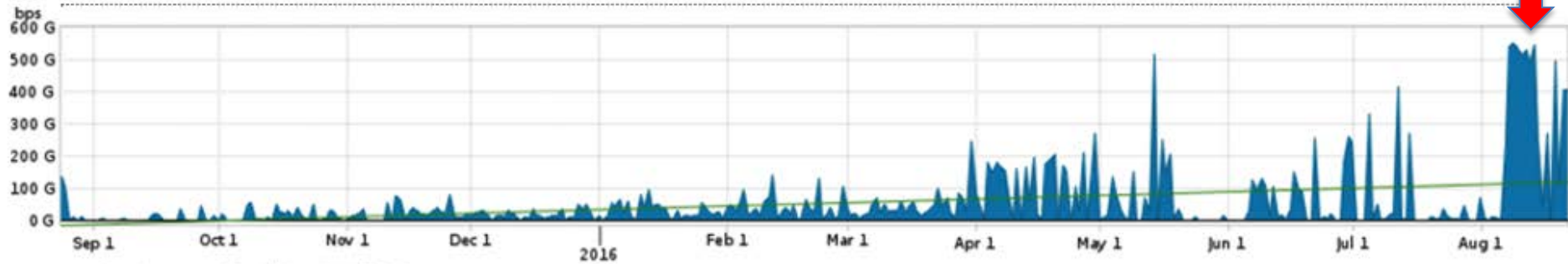
同様のTelnetサービスが動作する機器を探索し感染を広める



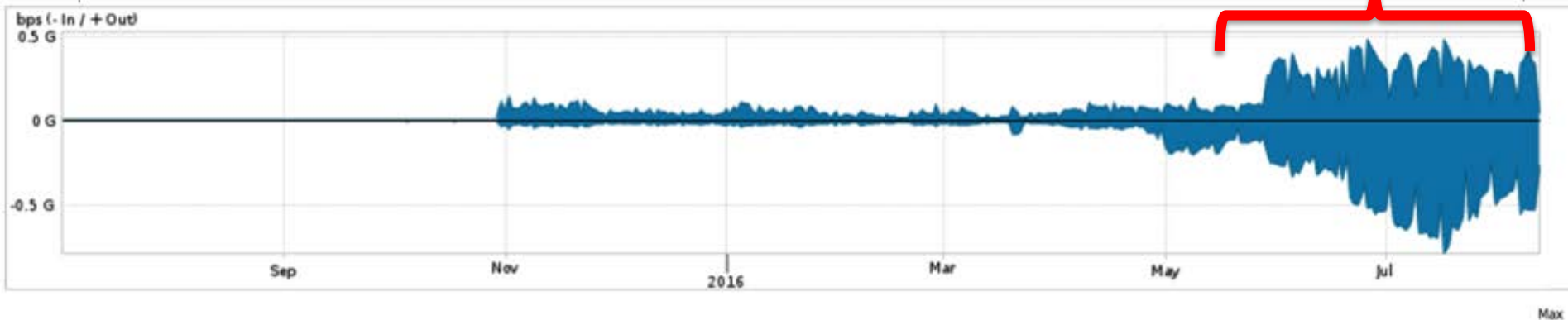
感染機器

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）

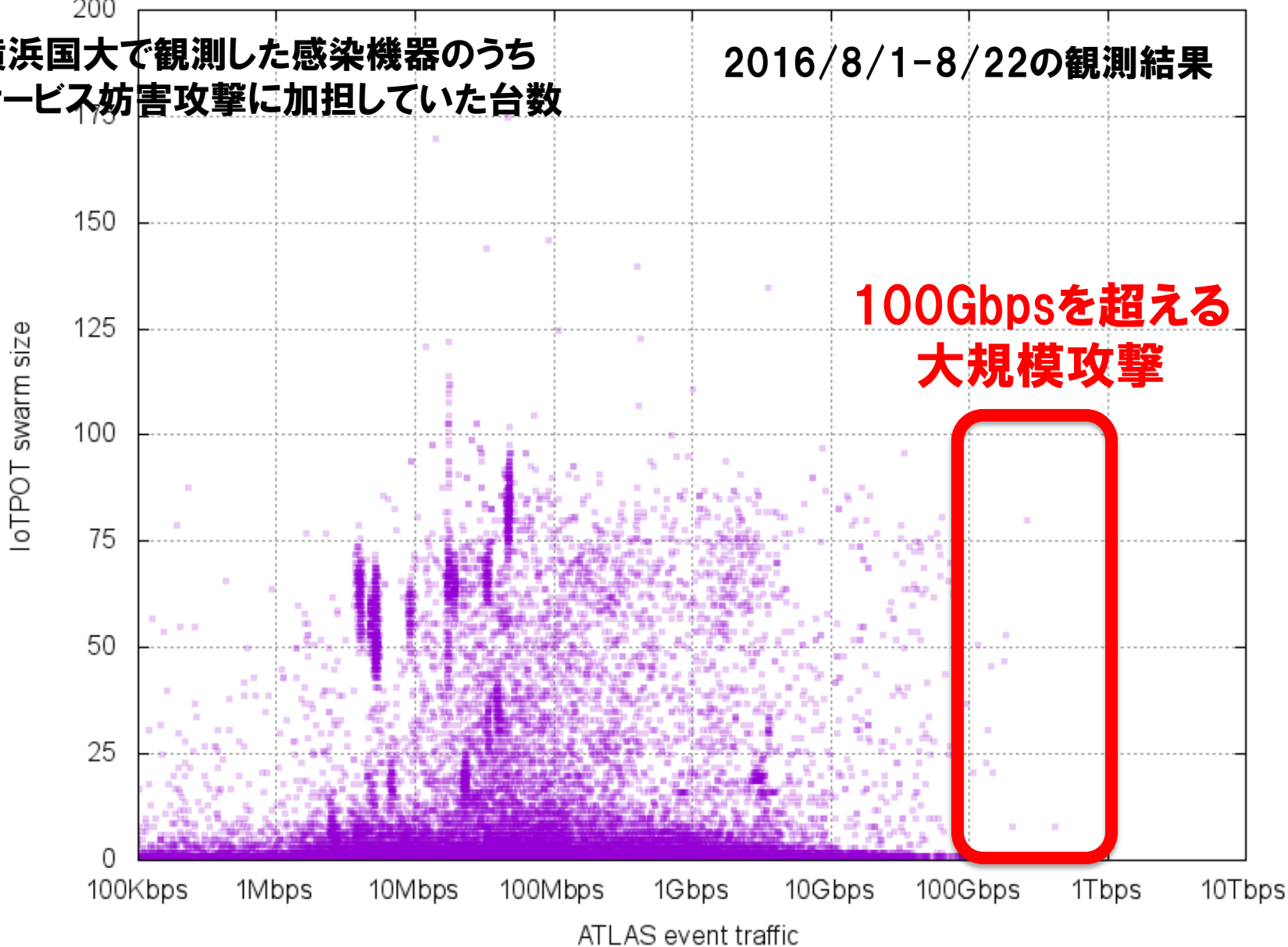


本データは米国Arbor Networks社から提供を受けたものです



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

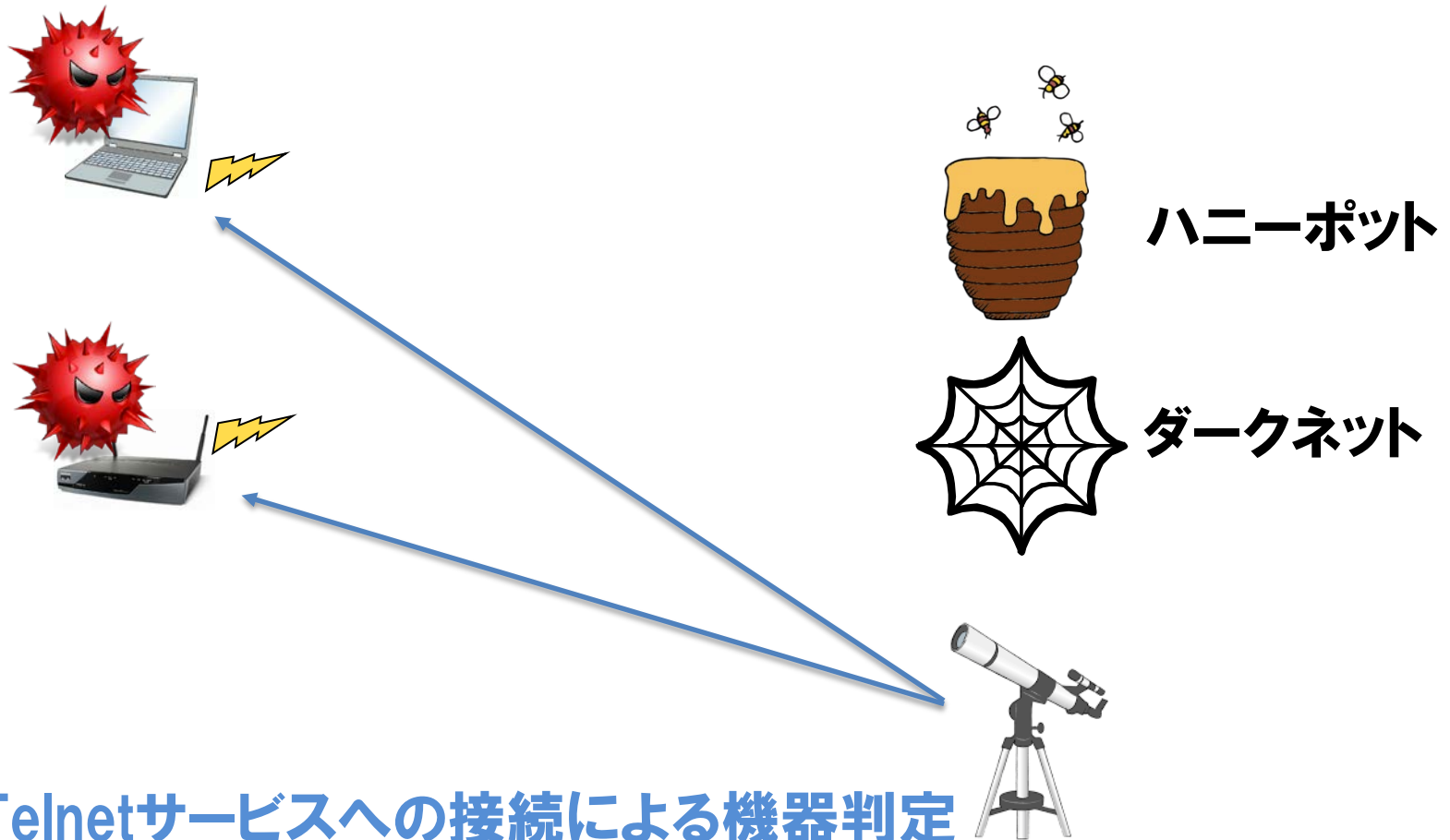
- ダークネットモニタリング
- ハニーポット

- **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

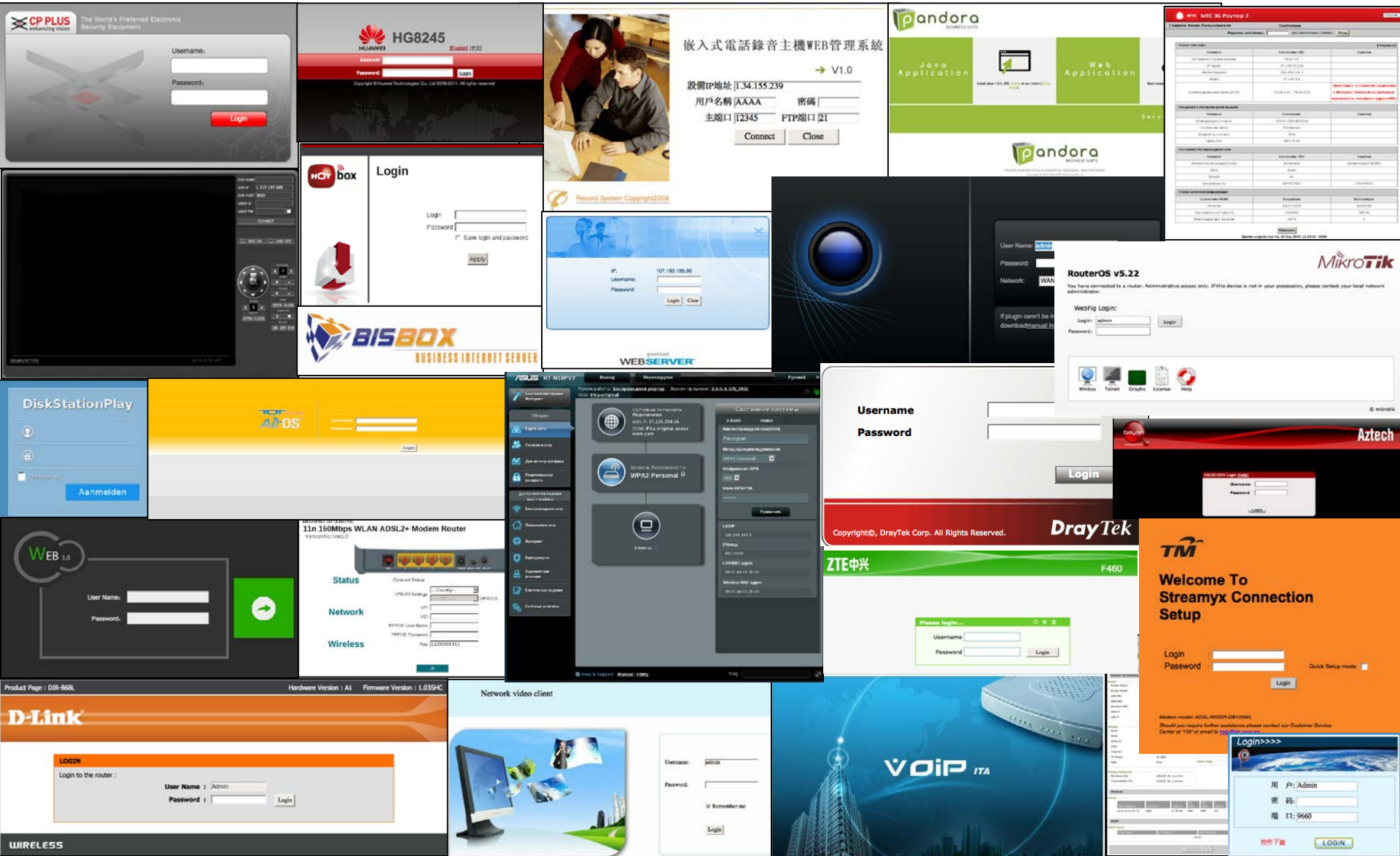
- Web, Telnet, FTP等へのアクセスによる機器、システムの判定
- バックドアポート等の確認

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



攻撃元機器のTelnetバナーの例 (再掲)

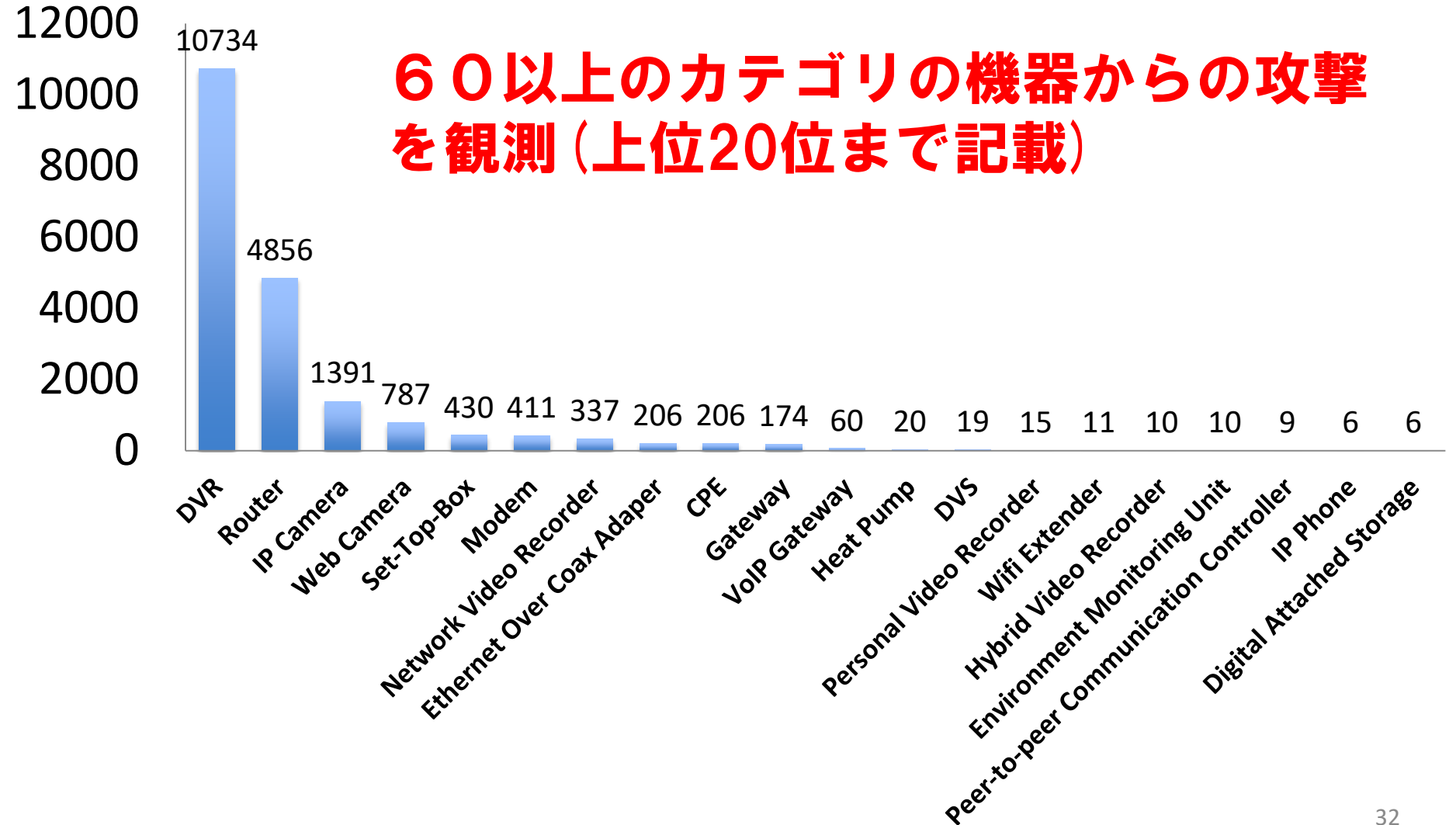
```
op .3.0.dm800se
BC 3 ADSL Router
BC 3 Broadband Router
BC 3 xDSL Router
Ro CLI User Access Verification
op 4 et4x00
Ai v2 login:
Hi on login:
MX oIP-AG login:
Ne login:
TL ON login:
ad login:
dm .login:
dv login:
et login:
```

ハニーポットで観測された感染機器の種類

IPアドレス数

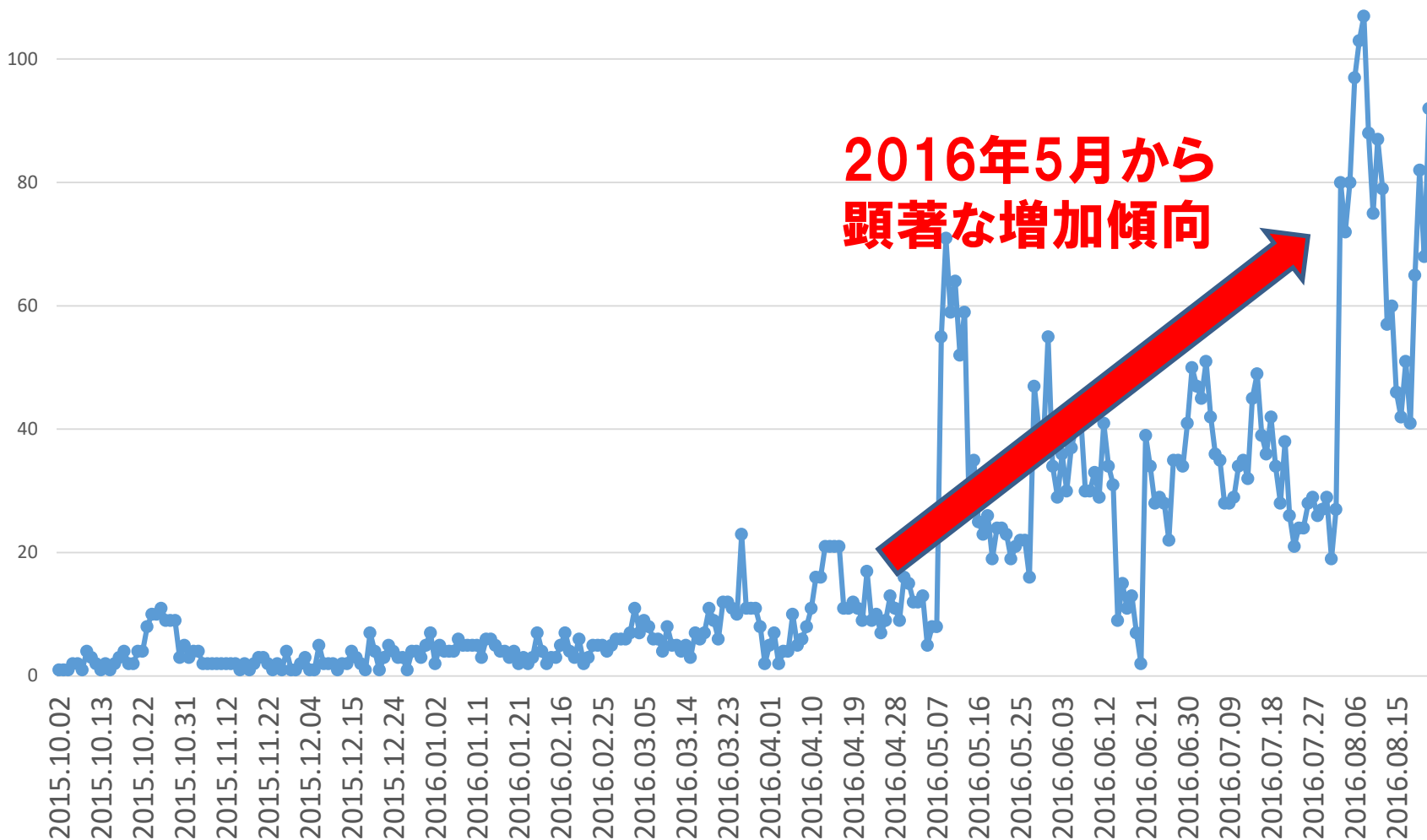
分析対象期間: 2015/5/01-9/30

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)



日本国内 感染機器台数（日ごとにカウント）

IPアドレス/日



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**
 - 感染機器数は増加（侵入に使用するid/passwordも急激に増加）
 - 国内の感染機器数も増加
 - 国内メーカーの感染事例を複数確認
 - 大規模サービス妨害攻撃への加担が確認（600Gbps超の攻撃も）
 - ミシガン大学の大規模調査は、Telnet動作機器がさらに多く存在することを示唆

ちょっと脱線

**Telnet以外は
どうなっている
のでしょうか？**

監視カメラ
“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)

World online live cameras directory | [Avis](#) | [Panasonic](#) | [PanasonicHD](#) | [Linksys](#) | [Sony](#) | [TPLink](#) | [Foscam](#) | [Netcam](#) | [New online cameras](#) | [Sitemap by cities](#)

[Add surveillance camera](#) | [FAQ](#) | [Contacts](#) | [-](#)

- United States(4916)
- Turkey(2392)
- Japan(1555)
- Italy(1107)
- France(987)
- Russian Federation(739)
- United Kingdom(651)
- Netherlands(604)
- India(604)
- Germany(329)
- Sweden(290)
- Spain(288)
- Czech Republic(268)

IP cameras: united states

**日本はカメラ
公開台数
第3位
(2016/9/
15現在)**



9 | 10 | ... 1099 →



Watch Sony camera in
United States
Aurora

Watch Sony camera in
United States
Groton

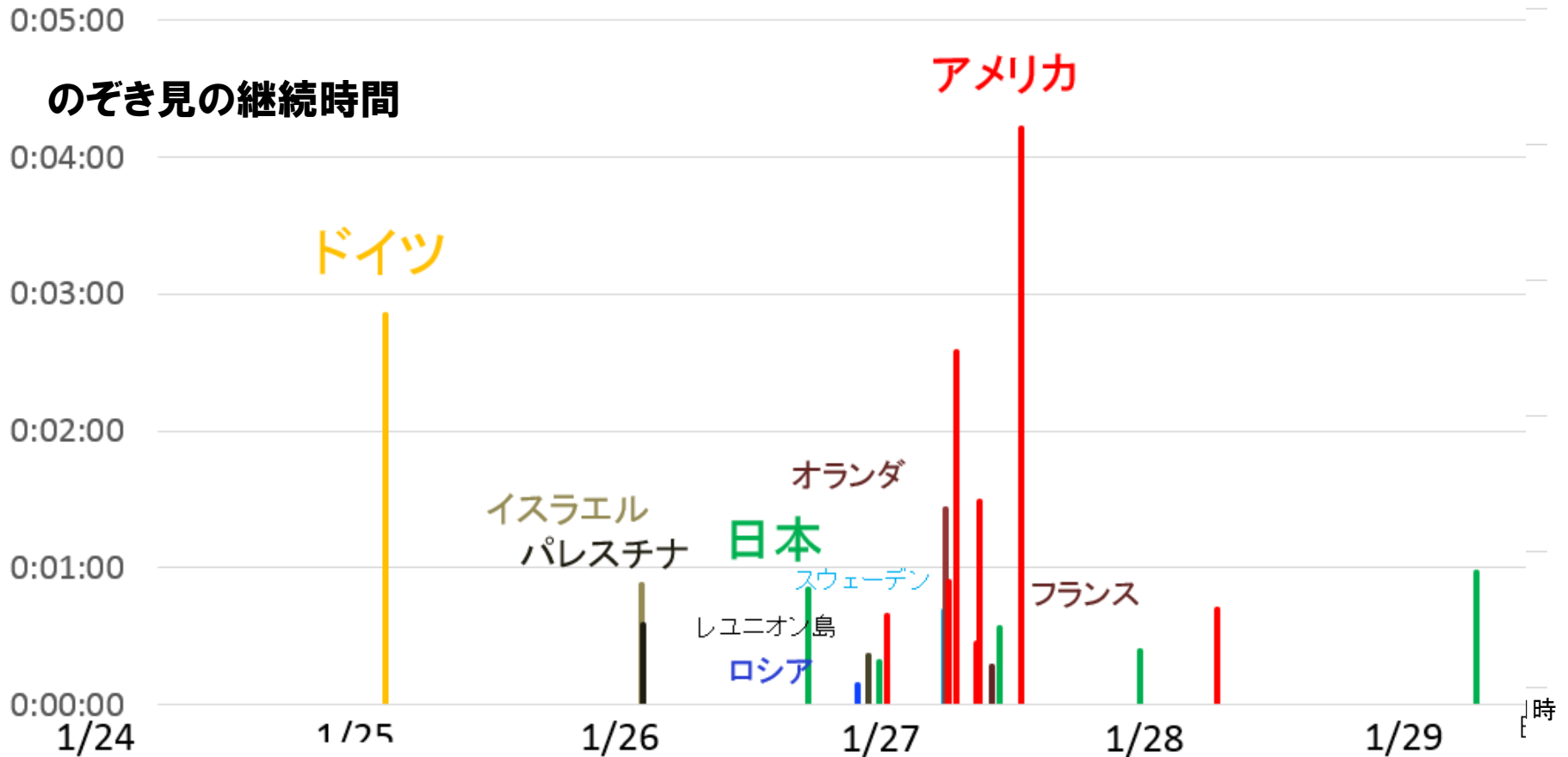
- [City](#)
- [Kitchen](#)
- [Sport](#)
- [Cofeehouse](#)
- [Service](#)
- [Entertainment](#)
- [Interesting](#)
- [Village](#)
- [Server](#)
- [Religion](#)
- [Mall](#)
- [Square](#)
- [Barbershop](#)
- [Airline](#)
- [Animal](#)
- [Warehouse](#)
- [Bar](#)
- [River](#)
- [Beach](#)
- [Construction](#)
- [Guess](#)

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



無断でIPカメラ映像を公開する WebサイトInsecam (ロシア)

The screenshot shows the Insecam website interface. At the top, there are navigation links for various camera brands: Axis, Panasonic, PanasonicHD, Linksys, Sony, TPLink, Foscam, Netcam, New online cameras, and Sitemap by cities. Below this is a search bar and a list of countries with the number of cameras in each. The 'Japan' category is selected, showing a list of cameras with pagination from 1 to 589. A yellow callout bubble points to a server rack image, containing the text 'おとりカメラの映像が掲載!' (Surveillance camera footage is posted!). The server rack image shows a login form with fields for 'Username' and 'password'.

おとりカメラの
映像が掲載！

1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | ... 589 →

Watch [redacted] camera in Japan Tokyo

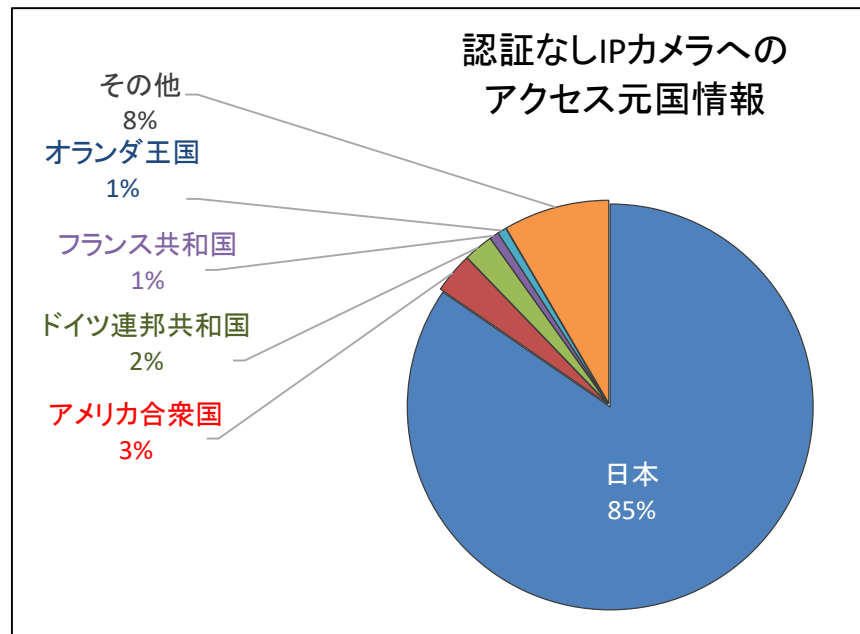
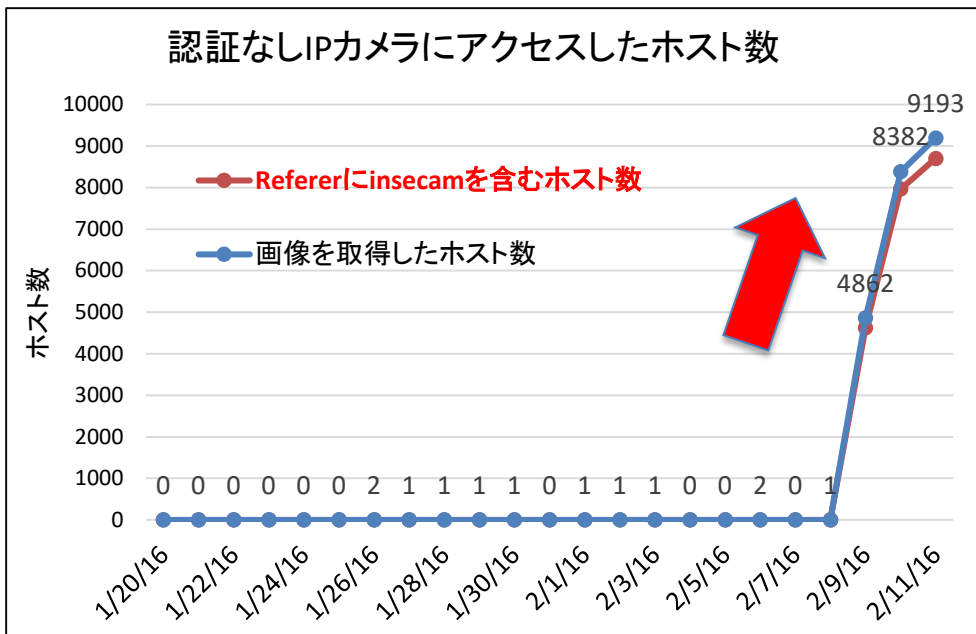
Watch [redacted] camera in Japan Tokyo

Username
password

すべてのダウンロードを表示

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

IOT機器の WEBインターフェースの アクセス制御の状況

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

多数のWiFiルータの発見

- WiFiルータを独自探索により700件以上、Censysにより3000件以上発見した。いずれもオンラインマニュアル等からデフォルトID/ PASSWORDが取得可能
- ビルの空調制御や排水処理システムなどの管理画面（要認証）が発見された
- ユーザ名固定、パスワード空間が狭いなど、認証が脆弱なものを多数含んでいた
- 認証なしに設定変更可能と思われる機器も含まれていた
- 重要と思われるケースについてはメーカーに情報提供済み。（対応中のため詳細説明は控えさせていただきます）

調査の結果わかったこと

Telnetだけでなく、多くの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（ただし、意図して公開している可能性もある）
- 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あれば、デフォルトのままの可能性も十分考えられる）

対策について

デバイス大量感染の元凶はTelnet

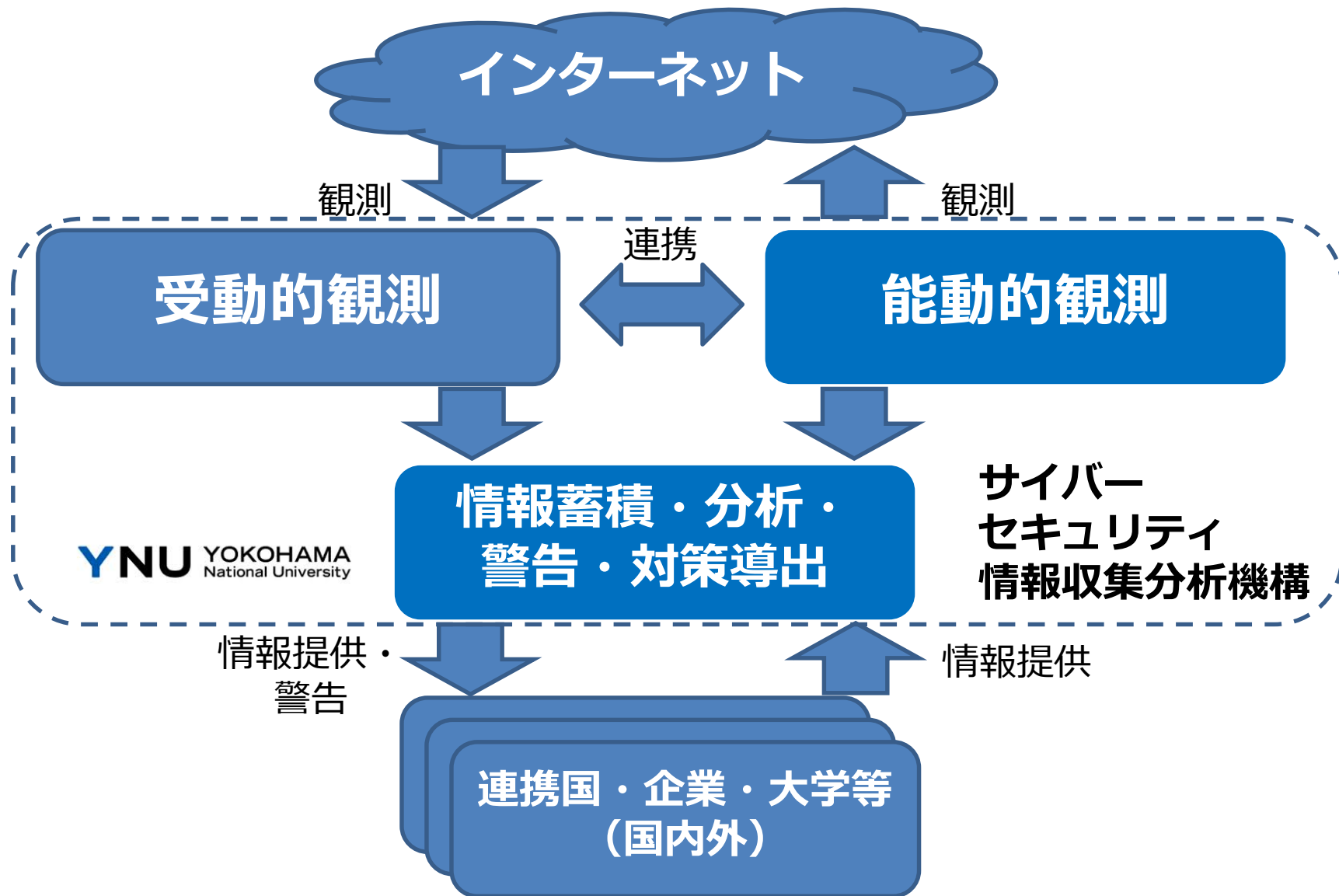
多様なはずのIoTデバイスが
Telnetという共通のセキュリティ問題を
共有してしまっている

<現状のギャップ>

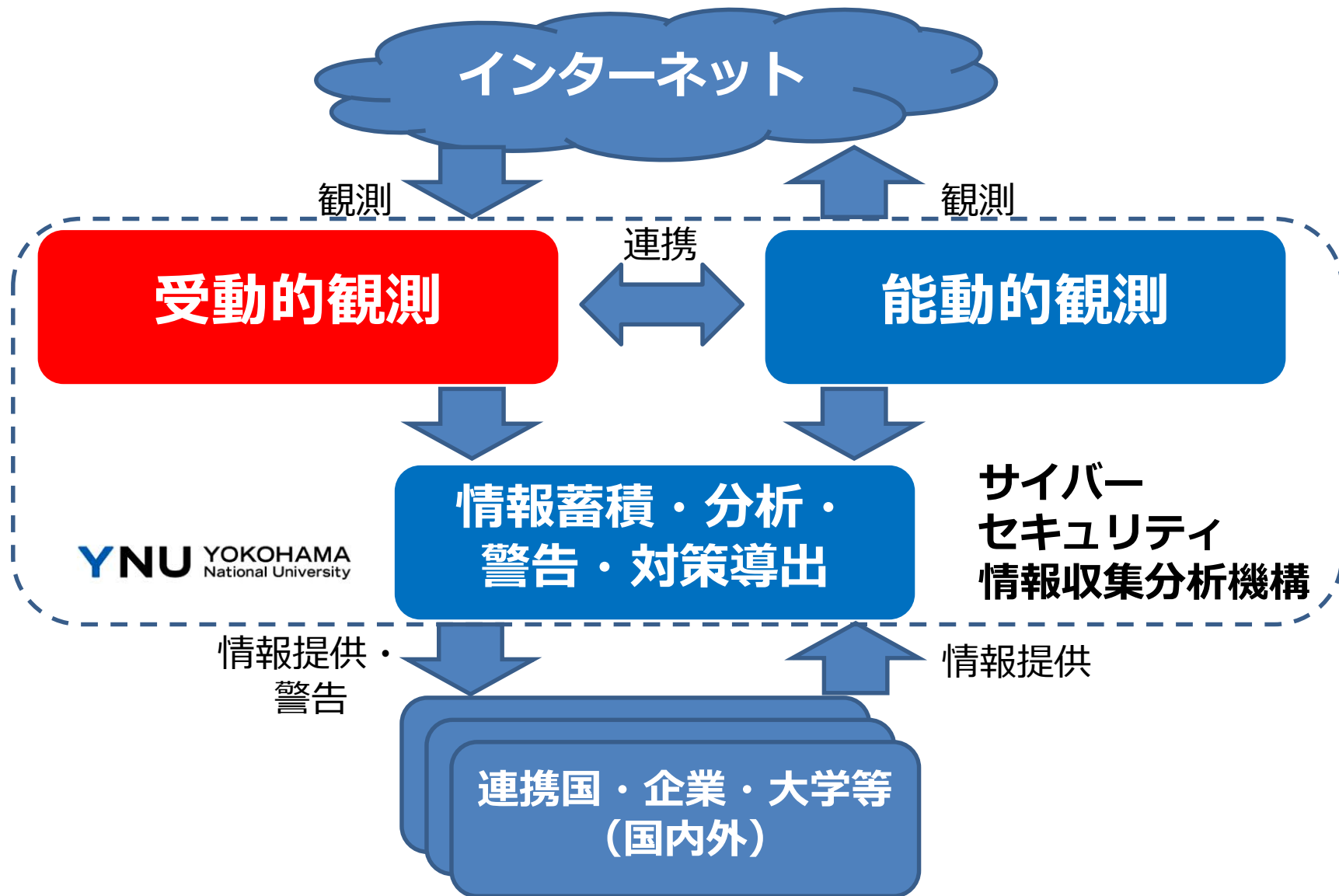
- 製造者側・利用者側は認識していない
 - 攻撃者側は認識している
(ネットワーク攻撃の5割以上がTelnet)

**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**

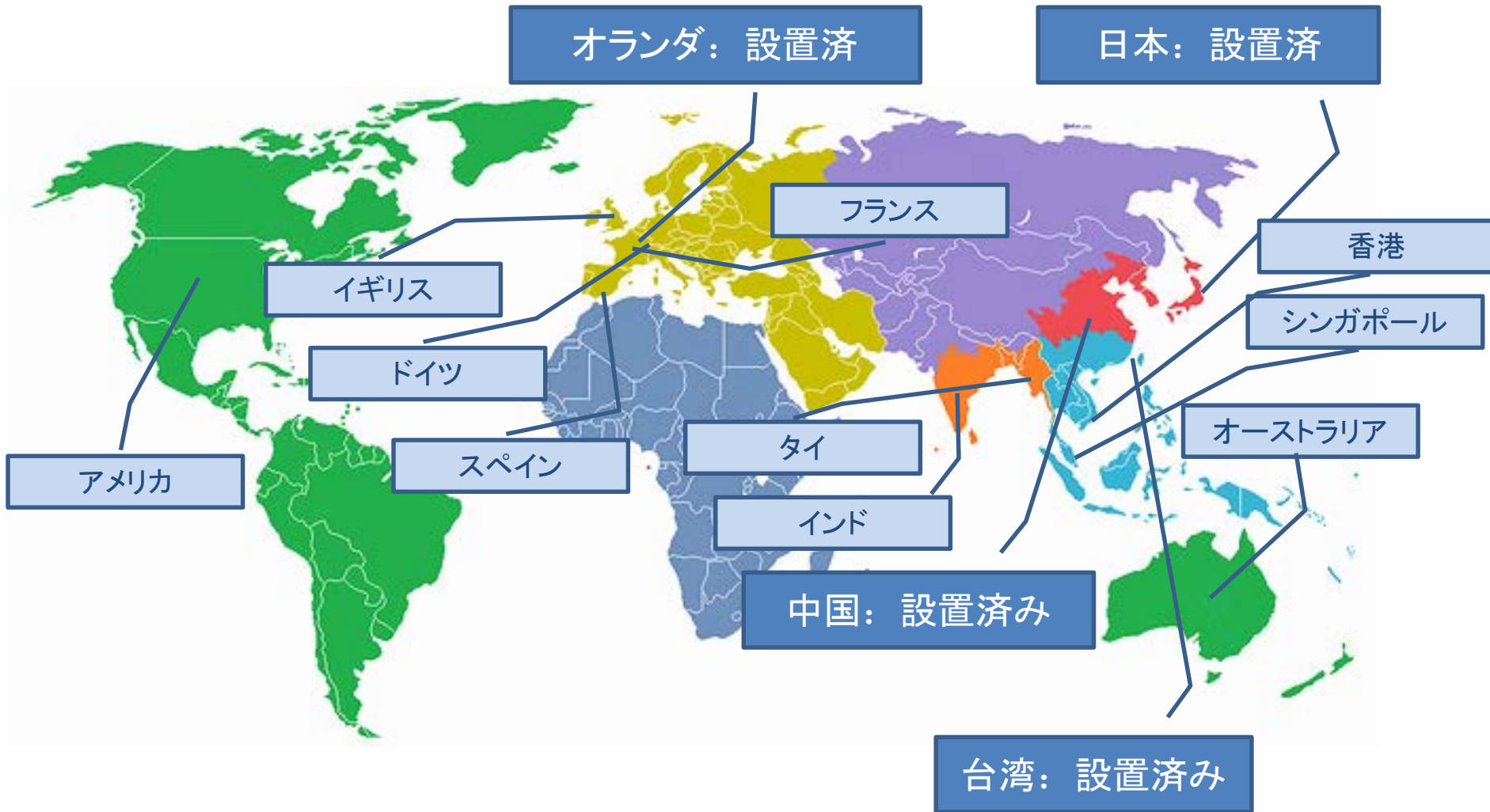
能動的観測と受動的観測を融合させたサイバーセキュリティ情報収集分析機構



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



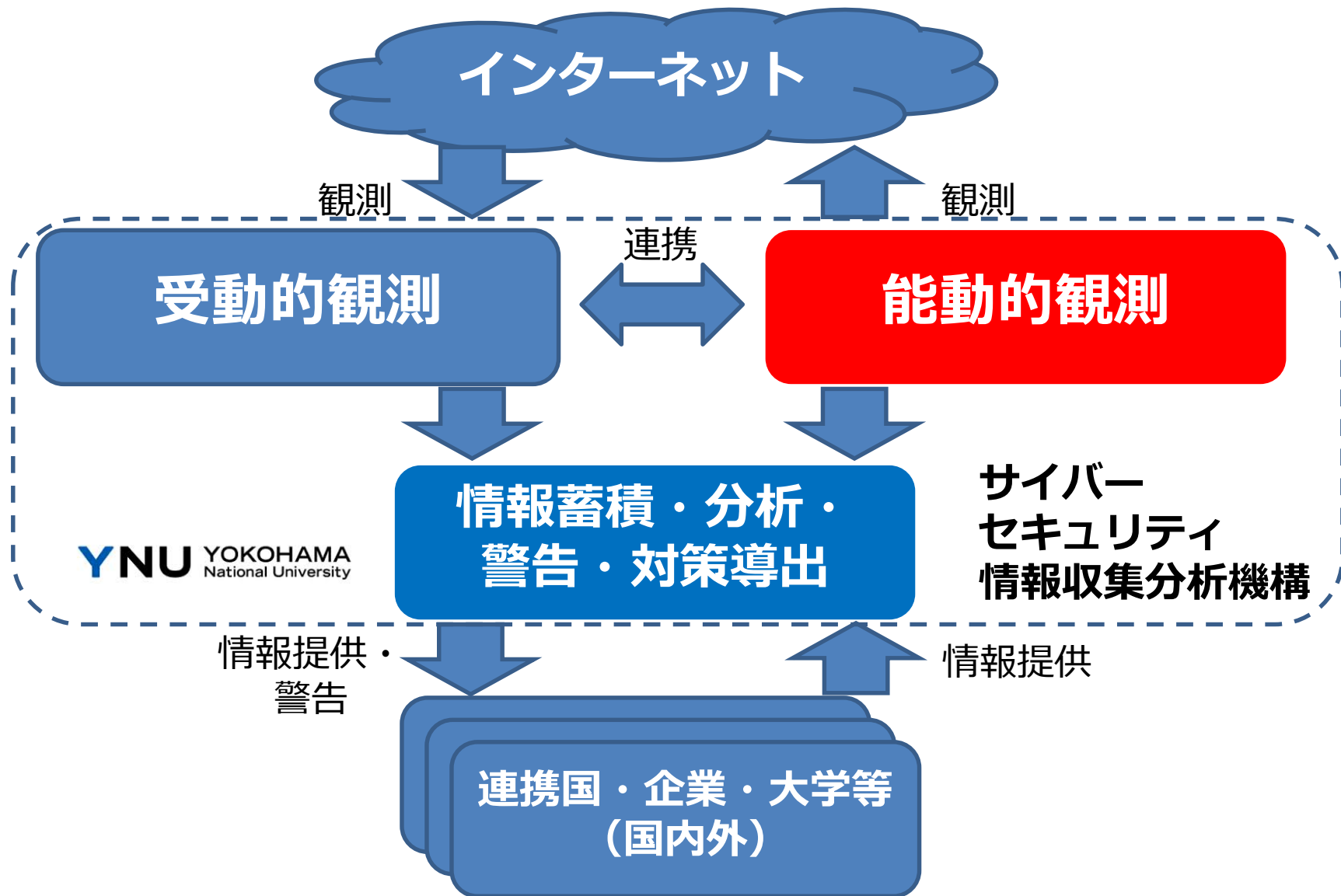
観測地点(国)の拡大



IoT向けハニーポット等の国際展開・機能拡張

- IoTハニーポットの国際展開
 - 現在は国内、オランダ、台湾、中国のみに設置
 - 10カ国・地域に追加展開準備中
 - 研究者によるボランティアセンサの増加
(現在、3カ国)
- 機能拡張
 - Telnet攻撃以外も観測可能に
 - 様々な脆弱性、機器の正確なエミュレート

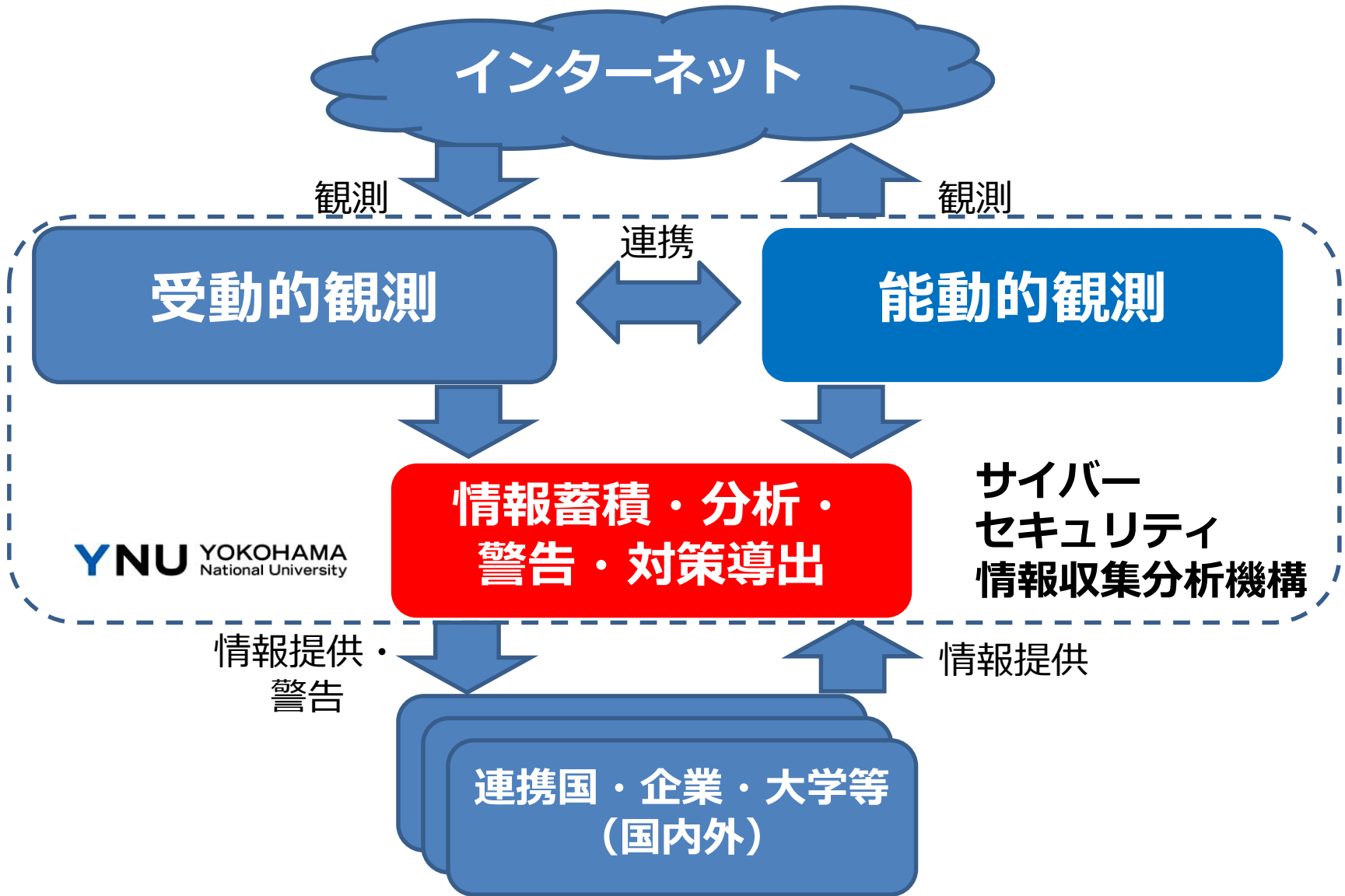
能動的観測と受動的観測を融合させた サイバーセキュリティ情報収集分析機構



能動的観測の高度化

- **攻撃元機器・システムの種別（メーカー、型番など）を特定する精度の向上**
 - オランダ デルフト工科大と連携
 - **新たな感染機器（医療機器等）の発見**
 - 個々の機器を判別する技術の開発（IPアドレスが変更しても感染機器の追跡調査が可能）
- **大規模な能動的観測を行っているCenSys、Shodanのデータ利用を検討中**
- **ローカル調査も実施**

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

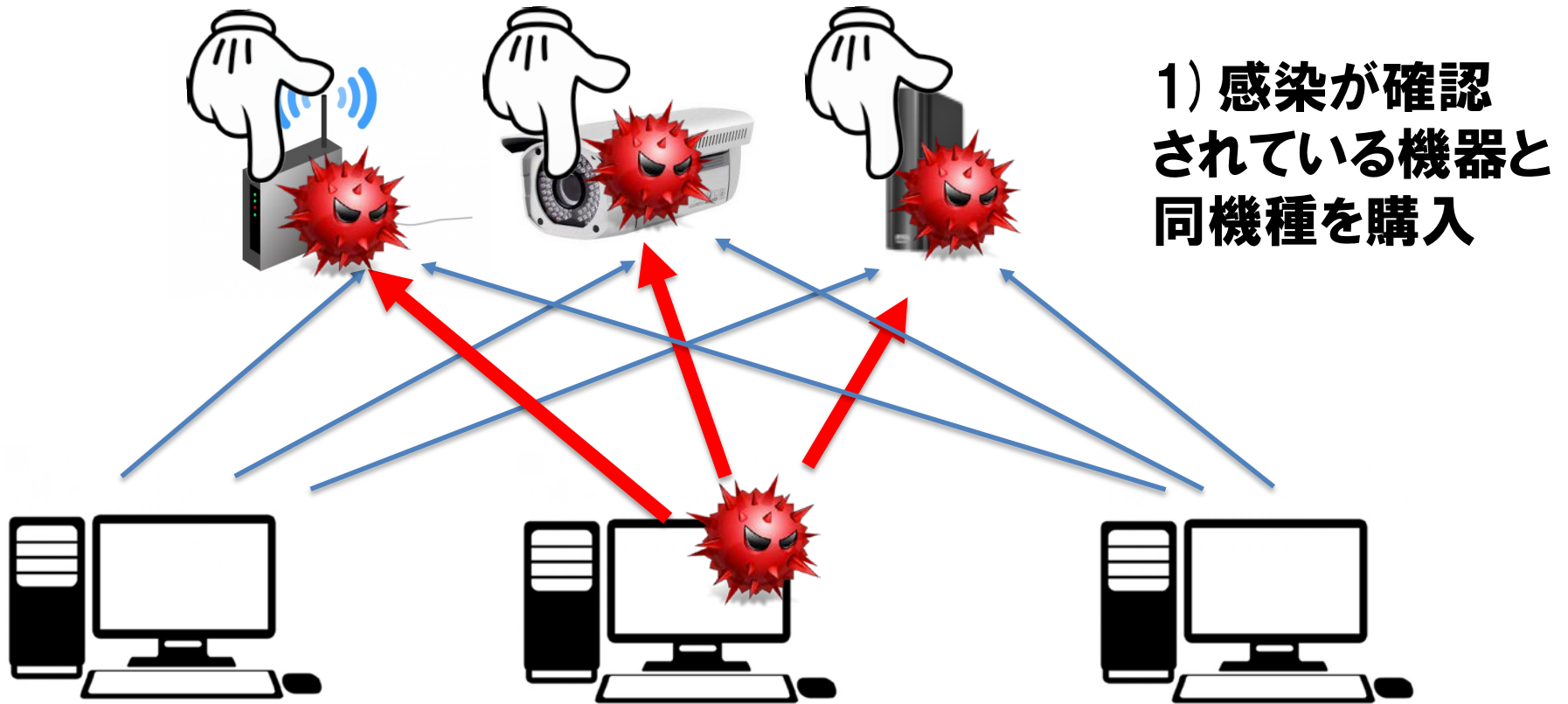


情報蓄積・分析・警告・対策導出機能の高度化

- **情報蓄積・検索能力の向上**
 - ビッグデータ分析技術の導入
- **分析技術の向上**
 - マルウェア動的解析・静的解析
 - ソフトウェア・ファームウェア脆弱性分析
- **警告・通報**
 - **感染機器情報の提供**
JPCERT/CC, 内閣サイバーセキュリティセンター, 各国CERT, メーカー
- **対策導出**
 - **マルウェア機能無効化、駆除、パッチ、IoT向けペネトレーションツールの開発**

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⁵⁸

IoTマルウェア駆除実験 結果1 (外国製A社ルータ)

	マルウェア1	マルウェア2	マルウェア3	マルウェア4	マルウェア5
①再起動 (rebootコマンド)	駆除成功・ 機器設定も 保存される	駆除成功・ 機器設定も 保存される	マルウェアが 動作せず	駆除成功・ 機器設定も 保存される	駆除成功・ 機器設定も 保存される
②主電源 OFF	駆除成功・ 機器設定も 保存される	駆除成功・ 機器設定も 保存される	マルウェアが 動作せず	駆除成功・ 機器設定も 保存される	駆除成功・ 機器設定も 保存される
③工場出荷 状態(初期 状態)に戻す	駆除成功 ただし機器 設定も初期 状態になる	駆除成功 ただし機器 設定も初期 状態になる	マルウェアが 動作せず	駆除成功 ただし機器 設定も初期 状態になる	駆除成功 ただし機器 設定も初期 状態になる

①rebootコマンドによる機器再起動

②主電源OFF

③工場出荷(初期)状態に戻す

のいずれでも4種類のマルウェア駆除が可能だが主電源OFF
またはrebootコマンドにより機器設定を失わずに駆除が可能

IoTマルウェア駆除実験 結果2 (外国製B社ルータ)

	マルウェア1	マルウェア2	マルウェア3	マルウェア4	マルウェア5
①再起動 (rebootコマンド)	駆除成功・ 機器設定も 保存される	駆除成功・ 機器設定も 保存される	マルウェアが 動作せず	駆除成功・ 機器設定も 保存される	駆除成功・ 機器設定も 保存される
②主電源 OFF	駆除成功・ 機器設定も 保存される	駆除成功・ 機器設定も 保存される	マルウェアが 動作せず	駆除成功・ 機器設定も 保存される	駆除成功・ 機器設定も 保存される
③工場出荷 状態(初期 状態)に戻す	駆除成功 ただし機器 設定も初期 状態になる	駆除成功 ただし機器 設定も初期 状態になる	マルウェアが 動作せず	駆除成功 ただし機器 設定も初期 状態になる	駆除成功 ただし機器 設定も初期 状態になる

A社ルータと全く同様の結果

IoTマルウェア駆除実験 結果3 (外国製C社IPカメラ)

	マルウェア1	マルウェア2	マルウェア3	マルウェア4	マルウェア5
①再起動 (rebootコマンド)	駆除成功・ 機器設定も 保存される	駆除成功・ 機器設定も 保存される	駆除成功・ 機器設定も 保存される	駆除成功・ 機器設定も 保存される	駆除成功・ 機器設定も 保存される
②主電源 OFF	駆除成功 ただし機器 設定も初期 状態になる	駆除成功 ただし機器 設定も初期 状態になる	駆除成功 ただし機器 設定も初期 状態になる	駆除成功 ただし機器 設定も初期 状態になる	駆除成功 ただし機器 設定も初期 状態になる
③工場出荷 状態(初期 状態)に戻す	駆除成功 ただし機器 設定も初期 状態になる	駆除成功 ただし機器 設定も初期 状態になる	駆除成功 ただし機器 設定も初期 状態になる	駆除成功 ただし機器 設定も初期 状態になる	駆除成功 ただし機器 設定も初期 状態になる

①rebootコマンドによる機器再起動

②主電源OFF

③工場出荷(初期)状態に戻す

のいずれでも5種類のマルウェア駆除が可能だが、rebootコマンドにより機器設定を失わずに駆除が可能

IoTマルウェア駆除実験 結果4 (国産C社ネットワークストレージ)

	マルウェア1	マルウェア2	マルウェア3	マルウェア4	マルウェア5
①再起動 (rebootコマンド)	コマンド使用 できず	コマンド使用 できず	コマンド使用 できず	コマンド使用 できず	コマンド使用 できず
②主電源 OFF	駆除成功・ 機器設定も 保存される	駆除成功・ 機器設定も 保存される	駆除成功・ 機器設定も 保存される	駆除成功・ 機器設定も 保存される	駆除成功・ 機器設定も 保存される
③工場出荷 状態(初期 状態)に戻す	駆除成功 ただし機器 設定も初期 状態になる	駆除成功 ただし機器 設定も初期 状態になる	駆除成功 ただし機器 設定も初期 状態になる	駆除成功 ただし機器 設定も初期 状態になる	駆除成功 ただし機器 設定も初期 状態になる

①主電源OFF

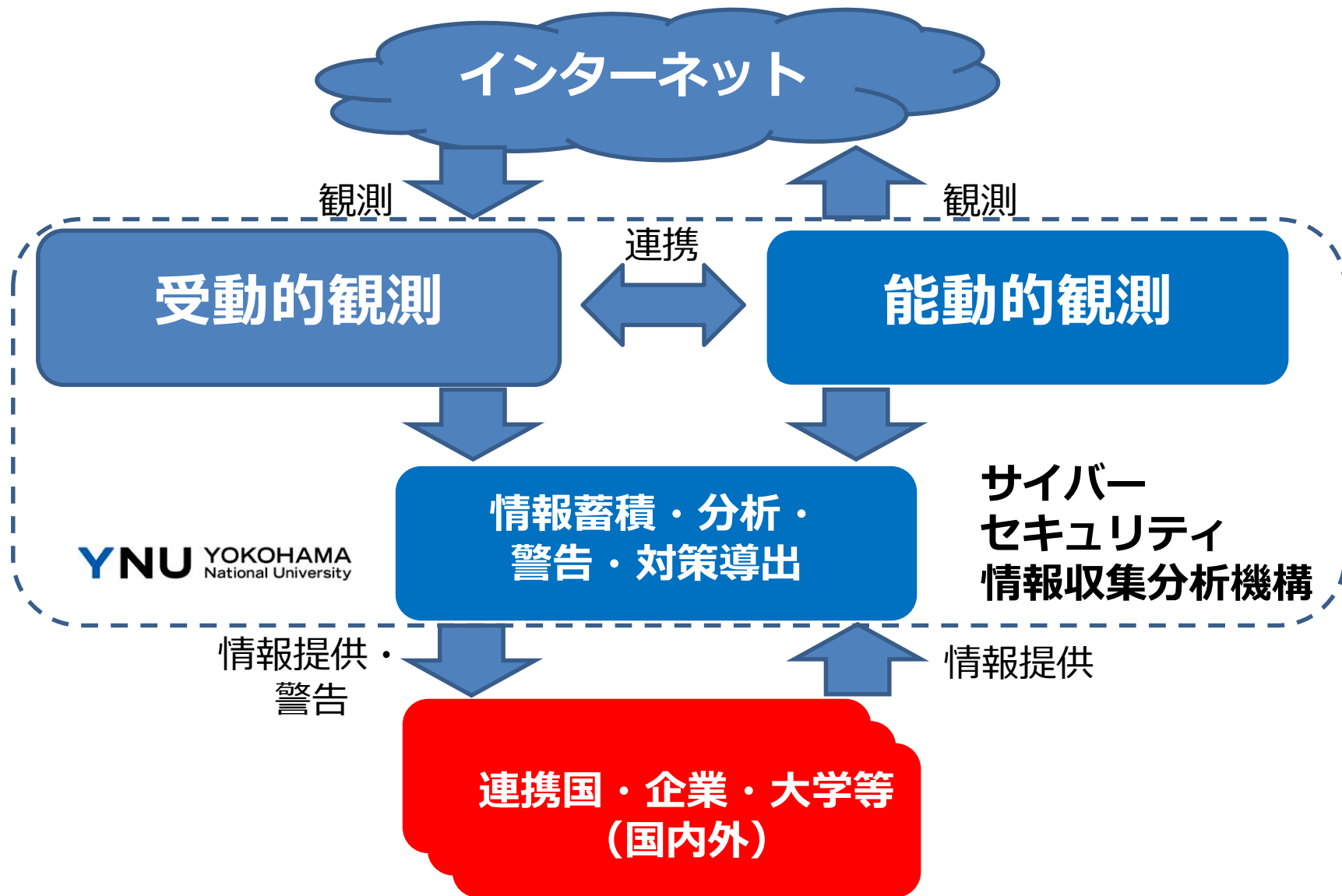
②工場出荷(初期)状態に戻す

のいずれでも**マルウェア2の駆除が可能**

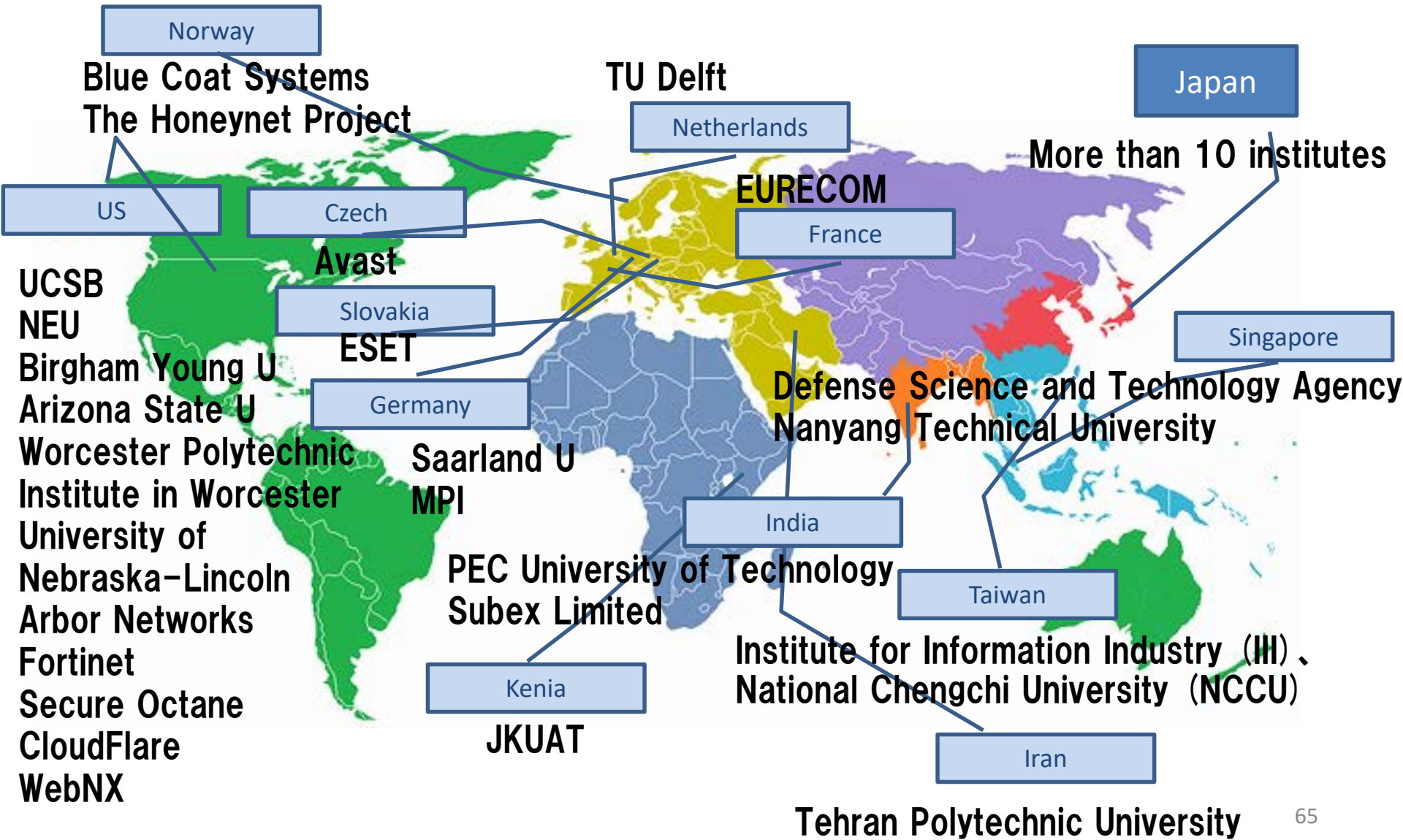
駆除実験まとめ

- 実験に使用した全てのIoTマルウェアは不揮発領域に自身のコピーを作っておらず、ルータ、IPカメラ、ネットワークストレージのいずれについても再起動/電源OFF/工場出荷状態へ戻すことにより**容易に駆除が可能**だった
- この理由として以下が考えられるが詳細は要調査
 - いつでも感染させられるので定常的に感染させる必要がない？(ただし、攻撃者間でも感染機器の争奪戦があるため、いつでも感染させられるとは言い切れない)
 - 機器により内部構成が異なるため、汎用的に継続感染させることが困難？
- 感染機器さえ正確にわかれば、駆除自体は容易であるため、「**感染機器発見→駆除→Telnet停止**」という一連の**対策により、再感染を止められる可能性がある**(ただし、再起動するたびにTelnet停止するか、ファームウェア更新により永続的に対策を行う必要がある)

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



観測情報を世界40以上の研究組織 セキュリティ企業に提供中



Telnetの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)

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
- 上記は初歩的なセキュリティ対策により解決可能であるが、これを国内外の機器ベンダに周知、対応徹底するのは、運用上は非常に困難
- 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ーの自助努力のみで**現状が自然回復するとは考えにくい**
- 感染機器の**発見・追跡・通知・駆除・脆弱性修正**といった対策を行う施策が必要
→ 施策実施時に必要となるコア技術の研究開発



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。