IoTにおけるサイバー攻撃の実態とその対策

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9回情報戦略フォーラム（2017.8.9）

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

- 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

デバイスはWebおよびTelnetの応答から判断しています.

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

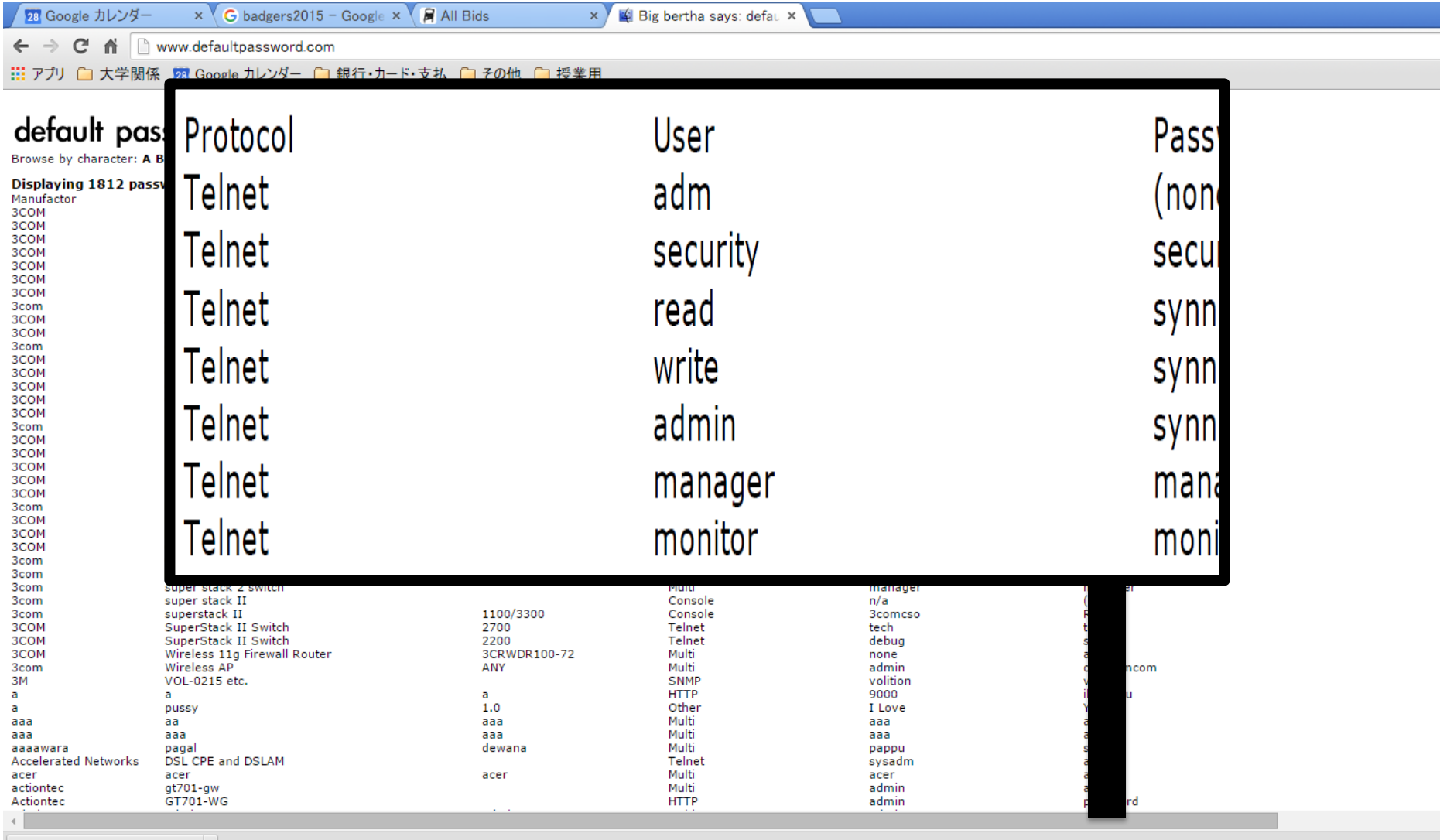
しかも多くは
デフォルト/弱いパスワードで

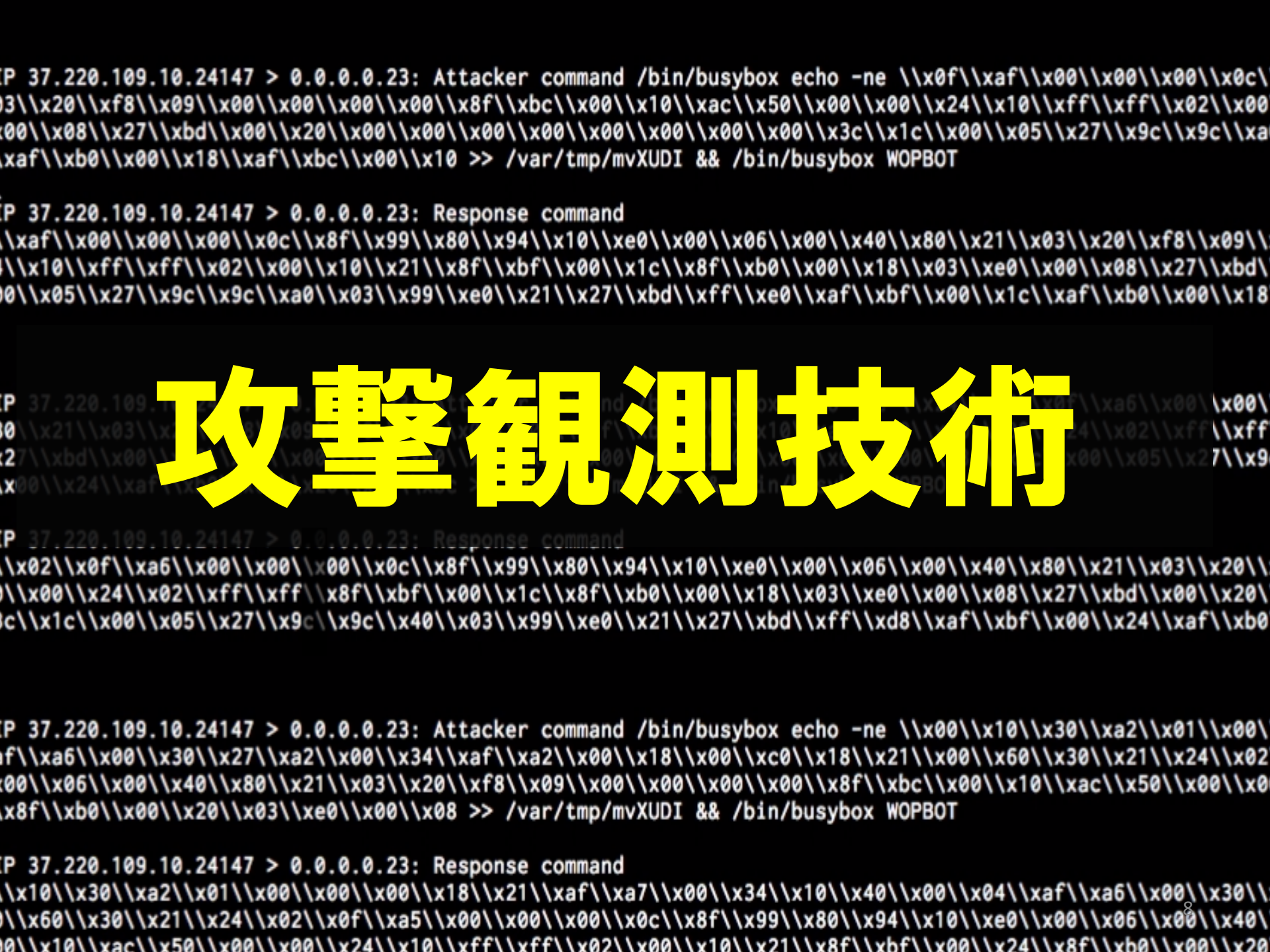
```
[shogo@www9058up ~]$ telnet x.x.243.13
Trying x.x.243.13...
Connected to x.x.243.13.
Escape character is '^]'.

[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.
```

デフォルトパスワードはWeb等でも簡単に手に入れられます



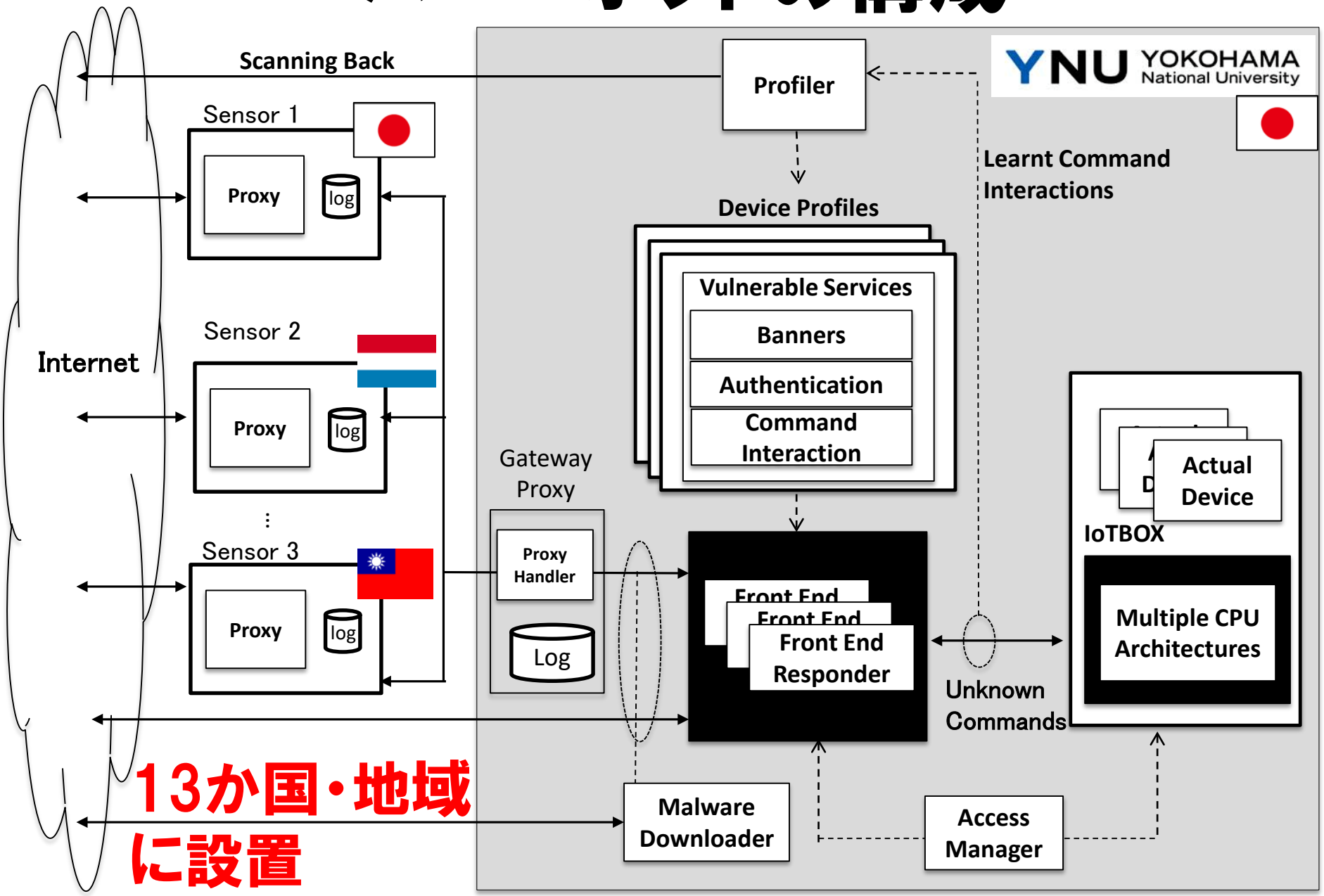

P 37.220.109.10.24147 > 0.0.0.0.23: Attacker command /bin/busybox echo -ne \\x0f\\xaf\\x00\\x00\\x00\\x0c\
03\\x20\\xf8\\x09\\x00\\x00\\x00\\x00\\x8f\\xbc\\x00\\x10\\xac\\x50\\x00\\x00\\x24\\x10\\xff\\xff\\x02\\x00
x00\\x08\\x27\\xbd\\x00\\x20\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x3c\\x1c\\x00\\x05\\x27\\x9c\\x9c\\xa
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\\
\\x10\\xff\\xff\\x02\\x00\\x10\\x21\\x8f\\xbf\\x00\\x1c\\x8f\\xb0\\x00\\x18\\x03\\xe0\\x00\\x08\\x27\\xbd\
0\\x05\\x27\\x9c\\x9c\\xa0\\x03\\x99\\xe0\\x21\\x27\\xbd\\xff\\xe0\\xaf\\xbf\\x00\\x1c\\xaf\\xb0\\x00\\x18
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\
c\\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
00\\x06\\x00\\x40\\x80\\x21\\x03\\x20\\xf8\\x09\\x00\\x00\\x00\\x00\\x8f\\xbc\\x00\\x10\\xac\\x50\\x00\\x0
x8f\\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\\
\\x60\\x30\\x21\\x24\\x02\\x0f\\xa5\\x00\\x00\\x00\\x0c\\x8f\\x99\\x80\\x94\\x10\\xe0\\x00\\x06\\x00\\x40\
0\\x10\\xac\\x50\\x00\\x00\\x24\\x10\\xff\\xff\\x02\\x00\\x10\\x21\\x8f\\xbf\\x00\\x24\\x8f\\xb0\\x00\\x20

攻撃観測技術

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

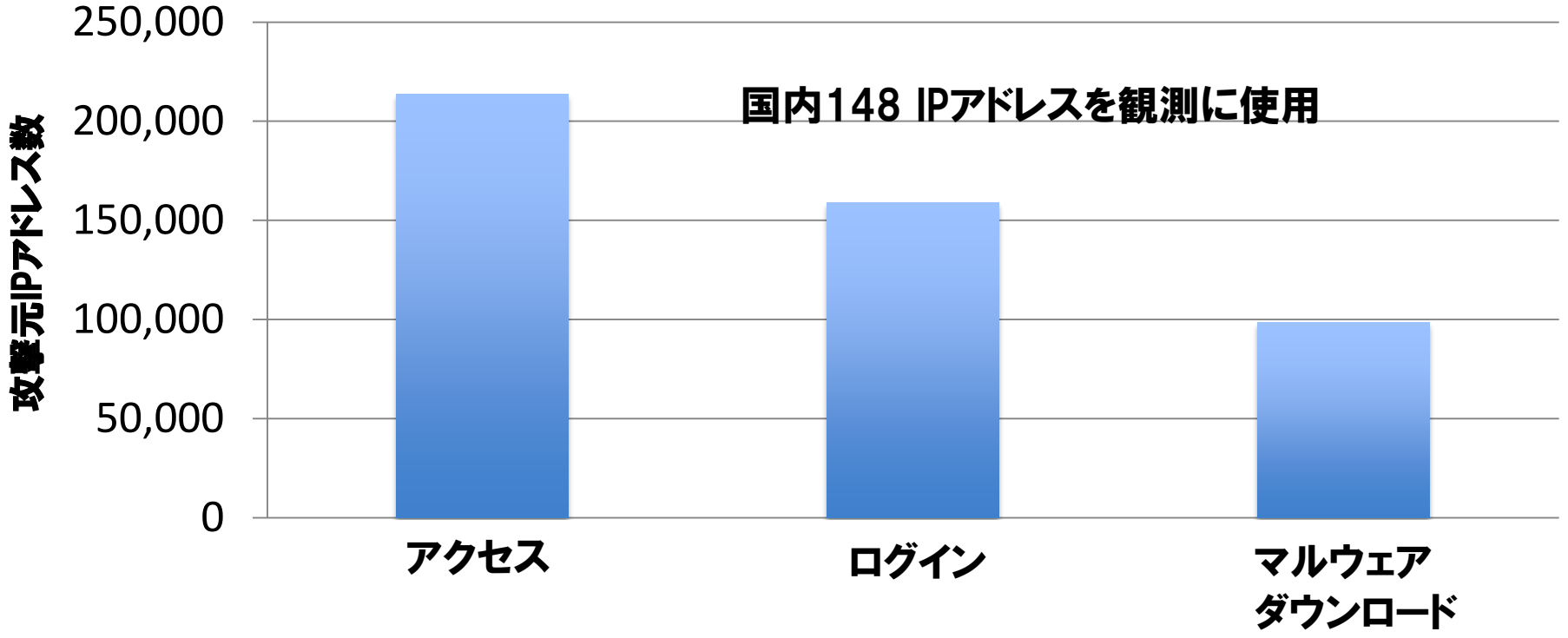
脆弱な機器を模擬した囮システム（ハニーポット）により攻撃元と通信を行い、攻撃の観測・マルウェア捕獲し、詳細解析を行う

ハニーポットの構成


Scanning Back
Profiler
YNU YOKOHAMA National University
Sensor 1
Proxy
log
Learnt Command Interactions
Device Profiles
Vulnerable Services
Banners
Authentication
Command Interaction
Internet
Sensor 2
Proxy
log
Gateway Proxy
Actual Device
IoTBOX
Sensor 3
Proxy
log
Proxy Handler
Log
Front End
Front End
Front End Responder
Multiple CPU Architectures
Unknown Commands
13か国・地域に設置
Malware Downloader
Access Manager

観測結果(2015)

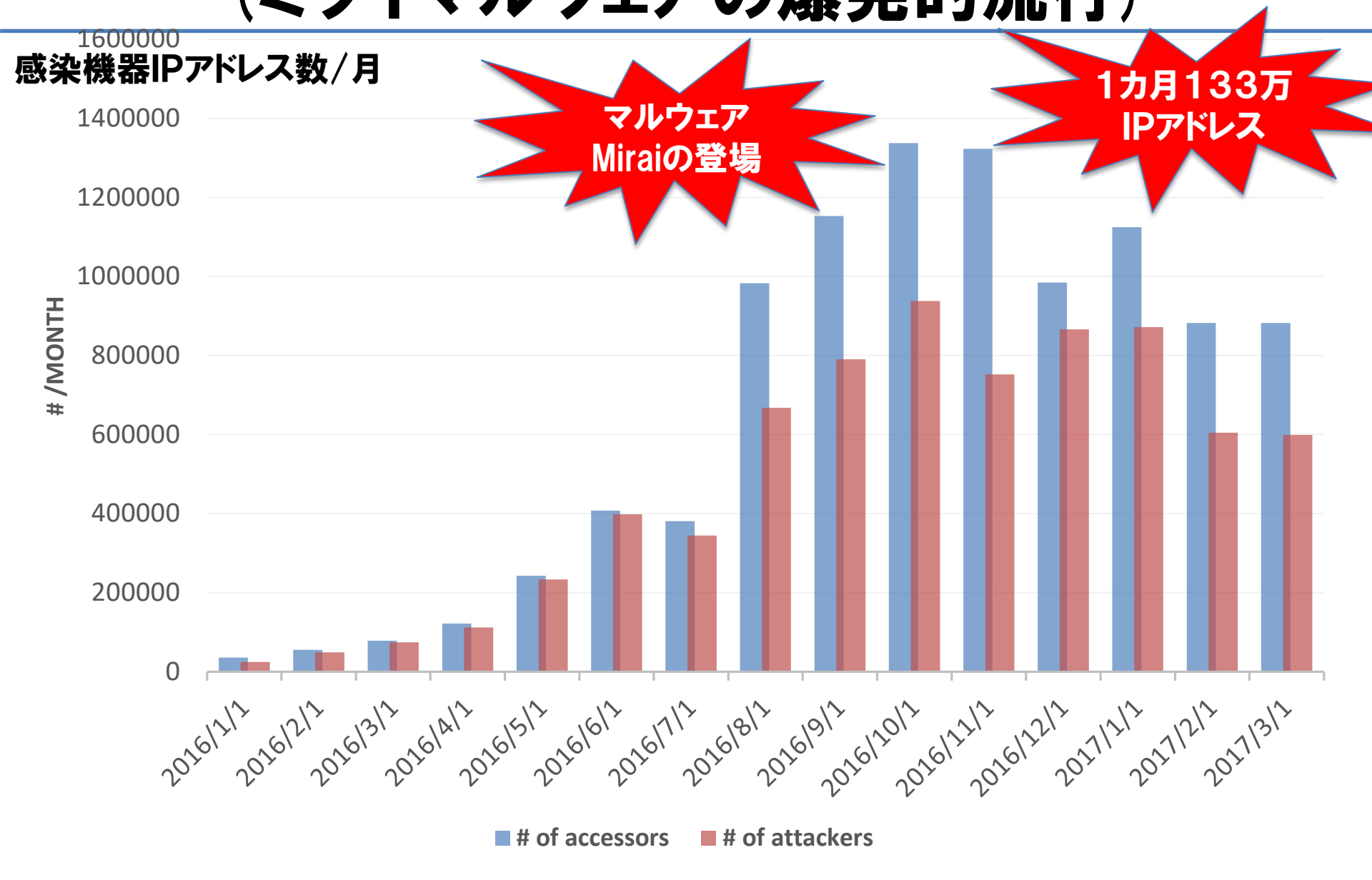
観測期間:2015/4/1～2015/7/31(122日)



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

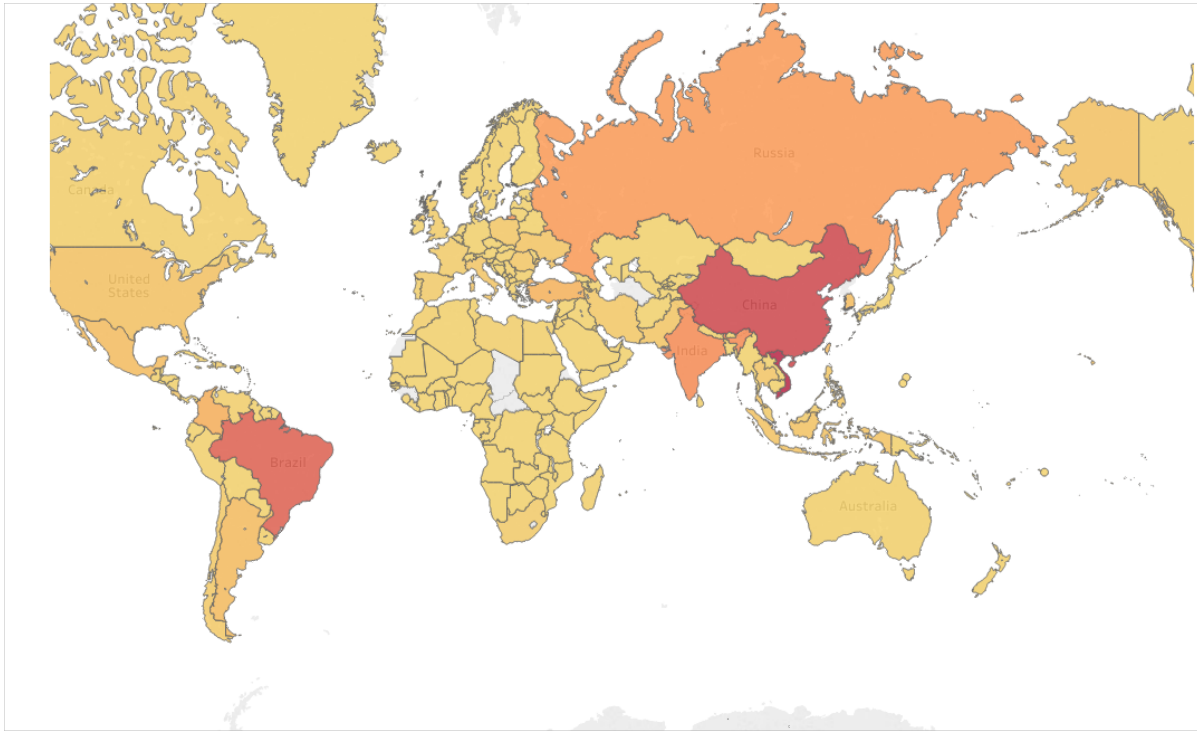
2016後半に攻撃が急増
(ミライマルウェアの爆発的流行)



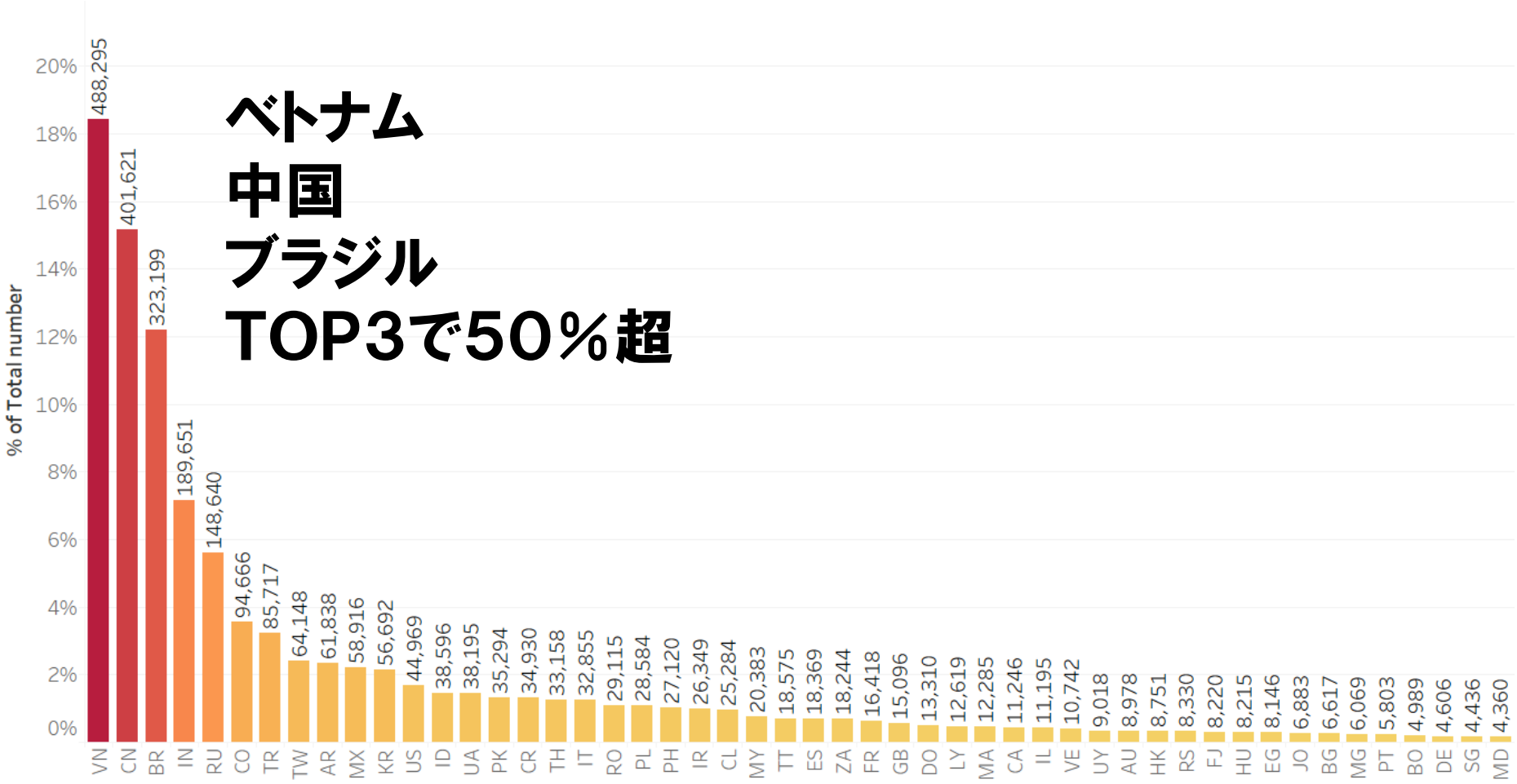
世界的に広がる感染

- **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

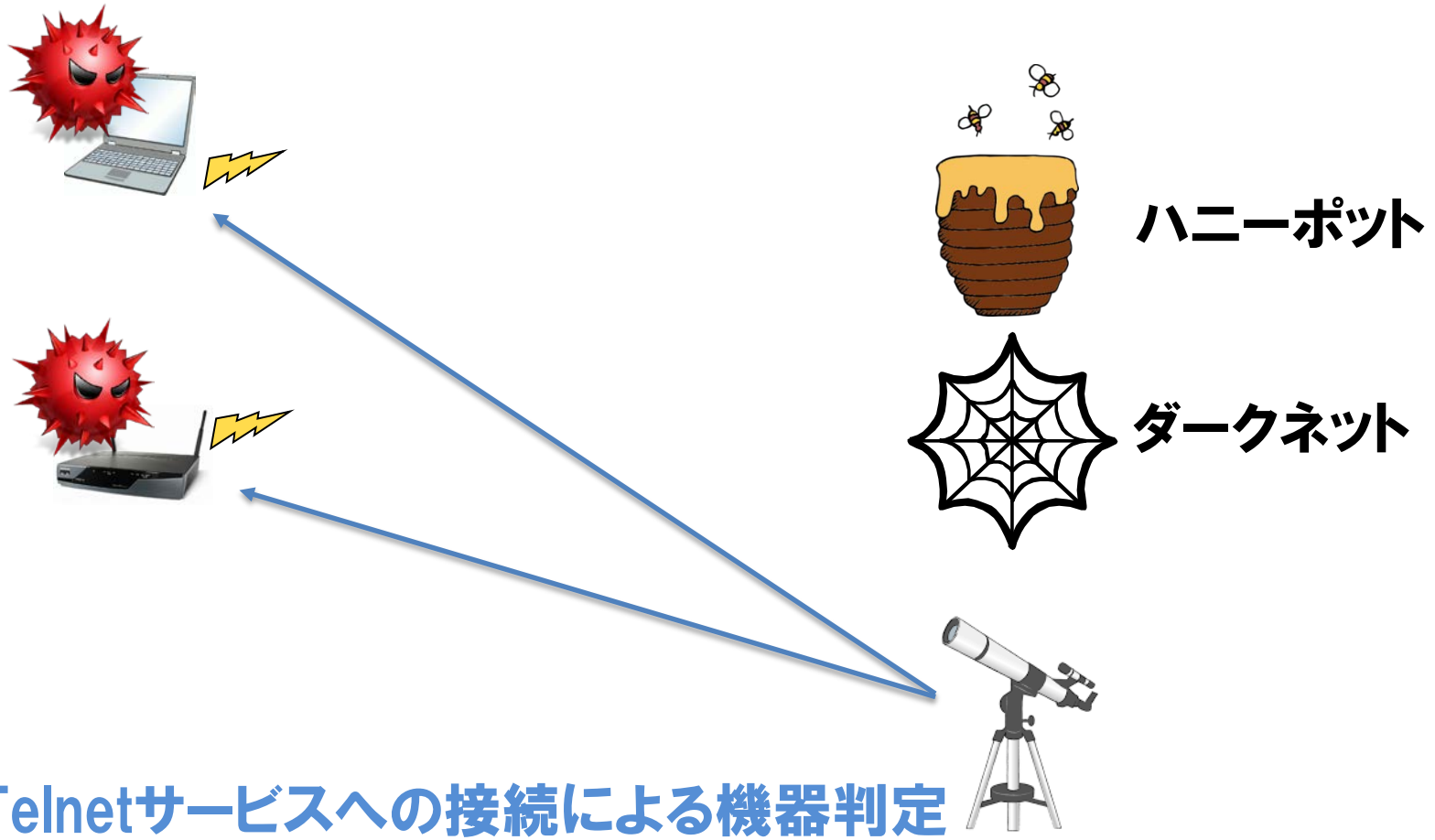


国別感染機器台数（IPアドレス）



ベトナム
中国
ブラジル
TOP3で50％超

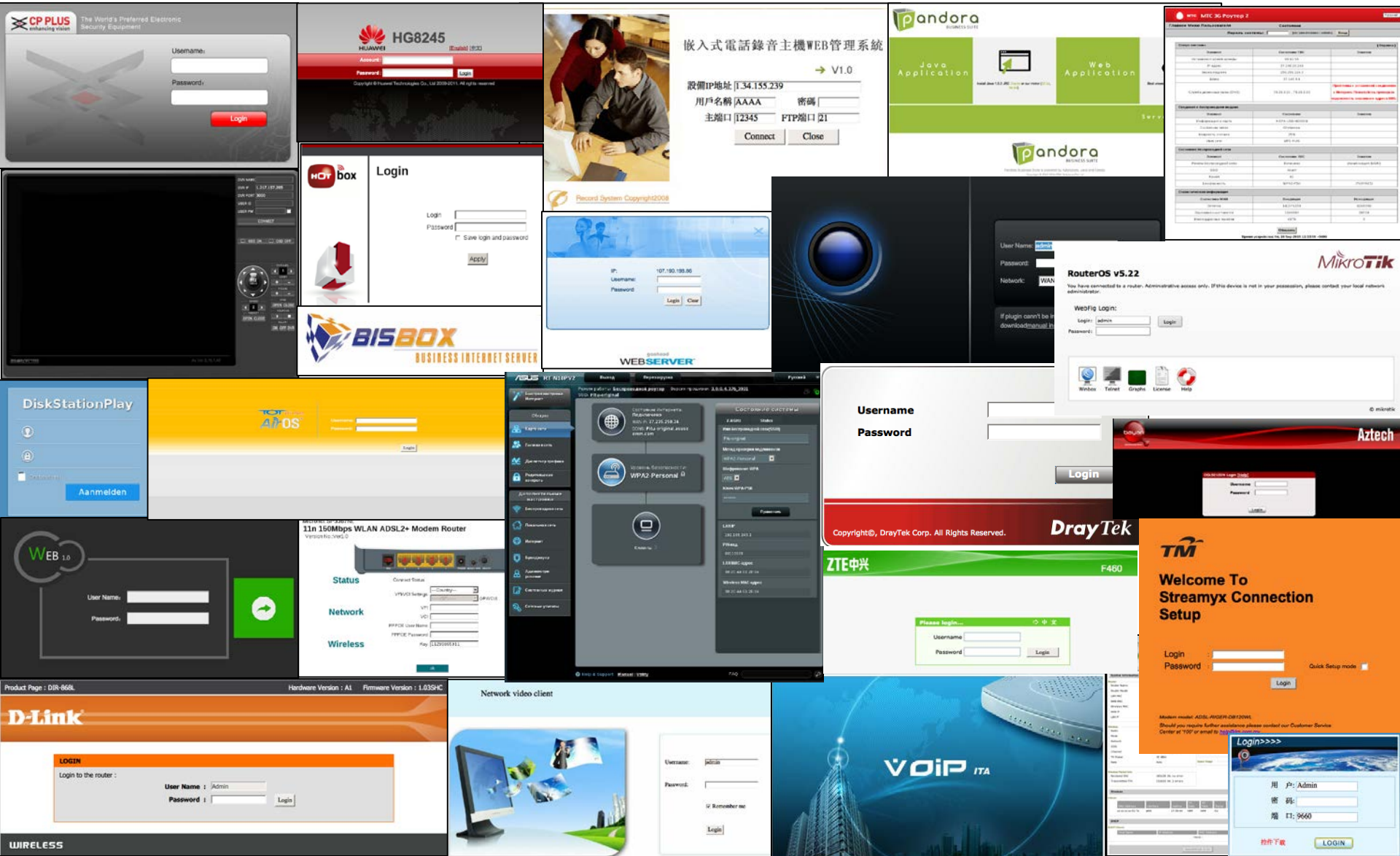
攻撃元機器の判定



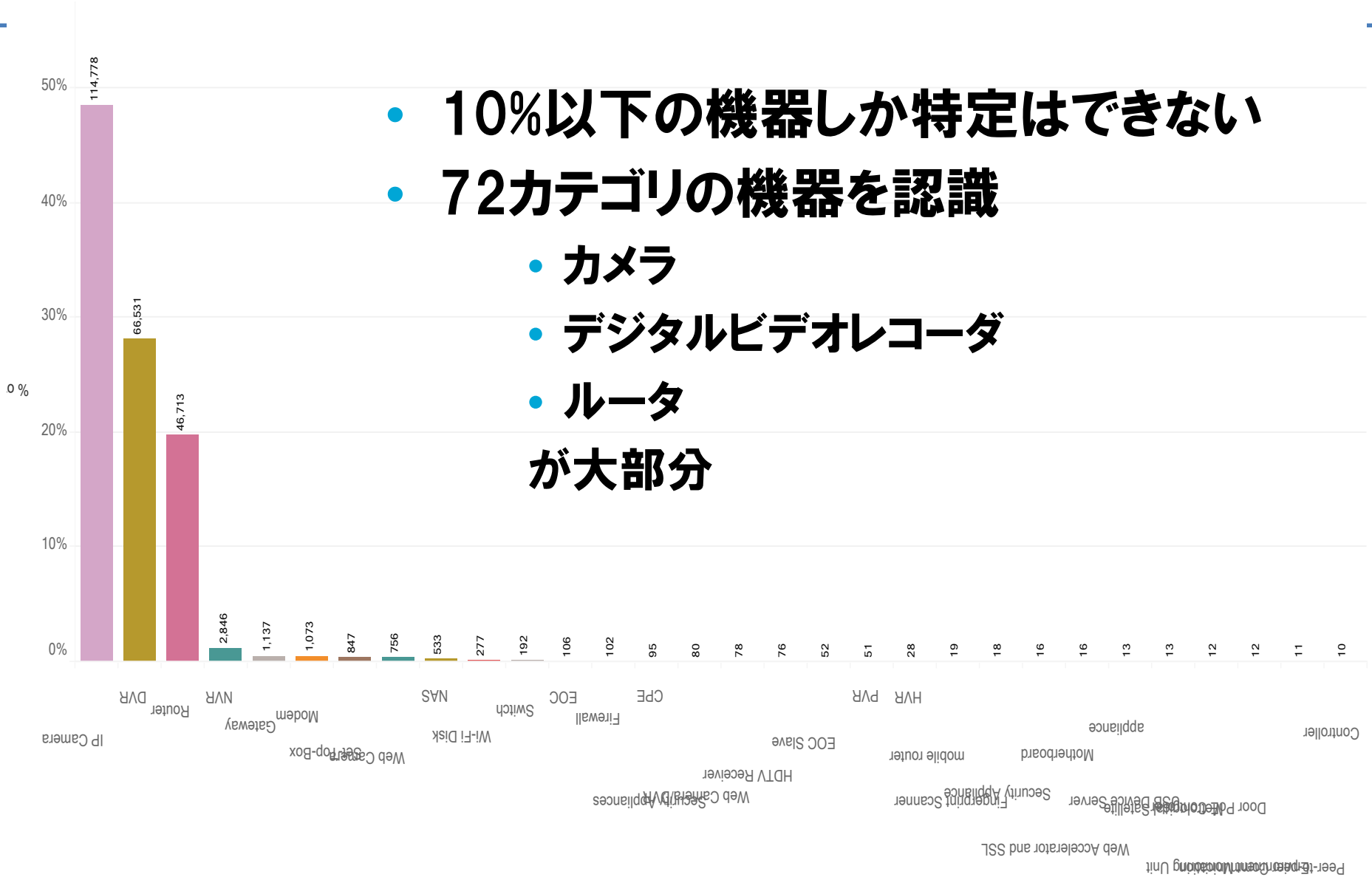
Web、Telnetサービスへの接続による機器判定

→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

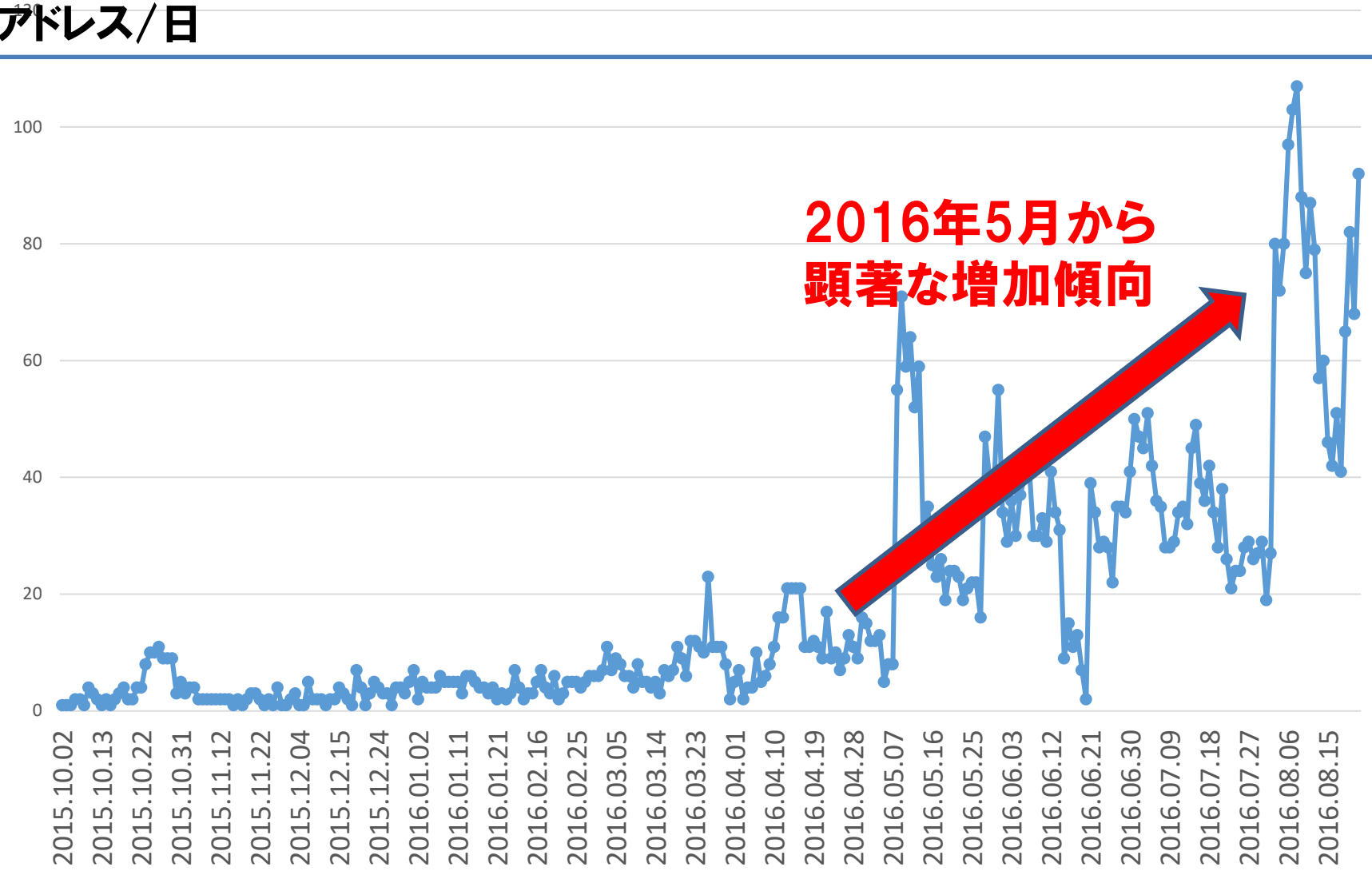


- 10%以下の機器しか特定はできない
- 72カテゴリの機器を認識
  - カメラ
  - デジタルビデオレコーダ
  - ルータ

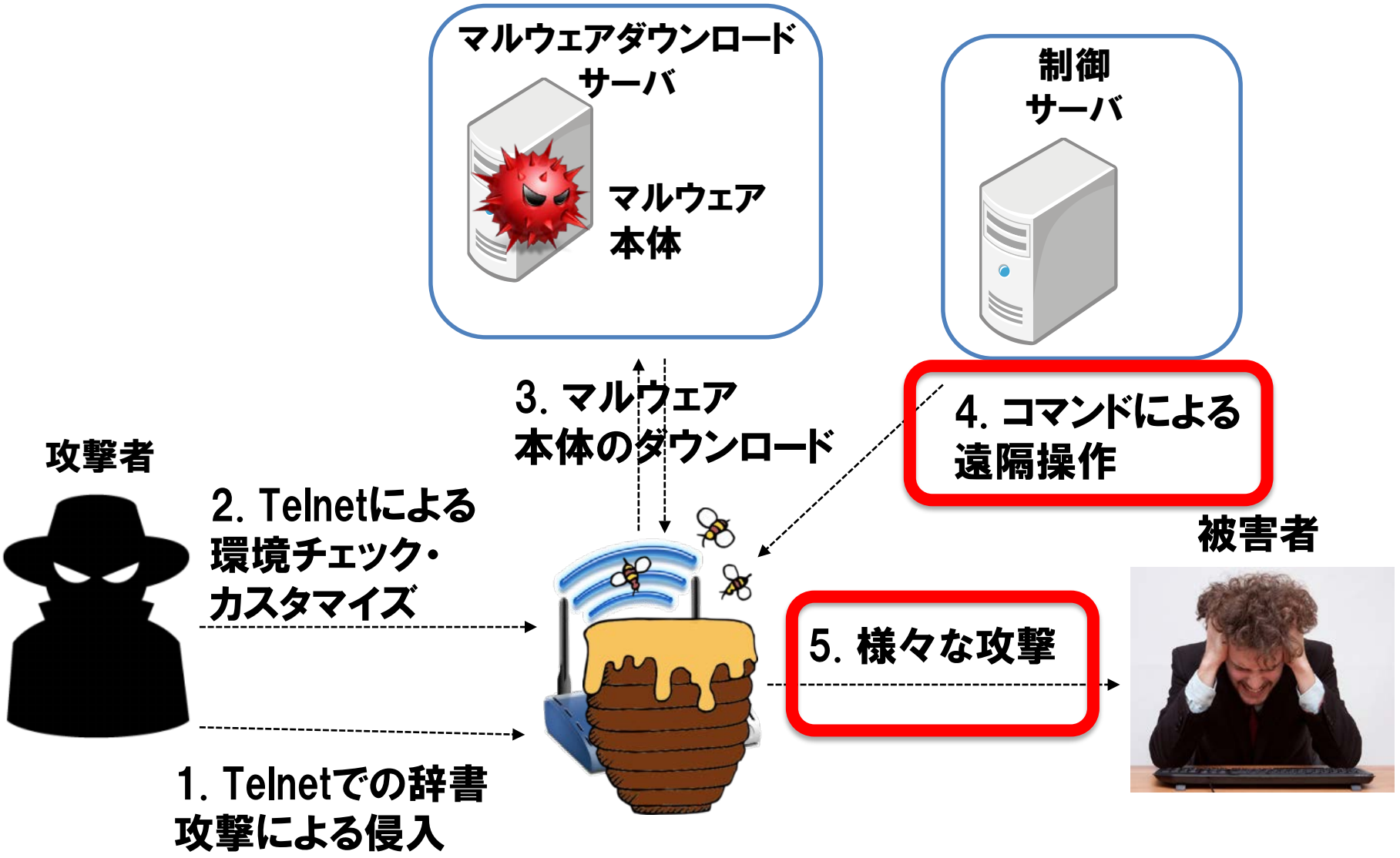
  が大部分

日本国内 感染機器台数（日ごとにカウント）

IPアドレス/日



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?

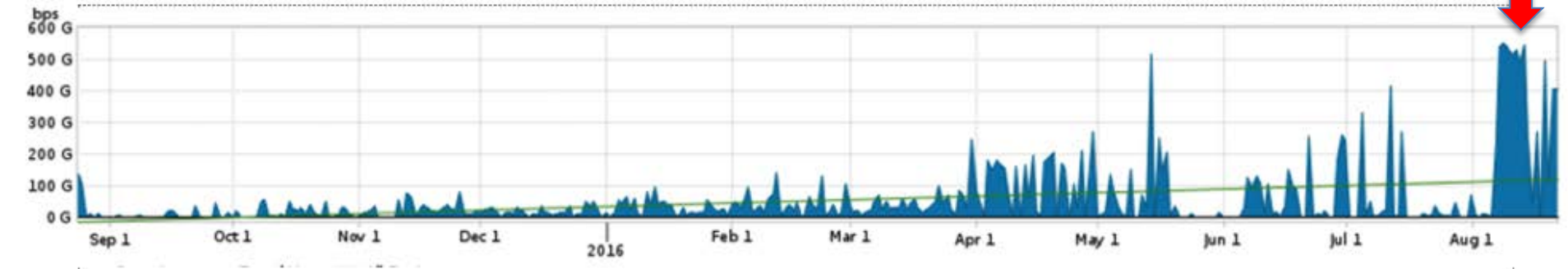
応答が遅延

“zmr666.com”の
権威DNSサーバ

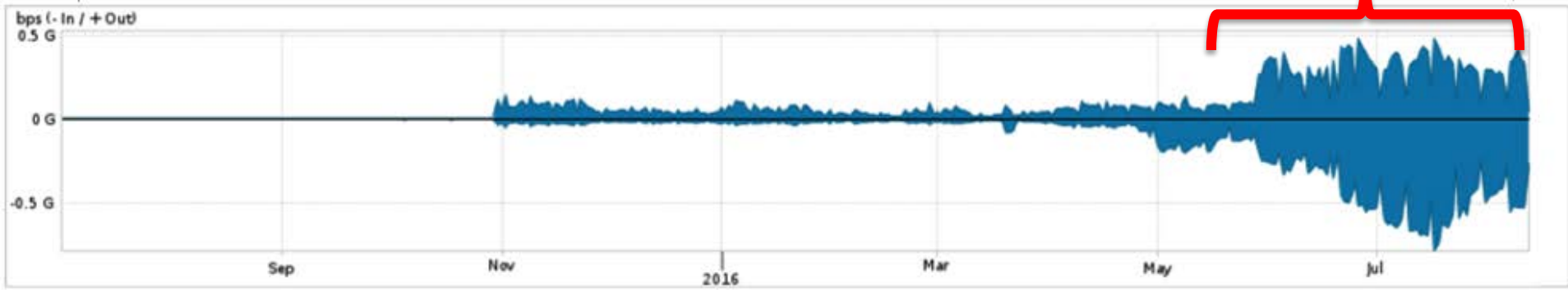
感染機器

Tokyo Olympics, what to expect

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



Telnet通信の急増（感染機器の増加＝攻撃準備）

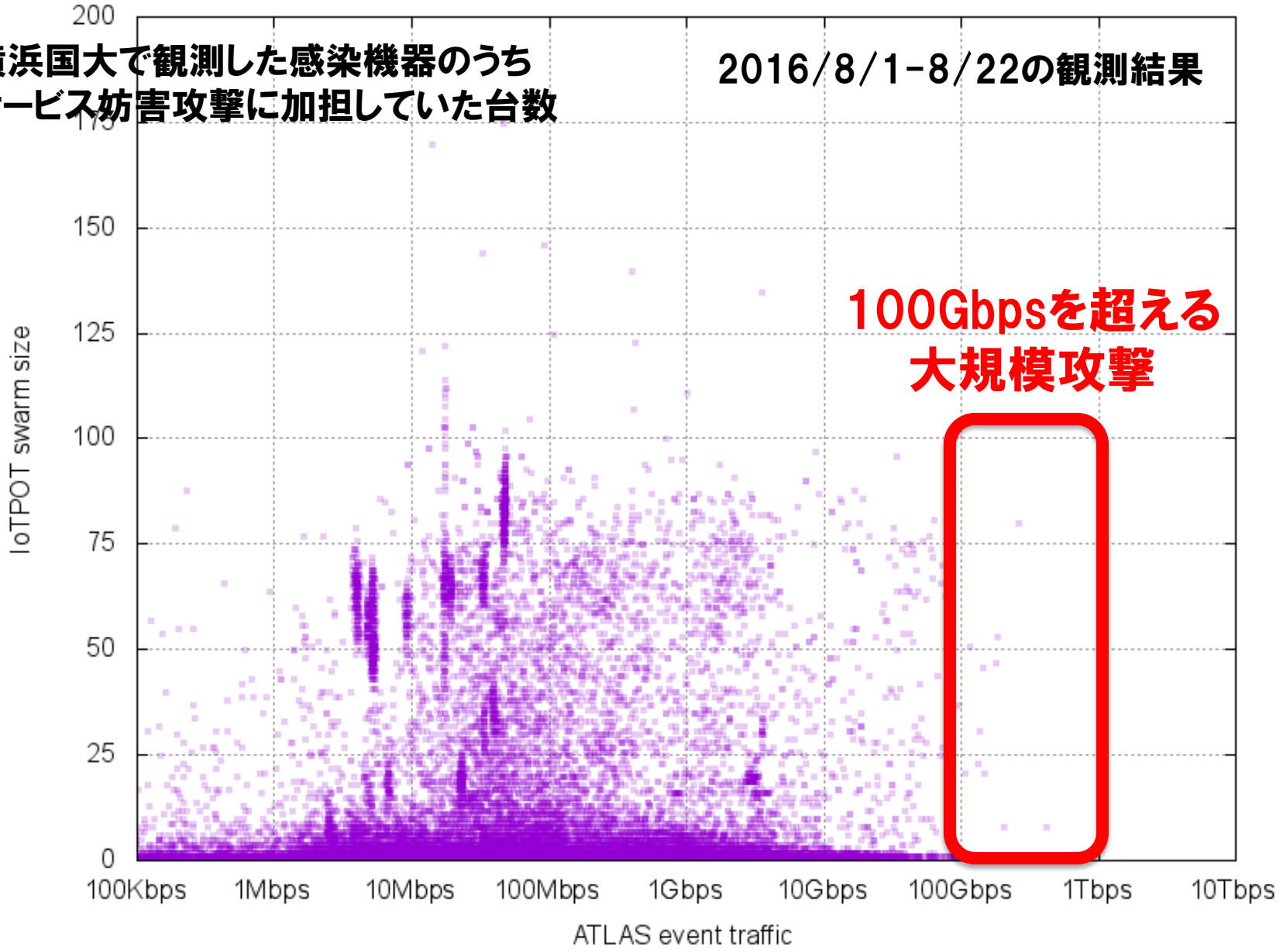


本データは米国Arbor Networks社から提供を受けたものです

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。

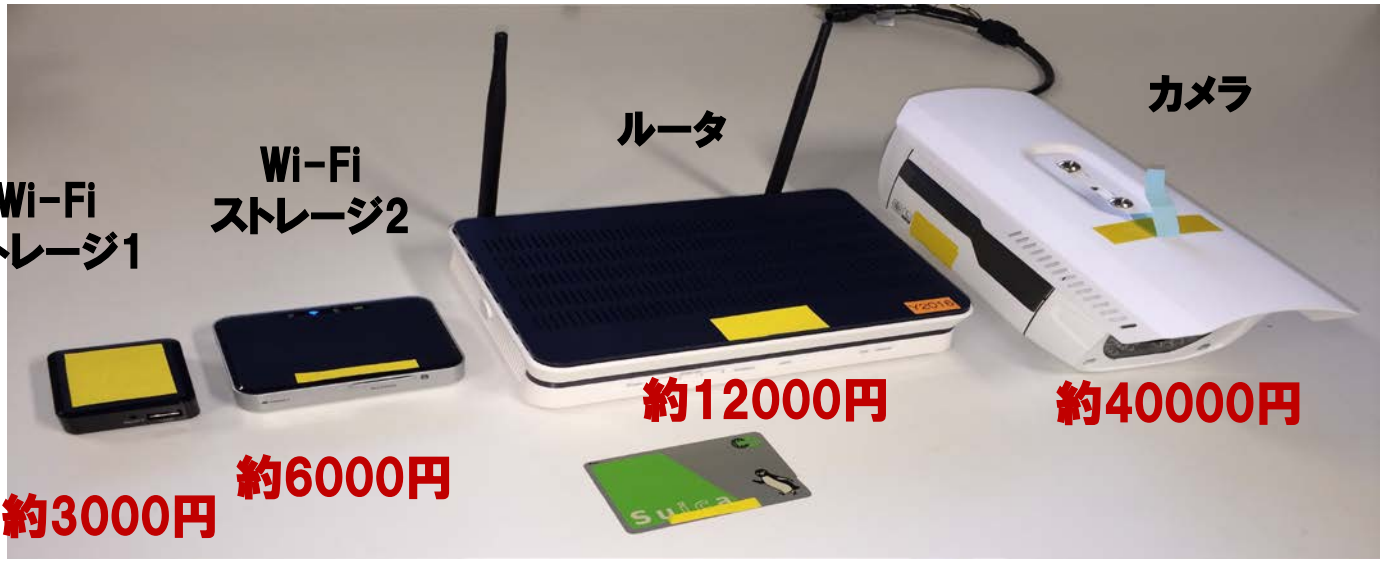
攻撃はどこまで大きくなるのか？

理論的上限値を試算

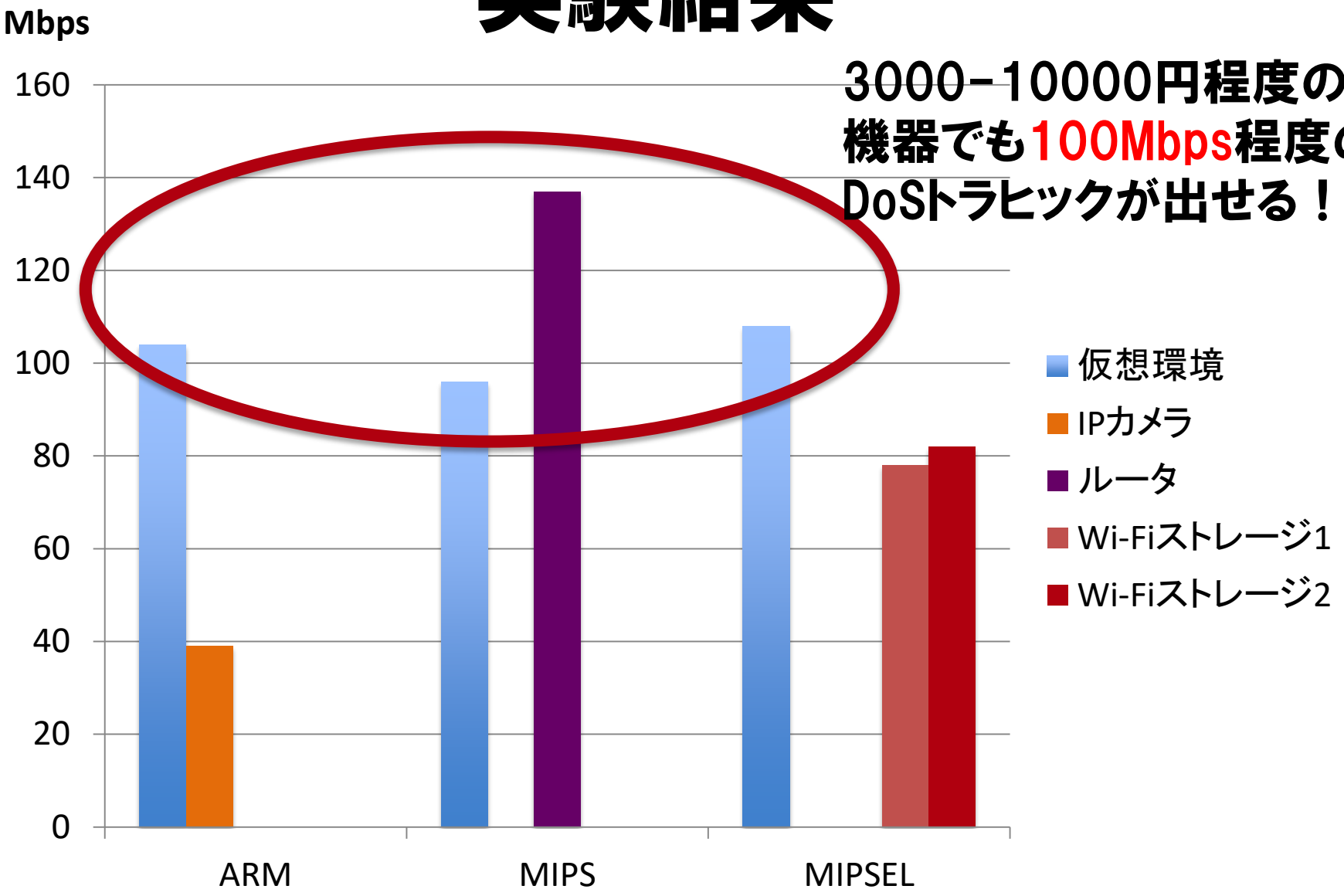
- １台あたり、どのくらいの出力が出る？
  (アップリンクの上限値も考慮)
- 攻撃者は何台くらい同時に操れる？

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



3000-10000円程度の機器でも100Mbps程度のDoSトラヒックが出せる！

IoTボットネットによるDoS攻撃理論値上限

1日当たりに観測されるボット台数（IPアドレス数） X 最小値（各アドレスレンジのアップリンク帯域実測値†, IoTデバイス1台当たりの出力平均値）

†M-Lab. 2016. NDT (Network Diagnostic Test). https://www.measurementlab.net/tools/ndt. (2016).

本分析結果は横浜国立大学、NICT、ドイツ・ザールラント大学、オランダ・デルフト工科大学の共同研究により得られました.

対策について

デバイス大量感染の元凶はTelnet

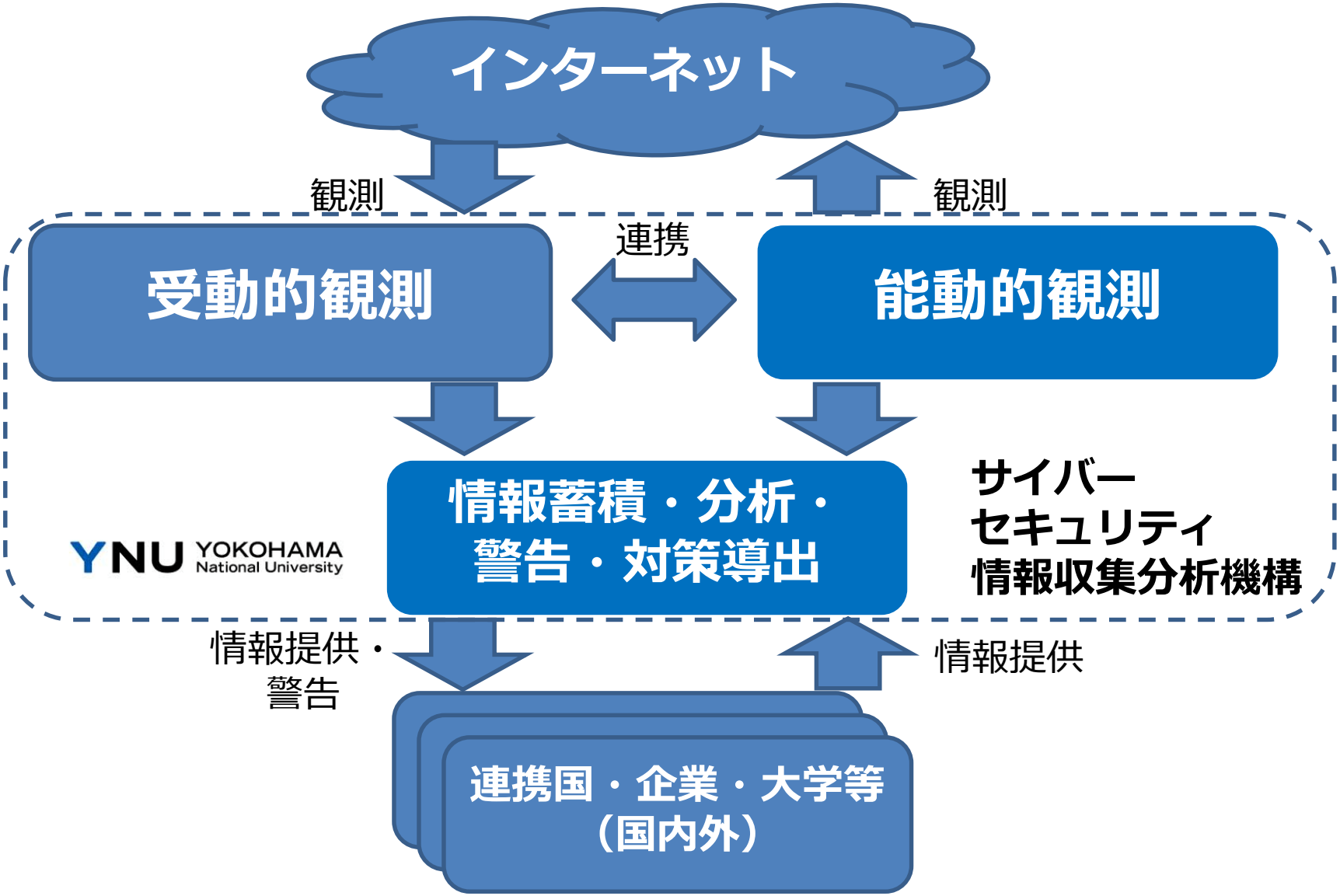
多様なはずのIoTデバイスが
Telnetという共通のセキュリティ問題を
共有してしまっている

＜現状のギャップ＞
・製造者側・利用者側は認識していない

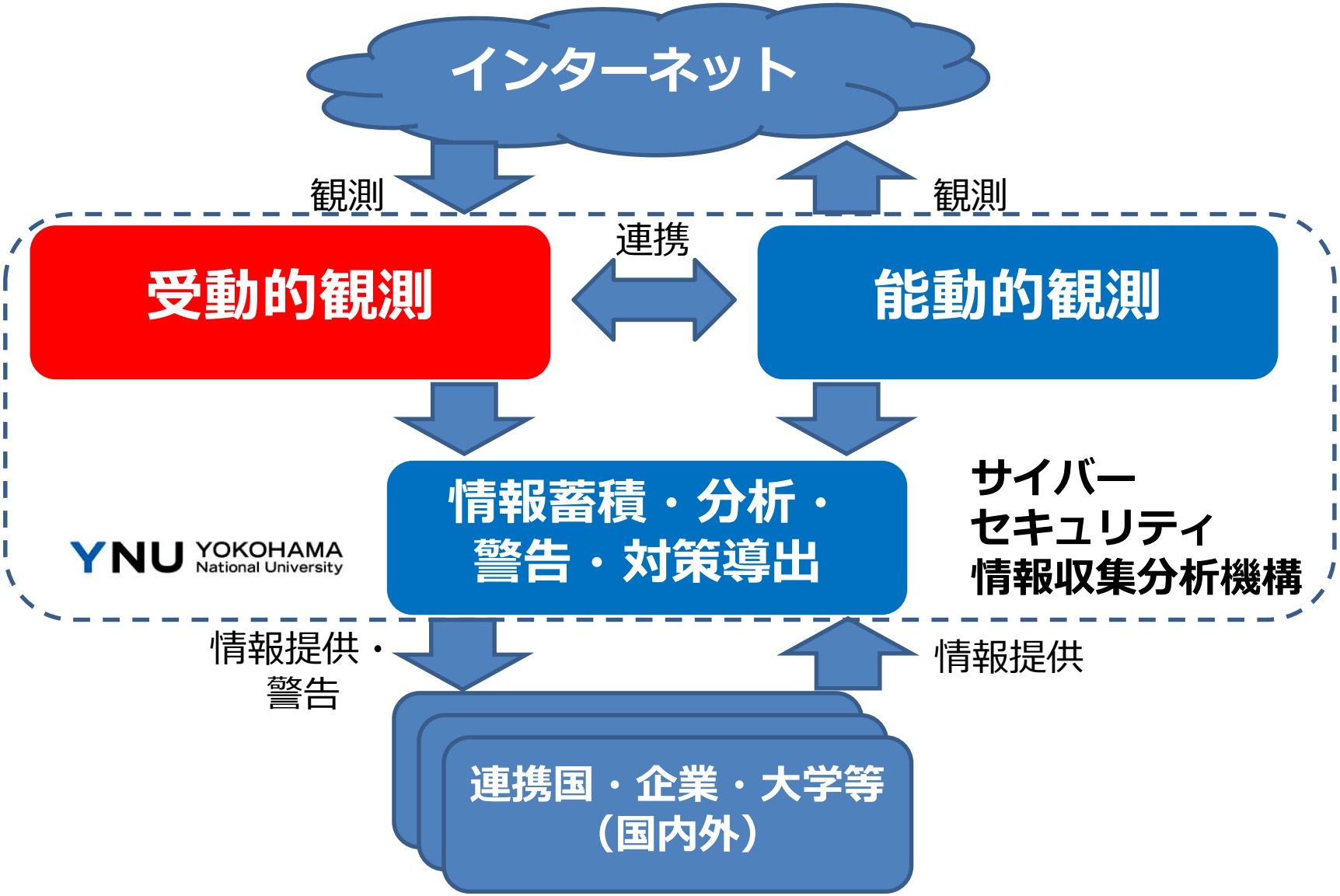
・　攻撃者側は認識している
（ネットワーク攻撃の5割以上がTelnet）

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

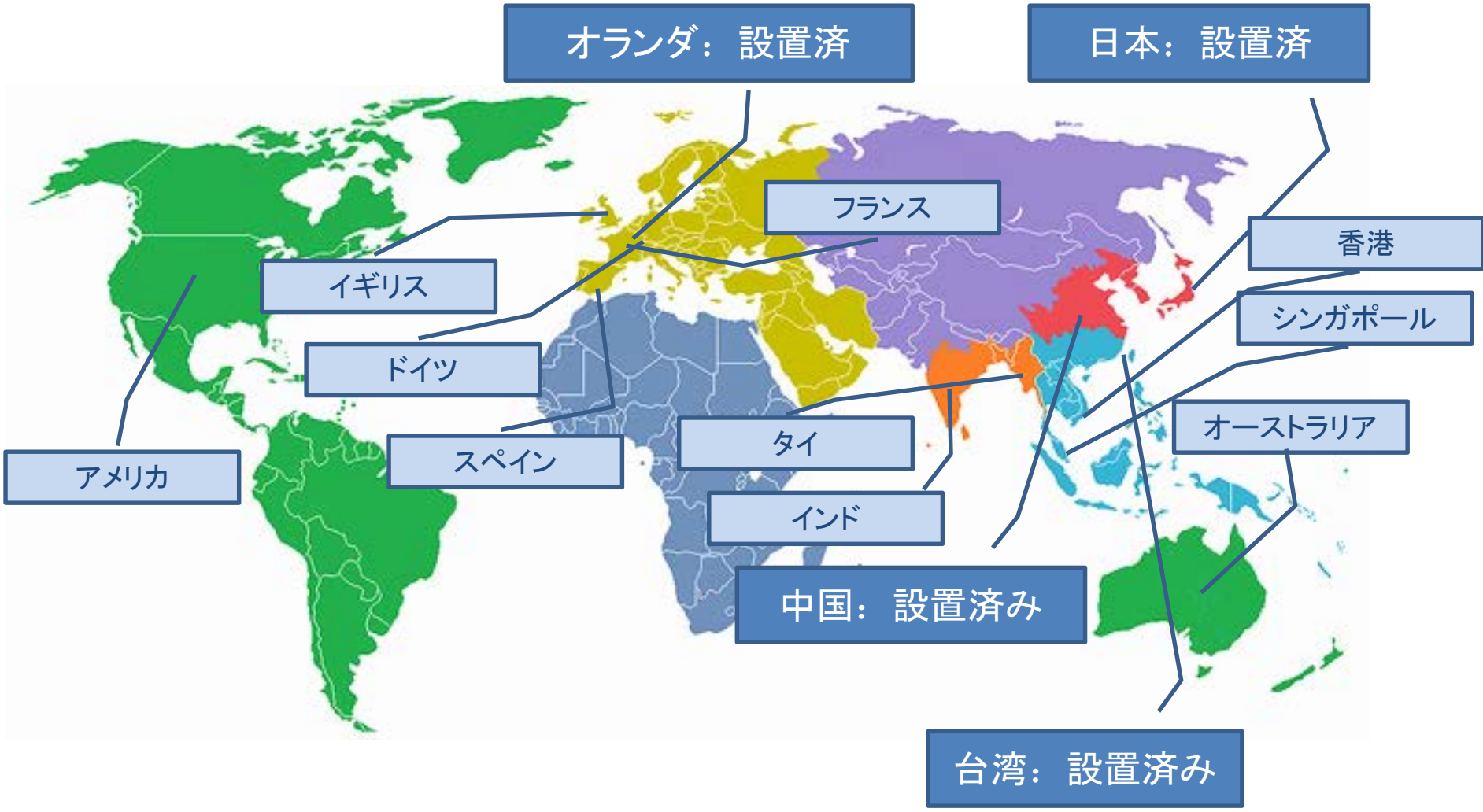
能動的観測と受動的観測を融合させた サイバーセキュリティ情報収集分析機構



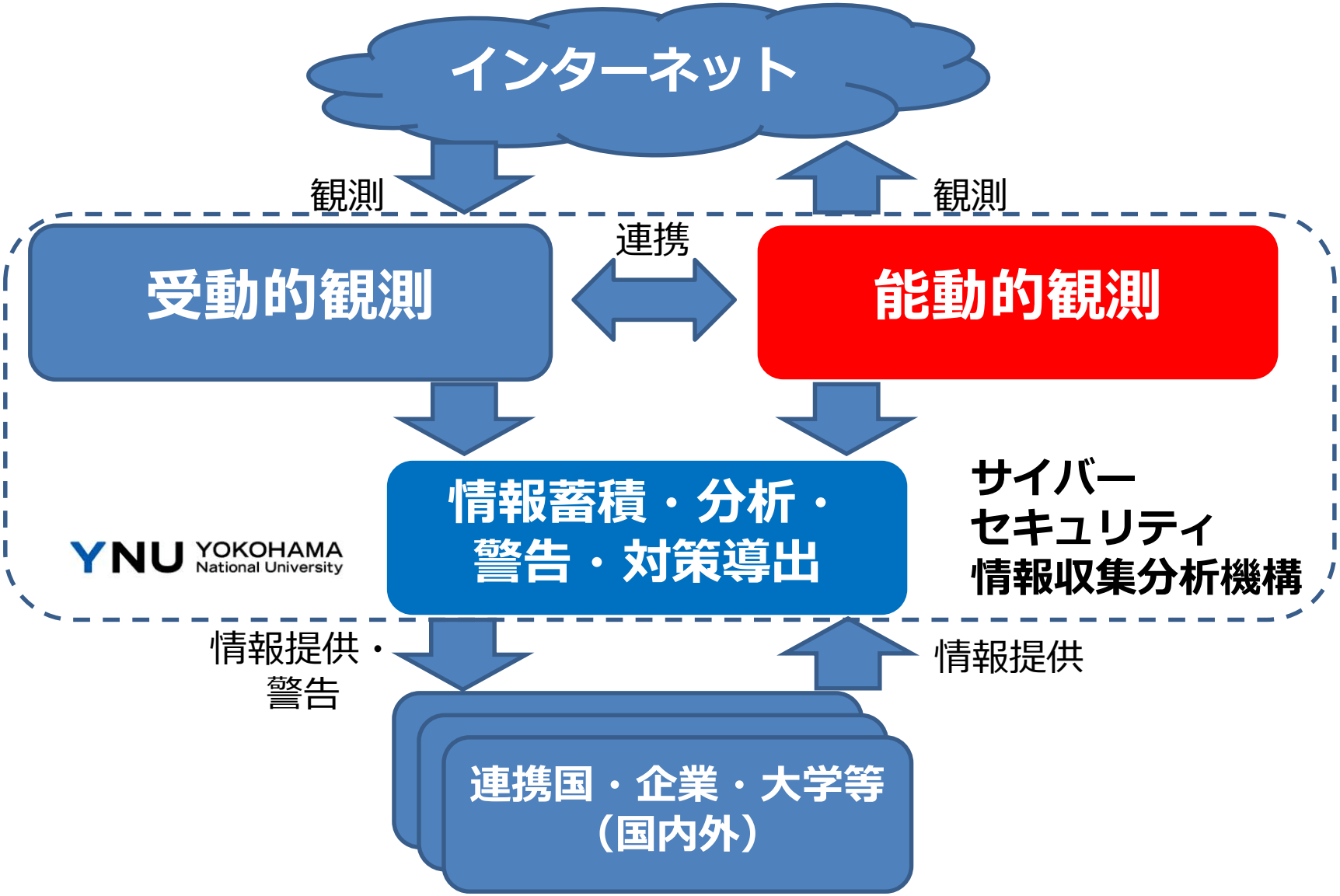
能動的観測と受動的観測を融合させた サイバーセキュリティ情報収集分析機構



観測地点（国）の拡大


オランダ：設置済
日本：設置済
フランス
香港
イギリス
シンガポール
ドイツ
オーストラリア
タイ
スペイン
アメリカ
インド
中国：設置済み
台湾：設置済み

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



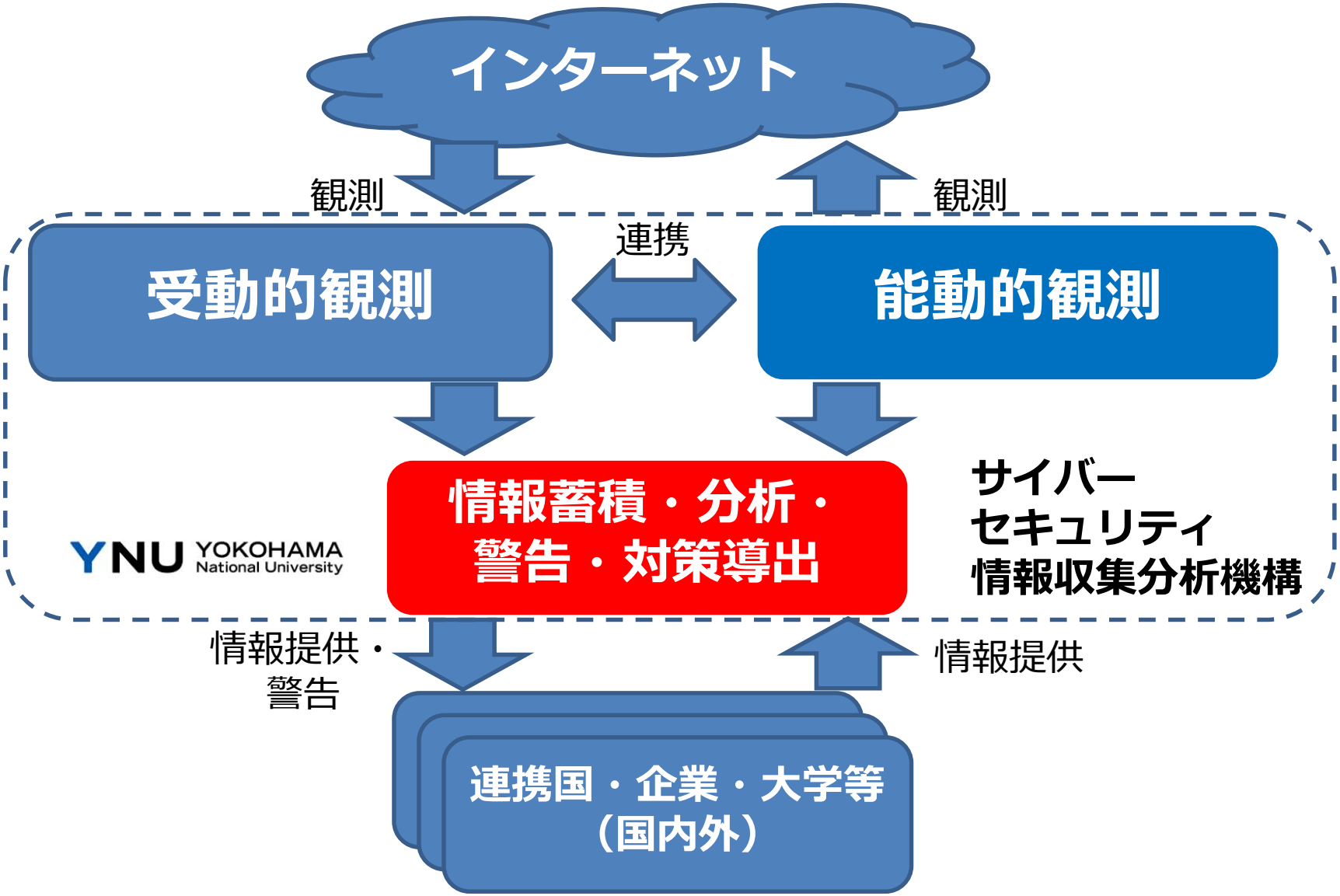
能動的観測の高度化

- 攻撃元機器・システムの種別（メーカ、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



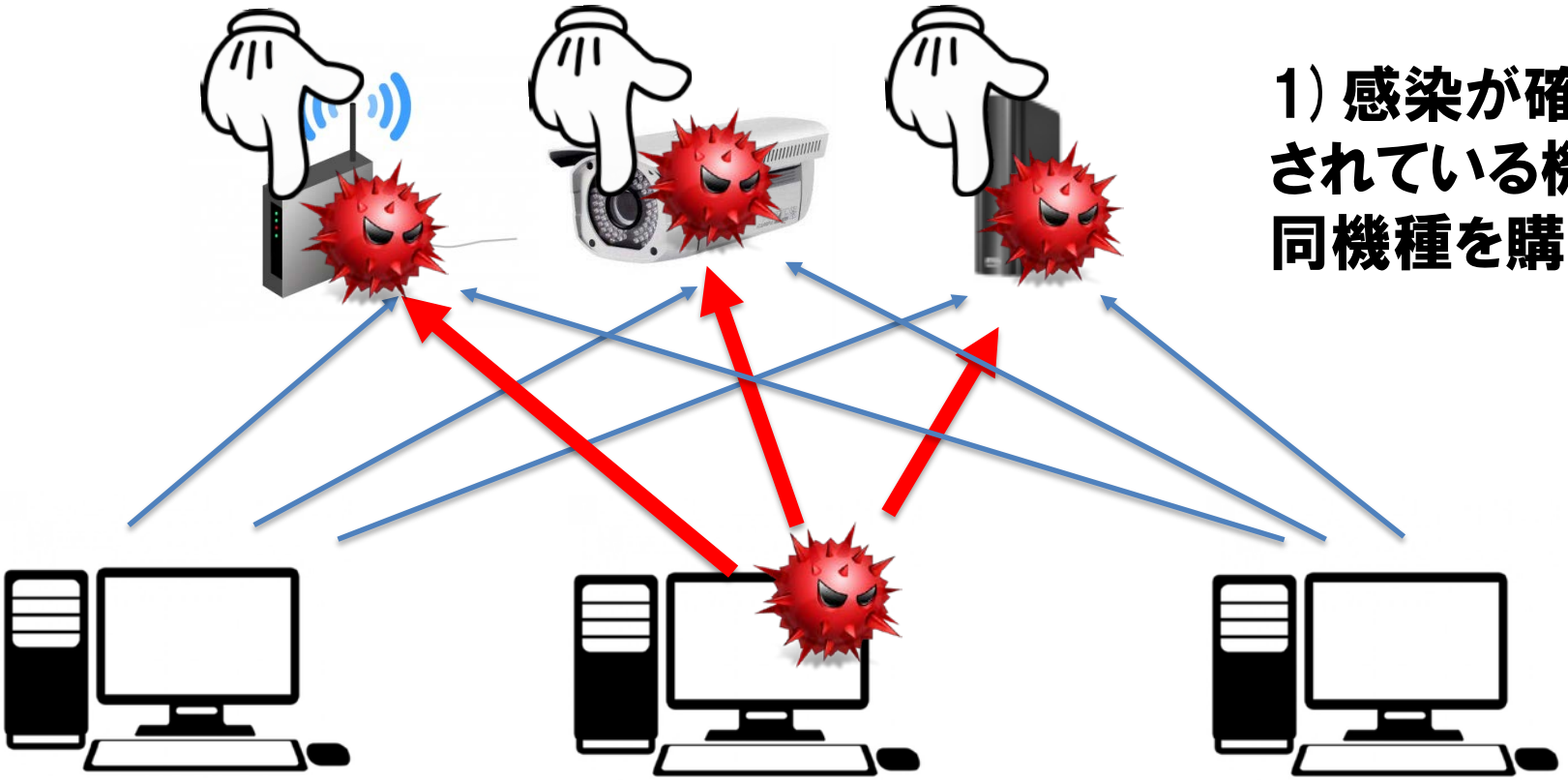
情報蓄積・分析・警告・対策導出機能の高度化

- 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
- 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

駆除実験使用機器

機器名	種類	メーカ国	Telnet ID/password	CPU アーキテクチャ
A	IPカメラ	台湾	admin/********** （管理者権限）	ARM
B	プリンター	アメリカ	itadmin/**** admin/**** user/**** （全てユーザ権限）	ARM
C	ルータ	台湾	admin/**** （管理者権限）	MIPS
D	Wi-Fiストレージ	日本	admin/**** （ユーザ権限） root/******** （管理者権限）	MIPSEL
E	Wi-Fiストレージ	日本	admin/**** （ユーザ権限） root/******** （管理者権限）	MIPSEL
F	Wi-Fiストレージ	アメリカ	admin/**** （ユーザ権限） root/******** （管理者権限）	MIPSEL
G	衛星放送受信機	ドイツ	認証なし	SH

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

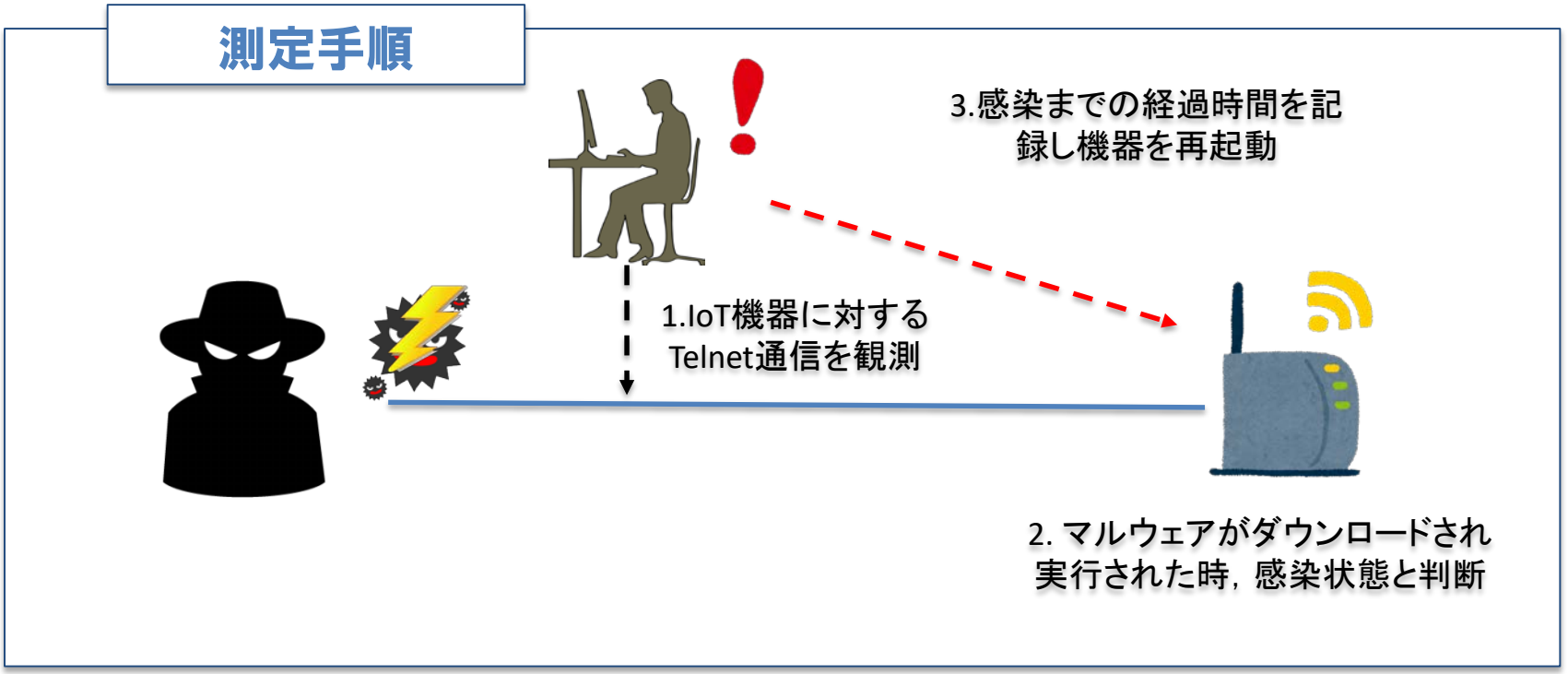
rebootコマンドが正常に動作せず

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



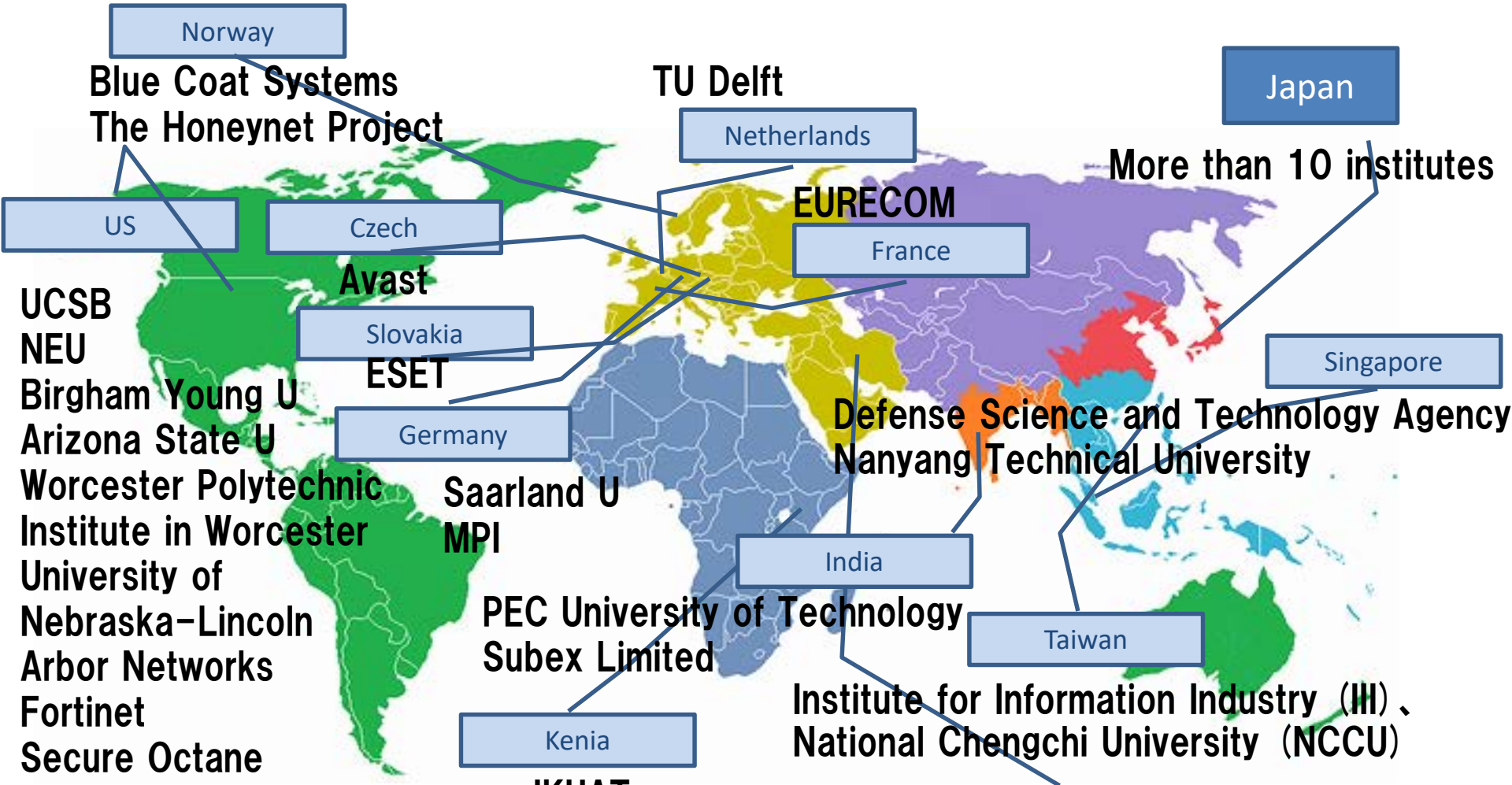
感染時間観測結果

	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

観測情報を世界50以上の研究組織セキュリティ企業に提供中



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

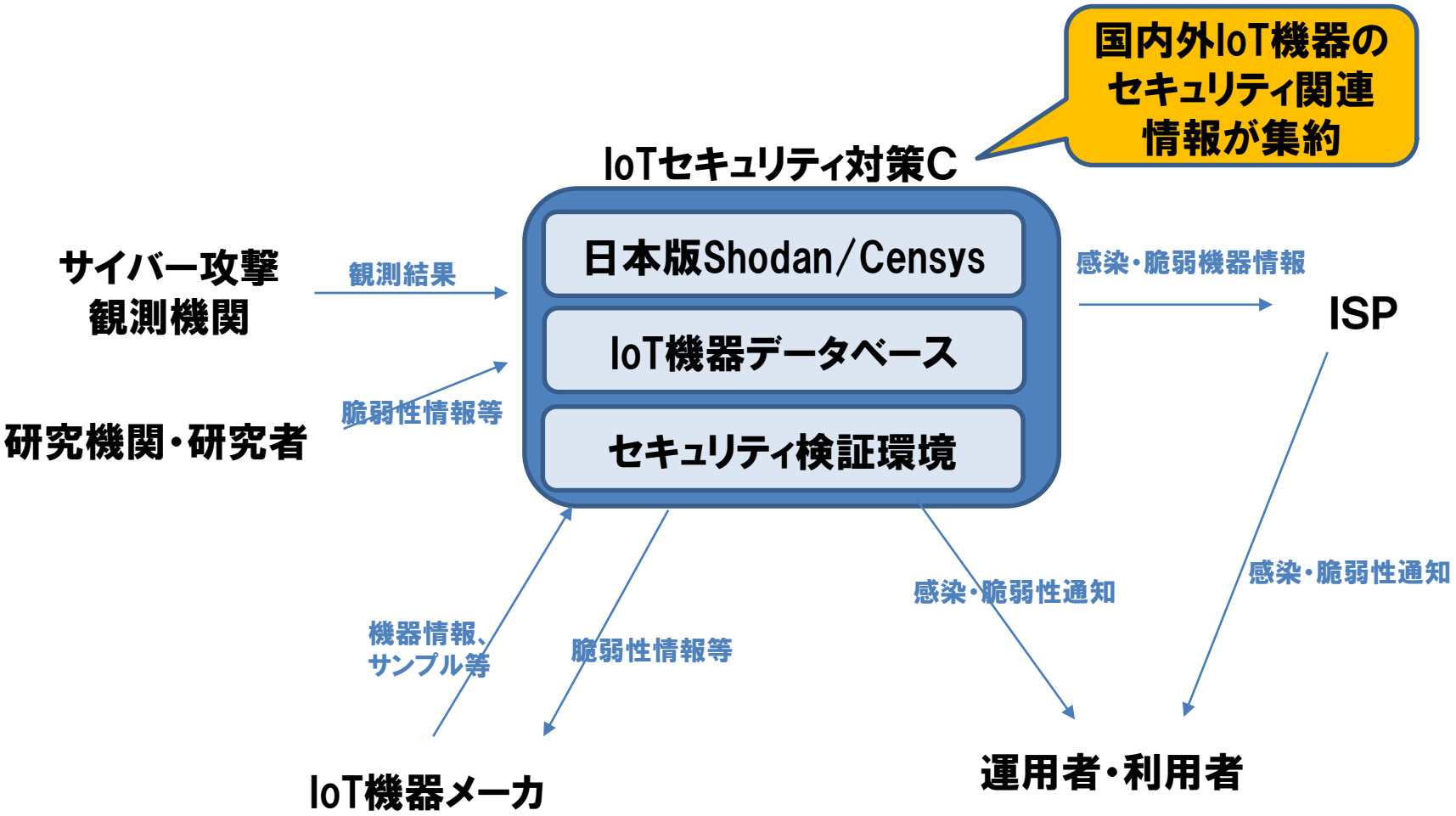
短期的対策

- 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
- 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。