データドリブンのドライバであるIoT、5G、AI に関するセキュリティ技術の動向

中尾　康二

情報通信研究機構（NICT）主管研究員

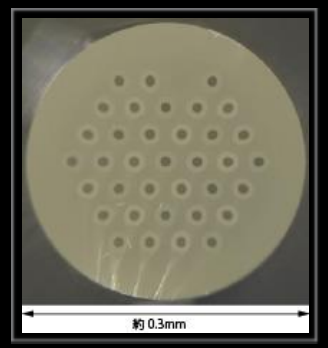
横浜国大　客員教授

内閣官房　NISC　サイバーセキュリティ参与

国立研究開発法人 情報通信研究機構とは？

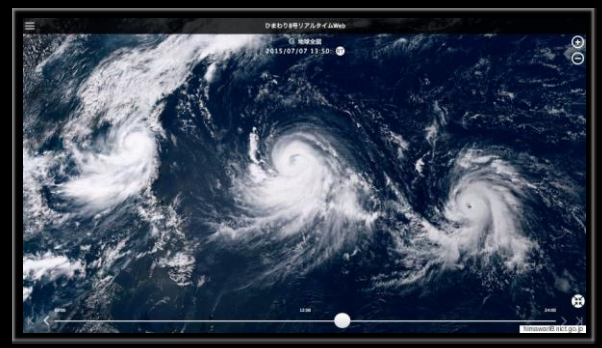
● 情報通信分野を専門とする日本で唯一の公的研究機関

日本標準時の生成・配信
（うるう秒挿入）



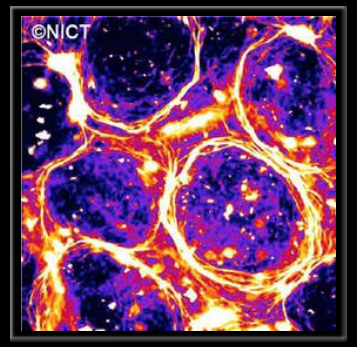
光通信システム
（ペタbps級 マルチコアファイバ）

宇宙通信システム
（超高速インターネット衛星きずな）



サイエンスクラウド
（ひまわり8号リアルタイムWeb）

電磁波センシング
（Pi-SAR2による3.11直後の仙台空港）

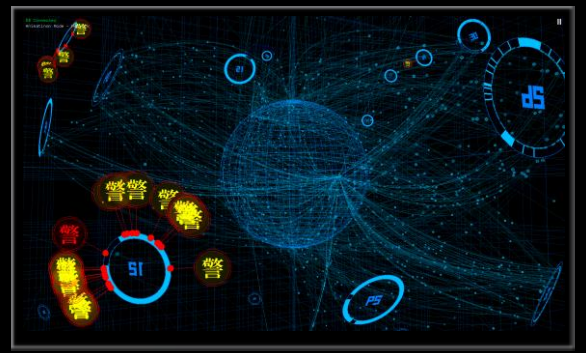


バイオ・ナノICT
（生体分子の自己組織化）

脳情報通信融合
（ブレイン・マシーン・インターフェイス）

多言語音声翻訳
（多言語音声翻訳アプリVoiceTra）

超臨場感コミュニケーション
（初音ミクさんの電子ホログラフィ）



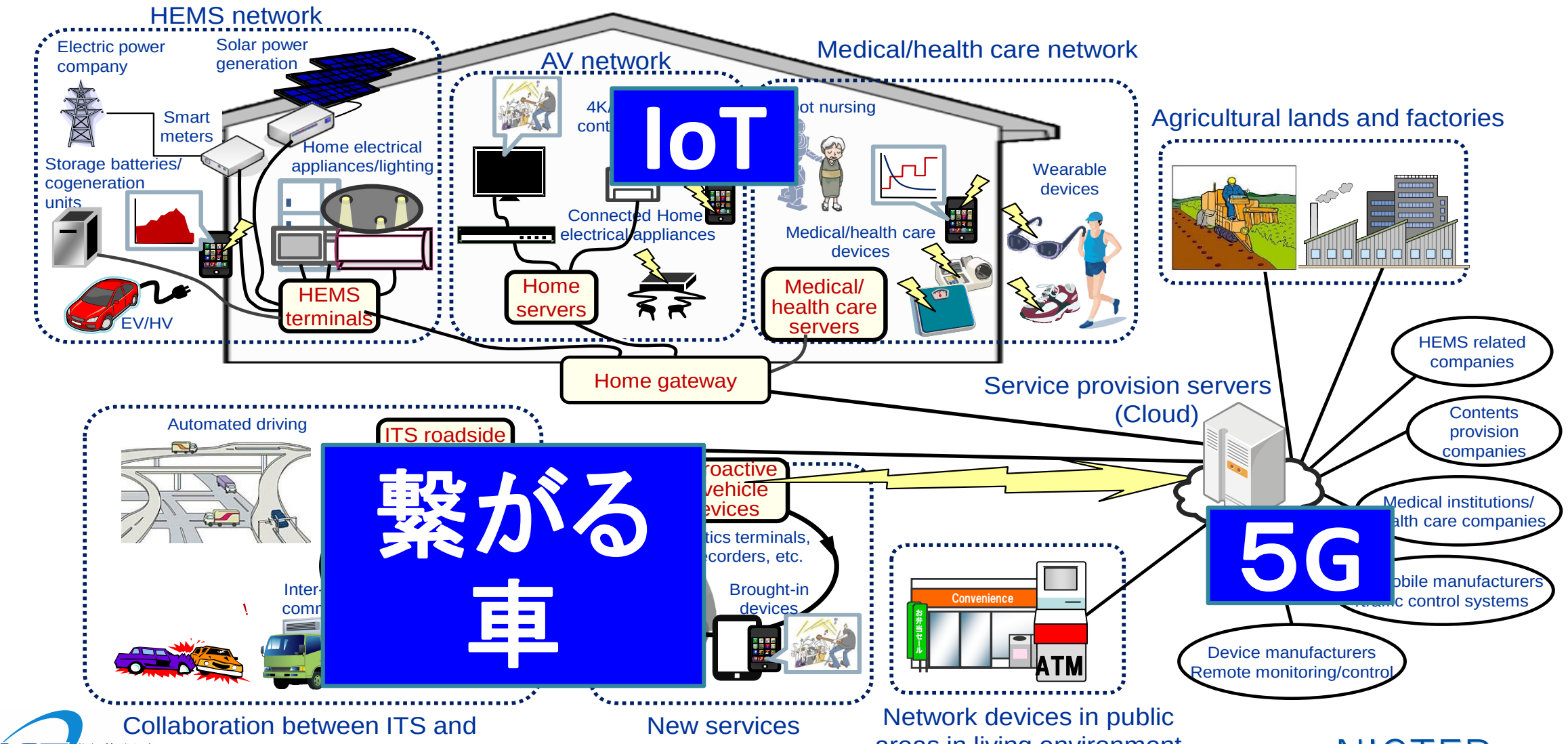
サイバーセキュリティ
（対サイバー攻撃アラートシステムDAEDALUS）

本講演では

「データドリブン（Data Driven）」とは、売上データや利用者からの収集データ、WEB解析データなど、様々なデータに基づいて判断・アクションする事。

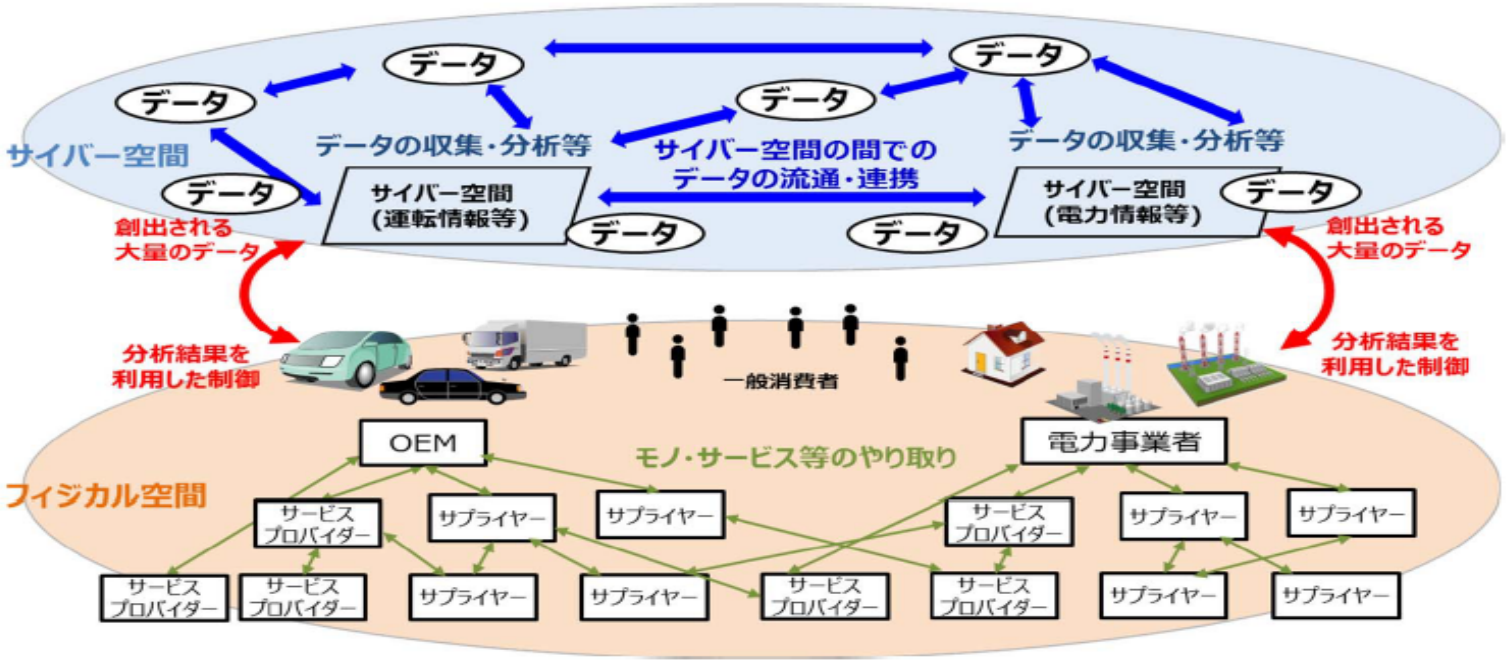
本稿では、データドリブンの世界を牽引する重要な要素である、１)IoT、２)５G、３）繋がる車　におけるセキュリティ脅威、対策について述べ、データドリブンによるデータ分析などのアクションの主役となる「AIの活用」について解説する。

IoTの世界を起点としたデータドリブンによるビジネス展開



サイバー空間とフィジカル空間が高度に融合した「Society5.0」の到来

- 我が国では、**サイバー空間とフィジカル空間を高度に融合**させることにより、多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立する超スマート社会「**Society5.0**」の実現を提唱。
- **「Society5.0」では、付加価値を創造するための一連の活動（サプライチェーン） の形態が、より柔軟で動的なものに変化。**この**新たな形のサプライチェーンを価値創造過程（バリュークリエイションプロセス）**と定義。
- 一方で、**サイバー空間とフィジカル空間の融合により、サイバー攻撃の脅威が増大。**



Society5.0の社会におけるモノ・データ等のつながりのイメージ

大量のデータの流通・連携
⇒データの性質に応じた管理の重要性が増大

フィジカル空間とサイバー空間の融合
⇒フィジカル空間までサイバー攻撃が到達

複雑につながるサプライチェーン
⇒影響範囲が拡大

見えている最近のセキュリティ上の脅威は？

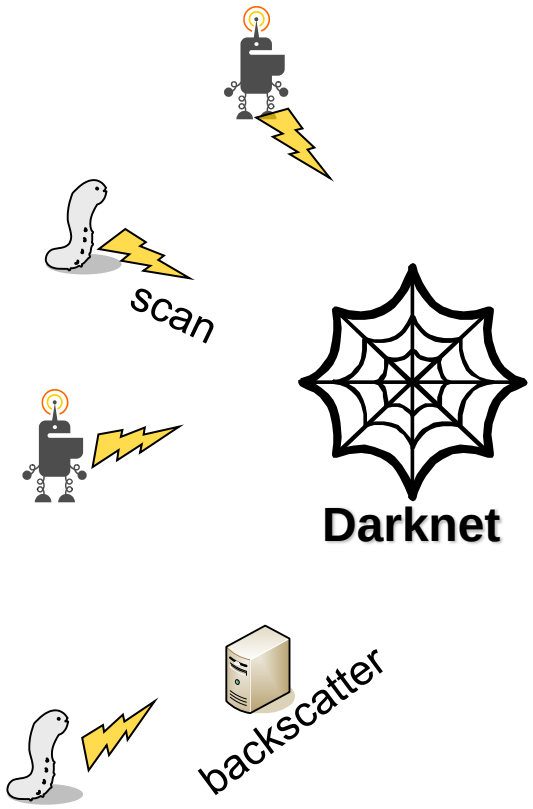
ダークネットで何が見えているのか？

●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

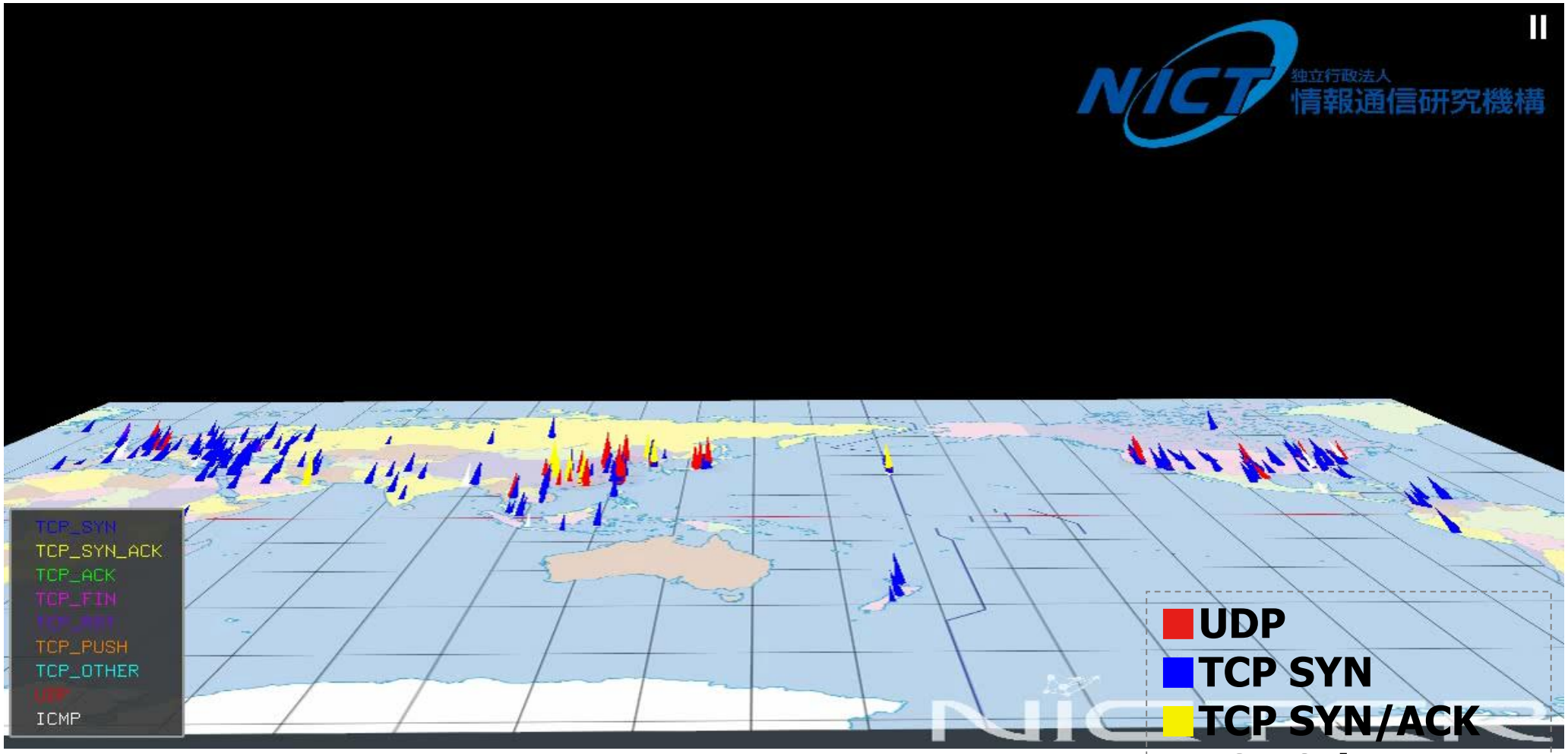
●DDoS攻撃の跳ね返り
- ✓ 送信元IPアドレス偽装されたSYN Flood
- ✓ 被攻撃サーバからの応答（SYN-ACK）
- ✓ DDoS攻撃の早期検知（1パケット目から）

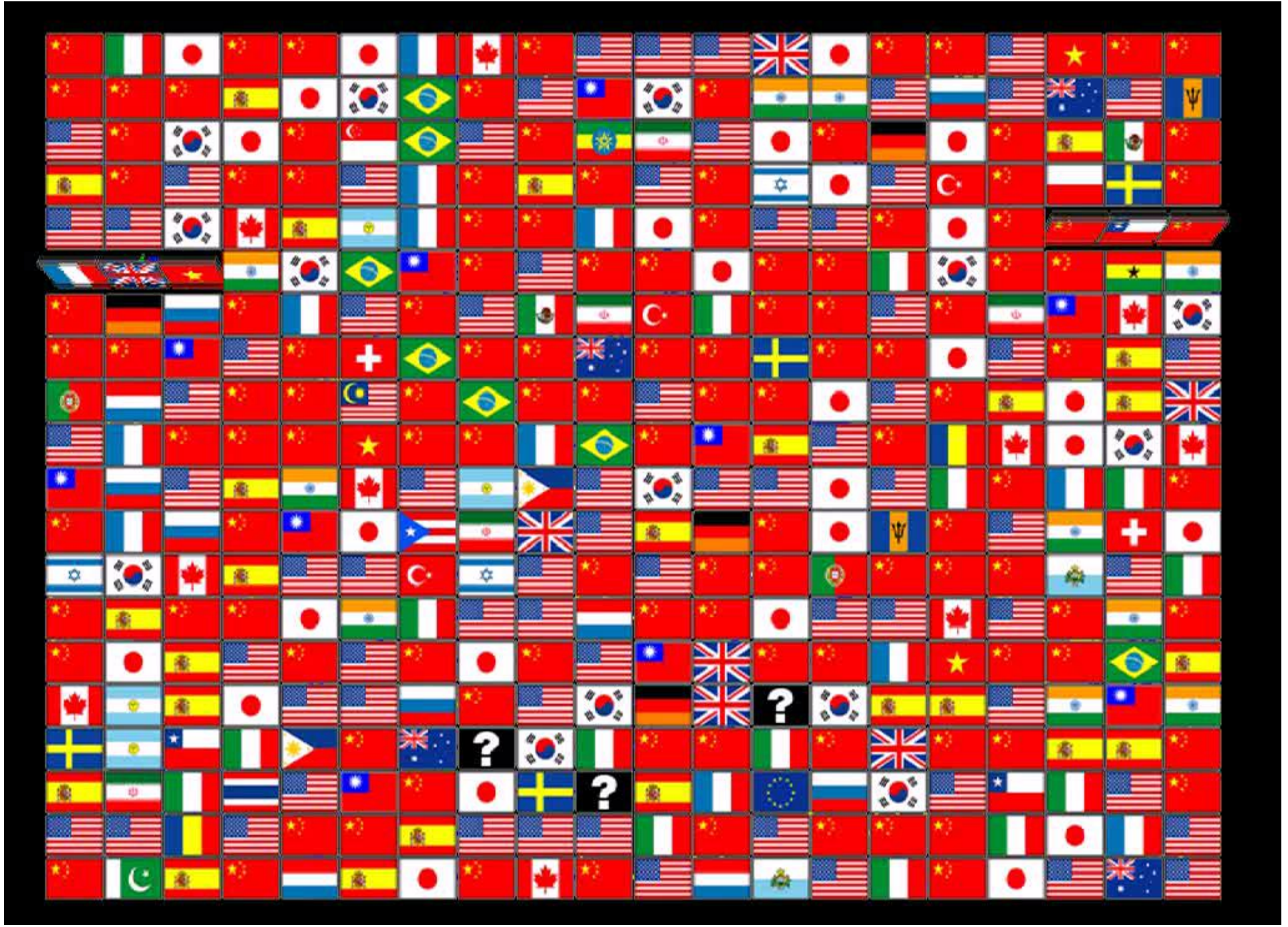
●リフレクション攻撃の準備活動
- ✓ DNS Open Resolver探索
- ✓ NTP探索　　etc.

●設定ミス
- ✓ 組織内ダークネット



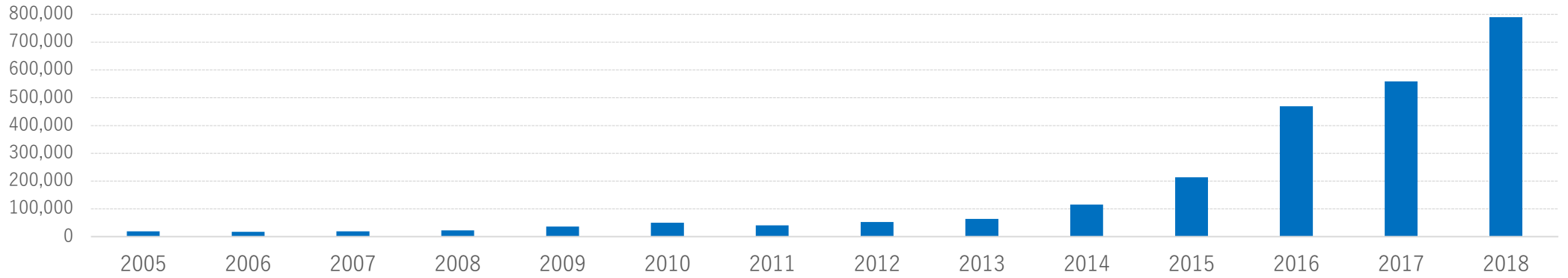
nicter-Atlas（ダークネット観測システム）による全スキャン





NICTER観測統計（2005-2018）

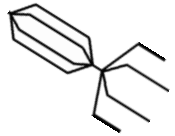
年	年間総観測パケット数	観測IPアドレス数	１IPアドレス当たりの年間総観測パケット数
2005	約 3.1億	約1.6万	19,066
2006	約 8.1億	約10万	17,231
2007	約19.9億	約10万	19,118
2008	約22.9億	約12万	22,710
2009	約35.7億	約12万	36,190
2010	約56.5億	約12万	50,128
2011	約45.4億	約12万	40,654
2012	約77.8億	約19万	53,085
2013	約128.8億	約21万	63,655
2014	約256.6億	約24万	115,323
2015	約545.1億	約28万	213,523
2016	約1,281億	約30万	469,104
2017	約1,504億	約30万	559,125
2018	**約2,121億**	約30万	**789,876**



１IPアドレスあたりの年間総観測パケット数

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

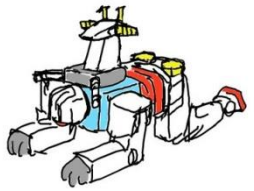


ウイルス

- **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

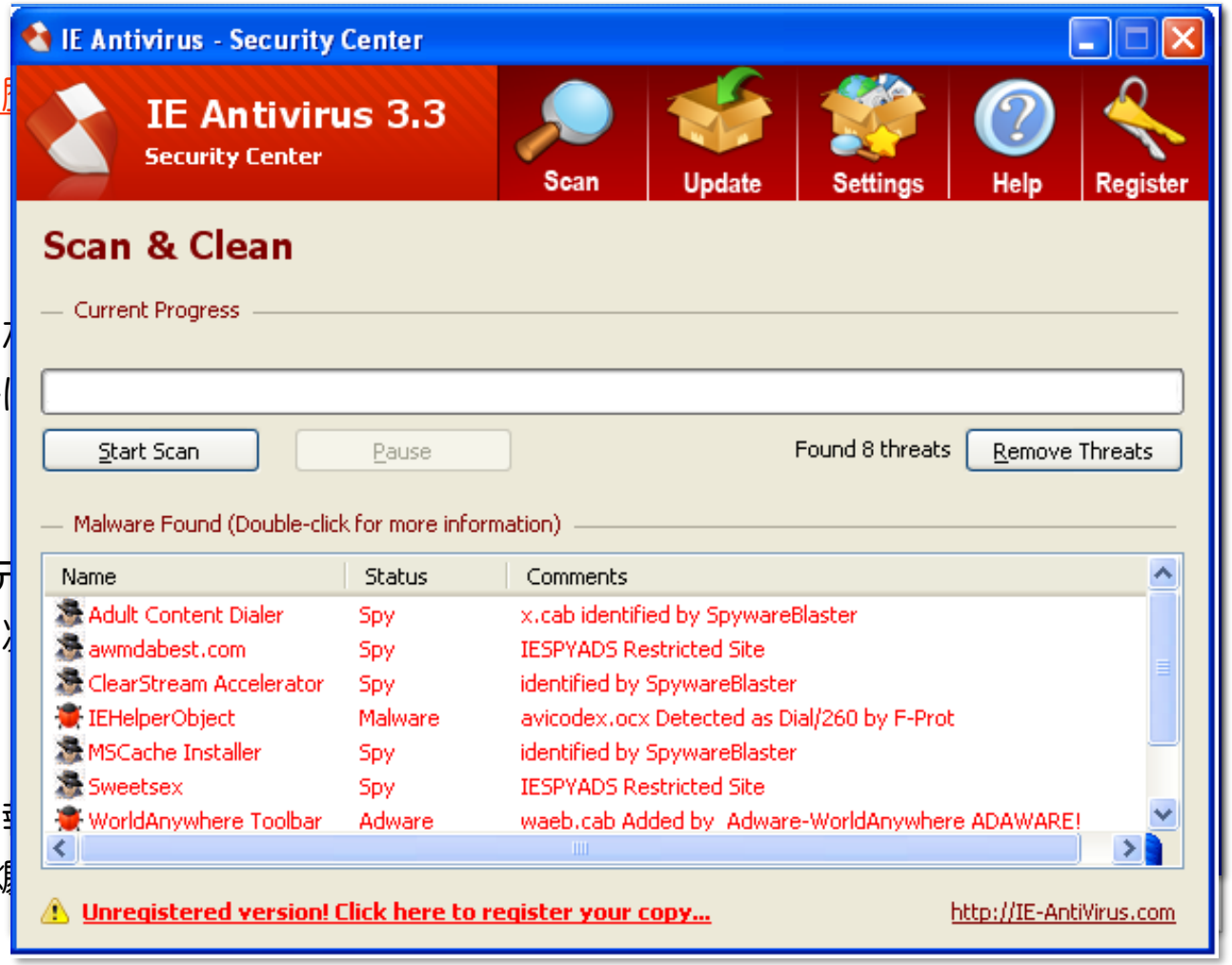


トロイの木馬

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



最近見えている脅威(攻撃)

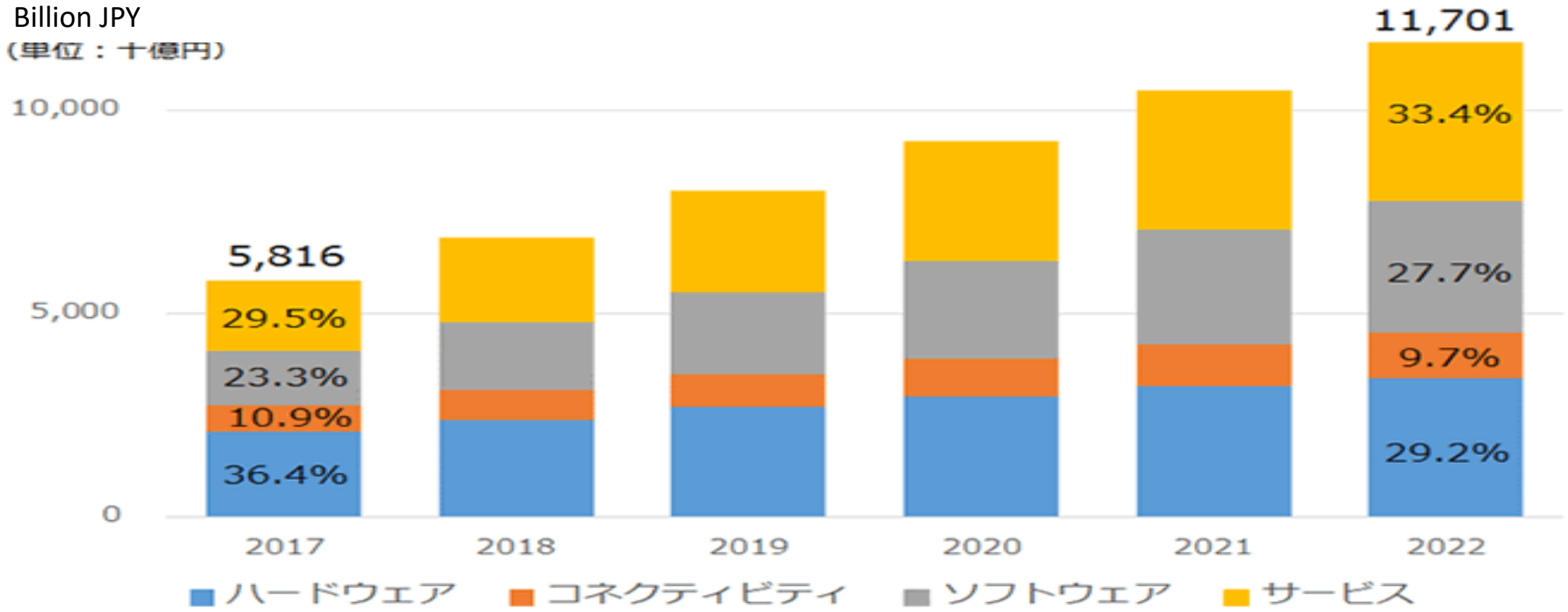
1. ランサムウェア(WannaCry, Emotet等)
2. DDoS
   (DR-DoS、Application DoSの攻撃等)
3. **APTに関係する攻撃(標的型攻撃)**
   (年金機構、三菱電機などへの攻撃)ー Stardust技術等
4. BEC(Business Email Compromise)
5. フィッシング
6. インターネットバンキングを狙う攻撃

   などなど


IoT
Internet of Things
横浜国立大学
吉岡研究室による調査
14
HG8245
嵌入式電話錄音主機WEB管理系統
V1.0
Java Application
Web Application
pandora
BISBOX
RouterOS v5.22
11n 150Mbps WLAN ADSL2+ Modem Router
DrayTek
ZTE中兴
F460
Welcome To Streamyx Connection Setup
Network video client

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

1. Automobile
2. Objects
3. Human
4. Livestock

Monitoring Analysis

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

Optimization

18. Energy Consumption
19. Factory Production
20. Supply-Chain
21. Delivery Route

New Services

22. Sharing service
23. Wearable Device
24. Smart Product
25. Connected Car
26. Smart/Telematics Insurance
27. Smart retails
28. IoT Payment Device

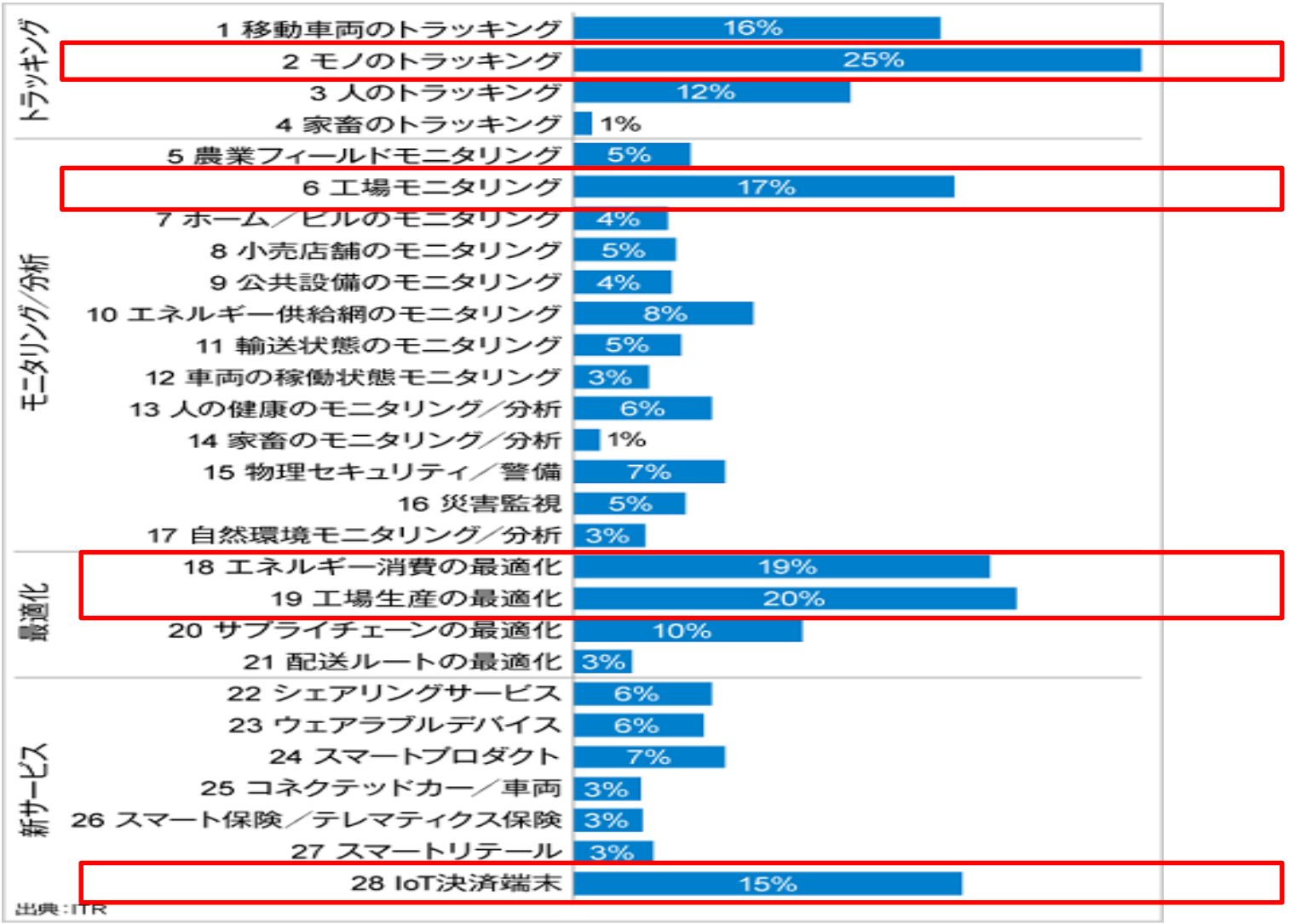
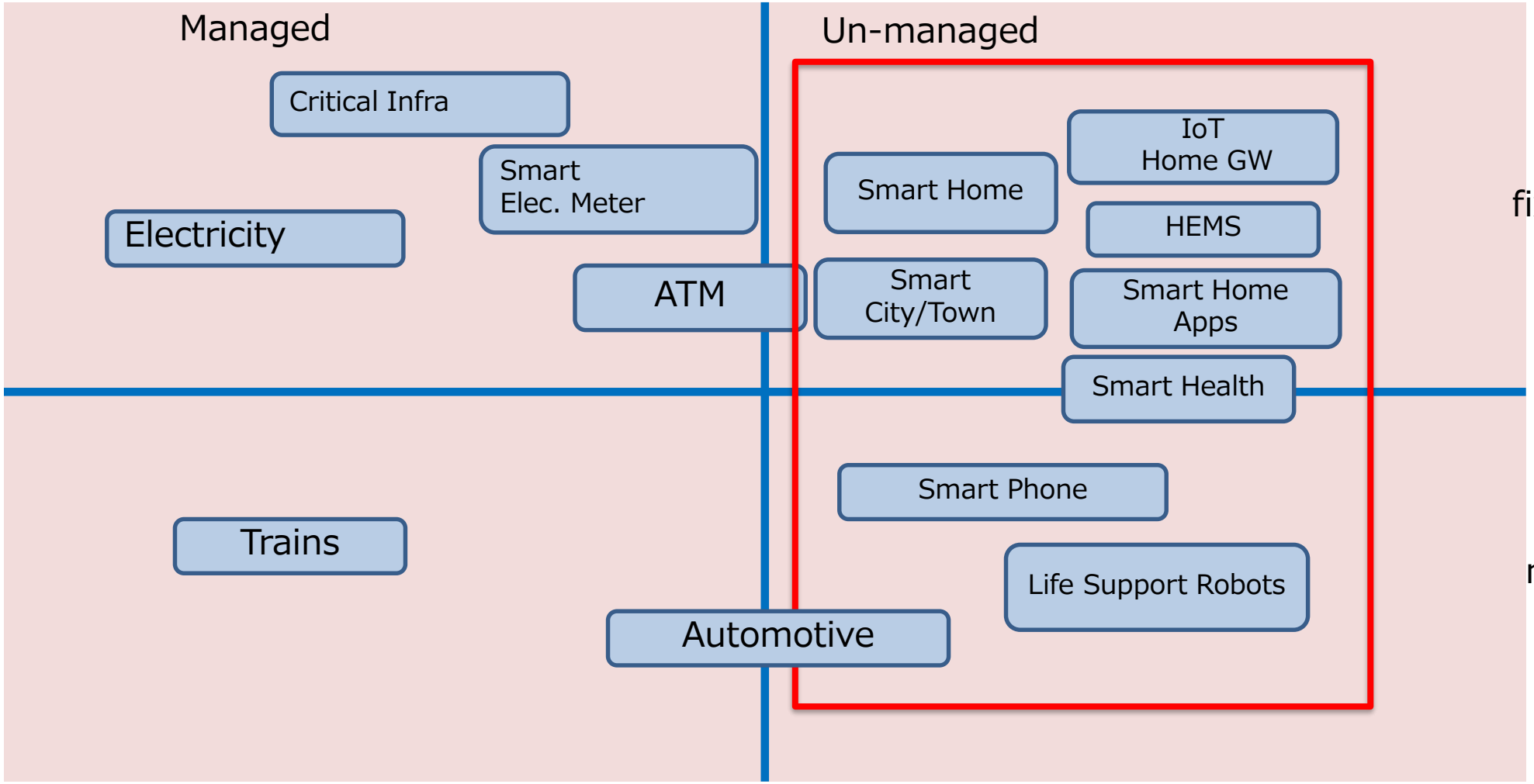


図. IoT導入企業における分野ごとの実施率（全業界平均）

ITR/2017

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

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.

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 ready to join 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 concerns pro boost in IoT services

by

News roundup: As Internet of Things concerns become rise reality, one vendor is quick to offer IoT to combat the risks. Plus: 1% of users create e risk; Target pays up; Apple devices ly secured in the enterprise.

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

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

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].3.0.dm800s
[redacted].login: root
Password:12345

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

リモートログイン成功

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
- 機器のライフサイクルが長い
- 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
- かなり重要なアプリケーションにも活用されているため、インパクトが大きい場合がある

などなど

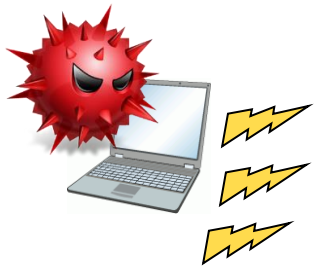
攻撃の観測のための2つのアプローチ

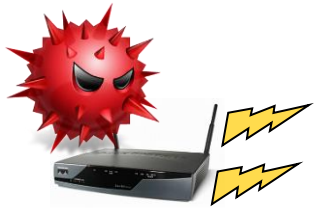
» （これまでの）受動（passive）型：
観測用ネットワークで攻撃が来るのを待つ
- ダークネットモニタリング
- ハニーポット

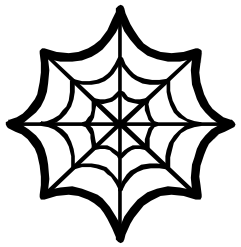
» 能動（active）型：
インターネット上の攻撃ホスト情報・脆弱性等を自ら探索する
- Web, Telnet, FTP等へのアクセスによる機器、システムの判定
- バックドアポート等の確認

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



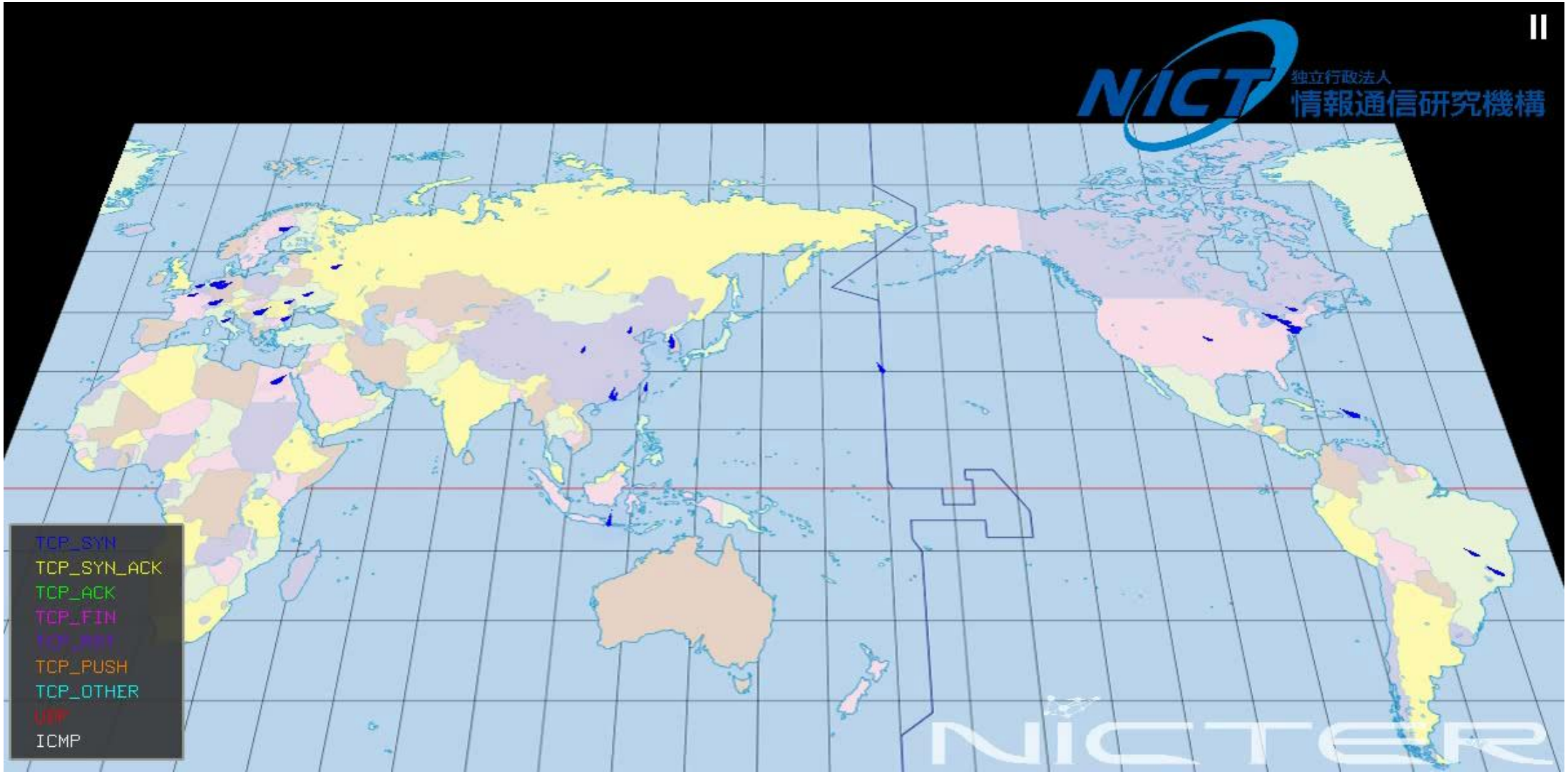




ダークネット

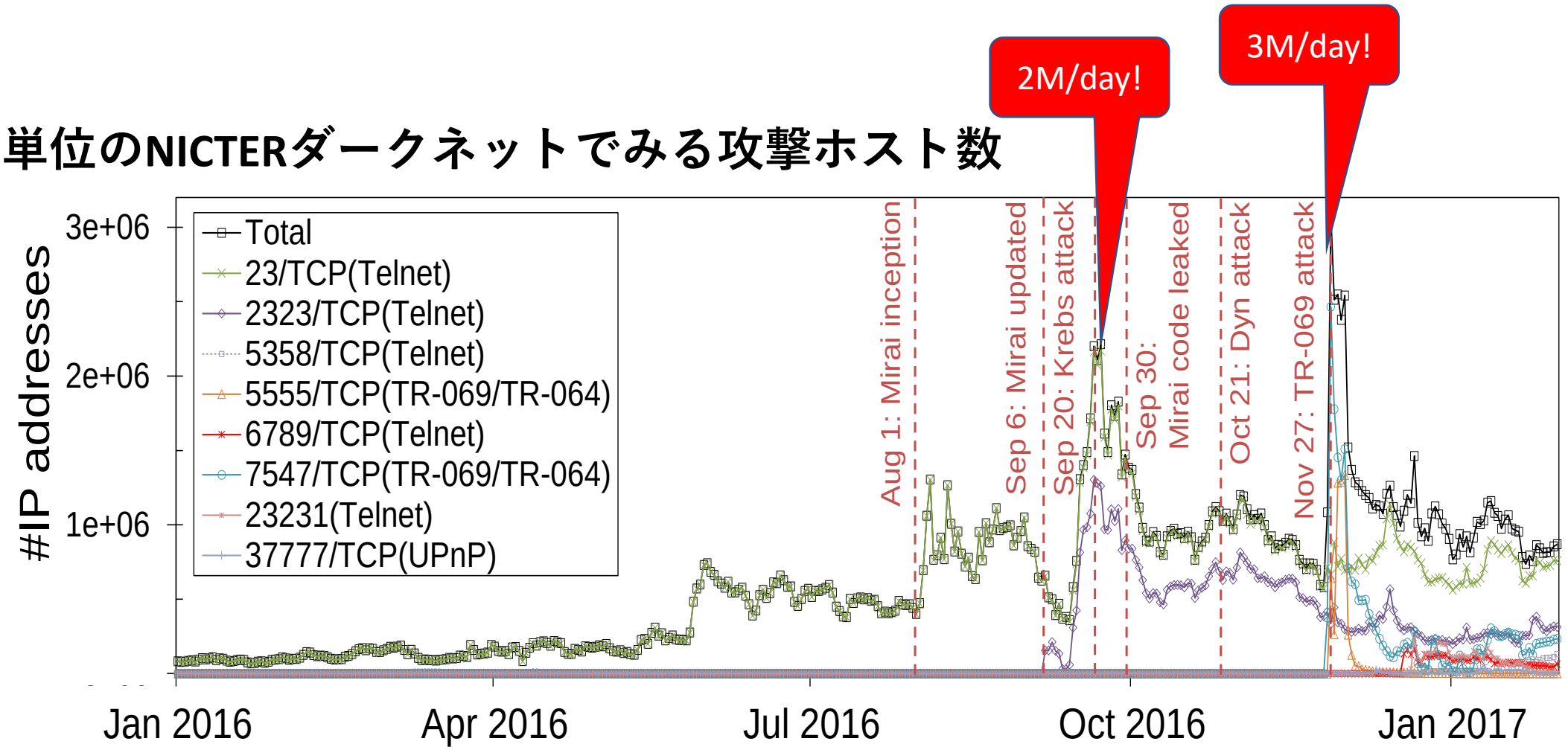
マルウェア（不正プログラム）に感染して外部に無作為に攻撃を行っているパソコン、デバイスからの攻撃の観測に有効

nicter-Atlasに“Port23”のスキャン

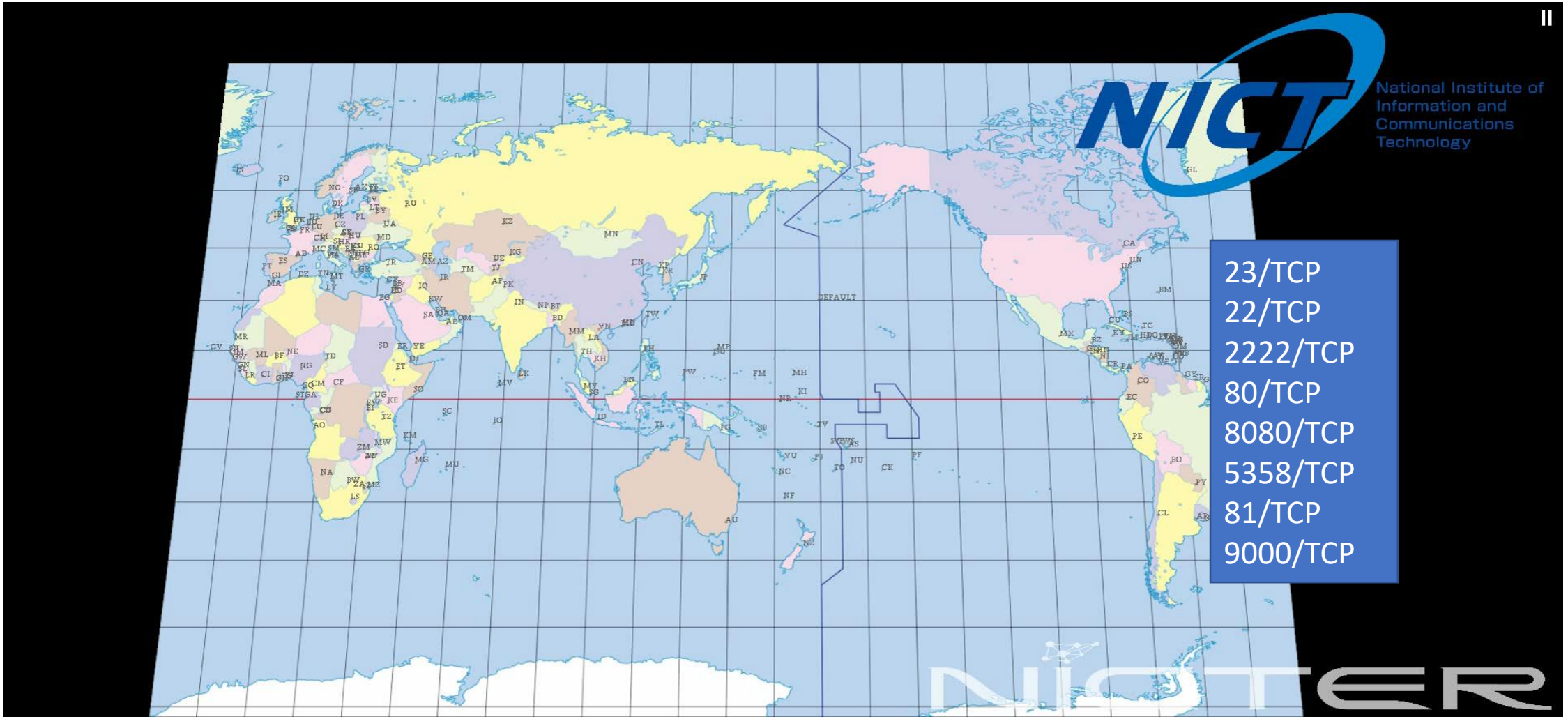


IoT関連ポートへのスキャンはますます増加・多様化

日単位のNICTERダークネットでみる攻撃ホスト数

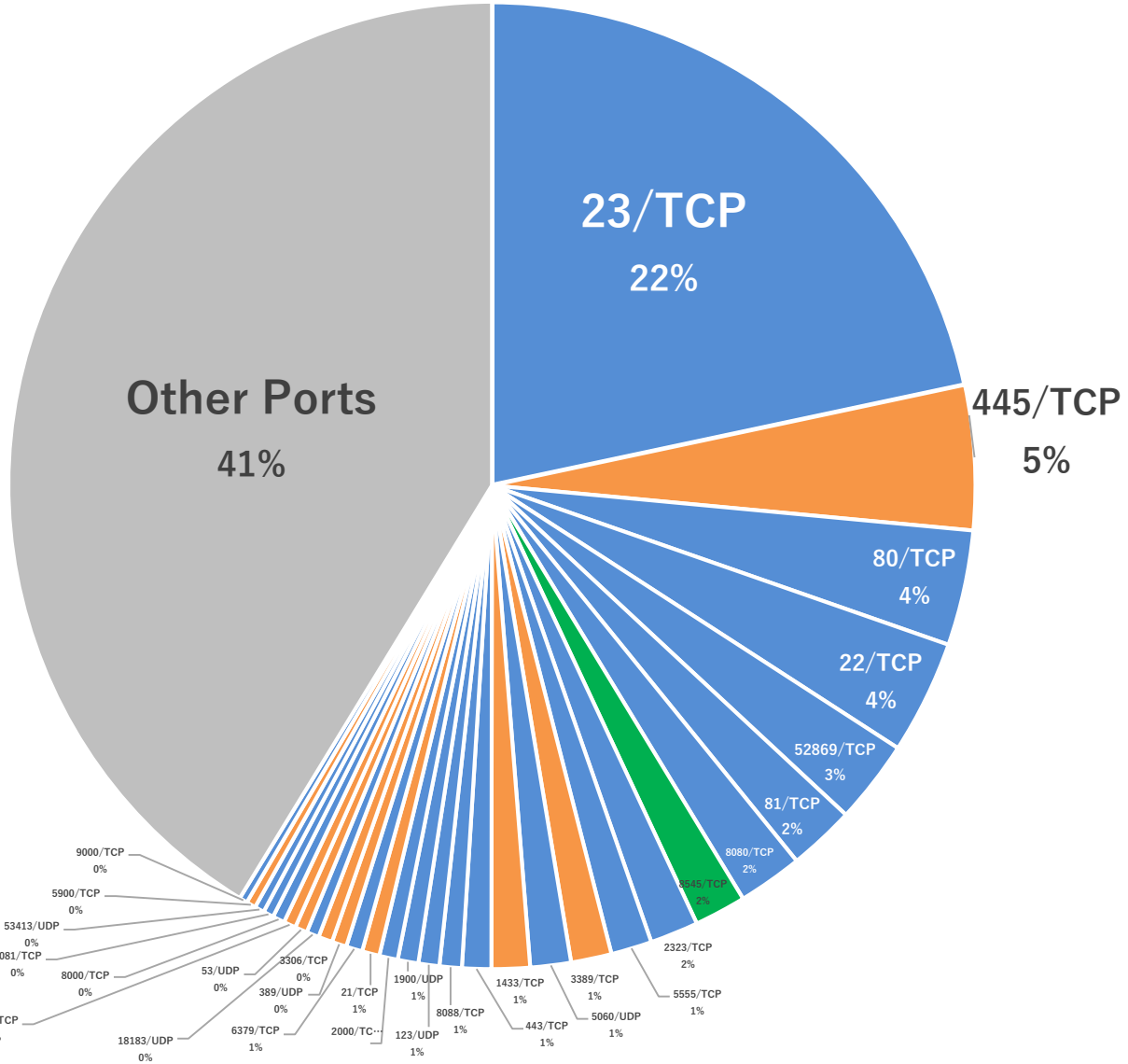


IoT攻撃に関連するポート群へのスキャン
（ポート23へのスキャンを含む）



感染機器の分布（2018年）

- NICTER 観測レポート 2018：宛先ポート番号別パケット数分布 -



IoT ＝ **47.7%**（上位30ポート中）

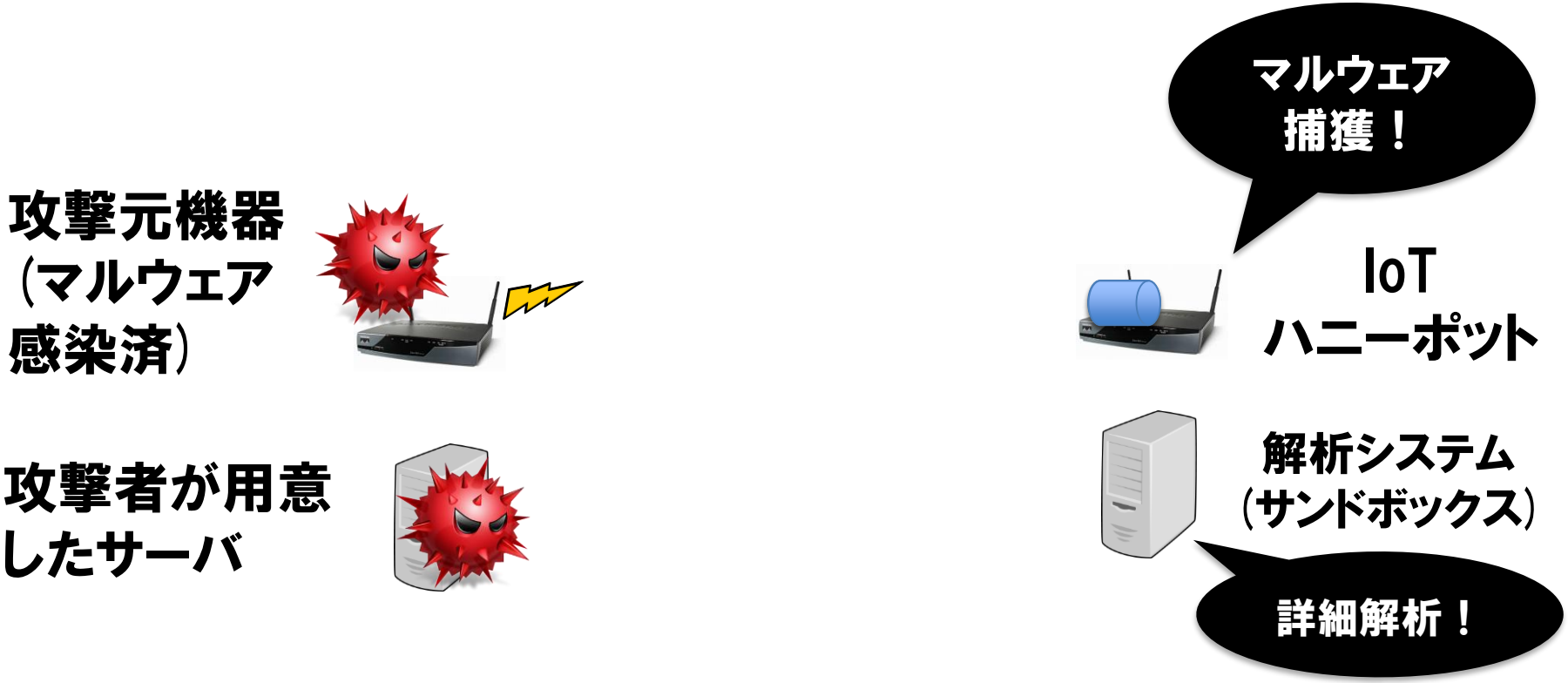
ポート番号	攻撃対象
23/TCP	IoT機器 （Webカメラ等）
445/TCP	Windows（サーバサービス）
80/TCP	Webサーバ（HTTP）
22/TCP	IoT機器（ルータ等） 認証サーバ（SSH）
52869/TCP	IoT機器（ホームルータ等）
81/TCP	IoT機器（ホームルータ等）
8080/TCP	IoT機器（Webカメラ等）
8545/TCP	イーサリアム（仮想通貨）
2323/TCP	IoT機器（Webカメラ等）
5555/TCP	Android機器 （セットトップボックス等）

National Institute of Information and Communications Technology

NICTER
Network Incident analysis Center for Tactical Emergency Response

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

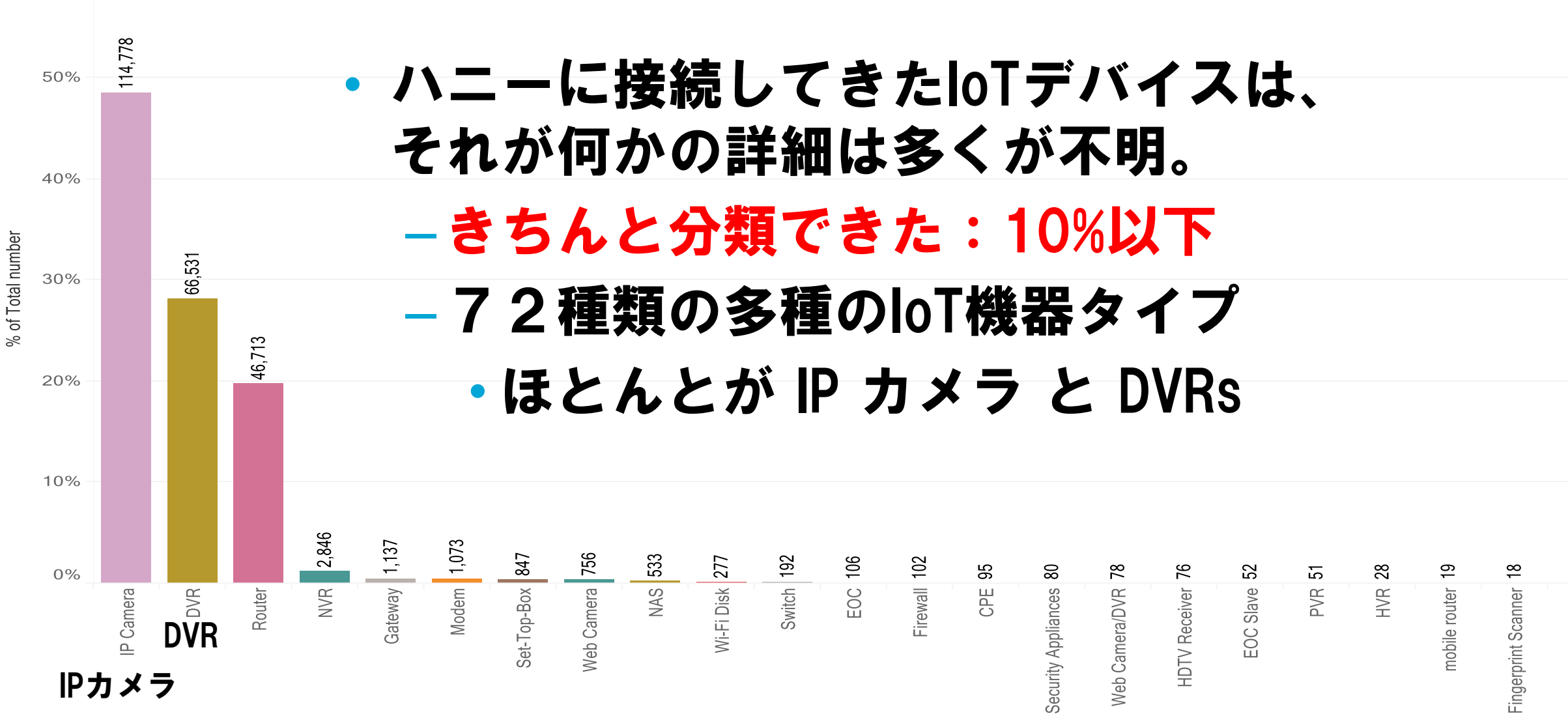
Security Appliance

Internet Communication Module

Video Broadcaster

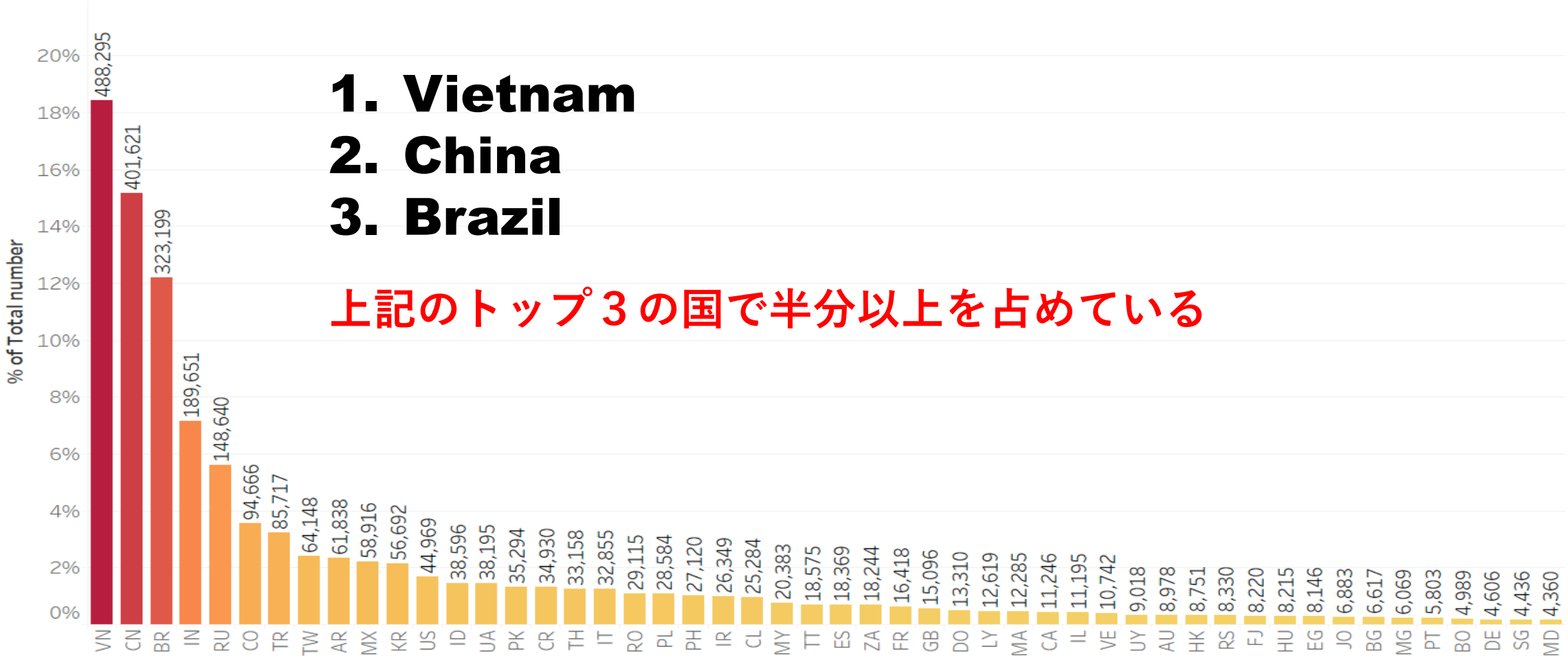
Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, and Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, “IoTPOT: Analysing the Rise of IoT Compromises,” 9th USENIX Workshop on Offensive Technologies (USENIX WOOT 2015).

感染IoT機器の種別



- 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 カメラ と DVRs

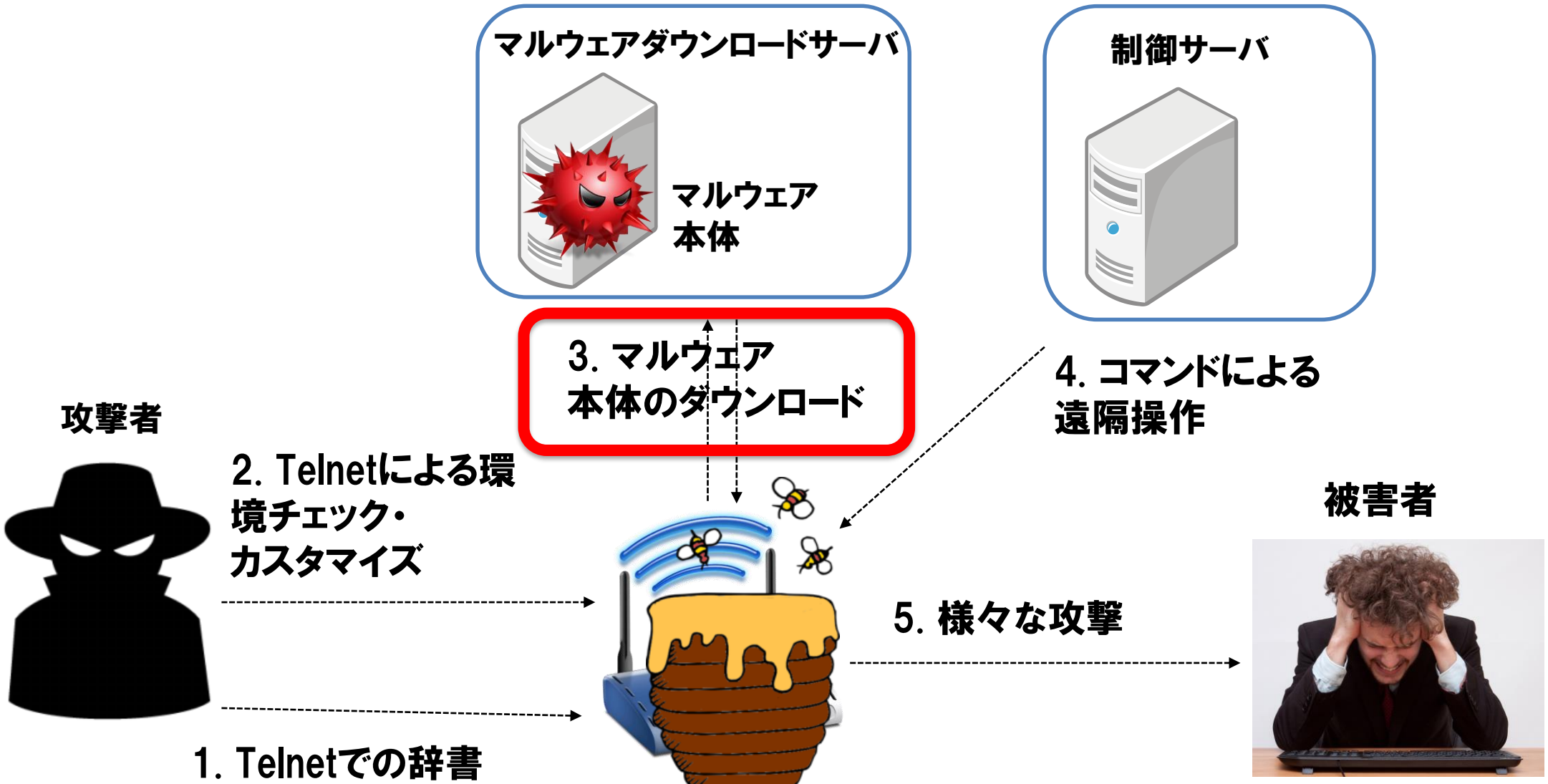
IPアドレス数の観点から、感染国の状況



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

Telnetベースのマルウェア感染の流れ



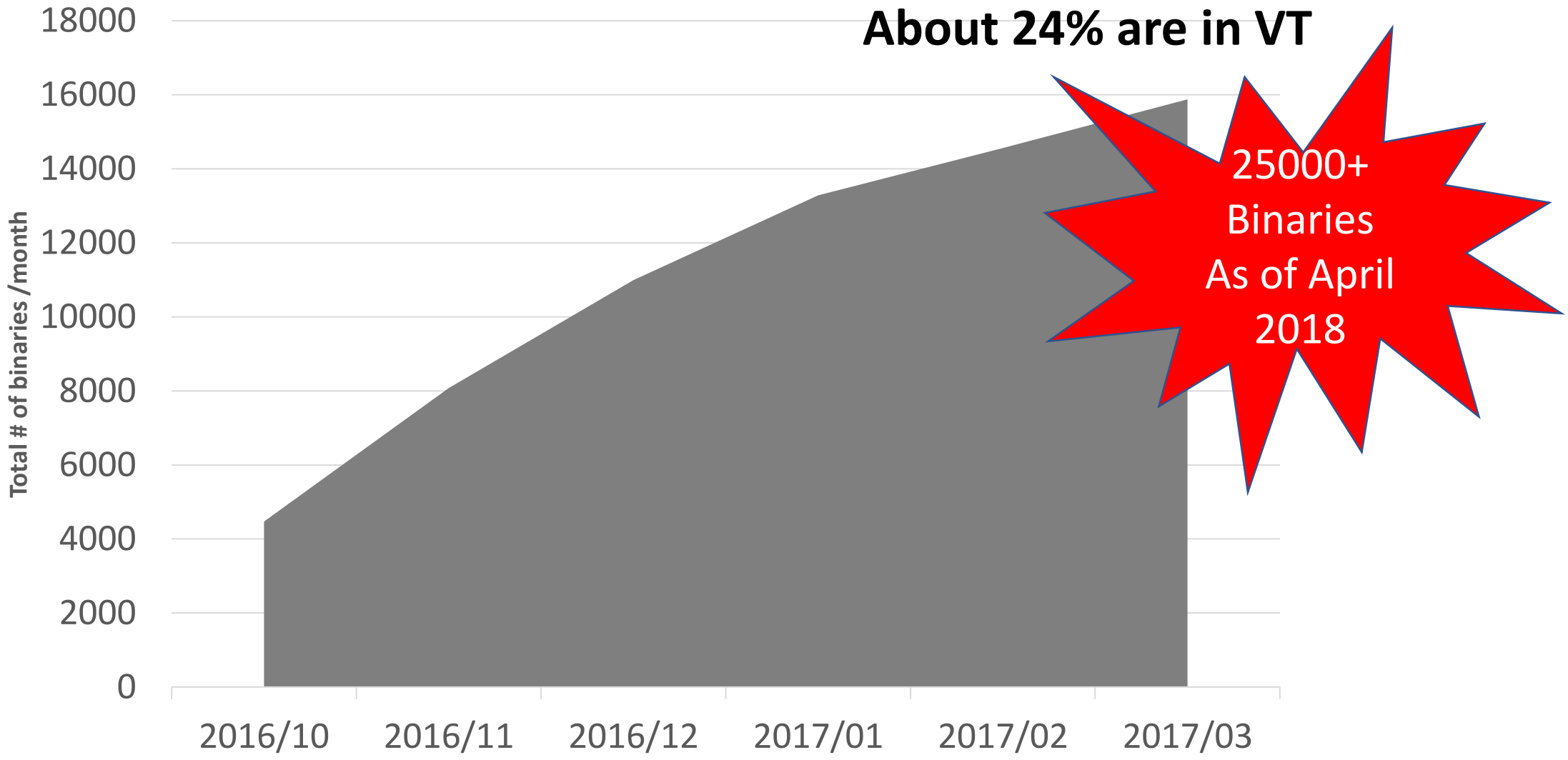
マルウェアのバイナリーDLの例

```
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
ox ./ cat mipsel > busybox; rm mipsel; cp busybox systemr; rm busybox; ./systemr & sleep 1
./ cat arm > busybox; rm arm; cp busybox systemr; rm busybox; ./systemr && sleep 1
x ./; cat arm7 > busybox; rm arm7; cp busybox arm7; rm busybox; ./arm7 && sleep 2
./ cat ppc > busybox; rm ppc; cp busybox systemr; rm busybox; ./systemr & sleep 1
ox ./ cat superh > busybox; rm superh; cp busybox systemr; rm busybox; ./systemr && sleep 1
ox ./ cat mips16 > busybox; rm mips16; cp busybox systemr; rm busybox; ./systemr & sleep 1
./; cat i586 > busybox; rm i586; cp busybox systemr; rm busybox; ./systemr && sleep 1
./; cat i686 > busybox; rm i686; cp busybox systemr; rm busybox; ./systemr && sleep 2
ox ./; cat x > busybox; rm x; cp busybox systemr; rm busybox; ./systemr && sleep 1
./; cat m68 > busybox; rm m68; cp busybox systemr; rm busybox; ./systemr && sleep 1
```

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

```
66 #echo
67 #exit
bin.sh [RO]                                                    67,1          末尾
```

捕獲できているバイナリー



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）

Mirai情報（続）

DDoS攻撃

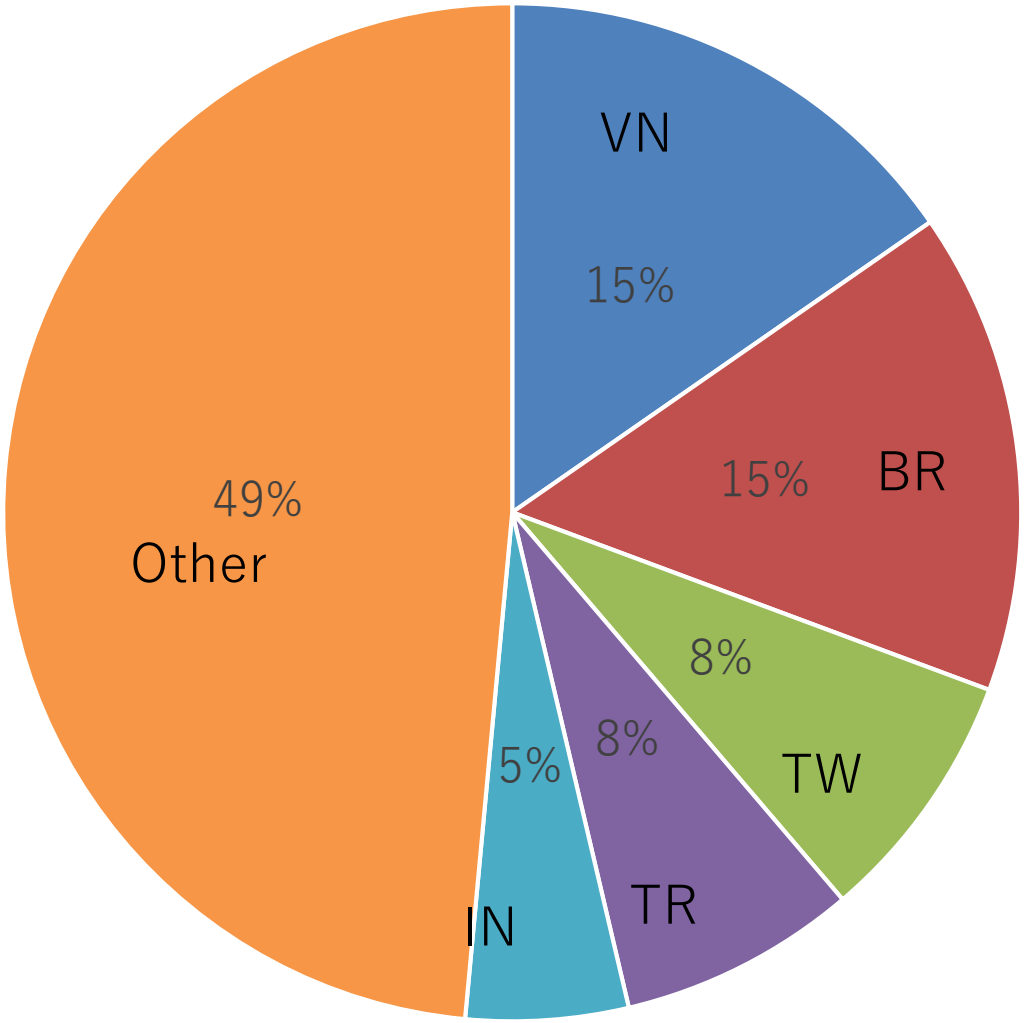
- Krebs on Security（16/9/20）
  -Akamaiサービス

- DYN社DNSサーバ(16/10/21)
  -Netflix
  -Twitter
  -Amazon

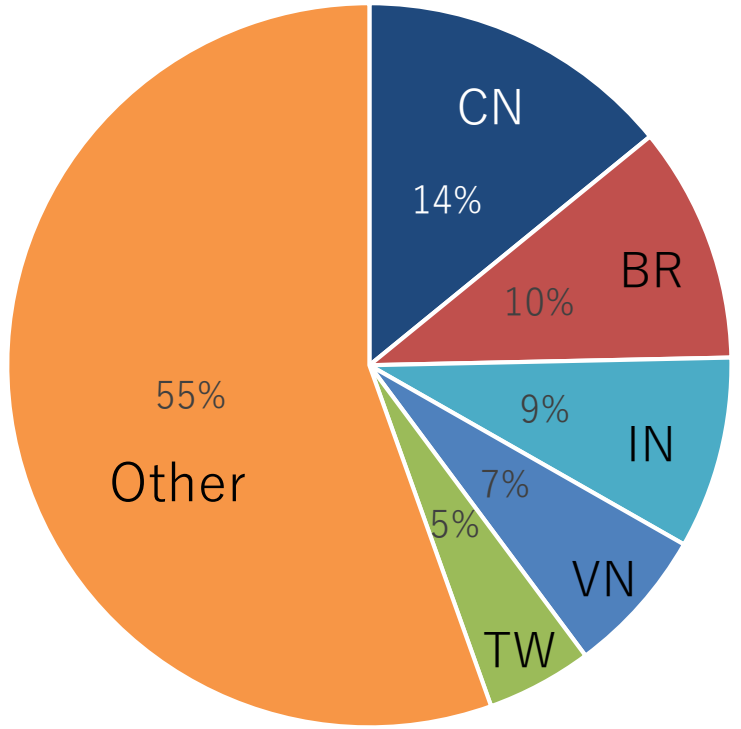
- **感染機器**
  -プリンタ
  -カメラ
  -ルータ
  -DVR

- **対応アーキテクチャ**
  -ARM
  -ARM7
  -MIPS
  -PowerPC
  -SH4
  -SPARC
  -X86

発生時の送信元国傾向



Miraiの感染国
(2016/08/01)



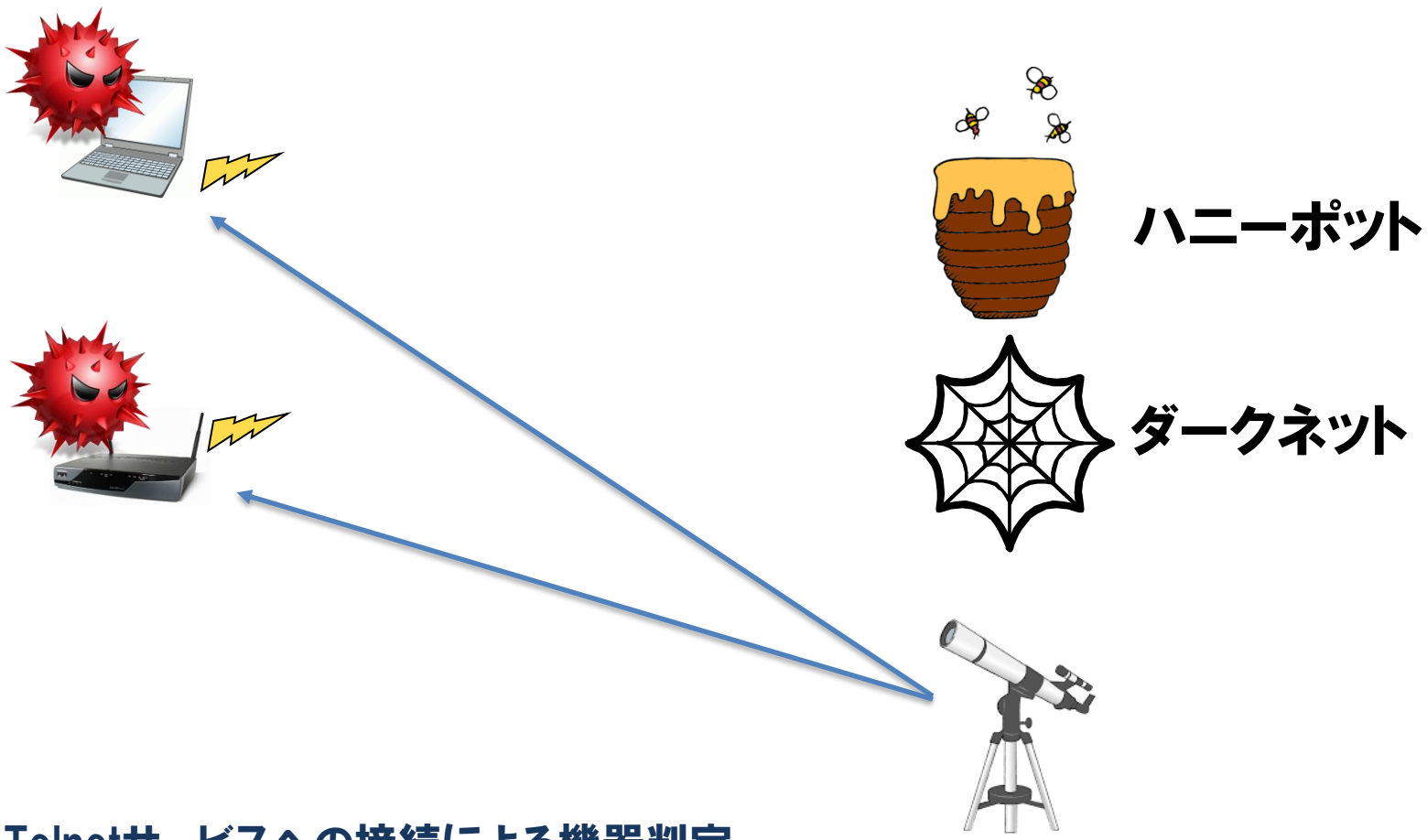
Mirai発生前のIoT感染国
(2016/07/31)

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

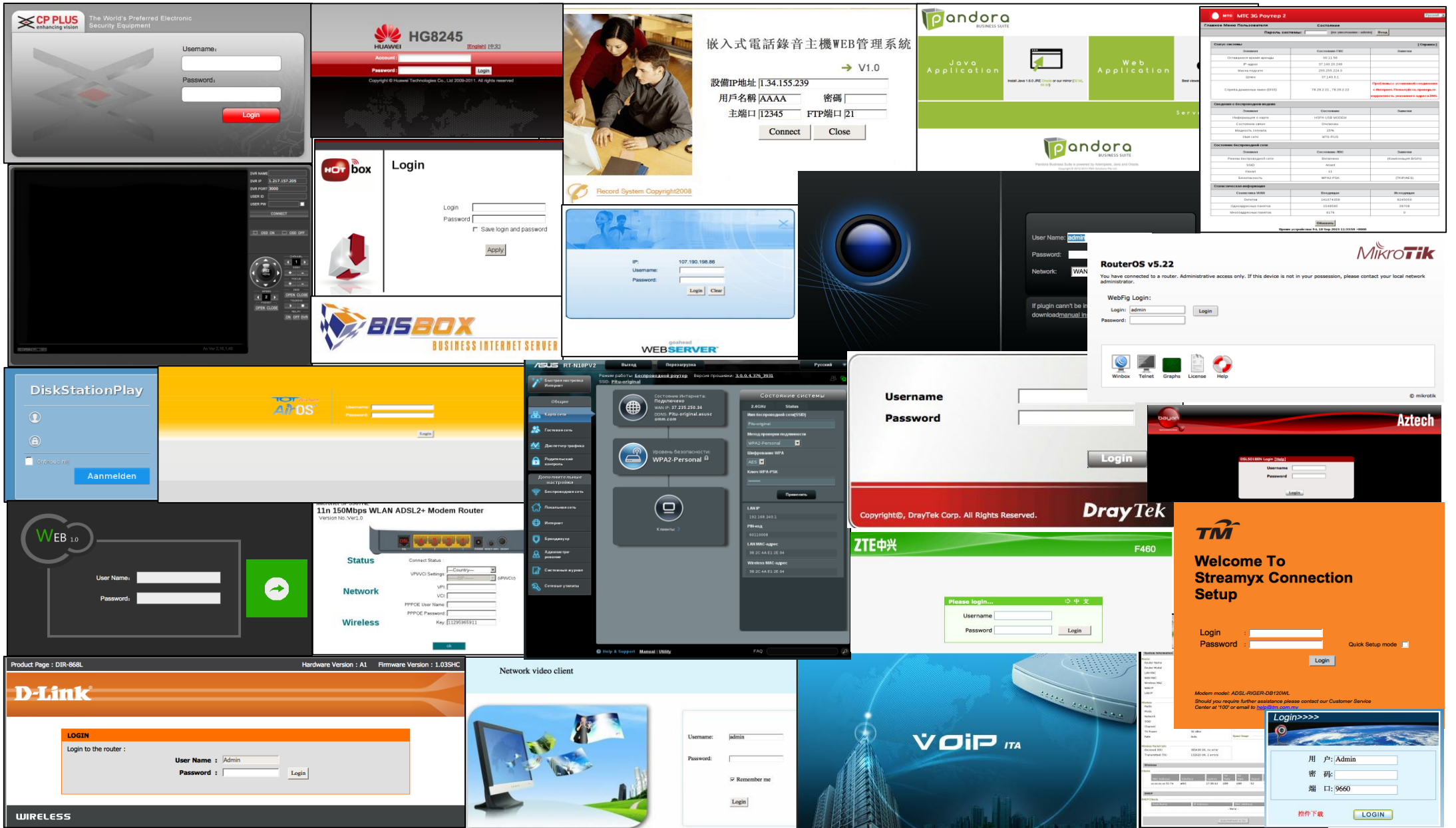
攻撃元機器の判定



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



感染機器の種別の推定

- 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
  - [illegible]
  - [illegible]
- 電[illegible]
  - 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









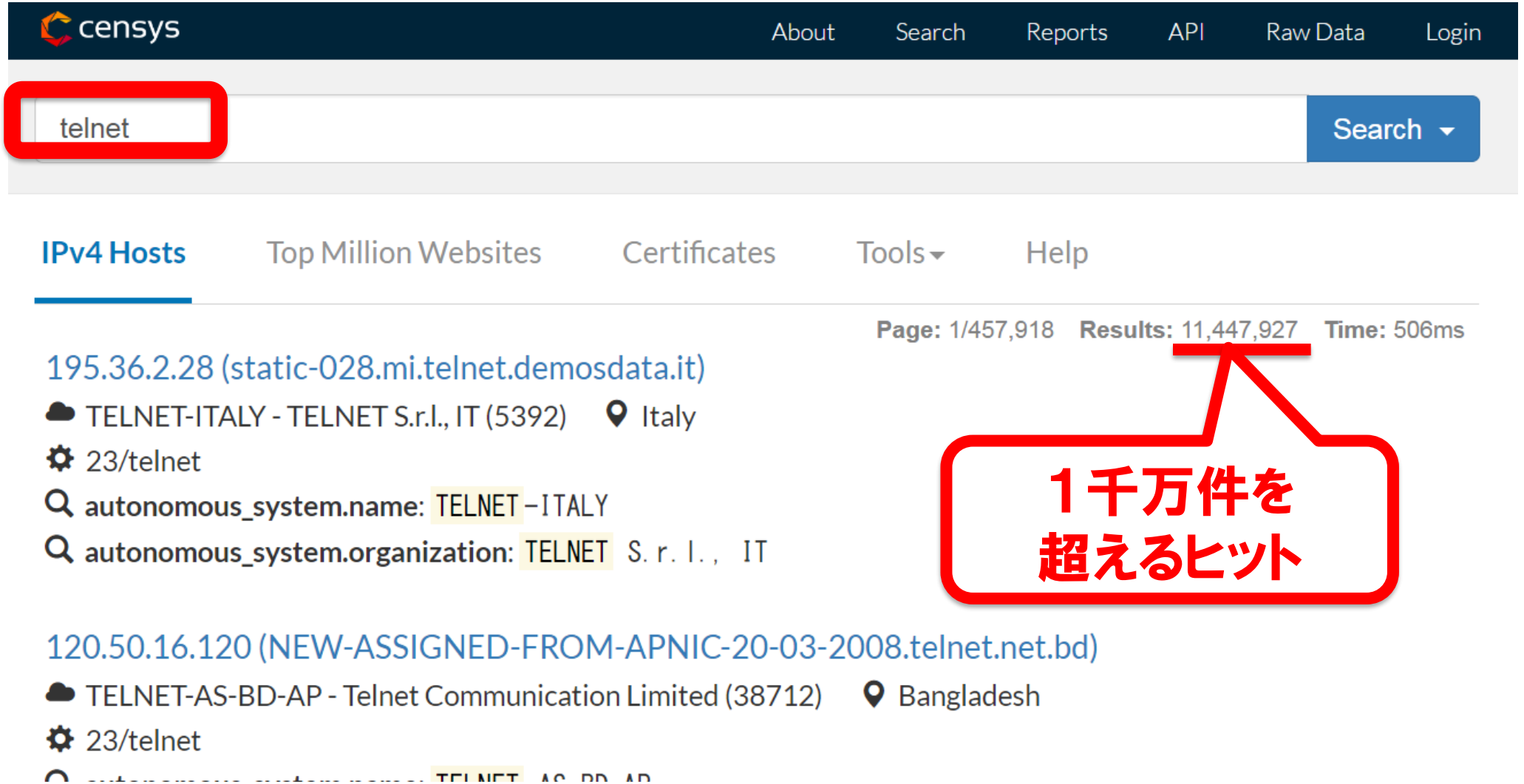
国内メーカの機器の感染事例も複数確認
感染機器情報はJPCERT/CC，内閣サイバーセキュリティセンターに情報提供、または、メーカに直接情報提供済

- 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
  - [illegible]ータ
  - [illegible]W
  - 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



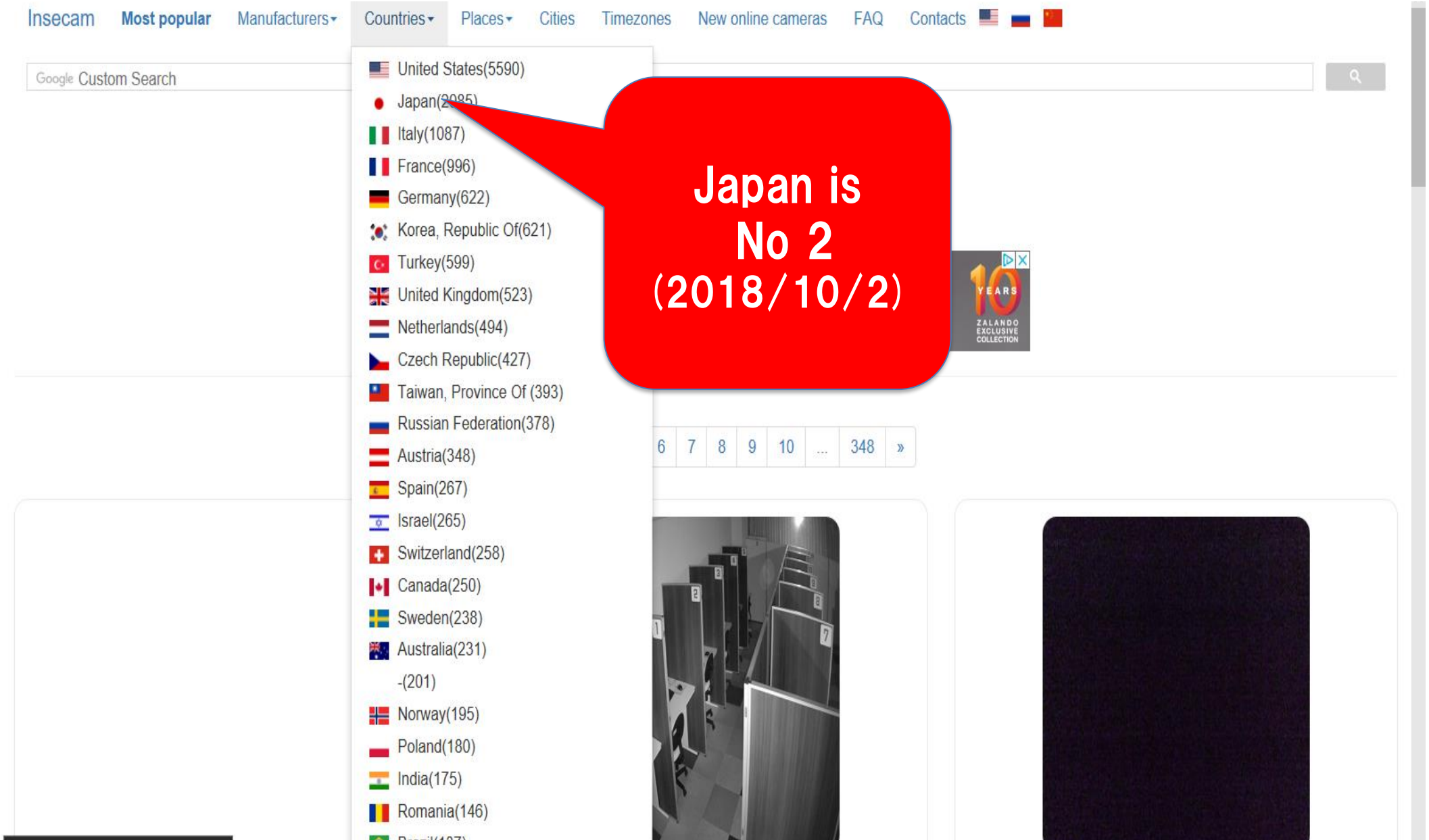



世界中の機器をスキャンした結果を公開しているサイトCensys (ミシガン大学)



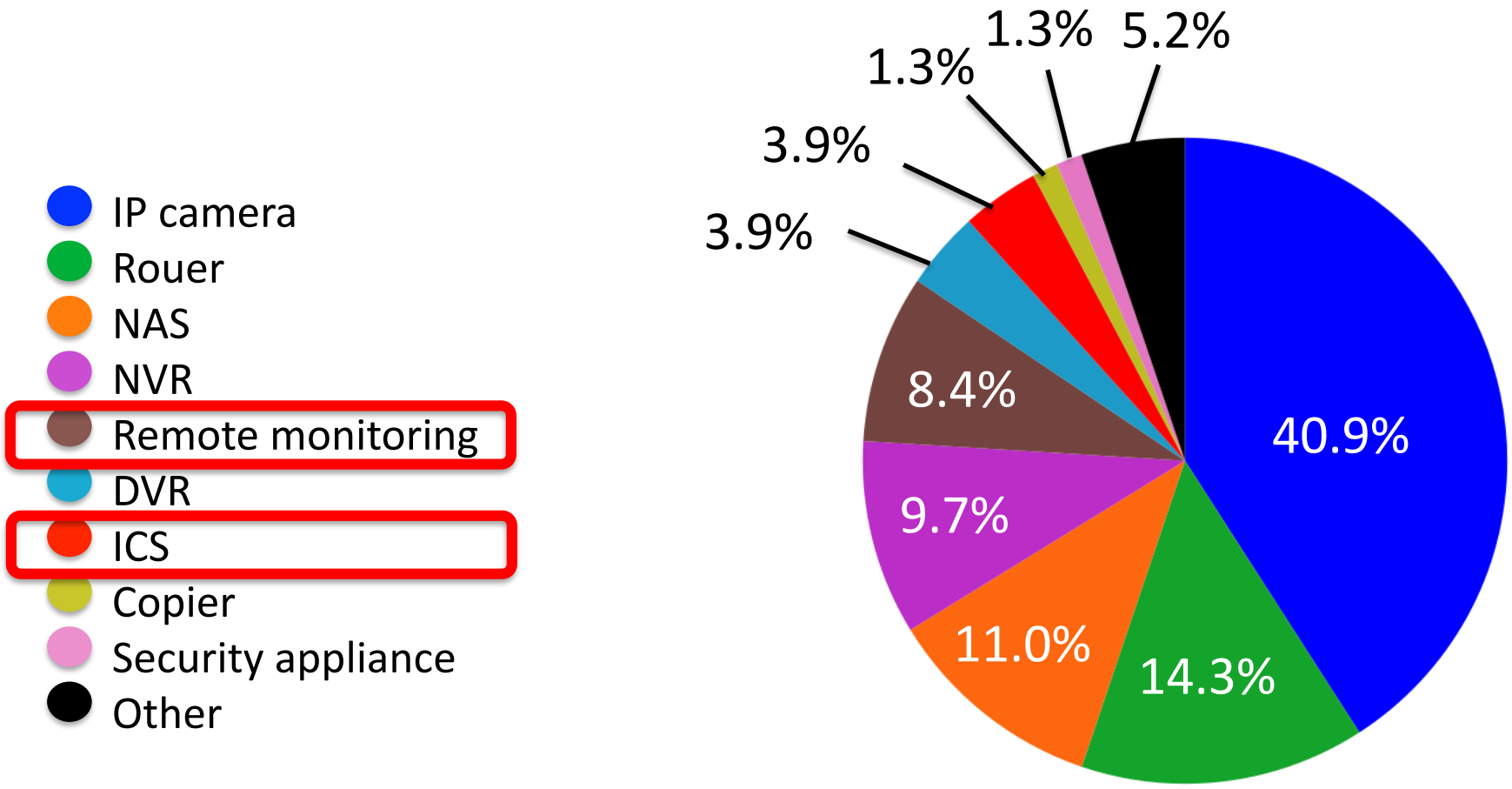
ネットワークカメラ画像無断公開サイト：Insecam

https://www.insecam.org/



見つかった脆弱な IoT 機器

一つASから154種類の脆弱なIoT機器が見つかった

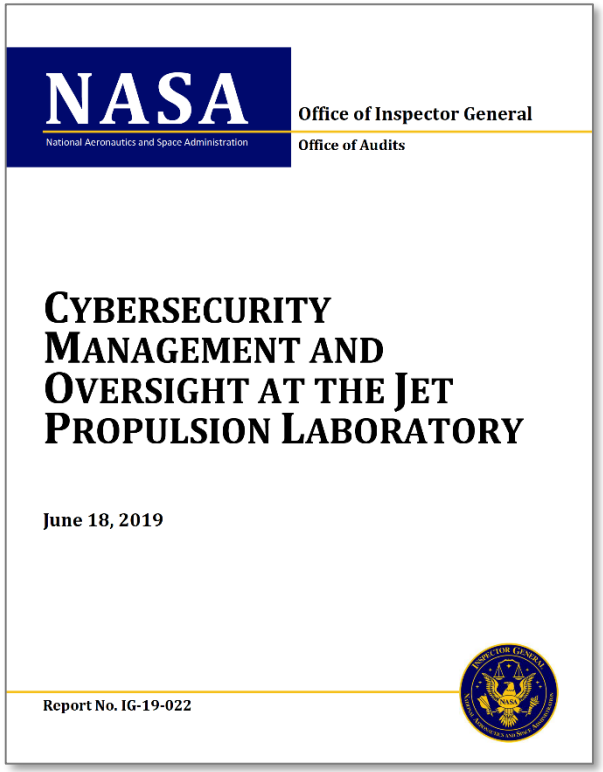


事例:
Waterworks Monitoring System

事例:

最近、NASAへのサイバー攻撃（2019）

- NASAのジェット推進研究所（JPL）から機密データ漏洩
- 無許可接続されたRaspberry Piが原因（野良IoT）



NASA
National Aeronautics and Space Administration

Office of Inspector General
Office of Audits

CYBERSECURITY MANAGEMENT AND OVERSIGHT AT THE JET PROPULSION LABORATORY

June 18, 2019

Report No. IG-19-022

itmedia.co.jp

NASA、サイバー攻撃で機密データ流出　侵入口は無許可接続の「Raspberry Pi」 - ITmedia NEWS

ITmedia NEWS > セキュリティ > NASA、サイバー攻撃で機密データ流出　侵入口は無許...

NASA、サイバー攻撃で機密データ流出　侵入口は無許可接続の「Raspberry Pi」

2019年06月23日 07時45分 公開　[ITmedia]

印刷　1905　Share　B!　828

米航空宇宙局（NASA）のジェット推進研究所（JPL）の研究データが昨年、サイバー攻撃により盗まれていたことが、米連邦政府の監察総監室（OIG）が6月18日付で公開した報告書（リンク先はPDF）で明らかになった。

2018年4月にJPLのネットワークに侵入した攻撃者が約10カ月の間ネットワーク内の多数の脆弱性を利用して行動範囲を広げ、火星科学研究探査機のデータを含む約500MBの機密データを盗んだ。深宇宙通信情報網DSN（ディープスペースネットワーク）のデータにもアクセスした痕跡があるため、JPLのネットワークからDSNの宇宙飛行関連システムを切断したという。

攻撃者の侵入口はJPLのネットワークに無許可で接続していたRaspberry Pi端末だった。本来ならば最高情報責任者室（OCIO）がネットワークに接続するすべての端末を管理しているはずだが、正常に機能していなかった。管理者の1人はOIGに対し、新たに端末を接続する際はセキュリティデータベースに手動で登録することになっているが、更新機能がうまく動かないことがあり、そのまま登録を忘れることがあると語ったという。

Deep Space Network Dish in Goldstone, California

Source: NASA.

DSNのパラボラアンテナ（画像：NASA）

gigazine.net

NASAの機密データがRaspberry Piを侵入口として盗まれたと判明 - GIGAZINE

GIGAZINE

19万点超 著作権フリー音楽
日本最大級のBGM・効果音販売サービス「オーディオストック」 - Audiostock

2019年06月25日 19時00分　セキュリティ

NASAの機密データがRaspberry Piを侵入口として盗まれたと判明

by Les Pounder

アメリカ航空宇宙局(NASA)は、2018年にジェット推進研究所(JPL)のネットワークがハッキングされたことを確認しました。報告によると、ハッキングをしかけたクラッカーは、JPLのネットワークに無許可で接続されたRaspberry Piを侵入口として、データを盗み出したとのことです。

https://www.flickr.com/photos/biglesp/14234773312/"を新規タブで開く

https://oig.nasa.gov/docs/IG-19-022.pdf
https://www.itmedia.co.jp/news/articles/1906/23/news012.html
https://gigazine.net/news/20190625-nasa-hacked-raspberry-pi/

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購入

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

しかし、2018年５月には世界54カ国で50万台を超えるIoT機器が マルウェアVPNFilterに感染していることが確認されており、そのマルウェアは、再起動でも継続活動を行うもの。（持続感染性）

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

3.感染までの経過時間を記録し機器を再起動

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

2. マルウェアがダウンロードされ実行された時，感染状態と判断

最近、感染マルウェアの挙動として分かってきている事

1. **感染後、自動的にネットワーク環境を取得する**
   – Wi-Fi setting, SSID, Password

2. **環境設定変更に関する攻撃**
   – VPN, Firewall activation, DDNS, DNS, Firmware Update

3. **他のIoTマルウェアの感染をブロックするための試みを行う**
   – Firmware Update, Firewall activation

などなど

IoTのセキュリティ対策に関連する活動事例

総務省 「IoTセキュリティ戦略」

IoTセキュリティ総合対策（2017年10月公表）

①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。

②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。

③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。

④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。

⑤国際連携の推進

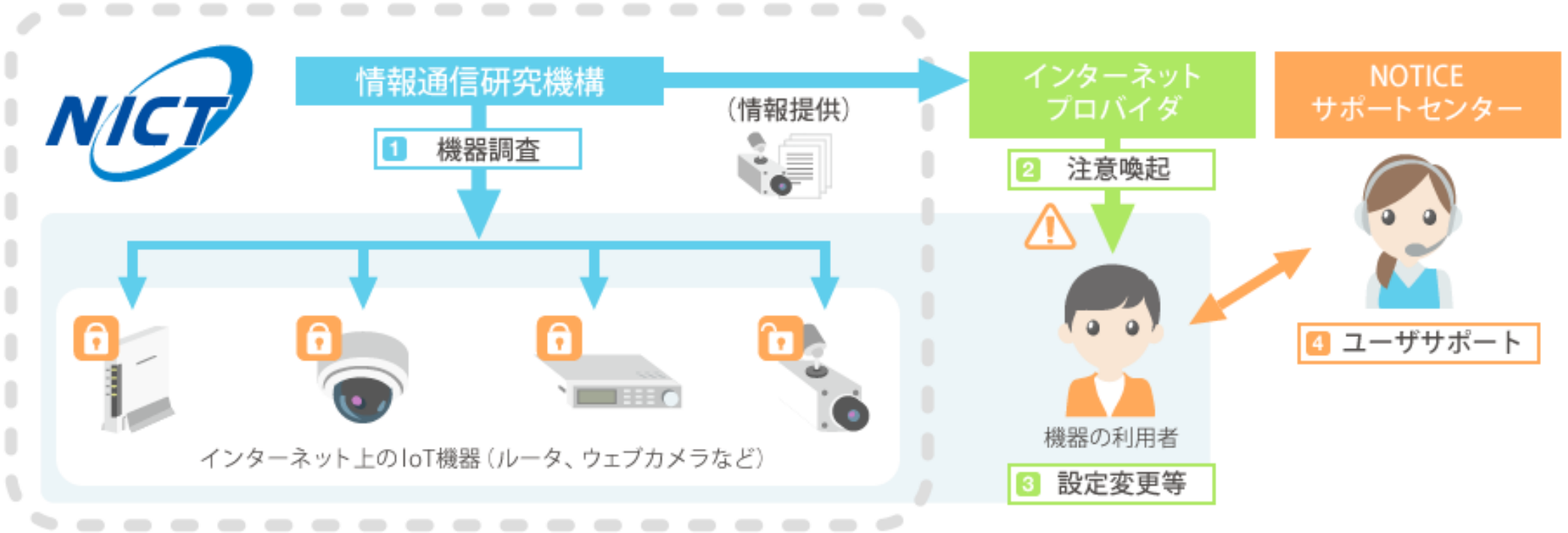
・ 二国間及び多国間の枠組みの中での情報共有やルール作り、人材育成、研究開発を推進。

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）

総合対策の進捗状況や今後の取組方針を整理し、「プログレスレポート」として公表（平成30年7月）

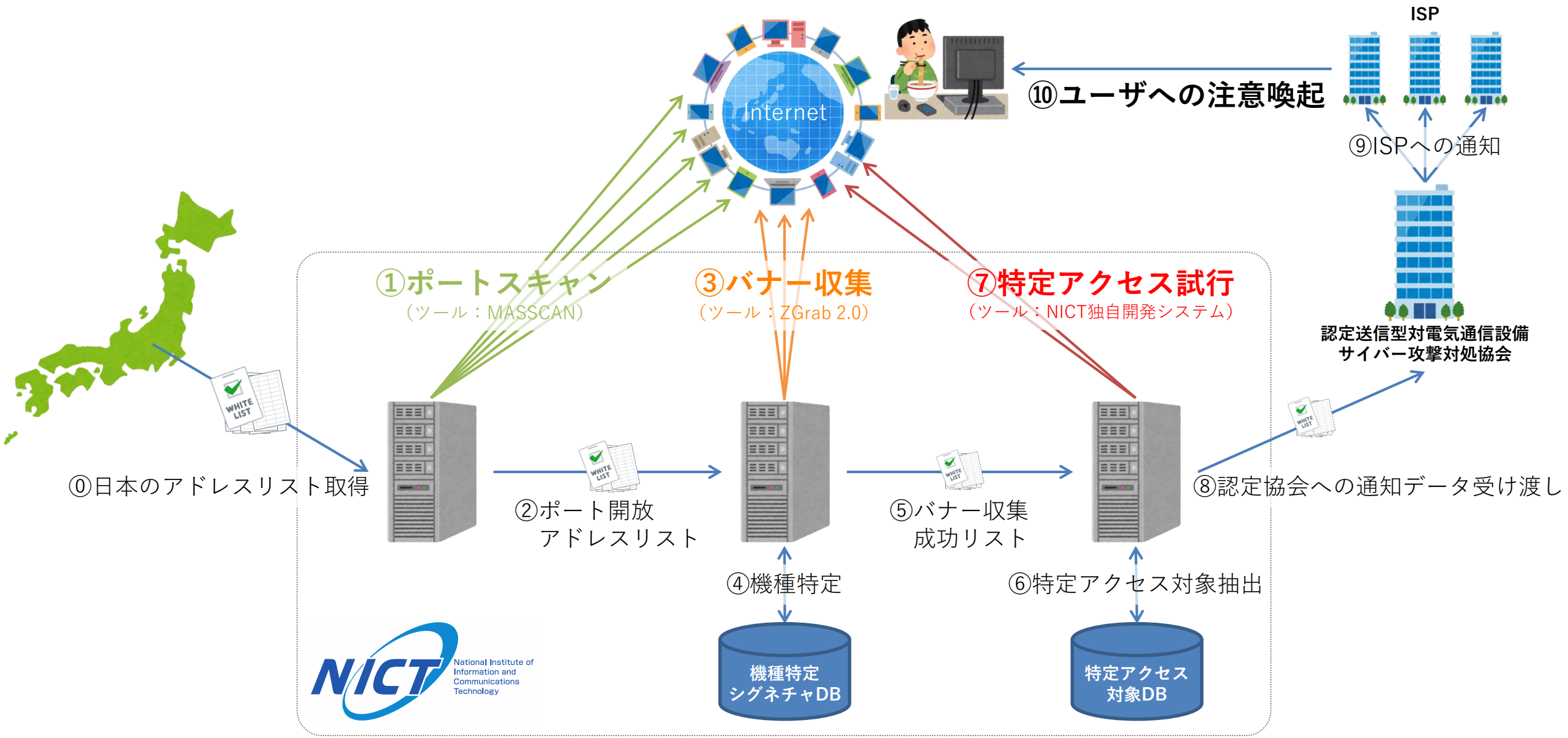
NOTICE

- **NOTICE: National Operation Towards IoT Clean Environment**
- 総務省、NICT、ISPが連携し、サイバー攻撃に悪用されるおそれのある機器の調査及び当該機器の利用者への注意喚起を行う取組



https://notice.go.jp/

NICTによるIoT機器調査の技術詳細



能動的対策と受動的対策

能動的対策

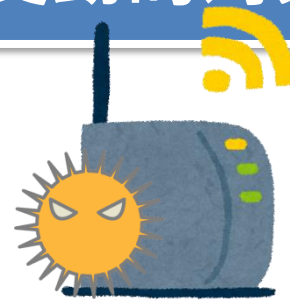
パスワード設定等に
不備があるIoT機器

能動的観測

NOTICE
National Operation Towards IoT Clean Environment

通知

受動的対策

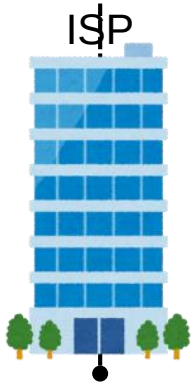


感染IoT機器

受動的観測

NICTER

通知



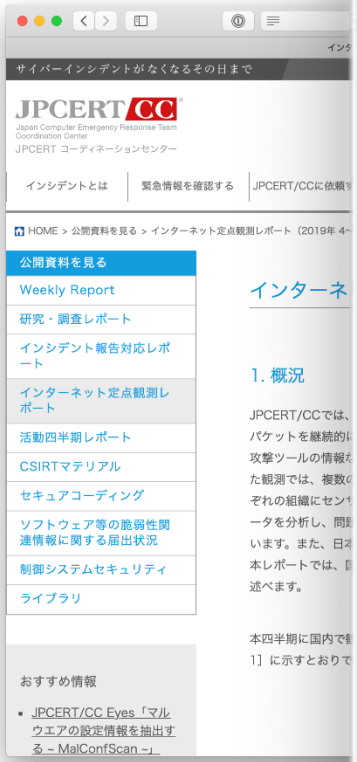
ISP

2019年9月NOTICE注意喚起の実施状況公開

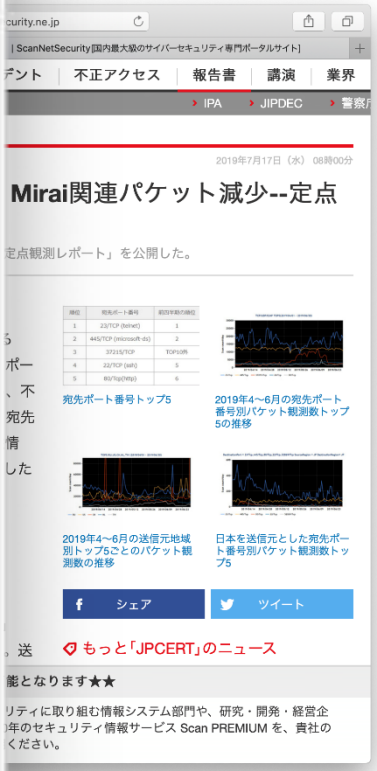
NOTICE National Operation Towards IoT Clean Environment（アクティブスキャン）　　NICTER（パッシブモニタリング）

NOTICEの取組結果	マルウェアに感染しているIoT機器の利用者への注意喚起の取組結果
調査対象となったIPアドレスのうち、 ID・パスワードが入力可能であったもの → **約98000件** 上記の内、ID・パスワードによりログインでき、 注意喚起の対象となったもの → **延べ505件**	感染が確認されたIPアドレス（日）の数 → **80件～559件**

出典：総務省、NICT、ICT-ISAC “脆弱なIoT機器及びマルウェアに感染しているIoT機器の利用者への注意喚起の実施状況”
http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00033.html



出典
https://www.jpce



NetSecurity
rticle/2019/07/17/42632.html

NICT National Institute of Information and Communications Technology

ICTER
ork Incident analysis Center for Tactical Emergency Response

NOTICE の「まとめ」

●NOTICEの舞台裏

✓NICT法改正

✓IoT機器調査の技術詳細

●NOTICEのこれから

✓これまで：抑制的なIoT機器調査

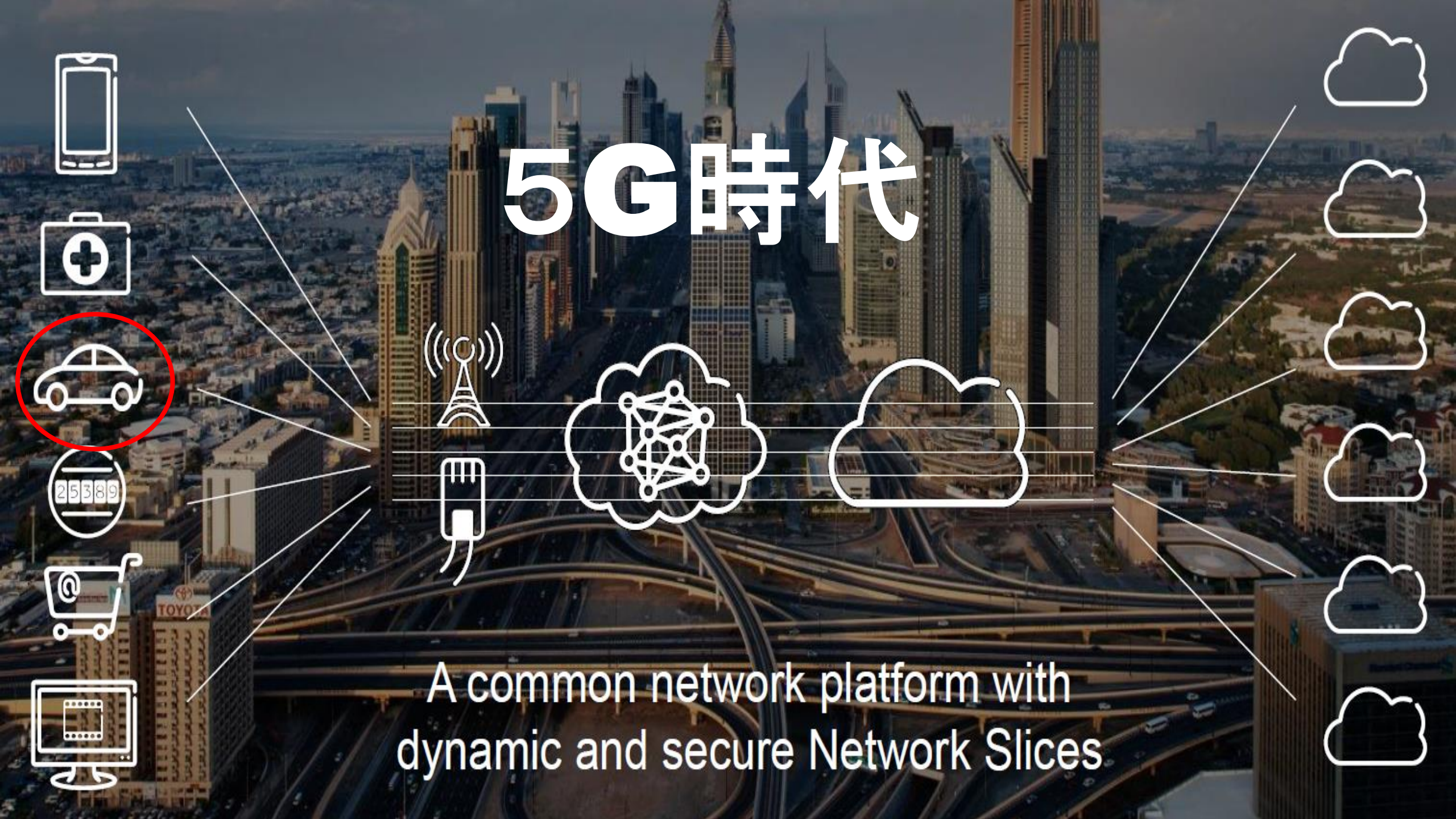
✓これから：

- 調査対象ポートの拡大
- ID/パスワードの増加
- 機器特定能力の強化　　etc. etc...

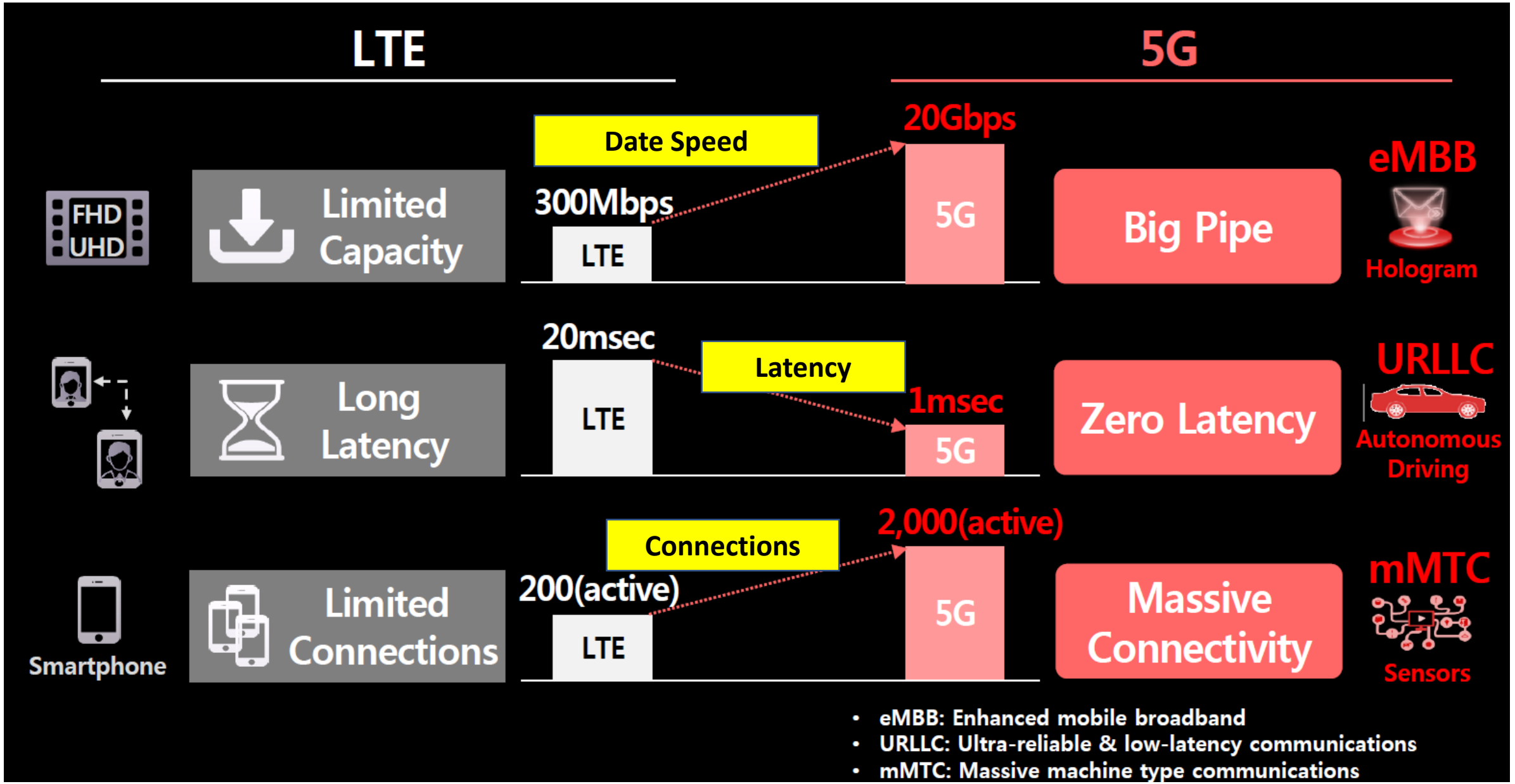
IoT機器調査業務は試行錯誤を重ねつつ
NICT職員が厳粛に進めておりますので
ご理解の程よろしくお願いいたします。

今後のIoTに関連する論点（研究開発含む）

1. 脆弱なIoTに対する具体的な対策（総務省）（研究開発含む）
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）
   管理策としては、27030と親和性あり
3. 国際/国内ガイドラインのさらなる整備（標準化）
4. 検出、分析、パッチ、運用などの自動化の研究開発
5. IoT環境に関わる認証スキームの整備（標準化）
6. 国際的な連携の強化（研究連携を含む）

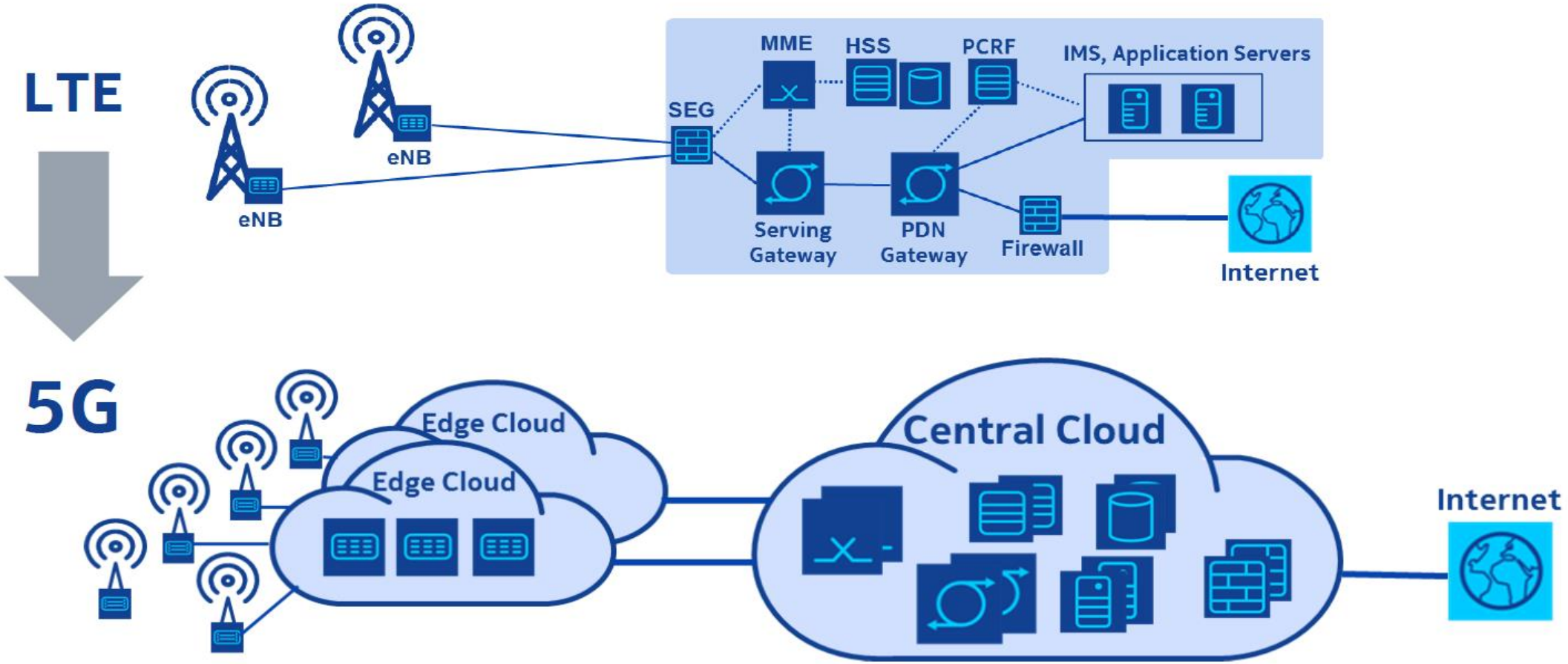

5G時代
A common network platform with
dynamic and secure Network Slices

LTEと比較した５Gの基本的な特徴



LTEから5Gへの新しいネットワークパラダイム

From LTE to 5G: Adopting New Networking Paradigms



NOKIA Bell Labs

想定される5Gの商用サービス（韓国の例）

Enhanced Mobile Broadband

Hyper-Realistic Media

All Wireless

Mission Critical Services

Connected Car

Remote Control

Massive IoT

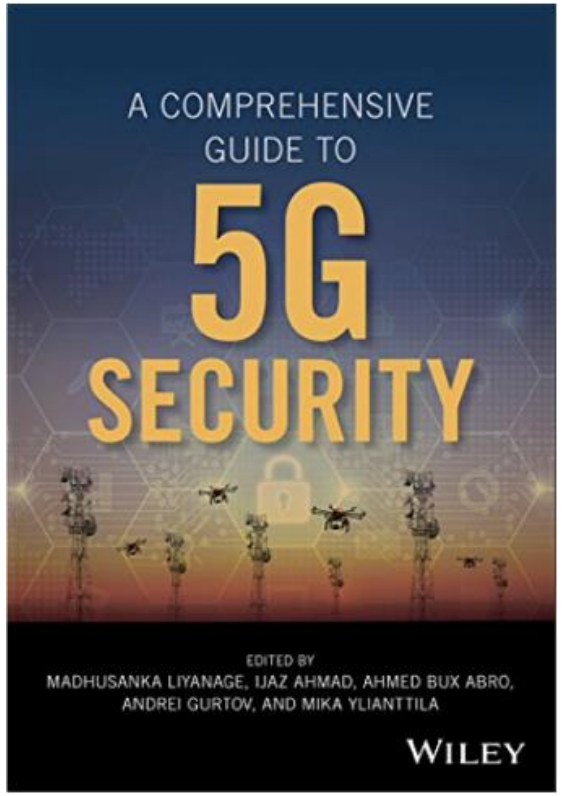
Home IoT

Smart City

Smart Grid

セキュリティの脅威：1Gから5G

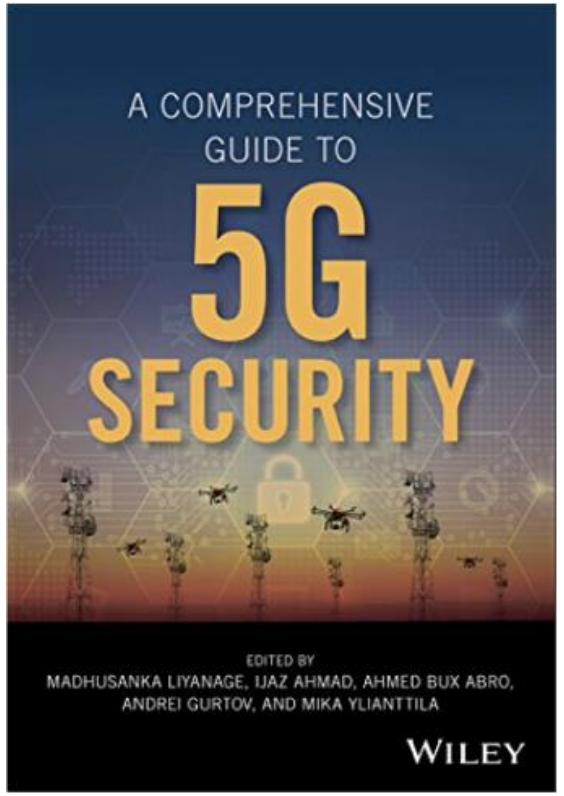
	年	アプリケーション	脅威
1G	1970-1980	音声通話	物理的盗聴, 詐欺
2G	1990-2004	音声通話 + テキスト	スパム, 不正基地局
3G	2004-2010	音声通話 + インターネット	ウイルス, スパイウェア, 不正アプリ
4G	2011-2015	音声通話 + ビデオ + インターネット	モバイルウェア, 標的型攻撃, DDoS攻撃
5G	2020	コネクテッド・ワールド	サイバー戦, スパイ活動, 重要インフラ攻撃



出典: “A Comprehensive Guide to 5G Security,” Wiley, Jan 2018.

5Gセキュリティのトピック

- Part II: 5Gネットワークセキュリティ
  - ✓ Physical Layer Security
  - ✓ 5G-WLAN Security
  - ✓ Safety of 5G Network Infrastructure
  - ✓ Customer Edge Switching: A Security Framework for 5G
  - ✓ Software Defined Security Monitoring in 5G Networks
- Part III: 5Gデバイス＆ユーザセキュリティ
  - ✓ IoT Security
  - ✓ User Privacy, Identity and Trust in 5G
  - ✓ 5G Positioning: Security and Privacy Aspects
- Part IV: 5Gクラウド＆仮想ネットワークセキュリティ
  - ✓ Mobile virtual Network Operators (MVNO) Security
  - ✓ NFV and NFV-based Security Services
  - ✓ Cloud and MEC Security
  - ✓ Regulatory Impact on 5G Security and Privacy



出典: “A Comprehensive Guide to 5G Security,” Wiley, Jan 2018.

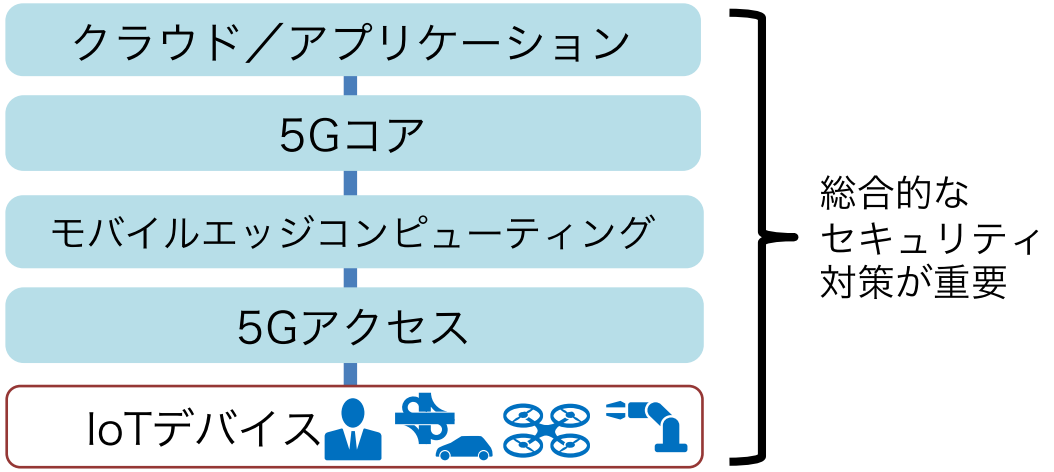
5G セキュリティに向けたNICTのアプローチ

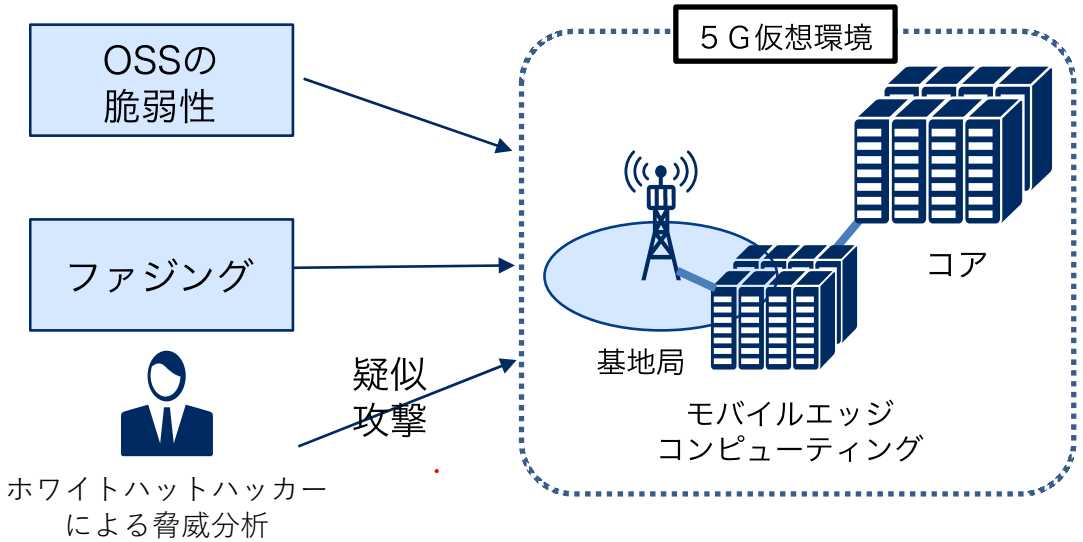
- 5Gは、IoT、クラウド、仮想化技術などを含む、統合されたシステム環境になっていることを考慮する必要がある。
- ５Gセキュリティを遂行するためには、対象となる５Gシステムの「脅威分析」、「リスク識別」、「セキュリティ要件の抽出」、「セキュリティ対策の実施と評価」、及び「セキュリティ機能の見直し」などのプロセスが必要である。
- 上記プロセスを推進するためには、５Gの対象システムの参照モデルの導出が重要となり、その検討が先だって重要となる。
- これらのプロセスにおいては、３GPPやGSMAなどの活動の動向を注視する必要がある。

国内における5Gセキュリティの検討

- 総務省直轄プロジェクト（2020年1月～）
  - ✓５Ｇネットワークにおける
    セキュリティ確保に向けた調査・検討
  - ✓KDDI, NTTドコモ、 NEC、 NICT
- 5Gセキュリティ 動向調査
- 5Gセキュリティ リスク分析
- 5Gセキュリティ 検証環境構築
- 5Gセキュリティ 脆弱性調査/脅威分析
- 5Gセキュリティ ガイドライン β 版

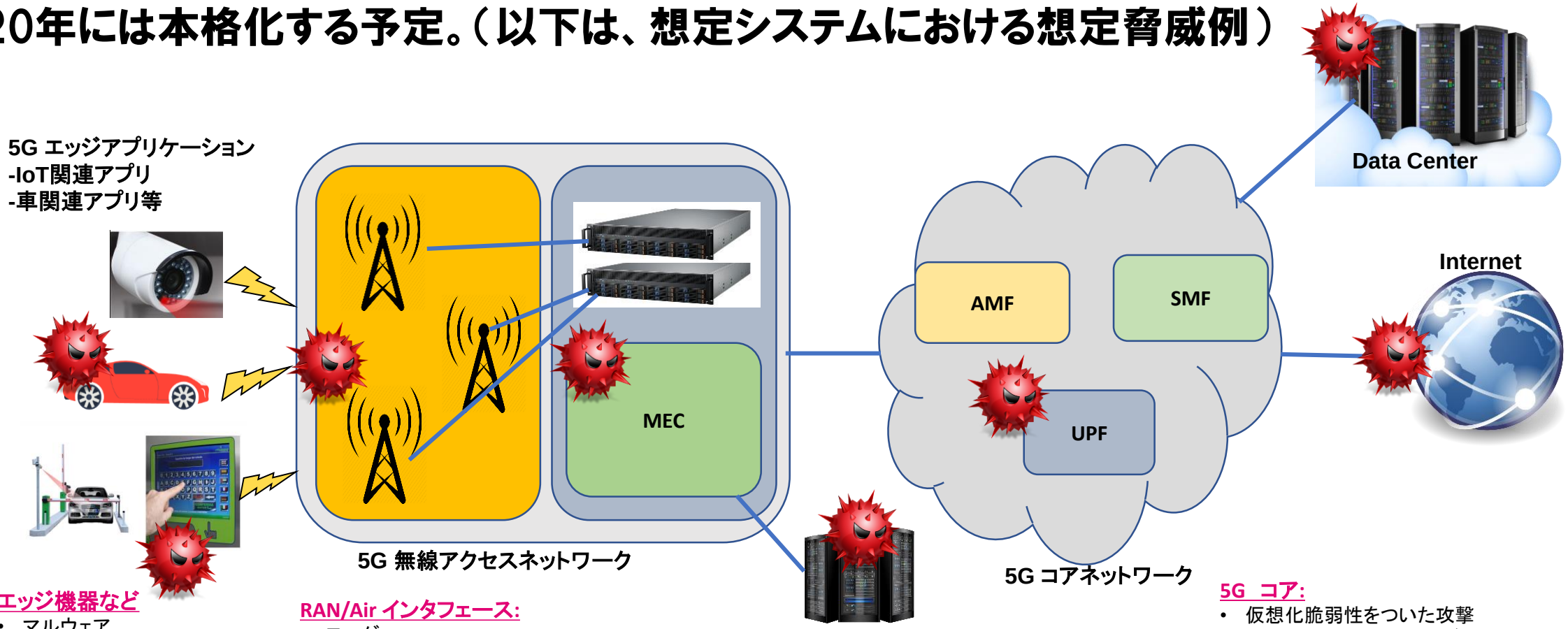
<5Gネットワークのイメージ>





5G セキュリティに向けた試み

NICTは、5Gシステムに内在する脆弱性や弱点を評価・解析するための活動を開始しており、2020年には本格化する予定。（以下は、想定システムにおける想定脅威例）



エッジ機器など
- マルウェア
- ダウングレード攻撃
- 中間者攻撃
- DDoS/DoS 攻撃
- サプライチェーンリスク
- Bluetooth/NFC/Wi-Fi
- ソフト/ファームへの攻撃
- 物理攻撃など

RAN/Air インタフェース:
- ローグ gNB
- 中間者攻撃
- パッシブ CP/UP スニーフィング
- ジャミング攻撃 (DoS 攻撃)
- 非認証帯域利用
- 物理攻撃など

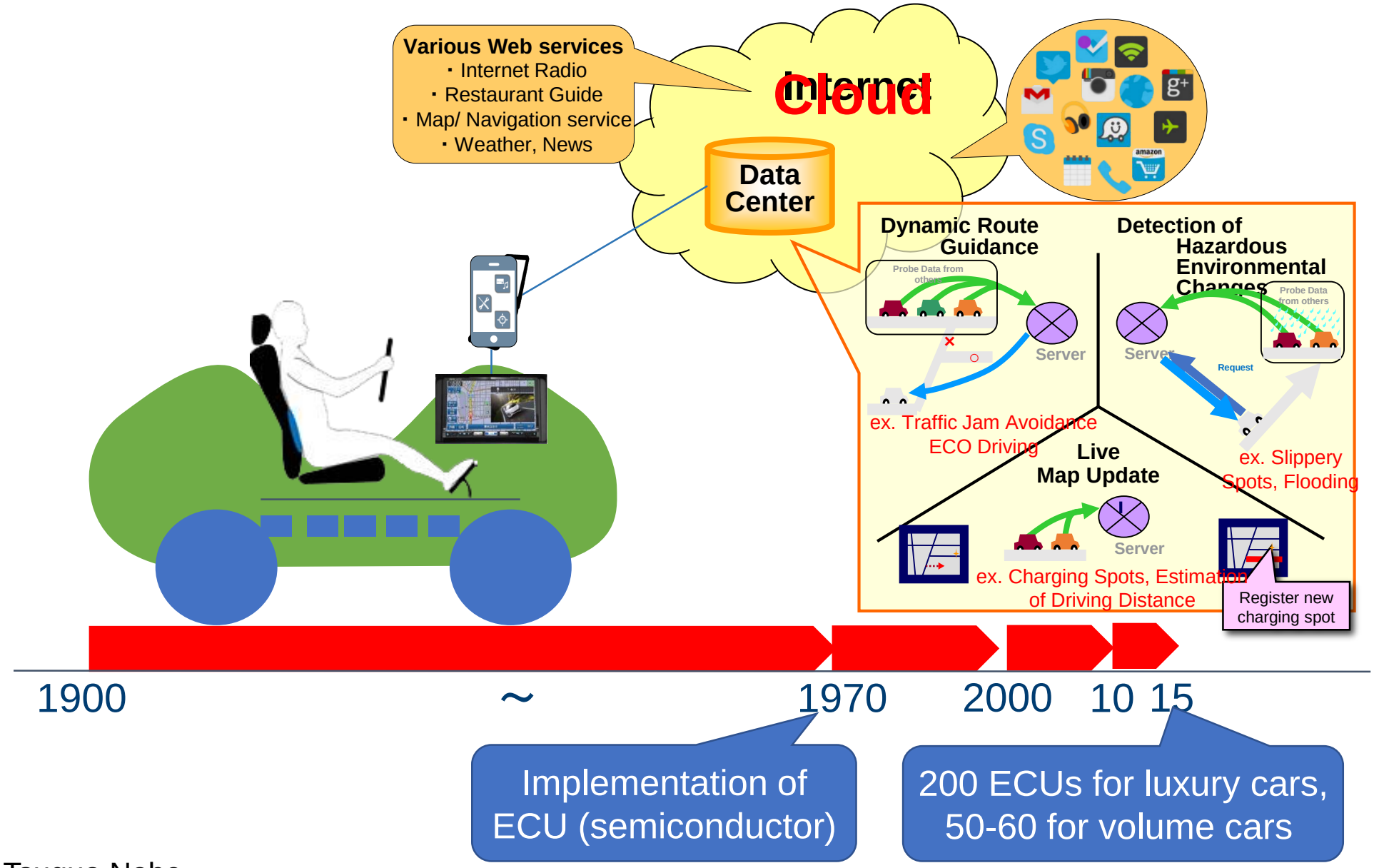
バックフォール等の通信:
- CP/UPスニーフィング
- 中間者攻撃
- MEC DoS
- ジャミング攻撃
- 物理攻撃など

ネットワークスライス/MEC:
- DDoS/DoS 攻撃
- OS/Software のハッキング
- 仮想化脆弱性をついた攻撃
- アプリケーション脆弱性をついた攻撃
- オーケストレーション　攻撃
- 物理攻撃など

5G　コア:
- 仮想化脆弱性をついた攻撃
- OS/Software のハッキング
- アプリケーション脆弱性をついた攻撃
- オーケストレーション　攻撃
- 不正メッセージフローによる攻撃
- ローミングの弱点を使った攻撃
- DDoS/DoS 攻撃
- API 脆弱性を突いた攻撃　など

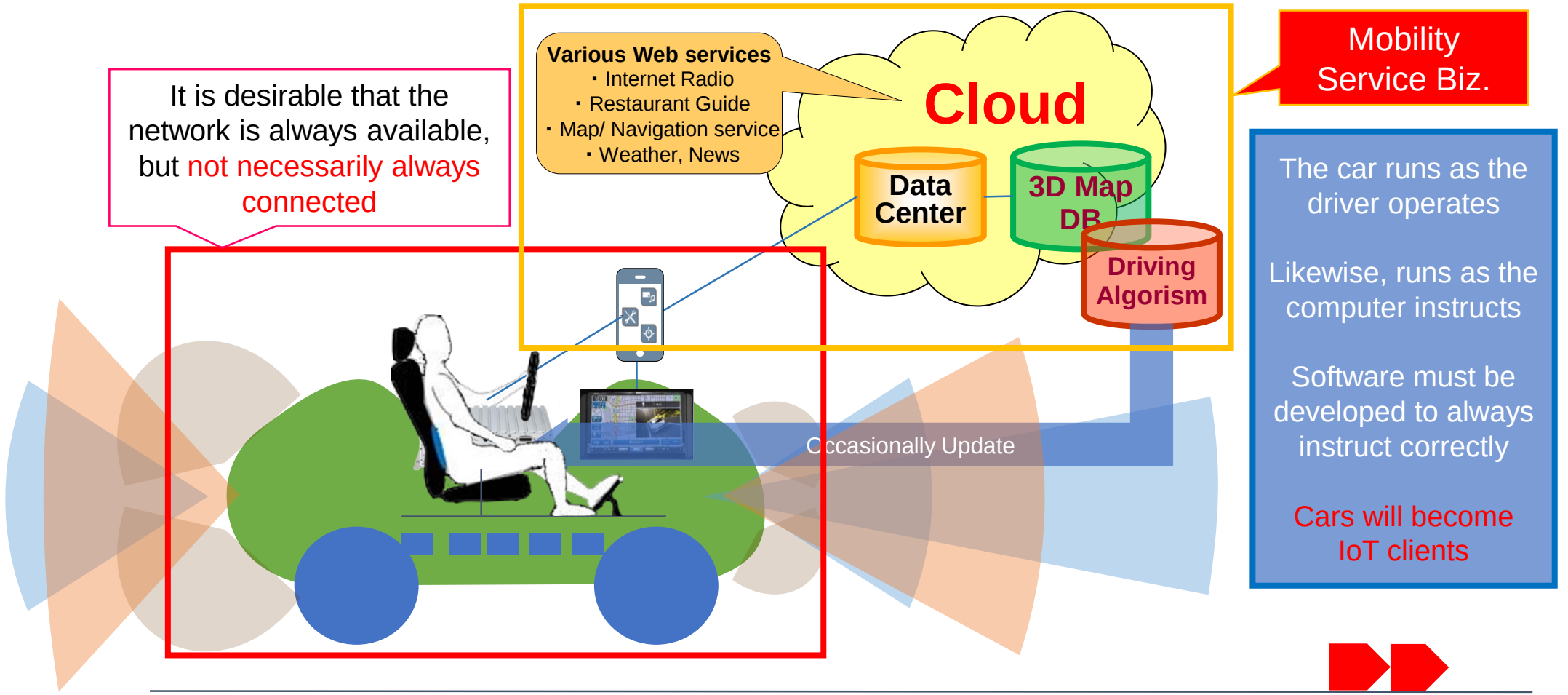
繋がる車の世界では・・・
（Connected Car）

Relation between Cars and ICT (Past, present and future)



Slide from Prof. Tsuguo Nobe

Relation between Cars and ICT (Past, present and future)

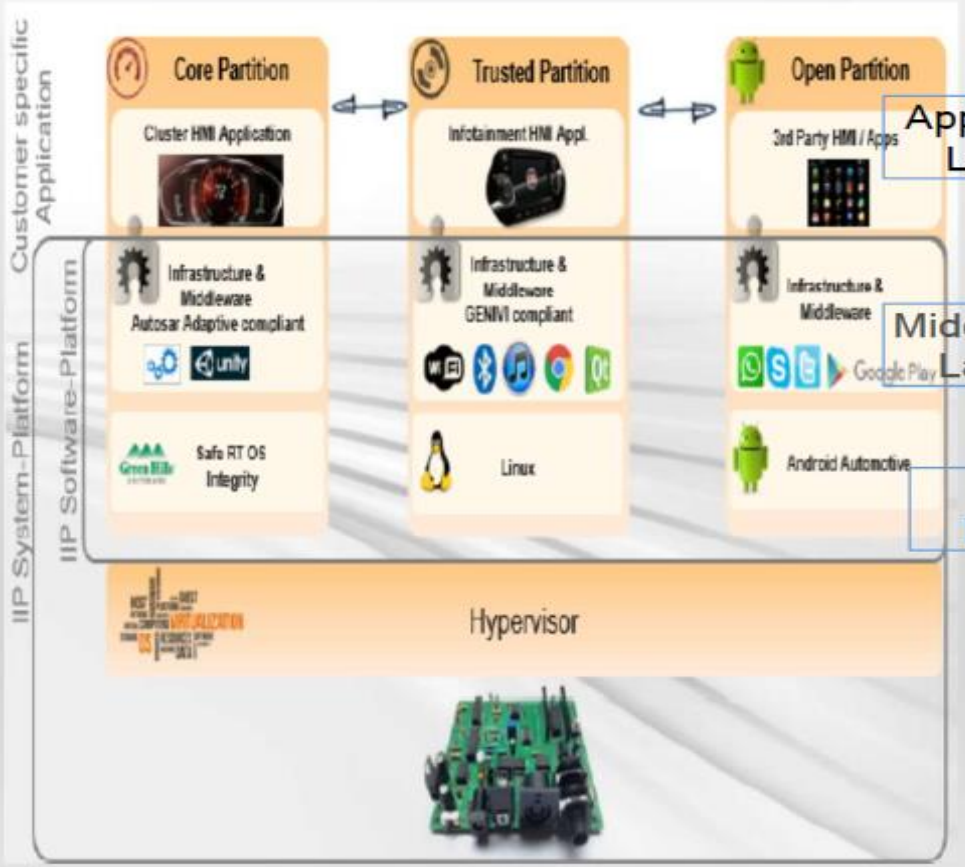


Slide from Prof. Tsuguo Nobe

車内がクラウドのようなシステム環境に

Hypervisor:

Several different Operating Systems is run on same Hardware, the communication between different systems sharing same data base



Application Layers

Middleware Layers

OS Layers

User Experience

Applications (UI)	Menu Screen, Navigation Screen, Media Screen, Call Screen, Popup, Soft Buttons, …
Application Framework	Qt, Java script, HTML5, Flash Air, X11, Win32
Application Services	Tuner, Navigation Core, Media Player, Telematics, Phone, Vehicle Controls, Voice Recognition, Software Update, …
Functional Elements	Network manager, Audio manager, Video manager, Microphone manager, Bluetooth manager, Wi-Fi manager, …
Device Drivers	I^2C, I^2S, UART, USB, LVDS, CVBS, CAN, LIN, Wi-Fi, Bluetooth,Ethernet, …
Operating System & Kernel	Linux, Android, QNX, Windows Embedded, …

Hardware

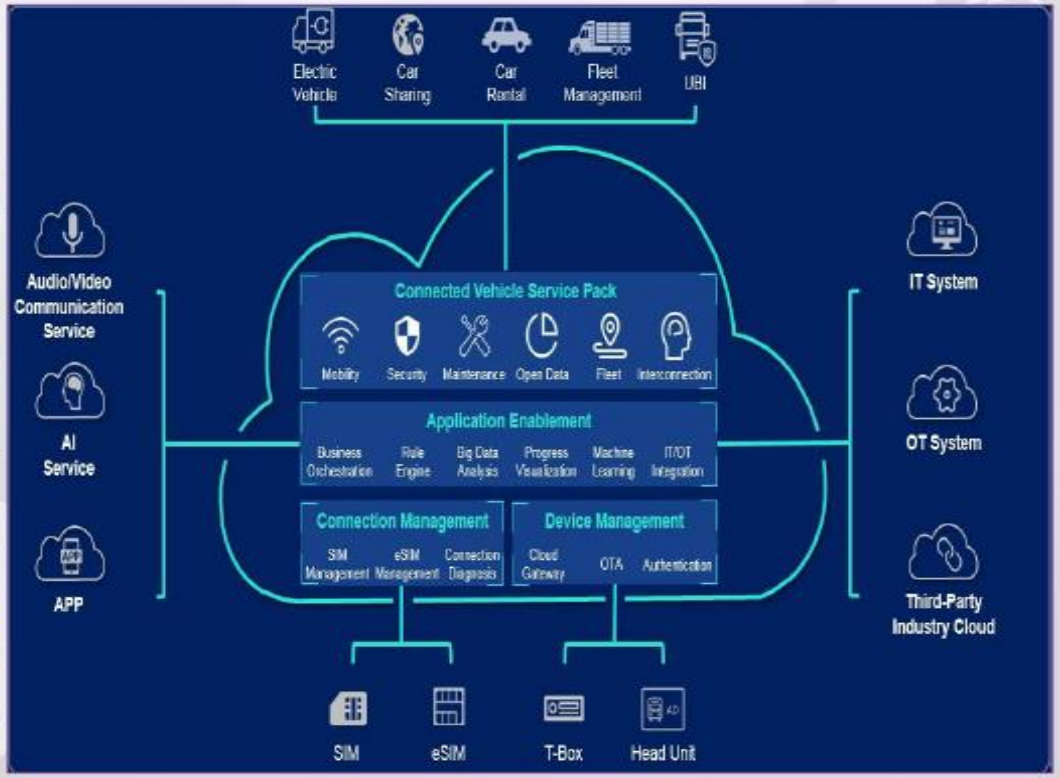
インテリジェントマルチメディアサービス

7. Intelligent Multimedia services

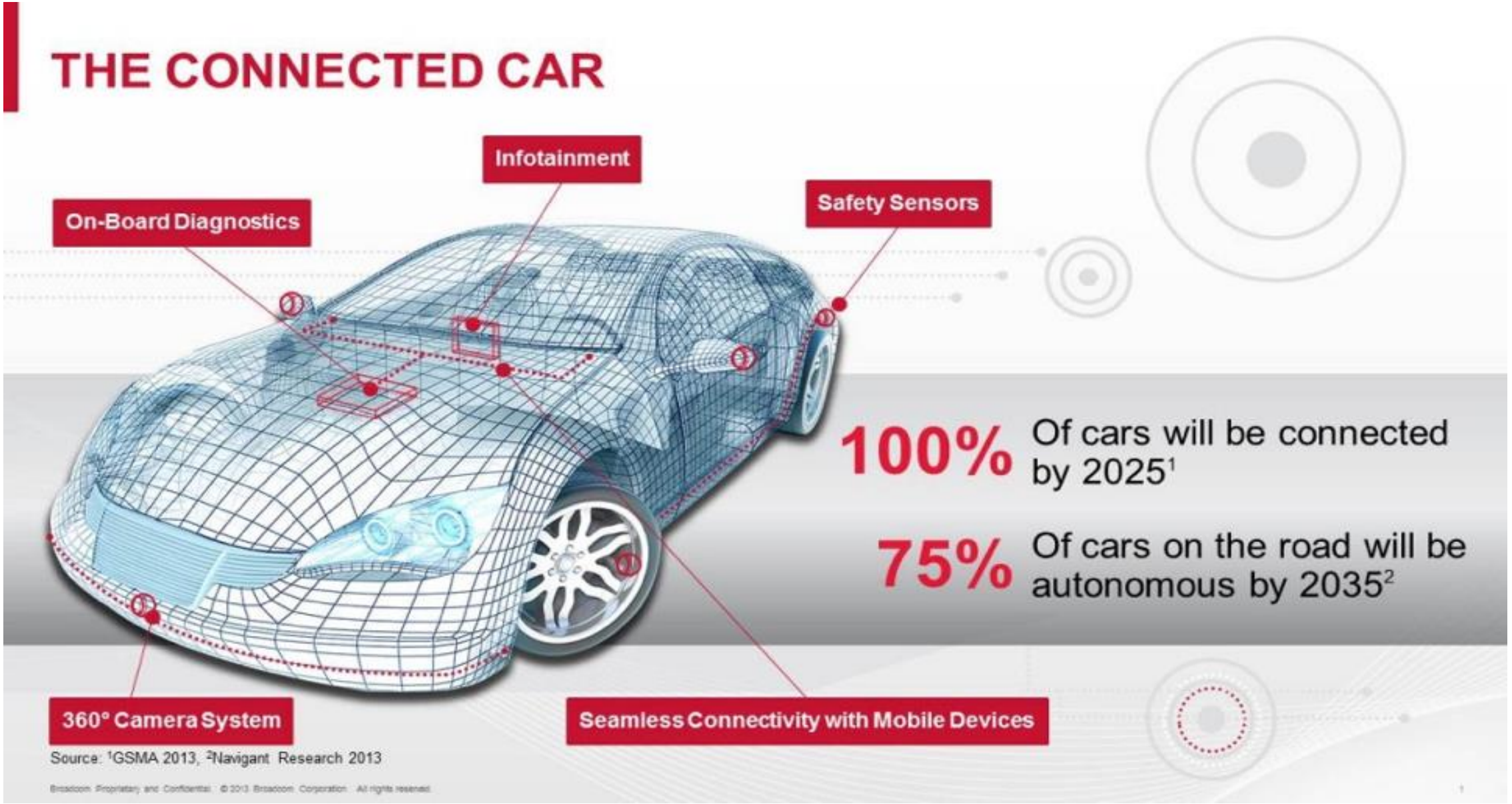
Artificial Intelligence and Machine learnings are integral part of VMS design.

加えて、インテリジェントな接続性を具備

8. Intelligent Connectivity

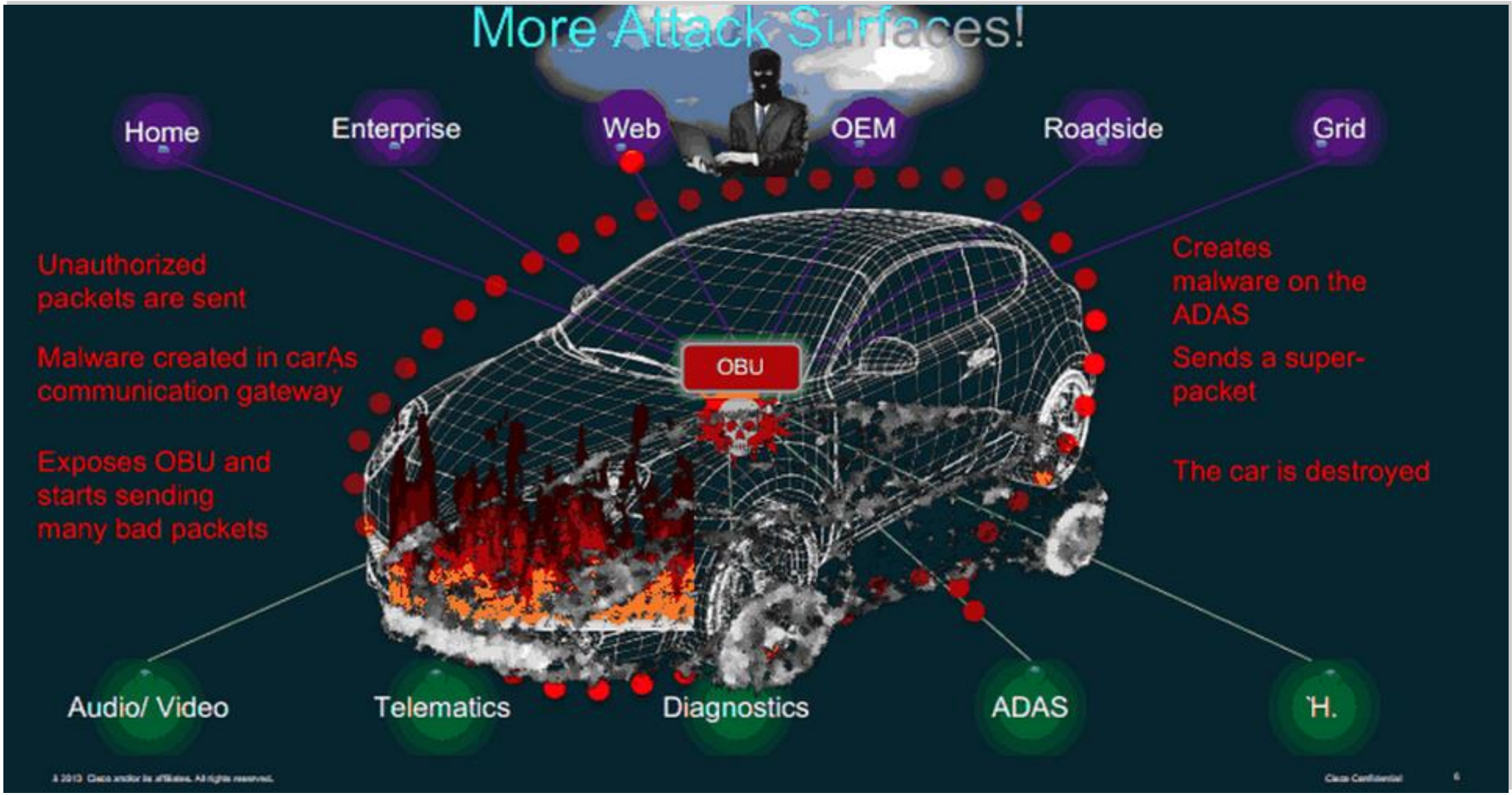


議論の中心に “Connected Car”がある。



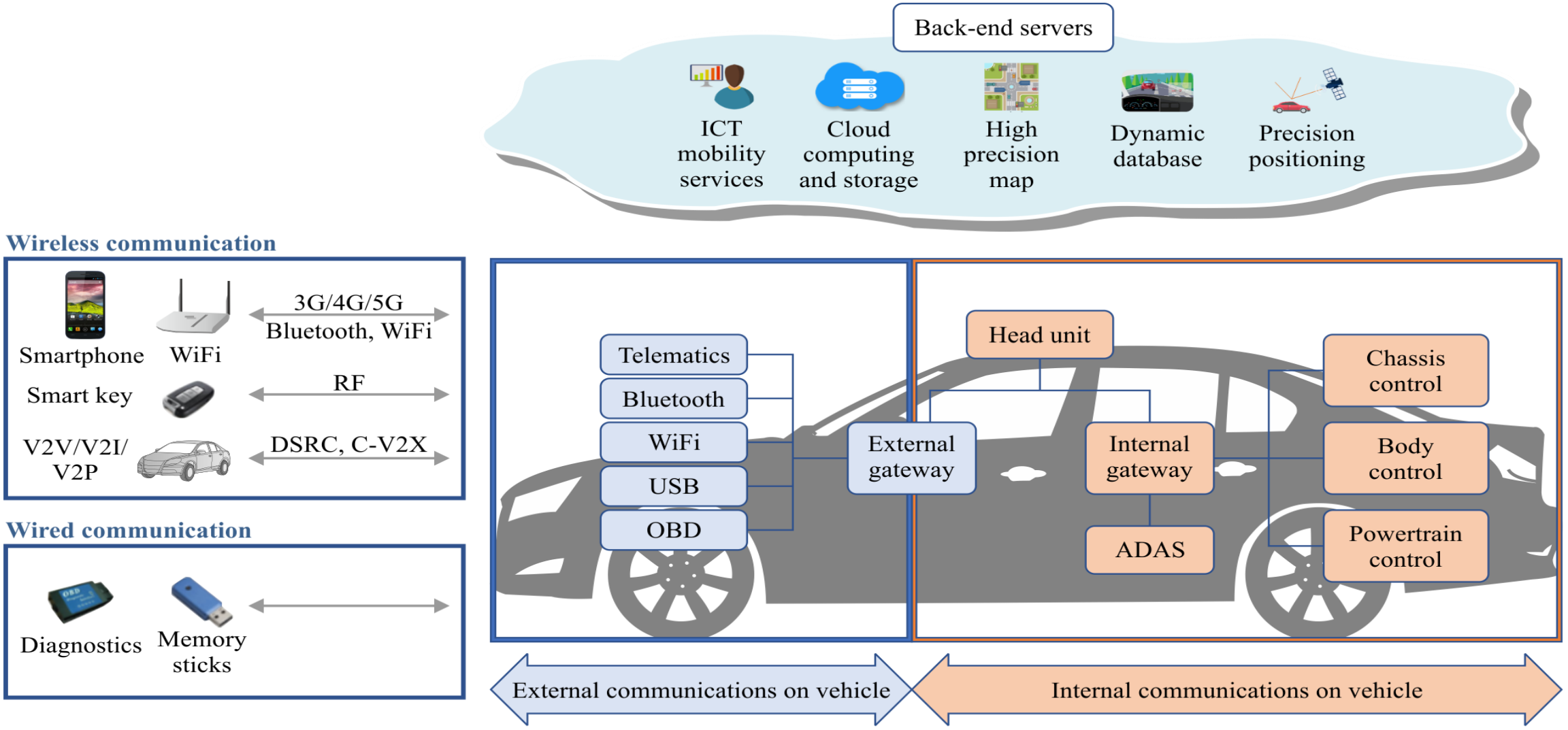
http://johndayautomotivelectronics.com/top-five-technologies-enabling-the-connected-car/

増え続ける攻撃インターフェース



http://gigaom.com/2013/08/06/ciscos-remedy-for-connected-car-security-treat-the-car-like-an-enterprise/

繋がる車の環境（エコシステム）



X.1371(19)_FII.1

想定される繋がる車への脅威

繋がる車、エコシステムへの脅威

1. バックエンドシステムの脅威
2. 通信チャネルから来る車への脅威
3. アップデータ手続きから来る車への脅威
4. 意図しない人の行動から来る車への脅威
5. 外部接続性や実際の接続から来る車への脅威

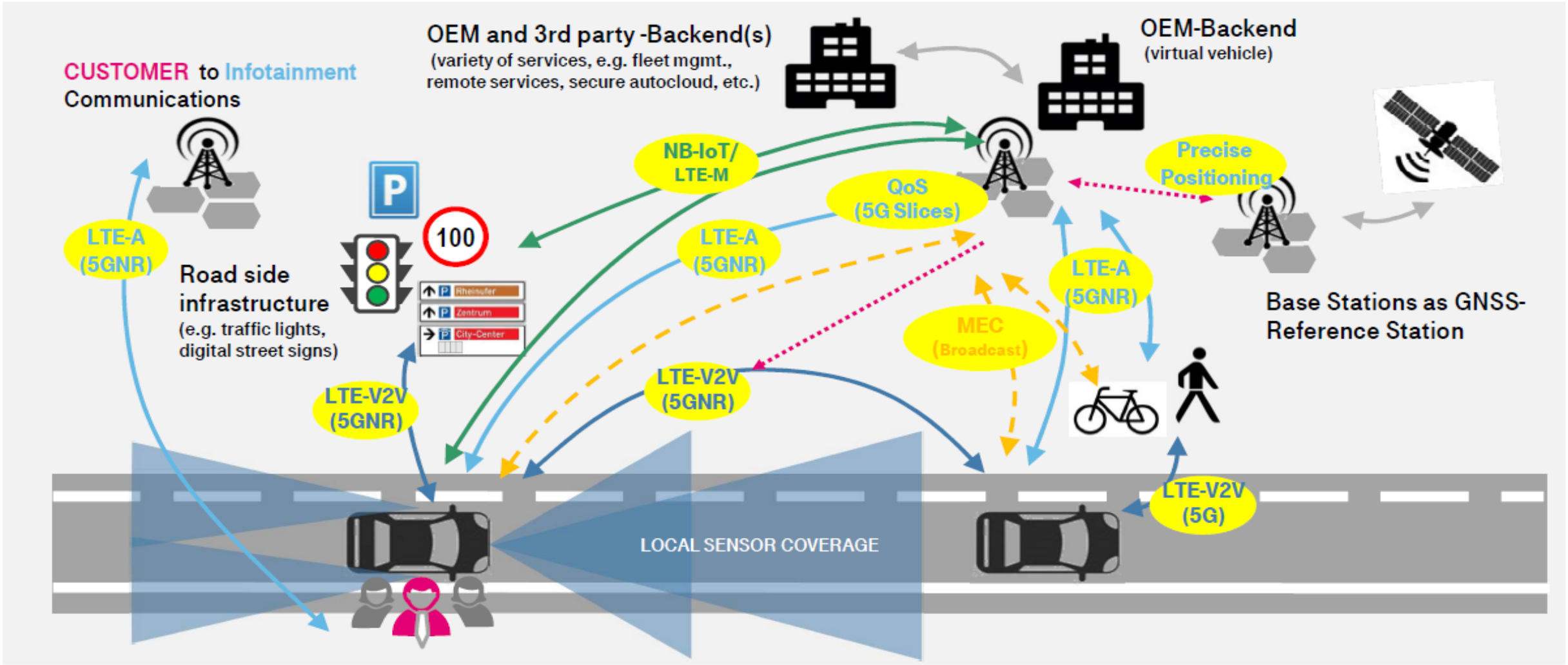
脅威と関連する潜在的な情報

1. 攻撃の潜在的標的化、車への攻撃のモティベーション
2. 完全に防御ができていない部分にある潜在的な脆弱性

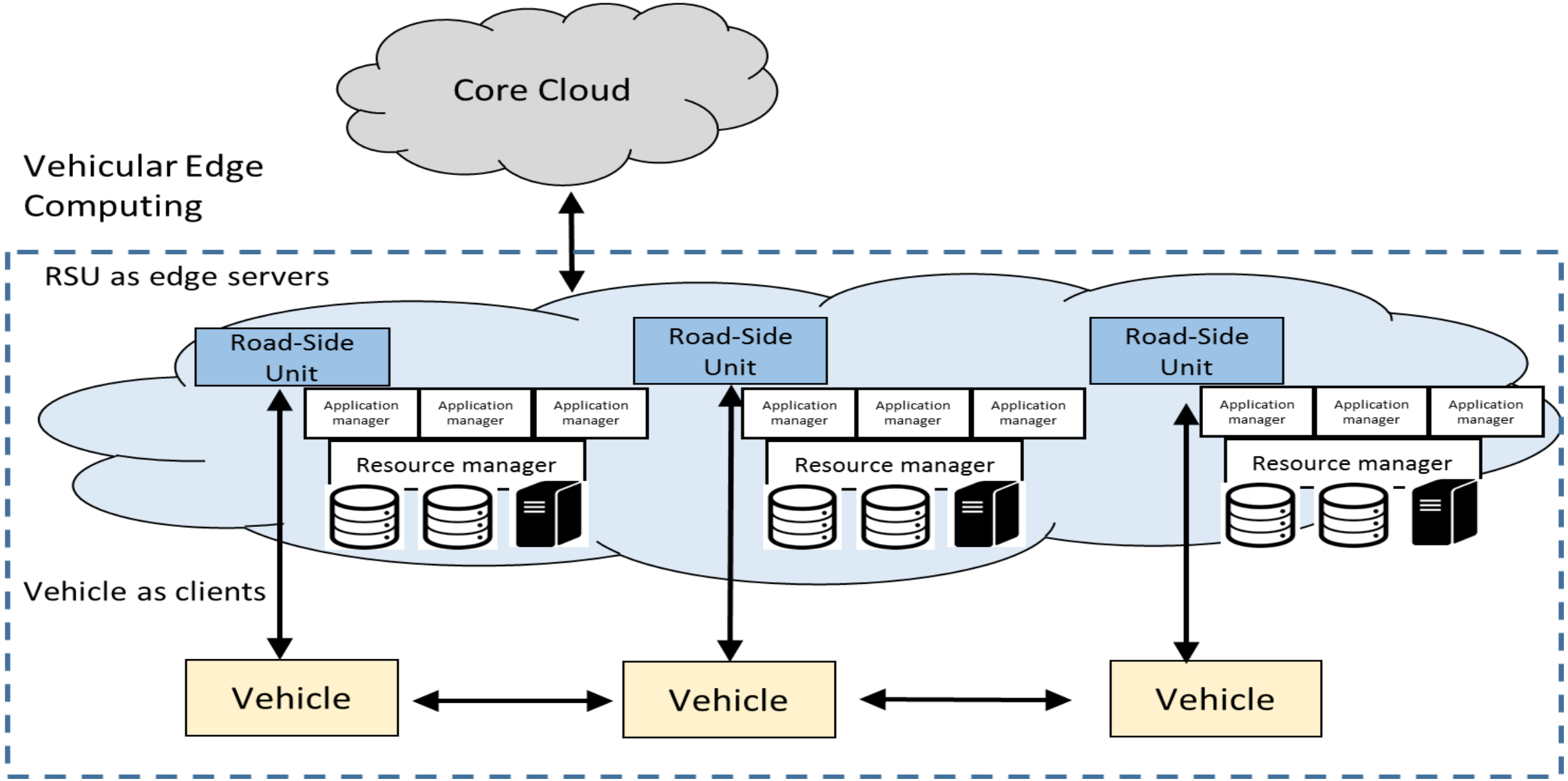
UNECE WP29 Cybersecurity Recommendation, X.1371より抜粋

車では５G無線環境の活用を想定！

EXTENDED AUTOMOTIVE CELLULAR CONNECTIVITY LANDSCAPE



5Gを想定した、エッジコンピューティングによる繋がる車



ITU-T X.itssec-5 ドラフトより抜粋

事例（国家主導プロジェクト）杭州ETシティブレイン

https://jp.alibabacloud.com/solutions/et/city

ET City Brain の革新的なプラクティス

＜事故や渋滞の検出とスマートな対応＞

- コミュニティと公共の安全
- 交通渋滞と信号制御
- 公共交通機関と配車
- 事故や渋滞の検出とスマートな対応

＜効果＞

より多くの事故や渋滞をインテリジェントに検出し、平均処理時間を削減

＜実装方法＞

ビデオ映像から交通事故や渋滞を認識することで、ET City Brain はインターネットデータとアラームデータを統合し、都市全体の交通事故を即座に包括的に把握します。また、スマートな配車テクノロジを使用し、警察、消防、救急、その他の車両に対して統合的な配車指令を実行します。さらに、緊急対応車両が緊急現場に向けて優先的に通行できるよう、信号の調整も行います。

City Event Detection and Analysis

2017-12-15 15:40:32

Event Detection

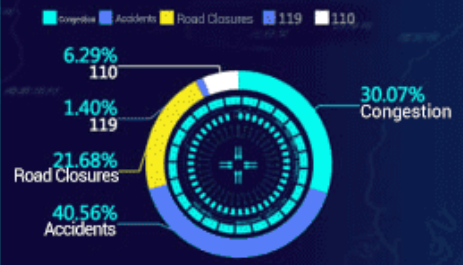
Daily Alerts

9,832

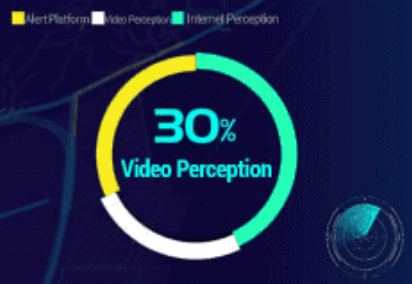
Total Videos

2,458

Event Type Distribution



Sensor Distribution



Event Processing

Total Responses	Average Response Time	Priority Passes
176	58 sec	08

Police Vehicles	Ambulances	Fire Trucks
87	32	19

Event Alerts

Time	Location	Event Type
2017-09-24 09:35:51.051	Fengqing Ave and Jianshe 4th Rd intersection	122
2017-09-13 19:32:12.012	Gualiguanghua Rd, in front of the stadium	122
2017-09-21 22:31:33.033	Billboard fire outside of Dangshan Baodao Glasses	119
2017-09-23 12:54:27.027	Hornets nest in external AC unit, apt 1501, building 4, Jiajing Gardens	119
2017-09-26 15:50:46.046	Hornets nest, Taihehua Gardens, Rose Court, building 7, unit 1, apt 402	119
2017-09-29 08:13:00.000	Accident, Nanzhuangdou Hub, westbound	AutoNavi user

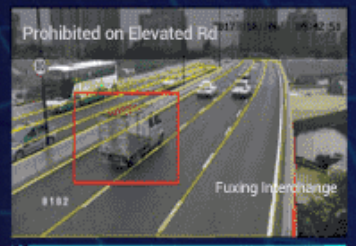
Current Event

Event Time: 2017-10-06 09:43:00.000

Event Location: Fuxing Interchange

Processing Status: Dispatched

Sensor: Video Recognition



Vehicle Dispatch

Plate No.	Vehicle Type	ETA
1	Ambulance	8m22s
2	Police Car	5m39s
3	Ambulance	15m3s
4	Police Car	15m15s
5	Fire Truck	20m34s
1	Ambulance	8m22s
2	Police Car	5m39s
3	Ambulance	15m3s

Ambulance Green Light Priority Example

（ETシティブレイン）コミュニティと公共の安全

- 効果:
  セキュリティと緊急対応時間を効率化し、プロアクティブな公安や安全対策を実現
- 実装方法:
  ビデオ解析テクノロジを使用して都市全体をインデックス化。また、ビデオ認識アルゴリズムにより、当局は公共の安全とセキュリティ確保のための予防的措置が取れるようにする。

コネクテッドカーの現状とNICTの方向

- **将来の自動車業界に対し、ICTは多大な価値を与えることになる。**
  - Deep Learningの車への応用により、自動運転（レベル４）は2020年～2022年には商用化されていくものと期待。，
- **米国、欧州などは、「繋がる車」、「自動化された車」、「車のシェア及び極端に電子化」を目指した流れに向かっている。**
  - 他輸送サービスとの融合による、マルチモーダル化の推進も想定
- **自動車関連のビジネスは、クラウド/IoTに基づくサービスに移行していく傾向が高く、そのため、多くのIT企業へのビジネスチャンスが広がっている。**
- **NICTとしては、以下の視点で研究を推進中**
  - 高度化された車を対象とした脆弱性検証（CAN、インフォテインメント系、センサ系、デバイスローレイヤ等）
  - 車での活用を想定した「軽量暗号化」の研究
  - 検証結果などをまとめた車のセキュリティ標準化への貢献

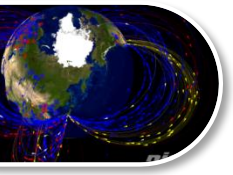
繋がる車のためのセキュリティ対策研究

1. ソフトウェア/ファームウェアへの安全なリモートパッチのための研究(国際標準化や国内OEMでの審議が活性化中)
2. 高度化された車を対象とした脆弱性検証(CAN、インフォテインメント系、センサ系、デバイスローレイヤ等)に関する研究
3. 車への侵入検知システムなどの対策研究
4. エッジコンピューティング等の活用による新たなサービスのためのセキュリティ確保の研究
5. 車等の環境において活用が期待される軽量暗号の研究

など

参考として、ISO/SAE 21434 （Road vehicles — Cybersecurity engineering） 等

NICTサイバーセキュリティ研究室の研究相関図



Network Incident analysis Center for Tactical Emergency Response

NICTER

Direct Alert Environment for Darknet And Livenet Unified Security

DAEDALUS

Passive

NICTER Real-network Visual ANAlyzer KAI

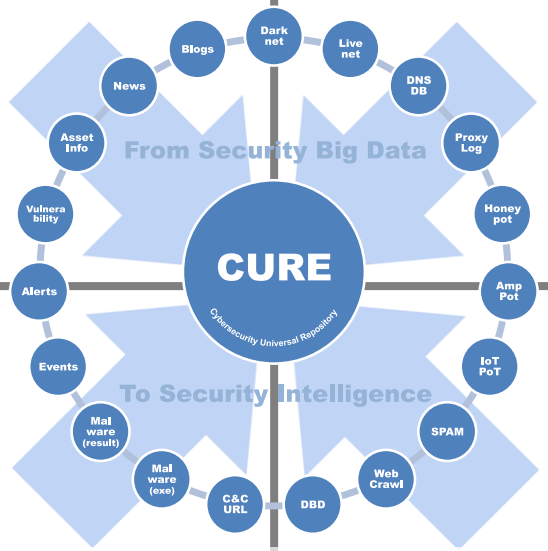
NIRVANA改

NICTER Real-network Visual ANAlyzer KAI-II

NIRVANA改弐

Global (indiscriminate attack)

(targeted attack) Local



Cybersecurity Universal REpository

CURE

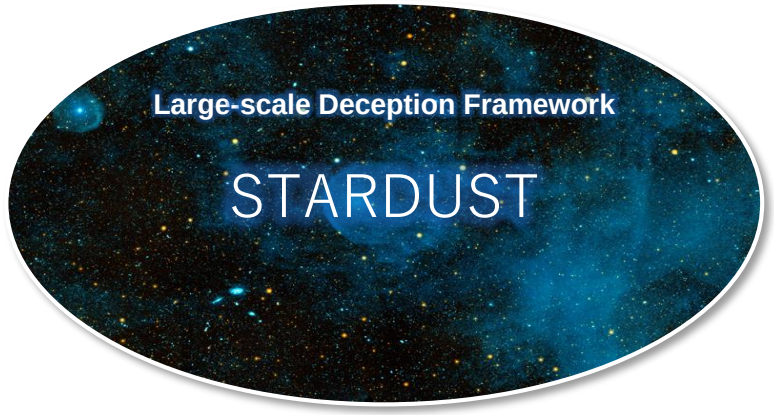
Active

Honeypot for Amplification Attack

AmpPOT#

Honeypot for IoT Malware

IoTPOT#



Collaborative research with Yokohama National Univ. and Saarland Univ.

サイバーセキュリティの研究開発における今後の重点課題

●データドリブンなサイバーセキュリティ研究

- ✓ NICTを日本最大のセキュリティビッグデータの集積地に
- ✓ セキュリティビッグデータからセキュリティインテリジェンスへ

●AI x Cybersecurity

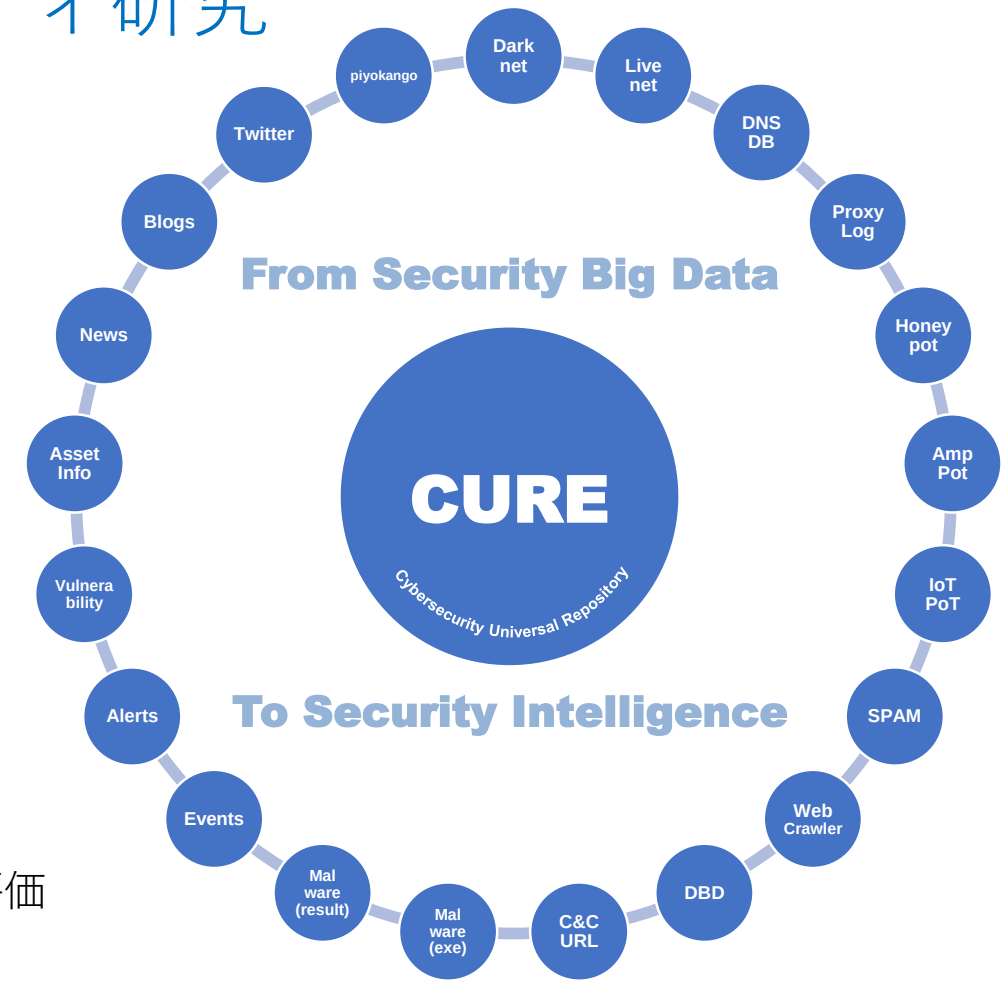
- ✓ 実データに基づくリアルタイム機械学習エンジン開発
- ✓ 機械学習技術を応用したセキュリティオペーレーション高速化

●5Gセキュリティ

- ✓ 5Gネットワークのコア/エッジ/アクセスのセキュリティ検証
- ✓ NICT＋通信キャリア＋機器ベンダーによる検証体制構築

●セキュリティ自給率の向上

- ✓ NICT自身をテストベッドとした国産セキュリティ技術の検証・評価
- ✓ 国産セキュリティ技術を創り・育て・世界へ展開



NICTサイバーセキュリティ研究室の研究相関図（２）

Network Incident analysis Center for Tactical Emergency Response

NICTER

Direct Alert Environment for Darknet And Livenet Unified Security

DAEDALUS

Passive

NICTER Real-network Visual ANAlyzer KAI

NIRVANA改

NICTER Real-network Visual ANAlyzer KAI-II

+ AI & 5G

Global (indiscriminate attack)

(targeted attack) Local

Honeypot for Amplification Attack

AmpPOT#

Honeypot for IoT Malware

IoTPOT#

including Automotive

(Commission Research)

CURE

Active

Collaborative research with Yokohama National Univ. and Saarland Univ.

AIに関連するNICTで注力しているドメイン

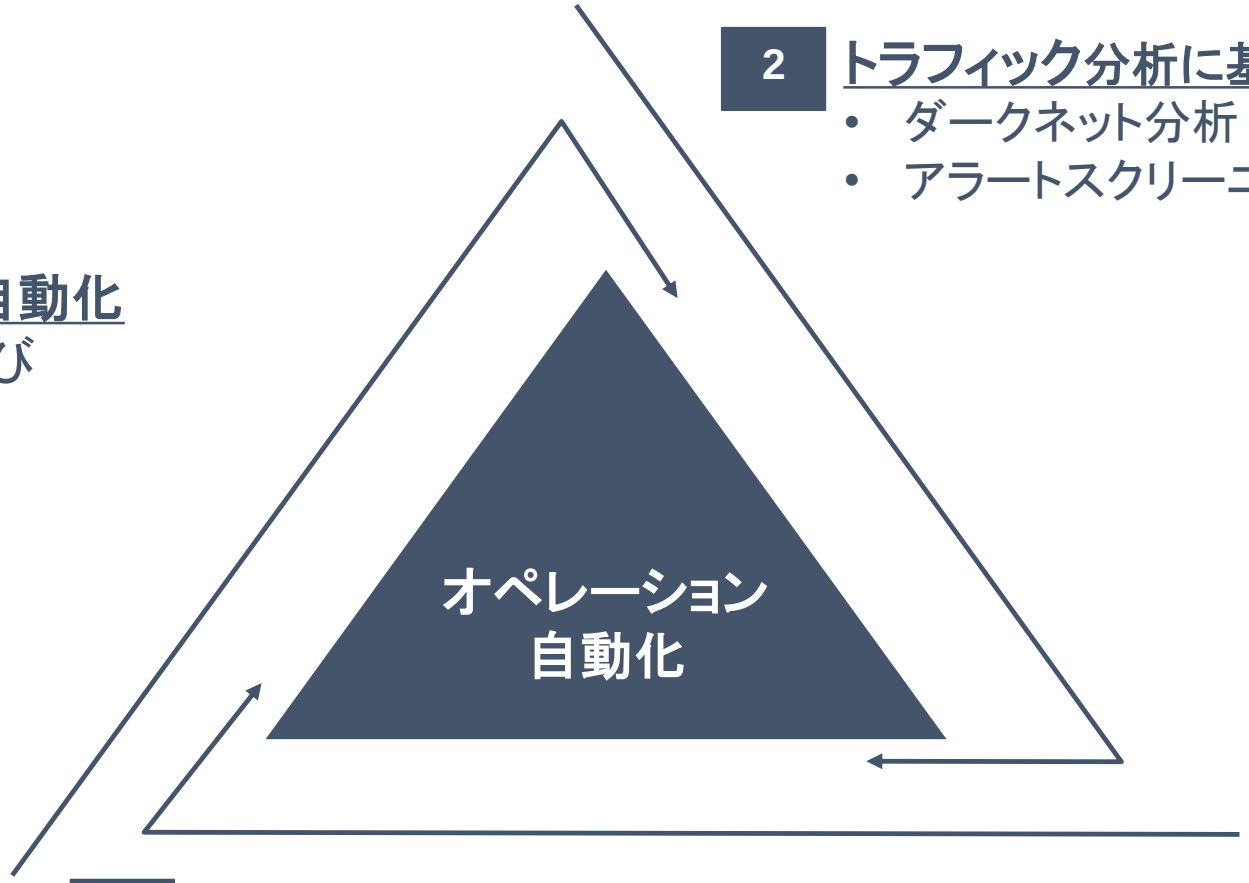
1

マルウェア機能分析自動化

- Androidアプリおよびマーケット分析
- IoTマルウェア分析
- 囮文書分析

2 **トラフィック分析に基づく攻撃の検知・脅威予測**

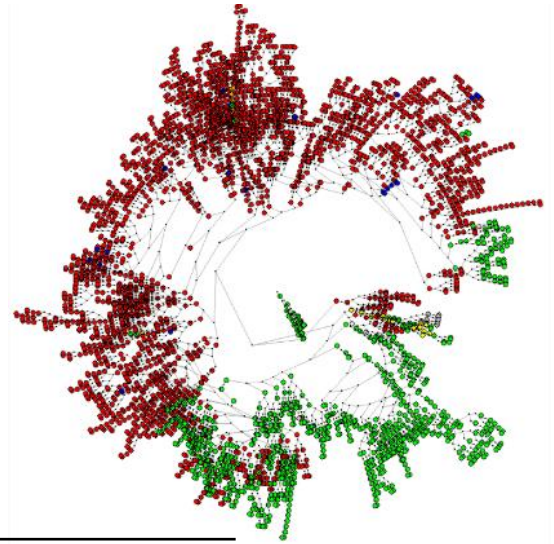
- ダークネット分析
- アラートスクリーニング



3 **インテリジェンス情報の生成・分析**

- 脆弱性の深刻度評価
- 脆弱性情報の分類
- 脅威情報の関連性評価

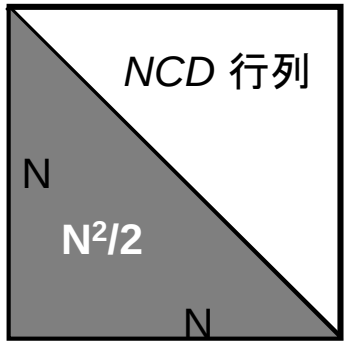
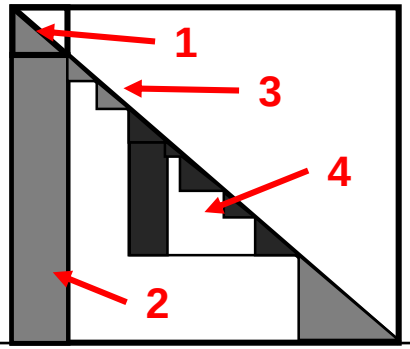
1 事例：IoTマルウェアの系統樹によるマルウェアクラスタリング



目的: 大規模なマルウェアを高速かつ逐次的に効率良く解析すること
- クラスタリング，マルウェア変遷確認，機能の差分抽出などの実施
- 現時点では小規模データセットにて実施

提案アルゴリズム
- マルウェアバイナリコード同士の類似度(距離)を測り，系統樹を作成
  (距離はNCDを、系統樹作成にはneighbor joining methodを、それぞれ活用)
- 特に、全データ間の距離計算を避け、必要最小限のデータ間の計算のみ実施

評価実験
- データセットとしてARMアーキテクチャの4,109検体を活用
  (Bashlite 3,114検体、
  Mirai 919検体、その他76検体)
- 処理時間: 約20～50倍高速化
- 正解率: 約97%　（従来比+2.5%)

	従来アルゴリズム	提案アルゴリズム
イメージ		
処理時間	243.4時間	4.4時間～11.6時間
クラスタリング正解率	94.42%	96.58%～97.62%

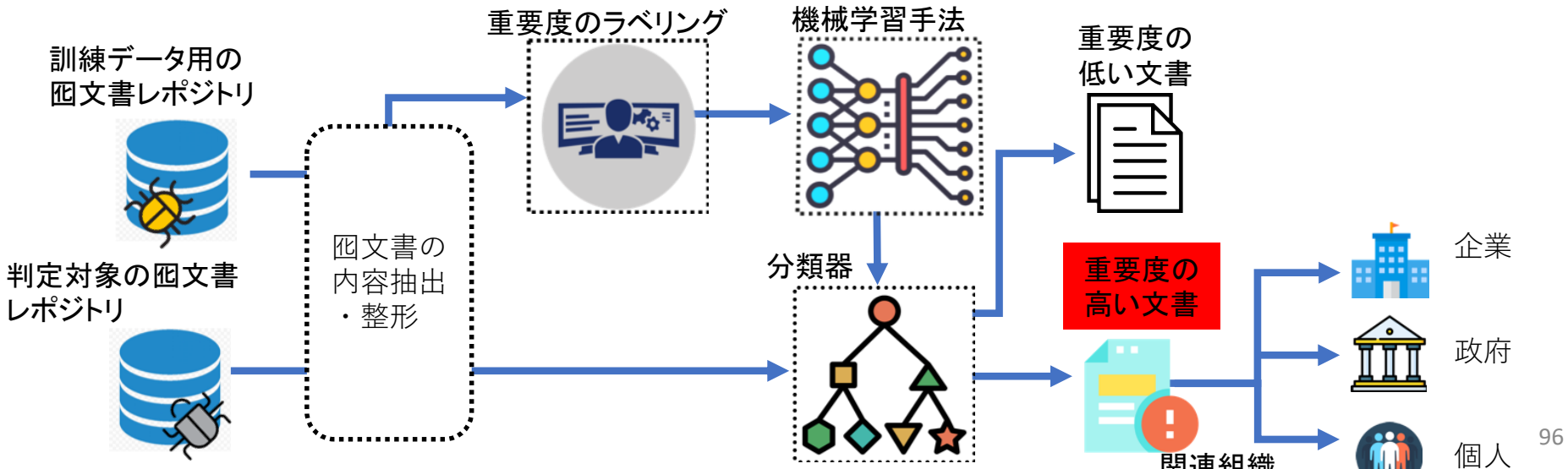
今後の予定
- 大規模クラスタリング
- 逐次処理化
- 性能保証・パラメータ最適化

Source: T.He, et al, "A Fast Algorithm for Constructing Phylogenetic Trees with App. to IoT Malware Clustering," ICONIP, 2019.

1 事例：囮文書分析に基づく標的型攻撃の分析

標的型攻撃の分析技術の研究開発

- 背景
  - ✓ 標的型攻撃の一つに、攻撃対象者に関連する文書（以下、囮文書）に見せかけたマルウェアをメールに添付して送信する攻撃がある。このような囮文書の内容を分析することで、標的型攻撃の早期発見や実態把握、対処をするための手掛りが得られる可能性がある。
- 課題
  - ✓ 不特定多数にむけた囮文書（重要度:低）と特定の個人や組織を狙う囮文書（重要度:高い）があり、重要度の高い囮文書だけ分析対象にしたい
- アプローチ
  - ✓ 囮文書のなかに特定の個人や組織を狙った攻撃の可能性を示唆する特徴がないか調査し、その特徴をもとにAI/機械学習法により重要な囮文書を自動判定する。



囮文書の重要度判定フローと関連組織への通知

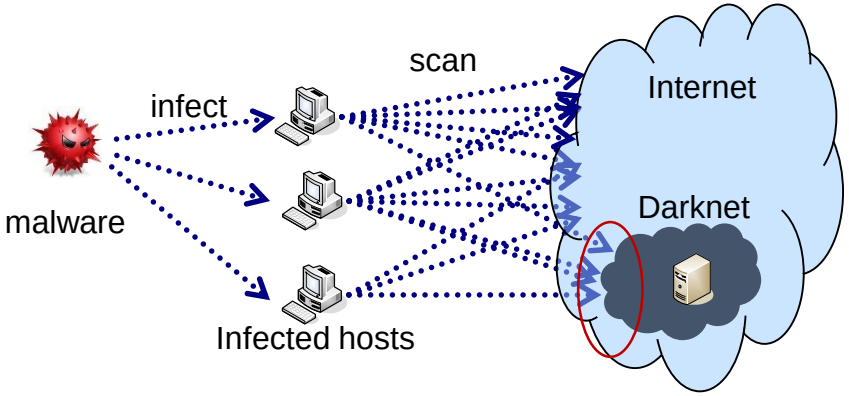
2 事例：マルウェア活動の自動検知に関する研究開発

目的

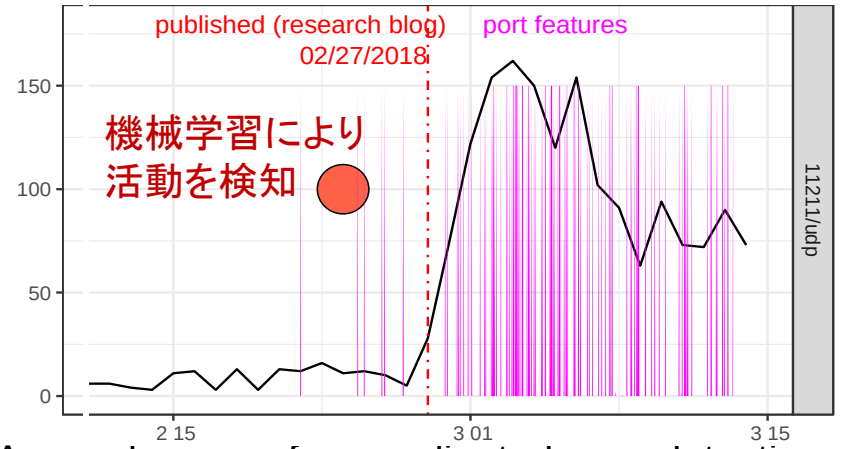
- マルウェアの活動の活性化をいち早く、リアルタイムに検知。特に、人手で検知するのが困難なものを検知したい

アプローチ

- ダークネット空間に到着するパケットの送信元の同期性を教師なし機械学習により分析
- 他の時間帯に比べ同期性の強い時間帯や，その時間帯内で強い同期性を示すホスト群を異常検知し，アラートを発行する.



Scans reach NICT sensors on the darknet



A sample case of a coordinated scan detection
(x: date/time, y: number of sources)

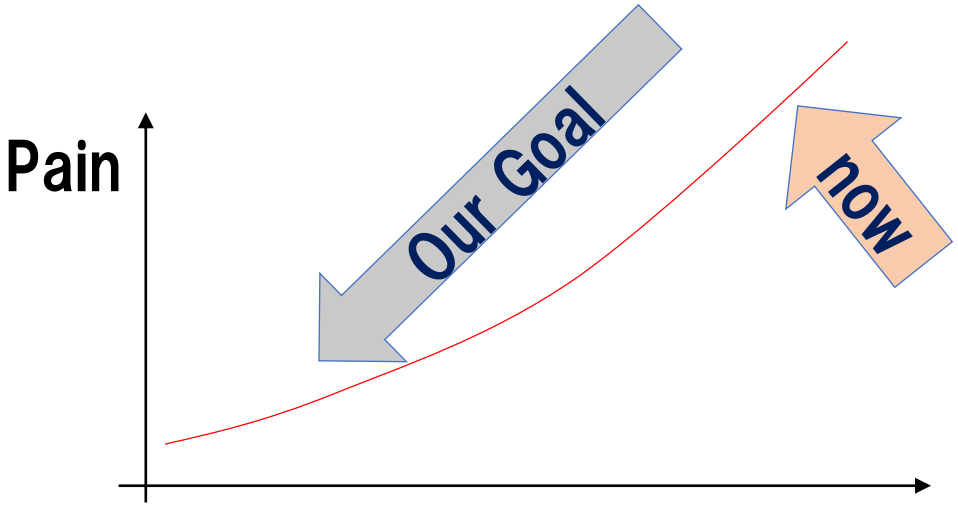
Source: C.Han, et al, "Real-Time Detection of Malware Activities by Analyzing Darknet Traffic Using GLasso," TrustCom, 2019.
H.Kanehara, et. al., "Real-Time Botnet Detection Using Nonnegative Tucker Decomposition," SAC, 2019.

事例：セキュリティオペレータの負荷の軽減

アラート
~ 100,000/day

精査が必要な
アラート
~ 100/day

対処が必要な
アラート
~ 5 /day

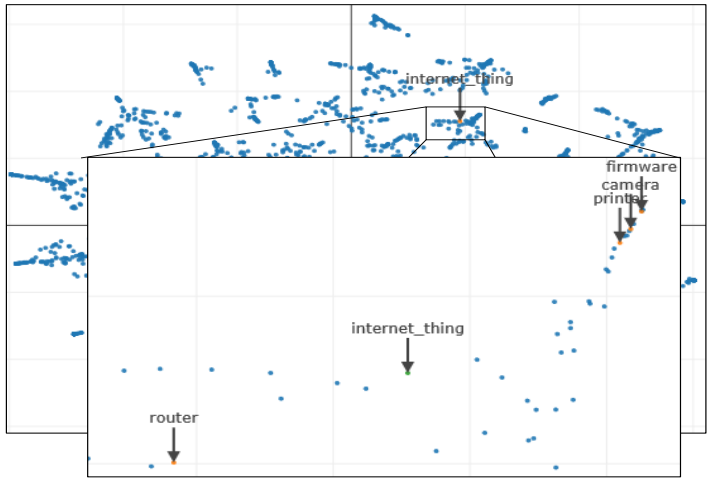


専門家が1日4時間もの時間を費やしているのが現状

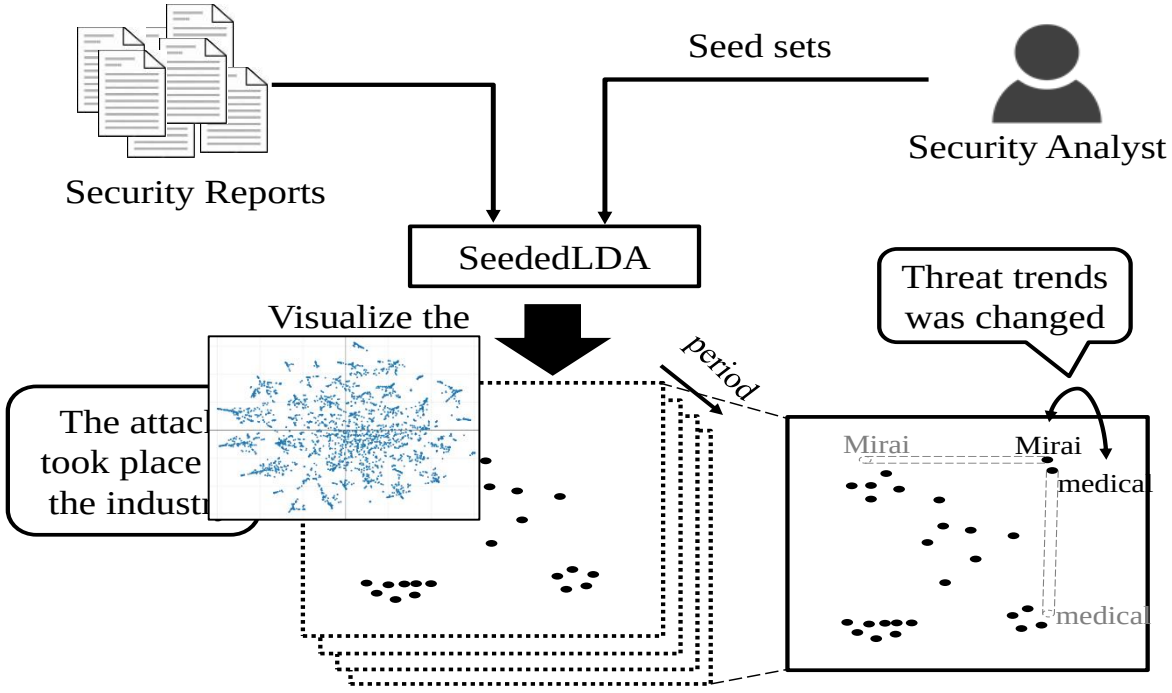
Source: M.Aminanto, et. al., "Combating Threat-Alert Fatigue with Online Anomaly Detection using Isolation Forest," ICONIP, 2019.

事例：セキュリティレポートの自動分類

- 研究背景: 高度化するサイバー攻撃 –セキュリティレポートを用いたインシデント対策–
- 課題: 人手でセキュリティレポートから情報収集・分析する負担が大きい
- アプローチ
  - ✓話題誘導するトピックモデル（SeededLDA）によりセキュリティレポートを学習
  - ✓単語の関係性の可視化から攻撃手法や攻撃傾向を分析する
- 結果
  - ✓出力結果から、以下の傾向を把握可能
    - ➢攻撃手法
    - ➢攻撃傾向の変化



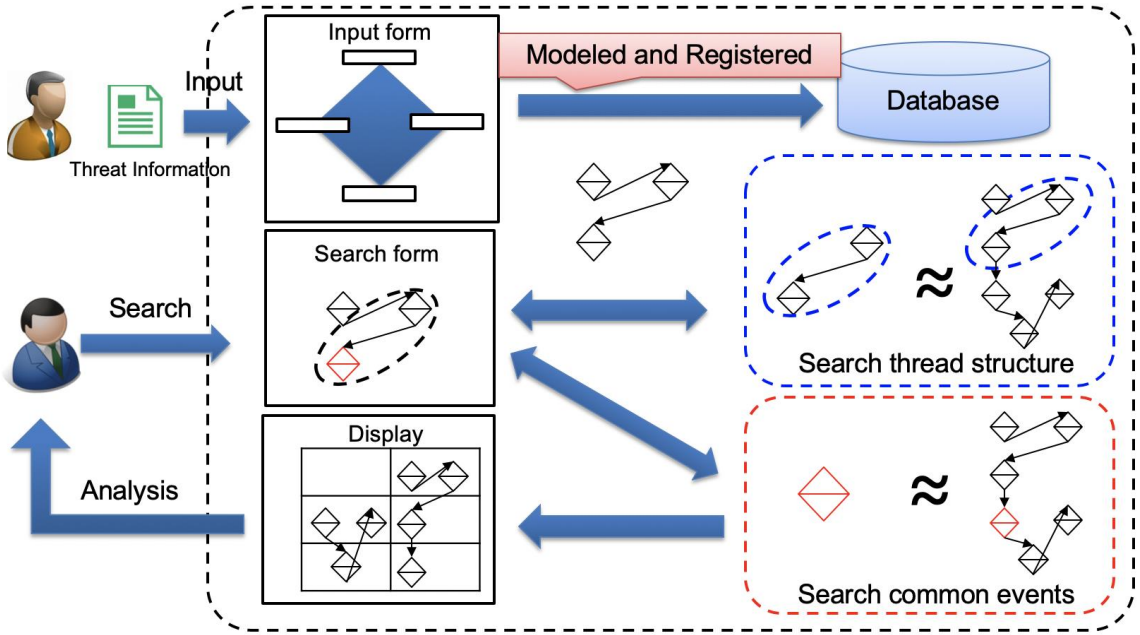
IoT Industryに関する出力結果例



処理の流れ

脅威情報のモデル化を利用した解析システム

- 研究背景: 様々なフォーマットで記述されている脅威情報が日々増加している
- 課題: 一連の攻撃情報を統一された形式で比較することが困難
- アプローチ
  - ✓脅威情報のフォーマットや解析者による入力値の差異を吸収可能なシステムを構築する
  - ✓各脅威情報をダイヤモンドモデルに落とし込むことで、インシデント間を比較可能とする
- 結果
  - ✓モデル化・データベースへの格納・インシデントの比較が可能なシステムを構築した



提案システム

	PA150825	ML160805	Pp161115	Sy121010	Sy130523	SW131212
date	2015/08/25	2016/08/05	2016/11/15	2012/10/10	2013/05/23	2013/12/12
Adversary						
Reconnaissance						
Weaponization						
Delivery	C8		C8, C21,C22 I12 C8 C21	I1 C1 I2 C2	I1 C1 etc. I3 C2	I4 C8 I5 C9
Exploitation			I7	C3	C6	C10 C11
Installation	C14, C15, C16, C17	C17 C20	I13 I14 C23 C17 C24	C4 C5	C7	C7 C12 C13
C2	I7 I8	I9, I10, I11	I15 I16	I2		I6
Action on Objectives	C18 V2		V3, V4, V5	V1		
Victim	EU and North America		EU and North America		Spanish-speaking countries in Latin America	

I1:goo.gl Link,I2:a URL on Hotfile.com,I3:a URL on 4shared.com,I4:auto-notify@ups.com,I5:auto@ups.com,
I6:feed404.dnsquery.com (Host),I7:securevpnalam.net,I8:hsshvpn.net,I9:smoktruefalse.com,I10:prince-of-persia24.ru,
I11:med-global-fox.com,I12:hxxp://intranet.excelsharepoint[.]com/,
I13:hxxp://info.docs-sharepoint[.]com/,I14:hxxp://networkupdate[.]online/,I15:hxxp://webfeed.updatesnetwork[.]com,I16:hxxp://invoicesharepoint[.]com/
C1:Skype,C2:.zip Files,C3:a legitimate instant messaging file,C4:W32.IRCBot.NG,C5:W32.Phopifas,C6:.exe file,
C7:Downloader.Liftoh,C8:Spear-phish email,C9:a RTF file disguised as a .doc file,C10:CVE-2012-0158,C11:CVE-2010-3333,C12:Bitcoin miner,
C13:a variant of Zeus/Zbot(version 2.1.1.2),C14:Retefe,C15:Windows PowerShell,C16:a fake 'thawte Inc.' certificate,C17:Smoke Loader,
C18:man-in-the-middle attack,C20:IRC bot,C21:.doc file,C22:Web Link,C23:Kronos,C24:ScanPOS
V1:Victim's contacts,V2:the data for the bank,V3:The stolen track data,V4:The process in which the data was found,V5:The username

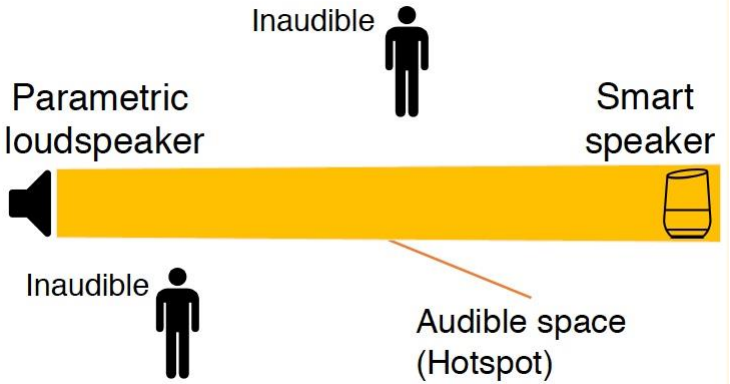
システム出力結果例

Source: T.Nagai, et al, ``Understanding Attack Trends from Security Blog Posts Using Guided-topic Model``, JIP, 2019

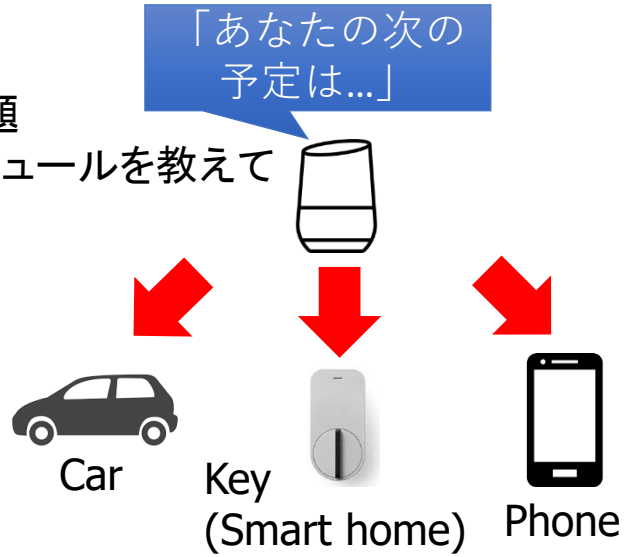
AIのためのセキュリティ（事例：音響セキュリティ）

「Audio Hotspot」攻撃を検証

- 攻撃者は誰にも気づかれずに音声認識デバイスを操作可能
- それを検証すべく、パラメトリックスピーカーを利用して指向性サウンドビームを生成し、音声コマンドを入力する実験を実施



1. プライバシー問題
例)「私のスケジュールを教えてください」



2. 接続デバイスを制御可能
例) ドアの開錠、車の制御、他人への電話

対策
機械学習を用いて録音ボイスとそうでないものを識別する手法を提案・検証

Source: R.Iijima et al, "Audio Hotspot Attack: An Attack on Voice Assistance Systems Using Directional Sound Beams," TETC, 2019.

サイバーセキュリティの研究開発の方向性

1)サプライチェーンリスク:
- サプライチェーンは複雑化が進行しており、十分な検討が必要
- すべてのレベルの管理者をより強化（セキュリティ的に）する必要性がある
- サプライチェーンリスクに備えた技術的な検証評価環境（プラットフォーム）の実施が要

2)サイバー攻撃を想定した観測、分析、共有のためのプラットフォームの強化
- 関係者（組織）間での情報共有が必須
- 継続的な観測と分析を実施し、適切なセキュリティレベル力の向上を実施すべき
- 特に、深層分析のためには、AI(ML/DL)をサイバーセキュリティのために効果的に活用することが重要

3)暗号化、認証などの基盤技術の研究開発の推進
- QKD, PQC, 軽量暗号– 特定の応用にどのように適用するかなども鍵
- 暗号技術等の基盤技術を適切に利用する技術の研究も重要ー無駄な計算資源を使わず、安全な通信環境を実現するため

4)数ある応用に対するセキュリティ研究の促進
- IoT, Cloud, Big data, Smart-city, DLT, 5G, Connected Car, Transportation (ITS), Maritime等
- 各応用において、参照モデルを明確にし、そこに存在する「脅威」を分析・評価することが特に重要
- 該応用のためのセキュリティ管理策（対策）の導出、及びそれらを実際の試験環境において評価することが重要

5)産官学間の協調連携のコミュニティを育成する
- どのように産官学連携コミュニティを形成するのか　–　規模的に、ローカルから始め、グローバル、国際と展開できれば理想

まとめ

1. 攻撃者の標的や攻撃の種別によって、攻撃から与えられるインパクトが異なる。常に、我々は何の脅威と戦っているかを明確にしておく必要がある。

2. IoTや5G等への多くの脅威(攻撃)に対し、セキュリティ対策が多様な形で適用される。しかし、以下のような対策に関する分類や倫理的な見解が存在する。
   - ✓ Passive Defense:基本対策、FW、AV、Patch管理、監視等
   - ✓ Low Impact Active Defense:アクティブ情報共有、サンドボックス/ハニーポット(例:IoT/DRDoS)、ハンティング(例:Stardust)、Darknet(NICTER)、Beacon、DeepWeb等
   - ✓ High Impact Active Defense:ボットテイクダウン、連携制裁、White ランサム等
   - ✓ Offensive Cyber:反撃、敵の破壊(許可なく)等

3. AI技術を効果的に活用することにより、早期の段階で「攻撃(予兆)を観測(補足)」し、知見を収集、分析することにより、現状分析だけではなく、今後起こるであろう攻撃の予測を実施。そのための「情報共有」が重要となる。

Thank you for listening