IoTセキュリティ標準化の概観

–ITU-T SG17, ISO/IEC SC27, IETF–

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

Cyber Security Risk（サイバーセキュリティリスク）

- **THREATS（脅威） AND RISKS（リスク）**
  - Risks to operations, information, people, processes, services, applications, and technology （運用、情報、人、プロセス、サービス、アプリ、技術に対するリスク）
  - Threats to society and consumers（社会や消費者に対する脅威）
  - Threats to national infrastructure（国のインフラに対する脅威）
- **IMPACT（インパクト、影響）**
  - Financial loss, disruption or damage to systems and services due to the destructive power of cyber attack/incident （経済的損失、サイバー攻撃やサイバー事故による破壊的な仕業から来るシステム/サービスへのダメージ、不全）
  - Leakage, theft, destruction of critical and sensitive information （重要な情報、センシティブな情報の漏洩、盗難、破壊）

International CYBER Standards （国際的なサイバー関連の規格（標準文書））

グローバルなサイバースペースコミュニティ、開発者、および関係者は、サイバー犯罪との闘いを支援するために、国際的なサイバーセキュリティおよびプライバシー標準を開発することを目指している。

すなわち、国際的なサイバー標準の実装（策定）は、組織、政府が次の内容を行うために、具体的に役立つ。

- サイバーリスクを軽減および最小化
- サイバー攻撃の影響と破壊的な影響の最小化
- 使用するITベースのシステム、サービス、インフラストラクチャへの投資を保護し、機密情報や重要情報を保護する

サイバー空間に関する標準化におけるいくつかの利点

多くの関係者と協力し、開発物の共有化、お互いが学習し、一定の合意形成のもとで、国際サイバー標準を開発することは、以下の素晴らしい効果がある。

- ✓すべての関係者の保護、セキュリティ、および安全性の向上
- ✓適合性評価の基準（認証、テスト、検査）
- ✓コミュニケーション、革新、取引、グローバルガバナンスを促進するための相互理解と共通言語の基礎
- ✓国家のサイバー政策とプログラムを補完し支援する

標準化作業の参画団体

World Standards Cooperation (WSC)

IETF

For Internet Standards

Regional Standards Bodies

Asia-Pacific

Europe (CEN, CENELEC, ETSI)

Americas

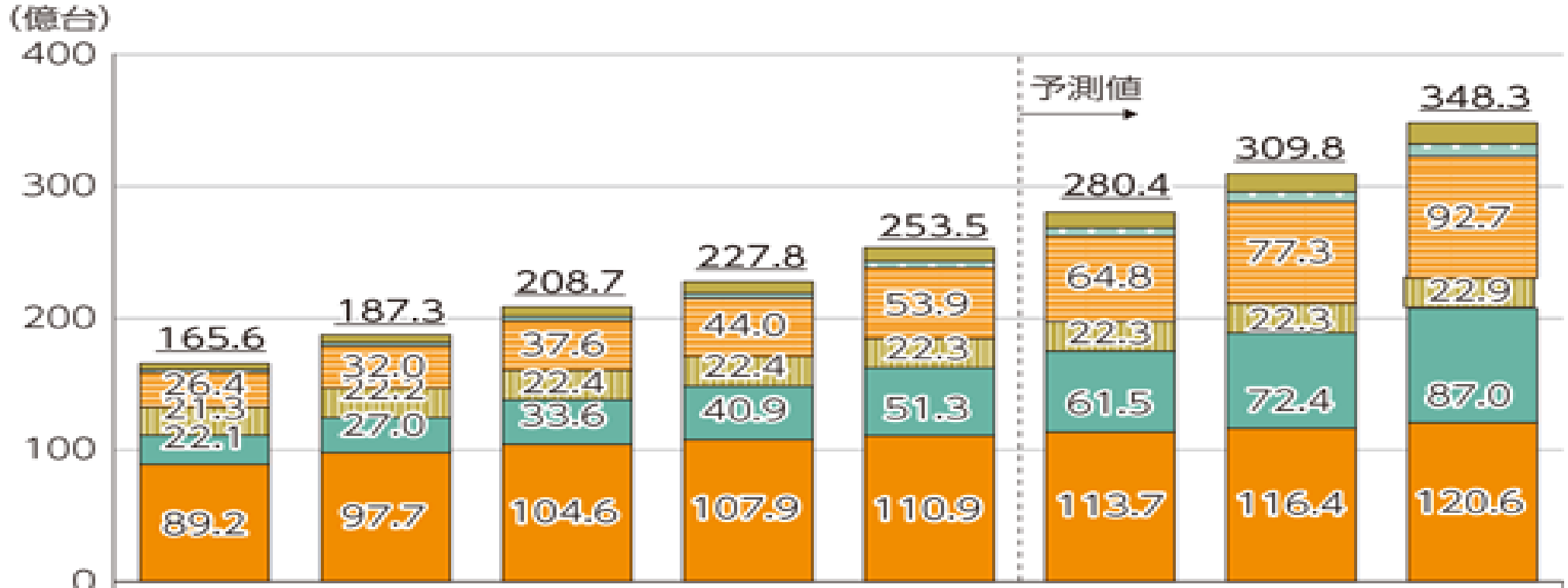
Liaisons (industry groups, consumer groups etc.)

National Standards Bodies (AFNOR, ANSI, BSI, DIN, SAC etc.)

Regulatory Bodies, Government Bodies …

IoT時代

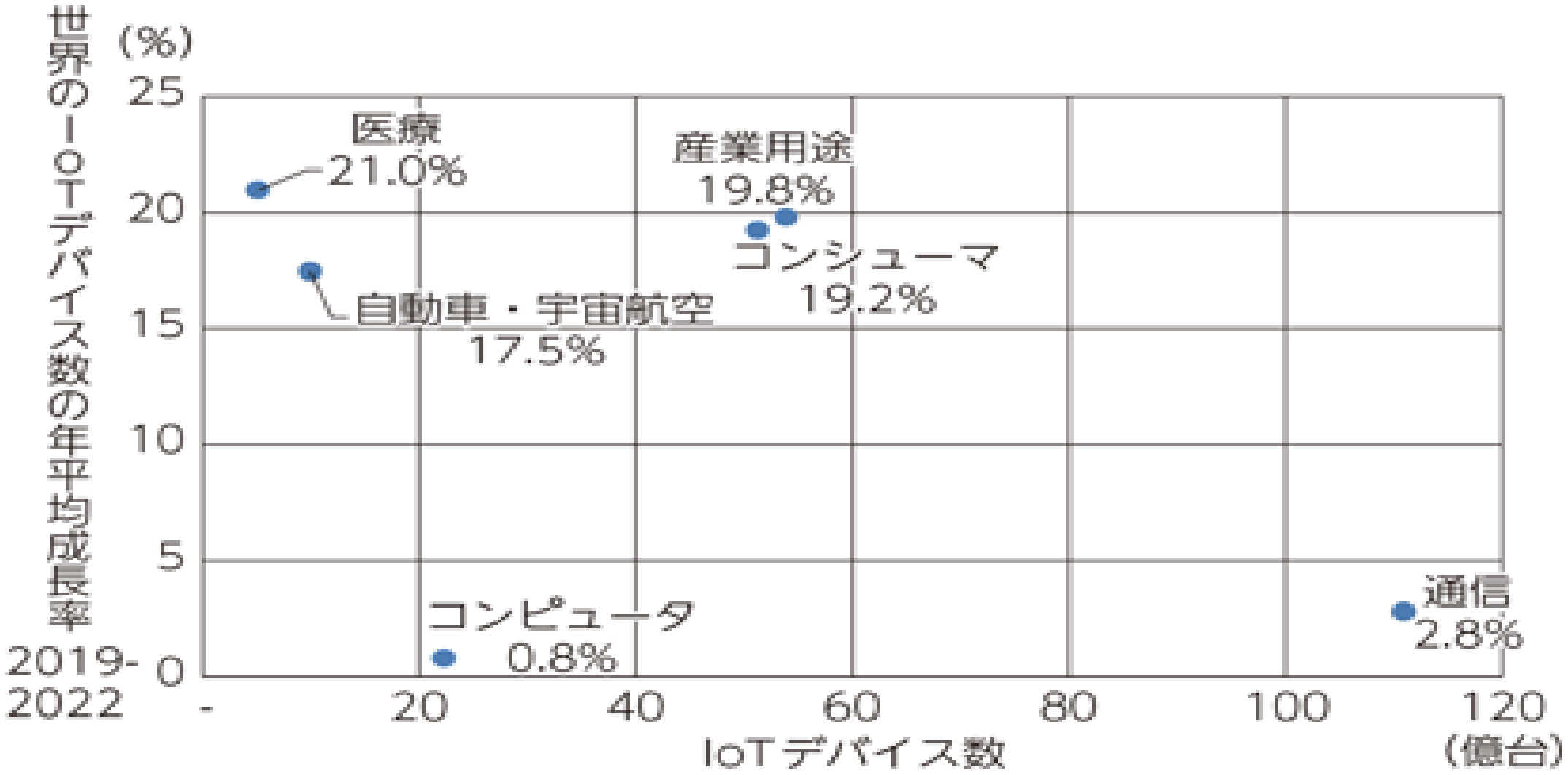
世界のIoTデバイス数の推移及び予測



	2015	2016	2017	2018	2019	2020	2021	2022
合計	165.6	187.3	208.7	227.8	253.5	280.4	309.8	348.3
自動車・宇宙航空	4.5	5.7	7.1	8.6	9.9	11.7	13.7	16.1
医療	2.2	2.7	3.3	4.1	5.1	6.3	7.6	9.1
産業用途	26.4	32.0	37.6	44.0	53.9	64.8	77.3	92.7
コンピュータ	21.3	22.2	22.4	22.4	22.3	22.3	22.3	22.9
コンシューマ	22.1	27.0	33.6	40.9	51.3	61.5	72.4	87.0
通信	89.2	97.7	104.6	107.9	110.9	113.7	116.4	120.6

出典：　総務省情報通信白書　令和2年　IoTデバイスの急速な普及

分野・産業別の世界のIoTデバイス数及び成長率予測



出典： 総務省情報通信白書　令和2年　IoTデバイスの急速な普及

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

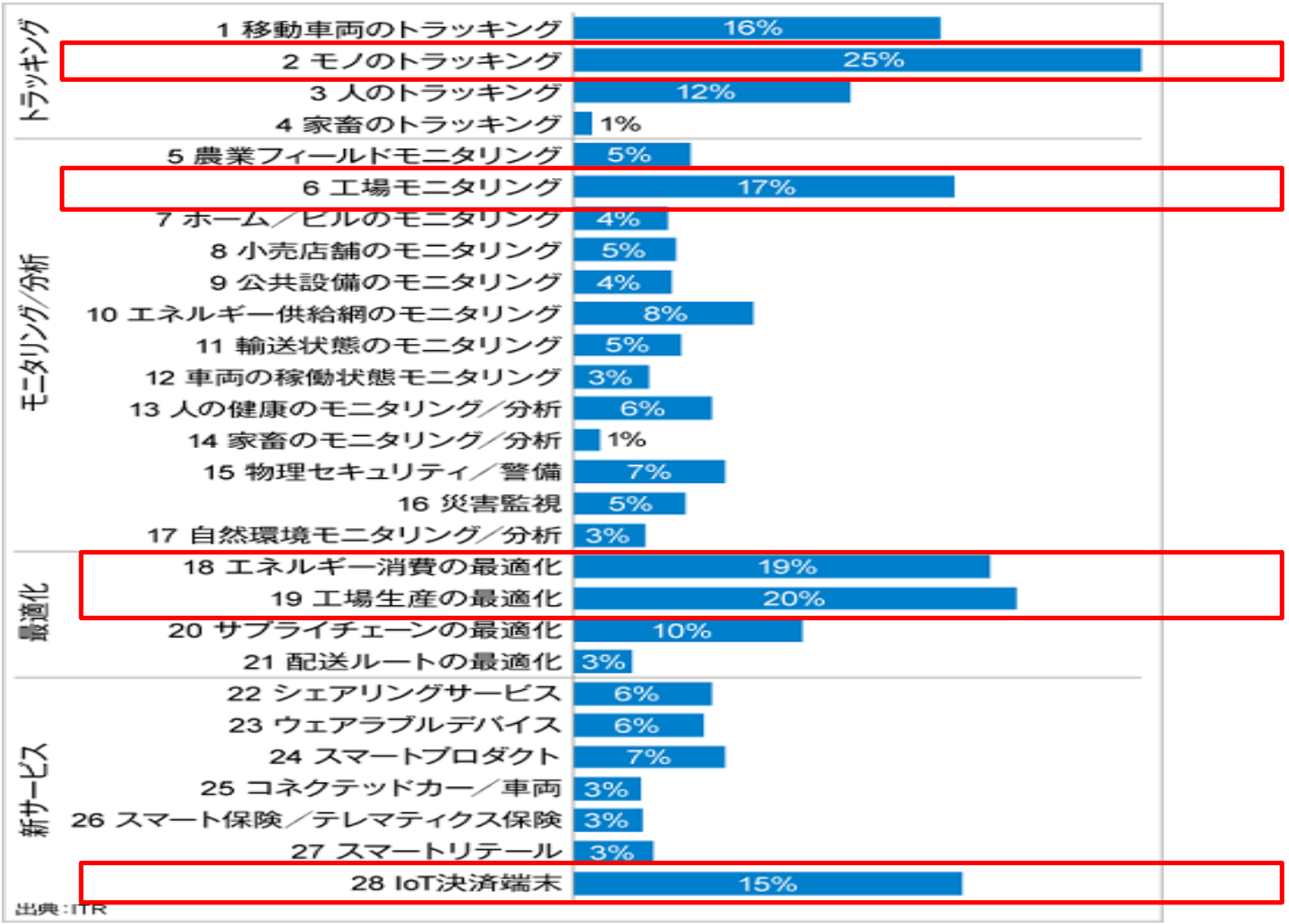


図. IoT導入企業における分野ごとの実施率（全業界平均）

ITR/2017

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

5G時代の背景

（出典）日立製作所、ユースケース：5G

○ 5G等の高度な無線通信サービスの特徴：
超高速・多用途・超低遅延・超高信頼性・超カバレッジ

○ 多種多様なユースケース：
重要インフラ（医療系、交通系等）での遠隔制御、
超仮想現実、繋がる交通機関、スマートシティ、スマートホーム等

○ 多様な構造化の検討：
IoT等のセンサーによるデータ取得と取得データの統合解析の体系化
・経済産業省：サイバーフィジカルシステム（CPS）－ CPSF
・国際標準化：デジタルツイン（DT）－ 仮想現実の世界等

○ システムの複雑化、高度化によるセキュリティの課題：
・多くのステークフォルダーの関与による脅威分析の難しさ
・脅威軽減にむけたセキュリティ対策導入の複雑化
・セキュリティ確保に向けたシステムの維持運用の大変さ
・考慮すべきセキュリティ課題の増大化（クラウドセキュリティ、
IoTセキュリティ、AIセキュリティ等）

5Gのユースケース事例（韓国の場合）

高度モバイルブロードバンド

Hyper-Realistic Media

All Wireless

ミッションクリティカルサービス

Connected Car

Remote Control

マッシブ(Massive)IoT

Home IoT

Smart City

Smart Grid

ITU-T SG17 5G Workshopから抜粋

事例（繋がる車における安全支援）

車の安全走行を目的とした走行状況の実時間観測と実時間分析により、衝突回避などのアラートの発行を目的とする。（上記は、EUと中国との実証実験例）

ITU-T FG-VM　資料からの抜粋

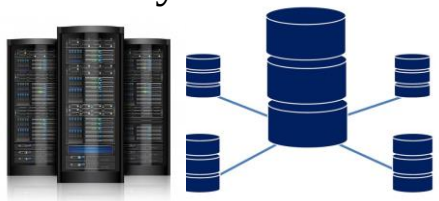
事例（ロボットによる遠隔手術）

ロボット遠隔手術 実用化に挑む 九大や鹿児島大...www.nishinippon.co.jp

Connections in cyber space

Data processing, analysis, management
(Integrated analysis of data collected at multiple points, processing and accumulation, and feedback of appropriate analysis results to IoT consumers in Physical space)

Analysis servers



Data transcription in Cyber/Physical

Data transmission

Camera data
Environmental data
Healthcare data

Feedback of analysis results

Data transmission

Camera data
Activity Log
Location data

Feedback of analysis results

Manufacture IoT devices

Sell IoT devices

Use IoT devices

Use IoT devices

Device manufacturer

Mass retailer

IoT consumer

IoT consumer

Connections in physical space

SC27/WG4で議論されているCPSの概念モデル（案：中尾作成）

ISO/IEC JTC1/SC27で採用されているCPS概念モデル

Analysis Tier
(Connections among IT Tools and People)

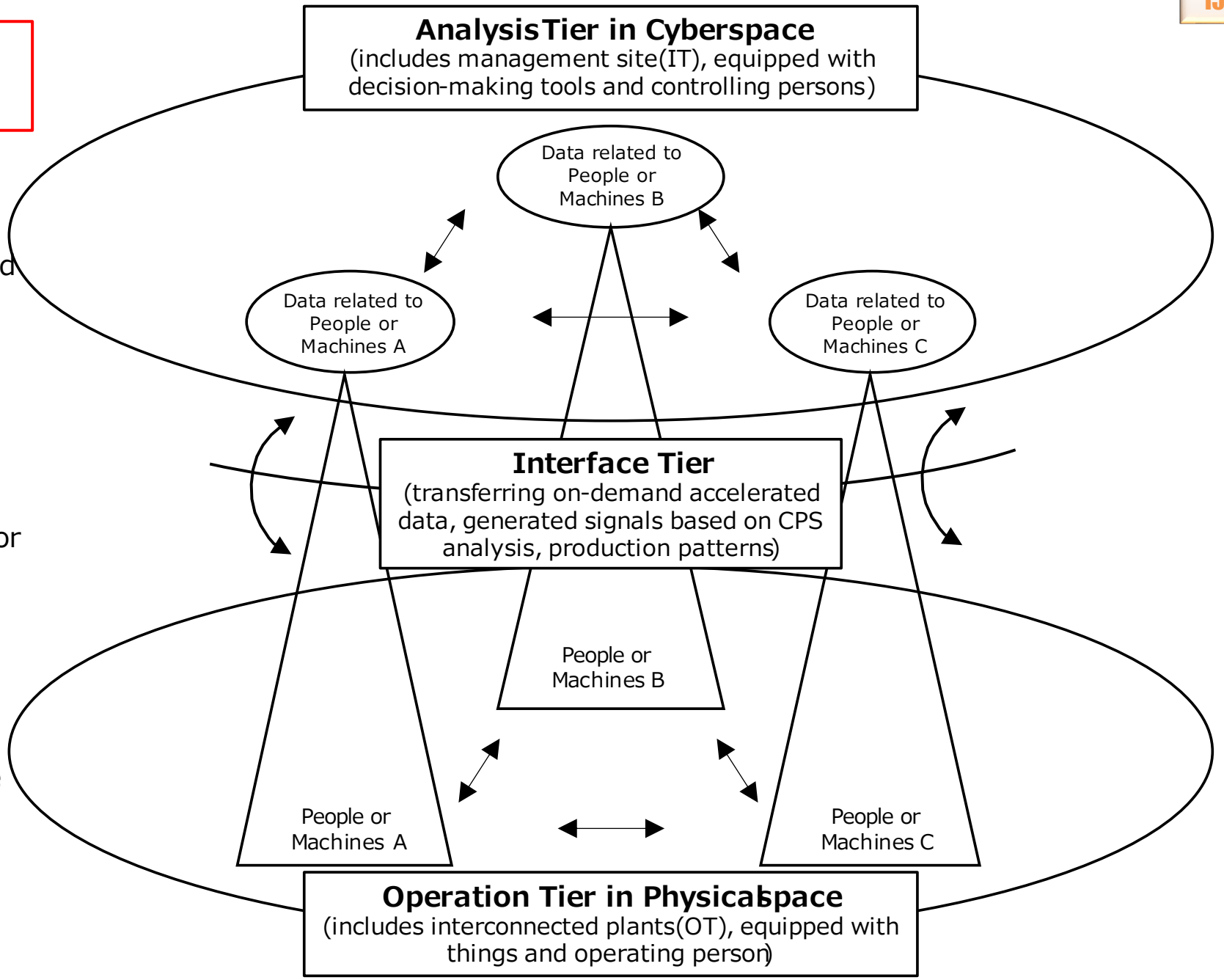
Trustworthiness of data is a key for secured products and services

Interface Tier
(On-demand Interconnecting forward and backward Transfer Functions)

Trustworthiness of data streams is a key for secure operation of cyber-physical systems

Operation Tier
(Connections among Machines and People)

Trustworthiness of business processes is a key for secured products and services



IPカメラの場合

ネットワークカメラ画像無断公開サイト：Insecam

https://www.insecam.org/

ネットワークカメラ画像無断公開サイト：Insecam

https://www.insecam.org/

Insecam **Most popular** Manufacturers Countries Places Cities Timezones New online cameras FAQ Contacts

ENHANCED BY Google

Insecam - Live cameras directory

Welcome to Insecam project. The world biggest directory of online surveillance security cameras. Select a country to watch live street, traffic, parking, office, road, beach, earth online webcams. Now you can search live web cams around the world. You can find here Axis, Panasonic, Linksys, Sony, TPLink, Foscam and a lot of other network video cams available online without a password. Mozilla Firefox browser is recommended to watch network cameras.

The following actions were made to Insecam for the protection of individual privacy:

- Only filtered cameras are available now. This way none of the cameras on Insecam invade anybody's private life

ENHANCED BY Google

- United States(3572)
- Korea, Republic Of(2612)
- Japan(1651)
- Taiwan, Province Of (9
- Italy(756)
- Russian Federation(736)
- Germany(634)
- France(520)
- Iran, Islamic Republic(312)
- Austria(301)
- United Kingdom(292)
- Viet Nam(290)
- Switzerland(267)
- Czech Republic(242)
- Spain(231)
- Belgium(231)
- Netherlands(228)
- Canada(192)
- Brazil(177)

Japan is No 3 (2022/2/7)

Inse

Welcome to Insecam project. nline surveillance security cameras. Select a country to watch live stree ach, earth online webcams. Now you can search live web cams arou Axis, Panasonic, Linksys, Sony, TPLink, Foscam and a lot of other n line without a password. Mozilla Firefox brov etwork cameras.

The following actio e protection of individual privacy:

- Only filtered cameras are av he cameras on Insecam invade anybody's

Examples of Images from Insecam (Japan)

Watch ChannelVision camera in Japan,Tokyo

Watch Canon camera in Japan,Fukuoka

Watch Canon camera in Japan,Saitama

Cyber attacks in IoT on the rise

Thingbots: The Future of Botnets in the Internet of Things

February 20, 2016 | By Paul Sabanal

The Internet of Things (IoT
upon us. Everything from
home appliances, watches
even children's toys are be
connected online. It is proj
that by the year 2020, ther
be more 25 billion devices

Home Router Botnet Leveraged in Large DDoS Attack

Is your refrigerator really part of a massive spam-sending botnet?

Ars unravels the report that hackers have commandeered 100,000 smart devices

by Dan Goodin - Jan 18, 2014 5:25am JST

Internet of Things security 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

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

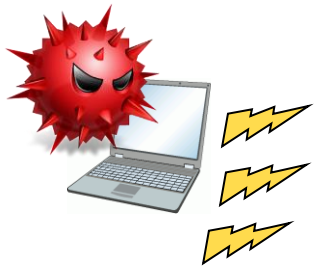
なぜIoT 機器が感染？？

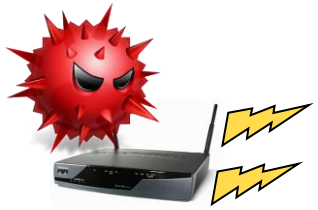
- **24/7** オンライン
- **AV**がない
- 弱い/デフォルトの**ID/PW**の使用
- 機器のライフサイクルが長い
- グローバル **IP** を持ち、インターネットへの接続を開いている
- かなり重要なアプリケーションにも活用されているため、インパクトが大きい場合がある

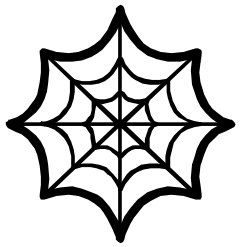
などなど

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



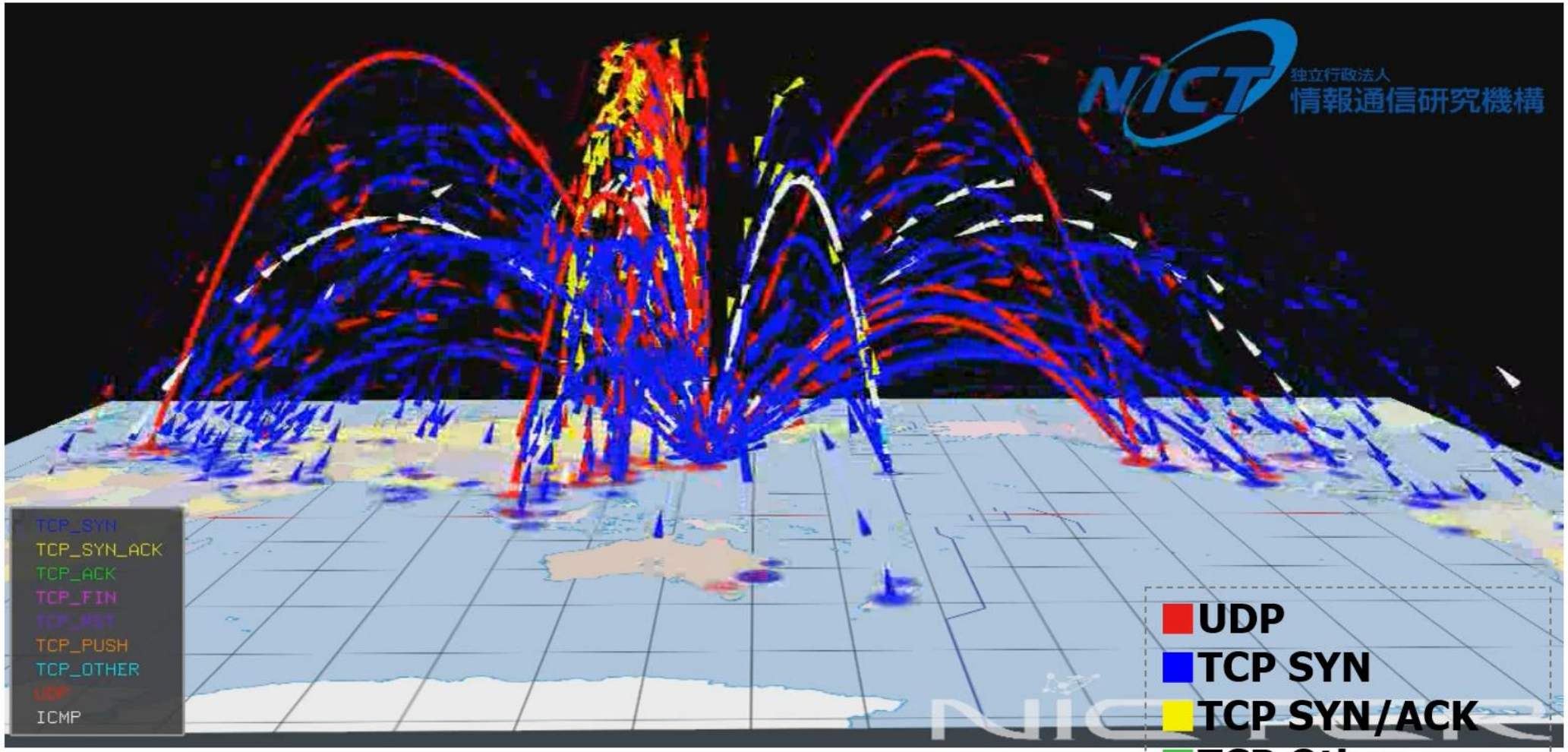




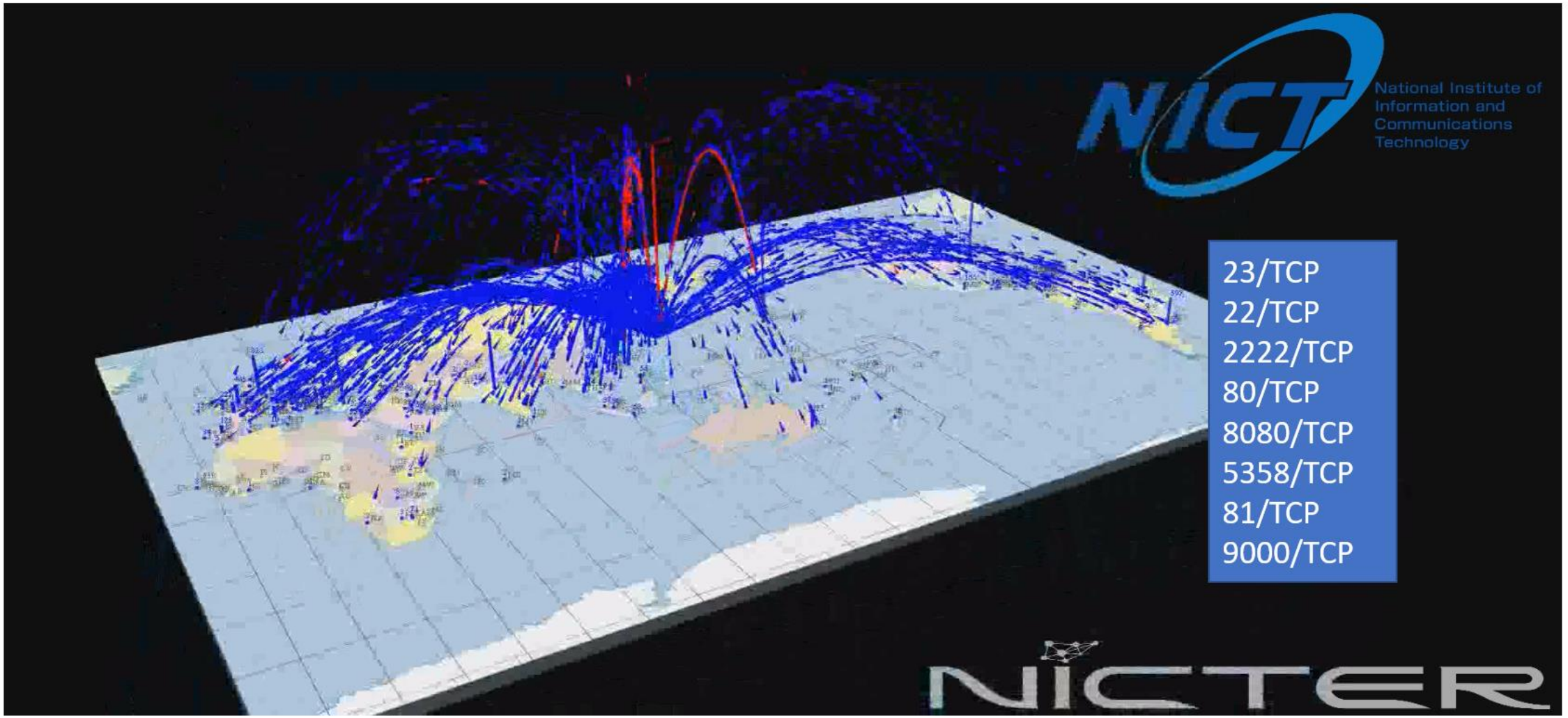
ダークネット

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（ダークネット観測システム）による全スキャン



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）

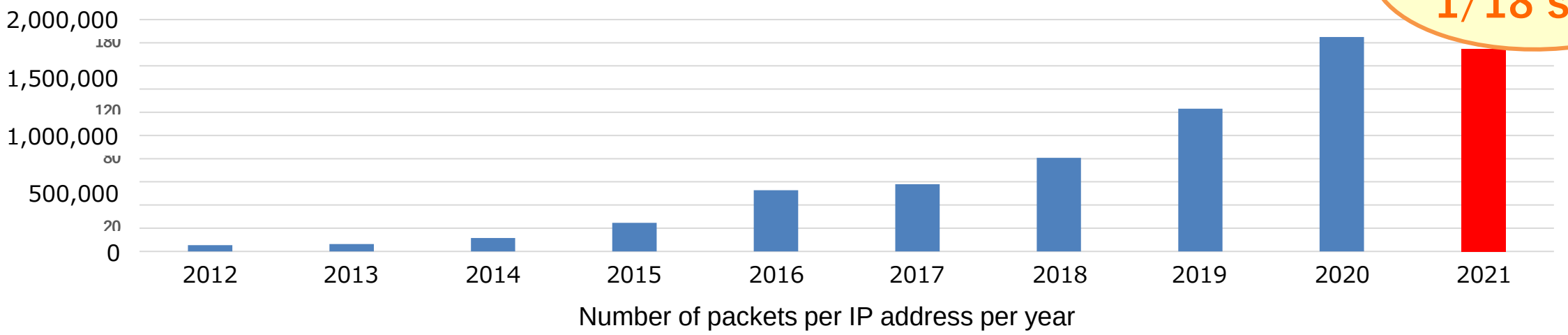


直近10年におけるダークネットトラヒック統計情報

Year	Number of packets par year	Number of IP address for darknet	Number of packets par 1 IP address per year
2012	7.8 billion	190,276	53,206
2013	12.9 billion	209,174	63,682
2014	24.1 billion	212,878	115,335
2015	63.2 billion	270,973	245,540
2016	144.0 billion	274,872	527,888
2017	155.9 billion	253,086	578,750
2018	216.9 billion	273,292	806,877
2019	375.6 billion	309,769	1,231,331
2020	570.5 billion	307,985	1,849,817
2021	**518.0 billion**	**289,946**	**1,747,685**

No. of packets

1/18 sec.



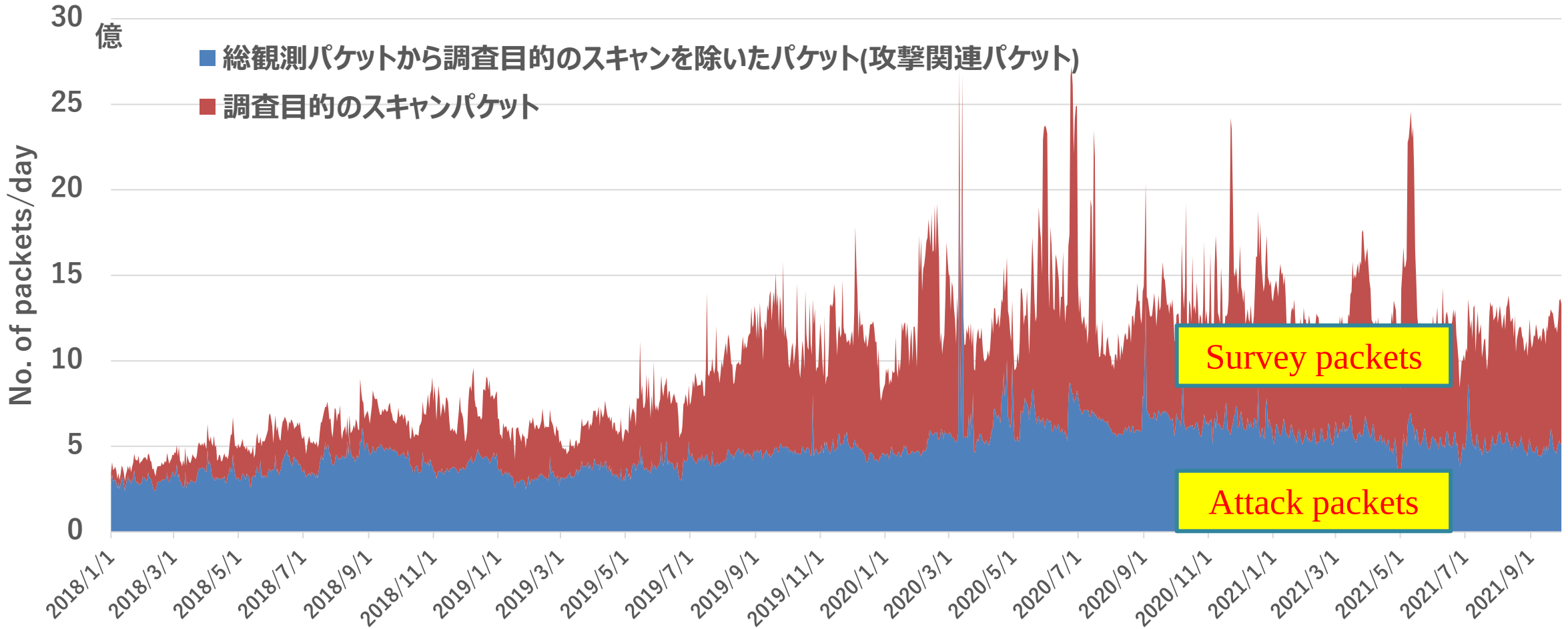
調査用スキャン – NICTERにおけるノイズ

- 2018年から広範囲に調査目的のスキャン活動が増加している。

送信元不明のIPアドレス（ユニークホスト）は、2020年に3,676件、2021年9月末までに2,935件と多く観測された。これらは、以下のような特徴を持つ。

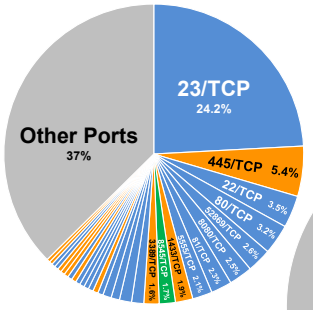
- 全ポートスキャン
- 広域ネットワークスキャン
- 1日に1億～4億パケットを送信するIPアドレスが存在する

実際の攻撃用スキャンと調査目的スキャン

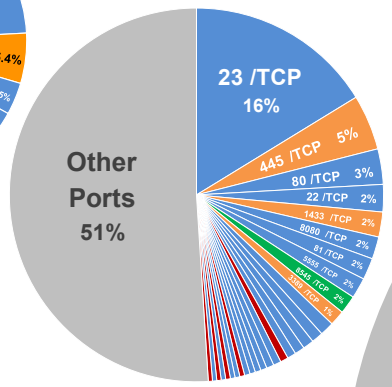


過去3年間の調査目的のスキャン数（赤色）は、緩やかな上昇傾向にある。

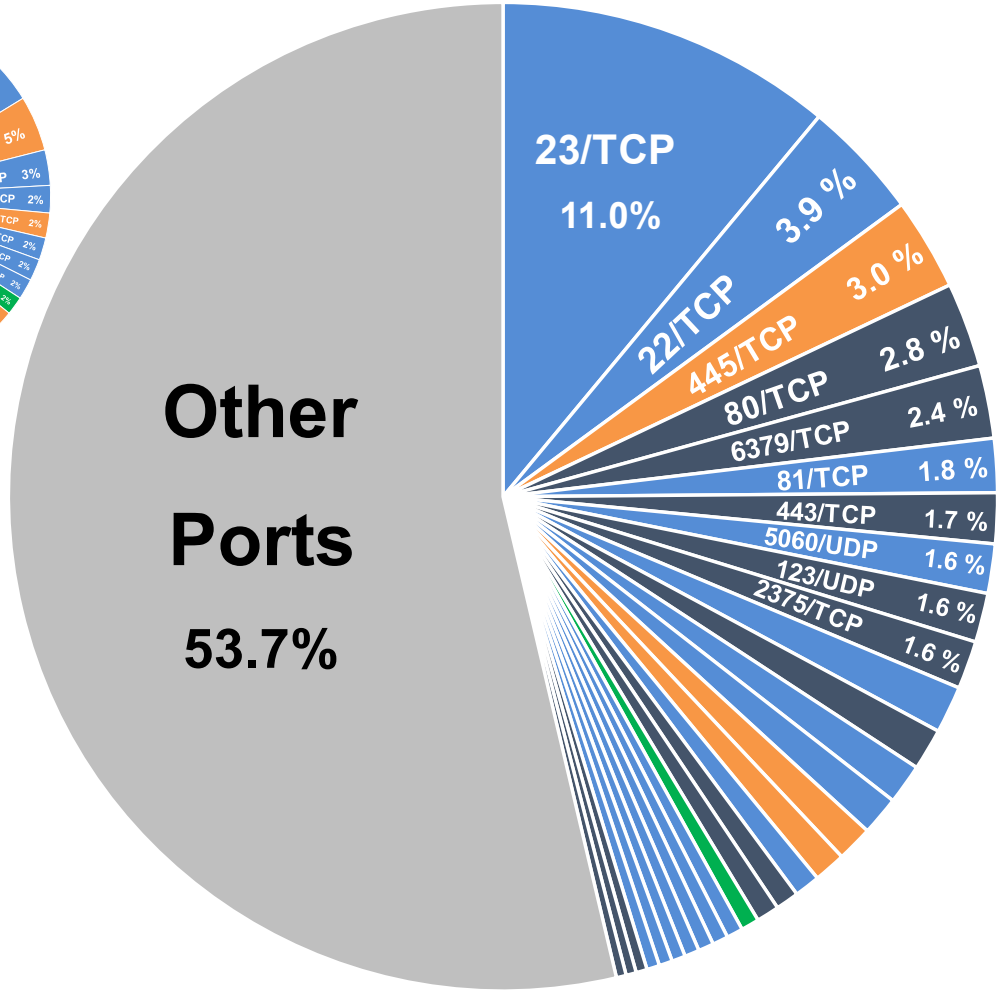
NICTER (2021)によって観測された上位10ポート



2019



2020



2021

Dst Port	Target
23/TCP	Telnet (Router, Web Came, etc.)
22/TCP	SSH (Server, Router, etc.)
445/TCP	Microsoft-DS (SMB, Samba, etc.)
80/TCP	HTTP (Web UI, etc.)
6379/TCP	Redis
81/TCP	HTTP (Home Router, etc.)
443/TCP	HTTPS (Web Server, etc.)
5060/UDP	SIP (PBX, Router, etc.)
123/UDP	NTP
2375/TCP	Docker REST API

(Excluding packets from large-scale scanners)

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機器数の急激な増加に伴い、IoT機器の脆弱性を狙ったサイバー脅威も増加傾向にある。脅威の高まりを受け、各国はIoT機器の安全性確保に向けた取組に力を入れている。

- IoT機器数の急激な増加に伴い、IoT機器の脆弱性を狙ったサイバー脅威も増加傾向にある。
- Kasperskyの調査によれば、**2021年上半期だけで、2020年の2倍以上のIoT機器に対するサイバー攻撃が発生**した。
- また、IBM Security X-Forceの調査によれば、2019年第3四半期から2020年第4四半期にかけて、**IoT機器を対象としたマルウェアの活動が3,000%増加**した。
- 同調査によれば、2020年から2021年にかけて脆弱性全体の増加率は0.4%の増加に留まった一方で、**IoT機器関連の脆弱性の件数は16%も増加**した。
- 加えて、Checkpointの研究者は、IoT機器に対するサイバー攻撃は日々増加するだけでなく、**洗練かつ広範で破壊的になりつつある**ことを指摘している。
- IoT機器に対する脅威の高まりを受け、各国はIoT機器の安全性確保に向けた取組に力を入れている。

IoT機器を対象としたサイバー脅威に関する動向

IoT機器を対象としたサイバー攻撃の増加率	200% （2020年一年間→2021年上半期）
IoT機器を対象としたマルウェア活動の増加率	3,000% （2019年第3四半期→2020年第4四半期）
IoT機器に関係する脆弱性件数の増加率	16% （2020年→2021年）

出所）Threatpost, IoT Attacks Skyrocket, Doubling in 6 Months https://threatpost.com/iot-attacks-doubling/169224/
IBM Security X-Force, X-Force 脅威インテリジェンス・インデックス 2022 https://www.ibm.com/security/jp-ja/data-breach/threat-intelligence/, https://www.ibm.com/downloads/cas/QA59ZP3P
Checkpoint, Protecting IoT Devices from Within – Why IoT Devices Need A Different Security Approach? https://blog.checkpoint.com/2022/07/25/protecting-iot-devices-from-within-why-iot-devices-need-a-different-security-approach/

「IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会（METI）」資料から抜粋

世界（日本を含めた）におけるIoTセキュリティ活動・法令等の概観

「IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会（METI）」資料から抜粋

メーカーによる任意対策に関する取組（ガイドライン、任意認証制度・ラベリング制度 等）

メーカーによる対策義務に関する取組（法規制）

MRI

米国では、IoT機器のセキュリティに関する複数のガイドラインが発表されているほか、セキュリティラベリング制度の検討がなされている。また、一部の州では対策が義務化されている。

- 米国政府におけるIoT機器の安全性確保に向けた近年の代表的な取組として、2020年に「IoT Cybersecurity Improvement Act of 2020」が成立し、**連邦政府がIoT機器を調達する際のガイドライン（NIST SP 800-213）が策定**された。
- また、2021年に署名されたサイバーセキュリティを強化する大統領令（Executive Order on Improving the Nation's Cybersecurity）に基づき**消費者向けIoT製品に対するセキュリティラベリング制度の構築が検討されている**。
- そのほか、州の取組として、**カリフォルニア州やオレゴン州ではIoT機器に対するセキュリティ対策が義務化**されている。

IoT Cybersecurity Improvement Act of 2020（2020年12月）

- NISTに対して、**政府機関が所有・管理する情報システムに接続されたIoT機器を、適切に使用・管理するための標準やガイドラインの作成を指示**した。
- 本法律の制定を受け、2021年11月、NISTより、連邦政府がIoT機器を調達する際のガイドラインであるNIST SP 800-213及びNIST SP 800-213Aが公表された。これらのガイドラインでは、具体的なセキュリティ対策内容について、NISTIR 8259シリーズが引用されている。

Executive Order on Improving the Nation's Cybersecurity（2021年5月）

- NISTに対して消費者向けIoT製品のラベリング制度の検討を指示。
- 2022年2月、NISTは消費者向けIoT製品に対するラベリング制度に関する考慮事項を示した文書を発表し、ラベリングのためのベースライン基準として、NISTIR 8259に基づく基準を推奨した。ただし、具体的な制度オーナー、評価方法、ラベルの種類等は定められておらず、今後の検討事項に位置づけられている。
- 2022年10月、**ホワイトハウスは、消費者向けIoT製品のラベリング制度の構築に向け、企業、団体及び政府機関のステークホルダー間で議論を実施。**ラベル付与の方法については、米国政府の基準に基づき、審査・承認された機関によってテストする方針を示しつつ、まずルーター及びホームカメラ※から着手して、**2023年春の制度展開を目指すと発表**した。

SB-327 Information privacy: connected devices（カリフォルニア州、2020年1月）

HB-2395 Oregon Cybersecurity Bill（オレゴン州、2020年1月）

- IoT機器（インターネットに接続するコネクテッドデバイス）に対するセキュリティ強化を目的とした法律で、**それぞれの州でIoT機器を販売するメーカーに対し、パスワードの管理等を含む合理的なセキュリティ機能を具備することを求めた**。
- 対象となる機器について、インターネットに直接的・間接的に接続される機器が対象となるが、他の法令やガイダンスに基づくセキュリティ要件の対象となっている製品（産業用IoT製品、PC、サーバー、モバイル端末等のIT製品等）は対象外である。

「IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会（METI）」資料から抜粋

出所）各種動向に関する公開情報に基づき三菱総合研究所作成

※ この2機器の選定理由として、最も一般的かつリスクが高い機器であることを挙げている。

メーカーによる任意対策に関する取組（ガイドライン、任意認証制度・ラベリング制度 等）

メーカーによる対策義務に関する取組（法規制）

英国では、2018年に消費者向けIoT製品のセキュリティに関する行動規範が発表されたほか、消費者向けIoT製品に対する対策の義務化を求める法律の検討が進められている。

- 英国政府におけるIoT機器の安全性確保に向けた近年の代表的な取組として、2018年にDCMS（デジタル・文化・メディア・スポーツ省）が、**消費者向けIoT製品のセキュリティに関する13の行動規範である「Code of Practice for Consumer IoT Security」を公開**した。
- DCMSは本規範をEU全体に普及させるべく技術仕様の国際標準化をETSIに提案し、**本規範に基づく欧州規格であるEN 303 645が2019年11月に発表**された。
- また、**消費者向けIoT製品に対してセキュリティ対策の義務化を求める法律（Product Security and Telecommunications Infrastructure）の検討が現在進められている**。

Code of Practice for Consumer IoT Security（2018年10月）

- **消費者向けIoT製品のセキュリティに関する13の行動規範**で、消費者向けIoT製品の設計段階で安全性が確保されるよう、また利用者がデジタルの世界を安心して楽しめるようにガイドラインを設けることで、IoT製品の開発、製造、販売に携わる利害関係者を支援することを目的としている。
- 対象製品について、インターネットやホームネットワーク（両方又はその一方）と関連サービスに接続する消費者向けIoT製品を対象としている。
- 英国DCMSは**本行動規範をEU全体に普及させるべく、技術仕様の国際標準化をETSIに提案**した。ETSIはこの提案に基づき、EU加盟各国のステークホルダーによる討議を実施し、2019年2月にTS（技術仕様）であるETSI TS 103 645を公表、2019年11月には、**EN 303 645として欧州規格化**された。なお、ETSI EN 303 645はフィンランド、ドイツ、シンガポールのラベリング制度のベースとなっているほか、右記PSTI法案のベースにもなっている。

「IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会（METI）」資料から抜粋

Product Security and Telecommunications Infrastructure （検討中）

- 2021年11月24日に**庶民院（下院）に提出された法案で、インターネットに接続するスマートフォン、スマートTV、スマートスピーカー等の機器に対して、セキュリティ対策を義務化**する内容が含まれている。2022年10月27日時点で、**庶民院・貴族院（上院）の両方を通過し、国王の裁可に向けた最終修正段階**である。
- 具体的な対策として、デフォルトパスワードの禁止、脆弱性開示ポリシーの開示、セキュリティアップデートを受ける期間に関する情報の開示の3点が含まれ、自己適合宣言又は第三者評価による適合性評価が必要となる。
- 現状の法案では、法案には遵守しない企業に対する罰金に関する条項も含まれており、最高1,000万ポンド又は当該企業の全世界売上高の4%以内の罰金が科せられる内容となっている。
- 対象となる企業について、機器のメーカーだけでなく、輸入業者や販売業者も含まれる。
- なお、法案が可決された後、完全に施行される前に少なくとも12ヶ月の準備期間を設ける予定であることが示されている。

出所）各種動向に関する公開情報に基づき三菱総合研究所作成

メーカーによる任意対策に関する取組（ガイドライン、任意認証制度・ラベリング制度 等）

メーカーによる対策義務に関する取組（法規制）

欧州では、IoT機器を含む製品の認証スキームが検討されているほか、無線機器に対するセキュリティ対策が2024年8月から義務化される予定である。

- 欧州全体のIoT機器の安全性確保に向けた近年の代表的な取組として、2019年に「EUサイバーセキュリティ法」が施行され、欧州での**IoT機器を含む製品の認証スキームであるEUCC（Common Criteria based European Candidate Cybersecurity Certification Scheme）が検討されている**。
- 2022年9月に**EU市場に投入されるデジタル製品のセキュリティ対応を義務付ける「EUサイバーレジリエンス法」の草案を発表**。2025年後半の施行を予定しており、**対象製品の上市にあたってはセキュリティ要件への適合性証明（自己適合宣言もしくは第三者認証）が求められる**。
- 加えて、**無線機器に関する「EU無線機器指令（RED）（2014/53/EU）」にセキュリティに関する要件が追加**され、**2024年8月から欧州で販売する無線機器に対するセキュリティ対策が義務化**される。

EUサイバーセキュリティ法（2019年6月）

- 2004年に設立されたENISAの役割を強化するとともに、**EUにおけるデジタル関連製品・サービス・プロセスのサイバーセキュリティ認証制度（EUCC）の枠組みを設置**した。
- EUCCはサイバーセキュリティ法に基づく任意の認証制度で、その枠組みも同法に定められており、既存のCC（Common Criteria）のスキームの後継として機能させることを目的としている。
- 2021年5月には、EUCCのスキーム候補に関する報告書（Ver 1.1.1）を公表し、ISO/IEC 15408とISO/IEC 18045に基づいて、ICT製品のサイバーセキュリティの認証を検討していることを発表した。

EUサイバーレジリエンス法（2022年9月草案発表、2025年後半施行予定）

- 2022年9月15日、欧州委員会は、**EU市場に投入されるデジタル製品のセキュリティ対応を義務付けるEU Cyber Resilience Actの草案を発表**した。
- ソフトウェアやハードウェアを含む、他の製品やネットワークへの直接的・間接的な接続が存在するあらゆるデジタル製品が対象となるが、既存の規則で対象となる製品は対象外である。
- 求められる対策として、リスクに応じた適切なレベルのサイバーセキュリティを確保するように設計、開発、生産することのほか、悪用可能な既知の脆弱性がない状態とすること、製品のSBOMを作成すること等、多岐にわたる対策が求められる。
- 対象製品の上市に当たって、当該製品に対するセキュリティ要件への適合性証明（自己適合宣言もしくは第三者認証）が求められる。

EU無線機器指令（RED）（2014/53/EU）（2022年2月発行、2024年8月より義務化予定）

- 2022年1月12日、欧州委員会は、**Radio Equipment Directive（欧州無線機器指令）のサイバーセキュリティ関連条項の施行に関する委任規則（EU）2022/30が発行**し、EU市場に投入される無線機器に対してセキュリティの強化を求めた。
- 具体的な規則は2024年8月1日より義務化。
- 対象機器について、直接・間接問わずインターネットに接続される無線機器が対象となる。
- 求められる対策として、許容できないサービスの低下を引き起こさないこと、個人データ及びプライバシーを保護するための手段を組み込んでいること、不正行為から保護するための一定の機能をサポートすることの3点が求められているが、具体的な規格要件は2023年10月までに準備される予定である。

「IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会（METI）」資料から抜粋

出所）各種動向に関する公開情報に基づき三菱総合研究所作成

メーカーによる任意対策に関する取組（ガイドライン、任意認証制度・ラベリング制度 等）

メーカーによる対策義務に関する取組（法規制）

MRI

ドイツ、シンガポール、フィンランドでは消費者向けIoT製品に対するセキュリティラベリング制度を既に運用開始しているほか、オーストラリアでは当該制度の運用に向けた検討を進めている。

- その他諸外国政府におけるIoT機器の安全性確保に向けた近年の代表的な取組として、**ドイツ、シンガポール、フィンランドでは、消費者向けIoT製品に対するセキュリティラベリング制度が既に開始している**ほか、**オーストラリアでも同様のラベリング制度の構築に向けた検討がなされている**。

IT-Sicherheitskennzeichen (IT Security Label)（2021年12月～）

- 対象製品について、現状ではブロードバンドルーター、電子メールサービス、スマートテレビ、スマートスピーカー等の消費者向けIoT製品のみを対象としているが、今後対象製品を拡大する方針を示している。
- ラベル付与のためには、**ETSI EN 303 645の要件に加え、各製品分野のセキュリティ要件（BSI及びETSIが作成）を満たしていることを、認定を受けたセキュリティ機関によって評価されることが必要**となる。
- 2022年10月27日時点（制度開始後11ヶ月）で34製品・サービスがラベルを取得している。

相互運用実施

Cybersecurity Labelling Scheme (CLS)（2020年10月～）

- すべての消費者向けIoT製品がラベリングの対象である。
- ラベルは4段階に分かれ、**レベル1・2は開発者の自己適合宣言で取得可能、レベル3・4では第三者機関による検証が必要**となる。ラベル付与のためにはETSI EN 303 645の要件に加え、レベル3では、第三者機関によるバイナリ解析、レベル4では機器に対するペネトレーションテストにクリアする必要がある。
- 2022年10月27日時点（制度開始後22ヶ月）で222製品がラベルを取得しているほか、本制度の要件はISO/IEC 27404として、国際標準化に向けた提案がなされている。

Finnish Cybersecurity Label（2020年1月～）

- 対象製品について、インターネットに接続され、デジタル形式でデータを処理・伝送する製品・サービスを対象としている。
- ラベル付与のためには、**ETSI EN 303 645をベースに作成された情報セキュリティ要件を満たしていることを、認定を受けたセキュリティ機関によって評価されることが必要**となる。
- 2022年10月27日時点（制度開始後36ヶ月）で17製品がラベルを取得している。
- シンガポールのCLSとの相互運用を行っており、本制度でラベルが付与された製品は、シンガポールのCLSでレベル3を満たしていると認められる。

Labelling for Smart Devices（検討中）

- インターネットやホームネットワークに接続される前提で開発された、**あらゆる消費者向けのスマートデバイスを対象としたセキュリティラベリング制度の検討が進められている**。
- ラベル付与のための基準として、ETSI EN 303 645を採用する方針が示されている。
- なお、2021年にはBETA（豪州政府行動経済学チーム）がIoT製品のセキュリティラベルの有効性に関する調査を実施し、セキュリティラベルが付与されることで、IoT製品に対する消費者の支払意思額が増加することを示した。

出所）各種動向に関する公開情報に基づき三菱総合研究所作成

「IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会（METI）」資料から抜粋

我が国においてもIoT機器の安全性確保に向けた取組を推進してきており、代表的な取組として、IoT製品メーカーの対策を支援するガイドラインを複数発表している。

- 我が国においてもIoT機器の安全性確保に向けた取組を推進してきた。
- 代表的な取組として、経済産業省、IPA、総務省等は**メーカーのセキュリティ対策を支援するガイドラインを複数発表**している。

#	文書タイトル	発行時期	発行者	文書概要
1	サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）	2019年4月	経済産業省	新たなサプライチェーン構造において求められるセキュリティ対策の全体像を整理し、セキュリティ対策例をまとめた文書
2	IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）	2020年11月	経済産業省	IoT機器・システムをリスクに応じてカテゴライズし、各カテゴリに対するセキュリティ・セーフティ要求の検討の考え方を示した文書
3	機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き	2021年4月	経済産業省	機器のセキュリティ検証において検証サービス事業者や検証依頼者が実施すべき事項等について整理した文書
4	電気用品、ガス用品等製品のIoT化等による安全確保の在り方に関するガイドライン	2021年4月	経済産業省	家電製品などがインターネット環境で使われることで想定されるリスクに対し、安全確保の在り方を示した文書
5	IoTセキュリティ・セーフティ・フレームワーク Version 1.0 実践に向けたユースケース集	2022年4月	経済産業省	一連のIoT-SSFの適用の流れを、複数のユースケースを用いて例示した文書
6	IoTセキュリティガイドライン ver 1.0	2016年7月	IoT推進コンソーシアム、総務省、経済産業省	リスクに応じた適切なサイバーセキュリティ対策を検討するための考え方を、分野を特定せずまとめた文書
7	つながる世界のセーフティ&セキュリティ設計入門	2015年10月	IPA	IoT製品のセーフティ設計・セキュリティ設計の手法の用い方について解説した文書
8	つながる世界の開発指針	2016年3月	IPA	IoT製品の開発時に考慮すべき安全安心に関わる事項を指針としてとりまとめた文書
9	IoT開発におけるセキュリティ設計の手引き	2016年5月	IPA	IoT製品のセキュリティ設計を担当する開発者に向けた手引きとして、参考となる情報をまとめた文書
10	つながる世界の品質確保に向けた手引き	2018年6月	IPA	IoT製品やシステムの品質をライフサイクルにわたり確保・維持するために注意が必要となるポイントをまとめた文書
11	脆弱性対処に向けた製品開発者向けガイド	2020年8月	IPA	製品開発者において実施すべき脆弱性対処と、その開示方法を掲載した文書
12	IoT機器等を開発する中小企業向けのセキュリティ対策に関するガイドライン（仮称）	作成中	経済産業省（予定）	中小のIoT機器メーカーが現実的に対応可能な範囲で実施が求められる対策を示した文書（予定）

出所）各種ガイドラインや検討に基づき三菱総合研究所作成

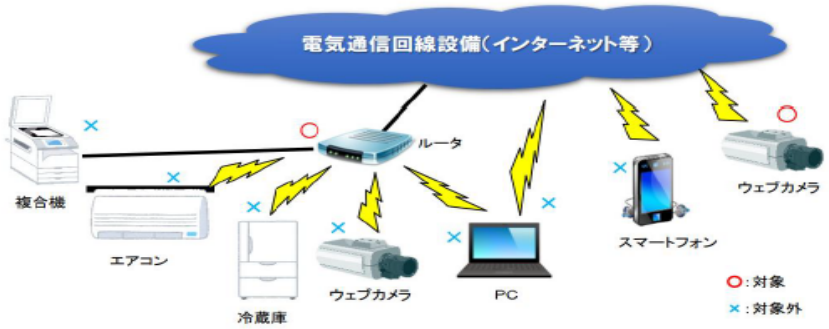
「IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会（METI）」資料から抜粋

総務省の端末設備等規則の一部改正により、インターネットに直接接続するIoT機器におけるセキュリティ対策の実装が義務化されている。

- 総務省は端末設備等規則（省令）（第34条の10）を2020年4月に一部改正し、**電気通信業者のネットワークに直接接続する同規則の施行後に販売されたIoT機器においてアクセス制御機能、初期パスワードの変更機能、ソフトウェアの更新機能の実装を原則義務化**した。
- また、総務省及びNICTは、**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の取組であるNOTICE（National Operation Towards IoT Clean Environment）を2019年2月から開始**している。

端末設備等規則（省令）（第34条の10）（2020年4月より原則義務化）

- 端末設備等規則の一部改正が施行され、**電気通信業者のネットワークに直接接続するIoT機器においてアクセス制御機能、初期パスワードの変更機能、ソフトウェアの更新機能の実装が原則義務化**された。
- 対象となる設備のイメージは以下のとおりであり、例えば、ルータやインターネットに直接接続するウェブカメラ等は該当するが、電気通信回線設備（インターネット等）に直接接続して使用されない機器、PC・スマートフォン、専用線のみにつながる機器等は対象外である。



NOTICE（National Operation Towards IoT Clean Environment）（2019年2月～）

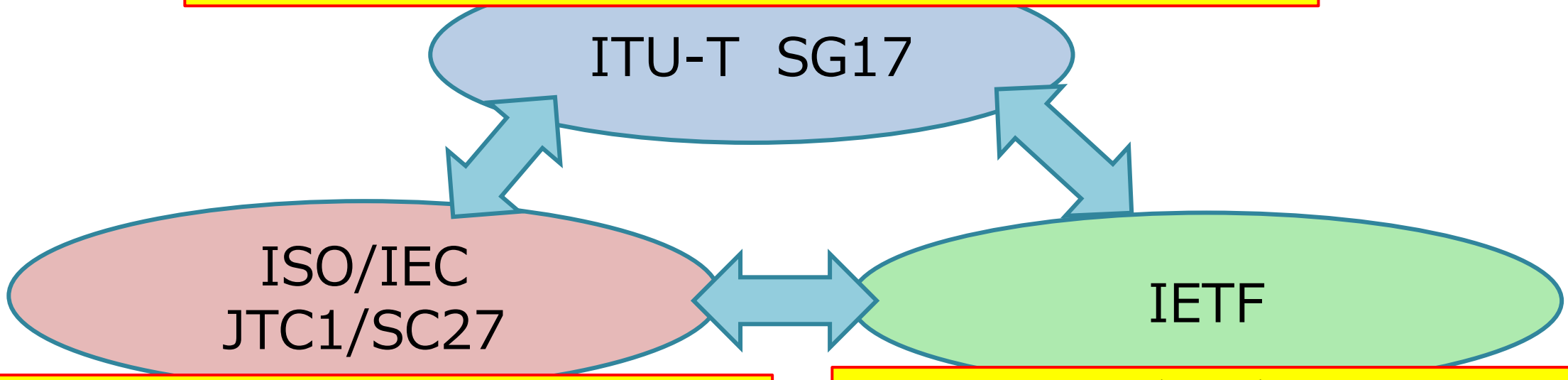
- インターネットサービスプロバイダー（ISP）と連携した、**サイバー攻撃に悪用されるおそれのあるIoT機器の調査及び当該機器の利用者への注意喚起を行う取組**である。
- NICTがインターネット上のIoT機器に容易に推測されるパスワードの入力等を行うことで、サイバー攻撃に悪用されるおそれのある機器を調査し、当該機器の情報をISPに通知する。
- ISPは、NICTから受け取った情報を元に当該機器の利用者を特定し、電子メールや郵送などにより注意喚起を行う。
- 2022年8月時点で73社のISPと連携し、当該ISPの約1.12億のIPアドレスに対して調査を実施した。
- 調査の結果、ログインが可能であり、注意喚起対象としてISPに通知されたIoT機器の件数は2022年8月分で4,381件であった。

「IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会（METI）」資料から抜粋

出所）総務省、電気通信事業法に基づく端末機器の基準認証に関するガイドライン(第２版) https://www.soumu.go.jp/main_content/000744264.pdf
NOTICEホームページ https://notice.go.jp/

国際標準化活動の全体像

通信事業者を中心とした標準化団体。SG17が、セキュリティ全般の標準化（勧告化）を実施。適用範囲は、通信だけではなく、機器やサービスの開発者・提供者を対象としている。IoTについては、IoTシステムの構成要素に関連する要件やガイダンス、及びユースケースに特化したセキュリティ技術が主



一般的なセキュリティ技術にかかわる国際標準を策定している。対象としては、サイバーセキュリティ、プライバシー、セキュリティマネジメントに係る技術要件やガイドラインを広くカバーしている。IoTについては、基盤的なガイドライン、IoT機器の基本要件、セキュリティラベリング等に関する規格化が主。

インターネット技術を標準化対象としており、セキュリティについては、機能の実装技術や具体的な活用技術を中心に検討している。IoTについては、具体的IoT機器のファームアップデートなどの規格化を実施。

ITU-T SG17
Security

Study Group 17 における議長、副議長の方々

Mr Samir ABDELGAWAD
Egypt

Mr Heung Youl YOUM
Korea (Republic of)

Mr Gökhan EVREN
Turkey

Mr Yutaka MIYAKE
Japan

Ms Lia MOLINARI
Argentina

Mr Greg Ratta
USA

Mr Arnaud Taddei
UK

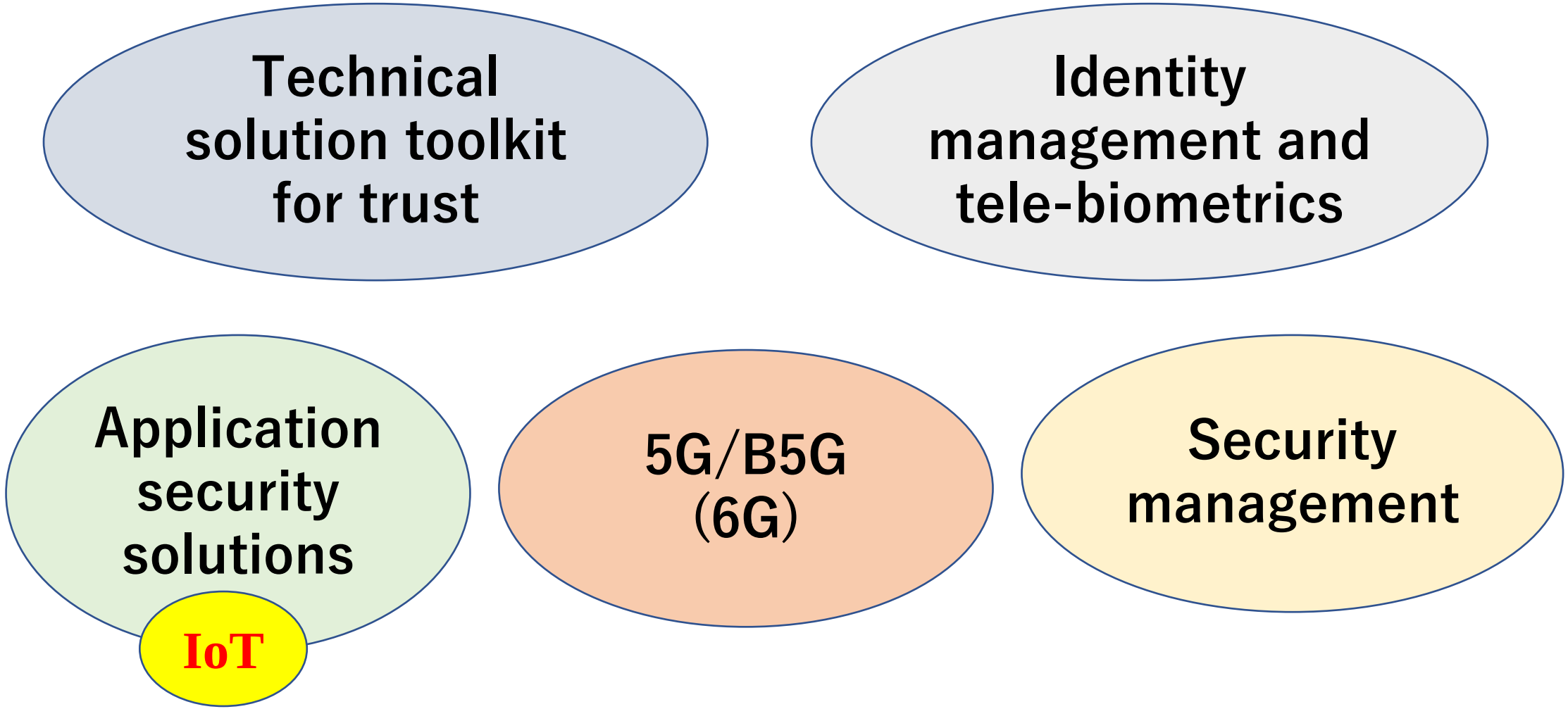
Ms Wala TURKI LATROUS Tunisia

Mr Liang WEI
P.R. China

SG17におけるワーキンググループの構成

- **WP 1　Security strategy and coordination**
  - Q1/17　Security standardization strategy and coordination
  - Q15/17　Security for/by emerging technologies including quantum-based security
- **WP 2　5G, IoT and ITS security**
  - Q2/17　Security architecture and network security
  - Q6/17　Security for telecommunication services and Internet of Things
  - Q13/17　Intelligent transport system (ITS) security
- **WP 3　Cybersecurity and management**
  - Q3/17　Telecommunication information security management and security services
  - Q4/17　Cybersecurity and countering spam
- **WP 4　Service and application security**
  - Q7/17　Secure application services
  - Q8/17　Cloud computing and Big data infrastructure security
  - Q14/17　Distributed Ledger Technology (DLT) security
- **WP 5　Fundamental security technologies**
  - Q10/17　Identity management and telebiometrics architecture and mechanisms
  - Q11/17　Generic technologies (such as Directory, PKI, Formal languages, Object Identifiers) to support secure applications

Study Group 17における主なトピック



SG17参加国 （主な参加国：CJK+US/UKなど）

ITU-T SG17におけるIoT 国際標準の紹介

詳細は中尾から後ほど講演

SG17　課題６

- X.1352: Security requirements for Internet of things devices and gateway
- X.1353 (draft): Security methodology for zero-touch Deployment in massive IoT based on blockchain
- X.1361: Security framework for the Internet of things based on the gateway model
- X.1362: Simple encryption procedure for Internet of things (IoT) environments
- X.1363: Technical framework of personally identifiable information handling system in Internet of things environment
- X.1364: Security requirements and framework for narrowband Internet of things
- X.1365: Security methodology for the use of identity-based cryptography in support of Internet of things (IoT) services over telecommunication networks
- X.1366: Aggregate message authentication schemes for Internet of things environment
- X.1367: Standard format for Internet of things error logs for security incident operations
- X.1368: Secure firmware or software update for Internet of things devices
- X.1369: Security requirements for IoT service platform

ISO/IEC JTC1/SC27

ISO/IEC JTC 1/SC 27 (Information security, cybersecurity and privacy protection) 構造

WG 1	WG 2	WG 3	WG 4	WG 5
Information security management systems	Cryptography and security mechanisms	Security evaluation, testing and specification	Security controls and service	Identity management and privacy technologies

75 countries (NSB) involved (51 P-members and 25 O-members)
36 external liaison bodies (L-members), 32 internal liaisons
950+ experts (NSB + Liaison Bodies)

Total number of projects = 264, Number of active projects = 88, Published standards = 182

ISO/IEC JTC 1/SC 27

Information Security Management Organistion of Standards Work Within SC 27

Information security management system (ISMS) requirements

plus

ISMS supporting guidance - codes of practice of information security controls, ISMS risk management, ISMS performance evaluation and ISMS implementation guidance

ISMS sector specific security controls *(including application and sector specific e.g. Cloud, Telecoms, Energy, Finance)* **and sector-specific use of ISMS requirements standard**

Security services and controls *(focusing on contributing to security controls and mechanisms, cover[illegible]ss for bu[illegible] IT netw[illegible] party services, supplier relationships (including Cloud), IDS, incident management, cyber security, application security, disaster recovery, forensics, digital redaction, time-stamping and other areas)*

IoT

Identity management and privacy technologies *(including application specific (e.g. cloud and PII), privacy impact analysis, privcy framework, identity management framework, entity authentication assurance framework, biometric information protection, biometric authentication)*

ISMS accreditation, certification and auditing *(including acreddited CB requirements, guidance on ISMS auditong and guidelines for auditors on ISMS controls)*

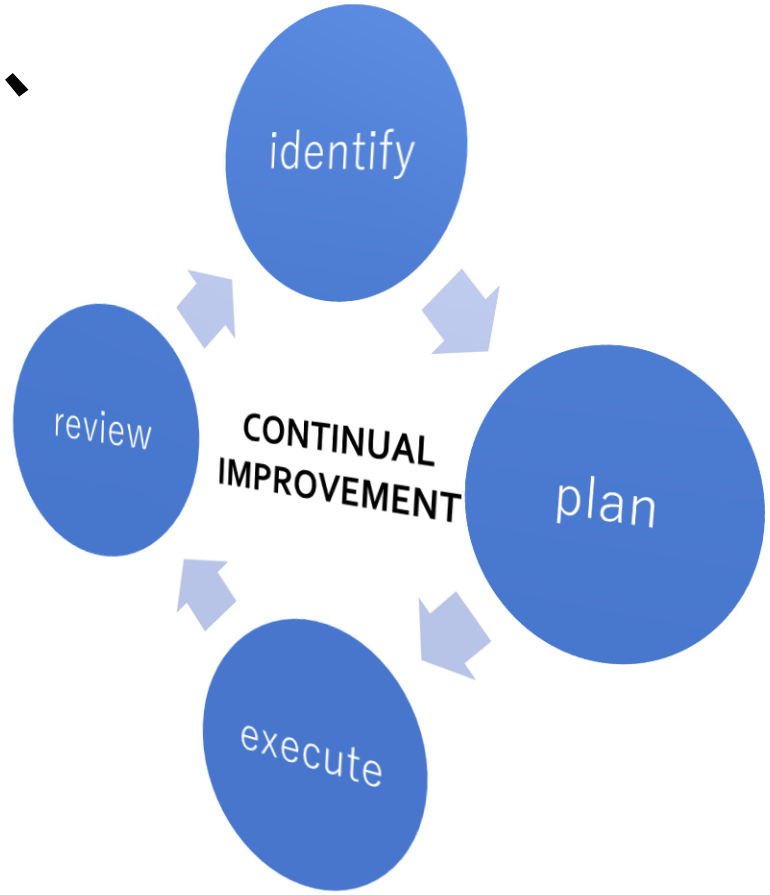
Security Evaluation, Testing and Specification *(including evaluation criteria for IT security, framework for IT security assurance, methodology for IT security evaluation, cryptographic algorithms and security mechanisms conformance testing, security assessment of operational systems, SSE-CMM, vulnerability disclosure, vulnerability handling processes, physical security attacks, mitigation techniques and security requirements)*

Cryptographic and security mechanisms *(including encryption, digital signature, authentication mechansisms, data integrity, non-repudiation, key management, prime number generation, random number generation, hash functions)*

ISO/IEC 27001 ISMS（Information security management system）がコア規格

サイバーセキュリティのマネジメントについては、その継続的な改善が重要：

- Anticipate
- Prepare
- Protect
- Reactive & Responsive
- Adaptive *(business plasticity)*
- CONTINUAL IMPROVEMENT



SC27におけるIoT 国際標準の紹介

詳細は山下様から後ほど講演

ISO/IEC JTC1/SC27

ISO/IEC 27400 series: IoT security and privacy

- ISO/IEC 27400: Guideline (IS)
- ISO/IEC 27402: Device baseline requirements (CD)
- ISO/IEC 27403: Guidelines for IoT-domotics (CD)
- ISO/IEC 27404: Universal cybersecurity labelling framework for consumer IoT (PWI)

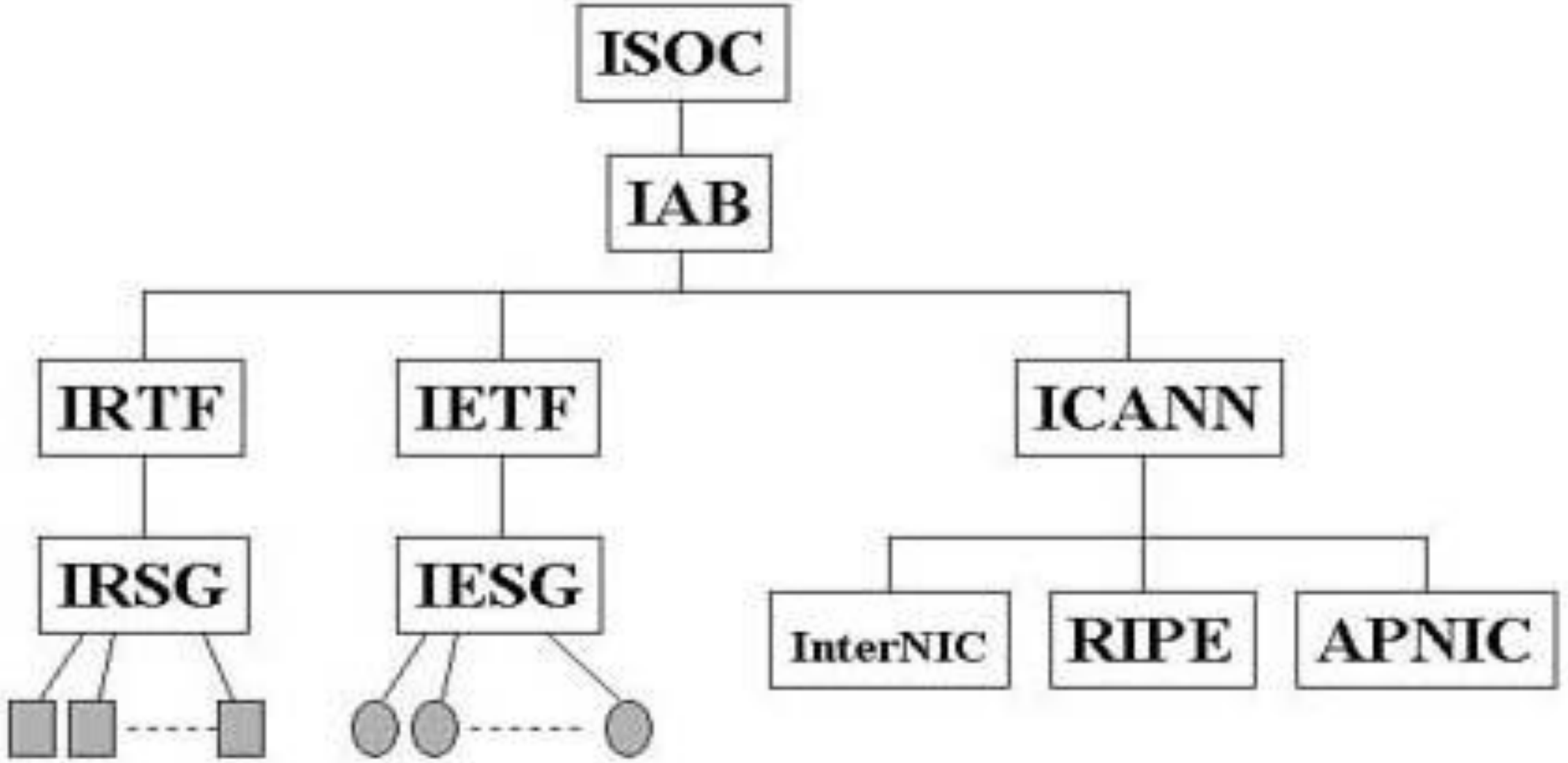
ISO/IEC 5689: Security framework and use cases for CPS (PWI)

- 注：PWI(Preliminary Work Item)とは、規格案件になる前の暫定的な作業項目を指す。

詳細は礒部様から後ほど講演

IETF
Internet Engineering Task Force

IETFの組織構造



IESG (Internet Engineering Steering Group)で扱う技術エリア

- General (gen, 統括的技術エリア)
- Applications Area (app、アプリケーションエリア)
- Internet Area (int、インターネット技術エリア)
- Operations & Management Area (ops、運用管理技術エリア)
- Routing Area (rtg、経路制御技術エリア)
- Security Area (sec、セキュリティ技術エリア)
- Transport Area (tsv、転送プロトコル技術エリア)
- User Services Area (usv、ユーザーサービスエリア)

IoTに関連した取り組み

詳細は礒部様から後ほど講演

- Constrained Device (制約付きデバイス,RFC7228)
  - 処理性能や消費電力に制約のあるデバイスという位置づけ
  - Classが定義され、ターゲットデバイスの指定などに使われる

Name	data size (e.g., RAM)	code size (e.g., Flash)
Class 0, C0	<< 10 KiB	<< 100 KiB
Class 1, C1	~ 10 KiB	~ 100 KiB
Class 2, C2	~ 50 KiB	~ 250 KiB

Table 1: Classes of Constrained Devices (KiB = 1024 bytes)

- IoTデバイス向け規格
  - CoAP(Constrained Application Protocol)
    HTTPレイヤーに相当する通信プロトコル
  - ACE(Authentication and Authorization for Constrained Environments)
    IoTデバイス向けの認証プロトコル

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）：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

IoTにおける多様なステージにおけるセキュリティ検討

1. IoT機器等の製品化前のセキュリティ
   ISO/IEC 27400, 27402, IoT device certification (他国）, etc.
2. IoTシステムを運用する前のセキュリティ
   ISO/IEC 27400, etc.
3. IoTシステム（機器）を実際に利用・運用する際のセキュリティ
   MIC project（NOTICE等）, ISO/IEC 27400, etc.
4. IoTシステムのライフタイムの終了時
   ISO/IEC 27400, 27402, etc.

では、国際標準をどのように活用するか

例としては

「認証」とその関連技術として活用

- ✓ Telecom Organizations:
  ISO/IEC 27001/27002+ITU-T X.1051 | ISO/IEC 27011
- ✓ Cloud Service Providers:
  ISO/IEC 27001/27002 + ITU-T X.1603 | ISO/IEC 27017
- ✓ IoT Stakeholders (user, provider, developer): ISO/IEC 27400 and ITU-T X.sc-iot (under development)

新しいセキュリティ技術の方向性提示として活用

- ✓ IoT area
- ✓ 5G area;

インシデント管理をより改善するために活用

- ✓ ISO/IEC 27035, ITU-T X.1056

標準的な言語や基本体系として活用

- ✓ Asn.1, X.509 certificate, STIX/TAXII

今後のセキュリティ標準化の方向性（IoTも含めた全般）

a. ISMS認証スキームを適用することに一定の時流。ただし、既存のISMSは、動的に変化する多様な最新の脅威を正しくカバーしていないことが問題。

b. サイバー攻撃（脅威）を効果的かつ迅速に管理するには、実行可能なISMS継続的改善プロセスモデルに関連して、実行可能なサイバーセキュリティ管理の導入が必要。

c. このアプローチでは、脅威の分析と、サードパーティの監視機能の調整を伴う効果的な監視手法が重要。

d. 組織内、FW/IDSなどの対策間の相関、AVとPKIは重要。さらに、インシデントを検出するには、効果的な監視スキームの準備が必要。

e. 外部との協調的調整のために、利害関係者間での効果的なサイバーセキュリティ情報交換と、有効な分析および監視機能を信頼できる外部と実施する必要がある。

f. このアプローチは、継続的な改善プロセスのためにさらに研究および検討される必要がある。

g. 上記を達成するための、重要な手段として、「国際標準化」の活用が期待されている。

Thank you for listening Q&A