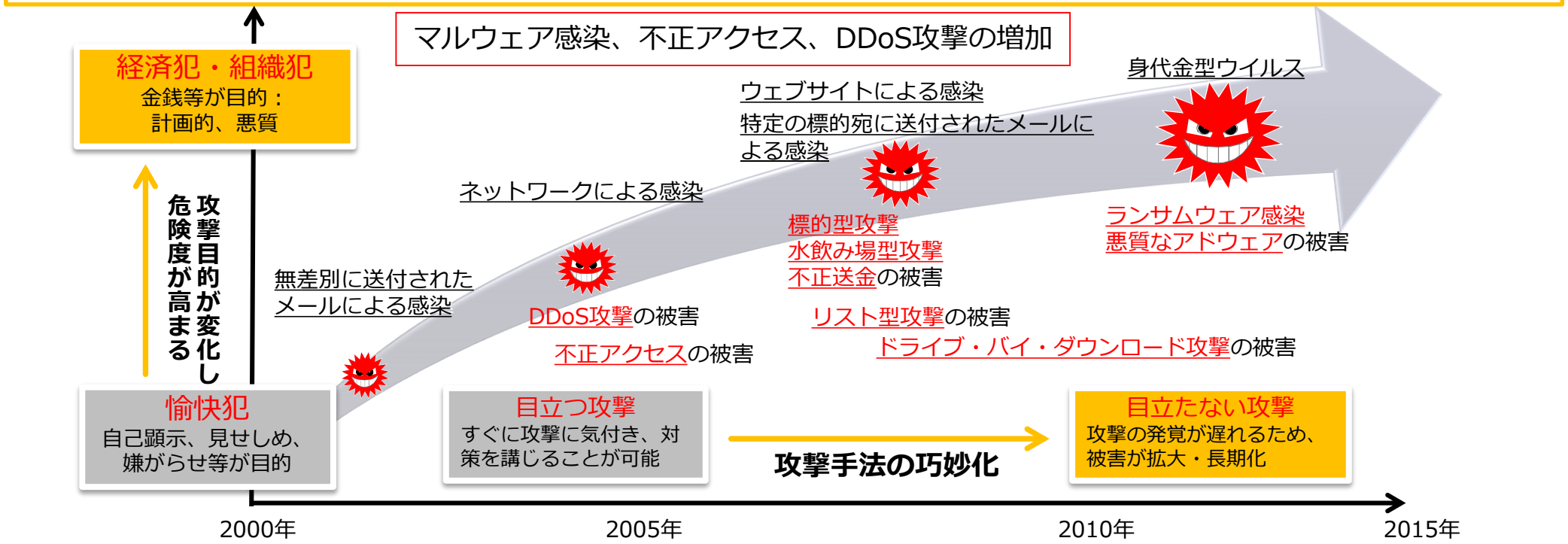
総務省
Ministry of Internal Affairs and Communications

IoT時代のセキュリティ政策について

平成３０年１１月８日
総務省
サイバーセキュリティ統括官付
参事官　木村　公彦

サイバーセキュリティ上の脅威の増大

インターネット等の情報通信技術は社会経済活動の基盤であると同時に我が国の成長力の鍵であるが、昨今、サイバーセキュリティ上の脅威が悪質化・巧妙化し、その被害が深刻化。



国内事例

2015年5月: **日本年金機構**の職員が利用する端末がマルウェアに感染し、年金加入者に関する情報約125万件が流出（**標的型攻撃**）

2015年10月: **金融庁**の注意喚起を装ったフィッシングサイトを確認、国内銀行のセキュリティを向上させるためと称し、口座番号、パスワード、第二認証などの情報を騙し取られる恐れ（**フィッシング攻撃**）

2015年11月: **東京五輪組織委員会**のホームページにサイバー攻撃、約12時間閲覧不能（**DDoS攻撃**）

2016年6月: **i.JTB（JTBのグループ会社）**の職員が利用する端末が、マルウェアに感染し、パスポート番号を含む個人情報が流出した可能性（**標的型攻撃**）

2017年5月: 国内（行政、民間企業、病院等）において、**WannaCry**による被害が確認。企業内のシステム停止などの障害が発生した。（**ランサムウェア**）

海外事例

2015年4月: **フランスのテレビネットワーク TV５ Monde** がサイバー攻撃を受け、放送が一時中断（**標的型攻撃**）

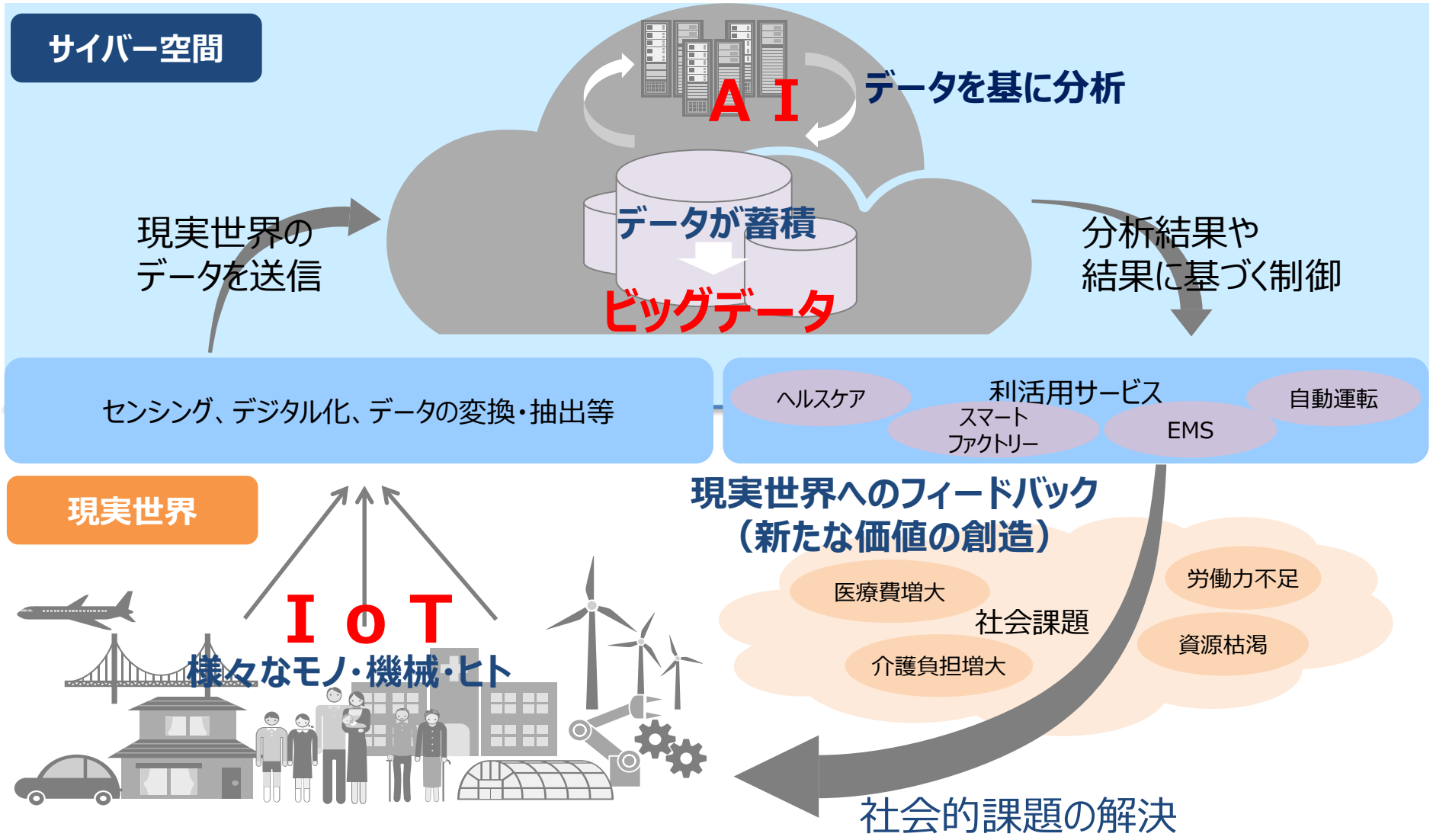
2015年6月: **米国の人事管理局（OPM）**が不正にアクセスされ、政府職員の個人情報が流出（**不正アクセス**）

2015年12月: **ウクライナの電力会社**のシステムがマルウェアに感染し、停電が発生（**標的型攻撃**）

2016年10月: **米国のDyn社**のDNSサーバが大規模なDDoS攻撃を受け、同社のDNSサービスの提供を受けていた企業のサービスにアクセスしにくくなる等の障害が発生（**DDoS攻撃**）

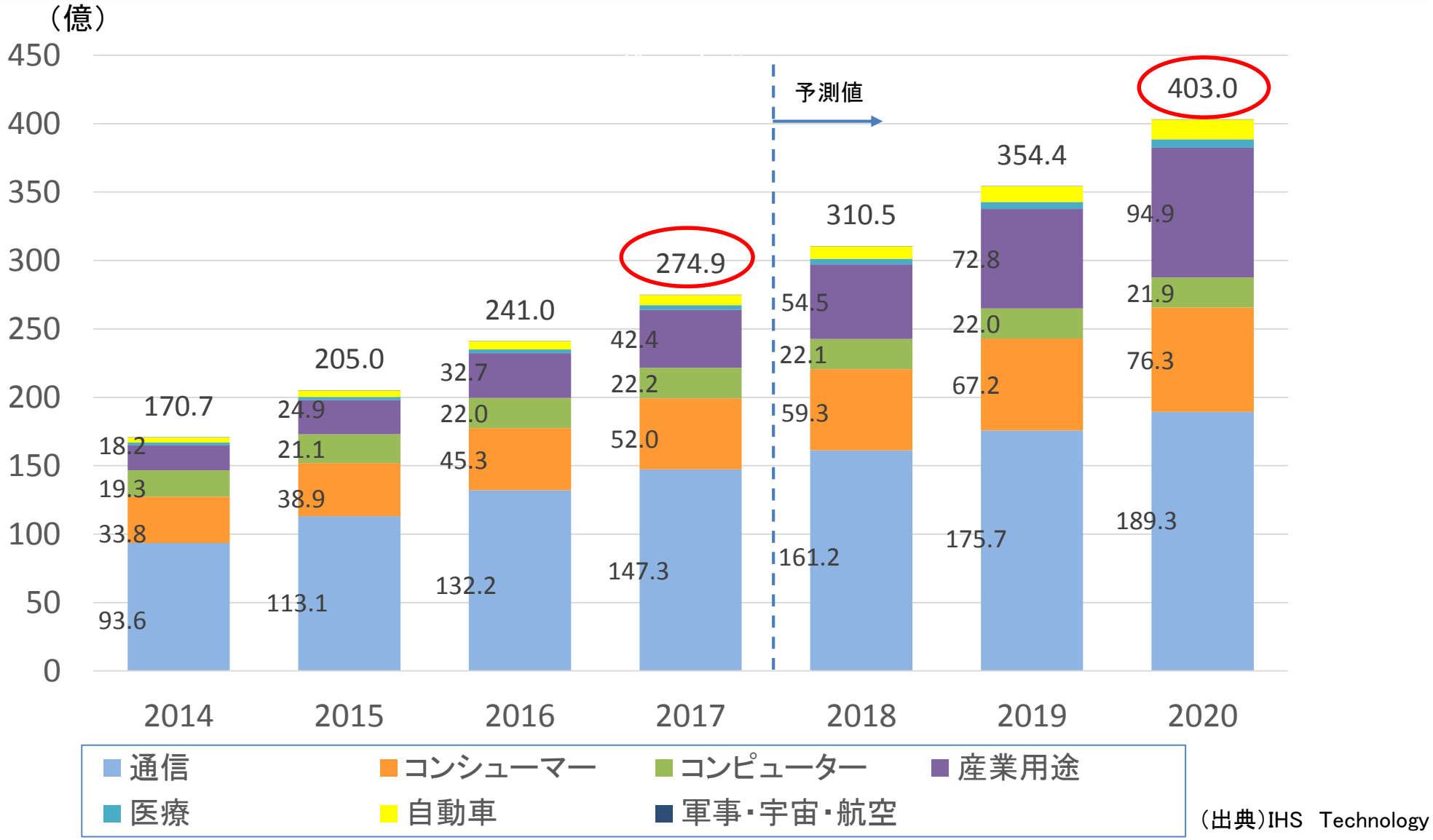
2017年5月: 世界各国（アメリカ、イギリス、中国、ロシア等）で**WannaCry**の感染被害が発生。行政、民間企業、医療等の多くの組織に影響を及ぼした。（**ランサムウェア**）

Society5.0の実現に向けたサイバーセキュリティの重要性



IoT機器の増加

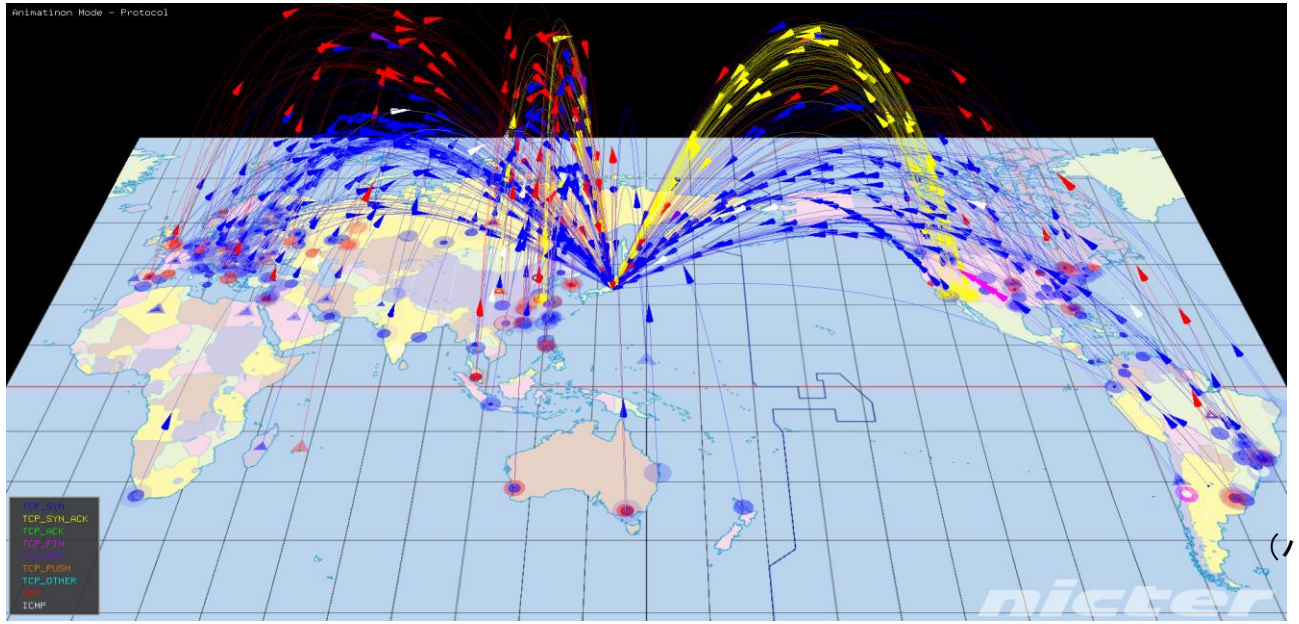
○ IHS Technology の推定によれば、2017年時点でインターネットにつながるモノ（IoT機器）の数は275億個であり、2020年までに約1.5倍の403億個まで増加する見込み。

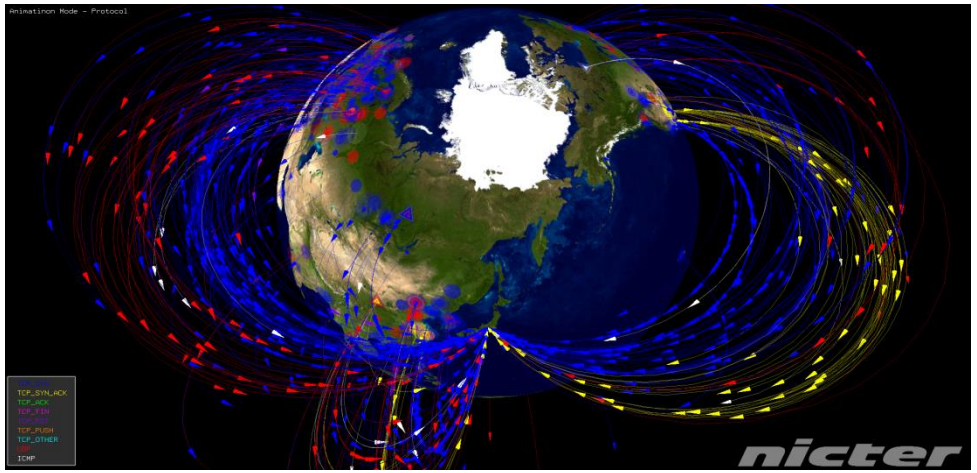


（出典）IHS Technology

IoT機器を狙った攻撃が急増（NICTERによる観測）

➢ 国立研究開発法人 情報通信研究機構（NICT）では、未使用のIPアドレスブロック30万個（ダークネット）を活用し、グローバルにサイバー攻撃の状況を観測。





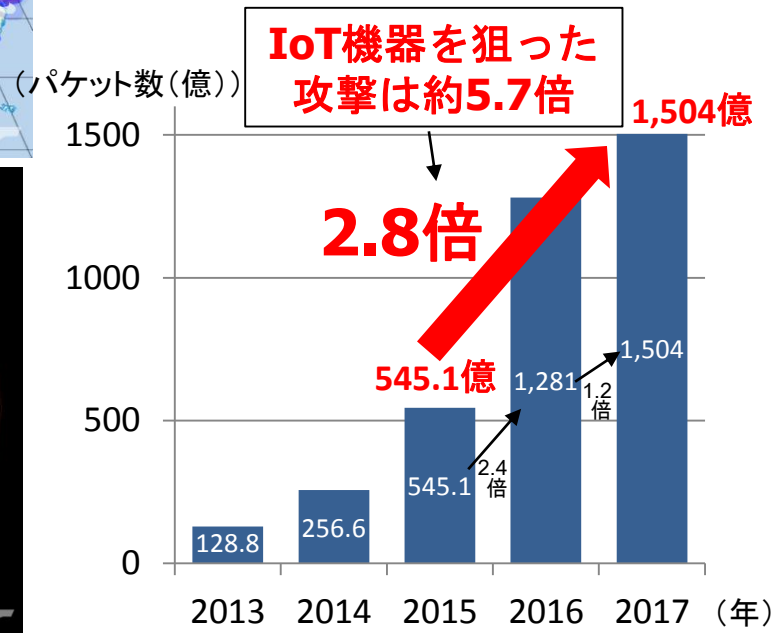
- TCP SYN
- TCP SYN/ACK
- TCP ACK
- TCP FIN
- TCP RESET
- TCP PUSH
- TCP Other
- UDP
- ICMP

・ダークネットに飛来するパケットの送信元アドレスから緯度・経度を推定し、世界地図上で可視化

・色：パケットごとにプロトコル等を表現

NITCERで１年間に観測されたサイバー攻撃回数

・2年間で2．8倍
（2015年→2016年：2．4倍、2016年→2017年：1．2倍）



IoT機器のセキュリティ上の課題

- IoT機器は、製造業者や利用者が機器のセキュリティ対策を講じる上で制約があり、長期間インターネットに接続されることから、乗っ取られやすく、サイバー攻撃に用いられやすい
- また、IoT機器は数が多く、今後も急増する見込みであるため、乗っ取られる機器数も多くなり、攻撃に用いられるとインターネットの通信に著しい支障が生じるおそれがある

従来のインターネットに接続される機器とIoT機器の特徴の比較

PC等の従来機器	センサーや家電等のIoT機器
● 機器の演算処理能力が比較的高く、アンチウィルスソフトやファイアウォール等のセキュリティソフトの導入による高度な対策が可能	● 機器の演算処理能力が比較的低く、アンチウィルスソフトやファイアウォール等のセキュリティソフトの導入による高度な対策は困難
● 機器のライフサイクルが短く、脆弱性を有する機器も一定期間後にセキュリティ強度の高い新たな機器に置き換わる見込み	● 機器のライフサイクルが長く、10年以上の長期にわたって利用されるものも多いため、脆弱性を有したままネットワークに接続され続けるおそれ
● 画面等を通じた、人的管理が容易	● 画面等がないものが多く、人的管理が困難
● ネットワークに接続される機器数は多いが、IoT機器と比べ今後の増加数は少ない見込み	● ネットワークに接続される機器数が膨大であり、今後も急増する見込み

サイバーセキュリティ戦略（2018年7月27日閣議決定）の全体構成

○ サイバーセキュリティ基本法に基づく２回目の「サイバーセキュリティに関する基本的な計画」。2020年以降の目指す姿も念頭に、我が国の基本的な立場等と今後３年間（2018年～2021年）の諸施策の目標及び実施方針を国内外に示すもの。

1 策定の趣旨・背景

- サイバー空間がもたらす人類が経験したことのないパラダイムシフト（Society5.0）
- サイバー空間と実空間の一体化の進展に伴う脅威の深刻化、2020年東京大会を見据えた新たな戦略の必要性

2 サイバー空間に係る認識

- 人工知能（AI）、IoTなど科学的知見・技術革新やサービス利用が社会に定着し、人々に豊かさをもたらしている。
- 技術・サービスを制御できなくなるおそれは常に内在。IoT、重要インフラ、サプライチェーンを狙った攻撃等により、国家の関与が疑われる事案も含め、多大な経済的・社会的損失が生ずる可能性は指数関数的に拡大

3 本戦略の目的

- 基本的な立場の堅持（基本法の目的、基本的な理念（自由、公正かつ安全なサイバー空間）及び基本原則）
- 目指すサイバーセキュリティの基本的な在り方：持続的な発展のためのサイバーセキュリティ（サイバーセキュリティエコシステム）の推進。３つの観点（①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働）からの取組を推進

4 目的達成のための施策

経済社会の活力の向上及び持続的発展

～新たな価値創出を支えるサイバーセキュリティの推進～

- 新たな価値創出を支えるサイバーセキュリティの推進
- 多様なつながりから価値を生み出すサプライチェーンの実現
- 安全なIoTシステムの構築

国民が安全で安心して暮らせる社会の実現

～国民・社会を守る任務を保証～

- 国民・社会を守るための取組
- 官民一体となった重要インフラの防護
- 政府機関等におけるセキュリティ強化・充実
- 大学等における安全・安心な教育・研究環境の確保
- 2020年東京大会とその後を見据えた取組
- 従来の枠を超えた情報共有・連携体制の構築
- 大規模サイバー攻撃事態等への対処態勢の強化

国際社会の平和・安定及び我が国の安全保障への寄与

～自由、公正かつ安全なサイバー空間の堅持～

- 自由、公正かつ安全なサイバー空間の堅持
- 我が国の防御力・抑止力・状況把握力の強化
- 国際協力・連携

横断的施策

- 人材育成・確保
- 研究開発の推進
- 全員参加による協働

5 推進体制

内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化を図るとともに、同センターが調整・連携の主導的役割を担う。

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）

IoT機器の脆弱性調査

● IoT機器などを悪用した**サイバー攻撃の深刻化**を踏まえ、国立研究開発法人情報通信研究機構（NICT）の業務に、**パスワード設定等に不備のあるIoT機器の調査**等を追加（**5年間の時限措置**）する等を内容とする**国立研究開発法人情報通信研究機構法を平成30年5月に改正。**　※ 改正法の施行日は平成30年11月1日

サイバー脅威の深刻化

•IoT機器の急激な増加に伴い、IoT機器を踏み台とするサイバー攻撃の脅威が顕在化。

※IoT機器を狙った攻撃は全体の3分の2（2016年）

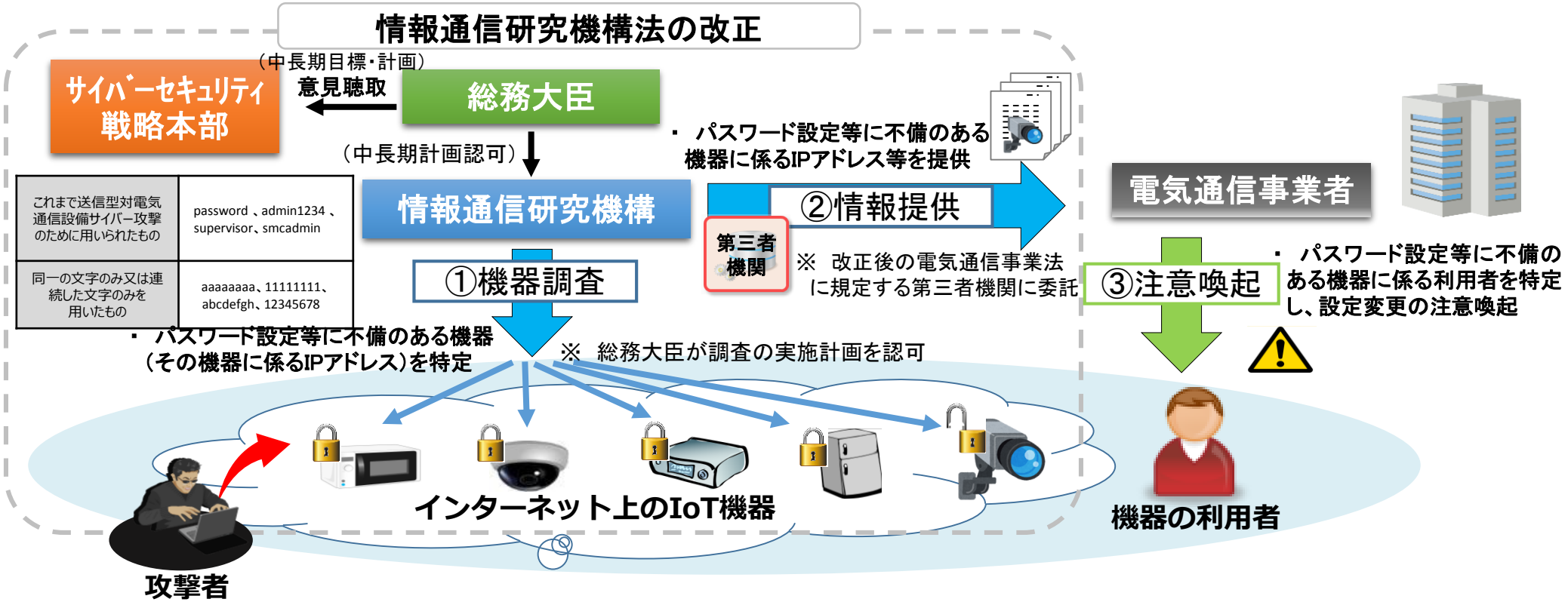
対策の必要性

•パスワード設定等に不備のあるIoT機器の実態を把握するため、調査機能の強化が急務。

体制の整備

•NICTに機器調査に係る業務を追加し、電気通信事業者と連携しつつ対策を推進（下図）。

情報通信研究機構法の改正



研究開発の推進

広域ネットワークスキャンの軽量化

ハードウェア脆弱性への対応

国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

NICTにおける基礎的・
基盤的な研究開発の推進

スマートシティのセキュリティ
対策の強化

AIを活用したサイバー攻撃
検知・解析技術の研究開発

衛星通信におけるセキュリティ技術
の研究開発発

企業におけるサイバー攻撃被害の状況

表 1：2017 年 個人情報漏えいインシデント 概要データ【速報】

漏えい人数	519 万 8,142 人
インシデント件数	386 件
想定損害賠償総額	1,914 億 2,742 万円
一件当たりの平均漏えい人数	1 万 4,894 人
一件当たり平均損害賠償額	5 億 4,850 万円
一人当たり平均損害賠償額	2 万 3,601 円

表 2：2017 年 個人情報漏えいインシデント トップ 10

No.	漏えい人数	業種	原因
1	118 万 8,355 人	製造業	不正アクセス
2	67 万 6,290 人	公務	不正アクセス
3	59 万 7,452 人	情報通信業	不正アクセス
4	37 万 1,200 人	情報通信業	不正アクセス
5	19 万 9,169 人	公務	不正アクセス
6	19 万人	サービス業	管理ミス
7	18 万 4,981 人	公務	管理ミス
8	16 万 3,000 人	公務	紛失・置忘れ
9	14 万　408 人	情報通信業	不正アクセス
10	13 万 1,936 人	卸売業，小売業	不正アクセス

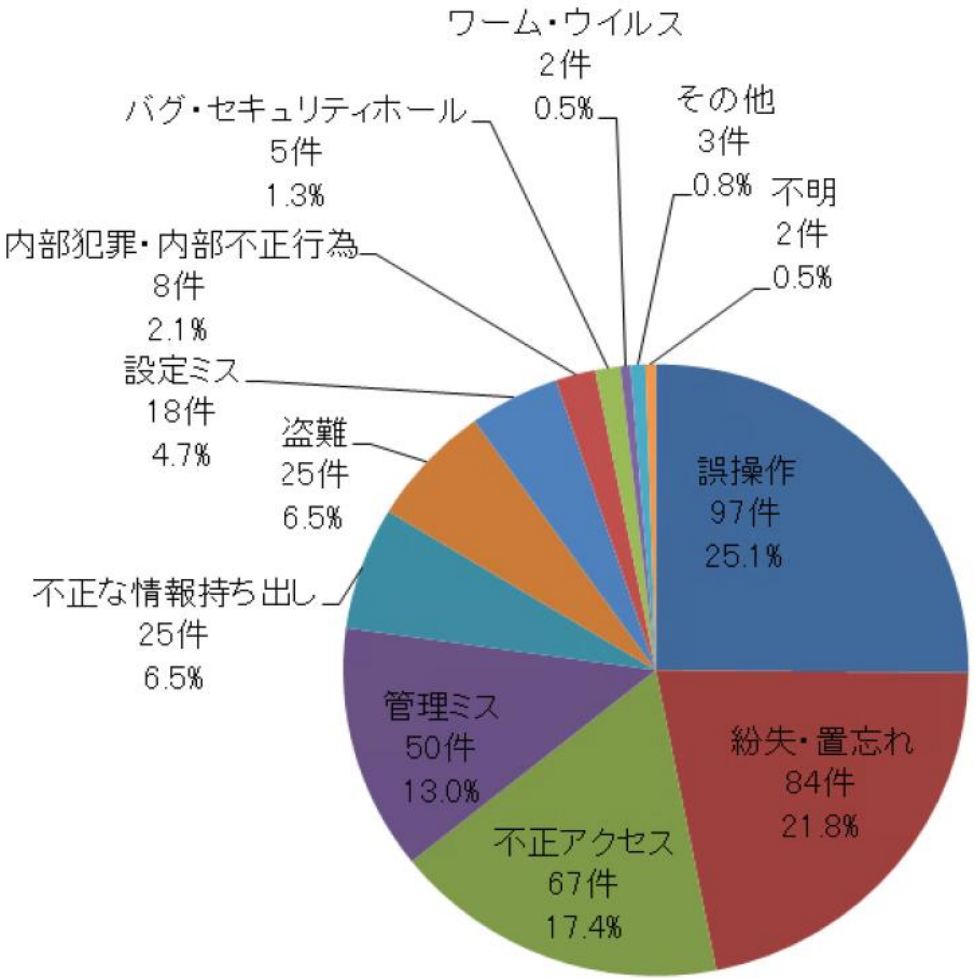


図 3：原因別の漏えい件数

（出典）JNSA＆長崎県立大学“2017年情報セキュリティインシデントに関する調査報告書（速報版）”（2018年6月）

セキュリティ人材の育成（ナショナルサイバートレーニングセンター）

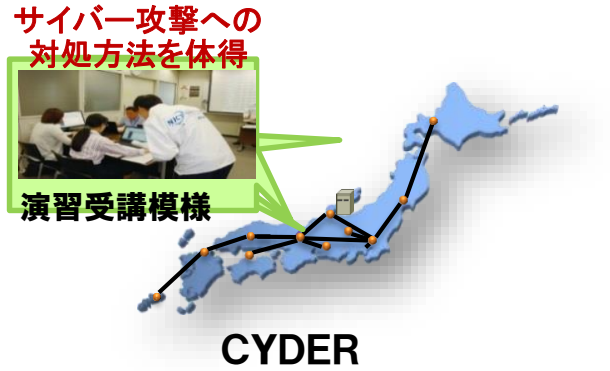
○　巧妙化・複合化するサイバー攻撃に対し、実践的な対処能力を持つセキュリティ人材を育成するため、平成２９年４月より、情報通信研究機構（NICT）の「ナショナルサイバートレーニングセンター」において、以下の実践的サイバー演習等を積極的に推進。

① 国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者等を対象とした実践的サイバー防御演習（CYDER）
　⇒ 平成29年度は3009名が受講。平成30年度においても同規模で実施予定。

② 2020年東京オリンピック・パラリンピック競技大会に向けた大会関連組織のセキュリティ担当者等を対象者とした実践的サイバー演習（サイバーコロッセオ）
　⇒ 平成29年度は74名が受講。平成30年度は最大150名規模で実施予定。

③ 若手セキュリティイノベーターの育成（SecHack365）
　⇒ 平成29年度は39名が１年間のプログラムを修了。平成30年度は50名を受講者として選定。

新たな手法のサイバー攻撃にも対応できる演習プログラム・教育コンテンツを開発



CYDER

サイバーコロッセオ


SecHack365

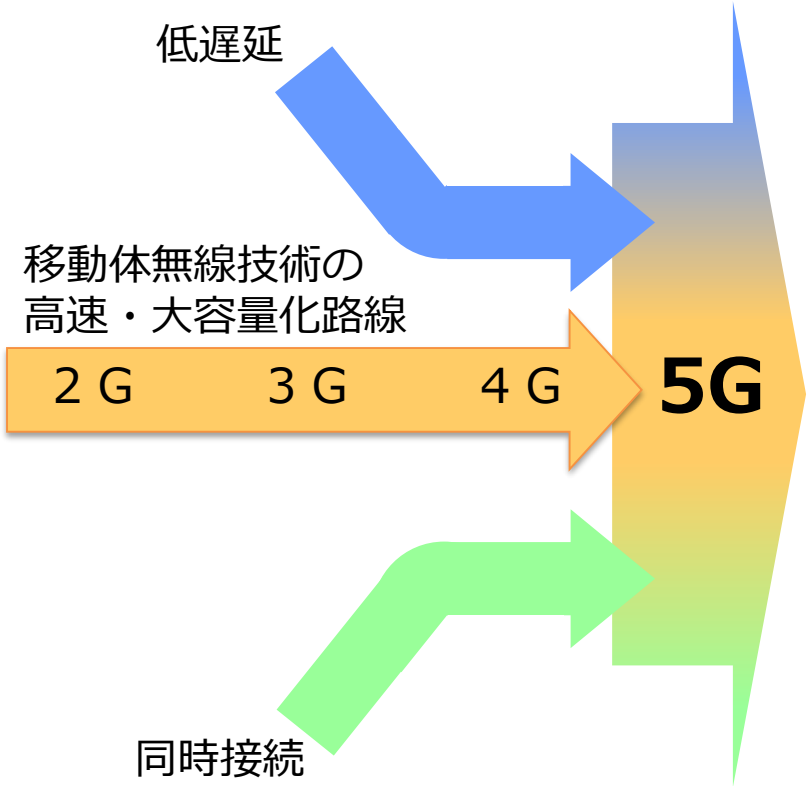
国際連携の推進


国際標準化の推進
国際的なISAC間連携
ASEAN各国との連携
サイバー空間における
国際ルールを巡る議論
への積極的参画

第５世代移動通信システム(5G)とは

<5Gの主要性能>		
	超高速	最高伝送速度 10Gbps （現行LTEの100倍）
	超低遅延	1ミリ秒程度の遅延 （現行LTEの1/10）
	多数同時接続	100万台/km²の接続機器数 （現行LTEの100倍）

5Gは、AI/IoT時代のICT基盤



超高速

現在の移動通信システムより100倍速いブロードバンドサービスを提供

⇒ **２時間の映画を３秒でダウンロード**

超低遅延

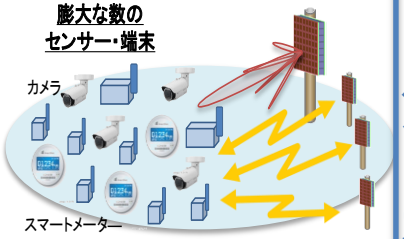
利用者が遅延（タイムラグ）を意識することなく、リアルタイムに遠隔地のロボット等を操作・制御

ロボットを遠隔制御

⇒ **ロボット等の精緻な操作をリアルタイム通信で実現**

多数同時接続

スマホ、PCをはじめ、身の回りのあらゆる機器がネットに接続



⇒ **自宅部屋内の約100個の端末・センサーがネットに接続**
（現行技術では、スマホ、PCなど数個）

社会的なインパクト大

ご清聴ありがとうございました

総務省
Ministry of Internal Affairs and Communications