総務省

# データ主導社会と
# サイバーセキュリティ

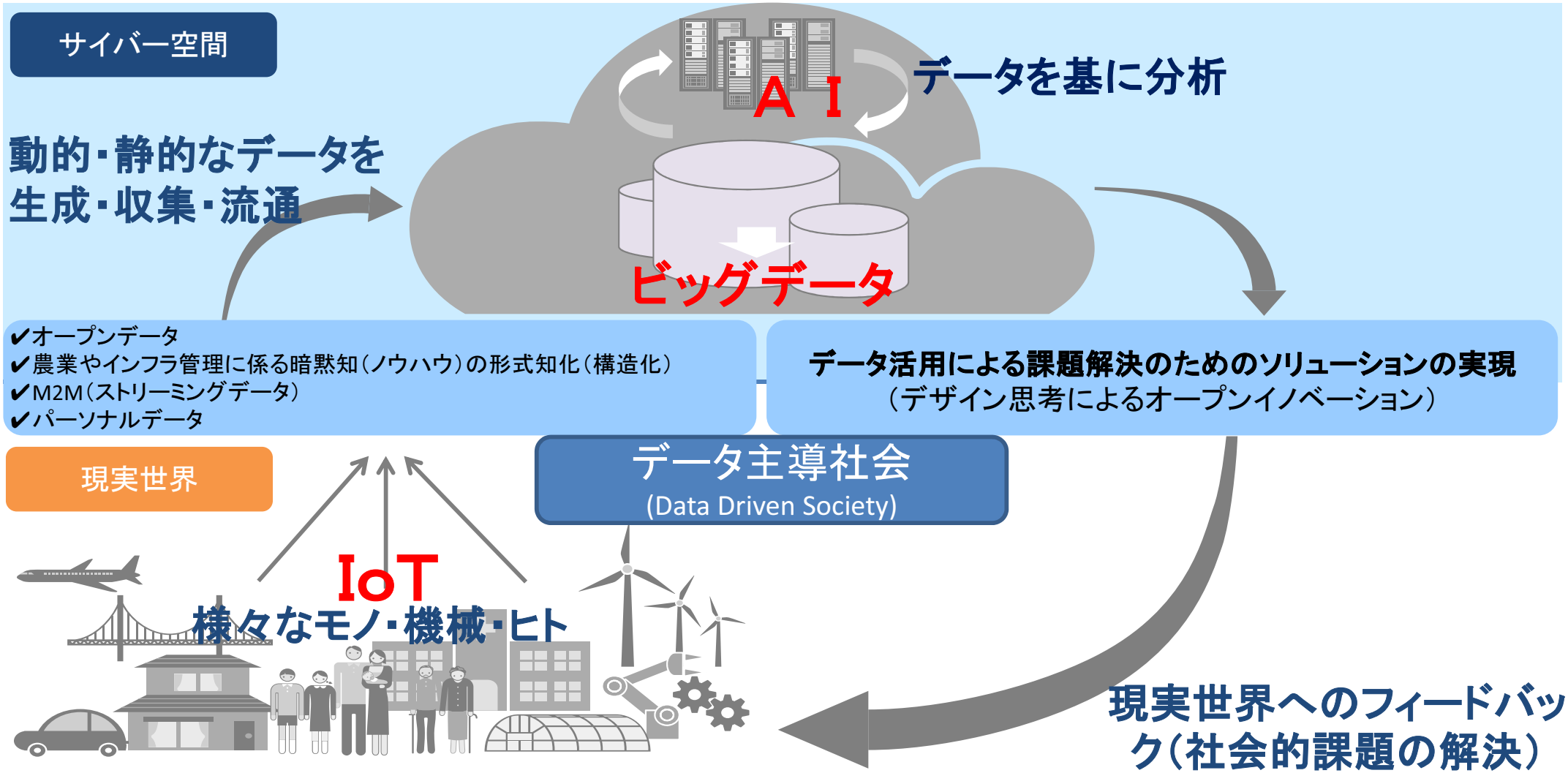
2017年8月9日

**総務省政策統括官（情報セキュリティ担当）**

**谷　脇　　康　彦**

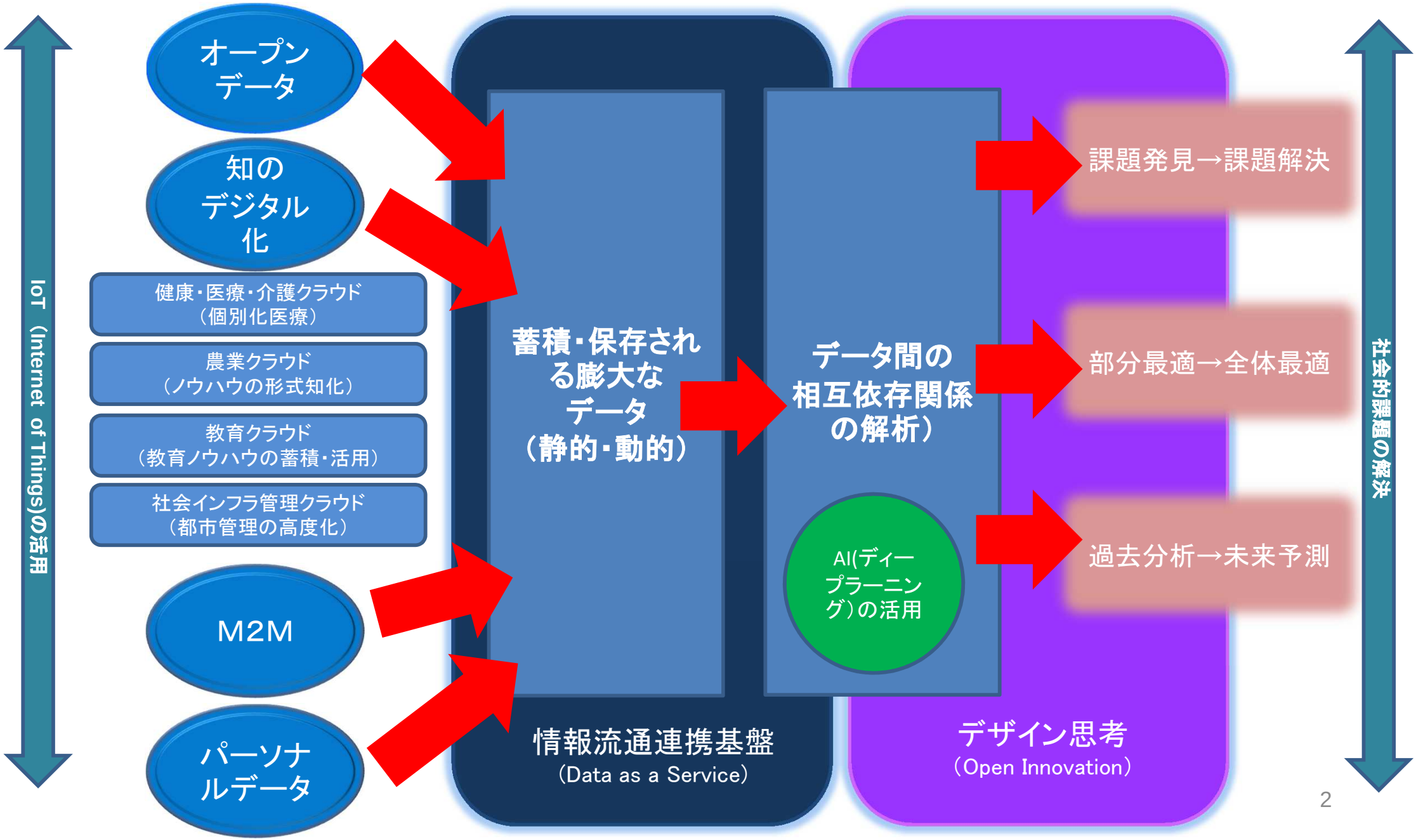
# データ主導社会：基本的枠組み





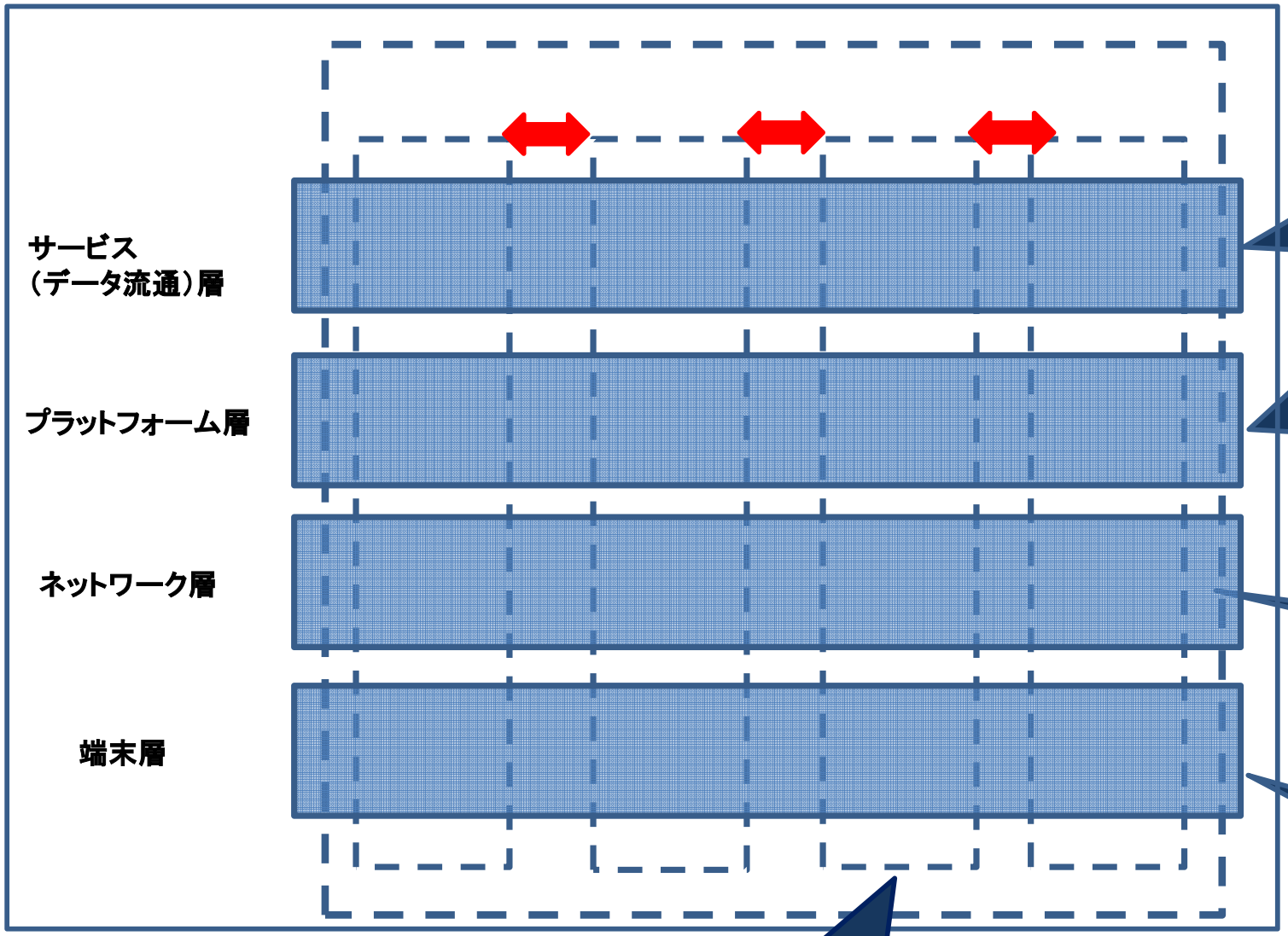
# データ主導社会（Data Driven Society）





# IoT総合戦略（2017年1月）






## レイヤー別施策

■データ利活用の促進等に必要なルールの明確化等
■データ取引市場の整備
■分野横断的なデータ連携環境の整備

■認証連携基盤の構築
■パーソナルデータの活用と個人の情報コントローラビリティの確保（privacy by design）
■システミックリスクへの対応（security by design）

■SDN/NFVの実装化
■5Gの実現
■ICT人材の育成

■安心安全な自律型モビリティシステム
■多様なIoT端末の効率的な管理運用
■次世代AI技術の研究開発及び社会実装に向けた取組の推進

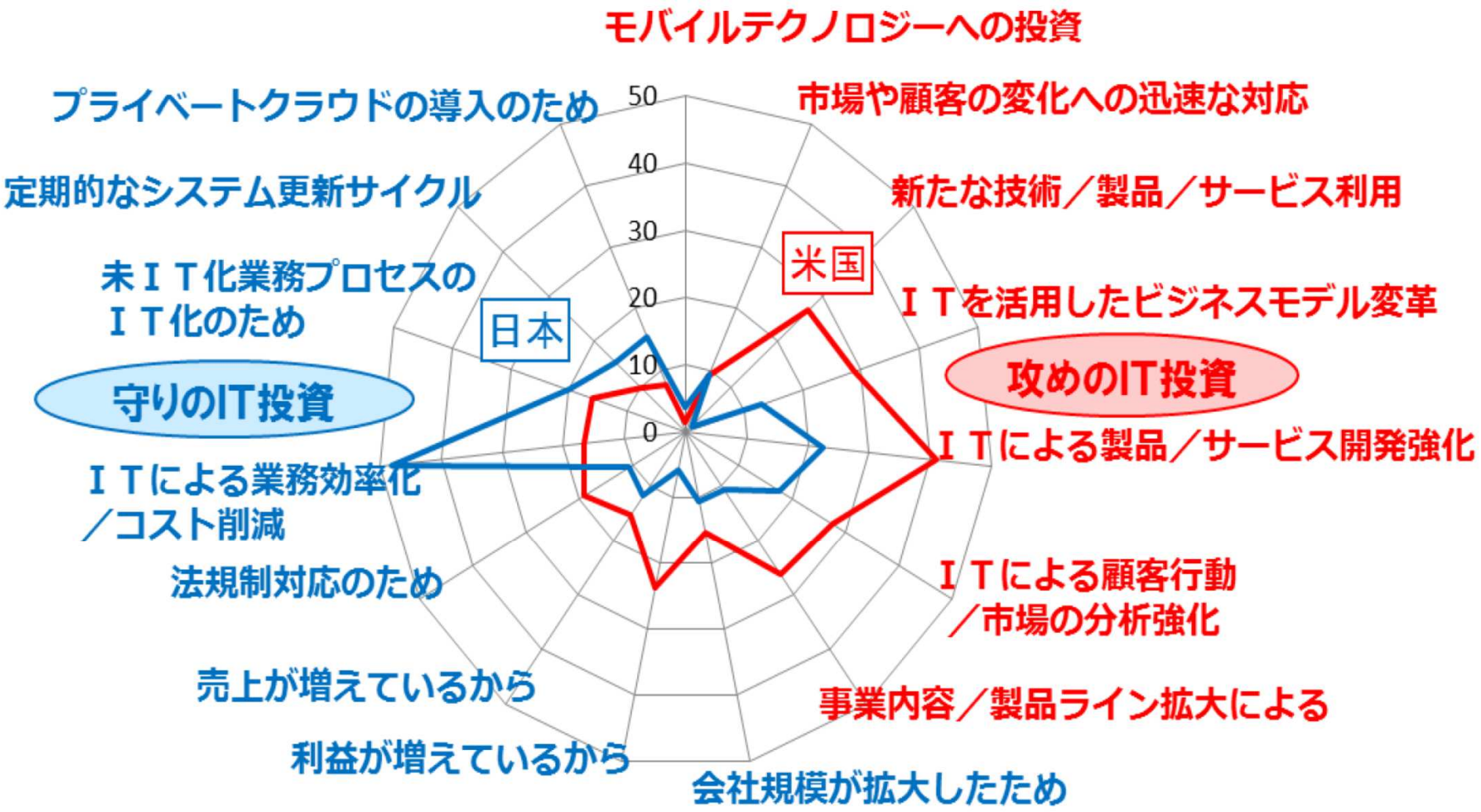
## レイヤー縦断（垂直）型施策

■地域におけるIoTの普及促進
■AIネットワーク化の推進
■国際的な政策対話と国際標準化の推進

# IT投資の日米比較



**これまでのIT予算を増額する企業における増額予算の用途（日米比較）**




※出典：一般社団法人　電子情報技術産業協会（JEITA）、IDC Japan（株）「ITを活用した経営に対する日米企業の相違分析」調査結果（2013年10月）



（参考）「平成28年情報通信に関する現状報告」（「情報通信白書」）より引用。

# 2030年までの経済成長シナリオ（17年情報通信白書）



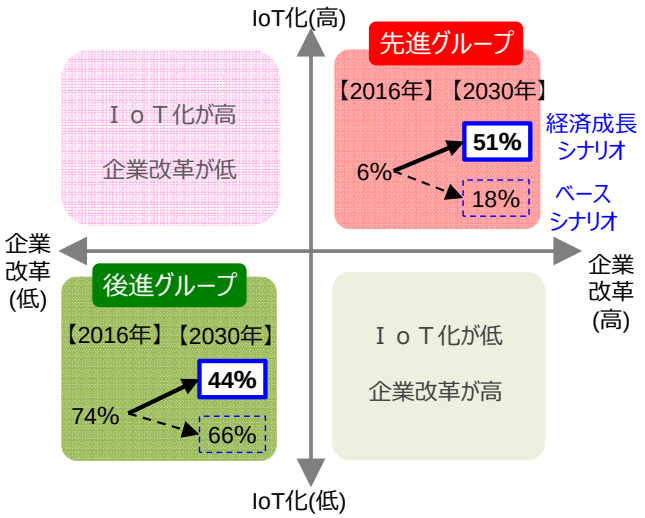
## 2030年までの経済成長経路

IoT化（※1）
企業改革（※2）
→ ICT投入額の増加 → 実質GDPの増加

**※1 IoT化**
・IoT・AIの導入

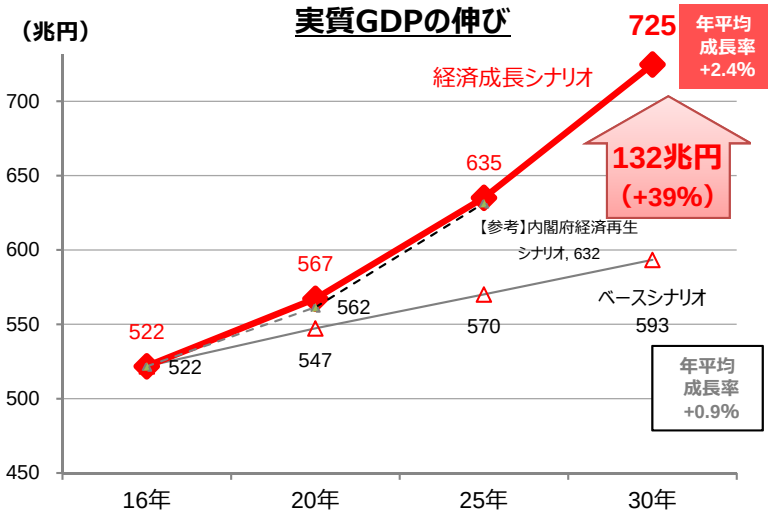
**※2 企業改革**
・社内・外での業務改革
・人材面の対応・投資
・知的財産投資
・海外投資
・M&A

### 2つのシナリオ下での企業分類




## IoT化のインパクト

### 実質GDPの伸び




**● 内閣府試算**

年に2回「中長期の経済財政に関する試算」を経済財政諮問会議に提出。
2025年までの間「経済再生」と「ベースライン」の2つのシナリオを置いている。
・経済再生：中長期的に経済成長率が実質2%、名目3%以上になると想定。
・ベースライン：経済が足元の潜在成長率並みで推移し、中長期的に経済成長率は実質1%弱、名目1%半ば程度になると想定

**● 情報通信白書における試算**

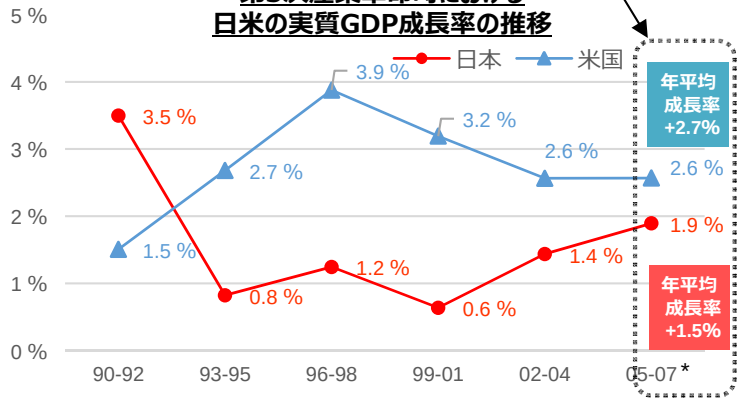
内閣府試算を参考にしつつ、IoT化と企業改革が進展することで、企業の生産性向上や新商品・新サービスによる需要創出の発現時期が早まり、ベースシナリオから各種変数が変化すると想定。

| | 項目 | 16年 | 20年 | 25年 | 30年 |
|---|---|---|---|---|---|
| 経済成長シナリオ | 実質GDP | 100 | 109 | 122 | 139 |
| | 実質ICT投入 | 100 | 139 | 197 | 285 |
| ベースシナリオ | 実質GDP | 100 | 105 | 109 | 114 |
| | 実質ICT投入 | 100 | 114 | 129 | 146 |

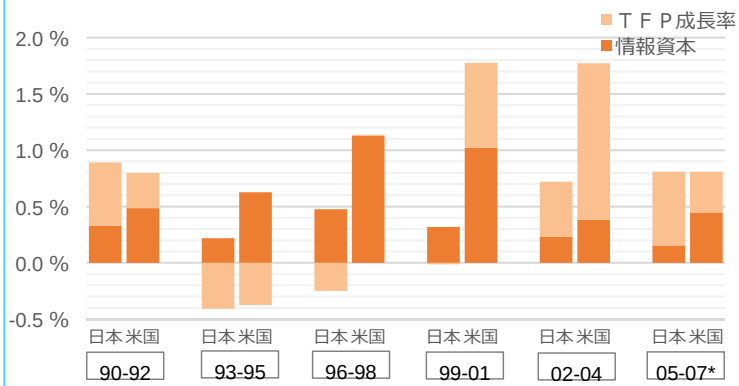
## 【参考】「第３次産業革命（1990-）」の検証

第3次産業革命（ICT革命）において、我が国では情報資本が蓄積され経済成長が見られたものの、米国ではより高い成長を実現

### 第3次産業革命時における日米の実質GDP成長率の推移




### 日米のTFP及び情報資本の実質成長率への寄与




*TFP(全要素生産性)： 生産要素(資本、労働)以外で付加価値増加に寄与する部分。技術の進歩や、無形資本の蓄積、労働者のスキル向上、経営効率の改善などを表す。

（参考）「平成29年情報通信に関する現状報告」（「情報通信白書」）より引用。

# 未来投資戦略2017（17年6月）



## Ⅰ. Society 5.0に向けた戦略分野

### 1. 健康寿命の延伸
- **データ利活用基盤の構築**
- 保険者・経営者による「個人の行動変容の本格化」
- 遠隔診療、AI開発・実用化
- 自立支援に向けた科学的介護の実現
- 革新的な再生医療等製品等の創出促進、医療・介護の国際展開の推進

### 2. 移動革命の実現
- 世界に先駆けた実証
- データの戦略的収集・活用、協調的領域の拡大
- 国際的な制度間競争を見据えた制度整備

### 3. サプライチェーンの次世代化
- データ連携の制度整備
- データ連携の先進事例創出・展開

### 4. 快適なインフラ・まちづくり
- インフラ整備・維持管理の生産性向上

### 5. FinTech

## Ⅱ. Society 5.0に向けた横割課題

**価値の源泉の創出**

### 1. データ利活用基盤・制度構築
- 公共データのオープン化
- 社会のデータ流通促進、知財・標準の強化

### 2. 教育・人材力の抜本強化
- 世界に先駆けた実証
- データの戦略的収集・活用、協調的領域の拡大
- 国際的な制度間競争を見据えた制度整備

### 3. イノベーション・ベンチャーを生み出す好循環システム

**価値の最大化を後押しする仕組み**

### 1. 規制の「サンドボックス」の創設
### 2. 規制改革・行政手続簡素化・IT化の一体的推進
### 3. 「稼ぐ力」の強化
### 4. 公的サービス・資産の民間開放
### 5. 国家戦略特区の加速的推進
### 6. サイバーセキュリティ
### 7. シェアリングエコノミー

## Ⅲ. 地域経済好循環システムの構築

## Ⅳ. 海外の成長市場の取り組み

# IoT総合戦略（2017年1月）：具体的施策



データ利活用型スマートシティ

情報取引市場・情報銀行に係る環境整備

IoT人材の育成

ブロックチェーン技術の活用

＋

サイバーセキュリティ対策の強化

# データ利活用型スマートシティ

# 海外におけるスマートシティ　–デンマーク・コペンハーゲン市–



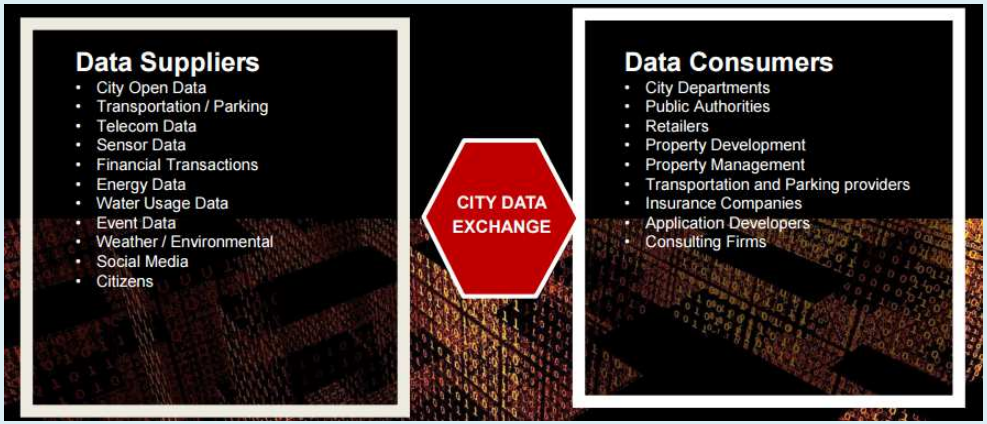
## プラットフォームの概要

- 個々のデータを1つのプラットフォームに統合し、データ収集、統合、共有を一元化。



## データ利活用の方法

- 街灯にWi-Fi等を設置し、人や車、バイクなどの移動データを分析。
- 交通車両をリアルタイムで追跡し、信号機等の最適化を図り、CO2の削減と移動時間の短縮を実現。
- 携帯電話、ゴミ箱に設置したセンサー、下水処理システム等から大気質やCO2排出量に関するデータを回収し、大気汚染の改善やCO2排出量の削減に活用。
- コペンハーゲン空港の利用者の携帯電話からのWi-Fiアクセスにより、位置と動きをリアルタイムで3Dマッピングし、行動・利用予測に活用。
- 集めたビックデータは、企業間による都市ビッグデータ取引市場の創設（City Data Exchange）や、公共・民間データの統合に活用する予定。




＜City Data Exchangeのイメージ＞

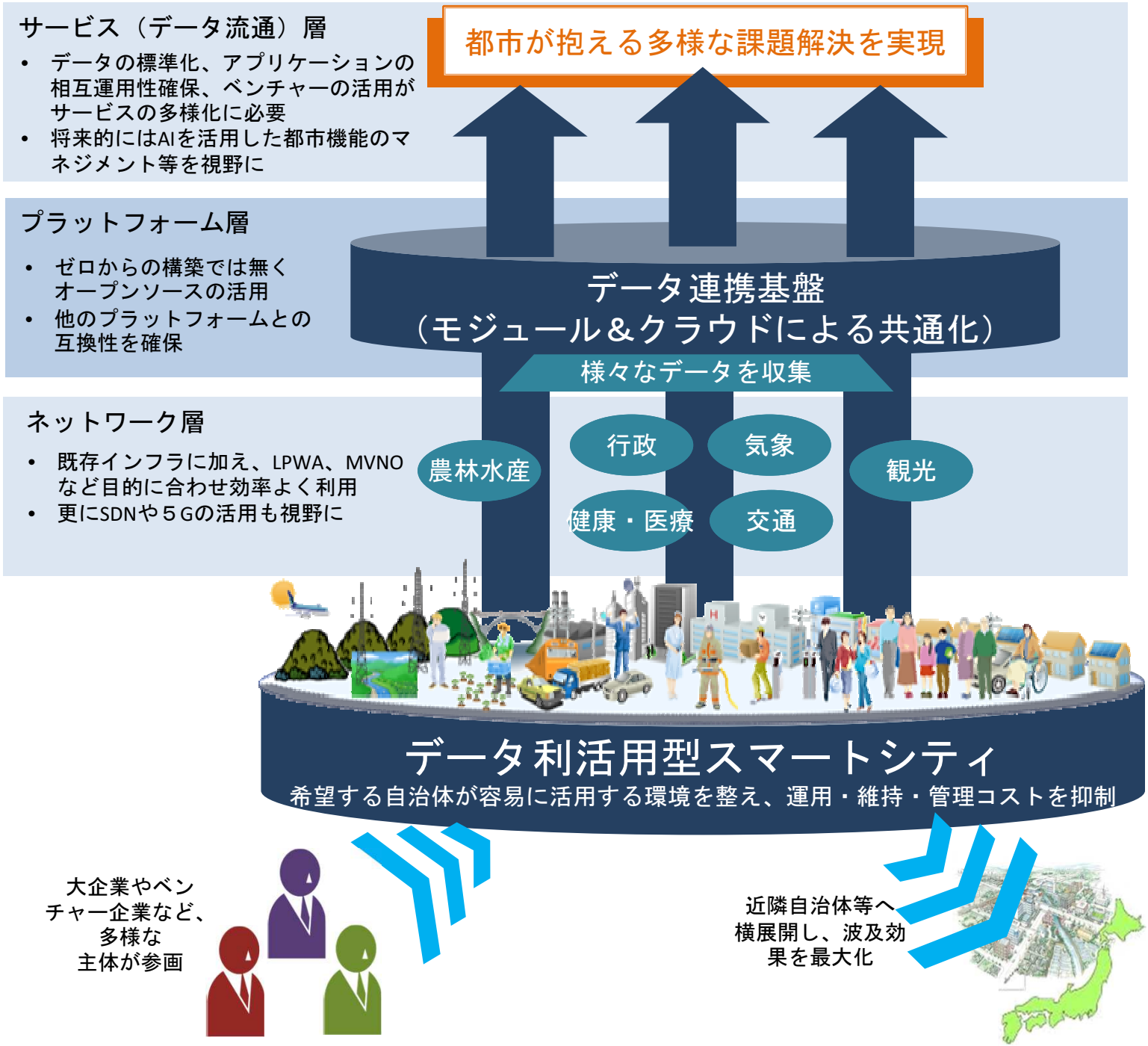
交通、エネルギー、水、ソーシャルメディア等のデータを、市・公共機関、各民間企業（リテール事業者、不動産屋、保険会社、アプリケーション開発者、コンサルタント等）に提供。



（出典）ICT街づくり推進会議スマートシティ検討WG第４回野村総合研究所説明

# データ利活用型スマートシティの基本構想






## 対象

- 拡張可能性や持続可能性の観点から、都市全体、鉄道沿線、街区が主たる対象
- スクラッチからの開発と既存の街の再開発への導入の2種類があることに留意

## 計画段階

- ICT関連事業者が街づくり計画段階の初期から参画
- 自治体の首長による強いコミットメント
- 全体を統括して横串を通す自治体内の組織

## 構築段階

- PPP/PFIなど民間と連携したファイナンスを活用
- 地元の有志企業からの出資
- ソーシャルインパクトボンドの活用も考慮

## 運用段階

- 横断的なマネジメントを行う組織が鍵
- ICT企業がエリアマネジメント組織に参画し、データを利活用
- PDCAを回すことで、スマートシティのバージョンアップを図る

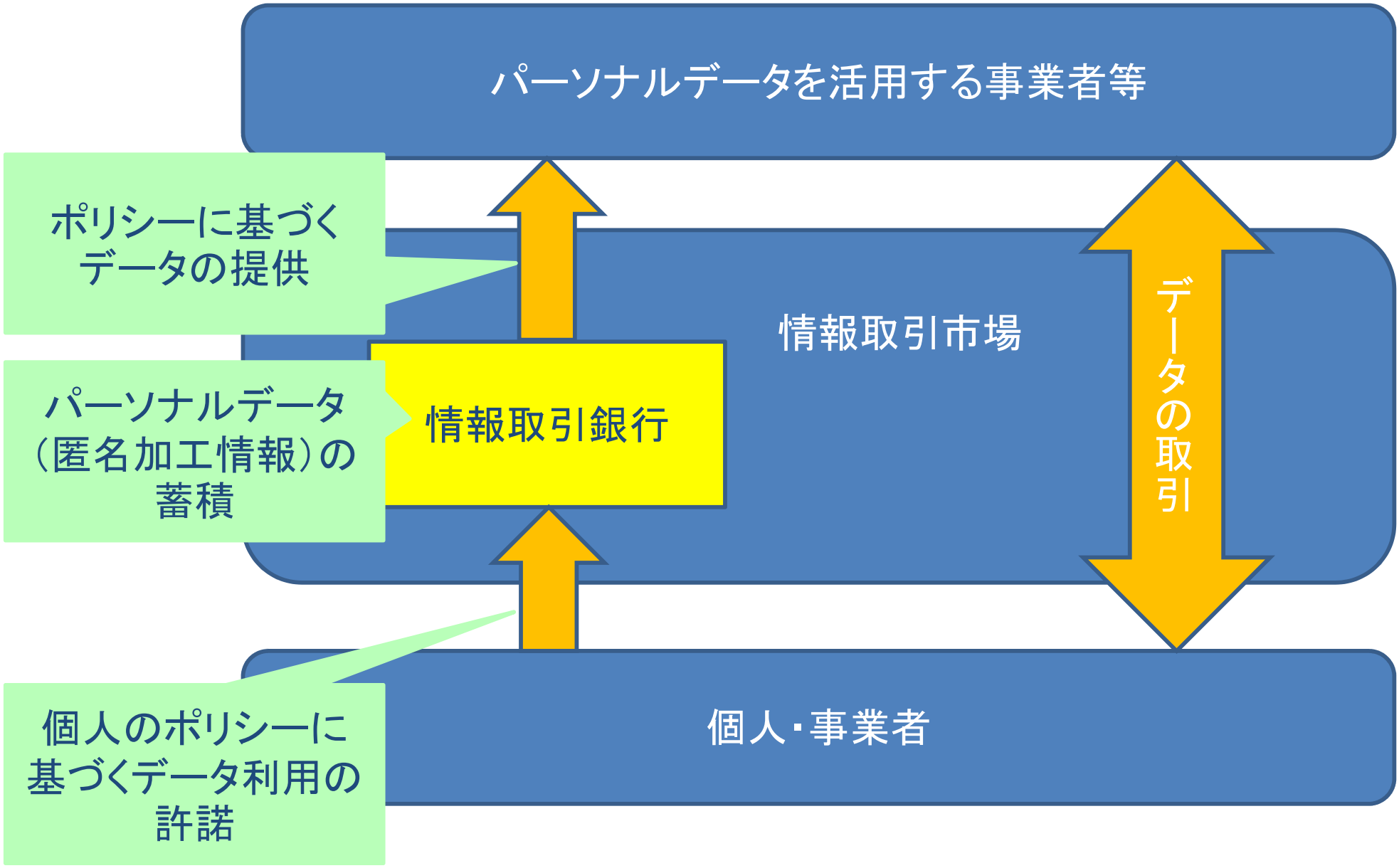
## 【地域におけるIoTの普及促進】

■地域の課題解決を促進するため、地方公共団体等に対して、データ利活用に資するIoTの地域実装に係る計画策定支援、専門人材派遣等の人的支援、必要なルールの明確化、成功事例の横展開等の民間資金・ノウハウを活用した施策のパッケージ支援及び共通するオープンなプラットフォーム上で観光、防災等の分野でデータを利活用してサービスを提供するスマートシティの構築を積極的に行い、2020年度までに延べ800以上の地域・団体による成功事例を創出する。

# 情報取引市場・情報銀行に係る環境整備

# 情報取引市場




パーソナルデータを活用する事業者等
ポリシーに基づく
データの提供
情報取引市場
パーソナルデータ
（匿名加工情報）の
蓄積
情報取引銀行
データの取引
個人のポリシーに
基づくデータ利用の
許諾
個人・事業者

## 【情報取引市場等】

■個人の関与の下でパーソナルデータの流通・活用を進める仕組みであるPDS（Personal Data Store)や情報銀行、データ取引市場等について、その具体的なメリットの「見える化」に配慮しつつ、観光や医療・介護・ヘルスケア等の分野における官民連携実証事業の推進等を通じて先駆的な取り組みを後押しするとともに、具体的プロジェクトの創出に取り組む。

■実証事業や諸外国における検討状況等を踏まえてデータ流通・活用をさらに促進するため、情報銀行やデータ取引市場について、個人の関与の下で信頼性、公正性、透明性を確保するための制度の在り方などについて検討し、本年中に結論を得る。

# ブロックチェーン技術の活用

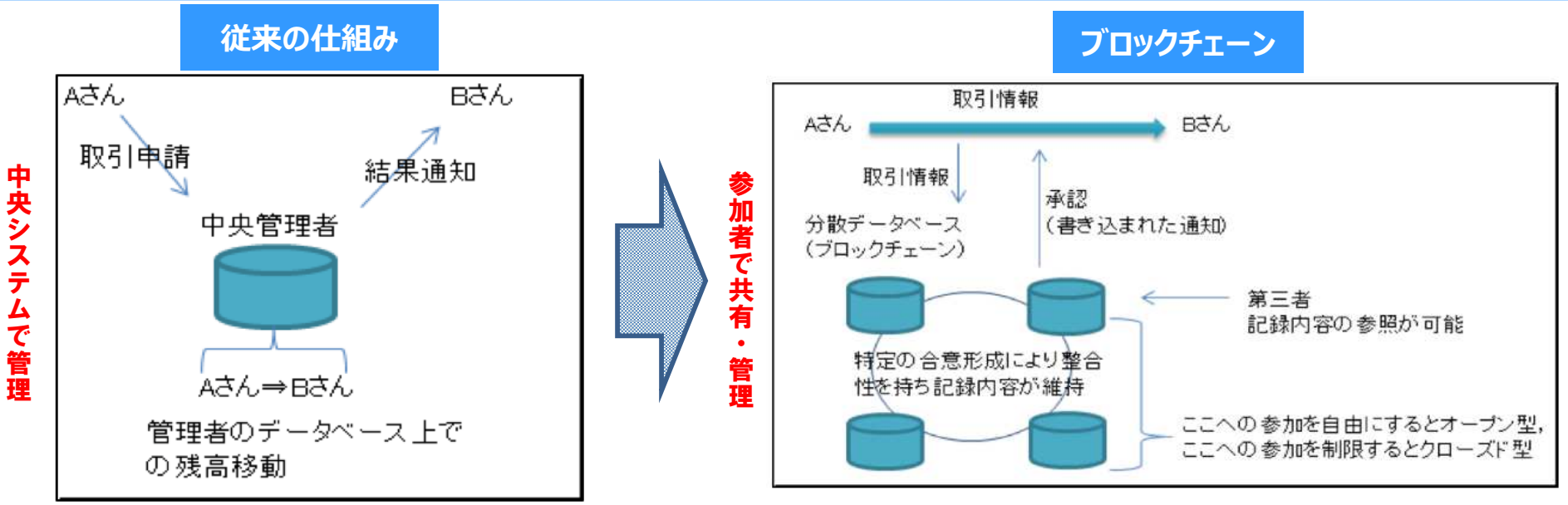
# ブロックチェーン技術の活用の可能性

○ブロックチェーンは、分散管理を基本とするデータベースの信頼性向上のための技術（**分散台帳技術**）。特定の管理者・システムで集中管理を行うのではなく、参加者全員が取引台帳を共有し、検証可能な仕組み。

○ **「改ざんが極めて困難」「落ちない（安定運用）」「効率的に構築可能」などの特色。**

○このほか、IoT機器の管理や、定期報告等の「履歴」を管理するニーズがある分野においても、効率的にデータベースを構築・管理する観点から活用の可能性。

○さらに、ブロックチェーンに書き込むデータの信頼性を確保するため、認証手段と組み合わせることで、より強固で信頼できるプラットフォームとなることも期待。

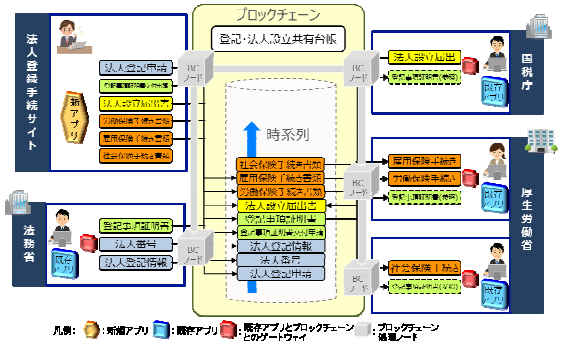
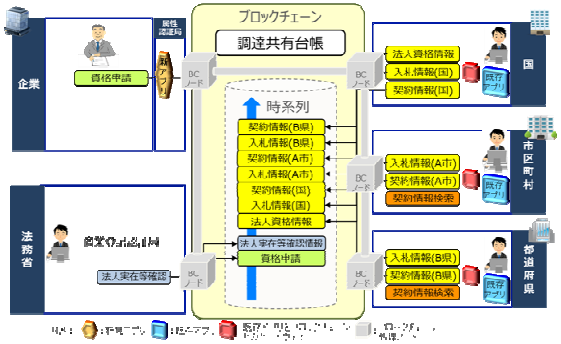
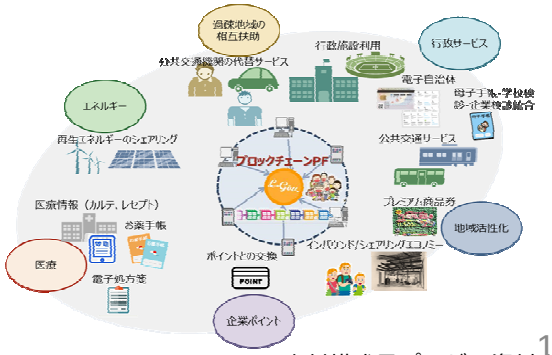



（ビットコインニュース「『ブロックチェーンとは結局何なのか』ビジネスパーソン向けに徹底解説＆ブロックチェーンの衝撃・金融サービスへの応用補足説明」（2016.7.12後藤あつし氏寄稿）から図を引用）

# ブロックチェーン技術のユースケース



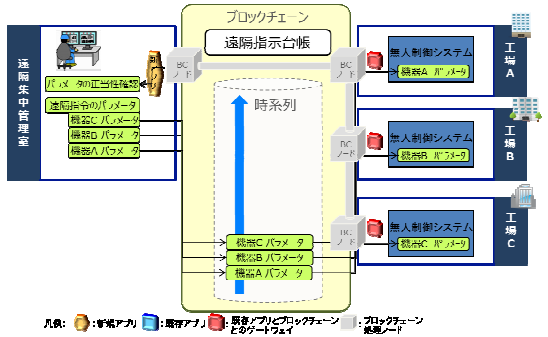
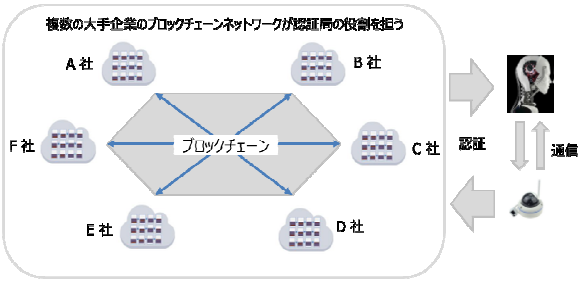
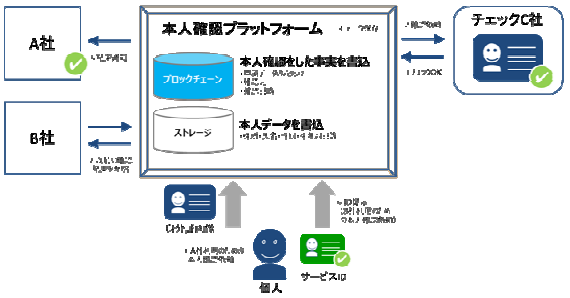
## 1．行政手続など公的分野での活用

| | ユースケース | ユースケースの概要 |
|---|---|---|
| (1) | 法人設立手続 | ・法人の設立等に伴う手続にブロッチェーンを活用し、登記事項証明書を関係行政機関で共有することで、オンラインでの登記事項証明の真正性を確保するとともに、手続の負担・コスト軽減と迅速化を実現。<br>  <br><br>貝塚構成員プレゼン資料より |
| (2) | **政府調達手続** | ・国と自治体の電子調達手続にブロックチェーンを活用し、入札参加資格申請の簡素化・共通化による官民の事務処理の効率化を図るとともに、国・自治体を通じた調達実績を共有することによって、国・自治体での調達コストの削減を実現。<br>  <br><br>貝塚構成員プレゼン資料より |
| (3) | 電子自治体 | ・地域振興ポイント等の各種ポイントの運用管理、受注先との手形債権の管理、母子保健・学校検診・企業検診をカバーするPHRの管理等、安定的かつセキュアな環境の下で、多数当事者間でのデータ共有等が必要となる住民向けサービスをブロックチェーン上でリーズナブルに提供することで、効率的な電子自治体を構築。<br>  <br><br>中村構成員プレゼン資料より |

# ブロックチェーン技術のユースケース



## 2．IoTなど民間サービスでの活用

| | ユースケース | ユースケースの概要 |
|---|---|---|
| (1) | 遠隔制御システム等におけるソフトウェアのバージョン管理 | ・遠隔制御システム等の稼働パラメータ等のソフトウェアについて、ブロックチェーンの耐改ざん性を活かして管理し、その不正書き換えを防ぐとともに、脆弱性のある箇所にセキュリティ対策を緊急に施す等の措置により、サイバー攻撃に対処。<br>  <br><br>貝塚構成員プレゼン資料より |
| (2) | **IoT機器の信頼性向上** | ・IoT機器の認証情報（どのIoT機器が通信したのか）をブロックチェーンで管理することで、認証情報の信頼性を向上するという直接の目的のほか、サイバー攻撃を探知してIoT機器のセキュリティ回復、IoT機器間の通信暗号化やIoT機器が生成するデータの真正性確保を通じたビッグデータの信頼性向上を実現。<br>  <br><br>合同会社Keychain 三島様 プレゼン資料より |
| (3) | シェアリングサービスにおける本人確認手続 | ・運転免許証やマイナンバーカード等により本人確認を行った結果をパブリックブロックチェーンに記録することにより、本人確認サービスの信頼性の向上を図るとともに、シェアリングサービスにおける本人確認を業界で共通化し、本人確認の煩雑さを解消。<br>  <br><br>北村構成員・肥後構成員プレゼン資料より |

# ブロックチェーン技術に関する諸外国の動向



## 1．エストニア

- **各省庁や民間のデータベースをインターネット経由で相互参照可能とするプラットフォーム（X-ROAD）において、ブロックチェーン技術を採用**。このプラットフォームとIDカードを用いた電子認証とを組み合わせることで、世界最先端レベルの電子政府を実現。

## 2．英国

- **政府がブロックチェーン技術を公共分野で活用する５つのユースケースを提案**するなど、ブロックチェーン技術の活用について非常に積極的に取り組んでいる国の一つ。
- ユースケースとして、**社会保障給付、国際援助といった金銭給付**をはじめ、**知的財産、特許等の登録データベースへの活用**や**ソフトウェア改ざん検知による重要インフラ防御**など、行政全般にわたってブロックチェーン技術を活用するアイデアを提案。

## 3．その他

- スウェーデン、米国、オランダなどの欧米諸国のみならず、ジョージア（グルジア）、ホンジュラス、ガーナといった途上国でも、**不動産登記や取引の記録へのブロックチェーン技術の活用**が検討されてきている。

## 【ブロックチェーン】

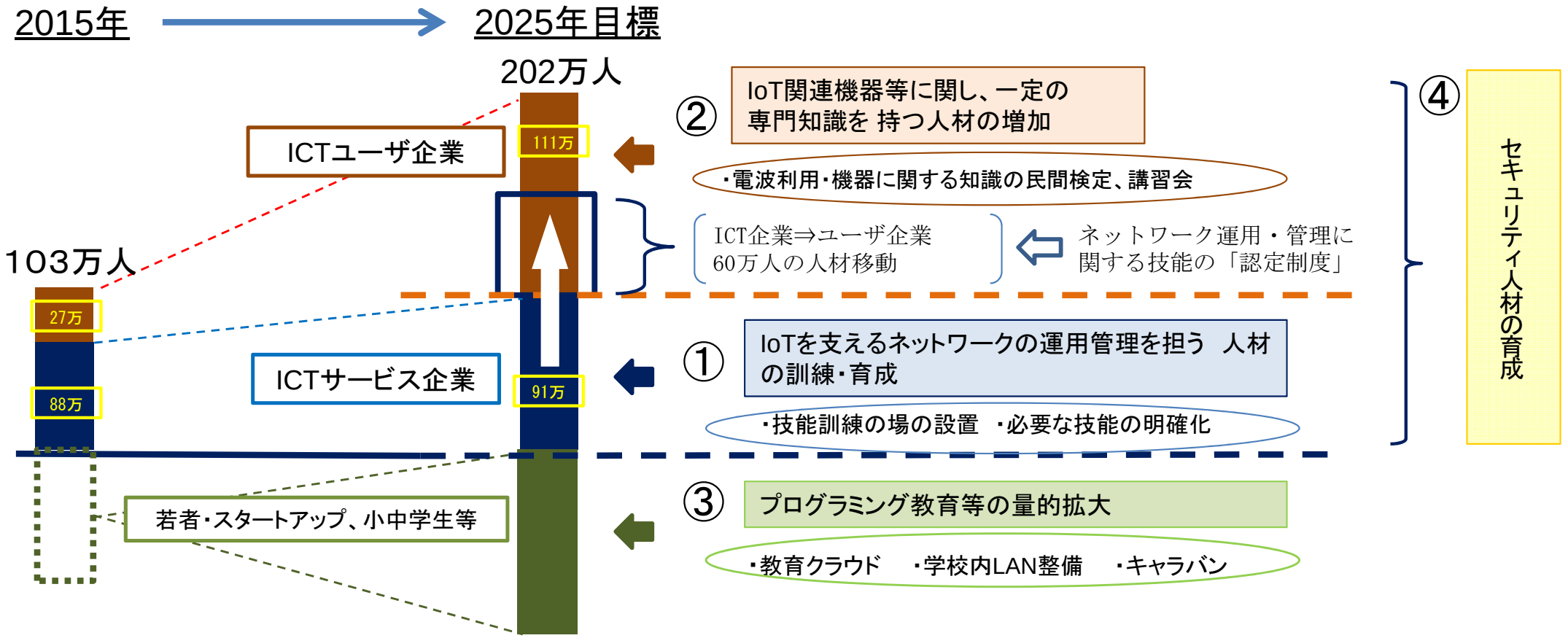
■ブロックチェーン技術について、本年度中を目処に、政府調達や申請手続等の分野で、政府の情報システム等への先行的な導入を見据えた実証に着手。

■その際、電子委任状に係る制度やサンドボックス制度の活用、個別機器等への分散型認証の仕組みの構築やブロックチェーンに記録されるデータの真正性確保やアクセス権確認のための公的個人認証の活用、スマートコントラクトを活用した手続きの効率化の促進等の実現に向けて、運用・ルール面の課題について検討。

■その結果も踏まえ、こうした新たな技術も取り込んだ業務改革により、効率性や利便性の向上に資する革新的な電子行政の実現に向けた計画を、来年度を目処に策定。

# IoT人材の育成

# IoT人材育成の必要性




（出典）情報通信審議会 第2次答申「IoT/ビッグデータ時代に向けた新たな情報通信政策の在り方」、
IPA「IT人材白書2015」、総務省等「情報通信業基本調査報告書(平成28年3月)」等より推計

# 【IoT人材の育成】

■IoTを支えるネットワークの運用・管理人材の育成について、2017年内に、ソフトウェア・仮想化技術などを活用したネットワークの運用・管理に必要なスキルを明確化するとともに、スキルを身に付けるための実習・訓練、スキルの認定を一貫して行う体制を立ち上げ、実習・訓練を開始。

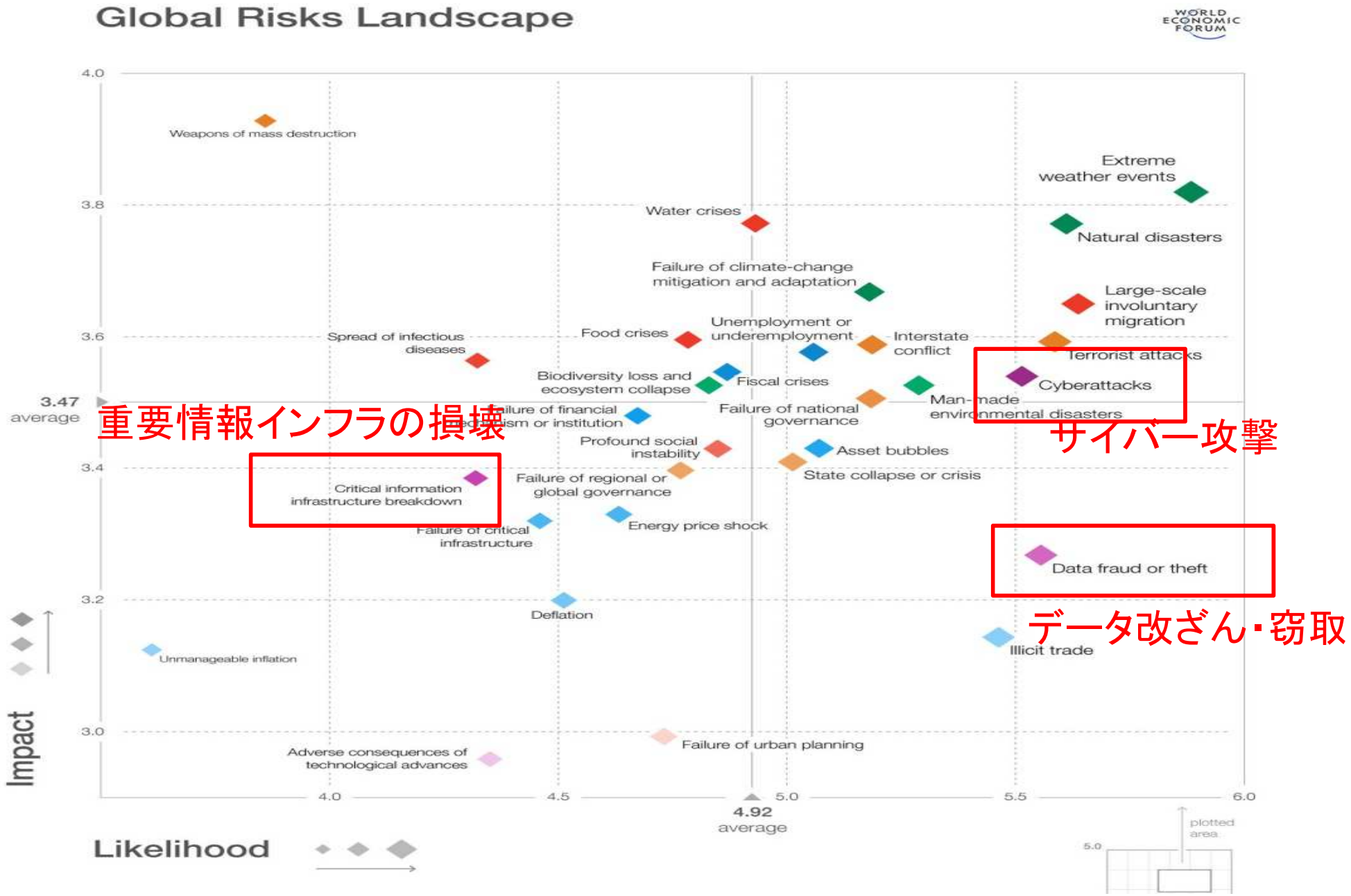
■「サイバーセキュリティ人材育成プログラム」（平成29年4月18日サイバーセキュリティ戦略本部決定）に基づき、重要インフラ・産業基盤等の中核人材育成、官公庁及び重要インフラ事業者等を対象とした実践的演習、若年層の発掘・育成などの各種人材育成施策を、各施策間の連携強化を図りつつ推進する。

■学校でのプログラミング教育を通じてITへの興味・関心を高めた児童生徒等に対し、地域において発展的・継続的に学べる環境づくりに資するガイドラインを策定。

# サイバーセキュリティ対策の強化

# グローバルリスクに対する評価

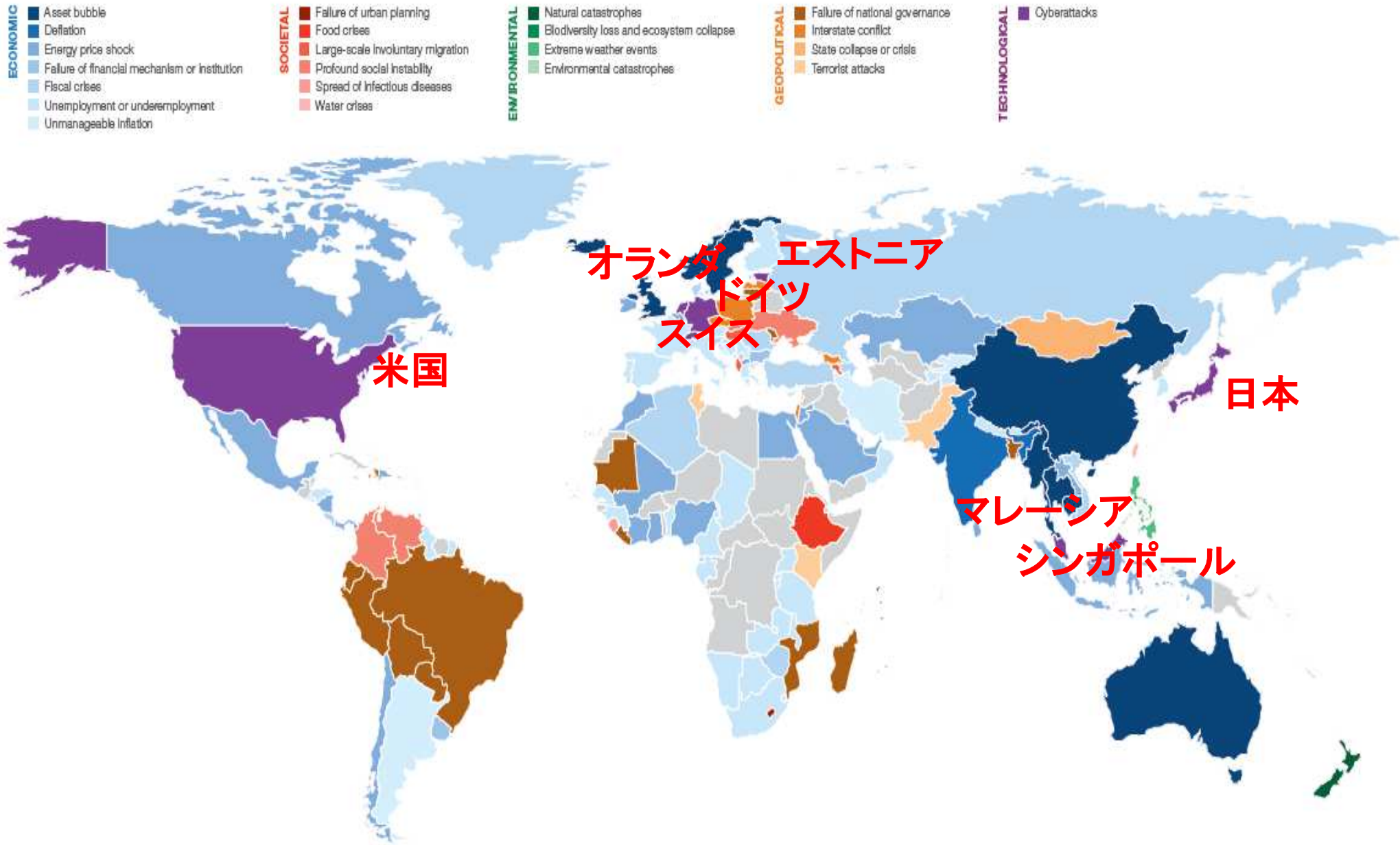





（出典）World Economic Forum “The Global Risks Report 2017 : 12th Edition” (January 2017)

# 各国別・最大リスク要素



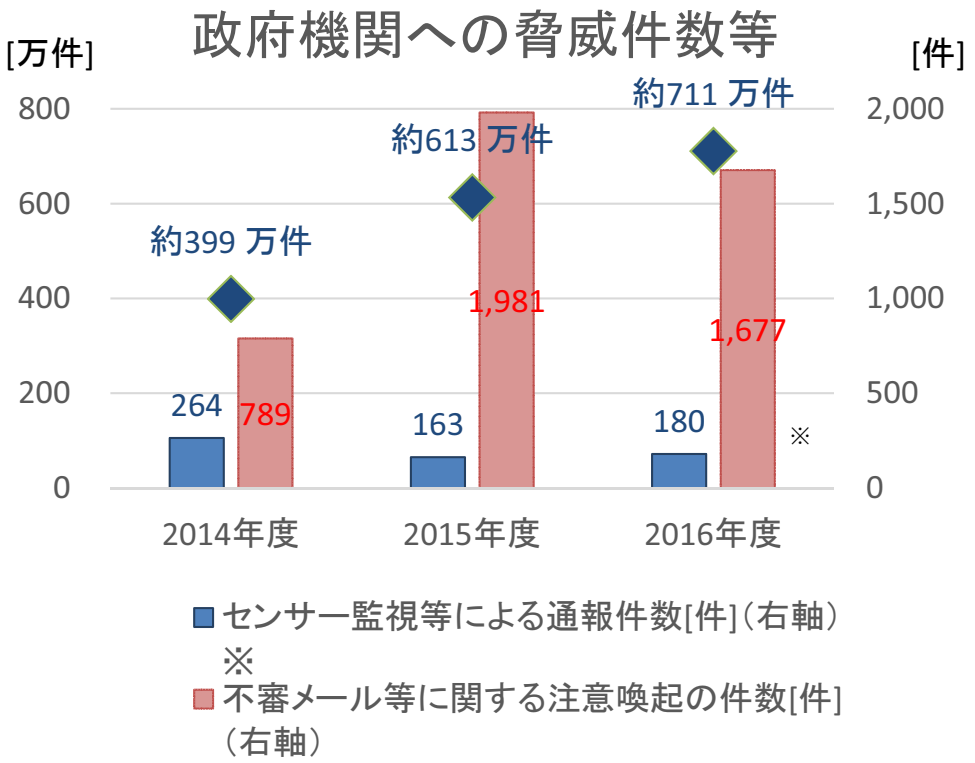



（出典）World Economic Forum “The Global Risks Report 2016 : 11th Edition” (January 2016)

# リスクの深刻化

## 政府機関等における情勢

- ウェブアプリケーション（Apache Struts等）の脆弱性を悪用した攻撃等、依然として政府機関等を対象とした攻撃が頻発。
- 国による**監視、監査、原因究明調査等の範囲を拡大するための法改正を実施**（2016年４月成立、同年10月施行）。




※　GSOC（政府機関情報セキュリティ横断監視・即応調整チーム）により各府省庁等に置かれたセンサーが検知等したイベントを通知した件数。

**【外部からの攻撃に係る2015年度の特徴】**

- センサー監視等による**脅威件数は約711万件**となり、**前年度比で約１００万件増加**。**約４．４秒に１回**、脅威を認知。
- センサー監視等による通報件数は前年度から増加（１８０件）。
- 不審メール等の**注意喚起件数**は急増した２０１５年度と同様に**1,500件を越え、高止まりしている状況**（1,677件）。

**【政府機関等に対する不振メールの添付ファイル形式の傾向】**

- 実行ファイル及びOfficeファイルが依然として多くの割合を占める一方、**スクリプト形式（JScript、VBScript等）の割合が2016年度には４３%と大きく増加。**

（出典）NISC「サイバーセキュリティ政策に係る年次報告（2016年度）」（2017年7月）

# リスクの拡散



**ＰＣ**

多くの職場・家庭に普及し、インターネットに接続
（2016年末：PC普及率 73.0%、インターネット普及率 ８３.5%）

※2017版情報通信白書（総務省）

**スマートフォン**

世帯保有率が5年間で2.5倍に急増
（2011年末：29.3%→2016年末：71.8%）

※2017版情報通信白書（総務省）

**自動車**

一台に搭載される車載コンピュータは100個以上、
ソフトウェアの量は約1000万行

**スマートメーター**
**（次世代電力量計）**

電力会社による開発・導入の開始

［主な予定］
・東京：2020年度までに2700万台の導入完了
・関西：2022年度までに1300万台の導入完了

# リスクのグローバル化



（注）海外のサイバー攻撃事案（報道ベース）

## ○ ソニー・ピクチャーズ・エンターテイメント（2014年11月下旬）

2014年11月、「平和の守護者（Guardians of Peace）」を名乗る組織が、システムに侵入し、同社の数千に及ぶ社内文書や未公開の4作品を含む5作品の同社映画全編の違法コピーがオンライン上に流出。米国政府は、12月19日、当該サイバー攻撃を北朝鮮政府による犯行とし、翌月2日、大統領令を発出し追加的な経済制裁を実施。

## ○ 保険会社アンセム（2015年2月上旬）

2015年2月、同社に対するサイバー攻撃により、8,000万人分に及ぶ新旧加入者や従業員の個人情報が盗まれた。氏名、生年月日、加入者ID、社会保障番号、住所、電話番号、電子メールアドレス、勤務先情報が漏えいしたが、クレジットカードや医療記録などの情報は流出した形跡はないとしている。なお、攻撃者は米国人事管理局（OPM）（後述）へのサイバー攻撃を行った中国人民解放軍ハッカー部隊であるとの可能性も指摘されている。

## ○ フランスTV5モンド（2015年4月上旬）

2015年4月8～9日、フランス国営テレビTV5モンドは、イスラム国に所属すると主張するグループ「Cybercalophate」によってTVチャンネル、Web、FaceBookが乗っ取られ、イスラム国の犯行を主張するメッセージが表示されていた。4月10日、フランス国防省は、調査の結果、軍の機密情報が漏えいすることはなかったと発表した。

## ○ ドイツ連邦委議会（2015年5月上旬）

2015年5月15日、ドイツ連邦議会（下院）のサーバにサイバー攻撃を受け、約2万台のパソコンが外部から自由に操作できる状態となった。メルケル首相の下院事務局のパソコンも感染。情報機関のトップは、手法が極めて巧妙であることからロシアの関与を示唆している。少なくとも5人の議員のパソコンからデータ流出が確認されており、それ以外の情報も流出するおそれがあるとしている。

## ○ 米国人事管理局（2015年6月上旬）

2015年6月4日、米国人事管理局は、システムが侵入され、2，210万件の職員及び元職員の個人情報が流出したと発表 。同局は、情報流出による影響を調べているが、人事管理局や内務省だけでなく、ほぼすべての連邦政府機関に及ぶとされる。さらに数百万人の職員の情報が流出していた可能性もあるとしている。専門家の見解では、中国人民解放軍のハッカー部隊である「ディープ・パンダ」と呼ばれる組織が今回の攻撃及び保険会社アンセムへの攻撃を実施したとされている。

## ○ オーストラリア気象局（2015年12月上旬）

2015年12月2日、オーストラリア気象局が保有する同国最大のスーパーコンピュータが大規模なサイバー攻撃を受けた。同コンピュータは国防省のネットワークとつながっており、政府のシステムが危険にさらされたとされるが、被害の詳細は不明である。オーストラリア政府関係者は、中国の関与を示唆しているが、中国外務省はサイバー攻撃への関与を否定した。なお、同気象局は、公式発表において、「セキュリティに関する問題にコメントしない」としている。

## ○ ウクライナ電力供給会社（2015年12月下旬）

2015年12月23日、ウクライナ西部のイヴァーノ＝フランキーウシク地域で、変電所の遮断により、約6時間の停電が発生した。電力供給会社でマルウェアが発見されているが、マルウェアが停電につながったとする因果関係は確認されていない。ウクライナ保安庁は、ロシアの関与を示唆しているが、ロシア政府は反論している。

## ○ イスラエル電力公社（2016年1月下旬）

2016年1月26日、イスラエル電力公社が過去最大規模のサイバー攻撃を受けた。このサイバー攻撃で電力供給に支障が生じてはいなかったとされている。後日、攻撃は、ランサムウェアを用いた金銭目的であることが濃厚であると報じられた。

# サイバーセキュリティ基本法（１５年１月全面施行）



| | 施行前 | | 施行後 |
|---|---|---|---|
| 政府の推進体制 | 内閣<br>IT戦略本部（本部長：総理大臣）<br>NSC（議長：総理大臣）<br>情報セキュリティ政策会議 ← IT本部長決定<br>情報セキュリティセンター ← 総理大臣決定 | 法律・政令で設置根拠を明確化 | 内閣<br>IT戦略本部 ⟷ 緊密連携 ⟷ **サイバーセキュリティ戦略本部**（本部長：内閣官房長官） ⟷ 緊密連携 ⟷ NSC<br>内閣サイバーセキュリティセンター(NISC)<br>基本法<br>政令(官房組織令) |
| 各省への権限 | 各省との合意に基づく取組<br>• 各府省等による自主的な監査<br>• 事案発生時、必要に応じ、解析等の協力を実施 | 権限強化 | サイバーセキュリティ基本法に根拠を持つ権限<br>• 政府機関への第三者(本部・NISC)による監査 ※<br>※ マネジメント監査とシステムへの擬似的攻撃を実施<br>• 重大な事案発生時における原因究明調査<br>• 政府機関からの資料等提出義務、本部長による勧告権 |
| 基本戦略 | 「サイバーセキュリティ戦略」<br>（平成25年６月情報セキュリティ政策会議決定） | 格上げ | 基本法に基づく新たな「サイバーセキュリティ戦略」<br>（IT戦略本部・NSCへ意見聴取の上、平成２７年９月、閣議決定・国会報告） |

# 日本年金機構事案（2015年5月）の概要



◆ プロキシログの解析により、不審な通信先23件、不審な通信を行った端末31台を特定、不審メールと突合。

| 不審メールの番号 | 受信日 | 不審メールの概要 | 発生した不審な通信 |
|---|---|---|---|
| Ⅰ | 5月8日(金) | 件名：「厚生年金基金制度の見直しについて(試案)に関する意見」<br>宛先：公開メールアドレス(2)<br>リンク：商用オンラインストレージ | 端末1台が不正プログラムに感染、不審な通信が発生。約4時間後に端末の通信ケーブルを抜線、その後は不審な通信なし。 |
| Ⅱ | 5月18日(月) | 件名：給付研究委員会オープンセミナーのご案内<br>宛先：非公開の個人メールアドレス(98)<br>添付ファイル：給付研究委員会オープンセミナーのご案内.lzh | 端末3台が不正プログラムに感染、不審な通信が発生するも接続先への通信は失敗。 |
| Ⅲ | 5月18日(月)<br>～<br>5月19日(火) | 件名：厚生年金徴収関係研修資料<br>宛先：非公開の個人メールアドレス(20)<br>添付ファイル：厚生年金徴収関係研修資料（150331厚生年金徴収支援G）.lzh（16）<br>リンク：商用オンラインストレージ(4) | 不審な通信は発生せず。 |
| Ⅳ | 5月20日(水) | 件名：【医療費通知】<br>宛先：公開メールアドレス(3)<br>添付ファイル：医療費通知のお知らせ.lzh | 20日午後、端末1台が不正プログラムに感染、不審な通信が発生。数時間以内に、他の6台の端末からも不審な通信が発生。<br>21日から23日にかけて、合計21台の端末から国内のサーバ(接続先X)への多数の通信。 |

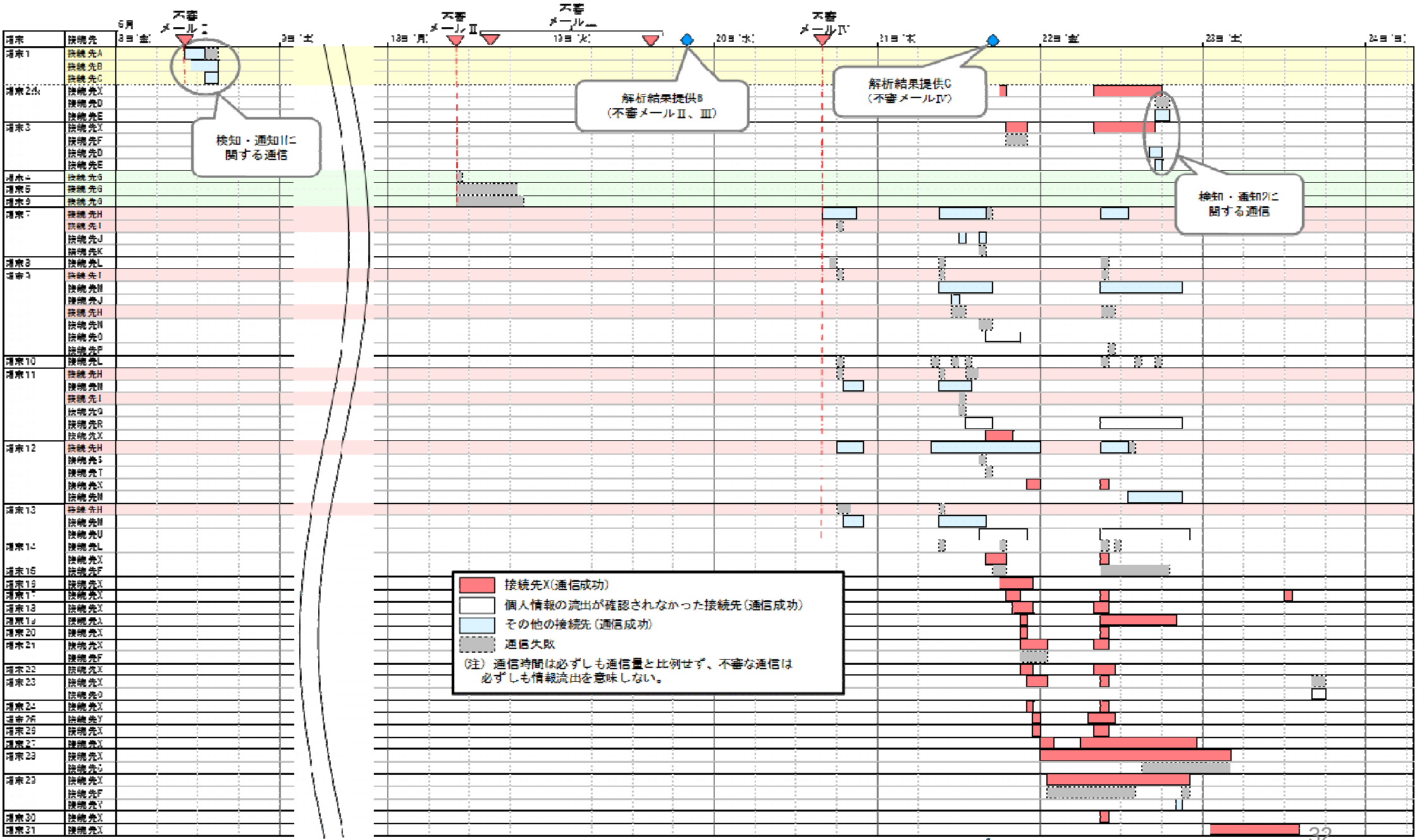
◆ NISCでは、不審メールⅡ及び不審メールⅢに関する解析結果を5月19日夜に、不審メールⅣに関する解析結果を5月21日夕刻に、それぞれ厚労省情参室に提供しているが、これらの解析結果には不正プログラムの接続先に関する情報が含まれていた。

◆ 5月22日にNISCにおいて不審な通信を検知し厚労省に通知した後、機構による調査の過程で接続先Xへの多数の通信が判明した。

(出典)サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査報告」（2015年8月）

# 日本年金機構事案：感染端末と不審な通信

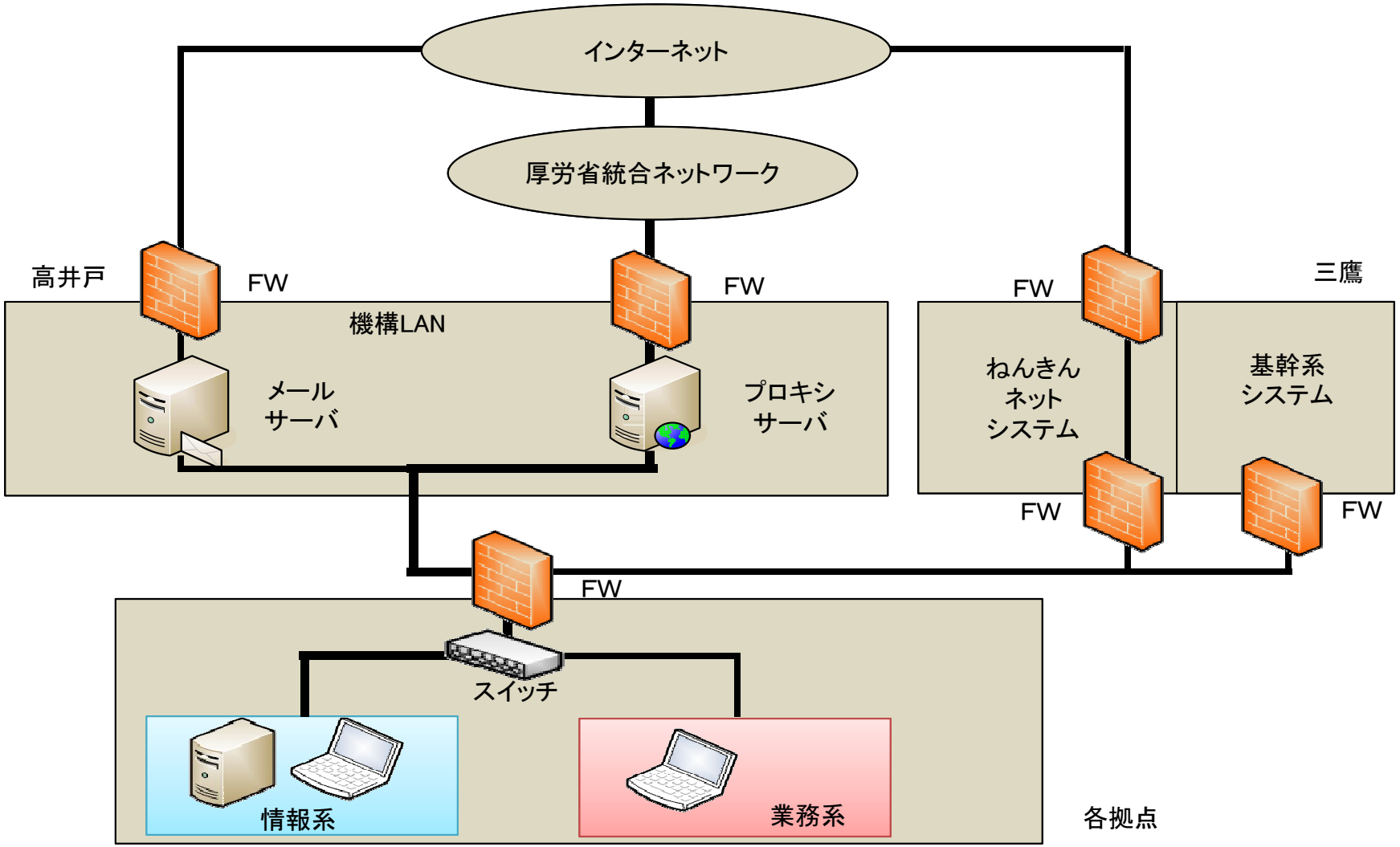





(出典)サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査報告」(2015年8月)

# 日本年金機構における情報システム（概要）








(出典）サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査報告」（2015年8月）

# 日本年金機構事案：攻撃の特徴と対策



## □ 標的型攻撃の特徴

- 標的型攻撃は巧妙化しており、使われるメールも見分けが困難。
  →メール開封を前提とした対策が必要。
- 攻撃者は乗っ取った端末を足掛かりとして、侵入を拡大させる。
  →初期段階での認知・対処、侵入範囲を拡大させないためのシステム設計・構築・運用が重要。

## □ 標的型攻撃に対する情報システム防御策等の考え方

自組織の情報・システム・業務を守る目的・対策について考え、職務・職責に応じて実施することが求められる。

［検討対策例］

◆ システム防御策

- メールに添付された実行形式のファイルを取り込まない・起動できないようにシステム設定。
- 既知の脆弱性を放置しないようにアップデート等を行う。脆弱性診断を実施。ウェブブラウザの拡張機能の必要最小限の使用。
- 侵入範囲が拡大しにくいように設定・運用。
- 業務・情報の性質等に応じて重要な情報に攻撃が到達しないよう、システム分離。
- システム分離したときに各システムで扱える情報・できない情報につきルール化し、職員に徹底。
- ローカル管理者権限のパスワードを共通とする範囲の最小限化。
- 不要な管理アカウントの確実な消去。
- 内部ネットワークにおける異常を検知する仕組みの整備。　　等

◆ インシデント対策に係る対策

- 不審メールの受信（不正プログラム動作の可能性）につき攻撃者が繰り返して攻撃を試みるものとして継続的に対応。
- システム構築・運用事業者とは独立した専門性の高い事業者への依頼等、平素からの準備。
- CISO等権限を有する者の下でのインシデント対応。



(出典）サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査報告」（2015年8月）

# サイバーセキュリティ基本法及び情報処理促進法の一部改正（16年10月）



日本年金機構の情報流出事案等を踏まえ、政府機関等のサイバーセキュリティ対策の抜本的強化を図るため、サイバーセキュリティ基本法等の改正を行う必要。

■ 国が行う不正な通信の監視、監査、原因究明調査等の対象範囲を拡大
■ サイバーセキュリティ戦略本部の一部事務を独立行政法人情報処理推進機構（IPA）等に委託

## 基本法

| | 中央省庁 | 独立行政法人 | 特殊法人・認可法人 |
|---|---|---|---|
| 監査 | 現行法 | | 拡大 |
| 原因究明調査 | 現行法 | 拡大 | 拡大 |
| 監視（GSOC） | 現行法 | 拡大 | 拡大 |

**一部事務を委託**
（秘密保持義務等を規定）

IPAその他政令で定める法人

**サイバーセキュリティ戦略本部が指定**
（日本年金機構等を想定）
※ 当該法人におけるサイバーセキュリティが確保されない場合に生ずる国民生活又は経済活動に及ぼす影響を勘案

（2016年10月本部決定）
■地方公共団体情報システム機構
■地方公務員共済組合連合会
■地方職員共済組合
■全国市町村職員共済組合連合会
■国家公務員共催組合連合会
■日本私立学校振興・共済事業団
■公立学校共済組合
■日本年金機構

## 情促法

■ サイバーセキュリティ対策の強化に係る観点から、以下の規定の整備を行う。
- 本部から委託を受ける事務に係るIPAの業務追加
- 情報処理安全確保支援士制度の創設（名称独占、更新制、秘密保持義務等）
- ソフトウェアの脆弱性情報等の公表の方法・手続を整備

# サイバーセキュリティ戦略（15年9月閣議決定）



## 1 サイバー空間に係る認識

- サイバー空間は、「**無限の価値を産むフロンティア**」である人工空間であり、人々の経済社会の活動基盤
- あらゆるモノがネットワークに連接され、実空間とサイバー空間との融合が高度に深化した「**連接融合情報社会（連融情報社会）**」が到来
  同時に、サイバー攻撃の被害規模や社会的影響が年々拡大、脅威の更なる深刻化が予想

## 2 目的

- 「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって「**経済社会の活力の向上及び持続的発展**」、「**国民が安全で安心して暮らせる社会の実現**」、「**国際社会の平和・安定及び我が国の安全保障**」に寄与する。

## 3 基本原則

① 情報の自由な流通の確保　② 法の支配　③ 開放性　④ 自律性　⑤ 多様な主体の連携

## 4 目的達成のための施策

①後手から**先手**へ　／　②受動から**主導**へ　／　③サイバー空間から**融合**空間へ

### 経済社会の活力の向上及び持続的発展

～ 費用から投資へ ～

■ **安全なIoTシステムの創出**
安全なIoT活用による新産業創出

■ **セキュリティマインドを持った企業経営の推進**
経営層の意識改革、組織内体制の整備

■ **セキュリティに係るビジネス環境の整備**
ファンドによるセキュリティ産業の振興

### 国民が安全で安心して暮らせる社会の実現

～ 2020年・その後に向けた基盤形成 ～

■ **国民・社会を守るための取組**
事業者の取組促進、普及啓発、サイバー犯罪対策

■ **重要インフラを守るための取組**
防護対象の継続的見直し、情報共有の活性化

■ **政府機関を守るための取組**
攻撃を前提とした防御力強化、監査を通じた徹底

### 国際社会の平和・安定及び我が国の安全保障

～ サイバー空間における積極的平和主義 ～

■ **我が国の安全の確保**
警察・自衛隊等のサイバー対処能力強化

■ **国際社会の平和・安定**
国際的な「法の支配」確立、信頼醸成推進

■ **世界各国との協力・連携**
米国・ASEANを始めとする諸国との協力・連携

### 横断的施策

■ **研究開発の推進**
攻撃検知・防御能力向上(分析手法・法制度を含む)のための研究開発

■ **人材の育成・確保**
ハイブリッド型人材の育成、実践的演習、突出人材の発掘・確保、キャリアパス構築

## 5 推進体制

- 官民及び関係省庁間の連携強化、オリンピック・パラリンピック東京大会等に向けた対応

# 企業におけるサイバー攻撃被害の状況



表 5-3：一件あたりの平均損害賠償額の経年変化

| | 一件あたりの平均想定損害賠償額 | (参考) 想定損害賠償総額 |
|---|---|---|
| 2005 年 | 5 億 3,935 万円 | 約 5,329 億円 |
| 2006 年 | 4 億 8,156 万円 | 約 4,570 億円 |
| 2007 年 | 27 億 9,347 万円 | 約 2 兆 2,711 億円 |
| 2008 年 | 1 億 8,552 万円 | 約 2,367 億円 |
| 2009 年 | 2 億 6,683 万円 | 約 3,890 億円 |
| 2010 年 | 7,551 万円 | 約 1,215 億円 |
| 2011 年 | 1 億 2,810 万円 | 約 1,900 億円 |
| 2012 年 | 9,313 万円 | 約 2,133 億円 |
| 2013 年 | 1 億 6,575 万円 | 約 1,439 億円 |
| 2014 年 | 10 億 8,561 万円 | 約 1 兆 6,642 億円 |
| 2015 年 | 3 億 2,192 万円 | 約 2,527 億円 |
| 2016 年 | 6 億 7,439 万円 | 約 2,994 億円 |

(1) 単年分析(件数)

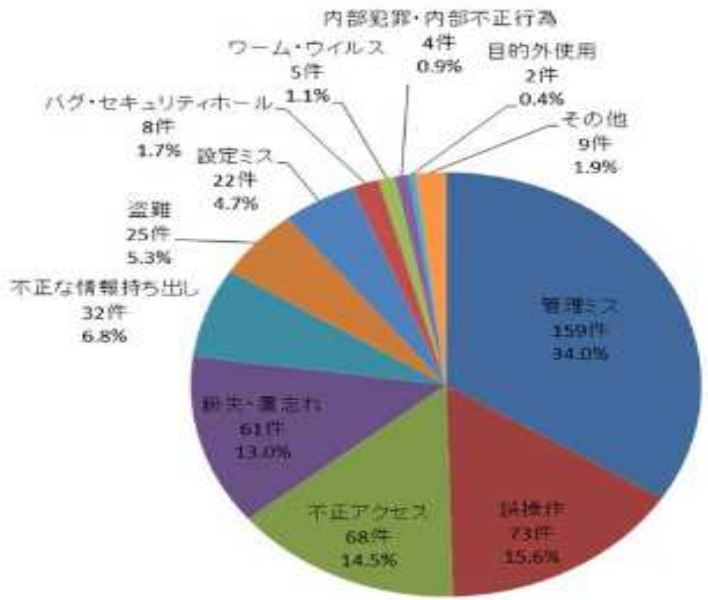



図 4-8：漏えい原因比率（件数）

表 4-2：インシデント・トップ 10

| No. | 漏えい人数 | 業種 | 原因 |
|---|---|---|---|
| 1 | 793 万人 | 生活関連サービス業，娯楽業 | ワーム・ウイルス |
| 2 | 98 万人 | 情報通信業 | 不正アクセス |
| 3 | 81 万人 | 電気・ガス・熱供給・水道業 | 紛失・置忘れ |
| 4 | 64 万人 | 情報通信業 | 不正アクセス |
| 5 | 58 万 9463 人 | 情報通信業 | 不正アクセス |
| 6 | 42 万 8138 人 | 情報通信業 | 不正アクセス |
| 7 | 42 万 1313 人 | 卸売業，小売業 | 不正アクセス |
| 8 | 35 万人 | 生活関連サービス業，娯楽業 | 不正アクセス |
| 9 | 21 万 9025 人 | 卸売業，小売業 | 不正アクセス |
| 10 | 21 万人 | 電気・ガス・熱供給・水道業 | 管理ミス |

(出典)JNSA＆長崎県立大学“情報セキュリティインシデントに関する調査報告書”(2017年6月14日)

# 企業の経営課題としてのサイバーセキュリティ



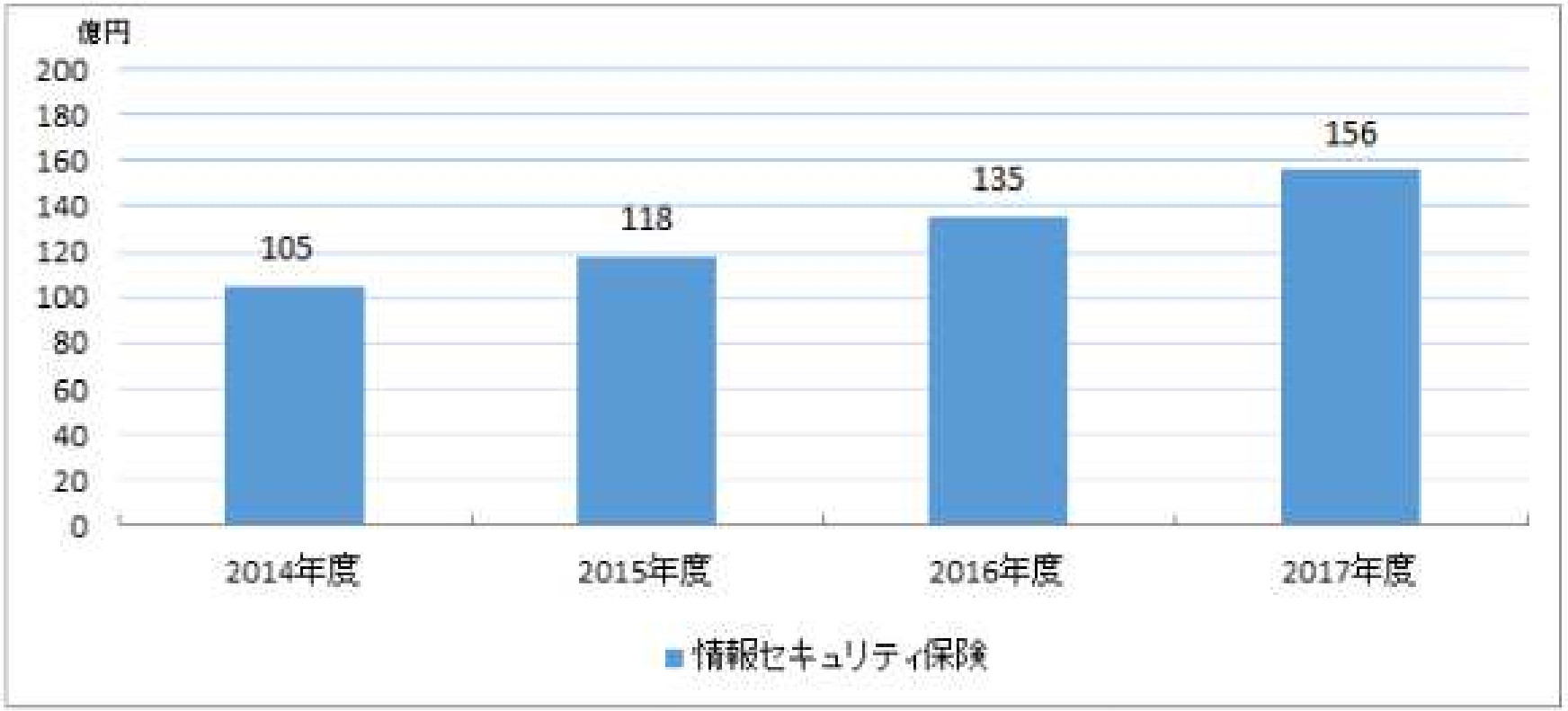
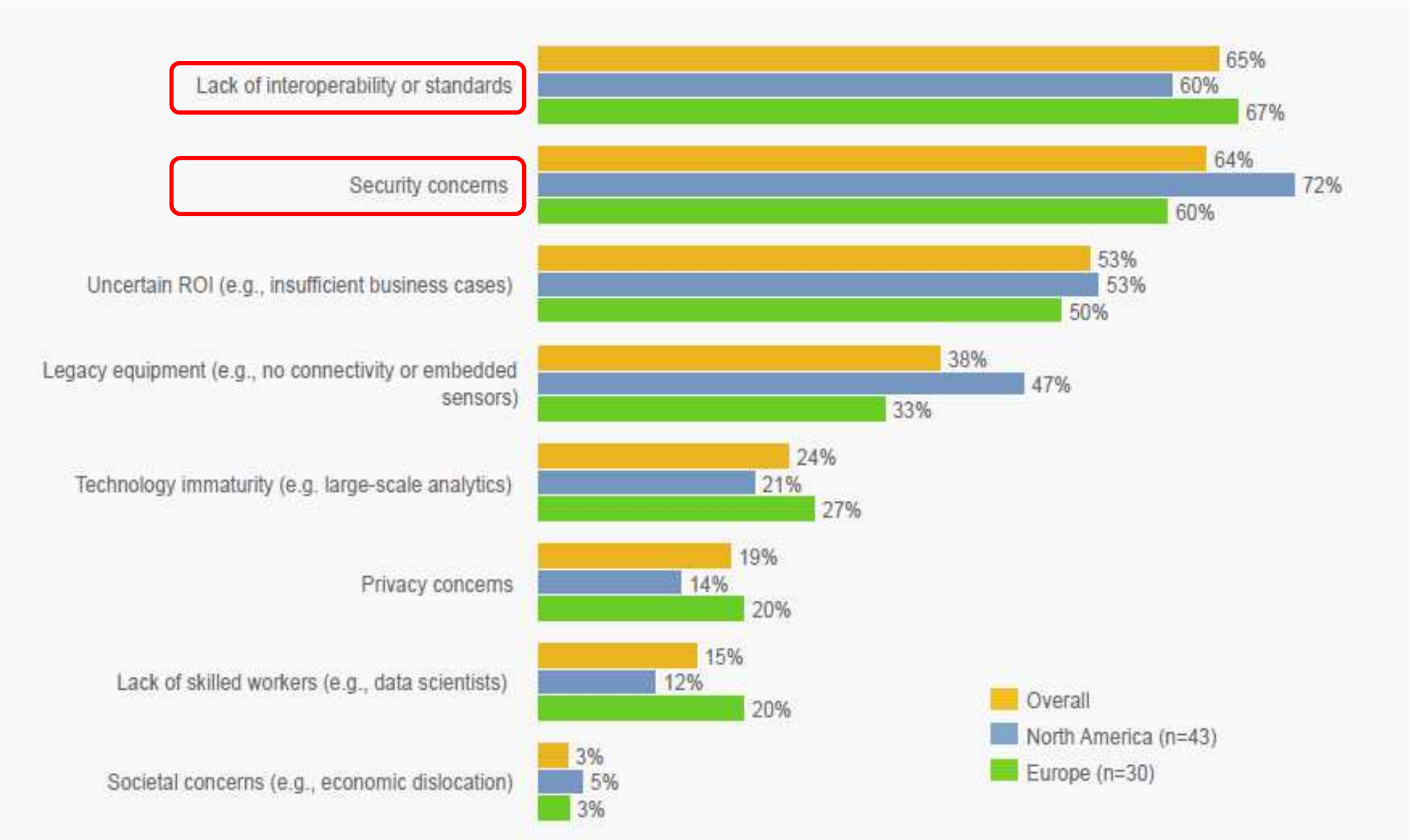



図 25　国内情報セキュリティ保険市場推移

（出典）JNSA“2016年度情報セキュリティ市場調査報告書”（2017年6月）

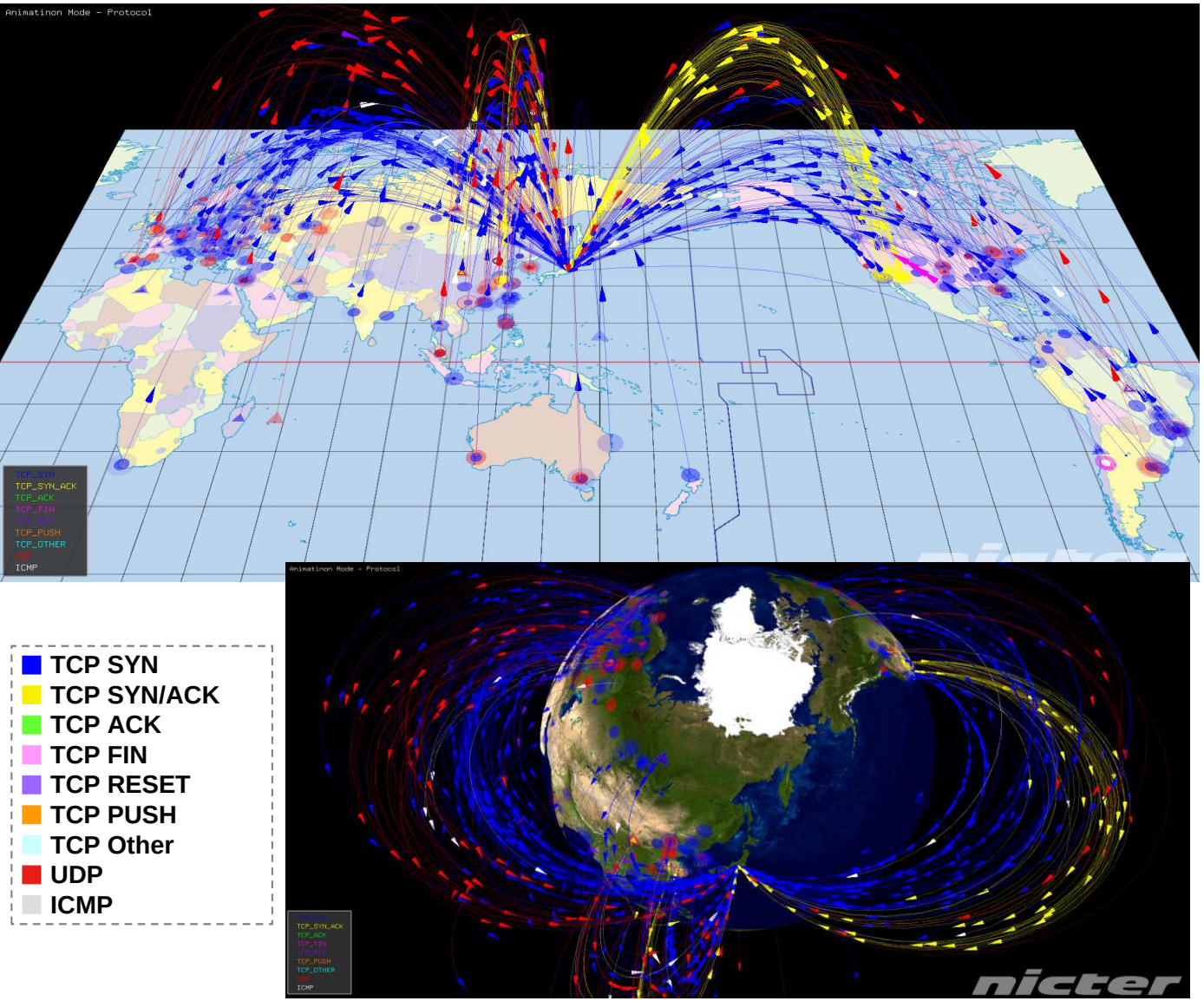
# IoT普及促進の鍵となるセキュリティ




（Source)World Economic Forum, “Industrial Internet of Things : Unleashing the Protection of Connected Products and Services” (January 2015)

# 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。

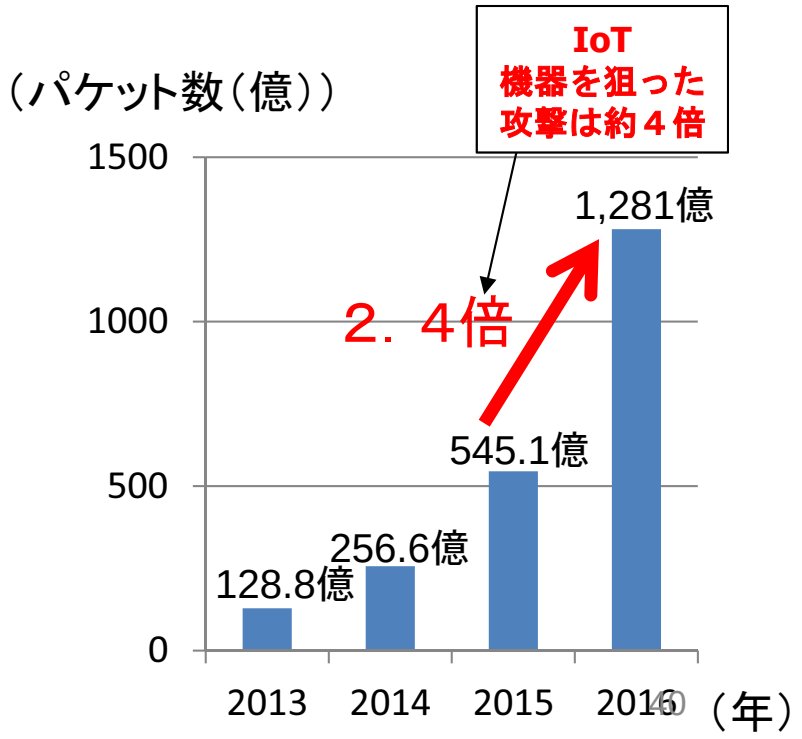



- TCP SYN
- TCP SYN/ACK
- TCP ACK
- TCP FIN
- TCP RESET
- TCP PUSH
- TCP Other
- UDP
- ICMP

・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

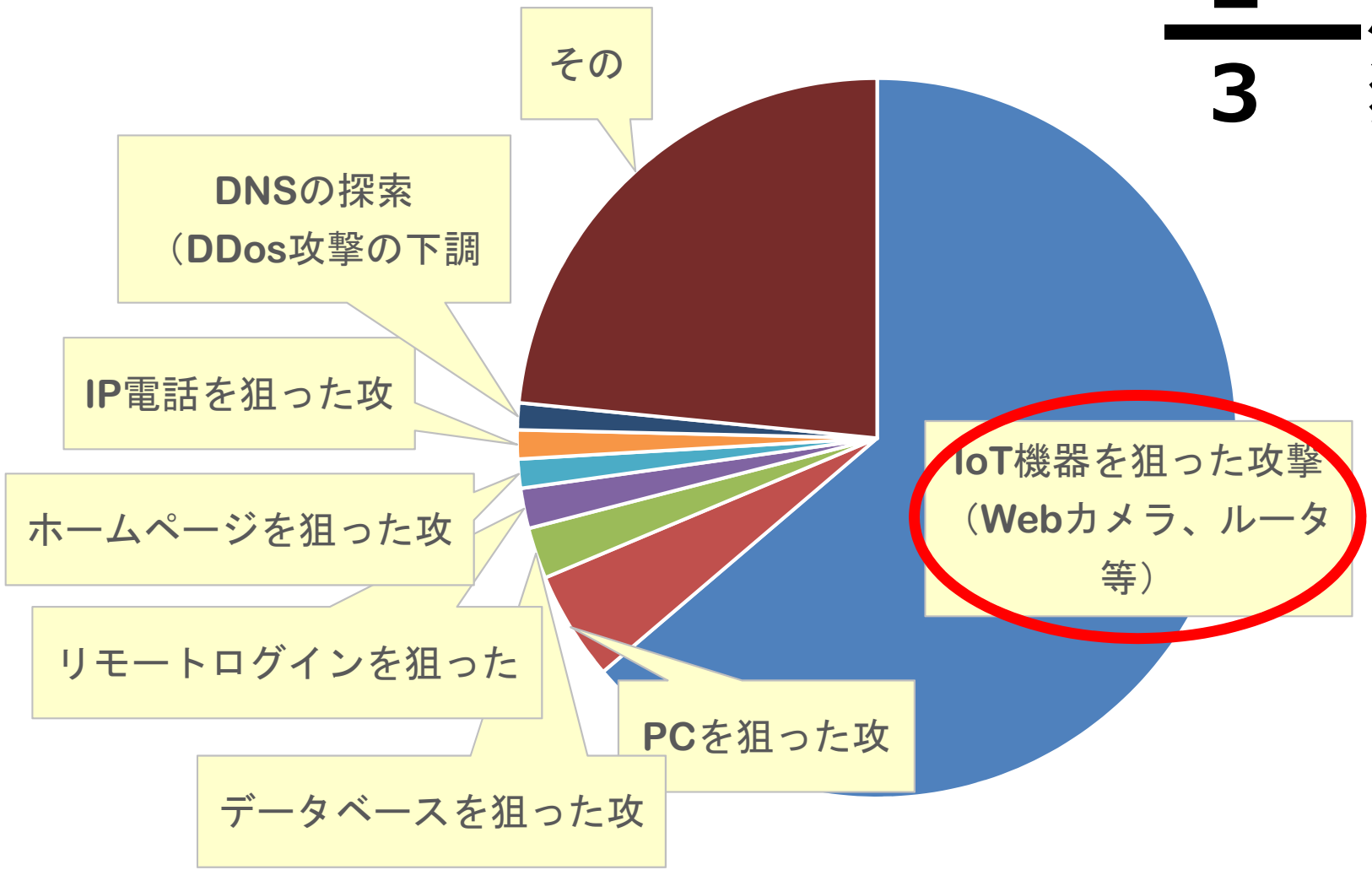
1年間で観測されたサイバー攻撃回数



# サイバー攻撃の内訳（16年、NICTERによる観測）

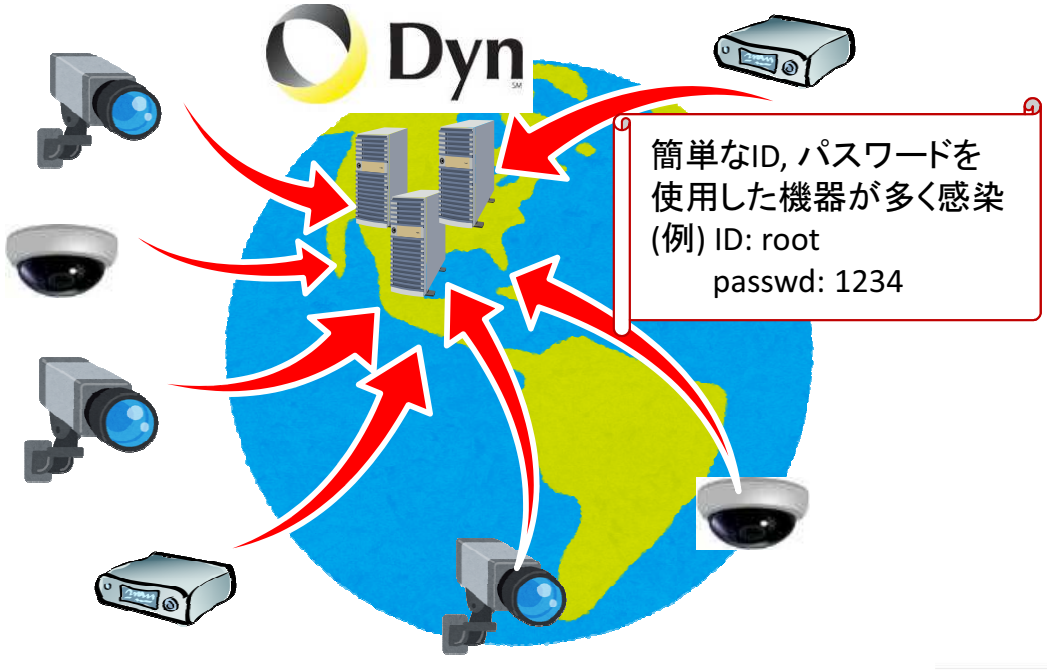
観測された全サイバー攻撃1,281億パケットのうち、

**2/3 がIoTを狙っている！**



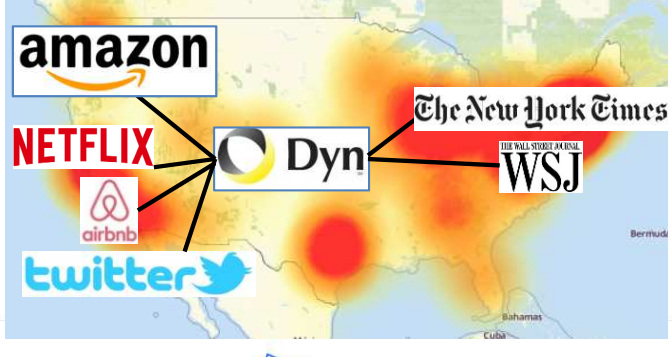
# IoTによる大規模DDoS攻撃

- 2016年10月21日米国のDyn社のDNSサーバーに対し、大規模なDDoS攻撃が2回発生。
- 同社から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。サイバー攻撃の元は、「Mirai」というマルウェアに感染した大量のIoT機器。



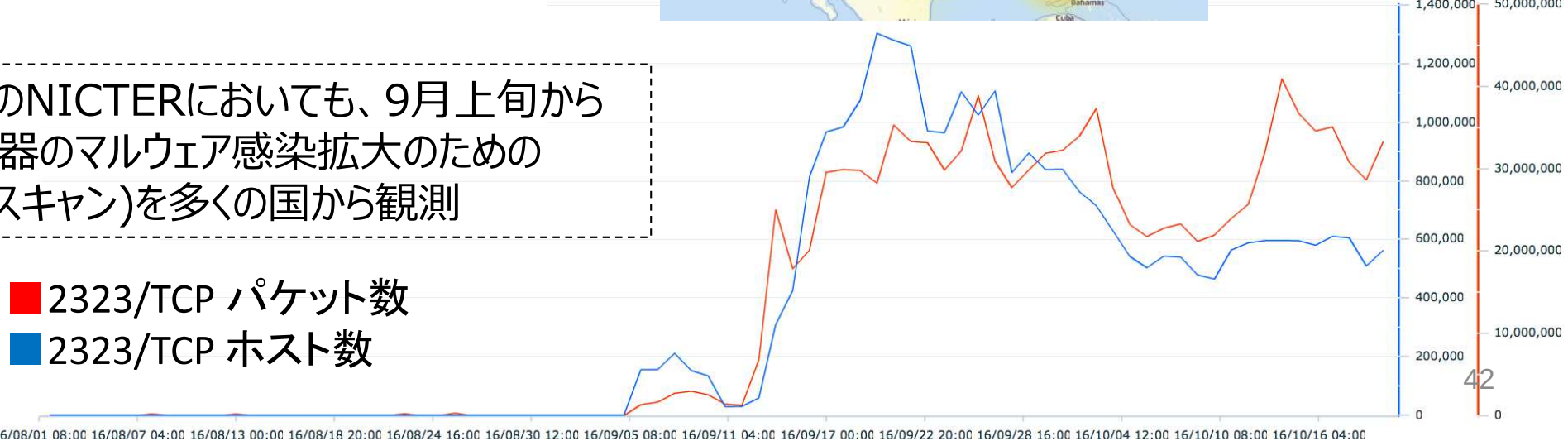

- ✓ マルウェアに感染した10万台を超えるIoT機器からDyn社のシステムに対し大量の通信が発生
- ✓ 最大で1.2Tbpsに達したとの報告もあり。

**システムダウンの状況**




Dyn社のDNSサービスを使用した数多くの大手インターネットサービスやニュースサイトに影響

- ✓ NICTのNICTERにおいても、9月上旬からIoT機器のマルウェア感染拡大のための通信(スキャン)を多くの国から観測



# IoTセキュリティガイドライン（ver1.0、16年7月）

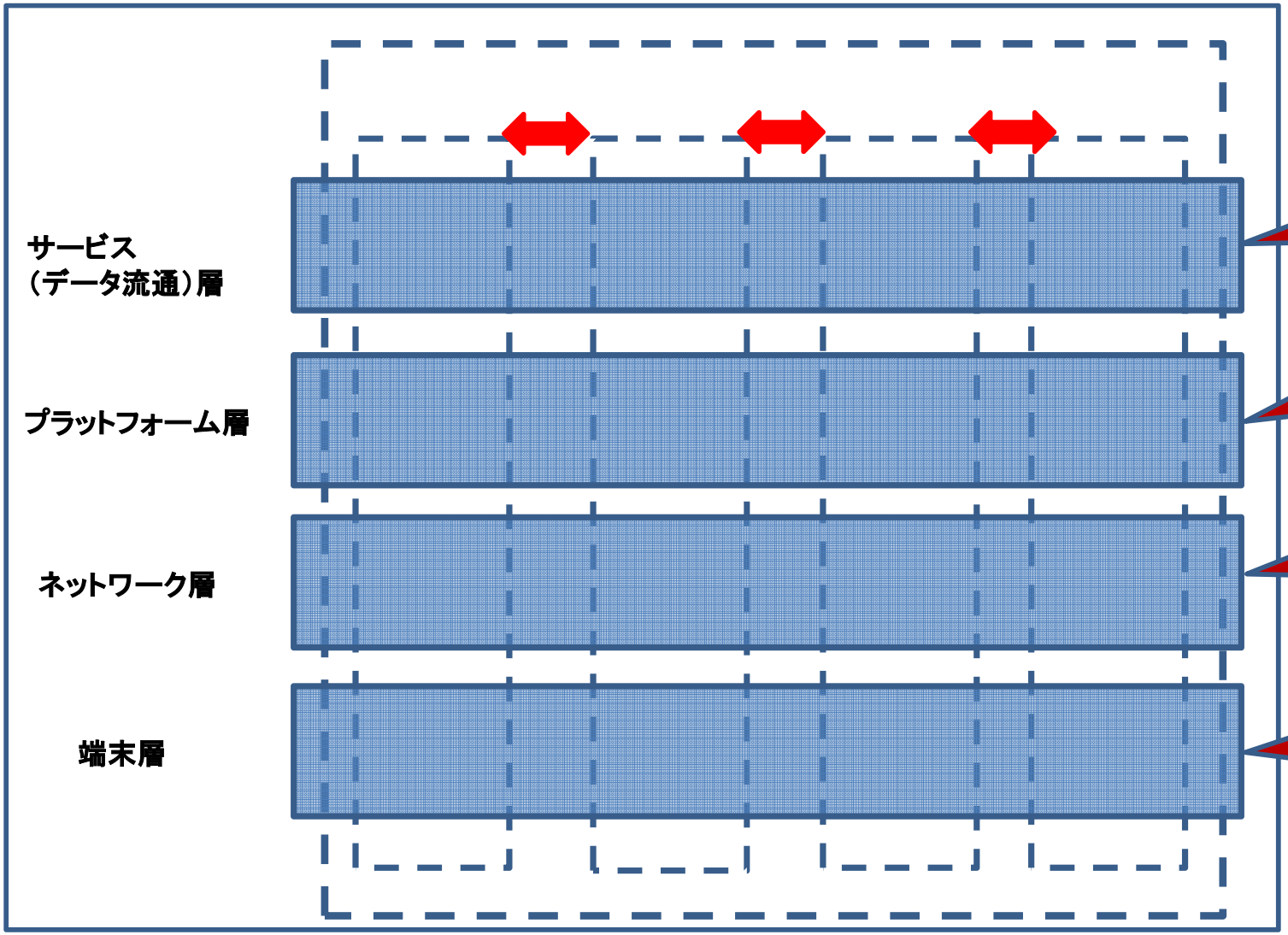
- IoT機器の設計・製造及びネットワークの接続等に関するセキュリティガイドライン。
- IoT推進コンソーシアム、総務省及び経産省の3者連名で策定・公表。

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

**セキュリティ対策の困難なIoT機器をネットワークに接続する場合、インターネットへつながる手前でセキュアなゲートウェイを経由させる等、セキュリティを確保する手段を講じる。**

# IoTシステム（System of Systems）とサイバーセキュリティ






IoTシステムは社会基盤として機能

■データの真正性確保のための対策強化
■暗号化技術の高度化

■異なるシステム間のセキュリティ対策の運用基準の共通化
■異なるシステム間の情報共有体制の強化

■ネットワーク脆弱性への対策（5GやLPWAを含む）
■SDN/NFVに係るセキュリティ対策

■IoT端末※の脆弱性の管理・検知・切り離し（ハードウェア脆弱性を含む）

**※既設端末と新設端末に分けた対策が必要。**

■脆弱性対策に係る体制の整備
■研究開発の推進
■民間セキュリティ投資の促進
■人材育成の強化
■国際連携の推進（標準化を含む）

# IoT推進コンソーシアム



■ IoT／ビッグデータ／人工知能時代に対応し、企業・業種の枠を超えて産学官で利活用を促進するため、総務省及び経済産業省の共同の呼びかけのもと、民主導の組織として「IoT推進コンソーシアム」を設立。（平成27年10月23日（金）に設立総会を開催。）
■ 技術開発、利活用、政策課題の解決に向けた提言等を実施。　（会員法人数3,115社（平成29年6月30日現在））

**総　会**
■ 会長
■ 副会長

**運営委員会**　（15名）

| | | |
|---|---|---|
| 会長 | 村井　純 | 慶應義塾大学 環境情報学部長兼教授 |
| 副会長 | 鵜浦　博夫 | 日本電信電話株式会社 代表取締役社長 |
| | 中西　宏明 | 株式会社日立製作所 執行役会長兼ＣＥＯ |

**運営委員会メンバー**　委員長　村井　純　慶應義塾大学 環境情報学部長兼教授

| | | | |
|---|---|---|---|
| 大久保　秀之 | 三菱電機株式会社　代表執行役 | 須藤　修 | 東京大学大学院　教授 |
| 越塚　登 | 東京大学大学院　教授 | 堂元　光 | 日本放送協会　副会長 |
| 小柴　満信 | JSR株式会社　社長 | 徳田　英幸 | 慶應義塾大学大学院　教授 |
| 齊藤　裕 | 株式会社日立製作所　副社長 | 野原　佐和子 | イプシ・マーケティング研究所　社長 |
| 坂内　正夫 | 情報通信研究機構　理事長 | 程　近智 | アクセンチュア株式会社 会長 |
| 志賀　俊之 | 産業革新機構　会長(CEO) | 林　いづみ | 弁護士 |
| 篠原　弘道 | 日本電信電話株式会社　副社長 | 松尾　豊 | 東京大学　准教授 |

**技術開発WG（スマートIoT推進フォーラム）**
ﾈｯﾄﾜｰｸ等のIoT関連技術の開発・実証、標準化等

**先進的ﾓﾃﾞﾙ事業推進WG（IoT推進ラボ）**
先進的なﾓﾃﾞﾙ事業の創出、規制改革等の環境整備

**IoTセキュリティWG**
IoT機器のネット接続に関するガイドラインの検討等

**データ流通促進WG**
データ流通のニーズの高い分野の課題検討等

協力　協力

総務省、経済産業省　等

# 頻発する重要インフラを狙ったサイバー攻撃



## ハッキング対策で自動車をリコール

2015年7月、クライスラー車が乗っ取られる模様がネット上で公開。クライスラー社は該当車約140万台を自主的にリコール。

## 米医療機関で医療行為に支障

2016年2月、米国カリフォルニアの医療機関（Hollywood Presbyterian Medical Center）がサイバー攻撃を受け、多くのシステムがランサムウエアに感染。患者情報や検査結果等が閲覧できなくなり、一部患者は他病院に移送された。

## 米SPE社へのサイバー攻撃

2014年11月、米国ソニー・ピクチャーズ・エンターテイメント(SPE)社がサイバー攻撃を受け、数千に及ぶ社内文書や未公開作品を含む映画がオンライン上に流出。

## 米医療機関から220万件の個人情報漏えい

2015年10月3日、米国フロリダの医療機関(cancer clinic 21st Century Oncology)のシステムが不正アクセスを受け、データベースから患者と医師の個人情報が漏えい。



## 仏テレビ局が放送中断

2015年4月8～9日、フランスの国営放送（TV5モンド）がサイバー攻撃を受け、放送できない状態となったほか、同放送局の公式Facebookアカウントが乗っ取られた。

## 米金融機関から8300万件の顧客情報流出

2014年8月、JPモルガン・チェースへのサイバー攻撃により、8300万件の顧客情報が流出。

## ウクライナ西部で大規模停電

2015年12月23日、ウクライナ西部で停電が発生。復旧に約6時間を要し40～70万人程度が影響を受けた。電力供給会社（Prykarpattyaoblenergo）は、「原因は遠隔操作による外部からの侵入の可能性が高い」と発表。

# 制御システムの汎用化の進展

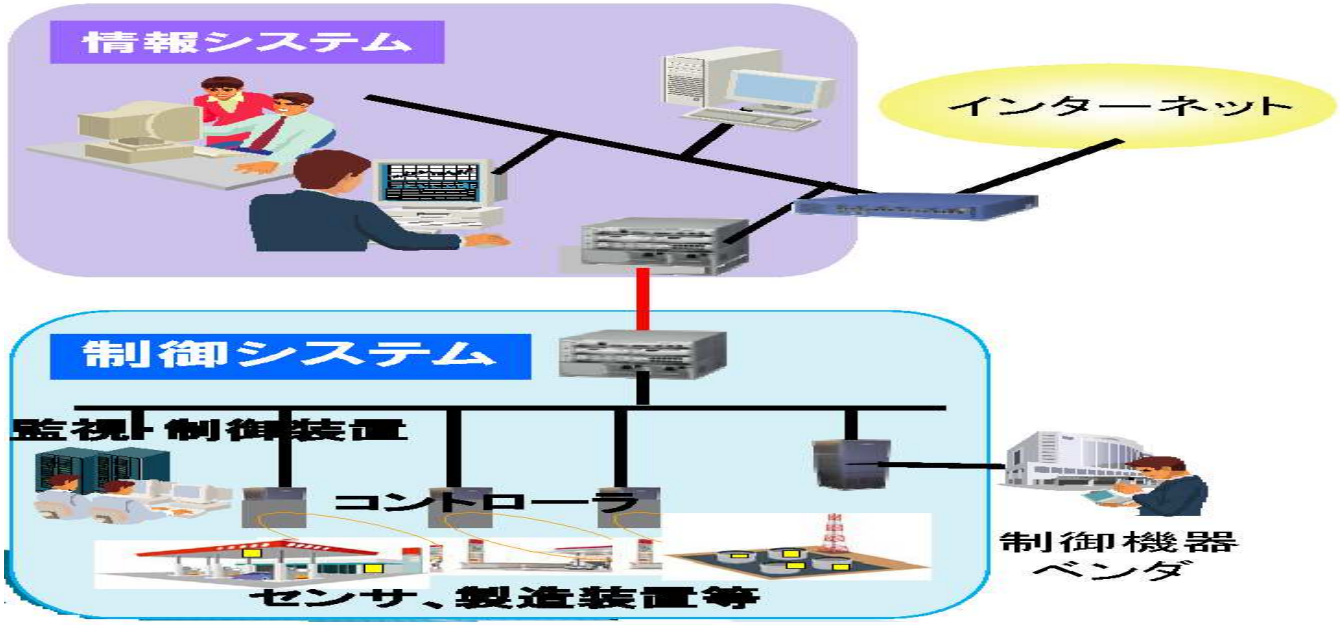


**従来**

制御システムは事業者毎に固有の仕様部分が多く、詳細な内部仕様等を把握できない限り、外部からの攻撃は難しいものであった。

**最近**

○ 標準プロトコルや汎用製品が仕様に採用され、汎用化が進んでいる。
○ 外部ネットワークにも接続されるようになっている。
○ このような状況から事業者及びシステム開発企業の利便性が向上してきている反面、攻撃対象になりやすいという特徴が現れてきている。



# 重要インフラの情報セキュリティ対策



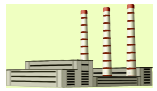
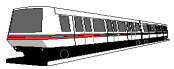
## 官民連携による重要インフラ防護の推進

重要インフラにおけるサービスの持続的な提供を行い、自然災害やサイバー攻撃等に起因するIT障害が国民生活や社会経済活動に重大な影響を及ぼさないよう、IT障害の発生を可能な限り減らすとともにIT障害発生時の迅速な復旧を図ることで重要インフラを防護する

### 重要インフラ（13分野）

- 情報通信
- 金融
- 航空
- 鉄道
- 電力
- ガス
- 政府・行政サービス（含・地方公共団体）
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油

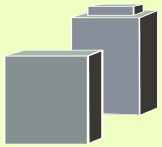



NISCによる調整・連携

### 重要インフラ所管省庁（5省庁）

### 関係機関等



## 重要インフラの情報セキュリティに係る第４次行動計画（１７年４月戦略本部決定）

### 安全基準等の整備・浸透

### 情報共有体制の強化

IT

### 障害対応体制の強化

### リスクマネジメント

### 防護基盤の強化

# 重要インフラの情報セキュリティ対策に係る第四次行動計画



## 1．本行動計画のポイント

◆ 重要インフラサービスを、安全かつ持続的に提供できるよう、自然災害やサイバー攻撃等に起因する重要インフラサービス障害の発生を可能な限り減らし、迅速な復旧が可能となるよう、経営層の積極的な関与の下、情報セキュリティ対策に関する取組を推進。（機能保証の考え方）

◆ また、取組を通じ、オリパラ大会に関係する重要なサービスの安全かつ持続的な提供も図る。

## 2．重要インフラの情報セキュリティ対策の現状と課題

◆ 第３次行動計画に基づく施策群により、自主的な取組が浸透しつつあるが、ＰＤＣＡのうちＣＡに課題。一部で先導的な取組も進展。

◆ 機能保証のため、情報系（ＩＴ）に限らず、制御系（ＯＴ）を含めた情報共有の質・量の改善や、重要インフラサービス障害に備えた対処態勢の整備が必要。

◆ 国内外の多様な主体との連携、情報収集・分析に基づく国民への適切な発信の継続・改善が必要。

## 3．本行動計画の３つの重点

次の３つを重点として、第３次行動計画の５つの施策群の補強・改善を図る。

### ① 先導的取組の推進（クラス分け）

■ 他分野からの依存度が高く、比較的短時間のサービス障害でも影響が拡大するおそれがある分野（例：電力、通信、金融）において、一部事業者における先導的な取組（ＩＳＡＣ※の設置やリスクマネジメントの確立等）を強化・推進

※所属事業者間で秘密保持契約を締結するなど、より機密性の高い情報の共有等を目的とした組織

■ 上記先導的な取組みの、当該重要インフラ分野内の他の事業者等及び他の重要インフラ分野への展開による我が国全体の防護能力の強化

### ② オリパラ大会も見据えた情報共有体制の強化

■ サービス障害の深刻度判断基準の導入に向けた検討

■ 連絡形態の多様化（連絡元の匿名化、セプター※事務局・情報セキュリティ関係機関経由）による情報共有の障壁の排除。分野横断的な情報を内閣官房に集約する仕組みの検討

※重要インフラ事業者等の情報共有を担う組織

■ ホットライン構築も可能な情報共有システムの整備（自動化、省力化、迅速化、確実化）

■ 情報連絡・情報提供の範囲にＯＴ、ＩｏＴ等を含むことを明確化（ＩＴ障害→重要インフラサービス障害）

■ 演習の改善、演習成果の浸透による防護能力の維持・向上

■ サプライチェーンを含む「面としての防護」に向け範囲の拡大

### ③ リスクマネジメントを踏まえた対処態勢整備の推進

■ 「機能保証に向けたリスクアセスメントガイドライン」の提供及び説明会の実施等によるリスクアセスメントの浸透

■ 事業継続計画及び緊急時対応計画（コンティンジェンシープラン）の策定等による重要インフラ事業者等の対処態勢の整備

■ 事業者等における内部監査等の取組において、リスクマネジメント及び対処態勢における監査の観点の提供等による「モニタリング及びレビュー」を強化

## 4．本行動計画の期間

➢ 第４次行動計画（案）はオリパラ大会開催までを視野に入れ、大会終了後に見直しを実施。その間であっても、必要に応じて見直す。



（出典）サイバーセキュリティ戦略本部会合資料（2017年3月）

# 機能(任務)保障の考え方

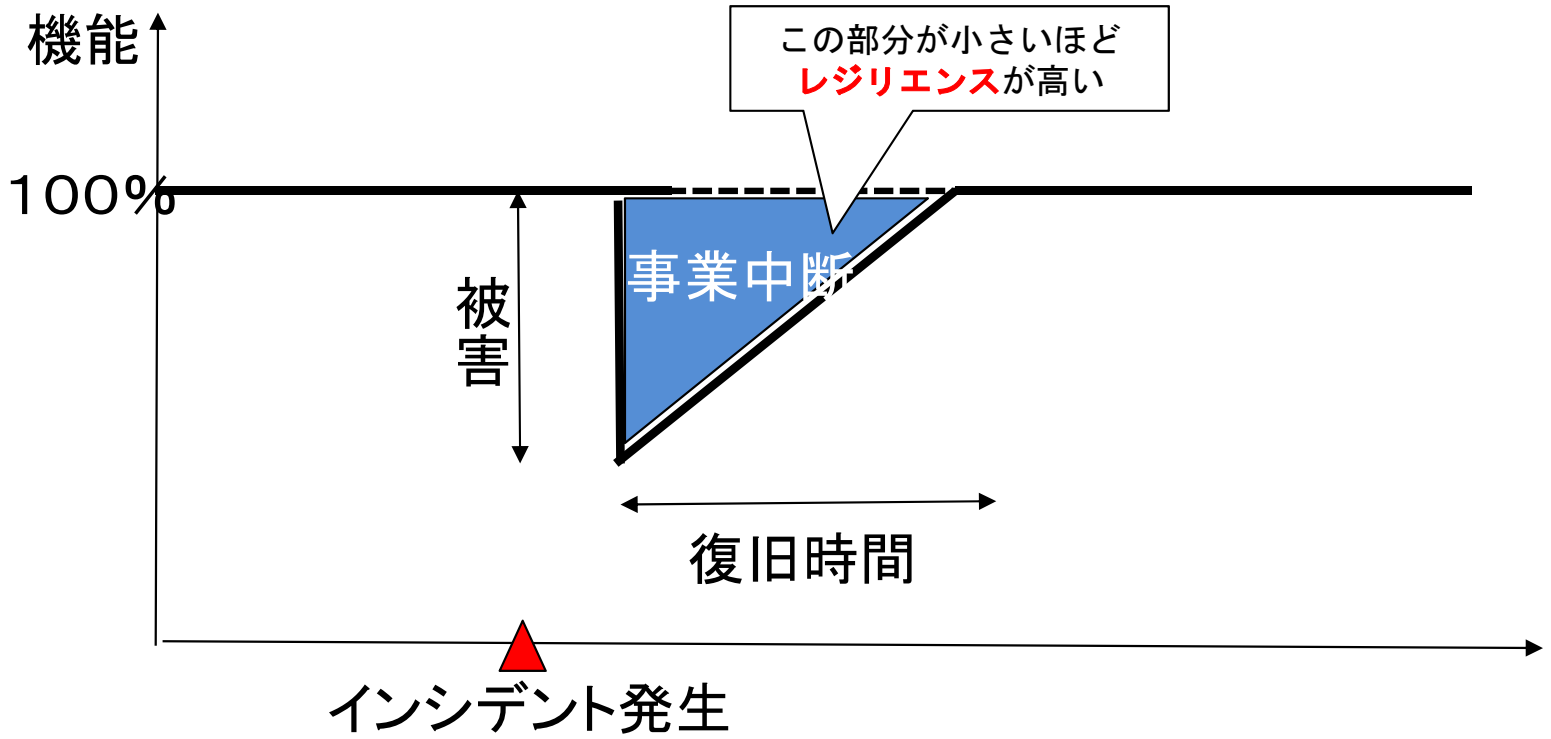


## 機能保障 (Mission Assurance)

(DoDの)任務に必須の機能の性能(パフォーマンス)に不可欠な能力・資産※の継続的な機能とレジリエンスを防御・確保するプロセス

※要員、装備、施設、ネットワーク、情報及び情報システム、インフラ及びサプライチェーンを含む。

(出典)DoD "Mission Assurance Strategy" (April 2012)




(出典)「レジリエンス社会」をつくる研究会編 "しなやかな社会の挑戦"(2016年3月、日経BPコンサルティング)を基に一部修正。

# NICTナショナルサイバーセキュリティセンター（17年4月設立）



■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企業等に対するサイバー攻撃について、実践的な演習を実施

⇒ *47都道府県で演習を実施し、演習規模を3000人まで拡大*

■2020年東京オリンピック・パラリンピック競技大会の適切な運営に向けたセキュリティ人材の育成

⇒ *2020年東京大会開催時に想定される、IoTを含む高度な攻撃に対応した演習を実施*

■若手セキュリティエンジニアの育成

⇒ *高専や大学等を通じて若手人材を募集し、セキュリティの技術開発を本格指導（29年度から実施）*

【平成29年度予算】 ナショナルサイバートレーニングセンターの構築：15.0億円
（【平成28年度予算】サイバー攻撃複合防御モデル・実践演習：7.2億円）


実践的な防御演習


東京大会に向けた人材育成

若手セキュリティエンジニアの育成

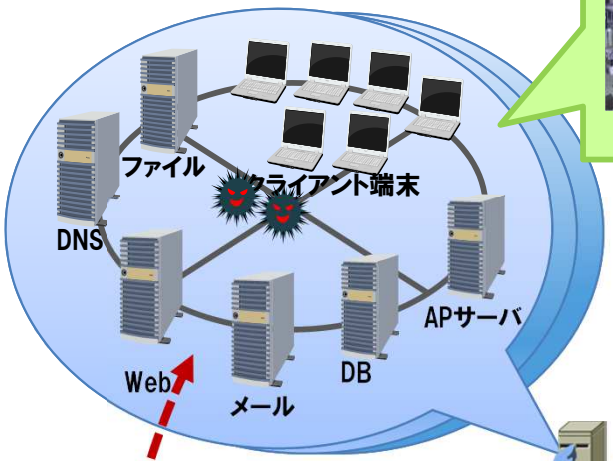
「ナショナルサイバートレーニングセンター」でプラットフォーム化

# 実践的サイバー防御演習

## CYDER: CYber Defense Exercise with Recurrence）

### 演習のイメージ

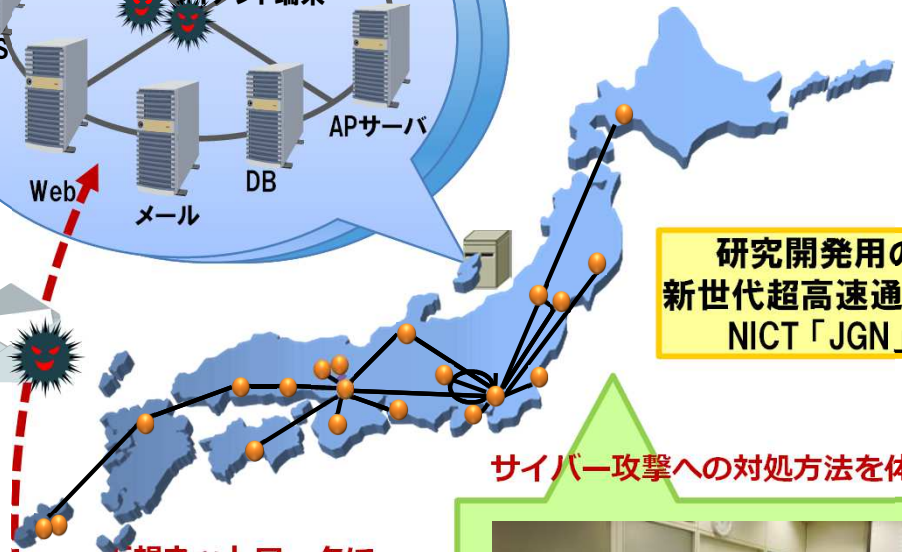
**大規模仮想LAN環境**
**（NICT「StarBED」により実現）**





石川県能美市

研究開発用の
新世代超高速通信網
NICT「JGN」



仮想ネットワークに
対して疑似攻撃を実施
（実際の不正プログラムを使用）

疑似攻撃者

サイバー攻撃への対処方法を体得

演習会場

### 演習の特徴

- **サイバー攻撃が発生した場合の被害を最小化するための一連の対処方法**（攻撃を受けた端末の特定・隔離、通信記録の解析による侵入経路や被害範囲の特定、同種攻撃の防御策、上司への報告等）**を体得**
- **150台の高性能サーバを用いた数千人規模の仮想ネットワーク環境**（国の行政機関や大企業を想定）**上で演習を実施**
- **我が国固有のサイバー攻撃事例を徹底分析し、最新の演習シナリオを用意**

### 平成２８年度の実施内容

**技術的知見を有するNICTを実施主体とするため、NICTへの業務追加を行う法改正を実施。**

（平成28年4月20日成立、5月31日施行）

→ **地方自治体等に対象を拡大し、全国11地域において、約1500人に実施**

### 平成29年度の実施予定

**演習規模を拡大し、全国47都道府県において約3000人に対し実施予定。**

# 2020東京大会に向けたサイバー演習

**2020年東京オリンピック・パラリンピックを想定した大規模演習基盤による演習の実施　（”サイバー・コロッセオ”）**

イメージ図


攻防戦によるサイバー演習


具体的内容

- 大規模クラウド環境を用いて、公式サイト、大会運営システムや、社会インフラの情報システム等を模擬したシステムを構築。
- 当該システムにより、大会開催時に想定されるサイバー攻撃を再現し、大会組織委員会のセキュリティ担当者を中心に、攻撃・防御手法の検証及び訓練を行う。

**大規模な演習を実施し、2020東京大会のサイバーセキュリティを確保**

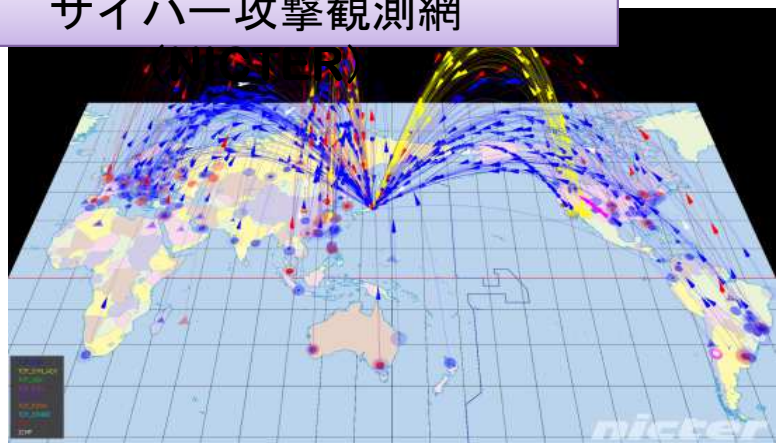
# 若手セキュリティエンジニア育成プログラム“SecHack365”



①未来のサイバーセキュリティ研究者・起業家の創出に向けて、NICTが若年層のICT人材を対象に、高度なセキュリティ技術を本格的に指導。
②NICTが、高専及び大学等と連携して若手ICT人材を公募し、自身の持つサイバーセキュリティの研究資産を活用し、実地研修及び遠隔開発による年間カリキュラムを用意。

## NICTの主な研究資産

### サイバー攻撃観測網



・未使用IPアドレスへの通信を観測し、サイバー攻撃の量や地理的情報等を可視化

### 大規模クラウド環境（StarBED）


・150台の高性能サーバから成る大規模な仮想ネットワークにより、サイバー演習環境を構築

## 対象者

・ 日本国内に居住する25歳以下の若手ICT人材
（NICTにおける選考の結果、47名が受講）

# 情報共有分析センター「ISAC」を通じた事業者間連携の強化



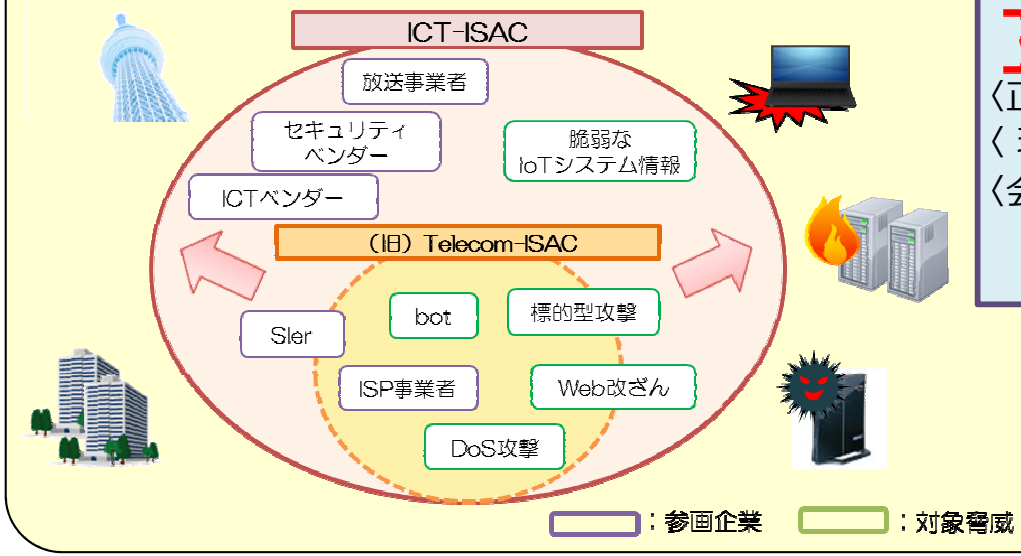
○ サイバー攻撃のインシデント情報等を収集・分析し、業界内で共有することを目的として、事業分野ごとに **ISAC（Information Sharing and Analysis Center：情報共有分析センター）**が設立され活動中。

○ 国内では、**2002年に他分野に先立ち、通信分野で「Telecom-ISAC Japan」が設立**。その後、**2014年に金融分野で「金融ISAC」が設立。2017年に電力分野で「電力ISAC」が設立**。

○ さらに、ICT分野全体にわたる情報共有機能を強化するため、「Telecom-ISAC Japan」が一般財団法人日本データ通信協会から独立し、**2016年３月に「ICT-ISAC Japan」として一般社団法人化**。ISP事業者の他、放送事業者、ICTベンダー及びセキュリティベンダー等にも働きかけ、順次拡大。

○ このような活動を通して、**他分野にも対しても情報共有の模範となるような先行的な情報共有モデルを示しつつ、我が国全体の情報共有機能強化を目指す**。

## 国内におけるISAC組織例：「ICT-ISAC Japan」の概要




ICT-ISAC JAPAN

〈正式名称〉（一社）ICT-ISAC

〈 理事長 〉齊藤忠夫

〈会員企業〉Telecom-ISACの既存会員であるISP事業者が順次移行するとともに、放送事業者、ICTベンダー及びセキュリティベンダー等にも働きかけ、順次拡大

Telecom-ISAC Japan

〈正式名称〉

〈 会　長 〉

〈会員企業〉

2017年7月現在、米国では、①自動車 ②航空、③通信、④防衛産業、⑤天然ガス供給事業、⑥電力、⑦危機管理、⑧金融、⑨情報技術、⑩海運、⑪自治体、⑫国民健康、⑬石油・天然ガス、⑭不動産、⑮研究・教育、⑯小売・サービス、⑰サプライチェーン、⑱陸上輸送、⑲公共輸送、⑳輸送バス、㉑水の21分野でISACが設置・活動中。

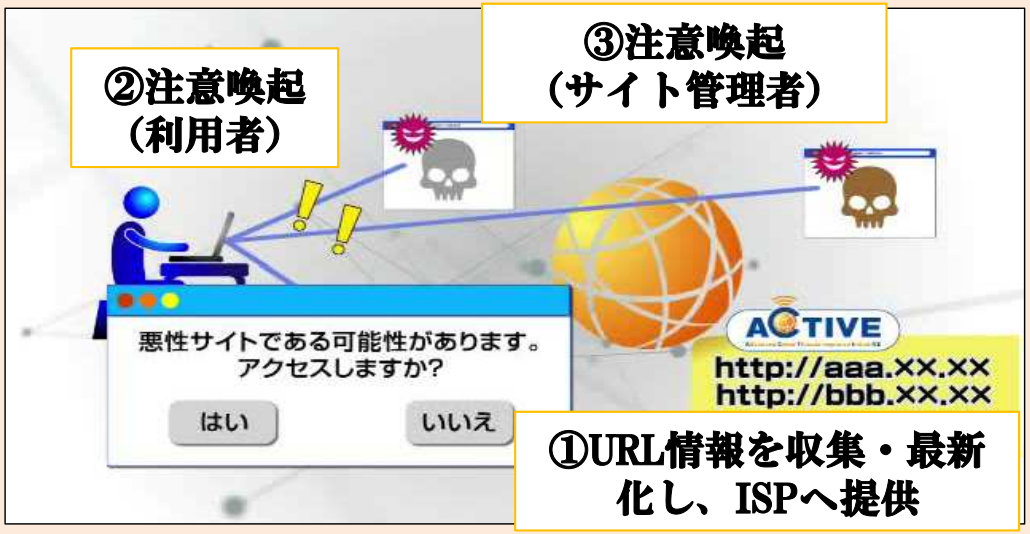
# ウィルス感染被害予防対策“ACTIVE”



平成25年11月からインターネットサービスプロバイダ（ISP）等との協力により、インターネット利用者を対象に、マルウェア配布サイトへのアクセスを未然に防止する等の実証実験を行う官民連携プロジェクト（ACTIVE）を実施。

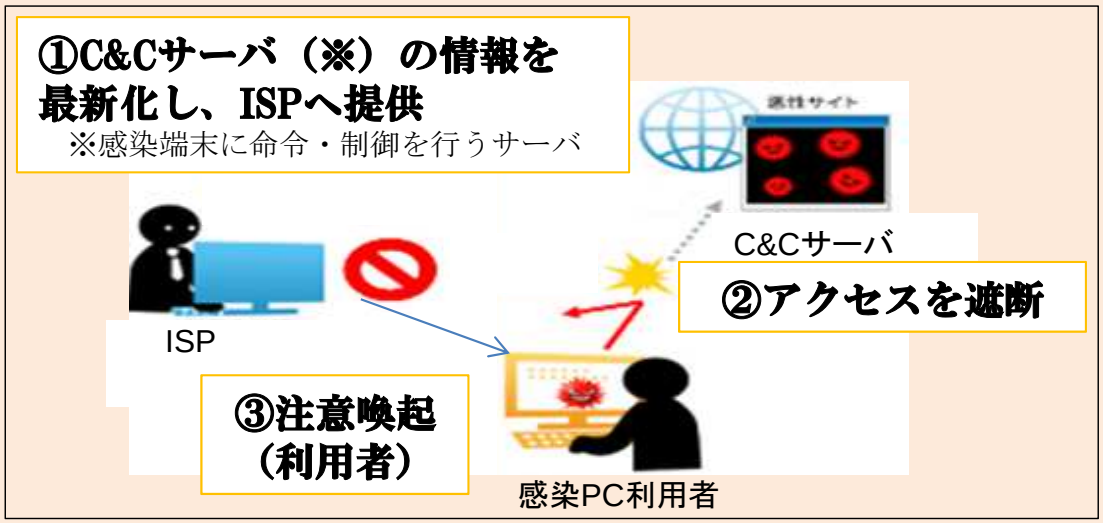
## ACTIVE（Advanced Cyber Threats response InitiatiVE）の取組

### （１）マルウェア感染防止の取組




**①マルウェア配布サイトのURL情報を最新化し、ISPへ提供。**
②マルウェア配布サイトにアクセスしようとする利用者にISPから注意喚起。
③マルウェア配布サイトの管理者に対しても適切な対策を取るよう注意喚起。

### （２）マルウェア被害未然防止の取組




**① C&Cサーバの情報を最新化し、ISPへ提供。**
② 感染PC利用者からのC&Cサーバへのアクセスを遮断する。
（2016年2月から2017年5月までに約1億297万件の遮断実績）
③ 感染PC利用者に注意喚起。

○ 実施期間：平成25～29年度
○ 所 要 額：平成25年度予算　4.8億円　　平成28年度予算　4.0億円の内数
　　平成26年度予算　3.5億円　　平成29年度予算　3.8億円の内数
　　平成27年度予算　2.3億円

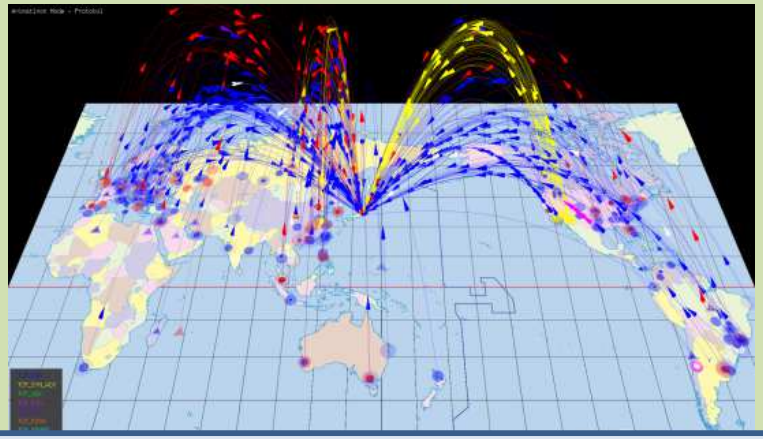
# 情報通信研究機構（NICT）におけるサイバーセキュリティ技術の成果展開



■　国立研究開発法人 情報通信研究機構（ＮＩＣＴ）では、研究開発の一環として、サイバーセキュリティ技術の成果展開を実施。無差別攻撃型（マルウェア）対策技術については、多くの自治体に導入が進むとともに、年金機構に対しても使用された標的型攻撃対策についても、早期導入に向けた取り組みを推進。

## ◆NICTER（ニクター）　【無差別型攻撃対策】

・ ダークネット（未使用ＩＰアドレス）への通信をセンサーで観測することで、**サイバー攻撃の地理的情報や攻撃量、攻撃手法等をリアルタイムに可視化**。
・ 本技術を応用して、地方公共団体情報システム機構（J-LIS）との協力により、**マルウェアに感染した自治体へアラートを提供**。



**６００自治体に導入済み**
**（２０１７年4月時点）**

## ◆NIRVANA改（ニルヴァーナ・カイ）　【標的型攻撃対策】

・ NICTERの技術を応用し、組織内にセンサーを設置して**組織内の通信状況をリアルタイムに可視化**するとともに、本技術について**2015年6月から技術移転開始**。
・ さらに、本技術と組み合わせ、**ネットワーク内での異常検知時に通信を自動遮断する技術**等を開発中。

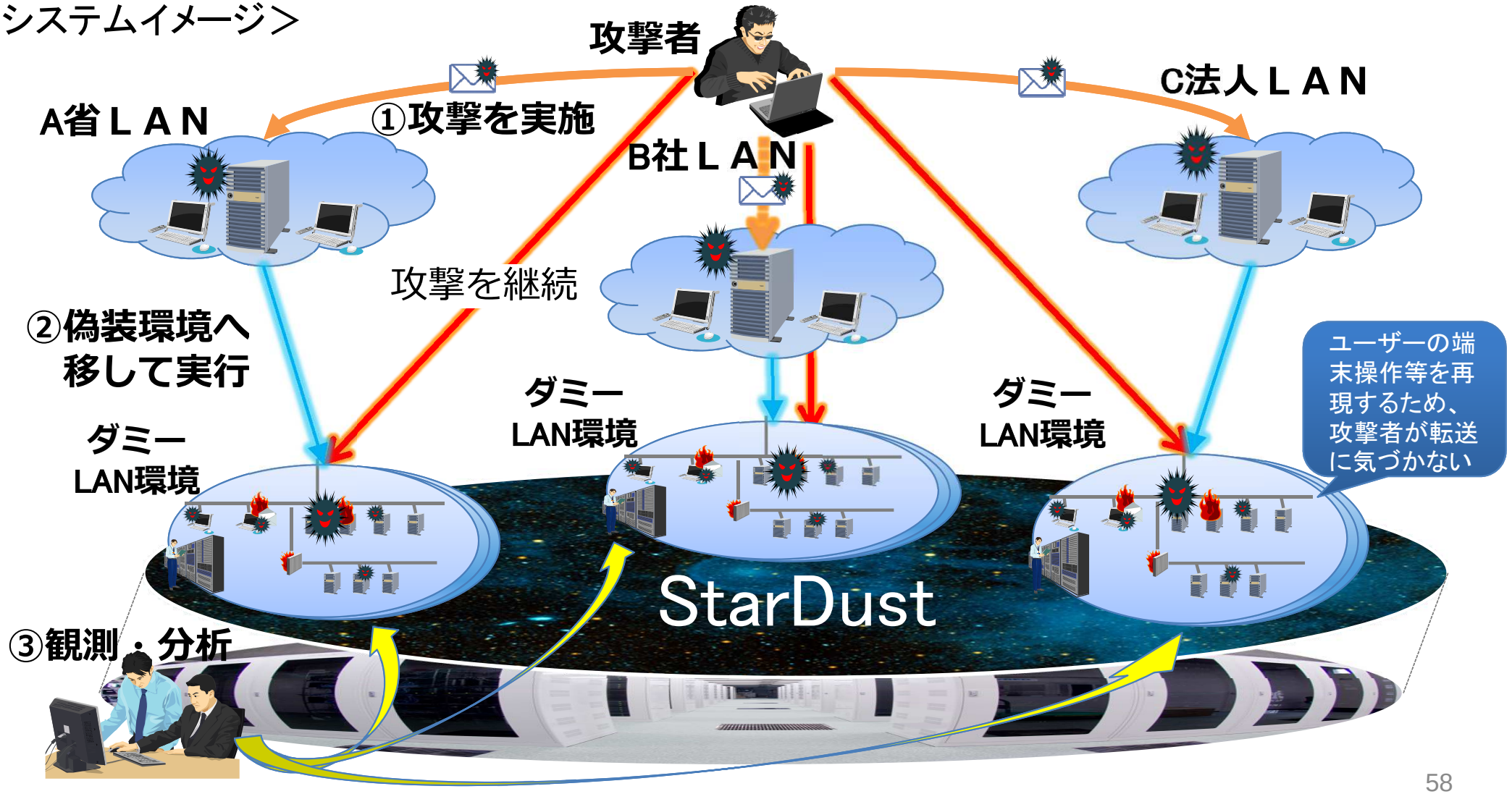

**技術移転を開始**
**（２０１５年６月）**

# サイバー攻撃誘引基盤（STARDUST）



■ NICTでは、標的型サイバー攻撃の詳細な手法を把握するため、①攻撃者が標的型メールを特定組織に送信した場合に、②不正な添付ファイル等を「あらかじめ構築した偽装環境」で実行し、③偽装環境で具体的な攻撃手段（入力コマンド等）の観測・分析が可能なシステム（StarDust）を研究開発している。

＜システムイメージ＞



# 未来投資戦略2017（サイバーセキュリティの確保、抜粋）

■IoT機器のセキュリティ対策の強化に向けて、継続的かつ広範な実態の把握、利用者等への対策の実施・周知、同様の被害を防止する取り組み等を推進するための官民等の関係者による連携の枠組みを本年度中に構築し、必要な対策を推進する。

■セキュリティ産業の活性化を推進するため、需要・供給両面から取り組みを進め、好循環を生み出す。

需要面に関しては、

- ●政府が積極的に調達すべきセキュリティ製品・サービス分野及び要件の明確化とリストの改定による活用の奨励
- ●サイバーセキュリティ経営ガイドライン等の普及啓発による中小企業も含めた更なる意識改革を図る
- ●IoT産業等の関連産業等の成長を見据え、企業におけるセキュリティ投資を促進

供給面に関しては、

- ●本年度中に一定の品質を備えたセキュリティ製品・サービスの認定制度を整備し、その供給を促す
- ●本年度中に策定する「サイバーセキュリティ研究開発戦略」に基づく技術開発やセキュリティバイデザインの普及推進等を図り、セキュリティ産業の国際競争力強化等を図る

# 国家安全保障戦略（１３年１２月閣議決定）

## Ⅲ　我が国を取り巻く安全保障環境と国家安全保障上の課題

### １　グローバルな安全保障環境と課題

#### （４）国際公共財（グローバル・コモンズ）に関するリスク

近年、海洋、宇宙空間、サイバー空間といった国際公共財（グローバル・コモンズ）に対する自由なアクセス及びその活用を妨げるリスクが拡散し、深刻化している。

（中　　略）

情報システムや情報通信ネットワーク等により構成されるグローバルな空間であるサイバー空間は、社会活動、経済活動、軍事活動等のあらゆる活動が依拠する場となっている。

一方、国家の秘密情報の窃取、基幹的な社会インフラシステムの破壊、軍事システムの妨害を意図したサイバー攻撃等によるリスクが深刻化しつつある。

我が国においても、社会システムを始め、あらゆるものがネットワーク化されつつある。このため、情報の自由な流通による経済成長やイノベーションを推進するために必要な場であるサイバー空間の防護は、我が国の安全保障を万全とする観点から、不可欠である。

# サイバー空間と国際法の適用関係（国連GGE、１５年６月）



*"In their use of ICTs,* ***States must observe, among other principles of international law, State sovereignty, the settlement of disputes by peaceful measures, and non-intervention in the internal affairs of States****."*（サイバー空間における国家主権、平和的紛争解決等）

*"****Existing obligations under international law are applicable to State use of ICTs*** *and States must comply with their obligations to respect and protect human rights and fundamental freedoms."*（国際法はサイバー空間に適用可能）

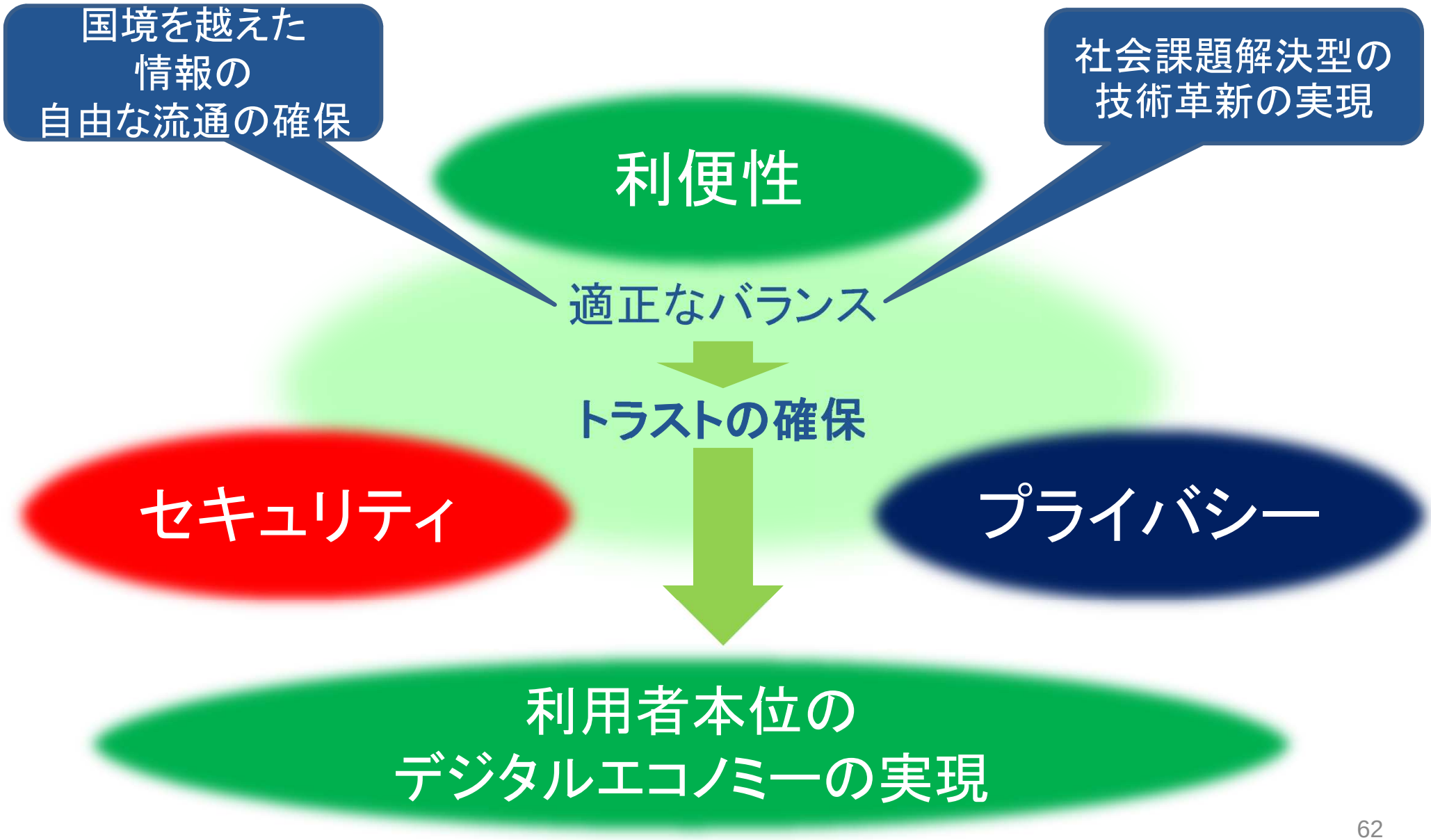
*"****States must not use proxies to commit internationally wrongful acts using ICTs****, and should seek to ensure that their territory is not used by non-State actors to commit such acts."*（サイバー空間における違法行為等への関与の禁止）

*"****The UN should play a leading role in promoting dialogue on the security of ICTs in their use by States****, and in developing common understandings on the application of international law and norms, rules and principles for responsible State behavior."*（サイバー空間を巡る議論における国連の主導的役割）

(Source) UN General Assembly, Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security (June 2015)

# デジタルエコノミーに求められる要素





# Any Question?