総務省
Ministry of Internal Affairs and Communications

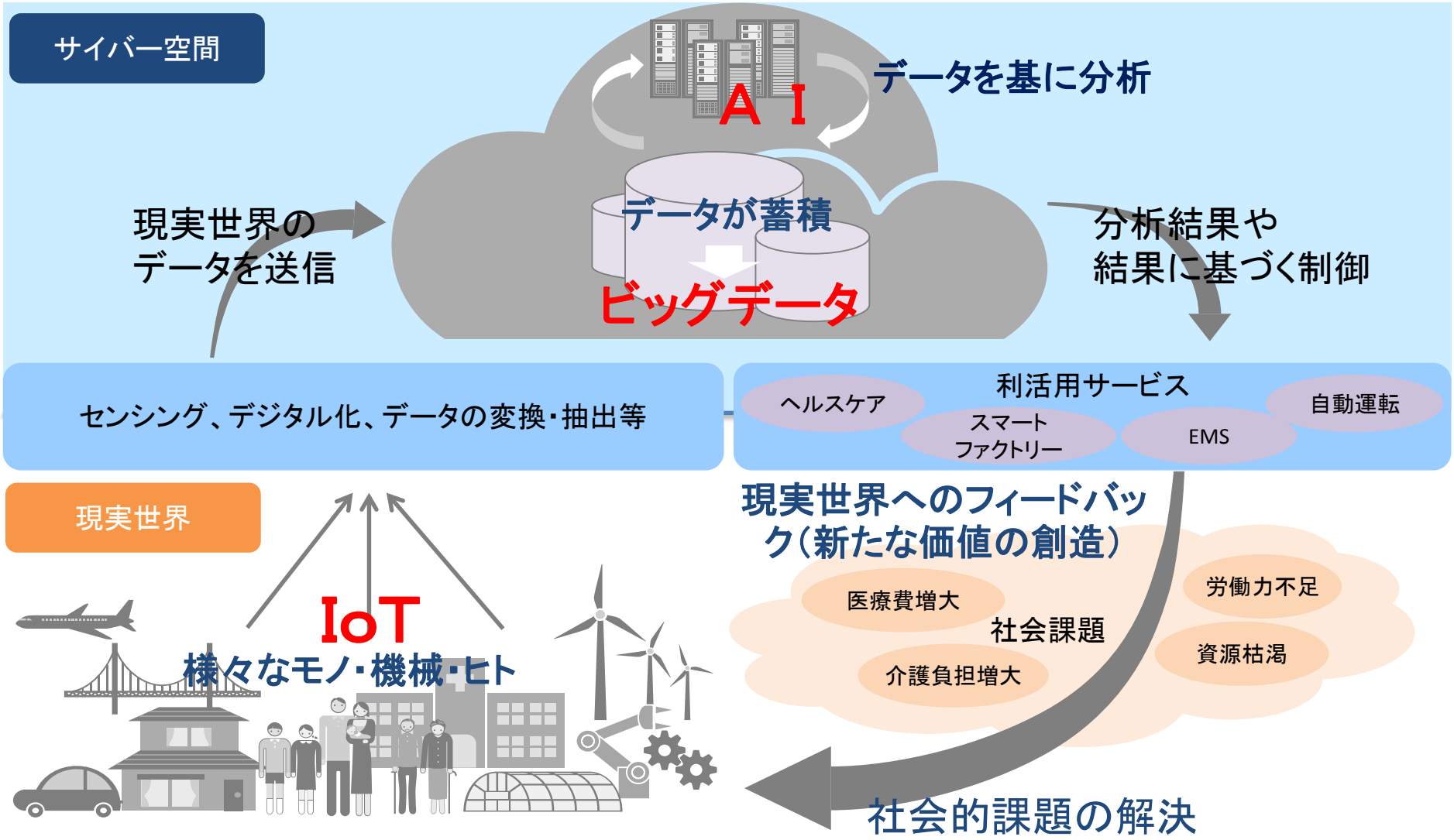
総務省におけるサイバーセキュリティ政策の最前線

2019年2月8日

総務省　サイバーセキュリティ統括官室
参事官補佐

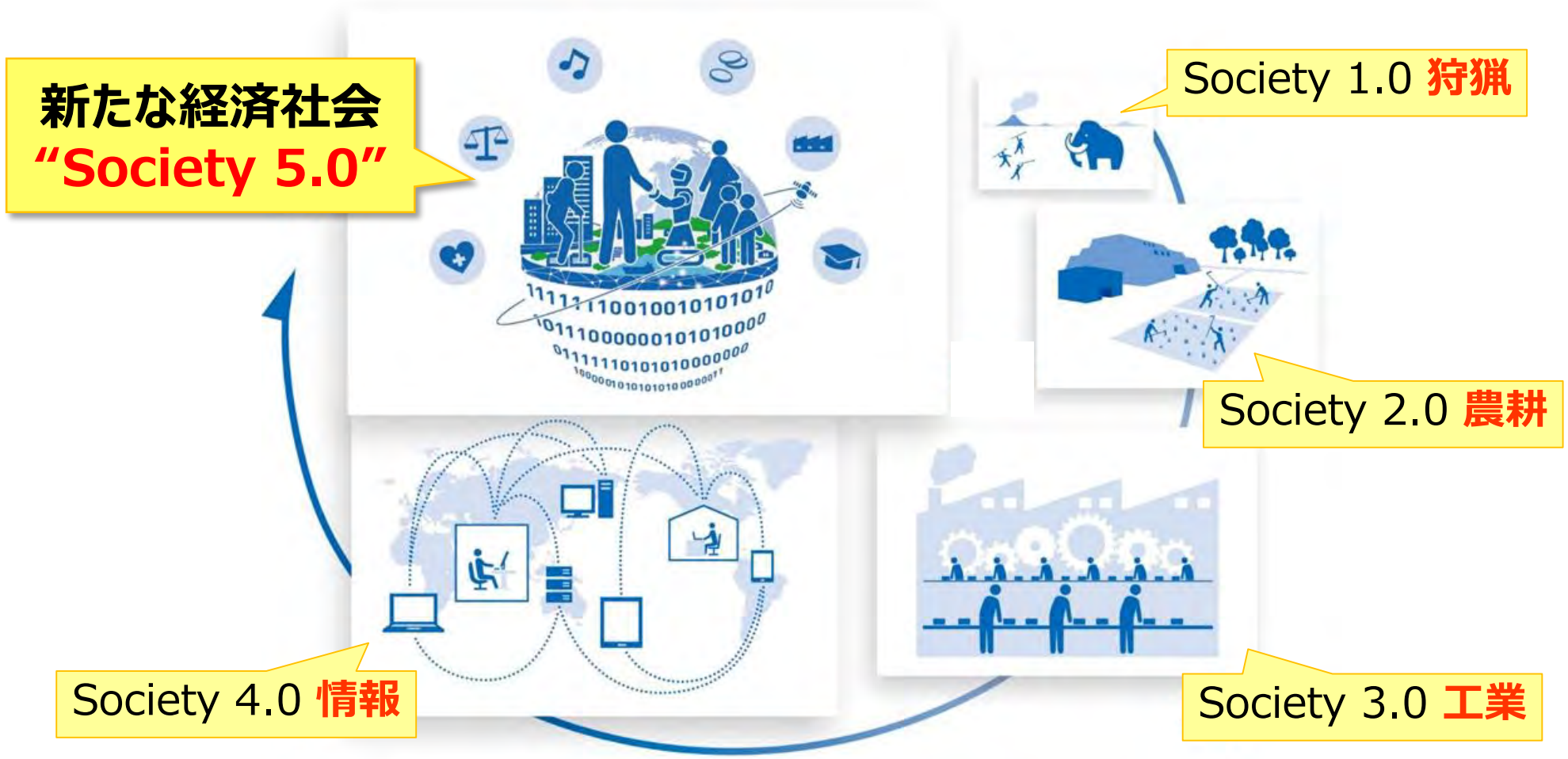
相川　航

データ主導社会


サイバー空間
AI
データを基に分析
現実世界の
データを送信
データが蓄積
ビッグデータ
分析結果や
結果に基づく制御
センシング、デジタル化、データの変換・抽出等
利活用サービス
ヘルスケア
スマート
ファクトリー
EMS
自動運転
現実世界
IoT
様々なモノ・機械・ヒト
現実世界へのフィードバック（新たな価値の創造）
医療費増大
介護負担増大
社会課題
労働力不足
資源枯渇
社会的課題の解決

Society 5.0とは

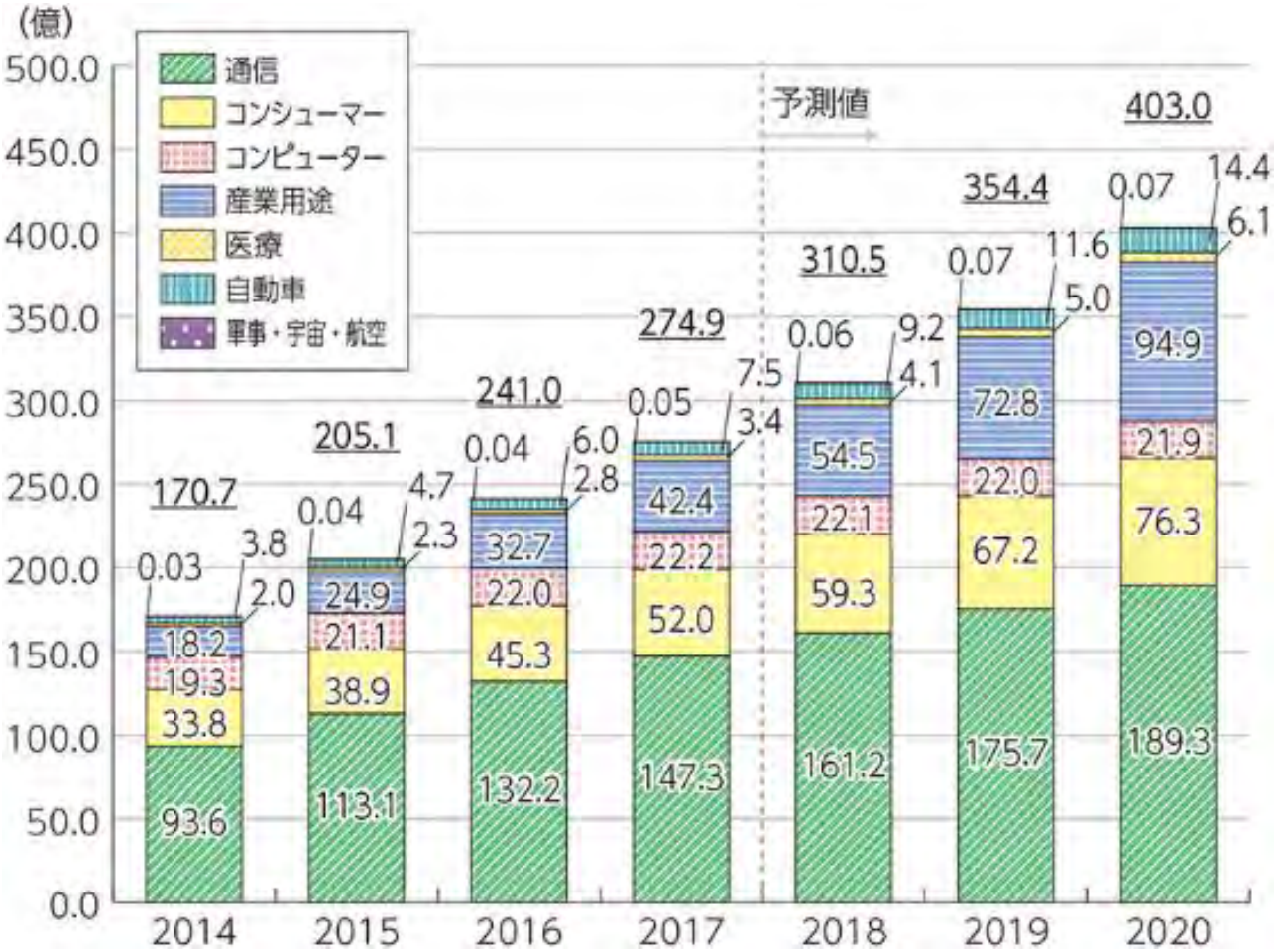
サイバー空間とフィジカル（現実）空間を高度に融合させたシステムにより、
経済発展と社会的課題の解決を両立する、
人間中心の**社会（Society）**

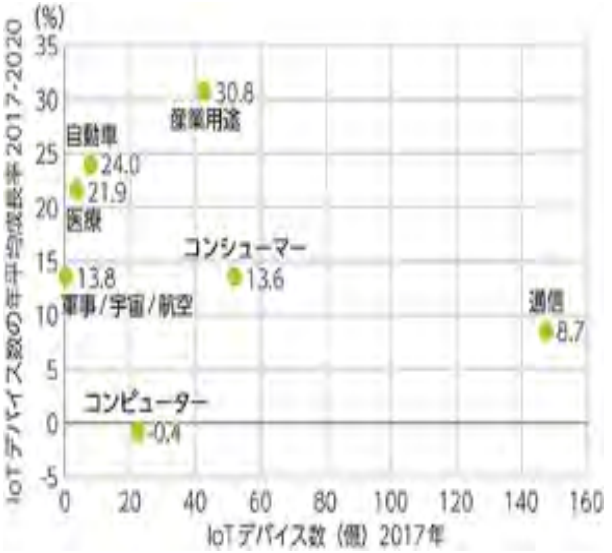


[内閣府作成]

世界のIoTデバイス数

- ✓ 2017年時点で稼働数が多いのはスマートフォンや通信機器などの「通信」。ただ、それらは市場が成熟しているため、今後は、相対的に低成長が見込まれる。
- ✓ 今後は、コネクテッドカーの普及によりIoT化の進展が見込まれる「自動車・輸送機器」、デジタルヘルスケアの市場が拡大している「医療」、スマート工場やスマートシティが拡大する「産業用途（工場、インフラ、物流）」などの高成長が予測される。





（出典）IHS　Technology

第５世代移動通信システム（５G）とは

5Gは、AI/IoT時代のICT基盤

低遅延

移動体無線技術の
高速・大容量化路線

２G　３G　４G

同時接続

5G

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

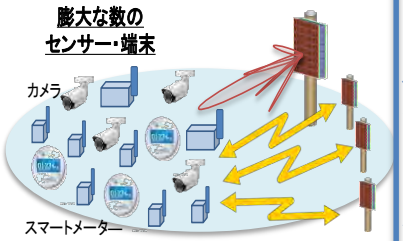
利用者が遅延（タイムラグ）を意識することなく、リアルタイムに遠隔地のロボット等を操作・制御

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

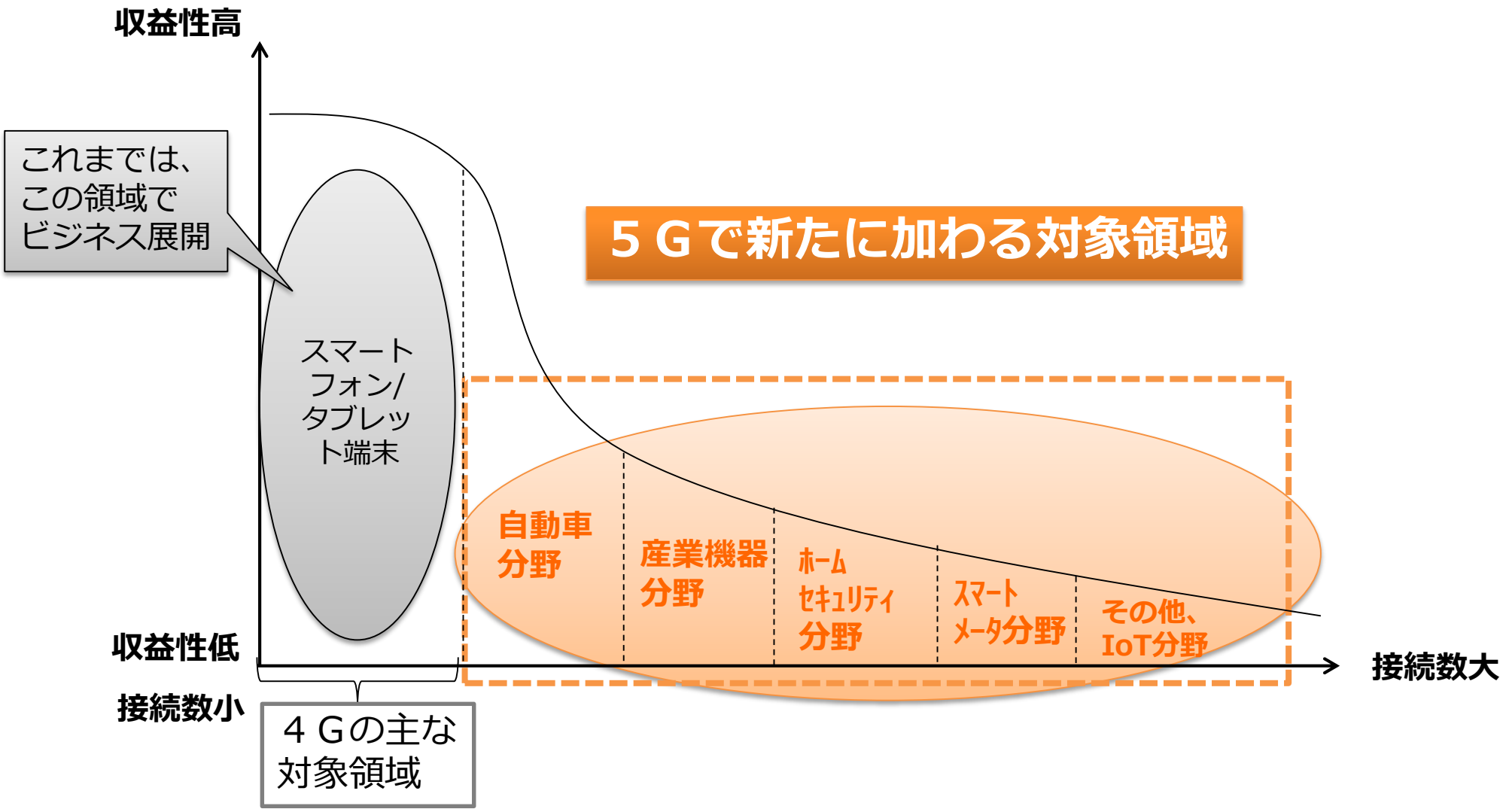


⇒ **自宅部屋内の約100個の端末・センサーがネットに接続**

（現行技術では、スマホ、PCなど数個）

社会的なインパクト大

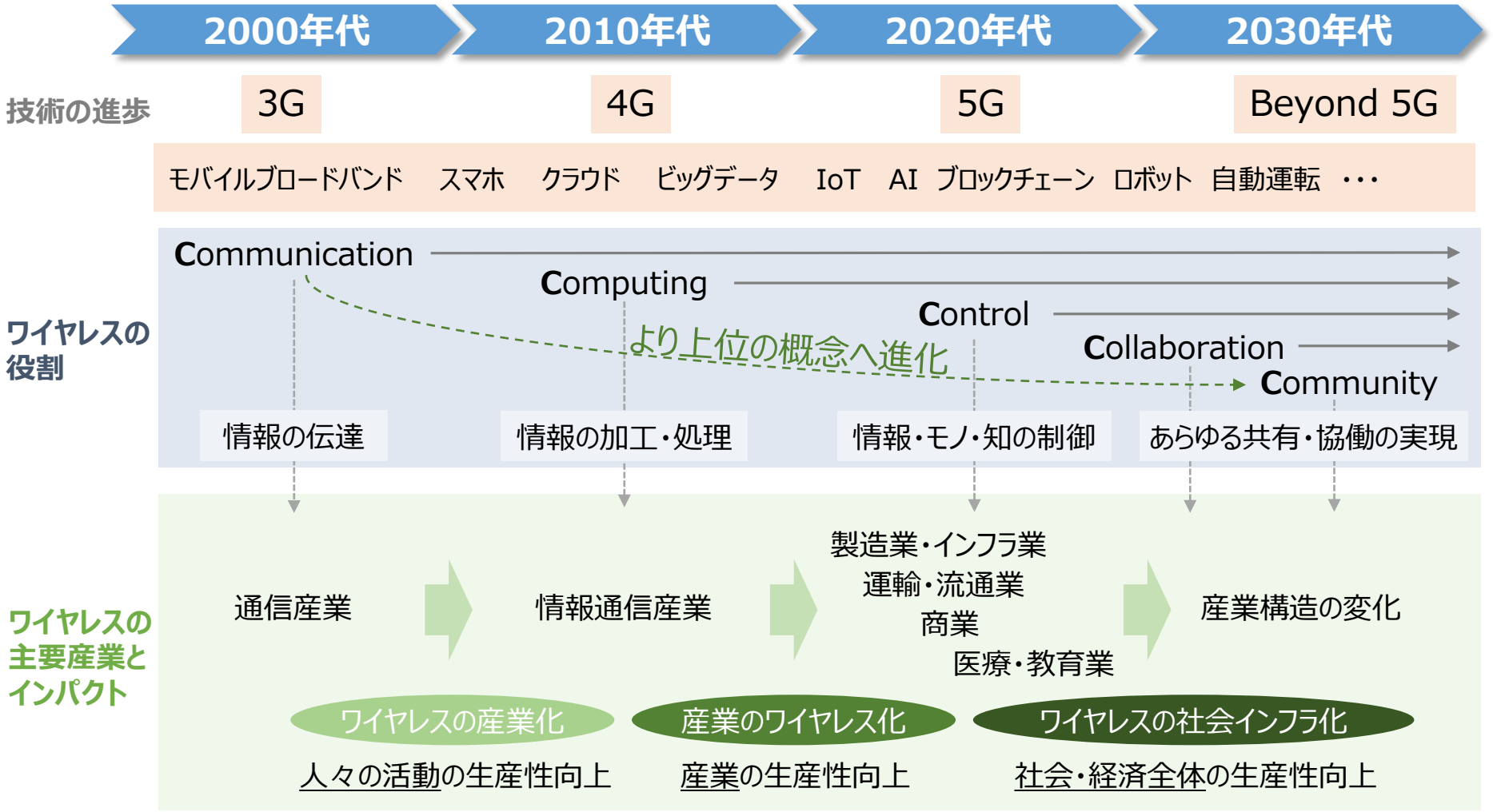
IoT時代の産業構造の変化



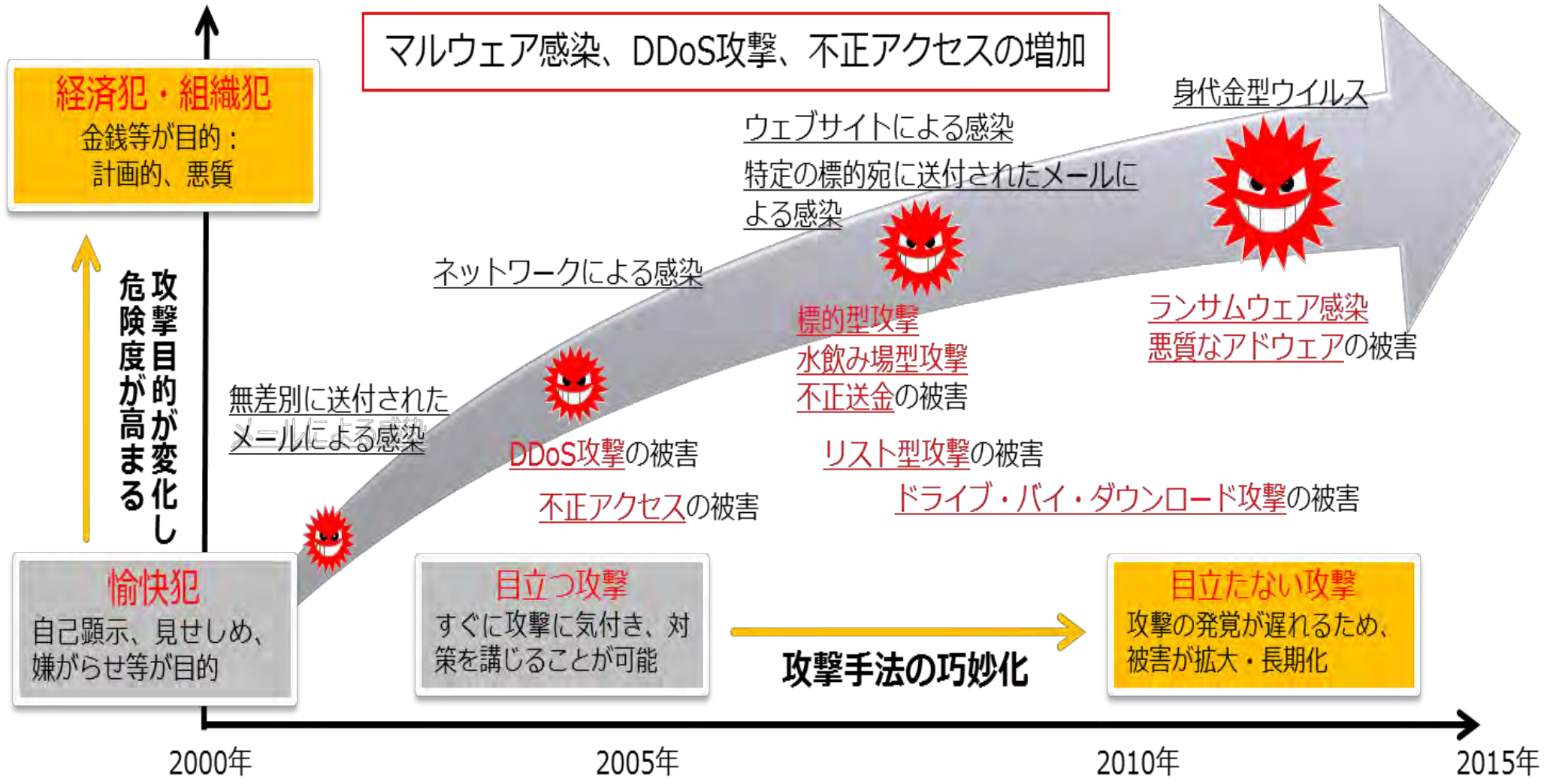
出典：日経コミュニケーション 2015/4月号を参考に作成

2030年代におけるワイヤレス

- ワイヤレス技術の機能は、情報の伝達手段（Communication）から、あらゆる共有や協働の実現手段（Collaboration）へと変わる
- ワイヤレスは通信産業からICT利用産業へと活躍の範囲を広げていき、2030年代にはあらゆる産業を支え、産業構造変化を促す社会インフラとなる



サイバーセキュリティ上の脅威の増大①



サイバーセキュリティ上の脅威の増大②

国内事例

2015年6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**）

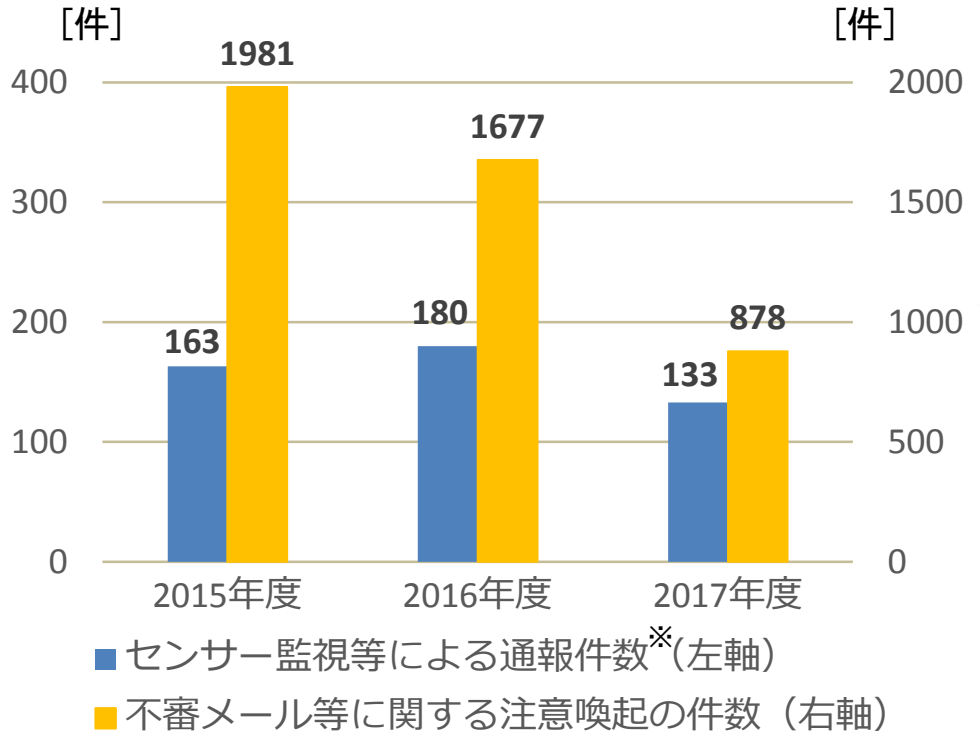
2016年10月：**米国のDyn社**のDNSサーバが大規模なDDoS攻撃を受け、同社のDNSサービスの提供を受けていた企業のサービスにアクセスしにくくなる等の障害が発生（**DDoS攻撃**）

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**）

リスクの深刻化

政府機関等への脅威

【政府機関等への脅威件数】



※ 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2017年度の特徴】

- センサー監視等による通報内容は、**ウェブアプリケーションの脆弱性を狙った攻撃、メールによる標的型攻撃がそれぞれ４割以上**。
- 不審メール等の注意喚起件数は減少しているものの、**依然として一定数を維持しており、攻撃は高度化・巧妙化している傾向**。

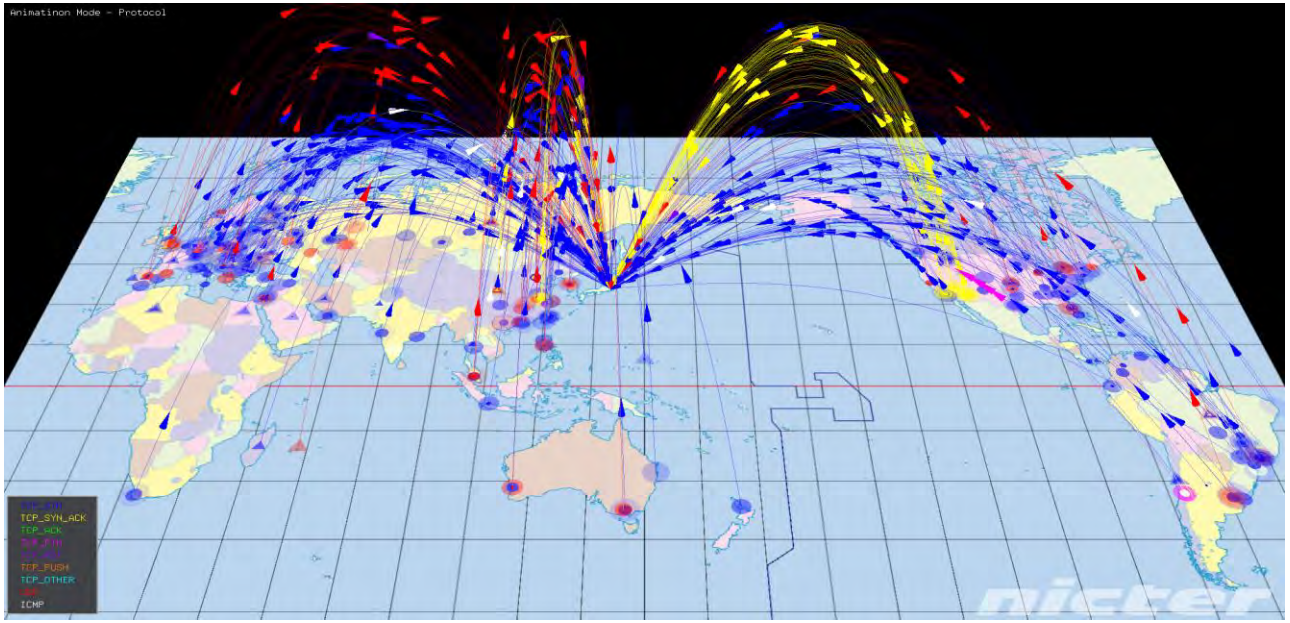
【政府機関等に対する2017年度の不審メールの傾向】

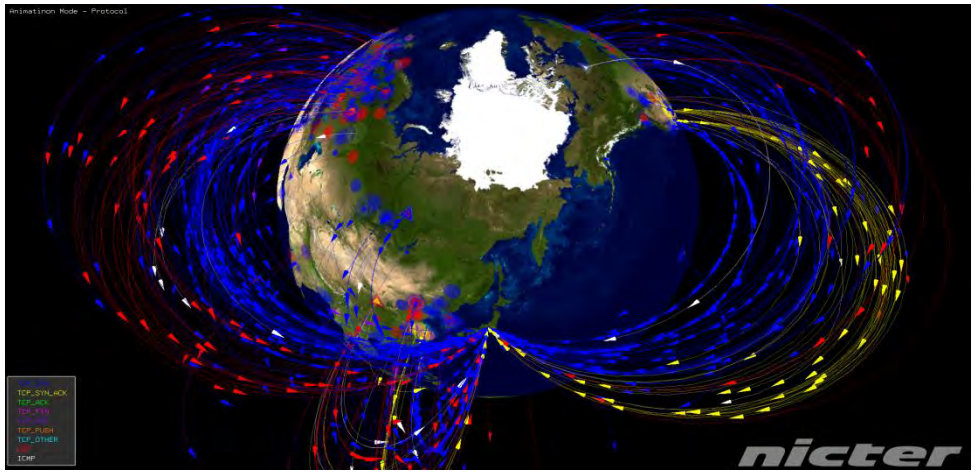
- 2016年度と比較して不審なファイルが添付されたメールの比率が減少し、**不審なURLが記載されたメールの比率が増加**。
- 不審メールに添付されたファイルの形式については、**約半数がOffice形式のファイル**であり、マクロを有効化すると悪性のマクロが動作し、インターネットからマルウェアをダウンロードさせるような攻撃を行うものも確認。

（参考）NISC「サイバーセキュリティ政策に係る年次報告（2017年度）」（2018年7月）

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

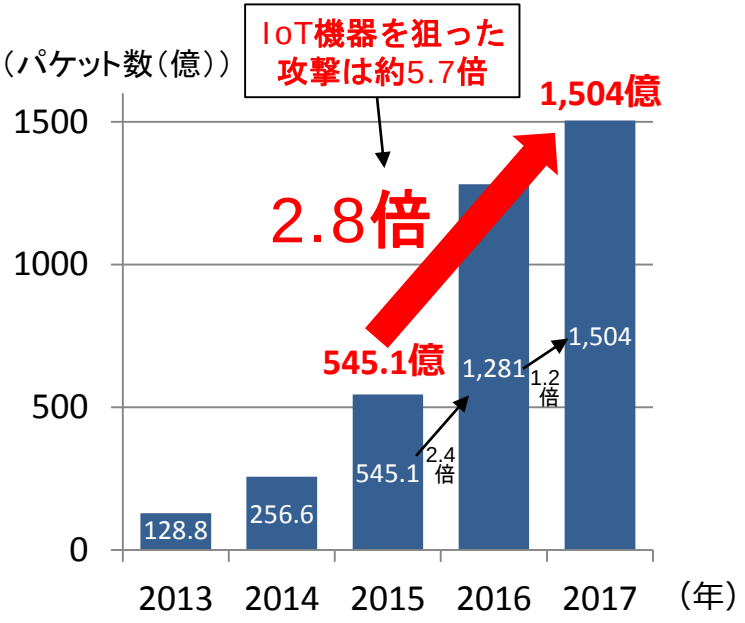
・ダークネットに飛来するパケットの送信元アドレスから緯度・経度を推定し、世界地図上で可視化

・色：パケットごとにプロトコル等を表現

NICTER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

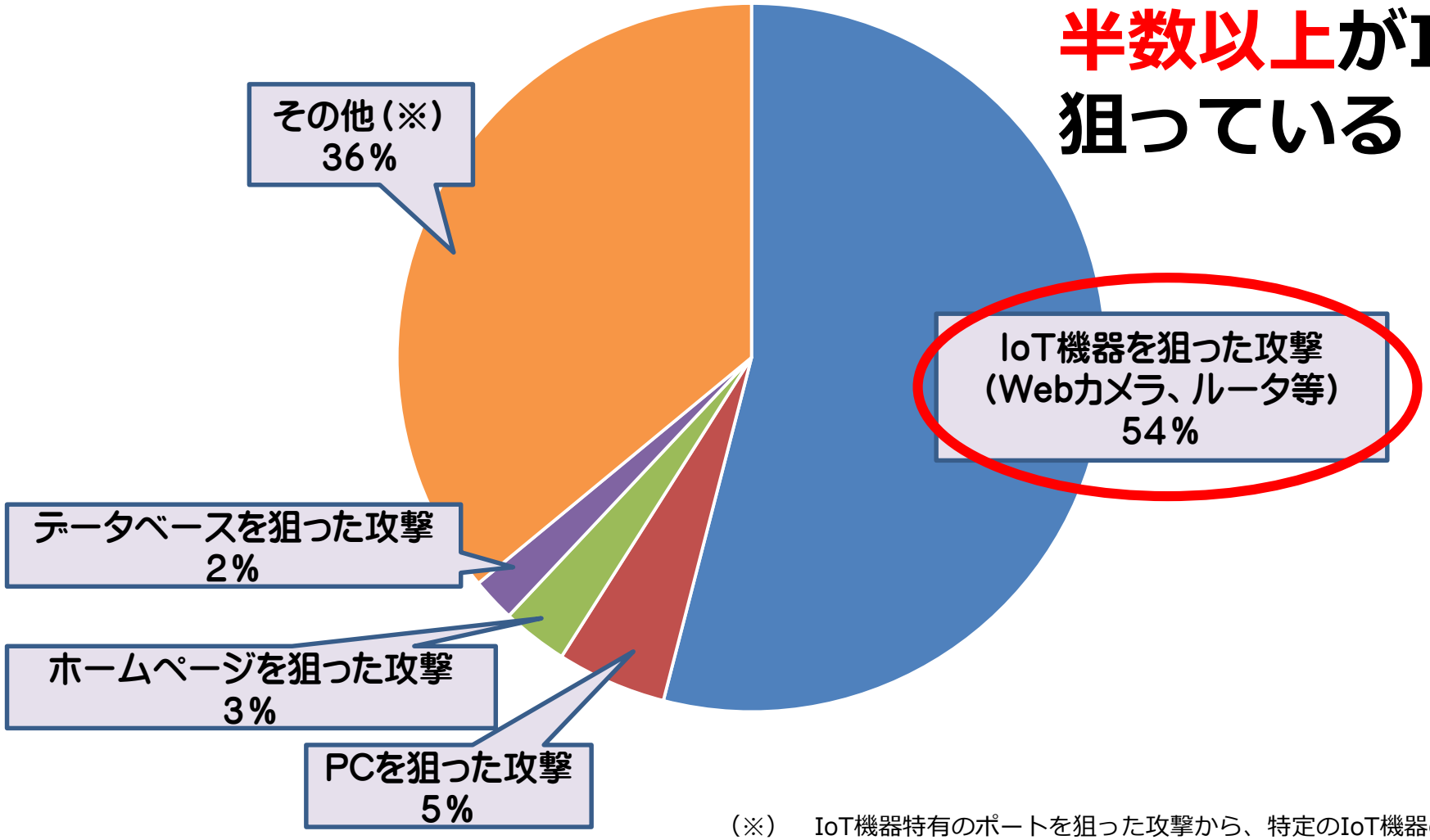
（2015年→2016年：2．4倍、2016年→2017年：1．2倍）



サイバー攻撃の内訳（平成29年、NICTERによる観測）

観測された全サイバー攻撃1,504億パケットのうち、

半数以上がIoTを狙っている！



（※）　IoT機器特有のポートを狙った攻撃から、特定のIoT機器の脆弱性を狙ったより高度な攻撃も観測されるようになっており、単純にポート番号だけから分類することが難しいIoT機器を狙った攻撃が「その他」に含まれている。

IoT機器のセキュリティ上の課題

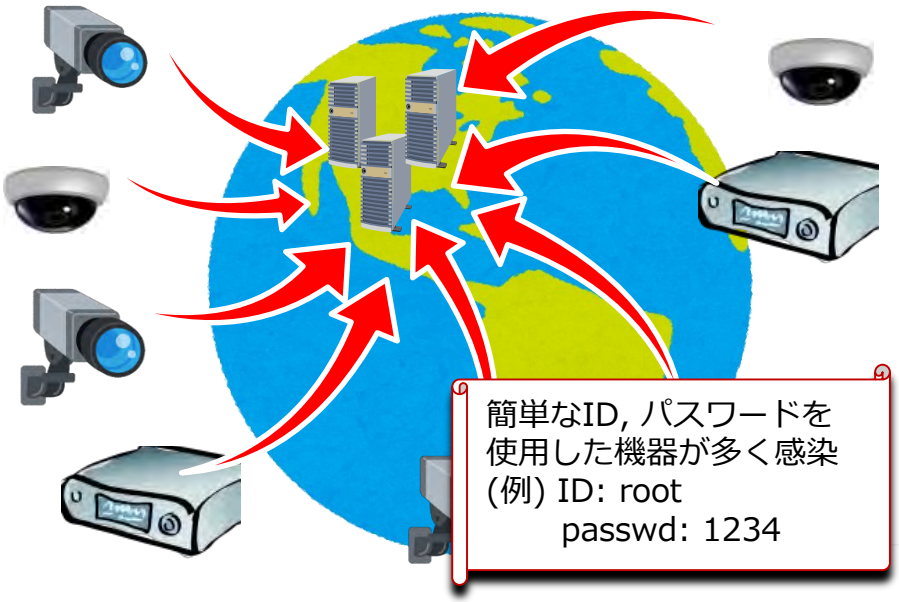
- IoT機器は、製造業者や利用者が機器のセキュリティ対策を講じる上で制約があり、長期間インターネットに接続されることから、乗っ取られやすく、サイバー攻撃に用いられやすい。
- また、IoT機器は数が多く、今後も急増する見込みであるため、乗っ取られる機器数も多くなり、攻撃に用いられるとインターネットの通信に著しい支障が生じるおそれがある。

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

IoTによる大規模DDoS攻撃について

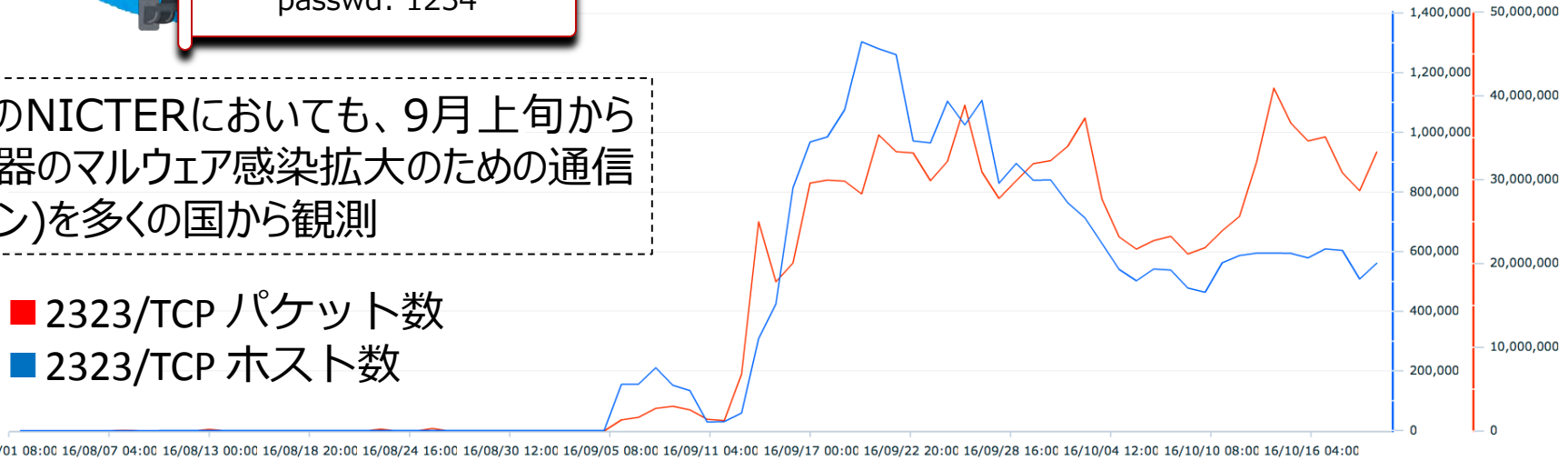
- **2016年10月21日米国のDyn社のDNSサーバーに対し、大規模なDDoS攻撃が２回発生。**
- **同社からDNSサービスの提供受けていた企業のサービスにアクセスしにくくなる等の障害が発生。**
- **サイバー攻撃の元は、「Mirai」というマルウェアに感染した大量のIoT機器。**



- ✓ 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。
- ✓ 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

出典: http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

- ✓ 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



政府全体のサイバーセキュリティ推進体制

内閣　内閣総理大臣

高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）

高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進

緊密連携

サイバーセキュリティ戦略本部（2015.1.9 ｻｲﾊﾞｰｾｷｭﾘﾃｨ基本法により設置）

本部長　内閣官房長官
副本部長　サイバーセキュリティ戦略本部に関する事務を担当する国務大臣
本部員　国家公安委員会委員長
総務大臣
外務大臣
経済産業大臣
防衛大臣
情報通信技術（ＩＴ）政策担当大臣
東京オリンピック競技大会・パラリンピック競技大会担当大臣
有識者（７名；10名以下）

閣僚が参画

※平成27年７月22日付け内閣総理大臣決定により本部員に指定

遠藤　信博	日本電気株式会社代表取締役会長
小野寺　正	ＫＤＤＩ株式会社代表取締役相談役
中谷　和弘	東京大学大学院法学政治学研究科教授
野原佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
林　紘一郎	情報セキュリティ大学院大学教授
前田　雅英	日本大学大学院法務研究科教授
村井　純	慶應義塾大学環境情報学部教授　大学院政策・メディア研究科委員長

重要インフラ専門調査会
研究開発戦略専門調査会
普及啓発・人材育成専門調査会
ｻｲﾊﾞｰｾｷｭﾘﾃｨ対策推進会議（CISO等連絡会議）

緊密連携

国家安全保障会議（NSC）

我が国の安全保障に関する重要事項を審議

（事務局）

内閣官房　内閣サイバーセキュリティセンター（2015.1.9 内閣官房組織令により設置）

内閣サイバーセキュリティセンター長
（内閣官房副長官補(事態対処・危機管理)が兼務）
副センター長（内閣審議官）
上席サイバーセキュリティ分析官
サイバーセキュリティ補佐官

政府機関・情報セキュリティ横断監視・即応調整チーム（ＧＳＯＣ）
情報セキュリティ緊急支援チーム（CYMAT）

協力

＜重要インフラ所管省庁＞
金融庁（金融機関）
総務省（地方公共団体、情報通信）
厚生労働省（医療、水道）
経済産業省（電力、ガス、化学、クレジット、石油）
国土交通省（鉄道、航空、物流、空港）

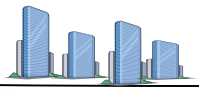
＜その他関係省庁＞
文部科学省（セキュリティ教育）等

協力

閣僚本部員５省庁

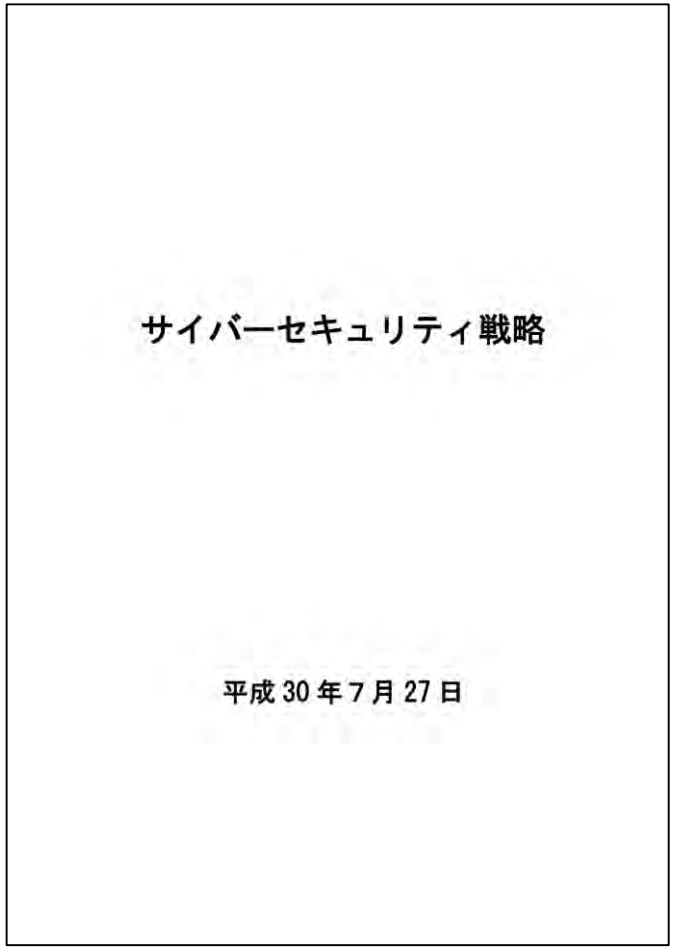
- 警察庁（サイバー犯罪・攻撃の取締り）
- 総務省（通信・ネットワーク政策）
- 外務省（外交・安全保障）
- 経済産業省（情報政策）
- 防衛省（国の防衛）


重要インフラ事業者等


政府機関（各府省庁）

企業


個人



【３つの主要観点】

①サービス提供者の任務保証

- ✓ 自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。

②リスクマネジメント

- ✓ 組織が担う「任務」の内容に応じて、リスクを特定・分析・評価し、リスクを許容し得る程度まで低減する対応をしていくこと。

③参加・連携・協働

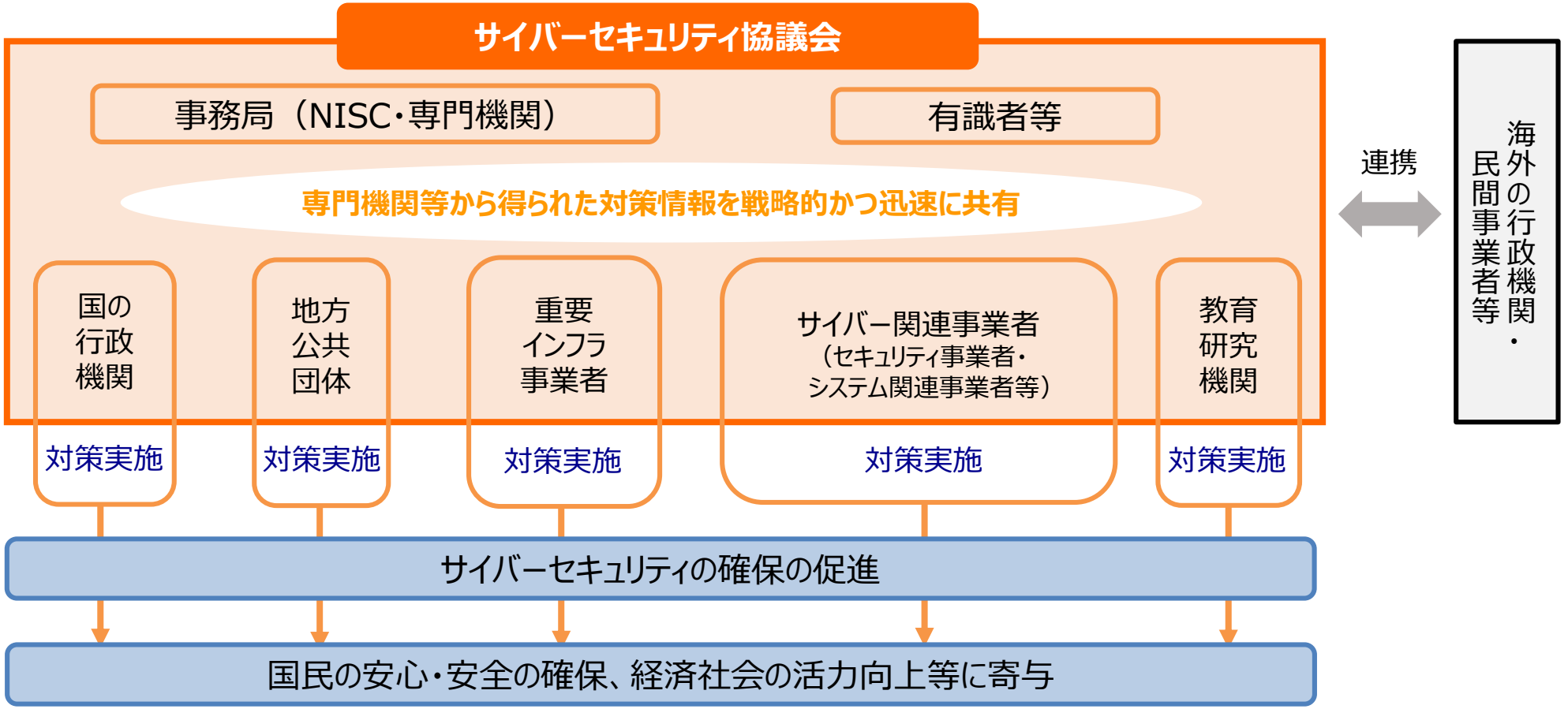
- ✓ サイバー空間の脅威から生じ得る被害やその拡大を防止するため、個人又は組織各々が、平時から講じる基本的な取組。

サイバーセキュリティ協議会（新設）の概要

概要

- **サイバーセキュリティ協議会の創設**

官民の多様な主体が相互に連携して情報共有を図り、必要な対策等について協議を行うための協議会を、サイバーセキュリティ戦略本部長等が創設するとともに、構成員に対して遵守事項（秘密保持、情報提供の協力）等を定める。



（出典）内閣官房内閣サイバーセキュリティセンター作成資料より総務省にて抜粋編集

Ⅰ. はじめに

Ⅱ. IoT化の急速な進展

Ⅲ. サイバーセキュリティ リスクの深刻化

Ⅳ. サイバーセキュリティ戦略

Ⅴ. IoTセキュリティ総合対策

Ⅵ. むすび

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機器のセキュリティ確保

○　現在使用されている機器への対策（IoT機器の脆弱性調査と注意喚起）

・　情報通信研究機構法を改正し、情報通信研究機構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（平成３０年１１月施行。５年間の時限措置）。通信事業者の協力を得て、平成３１年２月より、利用者への注意喚起を実施予定。

○　今後製造される機器への対策（技術基準の改正）

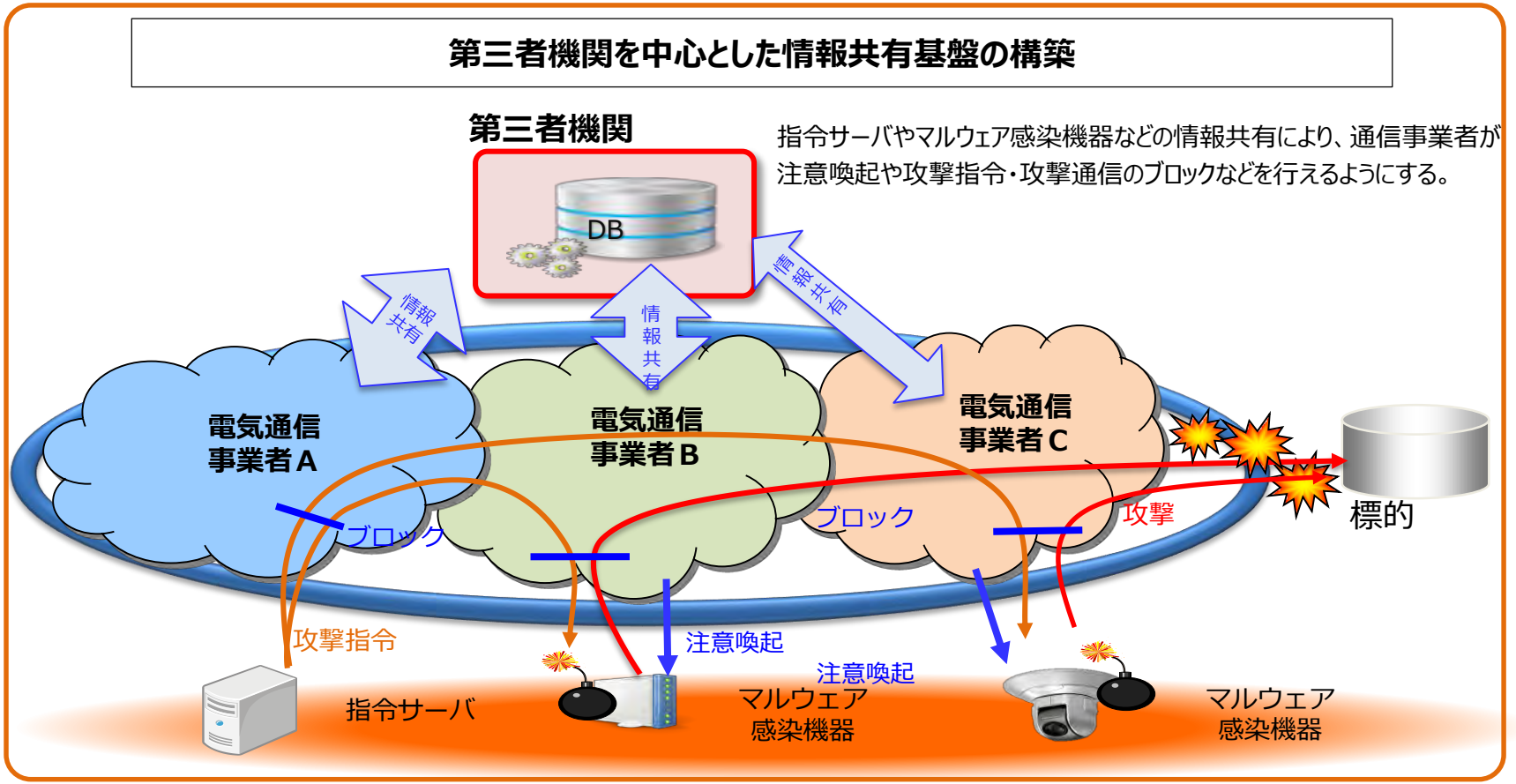
・　ＩｏＴ機器について、初期設定のパスワードの変更を促すなど適切なパスワード設定機能、ファームウェアの更新機能等のセキュリティ要件を追加する技術基準の改正を予定（平成３２年４月施行予定）。

電気通信事業法の一部改正（第三者機関を通じた情報共有）

- サイバー攻撃を行う**マルウェア感染機器**やそれらに**指令を出すサーバへの対処を促進**するため、**第三者機関**を中心として**通信事業者が必要な情報共有をする**ための制度を整備。

施行：平成30年11月1日

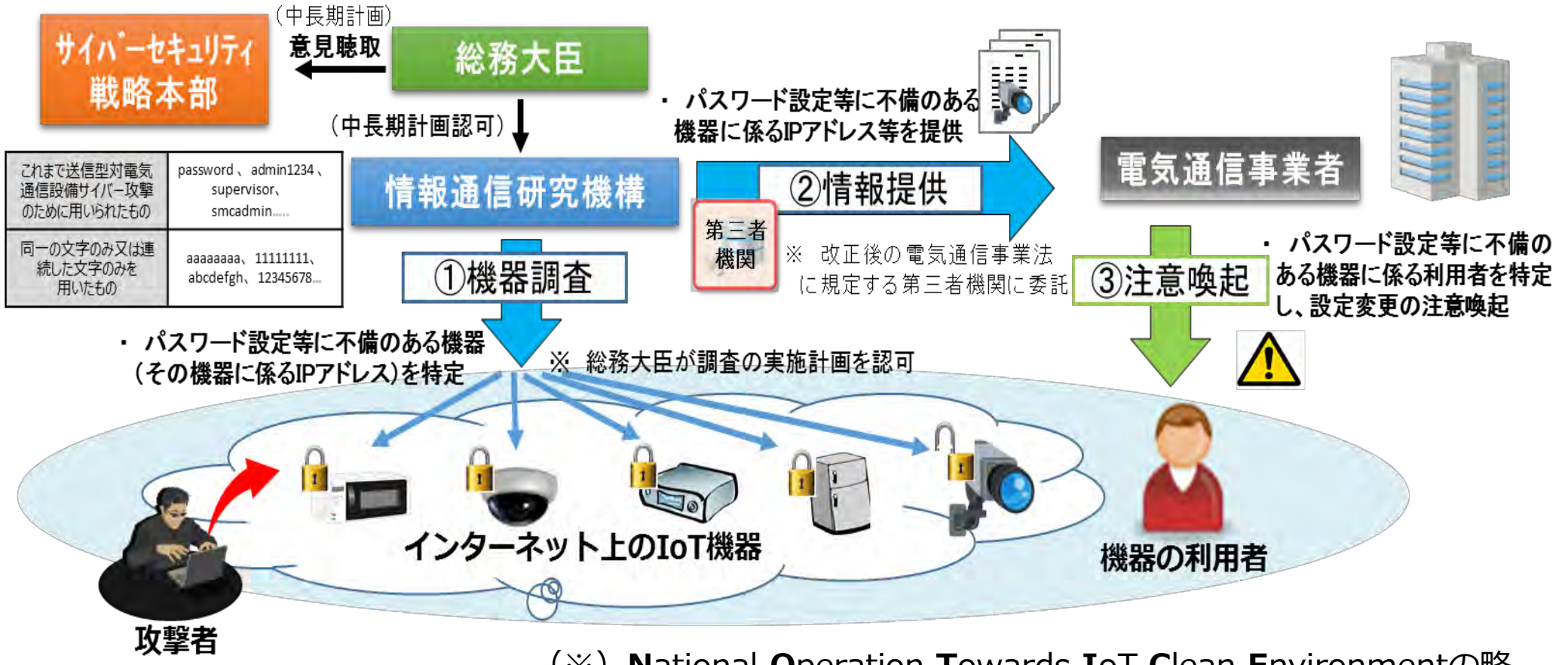
制度整備（イメージ）



IoT機器の脆弱性調査及び利用者への注意喚起プロジェクト「NOTICE」

- 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改正**（平成30年5月成立、11月施行）。
- 同法に基づき、平成31年2月より、NICTがIoT機器を調査し、電気通信事業者を通じて利用者への注意喚起を行うプロジェクト「NOTICE※」を開始予定。

プロジェクト「NOTICE」の全体像



（※） National Operation Towards IoT Clean Environmentの略

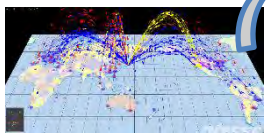
2 機械学習（AI技術）を活用したサイバーセキュリティの研究開発

○　NICTでは、巧妙化・高度化するサイバー攻撃に対して、機械学習を始めとするAI技術を活用したサイバーセキュリティの研究開発に取り組んでいる。

データセットの構築（例）

■ダークネット関連データ

未使用IPアドレスへの攻撃関連通信データ等



DB

■マルウェア関連データ

マルウェア検体等、静的・動的解析結果等

DB

■Android APK関連データ

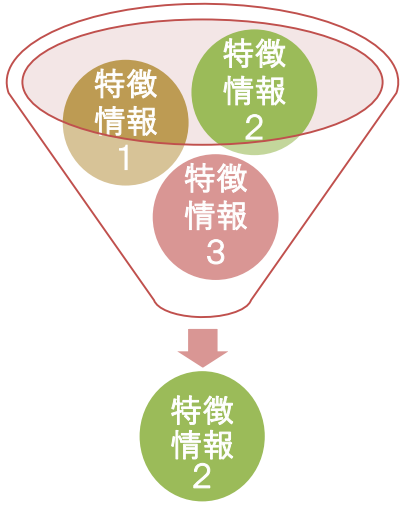
アプリのカテゴリ情報や説明文等

DB

機械学習技術の活用（例）

■特徴選択

多様な特徴情報から最も影響力の高い特徴情報を特定



■SVM（サポートベクタマシン）

特徴情報に基づき、機械学習技術（SVM）を用いて、データを分類。

攻撃パターンの分析やマルウェアの動作・影響分析等を自動化

研究開発成果

（事例１）DDoS攻撃の発生検知

ダークネットトラフィックにおける特徴情報を効果的に特定することで、DDoS攻撃の発生を早期に検知。

（事例２）パッカーの特定

マルウェアがどのようなパッカー（難読化ツール（※））を利用しているかを特定。

（事例３）Androidアプリ分析

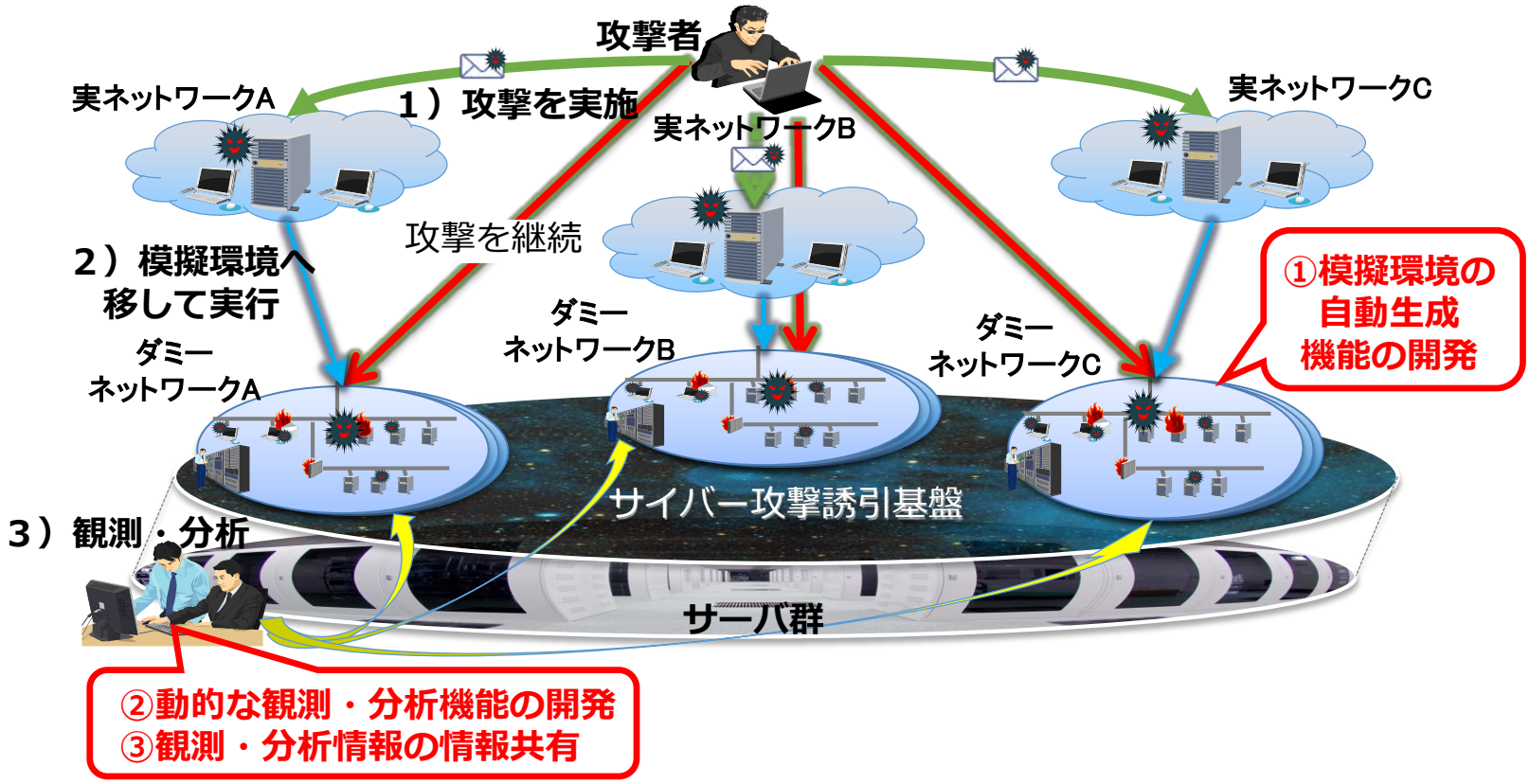
オンラインマーケットに配布されているアプリがマルウェアであるかどうかを判定。

（※）難読化ツールとは、実行形式ファイルをその機能を損なうことなく暗号化するツール。

サイバー攻撃誘引基盤の構築（STARDUST）

○　高度かつ複雑なサイバー攻撃に対処するため、政府や企業等の組織を模擬したネットワークに攻撃者を誘い込み、攻撃者の組織侵入後の詳細な挙動をリアルタイムに把握することが可能な、高度で効率的なサイバー攻撃誘引基盤を構築。

○　攻撃活動の早期収集や未知の標的型攻撃等を迅速に検知する技術等の実証を行うための研究開発環境を、情報通信研究機構（NICT）に整備。分析結果は、セキュリティ対策機関等と連携して情報共有を図り、安全なサイバー空間を実現。



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

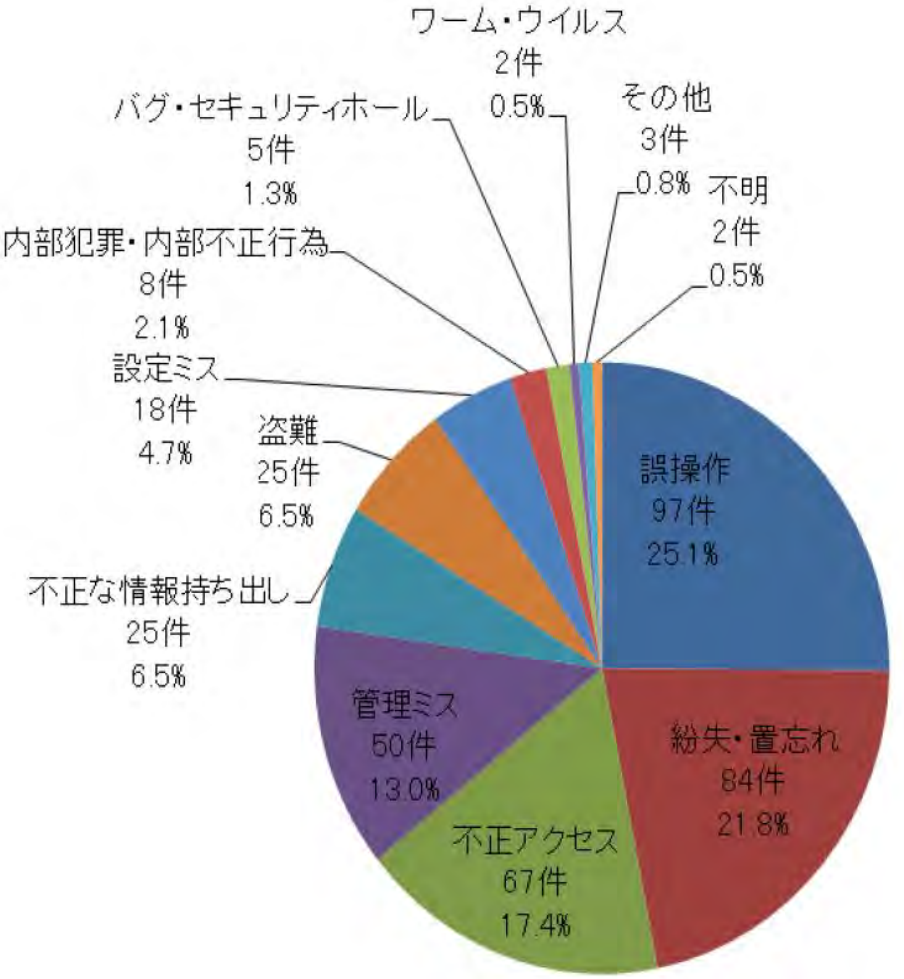
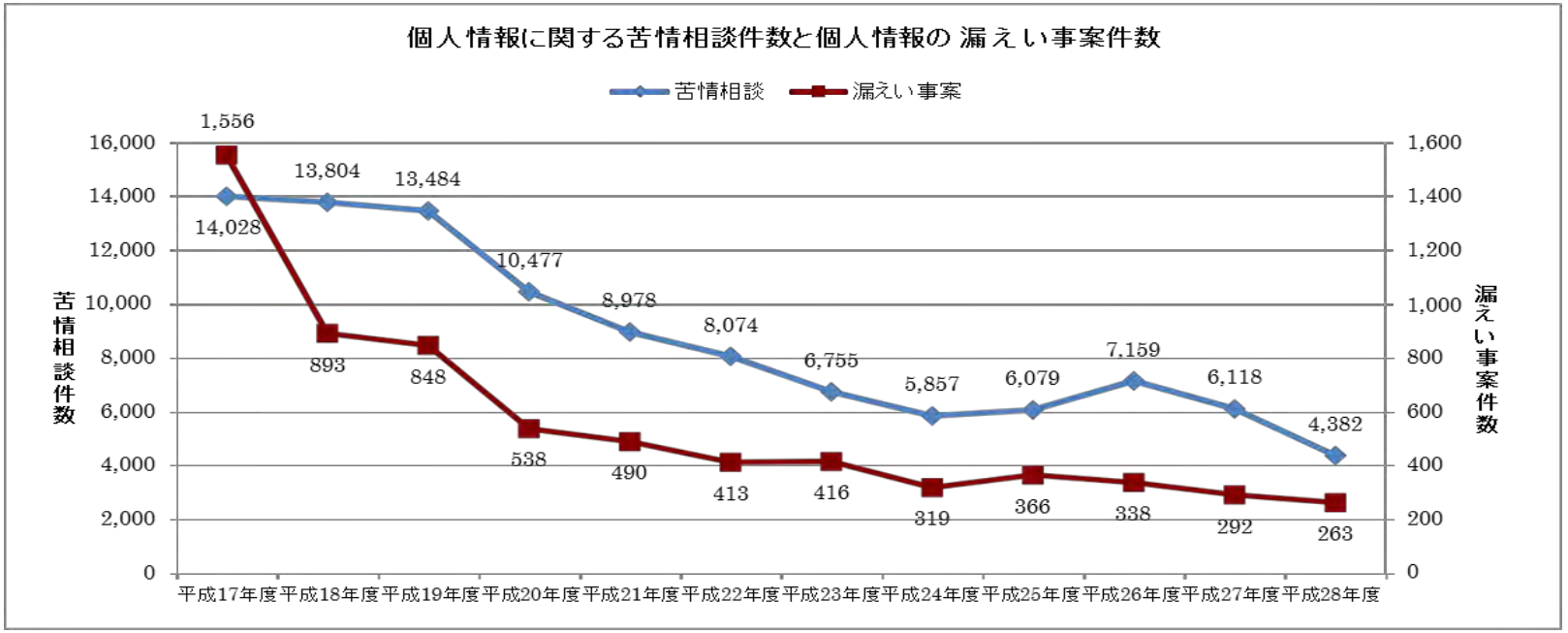


図 3：原因別の漏えい件数

（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）

平成28年度における個人情報漏えい事案（傾向）

■個人情報保護委員会が平成28年度の法施行状況について公表。
■漏えい件数は減少傾向にあるものの、**漏えい人数が多い事案は増加**。



■ 個人情報の漏えい状況（公表されたもの）

漏えいした人数	平成 28 年度		平成 27 年度	
	件数	（割合）	件数	（割合）
500 人以下	145	（55. 1%）	187	（64. 0%）
501～ 5, 000 人	53	（20. 2%）	51	（17. 5%）
5, 001～ 50, 000 人	39	（14. 8%）	39	（13. 4%）
50, 001 人以上	22	（8. 4%）	14	（4. 8%）
不明	4	（1. 5%）	1	（0. 3%）
合計	263	（100. 0%）	292	（100. 0%）

電子媒体のみ	紙媒体のみ	電子媒体と紙媒体	不明
78	64	3	1
36	17	0	0
29	10	0	0
22	0	0	0
3	0	0	0
168	91	3	1

【出典】個人情報保護委員会「平成28 年度個人情報の保護に関する法律施行状況の概要」（平成29年11月）

平成28年度における主な個人情報漏えい事案

■平成28年度中に事業者が公表した個人情報漏えい事案（所管府省において把握したものに限る）のうち、漏えいした個人情報が5万件超の事案を掲載。（**主要22件中19件がサイバー事案**）

	事業者	所管府省	公表日	漏えい人数（最大）	漏えい情報（主なもの）	漏えいの原因（斜自体は報告書には無い追記事項）
1	株式 会社A	A総務省	平成28年6月21日	約62万件	会員ID、会員パスワード、氏名、生年月 日、性別、メールアドレス、住所、職業、 電話番号、ポイント情報、決済手段区 分、PAIDメンバーID	不正アクセス（ぜい弱性）
2	株式会社B	総務省	平成28年6月14日	約33万件	氏名（漢字、カタカナ、ローマ字）、性別、 生年月日、メールアドレス、郵便番号、住 所、電話番号、パスポート番号、パスポート取得日	不正アクセス（JTB関連）
3	株式会社C	総務省	平成28年6月22日	約98万件	注文者氏名、注文者住所、注文者メール アドレス（PC/携帯）、注文者電話番号、 注文者コメント、管理者コメント、配送先 氏名、配送先住所、配送先電話番号、注 文金額、送状番号	不正アクセス（設定ミスによるファイル蔵置）
4	株式 会社D	D総務省	平成28年4月21日	約43万件	・氏名、住所、メールアドレス、電話番号 等	不正アクセス（OSコマンドイン ジェクション）
5	株式会社E	総務省	平成28年4月22日	約64万件	・氏名、住所、メールアドレス、電話番号、性別、年齢、職業	不正アクセス（OSコマンドイン ジェクション）
6	株式会社F	総務省	平成28年7月25日	約12万件	・パスワード、メールアドレス、電話番号 、住所、生年月日、氏名	不正アクセス（SQLインジェクション）
7	株式会社G	国土交通省（観光庁）	平成28年6月14日	約678万件	氏名、性別、生年月日、メールアドレス、 住所、郵便番号、電話番号、パスポート 番号、パスポート取得日	外部からの不正アクセス（添付ファイル）
8	協会H	厚生労働省	平成29年2月17日	約19万人分	氏名、健康保険証の記号番号、医療機 関コード、再審査を求める理由、再審査 結果	紛失（誤廃棄の可能性）（FD，CD等）
9	株式会社I	経済産業省	平成28年12月2日	約42万件	氏名、性別、生年月日、年齢、職業、電 話番号、メールアドレス、住所、購入履 歴、ログインパスワード、一部クレジットカード情報（カード会員名、カード番号、カード有効期限）	不正アクセス（ぜい弱性）
10	公益社団法人J	経済産業省	平成29年4月25日	約15万件	住所、氏名、電話番号、生年月日、ログインID、パスワード、メールアドレス 一部 クレジットカード情報（カード会 員名、カード番号、有効期限、セキュ リティコード）	不正アクセス（Apache Struts2 ぜい弱性）
11	株式会社K	経済産業省	平成29年3月23日	約118万件	氏名、生年月日電話番号、住所、性別、 メールアドレス	不正アクセス（Apache Struts2 ぜい弱性）
12	株式会社L	経済産業省 総務省	平成29年3月10日	約40万件	メールアドレス、クレジットカード番号、ク レジットカード有効期限、セキュリティコー ド、カード払い申込日、住所、氏名、電話 番号、生年月日、メールアドレス、加入月	不正アクセス（Apache Struts2 ぜい弱性）
13	株式 会社M	経済産業省	平成29年3月10日	36万件	クレジットカード番号、有効期限、メール アドレス	不正アクセス（Apache Struts2 ぜい弱性）
14	株式会社N	経済産業省	平成28年4月11日	約20万件	ユーザーID、パスワード、氏名、住所、電 話番号、メールアドレス、生年月日の内 顧客が登録した情報、加えて、537件はクレジットカード番号、有効期限、セキュリティコード	不正アクセス
15	株式 会社O	経済産業省	平成28年4月28日	約64万件	氏名、性別、住所、メールアドレス、家族 に関する情報 ※漏えい項目は公表せず。	不正アクセス（ケータイキットぜい弱性）
16	株式会社P	経済産業省	平成28年4月27日	約13万件	氏名、住所、電話番号、メールアドレ ス、ログイン会員ID及びパスワード、クレジットカード情報（カード番号、有 効期限、カード名義、セキュリティコー ド）うち、カード情報は7386件	不正アクセス（OpenSSLぜい弱性）
17	株式会社Q	経済産業省	平成28年8月23日	約21万件	氏名、住所、電話番号、法人担当者 名 ※漏えい項目は公表せず。	外付けハードディスクの紛失
18	株式会社R	経済産業省 総務省	平成28年8月26日	約11万件	クレジットカード情報（カード番号、カード 名義、有効期限、セキュリティコード）、会 員情報（メールアドレス、パスワード、氏 名、住所、電話番号、その他の登録情 報）	不正アクセス（ぜい弱性）
19	株式会社S	経済産業省 総務省	平成28年5月11日	約5万件	ニックネーム、メールアドレス、生年月 日、居住地域、性別 仮想通貨「コイン」の履歴情報	不正ログイン（リスト型攻撃）
20	株式会社T	経済産業省 総務省	平成28年11月29日	約58万件	ニックネーム、メールアドレス、生年月 日、居住地域、性別 仮想通貨「コイン」の履歴情報	不正アクセス（リスト型攻撃）
21	株式会社U	経済産業省	平成29年1月1日	約5万9千件	メールアドレス、氏名、生年月日、性 別、住所、郵便番号、電話番号	不正アクセス（SQLインジェクション）
22	株式会社W	経済産業省	平成29年2月27日	約120万件	氏名、住所、電話番号、生年月日、メールアドレス、性別 クレジットカード番号、カード有効期限	バックアップストレージの盗難

【出典】個人情報保護委員会「平成28 年度個人情報の保護に関する法律施行状況の概要」（平成29年11月）

経営層の意識改革の必要性

図1：直近の重要なサイバー対策として
「サプライチェーンへのセキュリティ基準の定着」を挙げた企業割合

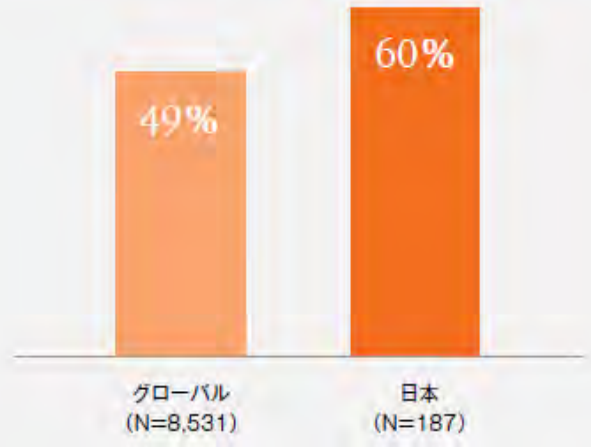
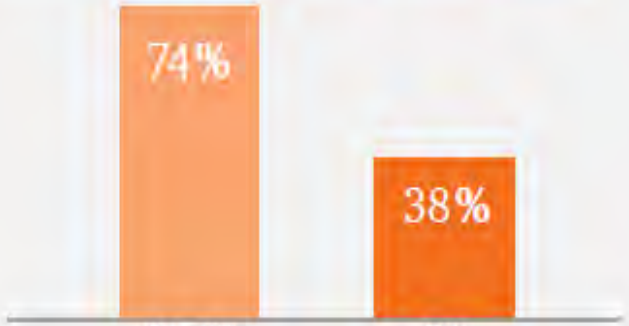


図2：IT-BCPが想定するリスクの割合

出典：PwC、「IT-BCPサーベイ報告書」(2014)

図4：サイバーセキュリティ対策に自信があると回答する企業の割合



（出典）PWC　Japanグループ「グローバル情報セキュリティ調査2018 Vol. 1」(2018年6月）

サイバー攻撃による経済的被害（米国、推計）

サイバー攻撃が米国に及ぼす年間の経済的損失を推計-----2016年時点
→ 570億ドル（6．1兆円）～1090億ドル（11．7兆円）
（対GDP比で0．31～0．58%）。

■サイバー攻撃の損害は攻撃を受けた企業と経済的に関連する企業にスピルオーバーし、経済に与える打撃を拡大。
- ・サイバー攻撃を受けた企業の株価の低下→他企業での（当該企業の）保有株式の資産価値の低下
- ・サイバー攻撃対策関連の支出の増大
- ・新しいICTの採用が鈍化→生産性が低下

■企業は共通する脆弱性を抱えているため、特定の脅威が企業の枠を越えて波及。共通する脆弱性の理解が不足していることがサイバー保険市場の発展を阻害。

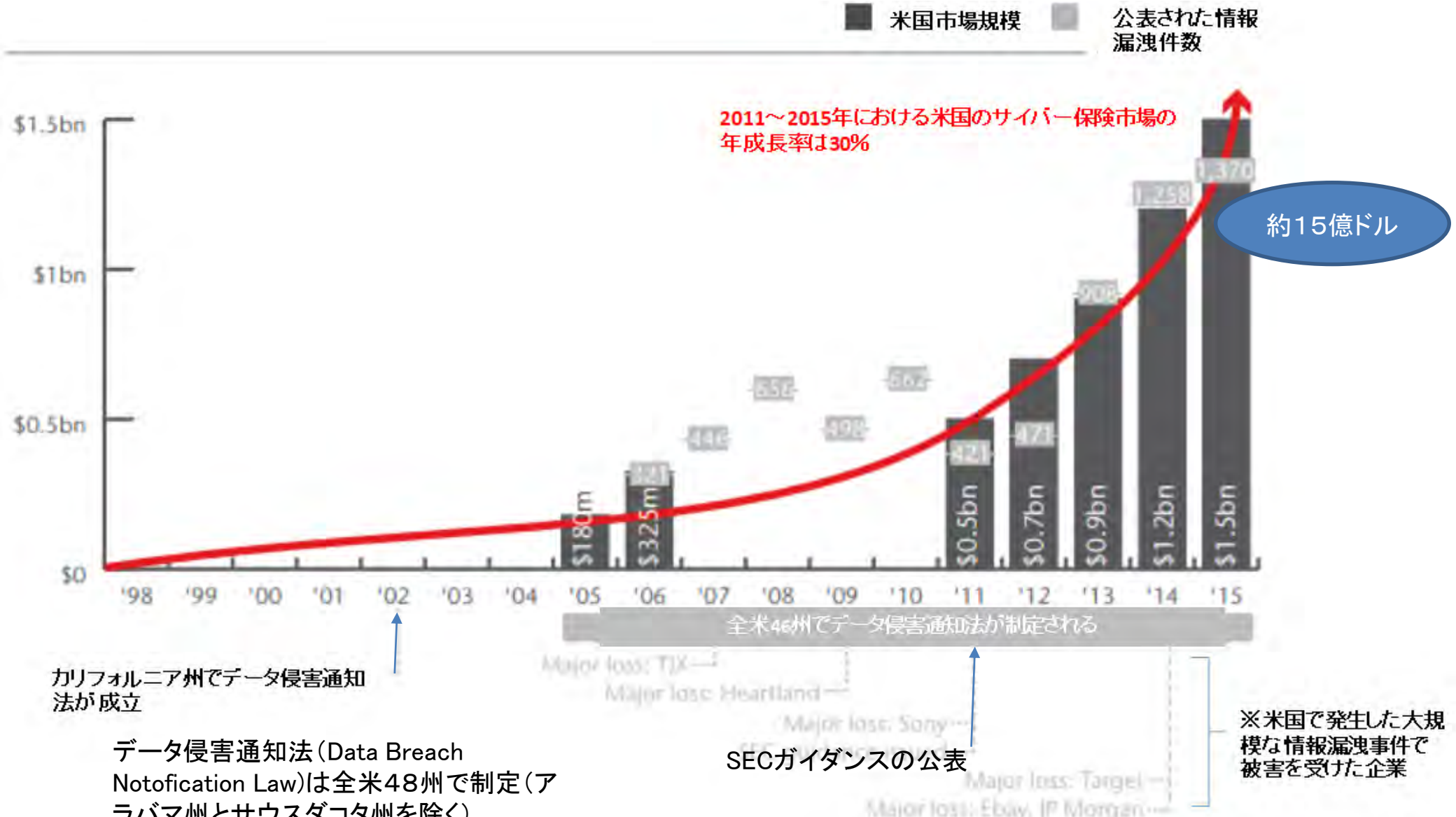
■データの欠如や不十分な情報共有がサイバー保険市場の発展を阻害。

■サイバーセキュリティは共通財。サイバーセキュリティの欠如は他企業や国民に負の外部性をもたらす。負の外部性に関する説明不足が社会的な最適水準のセキュリティ投資を実現することを阻み、過少投資にとどまる。

■政府の果たすべき役割
- ・情報開示の推進や重大なデータ侵害企業の制裁による企業リスクの外部性の内生化
- ・サイバーセキュリティ基礎研究の推進（民間企業におけるイノベーションの促進）
- ・セキュリティ基準の普及促進
- ・情報共有の促進（ISACやISAO）　　等

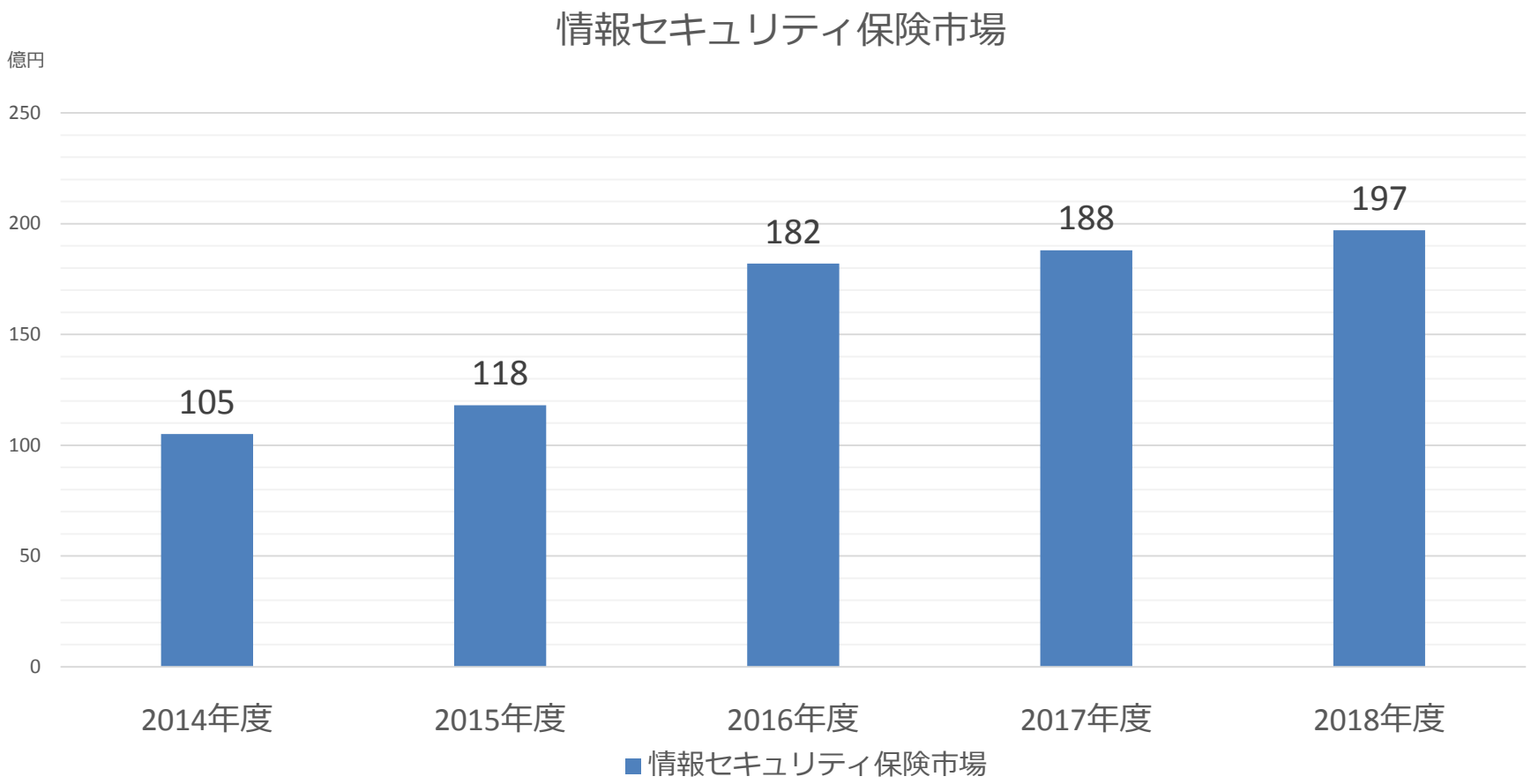
（出典）The council of Economic Advisers “The Cost of Malicious Cyber Activity to the U.S. Economy”(Feb. 2018)

米国におけるサイバーセキュリティ保険市場



（出典）中沢潔「米国におけるサイバー保険の現状」（JETRO/IPA NY、ニューヨーク便り、2017年11月）

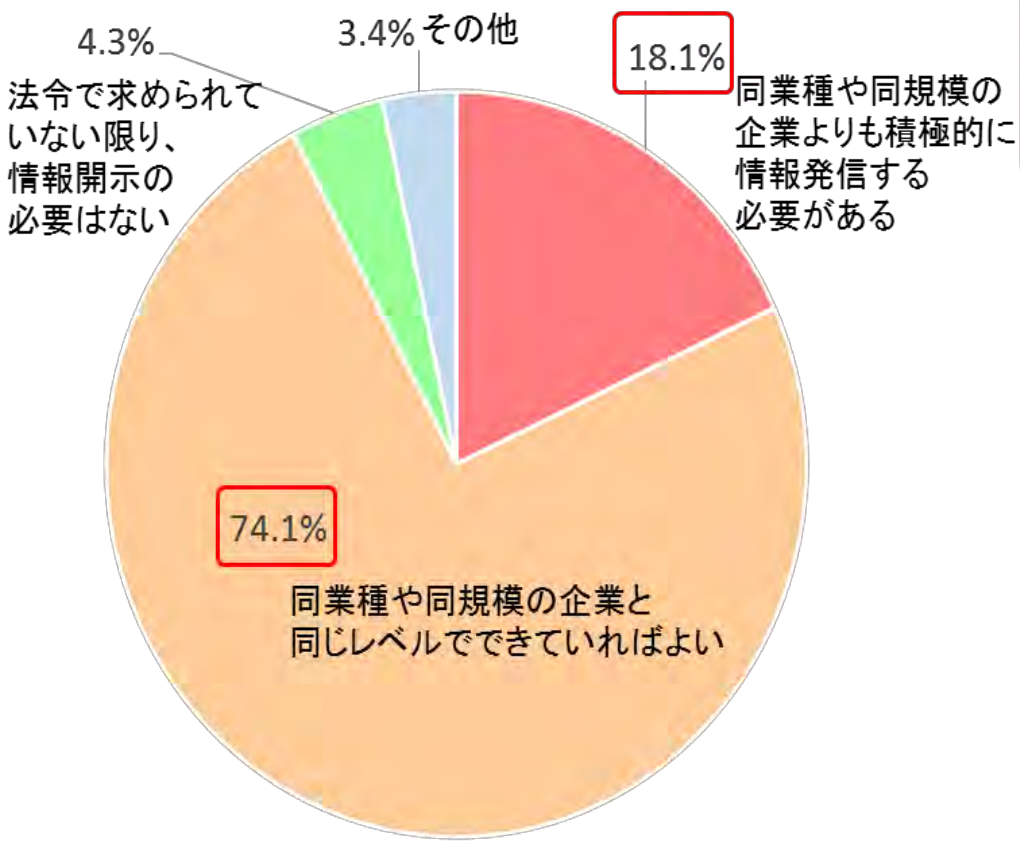
企業の経営課題としてのサイバーセキュリティ



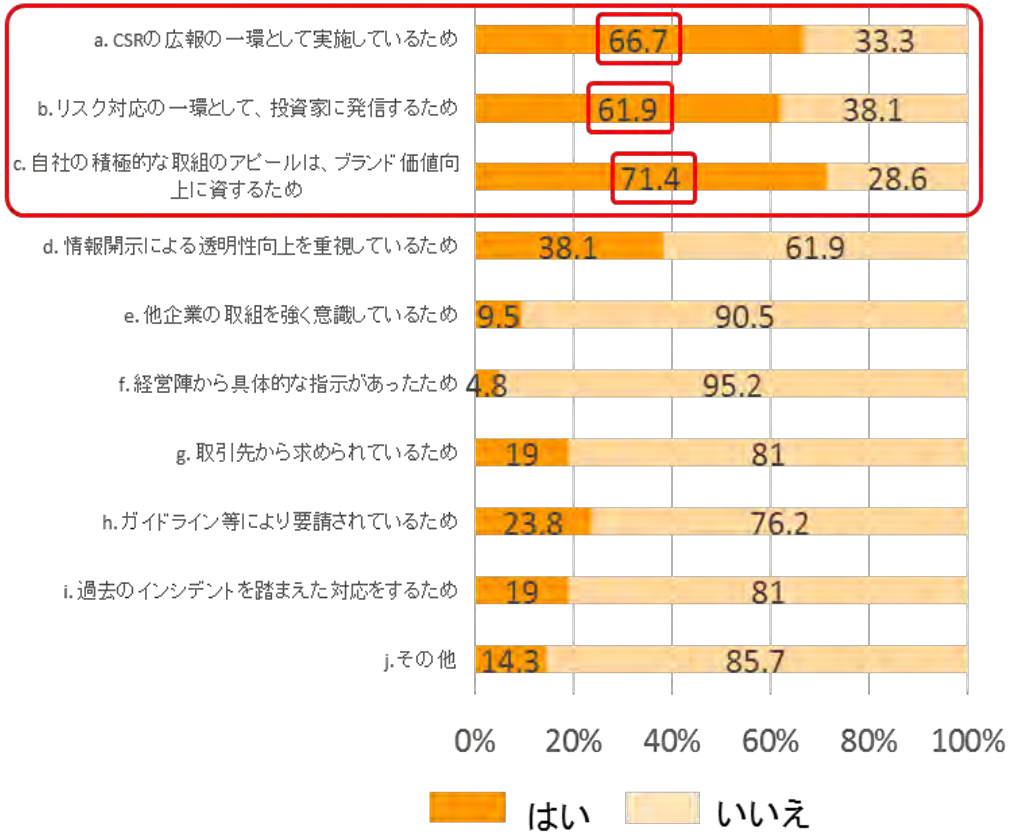
（出典）JNSA“2017年度 国内情報セキュリティ市場調査（速報値）”（2018年5月）

サイバーセキュリティ対策に関する情報開示（企業意識）

サイバーセキュリティに関する情報発信の姿勢



積極的に情報発信を行う理由



（注）対象企業については、平成26年11月１日現在の日経平均株価指数銘柄の225社に、調査期間中に入れ替えがあった１社を加え、226社としている。

（出典）NISC「平成28年度　企業のサイバーセキュリティ対策に関する調査報告書」（2017年）

各種報告書におけるセキュリティ対策の記載状況

報告書	記載状況
有価証券報告書	主に「事業等のリスク」の項目で記載。記載内容は、システムの停止や機密データの漏洩等に関する概略であり、詳細な対策の内容については記載されない傾向。
コーポレート・ガバナンス報告書	「内部統制システム等に関する事項」の項目において、セキュリティに関するグローバルな推進体制や情報セキュリティ及び個人情報保護に関する体制を整備する等、情報セキュリティへの対策に関する管理体制の整備について記載される傾向。
CSR報告書/サステナビリティ報告書	多くの企業が情報セキュリティに係る内容を報告書に記載している傾向にあり、情報セキュリティに係るリスクだけでなく、特に「セキュリティに関する基本方針等の策定状況」、「セキュリティに関する管理体制」、「社員に対する教育・人材育成」、「社外との情報共有体制」、「第三者評価・認証の取得状況」の5項目について記載される傾向がある。
情報セキュリティ報告書	経済産業省「情報セキュリティ報告書モデル」を参考に、技術面の取組、体制の構築、マネジメントシステムについて詳細に記載されている傾向。

総務省において、セキュリティ対策の情報開示の在り方について検討中。

③ IoT普及促進税制（コネクテッド・インダストリーズ税制）の創設

○ 一定のサイバーセキュリティ対策が講じられたデータ連携・利活用により、生産性を向上させる取組について、それに必要となるシステムや、センサー・ロボット等の導入に対して、特別償却30%又は税額控除3%（賃上げを伴う場合は5%）を措置。

○ 事業者は当該取組内容に関する事業計画を作成し、主務大臣が認定。認定計画に含まれる設備に対して、税制措置を適用（適用期限は、平成32年度末まで）。

※ 経済産業省との共管

【計画認定の要件】

①データ連携・利活用の内容

・社外データやこれまで取得したことのないデータを社内データと連携

・企業の競争力における重要データをグループ企業間や事業所間で連携

②セキュリティ面

必要なセキュリティ対策が講じられていることをセキュリティの専門家(登録セキスペ等)が担保

③生産性向上目標

投資年度から一定期間において、以下のいずれも達成見込みがあること

・労働生産性：年平均伸率２%以上

・投資利益率：年平均15%以上

課税の特例の内容

➢ 認定された事業計画に基づいて行う設備投資について、以下の措置を講じる。

対象設備	特別償却	税額控除
ソフトウェア 器具備品 機械装置	30%	3% （法人税額の15%を限度）
		５％ ※ （法人税額の20%を限度）

【対象設備の例】

データ収集機器（センサー等）、データ分析により自動化するロボット・工作機械、データ連携・分析に必要なシステム（サーバ、ＡＩ、ソフトウェア等）、サイバーセキュリティ対策製品　　等

最低投資合計額：5,000万円

※ 計画の認定に加え、平均給与等支給額の対前年度増加率≧３％を満たした場合。

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）

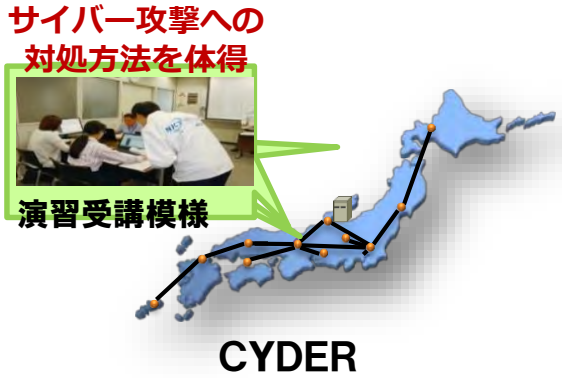
○　巧妙化・複合化するサイバー攻撃に対し、実践的な対処能力を持つセキュリティ人材を育成するため、平成２９年４月より、情報通信研究機構（NICT）の「ナショナルサイバートレーニングセンター」において、以下の実践的サイバー演習等を積極的に推進。

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

実践的サイバー防御演習（CYDER）（平成25年度～）

CYDER：CYber Defense Exercise with Recurrence

○　総務省は、情報通信研究機構（NICT）を通じて、**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の情報システム担当者等を対象**とした体験型の**実践的なサイバー防御演習（CYDER）**を実施。

○　**受講者は**、組織の情報システム担当職員として、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って**サイバー攻撃によるインシデントの検知から対応、報告、 回復までの**一連の対処方法を体験**。

○　平成29年度については、**全国で100回開催**され、**計3,009名が受講**。

演習のイメージ

CYDER演習風景

- NICT北陸StarBED技術センターに設置された大規模高性能サーバー群を活用し、行政機関等の実際のネットワークを模した大規模仮想LAN環境を構築。
- NICTの有する技術的知見を活用し、サイバー攻撃に係る我が国固有の傾向等を徹底分析し、現実のサイバー攻撃事例を再現した最新の演習シナリオを用意。

平成30年度の実施計画

コース	受講対象組織	開催地	開催回数
Aコース（初級）	（全組織共通）	47都道府県	60回
B-1コース（中級）	地方公共団体向け	全国11地域	20回
B-2コース（中級）	国の行政機関等向け	東京	10回
B-3コース（中級）	重要インフラ事業者向け	東京	10回

2020東京大会に向けたサイバー演習（サイバーコロッセオ）

○　近年さらに高度化・多様化するサイバー攻撃に備え、東京2020オリンピック・パラリンピック競技大会の適切な運営を確保することを目的として、**大会関連組織のセキュリティ担当者等を対象とした、**高度な攻撃に対処可能な人材の育成を行う**実践的サイバー演習「サイバーコロッセオ」を平成30年2月から本格的に実施**。

○　サイバーコロッセオは、**国立研究開発法人情報通信研究機構（NICT）が実施主体となり**、NICTが有する大規模演習環境及び長年のサイバーセキュリティ研究による知見を活かした、**実際の機器やソフトウエアの操作を伴う「実践的なトレーニング」を実施**。

イメージ図

■　大規模演習環境を用いて、東京大会の公式サイト、大会運営システム等ネットワーク環境を忠実に再現した、仮想のネットワーク環境を構築。

■　仮想のネットワーク環境上で、東京大会時に想定されるサイバー攻撃を擬似的に発生させ、攻撃・防御手法の検証及び訓練を実施。

東京2020オリンピック・パラリンピック競技大会のサイバーセキュリティを確保

若手セキュリティイノベータの育成（SecHack365）

○ 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の持つサイバーセキュリティの研究資産を活用し、若年層のICT人材を対象に実際のサイバー攻撃関連データに基づいたセキュリティ技術の研究・開発を、第一線で活躍する研究者・技術者が1年かけて継続的かつ本格的に指導。

○ 対象者は、日本国内に居住する25歳以下の若手ICT人材（平成29年度は39名が一年間のプログラムを修了。）

○ 受講者は、NICTの有する遠隔開発環境（NONSTOP（※））を活用し、年中どこからでも遠隔開発実習を行うことが可能。また、集合イベントとして、座学講座（研究倫理）やハッカソン等を実施。

（※） NONSTOP（NICTER Open Network Security Test-out Platform）では、NICTの長年にわたるサイバーセキュリティ研究によって得られた膨大なセキュリティ関連データを活用することができ、NONSTOP内に整備された様々な研究開発・解析用ツール類と、他では触れることのできない貴重なデータを用いて研究・開発に取り組むことが可能。

■ 遠隔開発実習、座学講座、ハッカソン等の組合せによる総合的な人材育成プログラム。

サイバーセキュリティに関する国際連携の推進

サイバー空間には国境がないため、サイバー攻撃への対処については、各国間での情報共有や人材育成等の連携が重要。

日ASEANサイバーセキュリティ能力構築センター(AJCCBC)

AJCCBC
ASEAN JAPAN CYBERSECURITY CAPACITY BUILDING CENTRE
Partnership by ASEAN and Japan

● 日ASEAN統合基金を活用したASEAN域内のセキュリティ人材育成プロジェクト(4年間で650人程度)。2018年9月にタイで開所。

■ プロジェクト概要

1. サイバーセキュリティ演習

政府機関・重要インフラ事業者等に対し、以下の演習プログラムを実施(年6回)

2. ASEAN Youth Cybersecurity Technical Challenge (Cyber SEA Game)

ASEAN各国から選抜された若手技術者・学生がサイバー攻撃対処能力を競う大会の開催(年1回)

イスラエルとのサイバーセキュリティ分野における協力覚書締結

● 2018年11月29日、総務省はイスラエル国家サイバー総局との間にサイバーセキュリティ分野における協力覚書を締結。

■ 協力分野

(1) サイバーセキュリティ政策に関する情報交換
(2) 研究開発
(3) 人材育成

ベンアリ駐日イスラエル大使と石田総務大臣による覚書締結式 (2018.11)

今後に向けて

- ✓サイバーセキュリティ対策は「費用」ではなく「投資」
- ✓経営者の皆様の問題意識が重要
- ✓その問題意識を実行に移すための「戦略マネジメント層」も重要
- ✓「自助」、「共助」、「公助」のバランス
- ✓守るべきものは何か、からの逆算

ご清聴ありがとうございました