重要インフラを中心とした サイバーセキュリティ政策

令　和　元　年　５　月　２　９　日

総務省サイバーセキュリティ統括官
竹　　内　　芳　　明

Ⅰ．サイバーセキュリティ リスクの深刻化

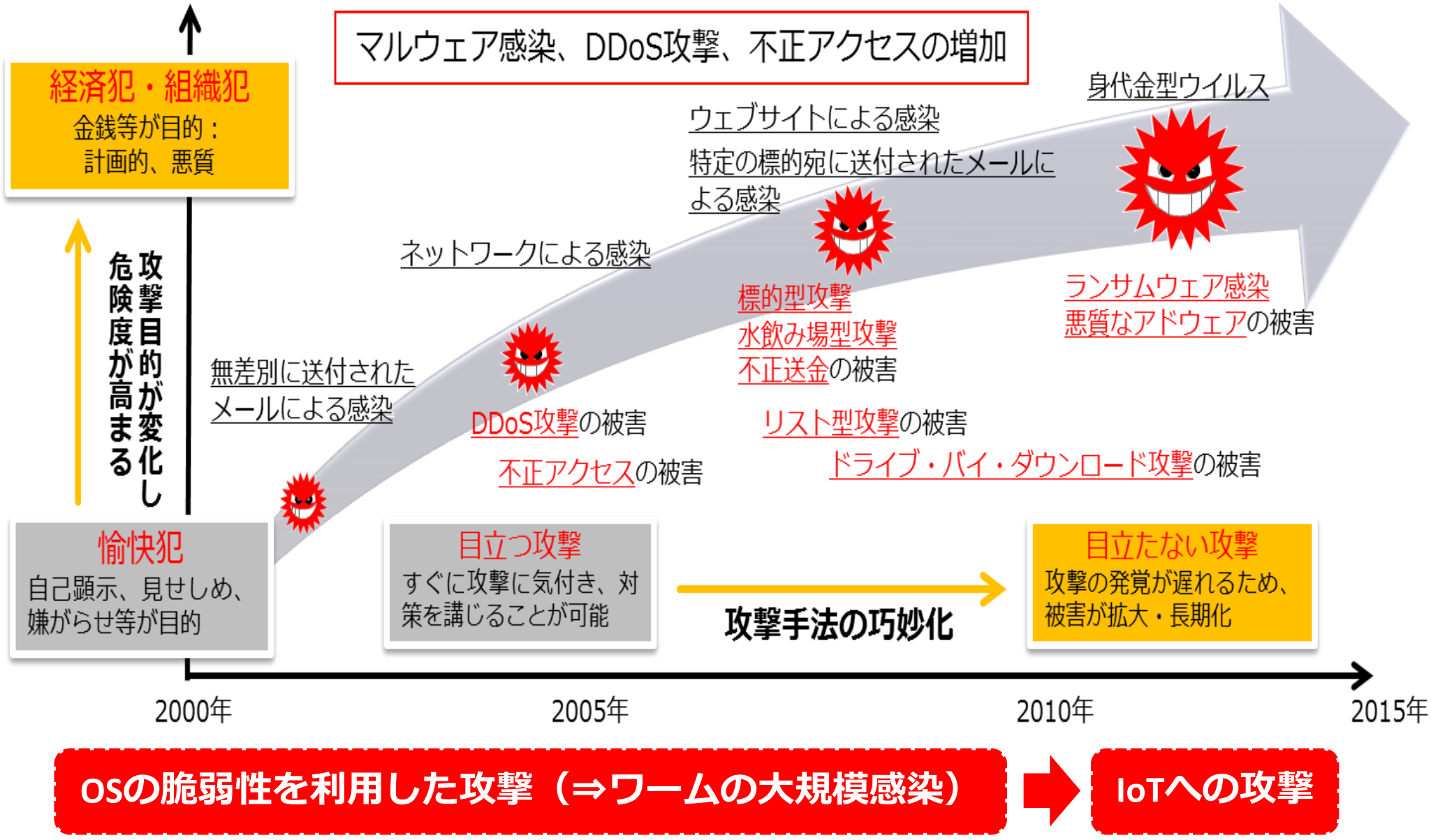
Ⅱ．5G／IoT化の急速な進展

Ⅲ．サイバーセキュリティ戦略

Ⅳ．IoTセキュリティ総合対策

Ⅴ．国家安全保障戦略

サイバーセキュリティ上の脅威の増大①



OSの脆弱性を利用した攻撃（⇒ワームの大規模感染） ➡ **IoTへの攻撃**

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**）

2018年1月： **コインチェック社**が保有していた仮想通貨が**不正アクセス**により外部へ送信され、顧客資産が流出。

海外事例

2015年4月: **フランスのテレビネットワークTV５Monde** 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**）

2017年10月: **米Yahoo社**で**不正アクセス**により約30億件の個人情報が流出していたことが判明。

制御システム等を標的にしたサイバー攻撃の事例

➢イランの核燃料施設へのサイバー攻撃 (2010)

USBを介してマルウェアが感染。未知のWindowsの脆弱性を利用し、核燃料施設のウラン濃縮用遠心分離器に誤作動を起こさせ、数千台に及ぶ遠心分離機が稼働不能に。

➢米国のダムへのサイバー攻撃 (2013)

米国ニューヨーク州のダム管理システムがサイバー攻撃を受け、システムに侵入された。実害はなかったが、水門を制御することが可能な状態となっていた。

➢ドイツの鉄鋼工場へのサイバー攻撃(2015)

ドイツの鉄鋼工場内において、フィッシングメールやソーシャルエンジニアリング等を組み合わせた手法により工場内ネットワークへのアクセス権が奪われ、システム全体に不具合が発生し、最終的に生産設備が損傷。

➢ウクライナの電力会社へのサイバー攻撃(2015)

電力会社へのマルウェアBlackEnergyを用いたサイバー攻撃により、ウクライナ西部で停電が発生。

➢ウクライナの電力会社へのサイバー攻撃(2016)

国営電力会社Ukrenergoの変電所がマルウェアを用いたサイバー攻撃を受け、キエフ北部及び周辺地域で停電が発生。

➢ワナクライ（世界同時多発の大規模サイバー攻撃）(2017)

Windowsの脆弱性を利用し、感染したパソコンのファイルを暗号化し、復旧のために金銭の支払いを要求するランサムウェア。世界的に感染が発生し、様々な被害が発生。

＜事例１＞　サイバー攻撃によるウクライナ停電

サイバー攻撃によりエネルギー供給が停止した初の事例
　2015年12月23日　変電所の遮断機切断で最大6時間の停電発生（ウクライナ）
　2016年12月17日　変電所の遮断機切断で1時間15分の停電発生（ウクライナ）

2015年
【概　要】
　①標的型メール攻撃（IT系への攻撃）
　　マルウエアを含む添付ファイルをメールで送付
　→マルウエアに感染させ、長期間の偵察活動で情報を収集
　②DOS攻撃で電話システムに支障発生（IT系への攻撃）
　→復旧活動を妨害
　③遠隔操作で変電所の遮断機を切断（OT系への攻撃）
　→最大6時間の停電発生（22万5千世帯）
　　※UPS（Uninterruptible Power Supply;非常時電源）が動作しないように設定

【被害】 攻撃者は、制御システムを遠隔から手動操作して停電を発生させた

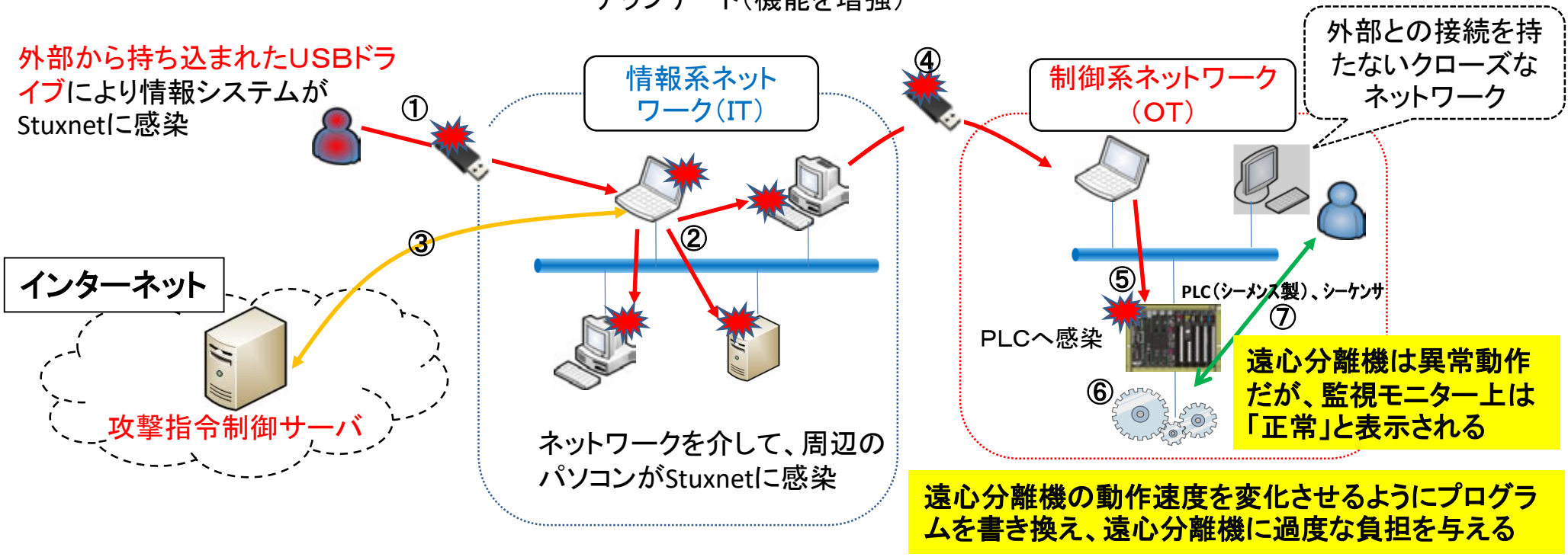
2016年
　2015年とほぼ同じ手法だが、PCに感染したマルウェアが発送電設備を直接操作し、1時間15分の停電発生

＜事例２＞　イラン原子力関係施設へのサイバー攻撃

2010年7月イランのブシェール原子力発電所及び同年11月イランのウラン濃縮施設がStuxnet（スタックスネット）と呼ばれるコンピュータウイルスによってサイバー攻撃を受けた。
→ 遠心分離機の相当数が稼働不能となり、プロジェクトの大幅遅延となった。

Stuxnetの解析から推定された攻撃手法

感染したパソコンは、攻撃指令制御サーバと通信を行いStuxnetをアップデート（機能を増強）



クローズドなシステムだからといって、100%安心とは言い切れない

＜事例３＞　大規模サイバー攻撃　WannaCry

2017年5月12日頃より、ランサムウェア（WannaCry）による被害が世界中で多数発生

【感染時の画面イメージ】

【ドイツ鉄道】
行先表示装置がWannaCryに感染
→行先案内表示装置を故障扱い

【被害を受けた国】

【概　要】 150か国30万台以上（国内：600カ所以上2000端末以上）のコンピューターに感染、
データを暗号化し、使用不能にする。身代金としてビットコインを要求
【攻撃形態】 不審メール開封による感染や、インターネットに接続している端末が感染するなど、
Windowsの脆弱性を利用した攻撃
【被害状況】 ルノー（フランス）,Telefonica（スペイン）,FedEx(アメリカ),ドイツ鉄道(ドイツ)など

【対策】
マイクロソフトが3月15日に出したセキュリティ更新プログラム（MS17-010)を適用
セキュリティパッチを適時使用　／　重要データはバックアップ

サイバーセキュリティ基本法の一部を改正する法律の概要

概要

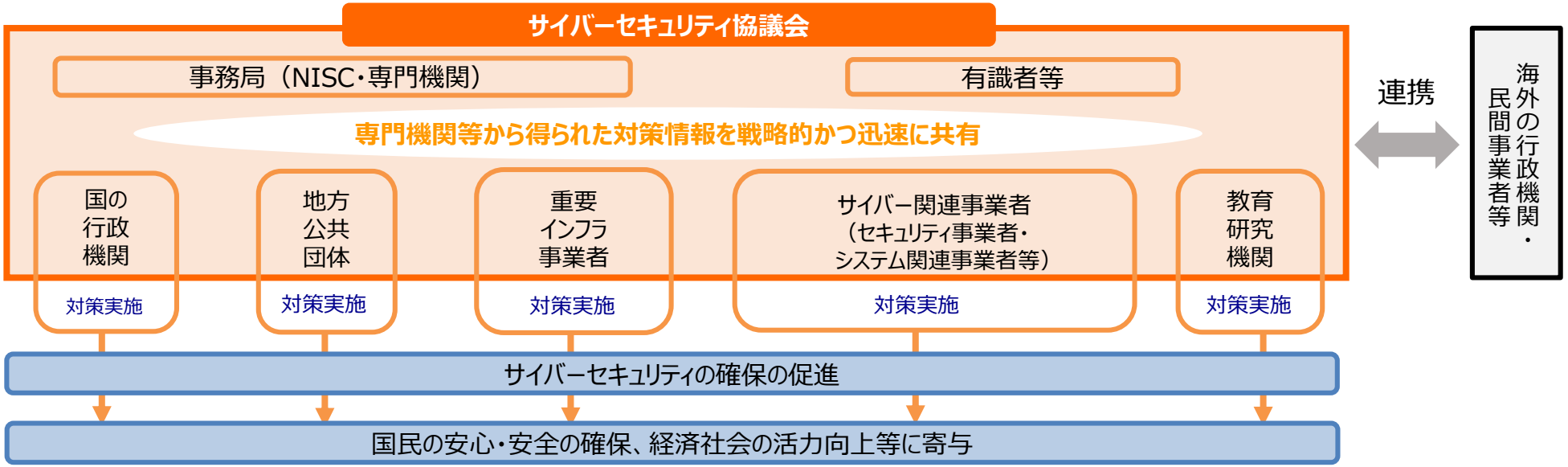
- **サイバーセキュリティ協議会の創設**

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。

- **サイバーセキュリティ戦略本部による連絡調整の推進**

本部の所掌事務に、事象が発生した場合における国内外の関係者との連絡調整に関する事務を追加し、当該事務の一部を政令で定める法人に委託することができることとするとともに、当該法人に対して秘密保持義務等を定める。

【施行期日】 公布の日から起算して一年を超えない範囲内において政令で定める日



Ⅰ．サイバーセキュリティ リスクの深刻化

Ⅱ．5G／IoT化の急速な進展

Ⅲ．サイバーセキュリティ戦略

Ⅳ．IoTセキュリティ総合対策

Ⅴ．国家安全保障戦略

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

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

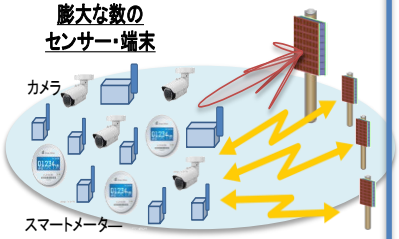
利用者が遅延（タイムラグ）を意識することなく、リアルタイムに遠隔地のロボット等を操作・制御

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

新たな社会インフラへ

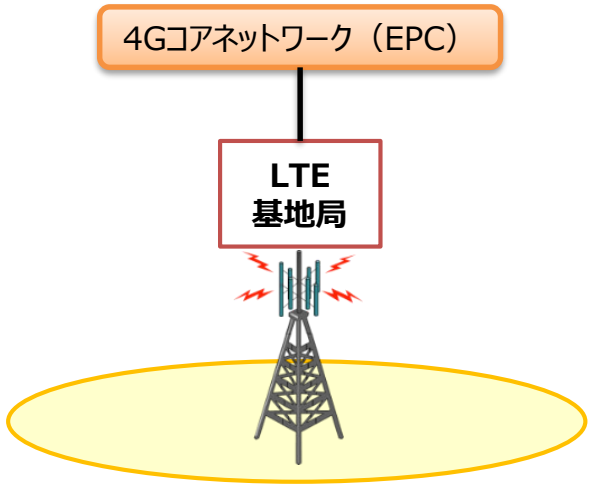
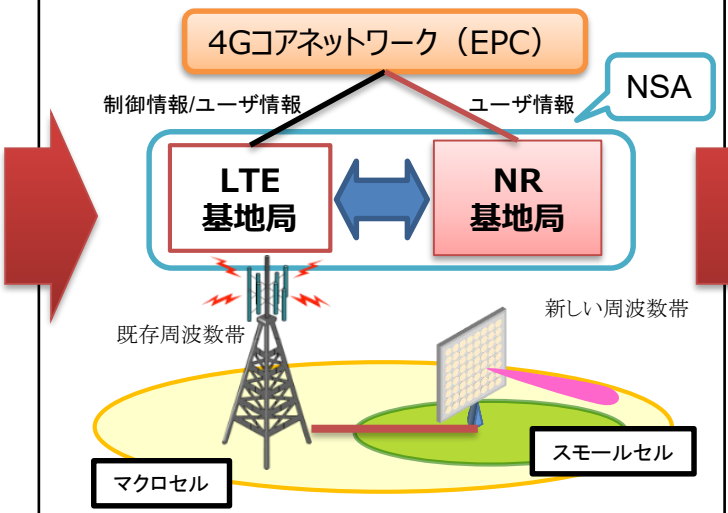
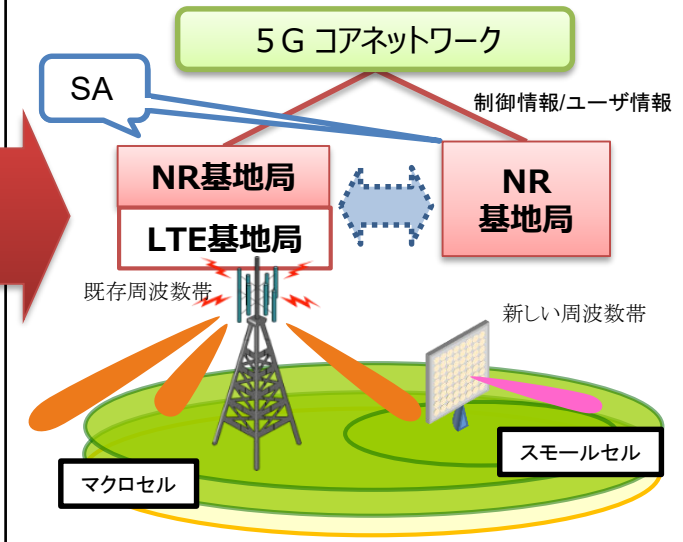
4Gから5Gへの移行

【2020年】 需要の高いエリアに、**5G用の新しい周波数帯を用いた「超高速」サービスが提供**。

新たな無線技術（NR）に対応した基地局は、LTE基地局と連携する**NSA（Non-Standalone）構成**で運用。

【202X年】 ネットワークスライシング等に対応した**5Gコアネットワークが導入**されるとともに、**SA（Standalone）構成**のNR基地局の運用が開始され、**既存周波数帯域へのNR導入が進展**。

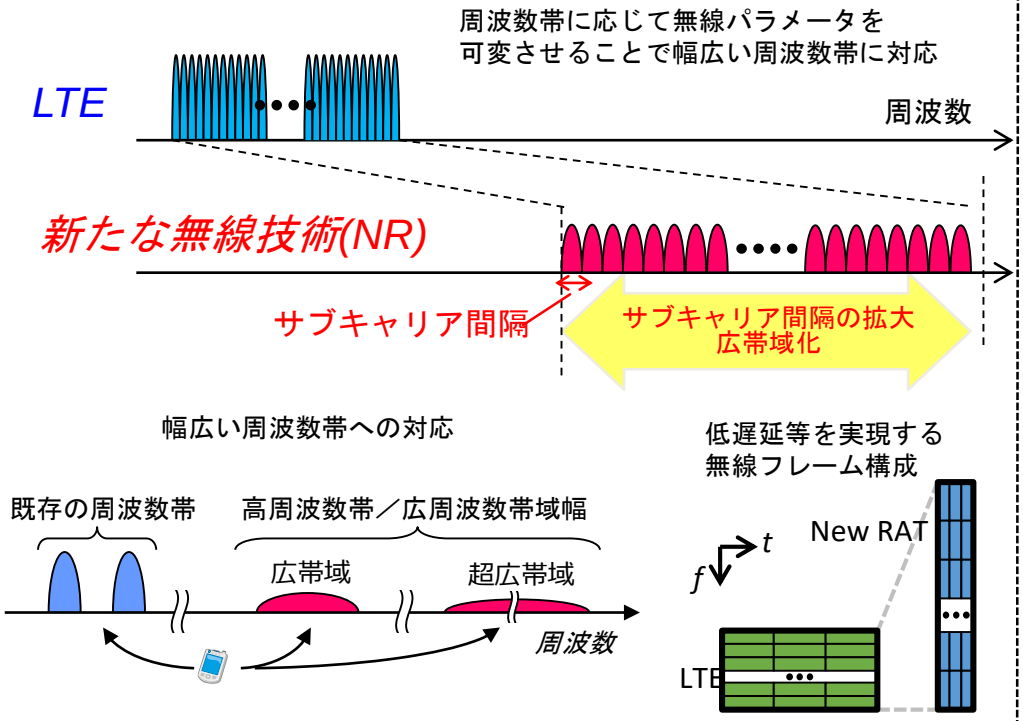
超高速、多数同時接続、高信頼・低遅延などの要求条件に対応した5Gサービスの提供が開始。

現在 【LTEの面展開】	2020年 【5G導入当初】	202X年 【5G普及期】
		

５Ｇのネットワーク構成 ①

5Gの新たな無線技術（5G NR）

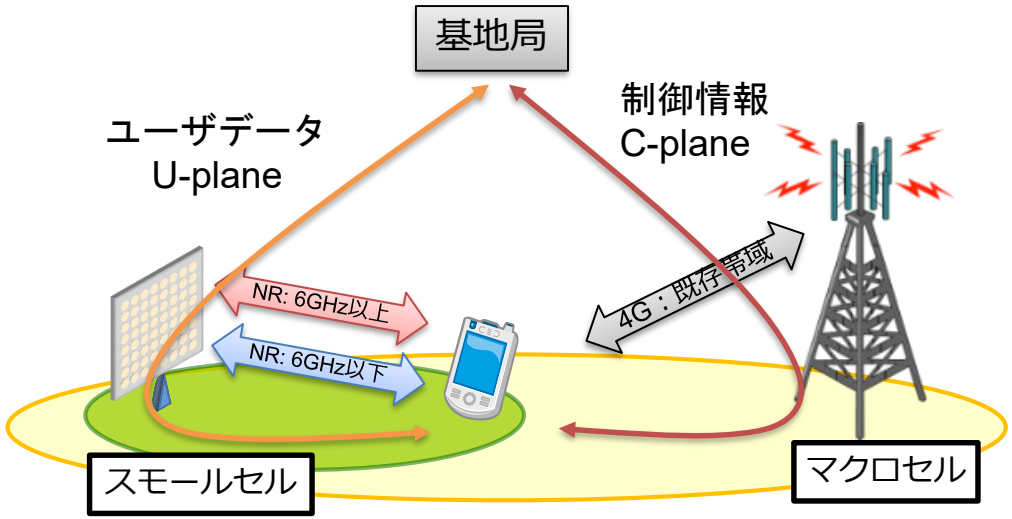
● 超高速実現に必要となる数百MHz以上の広周波数帯域への対応や、ミリ波などの高い周波数帯への対応、超低遅延を実現する無線フレーム構成等の新たな無線技術



制御情報（C）/ユーザデータ（U）分離

● 周波数帯やカバレッジ等の異なる複数のセルで制御情報とユーザデータを分離して伝送

● 具体的には、カバレッジの広いマクロセルで制御情報を提供（C-plane）し、超高速通信等が提供可能なスモールセルでユーザデータを提供（U-plane）



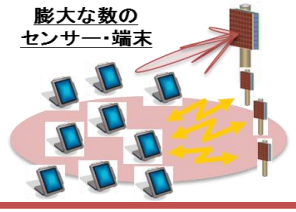
５Ｇのネットワーク構成 ②

ネットワークスライシング

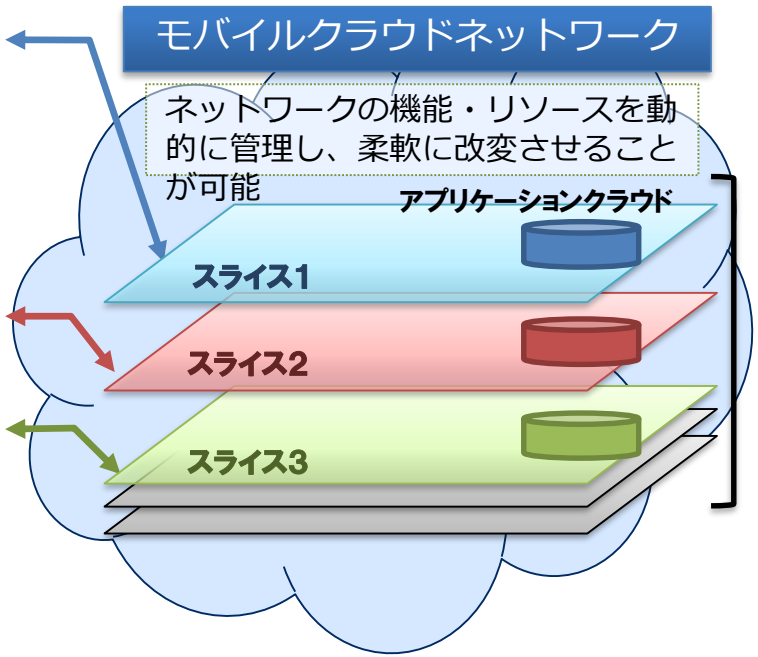
○ 現在は、画一のネットワークに異なる要件のアプリ・サービスのトラヒックが混在
○ ネットワークスライスを設定することで、アプリ・サービス毎にトラヒックの分離が可能

超高速（eMBB）

多数接続（mMTC）



超低遅延（URLLC）

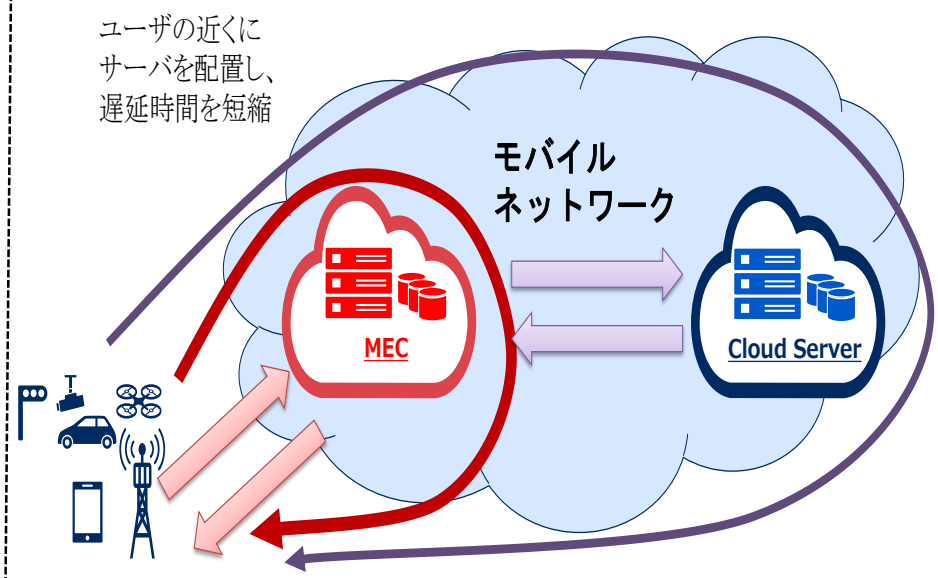


モバイル・エッジ・コンピューティング※

○ 超低遅延が求められる自動車などについて、ユーザの近くにデータ処理等を行うMECサーバを配置することで、高速（低遅延）でサービスを提供することが可能

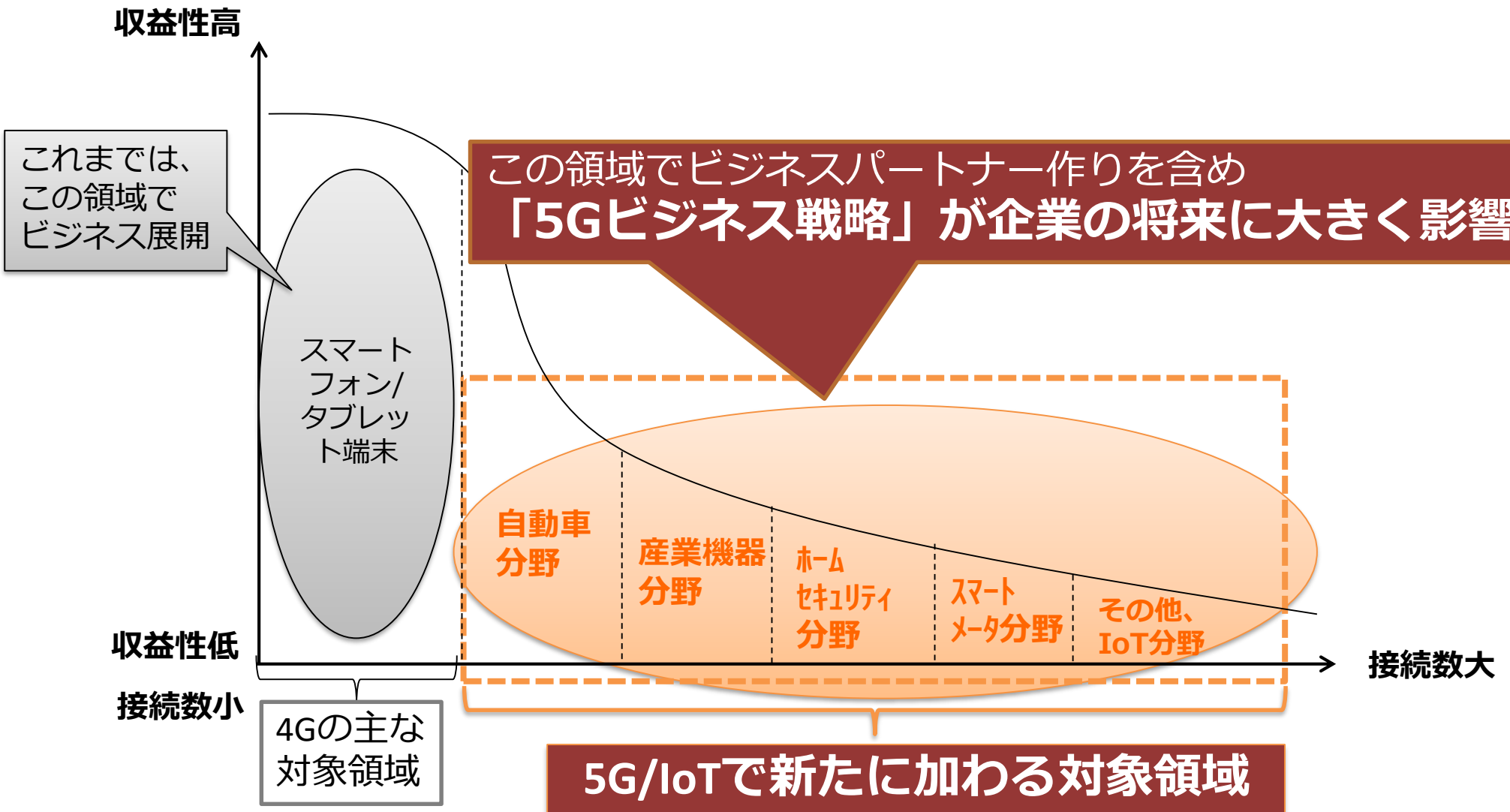
【現在】遅延大
（ネットワーク側のクラウドで処理）

【５Ｇ】低遅延
（ユーザ近くでデータ処理）



※ETSIでは、ネットワークエッジでクラウドやITサービスを提供する機能として、“Multi-access Edge Computing”という言葉が用いられている

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

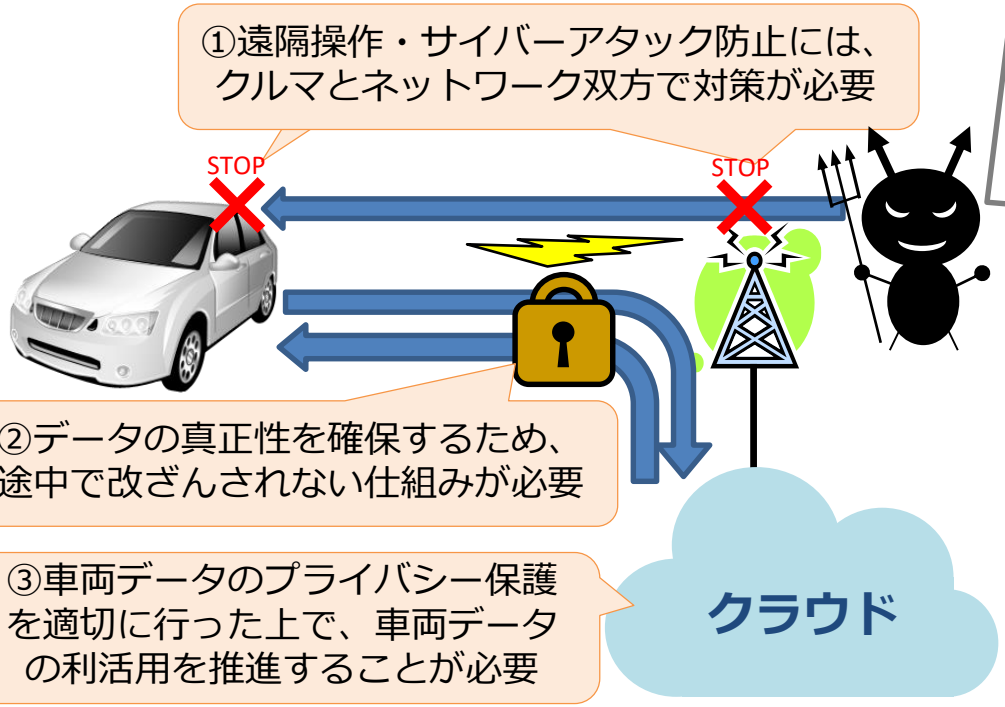
つながることによる「新たな脅威」

「Connected Car」の３つの脅威への対応

①遠隔操作・サイバーアタック対策

②データの真正性確保

③プライバシー保護



これからの「Connected Car」を想定したセキュリティ対策、サービス開発の推進が重要

【遠隔操作対策でリコールした例】

○2015年7月、クライスラーが140万台規模のリコールを実施

- 無線回線から車のコンピュータに侵入する実験が行われ、インターネットに公開されたことを受けて対応したもの
- 実験では以下のことが可能であった

①エンジンＯＦＦ

②ワイパーの操作

③加減速　等

出典：2015年7月25日日本経済新聞夕刊

【ネットワーク経由での攻撃例（盗難防止装置解除等）】

出典：Pen Test Partners Website https://www.pentestpartners.com/

Ⅰ．サイバーセキュリティ リスクの深刻化

Ⅱ．5G／IoT化の急速な進展

Ⅲ．サイバーセキュリティ戦略

Ⅳ．IoTセキュリティ総合対策

Ⅴ．国家安全保障戦略

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（８名；10名以下）

※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

閣僚が参画

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
後藤　厚宏　情報セキュリティ大学院大学学長
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
前田　雅英　日本大学大学院法務研究科教授
宮澤　英一　株式会社デジタルハーツホールディングス取締役会長
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

（平成31年2月10日現在）

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・即応調査チーム（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＞

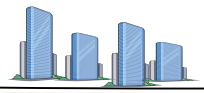
文部科学省（セキュリティ教育）等

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

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

1．新たな価値創出を支えるサイバーセキュリティの推進

＜施策例＞・**経営層の意識改革の促進（「費用」から「投資」へ）**

・投資に向けたインセンティブ創出（情報発信・開示による市場の評価、保険の活用）

・セキュリティ・バイ・デザインに基づくサイバーセキュリティビジネスの強化

2．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

＜施策例＞・**中小企業を含めたサプライチェーン（機器・データ・サービス等の供給網）におけるサイバーセキュリティ対策指針の策定**

3．安全なIoTシステムの構築

＜施策例＞・IoTシステムにおけるセキュリティの体系の整備と国際標準化

・**IoT機器の脆弱性対策モデルの構築・国際発信**

等

4　目的達成のための施策

国民が安全で安心して暮らせる社会の実現

1．国民・社会を守るための取組
＜施策例＞・脅威に対する事前の防御**（積極的サイバー防御）**策の構築
・サイバー犯罪への対策

2．官民一体となった重要インフラの防護
＜施策例＞・安全基準等の改善・浸透（サイバーセキュリティ対策の**関係法令等における保安規制としての位置付け**）
・地方公共団体のセキュリティ強化・充実

3．政府機関等におけるセキュリティ強化・充実
＜施策例＞・**情報システムの状態のリアルタイム管理の強化**
・先端技術の活用による先取り対応への挑戦

4．大学等における安全・安心な教育・研究環境の確保
＜施策例＞・**大学等**の多様性を踏まえた対策の推進

5．2020年東京大会とその後を見据えた取組
＜施策例＞・**サイバーセキュリティ対処調整センターの構築の推進**
・成果のレガシーとしての活用

6．従来の枠を超えた情報共有・連携体制の構築
＜施策例＞・**多様な主体の情報共有・連携の推進**

7．大規模サイバー攻撃事態等への対処態勢の強化
＜施策例＞・**サイバー空間と実空間の双方の危機管理に臨むための大規模サイバー攻撃事態等への対処態勢の強化**

等

4　目的達成のための施策

国際社会の平和・安定及び我が国の安全保障への寄与

1．自由、公正かつ安全なサイバー空間の堅持

＜施策例＞・**自由、公正かつ安全なサイバー空間**の理念の発信
・サイバー空間における法の支配の推進

2．我が国の防御力・抑止力・状況把握力の強化

＜施策例＞・国家の**強靭性の確保**（①任務保証、②我が国の先端技術・防衛関連技術の防護、③サイバー空間を悪用したテロ組織の活動への対策）
・サイバー攻撃に対する**抑止力の向上**（①実効的な抑止のための対応、②信頼醸成措置）
・サイバー空間の**状況把握の強化**（①関係機関の能力向上、②脅威情報連携）

3．国際協力・連携

＜施策例＞・**知見の共有・政策調整**
・事故対応等に係る国際連携の強化
・能力構築支援　等

4　目的達成のための施策

横断的施策

人材育成・確保

＜施策例＞
- **戦略マネジメント層の育成・定着**
- 実務者層・技術者層の育成（**高度人材**含む）
- 人材育成基盤の整備
- **政府人材**の確保・育成の強化
- 国際連携の推進

研究開発の推進

＜施策例＞
- 実践的な研究開発の推進（**検知・防御等の能力向上、不正プログラム等の技術的検証**を行うための体制整備）
- **AI等**中長期的な技術・社会の進化を視野に入れた対応

全員参加による協働

＜施策例＞
- サイバーセキュリティの普及啓発に向けた**アクションプランの策定、国民への情報発信**（サイバーセキュリティ月間の充実等）
- サイバーセキュリティ教育の推進

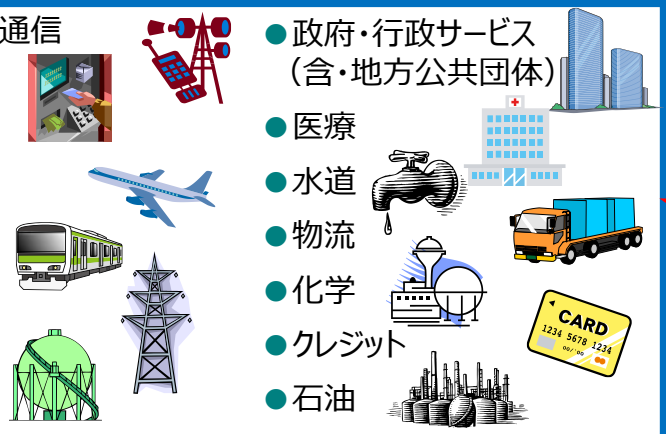
重要インフラの情報セキュリティ対策に係る第４次行動計画

官民連携による重要インフラ防護の推進

重要インフラにおいて、機能保証の考え方を踏まえ、サイバー攻撃や自然災害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すとともに、その発生時には迅速な復旧を図ることにより、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現する。

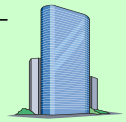
重要インフラ（１４分野）

- 情報通信
- 金融
- 航空
- 空港
- 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



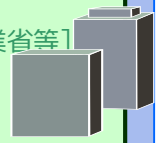
ＮＩＳＣによる調整・連携

重要インフラ所管省庁（５省庁）



- 金融庁　［金融］
- 総務省　［情報通信、行政］
- 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　［航空、空港、鉄道、物流］

関係機関等



- 情報セキュリティ関係省庁［総務省、経済産業省等］
- 事案対処省庁［警察庁、防衛省等］
- 防災関係府省庁［内閣府、各省庁等］
- 情報セキュリティ関係機関［NICT、IPA、JPCERT等］
- サイバー空間関連事業者［各種ベンダー等］

重要インフラの情報セキュリティ対策に係る第４次行動計画

安全基準等の整備・浸透

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

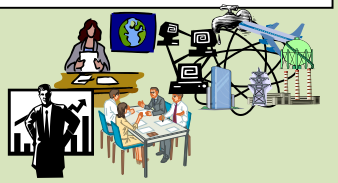
情報共有体制の強化

連絡形態の多様化や共有情報の明確化等による官民・分野横断的な情報共有体制の強化

障害対応体制の強化

官民が連携して行う演習等の実施、演習・訓練間の連携による重要インフラサービス障害対応体制の総合的な強化

リスクマネジメント及び対処態勢の整備



リスク評価やコンティンジェンシープラン策定等の対処態勢の整備を含む包括的なマネジメントの推進

防護基盤の強化

重要インフラに係る防護範囲の見直し、広報広聴活動、国際連携の推進、経営層への働きかけ、人材育成等の推進

総務省のサイバーセキュリティ推進体制

サイバーセキュリティ統括官（※）

審議官(国際技術、サイバーセキュリティ担当)（※）

参　事　官　（総括担当）

- 総括
- インシデント発生時の対応（通信・放送事業者）
- 新たなセキュリティ対策の検討
- 民間団体等を通じた情報共有の促進

参　事　官　（政策担当）

- IoT機器の脆弱性調査
- 法制度（NICT法、不正アクセス禁止法等）
- セキュリティ人材の育成、周知・啓発
- 暗号・電子署名の推進

参　事　官　（国際担当）

- 各種国際会議対応
- 諸外国との連携
- 研究開発

サイバーセキュリティ・情報化審議官

大臣官房企画課
サイバーセキュリティ・情報化推進室長

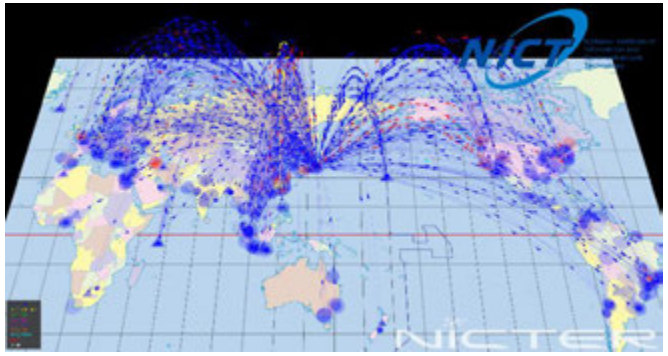
- インシデント発生時の対応（省内情報システム運用部局、所管独法等）
- 省内情報システム運用部局、所管独法等への注意喚起情報の発信
- 省内職員に対する情報セキュリティ訓練、教育の実施

（※）平成30年7月に新たに設置。

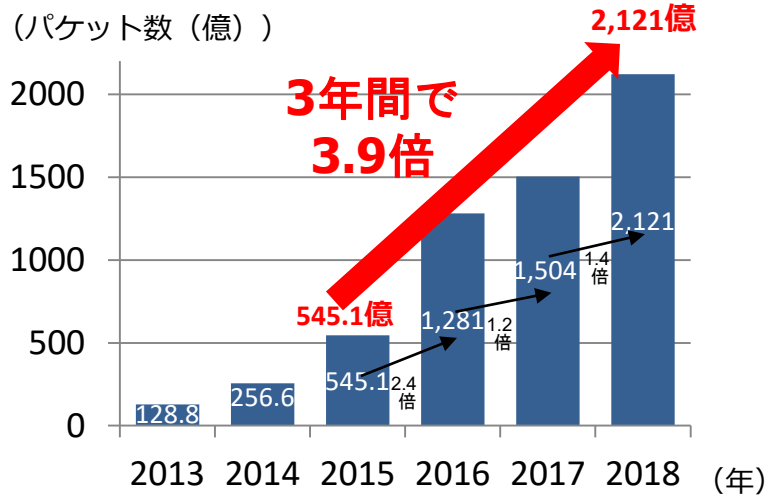
NICTERによるサイバー攻撃の観測

○　国立研究開発法人情報通信研究機構（NICT）では、大規模サイバー攻撃観測網であるNICTERにおいて、未使用のIPアドレス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。

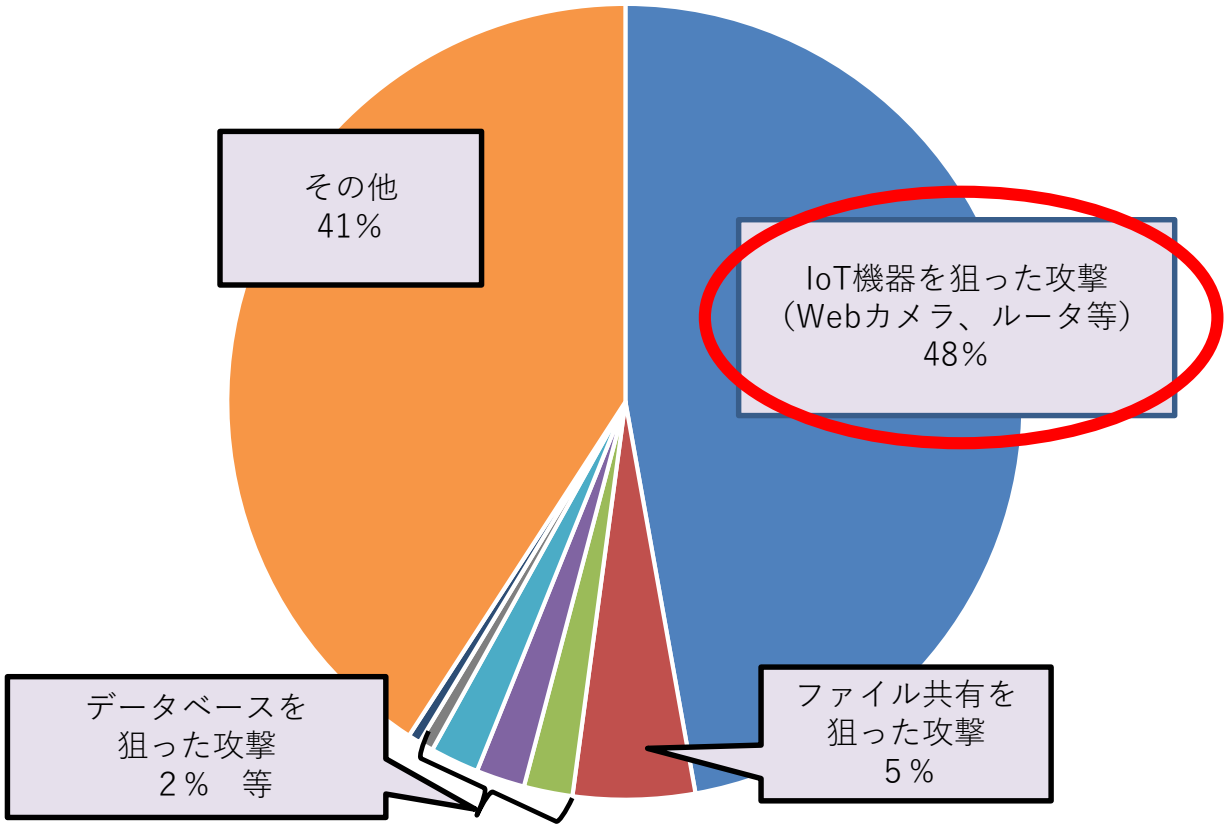
NITCERにより観測されるサイバー攻撃の様子



NITCERで１年間に観測された
サイバー攻撃回数



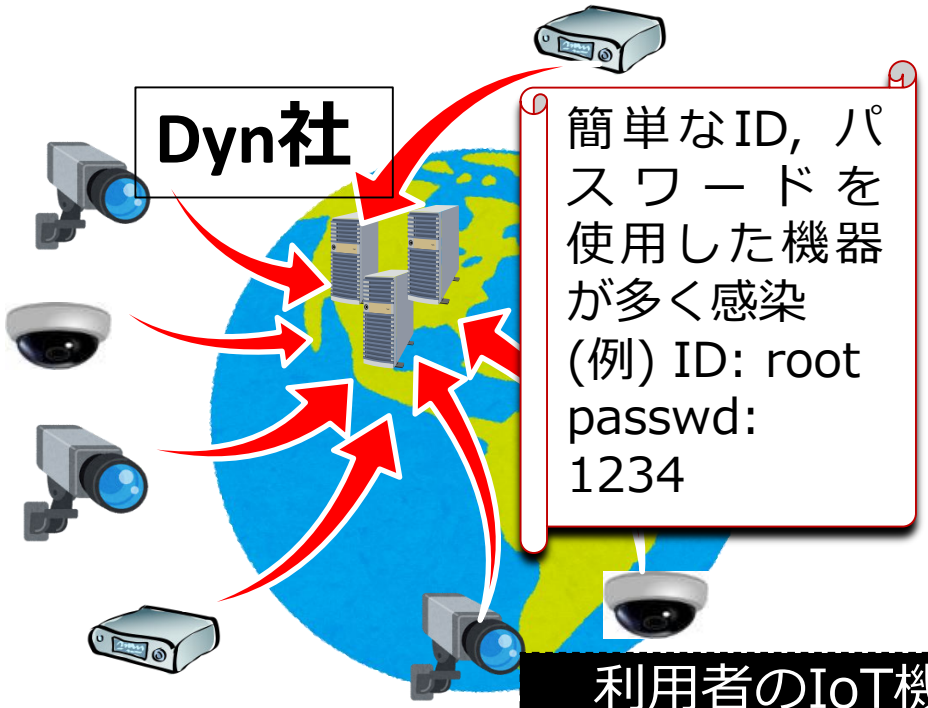
約半数がIoT機器を狙った攻撃



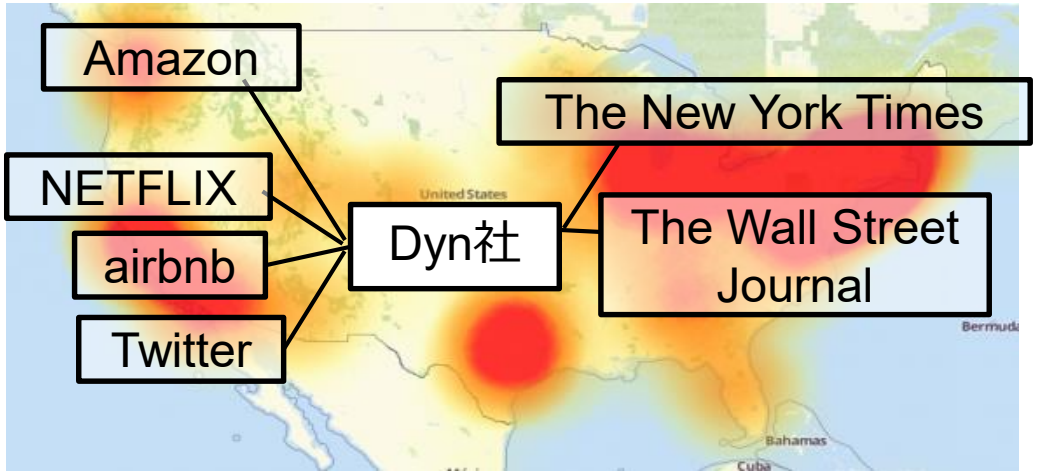
IoT機器を踏み台とした大規模DDoS攻撃

○　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攻撃が発生。その結果、多数の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。

○　「Mirai」というマルウェアに感染した10万台を超えるIoT機器から、大量の通信（最大1.2Tbps)が発生したことが原因。



システムダウンの状況



利用者のIoT機器がマルウェアMiraiの攻撃を受けた結果、攻撃者のツールとして利用される結果に。

Cyber Hygiene（サイバー空間を衛生的で健康に保つ）が重要

IoT機器がサイバー攻撃の対象として狙われやすい理由

①	脅威の影響範囲・影響度合いが大きい
②	IoT機器のライフサイクルが長い
③	IoT機器に対する監視が行き届きにくい
④	IoT機器側とネットワーク側の環境や特性の相互理解が不十分である
⑤	IoT機器の機能・性能が限られている
⑥	開発者が想定していなかった接続が行われる可能性がある

（参考）IoT機器における脅威の事例

①ウェブカメラの事例

ネットに接続されるウェブカメラなどの映像や音声がインターネット上で**誰でも閲覧できる設定**となっていることが判明。

②複合機の事例

日本の大学等において、複合機に保存されたデータがインターネット上で**誰でも閲覧できる設定**となっていた。

③水道関連設備

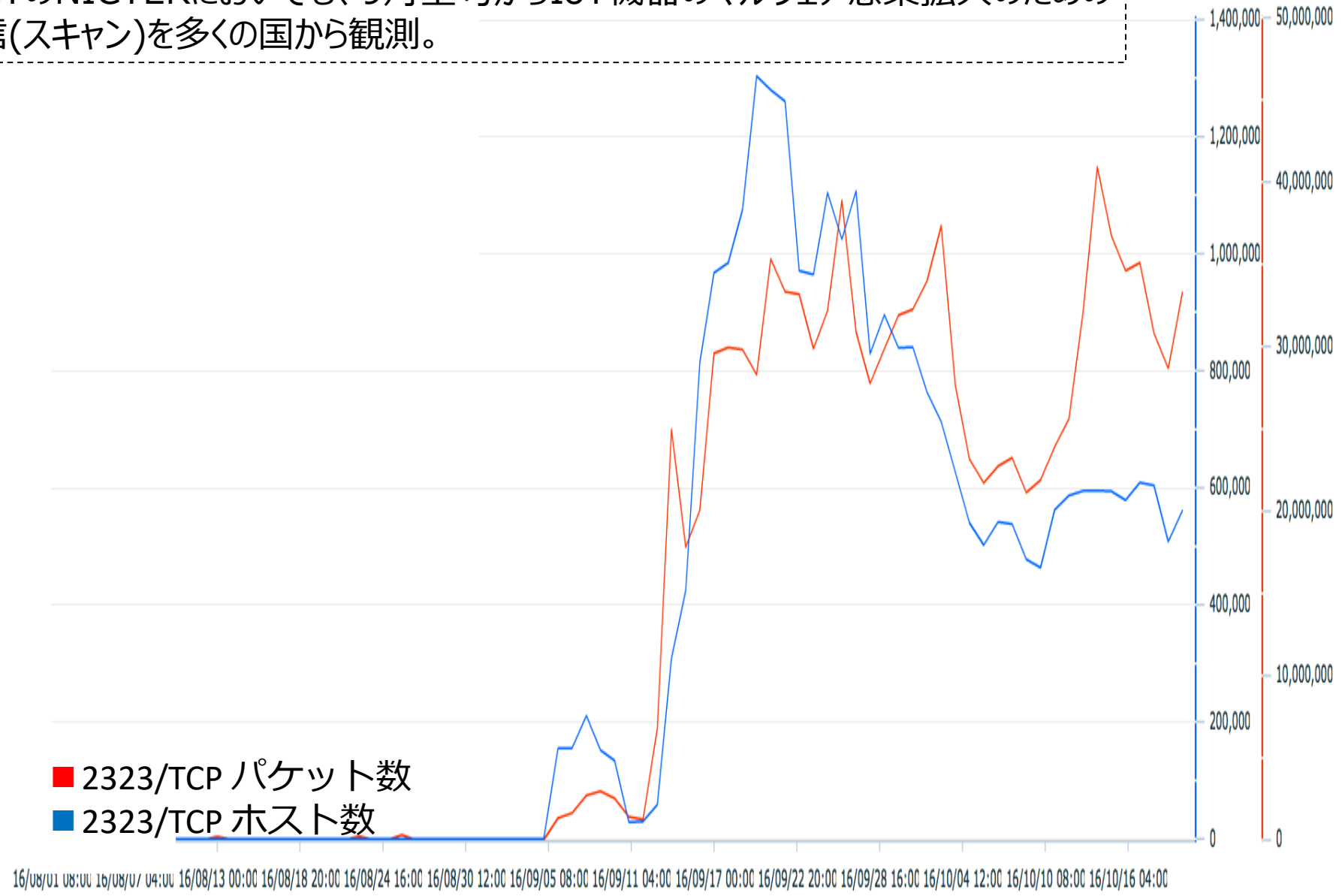
病院等に設置された水道関連設備のデータロガーがインターネット側からアクセス可能なまま運用　されており、**動作状況が外部から閲覧可能**な状態であることに加え、**第３者から運転モード(RUN/STOP)の切り替えが可能**な状態になっていた。

④電力監視設備

工場等に設置された電力監視機器システムがインターネット側からアクセス可能なまま運用されており、**警告の閾値の変更、警告の解除、プロキシ設定、再起動等の操作が、第３者が可能**な状態になっていた。

Dyn社への攻撃前の攻撃パケットの推移

✓ 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。



Ⅰ．サイバーセキュリティ リスクの深刻化

Ⅱ．5G／IoT化の急速な進展

Ⅲ．サイバーセキュリティ戦略

Ⅳ．IoTセキュリティ総合対策

Ⅴ．国家安全保障戦略

IoTセキュリティ総合対策（2017年10月公表）

①脆弱性対策に係る体制の整備

- IoT機器の脆弱性についてライフサイクル全体（設計・製造、販売、設置、運用・保守、利用）を見通した対策が必要。
- 脆弱性調査の実施等のための体制整備が必要。

②研究開発の推進

- セキュリティ運用の知見を情報共有し、ニーズにあった研究開発を促進。

③民間企業等における セキュリティ対策の促進

- 民間企業等のサイバーセキュリティに係る投資を促進。
- サイバー攻撃の被害及びその拡大防止のための、攻撃・脅威情報の共有の促進。

④人材育成の強化

- 圧倒的にセキュリティ人材が不足する中、実践的サイバー防御演習等を推進。

⑤国際連携の推進

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

半年に1度を目途としつつ、必要に応じて検証（関係府省と連携）

進捗状況や取組方針を整理し、「プログレスレポート」として公表（平成30年7月、令和元年5月）

脆弱なIoT機器への対策

○ 現在使用されている機器への対策（IoT機器の脆弱性調査）

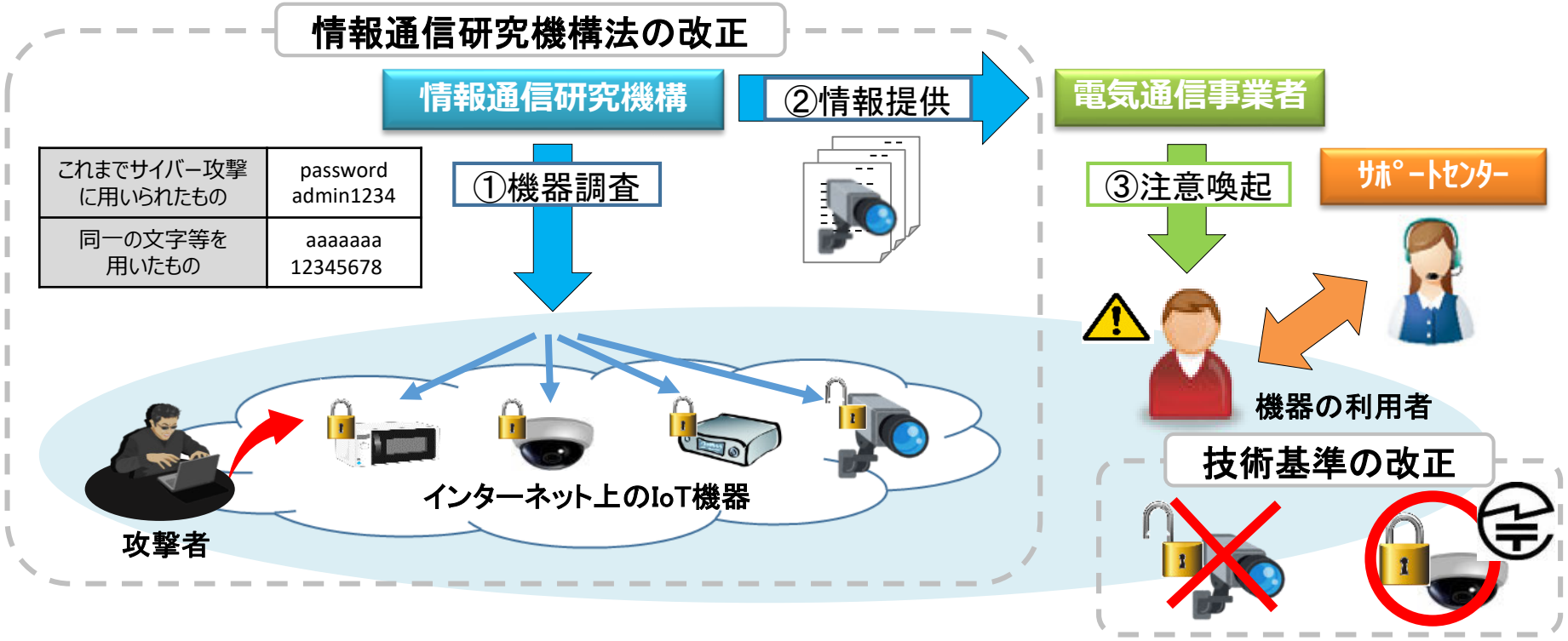
- 現在使用されているIoT機器への対応として、NICTがサイバー攻撃に悪用されるおそれのある機器を調査（※1）し、電気通信事業者を通じた利用者への注意喚起を行う取組「NOTICE（※2）」を2019年２月20日（水）より開始。

※1：サイバー攻撃に悪用されるおそれのあるIoT機器の調査等を実施するため、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。

※2：National Operation Towards IoT Clean Environment

○ 今後製造される機器への対策（技術基準の改正）

- 今後製造されるIoT機器については、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を改正を予定（2020年４月施行予定）。



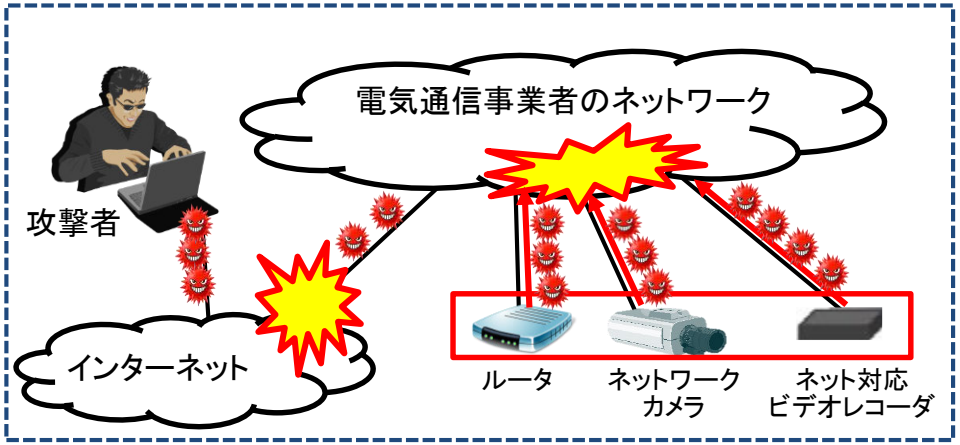
IoT機器のセキュリティ対策に関する技術基準の改正

【背景・課題】

- 近年、インターネットにつながるWebカメラやルータ等のIoT機器を悪用したサイバー攻撃により、通信網に深刻な障害を及ぼす事案※1が発生。
- その原因としては、パスワード設定の不備などによりIoT機器を悪用されるケースが多く、その対策が重要な課題。

※1 2016年10月、「Mirai」というマルウェアに感染した10万台を超えるIoT機器が、米国のDyn(ダイン)社のシステムを攻撃し、Dyn社のサーバーを利用してい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障害が発生。

＜IoT機器が乗っ取られてサイバー攻撃に悪用される事案のイメージ＞



【端末設備等規則（省令）の改正概要】

- インターネットプロトコルを使用し、電気通信回線設備を介して接続することにより、電気通信の送受信に係る機能を操作することが可能な端末設備について、最低限のセキュリティ対策として、以下の機能を具備することを技術基準(端末設備等規則)に追加する。

  ①アクセス制御機能※1(例えばアクセス制限をかけてパスワード入力を求め、正しいパスワードの入力時のみ制限を解除する機能のこと)

  ②初期設定のパスワードの変更を促す等の機能

  ③ソフトウェアの更新機能※1

  又は①～③と同等以上の機能※2

※1 ①と③の機能は、端末が電源オフになった後、再び電源オンに戻った際に、出荷時の初期状態に戻らず電源オフになる直前の状態を維持できることが必要。
※2 同等以上の機能を持つものとしては、国際標準ISO/IEC15408に基づくセキュリティ認証(CC認証)を受けた複合機等が含まれる。

- PCやスマートフォン等、利用者が随時かつ容易に任意のソフトウェアを導入することが可能な機器については本セキュリティ対策の対象外とする。

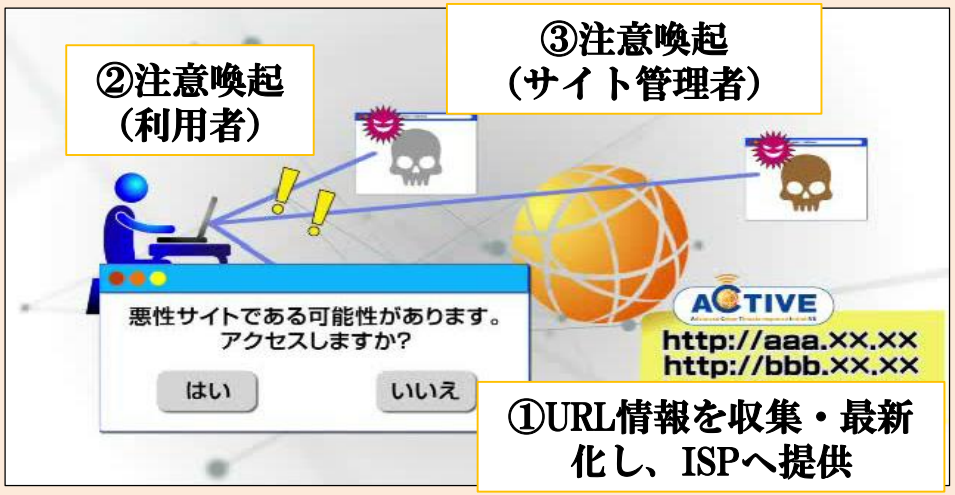
【今後の予定】

- 本年3月1日に改正省令を公布。来年(2020年)4月1日に改正省令を施行。
- 改正省令の運用方法や解釈等を定めるガイドラインも策定(本年4月)。

ウィルス感染被害予防対策“ACTIVE”

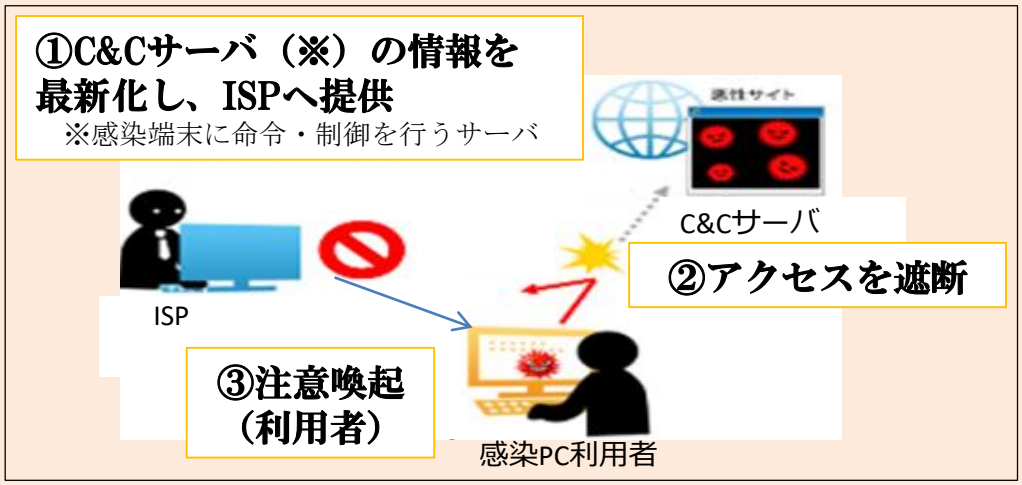
ACTIVE (Advanced Cyber Threats response InitiatiVE)

（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。
③ 感染PC利用者に注意喚起。

注意喚起件数：約5万件（2017年）　　通信遮断件数：約3．6億件（2017年）

○ 総務省の調査研究実施期間：平成25～29年度

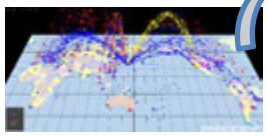
⇒　**現在は、事業者が自主的に実施。**

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

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



■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

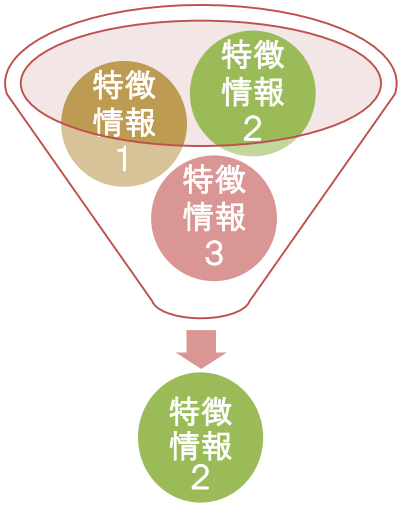
■Android APK関連データ

アプリのカテゴリ情報や説明文等

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。

安全な暗号利用の推進

○ 総務省では、電子政府等の安全性及び信頼性の確保を目的として、経済産業省と共同で暗号評価プロジェクトCRYPTREC（Cryptography Research and Evaluation Committees）を実施

○ CRYPTRECは、平成25年3月1日に、**「電子政府推奨暗号リスト」**（平成15年2月20日公表）を改定した「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）※1」を策定

※1：https://www.cryptrec.go.jp/list.html

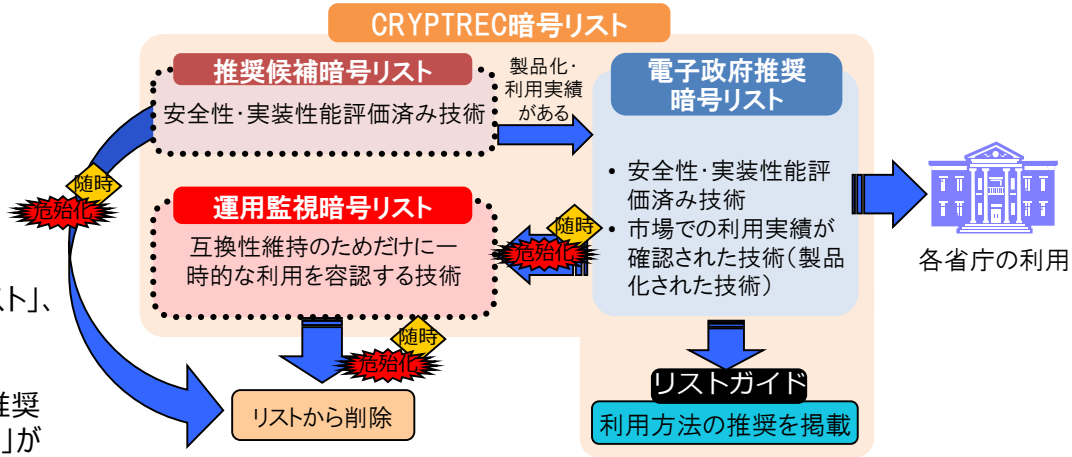
◇ CRYPTRECの概要

○ 活動内容

- 「CRYPTREC暗号リスト」※の公表
- 暗号技術の安全性等の監視及び評価を実施

※ CRYPTREC暗号リストは、「電子政府推奨暗号リスト」、「推奨候補暗号リスト」、「運用監視暗号リスト」から構成される。

※各府省庁における暗号化及び電子署名のアルゴリズムについて、「電子政府推奨暗号リストに記載されたものが使用可能な場合には、それを使用させること」が「政府機関等の情報セキュリティ対策のための統一基準」で定められている。



電子政府推奨暗号リスト改定の流れ

電子政府推奨暗号リスト

技術分野		暗号技術
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS
		RSASSA-PKCS1-v1_5
	守秘	RSA-OAEP
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号	該当なし
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	Kcipher-2

技術分野		暗号技術
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード	CCM
		GCM
メッセージ認証コード		CMAC
		HMAC
認証暗号		該当なし
エンティティ認証		ISO/IEC 9788-2
		ISO/IEC 9788-3

量子コンピュータ時代に向けた暗号の在り方の検討

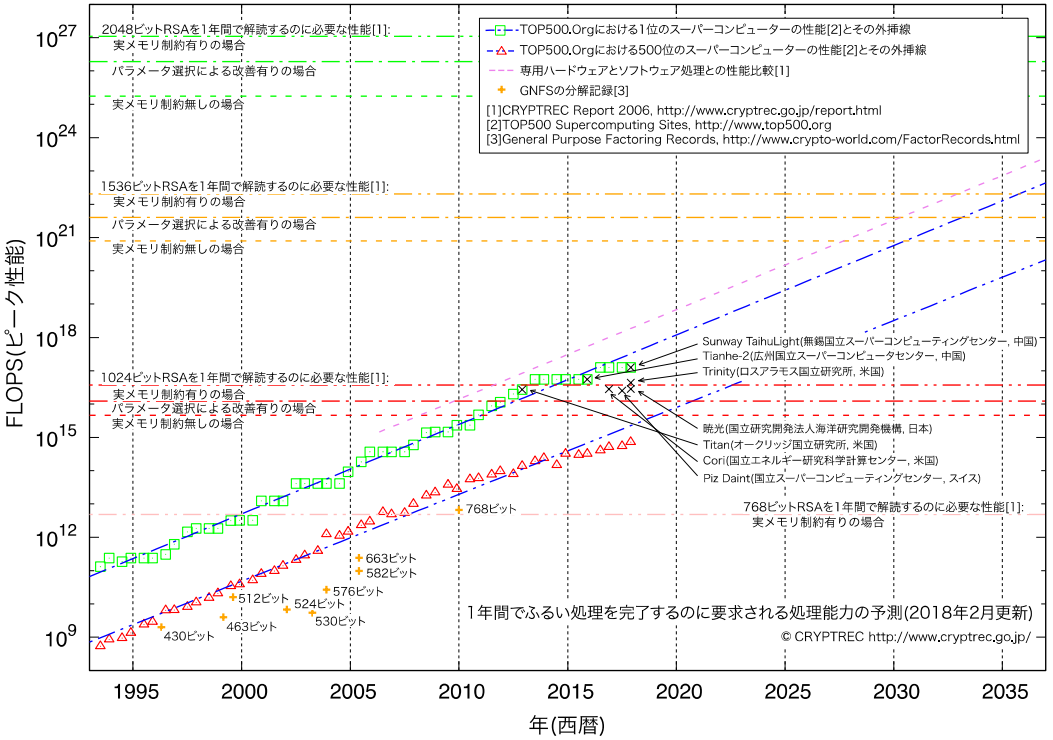


図１：素因数分解の困難性に関する計算量評価

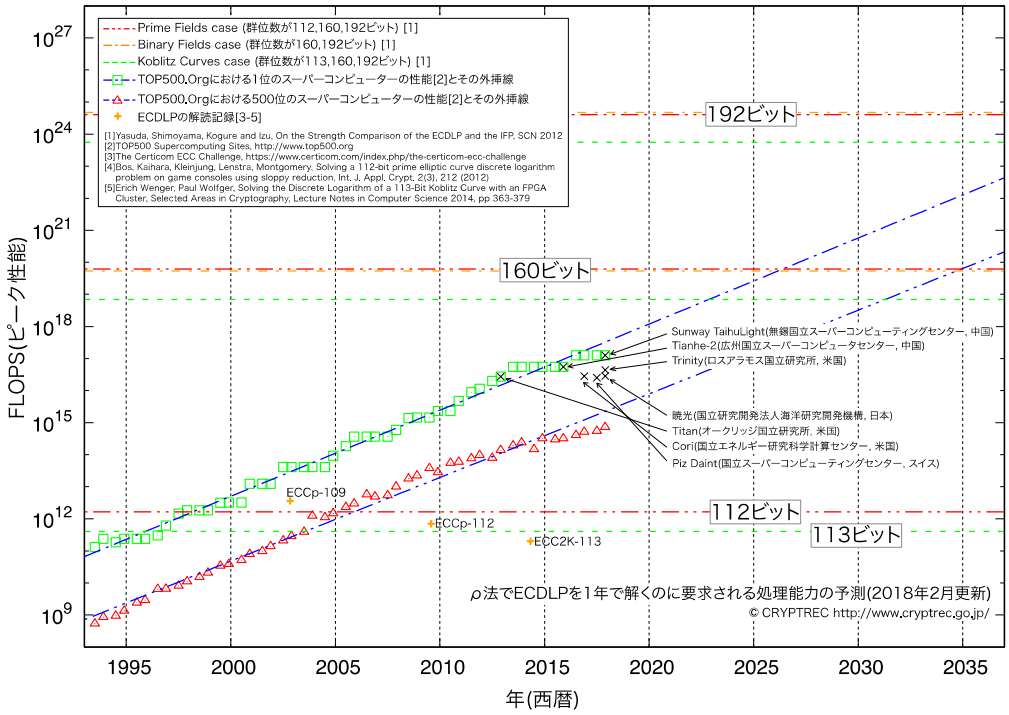


図２：楕円曲線上の離散対数計算の困難性に関する計算量評価

課題

- 遠くない将来に現在の**公開鍵暗号が容易に解読される**おそれ
- 大規模システムの**改修・更改**には**十年以上**を要する

「タスクフォース」を設置し、次期政府推奨暗号リストの要件、その他新たな暗号技術の動向を踏まえた検討を加速

セキュリティ対策情報開示の手引きの策定

※本年６月頃公表予定（５月１８日から意見募集中）

目的

- ✓ セキュリティ対策の情報開示が、企業にとっては自社の**社会的評価の向上**に、社会にとっては「セキュリティ対策の好循環（※）」を通じた社会全体の**セキュリティ対策の質の向上**につながることを踏まえ、企業が情報開示に当たって**How-Toを参照可能**なものとする。

手引き（仮称）の活用主体

- ✓ **社会的評価の向上のための自主的・能動的な情報開示**に一定の関心のある民間企業

対象とする情報開示

- ✓ **開示書類**を通じた情報開示を取り扱う。
- ✓ 開示書類の読み手は、**投資家、融資元、顧客・契約者・取引先、従業員、競合他社等を含む、社会全体の広範なステークホルダー**を想定。

内容

- ✓ 既に世の中に存在する**実例**を挙げた上で、各企業が自らの情報開示の実施に当たって**参考になる項目例や記載の粒度等**を記載する。

その他

- ✓ 情報開示のための**インセンティブ**の在り方については**手引きと並行して議論**の機会を設ける。

情報開示の手段

【各開示書類の記載内容の比較】

制度開示 ← → 任意開示

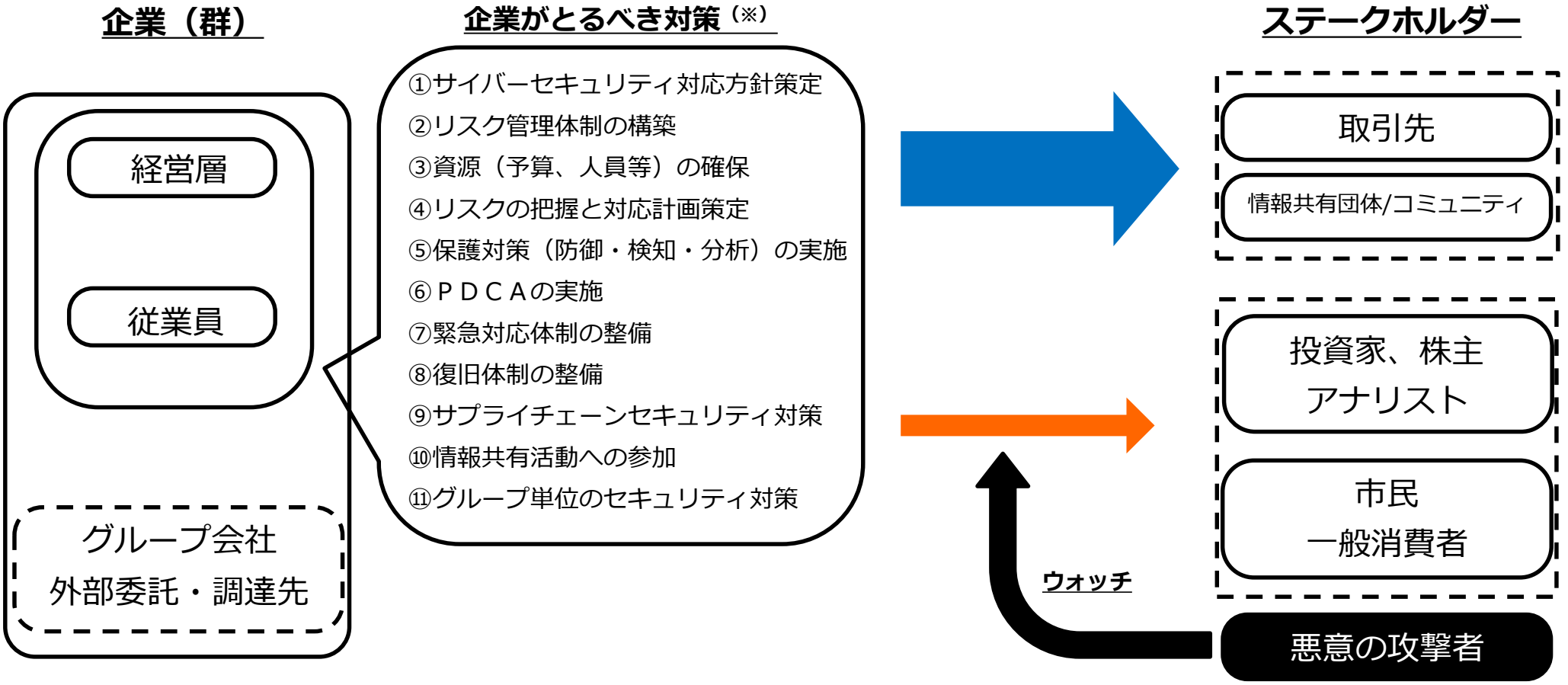
開示書類	有価証券報告書 コーポレートガバナンス報告書	CSR報告書 サステナビリティ報告書	情報セキュリティ報告書
記載量	**少ない**	**多い**	**セキュリティに特化**
閲覧者（想定）	✓**投資家**の投資判断を支援することを主目的とするため、閲覧対象者が限られている。	✓企業の取組、姿勢等をブランディングし、企業信頼度を高めることを目的とするため、**一般的な顧客**を幅広く対象。	✓内容がセキュリティに限られており、**セキュリティの専門家等**を閲覧者として想定。
記載内容	✓**リスク**としてのセキュリティや**企業統治**に必要な防止対策等、限定された項目・内容	✓**主要５項目（※）を中心に簡易で幅広い**記載内容	✓**セキュリティ対策に関する包括的かつ具体的**な内容

（※）①基本方針等の策定状況、②管理体制、③教育・人材育成、④社外との情報共有体制、⑤第三者評価・認証の５項目

（出典）企業のセキュリティ対策に係る情報開示の実態等に関する調査報告書（平成30年３月）をベースに総務省作成

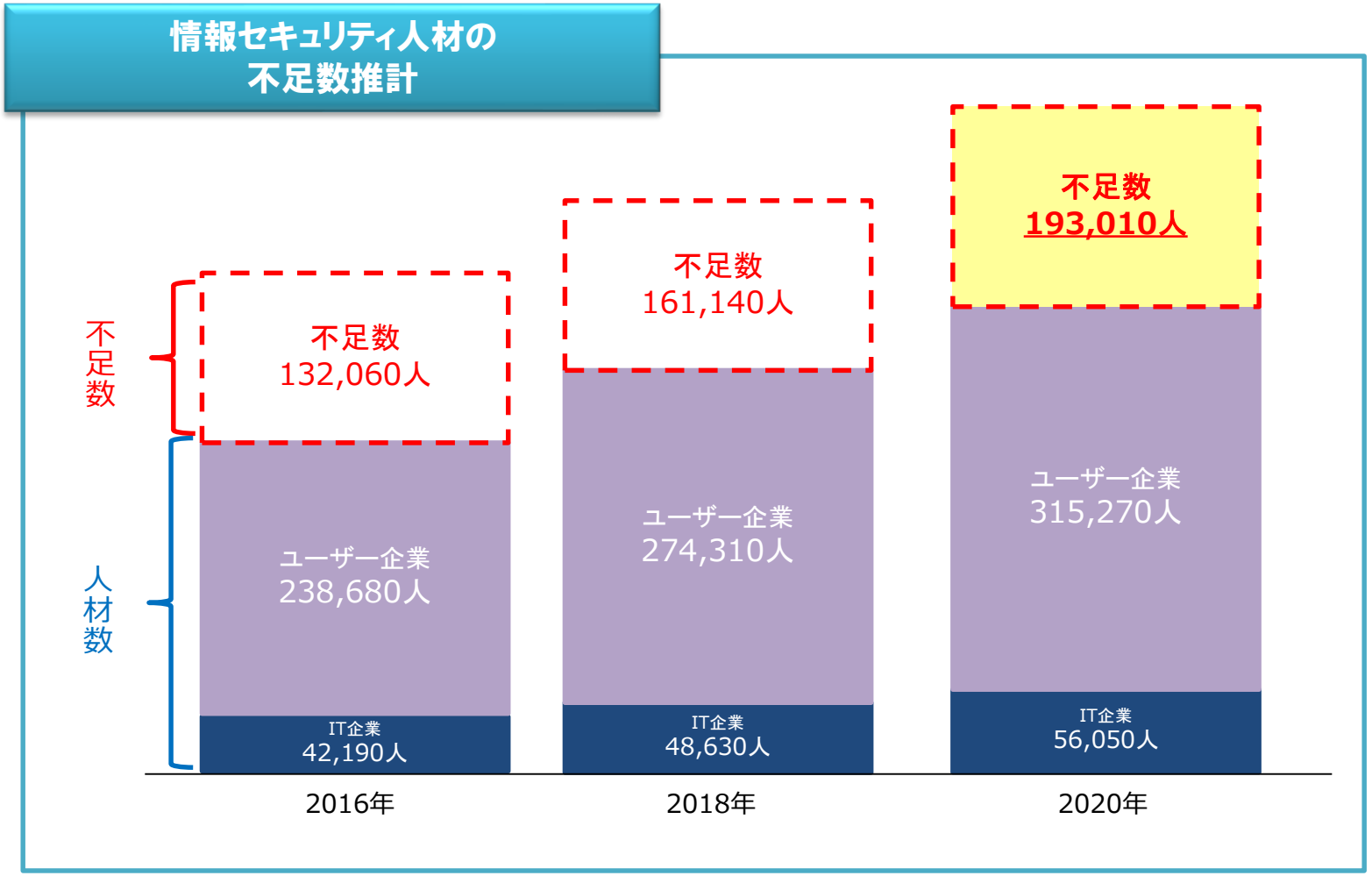
サイバーセキュリティ対策の情報開示について

- 企業におけるサイバーセキュリティ対策としては、いずれも重要であり、利用者等からすれば、これらの実施状況が開示されることにより、商品・サービスの選択などの際の参考になると考えられる。
- 一方で、例えば、サイバー攻撃への対応計画（④）や保護対策（⑤）を具体的に開示した場合は、サイバー攻撃等を誘発するリスクもあることから、④、⑤、⑦、⑧、⑨、⑪などについては開示する内容に留意が必要。



（※）サイバーセキュリティ経営ガイドライン等を参照

セキュリティ人材の不足



出典：経済産業省「IT人材の最新動向と将来推計に関する調査結果」（平成28年6月）及びみずほ情報総研「ITベンチャー等によるイノベーション促進のための人材育成・確保モデル事業　事業報告書 第2部 今後のIT人材需給推計モデル構築等 編」（平成28年3月）をもとに総務省作成
http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf
http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_fullreport.pdf

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）
　⇒ 年間約100回、約3千人規模で実施（1日コース、全都道府県で開催）。

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等大会関連組織のセキュリティ担当者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、平成30年度は137名が受講。

③ 25歳以下の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、平成30年度は46名が1年間のコースを終了。

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

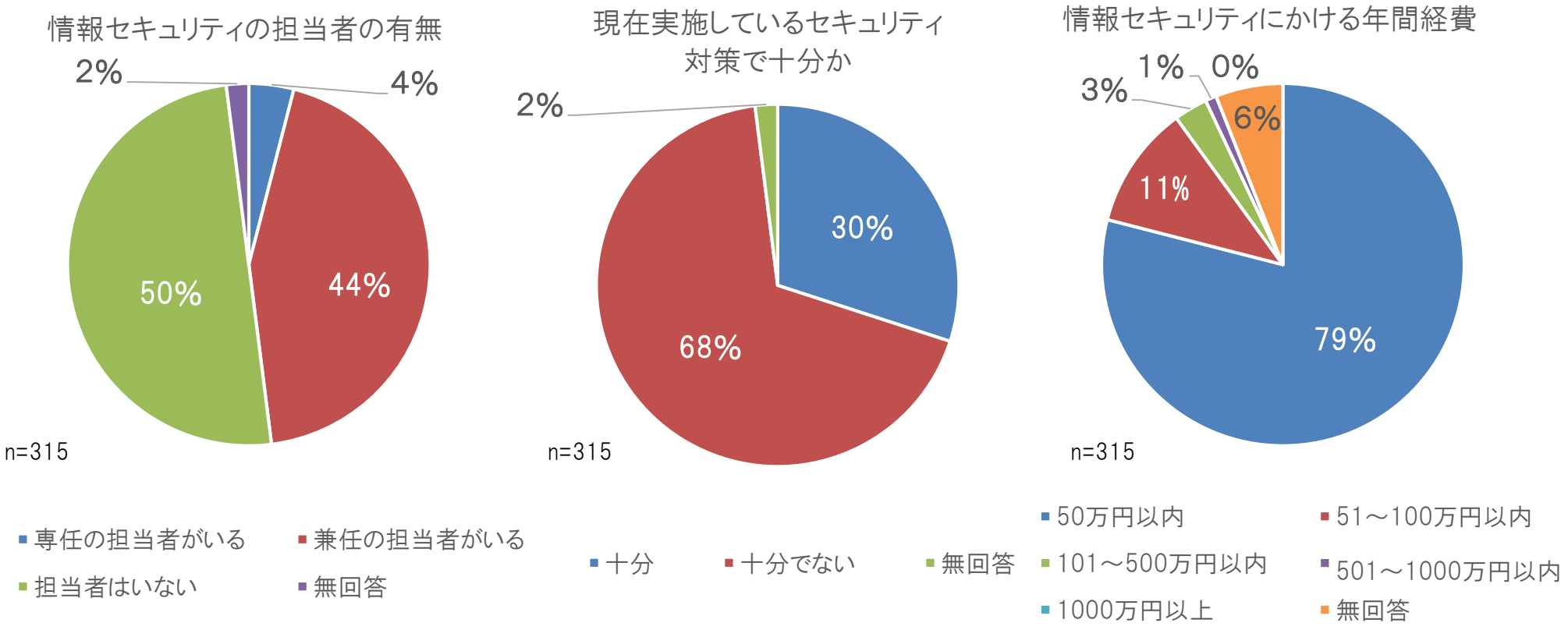
CYDER

サイバーコロッセオ

SecHack365

中小企業におけるサイバーセキュリティ対策の現状

○ 中小企業の過半数で、情報セキュリティ担当者がいない。担当者がいる場合でも、4割が他の業務との兼任。
○ 中小企業の多くが、経費や専門人材の不足を理由として、現在実施しているセキュリティ対策で十分でないと感じている。
○ 情報セキュリティにかける経費は、8割弱の中小企業が年間50万円以下。

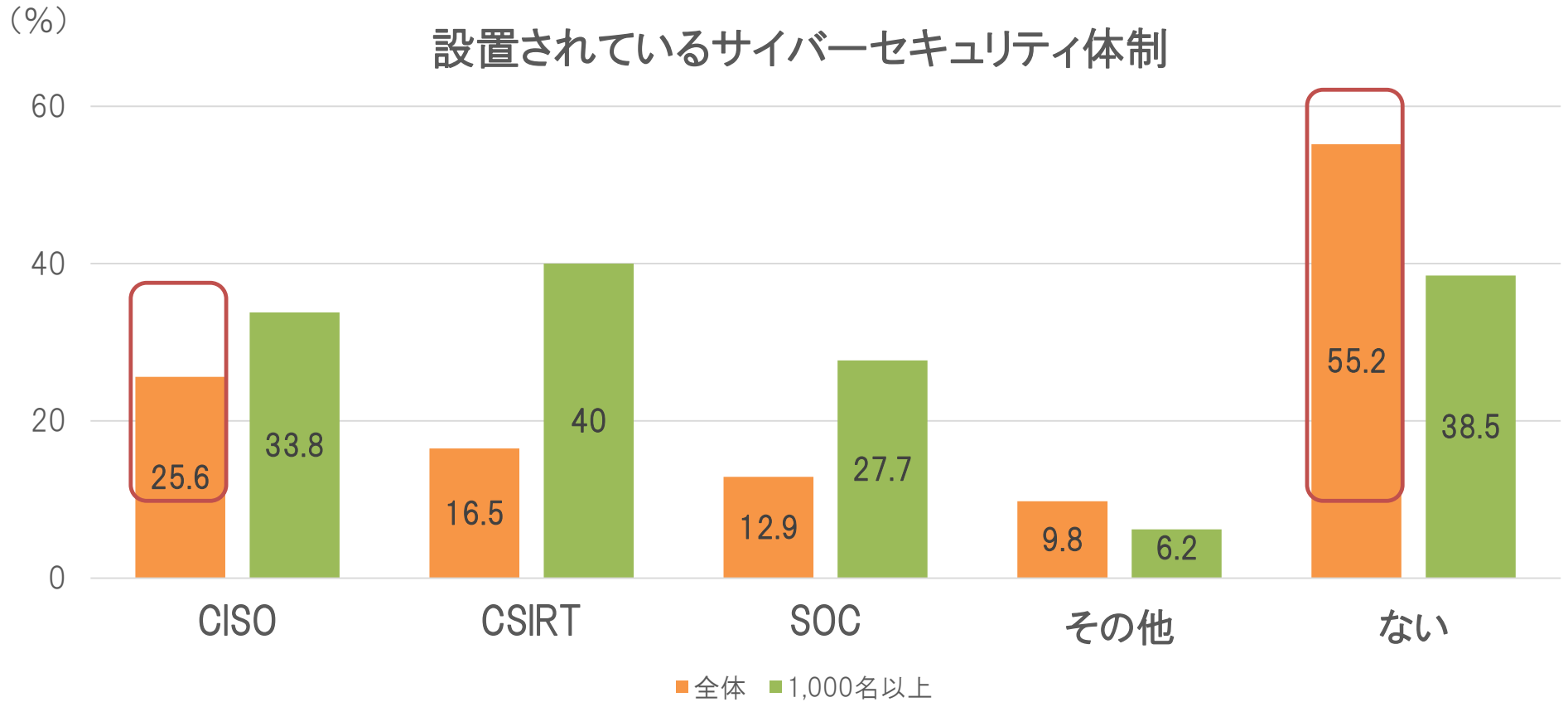


出典：大阪商工会議所「中小企業におけるサイバー攻撃対策に関するアンケート調査」（平成29年6月）をもとに総務省作成
http://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/Iken_Youbou/k290630cyb_ank.pdf

CISO、CSIRT等の規模別の設置割合

○　過半数の企業ではサイバーセキュリティ体制を構築していない状況であり、サイバーセキュリティ体制があると回答した企業のなかで最も多く設置されているのはCISOである。

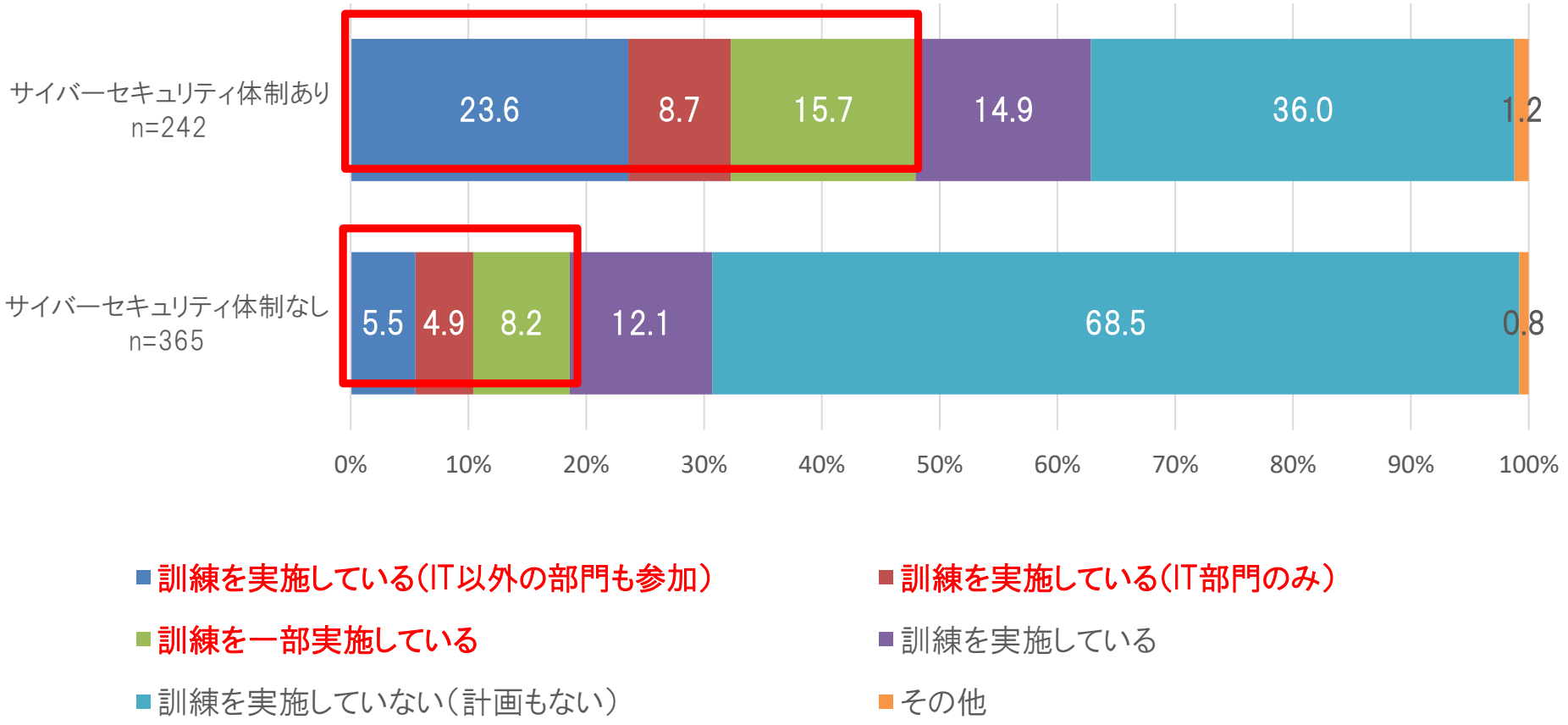
○　従業員数1,000名以上の企業以外では、CISO、CSIRT、SOCの設置が進んでいない。



出典：MS&ADインターリスク総研「企業の情報セキュリティ対策に関する実態調査報告書」（2018年12月）をもとに総務省作成

セキュリティ・インシデント発生時の訓練実施状況

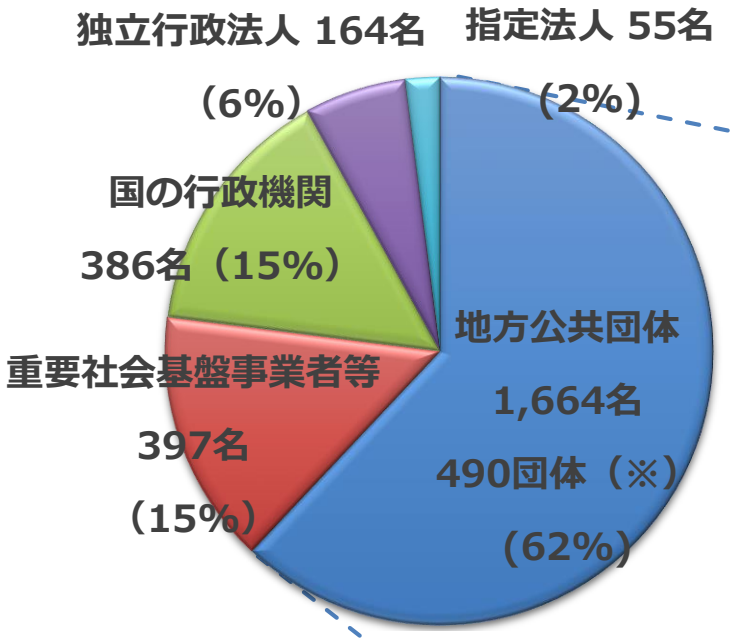
○　サイバーセキュリティ体制の有無で比較すると、体制のある組織・企業では、「訓練を実施している（IT以外の部門も参加）」、「訓練を実施している（IT部門のみ）」、「訓練を一部実施している」の合計が48.0%と半数近い。一方、体制が無い場合には、同合計が18.6%となっており、30ポイント近い差が出ている。



出典：MS&ADインターリスク総研「企業の情報セキュリティ対策に関する実態調査報告書」（2018年12月）をもとに総務省作成

実践的サイバー防御演習（CYDER）の受講実績（2018年度）

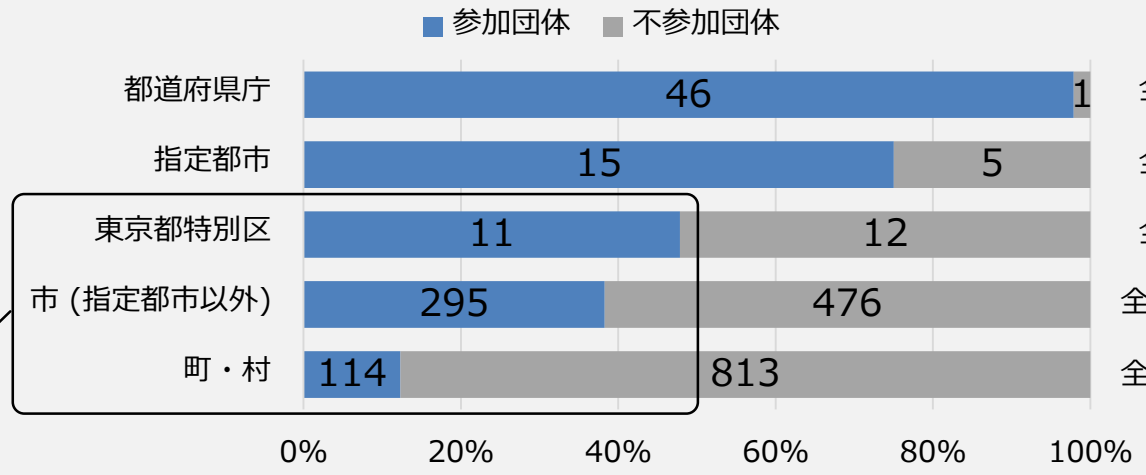
① 組織別の受講者数（全コース総数2,666名）



（※）地方公共団体481団体に加え、医療広域連合等９団体が受講

東京都特別区及び市は
半数以下であり、
町・村は12%

②地方公共団体（全1,788団体中481団体が受講）



地域におけるセキュリティ人材育成に向けた方策

1. 研修機会の偏在

気づきの機会がない
研修があっても参加者が少ない
地方で研修が開催されない
悪循環

2. 組織能力の偏在

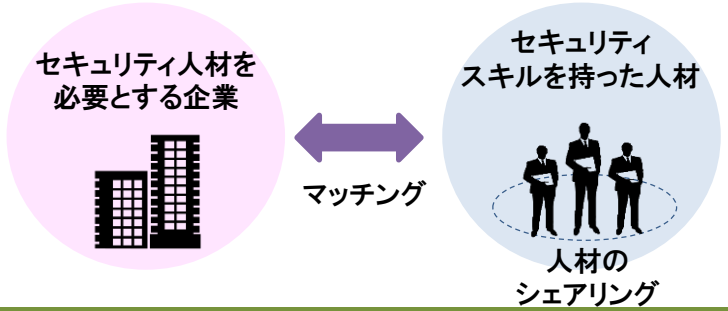
何をすればよいかわからない
専門人材を雇用できない
対策が進まない
悪循環

3. 就業機会の偏在

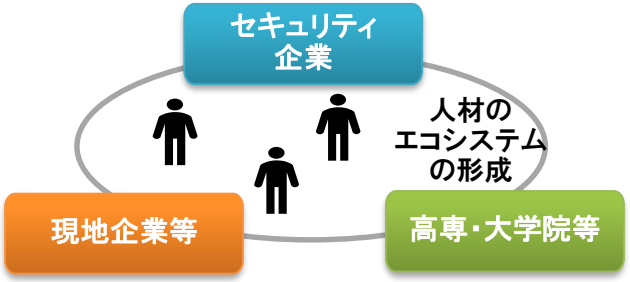
雇用の受け皿がない
地域の若年層がセキュリティ人材を目指さない
地域におけるセキュリティ人材がさらに不足
悪循環

1. 地域におけるセキュリティファシリテーターの育成

2. 地域でのセキュリティ人材のシェアリング



3. 地域におけるセキュリティ人材のエコシステムの形成



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

● 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)

５Ｇセキュリティ会議

・令和元年５月２～３日　チェコ共和国プラハ市
・チェコ政府が主催し、米国、EU、日本、NATO等約30ヶ国・機関が参加
・欧米の通信事業者（AT&T、独テレコム、Vodafone、O2）が特別セッションに参加。
・今後の新たな社会インフラとなる５Ｇのセキュリティ確保に関し、
「政策」、「技術」、「経済」、「セキュリティ、プライバシー及び強靭性」
の観点から議論。
・議長声明「プラハ提案」を成果文書として公表。

＜2019年5月5日　日本経済新聞＞

5G「第三国リスク考慮」

国際会議 ファーウェイ念頭に声明

【ベルリン＝宮下日出男】第5世代（5G）移動通信システム整備をめぐり、日米欧など約30カ国・機関が参加した国際会議が3日までの2日間、チェコの首都プラハで開かれた。通信大手の華為技術（ファーウェイ）などを抱える中国を念頭に5Gの通信網整備では「第三国」がもたらす「リスク」への考慮を促す議長声明を採択した。

国際会議はチェコ政府が主催し、日米のほか、オーストラリアや欧州連合（EU）、北大西洋条約機構（NATO）のセキュリティー担当者らが参加した。中露は参加していない。

議長声明は5Gの通信網整備にあたっては「第三国が事業者に与える全面的なリスクを考慮すべきだ」と提案した。名指しはしていないが、中国当局が華為に影響力を行使し、セキュリティー上の脅威となる事態に警鐘を鳴らした形だ。ただ、提案に拘束力はない。

華為製品をめぐっては、米国が機密漏洩などを警戒し、欧州など同盟諸国に5Gの通信網整備で排除を求めているが、欧州側は整備事業の遅れなどを懸念し、全面排除に慎重だ。このため会議では、5Gのセキュリティー確保に向けた協調的な対応を模索した。

＜2019年5月5日　産経新聞＞

「5G」通信網 防衛で連携

プラハ国際会議閉幕

【プラハ＝佐竹実】プラハで開いた次世代通信規格「5G」に関する国際会議は3日、サイバー攻撃などのリスク回避に向けて各国が連携を深めるとする議長声明を採択し、閉幕した。高速データ通信を可能にする5G通信網は国家の安全保障や国際社会の安定に直結するとして、高度なセキュリティーが必要だと主張した。

会議はチェコ政府が主導し、米国や欧州連合（EU）、日本、北大西洋条約機構（NATO）など約30カ国・機関が参加した。

出席者によると、米AT&Tや英ボーダフォン、独ドイツテレコムなど大手通信会社の代表も議論に加わった。

議長声明は5Gでどの通信機器を採用するかは各国の判断に任せるとするEUの方針を確認した。そのうえで「通信網やサービスは安全性や耐性の高さを念頭に構築されるべきだ」という原則を示した。

米国が安全性を問題視する中国の通信機器最大手、華為技術（ファーウェイ）を名指しで議論することはなかった。米国はファーウェイ製品を5Gのシステムに採用しないよう各国に働きかけているが、EUでは現行の4Gですでに採用している国が少なくなく、5Gでも使用を検討する国もある。「（ファーウェイを）採用した後でも安全性を管理する方法について話し合うことができる」（外交筋）との声もあった。

米政府関係者は3日、日本経済新聞の取材に「今回の会議は前向きな課題にどう取り組むかという内容で、満足している」と述べた。ファーウェイを一部の国で採用する動きがあることについては「答える立場にない」と語った。

Ⅰ．サイバーセキュリティ リスクの深刻化

Ⅱ．5G／IoT化の急速な進展

Ⅲ．サイバーセキュリティ戦略

Ⅳ．IoTセキュリティ総合対策

Ⅴ．国家安全保障戦略

サイバー空間と国際法の適用関係（国連GGE、2015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)

米国政府における攻撃元(Attribution)の特定

サイバー抑止戦略(Report on Cyber Deterrence Policy, White House, Dec. 2015)

1) 否定による抑止(Deterrence by denial)

2) コストを課すことによる抑止(Deterrence through cost imposition)

(注)各種報道に基づき作成。

事案	攻撃発生時期	攻撃国	概要	米国政府の対応
大手企業からの機密情報窃盗	2006年～2014年	中国	人民解放軍のサイバー攻撃部隊が米国の原子力発電、鉄鋼などの大手企業のシステムに侵入し、技術や設計の機密情報を盗んだ。	2014年5月19日司法長官が記者会見において、起訴罪状を公表。中国人民解放軍のサイバー部隊である「第61398部隊」の将校ら5人を起訴。
ソニー・ピクチャーズへのサイバー攻撃	2014年11月	北朝鮮	「平和の守護神」と名乗るグループがソニー・ピクチャーズ・エンターテイメント社のコンピュータシステムを攻撃し、個人情報や未公開映画等のデータを盗んだ。	2014年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日追加的な経済制裁を実施。
銀行等、ダムへのサイバー攻撃	2011年～2013年	イラン	イラン政府の命を受けたイランのセキュリティ企業社員が米国金融機関46社にDDoS攻撃を仕掛け、またニューヨークのダム制御システムに不正にアクセス。	2016年3月24日司法省が、イラン人7人が起訴されたと発表。
Yahoo.comの情報漏えい	2014年1月～2016年12月	ロシア	2016年9月22日に米ヤフーが5億件の個人情報漏えいを公表。(2017年10月公表の30億件の漏えいとは別件)	2017年3月15日にロシア情報機関の職員等4人を起訴。
WannaCryによるサイバー攻撃	2017 年5月12日	北朝鮮	150か国以上でランサムウェアの被害。英国では病院が感染し、しばらく治療ができなくなる事態に。	2017年12月19日北朝鮮の攻撃として非難。日英豪加ニュージーランドも同様に非難。
NotPetyaによるサイバー攻撃	2017 年6月27日	ロシア	ウクライナを中心に、被害が世界中に拡大。デンマークの海運会社Maerskは最大3億ドルの損失との見通し。	2018年2月15日ロシアが歴史上最も破壊的で損害の大きい攻撃を行ったと発表。英国もロシアの責任と発表。

米国「国家サイバー戦略」（2018年9月）

2018年9月20日、15年ぶりとなる新たな「国家サイバー戦略」を公表。同戦略は、ロシア、北朝鮮、中国等によるサイバー空間を介した活動に触れつつ、新たな脅威と戦略的競争に面しているとの認識の下、サイバーを他の分野から分離したものではなく、国力を構成するあらゆる分野に共通するものと位置づけ、以下の4本柱で構成。

1. 米国民、国土及び米国流の生活様式の保護

- 連邦政府のネットワーク及び情報の保全確保
  - ✓ 情報共有の促進や、正当な理由がある場合のリスクのあるベンダーの製品やサービスの排除等を通じた政府調達におけるサプライチェーンリスク管理
- 重要インフラの保護
  - ✓ （重要インフラ16分野のうち）通信、情報技術を含む7分野に対し、優先的にリスク低減のための取組を実施
  - ✓ 情報通信技術の提供主体（ICT事業者）との連携強化
    - ・情報通信を全てのセクターの基盤として特別に位置づけ
    - ・機密性のある脅威・脆弱性情報等をクリアランス取得ICT事業者と共有

2. 米国の繁栄の促進

- 活力のある強靱なデジタルエコノミーの促進
  - ✓ 連邦政府の購買力を活用し、安全なサプライチェーンへのインセンティブを与えつつ、次世代情報通信インフラの整備を加速化。民間セクタと協力し、5Gの進化とセキュリティを促進

3. 力を通じた平和の維持

- 受け入れられないサイバー空間における活動のアトリビューション及び抑止
  - ✓ 将来の悪質なサイバー活動を抑止するため、（外交、軍事等すべてのツールを利用して）迅速かつ透明性をもって対処

4. 米国の影響力の促進

サプライチェーン・リスク対策の重要性

【サイバーセキュリティ戦略（平成30年7月27日閣議決定）】

4.1.2 (2) サプライチェーンにおけるサイバーセキュリティを確保できる仕組みの構築

サプライチェーン全体としてのサイバーセキュリティを確保するためには、製造される機器、生成されて流通するデータ、それらを利用したサービス等のサプライチェーンの構成要素における信頼の確保が不可欠である。このため、それぞれの構成要素がセキュリティ要件を満たした形で生成・流通されるよう、要件の明確化を図るとともに、その要件が満たされていることを確認等することにより信頼を創出する仕組みの構築が必要である。また、サプライチェーンにおける調達者が機器・サービス等の利用に際し、その信頼を確認できるよう、官民が連携して、信頼性が証明されている機器・サービス等のリストの作成と管理を行う仕組みの構築が必要である。さらに、これらがサプライチェーンのつながりにおいて、連続的な仕組みとなるよう、トレーサビリティを確認するための仕組みと、創出された信頼そのものに対する攻撃を検知・防御するための仕組みを検討する。

4.2.3 政府機関等におけるセキュリティ強化・充実

（略）

複雑化・巧妙化しているサイバー攻撃に対しては、引き続き攻撃を前提とした多層防御や、サプライチェーンリスクへの対応を強化するとともに、新たな技術を活用し、従来の攻撃側優位の状況を改善するための取組を進めることが求められる。

（略）

4.4.2 (1) 実践的な研究開発の推進

（略）

特に、サプライチェーンにおける価値創出のプロセスにおける信頼の創出や証明、トレーサビリティの確保とこれらに対する攻撃の検知・防御に関する研究開発を進めるほか、機器に組み込まれた不正なハードウェアやソフトウェアを効率的に検出する技術開発、プラットフォームにおいて利用者の意図しない動作を生じさせるおそれがあるときにもデータや情報の真正性・可用性・機密性を確保するための研究開発を行う。

（略）

IT調達における「サプライチェーン・リスク対策」の遵守事項

【政府機関等の対策基準策定のためのガイドライン（平成30年度版）（平成30年7月25日）】

4.1.1 外部委託

遵守事項
(2) 外部委託に係る契約
(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めること。
(ウ) 委託事業の実施に当たり、委託先企業若しくはその従業員、再委託先又はその他の者によって、機関等の意図せざる変更が加えられないための管理体制

5.1.2 機器等の調達に係る規定の整備

遵守事項
(1) 機器等の調達に係る規定の整備
(a) 統括情報セキュリティ責任者は、機器等の選定基準を整備すること。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を機関等が確認できることを加えること。

IT調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ＜概要＞

（平成30年12月10日 関係省庁申合せ）

１．適用対象

各省庁等において下記に該当すると思われる情報システム等のうち、ＮＩＳＣ・ＩＴ室と協議のうえ、対象としたもの。

① 国家安全保障及び治安関係の業務を行うシステム

② 機密性の高い情報を取り扱うシステム並びに情報の漏洩及び情報の改ざんによる社会的・経済的混乱を招くおそれのある情報を取り扱うシステム

③ 番号制度関係の業務を行うシステム等、個人情報を極めて大量に取り扱う業務を行うシステム

④ 機能停止等の場合、各省庁における業務遂行に著しい影響を及ぼす基幹業務システム、LAN等の基盤システム

⑤ 運営経費が極めて大きいシステム

２．適用時期

平成31年度予算に基づき平成31年４月１日以降に調達手続（公告等）が開始されるもの

３．調達手続の流れ

「総合評価落札方式」や「企画競争」等を用い、RFIやRFPといった事前の情報取得や、審査の過程において、必要な情報を入手し評価することにより、サプライチェーン・リスク対策を実施。

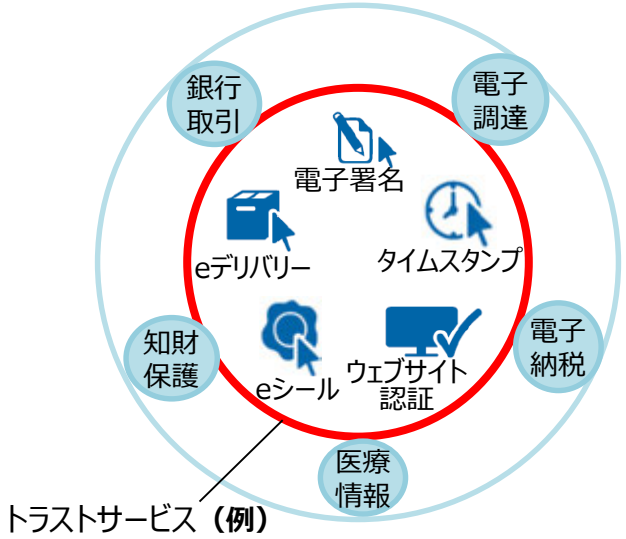
４．ＮＩＳＣ・ＩＴ室の助言

調達する情報システム等の構成品候補について、「製造業者」「機種」等の情報を事前に受けることで、「サプライチェーン・リスクに係る懸念が払拭できない」か否か、助言を行う。

トラストサービスの動向と制度化の意義

- Society5.0の実現に向けて、サイバー空間と実空間の一体化が加速的に進展し、実空間での様々な活動がサイバー空間に置き換わる中、その有効性を担保する基盤として、ネット利用者の本人確認やデータの改ざん防止等の仕組みであるトラストサービスが必要。
- EUでは、電子取引における確実性を確保し、市民、企業の経済活動の効率化を促進するため、2016年７月にeIDAS（electronic Identification and Authentication Services）規則を発効し、トラストサービスに関して包括的に規定。

EUにおけるトラストサービスのイメージ



電子署名

○ 自然人が電磁的に記録した情報について、その自然人が作成したことを示すもの。

タイムスタンプ

○ 電子データが、ある時刻に存在していたこととその時刻以降に改ざんされていないことを示すもの。

ウェブサイト認証

○ ウェブサイトが真正で正当な主体により管理されていることが保証できることを示すもの。

eシール

○ 文書の起源と完全性の確実性を保証し、電子文書等が法人によって発行されたことを示すもの。

eデリバリー

○ データの送受信の証明も含め、データ送信の取扱いに関する証拠を提供するもの。

検討の必要性

ネットワークにつながる人・組織・モノの認証やネットワーク上を流れるデータの完全性の確保等を実現するための我が国のトラストサービスの在り方について、EUにおけるeIDAS規則の制定等の動きも踏まえつつ、**国際的なサービスの進展を視野に入れた相互運用性の確保の観点からも、包括的な検討を行う**。

最後に、・・・貴社のCIAは大丈夫？

情報の機密性（Confidentiality）

- ○　不正アクセス（情報の窃取、漏洩）
- ○　標的型攻撃、フィッシング攻撃

セキュリティといえば、「機密性」にのみ目が行きがち。
これは重要だが、「完全性」及び「可用性」も同様に重要。

情報の完全性（Integrity）

- ○　不正アクセス（ホームページ改竄）
- ○　制御システムの破壊

情報の可用性（Availability）

- ○　DDoS攻撃
- ○　ランサムウェア
  （データ暗号化し身代金を要求。）

2019年2月より、サイバー攻撃に悪用されるおそれのあるIoT機器の調査、注意喚起を行うプロジェクト「NOTICE」※1を実施します。

セキュリティ対策が必要なIoT機器のユーザには、ご契約のインターネットプロバイダからパスワード設定変更などの注意喚起を行います。また、NOTICEサポートセンターにおいて、必要なセキュリティ対策をご案内します。※2

※1：総務省、国立研究開発法人情報通信研究機構（NICT）、インターネットプロバイダが連携して実施するプロジェクトです。
※2：インターネットプロバイダからの注意喚起や、NOTICEサポートセンターでの案内にあたり、費用の請求や、設定しているパスワードを聞き出すことは絶対にありません。

総務省
Ministry of Internal Affairs and Communications

■お問い合せ NOTICEサポートセンター
TEL:0120-769-318（無料・固定電話のみ） 03-4346-3318（有料）
IoTセキュリティ 検索
さらに詳しい情報はWEBでも公開中 https://notice.go.jp