資料16－1

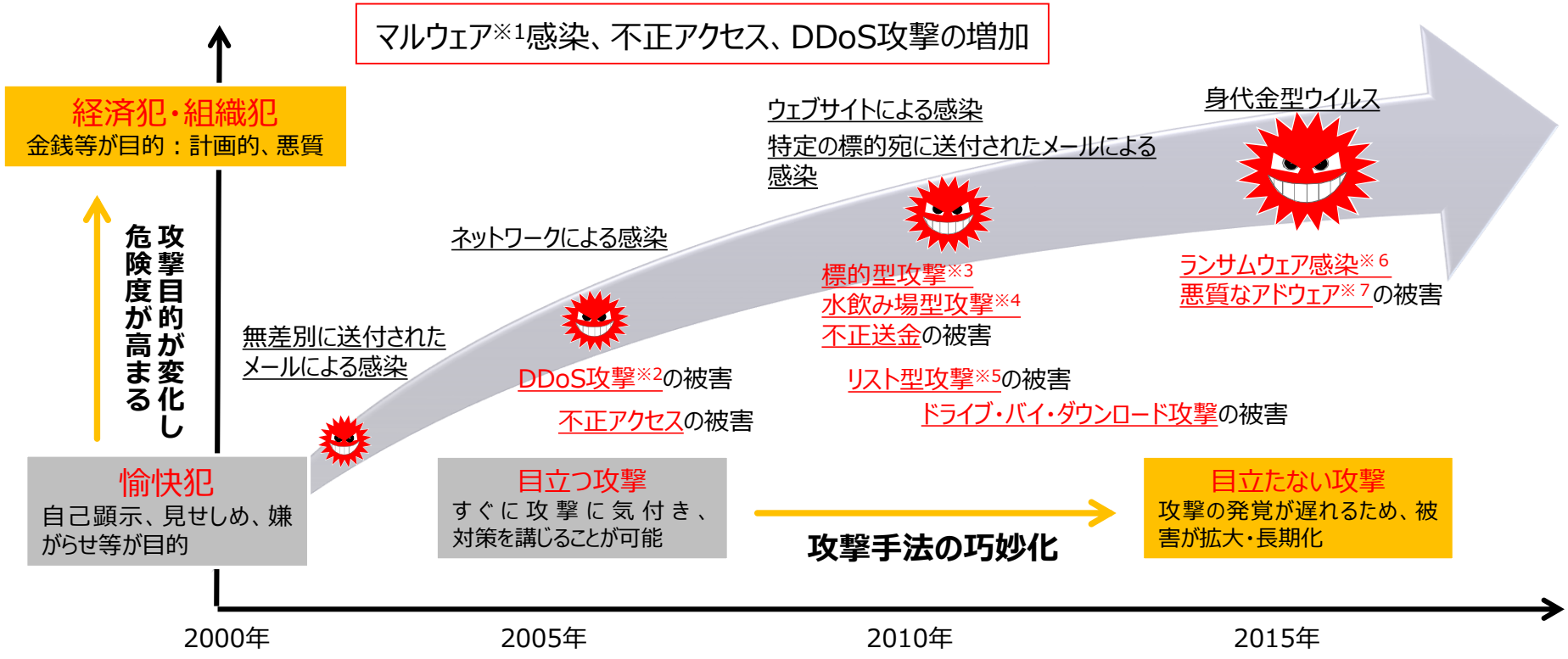
今後の検討課題等について

サイバーセキュリティタスクフォース事務局

令和元年 11月1日

サイバーセキュリティ上の脅威の増大

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



※1 マルウェア(Malware)　Malicious softwareの短縮語。コンピュータウイルスのような有害なソフトウェアの総称。

※2 DDoS攻撃　分散型サービス妨害攻撃（Distributed Denial of Service）のこと。多数の端末から一斉に大量のデータを特定宛先に送りつけ、宛先のサーバ等を動作不能にする攻撃。

※3 標的型攻撃　機密情報等の窃取を目的として、特定の個人や組織を標的として行われる攻撃。

※4 水飲み場型攻撃　標的組織が頻繁に閲覧するウェブサイトで待ち受け、標的組織に限定してマルウェアに感染させ、機密情報等を窃取する攻撃。

※5 リスト型攻撃　不正に入手した他者のID・パスワードをリストのように用いてWebサービスにログインを試み、個人情報の窃取等を行う攻撃。

※6 ランサムウェア(Ransomware)　身代金要求型ウイルスのこと。感染端末上にある文書などのファイルが暗号化され、暗号解除のためには金銭を要求される。

※7 アドウェア(Adware)　広告表示によって収入を得るソフトウエアの総称。狭義には、フリーウエアと共にインストールされ、ブラウザー利用時に広告を自動的に付加するソフト

昨今のサイバー攻撃の事例

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、年金加入者の情報約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（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暗号資産（仮想通貨）が外部へ送信され、顧客資産が流出（不正アクセス）

海外事例

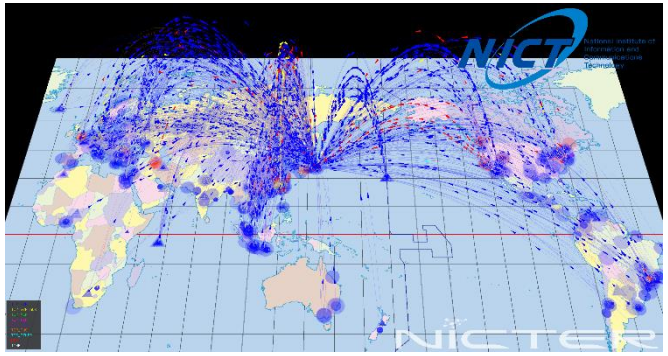
2015年４月	**フランスのテレビネットワーク TV５ Monde がサイバー攻撃を受け、放送が一時中断（標的型攻撃）**
2015年６月	米国の人事管理局（OPM）が不正にアクセスされ、政府職員の個人情報が流出（不正アクセス）
2015年12月	**ウクライナの電力会社のシステムがマルウェアに感染し、停電が発生（標的型攻撃）**
2016年10月	米国のDyn社のDNSサーバが大規模なDDoS攻撃を受け、同社のDNSサービスの提供を受けていた企業のサービスにアクセスしにくくなる等の障害が発生（DDoS攻撃）
2017年５月	**世界各国（アメリカ、イギリス、中国、ロシア等）でWannaCry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（ランサムウェア）**
2017年10月	米Yahoo社で約30億件の個人情報が流出していたことが判明（不正アクセス）
2019年９月	**エクアドルで国民ほぼ全員を含む約2000万人分の個人情報が海外に流出（不正アクセス）**

出典：各種公開資料等より総務省作成

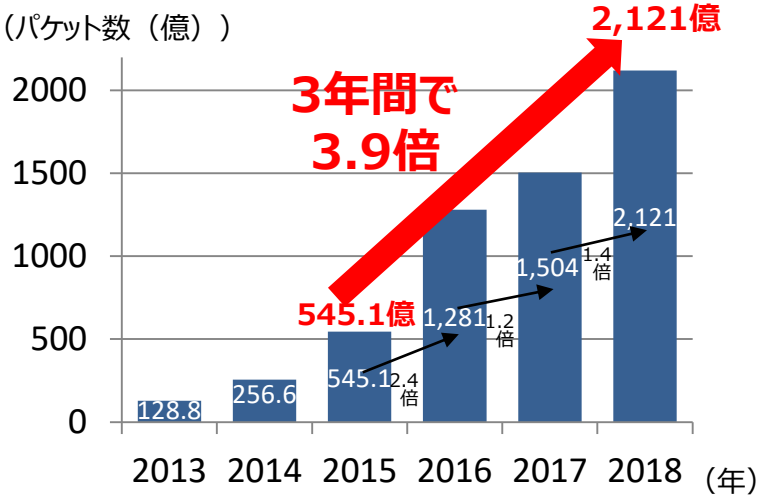
IoT機器を狙った攻撃

■ IoT機器を狙った攻撃は依然として多い。

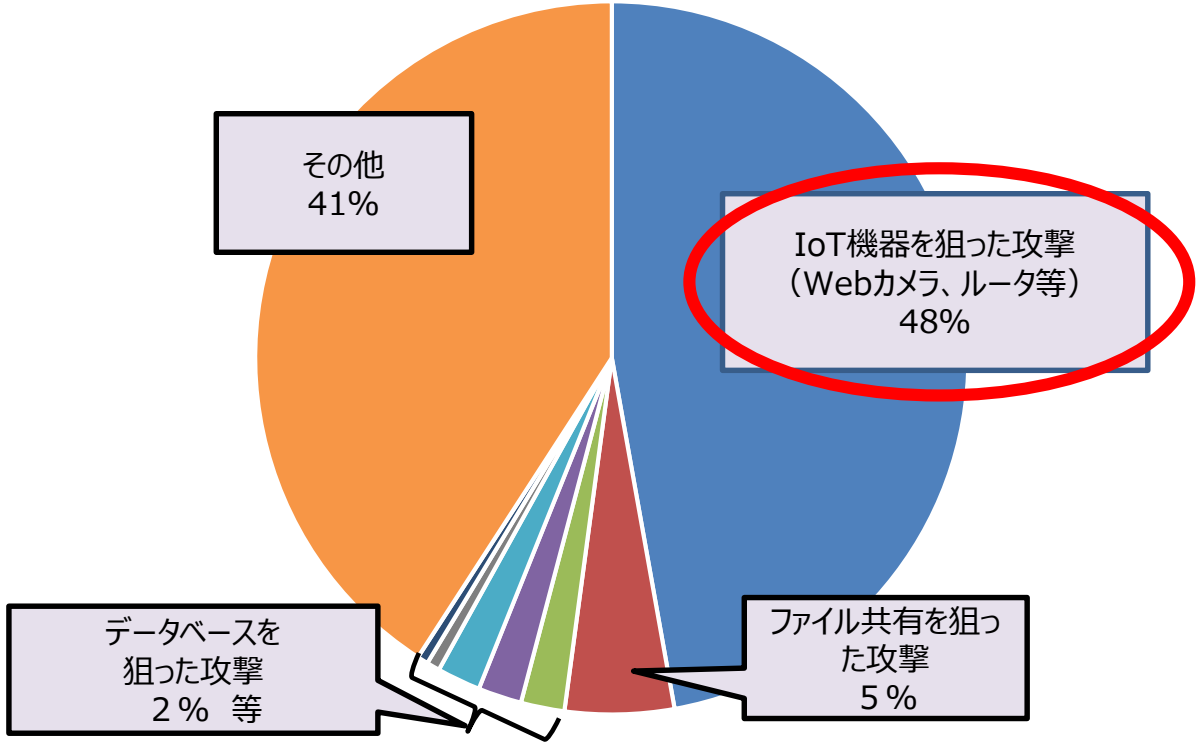
NICTERにより観測されるサイバー攻撃の様子



NICTER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



（注１）　NICTERで観測されたパケットのうち、サービスの種類（ポート番号）ごとに割合の多い上位から30位までを分析したもの。

（注２）　IoT機器を狙った攻撃は多様化しており、ポート番号だけでは分類しにくいものなど、「その他」に含まれているものもある。

IoT機器調査及び利用者への注意喚起結果（2019年9月まで）

■ 2019年９月までに調査のための手続が完了しているインターネット・サービス・プロバイダ（ISP）34社に係る約1.0億IPアドレスに対して調査を実施。

【NOTICEの取組結果】

ID・パスワードが入力可能であったもの → 約98,000件（直近での調査）【６月時点：約42,000件】

上記の内、ID・パスワードによりログインでき、注意喚起の対象となったもの → 延べ505件【６月時点：延べ147件】

【マルウェアに感染しているIoT機器の利用者への注意喚起の取組結果】

ISPに対する通知の対象となったもの → 80～559件（１日当たり）【６月時点：112～155件】

（参加ISP：計34社）

株式会社秋田ケーブルテレビ
イッツ・コミュニケーションズ株式会社
株式会社NTTドコモ
株式会社QTnet
ケーブルテレビ株式会社
山陰ケーブルビジョン株式会社
株式会社ZTV
株式会社TOKAIケーブルネットワーク
株式会社ベイ・コミュニケーションズ
株式会社朝日ネット
株式会社インターネットイニシアティブ
株式会社愛媛CATV
近鉄ケーブルネットワーク株式会社
株式会社ケーブルテレビ品川
株式会社シー・ティー・ワイ
ソニーネットワークコミュニケーションズ株式会社
ニフティ株式会社
アルテリア・ネットワークス株式会社
エヌ・ティ・ティ・コミュニケーションズ株式会社
株式会社オプテージ
KDDI株式会社
株式会社ケーブルネット鈴鹿
株式会社ジュピターテレコム（グループ会社計10社）
ソフトバンク株式会社
ビッグローブ株式会社

第5世代移動通信システム（5G）について

■ 第5世代移動通信システム（5G）は、超高速、超低遅延、多数同時接続を実現する新たな社会インフラとして期待されている一方、そのセキュリティの在り方についても今後検討していくことが必要。

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

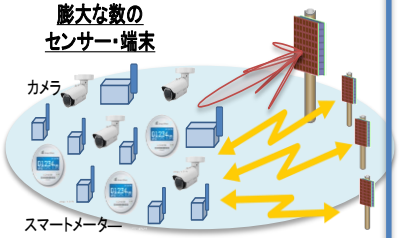
利用者が遅延（タイムラグ）を意識することなく、リアルタイムに遠隔地のロボット等を操作・制御

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）

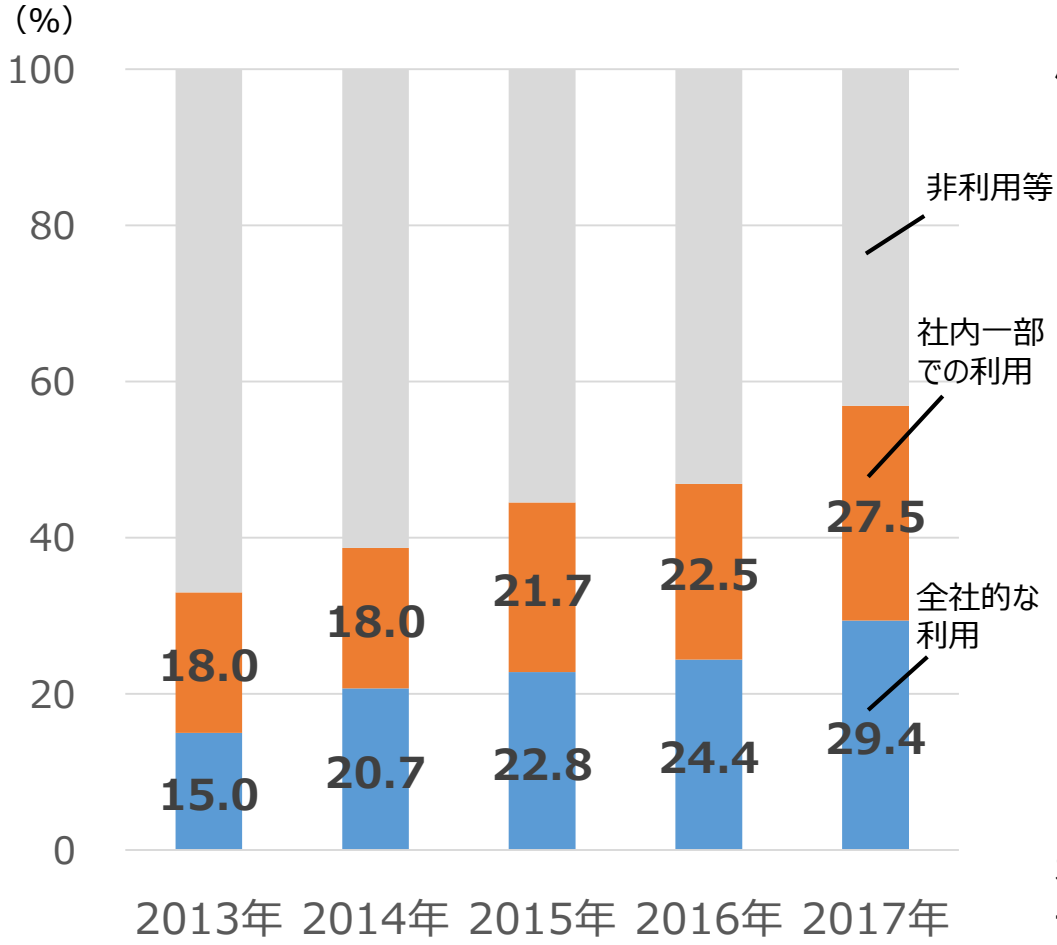
社会的なインパクト大

新たな社会インフラへ

クラウドサービスの利用の拡大とセキュリティ

■ 民間企業におけるクラウドサービスの利用率は年々拡大している一方で、サービスの可用性の確保といったセキュリティ対策の重要性が増している。

クラウドサービスの利用状況



出典：平成30年版　情報通信白書

クラウドサービスの停止事故

例）Amazon Web Service（AWS）における障害（2019年8月）

- AWSの東京リージョンの１つのアベイラビリティゾーン（AZ）において、空調設備の管理システムの障害が原因でサービス障害が発生。
- 原因はサードパーティ製の制御システムにおけるバグとフェイルセーフとして用意されていたパージモードの動作不良。
- 最終的な回復まで７～８時間を要し、同サービスを利用していた、決済、SNS、社内システム、ニュース・メディア、バイクシェアなど広範囲にわたる様々なサービス（※）が一時的に停止した。

社会全体にクラウドサービスが普及するにつれ、クラウドサービスの可用性を含むセキュリティの確保が重要な課題となっている。

公衆無線LANの利用者数の増大

- 公衆無線LANサービスの2018年度（平成30年度）の利用者数は、前年比で14%増の5,746万人（※）との推計結果。
- スマートフォンのパケット料金を抑えるために低価格・小容量のプランを選択するユーザーが増えた結果公衆無線LANサービスの利用ニーズが高まっていることが増加の要因と考えられる。

（※）内訳は、個人利用者 3,793万人、ビジネス利用者 451万人、訪日外国人利用者 1,502万人。

＊日本在住の個人・ビジネス利用者は各年度末（3月末時点）の利用者数。2018年度以降は予測値。

＊日本在住の個人・ビジネス利用者の定義は1か月に1回以上利用するアクティブユーザー。

＊訪日外国人利用者の定義は訪日時に1回以上利用したユーザーの年間合計数。

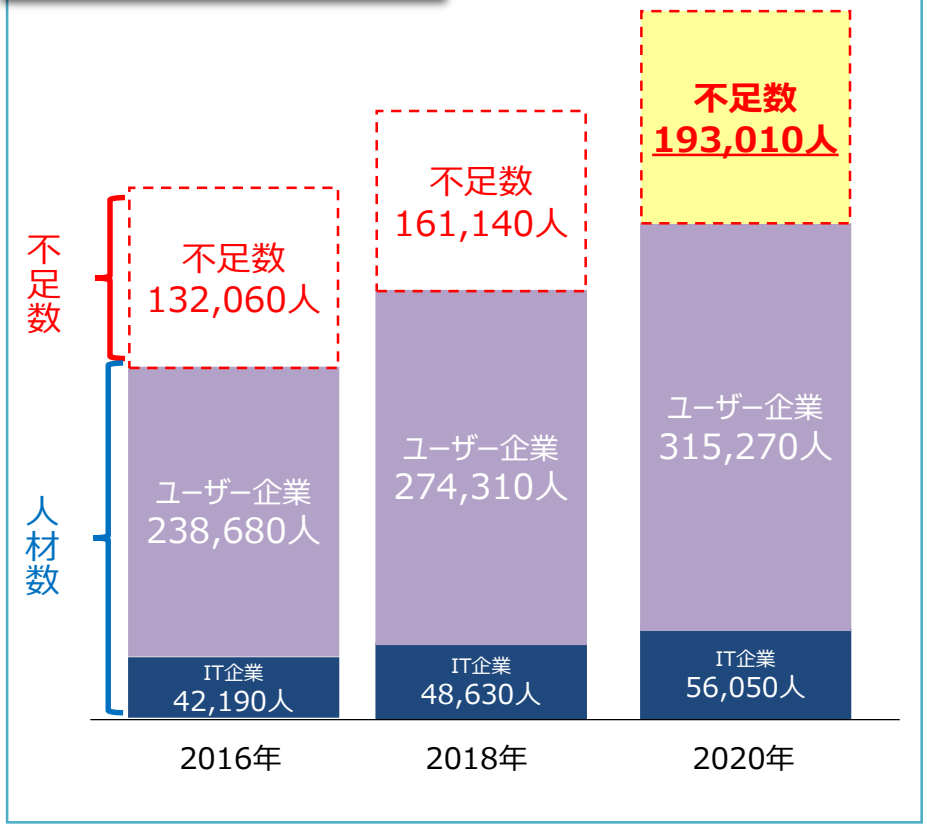
出典：株式会社ICT総研「2018年 公衆無線LANサービス利用者動向調査」

公衆無線LANの利用者が増大するにつれ、そのセキュリティについても適切に確保される必要がある。

セキュリティ人材の不足

■2016年時点で情報セキュリティ人材が13.2万人不足と推計。2020年には、不足数が19.3万人に増加するとも見込まれている。
■中小企業（従業員数５人～99人、100人～299人）では、2016年時点で最大15.6万人不足と推計。

情報セキュリティ人材の不足数推計



うち中小企業

従業員数	業種	セキュリティ人材不足数（専任者のみ）（人）
5～99 人	製造業	18,113.2
	サービス業	67,120.4
	その他	18,795.1
100～299 人	製造業	11,778.5
	サービス業	34,707.6
	その他	6,018.6
	計	156,533.4

※不足数を全て専任者で補う場合のシナリオ

従業員数	業種	セキュリティ人材不足数（専任者のみ）（人）
5～99 人	製造業	1,723.7
	サービス業	6,474.2
	その他	2,022.5
100～299 人	製造業	2,098.3
	サービス業	6,733.2
	その他	1,369.8
	計	20,421.7

※不足数を専任者と兼任者で補う場合のシナリオ

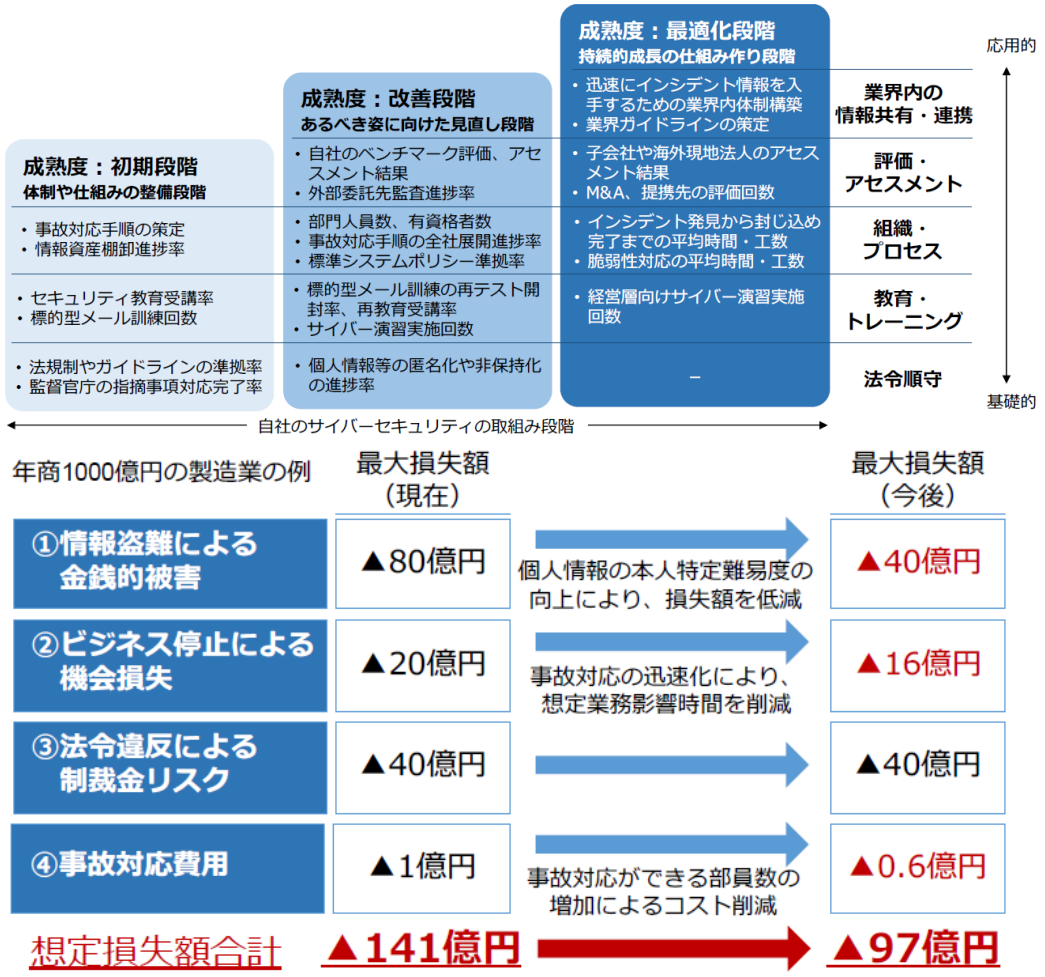
出典：経済産業省「IT人材の最新動向と将来推計に関する調査結果」（平成28年６月）及びみずほ情報総研「ITベンチャー等によるイノベーション促進のための人材育成・確保モデル事業　事業報告書 第２部 今後のIT人材需給推計モデル構築等 編」（平成28年３月）をもとに総務省作成
http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf
http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_fullreport.pdf

サイバーセキュリティの経済効果

- 企業は、サイバーセキュリティに関し、自組織の成熟度に応じた適切なKPIを設定して達成を図ることにより、セキュリティ事故が発生した場合の想定損失額の軽減などを実現できる可能性がある。
- そのためには、取締役・経営層がサイバーセキュリティの重要性を認識し、相応の態勢を築くことが必要である。

- （一社）日本サイバーセキュリティ・イノベーション委員会（JCIC）が作成した「サイバーセキュリティのKPIモデル（試論）」は、企業のセキュリティ事故による損失額を軽減し、デジタル技術を活用したイノベーションを推進するため、策定されている。

- KPI モデルから、自組織の成熟度に応じたKPIを選択し、当期の目標とする。右図の例では、①本人特定の難化、②事故対応の迅速化などのKPI 達成により、セキュリティ事故が発生した場合の想定損失額を97億円まで軽減できることを示している。



出典：2019年４月　損失額を減らすための「サイバーセキュリティのKPIモデル（試論）」（（一社）サイバーセキュリティ・イノベーション委員会）より

IoT・5Gセキュリティ総合対策について

■ IoT・5G時代にふさわしいサイバーセキュリティ対策の在り方について検討し、総務省として取り組むべき課題を「IoT・5Gセキュリティ総合対策」として、令和元年8月に公表（※）。【⇒参考資料2参照】

■ サイバーセキュリティの変化の速さを踏まえ、取り組むべき施策についてさらなる検討が必要。

● 直近で留意すべき事項

1 5Gのサービス開始に伴う新たなリスク
- ✓ 仮想化、ソフトウェア化、モバイルエッジコンピューティング
- ✓ 産業用途でのIoT機器の設置・運用

2 サプライチェーンリスクの管理の重要性
- ✓ ICTの製品・サービスの製造・流通過程でのリスク
- ✓ 委託先が踏み台となって攻撃を受けるケース

3 Society5.0の実現に向けたデータの流通・管理の重要性
- ✓ クラウドサービスやスマートシティなどのセキュリティの確保の重要性
- ✓ トラストサービスの必要性

4 サイバーセキュリティにおけるAI利活用の重要性
- ✓ AIの活用が進展する中で、特にAIを利活用したサイバーセキュリティ対策を促進することが必要

5 大規模な量子コンピュータの実用化の可能性
- ✓ 将来の大規模な量子コンピュータの実用化の可能性を踏まえ、現時点から新たな推奨暗号の在り方について検討の必要性

6 大規模な国際イベント等の開催
- ✓ ラグビーワールドカップや東京オリンピック・パラリンピック大会の円滑な実施、及びその後も見据え、対策の着実な実施が必要

● IoT・5Gセキュリティ総合対策の枠組み

総務省として重点的に対応すべき情報通信サービス・ネットワークの個別分野等に関する具体的施策

✓ ①IoT、②5G、③クラウドサービス、④スマートシティ、⑤トラストサービス、⑥公衆Wi-Fi、⑦重要インフラ、⑧地域

具体的施策間でも連携

連携 ↕ 連携 ↕ 連携 ↕ 連携 ↓

研究開発	人材育成 普及啓発	情報共有 情報開示	国際連携
✓ ハードウェア脆弱性 ✓ AI ✓ 暗号 など	✓ 2020東京大会向け人材育成 ✓ 地域の人材育成 など	✓ 情報共有基盤 ✓ 情報開示の促進 など	✓ ASEAN各国との連携 ✓ 国際標準化 など

（※）これに先立ち、2017年（平成29年）には、IoT機器・システムのセキュリティ等の確保を主眼においた「IoTセキュリティ総合対策」を策定・公表

今後の検討課題（例）

■ 検討の枠組みとして、「IoT・5Gセキュリティ総合対策」の基本的な柱立ては前提としつつも、例えば、以下のような論点について今後議論が必要ではないか。

※太字はIoT・5Gセキュリティ総合対策の関連する項目

【IoTのセキュリティ対策】

- 重要インフラ事業者が設置するIoT機器のセキュリティの確保に向けて取り組むべき事項はないか？

【公衆無線LANのセキュリティ対策】

- Wi-Fiの安全な利用のための周知を徹底する必要はないか？

【重要インフラとしての情報通信分野のセキュリティ対策】

- 重要インフラ事業者等のサイバーセキュリティ対策などは実効的に行われているのか？

【人材育成・普及啓発の推進】

- 地方公共団体や重要インフラ事業者等の人材育成を強化する必要はないか？

【情報共有・情報開示の促進】

- サイバーセキュリティの質の向上のための情報共有に関し、実効的な体制が構築・運営されているか？

e.t.c.

本日以降に構成員の皆様に頂いた御意見やコメントなどを踏まえながら、第17回以降の検討課題を設定し、「IoT・5Gセキュリティ総合対策」の改定も見据えつつ、議論を進めていただくことでどうか。

当面の想定スケジュール（案）

■　５月を目途に取りまとめ・公表をしていただくことを想定。