（案）

サイバーセキュリティ意識・行動強化プログラム

～「参加・連携・協働」の実現を目指して～

201〇月〇月〇日

サイバーセキュリティ戦略本部

目次

1　はじめに

2018 年７月に、サイバーセキュリティに関する今後３年間の諸施策の目標及び実施方針を国内外に示すための、新たな「サイバーセキュリティ戦略」が閣議決定された。同戦略においては、「サービス提供者の任務保障」、「リスクマネジメント」、「参加・連携・協働」の３つの観点から、サイバーセキュリティに関する官民の取組を推進することとし、信頼できるサイバー空間が自律的・持続的に進化・発展する「サイバーセキュリティエコシステム」を目指すこととされた。

とりわけ「参加・連携・協働」の観点については、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、個人や組織各々が平時から基本的な取組を講じていくことの重要性を提示するとともに、有用な情報の共有や相互の連携・協働を、サイバー空間における新たな公衆衛生活動と捉え、基本的な取組と位置付けた。

こうした点を踏まえ、産学官民の関係者が円滑かつ効果的に活動し、有機的に連携できるよう、同戦略においては、サイバーセキュリティの普及啓発に向けた総合的な戦略及びアクションプランを策定することされている。今回、2020 年の東京オリンピック・パラリンピックも見据えつつ、関係者の密接な連携を強化していくため、本プログラムを策定するものである。

2　現状

（1）インターネットの利用及びサイバーセキュリティ対策の状況

AI の進化に伴う幅広い産業での情報通信技術の活用や、IoT 機器で得られるデータを利活用した新たなビジネスの登場など、サイバー空間における新たな技術・サービスの活用が急速に拡大しており、社会に多くの恩恵をもたらすことが期待されている。このようにサイバー空間と実空間の一体化が進む中、これらの技術・サービスを制御できなくなるおそれは常に内在しており、サイバー空間での脅威によって多大な経済的・社会的損失が生じる可能性が急速に拡大している。

このような状況を踏まえ、本節では、インターネットの利用及びサイバーセキュリティ対策に関する個人や企業の状況を示す。

① 個人の状況

近年、スマートフォンの普及が進んでおり、2010 年から 2017 年にかけて、世帯保有率は 7.7 倍と急増している[1]。特に、10 代～40 代は、インターネットへ接続する端末として、スマートフォンを用いる場合が最も多い状況となっている[2]。IoT デバイスも、増加傾向にあり、2020 年には約 400 億個に拡大する見通しであり、白物・デジタル家電などコンシューマー向けのデバイス数についても、２倍以上に増加するとの予測がされている[3]。

サイバー空間におけるサービスの活用も拡大している。例えば、Fintech では従来の金融サービスの各分野において様々なサービスが登場[4]し、堅調に拡大を続けている[5]。また、インターネット利用者に占めるソーシャルネットワーキングサービス（SNS）の利用割合は、ほぼ全ての世代で拡大の傾向となっている。特に、

---

[1] 「平成29年通信利用動向調査」（2018年５月　総務省）国内における情報通信機器の保有状況推移より（参考１）

[2] 「平成30年版情報通信白書」（2018年７月　総務省）インターネット接続端末（世帯）より（参考２）

[3] 「平成30年版情報通信白書」（2018年７月　総務省）世界のIoTデバイス数の推移及び予測より（参考３）

[4] 「ICTによるイノベーションと新たなエコノミー形成に関する調査研究」（2018年３月　総務省）代表的なFinTechサービスの例より（参考４）

[5] 「ICTによるイノベーションと新たなエコノミー形成に関する調査研究」（2018年３月　総務省）電子マネー決済額より（参考５）

中学生～30 代の範囲では約７割、小学生についても約２割が利用している[6]。

このように、サイバー空間におけるサービスの利用が拡大する中、国民のサイバー空間に対する不安感も拡大を続けており、不安を感じる場所や犯罪として、インターネット空間やインターネットを利用した犯罪が最も多く挙げられている[7]ほか、図１のとおり、インターネットの利用に関連するトラブルに不安を感じる人も７割近くおり、増加傾向にある。

このような状況に対し、図２のとおり、個人がセキュリティ対策を実施する割合は着実に増加しているものの、セキュリティパッチの適用、セキュリティサービスソフトの導入、不審な電子メールの添付ファイルを開かないことや怪しいと思われるウェブサイトにはアクセスしないなどの基本的な対策を行う割合は４割～６割台に留まっているほか、対策を行っていても十分かどうか分からないと考えている人も多い[8]。さらに、公衆無線 LAN の利用に関しては、脅威の認知率及びセキュリティ対策の実施率については、いずれも訪日外国人の方が日本人に比べて高いといった状況も見られる[9]。このように、不安感の拡大が、必ずしも個人レベルでの具体的な対策の実施に十分に結びついていない状況が伺える。

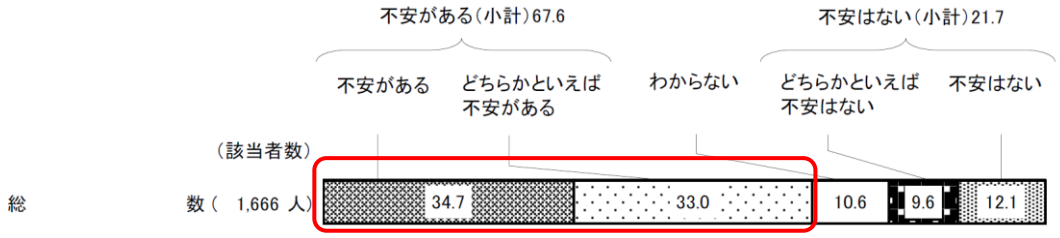
---

[6] 「平成29年版通信利用動向調査」（2018年５月　総務省）ソーシャルネットワーキングサービスの利用状況より（参考６）

[7] 「治安に関する世論調査」（2017年11月　内閣府）不安を感じる場所、不安を感じる犯罪より（参考７）

[8] 「インターネットの安全・安心に関する世論調査」（2018年11月　内閣府）インターネットを安全・安心に利用するための対策より（参考８）

[9] 「公衆無線LANセキュリティ分科会報告書」（2018年３月　総務省）利用者における公衆無線LANのセキュリティに関する意識、公衆無線LAN利用時の脅威の認知率とセキュリティ対策の実施率より（参考９）



（参考）インターネット利用に対する不安感

	該当者数	不安がある（小計）	不安がある	どちらかといえば不安がある	不安はない（小計）	どちらかといえば不安はない	不安はない	わからない
	人	%	%	%	%	%	%	%
平成19年11月調査	3,006	45.4	19.6	25.8	36.3	11.1	25.2	18.3
平成27年7月調査	1,722	56.4	28.0	28.3	36.0	13.6	22.4	7.6

※「あなたは、インターネットを利用することについて不安はありますか。それとも、不安はありませんか。この中から1つだけお答えください。」と聞いている。

図１　インターネットの利用に関連するトラブルへの不安感[10]

（出典：インターネットの安全・安心に関する世論調査（平成 30 年 11 月　内閣府））

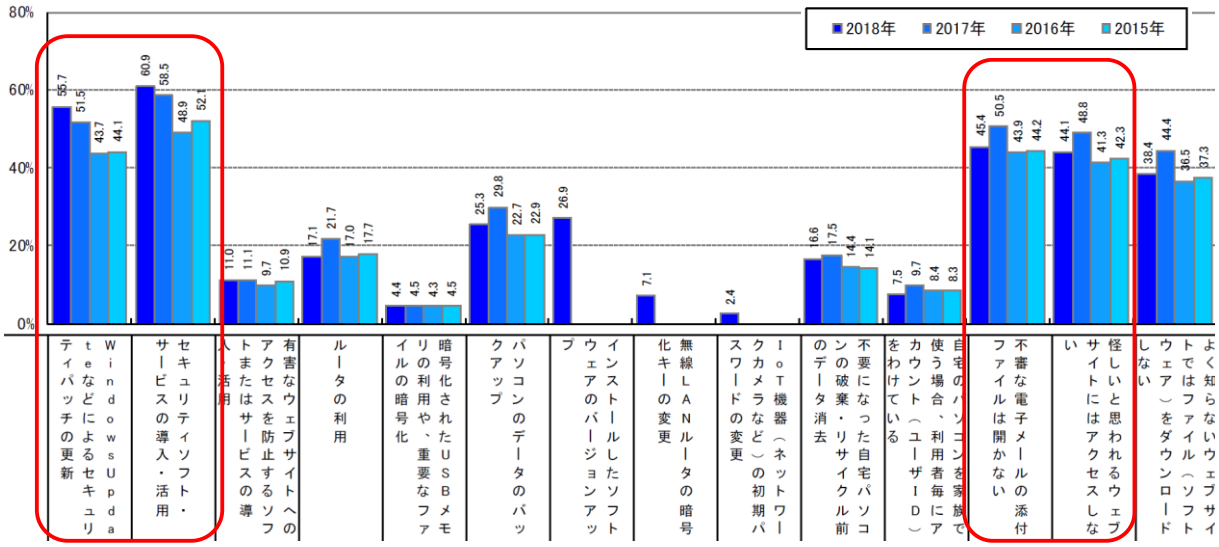


図２　セキュリティ対策の実施状況

（出典：2018 年度情報セキュリティの脅威に対する意識調査

（平成 30 年 12 月　独立行政法人情報処理推進機構（IPA））

[10] 「不安感がある（小計）」と回答した割合は、平成19年11月調査では45.4%、平成27年7月調査では56.4%となっている。

② 企業の状況

まず、図３のように企業の売上規模別でみると、売上の高い企業ほど、経営幹部のセキュリティへの関与の度合いが高い状況となっている。業種別では、金融業が最も関与の度合いが高く、約８割の企業でセキュリティの重要性が経営会議等で審議・報告されているほか、従業員に対するセキュリティ教育にも注力しているが、業種間で取組にばらつきが見られる状況である[11]。

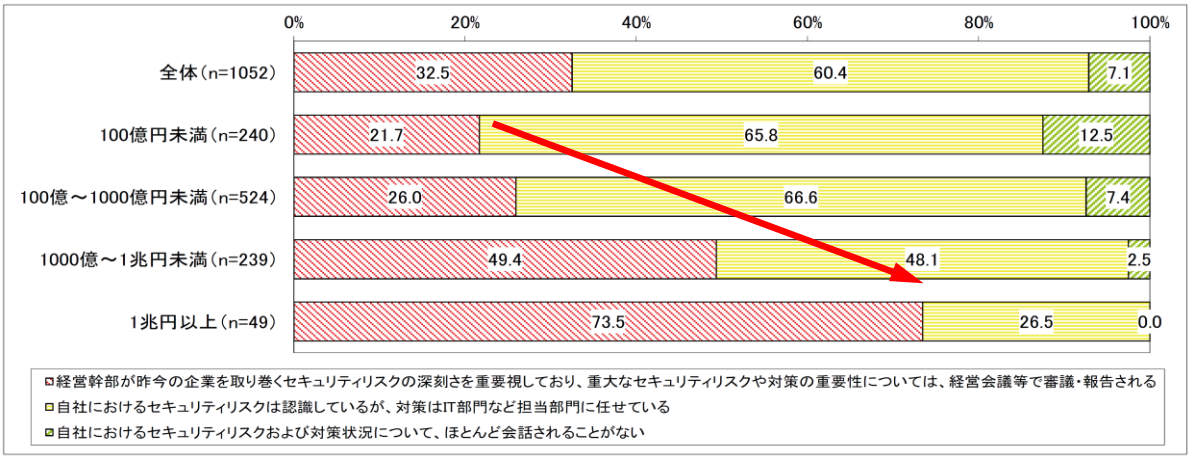


図３　経営幹部の情報セキュリティへの関与度合い（売上高別）

（出典：企業 IT 動向調査報告書 2016（2018 年４月　一般社団法人日本情報システム・ユーザー協会）

また、中小企業では、特に規模の小さい企業ほど、情報漏えい等への対応方法が規定されていない状況である[12]。加えて、図４のとおり、サイバーセキュリティに関する専門部署や担当者が置かれていない場合も多い。社内でのサイバーセキュリティ教育についても、「特に実施していない」との企業が全体の約６割を占めている[13]。

[11] 「企業IT動向調査報告書2018」（2018年４月　一般社団法人日本情報システム・ユーザー協会）業種グループ別経営幹部の情報セキュリティへの関与度合いより（参考10）
[12] 「2016年度中小企業における情報セキュリティ対策の実態調査報告書」（2017年８月　IPA）情報漏えい等の対応方法（企業規模別）より（参考11）
[13] 「2016年度中小企業における情報セキュリティ対策の実態調査報告書」（2017年８月　IPA）情報セキュリティ教育（企業規模別）より（参考12）

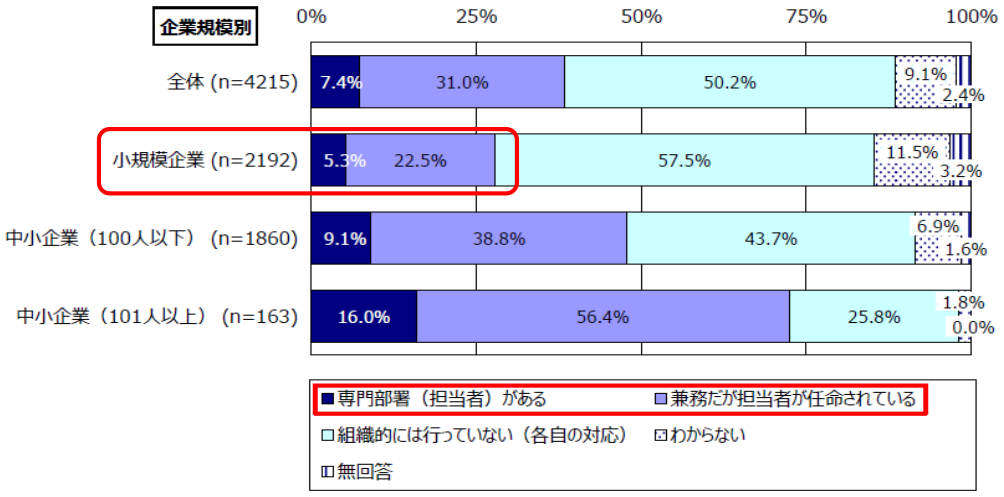


図４　情報セキュリティに係る専門部署または担当者の有無

（出典：2016 年度中小企業における情報セキュリティ対策の実態調査報告書（2017 年８月　IPA））

このような状況において、企業におけるサイバーセキュリティに関する取組の強化や、社内での教育の充実が求められているが、最近では、日本経済団体連合会が、平成 30 年３月に「経団連サイバーセキュリティ経営宣言」を公表している[14]ほか、経営層を対象としたトップセミナーを開催するなど、サイバーセキュリティの推進に向けた積極的な取組も進められている。今後は、こういった取組の裾野を拡大していくことが重要である。

[14] 経団連サイバーセキュリティ経営宣言：http://www.keidanren.or.jp/policy/2018/018.pdf

（2）官民の取組状況

現在、官民の様々な主体が各世代・各組織に向けて幅広く普及啓発の取組を実施している。これらを大きく「セミナー・イベント」、「ツール・コンテンツの提供」、「タイムリーな情報発信」に分類すると、主に以下のような取組が実施されている。

① セミナー・イベント

毎年２月から３月に、内閣サイバーセキュリティセンター（以下、「NISC」という。）が中心となって「サイバーセキュリティ月間」を開催し、官民の様々な普及啓発の取組が集中的に実施されている[15]。また、総務省・文部科学省のe-ネットキャラバン、文部科学省のネットモラルキャラバン隊などにより、全国各地でセミナーや出前講座を実施している。さらに、IPAが地域の商工団体等と共同して講習能力養成セミナーを実施するとともに、相談窓口を設置し、個人や企業からの問い合わせに対応している[16]。

② ツール・コンテンツの提供

NISCが、サイバーセキュリティに関する基本的な知識を紹介したハンドブックを作成し、普及に努めている[17]。また、総務省が、個人や企業向けに、公衆無線LANの利用に関する周知啓発を実施している。経済産業省・IPAでは、サイバーセキュリティに関する最新の動向を収集・分析し、報告書を公表するとともに、IPAでは、イベントでの資料配布や、情報漏えい対策ツールの提供などを行っている。

③ タイムリーな情報発信

NISC が、SNS を用いて、セキュリティに役立つ情報や、緊急情報を随時発信している[18]。また、JPCERT/CC とも連携して、ウェブサイトやメーリングリストを活用した情報提供を行っている。

---

[15] サイバーセキュリティ月間：https://www.nisc.go.jp/security-site/month/index.html
[16] 情報セキュリティ安心相談窓口：https://www.ipa.go.jp/security/anshin/index.html
[17] 情報セキュリティハンドブック：https://www.nisc.go.jp/security-site/handbook/index.html
[18] NISCのSNSアカウント：Twitter（NISC内閣サイバーセキュリティセンター @cas_nisc、内閣サイバー（注意・警戒情報） @nisc_forecast）、Facebook（内閣サイバーセキュリティセンターNISC @nisc.jp）、LINE（内閣サイバーセキュリティセンターNISC）

こうした取組を、取組の対象とその手段に分けて整理すると、図５のとおりとなる。今後は、官民のこうした幅広い取組の連携を推進し、効果的・効率的に実施していくことが重要である。

官民（※）の取組状況

※情報セキュリティ社会推進協議会に参画している一財、一社、NPO等を中心に記載

公的機関における取組　民間における取組

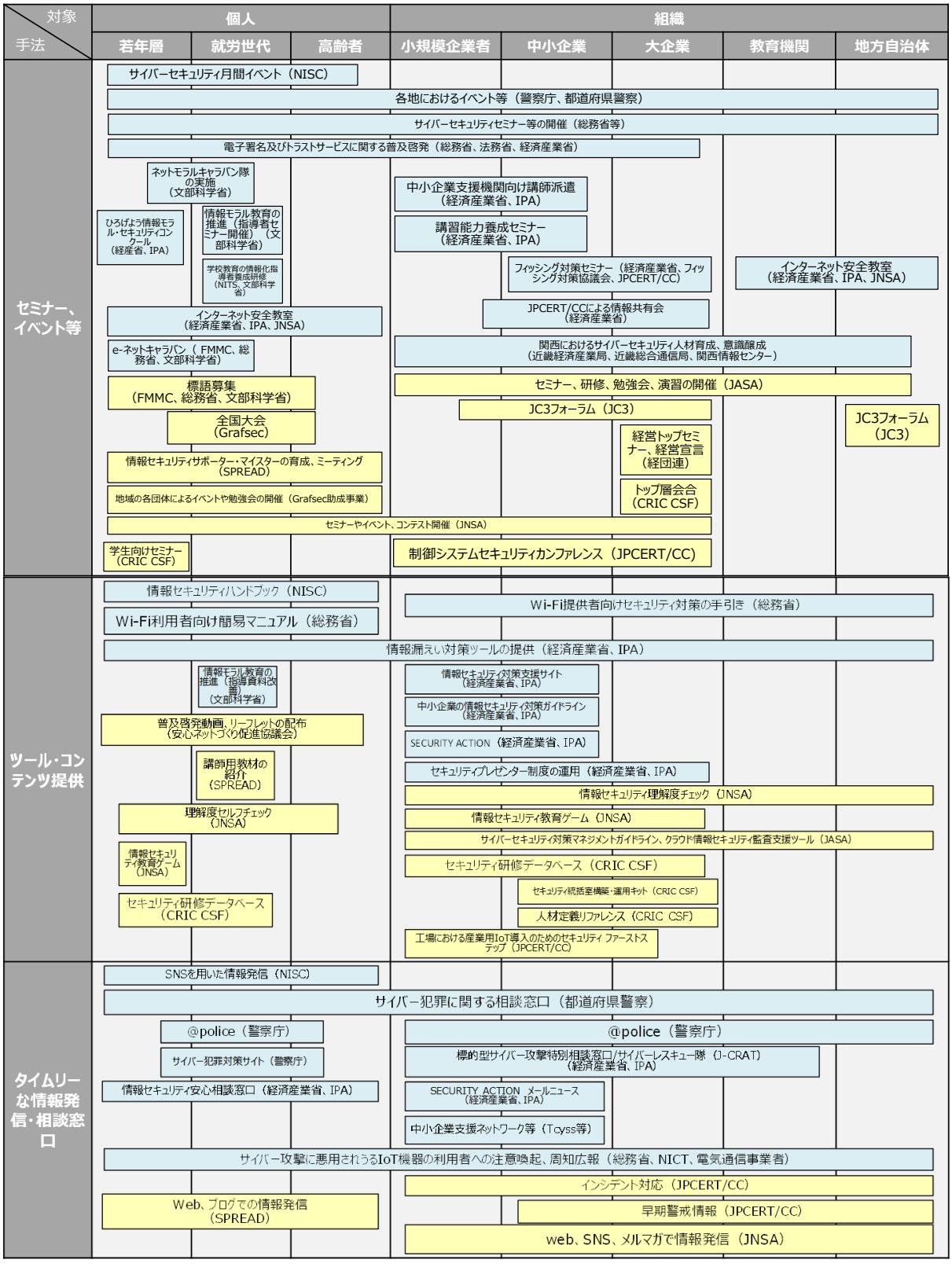


図５　各省庁及び民間団体の普及啓発施策に関する全体像（案）

参考　諸外国における取組の例

（1）米国における取組

米国においては、DHS（国土安全保障省）がサイバーセキュリティに関する啓発キャンペーン活動「Stop.Think.Connect.[19]」を立ち上げ、官民連携の協議会であるNCSA（National Cyber Security Alliance）が主導している。また、DHSが中心となりNCSAと連携して、2004年から、毎年10月にサイバーセキュリティ啓発月間（National Cybersecurity Awareness Month）[20]を開催している。

また、NIST（国立標準技術研究所）が主導するNICEイニシアティブ（National Initiative for Cybersecurity Education）において、統一性の確保を念頭に、サイバーセキュリティの普及啓発・人材育成を一体的に推進している[21]。

（2）英国における取組

政府全体の取組を、「個人」、「中小企業」、「大企業」の分類に分けて、関係機関の個別施策を整理して公開しているほか、内務省が中心となって行っている普及啓発キャンペーン「Cyber Aware」[22]では、事業者の参加登録の受付や、啓発ツールの提供を実施している。また、NCSC（National Cyber Security Centre）[23]では、組織・個人や、文章や分かりやすい画を用いたトピック別にガイダンスを提供している。また、個人向けでは年代に応じた教育プログラム等の紹介を行っている。

---

[19] Stop.Think.Connect.：https://www.stopthinkconnect.org/
[20] 米国の「サイバーセキュリティ啓発月間」：https://staysafeonline.org/ncsam/
https://www.dhs.gov/national-cyber-security-awareness-month
[21] NICE：https://www.nist.gov/itl/applied-cybersecurity/nice
[22] Cyber Aware：https://www.cyberaware.gov.uk/
[23] NCSC：https://www.ncsc.gov.uk/

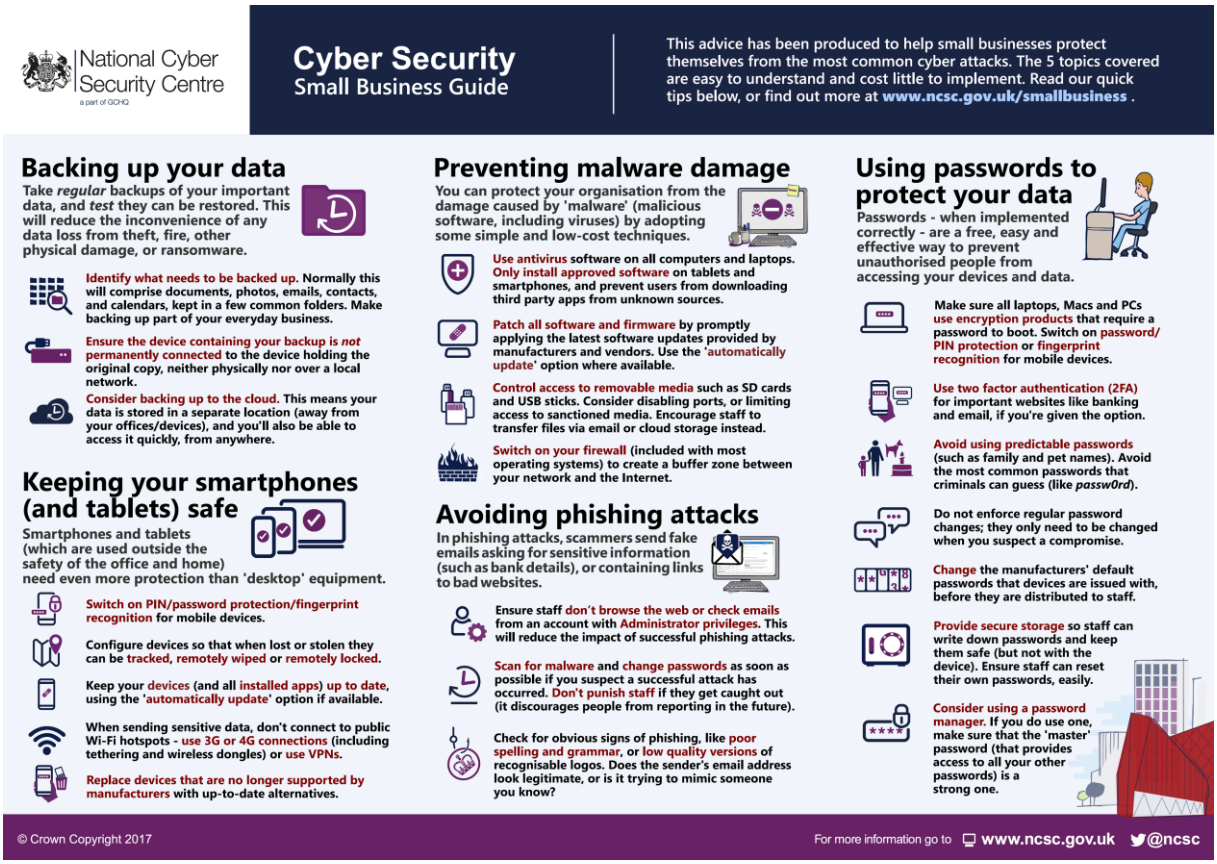


図６　NCSC が中小企業向けに作成・公表しているガイダンス

（出典：https://www.ncsc.gov.uk/information/infographics-ncsc）

３　今後の取組の基本的な考え方

（１）個人・組織における「自覚・行動」の促進

前述のとおり、個人においては、サイバー空間の利活用の拡大とともに、サイバー空間を悪用した犯罪に対する不安も広がっている一方、対策の実施率は半分程度に留まっており、具体的な活動に十分に結びついていない。また、大企業においては取組が進んでいるのに対し、中小企業においては担当者が置かれない場合も多く、サイバーセキュリティの取組が遅れている。

サイバーセキュリティについての情報は、官民からすでに数多く提供されているにも関わらず、国民一人一人や中小・小規模企業には行き届いていないという、インターネット通信で言われていた「ラストワンマイル」のように、いわば、「サイバーセキュリティのラストワンマイル」という状況が見られる。このような「ラストワンマイル」を解消するため、官民が、それぞれの施策間の連携を図りつつ、一体となって取り組み、個人や企業の自覚及び具体的な行動を促していくことが必要である。

（２）「３つの視点」からの取組の推進

これまでの官民による取組の結果、サイバーセキュリティ対策の実施状況について一定の向上が見られるものの、サイバー空間における繋がりが拡大する中、その中の一部で生じた問題が社会全体に影響を及ぼす恐れも急速に拡大している。また、今後、官民双方で情報通信技術の活用がさらに進むことが見込まれる中、サイバーセキュリティに関する個人や組織の取組が重要となる。

このような取組を促進させるためには、いわゆる公衆衛生活動のように、個人や組織がサイバーセキュリティに関する活動を行う世界を作り上げていく必要がある。その世界においては、サイバーセキュリティに向けた取組の必要性を個人一人一人や個々の組織が「自覚」し、対策を当たり前のこととして講じられるとともに、自覚をもって取り組んでいる個人や企業が自ら行うことが難しい部分に対しては、組織的なサポートが提供されるような取組が必要である。

その際、以下の３つの視点から取り組んでいくことが重要である。

① 継続的な実施

サイバーセキュリティは、技術の進展が早い分野ではあるものの、OS やソフトウェアのアップデートや、パスワードの管理等、技術が進展しても普遍的に必

要となる取組がある。このため、サイバーセキュリティに関する普及啓発を行う際には、基本的な対策をぶれることなく継続的に伝えていくことが必要となる。

② 対象ごとの適切なツール・コンテンツの提供

個人や企業によって、対策の効果的な伝達手段は異なる[24]。例えば、若者はSNS、高齢者は旧来のメディア、地域の中小企業は商工会、士業関係者、地方自治体等、中小企業をサポートする主体を通じた普及など、それぞれの対象にとって効果的な伝達手段の使い分けが重要である。また、各ツール・コンテンツの間の整合や、類似のツール・コンテンツの統合、利用者の属性を踏まえた分かりやすい情報提供といった取組も必要である。

③ 関係者間の連携の促進

各種の取組をより効果的・効率的に実施していくため、官民の関係者間の連携を強化する。特に、各地域において草の根で活動する主体との連携も更に強化することで、個人や企業それぞれに情報が行き渡る環境を整備し、「ラストワンマイル」の解消に繋げていくことが重要である。

また、これらの普及啓発に関する取組は優秀な人材育成の基盤としての役割も担う（図7は2011年に策定した「情報セキュリティ普及・啓発プログラム」で示された概念図）。各対象へ向けたすそ野の広い普及啓発と、企業におけるセキュリティや先端的な技術者など、より専門性が求められる層に向けた人材育成に併せて取り組んでいく。

[24] 「メディア定点調査2018」（博報堂DYメディアパートナーズ　メディア環境研究所）性年代別メディア総接触時間より（参考13）

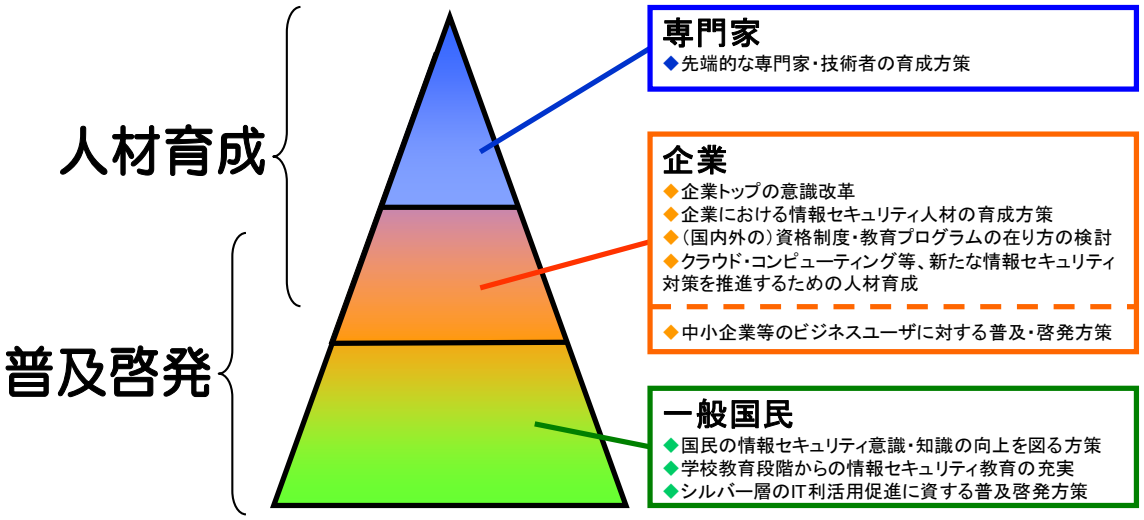


図７　情報セキュリティにおける普及・啓発と人材育成の関係

4　具体的取組の推進

（1）基本的な対策の徹底

2020 年の東京オリンピック・パラリンピック競技大会を控え、今後サイバー攻撃の脅威が高まる中、これを一つの契機として、個人や組織におけるサイバーセキュリティの意識を高めていく必要がある。具体的には、各個人や企業において、サイバーセキュリティに向けた取組の必要性を自覚し、当たり前のこととして取組を講じる状態を目指すため、必要な対策を継続的に伝えていく。

その取組の一環として、NISC 及び IPA が共同で示している現行の「インターネットを安全に利用するための情報セキュリティ対策９か条」について、必要な見直しを加えつつ、官民における各種の取組に浸透させることにより、個人や企業における基本的な対策を徹底し、全体の底上げを図る。

※「インターネットを安全に利用するための情報セキュリティ対策９か条」（2015 年２月 IPA、NISC 作成）

1. OS やソフトウェアは常に最新の状態にする
2. パスワードは貴重品の様に管理する
3. ログイン ID やパスワードは絶対教えない
4. 身に覚えのない添付ファイルは開かない
5. ウイルス対策ソフトを導入する
6. ネットショッピングでは信頼できるお店を選ぶ
7. 大切な情報は失う前に複製する
8. 外出先では機器の紛失・盗難に注意する
9. 困ったときは相談する

（2）重点的な対象とその内容

ICT の利活用の進展による恩恵は、若年層から高齢者層、また、大企業から中小企業まで、幅広い対象に広がっている。このような状況において、サイバーセキュリティ対策に関する普及啓発の取組も幅広く実施していくことが重要である。その上で、ICT 化の恩恵の広がりと比較して、特に中小企業、若年層、及び地域における取組については取組の効果が大きいと考えられる。そこで、これらについては、以下のとおり重点的に取組を実施していく。

① 中小企業

i.　重点化の背景

中小企業については、今後、サプライチェーンのICT化が進展する中で、中小企業への危害がサプライチェーン全体に広がり得ることや、攻撃者に踏み台として悪用される可能性が高まることなど、サイバーセキュリティの重要性が増している。特に、社員数が少ない小規模企業においては、自社でサイバーセキュリティに関する対策を講じたり、担当者を置いたりといったことが難しい状況も想定される。また、サイバーセキュリティに関する事故は、中小企業においても組織の事業継続に影響を及ぼしかねないとの調査も示されている[25]。こうした状況を踏まえ、中小企業がサイバーセキュリティ対策や社内における教育を着実に実施できるよう、中小企業に対して重点的な取組を実施する。

ii.　具体的取組の内容

- 特に小規模の事業者など、担当者を置けなかったり、セミナー等にも参加することが難しい企業の対策の向上に向けて、わかりやすい対策集を作成し、理解の向上を図る（NISC）
- サプライチェーン全体のサイバーセキュリティ対策の普及啓発に取り組むとともに、中小企業向けに、専門的なアドバイス、支援等を行う相談窓口を創設し、複数の地域で実証を行って中小企業のサイバーセキュリティレベルの実態等を明らかにし、中小企業が活用しやすいサービスの検討を行う。（経済産業省）
- 中小企業における対策の実施を促すため、「中小企業の情報セキュリティ対策ガイドライン」の普及を図るとともに、政策動向や中小企業のニーズを踏まえた改訂を行う。（経済産業省、IPA）
- 中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度「SECURITY ACTION」の活用を推進し、セキュリティレベル向上を図る。また、IT補助金において当該制度の活用を申請要件とすることや当該制度を活用した企業に対するサイバー保険の保険料の割引制度など、事業者が自己宣言することでメリットを得られる仕組みを構築することなどを通じ、普及を目指す。さらに、「SECURITY ACTION」宣言事業者への

[25] トレンドマイクロ社「法人組織におけるセキュリティ実態調査　2017年版」によると、重大被害を経験している組織での年間平均被害額を規模別でみると、5,000名以上規模の組織で平均3億2,347万円、50～99名規模の組織で平均1億5,128万円となっている。

メール配信を通じた情報提供を実施する。（経済産業省、IPA）

- 中小企業のIT・セキュリティ担当者・教育担当者及びその支援者を対象として、実践的な知識を学ぶことを目的とした「講習能力養成セミナー」を地域の商工団体やNPO法人等と連携して全国各地で開催する。（経済産業省、IPA）
- 中小企業支援者のスキル向上を目的として、全国の商工・士業団体等の中小企業支援機関の研修等へ情報セキュリティに関する講師の派遣を行うとともに、ツール等の説明・配布を行う。（経済産業省、IPA）
- 中小企業における情報セキュリティ対策水準の向上を目的とし、中小企業向けの学習コンテンツ等を提供するウェブサイトを運営する。また、同ウェブサイトを通じて中小企業支援者の活動をサポートするサービスを提供する。（経済産業省、IPA）
- 自治体が警察組織や中小企業支援機関、サイバーセキュリティ支援機関などと連携して設立した中小企業支援ネットワーク等において、サイバーセキュリティの啓発、情報共有、事案発生時の相互連携等に取り組むと共に、サイバーセキュリティ相談窓口を設け、電子申請や電話、窓口による相談対応を行う。（東京中小企業サイバーセキュリティ支援ネットワーク（Tcyss）等）
- 中小企業の経営者や現場管理者向けに産業用IoT機器導入時の基本的なセキュリティ対策の考え方等をわかりやすく解説した「工場における産業用IoT導入のためのセキュリティファーストステップ」の普及により、中小企業の制御システムセキュリティへの意識向上及び対策強化を図る。（JPCERT/CC）

② 若年層

i.　重点化の背景

近年は、インターネットの利用が拡大する中で、若年層の不正アクセス禁止法違反の検挙が他の世代に比べて高く、法令に関する知見が十分でない中で違反してしまうなど、無自覚なまま被害者から加害者となってしまう状況もみられる[26]。そこで、若年層が最低限のリテラシーを身に付けるための取組を進め

[26] 普及啓発・人材育成専門調査会　第９回会合（2018年10月10日）資料1-2　利用者視点の啓発と次世代技術者の育成（一般財団法人草の根サイバーセキュリティ運動全国連絡会　常務理事・事務局長　吉岡良平）より（参考14）

ることが必要である。その際、保護者や教師が教えるという取組だけでなく、例えば高等専門学校生が小中学生に教えるなど、若年層の中における取組も重要となる。

　加えて、若年層は今後のイノベーションを支える人材である。今後のICT分野を支える人材がサイバーセキュリティに関する素養も併せて身に付けることや、サイバーセキュリティ分野で卓越した潜在能力を有する人材を育成することは重要であることから、これらの先端的な人材の発掘と育成に向けた重点的な取組も必要である。

ii.　具体的取組の内容①（犯罪に巻き込まれない、犯罪を起こさないための取組）

- サイバー犯罪、サイバー攻撃による被害防止を目的として、各地域に根ざしたセミナー、講演、イベント等を引き続き行う。また、サイバーパトロールやインターネット利用者に対する講演活動等を行うサイバー防犯ボランティアについて、研修会を開催するなどして取組の拡大・活性化を図る。（警察庁、都道府県警察）
- 若年層に教育する現場の教員のサポートとなるよう、動画教材や指導手引書を活用したセミナーを実施する。また、独立行政法人教職員支援機構と連携し、情報通信技術を活用した指導や情報モラルに関する指導力の向上を図るため、各地域で情報教育の中核的な役割を担う教員等を対象とした研修を実施する。（文部科学省）
- 保護者等を対象として、インターネット上のマナーやスマートフォンに関する家庭でのルール作りの重要性への意識向上を目指したネットモラルキャラバン隊を引き続き実施する。（文部科学省）
- 小中高校生を対象とした「ひろげよう情報モラル・セキュリティコンクール」を継続的に開催し、情報モラル・セキュリティに関する標語、ポスター、４コマ漫画、書写作品を募集、表彰することで、意識向上を図る。（経済産業省、IPA）
- 子どもたちのインターネットの安全な利用に係る普及啓発を目的に、児童・生徒、保護者・教職員等に対する、学校等の現場での「出前講座」であるe-ネットキャラバンを引き続き実施する。（マルチメディア振興センター（FMMC）、総務省、文部科学省）

- 学校及び個人単位で情報通信の安心安全な利用のための標語の募集を行い、表彰することで、情報通信の安心・安全な利用や情報セキュリティに関する意識醸成を図る。（情報通信における安心安全推進協会（事務局：FMMC）、総務省、文部科学省）
- 地域の若年層に対するセキュリティ・モラル教育の展開を進めるため、佐世保工業高等専門学校の学生が、長崎県警よりサイバーセキュリティボランティアとして委嘱を受け、県内の小学校及び中学校に出向き、ネットやSNSの上手な使い方、セキュリティに関する講演やスマートフォンを用いた実演を行う。（独立行政法人国立高等専門学校機構、佐世保工業高等専門学校）
- 青少年のスマートフォン利用を中心としたインターネット利用のリスクとその対策について、青少年及び保護者向けのリーフレットを作成し、ウェブサイト等で配布する。（安心ネットづくり促進協議会）

iii. 具体的取組の内容②（先端的な人材の育成に向けた取組）

- 25歳以下の若年ICT人材を対象としたSecHack365を通じ、高度なセキュリティ技術を本格的に指導することで、セキュリティイノベーターの育成に取り組む。（国立研究開発法人情報通信研究機構（NICT）、総務省）
- セキュリティ・キャンプを通じ、若年層のセキュリティ意識向上と突出した人材の発掘・育成に取り組む。（経済産業省）
- コンピュータやネットワーク、データベース、プログラミング、数学等の知識を駆使して、サイバーセキュリティの技術を競う競技会（CTF：Capture The Flag）を通じて、実践的な情報セキュリティ人材の発掘・育成、技術の実践の場を提供する。（2017年度は、のべ102カ国から4,347人が参加。）（NPO日本ネットワークセキュリティ協会（JNSA））

③ 地域における取組の支援

i. 重点化の背景

サイバーセキュリティに関するセミナーやイベントは、大都市圏を中心に実施されており、地域では、セミナー等を行うための適切な講演者が十分でないなど、活動を行いたくてもできない状況がみられる。他方、各地域で主体的に取り組む事例も一部見受けられ、こうした活動への支援等、大都市圏のみなら

ず地域でもサイバーセキュリティに関する情報がすみずみまで行き渡るよう、支援を行っていくことが重要である。

ii.　具体的取組の内容

- サイバー犯罪、サイバー攻撃による被害防止を目的として、各地域に根ざしたセミナー、講演、イベント等を引き続き行う。また、サイバーパトロールやインターネット利用者に対する講演活動等を行うサイバー防犯ボランティアについて、研修会を開催するなどして取組の拡大・活性化を図る。（警察庁、都道府県警察）（再掲）
- サイバーセキュリティに係る現状や対策について広く知得していただくことを目的に、各地域において、サイバーセキュリティに関心のある個人や組織を対象に、地方総合通信局等が招いた有識者が講演等を行う。（総務省等）
- サプライチェーン全体のサイバーセキュリティ対策の普及啓発に取り組むとともに、中小企業向けに、専門的なアドバイス、支援等を行う相談窓口を創設し、複数の地域で実証を行って中小企業のサイバーセキュリティレベルの実態等を明らかにし、中小企業が活用しやすいサービスの検討を行う。（経済産業省）（再掲）
- 関西におけるサイバーセキュリティの重要性についての認識の醸成及び情報交換の活性化を図るとともに、サイバーセキュリティの向上に資する人材の発掘・育成の円滑化を進めるため、産学官等が連携した「関西サイバーセキュリティ・ネットワーク」を形成し、継続的にセミナー・イベント等を開催する。（関西サイバーセキュリティ・ネットワーク（共同事務局：近畿経済産業局、近畿総合通信局、関西情報センター））
- 地域の若年層に対するセキュリティ・モラル教育の展開を進めるため、佐世保工業高等専門学校の学生が、長崎県警よりサイバーセキュリティボランティアとして委嘱を受け、県内の小学校及び中学校に出向き、ネットやSNSの上手な使い方、セキュリティに関する講演やスマートフォンを用いた実演を行う。（独立行政法人国立高等専門学校機構、佐世保工業高等専門学校）（再掲）
- 地域でIT支援を行うボランティアの方々や情報セキュリティに関する知識・スキルの習得を目指す方等を対象とした「SPREAD情報セキュリティ

サポーター能力検定」・「SPREAD情報セキュリティマイスター検定」を各地で実施・普及し、地域での共助活動を促す。また、「サポーターズミーティング」を開催し、地域で活動するサポーター等の交流を図る。（一般社団法人セキュリティ対策推進協議会（SPREAD））

- 「全国大会」を開催し、地域においてサイバーセキュリティの普及啓発活動を行っている団体や、行政や中央で活動する関係機関を招き意見交換及び各者の交流を促す。（一般財団法人草の根サイバーセキュリティ運動全国連絡会（Grafsec））
- 公益を目的として、地域に密着して活動する非営利型の法人、団体、個人に対して助成を行い、活動の活発化を促す。（Grafsec）
- 全国の金融機関の底上げを目的として、金融ISAC AKC（Active Knowledge Center）ワーキンググループで、地域金融機関向けに地方ワークショップを開催し、最新事情に詳しい講師を派遣。セミナーや机上演習などを実施する。（一般社団法人金融ISAC）

（3）情報発信・相談窓口の充実

サイバーセキュリティに関する国民や企業の認識の向上に加えて、最新の脅威の情報や対策などを適時かつ迅速に発信することにより、国民や企業が自ら最新の取組を取ることができる環境を整備していくことが重要である。また、取組を実施する際に、専門的な内容や心配事を相談できるような窓口や、トラブルに直面した際の対応について相談できる敷居の低い窓口も必要となる。そこで、関係機関の連携を更に深め、情報発信や相談窓口の一層の充実に努めていく。

- 国民一人一人のセキュリティ意識向上を目的として、緊急時における注意・警戒情報やサイバーセキュリティに関する役立ち情報等について、NISC運営のSNSアカウントを用いた発信を引き続き行う。（NISC）
- 警察庁ウェブサイト「@police[27]」において、DoS攻撃の発生や不正プログラムに感染したコンピュータの動向等の把握を可能とする「リアルタイム検知ネットワークシステム」により分析した結果をインターネット観測結果として広く一般に公開するほか、特にセキュリティ対策が必要となる場合は、適切な被害防止対策を講じるよう注意喚起を行う[28]。（警察庁）

[27] @police：https://www.npa.go.jp/cyberpolice/
[28] 2017年度は、観測資料、注意喚起等27件を掲載

- 相談窓口においてサイバー犯罪に関する具体的な相談に対応する。（都道府県警察）
- サイバー攻撃に悪用されうる IoT 機器の利用者への注意喚起のため、NICT がパスワード設定等に不備のある IoT 機器を調査し、電気通信事業者を通じて利用者に注意喚起を行う。総務省がサポートセンターを設置し、注意喚起を受けた利用者の相談対応を行うとともに、関係者と連携して IoT 機器の適切なパスワード設定や注意喚起事業の周知広報を行う。（総務省、NICT、電気通信事業者）
- 国民から一般的な情報セキュリティ（ウイルスや不正アクセス）に関する技術的な相談を受け付ける「情報セキュリティ安心相談窓口」を提供する[29]。（経済産業省、IPA）
- 「標的型サイバー攻撃特別相談窓口」で、広く国民一般から相談や情報を受付けると共に、「サイバーレスキュー隊（J-CRAT）」において、標的型サイバー攻撃による被害拡大防止の助言を行う。更に、ウイルス感染に気づかないまま攻撃の踏み台にされている組織に対しては、感染の通知や対応、対策の計画支援などを行う[30]。（経済産業省、IPA）

こういった取組を重点的に進めていくとともに、取組を通じて得られた優良事例を共有し、横展開していくことが重要である。

[29]電子メールをはじめ、電話、FAX、郵送でも受け付けており、2017年度の相談件数は１万件超
[30] 2017年度は、412件の相談を受け付け、144件のレスキュー支援を実施

5　連携体制の強化

官民において、各地域で普及啓発に関する自主的な取組が既に幅広く行われている。こうした中で、NISC をはじめとした関係機関が連携し、各機関の役割や普及啓発の対象をしっかりと位置付けて、ラストワンマイルに情報が行き着くよう配慮しつつ取組を進めていくことが重要である。このため、各機関が連携・補完しながら効果的・効率的に実施する体制づくりを目指す。

⑴ポータルサイトによる取組の見える化及び連携推進

官民の取組のマッピングをベースとして、それぞれの取組について、対象となる層や伝達手法の見える化及び連携を推進するためのポータルサイトを構築する。その際、今回提示した施策に限らず、官民の取組を随時追加するとともに、各種の取組においてもポータルサイトの紹介を行うことや、優良事例の共有を図ることなど、関係者と連携して取組の強化を図る。

なお、見える化に際しては、諸外国の取組を参考にしながら、簡潔な情報提供と視覚的な分かりやすさを特に意識して取り組む。

⑵ツール・コンテンツの共有

異なる主体が用いている様々なツール・コンテンツ等を互いに共有できるよう、ポータルサイトに、関係者が広く利用可能な教材を掲載する。

⑶「サイバーセキュリティ月間」の推進

サイバーセキュリティ月間について、関係機関とも連携して積極的な周知活動を行い、国民への認知度の向上に努める。民間事業者による参画も更に進むよう、働きかける。

⑷国際的な連携の強化

Stop.Think.Connect.の取組など、国際的かつ先進的な取組とも連携を図りながら、関係者のセキュリティの意識向上を図る。加えて、ASEAN 諸国との間で、ツール・コンテンツの提供や産業サイバーセキュリティセンター（IPA）による日米共同演習の開催などの協力も合わせて実施していくことで、サイバーセキュリティの強化に努める。

⑸PDCA サイクルによる各施策の継続的な改善

ポータルサイトに掲載した取組について、その活用状況をフォローするとともに、普及啓発活動への寄与の状況の確認・改善を図るなど、PDCA サイクルを回していく。

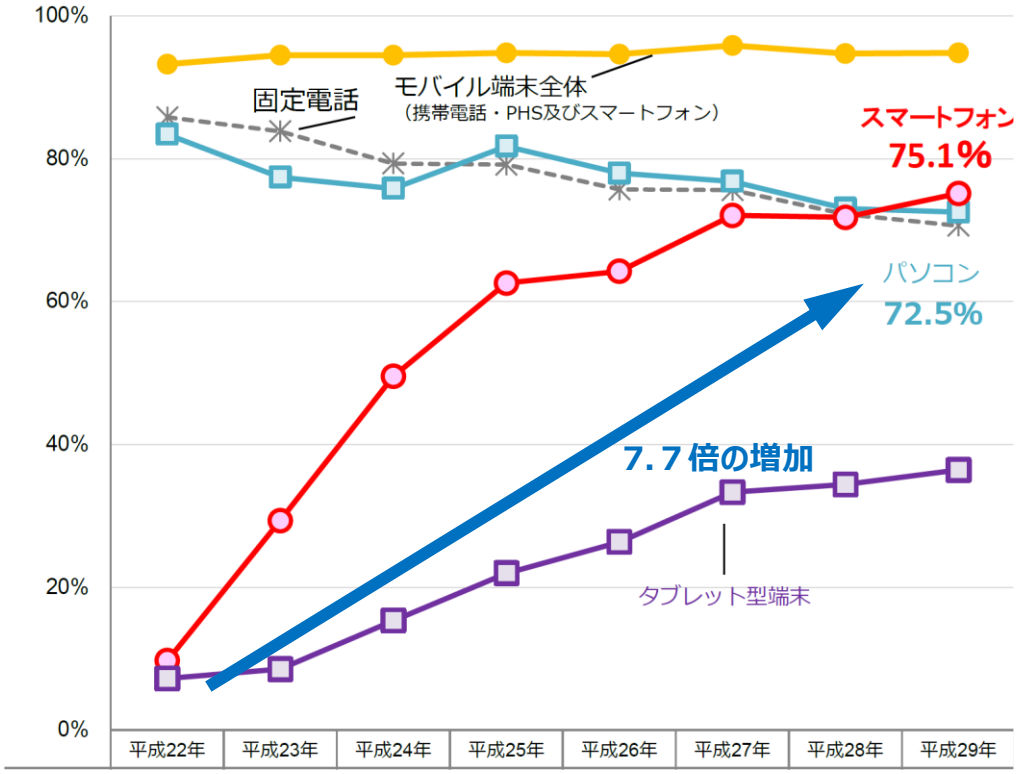
これらの取組により、効率的・効果的な実施体制を構築していく。

また、本プログラムの進捗状況については、普及啓発・人材育成専門調査会においてフォローアップを行う。その際には、取組の見える化やツール・コンテンツの共有が効果的に行われているかについて、取組に携わる各主体からのフィードバックにより評価を行う。加えて、サイバー空間における技術・サービスの進展の状況や、個人や企業におけるサイバーセキュリティ対策の実施状況等を踏まえ、必要に応じてプログラムの見直しを実施することとする。

参考資料

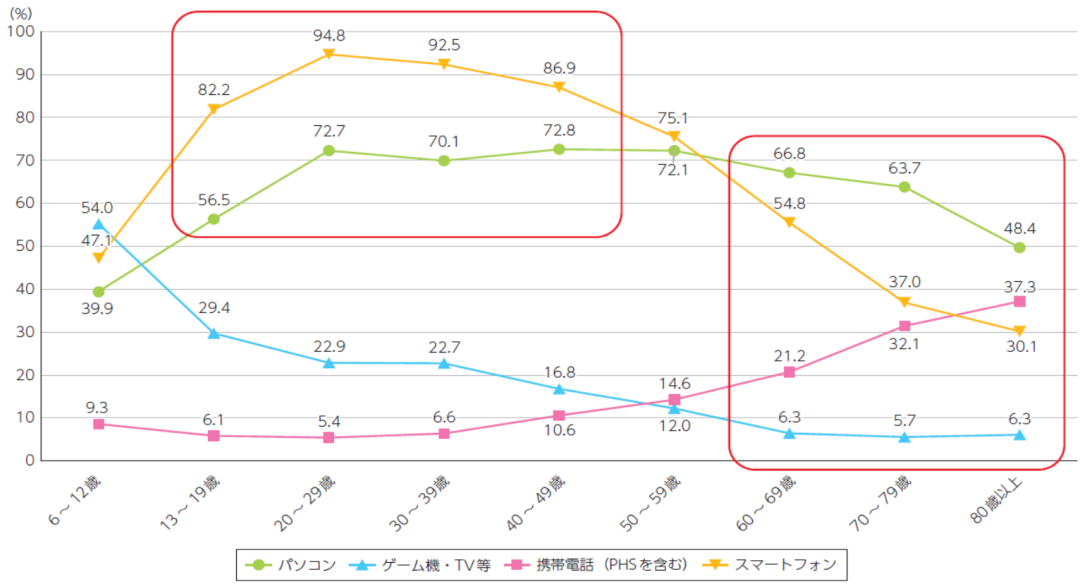
（参考１）　国内における情報通信機器の保有状況推移（世帯）

（出典：平成 29 年通信利用動向調査（2018 年５月　総務省））



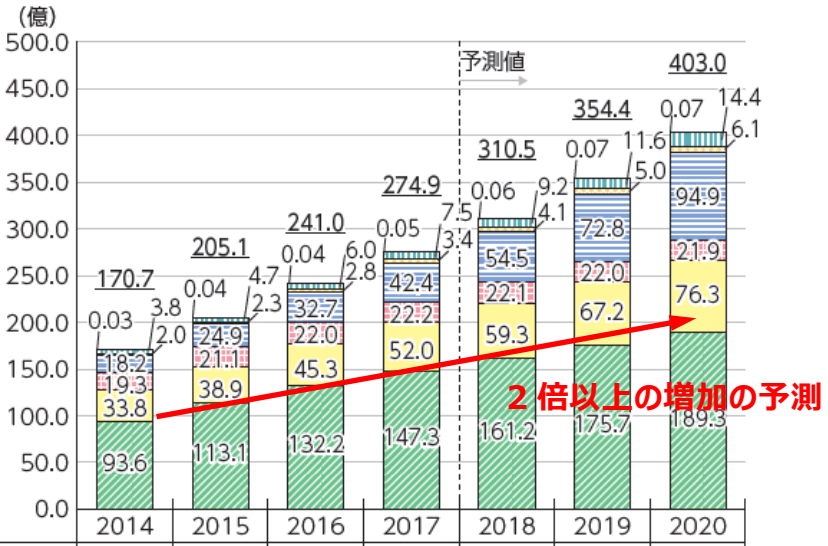
（参考２）　インターネット接続端末（世帯）

（出典：平成 30 年版情報通信白書（2018 年７月　総務省））



（参考３）　世界の IoT デバイス数の推移及び予測

（出典：平成 30 年版情報通信白書（2018 年７月　総務省））



	2014	2015	2016	2017	2018	2019	2020
合計	170.7	205.1	241.0	274.9	310.5	354.4	403.0
軍事・宇宙・航空	0.03	0.04	0.04	0.05	0.06	0.07	0.07
自動車	3.8	4.7	6.0	7.5	9.2	11.6	14.4
医療	2.0	2.3	2.8	3.4	4.1	5.0	6.1
産業用途	18.2	24.9	32.7	42.4	54.5	72.8	94.9
コンピューター	19.3	21.1	22.0	22.2	22.1	22.0	21.9
コンシューマー	33.8	38.9	45.3	52.0	59.3	67.2	76.3
通信	93.6	113.1	132.2	147.3	161.2	175.7	189.3

※「コンシューマー」の範囲：家電（白物・デジタル）、プリンターなどの PC 周辺機器、ポータブルオーディオ、スマートトイ、スポーツ・フィットネス、その他。

（参考４）　代表的な Fintech サービスの例

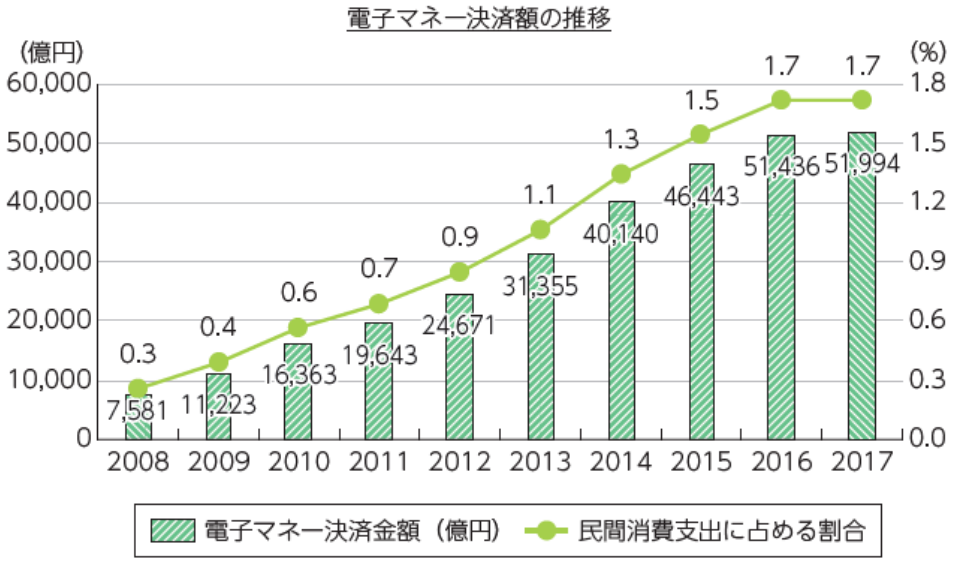
（出典：ICT によるイノベーションと新たなエコノミー形成に関する調査研究（2018 年３月　総務省））

代表的な FinTech サービス

区分	業態	分野・提供機能	代表的なFinTechサービスの例
業務	銀行	預金・資産管理	● PFM（Personal Financial Management）、バーチャルバンク
		融資	● P2P融資、ソーシャルレンディング、クラウドファンディング
	カード	決済	● モバイル決済、オンライン決済、モバイルPOS、自動支払
		送金	● オンライン送金、P2P送金
	証券	投資・資産運用	● ロボアドバイザー、オンライン証券・FP（Financial Planner）
インフラ		業務支援	● ビッグデータ分析、セキュリティ、クラウド型会計・労務サービス
		通貨・決済ネットワーク	● 仮想通貨決済・取引所、非中央集権型取引(ブロックチェーン)

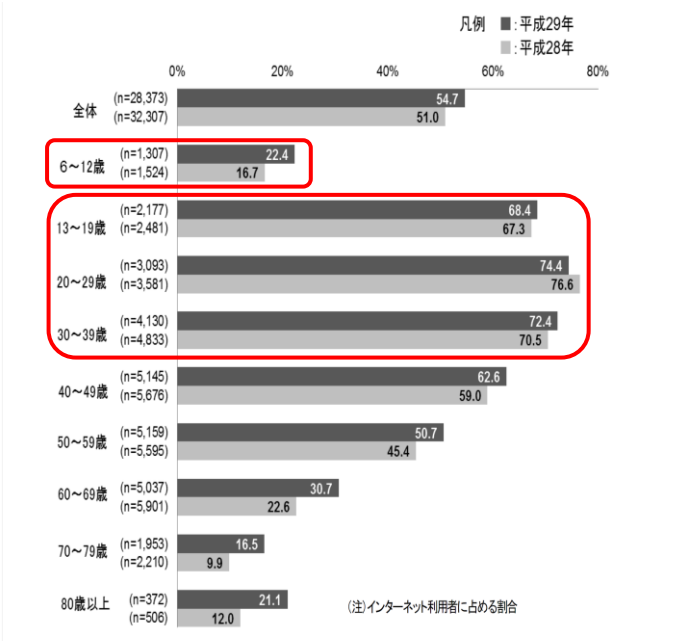
（参考５）　電子マネー決済額の推移

（出典：ICT によるイノベーションと新たなエコノミー形成に関する調査研究（2018 年３月　総務省））



（参考６）　ソーシャルネットワーキングサービスの利用状況

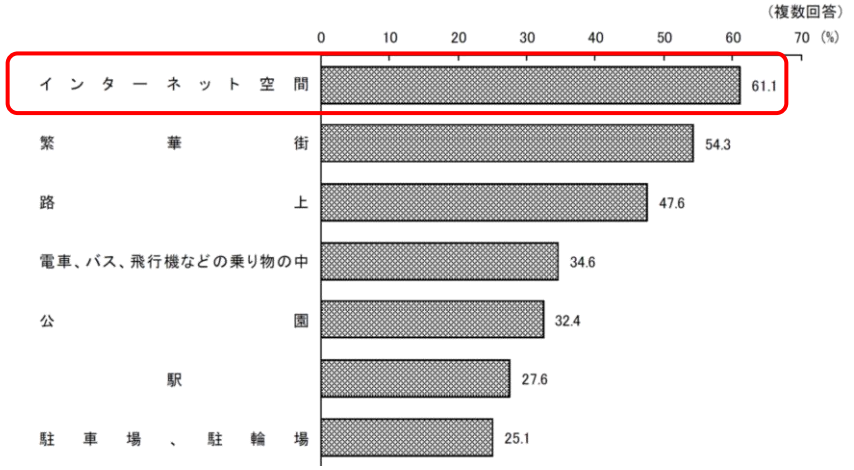
（出典：平成 29 年版通信利用動向調査（2018 年５月　総務省））



（参考７）

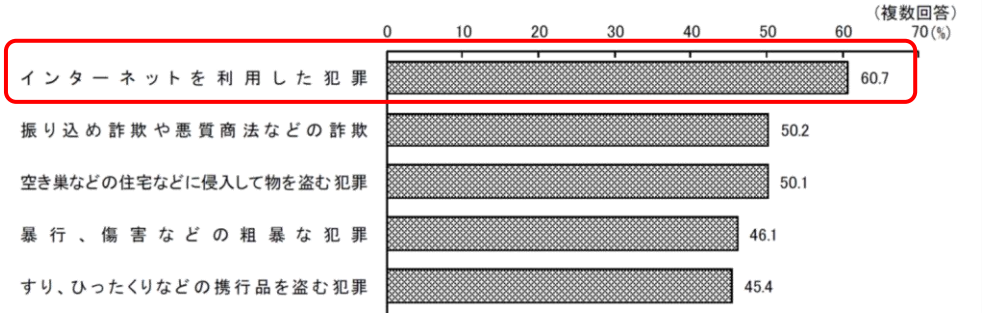
不安を感じる場所

（出典：治安に関する世論調査（2017 年 11 月　内閣府））



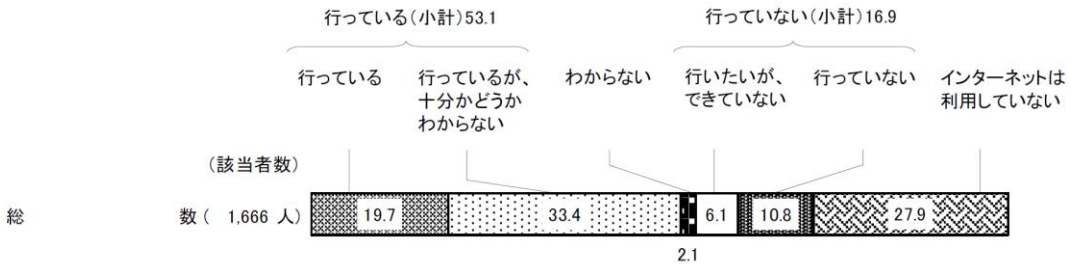
不安を感じる犯罪

（出典：治安に関する世論調査（2017 年 11 月　内閣府））



（参考８）　インターネットを安全・安心に利用するための対策

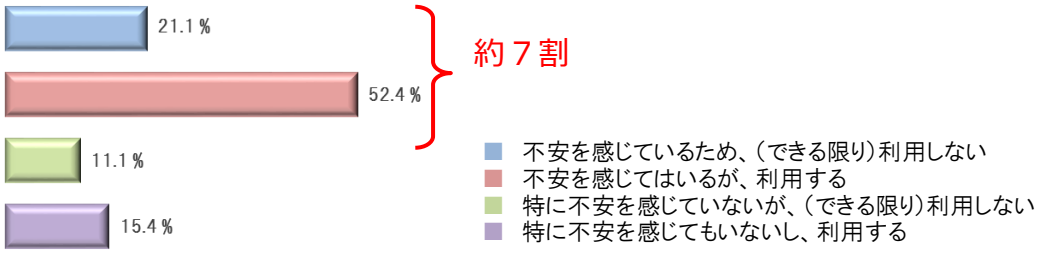
（出典：インターネットの安全・安心に関する世論調査（2018 年 11 月　内閣府））



（参考９）

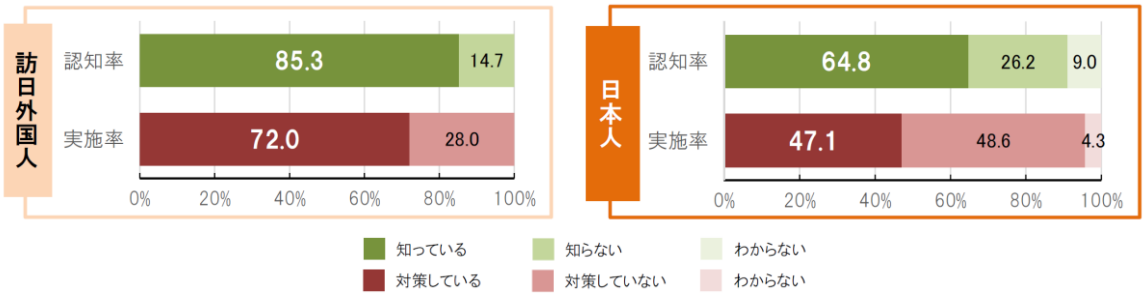
利用者における公衆無線 LAN のセキュリティに対する意識

（出典：公衆無線 LAN セキュリティ分科会報告書（2018 年３月　総務省））



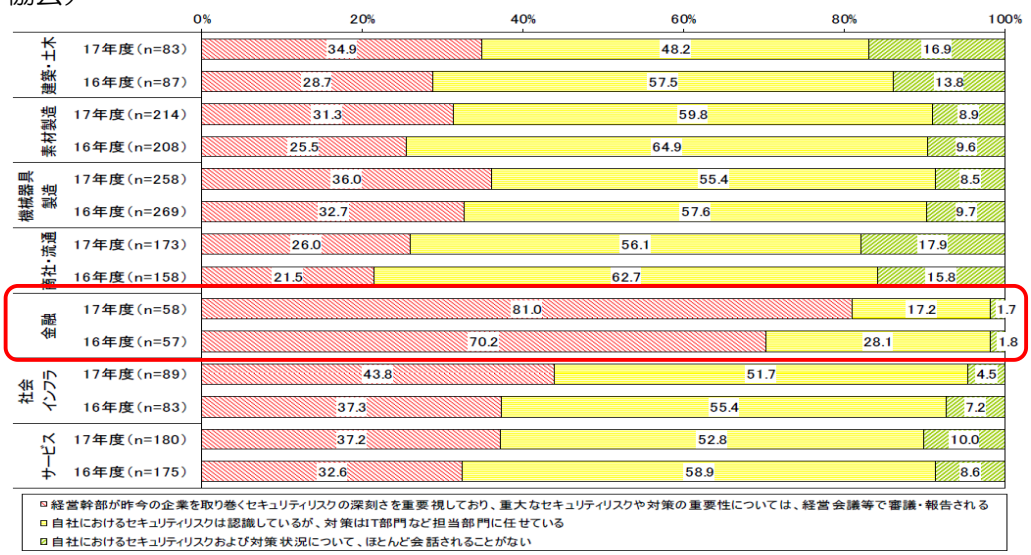
公衆無線 LAN 利用時の脅威の認知率とセキュリティ対策の実施率

（出典：公衆無線 LAN セキュリティ分科会報告書」（2018 年３月　総務省））



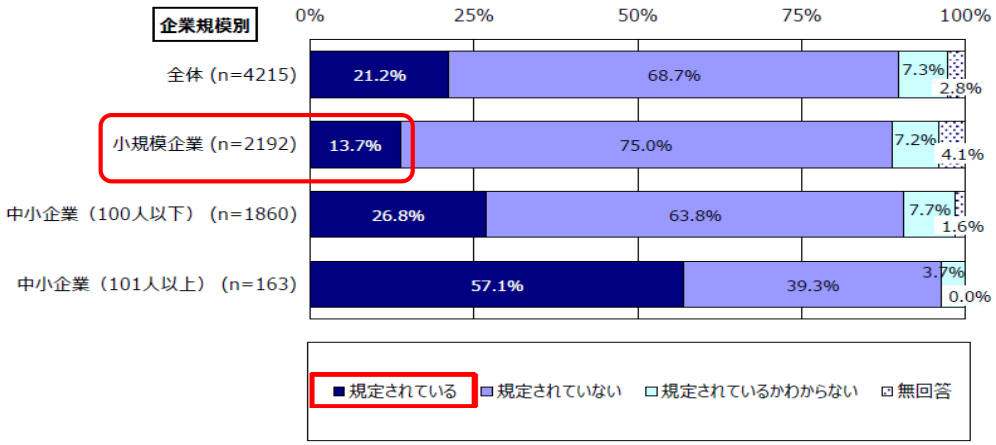
（参考 10）　経営幹部の情報セキュリティへの関与度合い（業種別）

（出典：企業 IT 動向調査報告書 2018（2018 年４月　一般社団法人日本情報システム・ユーザー協会）



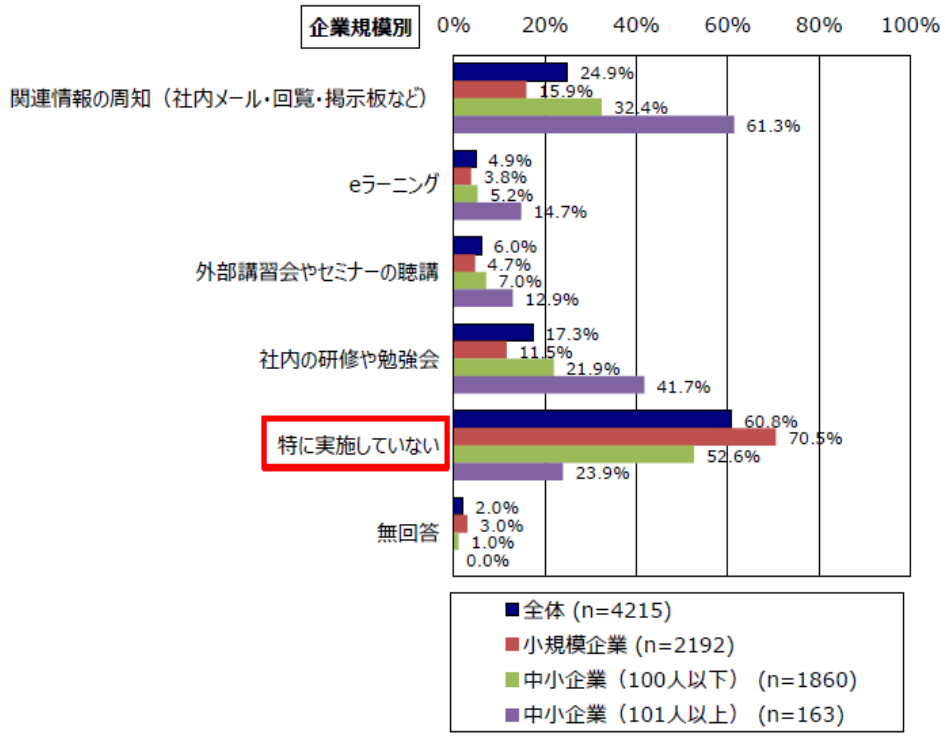
（参考 11）　情報漏えい等への対応方法に関する規定の有無

（出典：2016 年度中小企業における情報セキュリティ対策の実態調査報告書（2017 年８月　IPA））



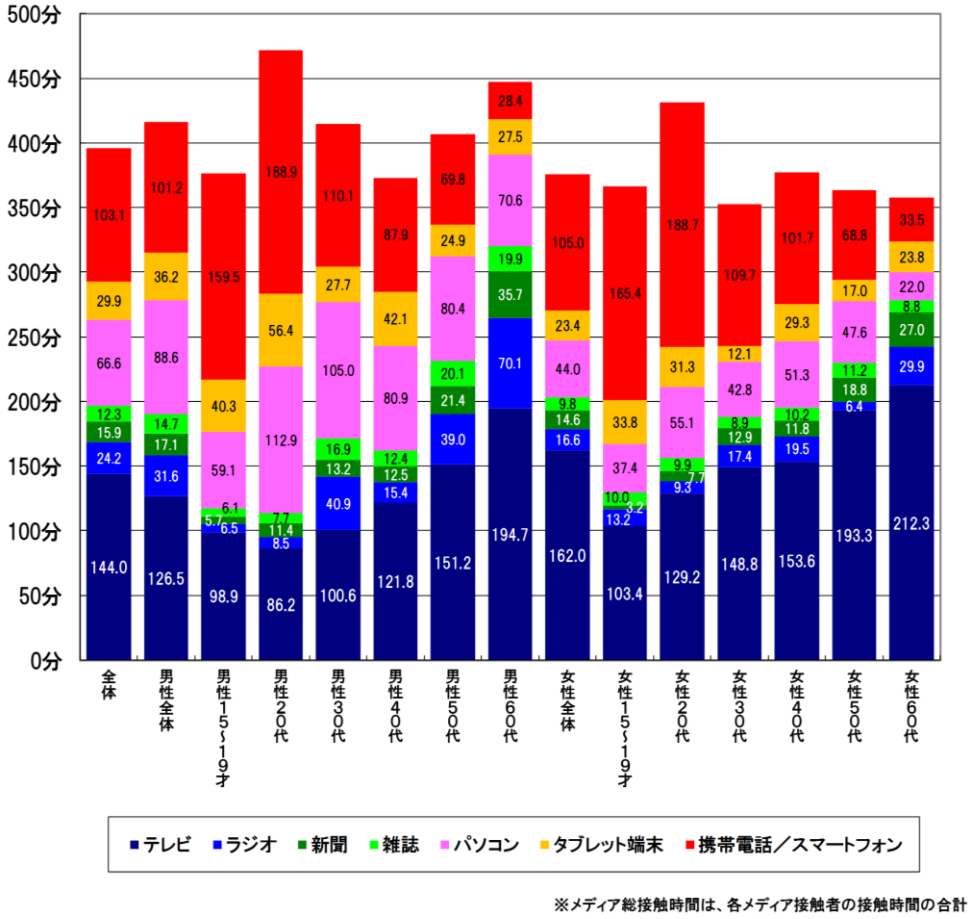
（参考 12）　社内での情報セキュリティ教育の状況

（出典：2016 年度中小企業における情報セキュリティ対策の実態調査報告書（2017 年８月　IPA））



（参考 13）　性年代別メディア総接触時間（１日あたり・週平均）：東京地区

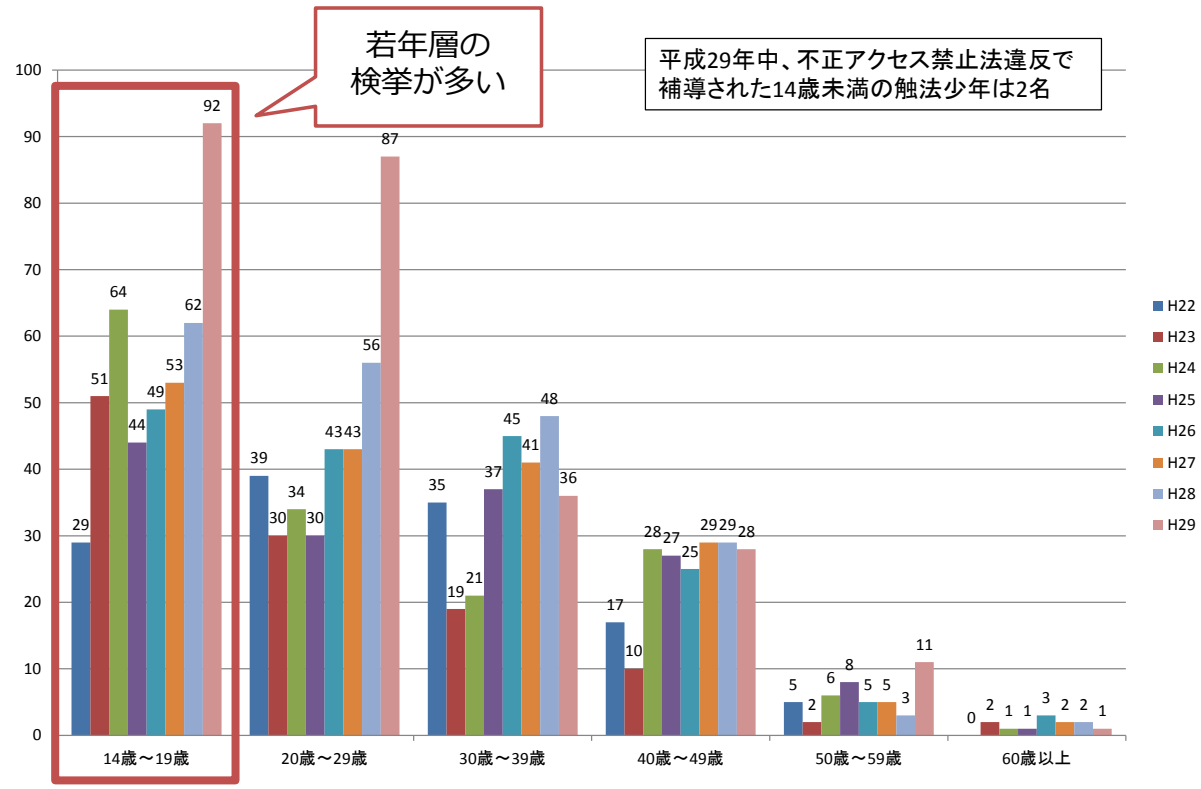
（出典：メディア定点調査 2018（博報堂 DY メディアパートナーズメディア環境研究所））



※メディア総接触時間は、各メディア接触者の接触時間の合計

（参考 14）　若年層の不正アクセス

（出典：利用者視点の啓発と次世代技術者の育成（一般財団法人草の根サイバーセキュリティ運動全国連絡会　常務理事・事務局長　吉岡良平））



国会公安委員会　総務大臣　経済産業大臣「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」（平成22年～平成29年）のデータより作図