

資料 1

サイバーセキュリティ意識・行動強化プログラム（案）

資料 1－1 「サイバーセキュリティ意識・行動強化プログラム（案）」（概要）

資料 1－2 「サイバーセキュリティ意識・行動強化プログラム（案）」（詳細概要）

資料 1－3 サイバーセキュリティ意識・行動強化プログラム（案）

「サイバーセキュリティ意識・行動強化プログラム（案）」（概要）

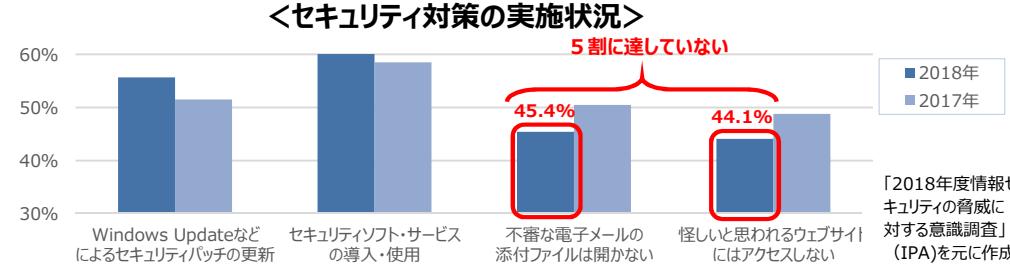
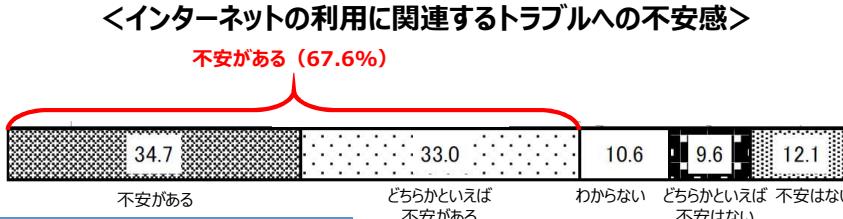
資料 1 – 1

1 はじめに

「サイバーセキュリティ戦略」(2018年7月閣議決定)に基づき、普及啓発について、2020年東京オリンピック・パラリンピック競技大会を見据えつつ、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、本プログラムを策定。

2 現状

- ①個人：AIやIoTの「生活」への浸透に伴い、インターネット利用への不安感が拡大。一方、具体的な対策の実施に十分に結びついていない。
- ②企業：中小企業では、特に規模の小さい企業ほど担当者が置かれない場合も多いなど、取組が遅れている。



3 今後の取組の基本的な考え方

- 対策に関する情報が国民一人一人や中小企業に必ずしも行き届いていない、いわば「サイバーセキュリティのラストワンマイル」の状況。
- 「3つの視点」から取組を推進：①継続的な実施、②対象に合わせた適切なツール・コンテンツの提供、③関係者間の連携の促進

4 具体的取組の推進

(1) 基本的な対策の徹底

- 個人や企業が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し、必要な対策を継続的に伝える

(取組の一例)

「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 NISC・IPA)の各種取組への浸透



(2) 重点的な対象とその内容

- 様々な対象に幅広く実施することを前提としつつ、以下の対象について、重点的に取組を実施

- 中小企業** 中小企業のトラブル対応を支援する「サイバーセキュリティお助け隊」の地域実証、「SECURITY ACTION」活用の促進、中小企業支援ネットワークによる啓発等
- 若年層** 無自覚なまま加害者になることを防ぐためのリテラシー向上の取組、先端的人材育成施策の推進
- 地域における取組の支援** 産学官連携型の取組の活性化、高専学生によるボランティア活動等



高専学生によるボランティア活動（提供：警察庁）

(3) 情報発信・相談窓口の充実

- 最新の脅威の情報・対策の適時かつ迅速な発信や相談できる窓口の確保等、自ら取り組むための環境を整備

(取組の一例) NISCにおけるSNSによる情報発信



5 連携体制の強化

- NISCをはじめとした関係機関が連携し、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推進**
①ポータルサイトによる取組の見える化・連携推進 ②ツール・コンテンツの共有 ③サイバーセキュリティ月間の推進 ④国際的連携の強化、⑤PDCAによる継続的改善
- 官民の様々な取組を集約するポータルサイトを構築し、対象となる層や伝達手法の見える化及び連携を推進**
- 個別施策の実施状況に加え、個人や企業の対策の実施状況等を分析し、本プログラムの内容・効果の定期的な評価、見直しを実施

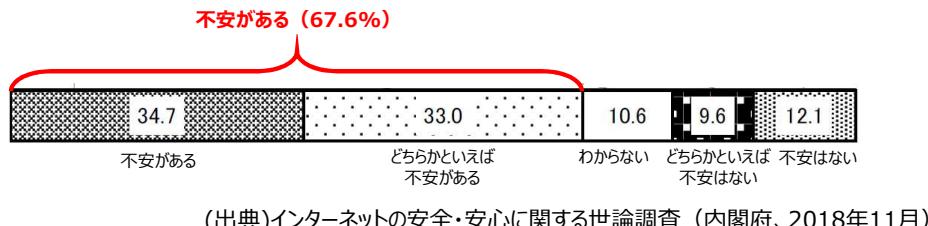
1 はじめに

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

- サイバー空間と実空間の一体化が進む中、サイバー空間の脅威により多大な経済的・社会的損失が生じる可能性も急速に拡大している。
- 個人においては、AIやIoTの「生活」への浸透に伴い、インターネットの利用に対する不安感も広がっている一方、対策の実施率は4割～6割台に留まっており、具体的な対策の実施に十分に結びついていない。
- 企業においては、売上の高い企業ほど取組が進んでいるのに対し、中小企業では、特に規模の小さい企業ほど担当者が置かれない場合も多いなど、サイバーセキュリティの取組が遅れている。

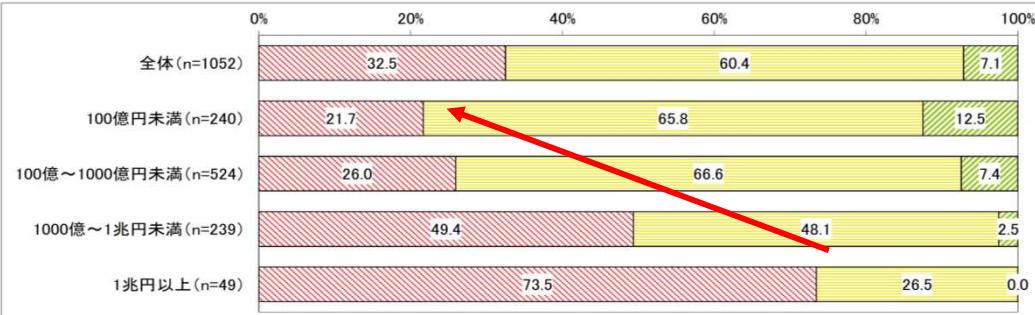
個人の状況

＜インターネットの利用に関するトラブルへの不安感＞

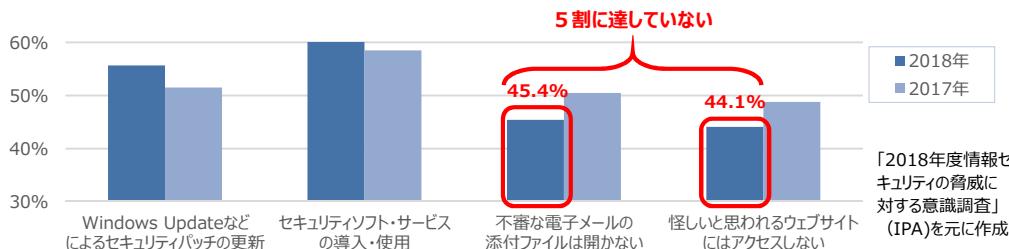


企業の状況

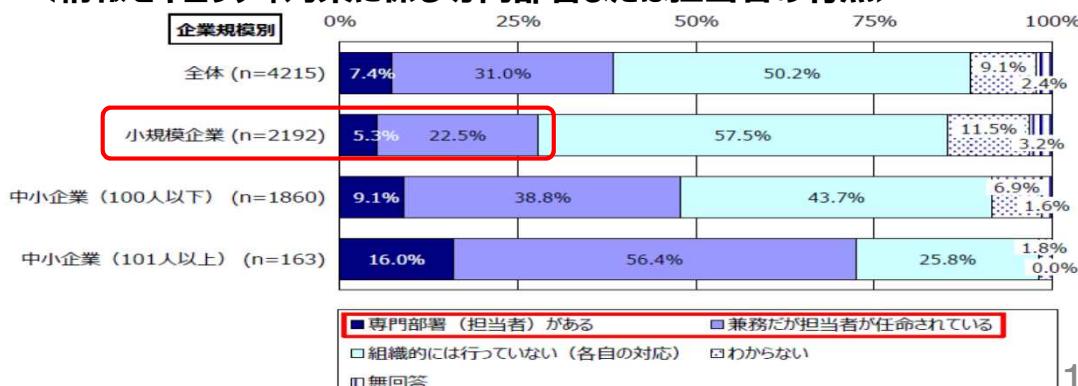
＜経営幹部の情報セキュリティへの関与度合い（売上高別）＞



＜セキュリティ対策の実施状況＞



＜情報セキュリティ対策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に実態調査報告書(IPA)

2 現状（2）官民の取組状況（1/2）

- 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。
- 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。

対象 手法	個人			組織				民間における取組 公的機関における取組
	若年層	就労世代	高齢者	小規模企業者	中小企業	大企業	教育機関	
セミナー、イベント等	サイバーセキュリティ月間イベント（NISC）							
	各地におけるイベント等（警察庁、都道府県警察）							
	サイバーセキュリティセミナー等の開催（総務省等）							
	電子署名及びトラストサービスに関する普及啓発（総務省、法務省、経済産業省）							
	ネットモラルキャラバン隊の実施（文部科学省）			中小企業支援機関向け講師派遣（経済産業省、IPA）				
	ひろげよう情報モラル・セキュリティコンクール（経産省、IPA）	情報モラル教育の推進（指導者セミナー開催）（文部科学省）	学校教育の情報化指導者養成研修（NITS、文部科学省）	講習能力養成セミナー（経済産業省、IPA）				
	インターネット安全教室（経済産業省、IPA）			JPCERT/CCによる情報共有会（経済産業省）			インターネット安全教室（経済産業省、IPA、JNSA）	
	e-ネットキャラバン（FMMC、総務省、文部科学省）			フィッシング対策セミナー（経済産業省、フィッシング対策協議会、JPCERT/CC）				
	標語募集（FMMC、総務省、文部科学省）			関西におけるサイバーセキュリティ人材育成、意識醸成（近畿経済産業局、近畿総合通信局、関西情報センター）				
	情報セキュリティサポート・マイスターの育成、ミーティング（SPREAD）			セミナー、研修、勉強会、演習の開催（JASA）				
	全国大会（Grafsec）			JC3フォーラム（JC3）			JC3フォーラム（JC3）	
	地域の各団体によるイベントや勉強会の開催（Grafsec助成事業）				経営トップセミナー、経営宣言（経団連）			
	セミナーやイベント、コンテスト開催（JNSA）				トップ層会合（CRIC CSF）			
	学生向けセミナー（CRIC CSF）			制御システムセキュリティカンファレンス（JPCERT/CC）				※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

2 現状（2）官民の取組状況（2/2）

ツール・コンテンツ提供	情報セキュリティハンドブック（NISC）				
	Wi-Fi利用者向け簡易マニュアル（総務省）				Wi-Fi提供者向けセキュリティ対策の手引き（総務省）
	情報漏えい対策ツールの提供（経済産業省、IPA）				
	情報モラル教育の推進（指導資料改善）（文部科学省）		情報セキュリティ対策支援サイト（経済産業省、IPA）		
	普及啓発動画、リーフレットの配布（安心ネットづくり促進協議会）		中小企業の情報セキュリティ対策ガイドライン（経済産業省、IPA）		
	講師用教材の紹介（SPREAD）		SECURITY ACTION（経済産業省、IPA）		
	理解度セルフチェック（JNSA）		セキュリティプレゼンター制度の運用（経済産業省、IPA）		情報セキュリティ理解度チェック（JNSA）
	情報セキュリティ教育ゲーム（JNSA）		情報セキュリティ教育ゲーム（JNSA）		サイバーセキュリティ対策マネジメントガイドライン、クラウド情報セキュリティ監査支援ツール（JASA）
	セキュリティ研修データベース（CRIC CSF）		セキュリティ研修データベース（CRIC CSF）	セキュリティ統括室構築・運用キット（CRIC CSF）	人材定義リファレンス（CRIC CSF）
			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（JPCERT/CC）		
タイムリーな情報発信・相談窓口	SNSを用いた情報発信（NISC）				
	サイバー犯罪に関する相談窓口（都道府県警察）				
	@police（警察庁）		@police（警察庁）		
	サイバー犯罪対策サイト（警察庁）		標的型サイバー攻撃特別相談窓口/サイバーレスキュー隊（J-CRAT）（経済産業省、IPA）		
	情報セキュリティ安心相談窓口（経済産業省、IPA）		SECURITY ACTION メールニュース（経済産業省、IPA）		
			中小企業支援ネットワーク等（Tcyss等）		
	サイバー攻撃に悪用されるIoT機器の利用者への注意喚起、周知広報（総務省、NICT、電気通信事業者）				
	Web、ブログでの情報発信（SPREAD）		インシデント対応（JPCERT/CC）		
			早期警戒情報（JPCERT/CC）		
			web、SNS、メルマガで情報発信（JNSA）		

民間における取組

公的機関における取組

3 今後の取組の基本的な考え方

- 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。
- 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、官民が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。

「3つの視点」からの取組の推進

①継続的な実施

- ・ 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。こうした基本的な対策を、ぶれることなく継続的に伝えていくことが重要である。

②対象に合わせた適切なツール・コンテンツの提供

- ・ 若者はSNS、高齢者はマスメディア、地域の中小企業は商工会・士業関係者・地方自治体等、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

- ・ より効果的・効率的な実施のため、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更なる連携強化などにより、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。

4 具体的取組の推進

(1) 基本的な対策の徹底

- 個人や企業が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。
- 「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、各種の取組に浸透させることにより、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 N I S C・I P A)

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化の恩恵は幅広い対象に広がっており、普及啓発も様々な対象に幅広く実施することが重要である。その上で、ICT化の恩恵の広がりと比較して効果が大きいと考えられる次の対象については、重点的に取り組む。

①中小企業：サプライチェーンのICT化の進展に伴う、対策の着実な実施

＜主な取組＞中小企業支援機関や損害保険会社等の連携により、中小企業のトラブル対応を支援する「サイバーセキュリティお助け隊」の地域実証、中小企業向けガイドラインの作成・普及、自己宣言の制度「SECURITY ACTION」への登録促進、中小企業支援ネットワークにおける啓発・情報共有・相談対応

②若年層：無自覚なまま加害者になることを防ぐためのリテラシー向上、今後のイノベーションを支える人材育成の推進

＜主な取組＞児童・生徒・教師・保護者等に向けたセミナー・出前講座、若年層を対象とした先端的な人材の育成に向けた取組

③地域における取組の支援：大都市に加え、各地域にも情報が行き渡るための環境整備

＜主な取組＞サイバー犯罪等の被害防止を目的としたセミナー等の実施、関西サイバーセキュリティ・ネットワークにおける産学官連携型の取組活性化、高専学生によるボランティア活動等のベストプラクティスの共有、民間の取組による能力検定や講師間の交流促進

(3) 情報発信・相談窓口の充実

- 最新の脅威の情報・対策を適時かつ迅速に発信することや、専門的な内容を相談できる窓口を確保することで、国民や企業・団体が自ら最新の取組を行える環境を整備することが重要である。

5 連携体制の強化

- N I S Cをはじめとした関係機関が連携し、各機関の役割や対象を位置付けて、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、互いに連携・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。
- 個人や企業の対策の実施状況等を分析し、本プログラムの内容・効果を定期的に評価するとともに、必要に応じて本プログラム自体の見直しを実施する。

①ポータルサイトによる取組の見える化及び連携推進

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、官民の取組を隨時追加するとともに、必要に応じ、関係者と連携して取組の強化を図る。

②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。

③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。

④国際的な連携の強化

国際的かつ先進的な取組との連携や、ASEAN諸国へのツール・コンテンツの提供などの協力を実施していく。

⑤P D C Aによる継続的な改善

個別施策の実施状況に加え、個人・企業における被害や具体的対策の実施状況等を分析し、今後注力すべき対象や取組を精査・明確化するなど、本プログラム自体の内容及び効果についても定期的に評価を行うことにより、P D C Aサイクルを回していく。

(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～

2019年〇月〇日
サイバーセキュリティ戦略本部

目次

1 はじめに	2
2 現状	3
(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	3
① 個人の状況	3
② 企業の状況	6
(2) 官民の取組状況	8
① セミナー・イベント	8
② ツール・コンテンツの提供	8
③ タイムリーな情報発信	8
参考 諸外国における取組の例	11
(1) 米国における取組	11
(2) 英国における取組	11
3 今後の取組の基本的な考え方	13
(1) 個人・組織における「自覚・行動」の促進	13
(2) 「3つの視点」からの取組の推進	13
4 具体的取組の推進	16
(1) 基本的な対策の徹底	16
(2) 重点的な対象とその内容	16
① 中小企業	17
② 若年層	18
③ 地域における取組の支援	21
(3) 情報発信・相談窓口の充実	22
5 連携体制の強化	24
参考資料	26

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・パラリンピック競技大会も見据えつつ、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、経済活動や国民生活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。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、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⁴。また、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⁵し、堅調に拡大を続けている⁶。更に、AI

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 「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）代表的なFinTechサービスの例より（参考5）

⁶ 「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

が搭載された家庭用スピーカーを始めとして、家庭向けの IoT 機器の普及も見込まれている⁷。

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し、国民の「生活」へ浸透するのに伴い、国民のサイバー空間に対する不安感も拡大を続けている。具体的には、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⁸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。また、実際にインターネット利用者を標的とした攻撃も近年増加している。例えば、フィッシングサイトへ誘導された国内のインターネット利用者の数は、2018年上半期では290万人を超えており、前期比で2.7倍と急激に増加している⁹。

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¹⁰。更に、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¹¹。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。

省)電子マネー決済額より（参考6）

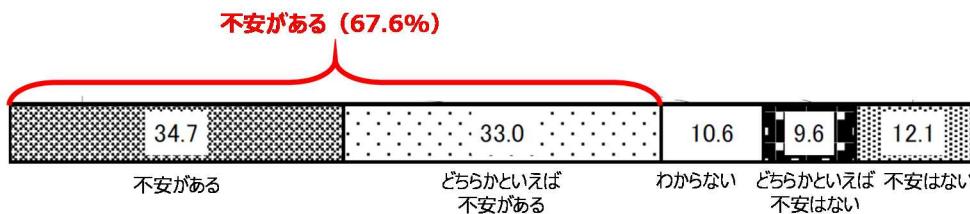
⁷ 「Forrester Data:Smart Home Devices Forecast, 2017 To 2022(US)」（2017年10月 Forrester）より（参考7）

⁸ 「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8）

⁹ 「2018年上半期セキュリティラウンドアップ クラウド時代の認証情報を狙いフィッシング詐欺が急増」（2018年9月 トレンドマイクロ株式会社）（参考9）

¹⁰ 「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10）

¹¹ 「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11）



(参考) インターネット利用に対する不安感に関する過去の調査結果

	該当者数	不安がある (小計)	不安はない (小計)			わからない		
			不安がある	どちらかとい えば不安が ある	どちらかとい えば不安は ない	不安はない	%	%
	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¹²

(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）)

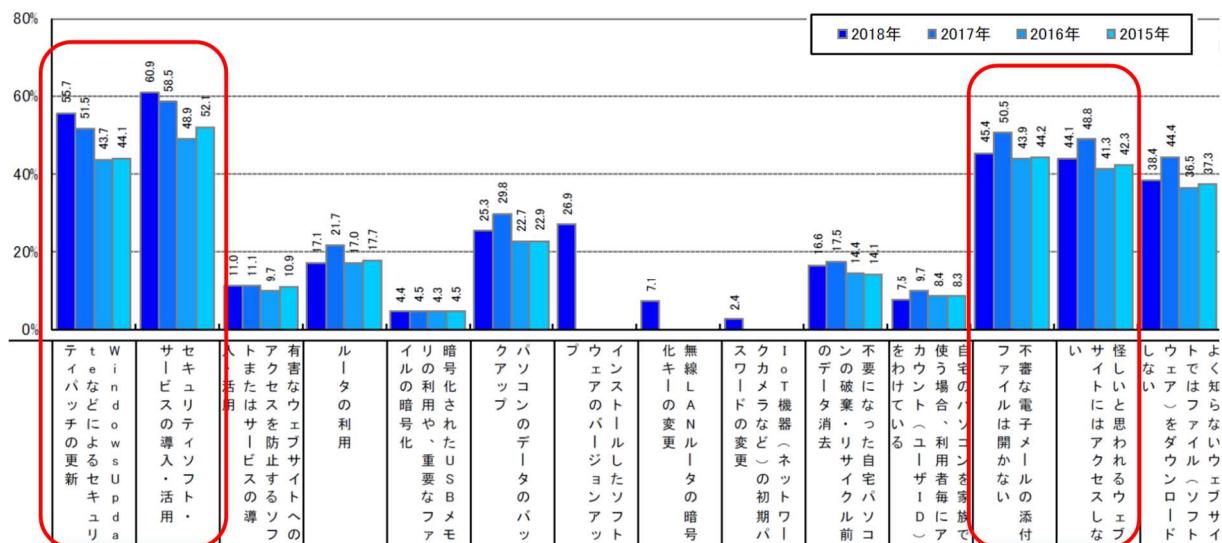


図2 セキュリティ対策の実施状況

(出典：2018年度情報セキュリティの脅威に対する意識調査

(2018年12月 独立行政法人情報処理推進機構(IPA)))

¹² 「不安感がある（小計）」と回答した割合は、2007年11月調査では45.4%、2015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、業種間で取組にはらつきが見られる状況である¹³。

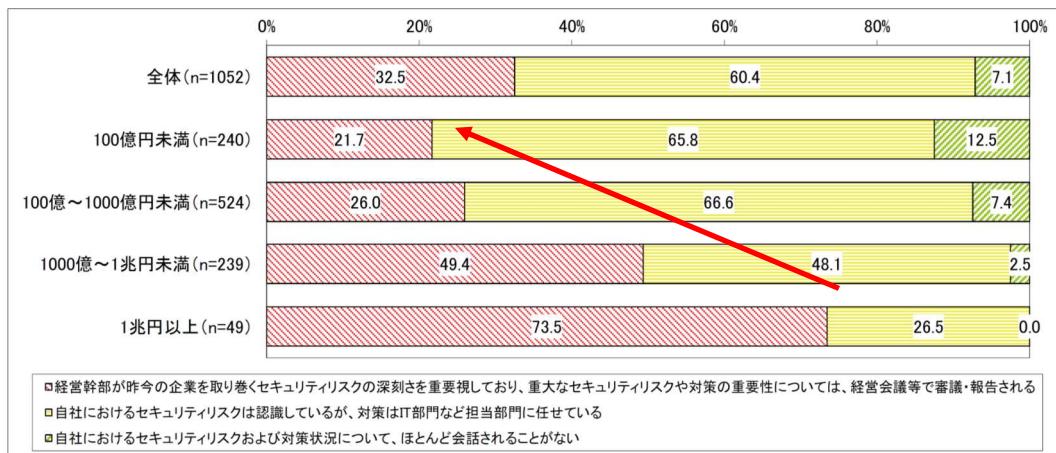


図3 経営幹部の情報セキュリティへの関与度合い（売上高別）

（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¹⁴。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¹⁵。

企業における被害の拡大も見られており、例えば、主に企業を狙ったビジネスメール詐欺（BEC：Business E-mail Compromise）犯罪については、2013年10月から2018年5月の間で累計約8万件、損失額は約125億ドルまで増

¹³ 「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12）

¹⁴ 「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13）

¹⁵ 「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14）

加するなど、世界的に拡大している¹⁶。

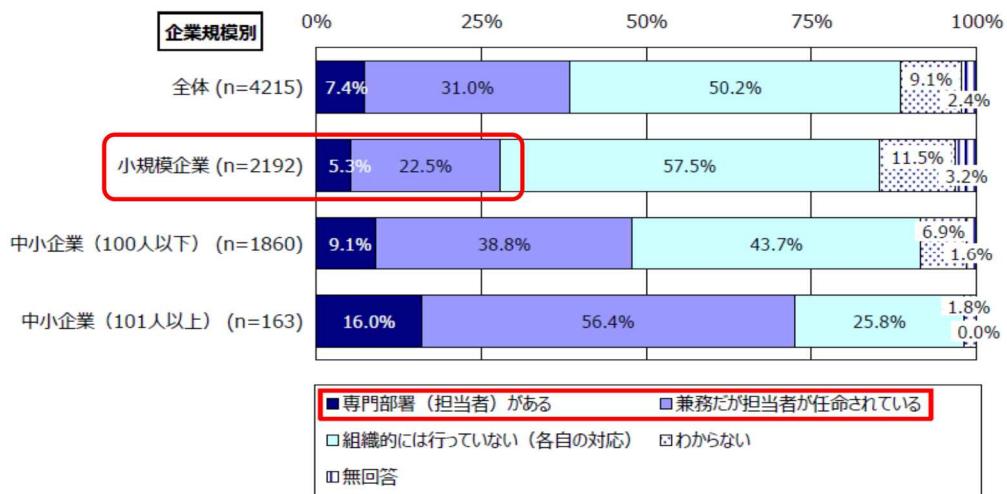


図4 情報セキュリティに係る専門部署または担当者の有無

(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、2018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¹⁷ほか、経営層を対象としたトップセミナーを開催している。また、中小企業においても、セキュリティ対策について自己宣言する制度「SECURITY ACTION」の登録事業者数の増加が見られる¹⁸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。

¹⁶ 「BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM」(2018年7月 米国連邦捜査局(FEDERAL BUREAU OF INVESTIGATION))

¹⁷ 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>

¹⁸ 2018年12月31日時点で、約6万7千の事業者が自己宣言を行っている。(出典：IPA「SECURITY ACTION 取組紹介」：<https://www.ipa.go.jp/security/security-action/activity/index.html>)

(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（NISC）を中心となって「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¹⁹。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。更に、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²⁰。

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²¹。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、緊急情報を隨時発信している²²。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。

¹⁹ サイバーセキュリティ月間：<https://www.nisc.go.jp/security-site/month/index.html>

²⁰ 情報セキュリティ安心相談窓口：<https://www.ipa.go.jp/security/anshin/index.html>

²¹ 情報セキュリティハンドブック：<https://www.nisc.go.jp/security-site/handbook/index.html>

²² 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ていくとともに、それぞれの取組が、ターゲットとする層に対して、具体的に、どの程度の規模で実施され、また、どのような効果を達成しているのかという点にも留意しつつ、全体としての取組を俯瞰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

対象 手法	個人			組織				民間における取組 公的機関における取組					
	若年層	就労世代	高齢者	小規模企業者	中小企業	大企業	教育機関						
セミナー、イベント等	サイバーセキュリティ月間イベント (NISC)			各地におけるイベント等 (警察庁、都道府県警察)				民間における取組 公的機関における取組					
	サイバーセキュリティセミナー等の開催 (総務省)												
	電子署名及びトラストサービスに関する普及啓発 (総務省、法務省、経済産業省)												
	ネットモラルキャラバン隊の実施 (文部科学省)	ひろげよう情報モラル・セキュリティコンクール (経産省、IPA)		中小企業支援機関向け講師派遣 (経済産業省、IPA)		講習能力養成セミナー (経済産業省、IPA)							
		学校教育の情報モラル養成研修 (NITS、文部科学省)		JPCERT/CCによる情報共有会 (経済産業省)		インターネット安全教室 (経済産業省、IPA、JNSA)							
		インターネット安全教室 (経済産業省、IPA)		フィッシング対策セミナー (経済産業省、フィッシング対策協議会、JPCERT/CC)		関西におけるサイバーセキュリティ人材育成、意識醸成 (近畿経済産業局、近畿総合通信局、関西情報センター)							
	e-ネットキャラバン (FMMC、総務省、文部科学省)		セミナー、研修、勉強会、演習の開催 (JASA)		JC3フォーラム (JC3)		JC3フォーラム (JC3)						
	標語募集 (FMMC、総務省、文部科学省)		JC3フォーラム (JC3)		経営トップセミナー、経営宣言 (経団連)								
	情報セキュリティソーター・マイスターの育成、ミーティング (SPREAD)		JC3フォーラム (JC3)		トップ層会合 (CRIC CSF)								
	全国大会 (Grafsec)		セミナーやイベント、コンテスト開催 (JNSA)		セミナーやイベント、コンテスト開催 (JNSA)								
	地域の各団体によるイベントや勉強会の開催 (Grafsec助成事業)		制御システムセキュリティカンファレンス (JPCERT/CC)		セミナーやイベント、コンテスト開催 (JNSA)								
	学生向けセミナー (CRIC CSF)		セミナーやイベント、コンテスト開催 (JNSA)		セミナーやイベント、コンテスト開催 (JNSA)								
ツール・コンテンツ提供	情報セキュリティハンドブック (NISC)		Wi-Fi利用者向け簡単マニュアル (総務省)		情報漏えい対策ツールの提供 (経済産業省、IPA)		JC3フォーラム (JC3)						
	情報セキュリティハンドブック (NISC)		Wi-Fi利用者向け簡単マニュアル (総務省)		情報漏えい対策ツールの提供 (経済産業省、IPA)								
	情報セキュリティハンドブック (NISC)		Wi-Fi利用者向け簡単マニュアル (総務省)		情報漏えい対策ツールの提供 (経済産業省、IPA)								
	情報セキュリティハンドブック (NISC)		Wi-Fi利用者向け簡単マニュアル (総務省)		情報漏えい対策ツールの提供 (経済産業省、IPA)								
	情報セキュリティハンドブック (NISC)		Wi-Fi利用者向け簡単マニュアル (総務省)		情報漏えい対策ツールの提供 (経済産業省、IPA)								
	情報セキュリティハンドブック (NISC)		Wi-Fi利用者向け簡単マニュアル (総務省)		情報漏えい対策ツールの提供 (経済産業省、IPA)								
	情報セキュリティハンドブック (NISC)		Wi-Fi利用者向け簡単マニュアル (総務省)		情報漏えい対策ツールの提供 (経済産業省、IPA)								
	情報セキュリティハンドブック (NISC)		Wi-Fi利用者向け簡単マニュアル (総務省)		情報漏えい対策ツールの提供 (経済産業省、IPA)								
	情報セキュリティハンドブック (NISC)		Wi-Fi利用者向け簡単マニュアル (総務省)		情報漏えい対策ツールの提供 (経済産業省、IPA)								
	情報セキュリティハンドブック (NISC)		Wi-Fi利用者向け簡単マニュアル (総務省)		情報漏えい対策ツールの提供 (経済産業省、IPA)								
タイムリーな情報発信・相談窓口	SNSを用いた情報発信 (NISC)		サイバー犯罪に関する相談窓口 (都道府県警察)		@police (警察庁)		JC3フォーラム (JC3)						
	SNSを用いた情報発信 (NISC)		サイバー犯罪に関する相談窓口 (都道府県警察)		@police (警察庁)								
	@police (警察庁)		@police (警察庁)		標的型サイバーアクション特別相談窓口/サイバースキュー隊 (J-CRAT) (経済産業省、IPA)								
	サイバー犯罪対策サイト (警察庁)		SECURITY ACTION メールニュース (経済産業省、IPA)		SECURITY ACTION メールニュース (経済産業省、IPA)								
	情報セキュリティ安心相談窓口 (経済産業省、IPA)		SECURITY ACTION メールニュース (経済産業省、IPA)		SECURITY ACTION メールニュース (経済産業省、IPA)								
	情報セキュリティ安心相談窓口 (経済産業省、IPA)		SECURITY ACTION メールニュース (経済産業省、IPA)		SECURITY ACTION メールニュース (経済産業省、IPA)								
	情報セキュリティ安心相談窓口 (経済産業省、IPA)		SECURITY ACTION メールニュース (経済産業省、IPA)		SECURITY ACTION メールニュース (経済産業省、IPA)								
ツール・コンテンツ提供	サイバー攻撃に悪用されるIoT機器の利用者への注意喚起、周知広報 (総務省、NICT、電気通信事業者)		インシデント対応 (JPCERT/CC)		早期警戒情報 (JPCERT/CC)		JC3フォーラム (JC3)						
	Web、ブログでの情報発信 (SPREAD)		早期警戒情報 (JPCERT/CC)		web、SNS、メールマガジンでの情報発信 (JNSA)								
	Web、ブログでの情報発信 (SPREAD)		早期警戒情報 (JPCERT/CC)		web、SNS、メールマガジンでの情報発信 (JNSA)								
	Web、ブログでの情報発信 (SPREAD)		早期警戒情報 (JPCERT/CC)		web、SNS、メールマガジンでの情報発信 (JNSA)								
	Web、ブログでの情報発信 (SPREAD)		早期警戒情報 (JPCERT/CC)		web、SNS、メールマガジンでの情報発信 (JNSA)								

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

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.^{23²⁴}」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）²⁵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²⁶。

(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」²⁷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）²⁸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。

²³ Stop.Think.Connect. : <https://www.stopthinkconnect.org/>

²⁴ 日本では、フィッシング対策協議会が2014年2月に「Stop.Think.Connect. Messaging Convention Inc.」と覚書を締結し、活動を実施。2018年12月時点で、国内22団体が参加。「Stop.Think.Connect. 資料ダウンロードセンター」（<https://stopthinkconnect.jp/interest/download/>）において、ツール・コンテンツを提供。

²⁵ 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>

²⁶ NICE : <https://www.nist.gov/itl/applied-cybersecurity/nice>

²⁷ Cyber Aware : <https://www.cyberaware.gov.uk/>

²⁸ NCSC : <https://www.ncsc.gov.uk/>

Cyber Security Small Business Guide

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at www.ncsc.gov.uk/smallbusiness.

Backing up your data

Take regular backups of your important data, and test they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.



Identify what needs to be backed up. Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.

Ensure the device containing your backup is not permanently connected to the device holding the original copy, neither physically nor over a local network.

Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.



Switch on PIN/password protection/fingerprint recognition for mobile devices.

Configure devices so that when lost or stolen they can be tracked, remotely wiped or remotely locked.

Keep your devices (and all installed apps) up to date, using the 'automatically update' option if available.

When sending sensitive data, don't connect to public Wi-Fi hotspots - use 3G or 4G connections (including tethering and wireless dongles) or use VPNs.

Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.



Use antivirus software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.



Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the 'automatically update' option where available.



Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.



Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.



Ensure staff don't browse the web or check emails from an account with Administrator privileges. This will reduce the impact of successful phishing attacks.



Scan for malware and change passwords as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).



Check for obvious signs of phishing, like poor spelling and grammar, or low quality versions of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.



Make sure all laptops, Macs and PCs use encryption products that require a password to boot. Switch on **password/PIN protection** or **fingerprint recognition** for mobile devices.



Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.



Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *password*).



Do not enforce regular password changes; they only need to be changed when you suspect a compromise.



Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.



Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.



Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.



© Crown Copyright 2017

For more information go to www.ncsc.gov.uk [@ncsc](https://twitter.com/ncsc)

図6 NCSCが中小企業向けに作成・公表しているガイド

(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っていた「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。国民一人一人や中小・小規模企業にいたる「ラストワンマイル」まで、情報の丁寧な展開を図っていくため、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更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 繼続的な実施

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²⁹。例えば、若者はSNS、高齢者はマスメディア、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、優秀な人材を育成するため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）。各対象へ向けた裾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。

²⁹ 「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15）

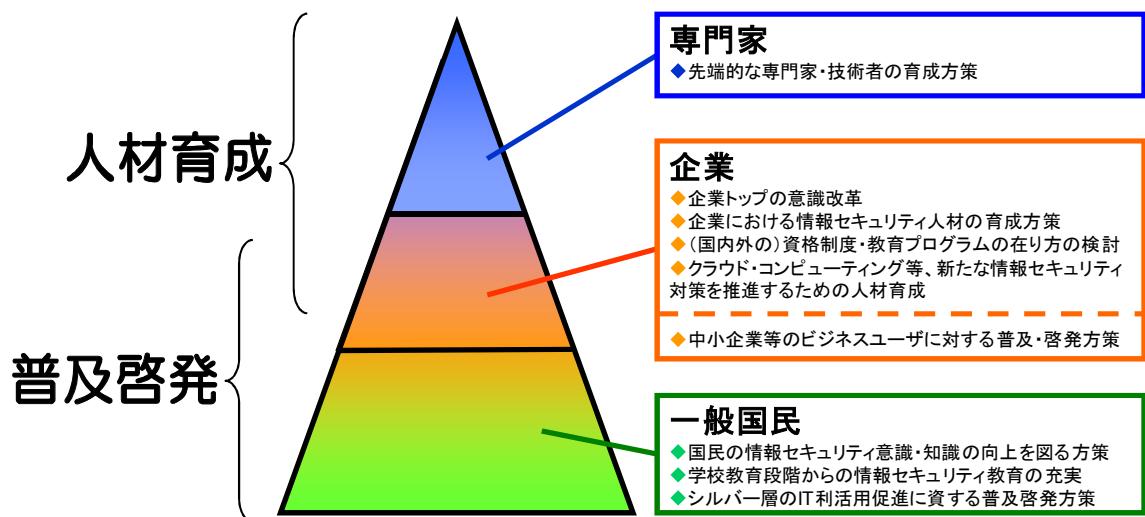


図7 情報セキュリティにおける普及・啓発と人材育成の関係

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. ウィ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³⁰。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、担当者を置くことが難しい企業や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、地域の中小企業支援機関や損害保険会社、ITシルバー人材等の連携により、中小企業のサイバーセキュリティに関するトラブル対応を支援する「サイバーセキュリティお助け隊」を創設するなど、中小企業のニーズに沿ったセキュリティ技術・サービスの地域実証を実施する。（経済産業省、IPA）
- 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導入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

³⁰ 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。

どを通じ、普及を目指す。更に、「SECURITY ACTION」宣言事業者への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）
- 「Stop.Think.Connect Small Business Resources」において、中小企業におけるセキュリティ教育を手助けするパッケージを公表し、対策の強化に繋げる。（National Cyber Security Alliance）

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³¹。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はなく、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ヤラバン隊を引き続き実施する。（文部科学省）
- 家庭や学校からインターネットにアクセスする一般の利用者を対象に、情報セキュリティに関する基礎知識を学習できるセミナー「インターネット安全教室」を、全国各地の民間団体等と協力して引き続き実施する。（経済産業省、IPA）

³¹ 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16）

- 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：FM MC）、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、IPA、一般社団法人セキュリティキャンプ協議会）
- 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、地域の中小企業支援機関や損害保険会社、ITシルバー人材等の連携により、中小企業のサイバーセキュリティに関するトラブル対応を支援する「サイバーセキュリティお助け隊」を創設するなど、中小企業のニーズに沿ったセキュリティ技術・サービスの地域実証を実施する。（経済産業省、IPA）（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ト能力検定」・「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、「サポートーズミーティング」を開催し、地域で活動するセン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「@police³²」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³³。（警察庁）
- 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る IoT 機器の利用者に注意喚起をするため、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³⁴。（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³⁵。（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。

³² @police : <https://www.npa.go.jp/cyberpolice/>

³³ 2017年度は、観測資料、注意喚起等27件を掲載

³⁴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

³⁵ 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。

(1) 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、官民の取組を隨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。

(2) 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。

(3) 「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。

(4) 國際的な連携の強化

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。

(5)PDCA サイクルによる継続的な改善

ポータルサイトに掲載した官民の取組について、その個別の実施状況をフォローすることに加え、サイバー空間における技術・サービスの進展を踏まえた個人・企業における被害や具体的対策の実施状況等を分析し、今後注力すべき対象や取組を精査、明確化するなど、本プログラム自体の内容・効果についても定期的に評価を行うことにより、PDCA サイクルを回していく。

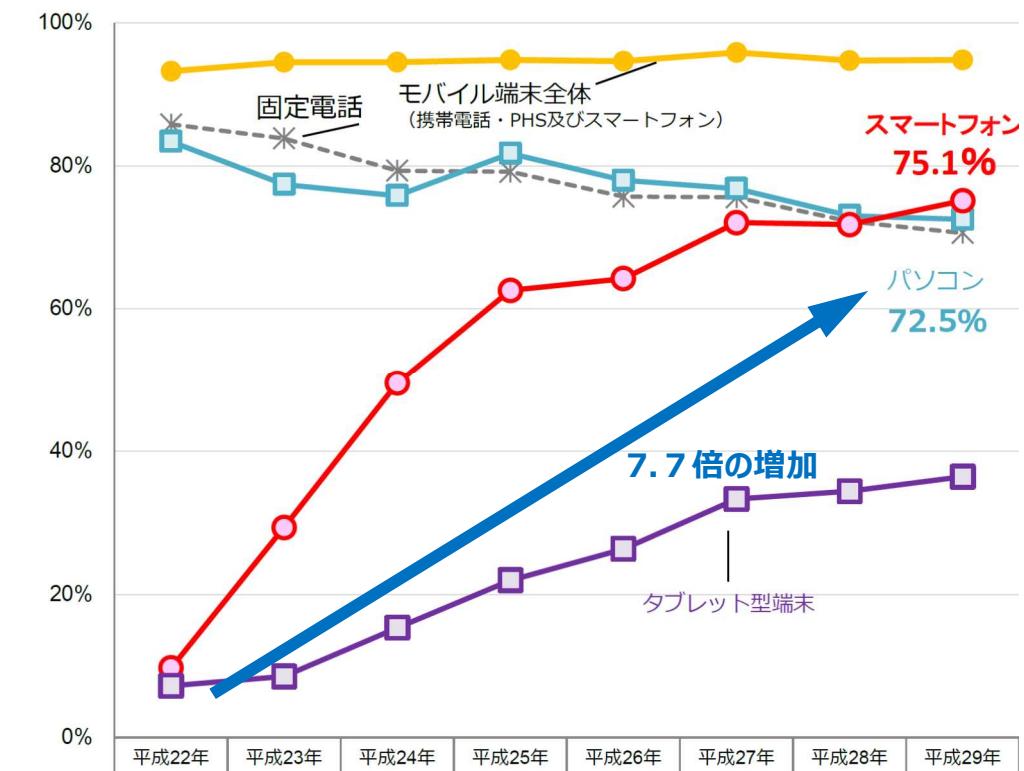
これらの取組により、効率的・効果的な実施体制を構築していく。

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定期的に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。また、上述のとおり、個別施策の実施状況に加えて、本プログラムの内容・効果についても定期的に評価を行い、必要に応じてプログラム自体の見直しを実施することとする。

参考資料

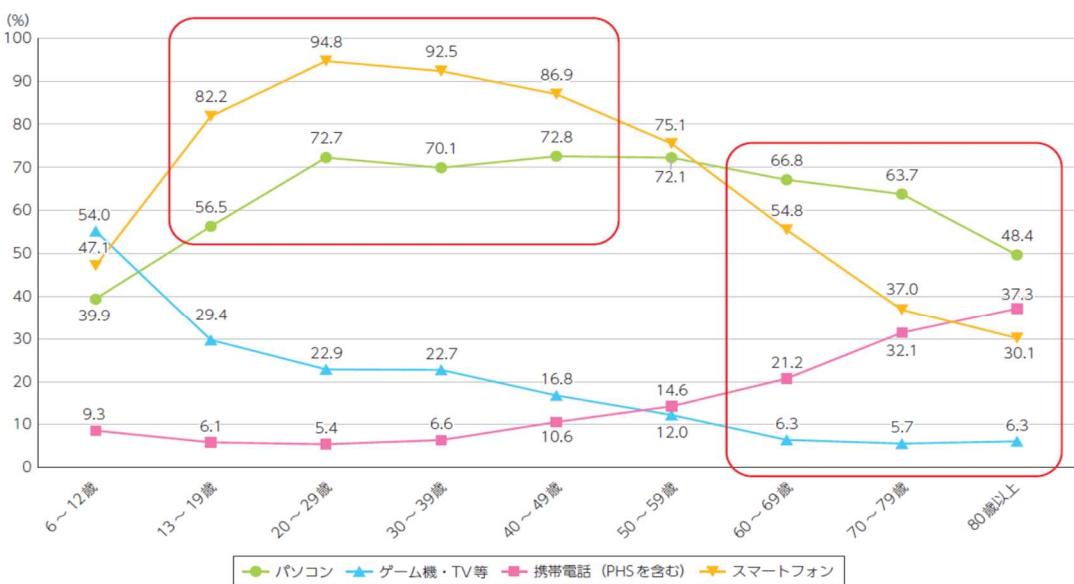
(参考1) 国内における情報通信機器の保有状況推移（世帯）

(出典：平成29年通信利用動向調査（2018年5月 総務省))



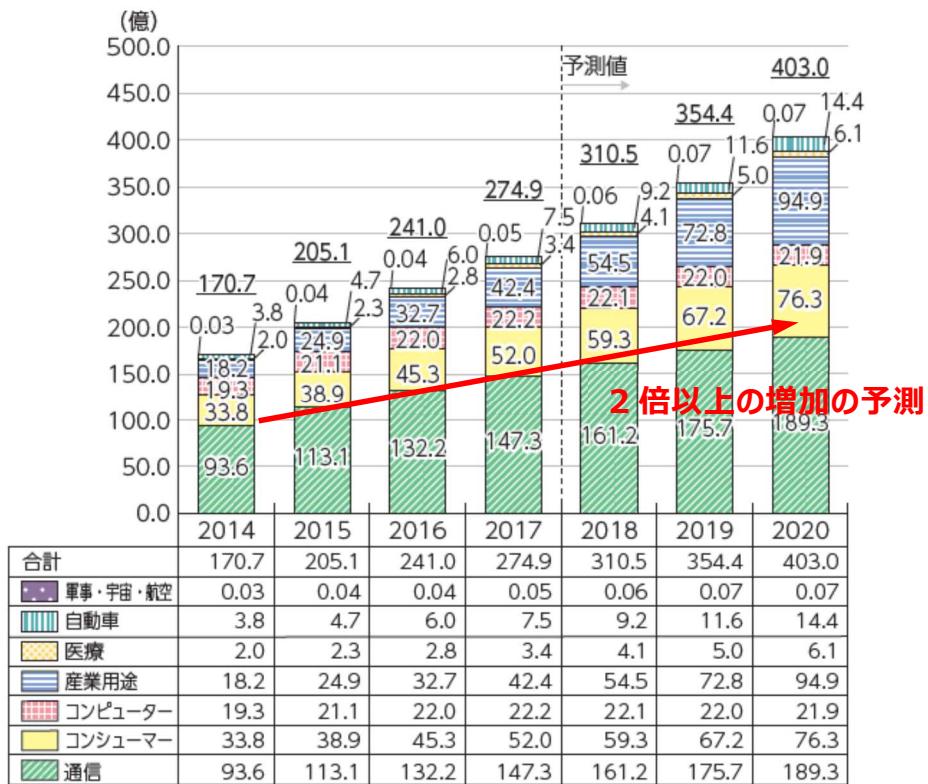
(参考2) インターネット接続端末（世帯）

(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

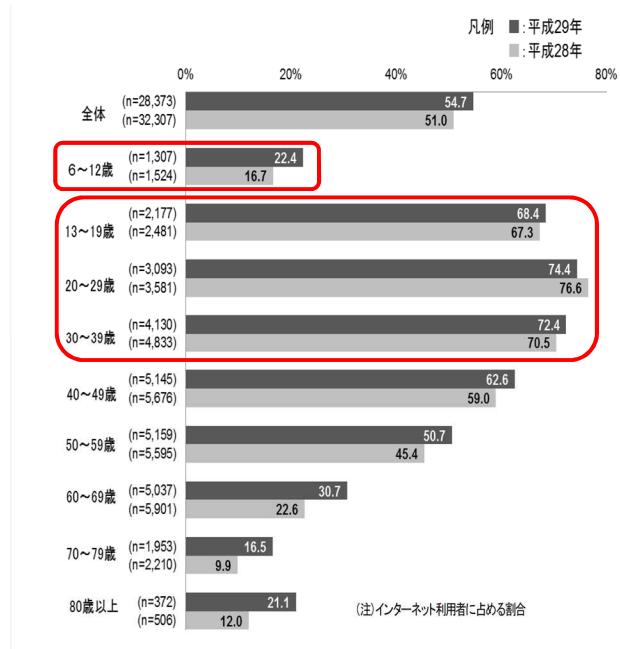
(出典：平成30年版情報通信白書（2018年7月 総務省）)



※「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) 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5) 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6) 電子マネー決済額の推移

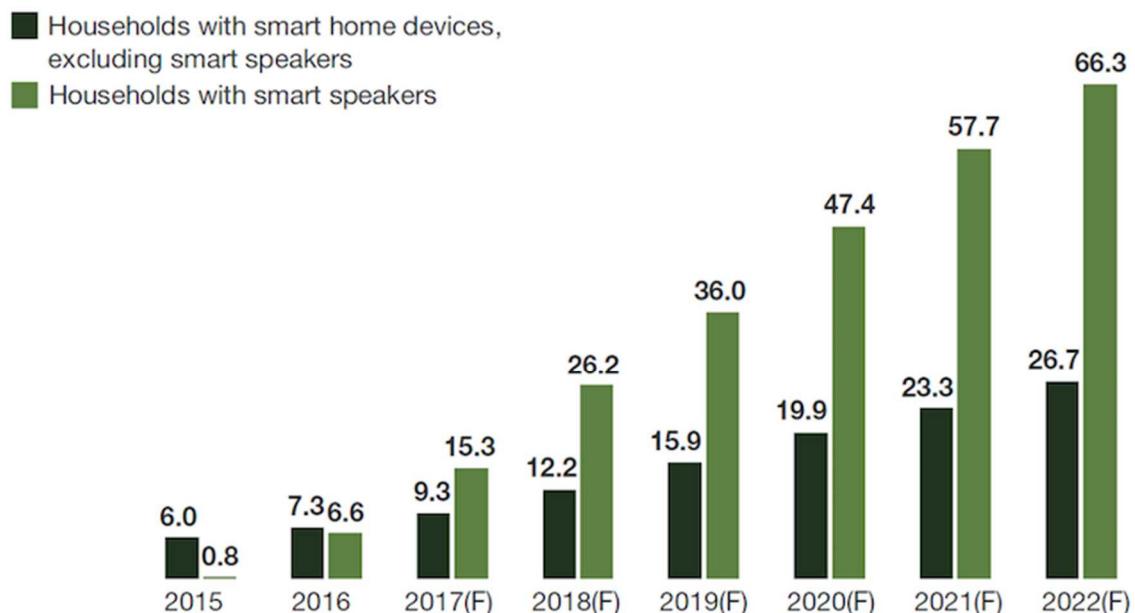
(出典：ICTによるイノベーションと新たなエコノミー形成に関する調査研究（2018年3月 総務省）)



(参考7)

家庭向け IoT 機器の普及予測 ※単位は百万世帯

(出典：Forrester Data:Smart Home Devices Forecast, 2017 To 2022(US) (2017年10月 Forrester))



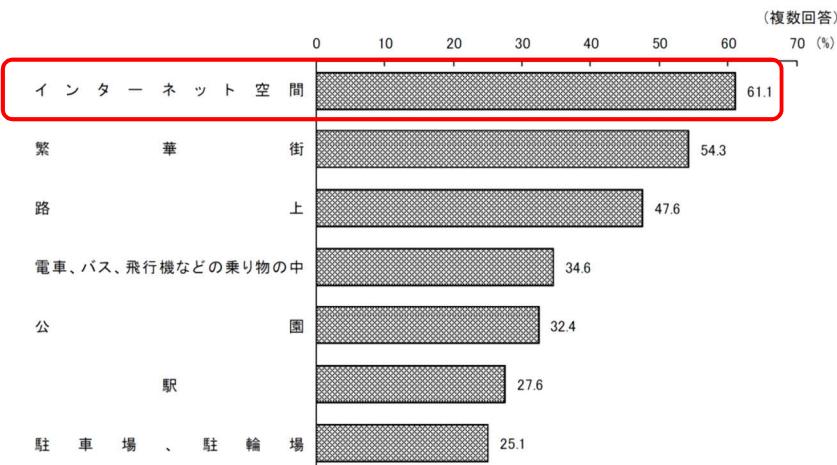
F = Forecast

Source: Forrester Data: Smart Home Devices Forecast, 2017 To 2022 (US)

(参考8)

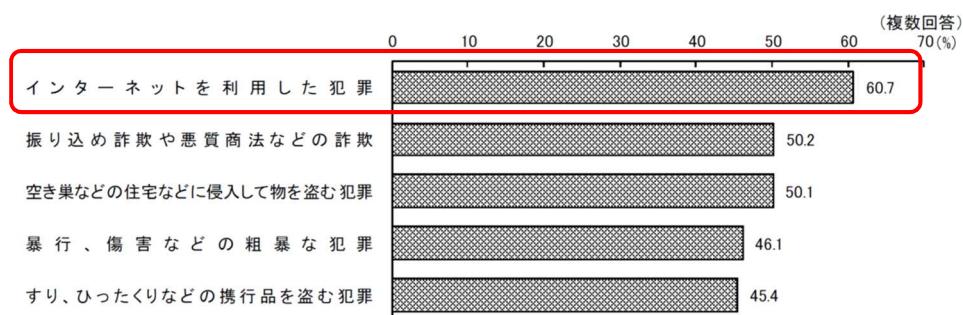
不安を感じる場所

(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

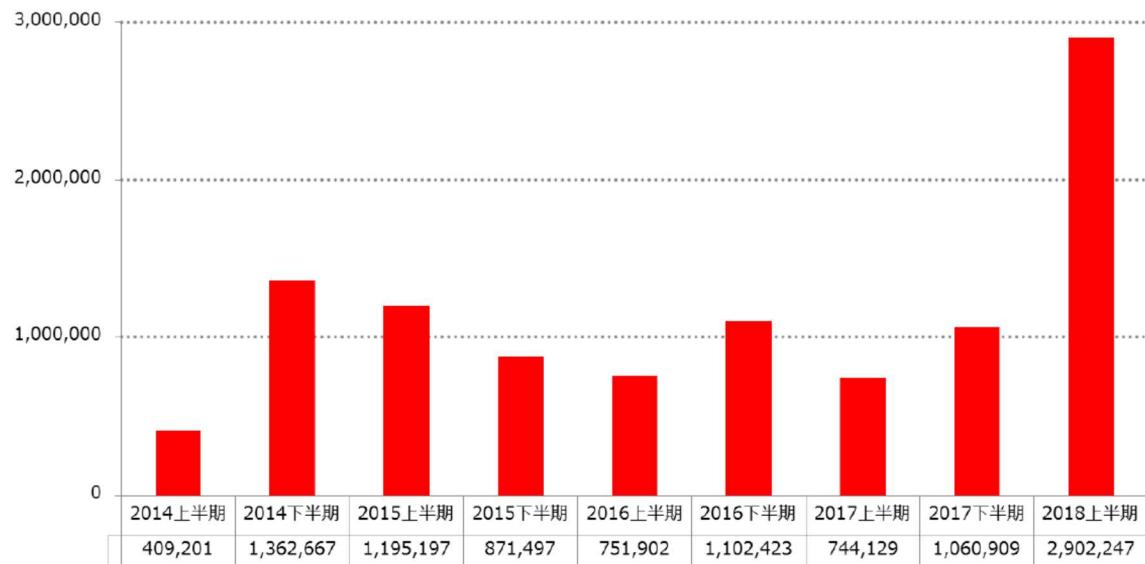
(出典：治安に関する世論調査（2017年11月 内閣府）)



(参考9)

日本国内からフィッシングサイトへ誘導された利用者数の推移

(出典：2018年上半期セキュリティラウンドアップ クラウド時代の認証情報を狙いフィッシング詐欺が急増（2018年9月 トレンドマイクロ株式会社）)



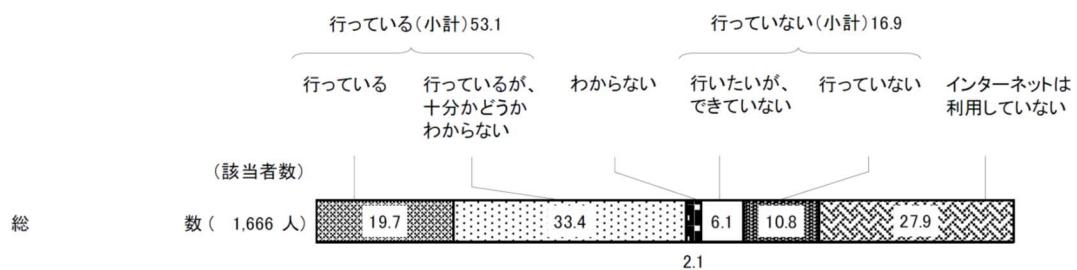
2018年上半期に公表された法人におけるクラウドメールサービス被害一覧

(出典：2018年上半期セキュリティラウンドアップ クラウド時代の認証情報を狙いフィッシング詐欺が急増（2018年9月 トレンドマイクロ株式会社）)

公表月	業種／業界	被害内容
4月	教育	スパムメール送信
4月	教育	スパムメール送信
5月	教育	情報漏えい
5月	教育	情報漏えい
6月	教育	情報漏えい
6月	金融	情報漏えい・スパムメール送信
6月	教育	情報漏えい
6月	教育	情報漏えい・スパムメール送信
6月	教育	情報漏えい

(参考 10) インターネットを安全・安心に利用するための対策

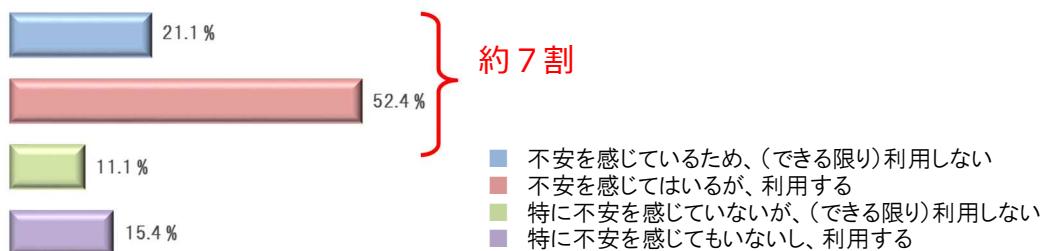
(出典：インターネットの安全・安心に関する世論調査（2018年11月 内閣府))



(参考 11)

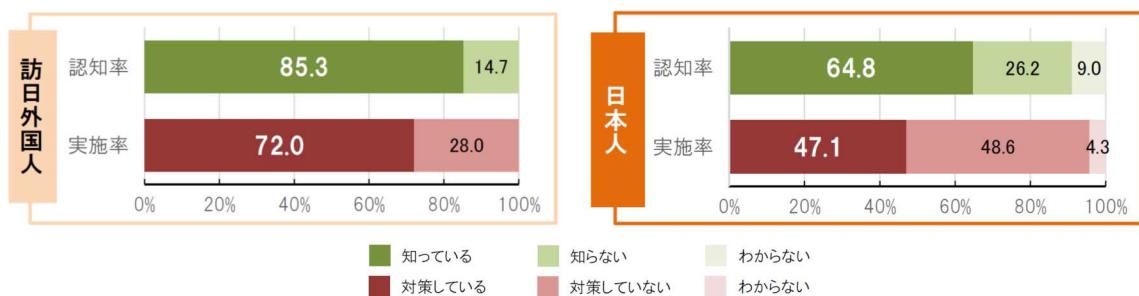
利用者における公衆無線 LAN のセキュリティに対する意識

(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))



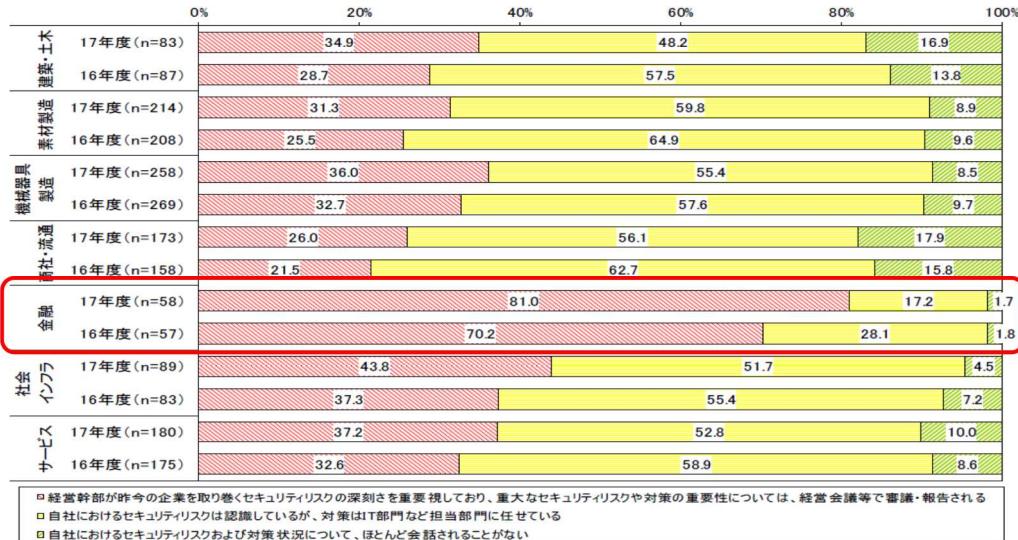
公衆無線 LAN 利用時の脅威の認知率とセキュリティ対策の実施率

(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))



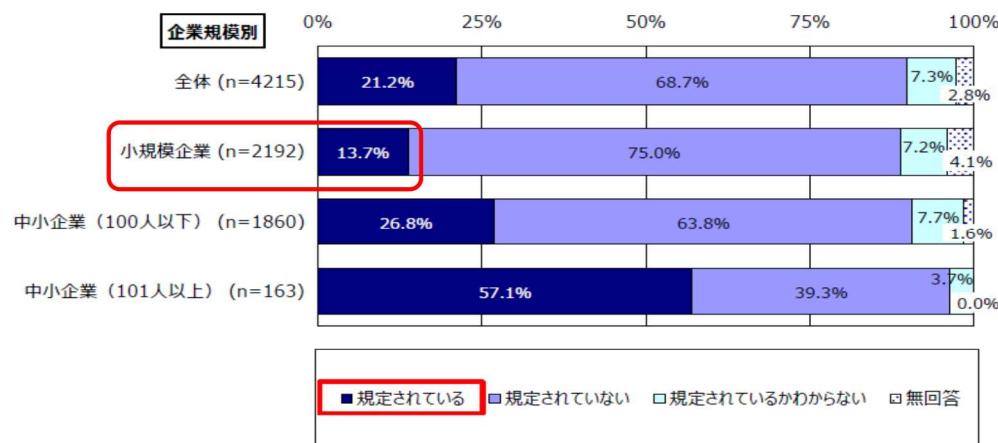
(参考 12) 経営幹部の情報セキュリティへの関与度合い（業種別）

(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)



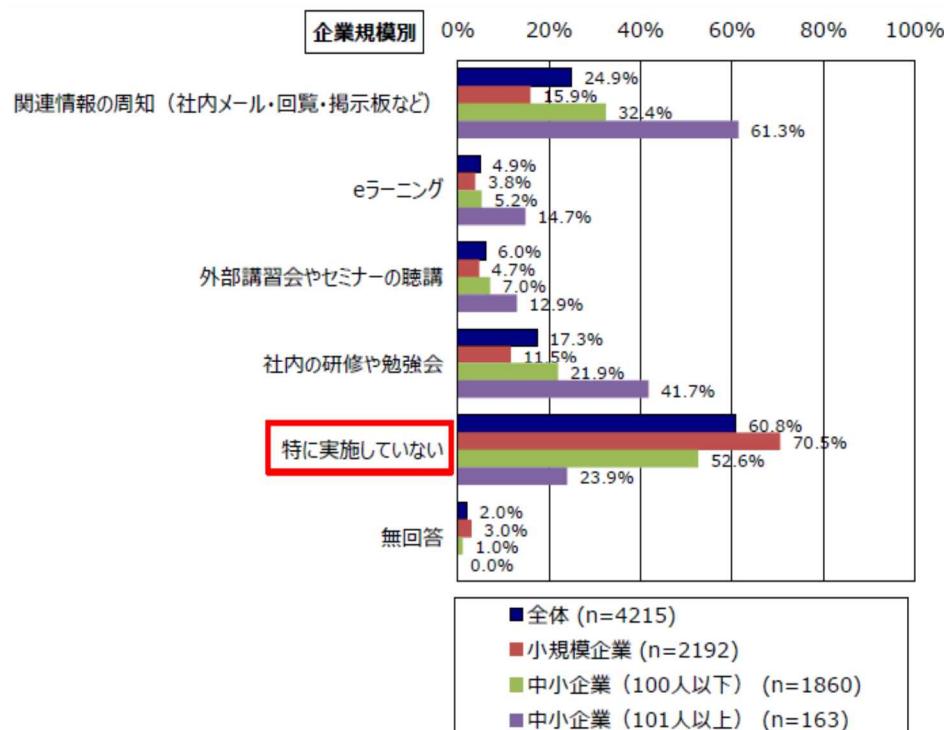
(参考 13) 情報漏えい等への対応方法に関する規定の有無

(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))



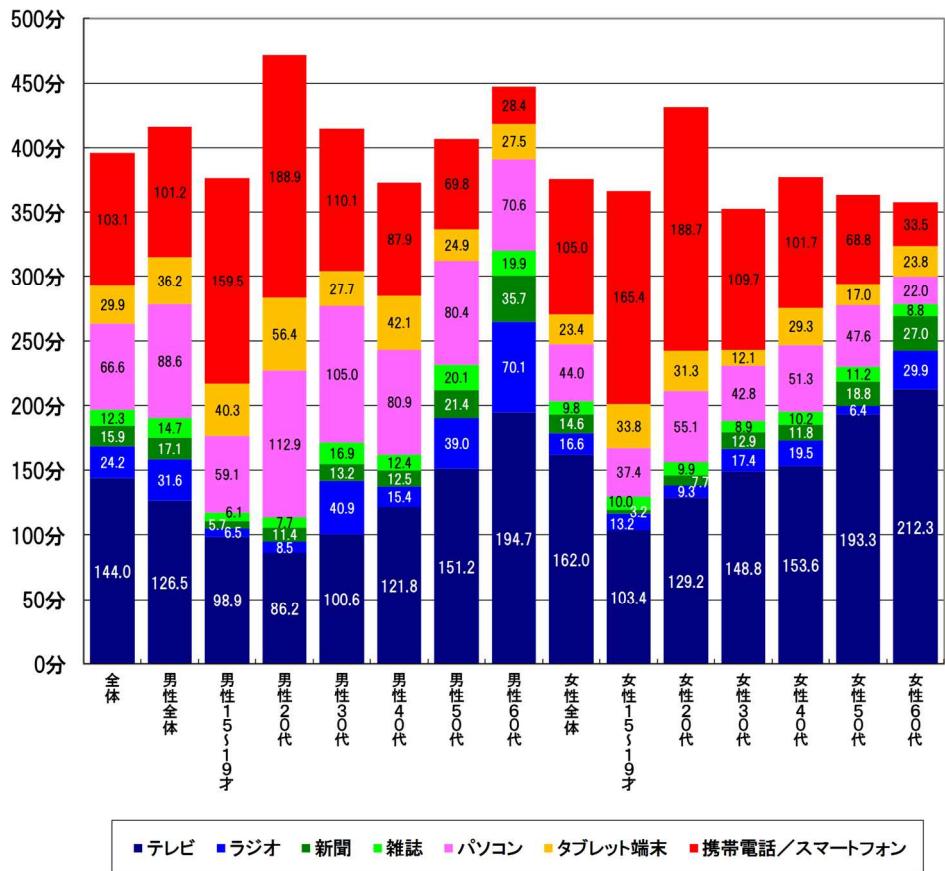
(参考 14) 社内での情報セキュリティ教育の状況

(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 15) 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 16) 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）)

