資料１－１

「サイバーセキュリティ普及啓発アクションプラン」（仮称）の策定について

平成30年10月10日
サイバーセキュリティ戦略本部普及啓発・人材育成専門調査会
内閣サイバーセキュリティセンター（NISC）

新たなサイバーセキュリティ戦略の概要

- 新たなサイバーセキュリティ戦略（平成30年7月閣議決定）は、我が国の基本的な立場等と今後３年間の諸施策の目標及び実施方針を国内外に示すもの。
- 同戦略において、内閣サイバーセキュリティセンター（NISC）が中心となって、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、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を策定することとされている。

サイバーセキュリティ戦略の概要

平成30年７月27日
閣 議 決 定

1 策定の趣旨・背景

- サイバー空間がもたらす人類が経験したことのないパラダイムシフト（Society5.0）
- サイバー空間と実空間の一体化の進展に伴う脅威の深刻化、2020年東京大会を見据えた新たな戦略の必要性

2 サイバー空間に係る認識

- 人工知能（AI）、IoTなど科学的知見・技術革新やサービス利用が社会に定着し、人々に豊かさをもたらしている。
- 技術・サービスを制御できなくなるおそれは常に内在。IoT、重要インフラ、サプライチェーンを狙った攻撃等により、国家の関与が疑われる事案も含め、多大な経済的・社会的損失が生ずる可能性は指数関数的に拡大

3 本戦略の目的

- 基本的な立場の堅持（基本法の目的、基本的な理念（自由、公正かつ安全なサイバー空間）及び基本原則）
- 目指すサイバーセキュリティの基本的な在り方：持続的な発展のためのサイバーセキュリティ（サイバーセキュリティエコシステム）の推進。３つの観点（①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働）からの取組を推進

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
～新たな価値創出を支えるサイバーセキュリティの推進～

- 新たな価値創出を支えるサイバーセキュリティの推進
- 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
- 安全なIoTシステムの構築

国民が安全で安心して暮らせる社会の実現
～国民・社会を守る任務を保証～

- 国民・社会を守るための取組
- 官民一体となった重要インフラの防護
- 政府機関等におけるセキュリティ強化・充実
- 大学等における安全・安心な教育・研究環境の確保
- 2020年東京大会とその後を見据えた取組
- 従来の枠を超えた情報共有・連携体制の構築
- 大規模サイバー攻撃事態等への対処態勢の強化

国際社会の平和・安定及び我が国の安全保障への寄与
～自由、公正かつ安全なサイバー空間の堅持～

- 自由、公正かつ安全なサイバー空間の堅持
- 我が国の防御力・抑止力・状況把握力の強化
- 国際協力・連携

横断的施策

- 人材育成・確保
- 研究開発の推進
- 全員参加による協働

サイバーセキュリティ普及啓発に向けたアクションプランの策定

5 推進体制

内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化を図るとともに、同センターが調整・連携の主導的役割を担う。

戦略策定の趣旨・背景及びサイバー空間に係る認識

中長期

策定の趣旨・背景

【（2015年戦略策定時）連接融合情報社会の到来】
～実空間のヒト・モノがネットワークに**連接**され、
実空間とサイバー空間の**融合**が高度に深化～

一体化

【サイバー空間と実空間の一体化、活動空間の拡張】

サイバー空間に係る認識

・AI、IoT 、Fintech 、ロボティクス、３Dプリンター 、AR/VR など、**サイバー空間における知見や技術・サービスが社会に定着し**、経済社会活動・国民生活の既存構造に変革をもたらす**イノベーションを牽引する一方で、不確実さは常に内在**

サイバー空間がもたらす恩恵

・サイバー空間における技術・サービスが**制御され、様々な分野で当然に利用されており、人々に豊かさをもたらしている。**
・深層学習による**AIの進化**により、既に幅広い産業に応用され始めている。
・**IoT機器で得られるデータ**を利活用した新たなビジネスやサービスが創出されつつある。

サイバー空間における脅威の深刻化

・サイバー空間における技術・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、多大な経済的・社会的な損失が生じ得る。**
・重要インフラサービスの障害やIoT機器の意図しない作動により、様々な**業務・機能・サービス障害が生じた場合、社会に大きな影響が生じ、国家安全保障上の問題**に発展する可能性
・サイバーセキュリティ対策の不備が、**金銭的な損害を直接引き起こし**、拡大することが予想される。

戦略の目指す姿（持続的な発展のためのサイバーセキュリティ　–「サイバーセキュリティエコシステム」の実現- ）

○　新しい価値やサービスが次々と創出されて人々に豊かさをもたらす社会（Society5.0※）の実現に寄与するため、実空間との一体化が進展しているサイバー空間の持続的な発展を目指す（「サイバーセキュリティエコシステム」の実現）。

○　このため、これまでの基本的な立場を堅持しつつ、３つの観点（①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働）から、官民のサイバーセキュリティに関する取組を推進していく。

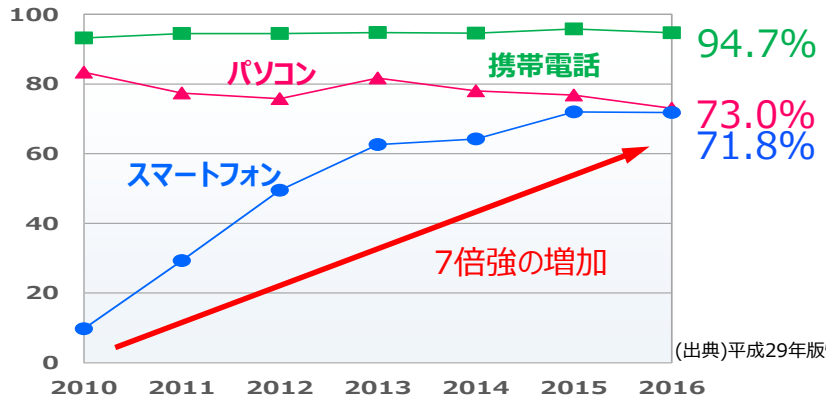
※ 狩猟社会、農耕社会、工業社会、情報社会に続く、人類史上５番目の新しい社会。新しい価値やサービスが次々と創出され、社会の主体たる人々に豊かさをもたらしていく。（未来投資戦略2017より）

＜サイバーセキュリティの基本的な在り方のイメージ＞

個人の状況①（スマートフォン・IoT等の利用状況）

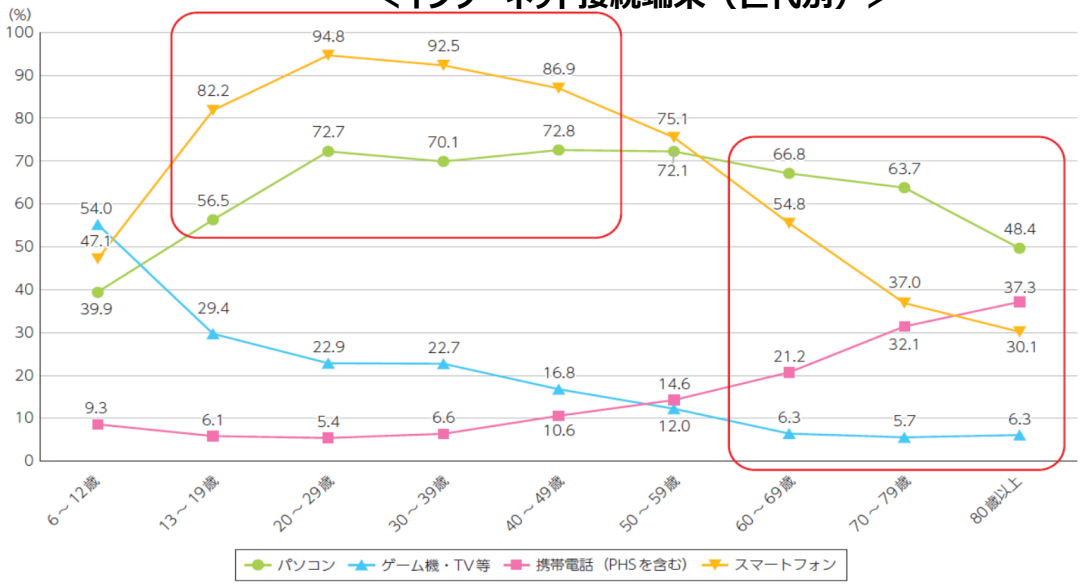
- スマートフォンの普及が進み、2010年から2016年にかけて、世帯保有率は7.4倍の急増。特に、10代～40代は、インターネットへ接続する端末として、スマートフォンを用いる場合が最も多い。
- IoTデバイスも、増加傾向にあり、2020年には約400億個に拡大する見通し。白物・デジタル家電などコンシューマー向けのデバイス数についても、２倍以上に増加するとの予測がされている。

＜国内における情報通信機器の保有状況推移（世帯）＞



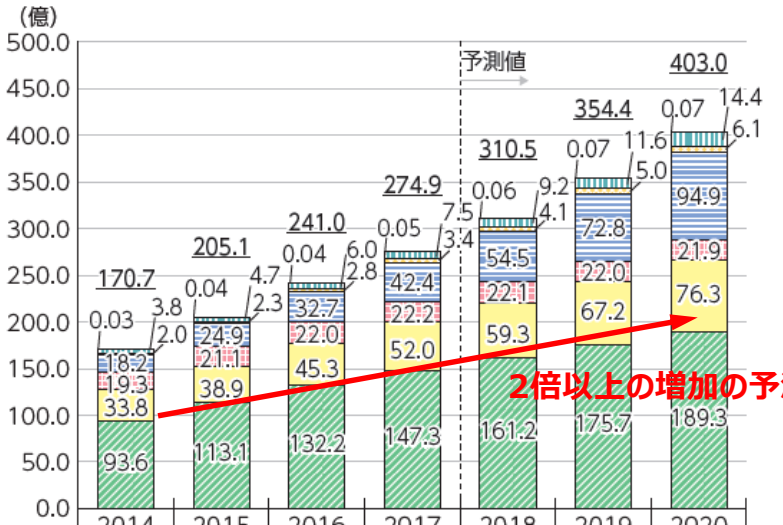
(出典)平成29年版情報通信白書（総務省）

＜インターネット接続端末（世代別）＞



(出典)平成30年版情報通信白書（総務省）

＜世界のIoTデバイス数の推移及び予測＞



	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

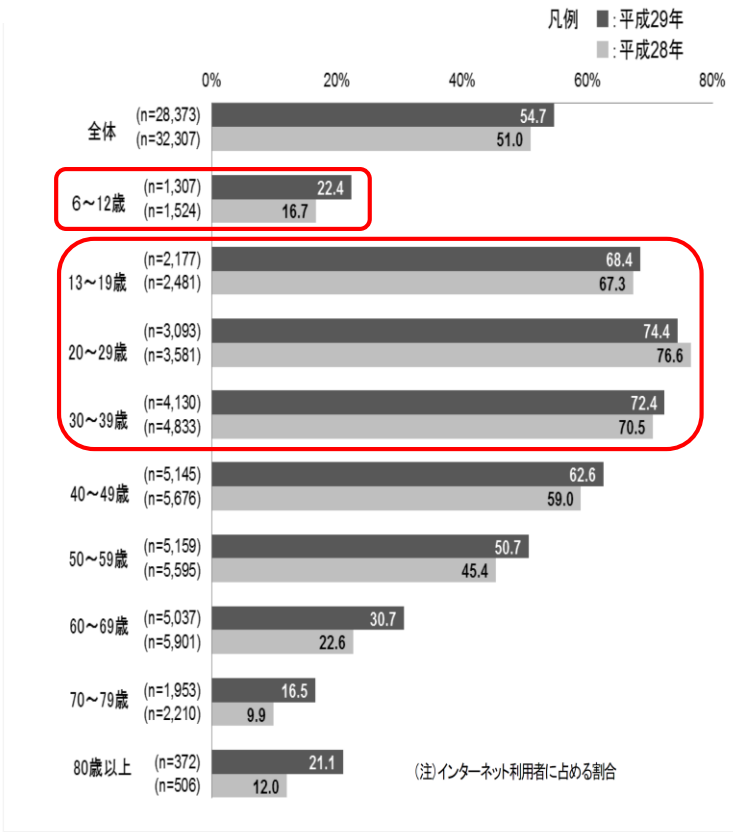
(出典)平成30年版情報通信白書（総務省）　（データはIHS Technology作成）

※「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。

個人の状況②（サービスの利用状況）

- 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。特に中学生～30代の範囲では約7割がSNSを利用。また、小学生についても約２割が利用している。
- 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。電子マネーの決済額も堅調に拡大している。

＜ソーシャルネットワーキングサービスの利用状況＞

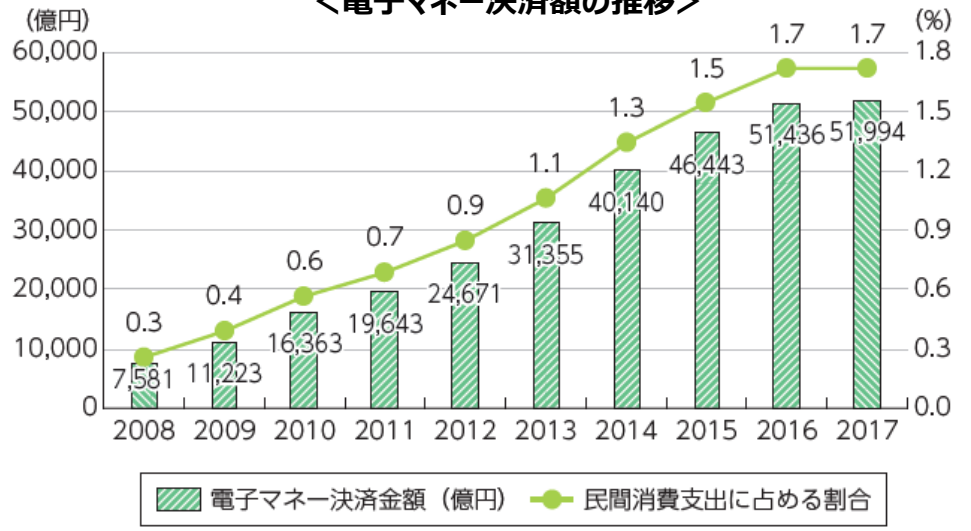


(出典)平成29年版通信利用動向調査（総務省）

＜代表的なFinTechサービスの例＞

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)

＜電子マネー決済額の推移＞

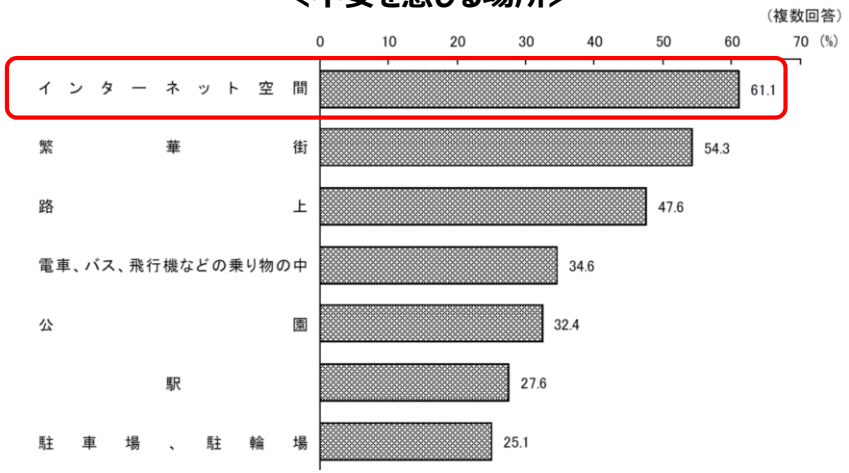


（出典）日本銀行「電子マネー係数」を元に作成

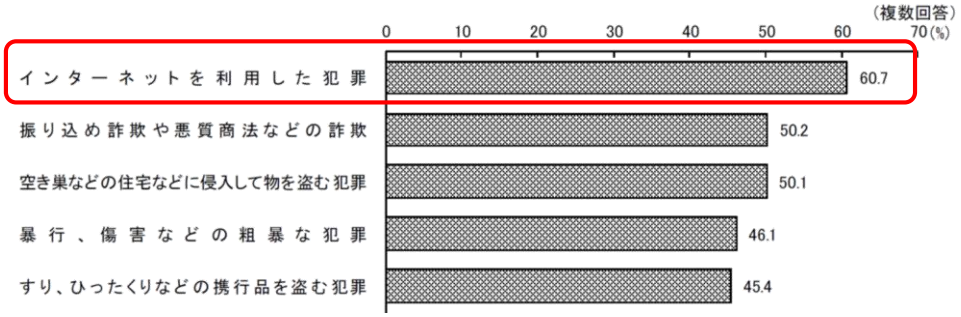
個人の状況③（不安感の増加とセキュリティ対策の状況）

- 「治安に関する世論調査」（平成29年11月）によると、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。
- 個人がセキュリティ対策を実施する割合は増加しているが、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対策を行う割合は、４割～５割台に留まっている。

＜不安を感じる場所＞

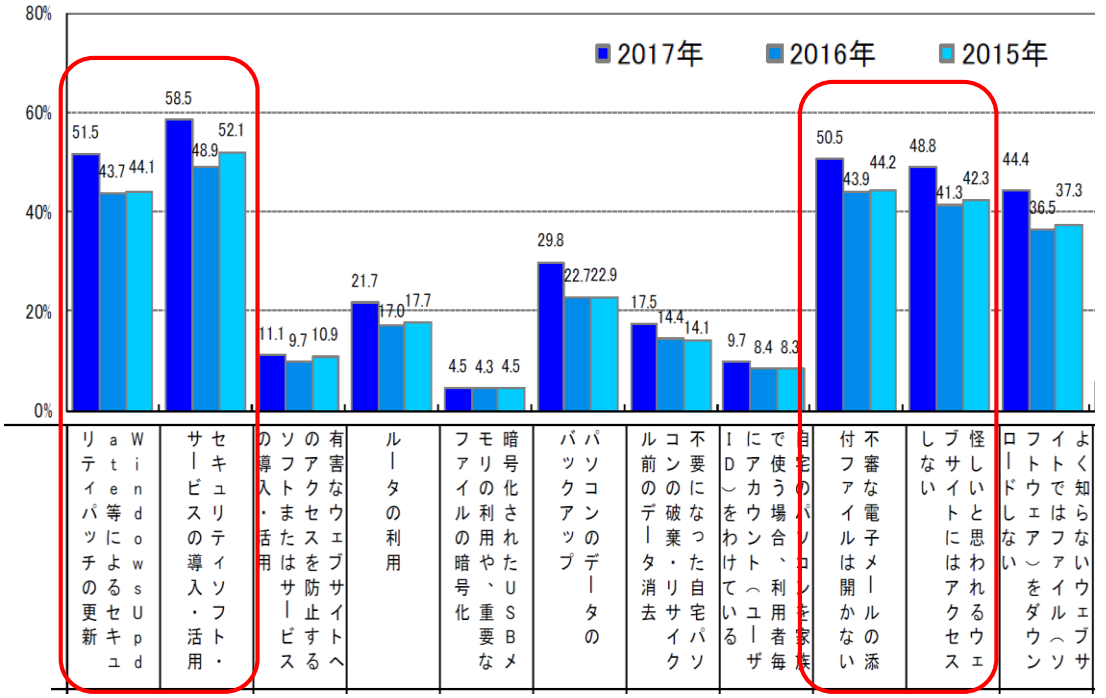


＜不安を感じる犯罪＞



(出典)治安に関する世論調査（内閣府、2017年11月）

＜セキュリティ対策の実施状況＞

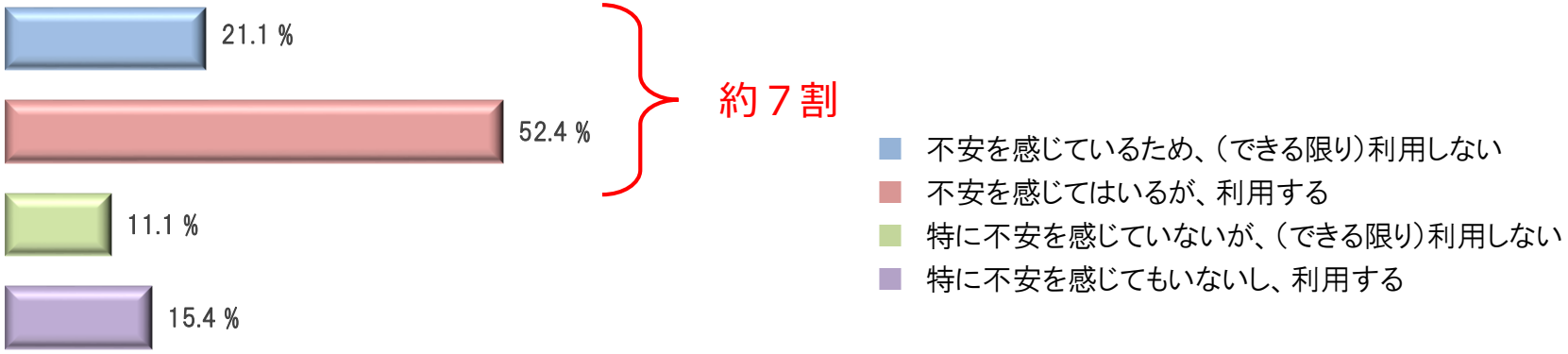


（出典）2017年度情報セキュリティの脅威に対する意識調査（IPA）

個人の状況④（不安感の増加とセキュリティ対策の状況）

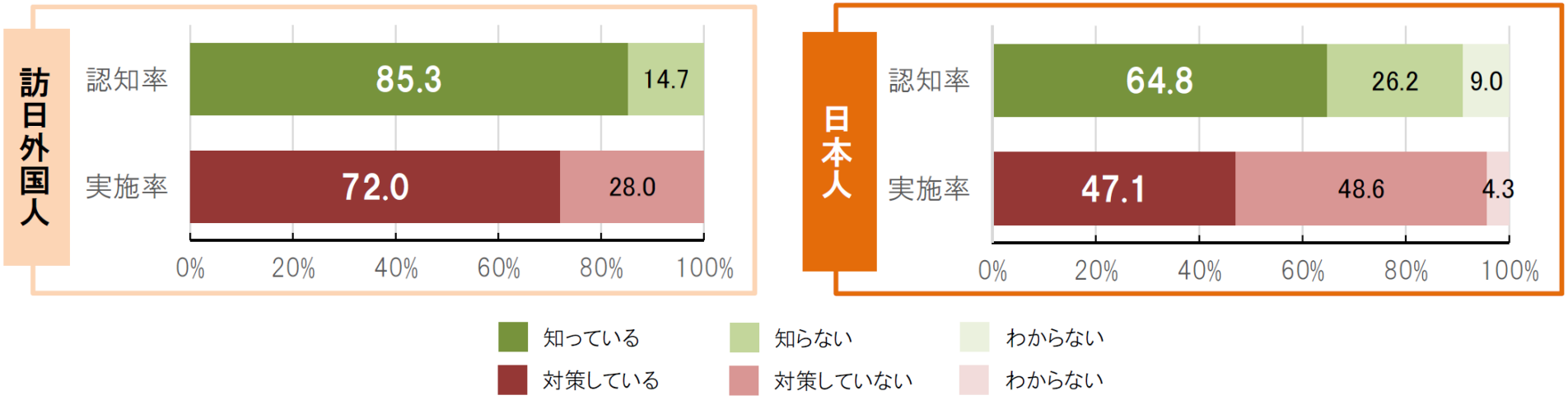
- 公衆無線LANの利用に関しては、脅威の認知率及びセキュリティ対策の実施率については、いずれも訪日外国人の方が、日本人に比べて高い。

＜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)利用者の無線LANサービスに関するセキュリティ意識調査（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＞

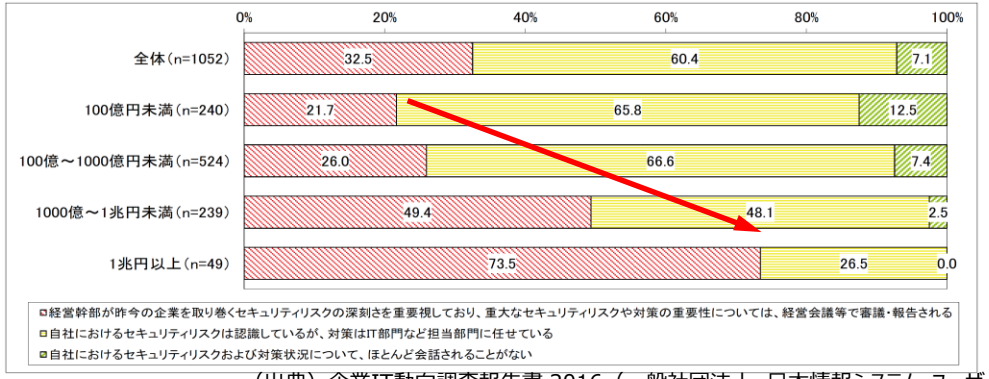


(出典)公衆無線LANセキュリティ分科会報告書（総務省）

企業の状況①（大企業における取組）

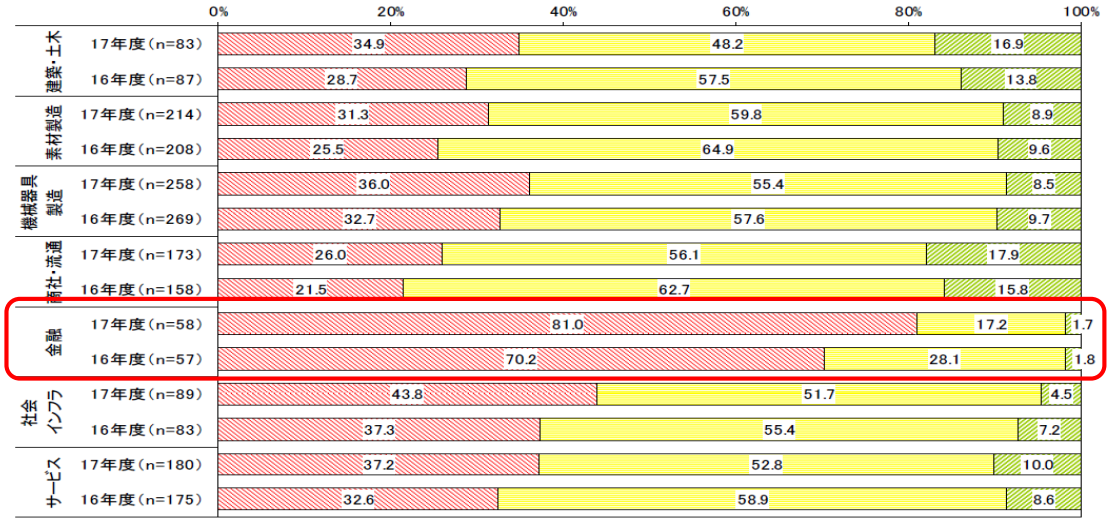
- 売上規模別でみると、売上の高い企業ほど、経営幹部のセキュリティへの関与の度合いが高い。また、業種別では、金融業が最も関与の度合いが高く、約８割の企業でセキュリティ対策の重要性が経営会議等で審議・報告されている。
- 経団連が、今年３月に「経団連サイバーセキュリティ宣言」を公表しているほか、経営層を対象としたトップセミナーを開催するなど、サイバーセキュリティ対策の推進に向けた積極的な取組が進められている。

＜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（一般社団法人　日本情報システム・ユーザー協会）

＜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（一般社団法人　日本情報システム・ユーザー協会）

＜経団連サイバーセキュリティ経営宣言＞

（2018年3月、日本経済団体連合会）

2018 年 3 月

一般社団法人 日本経済団体連合会

最新テクノロジーとデータを活用して社会全体の生産性向上と課題解決を図る「Society 5.0」に向け、あらゆる場面で IT との融合が進む一方、サイバー空間の秩序や安全に脅威を与える、著しい悪意を持った行為も多発している。いまやすべての企業にとって価値創造とリスクマネジメントの両面からサイバーセキュリティ対策に努めることが経営の重要課題となっている。

重要インフラの多くを担い、さまざまな製品やサービスを提供する経済界は、主体的に対策を講じる必要性を強く自覚する。

経済界は、全員参加でサイバーセキュリティ対策を推進し、安心・安全なサイバー空間の構築に貢献する。サイバー攻撃が激化する 2020 年の東京オリンピック・パラリンピック競技大会までを重点取り組み期間として、以下の事項の実践に努めることを宣言する。

1 経営課題としての認識

■経営者自らが最新情勢への理解を深めることを怠らず、サイバーセキュリティを投資と位置づけて積極的な経営に取り組む。
■経営者自らが現実を直視してリスクと向き合い、経営の重要課題として認識し、経営者としてのリーダーシップを発揮しつつ、自らの責任で対策に取り組む。

2 経営方針の策定と意思表明

■特定・防御だけでなく、検知・対応・復旧も重視した上で、経営方針やインシデントからの早期回復に向けた BCP(事業継続計画)の策定を行う。
■経営者が率先して社内外のステークホルダーに意思表明を行うとともに、認識するリスクとそれに応じた取り組みを各種報告書に自主的に記載するなど開示に努める。

3 社内外体制の構築・対策の実施

■予算・人員等のリソースを十分に確保するとともに、社内体制を整え、人的・技術的・物理的等の必要な対策を講じる。
■経営・企画管理・技術者・従業員の各層における人材育成と必要な教育を行う。
■取引先や委託先、海外も含めたサプライチェーン対策に努める。

4 対策を講じた製品・システムやサービスの社会への普及

■製品・システムやサービスの開発・設計・製造・提供をはじめとするさまざまな事業活動において、サイバーセキュリティ対策に努める。

5 安心・安全なエコシステムの構築への貢献

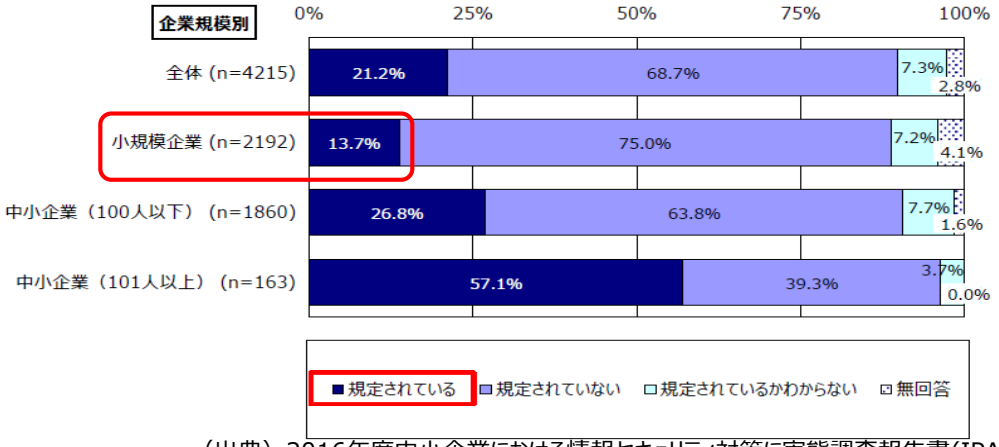
■関係官庁・組織・団体等との連携のもと、各自の積極的な情報提供による情報共有や国内外における対話、人的ネットワーク構築を図る。
■各種情報を踏まえた対策に関して注意喚起することによって、社会全体のサイバーセキュリティ強化に寄与する。

DECLARATION OF CYBER SECURITY MANAGEMENT

企業の状況②（中小企業における取組）

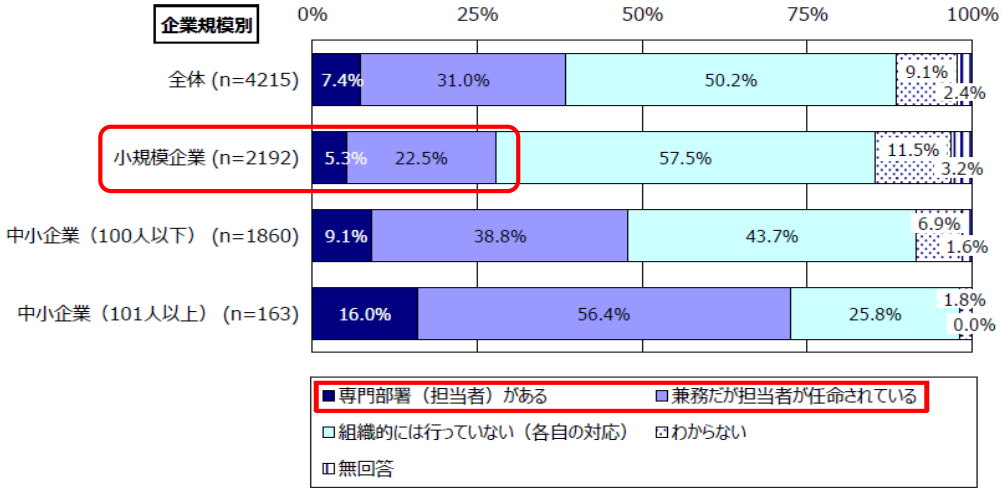
- 中小企業では、特に規模の小さい企業ほど、情報漏えい等への対応方法が規定されていない状況。また、サイバーセキュリティに関する専門部署や担当者が置かれていない場合も多い。
- 社内でのサイバーセキュリティ教育についても、「特に実施していない」との企業が全体の約６割を占める。

＜情報漏えい等への対応方法に関する規定の有無＞



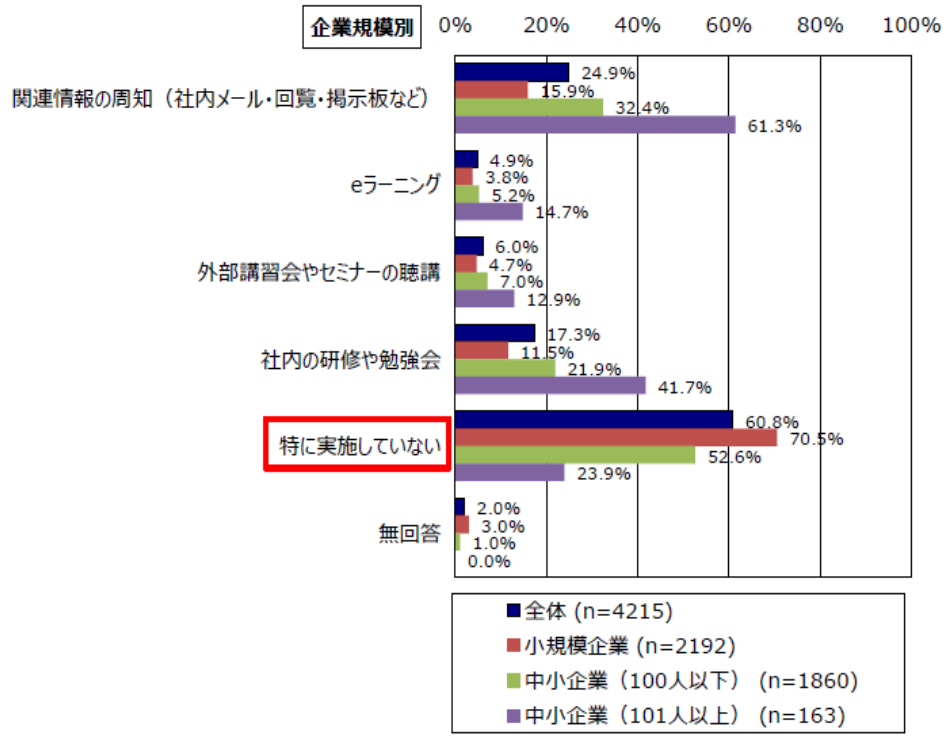
（出典）2016年度中小企業における情報セキュリティ対策に実態調査報告書(IPA)

＜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)

＜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に実態調査報告書(IPA)

政府における主な取組

＜政府における取組の例＞

	省庁	取組概要
セミナー、イベント等	NISC	「サイバーセキュリティ月間」をはじめとしたイベント等の実施
	総務省、法務省、経済産業省	電子署名等の利活用普及促進セミナー
	総務省、文部科学省	e-ネットキャラバン等の実施
	文部科学省	ネットモラルキャラバン隊の実施
	文部科学省	情報モラル教育に関する教員等に対するセミナーの実施
	文部科学省（教職員支援機構）	情報教育に関する教員等の研修の実施
	経済産業省（IPA）	情報セキュリティ安心相談窓口、標的型サイバー攻撃の特別相談窓口
	経済産業省（IPA）	標語・ポスター・４コマ漫画の募集、公表
	経済産業省（IPA）	インターネット安全教室の実施
ツール提供	NISC	情報セキュリティハンドブックの作成、普及活用
	経済産業省（IPA）	イベントへの出展や資料の配付、セキュリティプレゼンター制度の運用
	経済産業省（IPA）	情報漏えい対策ツールの提供
情報発信	NISC	SNS等を用いた情報発信
	総務省	公衆無線LANに関する利用者・提供者への周知啓発の実施
	経済産業省（IPA）	最新情報の公表
	経済産業省（IPA、JPCERT/CC）	webサイトやメーリングリストによる情報発信

※「サイバーセキュリティ2018」を元にNISC作成

3．普及啓発の取組状況

（参考）2018年「サイバーセキュリティ月間」（２月１日～３月18日）概要

- 2/1～3/18に、NISCが中核となりサイバーセキュリティに関する普及啓発活動を集中的に行う「サイバーセキュリティ月間」を実施。
- 「サイバーセキュリティは全員参加！」をキャッチフレーズに、普及啓発イベントや著名な作品とのタイアップ等を官民連携して実施。
- 特に本年は、NISCから全府省庁に改めて協力を呼びかけ、政府一体となって更に拡大した取組を実施。

NISC主催の普及啓発イベントの開催

○２月1日　キックオフサミット@六本木
- あかま内閣府副大臣より冒頭メッセージ。
- 各地域で活躍する普及啓発団体の取組紹介や啓発活動に関する課題について議論。
- イベントの模様をインターネット全国配信。10,000以上のアクセス数を達成。

○３月4日　アナログハックを目撃せよ！2018@秋葉原
- 幅広く国民のサイバーセキュリティに関する意識向上を図るため、官民連携によるイベントを実施。当日は約2,000名が来場。

○３月16日　NATIONAL 318(CYBER) EKIDEN
- 各府省庁対抗による、競技形式のサイバー攻撃対処訓練を実施。

<キックオフサミット>


<アナログハックを目撃せよ！2018>


<NATIONAL 318 EKIDEN>

官民等による月間関連行事の開催

○　全国で官民による計189件の関連行事を実施（29年度は155件）。

○　本年は、各府省庁の協力を得て、①重要インフラ、②中小企業等、③国民全般の分野における取組を拡大。


<SIP次世代農林水産業創造技術 生産システムフォーラム>

【主な取組例】

ー金融分野ー
- 2月15,16日 「金融ISACワークショップ」
- 主な参加者：金融ISAC会員等（約250名）

ー医療分野ー
- 2月21日 「医療・介護　総合EXPO・メディカルジャパン大阪　医療ITソリューション展セミナー講演」
- 主な参加者：医療関係者等（約300名）

ー農業分野ー
- 3月13日 「SIP次世代農林水産業創造技術　生産システムフォーラム」
- 主な参加者：農業事業者等（約300名）

トップメッセージの発信

- 菅官房長官のメッセージをWebサイト等を活用し発信。

著名な作品とのタイアップ

- サイバーセキュリティと親和性の高いTVアニメ『BEATLESS』とタイアップ。
- ポスター配布、ウェブバナーを関係機関のウェブページに掲載。

「情報セキュリティハンドブック」の普及

- サイバーセキュリティに関する基本的知識を分かりやすく紹介。
- 無料電子書籍に加え、スマホ・タブレット端末用の無料アプリ配信を実施。

情報発信の強化

- 政府広報との連携。
- NISC運営SNSでの発信。
- 日替わりコラムをHPに掲載。

ロゴマークの活用

- ロゴマークを活用して国及び国民全体の活動として一体的に推進。

3．普及啓発の取組状況
（参考）NISCにおける情報発信の取組

注意・警戒情報発信

Twitter「内閣サイバー（注意・警戒情報）」
・プログラムの更新情報やマルウェアの注意喚起情報を発信
・https://twitter.com/nisc_forecast
・フォロワー約3.4万人（男女7:3）（3月末より＋約5700人）

NISCの取組、サイバーセキュリティ関連情報発信

Twitter「NISC内閣サイバーセキュリティセンター」
・NISCの取組やサイバーセキュリティに関連する情報を発信
・https://twitter.com/cas_nisc
・フォロワー約2万人（男女3:1）（3月末より＋約1500人）

Webサイト「みんなでしっかりサイバーセキュリティ」
・サイバーセキュリティに関する基礎知識の紹介、情報発信
・http://www.nisc.go.jp/security-site/index.html
※NISCのHP（https://www.nisc.go.jp/）から移動可能

Facebook「内閣サイバーセキュリティセンターNISC」
・NISCの取組やサイバーセキュリティに関連する情報、読み物（１日１回）を発信
・https://www.facebook.com/nisc.jp
・フォロワー約2700人（30-50代男性が5割以上）（３月末より＋約280人）

LINE「内閣サイバーセキュリティセンターNISC」
・NISCの取組やサイバーセキュリティに関連する情報、読み物（１日１回）を発信
・ID：@nisc-forecast
・友だち約4.6万人（40代以上男女が多い）（３月末より＋860人）

<LINEで発信しているイラスト付コラム>

※フォロワー数等は平成30年８月末時点の数値

民間における取組

＜民間における取組の例＞

	省庁	取組概要
セミナー、イベント等	株式会社シマンテック	自治体向けエンドポイント有効活用セミナー、重要インフラ企業向けCSIRT ラウンドテーブル等
	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)	全国大会 「インターネットトラブルの対策～その相談例から考える～」等の開催
	一般財団法人マルチメディア振興センター(FMMC)	e-ネットキャラバン等の実施
	一般社団法人セキュリティ対策推進協議会（SPREAD）	「プロに学ぶ！セキュリティとモラルを教える人のための指導者養成セミナー」等の開催
	学校法人岩崎学園	セミナーや演習形式の講座の開催
	NPO日本ネットワークセキュリティ協会（JNSA）	各種セミナーの開催、サイバーセキュリティ小説コンテスト
ツール提供	安心ネットづくり促進協議会	スマホ利用に関する若年層及び保護者向けリーフレット等の作成・提供
	公益財団法人ベネッセこども基金	「初めてのスマホ安心ガイドブック」の発行
	一般社団法人セキュリティ対策推進協議会（SPREAD）	講師用教材の提供
	グーグル合同会社	「家族のためのオンラインセーフティガイド」の発行
情報発信	グーグル合同会社	モバイル端末を狙う攻撃手法とその対策を紹介
	ソフトバンク株式会社	社内メールマガジンによる情報発信
	一般社団法人セキュリティ対策推進協議会（SPREAD）	Facebook、Twitter、ウェブサイトにて情報発信

※情報セキュリティ社会推進協議会第４回総会（平成29年6月2日開催）資料７を元にNISC作成

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を推進。
- 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。

✓ 「Stop.Think.Connect」の推進

・DHSが、サイバーセキュリティ啓発キャンペーンとして「Stop.Think.Connect」を立ち上げ。官民連携の協議会であるNCSA（National Cyber Security Alliance）等が主導。

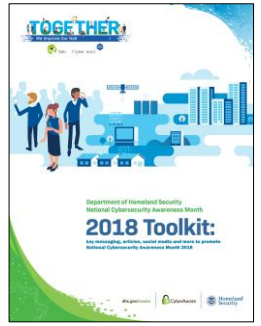
・本キャンペーンには、ENISA（欧州ネットワーク・情報セキュリティ機関）や日本の関係機関・企業も参加

STOP | THINK CONNECT™

Stop.Think.Connectのロゴマーク
[https://www.stopthinkconnect.org/]

✓ サイバーセキュリティ啓発月間（National Cybersecurity Awareness Month）の開催

・DHSが中心となりNCSAと連携して、毎年10月にサイバーセキュリティ啓発月間を開催。今年で15周年。



2018年版のツールキット
[https://www.dhs.gov/sites/default/files/publications/NCSAM_GeneralToolkit_final_0.pdf]

✓ 人材育成施策との連携

・NISTにおいて、国土安全保障省や国防省等と連携し、NICEイニシアティブを推進。

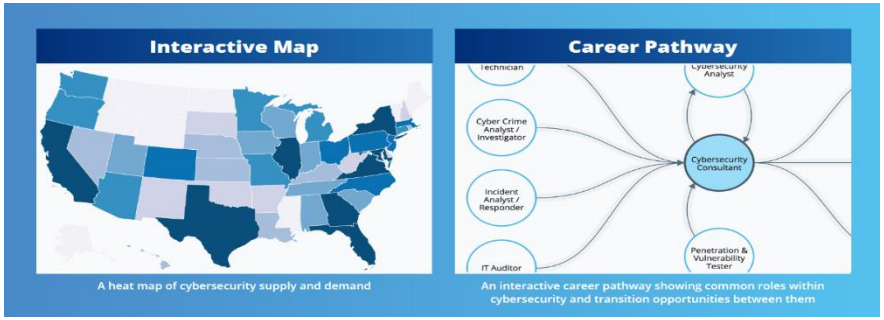
・主な取組として、

①国際競争力のあるサイバーセキュリティ人材の育成（対社会人）、

②将来のサイバーセキュリティ人材の拡大（対学生）

③サイバーセキュリティの普及啓発（対国民全般）を一体的に実施。

・NICEが支援するプロジェクトである「Cyberseek」において、米国内各都市の求人状況等を情報提供。



Cyberseekプロジェクトのwebサイト
[https://www.cyberseek.org/]

4. 諸外国の状況
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。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」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。
- NCSC（National Cyber Security Centre）では、組織や個人、トピック別にガイダンス（文章や分かりやすい画）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。

＜取組の全体像（個人、中小企業、大企業）＞

[https://www.cyberaware.gov.uk/sites/cyberstreetwise/files/cyberawarelawenforcementtoolkit.pdf]

＜NCSCが中小企業向けに作成・公表している対策集＞

[https://www.ncsc.gov.uk/information/infographics-ncsc]

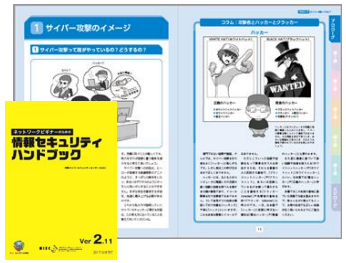
4．諸外国の状況
「サイバーセキュリティ国際キャンペーン」（2010～）

- NISCとASEAN諸国が連携して実施する、主として**外国人向けの意識啓発キャンペーン**。
- **サイバーセキュリティに関する基本的な対策を、外国人にもわかりやすく発信**する。
- 共通のキャッチフレーズは **“Be Aware, Secure, and Vigilant”**。

昨年制作した各種意識啓発マテリアルの作成（一部を翻訳してASEANへ提供）

ハンドブック

「情報セキュリティハンドブック」を英訳し、ASEAN各国へ展開。

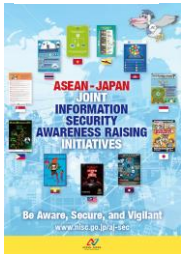


ポスター

国内用ポスターとASEAN10カ国及び日本のポスターをちりばめたコラージュポスターを作成。

国内用

コラージュ



コラム

ASEAN各国及び日本の識者によるコラムをWEBサイトに掲載

リンクバナー

キャンペーンバナーを作成し、関係府省庁や企業のWebサイトに掲載。

4コマ大喜利

4コマ漫画型の意識啓発素材を作成し、ASEAN各国語に翻訳してASEAN各国へ展開。

- 「サイバーセキュリティ国際キャンペーン」については、ASEAN各国の国内最大の意識啓発イベントが必ずしも10月ではないこと、日本国内在住者向けの意識啓発機会が2月にもあることを踏まえ、活動内容を見直している。
- 10月にだけ実施するのではなく、各国それぞれが実施している意識啓発イベントの機会を最大限活用するという観点から、今年の国際キャンペーンは、中小企業向けの意識啓発素材を日本が提供することで、各国の既存イベントを通じて共通メッセージを訴求することを目標として取り組む予定。

主な検討事項

【新たな「サイバーセキュリティ戦略」に基づく取組の方向性】

・ＡＩやIoT等の**サイバー空間を前提とする様々な技術やサービスが社会的に受容**され、あらゆる産業領域において当然に利用されるようになるなど、経済社会の大きな変化がみられる中、**個人・組織が自らの判断で対策を講ずることを前提**としつつ、**サイバーセキュリティの普及啓発について、どのような方向で取組を進めるべきか**。

・サイバー空間における利用動向やセキュリティの対策状況、また、2020年東京オリンピック・パラリンピック競技大会等の国際的なイベントを迎える中、**どのような層・分野に重点を置いて取組を進めることが必要か**。例えば、取組に遅れが見られる**中小企業**や将来のイノベーションを担う**若年層**に重点を置いて取組を進めることが効果的なのではないか。その他に、留意すべき層・分野があるか。

【様々な主体間の連携の方策】

・産学官民の様々な主体による取組が進められる中、**如何に全体を俯瞰して取組を進めていくべきか。**また、従来のコンテンツを有効活用するとの観点も含め、**様々な活動間の連携を深めるという観点から、政府にはどのような取組が求められるか。**その際に**NISCはどのような役割を果たすべきか。**

・サイバーセキュリティ月間について、今後、どのような活動を強化していくことが求められるか。

【効果的な普及啓発の方法】

・SNS等の新たなツールの利用が広まる中、旧来のメディアとの連携を含め、どのようなツールを活用していくことが効果的か。

【諸外国との連携のあり方】

・米国、英国、ASEAN等の取組状況を踏まえつつ、我が国ではどのような普及啓発の取組を行うべきか。また、**諸外国との連携のあり方について、どのように考えるか。**

以上を踏まえ、**産学官民の関係者が円滑かつ効果的に活動し、有機的に連携するためのアクションプランの基本的な在り方**について、どのように考えるか。

今後のスケジュール（案）

時期	2018年			2019年		
	10月	11月	12月	1月	2月	3月
普及啓発・人材育成専門調査会	**第９回専門調査会**（10/10）	**第10回専門調査会**（11月下旬）	意見募集実施	**専門調査会案　決定** **その後、ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略本部において決定**	**サイバーセキュリティ月間**（2/1～3/18）	