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）

サイバーセキュリティ普及啓発ロゴマーク

（商標登録第 5648615 号及び第 5648616 号）

○地球を包む3つのオブジェクトは、情報セキュリティ普及啓発のキャッチフレーズ「知る・守る・続ける」そのものであり、
・「知る」（青色）は、IT リスクなどの情報を冷静に理解し知る
・「守る」（緑色）は、安全・安心にインターネットを利用し、情報セキュリティ上の脅威から、身を守る
・「続ける」（赤色）は、情報セキュリティ対策を情熱を持って続ける
ことをそれぞれ意味する。

サイバーセキュリティ普及啓発ロゴマークは、産官学民連携したサイバーセキュリティ普及啓発を一層推進するため、有識者などの御意見を賜り、定められた。

本ロゴマークについては、政府機関だけでなく、広く関係機関・団体、企業等にも、長期間、様々なイベントに使用していただき、効果的な PR 活動に役立たせ、誰もが安心して情報通信技術の恩恵を享受し、国民一人一人がサイバーセキュリティについての関心を高めてほしいという願いが込められている。

目次

1. はじめに

2019 年 1 月、サイバーセキュリティに関する普及啓発活動を総合的にカバーする文書として、「サイバーセキュリティ意識・行動強化プログラム」[1]（以下、「前プログラム」という。）が策定された。これは 2018 年 7 月に閣議決定された前「サイバーセキュリティ戦略」[2]において、「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総合的な戦略及びアクションプランを策定すること」と明記されたことを背景に、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策定されたものである。

その後、新型コロナウイルス感染症の拡大と対策をはじめとする様々な社会経済情勢の変化に伴って、テレワークやオンライン教育の普及、ネットショッピングやオンライン行政手続きの利用増加など、世代や属性を問わずあらゆる層の国民のデジタル技術の活用、サイバー空間への参画が加速し、前プログラムが策定された 2019 年に比して、サイバー空間の公共性・重要性が高まっていることは論を俟たない。また、クラウドサービスの普及やサプライチェーンの複雑化などに伴ったリスクは増加しており、更には標的型攻撃、ランサムウェアの増加、匿名化技術や暗号技術の悪用による事後追跡の回避など、サイバー攻撃が複雑化・巧妙化している。

こうした状況を踏まえ、2021 年 9 月に閣議決定された「サイバーセキュリティ戦略」[3]においては、サイバー空間をある種の「公共空間」とみなし、これまでサイバー空間とはつながりの少なかった主体も含め、誰一人取り残さないサイバーセキュリティの確保に向けた「Cybersecurity for All」が掲げられ、「デジタル改革を踏まえたデジタルトランスフォーメーションとサイバーセキュリティの同時推進」、「公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保」及び「安全保障の観点からの取組強化」に取り組むこととされている。

当該戦略においては、デジタル改革が推進され、サイバー空間に参加する層が更に広がることを見越し、産学官民が一体となって取り組むべき、新たな普及啓発活動の指針の策定に向けて、「高齢者への対応を含め、当該アクションプランの見直しを検討すること」とされていることから、誰一人取り残さないサイバーセキュリティの確保に向けて本プログ

---

[1] サイバーセキュリティ戦略本部「サイバーセキュリティ意識・行動強化プログラム」（2019 年 1 月）
https://www.nisc.go.jp/pdf/policy/kihon-1/awareness2019.pdf

[2]「サイバーセキュリティ戦略」（2018 年 7 月）https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2018.pdf

[3]「サイバーセキュリティ戦略」（2021 年 9 月）https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf

ラムを見直すこととしたものである。

本文書は、産学官民で現状行われているサイバーセキュリティの確保に係る様々な普及啓発活動を踏まえ、今後の具体的な取組の方向性を明確化するものである。今回の新たなプログラムは、前プログラムの延長線上に位置しつつ、昨今の情勢の変化と国民の認識、世代間の差違などを整理することで、重点的に訴求すべき対象を明確化した。また、設定した重点対象に対して期待される具体的に取り組むべき事項を明確化した上で、相互の連携強化にも言及している。

本文書が、サイバーセキュリティ戦略とともに、産学官民の関係者が有機的に連携しつつ、サイバーセキュリティの普及啓発に向けた取組が円滑かつ効果的になされることを期待する。

2. 我が国のサイバーセキュリティを取り巻く現状

(1)ネット利用・対策等の状況

○ サイバー空間への多様な人々の参画の広がり

デジタル化の進展に伴い、社会・経済生活の様々な分野において、デジタル利活用が普及している。例えば、教育分野では、全ての学校に1人1台の端末と、高速大容量の通信ネットワークを一体的に整備する GIGA スクール構想が推進され、また、医療分野では、テレビ電話やスマートフォンのアプリを通じてオンライン診療や服薬指導を受けることが可能になっている。

インターネットへアクセスできる一番身近な端末であるスマートフォンの保有率は、2021年時点で、どの年齢層においても 80%を超えている(図 1 参照)。年齢別のインターネット利用率を見ると、こどもや高齢者の利用率が近年顕著に増加している(図 2 参照)一方、高齢者においては、スマートフォンの保有率に比してインターネットを利用していると回答する者の率が著しく低い年代もあり、自覚なくインターネットを利用している可能性も見受けられる。

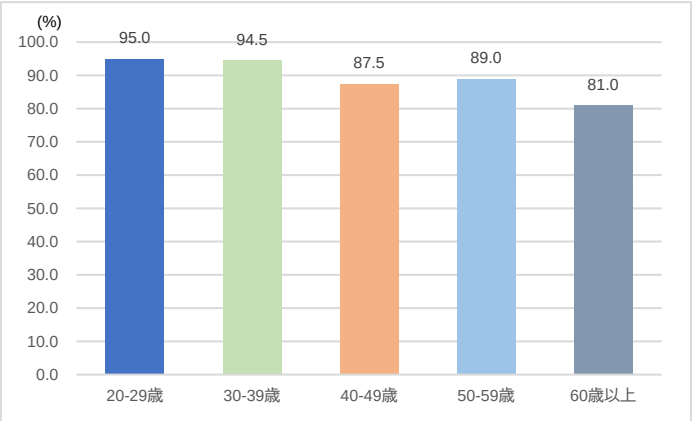

図 1 年齢別スマートフォン保有率[4]

[4] 総務省「ウィズコロナにおけるデジタル活用の実態と利用者意識の変化に関する調査研究」(2021)
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd111110.html

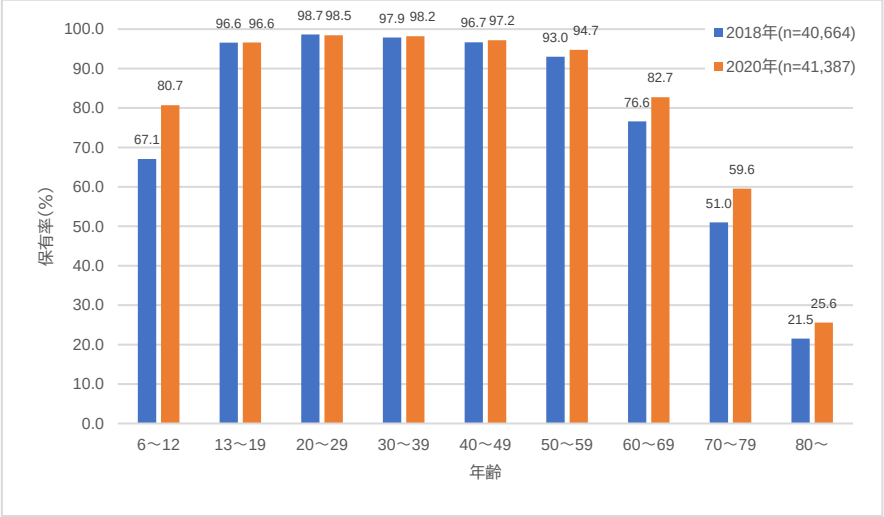

図 2 年齢別インターネット利用率[5]

また、新型コロナウイルス感染症の拡大に伴い、ネットショッピング利用世帯の割合は5割を超え（図 3参照）、テレワークは6割以上の企業で所属する社員の5割以上が実施するに至っている（図 4参照）。

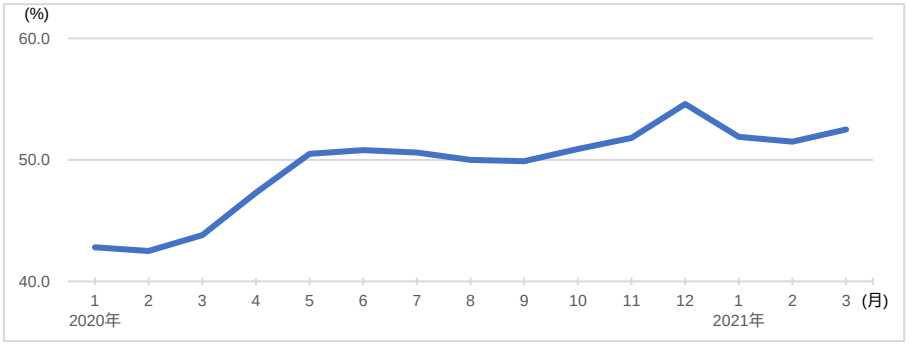

図 3 ネットショッピング利用世帯の割合[6]

[5] 総務省「通信利用動向調査」（2021）をもとに内閣サイバーセキュリティセンター（NISC）で作成
https://www.soumu.go.jp/johotsusintokei/statistics/statistics05.html

[6] 総務省「家計消費状況調査」
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd121310.html

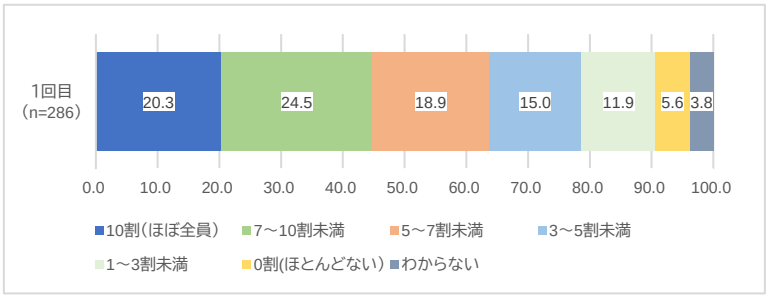

図 4 勤務先のテレワーク実施率[7]

更にオンライン行政手続きについては、利用率が6割を超え、年間件数も 2,500 件を超えるなど、今後も更なる増加が見込まれる。

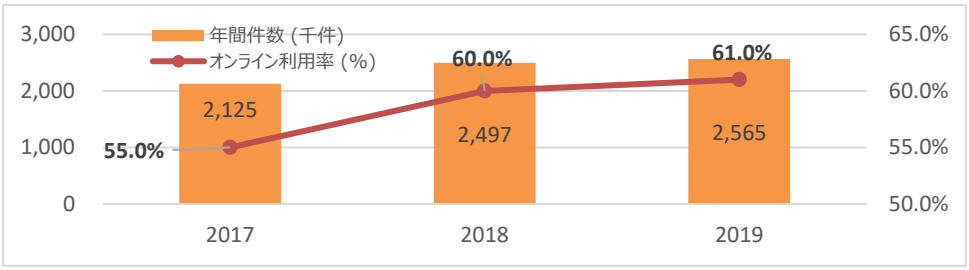

図 5 オンライン行政手続件数と利用率[8]

○ 脅威の動向・不安感

このように様々な社会経済活動がサイバー空間に拡大する中、インシデントが発生した際にサービスなどが継続して使うことができなくなる懸念も高まっており、サイバー空間における脅威が我々の国民生活へ与える影響は多大なものとなる恐れがある。

独立行政法人情報処理推進機構（IPA）では「情報セキュリティ 10 大脅威 2022」を公表している（表 1 参照）。

---

[7] 総務省「ウィズコロナにおけるデジタル活用の実態と利用者意識の変化に関する調査研究」（2021）をもとに NISC にて作成 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd123420.html

[8] 内閣官房 IT 総合戦略室・総務省「行政手続等の棚卸結果等の概要」を基に NISC で作成

表 1「情報セキュリティ 10 大脅威 2022」[9]

前年順位	個人	順位	組織	前年順位
2 位	フィッシングによる個人情報等の詐取	1 位	ランサムウェアによる被害	1 位
3 位	ネット上の誹謗・中傷・デマ	2 位	標的型攻撃による機密情報の窃取	2 位
4 位	メールや SMS 等を使った脅迫・詐欺の手口による金銭要求	3 位	サプライチェーンの弱点を悪用した攻撃	4 位
5 位	クレジットカード情報の不正利用	4 位	テレワーク等のニューノーマルな働き方を狙った攻撃	3 位
1 位	スマホ決済の不正利用	5 位	内部不正による情報漏えい	6 位
8 位	偽警告によるインターネット詐欺	6 位	脆弱性対策情報の公開に伴う悪用増加	10 位
9 位	不正アプリによるスマートフォン利用者への被害	7 位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7 位	インターネット上のサービスからの個人情報の窃取	8 位	ビジネスメール詐欺による金銭被害	5 位
6 位	インターネットバンキングの不正利用	9 位	予期せぬ IT 基盤の障害に伴う業務停止	7 位
10 位	インターネット上のサービスへの不正ログイン	10 位	不注意による情報漏えい等の被害	9 位

「個人」向け脅威では、インターネットの利用拡大やオンラインサービスの普及から新たな脅威の拡大が見て取れる。2019 年から 2 年連続 2 位にランクインし、今回初めて 1 位になった「フィッシングによる個人情報等の詐取」は、ネットショッピングとスマートフォンの利用拡大から、大手ショッピングサイトや金融機関などを騙ったフィッシングメール、宅配便の再配達受付サービスなどを装った SMS を送付するなどのスミッシングなどが多く確認されている。5 位には、スマートフォン決済の広がりから、「スマホ決済の不正利用」が位置付けられている。

なお、こどもや高齢者のサイバー空間への参画の拡大を背景とした、情報リテラシーに明るくない層への脅威の増加が見て取れる。1 位の「フィッシングによる個人情報等の詐取」に関しては、「不在通知の偽 SMS」に関する消費者生活相談件数の推移をみても、近年件数が顕著に増加するとともに、特に高齢者の割合が全体の約 3 割に及ぶなど目立つ傾向がある（図 6 参照）。また、特に若年層で問題として取り上げられがちな「ネット上の誹謗・中傷・デマ」が 2 位となっている。

[9] 独立行政法人情報処理推進機構「情報セキュリティ 10 大脅威 2022」
https://www.ipa.go.jp/security/vuln/10threats2022.html

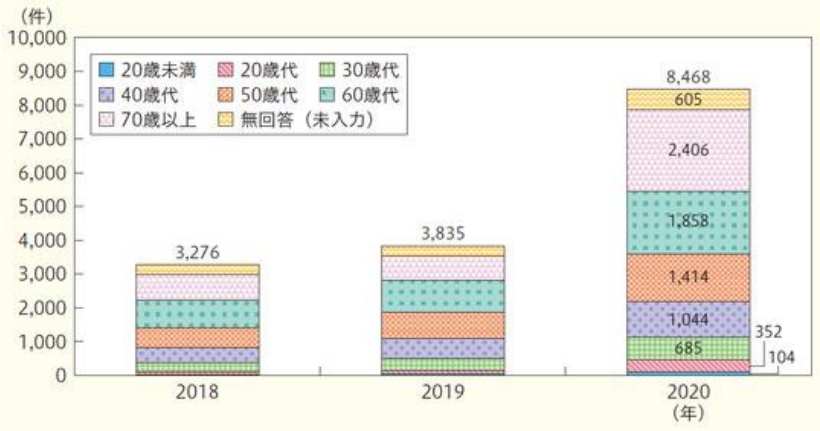

図 6 不在通知の偽 SMS に関する消費者生活相談件数の推移（年齢層別）[10]

このような脅威の増大を反映してか、インターネット利用時に不安に感じる人の割合は、7 割以上に達しており、その比率は増加している（図 7 参照）。

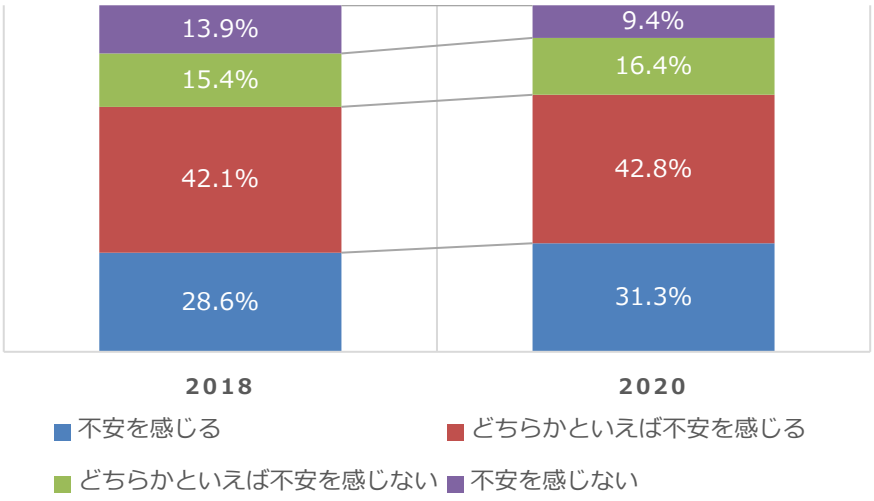

図 7 インターネット利用時に不安に感じる人の割合[11]

[10] 消費者庁「令和3年版 消費者白書」
https://www.caa.go.jp/policies/policy/consumer_research/white_paper/2021/white_paper_112.html

[11] 総務省「通信利用動向調査」の令和元年版及び令和 3 年版をもとに NISC で作成

一方、「組織」向け脅威では、企業規模や業種を問わず多数の被害が発生している「ランサムウェアによる被害」が、前年に引き続き1位となっている。この背景には、RaaS（Ransomware as a Service）とも呼ばれる、マルウェアの開発者と当該マルウェアを使って攻撃を行う攻撃者などで構成される、ランサムウェアの提供や身代金の回収を組織的に行うエコシステムが成立したことにより、高度な技術を持たなくても簡単に攻撃を行えるケースが増えていることなどが挙げられる。近時では、暗号化したデータ復元の見返りに加え、搾取したデータを公開しない見返りの金銭まで要求する、いわゆる「二重の脅迫」を行うランサムウェアの被害も発生している（図 8参照）。また、ランサムウェア攻撃は2位の「標的型攻撃による機密情報の窃取」とともになされることがあるが、2020 年に入り標的型メール攻撃が前年同期と比べて急増し[12]、その被害も引き続き止んでいない[13]。

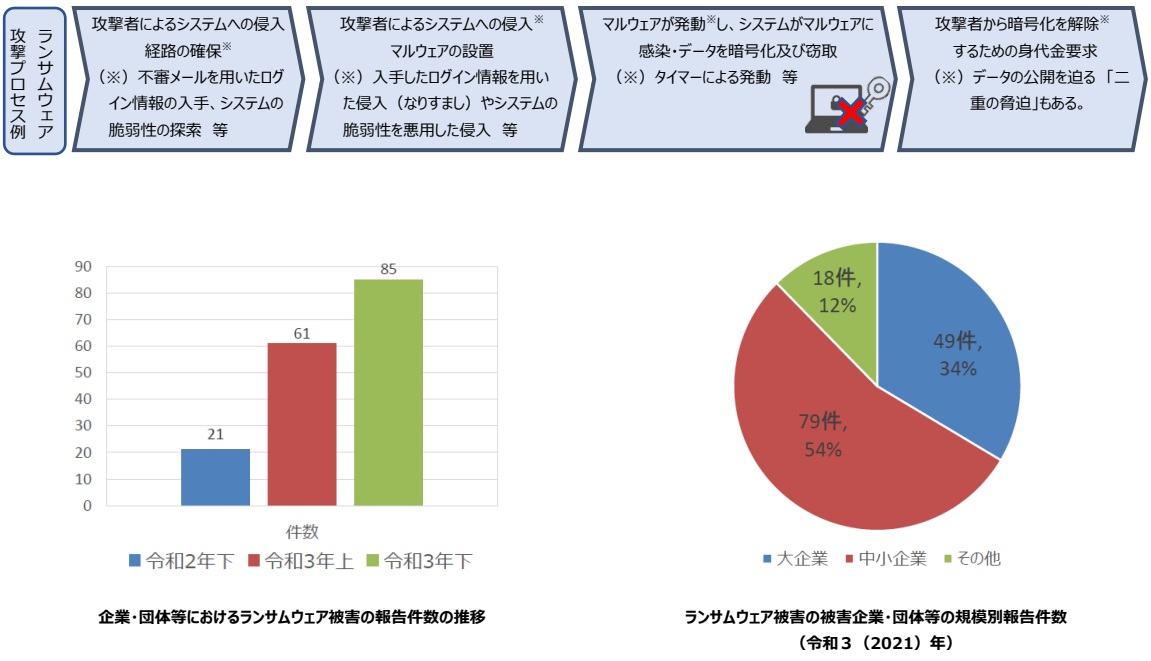

図 8 ランサムウェアの攻撃プロセス例及び被害の報告件数[14]

[12] 警察庁「令和2年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R02_kami_cyber_jousei.pdf

[13] 警察庁「令和3年におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf

[14] 被害の報告件数については、警察庁「令和3年におけるサイバー空間をめぐる脅威の情勢等について」を基に NISC 作成

また、「サプライチェーンの弱点を悪用した攻撃」が３位に、「テレワーク等のニューノーマルな働き方を狙った攻撃」が 4 位に位置付けられているなど、取引先や子会社、海外拠点といった相対的な弱点が狙われるケースや、生活様式の変化に伴う脅威が目立つ結果となっている。企業・組織においては、テレワークなどの普及に伴い個々の端末経由又はVPN機器の脆弱性を悪用されネットワークに侵入されるケースや、適切な設定が行われていないクラウドサービスが攻撃の標的とされるケースが増加しているほか、新型コロナウイルスワクチンに関するニュースに関連したフィッシングやビジネスメール詐欺（BEC: Business E-mail Compromise）などのコロナ禍に乗じたサイバー攻撃など、足元の環境変化をタイムリーに捉えたサイバー攻撃も現にみられている。

（2）現状の取組の課題

こうしたネット利用、対策などの状況を踏まえ、産学官民で下記のような取組が実施されているが、それぞれに以下のような課題が認められる。

	現状の取組例	課題
個人向け	・携帯電話販売代理店等による各種サポートサービス	・幅広い対象へのリーチ、サポートの質の担保
	・総務省「デジタル活用支援推進事業」※の実施 ※高齢者等が身近な場所でオンライン行政手続等のスマートフォンの利用方法を学べる講習会	・スマートフォンの利用の際にはサイバーセキュリティに関する認識も重要
	・IPA「インターネット安全教室」(ホームユーザー向け) の開催	・どこへ相談するべきかわからないユーザーが多い
	・中・高において「情報セキュリティ」に関する教育を実施(学習指導要領に位置づけ) ※小：各教科の学習を通じて情報活用能力において育成	・家庭でのルール設定、利用状況の把握の促進 若年層向け教育コンテンツの充実・活用
	・総務省・文部科学省「e-ネットキャラバン」※の実施 ※児童・生徒、保護者・教職員等を対象とした講座の提供	・認知度の向上
	・内閣府、総務省、関係省庁及び関係事業者「春のあんしんネット・新学期一斉行動」によるフィルタリングサービス等の普及啓発	・更なる加入率の向上
	・各都道府県警における「サイバー防犯ボランティア」の活動促進	・シニア層向けコンテンツの充実・活用、シニア層への展開
組織向け	・「サイバーセキュリティ経営ガイドライン」の改訂	・認知度の向上、ガイドラインの充実、経営層への訴求
	・「サイバーセキュリティお助け隊サービス」の創設	・認知度の向上
	・産業界主導のSC3を通じたサプライチェーン対策推進 ※サプライチェーン・サイバーセキュリティ・コンソーシアム	・下請企業等取引先への要請・支援の具体化
	・わかりやすい参考コンテンツの提供(例：テレワークセキュリティガイドライン)	・認知度・利便性の向上
	・コミュニティ形成の推進(地域SECUNITY(セキュリティ+コミュニティ)、サイバー対策協議会)	・地域における相談先・窓口が不明瞭
共通	・産学官民の施策をまとめたポータルサイトの運営	・掲載施策の充実、利便性の向上
	・基本的な対策をまとめた「安全・安心ハンドブック」の公開	・各主体による更なる利活用の促進
	・「サイバーセキュリティ月間」の推進	・更なる知名度の向上

図 9 官民の取組状況及び課題と今後の方向性

それぞれの対象の課題は概ね以下のようにまとめられる。

○ 個人向け

個人向けの脅威としては、フィッシング、ネット上の誹謗・中傷・デマ、メールや SNS などを使った脅迫・詐欺の手口による金銭要求が上位を占めている。フィッシングや脅迫・詐欺による金銭被害に懸念を抱く割合の多いシニア層向けの取組としては、現状、携帯電話販売代理店などによる各種サポートサービス、総務省「デジタル活用支援推進事業」の取組がなされているが、主眼が当てられているスマートフォンをはじめとしたデジタル活用の促進と同時に、サイバーセキュリティ意識の向上にも並行的に取り組む必要があると考えられる。また、ネット上の誹謗・中傷・デマが顕在化しやすい、こども向けの取組として、小・中・高における「情報セキュリティ」に関する教育や、総務省・文部科学省・一般財団法人マルチメディア振興センター（FMMC）が実施する「e-ネットキャラバン」があるが、活動の認知度の向上に課題があると見受けられる。さらに、これら個人向けの取組については、普及啓発を行う主体のリソース確保が困難な場合も多くみられる。

○ 組織向け

組織向けの脅威としては、ランサムウェアによる被害、標的型攻撃による機密情報の窃取、サプライチェーンの弱点を悪用した攻撃、テレワークなどのニューノーマルな働き方を狙った攻撃が上位を占めており、その多くは従業員への教育や経営者の意識向上によって改善され得るものであると考えられる。現状、企業経営者への意識向上に向けた取組としては、経済産業省「サイバーセキュリティ経営ガイドライン」の改訂、中小企業や地域企業に向けた「サイバーセキュリティお助け隊サービス」の創設、産業界主導のサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3：Supply Chain Cybersecurity Consortium）を通じたサプライチェーン対策推進、総務省「テレワークセキュリティガイドライン」の提供などが行われているが、その多くは認知度の向上が課題となっていると見受けられる。また、特に規模の小さい企業・組織については、セキュリティ対策を実行するための現実的なリソース不足が指摘されており、実態に即した効果的な取組が求められる。

○ 共通の取組

個人・組織の両方に向けたサイバーセキュリティの普及啓発の取組としては、例えば NISC における産学官民の施策をまとめたポータルサイトの運用、基本的な対策をまとめた「インターネットの安全・安心ハンドブック」の公開、サイバーセキュリティ月間の実施などが挙げられる。これらについては、共通的な普及啓発ツールとして各主体による更なる利活用の促進が望まれるが、情勢に応じた掲載内容の充実とともに利便性や認知度の向上が求められる。

3. 今後のサイバーセキュリティ確保に向けた取組の基本的な考え方

(1)原則

前述のとおり、デジタル活用の利便性が高まることにより多様な主体のサイバー空間への参画が拡大するとともに、同時に脅威も広がっているのが現状である。脅威の標的となる個人や組織を支援する取組が行われている一方、それら取組の認知不足や、サイバーセキュリティに対する理解、意識、リソースの不足から、その活用が最大限なされていない現状が見て取れる。

デジタル化の進展と併せてサイバーセキュリティ確保に向けた取組を同時に推進すること(DX with Cybersecurity)の重要性を認識しつつ、こうした現状を踏まえると、今後のサイバーセキュリティ確保に向けた取組の基本的な考え方、原則として、サイバー空間に参画する「全員」が自らの役割を主体的に自覚し、サイバーセキュリティの確保に取り組む自律性と多様な主体の連携、そのために必要となる普及啓発・情報発信の推進が挙げられる。現在、サイバー空間は実空間との融合が進み、サイバー空間に参画するあらゆる国民、セクター、地域などによるサイバーセキュリティの確保「Cybersecurity for All」が必要とされ、誰一人取り残さないよう、社会全体として目を配る時期に来ている。サイバー空間は、実空間における防犯対策や交通安全対策と同様、個人や組織がサイバーセキュリティに対する意識・理解を醸成し、基本的な取組を平時から行い、様々なリスクに自律的に対処すること、そして個々の努力にとどまらず、連携・協働することが不可欠である。同時に、各主体がリテラシーを身に付け、自らの判断で脅威から身を守れるように、そして関係者が一体として連携しやすくするように、行動強化につなげるための普及啓発・情報発信に取り組むことが重要である。

サイバーセキュリティ基本法(平成 26 年法律第 104 号)においても、普及啓発などの重要性が記載されている。具体的には、これら多様な主体が連携して積極的にサイバーセキュリティに関する施策を推進し、国民一人一人のサイバーセキュリティに関する認識を深め、自発的に対応することを促すとともに、サイバーセキュリティに対する脅威による被害を防ぎ、かつ、被害から迅速に復旧できる強靭な体制を構築するための取組を積極的に推進することを旨として行われなければならないとされており、行政機関や民間事業者などに対し、それぞれの役割に応じた責務を課すとともに、国民に対しては、サイバーセキュリティの重要性に関する関心と理解を深め、サイバーセキュリティの確保に必要な注意を払う努力を求めている。同時にサイバーセキュリティに関する教育及び学習の振興、普及啓発の施策の必要性を規定している。同法及びその他関係法令などにおける規定の趣旨を踏まえ、各主体に求められるサイバーセキュリティ確保に対する責務、連携、普及啓発に関する期待について次項より述べる。

① 国への期待

国は、サイバーセキュリティに関する総合的な施策を策定し、及び実施する責務を有するとともに、各主体の連携・協働を促し、サイバーセキュリティに関する普及啓発を講じるものとされている[15]。そのため、国は総合的なサイバーセキュリティに関する戦略や方針、アクションプランを策定し、各主体の連携・協同が円滑になされる施策を検討することに加えて、国民一人一人に広く普及啓発することが期待される。現在、普及啓発はウェブサイトや SNS を通じた活動が中心であるが、若年層は動画サイトなどを利用していたり、シニア層はテレビや新聞などのマスメディアを主たる情報収集の手段としているところ（図 10 参照）、各ターゲットを意識しつつ、普及啓発の手法を検討することが必要である。

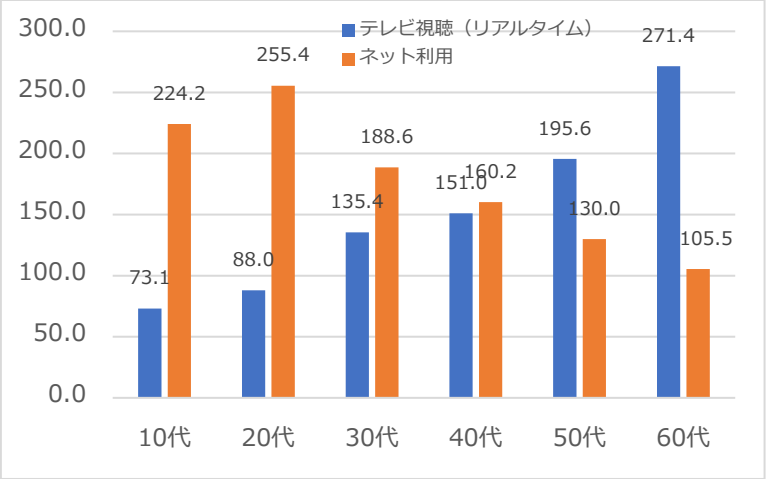

図 10 主なメディアの平均利用時間[16]

② 地域コミュニティ・地方公共団体への期待

○ 地方公共団体

地方公共団体は、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する[17]。そのため、各地域におけるサイバーセキュリティ確保のみならず、地域住民、

[15] サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 4 条及び第 23 条

[16] 総務省情報通信政策研究所「令和 2 年度情報通信メディアの利用時間と情報行動に関する調査」を基に NISC で作成

[17] サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 5 条

企業、各種関係者へのサイバーセキュリティ意識の向上のための取組が望まれる。

○ 都道府県警察

都道府県警察は、警察本部・警察署・交番など全ての組織を挙げて地域社会との連携を一層強化し、被害相談の受付・捜査・対策などを推進する役割を担うとされている[18]。そのため、サイバー防犯ボランティアなどの地域に根ざした各主体の活動や学校教育とも連携して、サイバーセキュリティ人材の育成や各種防犯活動など、サイバー犯罪防止のための取組が期待される。

○ 学校・教育研究機関

学校における教育の情報化の推進は、サイバーセキュリティの確保を図りつつ行われなければならないとされ[19]、児童・生徒への情報モラル教育だけでなく、保護者に児童・生徒の情報リテラシー教育を促すことは重要な活動としている[20]。そのため学校においては、学校におけるサイバーセキュリティの確保とともに児童・生徒及びその保護者へのサイバーセキュリティの理解と意識向上に取り組むことが期待される。

また、大学その他の教育研究機関は、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国や地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めることとされている[21]。そのため、地域におけるサイバーセキュリティの専門家として、コミュニティに貢献することが期待される。

③ 民間事業者等への期待

○ 重要社会基盤(インフラ)事業者

重要インフラ事業者は、そのサービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国や地方公共団体が実施するサイバーセキュリティに関する施

18 警察におけるサイバー戦略について(依命通達)

19 学校教育の情報化の推進に関する法律(令和元年法律第 47 号)第 3 条

20 教育情報セキュリティポリシーに関するガイドライン

21 サイバーセキュリティ基本法(平成 26 年法律第 104 号)第 8 条

策に協力するよう努めることとされている[22]。社会生活の基盤である重要インフラ事業者の責任は一般の企業よりも重く、サイバーセキュリティに対してより高い意識を持ち、取引先やサービス供給先を含めてより一層のサイバーセキュリティ確保し、関係者と協力しての各種施策の実行や、利用者を含めた普及啓発が期待される。

○ サイバー関連事業者

サイバー関連事業者[23]は、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国や地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるとされている[24]。そのため、利用者のサイバー空間の利活用促進とともに、利用者に対するサイバーセキュリティの普及啓発、健全なネットワーク環境の維持や、サプライチェーン全体を意識したサイバーセキュリティ確保と意識の向上が期待される。

○ その他の企業・組織

重要インフラ事業者やサイバー関連事業者以外の企業・組織も、自主的かつ積極的にサイバーセキュリティの確保に努め、国や地方公共団体の施策に協力する必要がある[25]。そのため、規模の大小にかかわらず、いかなる企業や組織も取引やサービスを介して顧客・利用者などに影響を与え得ることを認識しつつ、自社や取引先・顧客などを含めサイバーセキュリティ確保と意識向上、普及啓発の取組が期待される。

④ 家庭への期待

国民は、サイバーセキュリティの重要性に関する関心と理解を深め、サイバーセキュリティの確保に必要な注意を払うよう努めるとされている[26]。また、若年層に対して、保護者は、インターネットの利用の状況を適切に把握するとともに、インターネットの利用を適切に管

---

[22] サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 6 条

[23] サイバー関連事業者とは、インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者をいう。

[24] サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 7 条

[25] サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 7 条

[26] サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 9 条

理し、青少年のインターネットを適切に活用する能力の習得の促進に努めることとされている[27]。さらに、若年層のみならずシニア層に対しても、家庭内でサイバーセキュリティ意識向上などを行うことが期待される。

(2)ターゲット

前述のように、各主体によるサイバーセキュリティ確保に向けた自律的な対策や活動、多様な主体との連携、そのための普及啓発が期待されている。しかしながら、各主体の中には、自身ではどのような対策や活動を実施したらよいかわからない又は実施すべき取組がわかっていてもリソース不足などで実施できない者や、それらを支援や協力する取組があっても認知していない者もいる。このような主体には一層の特別な配慮が必要になる。特に以下に述べる主体については、自律的な取組(自助)や多様な主体の緊密連携(共助)が働きにくく、現状では必ずしもサイバーセキュリティの確保に関する各種の取組の普及啓発が行き届いているとは言い難いため、それぞれの層の特性などを勘案の上、各普及啓発主体が重点的に訴求すべき対象(ターゲット)となり得る。

① シニア・非就業層等

サイバー空間の広がりに伴い、自らが晒されている脅威が増大しているにもかかわらず、そもそもサイバー空間の脅威自体に関心がない、又は関心はあるが具体的な対策方法がわからないという、ICT 技術の進展についていきづらい者が想定される。

これに該当すると思われるのは、いまだ現実世界(リアル)とサイバー空間(バーチャル)が分断しており、インターネットをはじめとするサイバー空間を利用せずとも大きな支障なく生活できるシニア層、そのなかでも特にサイバー空間の利活用に慣れていない者や、サイバー空間を利用するが、学校や勤務先などでセキュリティ対策などのリテラシーを定期的にアップデートする機会を持たない非就業層である。サイバー空間を安全・安心に利活用するために必要なリテラシーなどの教育の状況については、インターネットや情報に関する倫理教育の受講経験をみると、世代が上がるほど、受講機会が少ない(図 11 参照)。また、主夫・主婦や非就業層など、勤務先や学校などの所属組織でリテラシー教育を受講する機会がないなど、脅威動向に応じた知識のアップデートがし難い、又は現行の情報発信にアクセスし難い層も存在している。

[27] 青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律(平成 20 年法律第 79 号)第 6 条

なかでもシニア層は、政府機関などによるインターネットを介した情報発信を受け取りにくいことなどから、自ら主体的に情報を入手したり、必要な対処を実施したりすることが難しい場合が想定される。

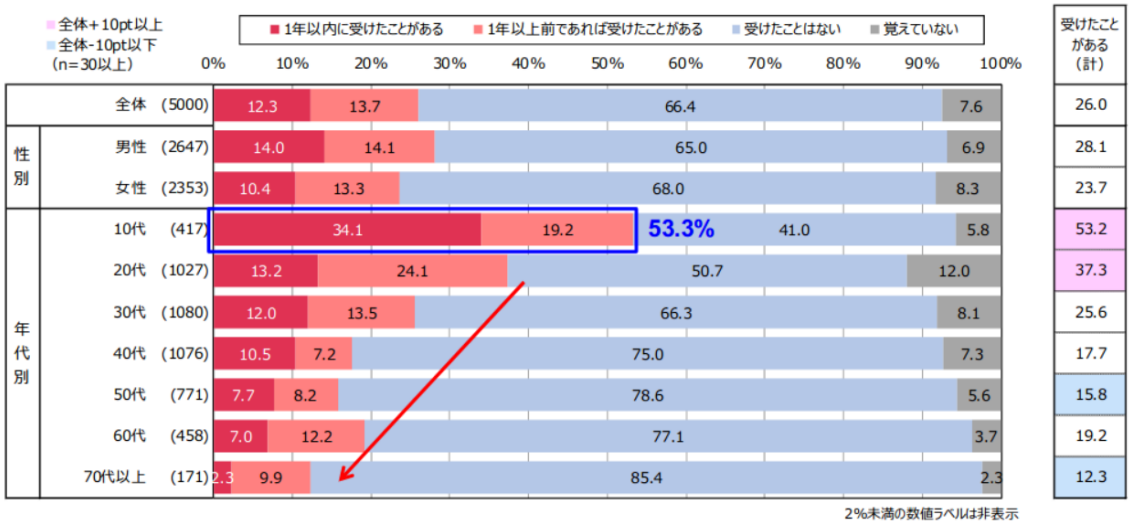

図 11 インターネットや情報に関する倫理教育の受講経験[28]

② こども層・家庭

GIGA スクール構想をはじめとする ICT 活用促進の取組の結果、18 歳以下のこども層によるサイバー空間の利活用も拡大している。特に、成年年齢が 18 歳に引き下げられ、一人で有効な契約ができる年齢も引き下げられたことから、サイバーセキュリティへの理解の必要性が高まっていると考えられる。また、こういった若年層は、新たな技術の活用にあたり、発達段階に応じた知識、理解力が身についていないこともあるため、被害者にも加害者にもなる恐れがある。

例えば、青少年へのサイバー犯罪被害について見ると、被害を未然に防ぐためのフィルタリング利用状況は、青少年の 5 割近くが利用していないことがわかる(図 12 参照)。被害児童のフィルタリング利用状況を見ると、被害にあった児童のうち 8 割がフィルタリングを利用していない(図 13 参照)。

[28] IPA「2021 年度情報セキュリティの倫理に対する意識調査」 https://www.ipa.go.jp/files/000096684.pdf

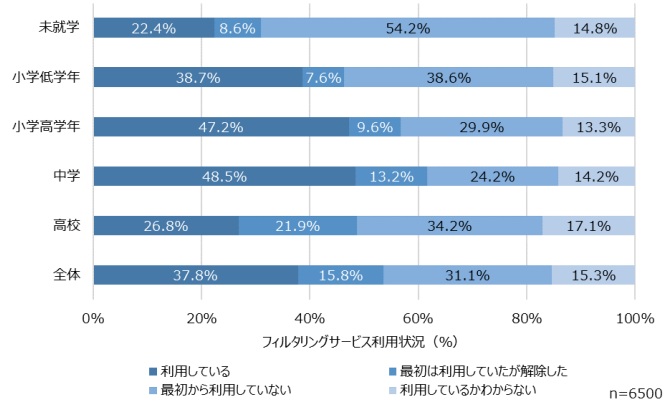

図 12 フィルタリング利用状況[29]

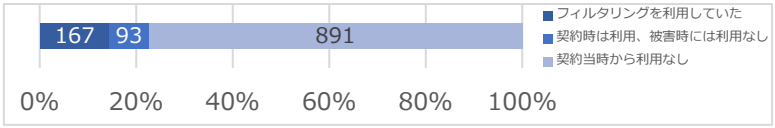

図 13 被害児童のフィルタリング利用状況[30]

また、中高生が不安を感じたときに相談できる相手として、保護者は学校の友達と並ぶ最も高い位置付けである（図 14 参照）。サイバー犯罪に巻き込まれないように、またサイバー犯罪の被害に適切に対処できるように、サイバー空間の利用に際して疑問や不安を感じたときに親子間でスムーズ対話・相談を促すためのツールや、保護者に対して、中高生の子が持つ疑問や不安を解決するためのわかりやすいガイダンスの提供などが必要となる。

[29] 総務省「我が国における青少年のインターネット利用に係るペアレンタルコントロールに関する調査結果」(2022) https://www.soumu.go.jp/main_content/000812949.pdf

[30] 警察庁「なくそう、子供の性被害。」関係統計を基に NISC で作成

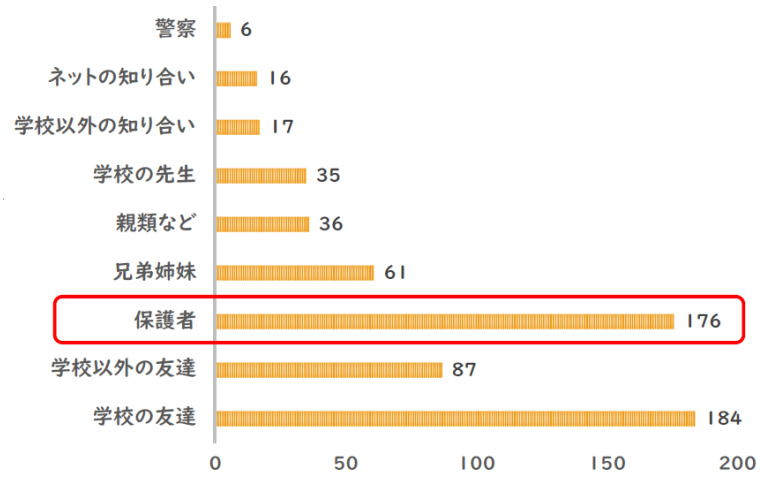

図 14 中高生の相談できる相手[31]

こども層は、現実世界とサイバー空間が他の年代に比べ相対的に近接しており、もはやインターネットの利用なくしては生活が成り立たない世代である一方、危険察知能力が十分に発達しておらず、興味本位で脅威に近づくような傾向もある。また、インターネット上に存在する多種多様な情報を様々な配信形式（例えば動画配信）で自らの興味関心に応じて主体的に取捨選択することもあり、政府機関などの既存のマス向け情報発信、例えば政府機関ウェブサイトにおいて単純な文字や画像で構成されたコンテンツだけでは関心を引きにくく、こども層が主体的にアクセスするインフルエンサーによる配信など、興味関心を引く情報発信を実施するなどの工夫が必要になる。

③ 中小企業・組織

コロナ禍への対応を余儀なくされることなどを通じ、ビジネスモデルの変革や働き方・雇用形態のあり方にも変化が及ぶ中で、デジタル化の機会は、地域、中小企業・組織、そしてサイバー空間とはつながりのなかった業種・業態の企業にも例外なく広がって来ている。

一方で、中小企業・組織がデジタル化と同時にサイバーセキュリティ対策に取り組むに当たって、資本や人材などの余力がある大企業とは異なり、セキュリティ対策に多額の予算を割くことができない、セキュリティ専任の人材を配置できないなど、財務・人材面でのリソース不足をはじめとするセキュリティ対策への負荷が大きいと考えられる。例えば、

[31] 岡崎女子大学 花田経子講師資料（対象 愛知県内2校の中高生データ, n=330）

2021 年 3 月に公表された中国地域における中小企業のサイバーセキュリティに対する調査結果[32]では、情報セキュリティ対策を進める上での課題をアンケート調査したところ、「人材が足りない」、「予算が足りない」というリソース不足が上位に挙げられている（図 15 参照）。また、当該調査では情報セキュリティのレベルを向上させるために必要とされるものについても調査されており、「経営者の情報セキュリティ意識向上」、「従業員の情報セキュリティ意識向上」の割合が高い（図 16 参照）。中小企業・組織における財政面や人材、経営層や従業員の意識向上は、特に重点的な支援が必要である。

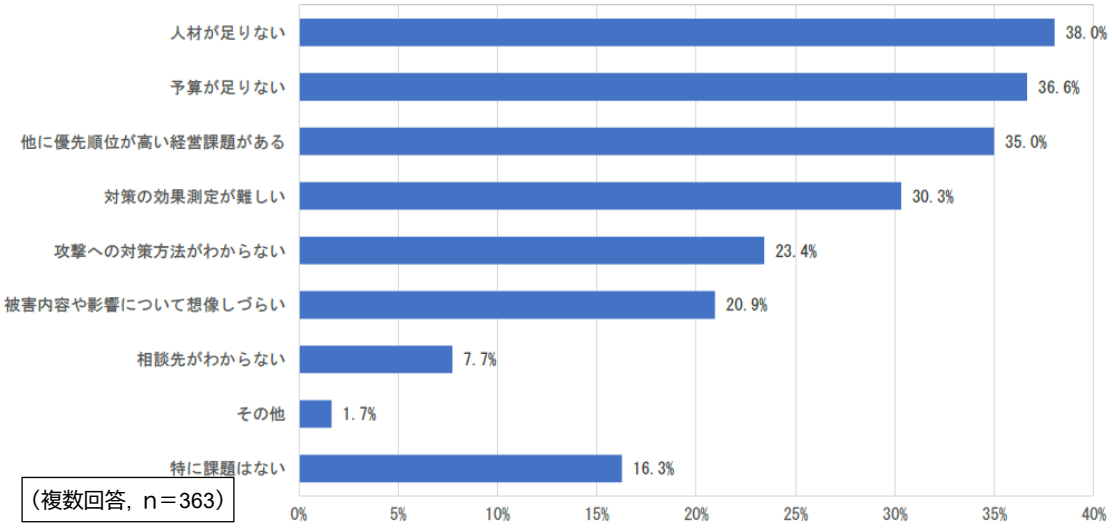

図 15 情報セキュリティ対策における課題【全体】

[32] 公益財団法人中国地域創造研究センター 「中国地域におけるセキュリティコミュニティ形成事業」報告書 (2021) https://www.chugoku.meti.go.jp/research/seijyo/210421_2.html

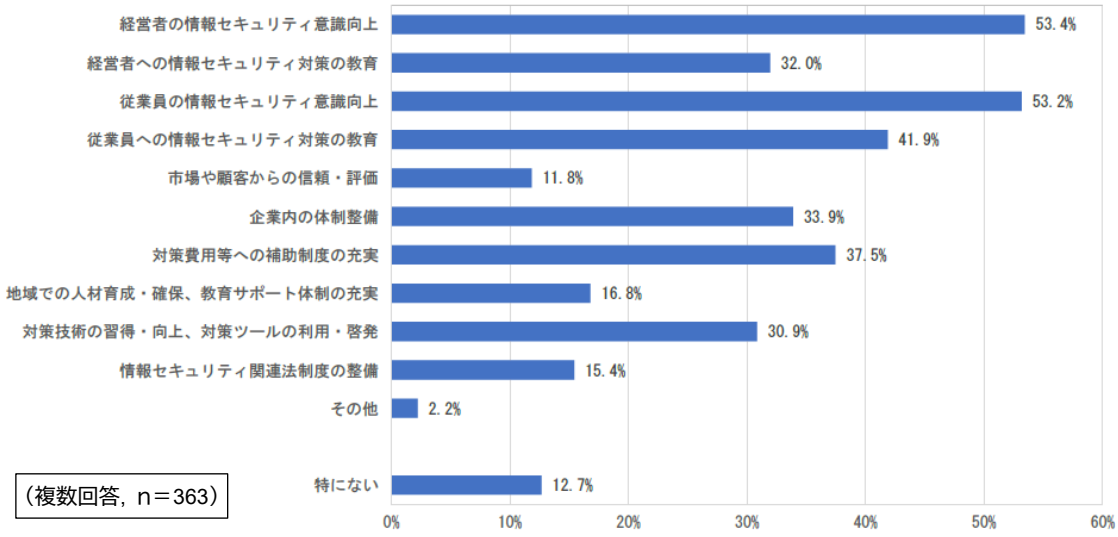

図 16 情報セキュリティのレベルを向上させるために必要なもの【全体】

(3)各普及啓発主体が担うべき役割

今までに述べた、各主体における求められるサイバーセキュリティ確保に対する責務、連携、普及啓発に関する期待や、訴求すべきターゲットを踏まえると、各主体が担うべき主な役割は以下のとおりとなる。

① 成年層・家庭

企業や各種団体などの組織に所属する就業層や各種学校に属する学生など、20 代から 50 代を中心とする成年層は、社会経済活動において日常的にサイバー空間を利用しており、既に一定の知識・リテラシーを有していると推測されることに加え、当該組織などにおいて定期的にサイバー空間を安全・安心に利用するために必要な知識などのアップデートを受けやすい状況にある。

そのため、これら成年層には、自らの親世代にあたるシニア層、及び子世代のこども層、非就業層といった家族・家庭環境で、自身でサイバーセキュリティの知識をアップデートするだけでなく、アップデートされたサイバーセキュリティの話題を挙げるなどして[33]、サイバー空間の利用に関する適切な知識・行動を自ら伝播していく役割が期待される。また、フ

[33] 家庭内でのサイバーセキュリティに関する会話は、学校などで学んだサイバーセキュリティを共有することもあり得るため、小中学生を含めた若年層による知識・行動の伝播も考えられる。

ィルタリングソフトウェア導入やサイバー空間の利用に際して疑問や不安を感じたときに、スムーズに相談しやすい環境作りの役割が期待される。

② 地域コミュニティ・地方公共団体

地域コミュニティや地方公共団体は、各地域における情報モラル・情報リテラシーの普及を主導する役割、及び各地域におけるサイバーセキュリティの取組や情報共有の基幹（ハブ）として各主体・対象間の「共助」を促進するほか、地域の中小企業・組織に対して必要な支援を提供するための仕組みや機会提供（例えば、地域企業や地方公共団体がサイバーセキュリティに関して業界内外も含め情報共有できる場の形成、地域でのセキュリティ専門家の活用、サイバーセキュリティに対して地域住民が困ったときなどの相談窓口や団体の紹介など）といった役割が期待される。

各都道府県警察においては、教育委員会、大学、高等専門学校などに対する講師派遣、出張講義などを通じて、地域社会全体のセキュリティ水準を向上させる役割、シニア層に対するコンテンツを充実させ、サイバーセキュリティに関する注意喚起を図る役割、サイバー防犯ボランティアと連携し、小中学校などやシニア層に対するサイバー防犯ボランティア活動を推進する役割が期待される。

また、各種学校では、児童・生徒及びその保護者に対する情報モラル・情報リテラシー教育の実施（例えば、教育課程としての情報教育、保護者に向けたサイバー犯罪と対応に関する情報共有、コンテンツ紹介）を通じて、こども層・家庭への普及啓発の役割が期待される。

③ 民間事業者等

民間事業者、とりわけ重要インフラ事業者は、人々の社会生活の基盤となるサービスを実施していることから、そのサービスを安定的かつ適切に提供に努める必要がある。自主的かつ積極的なサイバーセキュリティ確保、対処訓練、各府省庁及び重要インフラ事業者などとの間の情報収集・共有訓練、国や地方公共団体が実施するサイバーセキュリティに関する施策への協力を通じて、互いにサイバーセキュリティの意識や体制を向上・強化していく役割が期待される。

サイバー関連事業者などによるサービス、例えばプラットフォーム事業者が提供するデジタルサービスは、多くの国民に利用されていることから、これら事業者は、サイバー空間の利活用を促進することに加え、これを利活用するシニア層やこども層を含めた国民一人一人のサイバーセキュリティに対する認識を深め、自発的な対応を促すなど、シニア層やこ

ども層・家庭に対する普及啓発の役割が期待される。

その他の企業・組織は、自社のサイバーセキュリティ強化や、取引先などとコミュニケーションをしながら、互いにサイバーセキュリティ意識・体制強化の役割が期待される。規模の大小にかかわらず、企業・組織が様々な経済活動や取引を通じたサプライチェーンのつながりの中にある一方で、 サプライチェーンの弱点を狙った攻撃が顕在化しているところ、特にサプライチェーンで大きな影響を持つ大企業をはじめとした事業者・組織は、経営者を含めた自らのサイバーセキュリティに対する意識・体制の更なる向上・強化とともに、自組織のみならず、下請事業者をはじめとする取引先を含めた全体を通じたサイバーセキュリティ意識の向上に向けて取り組が望まれる。例えば、サプライチェーン全体でセキュリティ強化を目的としたコンソーシアムの活用、セキュリティ対策の一歩となる中小企業向けのサービスの利用推奨が考えられる。

以上の各普及啓発主体が担うべき役割と、主なターゲットの関係を図示すると以下のような概念図となる（図 17 参照）。

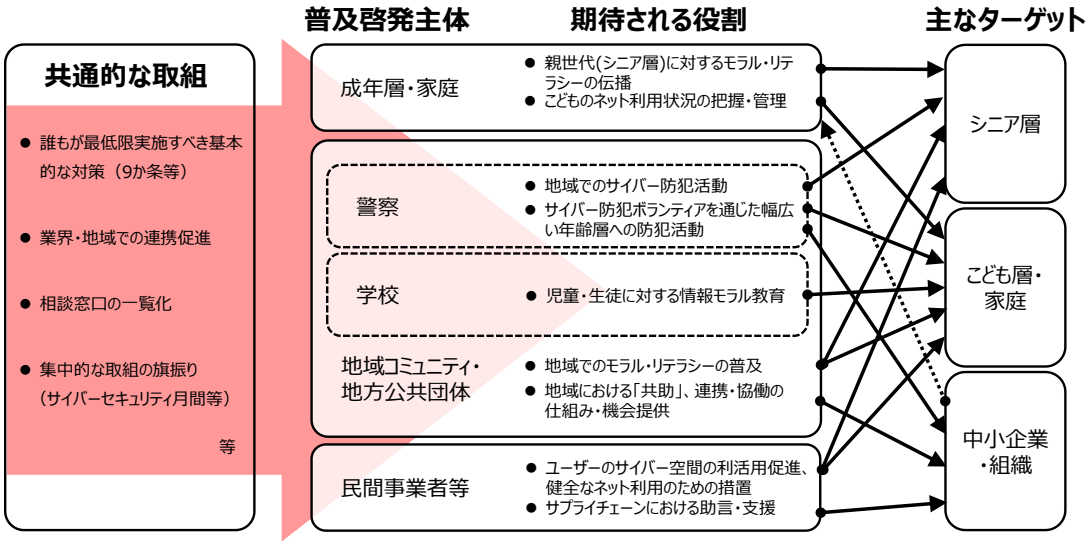

図 17 基本的な考え方の概念図

なお、本プログラムに記載された様々な主体の役割に基づく普及啓発に関する取組は、その副次的効果として、サイバーセキュリティ分野全般に対する関心を高め、人材を引きつけることにより、より専門性が求められる優秀な人材を育成するための基盤としての役

割を担うことも期待される。これは、誰一人取り残さない社会全体としてのサイバーセキュリティに通じる。

（4）誰もが最低限実施すべき基本的な対策:『サイバーセキュリティ対策9か条』

各普及啓発主体が担うべき役割とターゲットにかかわらず、サイバー空間への参画拡大に応じて日々増していくサイバー脅威に適切に対処していくためには、個人や組織におけるサイバーセキュリティの意識やそれらの取組の重要性に対する認識に加え、サイバーセキュリティ対策の実施率の向上が必要不可欠である。具体的には、全ての国民や組織が、サイバーセキュリティ対策の必要性を自覚した上で、脅威や技術の動向を踏まえて最低限実施すべきサイバーセキュリティ対策を実施することを、当たり前のこととして習慣化する必要がある。

そのためには、国民の誰もが最低限実施すべきサイバーセキュリティ対策とは何かを明確にし、誰もが理解・実施しやすい平易な内容で、継続的に周知・発信していく必要がある。

その取組の基礎として、IPA 及び NISC が共同で「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」を 2015 年 2 月に作成し、あらゆる層へサイバーセキュリティ対策を促した。作成から7年経過し、情勢が変化していく中、昨今の国民のデジタル活用やセキュリティ対策の実施状況、及び直近の技術・マルウェアなどの脅威動向などを踏まえて「サイバーセキュリティ対策 9 か条」をアップデートした（表 2 参照）。

この9か条を、国民の誰もが最低限実施すべき基本的なサイバーセキュリティ対策のベースラインと位置付け、産学官民の各普及啓発主体における一般国民向けの取組で共通的に活用していくことにより、全ての国民の基本的対策の実施を促進し、更に迅速に我が国全体のサイバーセキュリティ対策レベルの底上げを実現する。

表 2「サイバーセキュリティ対策9か条」（令和4年 IPA・NISC 更新）

1	OS やソフトウェアは常に最新の状態にしておこう
2	パスワードは長く複雑にして、他と使い回さないようにしよう
3	多要素認証を利用しよう
4	偽メールや偽サイトに騙されないように用心しよう
5	メールの添付ファイルや本文中のリンクに注意しよう
6	スマホや PC の画面ロックを利用しよう
7	大切な情報は失う前にバックアップ(複製)しよう
8	外出先では紛失・盗難・覗き見に注意しよう
9	困ったときはひとりで悩まず、まず相談しよう

4. 具体的な取組

(1)ターゲットへの重点対策

サイバー空間は、もはや人々の暮らしにとって実空間につらなる重要な一端を担っており、デジタル化の推進による恩恵は、若年層からシニア層、大企業から中小企業へ拡大している。このような新たにサイバー空間に参画してきた国民や企業は、前章で述べたように一層の特別な配慮が必要になり、各普及啓発主体が重点的に訴求すべき対象(ターゲット)となり得る。以下、それぞれのターゲットに対して実施が期待される取組について記載する。

① シニア・非就業層向け

シニア・非就業層については、より身近なデジタル利活用の推進とともに、サイバーセキュリティに関する意識向上や知識の拡充などに取り組む必要がある。例えば、デジタル活用支援推進事業では、主にシニア層向けではあるが、スマートフォンの利用方法などを学べる基礎的な講習会において、スマートフォンを安全に使うためのポイントに関する講座も提供している[34]。このようにスマートフォンをはじめとしたデジタル利用促進と同時に、サイバーセキュリティ対策を実施することの重要性の理解向上を図る取組が望まれる。

シニア・非就業層は、情報モラル・リテラシーなど、インターネットや情報に関する倫理教育を受講する機会が少ない傾向が見受けられることなどから、それらを学べる機会が必要である。例えば、携帯電話事業者による携帯電話販売代理店などでの安全教室やサポートサービスなどの取組や、経済産業省・IPA「インターネット安全教室」[35]のように、国民の情報モラル・情報リテラシーの向上を目的とした全国各地での講習会や教室の取組が望まれる。また、シニア・非就業層が集まりやすい場などにおいて、サイバー事案などによる被害防止や相談窓口の共有等を目的として、「サイバー防犯ボランティア」の活動を含め、都道府県警察による各地域に根ざしたセミナー、講演、イベントの実施など、インターネット利用者に対する啓発活動といった取組が望まれる。

シニア・非就業層がインターネットを利活用するに際して疑問や不安を感じたとき、気軽に相談できる場や信頼できる相談相手の存在も重要である。例えば、信頼できる相談先として、IPA「情報セキュリティ安心相談窓口」[36]、各都道府県警察本部、警察署などの相談窓

---

[34] デジタル活用支援推進事業 https://www.digi-katsu.go.jp/

[35] IPA 「インターネット安全教室」 https://www.ipa.go.jp/security/keihatsu/net-anzen.html

[36] IPA 「情報セキュリティ安心相談窓口」 https://www.ipa.go.jp/security/anshin/

口、警察相談専用電話「#9110」があることから、これらの認知度向上に係る取組も重要と考えられる。

② こども層・家庭向け

こども層・家庭向けの取組は、こども自身だけでなく、こどもを支援する教員や地域、そして家庭（主に保護者）など、様々な関係者に向けた取組が必要である。

まず、こども自身がサイバー空間で自身の安全・安心に取り組めるようにこども自身に対する情報モラル教育とサイバーセキュリティ意識向上に向けた取組が必要である。情報モラル教育という観点から言えば、例えば、GIGA スクール構想の推進による ICT 機器の利用拡大などにより、インターネット利用する機会が増大している。そのため、大学などの高等教育への連続性を意識しながら、引き続き、小学校・中学校・高等学校における「情報セキュリティ」に関する教育を更に充実させることで、児童・生徒の情報モラルなどを涵養することが望まれる。サイバーセキュリティに対する意識向上の観点から言えば、例えば、IPA で進めている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」[37]や、FMMC で進めている学校及び個人単位での「情報通信の安心安全な利用のための標語」[38]のように、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、書写作品などを募集、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取組が望まれる。

次に、こどもの情報教育を行う現場の教員サポートもこども層へのサイバーセキュリティ向上の一助になる。例えば、独立行政法人教職員支援機構による動画教材や指導手引書の活用や各地域で情報教育の中核的な役割を担う教員などを対象とした研修のように、現場の教員の指導教材の充実、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に向けた教員支援の取組が望まれる。また、総務省・文部科学省・FMMC が実施する「e-ネットキャラバン」[39]のように、児童・生徒及びその保護者や教職員などを対象とした講座の提供も望まれる。

そして、こどもを取り巻く地域活動を活性化させることで、こども情報リテラシーを高めサイバー犯罪を未然に防ぐことも必要である。例えば、前述の都道府県警察における「サイバー防犯ボランティア」活動のように、サイバーセキュリティに詳しい者がこども層を含め地域住民に普及啓発を行うことが望まれる。大学や工業高等専門学校の学生がサイバー

---

[37] IPA 「ひろげよう情報モラル・セキュリティコンクール」 https://www.ipa.go.jp/security/event/hyogo/

[38] FMMC 「情報通信の標語」 https://www.fmmc.or.jp/hyogo/

[39] FMMC 「e-ネットキャラバン」 https://www.fmmc.or.jp/e-netcaravan/

防犯ボランティアとして都道府県警察から委嘱を受け、県内の小学校、中学校などに出向いたり、オンラインにより 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といった取組[40]が、全国のこども層のサイバーセキュリティの更なる向上につながることが期待される。

家庭内の取組として、こどもを守る保護者に対する情報モラル・リテラシーの教育も重要である。例えば、文部科学省の委託事業である「ネットモラルキャラバン隊」のように、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などに対する意識向上を目指した取組が望まれる。また、保護者がこどもの安全・安心なサイバー空間の環境を整えることも重要である。例えば、内閣府、総務省、関係省庁及び関係事業者など「春のあんしんネット・新学期一斉行動」[41]のように、フィルタリングやペアレンタルコントロールなど、サイバー空間におけるこどもの被害発生を未然に防ぐ効果が期待されるサービスの加入促進や適切な活用に関する情報提供の取組も望まれる。

③ 中小企業・組織向け

中小企業・組織では、サイバーセキュリティに対する財務・人材面でのリソースが限られており、自身だけでのサイバーセキュリティ対策にも限りがある。そのため、中小企業・組織におけるサイバーセキュリティ対策支援は重要となる。例えば、経済産業省・IPA「サイバーセキュリティお助け隊」[42]では、地域の中小企業支援機関や損害保険会社、IT シルバー人材などと連携して、「見守り」「駆付け」「保険」など中小企業のセキュリティ対策に不可欠なサービスをワンパッケージで安価に提供している。このように中小企業・組織の実態に即した、サイバーセキュリティ対策を支援する取組が望まれる。

中小企業・組織のサイバーセキュリティ対策支援と同時にサイバーセキュリティに対して感度を高く、自律的に活動することも重要である。そのためには、経営層のサイバーセキュリティに対する理解や意識を更に高めることが重要である。例えば、経済産業省・IPA「中小企業の情報セキュリティ対策ガイドライン」[43]や「サイバーセキュリティ経営ガイドライン」

---

40 警察庁 「サイバー防犯ボランティア活動事例」
https://www.npa.go.jp/cyber/policy/volunteer/nagasaki.html

41 内閣府 令和 4 年「春のあんしんネット・新学期一斉行動」の取組
https://www8.cao.go.jp/youth/kankyou/internet_use/r04/index.html

42 IPA 「サイバーセキュリティお助け隊サービス制度」
https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html

43 IPA 「中小企業の情報セキュリティ対策ガイドライン」
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

[44]では、サイバーセキュリティ対策はコストではなく投資であると位置付け、経営者がリーダーシップを取ってセキュリティ対策を推進していくことが重要であることを示している。このように、経営層向けの意識を高めるための文書を公開し、近年の企業経営を取り巻く情勢の変化などを踏まえて改定などする取組が望まれる。

経営層の理解や意識向上とともに、サイバーセキュリティに積極的に取り組むためのインセンティブも重要である。例えば、経済産業省・IPA「SECURITY ACTION」[45]で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のように、中小企業の自発的な情報セキュリティ対策への取組を促す取組が望まれる。また、当該制度で自己宣言をすることで、IT 導入補助金の必須要件の一つを満たすなど、サイバー保険の保険料の割引に利用できる。このようにサイバーセキュリティに対する動機付けを高めるための取組も望まれる。

経営層の意識向上だけでなく、実際にサイバーセキュリティを担当する者の知識向上や支援も不可欠である。例えば、NISC「小さな中小企業と NPO 向け情報セキュリティハンドブック」[46]や前述の「中小企業の情報セキュリティ対策ガイドライン」を公開している。また、経済産業省・IPA「サイバーセキュリティ経営可視化ツール」[47]を提供し、自社のサイバーセキュリティの状況把握や、社内外の関係者とのコミュニケーションなどに活用できる。このように、中小企業向けにサイバーセキュリティ状況を把握するためのツールや、わかりやすい対策集・ガイドラインなどを公開し、必要に応じてより使いやすいものに改訂するなど、中小企業のサイバーセキュリティ担当者の知識向上を支援する取組が望まれる。

企業活動は自社だけで完結すること少なく、多種多様なステークホルダーと行うことになる。サプライチェーン・リスクの懸念が高まるなか、中小企業もサプライチェーンの一部として、その対応が求められており、一方で自身では意識されない場合もあり、サプライチェーン・リスクに対する理解や対策の支援も必要となる。例えば、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）では、企業のリスクマネジメント強化のための基本的な行動（（1）サプライチェーンを共有する企業間における高密度な情報共有、（2）機微技術情報の流出懸念がある場合の報告、（3）多数の関係者に影響する恐れがある場合の公表）を促進し、中小企業を含む日本のサプライチェーン全体でのサイバーセキュリティ対策の

---

[44] 経済産業省 「サイバーセキュリティ経営ガイドライン」
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

[45] IPA 「SECURITY ACTION」 https://www.ipa.go.jp/security/security-action/

[46] NISC 「小さな中小企業と NPO 向け情報セキュリティハンドブック」
https://security-portal.nisc.go.jp/blue_handbook/

[47] IPA 「サイバーセキュリティ経営可視化ツール」
https://www.ipa.go.jp/security/economics/checktool/index.html

強化に向けた活動を行っている。このように、産業界が一体となって中小企業を含むサプライチェーン全体でのサイバーセキュリティ対策の推進運動を進め、サプライチェーン・リスクへの理解、対策、認知度向上、利用促進を進める取組が望まれる。

中小企業がサイバーセキュリティに関して理解・相談できる場の存在も大切である。例えば、都道府県警察におけるサイバー防犯活動の他、東京都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（Tcyss）[48]では、情報セキュリティ対策の強化や情報流出事案などに関する相談を受け付け、内容により、Tcyss 参加団体などと連携して対応している。このように、サイバーセキュリティに関する相談、情報共有、事案発生時の相互連携などの取組が期待される。

（2）各主体の連携強化

多様な主体が活動するサイバー空間を持続的に発展させていくためには、各主体が自覚的にサイバーセキュリティ対策に取り組むだけでなく、各主体が密接に連携し、協働してサイバー空間の安全性を高めることが求められる。各主体が連携・補完しながら効果的・効率的に実施できるように、地域における支援の体制作り、必要な情報やコンテンツの整備・共通化、それらを含めサイバーセキュリティに関する業界内外を含めた情報共有や普及啓発に関する取組に関する情報発信、そして集中的な取組の実施が期待される。

① 地域における支援

実空間における地域を問わずサイバー空間の利活用は進んでいるが、サイバー空間でトラブルが起こった場合には、実空間での対応が行えるよう体制を整えておくことが必要であり、サイバーセキュリティに関する対策が日本のすみずみまで行き渡るよう、地域における支援を行っていくことが重要である。そのためには、各地域のサイバーセキュリティ協議会などを中心に、地域における様々なサイバーセキュリティ・コミュニティの形成を推進する必要がある。例えば、都道府県警察が構築する協議会等では、地方公共団体や民間事業者等が集まり、脅威情報や被害防止対策に資する情報の共有等を行っている。総務省・経済産業省「地域 SECUNITY」[49]では、地域の民間企業、行政機関、教育機関、関係団体などが、セキュリティについて語り合い、「共助」の関係を築くコミュニティの形成を進めており、セミナーやインシデント対応演習等の開催、地域内のビジネスマッチング、セキュリティ専

---

[48] 警視庁　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)
https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/tcyss.html

[49] 経済産業省 「地域 SECUNITY」 https://www.meti.go.jp/policy/netsecurity/secunity.html

門家を含めた人材交流、地域のセキュリティソリューション紹介などが行われている。また、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）では、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、活動の活発化を促したり、「全国大会」を開催して、加盟団体や、行政や中央で活動する関係機関と意見交換及び各者の交流機会を提供している。このように地域の「共助」の考え方に基づく課題解決・付加価値創出が行われる場を形成し、活用していく取組が望まれる。

地域住民や企業・組織に向けてサイバーセキュリティの支援や普及啓発をしていく人材の活用も必要である。例えば、デジタル庁が進めるデジタル推進委員[50]は、デジタル機器やサービスに不慣れな方にきめ細かなサポートなどを行うことで、社会全体として、デジタル社会の利便性を誰一人取り残されず享受できる環境を作っていくための取組である。デジタル推進委員の中には、自身のできる範囲内でサイバーセキュリティに関する支援をすることも考えられる。このようにデジタル利活用に明るい人材を活用し、デジタル社会の利便性を誰もが享受できる環境を作っていくため取組が望まれる。

各地域や産業毎の信頼できる相談相手・窓口を設置し、サイバー空間の利活用に際して疑問や不安を感じたとき、誰もが適切な支援を受けられる相談体制の充実が極めて重要となる。例えば、シニア・非就業層向けの取組でもあったとおり、各都道府県警察本部、警察署などにおいて相談窓口を設置している。また、地域 SECUNITY の一つである関西サイバーセキュリティ・ネットワークでは、近畿地域において、サイバーセキュリティ分野の困りごとや技術的な相談、サイバー被害に遭われた場合など、企業、個人事業主が相談できる窓口の一覧を情報発信している[51]。このように、サイバーセキュリティに関する相談体制や地域におけるセキュリティコミュニティの連絡先を一覧にするなどの取組が望まれる。

② コンテンツの整備・共通化

各主体で行われているサイバーセキュリティやその普及啓発に関する資料を集約し、コンテンツの整備・共通化はサイバーセキュリティを進める上で利便性が高く、有用なものとなる。例えば、NISC では各地域、各主体で実施しているサイバーセキュリティに関する普及啓発などの取組を集約したサイバーセキュリティ・ポータルサイトを運営している。また、当該サイトでは、基本的なサイバーセキュリティ対策をまとめた「インターネットの安全・安

[50] デジタル庁 「デジタル推進委員の取組」 https://www.digital.go.jp/policies/digital_promotion_staff/

[51] 経済産業省近畿経済産業局 「サイバーセキュリティ相談窓口＆地域セキュリティコミュニティ 一覧」 https://www.kansai.meti.go.jp/2-7it/k-cybersecurity-network/210120_3press.html

心ハンドブック」[52]や、「サイバーセキュリティ関係法令 Q&A ハンドブック」[53]をはじめ、政府機関などによるサイバーセキュリティ対策に関する各種ガイダンスの整備している。このように普及啓発に関する情報を集約し、誰もが容易に自分に必要な取組を検索・アクセスすることができる環境を整備し、更に継続的に内容をアップデートする取組が望まれる。

③ 情報発信

サイバーセキュリティに関して国民や企業・組織の意識向上に加えて、最新の脅威の情報や対策、普及啓発に関する情報について国民や企業・組織が知ることは、最新の取組実施つながるため、それら情報について適時かつ迅速に発信することが必要である。例えば、NISC をはじめ各府省庁は、SNS 公式アカウントやウェブサイトにてサイバーセキュリティに関連する情報掲載している。このように、各対象に必要な情報を適時発信する取組が望まれる。同時に、その情報の受け手である幅広い対象（サイバーセキュリティに興味を持っていない人も含む）の関心や、特性を考慮しながら、情報発信することが望まれる。例えば、シニア層に向けては公共交通機関や利用頻度の高い施設へのポスターの掲示やラジオなどのネットに頼らない情報発信、若年層に向けては、政府機関ウェブサイトだけでなく、これらの対象が主体的にアクセスしたくなる、興味関心を引く情報発信など、これまで以上に情報発信の手段や方法について工夫がなされる必要がある。

また、産学官民で連携し、各施策の更なる普及・認知度向上を目的としたセミナーなども積極的に開催も重要である。産学官民の各主体が密接に連携・協働してこれらの情報発信を実施することで、全ての国民や組織が、自らが具体的にどのような行動を取ればよいかを理解でき、かつ実際の行動を促すことができると考えられる。

④ 集中的な取組

サイバーセキュリティに関する普及啓発を集中的に行い、より多くの国民や企業・組織の関心を集めることが必要である。例えば、国民への重点的なサイバーセキュリティの普及啓発活動である「サイバーセキュリティ月間」のように、サイバーセキュリティに関する行事や期間中の情報発信やコンテンツの充実に向けた取組、報道機関やメディアを含む各種普及啓発主体との一体的な連携・協働による認知度・効果の向上に向けた取組が望まれる。

---

[52] NISC 「インターネットの安全・安心ハンドブック」 https://security-portal.nisc.go.jp/handbook/

[53] NISC 「サイバーセキュリティ関係法令 Q&A ハンドブック」
https://security-portal.nisc.go.jp/law_handbook/

こうした集中的な取組において、国民に対してサイバーセキュリティに関して簡潔で訴求しやすい事項・内容を共通して伝えていくことも大切である。例えば、全ての国民が最低限実施すべき基本的なサイバーセキュリティ対策としての「サイバーセキュリティ対策 9 か条」を、各主体による普及啓発活動で共通的に利用することも期待される。

5. 取組の PDCA・対外発信

普及啓発活動をしていく上で、フォローアップとそれに伴う継続的な改善は必要不可欠である。サイバーセキュリティ戦略本部では、毎年サイバーセキュリティの年次報告及び年次計画を発表しており、毎年度継続的にフォローアップし、継続的な改善を促していく。また、普及啓発・人材育成専門調査会においてもトピックとして報告し、委員などから意見を伺うなど、あらゆる場を活用していく。

対外発信においては、二国間及び多国間の枠組みによるサイバーセキュリティ確保や意識啓発、各種の国際的イベントや、基本方針[54]を踏まえた開発途上国への能力構築支援を活用し、発信を進める。また、そのために必要なコンテンツとして、例えば「サイバーセキュリティ対策9か条」などを英訳し発信する。

[54] サイバーセキュリティ戦略本部 「サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針」（2021 年 12 月）