NISC National center of Incident readiness and Strategy for Cybersecurity

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」の見直しについて

令和4年6月

内閣官房 内閣サイバーセキュリティセンター
基本戦略第1グループ

前回(2021年12月)の専門調査会での指摘事項(1/2)

■見直しにあたり踏まえるべき背景(近年の環境変化、サイバー空間の利用動向、攻撃の傾向)に関する意見

- ここ2～3年、フィッシングサイトの他にマルウェア経由の個人情報漏洩事案が顕著に増加。その原因の多くは、オンラインゲームの改造ツールや、CD-ROMへの書込み等業務で使う機能の違法コピーソフトのダウンロード等によるマルウェア感染。
- 行政手続のデジタル化が進んでいる。
- スマホのアプリをダウンロードする機会が増加しており、これによりトラブルに巻き込まれるケースも増えている。
- 自撮り画像のアップロード等による個人情報流出が課題。

■重点を置くべきターゲットに関する意見

- デジタルサービスを安心して利用してもらうためには、サービス提供側はもちろん、ユーザー側のセキュリティ意識を高めることが重要。
- 企業ではランサムウェアによる金銭窃取が顕著。一方、若年層ではSNS等でのいじめや個人情報窃取、性的被害など社会空間としてのサイバー空間におけるリテラシーが問われる問題が起きている。他方、シニア層ではサポート詐欺の被害など、ITリテラシーの低さに付け込む被害が課題。
- 利用促進しているマイナポータルの認証手続は難しく、高齢者に理解してもらうのは不可能に近いため、対応が必要。
- フォーカスを置くのが本当に高齢者だけでいいのか疑問。非正規雇用や専業主婦の方なども、サイバーセキュリティに関する知識がアップデートされづらいのではないか。このような層にもフォーカスを当てるべきではないか。
- 加齢に伴う認知・運動機能の低下によるトラブルも起きやすいと言われており、一部老人ホームではスマートフォンを入居者から預かっているという話も聞く。超高齢社会の中で、今後増えていく問題と認識。認知機能等が低下した方への対応として、ヘルスケア分野における研究や、保険業界での導入事例などとの連携も考えられると思う。
- ウィズコロナ・アフターコロナのサービスモデルとして、高齢者だけでなく、お手伝いが必要な方に対するユニバーサルサービスや、コロナ収束後に来日する外国人向けサービスなど、セグメントはもう少し幅広に考えた方がいいと思う。

前回(2021年12月)の専門調査会での指摘事項(2/2)

■各主体が担う役割に関する意見

- シニア層は子供よりも孫の言うことを聞く傾向にあるため、孫を介して注意喚起・情報発信してもらうことも一手。
- スマホ教室の取組は非常にコストがかかっていると思う。取組を更に拡大するのであれば、その社会的コストを社会全体でどのように分担していくのかについても議論が必要だと思う。
- セグメントごとのアプローチに加え、「面」で押さえていくことも重要。携帯電話販売代理店や家電量販店等の民間事業者、地域コミュニティ、警察等の連携を、国が音頭を取って行うべきではないか。

■具体的な取組に関する意見

- シニア層への普及啓発の方法論として、子供が自分の親をサポートしやすいIT環境の整備も重要。
- 製造業では、今後メーカー側が負う責任が増えていくようになると思う。高齢者を含む利用者の意識向上だけではなく、製造者側でユーザーの行動分析に基づく対応が適切になされているかなど、製造者の責任の所在に関する議論も必要ではないか。
- リテラシー教育について、小中高の指導要領には組み込まれているが、大学等の高等教育では手薄になっている。大学・高専では、AI戦略に基づく数理・データサイエンス・AI教育強化の一環で認定制度を運用している。サイバーセキュリティについても、制度の活用を含め、初等中等教育から高等教育への連続性を確保すべきではないか。
- 普及啓発の担い手として、シルバー人材サービスのサポートメニューにITサポートを加えるなど、高齢のIT・セキュリティ人材を活用する方策をぜひ検討頂きたい。

■実施上の課題に関する意見

- セキュリティ対策ソフトをインストールしていたが、これがマルウェアを検知する前に情報が漏洩していたケースが増加している。このように、情報が漏洩し攻撃側に利用されることを前提とした対策・情報発信が必要ではないか。
- 発信・アップデートされた情報に対して、各組織の担当者がキャッチアップしやすくなるよう、プッシュ型で情報提供する仕組みを設けていただきたい。
- 民間サービスが様々ある中で、各サービスに個別対応することには限界があるように思う。新たな民間サービスを逐一フォローすることは難しいが、行政サービスについては、ある程度統一してアクセシビリティを確保できるのではないか。

2022年「サイバーセキュリティ月間」（報告）

- 2010年より、毎年**2月1日から3月18日**を「**サイバーセキュリティ月間**」に設定。関係機関・団体と連携し、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実施**。
- 2022年は、**幅広い層に認知度高いコンテンツとのタイアップ**や、**事業者とコラボした具体的対策の発信**等を新たに実施。

情報発信の強化

- **トップメッセージ**
  月間の開始にあわせ**松野官房長官メッセージ**を発信

官房長官メッセージ
「サイバーセキュリティ月間」を一つの機会として、改めてサイバーセキュリティに意識を向け、**「全員参加」**で取組を進めていただきたい

- **事業者とコラボした具体的対策の発信**
  OSや無線LANルータに係る民間事業者・団体とコラボレーションし、**実際に利用される機器やサービスごと**に、アップデートや多要素認証の利用など、**最低限取り組むべき具体的対策**を発信
- **コラム**
  産・学・官・民の各分野で活躍している女性プレーヤーや、**東京2020大会の対策を担った方々**によるコラムを発信
- **SNS**
  上記内容について、期間中、Twitter等を用い積極的に情報発信

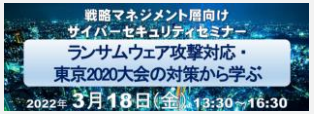
牧島かれん @makishimakaren · 2月1日
「サイバーセキュリティ月間」始まりました！#サイバーセキュリティは全員参加

- **タイアップ**
  『マクロス』とタイアップし幅広い世代に訴求できる**3種類のポスターを制作**
  各県警や学校等へのポスター配布、**デジタルサイネージ**の提供を実施

月間期間中のイベント等開催

＜NISCの取組＞

- **NISC-CTF**
  各府省庁・独法等の職員がサイバーセキュリティに関する幅広い技術・能力を競うオンライン競技会を開催(参加登録111名)
- **戦略マネジメント層向けWebセミナー**
  サイバー攻撃の被害を受けた企業等から経験を通じて得られた気付き、東京2020大会に行われたサイバーセキュリティ対策等を講演(参加登録547名)



＜民間主体の取組例＞

- **サイバーセキュリティマンデー**
  ユーザーに正しい知識を身につけてもらうことを目的に、2月の毎週月曜日に、サイバーセキュリティに関する情報を定期発信

- **みんなでシェアして、みんなを救おう。#迷惑メール展**
  フィッシング詐欺メール等の実例を、業界別や手法別にカテゴリ分けし、対策や実録コラムもあわせて掲載

その他、**本月間関連行事**は**オンライン中心に約140件開催**
中には、セキュリティに関する無料講座キャンペーン等もみられた

実施による主な効果

◆ 期間中の**特設ページPV(ページビュー)数は延べ約17万回**(前年比10%増)

※アンケート(n=1,050)

◆ **新たな対策の実施**(回答者の63%が実施:うち無線LANルータ26%、パスワード関連17%)**や身の回りの方への情報シェア**(回答者の53%が実施:うち家族30%、同僚20%)につながった。

※ 本月間の実施結果・アンケート結果については、官民のアクションプランである**「サイバーセキュリティ意識・行動強化プログラム」の見直しにも活用**予定

2022年「サイバーセキュリティ月間」（アンケート結果等）

■ インターネットを通じてサイバーセキュリティ月間の認知度や取組に関するアンケートを実施したが、世代別の回答率をみると、10代以下：9%／60代以上：7%と低い水準であった。

⇒従来のインターネット(SNS等)を通じた普及啓発・情報発信だけでは、子どもやシニア層等に十分な周知・訴求ができない可能性がある。

■ アンケートにおいて、「サイバーセキュリティに関して気を付けるべきことを伝えた人」は、20代～50代(26～33%)では「家族やパートナー」という回答が最多。 (cf. 10代以下(28%)・70代以上(25%)では「友人」が最多)

⇒勤務先等でサイバーセキュリティに関する知識をアップデートする機会のある就業層を通じて、家庭内で子どもや両親等に知識を伝えていく役割が期待できる。

■ 事業者とコラボした具体的対策の発信に関し、アンケート・Twitterにおいて「要点が纏まっており見やすかった」、「信頼できる機関による発信であり、周囲にも展開・推奨しやすい」等の好意的な反応が見られた一方で、「対策に関する発信内容が一般人にはまだ難しい」等の反応がみられた。

⇒呼びかけだけではなく、実際のユースケースにまで踏み込んだ対策方法や、動画等を活用した更にわかりやすいコンテンツの開発・更なる発信が必要である。

＜その他、アンケート等で挙げられた声【抜粋】＞

○家庭用の無線LANルーターに関し、アップデートが必要なことやサポート期間が設定されていることを知らなかった。(多数)

○高齢のスマートフォンユーザーには、初歩的なアドバイスが必要。

○通報や相談等のできる連絡先(電話番号やメールアドレス)を知りたい。

○全ての企業が強固なセキュリティ対策を実施できるわけではない。情報は漏えいすることを前提に、どのような対策・行動をすべきかの指針を示して欲しい。

各主体が負っている役割・責務等の例（1/2）

主体		法令等の規定の例
世代別	青少年の保護者	**〇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（平成二十年法律第七十九号）** （保護者の責務） 第六条　保護者は、インターネットにおいて青少年有害情報が多く流通していることを認識し、自らの教育方針及び青少年の発達段階に応じ、その保護する青少年について、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、青少年有害情報フィルタリングソフトウェアの利用その他の方法によりインターネットの利用を適切に管理し、及びその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ものとする。 ２　保護者は、携帯電話端末等からのインターネットの利用が不適切に行われた場合には、青少年の売春、犯罪の被害、いじめ等様々な問題が生じることに特に留意するものとする。
地域の主体	警察	**〇警察におけるサイバー戦略について（依命通達）（令和四年四月一日　警察庁次長）** 第２　サイバー事案への対処を担う主体 サイバー空間における脅威に的確に対処するには、各主体がそれぞれの役割を十分に理解し、相互に緊密な連携を図ることが重要である。 ２　都道府県警察 サイバー特別捜査隊の設置に伴い、今後は同隊において重大サイバー事案の捜査等を推進することとなるが、これによって、都道府県警察の責務は何ら減ずるものではない。 また、国民の安全・安心を確保するため、サイバー事案に関する実態把握から被害防止対策の浸透に至るまで、地域社会との連携の重要性は一層高まっていることから、都道府県警察は、警察本部・警察署・交番等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・対策等を推進する役割を担う。
	学校	**〇学校教育の情報化の推進に関する法律（令和元年法律第四十七号）** （基本理念） 第三条　（略） ５　学校教育の情報化の推進は、児童生徒等の個人情報の適正な取扱い及びサイバーセキュリティ（略）の確保を図りつつ行われなければならない。 ６　学校教育の情報化の推進は、児童生徒による情報通信技術の利用が児童生徒の健康、生活等に及ぼす影響に十分配慮して行われなければならない。 （学校の設置者の責務） 第六条　学校の設置者は、基本理念にのっとり、その設置する学校における学校教育の情報化の推進のために必要な措置を講ずる責務を有する。
	地方公共団体	**〇サイバーセキュリティ基本法（平成二十六年法律第百四号）** （基本理念） 第三条　（略） ２　サイバーセキュリティに関する施策の推進は、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。 （地方公共団体の責務） 第五条　地方公共団体は、基本理念にのっとり、国との適切な役割分担を踏まえて、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。

各主体が負っている役割・責務等の例（2/2）

主体		法令等の規定の例
地域の主体	関連事業者等 (携帯キャリア等)	**〇サイバーセキュリティ基本法（平成二十六年法律第百四号）** （基本理念） 第三条　（略） 2　サイバーセキュリティに関する施策の推進は、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。 （サイバー関連事業者その他の事業者の責務） 第七条　サイバー関連事業者（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。以下同じ。）その他の事業者は、基本理念にのっとり、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、国又は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ものとする。
事業者区分	親事業者	**〇下請中小企業振興法（昭和四十五年法律第百四十五号）に基づき経済産業大臣が定める振興基準** 第３　下請事業者の施設又は設備の導入、技術の向上及び事業の共同化に関する事項 ５）情報化への積極的対応 (2)親事業者は、前号の下請事業者による取組の支援のため、下請事業者の要請に応じ、管理能力の向上についての指導、標準的なコンピュータやソフトウェア、データベースの提供、オペレータの研修、セキュリティ対策の助言・支援及び国・地方自治体による情報化支援策の情報提供等の協力を行うものとする。（略）
	下請事業者	**〇下請中小企業振興法（昭和四十五年法律第百四十五号）に基づき経済産業大臣が定める振興基準** 第３下請事業者の施設又は設備の導入、技術の向上及び事業の共同化に関する事項 ５）情報化への積極的対応 (1)下請事業者は、管理能力の向上、事務量軽減、事務の迅速化等の業務工程の見直しによる効率性の向上のため、必要なセキュリティ対策と併せて、次の事項に積極的に対応していくものとする。（略）

※ 注：大企業等から取引先等へサイバーセキュリティ対策を要請する上で課題となりうる法規制の例

- 下請法における、親事業者の禁止行為(親事業者が指定する物・役務を強制的に購入・利用させる「購入・利用強制」等)
- 独占禁止法における、自己の取引上の地位が相手方に優越している一方の当事者が、取引の相手方に対し、その地位を利用して、正常な商慣習に照らし不当に不利益を与える行為(優越的地位の濫用)

誰もが最低限実施すべき対策：サイバーセキュリティ対策9か条

- 一般国民向けの普及啓発活動に関し、共通的に活用できる対策メッセージを整理。
- 国民のデジタル活用の状況や技術の進展、脅威の動向等を踏まえ、必要に応じて適時アップデート。

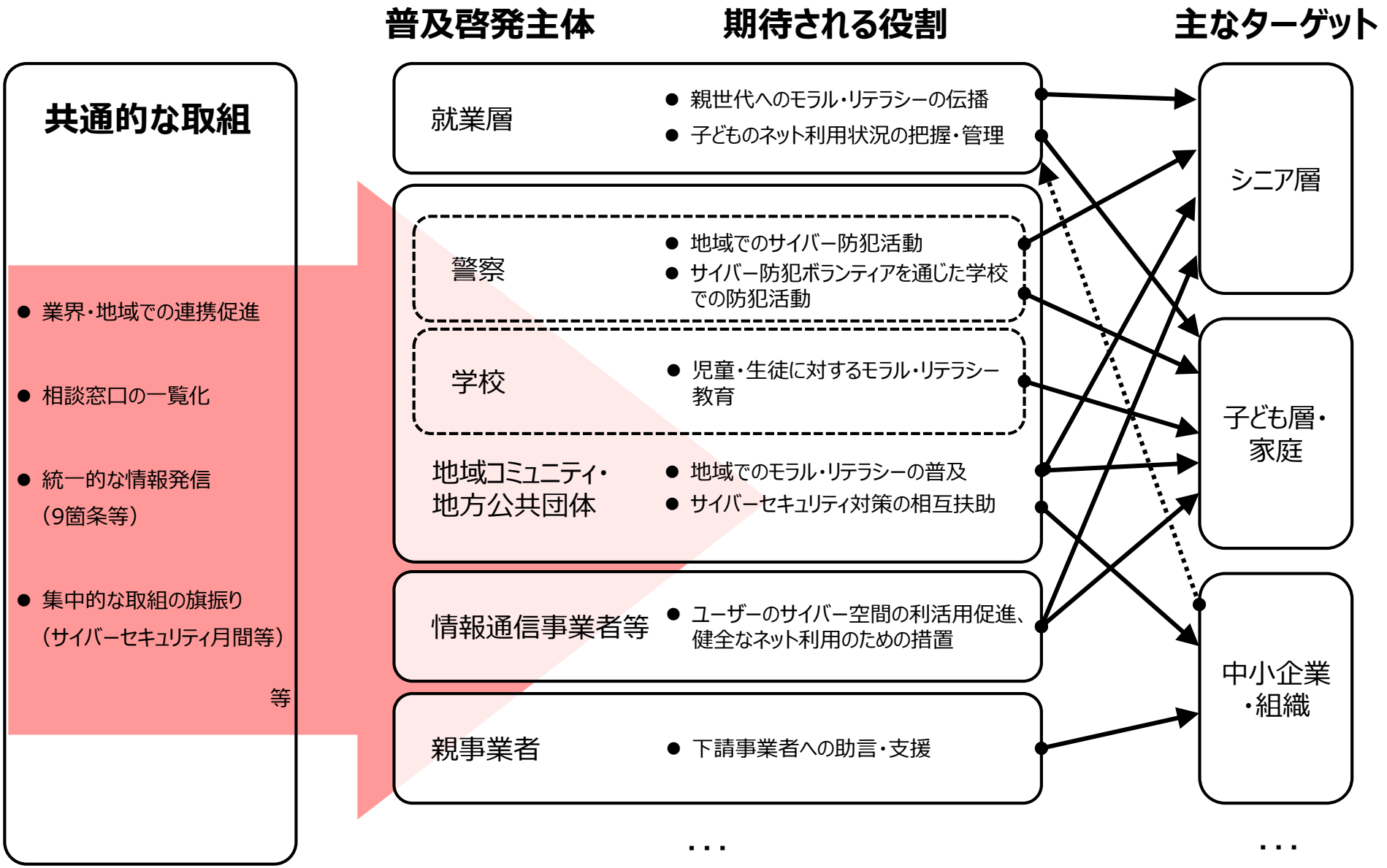
	9か条	備考
1	**OSやソフトウェアは常に最新の状態にしておこう**	○OSにセキュリティに関する機能が備わってない場合は、新たにセキュリティソフト・アプリを導入することも周知。 ○無線LANルーターのファームウェア更新も含めて周知。
2	**パスワードは長く複雑にして、他と使い回さないようにしよう**	○パスワードに関する留意点や安全なパスワードの作成方法、管理方法、使い回しの危険性について具体的に周知。
3	**多要素認証を利用しよう**	○近時、多くのOSメーカーが共通して推奨。
4	**偽メールや偽サイトに騙されないように用心しよう**	○Webサービスアカウント情報やサポート詐欺による金銭の搾取や、公式サイト以外からのアプリ等をダウンロードすること等に対する注意喚起。
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**	○近時再度猛威を振るうフィッシングメールやEmotetへの注意喚起などに関し、具体的な留意点を周知。
6	**スマホやPCの画面ロックを利用しよう**	○情報漏洩の防止等に高い効果が期待できる画面ロック機能(※シニア層程利用率低い)の活用推奨を含む。 ○この中で、指紋や顔等の生体認証の利用や、安易に他人に端末を渡したり、操作させたりすることの危険性にも触れる。
7	**大切な情報は失う前にバックアップ(複製)しよう**	○機器の故障やサイバー攻撃によって、スマホ等の機器に保存されているデータが滅失するリスクがあることを理解し、適切に複製・保管しておくことの重要性に言及。
8	**外出先では紛失・盗難・覗き見に注意しよう**	○飲食店等で離席時に端末をつい置き去りにすることや、公衆の場で利用する時に覗き見られたりすること(ソーシャル・エンジニアリング)への注意喚起。
9	**困った時はひとりで悩まず、まず相談**	○困ったり、迷ったりしたときに相談できる人を確保しておくことの重要性と、都道府県警やIPAをはじめとする相談窓口に言及。

※ 2015年にNISC・IPAで整理して発信した内容から一部アップデート（3・6を追加した上で、項目を整理）

対象別の取組の例と課題

	現状の取組例	課題
シニア層	・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	● 現時点でシニア層に特化した内容・形式ではない どこへ相談するべきかわからない高齢者が多い
子ども・家庭	・中：技術・家庭科／高：情報Ⅰ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 ⇒ 研修用教材の提供、担当教員の採用・配置の促進等	家庭でのルール設定、利用状況の把握の促進 ● 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・教職員等に対する無料の出前講座	● 認知度の向上
	・(一社)電気通信事業者協会等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	● 好事例の展開、教育機関との連携
中小企業・組織	・「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)	● 認知度の向上 クラウドサービスの設定ミスの防止
各主体の連携	・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・窓口の集約・可視化されていない
	・産学官民の施策をまとめたポータルサイトの充実	● 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」の充実	● 各種ガイドラインの関係性が不明瞭
	・「サイバーセキュリティ月間」の推進	● 更なる知名度の向上 ⇒ 民間企業・団体の更なる巻込

各普及啓発主体の役割イメージ



本日ご議論いただきたいこと

■ 本日は、**①下記の構成見直し(案)**、**②今後発展させるべき具体的な取組(4.)の方向性**について、ご議論をいただきたい。

⇒本日の議論を踏まえて、各省庁含め見直し案を検討、必要に応じて概算要求等に反映の上、秋頃に見直し本文(案)を改めてご議論をいただく予定。(その後、サイバーセキュリティ戦略本部に諮ることを想定)

「サイバーセキュリティ意識・行動強化プログラム」目次 見直し素案

1．はじめに

○制定の経緯：サイバー空間をめぐる環境変化(デジタル庁設立、コロナ禍によるデジタル化の進展)や、サイバー脅威の動向(サプライチェーン、国際情勢)、CS戦略(「見直しを検討する」)に基づき改定。

○文書の役割：産学官民の取組の方向性を示すもの。

※「人材育成」との関係性：「普及啓発」は多様な人材が活躍し、次世代を引きつける基盤に。人材育成施策は除外。

2．現状

（1）ネット利用・対策等の状況：サイバー空間に参画する層の拡大／それに伴うサイバーセキュリティ対策の不足

○個人：ネット・スマホの普及層拡大／行政手続電子化・ICT教育・遠隔医療等の進展／スミッシングの拡大

○企業・組織：中小企業・組織のデジタル化／製品・サービスのデジタル化進展、テレワークの普及／ランサムウェア被害の拡大

（2）現状の取組の課題：各省庁等の取組に関するPDCA

3．基本的な考え方

（1）原則：CS基本法上の各主体(国民・教育機関・サイバー関連事業者・国)の責務・努力・施策を再規定。「Cybersecurity for All」に基づき、誰一人取り残されないよう、社会全体として目を配る。

（2）ターゲット：

① ICT技術の進展についていきづらい → シニア層(＋認知・運動機能の問題等)、非就業層等

② ICT技術の活用に規範形成が追いつかない → 子ども層

③ セキュリティ対策の負荷が大きい → 中小企業・組織

3．基本的な考え方【つづき】

（3）各主体が担うべき役割：

主体の例：就業層、サプライチェーン(サプライヤ)、情報通信事業者等、地域(シニア活用含)、教育機関、業界団体等

（4）誰もが最低限実施すべき対策：9か条

4．具体的な取組：各重点対策につき、特に期待される役割を担う主体を明記し、代表的な施策のみ記載。

（1）ターゲットへの重点対策

① シニア層対策： 情報通信事業者等・地域団体、家族を通じた取組促進

② 子ども・家庭向け対策： 教育機関、家庭・親子、地域を通じた取組促進

③ 中小企業・組織向け対策：サプライチェーン(サプライヤ)を通じた取組促進

（2）各主体の連携強化

① 地域における支援・協議会の連携：例）地域ごとの窓口の一覧化

② 取組の一覧化：例）ポータルサイト、黄色ハンドブックの拡充

③ 情報発信： 例）SNSアカウント等の各主体の役割明確化

④ 集中的な取組：例）「サイバーセキュリティ月間」の企画の発展

5．取組のPDCA・対外発信

○専門調査会を活用し、年次報告プロセスでフォローアップ。必要に応じ改訂。

○外国人へのアプローチや対外発信を念頭に、必要なコンテンツ(特に9箇条)を英訳し発信。

※ アクションプラン表題について見直すことも検討の対象。