資料5

「情報セキュリティ普及・啓発プログラム」
今後の方向性ヒアリング結果

目的など

1．目的

- 現在の普及・啓発の中長期プログラムである、「情報セキュリティ普及・啓発プログラム」（2011年7月情報セキュリティ政策会議決定）は、3年間を対象と規定されており期限は2013年度まで。
- サイバーセキュリティ戦略（2013年5月情報セキュリティ政策会議決定）の中で、同プログラムを見直し、必要に応じて新たな計画等を策定するとされている。
- そこで、上記プログラムに次ぐ、2014年度以降の複数年度を対象としたプログラムの策定にあたって、取組むべき重点分野の抽出等に資する観点から、有識者（普及啓発・人材育成推進方策検討ワーキンググループ構成員）と意見交換を行っているもの。

2．意見交換事項

① これまでの普及・啓発プログラムについて
現在のプログラムの内容、進捗状況等

② 次期の普及・啓発プログラムの意義・目的
基本的考え方、目指すべき姿等

③ 今後取り組むべき重点分野
重点点的に取組むべき対象層、テーマ等

④ 普及啓発において発するメッセージと、伝達手段について
発信するメッセージの内容、発信する際の考慮点等

⑤ その他意見等

ワーキンググループ委員

小泉　カー 【主査】	学校法人尚美学園 尚美学園大学大学院 教授 文部科学省 生涯学習政策局 学習情報官
青田　哲	日本電信電話株式会社 技術企画部門 セキュリティ戦略担当 担当課長
石井　茂	独立行政法人情報処理推進機構 技術本部セキュリティセンター 普及グループ グループリーダー
伊藤　求	ニフティ株式会社 セキュリティ推進室 課長
井上　真由美	株式会社ミクシィ ユーザーサービス本部 CS推進部 健全化推進 渉外
尾花　紀子	ネット教育アナリスト
勝村　幸博	株式会社日経BP社 日経パソコン 編集 副編集長
川上　隆	学校法人岩崎学園 情報科学専門学校・横浜医療情報専門学校 教務部長
高　元伸	ヤフー株式会社 CSO室　室長
小屋　晋吾	トレンドマイクロ株式会社 執行役員 統合政策担当部長
近藤　則子	老テク研究会 事務局長
清水　啓一朗	ソフトバンクモバイル株式会社 セキュリティ本部 本部長
下村　正洋	株式会社ディアイティ 代表取締役社長 特定非営利活動法人日本ネットワークセキュリティ協会 事務局長 特定非営利活動法人日本セキュリティ監査協会 理事 セキュリティ対策推進協議会 代表
杉浦　昌	日本電気株式会社 CSIRT推進センター シニアエキスパート
高橋　正和	日本マイクロソフト株式会社 チーフセキュリティアドバイザー
千原　啓	グリー株式会社 経営基盤本部　政策企画部長
中森　康治	株式会社エヌ・ティ・ティ・ドコモ 情報セキュリティ部 情報管理担当部長
西本　逸郎	株式会社ラック CTO 専務理事
※土生　尚	日本放送協会 情報システム局 IT企画部長
藤本　浩司	株式会社電通 ビジネス統括局　局次長
前田　典彦	株式会社カスペルスキー 情報セキュリティラボ チーフセキュリティエヴァンゲリスト
武笠　貴史	KDDI株式会社 技術統括本部 運用本部 セキュリティオペレーションセンター CSIRT グループリーダー
村上　智	株式会社シマンテック 執行役員 セールスエンジニアリング本部長
本橋　裕次	マカフィー株式会社 サイバー戦略室兼グローバル・ガバメント・リレイションズ 室長
矢野　敏樹	グーグル株式会社 公共政策カウンセル
吉田　正彦	一般財団法人マルチメディア振興センター 特別研究主幹 プロジェクト企画部長

※ご担当者様交代と重なったため、ヒアリング実施できず。

コンセプト、基本的考え（その１）

①「セキュリティは日本の品質の一部。国力を示す指標の一つ」という考え方。

- 日本はコンタクトリスクについて注意を払うが、セキュリティの様な見えない敵に対して経験が浅い。欧米は逆。
- 社会的に見て、セキュリティは根幹。企業が他国と競争する上でセキュリティは重要であり、国力を示すベース（指標）の一つ。日本らしさを示すことが求められる。損得勘定ではなく、「やるしかない」という覚悟で臨むべき。日本の高品質の一つであって、「セキュリティをやらないとおかしい」といった意識の醸成が求められる。
- セキュリティの普及啓発には合意形成が必要。企業において、「セキュリティは品質の一部」という考え方の合意形成ができれば、取り組み方が変わる。他の例として、環境問題を品質確保の一つとの合意形成のもと、取組んでいった。

②「ポジティブな不安」によって「正しく怖がる」ことで、緊張感を持って行動する。

- 安心しきっていてはダメ。「やや不安。でも安全」。「やや不安」については、ポジティブな不安。前向きな不安があるから、危機意識が生まれ、緊張感を持って取り組むことができる。緊張感が無いと問題が発生する。
- 危ないから、怖いから「見ない、利用しない」といった「間違った怖がり方」では事故を防ぐことはできない。「正しく怖がる」ことが大切。
- セキュリティの怖い面を必要以上に露出すると、使わなくなるなど極端な考えの方も出てくる。あくまでもIT利活用があって、その中でセキュリティ対策が行われるという流れが必要。

③「本人のためのセキュリティ対策」という当事者意識を持たせ、年代に応じて本質を理解させる。

- 対象者にリーチするには、対象者が当事者意識を持つことが大事。
- 自分が加害者に成りうることを分かってもらう点について、もっと取り組むべき。
- 自分を守るために必要なモノという認識を持たせることが重要。あなたが楽をできるのよ！という訴求。
- 小学生は「べからず集」的な教え方が中心。中学生については、リスク教育等、本質を知るような教育。
- 「●●はダメ」だけでなく、「▲▲だから、●●はダメ」というように、本質の理解が必要。▲▲が理解できれば、利用シーン（ハード種類、アプリ種類、サービス種類等）が変わっても応用できる。
- 初等中等教育層への取組は、対象者のインセンティブを念頭に置くというよりは、当たり前の事として教育していく取組。初等中等教育を重視して、子供たちが社会に出た時に自然と（当たり前のように）できるようにする。

コンセプト、基本的考え（その２）

④愚直にやり続けるものもある。

- プログラムの中には、５年・１０年と愚直にやり続けるべきものもある。２月のセキュリティ月間や１０月の国際キャンペーンのような取組はその一例。

⑤対象者のインセンティブを確保する。

- インセンティブがあると、企業側も取組の糧になる。大規模企業においても、セキュリティ対策に対する効果説明には苦労している。

注力する所、ターゲット（その１）

①ターゲットを絞る。年齢層、旬な課題、女性、etc

- ターゲット層を絞ってそれぞれに対して普及啓発活動を展開。年齢層や、旬な技術課題に絞るというアプローチの他、女性をターゲットにすることも一案。
- ターゲットを絞り込むべき。個人と企業は伝えるメッセージが異なる。個人向けと考えた時に、特に注力する箇所は、「今、社会問題になっている所」に注力する。

②意見数No．１　小学校～高校の層をターゲットにする意見（子供の時に覚えたことは大人になっても忘れない）。

- ターゲット層を絞るのであれば、小学校～高校生までを対象にすると良い。この年齢時期に慎重さを学ばないと、中々身につかない。
- 子供を中心にアプローチすると良い。子供が大きくなった時には全体的にセキュリティが高まる。
- 子供の時に理解させ、成長した後に当たり前になっていることが必要。初等、中等教育の中で、子供に教え、先々を手当てすることが重要。
- 小中学生をターゲットにすると良い。小さいうちに身に着けたことは大人になっても忘れない。
- 中高生にターゲットを絞ってはどうか。子供たちが知ってたら、親や高齢者に教える。
- ターゲットは、保護者や教職員など、子供へ影響を与える層。
- 小中校の先生のセキュリティレベルは全体的に低い。
- 学校授業の情報科目は、その専門の先生が教えているのではなく、たまたま他の先生よりも知っているというケースが多い。先生も初心者。情報を担当する先生を組織的にサポートすることが有効。

③意見数No．２　高齢者をターゲットにする意見（学ぶ機会が少ないため国の支援強化が必要）。

- 高齢者にニーズがあることの背景は、知る機会が無いため。
- 高齢者は、ICTを学ぶ機会が無いので、この層へのケアも必要。子供や就労者は帰属する組織があるので、教わることができる。高齢者は組織に帰属していない。地域コミュニティ等に参加している人もいるが約60%程度。高齢者全般へ取組を届けることは困難。

注力する所、ターゲット（その２）

④意見数No．３　主婦をターゲットにする意見（理由は高齢者と同じ）。

- ４０～５０代の女性（主に主婦）を中心に普及させ、そこから子供や高齢者に伝わるようになる。
- ４０～５０歳の層は、ちょうどWindows95が出てきた時代にPCを使い始めている。この時代のPC利用者は、リテラシーを考えずにPCを使い始めておりケアが必要。この層は、ちょうど、若い経営者や、主婦の層に該当。
- 団塊世代の主婦層はICTを習う機会が無かったので、リテラシーが低い。

⑤意見数No．４　企業をターゲットにする意見（経済効果的側面を期待）。

- 環境問題は、まず企業が動いて、それが広がった。セキュリティについても、企業の社会責任として活動を広げることが出来るのではないか。企業としても、既に取り組んでいるケースもあり、この場合は新たな費用が掛かるわけではない。
- てっとり早く盛り上げるならば、企業をターゲットにして取組ことが良い。企業の取組が進めば経済の流れも変わる。

⑥旬な課題、技術的課題をターゲットにする意見。

- 今後どういう所に取組んでいくかについては、「Wi-fi、クラウド、スマフォ」。
- 例えば現在であれば、アカウント／パスワードの管理や、サクラサイト商法、ネットバンク被害。
- ターゲットを絞るならば、スマートフォン。課題は2つ。１つは不正アプリの問題。便利なツールを装ってユーザに利用させるなど手口が巧妙。代表的なアプリ提供サイトから、問題あるアプリを提供しているケースもあり、安心できるサイトが判断できない。２点目の課題は、様々な機能（お財布機能、クレジット機能、電話帳等）が１台の端末に搭載されている点。複合的な脅威を認識する必要がある。一般に、クレジットカードの取り扱いは慎重になる。スマフォもクレジットカードのようなモノなので、同じく慎重に取り扱うべき。
- 現在のスマートフォンの問題は、セキュリティというよりは、プライバシーをどう守るかのコンテキスト。スマフォのボット化によるDDos攻撃といった懸念はこれから。
- ターゲットについて、SNSも注力すべき。SNSでは個人の行動を自ら公開している。これら行動を追跡することで、攻撃者は有力な情報を得ることができる。公開範囲を「友人まで」と設定していても、誤って面識ない人と友達になってしまうと、自らの行動が攻撃者に晒される危険がある。

目標

①ターゲットを設定すべき。セキュリティ業界、企業、国民一体となって目標達成に向け活動する。

- ターゲットを絞りながら、そして、ゴールを明確にする。
- ゴールを設定できると、皆で目指すことができる。目標を設定すると良い。
- 皆で目標を掲げて活動することは良い。この場合、目標の達成度合いを測る指標が必要。
- ムーブメントを起こすには、共通言語（キャッチフレーズ）、目標を定めてPR活動を行うとともに、インセンティブが明確になると良い。

②具体的なターゲット例としては、具体的な数値目標が良い。

- 環境問題の時は、「チームマイナス6%」というメッセージがとても効果を発揮した。このメッセージには、具体的な数値目標があるので判り易い。セキュリティについても、例えば、意識の度合いや行動の度合いを目標にしてはどうか。
- セキュリティで普遍的に変わらないことは、「定期的に点検する習慣をつけること」。これを目標にしてはどうか。
- 数値目標があると判り易い。例えば、マルウエア感染率を●●%下げる。などあれば、キャリアも頑張り易い。

③ターゲット設定時の留意点（技術、マナー、危険性、対応策など分けて目標値を考える）。

- 技術の話と、マナーの話がまざると判り難い。これらを分けてKPIで表現すると判り易い。例えば、技術の話であれば、その施策を実施することで感染率を下げるとなる。マナーの話であれば、その施策を実施することで、アンチウイルスソフトを導入する割合が●●%向上するとなる。
- ターゲット（数値目標）を設定するべき。普及啓発活動に目標を設定するにあたり、その活動の指標について考える必要がある。「不安を感じる割合」を指標にした場合、これまでセキュリティを知らなかった層が、セキュリティの危険性を理解することで（これは望ましい状態なのだが）、「不安を感じる割合」が増加することになる。そのため、初心者向けの指標を別途考えるべき。指標は、「危険性」と「対応策」を分けて考えるべき。

手法（その１）

①店頭販売時の普及啓発を活性化させることが有効。

- 新聞広告は3秒、TVコマーシャルは15秒。時間制約の中で、極端なメッセージになる。セキュリティの場合は、もっと時間をかけて伝えるような媒体（リッチなメディア）が向く。例えば、販売店の店頭からの情報伝達が有効。店頭に来る人は、新聞・TVに比べて、長い時間をかけて店内の情報を見る。
- 国民へメッセージをリーチするシーンとして、販売店でスマフォなどを売る時が一つのケース。しかしながら販売店には説明義務がなく、必ずしも有効に機能していない。
- 販売窓口からの取組としては、例えば、スマフォお助けガイドや、安心Bookなどがある。

②ターゲットを絞って、ターゲットの言葉でメッセージを発信する。

- 万人に向けて作ったものが、万人にウケることは無い。ターゲットを絞って作ったものが、結果的に万人にウケることはある。広げることは後で考える。
- ターゲットの理解を引くために、ターゲットの言葉で考える（例：高齢者→おばあちゃんの言葉）。
- ターゲット層別にアプローチを分けることが必要。ターゲット層に応じてアプローチが異なる。総務省のスマートフォン3カ条は、知っている人が見ると判り易い表現。しかし、e-ネットキャラバンの対象となる主婦層には難しい表現。OSという言葉も理解できない。
- 子供を対象とした活動をしているにあたり、セミナー要望が多いのは６～７月。これは、新学期の後に、夏休み前に教えておきたいというニーズ。

③セキュリティ単独では無く、ICT利活用と一体した普及啓発が効果的。

- 青少年育成や、ICT利活用の普及啓発の場でセキュリティも説明を行うなど、セキュリティ以外が主役の普及啓発の場を有効に活用すると良い。
- セキュリティに限定せず、スマフォやタブレットの活用方法等、ICT利活用を学ぶ場が必要。そしてその講座の中で、セキュリティについても触れることが良い。
- 高齢者のサポート役として必要なのは、セキュリティの事をしっかり知っているような人ではなくて、端末の利用方法等の相談に乗ってあげるような人。セキュリティの高い知識は不要だが、セキュリティ対策で最低限のことをICT利活用の一環として教える。そしてそのような人が活動する上で、何らかの資格があった方が活動しやすい。

手法（その２）

④一体感ある活動を行う。

- セミナー等のイベントを一ヶ所から公開する。
- 皆で同じポスターやパンフを使うと一体感が出る。

⑤著作権フリーの資料を提供することを検討する。

- コンテンツの有効な活用を期待。最新情報を分かり易く、著作権フリーで、どこかのHP等にまとめて掲載。
- コンテンツの相互利用は良い取組み。著作権に配慮しながら実現したい。

⑥テレビ、お笑い、SNS、LINEなど、国民が日ごろから親しんでいる媒体の活用を検討する。

- TV番組からの訴求が効果的。人の心に入るためには、コント・お笑い・寸劇・ゴロ合わせなどを考え、面白おかしく伝えることが出来ると良い。ツイキャスを活用してはどうか。ニコ動も有効。ニコ動にするなら、オープン（会員以外が見られる）にしないと効果がない。動画の中で、四コマ漫画を流してもよい。
- 事故の悲惨さを知ってもらう取組も効果的。セキュリティもTVからの露出を増やすと良い。「警察24時」の中でサイバー犯罪捜査を取り上げることも考えられる。
- セキュリティ芸能人を用意できると、集客において、セキュリティ以外の目的で人が集まる。セキュリティギャグネタで盛り上がる等、一定の効果が期待できる。
- 子供から大人、高齢者と様々な層があるが、それぞれの層に応じて、『この人のいうことなら判る』という人がいる。そのような人から説明することが効果的。
- 効果的なリーチ方法としては、各種サービスを利用する時の一連の流れの中で、ポップアップ表示すると効果的。利用したいシーンで表示されれば、必然的にメッセージを確認する。
- 日ごろから使う所（スマフォや、SNS、等）からメッセージを伝える。日ごろから目にすることで、繰り返し効果が有効。
- 対象者へリーチする手段については、「LINE」が有効。
- 何かを伝える時は、文字だけでなく、動画。一番良いのは、実際に触れること。
- セキュリティの事件事故は、実際に経験しないと自分事と思うことができず対策をしない。疑似体験をすることが有効。

手法（その３）

⑦月間の取組みについて。

- イベントは複数設定するよりは、一つに集中させた方が判り易い。ニュースとして扱いやすいイベントが良い。キックオフイベントだけでは書きづらい。昔のように、ピンポイントで特定の日にちがあった方が良い。「月間」のような期間モノは記事になりにくい。
- セキュリティ月間のイベントをもっと大々的にイベント化する。例えば、２月の最初と最後でアンケート等の調査を行い、国民意識を集計を行うことはどうか。そしてそれを継続的に行うことで、活動成果の確認を行う。
- ２月以外も、継続的にイベント月があると良い。例えば、毎月テーマを変えて行うなど。頻度は、2ヶ月毎や、３か月毎でも良い。企業側が中心となって行うことでも良い。この場合、企業の販売促進目的とはしないことで、国からはその活動に対する後援や、HP掲載等、なんらかのお墨付きが欲しい。

⑧その他

- 手に取らせるためのメッセージと、やってもらうメッセージは違う。バナーの役割は手人ってもらうメッセージ。
- 運動に名前を付けて活動する。共通のシンボルを与える。企業が出しているセキュリティ報告書について、例えば国からのお墨付きを与える。
- セキュリティ対策OKの企業にお墨付きを与えるなどしても盛り上がる。
- 広告のプロを使うアプローチは効果的。IPAでもH23年度に広告を活用。トレインチャンネル（山手線）、雑誌、Yahooバナー等によって広告活動を実施。HPアクセス数が前年度比2倍という結果。広告には費用がかかる。皆が同じメッセージを使って、費用負担することができると良い。
- 普及啓発等の活動をHPに掲載したのでは、興味がある人にはリーチできるが、興味が無い人には届かない。Push型の広報を行う必要がある。過去にIPAが行ったトレインチャンネルのような方法や、TVやラジオ等の公共放送からの広告が良い。
- セキュリティは変化のスピードが速く、導入した対策の寿命が短い。導入した設備が減価償却前に陳腐化する。減価償却について何らかの手当てができると良い。
- アンチウイルスソフトは販売時にデフォルトONで売ってはどうか。例えば、販売店で、幾つかのソフトをデフォルトONで売っている。同じことが出来ないか。いらなくなればOFFにすれば良い。
- 委託先のセキュリティレベルについて、一定レベルの確保を求める。レベル確保のチェックはセキュリティ監査によって行う。

メッセージ

- メッセージについては、旬な最新情報を伝えるという切り口と、媒体等が変わってもかならず行うこと（OSパッチ更新など）を分けてそれぞれ発信することが良い。
- 個人向けは、個人として被害に合わないためにどうするかというメッセージであれば、自分の事として捉える。伝える内容は同じで、それぞれの層に合わせて表現を変える。この時、セキュリティに閉じるのではなく、ICTの普及啓発と一緒に進めるイメージではないか。
- 企業の場合は、経営層に対するメッセージが中心。アンチウイルスやFW、GW防御などは一通り入っているので、その運用を確実に回すための体制確保が中心。

- 東日本大震災以降、「情報」の関心が高まってきた。IT、ネットワークではない「情報」のアプローチが重要。「情報」を再認識（わかりやすくする）ことが必要。
- 生涯学習という言葉がある。健康、経済などの他に、「情報」についても学習する必要が出てきたことを伝える時期に来たのではないか。「世の中便利になった、ただし、便利のウラには危険がある。情報にも落とし穴がある。」というようなメッセージを伝えてはどうか。

- 今後スマフォも無くなるだろうし、キーボードも無くなり喋るだけで良い環境が出てくるとしたら、そのような技術変化が起きても変わらずに通じるメッセージを発信する。

サイバー・クリーン・デー（仮称）について

①「サイバー・クリーン・デー」の名称は判り難いという声が多数。何をする日か判る名称にすべきとの声が複数（「セキュリティ点検をする日」として、「セキュリティ・チェック・デー」）。

- 名称については、サイバークリーンセンターを知っているので特に違和感はない。
- 名称が判り難い。やってもらいたいことがズバリ判る名称が良い。攻撃に対する訓練の日にしてはどうか。
- 課題を明確にすると良い。その結果として名称が決まるのではないか。
- 「サイバー」という表現はどこか遠くの言葉のように聞こえる。自分の身の回りの出来事と感じる人は現時点では少なく、今の土壌にはそぐわない。大切なことは、自分の身に起こるんだという意識を醸成すること。
- 「サイバー」という言葉は一般国民向けには判り難く、何か別世界の言葉に思えてしまう。例えば「セキュリティ・チェックデー」という言葉の方が判り易い。サイバーという言葉を入れたいのであれば、長くなるが、「サイバー・セキュリティ・チェックデー」の方が、「サイバー・クリーン・デー」より判り易い。
- 「情報セキュリティ月間」では、何をするのかよくわからない。タイトルを「情報セキュリティ点検月間」とすると、具体的になって判り易い。

②表彰等イベントを行うことで、盛り上げ効果を期待する。

- 表彰を行うのであれば、サイバーセキュリティ業界から選出するのではなく、利用者の中でセキュリティをがんばった人を選出すると良い。
- 何か日にちを設定するならば、イベントがあるといい。体験型のイベントが良いのではないか。

③日にちについては、２月が多数。１０月は少数。年間通して訴求する観点から毎月という意見も。

- 継続的な活動が定着を生むので、２月ということであれば、それはそれで良いのではないか。
- 普及啓発活動は、現在のように２月、１０月に限定するのではなく、毎月１回、継続的（１０年続けるなど）に行うことが良い。例えば、毎月●日はセキュリティをチェックする日ということにしてはどうか。チェックする内容は毎月変えていっても良い。

④新置反対意見。

- 「サイバー・クリーン・ディ」については、それが国民運動に繋がるとは思えない。そのお金を、例えば、セミナー等の講師謝金等へ活用する方が効果的。例えば、セキュリティサポーター向け勉強会を●●人以上集めて行うなら、補助金を出します。ということが出来ないか。