資料１

普及啓発・人材育成推進方策検討ワーキンググループ
第４回会合　議事要旨（案）

１　日時

平成24年2月22日（水）　10：00 ～ 12：00

２　場所

内閣府別館９階会議室

３　出席者（敬称略）

（主査）	小泉　力一	尚美学園大学大学院教授
（委員）	浅川　玲	日本放送協会
	荒木　浩一	株式会社エヌ・ティ・ティ・ドコモ
	伊藤　求	ニフティ株式会社
	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
	川上　隆	学校法人岩崎学園
	小屋　晋吾	トレンドマイクロ株式会社
	佐竹　正範	ヤフー株式会社
	里中　慧	株式会社ミクシィ
	杉浦　昌	日本電気株式会社
	高橋　正和	日本マイクロソフト株式会社
	千原　啓	グリー株式会社
	長島　武生	日本電信電話株式会社
	平尾　芳郎	ソフトバンクモバイル株式会社
	藤本　浩司	株式会社電通
	前田　典彦	株式会社カスペルスキー
	武笠　貴史	KDDI株式会社
	村上　智	株式会社シマンテック
	本橋　裕次	マカフィー株式会社
（事務局）	占部　浩一郎	内閣審議官
	泉　宏哉	内閣参事官
	木本　裕司	内閣参事官
	花岡　一央	参事官補佐

４　資料

資料１　普及啓発・人材育成推進方策検討ワーキンググループ第３回会合　議事要旨
資料２　平成２４年度の情報セキュリティの普及啓発に関する基本的な考え方（案）
資料３　今後のスケジュール
参考資料　普及啓発・人材育成推進方策検討ワーキンググループ委員名簿
参考資料　政府インターネットテレビ・政府広報ラジオにおける情報セキュリティ啓発番組の配信について

５　議事概要

（１）平成２４年度の情報セキュリティの普及啓発に関する基本的な考え方について

事務局より資料２に沿って説明し、委員による意見交換が行われた。委員等からは以下のような意見が述べられた。

①普及啓発の基本的な考え方について

○　情報セキュリティには情報漏えい、ウイルス感染等いろいろな現象があるため、情報セキュリティの意識啓発として括ってしまうと焦点がぼやけるのではないか。現状の把握や目標の設定時にカテゴリわけをきっちりしたほうがよい。
○　目標設定時にKPIのような指標を定め、普及啓発施策により目標が達成されたのか評価できるようにしておくことが大事である。
○　問題がどのような要因で起こっているのかを分類し、大きな要因を普及啓発のターゲットとすれば、対象層も絞られてくる。重点志向で狙いを定めてはどうか。
○　スマートフォン時代を考慮し、今は顕在化していないがこれから起こりうるような問題も含め、優先度をつけて取り組んではどうか。
○　個人情報漏えいについては、通信業界では申込書の紛失等の事故を総務省に報告している。指標となるデータは産業界ごとに所管省庁で集計されていると思う。
○　JNSAが毎年の個人情報漏えいに関するデータをまとめ、分析したものを公開している。参考資料になると思う。
○　JNSAのデータは報道されたものをベースとしているので、メディアが興味を持ったかどうかというところに依存してしまう。データとして使うなら、監督官庁が持っているデータが使えるとよい。
○　企業における個人情報以外の機密漏えいや、個人のセキュリティ事故に関するデータはわからないため、事故ベースで計るのは難しい。行動や意識がどう変わったかという指標がよいのではないか。
○　事件事故についてはいろいろな業界で集計しているが、全体を包括的に捉えているものはあまりないように思う。一般の期待としては、官公庁のものは内閣官房で全体を見渡してもらえるとよいし、民間についても官主導で全体を見渡してもらいたい。
○　事故は、事故に至っていないインシデントのピラミッドの一番上の一つにす

ぎないので、事故以前のインシデントをいかに減らすかが対策には重要である。ただし、個人のPCのインシデントを調べるのは難しいため、どういう対策をしているのかという指標のほうが成果を見やすいと思う。

○　事故に着目するか対策に着目するか、ターゲットが個人であるか企業であるかによって難しさが違い、場合分けすると大きな数になると思う。一方、経年変化で変容をみることも大事であり、どのように計測、説明するかは難しいが、何らかの形でアプローチすべきと思う。

○　厳密に考えすぎると限られた時間の中では議論が難しい。もっとざっくり捉えて、不安を感じている程度、不安だから対策が必要だと感じる程度、必要と感じるから検索しようと思う程度といった意識の指標と、実際に検索行動をしたか、調べた対策を導入したかといった行動の指標を設定し、そのどこを普及啓発で解決していくかを考えるとよいと思う。

②情報セキュリティにおける普及啓発の考え方について

○　情報セキュリティに不安を感じることは対策の原動力となり、悪いことではない。目標は、不安を感じる人をなくすことではなく、情報セキュリティの重要性を知ってもらい、適切な対策を実施してもらうことではないか。

○　パスワードの変更のやり方がわからない、パッチを当てるやり方がわからないなど、パソコンの使い方がわからないところでつまずいている方が多い。一般向けにセキュリティ啓発をする際は、セキュリティだけではなくパソコンの使い方も教える必要がある。

○　「どこまでセキュリティ対策を行えばよいか不明」という課題設定はある程度できる人の発想である。できない人にとっては、何をするのが正しいのか具体的なことが分からないのではないか。

○　セキュリティの普及啓発は、いつどんなものが来るかわからないという点で防災教育に近いと思う。知識や意識の低い人がいることを前提に、トラブルに遭遇した後の被害を最小限にするにはどうするかという課題があると思う。

○　現状については、利用者の心理面等、社会科学的な見地での検討が足りないと思っており、このような切り口による真の原因の調査を長期的に進める必要があると思う。ある程度の期間で目に見える成果を出す観点と二段構えであるとよい。

○　課題や目標がやや専門的な感じがする。ITを正しく使いこなすにはどうするかなど、いわゆるリテラシー的な側面があったほうがよい。

○　サイバー空間も実社会の写像なので情報セキュリティ事故をゼロにはできない。なくすのではなく、いかに減らすかがポイントである。

○　技術的な対策とリテラシーの向上は両輪である。基本的な技術的対策は確実に実施してもらった上で、リテラシーとして気をつけることの啓発をやっていく必要がある。

○　どれだけ対策しても事故をゼロにはできないが、対策によりリスクは確実に下げられる。情報セキュリティ事故もほかの事故と同じであるということ自体

がメッセージとなりうる。
○　企業におけるセキュリティ対策も、事故をゼロにするのではなく去年より減らそうという観点でやっている。過去からの継続性がわかる指標を使って、よくなったのか悪くなったのかを定点観測する必要がある。
○　企業では、教育、システム的な備え、業務的な監査等、いろいろな取組をしている。同じ構造で一般向けに落とし込むことができれば、企業の取り組みを普遍的に使えるようになる。
○　インフルエンザが今あまり怖くないのは対処方法があるからである。ウイルスに感染したらこうなる、こういう対策をしたらよいというのをセットで啓発すればよいと思う。
○　セキュリティ対策の投資対効果を考えるセキュリティエコノミクスという考え方が出てきている。このような観点も踏まえ、現状ではこの程度まで対策するのが世間並みであるという目標を設定するのが我々の役目だと思う。
○　学校の授業に情報セキュリティの観点をもう少し入れて、子どもが学校で教わった内容をもとに家の環境をチェックするようになれば、家庭にも情報セキュリティ意識が入っていく気がする。
○　小学校の IT リテラシー教育の中で、自宅のパソコンのウイルスチェックや更新がどうなっているかをチェックさせて対策を親と話し合い、学級で報告させるようなことをすると効果があるかもしれない。

③具体的なメッセージ及びメッセージを伝える手段について
○　ターゲットや目標が広すぎると具体的な施策に落とし込めない。インターネットを利用している人のうち、たとえば個人情報の保護やウイルス感染に不安がある人にターゲットを絞って、改善の施策に結び付けてはどうか。
○　今までの話から、ターゲットは個人ユースで、少なくともセキュリティに不安を感じるくらいの意識があり、何らかの改善が見込める層としてはどうか。その改善を測定した結果が次の施策に繋がると思う。
○　カテゴリわけには単純化したモデルが必要だと思う。セキュリティに対する必要性の高低と認識の高低でマトリクスを作り、各カテゴリに仮想的な人格を想定し、どうリーチしていくかを考えてはどうか。
○　なかなかリーチできないと思える層も、シンプルなメッセージを入れていくと簡単な対策はやってくれたりする。切り捨てずにいろいろなリーチの仕方を試してみてはどうか。
○　本質的な議論はもう少し長期的に進めるとして、目の前の問題については現状が見えていない以上、やれるところからやるというのも現実的なやり方としてありうる。
○　セキュリティのポイントに関するチェックシートつきのリーフレットを企業向けと家庭向けにそれぞれ作成し、PDF を Web サイトで配布してはどうか。
○　人の心の動きとして、情報セキュリティを「使わない」「使い始める」「使い続ける」という段階があれば、「使わない」から「使い始める」の間のハードル

が高いため国として取り組んだほうがよい。みんなに興味を持ってもらう、不安に思ってもらうところを目標としてはどうか。

○　個人情報の保護やウイルス感染に不安がある人は、対策していても不安なのか、対策していなくて不安なのか、そのあたりをもう少し深掘りすることで、課題がより具体化され、啓発手法やツールも決まってくると思う。

○　このくらいはやってほしいという具体的な対策を５個くらい、1 年間から 2 年間かけて徹底的に啓発し、何人がそれを知ったか計測してはどうか。これだけでもある程度の底上げができると思う。

○　ポジティブなメッセージで啓発できないものか。セキュアな環境になることがどういういいことなのかを提示せずにネガティブなメッセージばかりいうと、知識や意識のない人は IT に見向きもしなくなってしまう。

○　セキュリティ対策をしていることがセールスポイントになるといったポジティブなメッセージは、過去にセキュリティ業界でも試みられたことがある。結局あまり響かずにネガティブなメッセージに戻ってしまったように思う。

○　マスメディアとしてテレビの威力は相当なものがある。セキュリティ芸人大賞を作ってはどうか。興味を持ってくれた人に対して真面目な受け皿がちゃんとあるような二重構造であるとよい。

○　何かテーマを決めてそれをずっと訴求するのがシンプルで分かり易い。自分のパスワードを見直す日を設けてはどうか。行動のきっかけになりうるし、メディアへの露出も期待できる。

○　パスワードを変える日を定めることについては、その日を狙ったフィッシングが現れると思われるため、慎重になる必要がある。

○　2 月の初め、米国のある会社がパスワードを変える日を設定したという Web の記事を読んだ。効果も期待できなくはないため、米国での実例等を踏まえて踏み込むという考え方もある。

○　守るべき対象が意識や知識のない人たちだとすると、メッセージを伝える手段がないことが普及啓発活動の課題ではないか。プッシュ型で強制的に情報伝達できるような仕組みをもつことも手法として考えられると思う。

○　伝達手段という意味では、学生たちがボランティアで普及啓発する仕組みを作れば大きな動きになる可能性がある。

○　デリバーする手段として、草の根的な活動で頼りにされている NPO のような組織に注意を払う必要がある。国やメーカーによるマスな活動と同時に、このような組織へのマテリアル提供等の支援が考えられる。

○　スマートフォンについては、話題にするなら来年よりも今年という気がする。ユーザーも極端に増えているし、どのターゲットにも関わるテーマである。

（2）今後のスケジュールについて

事務局より資料３に沿って説明。

－ 以 上 －