資料２

NISC National Information Security Center

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）

普及啓発の基本的な考え方

１　現状の把握・目標の設定

○　現象面（人の行動）は現在どのようになっており、それをどう変えていくのか

２　問題の抽出

○　問題→①顕在化している障害、②目標達成のためのハードル

３　課題の抽出、ターゲットと具体的目標の設定

○　課題→①普及啓発により解決すべき解決可能な問題、②複数の問題の背後にある根本的な要因

○　ターゲット→課題解決のためにコミュニケーションをとる相手はどのような者が適切か

○　具体的目標→選定課題について具体的にどのように状況に変えていくか

４　課題解決方策の検討

○　課題の原因となっているパーセプション（認識）とそれに基づく行動をいかに変えるか

○　ターゲットのパーセプションを変えるためには何を伝えればよいか。

○　そのためには、どのような手法が適切か

○　その方策で、本当に目標が達成できるのか。

具体例　～　飲酒運転撲滅キャンペーン　～

１　現状の把握・目標の設定

○　現状：飲酒運転あり→目標：飲酒運転なし

２　問題の抽出

○　問題→ばれないと思っている、他に交通手段がない、大した距離じゃない、酒に強いタイプだと思っている、一杯だけだから大丈夫と思っている　等々

３　課題の抽出、ターゲットと具体的目標の設定

○　課題→「一杯だけだから大丈夫と思っている」：これが根本にある意識
○　ターゲット→酒を飲むことがある運転者
○　具体的目標→「一杯だけだから大丈夫」という意識を改善し、たとえ大丈夫だと思っていても少しでも酒を飲んだら絶対に運転しないようにする

４　課題解決方策の検討

○　「一杯だけだから大丈夫」という意識とそれに基づく行動をいかに変えるか→「一杯だけでもそれは絶対運転に影響を与えている」という意識へと変えていく
○　そのために、「アルコールが抜けるには最低４時間は必要」、「少量飲酒での運転の怖さ」を伝えていく
○　伝える方法として、医者や専門家の声により、運転者との接点（ラジオ、車雑誌等）で伝達する

情報セキュリティについて①

1　現状の把握・目標の設定

○　現状：ITを活用するに当たり情報セキュリティが不安と考えている個人は全体の82.6%、企業は77.5%と多い。一方、何らかの情報セキュリティ対策をしている個人は全体の80.2%、企業は96.4%と多い。

○　目標：必要な対策を徹底し不安を感じる人をなくす

※　上記の数字は「ユビキタスネット社会における安心・安全なICT利用に関する調査」（平成21年）の結果から抽出

2　問題の抽出

○　問題～不安を感じている要因は？～

→個人情報の保護に不安がある（71.6%）、ウィルスの感染が心配（69.6%）、どこまでセキュリティ対策を行えばよいか不明（61.9%）、セキュリティ脅威が難解で具体的に理解できない（38.4%）、違法・有害情報が氾濫している（29.3%）　等々

※　上記の数字は「平成22年度通信利用動向調査」の結果から抽出

情報セキュリティについて②

3　課題の抽出、ターゲットと具体的目標の設定

○　課題→「どこまでセキュリティ対策を行えばよいか不明」という根本的な問題、どこまでやればよいか分からなければ対策は行わない、自発的には行わない、ウィルスに感染してから考えようと思ってしまう、対策が行わないから不安になる。

○　ターゲット→パソコン、インターネット等を利用している人

○　具体的目標→「どこまでセキュリティ対策を行えばよいか不明」である状態を改善し、自らきちんとあらかじめ必要な情報セキュリティ対策を講じることで、不安感を感じずITを利用できるようにする

4　課題解決方策の検討

○　どこまでセキュリティ対策を行えばよいか分からないという意識とそれに基づく行動をいかに変えるか→「どこまでやればよいのか自発的に情報を得ようとする」という意識に変えていく。

○　そのためには、情報セキュリティ対策を怠った場合どのような影響が生じるか、必要な情報セキュリティ対策とは具体的に何か、ということを、対象の属性に応じ内容を変えながら伝えていく。

○　方法として、ウェブサイト、SNS、パソコン関連の講座、講演等の場を通じて伝達する。

4　課題解決方策の検討　～　各論　～

○　そのためには、情報セキュリティ対策を怠った場合どのような影響が生じるか、必要な情報セキュリティ対策とは具体的に何か、ということを、対象の属性に応じ内容を変えながら伝えていく。

～　具体的なメッセージは何か　～

①　「対策を怠った場合どのような影響が生じるか」→そもそもセキュリティ対策の必要性を理解していない人に、対策の必要性を伝える

（例）ウィルス感染やID・パスワードの盗取により、重要情報や金銭が知らず知らずの間に奪われるおそれ

（例）他人のウィルス感染に知らず知らずの間に加担してしまうおそれ

・　具体的にどこまで影響を深掘りするか、何に重点を置くかは、対象ごとに異なる。

（例）企業：情報流出→信用失墜→金銭被害

（例）生徒・児童：情報流出→周囲の噂に→学校に居づらくなる

4　課題解決方策の検討　～　各論　～

② 「必要な情報セキュリティ対策」→セキュリティ対策の必要性は理解していても具体的に何をやればよいかわからない人に対策を伝える

・　必要な対策は、機器やトラブルといった切り口ごとに様々。
（例）パソコン：「情報セキュリティ３原則」、スマホ：３原則＋アプリケーションの入手に注意
（例）フィッシング・標的型攻撃→３原則のうち、不審なメール等にアクセスしないということの詳細な内容（これらの特徴にフォーカス）
→　最低限の対策（３原則）を基にすべきか。

・　具体的に何に重点を置き伝えるかは、対象ごとに異なる。
（例）企業：標的型攻撃
（例）高齢者、児童・生徒、家庭（個人）：フィッシング

※「情報セキュリティ３原則」
・個人情報等の重要な情報の扱いは慎重に
・パソコン等は常に最新のセキュリティ状態に
・不審なサイトやメールにアクセスしない

4　課題解決方策の検討　～　各論　～

○　手段として、ウェブサイト、SNS、パソコン関連の講座、講演等のパソコン等との関係がある場を通じて伝達する。

～　メッセージを伝える具体的方法、その考え方は　～

①　メインターゲットの年齢、性別、所属は様々→これらに共通する方法＋属性ごとに特有の方法か。

- 共通する方法→ターゲットはパソコン、スマホ等の機器を使う人→その機器を使う人なら通るところで伝達する
  （例）検索サイト、ポータルサイトからの誘導
- 属性ごとに特有の方法→ターゲットの属するコミュニティの活用
  （例）企業→経済関連団体の会合、講演会、経済雑誌
  （例）児童・生徒→学校、携帯サイト
  （例）高齢者→各種講習会、パソコン教室、新聞