資料８

基本計画検討委員会
ホームページにおける意見募集の結果について

○　募集期間
　　平成 20 年１月 18 日（金）　～　２月 15 日（金）
○　意見提出総数
　　５件（いずれも個人）（※）
　　詳細は次頁以降のとおり（到着順に掲載。）。

いただきました御意見につきましては、基本計画検討委員会の各委員に配布し、同委員会における検討の参考とさせていただきます。

（※）　募集時における「意見の提出方法」によらなかったものを除く。

平成20年２月21日

内閣官房情報セキュリティセンター

【１通目】

日本国内に於いて、現在は潜伏している情報サービスの危険性について。

固有のＩＤ、パスワードによって閲覧可能な招待制サイト。
最近はソーシャルネット・ワーキング・サービス（ＳＮＳ）などに登録し、
年々利用者が増えております。以前ではＰＣ端末でしか見れなかったｗｅｂページが
携帯電話の機能が向上した結果、それと変わらぬサービスを実現していると思われます。

（利用者が意図せず若しくは認識できない違法行為が第三者によって行われる可能性）

また、携帯電話に於いては本来の電話として必要とされる機能以外、
非常に多くの機能が付加されているのが主流になっています。
例えば撮影、録画（録音を含む）その他にも位置情報（ＧＰＳ）が挙げられます。

今や携帯電話の方がＰＣ利用者より多く、所有者層の年代も幅広いものと思われますが
ネットワークを利用できる高度な移動端末として見るならば、近頃のＷｅｂで発生する
脅威に対しても、ＰＣ以上に晒されているのが現状だと考えられます。
（携帯電話機に対する不正行為の懸念が高まっています）

実際、被害にあった場合の摘発の困難さや法律上での責任追及が難しいことも含めて
不正なプログラムと知ってのマルウエアの開発者、更に第三者的に悪用する者など
社会基盤を破壊する恐れのある事から、取り締まり強化がされる方向に進めて欲しいです。
（現行法の限界。そこから違法行為に対して認識が少ない現状）

【２通目】

「省庁の枠に縛られない、インフラ作りと体制、有機的な実行、予算と執行」
国民の安全は、「連続したセキュリティの確保」で守られるものだと考えます。

例えば　一人の小学生が朝起きてから夜寝るまでの間の生活を考えると
様々な危険に晒されています。　登下校、学校、　塾、　病院通いなど、
動きを追跡する（RFID付きランドセルを想定、電柱などにRFIDリーダーを敷設、
児童の行動を追跡できる、プライバシーの問題はあると思いますが）
するときにいくつかの省庁が監督する構造物や施設を通過しますが、
このような状況ではデータの保管をどうするか、施設の管理主体はどうするかなど
一省庁では、かばいきれない問題が多々あると考えます。

セキュリティはこれらのバウンダリーを超えて確保されるべきものだと思っており
インフラや、体制、実行は細切れではやっていけません。

一国民の生活の視点から見た情報セキュリティ政策　の観点で
ご検討いただけますよう、　お願いいたします。

【３通目】

【１】意見内容

情報セキュリティに関する情報の産業界や一般国民への殊更
正しい情報の提供・啓蒙を求めます。既に正しくない情報が
国民の間に流布されている場合は、すみやかに是正する情報
発信や啓蒙活動が求められると思料いたします。

一例を挙げれば、『暗証番号だけで機密を守る携帯電話と生体
認証装置搭載の携帯電話ではどちらがセキュリティの観点から
優れていますか？』と質問すると、１００人中９５人の市中の国民
が生体認証搭載の携帯電話の方が優れていると答える現況は
由々しきことです。正解は、暗証番号だけで機密を守る携帯電話
の方が優れています。
生体認証の弱点の一つは、ケガや体調不良などで本人なのに
拒否されるケースが避けられないことです。特にモバイル環境で
の使用が前提の生体認証搭載機器は殆ど全て「救済用パスワード
併用生体認証」の仕様になっています。すなわち、表玄関は生体
の照合で裏口はパスワード照合で鍵が開く仕様なのです。
しかし、生体認証装置搭載機器のパンフレットには、生体認証の
利便性とセキュリティが向上することを謳った内容が盛られ、多く
の国民は、公正取引委員会用語である”優良誤認（適正とは
いえない広告や表示によって、製品あるいはサービスが実際より
も著しく優良であると誤認すること）”に陥ってしまっています。

このような優良誤認状況は、ワンタイムパスワードでもしかりで、
ワンタイムパスワードは、パスワードの上位に位置づけられる本人
認証技術であるという誤った理解をしている国民が大多数と捉え
ています。
あくまでもワンタイムパスワードは、表示したデバイスが本物であ
ると証明するだけで、いま誰の手中にあるかは語ることはありませ
ん。
その他、暗号化製品の安全性評価、生体認証製品の照合精度
の評価、遠隔操作によるモバイル機器のデータを消去・無効化する
機能の安全性評価などでも優良誤認がまかり通っており、改めて
正確な情報発信・啓蒙が求められます。

【２】理由

国民の生命財産の保護に直結する情報セキュリティ関する情報は、医療薬品に関する情報と同等レベルの正鵠な情報が求められます。さらには優良誤認のまま外交防衛の国家機密情報の対策を講じることになれば由々しき国家安全保障の問題にもなりかねません。

また、安全安心なデジタル社会・ネットワーク社会の発展と維持のためには、情報セキュリティ技術の利用者である国民の信頼を得ることが不可欠です。

実際はセキュリティ効果が見込めないセキュリティ技術やセキュリティソリューションが優良誤認表示や不適切な表示によって普及してしまうと、利用者である国民のセキュリティ技術全般への信頼が失われ、政府が推進しているユビキタス社会が広く国民に受け入れられなくなる可能性がありえます。さらに国内だけでなく国際社会においても経済活動を中心とした諸活動への障壁となりかねないことも危惧されます。

上記につきご賢察いただき優良誤認情報に対し是正情報の発信及び啓蒙活動推進を、貴センターの情報セキュリティ政策に求めるものです。

【追伸】添付は、日本セキュリティマネジメント学会にて昨年６月の全国大会にて発表された研究論文『本人を認証する製品の優良誤認を防ぐための提言』の写しです。

参考文献として添付させていただきました。

【4通目】

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

【意見内容】＜２２頁～２３頁 人材育成について ＞

４項、５項に関連して、情報セキュリティ管理に責任を負うスタッフ部門では、業務経験者を確保し、情報セキュリティ管理と実業務とのバランス感覚を重視すべきと考える。

【理由】

各社様の情報セキュリティ管理を見させていただく機会があるが、うまくいっている企業は、情報セキュリティはトップダウンといいつつも、現場・業務に負荷をかけない配慮をしている。

うまくいっていない企業は、現場・業務への配慮が欠け、反発をくらい、実質的に現場・業務部門のサポタージュ・取組みの形骸化を招いていると推察。

情報セキュリティの技術云々も重要であるが、現場・業務部門のリスクベースのコミニケーションを進め、納得性を高く人を動かせる、業務経験がある人材が不可欠である。

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

【意見内容】＜１６頁～１７頁 IT提供企業の情報セキュリティ確保の役割について ＞

９項に関連し、「組み込まれない組込ソフト」については、「自身がパッチをダウンロードして適用すること」のハードルに比して、情報セキュリティ管理の確保に関して有効と考える。

ただし、自動適用される仕組みの場合には、なんらかの第三者機関による牽制が必要と考える。
（パッチの中身の検証に限界はあると思いますが）

【理由】

一般の方は、未だセキュリティパッチや脆弱性にルーズな状態と推察。

個人的にネットに繋がっていれば、自動的にファームアップしてくれるDVDデッキを保有しているが手間がかからない。

救える前提条件が多い（インターネットと接続できること等）が多いが

顧客の同意を得る手段があれば、取組み自体は有効である。

マスを相手にしている商品が大多数なので、これらの取組みの
トラブルは顕在化しやすく、企業の信用問題にも発展しかねないため、
企業努力はあてにしてよい、と考える。

ただ一企業の問題におさまらない可能性もあり、第三者機関の
関与・牽制は必要と思われる。

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

【意見内容】　＜１４頁～１５頁 中小企業の情報セキュリティについて ＞
６項の保険に関して、従前より保険と情報セキュリティを交える
商品は出ており、積極活用を促すことはできると考える。

【理由】
一般化しないのは、アセスメント結果をリスク点数に転換すること、
アセスメントできる人材の確保がネックとなっていると考える。

保険業界として、当分野の統計が取られていない（点数の裏づけとなる
記録がない）ことも活性化していない事情とも思われる。

自己申告によるアセスメントで、申告者の個別ごとに申告内容
（情報セキュリティ管理の充足度）が、「ぶれる」懸念も
あるためぶれない質問形式にしていけば自己申告による保険加入も
可能ではないか。
（悪意については、不正申告で処理できる）

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

【意見内容】　＜１２頁～１３頁＞
２項に関連して、個別の情報資産に対する法制化は、「何を守るか」
の対象・目的が明確であり有効と考える。

一つの業務に関して、目的別に複数の法令、ガイドラインが適用
され担当者の負荷増加がデメリットであるが、企業組織として
「やるべきこと」であり、上記のメリットのほうがはるかに
大きい

そのため＜２６頁＞１項の「情報セキュリティ基本法」に関しては、
不要という意見である。

【理由】

法制化されてるものは、各企業も動きが早い傾向にあるが
抽象的な基本法は混乱を招きやすいと推察。

問題は、複数の法令・ガイドラインを網羅して対応できる組織・人材
を確保し、目的別の法令を解釈し業務に組み込む部分である。

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

【意見内容】　＜１２頁～１３頁＞

７項に関連して、情報セキュリティの確保　＝　自分を不正の疑いから守る
というメッセージを強く打ち出す必要があると考える。

【理由】

現在のところ従業員は、情報セキュリティは他の人が考えること、
という傾向が強いと推察。（もしくは押し付けられている）

ただし、情報セキュリティの確保によって、より働きやすい環境に
変わる（手続きの明確化による責任の可視化、ログ等の取得による
不正をしていないことの証明が容易等）ことがきっちり伝わって
いないように思われる。

近年の内部統制の取組みにより、変革が求められるが、
「業務上仕方がなく」ではなく「自分を守るため」という点の
訴求も必要。

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

【意見内容】　＜１０項～１１項　＞

情報セキュリティの中で事業継続に取り組むのは、混乱する懸念がある。

情報セキュリティ管理と事業継続管理は、共通業務基盤として、
並ぶものとして明確にしたほうが望ましいと考える。
（どっちが先かというわけでなく、業務を考えるにあたっての
検討領域の一部として、情報セキュリティと業務継続管理が
あるイメージ）

【理由】

事業継続のための情報セキュリティという用法に違和感があります。

事業継続のための「手段」が明確になった段階で、その手段の中で
情報セキュリティの検討が開始される、という理解です。

例）業務継続用のバックアップサイトを借りる
⇒　通常の執務室と同レベルのファシリティのセキュリティ確保
⇒　再開用の業務マニュアルは、施錠された場所に保管
⇒　データリカバリー用データの暗号化して運搬
⇒　暗号鍵管理の運用
⇒　バックアップ回線のセキュリティ確保
等

情報セキュリティポリシーには、上記の手段に対する情報セキュリティ対策の手当ては、網羅されている前提。

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

【意見内容】　＜６頁＞

５項に関連して、ベースラインの過度な設定と安全策をとった拡大解釈が「対策疲れ」の原因と考える。

日本企業は、ベースラインが提示されることを前提に待ちになる姿勢が強いと推察。
これは、リスクマネジメントができる人材・組織が熟成されていないため何らかの基準に依拠したい表れと推察。

業務に即した情報セキュリティ対策を企業単独でリスク判断できる風土・文化作りが重要。

【理由】

ベースラインはミニマム要件として、各企業でリスクに応じた対策（利害関係者、第三者に説明責任が果たせる論拠）を上乗せするやり方が時流にあっていると思われる。

ただし、業界標準によるベースラインは目的が明確であり有効と考える。

また、リスクベースの考え方ができる人材育成が必要。
（例:内部統制の監査で、監査人と意見が戦えるイメージ）

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

【5通目】

①情報セキュリティ問題をめぐる現状と課題

情報セキュリティにおいては防御の対象の広がりと共に専門家による研究・対処が進む一方で、一般市民に置ける危機意識や対処方法に関する知識・技能の広がりが思ったより進まず、ある意味両者の乖離が顕著になっているように思われます。

その為、政府機関や企業の情報システムに対してのセキュリティ対策が徐々に進み、一般利用者に対するサービスとしてのセキュリティ対策(例えば携帯電話でのフィルタリングサービスなど)も広く提供される様になっているが、肝心の利用者である一般市民においては、そのものの意味合いや影響範囲などを理解する事無く活用される事により、セキュリティ問題の本質的な防御体制を構築するまでに至っていないと思います。

②現在の政府の政策（NISCと各省庁）及び今後の政策への要望

政府に置いては生命・財産のインフラ基盤に対する全体統括の立場でのセキュリティ対策を司る一方で、各都道府県を情報セキュリティ拠点として捉えて、そこを各々の独立したセンターとして位置付け、自立的にセキュリティ対策を推進していく上での対策立案・人材教育および啓蒙・全国・世界をまたがる情報共有基盤の提供元として活動する場として立ち上げる事が必要と思われます。

なお、情報セキュリティ拠点たる各都道府県においては、各小学校区などの地域のまとまりの単位でサブ拠点を設け、そこに複数名の専任者を配置し、地域住民の教育・啓蒙活動などの活動を進める様にする事、各サブ拠点の専任者間の情報共有を図る事、各知事・市長などの行政トップないしは直属の専任者がCIOとしてこれらのサブ拠点の専任者を統括する体制を整えることが必要ではないかと考えます。

③政府以外の主体に求めたいこと

一般市民に対しては上記体制が整った際に積極的に地区の活動に参画する事が望まれます。一方でNGO法人や大学・専門学校と言った教育機関、IT企業にはサブ拠点の専任者に対してボランティア的な各種支援を積極的に行なう必要があると考えます。それに当たっては組織としてボランティアを行なう人員へのインセンティブの提供の必要性も考慮して頂く必要があると考えます。

人体と同じように各一般市民を細胞一つ一つと捕らえ、細胞->組織->臓器->人体といった網目状・階層的に組織化した上で、各個人の教育・啓蒙を図れる体制が望まれると考えます。

【参考】

「第２次情報セキュリティ基本計画」（仮称）の策定に向けた、情報セキュリティ政策に関する意見の募集について

平成 20 年１月 18 日
内閣官房情報セキュリティセンター(NISC)

「情報セキュリティ政策会議」（議長：内閣官房長官）及び内閣官房情報セキュリティセンターでは、情報セキュリティ問題を俯瞰した我が国の中長期的な戦略である「第１次情報セキュリティ基本計画」（平成 18 年２月２日情報セキュリティ政策会議決定、以下、「第１次計画」という。）に基づき、情報セキュリティ政策を進めてまいりました。この第１次計画は、平成 20 年度で年限を迎えることになりますが、依然として情報セキュリティに関する問題が発生していることから、平成 21 年度以降を計画年度とする新たな中長期的な戦略の策定を考えております。

そこで、情報セキュリティ政策会議の下に基本計画検討委員会を設置し、計画の策定に必要な情報セキュリティ政策の在り方及び方向性に係る事項について調査検討を行うこととしましたが、同委員会における検討の参考とするため、下記の要領で国民の皆様から広く意見を募集いたします。

１．意見募集の内容

現在推進している情報セキュリティ政策全般、具体的には、

- 情報セキュリティ問題をめぐる現状と課題
- 現在の政府の政策（NISC と各省庁）及び今後の政策への要望
- 政府以外の主体に求めたいこと
- その他（自由記載）

がございましたら、後掲の要領に従い、意見の提出をお願いいたします。

なお、本件に関連して、第１回基本計画検討委員会で使用いたしました

- 「第２次情報セキュリティ基本計画」（仮称）に係る検討の視点（例） PDF

等の資料がございますので、適宜御参照ください。

また、以上は中長期計画である「第１次情報セキュリティ基本計画」 PDF 及び年度計画である「セキュア・ジャパン 2007」 PDF の内容と密接に関連するものですので、これらの計画の内容についても適宜御参照ください。

２．意見の提出方法

(1) 意見は、所属、氏名、住所（法人又は団体の場合は、名称、代表者の氏名、主たる事務所の所在地）及び連絡先（電話番号又はメールアドレス）を明記の上、日本語により作成願います。

(2) 意見は、電子メール、FAX 又は郵送の方法で御提出願います。
（電話による意見の受付けは致しかねますので、御了承下さい。）

《電子メールの場合》
送付先メールアドレス： i.nisc_keikaku@cas.go.jp
内閣官房情報セキュリティセンター（基本戦略担当）あて
※ 件名には、必ず、「情報セキュリティ政策への意見」と御記入ください。
また、添付ファイルの提出は受け付け致しかねますので、必ず電子メール本文に意見をテキスト形式で御記入下さい。

《ＦＡＸの場合》
送付先 FAX 番号: 03-3581-7652
内閣官房情報セキュリティセンター（基本戦略担当）あて
※ 様式については別添を御参照下さい。

《郵送の場合》
送付先住所：〒100-0014 東京都千代田区永田町 2-4-12
内閣官房情報セキュリティセンター（基本戦略担当）あて
※ 封書に朱書きで「情報セキュリティ政策への意見」と御記入願います。
また、様式については別添を御参照下さい。

(3) 提出期限は、平成 20 年（2008 年）２月 15 日（金）18:00（郵送の場合は同日必着）とします。

(4) 意見提出上の留意点
お寄せいただいた御意見については、委員会における検討の参考といたしますが、**個々の意見に対する回答はいたしかねますので、あらかじめ、その旨御了承願います。**
なお、結果の公表にあたり、意見を提出された方の氏名（法人等にあってはその名称）やその他属性に関する情報は公表する場合があります。

NISC プライバシーポリシー

＜連絡先＞： 内閣官房情報セキュリティセンター
（担当：寺本・山川・矢作）
住所：〒100-0014 東京都千代田区永田町 2-4-12
電話：（直通）03-3581-3768

別添

「「第２次情報セキュリティ基本計画」（仮称）の策定に向けた、情報セキュリティ政策に関する意見の募集について」意見提出フォーマット（例）

内閣官房情報セキュリティセンター（基本戦略担当）あて

H　　.　　.

所　属		(ふりがな) 氏　名（※）	
(ふりがな) 住　所（※）			
連絡先	（ふ り が な） 連絡担当者氏名： 電話： FAX： e-mail：		

※ 法人又は団体の場合は、名称、代表者の氏名及び主たる事務所の所在地を御記入ください。

（注）上記の住所・連絡先は手続き上必要な連絡のためにのみ使用します。

意見内容	
理　　由	