資料３－４

「次期情報セキュリティ基本計画に向けた第一次提言への意見募集の結果について

１　実施期間
平成２０年６月１９日～平成２０年７月１８日

２　応募意見提出者数
総数１０件（内訳：個人４件・団体６件）

３　意見提出者一覧（五十音順・敬称略）

※　個人での意見表明と明記された方、個人名のみを記載された方を、個人として計上させていただいております。

１　意見提出者

NPO 日本ネットワークセキュリティ協会　西日本支部

２　提出意見

（１）意見内容

ベンダー側を巻き込んで、優秀なものづくり技術を備えているにも拘わらず、情報セキュリティ確保を前提とした生産性の向上のための積極的なIT投資を行う事が出来ない中小・零細企業自身が安価かつ容易にICTを利活用する為の共通基盤づくりと情報セキュリティ対策を具体的に推進するための組織づくりが必要。

（２）理由

ITの利用・活用が遅れている情報セキュリティレベルの低い企業が大企業とのサプライチェーンから外されていく傾向は、優秀な技術を持ち、産業の要となっている中小・零細企業が数多く存在する関西一円、とりわけ、昔から「ものづくり」拠点としての存在を全国に示している大阪府にも顕著に現れてきている。

ICTを活用した生産性向上や営業力の強化のための十分なコストと量的・質的な人材が確保できないため、情報セキュリティ対策製品やICTを利活用するための製品、それらの関連サービスの導入について、その必要性や優先順位、自社への適合性、支払うコストの妥当性などの判断を十分に行なう事が出来無い事によるものである。

また、情報セキュリティ対策については“ここまでで十分”とする基準となる情報セキュリティ対策が決められないことから、利益・企業価値の最大化を目的とする大手企業とは異なり、企業継続を第一義とする中小企業経営者にとっては、経営圧迫の要因と判断する傾向が多く見られ、このままの状況では、独自の技術力・製品を持つ競争力のある中小企業であっても、情報セキュリティレベルが低いがために、ビジネス機会を減少させていくことは避けられず、ICTの利活用による業績向上が思う様に進まない現実と相俟って、企業体力に勝る大企業との格差はますます拡大、大企業に互してビジネスを行うことが難しくなり、相対的なポジションの低下に繋がっていく危険性は高いと憂慮される。

加えて、社会的に大きな被害を発生させることの無い様に、情報セキュリティ対策

の必要性自体が理解できないまたは自ら対策が実施できない個人、いわゆるIT弱者に対する救済措置が必要とされる。特に、セキュリティ情報・知識が個人のスキルに依存するIT弱者については、サポートされる側の知識のバラツキが大きく、手厚い救済措置を考慮する必要がある。

しかし、このような課題に対して中小・零細企業や個人が各社個別で取り組むということは、ヒト、モノ、カネ、情報の各側面の制約・限界からみて極めて難しい現実にある。

またセキュリティベンダーやSierの組織や団体はいくつも存在するが、あくまで供給者側の理論でビジネスとしての成立が前提であり、そもそもビジネスとして成立しにくい中小・零細企業が抱える先の課題に対して、有効な支援策を期待することは難しい。

このため、中小・零細企業が、ICT利活用課題と情報セキュリティ問題を解決するため、利用者自身がICT利活用と情報セキュリティ対策問題を議論し、具体的な解決策を探るための場が必要となるが利用者視点に立っての組織は残念ながら存在していないのが現状である。

１　意見提出者

NPO 日本ネットワークセキュリティ協会　パブコメ検討 WG

２　提出意見

第1章（2)への意見

・第１次情報セキュリティ基本計画における成果など、計画通りに進んだ項目などを詳細に伝えてほしい

理由：情報セキュリティに関する「継続」と「発展」についてより理解を深めるため

第1章（2)への意見

・情報セキュリティの範囲が広がるにつれ「事故前提社会」の意味も曖昧になりつつあるように思う。もう一度言葉の持つ意味を徹底する意味でも、脚注ではなく本文内で解説してほしい。

理由：事故前提社会という言葉は長く使われているが、言葉だけが独り歩きしているのではないかと思われるため

第1章（2)への意見

・「合理性」のなかで効果的・効率的に実施するとあるが、効果や効率を明確にするための指針を示してほしい

理由：情報セキュリティに十分なコストがかけられない企業ではその効果を明確にする事が難しいと思われるため

第2章（2)への意見

・米国におけるNISTのような海外組織との連携を密に取り、日本の政策を国際標準に反映できる団体を作ってほしい。

理由：国内の標準をいくら作ったとしても、結果的には海外の標準を利用する事が多く、国内の情報セキュリティ文化の発展に寄与しないため

第2章（2)への意見

・高品質・高信頼性・安心安全なジャパン・モデルを”世界と協調”させるにあたり、海外から見ても分かる（評価される）ような、より具体的で明確な判断基準を提示してほしい。

理由：国内で作られた技術や基準が海外で利用されたり、標準に適用されるようになることが「情報セキュリティ立国」の礎となると考えるため

第2章（2)への意見

・情報セキュリティに関して、我が国の技術は高い。しかし、日本発の基準（国際標準）は無い。標準化を進める組織を作ってほしい。

理由：国内で作られた技術や基準が海外で利用されたり、標準に適用されるようになる事が「情報セキュリティ立国」の礎となると考えるため

第3章（1)への意見

・事故前提社会だとはいえ、最低限守るべき情報セキュリティ基準を明示してほしい

理由：ガイドラインだけではなく、ベースラインを提示する事で全体的な水準を向上させてほしいから

最適な「水準」”は業界や企業により異なるし、常に変動するため″

第3章（1)への意見

・「事故前提社会」を実現するには、この位の事故でこの位の損害金額になったかなどの具体的な情報が必要になり、この情報収集、分析を行う場を設けてほしい

理由：行政だけではなく、民間における判断基準を明確にするため

第3章（2)への意見

・情報セキュリティの人材育成を発展させるためには、(韓国のように）国策として、国内の情報セキュリティ産業を発展させる、裾野を広げるような政策を取ってほしい。

理由：人材の必要性を明確にするような政策がないと思われるため。例えば、技術者やコンサルタントなど分野ごとの要求事項をなどを明確にしてほしい

第3章（2)への意見

・情報セキュリティに関する認証基準の整合性を図ってほしい

理由：プライバシーマークやISMS認証などのマネジメントにおいて、同様の要求事項にも関わらず、異なる対策を求められる場合があるため

第3章（3)への意見

・PDCAサイクルの「C」が明確になるような報告書を作成してほしい

理由：民間がそれを手本とし、活用するため

第4章（1)への意見

・情報セキュリティ事故が発生した場合など、個人が相談する窓口を一元的に、明確にしてほしい

理由：現状は、事故の報告をしたいと思っても、内容によって個人が問い合わせ先を判断する必要があり、事故の状況や実際の発生数を判断する事が難しいと思われるため

第4章（3)への意見

・「2つのアプローチ」が何をさしているのか明確ではないので、わかりやすく記載してほしい

理由：これを捉え間違えると、本政策の本旨が理解できないため

第6章（1)への意見

・統一的な視点および監査結果を必要に応じて公開してほしい

理由：民間がそれを手本とし、活用するため

１　意見提出者

（社）日本経済団体連合会情報通信委員会情報化部会 IT ガバナンス WG

２　提出意見

（１）地方自治体での情報セキュリティ確保の一層の推進（全般）

地方自治体は中央官庁に比べ、企業・個人にとって接点が広く、深い。国は地方自治体の自主性・自立性を十分配慮する必要があるとは言え、地方自治体における情報セキュリティの重要性を鑑みれば、以下の点を本基本計画に盛り込むことを検討するとともに、地方自治体間の手続きの違いや対応レベルの差をなくすよう業務プロセスの共通化を図るべきである。

・地方自治体における情報セキュリティ監査の実施と結果公表の奨励

・本基本計画の中間報告及び結果報告における、地方自治体での取組み状況報告の実施

（２）NISCの機能強化及び法制度の整備（P.28）

NISCが府省庁横断的に実効性のある情報セキュリティ対策を徹底するためには、電子行政推進法案（仮称）が次期通常国会に提出される予定であることも踏まえ、米FISMAと同様の法制度を整備するなど、NISCの機能強化に向けた具体的方策を本基本計画に盛り込むべきである。

（３）ISMS取得、情報セキュリティ監査の推進支援（P.31）

①　民間、公的機関を問わず、ISMS認証取得に向けた取組みは、情報セキュリティ推進に必須であるトップの認識を高める効果がある。したがって、認証取得を推奨・支援する活動が情報セキュリティ向上に繋がるという視点を、本基本計画に盛り込むべきである。

②　ISMS認証取得数では日本が世界一であることを踏まえ、国際貢献の一つとして日本の経験から指摘できる改善・改良項目を積極的にISO規格へ発信・反映するべきである。

例：ISO27001付属書A11.7項における「モバイルコンピューティング」項と「テレ

ワーキング」項の統合・改定。A12.3「暗号の利用」項の見直し。

③　自主的な内部監査であれ第三者による外部監査であれ、監査の実施は、PDCAを回すうえで必須のプロセスであり、情報セキュリティの維持・強化に有効である。したがって、企業や地方自治体の自主性・自立性を十分考慮したうえで、監査実施の普及拡大を推進する施策について検討するべきである。

（４）情報セキュリティ対策における定量的な評価基準の設定（P.33）

政府、地方自治体、企業を問わず、情報セキュリティにおけるPDCAを着実に回すためには定量的な評価基準が不可欠である。また、地方自治体や企業における情報セキュリティ対策は自主的に行われるべきであるが、恒常的に対策に取組んでいる地方自治体や企業が市場で適正に評価されるには、やはり定量的な評価基準が必要であり、その設定に向けた検討を行うべきである。

（５）安全な公文書管理に向けた取組み推進と民間適用への支援（新規）

電子行政の推進が急ピッチで進んでいることを鑑み、電子文書を含む公文書の安全な管理に向けた技術開発・標準化と、それを反映した法制度やガイドラインの整備が必要。また、その成果を民間にも開放し、私文書管理にも適用できるようにするべきである。

（６）FMC（Fixed Mobile Convergence：固定通信と移動通信の統合）等を前提とした対処の検討（新規）

2010～2011年にはアナログ地上波放送廃止後の周波数活用としての高速公共無線LANサービスや、家の固定電話と携帯電話の番号統一サービスが始まる計画があり、構内と構外、有線と無線等の区別の無い利用がビジネスでも個人でも進むと思われる。これまでのサービスのみを前提とした対応では対処しきれない課題が生じる可能性も視野に入れた検討を行い、必要に応じて本基本計画に課題を盛り込む必要がある。

１　意見提出者

弁護士／IT 法律事務所

２　提出意見

上記第1次提言は、「事故前提社会」への対応力強化と合理性に裏付けられたアプローチの実現を手段として「安心して利用可能な環境れの構築をするものとして構築されている。

しかしながら、現実の情報セキュリティの現場を考えるかぎり、このようなアプローチは、現代の情報セキュリティ状況に対する認識が不十分ではないかという懸念がある。

むしろ、もはやセキュリティの最大の問題は、犯罪組織によるボットネットなどの利用などによる攻撃の組織化・被害の多角化が最大の問題となってきているのであり、そのような脅威を正面から認識し、それに対してどのような準備をしなければならないかという認識をしなければならないものと考えられる。

かかる問題意識と共通のものとして「次世代の情報セキュリティ政策に関する研究会」の最終報告書がある。

http://www.soumu.go.jp/s-news/2008/080703_5.html

http://www.soumu.go.jp/s-news/2008/pdf/080703_5_bt1.pdf

ボット等の攻撃は、

(1) 国際性(越境性)- 法執行機関の協力の困難さ

(2) 匿名性(Anonymity-traceability) - 行為者に対する追跡のためのコストを隠れ蓑にしているのであり、むしろ、かかる観点に正面からきりこむことが、次期情報セキュリティの最大の課題と認識すべきである。

むしろ、 次期情報セキュリティの最大の課題は、 対応(reactive response)から防御(proactive defense)へとのセキュリティのパラダイムシフトである。

古典的な近代刑法の限界を見据えて組織犯罪対策をも念頭にいれた現代刑法の対応から示唆をいれるとき、 実体法面からの準備と事後対応の困難性対策の二つの側面が重要になる。

特に事後的な対応では､被害防止が困難であることを正面から見据えるべきとなる。この観点から､「 事前の情報入手」「攻撃側の通信解析手法の適法性化」「犯行途上の証拠収 集と防御」を論点としていれるべきである。

このためにポイントとなるのが事前防衛の概念であり、そのために

(1)通信主権の「再発見」(国際電気通信連合憲章 34条2項等)

と

(2)ISPとレジストラー　の防衛の枠組みの承認

が必要となるのである。

これらの論点の要素は、上記「次世代の情報セキュリティ政策に関する研究会」の最終報告書にも若干でているが、2008年における情報セキュリティの考え方を考えるときに、現在の「事故前提社会」への対応力強化という視点は、あまりにも現実のセキュリティの問題と乖離しているものと考えられ、基本的なフレームワークに対する再考をもとめたいと考える次第である。

１　意見提出者

北陸無線データ通信協議会

２　提出意見

(項目1)

全体の意見

目次・見出しが「中央揃え」もしくは極端に右にずれている。見出しの先頭に空白があり自動処理されて右にずれて表示されているように見える。ここは「左揃え」もしくは目次・見出しの空白を削除して自動処理にすればよいのではないのか。修正を望む。

(項目2)P.4

第一次基本計画に基づく取組は、おおむね当初の計画通りに実現できていると考えられる。

意見：無線LANセキュリティ問題については、事件の表面化が2008年夏より漸く始まったばかりである。総務省各総合通信局・警察との連携も十分とは言えず数多くの警告が無視され続け2004年と比較し危険な無線LANは少なくとも2倍にもなっている。それにも拘らず放置されてきたと認識。「一部に対応の遅れが指摘される分野もあるが」と無線LANセキュリティ問題を考慮に入れた表現を望む。

(項目3)p.16

「事故前提社会」そのもの、及びそこでの望ましい対応の仕方などについて、一般個人にもわかりやすい形で、意識及び実際の取組を向上するための施策などを検討するべきである。

意見：「検討するべきである」ではなく「検討及び実施するべきである」ではないのか。逃げ腰・曖昧な表現が今回の報告書では目につき、数字に基づく「冷徹」な判断が見えない作文だという非難は外していないと考える。無線LANのPDCAは混乱しきっており、泥沼状態という認識

(項目4)

☆事故前提社会について

事故前提社会という言葉に違和感を覚える。ＰＤＣＡサイクルが無線ＬＡＮセキュ

リティ問題を見る限りにおいて厳密に制度として「確立された。」ものでもなく、常に情報漏えいを引き起こしている無線ＬＡＮという通信形態が正確に論議された形跡もＮＩＳＣには見当たらない。ＮＩＳＣ内部では事実上放置されているものと考えている。専門委員の所属する組織でも暗号化されずに大量導入された無線ＬＡＮネットワークをこの春に運用開始した組織もある。高いレベルでの信頼・そして責任ある施策を実施できるのか日々疑問が積み上げられる毎日である。

長い期間（５年から１０年）情報セキュリティを専門にそして権限を持つ行政官が制度として確立されていない日本において、事故前提社会ということは安全対策の努力を自ら否定したと同義ではないのか。ＮＩＳＣの存在価値すらも否定する言葉であると考えるべきである。経済大国においては情報セキュリティの厳格な運用は経済の発展を阻害するものでしかなく、エネルギーの大量消費・消費物の大量販売によって生活を支えるものである。

経済大国たる日本において事故前提とはＮＩＳＣの安全・安心確保の考え方について問い直す必要がある。「事故前提社会」という定義について、今一度明確にして頂きたい。

事故を想定してその被害を低減する体制を目指すのであれば「情報事故被害低減社会」というべきであり、「事故前提」というのは情報セキュリティ上の犯罪は実際起こるまで放置するという意味にも取られる。ＮＩＳＣが組織として情報セキュリティにおける犯罪行為が公になり問題化するまで放置する事は組織の存在意義にも関わる事である。

事実、無線ＬＡＮセキュリティでは通信事業者の無線ＬＡＮは事実上放置されており、実際侵入して恐喝や業務妨害で書き込み者が逮捕されてもその無線ＬＡＮを提供した側に責任があるにも関わらずに刑事罰も無く被害者からの民事訴訟をも受けないという社会ではどこに利用者の責任と行動が期待できない。むしろそういう事実を放置して、問題化するまでは一切対応しないか実効性の疑われる「表示さえあれば良い」という消極的対応しか見いだせない。ここまで言えるのは、５年にもわたって積み重なった無線ＬＡＮの設置状況をデータとして見てきたからであり、後に示すが無線ＬＡＮのセキュリティに関する認識は広まってもこの1年に具体的には２５人に1人が具

体的な行動に移したともとれる具体的なデータがあるからである。モラル・意識の＜劇的な向上＞とは決して言えない結果に終わったと評価している。

このペースではスマートフォンを始め移動体通信における無線ＬＡＮの利用に関してその成長を止め安全・安心の確保のための厳しい規制が必要となるのは必至であり、無線ＬＡＮ利用における不正行為は爆発的に増え、政府・地方公共団体・企業・個人への恐喝・詐欺行為に多く使われるのは必至である。特に法人・団体の無線ＬＡＮは暗号が脆弱なものが未だに多く、この７月での最新調査でも暗号化無しで使用している団体の無線ＬＡＮが存在する。組織が取り扱うデータを抜き取って下さい・送信データをぜひ勝手に受信して下さいと言っているようなものであり、それらが当該の組織がそのデータを取られて金品を要求される事件が頻発するものと考える。

更に、無線通信における情報の傍受について無線通信を行う者と法的に詳しい者との間でこれまで多くの長い論議を続けて来たが､今だにクリア出来ない問題ががある。（項目５）p. 25

第四に、個人においては、人格形成の途上段階にある児童・生徒（中略）　一つの括りとするか検討する必要がある。意見：児童・生徒における携帯ゲーム機の普及は凄まじく（今年７月までに国内で３０００万台以上出荷)、それを用いた無線LANを通しての恐喝事件や天皇陛下を殺害する予告まで掲示板に書き込まれている。追跡調査を行うとこの様な粗暴な振る舞いを行う児童・生徒は巨大掲示板管理人との確執があったと考えている。掲示板における人権侵害の事例は非常に多く筆者も幾度も無く根拠のない誹謗を受けて警察や法律関係者（弁護士など）に相談した位、酷いものがある。掲示板を管理する側も削除に応じないなど削除を求める側がどの様な立場の人たちであっても掲示板を管理する側を訴えると言った途端に証拠保全と称して削除を放棄する事を繰り返している。この様な行為を児童・生徒が受けた場合の事を考えた場合、天皇陛下の殺害まで示して掲示板管理者を混乱に陥れるという流れは必然あると考える。個人に対する自己防衛は掲示板に関わらないとしか考えられない事態になっている。地元警察からも簡単にそう指摘された。これではもはや公的機関は当てに出来ないと自ら示したと同様である。今後とも「規制強化・法的安全確保」を進め掲示板管理者の逮捕・起訴も含めて徹底した取り締まりを必要とする時代になったと考え

る。例の掲示板管理者は「法律が無い」と言い裁判にも欠席し賠償命令が出ても応じず自らの事業を拡大させていまやネット社会の「カリスマ」として君臨している。掲示板が巨大権力を持ち始め法治国家を標榜する政府も取り込みに失敗しもはや収拾のつかない事態になったと考える。この状況で、情報セキュリティが児童・生徒そして一般市民に行き渡るのか。答えは自ずと見えています。先に示した児童・生徒が行った掲示板での恐喝事件の調査は７月中に終える考えであるが、松本市教育委員会は無線LANのタダ乗りに関して注意喚起はしないという回答を当方として得ている。生徒・児童に対してのPDCAすらそのサイクルは発生せずに放置という結果を招いたと考える。
(項目6)p.33（２）

対策支援主体に係る検討課題社会全体を視野に入れながら、情報セキュリティの観点からのリスクを的確に評価（アセスメント）する機能や、政府機関や社会全体として、どの程度の取組を行ぁば最適な水準の対策を行っていると言えるかといった水準を示す機能、施策対策の取り組み状況や効果を測るとともに取組の向上を支える機能などについて検討を行う。　情報システムに係る事故があった場合の調査や評価を行うとともにシステム自体の信頼性を高める機能に関する検討を行う。対策支援主体として情報関連事業者や地歩自治体の役割に係る検討を行う。意見：無線LANセキュリティという観点から言えばいま深刻な状態に置かれているというのが地方自治体である。最初に無線LANの存在について徹底的な調査を2008年内に行えないのか。新潟県では県組織の一部が未だに無線LANを暗号化無しで運用している可能性がある。現在確認中である。繰り返し注意、警告しても公務員らしい「完全な対応」というのは無線LANにおいてはもはや諦めなければならないと結論は間違っていないと考える。政府は調査の上、無線LANの使用・利用は個人情報を扱わない安全確保等の特定の用途以外全廃するべきである。無線LAN全廃についての法整備はもはや遅れに遅れており緊急避難的な措置であると考える。
(項目７)

☆全体に係る意見法で縛るという事は即通信業界のダイナミズムを奪うという原理主義な考ぁがこの提言でもしばしばみられる。その為、「検討する」という言葉が多用され本当に実行されるのか信用・信頼が出来ないものになっている。多くの通信事

業者・無線LAN製品製造販売業者・無線LAN向けチップ製造販売業者が現在進んでいる無線LAN製品をあらゆる移動通信端末に組み込み世界で年間数千万台、ノートパソコンまで含めると年間一億台を超えていくのではないのだろうか。　NISCも含めて各省庁に大量の情報機器が溢れ返った時代において適切な量の情報機器とその利用について明確なフレームを必要とする。移動体通信において国・地方公共団体・企業・個人及び生徒・児童が必要とする情報機器の数量から点検すべきではないのか。無線ＬＡＮは野放しであることもあり、正確な数字を出すのは難しいが、当方が行ってきた無線ＬＡＮ設置実態調査で大よその数字は出す事ができた。近く公表する予定である。情報機器のバブル状態・資源大量消費から見直し、そこから見積もられる情報犯罪のリスクを洗い出し被害金額や生徒・児童への心理的ストレス等のマイナス面を徹底的に洗い出し「使う」という立場まで見通したコスト見積もりを行うべきである。一つの大きなプロジェクトになるであろう。　有力な新製品が出れば大量販売ができ市場が活性化するとしているが大量の資源がどの様に扱われ消費されゴミになるのかも含めて分析を行い、情報セキュリティの欠落によりどこまで損失が出るのかを国民に分かる形で数値化し公表する作業が必要ではないのか。　当方は情報機器には課税を強化し、安全確保や法整備やそれに基づく組織の運営などを行い混乱した情報通信において一定の秩序確保は緊急命題だと考える。さらに、情報機器の利用に関する消費エネルギーやコストについての基礎となる研究が著しく欠落して個別に苦情や犯罪が起こって個別対応それも一時的な指示程度で収支を繰り返し混乱が拡大している。更にNISCはこんかいの提言で現行の公務員の人事制度では対応できないという事を明らかにしたと考える。　情報セキュリティ政策のガバナンスが脆弱すぎる事を改めて証明したと言って良い。　読み進めていくうちに内閣官房情報セキュリティセンターは一体何ができるのか？と。今回の第１次提言は将来の検討課題ばかり列挙されて、ウォーターフォールでの解決への手順やＰＤＣＡを正確に実行して結果を公表し成果を出すといったダイナミックな施策が出てこない「行き当たりばったり」という痛烈な言葉しか出てこない。この提言を出すような日本の情報セキュリティの大元で多くの問題を解決していく「能力」を持つ組織なのか。疑問が積みかさなるだけである。ましてや無線ＬＡＮの分野についてもＮＩＳＣと関係省庁の間のお手盛り評価という厳し

い評価を当方は下した。更に総務省は今だに某通信事業者単独で第三者が自由に出入りできる無線ＬＡＮが最大７０万台という数字が推測できる状態を放置している。今必要なのはＮＩＳＣと省庁間の綱引きより実効力ある情報セキュリティ対策であり関係法令の厳格化・厳罰化とそして課税である。いわゆる振り込め詐欺の横行で携帯電話会社各社は一体何をしているのかと。どこまで通信事業者が犯罪被害に対して救済などを行わず全て被害者の責任にして更に国の諸法令を盾に保身に走る事を繰り返している。事業者側にも一定の制裁が必要ではないのか。制裁なきところに秩序は無いはずです。　被害額が鰻登りに増大している情報セキュリティ分野で警察庁・防衛省を始めとする治安・国防担当の協力が本当に得られているのか？

一方情報産業・通信業界は国際競争の販売競争激化と技術開発の激化を旗印に情報通信分野での規制先送りを繰り返しているとしか見えない。無線ＬＡＮの分野では無線ＬＡＮの国際流通と国内法との間に壁が厳然と存在しているが、それに関して他国の認証が許せば国内の認証を認める等の大幅な制度改革を進める訳でもなく総務省認定の検査機関を通して複雑な検査を経なければ無線局として許可が下りない制度である。この制度の存在について市民からは苦情は出てくる事は無いだろう。

しかし、海外からの総務省未認可品の日本国内の運用は違法局設置となり電波法第４条&１１０条の違反となり警察が逮捕できる。しかしその検挙例は無線ＬＡＮにおいては逮捕までは行った例について当方は関知していない。現状で無線ＬＡＮは国際親善を推進するものなのか。答えは否としか言えない。消費拡大型の行政における安全確保についての限界を今回の次期情報セキュリティに向けた１次提言にみた。実効性ある提言には財源確保の裏打ちがあってこそ初めて為し得るものである。当方としては最大の提言は　「情報機器の販売・ネット利用における目的税の徴収」「情報機器の販売・ネット利用における規制の強化」「情報機器の販売・ネット利用における罰則の強化」情報機器・ネット利用への課税というタブーを打ち破りこの大きな柱を打ち立てない限り、情報セキュリティ推進について多くが行き詰まるか問題が棚上げになって結局のところ被害拡大を加速させるだけになると警告する。

②　今後、より具体的な調査検討を進めていくに際しての意見。具体的には、対策実施４領域（政府機関・地方公共団体／重要インフラ／企業／個人）横断的な情報セ

キュリティ基盤（技術戦略／人材の育成・確保／国際連携・協調／犯罪の取締り及び権利利益の保護・救済）における、情報セキュリティの観点からの課題と今後の政策への要望

③　その他自由意見（政府以外の主体に求めたいこと、等）に即し、②及び③について無線LANセキュリティ問題の立場から意見を述べる。

意見：国家機関・地方公共団体・企業・個人における無線ＬＡＮ及び総務省の認可を必要とする無線機の実態調査を強く求める。

各機関・団体・企業・個人が所有する無線機が一体どれだけありどの位利用されているのか正確な統計・データが存在しない。総務省データ通信課が示す公衆無線ＬＡＮ利用登録者はＩＳＰ（インターネットサービスプロバイダ）と契約する際に自動的に公衆無線ＬＡＮの登録が行われる為に「利用しなくても利用者として統計上現れる。」というものである。それを日本最大のＩＳＰ事業者行っており、もはや参考にしかならないものである。また通信事業を記録に残す時に多くの注釈を付けなければならない非常に厄介な統計である。いわゆる利用者の「水増し行為」が大手を振って記録に残されている事になる。

市場調査を行う時に現れる国の誤解を招く統計データが正確な実態を知る上で誤解と混乱の元になっていると指摘する。

６月にデータ通信課の意見募集を当方のミスで以下の点を指摘しできなかったために改めてここに示す。

総務省は公衆無線ＬＡＮの根拠となる法令を改正して、実利用者もしくはトラフィック量や利用時間など実需に合わせた統計データを示すべきである。

公衆無線ＬＡＮの定義は総務省と民間の間で異なっており、移動通信課が示した無線ＬＡＮガイドラインに示される「店舗開放型」が民間では公衆無線ＬＡＮとして扱われている。民間で言われる公衆無線ＬＡＮと政府が示す公衆無線ＬＡＮは事なり、電気通信事業者が行う無線ＬＡＮ通信サービスが政府のいう公衆無線ＬＡＮである。

「店舗開放型」の他にも海外で示された本来なら会員以外から有料で無線ＬＡＮを提供するいわゆる「個人所有無線ＬＡＮ開放型」というべきサービスがある。日

本では電気通信事業法違反やＩＳＰの定款に触れる問題で有料サービスは見送られた経緯がある。

政府と民間の間での公衆無線ＬＡＮの定義の混乱は公衆無線ＬＡＮの法的保護の論議を複雑化させており、偽公衆無線ＬＡＮ問題いわゆる悪魔の双子攻撃という情報セキュリティ上の問題解決の糸口すら掴めないのである。

本来ならＩＤ、パスワードをかすめ取る・偽サイトへ誘導しルートキット・スパイウェア等の悪意あるソフトウェアをアクセスする側に侵入させたりなどの攻撃から利用者を守るために偽公衆無線ＬＡＮは法的に禁止・排除される法律があってしかるべきである。しかし、現実には日本では偽公衆無線ＬＡＮを明確に禁止する法律は存在しない。

この夏に一部メディアは公衆無線ＬＡＮが増え、新幹線でも使える事になると公衆無線ＬＡＮを利用しようと盛んに宣伝を行っているが、偽公衆無線ＬＡＮや通信内容の傍受・盗聴そして暗号解読の危険等、無線ＬＡＮならではの脅威に関して一切伏せ利便性のみ強調する宣伝・紹介記事を示してる。当方として、法的保護が脆弱な上に情報漏えいの危険がある以上利便性ばかり示すのは問題であると出版社・担当者に注意を繰り返しているがビジネスの邪魔だとしか考えていないのであろう。無視を繰り返すだけである。

公衆無線ＬＡＮのＳＳＩＤやＷＥＰ鍵は公開されておりその情報はすぐ手に入る。そして公衆無線ＬＡＮの無線ＬＡＮアクセスポイントの成済ましも簡単である。店舗開放型無線LANであれば暗号すら掛っていない。そうなれば接続している利用者の通信データは全て抜き取られてしまうのです。この危険な攻撃を取り締まる法的根拠も脆弱であり、偽公衆無線ＬＡＮを国家として排除し、公衆無線ＬＡＮをビジネスとして支援する事もありませんでした。この偽公衆無線ＬＡＮという電気通信事業法や電波法の枠内では対処できない問題について情報セキュリティ上の立場から「緊急」な対応をお願いしたい。

○国家機関・地方公共団体における無線LAN

国土交通省某地方整備局において、暗号化無しの無線ＬＡＮの設置が引き続き行われている事を確認している。また、国立病院や独立行政法人・大学で無線ＬＡＮが広く設置され、この５月に新規に設置されたと発表があった大学で侵入に対する対策があるが盗聴・傍受に対して対策を取っていない無線ＬＡＮを３０台以上発見して非常に驚いた。

無線ＬＡＮ部分の暗号化すら行わないという事は情報セキュリティ対策を大学としてどうとらえているのかを示す一つの事実でしかないと考える。

地方公共団体でも何度も注意している団体であっても引き続き暗号化無しもしくは暗号解読が簡単な無線ＬＡＮを使用し続けている事例がこの７月も確認している。情報セキュリティ上脆弱な無線ＬＡＮの存在はどこまで底なし沼なのか？地方公共団体の情報セキュリティ確保がどこまで硬直化しているのかを示す事例であり、国家として地方公共団体においては無線ＬＡＮ全廃を真剣に検討して頂きたい。地方公共団体自身が無線ＬＡＮは脆弱で危険である事を知らずに取引事業者の一方的な利点と脆弱性の評価を極小にした営業の犠牲の上に税金を使い情報ネットを構築しているのかを洗い出すしかないものと考えます。

先日のＳＪ２００８において総務省自治政策局の地方公共団体向けの情報セキュリティポリシーガイドライン(H18年9月)を示してＮＩＳＣは当方の主張に反論をしたがそのポリシーを提案したのは当方である。その当方がそれでは間に合わないと言っているのです。真摯に今回の提言を受け止めて頂きたい。

○企業向け

企業向けについては公表を控えたいが酷い実態がある。売れている・セキュリティについて啓発されているだけでは済まない問題が多くあり、厳格な設置基準を設けてＷＥＰ利用の排除を法的に示すべき段階に来ていると提言します。企業であるため実態の公表については差し控えます。

○個人向けには事業者が最も重要である

個人については基本的にインターネットサービスプロバイダと無線ＬＡＮ製造販売会社の対応が全てであると言って良い。例えば大手通信事業者のＡ社の無線ＬＡＮを安全対策のためとして全面撤去した場合、日本の危険極まりない無線ＬＡＮの３分の

１から４分の１が一気に消滅するという調査結果を得ている。また自動暗号化については製品に入っている暗号鍵が有効であるのならこの1年で販売設置されたものについては99.3%という高い確率で暗号化された状態で設置されるという結果を得ている。自ら好んで暗号をしないという設置者は0.7%しか存在しないという結果である。2年前の結果は95％の暗号化率であり4.3%の暗号化率上昇は暗号を外す人が「減った」事を意味する重要な記録である。しかしながらこの上昇はもはや１００％近いものであり暗号を掛けるという啓蒙は十分に行き渡っているものと考えて良いものではないのかと。暗号化無しで出荷して自動暗号化を機能させる製品のこの１年での暗号化率は90.6%という結果を得た。９％の差をどのようにとらえるのか。現在のところ解釈に苦慮している。可能性として９％はそもそも無線LANの安全性を無視しているのかそれとも自動設定に失敗して暗号無しで放置しているのか等があるが、暗号化無しで出荷した製品では９％以上が暗号化無しで設置されるという事実がある。無線LANに係る法律を作るのであれば製品出荷の際、「暗号鍵の有効化」はこの結果から非常に有効であるのは理解できると考える。

つまり、安全対策は通信事業者・無線ＬＡＮ機器販売会社の対応が全てであり、先の大手通信事業者は安全対策をサボタージュして規模拡大・携帯電話との連携に邁進していると公然と非難できる。大手通信事業者は制裁を受けて当然の行為をしている。政府はそれを見逃しており、多くの無線ＬＡＮただ乗り常習者を生み出しても放置しているのは政府の責任であると指摘する。

○個人における無線LAN搭載ゲーム機の深刻な問題

更に日本には脆弱であるＷＥＰのみしか使えないゲーム機が２０００万台以上も国内に氾濫している。無線ＬＡＮアクセスポイントの増加はゲーム機が押上げたと考えられ、実のところ無線ＬＡＮ通信の傍受と暗号解読の容易さから簡単に無線ＬＡＮジャックが可能であり、高校生がそれを実行したらしい書き込みを掲示板で見つけている。このゲーム機問題は後々１０年後にも存在する問題だと考えて良い。ゲーム機販売会社に抜本的な対応を求めたいが、現行法では安全対策強化は出来ないであろう。個人において無線ＬＡＮセキュリティ問題はすでに破たんしているという一つの証左でもある。もはや取り返しのつかない間違いを犯し、その責任をだれも取らない形を

作るために無線ＬＡＮ全体の問題を蓋して無視するしか無いのだろうか。将に異常事態である。本来なら製造メーカーの責任であり、無線LANセキュリティ問題の大手通信会社に次ぐか匹敵する大問題であると。無線LANはビジネスには使えない遊びの世界のものであり情報セキュリティとは無縁であると主張する可能性もある。つまり公衆無線LANや社内無線LANネットワークの存在すら同社は否定する可能性もある。端末数だけで考えればゲーム機が最大の無線LAN端末である。ゲーム機に一定の制限を法的に考えなければならない時が既に来ているのです。無線LANは「ゲーム機のもの」となり、国家機関・地方公共団体・企業等の仕事・ビジネス用途では使用禁止の道を辿るしかなく、ゲーム機向けに設置された無線！LANアクセスポイントは不正なネットワーク侵入を簡単に許しネットの成り済まし詐欺・恐喝行為は減るどころか益々増大し陰湿・険悪化するであろう。○HPC（ハイパーフォマンスコンピューティング）の暗号解読能力に言及を　SJ2008にも指摘したがHPC(ハイパフォーマンスコンピューティング)という市場が昨年急速に立ち上がった。そしてこの夏には乱売合戦の様相を呈してきた。更に次世代機の姿もネット上で情報が乱れ飛んでいるが、来年にはHPC向けに調整されたパソコンで理論値８TFlops（単精度浮動小数点演算）という数字が可能性として見えている。パソコンの価格は30万円程度が見込まれるであろう。現行でHPC向けに調整されたパソコンで理論値4TFlopsが40～50万円程度で構築できる。HPC市場の成立と機器の加速的な進歩については情報セキュリティを考える上で特に注意を払って情報の収集と安全対策について考えなければならない基本的情報である。今回の提言で、数年前のスーパーコンピューターに匹敵かそれ以上の能力を持つ可能性のあるHPCについての評価が無いのは政府とぁてHPCの脅威を正確に評価していないのではないのか危惧する。極端な話来年にはHPC向けパソコンを５台並べてそれぞれ疎結合しクラスタリングシステムとして稼働すれば有名な地球シミュレーターと単純な計算だけなら肩を並べる可能性すらある。今回の提言ではHPCを始めとする暗号解読技術の進歩について政府及び識者の見解を求めなければならないと考える。

１　意見提出者

マイクロソフト株式会社

２　提出意見

該当箇所　28頁、第5章　（1）

意見内容　政府に派遣されるセキュリティ・コンサルタント及び政府がアウトソースする受託事業者等について、透明かつ実践的なガイドラインの策定が必要である。

理　　由　政府機関における情報セキュリティ対策の更なる推進にあたっては、「コンサルタントのような専門家の派遣による補完や能力向上」、及び「専門分野におけるアウトソーシングの戦略的な活用」が検討されるとあり、大変重要な取り組みであると認識している。より適切且つ実践的な取り組みを推進するため、かかるコンサルタント及びアウトソース先の該当要件等については、透明性を確保しつつ、適切なガイドライン等の策定が必要と考える。

該当箇所　7頁、第1章(2)②
10頁、第2章(1)②(ア)
14頁、第2章(2)③

意見内容　コストと利便性とセキュリティのバランスを考慮した適切なIT投資について、より具体性のある明確な提言が必要である。

理　　由　本提言において「事故前提社会」という認識に立ち、対応力強化や説明責任の明確化に向けた施策が検討されているのは大変重要な視点と考える。また、「ITによる人間性の解放 － ITルネサンス」なる考え方も成熟した情報セキュリティ社会のあるべき姿と思われる。しかしながら、一方で「必要な製品やサービス可能なかぎり低いコストで提供されるような環境が必要」と指摘しながら、他方では「コストと利便性のバランスをとりながら最適な水準のセキュリティ対策を実施すること」を推奨されており、本提言としての位置づけにやや矛盾があるばかりではなく、具体的な投資目標については明確な視点があるとは言えない。

該当箇所　20頁、第3章（1）②（イ）（c）

意見内容　セキュリティ水準に準拠し、適切な運用を行っているということを確認するための指針が必要である。また、それら取り組みに省庁の地方局や出先機関、独立法人等も含めるべきと考える。

理　　由　本提言において達成すべき基本目標として「（リスクに対して適切な水準のセキュリティを確保するためには）、適切な水準に関する認識を共有し、対策を確実に行うことが基本となるべき」とあるが、かかる水準への準拠や適切な運用について確実に実施されているということを確認するための指針を示す必要があると考える。また、対策実施主体の1つとなる省庁の地方局や出先機関、独立法人等についても適切に調査されるべきである。

該当箇所　21頁、第3章（1）②（イ）（b）

意見内容　「利益認識型の対策推進」について、具体性がない。

理　　由　本提言において、「利益認識型の対策推進へ軸足を移して行くことの検討も有効である」と指摘されているが、どのようなセキュリティ投資が組織のメリットや強みに転換し得るのか、具体的な例示が必要であると考える。

１　意見提出者

個人Ａ

２　提出意見

（１）情報セキュリティ人材の育成について

・　人材育成については、第一次基本計画で取り上げられ、取組みが進められているところと理解しているが、社会のニーズ総量に対して、供給は全く追い付いていないと言える。

・　問題点は3点挙げられる。

①　情報セキュリティ専門人材の処遇が不十分：先ず需要側ではその必要の認知が進みつつあるが、その価値の経済的評価が未確立で、社会的地位と経済面での処遇が不十分であり、その専門性に社会的・経済的魅力が伴っていない。供給を促す誘因が欠如している。

②　情報セキュリティに関する高等教育機関の未整備：大学等においては一部に高度な研究をする取組がある一方、社会の一線を担うための専門知識を持った学生を育成するカリキュラムや専攻科が全く不足しており、教育機会の供給面で大きく立ち遅れている。

③　学生・社会人にとってのキャリアパスとしての魅力の欠如：①②の現状から、学生や社会人にとってキャリアパス、あるいは専門職業領域としての認知も少なく、魅力がほとんど感じられない状態となっている。現実には、魅力以前に認知自体が極めて低レベルと言える。

・　つまり、社会は価値を評価できない、教育機関は機械を提供できない、個人は認知も低く魅力も感じにくく、また教育を受ける機会もない、という三無状態と言っても過言ではない。

・　第二次計画第1次提言において、人材育成は、政府機関の取るべき対策として、また、児童生徒段階での教育に言及はあるが、広く社会一般における人材育成、教育、然るべき処遇の必要性には触れていない。

・　特に後者の視点は人材育成ではなく、基本的リテラシの確立の視点であり、人材育成の一環に入れると論点を誤る怖れがある。

・　従い、上記「三無状態」をそれぞれ打破するための施策を盛り込むべくテーマ設定をされるよう希望する。
・　具体的施策の案としては、①公的及び民間のセキュリティ関連資格の充実と社会的認知の推進、②公的機関の調達に際しての資格要件への組み入れ、③大学での専攻科への補助や学生への奨学金付与、④内部統制や情報セキュリティガバナンスに関連して情報セキュリティ有資格者の関与が権威となりまたは優位となるような枠組みの整備、⑤情報セキュリティ有資格者に特化した（プレミアムの期待できる）就職・転職市場の形成誘導、等が考えられる。

（2）情報セキュリティ監査の推進
・　経済産業省が情報セキュリティ監査制度を立ち上げて5年が経過する。
・　この間、様々な定義における「情報セキュリティ監査」が行われるようになり、特に地方公共団体での取組みは相当程度浸透しつつあるように見受けられる。
・　その一方で企業における情報セキュリティ監査は、残念ながら普及と呼ぶには程遠い状態である。この間、「情報セキュリティ監査」本来の姿である「保証型情報セキュリティ監査」の枠組みも構築されたが、これまた残念ながら実用には程遠いと言わざるを得ない。
・　原因の一つに同制度の推進を担うNPO日本セキュリティ監査協会の力量如何もあることは否めないが、それ以上に行政の側からの支え、発展させるための取組みが不足していると感じている。
・　一つの課題は、情報セキュリティ監査に対する社会的要請や評価の喚起を、もう少し行政の関与が強い形で推進する必要があるのではないかということ。個人情報保護法の制定により、個人情報保護に関しては過剰反応と言われるほど社会の認知が進んだのに比べると、情報セキュリティ監査制度ならびにそれによる監査に対する社会的認識は弱い。（何でも法律で枠を作ることに対して、私は決して積極的な賛成論者ではないが、官による推奨や誘導は社会を変えるための有力な方法であるのは確かだと思う。）
・　今回の第一次提言の中では、第6章で政府機関ならびに重要インフラににについて

監査への言及はあるが、いずれも間接的な表現であり、セキュリティ対策を確保し促進するための仕組みとしての監査機能の位置づけや重要性の認知には結びつかない。また、民間における情報セキュリティ監査の推進には触れられていない。

- 第二次基本計画においては、情報セキュリティ監査を、社会的対策推進の有力な手段・仕組みとして位置づけ、官民挙げて取り組む視点をぜひ取り上げていただきたい。
- 監査に関するもう一つの課題は、制度を支える両輪の一つである情報セキュリティ監査人制度に対する行政のサポートが極めて弱いことである。監査制度も監査人も社会的認知や地位向上が進まないために悪循環的に縮小スパイラルが働いている。
- 監査人の育成に直接行政がサポートすることの是非は議論あるところと思うが、例えば公共団体の情報セキュリティ監査には監査人資格を有するものの関与を条件とすることは不当ではないであろう。
- 同様に情報セキュリティ監査企業台帳登録に際して、有資格者の確保を条件とすることは合理性があると考えるが、それすら実施されていないことは、行政からのサポートの意志の弱さを象徴しているように思える。
- セキュリティへの配慮が重視される物品や役務の調達において、情報セキュリティ監査の実施済み企業に入札資格を与える等の誘導策を期待したい。

（3）セキュアシステム構築のための学術体系の確立

- ネットワークからのセキュリティ脅威が深刻度を増している。スパムやフィッシングのような社会犯罪型もあるが、システムの脆弱性を衝いて侵入、破壊、情報漏洩、情報窃取を行う犯罪も後を絶たない。
- これらの原因の大半は､そのような攻撃を可能とするシステム側の脆弱性にあり、脆弱性をあらかじめ塞ぐことができれば、このような脅威は大幅に軽減される。
- そもそも論で言えばソフトウェア工学において生産性を優先させた結果、バグを最初から排除する工学的手法の開発を放棄し、人手と経験則とカットアンドトライの手法に依存していたことが問題であるが、ことがセキュリティに関わる場合には

それでは済まず、最初から脆弱性を作りこまない仕組みが非常に重要であるといえる。

- 私はソフトウェアについては素人であるが、その故に構造的におかしいことが客観的に見えると自負している。
- 特にWebアプリケーションは簡易言語により半素人でも見よう見まねで書けてしまう面があり、インシデントが後を絶たない要因になっていると見られる。IPA-JPCERT/CCの早期警戒プログラムでも、OSや汎用アプリケーションの脆弱性以上に、個別Webアプリケーションの脆弱性の指摘が上回っており、指摘しても対策がなされない例も多い。
- プログラミングに際して、セキュアなコードを書くこと、プラットフォームとしてセキュアOSの活用を心がけること等を広く社会に浸透させるべきである。これらは先ず、プログラミングの作法もしくは心得として社会的認知を形成することが必要である。
- そのためのキャンペーンや、どのようなアプローチをすればより安全なコーディングが可能かの知識・ノウハウの開発と普及が当面の課題であり、IPAのような取組み主体の指定、大学・研究機関における研究開発の促進、啓蒙啓発活動等の施策が考えられる。
- より根本的な問題としては、システムが本質的にセキュアなものとして構築できるアーキテクチャの確立、そのための方法論が学術的に体系付けられることが必要ではないかと考えている。このための基礎的な研究を、この際イニシエートされることを期待したい。
- 中期の政策課題という視点で見たときには、このような新たな思想に基づく基礎的研究をテーマとして取り上げてみてもいいのではないか。このような発想に立った研究が成果を生み出せば、ソフトウェア工学の分野では世界に向けての貢献の度合が少ない日本の実績となるのではないかと愚考している。

以上、十分整理されていない文章で恐縮ですが、日頃セキュリティに関わる場で仕事をしている中で感じていることの中から、今回の第一次提言に照らして申し上げたいことを3点に絞って記させていただきました。なんらかお役に立てば幸いです。

１　意見提出者

個人Ｂ

２　提出意見

「次期情報セキュリティ基本計画に向けた第１次提言」を拝読しました。本提言を纏められました、関係各位のご努力に敬意を表します。さて大変に示唆に富む内容ですが、ＩＴが深く生活に浸透している現在、一国民として今後の情報セキュリティを考えた場合、更に以下の視点の追加が必要ではないかと感じております。ご検討頂ければ幸いです。

（１）「『ＩＴ』に係わる技術面・運用面の対策に加えた、人的側面の対策への更なる尽力」の必要性。

基本目標の「ＩＴを安心して利用可能な環境」を読み砕いた場合、「安心して利用可能な『ＩＴ』」に加えて、「安心して利用可能な『ＩＴ環境』」の視点も必要ではないでしょか。つまり「ＩＴ」自体は技術的・運用的に安心して利用可能な環境であっても、それを悪用する人間が居て、結果として「安心して利用可能な『ＩＴ環境』」にならない問題、が急増している事に着目する必要があると思うのです。

具体的には：振り込め詐欺・出会い系サイト犯罪・児童買春・ネットいじめ、脅迫・ネットオークション詐欺

等等人的側面の問題は多発しており、何処までを範疇とするかの議論はあると思いますが、「犯罪のサイバー化」対策に関する視点、またその被害者となる「ＩＴ／情報セキュリティ弱者」対策の検討を加えて頂きたく存じます。

（２）「ＩＴが新たな脅威を産まない・脆弱性を持たない」対策の必要性今後情報家電・ホームネットワークの進展は明白です。

過去家庭のＶＴＲが踏み台になった事例がありましたが、今後ＩＴが入り込んだ情報家電・ホームネットワークの進展により、国民に対するＩＴ脅威が増大する危険があります。特に情報家電・ホームネットワークは国民にとってブラックボックスであり、対策も採れません。脆弱性の無い情報家電・ホームネットワークを提供する事、

更に緊急対応の方法、またそのインフラ造り等、至急検討を開始する必要があると思われます。

１　意見提出者

個人Ｃ

２　提出意見

（１）意見内容：

「事故前提社会」とういう表現について、「事故想定社会」に改めるべき。

（２）理由

「前提」とは、「物事を成す土台となるもの」などが一般的な意味である。社会を成す土台が事故であるという語法は明らかな誤用である。本文中では、たびたび、事故が発生するのは仕方がないと言うわけではないという趣旨の説明を繰り返しているが、その場合の正しい日本語は「想定」である。「事故前提社会」の意味として誤解しないで欲しいとして、上記の趣旨の説明をしているが、そもそも、自らが間違った用語を使っておきながら、誤解しないで欲しいというのは、馬鹿げている。正しい用語を使えば、誤解は誤った用語を使う程には生じない。社会を成す土台が事故であると主張するのでなければ、言葉を改めて、「事故想定社会」などの正しい日本語表現とすべきでさる。この誤用は、貴センターのすべての資料等に従前からあるものであるが、新規のものについて訂正をはかるべきである。誤用しておきながら、いったん使ったものだからという理由で、誤用をそのまま訂正せずに、日本語の意味を不当に異なるものにすりかえた解釈を強いることは、健全な社会を標榜しようとする立場として許されることではない。情報セキュリティにおいてＰＤＣＡなどのマネジメントシステムの構築を促しておきながら、自らが「見直し」もできないということのないように、十分な確認をお願いしたい。

１　意見提出者

個人Ｄ

２　提出意見

【意見内容】　＜１４頁　ＩＴルネサンスについて　＞

「ＩＴルネサンス」「ＩＴからの人間性の解放」「ＩＴによる人間性の解放」と説明全般について、「情報セキュリティ立国」のつながりに唐突感、違和感があります。

本旨は、「セキュアなＩＴ基盤」を前提に「人がＩＴを使いこなす社会」の実現であると思いますが、「ＩＴの利活用」「デジタルデバイド問題」等別のテーマな気がしております。より平易でわかりやすい表記・表現にしたほうがよい、と考えます。

【意見内容】　＜３２頁　重要インフラに係る監査について＞

重要インフラを担う「情報システム・ネットワーク網」について、維持管理する企業はもとより、アウトソーシング・開発を受託している会社に対する直接の点検権を留保し、直轄官庁が点検できるフレームワークが必要である、と考える。

近年、人員削減・コスト削減の悪影響が、モノの質、サービスの質の低下に現れており、経済性の判断をベースとする企業では、サービス水準を維持するための態勢をコストで判断しがちである傾向があると考える。

特に、労働環境に起因するヒューマンエラー、エラー発生からの改善のの仕組み（エラー事例の共有）があるか、とオペレーショナルリスクに対する企業の態勢を点検で問うことが効果的でないか、と考える。

【意見内容】　＜３２頁　重要インフラについて＞

重要インフラを担う「情報システム・ネットワーク網」について、維持管理する企業からの「障害事例」の共有による、社会への還元するスキーム作り（個別の企業内で失敗事例を囲い込まない）が必要と考えます。

企業の内部情報を出すことになるので、第三者性や社会貢献としての文化・意識付けの醸成が必要であり、社会として同種トラブルを発生させない風土作りが必要と考えます。

【意見内容】＜２１頁　政府機関における「特別管理秘密」について＞

特定のシステムについては、独自のアーキタクチャによる国産品による情報システムをベースにする極端な施策があってもよい、と考えます。

オープンな製品については、バックドア等の風聞がありますし、この部分の安心感もあると思います。コスト面等の阻害要因はあるとは思いますが、日本独自のセキュリティ技術をもっていることは、国際的にも評価を受ける部分だと思います。

防衛というレベルでも必要だと思われます。

【意見内容】　＜２５頁　自己防衛できる個人としての意識改革＞

近年の治安悪化に伴い個々人の自己防衛の認識は高まっている。直接的な暴力だけでなく、サイバースペース上の自己防衛について、企業に所属していない一般国民は無防備であると思われる。（企業の所属メンバーは、教育・研修の機会がある）

コンピュータウイルス対策ソフトを導入する必要性を感じずに（そもそも必要だと思っていない）インターネットを利用している一般国民も未だ多いと思われる。

自己防衛できる個人の意識改革が大きなテーマではないか、と思われる。