資料８

基本計画検討委員会　各委員提出意見

目次

※有識者としての各委員の個人的な意見であって所属する組織を代表するものではありません。

内閣官房情報セキュリティセンター基本計画検討委員会
意見募集へのコメント

２００７．０２．０６

（株）CSK ホールディングス　代表取締役
（財）情報サービス産業協会　副会長
有賀　貞一

先日の基本計画検討委員会では、次のような点をお話した。

- 検討の視点が多岐にわたっているので、メリハリを付けて議論する必要がある。
- 情報セキュリティの問題を、ネットワークやエンタープライズソフトの観点から捉える方は多いが、組み込みの観点からの把握も重要である。
- 組み込みソフト、組み込まれない組み込みソフト（サーバサイドからダウンローダブルな組み込み用ソフト）が急増している。またそれらを含めて、従来型のエンタープライズソフトと連動することでトータルに作用する社会システムが増加する。
- 情報セキュリティ確保のため、リモートメンテナンス可能な組み込みソフトの増加を課題として捉えておくべき。
- 情報セキュリティに関する業種ごとのルール・ガイドラインに、真にソフトの側面からの考え方が入っているか疑問。
- ソフトの品質、信頼性に関しては、法律も含む規制が必要ではないか。

以下に、追加でコメントをいくつか。

１）検討すべき項目が多数あるが、国家・社会の運営に支障をきたす**有事における対応**に関する事項と、通常活動として**平時に行うべき事項**を分別してはどうか。

たとえば、重要インフラにおけるＩＴシステムトラブル発生時における、社会活動継続計画（ＳＣＰ：Social Activity Continuity Plan）的なものをまとめるなどが前者である。後者としては情報セキュリティ対策として提示されている大半の事項が当てはまる。

有事の場合は、平時とはまったく違った対応が必要であるが、日本の場合、ややもすると「有事の想定」と「生き残るための作戦つくり」が忌避されやすい。したがって事態が発生してから泥縄的に対応策がとられることから、混乱度合が高まる。たとえば、先般の NHK の番組でも若干取り上げられたが、Pandemic-Flu（パンデミック・フルー：世界規模での鳥インフルエンザ等の疫病発生）の様な事態への対応策策定は十分でない。

米国では、すでに、昨年の 9 月 24 日から 3 週間に渡って金融機関におけるパンデミック・フルーに対する机上演習（シミュレーション）が行われた。米国財務省と証券・金融業協会がスポンサーで、この種のＢＣＰ（ビジネス継続計画）訓練としては過去最大の 2700 金融機関、のべ 1 万人が参加した。1 月 24 日にはその報告書も公開された。

http://www.treas.gov/press/releases/hp769.htm
http://www.treasury.gov/offices/domestic-finance/financial-institution/cip/pdf/pandemic-flu-report-012008.pdf

純粋にＩＴのみの訓練ではないが、ＩＴ関連としても興味深い結果が出ている。
http://it.nikkei.co.jp/business/column/aruga_gyokai.aspx?n=MMIT0z000004022008
（私が関連事項とともにまとめ日経ネットに掲載したもの）

日本においても昨年 2 月 7 日に重要インフラに関する類似の分野横断的演習は行われているものの、会議形式による短期的なものにとどまり、最終報告も明確ではない。

２）パンデミック・フルーレベルまでいかなくとも、
・ 電力供給の断絶
・ 通信回線網に対する物理的なテロ活動
・ 重要インフラ業種への DoS 等のサイバー攻撃
・ 携帯電話の高度化により返ってやりやすくなったサイバー攻撃など
社会活動に大きな影響を与える「有事」に対して、ＳＣＰ・ＢＣＰが出来ているとは言いがたい。また事象が発生した場合に、関連省庁ならびに関連産業・企業が横断的な対応体制を迅速に取れるかどうかは疑問である。

より具体的に事態の発生状況を想定し、**ＳＣＰ・ＢＣＰを作成**し（作成させ）、**シミュレーション訓練**を定期的に行うなどが必要である。その結果、とるべき対応策に新たなものが出てくる可能性が高く、より実践的である。

同じく、現在設定されている重要インフラ 10 業種においては、情報セキュリティに関する安全基準等が制定されていることになっているが、業種内各社のＢＣＰプラスアルファ的なものでは、先述のような有事には対応できまい。

３）個人情報保護や情報漏えい対策、情報セキュリティ教育普及など、平時にやっておくべきことは多いが、情報セキュリティセンターの役割をそちらに重点を置いたものにすべきではなかろう。

平時における活動は関連組織が役割分担をして実施することが可能であるからだ。ＮＩＳＣにおいては各論の抽出、分析、役割分担の想定を行うことは当然であるが、重点的には、できるだけ問題を出さないようにするための**根本対策を議論**し、対応策を講じるべきだ。

より具体的には、
・ ＩＣカード上に生体情報を蓄積し、個人認証に利用するといった危険な方式を再検討することが例として挙げられる。ＩＣカード上に暗号化されているといっても、所詮デジ

タルデータであるから、解読可能なものである。生体情報は個人特有なものであるから、解読されると２度と同じものは使えない（すなわちその個人は地上に存在しないものとなる）という危険性がある。学会等でも危険性をたびたび警告されているが、まじめに議論されないうちに、メーカの宣伝のみが先行する結果となっている。このような状況に事前に指針を出すような活動が望まれる。

・ 類似のものとしては、メモリーやストーレッジデバイスの低廉化で、システム上のいろいろな場所に重要データが蓄積されつつある点が挙げられる。先般の駅自動改札機のトラブルにみられるように、改札機１台、１台のフラッシュメモリにＩＣカードのネガティブ情報を蓄積するというアーキテクチャデザイン自体が問題と思われるが、このような点については議論されず、単なるソフトのバグとして片付けられている。古いアーキテクチャしか取れなかったシステム設計を改めるとともに、システム内でのデータ蓄積・利用・管理のあり方などへの指針が必要である。これらを、企業サイドの自助努力に依存するのみでは無理がある。

などいくつもあげられる。

たとえばソフトウェア・エンジニアリング・センター（ＩＰＡ）などとの連携により、情報セキュリティを保つための品質・信頼性に関するルール・ガイドラインの設定を図るといった活動が要請される。更にはその成果を国際規格等に反映させることも重要である。

以上

2008/02/07

読売新聞東京本社論説委員
井川　陽次郎

今のところ、以下のような点が課題と考えています。

■法制度の整備

最近、コンピューターウイルスの作成者を摘発した例が報じられました。ただ、容疑は著作権法違反でした。ウイルス作成を罰する法律がないことが理由でした。警察の機転は尊重するとして、問題は、ウイルスの作成を罰する刑法の改正案が出ているにもかかわらず放置されていることでしょう。ウイルスの害は甚大です。

やはり重要インフラである鉄道に、特別な法律として「列車往来妨害罪」があることを考えれば、ウイルスについても国会できちんと議論されるよう、提案した政府として適切な対応が求められます。

ただ、課題はこれにとどまりません。情報セキュリティーに関連する法制度は、現在のままで十分なのか、本格的に議論をすべき段階にある、と提案したいと思います。例えばネット事業者が取るべき安全確保のための技術水準を仕様として示して対応を義務づけるということも考えられます。現状では、一見、きちんとつながり、動いているようでも内実は危ういという例もあるようです。利用者には内実がすぐに見えないため、問題が起きても責任を問えない、という実態もあります。

むろん法制度については必要かどうかを含めて多様な意見があります。幅広く、内外で法制度の状況を把握して、対応を検討してみてはどうでしょうか。

■利便性について

現在の情報セキュリティはあまりにも利便性を軽視しているように思います。ただ、どうすれば、これを解消できるか、即効薬は見つかりにくい。そこで、この分野について本格的な研究を政府として後押しすべきではないか、と提案します。これを含めて、情報セキュリティ分野の研究開発は、現状どうなっているのか、検証して、さらに伸ばせる可能性がある分野があれば、支援段を考えてもいいと考えます。

■人材の育成、教育

情報セキュリティ分野の人材育成策が重要ではないでしょうか。この分野の技術者は社会的に、必ずしも重要視されているとは思いません。しかし、優秀な人材が育ち、さらにこうした専門家が一定の発言力を備えていることが、今後の対策等では重要です。

情報セキュリティ基本検討に関するコメント

2008.02.04

大成建設　木内里美

情報セキュリティにはいろいろな事象と広範囲な関連や影響があるため、広い視野と見識から問題を抽出し対策を論じる必要があると感じています。初回の会合でも各委員からも広範な意見が出されましたが、論点の整理のためにもマルチプルな視点での意見集積が重要であろうと考え、思いつくままに感じていることを書き出してみました。したがって既に出ていた意見と被っていたり、体系だった構成にはなっておりませんが、参考意見としてお取り扱い下さい。

■　情報セキュリティの定義に関すること

- 情報セキュリティの定義は情報の「機密性」、「完全性」、「可用性」の確保であるとされてきているが、「可用性」の観点には「止めない運用」も含まれていて、インフラ運用の重要なポイントである。
- 可用性の問題にはソフトウェアの品質が大きく影響している。しかし情報通信産業のなかではその品質を担保する仕組みがない。一定の技術レベルを持った資格者がその資格責任において品質を担保することはない。またパッケージのような第三者ソフトウェア製品を組み込むような場合でも、製品に不具合があってもPL法で求められるような責任はないし、修正プログラムの一方的な配布で片付けられてしまう。
- 情報セキュリティでは攻撃や漏洩問題に視点が偏りすぎる傾向があり、安全・安心に活用する環境をどう維持していくかという広い視野が望まれる。

■　対象とレベル、人材育成のこと：国防危機管理レベル、企業レベル、国民社会レベル

- 第一次基本計画でも対象となる4領域が定められている。重要インフラが官民対応と被るのでカテゴライズとしては違和感があるが、共通課題の枠組みとしては良いと思う。
- ただ実行すべきリスクマネジメントのレベルは大きく異なっていると思われ、特に国防の観点からの安全保障については格別の対策が必要ではないかと思われ、それに対応できる極めて高度な人材育成問題も関わってくる。
- セキュリティ人材育成については、文部科学省で進めている「先導的ITスペシャリスト育成推進プログラム」が本年度セキュリティ人材育成に拡張され、2 校を強化拠点対象校としてわずかな予算配分をしたが、そのプログラムによって求められる人材が育成されるとは考えにくい。
- 経団連では特別高度な情報技術者を輩出できる「ナショナルセンター構想」の提言をしたが、先取的な他国の事例で明白なように、政府が主体的に、積極的に政策として推進する必要性を感じている。
- 電子政府を含む情報通信政策を進めるにあたって、政府機関・地方公共団体で最も欠落していることはITガバナンスであろうと思われる。ITガバナンスによって、「全体最適化」、「リスクコントロール」、「コストコントロール」が適切に行われていない現状を打破しないかぎり、効率的な行政と社会システムの構築は難しい。
- 企業においても同様で、ITガバナンスが確立されている企業とそうでない企業では投資や戦略のアウトプットに大きな差が出ている。ある種の危機感、トップのリーディング（コミットメント）、強力な推進力（推進組織・権限・キーマン）、パートナーを巻き込んだ改善、地道な活動の継続といった成功のための共通要素を、ベストプラクティスをもとに水平展開しなければならない。
- 個人においては、インターネット社会に生きる国民として意識の高揚を図るとともに、安心・

安全の根本になる国民ID管理を躊躇なく行うことではないかと思う。納税番号でも住基ネットの番号でも実質的には個人識別番号を付与しているにも関わらず、監視社会になるという漠然とした懸念意見や様々な事情から明言断行できない実態は、国際社会から「関係のない国」に追いやられていく危惧さえ強く感じる。電子政府やワンストップサービスが進まない大きな要素が国民ID管理にありながら、扱いが聖域化されたようなところに問題を感じている。

- それを進める前提として、行政サイドの情報管理の信頼性の問題がある。この信頼性を向上しなければ、国民の同意を得ることが難しくなるだろう。英国のナショナル・インシュランス・ナンバー、米国のソーシャル・セキュリティ・ナンバー、スウェーデンのパーソナル・ナンバーをはじめとして、近隣の中国でも韓国でも国民ID管理が機能しているのに日本ができていないことは情報セキュリティや国民の安全保障の上でも恥ずべきことである。
- 昨年 11 月 20 日に施行された入国管理における外国人の生体認証でも、即日に何件もの偽造パスポートを発見しており、システムの有効性より不正入国の実態に驚く。国民の安心・安全にはトレーサビリティが要求される時代になったことを強く認識したい。
- また、重要インフラには携帯ネットワークを考慮する必要がある。携帯のネット利用はまだコンシューマが中心でビジネス利用はこれからと思われるが、いずれIP携帯が一般化する段階では携帯のセキュリティ問題は格段に大きくなってくることは間違いない。

■ リスクマネジメントの一部と言う理解：テクニカルとマネジメント

- 情報セキュリティはリスクマネジメントの一つの要素であるが、あまりにも特別な扱いになっているところがあり、他の多くのリスクとのバランスを考慮したほうがよいと思われる。例えば企業では法務リスク、財務リスク、労務リスクが内的リスクとして存在し、社会経済リスクや災害リスクなど外的なリスクにも影響を受けるが、情報セキュリティの位置づけも社内外のリスクとして適切に認識される必要がある。
- リスクマネジメントには体系化されたプロセス概念やリスクコントロールの手法があり、回避ばかりではなく低減や移転や受容などで影響を最小限にすることであるから、しっかりとした分析を行い、リスク対応の手段を選択できるように導く必要がある。
- リスクが大きいものはリターンも多いわけで、情報通信がもたらす社会的な利便性は上手に活用されなければならない。この利便性と情報セキュリティ問題がトレードオフになってはならない。モバイルPCからの情報漏洩が心配されるからといって、携帯すること自体を禁止してしまう企業があるが、それでは知恵がない。だからリスクコントロールによって利便性を損なわないようにするんだという発想が欠けている。
- ITにはどの側面にもテクニカルとマネジメントの要素がある。情報セキュリティにおいても、テクニカルな面とマネジメントの面と両面で考えなければならない。テクニカルな面ではセキュアOS、セキュアプログラミング、セキュアネットワーク、暗号技術、認証技術など様々な技術的対応があり、マネジメントではリスクコントロール、システムオペレーション、意識啓発などの人的なマネジメントなどが考えられる。いずれも高度な人材育成が求められる領域でもある。

■ 情報関連に関わるステイタスの問題

- 情報関連の仕事は総じてステイタスが低いままになっている。一方では社会や経営の重要なインフラと言われながら、仕事も就労者もステイタスが高くない。
- 企業での情報関連業務は、管理業務の機械化処理という支援作業が原点にあった。かなり専門的な知識が必要なことから、それが返って専門組織の孤立化を招いてきた面は否めない。セキュリティ関連はさらに専門性が高く、担当者が孤立化しやすい。必要ではあるが経営や事業のコアではない。それが人事と関連することにより認知を受けずモチベーションを下げていく。

- 1990 年以降、ネットワークが進むにつれ経営や事業のインフラ化が進み、官においても個人においても情報通信の位置づけは激変したが、社会的なステイタスは上がったとは言えない。官においても、情報担当の実態をみれば明らかである。
- これはトップの意識や当事者の意識の問題が大きいことと、ガバナンスを強化することによって認識、権限、コントロールを高めていかないと改善されない。情報産業においても、経営品質を向上させ、取引慣行の改善や生産品質管理などに努力を払うべきである。展望なき産業に優秀な人材は集まってこない。
- 情報産業にはソフトウェア構築士のような概念の品質を担保する仕組みを導入すべきである。品質管理につながる制度的な見直しも必要である。たとえば製造体制報告制度、積算基準、出来高査定などであり、会計制度の見直しから導入されることになった進行基準の適用も品質向上に寄与するものと期待される。

■ 官の役割について

- 官の役割は「国を守る、国民を守る」視点にあり、枠組みも大切であるが実践が情報セキュリティの要であると言える。自らの改善実践と自治体への指導によって情報セキュリティに対する関心を醸成することが肝要である。
- 国民の安全の観点からは、国民ID管理制度に積極的に取り組むべきである。
- 情報通信関連の行政情報ガバナンスを担う組織構造がない。ガバナンス構造は省庁統合で出来るものではなく、全体最適、機能統合、利害調整を行うため省庁間に横串を刺せる独立した権限をもつ必要がある。一つの方法として内閣府に「電子政府センター（仮称）」を置き、政府の情報ガバナンス組織と位置づける。セキュリティセンターはその中に機能を統合する。
- 電子政府センター（仮称）は、国民サービスシステム、行政組織管理システム、情報インフラの政策、計画、実施、監視、評価、改善のサイクルを実践し、地方自治体への指導、支援によってレベル向上を図る。また、セキュリティ管理の容易性からも、効率性からも、コスト削減からも行政組織管理システムは統合し横断的運用が望まれる。

■ 情報セキュリティを難解なものとしない配慮について

- 情報通信関連は用語からして理解を妨げている。企業経営においても経営者の関心をそぐ一つの要因になっている。平易な日本語表現に留意すべきである。
- 情報セキュリティ分野はさらに専門化する技術分野であることから、その傾向が強くさらに平易な表現か、内容をわかりやすくする努力が必要である。
- 例えば状況の説明には類似の事象などを活用して理解を促す。情報セキュリティ問題は関心の高くなっている地球温暖化問題とよく似ている。顕在プロセスやリスクの大きさ、対応の困難性、意識の高揚と日々の積み上げの必要性など共通点が多い。

■ 国際的な目でのベンチマーキング

- ネットワークはグローバルに広がっているわけであるから、日本の事情や論理だけで情報セキュリティを論じても意味がない。常にグローバルな目で検証する必要がある。
- 独自にこだわらず、先進的な事例、制度（ベストプラクティス）について研究し、有効なものは導入するべきである。
- 基本計画としてのレベルを国際的なベンチマークでレビューすることが望ましい。

■ 中小企業への配慮

- 多くの中小企業は情報セキュリティコストに耐えられない、あるいは対応できる人材がいな

いと言うのが実態である。おそらく地方自治体や教育機関などにも同様の事情があるように考えられる。企業では大手が牽引する仕組みづくりが必要である。

- 日本の産業は多くの中小企業の存在で成り立っている。そのパートナー企業のセキュリティレベルが向上しなければ、全体の系としてのセキュリティレベルが向上しない。ツールには共同運営型などの工夫を、人材には育成支援などが望まれる。
- セキュリティ技術についても中小のベンチャーが優れた技術開発をしていたり、海外から注目される技術を持ってきたりしている。ベンチャーインキュベーションの仕組みがしっかりしていない日本では、特に政府や大手企業がこれらの技術を見極めてチャレンジャブルに導入し、ベンチャー支援をすることも重要である。

■ サイバーモラルと国民のセキュリティ教育について

- サイバー犯罪はその芽生えのうちから排除する必要がある。労働災害におけるハインリッヒの法則のように、インシデントを認識して改善排除しアクシデントに至らないようにマネジメントされなければならない。
- 情報セキュリティの脆弱性への対応は、技術的に出来ないように遮断してしまう手法と監視や高度なトレーサビリティによって起こりにくくかつ復帰が容易なようにする手法がある。高度に教育された人間が反対の立場に回れば、高度なセキュリティ侵害を起こせるわけであるから技術や人材育成で問題が解決しないことも明白である。悪意のある行為や犯罪の監視やトレースが確実にできる技術や仕組みはその抑止に効果的である。
- ウェブやネットワークを通じた商行為において、ピクセルタグ、ウェブバグ、ウェブビーコンと呼ばれる仕組みを使ってウェブの参照やメールによって個人情報を一方的に取得する行為がある。プライバシーポリシーに明記してあることもあるが、これらの行為には一定の規制が必要と思われる。
- 同様にパッケージソフトなどにおいても、エージェントソフトを潜り込ませてパソコン内の情報を収集発信させている行為は、本質的にボットと変わりがない。このようなエージェントソフトについては、目的、仕組み、影響、取得している情報など機能開示義務を求めるべきである。また一方的な使用許諾と抱き合わせにするのではなく、その受け入れについて、合意確認も必要と考える。
- 国民のセキュリティ意識の高揚はサイバー犯罪の抑止に有効と考えられる。小学校からの基礎教育と地球温暖化防止活動のチーム・マイナス６％のようなわかりやすい啓発活動が望まれる。

以上

内閣官房 情報セキュリティセンター
基本計画検討委員会事務局 殿

《 基本計画検討委員会 》

今後の検討・審議へのコメント

2008年2月6日

株式会社NTTデータ
代表取締役副社長　重木昭信

はじめに

１月１６日の第一回・基本計画検討委員会でご指示のありました

○　検討の視点として追加すべき事項、重点を置くべき事項、
　その他構成・分類に関する意見

○　対応策や反論など、個々の視点に対する意見

○　その他参考となる事項

に関し

□　検討事項の整理の方針

□　特に重点を置くべき事項

について、意見をご提出させて頂きます。

※　以下の本文中、 pXXという記載は、第一回（1月16日）委員会資料『資料５　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）』の該当ページを意味します。

検討事項の整理の方針

- 検討事項の整理の方針について
  - **全体を通じて、全てを議論するには論点が多く、絞り込みが必要。**
  - 論点の絞り込みや、優先順位付けの観点として
    - **どのような脅威を想定するかというのが対応の基本なので、脅威の明確化から論点を絞るのが良い。**
    - **情報システムの使われ方が、単なる情報処理に止まらずに、情報の管理とコミュニケーションの手段へと変化していることに、着目すべき。**
    - 「規制強化や強制力で、牽引すべき」課題・論点と、「規制緩和、市場原理や自主性で牽引すべき」課題・論点を明確に分けた上で、それぞれ優先順位を決めていくべき。
  - 規制強化と緩和のバランス
    - 情報は共有・活用させることに価値があるものであり、安全だけを強調するのは弊害がある。情報の更なる活用の推進を考える上で情報セキュリティをどう位置づけるか、という観点が重要。
    - 過度のセキュリティ対策によって業務効率の低下、従業員の精神的負担増、委託先企業への負担増などのケースが多々見られる点も問題となってきており、この様な実態を踏まえた検討が必要。
- 第一次基本計画や日本の現状の評価と、今後の検討方針について
  - 基本的な枠組み（4領域＋横断的分野）の定義については、新たに加えるべき領域、分野などは特になく、現状のままで良い。枠組みそのものの議論よりも、より具体的な議論を推進するべき。
  - PDCAサイクルで言えば、第一次基本計画は「PD」のフェーズが中心。第二次基本計画では、「PD」はもちろんのこと、「CA」に力点を置いた計画とすべき。
  - 特に、第一次基本計画の遂行によって、「何が」「どのように」変化したのか？　または変化しなかったのか？という評価をしっかり行うことが重要。
    - 変化したものについては、変化によって生じた効果、問題点を明確にすること。
    - 変化しなかったものについては、その原因の掘り下げをきちんと行なうべき。

特に重点を置くべき事項

- 「100%事前防止意識の払拭」と、対策の充実 （⇒ p5 「4. 100%事前防止意識の払拭 」）
  - 情報セキュリティには、大きく分けて下記の二つの課題がある。
    - 情報の漏洩を守る
    - 情報システムを機能させることを守る
  - **両者とも、「安全に絶対はない」（＝100％安全を前提としない）と認識し、検討・立案するべき。**
    - **守ることだけでなく、万一に備えた対処策の検討が必要。**
    - **絶対の品質を求めすぎると、万一の対応策に対する議論が抜けてしまう。**

（参考） 海外の動向など

- 2007年のIGF（インターネット・ガバナンス・フォーラム）のセキュリティメインセッションでも
  - 「100%未来を予測することは不可能」
  - 「予防だけでなく、事後の対策の重要性」を認め、「セキュア」（事前の予防に注目）で「レジリエント」（事後の対応に注目）なネットワーク

  という考え方が打ち出されている。
- 日本においても、経産省の「情報セキュリティ総合戦略」（2003/10/10） の中で言及されている。具体的には、①事故・事件の回避（予防）、②被害の最小化・極限化、③回復力の最適化を図った対応の徹底化 が謳われている。

特に重点を置くべき事項

- 重要インフラ
  - **単独のシステムで動く時代から、ネットワークで相互に接続されて依存関係にあるシステムを前提として考える必要がある。**
    - **ひとつのトラブルが、他システムへ拡散して大きな被害をもたらすのを防ぐ仕組みも重要。**
      - ≫ 単独では重要インフラと考え難いシステムも、相互依存関係の中で重要インフラと成り得る。
    - **具体的には、インターネットが機能しない場合の対策を重要システムでは考える必要がある。**
  - 大規模な災害、サイバーテロなどを想定した，連携体制の整備が重要。政府関係者、重要インフラ企業のCEO、CIO、CTO、CISO、セキュリティ専門家などが、緊急に連絡を取れるようなインフラの整備を検討するべき。
- 人材育成・適正配置
  - リスクの程度を把握し、その対策の立案・実施（あるいは許容）に関し、適切に判断できる様な人材の更なる育成が急務。
  - セキュリティ人材が大企業や中央省庁だけでなく，中小企業・地方の企業や地方公共団体にも適正に配置・活躍できる様な政策の整備。
- 中小企業への配慮
  - セキュリティ対策コストの肥大化とインセンティブ
    - 各種ガイドラインなど複数の情報セキュリティの指標・基準が併存。
    - セキュリティ対策のコストは中小企業にとって特に非常に重い負担となってきている。
    - セキュリティ対策を強化した企業が社会的に評価され、競争力強化につながるような施策を検討するべき。

基本計画検討について

2008 年 2 月 2 日

ＮＰＯ日本ネットワークセキュリティ協会
下村正洋

１．業種や業態別などによるセキュリティ対策の提示まで踏み込むべきではないか

ある情報がその情報の提供者とその利用者との間でやり取りされる場合、複数の事業者（組織）や人を介して行われる。このとき、それぞれの事業者や人が果たすべき情報に対する責任を明確にすることにより、それぞれの事業者や人がなすべき対策が明確になってくる。これは、裏返して考えるとそれぞれの事業者や人が情報に対してできる対策の限界を示すことでもあり残留リスクを明確にすることでもある。

この残留リスクを利用者に明示することにより利用者はその利用においてリスクを認知することができ、それに対する利用者としてのリスク対策（対策とは言えず、覚悟？かもしれないが）がなされると考える。つまり、社会的コンセンサスの形成を促す。このなすべき対策を実行するために、法の見直し・制度の見直し・必要とされるリテラシー（モラル）教育なども同時に検討し、実行することが必要と考える。もちろん人権や民主主義に対して配慮することは大前提である。

これらの対策は時代の変化、特にＩＴ技術の進展により変更されることが予想されることから、これらの変化に対応してタイムリーに対策の指針を策定し提示する仕組みも検討しなければならない。現在利用できると考えられる制度や組織には、情報共有体制、情報セキュリティ監査制度、ＩＳＭＳ、ＣＣ、公共団体、業界団体等が考えられる。

２．取り残される個人に対して

インターネット利用に対して 4 割以上が不安を感じているという中で、ＰＣや携帯電話だけでなく、情報家電やゲーム機が家庭に広まろうとしている。これらは、単にその本来持っている機能（ＴＶを見る、聞く、遊ぶ）ということのみでなく、これらの装置が情報社会の端末として機能することが当然ながら予見される。

もし、これらの端末を利用できない個人が発生した場合、高度情報社会の恩恵を享受できない個人が出てくるのは明らかである。現在、これらの個人向けのサービスが発生している状況は散見されるが、これらを加速する必要があると考える。

３．脅威などの専門的研究の推し進め

ソーシャルエンジニアリングなどを駆使した攻撃手法を研究し、犯罪者（悪意のある人々）より早く、情報システムを含む社会システムなどの脆弱性を研究することが必要と考え、これらを進めるための体制を作り上げる。このような研究は我が国では忌み嫌われるかもしれないが、国家安全保障も考えると必要ではないか。

また、加えて情報漏洩など事件・事故が発生した後のその影響や実態について調査することも必要である。情報漏洩件数は集計されているが、それによる被害実態（漏洩したことによる謝罪や風評被害ではなく）も追跡しなければならない。

平成 20 年 2 月 4 日

関彰商事株式会社
関 正樹

情報セキュリティに関する現状の課題

（地方の中小企業の見地から）

地方経済は依然として厳しい状況が続いており、最近の日本経済の減速を懸念する予測がこれに追い打ちをかけているように思います。このような中、特に中小の企業においては情報セキュリティ対策の為の投資は最小限に止めざるを得ないのが実情です。

しかしながら、情報セキュリティ対策は地方の中小の企業であるからといって対応せずに済むことでないと考えます。

以下に中小の企業が抱えていると思われる現状の課題と、要望事項を記述いたします。

1．現状の課題（情報セキュリティ対策が進まない理由）

1）利用者のリスク認識不足

少し前まで、パソコンの利用者の中にはウィルスに感染していることに気づかず「最近、パソコンが調子悪い」と言いながら、使い続けている人もいたということを聞いています。結局、利用者にとっては、セキュリティやウィルス被害よりも、今日EXCELが使えるかどうかが重要になってしまっているようです。

2）経営者のリスク認識不足

パソコンやインターネットは日常の事業を進める上で必要なものになっています。しかしITの恩恵の裏に潜むリスクにまだ目を向け切れていないのが現実です。特に小さな企業の経営者からすれば、情報セキュリティに関するリスクよりも、現実は売掛金の回収や資金繰りに関するリスクの方がはるかに高いものになってしまっています。

また、情報流失は内部の人間からとよく言われます。とりわけ退職者が関与する場合が多いと聞いております。退職者のモラルが低下し、情報漏えいにつながっているようです。 一部では、これを防止するために、パソコンのデータを外部媒体にコピーすることを禁止したり、操作の履歴を保存するソフトウェアを導入したりという例もあるようです。社員との厚い信頼関係を保つと同時に、退職した元社員を情報漏えいの犯人にしない配慮も必要であると思います。

3）業務効率とコストの問題

情報セキュリティを確保するためには何らかの対策を実施する上で費用が発生します。導入の際の初期費用と運用コストの両方です。

また、対策を実施することで、業務効率の低下も起こり得ます。

ある企業においては個人情報をファクシミリで送信するのに、

・事前に送信先に電話をし、送信先のファクシミリの前で待機してもらう

・送信の際には送信先の電話番号を2人以上で確認した上で送信する

・送信直後、送信先に電話し間違いなく送信されたか否かを確認する

という手順を定めて実施しています。

重要な個人情報ですからこれくらいの配慮は必要ですが、ファクシミリを使って紙を一枚送信するのに、電話を2回し自分も含め3人を一時的にせよ拘束することになり、業務効率は著しく低下してしまいます。もちろん暗号化等の情報技術を駆使し送信手段そのものを変更すれば効率を高めて漏えいリスクも低減することができますが多大なコストがかかってきます。

難しいですが「何をどこまで行えばよいか」を見極め、業務効率とコストのバランスを考えた施策が必要だと思います。

4）投資効果が見えにくい

弊社は、ISO27001 の認証を取得しました。一部門での取得でしたが、社内のイントラネットの整備費用とあわせて 2,000 万円弱を投じました。中小企業においては決して小さな額ではないと思います。

大きな事故もなく業務を継続できているのは、十分では無いにしろいくらかの備えを行ってきているからであると考えております。投資が直接利益につながる訳ではありませんが、一定の効果をあげているという指標が必要であると感じています。

2. 具体的な要望事項

1） 対策の優先付けの明示化と財政的な補助

ある程度生産性を低下させずに十分な対策を実施するには、それなりの物理的な投資が必要です。できれば、対策を「どこまでやれば十分か」とういう優先付けを明示していただくのと共に、物理的な投資が容易に行える財政補助的な施策があればありがたいと思います。

2） 啓蒙や教育の促進

まだまだ人的側面、特に意識面で十分でないと感じられます。一企業として社内教育を実施していくことは勿論ですが、零細な企業や一般家庭を含む社会全体を啓蒙していく必要があると思います。このような教育を推進していくような施策があればありがたいと思います。

以上

2008 年 2 月 7 日

「第２次情報セキュリティ基本計画」検討の視点について

生活経済ジャーナリスト　高橋伸子

生活者の安心・安全の確保の観点から、次の事項を追加的な意見として提出させていただきます。

〇IT は今や道路や鉄道、上下水道、ガス、電気などと同様に社会的経済基盤と社会的生産基盤を形成するインフラでありライフラインである。そうした認識のもとに、セキュリティについて国民が守るべきこと（個人が行う対策を含む）と、それを脅かす者への罰則、免責など、責任分担のルールや周知徹底をはかるための方策を検討すべき。

〇ネットワークに起因するのか、端末等の不具合に起因するのか、使用法の誤りに起因するのかが容易には判断できないトラブルの増加が懸念される。被害回復や損害賠償などを容易にするための駆け込み寺的な相談窓口や裁判外紛争処理制度などの整備について検討すべき。

〇万全を期しても、かならず事故は起こるとの考えに立って、セキュリティが破られた時の緊急対応について十分な検討を行うべき。その際、物理的な対応のみならず、センシティブな情報の搾取等に対する精神的なケアも対策に入れるべき。

〇重要通信とそうでないもの、という区別、企業と個人、という区別のほかに、弱者保護（高齢者、障害者、こども、その他メディアリテラシーに欠ける者に対する保護））の視点での対策の検討が必要。

〇個人に対する普及啓発、教育の取り組みについては、家庭教育、学校教育、社会人教育に分けて、取り組みの現状を把握したうえで、効果的、効率的に推進する方策を検討すべき。

〇個人については、被害者のみならず、加害者とならないための教育のあり方等の検討を行うべきである。

〇サイバー犯罪に迅速に対応してくれる専門人材の養成と配備に関する検討が必要。

〇情報セキュリティの安全基準の不断の見直しと「危害情報」「注意喚起情報」などの発信に関する検討（主体、経路など）を行うべき。

〇技術で対応すべきことと、法や制度で対応すべきことを切り分けて検討をすすめることが必要。

〇ウイルス対策ソフトウェアをインストールしている消費者のほとんどは、自分たちのコンピュータがサイバー攻撃から守られていると信じているが、システムを実際に調べたらアップデートを適切に行っていた人は52%にすぎなかったという調査結果が米国で発表されている。わが国でもおそらく同じような状況であると考えられる。専門用語の多用など、一般の消費者にはわかりにくいサービス提供に対する改善を事業者にどのように促すかの検討も必要である。　　以上

２００８年2月６日

基本計画検討委員会への意見等

日本銀行　富永 新

１．議論の前提となる条件の明示を

「高度なＩＴ社会」といった、本委員会の議論の前提を、明確に示し、認識を共有化する必要がある。

例えば（事業継続計画を検討する場合の「首都直下地震の被災想定」のように)「X年におけるインターネット普及率、ブロードバンド化率、ネットビジネスの規模、重要インフラのＩＴ依存度、官民双方の情報セキュリティ実施レベル、企業活動のグローバライゼーション状況？・・・」等を、事務局から極力数値で示し、これを所与の前提に置いて議論した方が良い。

また、次期基本計画はどの程度の期間を対象とするのか（上記X年は、３年後なのか、５～１０年後なのか）を明示しないと、各委員の想定するスパンやそれに応じて想定される社会状況が食い違い、その結果、議論が混乱する惧れが大きいと思われる。

２．重要事項や担当分野を絞り込んで議論を

現在、検討ポイントは網羅的に整理されているが、論点が多過ぎて発散しないよう、リスクベースで重要事項を選択して議論する必要がある。検討の視点としては、①国民生活への影響度、②強制の必要性（must か recommended か)、③主体別重要度（国、重要インフラ、一般企業、個人)、④時限性（現在の課題と将来的な可能性)、等があろうが、何に力点を置くのかを、早期に明確にする必要がある。

いずれにせよ、「自己責任原則（前提としての情報開示)」や「市場原理優先（必要最低限の介入)」、「費用対効果重視（経営的視座からの考察)」といったベースライン（基本原則）をしっかりと設定・確認しておきたい。

――　これらの事項に異論がある場合には、ここから議論する必要があろう。

【重要なポイントと対応】

事務局提示の論点（検討の視点）の中では、以下のような点を議論する優先度が高いものと思量。

（１）外部委託（アウトソーシング）と責任の所在問題

――　金融界では外部委託が進んでおり、共同システム（センター）の隆盛もあって、実質的な当事者がＩＴベンダーに移転している状況を踏まえた議論が不可欠。

（２）外部不経済の社会的コストと受益者負担（セキュリティ対策費用の出所）

―― セキュリティや障害対策の必要性をリスク計量的に立証しようとした場合、外部不経済まで算入しない限り、費用対効果は均衡しない。

―― 所要のセキュリティ対策に必要なコストを手数料等に転嫁して良い旨の社会的認識（顧客の受容）が形成されない限り、営利事業上は成り立たない。

（３）ＩＴ障害対策と事業継続

―― 障害対策（品質向上や障害時対応）は、過去にも各種の検討蓄積がある中で、これ以上の検討は限界的である可能性。

―― 従って、一定の確率で大規模なＩＴ障害が起きることを前提に、重要かつ今日的なテーマである事業継続に関し、議論し認識を共有する価値が大きい（但し、地震や新型疫病は対象外）。

（注）こうしたテーマまで「情報セキュリティ」の名（狭義セキュリティ＝機密性を連想され易い）の下で行うのか、名前の変更まで考えるのか、は検討の余地。

一方、以下のようなテーマは、相対的に後順位が適当か。

・「社会環境とＩＴが果たす役割」は、事務局で上記前提条件の一環として設定することが効率的。

・「国家安全保障」や「都市と地域」「担当者任せの幹部」「中小企業問題」といったテーマは議論する実効性に乏しいのではないか。

３．バランスの取れた現実的目標設定を

「ＩＴ障害／ＩＴ利用者の不安ゼロを目指す」といった実現不可能な目標設定は、不適当ではないかと考える（少なくとも「不特定多数の顧客に影響を与えるような重要障害は・・・」とか限定すべき）。コストやリスクテイクとバランスがとれた議論を期待したい。

新技術などＩＴの魅力はリスクと裏腹の関係にあることを理解し、一定のリスクを許容しつつ、適切なコントロールの下でＩＴ利用を図るべきと考える。こうした中で重要なのは、リスクが顕現化した場合の影響を最小限に抑え、迅速に復旧することと、原因究明および再発防止のための仕組みを設けることであろう。

４．各主体毎の性格に応じた議論を

政府や重要インフラなど、しっかりと対策を講ずべきところと、企業・個人等の自主性（市場原理）に委ねるべきところでは、対策に強弱をつけるのが適当と考える。画一的な議論は有効でない。

―― 金融分野で言えば、全銀システム（センター）等、金融決済ネットワークや主要な市場参加者は重要インフラだが、個別の金融機関（特に中小の地域金融機関等）までが各々全て重要インフラなのか、といった点も議論のうえ、定義を明確化する必要があるのではないか。

国レベルで音頭をとった方が効率的に進展するテーマも存在。金融分野で例を挙げれば、キャッシュカードの安全性向上などは、業界横断的なインフラ対応（IC カード化＜磁気カード廃止＞）を要し、顧客の抵抗感も予想されるため、こうした事例に該当すると思われる。ただし、こうしたテーマは限定的であろう。

＜参考資料＞

日本銀行では、考査やオフサイト・モニタリングを通じて得られた知見をまとめた各種ペーパーを公表している。金融界を中心に情報を広く共有し、情報セキュリティ対策や事業（業務）継続体制の整備に資することが目的で、今回の議論でも参考にして頂ければ幸甚である。

＜主な日本銀行公表資料＞

公表時期	資料名・Web サイト
07.9.21	地域金融機関におけるシステム・プロジェクト管理の現状について（地域金融機関 147 行庫へのアンケート調査結果） http://www.boj.or.jp/type/ronbun/ron/research07/ron0709a.htm
07.3.29	業務継続体制の整備状況に関するアンケート（2006 年 12 月）調査結果 http://www.boj.or.jp/type/ronbun/ron/research07/ron0703d.htm
07.3.15	事例からみたコンピュータ・システム・リスク管理の具体策 http://www.boj.or.jp/type/ronbun/ron/research07/ron0703a.htm
06.9.20	金融高度化セミナー「金融機関における業務継続体制の高度化に向けて」 金融機関の業務継続強化に向けた課題と対応 http://www.boj.or.jp/type/release/zuiji_new/data/fsc0609a1.pdf
03.7.25	金融機関における業務継続体制の整備について http://www.boj.or.jp/type/release/zuiji/kako03/fsk0307a.htm
02.6.28	インタビュー「金融機関のシステムリスク動向とその管理について」 http://www.boj.or.jp/type/pub/nichiginq/out033.htm
01.9.12	わが国金融機関におけるシステムリスクの管理状況と留意点 http://www.boj.or.jp/type/release/zuiji/kako02/fsk0109a.htm
01.4.17	金融機関業務のアウトソーシングに際してのリスク管理 http://www.boj.or.jp/type/release/zuiji/kako02/fsk0104b.htm
00.4.18	金融機関における情報セキュリティの重要性と対応策 http://www.boj.or.jp/type/release/zuiji/kako02/fsk0004a.htm

＜主な個人名寄稿＞

公表時期	資料名・Web サイト
07.10.22	金融財政事情 2007 年 10 月 22 日号「システム・プロジェクトの現状から課題を探る」 ― 金融機関主導によるシステムの構築と管理を
07.7.12	リージョナルバンキング 2007 年 7 月号 「金融機関における業務継続体制の強化に向けて」
	＜中略＞

01.12.3	日経コンピュータ 2001年12月3日号「米国同時テロから教訓を得る」 ― 企業の「情報」と「リスク」について再考せよ：金融機関のリスク管理を再考 http://ITpro.nikkeibp.co.jp/article/COLUMN/20070907/281493/?P=5&ST=management （Web掲載07.9.12＜日経BP社ITpro＞）
01.8.13	日経コンピュータ 2001年8月13日号「リスク対策はバランスが肝心」 http://ITpro.nikkeibp.co.jp/article/COLUMN/20071126/287956/?P=1&ST=management （Web掲載07.12.17＜日経BP社ITpro＞）

また、日本銀行金融研究所では、新しい情報セキュリティ技術に関する研究を行っている。金融研究所のWebサイト（http://www.imes.boj.or.jp/）では電子マネー、暗号方式、電子認証、インターネット・バンキング、キャッシュカード、生体認証、等に関する各種論文が多数入手可能である。

―― 個別論文の紹介は割愛するが、こちらも適宜利用されたい。

以 上

情報セキュリティ政策会議　基本検討委員会コメント

平成 20 年 2 月 6 日
東日本旅客鉄道株式会社
深谷　聖治

【会議席上で申し上げた意見】

・業務の内容に応じて様々なシステムの作り方、運用の仕方がある。
・施策の検討にあたって、全体に適用ということで過度に一般化することによって、施策の実効性を低下させることもありうる。
・施策の実効性をいかに確保するかという観点が重要と考える。

・システム障害を起こさない取組みは当然必要であるが、それでも発生した場合の対処、影響範囲の限定、早期復旧なども重要である。

【補足説明】

○　対象とする脅威（リスク）の明確化

・情報システムの脅威として「国民生活及び社会経済活動に多大なる影響を及ぼす脅威」と「利用者の利便性の低下」の事象を混同すべきではない。
・基本計画の対象を「国民生活及び社会経済活動に多大なる影響を及ぼす脅威」に重点をおいて議論したい。
・脅威ごとにセキュリティのレベルがあり一律な施策の実施は情報システムの使いやすさ、サービスの低下を招くことがある。

○　自主性の尊重

・業務の内容に応じてシステムの作り方、運用の仕方があり、提供サービス内容、サービス提供方法なども業種業態によっても異なる。
・施策を一律に適用するのではなく、事業者、分野の特性を踏まえたものにするとともに、自主性を尊重した方が実効性のあがる施策もある。

○　重要インフラ事業者での検討

・鉄道分野も重要インフラ事業者と位置づけられ、第 1 次情報セキュリティ基本計画に基づき、情報セキュリティ対策に係る行動計画を定めると共に、各インフラ分野との相互依存性について分析・検討を行っている。これらの取組みを通じて得られた知見を次期基本計画に反映させていきたい。

第１回基本計画検討委員会コメント

２００８年２月７日

環境省ＣＩＯ補佐官　満塩　尚史

第１回の会議で述べさせて頂いたコメント以外で「検討の視点として追加すべき事項、重点を置くべき事項」に関して、意見を記載しておきます。

● リスク感覚を持った社会文化の構築の必要性

セキュリティの基本概念として、ＯＥＣＤで述べられている「Culture of Security」の概念は、重要であると考える。（誰かが設定したセキュリティポリシーに基づいて）セキュリティ機能を意識しないところに埋め込んで、自動化することは、重要である。しかしながら、この自動化されたセキュリティの場合、短期的には問題ない状況を作ることができるかもしれないが、長期的視点では、人々、企業、社会の新しいリスクに対応する能力を奪ってしまったり、創造的な視点を失わさせる可能性がある。そのため、セキュリティという、狭い範囲でなくても良いので、リスクに関する感覚を持った文化を築くべきであると考える。

このリスク感覚を持った文化を構築することが、リスク回避だけではなく、リスク保有をどう考えるかということつながっていると考える。今、リスクに関する感覚を持った人々や組織が少ないので、すべてのセキュリティの話がリスク回避、リスク転化、リスク軽減になってしまい、リスクを保有してビジネス（社会活動）を行うかを考えない状況が生まれてきているのであると考える。

● セキュリティポリシーの具現化の必要性

具体的なリスク感覚を社会で共有し、政府機関統一基準をはじめとするセキュリティポリシーの具現化を行うためには、以下のことが必要ではないかと考える。

- 共通認識に基づいた共通言語を持つ。

  今日、現在でも、セキュリティに関する用語が、多くの人々の中でイメージが異なっており、議論がかみ合わない状況が多々ある。そのため、用語や言語に対する共通認識が、必要であると考える。このような用語の共通認識は、もっと早期で行うイメージもあると思うが、これまで、このような用語の共通認識を議論する状態でもなかったのではないかと考える。それが、第１次情報セキュリティ基本計画を通じ、社会的にも、技術者でも、それぞれの立場での「気づき」が、一段落し、共通認識を議論できる状態になったのではないかと考える。

- 抽象的な記述の具体的なイメージを作る。

  最近、情報セキュリティポリシーが網羅性、普遍性を確保するために抽象的な記述になっている状況が多々見られる。この抽象化に関しては、一定の理解はできるが、実際の現

場で個々に説明するシーンを考えた場合、かなり、説明しにくい。それと同様に、セキュリティとしての「べき論」は、いろいろな書籍として出版されたり、講演会等でも説明されて理解してもらえるような状況が生まれ始めている。一方、具体的な情報システムのアーキテクチャや設定等は、十分社会的に認知されているという状況ではない。そのため、セキュリティ担当者やSIerの中では、セキュリティポリシーに従った情報システムのアーキテクチャーや設定等の具体的な内容が必要とされ始めていると考える。この状況は米国でも同様であると認識しており、その解決方法の一例としては、米国NISTの「Security Configuration Checklist Repository」活動であると考える。日本においても、一般の人、企業のＩＴ部門、技術者等が、それぞれ利用する情報システムのセキュリティを意識した適切かつ具体的な設定等のrepositoryが必要になってくるのではないかと考える。

- 中小企業（地方自治体を含む）における情報セキュリティ実現方策の検討の必要性

大企業（大組織）における情報セキュリティ対策は、自組織に対するリスク分析を基礎としたISMSを中心に社会として実現されつつあると感じている。一方、中小企業（地方自治体を含む）においては、情報システムは利用しており、情報セキュリティの必要性も認識してはいるもののコスト面や人的リソースの問題から、セキュリティ対策が十分実施できていない状況もあるように感じる。これらの企業や組織の対しては、ISMSのようなリスクベースの対策アプローチだけではなく、ベースライン的な対策アプローチも有効的かもしれない。これまで、組織サイズを考慮したセキュリティ対策の施策は多く見受けられなかったと理解しているが、第２次情報セキュリティ基本計画では、組織サイズを考慮した情報セキュリティ実現方策を検討する必要があるのではないかと考える。
この一例が、前述の「抽象的な記述の具体的なイメージを作る。」につながると考える。

- 更なる人材育成の必要性

人材教育の強化は、重要な検討課題だと考える。人材教育は、昨年の専門委員会での議論も踏まえて、専門家だけでなく、それ以外のユーザ、管理者、セキュリティ専門以外の技術者など、いくつかの分野に分けた教育育成が必要であると考える。
また、分野としてもテクノロジーから運用、法制度までの広範囲の中からバランスを考慮しつつ、それぞれの役割に応じた教育育成が必要である。

- 政府機関におけるチェック機能の必要性

政府機関においては、政府機関統一基準をベースにセキュリティ対策がマネジメントとして埋め込まれ始めている。しかしながら、PDCAサイクルの中でセキュリティに関するチェック機能（特に監査的な機能と指導的な機能）をどのように実効性を確保した上で埋め込んでいくか検討する必要があると考える。

- 政府機関における電子政府構築の活動とNISCの活動の更なる連携の必要性

情報システムのセキュリティは、運用に入ってから考慮すればいいというものではなく、当然ながら企画、構築時から十分考慮すべきであると考える。そのため、政府機関の場合でも、情報システムの企画、構築時からセキュリティも考慮すべきであると考える。現在、政府機関の情報システム企画、構築の活動は、電子政府構築として、ガイドライン等の整備、各省の組織面の整備の推進等が進められている。一方、情報セキュリティに関しては、NISCが中心となり政府機関統一基準をもって各省への導入が進んできている。これらの電子政府構築の活動とNISCの情報セキュリティに関する活動が、十分に有機的に絡み合って活動しているとは言いがたい。今後、情報セキュリティを情報システムの中に具体化していくことを想定した場合、電子政府構築の活動とNISCの活動が、今以上に連携して頂く必要があると考える。

以上

2008/02/12

北陸先端科学技術大学院大学情報科学研究科教授
宮地　充子

第１回基本計画検討委員会 コメント

○　検討の視点として追加すべき事項、重点を置くべき事項、その他構成・分類に関する意見
○　対応策や反論など、個々の視点に対する意見
○　その他参考となる事項

情報セキュリティに関わる解決すべき問題は多岐にわたり，関与する機関も複数であるといえる。しかし、それらの問題を全ての組織及び団体が、完全に放置している分けではなく、独立に取り組んでいる組織及び団体も存在する。

しかし、費用対効果の観点からどこまでその対策が必要か有効か見えないこともあり、恒常的に各組織及び団体での取り組みを期待するのは厳しい。

上記の観点から、情報セキュリティに関わる問題は、一つの横断的な組織で解決のめどがつくまで、恒久的に取り扱うことが望ましいと思われる。この観点で本基本計画検討委員会は何を目的に進めるのか？をまず明確にすべきと思われる。それにより今後議論する内容が変わるといえる。

1. 本検討委員会が情報セキュリティの問題を議論し、その解決方法及び方向性まで決定する委員会を目指すなら、重要問題に優先順位をつけ、優先順位の高い問題から解決方法を議論，あるいは解決すべき組織を明確に（あるいは新たに組織化）することまで進めることが望ましいと思われる。

2. 本検討委員会が情報セキュリティの問題を議論し、政府／国民へ向けて警鐘を促す、あるいは、ガイドラインを作成するのが目的ならば、一歩進めて情報セキュリティの問題を取り扱い，かつ、問題解決の方向性を議論する組織の組織化の提案まで踏み込めることが望ましい。

2008 年 2 月 5 日
綜合警備保障株式会社参与
三輪 信雄

一般に、大企業におけるセキュリティ対策は、ほぼ進んでいるものの中小企業における情報セキュリティ対策は遅れている、と言われています。
中小企業には、「やる気」「お金」「ヒト」のどれもが無い、とされており、そのモチベーションの向上に頭を悩ませているのが現状と思われます。私は、中小企業は取引先大企業から取引条件提示として、情報セキュリティ対策を明示されないと対策が進まないのでは、と考えています。
ちょうど、情報セキュリティ格付け会社がスタートすると聞いておりますが、それもひとつの解であると認識しています。ところが全ての会社がその格付けを受ける、のは本来の対策ではありません。格付けは程度を明確にするものであり、対策そのものではないからです。

まずは、中小企業のセキュリティ対策を推進するには以下が有効と思われます。

・情報漏えい対策の対象は、個人情報だけでなく取引先情報を含む「機密情報」である。
・業務委託元企業(大企業)も業務委託先企業(中小企業)も、お互いに「やってることがわかる対策」があればよい。
・情報セキュリティ業務のアウトソースサービスを利用していることで「やってることがわかる」のではないか？
・そのためには、情報セキュリティ業務のアウトソースサービス(SaaS など)のサービス品質の定義もしくは認証が必要。つまり、情報セキュリティ対策主体の認証ではなく、情報セキュリティサービス提供主体を認証して、それを利用してる企業は安全であろう、という仕組みである。

業務委託先企業は上記サービスを利用していることで、安全で安価なサービスを受けることができ、業務委託元企業も監督業務を簡略化することができ、情報セキュリティコストの削減とレベル向上、そして情報セキュリティ産業の活性化などを同時に実現できるものと考えます。
さらに、上記仕組みは海外の「オフショア」オフィスにおける情報セキュリティ対策をも実現することが出来るので、競争力のある海外進出が可能となります。

上記情報セキュリティ SaaS として有効なものの例には以下が考えられます。

・パソコン操作履歴を外部データセンターに保管
・パソコン操作の中で、外部記憶媒体の利用などのセキュリティポリシーの適用などの遠隔管理
・パソコンデータの保管
・物理セキュリティ(出入管理、監視カメラデータなど)と IT セキュリティ(ログオンや操作記録など)を連動させた統合セキュリティ遠隔監視システム
・ログの遠隔預かりサービス

また、「ログ」と一般的に言われるものの定義が必要と考えています。内部からの情報漏えいは比較的時間的に後になってから発覚することが多く、そのときには必要なログが残されていない、ということが一般的です。原因としては、

・必要なログの種類が定義されていないので、なんとなくログらしきものを取得していると、ログをとっている、とされてしまう。
・ログを保管する期間が短すぎる。
・ログが安全な状態で保管されていない(パソコンの操作ログがパソコンに保管されていたりする)。

などが考えられます。従って、以下のようなガイドラインを「明示」しなければこの問題は解決されないと思われます。

・パソコンの操作ログとしてはファイル名や起動アプリケーションなど必要項目の例示
・ネットワーク監視のログとしては、メールの送信元、送信先
・サーバアクセスログとしては PC 名とファイル名
・ログオン記録は単純なユーザ名だけではなく、カード ID や生態認証、監視カメラやドアの入室記録など本人が否定することを前提とした本人特定データ
・ログは少なくとも１年、推奨は３年

ログというと ISP が実現不可能と主張することがありますが、本提案は各企業の社内におけるデータであり、これらを SaaS で提供することによりコスト負担の少ない仕組みになると考えております。

以上、長くなりましたが、中小企業のセキュリティ対策が少しでもコスト負担の軽い形で普及することを願っております。

2008.2.6

情報セキュリティ政策会議基本計画検討委員会御中

慶應義塾大学教授　安冨　潔

「第２次情報セキュリティ基本計画」（仮称）検討にあたって

第１回検討委員会において事務当局から説明がなされた内容でほぼ集約されていると考えますが，「情報セキュリティ分野における犯罪の取締り，権利利益の保護・救済について」及び「その他の検討の視点（１）（２）」について若干の意見を述べさせていただきます。

１）サイバー犯罪に関する条約について

サイバー犯罪に関する条約は，平成 16 年 4 月 21 日国会において承認され，平成 16 年 7 月 1 日その効力が発生していますが，同条約で締約国に義務づけている実体法・手続法がいまだ国内法として制定されていない状況にあります。これはサイバー犯罪対策への国際協力を果たしていないものであり，早急に立法がなされるべきですが，加えてその実効性ある取締り体制の整備を図るべきと考えます。

２）情報セキュリティと法制度との関係について

情報セキュリティ基本計画となるサイバー空間における保護・救済されるべき権利・利益をどのように考えるかについては，情報セキュリティそれ自体の保護と現行法制度との間における整合性が保たれていないといえます。法制度は，その保護・救済される権利利益（保護法益）の保護を主たる目的として制度設計されますが，情報セキュリティが損なわれた場合にさまざまな権利・利益の侵害が生じうるにもかかわらず，その場合にも情報セキュリティそれ自体が保護法益としてとらえられているわけではありません。保護・救済の対象となる情報セキュリティについての定義を設ける必要があると考えます。なお，その際，既存の法制度との整合性が求められますが，知的財産法の一部を除いて，わが国では伝統的に有体物に化体した情報を保護する制度をとり，情報それ自体を保護するという制度設計にはなっていないことに留意する必要があります。ＩＴ時代の要請にふさわしい「情報」自体を保護法益とする制度を構築することがあってもよいと考えます。その意味で「情報セキュリティ基本法」の策定を積極的に検討していただければ幸いです。

３）その他

情報保護に関する一般的な法制度も検討課題ではあります。もっとも，法益侵害に対する罰則を設けることは，保護法益としての「情報」の性質によって規定されることになると考えますが，刑罰の一般予防的効果は別として，実効性を伴うものとして具体的に規定できるのかは慎重に検討されるべきと考えます。

以上

2008/02/06

監査法人トーマツ
和貝　亨介

社会的規範の必要性

社会の情報セキュリティを大きく担う存在である企業は、事業に支障が生じないよう、過去の自社あるいは他社の事例を参考に、情報セキュリティ対策を講じてきている。しかしながら、それは手探りの状態であり、必要なリスクの検討が不十分であったり、情報機器ベンダーの提案をそのまま受け入れるなど、情報セキュリティ対策に不備不足を生じている場合や過剰な投資をしている場合も少なくない。

これらの原因のひとつは、情報セキュリティ対策を、どのように実施すべきかの規範が十分でないことによると考えられる。投資効果が必ずしも透明でない情報セキュリティ対策については、社会的見地からの規範としての目安の提供も必要である。情報セキュリティ対策をすべての企業に一律に規定することは困難であり、また企業毎の分析に基づかなければならないが、業種、業態、規模等を勘案し、少なくとも情報セキュリティの障害が企業自体、企業の取引先、サービスの利用者等、社会的に広範に、重要な影響を及ぼすものについては、法令等のより拘束性を持った規範の遵守を促すべきであろう。規範的なものとして既にガイドライン、指針等、公表されているものもあるが、より精緻な規定を整備し、情報セキュリティ対策の促進を図っていくべきことが要請される。

規範の遵守に伴って、企業はその説明責任を有することになるが、第１次情報セキュリティ基本計画にも謳われていた情報セキュリティ監査等第三者評価制度の導入も同時に実行されることが求められよう。

個人意識の高揚施策

第１次情報セキュリティ基本計画によれは、「IT 利用に不安を感じる個人を限りなくゼロに」という目標が掲げられている。個人のためにする施策は重要であるが、あわせて個人が積極的に情報セキュリティに関与する意識・姿勢の創成も肝要である。OECD にいう「セキュリティ文化」の実現には、個人の情報セキュリティへの参加が欠かせないであろう。

情報セキュリティ倫理に関する比較的初等の段階からの教育や、個人の利用する情報機器についての情報セキュリティ機能の周知活動など、個人意識の高揚を図るとともに、情報セキュリティ脅威に対する個人の対応についての支援施策も考慮すべきである。緊急時対応における情報セキュリティに関する個人行動について、例えば企業における BCP(ビジネスコンティニュイティプラン)を参考として、個人 BCP(ビヘイビアコントロールプラン)の保持を推進するなど、有用な施策を検討する方向を目指すべきであろう。